Cisco Meeting Server

Cisco Meeting Server リリース 3.10

MMP コマンド ライン リファレンス

2024 年 9 月 27 日

目次

変更履歴

日付	変更の概要
2024 年 9 月 27 日	Cisco Meeting Server 3.10 ソフトウェアの新しいバージョン。
2024 年 3 月 5 日	Cisco Meeting Server 3.9 ソフトウェアの新しいバージョン。 「MMPの追加と変更の概要」を参照してください。
2023 年 9 月 7 日	Cisco Meeting Server 3.8 ソフトウェアの新しいバージョン。 「MMPの追加と変更の概要」を参照してください。
2023 年 3 月 16 日	Cisco Meeting Server 3.7 ソフトウェアの新しいバージョン。 MMP の追加と変更の概要を参照してください。
2022 年 10 月 19 日	軽微な修正。
2022 年 8 月 23 日	Meeting Server 3.6 ソフトウェアの新しいバージョン。 「MMP の追加と変更の概要」を参照してください。
2022 年 4 月 20 日	ミーティングサーバ 3.5 ソフトウェアの新しいバージョンです。 「MMP の追加と変更の概要」を参照してください。
2021 年 12 月 21 日	「TLS 証明書の検証セクション」のコマンドの説明のリンクを更新しました。
2021 年 12 月 15 日	Meeting Server 3.4 ソフトウェアの新しいバージョン。 「MMP の追加と変更の概要」を参照してください。
2021 年 8 月 24 日	Meeting Server 3.3 ソフトウェアの新しいバージョン。
2021 年 5 月 19 日	Medium OVA Expressway の推奨事項でドキュメントを更新しました。
2021 年 4 月 16 日	「2.1 Network Interface（iFace）コマンド」のセクションで Interface コマンドの MTU を移動しました。 MTU 情報に関するメモを更新しました。
2021 年 4 月 9 日	Meeting Server 3.2 ソフトウェアの新しいバージョン。
2021 年 3 月 16 日	完全にサポートされている機能であるミーティングサーバ上の短期資格情報についてドキュメントを更新しました。
2020 年 12 月 4 日	pcap セクションにメモを追加しました
2020 年 11 月 30 日	バージョン 3.1 ソフトウェアの新しいバージョン
2020 年 10 月 15 日	re. MTU 情報に明確化するためのメモを追加しました。 その他軽微な修正。
2020 年 9 月 11 日	軽微な修正。
2020 年 8 月 21 日	軽微な修正。
2020 年 7 月 29 日	バージョン 3.0 ソフトウェアの新しいバージョン

1 はじめに

Cisco Meeting Server ソフトウェアは、Cisco Unified Computing Server (UCS) テクノロジに基づく特定のサーバ、または仕様ベースの VM サーバでホストできます。 本ドキュメントでは、Cisco Meeting Server を Meeting Server と呼びます。

メモ: Cisco ミーティングサーバソフトウェアバージョン 3.0 以降は X シリーズサーバをサポートしていません。

Cisco ミーティングサーバには、プラットフォームとアプリケーションの 2 つのレイヤーがあります。 プラットフォームは、メインボード管理プロセッサ (MMP) を通じて構成されます。 アプリケーションは、独自の設定インターフェイスを持つこの管理プラットフォーム上で実行されます。

MMP は、低レベルのブートストラップと構成に使用されます。 コマンドライン インターフェイスを提供します。 Cisco ミーティングサーバ 2000 では、MMP コマンドラインインターフェースは Serial Over LAN 接続を通してアクセスされます。 仮想化された展開 (Cisco ミーティングサーバ 1000、および仕様ベースの VM サーバ) では、MMP は仮想インターフェイス A でアクセスされます。

アプリケーションレベルの管理 (通話とメディアの管理) は API 経由で実行されます。簡単な展開の場合はウェブ管理インターフェイス経由で実行できます。ウェブ管理インターフェイスは利用可能なイーサネットインターフェイスのいずれか 1 つ上で実行するように設定できます。

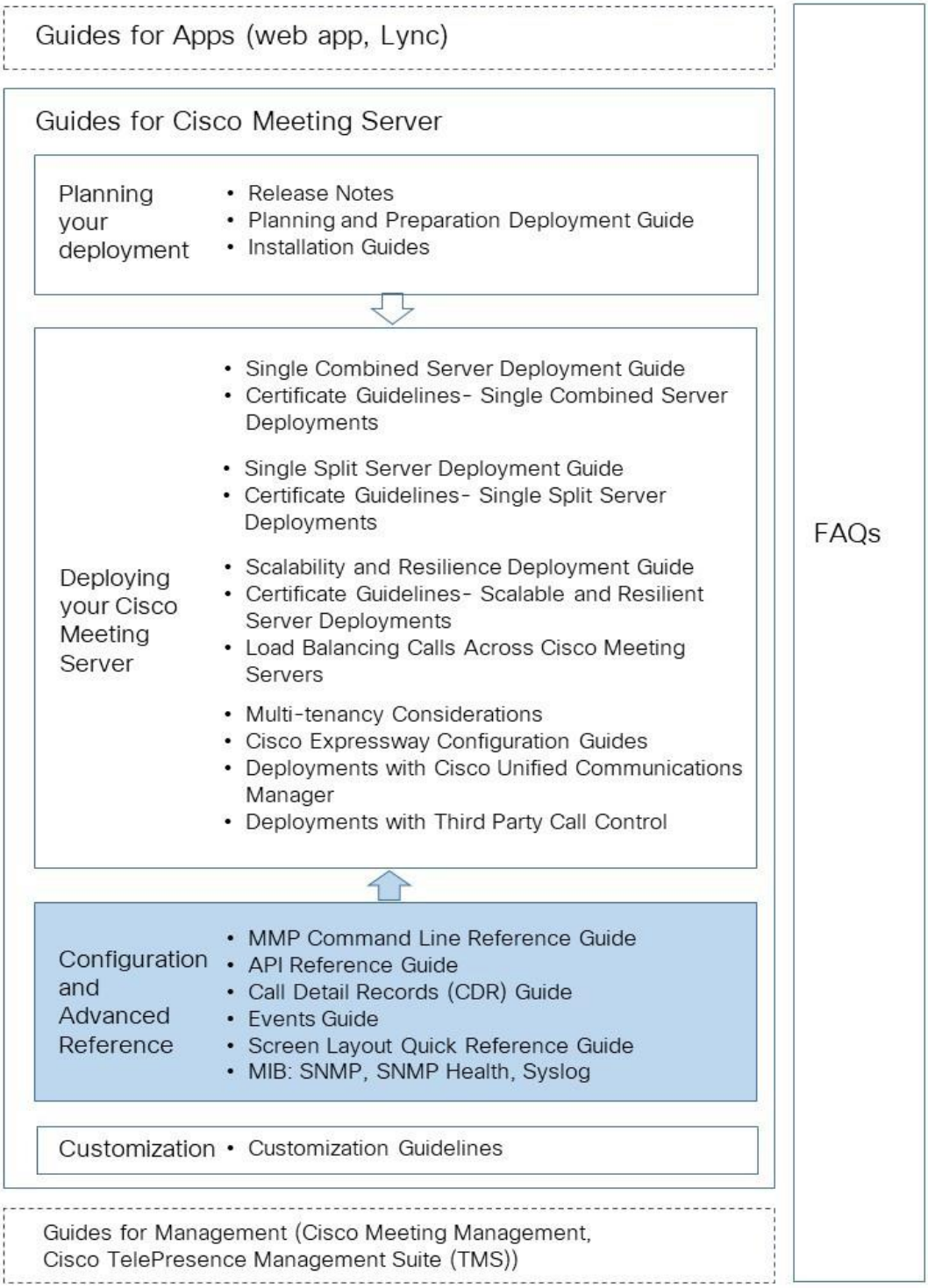
メモ: 以降、本書では Cisco ミーティングサーバソフトウェアを指すことを「ミーティングサーバ」と呼びます。

1.1 このドキュメントの使用方法

このガイドでは MMP について説明します。特に記載がない限り、情報は Cisco Meeting Server 2000、Cisco Meeting Server 1000、および仮想化展開に等しく適用されます。

これらのドキュメントは、cisco.com でご確認いただけます。

図 1: Cisco ミーティングサーバのドキュメント (バージョン 3.10 用)



1.2 MMP にアクセスする

1.2.1 Cisco ミーティングサーバ 2000

Cisco Meeting Server 2000 上の Serial Over LAN 接続を介して MMP コマンドライン インタフェースにアクセスします。MMP を使用する前に、Serial Over LAN 接続で IP アドレスと資格情報を設定する必要があります。 Serial Over LAN 接続の設定の詳細は、『Cisco Meeting Server 2000 インストールガイド』を参照してください。

初期構成後、SSH クライアントを使用して Serial Over LAN 接続の IP アドレスに接続し、構成された管理アカウントの資格情報を使用して MMP にログインします。

1.2.2 仮想化された展開 (Cisco Meeting Server 1000 および仕様ベースの VM サーバ)

仮想化された展開では、MMP は VSphere コンソールタブ (仮想インターフェイス A) からアクセスされ、MMP 管理者ユーザのログイン資格情報を必要とします (「MMP ユーザアカウント コマンド」を参照してください)。 これらはインストール手順の一部としてセットアップされます。「仮想化展開のための Cisco Meeting Server インストール ガイド」を参照してください。

1.2.3 Cisco Meeting Server プラットフォーム間の特定のコマンドの違い

実行中の Cisco Meeting Server 2000 と 仮想化 Cisco Meeting Server には違いがあります。

コマンド	Cisco Meeting Server 2000	Cisco Meeting Server 1000 および仮想 Cisco Meeting Server
shutdown	MMP では利用できません。 電源を切る前に、Cisco UCS マネージャを使用して、ブレードサーバの電源を 切ってください。	vSphere の電源ボタンは使用しないでください。 **シャットダウン** コマンドを使用してください。
状態	MMP では利用できません。 Cisco UCS Manager	使用不可
シリアル番号:	サーバのシリアル番号を返します。	使用不可
dns	インターフェイスを指定しないでください。 例 **dns add forwardzone <domain-name> <server ip>**	インターフェイスを指定しないでください。 例 **dns add forwardzone <domain-name> <server ip>**
user evict	バージョン 2.9 から利用可能	応答可能

1.3 MMP 間のファイル転送

Secure File Transfer Protocol（SFTP）を使用すると、MMP 間でファイルを転送できます。Windows では、WinSCP (http://winscp.net/eng/index.php) を推奨しますが、どのクライアントでも使用できます。 SFTP は次のファイルの転送に使用されます:

- ソフトウェア アップグレード イメージ
- 構成のスナップショット
- セキュリティ証明書
- ライセンスファイル
- システムログファイル (Cisco サポートの指示による)
- クラッシュ診断ファイル (Cisco サポートの指示による)

ipv4 MMP 、または **ipv6** MMP コマンド（状況に応じて適切な方）を使用して、SFTP クライアントを MMP のIP アドレスに接続します。 MMP 管理者ユーザの資格情報を使用してログインします (MMP ユーザアカウントコマンドを参照してください)。

1.3.1 SFTP クライアントで確認できるファイル

設定後、SFTP を使用して MMP にアクセスすると、以下のファイルが表示されます (license.dat 以外はすべて異なる名前である可能性がありますが、以下はインストールおよび展開ガイドで使用されるファイル名の例です):

- Server.crt、webbridge.crt
- license.dat (必須の名前)
- boot.json および live.json
- server.key、webbridge.key
- cacert.pem、privkey.pem、server.pem

1.4 利用できる MMP コマンドは?

利用可能なコマンドとそのパラメータの一覧を表示するには、次のコマンドを入力します:

help

1 つのコマンドタイプの詳細を表示する：

help<コマンド名>

これらのコマンドについては以下のセクションで説明されています。 すべてのコマンドは、MMP コマンドラインインタフェースのプロンプトから入力します。 以下に例を示します。

iface (a|b|c|d) <speed> (on|off)

ここで

() はオプションの選択肢を示し、そのうちの 1 つを使用 – 括弧なし

<> は適切な値を入力する必要があるパラメータを示し、

[ ] はオプションのパラメータを示します

一部のコマンドの後には、同じ表セル内で 1 つまたは複数の青色で例が示されています。

コマンド/例	説明/メモ
iface (a|b|c|d)	指定したインタフェースのネットワークインタフェース構成を表示します A、B、C、および D インターフェイスは、全二重自動ネゴシエーションに制限されていることに注意してください。

1.5 MMP コマンドの記述と補完

MMP コマンドでは次の機能を使用できます:

- Tab: Tab キーを押してコマンドをオートコンプリートします。 たとえば、**help ti** とタイプした後に Tab キーを押すと、**help timezone** が作成されます。 しかし、可能なコマンドが複数ある場合、Tab をもう一度押しても代替コマンドは提供されません。 たとえば、**help we** の後に、Tab キーを押すと、**help webadmin** が指定され、もう一度押すと、**help webbridge** は指定されません。
- 左および右矢印キー 入力したコマンド行に沿ってカーソルを移動する
- 上下矢印キーでコマンド履歴を循環

- 二重引用符: 複数の単語を入力する場合は、"" を使用します。例:

```
pki csr デモ CN:"callbridge.example.com" OU:"Cisco Support" O:Cisco L:
"New York" ST:NY C:US
```

キーボードのショートカットを使用できます：

- CTRL-p: 前のコマンドを表示します
- CTRL-n：コマンド履歴の次のコマンドを表示します
- CTRL-d：カーソルの下の文字を削除するか、空の行で使用した場合、終了します
- CTRL-c：現在実行中のコマンドを中止します
- CTRL-a：行の先頭に移動します
- CTRL-e：行末に移動します
- CTRL-l：ターミナルを消去します
- CTRL-k：カーソル位置から行末までを削除します
- CTRL-m：Return キーと同じです
- CTRL-w: カーソルの左にある単語を削除する
- CTRL-u: 現在の行を削除する
- CTRL-f：一文字前に移動します
- CTRL-b: 文字を後方に移動する
- CTRL-t: 現在の文字と前の文字を入れ替える

1.6 予約済みポート

ポート 8081 は、webadmin が有効な場合、ループバックで予約されますが、webadmin が無効な場合、予約されません。 ポート 8080 は常に開いています。

ポート 5060 は常に開いていますが、ポート 5061 は、証明書が Call Bridge に適用されている場合にのみ開いています。

2 ネットワークコマンド

2.1 Network Interface（iface）コマンド

コマンド/例	説明/メモ
iface (a|b|c|d)	指定したインタフェースのネットワークインタフェース構成を表示します A、B、C、および D インターフェイスは、全二重自動ネゴシエーションに制限されていることに注意してください。
iface <interface> mtu <value> **iface a mtu 1400**	インターフェイスの最大転送ユニットサイズをバイトで設定します。 **メモ：**すべての Meeting Server 2000 デプロイ、および VMWare バージョン 6.7U2 以降を実行している VM および Meeting Server 1000 デプロイでは、MTU は受信パケットと送信パケットの両方のパケットに適用されます。 設定された MTU より大きい受信パケットはインタフェースによりドロップされ、パケット損失および低品質の原因となり、まれに接続の問題が発生します。 6.7U2 以前の VMware バージョンを実行している VM および Meeting Server 1000 デプロイでは、MTU は発信パケットにのみ適用され、設定された MTU より大きいパケットはインターフェイスで受信できます。 デフォルトの MTU は 1500 バイトです。 これらの MTU 制限によりインターフェイスがパケットをドロップしないよう、ネットワークで MTU を設定する必要があります。

2.2 IP コマンド

2.2.1 IPv4 コマンド

コマンド/例	説明/メモ
ipv4 (a|b|c|d)	設定と観察されたネットワーク値を一覧します
ipv4 (a|b|c|d) dhcp	指定されたインターフェイスで dhcp を有効にします
ipv4 (a|b|c|d) (enable|disable)	指定されたインターフェイスを有効または無効にします メモ：このコマンドは設定を消去せず、無効にするだけです。
ipv4 (a|b|c|d) add <server IP address>/<Prefix Length> **<デフォルトゲートウェイ>** **ipv4 a add 10.1.2.3/16 10.1.1.1**	指定されたプレフィックスの長さとエグレスパケットのデフォルトゲートウェイを持つインターフェイスに IPv4 アドレスを設定します。 この例では、A をアドレス 10.1.2.3 でサブネット 10.1.0.0/16 に設定しています。 これ以上特定のルートがない場合、A から出るパケットは、ゲートウェイ 10.1.1.1 経由で送信されます。
ipv4 (a|b|c|d) del <server IP address>	指定されたインターフェースの IPv4 アドレスを削除します
ipv4 (a|b|c|d) デフォルト	アウトバウンド接続のラストリゾートのインターフェイスを選択します。 リモートホストに接続するとき、どのインタフェースが使用されるべきか、コンテキストから常に認識されるわけではありません。 対照的に、リモートホストによって開始された接続への応答は、接続が受け入れられたインタフェースを使用します。 これは、強力な IP モデルと呼ばれることがあります。
ipv4 (a|b|c|d) route add <address>/<prefix length> ipv4 (a|b|c|d) route del **<アドレス>/<プレフィックスの長さ>** **ipv4 b route add 192.168.100.0/24**	スタティック ルートを追加して、特定のインターフェイスから特定のサブネットをルーティングできるようにします。 これは、複数のインターフェイスが有効になっていて、特定のサブネットのトラフィックが特定のインターフェイスのゲートウェイにルーティングされるようにする固有のルーティング シナリオ用です。 メモ: 通常、デフォルトルートの手動設定は必要ではなく、問題が発生する可能性があります。 192.168.100.x 宛てのすべてのトラフィックは、インターフェイス b からインターフェイス b のゲートウェイへとルーティングされます

2.2.2 IPv6 コマンド

ミーティングサーバは、インタフェースごとに複数の IPv6 アドレス、自動設定されたアドレスと静的アドレスをサポートします。

コマンド/例	説明/メモ
ipv6 (a|b|c|d)	設定と観察されたネットワーク値を一覧します
ipv6 (a|b|c|d) を有効にする	指定されたインタフェースの IPv6 の自動設定を開始します。リンクローカルアドレスが生成されます。 重複アドレス検出 (DAD) が完了し、SLAAC が有効になっている場合、ルーター要請が送信されます。 ルーター通知を受信した場合、 • 通知されたプレフィックスは、グローバル アドレスの構築に使用されます。 • 任意の RDDNS オプションを使用して DNS を設定します • 「管理対象」または「その他」のフラグが設定されている場合、DHCPv6 が開始されます。 ルーター通知に「管理」または「その他」のビットが設定されていない場合、DHCPv6 は使用されません ルーター要請が 3 回送信された後にルーター通知が受信されない場合、DHCPv6 が開始されます。
ipv6 (a|b|c|d) disable	指定されたインターフェースで IPv6 を無効にする
ipv6 <interface> slaac (enable|disable)	SLAAC を有効/無効にします
ipv6 (a|b|c|d) add <アドレス>/<プレフィックスの長さ> ipv6 a add 2001::2/64	SLAAC が無効になっている場合、静的アドレスと静的ルーターアドレスを追加する必要があります。 静的ルーターを追加するには、SLAAC が検出したアドとルーターが静的に設計されたアドレスと共存できることに注意してください。 ミーティングサーバは、自動設定されたアドレスと静的アドレスをサポートしています。 指定されたインターフェイス上に IPv6 アドレスを静的に設定するには、このコマンドを使用します
ipv6 (a|b|c|d) del <address> **ipv6 a del 2001::2/64**	IPv6 アドレスを削除します
ipv6 <interface> router add|del <アドレス>	

2.3 ネットワーク診断コマンド

2.3.1 IPv4 ネットワーク診断コマンド

IPv4 を有効にすると、次のコマンドを使用できます。

コマンド/例	説明/メモ
ping<ターゲットアドレス|ホスト名>	ミーティングサーバからターゲット IP アドレスまたはホスト名への ping
traceroute <target address|hostname>	Meeting Server から対象の IP アドレスまたはホスト名にトレースルートします

2.3.2 IPv6 ネットワーク診断コマンド

IPv6 を有効にすると、次のコマンドを使用できます。

コマンド/例	説明/メモ
ping6 <target address|hostname>	ミーティングサーバからターゲット IPv6 アドレスまたはホスト名への ping
traceroute6 <target address|hostname>	Meeting Server から対象の IPv6 アドレスまたはホスト名にトレースルートします

2.3.3 パケットキャプチャ

メモ：Meeting Server でパケットをキャプチャできても、Meeting Server が操作する高いパケットレートにより、パケットは、通話処理時の Meeting Server の通常運用を妨げるのではなく、パケットキャプチャからドロップされる場合があります。 パケットキャプチャでのパケットのドロップを避けるため、Cisco は Meeting Server 上ではなく、ネットワークスイッチでパケットをキャプチャすることを推奨しています。

コマンド/例	説明/メモ
pcap (a|b|c|d)	指定したインターフェイス上で即時パケットキャプチャを開始し、Ctrl-C を押すと停止します。 Pcap ファイルの名前が表示されます。 このファイルは SFTP 経由でダウンロードできます。 **pcap** コマンドは、ローテーションで複数ファイルのパケットをキャプチャします。 Pcap ファイルのサイズが 500MB を超えると、パケットは新しいファイルにキャプチャされます。 Meeting Server は、最大 4 つの pcap ファイルを保存し、一度に保存できる合計最大ファイルサイズは 2GB です。 4 番目の pcap ファイルのサイズが 500MB を超えると、最も古い pcap ファイルが削除され、新しいファイルでパケットのキャプチャが続行されます。
pcap (a|b|c|d|any) [snaplen <n>] [filter<pcap-filter-expression>]	**any** 、複数のインターフェイス、つまり全ての有効なインターフェイスでパケットキャプチャを許可します（有効になっていないインターフェイスはスキップされます）。 **メモ**: 複数のインタフェースからキャプチャする場合、各インタフェースは別の一時ファイルにキャプチャされ、キャプチャが停止したときにファイルがマージされるため、追加のディスク容量が必要です。 そのため、複数のインターフェイスでキャプチャするときに使用できるストレージは、単一のインターフェイスでキャプチャするときに使用できるストレージの半分になります。 **snaplen** は、キャプチャされた各パケットが最大数（n）のバイトを超える場合、その長さで切り捨てられます。 結果として、より多くのパケットを同じファイルサイズ制限に収めることができます。 **filter** は、文字列の貢献に一致するパケットのみを選択します。 これにより、キャプチャ対象のパケットのみが減り、他のパケットでディスク スペースが無駄に消費されることがなくなります。 この文字列の解析とパケットフィルタリングは、tcpdump で使用されるものとまったく同じライブラリで実行されるため、これはまったく同じ表現力とパフォーマンスを持ちます。 必要に応じて、フィルタ式は約 4080 文字まで入力できます。 **snaplen** および **filter** オプションは、バージョン 3.1 から追加されました。

2.4 QoS/DSCP コマンド

Meeting Server は、（TOS ではなく）DSCP Hex の QoS/DSCP 値をサポートします。 すべての値が標準というわけではありませんが、下位互換性のために 0 から 63 の任意の DSCP 値を許可するという米国連邦政府機関の要件に従います。

10 進数、16 進数（大文字と小文字の区別なし）、8 進数の入力をサポートしています。それぞれ、46、0x2E（または 0x2e）、056 を入力しても、結果は同じです。

たとえば、EF 音声、AF31 シグナリング/データ、AF41 ビデオは次のとおりです。

EF = 0x2E DSCP Hex、AF31 = 0x1A DSCP Hex、AF41 = 0x22 DSCP Hex

DSCP 設定は、IPv4 と IPv6 で独立した値で定義できます。 例えば、oa&m を IPv4 には 0x4 および IPv6 には、0x6 に設定すると、SSH トラフィックは IPv4 接続では 0x4、IPv6 接続では 0x6 でマークされます。

メモ：変更を有効にするにはサービスのリスタートが必要です。Core サーバーを再起動することが推奨されます。

コマンド/例	説明/メモ
dscp (4|6) <traffic type> (<DSCP value>|none)	DSCP トラフィックを設定します。 DSCP トラフィック カテゴリとこれらのカテゴリ内のトラフィック タイプは次のとおりです。 ▪ シグナリング (SIP、AS-SIP シグナリング) ▪ 保証された音声（AS-SIP の任意の音声） ▪ 音声 (その他の音声) ▪ 保証型マルチメディア（AS-SIP のビデオ） ▪ マルチメディア（その他のビデオ） ▪ マルチメディアライブ配信（webbridge メディア）（現在は使用されていません） ▪ 低遅延（現在は使用されていません） ▪ oa&m（ウェブ管理、LDAP、SSH、SFTP） （oa&m = 運用、管理、およびマネジメント）
dscp 4 voice 0x2E **dscp 4 voice 46**	
DSCP 4 oa&m 0x22	IPv4 用の oa&m を設定
DSCP 4 oa&m なし	設定を削除します
dscp assured (true|false)	「音声」および「マルチメディア」トラフィックタイプに対して、保証型および非保証型 DSCP 値の両方を設定することが可能です。上記を参照してください。 このコマンドを使用して、保証型値または非保証型値の使用を強制します。
dscp assured true	たとえば、すべての音声とビデオデータに対して保証された音声と保証されたマルチメディア DSCP 値の使用を強制するために、このコマンドを使用します。

3 DNS コマンド

コマンド/例	説明/メモ
dns	現在の DNS 構成の詳細を表示します
dns add forwardzone <domain-name> <サーバ IP> **dns add forwardzone example.org 192.168.0.1**	順ゾーンを設定します。 順ゾーンは、ドメイン名と少なくとも 1 つのサーバアドレスで構成されるペアです。 名前が DNS 階層で指定されたドメイン名より下にある場合、DNS リゾルバーは指定されたサーバにクエリを実行できます。 任意の特定のドメイン名に対して複数のサーバーを指定して、ロードバランシングとフェイルオーバーを提供できます。 「.」を指定するのが一般的です。これは、すべてのドメイン名に一致する DNS 階層のルート、つまりドメイン名を意味します。
dns del forwardzone <domain-name> <サーバ IP>	指定された forward zone を削除します
dns add trustanchor <anchor> **dnsadd trustanchor ". IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5"**	Domain Name System Security Extensions（DNSSEC）にトラストアンカーを追加します。 トラストアンカーは、引用符で囲まれた DNS リソースレコードフォームで指定する必要があります - 例を参照してください。 詳細については、[1] を参照してください。
dns del trustanchor <zonename> **dns del trustanchor**	トラストアンカーを削除します。 zonename は、アンカーを表すリソース レコード (RR) 中のドメイン名です。 この例では、上記の例でインストールされたトラスト アンカーを削除します。

コマンド/例	説明/メモ
dns add rr <DNS RR> **dns add rr "sipserver.local. IN A 172.16.48.1"** **dns add rr "_sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.local."**	外部 DNS サーバで構成されていない、またはオーバーライドする必要がある値を DNS リゾルバーが返すように構成するには、外部 DNS サーバにクエリする代わりに返されるカスタム リソース レコード (RR) を構成できます。 次の形式の引用符で囲まれた RR を受け入れます。 **OWNER <OPTIONAL TTL> CLASS TYPE TYPE-SPECIFIC-DATA** たとえば、 A records sipserver.local. IN A 172.16.48.1 AAAA records example.com. aaaa 3ffe:1900:4545:2:02d0:09ff:fef7:6d2c SRV records _sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.local メモ：単一のレコードタイプに複数の RR を作成したい場合、外部 DNS サーバーを使用して作成する必要があります。 ミーティングサーバは単一のレコードタイプで複数の RR をサポートしておらず、最新の RR のみを保存します。たとえば、Meeting Server は 1 つの SRV レコードのみを保存します。 _sipinternaltls._tcp などは、_sipinternaltls._tcp に対して、2 つの異なる RR を保存しません。
dns del rr <owner-name> <type> **dns del rr _sip._tcp.example.com. SRV dns del rr sipserver.local. A**	
dns lookup <a|aaaa|srv> <hostname> **DNS lookup srv _sip._tcp.example.com**	ルックアップは、SRV 結果を詳細に調べます。 つまり、SRV レコードがドメイン名を返すとき、これは A および AAAA ルックアップによって解決されます。
dns flush	これにより、Meeting Server の DNS キャッシュがクリアされます。

4 ファイアウォールコマンド

MMP はメディア インターフェースのための簡単なファイアウォール ルールの作成をサポートします。 インターフェースにファイアウォールルールを設定したら、そのインターフェースでファイアウォールを有効にします。

メモ: これは、完全なスタンドアロンのファイアウォール ソリューションの代替を意図したものではありません。

ファイアウォールルールは各インターフェイスに個別に指定する必要があります。

インターフェイスの各ファイアウォール ルールは タグで識別されます。 これらは、ステータス出力で確認できます。例:

```
インターフェイス（Interface）      : [有効
（Enabled）]                       : false
Default policy                     : allow

タグ      ルール
---       ----
0         drop 80
```

注意: シリアルコンソールが利用可能な場合は、それを使用してファイアウォールを設定することを推奨します。SSH を使用する場合、ルールのエラーにより SSH ポートがアクセス不能になるからです。

コマンド/例	説明/メモ
firewall <iface> default (allow|deny) **firewall a default deny**	インターフェイスでファイアウォールを有効にする前に、このコマンドを使用してデフォルトポリシーを設定する必要があります。 許可ポリシーはどのルールにもマッチしないすべてのパケットを許可し、拒否ポリシーはどのルールにもマッチしないすべてのパケットを破棄します ルールが設定されていない場合、インターフェイス a のすべてのパケットがドロップされます。

コマンド/例	説明/メモ
firewall <iface> enable	指定されたインターフェイスでファイアウォールを有効にします。
firewall <iface> disable	指定されたインターフェースでファイアウォールを無効にします。
firewall <iface>	指定されたインターフェイスの現在のファイアウォール設定を表示します
firewall a	インターフェイス a のステータスとルールセットを表示します
firewall <iface> allow <port> [/<proto>] [from <host>[/<prefix>]] **firewall <iface> deny <port> [/<proto>] [from <host>[/<prefix>]]**	これらのコマンドでルールを追加します。 <ポート>引数は、数字（例、「80」）または IANA サービス 名レジストリ（例、「http」）からのサービス名のいずれかで指定できます。 protocol 引数は、tcp または udp のいずれかです。 省略すると、ルールは TCP と UDP の両方のパケットに一致します。
firewall a allow http/tcp	インターフェイス A のポート 80 で TCP パケットを許可します
firewall a deny 678	メディア インターフェイス A のポート 678 上のすべてのパケットをドロップする
ファイアウォール a は 192.168.1.0/28 からの ssh を許可します	オプションの **from** 句では、ルールが適用されるホストを制限します。 これは IPv4 または IPv6 のアドレスとして指定されます サブネットを示すオプションのプレフィックス長。 192.168.1.0 と 192.168.1.255 間の 256 IPv4 アドレスからインターフェイス a への SSH アクセスを許可します
firewall <iface> delete <tag> **firewall a delete 0**	ルールを削除するには、このコマンドでその タグを使用します。 このテーブルの上の 1 つのルールを削除します。

5 LDAP コマンド

新しい **ldap** オプションが **user add** MMP コマンドに追加されました。これにより、LDAP サーバーの詳細、ディレクトリ検索パラメータ、TLS 設定の設定、および LDAP 認証の有効化または無効化が可能になります。

LDAP ユーザの追加を有効にするために、新しいオプション [**ldap**] がコマンドに追加されます。

```
user add <username> (admin|crypto|audit|appadmin|api) [ldap]
```

メモ: ミーティングサーバ API は LDAP 認証によるユーザへのアクセスをサポートしていません。

---

help ldap コマンドの出力:

```
cms> help ldap
MMP ユーザー用に LDAP クライアントを設定す
る使用例：

    ldap
    ldap server <hostname|address> <port>
    ldap protocol (ldap|ldaps)
    ldap binddn <username>
    ldap basedn <base DN>
    ldap login_attr <attribute>
    ldap filter <filter>
    ldap remove <binddn|filter|trust>
    ldap trust <crt bundle>
    ldap verify (enable|disable)
    ldap min-tls-version <minimum version string>
    ldap enable
    LDAP 無効
    LDAP ステータス
```

注：

user list MMP コマンドは、ログインしている LDAP ユーザーを含むように拡張されます。

LDAP ユーザーに適用される **user rule** パラメータのみが max_failed_logins, max_idle, and max_sessions になります。 このコマンドの他のパラメータは LDAP ユーザーには適用されません。

user expire MMP コマンドは、LDAP ユーザーには対応していません。

コマンド/例	説明/メモ
LDAP	LDAP 構成に関する情報を表示します。
ldap server <hostname|address> <port>	LDAP サーバをホスト名または IP アドレス、およびポート番号で指定します。 これは必須です。
LDAP プロトコル (ldap|ldaps)	使用する LDAP プロトコルを指定します。 LDAP サーバへの安全な接続を使用するには、ldaps を使用する必要があります。 プロトコルの指定は必須です。
ldap binddn <username> **ldap binddn cn=binduser,oi=user,dc=domain,dc=com** **ldap binddn "cn=binduser,o=My Company,dc=domain,dc=com"** **ldap binddn domain\\username**	検索のためにディレクトリサーバ にバインドする識別名を追加します。 binddn パラメータはオプションです。 指定しない場合、匿名バインド要求が使用されます。 バインドユーザはディレクトリの検索権限を持っている必要があります。 このコマンドにより、オプションのバインドパスワードの入力が求められます。 引数にスペースが含まれる場合、引数を引用符で囲む必要があります。バックスラッシュが含まれる場合、前にバックスラッシュを付けて、エスケープする必要があります。
ldap basedn <base DN>	検索ベースとして使用するベース識別名を指定します。 basedn の指定は必須です。 引数にスペースが含まれる場合、引数を引用符で囲む必要があります。バックスラッシュが含まれる場合、前にバックスラッシュを付けて、エスケープする必要があります。
ldap login_attr<attribute>	uid、userPrincipalName、sAMAccountName など、ユーザを一意に識別する LDAP 属性名を指定します。 ログインするには、属性値が事前設定された MMP ユーザ名と一致する必要があります。 属性の指定は必須です。
ldap filter <filter> **ldap filter (&(objectClass=*)(memberOf=CN=admins,DC=example,DC=com))**	LDAP 検索フィルターをセットアップします。 フィルタの指定は任意です。 フィルターが指定されていない場合、デフォルト値 (objectClass=*) が使用されます。 有効な LDAP フィルタ構文を使用し、それを括弧で囲む必要があります。
ldap remove (binddn|filter|trust)	以前にセットアップされた binddn、filter、または trust パラメータを削除します。
ldap trust <crt bundle>	特定のバンドルの証明書を使用して証明書を検証するようにシステムを設定します。 LDAP サーバーへのセキュアな接続を使用するには、これを信頼された CA で設定する必要があります。

コマンド/例	説明/メモ
ldap verify (enable|disable)	LDAP サーバに接続するための証明書の検証を有効または無効にします。 LDAP サーバへの安全な接続を使用するには、証明書の検証を有効にする必要があります。 無効にすると、Meeting Server は、信頼された証明書を要求または確認しません。
ldap min-tls-version <minimum version string>	システムが使用する最小の TLS バージョンを設定します。 可能な値は、1.0、1.1、および 1.2. 構成されていない場合、最小 TLS バージョンは 1.2 に設定されます。 **メモ**: ミーティングサーバは、最小バージョンを TLS 1.3 に設定することをサポートしていません。
ldap enable	LDAP サービスを有効にします。
ldap disable	LDAP サービスを無効にします。
ldap status	ldap サービスのステータスを 実行中と表示します。これは、サービスが実行中であることを示します。 実行されていない - サービスは有効になっていますが、実行されていません。 ログで詳細を確認してください。 無効 - サービスは無効になっています

6 スケジューラコマンド

ミーティングのスケジュールは、新しい Scheduler コンポーネントによって有効化されます。このコンポーネントは、新しい **scheduler** MMP コマンド によって設定できます。

メールサーバの構成の詳細は、以下にリストされている新しい **スケジューラ** MMP コマンドで提供されます。

コマンド / 例	説明/メモ
スケジューラ **scheduler status**	Scheduler の現在のステータスを表示します。
スケジューラ（有効 | 無効）	スケジューラを有効または無効にします。
scheduler restart	スケジューラを再起動します。
scheduler https listen <interface> <ポート>	Scheduler がリッスンするインターフェイスとポートのペアを設定します。
scheduler https listen none	スケジューラの管理 API インターフェースを無効にします。
scheduler https certs <key-file> <crt-fullchain-file>	管理 API で使用されるサーバ証明書だけでなく、アウトバウンド接続を行うときに使用される証明書も構成します。たとえば、c2w リンクまたは Call Bridge への API 呼び出し。
scheduler https certs none	管理 API の証明書構成を削除します。
scheduler c2w certs <key-file> <crt-fullchain-file>	Web Bridge 3 に提示証明書バンドルを設定します。
scheduler c2w certs none	ウェブブリッジ 3 への TLS 接続の証明書設定を削除します。
scheduler c2w trust <crt-bundle>	ウェブブリッジへの接続を確認するための信頼バンドルを設定します。
scheduler c2w trust none	ウェブ ブリッジ 3 の証明書バンドルをスケジューラの信頼ストアから削除します。
scheduler email server <hostname|address> <port>	スケジューラがメールを送信する SMTP サーバを設定します。
scheduler email server none	スケジューラからメールサーバ設定を削除します。
scheduler email username <smtp user- name>	SMTP サーバでの認証に使用されるメールアカウントを設定します。ミーティングの開催者の代理としてメールを送信するには、このアカウントに適切な権限が付与されている必要があります。 **メモ：**参加者へのメールは、このコマンドを使用して設定されたアカウントから送信されるのではなく、ミーティング開催者の差出人のアドレスを使用して送信されます。

コマンド/例	説明/メモ
scheduler email remove username	SMTP 認証用に設定されたメールユーザー名を削除します。
スケジューラメールプロトコル<smtp | smtps>	スケジューラとメールサーバの通信を次のように指定します: smtp: プレーン テキスト TCP (smtp) 経由 smtps: 暗号化された TLS チャネル経由
scheduler email auth (enable | dis- able)	SMTP 認証を有効または無効にします。
scheduler email starttls (enable | disable)	SMTP 接続の便宜的 TLS を有効または無効にします。
scheduler email trust <bundle> | none	（オプション）メールサーバーの信頼できるバンドルの設定を許可します。 設定されている場合、設定済みのハンドルを使用して、メールサーバーの証明書が検証されます。 構成されていない場合、証明書の検証は行われません。
scheduler email common-address <address@mail.domain> "<Display name>"	ミーティングサーバ上で共通のメールアドレスと表示名を設定します。 スケジューラが共通のメールアドレスから参加者にミーティング招待状を送信します。 空白のままにすると、スケジューラは開催者のメールアドレスから招待メールを送信します。
scheduler email common-address none	設定済みの共通メールアドレスと表示名を削除します。
scheduler timedLogging	時限ロギングのステータスを取得します。
scheduler timedLogging (webBridge|ap- i|email) <time>	指定した期間のログ記録を有効にします。

7 証明書によるプロビジョニング

以下の PKI (公開鍵基盤) コマンドを使用します。

キーファイルには、PEM または DER のいずれかとしてエンコードされ、.key、.pem、または .der のファイル名拡張子を持つ RSA または DSA キーが含まれている必要があります。 証明書ファイルは、PEM または DER としてエンコードされた x509 証明書であり、ファイル名の拡張子は .crt、.cer、.pem、または .der です。

ファイル名には、英数字、ハイフンおよび下線文字の後に上記のいずれかの拡張子を付けることができます。 サービスごとの証明書とキーファイルの名前を選択できます。すべてのサービスで同じファイル ペアを使用する場合でも同様です。

秘密鍵と証明書ファイルは SFTP 経由でアップロードする必要があります。

コマンド/例	説明/メモ
pki	現在の PKI の使用状況を表示します。
pki list	秘密鍵、証明書、証明書署名要求 CSR などの PKI ファイルを一覧表示します。
pki inspect <filename>	ファイルを検査し、ファイルが秘密鍵、証明書、CSR または不明のいずれであるかを表示します。 証明書の場合、様々な詳細が表示されます。ファイルに証明書のバンドルが含まれている場合、バンドルの各要素に関する情報が表示されます。 PEM および DER 形式のファイルの両方が処理されます。
pki match <key> <certificate>	このコマンドは、指定されたキーとシステム上の証明書が一致するかどうかを確認します。 プライベートキーと証明書は、1 つの使用可能な ID の 2 等分であり、サービス（例：HTTPS）で使用される場合は一致する必要があります。
pki verify <cert> <cert bundle/CA cert> [<CA cert>] **pki verify server.pem bundle.pem rootca.pem** **pki verify server.pem bundle.pem**	証明書は Certificate Authority（CA）によって署名されている場合があり、CA は中間 CA 証明書の「証明書バンドル」と、場合によっては独自のファイルで CA 証明書を提供します。 証明書が CA によって署名され、証明書バンドルを使用してこれを表明できることを確認するには、このコマンドを使用します。
pki unlock <key>	多くの場合、秘密鍵にはパスワード保護が提供されます。 ミーティング サーバで使用するには、キーのロックが解除されている必要があります。 このコマンドにより、ターゲットファイルのロックを解除するためのパスワードの入力が求められます。 ロックされた名前は、同じ名前のロック解除されたキーによって置き換えられます

コマンド/例	説明/メモ
pki csr <key/cert basename> [<attribute>:<value>] **pki csr dbserver CN:server01.db.example.com subjectAltName:server02.db.example.com**	プライベート キー マテリアルの生成に関する要件を満たしている Cisco を信頼することに問題ないユーザーの場合、プライベートキーと関連する証明書署名要求（CSR）を生成できます。 <key/cert basename>新しいキーと CSR を識別する文字列です (例えば、「new」は「new.key」と「new.csr」ファイルになります) CSR の属性は、コロン (":") で区切られた属性名と値のペアで指定できます。 属性は次のとおりです。 CN: 証明書に記載される commonName CommonName はシステムの DNS 名である必要があります。 OU: 組織単位 O: 組織 L：地域 ST：州 C：国 emailAddress: メールアドレス CSR ファイルは SFTP でダウンロードし、Certificate Authority（CA）に署名してもらうことができます。(または、CSR ファイルを「pki sign」コマンドで使用して、ローカルで証明書を生成することもできます。) 戻ったら SFTP 経由でアップロードする必要があります。 その後、証明書として使用できます。 メモ：**pki csr <key/cert basename> [<attribute>:<value>]** は、属性として、subjectAltName を取得します。 IP アドレスとドメイン名は、コンマ区切りリストの subjectAltName でサポートされています。 次に例を示します。 **pki csr test1 CN:example.exampledemo.com subjectAltName:exampledemo.com** **pki csr test2 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com** **pki csr test3**

コマンド/例	説明/メモ
	CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com, 192.168.1.25,server.exampledemo.com, join.exampledemo.com, test.exampledemo.com 証明書のサイズと チェーン内の証明書の数を最小限に維持します。維持しないと、TLS ハンドシェイクのラウンドトリップタイムが長くなります。
pki selfsigned <key/cert basename> [<attribute>:<value>] **pki selfsigned dbca CN:"my company CA" OU:"My company" O:cms L:Raleigh ST:"North Carolina" C:US**	このコマンドを使用して、自己署名証明書を生成できます。 <key/cert basename> は、生成されるキーと証明書を示します。たとえば、「pki selfsigned new」は、「new.key and new.crt」（自己署名）を作成します。 証明書の属性は、コロン (":") で区切られた属性名と値のペアで指定できます。 属性は次のとおりです。 CN：commonName。 証明書がエンドエンティティ証明書として使用される場合、commonName は関連するサービスの DNS 名である必要があります。 OU: 組織単位 O: 組織 L：地域 ST：州 C：国 emailAddress: メールアドレス 自己署名証明書は CSR の署名に使用できます。 これらは、データベース クラスターなどの内部サービスに展開する場合に便利です。 ウェブ サービスなどの外部サービスの場合は、外部 CA を使用します。
pki sign <csr/cert basename> <CA key/cert basename> **pki sign dbserver dbca** **pki sign dbclient dbca**	このコマンドは、<csr/cert basename> が識別する CSR に署名し、<CA key/cert basename> が識別する CA 証明書とキーを使用して、署名された同じベースネームを持つ証明書を作成します。 <csr/cert basename> ファイルおよび <CA key/cert basename> ファイルは、「pki csr」および「pki selfsigned」のコマンドでそれぞれ生成されます。

コマンド/例	説明/メモ
pki pkcs12-to-ssh <username>	PKCS#12 ファイルに保存されたパブリック SSH キーを使用できますが、最初に処理する必要があります。このコマンドは、<username>.pub という名前でアップロードされた PKCS#12 ファイルから使用可能な公開鍵を抽出します。pkcs#12 ファイルのパスワードの入力を求めるプロンプトが表示されます。 完了後、pkcs#12 ファイルはパスワード保護なしの使用可能なキーに置換されます。 メモ: pkcs#12 ファイルに含まれるその他のデータは失われます。
pki pkcs12-to-ssh john	ジョンというユーザーにアップロードされた PKCS#12 ファイルである john.pub のキーは、コマンドを実行可能にすることで、使用できるようになります。

コマンド/例	説明/メモ
pki	現在の PKI の使用状況を表示します。
pki list	秘密鍵、証明書、証明書署名要求 CSR などの PKI ファイルを一覧表示します。
pki inspect <filename>	ファイルを検査し、ファイルが秘密鍵、証明書、CSR または不明のいずれであるかを表示します。 証明書の場合、様々な詳細が表示されます。 ファイルに証明書のバンドルが含まれている場合、バンドルの各要素に関する情報が表示されます。 PEM および DER 形式のファイルの両方が処理されます。
pki match <key> <certificate>	このコマンドは、指定されたキーとシステム上の証明書が一致するかどうかを確認します。 プライベートキーと証明書は、1 つの使用可能な ID の 2 等分であり、サービス（例：callbridge）で使用される場合は一致する必要があります。
pki verify <cert> <cert bundle/CA cert> [<CA cert>] **pki verify server.pem bundle.pem rootca.pem** **pki verify server. pem bundle.pem**	証明書は認証局 (CA) によって署名されている場合があり、CA は中間 CA 証明書の「証明書バンドル」と、場合によっては CA 証明書を独自のファイルで提供します。 証明書が CA によって署名され、証明書バンドルを使用してこれを表明できることを確認するには、このコマンドを使用します。

コマンド/例	説明/メモ
pki unlock <key>	多くの場合、秘密鍵はパスワードで保護されています。 Meeting Server で使用するには、キーのロックを解除する必要があります。 このコマンドにより、ターゲットファイルのロックを解除するためのパスワードの入力が求められます。 ロックされた名前は、同じ名前のロック解除されたキーによって置き換えられます
pki csr <key/cert basename> [<attribute>:<value>] **pki csr example CN:www.example.com OU:"My Desk" O:"My Office" L:"San Jose" ST:California C:US**	プライベート キー マテリアルの生成に関する要件を満たしている Cisco を信頼することに問題ないユーザーの場合、プライベートキーと関連する証明書署名要求（CSR）を生成できます。 <key/cert basename>は新しいキーと CSR を識別する文字列です (例えば、「new」は「new.key」と「new.csr」ファイルになります) CSR の属性は、コロン (":") で区切られた属性名と値のペアで指定できます。 属性は次のとおりです。 CN：証明書に記載する CommonName です。 CommonName はシステムの DNS 名である必要があります。 OU: 組織単位 O: 組織 L: 市区町村 ST: 州 C: 国 emailAddress：メールアドレス CSR ファイルは SFTP でダウンロードし、認証局 (CA) に渡して署名をもらうことができます。 (または、CSR ファイルを「pki sign」コマンドで使用して、ローカルで証明書を生成することもできます。) 戻ったら SFTP 経由でアップロードする必要があります。 その後、証明書として使用できます。 メモ：1.6.11 以降から、**pki csr <key/cert basename> [<attribute>:<value>]** は、属性として、subjectAltName を取得します。 IP アドレスとドメイン名は、コンマ区切りリストの subjectAltName でサポートされています。 次に例を示します。 **pki csr test1 CN:example.exampledemo.com subjectAltName:exampledemo.com** **pki csr test2 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com** **pki csr test3 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com, 192.168.1.25,exampledemo.com, server.exampledemo.com,join.exampledemo.com, test.exampledemo.com** 証明書のサイズと数を チェーンを最小限に抑えます。そうしないと、TLS ハンドシェイクの往復時間が長くなります。

コマンド/例	説明/メモ
pki selfsigned <key/cert basename> [<attribute>:<value>]	このコマンドを使用して、自己署名証明書を生成できます。 <key/cert basename> は、生成されるキーと証明書を示します。たとえば、「pki selfsigned new」は、「new.key and new.crt」（自己署名）を作成します。 CSR の属性は、コロン (":") で区切られた属性名と値のペアで指定できます。 属性は次のとおりです。 CN：証明書に記載する CommonName です。 CommonName はシステムの DNS 名である必要があります。 OU: 組織単位 O: 組織 L：地域 ST：州 C：国 emailAddress: メールアドレス CSR ファイルは SFTP でダウンロードし、Certificate Authority（CA）に署名してもらうことができます。 戻ったら SFTP 経由でアップロードする必要があります。 その後、証明書として使用できます。 証明書のサイズとチェーン内の証明書の数を最小限に維持します。維持しないと、TLS ハンドシェイクのラウンドトリップタイムが長くなります。
pki sign <csr/cert basename> <CA キー/証明書ベース名>	このコマンドは、<csr/cert basename>で識別される csr に署名します。<CA key/cert basename>により識別される CA 証明書およびキーで署名された、同じベースネームを持つ証明書を生成します。 <csr/cert basename> ファイルおよび <CA key/cert basename> ファイルは、「pki csr」および「pki selfsigned」のコマンドでそれぞれ生成されます。
pki pkcs12-to-ssh <username> **pki pkcs12-to-ssh john**	PKCS#12 ファイルに保存された SSH 公開鍵を使用できますが、最初に処理する必要があります。 このコマンドは、<username>.pub という名前でアップロードされた PKCS#12 ファイルから使用可能な公開鍵を抽出します。pkcs#12 ファイルのパスワードの入力を求めるプロンプトが表示されます。 完了後、pkcs#12 ファイルはパスワード保護なしの使用可能なキーに置換されます。 メモ: pkcs#12 ファイルに含まれるその他のデータは失われます。 ジョンというユーザーにアップロードされた PKCS#12 ファイルである john.pub のキーは、コマンドを実行可能にすることで、使用できるようになります。

7.1 TLS 証明書の検証

メモ: TLS 証明書の検証が有効になっている場合、リモートデバイスの証明書にサーバとクライアントの両方の認証属性が定義されていることを確認してください。 これにより、発信と着信の両方の TLS 接続が受け入れられます。

メモ：セキュアな接続を使用して、LDAP サーバーを設定する際、MMP の tls ldap コマンドを使用して、TLS 証明書検証が設定されるまで、接続は完全に安全ではありません。

Meeting Server は、SIP、LDAP、SYSLOG、HTTPS（インバウンド接続：API、Web Admin および Web Bridge 3、アウトバウンド接続：CDR）および RTMPS のすべてのサービスに対してデフォルトで、TLS 1.3 および DTLS 1.2 を使用します。 TLS 1.3 は HTTP/SIP インターフェース上でベスト エフォートを使用してネゴシエートされ、リモート エンドがサポートしていない場合は TLS 1.2 にフォールバックします。

TLS 1.3 または 1.2 を実装していない古いソフトウェアとの相互運用に必要な場合、プロトコルの下位バージョンを SIP、LDAP、および HTTPS サービスの最小 TLS バージョンとして設定できます。 以下の「**tls <service> min-tls-version <minimum version string>**」および「**tls min- dtls-version <minimum version string>**」コマンドを参照してください。

注：

- すべてのコンポーネントがアップグレードされ、TLS 1.3 をサポートしますが、次の例外があります。スケジューラ コンポーネントが webBridge と TLS 1.3 をネゴシエートしません。
- TLS 1.3 は Cisco Unified Communications Manager with SIP インターフェイスをサポートしますが、Cisco Unified Communications Manager IM & Presence 相互運用シナリオでは検証されておらず、今後のリリースで検証されます。
- DTLS バージョンに変更はありません。 Meeting Server は、引き続き、デフォルトとして、1.2 を含む DTLS 1.2 以下をサポートします。
- 暗号設定の TLS 1.3 サポートは検証されていません。
- Meeting Server は現在、TLS 1.3 への最小バージョンの設定をサポートしていません。
- TLS 1.0 および 1.1 のサポートは、今後のリリースで削除されます。

メモ：tls 設定を適用するには、Call Bridge を再起動する必要があります。 ただし、tls syslog 設定が修正されると、syslog サーバーを無効化し、Call Bridge を再起動した後に有効化する必要があります。

コマンド/例	説明/メモ
tls <service> **tls ldap**	サービスの設定、つまり、sip|ldap|syslog|dtls|webadmin|rtmps を表示します（メモ：バージョン 3.1 からの RTMPS サポート）。 LDAP の設定を表示します。
tls <service> trust <crt bundle> **tls ldap trust ldap.crt**	特定の証明書バンドルを使用してリモートサービスの証明書を検証するようにシステムを設定します
tls <service> verify (enable|dis-able|ocsp)	サービスの証明書の検証を有効/無効にします。 有効にし、システムがリモートサービスの証明書の確認に失敗した場合、接続が中止されます。 証明書失効ステータスを確認するために、リモートサービスがステープル OCSP 応答を返すという追加要件で検証を有効にします。 システムが証明書の有効性を確認しなかった場合、または証明書の失効ステータスが不明または失効の場合、リモートサービスへの接続は中止されます。
tls sip ciphe rs <cipher string>	tls cipher コマンドの使用が必要な場合については、以下の説明を参照してください。 暗号文字列の形式は、OpenSSL が使用する暗号のコロン区切りのリストです（https://www.openssl.org/docs/manmaster/man1/openssl-ciphers.html#CIPHER-LIST- FORMAT）。 現在のデフォルトの暗号サポートは次のとおりです。 "ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:R SA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES"（バージョン 2.4.2 まで） "ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:R SA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:!aECDH"（バージョン 2.4.3 以降) ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RS A+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:!aECDH **メモ：**「:!aDH:!aECDH:!SEED:!eNULL:!aNULL:!ARIA:!AESCCM8」は、非常に脆弱な暗号を禁止するために、設定済み暗号文字列に自動で追加されます。

Com- mand/Examples	説明/メモ
tls <service> min-tls-version <minimum version string>	このコマンドを使用して、Meeting Server が使用するデフォルト TLS バージョンを変更します （バージョン 2.3 以降）。 メモ：TLS の最小バージョンを変更する場合、**callbridge restart** コマンドを使用して、Call Bridge サービスを再起動する必要があります。 ミーティングサーバはすべてのサービスに TLS 1.3 を使用し、リモートエンドがサポートしていない場合は 1.2 にフォールバックします。 TLS 1.3 または 1.2 が実装されていない古いソフトウェアとの相互運用に必要な場合、SIP、LDAP、および HTTPS の最小 TLS バージョンを下位バージョンのプロトコルに構成できます。
tls sip min- tls-version 1.1	SIP に TLS バージョン 1.1 以降を使用する
tls ldap min-tls-version 1.1	LDAP に TLS バージョン 1.1 以降を使用する
tls min-dtls-version <最小バージョン文字列>	システムが使用する最小の DTLS バージョンを設定します。 （バージョン 2.3 以降）。メモ：TLS の最小バージョンを変更する場合、**callbridge restart** コマンドを使用して、Call Bridge サービスを再起動する必要があります。 (バージョン 2.3 以降)
tls min-dtls-version 1.1	DTLS 1.2 が実装されていない古いソフトウェアとの相互運用に必要な場合、プロトコルの下位バージョンを使用するように DTLS を設定します。

デフォルトでは、ミーティングサーバは tcp ポート 5061 の SIP TLS を含め、すべての TLS 接続に安全な暗号のみを使用します。しかし、これはミーティングサーバが古い、安全性の低いデバイスとの TLS コールを発信できないことを意味する場合があります。 デプロイに古いキットがある場合、この tls ciphers コマンドを使用して、古いデバイスが受け入れられる暗号のリストを指定します。 暗号化の詳細については、『Openssl ガイド』を参照してください。

デバイスが安全な暗号を処理できない場合の症状には、次のようなものがあります。

- デバイスへの SIP TLS 呼び出しが失敗します。
- デバイスで HTTPS アクセスが機能しません。
- エラーがログに表示されます。

8 Cisco ミーティングサーバを構成するためのコマンド

メモ：Cisco Meeting Server 2000 の正常性を判断するには、Cisco UCS Manager を使用します。

コマンド/例	説明/メモ
アップタイム	ミーティングサーバが最後に再起動してから経過した時間を表示します。
shutdown	プロンプトへの応答で Y を入力すると、ミーティングサーバの電源がオフになります。 メモ：Cisco Meeting Server 2000 の MMP 経由ではシャットダウンはできません。電源を切る前に、Cisco UCS Manager を使用して、ブレードサーバーの電源を切ります。 VM をシャットダウンするには、「shutdown」という MMP コマンドを使用する必要があります。 これにより、ミーティングサーバは、ミーティングの参加者を含むすべての接続済みデバイスおよび Meeting Management に適切な切断メッセージを送信します。
ホスト名<名前> **ホスト名 mybox.mydomain**	サーバのホスト名を設定します。 メモ: このコマンドを発行した後、再起動が必要です。
タイムゾーン **タイムゾーン<タイムゾーン名>** **タイムゾーン ヨーロッパ/ロンドン** **timezone list**	現在設定されているタイムゾーンを表示します ミーティングサーバのタイムゾーンを設定します。 ミーティングサーバは、標準の IANA タイムゾーンデータベースを使用します。 一覧については、この リンク を参照してください。 メモ: このコマンドを発行した後、再起動が必要です。 利用可能なタイムゾーンの完全なリストを印刷します。 メモ：GMT や Etc/GMT<offset> からのオフセットを持つタイムゾーンを選択する場合、オフセットには POSIX スタイルの記号が使用されます。 結果として、香港のタイムゾーンは Etc/GMT-8 であり、Etc/GMT+8 ではありません。

コマンド/例	説明/メモ
ntp server add|del <host>	NTP サーバを構成/削除します。 <host> には、名前または IP アドレスが指定できます
ntp status	NTP サーバーのステータスを確認します
ntp サーバリスト	設定済みの NTP サーバー一覧を表示する
ntp groupkey <keyfile>	自動キー サポートのために NTPv4 グループ キーを追加します
ntp autokey (enable|disable)	自動キー サポートを有効または無効にします
ntp groupkey group.key **ntp autokey enable**	たとえば、SFTP を使用してグループキーファイルを「group.key」にアップロードし、これらのコマンドで設定します。
date	現在のシステム (UTC) とローカル時刻を表示します。
date set <date> <time>	日付と時刻を設定します。 このコマンドは、仮想化デプロイや NTP サーバーを使用しないサーバーデプロイのみで必要です。 日付と時刻に使用できる形式は次のとおりです。 • ISO 8601 形式（%Y-%m-%d）+ 時間がスペースで区切られた 24 時間表示 • %m/%d/%y + 24 時間表示
date set 2013-08-17 13:04	メモ: NTP サーバを持つシステムのユーザはこのコマンドを使用する必要はありません。
リブート（**reboot**）	ミーティングサーバを再起動します。 メモ: ミーティングサーバを再起動すると、すべての通話が切断されます。 このプロセスが完了するまで数分かかります。
license	このコマンドは仮想サーバにのみ適用されます。 Meeting Server ライセンスステータスを確認し、ライセンスが付与されている機能を表示します（例： 機能：callbridge ステータス：有効期限： 2014-JUl-01（残り 12 日）

コマンド/例	説明/メモ
コールブリッジ	現在の状況を表示します
callbridge listen (interface allowed list|none) **callbridge listen a**	Call Bridge がリッスンする 1 つ以上のインターフェイス (A、B、C または D から選択) を設定します。
callbridge listen none	Call Bridge を停止し、リッスン サービスを無効にします。ただし、Call Bridge は有効なままです。
callbridge prefer <interface>	インタフェース許可リストから「優先」SIP インターフェイスとしてインターフェイスを 1 つ選択します。ルーティングまたはヒューリスティックを使用して、固有のインターフェイスが選択できない場合は、このインターフェイスを連絡先アドレスとして使用します。
callbridge certs <key-file> <cert- file>[<crt-bundle>]	ミーティングサーバ、およびオプションで、CA が提供する CA 証明書バンドルのキーファイル名と証明書ファイル名を定義します。(第 7 章.)
callbridge certs none	証明書の構成を削除します

コマンド/例	説明/メモ
callbridge trust cluster <trusted cluster certificate bundle>	Call Bridge を設定して、証明書の特定のバンドルを使用して、クラスタで Call Bridge の ID を検証します。 バンドルは、証明書チェーン、または信頼できる証明書の許可されたリストのいずれかになります。 (バージョン 2.4 以降)。
callbridge trust cluster none	Call Bridge のトラストストアから Call Bridge クラスタの証明書バンドルを削除します （バージョン 2.4 以降）。
callbridge trust branding <trusted branding server certificate whitelist>	指定された証明書を使用して、ブランディングサーバー証明書と検証するように、Call Bridge を設定します （3.5 以降） メモ：ブランディングサーバーが HTTPS でホストされている場合、有効な CA または同じ CA が Meeting Server とブランディングサーバー証明書に署名する必要があります。有効な CA がブランディングサーバー証明書に署名しなかった場合、Meeting Server とブランディングサーバー間の通信が失敗する場合があります。
callbridge wc3jwt expiry <expiry time in hours>	ウェブ アプリ セッションのタイムアウト時間を時間単位で設定します。 1 ～ 24 までの整数を使用できます。未設定の場合、デフォルト値は 24 です。 **メモ：**変更を適用するためには、Call Bridge を再起動します。
callbridge av1 enable|disable	AV1 サポートを有効または無効にします。 Call Bridge を再起動して、変更を適用します。 **有効にする** - 有効な場合、ウェブ アプリ ミーティング中のコンテンツは AV1 形式で送受信されます。 **無効にする** - 無効な場合、コンテンツは AV1 形式で共有されません。 **注：** • AV1 送信は Chrome ブラウザでのみテストされ、認定されています。 • AV1 が Meeting Server で有効になっているが、ブラウザで、サポートされていない場合、コンテンツはブラウザ対応のコーデックで送信されます。
callbridge restart	コア メディア サービスを再起動します。 メモ: ミーティングサーバを再起動すると、すべての通話が切断されます。 このプロセスが完了するまで数分かかります。

コマンド/例	説明/メモ
syslog server add <hostname> [<port>] **syslog server del <hostname>** **syslog server add tls:syslog.example.com 514**	ミーティングサーバは TCP (UDP ではなく) 経由でリモート syslog サーバにログファイルを送信可能 ポートのデフォルトは 514 です 転送中の syslog データを保護するために TLS を使用するよう指定するには、リモートサーバのホスト名/IP アドレスの前に「tls:」を付けます。
syslog	現在の syslog 構成を一覧表示します
syslog enable **syslog disable**	syslog メカニズムを有効にします
syslog audit add <hostname> **syslog audit add audit-server.example.org** **syslog audit del <hostname>**	監査ログが送信されるサーバを定義します。 監査ログは完全なシステムログのサブセットであり、セキュリティイベント（ログインなど）と設定変更に関する情報が含まれています。 メモ: これらの syslog 監査コマンドは、監査の役割を持つユーザのみが実行できます。
http の監査 (enable|disable)	HTTP トランザクションの詳細な監査を有効または無効にします
syslog tail [<number of lines>]	最新のログメッセージを表示します。 デフォルトでは、これは 10 のメッセージですが、オプションの引数で数を変更することができます
syslog page	完全なログをインタラクティブに表示します。 スペースバーを押して、ログメッセージの次のページを表示します。q を押して終了します。
syslog follow	リアルタイムで書き込まれたログメッセージを表示します。Ctrl+C を押すと、出力を停止して管理シェルに戻ります。
syslog 検索<文字列> **syslog 検索エラー**	特定のパターンに一致するメッセージのみを表示する メモ：現在のユーザーに audit ロールが付与されている場合、tail コマンドと search コマンドは監査ログメッセージを表示します。付与されていない場合、システムログからのメッセージが表示されます。 システムログのダウンロードについては、「セクション 12.6」を参照してください。
syslog rotate <filename> **syslog rotate mylog**	指定したファイル名でログファイルを永久的に保存し、アクティブなシステムログを空にします。 保存したファイルは SFTP を使ってダウンロードできます。
version	現在ミーティングサーバにインストールされているソフトウェアのリリースを表示します。

8.1 連邦情報処理標準

ミーティングサーバは、FIPS 140-2 レベル 1 認定ソフトウェア暗号モジュール (http://en.wikipedia.org/wiki/FIPS_140-2) を提供します。 FIPS 認定を受けている Cisco ミーティングサーバソフトウェアのリリースについての情報は、この リンクをクリックしてください。

FIPS モードを有効にすることで、暗号操作はこのモジュールを使用して実行され、暗号操作は FIPS 承認済み暗号アルゴリズムに制限されます。

コマンド/例	説明/メモ
fips	FIPS モードが有効かどうかを表示します
fips enable **fips disable**	ネットワークトラフィックのすべての暗号化操作で FIPS-140-2 モード暗号化を有効にします。 FIPS モードの有効化または無効化後は、再起動が必要です
FIPS テスト	組み込みの FIPS テストを実行します

9 MMP ユーザーアカウントコマンド

MMP ユーザーアカウントのロールは以下のとおりです。

- admin：MMP 管理者。すべてのタスクを実行することが許可されています
- crypto：MMP 暗号演算子。暗号関連タスクを実行することが許可されています
- audit：監査ログを Syslog サーバーに送信します（送信方法は『導入ガイド』の「リモート Syslog サーバー」セクションを参照してください）
- appadmin：ウェブ管理インタフェース経由でアプリケーションレベルの設定を実行できます
- api：API を使用できます。 「api」ユーザーロールは、以前にウェブ管理インターフェイスを経由で設定されていることに注意してください
- ldap：追加されたユーザーは LDAP ユーザーです。

メモ: このセクションのコマンドでセットアップされるユーザアカウントを、Active Directory を使用してセットアップされ、Cisco ミーティングアプリにログインして発信できるアカウントと混同しないようにしてください。

特に断りのない限り、次のコマンドを使用するには、管理者権限で MMP アカウントにログインする必要があります。

コマンド/例	説明/メモ
user add <username> (admin|crypto|audit|appadmin|api) [ldap]	指定されたタイプ（上記を参照）の新しい MMP ユーザーを作成します。または、作成されたユーザーが LDAP ユーザーです。 意図したパスワードが設定されていることを確認するために、ユーザのパスワードを 2 回入力するように指示します。 初回ログイン時に、ユーザは新しいパスワードを設定するように求められます。 **注意**: LDAP ユーザを除き、ユーザパスワードは 6 ヶ月後に期限切れになります。
user del <username>	システムからユーザを削除します。 **警告** : **user del <username>** は、すでにログインしているユーザーを自動削除しません。**user list** を使用して、ユーザーがログインしているかどうかを確認することが推奨されます。ログインしている場合は、**user evict <username>** を使用して削除する前にすべてのセッションを終了させてください。
ユーザリスト	ユーザー、ユーザーのロール、パスワードの有効期限、ログインの有無の一覧を表示します。
user info <username>	役割、最後のログイン、最後のログイン以降に失敗したログイン試行回数、前回のパスワード変更、パスワードの有効期限、アカウントがロックされているかどうかなど、ユーザの詳細を表示します。
user evict <username>	ユーザを MMP セッションからログアウトします。 メモ:ウェブ管理セッションで現在アクティブなユーザに対してこのコマンドを使用すると、MMP セッションがフリーズし、MMP に再ログインする必要があります。 **メモ**: バージョン 2.9 以降、このコマンドは Cisco Meeting Server 2000 で利用できます。
user unlock <username>	最大失敗ログイン数を超過したことが原因で発生したユーザのログインのロックを解除します
passwd [<username>]	自分のパスワードまたは他のユーザのパスワードを変更する:手順に従って操作してください。 ユーザー名は任意です。これにより、管理者は別のユーザーのパスワードをリセットできます。 引数なしで実行すると、コマンドは現在のユーザのパスワードを変更します。 現在のユーザの認証が必要です。

コマンド/例	説明/メモ
user expire <username>	ユーザの次回ログイン時に新しいパスワードを設定するよう強制します。 メモ: このコマンドはユーザタイプ「api」には適用されません。パスワードは時間の経過とともに期限切れになりますが、このコマンドでパスワードの変更を強制することはできません。
user host <username> add|del <hostname> **user host bob add 192.168.1.3**	ドメイン名または IP アドレスで指定された許可リストのホストからのユーザーのリモートアクセスを制御します。 メモ：**user info** コマンドは、許可されているホストの最新のリスト（ある場合）を表示します（上記を参照）。 ボブがログインしようとしたときに、リモートホストが受け入れ可能なソースアドレスのリストに 192.168.1.3 を追加します
user duty <username> <duty hours> **user duty <username> none** **user duty bob Wk0900-1700|Sa1200-1300**	ユーザの勤務時間を制限します 勤務時間のパラメータは、ユーザがシステムにアクセスできる時間を示すために使用されます。 形式は日時範囲のエントリのリストです。 曜日は 2 文字で表示します：Mo、Tu、We、Th、Fr、Sa、Su。 すべての平日（土曜日と日曜日を除く日）は Wk で表され、週末は Wd で表され、すべての曜日は Al で表されます。繰り返される日は無効 MoMo = 曜日なし、MoWk = 月曜日を除くすべての平日になるため注意が必要です。 プレフィックス「!」が付いた曜日/時間範囲は、「次の文字以外」を示します。例: !MoTu は月曜と火曜以外の意味です。 時間範囲は 2 つの 24 時間表記 HHMM で、ハイフン「-」で区切られており、これは開始時刻と終了時刻を示します。 終了時刻が開始時刻より早い場合、その業務は翌日まで継続することを示します。 「|」記号を使用して複数のルールを組み合わせると、「または」を意味します。例：MoTu1200-1400|We1400-1500 は、月曜日または火曜日の 1200 から 1400、または水曜日の 1400 から 1500。 平日の営業時間の 9 時から 5 時と土曜日の 12 時から 13 時にボブへのアクセスを許可します

9.1 パスワード規則

パスワードの強制には 2 つの方法があります:

- 脆弱なパスワードを防ぐために、辞書をアップロードして新しいパスワードをチェックすることができます。 新しいパスワードが辞書内の項目と一致する場合、そのパスワードは拒否されます。
    - dictionary は、各行に 1 単語または 1 つの語句の dictionary という名前のテキストファイルでなければなりません。
    - 各行は、Windows のキャリッジリターンラインフィードシーケンスではなく、単一のラインフィード文字で終了する必要があります
    - SFTP を使用して辞書をアップロードし、チェックを有効にします。例：

```
sftp>put passwordlist.txt dictionary
```

- より安全なパスワードの使用を強制する多くのコマンドがあります。 これらすべてのコマンドには管理者レベルのアクセスが必要です。

注意：パスワードの有効期限は 6 か月です。

注意: 他の構成で管理者資格情報を再利用しないでください。 たとえば、TURN サーバーのユーザー名とパスワードは固有でなければなりません。

コマンド/例	説明/メモ
user rule max_history <number>	新しいパスワードとユーザーの以前のパスワードを比較して、パスワードの再使用を防止する
user rule password_age <番号>	パスワードの有効期間の上限を日数で指定します。
user rule min_password_age <番号>	パスワードをリセットできるようになるまでの最小間隔を設定することで、パスワード履歴コントロールが回避されるのを防ぎます。 メモ：この間隔は、管理者が「user expire <username>」コマンドを入力するとオーバーライドされます。
user rule min_length <number>	パスワードの最小文字数を設定します
user rule min_special <番号>	特殊文字の最小数を設定します: !@#$%^&*()_+=?><,."\/
user rule min_uppercase <番号>	パスワードに使用する最小の大文字数を設定します
ユーザ規則 (min_lowercase) <番号>	パスワードに使用する最小の小文字数を設定します
user rule longest_digits_run <番号>	パスワードで使用できる連続した数字の最大数を設定します
user rule min_digits <番号>	パスワードで使用できる数字の最小数を設定します
user rule max_repeated_char <番号>	繰り返すことができる最大連続文字数を設定します
user rule min_changed_ characters <number>	新しいパスワードで古いパスワードと異なる必要がある文字位置の最小数を設定します
ユーザルール only_ascii <true|false>	パスワードを ASCII 文字に制限する
ユーザルール no_username <true|false>	ユーザ名を含むパスワードが設定されるのを防ぎます。
user rule no_palindrome <true|false>	回文となるパスワードが設定されるのを防ぎます

コマンド/例	説明/メモ
user rule max_failed_logins <試行回数>	LDAP 経由で認証する MMP ユーザーまたは Cisco Meeting App ユーザーに対して、15 分間のロックが始まる前に許容されるログイン失敗回数を設定します。 ミーティングサーバ上で開催されるミーティングへのゲスト アクセスには影響しません。 0 に設定すると、このルールは有効な資格情報を持つユーザーをロックします。 **user rule max_ failed_logins <attempts>** を有効にするには、Call Bridge を再起動する必要があります。 変更はすぐに MMP ユーザに適用されます。 ロックされた MMP ユーザは MMP 管理者によりロック解除できますが、ロックアウトタイマーが切れる前に LDAP ユーザをロック解除することはできません。 ログイン失敗の最大回数が設定されていない場合、MMP ユーザに対してロックアウトメカニズムが無効になりますが、LDAP 経由で認証するユーザの既定のログイン試行の失敗数は 20 です。
ユーザルール max_idle<number>	アカウントがロックされるまでのアイドル状態を維持する最大日数を設定します。 最小値は 1 です。 メモ：アイドル時間が設定されていない場合、何も強制されません。
user rule max_sessions <number> **user rule max_sessions none**	ユーザーを SSH、SFTP、またはウェブ管理セッションの同時進行の数 <number> に制限します。 たとえば、セッションの最大数が 5 として設定されている場合、5 つの SSH、または 5 つのウェブ管理、または 5 つの SFTP セッションを同時に維持できます。 セッションの制限を解除します

9.2 Common Access Card (CAC) 統合

Common Access Card (CAC) は、コンピュータ機能にアクセスするための認証トークンとして使用されます。 CAC には抽出できない秘密鍵が含まれていますが、カード上の暗号ハードウェアで使用してカード所有者の身元を証明することができます。 ミーティングサーバは、CAC を使用した SSH およびウェブ管理インタフェースへの管理ログインをサポートしています。

コマンド/例	説明/メモ
cac **cac enable|disable** **cac enable strict**	現在の構成を表示します CAC ログインを有効にするには、cac enable を実行します これを（復旧ボタンの使用を除く）許可された唯一のリモートログイン方法にするには、cac enable strict を使用します。 このコマンドはシリアルケーブルを使った通常のログインを無効にします。 CAC ログインを有効にする前に、サービスが構成されていることを確認するためのチェックが行われます。 「strict」オプションによるパスワードログインをオフにする前に、セットアップが正しいかどうかをテストするために、「strict」を指定せずに cac enable を使用することが推奨されます。 メモ：クライアントログインへの証明書ベースのアクセスの拡張はベータ機能です。テスト環境でのみ使用し、本番環境では使用しないでください。 メモ： - cac が有効な場合、適切なクライアントからの証明書ベースのログインを使用することが可能です。 この方法で接続するユーザは、システムにアクセスするためにパスワードを入力する必要がありません。 - cac enable strict が適用されている場合、ユーザーは Cisco Meeting App にログインする前に CAC 経由でログインする必要があります。
cac issuer <issuer cert-bundle>	CAC ユーザを検証するには、SFTP を使用して発行元の証明書バンドルを MMP にアップロードする必要があります。 正当な資格情報は、発行者の証明書の 1 つによって暗号署名されます。そうでない場合、ログインは失敗します。 詳細については、サイトの暗号責任者に問い合わせてください。
cac ocsp 有効化|無効化	Online Certificate Status Protocol (OCSP) は、証明書の有効性と失効状況を確認するためのメカニズムです。 MMP はこれを使用して、ログインに使用された CAC が有効かどうか、特に失効していないかどうかを確認できます。 MMP が「strict」CAC モードで設定されている場合 (パスワードなしのログイン - 上記を参照)、証明書を失効させることで、MMP へのアクセスを一元的に制限できます。 OCSP は特別な設定なしで有効にできます。 このモードでは、OCSP レスポンダーの URL は、存在する場合、MMP に提示された CAC 資格情報から読み取られます。 OCSP レスポンダーが存在しない場合、または OCSP レスポンダーが利用できない場合 (ダウンしている、ルーティングできないなど)、CAC ログインは失敗します。

コマンド/例	説明/メモ
cac ocsp **レスポンダ** <URL|**なし**>	OCSP レスポンダの URL を設定するにはこのコマンドを使用します。 この URL は、CAC により提供される URL を上書きします。
cac ocsp certs<key-file> <crt-file>	一部の OCSP レスポンダーでは、OCSP 要求に要求者が署名する必要があります。 このコマンドは、この操作に対して秘密鍵と (一致する) 公開証明書を指定します。 OCSP レスポンダは、署名証明書が特定の認証機関、おそらく CAC 証明書の発行者によって署名されていることを要求する可能性があります。 これはサイトローカルな考慮事項です。
cac ocsp certs none	証明書の構成を削除します

9.2.1 SSH ログインの構成

X509 ベースの公開鍵交換は SSH クライアントで広くサポートされていないため、CAC を使用した SSH ログインには追加の構成手順が必要です。 CAC からの公開 X509 証明書を抽出し、それを SSH パブリックキーとして SFTP を使用して MMP にアップロードする必要があります。 CAC からパブリック X509 証明書を取得するにはさまざまな方法があります。最も簡単な方法の 1 つは、CAC が有効なウェブブラウザを使用してキーをエクスポートすることです。

Firefox **および** Chrome:

Firefox または Chrome ブラウザで、次のような URL を入力します。 https://ca.cern.ch/ca/Help/?kbid=040111。 手順に従って資格情報をエクスポートします。

エクスポート後、SFTP を使用して、pkcs#12 ファイルを <username>.pub MMP にアップロードします。<username> は、関連するユーザーのユーザー名に置き換えます。 その後、上記の説明に従って、次のコマンドを実行します：

```
pki pkcs12-to-ssh <username>
```

Internet Explorer:

IE は、CAC（パブリック）資格情報を DER でエンコードされた X509 としてエクスポートします。これは、アップロード可能で、追加の手順（cf. pkcs#12）を実行しなくても使用できます。

9.3 キーベースの SSH ログイン

キーベースの認証が成功した場合に SSH ログインがパスワード認証をバイパスするように、ミーティングサーバに SSH 公開キーをインストールすることができます。

手順の概要:

1. パブリックキーに **<username>.pub** と名付けます（**<username>** は、ログインに基づきキーを付与したい既存の Meeting Server MMP ユーザーで置き換えます）。
2. sftp the **<username>.pub** key to the **<CMS mmp address>**
3. ssh **<username>@<CMS mmp address>** を試行します（初回はパスワードが求められる場合がありますが、それ以降のログインではパスワードは必要ありません）。

9.4 SSH 指紋認証

取得したキーに対して Meeting Server がプロンプトしたキーを検証するには、**ssh server_key list** の MMP コマンドを使用します。

出力には、Meeting Server ホスト内のすべての既存キーのサイズ、タイプ、フィンガープリントのキーのリストおよび以下のキーが表示されます。

- ssh_host_dsa_key.pub
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key.pub
- ssh_host_key.pub
- ssh_host_rsa_key.pub

.

10 Cisco Jabber のプレゼンスを更新する Call Bridge の設定コマンド

Cisco Jabber のユーザーステータスを更新するために次の MMP コマンドが導入されました。

コマンド / 例	説明
callbridge ucm add <host-name/IP> <axl_user> <pres-ence_user>	ミーティングサーバに Cisco Unified Communications Manager ノードを追加します。 このコマンドは、AXL ユーザとプレゼンスユーザのパスワードの入力をユーザに促します。
callbridge ucm del <host-name/IP>	サーバから Cisco Unified Communications Manager を削除します。
callbridge ucm <hostname/IP> axl_service status	AXL サービスの状況を検証します。 このコマンドは、AXL ユーザのパスワードを入力するようにユーザにプロンプトします。
callbridge imps <host- name/IP> <presence_user> presence_service status	プレゼンスサービスの状況を検証します。 このコマンドは、プレゼンスユーザのパスワードを入力するようユーザにプロンプトします。
callbridge ucm list	ミーティングサーバに追加された Cisco Unified Communications Manager の詳細を、そのホスト名/IP、AXL ユーザ、およびプレゼンスユーザと共に一覧表示します。

10.1 Meeting Server と Cisco Unified Communications Manager/Cisco Unified Communications Manager IM & プレゼンスサーバ間でセキュリティで保護された通信を有効化する

エンティティ間で CA 証明書バンドルをインストールして検証することで、Meeting Server と Cisco Unified Communications Manager/Cisco Unified Communications Manager IM & プレゼンスサーバ間で安全な通信が可能になります。

IMP サーバ用の CUPS 証明書および Cisco Unified Communications Manager 用の Tomcat 証明書がミーティングサーバにアップロードされ、確認されている必要があります。

Cisco Unified Communications Manager および Cisco Unified Communications Manager IM & プレゼンスの証明書をインストールするには：

1. SFTP クライアントを使用してミーティングサーバにログインし、認証局バンドルファイルをミーティングサーバにコピーします。
2. ミーティングサーバの MMP に SSH で接続します。

3. 次のコマンドを使用して、Cisco Unified Communications Manager および Cisco Unified Communications Manager IM & プレゼンスの証明書を割り当てます：

   a. Cisco Unified Communications Manager の場合:

      callbridge ucm certs <cert-bundle>

   b. Cisco Unified Communications Manager IM & プレゼンスの場合：

      callbridge imps certs <cert-bundle>

Cisco Unified Communications Manager IM &プレゼンスの TLS 証明書を確認するには：Cisco Unified Communications Manager および
Cisco Unified Communications Manager IM & Presence サーバで次のコマンドを使用します:

1. ミーティングサーバと Cisco Unified Communications Manager 間の TLS 検証を有効/無効にするには:
   callbridge ucm verify <enable/disable>
2. Meeting Server および Cisco Unified Communications Manager IM & プレゼンス間の TLS 検証を有効または無効にするには、次を使用します：
   callbridge imps verify <enable/disable>
3. コマンドを使用してこれらの変更を適用するには、Call Bridge を再起動します。
   callbridgerestart
4. MMP コマンドを使用すると、Cisco Unified Communications Manager サービスを確認できます。
   callbridge imps <hostname/IP> <presence_user> presence_service status

---

メモ：MMP コマンドである **callbridge ucm certs none** または **callbridge imps certs none** を使用して、それぞれ Cisco Unified Communications Manager または Cisco Unified Communications Manager IM & プレゼンスの証明書を Meeting Server から削除します。

コマンド / 例	説明
callbridge ucm certs <cert-bundle>	Cisco Unified Communications Manager に CA の信頼できる証明書を追加します。
callbridge ucm verify <有効/無効>	ミーティングサーバと Cisco Unified Communications Manager 間の TLS 検証を有効/無効にします。
callbridge ucm certs none	ミーティングサーバと Cisco Unified Communications Manager 間の TLS 検証のために追加された証明書を削除します。
callbridge imps certs <cert-bundle>	Cisco Unified Communications Manager IM & プレゼンスサーバのための信頼できる CA 証明書を追加します。

コマンド / 例	説明
callbridge imps verify <有効/無効>	Meeting Server および Cisco Unified Communications Manager IM & プレゼンスサーバ間の TLS 検証を有効または無効にします。
callbridge imps certs none	ミーティングサーバと Cisco Unified Communications Manager IM & Presence サーバ間の TLS 検証のために追加された証明書を削除します。

11 アプリケーション構成コマンド

11.1 ウェブブリッジ 3 のコマンド

『導入ガイド』の指示に従ってウェブブリッジ 3 をセットアップします。このセクションでは、コマンドのリファレンスのみを提供します。

メモ：「Call Bridge to Web Bridge」プロトコル（C2W）は、Call Bridge と WebBridge3 間のリンクです。

Cisco Meeting Server web app を使用するために Web Bridge 3 をデプロイする MMP コマンド – ユーザーがミーティング（音声およびビデオ）に参加できるようにする Cisco Meeting Server 向けの新しいブラウザベースクライアント
– 下の表を参照してください。

コマンド	説明
webbridge3	Web Bridge 3 の現在の値セットを表示します
help webbridge3	すべての webbridge3 サブコマンドのヘルプを表示します
webbridge3 restart	WebBridge3 を再起動します
webbridge3 (enable|disable)	Web Bridge 3 を有効または無効にします。
webbridge3 https listen <*interface*:port allowed list>	ウェブブリッジ 3 がリッスンするインターフェースとポートをセットアップします。 **webbridge3 enable** コマンドを使用して、サービスがリッスンを開始するようにします。 ポートにデフォルト値はありません。指定する必要があります。
webbridge3 https certs <key-file> <crt-fullchain-file>	ウェブ ブリッジ 3 の HTTPS 証明書を設定します。これらの証明書はウェブブラウザに提示されるため、認証局 (CA) によって署名され、ホスト名/目的などが一致する必要があります。 (証明書ファイルは、エンド エンティティ証明書で開始し、ルート証明書で終了する証明書の完全なチェーンです。)
webbridge3 https certs none	HTTPS 証明書構成を削除します

コマンド	説明
webbridge3 https frame-ancestors <frame-ancestors space-separated string> **webbridge3 https frame-ancestors none** **webBridge3 https フレーム-先祖** **https://*.example.com** **https://customdomain.example2.com:8000**	管理者が、**content- security-policy** ヘッダーに返される frame- ancestors カスタム値を指定することを許可します。これにより、Web App を他のウェブページに埋め込むことができます。 クラスタのセットアップでは、このコマンドは展開内のすべてのウェブ ブリッジで設定する必要があります。 バージョン 3.2 から追加されました。
webbridge3 http-redirect (enable [port]|disable)	(オプション) HTTP 接続用のポートを設定することで HTTP リダイレクトを有効/無効にします。 このポートは、Web App が設定されているすべての Meeting Server インターフェイスに対して解放されます。 着信 HTTP 接続は、到達したインターフェイスに一致する HTTPS ポートに自動的にリダイレクトされます。 デフォルトポートは、80 です（**webbridge3 http-redirect enable [port]**で指定していない場合）。
webbridge3 c2w listen <*interface*:port allowed list>	C2W 接続を設定します。 ウェブブリッジ 3 がリッスンするインターフェースとポートをセットアップします。 **webbridge3 enable** コマンドを使用して、サービスがリッスンを開始するようにします。 このアドレス/ポートには、Call Bridge からのみアクセスできるようにすることをお勧めします。
webbridge3 c2w certs <key-file> <crt-fullchain-file>	C2W 接続の証明書を構成します。C2W 接続に使用される SSL サーバ証明書を構成する必要があります。C2W 証明書は、C2W プロトコル接続ポートに接続している Call Bridge にのみ提示され、ホスト名/目的などが一致する必要があります。 (証明書ファイルは、エンド エンティティ証明書で開始し、ルート証明書で終了する証明書の完全なチェーンです。)
webbridge3 c2w certs none	C2W 接続証明書の構成を削除します。
webbridge3 c2w trust <crt-bundle>	Web Bridge 3 C2W サーバーが Call Bridge クライアント証明書に対して検証する信頼できるバンドルを設定して、それらを信頼するかどうかを判断します。
webbridge3 c2w trust none	C2W 接続信頼バンドル構成を削除します。

コマンド	説明
webbridge3 audiopriflag (enable|disable)	Web App の自動優先設定機能を有効または無効にします。 コマンドが設定されていない場合、この機能はデフォルトで有効になります。 有効にする - Web App は、低帯域幅のシナリオでビデオとコンテンツ共有をオフにします。 無効にする - ウェブ アプリは、不安定なネットワークではアクションを実行しません。
webbridge3 options <space-separated options>	指定の機能をオンにします。複数の機能を有効にする場合は、feature_ names をスペースで区切ります。このコマンドは、Cisco サポートまたは Cisco EFT の指示の下でのみ使用してください。 これらの機能は本番環境での使用には適していません。 機能は、再起動しても有効なままですが、アップグレードコマンドを使用すると自動的に消去されます。 (このコマンドは現在サポートされていません。)
webbridge3 options none	webbridge options <feature_ name> コマンドを使用してこれまでオンだった機能をすべてオフにします。Cisco Support または Cisco EFT の指示の下でのみ使用してください。 (このコマンドは現在サポートされていません。)
webbridge3 status	ウェブブリッジ 3 の現在の設定を表示します

11.2 TURN Server コマンド

Expressway (Large OVA または CE1200) は、中程度のウェブ アプリ スケール要件を持つ展開 (つまり、800 コール以下) に推奨されるソリューションです。 Expressway (Medium OVA) は、小規模なウェブ アプリ スケール要件を持つ展開 (つまり、200 コール以下) で推奨されるソリューションです。 しかし、より大きなウェブ アプリ スケールを必要とする展開では、バージョン 3.1 から、必須のソリューションとして Cisco Meeting Server ウェブ エッジを推奨します。

メモ: TURN Server コンポーネントは Cisco Meeting Server 2000 では利用できません。

メモ: TURN サーバコンポーネントは、UDP の標準ポート 3478 を常にサポートします。Cisco Meeting Server ウェブエッジをデプロイする際、API ノード /turnServers "type"パラメータは「cms」に設定する必要があります。 このパラメータが未設定の場合、デフォルト値は、[標準（standard）] で、クライアントに TCP/UDP ポート 443 を使用して、TURN サーバーに接続するよう指示します。 type パラメータ値の詳細については、『Cisco Meeting Server API リファレンスガイド』の「*TURN サーバーを設定して変更する*」を参照してください。

TURN サーバの設定については、導入ガイドに記載されています。 このセクションでは、コマンドリファレンスについて説明します。

コマンド/例	説明/メモ
turn restart	TURN サーバを再起動します。
turn listen <interface allowed list|none> **turn listen a b**	リッスンするインターフェイスのリストをセットアップします。 リッスンを開始するには、turn enable コマンドを使用してサービスを有効化する必要があります。
turn listen none	TURN サーバーのリスニングを停止します。
turn tls <port|none>	TURN に使用する追加ポートを設定し、TURN の TCP 使用を有効にします。 メモ：すべての 3 つのサービスについて、指定されたポートとポート 3478 の両方で、TCP トラフィックと UDP をリッスンするように TURN を設定します。 このオプションは、TURN が UDP 以外の任意のサービスをリッスンするように、また TURN が 3478 以外の任意のポートをリッスンするように設定する必要があります。
turn certs <keyfile> <certificate file> [<cert-bundle>]	サーバ切り替えアプリケーション、およびオプションで、CA が提供する CA 証明書バンドルの秘密鍵ファイルの名前と .crt ファイルを定義します。(セクション 証明書によるプロビジョニングも参照してください。) このオプションは「turn tls <port>」を使用する場合に必要です。
turn certs none	証明書の構成を削除します。

コマンド/例	説明/メモ
turn (enable|disable)	TURN サーバを有効または無効にします。
turn credentials <username> <パスワード><領域> **turn credentials myusername mypassword example.com**	TURN サーバの長期資格情報を設定します。
turn public-ip <public ip> **turn delete public-ip**	TURN サーバのパブリック IP アドレスをセットアップします。 TURN サーバーのパブリック IP アドレスを削除します。
turn high-capacity-mode (enable|disable)	TURN と Web App が実行されている Meeting Server で増加した Web App リスケール（デフォルトで有効）のサポートを実装 – これは、ウェブエッジに Meeting Server を使用する際により高いパケットスループットを許可します。 Cisco サポートから指示された場合にのみ無効にしてください。 （バージョン 3.1 以降）
turn short_term_credentials_mode (enable|disable)	TURN サーバの資格情報モードの短期と長期を切り替えます。 デフォルトでは、**無効です** （バージョン 3.1 以降）
turn short_term_credentials <shared secret> <realm> **turn short_term_credentials mysharedsecret example.com**	TURN サーバが短期証明書を使用するために必要な共有シークレットと領域を指定します。 （バージョン 3.1 以降）

11.3 ウェブ管理インタフェースコマンド

メモ: ポート 8081 は、webadmin が有効な場合、ループバック時に予約されます。しかし、webadmin が無効の場合は、予約されません。 ポート 8080 は常に開いています。

コマンド/例	説明/メモ
webadmin	構成を表示します
webadmin restart	ウェブ管理インタフェースを再起動する
webadmin listen (a|b|c|d) [<port>] **webadmin listen a** **webadmin listen a 443**	ウェブ管理インターフェースがリッスンするためのインターフェースをセットアップします。 リッスンを開始するには、**webadmin enable** コマンドを使用してサービスを有効化する必要があります。 デフォルトはポート 443 です。

コマンド/例	説明/メモ
webadmin listen none	ウェブ管理インタフェースのリッスンを停止します。
webadmin (enable|disable)	ウェブ管理インターフェイスを有効または無効にします。 有効にすると、サービスを開始する前に、「リッスンするインターフェイスが設定されていること」、「証明書が一致していること」、「ポートが他のサービスと衝突していないこと」などいくつかのチェックが行われます。
webadmin certs <keyfile-name> <crt filename> [<crt-bundle>] **Webadmin 証明書 なし**	ウェブ管理インタフェースのキーファイルおよび .crt ファイルの名前を指定し、オプションで、CA が提供する CA 証明書バンドルを提供します 証明書の構成を削除します
webadmin http-redirect (enable|disable)	ウェブ管理インターフェイスの HTTP リダイレクトを有効または無効にします。
webadmin status	ウェブ管理インタフェースのステータスを表示します

メモ: MMP ユーザアカウントはウェブ管理インタフェースへのログインにも使用されます。

11.4 データベースクラスタリングコマンド

これらのデータベース クラスタリング コマンドは、『拡張性および復元力の導入ガイド』および『証明書のガイドライン』で説明されています。

バージョン 2.7 から、データベースクラスタはクラスタ中のデータベースを保持または接続する各ミーティングサーバで設定された同じ CA によって署名されたクライアントとサーバ証明書を必要とします。証明書の使用を強制することで、クラスター全体の機密性と認証の両方が保証されます。

メモ：データベースクラスタが、証明書が不要の以前のバージョンの Meeting Server ソフトウェアを使用して、証明書なしで設定された場合、バージョン 2.7 へのアップグレード時に、データベースは停止し、証明書が設定され、データベースクラスタが再作成されるまで到達不能になります。

メモ：<*ca_crt*> は、データベースクラスタ CA 証明書バンドルです。 これはトラストストアとしても使用され、バンドル内に存在するルート証明書で終わる有効な証明書の名前と証明書チェーンを提供するデータベース接続が承認されます。

コマンド/例	説明/メモ
database cluster status	このデータベースインスタンスの観点から、クラスタリングステータスを表示します。 **メモ**: 2.7 以降、このコマンドは構成済み証明書の欠如をハイライト表示します。
database cluster localnode <インターフェース>	このコマンドは、新しいデータベースクラスターを初期化する前に、最初のプライマリデータベースをホストするサーバで実行する必要があります。 <interface> は [a|b|c|d] の形式になります。インターフェイス名（最初の IPv6 アドレスが優先されますが、それ以外の場合は、最初の IPv4 アドレスが選択されます）例：database cluster localnode a ipv4:[a|b|c|d] - IPv4 に制限されたインターフェイス名（最初の IPv4 アドレスが選択されます）例：database cluster localnode ipv4:a ipv6:[a|b|c|d] - IPv6 に制限されたインターフェイス名（初めの IPv6 アドレスが選択されます）例：database cluster localnode ipv6:a <IP アドレス>- 特定の IP アドレス (IPv4 または IPv6) 例：database cluster localnode 10.1.3.9
database cluster initialize	このサーバーの最新のデータベースコンテンツを唯一のデータベースインスタンスであるプライマリとして新しいデータベースクラスタを作成します。 このコマンドは、postgres をクラスタモードに再設定します。つまり、外部インターフェイスをリッスンし、SSL を使用して、データベースクラスタを使用するようにローカルの Call Bridge（有効な場合）を再設定して再起動します。 **メモ：**2.7 以降、このコマンドは、有効な証明書、キー、CA 証明書がデータベースクライアントとサーバーにアップロードされていないと実行できません。

コマンド/例	説明/メモ
database cluster join <hostname/IP address>	プライマリデータベースのコンテンツをこのサーバーにコピーし、このサーバー上のデータベースの最新のコンテンツを破壊するクラスタの一部として、新しいデータベースインスタンスを作成します。 <hostname/ip address> は、クラスタ内の既存のデータベースにできます。 ローカル Call ブリッジが存在し、有効になっている場合、再設定して再起動し、データベース クラスタを使用します。 **注意**: 2.7 以降、このコマンドは有効な証明書、キー、および CA 証明書がデータベースクライアントとサーバにアップロードされていないと実行できません。
database cluster connect <hostname/IP address>	Call Bridge をデータベース クラスターに接続します。 データベースクラスタを使用するために Call Bridge（有効になっている場合）を再設定し、再起動します。 任意のローカル データベース (Call Bridge と同じホスト サーバ上) の使用を無効にします。ただし、データベースのコンテンツは保持され、このホスト サーバ上でデータベース クラスターの削除コマンドが実行された後でも読み取ることができます (以下を参照)。 **注意**: 2.7 以降、このコマンドは有効な証明書、キー、および CA 証明書がデータベースクライアントとサーバにアップロードされていないと実行できません。
データベースクラスタ証明書 **<server_key> <server_crt><client_key><client_crt><ca_crt>** **database cluster certs dbcluster_server.key dbcluster_server.crt dbcluster_client.key dbcluster_client.crt dbcluster_ca.crt**	データベースクラスターで接続を保護するために使用される証明書を設定します。 証明書は、データベースクラスターを有効にする前に構成する必要があります。
database cluster certs <client_key> <client_crt><ca_crt> **database cluster certs dbcluster_client.key dbcluster_client.crt dbcluster_ca.crt**	Call Bridge 上に共有データベースが存在しないデータベースクラスタで接続を保護するために使用される証明書を設定します。
database cluster certs none	証明書の設定を削除します。 データベースクラスタを再度有効にするには、証明書を再度設定する必要があります。

コマンド/例	説明/メモ
database cluster remove	データベースホストサーバーで実行されている場合は、クラスタから 1 つのデータベースを削除し、Call Bridge のみがあるホストサーバーで実行されている場合は、Call Bridge を「接続解除」します。またはサーバーがクラスタ化されたデータベースと Call Bridge の両方をホストしている場合は、両方を削除します。
database cluster upgrade_schema	クラスタのデータベース スキーマ バージョンをこのノードが要求するバージョンにアップグレードします。次のコマンドを実行することをお勧めします: • プライマリデータベース上。ただし、任意のデータベースインスタンスで実行できます • データベースインスタンスをホストしている任意のサーバーまたは Call Bridge で各ソフトウェアをアップグレードした後
database cluster clear_error	スキーマのアップグレード (前のコマンドを参照) などの前の操作が失敗した場合、このコマンドは状態を手動でリセットします。 このコマンドは Cisco サポートから指示された場合にのみ実行してください。
database cluster verifymode <full/ca>	データベース検証モードを設定します。 **full** - Meeting Server は他の検証と共に、サーバー ID がサーバー証明書に保管された名前と一致するかどうかを検証します。 **ca** - ミーティングサーバは、サーバのアイデンティティを検証することなく、ルート証明書までの証明書チェーンからノードを検証します。 指定がない場合、検証モードはデフォルトで ca です。

11.5 アップローダのコマンド

メモ: アップローダは Cisco Meeting Server 2000 では利用できません。

アップローダは、ビデオ コンテンツ管理に Vbrick Rev を使用することを簡素化します。 このセクションでは、アップローダのコマンド リファレンスを提供します。

コマンド	説明
アップローダ (enable|disable)	アップローダ コンポーネントを有効または無効にします。 アップロードを設定する前に、コンポーネントが無効になっていることを確認してください。
uploader nfs <host-name/IP>:<directory>	アップローダが監視する NFS を指定します。
uploader (cms|rev) host <host-name>	Meeting Server（cms）のホスト名と Vbrick Rev サーバーのホストで Uploader を設定します。 デフォルトのポートは 443 です。
uploader (cms|rev) port <port>	アップローダを、ミーティング サーバ (cms) への接続に使用するポートと Vbrick Rev サーバ用のポートを設定します。 デフォルトのポートは 443 です。
uploader (cms|rev) user <user-name>	ミーティング サーバの API へのアクセス権を持つユーザと Vbrick Rev サーバへのアクセス権を持つユーザでアップローダを構成します。
uploader (cms|rev) password	指定のミーティングサーバユーザと Vbrick Rev ユーザのパスワードを使ってアップローダを構成します。
uploader (cms|rev) trust (<crt-bundle>|none)	指定された証明書バンドルをミーティングサーバまたは Vbrick Rev サーバの信頼ストアにアップロードします。 **なし** 指定されたトラストストアから証明書のバンドルを削除します。 メモ: アップローダは、ミーティングサーバ信頼ストアおよび Vbrick Rev トラストストアに証明書バンドルがないと機能しません。
uploader edit (<uploader-team name>|none)	バージョン 2.4.0 ではサポートされていません。
uploader view (<uploader-team name>|none)	バージョン 2.4.0 ではサポートされていません。
uploader access <Private|Public|AllUsers>	ビデオ録画へのアクセス権限を設定する
uploader cospace_member_access <view|edit|none>	スペースのメンバーに、録画の表示と編集を許可します。**none** は、スペースのメンバーの表示または編集権限を削除します。
uploader recording_owned_by_cospace_owner <true|false>	true は、スペースの所有者をこれらのビデオ録画の単独の所有者として選択します。
uploader fallback_owner (<user-name>|none)	スペースの所有者が、VbrickRev でリストされていない場合、名前付きのユーザーをビデオ録画のフォールバック所有者として使用します。none は、フォールバック所有者を削除します。
uploader comments (enable|disable)	ビデオ録画へのコメントを有効または無効にします。 デフォルトでは無効になっています。

コマンド	説明
uploader ratings (enable|disable)	ビデオ録画評価を有効または無効にします。 デフォルトでは無効になっています。
uploader downloads (enable|disable)	ダウンロードの権限を設定し、ビデオ録画のダウンロードを有効または無効にします。
uploader initial_state (<active|inactive>)	Vbrick Rev. に最初にアップロードされたときの録画ビデオの初期状態を設定します。[デフォルト] がアクティブです。
uploader delete_after_upload (<true|false>)	アップロード完了後に NFS から録画を削除するかどうかを選択します。 デフォルトは false です。

メモ：uploader debug (<true|false>) コマンドは、バージョン 2.4 から削除され、デバッグ情報は自動で syslog サーバーに送信されます。

11.6 Recorder コマンド

メモ: レコーダーは Cisco Meeting Server 2000 では利用できません。

このセクションでは、レコーダーのコマンド リファレンスを提供します。 適切な導入ガイドの指示に従って、レコーダーをデプロイします。

コマンド/例	説明/メモ
recorder restart **recorder**	レコーダーを再起動します レコーダーの現在の構成を表示します
recorder sip certs	SIP 証明書を設定することを許可します （バージョン 3.0 から追加）。
recorder sip listen <interface> <tcp-port|none> <tls-port|none>	SIP レコーダー/ストリーマコンポーネントは、https 接続をリッスンする必要はありませんが、SIP 接続をリッスンする必要があります。 この新しい MMP コマンドは、TCP と TLS の両方を設定するために導入されました （バージョン 3.0 から追加）。
recorder sip trace <1m|10m|30m|24h|on|off>	すべての SIP メッセージのロギングをオンにします。 すべての SIP メッセージはレコーダーに記録されます。 デフォルトはオフです。 「on」で一定期間、または永久的に有効化できます。（バージョン 3.0 から追加されました。）

コマンド/例	説明/メモ
recorder limit <value|none>	拡張性を許可するためにレコーダー制限を設定します。これは、この上限を超えるとコールが拒否されるため、コール コントロールは別のデバイスにフェイルオーバーできます。 (バージョン 3.0 から追加)。
recorder (enable|disable)	レコーダーを有効または無効にします
recorder nfs <ホスト名/IP>:<ディレクトリ>	レコーダーにネットワークファイルサーバ (nfs) および録画を保存するフォルダの詳細を提供します。
recorder resolution <audio|720|1080>	レコーダーが録画するミーティングの解像度を設定します。 既定は 720p30 です。 1080 を選択すると、レコーダーは p30 を実行できます。 (バージョン 2.4 以降。)

11.7 ストリーマー コマンド

メモ: ストリーマは Cisco Meeting Server 2000 では利用できません。

このセクションでは、Streamer のコマンドリファレンスを提供します。 適切な展開ガイドの指示に従ってストリーマを展開します。

コマンド/例	説明/メモ
streamer restart **streamer**	Streamer を再起動する ストリーマの現在の設定を表示します
ストリーマ sip 証明書	SIP 証明書を設定することを許可します。 (バージョン 3.0 から追加。)
ストリーマの制限<値|なし>	拡張性を許可するためにストリーマ制限を設定します。この上限を超えると通話が拒否され、通話コントロールが別のデバイスにフェイルオーバーします。 バージョン 3.0 から追加されました。
ストリーマ sip リッスン <インターフェイス> <tcp-port|none> <tls-port|none>	SIP レコーダー/ストリーマー コンポーネントは、https 接続をリッスンする必要はありませんが、SIP 接続をリッスンする必要があります。 この新しい MMP コマンドは、TCP と TLS の両方を設定するために導入されました。 (バージョン 3.0 から追加されました。)
streamer (enable|disable)	Streamer を有効または無効にします。 設定する前に Streamer を無効にする必要があります。 設定が済んだら、ストリーマを有効にする必要があります。

11.8 MeetingApps コマンド

MeetingApps サービスはミーティング サーバに実装され、参加者がミーティング中にファイルを共有してアンケートを実行できるようにします。 他のサービスなしで、スタンドアロンの Meeting Server ノードで設定する必要があります。 Web App は、セキュリティで保護された環境で MeetingApps と通信し、ファイル共有とアンケートにアクセスします。

このセクションでは、MeetingApps を設定するコマンドを一覧します。 MeetingApps と Web Bridge を設定する手順は、『*導sss入ガイド*』に記載されています。

メモ：MeetingApps サービスは Meeting Server 2000 では設定できません。

コマンド / 例	説明
meetingapps	MeetingApps の設定済みパラメータを表示します。
meetingapps https listen <interface> <port>	MeetingApps がリッスンするインターフェイスとポートを設定します。
meetingapps https listen none	MeetingApps のインターフェイスとポート設定を削除します。
meetingapps gen- secret	ウェブブリッジと MeetingApp の接続を認証するために使用されるキーを生成します。
meetingapps https certs <key-file> <crt-fullchain-file>	MeetingApp の HTTPS 証明書を設定します。 有効な Certificate Authority（CA）によって署名された、公開・信頼されている HTTPS 証明書を使用することが推奨されます。
meetingapps https certs none	HTTPS 証明書の設定を削除します。
meetingapps (enable|disable)	MeetingApp を有効または無効にします。
meetingapps restart	MeetingApps サービスを再起動します。
meetingapps status	MeetingApps の状況を表示します。 たとえば、実行中、開始中などです。
webbridge3 meetingapps add <ホスト名><ポート> **<シークレットキー>**	MeetingApps のホスト名、ポート番号、**meetingapps gensecret** コマンドを使用して生成された秘密鍵を設定します。
webbridge3 meetingapps add none	Web Bridge で設定されている MeetingApps を消去します。
meetingapps dbcleanup	古いファイルまたはデータをデータベースから消去します。 **メモ：**このコマンドは、MeetingApps サービスが無効な場合に実行する必要があります。

12 その他のコマンド

12.1 モデル（Model）

コマンド/例	説明/メモ
モデル	Cisco Meeting Server 展開モデルを表示します。 仮想化デプロイが CMS VM として表示されます。

12.2 Meeting Server のシリアル番号

コマンド/例	説明/メモ
シリアル番号:	ミーティングサーバのシリアル番号を表示します。 このコマンドは仮想展開には適用されないことに注意してください。

12.3 本日のメッセージ

管理者権限を持つ MMP ユーザは、このセクションのコマンドを発行できます。

メモ: motd コマンドは、ミーティングアプリのバージョン 1.9 以前でのみサポートされています。

コマンド/例	説明/メモ
motd	ある場合、その日の最新のメッセージを表示します。
motd add "<message text>"	ログイン後、バナーに <message> を表示します 2048 文字以下のメッセージは、SFTP で「motd」にファイルをコピーすることで設定できます。
motd del	[今日のメッセージ] を削除します。

12.4 ログイン前の法的警告バナー

組織がログイン前の法的警告を要求している場合、管理者権限を持つ MMP ユーザは次のコマンドを使用できます。

コマンド/例	説明/メモ
`login_warning`	最新のログイン警告メッセージを表示します（ある場合）。
`login_warning add "<message>"`	ログインする前に法的警告を表示する 2048 文字を超えないメッセージは、SFTP でファイルを [login_warning] にコピーすることで設定できます。
`login_warning del`	法的警告を削除します

12.5 SNMP コマンド

メモ：Meeting Server 2000 は SNMP をサポートしないため、snmp コマンドは使用できません。

12.5.1 一般情報

MIB は SFTP を使用して任意の Cisco ミーティングサーバからダウンロードできます。

仮想展開 (Cisco ミーティングサーバ 1000、または仕様ベースの VM サーバ) の MIB ファイルは以下のとおりです。

- ACANO-MIB.txt
- ACANO-SYSLOG-MIB.txt

これらのファイルを SNMP 実装の検索パスに配置します。例： ~/.snmp/mibs (Net- SNMP 用)。

メモ：MIB は今後のリリースで名前が変更される予定で、Cisco Meeting Server へのブランド変更を反映します。

MMP インターフェイスは最小限のユーザ設定オプションのみを提供します。 より複雑な要件を処理するには、MMP インターフェイスを使用して初期ユーザーを作成し、ユーザーデータベースを直接管理します。たとえば、Net-SNMP パッケージの snmpusm を使用します。

ミーティングサーバは、SNMP バージョン 1/2c と 3 の両方をサポートしています。設定はそれぞれで異なります。 SNMP バージョン 1/2c のセキュリティへの影響に注意してください。強力な認証をサポートしていないため、コミュニティ文字列を知っている人は誰でもサーバにクエリを実行できます。

12.5.2 SNMP v1/2c コマンド

v1/2c のアクセス コントロールは「コミュニティ」に基づいています。 これらは、SNMP が無効になっている場合、MMP インターフェイス経由で作成できます。

コマンド/例	説明/メモ
snmp community add <name> [IP address/prefix] **snmp community del <name>**	v1/2c のアクセス コントロールは「コミュニティ」に基づいています。 これらは、SNMP が無効になっているときに、MMP 経由で作成および削除できます。 **メモ**：SNMP コミュニティ名には英数字と下線のみ使用できます。ダッシュを含むその他の特殊文字はエラーメッセージを返します。
snmp community add public	コミュニティ文字列「public」を使用すれば、どこからでも完全なツリーにアクセスできるようになります。
snmp community add local 10.1.0.0/16	アクセスを許可しますが、指定されたサブネットからのアクセスに限定します。
snmp (enable|disable)	SNMP v1/2c を有効/無効にします

12.5.3 SNMP v3 コマンド

v3 のアクセス制御はユーザに基づいています。 これらは MMP インターフェイスから作成できます。

コマンド/例	説明/メモ
snmp user add <name> <パスワード>(MD5|SHA) (DES|AES)	v3 のアクセス制御はユーザに基づいています。 指定されたパスワードで認証に「MD5」アルゴリズム、暗号化に「DES」アルゴリズムを使用して、完全なツリーへのアクセス権を持つユーザーを作成します。 **注意**：SNMP ユーザ名には英数字とアンダースコアのみ使用できます。ダッシュを含むその他の特殊文字がある場合はエラーメッセージが返されます。
snmp user del <name>	SNMP ユーザを削除します。
snmp (enable|disable)	SNMP v3 を有効/無効にします。

12.5.4 SNMP トラップレシーバーの設定

コマンド/例	説明/メモ
snmp trap enable <hostname> <agent community string> snmp trap disable **snmp trap enable mybox public**	SNMP トラップ レシーバを設定します。 <hostname>はトラップを受信するマシンのホスト名で、 <community string>は、使用されるコミュニティ文字列です。

12.6 システムログのダウンロード

システムログは最大 100MB です。 この制限に達すると、最も古いメッセージが破棄され、新しいメッセージのためのスペースを作ります。 ログが 75% に達すると SNMP トラップが生成されますの容量。

コンプライアンスまたはその他の理由でログデータを保持する必要があり、リモート syslog サーバが使用されていない場合、次のことができます:

- SFTP ツールを使用して MMP に接続し、システムログファイルをサーバーからローカルファイルストアにコピーします。 これにより、最新のコンテンツはそのまま残ります
- **syslog rotate <filename>** コマンドを使用すると、ログファイルを永久的に保存できます。 アクティブなシステムログは空になります。 この保存したファイルは SFTP を使用してダウンロードできます

  例：**syslog rotate mylog**
- audit ロールが付与されているユーザーは、**syslog audit rotate <filename>** を使用して監査ログを保存できます。

12.7 ログバンドルの生成とダウンロード

ミーティングサーバは、ミーティングサーバの様々なコンポーネントの構成と状態を含むログバンドルを生成することができます。 このログバンドルには、syslog および live.JSON ファイルが含まれます。 問題に関して Cisco サポートに連絡する際は、これらのファイルをご提供いただくと、早く分析ができます。

ミーティングサーバのログバンドルは以下の方法で生成されます:

- Meeting Server 管理者は、MMP 管理者ユーザー資格情報を使用して、SFTP クライアントを MMP IP アドレスに接続すると、ログ バンドル ダウンロード プロセスを開始できます。 システムは、logbundle.tar.gz というファイル名でログバンドルを生成しダウンロードします。
- 代わりに、管理者は、**generate_logbundle** コマンドを使用してダウンロードプロセスを開始する前に、ログバンドルを生成できます。 generatedlogbundle.tar.gz という名前のログバンドルが生成されます。

コマンド/例	説明/メモ
generate_logbundle	それぞれの Meeting Server で generatedlogbundle.tar.gz というファイル名のログバンドルを生成します。 **メモ**: このコマンドが実行されるたびに、前に生成されたログバンドルが最新のログバンドルで置換されます。

以下の手順でログ バンドルをダウンロードします。

1. SFTP クライアントを MMP の IP アドレスに接続します。
2. MMP 管理者ユーザの資格情報を使用してログインします。
3. ログバンドルをダウンロードする場所でこれらのコマンドを実行します。
   a. **sftp get logbundle.tar.gz**
   b. **sftp get generatedlogbundle.tar.gz**
4. logbundle.tar.gz/generatedlogbundle.tar.gz ファイルをローカルフォルダにコピーします。
5. ファイル名を変更し、ファイル名の logbundle の箇所を変更し、ファイルを生成するサーバーを特定します。 これは複数サーバの展開では重要です。
6. 名前を変更したファイルを分析のために Cisco サポート担当者に送信します。

log bundle.tar.gz の初期ファイルサイズは、1 KB です、SFTP 経由で転送した場合、サイズは、ファイル数とそのサイズに応じて大きくなります。

メモ：お使いのコンピューターと Meeting Server 間でネットワーク接続が遅いなどの原因で logbundle がダウンロードできない場合は、ログファイルと live.json ファイルをダウンロードして、Cisco サポートにご送信ください。

12.8 ディスク使用量

コマンド/例	説明/メモ
df	MMP とモジュール 0 の両方のディスク使用量を、パーティションごとの使用量と inode 使用量で表示します。

12.9 システム構成のバックアップと復元

メモ: バックアップコマンドは仮想化ソリューションでも利用できます。

コマンド/例	説明/メモ
バックアップリスト	サーバ上のバックアップファイルの一覧を表示します。
バックアップスナップショット <name>	ミーティングサーバの完全なスナップショットを作成します。 SFTP 経由でダウンロードするためのファイル <name>.bak が作成されます。 このコマンドを定期的に使用することを強く推奨します。 ファイル名の最大文字数は 256 です。 **注意**: バックアップファイルには SSO ファイルとローカルでホストされているブランディングファイルは含まれません。
backup rollback <name>	バックアップされたサーバのシステムを復元します。これにはサーバの構成のロールバックが含まれます。 ミーティングサーバ上にバックアップファイルがない場合は、このロールバックコマンドを実行する前に、SFTP を使用してミーティングサーバにバックアップファイルをアップロードする必要があります。 ファイル名の最大文字数は 256 文字です。 メモ: このコマンドは、システム上の license.dat ファイルおよびすべての証明書と秘密鍵だけでなく、既存の設定を上書きし、ミーティングサーバを再起動します。 そのため、使用には注意が必要です。 このバックアップを別のサーバに復元する場合、既存の license.dat ファイルと証明書を事前にコピーしておく必要があります。バックアップのロールバックプロセス中にこれらが上書きされるためです。 license.dat ファイルはサーバーの MAC アドレスに関連付けられるため、別のサーバーのバックアップから復元すると失敗し、サーバーがオンラインに戻った後に、置き換える必要があります。

12.10 ミーティングサーバのアップグレード

コマンド/例	説明/メモ
アップグレード [<filename>]	ミーティングサーバをアップグレードします。 このコマンドを発行する前に、アップグレードしたいバージョンのイメージファイルをアップロードしておく必要があります。 アップグレード時に、システム全体のバックアップが自動的に作成されます。 バックアップ名は現在のソフトウェアバージョンに由来します。例えば、R2.9 から R3.0 へのアップグレードの場合、バックアップの名前は 2_9.bak になります。 ファイル名が指定されていない場合のデフォルトのファイル名は、upgrade.img です。 バージョン 3.0 以降、このコマンドは、指定されたイメージで Meeting Server をアップグレードをする前に、署名と整合性チェックを行います。**upgrade <name> verify** コマンドが以前にそのイメージを実行していた場合でも、チェックは行われます。 バージョン 3.0 から更新されました。 バージョン 3.7 以降、Meeting Server は、データベースクラスタがサーバー設定で有効かどうかを特定し、それに応じて、アップグレードするまえにノードのクラスタ解除を行うようユーザーに通知します。30 秒以内に CTRL+C を押すと、アップグレードプロセスを中止できます。
upgrade <filename> [no-backup]	慎重に使用してください。
アップグレードリスト	システム上のアップグレードイメージの一覧を取得するには
upgrade delete <name> **upgrade delete upgrade.img**	アップグレードイメージは、SFTP またはこの CLI コマンドを使用して削除されるまで保持されます。
upgrade <filename> verify	アップグレード中に通常行われるすべての整合性と署名のチェックを行いますが、アップグレードは続行しません。 このコマンドを使って画像の種類を表示することもできます。 バージョン 3.0 から追加されました。
authenticity	実行中のイメージがどのように検証されたか（キーのタイプと名前）、現在ロードされているパブリックキーとその詳細（タイプ、名前、ソース）など、ソフトウェアの信頼性に関するすべての情報を表示します。 また、キーが信頼できるものかどうかも表示します。SPECIAL キーがインストールされている場合、その署名が MASTER キーで検証されたかどうかを検証します（他のキーは内部で、 常に信頼されています)。 バージョン 3.0 から追加されました。

コマンド/例	説明/メモ
authenticity key add <キーファイル>	SPECIAL キーをインストールします。 SPECIAL キーは一度に 1 つしかインストールできません。 バージョン 3.0 から追加されました。
認証キー なし	現在インストールされている SPECIAL キーを削除します。 このコマンドは、別のキーをインストールする前にキーを削除する場合、またはキーが使用されなくなった場合に使用する必要があります。 バージョン 3.0 から追加されました。

12.11 ミーティングサーバをリセットする

コマンド/例	説明/メモ
factory_reset (full|app)	「フル」オプションはすべてのユーザ設定を削除します。システムにインストールされた資格情報はすべて失われます。 その後、『設置ガイド』の手順を実行して、Meeting Server を再度デプロイする必要があります。 「アプリ」オプションは、Active Directory 同期データとスペース (coSpace)、Lync および SIP 構成を削除します。MMP 構成は残ります。 コマンドが完了すると、システムが再起動されます。

付録 A バージョン 3.0 MMP コマンドの削除

3.0 の Meeting Server から削除された機能やコンポーネント関連のすべての MMP コマンドは以下のとおりです。

- H.323 ゲートウェイコマンド (**h323_gateway**)
- Web Bridge 2 コマンド（**webbridge**）
- XMPP サーバコマンド (**xmpp**)
- XMPP multi-domains コマンド（**xmpp multi_domain**）
- XMPP resiliency コマンド（**xmpp cluster**）
- Load Balancer コマンド（**loadbalancer**）
- トランクコマンド (**trunk**)
- SIP edge コマンド（**sipedge および edge-related callbridge**）
- XMPP に依存するレコーダーとストリーマのコマンド
- X シリーズサーバに適用可能な MMP コマンド

表 1：Meeting Server 設定関連で削除されたコマンド

コマンド/例	説明/メモ
状態	Meeting Server の温度、電圧、その他正常性に関する情報を表示します。 メモ：health コマンドは、仮想化デプロイでは利用できません。
callbridge trust xmpp <trusted xmpp certificate allowed list	XMPP サーバのアイデンティティを検証するために、特定の許可リストの証明書を使用するように、Call Bridge を設定します。 (バージョン 2.4 以降)
callbridge trust xmpp none	XMPP 証明書許可リストを Call Bridge 信頼ストアから削除します。 (バージョン 2.4 以降)

表 2: 削除された XMPP サーバコマンド

コマンド/例	説明/メモ
xmpp **xmpp status**	現在の構成を表示します
xmpp restart **xmpp domain <domain-name>**	XMPP サーバーを再起動する XMPP サーバーのコンポーネントシークレットを作成します
xmpp listen <interface allowed list|none> **xmpp listen a b** **xmpp listen none**	インターフェイスの許可リストをセットアップします。 xmpp enable コマンドでリッスンを開始するには、サービスを有効にする必要があります。 XMPP サーバーのリスニングを停止します
xmpp (enable|disable)	XMPP サーバーを有効または無効にします
xmpp certs <key-file> <crt-file> [<crt-bundle>] **xmpp certs none**	XMPP サーバのキー ファイルと証明書ファイルの名前、およびオプションで、CA が提供する CA 証明書バンドルを定義します。 証明書の構成を削除します
xmpp motd add <message> **xmpp motd del**	Cisco ミーティング アプリまたは XMPP クライアントのログイン時に表示される「今日のメッセージ」を設定します。 日次メッセージを削除します。 2048 文字以下のメッセージは、SFTP で xmpp.motd にファイルをコピーすることで設定できます。 xmpp.motd を何らかの方法で変更すると、XMPP サーバが再起動されます。 **メモ： motd** コマンドは、バージョン 1.9 以前の Meeting Server バージョンでのみサポートされています。
xmpp max_sessions <number> **xmpp max_sessions none** **xmpp max_sessions 3**	各ユーザが XMPP サーバで保持できる同時 XMPP セッションの数、つまり同時ログイン数を制限します。 これにより、単一のユーザがシステムリソースを使い果たすことを防ぎます。 ユーザごとの XMPP セッションの制限を削除します。 ユーザに最大で iPad、iPhone、および PC のログインしかないと予想される場合、最大セッション数を 3 に設定します。

コマンド/例	説明/メモ
	これらの xmpp callbridge コマンドについては、『拡張性および復元力の導入ガイド』で説明されています。
xmpp callbridge add <component name>	新しい Call Bridge からの接続を許可するように XMPP サーバを設定します。 メモ：シークレットが生成されます。これは、XMPP 復元力を設定する際に必要です。 その Call Bridge の [ウェブ] 管理インターフェイスに移動し、XMPP サーバに接続するように設定します。
xmpp callbridge del <component name>	Call Bridge が XMPP サーバにアクセスするのを停止します。
xmpp callbridge list	各 Call Bridge では、ドメイン、component_secret、および接続状況を一覧表示します
xmpp callbridge add-secret <callbridge>	XMPP 復元に必要です。 XMPP クラスタの他のノードに、Call Bridge をクラスタの最初のノードに接続することで生成されたシークレットを追加するために使用します。
xmpp リセット	XMPP サーバーをスタンドアロン設定に戻します（追加された Call Bridge を削除します）。 設定を再起動する必要がある場合にのみ、このコマンドを使用します。

表 3: 削除されたロードバランサーコマンド

コマンド/例	説明/メモ
loadbalancer list [<tag>]	すべてのロードバランサー設定を一覧表示するか、タグが指定されている場合は、そのロードバランサーの設定のみを一覧表示します
loadbalancer (enable|disable) <tag> **loadbalancer enable exampleEdge**	ロードバランサーを有効または無効にします パブリックポート（下記参照）は、サービス接続へのトランクが作成されるまで解放されないのでご注意ください。
loadbalancer create <tag> **loadbalancer create exampleEdge**	Creates a load balancer
loadbalancer trunk <tag> <iface> [:<port>] **loadbalancer trunk exampleEdge a:3999** **loadbalancer public <tag> <iface> [:<port allowed list>]** **loadbalancer public exampleEdge b:5222** **loadbalancer public exampleEdge b:5222 lo:5222**	トランク インターフェイスとポートを設定します パブリック インターフェイスとポート (クライアント接続を受け入れるため) を設定します 共通エッジデプロイでは、Web Bridge も有効にし、Core to Edge トランクを使用する必要があります。 これを許可するには、ループバック インターフェイスをパブリック インターフェイスとして設定します。

コマンド/例	説明/メモ
loadbalancer auth <tag> <key-file> <cert-file> <trust-bundle> **loadbalancer auth exampleEdge acano.key acano.crt trust.pem**	トランクへの認証に使用される秘密鍵と証明書、およびトランクによって提供される信頼できる証明書を設定します。 TLS 接続の作成時にトランクが信頼バンドル内のいずれかの証明書を提示し、ロードバランサーが提示する証明書をトランクが承認する場合、接続は成功します。 具体的には、信頼バンドルに証明書の有効なチェーンが含まれており、チェーンの最後に CA が発行した提示された証明書がある場合、認証は成功します。 そうでない場合、接続は拒否されます。 特に、自己署名証明書が使用される場合、公開証明書を信頼バンドルに配置できるため、認証は成功します。
loadbalancer delete <tag>	ロードバランサ設定を削除します。

表 4：削除された Trunk コマンド

コマンド/例	説明/メモ
トランクリスト [<タグ>]	すべての Core 設定を一覧表示するか、タグが指定されている場合はその Core の設定のみを一覧表示します
trunk (enable|disable) <tag>	Core を有効または無効にします
trunk create <tag> <port or service name> **trunk create trunktoExampleEdge xmpp**	XMPP のトランク インスタンスを作成します。
トランク エッジ **<tag><edge name|ip address>[:<port>]**	トランクする Edge のドメイン名または IP アドレスを設定します。 ドメイン名は複数の IP アドレスに解決されることに注意してください。 その場合、すべてのアドレスに対して接続が試みられます。 ポートが指定されていない場合、ポートはドメイン名の DNS SRV ルックアップによって発見できると想定されます
trunk auth <tag> <key-file> <cert-file> <trust-bundle>	エッジ サーバへの認証に使用される秘密鍵と証明書、およびエッジ サーバによって提供される信頼できる証明書を構成します。
trunk delete <tag>	Core 構成を削除します。

コマンド/例	説明/メモ

trunk debug <tag>	このコマンドは、Cisco サポートの指示の下でのみ使用してください。 診断結果は以下のとおりです。
	- エッジサーバ名の DNS 結果
	- TLS 接続を作成し、各アドレスに対して認証を試みます
	- 成功した場合、コアサーバからのデバッグ情報。これには以下が含まれます。
	  - 問題のエッジサーバへの「コア」接続 (エッジサーバへのトランク接続) のリスト
	  - そのエッジサーバにより現在処理されているクライアント接続
	  - Edge サーバーのメモリ使用統計情報

表 5：XMPP マルチドメインをサポート関連で削除されたコマンド

コマンド/例	説明/メモ
xmpp multi_domain add <domain name> <key-file> <crt-file> [<crt-bundle>]	XMPP サーバがリッスンする別のドメインを追加します。 CA から提供された秘密鍵、証明書、およびオプションの証明書バンドルを指定します。この変更を有効にするために XMPP サーバを再起動してください。 メモ: XMPP サーバは、秘密鍵または証明書ファイルがないか無効な場合には起動しません。
xmpp multi_domain del <domain name>	XMPP サーバがリッスンするドメインを削除します。
xmpp マルチドメイン リスト	XMPP サーバーがリッスンするドメインを一覧します。

表 6：削除された XMPP resiliency コマンド

コマンド/例	説明/メモ
xmpp cluster enable|disable	XMPP クラスタリングを有効/無効にします。 XMPP クラスタの有効化は、ノードで XMPP を有効にする前に行う必要があります。 XMPP クラスタが無効で XMPP が開始されている場合、スタンドアロンモードで XMPP サーバーが開始されます。
xmpp cluster trust <trustbundle.pem>	XMPP クラスタが信頼する証明書バンドルを指定します。 <trustbundle.pem> は、クラスタ内の XMPP サーバーのすべての証明書を含む必要があります。 証明書は、XMPP を使用してすでに XMPP サーバーに適用されている必要があります。 certs コマンド。 このメカニズムにより、クラスター内の異なる xmpp ノードがお互いを信頼し、フェイルオーバー操作とノード間のトラフィックの転送を有効にします。
xmpp cluster status	xmpp クラスターのライブ状態を報告します。 クラスタが失敗した場合、このコマンドはこのミーティングサーバ上で実行されている xmpp サーバの統計のみを返します。 このコマンドを使用して、接続の問題の診断を試みてください。
xmpp cluster initialize	クラスターを初期化します。 このコマンドで 1 ノードのライブ xmpp クラスターが作成されますが、他のノード (xmpp サーバ) をこのクラスターに参加させることができます。
xmpp cluster join <cluster>	このノードをクラスタに追加します。 <cluster> は、クラスタの最初のノードの IP アドレスです（コマンド xmpp cluster initialize を参照してください）。
xmpp cluster remove	このノードをクラスタから削除します。 これには、ノードが稼働している必要があります。
xmpp cluster remove <node>	指定されたノードをクラスターから削除します。ここで、 <ノード>は、ノードの IP アドレスまたはドメイン名です。 これにより、ノードが応答しない場合に、クラスターからノードを削除することができます。

コマンド/例	説明/メモ
xmpp callbridge add-secret <callbridge> シークレットを入力してください：<シークレット>	Call Bridge シークレットを XMPP サーバに追加します。 クラスター内の最初の XMPP サーバ ノードに Call Bridge を接続するときに作成されたシークレットで、他のノードを構成するために使用されます。 このコマンドにより、Call Bridge は多くの XMPP サーバと資格情報を共有できます。

表 7: 削除されたウェブ ブリッジ コマンド (レガシーのウェブ ブリッジ 2 のセットアップ用)

コマンド/例	説明/メモ
webbridge restart **webbridge status**	ウェブブリッジを再起動する 現在の構成を表示します
webbridge listen <a|b|c|d|none [:<port>] allowed list> **webbridge listen a b**	ウェブ ブリッジが待機するインターフェースとポートをセットアップします。 webbridge enable コマンドを使用して、サービスがリッスンを開始するようにします。 オプションのポート引数のデフォルトは 443 です。
webbridge listen none	Web Bridge のリッスンを停止します。
WebBridge (enable|disable)	Web Bridge を有効または無効にします
webbridge certs <keyfile-name> <crt ファイル名>[<crt-バンドル>] **webbridge certs none**	Web Bridge のキーファイルおよび .crt ファイルの名前を指定し、オプションで、CA が提供する CA 証明書バンドルを提供します 証明書の構成を削除します
webbridge clickonce <url|none> **webbridge clickonce none**	clickonce リンクのロケーションを定義します。 URL の先頭には http://、https://、または FTP:// が必要です。また、それは有効な URL でなければなりません。 ユーザーが、Internet Explorer（clickonce でサポートされている唯一のブラウザ）を使用して、会議招待リンクまたは coSpace ウェブリンク（例：https://www.join.cisco.com/invited.sf?id=1234）をたどると、ユーザーはデフォルトではなく、設定された clickonce ロケーションにリダイレクトされます。 このリダイレクトが発生すると、PC クライアントが自動的に起動し (まだインストールされていない場合はダウンロードされ)、call/coSpace がダイヤルされます。 すべての clickonce リダイレクト動作を無効にします

コマンド/例	説明/メモ
webbridge msi (<url>|none) **webbridge dmg (<url>|none)** **webbridge ios (<url>|none)** **webbridge ios none**	WebRTC ユーザに提供される Windows msi、Mac OSX dmg、iOS インストーラのダウンロード場所を設定します 設定解除するには、パラメータ none を使用して適切なコマンドを使用します
webbridge trust <crt-bundle|crt-file> **webbridge trust none**	ゲスト アカウントとカスタマイズ内容 (背景画像など) の設定をどの Call Bridge インスタンスに許可するかを制御します。 信頼できる Call Bridge が Web Bridge と同じサーバーで実行されている場合、Call Bridge 公開証明書/証明書バンドルの名前を指定して webbridge trust コマンドを発行するだけで十分です。 Call Bridge が別のサーバで実行されている場合、Call Bridge の公開証明書/証明書バンドルは、まず SFTP を使用してウェブブリッジサーバにコピーする必要があります。 **メモ：** クラスタ化された Call Bridge デプロイで、Call Bridge に異なる証明書がある場合、証明書を 1 つのバンドルにまとめます。
webbridge trust xmpp <trusted xmpp certificate allowed list>	XMPP サーバのアイデンティティを検証するために、証明書の特定の許可リストを使用するようにウェブブリッジを設定します。 （バージョン 2.4 以降）
webbridge trust xmpp none	ウェブブリッジの信頼ストアから XMPP 証明書許可リストを削除します。 （バージョン 2.4 以降）
webbridge http-redirect (enable|disable)	HTTP リダイレクトを有効/無効にします
webbridge url-redirect (<url>|none)	URL リダイレクトの場所を設定します。 設定を解除するには、**none** パラメータを指定してコマンドを使用します
WebBridge オプション<feature_name1 feature_name2> **WebBridge オプション cma.webrtc.ios**	指定の機能をオンにします。複数の機能を有効にする場合は、feature_ names をスペースで区切ります。 このコマンドは、Cisco サポートまたは Cisco EFT の指示の下でのみ使用してください。 これらの機能は本番環境での使用には適していません。 機能は再起動しても有効のままですが、upgrade コマンドを使用すると自動的に消去されます。 (バージョン 2.5 以降)。
webBridge オプション なし	**webbridge options <feature_name>** コマンドを使用して、これまでオンだった機能をすべてオフにします。 Cisco Support または Cisco EFT の指示の下でのみ使用してください。 (バージョン 2.5 以降)。

表 8：SIP Edge コンポーネント設定関連で削除されたコマンド

コマンド/例	説明/メモ
callbridge add edge <ip address>:<port>	Call Bridge が使用する SIP Edge を追加します。
callbridge del edge	SIP Edge を削除します
callbridge trust edge <certificate file>	SIP Edge との間の接続で信頼する Call Bridge の証明書を指定します。 これは SIP Edge の証明書です。
sipedge プライベート<インターフェイス>:<ポート>	Call Bridge の接続の内部インターフェイスとポートを指定します
sipedge public <interface>:<port>	外部システムとの間で接続するための外部インタフェースとポートを指定する
sipedge パブリック IP<アドレス> **sipedge パブリック IP なし**	SIP Edge に到達できる NAT アドレスを構成または削除します。
sipedge certs <key-file> <crt-file> <trusted-bundle>	Call Bridge からの接続用の SIP Edge のプライベートキーと証明書、そして信頼できる証明書のバンドルを設定します。
sipedge の有効化 **sipedge の無効化**	SIP Edge コンポーネントを有効または無効にします
sipedge restart	SIP Edge コンポーネントを再起動します。 SIP エッジで証明書を変更した後にこのコマンドを使用します。 重要な通話がアクティブなときは、このコマンドを使用しないでください。

表 9：Meeting Server による H.323 通話の受発信用設定関連で削除されたコマンド

コマンド/例	説明/メモ
h323_gateway enable/disable/restart	ゲートウェイは適切に構成されていない限り開始されません。
h323_gateway certs <keyfile> <証明書ファイル>[<cert- バンドル>]	プライベートキーファイルと.crt ファイルの名前を定義します H.323 ゲートウェイアプリケーションおよび、オプションで、CA により提供される CA 証明書バンドル。(セクション 証明書によるプロビジョニングも参照してください。)
h323_gateway certs none	証明書の構成を削除します

コマンド/例	説明/メモ
h323_gateway h323_nexthop <host/ip> **h323_gateway del h323_nexthop**	すべての発信 H.323 通話にこの IP アドレスを接続し、この IP アドレス のデバイスがルーティングを処理するようにします。このアドレスが設定されていない場合、IP ダイヤルのみが機能します。 通常、この IP アドレスは Cisco VCS/Polycom DMA であり、Cisco Meeting Server H.323 ゲートウェイとサードパーティデバイス（H.323 ゲートキーパー）間で H.323 トランクが確立されます。 H.323 ゲートウェイはデバイスに登録せず、通話をそれらに転送するだけです。デバイスは、これらの通話を受け入れるように適切に設定する必要があります。
h323_gateway default_uri <uri> **h323_gateway del default_uri**	これはオプションです。 着信 H.323 通話に宛て先が無い場合（通常、H.323 ゲートウェイが IP アドレスでダイヤルされている場合のみ）、SIP コールは、default_uri に設定されたものに対して行われます。 default_uri は、IVR を指すか、または直接 coSpace を指します。 設定されていない場合、呼び出しは拒否されます。
h323_gateway sip_domain<uri> **h323_gateway del sip_domain <uri>**	これはオプションです。 宛先アドレスにドメインを含まずにゲートウェイに着信 H.323 通話が発信された場合、Call Bridge への SIP コールが発信される前に、@<sip_domain>が宛先アドレスに追加されます。
h323_gateway sip_domain_strip <はい/いいえ>	[はい（yes）] に設定され、「h323_gateway sip_domain」が設定されている場合、SIP コールがゲートウェイに発信されるとき、H.323 コールが発信される前に、発信元アドレス（存在する場合）から @<sip_domain>が削除されます。 H.323 コール。
h323_gateway h323_domain <uri> **h323_gateway del h323_domain <uri>**	これはオプションです。 発信元アドレスにドメインを含まないでゲートウェイに H.323 コールを発信する場合、SIP コールが発信される前に発信音アドレスに @<h323_domain> が追加されます。
h323_gateway h323_domain_strip <はい/いいえ>	[はい（yes）] に設定され、「h323_gateway h323_domain」が設定されている場合、SIP コールが発信され、H.323 コールが発信される前に、宛先アドレス（存在する場合）から @<h323_domain> が削除されます。
h323_gateway h323_interfaces <interface list> **h323_gateway sip_interfaces <インターフェースリスト>**	ゲートウェイを開始するために設定する必要がありますが、実際の設定では現在無視されています。

コマンド/例	説明/メモ
h323_gateway sip_port <port>	SIP 側がリッスンするポート。 デフォルトは 6061 です。 メモ：デフォルトポートを 6061 から変更する場合で、H.323 ゲートウェイと Call Bridge が同じサーバーにある場合、Call Bridge が使用しているポート 5061 を使用しないでください。 ゲートウェイが再開されるまで、変更は適用されません。 H.323 ゲートウェイは常に TLS 接続を想定しています。そのため、Call Bridge の発信ダイヤルプランルールで [暗号化済（Encrypted）] を選択する必要があります。
h323_gateway sip_proxy <uri>	これを Call Bridge の IP アドレスに設定するか、複数の Call Bridge がある場合はドメイン名（DNS 経由）を使用します。 すべての着信 H.323 通話はこの URI に転送されます Call Bridge と H.323 ゲートウェイが同じホスト上にある場合、IP アドレス 127.0.0.1 を使用します。 Call Bridge と H.323 ゲートウェイが異なるホスト上にある場合は、Call Bridge の IP アドレスを使用します。
h323_gateway restrict_codecs <はい/いいえ>	「はい」に設定すると、H.323 ゲートウェイは、相互運用性の問題を引き起こす可能性が低いコーデックの安全なセットに制限されます。 現在このセットは G.711/G.722/G.728/H.261/H.263/H.263+/H.264 です。 この機能により無効になるコーデックは、G.722.1 および AAC です。
h323_gateway disable_content <はい/いいえ>	「はい」に設定すると、H.239 コンテンツは無効になります。
h323_gateway trace_level <level>	Cisco サポートによるトラブルシューティングを支援するために、追加のログを提供します。 レベル 0、1、2、または 3 のトレースを提供するように求められる場合があります。

表 10：削除された XMPP recorder コマンド

コマンド	説明
recorder listen <a|b|c|d|lo|none [:<port>] allowed list> **recorder listen a b**	レコーダーがリッスンするインターフェイスとポートをセットアップします。 recorder enable コマンドを使用して、サービスがリッスンを開始するようにします。 オプションのポート引数のデフォルトは 443 です。
recorder listen none	レコーダーの聞き取りを停止します。
recorder certs <keyfile-name> <crt ファイル名>[<crt-バンドル>]	Recorder のキーファイルおよび .crt ファイルの名前を指定し、オプションで、CA が提供する CA 証明書バンドルを提供します
ストリーマ証明書なし	バージョン 3.0(ベータ 2) で廃止されました。 証明書の構成を削除します
recorder certs none	証明書設定を削除する
streamer trust <crt-bundle|crt-file>	レコーダーへの接続を許可する Call Bridge インスタンスを制御します。 信頼できる Call Bridge が Recorder と同じサーバーで実行されている場合、Call Bridge 公開証明書/証明書バンドルの名前を指定して recorder trust コマンドを発行するだけで十分です。 Call Bridge が別のサーバで実行されている場合、Call Bridge の公開証明書/証明書バンドルは、まず SFTP を使用してレコーダーが有効になっているサーバにコピーする必要があります。

表 11: 削除された XMPP ストリーマコマンド

コマンド	説明
streamer listen <a|b|c|d|lo|none [:<port>] allowed list> **recorder listen a b**	Streamer がリッスンするインターフェイスとポートをセットアップします。 streamer enable コマンドを使用して、サービスがリッスンを開始するようにします。 オプションのポート引数のデフォルトは 443 です。
ストリーマ証明書なし	証明書の構成を削除します
ストリーマ証明書<keyfile-name> <crt ファイル名>[<crt-バンドル>]	Streamer のキーファイルおよび .crt ファイルの名前を指定し、オプションで、CA が提供する CA 証明書バンドルを提供します

コマンド	説明
streamer trust <crt-bundle|crt-file>	ストリーマへの接続を許可する Call Bridge インスタンスを制御します。 信頼できる Call Bridge が streamer と同じサーバーで実行されている場合、Call Bridge 公開証明書/証明書バンドルの名前を指定して streamer trust コマンドを発行するだけで十分です。 Call Bridge が別のサーバで実行されている場合、SFTP を使用して有効になっているストリーマを使用して、サーバーに Call Bridge の公開証明書/証明書バンドルを最初にコピーする必要があります。
streamer trust none	信頼設定の設定を解除します。
streamer listen <a|b|c|d|lo|none [:<port>] allowed list> **recorder listen a b**	Streamer がリッスンするインターフェイスとポートをセットアップします。 streamer enable コマンドを使用して、サービスがリッスンを開始するようにします。 オプションのポート引数のデフォルトは 443 です。

Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 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。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

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

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

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

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

Cisco の商標または登録商標