Cisco Meeting Server

Cisco Meeting Server 2.8

Cisco Meeting Server 1000 と仮想化導入のインストール ガイド

2019 年 11 月 27 日

目次

変更履歴

日付	変更点
2019 年 11 月 27 日	400v/410v への言及が削除されました。
2019 年 11 月 13 日	ESXi のサポートがバージョン 2.8 用に更新、変更されました。
2019 年 7 月 16 日	本ドキュメントの誤った記述が訂正され、設置に関する章が再度挿入されました。
2019 年 5 月 30 日	ドキュメントの小幅の訂正
2019 年 4 月 26 日	サポートされる VMware ESXi のバージョンが更新されました。
2019 年 4 月 9 日	その他の修正。
2019 年 4 月 2 日	ESXi 6.5 Web クライアントを使用して OVA ファイルから Meeting Server を展開するための情報が追加されました。 その他の修正。
2019 年 1 月 28 日	Cisco UCS C220 M5 ラック サーバを使用した Cisco Meeting Server 1000 は、M4 の付いたものより優先されます。（2018 年 11 月以降）。
2018 年 11 月 29 日	その他の修正。
2018 年 9 月 24 日	Hyper-V の項とリファレンスが削除されました。
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 のサポートが追加されました。
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が追加されました。AWS のリファレンスが削除されました。

1 はじめに

Cisco Meeting Server は、Microsoft、Avaya など、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、Web コンテンツのスケーラブルなソフトウェア プラットホームです。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、人と人と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 vmx-1x をサポートする VMware ESXi 6.x を使用する仮想化導入として動作します。

- Cisco Meeting Server 1000（事前設定された Cisco UCS C220 ラック サーバ。2019 年の冒頭より、M4 のバリエーションが M5 に取って代わられました）。
- 仕様ベースの VM プラットフォーム。

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。

Cisco Meeting Server のバージョン	ESXi バージョン	注
2.8	ESXi 6.7、 ESXi 6.5 アップデート 2 以降のビルド、 ESXi 6.0 アップデート 3	M4 およびスペックベースのサーバでのサポートが追加されました。
2.6 および 2.7	ESXi 6.7 または ESXi 6.5 アップデート 2	ESXi 6.7 または ESXi 6.5 アップデート 2 は Cisco Meeting Server 1000 M5 でのみサポートされます。 注：VMware の変更により、Cisco Meeting Server 1000 M4、または仕様ベースの VM の ESXi 6.7 または ESXi 6.5 アップデート 2 へのアップグレードは推奨されません。これは、ESXi 6.7 にアップグレードされた Cisco Meeting Server 1000 M4 が高負荷の下で動作している場合に、大量のパケット損失が観測されることに起因します。Cisco Meeting Server 1000 M5 は VMware の変更によって影響を受けません。
2.6	ESXi 5.5	すべての Cisco Meeting Server プラットフォームでサポートされなくなりました。
2.4 および 2.5	ESXi 6.5 および ESX 6.0 アップデート 3	ESXi 6.5 と ESX 6.0 Update 3 のどちらを使用しても、TLS 1.0 および TLS 1.1 による ESXi との通信を無効化できます。

注：バージョン 2.4 から、Cisco Meeting Server ソフトウェアは Microsoft Hyper-V 仮想化展開をサポートされません。

分割導入やスケーラブルな導入では多くの場合、Cisco Meeting Server の仮想導入はエッジ サーバとして使用されています。

機能と、参加者のユーザ エクスペリエンスは、同じソフトウェア バージョンを実行するすべてのプラットフォームで同じです。ただし、仮想化導入と物理導入（Cisco Meeting Server 2000 と X シリーズ サーバ）は互いに交換できません。たとえば、仮想化導入でバックアップを作成し、X シリーズ サーバでロール バックすることはできません。この逆もできません。

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 6.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 を設定し、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：Cisco Meeting Server 1000 の Cisco UCS ESXi におけるデフォルト クレデンシャルでは、**`root`** としてログインし、 **`password`** をパスワードとして使用します。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。

スペックベースの 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 このマニュアルの使用方法

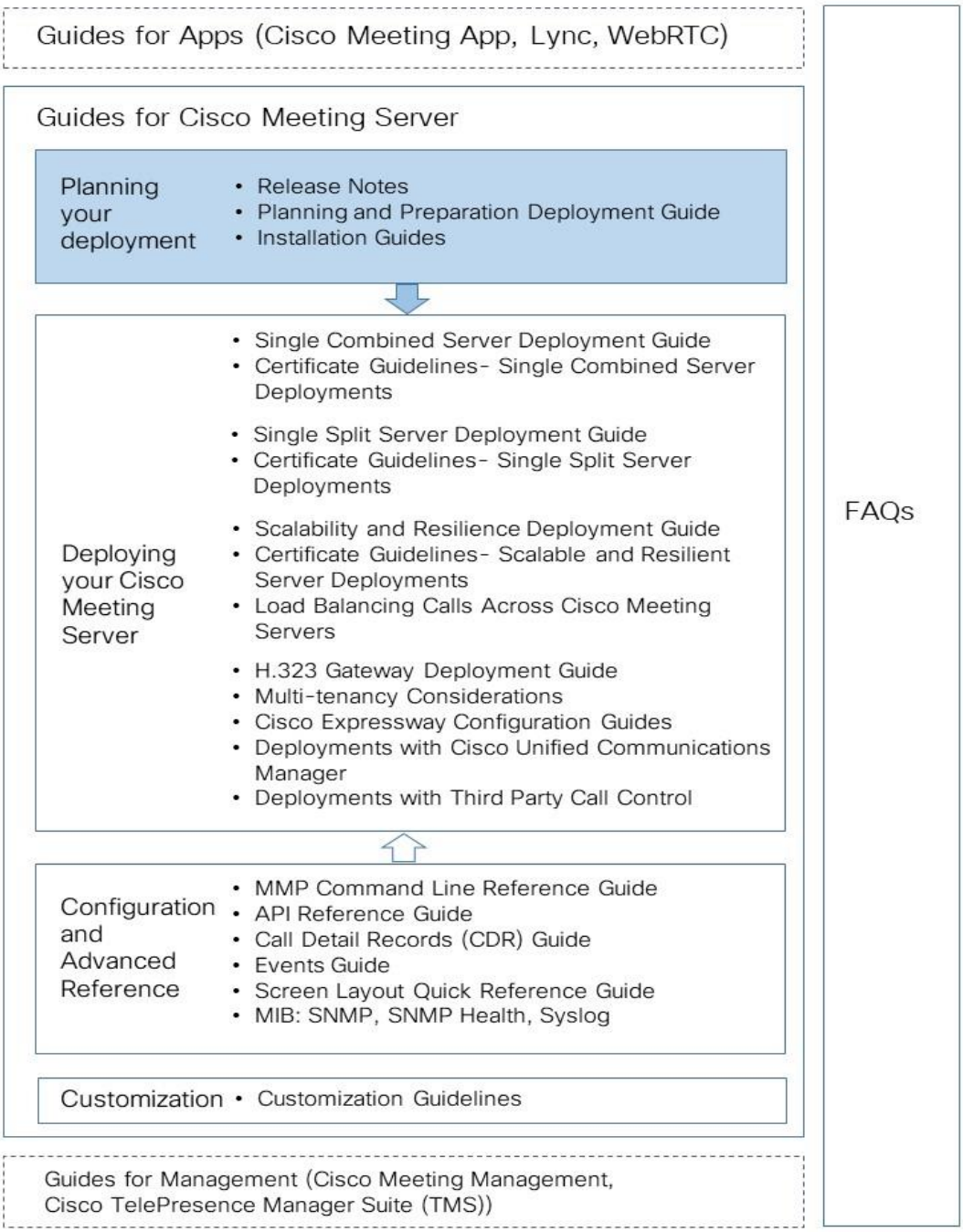
このガイドでは、Cisco Meeting Server 1000 と仕様ベースの VM 導入のインストールについて説明します。
Cisco Meeting Server 1000 は事前にソフトウェアがインストールされて出荷されます。Cisco Meeting Server 1000 の設定を開始するには、このガイドの第 3 章に進む前に、第 2.4 項に進んでください。

注：Cisco Meeting Server 1000 には仕様ベースの VM サーバ向けのさまざまな設定があり、事前に設定されています。この設置は変更しないでください。

スペックベースの VM 導入をインストールする場合、第 3 章に進んで VM を設定する前に第 2 章に進んでください。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 を設定し、ライセンスを適用したら、『導入の計画および準備ガイド』を使用して適切な導入を決定し、次に対象となる導入と最も関連性の高い導入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導入用ドキュメント



注：シスコのユーザ ドキュメントで使用するアドレス範囲は、RFC 5737 で文書化用の明示的な予約対象として定義されているアドレス範囲です。Meeting Server ユーザ ドキュメントの IP アドレスは、特に明記しない限り、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 各種 MMP コマンドの違い

MMP コマンドの全セットについては、MMP コマンド リファレンスで詳しく説明されています。Cisco Meeting Server 2000 または Acano X シリーズ サーバの実行と、仮想化された Cisco Meeting Server の実行には、いくつかの違いがあります。

コマンド	Cisco Meeting Server 2000 上	Cisco Meeting Server 1000 上、および仮想化された Cisco Meeting Server 上	Acano X シリーズ サーバ上
shutdown	MMP では使用できません。ブレード サーバの電源を切断するには、まず Cisco UCS Manager 上での電源切断を行います。	vSphere の電源ボタンは使用しないでください。代わりに、**shutdown** コマンドを使用します。	プロンプトが表示されたら、「Y」を入力します。これで、サーバの電源を安全に切断できるようになりました。
health	MMP では使用できません。Cisco UCS Manager を使用します。	該当なし	サーバが健全かどうかを返します。
serial	サーバのシリアル番号を返します。	該当なし	サーバのシリアル番号を返します。
dns	インターフェイスは指定しないでください。 次に例を示します。 **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。次に例を示します。 **dns add forwardzone <domain-name> <server ip>**	インターフェイスとして mmp または app を指定する必要があります。次に例を示します。 **dns mmp add forwardzone <domain-name> <server ip>**
user evict	該当なし	使用可能	使用可能

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

コンポーネント	Cisco Meeting Server 2000 上	Cisco Meeting Server 1000 上、および仮想化された Cisco Meeting Server 上	Acano X シリーズ サーバ上
Call Bridge	提供されています。	提供されています。	提供されています。
Web Bridge	提供されています。	提供されています。	提供されています。
XMPP Server	提供されています。	提供されています。	提供されています。
データベース	提供されています。	提供されています。	提供されています。
TURN サーバ	使用できません。	提供されています。	提供されています。
ロード バランサ	使用できません。	提供されています。	提供されています。
Recorder	使用できません。	提供されています。	提供されています。
ストリーマ	使用できません。	提供されています。	提供されています。
H.323 ゲートウェイ	使用できません。	提供されています。	提供されています。
SNMP MIB	現在使用できません。	提供されています。	提供されています。

2 導入

この章は、仕様ベースの VM プラットフォームおよび Cisco Meeting Server 1000 への導入に適用されます。VMware ホストを導入する場合は第 2.2 項に従います。Cisco Meeting Server 1000 を導入する場合は第 2.4 項に従います。

2.1 ご使用になる前に

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 を設定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（単一統合型サーバ導入モデル）
- 内部ネットワークに導入されたコア サーバ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、すべての導入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、本ソフトウェア バージョンのリリース ノートの手順に従います。

2.1.2 Cisco Meeting Server の VM 導入としてのホスト要件

Cisco Meeting Server は 幅広い標準的な Cisco サーバにおいて、VM 導入として動作します。さまざまな導入に関しては、こちらの VM 設定の要件および UCS のテスト済みのリファレンス設定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 サーバ上でも動作します。Klas VoyagerVM や DTECH LABS M3-SE-SVR2 などの小型フォーム ファクタのシステムや高耐久化システムにも対応しています。このソフトウェアは、クラウド サービスと同様に VMware ESXi に導入できます。

表 1：サード パーティのサーバで実行されている Cisco Meeting Server のホスト要件

	最小ハードウェア	推奨
サーバのメーカー	任意（Any）	任意（Any）
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	1 GB（1 コアあたり）*	1 GB（1 コアあたり）*
ストレージ	100GB	100GB
ハイパーバイザ	仮想ハードウェア vsm-11 を使用した VMware ESXi 6.0 の最新アップデート	仮想ハードウェア vsm-13 を使用した VMware ESXi 6.5 のデート。 注：詳細については、VMware のドキュメントを参照して

* 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：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 との通信を可能または不能にするためのツールが用意されています。

表 2：推奨されるコア VM の構成

720p30 コール レッグ	CPU の設定	RAM の設定	システムの例
50	Dual Intel E5-2680v2	32 GB（8 x 4 GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
40	Dual Intel E5-2680v2	32 GB（8 x 4 GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
25	Single Intel E5-2680v2	16 GB（4 x 4 GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
15	Single Intel E5-2640v2	8 GB（4 x 2 GB）	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8

また、次の点に注意してください。

- 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てください。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 ポートを共有する設定にしないでください。そのように設定すると、パケット損失が突然大量に発生したり、音声やビデオの品質が低下したりする可能性があることが社内テストにより判明しています。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設定するか、または無効にしてください。
- 使用できる場合は、ホストでハイパースレッドを有効にする必要があります。有効にしない場合、処理能力が最大で 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 プロセッサの処理能力は、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、実稼動環境には 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。専用の条件は次のとおりです。
  - 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 のみに与える、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 のない状態にする。
  - 仮想化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。[会議（Conferencing）] 見出しの下の Cisco Meeting Server をクリックします。
- EVC モードが有効化された VMware ハイパーバイザが使用されている場合、EVC は次のモードのいずれか以上に設定する必要があります。

  「B1」/AMD Opteron™ Generation 4

  「L2」/Intel® Nehalem generation（旧製品名 Intel® Xeon Core™ i7）

  上記よりも古い CPU との互換性が求められる EVC モードは、SSE 4.2 が無効化されるためサポートされません。ここでは SSE4.2 が必要です。
- 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 4 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へのインストール

注：仮想化導入の 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。これは、ovf フォルダおよび関連ファイルを提供した Acano サーバ リリースとは異なります。

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。

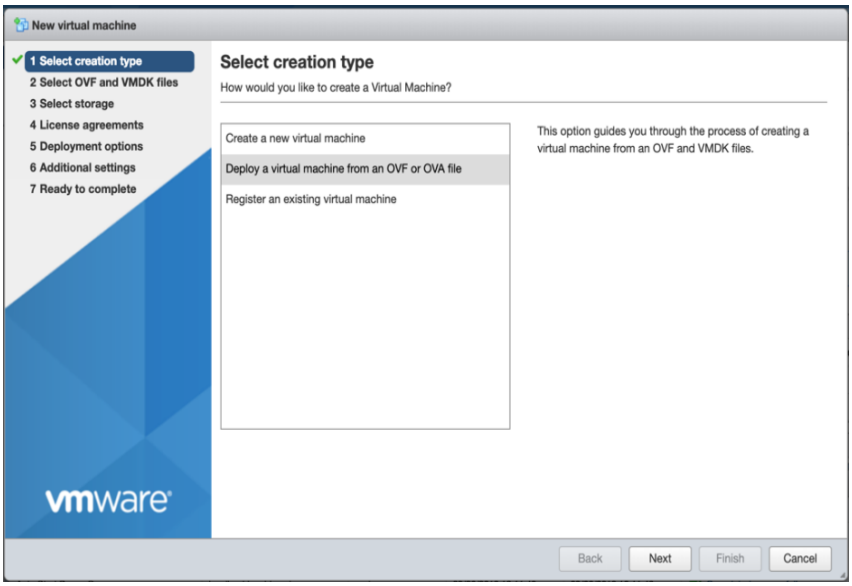
- EVC モードが有効化された VMware ハイパーバイザが使用されている場合、EVC は次のモードのいずれか以上に設定する必要があります。
  「B1」/AMD Opteron™ Generation 4
  「L2」/Intel® Nehalem generation（旧製品名 Intel® Xeon Core™ i7）
  上記よりも古い CPU との互換性が求められる EVC モードは、SSE 4.2 が無効化されるためサポートされません。ここでは SSE4.2 が必要です。
- Call Bridge のアクティベーション キーは、メディアのコールに必要です。アクティベーション 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 4 章と付録 B を参照してください。

2.3 OVA ファイルから ESXi 6.5 Web クライアントを使用して Meeting Server を導入

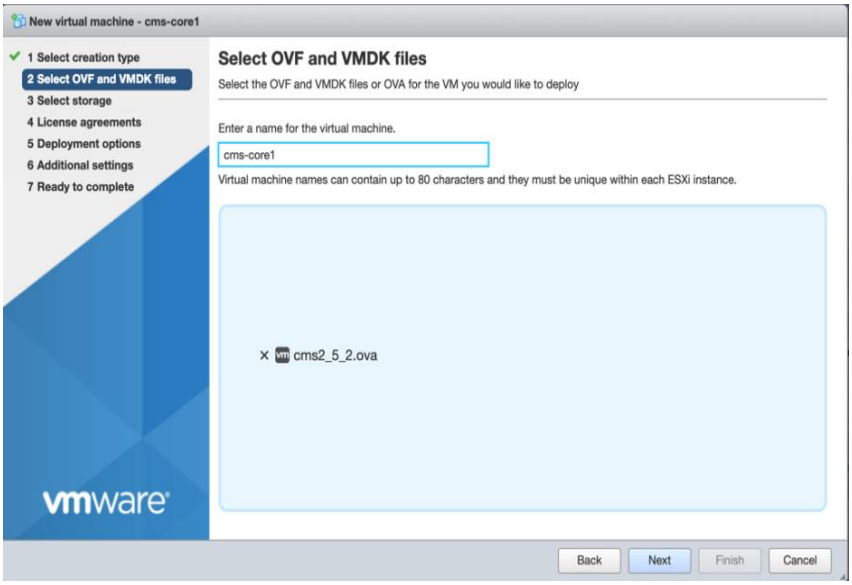
注：仮想化導入の Cisco Meeting Server のすべてのリリースで、新規導入の場合は .ova ファイルが作成され、最新リリースへのアップグレードの場合はアップグレード イメージ（.img）が作成されます。これは、ovf フォルダおよび関連ファイルを提供した Acano サーバ リリースとは異なります。

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。

1. .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 クライアントでは、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導入（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。

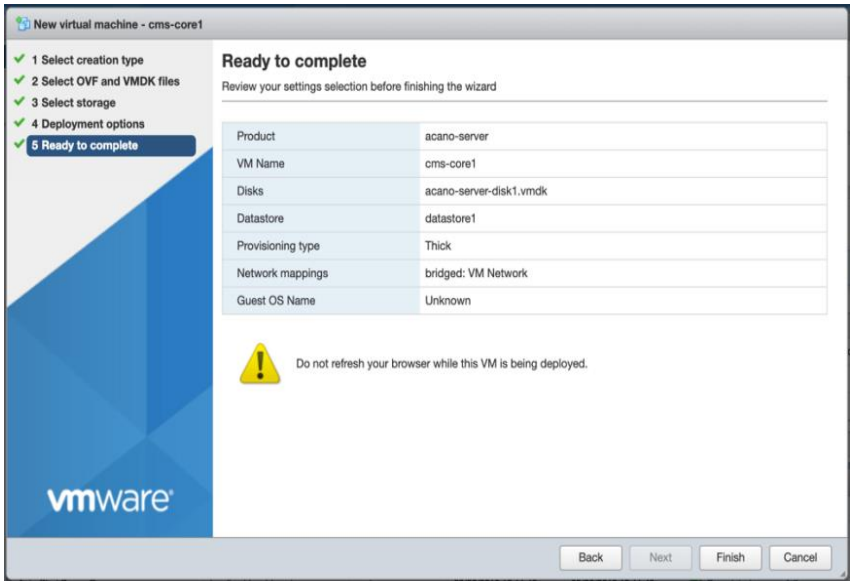


4. 任意の仮想マシン名を入力し、ステップ 1 でダウンロードした .ova ファイルを参照するかドロップして、それを選択します。



5. ウィザードの指示に従います。次の設定を行います。
   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 の接続先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. **[導入後に電源をオン（Power on after deployment）]** がオフになっていることを確認します。
   e. **[終了（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。

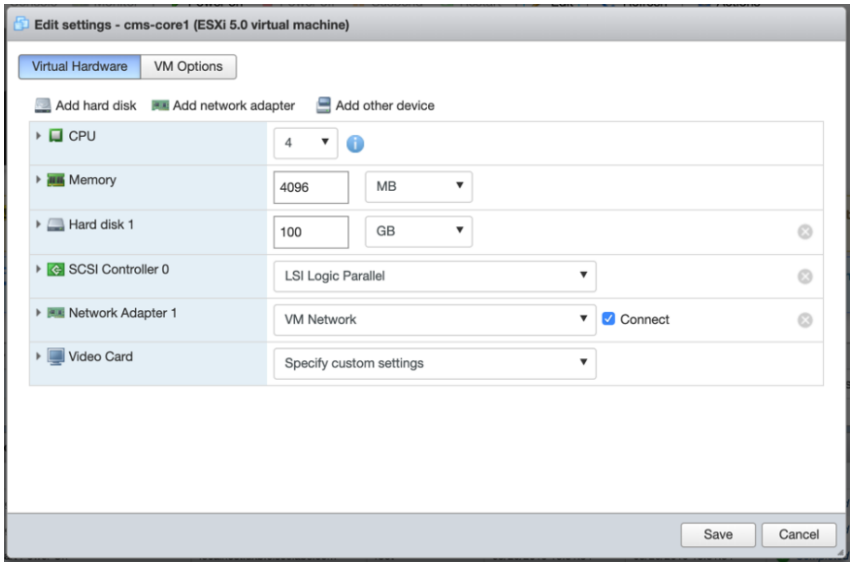


6. 完了すると、新しい Cisco Meeting Server VM が **[仮想マシン（Virtual Machines）]** に表示されるようになります。
7. VM のリストから Cisco Meeting Server VM を選択します。
8. **[アクション（Actions）]** ボタンで **[設定を編集...（Edit Settings...）]** を選択します。
   a. **VM 設定**を編集し、**CPU** を選択します。**CPU の数**を希望する数に設定します（4 が最小、24 が最大です）。スケーリングの詳細については、導入ガイドを参照してください。推奨される CPU 数は、小規模導入の場合は 4 基、大規模導入の場合は 8 基です。VM の設定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 [英語] 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。

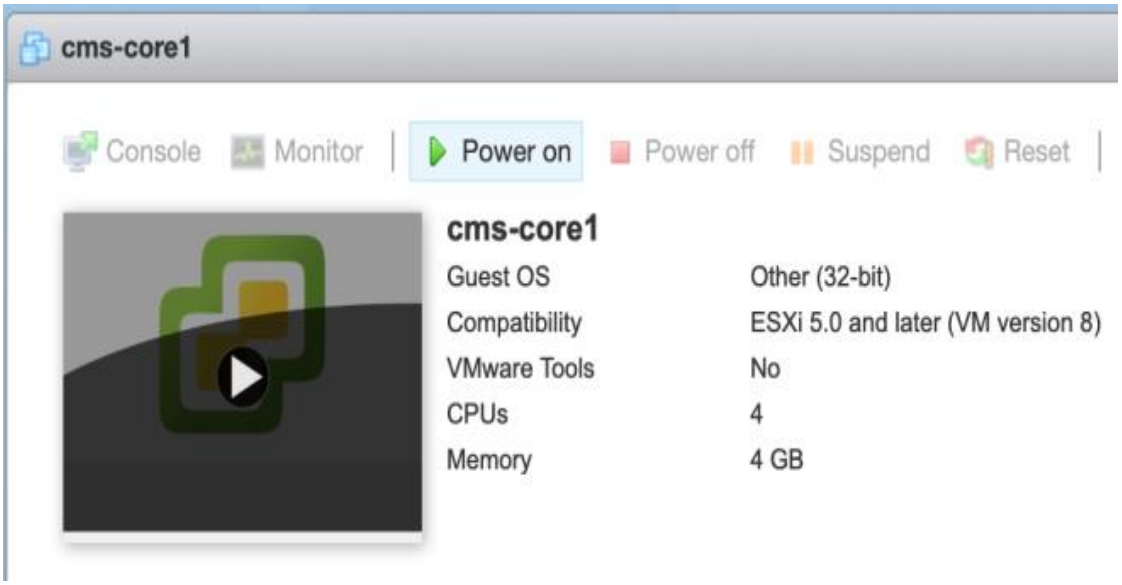
      vCPU の数を設定したら、[ソケットあたりのコア数（Cores per Socket）] を CPU の個数と同じ値に設定することができます。これにより、ソケット数が 1 に設定されます。

注：**[管理（Manage）] > [設定（Settings）] > [プロセッサ（Processors）]** をクリックすると、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。

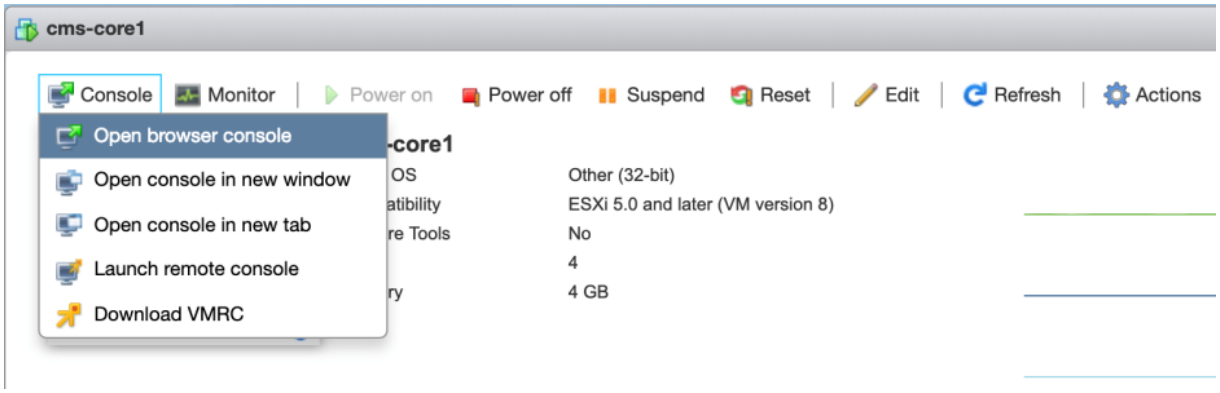
c. RAM が 4 GB 以上に設定されていること、およびディスク容量が 100 GB に設定されていることを確認します。



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. ユーザ名「admin」とパスワード「admin」を使用してログインします。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 章に進んでください。

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

2.4.1 ご使用になる前に 3000

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 コードまたは顧客により提供された 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電子メール
- 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と USB キーボード
    または
  - PC、シリアル アダプタ 、シスコ シリアル ケーブル、ターミナル 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 を特定の場所に配置するか、または必要に応じてラックに配置します。導入内容に応じて、『Cisco UCS C220 M5 Installation Guide』または『Cisco UCS C220 M4 Installation Guide』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. ターミナル プログラムを開いてシリアル ポート/アダプタに割り当てられた COM ポートを選択し、ターミナルの設定を「115200 ボー」、「パリティなし」、「8 データ ビット」、「1 ストップ ビット」にします。
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、Ethernet1 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て設定した後に、その LAN を Ethernet1 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 アドレスで設定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. ターミナル 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名とパスワード（ユーザ名： **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設定が表示されます。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 スコープに存在していることを前提としています）。

```
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** と入力して変更内容を確認します。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、設定した 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、ユーザ名とパスワードのフィールドを含むシスコ ランディング ページが表示されます。
13. ユーザ名 **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、セキュリティに関する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、サーバに直接接続された様子を再現したモニタ画像が表示されるまで続行します。サーバ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]** を選択してサーバを起動します。数分後にブートし、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設定

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へのコンソール アクセスが必要です。

サーバの電源が投入され、VMware コンソール画面が表示されていることを確認し、**F2** を押して設定を行うか、または **F12** を押してシャットダウンします。

1. **F2** を押して、サーバを設定します。デフォルトのユーザ名は **root**、デフォルトのパスワードは **`password`** 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、**[パスワードの設定（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設定（Configure Management Network）]** を選択し、次に **[IPv4 の設定（IPv4 Configuration）]** を選択します。
4. 使用するネットワーク設定のオプション（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. （任意）Meeting Server アプリケーションから、異なる VLAN 経由で Hypervisor 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 を設定してください。
6. ログアウトするには、**Esc** キーを押してメイン メニューに戻り、**Esc** キーをもう一度押します。

   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ていないため、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 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 ケーブルをサーバの M1 インターフェイスから取り外し、Ethernet1 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。サーバを再起動するには、サーバの前面にある電源ボタンを短く押します。サーバが自動シャット 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、サーバが取得した IP アドレスは参照できなくなります。サーバ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、サーバ背面の Ethernet1 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 インスタンスの設定

ここでは、VMware インスタンスに接続し、Hypervisor の初期設定を完了します。

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. ユーザ名：**root** と、VMware ネットワーク管理設定で設定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. 接続ウィンドウで vSphere クライアントを開き、VMware インスタンスの IP アドレス、ユーザ名：**root** 、そして VMware ネットワーク管理設定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、サーバに接続します。
3. サーバに接続する際、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 の設定

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

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 [設定（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チェックし、**[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設定ページを閉じます。

2.4.5 タスク 4：VMware ライセンスの取得と有効化

VMware ライセンスをシスコに注文した場合、ライセンスはアクティベーション コードとして、シスコから別個のパッケージまたは電子メールで送付されます。Cisco Meeting Server 1000 1 台あたりに 1 CPU ライセンスが 2 つ必要です。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、インターネットと電子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シスコ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 コードが電子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、次の VMware KB の記事を参照してください。 https://kb.vmware.com/s/article/2006973
   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 **[設定（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. 現在の評価版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 Hypervisor 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 クライアントを開いたら、Meeting Server の IP アドレス、ユーザ名：**root**、以前に設定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 ソフトウェアの設定を続行できます。
4. ネットワークに DHCP が存在しない場合、第 3 章（または MMP Command Line Reference Guide）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抑制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. ユーザ名「admin」とパスワード「admin」を使用してログインします。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 ヵ月後に期限が切れます。

その他の設定プロセスについては第 3 章で説明します。

3 設定

3.1 Cisco Meeting Server 管理者アカウントの作成

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

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

注意：パスワードは 6 ヵ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 アカウントは、Call Bridge の Web 管理画面インターフェイスへのログインにも使用できます。Web 管理画面インターフェイス経由でユーザ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 Command Reference』を参照してください。

Cisco Meeting Server の仮想化導入には、最初はネットワーク インターフェイスが 1 つしかありませんが、最大 4 つまでサポートされます（次の項を参照してください）。初期設定のインターフェイスは「a」です。これは、Acano X シリーズ サーバのインターフェイス A に相当します。MMP は、仮想導入ではこの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、二重、および自動ネゴシエーションの各パラメータを設定するには、**iface** 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設定を表示するには、MMP で次のコマンドを入力します。

   `iface a`

   a. コマンド **`iface (admin|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）、二重、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切り替えるには、コマンド **iface a autoneg <on|off>** を使用します。次に例を示します。

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 on に設定することをお勧めします。

2. 「a」インターフェイスは、DHCP を使用するように初期設定されています。既存の設定を表示するには、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 の設定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. スタティック 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 マスクおよびデフォルト ゲートウェイを指定して、静的 IP アドレスを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

3. DNS を設定します。

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 は簡素化された導入に必須です。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 リゾルバーを指すように Meeting Server を設定することを推奨します。

a. dns 設定を出力するには、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：順ゾーン（forwardzone）とは、ドメイン名とサーバ アドレスから構成された 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に問い合わせることができます。ロード バランシングとフェイル オーバーを可能にするには、特定のドメイン名に対して複数のサーバを指定します。一般的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。

次に例を示します。

```
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>
```

次に例を示します。

```
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 仮想化導入は、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「Adding and Modifying Virtual Network Adapters」を参照してください。

---

4. 新しいアダプタを追加したら、MMP 上で使用するインターフェイスを有効にします。たとえば、**ipv4 b enable** などのコマンドを使用できます。
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 をリブートします。

3.4 Call Bridge の設定

Call Bridge は、SIP コール制御デバイスおよび Lync Front End（FE）サーバとの 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）を設定できます。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. 『証明書のガイドライン』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実行して、Call Bridge が証明書を使用し、Lync FE サーバと 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 管理画面インターフェイスの設定

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

Web 管理画面インターフェイスの設定に含まれる秘密キー/証明書ペアの作成については第 3.5.1 項を、MMP への秘密キー/証明書ペアのアップロードについては第 3.5.2 項を参照してください。

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

3.5.1 Web 管理画面インターフェイスの証明書の作成

Web 管理画面インターフェイスは HTTPS を介してのみアクセスできるため、セキュリティ証明書を作成し、Cisco Meeting Server にインストールする必要があります。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 管理画面インターフェイスではなく API を介して Call Bridge を設定する場合も、Web 管理画面インターフェイスの証明書はアップロードしておく必要があります。

下記の情報は、シスコが秘密キー マテリアルの生成要件を満たしていることを想定しています。必要に応じて、パブリック認証局（CA）を使用して、秘密キーと証明書を外部で作成することもできます。外部で生成したキーと証明書のペアを、SFTP を使用して Cisco Meeting Server の MMP 上にロードします。署名済み証明書を取得したら、第 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 にログインしてコマンド
`pki selfsigned <key/cert basename>`
を使用します。**`<key/cert basename>`** の箇所では、生成されるキーと証明書を識別します。たとえば「pki selfsigned webadmin」と指定した場合、webadmin.key と、自己署名された webadmin.crt が作成されます。自己署名証明書を実稼働環境で使用することは推奨されません。

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>]`

   引数の説明

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

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

   - CN： commonName（共通名）。これは証明書上に存在しなければなりません。DNS A レコード内で Common Name と定義された FQDN を使用します。従わない場合、ブラウザで証明書エラーが発生します。
   - OU：組織ユニット
   - O：Organization（組織）
   - L：Locality（地域）

- ST：State（州/都道府県）
- C：Country（国）
- emailAddress

2 単語以上の長さの値には、たとえば、次のように引用符を使用します。

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

2. CSR を次のいずれかに送信します。
   - 認証局（CA）。たとえば、要求側のアイデンティティを確認し、署名付き証明書を発行する Verisign など。
   - ローカルまたは組織の認証局。たとえば、Active Directory 証明書サービスの役割がインストールされている Active Directory サーバなど（付録 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 によって証明書チェーンが発行された場合は、チェーンから証明書を抽出する必要があります。証明書ファイルを開き、特定の証明書の BEGIN CERTIFICATE および END CERTIFICATE 行を含むテキストをコピーして、テキスト ファイルに貼り付けます。このファイルを .crt、.cer、または .pem 拡張子で証明書として保存します。残りの証明書チェーンをコピーして別のファイルに貼り付けます。中間証明書チェーンであることがわかる明確な名前を付けて、同じ拡張子（.crt、.cer、または .pem）を使用してください。中間証明書チェーンは、チェーンを発行した CA の証明書が最初でルート CA の証明書がチェーンの最後になる順番で並べる必要があります。

3.5.2 HTTPS アクセス用 Web 管理画面インターフェイスの設定

注：Web 管理画面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 管理画面インターフェイスと Web Bridge の両方で同じインターフェイスを使用する場合、MMP コマンド **webadmin listen <interface><port>** を使用して、Web 管理画面インターフェイスのポートを 445 などの非標準ポートに変更する必要があります。

---

1. MMP への SSH 接続を確立し、サインインします。
2. Web 管理画面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 管理画面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>]
   ```

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 により証明書バンドルが提供されている場合は、バンドルも個別のファイルとして証明書に含めます。次に例を示します。

```
webadmin certs webadmin.key webadmin.crt webadminbundle.crt
```

5. Web 管理画面インターフェイスを再起動します。

```
webadmin restart
```

6. Web 管理画面インターフェイスを有効にします。

```
webadmin enable
```

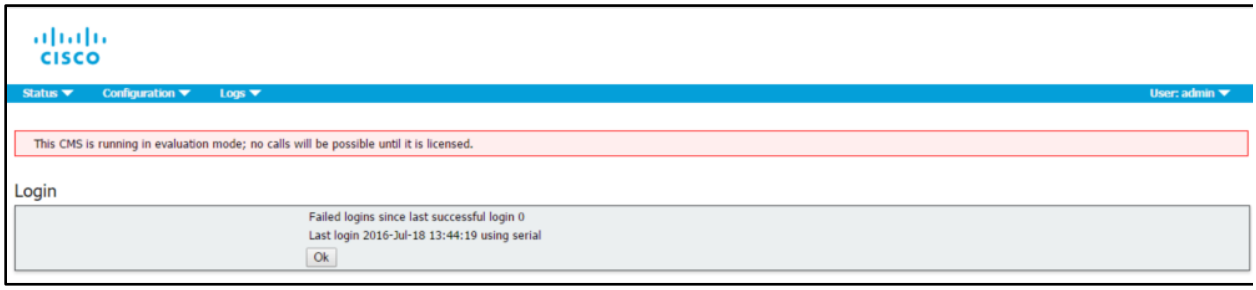
次に例を示します。

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

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

次の図 2 に示すバナーは、cms.lic ライセンス ファイルがアップロードされるまで表示されます。

図 2：評価モードの Cisco Meeting Server



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

Call Bridge を設定した後でライセンス ファイルを取得し、適用する方法については、第 4 項を参照してください。

4 ライセンス ファイルの取得および入力

Cisco Meeting Server のすべての仮想化導入にライセンス ファイルが必要です。ライセンス ファイルは、仮想サーバの MAC アドレス用です。

付録 A で、Cisco Meeting Server 用に購入が可能なシスコのライセンスについて説明します。ライセンスを購入した後で、この章に従って Cisco Meeting Server にライセンスを適用します。

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

この項は、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 コードを受信していることを前提としています。

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

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

   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 プラットフォームの MAC アドレスではありません。

2. シスコ製品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. 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提供されます。Zip ファイルを展開し、展開後の .lic ファイルの名前を **cms.lic** に変更します。
4. 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。
5. コマンド **`callbridge restart`** を使用して Call Bridge を再起動します。
6. Call Bridge を再起動した後、ライセンス ステータスを確認するには、**`lincense`** を入力します。

   有効化された機能と有効期限が表示されます。

4.2 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設定しておく必要があります。

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

注：クラスタ化する複数サーバ（単一結合サーバ、あるいは分割のコア サーバまたはエッジ サーバ）を導入する場合、詳細は『Scalability & Resilience Deployment Guide』の付録 *『Sharing Call Bridge licenses within a cluster』* を参照してください。

これで、Cisco Meeting Server を設定する準備が整いました。次の場所にある導入に適したガイドを参照してください。

- Single Combined Server Deployment Guide：単一のホスト サーバに導入する場合
- Single Split Server Deployment Guide：分割コア/エッジ導入環境に導入する場合
- Scalability & Resilience Guide：クラスタ化する複数サーバ（単一結合サーバ、あるいは分割のコア サーバまたはエッジ サーバ）を導入する場合。

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。

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 サーバまたは Cisco UCS C220 M4 ラック サーバ

重量：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）

動作湿度：5 ～ 93 %（結露しないこと）

A.3　電気仕様

該当する『Cisco UCS C220 Server Installation and Service Guide』の「Power Supply Specifications」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。

VMware は、最近のバージョン（ESXi 6.0 アップデート 3、6.5 アップデート 2 および 6.7）で変更を行っています。これにより、Cisco Meeting Server バージョン 2.8 での音声通話のスループットが低下しました（ビデオのキャパシティは影響を受けません）。次の表は、2.8 の新しいコール キャパシティの数値を示しています。

注：キャパシティの数値は、SCA（サイド チャネル対応）スケジューラのいずれのバージョンでもなく、デフォルトの ESXi スケジューラを使用することを想定しています（ESXi 6.7 により、スケジューラの 2 番目のバージョンが追加されます）。

表 3：コール キャパシティ

コールのタイプ	Cisco Meeting Server 2000	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5
フル HD 通話（1080p30）	350	48	48
HD 通話（720p30）	700	96	96
SD 通話（448p30）	1000	192	192
音声通話	3000	1700	2200

付録 B　シスコ ライセンス

Cisco Meeting Server とシスコのユーザ ライセンスにはアクティベーション キーおよびライセンスが必要です。シスコのライセンスを購入し適用する方法については、第 4 項を参照してください。

B.1 Cisco Meeting Server のライセンスとアクティベーション キー

次の機能を使用するには、Meeting Server にライセンスがインストールされている必要があります。

- Call Bridge
- 録画
- ストリーミング

バージョン 2.4 から、WebRTC アプリのログイン ページ、IVR メッセージ、SIP または Lync のコール メッセージまたは招待テキストに単一または複数のブランドを適用するためにブランドのライセンスを購入する必要がなくなりました。

XMPP アクティベーション キーは Cisco Meeting Server ソフトウェアに含まれています。

機能ライセンスの他にユーザ ライセンスも購入する必要があります。ユーザ ライセンスには次の異なる 3 種類があります。

- PMP Plus
- SMP Plus
- ACU

B.1.1 Call Bridge のアクティベーション キー

アクティベーション キーによって、Call Bridge をメディア コールに使用できます。アクティベーション キーを次の場所にインストールする必要があります。

- Cisco Meeting Server 1000
- Cisco Meeting Server ソフトウェアがインストールされ、結合サーバ導入（すべてのコンポーネントが同じサーバ上に存在する）として設定された VM サーバ
- Cisco Meeting Server ソフトウェアがインストールされ、分割サーバ導入の Core サーバとして設定された VM サーバ

コールを発信するには、Call Bridge をアクティブ化する必要があります。製品を評価するためにデモ ライセンスが必要な場合は、シスコのセールス担当者にお問い合わせください。

Acano X シリーズ サーバにアクティベーション キーは必要ありません。エッジ サーバとして設定された VM は、Call Bridge のアクティベーション キーは不要です。

ライセンス ファイルをアップロードした後に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設定する必要があります。これらの手順は、Cisco Meeting Server の設定の一部であり、Cisco Meeting Server 導入ガイドに記載されています。

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

B.1.2 録画

録画は、1 つのライセンスで 1 つの同時録画が許可されるライセンス キーによって制御されます。ライセンスは、レコーダーをホストしているサーバではなく、レコーダーに接続している Call Bridge をホストするサーバ（Core サーバ）に適用します。

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

録画ライセンス キーを購入するには、次の情報が必要です。

- 同時録画の数
- Call Bridge をホストするサーバ上のインターフェイス A の MAC アドレス

B.1.3 XMPP ライセンス

シスコ ミーティング アプリケーションをご利用のお客様は、XMPP サーバ アプリケーションを実行するサーバに XMPP ライセンスをインストールする必要があります。XMPP ライセンスは Cisco Meeting Server ソフトウェアに含まれています。また、XMPP サーバと同じ Cisco Meeting Server で有効化されている Call Bridge も必要です。

B.2　シスコのユーザ ライセンス

シスコのマルチパーティ ライセンスは Cisco Meeting Server で使用されるプライマリ ライセンス モデルです。引き続き、Acano 容量単位（ACU）を購入することができますが、マルチパーティ ライセンスと同じ Call Bridge では使用できません。ACU をマルチパーティ ライセンスに移行する必要がある場合は、シスコのセールス担当者にお問い合わせください。

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

B.2.1 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に対して、ネームド ホスト ライセンスを個別に割り当てます。このライセンスは、Cisco UWL Meeting（PMP Plus を含む）を通じて購入できます。Personal Multiparty Plus は、ビデオ会議向けのオールインワン ライセンスです。導入されている Cisco Meeting Server ハードウェアの制限内である限り、主催できる会議の参加者数に制限はありません。会議には、任意のエンドポイントから誰でも参加できます。ライセンスでは、フル HD 1080p60 品質までのビデオ、オーディオ、およびコンテンツ共有がサポートされています。

注：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に使用されます。

B.2.2 Shared Multiparty Plus ライセンス

Shared Multiparty Plus（SMP Plus）では同時ライセンスが提供されており、ビデオ会議を主催する頻度が低い複数のユーザが共有できます。SMP は、ルーム エンドポイントの購入時に UCM TP Room Registration ライセンスと共に割引価格で購入するか、あるいは個別に購入することができます。Shared Multiparty Plus は、Cisco UWL Meeting ライセンスを持たないすべての従業員が、ビデオ会議へのアクセスに使用できます。これは、導入しているルーム システムが多数の従業員によって共有される場合に最適です。Cisco UWL Meeting ライセンスの有無にかかわらず、すべての従業員が同じ機能を活用できます。たとえば、各自のスペースで会議を主催したり、アドホック会議を立ち上げたり、会議の予定を作成したりすることができます。共有ホスト ライセンスごとに 1 つの同時ビデオ会議がサポートされます。（導入されているハードウェアの制限内である限り）参加者数の制限はありません。各 Shared Multiparty Plus ライセンスには、Cisco Expressway 向けリッチ メディア セッション（RMS）ライセンスが 1 つ含まれています。このライセンスを使用して、Business-to-Business（B2B）ビデオ会議を実行できます。

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

Acano キャパシティ ユニット（ACU）は Cisco Meeting Server キャパシティ ユニットに名称変更されました。各キャパシティ ユニット（CU）は、12 個のオーディオ ポート、つまり表 4 に示した Cisco Meeting Server ソフトウェアへの同時メディア ストリームの品質をサポートしています。

表 4：キャパシティ ユニット ライセンス

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

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

B.3 シスコ ユーザ ライセンスの適用方法

スペースで会議を開始すると、シスコ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。

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

B.4　シスコ ユーザ ライセンスの設定

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

- /system/licensing オブジェクト。これは、Cisco Meeting Server のコンポーネントがライセンスを持ち、有効化されるかどうかを管理者が決定できるようにします。
- /system/multipartyLicensing オブジェクト。これには、使用可能なライセンスと使用中のライセンスの数が返されます。
- /system/multipartyLicensing/activePersonalLicenses オブジェクト。これは、Personal Multiparty Plus ユーザ ライセンスを使用しているアクティブ コールの数を示します。
- hostId パラメータ。このパラメータは /system/MPLicenseUsage（バージョン 2.6 以降）に追加されたものであり、ライセンス使用状況スナップショットの取得先となるホストを識別します。
- userProfile フィールド。このフィールドが LDAP 同期対象に含まれるようになりました。
- userProfile の hasLicense フィールド。これは、ユーザがライセンスを持っているかどうかを示します。
- ownerId および ownerJid フィールド。これらのフィールドは /coSpace オブジェクトごとに存在します。存在する場合、ownerId フィールドはこの coSpace を所有するユーザの GUID を保持し、ownerJid はユーザの JID を保持します。

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

付録 C ブランディング

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

- 背景イメージの WebRTC アプリ記号、サインイン ロゴ、サインイン ロゴの下のテキスト、ブラウザ タブのテキスト
- IVR メッセージ
- SIP および Lync の参加者のスプラッシュ画面イメージと、すべての音声プロンプトまたはメッセージ
- ミーティング招待状のテキスト

バージョン 2.4 からは、これらのカスタマイズ可能な機能に 1 つまたは複数のブランドを適用するためのライセンスは必要ありません。1 つのリソースセット（WebRTC アプリの 1 つのサインインページ、1 組の音声指示、1 つの招待テキスト）だけを指定した単一ブランドを適用する場合、それらのリソースは導入内のすべてのスペース、IVR、および Web Bridge に使用されます。複数のブランディングでは、異なるスペース、IVR、および Web Bridge に異なるリソースを使用できます。リソースは、API を使用してシステム、テナント、スペースまたは IVR のレベルで割り当てることができます。

付録 D　VM のサイジング

Cisco Meeting Server は最大の柔軟性を持つように設計されています。拡張性が非常に高く、最適化された Acano X シリーズ サーバと VM 導入を「組み合わせる」ことが可能になります。たとえば、エッジ サーバ上で VM を使用し、スケーラブルな分散アーキテクチャのコアで Acano X シリーズサーバを使用したり、VM 導入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に配置したりすることができます。

また、Cisco Meeting Server ソフトウェアが稼動可能なさまざまな標準サーバ/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）の導入で実行できます。たとえば、次のような場合です。

- 単一の VM はあらゆるコンポーネントを実行できます。
- 単一の VM では、Call Bridge やその他のコア コンポーネント（XMPP サーバ、H.323 ゲートウェイなど）を実行する Acano X シリーズ サーバに接続するエッジ コンポーネント（Web Bridge、TURN サーバ、ロード バランサ）を実行できます。
- エッジ コンポーネントが稼動する VM に、Call Bridge などのコア コンポーネントが稼動する別の VM を接続。

図 3 に、Cisco Meeting Server の各ソフトウェア コンポーネントと標準的な導入を示します。各インスタンスは、VM または Acano X シリーズ サーバ上に配置できます。

図 3：Cisco Meeting Server の各ソフトウェア コンポーネントと標準的な導入

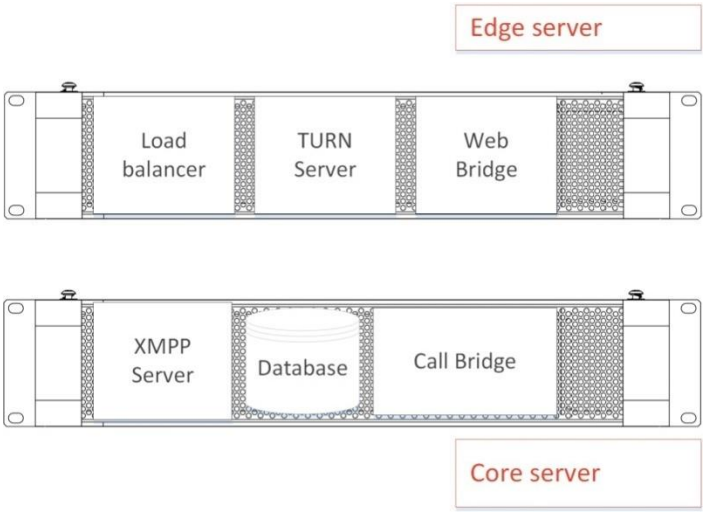
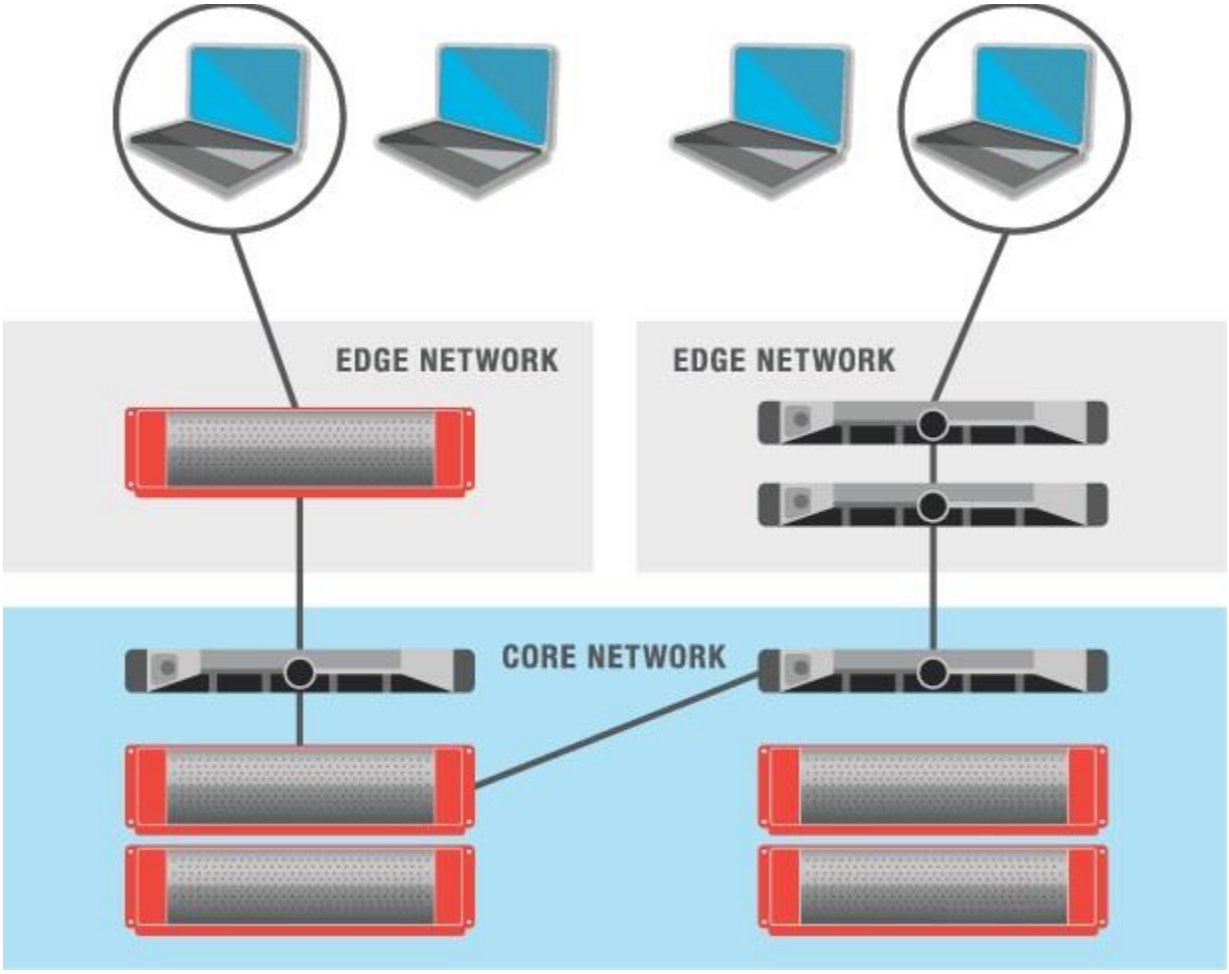


図 4 に、VM と Acano X シリーズ サーバの両方を使用した、Cisco Meeting Server の分散型導入を示します。2 つのシスコ ミーティング アプリケーションのシグナリングとメディア パスの例を示しています。

図 4：VM と Acano サーバの両方を使用した分散型 Acano 展開



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 エクスペリエンスが実現できます。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。

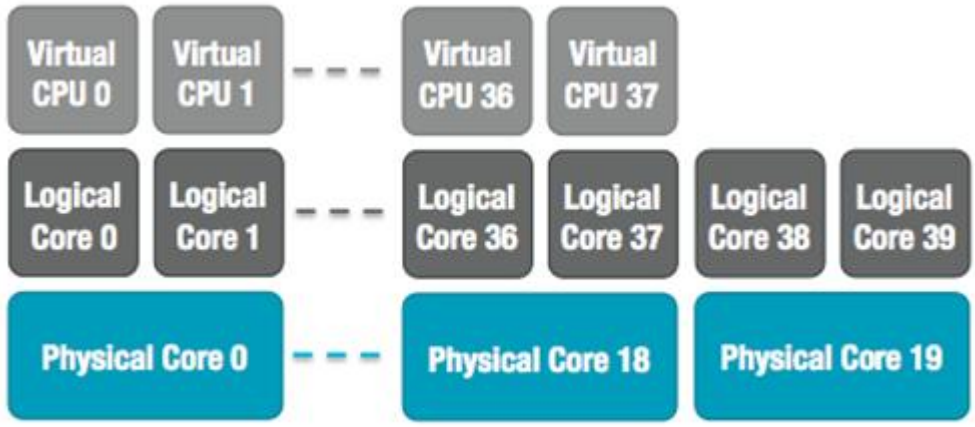
D.1　Call Bridge VM

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、およそ 2.5 の 720p30 H.264 コール レッグを処理できます。処理能力は 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。ハイパースレッドが有効になっている場合、使用可能な論理コアの数は物理コアの 2 倍になるため、上記のデュアル E5-2680v2 システムでは仮想 CPU の数が 40 個になり、そのうち 38 個を VM に割り当てる必要があります。ソケット数とソケットあたりのコア数の両方を選択できる場合、すべての仮想 CPU コアを使用して 1 個のソケットを構成する必要があります。

図 5：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。上記の推奨事項に従って正しく設定された Cisco Meeting Server VM は、処理能力を超えた場合、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。

基盤となる物理 CPU コアごとに 1 GB の RAM を VM に割り当てる必要があります。上記のシステムでは、使用中の 19 個の物理 CPU コアに対応し、VM を 19 GB で設定する必要があります。

D.2　エッジ VM

他のコンポーネントの要件は Call Bridge VM ほどは高くありません。分割コア/エッジ導入の VM であってもエッジ VM でエッジ機能（Web Bridge、TURN サーバ、ロード バランサ）を実現できます。このエッジ VM は、コア VM またはコアとして設定された Acano X シリーズ サーバとつなぐことができます。

Acano X シリーズ サーバにエッジ サービスを提供するための VM は、8 個以上の仮想 CPU と 8 GB 以上の RAM で構成する必要があります。単一コア VM にエッジ サービスを提供する VM は、最低 4 個の仮想 CPU と 4 GB の RAM で構成する必要があります。

D.3　データベース VM

注：この項の内容は、1 つ以上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。

- 4 つの vCPU、8 GB の RAM、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、導入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る Cisco UCS C220 を使用することもできますが、VM データベースが使用するサーバ リソースの全体に占める割合はごくわずかです。このサーバを使用する場合、必要に応じて他の VM も VM データベースと同じサーバ上でホストできます。

D.4　レコーダとストリーマの VM

レコーダとストリーマの実稼働での使用には、専用の VM で稼働させるか、レコーダ/ストリーマが組み合わされた VM の一部として稼働させる導入環境が推奨されます。

ストリーマ専用の場合、VM は 720p30 の同時録画につき 1 個の vCPU および 0.5 GB のメモリで、また 6 個の同時ストリームにつき 1 個の vCPU および 1GB のメモリでサイズ調整し、vCPU は最小で 4 個、最大で 32 個備えている必要があります。

レコーダ専用の場合、VM は 720p30 の同時録画につき 1 個の vCPU および 0.5 GB のメモリでサイズ調整し、vCPU は最小で 4 個、最大で 24 個備えている必要があります。レコーダは、さまざまなビット レートを使用するため、録画にどれくらいストレージが必要かを正確に予測することはできません。シスコのテストでは、サイズが 720p30 の録画で 1 時間に 300 ～ 800 MB の使用が確認されました。予測する場合は、1 時間あたり 1 GB を想定しておけば安全です。

レコーダとストリーマを組み合わせる場合、VM は 720p30 の同時録画につき 1 個の vCPU および 0.5 GB のメモリで、また 6 個の同時ストリームにつき 1 個の vCPU および 1GB のメモリでサイズ調整し、最小で 4 個、最大で 24 個の vCPU を備えている必要があります。

注：単一のホストで複数の仮想マシンを実行する場合、第 D.1 項の共存ルールに従う必要があります。遅延感度機能を使用する場合、レコーダ/ストリーマの VM は「High」に設定する必要があります。

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。そうすることで、ESXi カーネルが管理とネットワーク運用に CPU コアを使用できるようになります。

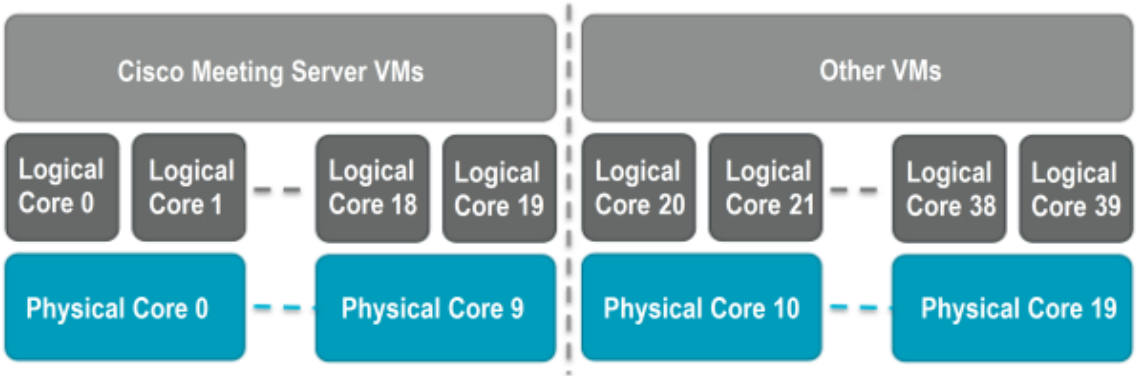
社内テストの一部として、定期的にさまざまな CPU 構成とサーバ構成の性能を測定しています。これらのテスト時には、徐々に模擬コールを追加し、VM に対する要求が少しずつ増加して処理能力を超えるようにします。ユーザ エクスペリエンスを保証するため、複数の統計情報を監視しています。さらに ESXi の統計情報も監視し、診断ログを収集しています。

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、この処理能力を提供するには 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 で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 スケジューラ用に、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もあります。

図 6：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 vMotion と VMware High Availability（HA）の各テクノロジーは、すべてサポートされます。VMware Fault Tolerance（FT）は、1 個の仮想コアの 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すべてサポートされます。

注：EVC モードが有効化された VMware ハイパーバイザが使用されている場合、EVC は次のモードのいずれか以上に設定する必要があります。

「B1」/AMD Opteron™ Generation 4

「L2」/Intel® Nehalem generation（旧製品名 Intel® Xeon Core™ i7）

上記よりも古い CPU との互換性が求められる EVC モードは、SSE 4.2 が無効化されるためサポートされません。ここでは SSE4.2 が必要です。

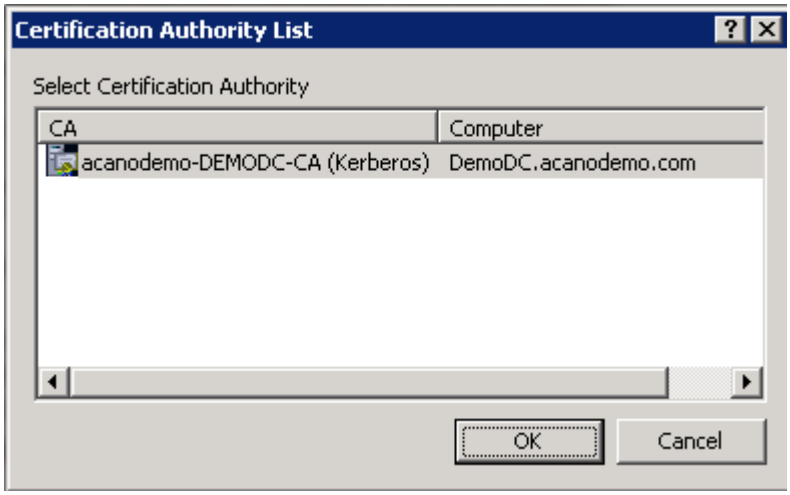
付録 F　ローカル認証局によって署名された証明書の作成

この付録では、Active Directory Certificate Services のロールを持つ Microsoft Active Directory サーバなどの ローカル CA を使用して、CSR に署名する手順について説明します。

1. ファイルを CA に転送します。
2. CA サーバ上のコマンド ライン管理シェルで次のコマンドを発行します。コマンドのパスと CSR 名は適切な内容に置き換えます。

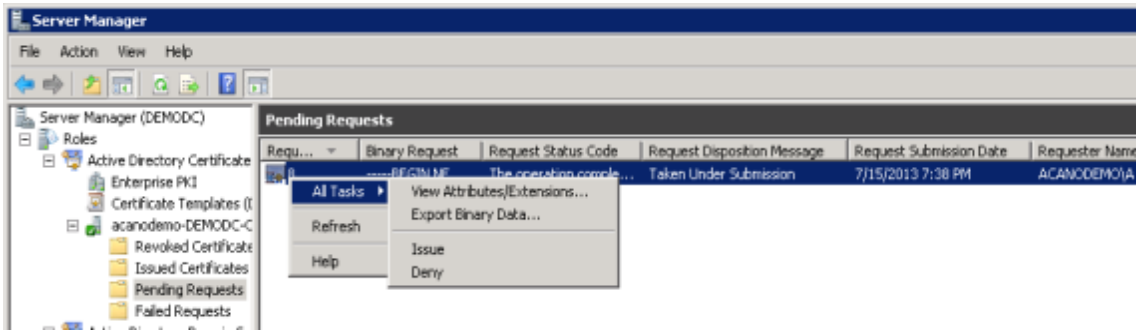
   ```
   certreq -submit -attrib "CertificateTemplate:WebServer"
   C:\Users\Administrator\Desktop\webadmin.csr
   ```

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。適切な CA を選択し、[OK] をクリックします。

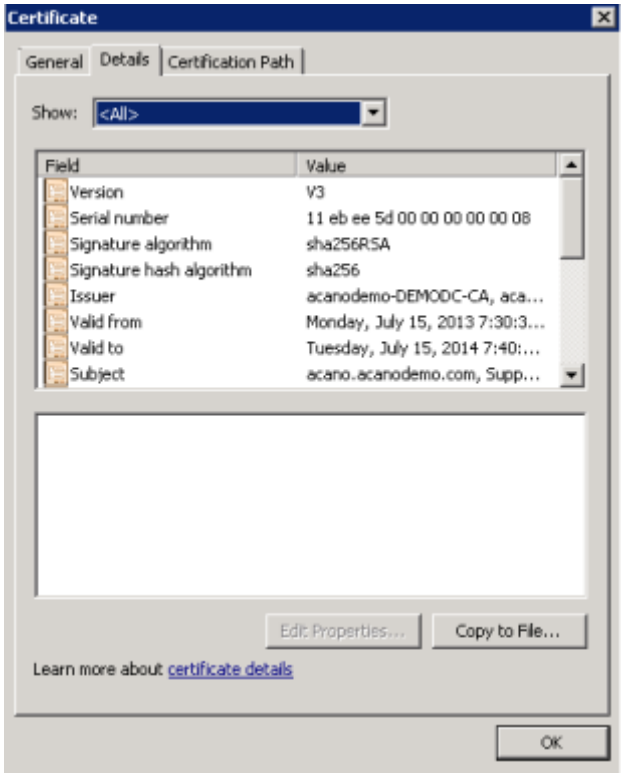


4. 次のいずれかを実行します。
   - ご使用の Windows アカウントに証明書を発行する権限がある場合、生成された証明書（webadmin.crt など）を保存するためのプロンプトが表示されます。下の手順 c に進みます。
   - 生成された証明書を発行するためのプロンプトが表示されない場合、代わりにコマンド プロンプト ウィンドウに「証明書の要求は保留中です：提出済みです（Certificate request is pending: taken under submission）」というメッセージが表示され、「要求 ID（Request ID）」がリスト表示されます。RequestID をメモしてから、下記の手順を実行し、その後手順 c に進みます。

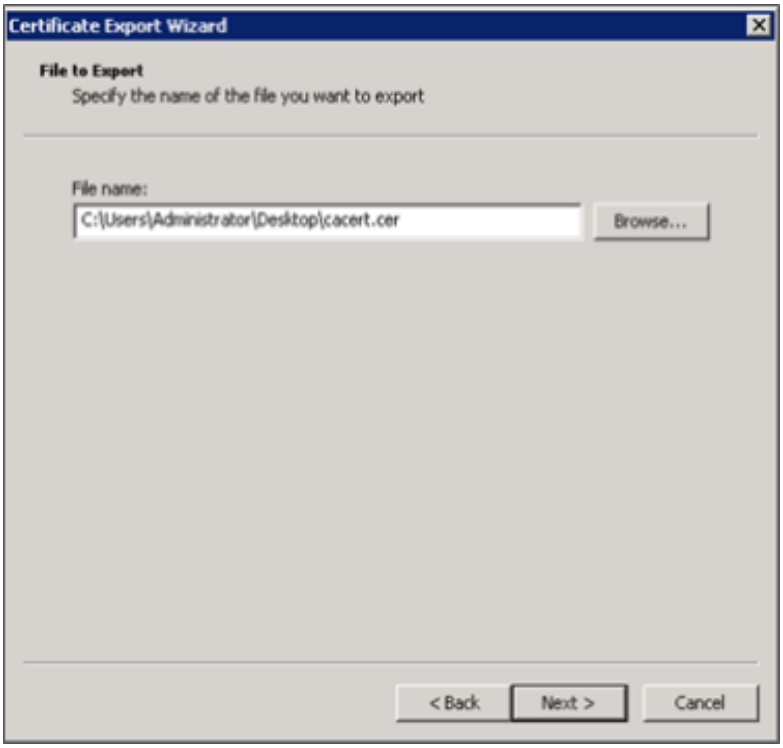
5. CA の [Server Manager] ページで、CA のロールの下にある Pending Requests フォルダを見つけます。
6. CMD ウィンドウに表示された要求 ID に一致する保留中の要求を右クリックして、[すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。



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



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



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

SFTP を使用して証明書（webadmin.crt など）と秘密キーを Cisco Meeting Server の MMP へ転送します。当該の項を参照してください。

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

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、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任となります。

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

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。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とソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

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

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと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 トポロジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

このドキュメントのすべての印刷版と複製ソフトは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。

シスコの商標