Cisco Meeting Server

Cisco Meeting Server リリース 3.6

Cisco Meeting Server 2000 設置ガイド

2024 年 4 月 22 日

目次

変更事項

バージョンの日付	変更
2022 年 8 月 23 日	バージョン 3.6 用に更新されました。
2022 年 4 月 20 日	バージョン 3.5 用に更新されました。 スケジューラ コンポーネントのコンテンツを追加しました。
2021 年 12 月 15 日	バージョン 3.4 用に更新されました。
2021 年 9 月 14 日	付録 F を更新して、UCS マネージャのファームウェア バージョンを含めました。
2021 年 8 月 25 日	付録 F に相互運用ページへのリンクを追加しました。暗号化されたコールがライセンスのない状態では処理されないことを明確にするコンテンツを追加しました。
2021 年 8 月 24 日	バージョン 3.3 用に更新されました。 Cisco Meeting Server プラットフォームでサポートされるユーザー数に関する内容を追加しました。
2021 年 5 月 6 日	付録 A の「技術仕様」に「ドライバ仕様」のセクションを追加。
2021 年 4 月 8 日	バージョン 3.2 で更新。 Cisco Meeting Server プラットフォームによるコールキャパシティを更新。
2020 年 11 月 30 日	バージョン 3.1 で更新。
2020 年 9 月 10 日	UCS Manager のアップグレードに関する新しい付録が追加されました。
2020 年 8 月 19 日	バージョン 3.0 で更新。
2020 年 4 月 8 日	**`user evict`** は、Meeting Server 2000 のバージョン 2.9 から使用可能。
2019 年 10 月 25 日	Meeting Server 2000 で使用できない MMP コマンド **`user evict`** を追加
2019 年 8 月 28 日	Meeting Server 2000 が複数のインターフェイスをサポートしていないことを明確にするためのメモを追加しました。
2019 年 8 月 6 日	マイナー修正。 ファブリックの相互接続フェールオーバーの有効化についてのメモを追加しました。
2019 年 4 月 25 日	Call Bridge グループ内の Cisco Meeting Server 2000 におけるフル HD および HD のコール キャパシティの増強と、バージョン 2.6 からの負荷制限の引き上げについて更新しました。
2019 年 3 月 15 日	Cisco UCS B200 M5 ブレード サーバ搭載の Cisco Meeting Server 2000 が M4 搭載のバージョンに置き換わりました。（2019 年初めより）
2018 年 12 月 10 日	Cisco Meeting Server 2000 のコール キャパシティについての情報が更新されました。

1 はじめに

Cisco Meeting Server 2000 は、Microsoft、Avaya など、他のベンダーのさまざまなサードパーティ製品と相互動作する音声、ビデオ、Web コンテンツのスケーラブルな高性能ソフトウェアプラットホームです。Cisco Meeting Server 2000 を使用することで、場所、デバイス、テクノロジーを問わずに、人と人とが結びつくことができます。

Cisco Meeting Server 2000 は、仮想化された導入としてではなく、物理的な展開としての Cisco Meeting Server ソフトウェアを実行する Cisco UCS テクノロジーに基づいています。これにより、より優れたパフォーマンスが得られ、UCS プラットフォームの高パフォーマンス機能を利用できるようになります。

Cisco Meeting Server 2000 は、大量のコールを処理できるように設計されたコア ネットワーク デバイスです。この機能をサポートするために、Call Bridge および Web Bridge コンポーネントのみが設定可能となっています。Cisco Meeting Server 2000 は TURN サーバのエッジコンポーネントが利用できないため、Meeting Server を分散して展開する場合に Edge サーバには適していません。Cisco Meeting Server Web アプリのユーザに対するファイアウォール トラバーサルのサポートが必要な展開では、TURN サーバーを別の Cisco Meeting Server 1000 または仕様準拠の VM サーバーに展開する必要があります。

さらに、レコーダ コンポーネントとストリーマ コンポーネントは、キャパシティの低い Cisco Meeting Server 1000 および仕様ベースの VM サーバに向いているため、Cisco Meeting Server 2000 では利用できません。

Cisco Meeting Server 2000 は、単一の分割サーバー展開のコア サーバーとして、または拡張可能な展開における複数のコアノードの 1 つとして、内部ネットワークに 1 台のサーバーとして展開できます。Cisco Meeting Server 1000、仕様ベースの VM サーバを含む展開の一部として導入できます。ただし、どのサーバも同じバージョンのソフトウェアを実行していることが条件となります。機能と、参加者のユーザ エクスペリエンスは、同じソフトウェア バージョンを実行するすべてのプラットフォームで同じです。

注：

- 仮想化された展開でバックアップを作成し、Cisco Meeting Server 2000 でロールバックすることはできません。この逆もできません。
- Meeting Server は、セキュアブートをサポートしません。

注：2019 年 8 月頃から、新しい Cisco Meeting Server 2000 でファブリック インターコネクト フェールオーバーがデフォルトで有効になる予定です。ただし、手動でデバイスを設定してフェールオーバーを有効にする必要がある場合は、こちらを参照してください。

注：Meeting Server 3.0 では、Cisco Meeting Management 3.0（またはそれ以降）を使用するための必須の要件が導入されています。Meeting Management は、製品登録と、スマートライセンスのサポートに関連するスマートアカウント（セットアップされている場合）とのやり取りを処理します。

1.1 Cisco Meeting Server 2000 の概要

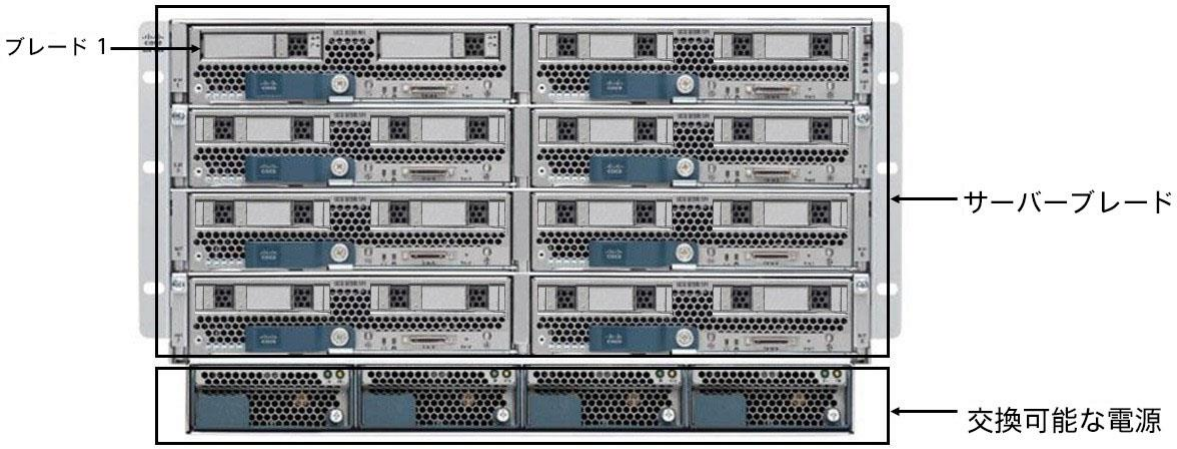
Cisco Meeting Server 2000 は Cisco UCS テクノロジーに基づいており、次の要素で構成されています。

- Cisco UCS 5108 ブレードサーバーシャーシ。シャーシは 6 RU 高であり、ブレード装着時の重量は約 115+ kg（254+ ポンド）です。
- Cisco UCS 6324 ファブリック インターコネクト モジュール 2 台（障害が発生した場合に冗長性を確保するため）。ファブリック インターコネクト モジュールはどちらも Cisco UCS Manager をホストし、実行しており、モジュールを設定できるようになっています。各ファブリック インターコネクト モジュールには、以下が備わっています。
  - 10 Gbps SFP+ ネットワーク ポート 4 つ。両方のファブリック インターコネクトのポート 1 は「アップリンクポート」として設定されており、Cisco Meeting Server のポート A に対応付けられています。ファブリック インターコネクトはどちらもフェールオーバーをサポートするように設定されており、ファブリック インターコネクトのどちらかに障害が発生した場合、Cisco Meeting Server 2000 はもう一方のファブリック インターコネクトにフェールオーバーします。イーサネット ポート 1 がいずれかのファブリック インターコネクトで失敗した場合、ネットワーク トラフィックはもう一方のイーサネット ポート 1 に移動されます。両方のファブリック インターコネクトのポート 4 は、内部使用のために予約されています。ポート 2 と 3 は未使用です。
  - シリアル端末に接続するためのコンソールポート。Cisco UCS Manager を介してファブリック インターコネクト モジュールを設定するために使用します。このポートを使用して、Cisco UCS Manager コマンド ライン インターフェイス（CLI）コマンド経由でシャーシを設定し、制御することもできます。
  - アウトオブバンド 100/1000 Mbps 管理ポート（MGMT というラベル付き）。UCS Manager コマンド ライン インターフェイスおよびグラフィック インターフェイスを使用してシャーシを設定、制御するために使用します。このポートは、MMP シリアルコンソールへのアウトオブバンドアクセスも提供します（「セクション 1.1.1.」 を参照）このポートの使用方法の詳細については、 『Cisco UCS Manager GUI 構成ガイド』を参照してください。
  - USB ポート（現在は未使用）。
- Cisco UCS B200 ブレードサーバー（M5 または M4）8 台。スロット 1 に装備されているブレード サーバには、RAID 1 ミラーとして設定された 2 台のハード ドライブが搭載されています。ブレードサーバー 1 は、Cisco Meeting Server アプリケーションの制御ブレードまたは MMP として動作し、 MMP コマンドラインインターフェイスを使用して設定されます。他の 7 台のブレードサーバにはハードドライブはなく、メディア処理に使用されるため、設定は必要ありません。

- ホットスワップ可能な電源装置 4 台。
- ホットスワップ可能なファン モジュール 8 台。シャーシ全体の冷却を行います。

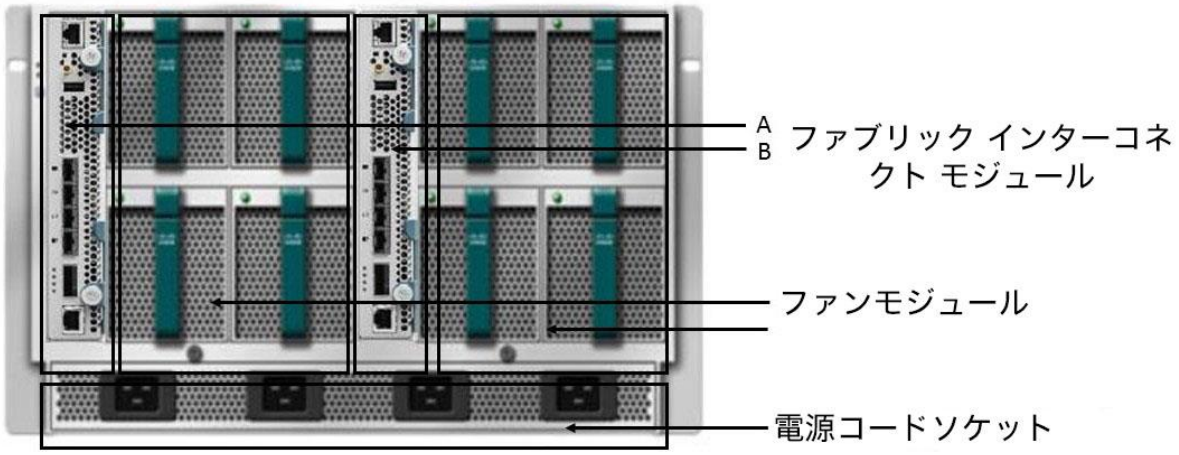
ブレードサーバと電源装置はユニットの前面から設置されています（図 1 を参照）。

図 1：8 台のサーバーモジュールと 4 台の交換可能な電源装置が設置されたユニットの前面



ファブリック インターコネクト モジュールとファンモジュールは、ユニットの背面にある電源装置ケーブルソケットの上に取り付けられています（図 2 を参照）

図 2：ファブリック インターコネクト モジュール、ファンモジュール 8 個、電源装置のケーブルソケット 4 つがあるユニットの背面



冗長性機能に関する注：Cisco Meeting Server 2000 では、Cisco UCS-B プラットフォームで提供されている冗長性機能をすべてサポートしています。これには、ファン、電源装置、ファブリック インターコネクト フェールオーバー、サーバー ブレードの障害、ネットワーク フェールオーバーが含まれます。

- ファブリック インターコネクト フェールオーバー：各ファブリック インターコネクトのイーサネットポート 1 は、フェールオーバーをサポートするように設定されています。ファブリック インターコネクトのいずれかに障害が発生した場合、Cisco Meeting Server 2000 はもう一方のインターコネクトにフェールオーバーします。イーサネット ポート 1 がいずれかのファブリック インターコネクトで失敗した場合、ネットワーク トラフィックはもう一方のイーサネット ポート 1 に移動されます。
- メディア処理に使用される 7 個のメディア ブレード（2 ～ 8 の番号付き）このブレードのいずれかがオフラインになるか削除されると、Cisco Meeting Server 2000 は引き続き実行されますが、容量が少なくなります。スロット 1 のブレード サーバがオフラインになったり故障したりすると、Cisco Meeting Server の MMP とアプリケーションが機能しないため、このブレードは重要です。
- ホットスワップ可能な電源装置 4 台。サーバは 3 台の電源装置でも安全に動作しますが、障害のある電源装置はできるだけ早く交換することをおすすめします。
- ホットスワップ可能なファン モジュール 8 台。シャーシ全体の冷却を行います。ファンに障害が発生するか、ファンモジュールが取り外された場合、ファンのコントローラは温度センサーを使用して、残りのファンの回転速度を上げるかどうかを判断します。

1.1.1 インターフェイスと管理

Cisco Meeting Server 2000 には、Cisco Meeting Server プラットフォーム、アプリケーション層、Cisco meeting Server ソフトウェアの下にある物理ハードウェア プラットフォームの 3 つの層があります。

- Cisco Meeting Server のプラットフォーム層は、メインボード管理プロセッサ（MMP）コマンド ライン インターフェイスを使用して設定されます。MMP は、低レベルのブートストラップ、および Cisco Meeting Server コンポーネント（Call Bridge、Web Bridge、データベース）の構成に使用されます。Cisco Meeting Server 2000 では、ブレード 1 はサーバの MMP として動作します。Serial over LAN（SoL）接続は、MMP にアクセスするために提供されています。SoL を使用すると、シャーシへの物理的アクセスは必要ありません。MMP にアクセスする前に、ファブリック インターコネクト モジュールのネットワーク設定を構成する必要があります（セクション 3 を参照）。ファブリック インターコネクト モジュールを設定すると、SSH を使用して MMP にログインできます。

- Cisco Meeting Server のアプリケーション層は、独自の設定インターフェイスを備えたこの管理プラットフォーム上で実行されます。アプリケーション レベルの管理（コールとメディアの管理）は、Cisco Meeting Server の Web 管理インターフェイス、REST API、またはその両方を通じて実行されます。API は、Web 管理インターフェイスを介してルーティングされます。MMP の初期設定時に、管理者はネットワーク インターフェイスを定義し、IP アドレス（「A」ネットワーク インターフェイスというラベル付き）を割り当てます。この MMP ネットワーク インターフェイスは、アプリケーション層とその管理インターフェイス（Web 管理インターフェイスと REST API インターフェイス）にアクセスするために使用されます。Cisco Meeting Server 2000 では、この「A」ネットワーク インターフェイスは、ファブリック インターコネクト モジュールのポート 1 に設定されているアップリンクを介して外部ネットワークに接続される仮想接続です。

  注：Cisco Meeting Server 2000 プラットフォームでは複数のインターフェイスをサポートしていません（つまり「ipv4 b| c | d」の設定は Cisco Meeting Server 2000 プラットフォームではサポートされていません）。

- ハードウェア プラットフォームは、Cisco Meeting Server ソフトウェアをホストします。Cisco Meeting Server 2000 の場合、これは UCS Manager を介して管理される UCS シャーシです。UCS Manager は、シャーシに取り付けられたファブリック インターコネクト モジュールのクラスタ ペア上で動作し、自己完結型です。ハードウェア、またはハードウェアが提供する仮想要素を設定する場合は、UCS Manager のコマンド ライン インターフェイスまたは Web インターフェイスを介して管理が行われます。UCS Manager インターフェイスには、ファブリック インターコネクト モジュール上のシリアル コンソールまたはアウトオブバンド 100/1000 Mbps 管理ポートからアクセスします。

  注意: プラットフォーム (UCS シャーシによって管理される UCS シャーシおよびモジュール) が最新のパッチで更新されていることを確認してください。CiscoUCS Manager ファームウェア 管理ガイドの指示に従ってください。プラットフォームが最新の状態に維持されていないと、Cisco Meeting Server のセキュリティが低下する場合があります。

ヒント：Cisco Meeting Server 2000 を設定する際は、実行する設定タスクにどの層を使用するかを理解し、適切なネットワーク接続を使用することが重要です。

1.2 本ガイドの使用方法

このガイドは、Cisco Meeting Server 2000 および Cisco Meeting Server ソフトウェア用に提供されているマニュアル セットの一部です。詳細については 図 3 を参照してください。

このガイドでは、以下の内容について扱います。

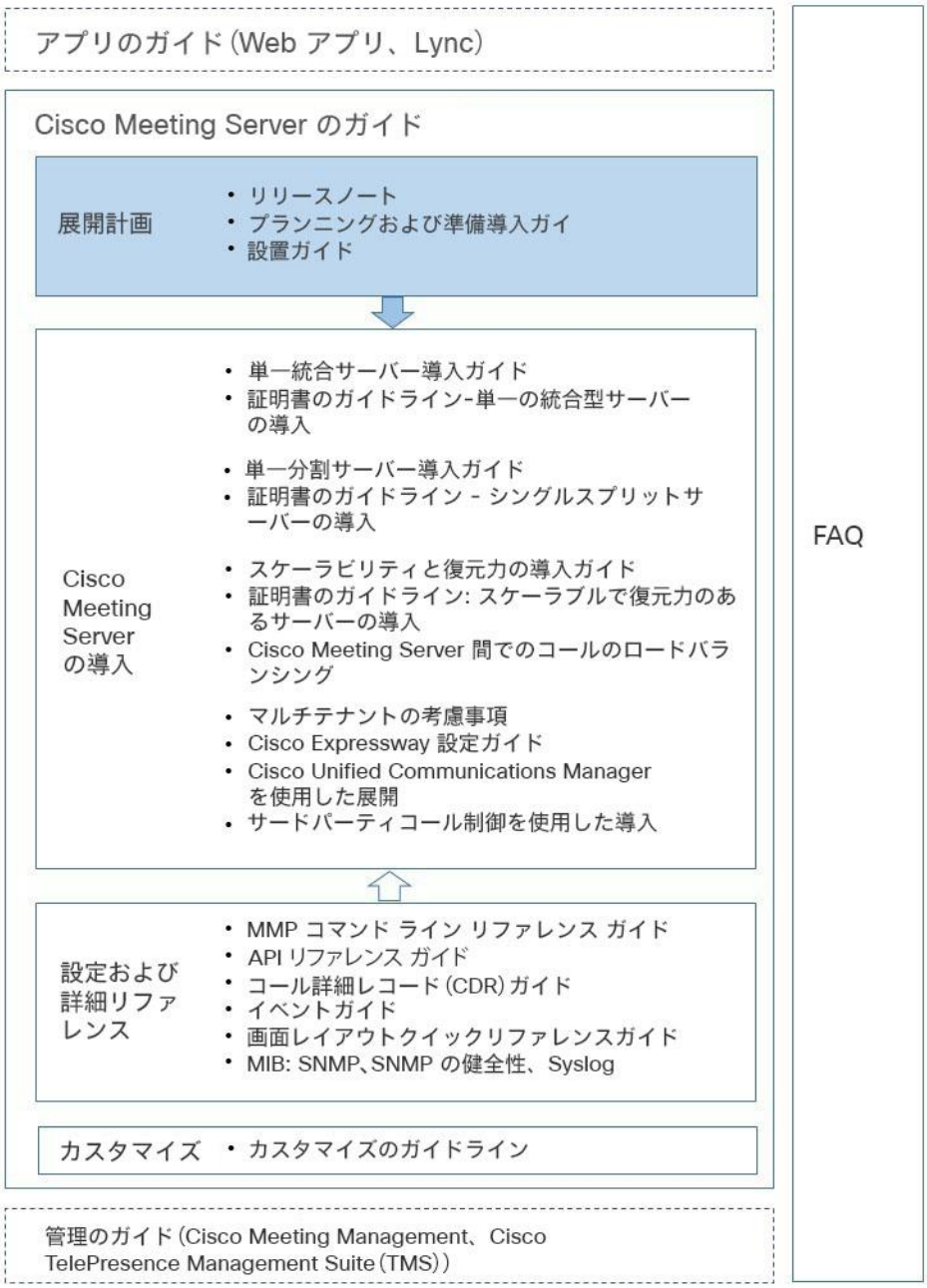
- Cisco Meeting Server 2000 の物理的な設置については、第 2 章を参照してください。
- ファブリック インターコネクト モジュールの構成については、第 3 章を参照してください。
- MMP へのアクセスをセットアップし、Call Bridge を構成する方法については、第 4 章を参照してください。
- 購入したライセンスとアクティベーション コードを Call Bridge にアップロードする方法については、第 1 章を参照してください。

次に、導入環境に合わせて Cisco Meeting Server を設定する必要があります。詳細については図 3 の導入ガイドを参照してください。

1.2.1 コマンド

このドキュメントでは、コマンドは黒文字で示されており、表示どおりに入力する必要があります。ただし、山括弧 <> で囲まれているパラメータについては、適切な値に置き換えてください。サンプルは**青文字**で示されており、導入環境に合わせて変更する必要があります。

図 3：Cisco Meeting Server のインストールおよび展開用ドキュメント



2 サーバのインストール

2.1 概要

この章は、次の項で構成されています。

- Cisco Meeting Server 2000 を 19 インチのラック システムに設置する。
- ケーブルと電源装置を接続する。

2.2 ラックシステムへのシャーシの取り付け

Cisco Meeting Server 2000 は 8 台のブレード サーバがすべて取り付けられた状態で出荷されており、重量およそ 115+ kg（254+ kg）です。**各ブレードサーバの出荷時のスロットをメモしたうえで**、ブレード サーバをスロットから慎重に取り外します。取り外したブレードは、シャーシを業界標準 19 インチのラックシステムに設置している間、安全な場所に保管することをお勧めします。シャーシには 6 RU のスペースが必要です。

ヒント：各ブレードに出荷時のスロット番号をラベル付けしておくと、シャーシをラックに取り付けた後、どのスロットに再び取り付けるかを確認できます。どのブレードがどのスロットに入るかをメモし忘れた場合、取り付けに余分な時間と設定が必要になります。

警告：少なくとも大人 2 名で持ち上げ、シャーシをラッキングシステムに取り付けます。シャーシは非常に重いため、大人 1 人で持ち上げるのは危険です。

シャーシを取り付けたら、各ブレードをシャーシに注意深く挿入し直して、2 台のハードディスクを搭載したブレードサーバーがスロット 1 に挿入されていることを確認します。66 ページの *「スロット間のブレードサーバーのスワッピング」*にある手順に従う必要がない場合、その他のブレードは出荷時と同じスロットに挿入し直すことをお勧めします。

次の項目については、『Cisco UCS 5108 ブレードサーバーシャーシ設置ガイド』の指示に従ってください。

- シャーシの外部に必要な周囲温度範囲
- シャーシの移動方法
- シャーシへのレールの取り付け
- ラックへのシャーシの取り付け
- 電源装置の接続

詳細については、以下を参照してください。

- シャーシからのブレード サーバの取り外し
- ブレード サーバの取り付け
- ブレード サーバの前面パネルにある LED の意味
- リセット ボタンの使用
- ブレードサーバの技術仕様

必要に応じて、『Cisco UCS B200 M5 ブレードサーバー設置/サービスノート』または『Cisco UCS B200 M4 ブレード サーバー設置/サービスノート』の手順に従ってください。

2.3 Cisco Meeting Server 2000 をネットワークに接続するために必要なもの

- ファブリック インターコネクト モジュールの管理ポートに接続するための 100/1000 スイッチ ポート 2 つ。
- 各ファブリック インターコネクト モジュールのポート 1 に接続するための 10 Gbps スイッチ ポート 2 つ。
- 5 つの IP アドレス:
  - 3 つの静的 IP アドレス（各ファブリック インターコネクト上の管理（MGMT）ポートにつき 1 つと共有アドレス 1 つ）。これらの IP アドレスは、管理 VLAN 上に設定する必要があります。詳細については、セクション 3.2を参照してください。
  - Serial over LAN（SoL）を使用してブレードサーバー 1 の MMP シリアルコンソールにアクセスするための静的 IP アドレス 1 つ。SoL アクセスはファブリック インターコネクト モジュールの管理ポートを介して行われるため、この IP アドレスは管理 VLAN 上に設定してください。詳細については、セクション 3.4 を参照してください。
  - 両方のファブリック インターコネクト モジュール上のポート 1（ポート A）を介して Cisco Meeting Server アプリケーションにアクセスするための静的 IP アドレス 1 つ。この IP アドレスは、管理 VLAN とは別の VLAN 上に設定する必要があります。詳細については、セクション 4.3 を参照してください。

2.4 ケーブルの接続

ファブリック インターコネクト A で、次のように接続します。

- 管理ポートを管理ネットワークの 100/1000Mbps スイッチ ポートに接続します。
- ポート 1 に適切な 10Gbps SFP+ トランシーバモジュールを取り付け、このポートをネットワークの 10Gbps スイッチポートに接続します。このポートはスイッチポートであり、トランクとして構成されていないことが条件となります。
- シリアル コンソール ポートをコンソール端末に接続します。これはファブリック インターコネクト モジュールを設定するためです。
- ポート 2 とポート 3 は現在使用されていません。

ファブリック インターコネクト B も同じように接続します。

注：ファブリック インターコネクト A または B のポート 4 に SFP+ トランシーバを取り付けないでください。また、いずれのポート 4 もネットワークに接続しないでください。ポート 4 は内部使用専用です。

2.5 電源オン/オフ

電源コードをユニット背面の電源装置のソケットに差し込みます。シャーシに電力が供給されると、ファブリック インターコネクト モジュールが起動し始めます。ブレードサーバーは、電源をオンにするまでスタンバイモード（黄色の LED が点灯）のままになります（セクション 3.10 を参照）。電源を入れると、ブレード サーバの LED が緑色になります。

シャーシの電源を取り外す前に、ブレードサーバーをスタンバイモードにする必要があります（付録 G.1 を参照）。

2.6 次のステップ

Cisco Meeting Server 2000 の物理的設置の後、サーバーをネットワークに接続できるようにファブリック インターコネクト モジュールを設定する必要があります。詳細については第 3 章を参照してください。

3 ファブリック インターコネクト モジュールの設定

この章では、サーバがネットワークに接続できるよう、ファブリック インターコネクト モジュールの初期設定を行う方法について詳しく説明します。

この章は、次の項で構成されています。

- 両方のファブリック インターコネクト モジュールに割り当てられたデフォルト管理者パスワードの変更。
- SSH を介したファブリック インターコネクトを管理するための新しい静的 IP アドレスの割り当て。これには、ファブリック インターコネクト モジュールをクラスタとして管理するための共有アドレスの定義も含まれます。
- SoL を使用して Cisco Meeting Server の MMP レイヤーにアクセスするためのデフォルト管理者パスワードの変更。SoL は、シャーシ内のファブリック インターコネクト モジュールのいずれかにあるシリアル ポートに接続するために使用されます。この接続により、Cisco Meeting Server の MMP にアクセスできるようになります。
- SoL を介して MMP にアクセスするための新しい静的 IP アドレスの割り当て。
- システム名の変更。
- Meeting Server の DNS の設定。
- Meeting Server のタイムゾーンの設定。
- Meeting Server の NTP の設定。
- ポート 1 のアップリンク速度の設定。
- ブレードサーバの電源投入。
- UCS Manager を使用したブレードの動作の確認。
- ファブリック インターコネクト モジュールの証明書のインストール。

初期設定には、次の情報が必要です。

- ファブリック インターコネクトの管理者アカウントのパスワード。Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。
- 各ファブリック インターコネクト モジュールと共有 IP アドレスの新しい IPv4（または IPv6）アドレス、サブネットマスク、デフォルトゲートウェイ。IP アドレスはすべて管理ネットワーク VLAN 上に設定する必要があります。
- SoL を使用して MMP シリアル コンソールにアクセスするための管理者パスワード。
- SoL 接続経由で MMP コマンドラインにアクセスするための新しい IPv4（または IPv6）アドレス。

- システム名。
- 管理 VLAN 上の DNS サーバの IPv4 アドレス（または IPv6 アドレス）。
- ファブリック インターコネクト モジュールによって使用されるタイムゾーン。
- MMP ネットワーク ポートの MACアドレス。

この章のタスクを完了すると、Cisco Meeting Server 2000 の MMP にログインし、Meeting Server のコンポーネント（Call Bridge、Web Bridge など）を構成する準備ができます。詳細については第 4 章を参照してください。

3.1 ファブリック インターコネクト モジュールのデフォルト管理者パスワードの変更

初期設定を行うには、各ファブリック インターコネクト モジュールのコンソール ポートにシリアル端末を接続する必要があります。

1. シリアル端末をファブリック インターコネクト A のコンソール ポートに接続します。
2. シリアル端末のパラメータを 9600 ボー、8 データ ビット、パリティなし、1 ストップ ビットに設定します。
3. UCS Manager のデフォルトのパスワード "C1sc0123" を使用して "admin" としてログインします。
4. 次の例に示すコマンドを使用して、管理者アカウントのパスワードを変更します。

注：ファブリック インターコネクト モジュールはクラスタ化されているため、ファブリック インターコネクト B に対してこの手順を繰り返す必要はありません。

例：

```
Cisco UCS Mini 6324 Series Fabric Interconnect
UCS-A login: admin
Password: C1sc0123
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac Copyright (c) 2009, Cisco Systems, Inc.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
UCS-A# scope security
UCS-A /security # set password
Enter new password:
Confirm new password:
UCS-A /security* # commit-buffer
UCS-A /security # exit
UCS-A#
```

3.2 ファブリック インターコネクト モジュールの新しい IP アドレスの割り当て

各ファブリック インターコネクト モジュールに新しい静的 IP アドレスを割り当て、両方のモジュールで共有されるもう 1 つのアドレスを割り当てます。共有 IP アドレスは、クラスタ化されたファブリック インターコネクト モジュール上で実行されている UCS Manager へのアクセスに使用されます。

3 つの IP アドレスはすべて同時に変更する必要があり、管理用 VLAN サブネットなど、同じサブネット上に存在する必要があります。

アドレスの設定は、ファブリック インターコネクト モジュールのいずれかを使用して行うことができます。

たとえば、IPv4 を使用している場合は、次のようになります。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 10.1.1.111 netmask
255.255.255.0 gw 10.1.1.110
UCS-A /fabric-interconnect* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # set out-of-band ip 10.1.1.112 netmask
255.255.255.0 gw 10.1.1.110
UCS-A /fabric-interconnect* # scope
system UCS-A /system* # set virtual-ip
10.1.1.113 UCS-A /system* # commit-buffer
UCS-A /system # exit
UCS-A#
```

たとえば、IPv6 を使用している場合は、次のようになります。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001:10::157
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6 2001:10::158
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* #set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope system
UCS-A /system* # set virtual-ip ipv6 2001:10::156
UCS-A /system* # commit-buffer
UCS-A /system # exit
UCS-A#
```

3.3 MMP Serial over LAN アカウントのデフォルト管理者パスワードの変更

MMP（メインボード管理プロセッサ）には、SoL 接続を使用してアクセスします。この仮想シリアルポートに接続すると、Cisco Meeting Server コンソールに渡される前に、SoL インターフェイスに固有のユーザー名とパスワードを入力するように求められます。デフォルトのアカウントとパスワードは出荷前に設定されていますが、セキュリティのため、このデフォルトのパスワードを変更する必要があります。デフォルトの mmp を使用しない場合は、新しい管理者アカウントを作成することもできます。詳細については、セクション 3.3.1を参照してください。

1. ファブリック インターコネクト モジュールのいずれかのコマンド ライン インターフェイスにログインして、MMP SoL アカウントの管理者パスワードをデフォルトの "c1sco1234" から変更します。

例：

```
UCS-A# scope org /CMS
UCS-A /org/ # enter ipmi-access-profile CMS2000-IPMI
UCS-A /org/ipmi-access-profile # enter ipmi-user mmp
UCS-A /org/ipmi-access-profile/ipmi-user # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user # exit
UCS-A /org/ipmi-access-profile # exit
UCS-A /org # exit
UCS-A#
```

3.3.1 SoL アクセス用の新しいユーザアカウントの作成

デフォルトの mmp アカウントを使用するのではなく、SoL アクセス用の新しいユーザを作成する場合は、次の手順を実行します。その際、**「fred」**という名前を適切なユーザー名に置き換えます。

注：`show ipmi-user` 回線と応答はオプションです。

```
UCS-A# scope org /CMS
UCS-A /org # enter ipmi-access-profile CMS2000-IPMI
UCS-A /org/ipmi-access-profile # create ipmi-user fred
UCS-A /org/ipmi-access-profile/ipmi-user* # set privilege admin
UCS-A /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
```

```
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user # exit
UCS-A /org/ipmi-access-profile # show ipmi-user

 IPMI user:
       User Name      End point user privilege   Password      Description
---------------------- ---------------------------------- ---------- ----------
       fred           Admin                      ****
       mmp            Admin                      ****


UCS-A /org/ipmi-access-profile # exit
UCS-A /org # exit
UCS-A#
```

3.3.2 SoL アクセス用の mmp ユーザアカウントの削除

SoL アクセス用の新しいユーザ アカウントを作成したら、デフォルトの mmp アカウントを削除します。

```
UCS-A# scope org /CMS
UCS-A /org # enter ipmi-access-profile CMS2000-IPMI
UCS-A /org/ipmi-access-profile # delete ipmi-user mmp
UCS-A /org/ipmi-access-profile* # commit-buffer
UCS-A /org/ipmi-access-profile # exit
UCS-A /org # exit
UCS-A#
```

3.4 MMP Serial over LAN 接続にアクセスするための新しい IP アドレスの割り当て

Serial over LAN 接続にアクセスするための IP アドレスを割り当てるには、単一の IP アドレスで構成される IP アドレスブロックを作成し、DNS サーバーを一次使用と二次使用のために割り当てます。

手順は以下のとおりです。

1. Serial Over LAN 接続に割り当てられている IP アドレスのブロックについて、既存の設定を確認します。1 つの IP アドレスのブロックが割り当てられており、その値が展開に適している場合は、次の項に進みます。それ以外の場合は、**delete block<first ip address> <last ip address>** コマンドを使用してブロックの割り当て解除を行います。
2. 1 つの IP アドレスを含むブロックを作成します。 **create block <first ip address> <last ip address> <gateway IP address> <subnet mask>**コマンドを使用します。このブロックは、1 つの IP アドレスで構成され、ファブリック インターコネクトの管理 IP アドレスと同じ管理サブネット内に存在する必要があります。

注：Cisco Meeting Server 2000 の MMP SoL 接続に、別の VLAN またはサブネットを使用することは推奨しません。

3. プライマリ DNS とセカンダリ DNS の IP アドレスを指定します。

たとえば、IPv4 を使用している場合は、次のようになります。

```
UCS-A# scope org /CMS
UCS-A /org/ # enter ip-pool CMS2000-MMP-CIMC
UCS-A /org/ip-pool # show block detail
Block of IP Addresses:
From: 10.1.1.51
To: 10.1.1.51
Default Gateway: 10.1.1.1
Subnet Mask: 255.255.255.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
UCS-A /org/ip-pool # delete block 10.1.1.51 10.1.1.51
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool # create block 10.1.1.2 10.1.1.2 10.1.1.1 255.255.255.0
UCS-A /org/ip-pool/block* # set primary-dns 10.1.1.3 secondary-dns 10.1.1.4
UCS-A /org/ip-pool/block* # commit-buffer
UCS-A /org/ip-pool/block # exit
UCS-A /org/ip-pool # exit
UCS-A /org # exit
UCS-A#
```

3.5 UCS Manager のシステム名の変更

システム名は、サーバーの場所または用途を反映するように変更できます。

例：

```
UCS-A# scope system
UCS-A /system # set name CMS2000-London
Warning: System name modification changes FC zone name and redeploys them non-
disruptively
UCS-A /system* # commit-buffer
UCS-A /system # exit
CMS2000-London#
```

3.6 UCS Manager 用の DNS の設定

ファブリック インターコネクト モジュールが UCS Manager に使用する DNS サーバーを設定する必要があります。

注：UCS Manager で使用される DNS サーバーは、セクション 3.4 で設定され、ブレード 1 の Cisco Integrated Management Controller（CIMC）で使用されるプライマリ DNS サーバーとセカンダリ DNS サーバーとは異なる場合があります。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create dns 10.1.1.3
UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system # exit
UCS-A#
```

3.7 タイムゾーンの設定

Cisco Meeting Server 2000 のタイムゾーンを設定します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa          4) Arctic Ocean         7) Australia         10) Pacific
Ocean
 2) Americas        5) Asia                 8) Europe
 3) Antarctica      6) Atlantic Ocean       9) Indian Ocean

Please select a country.
1) Anguilla 19) Dominican Republic 37) Peru
2) Antigua & Barbuda 20) Ecuador 38) Puerto Rico
3) Argentina 21) El Salvador 39) St Barthelemy
4) Aruba 22) French Guiana 40) St Kitts & Nevis
5) Bahamas 23) Greenland 41) St Lucia
6) Barbados 24) Grenada 42) St Maarten (Dutch)
7) Belize 25) Guadeloupe 43) St Martin (French)
8) Bolivia 26) Guatemala 44) St Pierre & Miquelon
9) Brazil 27) Guyana 45) St Vincent
10) Canada 28) Haiti 46) Suriname
11) Caribbean NL 29) Honduras 47) Trinidad & Tobago
12) Cayman Islands 30) Jamaica 48) Turks & Caicos Is
13) Chile 31) Martinique 49) United States
14) Colombia 32) Mexico 50) Uruguay
15) Costa Rica 33) Montserrat 51) Venezuela
16) Cuba 34) Nicaragua 52) Virgin Islands (UK)
17) Curacao 35) Panama 53) Virgin Islands (US)
18) Dominica 36) Paraguay
#? 49

Please select one of the following time zone regions.
```

```
1) Eastern (most areas) 16) Central - ND (Morton rural)
2) Eastern - MI (most areas) 17) Central - ND (Mercer)
3) Eastern - KY (Louisville area) 18) Mountain (most areas)
4) Eastern - KY (Wayne) 19) Mountain - ID (south); OR (east)
5) Eastern - IN (most areas) 20) MST - Arizona (except Navajo)
6) Eastern - IN (Da, Du, K, Mn) 21) Pacific
7) Eastern - IN (Pulaski) 22) Alaska (most areas)
8) Eastern - IN (Crawford) 23) Alaska - Juneau area
9) Eastern - IN (Pike) 24) Alaska - Sitka area
10) Eastern - IN (Switzerland) 25) Alaska - Annette Island
11) Central (most areas) 26) Alaska - Yakutat
12) Central - IN (Perry) 27) Alaska (west)
13) Central - IN (Starke) 28) Aleutian Islands
14) Central - MI (Wisconsin border) 29) Hawaii
15) Central - ND (Oliver)
#? 21

The following information has been given:
United States
Pacific

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now: Sat Apr 23 05:08:43 PDT 2011.
Universal Time is now: Sat Apr 23 12:08:43 UTC 2011.
Is the above information OK
1) Yes
2) No
#? 1
UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system # exit
UCS-A#
```

3.8 NTP の設定

タイムゾーンを設定したら、次にファブリック インターコネクト モジュールが使用する NTP サーバを設定します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create ntp-server pool.ntp.org
UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system #exit
UCS-A#
```

3.9 ポート 1 のアップリンク速度の構成。

注：各ファブリック インターコネクト モジュールのアップリンク ポートには、10Gbps 接続を使用します。

両方のファブリック インターコネクト モジュールのアップリンク ポートの速度を設定します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope interface 1 1
UCS-A /eth-uplink/fabric/interface # set speed 10gbps
UCS-A /eth-uplink/fabric/interface* #commit-buffer
UCS-A /eth-uplink/fabric/interface # exit
UCS-A /eth-uplink/fabric # exit
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # scope interface 1 1
UCS-A /eth-uplink/fabric/interface # set speed 10gbps
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/fabric/interface # exit
UCS-A /eth-uplink/fabric # exit
UCS-A /eth-uplink # exit
UCS-A#
```

3.10 ブレードサーバの電源投入

8 台のブレードサーバーはそれぞれ、ファブリック インターコネクト モジュールのいずれかを介して電源をオンにする必要があります。

注：電源をオンにすると、ブレードサーバーは最後の電源状態を記憶します。電源障害が発生した場合、このセクションのコマンドを再実行しなくても、ブレードサーバーの電源はオンになります。

例：

```
UCS-A# scope org /CMS
UCS-A /org # scope service-profile CMS2000-MMP
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA2
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
```

```
UCS-A /org # scope service-profile CMS2000-MEDIA3
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA4
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA5
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA6
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA7
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA8
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # exit
UCS-A#
```

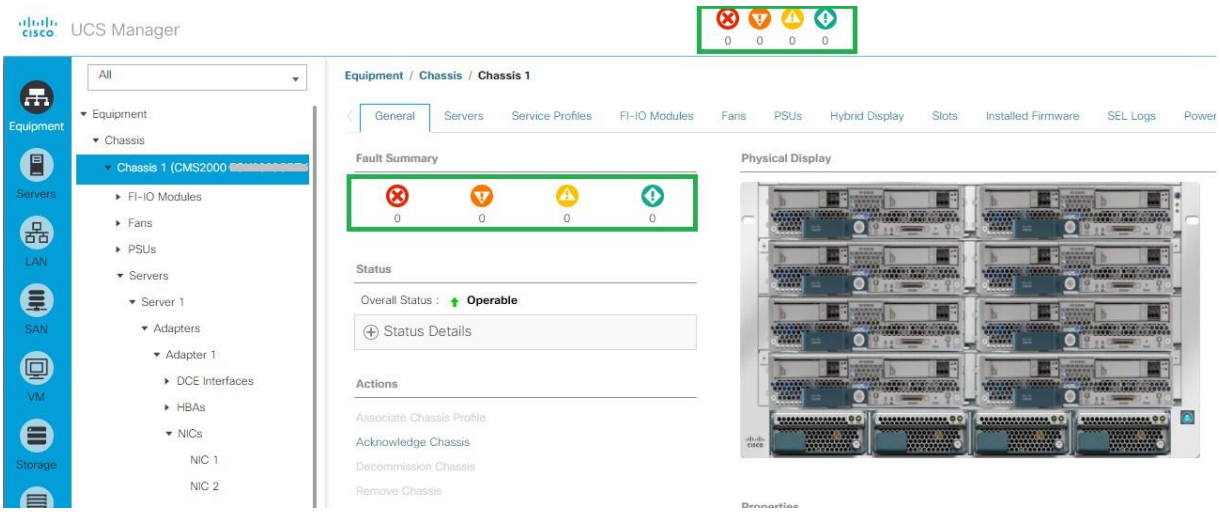
3.11 Cisco Meeting Server の状態の確認

Cisco UCS Manager GUI を使用すると、Cisco Meeting Server 2000 シャーシ内のファブリック インターコネクト モジュールとブレード サーバの稼働状態を監視できます。詳細については、『Cisco UCS Manager システムモニタリングガイド』を参照してください。

ブレードサーバーが稼働していることを確認するには、[障害サマリー（Fault Summary）] ページ（ 図 4 参照）を使用します。それぞれの種類の障害は異なるアイコンで表されます。各アイコンの下にある数字は、システムで発生したその種類の障害の数を示しています。アイコンをクリックすると、Cisco UCS Manager の GUI で [作業（Work）] 領域に [障害（Faults）] タブが開き、そのタイプに属するすべての障害の詳細情報が表示されます。

ブレードサーバーにクリティカルアラート（赤色のアイコン）が表示された場合は、シスコ サポートに問い合わせる前に、『 トラブルシューティング リファレンス ガイド』を参照してください。 ブレード 2 ～ 8 の 1 つ以上がオフラインになるか、削除された場合、Cisco Meeting Server 2000 は引き続き稼働しますが、キャパシティが少なくなります。スロット 1 のブレードサーバーがオフラインになったり故障したりすると、Cisco Meeting Server の MMP とアプリケーションが機能しなくなるため、このブレードは重要です。

図 4：UCS Manager の [障害サマリー（Fault Summary）] ページ



3.12 ファブリック インターコネクト モジュールへの証明書の適用

Cisco Meeting Server 2000 は、ファブリック インターコネクト モジュールに自己署名付きの証明書が適用された状態で出荷されます。この証明書を任意の証明書に置き換えるには、『Cisco UCS Manager アドミニストレーション ガイド』の手順に従ってください。

3.13 次のステップ

ファブリック インターコネクト モジュールを設定し、ブレードサーバーの電源を入れたら、次に MMP を使用して Cisco Meeting Server のコンポーネントを設定します。第 4 章では、MMP を使用して Call Bridge の初期設定を行う方法について説明します。

4 MMP を使用した Cisco Meeting Server 2000 の設定

この章では、MMP を使用して Call Bridge の初期設定を行う方法について詳しく説明します。また、MMP を使用して他のコンポーネントも設定する必要があります。ただし、どのコンポーネントの設定が必要かは展開形態によって異なります。コンポーネントの設定については、『Cisco Meeting Server 導入ガイド』で説明されています。

4.1 Serial over LAN 経由での MMP CLI へのログイン

Cisco Meeting Server の初期設定を行うには、第 3.3 項および第 3.4 項で設定した Serial Over LAN 接続を介して MMP コマンド ライン インターフェイスにアクセスします。SSH クライアントを使用して、 セクション 3.4 で設定した Serial Over LAN 接続用の IP アドレスに接続し、セクション 3.3 で設定したログイン情報を使用してログインします。

例：

```
ssh <username>@<ip address>
ssh mmp@10.1.1.2
mmp@10.1.1.2's password:
CISCO Serial Over LAN:
Close Network Connection to Exit
```

正常にログインすると、Serial Over LAN 接続によって MMP 仮想コンソールに渡されます（注：Serial Over LAN 接続を切断するには、サーバへの SSH セッションを閉じる必要があります）。MMP コンソールには CMS ログイン プロンプトがあります。デフォルトのユーザーアカウント [admin] を使用して MMP にログインします。パスワードは「admin」です。その後、[admin] アカウントに新しいパスワードをすぐ設定するように求められます。

```
Welcome to the CMS 2000
CMS login: admin
パスワードを入力してください： *****
Password reset forced by administrator Please
enter new password:
Please enter new password again:
Failed logins since last successful login 0
Last login 2017-May-24 15:43:06 using serial
```

4.2 Cisco Meeting Server 管理者アカウントの作成

ユーザー名が「admin」のアカウントは安全ではありません。セキュリティを確保するため、独自の管理者アカウントを作成することをお勧めします。また、パスワードを忘れてしまった場合に備え、管理者アカウントを 2 つ用意しておくことが理想的です。そうしておけば、もう 1 つのアカウントでログインし、忘れたパスワードをリセットできます。

MMP コマンド **`user add <name> admin`** を使用します。詳細については、『MMP コマンドライン リファレンス ガイド』を参照してください。パスワードを求めるプロンプトが表示されたら、パスワードを 2 回入力します。新しいアカウントでログインすると、パスワードを変更するように求められます。

注意：パスワードは 6 か月後に期限が切れます。

新しい管理アカウントを作成したら、デフォルトの「admin」アカウントを削除します。

注：管理者レベルの MMP ユーザーアカウントは、Call Bridge の Web 管理インターフェイスへのログインにも使用できます。Web 管理画面インターフェイスを通じて、ユーザを作成することはできません。

4.3 Cisco Meeting Server のネットワーク インターフェイスのセットアップ

ポート A のネットワーク インターフェイスの速度は、セクション 3.9でファブリック インターコネクト モジュールを介して設定したため、ここで設定する必要はありません。

ただし、次の設定を行う必要があります。

- dhcp または静的アドレスのいずれかを使用してポート A の IP アドレスを設定する
- DNS を設定する

ネットワーク インターフェイスとポート A の IP アドレスを設定すると、この IP アドレスを使用して MMP にアクセスできます。MMP SoL は、ポート A にアクセス不能になった場合にのみ使用してください。SFTP にはポート A を介してのみアクセスできます。

4.3.1 DHCP を使用したポート A の IP アドレスの設定

ポート A で dhcp を有効にするには、次のように入力します。

```
ipv4 dhcp
```

注：IPv6 を使用している場合に使用する同様のコマンド一式があります。詳細な説明については、『MMP Command Reference』を参照してください。

次に、構成した dhcp 設定を確認するには、次のコマンドを入力します。

```
ipv4 a
```

4.3.2 ポート A の静的 IP アドレスの設定

<ipv4|ipv6> a addコマンドを使用し、指定したサブネットマスクおよびデフォルトゲートウェイで、静的 IP アドレスをポート A に追加します。

たとえば、プレフィックス長 16（ネットマスク 255.255.0.0）とゲートウェイ 10.1.1.1 を指定してアドレス 10.1.1.6 をポート A に追加するには、次のように入力します。

```
ipv4 a add 10.1.1.6/16 10.1.1.1
```

この IPv4 アドレスを削除するには、次のコマンドを入力します。

```
ipv4 a del 10.1.1.6
```

4.3.3 DNS 構成の設定

1. DNS 設定を出力するには、次のように入力します。

   ```
   dns
   ```

2. DNS を設定するには、次のように入力します。

   ```
   dns add forwardzone <domain name> <server IP>
   ```

   注：フォワードゾーン（forwardzone）とは、ドメイン名とサーバーアドレスで構成されるペアです。ある名前が DNS 階層内の特定のドメイン名の下にある場合、DNS リゾルバでその特定のサーバーに問い合わせることができます。ロードバランシングとフェイルオーバーを可能にするには、特定のドメイン名に対して複数のサーバーを指定します。一般的な使用法は、ドメイン名として「.」、つまり DNS 階層のルートを指定することです。これはすべてのドメイン名に一致します。つまり、サーバが IP 10.1.1.3 にある場合、次のコマンドを入力します。

   ```
   dns add forwardzone . 10.1.1.3
   ```

DNS エントリを削除する必要がある場合は、次のように入力します。

```
dns del forwardzone <domain name> <server IP>
```

例：

```
dns del forwardzone . 10.1.1.10
```

4.4 インストールされているソフトウェアの確認

Cisco Meeting Server 2000 は、Cisco Meeting Server ソフトウェアがあらかじめインストールされた状態で出荷されます。Call Bridge 用の Web 管理画面インターフェイスを設定する前に、最新の Cisco Meeting Server ソフトウェアがインストールされているか確認することをお勧めします。

- インストールされているソフトウェアのバージョンを表示するには、MMP コマンド **version**を使用します。

- 利用可能な最新のソフトウェアを確認するには、こちらの リンクに移動します。Cisco Meeting Server 2000 は、VM 展開に対する異なるインストールファイルであることに注意してください。

Cisco Meeting Server ソフトウェアをアップグレードするには、該当するソフトウェアバージョンのリリースノートの手順に従ってください。アップグレードする前に、システム設定をバックアップしてください。

ヒント：ポート A の設定が完了したので、SFTP を使用して、ポート A 経由で Cisco Meeting Server ソフトウェアをバックアップおよびアップグレードできます。

4.5 Web 管理画面インターフェイスの設定

Web 管理画面インターフェイスは Call Bridge へのインターフェイスとして機能します。Cisco Meeting Server の API はこの Web インターフェイスでルーティングされます。

Web 管理インターフェイスを設定するには、秘密キー/証明書のペアを作成し（セクション 4.5.1 を参照）、秘密キー/証明書のペアを MMP にアップロードし、ポート A をリッスンするようにインターフェイスを設定する（セクション 4.5.2 を参照）必要があります。

Web 管理画面インターフェイスが有効になると、Call Bridge の設定に API または Web 管理のいずれかを使用できるようになります。

4.5.1 Web 管理画面インターフェイスの証明書の作成

Web 管理画面インターフェイスは HTTPS を介してのみアクセスできるため、セキュリティ証明書を作成し、Cisco Meeting Server にインストールする必要があります。

注：Web 管理画面インターフェイスではなく API を介して Call Bridge を構成する場合も、Web 管理画面インターフェイスの証明書をアップロードしておく必要があります。

下記の情報は、Cisco が秘密キー マテリアルの生成要件を満たしていることを想定しています。必要に応じて、パブリック認証局（CA）を使用して、秘密キーと証明書を外部で生成することもできます。外部で生成したキーと証明書のペアを、SFTP を使用して Cisco Meeting Server の MMP 上にロードします。署名済み証明書を取得したら、第 4.5.2 項に進みます。

注：Cisco Meeting Server をラボ環境でテストする場合は、サーバーでキーと自己署名証明書を生成することができます。自己署名証明書と秘密キーを作成するには、MMP にログインして次のコマンドを使用します。

pki selfsigned <key/cert basename>

ここで **<key/cert basename>**は、生成するキーと証明書を識別します。たとえば、「pki selfsigned webadmin」と入力すると、webadmin.key と webadmin.crt（自己署名証明書）が作成されます。自己署名証明書は、実稼動環境では使用しないことをお勧めします（http://en.wikipedia.org/wiki/Self-signed_certificate [英語] を参照）。

MMP コマンド **pki csr** を使用して、秘密キーと、関連する証明書署名要求を生成し、CA での署名用にエクスポートする方法を次の手順で示します。

1. MMP にログインして、次のコマンドで秘密キーと証明書署名要求（CSR）を生成します。

   pki csr <key/cert basename> [<attribute>:<value>]

   値は次のとおりです。

   <key/cert basename> は、新しいキーと CSR を識別する文字列です（たとえば「webadmin」と入力すると、「webadmin.key」ファイルと「webadmin.csr」ファイルが作成されます）。

   また、オプションで許可される各属性は次のとおりで、コロンで区切る必要があります。

   - CN：証明書に必要な commonName。CN には DNS A レコードで定義した FQDN を使用します。その FQDN を使用しなかった場合は、ブラウザ証明書のエラーが発生します。
   - OU：組織単位
   - O：組織
   - L：地名
   - ST：州
   - C：国
   - emailAddress

   複数の単語で指定する場合は、次のように値を引用符で囲みます。

   pki csr example CN:example.com "OU:Accounts UK" "O:My Company"

2. 次のいずれかに CSR を送信します。
   - 認証局（CA）。たとえば、要求側のアイデンティティを確認し、署名付き証明書を発行する Verisign など。
   - ローカルまたは組織の認証局への送信。たとえば、Active Directory 証明書サービスの役割がインストールされている Active Directory サーバーなど（付録 E を参照してください）。

注：Cisco Meeting Server に署名付き証明書と秘密キーを転送する前に、証明書ファイルを確認してください。CA によって証明書チェーンが発行された場合は、チェーンから証明書を抽出する必要があります。証明書ファイルを開き、特定の証明書の BEGIN CERTIFICATE および END CERTIFICATE 行を含むテキストをコピーして、テキスト ファイルに貼り付けます。このファイルを .crt、.cer、または .pem 拡張子で証明書として保存します。残りの証明書チェーンをコピーして別のファイルに貼り付けます。中間証明書チェーンであることがわかる明確な名前を付けて、同じ拡張子（.crt、.cer、または .pem）を使用してください。中間証明書チェーンは、チェーンを発行した CA の証明書が最初でルート CA の証明書がチェーンの最後になる順番で並べる必要があります。

4.5.2 HTTPS アクセス用 Web 管理画面インターフェイスの設定

1. セクション 3.4 で設定した IP アドレスに SSH を介して接続し、SoL 接続を使用して MMP コマンドラインにアクセスします。 セクション 3.3 で設定した admin ユーザー名とパスワードを使用してログインします。
2. SFTP を使用して秘密キー/証明書ペアをアップロードします。オプションで証明書バンドルもアップロードします。
3. 次のコマンドを入力して、手順 2 でアップロードしたファイルを Web 管理者インターフェイスに割り当て、ポート A を使用するようにインターフェイスを設定します。

```
webadmin certs webadmin.key webadmin.crt
webadmin listen a 443
webadmin restart
webadmin enable
```

4. Web 管理画面インターフェイスにアクセスできるかどうかをテストします。ブラウザで、たとえば https://cms-server.mycompany.com のような URL（または IP アドレス）を入力し、先ほど作成した MMP ユーザーアカウントを使用してログインします。

注：バージョン 3.0 より、ライセンスがなくても 90 日間はフル機能をトライアルモードで使用できます。この場合、この間に Web 管理インターフェイスに「この CMS は現在ライセンスがありません」と表示されます。スマートライセンスの詳細と 3.0 におけるライセンスの仕組みについては、**「付録 B」を参照してください。**

4.6 スケジューラの電子メールサーバーの設定

このセクションでは、スケジューラコンポーネントの電子メールサーバーを設定する手順について説明します。会議がスケジュール、キャンセル、または変更されると、電子メール通知が参加者に送信されます。スケジューラは、SMTP 電子メールサーバーの設定を介した電子メール通知の送信をサポートします。

サーバーアドレスとポートの設定、電子メールプロトコルの有効化、および認証用のユーザー名の設定は、次のスケジューラ MMP コマンドを介して指定します。

```
scheduler email server <hostname|address> <port>
scheduler email server none
scheduler email username <smtp username>
scheduler email protocol <smtp|smtps>
scheduler email auth <enable|disable>
scheduler email starttls <enable|disable>
```

サーバーアドレスが設定されていない場合、電子メールはスケジューラで設定されません。スケジューラが電子メール招待を送信するには、少なくとも 1 つの電子メールサーバーを設定する必要があります。電子メールは、会議のスケジュールに使用されたスケジューラからではなく、任意のスケジューラから送信できます。電子メールサーバーがダウンした場合は、別のスケジューラが電子メールを送信します。

スケジューラは、次のタイプの電子メール設定をサポートしています。

1. SMTP
2. 認証済みログインによる SMTP（認証ログイン）
3. SMTP と STARTTLS
4. 認証ログインと STARTTLS を使用した SMTP
5. SMTPS（SMTP トランザクション全体のエンドツーエンドの TLS 暗号化）
6. 認証ログインによる SMTPS

注：Exchange Server 2016 CU22 - 15.1.2375.7 および Exchange Server 2019 CU11 - 15.2.986.5 を使用することをお勧めします。

会議の招待状は、共通の電子メールアドレスからすべての参加者に送信できます。MMP コマンド **`scheduler email common-address <address@mail.domain> "<Display name>"`** は、Meeting Server で共通 E メールアドレスと表示名を構成します。 スケジューラは、共通の電子メールアドレスから参加者に会議の招待状を送信します。

共通の電子メールアドレスが空白の場合、スケジューラは主催者の電子メールアドレスから電子メール招待状を送信します。

注：共通の電子メールアドレスが設定されていない場合、SMTP サーバーによる認証には、MMP コマンド **`scheduler email username <smtp user-name>`** を使用して電子メールアドレスを設定する必要があります。MMP で設定されたこのアカウントには、Web アプリ ユーザーの代わりに電子メールを送信できる適切な権限が必要です。

送信者を識別するために、電子メールアドレスの他に主催者の名前を表示名として含めることもできます。Web アプリを使用して会議がスケジュールされると、Web アプリは、会議をスケジュールしたユーザーの名前を主催者の表示名としてスケジューラに送信します。 スケジューラ API にオプションのパラメータ **`organizeDisplayName`** を含めることによって、任意の名前を表示名として設定できます。

電子メール招待状の配信に失敗した場合、スケジューラは定期的に送信を再試行します。スケジューラの電子メールキュークリーナーは、特定の有効期限後に、キューに入れられた失敗した電子メールをクリーンアップします。

4.6.1 SMTP を使用したスケジューラ電子メール設定

スケジューラが SMTP 経由で電子メール通知を送信できるようにするには、電子メールサーバーが指定されたポートで SMTP プロトコルをリッスンするように設定します。

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   ```
   scheduler disable
   ```

2. 電子メールサーバーとポートを設定します。

   ```
   scheduler email server <hostname|address> <port>
   ```

   例

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. スケジューラを有効にします。

   ```
   scheduler enable
   ```

4.6.2 認証ログイン設定を使用したスケジューラ SMTP

スケジューラが認証ログインを使用して SMTP 経由で電子メール通知を送信できるようにするには、電子メール サーバーが指定されたポートで SMTP プロトコルをリッスンするように設定し、SMTP サーバーが認証ログインをサポートできるようにし、認証用のユーザーアカウントを設定します。MMP で設定されたこのアカウントには、Web アプリユーザーの代わりに電子メールを送信できる適切な権限が必要です。

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   ```
   scheduler disable
   ```

2. 電子メールサーバーとポートを設定します。

   ```
   scheduler email server <hostname|address> <port>
   ```

   例

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. 認証ログインオプションを有効にします。

   ```
   scheduler email auth enable
   ```

4. 認証に使用するユーザー名を設定します：
   ```
   scheduler email username <username>
   ```
   パスワードを入力します：

   ```
   scheduler email username test@test.com
   Please enter password:
   Please enter password again:
   ```

5. スケジューラを有効にします。

   ```
   scheduler enable
   ```

4.6.3 スケジューラの SMTP および STARTTLS 構成

スケジューラが SMTP および STARTTLS 経由で電子メール通知を送信できるようにするには、電子メールサーバーが指定されたポートで SMTP プロトコルをリッスンするように設定し、STARTTLS を有効にします。

TLS 接続を確立するために、TLS ハンドシェイクには、電子メールサーバーとスケジューラ間の証明書交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼するように設定されており、電子メールサーバーからの証明書をすべて受け入れることで、TLS 接続が正常に確立します。ただし、スケジューラには、特定の証明書を設定するための追加オプションがあります。このモードでは、スケジューラは設定済みの証明書のみを受け入れて信頼します。

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable

2. 電子メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   例

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. STARTTLS オプションを有効にします。

   scheduler email starttls enable

4. 特定の証明書を使用するには、まず、証明書をインポートして、SFTP 経由で Meeting Server VM にアップロードします。次に、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定される証明書は有効な証明書である必要があります。たとえば、共通名または SAN 名が電子メールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。同様に、証明書が認証局によって発行されている場合、またはチェーンに中間証明書がある場合は、ルート CA 証明書を設定するか、ルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

5. スケジューラコンポーネントを有効にします。

   scheduler enable

4.6.4 STARTTLS 構成を介した認証ログインを使用したスケジューラ SMTP

スケジューラが認証ログインと STARTTLS を使用して SMTP 経由で電子メール通知を送信できるようにするには、電子メールサーバーが指定されたポートで SMTP プロトコルをリッスンするように設定します。さらに、SMTP サーバーが認証ログインをサポートできるようにし、認証に使用されるユーザーアカウントを設定し、STARTTLS を有効にします。

TLS 接続を確立するために、TLS ハンドシェイクには、電子メールサーバーとスケジューラ間の証明書交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼するように設定されており、電子メールサーバーからの証明書をすべて受け入れることで、TLS 接続が正常に確立します。ただし、スケジューラには、特定の証明書を設定するための追加オプションがあります。このモードでは、スケジューラは設定済みの証明書のみを受け入れて信頼します。

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable

2. 指定された電子メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   例

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. 認証ログインオプションを有効にします。

   scheduler email auth enable

4. 認証に使用するユーザー名を設定します。

   scheduler email username <username>
   パスワードを入力します。

   ```
   scheduler email username test@test.com
   Please enter password:
   Please enter password again:
   ```

5. STARTTLS オプションを有効にします。

   scheduler email starttls enable

6. 特定の証明書を使用するには、まず、証明書をインポートして、SFTP 経由で Meeting Server VM にアップロードします。次に、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>
   設定される証明書は有効な証明書である必要があります。たとえば、共通名または SAN 名が電子メールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。同様に、証明書が認証局によって発行されている場合、またはチェーンに中間証明書がある場合は、ルート CA 証明書を設定するか、ルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

7. スケジューラコンポーネントを有効にします。

   scheduler enable

4.6.5 スケジューラの SMTPS 設定

スケジューラが SMTPS 経由で電子メール通知を送信できるようにするには、特定のポートでエンドツーエンドの SMTP 暗号化をサポートするように電子メール サーバーを設定します。

TLS 接続を確立するために、TLS ハンドシェイクには、電子メールサーバーとスケジューラ間の証明書交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼するように設定されており、電子メールサーバーからの証明書をすべて受け入れることで、TLS 接続が正常に確立します。ただし、スケジューラには、特定の証明書を設定するための追加オプションがあります。このモードでは、スケジューラは設定済みの証明書のみを受け入れて信頼します。

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable
2. 指定された電子メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   例

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```
3. 電子メールプロトコルを SMTPS に設定します。

   scheduler email protcol smtps
4. 特定の証明書を使用するには、まず、証明書をインポートして、SFTP 経由で Meeting Server VM にアップロードします。次に、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定される証明書は有効な証明書である必要があります。たとえば、共通名または SAN 名が電子メールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。同様に、証明書が認証局によって発行されている場合、またはチェーンに中間証明書がある場合は、ルート CA 証明書を設定するか、ルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。
5. スケジューラコンポーネントを有効にして、SMTPS を使用する電子メール設定を完了します。

   scheduler enable

4.6.6 認証ログイン設定を使用したスケジューラ SMTPS

スケジューラが認証ログインを使用して SMTPS 経由で電子メール通知を送信できるようにするには、特定のポートでエンドツーエンドの SMTP 暗号化をサポートするように電子メールサーバーを設定します。さらに、SMTPS サーバーが認証ログインをサポートできるようにし、認証に使用されるユーザーアカウントを設定します。

TLS 接続を確立するために、TLS ハンドシェイクには、電子メールサーバーとスケジューラ間の証明書交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼するように設定されており、電子メールサーバーからの証明書をすべて受け入れることで、TLS 接続が正常に確立します。ただし、スケジューラには、特定の証明書を設定するための追加オプションがあります。このモードでは、スケジューラは設定済みの証明書のみを受け入れて信頼します。

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable

2. 指定された電子メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   例

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. 認証ログインオプションを有効にします。

   scheduler email auth enable

4. 認証に使用されるユーザーのユーザー名を設定します。

   scheduler email username <username>

   パスワードを入力します。

   ```
   scheduler email username test@test.com

   Please enter password:
   Please enter password again:
   ```

5. 電子メールプロトコルを SMTPS に設定します。

   scheduler email protcol smtps

6. 特定の証明書を使用するには、まず、証明書をインポートして、SFTP 経由で Meeting Server VM にアップロードします。次に、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定される証明書は有効な証明書である必要があります。たとえば、共通名または SAN 名が電子メールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。同様に、証明書が認証局によって発行されている場合、またはチェーンに中間証明書がある場合は、ルート CA 証明書を設定するか、ルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

7. スケジューラコンポーネントを有効にして、認証ログインで SMTPS を使用する電子メール設定を完了します。

   scheduler enable

4.6.7 スケジューラの詳細ロギング

スケジューラは、スケジューラ timedLogging MMP コマンドを使用して、Web Bridge 接続、電子メール通知、および API の詳細ログを有効にするオプションをサポートしています。

timedLogging が有効になっていない場合、Meeting Server は次の出力を表示します。

```
cms-vm> scheduler timedLogging
{
"webBridge": "0",
"api": "0",
"email": "0"
}
```

timedLogging オプションのいずれかを有効にするには、次のコマンドを使用します。

scheduler timedLogging (webBridge|api|email) <time>

例

```
cms-vm> scheduler timedLogging webBridge 600
SUCCESS
```

time 変数は秒単位で表され、設定された期間の timedLogging を有効にします。

```
cms-vm> scheduler timedLogging
{
"webBridge": "594",
"api": "0",
"email": "0"
}
```

設定された期間が終了するか、特定の調査またはトラブルシューティングの手順が完了したら、SFTP を使用してログファイルをダウンロードします。

5 Cisco Meeting Server 展開の計画

注：バージョン 3.0 から、ライセンスがなくても 90 日間はフル機能をトライアルモードで使用できます。

初期設定を完了すると、Cisco Meeting Server 2000 は、次の方法で導入できます。

- 単一サーバー。通常、多数の内線コールが同時に発生する 1 つの場所がある組織に適しています。コールキャパシティ情報については、 A.4 を参照してください。
- 分割展開。この場合、Cisco Meeting Server 2000 は内部ネットワーク上に展開されているコアノードになり、DMZ に展開されている エッジコンポーネント（TURN サーバー）は Edge サーバー（Cisco Meeting Server 1000、Cisco Meeting Server 仕様準拠の VM サーバー、Cisco Expressway）で有効になります。

  Cisco Meeting Server Web Edge ソリューションの展開の詳細については、『導入ガイド（バージョン 3.1 以降）』を参照してください。
- スケーラビリティと耐障害性を備えた導入の複数コア ノードの 1 つとして。これは、大規模な会議、使用率の増加、ダウンタイムの最小化をサポートするための導入形態です。

導入の計画および準備ガイドを使用して適切な導入形態を決定した後、該当する導入ガイドと証明書ガイドに従います。

付録 A 技術仕様

A.1 物理仕様

シャーシ：Cisco UCS 5108 ブレードサーバシャーシ
重さ：115+ kg（254+ ポンド）
サイズ：高さ 6RU

ラック要件：19 インチ標準ラック

A.2 環境仕様

動作温度：10 ~ 35°C（50 ~ 95°F）
動作する湿度：5 ~ 93%（結露しないこと）

A.3 電気的仕様

最大電力：	230V で 3.36kW、14.74A
	3.38kW @ 115V、29.48A
電源	4 X 2500W のプラチナ AC ホットプラグ電源装置

A.4 ビデオおよび音声の仕様

この表は、Cisco Meeting Server ソフトウェアをホストしているプラットフォームのコール キャパシティの比較を示しています。

表 1：Meeting Server プラットフォームのコール キャパシティ

通話タイプ	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000 M5v2
フル HD 通話 1080p60 ビデオ 720p30 コンテンツ	30	218
フル HD 通話 1080p30 ビデオ 1080p30/4K7 コンテンツ	30	218
フル HD 通話 1080p30 ビデオ 720p30 コンテンツ	60	437

通話タイプ	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000 M5v2
HD 通話 720p30 ビデオ 720p5 コンテンツ	120	875
SD 通話 480p30 ビデオ 720p5 コンテンツ	240	1250
音声通話（G.711）	2200	3,000

注：バージョン 3.2 以降、Meeting Server は Meeting Server 1000 M5v2 と Meeting Server 2000 M5v2 のハードウェアバリアントでのコールキャパシティの増加をサポートします。

A.5 Cisco Meeting Server でサポートされるユーザー数

バージョン 3.3 以降、Cisco Meeting Server クラスタは、データベースが配置されているサーバーに応じて、最大 300,000 のユーザをサポートできます。クラスタ内のすべてのデータベースは、同じ仕様のサーバー上にある必要があります。

表 2: Cisco Meeting Server でサポートされるユーザー数

Cisco Meeting Server	最大ユーザ数
Meeting Server 2000 M5v2	300,000
Meeting Server 2000 M5v1	200,000
Meeting Server 2000 M4、Meeting Server 1000 M4、M5v1、M5v2、および仕様ベースのサーバー	75,000

注：多数のユーザの LDAP 同期により、通話の参加時間が長くなる可能性があります。メンテナンス時間帯またはオフピーク時に、新しいユーザ/coSpace を Meeting Server に追加することをお勧めします。

A.6 帯域幅の要件：

Cisco Meeting Server 2000 は、同時に最大 700 台の 720p HD コールをサポートします。これには、3 ～ 4 Gbps のネットワーク帯域幅が必要です。

A.7 ドライバ仕様

次の表に、Cisco Meeting Server でサポートされているドライバのバージョンを示します。

要因	サポートされているバージョン
Linux カーネル	4.4.225
Enic ドライバ	2.3.0.20
MegaRAID SAS	06.808.16.00-rc1

付録 B シスコライセンス

Cisco Meeting Server のライセンスが必要です。バージョン 3.4 以降、Meeting Server にはスマートライセンスが必須です。既存のローカルライセンスは、ライセンスの有効期限が切れるまで引き続きサポートされます。このセクションでは、スマートライセンス方式のライセンス情報について説明します。

B.1 スマートライセンス

Meeting Server のバージョン 3.0 では、Cisco Meeting Management バージョン 3.0 以降を使用した Cisco Meeting Server でのスマートライセンスのサポートが導入されています。今回のソフトウェア ライセンス モデルへの移行、つまり従来の製品アクティベーションキー（PAK）ライセンスからスマートライセンスへの移行により、ライセンスの購入、登録、ソフトウェア管理のユーザーエクスペリエンスが向上します。また、Meeting Server でも、他のシスコ製品におけるソフトウェアライセンスの方法と同様に Cisco スマートアカウントを利用します。これは、組織全体でライセンスの表示、格納、管理ができる一元的なリポジトリです。

注：Cisco スマートライセンスクラウド証明書は 2023 年 2 月に更新されます。更新後、スマートライセンスクラウドとの直接通信、またはオンプレミスの Cisco Smart Software Manager (SSM) を介した通信はすべて影響を受けます。2023 年 2 月までに Meeting Management 3.6 にアップグレードすることをお勧めします。SLR/PLR のお客様は、新しいライセンスの取得、手動同期の実行、または新しいコールブリッジの追加のために、Meeting Management 3.6 にアップグレードする必要もあります。

すべての新規ライセンス購入で引き続き PAK コードが提供されます。すべてのライセンスは Meeting Management が同期するスマートアカウントで利用可能になるため、この PAK コードは参照用に保持されます。

詳細について、またスマートアカウントを作成するには、 https://software.cisco.com にアクセスして、[スマートライセンス（Smart Licensing）] を選択してください。

3.0 より前のバージョンからの Meeting Server ライセンスの変更は次のとおりです。

- バージョン 3.0 では Cisco Meeting Management バージョン 3.0 以降が必須です。Meeting Management は Meeting Server ライセンスファイルを読み取り、製品登録と、スマートアカウント（セットアップされている場合）とのやり取りを処理することができます。
- スマートアカウントに存在する 1 セットの Meeting Server ライセンスを使用して、複数のクラスタにライセンスを付与できるようになり、3.0 より前のバージョンでのように個々の Meeting Server インスタンスにライセンスファイルをロードする必要がなくなります。

- スマート ライセンスを使用した Meeting Management では、クラスタあたりいくつの Call Bridge が使用されているかをトラッキングできるため、R-CMS-K9 アクティベーション ライセンスは不要になります。
- 既存のライセンスがない新規の展開の場合は、次のようになります。
  - 新規購入のライセンスはデフォルトでスマート対応になっておりスマート アカウントが必要な場合があります。Meeting Management にライセンスの詳細情報を入力すると、スマート アカウントで保有されているライセンスに対してライセンスの詳細情報が検証されます。
- 各 Call Bridge にローカルのライセンス ファイルがある既存の環境の場合は、次のようになります。
  - Cisco Smart Software Manager（CSSM）ポータルを使用してスマートアカウントに移行し、既存のライセンスをスマートに変換するオプションを選択することができます。
- SMP Plus と PMP Plus のライセンス使用状況が合算され、ある特定の 1 日の使用数が超過であるかどうか判別されます（いずれかのライセンスが超過した場合、その日は終日、使用数が使用権を超えていると見なされます）。他の機能のライセンス（録音やカスタム レイアウトなど）は個別に評価され、（スマート アカウントにライセンスが存在する前提で）Meeting Management を通じて有効化されます。

注：「超過（overage）」という言葉は、ライセンスの使用数が使用権を超えている状態を表します。

注：3.0 のすべての展開で Meeting Management が必須であるため、大規模なカスタマー展開の場合は、アクティブな Meeting Management を使用せずに、新規ライセンス専用モードで Meeting Management を展開できます。

B.2 スマートアカウントとバーチャルアカウントの情報

スマートアカウントにはバーチャルアカウントを含めることができます。これにより、部門別などの任意の指定でライセンスを整理できます。Meeting Server と Meeting Management でスマート バーチャル アカウントを使用する場合の重要な注意事項を以下に示します。

- 単一の Meeting Management に対する Meeting Server クラスタを、それぞれ 1 つのユーザ定義のスマート バーチャル アカウントにリンクする必要があります。
- 各バーチャル アカウントは、スマート ライセンスを処理するように設定された 単一の Meeting Management サーバにのみ接続できます。
- 1 つの Meeting Management のみをスマートに構成します。スマートライセンス用に重複する 2 つ目の Meeting Management を構成**しない**ことを推奨します。ライセンス使用数の二重カウントが発生します。

- PMP Plus、SMP Plus、録音/ストリーミングのライセンスは、単一の Meeting Management インスタンスと単一のバーチャルアカウント内でのスマートライセンスを使用している複数のクラスタで共有できます。
- ACU ライセンスは、Meeting Management ライセンスダッシュボードでは使用できません。ACU は 3.0 以降ではサポートされていません。

B.3 Meeting Server のスマートライセンスの仕組み：概要

Meeting Server 3.0 以降でライセンスが機能するためには Meeting Management が必須です。スマートを使用した新規ライセンス、または既存ユーザーの場合はインストール済みライセンスファイルをサポートするために、Meeting Server と Meeting Management の間の新しい信頼とやり取りが導入されています。Meeting Management が Meeting Server にライセンスを付与できるようにする仕組みが、この信頼リンクです。

注：スマートライセンスの管理に Cisco Meeting Management 使用する方法の詳細については、『Meeting Management 3.0 管理者ガイド』を参照してください。

スマート ライセンスを実装するための概要レベルのワークフローを以下に示します。

1. Meeting Management をスマート ライセンス バーチャル アカウントに登録します。
2. Meeting Server の初回起動時には、ライセンス ステータス値は定義されていない状態です。

   注：ライセンスがなくても 90 日間はフル機能をトライアルモードで使用できます。

   ---

3. スマートライセンスを管理するためにセットアップされた Meeting Management インスタンスに Meeting Server が初めて接続すると、その Meeting Server に以前にライセンスが適用されていたかどうかがチェックされます。適用されていなかった場合は、ライセンス有効期限が 90 日後に設定されます。

   付録 B.5 に示されているように、ライセンスの有効期限は Meeting Management に表示され、clusterLicensing API でも返されます。

   注：機能ライセンスはいずれも有効期限が最大で 90 日後までとなります。

   ---

4. Meeting Management は、Meeting Server の遵守状態を確保するのに必要なライセンスがあることをチェックするために、毎日、クラスタの Meeting Server ライセンス使用状況を照合し、スマートアカウントに対してレポートします。スマート アカウントは Meeting Management に応答し、Meeting Server が遵守状態であるかどうかを提示します。その後、Meeting Management は、次のようにして有効期限を適切に設定します。

   a. Meeting Management が、ライセンスが存在しており特定の機能の使用権があることを特定すると、有効期限が 90 日後に延長されます。

> 注：Meeting Server が Meeting Management に接続して 90 日間の使用状況データを送信しなかった場合、Meeting Server のライセンスは更新されず、期限切れになります。ライセンスの有効期限が切れた場合の強制アクションの詳細については、セクション付録 B を参照してください。

ライセンスの使用数が使用権を超えている場合、またはライセンスが見つからない場合は、次の強制措置が発生します。

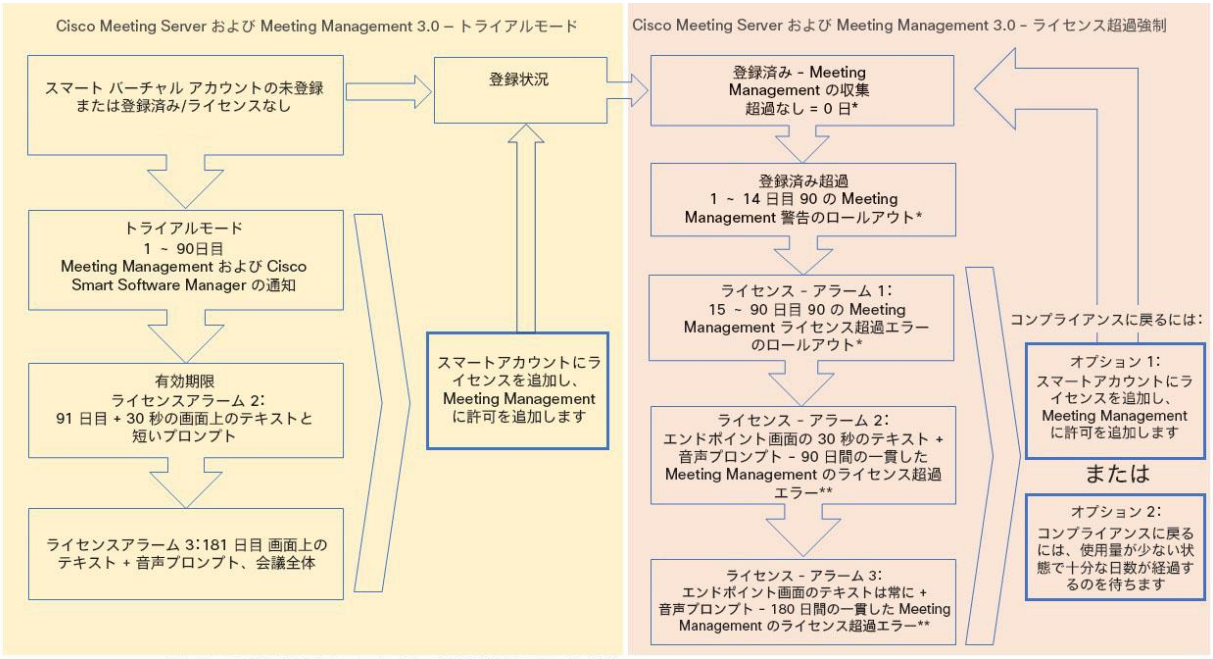
b. 遵守状態でなかったのが過去 90 日間のうち 15 日未満であることを Meeting Management が特定した場合、これを許容して Meeting Server の有効期限をその時点から 90 日後に再設定します。管理者に、ライセンス不足を通知するビジュアル警告が表示されます。

c. 遵守状態でなかったのが過去 90 日間のうち 15 日を超えていることを Meeting Management が特定した場合、第 1 レベルの強制（アラーム 1）、つまり、Meeting Management インターフェイスに非遵守の通知が表示されます。

d. ライセンス超過が続く場合、Meeting Management は 90 日間の計算をリセットせず、新規ライセンスの追加期限までの日数がカウントダウンされます。ライセンスが追加されない場合、付録 B に示すように、会議に参加するすべての参加者に対してアラームレベル 2 と 3 が有効になります。

付録 B に、左側に示したトライアルモードでの初回起動から、右側に示したライセンス超過による強制までの、強制フローを示します。

図 5：Cisco Meeting Server と Cisco Meeting Management スマート ライセンスの強制フロー



* ライセンス超過日数のカウント（つまり、使用量が権限よりも多い場合）
** Meeting Management がエラー状態（つまり、過去 90 日間のうち連続して 15 日間のライセンス超過がある状態）にある日数のカウント
† 正確な応答を確実にするために、管理者は Meeting Management 内でスマートアカウントに保持されているライセンス数を指定する必要があります

B.4 ライセンス機能の有効期限切れによる強制アクション

従来は、Meeting Server は再起動時にのみライセンス ファイルを評価していました。3.0 以降では、機能にライセンスが付与されているかどうかの現在のステータスは動的に変化する可能性があります。たとえば、機能ライセンスの有効期限が切れた（従来はこれは再起動されるまで明らかになりませんでした）、API の変更があったなどの理由によるものです。Meeting Management は、スマートライセンスを使用して強制アクションを計算します。

注：スマートライセンスポータルを使用して、「ライセンス不足」の電子メール通知を有効にすることができます。

機能ライセンスが期限切れになると、表 3 に示したアクションが発生します。

表 3：期限切れライセンスの強制アクション

機能	アクション
callBridge callBridgeNoEncryption PMP/SMP	期限切れの場合：すべての参加者およびすべてのミーティングに対し、ミーティング参加時にビジュアルなテキスト メッセージが画面に 30 秒間表示され、音声プロンプトが再生されます。（アラーム レベル 2） 90 日以上前に期限切れとなりライセンスが存在しない場合：それ以前と同様ですが、メッセージは永続的に表示されます。「Your deployment is out of licensing compliance, please contact your administrator（ライセンスが遵守されていません。管理者に連絡してください）」という音声プロンプトが再生されます。（アラームレベル 3）。ただし、暗号化された呼び出しは、ライセンスのない状態では処理されません。 注：前述のアクションを回避するために必要なのは callBridge または callBridgeNoEncryption のみです。
customizations	期限切れであるか、ライセンスが存在しない場合、カスタマイズ機能は会議中にアクティブになりません。
recording	期限切れまたはライセンスが存在しない場合、（サードパーティのレコーダーであるかどうかにかかわらず）新規の録画を開始できなくなります。 このライセンスは録画とストリーミングに該当するため、ストリーミングにも同じ制限が適用されます。

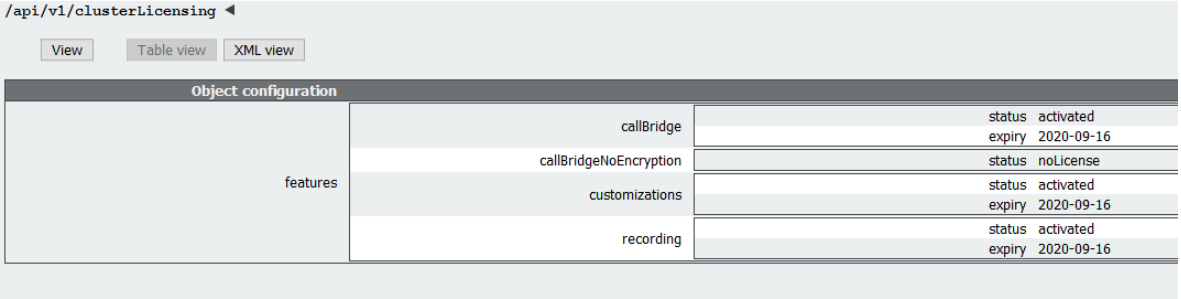
アラーム 2 と 3 をオフにするには、単純にライセンスをスマート アカウントに追加します。

B.5 ライセンス情報の取得方法（スマートライセンス）

Meeting Server Web 管理インターフェイスを使用してクラスタのライセンス情報を取得するには、次の手順を実行します。

1. Meeting Server Web 管理インターフェイスにログインし、[設定（Configuration）] > [API] を選択します。
2. API オブジェクトのリストから、/api/v1/clusterLicensing の後ろにある ▶ をタップします
3. クラスタの現在のライセンス ステータスが、次の例のように表示されます。

図 6：clusterLicensing API：ライセンスステータス



B.6 Cisco Meeting Server ライセンス

次の機能にはライセンスが必要です。

- Call Bridge
- 暗号化なしの Call Bridge
- カスタマイズ（カスタムレイアウト用）
- 録音またはストリーミング

機能ライセンスの他にユーザ ライセンスも購入する必要があります。ユーザ ライセンスには次の異なる 2 種類があります。

- PMP Plus、
- SMP Plus、

注：ライセンスがなくても 90 日間はフル機能をトライアルモードで使用できます。

ユーザ のライセンスについては、セクション B.8 を参照してください。

注：Cisco Meeting Server 1000、Cisco Meeting Server、VM ソフトウェア画像について、SIP メディア暗号化が有効になったアクティベーションキー、または SIP メディア暗号化が無効になったアクティベーションキー（暗号化されていない SIP メディア）の購入を選択することができます。暗号化されていない SIP メディアモードとアクティベーションキーの詳細については、『導入ガイド』を参照してください。

B.6.1 Personal Multiparty Plus ライセンス

Personal Multiparty Plus（PMP Plus）は、特にビデオ会議を頻繁に主催するユーザーに対して、ネームドホストライセンスを個別に割り当てます。これは、Cisco UWL ミーティングまたは Flex ミーティング（PMP Plus を含む）経由で購入できます。Personal Multiparty Plus は、ビデオ会議向けのオールインワン ライセンスです。（展開されている Cisco Meeting Server ハードウェアの制限内である限り）主催できる会議の参加者数に制限はありません。会議には、任意のエンドポイントから誰でも参加できます。ライセンスでは、フル HD 1080p60 品質までのビデオ、オーディオ、およびコンテンツ共有がサポートされています。

注：Unified Communications Manager を使用すると、アドホック会議の開催者を特定することができます。また、開催者に PMP Plus ライセンスが割り当てられている場合は、そのライセンスが会議で使用されます。

注：個人の PMP Plus を使用したアクティブなコール数を決定するには、次の API オブジェクトでパラメータ **`callsActive`** を使用します：**`/system/multipartyLicensing/activePersonalLicenses`**。通常、2 件のコールをアクティブにし、1 つの開始と他方の終了を可能にします。Call Bridge のクラスタ上にコールがある場合、次の API オブジェクトでパラメータ **`weightedCallsActive`** を使用します。**`/system/multipartyLicensing/activePersonalLicenses`**（クラスタ内の各 Call Bridge について）。クラスタ全体の **`weightedCallsActive`** の合計数は、個人の PMP Plus ライセンスを使用したクラスタ上で区別されるコール数に一致します。PMP Plus ライセンスを超過した場合は、SMP Plus ライセンスが割り当てられます（セクション B.9 を参照）。

B.6.2 Shared Multiparty Plus ライセンス

Shared Multiparty Plus（SMP Plus）では同時ライセンスが提供されており、ビデオ会議を主催する頻度が低い複数のユーザが共有できます。Shared Multiparty Plus は、PMP Plus ホストライセンスを持たないすべての従業員が、ビデオ会議へのアクセスに使用できます。これは、導入しているルーム システムが多数の従業員によって共有される場合に最適です。PMP Plus または SMP Plus ライセンスを使用しているすべてのユーザは、同じエクスペリエンスを享受でき、スペースでのミーティングのホスト、アドホックミーティングの開始、または今後のミーティングのスケジュール設定を行うことができます。共有ホスト ライセンスごとに 1 つの同時ビデオ会議がサポートされます。（導入されているハードウェアの制限内である限り）参加者数の制限はありません。

注：必要な SMP Plus ライセンスの数を決定するには、API オブジェクト **`/system/multipartyLicensing`** でパラメータ **`callsWithoutPersonalLicense`** を使用します。Call Bridge のクラスタ上にコールがある場合、クラスタ内の Call Bridge ごとに API オブジェクト **`/system/multipartyLicensing`**でパラメータ **`weightedCallsWithoutPersonalLicense`** を使用します。クラスタ全体の **`weightedCallsWithoutPersonalLicense`**の合計数は、SMP Plus ライセンスを必要とする、クラスタ上で区別されるコール数に一致します。

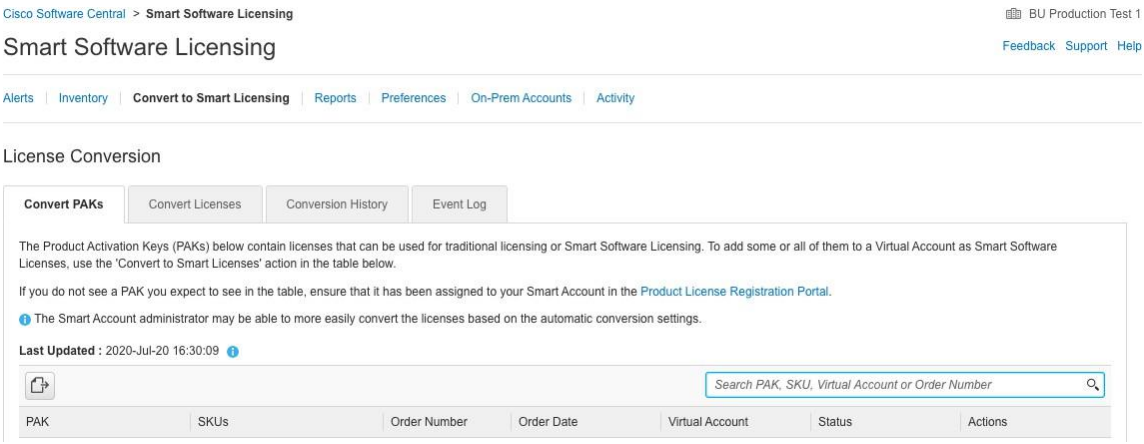
B.7 スマートライセンス登録プロセス

スマートライセンスを有効にするには、以下の手順を実行します。

1. Cisco Smart Software Manager（CSSM）ポータルにサインインし、Meeting Server ライセンスを持つバーチャルアカウントを選択します。
2. 登録トークンを生成します。
3. トークンをクリップボードにコピーします。
4. ライセンスレポートに使用する Meeting Management のインスタンスを開きます。
5. [設定（Settings）] ページ の [ライセンス（Licensing）] タブに移動します。
6. [変更（Change）] をクリックします。
7. [スマートライセンス（Smart Licensing）] を選択して、[保存（Save）] します。
8. [登録（Register）] をクリックします。
9. 登録トークンを貼り付けます（これにより、Meeting Management はスマートライセンスポータルに接続できます）。
10. [登録（Register）] をクリックします。
11. 登録された場合は、バーチャルアカウントにあるライセンスの数を確認します。
12. Meeting Management で、[ライセンス（Licenses）] ページに移動します。
13. バーチャルアカウントにあるライセンスのライセンス情報を入力します。

    バーチャルアカウント内でライセンスが表示されない場合、[ライセンスの変換（Convert Licenses）] タブを使用して PAK を検索します。その後、 図 7 のとおりに [ライセンスの変換（Convert Licenses）] を選択します。（ライセンスが見当たらない場合は、licensing@cisco.com にE メールを送信してケースをオープンしてください）。

図 7：スマートライセンスのライセンス転換



B.8 ユーザーに対する Personal Multiparty ライセンスの割り当て

このプロセスでは、ユーザを単一の LDAP ソースからインポートする必要があります。『Meeting Management 管理者ガイド』の「プロビジョニング：ユーザーをインポート」の章を参照してください。

B.8.1 特定のユーザにライセンスがあるかを判断する方法

1. API オブジェクトのリストから、/users の後ろにある ▶ をタップします。
   a. 特定のユーザーの object id を選択します。
   b. このユーザに関連付けられている userProfile の object id を特定します
2. API オブジェクトのリストから、/userProfiles の後ろにある ▶ をタップします
   a. 特定の userProfile の object id を選択します。
   b. パラメータ hasLicence の設定を検索します。true に設定されている場合、手順 1 で特定されたユーザーは Cisco Multiparty ユーザーライセンスに関連付けられています。false に設定されている場合、ユーザは Cisco Multiparty ユーザライセンスに関連付けられていません。

   注：userProfile が削除されている場合、userProfile は ldapSource とインポートされたユーザに対して設定されていません。

B.9 Cisco Multiparty ライセンスの割り当て方法

スペースで会議を開始すると、Cisco のライセンスがそのスペースに割り当てられます。
Cisco Meeting Server がどのライセンスを割り当てるかは、次のルールによって決まります。

- スペース所有者が定義されており、Cisco PMP Plus ライセンスが割り当てられた Meeting Server がインポートした LDAP ユーザに対応している場合、そのユーザが会議でアクティブであるかどうかに関係なく、そのオーナーのライセンスが割り当てられます。割り当てられていない場合は、その後
- Cisco Unified Communications Manager のアドホックエスカレーション経由で会議が作成された場合、Cisco Unified Communications Manager は会議をエスカレーションしたユーザの GUID を提供します。その GUID が、Meeting Server によってインポートされ、Cisco PMP Plus ライセンスを割り当てられているユーザに対応している場合 、そのユーザのライセンスが割り当てられます。それ以外の場合で、
- 会議が Cisco TMS バージョン 15.6 以降を使用してスケジュールされている場合、TMS は会議の所有者を提供します。そのユーザが、ユーザ ID/電子メールアドレスを使用して割り当てられた Cisco PMP Plus ライセンスを持つ Meeting Server のインポートされた LDAP ユーザーに対応する場合、そのユーザーのライセンスが割り当てられます。割り当てられていない場合は、
- Cisco SMP プラスライセンスが割り当てられています。

B.10 Cisco Multiparty ライセンスの使用状況の判断

Meeting Management を使用して、Multiparty ライセンスの使用状況を確認することを推奨します。ただし、API は使用できます。

以下の表 4 には、Multiparty ライセンスの使用を決定するために使用できる API オブジェクトとパラメータをリストしています。

表 4：Multiparty ライセンスの使用状況に関連するオブジェクトとパラメータ

API オブジェクト	パラメータ	使用先
/system/licensing	personal, shared	Cisco Meeting Server のコンポーネントが Multiparty ライセンスを持ち、アクティブ化されているかどうかを確認します。値は次のとおりです：ライセンスなし、アクティブ化、猶予、有効期限切れ。 有効期限と番号の上限も提供します。
/system/multipartyLicensing	PersonalLicenseLimit、 sharedLicenseLimit、 personalLicenses、 callsWithoutPersonalLicense、 weightedCallsWithoutPersonalLicense	ライセンス数について、使用可能なものと使用中のものを示します
/system/multipartyLicensing/ activePersonalLicenses	callsActive、 weightedCallsActive	Personal Multiparty Plus ユーザライセンスを使用しているアクティブコールの数を示します。
/userProfiles	hasLicense	ユーザが Cisco Multiparty ユーザライセンスに関連付けられているかどうかを示します

これらの追加オブジェクトと、Cisco Multiparty ライセンスをサポートするフィールドについての詳細は、『Cisco Meeting Server API リファレンスガイド』を参照してください。

B.11 SMP Plus ライセンス使用率の計算

次の特定のシナリオでは、会議に使用される SMP Plus ライセンスは、フル SMP Plus ライセンスの 1/6 に減少します。

- 参加者がビデオを使用していない場合の音声のみの会議は、
- Meeting Server が録音またはストリーミングを行っている場合を除き、Lync ゲートウェイコールは、その時点では完全な会議と見なされ、完全な SMP Plus ライセンスが消費されます。
- Web アプリと SIP エンドポイント、または 2 つの Web アプリが関係するポイントツーポイントコール（Meeting Server が録音またはストリーミングの場合を除く）は、この時点ではフル会議と見なされ、SMP Plus のフルライセンスが使用されます。

SMP Plus のフルライセンスでは、オーナープロパティが定義されていないスペースから、または PMP Plus ライセンスのないインポート済み LDAP ユーザが所有している、または PMP Plus ライセンスがすでに使用されているインポート済み LDAP ユーザが所有している、すべての音声ビデオ会議に使用されます。これは参加者の数に関係ありません。

注：ポイント ツー ポイント コールは次のように定義されます。

- Meeting Server に永続的なスペースがない
- レコーダーまたはストリーマーを含む、2 人以下の参加者
- LYNC AVMCU でホストされている参加者がいない

これには、Lync ゲートウェイコール、および他のタイプのコール（ポイントツーポイント Web アプリから Web アプリ、Web アプリから SIP、SIP から SIP まで）が含まれます。

B.12 Meeting Server からのライセンス使用状況スナップショットの取得

管理者は Meeting Server からライセンス使用状況を取得できます。Web 管理インターフェイスを使用している間は、POSTMAN などの API ツールを使用しますが、これらのツールにはアクセスできません。

展開内の Meeting Server のホスト ID を取得するには、**`/system/MPLicenseUsage/knownHosts`** で GET を使用します。リストの最初のページ以外のホスト ID を取得するために必要な場合は、オフセットと制限を指定します。

指定されたホスト ID を持つ Meeting Server の Call Bridge からライセンスの使用状況を取得するには、**`/system/MPLicenseUsage`**で GET を使用します。スナップショットの開始時刻と終了時刻を指定します。
使用中の個人ライセンスの数、使用中の共有ライセンスの数（音声のみ、ポイントツーポイント、または録音でもポイントツーポイントでもない）、録音されているコールの数、およびストリーミングされたコールの数に関する情報を提供します。

注：個人ライセンスと共有ライセンスは、コールがまたがる Call Bridges の数によって正規化されます。

B.13 ライセンスレポート

Meeting Management には過去 90 日間のライセンスレポート/使用状況の情報があり、Cisco Smart Software Manager にもライセンスレポート情報があります。録音ライセンスの使用状況は、同時に録音する会議の数を示します。同様に、ストリーミングライセンスの使用状況は、同時にストリーミングされている会議の数を示します。

B.14 レガシーライセンスファイル方式

このセクションは、従来のライセンス方式を使用している場合にのみ適用されます。バージョン 3.4 から、従来のライセンスのサポートは非推奨になりました。既存のローカルライセンスは、ライセンスの有効期限が切れるまで引き続きサポートされます。

B.14.1 ライセンスファイルの適用

Cisco Meeting Server 2000 にはライセンスファイルが必要です。このライセンスを適用すると、Call Bridge がアクティブになり、会議を作成できるようになります。ライセンスファイルは、ポート A に割り当てられた MAC アドレスに関連付けられています。
A.
ライセンスを購入した後は、この章に従って、従来のライセンス方法を使用している場合にのみ Cisco Meeting Server にライセンスを適用してください。

B.14.1.1 Cisco Meeting Server 2000 へのライセンスファイルの転送

この項は、Call Bridge がリッスンするポートがすでに設定されており、Call Bridge 証明書がアップロード済みであることを前提としています。

SFTP を使用して、Meeting Server にライセンス ファイルを転送します。すでにポート A の IP アドレスがわかっている場合は、手順 1 を省略してください。

1. セクション 3.4 で設定したポート A の IP アドレスに SSH を介して接続し、セクション 3.3 で設定した admin ユーザ名とパスワードを使用してログインします。MMP コマンド **`ipv4 a`** または **`ipv6 a`** を使用して、ポート A の IP アドレスを調べます。
2. SFTP を使用して、cms.lic ファイルをポート A の IP アドレスにアップロードします。
3. ポート A の IP アドレスに SSH を介して接続し、MMP の admin ユーザの資格情報を使用してログインします。
4. MMP コマンド **`callbridge restart`** を使用して Call Bridge を再起動します。これにより、ライセンス ファイルが適用されます。
5. Call Bridge を再起動した後、MMP コマンド **`license`** を入力して、ライセンスのステータスを確認します。

   有効化された機能と有効期限が表示されます。

注：バージョン 3.0 より、ライセンスがなくても 90 日間はフル機能をトライアルモードで使用できます。この場合、この間に Web 管理インターフェイスに「この CMS は現在ライセンスがありません」と表示されます。スマートライセンスの詳細と 3.0 におけるライセンスの仕組みについては、「付録 B」を参照してください。

B.14.2 従来のライセンス方法を使用したCisco のユーザーライセンスの取得

このセクションでは、Cisco パートナーから Meeting Server に必要なライセンスをすでに購入し、PAK コードを受け取っていることを前提としています。

この手順に従い、シスコ製品ライセンス登録ポータル を使用して、PAK コードと Meeting Server の MAC アドレスを登録してください。

1. Meeting Server の MAC アドレスを取得するには、サーバの MMP にログインして **`iface a`** の MMP コマンドを入力します。
2. シスコライセンス登録ポータルを開いて、PAK コードと Meeting Server の MAC アドレスを登録します。
3. PAK に R-CMS-K9 アクティベーション ライセンスが割り当てられていない場合は、機能ライセンスの他にこの PAK が必要です。
4. ライセンスポータルでは、ライセンスファイルの圧縮コピーが電子メールで送信されます。zip ファイルを解凍し、解凍後の xxxxx.lic ファイルの名前を **`cms.lic`** に変更します。
5. SFTP クライアントを使用して Meeting Server にログインし、Meeting Server ファイルシステムに **`cms.lic`** ファイルをコピーします。
6. MMP コマンド **`callbridge restart`** を使用して Call Bridge を再起動します。
7. Call Bridge を再起動した後、MMP コマンド **`license`** を入力して、ライセンスのステータスを確認します。

   有効化された機能と有効期限が表示されます。

付録 C ブランディング

Meeting Server 上でホストされるミーティングの参加体験の側面にはブランディングできるものがあり、それらは次のとおりです。

- サインイン背景イメージの Web アプリ、サインインロゴ、サインインロゴアイコンの下のテキスト、ブラウザタブのテキスト
- IVR メッセージ
- SIP および Lync の参加者のスプラッシュ画面イメージと、すべての音声プロンプトまたはメッセージ
- ミーティングへの招待メールのテキストを入力します。

1 つのリソースセット（Web アプリの 1 つのサインインページ、1 組の音声指示、1 つの招待テキスト）だけを指定した単一ブランドを適用する場合、それらのリソースは導入内のすべてのスペース、IVR、および Web Bridge に使用されます。複数のブランディングでは、異なるスペース、IVR、および Web Bridge に異なるリソースを使用できます。リソースは、API を使用してシステム、テナント、スペースまたは IVR のレベルで割り当てることができます。

ブランディングの詳細については、『カスタマイズガイドライン』を参照してください。

付録 D Cisco Meeting Server 2000 と仮想化展開の間での MMP と API の違い

D.1 特定の MMP コマンドの違い

MMP コマンドの全セットについては、MMP コマンド リファレンスで詳しく説明されています。Cisco Meeting Server 2000 の実行は、仮想化された Cisco Meeting Server と比べるといくつかの違いがあります。

コマンド	Cisco Meeting Server 2000 上	Cisco Meeting Server 1000 上、および仮想化された Cisco Meeting Server上
shutdown	MMP では利用できません。ブレードサーバの電源を切断するには、まず Cisco UCS Manager 上で電源を切断します。	VSphere の電源ボタンは使用しないでください。代わりに、**shutdown** コマンドを使用します。
health	MMP では利用できません。Cisco UCS Manager を使用します。	使用不可
serial	サーバのシリアル番号を返します。	使用不可
dns	インターフェイスは指定しないでください。 例： **dns add forwardzone <domain-name> <server ip>**	インターフェイスは指定しないでください。 例： **dns add forwardzone <domain-name> <server ip>**
user evict	バージョン 2.9 から利用可能	使用可能

D.2 異なるプラットフォームで有効にされたコンポーネント間の違い

次の表に、Cisco Meeting Server のさまざまなプラットフォームで利用可能なコンポーネントを示します。プラットフォーム上で利用できないコンポーネントの場合、そのコンポーネントに固有の MMP および API コマンドも利用できません。たとえば、TURN Server の MMP および API コマンドは、Cisco Meeting Server 2000 では利用できません。

コンポーネント	Cisco Meeting Server 2000 上	Cisco Meeting Server 1000 上、および仮想化された Cisco Meeting Server上
Call Bridge	使用可能	使用可能

コンポーネント	Cisco Meeting Server 2000 上	Cisco Meeting Server 1000 上、および仮想化された Cisco Meeting Server上
Web ブリッジ 3	使用可能	使用可能
データベース	使用可能	使用可能
スケジューラ	使用可能	使用可能
TURN サーバ	使用不可	使用可能
レコーダー	使用不可	使用可能
アップローダ	使用不可	使用可能
ストリーマ	使用不可	使用可能
SNMP MIB	現在使用不可	使用可能

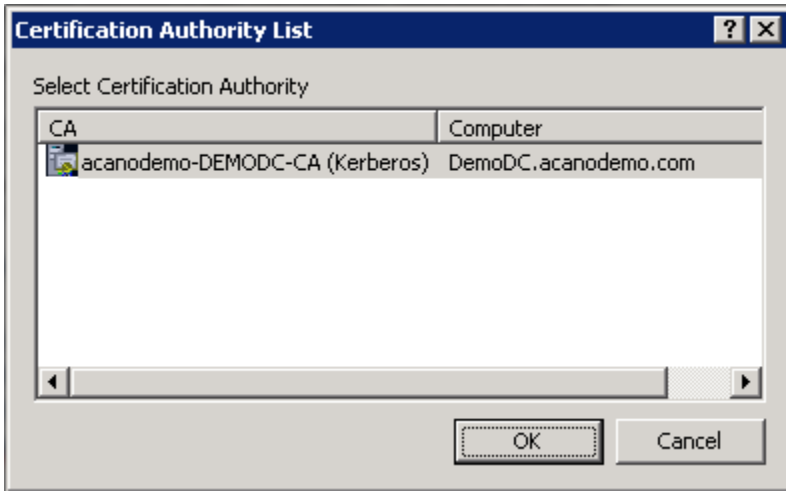
付録 E ローカル認証局によって署名された証明書の作成

この付録では、Active Directory Certificate Services のロールがインストールされている Microsoft Active Directory サーバーなどの ローカル CA を使用して、CSR に署名する手順について説明します。

1. ファイルを CA に転送します。
2. CA サーバ上のコマンド ライン管理シェルで、次のコマンドを、パスと CSR 名をお客様の情報に置き換えて発行します。

   ```
   certreq -submit -attrib "CertificateTemplate:WebServer"
   C:\Users\Administrator\Desktop\webadmin.csr
   ```

3. このコマンドを入力すると、次のような CA 選択リストが表示されます。正しい CA を選択して、[OK] をクリックします。

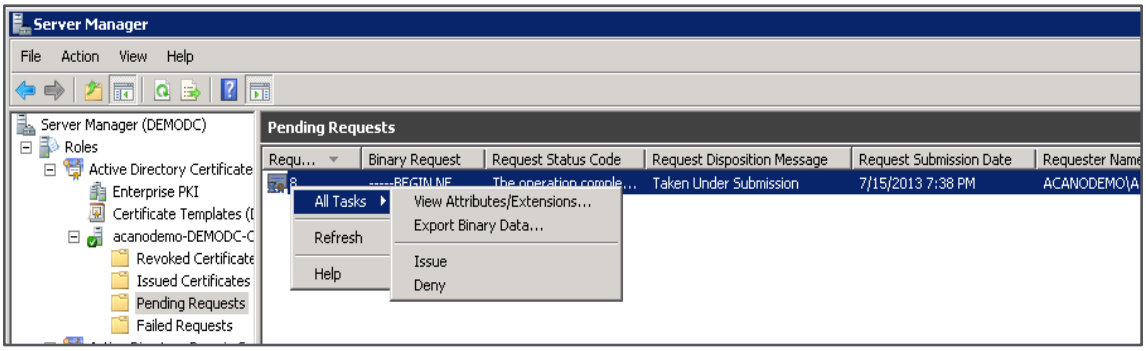


4. 次のいずれかを実行します。
   - 証明書発行許可を持つ Windows アカウントを使用している場合は、生成された証明書を（webadmin.crt などの名前で）保存するよう求めるプロンプトが表示されます。下記の手順 c に進みます。
   - 生成された証明書を発行するためのプロンプトが表示されない場合、代わりに次のようにコマンド プロンプト ウィンドウに「証明書の要求は保留中です：提出済みです（Certificate request is pending: taken under submission）」というメッセージが表示され、「要求 ID（Request ID）」がリスト表示されます。RequestID をメモしてから、下記の手順を実行し、その後手順 c に進みます。

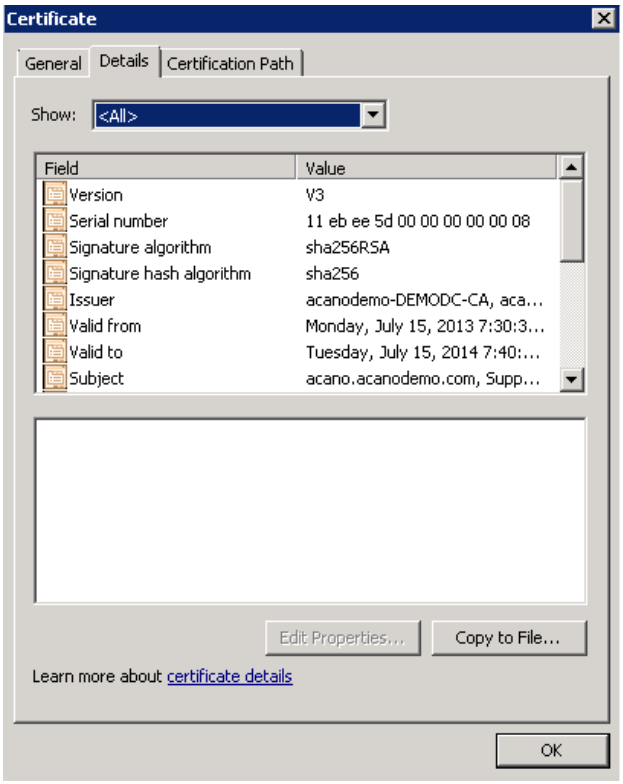
```
C:\Users\Administrator>certreq -submit -attrib "CertificateTemplate:WebServer" C
:\Users\Administrator\Desktop\demokitcsr.pem
Active Directory Enrollment Policy
  {0BD5D0B7-591F-4C77-AFEC-3C0E470F77D5}
  ldap:
RequestId: 8
RequestId: "8"
Certificate request is pending: Taken Under Submission (0)

C:\Users\Administrator>_
```

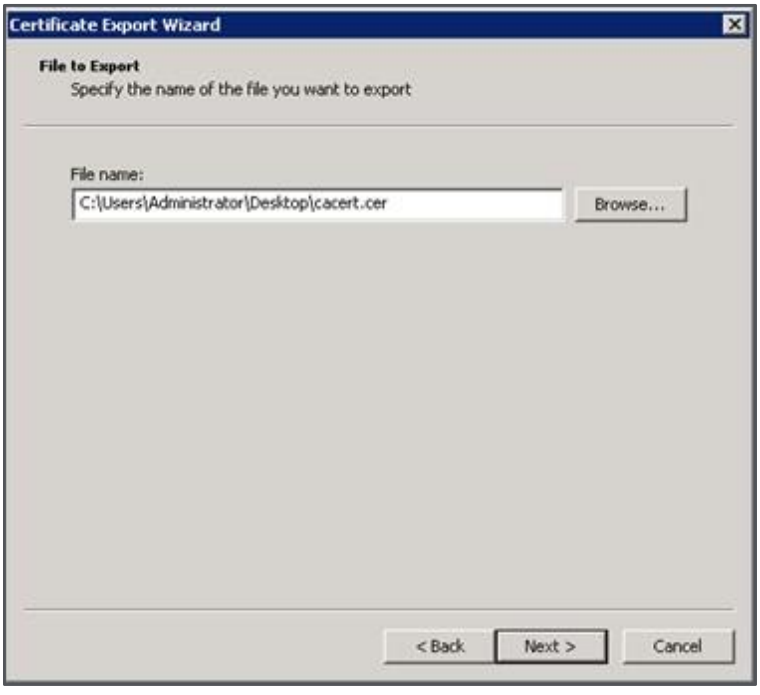
5. CA の [サーバーマネージャ（Server Manager）] ページで、CA のロールの下にある Pending Requests フォルダを見つけます。
6. CMD ウィンドウに表示された要求 ID に一致する保留中の要求を右クリックして、[すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。



7. 発行された署名付き証明書が [発行した証明書（Issued Certificates）] フォルダに保存されます。証明書をダブルクリックして開き、[**詳細（Details）**]タブを開きます（右図を参照）。



8. [ファイルにコピー（Copy to File）] をクリックすると、[証明書エクスポートウィザード（Certificate Export Wizard）] が開始します。
9. Base-64 encoded X.509（.CER）を選択して、[次へ（Next）] をクリックします。
10. 証明書の保存先を開き、 **webadmin** などの名前を入力して、[次へ（Next）] をクリックします。



11. 生成された証明書の名前を **webadmin.crt** に変更します。

SFTP を使用して証明書（webadmin.crt など）と秘密キーを Cisco Meeting Server の MMP へ転送します。詳細についてはセクション 4.5.2を参照してください。

注意：Web Enrolment 機能がインストールされている CA を使用している場合は、BEGIN CERTIFICATE REQUEST の行と END CERTIFICATE REQUEST の行を含めて CSR テキストをコピーすることによって発行できます。証明書が発行されたら、証明書チェーンはコピーせず、証明書のみをコピーします。BEGIN CERTIFICATE 行と END CERTIFICATE 行など、すべてのテキストを必ず含めてから、テキスト ファイルに貼り付けてください。次に、このファイルを証明書として、拡張子を .pem、.cer、または .crt で保存します。

付録 F UCS Manager のアップグレード

Cisco Meeting Server 2000 は、2 つの UCS 6324 ファブリックインターコネクトと 8 つの UCS B シリーズブレードサーバーの計算リソースが入力された Cisco UCS 5108 ブレードサーバーシャーシで実行されます。

『Cisco UCS Manager ファームウェア管理ガイド』リリース 4.2 (1f)、4.1、または 4.0 の説明に従って、ファームウェアをアップグレードします。ここをクリックして、相互運用性がテストされた利用可能な UCS Manager のバージョンを表示します。

この付録には、ブレードのファームウェアバージョンの設定に使用する CMS2000-FW ポリシーを更新するために必要な簡単な手順が含まれます。

F.1 Cisco UCS Manager ファームウェア 4.0(x)、4.1(x)、または 4.2(1f) へのアップグレード

3.1(3) または 3.2(3) より前のリリースからリリース 4.0(x)、4.1(x)、または 4.2(1f) への直接アップグレードはサポートされていません。リリース 4.0(x)、4.1(x)、または 4.2(1f) にアップグレードするには、次の順序で手順を実行します。

1. リリース 3.1(3) または 3.2(3) にインフラストラクチャ A バンドルをアップグレードします。
2. CMS2000-FW ホスト ファームウェア パッケージを変更して、すべてのサーバの B バンドルをリリース 3.1 (3) または 3.2 (3) にアップグレードします。
3. リリース 4.0(x)、4.1(x)、または 4.2(1f) にインフラストラクチャ A バンドルをアップグレードします。
4. CMS2000-FW ホスト ファームウェア パッケージを変更して、すべてのサーバーの B バンドルをリリース 4.0(x)、4.1(x)、または 4.2(1f) にアップグレードします。

F.2 CMS2000-FW ポリシーのホスト ファームウェア パッケージの更新

前提条件：

ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認します。

F.2.1 CLI を使用した CMS2000-FW ポリシーの更新

```
UCS-A# scope org CMS
UCS-A /org # scope fw-host-pack CMS2000-FW
UCS-A /org/fw-host-pack # show detail
```

```
Server Host Pack:
Name: CMS/CMS2000-FW
Mode: Staged
Description: CMS2000 Blade Server Firmware Package
Policy Owner: Local
B-Series Package Version: 3.2(3k)B
C-Series Package Version:
Service Pack Version:

UCS-A /org/fw-host-pack # set blade-vers 4.1(1d)B
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack # top
UCS-A#
```

F.2.2 GUI を使用した CMS2000-FW ポリシーの更新

1. [ナビゲーション（Navigation）] ペインで [サーバ（Servers）] をクリックします。
2. [サーバ（Servers）] > [ポリシー（Policies）] を展開します。
3. CMS 組織のノードを展開します。
4. [ホスト ファームウェア パッケージ（Host Firmware Packages）] を展開し、CMS2000-FW ポリシーを選択します。
5. [ワーク（Work）] ペインで [全般（General）] タブをクリックします。
6. ホスト ファームウェア パッケージのコンポーネントを変更するには、[パッケージ バージョンの変更（Modify Package Versions）] をクリックします。[パッケージバージョンの変更（Modify Package Versions）] ウィンドウが表示されます。
7. ブレードパッケージを変更するには、[ブレードパッケージ（Blade Package]）] ドロップダウンリストで、ブレードパッケージバージョンを選択します。
8. [OK] をクリックします。

   Cisco UCS Manager はモデル番号とベンダーを、このポリシーがインクルードされているサービスプロファイルに関連付けられているすべてのサーバーと照合します。モデル番号とベンダーがポリシー内のファームウェアバージョンに一致する場合、Cisco UCS Manager は、サービスプロファイルに含まれているメンテナンスポリシー内の設定に従ってファームウェアを更新します。

付録 G その他の Cisco UCS Manager コマンド

この付録では、Cisco UCS Manager のいくつかのコマンドについて説明しています。これらのコマンドは Cisco Meeting Server 2000 の初期セットアップ時に使用すると便利ですが、必須ではありません。

G.1 ブレードサーバの電源切断

シャーシから電源を取り外す前に、8 台のブレードサーバーすべての電源を切る必要があります。

例：

```
UCS-A# scope org /CMS
UCS-A /org # scope service-profile CMS2000-MMP
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA2
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA3
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA4
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA5
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA6
UCS-A /org/service-profile# power down
UCS-A /org/service-profile*# commit-buffer
UCS-A /org/service-profile# exit
UCS-A /org # scope service-profile CMS2000-MEDIA7
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA8
UCS-A /org/service-profile # power down
```

```
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # exit
UCS-A#
```

G.2 スロット間のブレードサーバのスワッピング

ラックへの取り付けの最中にブレードをスロット間でスワッピングした場合、現在のスロットで使用する前にブレードを認識する必要があります。**show server status**コマンドを使用してスロットを確認し、不一致のあるスロットを認識します。この認識により、ブレードサーバーとファブリック インターコネクト モジュール間の接続が再構築されます。この処理は、完了までに最大 20 分ほどかかります。

注：2 台のハード ドライブを取り付けたブレードサーバは、スロット 1 に設置する必要があります。

```
UCS-A # show server status
 Server  Slot Status    Availability   Overall Status    Discovery
------------------------------  -------------------  ----------------------------------------
 1/1     Equipped       Unavailable    Ok                Complete
 1/2     Equipped       Unavailable    Ok                Complete
 1/3     Equipped       Unavailable    Ok                Complete
 1/4     Mismatch       Unavailable    Compute Mismatch  Retry
 1/5     Mismatch       Unavailable    Compute Mismatch  Retry
 1/6     Equipped       Unavailable    Ok                Complete
 1/7     Equipped       Unavailable    Ok                Complete
 1/8     Equipped       Unavailable    Ok                Complete
UCS-A# acknowledge slot 1/4
UCS-A* # acknowledge slot 1/5
UCS-A* # commit-buffer
UCS-A#
```

すべてのブレードが検出されるまで待ってから、続行します。

```
UCS-A # show server status
 Server  Slot Status    Availability   Overall Status    Discovery
------------------------------  -------------------  ----------------------  ---------------
 1/1     Equipped       Unavailable    Ok                Complete
 1/2     Equipped       Unavailable    Ok                Complete
 1/3     Equipped       Unavailable    Ok                Complete
 1/4     Equipped       Unavailable    Ok                Complete
 1/5     Equipped       Unavailable    Ok                Complete
 1/6     Equipped       Unavailable    Ok                Complete
 1/7     Equipped       Unavailable    Ok                Complete
 1/8     Equipped       Unavailable    Ok                Complete
```

G.3 Serial over LAN の無効化（オプション）

MMP へのアクセスに Serial over LAN 接続を使用しない場合は、SoL ポリシーを無効にできます。

注意：MMP の初期設定を完了するには SoL が必要です。ネットワーク IP アドレスで Cisco Meeting Server を設定するまで、SoL を無効にしないでください。

```
UCS-A# scope org /CMS
UCS-A /org/ # scope sol-policy CMS2000-MMP-SOL
UCS-A /org/sol-policy # show detail

SOL Policy:

  Name: CMS/CMS-2000-SOL
   SOL State: Enable
   Speed:115200
   Decription:
   Policy Owner: Local

UCS-A /org/sol-policy # disable
UCS-A /org/sol-policy* # commit-buffer
UCS-A /org/sol-policy # exit
UCS-A /org # exit
UCS-A#
```

G.3.1 無効化した Serial over LAN の再有効化

SoL を再有効化する必要があるのは、以前に SoL を無効化したが、SoL が必要になった場合のみです。

```
UCS-A# scope org /CMS
UCS-A /org # scope sol-policy CMS2000-MMP-SOL
UCS-A /org/sol-policy # show detail

SOL Policy:

  Name: CMS/CMS-2000-SOL
   SOL State: Disable
   Speed:115200
   Decription:
   Policy Owner: Local

UCS-A /org/sol-policy # enable
UCS-A /org/sol-policy* # commit-buffer
UCS-A /org/sol-policy # exit
UCS-A /org # exit
UCS-A#
```

Cisco の法的情報

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となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、これらは、参考資料によって本書に含まれています。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。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。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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。マニュアルの中の例、コマンド出力、ネットワーク トポロジー図、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 IP 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。

この文書の印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理対象外と見なされます。最新版については、現在のオンライン バージョンを参照してください。

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

Cisco の商標