Cisco Meeting Server

Cisco Meeting Server 2000

インストールガイド

2020 年 2 月 6 日

目次

変更事項

バージョンの日付	変更
2019 年 10 月 25 日	Meeting Server 2000 で利用できない MMP コマンド **user evict** が追加されました。
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 概要

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、Call Bridge、Web Bridge、XMPP サーバ 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、分割された Meeting Server 展開の Edge サーバとしては適していません。これは、TURN サーバおよびロード バランサ Edge コンポーネントが利用できないためです。外部の Cisco Meeting App クライアントに対するファイアウォールト越えのサポートが必要な場合は、別の Cisco Meeting Server 1000 または仕様ベースの VM サーバ上に、TURN サーバとロード バランサ コンポーネントを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、1 つの分割サーバ展開のコア サーバとして、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 台のサーバとして導入できます。Cisco Meeting Server 1000、Acano X シリーズ サーバ、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：仮想化導入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ず、この逆もできません。また、Acano X シリーズ サーバからバックアップを作成して、Cisco Meeting Server 2000 にロールバックすることも、その逆もできません。

{b}注：{/b}2019 年 8 月頃から、新しい Cisco Meeting Server 2000 では、ファブリック相互接続のフェールオーバーがデフォルトで有効になってます。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。

Cisco Meeting Server1.1　2000 のコール キャパシティ

バージョン 2.4 では、Cisco Meeting Server 2000 の HD/FullHD コール キャパシティは引き上げられましたが、新しいキャパシティは Call Bridge グループおよび負荷分散ではサポートされていませんでした。詳細は表 2 を参照してください。バージョン 2.6 から Cisco Meeting Server 2000 プラットフォームの負荷制限ロジックが更新され、次の表 1 に示すコール キャパシティが、Call Bridge グループ、Call Bridge クラスタリング、負荷分散を使用して展開できるようになりました。

バージョン 2.6 から、Cisco Meeting Server 2000 プラットフォームの **loadlimit** が 50 万から 70 万に増加し、異なるコール解像度の負荷計算が新しい 70 万制限に一致するように更新されました他の Meeting Server プラットフォームの負荷制限は、以前と同様に維持されます。これらの変更は Cisco Meeting Server 2000 にのみ適用されます。

{b}注：{/b}負荷制限と負荷分散を使用している既存の Cisco Meeting Server 2000 展開では、バージョン 2.6 へのアップグレード後に、この新しい機能を使用して、SD コールのキャパシティの低下を避けるために、**loadlimit** の値を手動で更新する必要があります。

表 1：Cisco Meeting Server 2000 バージョン 2.6 以降のコール キャパシティ

コールのタイプ	Cisco Meeting Server 2000 (シングル、クラスタ、または Call Bridge グループ内) のバージョン 2.6 からのコールキャパシティ
フル HD 通話 (1080p30)	350
HD (720p30)	700
SD (448p30)	1000
音声	3000

表 2：Cisco Meeting Server 2000 バージョン 2.4 および 2.5 のコール キャパシティ

コールのタイプ	単一 Cisco Meeting Server 2000 またはクラスタ化されたサーバ (バージョン 2.4 および 2.5) のコールキャパシティ	Call Bridge グループ内の Cisco Meeting Server 2000 のコールキャパシティ、バージョン 2.4 および 2.5
フル HD 通話 (1080p30)	350	250
HD (720p30)	700	500
SD (448p30)	1000	1000
音声	3,000	3,000

{b}注：{/b} 上記の表の容量は計算負荷に基づいて概算であり、実際のキャパシティは動的解像度、ストリーム数、コンテンツ共有などのリアルタイム要因によって異なります。コールカウントには、分散リンク、レコーダ/クライアント、ゲートウェイコールレッグなどの非参加者コールレッグも含まれます。負荷制限は、限定された参加者数のメトリックではなく、単一の Meeting Server インスタンス上のすべての要素にわたって総使用率を制限する手段を提供します。

{b}注：{/b}すべての Meeting server プラットフォームでのサーバごとの会議ごとの参加者の制限は 450 のままで、分散型サーバ間の会議あたりの参加者数は 2600 のままです。

Cisco Meeting Server1.2 2000 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。

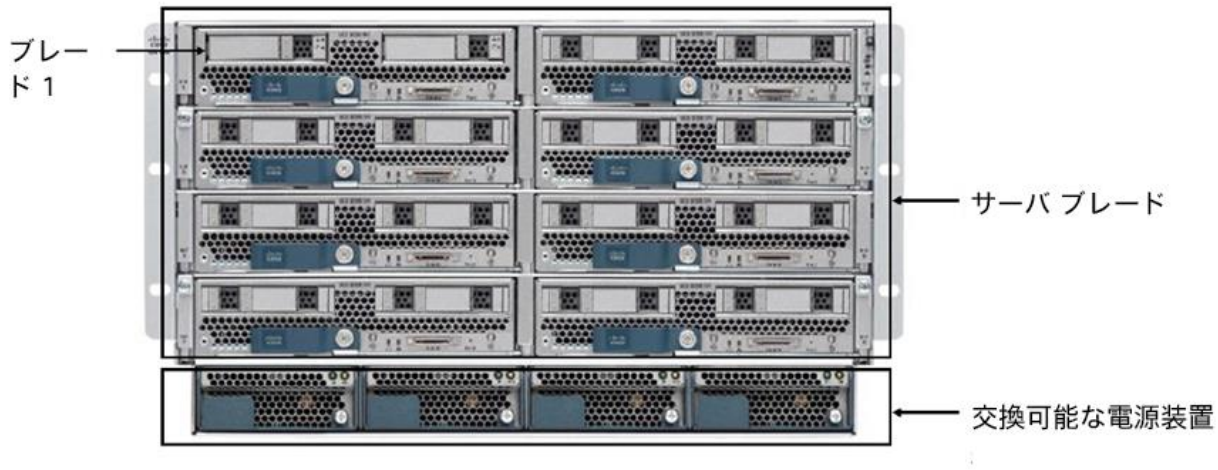
- Cisco UCS 5108 ブレード サーバ シャーシ。シャーシは 6 RU 高であり、ブレード装備時の重量はおよそ 115+ kg（254+ ポンド）です。
- Cisco UCS 6324 ファブリック インターコネクト モジュール 2 台（障害が発生した場合に冗長性を確保するため）。ファブリック インターコネクト モジュールはどちらも Cisco UCS Manager をホスト、実行しており、モジュールを設定できるようになっています。各ファブリック インターコネクト モジュールには、以下が備わっています。
    - 10 Gbps SFP+ ネットワーク ポート 4 つ。両ファブリック 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 に対応付けされています。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、制御することもできます。
    - 帯域外 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 コンソールへの帯域外アクセスも提供します（第 1.2.1 項を参照）。このポートの使用方法の詳細については、『Cisco UCS Manager GUI コンフィギュレーション 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（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 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ています。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。

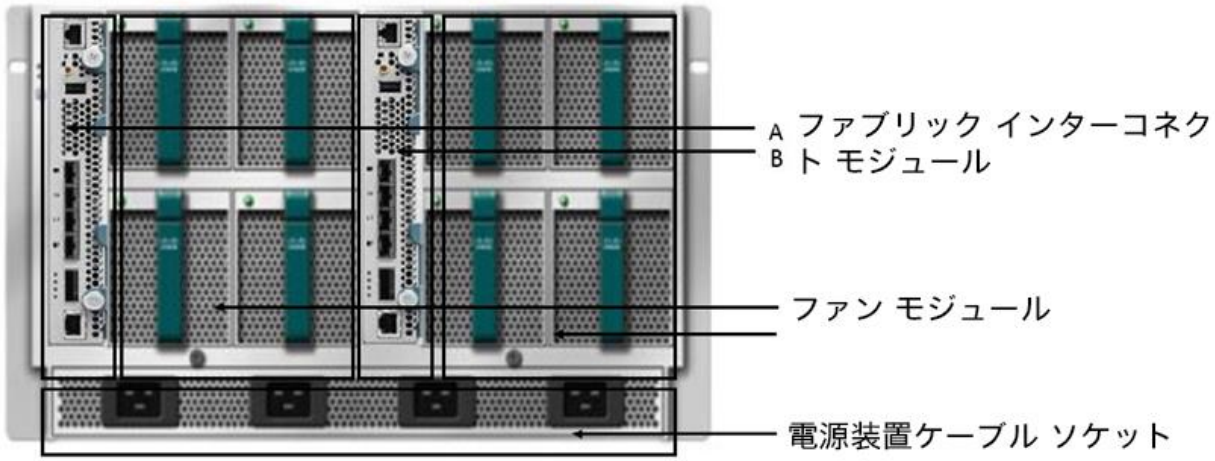
ブレード サーバと電源装置はユニットの前面から設置されています（図 1 を参照）。

図 1：8 台のサーバ 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 ソケットの上から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意：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 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。

1.2.1 インターフェイスおよび管理

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、XMPP サーバ、データベース）の設定に使用されます。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（第 3 項を参照）。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。

{b}注：{/b} 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 コンソールまたは帯域外の 100/1000 Mbps 管理ポートからアクセスします。

{color：#FF3722}{b}注意：{/b}{/color}プラットフォーム（UCS Manager 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。確認するには、『Cisco UCS 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。

{b}ヒント：{/b}Cisco Meeting Server 2000 を設定する際は、実行する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必要です。

1.3 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。

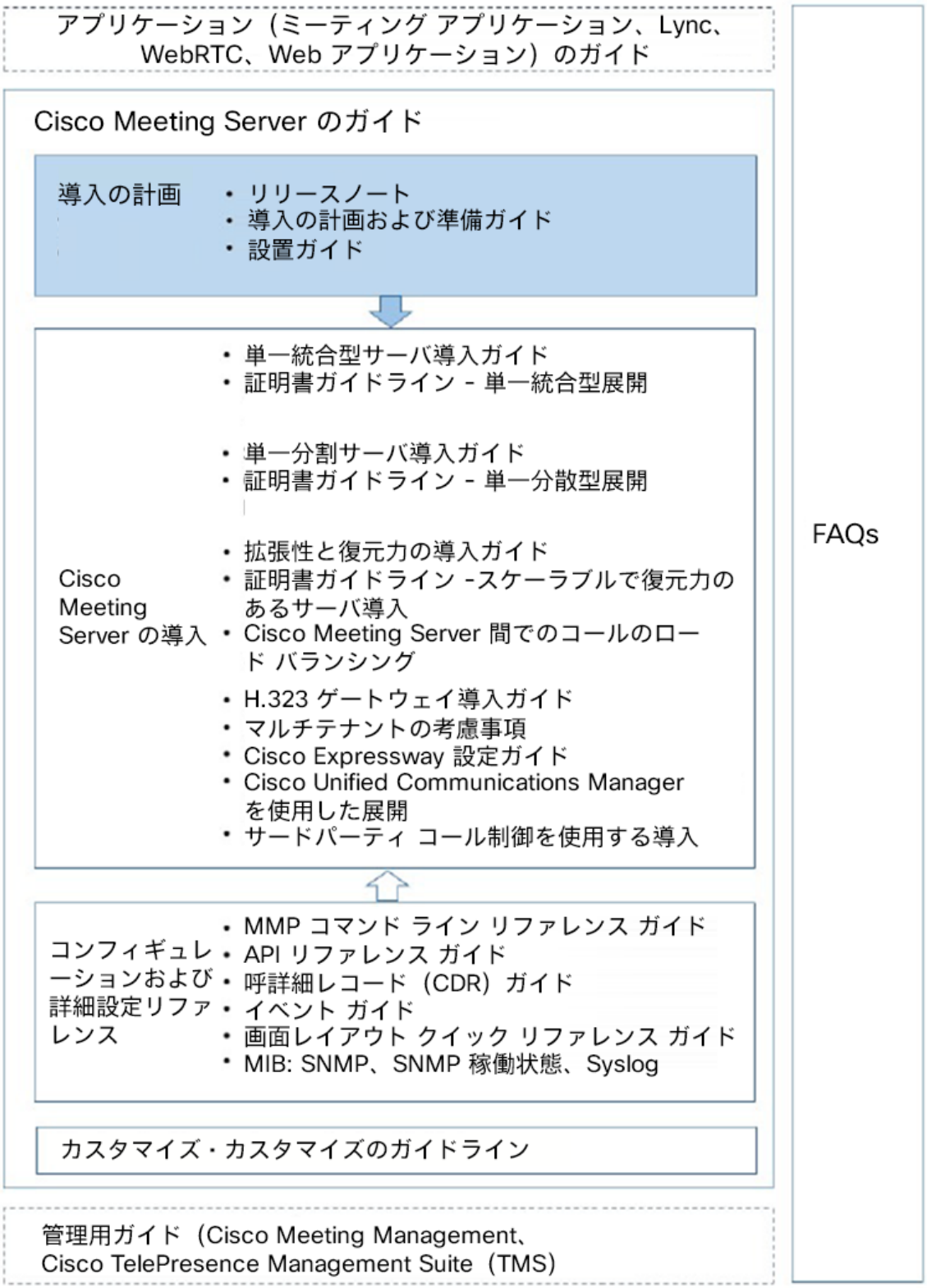
- Cisco Meeting Server 2000 の物理的な設置については、第 2 章を参照してください。
- ファブリック インターコネクト モジュールの設定については、第 3 章を参照してください。
- MMP へのアクセスをセットアップし、Call Bridge を設定する方法については、第 4 章を参照してください。
- 購入したライセンスとアクティベーション コードを Call Bridge にアップロードする方法については、第 5 章を参照してください。

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。

1.3.1 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導入用ドキュメント


アプリケーション（ミーティング アプリケーション、Lync、WebRTC、Web アプリケーション）のガイド
Cisco Meeting Server のガイド
導入の計画
• リリースノート
• 導入の計画および準備ガイド
• 設置ガイド
Cisco Meeting Server の導入
• 単一統合型サーバ導入ガイド
• 証明書ガイドライン - 単一統合型展開
• 単一分割サーバ導入ガイド
• 証明書ガイドライン - 単一分散型展開
• 拡張性と復元力の導入ガイド
• 証明書ガイドライン -スケーラブルで復元力のあるサーバ導入
• Cisco Meeting Server 間でのコールのロード バランシング
• H.323 ゲートウェイ導入ガイド
• マルチテナントの考慮事項
• Cisco Expressway 設定ガイド
• Cisco Unified Communications Manager を使用した展開
• サードパーティ コール制御を使用する導入
コンフィギュレーションおよび詳細設定リファレンス
• MMP コマンド ライン リファレンス ガイド
• API リファレンス ガイド
• 呼詳細レコード（CDR）ガイド
• イベント ガイド
• 画面レイアウト クイック リファレンス ガイド
• MIB: SNMP、SNMP 稼働状態、Syslog
カスタマイズ・カスタマイズのガイドライン
管理用ガイド（Cisco Meeting Management、Cisco TelePresence Management Suite（TMS）
FAQs

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。

{b}ヒント：{/b}各ブレードは、出荷時のスロット番号で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。

{color：#FF3722}{b}警告：{/b}{/color}シャーシを持ち上げ、ラック システムに取り付ける際は、大人 2 人以上で作業してください。シャーシが非常に重いため、大人 1 人で持ち上げると危険です。

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 サーバがスロット 1 に挿入されていることを確認します。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。挿入するスロットを変える場合は、50 ページの「*スロット間でブレードサーバをスワッピングする*」にある手順を実行する必要があります。

次の項目ついては、『Cisco UCS 5108 ブレード サーバのシャーシ取り付けガイド』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 U CS B200 M5 ブレードサーバ設置/サービス ノート』または『Cisco UCS B200 M4 ブレード サーバ設置/サービス ノート』の手順に従ってください。

2.3 Cisco Meeting サーバ 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、第 3.2 項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 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、第 3.4 項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、第 4.3 項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、トランクとして設定されていないこと**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。

{b 注：{/b} 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（第 3.10 項 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 サーバをスタンバイ モードにする必要があります（付録 F.1 を参照）。

2.6 次のステップ

Cisco Meeting Server 2000 の取り付け、設置が完了したら、サーバ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 モジュールの構成

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）を設定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 "C1sco123" 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。

{b}注：{/b}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 コンソールに渡す前に、SoL インターフェイスに固有のユーザ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、第 3.3.1 項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

SoL アクセス用の新しいユーザを作成する場合は、デフォルトの mmp アカウントを使用するのではなく、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名に置き換えてください。

{b}注：{/b} 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:
       ユーザ名        エンドポイント  ユーザ権限       パスワード     説明
       ----------    ------------------------  ----------   -----------
       fred          管理者                    ****
       mmp           管理者                    ****

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>** コマンドを使ってブロックの割り当てを解除します。
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。

{b}注：{/b}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お勧めしません。

---

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、サーバの場所または用途を反映するように変更することができます。

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 サーバを設定します。

{b}注：{/b}UCS Manager で使用される DNS サーバは、第 3.4 項で設定される、ブレード 1 の Cisco 統合管理コントローラー（CIMC）で使用されるプライマリ DNS サーバとセカンダリ DNS サーバ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設定

{b}注：{/b}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。

{b}注：{/b}電源をオンにすると、ブレード サーバは最後の電源の状態を記憶します。電源障害が発生した場合、この項のコマンドを再実行しなくてもブレード サーバ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#
```

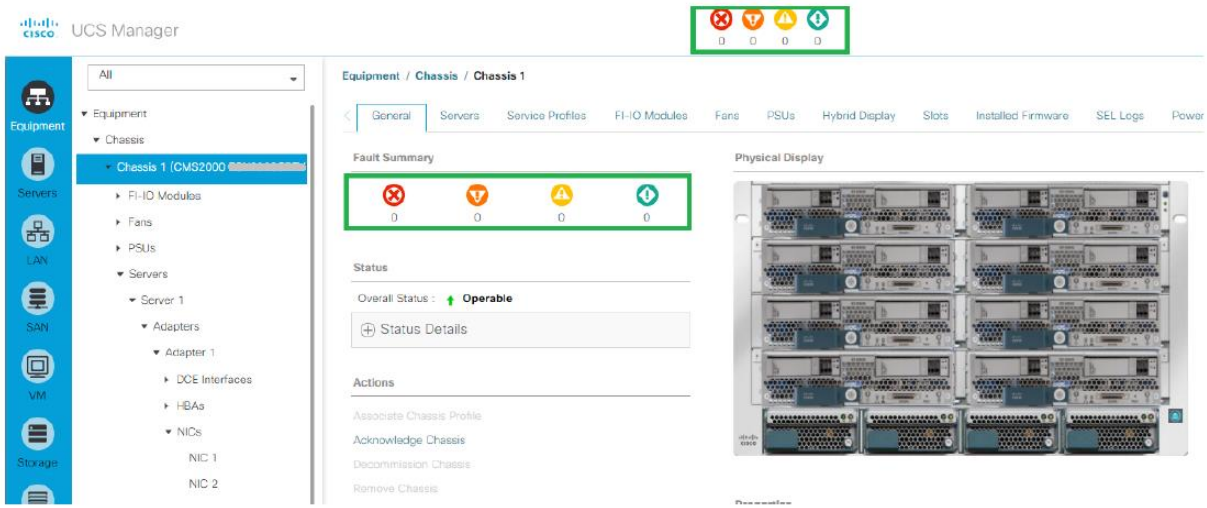
3.11 Cisco Meeting Server の状態の確認

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 サーバでクリティカル 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『Cisco UCS Manager 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、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。

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 管理ガイド』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 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導入形態によって異なります。Call Bridge 以外の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、第 3.4 項で設定した Serial Over LAN 接続用の IP アドレスに接続し、第 3.3 項で設定した資格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 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。初めてログインした場合、[admin] アカウントに新しいパスワードを設定するように求められます。

```
Welcome to the CMS 2000
acano login: admin
Please enter password: admin
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 Command Reference Guide』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。

{color：#FF3722}{b}注意：{/b}{/color} パスワードの有効期限は 6 か月です。

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。

{b}注：{/b}管理者レベルの MMP ユーザ アカウントは、Call Bridge の Web 管理画面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、第 3.9 項でファブリック 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 にアクセスできるようになります。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 a dhcp
```

{b}注：{/b}IPv6 を使用す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、特定のサブネット マスクおよびデフォルト ゲートウェイを指定して、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 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>
   ```

   {b}注：{/b}正引きゾーン（forwardzone）とは、ドメイン名とサーバ アドレスから構成されるペアのことです。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>
```

例を示します。

```
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、このリンクに移動します。Cisco Meeting Server 2000 は、VM デプロイメントまたは Acano X シリーズ サーバとは別のインストール ファイルです。

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。

{b}ヒント：{/b}ポート A の設定が完了しているため、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 管理画面インターフェイスの設定に含まれる秘密キー/証明書ペアの作成については第 4.5.1 項を、MMP への秘密キー/証明書ペアのアップロードとポート A をリッスンするインターフェイスの設定については第 4.5.2 項を参照してください。

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。

{b}注：{/b} Web 管理画面インターフェイスではなく API を介して Call Bridge を設定する場合も、Web 管理画面インターフェイスの証明書はアップロードしておく必要があります。

下記の情報は、シスコが秘密キー 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作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。

{b}注：{/b}Cisco Meeting Server をラボ環境でテストする場合は、サーバでキーと自己署名証明書を生成できます。自己署名証明書と秘密キーを作成するには、MMP にログインしてコマンド **`pki selfsigned <key/cert basename>`** を使用します。**`<key/cert basename>`** の箇所では、生成されるキーと証明書を識別するための文字列を指定します。たとえば「pki selfsigned webadmin」と指定した場合、webadmin.key と、自己署名された webadmin.crt 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>]`

   引数の説明

   `<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：Organizational Unit（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。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 サーバなど（付録 E を参照してください）。

{b}注：{/b}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

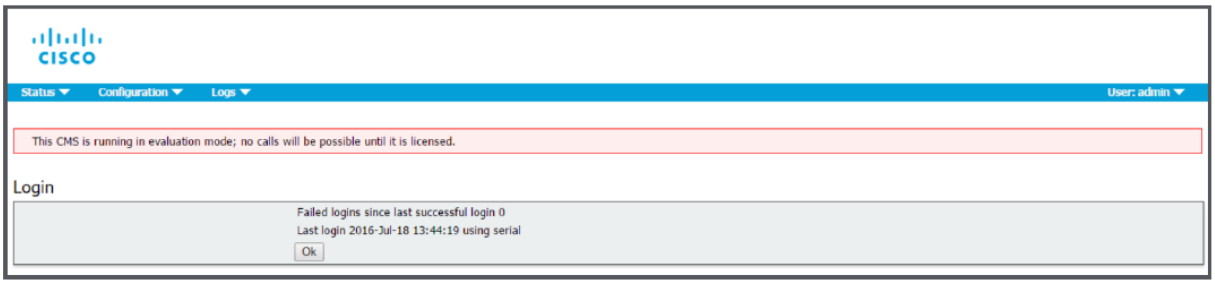
1. 第 3.4 項で設定した IP アドレスに SSH を介して接続し、SoL 接続を使用して MMP コマンドラインにアクセスします。第 3.3 項で設定した admin ユーザ名とパスワードを使用してログインします。
2. SFTP を使用して秘密キー/証明書ペアをアップロードします。オプションで証明書バンドルもアップロードします。
3. 次のコマンドを入力して、手順 2 でアップロードしたファイルを Web 管理者インターフェイスに割り当て、ポート A を使用するようにインターフェイスを設定します。

```
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、こちらで作成した MMP ユーザ アカウントを使用してログインします。

   次の図 5 に示すバナーは、cms.lic ライセンス ファイルがアップロードされるまで表示されます。

図 5：評価モードの Cisco Meeting Server



ライセンス ファイルをアップロードして割り当てると（第 5.2 項を参照）、バナーが削除されます。ただし、ライセンスを割り当てる前に、Call Bridge がリッスンし、Call Bridge 証明書をアップロードするポートを設定する必要があります。Call Bridge に必要な証明書のタイプは導入環境によって決まるため、これについては導入ガイドで説明しています。

Call Bridge を設定した後でライセンスファイルを取得し、適用する方法については、第 5 章を参照してください。

5　ライセンス ファイルの購入と適用

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、コール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。

次の機能を使用する場合は、サーバのライセンスおよびユーザ ライセンスのライセンスのほかに、ライセンス認証キーも購入する必要があります。

- 録画
- ストリーミング

アクティベーション キーおよび利用可能なユーザ ライセンスのタイプの詳細については、付録 B を参照してください。

{b}注：{/b}バージョン 2.4 以降では、1 つまたは複数のブランドを WebRTC のサインイン ページ、IVR メッセージ、SIP/Lync のコール メッセージまたはミーティング招待状のテキストに適用するためのライセンスは必要ありません。詳細については、付録 C を参照してください。

5.1　ライセンスの購入

シスコと契約のあるお客様：

1. シスコの e コマース ツールを使用してアクティベーション キーおよびライセンスを購入します。

   「PAK」コード、および Web サイトの URL が記載された電子メールを受信します。このサイトで、PAK コードと Cisco Meeting Server 2000 の MAC アドレスを登録する必要があります。

2. Meeting Server の PAK コードと MAC アドレスを登録します。
3. 単一のライセンス ファイルが電子メールで送信されます。

5.2　Cisco Meeting Server 2000 へのライセンス ファイルの転送

{b}注：{/b}ライセンス ファイルの名前を、転送前または転送中に cms.lic に変更します。

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. 第 3.4 項で設定したポート A の IP アドレスに SSH を介して接続し、第 3.3 項で設定した 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。

ライセンス ファイルが適用されると、Web 管理画面インターフェイスにサインインしたときに "Call Bridge requires activation" というバナーは表示されなくなります。

これで、導入に向けて Cisco Meeting Server を設定する準備が整いました。詳細については、第 6 項を参照してください。

6 Cisco Meeting Server の導入計画

{b}注：{/b}サーバを導入する前に cms.lic ライセンス ファイルをインストールする必要があります。第 5 章の手順に従います。

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。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 キャパシティの情報については、「Cisco Meeting Server 2000 コール キャパシティ」を参照してください。
- 分割展開。この場合、Cisco Meeting Server 2000 が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、ロードバランサー）が Edge サーバ（Cisco Meeting Server 1000、Cisco Meeting Server 仕様ベースの VM サーバ、Acano X シリーズ サーバ、Cisco Expressway）で有効になります。
- 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

重量：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）

動作湿度：5 ～ 93 %（結露しないこと）

A.3 電気仕様

最大電力： 3.36 kW @ 230V、14.74 A

3.38kW @ 115V、29.48A

電源ユニット 2500W プラチナ AC ホットプラグ電源装置 4 台

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 3：コール キャパシティ

コールのタイプ	Cisco Meeting Server 2000（注 1）	Cisco Meeting Server 1000	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5
フル HD 通話（1080p30）	350	48	48	48
HD 通話（720p30）	700	96	96	96

コールのタイプ	Cisco Meeting Server 2000（注 1）	Cisco Meeting Server 1000	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5
SD 通話（448p30）	1000	192	192	192
音声通話	3,000	3,000	1700	2200

{b}注：{/b}Cisco Meeting Server 2000 のソフトウェア バージョン 2.4 および 2.5 に比べて増加したソフトウェア バージョン 2.6 のコール キャパシティについての詳細は、第 1.1 項の表 1 と 2 を参照してください。

A.5 帯域幅要件

バージョン 2.4 以降の Cisco Meeting Server 2000 では、最大 700 の 720p HD 同時コールがサポートされています。これには、3 ～ 4 Gbps のネットワーク帯域幅が必要です。

付録 B シスコ ライセンス

Cisco Meeting Server ソフトウェアは、Cisco Meeting Server 2000 上で動作します。特定の機能やシスコのユーザ ライセンスを有効にするには、アクティベーション キーが必要です。シスコのアクティベーション キーおよびライセンスの購入と適用の詳細については、第 5.2 項を参照してください。

Cisco Meeting ServerB.1　アクティベーション キー

アクティベーション キーは、次の機能を使用するために必要です。

- Call Bridge
- 録画
- ストリーミング

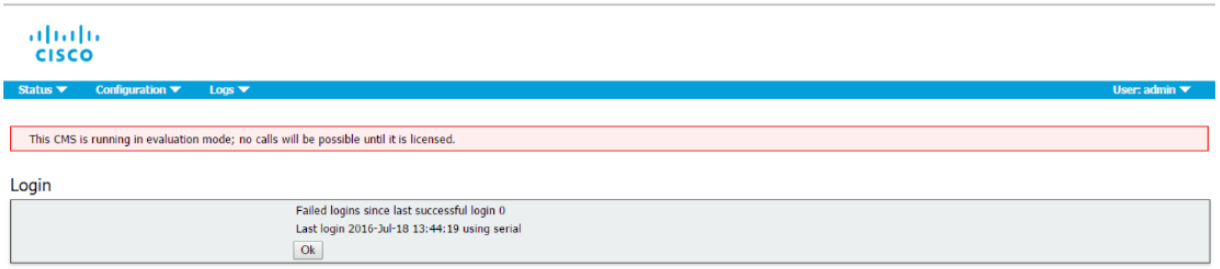
これらのキーは、cms.lic に含まれています。このライセンス ファイルの取得の詳細については、第 5.1 項を参照してください。

{b}注：{/b}バージョン 2.4 以降では、1 つまたは複数のブランドを WebRTC のサインイン ページ、IVR メッセージ、SIP/Lync のコール メッセージまたはミーティング招待状のテキストに適用するためのライセンスは必要ありません。詳細については、付録 C を参照してください。

B.1.1　Call Bridge のアクティベーション

コールを作成するには、Call Bridge がアクティブ化されている必要があります。Call Bridge をアクティブ化するには、cms.lic ファイルを Meeting Server にアップロードしてから、MMP コマンド **`callbridge restart`** を使って Call Bridge を再起動します。

有効な cms.lic ファイルがアップロードされるまで、Web 管理画面インターフェイスにはバナー「この CMS は評価モードで実行されています。ライセンスが付与されるまでコールは不可能です（This CMS is running in evaluation mode; no calls will be possible until it is licensed）」が表示されます。ライセンス ファイルをアップロードすると、バナーが削除されます。



B.1.2 録画

録画は、ライセンス キーによって制御されます。このライセンス キーでは、1 つのライセンスで 1 つの同時録画ができます。ライセンスは、レコーダーをホストしているレコーダではなく、Call Bridge（コア サーバ）をホストし、レコーダに接続するサーバに適用されます。

{b}注：{/b}レコーダーの実稼働での使用には、少なくとも 4 個の物理コアと 4 GB を搭載した専用 VM で実行する導入環境が推奨されます。このような導入環境では、レコーダーは物理コア当たり 2 つの同時録画サポートするため、最大で 8 つの同時録画をサポートします。

録画ライセンス キーを購入するには、次の情報が必要です。

- 同時録画の数
- ポート A に割り当てられている MAC アドレスについては、第 3 項を参照してください。

B.1.3 ストリーミング

ストリーミングには、ストリーマをホストするサーバではなく、Call Bridge をホストする Meeting Server にロードされる 1 つ以上のライセンスが必要です。1 つのレコーディング ライセンスは 1 つの同時ストリーミングまたは 1 つの録画をサポートし、既存のレコーディング ライセンスでは、ストリーミングが可能です。バージョン 2.1 以降では、1 つの録画/ストリーミング ライセンスまたは追加ポートを含むスターター キットを使用できます。

{b}注：{/b}ストリーマの実稼働での使用に推奨される導入環境は、6 個の同時ストリームにつき 1 個の vCPU および 1GB のメモリを持ち、最低で 4 個の vCPU および最大で 32 個の vCPU を備えている専用 VM で実行することです。

B.2 シスコのユーザ ライセンス

コール マルチパーティ ライセンスは、Cisco Meeting Server に使用される主なライセンスモデルです。Acano Capacity Unit（ACU）を購入することはできますが、マルチパーティ ライセンスと同一の Call Bridge で使用することはできません。ACU をマルチパーティ ライセンスに移行する必要がある場合は、シスコのセールス担当者にお問い合わせください。

マルチパーティ ライセンスには、ネームド ホスト ライセンスを提供する Personal Multiparty Plus（PMP Plus）ライセンスと、共有ホスト ライセンスを提供する Shared Multiparty Plus（SMP Plus）ライセンスの 2 種類があります。Personal Multiparty Plus ライセンスと Shared Multiparty Plus ライセンスは、同じサーバで使用できます。

Personal Multiparty Plus B.2.1 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。このライセンスは、Cisco UWL Meeting（PMP Plus を含む）を通じて購入できます。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。（導入されている 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。

{b}注：{/b}アドホック会議の開催者は特定することができ、開催者に PMP+ 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に使用されます。

Shared Multiparty Plus B.2.2 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。SMP は、ルーム エンドポイントの購入時に UCM TP Room Registration ライセンスと共に割引価格で購入するか、あるいは個別に購入することができます。Shared Multiparty Plus は、Cisco UWL Meeting 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。Cisco UWL Meeting ライセンスの有無にかかわらず、すべての従業員が同じ機能を活用できます。たとえば、各自のスペースで会議を主催したり、アドホック会議を立ち上げたり、会議の予定を作成したりすることができます。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。各 Shared Multiparty Plus ライセンスに

は、Cisco Expressway 向けリッチ メディア セッション（RMS）ライセンスが 1 つ含まれています。このライセンスを使用して、Business-to-Business（B2B）ビデオ会議を実行できます。

Cisco Meeting Server B.2.3　キャパシティ ユニット

Acano キャパシティ ユニット（ACU）は Cisco Meeting Server キャパシティ ユニットに名称変更されました。各容量単位（CU）は、12 個のオーディオ ポートまたはミーティング サーバ ソフトウェアに対する次の数の同時メディア ストリームをサポートします（CU ソフトウェア ライセンスの利用条件については、こちらを参照してください）。

表 4：容量単位ライセンス

メディアストリーム	キャパシティ ユニットあたりのライセンス数	コール レッグごとに必要なライセンス数
1080p30	0.5	2
720p30	1	1
480p30	2	0.5

各 CU により、少なくとも 1 人のビデオ参加者がいる会議ごとに、コンテンツを共有できる権限もライセンス取得者に付与されます。詳細については、CU ライセンスの利用条件を参照してください。

B.3　シスコ ユーザ ライセンスの適用方法

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。ライセンスの割り当て先となるミーティング サーバは、次の規則によって決定されます。

- シスコ PMP Plus ライセンスを持つ 1 人以上のメンバーがスペースに参加している場合は、いずれかのライセンスが使用されます。
- そのスペースの作成者（所有者）が Cisco PMP Plus ライセンスを持っている場合、ライセンスの所有者が割り当てられます。それ以外の場合で、
- シスコ SMP Plus ライセンスがある場合は、そのライセンスが割り当てられます。

B.4 シスコ ユーザ ライセンスの設定

次のオブジェクトとフィールドが API に追加され、管理でマルチパーティ ライセンスの使用を決定できるようになりました。

- 新規/システム/ライセンス オブジェクト。これは、ミーティング サーバのコンポーネントがライセンスを持ち、有効化されるかどうかを管理者が決定できるようにします。
- 新しい /system/multipartyLicensing オブジェクト（使用可能なライセンスと使用中のライセンスの数を返す）
- 新しい /system/multipartyLicensing/activePersonalLicenses オブジェクト（Personal Multiparty Plus ユーザ ライセンスを使用しているアクティブ コールの数を示す）、
- LDAP 同期の一環としての新規 userProfile フィールド
- userProfile の新しい hasLicense フィールド（ユーザがライセンスを持っているかどうかを示す）
- /coSpace オブジェクトごとの新規 ownerId および ownerJid フィールド。存在する場合、ownerId フィールドは、この coSpace を所有するユーザの GUID を保持します。また、ownerJid は、ユーザの JID を保持します。

{b}注：{/b}所有者は、/coSpace オブジェクトを POST または PUT するときに ownerJid フィールドを使用して設定されます。/coSpace を GET すると、ユーザの ownerJid と ownerId の両方が返されます。

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。

- 背景イメージの WebRTC アプリ記号、サインインロゴ、サインインロゴの下のテキスト、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
- ミーティング招待状のテキスト

バージョン 2.4 からは、これらのカスタマイズ可能な機能に 1 つまたは複数のブランドを適用するためのライセンスは必要ありません。1 つのリソースセット（WebRTC 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。

付録 D Cisco Meeting Server 2000 と仮想化導入の間での 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 の実行と、Cisco Meeting Server または Acano X シリーズ サーバの実行には、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	Acano X シリーズサーバ上
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 上での電源切断を行います。	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。	プロンプトが表示されたら、"Y" を入力します。これで、サーバの電源を安全に切断できるようになりました。
ヘルス	MMP では利用できません。Cisco UCS Manager を使用します。	使用不可	サーバが健全かどうかを返します。
serial	サーバのシリアル番号を返します。	使用不可	サーバのシリアル番号を返します。
dns	インターフェイスは指定しないでください。 例を挙げましょう。 **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。例を挙げましょう。 **dns add forwardzone <domain-name> <server ip>**	インターフェイスとして mmp または app を指定する必要があります。例を挙げましょう。 **dns mmp add forwardzone <domain-name> <server ip>**
user evict	使用不可	使用可能	使用可能

D.2 異なるプラットフォームで有効化されている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	Acano X シリーズサーバ上
Call Bridge	提供されています。	提供されています。	提供されています。
Web Bridge	提供されています。	提供されています。	提供されています。
XMPP Server	提供されています。	提供されています。	提供されています。
データベース	提供されています。	提供されています。	提供されています。
TURN サーバ	非対応	提供されています。	提供されています。
ロード バランサ	非対応	提供されています。	提供されています。
レコーダー	非対応	提供されています。	提供されています。
ストリーマ	非対応	提供されています。	提供されています。
H.323 ゲートウェイ	非対応	提供されています。	提供されています。
SNMP MIB	現在のところ、利用可能ではありません。	提供されています。	提供されています。

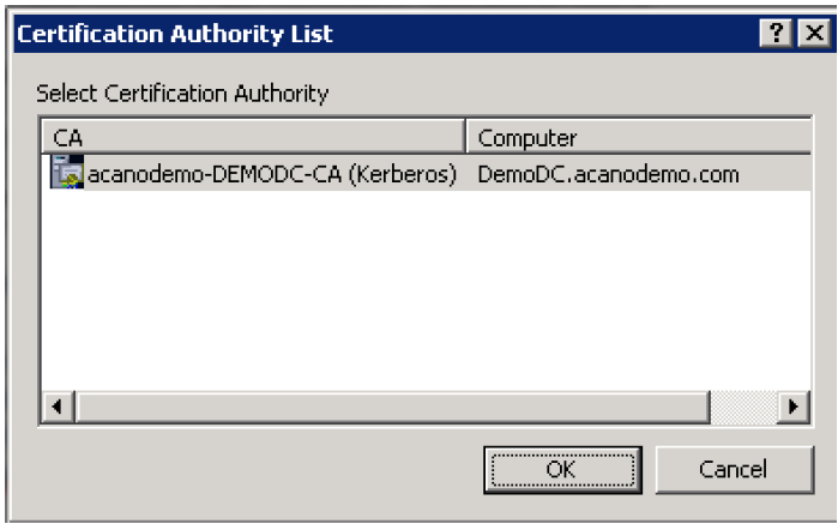
付録 E ローカル認証局によって署名された証明書の作成

この付録では、Active Directory Certificate Services のロールを持つ Microsoft Active Directory サーバなどの 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
   ```

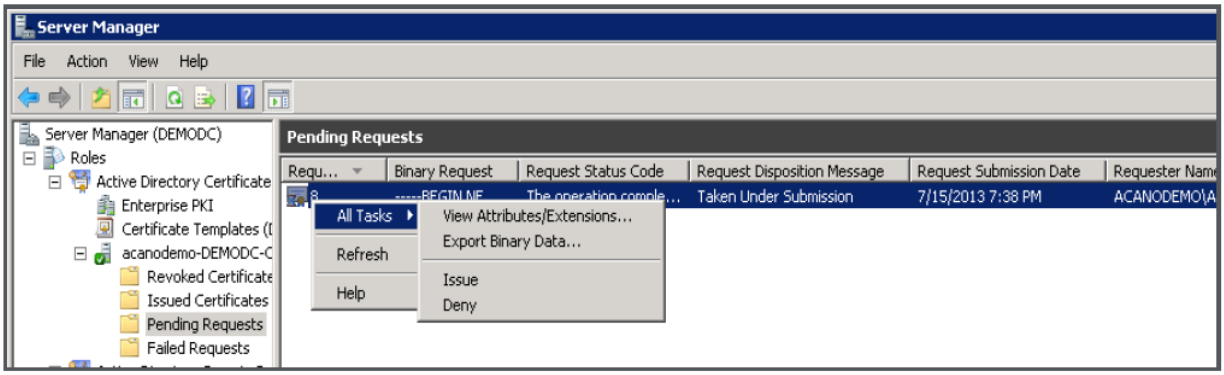
3. このコマンドを入力すると、次のような CA 選択リストが表示されます。正しい CA を選択して、[OK] をクリックします。



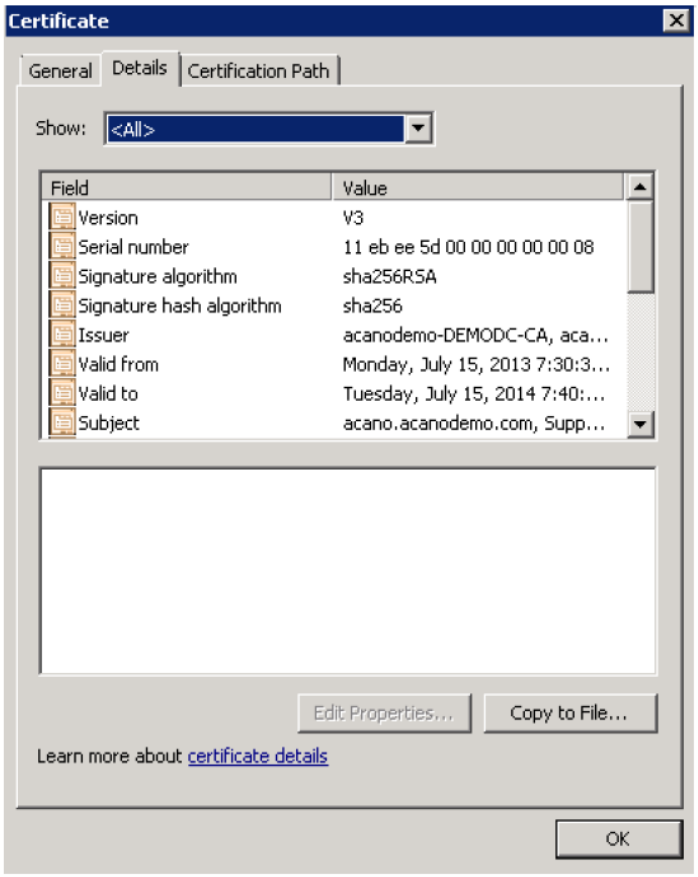
4. 次のいずれかを実行します。
   - 証明書発行許可を持つ Windows アカウントを使用している場合は、生成された証明書を（webadmin.crt などの名前で）保存するよう求めるプロンプトが表示されます。下記の手順 c に進みます。
   - 生成された証明書を発行するためのプロンプトが表示されない場合、代わりに次のようにコマンド プロンプト ウィンドウに「証明書の要求は保留中です：提出済みです（Certificate request is pending: taken under submission）」というメッセージが表示さ

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。

5. CA の [サーバ 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。



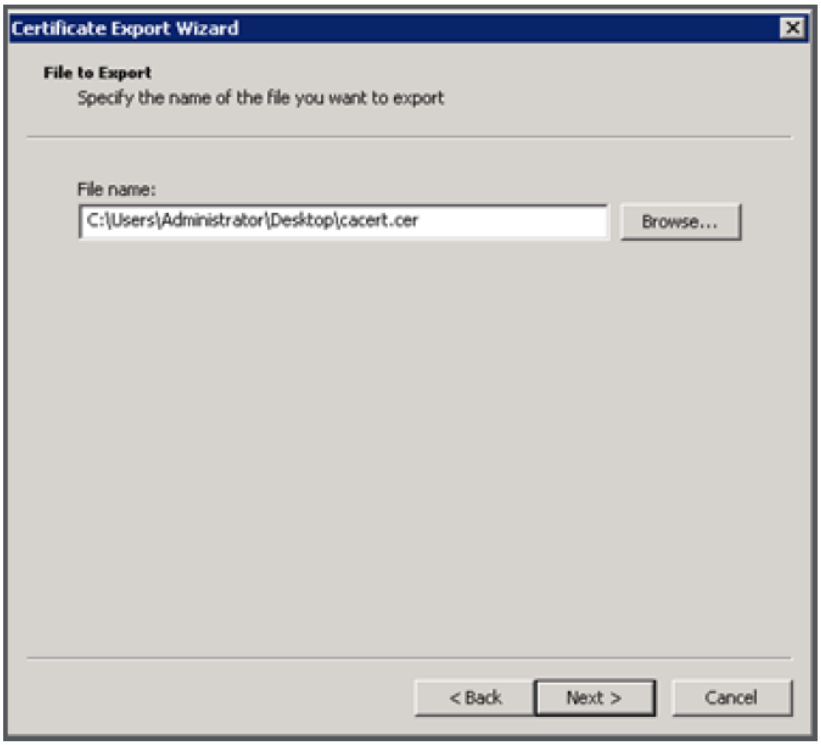
7. 発行された署名付き証明書が [発行した証明書（Issued Certificates）] フォルダに保存されます。証明書をダブルクリックして開き、**[詳細（Details）]** タブを開きます（右図を参照）。



8. [**ファイルにコピー（Copy to File）**] をクリックします。これにより、[証明書のエクスポートウィザード（Certificate Export Wizard）] が開始されます。

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。詳細については第 4.5 項を参照してください。

{color: #FF3722}{b}注意：{/b}{/color} 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 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。

F.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#
```

F.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。

{b}注：{/b}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
```

サーバ	スロットステータス	利用状態	全体のステータス	ディスカバリ
1/1	搭載	応対不可	Ok	高い
1/2	搭載	応対不可	Ok	高い
1/3	搭載	応対不可	Ok	高い
1/4	不一致	応対不可	コンピューティングの不一致	再試行
1/5	不一致	応対不可	コンピューティングの不一致	再試行
1/6	搭載	応対不可	Ok	高い
1/7	搭載	応対不可	Ok	高い
1/8	搭載	応対不可	Ok	高い

```
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
```

サーバ	スロットステータス	利用状態	全体のステータス	ディスカバリ
1/1	搭載	応対不可	Ok	高い
1/2	搭載	応対不可	Ok	高い
1/3	搭載	応対不可	Ok	高い
1/4	搭載	応対不可	Ok	高い
1/5	搭載	応対不可	Ok	高い
1/6	搭載	応対不可	Ok	高い
1/7	搭載	応対不可	Ok	高い

サーバ	スロットステータス	利用状態	全体のステータス	ディスカバリ
1/8	搭載	応対不可	Ok	高い

F.3 Serial over LAN の無効化（任意）

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。

{color: #FF3722}{b}注意：{/b}{/color}MMP の初期設定には 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 ポリシー:

   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#
```

F.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 ポリシー:

   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。

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（http://www.cisco.com/web/JP/about/office/index.html）をご覧ください。

Cisco の商標または登録商標