



## **Cisco Unified Communications Operating System アドミネストレーション ガイド for Cisco Unity Connection**

リリース 10.x  
2013 年 11 月発行

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

シスコは世界各国 200 箇所にオフィスを開設しています。  
各オフィスの住所、電話番号、FAX 番号は当社の Web サイト  
([www.cisco.com/go/offices](http://www.cisco.com/go/offices)) をご覧ください。

Text Part Number:

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

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

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Unified Communications Operating System アドミニストレーションガイド for Cisco Unity Connection リリース 10.x  
© 2013 Cisco Systems, Inc. All rights reserved.



はじめに	vii
対象読者および使用	vii
表記法	vii
関連資料	ix
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**

<b>イントロダクション</b>	<b>1-1</b>
概要	1-1
ブラウザ要件	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 (Security Configuration)]	1-3
ソフトウェアのアップグレード	1-3
コマンドライン インターフェイス	1-4

---

**CHAPTER 2**

<b>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</b>	<b>2-1</b>
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**

<b>ステータスと設定</b>	<b>3-1</b>
クラスタ ノード	3-1
ハードウェア ステータス	3-2
ネットワークの設定	3-2
インストールされているソフトウェア	3-4
システム ステータス	3-4
IP プリファレンス	3-5

---

**CHAPTER 4**

<b>設定</b>	<b>4-1</b>
IP 設定	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 4-2  
 NTP サーバ 4-2  
 SMTP 設定 4-3  
 時刻設定 4-4

CHAPTER 5

**システム再起動** 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 5-1  
 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  
 証明書と証明書信頼リストの管理 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  
         証明書の再生成 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 6-4  
         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  
         証明書署名要求の生成 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モニタ 6-9  
 IPSEC 管理 6-9  
     新しい IPsec ポリシーの設定 6-10  
     既存の IPsec ポリシーの管理 6-11

CHAPTER 7

**ソフトウェアのアップグレード** 7-1  
 カスタム ログイン メッセージの設定 7-1

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

ここでは、次の項について説明します。

- 「対象読者および使用」 (P.vii)
- 「表記法」 (P.vii)
- 「関連資料」 (P.ix)
- 「マニュアルの入手方法およびテクニカル サポート」 (P.ix)
- 「シスコ製品のセキュリティ」 (P.ix)

## 対象読者および使用

『Cisco Unified Communications Operating System アドミニストレーションガイド』は、Cisco Unified Communications オペレーティング システム のグラフィカル ユーザ インターフェイス (GUI) の使用に関する情報を提供します。

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。

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コマンドライン インターフェイス (CLI) の詳細については、『Command Line Interface Reference Guide for Cisco Unified Communications Solutions』を参照してください。

## 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 <b>太字</b> 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、 <i>イタリック体</i> 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、 <b>波カッコ</b> で囲み、縦棒で区切って示しています。

表記法	説明
[ 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。
	このポインタは、例の中の重要な行を強調しています。
^	^ 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わせは、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

「時間の節約に役立つ操作」です。記述されている操作を実行すると時間を節約できます。

ヒントは、次のように表しています。



ヒント

役立つ「ヒント」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。

## 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](http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html)

## 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。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

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

## 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](http://www.access.gpo.gov/bis/ear/ear_data.html)





# イントロダクション

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」 (P.1-1)
- 「ブラウザ要件」 (P.1-2)
- 「オペレーティング システムのステータスと設定」 (P.1-2)
- 「設定」 (P.1-2)
- 「[セキュリティ設定 (Security Configuration) ]」 (P.1-3)
- 「ソフトウェアのアップグレード」 (P.1-3)
- 「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。」 (P.1-4)
- 「コマンドライン インターフェイス」 (P.1-4)

## 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 8	<ul style="list-style-type: none"> <li>• Microsoft XP service pack 3</li> <li>• Microsoft Vista service pack 2 以降のサービスパック</li> <li>• 最新のサービス パックをインストールした Microsoft Windows 7</li> </ul>
Mozilla Firefox 3.x	<ul style="list-style-type: none"> <li>• Microsoft XP service pack 3</li> <li>• Microsoft Vista service pack 2 以降のサービスパック</li> <li>• 最新のサービス パックをインストールした Microsoft Windows 7</li> <li>• 最新のサービス パックをインストールした Apple MAC OS X</li> </ul>
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

[表示 (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

[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 サーバ (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 設定 (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。

[設定 (Settings) ] > [バージョン (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。

- [バージョンの切り替え (Switch Versions) ] : 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。
- [現在のバージョン (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。
- [システムのシャットダウン (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「システム再起動」を参照してください。

## [セキュリティ設定 (Security Configuration) ]

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。[セキュリティ (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。

- [証明書の管理 (Certificate Management) ] : 証明書、証明書信頼リスト (CTL)、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、および再作成を行うことができます。[証明書の管理 (Certificate Management) ] を使用すると、サーバ上の証明書の有効期限をモニタすることもできます。
- [IPSEC の管理 (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。

## ソフトウェアのアップグレード

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。

[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、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、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、システムで新しいソフトウェア バージョンが実行されません。



(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。このシステムでアップロードおよび処理できるソフトウェアは、シスコによって承認されたものだけです。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「ソフトウェアのアップグレード」を参照してください。

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



## 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 ([戻る (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 Unity Connection Administration の URL を参照します。

**ステップ 2** [Cisco Unified CM の管理 (Cisco Unity Connection Administration)] ウィンドウの右上にある [ナビゲーション (Navigation)] メニューで [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 システムの管理へのログイン (Cisco Unified Communications オペレーティング システム Administration Logon)] ウィンドウが表示されます。



(注) また、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 (Cisco Unified Operating System Administration)] 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** [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 オペレーティング システム 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は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、サブスクリバサーバ上の Cisco Unified CM の管理 ウィンドウで問題が発生します。



(注)

この手順中、物理的にシステムにアクセスできることを確認するために、有効な CD または DVD をディスク ドライブから取り出し、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**

[プラットフォームパスワードのリセットへようこそ (Welcome to platform password reset)] ウィンドウが表示されます。

**ステップ 2** 何か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** 何かキーを押して続行します。

CD または DVD をディスク ドライブから取り出してあるかが確認されます。

**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。

ディスクを挿入したかが確認されます。

**ステップ 6** ディスクが挿入されていることが確認されると、次のいずれかのオプションを入力して続行するように指示されます。

- 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。
- 終了する場合は、**q** を入力します。

**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。

パスワードは 6 文字以上で指定する必要があります。新しいパスワードの強度がチェックされます。パスワードが強度テストにパスしない場合、新しいパスワードを入力するように指示されます。

**ステップ 9** 新しいパスワードの強度が検証されると、パスワードがリセットされ、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に指示されます。

■ 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



## 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」 (P.3-1)
- 「ハードウェア ステータス」 (P.3-2)
- 「ネットワークの設定」 (P.3-2)
- 「インストールされているソフトウェア」 (P.3-4)
- 「システム ステータス」 (P.3-4)
- 「IP プリファレンス」 (P.3-5)

## 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 オペレーティング システムの管理 (Cisco Unified Communications オペレーティング システム Administration) ] ウィンドウで [表示 (Show) ] > [クラスタ (Cluster) ] の順に移動します。
- [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 (Cluster Nodes) ] のフィールドの説明

フィールド	説明
ホストネーム (Hostname)	サーバの完全なホスト名が表示されます。
IP アドレス (IP Address)	サーバの IP アドレスが表示されます。
エイリアス (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。
ノードのタイプ (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 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 オペレーティング システム Administration) ] ウィンドウから [表示 (Show) ] > [ハードウェア (Hardware) ] の順に移動します。
- [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については、表 3-2 を参照してください。

表 3-2 [ハードウェア ステータス (Hardware Status) ] のフィールドの説明

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 が表示されます。
プロセッサ速度 (Processor Speed)	プロセッサの速度が表示されます。
CPU タイプ (CPU Type)	プラットフォーム サーバのプロセッサのタイプが表示されます。
メモリ (Memory)	メモリの合計量が MB 単位で表示されます。
オブジェクト ID (Object ID)	オブジェクト ID が表示されます。
OS のバージョン (OS Version)	オペレーティング システムのバージョンが表示されます。
RAID の詳細 (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。

## ネットワークの設定

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。ネットワーク耐障害性が有効になっている場合、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。ネットワーク耐障害性が有効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 オペレーティング システム Administration) ] ウィンドウから [表示 (Show) ] > [ネットワーク (Network) ] の順に移動します。

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

**ステップ 2** [ ネットワーク設定 (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 [ ネットワークの設定 (Network Configuration) ] のフィールドの説明

フィールド	説明
<b>イーサネットの詳細 (Ethernet Details)</b>	
DHCP	イーサネット ポート 0 に対して 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 のポートがアップしているか、またはダウンしているかを示します。
IP アドレス (IP Address)	イーサネット ポート 0 の IP アドレスが表示されます (ネットワーク耐障害性 (NFT) が有効な場合はイーサネット ポート 1 の IP アドレスも表示)。
IP マスク (IP Mask)	イーサネット ポート 0 の IP マスクが表示されます (NFT が有効の場合はイーサネット ポート 1 の IP マスクも表示)。
リンク検出済み (Link Detected)	アクティブ リンクが存在するかどうかを示します。
キューの長さ (Queue Length)	キューの長さが表示されます。
MTU	最大伝送単位が表示されます。
MAC アドレス (MAC Address)	ポートのハードウェア アドレスが表示されます。
受信済み統計 (RX) (Receive Statistics (RX))	受信したバイト数、パケット数、エラー数に加えて、廃棄、およびオーバーランの統計情報が表示されます。
送信済み統計 (TX) (Transmit Statistics (TX))	送信したバイト数、パケット数、エラー数に加えて、廃棄、キャリア、およびコリジョンの統計情報が表示されます。
<b>DNS の詳細 (DNS Details)</b>	
プライマリ (Primary)	プライマリ ドメイン ネーム サーバの IP アドレスが表示されます。
セカンダリ (Secondary)	セカンダリ ドメイン ネーム サーバの IP アドレスが表示されます。
Optionsosadmin-3-2	設定されている DNS オプションが表示されます。
ドメイン (Domain)	サーバのドメインが表示されます。
ゲートウェイ (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 オペレーティング システムの管理 (Cisco Unified Communications オペレーティング システム Administration) ] ウィンドウから [表示 (Show) ] > [ソフトウェア (Software) ] の順に移動します。
- [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) ] のフィールドの説明

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 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。
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)	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が表示されます。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。
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)	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が表示されます。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 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 オペレーティング システム Administration) ] ウィンドウから、[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については、表 3-5 を参照してください。

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

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 ホストの名前が表示されます。
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た日時が表示されます。
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が表示されます。
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が表示されます。
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が表示されます。
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が表示されます。
アップタイム (Uptime)	システムのアップタイム情報が表示されます。
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表示されます。
メモリ (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。
ディスク/アクティブ (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。
ディスク/非アクティブ (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。
ディスク/ロギング (Disk/logging)	ディスク ロギング用のディスクの容量の合計、空き容量、使用量が表示されます。

## IP プリファレンス

[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)
- 部品番号 (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 オペレーティング システム 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** データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、[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。条件を追加すると、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) ] 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 設定 (IP Preferences) ] フィールドの説明

フィールド	説明
アプリケーション (Application)	ポートを使用 (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)。
部品番号 (Port Number)	数字のポート番号。
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。 <ul style="list-style-type: none"> <li>• [パブリック (Public) ] : すべてのトラフィックが許可される</li> <li>• [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</li> <li>• [非通知 (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</li> </ul>

表 3-6 [IP 設定 (IP Preferences)] フィールドの説明

フィールド	説明
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)	ポートの使用状況のステータス <ul style="list-style-type: none"><li>• [有効 (Enabled)] : アプリケーションで使用されており、ファイアウォールで開かれている</li><li>• [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</li></ul>
説明 (Description)	ポートの使用状況に関する簡単な説明。





## 設定

---

IP 設定、ホスト設定、およびネットワーク タイム プロトコル (NTP) 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。

この章は、次の項で構成されています。

- 「IP 設定」 (P.4-1)
- 「NTP サーバ」 (P.4-2)
- 「SMTP 設定」 (P.4-3)
- 「時刻設定」 (P.4-4)

## IP 設定

[IP 設定 (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。

ここでは、次のトピックについて説明します。

- 「イーサネット設定」 (P.4-1)
- 「イーサネット IPv6 設定」 (P.4-2)
- 「パブリッシャ 設定」 (P.4-2)

## イーサネット設定

[IP 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。

イーサネットの設定はすべて Eth0 にのみ適用されます。Eth1 の設定は設定できません。Eth0 の最大伝送単位 (MTU) のデフォルト値は 1500 です。

IP 設定を表示するには、次の手順を実行します。



**注意**

Cisco Unity Connection の IP 設定を変更するには、次の手順を使用しないでください。

Connection サーバの IP アドレスを変更する方法については、[http://www.cisco.com/en/US/products/ps6509/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html) にある Cisco Unity Connection の「Changing the IP Addresses of Cisco Unity Connection Servers」のアップ

ブグレードガイドを参照してください。

Connection サーバのホスト名の変更する方法については、  
[http://www.cisco.com/en/US/products/ps6509/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html) にある  
 Cisco Unity Connection の アップグレードガイドの「Renaming Cisco Unity Connection Servers」  
 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 オペレーティング システム Administration) ] ウィンドウで、[ 設定 (Settings) ] > [IP] > [イーサネット (Ethernet) ] の順に移動します。
- [イーサネットの設定 (Ethernet Settings) ] ウィンドウの表示。[イーサネットの設定 (Ethernet Settings) ] 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。

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

フィールド	説明
DHCP	DHCP が有効か無効かを示します。
ホストネーム (Hostname)	サーバのホスト名が表示されます。
IP アドレス (IP Address)	システムの IP アドレスが表示されます。
サブネット マスク (Subnet Mask)	IP サブネット マスク アドレスが表示されます。
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 アドレスが表示されます。

## イーサネット IPv6 設定

## パブリッシャ 設定

## 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。



### 注意

Connection が仮想マシンにインストールされている場合は、リスト内で最初のサーバの NTP サーバを変更すると、ライセンス MAC の計算値も変更され、Connection ライセンスが無効になります。

Connection ライセンスの代替を取得する方法については、  
[http://www.cisco.com/en/US/products/ps6509/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html) にある  
 Cisco Unity Connection 10.x のシステム アドミネストレーションガイドの「Managing Licenses in Cisco Unity Connection」を参照してください。



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

[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 サーバの追加、削除、または変更ができます。



(注) 発生する可能性のある互換性の問題、精度の問題、およびネットワーク ジッターの問題を回避するには、プライマリ ノードに指定する外部 NTP サーバが 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は、外部 NTP サーバが NTP v4 でなければなりません。

- NTP サーバを削除するには、該当サーバの前にあるチェックボックスをオンにしてから [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から、[保存 (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、[保存 (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 サーバに変更を加える場合は、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 サーバの設定 (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、[設定 (Settings) ] > [NTP] の順に選択します。



(注) NTP サーバの削除、変更、または追加後には、クラスタ内の他のすべてのノードを再起動して、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。



### 注意

Connection が仮想マシンにインストールされる場合、SMTP ホスト名または IP アドレスを変更すると、ライセンス MAC の計算値も変更され、Connection ライセンスが無効になります。

Connection ライセンスの代替を取得する方法については、[http://www.cisco.com/en/US/products/ps6509/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html) にある

*Cisco Unity Connection 10.x* のシステム アドミニストレーション ガイドの「Managing Licenses in Cisco Unity Connection」を参照してください。



#### ヒント

システムからの電子メール受信する場合は、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 オペレーティング システム Administration) ] ウィンドウで、[設定 (Settings) ] > [SMTP] の順に移動します。  
[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 アドレスを入力するか、または変更します。
- 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.4-2) 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 オペレーティング システム Administration) ] ウィンドウで、[設定 (Settings) ] > [時間 (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 [保存 (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。



## システム再起動

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」(P.5-1)
- 「現在のバージョンの再起動」(P.5-1)
- 「システムのシャットダウン」(P.5-2)

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

[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、[バージョンの切り替え (Switch Versions) ] をクリックします。操作を中止する場合は、[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 オペレーティング システムの管理 (Cisco Unified Communications オペレーティング システム Administration) ] ウィンドウで、[設定 (Settings) ] > [バージョン (Version) ] の順に移動します。
- [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 [リスタート (Restart) ] をクリックします。操作を中止する場合は [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、現在のパーティションのシステムが、バージョンを切り替えずに再起動します。

## 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 オペレーティング システムの管理 (Cisco Unified Communications オペレーティング システム Administration) ] ウィンドウで、[設定 (Settings) ] > [バージョン (Version) ] の順に移動します。
- [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 [シャットダウン (Shutdown) ] をクリックします。操作を中止する場合は [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、すべてのプロセスが中断され、システムが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 Unified Communications Solutions*』を参照してください。
-





## 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」 (P.6-1)
- 「証明書と証明書信頼リストの管理」 (P.6-1)
- 「IPSEC 管理」 (P.6-9)

### 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** [ツール (Tools)] > [インターネット オプション (Internet Options)] を選択します。
  - ステップ 3** [詳細設定 (Advanced)] タブをクリックします。
  - ステップ 4** [詳細設定 (Advanced)] タブの [セキュリティ (Security)] セクションまでスクロールします。
  - 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 (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) [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 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。  
[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 (Find)] コントロールを使用して、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。  
[証明書の設定 (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 [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)] リストの [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 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。  
[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 (Find)] コントロールを使用して、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。  
[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 (File Download)] ダイアログボックスで、[保存 (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](#)
- [証明書の再生成](#)

## 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。[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、「[証明書署名要求の生成](#)」(P.6-7) 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)] を選択します。  
[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 (Find)] コントロールを使用して、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。  
[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)] を選択します。  
[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表示されます。
- 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。



### (注)

Cisco Unified Communications オペレーティング システム で証明書を再生成したら、バックアップを実行して、最新のバックアップに再生成した証明書が含まれるようにします。バックアップに再生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作成されます。
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グローバル固有識別子 (GUID) 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 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証明書信頼リスト (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 サービスアビリティ (Cisco Unified Serviceability)] > [ツール (Tools)] > [サービスの有効化 (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)

信頼証明書は他のクラスタ ノードに自動的に配信されません。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別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** [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。  
[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表示されます。

- 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 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 [ルート証明書 (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。
- [ファイルのアップロード (Upload File)] テキストボックスに、ファイルのパスを入力します。
  - [参照 (Browse)] ボタンをクリックしてファイルを選択し、[開く (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、[ファイルのアップロード (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** [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。  
[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表示されます。
- 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 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 [ルート証明書 (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。
- [ファイルのアップロード (Upload File)] テキストボックスに、ファイルのパスを入力します。
  - [参照 (Browse)] ボタンをクリックしてファイルを選択し、[開く (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、[ファイルのアップロード (Upload File)] ボタンをクリックします。
- 

## ディレクトリの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)] を選択します。  
[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表示されます。
- ステップ 3** [証明書の名前 (Certificate Name)] リストから、[ディレクトリの信頼性 (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 [ファイルのアップロード (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、[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 (ツール) ] > [コントロールセンターの機能サービス (Control Center - Feature Services) ] の順に選択します。
- 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、サードパーティの認証局 (CA) が PKCS # 10 証明書署名要求 (CSR) を使用し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。

	タスク	詳細情報
ステップ 1	サーバに CSR を作成します。	「証明書署名要求の生成」(P.6-7) を参照してください。
ステップ 2	CSR を PC にダウンロードします。	「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します。	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します。	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します。	「証明書のアップロード」(P.6-4) 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します。	「証明書のアップロード」(P.6-4) を参照してください。

	タスク	詳細情報
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	新しい証明書の影響を受けるサービスを再起動します。	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。  <b>(注)</b> 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。

## 証明書署名要求の生成

証明書署名要求（CSR）を作成するには、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)] を選択します。  
[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表示されます。
- 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な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** [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)] を選択します。

- [ 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表示されます。
- 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 (File Download) ] ダイアログボックスで、[ 保存 (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 エンコーディング フォーマットで、CSR は PEM エンコーディング フォーマットで生成されます。また、PEM および DER エンコード形式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してアップロードします。

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、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 [ 証明書のアップロード (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 の信頼性 (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 (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モニタ

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電子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、[セキュリティ (Security)] > [証明書モニタ (Certificate Monitor)] を選択します。
- [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。[証明書の有効期限日の監視 (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)] フィールドの説明

フィールド	説明
通知開始時期 (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。
通知の頻度 (Notification Frequency)	通知の頻度を時間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)	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。
メール ID (Email IDs)	通知の送信先電子メール アドレスを入力します。 <b>(注)</b> システムから通知を送信するには、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 [セキュリティ (Security)] > [IPSEC 設定 (IPSEC Configuration)] を選択します。  
[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、[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 (IPSEC Policy and Association)] フィールドと説明

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。名前には、文字、数字、ハイフンのみを使用できます。
ポリシー名 (Policy Name)	IPsec ポリシーの名前を指定します。名前には、文字、数字、ハイフンのみを使用できます。
認証方式 (Authentication Method)	認証方式を指定します。
事前共有キー (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。
ピア タイプ (Peer Type)	ピアのタイプが同じか異なるかを指定します。
接続先アドレス (Destination Address)	接続先の IP アドレスまたは FQDN を指定します。
宛先ポート (Destination Port)	接続先のポート番号を指定します。
接続元のアドレス (Source Address)	ソースの IP アドレスまたは FQDN を指定します。

表 6-3 [IPSEC ポリシーとアソシエーション (IPSEC Policy and Association) ] フィールドと説明

フィールド	説明
送信元ポート (Source Port)	ソースのポート番号を指定します。
モード (Mode)	転送モードを指定します。
リモートポート (Remote Port)	接続先で使用されるポート番号を指定します。
プロトコル (Protocol)	次のプロトコルまたは Any を指定します。 <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• 任意 (Any)</li> </ul>
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。 <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> </ul>
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。 <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> </ul>
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。 <ul style="list-style-type: none"> <li>• NULL_ENC</li> <li>• DES</li> <li>• 3DES</li> <li>• BLOWFISH</li> <li>• RIJNDAEL</li> </ul>
フェーズ 1 のライフタイム (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。
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。2、1 および 5 から選択できます。
フェーズ 2 のライフタイム (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。
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。2、1 および 5 から選択できます。
ポリシーを有効 (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** [セキュリティ (Security)] > [IPSEC 設定 (IPSEC Configuration)] を選択します。



(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 システムの管理に再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、または無効にするには、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 ポリシーの設定 (IPSEC Policy Configuration)] ウィンドウが表示されます。

b. ポリシーをイネーブルまたはディセーブルにするには、[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横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)] をクリックするとすべてのポリシーを選択でき、[すべてをクリア (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. [選択項目の削除 (Delete Selected)] をクリックします。



## ソフトウェアのアップグレード

### カスタム ログイン メッセージの設定

カスタマイズされたログイン 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 オペレーティング システムの管理 (Cisco Unified Communications オペレーティング システム Administration) ] ウィンドウで、[ソフトウェア アップグレード (Software Upgrades) ] > [ログイン メッセージのカスタマイズ (Customized Logon Message) ] を選択します。  
[ログインメッセージのカスタマイズ (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 ファイルを選択するには、[参照 (Browse) ] をクリックします。
- ステップ 3** [Upload File (ファイルのアップロード) ] 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イン メッセージが表示されます。

- ステップ 4** デフォルトのログイン メッセージに戻すには、[削除 (Delete) ] をクリックします。  
カスタマイズされたログイン メッセージが削除され、システムにデフォルトのログイン メッセージが表示されます。





## 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。

この章は、次の項で構成されています。

- 「ping」(P.8-1)
- 「リモート サポート」(P.8-2)

## ping

[ping ユーティリティ (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 オペレーティング システム Administration) ] ウィンドウで、[サービス (Services) ] > [Ping] の順に移動します。

[リモートの ping (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 を指定した場合は、ping コマンドを入力してもリアルタイムでは ping の日時が表示されません。ping コマンドでデータが表示されるのは、指定した回数の 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。

[リモートの ping (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

[リモート アカウントのサポート (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。この制限時間は、さまざまな値に設定できます。
2. リモート サポート アカウントを設定すると、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 オペレーティング システム Administration)] ウィンドウで、[サービス (Services)] > [リモート サポート (Remote Support)] の順に移動します。
- [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 文字以上にする必要があり、すべてアルファベットの小文字を使用します。
- 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間を日数で入力します。
- デフォルトのアカウントの有効期限は 30 日です。
- ステップ 4** [保存 (Save)] をクリックします。
- [リモート サポートのステータス (Remote Support Status)] ウィンドウが表示されます。[リモート サポートのステータス (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、[削除 (Delete)] ボタンをクリックします。
-

表 8-1 [リモート サポートのステータス (Remote Support Status)] 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)	使用中のデコーダのバージョンが表示されます。
アカウント名 (Account name)	リモート サポート アカウントの名前が表示されます。
有効期限 (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が表示されます。
パス フレーズ (Pass phrase)	生成されたパス フレーズが表示されます。





---

## C

### Certificate Trust List

「CTL」を参照

### CTL

アップロード [6-4](#)

管理 [6-1](#)

---

## I

### IPSec

新しいポリシーの設定 [6-10](#)

管理 [6-9](#)

ポリシーの表示 [6-11](#)

ポリシーの変更 [6-11](#)

ポリシー フィールド (表) [6-10](#)

---

## N

NTP サーバ設定 [4-2](#)

---

## P

ping [8-1](#)

---

## S

SMTP 設定 [4-3](#)

---

## い

イーサネット設定 [4-1](#)

インストールされているソフトウェア

手順 [3-4](#)

フィールド (表) [3-4](#)

---

## お

### オペレーティング システム

再起動 [5-1](#)

ネットワーク ステータス フィールド (表) [3-3](#)

ハードウェア ステータス

手順 [3-2](#)

フィールド (表) [3-2](#)

はじめに [1-1](#)

ログイン [2-1](#)

---

## <

### クラスタ ノード

手順 [3-1](#)

フィールド (表) [3-1](#)

---

## さ

### サービス

ping [8-1](#)

リモート サポート

概要 [8-2](#)

設定 [8-2](#)

### 再起動

現在のバージョン [5-1](#)

---

## し

時刻設定 [4-4](#)

## システム

シャットダウン [5-2](#)

ステータス

手順 [3-4](#)フィールド (表) [3-5](#)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](#)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](#)有効期限モニタ フィールド (表) [6-9](#)パブリッシャ [4-2](#)

## そ

ソフトウェア

インストールされている

手順 [3-4](#)フィールド (表) [3-4](#)

## ね

ネットワーク ステータス

フィールド (表) [3-3](#)

## の

ノード、クラスタ

手順 [3-1](#)フィールド (表) [3-1](#)

## す

## ステータス

システム

手順 [3-4](#)フィールド (表) [3-5](#)

ネットワーク

フィールド (表) [3-3](#)

ハードウェア

手順 [3-2](#)フィールド (表) [3-2](#)

## せ

## 設定

IP [4-1](#)NTP サーバ [4-2](#)SMTP [4-3](#)

イーサネット

手順 [4-1](#)フィールド (表) [4-2](#)時刻 [4-4](#)

## は

バージョン、再起動 [5-1](#)

ハードウェア、ステータス

手順 [3-2](#)フィールド (表) [3-2](#)パブリッシャ設定 [4-2](#)

## り

リモート サポート

ステータス フィールド (表) [8-3](#)設定 [8-2](#)

## ろ

ログイン

概要 [2-1](#)

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>