Cisco Meeting Server

Cisco Meeting Server リリース 3.12

Cisco Meeting Server 2000 インストールガイド

2025 年 12 月 12 日

Cisco Systems, Inc. www.cisco.com

コンテンツ

変更内容

バージョン日付	変更内容（Change）
2025 年 10 月 31 日	バージョン 3.12 で更新。

1 はじめに

Cisco Meeting Server 2000 は、音声、ビデオ、ウェブコンテンツ向けの高性能でスケーラブルなプラットフォームです。Microsoft、Avaya、その他のベンダーのさまざまなサードパーティ製品と相互運用できます。Cisco Meeting Server 2000 を使用すると、場所、デバイス、またはテクノロジに関係なく、人々がつながります。

Cisco Meeting Server 2000 は Cisco UCS 技術に基づいており、仮想化された展開としてではなく、物理的な展開として Cisco Meeting Server ソフトウェアを実行しています。これにより、パフォーマンスが向上し、UCS プラットフォームの高性能機能が利用されます。

Cisco Meeting Server 2000 は、大量のコールを処理するため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 およびウェブブリッジのコンポーネントのみを設定で利用できます。Cisco Meeting Server 2000 は、複数の Meeting Server が展開されている場合のエッジサーバーとしては適していません。TURN サーバーエッジコンポーネントが利用できないためです。
Cisco Meeting Server ウェブアプリユーザーにファイアウォール トラバーサル サポートが必要な導入では、TURN サーバーを別の Cisco Meeting Server 1000 または仕様ベースの VM サーバーに導入する必要があります。

さらに、レコーダーとストリーマーコンポーネントは Cisco Meeting Server 2000 では利用できません。小容量の Cisco Meeting Server 1000 と仕様ベースの VM サーバーにより適しているためです。

Cisco Meeting Server 2000 は、内部ネットワーク上の単一サーバーとして、単一の分割サーバー導入におけるコアサーバーとして、またはスケーラブルな導入における複数のコアノードの 1 つとして導入することができます。Cisco Meeting Server 1000 番台、および仕様ベースの VM サーバーを含む導入の一部にすることができます。ただし、すべてが同じソフトウェアバージョンを実行している必要があります。参加者の機能性およびユーザー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しているすべてのプラットフォームで同一です。

注：

- 仮想化された導入からバックアップを作成し、特定の環境でロールバックすることはできません。
  Cisco Meeting Server 2000 またはその逆。
- Meeting Server はセキュアブートをサポートしていません。

メモ：2019 年 8 月頃から、新しい Cisco Meeting Server 2000 では Fabric Interconnect のフェイルオーバーがデフォルトで有効になります。ただし、デバイスを手動で設定してフェイ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）が必須となりました。Meeting Management は、Smart Licensing サポートのための製品の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）との対話を処理します。

1.1 Cisco Meeting Server 2000 概要

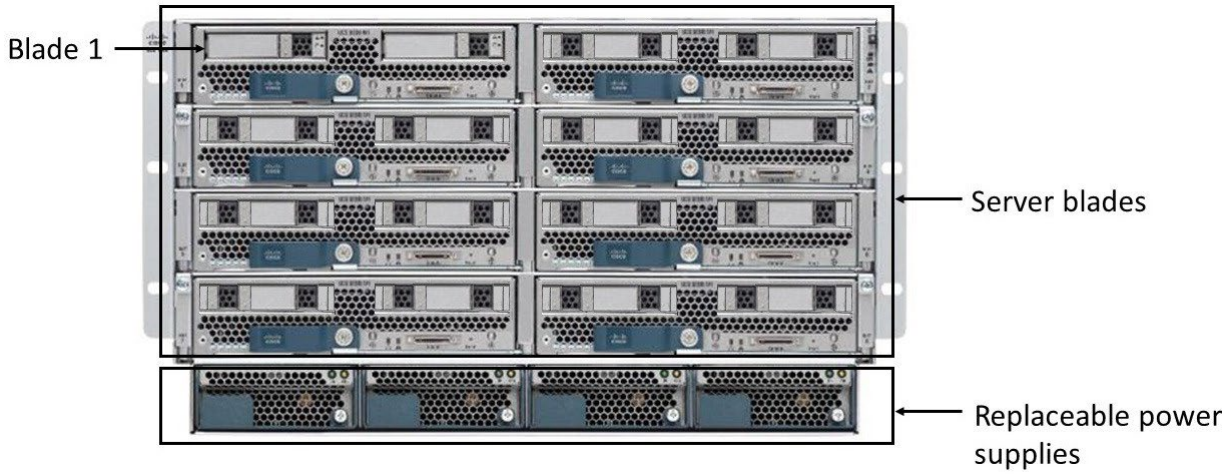
Cisco Meeting Server 2000 は、Cisco UCS テクノロジーに基づいており、以下のもので構成されています。

- a Cisco UCS 5108 ブレードサーバシャシー。ブレードを取り付けた場合の高さは 6 RU、重さは約 115+kg（254+ ポンド）になります。
- 2 個の Cisco UCS 6324 ファブリックインターコネクトモジュールにより、1 個が故障した場合の冗長性を提供します。両方の Fabric Interconnect モジュールは、モジュールの構成を有効にする Cisco UCS マネージャーをホストし、実行します。各 Fabric Interconnect モジュールには次の機能があります。
    - 4 x 10 Gbps SFP+ ネットワークポート。両方の Fabric Interconnect のポート 1 は、「アップリンクポート」として構成され、Cisco Meeting Server 用に ポート A にマッピングされます。両方の Fabric Interconnect がフェイルオーバーをサポートするように設定されています。1 つの Fabric Interconnect で障害が発生すると、Cisco Meeting Server 2000 はもう一方を使用するようにフェイルオーバーします。いずれかの Fabric Interconnect でイーサネットポート 1 に障害が発生した場合、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 Fabric Interconnect 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 および 3 は使用されません。
    - 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 を通じて Fabric Interconnect モジュールを設定します。また、Cisco UCS マネージャー コマンド ライン インターフェース（CLI）コマンドでシャシーを設定、コントロールするためにも使用できます。

    - アウトオブバンド 100/1000 Mbps 管理ポート MGMT とラベル付けされており、UCS Manager コマンドラインおよびグラフィックインターフェイスを使用して、シャシーを設定および制御することができます。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。1.1.1 の項を参照してください。 このポートの使用に関する詳細は、『Cisco UCS Manager GUI 設定ガイド』を参照してください。
    - USB ポートは現在使用されていません。
- 8 台の Cisco UCS B200 ブレードサーバー（M5 または M4）。スロット 1 に取り付けられたブレードサーバーには、RAID 1 ミラーとして設定された 2 つのハードドライブがあります。ブレードサーバー 1 は、Cisco Meeting Server アプリケーションのコントロールブレードまたは MMP として機能します。これは、MMP コマンドラインインターフェースで設定します。他の 7 台のブレードサーバーにはハードドライブがなく、メディアの処理に使用されます。設定は必要ありません。
- ホットスワップ可能な 4 つの電源。
- ホットスワップ可能な 8 つのファンモジュールにより、シャシー全体を冷却します。

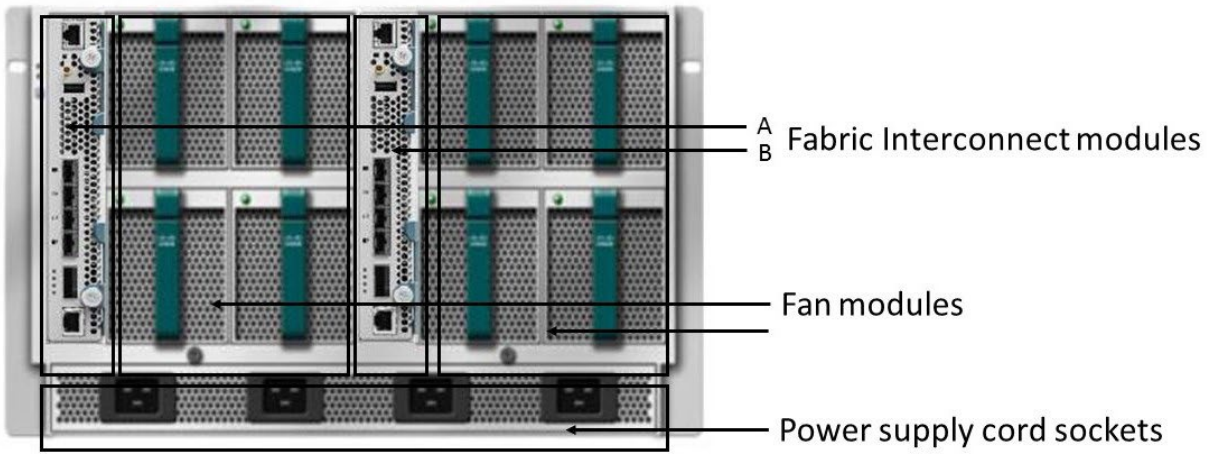
ブレードサーバーと電源はユニットの前面にインストールします。図 1 を参照してください。

図 1：8 個のサーバーモジュールと 4 個の交換可能な電源を示すユニットの前面



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、ユニット背面の 電源コードソケットの上から取り付けます。参照 図 2

図 2：ユニットの背面にはファブリック インターコネクト モジュール、8 個のファンモジュール、4 個の電源コードソケットが示されています



冗長性機能に関するメモ：Cisco Meeting Server 2000 は、Cisco UCS-B プラットフォームが提供するすべての冗長性機能をサポートしています。これには、ファン、電源、Fabric Interconnect フェイルオーバー、サーバーブレード障害、およびネットワークフェールオーバーします。

- Fabric Interconnect のフェイルオーバー - 各 Fabric Interconnect のイーサネット ポート 1 はフェイルオーバーをサポートするように構成されます。Fabric Interconnect の 1 つで障害が発生した場合、Cisco Meeting Server 2000 はもう一方を使用してフェイルオーバーします。いずれかの Fabric Interconnect でイーサネットポート 1 に障害が発生した場合、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 に移動します。
- メディア処理に使用される 7 つのメディアブレード（2 から 8 の番号）これらのブレードのいずれかがオフラインになっているか、削除されている場合、Cisco Meeting Server 2000 は引き続き実行されますが、処理能力は低下します。スロット 1 のブレードサーバーは、そのブレードがオフラインまたは故障の場合、Cisco Meeting Server の MMP およびアプリケーションが機能しないため、重要です。
- ホットスワップ可能な 4 つの電源。サーバーは 3 つの電源装置で安全に動作できますが、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勧めします。
- ホットスワップ可能な 8 つのファンモジュールにより、シャシー全体を冷却します。ファンコントローラーは温度センサーを使用して、ファンに障害が発生した場合、またはファンモジュールが取り外された場合に、残りのファンをより速く回転させるかどうかを決定します。

1.1.1 インターフェイスと管理

Cisco Meeting Server 2000 には 3 つの層があります。Cisco Meeting Server プラットフォームとアプリケーション層、そして Cisco Meeting Server ソフトウェアの下の物理ハードウェアプラットフォームです。

- Cisco Meeting Server のプラットフォームレイヤーは、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通じて構成します。MMP は、低レベルブートストラッピング、および Cisco Meeting Server コンポーネント（Call Bridge、ウェブブリッジ、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 がサーバーの MMP として機能します。MMP へのアクセスを提供するため、Serial over LAN SoL 接続が提供されます。SoL を使用するということは、シャシーに物理的にアクセスする必要がないということです。MMP にアクセスする前に、Fabric Interconnect 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 項を参照してください。Fabric Interconnect モジュールの設定が済んだら、SSH を使って MMP にログインできるようになります。
- Cisco Meeting Server のアプリケーション層は、この管理プラットフォーム上で動作し、独自の設定インターフェイスを使用します。アプリケーションレベルの管理（通話とメディアの管理）は、Cisco Meeting Server のウェブ管理インターフェイスや REST API を通じて行われます。API はウェブ管理インターフェイスを通じ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、それに IP アドレス（「A」ネットワークインターフェイスのラベル）を割り当てます。この MMP ネットワーク インターフェースは、アプリケーションレイヤーとその管理インターフェース（ウェブ管理および REST API）へのアクセスに使用されます。Cisco Meeting Server 2000 では、この「A」ネットワークインターフェイスは、Fabric Interconnect モジュールのポート 1 で設定された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。

メモ：Cisco Meeting Server 2000 プラットフォームは複数のインターフェイスをサポートしていません（例えば、'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 で管理される UCS シャシーです。UCS Manager は、シャシーにインストールされた、自己完結型の Fabric Interconnect モジュールのクラスター化ペアで実行されます。ハードウェア、またはそれが提供する仮想要素を設定するとき、管理は UCS Manager のコマンドライン インターフェイスまたはウェブインターフェイスを通じて行われます。UCS Manager インターフェイスには、シリアルコンソールまたは Fabric Interconnect モジュールの帯域外 100/1000 Mbps 管理ポート経由でアクセスします。

  注意：プラットフォーム (UCS マネージャにより管理される UCS シャシーおよびモジュール) が最新のパッチで最新のものであることを確認します。『Cisco UCS Manager Firmware Management Guide』の指示に従います。プラットフォームのメンテナンスを怠ると、Cisco Meeting Server のセキュリティが損なわれる可能性があります。

ヒント：Cisco Meeting Server 2000 の設定を行う際には、希望する設定作業に対してどのレイヤー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 このガイドの使い方

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るマニュアルセットの一部です。 図 3 を参照してください。

このガイドの内容：

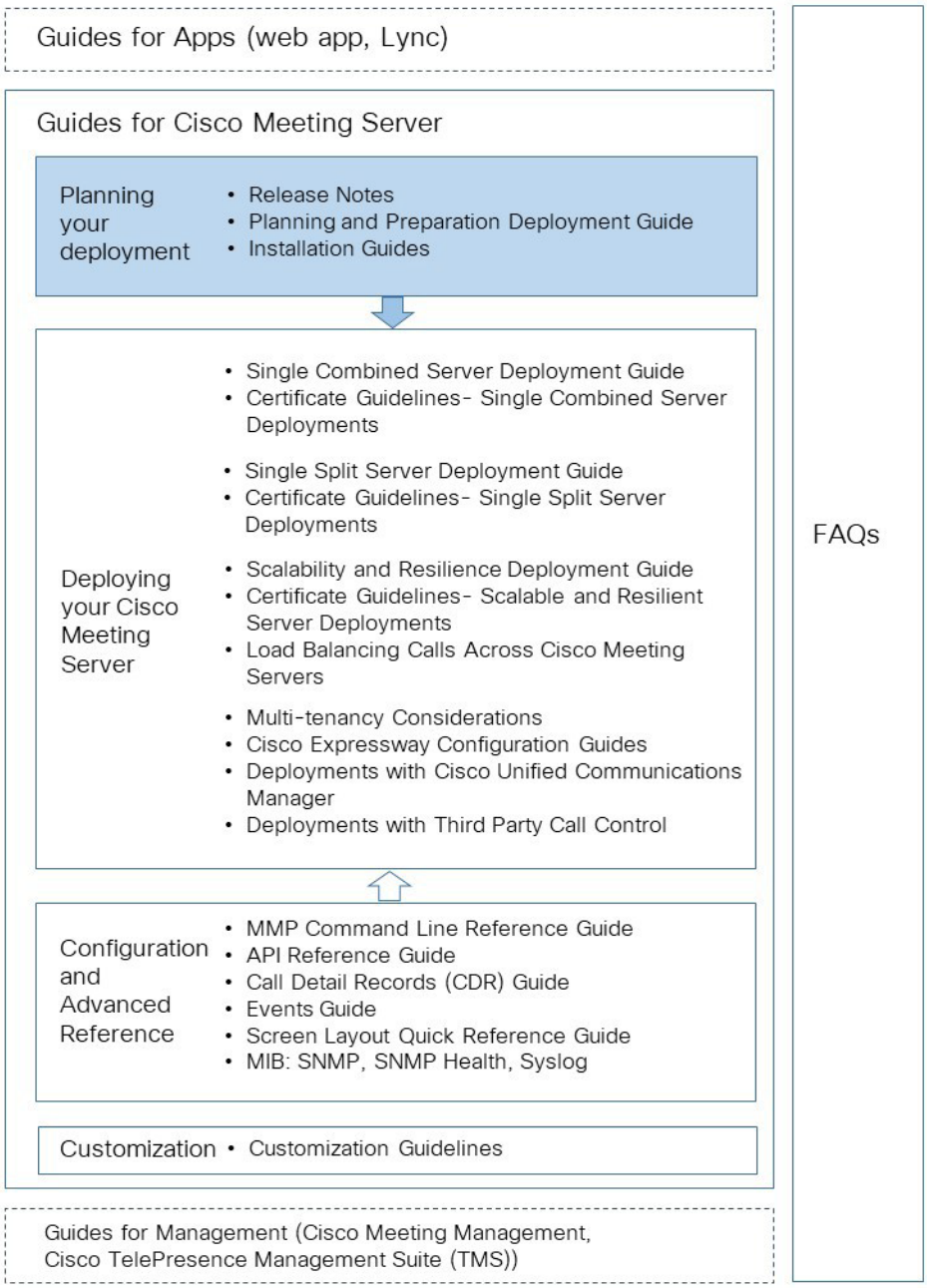
- Cisco Meeting Server 2000 の物理的なインストールについては、第 2 章を参照してください。
- ファブリック インターコネクト モジュールの設定については、 第 3 章を参照してください。
- MMP へのアクセスのセットアップと Call Bridge の設定については、第 4 章を参照してください。
- 購入したライセンスとアクティベーション コードを Call Bridge にアップロードする方法については、第 1 章を参照してください。

特定の導入に合わせて Cisco Meeting Server を設定する必要があります。ガイダンスについては、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、コマンドは黒で表示され、指定どおりに入力する必要があります。括弧内に適切な値を入力します。**青** で例を参照できます。これらは実際の導入に合わせて変更する必要があります。

図 3：Cisco Meeting Server のインストールと導入のドキュメント



2 サーバーをインストールする

2.1 概要

この章の内容：

- 19 インチラックシステムに Cisco Meeting Server 2000 を取り付ける。
- ケーブルと電源を接続する。

2.2 ラックシステムにシャシーを設置する

Cisco Meeting Server 2000 は、8 台のブレードサーバーすべてがインストールされた状態で出荷され、重さは約 115+kg（254+ ポンド）あります。ブレードサーバーをスロットから慎重に取り外し 、**各サーバーがどのスロットで**出荷されたかを記録しておきます。その後、ブレードを安全な場所に保管してください。業界標準の 19 インチラックシステムに取り付けることができます。シャシーには 6 RU のスペースが必要です。

ヒント：ブレードごとに、出荷時のスロット番号のラベルを付けてください。これにより、ラックにシャシーを設置した後に、どのスロットに再度取り付けるかを確認することができます。どのブレードをどのスロットに入れるかを記録していないと、追加の時間と追加の構成が発生し、取り付け作業を完了します。

警告： 少なくとも 2 名の大人で持ち上げて、ラックシステムに取り付けてください。シャシーは、成人 1 人では安全に持ち上げるには重すぎます。

シャシーが取り付けられたら、各ブレードを慎重にシャシーに再挿入し、2 つのハードディスクを持つ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。他のブレードを出荷時と同じスロットに挿入することをお勧めします。有効になっていない場合は、「スロット間でブレードサーバーを交換する」75 ページの手順を行う必要があります。

『Cisco UCS 5108 ブレードサーバーシャシー設置ガイド』 の指示に従ってください:

- シャシーの外部で必要な周囲温度範囲、
- シャシーを移動する方法、

- シャシーにレールを取り付ける、
- ラックにシャシーを設置する、
- 電源を接続します。詳細について

は、以下を参照してください。

- ブレードサーバーをシャシーから削除し、
- ブレードサーバーをインストールする、
- ブレードサーバーのフロントパネルにある LED の意味
- [リセット（Reset）] ボタンを使用して、
- ブレードサーバーの技術仕様。

必要に応じて、『Cisco UCS B200 M5 ブレード サーバのインストールおよびサービス ノート』または『Cisco UCS B200 M4 ブレード サーバのインストールおよびサービス 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 個。
- 各 Fabric Interconnect 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 個。
- IP アドレス 5 つ：
  - 3 つの静的 IP アドレス（各 Fabric Interconnect の管理（MGMT）ポートごとに 1 つ）、および共有アドレス。これらの IP アドレスは管理 VLAN 上にある必要があります。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 上の MMP シリアルコンソールにアクセスするための 1 つの静的 IP アドレス。SoL アクセスは Fabric Interconnect モジュールの MGMT ポート経由であるため、この IP アドレスは管理 VLAN 上にある必要があります。セクション 3.4 を参照してください。

- 両方の Fabric Interconnect モジュール上のポート 1（ポート A）を通じて Cisco Meeting Server アプリケーションにアクセスするための 1 つの静的 IP アドレス。この IP アドレスは、管理 VLAN とは異なる VLAN 上にある必要があります。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

Fabric Interconnect A で、以下を接続します。

- 管理ポートを管理ネットワーク上の 100/1000Mbps スイッチポートに、
- 適切な 10Gbps SFP+ 送受信モジュールをポート 1 にインストールし、そのポートをネットワーク上の 10Gbps スイッチポートに接続します。**これはスイッチポートでなければならず、トランクとして設定しないでください。**
- シリアルコンソールポートをコンソール端末に接続して、Fabric Interconnect モジュールを設定します。
- ポート 2 および 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 に対して、接続を繰り返します。

メモ：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+ 送受信機をインストールしたり、ポート 4 をネットワークに接続したりしないでください。ポート 4 は内部使用のみです。

2.5 電源オン/オフ

ユニット後部の電源ソケットに電源コードを接続します。シャシーに電力が供給されると、Fabric Interconnect モジュールが起動します。ブレードサーバーは電源が入るまでスタンバイモードです（黄色の LED が点灯）。セクション 3.10 を参照してください。電源がオンになると、ブレードサーバーの LED が緑に点灯します。

シャシーの電源を切る前に、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を参照してください。

2.6 次のステップ

Cisco Meeting Server 2000 を物理的に設置した後で、サーバーがネットワークに接続するように、Fabric Interconnect モジュールを設定する必要があります。第 3 章を参照してください。

3 Fabric Interconnect モジュールを設定する

この章では、サーバーがネットワークに接続するための、Fabric Interconnect モジュールの初期設定について詳しく説明します。

この章の内容：

- 両方の Fabric Interconnect モジュールに割り当てられたデフォルトの admin パスワードを変更する。
- SSH 経由で Fabric Interconnects を管理するために、新しい IP 静的アドレスを指定する。これには、クラスターとして Fabric Interconnect モジュールを管理するための共有アドレスの定義が含まれます。
- デフォルトの管理者パスワードを変更して、Serial over LAN SoL を使用して Cisco ミーティングサーバの MMP レイヤーにアクセスする。SoL を使用して、シャシーの Fabric Interconnect モジュールの 1 つのシリアルポートに接続します。これにより、Cisco Meeting Server の MMP にアクセスできるようになります。
- SoL 経由で MMP にアクセスするために、新しい静的 IP アドレスを指定する。
- システム名を変更する。
- Meeting Server に DNS を設定する。
- Meeting Server のタイムゾーンを設定する。
- Meeting Server に NTP を設定する。
- ポート 1 のアップリンク速度を設定する。
- ブレードサーバーの電源をオンにする
- UCS Manager を使用してブレードの動作を確認する。
- ファブリック インターコネクト モジュールの証明書をインストールしています。

初期セットアップ中に、以下の情報を指定する必要があります。

- Fabric Interconnect モジュールの管理者アカウントのパスワード。Cisco UCS Manager パスワードのガイドラインに準拠した、安全性の高いパスワードを選択します。

- 各 Fabric Interconnect モジュール用の新しい 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、および共有 IP アドレス。すべての IP アドレスが管理ネットワーク VLAN 上にある必要があります。
- 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 admin パスワード。
- 新しい IPv4（または IPv6）アドレスを使用して SoL 接続経由で MMP コマンド ラインにアクセスする必要があります。
- システム名。
- 管理 VLAN 上の DNS サーバーの IPv4 アドレス（または IPv6 アドレス）。
- Fabric Interconnect モジュールが使用するタイムゾーン。
- MMP ネットワークポートの MAC アドレス

この章の作業を完了すると、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。第 4 章を参照してください。

3.1 Fabric Interconnect モジュールのデフォルトの管理者パスワードを変更する

初期設定を行うには、シリアル端末を各 Fabric Interconnect モジュールのコンソールポートに接続する必要があります。

1. シリアル端末を Fabric Interconnect 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. 「C1sc0123」の UCS Manager のデフォルトパスワードを使用して、「admin」としてログインします。
4. 以下の例のコマンドを使用して、admin アカウントのパスワードを変更します。

メモ：Fabric インターコネクトモジュールがクラスタリングされるため、これらの手順を Fabric Interconnect B に対して繰り返す必要はありません。

次に例を示します。

Cisco UCS Mini 6324 シリーズ ファブリック インター

コネクト UCS-A ログイン: **管理者**

パスワード：**C1sc0123**

Cisco Nexus オペレーティングシステム（NX-OS）ソフトウェア

TAC サポート：http://www.cisco.com/tac Copyright (c) 2009、Cisco Systems, Inc.すべての権利を保有します。

このソフトウェアに含まれる特定の著作物の著作権は他の第三者に所有されており、ライセンスに基づき使用および配布されます。このソフトウェアの特定のコンポーネントは、GNU General Public License（GPL）バージョン 2.0 または GNU 劣等一般公衆利用許諾書（LGPL）バージョン 2.1 に基づいてライセンスされています。

各ライセンスのコピーは、http://www.opensource.org/licenses/gpl-2.0.php および http://www.opensource.org/licenses/lgpl-2.1.php で入手できます。

```
UCS-A# スコープ セキュリティ
UCS-A /security # set password
新しいパスワードの入力：新しい
パスワードの再確認：
UCS-A /security* # commit-buffer
UCS-A /security # exit
UCS-A#
```

3.2 Fabric Interconnect モジュールに新しい IP アドレスを割り当てる

新しい静的 IP アドレスを各 Fabric Interconnect モジュールに割り当て、両方のモジュールで共有される別のアドレスを割り当てます。共有 IP アドレスは、クラスター化された Fabric Interconnect モジュールで実行されている UCS Manager にアクセスするために使用されます。

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

アドレスの設定は、Fabric Interconnect モジュールの 1 つを通して行うことができます。

たとえば、IPv4 を使用する場合：

```
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 を使用する場合：

```
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の管理者パスワードを変更する

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コンソールに移動する前に、

SoLインターフェース固有のユーザー名とパスワードの入力を求められます。工場出荷時にデフォルトのアカウントとパスワードが設定されています。セキュリティのため、お客様はこのデフォルトパスワードを変更する必要があります。デフォルトの mmp を使用したくない場合は、新しい管理者アカウントを作成することもできます。セクション 3.3.1 を参照してください。

1. Fabric Interconnect モジュールの 1 つのコマンドライン インターフェイスにログインしている間に、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。

次に例を示します。

```
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を作成する

デフォルトの mmp アカウントを使用するのではなく、新しいユーザーを SOL アクセス用に作成する場合は、次の手順に従って、名前 fred を適切なユーザー名に置換します。

メモ： show ipmi-user の行とレスポンスはオプションです。

```
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:
    ユーザー名前    End point user privilege    [パスワード（Password）]    説明
    ------------    ------------------------    ------------------------    -------
    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 ユーザアカウントを削除する

SoL アクセスのための新しいユーザーアカウントを作成した後、既定の 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 アドレスを指定する

Serial Over LAN 接続にアクセスするための IP アドレスを指定するには、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、それから DNS サーバーをプライマリ使用とセカンダリ使用に指定します。

手順は以下のとおりです。

1. Serial Over LAN 接続に割り当てられた IP アドレスのブロックの既存の設定を確認してください。単一の IP アドレスのブロックが割り当てられており、その値が導入に適している場合は、次のセクションに進みます。**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を解除します。
2. 単一の IP アドレスの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。これは、単一の IP アドレスを含む必要があり、Fabric Interconnect 管理 IP アドレスと同じ管理サブネットにある必要があります。

   メモ：Cisco では、Cisco Meeting Server 2000 MMP SoL 接続に別の VLAN またはサブネットを使用することを推奨していません。

   ---

3. プライマリとセカンダリの DNS IP アドレスを指定します。

たとえば、IPv4 を使用する場合：

```
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 システム名を変更する

システム名は、サーバーの場所や用途に合わせて変更できます。

次に例を示します。

```
UCS-A# scope system
UCS-A /system # set name CMS2000-London
警告：システム名の変更は FC ゾーン名を変更し、再導入します

UCS-A /system* # commit-buffer
UCS-A /system # exit
CMS2000-London#
```

3.6 UCS Manager に DNS を設定する

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。

メモ：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 で Cisco Integrated Management Controller（CIMC）に使用されます。

```
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 タイムゾーンを設定する

Cisco Meeting Server 2000 のタイムゾーンを設定する必要があります。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # set timezone
```

タイムゾーンのルールを正しく設定するために、ロケーションを特定してください。大陸または大洋を選択してください。

1) アフリカ	4) 北極海	7) オーストラリア	10) 太平洋
2) アメリカ地域	5) アジア	8) 欧州	
3) 南極	6) 大西洋	9) インド洋	

国を選択してください

1) アンギラ 19) ドミニカ共和国 37) ペルー

2) アンティグアバーブーダ 20) エクアドル 38) プエルトリコ

3) アルゼンチン 21) エルサルバドル 39) セント・バルテルミー

4) Aruba 22) フランス領ギアナ 40) St Kitts &ネイビス

5) バハマ 23) グリーンランド 41) セントルシア

6) バルバドス 24) グレナダ 42) セント・マーティン（オランダ語）

7) 25) グアドループ) 43) サン・マルタン （フランス語）

8) ボリビア 26) グアテマラ 44) サンピエール島・ミクロン島

9) ブラジル 27) ガイアナ 45) セントビンセント

10) カナダ 28) ハイチ 46) スリナム

11) カリブ諸島 NL 29) ホンジュラス 47) トリニダード&トバゴ

12) ケイマン諸島 30) ジャマイカ 48) タークス & カイコス諸島

13) チリ 31) マルティニーク 49) アメリカ合衆国

14) コロンビア 32) メキシコ 50) ウルグアイ

15) コスタリカ 33) モントセラト 51) ベネズエラ

16) キューバ 34) ニカラグア 52) ヴァージン諸島（英国）

17) キュラソー 35) パナマ 53) バージン諸島（米国）

18) 36) ドミニカ 36) パラグアイ

#?**49**

次のいずれかのタイムゾーン地域を選択してください。

1) 東部（ほとんどの地域）16) 中部 - ND（モートン郊外）

2) 東部 - MI（ほとんどの地域）17) 中部 - ND（マーサー）

3) 東部 - KY（ルイスビル地域）18) 山岳部（ほとんどの地域）

4) 東部- KY（ウェイン）19) 山岳 - ID（南部）、OR（東部）

5) 東部 - IN（ほとんどの地域）20) MST - アリゾナ（ナバホを除く）

6) 東部- IN（Da, Du, K, Man）21) 太平洋

7) 東部 - IN（プラスキ）22) アラスカ（ほとんどの地域）

8) 東部 - IN（クロフォード）23) アラスカ - ジュノーエリア

9) 東部- IN（パイク）24) アラスカ - シトカ地域

10) 東部 - IN（スイス）25) アラスカ - アネット島

11) 中央（ほとんどのエリア）26) アラスカ - ヤクタット

12) 中部- IN（ペリー）27) アラスカ（西部）

13) 中部 - IN（スターク）28) アリューシャン列島

14) 中部 - MI（ウィスコンシン州との境界）29) ハワイ州

15) 中央部 - ND（オリバー）

#?**21**

次の情報が指定されています。

米国太平洋

そのため、タイムゾーンは「アメリカ/ロサンゼルス」に設定されます。現

地時刻は、現在 2011 年 4 月 23 日（土）23 05:08:43 PDT です。

世界標準時刻は、現在 2011 年 4 月 23 日（土）23 12:08:43

UTC です。上記でよろしいですか

1) はい

2) なし

#?**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、Fabric インターコネクトモジュールが使用する NTP サーバーを設定する必要があります。

```
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を設定する

メモ：各 Fabric Interconnect モジュールのアップリンクポートに 10Gbps 接続を使用します。

両方の Fabric Interconnect モジュールで、アップリンクポートの速度を設定する必要があります。

```
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 ブレードサーバーの電源をオンにする

8 台のブレードサーバーはそれぞれ、いずれかの Fabric Interconnect モジュール経由で電源をオンにする必要があります。

メモ：電源をオンにした後、ブレードサーバーは前回の電源状態を記憶しています。停電が発生した場合、ブレードサーバーの電源がオンになります。このセクションのコマンドを再度実行する必要はありません。

次に例を示します。

```
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#
```

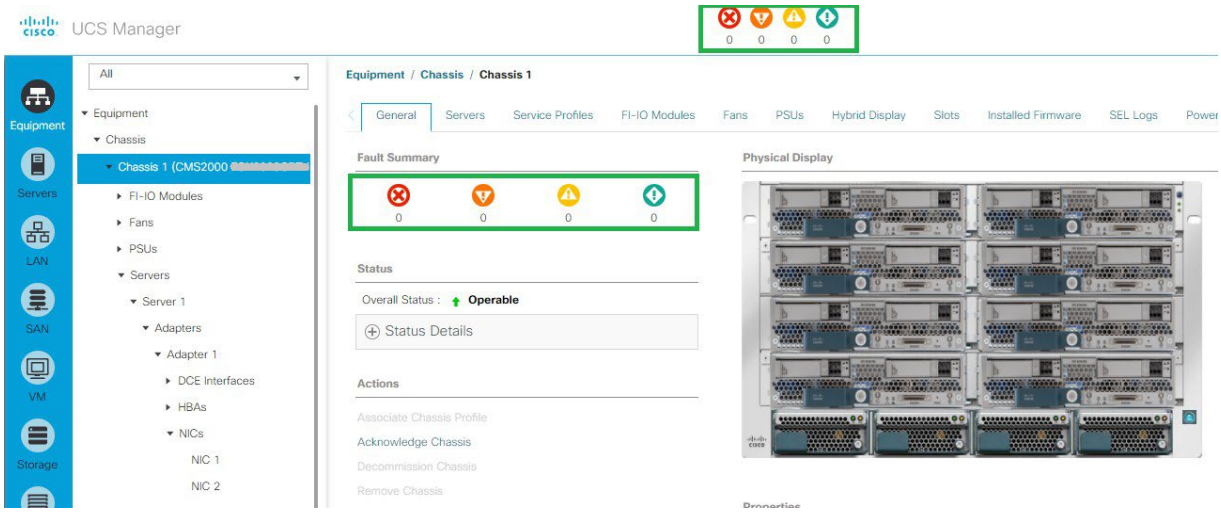
3.11 Cisco Meeting Server の状態を確認する

Cisco UCS Manager GUI を使用すると、Cisco Meeting Server 2000 シャシー内の Fabric Interconnect モジュールとブレードサーバーの状態を監視することができます。詳細については、『Cisco UCS Manager システム監視ガイド』を参照してください。

[障害の概要（Fault Summary）] ページ （図 4 を参照）を使用して、ブレードサーバーが稼働していることを確認します。障害の各タイプは異なるアイコンで表示されます。各アイコンの下の数字は、システムで発生したそのタイプの障害の数を示します。アイコンをクリックすると、マネージャ GUI は [作業（Work）] 領域に [障害（Faults）] タブを開き、そのタイプのすべての障害の詳細を表示します。

いずれかのブレードサーバーでクリティカルアラーム（赤いアイコン）が表示されている場合は、Cisco サポート に問い合わせる前に『Cisco UCS 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 のうちの 1 つ以上がオフラインかまたは削除された場合、Cisco Meeting Server 2000 は稼働し続けますが、容量は減ります。スロット 1 のブレードサーバーは、そのブレードがオフラインまたは故障の場合、Cisco Meeting Server の MMP およびアプリケーションが機能しないため、重要です。

図 4: UCS Manager の障害概要ページ



3.12 証明書を Fabric Interconnect モジュールに適用する

Cisco Meeting Server 2000は、Fabric Interconnectモジュールに自己署名証明書が適用された状態で出荷されます。これらの証明書を独自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』の指示に従ってください。

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オンにすると、MMP を通じて Cisco Meeting Server のコンポーネントを設定する準備ができています。第 4 章 では、MMP による Call Bridge の初期設定について説明します。

4 MMP 経由で Cisco Meeting Server 2000 を設定する

この章では、MMP を通じた Call Bridge の初期設定について詳しく説明します。MMP を通じて他のコンポーネントも設定する必要がありますが、どのコンポーネントは展開によって異なります。これらの設定については、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 MMP CLI にログインする

Cisco Meeting Server の初期設定を完了するには、セクション 3.3 および 3.2 で設定した Serial Over LAN 接続を使用して MMP コマンドラインインタフェースにアクセスします。3.4.SSH クライアントを使用して、シリアルオーバー LAN 接続のために、 セクション 3.4 で設定した IP アドレスに接続し、 セクション 3.3 で設定した証明書を使用してログインします。

次に例を示します。

```
ssh <username>@<ip address>
ssh mmp@10.1.1.2
mmp@10.1.1.2's password:
CISCO Serial Over LAN：
```

ネットワーク接続を閉じて終了します

ログインに成功すると、Serial Over LAN 接続により MMP 仮想コンソールに移動します。（メモ：Serial Over LAN 接続を切断するには、サーバーへの SSH セッションを閉じる必要があります。）ユーザ名「admin」でログインし、Enter キーを押してパスワードフィールドをスキップします。「admin」アカウントの新しいパスワードを設定するよう促すプロンプトがすぐに表示されます。

```
CMS 2000 へようこそ CMS ロ
```

グイン：**管理者**

パスワードを入力してください：
管理者によるパスワードのリセットが強制されました パス

ワードの有効期限が切れました
新しいパスワードを入力してください：
新しいパスワードを再度入力してください：

4.2 独自の Cisco ミーティングサーバー管理者アカウントを作成する

ユーザー名「admin」は安全性が低いため、セキュリティ上の理由から、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。さらに、1 つのアカウントのパスワードをなくした場合に備えて、2 つの管理者アカウントを持っておくことをお勧めします。そうした場合でも、もう一方のアカウントでログインして、なくし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 コマンドリファレンスガイド』を参照してください。パスワードを 2 回入力するように指示されます。新しいアカウントでログインすると、パスワードの変更が求められます。

注意：パスワードの有効期限は 6 か月です。

新しい管理者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。

メモ：管理者レベルの MMP ユーザーアカウントは、Call Bridge のウェブ管理インターフェイスにログインするためにも使用できます。ウェブ管理インターフェイスを通じてユーザー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ースをセットアップする

セクション 3.9 で Fabric Interconnect モジュールを通じて設定した、ポート A のネットワークインターフェイス速度を設定する必要はありません。

ただし、次の操作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 アドレスを設定し、
- DNS 構成を設定します。

ポート A のネットワーク インターフェイスと IP アドレスが設定されると、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 がアクセス不能になった場合にのみ使用する必要があります。SFTP はポート A 経由でのみアクセスでき、

4.3.1 DHCP を使用してポート A の IP アドレスを設定する

ポート A で dhcp を有効にするには、次を入力します。

```
ipv4 a dhcp
```

メモ：IPv6 を使用している場合は、同様のコマンドセットを使用できます。完全な説明については、『MMP コマンドリファレンス』を参照してください。

---

dhcp で構成された設定を確認するには、次を入力します。

```
ipv4 a
```

4.3.2 ポート A に IP 静的アドレスを設定する

<ipv4|ipv6> a add コマンドを使用して、指定されたサブネットマスクとデフォルトゲートウェイを持つポート A に静的な IP アドレスを追加します。

たとえば、プレフィックス長 16（ネットマスク 255.255.0.0）の ipv4 アドレス 10.1.1.6（ネットマスク 255.255.0.0）をゲートウェイ 10.1.1.1 でポート 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
```

IPv4 アドレスを削除するには、次のように入力します。

```
ipv4 a del 10.1.1.6
```

4.3.3 DNS 構成を設定する

1. DNS 構成を出力するには、次を入力します。

   ```
   dns
   ```

2. DNS 構成を設定するには、次を入力します。

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

   メモ：フォワードゾーンは、ドメイン名とサーバアドレスのペアです。名前が DNS 階層で指定のドメイン名より下にある場合、DNS リゾルバーは指定のサーバーにクエリできます。任意の特定のドメイン名に対して複数のサーバーを指定して、ロードバランシングとフェイルオーバーを提供できます。"." を指定するのが一般的です。ドメイン名として、すなわち、すべてのドメイン名にマッチする DNS 階層のルート、すなわち、サーバーが IP 10.1.1.3 上にある場合

   ```
   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、次を使用します。

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

たとえば、

```
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を確認する

Cisco Meeting Server 2000 は、Cisco Meeting Server ソフトウェアがプリインストールされた状態で出荷されます。Call Bridge のウェブ管理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ことを確認することをおすすめします。

- MMP コマンド **version** を使用して、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します。
- このリンク に移動して最新のソフトウェアを確認します。Cisco Meeting Server 2000 は VM 展開とは別の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、ソフトウェアバージョンに対して公開されている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、必ず設定をバックアップしてください。

ヒント：これでポート A が設定されました。SFTP を使用して、ポート A 経由で Cisco Meeting Server ソフトウェアのバックアップとアップグレードを行います。

4.5 ウェブ管理インタフェースを設定する

ウェブ管理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 はこのウェブインターフェイスを通してルーティングされます。

ウェブ管理インターフェイスの設定には、秘密鍵/証明書ペアの作成（セクション 4.5.1 を参照）、MMP への秘密鍵/証明書のペアのアップロード、リッスンするためのインターフェイスの設定が含まれます。ポート A 経由で接続するには、セクション 4.5.2 を参照してください。

ウェブ管理インターフェイスが有効になると、API またはウェブ管理のいずれかを使用して、Call Bridge を設定できます。

4.5.1 ウェブ管理インターフェイス用の証明書を作成する

ウェブ管理インタフェースは HTTPS 経由でのみアクセス可能です。セキュリティ証明書を作成し、それをCisco Meeting Server にインストールする必要があります。

メモ：ウェブ管理インターフェイスではなく、API を通じて Call Bridge を設定する場合でも、ウェブ管理インターフェイス用に証明書をアップロードする必要があります。

以下の情報は、Cisco が秘密鍵の生成の要件を満たしていることを信頼していることを前提としています。必要に応じて、公開 Certificate Authority（CA）を使用して秘密鍵と証明書を外部で生成し、外部で生成されたキー/証明書のペアを SFTP を使用して Cisco Meeting Server の MMP にロードすることもできます。署名付き証明書を取得したら、セクション 4.5.2 に移動します。

メモ：Cisco Meeting Server をラボ環境でテストする場合、サーバー上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鍵を作成するには、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、生成されるキーと証明書を指定します。例：「pkiself signed webadmin」は、webadmin.key と webadmin.crt（自己署名）を作成します。プロダクション環境での自己署名証明書の使用は推奨されていません（http://en.wikipedia.org/wiki/Self-signed_certificate を参照）

以下の手順では、MMP コマンド pki csr を使用して秘密鍵と関連する証明書署名リクエストを生成し、CA 署名用にエクスポートする方法について説明します。

1. MMP にログインし、秘密鍵と証明書の署名リクエストを生成します（CSR）。

   `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（例えば、「webadmin」と入力すると「webadmin.key」と「webadmin.csr」ファイルになります）

   許可されているがオプションの属性は次のとおりで、コロンで区切る必要があります。

- CN：証明書に記載される CommonName です。DNS A レコードで定義された FQDN を共通名として使用します。これを行わないと、ブラウザの証明書エラーが発生します。
- OU：部門名
- O：組織
- L：所在地
- ST：都道府県
- C：国
- emailAddress

1 単語以上の長さの値には引用符を使用します。例：

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

2. 次のいずれかの場所に CSR を送信します。
   - Verisign などの Certificate Authority（CA）要求者の身元を確認し、署名付き証明書を発行する Verisign。
   - Active Directory 証明書サービスの役割がインストールされた Active Directory サーバーなど、ローカルまたは組織の Certificate Authority への接続については、 付録 E を参照してください。

メモ：署名済み証明書と秘密鍵をミーティングサーバーに転送する前に、証明書ファイルを確認してください。CA が証明書のチェーンを発行している場合、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、BEGIN CERTIFICATE および END CERTIFICATE の行を含む特定の証明書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。.crt、.cer または .pem の拡張子を持つ証明書としてファイルを保存します。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と認識できるように明確な名前を付け、同じ拡張子（.crt、.cer または .pem）を使用します。中間証明書チェーンは順番通りである必要があります。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です。

4.5.2 HTTPS アクセスのためのウェブ管理インタフェースを設定する

1. セクション 3.4 で設定した IP アドレスに SSH 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 で設定した管理者のユーザー名とパスワードを使用してログインしてください。
2. SFTP を使用して、秘密鍵/証明書のペアとオプションの証明書バンドルをアップロードします。
3. 次のコマンドを入力して、ステップ 2 でアップロードしたファイルをウェブ管理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構成します。

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

4. ウェブ管理者インタフェースにアクセスできることをテストします。たとえば、ブラウザに https://cms-server.mycompany.com（または IP アドレス）に相当するものを入力し、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。

メモ：バージョン 3.0 からは、ライセンスなしでトライアルモードを 90 日間のフル機能期間として使用できます。この場合、ウェブ管理インターフェイスには、この期間中、「この CMS は現在ライセンスされていません」と表示されます。Smart licensing の詳細および 3.0 での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 スケジューラ用のメールサーバーを設定する

このセクションでは、スケジューラコンポーネント用にメールサーバーを設定する手順について説明します。ミーティングがスケジュール、キャンセル、または変更されると、メール通知が参加者に送信されます。スケジューラは、SMTP メールサーバーの設定を介した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構成、メールプロトコルの有効化、認証のためのユーザー名の設定は、次のスケジューラ MMP コマンドで指定します。

```
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、メールはスケジューラで設定されません。スケジューラがメール招待を送信するには、少なくとも 1 つのメールサーバーを設定する必要があります。メールは、ミーティング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。メールサーバーがダウンした場合、別のスケジューラがメールを送信します。

ミーティング サーバが 5000 ミリ秒 (5 秒) 以内に Exchange 電子メール サーバから応答を受信しない場合、スケジューラは要求を自動的に拒否します。

スケジューラは、次のタイプのメール設定をサポートしています。

1. SMTP
2. SMTP と認証済みログイン（Auth Login）
3. SMTP および STARTTLS
4. SMTP（認証ログインと STARTTLS 使用）
5. SMTPS （トランザクション全体でエンドツーエンド TLS 暗号化）
6. SMTPS（認証ログインあり）

メモ：Exchange Server 2016 CU22 - 15.1.2375.7 および Exchange Server 2019 CU11 - 15.2.986.5 の使用をお勧めします。

ミーティングの招待状は、共通の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、ミーティングサーバー上で共通のメールアドレスと表示名を設定します。スケジューラが共通のメールアドレスから参加者にミーティング招待状を送信します。

共通メールアドレスが空の場合、スケジューラは開催者のメールアドレスから招待メールを送信します。

メモ：共通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では、MMP コマンド **scheduler email username <smtp user-name>** を使用してメールアドレスを設定する必要があります。MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりに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、表示名としてメールアドレスの他に開催者名を含めることもできます。ウェブアプリを使用してミーティングがスケジュールされると、ウェブアプリはミーティングをスケジュールしているユーザーの名前を開催者の表示名としてスケジューラに送信します。任意の名前を表示名として設定するには、オプションのパラメータ **organizationDisplayName** をスケジューラ API に含めることができます。

メール招待状が配信されなかった場合、スケジューラは定期的に送信を再試行します。スケジューラのメールキュークリーンアップは、特定の有効期限後に、キューに入れられた失敗メールをクリーンアップします。

4.6.1 スケジューラメールの設定（SMTP あり）

スケジューラが SMTP 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定ポートでリッスンするように設定します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   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 スケジューラ SMTP（認証ログイン設定あり）

スケジューラが SMTP（認証ログインあり）経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコル用の指定ポートでリッスンするように設定し、SMTP サーバーを有効にします。

認証ログインをサポートし、認証用のユーザーアカウントを設定します。MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりにメールを送信できる適切な権限が必要です。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

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

3. [認証ログイン（Auth Login）] 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てください。

   scheduler email username <username>

   パスワードを入力してください。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

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 SMTP と STARTTLS の設定

スケジューラが SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートで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の、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。しかし、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された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>
   たとえば、

   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、SFTP 経由で Meeting Server VM にアップロードします。それから、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>
   設定された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 名がメールサーバーーの 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 Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、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 スケジューラ SMTP（STARTTLS 設定による認証ログインあり）

スケジューラが Auth Login を使用した SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートでリッスンするように設定し、STARTTLS を有効にします。さらに、SMTP サーバーを有効にしてログイン認証をサポートし、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の、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。しかし、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された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

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

3. [認証ログイン（Auth Login）] 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
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

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、SFTP 経由で Meeting Server VM にアップロードします。それから、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>

   設定された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 名がメールサーバーーの 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 Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、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 SMTPS の構成

スケジューラが SMTPS 経由で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 SMTP 暗号化をサポートするようにメールサーバーを設定します。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。しかし、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された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

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

3. メールプロトコルを SMTPS 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、SFTP 経由で Meeting Server VM にアップロードします。それから、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>

   設定された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 名がメールサーバーーの 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 Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、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が SMTPS を使用してメール設定を完了できるようにします。

   scheduler enable

4.6.6 スケジューラ SMTPS（認証ログイン設定あり）

スケジューラが Auth Login を使用した SMTPS 経由で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 SMTP 暗号化をサポートするようにメールサーバーを設定します。さらに、SMTPS サーバーが Auth Login をサポートするようにし、認証に使用す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の、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。しかし、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された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

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

3. [認証ログイン（Auth Login）] 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

   パスワードを入力してください：

   パスワードを再度入力してください：

5. メールプロトコルを SMTPS 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、SFTP 経由で Meeting Server VM にアップロードします。それから、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>

   設定された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 Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、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が Auth Login で SMTPS を使用してメール設定を完了できるようにします。

   scheduler enable

4.6.7 スケジューラの詳細ログ

スケジューラは、ウェブブリッジ接続、メール通知、およびスケジューラ timedLogging MMP コマンドを使用した API の詳細なログを有効にするオプションをサポートしています。

timedLogging が有効ではない場合、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>
```

たとえば、

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

time 変数は秒単位で表され、設定された継続時間の timedLogging を有効にします。

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

設定した継続時間が経過するか、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 の導入を計画する

メモ：バージョン 3.0 からは、ライセンスなしでトライアルモードを 90 日間のフル機能期間として使用できます。

初期設定後、Cisco Meeting Server 2000 は次の場所で導入できます。

- 単一のサーバーは、通常、多数の同時内部呼び出しを必要とする 1 つの場所を持つ組織に適しています。通話容量の情報については、A.4 を参照してください。
- Cisco Meeting Server 2000 が内部ネットワークに導入されたコアノードであり、エッジコンポーネント（TURN サーバー）がエッジサーバー（Cisco Meeting Server 1000、Cisco Meeting Server 仕様に基づく VM server、Cisco Expressway）が DMZ に導入されます。

  Cisco Meeting Server ウェブエッジ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。
- スケーラブルで復元力のある展開の複数のコアノードの 1 つとして、大規模な電話会議、使用量の増加をサポートし、ダウンタイムを最小限に抑えます。

適切な導入を決定するためのガイドとして『計画と準備の導入ガイド』を使用し、導入と証明書のガイドに従ってください。

付録 A 技術仕様

A.1 物理仕様：

シャシー：Cisco UCS 5108 ブレードサーバーシャシー 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 電気的仕様

最大電力：	230V で 3.36KW、14.74A
	115V で 3.38KW、29.48A
電源	4 x 2500W Plattin HD ホットプラグ対応電源

A.4 ビデオおよび音声仕様：

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間でのコールキャパシティの比較を示しています。

表 1：ミーティングサーバプラットフォーム間の通話容量

通話のタイプ	Cisco Meeting Server 1000 M6	Cisco Meeting Server Small M7	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M6
フル HD の通話 1080p60 ビデオ 720p30 コンテンツ	40	60	175	324
フル HD コール 1080p30 ビデオ 1080p30/4K7 コンテンツ	40	60	175	324
フル HD 通話 1080p30 ビデオ 720p30 コンテンツ	80	120	350	648
HD 通話 720p30 ビデオ 720p5 コンテンツ	160	240	700	1296
SD 通話 480p30 ビデオ 720p5 コンテンツ	320	480	1000	1875
音声通話 （G.711）	3000	3000	3000	3200

注: Meeting Server Small M7 バリアントは、最大 94 個の vCPU と 128 GB の RAM 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

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に応じて最大 300,000 人のユーザをサポートできます。クラスタ中のすべてのデータベースは、同じスペックサーバー上になければなりません。

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

Cisco Meeting Server	ユーザーの発信者最大数
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

メモ：多数のユーザーを LDAP 同期すると、通話参加時間が長くなる可能性があります。メンテナンス期間中またはオフピーク時に、Meeting Serverに新しいユーザー/スペースを追加することをお勧めします。

A.6 帯域幅要件

Cisco Meeting Server 2000 は、720p で最大 700 件の同時通話をサポートします。これには 3 4 Gbps のネットワーク帯域幅が必要です。

A.7 ドライバーの仕様

次の表は、Cisco ミーティングサーバーでサポートされているドライバーのバージョンを示しています。

ドライバ	サポートされるバージョン
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 Cisco ライセンス

このセクションでは、Smart Licensing のライセンス情報について説明します。

B.1 スマートアカウントおよびバーチャルアカウント情報

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。バーチャルアカウントを使えば、部門ごとなど、指定の指定ごとにライセンスを整理することができます。Meeting Server および Meeting Management でスマートバーチャルアカウントを使用する際の注意事項は以下の通りです。

- 単一のミーティング管理に対する各 Meeting Server クラスタは、ユーザー定義のスマート バーチャル アカウントにリンクされている必要があります。
- 各バーチャルアカウントは、Smart Licensing を処理するように設定された単一のミーティング管理サーバーのみに接続できます。
- 1 つのミーティング管理のみをスマートに設定します。Smart Licensing の 2 つ目の冗長ミーティング管理を Smart に設定**しないでください。**ライセンス使用数の二重カウントが発生するため、お勧めしません。
- PMP Plus、SMP Plus、および録画/ストリーミングライセンスは、単一のバーチャルアカウント内の単一のミーティング管理インスタンスおよび Smart Licensing を使用して、複数のクラスターにわたって共有できます。

B.2 Meeting Server でのスマートライセンスの仕組み - 概要

Meeting Server でライセンスが機能するには、Meeting Management が必須です。Meeting Server と Meeting Management の間の信頼と相互作用は、Smart を使用したライセンシング、または既存の顧客の場合はインストール済みのライセンスファイルの使用をサポートします。この信頼されたリンクにより、ミーティング管理は Meeting Server にライセンスを付与します。

メモ：Cisco Meeting 管理を使った Smart Licensing の管理の詳細は、『ミーティング管理管理者ガイド』を参照してください。

Smart Licensing を実装するためのワークフローの概要は以下の通りです。

1. ミーティング管理を Smart Licensing バーチャルアカウントに登録します。
2. Meeting Server が最初に起動したとき、ライセンス状況の値は定義されていません。

メモ：トライアルモードは、90 日間のフル機能の期間、ライセンスなしで使用できます。

---

3. Meeting Server は、Smart Licensing を管理するためにセットアップされたミーティング管理インスタンスに最初に接続するときに、Meeting Server にライセンスが以前に適用されているかどうかを確認します。有効になっていない場合、ライセンスの有効期限が 90 日後に設定されます。

   ライセンスの有効期限はミーティング管理に表示され、また付録 B.5 に示すように clusterLicensing API にも返されます。

   メモ：機能ライセンスの有効期限は、最大で 90 日後になります。

   ---

4. Meeting Management は、Meeting Server が準拠していることを確認するために必要なライセンスがあるかどうかを確認するために、クラスターの Meeting Server ライセンスの使用状況を照合し、スマートアカウントに日単位でレポートを行います。スマートアカウントはミーティング管理に応答し、Meeting Server が準拠しているかどうかを示します。ミーティング管理では、有効期限を次のように適切に設定します。

   a. ミーティング管理が、ライセンスが存在し、特定の機能の利用権限を下回っていることを確認した場合、有効期限は 90 日後に延長されます。

      メモ：Meeting Server がミーティング管理に接続せず、90 日間の使用状況データを送信しない場合、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措置については、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資格を超える場合、またはライセンスが見つからない場合、施行は次のように行われます。

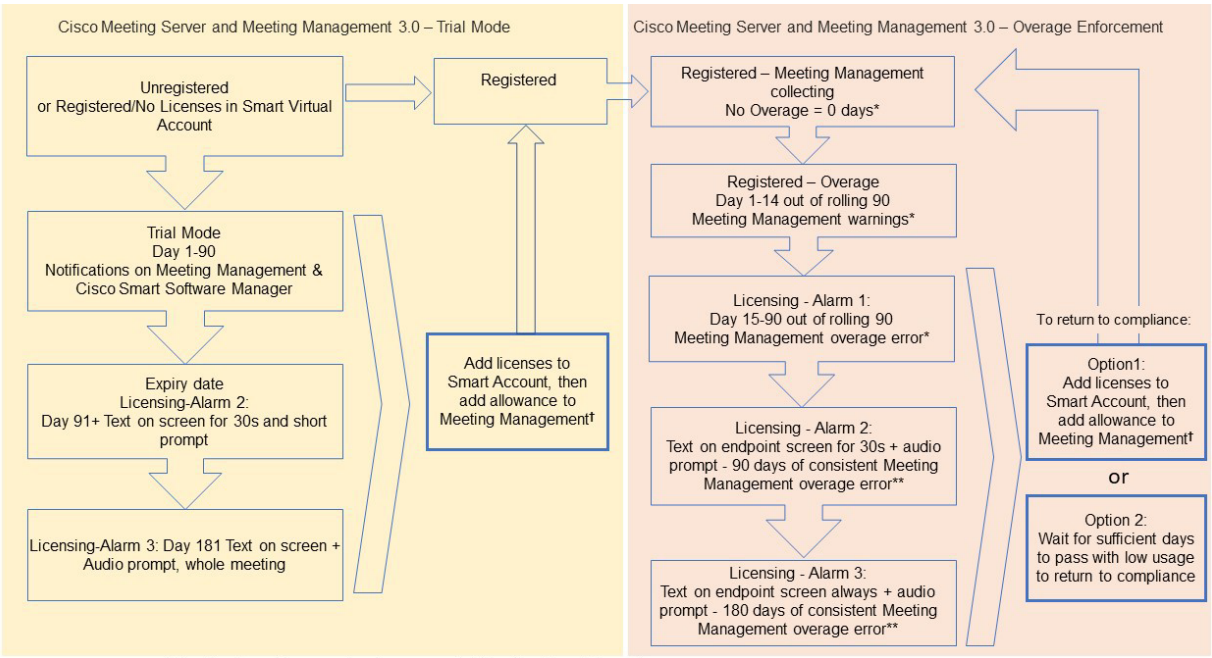
   b. ミーティング管理が過去 90 日間のうち 15 日間未満が非準拠であると特定した場合、これを許可し、Meeting Server の有効期限日をその時点から 90 日後の将来にリセットします。管理者は「ライセンスが不十分」を通知する視覚的な警告を受け取ります。

c. ミーティング管理で過去 90 日間のうち 15 日間以上で準拠していないことが確認された場合、第 1 レベルの強制（アラーム 1）が発生します。つまり、ミーティング管理インターフェイスに準拠していないことが通知されます。

d. 超過が続く場合、ミーティング管理は 90 日のクロックをリセットしません。新しいライセンスを追加するための xx 日間のカウントダウンが表示されます。そうしないと、ミーティング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。

付録 B の左側にトライアルモードで最初に起動してから、右側に超過数の施行に至るまでの強制フローを示します。

図 5：Cisco Meeting Server および Cisco Meeting Management Smart Licensing の強制フロー



* Counting days of overage (i.e. where usage is higher than the entitlement)
** Counting days where Meeting Management is in an error state (i.e. the state where there are 15 continuous days overage out of the last 90 days)
† To ensure accurate reporting, the administrator needs to specify within Meeting Management the number of licenses that are held in the Smart Account

B.3 期限切れライセンス機能の強制アクション

以前は、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 から、機能がライセンスされているかどうかの現在のステータスが動的に変更される可能性があります。これは、機能ライセンスの有効期限が切れている場合や（以前は再起動するまで確認できなかった場合）、または API が変更された場合などです。ミーティング管理で強制措置が Smart Licensing で計算されます。

メモ：Smart Licensing ポータルを使用して、「不十分なライセンス」のメール通知を有効にできます。

ライセンス機能の有効期限が切れると、 表 3 に記載のアクションが行われます。

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	有効期限が切れた場合：すべての参加者/すべてのミーティングのミーティングに参加するときに、視覚的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になった場合、またはライセンスが存在しない場合：以前と同じですが、ビジュアルメッセージは永久的なものです。音声プロンプトにより、「展開はライセンスに準拠していません。管理者に連絡してください」が再生されます。（アラームレベル 3）ただし、暗号化されたコールは、ライセンスなし状態では処理されません。 メモ：上記のアクションを防ぐには、callBridge または callBridgeNoEncryption のみが必要です。
callBridgeNoEncryption	
PMP/SMP	
customizations	有効期限が切れているか、存在しない場合、ミーティング中にカスタマイズ機能はアクティブになりません。
recording	有効期限が切れているか、出席していない場合、新しい録画を開始することはできません（サードパーティのレコーダーかどうかは関係ありません）。 このライセンスは録画とストリーミングを表すため、同じ制限がストリーミングにも適用されます。

アラーム 2 および 3 をオフにするには、スマートアカウントにライセンスを追加するだけです。

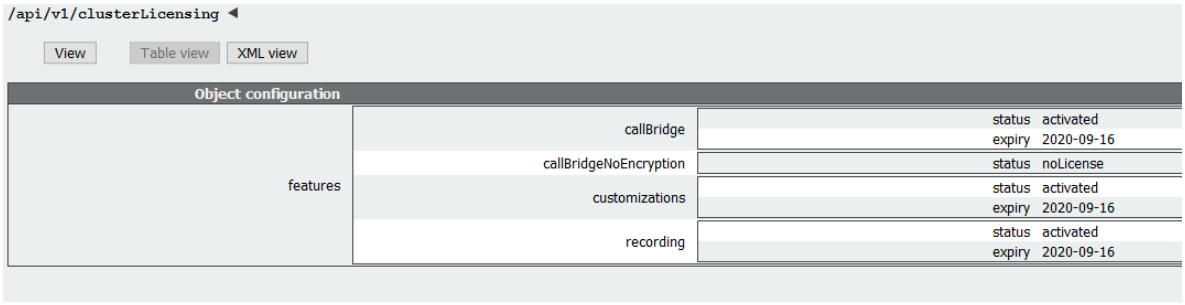
B.4 ライセンス情報を取得する方法（Smart Licensing）

Meeting Serverのウェブ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、

1. Meeting Serverのウェブ管理インタフェースにログインして 設定（Configuration）>API を選択します。
2. API オブジェクトのリストで、/api/v1/clusterLicensing 後にタップします。

3. クラスターの現在のライセンス状況は、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.5 Cisco Meeting Server ライセンス

次の機能を使用するにはライセンスが必要です。

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

機能ライセンスに加えて、ユーザーライセンスも購入する必要があります。ユーザーライセンスには 2 つの異なるタイプがあります。

- PMP Plus、
- SMP Plus、

メモ：トライアルモードは、90 日間のフル機能の期間、ライセンスなしで使用できます。

ユーザ ライセンスの詳細については、 セクション B.7 を参照してください。

注: Cisco Meeting Server Small、Cisco Meeting Server、および VM ソフトウェア イメージのアクティベーション キーを購入する際に、SIP メディア暗号化が有効になっているか、SIP メディア暗号化が無効になっているか (暗号化されていない SIP メディア) を選択できます。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.5.1 パーソナル Multiparty Plus ライセンス

Personal Multiparty Plus（PMP Plus）は、頻繁にビデオミーティングを主催する特定のユーザーに割り当てられた指名主催者ライセンスを提供します。これは、Cisco UWL Meetings または Flex Meetings（PMP Plus を含む）を通じて購入できます。Personal Multiparty Plus は、ビデオ会議のためのオールインワンのライセンス製品です。これにより、ユーザーはあらゆるサイズの電話会議を開催できます（導入された Cisco Meeting Server ハードウェアの制限内）。誰でもどのエンドポイントからでもミーティングに参加でき、このライセンスは最大 HD 1080p60 品質のビデオ、音声、コンテンツ共有に対応します。

メモ：Unified Communications Manager を使用すると、アドホック電話会議の開始者を識別することができます。PMP Plus ライセンスが割り当てられている場合は、それが電話会議で使用されます。

メモ：個人の PMP Plus ライセンスを使用するアクティブな通話数を確認するには、パラメータ **`callsActive`** を API オブジェクトで使用します。**`/system/multipartyLicensing/activePersonalLicenses`**.通常、2 つのコールをアクティブにできるため、1 つは開始、もう 1 つは終了とします。通話が Call Bridge のクラスターで発生する場合、パラメータ **`weightedCallsActive`** を API オブジェクトで使用します。**`/system/multipartyLicensing/activePersonalLicenses`** for each Call Bridge in the cluster.クラスター全体の **`weightedCallsActive`** の合計が、個人のPMP Plusライセンスを使用するクラスタ上の個別のコール数と一致します。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.8 を参照してください。

B.5.2 Shared Multiparty Plus ライセンス

Shared Multiparty Plus (SMP Plus) は、まれにビデオミーティングを主催する複数のユーザーによって共有される同時ライセンスを提供します。Shared Multiparty Plus は、PMP Plus 主催者ライセンスを持たないすべての従業員がビデオ会議にアクセスできるようにします。これは、多くの従業員が共有する会議室システムを展開している顧客に最適です。PMP Plus を持つユーザまたは SMP Plus ライセンスを使用するユーザーは、同じように優れたエクスペリエンスを得ることができます。スペースでミーティングを主催したり、アドホック ミーティングを開始したり、今後のミーティングをスケジュールしたりできます。各共有主催者ライセンスは、任意のサイズ (展開されたハードウェアの制限内) の 1 つの同時ビデオ ミーティングをサポートします。

注： 必要な SMP Plus ライセンスの数を確認するには、パラメータ **`callsWithoutPersonalLicense`** を使用します。API **`/system /multipartyLicensing`**.通話が Call Bridge のクラスター上にある場合は、パラメータ **`weightedCallsWithoutPersonalLicense`** を API object **`/system/multipartyLicensing`** で使用します。> クラスター内の各 Call Bridge に対して。クラスター全体の **`weightedCallsWithoutPersonalLicense`** の合計は、SMP Plus ライセンスを必要とするクラスター上の個別の通話の数と一致します。

B.6 スマートライセンシング登録プロセス

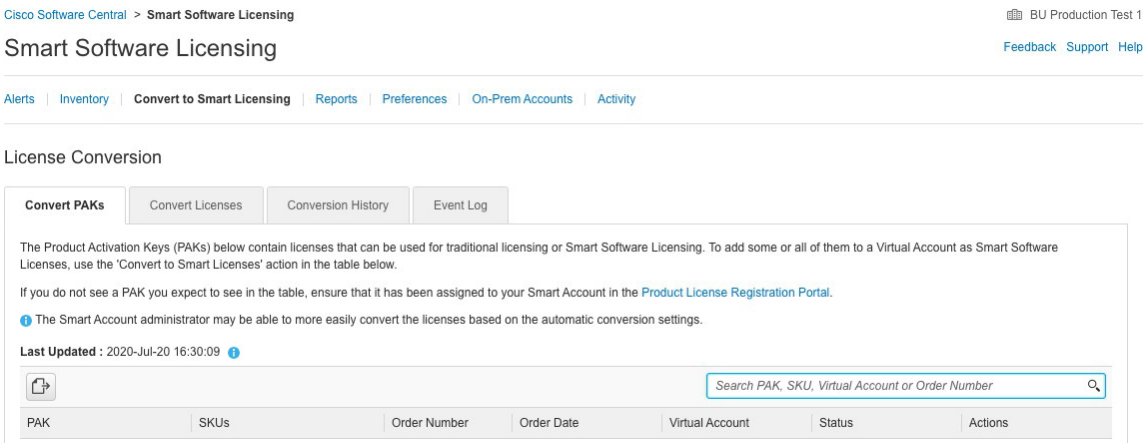
スマートライセンシングの有効化

1. Cisco Smart Software Manager (CSSM) ポータル にログインし、[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ミーティング管理のインスタンスを開きます。
5. **設定** ページの **[ライセンス]** タブに移動します。
6. [**変更**] をクリックします。
7. [Smart Licensing] を選択し、 **[保存]** を選択します。
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、ミーティング管理を Smart Licensing ポータルに接続できます)。
10. **[登録（Register）]** をクリックします。
11. 登録が済んだら、バーチャルアカウントにあるライセンス数を確認してください。
12. ミーティング管理で、 **ライセンス** ページに移動します。

13. バーチャルアカウントで所有す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に表示されていないライセンスがある場合は、[**ライセンスの変換**] タブを使用し、PAK で検索し、**[ライセンスの変換] を選択します。** 追加 図 7 に従います。(ライセンスが見つからない場合は、 licensing@cisco.com にメールを送信してケースを開きます。)

図 7: Smart Licensing のライセンス変換



B.7 ユーザーに Personal Multiparty ライセンスを指定する

このプロセスでは、ユーザーが単一の LDAP ソースからインポートされる必要があります。詳細については、『ミーティング管理管理者ガイド』の「プロビジョニング - ユーザーのインポート」の章を参照してください。

B.7.1 特定のユーザがライセンスを持っているかどうかを確認するには:

1. API オブジェクトのリストで、[**/users 回の後**] の ► をタップします。
   a. 特定のユーザーの **オブジェクト ID** を選択します
   b. このユーザーに関連付けられた **userProfile** の **オブジェクト ID** を特定する
2. API オブジェクトのリストで、[**/users 回の後**] の ► をタップします。
   a. 特定のユーザーの **オブジェクト ID** を選択します

b. パラメータ **hasLicence**の設定を確認してください。**true** に設定すると、ステップ 1 で特定されたユーザーが Cisco Multiparty ユーザライセンスに関連付けられます。**false** に設定すると、ユーザーに Cisco Multiparty ユーザライセンスは関連付けられません。

注： userProfile が削除されると、ldapSource およびインポートされたユーザーの userProfile の設定が解除されます。

B.8 Cisco Multiparty ライセンスの割り当て方法

スペースでミーティングが開始されると、Cisco ライセンスがスペースに割り当てられます。Cisco Meeting Serverにより割り当てられるライセンスは、以下のルールにより決定されます。

- 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ている、Meeting Serverからインポートされた LDAP ユーザーに対応する場合、その所有者のライセンスは、その人物が電話会議でアクティブであるかどうかに関係なく割り当てられます。
- ミーティングが Cisco Unified Communications Manager からのアドホック エスカレーションで作成された場合、Cisco Unified Communications Manager はミーティングをエスカレートするユーザーの GUID を提供します。その GUID が、Meeting Serverからインポートされた Cisco PMP Plus ライセンスを持つ 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。そうでない場合は、
- ミーティングが Cisco TMS バージョン 15.6 以降からスケジュールされた場合、TMS はミーティングの所有者に情報を提供します。そのユーザーが、Cisco PMP Plus ライセンスが割り当てられたユーザ ID/メールアドレスで、Meeting Serverからインポートされた 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ミーティングに割り当てられます。そうでない場合は、次に、
- Cisco SMP Plus ライセンスが割り当てられている。

B.9 Cisco Multiparty ライセンスの使用状況を確認する

マルチパーティライセンスの使用状況を表示するには、Meeting Management を使用することをお勧めします。ただし、API は使用できます。

表 4 は、Multiparty ライセンスの消費量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の一覧です。

表 4: マルチパーティライセンスの使用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	使用目的...
/system/license	個人用、共有	Cisco Meeting Server のコンポーネントが Multiparty ライセンスを持ち、アクティベートされているかどうかを判別します。値は次のとおりです: noLicense、アクティブ化、猶予、期限切れ。 有効期限日と上限数も表示されます。
/system/multipartyLicensing	PersonalLicenseLimit、sharedLicenseLimit、personalLicenses、callsWithoutPersonalLicense、weightedCallsWithoutPersonalLicense	利用可能で使用中のライセンスの数を示します
/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なコール数を示します。
/userProfiles	hasLicense	ユーザーが 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。

Cisco Multiparty ライセンスをサポートするための、これらの追加のオブジェクトとフィールドの詳細については、『Cisco Meeting Server API リファレンスガイド』を参照してください。

B.10 SMP Plus ライセンスの使用数を計算する

次の特定のシナリオにおいて、ミーティングで使用される SMP Plus ライセンスは、フルライセンスの 1/6 に減らされます。

- 出席者がビデオを使用していない音声のみの電話会議
- Lync ゲートウェイ通話 (Meeting Serverが記録またはストリーミングを行っている場合を除く)
- ウェブアプリと 1 つの SIP エンドポイント、または 2 つのウェブアプリが関係する二地点間コールMeeting Serverが録画またはストリーミング中の場合を除き、録画中またはストリーミング中は完全な電話会議と見なされ、SMP Plus ライセンスが消費されます。

フル SMP Plus ライセンスは、所有者のプロパティが未定義のスペースからインスタンス化された音声/ビデオ会議、PMP Plus ライセンスを持たないインポートされた LDAP ユーザーが所有、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された LDAP ユーザーが所有する音声ビデオ会議です。これは参加者数に関係ありません。

注： ポイントツーポイント通話は次のように定義されます:

- Meeting Server 上に永久スペースがない
- レコーダーまたはストリーマを含めて 2 人未満の参加者
- Lync AVMCU で主催されている参加者がいない、

これには、Lync ゲートウェイ通話だけでなく、他のタイプの通話 (ポイントツーポイント ウェブ アプリからウェブ アプリ、ウェブ アプリから SIP、および SIP から SIP) が含まれます。

B.11 ミーティングサーバーからライセンス使用状況のスナップショットを取得する

管理者はMeeting Serverからライセンスの使用状況を取得できます。これらにはウェブ管理インターフェイスからはアクセスできません。代わりに、POSTMAN:

展開内のMeeting Serverの主催者 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主催者 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。

/system/MPLicenseUsage で GET を使用して、指定された主催者 ID を持つMeeting Serverの Call Bridge からライセンスの使用状況を取得します。スナップショットの開始時刻と終了時刻を指定します。
使用中のパーソナルライセンス数、使用中の音声のみ、ポイントツーポイント、または音声でもポイントツーポイントでもないライセンスの数、記録されている通話の数、ストリーミングされた通話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、通話がスパンする Call Bridge の数で正規化されます。

B.12 ライセンスレポート

ミーティング管理には、過去 90 日間のライセンスレポート/使用情報があります。Cisco Smart Software Manager にはライセンスレポート情報も含まれます。録画ライセンスの使用は同時に録画する会議の数を示し、同様にストリーミング ライセンスの使用は同時にストリーミングする会議の数を示します。

B.13 レガシーライセンスファイルによる方法

この項は、従来のライセンス方法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廃止されました。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.13.1 ライセンスファイルの適用

Cisco Meeting Server 2000 で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 がアクティベートされ、通話を発信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。

ライセンスを購入した後、従来のライセンス方法を使用している場合にのみ、この章に従って Cisco Meeting Server にライセンスを適用してください。

B.13.1.1 ライセンスファイルを Cisco Meeting Server 2000 に転送する

このセクションでは、Call Bridge がリッスンするポートをすでに設定しており、Call Bridge 証明書をアップロードしていることを前提としています。

SFTP を使用してライセンスファイルをミーティングサーバに転送します。ポート A の IP アドレスがすでにわかっている場合は、手順 1 を省略します。

1. で構成されたポート A の IP アドレスに SSH 接続する セクション 3.4は、管理者のユーザ名とパスワードを使用してログインします。 セクション 3.3。MMP コマンド **`ipv4 a`** または **`ipv6 a`** を使用して、ポート A の IP アドレスを見つけます。
2. cms.lic ファイルを SFTP を使用してポート 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 で接続し、MMP 管理者ユーザの資格情報を使用してログインします。
4. MMP コマンドを使用して Call Bridge を再起動する **`callBridge の再起動`**。これにより、ライセンスファイルが適用されます。
5. Call Bridge を再起動したら、MMP コマンドを入力してライセンスのステータスを確認します。
   `license`
   アクティブ化された機能と有効期限が表示されます。

メモ：バージョン 3.0 からは、ライセンスなしでトライアルモードを 90 日間のフル機能期間として使用できます。この場合、ウェブ管理インターフェイスには、この期間中、「この CMS は現在ライセンスされていません」と表示されます。Smart licensing の詳細および 3.0 での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.13.2 従来のライセンス方法を使用して Cisco ユーザライセンスを取得する

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

これらの手順に従い、次のアドレスを使用して、Meeting Server の MAC アドレスに PAK コードを登録します。Cisco ライセンス登録ポータルサイト。

1. サーバーの MMP にログインしてMeeting Server の MAC アドレスを取得し、MMP コマンドを入力します: **a の場合**
2. Cisco ライセンス登録ポータルサイト そしてMeeting Server の PAK コードと MAC アドレスを登録してください。
3. PAK に R-CMS-K9 アクティベーション ライセンスがない場合、機能ライセンスに加えてこの PAK が必要になります。
4. ライセンスポータルからライセンスファイルの zip 圧縮されたコピーがメールで送信されます。Zip ファイルを解凍し、結果として得られた xxxxx.lic ファイルの名前を **cms.lic**。
5. SFTP クライアントを使用して Meeting Server にログインし、 **cms.lic** ファイルを Meeting Server ファイルシステムにコピーする必要があります。
6. MMP コマンドを使用して Call Bridge を再起動する **callbridge restart**
7. Call Bridge を再起動したら、MMP コマンドを入力してライセンスのステータスを確認します。
   license
   アクティブ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 で主催される参加者のミーティング体験の一部は、ブランド化することができます。これには次のような要素が含まれます。

- [セルフビュー] ペイン内のウェブアプリのサインイン背景画像、サインイン ロゴ、サインイン ロゴの下のテキスト、アイコン、カスタム仮想背景画像、およびブラウザー タブ上のテキスト
- IVR メッセージ
- SIP および Lync 参加者のスプラッシュ画面の画像、およびすべての音声プロンプト/メッセージ、
- ミーティング招待状のテキスト。

単一のリソース セットのみが指定された単一のブランドを適用する場合（ウェブアプリのサインインページ 1 つ、音声プロンプト 1 つ、招待テキスト 1 つ）、こ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により、異なるスペース、IVR、Web Bridge に異なるリソースを使用できます。リソースは、システム、テナント、スペース、または IVR レベルで、API を使用して割り当てることができます。

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

付録 D Cisco Meeting Server 2000と仮想化環境でのMMPとAPIの違い

D.1 特定の MMP コマンドの違い

すべての MMP コマンドについては、 MMP コマンドリファレンス を参照してください。Cisco Meeting Server 2000 を実行すると、仮想化された Cisco Meeting Server と比較して、いくつかの違いがあります。

コマンド	Cisco Meeting Server 2000	Cisco Meeting Server 1000 /Cisco Meeting Server Small および仮想 Cisco Meeting Server
shutdown	MMP では利用できません。電源を切る前に、Cisco UCS マネージャを使用して、ブレードサーバの電源を 切ってください。	vSphere の電源ボタンは使用しないでください。**シャットダウン** コマンドを使用してください。
状態	MMP では利用できません。Cisco UCS Manager	使用不可
シリアル番号:	サーバーのシリアル番号を返します。	使用不可
dns	インターフェイスを指定しないでください。 例 **dns add forwardzone <domain-name> <server ip>**	インターフェイスを指定しないでください。 例 **dns add forwardzone <domain-name> <server ip>**
user evict	応答可能	応答可能

D.2 異なるプラットフォームで有効になるコンポーネントの違い

下の表は、異なる Cisco Meeting Server プラットフォームで利用できるコンポーネントの一覧です。プラットフォームでコンポーネントが利用できない場合、そのコンポーネントに特有の MMP および API コマンドは利用できません。例えば、TURN サーバー用の 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	Cisco Meeting Server1000/ Small および仮想 Cisco Meeting Server
Call Bridge	応答可能	応答可能
Web Bridge 3	応答可能	応答可能
データベース	応答可能	応答可能
スケジューラ	応答可能	応答可能
TURN サーバ	使用不可	応答可能
レコーダ	使用不可	応答可能
アップローダー	使用不可	応答可能
ストリーマー	使用不可	応答可能
SNMP MIB	機能は現在使用できません	応答可能

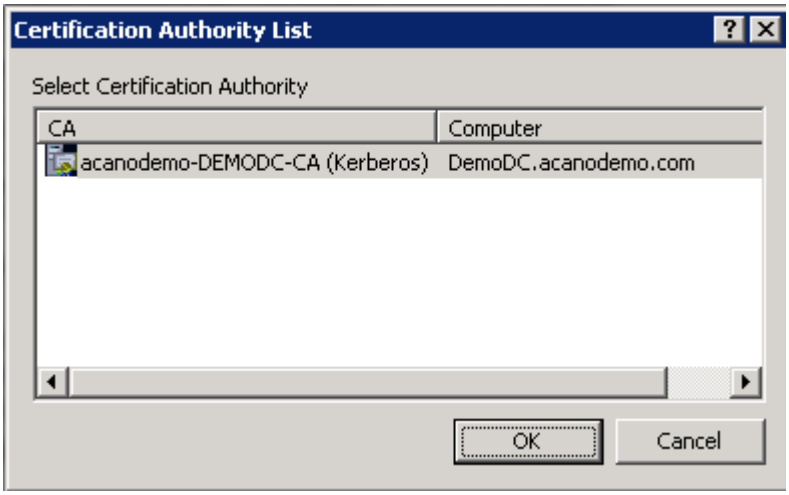
付録 E ローカルの Certificate Authority によって署名された証明書を作成する

この付録では、Active Directory 証明書サービスの役割がインストールされた 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 サーバーのコマンドライン管理シェルで以下のコマンドを発行し、パスと CSR 名をお客様の情報に置き換えます。

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

3. 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、[OK] をクリックします。

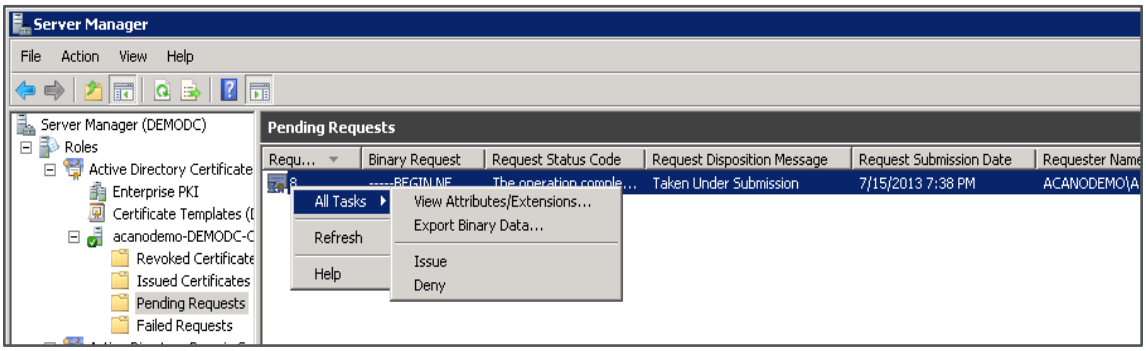


4. 次のいずれかを実行します。
   - Windows アカウントに証明書を発行する権限がある場合、生成された証明書を webadmin.crt などとして保存するように指示されます。下記の手順 c に進みます。
   - 生成された証明書を発行するプロンプトが表示されず、代わりにコマンドプロンプトウィンドウに、「証明書の要求が保留中: 取得済み、送信中」というメッセージが表示され、次のように要求 ID がリストされている場合は、RequestID をメモし、次の手順を実行してから手順 c に進みます。

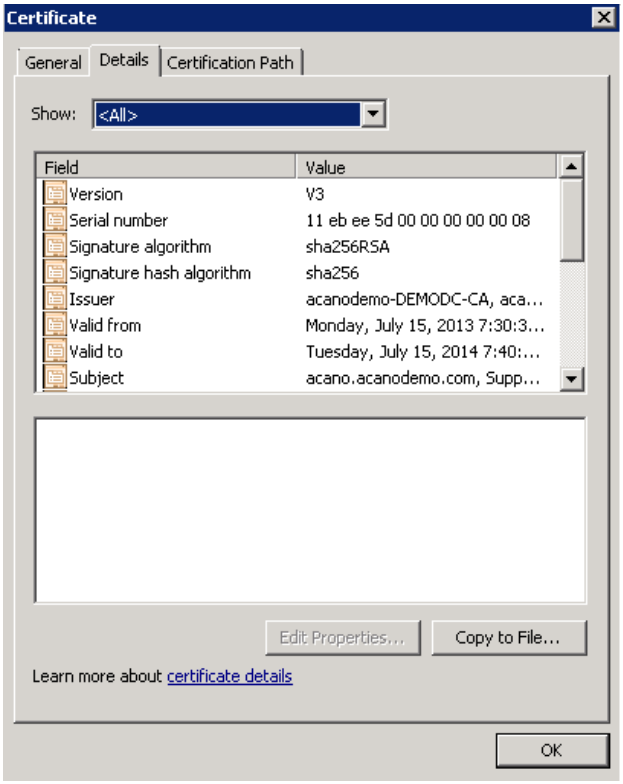
```
C:\Users\Administrator>certreq -submit -attrib "CertificateTemplate:WebServer" C
:\Users\Administrator\Desktop\demokitcsr.pem
Active Directory Enrollment Policy
  {0BD5D0B7-591F-4C77-AFEC-3C0E470F77D5}
  ldap:
RequestId: 8
RequestId: "8"
Certificate request is pending: Taken Under Submission (0)

C:\Users\Administrator>_
```

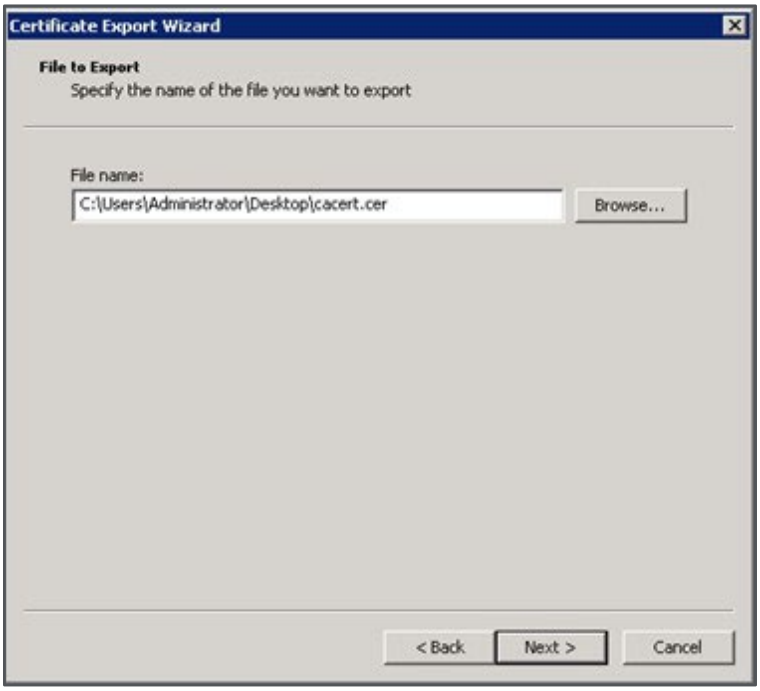
5. CA の [サーバ マネージャ] ページを使用して、[CA ロール] の下の [保留中のリクエスト] フォルダを見つけます。
6. [CMD] ウィンドウに表示されたリクエスト ID に一致する保留中のリクエストを右クリックし、**[すべてのタスク（All Tasks）] > [問題（Issue）]** を選択します。



7. 結果として署名された証明書は、[発行された証明書] フォルダーにあります。証明書をダブルクリックして開き、**[詳細]** タブを開きます (右を参照)。



8. **[ファイルにコピー]** をクリックして、証明書のエクスポートウィザードを開始します。
9. [Base-64 エンコード X.509 (.CER)] を選択して [**次へ**] をクリックします。
10. 証明書を保存する場所を参照し、 **`webadmin`** などの名前を入力して、[**次へ**] をクリックします。



11. 作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（例：webadmin.crt）と秘密キーを Cisco Meeting Server の MMP に転送します。 セクション 4.5.2 を参照してください。

注意: ウェブ登録機能がインストールされた CA を使用している場合は、BEGIN CERTIFICATE REQUEST および END CERTIFICATE REQUEST の行を含む CSR テキストをコピーして送信することができます。証明書が発行されたら、証明書のみをコピーし、証明書チェーンはコピーしません。BEGIN CERTIFICATE および END CERTIFICATE の行を含むすべてのテキストを含めて、テキストファイルに貼り付けてください。.crt、.cer または .pem の拡張子を持つ証明書としてファイルを保存します。

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 コンピューティング リソースが搭載された Cisco UCS 5108 ブレード サーバ シャシーで実行されます。

Cisco UCS Manager ファームウェア管理ガイド リリース 4.3 (x)、4.2(x)、4.1、または 4.0 の手順に従い、ファームウェアをアップグレードしてください。ここ をクリックして 、相互運用性テスト済みの利用可能な UCS Manager のバージョンを確認してください。

この付録には、ブレードのファームウェア バージョンを設定するために使用される CMS2000-FW ポリシーを更新するために必要な簡略化された手順が記載されています。

F.1 Cisco UCS Manager ファームウェア 4.0(x)、4.1(x)、4.2(x)、4.3(x) 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 Release 4.0(x)、4.1(x)、4.2(x)、4.3(x) 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)、4.2(x)、または 4.3(x) にアップグレードするには、次の手順をこの順番で行います。

1. インフラストラクチャ A 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。
2. 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) にアップグレードするためには、CMS2000-ファームウェアホストファームウェアパッケージを変更してください。
3. インフラストラクチャ A バンドルをリリース 4.0(x)、4.1(x)、4.2(x)、または 4.3 (x) にアップグレードします。
4. すべてのサーバの B バンドルをリリース 4.0(x)、4.1(x)4.2(x)、または 4.3 (x) にアップグレードするためには、CMS2000-ファームウェアホストファームウェアパッケージを変更してください。

F.2 CMS2000-ファームウェアポリシー用に主催者ファームウェアパッケージを更新する

前提条件：

適切なファームウェアが Fabric Interconnect に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-ファームウェアポリシーを更新する

```
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-ファームウェアポリシーを更新する

1. ナビゲーション ペインで、次をクリックします。 **サーバ**。
2. 開く **サーバ > ポリシー**。
3. ノードを展開します CMS 表示されます。
4. 開く **主催者ファームウェアパッケージ** を選択し、 CMS2000-FW します。
5. [**作業** ペインで **全般** 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**。[**パッケージバージョンの変更** 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** ドロップダウンリストから、ブレードの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 マネージャは、このポリシーを含むサービス プロファイルに関連付けられたすべてのサーバに対して、モデル番号とベンダーを確認します。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合、Cisco UCS マネージャは、サービス プロファイルに含まれるメンテナンス ポリシーの設定に従って、ファームウェアを更新します。

付録 G 追加の Cisco UCS Manager コマンド

この付録では、便利だが Cisco Meeting Server 2000 の初期セットアップには必要ないいくつかの Cisco UCS マネージャコマンドを紹介します。

G.1 ブレードサーバーの電源をオフにする

8 台のブレードサーバすべての電源を切ってから、電源をシャシーから取り除く必要があります。次に例を示します。

```
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 スロット間でブレードサーバーをスワップする

ラッキング中にブレードがスロット間でスワップされた場合、現在のスロットで使用される前に確認される必要があります。**show serverstatus** コマンドを使用してスロットを確認し、不一致のスロットを確認します。受信確認は、ブレードサーバと Fabric Interconnect モジュール間の接続を再構築します。完了には最大 20 分かかる場合があります。

メモ: 2 つのハードドライブを装備するブレードサーバは、スロット 1 にインストールする必要があります。

```
UCS-A# show server status
```

[サーバ（Server）]	Slot Status	プログラムの利用	全体	Status（ステータス）	ディスカバリ
1/1	装備済み	連絡不可能	OK		完了
1/2	装備済み	連絡不可能	OK		完了
1/3	装備済み	連絡不可能	OK		完了
1/4	不一致	連絡不可能		算出	不一致の再試行
1/5	不一致	連絡不可能		算出	不一致の再試行
1/6	装備済み	連絡不可能	OK		完了
1/7	装備済み	連絡不可能	OK		完了
1/8	装備済み	連絡不可能	OK		完了

```
UCS-A# 承認スロット 1/4

UCS-A* # 承認スロット 1/5

UCS-A* # commit-バッファ

UCS-A#
```

すべてのブレードが検出を完了するまで待ってから続行してください。

```
UCS-A# show server status
```

[サーバ（Server）]	Slot Status	プログラムの利用	全体 Status（ステータス）	ディスカバリ
1/1	装備済み	連絡不可能	OK	完了
1/2	装備済み	連絡不可能	OK	完了
1/3	装備済み	連絡不可能	OK	完了
1/4	装備済み	連絡不可能	OK	完了
1/5	装備済み	連絡不可能	OK	完了
1/6	装備済み	連絡不可能	OK	完了
1/7	装備済み	連絡不可能	OK	完了
1/8	装備済み	連絡不可能	OK	完了

G.3 Serial over LAN を無効にする（オプション）

MMP にアクセスするために Serial over LAN 接続を使用したくない場合は、SoL ポリシーを無効にすることができます。

注意: MMP の初期構成を完了するには SoL が必要です。Cisco Meeting Server にネットワーク IP アドレスを設定するまで、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 無効にした Serial over LAN を再度有効にする

以前 SoL を無効にしていて、今後 SoL を使用する場合にのみ、再度有効にする必要があります。

```
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式、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になります。

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

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。全著作権所有。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。CISCO およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズ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システムズ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。

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

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 の商標または登録商標