Cisco Meeting Server

Cisco Meeting Server 3.7

Cisco Meeting Server 1000 と仮想化展開の設置ガイド

2023 年 11 月 3 日

Cisco Systems, Inc. www.cisco.com

目次

変更履歴

日付	変更点
2023 年 3 月 16 日	バージョン 3.7 用に更新。
2022 年 8 月 23 日	バージョン 3.6 用に更新。
2022 年 4 月 20 日	バージョン 3.5 用に更新。
2022 年 1 月 10 日	データベース VM でサポートされる vCPU 数を更新
2021 年 12 月 15 日	バージョン 3.4 用に更新。
2021 年 9 月 3 日	付録 E のマイナーな編集。
2021 年 8 月 24 日	バージョン 3.3 用に更新。
2021 年 5 月 19 日	Web アプリの通話キャパシティと中規模 OVA Expressway の推奨事項に関するドキュメントを更新。
2021 年 4 月 22 日	スマートライセンスに関する「ご使用になる前に」の注意事項を追加。 表 2 を更新。
2021 年 4 月 14 日	バージョン 3.2 用に更新されました。 Cisco Meeting Server プラットフォーム、ESXi サポート、および coSpace 増加の RAM 要件によるコールキャパシティを更新。
2020 年 12 月 9 日	軽微な修正。
2020 年 11 月 30 日	バージョン 3.1 で更新。
2020 年 10 月 30 日	ESXi の情報を更新。
2020 年 10 月 6 日	マイナー修正。
2020 年 9 月 9 日	軽微な修正。
2020 年 9 月 2 日	レコーダー/ストリーマの VM の最小要件を 4 vCPU コアに明確化する軽微な編集。
2020 年 8 月 10 日	バージョン 3.0 用に更新。 X シリーズサーバーへの参照を削除。
2020 年 4 月 1 日	破損リンクを修正。
2019 年 11 月 27 日	400v/410v の参照資料を削除。
2019 年 11 月 13 日	ESXi のサポートをバージョン 2.8 用に更新、変更。
2019 年 7 月 16 日	本ドキュメントの誤った記述が訂正され、設置に関する章を再度挿入。
2019 年 5 月 30 日	ドキュメントのマイナー修正
2019 年 4 月 26 日	サポートされる VMware ESXi のバージョンを更新

日付	変更点
2019 年 4 月 9 日	その他の訂正。
2019 年 4 月 2 日	ESXi 6.5 Web Client を使用して OVA ファイルから Meeting Server を展開するための情報を追加。 その他の訂正。
2019 年 1 月 28 日	Cisco UCS C220 M5 ラックサーバーを使用した Cisco Meeting Server 1000 は、M4 の付いたものより優先されます。（2018 年 11 月から）。
2018 年 11 月 29 日	その他の訂正。
2018 年 9 月 24 日	Hyper-V の項とリファレンスを削除。
2017 年 12 月 20 日	Cisco Meeting Server バージョン 2.3 の ESXi 6.5 および ESXi 6.0 Update 3 のサポートを追加。
2017 年 11 月 27 日	Cisco Meeting Server 1000 のインストールに関するその他の詳細情報を追加。 AWS のリファレンスを削除。

1 はじめに

Cisco Meeting Server は、Microsoft、Avaya、およびその他のベンダーのさまざまなサードパーティキットと統合する、音声、ビデオ、および Web コンテンツのスケーラブルなソフトウェアプラットフォームです。Cisco Meeting Server 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、人と人が結びつくことができます。

Cisco Meeting Server ソフトウェアは、次のプラットフォームにロードされ、仮想ハードウェア vsm-1x をサポートする VMware ESXi 6.x を使用する仮想化展開として動作します。

- Cisco Meeting Server 1000（事前設定済みの Cisco UCS C220 ラックサーバー。2019 年の冒頭より、M4 Rack Server は M5 Rack Server になりました）。
- 仕様ベースの VM プラットフォーム。

注: バージョン 3.7 以降、ミーティングサーバーは ESXi バージョン 6.0 以下をサポートしません。これらのバージョン（ESXi 6.0/5.5）の .ova ファイルは提供されません。

次の表は、現行バージョンの Cisco Meeting Server ソフトウェアでサポートされている ESXi のバージョンを示しています。

表 1：ESXi バージョンのサポート

Cisco Meeting Server バージョン	ESXi バージョン
3.7	ESXi 6.5 P09 ESXi 6.7 P08 ESXi 7.0 アップデート 3j
3.6	ESXi 6.5 EP26 ESXi 6.7 EP 23 ESXi 7.0 アップデート 3d
3.5	ESXi 6.5 P07 ESXi 6.7 EP 23 ESXi 7.0 アップデート 3d
3.4	ESXi 6.5 P07 ESXi 6.7 P05 ESXi 7.0 アップデート 2a

分割された展開やスケーラブルな展開では多くの場合、Cisco Meeting Server の仮想展開はエッジサーバーとして使用されています。

機能と、参加者のユーザー体験は、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。ただし、仮想化された展開と物理展開（Cisco Meeting Server 2000）には互換性がありません。たとえば、仮想化された展開でバックアップを作成し、Cisco Meeting Server 2000 でロールバックすることはできません。この逆もできません。

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

1.1 仮想化プラットフォームの概要

注意： Cisco Meeting Server ソフトウェアを実行している仮想化プラットフォームに関係なく、最新のパッチによりプラットフォームが最新の状態になっていることを確認してください。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。

Cisco Meeting Server 1000：VMware ESXi バージョン 7.x と Cisco Meeting Server が出荷時に事前インストールされています。ただし、利用可能な最新バージョンの Cisco Meeting Server ソフトウェアではない場合があります。このガイドの手順に従って、Cisco Meeting Server 1000 を構成し、ライセンスを適用してください。Cisco Meeting Server が動作可能になったら、MMP コマンド **`version`** を使用して、インストールされたソフトウェアのバージョンを確認してください。最新のソフトウェアは こちら から入手できます。Cisco Meeting Server 1000 にインストールされたソフトウェアをアップグレードするには、当該ソフトウェアバージョンのリリースノートの指示に従ってください。

注：Meeting Server に ESXi 6.x が同梱されている場合、Cisco Meeting Server 1000 のデフォルトの Cisco UCS ESXi 6.x ログイン情報は、**`root`** でログインし、パスワードは **`password`** です。Meeting Server に ESXi 7.x が同梱されている場合、Cisco Meeting Server 1000 のデフォルトの Cisco UCS ESXi 7.x ログイン情報は、**`root`** でログインし、パスワードは **`c!SCo123`** です。

このログイン管理アカウントは変更することをお勧めします。パスワード変更の際、Cisco UCS ESXi には複雑なパスワードが必要になることに注意してください。

仕様ベースの VM プラットフォーム：過去の仮想化された Cisco Meeting Server のインストールからサーバーをアップグレードする場合は、Cisco Meeting Server のリリースノートの指示に従ってください。新規インストールの場合は、本ガイドに従って VM を作成して Cisco Meeting Server ソフトウェアをインストールします。

1.2 本ガイドの使用方法

このガイドでは、Cisco Meeting Server 1000 と仕様ベースの VM 展開の設置について説明します。

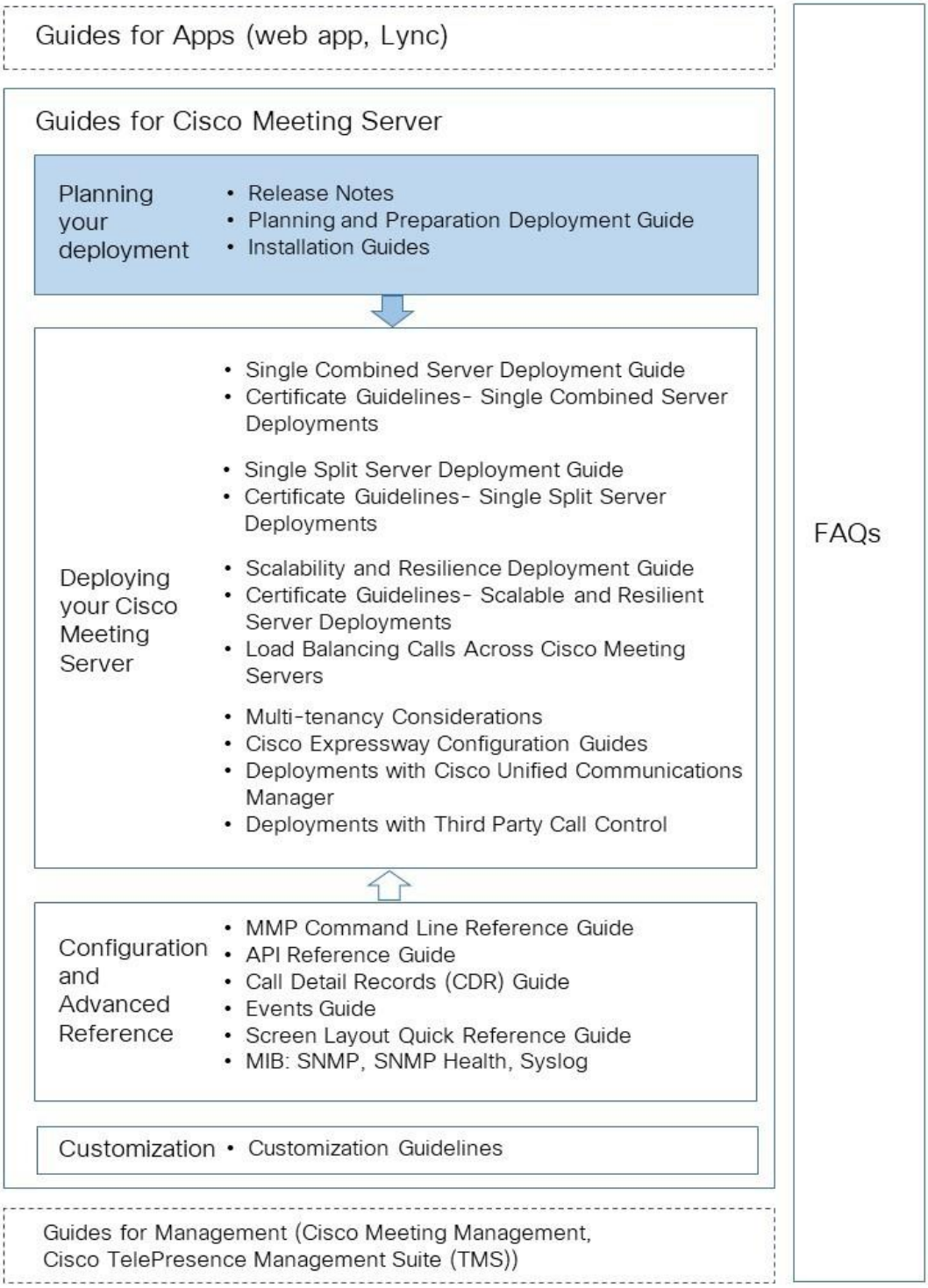
Cisco Meeting Server 1000 は事前にソフトウェアがインストールした状態で出荷されます。Cisco Meeting Server 1000 の構成を開始するには、このガイドの セクション 2.4 に進んでから、第 3 章に進んでください。

注：Cisco Meeting Server 1000 には仕様ベースの VM サーバー向けのさまざまな設定があり、事前設定されています。これらの設定を変更しないでください。

仕様準拠の VM 展開をインストールする場合、 第 2 章に進んでから第 3 章に進んで VM を構成してください。第 2 章は、VMware に精通した管理者を対象としています。

Cisco Meeting Server を構成し、ライセンスを適用したら、『展開の計画および準備導入ガイド』を使用して適切な展開を決定します。次に、対象となる展開と最も関連性の高い展開および証明書ガイドに従います。図 1 を参照してください。これらのドキュメントは、cisco.com から入手できます。

図 1：Cisco Meeting Server のインストールおよび展開用ドキュメント



注：Cisco のユーザーマニュアルで使用するアドレスの範囲は、RFC 5737 に定義されており、文書化用として明示的に予約されています。Meeting Server ユーザーマニュアルの IP アドレスは、特に明記しない限り、お使いのネットワークでルーティング可能な正しい IP アドレスで置き換える必要があります。

1.3 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』で詳述されています。Cisco Meeting Server 2000 の実行は、仮想化された Cisco Meeting Server と比べるといくつかの違いがあります。

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

1.4 異なるプラットフォームで有効にされたコンポーネント間の違い

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

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

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

2 設置

この章は、仕様準拠の VM プラットフォームおよび Cisco Meeting Server 1000 への展開に適用されます。VMware ホストを展開するには、セクション 2.2 に従ってください。Cisco Meeting Server 1000 を展開するには、セクション 2.4 に従ってください。

2.1 はじめる前に

2.1.1 Cisco Meeting Server ソフトウェアについて

Cisco Meeting Server ソフトウェアは、VMware ユーザー用の .ova ファイルとして提供されています。これは、単一のネットワーク インターフェイス、および Cisco Meeting Server アプリケーションを含む仮想ディスクを使用して新規 VM をセットアップするためのテンプレートです。

インストール後、次のように実行できる、十分に機能している Cisco Meeting Server を使用できます。

- 単一のサーバーで有効になっているすべてのコンポーネントを備えた完全なソリューション（単一統合型サーバー導入モデル）
- 内部ネットワークに導入されたコアサーバーで有効になっている一部のコンポーネントと、DMZ に導入されたエッジサーバーで有効になっている他のコンポーネントで構成される分割導入（単一分割サーバー導入モデル）
- 用途の拡大をサポートしダウンタイムを最小化するためにクラスタ化された、複数の Call Bridge とデータベースで構成される拡張性と耐障害性を備えた導入

同じ .ova ファイルが、すべての展開のインストールで使用されます。

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。

注：Meeting Management が必要な場合に 3.0 以降にスマートライセンスに関する問題を回避するには、Meeting Server を複製する代わりに、新しい Meeting Server を毎回インストールしてください。または、完全な工場出荷時の状態にリセットして、すでに複製されている VM Meeting Servers の新しい同一のホスト ID を割り当てることができます。

2.1.2 Cisco Meeting Server の VM 展開としてのホスト要件

Cisco Meeting Server は幅広い標準的な Cisco サーバーにおいて、VM 展開として動作します。さまざまな展開については、こちらの VM 展開の要件および UCS のテスト済みのリファレンス構成のリンク を参照してください。

Cisco Meeting Server は、Intel および AMD の両方のプロセッサを含む、Dell および HP のシステムなど、サードパーティサーバー上でも動作します。小型フォームファクタで、Klas VoyagerVM

や DTECH LABS M3-SE-SVR2 のような高耐久システムもサポートされています。このソフトウェアは、クラウドサービスと同様に VMware ESXi に展開できます。

表 2：サードパーティのサーバーで実行されている Cisco Meeting Server のホスト要件

	最小	推奨
サーバーのメーカー	すべて	すべて
プロセッサ タイプ	Intel Nehalem マイクロアーキテクチャ AMD Bulldozer マイクロアーキテクチャ	Intel Xeon 2600 v2 以降
プロセッサの周波数	2.0GHz	2.5Ghz
RAM	論理コアあたり 1 GB*	論理コアあたり 1 GB*
ストレージ	100 GB	100 GB

* ハイパーバイザやホスト上のその他の VM で使用するためには、システムに追加メモリが必要です。

注：Meeting Server は、シングルソケットサーバーとデュアルソケットサーバーのみをサポートしています。

注：ESXi 6.5 および ESX 6.0 アップデート 3 には、TLS 1.0 および TLS 1.1 と ESXi との通信を無効化できるようにするためのツールが用意されています。

表 3：推奨されるコア VM の構成

720p30 コールレッグ	CPU 構成	RAM 構成	システム例
50	Dual Intel E5-2680v2	32 GB（8x4GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
40	Dual Intel E5-2650v2	32 GB（8x4GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
25	Single Intel E5-2680v2	16 GB（4x4GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
15	Single Intel E5-2640v2	8 GB（4x2GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8

さらに、以下を実行できます。

- 利用可能なメモリの帯域幅を最大にするために、すべてのメモリチャネルにメモリを実装します。NUMA システムに対する特別な要件はありません。
- アウトオブバンド管理システムは、VM とネットワークポートを共有する構成にしないでください。社内テストにより、パケット損失が急増して、音声やビデオの品質が低下する可能性があることが判明しています。アウトオブバンド管理は、専用のネットワークポートを使用するように構成するか、または無効にしてください。
- ハイパースレッドが使用できる場合は、それをホストで有効にする必要があります。有効にしない場合、キャパシティが最大で 30% 低下します。
- AMD プロセッサと Intel プロセッサを比較する場合、AMD の「モジュール」の数（リソースを共有する「コア」のペア）と Intel の「コア」の数（「ハイパースレッド」のペアを実行する）とを比べる必要があります。AMD プロセッサのキャパシティは、同等の Intel プロセッサの 60 ～ 70% であることが社内テストにより判明しています。このため、実稼動展開には Intel プロセッサを推奨します。
- 使用する CPU は、Cisco Meeting Server 専用である必要があります。実現方法は以下の通りです。
  - ホストで 1 台の VM のみを実行する。または
  - 特定のコアにホストのすべての VM をピニングし、割り当てたコアの使用権を Cisco Meeting Server のみに与え、さらに、物理コアはハイパーバイザのためにピニングされた VM がない状態にする。
  - 仮想環境におけるユニファイド コミュニケーションの共存要件に従う。[ミーティング（Meeting）] 見出しの下の [Cisco Meeting Server] をクリックします。
- EVC モードが有効な VMWare Hypervisor を使用する場合は、EVC を次のいずれかのモード以上に設定する必要があります。
  “B1”/AMD Opteron™ 第 4 世代
  「L2」/Intel® Nehalem 世代（以前の Intel® Xeon Core™ i7）
  上記にリストしたものより古い CPU との互換性を強制する EVC モードは、SSE 4.2 を無効にするため、サポートされていません。SSE 4.2 は必須です。
- Call Bridge のアクティベーションキーは、メディアのコールに必要です。アクティベーションキーを取得するには、仮想サーバーの MAC アドレスが必要です。ライセンスの詳細については、第 1 章と付録 B を参照してください。

2.2 VMware を介した仕様ベースのサーバーへのインストール

注：仮想化された展開には、Cisco Meeting Server のすべてのリリースに対して、新しい展開用の .ova ファイルと、最新リリースにアップグレードするためのアップグレード画像（.img）があります。

新規インストールの場合はこの項を参照し、アップグレードの場合はリリースノートを参照してください。

- EVC モードが有効な VMWare Hypervisor を使用する場合は、EVC を次のいずれかのモード以上に設定する必要があります。
  “B1”/AMD Opteron™ 第 4 世代
  「L2」/Intel® Nehalem 世代（以前の Intel® Xeon Core™ i7）
  上記にリストしたものより古い CPU との互換性を強制する EVC モードは、SSE 4.2 を無効にするため、サポートされていません。SSE 4.2 は必須です。
- Call Bridge のアクティベーションキーは、メディアのコールに必要です。アクティベーションキーを取得するには、仮想サーバーの MAC アドレスが必要です。ライセンスの詳細については、第 1 章と付録 B を参照してください。

2.3 OVA ファイルから ESXi Web クライアントを使用した Meeting Server の展開

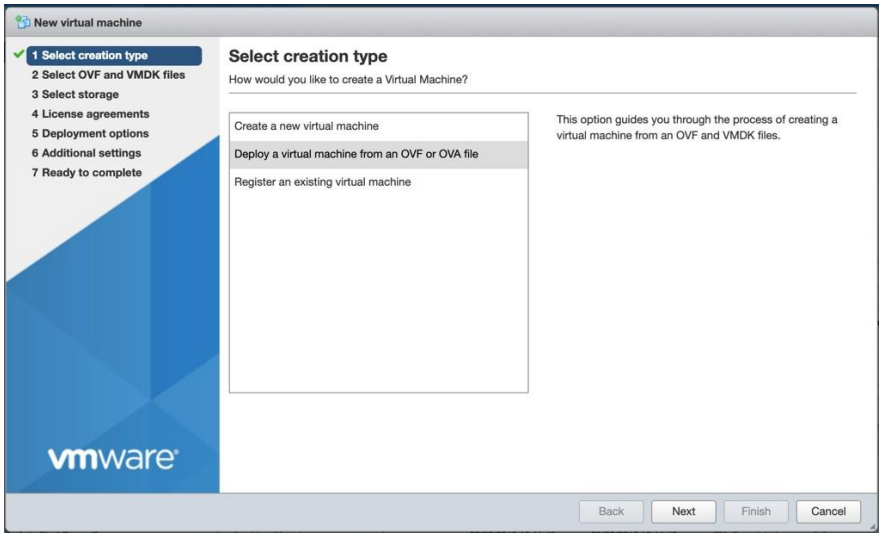
仮想化展開の Cisco Meeting Server のすべてのリリースで、新規導入の場合は .ova ファイルが作成され、最新リリースへのアップグレードの場合はアップグレードイメージ（.img）が作成されます。

新規インストールの場合はこの項を参照し、アップグレードの場合はリリースノートを参照してください。

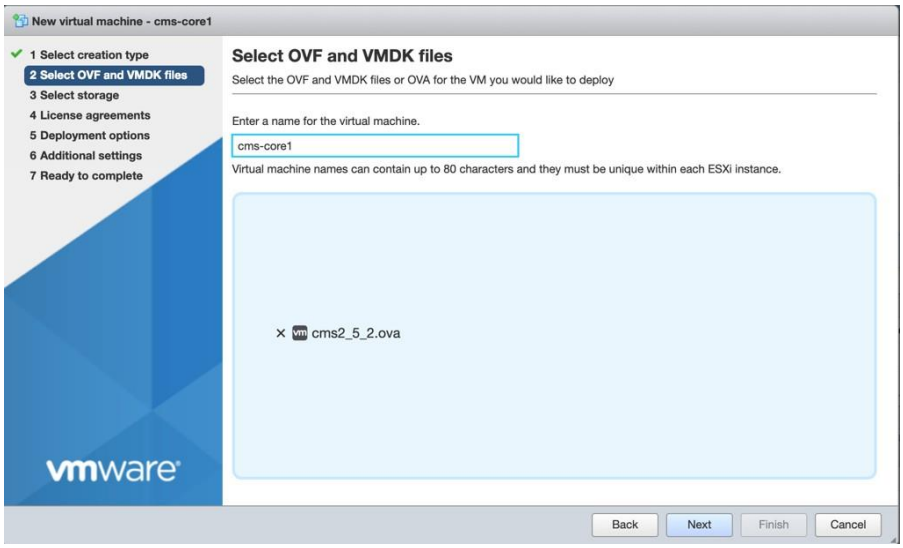
注：バージョン 3.7 以降、ミーティングサーバーは ESXi バージョン 6.0 以下をサポートしません。これらのバージョン（ESXi 6.0/5.5）の .ova ファイルは提供されません。

---

1. 該当する OVA ファイルを シスコの Web サイトからダウンロードします。
2. vSphere クライアントで、左側の [**ナビゲータ**（Navigator）] タブ内のホストに移動し、[VM **の作成/登録**（Create/Register VM）] を選択します。
3. [**作成タイプの選択**（Select creation type）] **で、**[OVF または OVA ファイルから仮想マシンを展開（Deploy a virtual machine from an OVF or OVA file）] **を選択し、**[次へ（Next）] **をクリックします。**

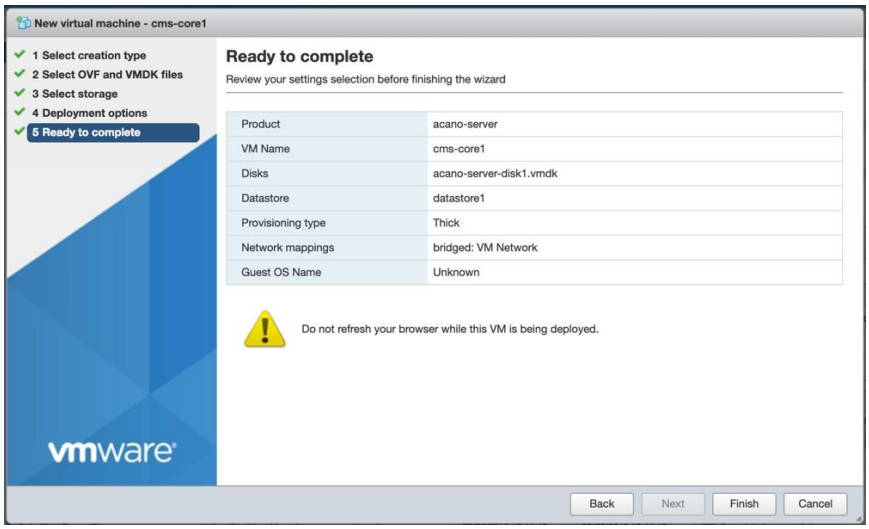


4. 任意の仮想マシン名を入力し、ステップ 1 でダウンロードした .ova ファイルを参照するかドロップして、それを選択します。



5. ウィザードの指示に従います。選択する設定は、次の通りです。
   a. VM の構成ファイルとディスクファイルを格納するデータストアを選択します。
   b. VM の宛て先ポートとなるネットワークマッピングを選択します。
   c. [ディスクプロビジョニング（Disk provisioning）] を [**シック**（Thick）] に設定します。
   d. [展開後に電源をオン（Power on after deployment）] **がオフになっていることを確認します**。
   e. [**完了**（Finish）] をクリックします。

注：仮想ホストのセットアップ方法によっては、一部のウィザード設定の表示または選択ができなくなる場合があります。



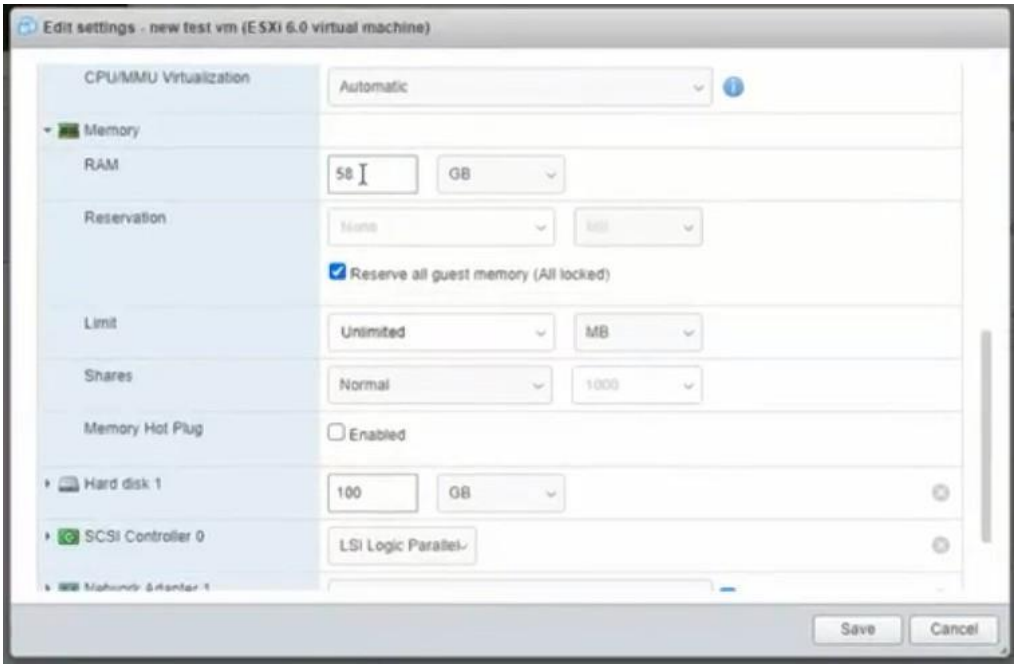
6. 完了すると、新しい Cisco Meeting Server VM が [**仮想マシン**（Virtual Machines）] に表示されます。
7. VM のリストから [Cisco Meeting Server VM] を選択します。
8. [**アクション**（Actions）] ボタンから [**設定を編集**...（Edit Settings...）] を選択します。
   a. [VM **設定**（VM settings）] を編集し、[CPU] を選択します。[CPU **の数**（Number of CPUs）] に希望する数を設定します（4 が最小です）。スケーリングの詳細については、『導入ガイド』を参照してください。VM 設定の要件の詳細については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-meeting-server.html と 付録 D を参照してください。
   b. [ソケットあたりのコア数（Number of Cores per Socket）] **を次のいずれかに設定します**。
      - ハイパースレッディング対応デュアルプロセッサホストでは、[**ソケットあたりのコア数**（Number of Cores per Socket）] を、論理コア数から 2 を差し引いた数に設定します。
      - ハイパースレッディング非対応デュアルプロセッサホストでは、[**ソケットあたりのコア数**（Number of Cores per Socket）] を、論理コア数から 1 を差し引いた数に設定します。
      - シングルプロセッサホストでは、[**ソケットあたりのコア数**（Number of Cores per Socket）] を論理コア数に設定します。

      基盤となるハードウェアをミラーリングするようにソケットの数を設定することを推奨します。

      注：[**管理**（Manage）] > [**設定**（Settings）] > [**プロセッサ**（Processors）] の順に選択すると、論理コアの数が vSphere Web クライアントに表示されます。詳細については、https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.resmgmt.doc/GUID-E09F36DF-E31F-417D-9865-06E351D8AF15.html を参照してください。

      ---

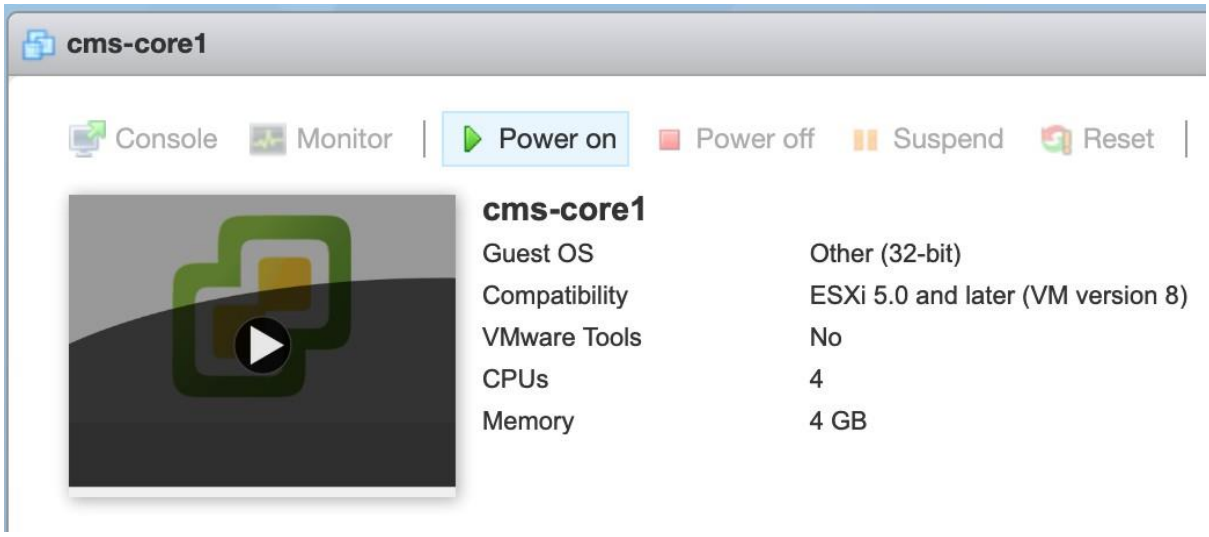
   c. [メモリ（Memory）] をクリックし、RAM が 4 GB 以上に設定されていることを確認します。



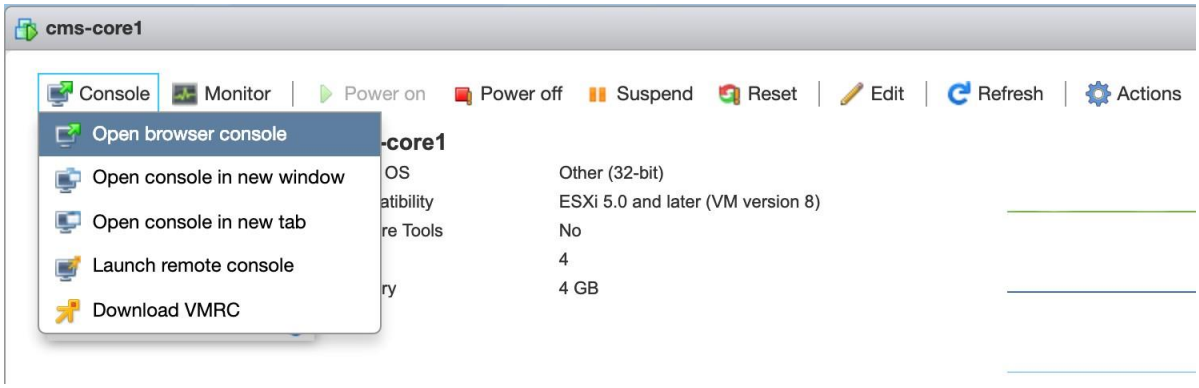
i. M4 および M5v1 バリアントでの ESXi 7.0 ベースのインストールの場合、[**すべてのゲストメモリを予約する（すべてがロックされています）**] チェックボックスをオンにします。

d. ディスク容量を 100 GB に設定します。

9. [**電源オン**（Power On）] をクリックします。



10. [**コンソール**（Console）] タブをクリックして、ブラウザコンソール（または VMware リモートコンソールがインストールされている場合はリモートコンソール）を開きます。



11. ユーザー名「admin」とパスワード「admin」でログインします。パスワード「admin」を変更するように求められます。これで MMP にログインできました。第 3 章に進みます。

2.4 Cisco Meeting Server 1000 のインストールおよび初期構成

2.4.1 はじめる前に

インストールを完了するには以下が必要となります。

- PAK ライセンス番号
- VMware ライセンスのアクティベーションコードまたはお客様提供の VMware ライセンスキー
- ライセンス取得手順を完了するために利用できるインターネットと E メール
- vSphere Client 6.0 を実行する Windows コンピュータまたは vSphere クライアントをコンピュータにインストールする権限
- 次のいずれかのコンソール：
    - VGA コネクタを搭載したモニターと USB キーボード
      または
    - PC、シリアルアダプタ、Cisco シリアルケーブル、端末プログラム、ネットワーク接続、JAVA がインストールされ、有効化されている Internet Explorer または Firefox

2.4.2 タスク 1： 開梱と初期起動

1. Meeting Server、電源コード、コンソールアダプタ、ラックキットを開梱します。
2. Meeting Server を所定の位置に配置するか、または必要に応じてラックマウントを配置します。展開内容に応じて、『Cisco UCS C220 M5 設置ガイド』または『Cisco UCS C220 M4 設置ガイド』を参照してください。
3. Meeting Server の背面の Ethernet1 ポートにイーサネットケーブルを接続し、イーサネットネットワークに接続します。
4. 各電源モジュールに電源コードを接続し、電源に接続します。

5. Meeting Server の前面にある電源ボタンを押します。Meeting Server は初回電源投入後、停止と再起動の動作を 1 回以上自動で行います。
6. 続行するには、コンソールを Meeting Server に接続します。モニタとキーボードを使用することも、またはネットワーク接続を介して仮想コンソールを使用することもできます。次のオプションから選択します。

2.4.2.1 コンソールオプション 1：モニターとキーボード

1. Meeting Server の背面の VGA ポート、または前面のコンソールポートに VGA 接続でモニターを接続します。
2. Meeting Server の背面の USB ポート、または前面のコンソールポートにキーボードを接続します。

   Meeting Server の起動が完了すると VMware コンソール画面が自動的に起動し、モニターに表示されます。

2.4.2.2 コンソールオプション 2：ネットワークを介した仮想コンソール

モニターとキーボードを Meeting Server に接続して使用できない場合は、この方法を使用します。

1. ルータやスイッチに付属している標準的な青色の Cisco RJ-45 to DB-9 ヌルシリアルケーブルを使用して、コンピュータのシリアルポートを、Meeting Server の背面にある「10101」というラベルの付いた RJ-45 ポートに接続します。
2. 端末プログラムを開き、シリアルポート/アダプタの COM ポートを選択し、端末の設定を [115200 ボー（115200 baud）]、[パリティなし（No Parity）]、[8 データビット（8 data bits）]、[1 ストップビット（1 stop bit）]に設定します。
3. 2 番目のイーサネット LAN ポートを、M1 という名前の Meeting Server の背面にある RJ-45 ポートに接続します。1 つのネットワーク接続用だけのリソースがある場合は、イーサネット 1 に接続されている LAN を削除し、一時的に M1 ポートに使用して、仮想コンソールを有効にし、構成後にイーサネット 1 に戻します。仮想コンソールを使用するには、M1 ポートに接続し、M1 ポートを有効な IP アドレスで構成する必要があります。
4. Meeting Server に電源モジュールが接続されていることを確認します。接続されていない場合、CIMC 管理インターフェイスが起動できるように数分間接続します。CIMC を機能させるために Meeting Server の電源を入れる必要はありませんが、電源に接続する必要があります。（CIMC のステータスを示す外部インジケータはありません。）
5. 端末プログラムで Esc キーと 9 キーを同時に押すと、ポートが CIMC に切り替わります。ユーザー名のプロンプトが表示されます。
6. デフォルトのユーザー名とパスワード（ユーザー名：**admin**、パスワード：**password**）を入力します。
7. 初回ログイン時に、任意のパスワードに変更するよう促されます。プロンプトに従って新しいパスワードを設定します。
8. ログインしてから、コマンドプロンプトでコマンド **scope cimc** を入力すると、コマンドプロンプトが変化し、CIMC メニューが表示されます。

9. コマンド **show network detail** を入力すると、サーバーが DHCP を介して取得した現在の IP アドレス（DHCP がネットワーク上で利用可能な場合）を含む、管理イーサネット インターフェイスの現在の構成が表示されます。表示された IPv4 アドレスを書き留めます（DHCP が利用可能な場合）。
10. DHCP が利用可能ではなく、固定 IP を設定する必要がある場合、次のコマンドを使用します。赤字で示された値の例を、お使いのネットワークに適したものに変更してください。（これらのコマンドは、すでに CIMC の有効範囲内にあると仮定します）。

```
scope network
set dns-use-dhcp no
set dhcp-enabled no
set v4-addr 10.1.2.3
set v4-netmask 255.255.255.0
set v4-gateway 10.1.2.1
commit
```

11. **show network detail** と入力して、変更を確認します。完了したら、コマンド **exit** を 2 回入力して CIMC からログアウトします。
12. PC のブラウザに切り替え、構成した IP アドレスか、または CIMC シリアルインターフェイスから取得した IP アドレスを参照します。証明書に関するセキュリティ警告を無視すると、ユーザー名とパスワードのフィールドを含む Cisco ランディングページが表示されます。
13. ユーザー名 **admin** と、CIMC への初回接続時に設定したパスワードを使用してログインします。
14. [**サーバーの概要**（Server Summary）] ページのロード時に、[**アクション**（Actions）] の [KVM **コンソールの起動**（Launch KVM Console）] リンクをクリックします。JAVA 仮想コンソールアプリケーションがロードされます。お使いのオペレーティングシステムやブラウザによっては、セキュリティに警告やダイアログが表示され、確認と同意を求められる場合があります。アプリケーションがロードされ、サーバーに直接接続された様子を再現したモニター画像が表示されます。サーバーの電源がオフの場合、大きな緑色のウィンドウに [**信号なし**（No Signal）] と表示されます。
15. サーバーの電源がオフの場合、[**電源**（Power）] メニューで [**電源オン**（Power On）] を選択してサーバーを起動します。数分後に起動し、VMware コンソール画面が表示されます。

これで、ローカルモニタおよびキーボードを使用して接続する場合と同様に、仮想コンソールを使用できるようになりました。

2.4.3 タスク 2：VMware ネットワーク管理の構成

次の手順を完了するには、モニタまたは仮想コンソールによるサーバーへのコンソール アクセスが必要です。

サーバーの電源が入っていることと、VMware コンソール画面が表示されていることを確認し、F2 を押して構成するか、F12 を押してシャットダウンします。

1. F2 を押して、サーバーを構成します。デフォルトのユーザー名は **root** であり、デフォルトのパスワードはインストールされている ESXi のバージョンによって異なります。つまり、Meeting Server 1000 に ESXi 6.x が同梱されていた場合、デフォルトのパスワードは **password** です。ESXi 7.x が同梱されていた場合、デフォルトのパスワードは **c!SCo123** です。
2. デフォルトのパスワードを変更することをお勧めします。
   a. メニューオプションで矢印キーと Enter キーを使用して、[**パスワードの構成**（Configure Password）] を選択します。
   b. 指示に従って、VMware root アカウントで使用するパスワードを設定します。
      注：VMware では複雑度の高いパスワードが求められます。特殊文字、大文字、英数字を含む強力なパスワードを使用してください。
3. メニューオプションで矢印キーと Enter キーを使用して [**管理ネットワークの構成**（Configure Management Network）] を選択し、次に [IPv4 **の構成**（IPv4 Configuration）] を選択します。
4. 使用するネットワーク構成のオプション（DHCP または固定 IP の割り当て）を選択し、ネットワークに適した IPv4 アドレス、マスク、ゲートウェイを設定します。
   リマインダ：この IP アドレスは VMware Hypervisior を対象としたものであり、Meeting Server アプリケーションを対象としたものではありません。Meeting Server アプリケーションとは異なるアドレスを使用する必要があります。
5. （オプション）Meeting Server アプリケーションから、異なる VLAN 経由で ハイパーバイザの管理機能にアクセスする場合、管理インターフェイスに関連付ける VLAN を構成してください。
6. Escape キーを押してメインメニューに戻り、Escape キーをもう一度押してログアウトします。

   VMware 管理 IP アドレスは、画面の左下に表示されます。

2.4.3.1 仮想コンソールの使用に役立つ情報

- CIMC は Meeting Server の強力なアウトオブバンド管理インターフェイスであり、Meeting Server をラックまたはコンピュータルームに設置する場合に使用が推奨されます。この管理インターフェイスは VMware または Meeting Server アプリケーションでは使用されないため、接続を維持するには、M1 イーサネットポート専用の LAN 接続を確保する必要があります。（Cisco UCS サーバーマニュアルの NIC 共有のオプションもご利用いただけます）。

- 単一のネットワーク接続のみで仮想コンソールを使用し、また同じネットワーク接続を M1 インターフェイスでも一時的に使用していた場合：

    a. インストールを完了するために仮想コンソールを使用する必要はありません。イーサネットケーブルをサーバーの M1 インターフェイスから取り外し、イーサネット 1 ポートに接続し直します。

    b. VMware 管理インターフェイスで DHCP を使用している場合、イーサネットケーブルを接続してからサーバーを再起動し、新しい IP アドレスを取得する必要があります。再起動するには、サーバーの前面にある電源ボタンを短く押すと、サーバーは、自動シャットダウンを開始します（これには数分かかります）。電源がオフになったら、電源ボタンを押して電源を入れ直します。仮想コンソールで使用していたネットワークが遮断されたため、サーバーが取得した IP アドレスは参照できなくなります。サーバーに割り当てられていた IP アドレスを確認するには、DHCP 管理者に問い合わせてください。Ethernet1 インターフェイスの MAC アドレスは、Cisco Meeting Server 1000 の前面の引き出しタブで確認できます。

これで、サーバー背面のイーサネット 1 ポートにイーサネットを接続し、使用中の IP アドレスを VMware 管理ネットワークで確認できるようになりました。

2.4.4 タスク 3：vSphere クライアントを使用した VMware インスタンスの構成

ここでは、VMware インスタンスに接続し、ハイパーバイザの初期構成を完了します。

1. vSphere 6.0 または 6.5 クライアントがまだインストールされておらず、インストールする必要がある場合、次の手順に従います。

    a. ローカルの VMware インスタンスからダウンロードする。

        i. インターネットブラウザを使用して、新しいサーバーの IP アドレスを参照します（例：http://IPaddress）。

        ii. [このホストのインベントリ内のデータベースを参照（Browse database in this host's inventory）] のリンクをクリックします。

        iii. ユーザー名 **root** と、VMware ネットワーク管理設定で構成したパスワードを入力します。

        iv. datastore1\OVA-ISO\VMware\ に移動し、[VMware-viclient...] のリンクをクリックして、クライアントインストーラをダウンロードします。

        v. ダウンロードが完了したら、ファイルを探してプログラムを実行し、vSphere クライアントをインストールします。

2. vSphere クライアントを開き、接続ウィンドウに VMware インスタンスの IP アドレス、ユーザー名 **root**、および VMware ネットワーク管理構成で設定したパスワードを入力します。[**ログイン**（Login）] をクリックして、サーバーに接続します。
3. サーバーに接続する際、SSL 証明書に関する警告が表示されたら、[**無視**（Ignore）] をクリックして続行します。接続時に VMware の評価に関する通知が表示されたら、[OK] をクリックします。

2.4.4.1 VMware NTP の構成

ログが正確に記録されるように、Hypervisor で有効な NTP ソースを構成します。

1. vSphere クライアントで Meeting Server に接続し、左側のパネルにある [Meeting Server] をクリックして選択します。
2. 右側のパネルで [**構成**（Configuration）] タブをクリックし、[**ソフトウェア**（Software）] の [**時間の設定**（Time Configuration）] をクリックします。
3. 表示されたページの右上隅にある [**プロパティ**（Properties）] リンクをクリックします。
4. [**プロパティ**（Properties）] ウィンドウで [NTP **クライアントを有効化**（NTP Client Enabled）] チェックボックスをオンにし、[**オプション**（Options）] ボタンをクリックします。
5. リストの [NTP **設定**（NTP Settings）] をクリックし、[**追加**（Add）] ボタンをクリックして、使用する NTP ソースを追加します。
6. リストから [**一般**（General）] を選択します。
7. サービスを [**ホストによる開始および停止**（Start and Stop with the host）] に変更します。
8. [**開始**（Start）] をクリックしてサービスを開始します。
9. [OK] を 2 回クリックして時間構成ページを閉じます。

2.4.5 タスク 4：VMware ライセンスの取得と有効化

VMware ライセンスを Cisco に注文した場合、ライセンスはアクティベーションコードとして、Cisco から別個のパッケージまたは E メールで送付されます。1 台の Cisco Meeting Server 1000あたり 2 つの 1-CPU ライセンスが必要です。このアクティベーションコードは VMware の公開 Web サイトでライセンスキーに変換する必要があります。このタスクを完了するには、インターネットと E メールを利用する必要があります。

2.4.5.1 VMware アクティベーションキーの有効化

1. インターネットブラウザ（このタスクには Google Chrome 以外のブラウザを使用することを Cisco では推奨しています）を使用して、https://www.vmware.com/oem/code.do?Name=CISCO-RESELL-AC にアクセスします。
2. VMware アカウントを使用してログインします。アカウントをお持ちでない場合、上記の Web ページで指定された手順に従って新しい VMware プロファイルを作成します。
3. ログインしたら、ソフトウェア アクティベーション コードの割り当てに関する組織のポリシーに従い、アクティベーションコードを入力します。手順を完了すると、VMware からライセンスコードが E メールで送信されます。
4. VMware アカウントにライセンスが追加されたら、2 つのシングル CPU ライセンスを組み合わせ、単一のデュアル CPU ライセンスにする必要があります。この手順は myVMware ポータルで行います。これらの手順についての詳細は、https://kb.vmware.com/s/article/2006973 の VMware KB の記事を参照してください。**ヒント**：VMware プロファイルにライセンスを追加した直後にライセンスを組み合わせると、問題が発生する場合があります。その場合は 5 ～ 10 分間待ってからもう一度やり直してください。問題が続く場合、VMware ライセンスサポートに連絡し、ライセンスの組み合わせに関するサポートを依頼してください。
5. 2 つのライセンスを組み合わせて新しいライセンスキーを作成したら、vSphere クライアントを開き、Meeting Server に接続されていない場合は接続して、左側のパネルのツリーにある [Meeting Server] をクリックしてください。
6. 右側のパネルの [**構成**（Configuration）] タブを選択し、[**ソフトウェア**（Software）] を選択してから、[**ライセンスを付与された機能**（Licensed Features）] をクリックします。
7. 現在の評価の詳細が表示されたら、ページ右上隅にある [**編集**（Edit）] リンクをクリックします。
8. 表示されたウィンドウで [**このホストに新しいキーを割り当てる**（Assign a new key to this host）] を選択して [**入力**（Enter）] ボタンをクリックし、ライセンスキーを入力します。
9. [OK] をクリックしてダイアログウィンドウを閉じます。

これで ハイパーバイザの基本的なセットアップが完了しました。

2.4.6 タスク 5：Cisco Meeting Server 1000 コンソールへのアクセス

Meeting Server のインスタンス自体には、固有の IP アドレスに接続するか、または vSphere クライアントコンソール機能を経由して接続することでアクセスできます。

1. vSphere クライアントを開き、Meeting Server の IP アドレス、ユーザー名 **root**、および以前に構成したパスワードを使用してログインします。
2. 左側のパネルから [Meeting Server] を選択し、プラス記号（+）を使用してツリーを展開します。Cisco Meeting Server という名前の仮想マシンと、電源がオンであることを示す緑色の矢印が表示されます。
3. ネットワークに DHCP が存在する場合、Meeting Server の現在の IP アドレスを確認するには、Cisco Meeting Server VM が強調表示された状態で [**概要**（Summary）] タブをクリックします。Meeting Server が取得した IP アドレスが [**全般**（General）] セクションに表示されます。その IP アドレスに ssh でアクセスし、Meeting Server ソフトウェアの構成を続行できます。
4. ネットワークに DHCP が存在しない場合、第 3 章（または『MMP コマンド ライン リファレンスガイド』）の説明に従い、vSphere クライアントの仮想マシンコンソールと Meeting Server MMP コマンド **ipv4** または **ipv6** を使用して、VM に IP アドレスを割り当てる必要があります。
5. コンソールにアクセスするには、Meeting Server VM が選択された状態で vSphere クライアントの［**コンソール**（Console）］タブをクリックします。画面が空白の場合は、ウィンドウ内をクリックして Enter キーを押します。ログインプロンプトが表示されます。
   ヒント：コンソールウィンドウの外部でマウス制御を再度機能させるには、Ctrl キーと Alt キーを同時に押します。
6. ユーザー名「admin」とパスワード「admin」でログインします。パスワード「admin」を変更するように求められます。

注意：パスワードは 6 か月後に期限が切れます。

その他の構成プロセスについては、第 3 章で説明します。

3 構成

3.1 Cisco Meeting Server 管理者アカウントの作成

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

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

注意：パスワードは 6 か月後に期限が切れます。

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

注：管理者レベルの MMP ユーザーアカウントは、Call Bridge の Web 管理インターフェイスへのログインにも使用できます。Web 管理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。

3.2 IPv4 用ネットワーク インターフェイスの設定

注：以下の手順は IPv4 向けですが、IPv6 の場合も同様のコマンドを使用します。詳細な説明については、『MMP コマンドリファレンス』を参照してください。

Cisco Meeting Server の仮想化展開では、最初はネットワーク インターフェイスが 1 つ（インターフェイス「a」）しかありませんが、最大 4 つまでサポートされます（次のセクションを参照してください）。MMP は、仮想化された展開ではインターフェイス上で実行されます。

1. ネットワーク インターフェイスの速度、デュプレックス、および自動ネゴシエーションの各パラメータを構成するには、 **`iface`** MMP コマンドを使用します。たとえば、「a」インターフェイスに現在の構成を表示するには、MMP で次のコマンドを入力します。

   `iface a`

   a. コマンド **`iface (a|b|c|d) <speed> (full|on|off)`** を使用して、ネットワーク インターフェイスの速度（Mbps）、デュプレックス、および自動ネゴシエーションの各パラメータを設定します。たとえば、インターフェイスを 1 GE、全二重に設定するには、次のようにします。

      `iface a 1000 full`

   b. 自動ネゴシエーションをオンまたはオフにするには、コマンド **`iface a autoneg`** を使用します。**`<on|off>`**. 以下にその例を示します。

```
iface a autoneg on
```

注：ネットワーク インターフェイスは、特別な理由がある場合を除き、自動ネゴシエーションを [オン（On）] に設定することを推奨します。

2. 「a」インターフェイスは、DHCP を使用するように初期構成されています。既存の構成を表示するには、次のように入力します。

```
ipv4 a
```

   a. DHCP IP 割り当てを使用する場合は、IP の構成をこれ以上追加する必要はないため、手順 3 に進みます。
   b. 静的 IP アドレス割り当てを使用する場合は、次のようにします。

      ipv4 add コマンドを使用し、特定のサブネットマスクとデフォルトゲートウェイを指定して、静的 IP アドレスをインターフェイスに追加します。

      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 10.1.2.4 をインターフェイスに追加するには、次のように入力します。

```
ipv4 a add 10.1.2.4/16 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 <address>
```

3. ドメインネームシステム（DNS）構成の設定

   Meeting Server では、その多くのアクティビティに SRV レコードのルックアップなど DNS ルックアップを行う必要があります。また、Meeting Server は簡素化された展開に必須です。forwardzone の値にピリオド「.」を使用して、ネットワークのデフォルトの DNS リゾルバを指すように Meeting Server を設定することを推奨します。

   a. DNS 構成を出力するには、次のように入力します。

```
dns
```

   b. アプリケーション DNS サーバーを設定するには、次のコマンドを使用します。

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

      注：正引きゾーンとは、ドメイン名とサーバーアドレスから構成された 1 つのペアのことです。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ーにクエリできます。ロードバランシングとフェイルオーバーを可能にするには、特定のドメイン名に対して複数のサーバーを指定します。一般的にはドメイン名として「.」を指定します。これは DNS 階層のルートを表し、すべてのドメイン名と一致します。

      例：

```
dns add forwardzone . 10.1.1.33
```

   c. DNS エントリを削除する必要がある場合は、次のコマンドを使用します。

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

      例：

```
dns del forwardzone. 10.1.1.33
```

3.3 ネットワーク インターフェイスの追加

Cisco Meeting Server 仮想化展開は、最大 4 つのインターフェイス（a、b、c、d）をサポートします。

必要に応じて、VMware に 2 つ目のネットワーク インターフェイスを追加できます。ただし、Cisco Meeting Server の任意の 2 つのインターフェイスを同じサブネットに入れることはできません。

1. vSphere クライアントで、[**ホストおよびクラスタ（Hosts and Clusters）**] リストから VM を見つけます
2. [**仮想マシンの設定を編集（Edit Virtual Machine Settings）**] を選択します。
3. タイプ VMXNET3 のネットワークアダプタを追加します。

注：VMXNET3 ではないイーサネットアダプタを選択すると、ネットワーク接続の問題が発生してライセンスが無効になることがあります。

注：イーサネットアダプタの追加または変更の詳細については、VMware Web ページの「仮想ネットワークアダプタの追加と変更」を参照してください。

---

4. 新しいアダプタを追加したら、次のコマンドを使用して、MMP でインターフェイスを有効にします。例：**`ipv4 b enable`**
5. アドレスとゲートウェイを手動で追加できるようにするため、または、アドレスとゲートウェイが、インターフェイスが有効になっている場合に DHCP によって自動的にピックアップされるようにするため、VM を再起動します。

3.4 Call Bridge の構成

Call Bridge は、SIP 呼制御デバイスおよび Lync Front End（FE）サーバーとの TLS 接続を確立するために使用するキーと証明書のペアを必要とします。Lync を使用する場合、この証明書は Lync FE サーバーが信頼できるものである必要があります。

コマンド **`callbridge listen <interface>`** を使用して、リスニングインターフェイス（A、B、C、D から選択）を構成できます。デフォルトでは、Call Bridge はどのインターフェイス上でもリッスンしていません。

1. 『証明書ガイドライン』の説明に従って、証明書を作成およびアップロードします。
2. MMP にサインインして、Call Bridge がインターフェイス A 上でリッスンするように構成します。

```
callbridge listen a
```

注：Call Bridge は、別の IP アドレスに NAT 変換されていないネットワーク インターフェイスでリスニングしている必要があります。これは、Call Bridge がリモートサイトと通信するときに、SIP メッセージのインターフェイスで構成されているものと同一の IP を転送する必要があるためです。

---

3. 以下のようなコマンドを使用して、Call Bridge が証明書を使用するように構成し、たとえば、Lync FE サーバーと Call Bridge との間で TLS 接続を確立できるようにします。

   callbridge certs callbridge.key callbridge.crt

   コマンド全体と、CA により提供された証明書バンドルの使用については、『証明書のガイドライン』で説明されています。

4. 変更を適用するには、Call Bridge インターフェイスを再起動します。

   callbridge restart

3.5 Web 管理インターフェイスを設定する

Web 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 Web インターフェイスでルーティングされます。

Web 管理インターフェイスの構成には、秘密キー/証明書ペアを作成し（セクション 3.5.1 を参照）、秘密キー/証明書ペアを MMP にアップロードする必要があります（セクション 3.5.2 を参照）。

Web 管理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。

3.5.1 Web 管理インターフェイスの証明書を作成する

Web 管理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。実稼働環境向けの『証明書ガイドライン』で説明されている手順に従ってください。この項では、ラボ環境において自己署名証明書でテストを行う方法を示しています。

注：Web 管理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 管理インターフェイスの証明書をアップロードしておく必要があります。

下記の情報は、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 3.5.2 項に進みます。

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

pki selfsigned <key/cert basename>

ここで、**<key/cert basename>** は、生成されるキーと証明書を識別します。

たとえば、「pki selfsigned webadmin」は、webadmin.key および webadmin.crt（自己署名済み）を作成します。自己署名証明書を実稼動環境で使用することは推奨されていません。

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

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

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

   値は次のとおりです。

   <key/cert basename> は、新しいキーと証明書署名リクエスト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。Common Name には DNS A レコードで定義した FQDN を使用します。その FQDN を使用しなかった場合は、ブラウザ証明書のエラーが発生します。
   - OU：組織単位（Organizational Unit）
   - 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. 次のいずれかに証明書署名要求を送信します。

   - リクエスト送信者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
     たとえば、Verisign など認証局（CA）宛て。
   - ローカルまたは組織の認証局宛て。たとえば、Active Directory 証明書サービスの役割がインストールされている Active Directory サーバーなど（ 付録 F を参照してください）。

注：Cisco Meeting Server に署名付き証明書と秘密キーを転送する前に、証明書ファイルを確認してください。CA が証明書チェーンを発行した場合は、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 行と 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 拡張子を付けて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ように順に並べる必要があります。

3.5.2 HTTPS アクセス用 Web 管理インターフェイスを設定する

注：Web 管理インターフェイスは、インターフェイス A でポート 443 を使用するように自動的にセットアップされます。ただし、Web Bridge でも TCP ポート 443 は使用されます。Web 管理インターフェイスと Web Bridge の両方が同じインターフェイスを使用する場合は、Web のポートを変更する必要があります。445 などの非標準ポートへの管理インターフェイスは、MMP コマンド **webadmin listen <interface> <port>** を使用します。

1. MMP への SSH 接続を確立し、サインインします。
2. Web 管理インターフェイスの秘密キー/証明書ペアおよび証明書バンドル（オプション）をアップロードするには、SFTP を使用します。
3. 証明書を割り当てる前に、Web 管理インターフェイスを無効にします。

   webadmin disable
4. 手順 2 でアップロードした秘密キー/証明書ペアを、次のコマンドを使用して割り当てます。

   webadmin certs <keyfile> <certificatefile> [<cert-bundle>]

   ここで、 **keyfile** と **certificatefile** は、それぞれ対応する秘密キーと証明書のファイル名です。CA によって証明書バンドルが提供された場合は、バンドルも個別のファイルとして証明書に含めます。以下にその例を示します。

   webadmin certs webadmin.key webadmin.crt webadminbundle.crt
5. Web 管理インターフェイスを再起動します。

   webadmin restart
6. Web 管理インターフェイスを有効にします。

   webadmin enable

以下にその例を示します。

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

Web 管理インターフェイスにアクセスできるかをテストします。つまり、https://cms-server.mycompany.com（または IP アドレス）と同等のものをブラウザに入力し、前の方法で作成した MMP ユーザーアカウントを使用してログインします。

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

3.6 スケジューラの Email サーバーの構成

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

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

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

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

スケジューラは、次のタイプの電子メール設定をサポートしています。

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

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

バージョン 3.4 移行では、ミーティングの招待をすべての参加者に共通の E メールアドレスから送信できます。MMP コマンド **scheduler email common-address <address@mail.domain>「<Display name>」** は、共通の E メールアドレスと表示名を Meeting Server に構成します。スケジューラは、共通の電子メールアドレスから参加者にミーティングの招待を送信します。

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

注：共通の E メールアドレスが設定されていない場合、SMTP サーバーによる認証には、MMP コマンド **scheduler email username** を使用して E メールアドレスを設定する必要があります。**<smtp user-name>**。MMP で設定されたこのアカウントには、Web アプリケーションユーザーの代わりに E 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、E メールアドレスの他に主催者の名前を表示名として含めることもできます。Web アプリを使用して会議がスケジュールされると、Web アプリケーションは、会議をスケジュールするユーザーの名前を主催者の表示名としてスケジューラに送信します。スケジューラ API にオプションのパラメータ **organizeDisplayName** を含めることによって、任意の名前を表示名として設定できます。

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

3.6.1 SMTP を使用してスケジューラ E メールを設定する

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

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable
2. E メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   例：

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```
3. スケジューラを有効にします。

   scheduler enable

3.6.2 認証ログイン設定を使用したスケジューラ SMTP

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

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable
2. E メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

例：

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

3. 認証ログインオプションを有効にします。

```
scheduler email auth enable
```

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

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

5. スケジューラを有効にします。

```
scheduler enable
```

3.6.3 スケジューラの SMTP および STARTTLS 設定

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

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

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

```
scheduler disable
```

2. E メールサーバーとポートを設定します。

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

   例：

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

3. STARTTLS オプションを有効にします。

```
scheduler email starttls enable
```

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

```
scheduler email trust <cert or bundle name>
```

   設定される証明書は有効な証明書である必要があります。たとえば、共通名または SAN 名が電子メールサーバーの FQDN と一致している必要があり、証明書が期限切れ

になっていない必要があります。同様に、証明書が認証局によって発行されている場合、またはチェーンに中間証明書がある場合は、ルート CA 証明書を設定するか、ルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

5. スケジューラコンポーネントを有効にします。

   scheduler enable

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

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

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

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable

2. 指定された E メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   例：

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

3. 認証ログインオプションを有効にします。

   scheduler email auth enable

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

   ```
   scheduler email username test@test.com

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

5. STARTTLS オプションを有効にします。

   scheduler email starttls enable

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

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

7. スケジューラコンポーネントを有効にします。

   scheduler enable

3.6.5 スケジューラ SMTPS 設定

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

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

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable

2. 指定された E メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>
   例：

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

3. E メールプロトコルを SMTPS に設定します。

   scheduler email protcol smtps

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

   scheduler email trust <cert or bundle name>
   設定される証明書は有効な証明書である必要があります。たとえば、共通名または SAN 名が E メールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。同様に、証明書が認証局によって発行されている場合、またはチェーンに中間証明書がある場合は、ルート CA 証明書を設定するか、代わりに 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構成します。

5. スケジューラコンポーネントを有効にして、SMTPS を使用する E メール設定を完了します。

   scheduler enable

3.6.6 認証ログイン設定を使用したスケジューラ SMTPS

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

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

1. 現在実行中の場合は、スケジューラコンポーネントを無効にします。

   scheduler disable

2. 指定された E メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   例：

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

3. 認証ログインオプションを有効にします。

   scheduler email auth enable

4. 認証に使用されるユーザーのユーザー名を設定します。

   scheduler email username <username>

   パスワードを入力します。

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

5. E メールプロトコルを SMTPS に設定します。

   scheduler email protcol smtps

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

   scheduler email trust <cert or bundle name>

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

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

```
scheduler enable
```

3.6.7 スケジューラの詳細ロギング

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

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

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

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

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

例：

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

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

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

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

付録 A Cisco Meeting Server 1000 の技術仕様

A.1 物理仕様：

シャーシ：Cisco UCS C220 M5 ラックサーバー または Cisco UCS C220 M4 ラックサーバー

重さ：18+ kg（40 ポンド）
サイズ：高さ 1RU

ラック要件：19 インチ標準ラック

A.2 環境仕様

動作温度：5 ～ 35°C（41 ～ 95°F）
動作する湿度 ：5 ～ 93%（結露しないこと）

A.3 電気的仕様

該当する『Cisco UCS C220 M4 Server 設置およびサービスガイド』の「電源仕様」を参照してください。

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 4：Meeting Server プラットフォームのコールキャパシティ

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

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

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

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

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

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

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

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

付録 B シスコライセンス

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

B.1 スマートライセンス

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

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

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

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

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

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

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

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

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

B.2 スマートアカウントとバーチャル アカウントの情報

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

- 単一の Meeting Management に対する Meeting Server クラスタを、それぞれ 1 つのユーザー定義のスマート バーチャル アカウントにリンクする必要があります。
- 各バーチャルアカウントは、スマートライセンスを処理するように設定された 単一の Meeting Management サーバーにのみ接続できます。

- 1 つの Meeting Management のみをスマートに構成します。スマートライセンス用に重複する 2 つ目の Meeting Management を構成**しない**ことを推奨します。ライセンス使用数の二重カウントが発生します。
- PMP Plus、SMP Plus、録画/ストリーミングのライセンスは、単一の Meeting Management インスタンスと単一のバーチャルアカウント内でのスマートライセンスを使用している複数のクラスタで共有できます。
- ACU ライセンスは、Meeting Management ライセンスダッシュボードでは使用できません。ACU は 3.0 以降ではサポートされていません。

B.3 Meeting Server のスマートライセンスの仕組み：概要

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

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

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

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

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

   ---

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

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

注：機能ライセンスはいずれも有効期限が最大で 90 日後までとなります。

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

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

      注：Meeting Server が Meeting Management に接続して 90 日間の使用状況データを送信しなかった場合、Meeting Server のライセンスは更新されず、期限切れになります。ライセンスの有効期限が切れた場合の強制アクションの詳細については、セクション B.4 を参照してください。

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

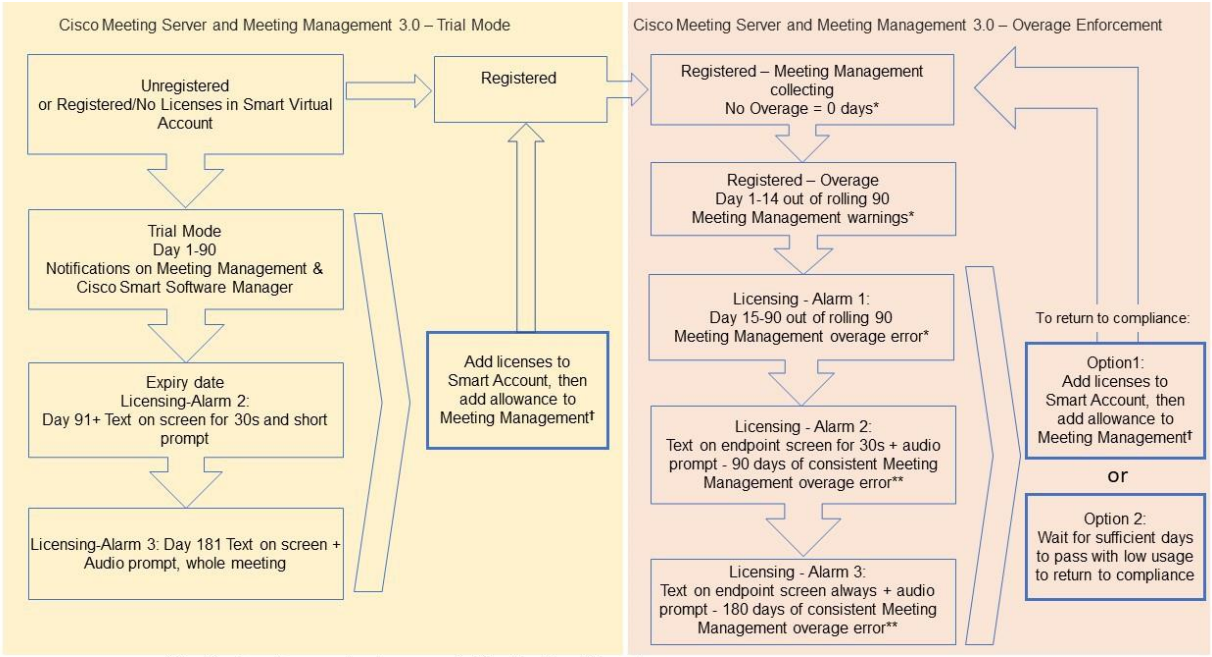
   b. 遵守状態でなかったのが過去 90 日間のうち 15 日未満であることを Meeting Management が特定した場合、これを許容して Meeting Server の有効期限をその時点から 90 日後に再設定します。管理者に、ライセンス不足を通知するビジュアル警告が表示されます。

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

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

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

図 2：Cisco Meeting Server と Cisco Meeting Management スマート ライセンスの強制フロー



* 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.4 ライセンス機能の有効期限切れによる強制アクション

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

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

機能ライセンスが期限切れになると、表 6 に示したアクションが発生します。

表 6：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	期限切れの場合：すべての参加者およびすべてのミーティングに対し、ミーティング参加時にビジュアルなテキスト メッセージが画面に 30 秒間表示され、オーディオによる指示が再生されます。（アラーム レベル 2）
callBridgeNoEncryption	90 日以上前に期限切れとなりライセンスが存在しない場合：それ以前と同様ですが、メッセージは永続的に表示されます。「Your deployment is out of licensing compliance, please contact your administrator（ライセンスが遵守されていません。管理者に連絡してください）」というオーディオによる指示が再生されます。（アラームレベル 3）。 ただし、暗号化された呼び出しは、ライセンスのない状態では処理されません。 注：前述のアクションを回避するために必要なのは callBridge または callBridgeNoEncryption のみです。
PMP/SMP	
customizations	期限切れであるかライセンスが存在しない場合、カスタマイズ機能はミーティング中にアクティブになりません。
録音	期限切れまたはライセンスが存在しない場合、（サードパーティのレコーダーであるかどうかにかかわらず）新規の録画を開始できなくなります。 このライセンスは録画とストリーミングに該当するため、ストリーミングにも同じ制限が適用されます。

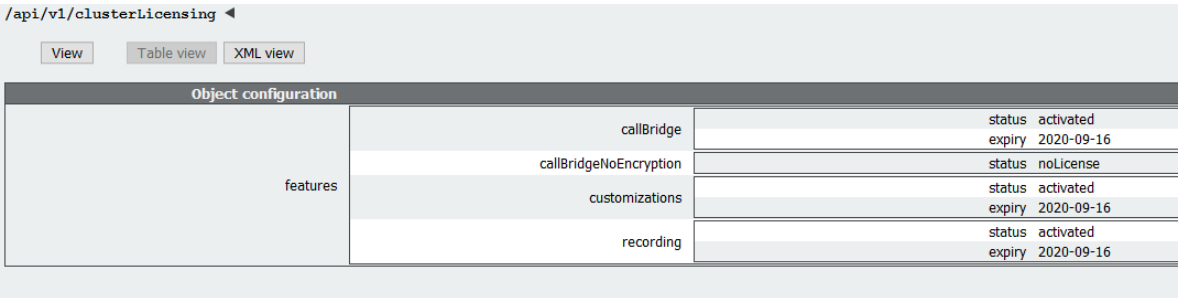
アラーム 2 と 3 をオフにするには、単純にライセンスをスマートアカウントに追加します。

B.5 ライセンス情報の取得方法（スマートライセンス）

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

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

図 3：clusterLicensing API：ライセンスステータス



B.6 Cisco Meeting Server ライセンス

次の機能にはライセンスが必要です。

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

機能ライセンスの他にユーザ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は 2 種類あります。

- PMP Plus
- SMP Plus

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

ユーザー のライセンスについては、セクション B.8 を参照してください。

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

B.6.1 Personal Multiparty Plus ライセンス

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

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

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

B.6.2 Shared Multiparty Plus ライセンス

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

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

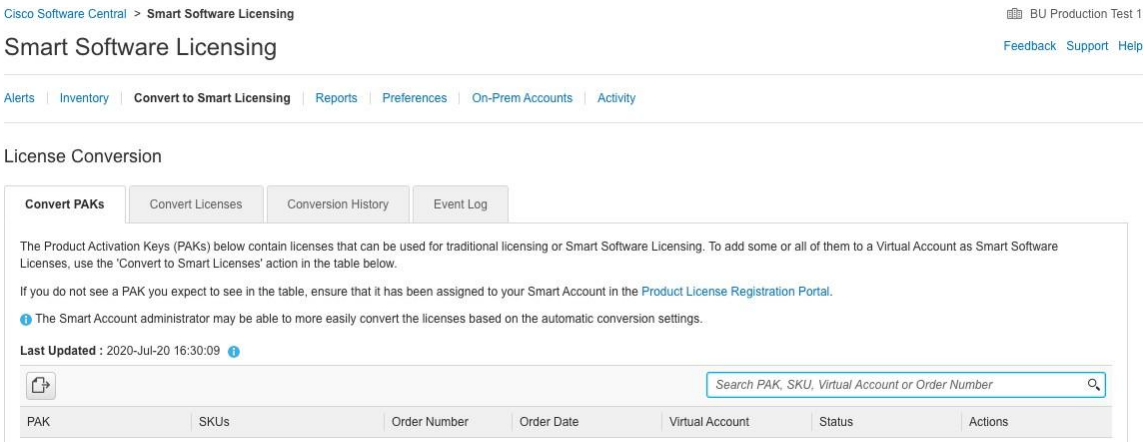
B.7 スマートライセンス登録プロセス

スマートライセンスを有効にするには、以下の手順を実行します。

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

バーチャル アカウント内でライセンスが表示されない場合、[**ライセンスの変換**（Convert Licenses）] タブを使用して PAK を検索します。その後、図 4 のとおりに [**ライセンスの変換**（Convert Licenses）] を選択します。（ライセンスが見当たらない場合は、licensing@cisco.com に連絡してケースを開始してください）。

図 4：スマートライセンスのライセンス転換



B.8 ユーザーに Personal Multiparty ライセンスを割り当てる

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

B.8.1 特定のユーザーにライセンスがあるかを判断する方法：

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

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

B.9 Cisco Multiparty ライセンスの割り当て方法

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

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

B.10 Cisco Multiparty ライセンスの使用状況の判断

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

以下の表 7 には、Multiparty ライセンスの使用を決定するために使用できる API オブジェクトとパラメータをリストしています。

表 7：Multiparty ライセンスの使用状況に関連するオブジェクトとパラメータ

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

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

B.11 SMP Plus ライセンスの使用率を計算する

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

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

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

注：ポイントツーポイントコールは次のように定義されます。

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

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

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

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

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

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

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

B.13 ライセンスレポート

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

B.14 レガシーライセンスファイル方式

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

B.14.1 ライセンスファイルの取得および入力

Cisco Meeting Server のすべての仮想化展開にライセンスファイルが必要です。ライセンスファイルは、仮想サーバーの MAC アドレス用です。

注：Cisco Meeting Server 2.0 を既存の展開にアップロードする場合は、Acano サーバー用に発行された「acano.lic」ライセンスを引き続き使用できます。ただし、展開を拡張する場合は、Cisco ライセンスを購入する必要があります。

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

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

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

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

1. Meeting Server の MAC アドレスを取得するには、サーバーの MMP にログインして MMP コマンド **`iface a`** を入力します。

   注：これは、VM の MAC アドレスであり、VM がインストールされているサーバープラットフォームの MAC アドレスではありません。

2. シスコライセンス登録ポータルを開いて、PAK コードと Meeting Server の MAC アドレスを登録します。

3. PAK に R-CMS-K9 アクティベーション ライセンスが割り当てられていない場合は、機能ライセンスの他にこの PAK が必要です。
4. ライセンスポータルでは、ライセンスファイルの圧縮コピーが電子メールで送信されます。zip ファイルを解凍し、解凍後の xxxxx.lic ファイルの名前を **cms.lic** に変更します。
5. SFTP クライアントを使用して Meeting Server にログインし、Meeting Server ファイルシステムに **cms.lic** ファイルをコピーします。
6. MMP コマンド **callbridge restart** を使用して Call Bridge を再起動します。
7. Call Bridge を再起動した後、次の 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
   有効化された機能と有効期限が表示されます。

B.14.1.2 ライセンスファイルの転送後

ライセンスを適用するには、Call Bridge を再起動する必要があります。ただし、再起動する前に、Call Bridge 証明書と、Call Bridge がリッスンするポートを構成する必要があります。

ライセンスファイルが適用されると、Web 管理インターフェイスにサインインしたときに [Call Bridge をアクティブ化する必要があります（Call Bridge requires activation）] というバナーは表示されなくなります。

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

注：クラスタ化する複数のサーバー（単一の統合サーバー、または分割コアサーバーまたは Edge サーバー）を展開する場合、従来のライセンス方法を使用している場合の詳細については、『拡張性と復元力の導入ガイド』の付録*「クラスタ内での Call Bridge ライセンスの共有」*を参照してください。 それ以外の場合は、「スマートライセンス」のセクションを参照してください。スマート アカウント内で複数のクラスタに Meeting Server ライセンス 1 セットを与え、3.0 以前のように個々の Meeting Server インスタンスにライセンスファイルをロードする必要がなくなりました。

これで、Cisco Meeting Server を構成する準備が整いました。導入に適したガイドについては、以下およびこちらを参照してください。

- 単一統合型サーバー導入ガイド：単一のホストサーバーに展開する場合
- 単一分割サーバー導入ガイド：分割コア/エッジ展開環境に導入する場合
- 拡張性と復元力ガイド：クラスタ化する複数サーバー（単一結合サーバー、あるいは分割のコアサーバーまたはエッジサーバー）を展開する場合。

Cisco Meeting Server をシャットダウンするときには、vSphere の電源ボタンを使用せずに、必ず **shutdown** コマンドを使用してください。

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

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

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

1. Meeting Server の MAC アドレスを取得するには、サーバーの MMP にログインして MMP コマンド **`iface a`** を入力します。

   注：これは、VM の MAC アドレスであり、VM がインストールされているサーバープラットフォームの MAC アドレスではありません。

   ---

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

付録 C ブランディング

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

- サインイン バックグラウンド イメージの Web アプリ、サインインロゴ、サインインロゴアイコンの下のテキスト、セルフビューペインのカスタム仮想バックグラウンド画像、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、すべてのオーディオによる指示またはメッセージ
- ミーティングへの招待メールのテキスト。

1 つのリソースセット（Web アプリケーションの 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、IVR のレベルで割り当てることができます。

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

付録 D VM のサイジング

Cisco Meeting Server は、最大限の柔軟性を提供するように設計されています。高い拡張性により、Cisco Meeting Server 2000、Cisco Meeting Server 1000、VM 展開の「組み合わせと照合」が可能になります。たとえば、VM をエッジサーバーとして、Cisco Meeting Server 2000 と Cisco Meeting Server 1000 をコアとして使用して拡張性の高い分散アーキテクチャを実現したり、VM 展開内のすべてのコンポーネントを単一の標準化されたサーバーに配置したりできます。

また、Cisco Meeting Server ソフトウェアが稼働可能なさまざまな標準サーバーおよび仕様においても最大限の柔軟性を実現できます。付録 E では、最も一般的な仮想化テクノロジーの 1 つである VMware について詳しく説明しています。Cisco Meeting Server ソフトウェアは、ポータブルで堅牢なフォームファクタを必要とするアプリケーション向けなど、より特化したサーバー上でも有効に動作します。

Cisco Meeting Server 全体または Cisco Meeting Server の個別のコンポーネントを、仮想マシン（VM）の展開で実行できます。例：

- 展開をテストする目的の場合は、すべてのコンポーネントを 1 台の VM で実行できます（図 5 を参照）。

  注：実稼働のネットワークでは、レコーダーコンポーネントとストリーマコンポーネントは、会議をホストしているサーバーとは異なる Meeting Server 上で有効にする必要があります。

- 単一の VM は、TURN サーバーとともにエッジコンポーネントとして Web Bridge を実行し、Call Bridge を実行するコアネットワークで Cisco Meeting Server 2000 または Cisco Meeting Server 1000 に接続し、他のコアコンポーネントを実行している別の VM を実行できます。

  注：Cisco Expressway をネットワークのエッジで使用する場合、VM の TURN サーバーコンポーネントを有効にする必要はなく、Web Bridge は会議をホストする Call Bridge のある Meeting Server に配置する必要があります。

- 1 つの VM がエッジコンポーネントを実行し、Call Bridge とデータベースを実行している 2 番目の VM に接続し、3 番目の VM は他のコアコンポーネントを実行します。

図 5 は、1 つのサーバーで有効になっている Cisco Meeting Server ソフトウェアコンポーネントを示しています。図 6 は、エッジサーバーとコアサーバーに展開されている Cisco Meeting Server ソフトウェアコンポーネントを示しています。

図 5：1 つのサーバーで有効な Cisco Meeting Server ソフトウェアコンポーネント

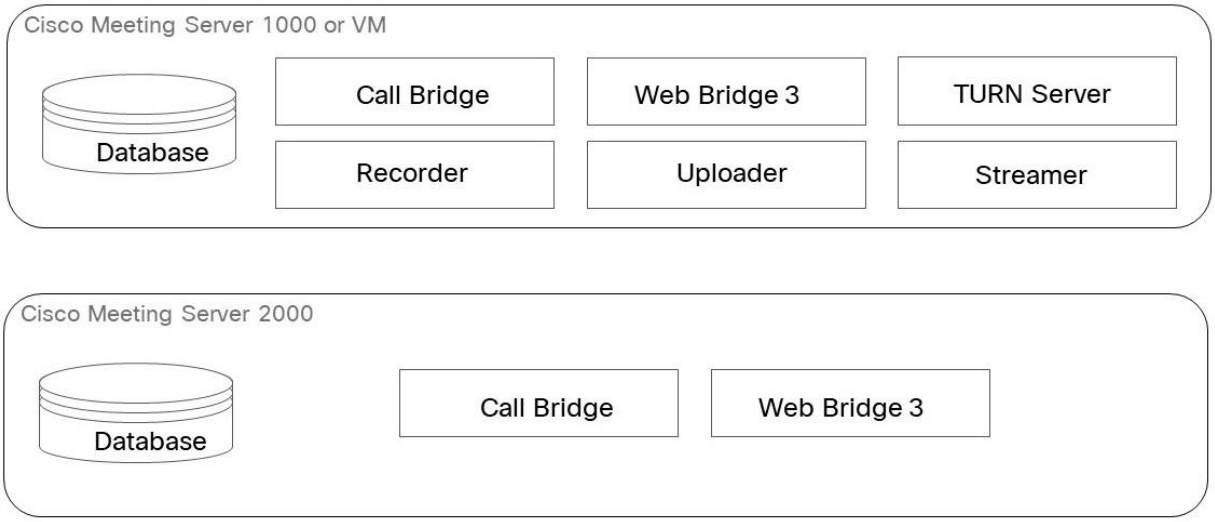
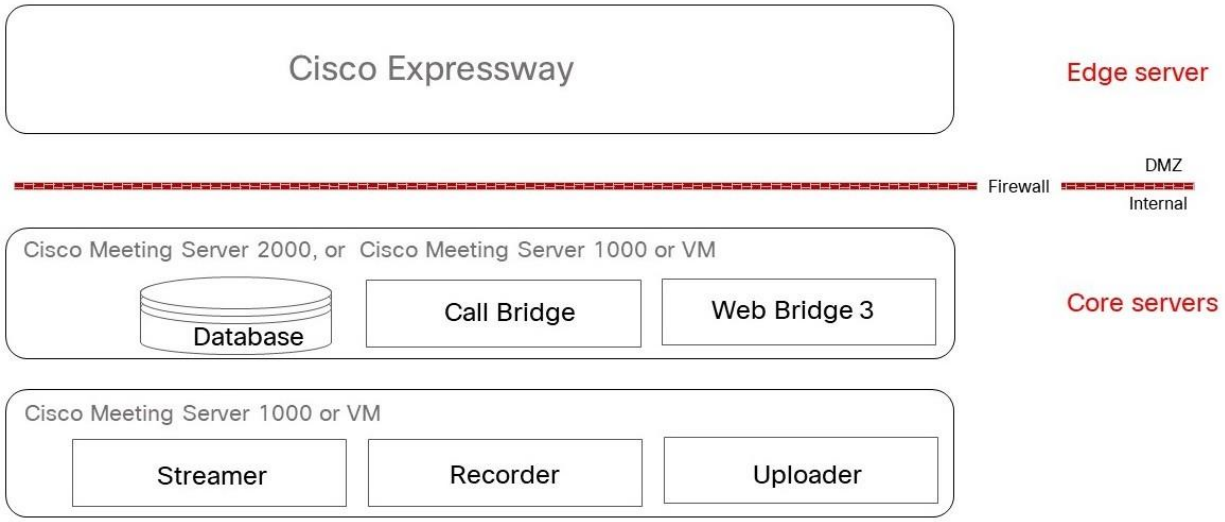


図 6：TURN サーバーとエッジが Web Bridge 3 である Cisco Meeting Server ソフトウェアコンポーネント



1 つ以上の Cisco Meeting Server コンポーネントを実行するように VM を構成する場合、ホスト全体をその VM 専用にすることを推奨します。これにより、リアルタイムのメディアアプリケーションの最適なパフォーマンスと、質の高いエンドユーザー体験が実現できます。VM のサイジングは、使用するコンポーネントによって異なります。

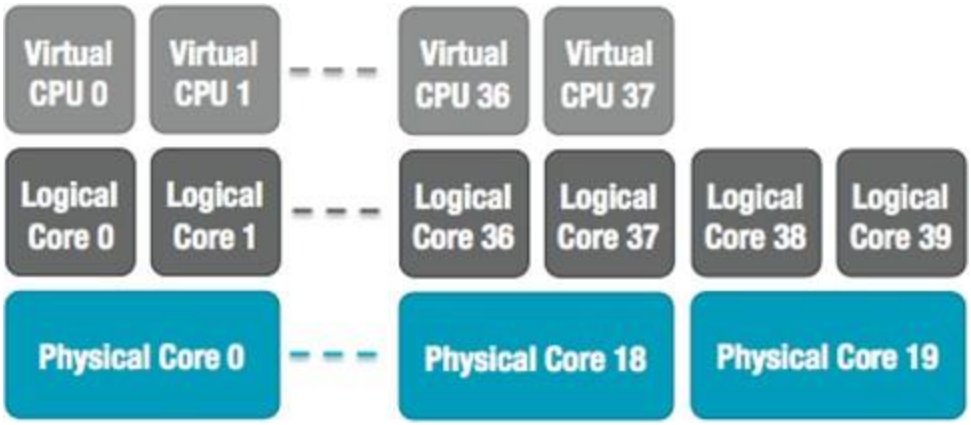
D.1 Call Bridge VM

Call Bridge では、Cisco Meeting Server 用にメディア トランスコーディングが実行されます。要件は全コンポーネントの中で最も高くなっています。

ハイパースレッドを有効にした場合、2.5 GHz で動作する Intel Xeon 2600 シリーズ（またはそれ以降）の CPU の各物理コアは、約 2.5 の 720p30 H.264 コールレッグを処理できます。キャパシティは CPU コア数と周波数に比例するので、20 個の物理コアを備えた 2 ソケットの E5- 2680v2 システムでは、50 の 720p30 H.264 コールレッグを処理できることになります。

VM は、ホストの物理コアのうち 1 個を除きすべて使用するように構成する必要があります。ハイパースレッドを有効にすると、物理コアの 2 倍の数の論理コアが利用できます。つまり上記の E5-2680v2 デュアル搭載システムでは仮想 CPU の数は 40 個になり、そのうちの 38 個を VM に割り当てる必要があります。基盤となるハードウェアをミラーリングするようにソケットの数を設定することを推奨します。

図 7：E5-2680v2 デュアル搭載のホストに対する仮想 CPU コアの割り当て



Cisco Meeting Server VM の仮想 CPU の数を誤って設定したか、または VM 間で CPU リソースに対する競合が発生したために、ホストのオーバーサブスクリプションが発生すると、スケジュールの遅延やメディア品質の低下が生じます。物理コアの数を超えて vCPU の数を割り当てることは、CPU リソースのコミットメントを超えています。この CPU コミットメント超過により、VM の CPU 使用率統計が歪み、CPU 待受時間が増加します。CPU のコミットメントは、ワークロードに固有の検討事項であるため、より一般的な解決策と競合する可能性があります。この vCPU コミットメントは Cisco Meeting Server が意図しているもので、ホストからピーク時のパフォーマンスを抽出する経験的テストの結果です。上記の推奨事項に従って正しく構成された Cisco Meeting Server VM は、キャパシティを超えた場合、フレームレートまたは解像度、あるいはその両方が段階的に低下します。

基になる物理 CPU コアごとに 1 GB の RAM を VM に割り当て、最小 4 GB の RAM を割り当てる必要があります。上記のシステムの場合、19 個の物理 CPU コアを使用しているので、VM には 19 GB を割り当てて構成する必要があります。

Call Bridge VM の RAM 要件は vCPU あたり 1GB で、最小 4 GB の RAM ですが、推奨される最小は 8 GB です。75,000 の cospace を超えて展開する場合に cospace の規模を拡大するには、すべての Call Bridge とデータベース VM に対して、100,000 の cospace あたり 1GB の RAM を追加する必要があります。上記の Call Bridge VM の例では、50 HD のポートと 275,000 の cospaces をサポートするには、50 HD ポートをサポートするには 38 GB の RAM と、75,000 を超える 200,000 の cospace で 2 GB の RAM が必要です。

D.2 Web Edge VM

Expressway（Large OVA または CE1200）は、中規模の Web アプリの要件（つまり 800 コール以下）の導入に推奨されるソリューションです。Expressway（中規模 OVA）は、小規模の Web アプリの要件（つまり 200 コール以下）の導入に推奨されるソリューションです。ただし、Web アプリの規模を大きくする必要がある導入の場合は、バージョン 3.1 から、必要なソリューションとして Cisco Meeting Server Web Edge を推奨します。

D.2.1 Edge サーバーの構成

エッジサーバーの役割では、2 つの仮想マシンハードウェア構成がサポートされています。これらの構成は、サポートされる最小ハードウェア要件とそれらがサポートする容量を定義します。

「小規模」Edge サーバー

サポートされている Cisco ハードウェアについて次の仕様の Cisco Meeting Server VM 1 台

- 4 GB RAM
- vCPU x 4
- 1 Gbps のネットワークインターフェイス

「大規模」Edge サーバー

サポートされている Cisco ハードウェアについて次の仕様の Cisco Meeting Server VM 1 台

- 8 GB RAM
- vCPU x 16
- 10 Gbps のネットワークインターフェイス

推奨されるプロセッサの仕様：

2.5GHz 以上で実行されている Intel Xeon E5 2600 などのプロセッサ仕様を推奨します。1 つの vCPU から 1 つの物理 CPU をお勧めします。

NIC **要件：**

Cisco は、TURN サーバーに単一の NIC 設定を使用した分割型サーバー展開をテストおよび検証しました。したがって、バージョン 3.0 からは、TURN サーバーのリッスンポートを 1 つのインターフェイスでのみ構成することをお勧めします。

共存のサポート：

Edge サーバーは他の VM と同じ場所に常駐することができます。ただし、4 つの vCPUVM ごとに 1 Gbps の NIC 要件があり、16 の vCPU ごとに 10 Gbps の NIC 要件があります。VM ホストには、すべてのアプリケーションに十分な NIC 容量が必要です。

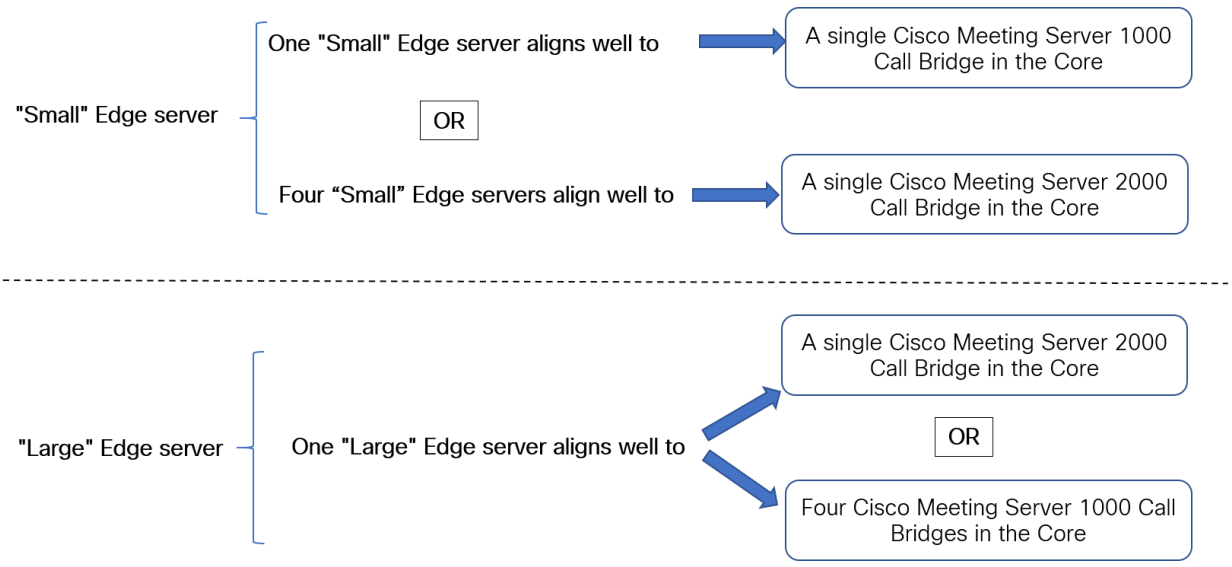
注：

- Meeting Server 1000 M4 ハードウェアは、1Gbps NIC をサポートします。Meeting Server M5 以降のハードウェアは、10Gbps NIC をサポートします。

表 8：エッジサーバー Web アプリのコールキャパシティ

コールのタイプ	小規模なエッジ VM のコールキャパシティ	大規模なエッジ VM のコールキャパシティ
フル HD 通話（1080p30）ビデオ	100	350
HD コール 720p30 ビデオ	175	700
SD コール 448p30 ビデオ	250	1,000
音声通話（G.711）	850	3,000

2 つの Edge サーバー構成は、Call Bridge に Cisco Meeting Server アプライアンスを使用する場合に、Edge キャパシティを Core Call Bridge キャパシティに簡単に一致させるキャパシティを提供します。



コア Call Bridge がサポートする Call Bridge コールキャパシティ、および使用されている Edge サーバーのハードウェア構成を確認して、必要な Edge サーバーの数を決定します。

D.2.2 導入に関する考慮事項

- 同じ Call Bridge または Call Bridge グループを処理するすべてのエッジサーバーの容量を同じにすることをお勧めします。つまり、4 つの vCPU すべて、または 16 の vCPU すべてを、両方を組み合わせて使用するのではなく、同じ容量にすることをお勧めします。

- スケーラブルまたは復元力のある展開にするためには、Call Bridge グループを設定することをお勧めします。これにより、TURN サーバーの一意のグループを各 Call Bridge グループに割り当てることができます。これは、ロードバランシングを支援し、TURN サーバーを Call Bridge で適切に地理的に配置するのに役立ちます。
- Web アプリが SIP スケール（クラスタごとに最大 24 の Call Bridge）に対応するために、複数の Edge サーバーがサポートされます。ただし、Call Bridge グループは、グループごとに最大 10 台の Edge サーバーのみをサポートします。10 台を超える Edge サーバーが必要な拡張性または復元力のある展開のためには、複数の Call Bridge グループが必要です。
- Meeting Server Edge ソリューションをサポートするため、TURN の拡張性モードを有効にする新しい MMP コマンド **`turn high-capacity-mode (enable|disable)`** が導入されています。この設定はデフォルトでイネーブルになっています。

Cisco Meeting Server Web Edge ソリューションの展開の詳細については、『導入ガイド（バージョン 3.1 以降）』を参照してください。

D.3 データベース VM

注：このセクションの内容は、1 つまたは複数の外部データベースを使用する場合にのみ該当します。

データベースのホストサーバーに厳しい CPU 要件はありませんが、大容量のストレージとメモリが必要です。要件を満たす VM ホストは必須ではありませんが、推奨されています。

- 8 つの vCPU、8 GB RAM[1]、100 GB のデータストア

  （OVF をこれらのパラメータに設定して、展開後のデフォルトにします）
- サンディブリッジ（以降）クラスの Intel プロセッサ（E5-2670 や E5-2680 v2 など）。
- データ ストアは、IOPS の高い SAN またはローカル SSD ストレージに配置する必要があります。
- データは、OS と同じ vDisk 上に存在している必要があります。

現在、Cisco Meeting Server 1000 のホストとして使用されている Cisco UCS C220 を使用することもできますが、VM データベースはサーバーリソースのごく一部しか使用しません。このサーバーを使用する場合、必要に応じて他の VM も VM データベースと同じサーバー上でホストできます。

[1] データベース VM の RAM 要件は、8 GB と、75,000 を超えた分について 100,000 の cospace あたり 1 GB の RAM です。たとえば、375,000 の cospace をサポートする展開環境のデータベース VM では、8 GB の最小 RAM 要件と、75,000 を超える分について 300,000 の cospace をサポートするために 3 GB の RAM が必要です。

D.4 レコーダーとストリーマ VM

注：新しい内部 SIP レコーダーおよびストリーマサービスは、Meeting Server の Call Bridge によって渡される特定の SIP ヘッダーパラメータに依存するため、外部の録画サービスまたはストリーミングサービスとして使用することはできません。Meeting Server の Call Bridge ではない他のソースからのコールが接続されると、想定されている特定の SIP ヘッダーが見つからないため、レコーダーおよびストリーマーはそのコールを拒否します。

D.4.1 新しい内部 SIP レコーダーコンポーネント用の VM のサイジング

レコーダーの実稼働での使用に推奨される展開環境は、少なくとも vCPU コア 4 つと RAM 4GB を搭載した専用 VM で実行することです。次の表に、録画タイプごとのパフォーマンスとリソース使用率を示します。

表 9：内部 SIP レコーダーのパフォーマンスとリソース使用率

録画設定	vCPU あたりの録画数	録画に必要な RAM	1 時間あたりのディスク予算	最大同時録画数
720p	2	0.5 GB	1 GB	40
1080p	1	1 GB	2 GB	20
音声	16	100 MB	150 MB	100

注意すべき重要事項（新しい内部レコーダーコンポーネントにのみ適用されます）：

- ホストの物理コア数まで vCPU を追加するとパフォーマンスが比例して拡張されます。

D.4.2 新しい内部 SIP ストリーマコンポーネント用の VM のサイジング

ストリーマの実稼働での使用に推奨される展開環境は、少なくとも vCPU コア 4 つと RAM 4GB を搭載した専用 VM で実行することです。次の表に、推奨される 3 つの最小仕様と、その仕様で処理可能なストリーム数を示します。

表 10：内部 SIP ストリーマの推奨仕様

vCPU の数	RAM	720p ストリームの数	1080p ストリームの数	オーディオのみのストリームの数
4	4 GB	50	37	100
4	8 GB	100	75	200
8	8 GB	200	150	200

注意すべき重要事項（新しい内部ストリーマコンポーネントにのみ適用されます）：

- vCPU 数が物理コア数をオーバーサブスクライブすることは避けるべきです。
- サポートされる 720p ストリームの最大数は、vCPU の増設に関係なく 200 です。
- サポートされる 1080p ストリームの最大数は、vCPU の増設に関係なく 150 です。
- サポートされるオーディオ専用ストリームの最大数は、vCPU の増設に関係なく 200 です。

D.5 Web Scheduler

スケジューラは、エンドユーザーが Web アプリを介して会議をスケジュールできるようにする Meeting Server コンポーネントです。 これは、VM 展開上の Meeting Server 1000、Meeting Server 2000、および Meeting Server でサポートされています。仕様ベースの VM プラットフォーム上の Meeting Server では、スケジューラコンポーネントを実行するために追加の 4 GB の RAM が必要です。Meeting Server 1000 および Meeting Server 2000 には、追加の RAM 要件はありません。スケジューラは、SMTP 電子メールサーバーの設定を介した電子メール通知の送信をサポートします。電子メールサーバー設定の詳細については、『Cisco Meeting Server 設置ガイド』を参照してください。

1 つのスケジューラで 150,000 の会議をサポートします。回復力を提供するために 2 つまたは 3 つのスケジューラを追加できますが、キャパシティは 150,000 のスケジュールされた会議のままです。スケジュールされたミーティングデータは Meeting Server データベースに保存され、クラスタ化されたデータベースとシングル ボックス データベースの両方の展開がサポートされています。

スケジューラは、Meeting Server MMP を使用して新しいコンポーネントとして導入されます。スケジューラが有効になっている場合は、ループバック インターフェイスを介して Call Bridge に API 要求を行います。したがって、スケジューラは、Call Bridge もホストしている Meeting Server に展開する必要があります。リモート Call Bridge を使用するようにスケジューラを設定することはできません。スケジューラの展開方法の詳細については、『Cisco Meeting Server 導入ガイド』を参照してください。

D.6 MeetingApps

ファイル共有をサポートするために、MeetingApps と呼ばれる新しいサービスが導入されました。MeetingApp は、他のサービスを使用せずに、スタンドアロンの Meeting Server ノードで構成する必要があります。参加者が外部ネットワークまたは内部ネットワークのどちらから参加しているかに応じて、MeetingApps を DMZ ネットワークまたは内部ネットワークで適宜構成できます。

MeetingApps サービスは、Meeting Server 2000 では構成できません。MeetingApp は、仕様ベースの Meeting Server の仮想化展開でのみ構成することをお勧めします。ただし、次の仕様に基づいて、Meeting Server 2000 または Meeting Server 1000 を、VM 展開上のミーティング アプリケーションとともに Call Bridge または Web Bridge として使用できます。

vCPU の数	RAM	ディスク容量
8	16 GB	100 GB

MeetingApps は、MMP コマンド **`meetingapps`** を使用して、Meeting Server の VM 展開で構成できます。

付録 E VMWare に関するその他の情報

E.1 VMWare

コア VM はホスト全体を使用するように構成する必要があります。これにより、ESXi カーネルは管理とネットワーク運用に CPU コアを使用できます。

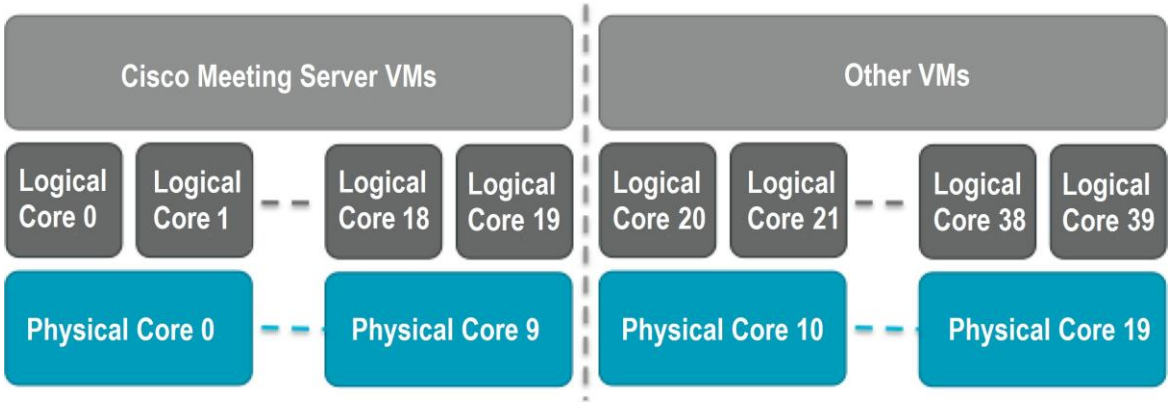
社内テストの一部として、定期的にさまざまな CPU 構成とサーバー構成の性能を測定しています。これらのテスト時には、徐々に模擬コールを追加し、VM に対する要求が少しずつ増加してキャパシティを超えるようにします。ユーザー体験を保証するため、複数の統計情報を監視しています。さらに ESXi の統計情報も監視し、診断ログを収集しています。

推奨されませんが、競合を防ぐために CPU 隔離ドメインが作成されている限り、Cisco Meeting Server VM とともに他の VM を実行することは可能です。この方法は「anti-pinning（アンチピニング）」と呼ばれ、すべての VM をコアのサブセットに明示的に固定します。Cisco Meeting Server VM は、そのコアに固定されている唯一の VM である必要があり、他のすべての VM は他のコアに明示的に固定されていなければなりません。

たとえば、20 コアのデュアル E5-2680v2 のホストを利用でき、25 の同時 720p30 コールレッグしか必要としない場合は、アンチピニングを使用できます。コアあたり 2.5 コールの比率を使用して、このキャパシティを提供するには 10 個の物理コアが必要です。10 個のコアは他のタスクに使用できます。

ハイパースレッドを有効にしていると、40 の論理コアを利用でき、ESXi は、これらの論理コアにインデックスとして 0 ～ 39 のラベルを付けます。Cisco Meeting Server VM には 20 の仮想 CPU を割り当てて、スケジュール設定のアフィニティを 0 ～ 19 で構成する必要があります。隔離ドメインのペアを作成するために、ホスト上で実行される他の VM すべてをアフィニティ 20 ～ 39 で明示的に構成する必要があります。また、ESXi ハイパーバイザ用に、物理コアに VM を固定しないようにすることが必要な場合があります。

図 8：ピニングにより作成された VM の隔離ドメイン



VMXNet3 仮想ネットワークアダプタを推奨します。このアダプタは、他のアダプタタイプよりもオーバーヘッドが少ないためです。仮想ネットワークアダプタは、すべて同じタイプである必要があります。

VMware Fault Tolerance（FT）は、1 つの仮想コアの VM に制限されるためサポートされません。VMware vCenter Operations Manager などの高水準のツールは完全にサポートされます。

注：EVC モードを有効にした VMware ハイパーバイザを使用する場合、EVC を次のいずれかのモード以上に設定する必要があります。

“B1”/AMD Opteron™ 第 4 世代

「L2」/Intel® Nehalem 世代（以前の Intel® Xeon Core™ i7）

上記にリストしたものより古い CPU との互換性を強制する EVC モードは、SSE 4.2 を無効にするため、サポートされていません。SSE 4.2 は必須です。

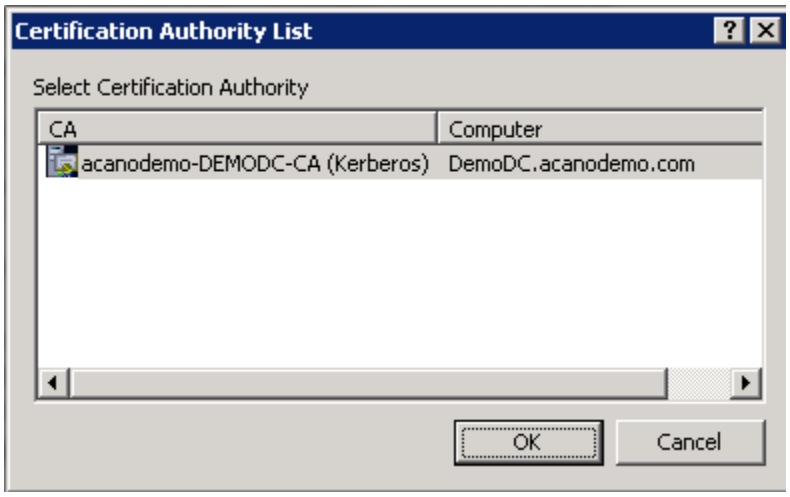
付録 F ローカル認証局によって署名された証明書の作成

この付録では、Active Directory Certificate Services のロールがインストールされている Microsoft Active Directory サーバーなどのローカル CA を使用して、証明書署名要求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、パスと証明書署名要求名をお客様の情報に置き換えて発行します。

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

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

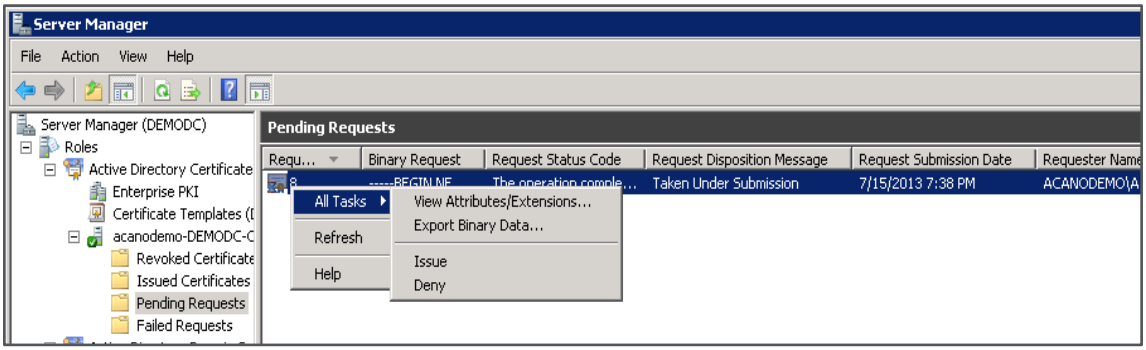


4. 次のいずれかを実行します。
   - 証明書発行許可を持つ Windows アカウントを使用している場合は、生成された証明書を（webadmin.crt などの名前で）保存するよう求めるプロンプトが表示されます。下記の手順 c に進みます。
   - 生成された証明書を発行するためのプロンプトが表示されない場合、代わりに次のようにコマンドプロンプトウィンドウに [証明書の要求は保留中です：提出済みです（Certificate request is pending: taken under submission）] というメッセージが表示され、[要求 ID（Request ID）] がリス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

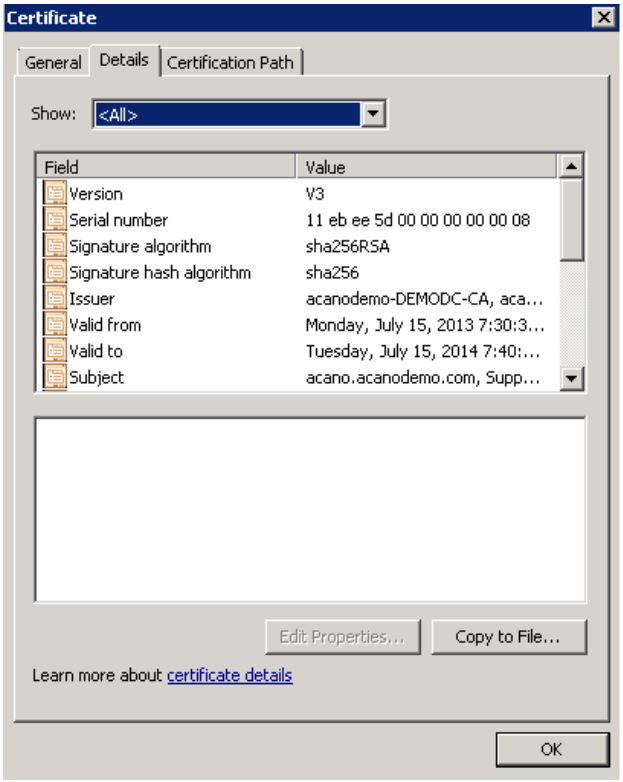
```
C:\Users\Administrator>certreq -submit -attrib "CertificateTemplate:WebServer" C
:\Users\Administrator\Desktop\demokitcsr.pem
Active Directory Enrollment Policy
  {0BD5D0B7-591F-4C77-AFEC-3C0E470F77D5}
  ldap:
RequestId: 8
RequestId: "8"
Certificate request is pending: Taken Under Submission (0)

C:\Users\Administrator>_
```

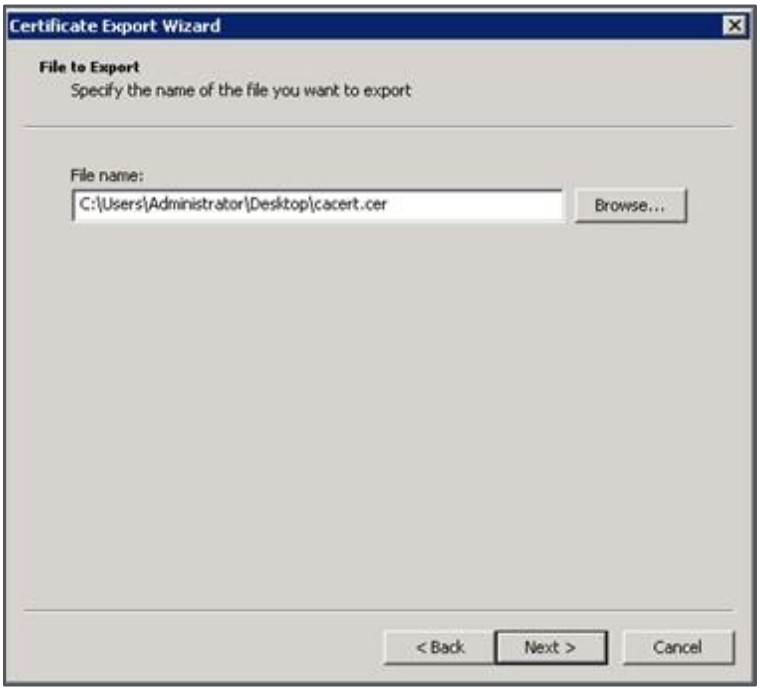
5. CA の [サーバーマネージャ（Server Manager）] ページの [CA のロール（CA Role）] にある Pending Requests フォルダを見つけます。
6. [CMD] ウィンドウに表示された要求 ID に一致する保留中の要求を右クリックして、[**すべてのタスク**（All Tasks）] > [**発行**（Issue）] の順に選択します。



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



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



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

SFTP を使用して証明書（webadmin.crt など）と秘密キーを Cisco Meeting Server の MMP へ転送します。詳細についてはセクション 3.5.2 を参照してください。

注意：Web Enrolment 機能がインストールされている CA を使用している場合は、BEGIN CERTIFICATE REQUEST の行と END CERTIFICATE REQUEST の行を含めて証明書署名要求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。

シスコの法的情報

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

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。ソフトウェアライセンスまたは限定保証書が見つからない場合は、CISCO の代理店に連絡してコピーを入手してください。

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。マニュアル内の例、コマンド出力、ネットワークトポロジ図などの図は、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。最新バージョンについては、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/jp/go/offices）をご覧ください。

シスコの商標