Cisco WebEx Meetings Server Release リリース 2.8 のプランニングガイドとシステム要件

初版：2016 年 11 月 01 日

最終更新：2017 年 04 月 14 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.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、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

一般的なシステム要件 1

Cisco WebEx Meetings Server ベストプラクティス 6

WebEx生産性向上ツール 8

ユーザ 8

システムでの展開サイズ 8

vCenter 共存の要件 9

システムの仮想マシン 9

ハードウェアの最低必要要件 10

CWMS および ESXi ホストが消費するリソース 12

50 ユーザーのシステム 13

250 ユーザーのシステム 16

800 ユーザーのシステム 20

2000 ユーザーのシステム 23

システム容量マトリックス 28

サポートされているアップグレードパス 32

サポートされているアップグレードパス 34

Cisco WebEx Meetings Server の紹介 37

Cisco Unified MeetingPlace のお客様向け情報 39

シングルデータセンターの展開 39

シングルデータセンターを結合してマルチデータセンター (MDC) システムを作成 40

システムでの VMware vSphere の使用 40

VMware vSphere に現行システムに展開するメリット 41

IOPS およびストレージシステムのパフォーマンス 43

VMware vSphere ESXi のインストールとストレージの構成 45

ミーティングへの参加 46

ネットワーク上での仮想マシンのレイアウト 49

システムに応じた異なるタイプのネットワークトポロジ 50

内部インターネットリバースプロキシ (IRP) のネットワークトポロジ 50
非スプリットホライズンネットワークトポロジ 51
すべての内部ネットワークトポロジ 53
スプリットホライズンネットワークトポロジ 54
HA または MDC 展開の冗長性 56
インターネットリバースプロキシに関するネットワークの検討事項 58
ネットワーク帯域要件 60
マルチデータセンターのネットワーク要件 64
帯域幅集約のための NIC チーミング 65
ロードバランシング 66
システムのネットワークチェックリスト 69
自動展開およびパブリックアクセスによるインストールまたは拡張のネットワークチェックリスト 71
手動展開、パブリックアクセスおよびすべての内部仮想マシンによるインストールまたは拡張のネットワークチェックリスト 73
自動展開、パブリックアクセスおよび非スピリットホライズンDNSによるインストールまたは拡張のネットワークチェックリスト 77
手動展開、パブリックアクセスおよび非スピリットホライズンDNSによるインストールまたは拡張のネットワークチェックリスト 79
自動展開、パブリックアクセスおよびスピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト 83
手動展開、パブリックアクセスおよびスピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト 85
自動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト 89
手動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト 91
WebEx サイト および WebEx 管理のURL 93
すべての仮想マシンが内部ネットワークにある場合のポートアクセス 95
DMZ ネットワーク内のインターネットリバースプロキシを使用するポートアクセス 95
外部ファイアフォールのポートアクセス 96

内部ファイアウォールのポートアアクセス 97
VMware vCenter ポート 102
Cisco WebEx Meeting Center ポート 103
システムでの NAT の使用 104
フォワードプロキシ 107
Cisco Unified Communications Manager（CUCM）の設定 109
MDC 環境での CUCM 110
開始する前に 110
MDC 環境の CUCM 安全電話会議 111
マルチデータセンターの CUCM 構成チェックリスト 111
高可用性を含む、または含まない CUCM 構成チェックリスト 112
CWMS マルチデータセンターシステムでの CUCM の構成 113
200 または 800 ユーザーのマルチデータセンターシステムにおける CUCM の構成 113
2000 ユーザーのマルチデータセンターシステムにおける CUCM の構成 115
高可用性と非高可用性システムの CUCM の設定 116
高可用性なしの 50、250、800 ユーザーシステムでの CUCM 設定 116
高可用性の 50、250、800 ユーザーシステムでの CUCM 設定 117
高可用性の 2,000 ユーザーシステムがない CUCM 設定 118
高可用性の 2,000 ユーザーシステムでの CUCM 設定 119
SIP トランクセキュリティプロファイルの設定 121
Outlook 連携を無効にするロードバランスポイントの SIP トランクセキュリティプロファイルの設定 121
アプリケーションポイントの SIP トランクセキュリティプロファイルの設定 122
SIP プロファイルの設定 123
標準 SIP プロファイルの設定 123
TLS SIP プロファイルの設定 123
IPv6 SIP プロファイルの設定 124
TLS を使用する CUCM 証明書管理 124
Cisco WebEx Meetings Server 証明書のアップロード 125
サードパーティの CUCM 証明書のインストール 125
CUCM 証明書のダウンロード 127
証明書署名リクエスト（CSR）バージョン 2.6 以降の生成 127

証明書署名リクエスト（CSR）バージョン 2.5 以前の生成 129
SIP トランクの設定 131
ロードバランスポイントへの SIP トランクの設定 131
アプリケーションポイント用の SIP トランクの設定 133
ルートグループの設定 134
ルートリストの設定 135
ルートパターンの設定 136
SIP ルートパターンの設定 137
CUCM 機能の互換性とサポート 137
オーディオエンドポイント互換性 140
アプリケーションのダウンロードについて 143
管理サイトからのアプリケーションのダウンロード 144
アプリケーション ZIP ファイルの内容 145
アプリケーション言語キー 145
生産性向上ツール ZIP ファイルの内容 146
WebEx Meetings Client ZIP ファイルの内容 147
ネットワーク録画プレーヤー ZIP ファイルの内容 147
Cisco WebEx 生産性向上ツールの複数展開 148
コマンドラインを使用した生産性向上ツールのサイレントインストール 148
コマンドラインインターフェースを使用した生産性向上ツールのサイレントアンインストール 150
SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度 150
SMS システム毎無人プログラムを使用する WebEx 生産性向上ツールの提供 151
SMS システム毎無人プログラムを使用する生産性向上ツールのコンポーネントの削除 152
SMS システム毎無人プログラムを使用する生産性向上ツールの追加 153
SMS システム毎無人プログラムを使用する生産性向上ツールのアンインストール 155
プログラムの提供による WebEx 生産性向上ツールの新しいバージョンへの更新 155
定義からのパッケージの作成 156
Meetings アプリケーションの複数展開 156

Cisco WebEx Meetings のインストール 157
ローカルで Cisco WebEx Meetings アプリケーションのアンインストール 157
コマンドラインを使用したミーティングアプリケーションのサイレントインストール 158
コマンドラインインターフェースを使用したミーティングアプリケーションのサイレントアンインストール 158
SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度 159
SMS システム毎無人プログラムを使用する生産性向上ツールの提供 159
SMS システム毎アンインストールプログラムを使用する Cisco WebEx Meetings アプリケーションのアンインストール 161
ネットワーク録画プレーヤーの複数展開 161
ネットワーク録画プレーヤーのインストール 161
コマンドラインを使用した Recording Player のサイレントインストール 162
コマンドラインインターフェースを使用した Recording Player のサイレントアンインストール 163
Microsoft Systems Management Server 2003 (SMS) を使用した CWMS アプリケーションのインストール 163
SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度 163
SMS システム毎無人プログラムを使用する Cisco WebEx ネットワーク録画プレーヤーの提供 164
システム毎アンインストールプログラムを使用する Cisco WebEx ネットワーク録画プレーヤーのアンインストール 165
更新実行後の設定の再構成 166
シングルサインオンの概要 167
シングルサインオンの利点 168
SAML 2.0 シングルサインオンの設定の概要 169
エンドユーザと管理用のサインインのための SAML SSO 170
クラウドベースの WebEx ミーティングサービスと WebEx Meetings Server の間の SAML 2.0 シングルサインオンの違い 171
SAML アサーション属性 177
サポートされている SAML アサーション属性 177
オプションのパラメーター 181

タイムゾーン値 181
国番号 185
地域の値 195
言語の値 196
言語コード 197
ミーティング録画のためのストレージ要件 199
システムバックアップファイル用ストレージ要件 200
サポートされている SNMP MIB 201
CWMS システム情報 MIBS 201
CPU 関連の MIB 202
CWMS メモリ情報 205
ディスク使用率 206
サポートされている SNMP トラップ 207
通知イベント 207
トラップデータ 208
共通の PC システム要件 211
Windows のオペレーティングシステム要件 212
MACのオペレーティングシステム要件 216
モバイルデバイスのオペレーティングシステム要件 216
Citrix XenDesktop および XenApp の対応 217
Cisco WebEx Meetings アプリケーションおよび生産性向上ツール互換性マトリクス 217
主催者ライセンスについて 220
Cisco Unified Communications Manager (CUCM) の統合 221
Session Manager Edition (SME) 統合に対応しています。 221
オーディオエンドポイント互換性 222

第 1 章

一般的なシステム要件

Cisco WebEx Meetings Server は、このセクションに記載の仕様に適合している Cisco UCS サーバーと互換性があります。

重要

リリース 1.x からリリース 2.0 またはリリース 2.5 など、Cisco WebEx Meeting Server のメジャーリリースに対するアップグレードを実行するとき、管理仮想マシンを含む ESXi ホスト (Cisco UCS サーバー) には最低 1.5 TB の空き容量が必要です。 さまざまなサイズのユーザーシステムについて説明している、本文書中の50 ユーザーのシステム, （13 ページ）から始まるセクションを参照してください。 アップグレード中は、ネットワーク上で同時に 2 セットの仮想マシンが存在する必要があります。Release 1.x を実行中の元の仮想マシンとアップグレード用の仮想マシンです。 詳細については、http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.htmlの『CWMS管理者ガイド』の「システムのアップグレード」を参照してください。

モジュール	要件に関するメモ
ホストのサーバーおよびプロセッサ	• Cisco UCS「*C-series*」ラックサーバーまたは同等の「*B-series*」ブレードサーバー。 • AES-NI インストラクションセットがサポートします。 • 2.4 GHz 以上のプロセッサクロック速度。 （注） サードパーティーのハードウェアはサポート対象外です。

モジュール	要件に関するメモ
ネットワークインターフェース これらの要件は、（Cisco WebEx Meetings Server 仮想マシンの）ESXi ホスト間にある NIC とイーサネットスイッチに適用され、外部ネットワークインターフェースには適用されません。	• 非冗長設定で最小 1 物理 NIC。 インターネットリバースプロキシ（IRP）と管理仮想マシンがホストを共有する場合の特定の要件については、50 ユーザーのシステム，（13 ページ）セクションを参照してください。 • 冗長設定には、すべての NIC インターフェースを重複し（*teamed* または *bonded*）、独立したスイッチ・ファブリックに接続する必要があります。 • VMware 管理ネットワーク用に追加 NIC （オプション）
[1]ESXi ホスト用に Internal（DAS）ストレージ（内部仮想マシンが展開されている場合）	• 最低でも RAID-10 または RAID-5 構成で 4 ドライブ • システムを新規に展開またはアップグレードするには、最低で 1.5 TB の使用可能ストレージが必要です • Cisco WebEx Meetings Server リリース 1.X を 2.X へアップグレードする場合、お使いのシステムおよび仮想マシンのサイズによってそれぞれ、各 ESXi ホストには 172 GB から 1118 GB までの空き容量が必要です。 さまざまなサイズのユーザーシステムについて説明している、本文書中の50 ユーザーのシステム，（13 ページ）から始まるセクションを参照してください。 • ESXi 用にオプションの 2 つめのアレイ （注） 仮想マシンはストレージにシックプロビジョニングを使用する必要があります。
ESXi ホスト用に Internal（DAS）ストレージ（IRP仮想マシンが展開されている場合）	• RAID-1構成で最低ドライブ 2 個 • 使用可能ストレージ 300 GB 以上 • 内部仮想マシンと同じ設定を使用可能 （注） 仮想マシンはストレージにシックプロビジョニングを使用する必要があります。

モジュール	要件に関するメモ
SAN ストレージ	• DASの代理として使用できます（同じ量の保存容量を割り当てることを推奨します）。 • B シリーズのブレードサーバーには、2 つのハードディスクドライブだけがあります。 Cisco UCS B-シリーズブレードサーバーを使っていてCWMS リリース 2.X へのアップグレードを予定している場合、RAID 5 またはRAID 10 設定のいずれかで4つのハードディスクドライブに対応するためには SAN ストレージを使う必要があります。 • サポート担当者が SAN のパフォーマンスをモニタリングおよび調整する展開にのみ推奨。 （注） 新しい Vmware 要件、および今後のシステムの成長のためにさらにストレージを追加する責任は自分にあります。 • ファイバーチャンネル（FC）または 10 GB イーサネット以上のファイバーチャンネル（FCoE）のみ。 • パフォーマンス要件は DAS と同様です。 • vSphere で測定された最小総遅延は 20 ms です。詳細については、「ストレージ」セクション（http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage）を参照してください。 • 仮想マシンに必要な合計容量: CWMS システムの各仮想マシンに予約されたストレージリソースの合計。 （注） 仮想マシンはストレージにシックプロビジョニングを使用する必要があります。

モジュール	要件に関するメモ
[2]NAS ストレージ	• DAS または SAN の代理として使用できます（同じ量の保存容量を割り当てることを推奨します）。 • Cisco UCS C サーバーラックを備えた NAS ストレージサーバーの使用を推奨します。 • サポート担当者が NAS のパフォーマンスをモニタリングおよび調整する展開にのみ推奨。 新しい Vmware 要件、および今後のシステムの成長のためにさらにストレージを追加する責任は自分にあります。 • ファイバーチャンネル（FC）、ネットワークファイルシステム（NFS）、SCSI のみ。詳細については、http://docwiki.cisco.com/wiki/UC_Virtualization_Storage_System_Design_Requirements#General_Guidelines_for_SAN.2FNAS を参照してください。 • パフォーマンス要件は DAS と同様です。 • vSphere で測定された最小総遅延は 20 ms です。詳細については、http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage を参照してください。 • 仮想マシンに必要な合計容量: CWMS システムの各仮想マシンに予約されたストレージリソースの合計。 • ファイルサーバーは、アレイ統合の vStorage API（VAAI）をサポートし、シックプロビジョニングを使用する必要があります。 （注） NAS ストレージのデフォルトプロビジョニングスキームはシンプロビジョニングですが、仮想マシンはストレージのためにシックプロビジョニングを使用する必要があります。（シンプロビジョニングはサポート対象外です。） NAS ストレージの展開に対してシックプロビジョニングを使用できるようにするために、ストレージベンダーは Cisco WebEx Meetings Server 展開で使用するすべての UCS サーバーにインストールする必要がある VAAI のプラグインを提供します。

モジュール	要件に関するメモ
ハイパーバイザ	ESXi バージョンおよび vSphere ライセンスはハードウェアの最低必要要件, （10 ページ） セクションで説明されています。 VMware Vsphere が必要でこれのみをサポートします。他のハイパーバイザ製品はサポート対象外です。 vCenter Server 5.0、5.0 アップデート 1、5.0 アップデート 2、5.1、5.1 アップデート 1、5.5、 6.0（CWMS 2.6MR1 以降） vSphere ライセンスについてはハードウェアの最低必要要件 セクションに記載されています。 プロセッサソケット当たりに 1 つの VMware ライセンス 共存: • vCenter は、システム要件にプロセッサとメモリ要件が追加されている CWMS と共存できます。 • vCenter 共存設定は、50 および 250 ユーザーシステムのみでサポートされています。 • 同じ物理的 ESXi ホスト上での Cisco Unified Communications 製品との共存はサポートされていません。 • 同じ物理 ESXi ホスト上での非 CWMS 仮想マシンとの共存はサポートされていません。 システムの電源が入っている状態での Distributed Resource Scheduler（DRS）、クローニング、フォールトトレランス（FT）、および vMotion またはストレージ vMotion などの高度 VMware vSphere 機能はサポート対象外です。
メールサーバ	• システムがメール送信に使用するメールサーバの完全修飾ドメイン名 （FQDN）。 • SMTP ポート番号のデフォルト値は、25 または 465（安全な SMTP ポート番号） です。 • サードパーティの証明書を備えた、TLS 対応の電子メールサーバーを使用するには、証明書をシステムにインポートする必要があります。 詳細については、http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.htmlにある『管理者ガイド』の「証明書の管理」を参照してください。

モジュール	要件に関するメモ
ライセンス数	MDC ライセンス—MDC ライセンスは、マルチデータセンターシステム中の各データセンターに必要です。 MDC ライセンスはシングルデータセンターを備えたシステムに必要です。 主催者ライセンス—ミーティングを主催する各ユーザーは、WebEx Web、WebEx 音声、パーソナル会議、またはブラストダイヤルミーティングの主催者ライセンスを持っている必要があります。 主催者ライセンスの詳細については、主催者ライセンスについて，（220ページ）を参照してください。

1 組織にストレージ領域ネットワーク（SAN）を管理する専門知識がある場合、直接接続されたストレージ上での SAN をお勧めします。 SAN はローカルディスクアレイよりも信頼性があります。
2 ネットワークファイルシステム（NFS）にデータベースやミーティング録画の定期的な自動バックアップを保管するための十分な容量があることを確認してください。 (CWMS は NFS バージョン 2、3、4 をサポートします。)

- Cisco WebEx Meetings Server ベストプラクティス，6 ページ
- WebEx生産性向上ツール，8 ページ
- ユーザ，8 ページ
- システムでの展開サイズ，8 ページ
- vCenter 共存の要件，9 ページ
- システムの仮想マシン，9 ページ
- ハードウェアの最低必要要件，10 ページ
- システム容量マトリックス，28 ページ
- サポートされているアップグレードパス，32 ページ
- サポートされているアップグレードパス，34 ページ

Cisco WebEx Meetings Server ベストプラクティス

以下は Cisco WebEx Meetings Server システムを構成し、維持するときに参照する必要があるベストプラクティスのリストです。

- UPS を使用して仮想マシンホストの電源を入れて、電源の中断を最小限に抑えます。 電源障害が繰り返されると、ホストシステムや仮想マシンが損傷することがあります。
- システムを常にメンテナンスモードにしてから、ゲストオペレーティングシステムをシャットダウンします。

- システムシャットダウンを必要とするスケジュールされたイベントやその他の状況では、ゲストオペレーティングシステムをシャットダウンすることにより、仮想マシンを自動シャットダウンします。
- システムは必要な場合に自動的に修理するように設計されており、再起動によりこのプロセスが中断する場合があります。 修正するために、システムを再起動することはお勧めしません。 システムが不健全な状態にある場合は、Cisco TAC にご連絡ください。 システムは指示されたとき、またはデータセンターのメンテナンスなどスケジュールされたイベントのときにのみ電源を切るようにします。
- ネットワーク冗長性を構成して、ネットワーク障害を最小限に抑えます。 詳細は、『*Cisco WebEx Meetings Server* 管理者ガイド』の「高可用性システムの追加について」のセクションを参照してください。
- 仮想マシンのスナップショットを使用すると、システムの負荷があまりかかっていないときでも、ユーザエクスペリエンスに影響を与えるようにシステムパフォーマンスに悪影響を与えることがあります。
- システムに問題がある場合、VMware VCenter 環境をチェックして、VCenter またはネットワークの状況が問題を生じさせているかどうかを判断してください。
- 障害が発生した場合でも、システムが動作を継続できる確率を高めるために、高可用性を設定します。
- 高可用性システムがあり、セカンダリシステムが故障した場合、既存のセカンダリシステムを削除し（『*Cisco WebEx Meetings Server* 管理ガイド』の「高可用性システムの削除」を参照）、新しいセカンダリシステムを追加することで修理できます（『*Cisco WebEx Meetings Server* 管理ガイド』の「高可用性システムの追加」を参照）。 高可用性システムのプライマリシステムが失敗した場合、この手順を使用して修理できません。 災害復旧手順を使用してプライマリシステムを回復してから、新しいセカンダリシステムを追加することをお勧めします。 新しいセカンダリシステムを追加するまで、お使いの展開は完全な冗長性なしに動作します。 この手順は、セカンダリ仮想マシンのどれかが故障した場合に予期しない障害を避けるのに役立ちます。 詳細については、『*Cisco WebEx Meetings Server* 管理ガイド』の「災害復旧機能の使用」を参照してください。
- システムはNFSに最新のシステムのバックアップのみを維持し、毎日、それ以前のインスタンスは削除するため、他のメディアに最近のバックアップをいくつか維持することをお勧めします。

制約事項 NFS ファイルとディレクトリでさまざまなスクリプトを実行するため、Cisco WebEx Meetings Server が使用する NFS 共有でファイルまたはディレクトリを手動で作成しないでください。 NFS ストレージサーバーは Cisco WebEx Meetings Server が独占的に使用する必要があります。

- ダッシュボードを使用して、NFS、CPU、およびストレージの健全状態を監視します。 ストレージと CPU のダッシュボード警告が有効になっていることを推奨します。

- もしディレクトリ統合を使用する場合は、「*Cisco WebEx Meetings Server* 管理ガイド」の「ユーザーの管理」にある「ディレクトリ統合の設定」の情報を参照してください。
- Cisco WebEx Meetings Server を使用する場合、CallManager インターフェースの CUCM 上の関連する SIP トランクの [Media Termination Point が必要] チェックボックス（**[トランク設定]** ページ内）が解除されている必要があります。 詳細については、ロードバランスポイントへの SIP トランクの設定, （131 ページ） および アプリケーションポイント用の SIP トランクの設定, （133 ページ） をご覧ください。
- Cisco WebEx Meetings Server Release 2.0 以降を実行し、B シリーズのブレードサーバーを使用する場合、ハードドライブの要件を満たすために、SAN ストレージを使用する必要があります。 SAN の要件の詳細については、一般的なシステム要件, （1 ページ）を参照してください。

WebEx生産性向上ツール

WebEx 生産性向上ツールによって、ユーザーは Microsoft® Outlook® などのアプリケーション中から、WebEx Meetings セッションを開始、スケジュール、または参加できます。 Cisco WebEx 生産性向上ツールに関する詳細情報については、http://www.webex.com/support/productivity-tools.htmlを参照してください。

Cisco WebEx Meetings Server は [設定] > [ダウンロード] ページから入手できる、最新バージョンの WebEx アプリケーションをサポートします。 システムのアップグレードを実行したあと、ユーザーが WebEx 生産性向上ツールの古いバージョンを実行している場合、ミーティングをスケジュール、開始、および参加できますが、最新の機能は利用できません。 最適な環境にするため、最新の WebEx 生産性向上ツールの .msi を静かにプッシュすることを推奨します。 (Cisco WebEx Meetings アプリケーションおよび生産性向上ツール互換性マトリクス, （217 ページ）を参照。)

ユーザ

システムは、最大40万ユーザアカウントをライフタイムサポートします。 この数値には、アクティブおよび非アクティブのユーザアカウントが含まれます。 この最大数は、ユーザデータベースの予測成長に対応できる数値です。

管理者はユーザーをシステムから削除できません。 その代わり、ユーザーは非アクティブ化されます。 この設計により、ユーザが長期間アクティブでない場合でも、前に無効化したユーザアカウントを管理者が再度アクティブにすることができます。 ユーザのミーティングや他のコンテンツ（録画を含む）は復元できます。

システムでの展開サイズ

システムのサイズを決定する際は、ある時点で何人のユーザがシステムを使用すると予想されるかを考慮してください。 たとえば、50ユーザーシステムでは、同時にミーティングに出席できる最大数は 50 です。 50 人より多くのユーザーがミーティングに参加しようとする場合、ユーザー

の最大数を超えた後でミーティングに参加しようとするすべてのユーザーに対し、エラーメッセージが表示され、システムはこれらのユーザーがミーティングに参加することを禁止します。

- 50 ユーザーのシステム，（13 ページ）
- 250 ユーザーのシステム，（16 ページ）
- 800 ユーザーのシステム，（20 ページ）
- 2000 ユーザーのシステム，（23 ページ）

システムのサイズを決定する際に考慮すべきこと:

- 稀な、通常通りでない状況も含め、ある時点でミーティングに参加すると予想されるユーザーの最大数を決定してください。
- ハードウェアが大きなサイズシステムの最小要件を満たすか、超えるハードウェアである限り、システムサイズをいつでも大きなサイズに拡張できます。それ以外の場合は、追加ハードウェアを購入しなければなりません。
- 高可用性 (HA) またはマルチデータセンター (MDC) をシステムに追加する予定がある場合、ハードウェアを購入する際に、HA または MDC システムに対応する追加の仮想マシンを含めるようにしてください。
-

vCenter 共存の要件

VMware vCenter サーバーまたは vCenter Server アプライアンスは、例によっては他の仮想マシンまたは Cisco WebEx Meetings Server （CWMS）仮想マシンで使用と共存きます。

50 または 250 ユーザーシステムで、VMware vCenter は同じホスト上で CWMS と共存できます。しかし、追加 RAM を注文するか Cisco UCS サーバーにインストールしている必要があります。必要な RAM の正確な大きさについては、『ハードウェアの最低必要要件』 のシステムサイズの要件を参照してください。

システムの仮想マシン

これらは、システムのために作成された仮想マシンです。 より小さなシステムサイズでは、いくつかの機能が 1 台の仮想マシンに組み込まれています。

- 管理—システムの「中心的ノード」。 システムデータベースを含め、管理機能を提供する。
- メディア—メディアサービス（オーディオビデオ機能、電話およびミーティングサービス）を提供する。

  50 同時ユーザシステムでは管理用仮想マシンに含まれている。

- ウェブ — ウェブサービス（ミーティングリストや録画）を提供する。 ユーザが今後のミーティングをスケジュールできます。

  管理仮想マシンは、50、250 または800 同時ユーザシステムに含める。

  エンドユーザは WebEx ウェブサイトにサインインします。 管理者は、管理ウェブサイトにサインインします。

- インターネットリバースプロキシ（IRP）—パブリックアクセスを提供し、ユーザがインターネットやモバイルデバイスからミーティングをホストまたは参加できるようにする。 モバイルワーカーがミーティングに参加するには、インターネットリバースプロキシが必要です。

（注） この製品で提供されているインターネットリバースプロキシは、このシステムでしか使用できません。 他のベンダーによって提供されたインターネットリバースプロキシまたはウェブロードバランサは、サポートされていません。この製品で提供されているインターネットのリバースプロキシは、インターネットからミーティングに参加する外部ユーザーからのリアルタイムのウェブ、オーディオ、およびデータ共有トラフィックを取り扱うように最適化されています。

（注） 本書では、管理用仮想マシン（および該当する場合はメディア、ウェブ仮想マシン）に「内部仮想マシン」という用語を使用しています。

インターネットリバースプロキシは、DMZ ネットワーク（非スピリットホライズンおよびスプリットホライズンネットワーク）または内部ネットワーク（すべての内部ネットワーク）に設置できます。

- 非スプリットホライズンネットワークトポロジ, （51 ページ）
- スプリットホライズンネットワークトポロジ, （54 ページ）
- 内部インターネットリバースプロキシ (IRP) のネットワークトポロジ, （50 ページ）

ハードウェアの最低必要要件

このセクションでは、各サイズのシステムに使用できる Cisco UCS サーバーの一部を記載しています。 各システムに対する固有の要件については、以下を参照してください。

- 50 ユーザーのシステム
- 250 ユーザーのシステム
- 800 ユーザーのシステム
- 2000 ユーザーのシステム

『Cisco WebEx Meetings Server Ordering Guide』も参照してください (http://www.cisco.com/c/en/us/products/conferencing/webex-meetings-server/sales-resources-listing.html)。

表 *1*：*ESXi* バージョンとライセンスタイプ

システムサイズ	ESXi バージョン	vSphere ライセンスタイプ
50 または 250	5.0、5.0 アップデート 1、5.1、6.0	Standard Edition、Enterprise Edition、Enterprise Plus Edition
800 または 2000	5.0 または 5.0 アップデート 1	Enterprise Plus Edition のみ
	5.1 から 5.5[3]	Enterprise Edition、Enterprise Plus Edition
	5.5 以降[1]	Standard Edition、Enterprise Edition、Enterprise Plus Edition
	6.0	Standard Edition、Enterprise Edition、Enterprise Plus Edition

3 「以降」とは、フルバージョンではなく、アップデートを意味します。 たとえば、5.5 アップデート 1 または 5.1 アップデート 2 です。

表 *2*：ホストモデル

展開サイズ	UCS モデルの例
50 ユーザ	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
250 ユーザ	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
800 ユーザ	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3 （2.0 以降）

展開サイズ	UCS モデルの例
2000 ユーザ	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3 （2.0 以降）

vCenter との共存は、50 および 250 ユーザーシステム展開のみでサポートされています。 同じ物理ホスト上での Cisco Unified Communications 製品との共存はサポートされていません。

システムでUCSハードウェアの古いモデルを使用することができますが、より良いユーザーエクスペリエンスのためには、表にリストされているハードウェアをお使いください。 たとえば、UCS C220 M3 をすでにお持ちの場合は、250 ユーザーシステムにそのハードウェアを使用することができます。

Cisco WebEx Meetings Server Release 2.0 にアップグレードするときは、アップグレードされたシステムが SAN ストレージを仮想マシンに使用する限り、2x ローカルハードドライブを備えた Cisco UCS B200 M3 ブレードサーバーを使用することは可能です。 B シリーズのブレードサーバーを備えた SAN ストレージを使用することで、システムは Cisco WebEx Meetings Server に対する RAID 5 または RAID 10 構成要件の 4 つのハードディスクドライブに適合します。

（注） 2.0 以降を使用する800 ユーザー、および 2000 ユーザーのシステムの場合、DMZ ホスト上に追加の仮想マシンを展開しないことを推奨します。 これにより、メディア接続でパケットの紛失が増加し、遅延が顕著になる可能性があります。

CWMS および ESXi ホストが消費するリソース

Cisco WebEx Meetings Server は ESXi ホストにある 1 台以上の仮想マシンで展開されます。 CPU とメモリリソース、およびストレージスペースは、Cisco WebEx Meetings Server（CWMS）と ESXi（物理 Cisco UCS サーバーでの仮想化を可能にする Vmware コンポーネント）によって消費されます。 システムサイズによって、vCenter と複数の仮想マシンを同じ Cisco UCS サーバーで実行できる場合があります。

CWMS はリソース予約 をその仮想マシンに用いてシステムスケーラビリティを保証します。 他の Vmware のワークロードは、CPU と他のリソースを仮想マシンから取り去りません。 各システムサイズの最小要件には、以下のものをサポートするために十分なリソースが含まれます。

- CWMS 用サービスの質をピークシステム使用（最大容量）で継続。
- VMware ESXi。
- VMware vCenter（共存の場合）。

vCenter Server の要件については、ナレッジベースを参照して、「vCenter Server 5.0 のインストールのベストプラクティス」、「vCenter Server 5.1 のインストールのベストプラクティス」、または「Installing vCenter Server 5.5 best practices」をそれぞれ検索してください。

- 仮想マシンの Vmware スナップショット（これらは可能な限りすぐに削除してください。そうしない場合、重度のパフォーマンス劣化を経験する可能性があります）。

  一部のスナップショットは元の仮想マシンと同じ大きさになる場合があるので、スナップショットのための余分なディスクスペースが必要です。 場合によっては、vSphere はスナップショットを削除してストレージスペースを作成し、前のスナップショットにロールバックする能力に支障をきたすことがあります。

- サーバの通常のライフサイクルを通した Cisco UCS サーバの使用

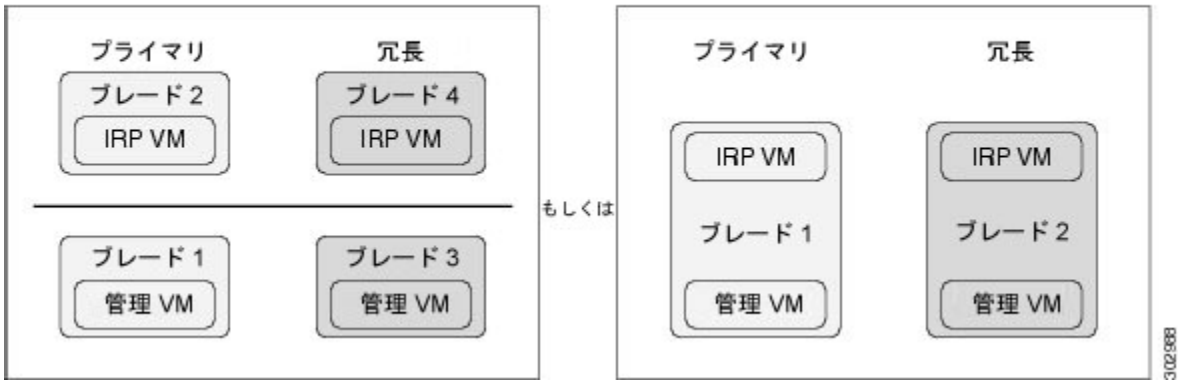
OVA ファイルで指定されているハードウェア要件は、Cisco WebEx Meetings Server を展開するために必要な最小要件です。 これらの要件には、VMware vCenter または ESXi の CPU、メモリ、またはストレージの要件は含まれていません。

注意 この文書の表にリストされている構成以外での共存はサポートされていません。 当社のシステム要件を無視すると、仮想マシンが起動しない場合があります。 仮想マシンの展開は、vCenter OVA 展開中で最も早期の画面内で止まる可能性があります。

50 ユーザーのシステム

50 ユーザーのシステムはマイクロシステムとも呼ばれます。 (マルチデータセンター (MDC) はマイクロシステムでは利用できません。) 図は2種類の 50 ユーザー展開を示しています。 (冗長な仮想マシンは高可用性 (HA) のサポートを実証します。)

仮想マシンレイアウト
50 同時ユーザー導入



テーブルでは、システムでの ESXi ホスト（Cisco UCS サーバー）の最小ハードウェア要件がリストされます。 最後の 2 列には Cisco WebEx Meetings Server を新規にインストールするのに必要な空き容量、および既存の Cisco UCS サーバーを使用して Cisco WebEx Meetings Server リリース

1.5MR3 をリリース 2.x へアップグレードするのに自動アップグレードを使用する時に必要な空き容量が表示されています。 詳細ついては、一般的なシステム要件をご覧ください。

帯域幅の要件に関する情報については、ネットワーク帯域要件, （60 ページ）を参照してください。

（注） IOPS 情報については、VMware vSphere に現行システムに展開するメリット, （41 ページ） を参照してください。

vCenter との共存は、以下のテーブルで構成されている通りの 50 ユーザーのシステムでサポートされています。

ESX i ホスト（Cisco UCS サーバ）の仮想マシン	CPU コア	メモリー (GB)	イーサネットポート	新規インストールに関するハードドライブストレージ要件	1.5MR3 から 2.X へ自動アップグレードするのに必要なハードドライブストレージは無料です[4]
管理者	4（ESXi 5.0） 6 (ESXi 5.1 以降)	24	管理用仮想マシンのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む ESXi 管理ネットワーク用に 1 つ推奨	1.5 TB、最低 7,200 RPM	自動インストールの場合、1118 GB。
管理者および vCenter（共存)	6（ESXi 5.0） 8 (ESXi 5.1 以降)	36	管理用仮想マシンのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む vCenter 用に 1 つ ESXi 管理ネットワーク用に 1 つ推奨	1.5 TB、最低 7,200 RPM	1078 GB この数字は vCenter を 40 GB でセットアップしたという前提に基づいています。
インターネットリバースプロキシ (IRP)	4（ESXi 5.0） 6 (ESXi 5.1 以降)	12	IRP 仮想マシンのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む ESXi 管理ネットワーク用に 1 つ推奨	300 GB、最低 7,200 RPM	172 GB

ESX i ホスト（Cisco UCS サーバ）の仮想マシン	CPU コア	メモリー (GB)	イーサネットポート	新規インストールに関するハードドライブストレージ要件	1.5MR3 から 2.X へ自動アップグレードするのに必要なハードドライブストレージは無料です[4]
管理者および IRP（共存）	8	36	管理用仮想マシンのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む IRP 仮想マシンのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む ESXi 管理ネットワーク用に 1 つ推奨	1.5 TB、最低 7,200 RPM	990 GB
管理者および IRP および vCenter（すべて共存）	12	40	管理用仮想マシンのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む IRP 仮想マシンのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む vCenter 用に 1 つ ESXi 管理ネットワーク用に 1 つ推奨	1.5 TB、最低 7,200 RPM	950 GB この数字は vCenter を 40 GB でセットアップしたという前提に基づいています。

4 すべての仮想マシンを手動で展開しする手動アップグレードを選択し、同じハードウェアを使用する場合、自動アップグレードに必要な空きスペースの 2 倍の空きスペースが必要です。

（注） 高可用性 (HA) システムを使用する場合、両方のシステムをサポートするように、プライマリシステムのハードウェア要件と量を 2 倍にしてください。

50 ユーザーシステムの仮想マシンによって予約されたリソース

このセクションでは、仮想マシンがどれほどのメディアを使用し、どれほどの VMware の専門知識を必要としているかを説明します。 CPU リソースは vCPU（コア）と MHz（CPU サイクル）として指定されています。 VMware Vmkernel は MHz サイクルを使用して、CPU スケジューリングを制御します。

メモリリソースは最大メモリと予約メモリによって指定されています。 予約メモリは、同じ物理 Cisco UCS サーバにある他の仮想マシンとは共有されません。

ディスクリソース（ストレージ）は 2 つの別々の領域で制御されます。 OVA ビルドの間に、CentOS ファイルシステムのパーティションサイズによって最小ディスクサイズが決定されます。次に、vCenter によって使用可能な最大ディスクスペースが制御されます。

最小 vCPU 数を持たない仮想マシンの展開を試行すると、仮想マシンの OVA 展開は失敗します。最小合計 MHz プロセッサ速度を持たない仮想マシンの展開を試行すると、仮想マシンの電源が入りません。

重要 このテーブルにある数値には、VMware ESXi または vCenter のリソースが含まれていません。CWMS および ESXi ホストが消費するリソース, （12 ページ）を参照してください。

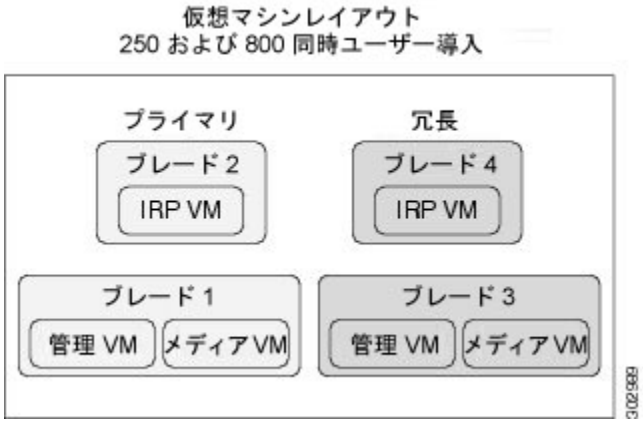
仮想マシンタイプ	仮想 CPU（vCPU）	CPU[5]（MHz）	予約メモリ/合計メモリ[6](GB)	ディスク（GB）
管理者	4	8000	12..14	418
インターネットリバースプロキシ	4	8000	4..4	128

5 物理 CPU の数に CPU チップの速度（MHz）をかけることで取得する数。 ハイパースレッディングはこの計算に含まれていません。 （物理 CPU は 2.4 GHz 以上のクロック速度を持つ必要があります。）

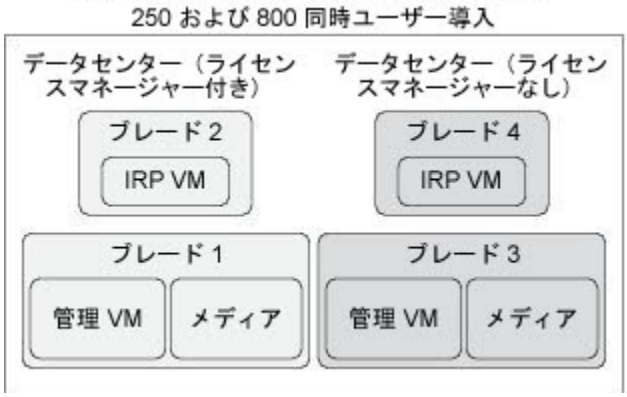
6 メディア機能のある仮想マシンには、追加の非予約メモリがあります。メモリ=予約/合計

250 ユーザーのシステム

250 ユーザーのシステムは小システムとも呼ばれます。 この図は2種類の 250 ユーザー展開を示しています。 冗長な仮想マシンは高可用性 (HA) のサポートを実証します。 システムが HA をサポートしない場合、**プライマリ**だけを展開します。



この図は、Internet Reverse Proxy (IRP) に対応するマルチデータセンター (MDC) システムを形成する 2 つのデータセンターを含む 250 ユーザーのシステムのレイアウトを示します。 License Manager は 1 つのデータセンター上だけで動作します。



テーブルでは、システムでの ESXi ホスト（Cisco UCS サーバー）の最小ハードウェア要件がリストされます。 最後の 2 列には Cisco WebEx Meetings Server を新規にインストールするのに必要な空き容量、および既存の Cisco UCS サーバーを使用して Cisco WebEx Meetings Server リリース 1.5MR3 をリリース 2.x へアップグレードするのに自動アップグレードを使用する時に必要な空き容量が表示されています。 詳細ついては、一般的なシステム要件をご覧ください。

帯域幅の要件に関する情報については、ネットワーク帯域要件, （60 ページ）を参照してください。

IOPS 情報については、VMware vSphere に現行システムに展開するメリット, （41 ページ） を参照してください。

vCenter との共存は、以下のテーブルで構成されている通りの 250 ユーザのシステムでサポートされています。

ESX i ホスト（Cisco UCS サーバ）の仮想マシン	CPU コア	メモリー (GB)	イーサネットポート	新規インストールに関するハードドライブストレージ要件	1.5MR3 から 2.X へ自動アップグレードするのに必要なハードドライブストレージは無料です[7]
管理者およびメディア	12	52	• 管理とメディアのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	1.5 TB、最低 7200 RPM	990 GB
（管理者およびメディア）および vCenter（共存）	16	56	• 管理とメディアのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨 • vCenter 用に 1 つ	1.5 TB、最低 7200 RPM	950 GB （この数字は vCenter を 40 GB でセットアップしたという前提に基づいています。）
インターネットリバースプロキシ (IRP)	12	36	• IRP のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	300 GB、最低 7200 RPM	172 GB

[7] すべての仮想マシンを手動で展開しする手動アップグレードを選択し、同じハードウェアを使用する場合、自動アップグレードに必要な空きスペースの 2 倍の空きスペースが必要です。

（注） HA システムを使用する場合、プライマリシステムの場合と同様に、HA システムのハードウェアと数量を購入します。

250 ユーザーシステムの仮想マシンによって予約されたリソース

このセクションでは、仮想マシンがどれほどのメディアを使用し、どれほどの VMware の専門知識を必要としているかを説明します。 CPU リソースは vCPU（コア）と MHz（CPU サイクル）として指定されています。 VMware Vmkernel は MHz サイクルを使用して、CPU スケジューリングを制御します。

メモリリソースは最大メモリと予約メモリによって指定されています。 予約メモリは、同じ物理 Cisco UCS サーバにある他の仮想マシンとは共有されません。

ディスクリソース（ストレージ）は 2 つの別々の領域で制御されます。 OVA ビルドの間に、CentOS ファイルシステムのパーティションサイズによって最小ディスクサイズが決定されます。次に、vCenter によって使用可能な最大ディスクスペースが制御されます。

最小 vCPU 数を持たない仮想マシンの展開を試行すると、仮想マシンの OVA 展開は失敗します。最小合計 MHz プロセッサ速度を持たない仮想マシンの展開を試行すると、仮想マシンの電源が入りません。

重要 このテーブルにある数値には、VMware ESXi または vCenter のリソースが含まれていません。CWMS および ESXi ホストが消費するリソースをご覧ください。

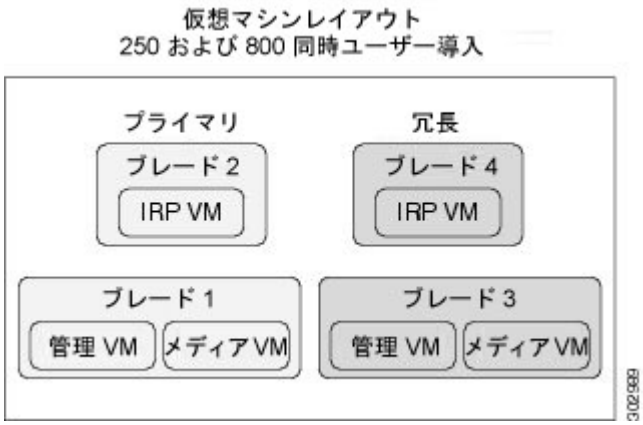
仮想マシンタイプ	仮想 CPU（vCPU）	CPU[8]（MHz）	予約メモリ/合計メモリ[9](GB)	ディスク（GB）
管理者	4	8000	16..16	418
メディア	8	16,480	13..23	128
インターネットリバースプロキシ	8	16,480	6..6	128

[8] 物理 CPU の数に CPU チップの速度（MHz）をかけることで取得する数。 ハイパースレッディングはこの計算に含まれていません。（物理 CPU は 2.4 GHz 以上のクロック速度を持つ必要があります。）

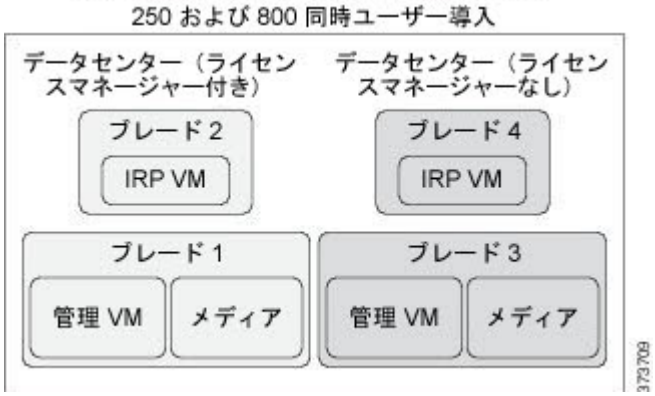
[9] メディア機能のある仮想マシンには、追加の非予約メモリがあります。メモリ=予約/合計

800 ユーザーのシステム

800 ユーザーのシステムは中システムとも呼ばれます。 この図は2種類の 800 ユーザー展開を示しています。 冗長な仮想マシンは高可用性 (HA) のサポートを実証します。



この図は、Internet Reverse Proxy (IRP) に対応するマルチデータセンター (MDC) システムを形成する 2 つのデータセンターを含む 800 ユーザーのシステムのレイアウトを示します。 License Manager は 1 つのデータセンター上だけで動作します。



テーブルでは、システムでの ESXi ホスト（Cisco UCS サーバー）の最小ハードウェア要件がリストされます。 最後の 2 列には Cisco WebEx Meetings Server を新規にインストールするのに必要な空き容量、および既存の Cisco UCS サーバーを使用して Cisco WebEx Meetings Server リリース 1.5MR3 をリリース 2.x へアップグレードするのに自動アップグレードを使用する時に必要な空き容量が表示されています。 詳細ついては、一般的なシステム要件をご覧ください。

帯域幅の要件に関する情報については、ネットワーク帯域要件, （60 ページ）を参照してください。

（注） 800 ユーザーシステムの展開では vCenter との共存はサポートされていません。

IOPS 情報については、VMware vSphere に現行システムに展開するメリット，（41 ページ） を参照してください。

ESX i ホスト（Cisco UCS サーバ）の仮想マシン	CPU コア	メモリー (GB)	イーサネットポート	新規インストールに関するハードドライブストレージ要件	1.5MR3 から 2.X へ自動アップグレードするのに必要なハードドライブストレージは無料です[10]
管理およびメディア（組み合わせ）	40	80	• 管理とメディアのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	1.5 TB、最低 10,000 RPM	990 GB
インターネットリバースプロキシ (IRP)	40	36	• IRP のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	300 GB、最低 10,000 RPM	172 GB

10 すべての仮想マシンを手動で展開しする手動アップグレードを選択し、同じハードウェアを使用する場合、自動アップグレードに必要な空きスペースの 2 倍の空きスペースが必要です。

（注） HA システムの使用を予定している場合は、プライマリシステムとして同一のシステム要件で同じ数量を購入してください。

800 ユーザーのシステムの場合、DMZ ホスト上に追加の仮想マシンを展開しないことを推奨します。 これにより、メディア接続でパケットの紛失が増加し、遅延が顕著になる可能性があります。

800 ユーザーシステムの仮想マシンによって予約されたリソース

このセクションでは、仮想マシンがどれほどのメディアを使用し、どれほどの VMware の専門知識を必要としているかを説明します。 CPU リソースは vCPU（コア）と MHz（CPU サイクル）として指定されています。 VMware Vmkernel は MHz サイクルを使用して、CPU スケジューリングを制御します。

メモリリソースは最大メモリと予約メモリによって指定されています。 予約メモリは、同じ物理 Cisco UCS サーバにある他の仮想マシンとは共有されません。

ディスクリソース（ストレージ）は 2 つの別々の領域で制御されます。 OVA ビルドの間に、CentOS ファイルシステムのパーティションサイズによって最小ディスクサイズが決定されます。次に、vCenter によって使用可能な最大ディスクスペースが制御されます。

最小 vCPU 数を持たない仮想マシンの展開を試行すると、仮想マシンの OVA 展開は失敗します。最小合計 MHz プロセッサ速度を持たない仮想マシンの展開を試行すると、仮想マシンの電源が入りません。

重要 このテーブルにある数値には、VMware ESXi のリソースが含まれていません。 CWMS および ESXi ホストが消費するリソース，（12 ページ）を参照してください。

仮想マシンタイプ	仮想 CPU（vCPU）	CPU[11]（MHz）	予約メモリ/合計メモリ[12](GB)	ディスク（GB）
管理者	10	20,600	16..16	418
メディア	30	60,800	14..44	128
インターネットリバースプロキシ	20	41,200	10/10/2013 12:00:00 AM	128

11 物理 CPU の数に CPU チップの速度（MHz）をかけることで取得する数。 ハイパースレッディングはこの計算に含まれていません。（物理 CPU は 2.4 GHz 以上のクロック速度を持つ必要があります。）

12 メディア機能のある仮想マシンには、追加の非予約メモリがあります。メモリ=予約/合計

2000 ユーザーのシステム

2000 ユーザーのシステムは大システムとも呼ばれます。 この図は高可用性 (HA) と Internet Reverse Proxy (IRP) に対応した 2000 ユーザーシステムを示しています。 HA 仮想マシンは**冗長**な仮想マシンとして表示されます。 システムが HA をサポートしない場合、**プライマリ**だけを展開します。

この図は、Internet Reverse Proxy (IRP) に対応するマルチデータセンター (MDC) システムを形成する 2 つのデータセンターを含む 2000 ユーザーのシステムの展開を示します。 License Manager は 1 つのデータセンター上だけで動作します。

重要 図で示されているすべての仮想マシンを展開することを推奨します。 物理サーバーに種類の異なる仮想マシンを展開すると、ハードウェアの不具合が発生した場合にシステムがシャットダウンする可能性を減らすことができます。 （例えば、メディア仮想マシンとウェブ仮想マシンを 1 つの物理サーバーに配備すると、2 つのウェブ仮想マシンを同じ物理サーバーに配備した場合より回復力があります。）

大規模なシステムでは、均等ロードバランスポイント規則 (詳細については ロードバランシング, （66 ページ）を参照) からの排除があり、メディア 1 とメディア 2 に SIP トランクロードバランサーがあり、メディア 3 とメディア HA (オプション) にロードバランサーがありません。 プライマリシステムのメディア 1 と 2 の両方に障害がある場合、CWMS の電話サービスはすべて停止します。 システムが HA 展開である場合、冗長性により単一仮想マシンの障害が緩和されます。

テーブルでは、システムでの ESXi ホスト（Cisco UCS サーバー）の最小ハードウェア要件がリストされます。 最後の 2 列には Cisco WebEx Meetings Server を新規にインストールするのに必要な空き容量、および既存の Cisco UCS サーバーを使用して Cisco WebEx Meetings Server リリース 1.5MR3 をリリース 2.x へアップグレードするのに自動アップグレードを使用する時に必要な空き容量が表示されています。 詳細ついては、一般的なシステム要件をご覧ください。

帯域幅の要件に関する情報については、ネットワーク帯域要件, （60 ページ）を参照してください。

HA システムを追加する場合、これらの仮想マシンは、「冗長」仮想マシンとして表示されます。 HA が必要ない場合は、プライマリシステムのみを展開します。

（注） 2,000 ユーザーシステムの展開では vCenter との共存はサポートされていません。

（注） IOPS 情報については、VMware vSphere に現行システムに展開するメリット, （41 ページ） を参照してください。

ESX i ホスト（Cisco UCS サーバ）の仮想マシン	CPU コア	メモリー (GB)	イーサネットポート	新規インストールに関するハードドライブストレージ要件	1.5MR3 から 2.X へ自動アップグレードするのに必要なハードドライブストレージは無料です[13]
メディア1 および管理（組み合わせ）	40	80	• メディア 1 と管理のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	1.5 TB、最低 10,000 RPM	990 GB
メディア2 およびウェブ1（組み合わせ）	40	80	• メディア 2 とウェブ 1 のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	1 TB、最低 10,000 RPM	768 GB
メディア3 およびウェブ2（組み合わせ）	40	80	• メディア 3 とウェブ 2 のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	1 TB、最低 10,000 RPM	768 GB

ESX i ホスト（Cisco UCS サーバ）の仮想マシン	CPU コア	メモリー (GB)	イーサネットポート	新規インストールに関するハードドライブストレージ要件	1.5MR3 から 2.X へ自動アップグレードするのに必要なハードドライブストレージは無料です[13]
インターネットリバースプロキシ (IRP)	40	36	• IRP のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi管理ネットワーク用に 1 つ推奨	300 GB、最低 10,000 RPM	172 GB
HA用にメディアおよび管理（組み合わせ）	40	80	• メディアと管理のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi管理ネットワーク用に 1 つ推奨	1.5 TB、最低 10,000 RPM	990 GB
HA 用ウェブ	40	80	• ウェブのために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi管理ネットワーク用に 1 つ推奨	1 TB、最低 10,000 RPM	896 GB

ESX i ホスト（Cisco UCS サーバ）の仮想マシン	CPU コア	メモリー (GB)	イーサネットポート	新規インストールに関するハードドライブストレージ要件	1.5MR3 から 2.X へ自動アップグレードするのに必要なハードドライブストレージは無料です[13]
HA 用 IRP	40	36	• IRP のために 2 台で、NIC チーミングが冗長性のために使用される場合の 1 台を含む • ESXi 管理ネットワーク用に 1 つ推奨	300 GB、最低 10,000 RPM	172 GB

13 すべての仮想マシンを手動で展開しする手動アップグレードを選択し、同じハードウェアを使用する場合、自動アップグレードに必要な空きスペースの 2 倍の空きスペースが必要です。

（注） 2000 ユーザーのシステムの場合、DMZ ホスト上に追加の仮想マシンを展開しないことを推奨します。 これにより、メディア接続でパケットの紛失が増加し、遅延が顕著になる可能性があります。

2000 ユーザーシステムの仮想マシンによって予約されたリソース

このセクションでは、仮想マシンがどれほどのメディアを使用し、どれほどの VMware の専門知識を必要としているかを説明します。 CPU リソースは vCPU（コア）と MHz（CPU サイクル）として指定されています。 VMware Vmkernel は MHz サイクルを使用して、CPU スケジューリングを制御します。

メモリリソースは最大メモリと予約メモリによって指定されています。 予約メモリは、同じ物理 Cisco UCS サーバにある他の仮想マシンとは共有されません。

ディスクリソース（ストレージ）は 2 つの別々の領域で制御されます。 OVA ビルドの間に、CentOS ファイルシステムのパーティションサイズによって最小ディスクサイズが決定されます。次に、vCenter によって使用可能な最大ディスクスペースが制御されます。

最小 vCPU 数を持たない仮想マシンの展開を試行すると、仮想マシンの OVA 展開は失敗します。最小合計 MHz プロセッサ速度を持たない仮想マシンの展開を試行すると、仮想マシンの電源が入りません。

重要　このテーブルにある数値には、VMware ESXi のリソースが含まれていません。 CWMS および ESXi ホストが消費するリソースをご覧ください。

仮想マシンタイプ	仮想 CPU（vCPU）	CPU[14]（MHz）	予約メモリ/合計メモリ[15](GB)	ディスク（GB）
管理者	10	20,600	16..16	418 バージョン 2.6 以降では、OVA ファイルを用いて展開された新しいシステムは 513 である必要があります。
メディア	30	60,800	14..44	128
ウェブ	10	20,600	16..16	128
インターネットリバースプロキシ	20	41,200	10/10/2013 12:00:00 AM	128

14 物理 CPU の数に CPU チップの速度（MHz）をかけることで取得する数。 ハイパースレッディングはこの計算に含まれていません。 （物理 CPU は 2.4 GHz 以上のクロック速度を持つ必要があります。）
15 メディア機能のある仮想マシンには、追加の非予約メモリがあります。メモリ=予約/合計

システム容量マトリックス

重要なポイント:

- このセクションに示された情報は、ミーティングに少なくとも 2 人参加していることが基本的な前提条件の 1 つです。
- 同時のミーティング接続は、指定した時点でミーティングに参加している人数として定義されます。 たとえば、50 ユーザーシステムでは、最大の同時ミーティング接続はミーティングに合計 10 人（たとえば、1 人の主催者と 9 人の参加者）をそれぞれもつ 5 つの同時のミーティングから構成されることができます。
- 任意の時点で、ミーティング参加者の最大人数に達すると、他のユーザーはミーティングを開始したり、参加することができません。 ミーティング参加者の最大数のうち（2000、800、250、または 50 人）、半分の参加者しかビデオを使用できません。 ビデオは送受信として定

義され、ユーザーがビデオを共有するために、WebEx ウェブカムビデオまたはビデオファイル共有オプションを使用していることを意味します。

- デスクトップ共有はビデオとは見なされません。 このことは、250 ユーザーシステムでは、250 人が指定された時点でミーティング中にデスクトップを共有できることを意味します。
- 高可用性またはマルチデータセンターを追加しても、ミーティングを開催するためのシステムの容量は増加しません。800 ユーザーシステムは800 ユーザーシステムのままです。

下表の値は、Cisco WebEx Meetings Server システムの設計容量を示しています。 これらの仕様より大きい容量で稼働するシステムは、ユーザ満足度が低下し、システムが不安定になることがあります。 Cisco はこのようなレベルで容量限界を強制する権利があります。

（注） システムがシングルデータセンターから構成されるか、またはマルチデータセンターシステムであるかに関係なく、下の表にあるこれらの値は変わりません。

表 *3*：バージョン *2.5* 以降のシステム容量一覧

システム容量	2000 ユーザのシステム	800 ユーザのシステム	250 ユーザのシステム	50 ユーザのシステム	メモ
同時ミーティング接続の最大数（音声、ビデオ、およびウェブユーザー）	2000	800	250	50	指定された時間に同時に行われたミーティングに参加した人数。
最大同時音声接続（ミーティングクライアントからコンピュータを使用した電話会議の着信および音声接続）	2000	800	250	50	以下の機能がどの組み合わせで使用されているかに関係なく、システム容量は左記に示されているものと同じです。 • G.711、G.722、G.729 音声コーデック • IPv4 または IPv6 電話会議 • TLS/SRTP 音声暗号化

システム容量	2000 ユーザのシステム	800 ユーザのシステム	250 ユーザのシステム	50 ユーザのシステム	メモ
最大同時ビデオおよびビデオ共有ユーザ数	1000[16]	400	125	25	これらの数字は同時にビデオを共有するために使用できるミーティングの同時接続（または参加者）の最大数を示します。 同時ミーティングでビデオを共有するユーザーの数がこの制限に達すると、同時ミーティングに招待される残りのユーザーはミーティングに参加できるが、ビデオウィンドウはグレイアウトされます。 （注） 1 人のミーティング参加者がビデオを使用する場合、同一のミーティングにいる、他すべてのユーザーは、ビデオを使用していない場合でも、ビデオユーザーとして集計されます。 （注） デスクトップ共有はビデオとは見なされません。
1 つのミーティングでの最大参加者数	500	500	250	50	これらの数字はミーティングに参加することができる参加者の最大数を示します。
同時録画可能な最大ミーティング数	100	40	13	3	これは、同時に録画機能を使用できるミーティングの合計数です。
最大同時録画再生数	500	200	63	12	同時に行われる録画再生セッションの合計数です。 これはストレージシステムに保存する録画を指し、ユーザーのデスクトップにダウンロードされる録画は含みません。 （注） これらの再生セッションは、システムで同時ミーティング接続に含まれません。
ユーザープロファイルの最大数	400,000	400,000	400,000	400,000	この値にはアクティブおよび非アクティブユーザが含まれています。
最大同時ミーティング数	1000	400	125	25	同時にアクティブにできる個別のミーティング数。

システム容量	2000 ユーザのシステム	800 ユーザのシステム	250 ユーザのシステム	50 ユーザのシステム	メモ
最大通話回数 （1秒間の通話回数）	20	8	3	1	1秒間にミーティングにダイヤルインするユーザーの平均数です。 この数に達した後で、ミーティングにダイヤルインする次の数人のユーザーは、ミーティングに接続されるまで数秒待たされることになります。
最大同時サインイン数	1 秒あたり 20 ユーザ	1 秒あたり 8 ユーザ	1 秒あたり 3 ユーザ	1 秒あたり 1 ユーザ	1 秒間に WebEx サイトに同時にサインインできるユーザーの平均数です。 この数に達した後で、WebEx サイトにサインインする次の数人のユーザーは、ミーティングに接続されるまでさらに数秒待たされることになります。
最大総帯域幅使用	5 Gbps	2 Gbps	625 Mbps	125 Mbps	最大帯域幅でテストシステムを使用して、テストシステムを扱うことができる最大帯域幅です。 帯域幅の利用に関する詳細は、「プランニングガイド」の「システムのネットワーキングトポロジー」の「ネットワーク帯域幅要件」セクションを参照してください。「WebEx ネットワーク帯域幅ホワイトペーパー」を参照することもできます。

16 連邦情報処理規格 (FIPS 環境) では 800

（注） Cisco WebEx Meetings Server Release 2.0 以降を新しくインストールする場合、ストレージの要件は以下の通りです。

- 空き容量は、ローカル（DAS）または外部（SAN/NAS）のいずれでもかまいません。
- 管理仮想マシンを持つ ESXi ホスト（Cisco UCS サーバー）には 1.5 TB の空き容量が必要です。
- 管理仮想マシンの無い ESXi ホスト（Cisco UCS サーバー）には 1 TB の空き容量が必要です。
- 既存の Cisco UCS サーバーを使用して Cisco WebEx Meetings Server にアップグレードする際、UCS サーバーに管理仮想マシン（プライマリまたは HA システム）しかない場合は、ESXi ホストには 1118 GB の空きディスク容量が必要です。UCS サーバーに 1 つの管理仮想マシン（プライマリまたは HA システム）と 1 つのメディア仮想マシン（プライマリまたは HA システム）がある場合は、ESXi ホストには 990 GB の空きディスク容量が必要です。

詳細な情報については、**の「Cisco WebEx Meetings Server と** ESXi ホストによってhttp://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html消費されるリソース」のセクションをご覧ください。

ヒント すべてのサイズのユーザーシステム展開において、ミーティングの最長時間は 24 時間です。

（注） アップグレードを考えるとき、データストアのサイズの増大を見込んでください。元のシステムとアップグレードされたシステムは、アップグレードされたシステムのテストが完了し、元のシステムが削除されるまで、データストアを共有することになるからです。

さまざまなユーザーシステムサイズにおけるネットワーク帯域幅の要件の詳細については、本ガイドの「システムのネットワークトポロジ」の「ネットワーク帯域幅の要件」を参照してください。

サポートされているアップグレードパス

Cisco WebEx Meetings Server のこのリリースは、リリース 1.x から 2.8 へのアップグレードをサポートします。 次のポイントが適用されます。

- アップグレードは、システムに作成した主な変更を展開するためのシステムの置換として定義されます。
- アップデートとは、システムを段階的に改善することと定義されます。 アップデートでは、修正と小さい改善を展開します。

- アップデートでは、オリジナルシステムのすべてのデータが保持されます。アップグレードでは、ログを除く、オリジナルシステムのすべてのデータが保持されます。
- アップグレード中、ソフトウェアのメジャーバージョンをスキップできません。また、コンパニオンメンテナンスリリースへ直接移動します。

  たとえば、1.5MR5 から 2.8MR へアップグレードするには、1.5MR5 から 2.8 へアップグレードしてから、2.8MR へアップデートします。

（注） すべてのアップデートでダウンタイムが必要となります。 マルチデータセンターでは、両方のデータセンターを同時にアップデートします。

注意 他方の更新が完了し、両方が再起動ボタンを表示するまで、一方のデータセンターに対する再起動をクリックしないでください。 リリース 2.5MR6以降から 2.8 へアップデートする場合、アップデートが完了する前に一方のデータセンターを再起動して、他方のレプリケーションを中断させてください。

次のテーブルを使用して、Cisco WebEx Meetings Server Release 2.8 へアップデートまたはアップグレードする方法を決定してください。

インストールされたリリース	次のリリースへ	パス
1.0 から 1.1	2.8	**1** 1.5 へのアップデート **2** □□□MR5 パッチ 2 以降にアップデート **3** 2.8 へのアップグレード
1.5 から 1.5MR4	2.8	**1** □□□MR5 パッチ 2 以降にアップデート **2** 2.8 へのアップグレード
1.5 MR5	2.8	**1** □□□MR5 パッチ 2 以降にアップデート **2** 2.8 へのアップグレード
1.5 MR5 パッチ 2 以降	2.8	2.8 へのアップグレード
2.0 から 2.0MR8	2.8	**1** 2.0MR9 へのアップデート **2** 2.8 へのアップデート

インストールされたリリース	次のリリースへ	パス
2.0MR9 以降	2.8	2.8 へのアップデート
2.5 から 2.5MR5	2.8	1 2.5MR6 へのアップデート 2 2.8 へのアップデート
2.5MR6。	2.8	2.8 へのアップデート
2.6 から 2.6MR2	2.8	1 2.6MR3 へのアップデート 2 2.8 へのアップデート
2.6MR3 以降	2.8	2.8 へのアップデート
2.7 または 2.7MR	2.8	2.8 へのアップデート
2.8 または 2.8MR	2.8MR	2.8MR へのアップデート

重要 アップグレード中またはアップデート中に、システムの音声暗号化タイプ (音声暗号化は -AE/音声非暗号化は -AU) を変更することはできません。 展開後に、システムの音声暗号化タイプを変更するための唯一の方法は、システムを新規に展開することです。

詳細については、以下の文書を参照してください。

- *Cisco WebEx Meetings Server* 管理ガイド リリース *2.8*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Cisco WebEx Meetings Server* プランニングガイドとシステム要件リリース *2.8*: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

サポートされているアップグレードパス

Cisco WebEx Meetings Server のこのリリースは、リリース 1.x から 3.0 へのアップグレードをサポートします。 次のポイントが適用されます。

- アップグレードは、システムに作成した主な変更を展開するためのシステムの置換として定義されます。

- アップデートとは、システムを段階的に改善することと定義されます。アップデートでは、修正と小さい改善を展開します。
- アップデートでは、オリジナルシステムのすべてのデータが保持されます。アップグレートでは、ログを除く、オリジナルシステムのすべてのデータが保持されます。
- アップグレード中、ソフトウェアのメジャーバージョンをスキップできません。また、コンパニオンメンテナンスリリースへ直接移動します。

  たとえば、1.5MR5 から 3.0MR へアップグレードするには、1.5MR5 から 3.0 へアップグレードしてから、3.0MR へアップデートします。

（注） すべてのアップデートでダウンタイムが必要となります。 マルチデータセンターでは、両方のデータセンターを同時にアップデートします。

注意 他方の更新が完了し、両方が再起動ボタンを表示するまで、一方のデータセンターに対する再起動をクリックしないでください。 リリース 2.5MR6以降から 3.0 へアップデートする場合、アップデートが完了する前に一方のデータセンターを再起動して、他方のレプリケーションを中断させてください。

次のテーブルを使用して、Cisco WebEx Meetings Server Release 3.0 へアップデートまたはアップグレードする方法を決定してください。

インストールされたリリース	次のリリースへ	パス
1.0 から 1.1	2.8	**1** 1.5 へのアップデート **2** □□□MR5 パッチ 2 以降にアップデート **3** 2.8 へのアップグレード
1.5 から 1.5MR4	2.8	**1** □□□MR5 パッチ 2 以降にアップデート **2** 2.8 へのアップグレード
1.5 MR5	2.8	**1** □□□MR5 パッチ 2 以降にアップデート **2** 2.8 へのアップグレード
1.5 MR5 パッチ 2 以降	2.8	2.8 へのアップグレード

インストールされたリリース	次のリリースへ	パス
2.0 から 2.0MR8	3.0	1 2.0MR9 へのアップデート 2 3.0 へのアップデート
2.0MR9 以降	3.0	3.0 へのアップデート
2.5 から 2.5MR5	3.0	1 2.5MR6 へのアップデート 2 3.0 へのアップデート
2.5MR6。	3.0	3.0 へのアップデート
2.6 または 2.6MR	3.0	3.0 へのアップデート
2.7 または 2.7MR	3.0MR	3.0MR へのアップデート

重要 アップグレード中またはアップデート中に、システムの音声暗号化タイプ (音声暗号化は -AE/音声非暗号化は -AU) を変更することはできません。 展開後に、システムの音声暗号化タイプを変更するための唯一の方法は、システムを新規に展開することです。

詳細については、以下の文書を参照してください。

- *Cisco WebEx Meetings Server* 管理ガイド リリース *3.0*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Cisco WebEx Meetings Server* プランニングガイドとシステム要件リリース *3.0*: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

第 2 章

Cisco WebEx Meetings Server の紹介

Cisco Webex Meetings Server は、少ない電話会議費用でオーディオ、ビデオ、インターネットを組み合わせ、Cisco ユニファイドコミュニケーションへの投資を拡大させる安全で完全に可視化されたプライベートクラウド（オンプレミス）電話会議ソリューションです。

他の Cisco WebEx 製品と同様に、ドキュメント、アプリケーション、デスクトップ共有、注釈ツール、効率の良いミーティング管理のための完全制御ツール、アクティブトーカー機能を装備した統合された参加者リスト、ビデオスイッチング、録画、再生など、さまざまなリアルタイムのコラボレーションツールを提供します。 本製品は、高品質ビデオを採用しているため、きれいで鮮明なビデオ共有が実現します。

この電話会議ソリューションをデータセンターのファイアウォールの背後でご自分のプライベートクラウドに展開して、管理することができます。 これは、Cisco UCS サーバおよび VMware vSphere 専用です。 (特定の要件については、ハードウェアの最低必要要件, （10 ページ）を参照してください。) 短期間で仮想マシンを展開し、システムの設定および管理に必要なパワフルなツールを管理者に提供し、主なシステムメトリックスを見ることができます。

さらに、モバイルユーザはミーティングに出席および参加できます。 サポートされる端末については、モバイルデバイスのオペレーティングシステム要件, （216 ページ）を参照してください。

システムに関する重要な考慮事項

以下について注意してください。

- フォワードプロキシ — 制限付きでフォワードプロキシを使用することもできますが、フォワードプロキシはお勧めしません。 詳細については、『*Cisco WebEx Meetings Server* トラブルシューティングガイド』を参照してください。
- リバースプロキシ — この製品に含まれているインターネットリバースプロキシのみがサポートされています。
- NAT — このシステムの要件を満たしている場合サポートします。 詳細については、「システムでの NAT の使用」を参照してください。

- シングルデータセンター—シングルデータセンターでの展開は、Cisco WebEx Meetings Server のすべてのリリースでサポートされています。 詳細については、「シングルデータセンターの展開」を参照してください。
- マルチデータセンター—Cisco WebEx Meetings Server Release 2.5 以降を実行するデータセンターを結合して、複数のデータセンターから構成されるシステムを作成できます。 詳細については、マルチデータセンターについて (Cisco WebEx Meetings Server 管理者ガイドに記載) を参照してください。
- ストレージサーバー—マルチデータセンターシステム中の各データセンターには異なるストレージサーバーがあります。 同じストレージサーバーは複数のデータセンターをサポートできません。
- 高可用性システム—同じバージョンの Cisco WebEx Meetings Server を実行する冗長仮想マシンを備えているシステムとして定義されます。 プライマリシステム (シングルデータセンターシステム中) が故障した場合でも、高可用性システムは運用を継続します。 冗長（高可用性）仮想マシンはプライマリ仮想マシンと同じデータセンター内に共存することが必要です。 プライマリおよび高可用性システムの仮想マシンは同一の VLAN またはサブネットにする必要があります。

  高可用性システムを結合してマルチデータセンター環境を作成することはできません。
- Internet Reverse Proxy (IRP) Server—CWMS に対するパブリックアクセスを提供するために外部インターネットと社内ネットワーク間のプロキシとして配置される仮想マシン。 ユーザーがモバイル端末によってミーティングをスケジュールまたは出席することを許可する場合、または、インターネットから WebEx サイトへの安全なアクセスを提供する場合、Internet Reverse Proxy サーバーが必要です。 内部ネットワークにのみCisco WebExミーティングサーバーへのアクセスを制限する場合、Internet Reverse Proxy サーバーは不要です。 管理用の仮想マシンの実装に使用したのと同じ OVA ファイルを使用して、IRP 仮想マシンを展開します。 IRP 仮想マシンは、パブリック仮想 IP アドレスと同じサブネット上にある必要があります。
- 仮想 IP (VIP) アドレス—データセンター内の管理、メディア、およびウェブ仮想マシンと通信するのに使用します。
- プライベート仮想 IP (VIP) アドレス—管理仮想マシンで構成され、管理サイト URL と関連付けられます。 プライベート VIP アドレスがスプリットホライズン DNS 展開、または Internet Reverse Proxy サーバーが無い展開の内部 DNS サーバーで構成されている場合、プライベート仮想 IP アドレスは WebEx サイト URL と関連付けることもできます。
- パブリック仮想 IP (VIP) アドレス—Internet Reverse Proxy 管理仮想マシンで構成され、管理サイト URL だけと関連付けられます。 ユーザーがインターネットから WebEx サイトにアクセスできるように、外部 DNS サーバー上の WebEx サイト URL はパブリック 仮想 IP アドレスを解決できる必要があります。 Internet Reverse Proxy サーバーが無い場合、パブリック仮想 IP アドレスはシステム上で構成されません。

注意 システムを展開する場合に当社の推奨事項や要件を無視した場合、Cisco からの支援は得られません。 Cisco は当社のガイダンスに従わなかった結果として遭遇した問題については、責任を負いません。

Cisco WebEx Meetings Server の新機能と機能変更

『Cisco WebEx Meetings Server 1.1 のリリースノート』の「Cisco WebEx Meetings Server 1.1 の新機能と機能変更」というタイトルのセクションをリリースノートで参照してください。

- Cisco Unified MeetingPlace のお客様向け情報，39 ページ
- シングルデータセンターの展開，39 ページ
- シングルデータセンターを結合してマルチデータセンター (MDC) システムを作成，40 ページ
- システムでの VMware vSphere の使用，40 ページ
- IOPS およびストレージシステムのパフォーマンス，43 ページ
- VMware vSphere ESXi のインストールとストレージの構成，45 ページ
- ミーティングへの参加，46 ページ

Cisco Unified MeetingPlace のお客様向け情報

アーキテクチャの違いのため、Cisco Unified MeetingPlace から Cisco WebEx Meetings Server への移行パス（既存のユーザアカウント、カスタマイズ、およびミーティング用）はありません。 これらは、2 つの別の製品です。

ユーザーに新しいシステムに切り替えることを奨励すると同時に、一定期間 Cisco Unified MeetingPlace と Cisco WebEx Meetings Server の両方をサポートし続けることにより、ユーザーの移行を容易にすることができます。

シングルデータセンターの展開

Cisco WebEx Meeting Server (CWMS) はシングルでセンター (SDC) システムとして、および、任意で高可用性 (HA) システムまマルチデータセンター (MDC) システムとして展開できます (HA または MDC 展開の冗長性，（56 ページ）を参照)。 SDC システム (including a システム with HA support) には、試用期間後、主催者ライセンスだけが必要です。 MDC システムには、最低でも 2 つの MDC 機能ライセンス,、主催者ライセンスが必要で、MDC 試用期間はありません。

シングルデータセンターを結合してマルチデータセンター (MDC) システムを作成

Cisco WebEx Meeting Server Release 2.5 を実行する 2 つのデータセンターを結合して、シングルマルチデータセンター (MDC) システムを形成します。 最大 2 つのデータセンターを結合できます。 マルチデータセンターと高可用性システムの違いは、高可用性システムは同じ位置にありバックアップシステムとして 機能するということです。 MDC システムで、データセンターはそれぞれ異なる場所に配置でき、両方のデータセンターがシステム処理を行います。 HA または MDC 展開の冗長性, （56 ページ）を参照してください。 MDC システム中の各 CWMS データセンターに対し、1 つのライセンスを購入する必要があります。 MDC ライセンスは MDC システムを展開しようとする前に購入する必要がありあす。 （1 つのデータセンターを備えたシステムには機能ライセンスが必要ありません。） 結合するデータセンターを準備する方法、結合プロセス、結合プロセス完了時に 1 つのデータセンターから他のデータセンターへデータを持ち越す方法の詳細については、『*Cisco WebEx* 管理者ガイド リリース 2.5』の「データセンターを結合してマルチデータセンター (MDC) システムを作成」の章を参照してください（http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html）。

システムでの VMware vSphere の使用

重要 この製品は、VMware vSphere 仮想化プラットフォーム上でのみインストールされます。 VMWare Tools for CWMS はシステム配備中に自動的にインストールされます。手動でアップグレードしてはいけません。 VMWare Tools についての詳細は、 docwiki.cisco.com/wiki/VMware_Tools を参照してください。

- Cisco WebEx Meetings Server は、システム要件を満たす、またはそれ以上の同等の Cisco UCS サーバでも機能するよう設計されています。 ただし、時間を節約するため、標準 Cisco UCS サーバーの使用を推奨します。 ハードウェアと VMware の詳細情報については、を参照してください。ハードウェアの最低必要要件, （10 ページ）
- Cisco WebEx Meetings Server に対するハイパーバイザプラットフォームとして使用するために、VMware vSphere 5.0、5.0 アップデート 1、5.0 アップデート 2、5.1、5.1 アップデート 1 または 6.0 を購入する必要があります。

  （注） 安全上の理由から、5.1 はバージョン 1900470 以降である必要があります。

  以下のいずれかを実施します。

  - Cisco の GPL（グローバル価格リスト）から直接 vSphere を購入してください。 Cisco は VMware 公認のパートナーおよびディストリビュータです。

◦ VMware との直接法人契約を通じて、vSphere を VMware から購入してください。

VMware vSphere に現行システムに展開するメリット

このセクションでは、VMware vSphere および vCenter がCisco WebEx の製品を使用する必要がある理由について説明し、いくつかの考慮事項を示します。

システムの展開

- この製品は、VMware vSphere 互換 OVA 仮想アプライアンスとしてパッケージされており、DVD でのソフトウェアパッケージのコレクションとしては提供されていません。 OVA を展開するには vCenter が必須であり、これがないと製品をインストールできません。
- 仮想アプライアンスとしてパッケージすることで、時には 1 時間未満と極めて迅速な展開が可能となっています。
- OVA 仮想アプライアンスによる迅速なインストールを推進するために、ほとんどのサイズのシステムで自動システム展開を選択できます。 単に vCenter の資格情報を提供するだけで、手動での介入なしで、当社がお客様のシステムのすべての仮想マシンに展開いたします。 この革新によって、お客様の労働コストと時間を最小化できます。

（注） OVA テンプレートは、それぞれの仮想マシンに 2 つの仮想 NIC を作成します。 しかし、管理仮想マシンのみが両方の仮想 NIC を使用します。 その他のすべての Cisco WebEx Meetings Server (CWMS) 仮想マシンでは、1 つの仮想 NIC のみが使用され、もう 1 つは切断されます。

- CWMS のユーザーは VMware ESXi または対応する VMware ESXi のインストール可能な Cisco ISO イメージを実行する必要があります。 これらのエディションには、CWMS に必要な Cisco UCS サーバーのサポートに必要なドライバが含まれています。 詳細は、http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_26617.pdf を参照してください。

システムエラーからの簡単なリカバリ

変更が期待通りでない場合、VMware Data Recovery を使用することで、迅速に、システムを再展開することなく、システムに影響する変更を元に戻せます。

vSphere の検討事項

以下の検討事項に注意してください。

- 仮想マシンを別の ESXi ホストに移動させることができます。 ただし、新しい ESXi ホストでの仮想マシンのレイアウトは維持する必要があります。 言い換えれば、ウェブ仮想マシンと共存しているメディア仮想マシンの移動を計画する場合、それを別個の ESXi ホスト（それが唯一の仮想マシンである場合）に移動させるか、既にウェブ仮想マシンがある ESXi ホストに移動させる必要があります。

（注） 宛先 ESXi ホストが ソース ESXi ホストと同じシステム要件か確認する必要があります。

以下の VMware 機能は CWMS ではサポートされていません。

- VMotion と Storage VMotion (仮想マシンを移動できますが、これらのツールを使用して移動できません。)
- VMware Distributed Resource Schedule (DRS)
- vSphere High Availability (HA)
- vSphere クラスタリングおよびリソース共有
- 仮想マシンのクローニング

vSphere ベストプラクティス

- 仮想マシンのスナップショットを使用しないことを推奨します。 スナップショットを使用する場合、システム変更を確認した後、スナップショットを採用するか、すぐに削除します。 スナップショットを長期間維持すると、性能が大幅に落ちる場合があります。
- SAN 環境の場合、ディスクイメージを高い IOP 番号の SAN に展開します。

  800 ユーザーシステムにおけるOVA 展開のための平均 IOPS は、管理仮想マシンの場合は506 (最大IOPS は855)、メディア仮想マシンの場合は475 (最大IOPS は652)です。 これらの仮想マシンが作成されて電源がオンになると、URLを入力してウェブブラウザ上でシステム展開を続行することができます。 プライマリシステムの平均 IOPS は108 (最大 IOPS は 1558)、 セカンダリシステムの平均 IOPS は 163 (最大 IOPS は1736)です。
- SAN に十分な容量があることを確認してください。 スナップショットは、同じ SAN に保存されます。
- 最も簡単で将来拡張可能な展開として 10GB を展開します。
- 同じ vCenter を使用することですべての仮想マシンを管理することを推奨します。 こうすることにより、システムの復元が簡単になります。

ネットワーク帯域幅の詳細については、ネットワーク帯域要件, （60 ページ）を参照してください。

vCenter Server の要件

vSphere に加えて、vCenter Server もまた必要です。

- この仮想アプライアンスを展開するためには、vCenter を使用して、システムの仮想マシンを展開し、展開することも必要です。 この製品は、vCenter Server なしでは機能しません。
- Cisco は重要なシステムに影響を与える操作の前に、システムのバックアップとスナップショットをとることを推奨しています。 バックアップの作成により、更新が期待通りにでき

なかった場合に、変更をロールバックすることができます。 vCenter を使用してバックアップとスナップショットを自動化することができます。

- CWMS は vSphere Standard Edition に対応します。

800 と 2000 ユーザのシステム用の vSphere Edition

- 800 および 2000 ユーザシステムは、30～40 個の vCPU の仮想マシンから構成されます。 これらの仮想マシンは、SSL エンコーディングとデコーディング、オーディオストリームのミキシングなどの非常に計算集約のタスクを実行するために、これらの vCPU を使用します。

  vCPU 要件の詳細情報については、CWMS および ESXi ホストが消費するリソース，（12 ページ）を参照してください。

- ローエンドの vSphere エディションは多くの必要な vCPU をサポートしないため、最低限、vSphere 5.0 Enterprise Plus エディションまたは vSphere 5.1 Enterprise エディションを購入する必要があります。

IOPS およびストレージシステムのパフォーマンス

予想される最大 IOPS とスループット

以下の表は、単一の仮想マシンのシステムに最大の負荷がかかっている場合に予想される最大 IOPS とスループット値を示しています。

システムサイズ	仮想マシン	最大 Input/Output Operations (IOPS)	1 秒あたりの最大読み取りメガバイト	1 秒あたりの最大書き込みメガバイト
50 ユーザのシステム	管理者	450	1	15
	DMZ	70	0.3	0.3
250 ユーザのシステム	管理者	1400	1	25
	メディア	150	1	10
	DMZ	110	0.4	0.6
800 ユーザのシステム	管理者	1400	3	50
	メディア	300	1	30
	DMZ	150	1	1.5

システムサイズ	仮想マシン	最大 Input/Output Operations (IOPS)	1 秒あたりの最大読み取りメガバイト	1 秒あたりの最大書き込みメガバイト
2000 ユーザのシステム	管理者	1600	2.5	60
	メディア	300	1	25
	ウェブ	200	3	1.5
	DMZ	200	1.5	3

2000 ユーザーシステムのシステムリブート用の IOPS

以下の表は、2000 ユーザーシステムにおけるブート (リブート) プロセスのための IOPS 情報を示しています。

2000 ユーザーシステムの仮想マシン	システムブート (リブート) 用の IOPS	マイナーアップデート用の IOPS
管理者	2300	3000
メディア	2000	2000
ウェブ	1500	2000
ウェブ	1000	2000

2000 ユーザーシステムのバックアップ用の IOPS

以下の表は、2000 ユーザーシステムにおけるオフ時間で実行したバックアップのための IOPS 情報を示しています。

2000 ユーザーシステムの管理仮想マシン	バックアップ用の IOPS	1 秒あたりの最大読み取りメガバイト	1 秒あたりの最大書き込みメガバイト
1 GB バックアップ	2000	220	300
12 GB バックアップ	5000	320	600

VMware vSphere ESXi のインストールとストレージの構成

Cisco WebEx Meetings Server はソフトウェアベースのソリューションです。 これはハードウェア/ソフトウェアパッケージの組み合わせではありません。 ハードウェアがCPU、メモリ、およびストレージの要件を満たすか超える限り、ハードウェアプラットフォームを購入およびプロビジョニングする方法の選択肢があります。

Cisco WebEx Meetings Server は当社の最小要件を満たす Cisco UCS Server で展開できます。 または、本製品を当社の最小要件を越えているより最新でハイエンドのUCSサーバで展開することを選択できます。

複数 RAID コントローラとネットワークオプションを使用できます。 ローカル RAID の代わりにSANストレージの使用を選択できます。 当社は選択可能なあらゆるストレージ構成について、詳細を提供しません。

ただし、Cisco WebEx Meetings Server は Cisco UCS サーバで展開されるため、『*Cisco UCS* サーバ *RAID* ガイド』をhttp://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/raid/configuration/guide/RAID_GUIDE.htmlで参照してください。

- VMware vSphere ESXi を UCS B-Series バックサーバにインストールするには、http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_B-Series_VMware_Install.htmlを参照してください。
- VMware vSphere ESXi を UCS C-Series ラックサーバにインストールするには、http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_C-Series_VMware_Install.htmlを参照してください。

詳細についてはdocwiki.cisco.com/wiki/VMware_Toolsを参照してください。

RAID コントローラーでのキャッシュ書き込みの設定

最適なシステムパフォーマンスのために、RAID コントローラーでデフォルトの書き込み設定をチェックする必要があります。 デフォルトの書き込みには以下の 3 つの設定があります。 *BBU* によるライトバック、ライトスルー、常にライトバック です。 Cisco UCS Server のデフォルトの書き込みに適切な設定を選択するためのガイドラインの一部は、以下のとおりです。

- **BBU によるライトバック** - RAID コントローラーにバッテリーバックアップユニットをインストールした場合に、この設定を使用します。 システムの電源が失われた場合、バッテリーバックアップユニットがコントローラーのキャッシュメモリーの内容を保持します。

  バッテリーバックアップユニットが故障するか、オフラインになって再学習サイクルになった場合、BBUによるライトバック設定は自動的に**ライトスルー**キャッシュにフェイルバックします。 動作中のバッテリーバックアップユニットなしでは、ライトスルー設定はホストマシンの I/O サブシステムのパフォーマンス劣化が発生しますが、より安全です。

- **ライトスルー** -修正のバッテリーのバックアップを排除する必要がある場合、この設定を使用して、明示的にキャッシュを有効にしてください（[ディスクキャッシュ] オプションを使用）。 この設定はより良いが、最適ではないパフォーマンスを与えます。 障害のあるバッ

テリーを交換した後で、デフォルトの書き込み設定をBBUモードによるライトバックに安全に戻します。

- **常にライトバック** - RAID コントローラーを格納するホストが無停電電源装置に接続されている場合に、この設定を使用します。

ミーティングへの参加

エンドユーザーの Cisco WebEx Meetings Server のエクスペリエンスは、ユーザーがミーティングをスケジュール設定したり参加するウェブサイトのものです。 このウェブサイトには、オンラインミーティングに役立つリアルタイムの会議エレメントが含まれます。 ユーザはブラウザまたはデスクトップのクライアントからミーティングに参加できます。

エンドユーザーのエクスペリエンスの詳細については、WebEx サイトにサインインして、[ヘルプ] を選択します。

Windows ユーザ

以下は、ユーザーが PC 上で WebEx ミーティングに参加できる Windows 管理者権限をもっていることを前提としています。 そうではない場合は、システム管理者が IBM Tivoli などの標準デスクトップ管理ソフトウェアを使用してユーザーに WebEx Meetings アプリケーションクライアントをプッシュすることができます。 管理サイトからのアプリケーションのダウンロード, （144 ページ）を参照してください。

- Microsoft Internet Explorer の場合、ユーザーは、ActiveX コントロールまたは Java プラグインをインストール、WebEx Meetings アプリケーションインストーラをダウンロード、またはシステム一時フォルダ（TFSなど）でアプリケーションを実行することができます。 クライアントソフトウェアは、ユーザーがミーティングに初めて参加したときに自動的にダウンロードおよびインストールされます。
- Google Chrome および Mozilla Firefox の場合、ユーザーは、Java プラグインのインストール、WebEx Meetings アプリケーションのダウンロード、システム一時フォルダでアプリケーション実行ができます。 クライアントソフトウェアは、ユーザがミーティングに初めて参加したときに自動的にダウンロードおよびインストールされています。

ActiveX、Java プラグイン、WebEx Meetings アプリケーションのインストーラーまたは TFS 設定を変更する必要はありません。

Mac ユーザ

- Java が使用可能な場合、クライアントソフトウェアは、ユーザがミーティングに初めて参加したときに自動的にダウンロードおよびインストールされています。 （Java は Mac OS X Lion バージョン 10.7 と OS X Mountain Lion バージョン 10.8 では、デフォルトでオフに設定できます。）
- Java が無効の場合、ユーザは WebEx Meetings アプリケーションをダウンロードしてインストールできます。

マルチデータセンターシステムユーザー

WebEx サイトが、有名な証明機関による証明書ではなく、自己署名証明書を使用する場合、あなたのデータセンターが他のデータセンターに結合した後で、ユーザーはミーティングを開始または参加する前に、信頼されたルート証明書機関に各データセンターの証明書をインストールする必要があります。

Chrome および FireFox ブラウザの使用

Chrome 32 以降または Firefox 27[17]以降を使用している場合、Cisco WebEx プラグインをインストールするプロンプトが表示されることがあります。必要なプラグインをインストールするには、[ダウンロード] を選択し、指示に従ってください。

（注） プラグインをインストールしたら、それを有効にする必要がある場合があります。

- Chrome を使用している場合は、ページの右上に表示されるプラグインアイコンを選択し、[プラグインを常に許可する…] オプションをチェックし、[完了] を選択します。
- Firefox を使用している場合は、URL の先頭（https: の前）に表示されるプラグインアイコンを選択し、 [常に許可する] を選択します。

ミーティングが自動的に開始されない場合は、ページを最新表示します。

WebEx ミーティングを開始、または WebEx 録画を再生するために、Chrome 38 以降のブラウザを使用する場合、以下のワンタイムインストレーションを完了して、Cisco WebEx 拡張機能を Chrome ブラウザに追加する必要があるかもしれません。

1. [WebEx を Chrome に追加] を選択します。
2. Cisco WebEx Extension ダイアログで [フリー] を選択します。
3. [追加] を選択すると、Cisco WebEx 拡張機能が Chrome ブラウザに追加されます。
4. Cisco_WebEx_Add-on.exe ファイルを開き、[実行] を選択します。
5. インストールが完了したら、ページが更新されます。 ミーティングが自動的に開始されない場合は、ページを最新表示します。

17 *このポリシーにより影響を受ける Chrome と Firefox の正確なバージョンは、このマニュアルの発行時点で確定していませんでした。

第 3 章

ネットワーク上での仮想マシンのレイアウト

Cisco WebEx Meetings Server (CWMS) は 2 つのグループの仮想マシンから構成されています。 内部仮想マシンとオプションのインターネットリバースプロキシ (IRP) 仮想マシンです。 IRP は、外部ユーザーが VPN や CDMA モバイルを使用することなく、インターネットを利用してミーティングを主催または出席できるシステムに必要です。 IRP が無い場合、内部および VPN ユーザーだけがミーティングを主催または参加できます。 IRP の詳細は、インターネットリバースプロキシに関するネットワークの検討事項, （58 ページ）を参照してください。

内部仮想マシン

内部仮想マシンとは、管理用仮想マシン、および該当する場合は、メディアおよびウェブ仮想マシンを指します。

- 内部仮想マシンは、単一で共通の VLAN またはサブネット上にある必要があります。 システム展開時に、 IP アドレスの割り当てがこのルールに違反した場合、エラーメッセージが表示されます。 システムデザインは、高可用性（HA）仮想マシンを含む、すべての内部仮想マシンは、高帯域幅で、パケットロスのない、遅延 4 ms 未満の LAN により接続されているものとしています。

  音声、データ、ビデオ、およびSANすべてがネットワーク帯域に依存しています。 必要な負荷を処理できるネットワークを展開することが重要です。

- Cisco はすべての内部仮想マシンを同じイーサネットスイッチに配置することを推奨します。 ただし、高可用性システムをプロビジョニングする場合には、ネットワークレベルの冗長性を確保するために、2 個のイーサネットスイッチを展開することを推奨します。

- 代わりに、仮想マシンを同じデータセンターの異なるイーサネットスイッチに配置することにした場合、ネットワークはで記された特定の帯域幅要件およびネットワーク遅延要件を満たす必要がありますネットワーク帯域要件, （60 ページ）。 この状況では、スイッチ対スイッチのトランクが L3 レイテンシーおよび単一の物理スイッチと同じネットワーク特性を備えている必要があります。

HA とシステムに関する追加情報については、HA または MDC 展開の冗長性，（56 ページ）を参照してください。

- システムに応じた異なるタイプのネットワークトポロジ，50 ページ
- 内部インターネットリバースプロキシ (IRP) のネットワークトポロジ，50 ページ
- 非スプリットホライズンネットワークトポロジ，51 ページ
- すべての内部ネットワークトポロジ，53 ページ
- スプリットホライズンネットワークトポロジ，54 ページ
- HA または MDC 展開の冗長性，56 ページ
- インターネットリバースプロキシに関するネットワークの検討事項，58 ページ
- ネットワーク帯域要件，60 ページ
- 帯域幅集約のための NIC チーミング，65 ページ
- ロードバランシング，66 ページ

システムに応じた異なるタイプのネットワークトポロジ

この製品は、以下のネットワークトポロジをサポートしています。

- 内部インターネットリバースプロキシ (IRP) のネットワークトポロジ，（50 ページ）
- 非スプリットホライズンネットワークトポロジ，（51 ページ）
- すべての内部ネットワークトポロジ，（53 ページ）
- スプリットホライズンネットワークトポロジ，（54 ページ）

（注） 使用しているネットワークのトポロジにフォワードプロキシが含まれている場合、インターネットリバースプロキシが正しく動作するように、固有の要件を満たす必要があります。 詳細は、『*Cisco WebEx Meetings Server* トラブルシューティングガイド』を参照してください。

内部インターネットリバースプロキシ(IRP)のネットワークトポロジ

このセクションでは、インターネットリバースプロキシ (IRP) 仮想マシンを含む、システムのすべての仮想マシンが同じ内部ネットワークにある場合のネットワークトポロジについて説明します。

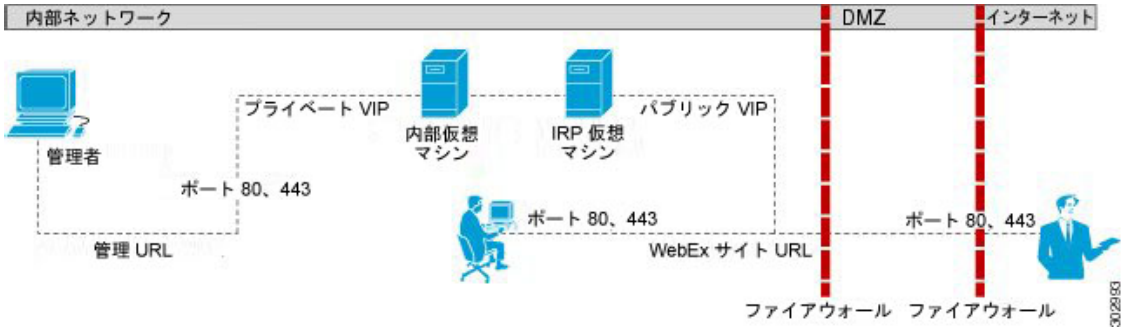
この設定はユーザにVPN接続なしでインターネットから安全にミーティングにサインインし、参加することを許可します。

自動展開を使用している場合は、すべての仮想マシン（IRP を含む）の ESXi ホスト は、同じ VMware vCenter から管理する必要があります。 この vCenter 情報は、システム自動展開時に必要です。

（注） この設定は、モバイルアクセスをサポートします。

システムの展開時に、管理 URL、WebEx サイト URL、プライベート VIP アドレス、パブリック VIP アドレスを定義します。 これら用語の詳細と、その使用については、『*Cisco WebEx Meetings Server* 管理ガイドの』「インストール」セクションを参照してください。

これは、すべての内部 IRP ネットワークトポロジの概略図です。



この展開に必要なポートアクセスのリストについては、すべての仮想マシンが内部ネットワークにある場合のポートアクセス, （95 ページ） を参照してください。

全内部 IRP ネットワークトポロジの利点

非スプリットホライズンネットワークトポロジと比較すると、DMZ内に仮想マシンが無く、内部ユーザーのネットワークトラフィックは、ミーティングを主催またはミーティングに出席するために、DMZ を通じて接続されません。

全内部 IRP ネットワークトポロジの欠点

パブリックアクセスでは（外部ユーザにシステムへのアクセスを許可）インターネットから内部ネットワークに直接受信ポート（80 と 443）を開く必要があります。

NAT の詳細は、インターネットリバースプロキシに関するネットワークの検討事項, （58 ページ）およびIRP を使用してパブリックアクセスをシステムに追加を参照してください。

非スプリットホライズンネットワークトポロジ

このセクションでは、非スプリットホライズンDNSがある場合のネットワークトポロジを説明します。 内部仮想マシン（管理、メディアおよびウェブ（該当する場合））は、内部ネットワークにあり、インターネットリバースプロキシは DMZ ネットワークにあります。

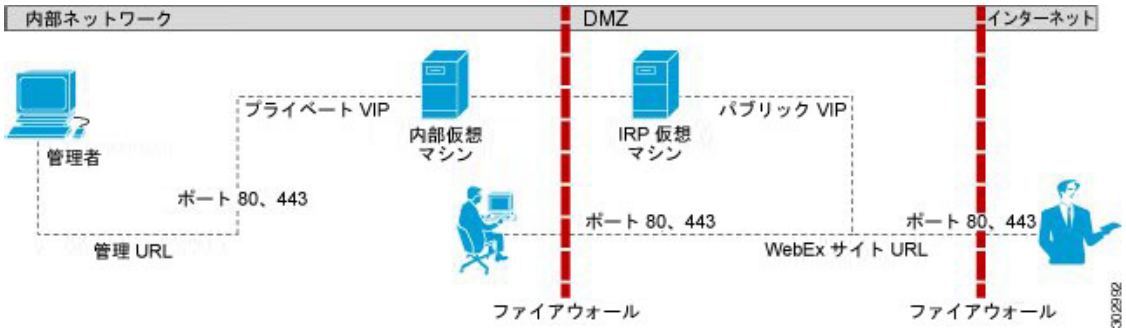
（注） この設定はユーザにVPN接続なしでインターネットから安全にミーティングにサインインし、参加することを許可します。

（注） この設定は、モバイルアクセスをサポートします。

この製品では、スプリットホライズンと非スプリットホライズンのネットワークトポロジの主な違いは、スプリットホライズンシステムでは内部ユーザがプライベート VIP アドレスを使用して WebEx サイト URL にアクセスすることです。 外部ユーザ（ファイアウォールの外側）は、パブリック VIP アドレスを使用して WebEx サイト URL にアクセスします。 非スプリットホライズンネットワークでは、すべてのユーザ（内部および外部）がパブリック VIP アドレスを使用して WebEx サイト URL にアクセスします。

システムの展開時に、管理 URL、WebEx サイト URL、プライベート VIP アドレス、パブリック VIP アドレスを定義します。 これら用語の詳細と、その使用については、『*Cisco WebEx Meetings Server* 管理ガイドの』「インストール」セクションを参照してください。

これは、非スプリットホライズンネットワークトポロジの概略図です。



（注） この展開に必要なポートアクセスのリストについては、DMZ ネットワーク内のインターネットリバースプロキシを使用するポートアクセス，（95 ページ） を参照してください。

非スプリットホライズンネットワークトポロジの利点

- ネットワークに入るトラフィック、出ていくトラフィックを厳密にコントロールできること。
- より一般的で単純な DNS ネットワークの要件に対応すること。

非スプリットホライズンネットワークトポロジの欠点

- セットアップが複雑であること。ただし、スプリットホライズンネットワークトポロジほど複雑ではない。

- 内部トラフィックが、DMZ ネットワークに流れる。 インターネットからのすべてのトラフィックが、内部 （プライベートネットワーク） からのトラフィックと共に、DMZ ネットワークのインターネットリバースプロキシに流れ、そこから内部仮想マシンに戻ることになる。
- 内部ネットワークトポロジと比べて、DMZ と内部ネットワークの間のファイアウォールで、より多くのポートを開く必要がある。
- 自動システム展開 （50、250、または 800 の同時ユーザのシステムのみ） では、vCenter でより複雑なセットアップが必要になる。
- 3 つのネットワークトポロジでは、すべてのミーティングの負荷がインターネットリバースプロキシにかかるため、この構成が最もネットワークのパフォーマンスに影響を与える。 複数のホップがあるため、ネットワークのレイテンシーも同様に影響を受ける。

（注） 非スプリットホライズン DNS 展開における NIC 速度の要件の詳細については、ネットワーク帯域要件, （60 ページ）を参照してください。

すべての内部ネットワークトポロジ

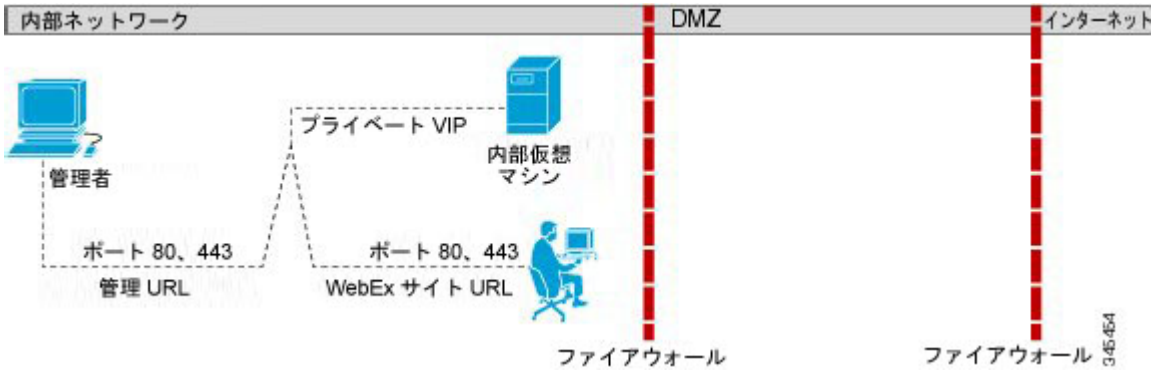
このセクションでは、システム内のすべての仮想マシンが同一の内部ネットワーク内に存在するネットワークトポロジについて説明します。 パブリックアクセスがありません。内部と VPN ユーザのみがミーティングを主催または参加できます。

（注） 自動展開を使用している場合は、すべての仮想マシンの ESXi ホストは、同じ VMware vCenter から管理する必要があります。 この vCenter 情報は、システム自動展開時に必要です。

（注） この設定は、モバイルアクセスをサポートしません。

システムの展開時に、管理 URL、WebEx サイト URL、プライベート VIP アドレスを定義します。これら用語の詳細と、その使用については、『*Cisco WebEx Meetings Server* 管理ガイドの』「インストール」セクションを参照してください。

これは、すべての内部ネットワークトポロジの概略図です。



全内部ネットワークトポロジの利点

- 仮想マシン間のネットワークホップがより少ないため、低い遅延を提供する。

全内部ネットワークトポロジの欠点

- パブリックアクセス（外部ユーザにシステムへのアクセスを許可）とモバイルユーザのためのアクセスがない。

スプリットホライズンネットワークトポロジ

このセクションでは、スプリットホライズンDNSがある場合のネットワークトポロジを説明します。 内部仮想マシン（管理、メディアおよびウェブ（該当する場合））は、内部ネットワークにあり、インターネットリバースプロキシは DMZ ネットワークにあります。

（注） この設定はユーザにVPN接続なしでインターネットから安全にミーティングにサインインし、参加することを許可します。

（注） この構成は、パブリック IP（インターネット）ネットワークからのモバイルアクセスのみをサポートしています。 モバイルアクセスは、内部（イントラネット）ネットワークではサポートされていません。

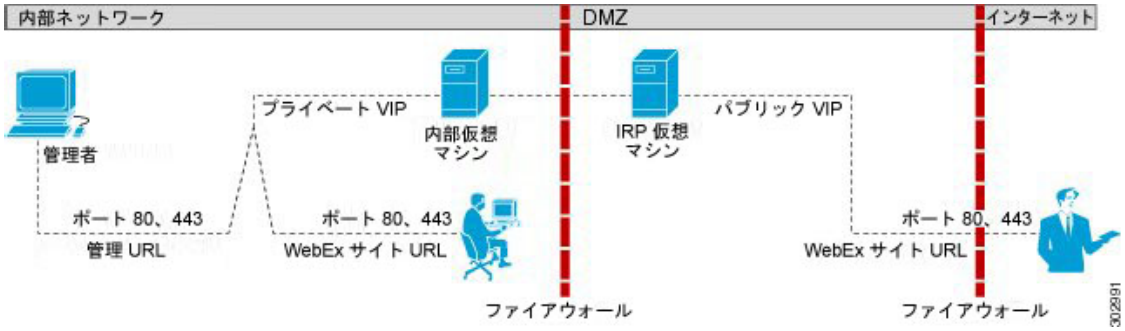
スプリットホライズン展開では、インターネットから生じるトラフィック（携帯データネットワークを利用しているモバイルユーザを含む）はインターネットリバースプロキシに送信されます。内部から生じるトラフィック（ローカル Wi-Fi を利用しているモバイルユーザを含む）は内部仮想マシンに直接送信されます。

この製品では、スプリットホライズンと非スプリットホライズンのネットワークトポロジの主な違いは、スプリットホライズンシステムでは内部ユーザがプライベート VIP アドレスを使用して WebEx サイト URL にアクセスすることです。 外部ユーザ（ファイアウォールの外側）は、パブリック VIP アドレスを使用して WebEx サイト URL にアクセスします。 非スプリットホライズン

ネットワークでは、すべてのユーザ（内部および外部）がパブリック VIP アドレスを使用して WebEx サイト URL にアクセスします。

システムの展開時に、管理 URL、WebEx サイト URL、プライベート VIP アドレス、パブリック VIP アドレスを定義します。 これら用語の詳細と、その使用については、『*Cisco WebEx Meetings Server* 管理ガイドの』「インストール」セクションを参照してください。

これは、スプリットホライズンネットワークトポロジの概略図です。



（注） この展開に必要なポートアクセスのリストについては、DMZ ネットワーク内のインターネットリバースプロキシを使用するポートアクセス，（95 ページ） を参照してください。

スプリットホライズンネットワークトポロジの利点

- ネットワークに入るトラフィック、出ていくトラフィックを厳密にコントロールできること。
- システムをヒットするネットワークトラフィックを分離できるため、負荷をより分散できる。

  インターネットから入るトラフィックは、インターネットリバースプロキシに流れる。内部（プライベートネットワーク）からのトラフィックは直接内部仮想マシン（管理、メディアおよびウェブ（該当する場合））へ流れる。
- パフォーマンスとレイテンシーは、非スプリットホライズン DNS より優れているが、すべての内部ネットワークトポロジよりは劣る。

スプリットホライズンネットワークトポロジの欠点

- 3 つの異なるネットワークトポロジで、セットアップが最も複雑。
- 高度な DNS マッピングを必要とする。
- 内部ネットワークトポロジと比べて、DMZ と内部ネットワークの間のファイアウォールで、より多くのポートを開く必要がある。
- 自動システム展開 （50、250、または 800 の同時ユーザのシステムのみ） では、vCenter でより複雑なセットアップが必要になる。

- ウェブリダイレクションのため、内部ユーザに対して、WebEx サイト URL がウェブサービスを含んでいる仮想マシンならびにメディア仮想マシンのホスト名を露出させる URL に置き換わってしまう。

スプリットホライズン DNS 展開における NIC 速度の要件の詳細については、ネットワーク帯域要件, （60 ページ）を参照してください。

HA または MDC 展開の冗長性

高可用性 (HA) は故障したプライマリ Cisco WebEx Meetings Server (CWMS) システムから同一の物理的な場所にあるバックアップ用の CWMS HA システムへのフェイルオーバーによって、冗長性を実現します。

CWMS マルチデータセンター (MDC) は複数のデータセンターを展開し、単一の CWMS システムに結合します。フェイルオーバーはHAシステムと似ていますが、MDCシステムデータセンターはユーザーにサービスを提供するピアで、地理的に制限されていません。 実際、地理的にユーザーに近い複数のデータセンターを展開すると、ネットワークのパフォーマンスが向上します。CWMS システムは HA と MDC の両方をサポートできません。

冗長性の条件:

- HA仮想マシンはプライマリ仮想マシンと同じデータセンター内に共存することが必要です。これらのすべての仮想マシンが同一の VLAN またはサブネット上になければなりません。プライマリ仮想マシン用に以前に定義されたのと、プライマリと HA のコンポーネント間の接続の速度と遅延要件は同じです。 データセンター間のシステムのプライマリおよびHA のコンポーネントの分割はサポートされません。

  MDC 仮想マシンは同一のデータセンターに置く必要はありません。

- すべての内部仮想マシンの間の接続は、スイッチまたはネットワークリンクに障害が発生し、プライマリと HA または MDC のコンポーネント間の接続を切断しないように、完全に冗長化されなければなりません。 この冗長性を実現するには、各ホストサーバーは複数の Ethernet スイッチとの間に冗長な接続を備えている必要があります。

- プライマリおよび HA のインターネットリバースプロキシ (IRP) 仮想マシンは共通の VLAN またはサブネット（通常、内部仮想マシンと同じサブネットではありません）上にある必要があります。インターネットリバースプロキシ仮想マシン間の接続は、内部仮想マシンと同様に、冗長化されなければなりません。

  MDC システム中のデータセンターを結合後、IRP はデータセンターで有効または無効にできます。 CWMS MDC システムのすべてのデータセンターの IRP 構成は合致しなければなりません。不一致があってはなりません。

HA または MDC システムの追加により、合計のシステム容量は増えません。 800 ユーザシステムを HA 付きまたはなしで展開できるかどうかにかかわらず、システム容量の合計は引き続き同じになります。音声の同時接続の最大数は 800 です。

HA または MDC システムは、展開での各仮想マシンタイプの冗長仮想マシンから構成されます。(仮想マシンの各タイプの説明については、システムの仮想マシン，（9 ページ）を参照してください。)例:

- 50 ユーザーシステムは管理用仮想マシンと、任意でパブリックアクセスのための Internet Reverse Proxy (IRP) 仮想マシンから構成されます。 HA（MDC を利用できない場合）システムを追加する場合、結合された 50 のユーザーシステムには、2 つの管理用仮想マシンおよび 2 つの IRP 仮想マシンを含みます。
- プライマリの 250 または 800 ユーザーシステムは、管理用仮想マシン、メディア仮想マシン、およびオプションで IRP 仮想マシンから構成されています。 HA または MDCシステムを追加する場合は、結合された 250 または 800 のユーザーシステムには、2 つの仮想マシンでは、2 つのメディア仮想マシン、および 2 つの IRP 仮想マシンを含みます。
- プライマリ 2000 ユーザーシステムは、管理用仮想マシン、3 つのメディア仮想マシン、2 つのウェブ仮想マシン、および任意で IRP 仮想マシンから構成されます。 HA または MDC システムを追加する場合は、結合された 2000 のユーザーシステムには、2 つの 管理者仮想マシン、4 つの（3 プラス 1 冗長）メディア仮想マシン、3 つの（2 つの冗長マシンと 1 つの冗長マシン）ウェブ仮想マシン、および 2 つの IRP 仮想マシンから構成されています。

HA または MDC システムでは、パブリック VIP アドレスと プライベート VIP アドレスがプライマリシステムと共有されます。 （パブリック VIP アドレスとプライベート VIP アドレスは異なり、共有されません。）1 つの仮想マシンが停止しているとき、もう一方の仮想マシンが同じ VIP アドレスを使用します。 この動作のため、仮想マシンの障害はDNS インフラストラクチャの通常でない要求を行わずに、エンドユーザに透過的に伝達されます（ミーティングは続行されるため）。 ただし、共有 VIP アドレスは単一のネットワークセグメントまたは VLAN だけで実装できます。2 つのデータベースで VLAN を分割すると、複数の問題が生じます。

プライマリおよびHA 内部仮想マシンは、同一のデータセンター内で接続される必要があります。これによって、仮想マシンの障害とネットワークの障害とを区別する問題を大幅に減らせます。分割ネットワークを許可することにより、ミーティング接続が分割され、データベースの更新が競合する場合があります。 それは複数のデータセンター間よりも、単一のデータセンター内に HA ネットワークセグメントを構築する方がはるかに実用的です。

MDC システムでは、データはすべてのデータセンターで複製されます (License Manager を除く)。したがって、データセンターがダウンするか、ネットワーク接続が切断しても、残存のデータセンターは地理的な場所と無関係に、ユーザーへサービスを提供し続けます。

障害許容差システムを構築するための最良の方法は、ほとんどのシステムコンポーネントで「すべてのアクティブ」として動作するときです。 ただし、特定のキーコンポーネント、特にデータベースサービスは「アクティブ/スタンバイ」です。 （HA システム内の ウェブサーバーおよびメディアコンポーネントは、プライマリシステムのコンポーネントに依存しています。） その接続上の任意の遅延または中断がミーティングに参加する場合は特に、ユーザーのための遅延をもたらします。 メディアサービスコンポーネント間の遅延は、ミーティング中に数人のユーザーの音声とビデオの遅延を増大させます。 （Cisco WebEx Meetings Server では、内部仮想マシン間で 4 ミリ秒のネットワーク遅延が許容されます。 詳細は、ネットワーク上での仮想マシンのレイアウト，（49 ページ） を参照してください。）

インターネットリバースプロキシに関するネットワークの検討事項

インターネットリバースプロキシ仮想マシンは、内部仮想マシンと同じ一般的ネットワーク要件を共有します。 非スプリットホライズンおよびスプリットホライズン DNS 構成では、インターネットリバースプロキシ仮想マシンは、内部ネットワークではなく、 DMZ ネットワークに展開します。

制約事項 Cisco UCS サーバが 2 個の NIC で構成されていても、Cisco WebEx Meetings Server は 1 個の NIC をインターネットに、およびもう 1 個の NIC をイントラネットにポイントすることをサポートしません。 この制限は vSphere（およびインターネットリバースプロキシ）によって使用される物理 NIC と仮想 NIC の間のマッピングに関わらず、適用されます。

インターネットリバースプロキシ仮想マシンは、使用する NIC の数に関わらず、常に単一の外部 VLAN に接続します。 複数の物理 NIC を使用し、それらが異なるスイッチまたはルーターに接続されている場合、NIC は同じ VLAN に接続されているままである必要があります。

そのため、インターネットリバースプロキシを使用して、（1 個をインターネットにポイントし、もう 1 個をイントラネットにポイントした状態で）2 個の別々のネットワークセグメントのトラフィックをつなげることはできません。 次のセクションでは、この目標を達成する方法について説明します。

内部仮想マシンとインターネットリバースプロキシ間の遅延

インターネットリバースプロキシの NIC とあらゆる内部仮想マシンの NIC 間のパスにおける、許容できる最大の往復遅延時間は 4 ミリ秒です。 このパスにおける過度の遅延は、音声、ビデオ、およびデスクトップ共有の機能を利用するエンドユーザーの使用可能な帯域幅を制限します。 たとえば、遅延が 4 秒から 8 秒に増加する場合、使用可能な帯域幅は半減し、エクスペリエンスは遅延が増えるにしたがって悪化します。

（注） 4 ミリ秒の遅延の制限は、いかなる Cisco WebEx Meetings Server コンポーネントとエンドユーザのエンドポイント間のパスには適用されません。

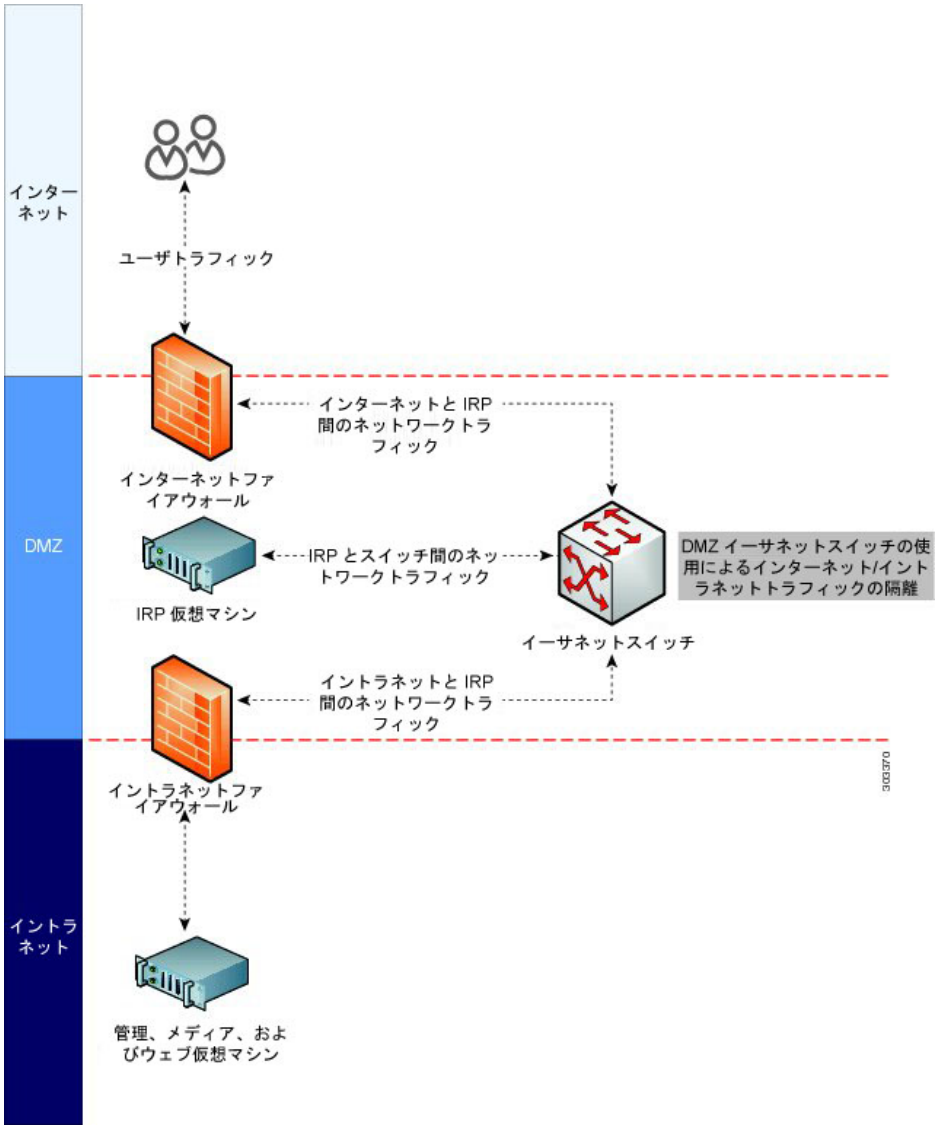
（注） IRP と 内部仮想マシン間における遅延が 4 秒を超える場合、Cisco WebEx Meetings Server インターネットリバースプロキシを通るエンドユーザーの接続に深刻な遅延が発生する可能性があります。

ネットワークトラフィックの隔離

DMZ イーサネットスイッチを使用することで、インターネットと内部ネットワーク間のネットワークトラフィックの隔離をセットアップできます。 以下の手順と図は、1 つの例を描写しています。

1. インターネットリバースプロキシをヘッドエンドスイッチまたはルーターに接続して、そのスイッチまたはルーターを使用して、インターネットとイントラネットのトラフィックを分割します。
2. スイッチまたはルーターがトラフィックを分割したら、その2つのトラフィック パターンをスイッチまたはルーターにある 2 個の別々の物理ポートにパイピングできます。 1 個のポートはイントラネットにポイントし、もう 1 つのポートはイントラネットにポイントします。

これは、サンプルのネットワークトポロジの図です。



ネットワーク帯域幅の要件に関する情報については、ネットワーク帯域要件, （60 ページ）を参照してください。

ネットワーク帯域要件

このセクションでは、50、250、800、および2000ユーザのシステムにおける帯域幅の要件について説明します。 このセクションで概説されている帯域幅の要件を満たすと、WebExミーティングを主催および参加するユーザに対して高品質のエンドユーザエクスペリエンスを提供し、ネットワークがウェブ共有、音声、およびビデオトラフィックの要求をサポートできることを確認するのに役立ちます。

エンドユーザセッションの帯域幅の推定

ユーザシステムのサイズに対し、ビデオ、音声、およびウェブ共有に要求されるトラフィックをサポートするために、ネットワーク帯域幅を推定することは重要です。 この製品の帯域幅の要件は、基本的にCisco WebExのクラウドサービスと同じです。 ネットワークプロビジョニングを最適化する場合、Cisco WebExクラウドサービスの使用帯域幅は『WebExネットワーク帯域幅ホワイトペーパー』に示されています。

以下の表の条件は、ビデオ、音声およびウェブ共有で予想される帯域幅を示します。

WebExミーティングコンポーネント	集約エンドユーザセッション帯域幅
ビデオ（360p + 6 サムネイル）	1.5 Mb/秒
音声	0.1 Mb/秒
ウェブ共有 （この値は、スライドを 30 秒ごとに進めることを想定しています。）	0.6 Mb/秒
合計最大帯域幅	2.2 Mb/秒

単一ユーザ接続では2.2 Mb/秒が予期される最大帯域幅ですが、Ciscoは帯域幅の要件を計算する場合、1.5 Mb/秒の予期される最大帯域幅を使用することを推奨します。 最大ユーザ数の半分のみがビデオ、音声、およびウェブ共有を用いる間に、残りのユーザは音声とウェブ共有のみが使用可能なため、これにより各ユーザ接続につき約1.5 Mb/秒の平均帯域幅が生じます。

『*WebEx* ネットワーク帯域幅ホワイトペーパー』を参照すると、前のテーブルにある帯域幅の値は最悪ケースのトラフィック状態に基づいていることが分かります。 平均帯域幅の使用率はそれよりかなり小さいですが、Ciscoは以下の理由で最悪ケースの数値を使用することを推奨します。

- 計算において最悪ケースの数値を使用することは、多用によるユーザエクスペリエンスの劣化を防ぐために、必要な帯域幅を提供すること助けます。

- Cisco WebEx Meetings Server はミーティング中に、同じデータを参加者に同時に送信します。WebEx 主催者がプレゼンテーションのページを進めるとき、そのページの画像（場合によって数メガバイトから成る）は各エンドポイントに別々に可能な限り早く同時に送信されます。

ネットワークパスでの帯域幅

以下のプロセスを使用して、さまざまなネットワークパスで必要な帯域幅を特定します。

1. 前のセクションで提供されているテーブルを使用して、ユーザセッションに対する平均帯域幅を特定します。
2. そのリンク上で同時接続が予期される最大ユーザ数を特定します。
3. 合計帯域幅に最大ユーザ数をかけます。

シナリオの例：

- インターネットから同時に最大 100 ユーザが接続することが予期される場合、ISP 接続および外部ファイアウォールからインターネットリバースプロキシを通して、恐らく 1.5 Mb/秒 × 100 = 150 Mb/秒の使用可能な帯域幅が必要になります。インターネットリバースプロキシの詳細については、を参照してください。インターネットリバースプロキシに関するネットワークの検討事項, （58 ページ）
- すべての接続がインターネットリバースプロキシを通過する 2000 ユーザシステムがあると想定します。 このシナリオでは、すべての 2000 ユーザのトラフィックがインターネットリバースプロキシに接続してから、インターネットリバースプロキシから内部仮想マシンに接続すると想定する必要があります。ネットワークの他の部分からインターネットリバースプロキシで受信される集計帯域幅は、2000 × 1.5 Mb/秒 = 3 Gb/秒になります。 非スプリットホライズンの詳細については、非スプリットホライズンネットワークトポロジ, （51 ページ）を参照してください。

（注） 同じ 3 Gb/秒のトラフィックがインターネットリバースプロキシを通して送受信され、それによってインターネットリバースプロキシの NIC が 6 Gb/秒のユーザトラフィックを処理することが要求されます。 インターネットリバースプロキシにおける NIC の帯域幅の詳細については、次のセクションを参照してください。

- スプリットホライズン DNS 展開で 2000 ユーザシステムがあると想定します。 このシナリオでは、インターネットユーザはインターネットリバースプロキシに接続し、イントラネットユーザは内部仮想マシンに直接接続します。 ユーザの 10 パーセントインターネットを使用してミーティングに接続するのに対し、90 パーセントのユーザがイントラネットを通して接続すると想定します。 結果として、インターネットリバースプロキシに入ってくる集約帯域幅がこれで約 300 Mb/秒になります（2000 ユーザの 10 パーセントに 1.5 Mb/秒をかけると、300 Mb/秒になる）。 その同じ 300 Gb/秒のトラフィックがインターネットリバースプロキシから通過してくる場合、インターネットリバースプロキシの NIC は 600 Gb/秒のユーザトラフィックを処理することが要求される可能性があります。 これは前のシナリオで説明された

非スプリットホライズン DNS 展開より劇的に低い帯域幅の要件です。 ネットワークトラフィックの削減はNICまたはスイッチインターフェース速度の推奨事項（次のセクションを参照）に直接影響を与え、それはより安い 1 Gb/秒 NIC をインターネットリバースプロキシの Cisco UCS サーバ、または DMZ ネットワークで 1 ギガビットイーサネットスイッチインフラストラクチャを展開することを可能にします。 スプリットホライズンの詳細については、スプリットホライズンネットワークトポロジ，（54 ページ）を参照してください。

（注） インターネットリバースプロキシの使用が 1000 Mb/秒のしきい値に少し近い場合、NIC チーミング用に構成されている 1 ギガビットイーサネット NIC を展開する必要がある場合があります。

詳細に関しては帯域幅集約のための NIC チーミング，（65 ページ）を参照してください。

Cisco WebEx Meetings Server ネットワークインターフェースでの帯域幅

スイッチングアーキテクチャとシステム間のダイレクトインターフェースでは、以下のテーブルに示されている最高速度にインターフェース NIC をプロビジョニングすることが推奨されます。これらの速度はローカルのスイッチングインフラストラクチャのみで、Cisco UCS サーバとヘッドエンドスイッチのポート間の接続性に適用されます。 これらが最悪ケースのトラフィック要件をサポートするために必要な推奨速度です。

システム容量	NIC またはスイッチインターフェース速度
50 ユーザのシステム	1 Gb/s
250 ユーザのシステム	1 Gb/s
800 ユーザのシステム	10 Gb/s[18][19]
2000 ユーザのシステム	10 Gb/s[20]

18 オプションで、UCS サーバで 2 個以上のギガビットイーサネット NIC およびヘッドエンドスイッチで NIC チーミングを使用することにより、NIC チーミングを展開することで、ネットワークインフラストラクチャの費用を削減できます。

19 800 ユーザーシステムの展開で内部 DAS ストレージを使用している場合、オプションで、UCS Server で 2 ギガビット以上のイーサネットNIC を使用して NIC チーミングを展開するか、またヘッドエンドスイッチで NIC チーミングを展開することで、ネットワークインフラストラクチャのコストを減らすことができます。 しかし、展開が SAN または NAS ストレージを使っている場合は 10 ギガビットイーサーネットリンクが必要になります。

20 非スプリットホライズン DNS 展開がある場合は、10 Gb/秒の要件は IRP と内部仮想マシンに関連します。 スプリットホライズン DNS 展開がある場合、IRP（およびDMZ ネットワーク）のネットワークインフラストラクチャの要求を削減できて、それによって「ネットワークパスでの帯域幅」セクションで説明されている通りに、より安い 1 Gb/秒 NIC をインターネットリバースプロキシの Cisco UCS サーバ、または DMZ ネットワークで 1 ギガビットイーサネットスイッチインフラストラクチャを展開することを可能にします。ただし、内部仮想マシン（および内部ネットワーク）では 10 Gb/秒の速度の要件が当てはまります。

スプリットホライズン DNS 展開に対する 1 Gb/秒 NICS とイーサネットスイッチの使用の詳細については、次のセクションである「スプリットホライズンDNS展開に関する帯域幅の検討事項」を参照してください。

NIC 速度の計算における想定：

- 集約エンドユーザセッションの帯域幅（1.5 Mb/秒）が前のテーブルに示されている NIC 速度を計算するために使用されました。
- 仮想マシン間のコントロールトラフィックは混雑していない必要があります。 これは特に 2000 ユーザシステム、および高可用性のためにプロビジョニングされたシステムに適用されます。 仮想マシンリンクでの重度の混雑は、システムの不安定性をもたらし、結果としてサービスの中断が生じる可能性があります。
- 録画とデータベースバックアップに使用される NAS ストレージへの接続は、混雑していない必要があります。
- プロトコルのオーバーヘッドと展開の非効率性は、1 Gb/秒または 10 Gb/秒の速度ラベルより大幅に小さい使用可能なリンクの帯域幅を生じさせます。
- ユーザがミーティングにログインするときに、トラフィックの大きな割合がインターネットリバースプロキシに到達する場合、すべてのユーザ接続がインターネットリバースプロキシの NIC を 2 回通過（送受信）することに留意する必要がります。 2,000 ユーザーのシステムを例として使用し、これはインターネットリバースプロキシの NIC が 6Gb/ 秒のユーザートラフィック（2,000 ユーザーに 1.5Mb/ 秒をかけると 3Gb/秒になり、それに送受信トラフィックのために2をかけると 6Gb/ 秒になる）を処理する必要がある可能性があることを意味します。

保守的に、ローカル接続がユーザメディアトラフィックに対して 60 パーセントの使用を超えないようにし、残りの 40 パーセントを他のトラフィック、異常なトラフィックバースト、およびネットワークオーバーヘッドのために使用可能にすることを要求します。 800 ユーザシステムを例として使用して、管理とメディア仮想マシンのエンドユーザトラフィックが 1.2 Gb/秒で、インターネットリバースプロキシ仮想マシンが 2.4 Gb/秒になると推定します。 60 パーセントルールを適用し、管理とメディア仮想マシンでは NIC が 2 Gb/秒（推定される管理とメディア仮想マシンのユーザートラフィックの 1.2 を推定される通常帯域幅消費である 60 パーセントで割ると 2.0 Gb/秒になる）、インターネットリバースプロキシ仮想マシンでは 4 Gb/秒を処理できるようにします。

（注） 前のテーブルで示されている NIC 速度は、SAN ストレージにアクセスするために使用される帯域幅を考慮に入れていません。 ファイバーチャンネルオーバーイーサネット（FCoE）が SAN 接続に使用されている場合、それを独自のネットワークインタフェースを使用するようにプロビジョニングする必要があります。

スプリットホライズン DNS 展開に関する帯域幅の検討事項

スプリットホライズン DNS 展開では、一部のユーザはインターネットからミーティングにログインし、そのトラフィックはインターネットリバースプロキシに到達し、内部ネットワークにいる大半のユーザはインターネットリバースプロキシに到達せずにミーティングにログインします。 スプリットホライズン DNS 展開では、ネットワークをスピードアップさせ、内部ネットワーク内にほとんどのトラフィックが残るようにトラフィックを分割すると、NIC チーミングを使用して低性能の NIC（1 Gb/秒 NIC）をインターネットリバースプロキシでプロビジョニング、およびイ

ンターネットリバースプロキシとインターネット間のスイッチングインフラストラクチャが1Gb/秒、または少なくとも2000ユーザのシステムにおいて推奨の10Gb/秒より低くなるようにプロビジョニングできる可能性があります。

たとえば、会社にインターネットから同時に2000ポートユーザシステムへのアクセスを望んでいる100人のユーザがいる場合、150Mb/秒の帯域幅が必要になります（1.5Mb/秒の集約ユーザセッション帯域幅 * 100人のユーザ = 150Mb/秒）。 これは定められている10Gb/秒のインターフェース要件とは対照的に、DMZネットワークからインターネットリバースプロキシのネットワークインフラストラクチャが1Gb/秒イーサネットスイッチである可能性があること、およびインターネットリバースプロキシのイーサネットNICインターフェースが1Gb/秒である可能性があることを暗示しています。 インターネットリバースプロキシで2倍のトラフィックが見られることを考慮に入れても（つまりNICが300Mb/秒のユーザートラフィックを処理することが必要になることを意味する）、（「Cisco WebEx Meetings Serverネットワークインターフェースでの帯域幅」セクションで説明されている通りに）60パーセントルールを適用するとそれは500Mb/秒になります。 1Gb/秒リンクでまだ十分ですが、100人のユーザーでなく250人のユーザーを想定すると十分でなくなります。

（注） 低域幅の最適化は、スプリットホライズンDNS展開におけるインターネットリバースプロキシのNICのみに対して適用されます。

非スプリットホライズンDNS展開では、10Gb/秒イーサネットスイッチとイーサネットNICインターフェースをインターネットリバースプロキシに展開する必要があります。

マルチデータセンターのネットワーク要件

2つのデータセンター間のネットワークリンクの要件は、以下のとおりです。

- 重要なデータセンター間通信には、4.5 Mbpsの帯域幅が保証されること。
- 200 ms未満の遅延（往復時間の遅延）。

データセンター間カスケード接続ミーティングのためのデータセンターのネットワーク要件は、以下のとおりです。

- 音声およびWebを使用する各カスケード接続ミーティングには、0.16 Mbpsが必要。
- 180pのLQビデオ、音声、およびWebを使用する各カスケード接続ミーティングには、0.66 Mbpsが必要。
- 360pのHQビデオ、音声、およびWebを使用する各カスケード接続ミーティングには、1.20 Mbpsが必要。
- 200 ms未満の遅延（往復時間の遅延）。

たとえば、最も厳しい条件として、2000ユーザーシステムがカスケード接続されている場合（1000ミーティングの最大数）。 半数がビデオを利用し、半数がビデオを利用しない場合:

- *HQ* ビデオ *:* 500 x 1.2 + 500 x 0.16 = 680 Mbps

- *LQ* ビデオ*:* 500 x 0.66 + 500 x 0.16 = 410 Mbps

800 ユーザーのシステム:

- *HQ* ビデオ*:* 680 / 2000 x 800 = 272 Mbps
- *LQ* ビデオ*:* 410 / 2000 x 800 = 164 Mbps

250 ユーザーのシステム:

- *HQ* ビデオ*:* 680 / 2000 x 250 = 85 Mbps
- *LQ* ビデオ*:* 410 / 2000 x 250 = 51.25 Mbps

詳細については、 http://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/white-paper-listing.htmlを参照してください。

帯域幅集約のための NIC チーミング

内部仮想マシンで ESXi ホストを含む UCS サーバで NIC チーミングを構成することには 2 つの利点があります。 NIC チーミングは物理ネットワークと仮想ネットワーク間のネットワークトラフィックをロードバランスし、ハードウェアの不具合またはネットワーク停止の発生時に、フェールオーバーを提供します。 さらに、10 Gb/秒 のインフラストラクチャが使用できない展開では、複数の 1 Gb/秒の NIC をチーミングすることで同等の結果を得られる可能性があります。

（注） 異なるサイズのユーザシステムに対して必要な NIC 速度の詳細については、この章の「Cisco WebEx Meetings Server ネットワークインターフェースでの帯域幅」のセクションを参照してください。

Cisco はすべてのユーザシステムサイズ（50、250、800、および 2000 ユーザのシステム）に対し、帯域幅ロードバランシングのための NIC チーミングをサポートしますが、それは 800 ユーザのシステムにおけるネットワーク費用の最適化を試みている顧客に最も役立ちます。 展開で内部DAS ストレージを使用する場合、Cisco UCS サーバーと 800 ユーザーのシステムにおけるヘッドエンドスイッチ間の送受信の帯域幅の要件は、最悪ケースのトラフィック要件をサポートするために、デュアル 1 ギガビットイーサネット NIC（または HA のあるシステムにおけるクアッド 1 ギガビットイーサネット NIC）の使用に類似すると推定されるため、UCS サーバーを 10 ギガビットイーサネット NIC でプロビジョニングする（または 10 ギガビットイーサネットヘッドエンドスイッチを購入する）必要性を軽減します。

（注） 展開が SAN または NAS ストレージを使用する場合、Cisco UCS サーバーと 800 ユーザーのシステムにおけるヘッドエンドスイッチ間の送受信の累積帯域幅の要件は、10 ギガビットイーサネットです。

（注） VMware での NIC チーミングのプロビジョニングに関する情報については、http://kb.vmware.com で VMware ドキュメントを参照し、「ESXi/ESX での NIC チーミング」を検索してください。

従来のネットワークインターフェースとイーサネットスイッチの使用を想定する場合、以下のプロセスで概説されているように、NIC チーミングと重複スイッチの使用により、冗長性を提供できます。

- IEEE 802.3ad/IEEE 802.1ax リンク集約制御プロトコル（LACP）をサポートするイーサネットスイッチをセットアップします。
- vCenter を使用し、Cisco WebEx Meetings Server 仮想マシンに関連付けられている仮想マシンポートグループを両方の物理アダプタに接続します。
- 両方の物理アダプタをスイッチに接続します。
- スイッチをプロビジョニングして、2 個のポートをチームとして静的にプロビジョニングします。
- VMware vSphere を使用して、NIC チーミングをアクティブ/アクティブに設定し、両方の NIC インターフェースにおけるスループットを許可します。

たとえば、800 ユーザの展開において、内部仮想マシンでの ESXi ホストでは各 10 Gb/秒リンクを 2 個の 1 Gb/秒リンクに代えることができて、インターネットリバースプロキシでは各 10 Gb/秒リンクを 4 個の 1 Gb/秒リンクに代えることができます。 （「HA 展開での冗長ネットワーク接続」セクションで説明されている通りに、HA のあるシステムでフォールトトレランスを得るには、リンク数を 2 倍にする必要があります。） 内部仮想マシンでの ESXi ホストで、2 個の 1 Gb/秒リンクを 1 個目のイーサネットスイッチに加えて、2 個の 1 Gb/秒リンクを 2 個目のイーサネットスイッチに接続します。

（注） 『*Cisco WebEx Meetings Server* システム要件』で示されているサーバ構成の例では、この目的のための NIC チーミングをサポートするために十分なネットワークインターフェースがありません。」

ロードバランシング

どのタイプのトラフィックが処理される場合でも、ロードバランシングは常に CWMS で実行され、構成できません。

システムはすべての Web ノードで均一なロードバランシングを試みます。 展開が High Availability (HA) の無いシステムの場合、そのシステム上にある Web ノードすべてで接続が分散されます。 HA 展開の場合、システムはプライマリシステムと HA システム両方で Web ノードをロードバランシングに利用します。 1 つに障害が発生し、すべての Web ノードで障害が発生したわけではない場合、システムは稼働を続けますが、容量は減少します。

Internet Reverse Proxy (IRP) ノードはエントリポイントであり、大部分のロードバランシングの決定はここで実行されます。 IRP ノードのみがシステムでアクティブになります。 HA 展開のないシステムには 1 つの IRP ノードのみがあります。 HA 展開のシステムには IRP ノードが 2 つあり、一方の IRP が非アクティブの間、もう一方の IRP がアクティブになります。 DNS 構成によっては、IRP は外部トラフィックすべて（非分割 DNS の場合、内部トラフィックすべて）に対応します。

複数のホストで障害が発生した場合、機能と容量に影響が生じる可能性があります。

第 4 章

システムのネットワークチェックリスト

ネットワークチェックリストは、DNS の構成やパブリックアクセスを有効（ユーザーがインターネットやモバイル端末からミーティングをホストまたは参加できる）にしているかどうかに応じて、システムに必要なネットワークの変更を一覧します。

自動システム展開（50、250、800 ユーザでの展開で推奨）を使用しているか、あるいは手動でのシステム展開（2000 ユーザでの展開で必要）であるかに応じて、該当するチェックリストを選択します。

- インターネットリバースプロキシを含めて、すべての仮想マシンが内部ネットワークにある（最も簡単な設定）。
  - 自動展開およびパブリックアクセスによるインストールまたは拡張のネットワークチェックリスト，（71 ページ）
  - 手動展開、パブリックアクセスおよびすべての内部仮想マシン によるインストールまたは拡張のネットワークチェックリスト，（73 ページ）
- 非スピリットホライズン DNS (もっとも一般的な DNS 構成)
  - 自動展開、パブリックアクセスおよび非スピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，（77 ページ）
  - 手動展開、パブリックアクセスおよび非スピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，（79 ページ）
- スプリットホライズン DNS
  - 自動展開、パブリックアクセスおよびスピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，（83 ページ）
  - 手動展開、パブリックアクセスおよびスピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，（85 ページ）
- パブリックアクセスなしのシステム

- 自動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト，（89 ページ）
- 手動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト，（91 ページ）

- 自動展開およびパブリックアクセスによるインストールまたは拡張のネットワークチェックリスト，71 ページ
- 手動展開、パブリックアクセスおよびすべての内部仮想マシンによるインストールまたは拡張のネットワークチェックリスト，73 ページ
- 自動展開、パブリックアクセスおよび非スピリット ホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，77 ページ
- 手動展開、パブリックアクセスおよび非スピリット ホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，79 ページ
- 自動展開、パブリックアクセスおよびスピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，83 ページ
- 手動展開、パブリックアクセスおよびスピリットホライズン DNS によるインストールまたは拡張のネットワークチェックリスト，85 ページ
- 自動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト，89 ページ
- 手動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト，91 ページ
- WebEx サイト および WebEx 管理のURL，93 ページ
- すべての仮想マシンが内部ネットワークにある場合のポートアクセス，95 ページ
- DMZ ネットワーク内のインターネットリバースプロキシを使用するポートアクセス，95 ページ
- VMware vCenter ポート，102 ページ
- Cisco WebEx Meeting Center ポート，103 ページ
- システムでの NAT の使用，104 ページ
- フォワードプロキシ，107 ページ

自動展開およびパブリックアクセスによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

自動展開では、当社がお客様のためにすべての仮想マシン（管理用仮想マシン以外）を展開いたします。 50、250、または 800 ユーザーのシステムを展開する場合は、必ず自動展開を選択することを推奨します。

- メディア仮想マシン（該当する場合）が、管理用仮想マシンと同じサブネットにあることを確認してください。
- インターネットリバースプロキシの仮想マシンが内部ネットワークにあることを確認します。
- すべての仮想マシン（インターネットリバースプロキシを含む）に対する ESXi ホストが、同じ VMware vCenter から管理されていることを確認します。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
インターネットリバースプロキシの実際の IP アドレス	内部（管理用仮想マシンと同じサブネットにある場合があります）	
管理 URL（システム専用、プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
WebEx サイト URL（システム専用、パブリック VIP アドレスにマッピングされる）	内部（インターネットリバースプロキシと同じサブネット）このIPアドレスは、パブリックからアクセスできる必要があります。	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

説明	ネットワークの場所	IP アドレス
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA インターネットリバースプロキシ（該当する場合）の実際の IP アドレス	内部[プライマリシステムのインターネットリバースプロキシと同じサブネット（ただし、プライベート IP アドレスで NAT を使用する場合がある）]	

DNS の構成

DNS サーバーを以下のようにアップデートします。 WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイトおよび WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名と IP アドレス: 管理用仮想マシンおよびメディア仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
インターネットリバースプロキシ仮想マシンのホスト名と IP アドレス。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
管理サイト URL およびプライベート VIP アドレス。	• <Administration-site-URL> <Private-VIP-address>
WebEx サイト URL およびパブリック VIP アドレス。	• <WebEx-site-URL> <Public-VIP-address>

ファイアウォールの構成

セキュリティ上の理由から、Internet Reverse Proxy を内部（管理およびメディア）仮想マシンとは別のサブネットに配置することを推奨しています。すべての仮想マシンが内部ネットワークにある場合のポートアクセス，（95 ページ）を参照してください。

ネットワークルーティングの設定

タスク	例
内部および DMZ ネットワーク間のレイヤー 3 のルーティングを有効にします	• 内部サブネット<internal-subnet>/24 • DMZ サブネット<DMZ-subnet>/24
パブリック VIP アドレスとインターネットリバースプロキシ仮想マシンが同じサブネット上にあることを確認します。 [全システムの仮想マシンを内部的に展開する場合（インターネットリバースプロキシが DMZ 内にない）、このサブネットは内部ネットワーク内にある必要があります。]	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
プライベート VIP アドレスと内部仮想マシンが同じサブネット上にあることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

手動展開、パブリックアクセスおよびすべての内部仮想マシンによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

手動展開の場合、vSphere クライアントで OVA ウィザードを使用してシステムのすべての仮想マシンを作成します。 その後で手動展開でシステムをインストールします。

2000 ユーザのシステムを展開する場合は、必ず手動展開を選択してください。

- 追加の内部仮想マシン（該当する場合、メディア、ウェブなど）が管理用仮想マシンと同じ内部サブネットにあることを確認します。
- インターネットリバースプロキシの仮想マシンが内部ネットワークにあることを確認します。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
2 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
3 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
ウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
2 番目のウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
インターネットリバースプロキシの実際の IP アドレス	内部（管理用仮想マシンと同じサブネットにある場合があります）	
管理 URL（システム専用、プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
WebEx サイト URL（システム専用、パブリック VIP アドレスにマッピングされる）	内部（インターネットリバースプロキシと同じサブネット） （注） この IP アドレスは、パブリックからアクセスできる必要があります。	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

説明	ネットワークの場所	IP アドレス
HAウェブ仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA インターネットリバースプロキシ（該当する場合）の実際の IP アドレス	内部 - プライマリシステムのインターネットリバースプロキシと同じサブネット（ただし、プライベート IP アドレスで NAT を使用する場合がある）	

DNS の構成

DNS の構成に以下の変更を加えます。

（注） WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイト および WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名とIPアドレスでDNSサーバを更新：管理用仮想マシンとメディアおよびウェブ仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
インターネットリバースプロキシ仮想マシンのホスト名と IP アドレスで DNS サーバを更新します。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
管理サイトの URL とプライベート VIP アドレスの情報を使って、DNS サーバを更新します。	• <Administration-site-URL> <Private-VIP-address>
WebEx サイトの URL とパブリック VIP アドレスの情報を使って、DNS サーバを更新します。	• <WebEx-site-URL> <Public-VIP-address>

ファイアウォールの構成

セキュリティ上の理由から、Cisco では、インターネットリバースプロキシを内部（該当する場合、管理、メディアおよびウェブ）仮想マシンとは別のサブネットに配置することを推奨しています。

推奨されないものの、当社ではすべての仮想マシン（インターネットリバースプロキシおよび内部）を同じサブネットに配置する構成もサポートしています。すべての仮想マシンが内部ネットワークにある場合のポートアクセス，（95 ページ）を参照してください。

ネットワークルーティングの設定

ネットワークルーティングに次の変更を行います。

タスク	これらの IP アドレスを比較する
次の仮想マシンの内部および DMZ ネットワーク間の L3（レイヤー 3 のルーティング）を有効化：管理用仮想マシン、および必要に応じてメディアとウェブ仮想マシン	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
パブリック VIP アドレスとインターネットリバースプロキシ仮想マシンが同じサブネット上にあることを確認します。 （注） 全システムの仮想マシンを内部的に展開する場合（インターネットリバースプロキシが DMZ 内にない）、このサブネットは内部ネットワーク内にある必要があります。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
プライベート VIP アドレスと内部仮想アドレス（管理、メディアおよび、必要に応じてウェブ仮想マシン）が同じサブネット上にあることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

自動展開、パブリックアクセスおよび非スピリットホライズンDNSによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

自動展開では、当社がお客様のためにすべての仮想マシン（管理用仮想マシン以外）を展開いたします。 50、250、または 800 ユーザーのシステムを展開する場合は、必ず自動展開を選択することを推奨します。

- メディア仮想マシン（該当する場合）が、管理用仮想マシンと同じサブネットにあることを確認してください。
- インターネットリバースプロキシの仮想マシンが DMZ ネットワークにあることを確認します。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
インターネットリバースプロキシの実際の IP アドレス	DMZ（ただし、プライベート IP アドレスで NAT を使用する場合がある）	
管理 URL（システム専用、 プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
WebEx サイト URL（システム専用、 パブリック VIPアドレスにマッピングされる）	DMZ（インターネットリバースプロキシと同じサブネット）	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

説明	ネットワークの場所	IP アドレス
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA インターネットリバースプロキシ（該当する場合）の実際の IP アドレス	DMZ [プライマリシステムのインターネットリバースプロキシと同じサブネット（ただし、プライベート IP アドレスで NAT を使用する場合がある）]	

DNS の構成

DNS サーバーを以下のようにアップデートします。 WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイトおよび WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名と IP アドレス: 管理用仮想マシンおよびメディア仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
インターネットリバースプロキシ仮想マシンのホスト名と IP アドレス。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
管理サイト URL およびプライベート VIP アドレス。	• <Administration-site-URL> <Private-VIP-address>
WebEx サイト URL およびパブリック VIP アドレス。	• <WebEx-site-URL> <Public-VIP-address>

ファイアウォールの構成

セキュリティ上の理由から、Internet Reverse Proxy を内部（管理およびメディア）仮想マシンとは別のサブネットに配置することを推奨しています。 すべての仮想マシンが内部ネットワークにある場合のポートアクセス，（95 ページ）を参照してください。

ネットワークルーティングの設定

ネットワークルーティングに次の変更を行います。

タスク	これらの IP アドレスを比較する
内部および DMZ ネットワーク間のレイヤー 3 のルーティングを有効にします	• 内部サブネット<internal-subnet>/24 • DMZ サブネット<DMZ-subnet>/24
パブリック VIP アドレスとインターネットリバースプロキシ仮想マシンが同じサブネット上にあることを確認します。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
プライベート VIP アドレスと内部仮想マシンが同じサブネット上にあることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

手動展開、パブリックアクセスおよび非スピリットホライズンDNSによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

手動展開の場合、vSphere クライアントで OVA ウィザードを使用してシステムのすべての仮想マシンを作成します。 その後で手動展開でシステムをインストールします。

2000 ユーザのシステムを展開する場合は、必ず手動展開を選択してください。

- 追加の内部仮想マシン（該当する場合、メディア、ウェブなど）が管理用仮想マシンと同じ内部サブネットにあることを確認します。

- インターネットリバースプロキシの仮想マシンが DMZ ネットワークにあることを確認します。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
2 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
3 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
ウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
2 番目のウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
インターネットリバースプロキシの実際の IP アドレス	DMZ（ただし、プライベート IP アドレスで NAT を使用する場合がある）	
管理 URL（システム専用、プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
WebEx サイト URL（システム専用、パブリック VIP アドレスにマッピングされる）	DMZ（インターネットリバースプロキシと同じサブネット）	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA ウェブ仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

説明	ネットワークの場所	IP アドレス
HA インターネットリバースプロキシ（該当する場合）の実際の IP アドレス	DMZ—プライマリシステムのインターネットリバースプロキシと同じサブネット（ただし、プライベート IP アドレスで NAT を使用する場合がある）	

DNS の構成

DNS の構成に以下の変更を加えます。

（注） WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイト および WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名と IP アドレスで DNS サーバを更新：管理用仮想マシンとメディアおよびウェブ仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
インターネットリバースプロキシ仮想マシンのホスト名と IP アドレスで DNS サーバを更新します。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
管理サイトの URL とプライベート VIP アドレスの情報を使って、DNS サーバを更新します。	• <Administration-site-URL> <Private-VIP-address>
WebEx サイトの URL とパブリック VIP アドレスの情報を使って、DNS サーバを更新します。	• <WebEx-site-URL> <Public-VIP-address>

ファイアウォールの構成

セキュリティ上の理由から、Cisco では、インターネットリバースプロキシを内部（該当する場合、管理、メディアおよびウェブ）仮想マシンとは別のサブネットに配置することを推奨しています。DMZ ネットワーク内のインターネットリバースプロキシを使用するポートアクセス，（95 ページ）を参照してください。

ネットワークルーティングの設定

ネットワークルーティングに次の変更を行います。

タスク	これらの IP アドレスを比較する
次の仮想マシンの内部および DMZ ネットワーク間の L3（レイヤー 3 のルーティング）を有効化：管理用仮想マシン、および必要に応じてメディアとウェブ仮想マシン	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
パブリック VIP アドレスとインターネットリバースプロキシ仮想マシンが同じサブネット上にあることを確認します。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
プライベート VIP アドレスと内部仮想アドレス（管理、メディアおよび、必要に応じてウェブ仮想マシン）が同じサブネット上にあることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

自動展開、パブリックアクセスおよびスピリットホライズンDNSによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

自動展開では、当社がお客様のためにすべての仮想マシン（管理用仮想マシン以外）を展開いたします。 50、250、または 800 ユーザーのシステムを展開する場合は、必ず自動展開を選択することを推奨します。

- メディア仮想マシン（該当する場合）が、管理用仮想マシンと同じサブネットにあることを確認してください。
- インターネットリバースプロキシの仮想マシンが DMZ ネットワークにあることを確認します。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
インターネットリバースプロキシの実際の IP アドレス	DMZ（ただし、プライベート IP アドレスで NAT を使用する場合がある）	
管理 URL（システム専用、 プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
WebEx サイト URL（システム専用、 2 つのVIPアドレスのマップ）： • 内部ユーザ—プライベート VIP アドレス • 外部ユーザ—パブリック VIP アドレス	• 内部ユーザ—内部（管理用仮想マシンと同じサブネット） • 外部ユーザ—DMZ（インターネットリバースプロキシと同じサブネット）	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

説明	ネットワークの場所	IP アドレス
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA インターネットリバースプロキシ（該当する場合）の実際の IP アドレス	DMZ [プライマリシステムのインターネットリバースプロキシと同じサブネット（ただし、プライベート IP アドレスで NAT を使用する場合がある）]	

DNS の構成

DNS サーバーを以下のようにアップデートします。 WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイトおよび WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名と IP アドレス: 管理用仮想マシンおよびメディア仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
DMZ 仮想マシンのホスト名と IP アドレス:	• <IRP-vm-FQDN> <IRP-vm-IP-address>
WebEx サイト URL、管理サイト URL、およびプライベート VIP アドレス 情報。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
WebEx サイト URL およびパブリック VIP アドレス。	• <WebEx-site-URL> <Public-VIP-address>

ファイアウォールの構成

セキュリティ上の理由から、Internet Reverse Proxy を内部（管理およびメディア）仮想マシンとは別のサブネットに配置することを推奨しています。 すべての仮想マシンが内部ネットワークにある場合のポートアクセス，（95 ページ）を参照してください。

ネットワークルーティングの設定

ネットワークルーティングに次の変更を行います。

タスク	これらの IP アドレスを比較する
内部および DMZ ネットワーク間のレイヤー 3 のルーティングを有効にします	• 内部サブネット<internal-subnet>/24 • DMZ サブネット<DMZ-subnet>/24
パブリック VIP アドレスとインターネットリバースプロキシ仮想マシンが同じサブネット上にあることを確認します。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
プライベート VIP アドレスと内部仮想マシンが同じサブネット上にあることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

手動展開、パブリックアクセスおよびスピリットホライズンDNSによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

手動展開の場合、vSphere クライアントで OVA ウィザードを使用してシステムのすべての仮想マシンを作成します。 その後で手動展開でシステムをインストールします。

2000 ユーザのシステムを展開する場合は、必ず手動展開を選択してください。

- 追加の内部仮想マシン（該当する場合、メディア、ウェブなど）が管理用仮想マシンと同じ内部サブネットにあることを確認します。

- インターネットリバースプロキシの仮想マシンが DMZ ネットワークにあることを確認します。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
2 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
3 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
ウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
2 番目のウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
インターネットリバースプロキシの実際の IP アドレス	DMZ（ただし、プライベート IP アドレスで NAT を使用する場合がある）	
管理 URL（システム専用、プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
WebEx サイト URL（システム専用、2 つの VIP アドレスのマップ） • 内部ユーザ—プライベート VIP アドレス • 外部ユーザ—パブリック VIP アドレス	• 内部ユーザ—内部（管理用仮想マシンと同じサブネット） • 外部ユーザ—DMZ（インターネットリバースプロキシと同じサブネット）	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

説明	ネットワークの場所	IP アドレス
HAウェブ仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA インターネットリバースプロキシ（該当する場合）の実際の IP アドレス	DMZ—プライマリシステムのインターネットリバースプロキシと同じサブネット（ただし、プライベート IP アドレスで NAT を使用する場合がある）	

DNS の構成

DNS の構成に以下の変更を加えます。

（注） WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイト および WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名とIPアドレスでDNSサーバ （内部検索用） を更新： 管理用仮想マシンとメディアおよびウェブ仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
DMZ仮想マシン用ホスト名とIPアドレスでDNSサーバ（内部検索用）を更新します。	• <IRP-vm-FQDN> <IRP-vm-IP-address>
WebExサイトURL、管理サイトURL、プライベート VIP アドレス情報で DNS サーバ（内部検索用）を更新します。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

タスク	例
WebExサイトURL、パブリック VIP アドレス情報でDNSサーバ（外部検索用）を更新します。	• <WebEx-site-URL> <Public-VIP-address>

ファイアウォールの構成

セキュリティ上の理由から、Cisco では、インターネットリバースプロキシを内部（該当する場合、管理、メディアおよびウェブ）仮想マシンとは別のサブネットに配置することを推奨しています。DMZ ネットワーク内のインターネットリバースプロキシを使用するポートアクセス，（95 ページ）を参照してください。

ネットワークルーティングの設定

ネットワークルーティングに次の変更を行います。

タスク	これらの IP アドレスを比較する
次の仮想マシンの内部および DMZ ネットワーク間の L3（レイヤー 3 のルーティング）を有効化：管理用仮想マシン、および必要に応じてメディアとウェブ仮想マシン	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
パブリック VIP アドレスとインターネットリバースプロキシ仮想マシンが同じサブネット上にあることを確認します。	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
プライベート VIP アドレスと内部仮想マシン（管理、メディア、ウェブなど）が同じサブネットになっていることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

自動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

自動展開では、当社がお客様のためにすべての仮想マシン（管理用仮想マシン以外）を展開いたします。 50、250、または 800 ユーザーのシステムを展開する場合は、必ず自動展開を選択することを推奨します。

メディア仮想マシン（該当する場合）が、管理用仮想マシンと同じサブネットにあることを確認してください。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
管理 URL（システム専用、 プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA インターネットリバースプロキシ（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

DNS の構成

DNS サーバーを以下のようにアップデートします。 WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイトおよび WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名と IP アドレス: 管理用仮想マシンおよびメディア仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
WebEx サイト URL、管理サイト URL、およびプライベート VIP アドレス 情報。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

ファイアウォールの構成

タスク	例
内部ネットワーク内のすべてのファイアウォールを構成し、ウェブブラウザがプライベート VIP アドレスにアクセスできるようにします。	HTTP <Private-VIP-address>:80 HTTP <Private-VIP-address>:443

ネットワークルーティングの設定

タスク	これらの IP アドレスを比較する
プライベート VIP アドレスと内部仮想マシンが同じサブネット上にあることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

手動展開および非パブリックアクセスによるインストールまたは拡張のネットワークチェックリスト

仮想マシンの展開

手動展開の場合、vSphere クライアントで OVA ウィザードを使用してシステムのすべての仮想マシンを作成します。 その後で手動展開でシステムをインストールします。

2000 ユーザのシステムを展開する場合は、必ず手動展開を選択してください。

- 追加の内部仮想マシン（該当する場合、メディア、ウェブなど）が管理用仮想マシンと同じ内部サブネットにあることを確認します。

必要な IP アドレス

説明	ネットワークの場所	IP アドレス
管理用仮想マシンの実際の IP アドレス	内部	
メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（管理用仮想マシンと同じサブネット）	
2 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
3 番目のメディア仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
ウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
2 番目のウェブ仮想マシンの実際の IP アドレス（2,000 ユーザのシステムのみ）	内部（管理用仮想マシンと同じサブネット）	
管理 URL（システム専用、プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
WebEx サイト URL（システム専用、プライベート VIP アドレスにマッピングされる）	内部（管理用仮想マシンと同じサブネット）	
HA 管理用仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	
HA メディア仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

説明	ネットワークの場所	IP アドレス
HAウェブ仮想マシン（該当する場合）の実際の IP アドレス	内部（プライマリシステムの管理用仮想マシンと同じサブネット）	

DNS の構成

DNS の構成に以下の変更を加えます。

（注） WebEx サイト URL と管理サイト URL のホスト名の部分には一部の制限があります。 使用できない単語のリストについては、WebEx サイト および WebEx 管理のURL, （93 ページ）を参照してください。

タスク	例
内部仮想マシンのホスト名とIPアドレスでDNSサーバ （内部検索用） を更新： 管理用仮想マシンとメディアおよびウェブ仮想マシン（該当する場合）。	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
管理サイトの URL、WebEx サイトの URL、プライベート VIP アドレスの情報を使って、DNS サーバを更新します。	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

ファイアウォールの構成

ファイアウォールの構成に次の変更を行います。

タスク	例
内部ネットワーク内のすべてのファイアウォールを構成し、ウェブブラウザがプライベート VIP アドレスにアクセスできるようにします。	• HTTP <Private-VIP-address>:80 • HTTP <Private-VIP-address>:443

ネットワークルーティングの設定

ネットワークルーティングに次の変更を行います。

タスク	これらの IP アドレスを比較する
プライベート VIP アドレスと内部仮想アドレス（管理、メディアおよび、必要に応じてウェブ仮想マシン）が同じサブネット上にあることを確認します。	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

WebEx サイト および WebEx 管理のURL

WebEx サイトの URL

ユーザーはこの WebEx サイト URL にアクセスしてミーティングをスケジュール、開催あるいは出席します。 この URL は、スプリットホライズン DNS の使用の有無によって、プライベート VIP アドレスまたはパブリック仮想 IP アドレスの名前解決が行われます。

- 「スプリットホライズン」DNS を所有していない場合、すべてのユーザーに対してパブリック VIP アドレスに名前解決されます。
- 「スプリットホライズン」DNSを所有している場合、外部ユーザに対してパブリック VIP アドレスに名前解決されます。
- 「スプリットホライズン」DNS を所有している場合、内部ユーザに対してプライベート VIP アドレスに名前解決されます。

（注） ポート 80 および 443 は WebEx サイト URL に対しオープンである必要があります。

WebEx 管理 URL

管理者は WebEx 管理 URL にアクセスしてシステムの構成、管理、監視を行います。 この URL はプライベート仮想 IP アドレスに名前解決されます。

（注） ポート 80 および 443 は WebEx Administration URL に対しオープンである必要があります。

WebEx サイトおよび WebEx 管理のURLに対する名前

これらのURLに対し、すべて小文字から成る名前をほとんど何でも選択できます。 ただし、URLには、以下をホスト名に使用できません。

- システムを構成する仮想マシンと同じホスト名
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld。
- version
- WBXService
- webex

すべての仮想マシンが内部ネットワークにある場合のポートアクセス

このセクションでは、内部ネットワークにすべてのシステム仮想マシン（管理、および該当する場合はメディア、ウェブ、インターネットリバースプロキシ）がある場合、外部のファイアウォールで必要となるポートアクセスを説明します。 これは、内部インターネットリバースプロキシネットワークトポロジです。 (Cisco WebEx Meeting Center ポート，（103 ページ）を参照。)

ファイアウォールまたは下に一覧されるポートへのロードバランシングソリューションリダイレクト要求によりエンドユーザがミーティングの主催および参加をできることを確認します。

- パブリック仮想 IP （VIP）アドレスに TCP ポート 80
- パブリック仮想 IP （VIP）アドレスに TCP ポート 443

（注） ウェブノードと管理ノードは設定したメールサーバーにSMTP要求を送信します。 社内のウェブ仮想マシン、管理仮想マシンとメールサーバー間にファイアウォールがある場合は、SMTPトラフィックがブロックされる場合があります。 メールサーバーの設定とメール通知を適切に動作させるために、ポート25、または465（安全なSMTPポート番号）がメールサーバーとウェブ仮想マシン、管理仮想マシンとの間で開いていることを確認する必要があります。

外部ファイアフォールのポートアクセス

パグリックアクセスが有効な場合は、インターネットから内部ネットワークのインターネットリバースプロキシ仮想マシンへの直接受信用に以下のポートを開きます。

DMZネットワーク内のインターネットリバースプロキシを使用するポートアクセス

このセクションでは、内部ネットワークに内部仮想マシン（管理、メディアおよびウェブ（該当する場合））があり、DMZ ネットワークにインターネットリバースプロキシ（IRP）がある場合の、内部および外部のファイアウォールで必要となるポートアクセスを説明します。 (Cisco WebEx Meeting Center ポート，（103 ページ）を参照。)

システムの仮想マシン用のESXiホストへのトラフィックを許可するアクセス制御リスト（ACL）を設定します。

外部ファイアフォールのポートアクセス

ポート 443（HTTPS）に加えてポート 80 （HTTP）を開くことでパブリックアクセスが有効になり、ユーザーは WebEx サイト URL をそれが HTTP か HTTPS かを覚える必要なく入力できます。ポート 80 が開いていても、ずべてのネットワークトラフィックがポート 443 を介して流れます（SSL 暗号化 HTTPS）。

重要 ファイアウォールまたは下に一覧されるポートへのロードバランシングソリューションリダイレクト要求によりエンドユーザーがミーティングの主催および参加をできることを確認します。

制約事項 パブリック VIP アドレスに到達するすべてのリクエストを拒否するように、IRP マシンの TCP ポート 64700 を設定します。 外部ファイアウォールでは、このポートへのアクセスを管理仮想マシンからのリクエストのみに制限します。

プロトコル	ポート	ソース	移動先	必要な理由
TCP	443	外部クライアント	IRP のパブリック VIP（Eth1）	外部クライアントが HTTPS を使用して WebEx サイト URL にアクセスします。外部クライアントマシンから IRP 仮想マシンに対して、TCP 接続が開始されます。
TCP	80	外部クライアント	IRP のパブリック VIP（Eth1）	HTTP を使って WebEx サイト URL にアクセスする外部クライアント。外部クライアントマシンから IRP 仮想マシンに対して、TCP 接続が開始されます。

プロトコル	ポート	ソース	移動先	必要な理由
TCP	8444 （2.5MR1、2.6、および2.0MR6HFで導入されました。）	外部クライアント	IRP のパブリック VIP（Eth1）	HTTPS を使って WebEx 録画にアクセスする外部クライアント。外部クライアントマシンから IRP 仮想マシンに対して、TCP 接続が開始されます。
UDP	53	IRP の実 IP（Eth0）	DNSサーバー	仮想マシンと DNS サーバの間にファイアウォールがある場合、システムが正常に展開され、動作するためには、これが必要です。

内部ファイアウォールのポートアクセス

内部ネットワークからDMZネットワークへの接続に制限がある場合は、次の表が適用されます。Allow TCP 接続送信 を内部ネットワークから DMZ ネットワークセグメント。

（注） 本製品が正しく動作するためには、DMZ セグメントから内部ネットワークへのTCP 接続を許可する必要はありません。

（注） iptables またはアクセス制御リスト（ACL）を使用して、ポート 64616 への接続が管理用仮想マシンからのみになるように、ファイアウォールを構成します。

（注） ウェブノードと管理ノードは設定したメールサーバーにSMTP要求を送信します。 社内のウェブ仮想マシン、管理仮想マシンとメールサーバー間にファイアウォールがある場合は、SMTP トラフィックがブロックされる場合があります。 メールサーバーの設定とメール通知を適切に動作させるために、ポート25、または465（安全なSMTPポート番号）がメールサーバーとウェブ仮想マシン、管理仮想マシンとの間で開いていることを確認する必要があります。

（注） 特に IRP が DMZ ネットワークにある場合、Internet Control Message Protocol (ICMP) echo のリクエストとリプライを許可します。そうでない場合は、もしICMPエコーリプライが受信されなければ、IRP 検出および DNS サーバー到達可能性確認は失敗する可能性があります。

プロトコル	ポート	ソース	移動先	必要な理由
TCP	64001	すべての内部仮想マシン（Eth0 IP）	IRP 仮想マシンの実 IP（Eth0）	IRP との逆接続を確立します。 TCP 接続は内部仮想マシンから IRP 仮想マシンで直接確立されます。
TCP	64002	管理およびウェブ用仮想マシン（Eth0 IP）	IRP 仮想マシンの実 IP（Eth0）	IRP との逆接続を確立します。 TCP 接続は内部仮想マシンから IRP 仮想マシンで直接確立されます。
TCP	7001	すべての内部仮想マシン（Eth0 IP）	IRP 仮想マシンの実 IP（Eth0）	IRP との逆接続を確立します。 TCP 接続は内部仮想マシンから IRP 仮想マシンで直接開始されます。

プロトコル	ポート	ソース	移動先	必要な理由
TCP	64616	管理用仮想マシン（Eth0 IP）	IRP 仮想マシンの実 IP（Eth0）	IRP に Bootstrap を使用します。 TCP 接続は管理用仮想マシンから IRP 仮想マシンで直接開始されます。 （注） iptables またはアクセス制御リスト（ACL）を使用して、ポート 64616 への接続が管理用仮想マシンからのみになるように、ファイアウォールを構成します。

プロトコル	ポート	ソース	移動先	必要な理由
TCP	64700	管理用仮想マシン（Eth0 IP）	IRP 仮想マシンの実 IP（Eth0）	IRP のログを収集します。 TCP 接続は管理用仮想マシンから IRP 仮想マシンで直接開始されます。 すべての Cisco WebEx Meetings Server 仮想マシンにおけるこのポートへのアクセスをファイアウォールルールで他の Cisco WebEx Meetings Server 仮想マシンのみに制限します。
TCP	22	任意の内部クライアントマシン。	IRP 仮想マシンの実 IP（Eth0）	リモートサポートアカウントを使用して IRP 仮想マシンの障害対応を行ないます。
TCP	443	任意の内部クライアントマシン。	管理用仮想マシンのプライベート VIP（Eth1） メディア仮想マシンの実 IP（Eth0）	HTTPS を使用して WebEx サイト URL にアクセスする内部ユーザー。 TCP 接続は内部クライアントマシンから管理用仮想仮想マシンで確立されます。
TCP	443	管理仮想マシンのプライベート VIP (Eth1) とメディア仮想マシンのリアル IP （Eth0）。	IRP のパブリック VIP（Eth1）	

プロトコル	ポート	ソース	移動先	必要な理由
TCP	65002	任意の内部クライアントマシン。	内部仮想マシン。	仮想マシン間のネットワークトラフィックをコントロールする。
TCP	65102	任意の内部クライアントマシン。	内部仮想マシン。	仮想マシン間のネットワークトラフィックをコントロールする。
TCP	80	任意の内部クライアントマシン。	管理用仮想マシンのプライベートVIP（Eth1）	http を使用して WebEx サイト URL にアクセスする内部ユーザー。TCP 接続は内部クライアントマシンから管理用仮想仮想マシンで確立されます。
UDP	53	すべての内部仮想マシン（Eth0 IP）	DNSサーバー	仮想マシンと DNS サーバーの間にファイアウォールがある場合、システムが正常に展開され、動作するためには、これが必要です。
TCP	8443	Cisco WebEx Meetings Server ウェブノード	CUCM	LDAP CUCM フェイルオーバーを可能にする、Cisco WebEx Meetings Server および CUCM 間のマルチデータセンターシステムにおける AXL トラフィック。

プロトコル	ポート	ソース	移動先	必要な理由
TCP	8444	録画ファイルのダウンロードで使用される Cisco WebEx ミーティングサーバー Web ノード	管理用仮想マシンのプライベート VIP（Eth1） メディア仮想マシンの実 IP（Eth0）	HTTPS を使用して WebEx サイト URL にアクセスする内部ユーザー。TCP 接続は内部クライアントマシンから管理用仮想仮想マシンで確立されます。

VMware vCenter ポート

展開時に開放されるポート

これらは、シングルデータセンター(SDC) Cisco WebEx Meetings Server (CWMS) の展開中に使用されるポートの一部です。 展開が完了すると、展開のみのために開いたポートを閉じることができます。

自動的なシステム展開中での安全な https 管理のために、TCP ポート 443 は vCenter と管理仮想マシンの間で両方向に開いておく必要があります。 管理仮想マシンはこのポートを使用して、vCenter 資格情報を指定して、vCenter で仮想マシンを自動的に展開します。

これらのリストされているポートは、ESXi ホストと vCenter 間の通信に使用されます。 ESXi ホストおよびvCenterが別の管理ネットワークに接続している場合は、ファイアウォールを通してこれらのポートを開く必要がない場合があります。 vCenter と ESXi ホストで使用するポートの完全なリストについては、VMware の資料を参照してください。

- UDP/TCP ポート 902、vCenter 管理用に vCenter と ESXi 間の両方向
- （オプション）TCP ポート 22、SSH 管理用に vSphere クライアントから ESXi ホストまで
- UDP ポート 514、システムの ESXi ホストから内部 syslog まで
- TCP ポート 5989、XML 管理用に vCenter と ESXi 間の両方向

音声とビデオデータ転送の外部クライアントに使用されるデフォルト UDP ポートは、SSL（ポート 443）です。

マルチデータセンターをサポートするために開放されるポート

内部マシン間で開放されるポート	tcp 8080 tcp 8081 tcp 8082 tcp 9809 tcp 9810 tcp 9811 tcp 9812 tcp 9813 tcp 9814 tcp 9815 tcp 9816 tcp 9817 tcp 9818 tcp 9819 tcp 9820 tcp 9840 tcp 6502 tcp 12340 tcp 12342 tcp 12442 tcp 7001 tcp 7003 tcp 7004 tcp 7005 tcp:5060 tcp 5061 tcp 5062 tcp 5063 tcp 22
内部マシンと仮想 IP の間で開放されるポート	tcp 443 tcp 80
Internet Reverse Proxy IP と内部マシンの間で開放されるポート	tcp 7001 tcp 64001 tcp 64700 tcp 64616
内部マシン間で開放される UDP ポート	udp 範囲:10000:19999 udp 範囲:16000:32000 udp 範囲:9000:9009 udp 5060 udp 5062

Cisco WebEx Meeting Center ポート

これらのポートは、Cisco WebEx Meeting Center と Cisco WebEx Meetings Server の間の通信に使用されます。

- UDP と SSL 間の音声とビデオデータの送信のために、社内クライアントに使用される UDP ポートには次のものがあります。
  - 50 ユーザーシステムの場合、UDP ポート 9000 を使用します
  - 250 ユーザーシステムの場合、UDP ポート 9000、9001、9002、9003 を使用します

- 800 ユーザーシステムの場合、UDP ポート 9000、9001、9002、9003、9004、9005、9006、9007、9008、9009 を使用します
- 2000 ユーザーシステムの場合、UDP ポート 9000、9001、9002、9003、9004、9005、9006、9007 を使用します

- 適切なネットワーク設定により、社内メディアサーバーは、Meeting Center で使用される任意のポートを通じて接続を行うことができます。
- インターネットリバースプロキシは、TCP ポート 80 と 443 を通じて Meeting Center からのみ接続を受け付けます。
- Web ノードから CUCM への AXL トラフィックはポート 8443 を通って渡されます。(CUCM を使った AXL ウェブサービスとディレクトリ同期の設定を参照。)

システムでの NAT の使用

Cisco は本製品のシステムで使用する仮想マシンIPアドレスおよび仮想IPアドレス（パブリックおよびプライベートVIP）に対するネットワークアドレス変換（NAT）トラバースをサポートしています。

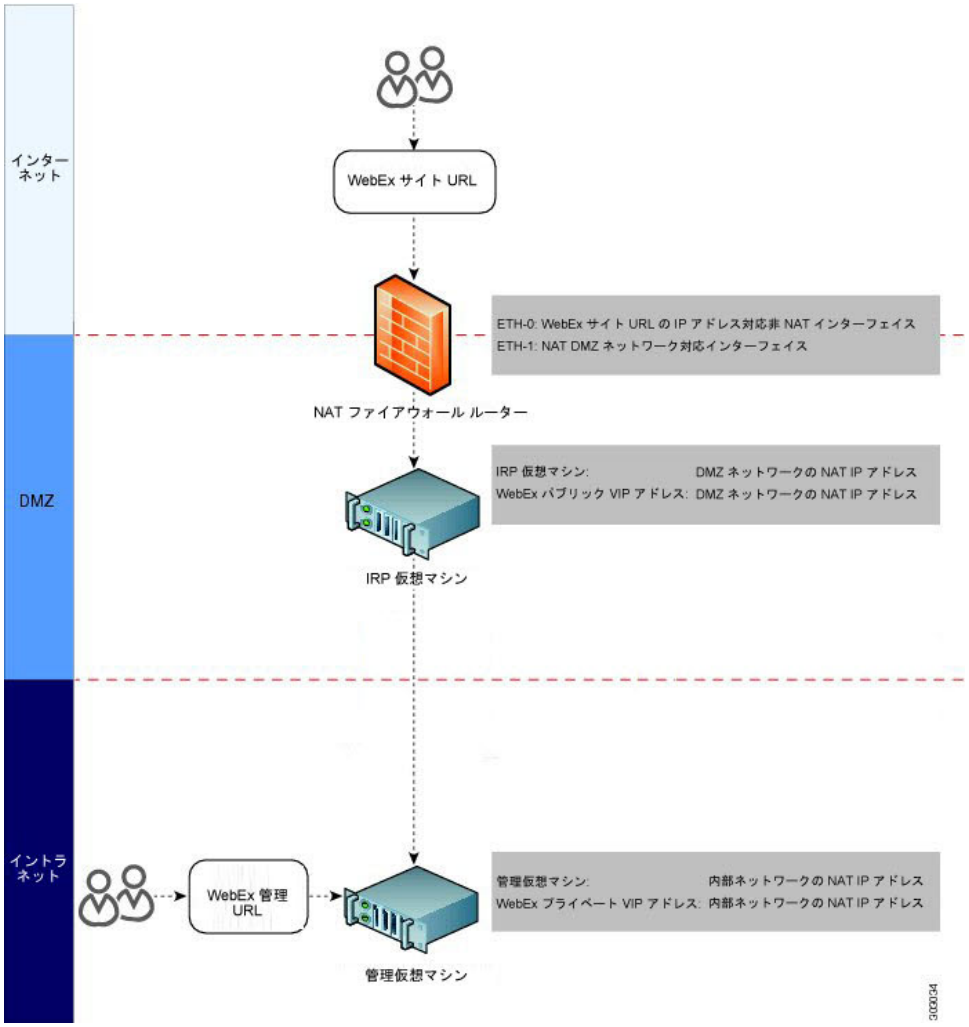
次の系統図は、High Availability（HA）のない 50 ユーザーシステムの一般的なNATトラバースを示しています。 NAT を使用することにより、製品に必要なパブリック *IP* アドレスの数を、2つ（HA が配備されている場合は 3 つ）から 1 つに減らすことができます。 全体的なシステム要件を満たしていれば、同様の NAT も展開することができます。

重要 複数のNATとファイアウォールの使用は、遅延を増加させ、ユーザのリアルタイムトラフィックの品質を劣化させる傾向にあります。

また、複数の NAT ドメインを使用するときに、これらの種々の NAT ドメインの間でルーティングすることには課題があります。 以下の要件が満たされる限り、NAT IP アドレスを使用できます。

- システムの仮想マシンはすべて、NAT-ed IP アドレスを使用できますが、Internet Reverse Proxy 仮想マシンは例外です。 管理用仮想マシンと Internet Reverse Proxy 仮想マシンとの間の NAT はサポートされません。 Internet Reverse Proxy 仮想マシン IP アドレス（実際の IP アドレス）は、内部ネットワークの管理用仮想マシンにより到達するものである必要があります。
- パブリック VIP アドレス自体は公開する必要はありませんが、インターネットから変換可能でなければなりません。
- 公開アクセスを展開するとき、WebEx サイト URL はインターネットで公開された IP アドレスにマップされることが必要です。 このインターネットで見える IP アドレスは、外部ユーザによりアクセス可能で、システム展開中に設定するパブリック VIP アドレスにマップ可能にもする必要があります。

  パブリック VIP アドレスをインターネットから見えるようにすることもできます。 パブリック VIP アドレスをインターネットで見えないようにする場合、インターネットから変換可能でなければなりません。



図では、外部ユーザが WebEx サイトにアクセスして、ミーティングの主催または参加しています。 DNS ルックアップ後に、WebEx サイトの IP アドレスは NAT パブリック IP アドレス（Eth0）です。 この NAT パブリック IP アドレスは、外部ネットワークと DMZ ネットワーク間の外部 NAT ファイアウォールルータ（ファイアウォールと NAT ルータ 1）です。

ファイアウォールルーターは外部ユーザからこの要求を受け取り、要求を内部的にルーターのNAT プライベート IP アドレス（DMZ ネットワークから見える Eth1）に送ります。 その後、Eth1 はパブリック VIP アドレス（WebEx サイトのプライベートネットワーキングセグメントの NAT IP アドレスでもある）にリクエストを送信します。

NAT IP アドレスは、パブリック VIP アドレスおよびインターネットリバースプロキシ IP アドレスに使用できます。 唯一の NAT パブリック IP アドレスは、NAT ファイアウォール ルーターの Eth0 IP アドレスです。

（注） この NAT ファイアウォール ルーター（インターネットと DMZ ネットワークの間）が受信パケットを正しくルートすることを保証するためには、NAT デバイスでポートマッピング設定をセットするか、同様のメカニズムを適用して、パケットが正しくパブリック VIP アドレスおよびインターネットリバースプロキシにルートしてください。

通常、DMZネットワークと内部ネットワークの間に第 2 内部NATファイアウォールルーターが設置されます。 外部 NAT ファイアウォールルーターと同様に、Eth0 はDMZ NAT プライベート IP アドレスであり、DMZ ネットワークのインタフェースです。 Eth1は、内部ネットワークへのインタフェースである NAT プライベート IP アドレスです。

NAT IP アドレスはプライベート VIP アドレスおよび管理用仮想マシンの IP アドレスに使用できます。

NAT の詳細は、http://www.cisco.com/c/en/us/tech/ip/ip-addressing-services/tech-tech-notes-list.html を参照してください。

フォワードプロキシ

使用しているネットワークのトポロジにフォワードプロキシが含まれている場合、インターネットリバースプロキシが正しく動作するように、固有の要件を満たす必要があります。 詳細については『*Cisco WebEx Meetings Server* トラブルシューティングガイド』の「システムでのフォワードプロキシの使用」を参照してください。

第 5 章

Cisco Unified Communications Manager（CUCM）の設定

Cisco WebEx Meetings Server で電話会議を有効にするには、1 つ (または複数) の Cisco Unified Communications Manager (CUCM) システムを構成して発信制御を管理する必要があります。 任意で、音声の高可用性のために、第 2 の CUCM システムを構成できます。

- MDC 環境での CUCM，110 ページ
- 開始する前に，110 ページ
- MDC 環境の CUCM 安全電話会議，111 ページ
- マルチデータセンターの CUCM 構成チェックリスト，111 ページ
- 高可用性を含む、または含まない CUCM 構成チェックリスト，112 ページ
- CWMS マルチデータセンターシステムでの CUCM の構成，113 ページ
- 高可用性と非高可用性システムの CUCM の設定，116 ページ
- SIP トランクセキュリティプロファイルの設定，121 ページ
- SIP プロファイルの設定，123 ページ
- TLS を使用する CUCM 証明書管理，124 ページ
- SIP トランクの設定，131 ページ
- ルートグループの設定，134 ページ
- ルートリストの設定，135 ページ
- ルートパターンの設定，136 ページ
- SIP ルートパターンの設定，137 ページ
- CUCM 機能の互換性とサポート，137 ページ

MDC 環境での CUCM

マルチデータセンター (MDC) 環境中の CUCM 構成はシングルデータセンター (SDC) 環境と同じです。 1 つのデータセンターで修正された構成パラメータは、他のデータセンター上で自動的に照合されます。

CUCM では、マルチデータセンター (MDC) 環境中の基本構成はシングルデータセンター (SDC) 環境と同じです。 ただし、すべてのデータセンターに対しトランクを構成する必要があります。 各データセンターは異なるルートパターンを持つことができます。 複数の CUCM を使用する場合、各データセンターは発信を転送するために、他のデータセンター内の CUCM に対する SIP トランクを持つ必要があります。

開始する前に

ロードバランサポイントとアプリケーションポイントの情報を Cisco Meetings Server の [**音声**] ページから取得してください。 ロードバランサポイントはコールロードバランシングを管理し、アプリケーションポイントはコール、会議の流れ、および機能のコントロールを管理します。 システムのサイズが異なると、ロードバランサポイントとアプリケーションポイントの数も異なり、数はカスタマイズされません。 管理サイトにサインインして、[設定] >>[音声] を選択して、この情報を表示します。

- サイズ（50/250/800/2000）
- 高可用性
- 転送タイプ

[**音声**] ページには、IP アドレスとポートを含むロードバランサポイントとアプリケーションポイントの情報を表示する SIP 設定表があります。 この表はまた、音声設定をはじめて行うときに表示される [**はじめての音声設定の構成**] ページにも表示されます。

CUCM が Cisco WebEx Meetings Server で機能するようにするために、CUCM は以下の基本構成と詳細構成を必要とします。

- 基本構成

（注） これらの構成は、複数の Cisco WebEx Meetings Server システムと共有できます。

  - SIP トランクセキュリティプロファイル
  - SIP プロファイル

- 特定の構成

（注） これらの構成は、個々の Cisco WebEx Meetings Server システムに対して行うことができ、複数のシステムでは共有できません。

- 証明書の管理
- SIP トランク
- ルートグループ
- ルートリスト
- ルートパターン
- SIP ルートパターン

MDC 環境の CUCM 安全電話会議

両証明書の共通名が同一のとき、電話会議 () の安全を保証するために必要に応じて、証明書をマルチデータセンター (MDC) 内のすべてのデータセンターから単一の Cisco Unified Call Manager (CUCM) へインポートすることはできません。

デフォルトでは、すべてのデータセンターの共通名は、システムのグローバルサイト URL です。しかし、共通名を独自にするには、 バージョン2.6 以上には 証明書署名リクエスト（CSR）バージョン 2.6 以降の生成, （127 ページ）を使って、またはバージョン2.5 以前には 証明書署名リクエスト（CSR）バージョン 2.5 以前の生成, （129 ページ） を使って証明書を生成できます。 グローバルサイト URL ではなくローカルサイト URL を共通名に使用してください。

システムの変更手続中 (サイトまたは管理 URL の変更、ホスト名の変更など) に生成された自己署名証明書では、共通名にグローバルサイト URL があるため、このタイプの操作が終わったら、ローカルサイト URL を含む証明書を手動で作成する必要があります。

マルチデータセンターの CUCM 構成チェックリスト

構成チェックリストは、マルチデータセンター (MDC) のシステムに対して構成する必要がある、各 Cisco Unified Communication Manager (CUCM) 構成の数を表示します。

システムサイズ	セキュリティプロファイル（基本構成）	SIP プロファイル（基本構成）	SIP トランク（固有の設定）	ルートグループ（特定の構成）	ルートリスト（特定の構成）	ルートパターン（特定の構成）	SIP ルートパターン（特定の構成）
250 ユーザ	2	1	4	1	1	いいえ	2
800 ユーザ	2	1	4	1	1	いいえ	2

システムサイズ	セキュリティプロファイル（基本構成）	SIP プロファイル（基本構成）	SIP トランク（固有の設定）	ルートグループ（特定の構成）	ルートリスト（特定の構成）	ルートパターン（特定の構成）	SIP ルートパターン（特定の構成）
2000 ユーザー、HA あり	2	1	6	1	1	いいえ	4

高可用性を含む、または含まない CUCM 構成チェックリスト

構成チェックリストは、 高可用性 (HA) を含む、または含まないシングルデータセンター (SDC) システムに対して構成する必要がある、各 Cisco Unified Communication Manager (CUCM) 構成の数を表示します。

システムサイズ	セキュリティプロファイル（基本構成）	SIP プロファイル（基本構成）	SIP トランク（固有の設定）	ルートグループ（特定の構成）	ルートリスト（特定の構成）	ルートパターン（特定の構成）	SIP ルートパターン（特定の構成）
50 ユーザ	2	1	2	1	1	いいえ[21]	1
50 ユーザー、HA あり	2	1	4	1	1	いいえ	2
250 ユーザ	2	1	2	1	1	いいえ	1
250 ユーザー、HA あり	2	1	4	1	1	いいえ	2
800 ユーザ	2	1	2	1	1	いいえ	1
800 ユーザー、HA あり	2	1	4	1	1	いいえ	2
2000 ユーザ	2	1	5	1	1	いいえ	3

システムサイズ	セキュリティプロファイル（基本構成）	SIP プロファイル（基本構成）	SIP トランク（固有の設定）	ルートグループ（特定の構成）	ルートリスト（特定の構成）	ルートパターン（特定の構成）	SIP ルートパターン（特定の構成）
2000 ユーザー、HA あり	2	1	6	1	1	いいえ	4

[21] N は、Cisco WebEx Meetings Server で設定するコールインアクセス番号の数です。

CWMS マルチデータセンターシステムでの CUCM の構成

通常、マルチデータセンター (MDC) 環境中の各サイトには、関連付けられた専用の CUCM クラスタがあります。 CUCM クラスタはクラスタ間トランク (ICT) を使用することで接続されます。各 CUCM クラスタにはローカル CWMS サイトに対するコールイン/インダイヤルのトランクがあります。 Session Manager Edition (SME) に対応しています。 CWMS はローカル CUCM クラスタの背後で構成できます。 各 CUCM には、MDC 中のメディア仮想マシンすべてに対する SIP REFER トランクがあります。

冗長性のため、各 CUCM クラスタにはすべてのデータセンターに対する INVITE トランクを含めることができます。 コールインルートパターンは、ローカルデータセンターに関連付けられた INVITE トランクに優先権を与え、障害発生時だけ、リモートデータセンターに対する INVITE トランクを使用します。

表 *4*：各 *CUCM* クラスタで構成された *CUCM SIP* トランク

配備	INVITE トランク　ロードバランサ (MACC)	REFER トランク—アプリケーションポイント (TAS)
小さく	2	2
標準	2	2
大きく	4	6

200または800ユーザーのマルチデータセンターシステムにおけるCUCMの構成

250 または 800 ユーザーマルチデータセンターシステムのためにCisco Unified Communications Manager (CUCM) を設定します。 通常、各データセンターにはローカル CUCM クラスタがあります。

はじめる前に

必要な情報

- 各データセンターに対し、1 つのロードバランスポイント IP アドレス
- 各データセンターに対し、1 つのアプリケーションポイント IP アドレス
- システムで構成するコールインアクセス番号の数

ステップ 1 既存の SIP トランクセキュリティプロファイルを確認し、それが Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを決定します。 それが要件を満たしていない場合、2 つの SIP トランクセキュリティプロファイルを設定してください。
使用中のロードバランスポイントに SIP トランクセキュリティプロファイルを追加し、アプリケーションポイントに SIP トランクセキュリティプロファイルを追加します。 Outlook 連携を無効にするロードバランスポイントの SIP トランクセキュリティプロファイルの設定, （121 ページ）とアプリケーションポイントの SIP トランクセキュリティプロファイルの設定, （122 ページ）を参照してください。

ステップ 2 既存の SIP プロファイルを確認し、それがご使用の Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを特定します。 それが要件を満たしていない場合、1 つの SIP プロファイルを設定します。
TLS SIP プロファイルの設定またはIPv6 SIP プロファイルの設定, （124 ページ）IPv6 SIP プロファイルの追加で説明される方法に従って、SIP プロファイルを設定します。

ステップ 3 ロードバランスポイントに 2 つの SIP トランクを設定します。
「ロードバランスポイントへの SIP トランクの設定」を参照してください。

ステップ 4 アプリケーションポイントに 2 つの SIP トランクを設定します。
「アプリケーションポイント用の SIP トランクの設定」を参照してください。

ステップ 5 ロードバランスポイントに設定した SIP トランクを使用して、1 つのルートグループを設定します。
「ルートグループの設定」を参照してください。

ステップ 6 上記で設定したルートグループを使用して 1 つのルートリストを設定します。
「ルートリストの設定」を参照してください。

ステップ 7 上記ルートリストを使用して *N*のルートパターンを設定します。
*N*は、管理者サイトのオーディオ設定で構成したコールインアクセス番号の数です。 「ルートパターンの設定」を参照してください。

ステップ 8 アプリケーションポイントに 2 つの SIP ルートパターンを設定します。
「SIP ルートパターンの設定」を参照してください。

2000 ユーザーのマルチデータセンターシステムにおける CUCM の構成

2000 ユーザーマルチデータセンター（MDC）システムのためにCisco Unified Communications Manager (CUCM) を設定します。 通常、各データセンターにはローカル CUCM クラスタがあります。

はじめる前に

必要な情報

- 各データセンターに対し、2 つのロードバランスポイント IP アドレス
- 各データセンターに対し、3 つのアプリケーションポイント IP アドレス
- システムで構成するコールインアクセス番号の数

ステップ 1 既存の SIP トランクセキュリティプロファイルを確認し、それが Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを決定します。 それが要件を満たしていない場合、2 つの SIP トランクセキュリティプロファイルを設定してください。
使用中のロードバランスポイントに SIP トランクセキュリティプロファイルを追加し、アプリケーションポイントに SIP トランクセキュリティプロファイルを追加します。 Outlook 連携を無効にするロードバランスポイントの SIP トランクセキュリティプロファイルの設定, （121 ページ）とアプリケーションポイントの SIP トランクセキュリティプロファイルの設定, （122 ページ）を参照してください。

ステップ 2 既存の SIP プロファイルを確認し、それがご使用の Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを特定します。 それが要件を満たしていない場合、1 つの SIP プロファイルを設定します。
TLS SIP プロファイルの設定またはIPv6 SIP プロファイルの設定, （124 ページ）IPv6 SIP プロファイルの追加で説明される方法に従って、SIP プロファイルを設定します。

ステップ 3 ロードバランスポイントに 2 つの SIP トランクを設定します。
「ロードバランスポイントへの SIP トランクの設定」を参照してください。

ステップ 4 アプリケーションポイントに 4 つの SIP トランクを設定します。
「アプリケーションポイント用の SIP トランクの設定」を参照してください。

ステップ 5 ロードバランスポイントに設定した SIP トランクを使用して、1 つのルートグループを設定します。
「ルートグループの設定」を参照してください。

ステップ 6 上記で設定したルートグループを使用して 1 つのルートリストを設定します。
「ルートリストの設定」を参照してください。

ステップ 7 上記ルートリストを使用して *N*のルートパターンを設定します。
*N*は、管理者サイトのオーディオ設定で構成したコールインアクセス番号の数です。 「ルートパターンの設定」を参照してください。

ステップ 8 アプリケーションポイントに 4 つの SIP ルートパターンを設定します。

「SIP ルートパターンの設定」を参照してください。

高可用性と非高可用性システムの CUCM の設定

以下のセクションでは、さまざまなサイズの高可用性と非高可用性システムを構成するために必要なタスクを説明します。

高可用性なしの 50、250、800 ユーザーシステムでの CUCM 設定

高可用性なしの 50、250、800 ユーザーシステムでの CUCM を設定します。

はじめる前に

必要な情報

- 1 つのロードバランスポイントの IP アドレス
- 1 つのアプリケーションポイントの IP アドレス
- システムで構成するコールインアクセス番号の数

ステップ 1 既存の SIP トランクセキュリティプロファイルを確認し、それが Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを決定します。 それが要件を満たしていない場合、2 つの SIP トランクセキュリティプロファイルを設定してください。
使用中のロードバランスポイントに SIP トランクセキュリティプロファイルを追加し、アプリケーションポイントに SIP トランクセキュリティプロファイルを追加します。 Outlook 連携を無効にするロードバランスポイントの SIP トランクセキュリティプロファイルの設定, （121 ページ）とアプリケーションポイントの SIP トランクセキュリティプロファイルの設定, （122 ページ）を参照してください。

ステップ 2 既存の SIP プロファイルを確認し、それがご使用の Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを特定します。 それが要件を満たしていない場合、1 つの SIP プロファイルを設定します。
TLS SIP プロファイルの設定またはIPv6 SIP プロファイルの設定, （124 ページ）IPv6 SIP プロファイルの追加で説明される方法に従って、SIP プロファイルを設定します。

ステップ 3 ロードバランスポイントに 1 つの SIP トランクを設定します。
「ロードバランスポイントへの SIP トランクの設定」を参照してください。

ステップ 4 アプリケーションポイントに 1 つの SIP トランクを設定します。
「アプリケーションポイント用の SIP トランクの設定」を参照してください。

ステップ 5 ロードバランスポイントに設定した SIP トランクを使用して、1 つのルートグループを設定します。

「ルートグループの設定」を参照してください。

ステップ 6 上記で設定したルートグループを使用して 1 つのルートリストを設定します。
「ルートリストの設定」を参照してください。

ステップ 7 上記ルートリストを使用して *N*のルートパターンを設定します。
*N*は、管理者サイトのオーディオ設定で構成したコールインアクセス番号の数です。「ルートパターンの設定」を参照してください。

ステップ 8 アプリケーションポイントに 2 つの SIP ルートパターンを設定します。
「SIP ルートパターンの設定」を参照してください。

高可用性の 50、250、800 ユーザーシステムでの CUCM 設定

このセクションでは、高可用性の 50、250、800 ユーザーのシステムで CUCM を設定する方法について必要な情報と詳細指示を示します。

必要な情報

- 2 つのロードバランスポイントの IP アドレス
- 2 つのアプリケーションポイントの IP アドレス
- システムで構成するコールインアクセス番号の数

構成手順

次の手順を行います。

タスク	説明	詳細情報
1	既存の SIP トランクセキュリティプロファイルを確認し、それが Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを決定します。 それが要件を満たしていない場合、2 つの SIP トランクセキュリティプロファイルを設定してください。	使用中のロードバランスポイントに SIP トランクセキュリティプロファイルを追加し、アプリケーションポイントに SIP トランクセキュリティプロファイルを追加します。Outlook連携を無効にするロードバランスポイントのSIPトランクセキュリティプロファイルの設定, （121ページ）とアプリケーションポイントの SIP トランクセキュリティプロファイルの設定, （122 ページ）を参照してください。

タスク	説明	詳細情報
2	既存の SIP プロファイルを確認し、それがご使用の Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを特定します。 それが要件を満たしていない場合、1 つの SIP プロファイルを設定します。	TLS SIP プロファイルの設定またはIPv6 SIP プロファイルの設定, （124 ページ）IPv6 SIP プロファイルの追加で説明される方法に従って、SIP プロファイルを設定します。
3	ロードバランスポイントに 2 つの SIP トランクを設定します。	「ロードバランスポイントへの SIP トランクの設定」を参照してください。
4	アプリケーションポイントに 2 つの SIP トランクを設定します。	「アプリケーションポイント用の SIP トランクの設定」を参照してください。
5	上記のタスク 3 のロードバランスポイントに設定した SIP トランクを使用して、1 つのルートグループを設定します。	「ルートグループの設定」を参照してください。
6	上記のタスク 5 で設定したルートグループを使用して 1 つのルートリストを設定します。	「ルートリストの設定」を参照してください。
7	上記ルートリストを使用して *N* のルートパターンを設定します。 *N* は、管理者サイトのオーディオ設定で構成したコールインアクセス番号の数です。	「ルートパターンの設定」を参照してください。
8	アプリケーションポイントに 2 つの SIP ルートパターンを設定します。	「SIP ルートパターンの設定」を参照してください。

高可用性の 2,000 ユーザーシステムがない CUCM 設定

高可用性でない 2000 ユーザーシステムのためにCisco Unified Communications Manager (CUCM) を設定します。

はじめる前に

必要な情報

- 2 つのロードバランスポイントの IP アドレス
- 3 つのアプリケーションポイントの IP アドレス

- システムで構成するコールインアクセス番号の数

ステップ 1 既存の SIP トランクセキュリティプロファイルを確認し、それが Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを決定します。 それが要件を満たしていない場合、2 つの SIP トランクセキュリティプロファイルを設定してください。
使用中のロードバランスポイントに SIP トランクセキュリティプロファイルを追加し、アプリケーションポイントに SIP トランクセキュリティプロファイルを追加します。 Outlook 連携を無効にするロードバランスポイントの SIP トランクセキュリティプロファイルの設定, （121 ページ）とアプリケーションポイントの SIP トランクセキュリティプロファイルの設定, （122 ページ）を参照してください。

ステップ 2 既存の SIP プロファイルを確認し、それがご使用の Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを特定します。 それが要件を満たしていない場合、1 つの SIP プロファイルを設定します。
TLS SIP プロファイルの設定またはIPv6 SIP プロファイルの設定, （124 ページ）IPv6 SIP プロファイルの追加で説明される方法に従って、SIP プロファイルを設定します。

ステップ 3 ロードバランスポイントに 2 つの SIP トランクを設定します。
「ロードバランスポイントへの SIP トランクの設定」を参照してください。

ステップ 4 アプリケーションポイントに 3 つの SIP トランクを設定します。
「アプリケーションポイント用の SIP トランクの設定」を参照してください。

ステップ 5 ロードバランスポイントに設定した SIP トランクを使用して、1 つのルートグループを設定します。
「ルートグループの設定」を参照してください。

ステップ 6 上記で設定したルートグループを使用して 1 つのルートリストを設定します。
「ルートリストの設定」を参照してください。

ステップ 7 上記ルートリストを使用して *N*のルートパターンを設定します。
*N*は、管理者サイトのオーディオ設定で構成したコールインアクセス番号の数です。 「ルートパターンの設定」を参照してください。

ステップ 8 アプリケーションポイントに 2 つの SIP ルートパターンを設定します。
「SIP ルートパターンの設定」を参照してください。

次の作業

高可用性の 2,000 ユーザーシステムでの CUCM 設定

高可用性の 2000 ユーザーシステムのためにCisco Unified Communications Manager (CUCM) を設定します。

はじめる前に

必要な情報

- 2 つのロードバランスポイントの IP アドレス
- 4 つのアプリケーションポイントの IP アドレス
- システムで構成するコールインアクセス番号の数

ステップ 1 既存の SIP トランクセキュリティプロファイルを確認し、それが Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを決定します。 それが要件を満たしていない場合、2 つの SIP トランクセキュリティプロファイルを設定してください。
使用中のロードバランスポイントに SIP トランクセキュリティプロファイルを追加し、アプリケーションポイントに SIP トランクセキュリティプロファイルを追加します。 Outlook 連携を無効にするロードバランスポイントの SIP トランクセキュリティプロファイルの設定, （121 ページ）とアプリケーションポイントの SIP トランクセキュリティプロファイルの設定, （122 ページ）を参照してください。

ステップ 2 既存の SIP プロファイルを確認し、それがご使用の Cisco WebEx Meetings Server のセットアップ要件を満たしているか否かを特定します。 それが要件を満たしていない場合、1 つの SIP プロファイルを設定します。
TLS SIP プロファイルの設定またはIPv6 SIP プロファイルの設定, （124 ページ）IPv6 SIP プロファイルの追加で説明される方法に従って、SIP プロファイルを設定します。

ステップ 3 ロードバランスポイントに 2 つの SIP トランクを設定します。
「ロードバランスポイントへの SIP トランクの設定」を参照してください。

ステップ 4 アプリケーションポイントに 4 つの SIP トランクを設定します。
「アプリケーションポイント用の SIP トランクの設定」を参照してください。

ステップ 5 ロードバランスポイントに設定した SIP トランクを使用して、1 つのルートグループを設定します。
「ルートグループの設定」を参照してください。

ステップ 6 上記で設定したルートグループを使用して 1 つのルートリストを設定します。
「ルートリストの設定」を参照してください。

ステップ 7 上記ルートリストを使用して *N*のルートパターンを設定します。
*N*は、管理者サイトのオーディオ設定で構成したコールインアクセス番号の数です。 「ルートパターンの設定」を参照してください。

ステップ 8 アプリケーションポイントに 2 つの SIP ルートパターンを設定します。
「SIP ルートパターンの設定」を参照してください。

次の作業

SIP トランクセキュリティプロファイルの設定

Outlook 連携を無効にするロードバランスポイントの SIP トランクセキュリティプロファイルの設定

はじめる前に

Cisco WebEx Meetings Server システムが TLS に設定されている場合は、セキュアな電話会議の証明書をインポートする必要があります。 詳細については、の『Cisco WebEx Meetings Server Administration Guidehttp://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html』の「セキュアな電話会議証明書のインポート」セクションを参照してください。

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [システム] > > [セキュリティ] > > [SIP トランクセキュリティプロファイル] を選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します。

- 名前 — SIP トランクセキュリティプロファイルを識別する名前を入力します。
- 端末セキュリティモード — UDP / TCP を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、[セキュアなし] を選択します。 TLS を使用して、CUCM を Cisco WebEx Meetings Server と通信する場合は、暗号化 を選択します。
- X.509 サブジェクト名 —TLS を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、証明書の名前を入力します。

  （注） TLS を使用して、CCUCM を Cisco WebEx Meetings Server と通信させる場合は、各システムが別の証明書を持っている必要があるため、別の Cisco WebEx Meetings Server システムが同じ SIP トランクセキュリティプロファイルを共有することはできません。 管理サイトからの Cisco WebEx Meetings Server 証明書の名前を取得します。 詳細については、管理者ガイドの「証明書の管理」を参照してください。

- 受信ポート - UDP / TCP を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、5060 を入力します。 TLS を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合、5061 を入力します。

（注） ページ上の他のフィールドを構成しないでください。デフォルト設定にしてください。

ステップ 6 [保存] を選択します。

アプリケーションポイントの SIP トランクセキュリティプロファイルの設定

はじめる前に

Cisco WebEx Meetings Server システムが TLS に設定されている場合は、セキュアな電話会議の証明書をインポートする必要があります。 詳細については、の『Cisco WebEx Meetings Server Administration Guidehttp://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html』の「セキュアな電話会議証明書のインポート」セクションを参照してください。

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [システム] > >[セキュリティ] >>[SIP トランクセキュリティプロファイル] を選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します。

- 名前 — SIP トランクセキュリティプロファイルを識別する名前を入力します。
- 端末セキュリティモード — UDP / TCP を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、[セキュアなし] を選択します。 TLS を使用して、CUCM を Cisco WebEx Meetings Server と通信する場合は、暗号化 を選択します。
- X.509 サブジェクト名 —TLS を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、証明書の名前を入力します。

  （注） TLS を使用して、CCUCM を Cisco WebEx Meetings Server と通信させる場合は、各システムが別の証明書を持っている必要があるため、別の Cisco WebEx Meetings Server システムが同じ SIP トランクセキュリティプロファイルを共有することはできません。 管理サイトからの Cisco WebEx Meetings Server 証明書の名前を取得します。 詳細については、管理者ガイドの「証明書の管理」を参照してください。

- 受信ポート - UDP / TCP を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、5062 を入力します。 TLS を使用して、CICM を Cisco WebEx Meetings Server と通信する場合は、5063 と入力します。

（注） ページ上の他のフィールドを構成しないでください。デフォルト設定にしてください。

ステップ 6 [保存] を選択します。

SIP プロファイルの設定

標準 SIP プロファイルの設定

標準 Session Initiation Protocol (SIP) プロファイルは、デフォルトの設定を使用しており、追加の構成手順は必要ありません。

TLS SIP プロファイルの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [デバイス] > [デバイス設定] >> [SIP プロファイル] と選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します。

- 名前 — SIP プロファイルの名前を入力します。
- アプリケーションによるリダイレクト — チェックボックスを選択します。

ページ上の他のフィールドを構成しないでください。フィールドはデフォルト設定にしてください。

ステップ 6 [保存] を選択します。

IPv6 SIP プロファイルの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [デバイス] > > [デバイス設定] > > [SIP プロファイル] と選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します。

- 名前 — SIP プロファイルの名前を入力します。
- [ANATを有効化] — チェックボックスをオンにします。

ページ上の他のフィールドを構成しないでください。フィールドはデフォルト設定にしてください。

ステップ 6 [保存] を選択します。

TLS を使用する CUCM 証明書管理

TLS を使用して、Cisco Unified Communications Manager (CUCM) に Cisco WebEx Meetings Server (CWMS) と通信させたい場合は、以下のアクションを行う必要があります。

- 管理サイトから CWMS 証明書を取得し、それを CUCM にアップロードします。

（注） CWMS がサードパーティ証明書を使用する場合、証明書チェーンのすべての証明書を CUCM にアップロードする必要があります。

- CUCM 証明書をダウンロードし、それを CWMS 管理サイトにアップロードします。

（注） CUCM はサードパーティの証明書を使用する場合、証明書チェーンの最後の証明書のみ (ルート証明機関 (CA) の証明書) を CWMS にアップロードする必要があります。

TLS を使用して、マルチデータセンター (MDC) システム中のすべてのデータセンターを同じ CUCM に接続する場合、CWMS は証明書の共通名に共通サイトの URL を使用できません。 CUCM 10.5 以前のバージョンは、共通の名前を持つ複数の証明書を同じ証明書として扱っているため、証明書の各共通名に対して、各データセンターのローカルサイト URL を使用する必要があります。

名前が異なっていない場合、第 2 のデータセンター証明書を CUCM にアップロード後、第 1 のデータセンター証明書は第 2 のデータセンター証明書によって置き換えられます。

詳細については、『管理ガイド』の「証明書の管理」を参照してください。詳細に関してはhttp://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.htmlを参照してください。

Cisco WebEx Meetings Server 証明書のアップロード

ステップ 1 Cisco WebEx Meetings Server 証明書をダウンロードし、エクスポートします。

a) Cisco WebEx Meetings Server 管理サイトにサインインします。
b) [設定] > [セキュリティ] > [証明書] の順に選択します。
c) SSL 証明書のセクションから、証明書の名前をコピーします。
d) [その他のオプション] > [SSL 証明書のエクスポートの順に選択します。
e) 証明書をローカルハードドライブに保存します。

ステップ 2 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 3 [Cisco Unified OS の管理] を選択します。

ステップ 4 [セキュリティ] >> [証明書の管理] を選択します。

ステップ 5 [証明書のアップロード]/[証明書チェーン] を選択します。

ステップ 6 [証明書名] ドロップダウンメニューで [CallManager 信頼] を選択します。

ステップ 7 [参照] ボタンを選択して、ローカルハードドライブに保存した証明書を選択します。

ステップ 8 [ファイルのアップロード] を選択します。
システムは「完了: 証明書アップロード」のメッセージを表示します。

ステップ 9 （オプション） Cisco WebEx Meetings Server が自己署名証明書を使用する場合は、ステップ 4 ～ 8 までを繰り返して、証明書チェーンからの中間証明書とルート証明機関（CA）証明書をアップロードしてください。

ステップ 10 [閉じる] を選択します。

次の作業

証明書の詳細については、『管理者ガイド』の「証明書の管理」（http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html）を参照してください。

サードパーティの CUCM 証明書のインストール

この手順では、Cisco WebEx Meetings Server にサードパーティの証明書をアップロードする方法を説明します。

はじめる前に

- 証明書署名リクエスト（CSR）を生成し、サードパーティの証明機関に送付して、証明書を申請してください。 証明書署名リクエスト（CSR）バージョン 2.6 以降の生成、 バージョン 2.6 以降または証明書署名リクエスト（CSR）バージョン 2.5 以前の生成, （129 ページ） バージョン 2.5 以前の指示を参照してください。
- 証明機関は、以下のような証明書チェーンを送付します。
  - 証明書 1（エンドユーザー） - 中間証明機関によりユーザー組織に発行されます。
  - 証明書 2（中間） - ルート証明機関より、中間の証明機関に発行されます。
  - 証明書 3（ルート CA） - ルート証明機関より発行されます。
- 証明書チェーンの複数の証明書を受け取る場合、ユーザーの証明書を先頭に、3 つの証明書を 1 つのファイルに連結する必要があります。

ステップ 1 サードパーティー証明書ファイルをお使いの 『Cisco WebEx Meetings サーバーに *Cisco WebEx Meetings Server* 管理者ガイド』 （http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html）に記載通りにインポートします。

ステップ 2 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 3 [Cisco Unified OS の管理] を選択します。

ステップ 4 [セキュリティ] > [証明書の管理] を選択します。

ステップ 5 [証明書のアップロード]/[証明書チェーン] を選択します。

ステップ 6 [証明書名] ドロップダウンメニューで [CallManager 信頼] を選択します。

ステップ 7 [参照] ボタンを選択して、ローカルハードドライブに保存したルート証明機関（CA）の証明書を選択します。
これは、最後になり、検証チェーンからの自己署名証明書であり、`CallManager.pem` 証明書を検証するために使用されます。

（注） ルート CA 証明書は `CallManager.pem` 証明書が作成されると同時に、証明機関から直接、取得できます。

ステップ 8 [ファイルのアップロード] を選択します。
システムが次のように表示するまで待ちます。「成功しました。 証明書がアップロードされました。」

ステップ 9 [閉じる] を選択します。

次の作業

証明書の詳細については、『管理者ガイド』の「証明書の管理」（http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html）を参照してください。

CUCM 証明書のダウンロード

この手順で、CUCMは自己署名証明書を使用するときのみ、必要です。 CUCMがサードパーティの証明書を使用する場合、証明書チェーンの最後の証明書（ルートCA証明書）のみをCisco WebEx Meeting Serverにアップロードする必要があります。 ルートCA証明書の取得方法については、証明機関（CA）にお問い合わせください。

CUCM 証明書を生成することに関する詳細は、CUCM ドキュメントを参照してください。

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified OS の管理] を選択します。

ステップ 3 [セキュリティ] >> [証明書の管理] を選択します。

ステップ 4 「証明書の名前」フィールドで名前が「CallManager」の証明書を検索します。 「.PEM ファイル」フィールドを選択します。

ステップ 5 ローカルのハードドライブに CUCM の証明書（CallManager.pem）を保存するために、[ダウンロード] を選択します。

次の作業

CUCM 証明書のアップロードの詳細については、『管理者ガイド』の「証明書の管理」を参照してください。
http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.htmlを参照してください。

証明書署名リクエスト（CSR）バージョン 2.6 以降の生成

CWMS 2.5 以降のバージョンで証明書署名リクエスト (CSR) と SSL 証明書の秘密鍵を生成するために使用されたハッシュ方法は SHA2 （SHA256 ）を使用します。

ステップ 1 管理サイトにサインインします。
マルチデータセンターシステムで、DNS はどのデータセンターダッシュボードが表示されるか決定します。 このダッシュボードを使用して、システムのすべてのデータセンターを管理します。

ステップ 2 [設定] > [セキュリティ] > [証明書] > [CWMS システムの証明書]の順に選択します。
マルチデータセンターシステムで、CWMS システムの証明書またはデータセンターの証明書 で継続します。

ステップ 3 希望するタイプの CSR で、[CSR を生成] を選択します。

2015 年 11 月 1 日、認証機関（VeriSign、GoDaddy など）は内部ドメイン名の証明書の発行を停止します (domain.local、domain.internal など）。 CWMS バージョン 2.0MR9 以前、展開中のコンポーネントすべてについて、サブジェクトの別名を持つ SSL 証明書を 1 つだけアップロードできました。顧客は完全なソリューションのために、高額な SAN SSL 証明書を購入する必要があります。 CWMS バージョン 2.5MR5 では、WebEx サイト URL SSL で、IRP サーバーで使用する認証局からの証明書を購入し、内部ネットワーク仮想マシンに自己署名 SSL 証明書を使用できます。

ステップ 4 **CSR (証明書署名リクエスト) の生成**ページのフィールドに必要事項を入力します。

オプション	説明
通称	[ローカルサイト URL] 証明書、[グローバルサイト URL] 証明書、または [ワイルドカード] 証明書を選択します。
サブジェクト名代替名: このオプションは、[サブジェクト名の代替名] を共通の名前タイプに選択した場合にのみ表示されます。	管理サイトと仮想マシン名 ワイルドカード共通名を選択した場合はサブジェクト名の代替名は必要ありません。
組織	組織名を入力します。
部	部署名を入力します。
City	市区町村を入力します。
都道府県	都道府県を入力します。
Country	国を選択します。
キーのサイズ	キーのサイズとして 2048 を選択します。
ハッシュアルゴリズム	ハッシュアルゴリズムとして SHA256 を選択します。

ステップ 5 [CSR 生成] を選択します。
[ファイルのダウンロード] ダイアログボックスが表示されます。

ステップ 6 [ダウンロード] を選択します。
CSR と関連する秘密鍵を含む圧縮ファイル（ZIP）ファイルを受信します。 CSR ファイルは、`csr.com` と呼ばれ、秘密鍵ファイルは、`csr_private_key.pem` と呼ばれます。

ステップ 7 VMware Data Recovery または VMware vSphere Data Protection を使用することで、システムをバックアップします。 VMware vCenter を使用してバックアップを作成するを参照してください。
システムをバックアップすると、復元に必要となる秘密鍵が生成されます。

証明書署名リクエスト（CSR）バージョン 2.5 以前の生成

CWMS 2.0 以前のバージョンで証明書署名リクエスト (CSR) と SSL 証明書の秘密鍵を生成するために使用されたハッシュ方法は SHA1 を使用します。 CWMS 2.5 以降は uses SHA2 (SHA256) を使用します。

内部と外部のアプリケーション証明書、および CSR には以下のオプションがあります。

- 鍵のタイプ:
  - RSA
  - EC
- 鍵タイプが RSA である場合、鍵の長さは 2048 です。
- RSA ハッシュアルゴリズム:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- EC 証明書の鍵サイズとハッシュアルゴリズム:
  - 鍵サイズ 256:
    - SHA256
    - SHA384
    - SHA512
  - 鍵サイズ 384:
    - SHA384
    - SHA512
  - 鍵サイズ 512:
    - SHA512

外部および内部証明書はタイプが一致する必要があります。 外部証明書は内部証明書に依存します。 たとえば、システムにRSA内部証明書がある場合、**外部自己署名証明書を生成する**ページで

は、鍵タイプはRSA (外部証明書の鍵タイプと同じ) しか選択できません。インストールされた内部鍵タイプと異なる鍵タイプの外部証明書を生成またはアップロードすることはできません。

ステップ 1 管理サイトにサインインします。
マルチデータセンターシステムで、DNS はどのデータセンターダッシュボードが表示されるか決定します。 このダッシュボードを使用して、システムのすべてのデータセンターを管理します。

ステップ 2 [設定] > [セキュリティ] > [証明書] > [CWMS システムの証明書]の順に選択します。
マルチデータセンターシステムで、CWMS システムの証明書またはデータセンターの証明書 で継続します。

ステップ 3 希望するタイプの CSR で、[CSR を生成] を選択します。
2015 年 11 月 1 日、認証機関 (VeriSign、GoDaddy など) は内部ドメイン名の証明書の発行を停止します (domain.local、domain.internal など)。 CWMS バージョン 2.0MR9 以前、展開中のコンポーネントすべてについて、サブジェクトの別名を持つSSL証明書を1つだけアップロードできました。顧客は完全なソリューションのために、高額な SAN SSL 証明書を購入する必要があります。 CWMS バージョン 2.5MR5 では、WebEx サイト URL SSL で、IRP サーバーで使用する認証局からの証明書を購入し、内部ネットワーク仮想マシンに自己署名 SSL 証明書を使用できます。

ステップ 4 **CSR (証明書署名リクエスト) の生成**ページのフィールドに必要事項を入力します。

オプション	説明
通称	[ローカルサイト URL] 証明書、[グローバルサイト URL] 証明書、または [ワイルドカード] 証明書を選択します。
サブジェクト名代替名: このオプションは、[サブジェクト名の代替名] を共通の名前タイプに選択した場合にのみ表示されます。	管理サイトと仮想マシン名 ワイルドカード共通名を選択した場合はサブジェクト名の代替名は必要ありません。
組織	組織名を入力します。
部	部署名を入力します。
City	市町村を入力してください。
都道府県	都道府県を入力してください。
Country	国を選択します。
キーのサイズ	キーのサイズとして 2048 を選択します。

ステップ 5 [CSR 生成] を選択します。

[ファイルのダウンロード] ダイアログボックスが表示されます。

ステップ 6 [ダウンロード] を選択します。
CSR と関連する秘密鍵を含む圧縮ファイル（ZIP）ファイルを受信します。 CSR ファイルは、`csr.com` と呼ばれ、秘密鍵ファイルは、`csr_private_key.pem` と呼ばれます。

ステップ 7 VMware Data Recovery または VMware vSphere Data Protection を使用することで、システムをバックアップします。 VMware vCenter を使用してバックアップを作成するを参照してください。
システムをバックアップすると、復元に必要となる秘密鍵が生成されます。

SIP トランクの設定

（注） 2000 のユーザーを高可用性（HA）複数のロードバランスとアプリケーションポイントに展開する時、CWMS ソリューション内の各ロードバランサとアプリケーションポイントは、専門 SIP トランクを持つことになります。同じトランク内で複数の宛先 IP アドレスは対応されません。

ロードバランスポイントへの SIP トランクの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [端末] > [トランク] を順に選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 [トランクタイプ] ドロップダウンメニューで [SIP トランク] を選択します。

（注） このページのその他のフィールドに変更を加えないでください。フィールドはデフォルト設定のままにします。

CUCM が Cisco WebEx Meeting Server と通信しているときは、[Media Termination Point が必要] チェックボックスは**[トランク設定]**ページ上で非選択状態にしておいてください。 Cisco WebEx Meetings Server を CUCM SIP 音声と使用していない場合、サードパーティの PBX インフラストラクチャを使用して電話サービスを提供するときに、 [Media Termination Point が必要] チェックボックスを選択できます。

ステップ 6 [次へ] を選択します。

ステップ 7 以下のフィールドを設定します。

- 端末名 - SIP トランクの名前を入力します。
- 端末プール - ドロップダウンメニューから適切な端末プールを選択します。

  その端末プールで設定された Cisco Unified Communications Manager Group がどれであるかを判別するために、[システム] > [端末プール] メニューを選択します。 このグループに属する Cisco Unified Communications Managers を検証するために、[システム] > [Cisco Unified CM Group] を選択します。

  （注） プライマリサーバーとセカンダリサーバーの IP アドレスを録画します。 Cisco WebEx Meetings Server のオーディオ設定を構成するときに、これらの IP アドレスを入力します。詳細は『管理ガイド』の「はじめての音声設定の構成」を参照してください。 『Cisco WebEx Meetings Server インストールとアップグレードガイド』を参照してください。
- 宛先アドレス - ロードバランスポイントの IPv4 アドレスを入力します。 「管理サイト」の [音声] ページの IP アドレスの SIP 構成表を参照してください。
- 宛先アドレス IPv6 - CUCM と Cisco WebEx Meetings Server の間で IPv6 を有効にする場合は、ロードバランスポイントの IPv6 アドレスを入力します。
- 宛先ポート — UDP / TCP を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、5060 を入力します。 TLS を使用して、CICM を Cisco WebEx Meetings Server と通信する場合は、5061 と入力します。
- SIP トランクセキュリティプロファイル - ドロップダウンメニューから、ロードバランスポイントのセキュリティプロファイルを選択します。
- SIP プロファイル - UDP / TCP を使用して、CUCM をCisco WebEx Meetings Server と通信させる場合、[標準 SIP プロファイル] を選択します。 TLS を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、[TLS SIP プロファイル] を選択します。 CUCM との Cisco WebEx Meetings Server の間の IPv6 を有効にする場合は、[IPv6 SIP プロファイル] を選択します。
- コール検索スペース - 電話番号を呼び出し、Cisco WebEx Meetings Server がコールアウトするCUCM で設定された電話番号やルート パターンをコールすることができる [コール検索スペース] を選択してください。 [コールルーティング] >>[コントロールのクラス] >>[コール検索スペース] を選択します。 コール検索スペースは、デバイスやルートパターンに一般的に割り当てられるルートパーティションの番号付きリストから構成されます。 コール検索スペースは、コールを完了しようとするときに、デバイス検索をコールするパーティションを決めます。 詳細については、『*Cisco Unified Communications Manager* 管理者ガイド』の「コール検索スペースの設定」または『*Cisco Unified Communications Manager* システムガイド』の「パーティションおよびコール検索スペース」を参照してください。
- コール検索スペースとダイアログ外コール検索スペースの再ルーティング—SIP ルートパターンように設定されるルートパーティションを含むコール検索スペースとダイアログ外コール検索スペースを選択します。 「SIP ルートパターンの設定」を参照してください。 これは<None>に設定されている場合、これはルートパターンセットを<None>に設定したルートパターンにコールをルートすることだけができ、SIP ルートパターンはルートパーティションを< None >に設定する必要があります。 Cisco WebEx Meetings Server のミーティングを開催するために、この設定が必要です。 詳細については、『*Cisco Unified Communications Manager* 管理者ガイド』の「コール検索スペースの設定」または

『*Cisco Unified Communications Manager* システムガイド』の「パーティションおよびコール検索スペース」を参照してください。

（注） このページのその他のフィールドに変更を加えないでください。フィールドはデフォルト設定のままにします。

ステップ 8 [保存] を選択します。

ステップ 9 [リセット] を選択し、ポップアップウィンドウで [リセットおよび再起動] を選択します。

アプリケーションポイント用の SIP トランクの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [端末] > [トランク] を順に選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 [トランクタイプ] ドロップダウンメニューで [SIP トランク] を選択します。

（注） このページのその他のフィールドに変更を加えないでください。値はデフォルト設定のままにします。

ステップ 6 [次へ] を選択します。

ステップ 7 以下のフィールドを設定します。

- デバイス名 — SIP トランクの名前を入力します。
- デバイスプール — ドロップダウンメニューから [デフォルト] を選択します。
- 宛先アドレス – アプリケーションサーバーの IPv4 アドレスを入力します。
- 宛先アドレス IPv6 - CUCM と Cisco WebEx Meetings Server の間で IPv6 を有効にする場合は、アプリケーションサーバーの IPv6 アドレスを入力します。
- 宛先ポート - UDP / TCP を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、5062を入力します。 TLS を使用して、CICM を Cisco WebEx Meetings Server と通信する場合は、5063と入力します。
- SIP トランクセキュリティプロファイル - ドロップダウンメニューから、アプリケーションサーバーのセキュリティプロファイルを選択します。
- SIP プロファイル - UDP / TCP を使用して、CUCM をCisco WebEx Meetings Server と通信させる場合、[標準 SIP プロファイル] を選択します。 TLS を使用して、CUCM を Cisco WebEx Meetings Server と通信させる場合は、[TLS SIP プロファイル] を選択します。 CUCM との Cisco WebEx Meetings Server の間の IPv6 を有効にする場合は、[IPv6 SIP プロファイル] を選択します。

- コール検索スペース - 電話番号を呼び出し、Cisco WebEx Meetings Server がコールできる CUCM で設定された電話番号やルートパターンをコールすることが可能な [コール検索スペース] を選択してください。 [コールルーティング] > [コントロールのクラス] > [コール検索スペース] を選択します。 コール検索スペースは、デバイスやルートパターンに一般的に割り当てられるルートパーティションの番号付きリストから構成されます。 コール検索スペースは、コールを完了しようとするときに、デバイス検索をコールするパーティションを決めます。 これが、< None > に設定されている場合、デバイスまたはルートパターンを、パーティションを<None>に設定してコールすることだけができます。 詳細については、『*Cisco Unified Communications Manager* 管理者ガイド』の「コール検索スペースの設定」か、『*Cisco Unified Communications Manager* システムガイド』の「パーティションおよびコール検索スペース」を参照してください。

（注） このページのその他のフィールドに変更を加えないでください。値はデフォルト設定のままにします。

CUCM が Cisco WebEx Meeting Server と通信しているときは、[Media Termination Point が必要] チェックボックスは[**トランク設定**]ページ上で非選択状態にしておいてください。 Cisco WebEx Meetings Server を CUCM SIP 音声と使用していない場合、サードパーティの PBX インフラストラクチャを使用して電話サービスを提供するときに、 [Media Termination Point が必要] チェックボックスを選択できます。

ステップ 8 [保存] を選択します。

ステップ 9 [リセット] を選択し、ポップアップウィンドウで [リセットおよび再起動] を選択します。
使用中の構成を完了するには、SIP トランクをリセットする必要があります。

ルートグループの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [コールルーティング] > [ルート/ハント] > [ルートグループ] を選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します

- ルートグループ名 — ルートグループに対して名前を入力します。
- 配布アルゴリズム。 ドロップダウンメニューから [円形] を選択します。

（注） [円形] を選択ことで、CUCM を待機中にするか、ルートグループの（N+1）番目のメンバーから開始できるようにします。 その場合、N 番目のメンバーは CUCM が最も最近コールを拡張したメンバーです。 N 番目のメンバーがルートグループの最後のメンバーである場合、CUCM はルートグループの先頭からコールを配布します。

- ルートグループに追加するデバイスの検索 - [利用可能なデバイス] リスト内の [ロードバランスポイントの SIP トランク] を選択します。 [ルートグループに追加] を選択します。

（注） このページ上の任意の他のフィールドを変更しないでください。 それらはデフォルト設定のままにします。

ステップ 6 [保存] を選択します。

次の作業

ルートグループのルートリストを作成します。ルートリストの設定, （135 ページ） に進みます。

ルートリストの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [コールルーティング] > [ルート/ハント] > [ルートリスト] を選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します

- 名前 — ルートリストの名前を入力します。
- Cisco Unified Communications Manager グループ - ドロップダウンリストメニューから [デフォルト] を選択します。

（注） このページのその他のフィールドに変更を加えないでください。フィールドはデフォルト設定のままにします。

ステップ 6 [保存] を選択します。

ステップ 7 [ルートグループを追加] を選択します。
[**ルートリスト詳細の設定**] のページが表示されます。

ステップ 8 [ルートグループ] ドロップダウンメニューから、以前に設定したルートグループを選択し、[保存] を選択します。
[**ルートリストの設定**] ページが表示されます。

ステップ 9 [保存] を選択します。

次の作業

ルートリストのルートパターンの設定をします。 ルートパターンの設定, （136 ページ） に進みます。

ルートパターンの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [コールルーティング] > [ルート/ハント] > [ルートパターン] を選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します

- ルートパターン— ルートパターンの名前をパターンを入力します。

  （注） 各ブラストダイヤルグループにルートパターンを追加します。ブラストダイヤルグループを作成するときに、 [設定] > [音声] > [ブラストダイヤルグループ] ページに管理でこの名前を入力する必要があるため、この名前を記録してください。

- ルートパーティション– Cisco WebEx Meetings Server をコールできる電話やデバイスによりアクセス可能なルートパーティションを選択します。 これが<None>に設定される場合、CUCMで設定される任意のデバイスは Cisco WebEx Meetings Server をコールすることができます。 詳細については、『*Cisco Unified Communications Manager* 管理者ガイド』の「コール検索スペースの設定」または『*Cisco Unified Communications Manager* システムガイド』の「パーティションおよびコール検索スペース」を参照してください。

- ゲートウェイ/ルートリスト— ドロップダウンメニューから、以前設定したルートリストを選択します。

（注） このページのその他のフィールドに変更を加えないでください。これらのフィールドはデフォルト設定のままにします。

ステップ 6 [保存] を選択します。

SIP ルートパターンの設定

ステップ 1 http://ccm-server/ にサインインします。ここで、*ccm-server* は Cisco Unified Communications Manager サーバの完全修飾ドメイン名または IP アドレスです。

ステップ 2 [Cisco Unified CM の管理] を選択します。

ステップ 3 [コールルーティング] > [SIP ルートパターン] を選択します。

ステップ 4 [新規追加] を選択します。

ステップ 5 以下のフィールドを設定します

- ルートパーティション□上記のセクション「アプリケーションポイントのSIPトランクの設定」から「コール検索スペースの再ルート」として設定されるコール検索スペースに含まれるルートパーティションを選択します。 これが<None>に設定される場合、アプリケーションポイントのSIPトランクに設定されたコール検索スペースの再ルートは＜None＞に設定する必要があります。 詳細については、『*Cisco Unified Communications Manager* 管理者ガイド』の「コール検索スペースの設定」または『*Cisco Unified Communications Manager* システムガイド』の「パーティションおよびコール検索スペース」を参照してください。
- パターンの使い方 — [IPアドレスのルーティング] を選択します。
- IPv4 パターン — アプリケーションポイントの IP アドレスを入力します。 「管理サイト」の [音声] ページの IP アドレスの SIP 構成表を参照してください。
- SIP トランク — ドロップダウンメニューからアプリケーションポイントに以前に設定した SIP トランクを選択します。

（注） このページのその他のフィールドに変更を加えないでください。これらのフィールドはデフォルト設定のままにします。

ステップ 6 [保存] を選択します。

CUCM 機能の互換性とサポート

CUCM 機能の互換性

Cisco WebEx Meetings Server (CWMS) は TLS/SRTP および CUCM 9.1、10.0、11.0(1a)または 11.5(1)SU1 のない Cisco Unified Call Manager (CUCM) 8.6 または 9.0 をサポートします。

重要 RSA 暗号化による署名アルゴリズム SHA256 で署名した証明書をサポートしない、CUCM の古いリリースでは、CUCM と CWMS 間の TLS 接続は失敗します。

この署名アルゴリズムをサポートするバージョンに CUCM をアップグレードするか、RSA 暗号化による SHA1 で署名したサードパーティの証明書を取得する必要があります。 最新のアメリカ国立標準技術研究所 (NIST) の推奨に従って、SHA1 はセキュリティ上の脆弱性があるため、デジタル署名の生成に使用してはいけません。

下表は、サポートされている CUCM のバージョンに対する機能の互換性を示しています。 Cisco WebEx Meetings Server システムの容量は、設定条件の影響を受けません。

（注） Cisco WebEx Meetings Server は一覧されていない CUCM バージョンまたはサードパーティの SIP プロキシ管理アプリケーションをサポートしていません。

表 *5*：サポートされたバージョンの *CUCM* の機能の互換性

機能	前提条件と特記事項
コールアウト（IPv6）	インストールプロセス中に、IPv6 アドレスで CWMS を構成します。
コールイン（IPv6）	インストールプロセス中に、IPv6 アドレスで CWMS を構成します。
TLS/SRTP	セキュリティ証明書で CWMS システムを構成します。
RFC2833。	CUCM SIP トランク設定でこのオプションを選択します。
KPML	CUCM SIP トランク設定でこのオプションを選択します。
キープアライブ—CWMS 送信	SIP OPTIONS メッセージを使って実施します。
キープアライブ—CWMS 受信	SIP OPTIONS メッセージを使って実施します。
サービスの質（QoS）	制御パケット
TCP	デフォルトのポートが以下であることを確認してください。 電話会議ロードバランスポイントでは 5060、電話会議アプリケーションポイントでは 5062 に設定します。

機能	前提条件と特記事項
TLS	デフォルトのポートが以下であることを確認してください。電話会議ロードバランスポイントでは5061、電話会議アプリケーションポイントでは 5063 に設定します。
UDP	デフォルトのポートが以下であることを確認してください。電話会議ロードバランスポイントでは5060、電話会議アプリケーションポイントでは 5062 に設定します。
自己署名式証明書	該当せず
サードパーティ証明書	該当せず

サポートされているテレフォニー機能

（注） BE6K（Business Edition 6000）製品の一部である CUCM 9.0ソフトウェアは、CWMS によりサポートされています。

- 通話保留
- 通話保留を解除
- 発信者ID表示（EP上）
- 発信者名表示（EP上）
- 通話転送（IPv4 間）
- 通話転送（IPv6 から IPv4）
- 通話転送（IPv4 kara IPv6）
- 通話転送（IPv6 間）

電話機能

CWMS は、G.711、G.722、およびG.729 コーデックを使用する参加者を同時にサポートできます。コーデック設定を変更してもシステムのパフォーマンスには影響しません。CWMS がサポートするパケットサイズ:

- g.711 音声コーデックの場合 10、20、または 30ms
- g.722 音声コーデックの場合 20ms
- g.729 音声コーデックの場合 10、20、30、40、50、または 60ms

機能	G.711。	G.722。	G.729。
ノイズ抑制	はい	はい	はい
快適なノイズ	はい	いいえ	いいえ
エコーの停止	いいえ	いいえ	いいえ
パケット損失の隠ぺい	はい	はい	いいえ
自動増幅率コントロール	はい	はい	はい
サービスの質（QoS）	はい	はい	はい

（注） Blast Dial プロンプトを含むすべてのカスタム音声プロンプトは、次の通りです。 8Khz、16 ビット、64kbps、momo、CCITT u-law (G.711).

オーディオエンドポイント互換性

Cisco Unified Communications Manager に接続するどの基準ベースの音声エンドポイントを使用しても、WebEx ミーティングに参加できます。 サポートされている音声エンドポイントには、Cisco IP 電話、Telepresence エンドポイント、および携帯電話と固定電話などの PSTN 端末が含まれます。 多くの音声エンドポイントは、音声とビデオの接続をサポートしています。 ただし、サポートされているのは、Cisco WebEx Meetings Server への音声接続のみです。

組織外部からのユーザーの PSTN 端末による WebEx ミーティングへの参加を許可するには、会社が Cisco サービス連携ルーター（ISR）などのアナログ- VoIP 変換ゲートウェイを展開する必要があります。 下記の IP電話は、Cisco WebEx Meetings Server でテスト済みです。

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator

- ライフサイズ・ビデオ電話
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20。
- EX 60
- EX 90

その他の Cisco Unified IT-互換のエンドポイントも通常通り動作するはずです。 各モデルに対する Cisco Unified Communications Manager と Device Packs によってサポートされる Cisco Unified IP Phones の一覧については、「Cisco Unified IP Phone Feature および Cisco Unified Communications Manager Device Pack Compatibility Matrix 」を参照してください。

第 6 章

アプリケーションのダウンロードについて

管理サイトで利用できるツールを使って CWMS アプリケーションを複数展開できます。 ダウンロードできるアプリケーションには、次のものが含まれます。

- WebEx Meetings アプリケーション—ミーティングのスケジューリング、出席、または主催のためのコアアプリケーションです。

  仮想化されたオペレーティングシステムでの WebEx Meetings アプリケーションの実行はサポートされていません。

  ユーザーが WebEx Meetings アプリケーションをまだインストールしていない場合、ユーザーが初めてミーティングに参加すると、そのアプリケーションが PC にダウンロードされます。 これにより、オンデマンドまたはサイレントで行うことができます。 ユーザーはミーティング中は Cisco WebEx Meetings アプリケーションを使用し、ミーティングが終了したらそれを削除するか、将来のミーティングの開始や参加のプロセスをスピードアップするために、アプリケーションのインストールを実行することを選択できます。 ユーザーに管理者権限がないため、これは失敗する場合があります。

- WebEx 生産性向上ツール—Microsoft™ Outlook® など、他のアプリケーションとの間でインターフェースとして機能するので、これらのアプリケーションを通じてミーティングの管理を行うことができるようになります。

  システムをアップデートまたはアップグレードしたら、WebEx Productivity Tools の旧バージョンをすべて削除して、最新バージョンをインストールします。

- WebEx ネットワーク記録プレーヤー—ミーティングの記録を再生します。 これにはミーティング中に表示された資料も含まれることがあります。

CWMSでは、アプリケーションの .MSI インストーラーを [管理] > [設定] > [ダウンロード] ページから入手できます。 詳細については、『CWMS プランニングガイド』の「管理サイトからのアプリケーションのダウンロード」を参照してください。

オフラインでユーザーのコンピュータにアプリケーションをプッシュしてから、アカウントが作成されたことをエンドユーザーに知らせることをお勧めします。 こうすることで、ユーザーがサインインしたらすぐにミーティングを開始または参加し、ネット—枠録画を再生できます。

ユーザーが管理者権限を持っている場合、ユーザーに自らエンドユーザーの**[ダウンロード]**ページからアプリケーションをダウンロードさせて、そのアプリケーションをインストールさせることができます。 この他に管理者アクションはありません。

ユーザーの PC に管理権限のないロックダウン環境で Cisco WebEx Meetings Server リリース 1.5 MR3 以降に**アップグレード**するとき、アップグレード手順を開始する前に、WebEx Meetings アプリケーションの新しいバージョンをすべてのユーザー PC にプッシュしてください。

- 管理サイトからのアプリケーションのダウンロード，144 ページ
- アプリケーション ZIP ファイルの内容，145 ページ
- Cisco WebEx 生産性向上ツールの複数展開，148 ページ
- Meetings アプリケーションの複数展開，156 ページ
- ネットワーク録画プレーヤーの複数展開，161 ページ
- 更新実行後の設定の再構成，166 ページ

管理サイトからのアプリケーションのダウンロード

管理者がユーザーに Cisco WebEx デスクトップアプリケーションを手動でダウンロードしたり、ユーザーが自分でダウンロードできるように許可したりするようにシステムを設定できます。

ステップ 1 管理サイトにサインインします。
マルチデータセンターシステムで、DNS はどのデータセンターダッシュボードが表示されるか決定します。 このダッシュボードを使用して、システムのすべてのデータセンターを管理します。

ステップ 2 [設定] > [ダウンロード] の順に選択します。

ステップ 3 ダウンロードの方法を選択します。

- ユーザーが WebEx デスクトップアプリケーションをダウンロードすることを許可します。
このオプションを使用して、PCの管理者権限を保有するユーザーが会議アプリケーションを管理することを許可します。
- WebEx アプリケーションをユーザーのデスクトップに手動でプッシュします。
このオプションを使用して、PCの管理者権限を持たないユーザーに対し、会議を有効にします。

  このオプションを選択すると、ウィンドウが拡大し、Cisco WebEx Meetings、生産性向上ツール、ネットワーク録画プレーヤーのセクションが表示されます。

ステップ 4 （任意） WebEx 生産性向上ツールの自動アップデートWebEx 生産性向上ツールの周期的、自動アップデートを構成します。 （**デフォルト**： 選択済み）

ステップ 5 [WebExデスクトップアプリケーションをユーザーのデスクトップに手動でプッシュする]を選択した場合:

a) WebEx Meetings セクションで、[ダウンロード] を選択してから ZIP ファイルをシステムに保存します。

b) 生産性向上ツールセクションで、[ダウンロード] を選択してから ZIP ファイルをシステムに保存します。
c) WebEx ネットワーク録画プレーヤーセクションで、[ダウンロード] を選択してから ZIP ファイルをシステムに保存します。

ステップ 6 [保存] を選択して、ダウンロード設定を保存します。
これは、ユーザーが WebEx デスクトップアプリケーションをダウンロードすることを許可する場合に特に重要です。

ステップ 7 （任意） [WebEx デスクトップアプリケーションをユーザーのデスクトップに手動でプッシュする]を選択した場合:

a) ダウンロードしたファイルを解凍します。
b) ZIP ファイルを開きます。
各 ZIP ファイルには、サポートされている言語すべてのアプリケーションインストーラが収納されています。 使用を推奨されるインストーラに関する情報については、アプリケーション ZIP ファイルの内容, （145 ページ）を参照してください。
c) プラットフォームと言語に適したインストーラーを選択し、ローカルのディレクトリフォルダに展開します。
この ZIP ファイルには、Windows プラットフォームに対応した MSI インストーラーが多言語サポートされて収納されています。

Cisco WebEx Meeting Server の各バージョンと適合する生産性向上ツールとミーティングアプリケーションのバージョンはCisco WebEx Meetings アプリケーションおよび生産性向上ツール互換性マトリクス, （217 ページ）に記載されています。

次の作業

本章に記載されている方法で MSI インストーラーを展開します。

アプリケーション ZIP ファイルの内容

このZIPファイルには、言語ごとに 1 つのインストーラアプリケーションが収納されています。

アプリケーション言語キー

各 ZIP ファイルの英語アプリケーションインストーラファイルは、言語接頭語なしで名前が付けられています。 その他の 12 カ国語のそれぞれのアプリケーションインストーラファイルには、それが含むアプリケーションの言語を示すファイル名の省略語が含まれます。 各言語に使用する省略語については、下表を参照してください。

省略語	LANGUAGE
B5。	繁体字中国語

省略語	LANGUAGE
DE	ドイツ語
ES	ラテンアメリカ系スペイン語
FR	フランス語
GB	簡体字中国語
IT	イタリア語
JP	日本語
KO	韓国語
NL	オランダ語
PT	ポルトガル語
RU	ロシア語
SP	スペイン語

生産性向上ツール ZIP ファイルの内容

生産性向上ツール ZIP ファイルには、次のファイルが含まれています。 上表のキーを使用して、各ファイルの言語を判別します。 生産性ツールにはMacバージョンはないので、注意してください。

- ptools.msi
- ptools_B5.msi。
- ptools_DE.msi
- ptools_ES.msi
- ptools_FR.msi
- ptools_GB.msi
- ptools_IT.msi
- ptools_JP.msi
- ptools_KO.msi
- ptools_NL.msi
- ptools_PT.msi
- ptools_RU.msi
- ptools_SP.msi

WebEx Meetings Client ZIP ファイルの内容

各Zipファイルに含まれたアプリケーションの言語を判別するために、アプリケーション言語キー, （145 ページ） のキーを使用してください。

バージョン 2.7 以降	バージョン 2.6 以降
webexmc.msi.msi	onpremmc.msi
webexmc_allinone.msi	onpremmc_B5.msi
webexmc.msi_B5.msi	onpremmc_DE.msi
webexmc.msi_DE.msi	onpremmc_ES.msi
webexmc.msi_ES.msi	onpremmc_FR.msi
webexmc.msi_FR.msi	onpremmc_GB.msi
webexmc.msi_GB.msi	onpremmc_IT.msi
webexmc.msi_IT.msi	onpremmc_JP.msi
webexmc.msi_JP.msi	onpremmc_KO.msi
webexmc.msi_KO.msi	onpremmc_NL.msi
webexmc.msi_NL.msi	onpremmc_PT.msi
webexmc.msi_PT.msi	onpremmc_RU.msi
webexmc.msi_RU.msi	onpremmc_SP.msi
webexmc.msi_SP.msi	webexmc_onprem.dmg (for Mac)
webexmc_onprem.dmg (for Mac)	

ネットワーク録画プレーヤー ZIP ファイルの内容

ネットワーク録画プレーヤーは、[ダウンロード]ページの「**ユーザーがWebExデスクトップアプリケーションをダウンロードすることを許可する**」を選択した場合のみに、ダウンロードおよび複数展開が可能です。 詳細は、『*Cisco WebEx Meetings Server* 管理者ガイド』の「ダウンロードの設定」のセクションを参照してください。

ネットワーク録画プレーヤー ZIP ファイルには、次のファイルが含まれています。 上表のキーを使用して、各ファイルの言語を判別します。

- nbr2player_onprem.msi。
- nbr2player_onprem_B5.msi。
- nbr2player_onprem_DE.msi。
- nbr2player_onprem_ES.msi。
- nbr2player_onprem_FR.msi。
- nbr2player_onprem_GB.msi。
- nbr2player_onprem_IT.msi。
- nbr2player_onprem_JP.msi。
- nbr2player_onprem_KO.msi。
- nbr2player_onprem_NL.msi。
- nbr2player_onprem_PT.msi。
- nbr2player_onprem_RU.msi。
- nbr2player_onprem_SP.msi。
- webexnbrplayer_intel.dmg (Mac)

Cisco WebEx 生産性向上ツールの複数展開

このセクションには、`ptools.ms` パッケージを利用した Cisco WebEx 生産性向上ツールのインストールに関連するタスクが記載されています。 単一コンピュータのインストールと大規模なインストールは Microsoft Systems Management Server 2003 (SMS) を利用することにより可能となります。

Cisco WebEx Meeting Server の各バージョンと適合する生産性向上ツールのバージョンは Cisco WebEx Meetings アプリケーションおよび生産性向上ツール互換性マトリクス, （217 ページ） に記載されています。

コマンドラインを使用した生産性向上ツールのサイレントインストール

管理者は、ユーザーのコンピュータにサインインして、サイレントモードで WebEx 生産性向上ツールをインストールできます。

はじめる前に

メンテナンスリリースをインストールするか、システムを新しいリリースにアップグレードする前に、Cisco WebEx 生産性向上ツールの前のバージョンをアンインストールする必要があります。

ステップ 1 ユーザのコンピュータにサインインします。

ステップ 2 MSI パッケージをコンピュータのハードドライブにダウンロードします。

ステップ 3 Windows コマンドプロンプトを開きます。
Windows 7 および Windows Vista では、[管理者として実行] を使用して、プロンプトウィンドウを開く必要があります。

ステップ 4 MSI コマンドを実行して、WebEx 生産性向上ツールをサイレントモードでインストールします。

例：
msiexec.exe /q /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1 MSN=1

パラメータ名:	値	説明
OI	1	Outlook との統合を有効にする
	0（デフォルト)	Outlook 統合無効
MSN	1	Microsoft Office Commuicator と Lync 用のインスタントメッセンジャーの組み込みを有効にする
MSN	0（デフォルト)	Microsoft Office Commuicator と Lync 用のインスタントメッセンジャーの組み込みを無効にする

ステップ 5 コンピュータを再起動します。

コマンドラインインターフェースを使用した生産性向上ツールのサイレントアンインストール

管理者は、ユーザーのコンピュータにサインインして、サイレントモードで生産性向上ツールをアンインストールできます。

ステップ 1 ユーザのコンピュータにサインインします。

ステップ 2 MSI パッケージをコンピュータのハードドライブにダウンロードします。

ステップ 3 Windows コマンドプロンプトを開きます。
Windows 7 および Windows Vista では、[管理者として実行] を使用して、プロンプトウィンドウを開く必要があります。

ステップ 4 MSI パッケージ ptool msi のコンポーネントすべてを、msiexec.exe /q /x "ptools.msi".コマンドを入力してアンインストールします。

SMS使用の際の、CWMSアプリケーションのサイレントインストールの限度

以下の制限は、Microsoft Systems Management Server 2003 (SMS)を使用するサイレントインストールに適用されます。

- SMS ユーザ毎モードはサポートされていません。
- SMS 管理者が WebEx 生産性向上ツールの機能を追加する場合、今までに機能をインストールしていなくても、管理者はまず **REMOVE** コマンドを実行し、次に **ADDSOURCE** コマンドを実行する必要があります。
- 管理者がパッケージを提供している間に、リモートデスクトップでユーザーがコンピュータにログオンした場合、そのユーザーは必ずコンピュータを再起動して、WebEx 生産性向上ツールの正常な動作を確認する必要があります。
- 複数展開は可能ですが、各ユーザーが資格情報を入力する必要があります。
- メンテナンスリリースを更新するか、新しいリリースにアップグレードする前に、ユーザーは Cisco WebEX 生産性向上ツールをアンインストールする必要があります。 アップグレードした後で、ユーザーに生産性向上ツールを手動でプッシュするか、ユーザーが[ダウンロード] ページから生産性向上ツールをダウンロードできます。
- Lync 統合を使用している場合は、サイレントインストールの後で、ユーザーはコンピュータを再起動して、すべてのインスタントメッセンジャーの統合が正常に動作するようにしなければなりません。

SMS システム毎無人プログラムを使用する WebEx 生産性向上ツールの提供

アップデートまたはアップグレードした後で、管理サイトを使用してユーザーに生産性向上ツールを手動でプッシュするか、ユーザーが**[ダウンロード]**ページから生産性向上ツールをダウンロードできます。

詳細は、Cisco WebEx Meetings Server 管理者ガイドの「ダウンロードの設定」のセクションを参照してください。

Microsoft Systems Management Server 2003（SMS）管理者であれば、SMS システム毎無人プログラムを使用して Cisco WebEx 生産性向上ツールを提供できます。

ステップ 1 定義からパッケージを作成します。 詳細については、定義からのパッケージの作成，（156 ページ）を参照してください。

ステップ 2 提供する前に、**「システム毎無人」**のプログラムオプションを変更してください。

a) SMS 管理者コンソールを開き、[サイトデータベース]> >[パッケージ]> >[Cisco WebEx LLC Cisco WebEx 生産性向上ツール 2.82]> > [プログラム]を選択します。

b) [システム毎無人プログラム] を右クリックしてから、[プロパティ] を選択して [**システム毎無人プログラムのプロパティ**] ダイアログボックスを開きます。

c) [環境] タブを選択します。

- [プログラムの実行条件] オプションで、[ユーザがログオンしているときのみ] を選択します。
- [実行モード] オプションで、[管理者権限で実行する] を選択します。 （[ユーザにこのプログラムの操作を許可する] はオンにしないでください。）

d) [全般]タブを選択します。

e) コマンドラインオプションに追加パラメータを追加して、Cisco WebEx 生産性向上ツールの一部のオプションを指定します。

- SITEURL="http://sample.webex.com"を追加して、会社で使用する WebEx サイト URL を指定します。
- 生産性向上ツールのフラグを追加すると、WebEx 生産性向上ツールのどのコンポーネントを有効にするか指定できます。 パラメータは大文字である必要があり、デフォルト値は 0（無効)です。

  下の例で、初期コマンドラインは msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi" です。
- 生産性向上ツールのフラグとパラメータをコマンドラインに追加します： msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1MSN=1

（注） パラメータの定義については、パラメータテーブルのコマンドラインを使用した生産性向上ツールのサイレントインストール，（148 ページ）を参照してください。

ステップ 3 プログラムを提供します。

a) SMS 管理者コンソールを起動し、[サイトデータベース] >> [パッケージ] >> [Cisco WebEx LLC Cisco WebEx 生産性向上ツール 2.82 英語版] >> [プログラム] と選択します。
b) [システム毎無人] を右クリックします。
c) [すべてのタスク] >> [ソフトウェアの配布] を選択します。
d) [プログラムの配布ウィザード] で [**次へ**] をクリックします。
e) SMS サーバを選択し、[次へ] を選択します。
f) コレクションを選択し、[次へ] を選択します。
g) [名前] フィールドに提供名を入力し、[次へ] を選択します。
h) 提供をサブコレクションにも適用するかどうかを指定し、[次へ] を選択します。
i) いつプログラムを提供するかを指定し、[次へ] を選択します。
j) プログラムを割り当てるかどうかを指定し、[次へ] を選択します。
k) [プログラムの配布完了ウィザード] ページで [**完了**] を選択します。
l) \Site Database\System Status\Advertisement Status ディレクトリに移動し、提供ステータスを確認します。通知を有効にしていると、プログラムが提供された後、割り当てられたプログラムが実行されることを通知するメッセージがユーザに表示されます。 割り当てられたプログラムがサイレントモードで実行されます。

SMS システム毎無人プログラムを使用する生産性向上ツールのコンポーネントの削除

次の手順を実行し、Microsoft Systems Management Server 2003 (SMS) を使用して、生産性向上ツールを削除します。

手順の概要

1. 新しいプログラムを作成し、SMS システム毎無人プログラムを使用する WebEx 生産性向上ツールの提供, （151 ページ）で説明されているとおり、「システムごとの無人プログラム」からすべてのオプションをコピーし、コマンド行を更新します。
2. ドメインにある指定された作業マシンのコレクションに、プログラムを提供します。 詳細については、SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度, （150 ページ）を参照してください。

手順の詳細

ステップ 1 新しいプログラムを作成し、SMS システム毎無人プログラムを使用する WebEx 生産性向上ツールの提供, （151 ページ）で説明されているとおり、「システムごとの無人プログラム」からすべてのオプションをコピーし、コマンド行を更新します。

a) SMS 管理者コンソールを開き、[サイトデータベース]> >[パッケージ]> >[Cisco WebEx LLC Cisco WebEx 生産性向上ツール 2.82]> > [プログラム]を選択します。
b) 空白エリアを右クリックしてから、[新規]> > [プログラム] を選択します。
c) プログラム名とデフォルトのコマンドラインを入力します。
d) [**プロパティ**] ダイアログボックスで、[環境] タブを選択します。
   - [プログラムの実行条件] オプションで、[ユーザがログオンしているときのみ] を選択します。
   - [実行モード] オプションで、[管理者権限で実行する] を選択します。 （[ユーザにこのプログラムの操作を許可する] はオンにしないでください。）
e) [全般] タブでコマンドラインを更新します。
f) REMOVE をコマンドラインに追加し、削除する機能を指定します。

   例：
   [OI] を削除したい場合は、次のコマンドを入力します。 msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"
   PTIM 値は、インスタントメッセンジャーに CWMS を組み込むためのものです。 例: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="PTIM"

ステップ 2 ドメインにある指定された作業マシンのコレクションに、プログラムを提供します。 詳細については、SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度, （150 ページ）を参照してください。
これらのマシンで Cisco WebEx 生産性向上ツールはサイレントモードで更新されます。

SMS システム毎無人プログラムを使用する生産性向上ツールの追加

管理者が生産性向上ツールにコンポーネントを追加するには、コンポーネントが以前にインストールされていない場合も、まず REMOVE を実行し、次に ADDSOURCEADDSOURCE を実行する必要があります。

ステップ 1 新しいプログラムを [`Add-phase1`] という名前で作成し、[システム毎無人プログラム] からすべてのオプションをコピーし、コマンドラインを更新します。

a) SMS 管理者コンソールを開き、[サイトデータベース]> >[パッケージ]> >[Cisco WebEx LLC Cisco WebEx 生産性向上ツール 2.82]> > [プログラム]を選択します。
b) 空白エリアを右クリックしてから、[新規]>[プログラム] を選択します。
c) プログラム名とデフォルトのコマンドラインを入力します。
d) [プロパティ] ダイアログボックスで、[環境] タブを選択します。
   - [プログラムの実行条件] オプションで、[ユーザがログオンしているときのみ] を選択します。

- [実行モード] オプションで、[管理者権限で実行する] を選択します。 （[ユーザにこのプログラムの操作を許可する] はオンにしないでください。）

e) [全般] タブでコマンドラインを更新します。
f) REMOVE をコマンドラインに追加し、追加する機能を指定します。

例：
OI と PITM（PITM 値はインスタントメッセンジャーに WebEx を組み込むためのものです） を追加する場合、まだインストールされていない場合でも、最初にそれらを削除する必要があります。 msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI,PTIM"

ステップ 2 ドメインにある指定された作業マシンのコレクションに、プログラムを提供します。 詳細については、SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度, （150 ページ）を参照してください。

ステップ 3 2 番目のプログラムを [Add-phrase2] という名前で作成し、[システム毎無人プログラム] からすべてのオプションをコピーし、コマンドラインを更新します。

a) SMS 管理者コンソールを開き、[サイトデータベース]> >[パッケージ]> >[Cisco WebEx LLC Cisco WebEx 生産性向上ツール 2.82]> > [プログラム]を選択します。
b) 空白エリアを右クリックしてから、[新規] > [プログラム] を選択します。
c) プログラム名とデフォルトのコマンドラインを入力します。
d) [プロパティ] ダイアログボックスで、[環境] タブを選択します。

- [プログラムの実行条件] オプションで、[ユーザがログオンしているときのみ] を選択します。
- [実行モード] オプションで、[管理者権限で実行する] を選択します。 （[ユーザにこのプログラムの操作を許可する] はオンにしないでください。）

e) [プロパティ] ダイアログボックスで、[詳細] タブを選択します。
f) [別のプログラムを最初に実行する] をオンにして、プログラム [Add-phase1] を選択します。
g) [全般] タブでコマンドラインを更新します。
h) ADDSOURCE をコマンドラインに追加し、追加する機能を指定します。

例：
[OI] と [PITM] を追加したい場合は、次のサンプルコマンドを使用します。 msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI,PTIM" OI=1 MSN=1

ステップ 4 ドメインにある指定された作業マシンのコレクションに、プログラムを提供します。 詳細については、SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度, （150 ページ）を参照してください。
これらのマシンで Cisco WebEx 生産性向上ツールはサイレントモードで更新されます。

SMSシステム毎無人プログラムを使用する生産性向上ツールのアンインストール

SMS 管理者であれば、以下の手順を実行し、SMS システム毎アンインストールプログラムを使用して Cisco WebEx 生産性向上ツールをアンインストールできます。

ステップ 1 定義からのパッケージの作成, （156 ページ） で作成した SMS インストールパッケージを使用します。

ステップ 2 システム毎アンインストールプログラムを提供して、Cisco WebEx 生産性向上ツールをアンインストールします。
マシンで、Cisco WebEx 生産性向上ツールがサイレントモードでアンインストールされます。

プログラムの提供によるWebEx生産性向上ツールの新しいバージョンへの更新

以下の手順を実行して、プログラムを提供し、Cisco WebEx 生産性向上ツールの新しいバージョンに更新します。

はじめる前に

メンテナンスリリースをインストールするか、システムを新しいリリースにアップグレードする前に、ユーザーはデスクトップで実行中の Cisco WebEX 生産性向上ツールをアンインストールする必要があります。 アップグレードした後で、管理サイトを使用してユーザーに生産性向上ツールを手動でプッシュするか、ユーザーが **[ダウンロード]** ページから生産性向上ツールをダウンロードできます。

管理サイトにサインインし、[設定] > [ダウンロード] を選択して、以下の設定を無効にします。

- Cisco WebEx 生産性向上ツールの自動更新
- ユーザが WebEx デスクトップアプリケーションをダウンロードすることを許可する

ステップ 1 WebEx 生産性向上ツールの MSI パッケージを使用して、新しい SMS インストールパッケージを作成します。
詳細については、定義からのパッケージの作成, （156 ページ） を参照してください。

ステップ 2 提供する前に、「システム毎無人」のプログラムオプションを変更してください。
詳細については、SMS システム毎無人プログラムを使用する生産性向上ツールの追加, （153 ページ） を参照してください。

ステップ 3 プログラムを提供します。 詳細については、SMS システム毎無人プログラムを使用する生産性向上ツールの追加, （153 ページ）を参照してください。
古い Cisco WebEx 生産性向上ツールが削除され、新しい Cisco WebEx 生産性向上ツールがサイレントモードでインストールされます。

定義からのパッケージの作成

ステップ 1 SMS 管理者コンソールを起動し、[サイトデータベース] > [パッケージ] と選択します。
ステップ 2 [パッケージ] を右クリックします。
ステップ 3 [新規] > [定義に基づくパッケージ] と選択します。
ステップ 4 **[定義に基づくパッケージの作成]** ウィザードで、[次へ] を選択します。
ステップ 5 [参照] を選択して探し、WebEx 生産性向上ツール MSI パッケージを選択してから、[次へ] を選択します。
ステップ 6 [常にソース ディレクトリからファイルを取得する] を選択してから、[次へ] を選択します。
ステップ 7 ソース ディレクトリの場所を選び、それから [次へ]を選択します。
ステップ 8 [完了] を選択します。
ステップ 9 [サイトデータベース] > > [パッケージ] > > [Cisco WebEx LLC Cisco WebEx 生産性向上ツール 2.82 英語版] > > [プログラム] と選択します。
6 つのプログラムが使用可能です。

Meetings アプリケーションの複数展開

このセクションは、組織が Cisco WebEx Meetings アプリケーションのインストールに関連するタスクを理解するのに役立つように設計されています。 このセクションは、単一コンピュータのインストールから Microsoft Systems Management Server 2003（SMS）を使用する大規模なインストールまでのさまざまなタイプのインストールをカバーする総合的なガイドです。

（注） 「サイレントインストール」は、アプリケーションをサイレントモードで展開することが可能であることを意味しますが、エンドユーザの構成が必要になります。

Cisco WebEx Meetings のインストール

はじめる前に

Cisco WebEx Meetings のインストーラには以下の前提条件があります。

- Cisco WebEx MSI パッケージのインストールには管理者の権限が必要です。 MSI パッケージはアクセスに管理者の権限が必要なデフォルトの OS プログラムフォルダにインストールされます。
- Cisco WebEx MSI パッケージは Windows Installer Service 2.0 以上用に開発されています。 ローカルマシンがそれより古いバージョンの場合は、新しいバージョンの Windows Installer Service が必要であることをユーザーに知らせるエラーメッセージが表示されます。 MIS パッケージを実行した後、基本MSIインタフェースがユーザーに表示されます。

ステップ 1 ユーザのコンピュータでインストーラを起動します。
インストールウィザードに最初のメッセージが表示されます。

ステップ 2 インストールのダイアログボックスが表示されるまで、いくつかのダイアログで [次へ] を選択します。

ステップ 3 [インストール] を選択します。

ステップ 4 インストールが完了したら、[完了] を選択します。

ローカルで Cisco WebEx Meetings アプリケーションのアンインストール

ユーザーのコンピュータにサインインして、Cisco WebEx Meetings アプリケーションをコントロールパネルまたはローカルハードドライブの WebEx フォルダからアンインストールできます。

はじめる前に

Cisco WebEx Meetings のアプリケーションがユーザーのコンピュータにインストールされます。

ステップ 1 ユーザのコンピュータにサインインします。

ステップ 2 Cisco WebEx Meetings のアプリケーションを削除するには、以下の手順に従います。

- [スタート] > [コントロールパネル] > [プログラムと機能]を選択します。 プログラムの一覧から、[Cisco WebEx Meetings] を選択し、その後 [アンインストール/変更] を選択します。
- [スタート] > Computer > [システム(C:)] > 「ProgramData」フォルダー > 「WebEx」フォルダーを順に選択します。 [atcliun.exe] を右クリックし、[削除] を選択します。

（注） atcliun.exe を WebEx フォルダからアンインストールすると、Cisco WebEx Meetings アプリケーションのオンプレミスおよびクラウドバージョンがユーザーのローカルハードドライブで保存されている場合、両方とも削除されます。 ただし、コントロールパネルを使用してアプリケーションをアンインストールした場合、アプリケーションのオンプレミスバージョンだけがアンインストールされます。

Cisco WebEx Meetings のアプリケーションがユーザーのコンピュータからアンインストールされます。

コマンドラインを使用したミーティングアプリケーションのサイレントインストール

管理者はユーザーのコンピュータにサインインして、WebEx Meetings アプリケーションをサイレントモードでインストールします。

ステップ 1 ユーザのコンピュータにサインインします。

ステップ 2 MSI パッケージをコンピュータのハードドライブにダウンロードします。

ステップ 3 Windows コマンドプロンプトを開きます。
Windows 7 および Windows Vista では、[管理者として実行] を使用して、プロンプトウィンドウを開く必要があります。

ステップ 4 MSI コマンドを入力して、Cisco WebEx Meetings アプリケーションをサイレントモードでインストールします。

例：
msiexec /i onpremmc.msi /qn を入力します。

ステップ 5 コンピュータを再起動します。

コマンドラインインターフェースを使用したミーティングアプリケーションのサイレントアンインストール

管理者は、ユーザーのコンピュータにサインインして、サイレントモードで Meetings アプリケーションをアンインストールできます。

ステップ 1 ユーザのコンピュータにサインインします。

ステップ 2 Windows コマンドプロンプトを開きます。

Windows 7 および Windows Vista では、[管理者として実行] を使用して、プロンプトウィンドウを開く必要があります。

ステップ 3 MSI パッケージ onpremmc.msi のコンポーネントをすべてアンインストールするには、コマンド msiexec/inbr2player_onprem.msi/qn を入力します。

SMS使用の際の、CWMSアプリケーションのサイレントインストールの限度

以下の制限は、Microsoft Systems Management Server 2003 (SMS)を使用するサイレントインストールに適用されます。

- SMS ユーザ毎モードはサポートされていません。
- SMS 管理者が WebEx 生産性向上ツールの機能を追加する場合、今までに機能をインストールしていなくても、管理者はまず **REMOVE** コマンドを実行し、次に **ADDSOURCE** コマンドを実行する必要があります。
- 管理者がパッケージを提供している間に、リモートデスクトップでユーザーがコンピュータにログオンした場合、そのユーザーは必ずコンピュータを再起動して、WebEx 生産性向上ツールの正常な動作を確認する必要があります。
- 複数展開は可能ですが、各ユーザーが資格情報を入力する必要があります。
- メンテナンスリリースを更新するか、新しいリリースにアップグレードする前に、ユーザーは Cisco WebEX 生産性向上ツールをアンインストールする必要があります。 アップグレードした後で、ユーザーに生産性向上ツールを手動でプッシュするか、ユーザーが[ダウンロード] ページから生産性向上ツールをダウンロードできます。
- Lync 統合を使用している場合は、サイレントインストールの後で、ユーザーはコンピュータを再起動して、すべてのインスタントメッセンジャーの統合が正常に動作するようにしなければなりません。

SMS システム毎無人プログラムを使用する生産性向上ツールの提供

Microsoft Systems Management Server 2003 (SMS) 管理者は Cisco WebEx Meetings アプリケーションが利用可能であることをシステム毎の無人プログラムを使用してお知らせできます。

はじめる前に

管理サイトにサインインして、ダウンロード設定でWebExデスクトップアプリケーションをユーザーのデスクトップにプッシュするよう設定します。 詳細は、Cisco WebEx Meetings Server 管理者ガイドの「ダウンロードの設定」のセクションを参照してください。

ステップ 1 定義からパッケージを作成します。 詳細については、定義からのパッケージの作成, （156 ページ）を参照してください。

ステップ 2 提供する前に、「システム毎無人」のプログラムオプションを変更してください。

a) SMS 管理者コンソールを起動し、[サイトデータベース] >> [パッケージ] >> [Cisco WebEx LLC Cisco WebEx Meeting アプリケーション英語版] >> [プログラム] と選択します。

b) [システム毎無人プログラム] オプションを右クリックしてから、[プロパティ] を選択して [**システム毎無人プログラムのプロパティ**] ダイアログボックスを開きます。

c) [環境] タブを選択します。

- [プログラムの実行条件] オプションで、[ユーザがログオンしているときのみ] を選択します。
- [実行モード] オプションで、[管理者権限で実行する] を選択します。 [ユーザにこのプログラムの操作を許可する] を選択しないでください。

d) [全般]タブを選択します。

e) コマンドラインオプションに追加パラメータを追加して、WebEx Meetings アプリケーションの一部のオプションを指定します。

例：
例えば、最初のコマンドラインには次を入力します： msiexec /i "onpremmc.msi" /qn

ステップ 3 これで、プログラムを提供できます。

a) SMS 管理者コンソールを起動し、[サイトデータベース] >> [パッケージ] >> [Cisco WebEx LLC Cisco WebEx Meeting アプリケーション英語版] >> [プログラム] と選択します。

b) [システム毎無人] を右クリックします。

c) [すべてのタスク] >> [ソフトウェアの配布] を選択します。

d) [プログラムの配布ウィザード] で [**次へ**] をクリックします。

e) SMS サーバを選択し、[次へ] を選択します。

f) コレクションを選択し、[次へ] を選択します。

g) [名前] フィールドに提供名を入力し、[次へ] を選択します。

h) 提供をサブコレクションにも適用するかどうかを指定し、[次へ] を選択します。

i) いつプログラムを提供するかを指定し、[次へ] を選択します。

j) プログラムを割り当てるかどうかを指定し、[次へ] を選択します。

k) [プログラムの配布完了ウィザード] ページで [**完了**] を選択します。

l) \Site Database\System Status\Advertisement Status ディレクトリに移動し、提供ステータスを確認します。

通知を有効にしていると、プログラムが提供された後、割り当てられたプログラムが実行されることを通知するメッセージがユーザに表示されます。 割り当てられたプログラムがサイレントモードで実行されます。

SMS システム毎アンインストールプログラムを使用する Cisco WebEx Meetings アプリケーションのアンインストール

SMS システム毎無人プログラムを使用する Cisco WebEx Meetings アプリケーションのアンインストール

ステップ 1 定義からのパッケージの作成, （156 ページ） で作成した SMS インストールパッケージを使用します。

ステップ 2 システム毎アンインストールプログラムを提供して、 Cisco WebEx Meetings アプリケーションをアンインストールします。
Cisco WebEx Meetings アプリケーションは、サイレントモードで指定したマシンからアンインストールされます。

ネットワーク録画プレーヤーの複数展開

このセクションは、単一コンピュータのインストールから Microsoft Systems Management Server 2003（SMS）を使用する大規模なインストールまでのさまざまなタイプのインストールをカバーする総合的なガイドです。

（注） 4GB を超えるネットワーク録画プレーヤーは Web ブラウザからアクセスする場合のみ再生できます。

ネットワーク録画プレーヤーのインストール

はじめる前に

- Cisco WebEx MSI パッケージはデフォルトで OS Programs フォルダにインストールされ、このフォルダにはアクセス権限が必要なため、標的デバイスに管理者権限があることを確認してください。

- Cisco WebEx MSI パッケージは Windows Installer Service 2.0 以上用に開発されました。 ローカルマシンがそれより古いバージョンの場合は、そのMISパッケージをインストールするには新しいバージョンの Windows Installer Service が必要であることをユーザーに知らせるエラーメッセージが表示されます。 MISパッケージを実行した後、MSIインタフェースを通してプロンプトがユーザーに表示されます。

ステップ 1 ユーザのコンピュータでインストーラを起動します。
インストールウィザードに最初のメッセージが表示されます。

ステップ 2 インストール用ダイアログボックスが表示されるまで、各ダイアログボックスで [次へ] を選択します。

ステップ 3 [インストール] を選択します。

ステップ 4 [完了] を選択します。

コマンドラインを使用した Recording Player のサイレントインストール

管理者は、ユーザーのコンピュータにサインインして、サイレントモードで WebEx Recording Playe をインストールできます。

ステップ 1 ユーザのコンピュータにサインインします。

ステップ 2 MSI パッケージをコンピュータのハードドライブにダウンロードします。

ステップ 3 Windows コマンドプロンプトを開きます。
Windows 7 および Windows Vista では、[管理者として実行] を使用して、プロンプトウィンドウを開く必要があります。

ステップ 4 MSI コマンドを入力して、WebEx Recording Player をサイレントにインストールします。

例：
msiexec/i nbr2player_onprem.msi/qn を入力します。

ステップ 5 コンピュータを再起動します。

コマンドラインインターフェースを使用した Recording Player のサイレントアンインストール

管理者は、ユーザーのコンピュータにサインインして、サイレントモードで Recording Player をアンインストールできます。

ステップ 1 ユーザのコンピュータにサインインします。

ステップ 2 MSI パッケージをコンピュータのハードドライブにダウンロードします。

ステップ 3 Windows コマンドプロンプトを開きます。
Windows 7 および Windows Vista では、[管理者として実行] を使用して、プロンプトウィンドウを開く必要があります。

ステップ 4 MSI パッケージ onpremmc.msi のコンポーネントをすべてアンインストールするには、コマンド msiexec/inbr2player_onprem.msi/qn を入力します。

Microsoft Systems Management Server 2003 (SMS) を使用した CWMS アプリケーションのインストール

SMS 使用の際の、CWMS アプリケーションのサイレントインストールの限度

以下の制限は、Microsoft Systems Management Server 2003 (SMS)を使用するサイレントインストールに適用されます。

- SMS ユーザ毎モードはサポートされていません。
- SMS 管理者が WebEx 生産性向上ツールの機能を追加する場合、今までに機能をインストールしていなくても、管理者はまず **REMOVE** コマンドを実行し、次に **ADDSOURCE** コマンドを実行する必要があります。
- 管理者がパッケージを提供している間に、リモートデスクトップでユーザーがコンピュータにログオンした場合、そのユーザーは必ずコンピュータを再起動して、WebEx 生産性向上ツールの正常な動作を確認する必要があります。
- 複数展開は可能ですが、各ユーザーが資格情報を入力する必要があります。
- メンテナンスリリースを更新するか、新しいリリースにアップグレードする前に、ユーザーは Cisco WebEX 生産性向上ツールをアンインストールする必要があります。 アップグレードした後で、ユーザーに生産性向上ツールを手動でプッシュするか、ユーザーが[ダウンロード] ページから生産性向上ツールをダウンロードできます。

- Lync 統合を使用している場合は、サイレントインストールの後で、ユーザーはコンピュータを再起動して、すべてのインスタントメッセンジャーの統合が正常に動作するようにしなければなりません。

SMSシステム毎無人プログラムを使用するCiscoWebExネットワーク録画プレーヤーの提供

SMS 管理者であれば、以下の手順を実行し、SMS システム毎無人プログラムを使用して Cisco WebEx ネットワーク録画プレーヤーを提供できます。

はじめる前に

管理サイトにサインインして、ダウンロード設定で Cisco WebEx Meetings デスクトップアプリケーションをユーザのデスクトップにプッシュするよう設定します。 詳細は、Cisco WebEx Meetings Server 管理者ガイドの「ダウンロードの設定」のセクションを参照してください。

手順の概要

1. 定義からパッケージを作成します。 詳細については、定義からのパッケージの作成, （156 ページ）を参照してください。
2. 提供する前に、「システム毎無人」のプログラムオプションを変更してください。
3. これで、プログラムを提供できます。

手順の詳細

ステップ 1 定義からパッケージを作成します。 詳細については、定義からのパッケージの作成, （156 ページ）を参照してください。

ステップ 2 提供する前に、「システム毎無人」のプログラムオプションを変更してください。

a) SMS 管理者コンソールを起動し、[サイトデータベース]> [パッケージ]> [Cisco WebEx LLC Cisco WebEx Cisco WebEx ネットワーク録画プレーヤー英語版] > [プログラム] と選択します。

b) [システム毎無人プログラム] オプションを右クリックしてから、[プロパティ] を選択して [**システム毎無人プログラムのプロパティ**] ダイアログボックスを開きます。

c) [環境] タブを選択します。

- [プログラムの実行条件] オプションで、[ユーザがログオンしているときのみ] を選択します。
- [実行モード] オプションで、[管理者権限で実行する] を選択します。 [ユーザにこのプログラムの操作を許可する] を選択しないでください。

d) [全般]タブを選択します。

e) コマンドラインオプションに追加パラメータを追加して、WebEx Meetings アプリケーションの一部のオプションを指定します。

例：

例えば、最初のコマンドラインには次を入力します： msiexec /i "nbr2player_onprem.msi" /qn

ステップ 3 これで、プログラムを提供できます。

a) SMS 管理者コンソールを起動し、[サイトデータベース]> [パッケージ]> [Cisco WebEx LLC Cisco WebEx Cisco WebEx ネットワーク録画プレーヤー英語版] > [プログラム] と選択します。
b) [システム毎無人] を右クリックします。
c) [すべてのタスク] > [ソフトウェアの配布] を選択します。
d) [プログラムの配布ウィザード] で [**次へ**] をクリックします。
e) SMS サーバを選択し、[次へ] を選択します。
f) コレクションを選択し、[次へ] を選択します。
g) [名前] フィールドに提供名を入力し、[次へ] を選択します。
h) 提供をサブコレクションにも適用するかどうかを指定し、[次へ] を選択します。
i) いつプログラムを提供するかを指定し、[次へ] を選択します。
j) プログラムを割り当てるかどうかを指定し、[次へ] を選択します。
k) [プログラムの配布完了ウィザード] ページで [**完了**] を選択します。
l) \Site Database\System Status\Advertisement Status ディレクトリに移動し、提供ステータスを確認します。通知を有効にしていると、プログラムが提供された後、割り当てられたプログラムが実行されることを通知するメッセージがユーザに表示されます。 割り当てられたプログラムがサイレントモードで実行されます。

システム毎アンインストールプログラムを使用する Cisco WebEx ネットワーク録画プレーヤーのアンインストール

SMS 管理者であれば、以下の手順を実行し、SMS システム毎無人アンインストールプログラムを使用して Cisco WebEx ネットワーク録画プレーヤーをアンインストールできます。

手順の概要

1. 定義からのパッケージの作成, （156 ページ） で作成した SMS インストールパッケージを使用します。
2. システム毎アンインストールプログラムを提供して、Cisco WebEx ネットワーク録画プレーヤーをアンインストールします。

手順の詳細

ステップ 1 定義からのパッケージの作成, （156 ページ） で作成した SMS インストールパッケージを使用します。

ステップ 2 システム毎アンインストールプログラムを提供して、Cisco WebEx ネットワーク録画プレーヤーをアンインストールします。

Cisco WebEx ネットワーク録画プレーヤーは、指定したマシンからサイレントモードでアンインストールされます。

更新実行後の設定の再構成

Cisco WebEx Meetings Server（CWMS）ソフトウェアの更新実行後は、複数展開したアプリケーションへのパスを更新する必要があります。 アップデート完了後、録画を再生するために初めて使用するとき、Network Recording Player は自動的にアップデートされます。

Mac システムの場合、パスは `/Users/(Local User)/Library/Application Support/WebEx Folder/` です。

Windows システムの場合、パスはバージョン、ダウンロードタイプ、ウェブブラウザタイプにより異なります。

- Windows 7 および Windows Vista: <SystemDisk>\ProgramData\WebEx
- 生産性向上ツールまたは WebEx Connect から、お使いの生産性向上ツールまたは WebEx Connect のパスを使用してください。
- MSIインストールを使用している場合は、常に固有のパスを使用してください。既存のファイルは無視されます。
- Windows 7 のダウンロードタイプを使用している場合は、固有のパスが使用されます。Windows XP では、GPC が登録済みの表の値を見つけることができると、既存フォルダを使用します。 見つけられない場合は、上述のように、固有のパスを使用します。

Windows と Mac システムの両方のクライアントアプリケーションは、更新されたシステムとの互換性を維持するために自動的に更新されます。

ロックダウン環境では、Windows システムに対して手動で更新を実行する必要がありますが、Mac システムに対しては必要ありません。

（注） Cisco WebEx Meeting Server のバージョンと適合する生産性向上ツールと Meetings アプリケーションのバージョンはCisco WebEx Meetings アプリケーションおよび生産性向上ツール互換性マトリクス，（217 ページ）に記載されています。

第 7 章

シングルサインオンの概要

SAML 2.0 のようなフェデレーションシングルサインオン（SSO）基準は、固有の認証および認証システムを持つ異なるウェブサイト間で資格情報や関連情報を受け渡すための安全なメカニズムを提供します。 SAML 2.0 は OASIS Security Services Technical Committee により開発されたオープンスタンダードです。

SAML 2.0 プロトコルは金融サービス、上級教育、政府関連、その他の業界セグメントで急伸し、大きな成功を果たしてきました。 SAML 2.0 はすべての主要なウェブアクセス管理ベンダーにより実装されています。 U.S. Government General Services Administration（GSA）では、SAML 2.0 認定となるために、U.S. E-Authentication Identity Federation プログラムにすべてのベンダーが参加することが必要になります。

SAML 2.0 準拠のウェブサイトは、SAML アサーションを介してユーザーの資格情報を交換します。 SAML アサーションは、ユーザ名や権限などの課題に関する信頼されているステートメントを含む XML ドキュメントです。 SAML アサーションは、信頼性を確保するために、デジタル署名されています。

大企業の多くでは、たとえば、Identity Ping Federate, CA SiteMinder, Open AM, and Windows ADFS 2.0 などの統合された Identity and Access Management（IAM）および Identity Provider（IdP）システムを会社のイントラネットに展開しています。 これらの IAM と IdP システムは従業員とパートナーのためのユーザの認証と SSO 要件を処理します。 IAM および IdP システムは、ファイアウォールの外にあるパートナーのウェブサイトを相互運用するために、SAML プロトコルを使用します。 ユーザーは IAM と IdP システムを利用して、Cisco WebEx ミーティングサービスにユーザーを自動的に認証します。 これにより、ユーザはユーザ名とパスワードを記憶して、Cisco WebEx サイトでミーティングを開始したり、参加する必要がないため、効率が向上します。

（注） WebEx Meetings Server は SAML 2.0 IdP のみをサポートしています。 これは、古い SAML 1.1 および WS-Federate 標準に基づく IdP をサポートしていません。 この制限は SAML 1.1 および WS-Federate を引き続きサポートするクラウドベースの Cisco WebEx ミーティング サービスと対照的です。 以下は、Cisco WebEx Meetings Server とうまく機能することが確認されている SAML 2.0 IdP のリストです。

- Microsoft ADFS 2.0 (Microsoft Windows Server 2008/Windows Server 2008 R2、または Windows Server 2012のAD FS サーバーロール用の無料アドオン)
- Microsoft ADFS 3.0（Windows Server 2012 の AD FS サーバーロール）
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

SAML 2.0 はオープンスタンダードなので、他の SAML 2.0 IdP も Cisco WebEx Meetings Server と共に動作する可能性があります。 しかし、Cisco は他の SAML 2.0 IdP を検証していません。 ですから、統合が機能することを確認することは、管理者の責任になります。

- シングルサインオンの利点，168 ページ
- SAML 2.0 シングルサインオンの設定の概要，169 ページ
- エンドユーザと管理用のサインインのための SAML SSO，170 ページ
- クラウドベースの WebEx ミーティングサービスと WebEx Meetings Server の間の SAML 2.0 シングルサインオンの違い，171 ページ
- SAML アサーション属性，177 ページ

シングルサインオンの利点

シングルサインオン（SSO）は以下のようにしてメリットがあります。

- 簡素化されたユーザー認証 — 開梱した時点で Cisco WebEx Meetings Server で、ユーザーはメールと Meetings Server システムに対して自分で選択したパスワードを使用してサインインする必要があります。 このアプローチでは、ほとんどの中小規模組織に対してうまく機能する一方で、大企業組織はセキュリティを強化するために、ユーザー認証をActive Directoryなど、会社の資格情報を使用するほうが好まれます。 この目標は SAML 2.0 SSO を使用することで達成できます。

（注） 安全な認証—SSO パスワードはユーザー認証後は決してCisco WebEx Meetings Server に送信または保管されません。

- 簡素化されたユーザ管理–通常の摩擦のために常に労働力が変化する大規模組織では、WebEx Meetings Serverを統合するときに、ユーザ管理のプロセスを自動化することを好みます。 このことは、以下を自動化することを意味します。
  - 従業員が組織に参加したときのユーザアカウントの作成
  - 従業員が組織内で別の役割を割り当てられたときのユーザアカウントの更新
  - 従業員が組織を退職したときのユーザアカウントの無効化

  これらのイベントの自動化は、Cisco WebEx Meetings Server 管理サイトの SSO セクションの 自動アカウント作成 および 自動アカウント更新 を設定することで行うことができます。 SAML IdPによってもサポートされる場合、これらの機能をオンにすることをお勧めします。 ユーザーが認証すると、「オンデマンド」でユーザーアカウントが自動的に作成されアップデートされ、ユーザーアカウントを手動で作成する必要がありません。 同様に、ユーザーは組織を退職した後にアカウントにサインインできなくなります。SAML 2.0 IdP はこれらのユーザーが基礎となる法人ディレクトリーのプロキシであるデータベースから削除された後でサインインできないようにブロックするためです。

SAML 2.0 シングルサインオンの設定の概要

重要 自分自身または所属組織の他の人がSAML 2.0 シングルサインオン（SSO）の経験がない限り、資格のある Cisco AUC パートナーまたは Cisco Advanced Services のサービスをご利用になることをお勧めします。 SAML SSO 設定はかなり複雑なため、このようにお勧めします。

注意 SAML応答に、いずれかのフィールドでキャリッジリターンがある場合、アップデート、アカウント作成、認証が失敗します。 SAML プロバイダはキャリッジリターンを含むデジタル署名を計算しますが、Cisco WebEx Meetings Server はデジタル署名が無効となるキャリッジリターンを削除しま

SAML 2.0 SSO の設定については、以下の手順を見直してください。

1. SAML 2.0 SSO インフラストラクチャが導入されていて、会社のディレクトリに組み込まれていることを確認してください。 このことは、SAML 2.0 IdP ソフトウェアと SSO 認証ウェブサイトのセットアップを意味します。 認証ウェブサイトは、ユーザが法人の資格情報を入力するポータルです。
2. ユーザが SSO 認証ウェブサイトにアクセスできることを確認します。 この手順は重要です。 サインプロセスの一部として、Cisco WebEx Meetings Server はユーザを認証ウェブサイトにリダイレクトするからです。

（注） Cisco WebEx Meetings Server システムでパブリック アクセスが有効になっていて、ユーザーがインターネットからミーティングにサインインし、参加できる場合、SSO認証ウェブサイトもまたインターネットからアクセスできることを確認することが重要です。 このことは、DMZ で SAML 2.0 IdP を展開することを意味します。 この追加ステップを踏まないと、ユーザーがインターネットから Cisco WebEx Meetings Server にサインインするときに、「404 site not found」エラーが表示されます。

3 これらの両方の方法を使用して、WebEx Meetings Server を SAML 2.0 IdP に接続します。

- Cisco WebEx Meetings Server 管理サイトで、 [設定] > [セキュリティ] > [統合 SSO] を選択し、 IdP パラメータを設定します。 （「Cisco WebEx Meetings Server 管理者ガイド」の *[統合シングルサインオン（SSO） 設定]* セクションを参照してください。）
- SAML 2.0 IdP ドキュメントの指示に従ってください。 これらの指示はベンダーによって変わります。 これは、資格のある Cisco AUC パートナーに連絡するか Cisco Advanced Services のサービスをご利用になることをお勧めするもう 1 つの理由であります。

（注） SAML 2.0 IdPD の設定には Cisco Developer Network の指示を使わないでください。 それらの指示はクラウドベースの Cisco WebEx 用であり、Cisco WebEx ミーティングサーバー向けではありません。

エンドユーザと管理用のサインインのための SAML SSO

SAML SSO はサインインの目的のみのために、通常管理サイトではなく、エンドユーザのサイトで構成されます。 SAML 2.0 SSO が組み込まれている Cisco WebEx Meetings Server サイトでは、ユーザ認証に関して SaaS WebEx の動作に酷似しています。 Cisco WebEx Meetings Server 管理者（および SaaS WebEx 管理者）は SAML SSO を使用してエンドユーザアカウントにサインインできますが、別のパスワードを使用して同じシステムにある管理者アカウントにサインインする必要があります。 これは SAML SSO iDP における致命的な失敗の発生時に、それでも管理者が管理サイトにアクセスできることを保証します。 このフェールセーフがないと、管理サイトが製品の障害でなく、SAML SSO IdP ソフトウェアの問題によってアクセス不可になるという状況に遭遇する可能性があります。 SAML SSO IdP ソフトウェアは Cisco WebEx Meetings Server（または SaaS WebEx）の外部にあるサーバにあるため、コントロールできません。

クラウドベースの WebEx ミーティングサービスと WebEx Meetings Server の間の SAML 2.0 シングルサインオンの違い

クラウドベースの Cisco WebEx ミーティング サービスはユーザ アカウントを作成するときに固有のユーザ ID を採用する一方で、Cisco WebEx Meetings Server はユーザ アカウントを作成するための基礎としてメールアドレスを使用します。 SAML 2.0 シングルオン（SSO）を展開するときに、クラウドベースの Cisco WebEx ミーティングサービスは、自動アカウント作成がオンのときに、UPN（ユーザープリンシパルネーム）から「@cisco.com」のようなメールドメインの削除を許可することにご注意ください。 これにより、ユーザー ID を基にしたユーザーアカウントが作成されます。 WebEx Meetings Server が完全なメールアドレスを使用して、ユーザーアカウントを作成するため、UPN からはメールのドメインを削除できません。

ID プロバイダ (IdP) サーバーは任意の一意な Active Directory (AD) フィールドを SSO 構成用の NameID として使用することができます。 SSO を使用して、アクティブ ユーザー用の電子メールアドレスを変更する場合、IdP サーバーでの NameID フィールドのマッピング変更します。

クラウドベースの Cisco WebEx ミーティング サービスはユーザ アカウントを作成するときに固有のユーザ ID を採用する一方で、Cisco WebEx Meetings Server はユーザ アカウントを作成するための基礎としてメールアドレスを使用します。 これは、SAML 2.0 シングルサインオン（SSO）にとって、以下の重要な要素があります。

- NameID フィールドにメールアドレスを入力することが SAML アサーションで必須になります。 このパラメータなしでは、ユーザー認証とアカウント作成は失敗します。Cisco WebEx Meetings Server は関連するメールアドレスなしで、ユーザーアカウントを作成することを許可しないためです。
- クラウドベースの Cisco WebEx ミーティングサービスは、自動アカウント作成がオンのときに、UPN（ユーザープリンシパルネーム）から「@cisco.com」のようなメールドメインの削除を許可します。 これにより、ユーザーIDを基にしたユーザーアカウントが作成されます。 WebEx Meetings Server が完全なメールアドレスを使用して、ユーザーアカウントを作成するため、UPN からはメールのドメインを削除できません。

Cisco WebEx Meetings サーバーをSAML 2.0 SSO なしで展開でき、展開後 SSO をオンにします。それを行うことは、次のようなユーザ認証、自動アカウント作成、自動アカウント更新機能への重要な影響があります。

シナリオ	ユーザ認証の動作	自動アカウント作成（AAC）オン	AAC オフ	アカウントの自動更新（AAU）オン	AAU オフ
SSO がオン状態ではありません。 ユーザーアカウントが CWMS システムで作成されました。	ユーザーはメールアドレスと自分で選択したパスワードを使用してサインインします。	該当せず	該当せず	該当せず	該当せず
SSO をオンにします。既存のアカウントを持つユーザーは、WebEx サイト、WebEx 生産性ツールまたは Cisco WebEx Meetings アプリに、モバイルデバイスでサインインします。	ユーザーは SAML 2.0 IdP 認証ウェブサイトへリダイレクトされ、自分のパスワードの代わりに企業認証情報を使ってサインインします。 有効なユーザーではない場合、SAML 2.0 IdP により WebEx Meetings Server を使用できないか、無効なユーザーであることを通知されます。	該当せず	該当せず	該当せず	該当せず

シナリオ	ユーザ認証の動作	自動アカウント作成（AAC）オン	AAC オフ	アカウントの自動更新（AAU）オン	AAU オフ
SSO がオン状態です。 ユーザはシステムに既存のアカウントをもっていません。	前のシナリオと同じです。	Cisco WebEx Meetings Server のユーザーアカウントは、ユーザーがサインインした後で、「オンデマンド」で作成されます。 前提条件: SAML アサーションが NameID フィールドで有効なメールアドレスが含まれている。	システムにアカウントを持たないユーザーがサインインでき、Cisco WebEx 以外にはアクセスできません。この状況を直すには： • AAC をオンにしたままにする。 • ユーザーアカウントを手動で作る。	該当せず	該当せず
SSO がオン状態です。前に SSO を使用したユーザーが再びサインインします。	「SSOをオンにします」シナリオと同様。	該当せず	該当せず	既存のユーザーアカウントは、NameID に変更がない限りは、その他の変更で自動的にユーザー認証情報に対して更新されます。	該当せず

シナリオ	ユーザ認証の動作	自動アカウント作成（AAC）オン	AAC オフ	アカウントの自動更新（AAU）オン	AAU オフ
SSOをオフにします。（あまりないシナリオです。） 前に SSO を使用したユーザーが再びサインインします。	ユーザーが企業の認証情報を入力すれば、Cisco WebEx はユーザーのメールアドレスと自分で選択したパスワードの入力を予測するため、サインインできません。この状況では、ユーザーに WebEx アカウントで自分で選択したパスワードをリセットする方法を教え、SSO をオフにする前に十分な時間を与えてください。 パスワードをリセットした後で、ユーザーはメールアドレスと自分で選択したパスワードを使用してサインインできます。	該当せず	該当せず	該当せず	該当せず

シナリオ	ユーザ認証の動作	自動アカウント作成（AAC）オン	AAC オフ	アカウントの自動更新（AAU）オン	AAU オフ
特殊ケース: ユーザはシステム管理者でもあります。 シナリオ A: ユーザは WebEx サイトにサインインします。 シナリオ B: ユーザはCisco WebEx 管理者サイトにサインインします。		シナリオ A: 前のシナリオと同じ結果です。 シナリオ B: 該当なし	シナリオ A: 前のシナリオと同じ結果です。 シナリオ B: 該当なし	シナリオ A: 前のシナリオと同じ結果です。 シナリオB: 該当なし	シナリオ A: 前のシナリオと同じ結果です。 シナリオB: 該当なし

シナリオ	ユーザ認証の動作	自動アカウント作成（AAC）オン	AAC オフ	アカウントの自動更新（AAU）オン	AAU オフ
	シナリオ A: 前のシナリオと同じ結果です。 シナリオ B: ユーザーが Cisco WebEx 管理サイトにサインインすると、ユーザーは常にメールアドレスと自分で選択したパスワードの入力を促されます。SSOはユーザーが Cisco WebEx 管理サイトにサインインした時に影響がありません。 これは製品に組み込まれたセキュリティ対策です。 これにより、システム管理者は常に Cisco WebEx 管理サイトにサインインできます。 Cisco WebEx 管理サイトも SSO をサポートする場合、SAL 2.0 IdP の誤作動または Cisco WebEx Meetings Server と SAML 2.0 IdP の間のネットワーク接続の損失は、シ				

シナリオ	ユーザ認証の動作	自動アカウント作成（AAC）オン	AAC オフ	アカウントの自動更新（AAU）オン	AAU オフ
	ステム管理者はサインインして製品を管理できなくなる状況をもたらす恐れがあります。				

SAML アサーション属性

以下のテーブルでは、Cisco WebEx Meetings Server によってサポートされている SAML アサーション属性がリストされています。 `lastname`、`firstname`、`email`、および `updatetimestamp` 属性を必ず構成してください。 `updatetimestamp` 属性が構成されていない限り、自動更新は機能しません。

サポートされている SAML アサーション属性

属性名	属性の意味	ユーザの自動作成で必須	入力値の範囲	コメント
lastname		はい		
firstname		はい		
Email		はい	有効なメール形式	SSO 設定でアカウント自動作成とアカウント自動更新が無効にされている場合も含めて、常に必要です。

属性名	属性の意味	ユーザの自動作成で必須	入力値の範囲	コメント
updatetimestamp	ユーザ情報のアップデート時間	いいえ	サポートされる形式 **長い形式**： サンプル：System.currentTimeMillis() **LDIF 形式**： yyyyMMddHHmmss yyyy-MM-dd HH:mm:ss サンプル：20090115213256 **UTC 形式** ("2009-10-09T06:00:32Z")	updateTimeStamp が欠落していると、IdP が AD にリンクされている場合に通常 whenChanged 項目にマッピングされているユーザの自動更新が実行できません。
optionalparams		いいえ		オプションのパラメーター，（181 ページ）を参照してください。
OPhoneCountry		いいえ		事務所電話国コード
OPhoneArea		いいえ		事務所電話市外局番
OPhoneLocal		いいえ	数字のみを入力します。たとえば、5551212。ダッシュやかっこなど数字以外を入力しないでください。	事務所電話市内番号
OPhoneExt		いいえ		事務所電話内線番号
FPhoneCountry		いいえ		代替電話国コード
FPhoneArea		いいえ		代替電話エリア
FPhoneLocal		いいえ		代わりの市内番号

属性名	属性の意味	ユーザの自動作成で必須	入力値の範囲	コメント
FPhoneExt		いいえ		代替内線番号
PPhoneCountry		いいえ		代替電話 2 国コード
PPhoneArea		いいえ		代替電話 2 市外局番
PPhoneLocal		いいえ		代替電話 2 市内番号
PPhoneExt		いいえ		代替電話 2 内線番号
MPhoneCountry		いいえ		携帯電話国コード
MPhoneArea		いいえ		携帯電話のエリア
MPhoneLocal		いいえ		ローカルの携帯電話
MPhoneExt		いいえ		携帯電話拡張機能
TimeZone		いいえ		タイムゾーン値, （181 ページ）を参照してください。
Address1		いいえ		Address1
Address2		いいえ		Address2
City		いいえ		City
State		いいえ		State
ZIP Code		いいえ		ZIP Code
Country		いいえ		国番号, （185 ページ）を参照してください。

属性名	属性の意味	ユーザの自動作成で必須	入力値の範囲	コメント
地域		いいえ		地域の値, （195 ページ）を参照してください。
LANGUAGE		いいえ		言語の値, （196 ページ）を参照してください。
TC1	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 1	インデックス 1
TC2	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 2	インデックス 2
TC3	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 3	インデックス 3
TC4	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 4	インデックス 4
TC5	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 5	インデックス 5
TC6	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 6	インデックス 6
TC7	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 7	インデックス 7

属性名	属性の意味	ユーザの自動作成で必須	入力値の範囲	コメント
TC8	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 8	インデックス 8
TC9	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 9	インデックス 9
TC10	文字列	いいえ	管理サイトのユーザーが入力したトラッキングコードグループ 10	インデックス 10

オプションのパラメーター

以下の通りに、optionalparams を設定できます。

- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="optionalparams">
- <saml:AttributeValue xsi:type="xs:string">市=トロント</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=オフ</saml:AttributeValue >
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="City">
- <saml:AttributeValue xsi:type="xs:string">トロント</saml:AttributeValue>
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="AA">
- <saml:AttributeValue xsi:type="xs:string">オフ</saml:AttributeValue>

タイムゾーン値

タイムゾーン	値
マーシャル諸島（日付変更線標準時、GMT-12:00）	0
サモア（サモア時間、GMT-11:00）	1

タイムゾーン	値
ホノルル（ハワイ時間、GMT-10:00）	2
アンカレッジ(アラスカ夏時間、GMT-08:00)	3
サンフランシスコ（太平洋夏時間、GMT-07:00）	4
アリゾナ（山地時間、GMT-07:00）	5
デンバー（山地夏時間、GMT-06:00）	6
シカゴ（中部夏時間、GMT-05:00）	7
メキシコシティ（メキシコ夏時間、GMT-05:00）	8
サスカチュワン（中部時間、GMT-06:00）	9
ボゴタ (アメリカ太平洋時間、GMT-05:00)	10
ニューヨーク（東部夏時間、GMT-04:00）	11
インディアナ（東部夏時間、GMT-04:00）	12
ハリファックス（大西洋夏時間、GMT-03:00）	13
ラバス (南アメリカ太平洋時間、GMT-04:00)	14
ニューファンドランド（ニューファンドランド夏時間、GMT-02:30）	15
ブラジリア (アメリカ東部標準時間、GMT-03:00)	16
ブエノスアイレス (アメリカ東部時間、GMT-03:00)	17
中部大西洋（中部大西洋時間、GMT-02:00）	18
アゾレス諸島（アゾレス夏時間、GMT）	19
レイキャビク（グリニッジ時間、GMT）	20
ロンドン（GMT 夏時間、GMT+01:00）	21
アムステムダム（ヨーロッパ夏時間、GMT+02:00）	22

タイムゾーン	値
パリ（ヨーロッパ夏時間、GMT+02:00）	23
ベルリン（ヨーロッパ夏時間、GMT+02:00）	25
アテネ（ギリシャ夏時間、GMT+03:00）	26
カイロ（エジプト時間、GMT+02:00）	28
プレトリア（南アフリカ時間、GMT+02:00）	29
ヘルシンキ（北ヨーロッパ夏時間、GMT+03:00）	30
テルアビブ（イスラエル夏時間、GMT+03:00）	31
リヤド（サウジアラビア時間、GMT+03:00）	32
モスクワ（ロシア時間、GMT+04:00）	33
ナイロビ（ナイロビ時間、GMT+03:00）	34
テヘラン（イラン夏時間、GMT+04:30）	35
アブダビ、マスカット（アラビア時間、GMT+04:00）	36
バクー（バクー夏時間、GMT+05:00）	37
カブール（アフガニスタン時間、GMT+04:30）	38
エカテリンブルグ（西アジア時間、GMT+06:00）	39
イスラマバード（西アジア時間、GMT+05:00）	40
ムンバイ（インド時間、GMT+05:30）	41
コロンボ（コロンボ時間、GMT+05:30）	42
アルマトイ（中央アジア時間、GMT+06:00)）	43
バンコク（バンコク時間、GMT+07:00）	44
北京（中国時間、GMT+08:00）	45

タイムゾーン	値
パース（オーストラリア西部時間、GMT+08:00）	46
シンガポール（シンガポール時間、GMT+08:00）	47
台北（台北時間、GMT+08:00）	48
東京（日本時間、GMT+09:00）	49
ソウル（韓国時間、GMT+09:00）	50
ヤクーツク（ヤクーツク時間、GMT+10:00）	51
アデレード（オーストラリア中部標準時、GMT+09:30）	52
ダーウィン（オーストラリア中部時間、GMT+09:30）	53
ブリスベン（オーストラリア東部時間、GMT+10:00）	54
シドニー（オーストラリア東部標準時、GMT+10:00）	55
グアム（西太平洋時間、GMT+10:00）	56
ホバート（タスマニア標準時、GMT+10:00）	57
ウラジオストク（ウラジオストク時間、GMT+11:00）	58
ソロモン諸島（中央太平洋時間、GMT+11:00）	59
ウェリントン（ニュージーランド標準時、GMT+12:00）	60
フィジー（フィジー時間、GMT+12:00）	61
ストックホルム（スウェーデン夏時間、GMT+02:00）	130
ティファナ（メキシコ太平洋夏時間、GMT-07:00）	131

タイムゾーン	値
チワワ（メキシコ山地夏時間、GMT-06:00）	132
カラカス (南アメリカ太平洋時間、GMT-04:30)	133
クアラルンプール（マレーシア時間、GMT+08:00）	134
レシフェ (アメリカ東部時間、GMT-03:00)	135
カサブランカ（モロッコ夏時間、GMT+01:00）	136
テグシガルパ（ホンジュラス時間、GMT-06:00）	137
ヌーク（グリーンランド夏時間、GMT-02:00）	138
アンマン（ヨルダン夏時間、GMT+03:00）	139
イスタンブール（東ヨーロッパ夏時間、GMT+03:00）	140
カトマンズ（ネパール時間、GMT+05:45）	141
ローマ（ヨーロッパ夏時間、GMT+02:00）	142
西アフリカ（西アフリカ時間、GMT+01:00）	143
マドリード（ヨーロッパ夏時間、GMT+02:00）	144

国番号

Country	コード
アフガニスタン	93
アルバニア	355
アルジェリア	213
サモア	1684
アンドラ	376
アンゴラ	244

Country	コード
アングイラ	1264
南極大陸	672_1
アンチグア（バーブーダを含む）	1268
アルゼンチン	54
アルメニア	374
アルーバ	297
アセンション島	247
オーストラリア	61
オーストリア	43
アゼルバイジャン	994
バハマ	1242
バーレーン	973
バングラディッシュ	880
バルバドス	1246
ベラルーシ共和国	375
ベルギー	32
ベリーズ	501
ベニン共和国	229
バミューダ	1441
ブータン	975
ボリビア共和国	591
ボスニアヘルツェゴヴィナ	387
ボツワナ	267

Country	コード
ブラジル	55
英領バージン諸島	1284
ブルネイ	673
ブルガリア	359
ブルキナソファ	226
ブルンジ共和国	257
カンボジア	855
カメルーン共和国	237
カナダ	1_1
ケープベルデ島	238
ケーマン諸島	1_9
中央アフリカ共和国	236
チャド共和国	235
チリ	56
中国	86
コロンビア	57
コモロ	269_1
クック諸島	682
コスタ・リカ	506
クロアチア	385
キューバ	53
サイプラス	357
チェコ共和国	420

Country	コード
デンマーク	45
ディエゴ・ガルシア	246
ジブティ共和国	253
ドミニカ	1767
ドミニカ共和国	1809
エクアドル	593
エジプト郊外カイロ	20
エルサルバドール	503
赤道ギニア	240
エリトリア	291
エストニア	372
エチオピア	251
フェロー諸島	298
フォークランド島	500
フィージー諸島	679
フィンランド	358
フランス	33
フランス領 （インド洋）	262
仏領ガーナ	594
仏領ポリネシア	689
ガボン共和国	241
ガンビア	220
グルジア	995

Country	コード
ドイツ	49
ガーナ	233
ジブラルタル	350
ギリシャ	30
グリーンランド	299
グレナダ	1473
グアドループ	590
グアンタナモ(米軍基地)	53_1
ガテマラ	502
ギニア共和国	224
ギニアビソー	245
ガイアナ	592
ハイチ	509
ホンジュラス	504
香港	852
ハンガリー	36
アイスランド	354
インド	91
インドネシア	62
イラン	98
イラク	964
アイルランド	353
イスラエル	972

Country	コード
イタリア	39_1
コートジボアール共和国	225
ジャマイカ	1876
日本	81
ヨルダン	962
カザフスタン	7_1
ケニア	254
キリバス	686
北朝鮮	850
大韓民国	82
クウェート	965
キルギスタン	996
ラオス	856
ラトビア	371
レバノン	961
レソト王国	266
リベリア共和国	231
リビア	218
リヒテンシュタイン公国	423
リトアニア	370
ルクセンブルグ	352
マカオ	853
マセドニア共和国	389

Country	コード
マダガスカル	261
マラウイ共和国	265
マレーシア	60
モルディブ	960
マリ共和国	223
マルタ共和国	356
マーシャル諸島	692
モーリタニア	222
モーリシャス	230
マヨット島	269
メキシコ共和国	52
ミクロネシア	691
モルドバ	373
モナコ	377
モンゴル	976
モンセラト	1664
モロッコ	212
モザンビーク	258
ミャンマー	95
ナミビア	264
ナウル	674
ネパール	977
オランダ	31

Country	コード
オランダ領アンティ―ル	599_2
ニューカレドニア	687
ニュージーランド	64
ニカラグア	505
ニジェール共和国	227
ニウエ島	683
ノーフォーク島	672
北マリアナ諸島	1670
ノルウェイ	47
オマーン	968
パキスタン	92
パラオ	680
パナマ共和国	507
パプア・ニューギニア	675
パラグアイ	595
ペルー	51
フィリピン	63
ポーランド	48
ポルトガル	351
プエルトリコ	1787
カタール	974
ルーマニア	40
ロシア	7

Country	コード
ルワンダ	250
サンマリノ	378
サントメ	239
サウジアラビア	966
セネガル共和国	221
セルビア	381
セイシェル諸島	248
シエラ・レオーネ	232
シンガポール	65
スロバキア	421
スロベニア	386
ソ\ロモン諸島	677
ソマリア	252
南アフリカ	27
スペイン	34
スリランカ	94
セントヘレナ	290
セントキッツアンドネヴィス	1869
セントルチア	1758
セントピエールアンドミグエロン	508
セントビンセント	1784
スーダン	249
スリナム共和国	597

Country	コード
スワジランド王国	268
スウェーデン	46
スイス	41
シリア	963
台湾	886
タジキスタン	992
タンザニア	255
タイ	66
トーゴー	228
トンガ諸島	676
トリニダッド・トバゴ共和国	1868
チュニジア	216
トルコ	90
トルクメニスタン	993
タークス・カイコス諸島	1649
トゥヴァル	688
ウガンダ	256
ウクライナ	380
アラブ首長国連邦	971
英国（グレートブリテンおよび北部アイルランド連合王国）	41
アメリカ	1
ウルグアイ	598

Country	コード
ウズベキスタン	998
バヌアツ共和国	678
バチカン市国	39
ベネゼエラ	58
ベトナム	84
ワリス・フテュナ諸島	681
西サモア	685
イエメン	967
ザミビア	260
ジンバブエ	263

地域の値

地域	値
米国	2
オーストラリア	3
カナダ	4
フランス語	5
中国	6
フランス	7
ドイツ	8
香港	9
イタリア	10
日本	11

地域	値
韓国	12
ニュージーランド	13
スペイン	14
スイス	15
台湾	16
英国（グレートブリテンおよび北部アイルランド連合王国）	17
メキシコ共和国	18
アルゼンチン	19
チリ	20
コロンビア	21
ベネゼエラ	22
ブラジル	23
ポルトガル	24
ベルギー	25
オランダ	26
ロシア	28
インド	29

言語の値

LANGUAGE	値
カステリョン系スペイン語	11
オランダ語	14

LANGUAGE	値
日本語	1
フランス語	7
ドイツ語	9
イタリア語	10
日本語	5
韓国語	6
ラテンアメリカ系スペイン語	12
ポルトガル語	15
ロシア語	16
簡体字中国語	3
繁体字中国語	4

言語コード

LANGUAGE	国番号
カステリョン系スペイン語	34
中国語	852, 853, 886
オランダ語	31, 32
フランス語	33, 242, 243
ドイツ語	41, 43, 49
イタリア語	39
日本語	81
韓国語	82
ラテンアメリカ系スペイン語	52, 54, 56, 57, 58,

LANGUAGE	国番号
中国標準語	86
ポルトガル語	55, 351
ロシア語	7
イギリス英語	44, 61, 64, 91
米国英語	1

第 8 章

ミーティング録画のためのストレージ要件

任意の容量のストレージサーバを設定できます。 保存されたCisco WebEx ミーティング録画の数は、構成された記憶容量の合計に依存します。

ユーザーが削除する録画をマークすると、ユーザーインターフェースから直ちに利用できなくなります。 これは3～6ヶ月間ストレージに保存されます。 このため、録画はコピーやバックアップができ、ユーザーが削除のマークを付けていても6ヶ月間は使用できます、（ユーザーがうっかり録画を Cisco WebEx Meeting Recordings ページから削除してしまったものの、録画はNetwork File System （NFS） ストレージサーバーに保存されている場合、Cisco テクニカルアシスタンスセンター（TAC）に連絡して録画を復旧する必要があります。

システム上の録画が3ヶ月間に割り当ての 75 □未満の使用であれば、録画は6ヶ月後に削除されます。 録画が3ヶ月間のいずれかの時点で割り当ての75 □を超えれば、システムは自動的にユーザーが削除設定した最初の 10 ファイルを削除します。

例えば、ユーザーが今日2つのファイルを削除することに決め、明日5つのファイルの削除を決め、 9つのファイルの削除を明後日決めます。 ストレージの使用が 75 □の値を超えていれば、システムは3か月後に最初の2ファイルを削除し、その次の日に次の5ファイルを、そのまた次の日に削除をマークした9つのふぁいるのうち最初の3ファイルを削除します。

組織がミーティングの録画を6ヶ月以上保存する必要があるなら、定期的に録画を他のメディアに保管します。

以下の表は1時間のミーティング録画に必要な記憶容量の合計に関する大体の見積もりを示しています。 これらの値は、6か月間のミーティング録画に必要な記憶容量の合計を見積もるのに役立ちます。

ミーティング内容	1 時間のミーティング録画に必要な大体の記憶容量
アプリケーション共有	36 MB
ボイス	30 MB
180p ビデオ	104 MB
360p ビデオ	337 MB

Webcam ビデオはミーティング録画の元の解像度で保存されます。 ただし、録画を再生する際は、ビデオの解像度は 180p ビデオに制限されます。

• システムバックアップファイル用ストレージ要件，200 ページ

システムバックアップファイル用ストレージ要件

ミーティング録画を除く、システムのバックアップに必要なストレージの、一般的に推奨される量は、最低 900 MB、または 3 つのバックアップファイルを保存するのに十分な容量です。 システムは古いバックアップファイルを消去し、最新のバックアップだけを保存します。

バックアップに必要なストレージスペースを決める際の配慮：

- ユーザー数
- 各日に開催されるミーティングの平均数
- 時間と共に増加するデータベースのサイズ
- HA の展開時、ネットワークの遅延、またはデータ複製中の高いシステム負荷によって、トランザクションジャーナルの転送が送れることがあります。 これによって、バックアップファイルのサイズが増加する可能性があります。

ダッシュボードはシステムバックアップのおよそのストレージ要件を示します。 ストレージサーバー上に、監視されるバックアップサイズの最低 3 倍の十分な保存領域を確保します。

第 9 章

サポートされている SNMP MIB

SNMP MIB ftp://ftp.cisco.com/pub/mibs/v2/CISCO-WBX-MEETING-MIB.my が Cisco WebEx Meetings Server によりサポートされています。 すべての MIB 変数が Cisco WebEx Meetings サーバーまたはすべての Cisco WebEx Meetings サーバー展開タイプに適用できるわけではありません。 例えば、MIB に関するデータセンター は Cisco WebEx Meetings サーバーシステムに適用しません。

- CWMS システム情報 MIBS，201 ページ
- CPU 関連の MIB，202 ページ
- CWMS メモリ情報，205 ページ
- ディスク使用率，206 ページ
- サポートされている SNMP トラップ，207 ページ

CWMS システム情報 MIBS

オブジェクト[22]	OID	説明
cwCommSystemVersion タイプ: 文字列	.1.3.6.1.4.1.9.9.809.1.1.1	Cisco WebEx システムバージョン
cwCommSystemObjectID タイプ: 匿名	.1.3.6.1.4.1.9.9.809.1.1.2	SNMPv2-MIB での定義通りの sysObjectID。

22 この表のすべてのオブジェクトがリードオンリー（RO）です。

CPU 関連の MIB

オブジェクト	読み込み/書き込み権限	OID	説明
cwCommCPUTotalUsage タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.1	ホスト部分による CPU 使用の割合。 合計 CPU 使用率の割合には、CPU ユーザー使用率、CPU システム使用率、および CPU nice 使用率が含まれています。CPU ユーザー時間 ユーザースペースで消費された CPU 時間 CPU システム時間 カーネルスペースで消費された CPU 時間 CPU nice時間 低優先度プロセスで消費された CPU 時間
cwCommCPUUsageWindow タイプ: Gauge32。	RW	.1.3.6.1.4.1.9.9.809.1.2.1.2	通知（トラップ）前の時間（秒）は CPU 使用が通常□マイナー/メジャー閾値を越え新しい閾値にあると示して送信されます。
cwCommCPUTotalNumber タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.3	システム上の CPU の数
cwCommCPUUsageTable タイプ: 該当せず	アクセスできません	.1.3.6.1.4.1.9.9.809.1.2.1.4	デバイスの CPU 使用率登録のリスト
cwCommCPUIndex タイプ: 署名なし	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.1	独自の CPU 識別子 すべての CPU には、それぞれの使用率およびブレークダウン値があります。

オブジェクト	読み込み/書き込み権限	OID	説明
cwCommCPUName タイプ: 文字列	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.2	CPU 名 たとえば、Intel(R) Xeon(TM) CPU 3.00GHz。
cwCommCPUUsage タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.3	使用している CPU リソース合計の割合 GHz は通常、CPU 性能を測るために使用されます。 GHz は、CPU 使用率カテゴリを測るためには大きすぎるため、KHz が測定単位として使用されます。 システム速度（KHz）は、各カテゴリの CPU KHz を獲得するそれぞれの CPU セクションの種類別に（たとえば、idle、nice、user）増えます。KHz は表内のすべての CPU カテゴリを測定する単位として使用されます。
cwCommCPUUsageUser タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.4	ユーザーモードで実行される CPU 電力。

オブジェクト	読み込み/書き込み権限	OID	説明
cwCommCPUUsageNice タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.5	低優先度プロセスで実行された CPU 時間 nice は UNIX と Linux にあるプログラムです。それは同じ名前のカーネルコールに直接マッピングされます。 Nice は、プロセスに他のプロセスより多いまたは少ない CPU 時間を与える、特定の優先度を持つユーティリティまたはシェルスクリプトを呼び出すために使用されます。
cwCommCPUUsageSystem タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.6	カーネルモードで実行される CPU 電力
cwCommCPUUsageIdle タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.7	アイドル状態での CPU 電力
cwCommCPUUsageIOWait タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.8	ディスク出入量の完了待機時に使用される CPU 電力。
cwCommCPUUsageIRQ タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.9	中断リクエスト処理時に使用される CPU 電力。
cwCommCPUUsageSoftIRQ タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.10	ソフトウェア中断処理時に使用される CPU 電力。
cwCommCPUUsageSteal タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.11	仮想環境で実行時に他のタスクに使用される CPU 電力。
cwCommCPUUsageCapacitySubTotal タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.12	現在の総 CPU 電力。

オブジェクト	読み込み/書き込み権限	OID	説明
cwCommCPUMonitoringStatus タイプ: 文字列	RO	.1.3.6.1.4.1.9.9.809.1.2.1.5	CPU リソースのモニタリング状況： • closed（0）-リソースは使用できません。 • open（1）-リソースは使用できます。
cwCommCPUCapacityTotal タイプ: Gauge32。	RO	.1.3.6.1.4.1.9.9.809.1.2.1.6	全体の CPU 容量。

CWMS メモリ情報

オブジェクト[23]	OID	説明
cwCommMEMUsage タイプ: Gauge32。	.1.3.6.1.4.1.9.9.809.1.2.2.1	仮想マシンの物理メモリ使用。
cwCommMEMMonitoringStatus タイプ: 文字列	.1.3.6.1.4.1.9.9.809.1.2.2.2	メモリリソースのモニタリングステータス： closed（0）-リソースは使用できません。 open（1）-リソースは使用できます。
cwCommMEMTotal タイプ: Gauge32。	.1.3.6.1.4.1.9.9.809.1.2.2.3	主催者の総物理メモリサイズ（KB）。
cwCommMEMSwapUsage タイプ: Gauge32。	.1.3.6.1.4.1.9.9.809.1.2.3.1	物理メモリ使用（□）と主催者のスワップメモリ使用。

オブジェクト[23]	OID	説明
cwCommMEMSwapMonitoringStatus タイプ: 文字列	.1.3.6.1.4.1.9.9.809.1.2.3.2	このオブジェクトは、メモリとスワップメモリの監視ステータスを提供します。 closed (0)- メモリとスワップメモリステータスが使用できます。 closed (1)- メモリとスワップメモリステータスが使用できません。

23 この表のすべてのオブジェクトがリードオンリー（RO）です。

ディスク使用率

オブジェクト[24]	OID	説明
cwCommDiskUsageCount	.1.3.6.1.4.1.9.9.809.1.2.5.1	このオブジェクトはシステムで使用可能なディスク（たとえば、ローカルディスク、リモートディスク、ミーティング録画ディスク）の数を示します。
cwCommDiskUsageIndex	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.1	このオブジェクトは、ディスク使用固有の管理情報を含むテーブルにあるエントリのインデックスです。
cwCommDiskPartitionName	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.2	ディスクパーティション名。たとえば、/opt または/dev のパーティション。
cwCommDiskUsage	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.3	現在の主催者のディスク使用量（□）。
cwCommDiskTotal	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.4	主催者のディスクスペースサイズ（MB）。

オブジェクト[24]	OID	説明
cwCommDiskMonitoringStatus	1.3.6.1.4.1.9.9.809.1.2.5.3	ディスクリソースのモニタリング状況： closed (0)- ディスク使用率の状況は使用できません。 closed (1)- ディスク使用率の状況は使用できません。

24 この表のすべてのオブジェクトがリードオンリー（RO）です。

サポートされている SNMP トラップ

SNMP MIB トラップが Cisco WebEx Meetings Server によりサポートされています。

通知イベント

cwCommSystemResourceUsageNormalEvent (.1.3.6.1.4.1.9.9.809.0.1)

システムリソース使用が 通常 ステータスから変わったときの通知。 システムはこの通知をその際に送信できます：

- CPUの cwCommCPUUsage 値は、事前に定義された CPU Minor Threshold の値未満に変化します。
- cwCommMEMUsage の値は、事前に定義された MEM Minor Threshold の値未満に変化します。
- cwCommMEMSwapUsage の値は、事前に定義された MEM SwapMinor Threshold の値未満に変化します。
- cwCommFileUsage の値は、事前に定義された File Minor Threshold の値未満に変化します。
- ディスクのcwCommDiskUsage の値は、事前に定義された Disk Minor Threshold の値未満に変化します。

cwCommSystemResourceUsageMinorEvent (.1.3.6.1.4.1.9.9.809.0.2)

システムリソース使用が マイナー ステータスから変わったときの通知。 このマイナー通知は、システムに問題があり、システム管理者がそれを解決する必要があることを意味します。 システムはこの通知をその際に送信できます：

- CPUのcwCommCPUUsageの値は、事前に定義された CPU Minor Threshold の値以上、および cwCommCPUMajorThreshold の値未満に変化します。
- cwCommMEMUsage の値は、事前に定義された MEM Minor Threshold の値以上、および事前に定義された MEM Major Threshold の値未満に変化します。

- cwCommMEMSwapUsage の値は、事前に定義された MEM Swap Minor Threshold の値以上、および事前に定義された MEM Swap Major Threshold の値未満に変化します。
- cwCommFileUsage の値は、事前に定義された File Minor Threshold の値以上、および事前に定義された File Major Threshold の値未満に変化します。
- ディスクの cwCommDiskUsage の値は、事前に定義された Disk Minor Threshold の値以上、および事前に定義された Disk Major Threshold の値未満に変化します。

cwCommSystemResourceUsageMajorEvent (.1.3.6.1.4.1.9.9.809.0.3)

この通知は、システムリソース使用率がメジャーステータスに変化することを示します。 このメジャー通知は、システムが重大なステータスの状態であることを意味します。システム管理者が即座に対処する必要があります。 システムはこの通知をその際に送信できます：

- CPUの cwCommCPUUsage 値は、事前に定義された CPU Major Threshold の値以上に変化します。
- cwCommMEMUsage の値は、事前に定義された MEM Major Thresholdの値以上に変化します。
- cwCommMEMSwapUsage の値は、事前に定義された MEM Swap Major Threshold の値以上に変化します。
- cwCommFileUsage の値は、事前に定義された File Major Threshold の値以上に変化します。
- cwCommDiskUsage の値は、事前に定義された Disk Major Threshold の値以上に変化します。

トラップデータ

サポートされているトラップデータ。 MIB フィルタをこれらのトラップを受信するためだけに設定することをお勧めします。

名前	OID	表記規則	説明
cwCommNotificationHostAddressType	.1.3.6.1.4.1.9.9.809.1.2.4.1	InetAddressType	cwCommNotificationHostAddresnsにより利用可能となったネットワークアドレスの種類
cwCommNotificationHostAddress	.1.3.6.1.4.1.9.9.809.1.2.4.2	InetAddress	通知とともに送付されるホスト IP アドレス。

名前	OID	表記規則	説明
cwCommNotificationResName	.1.3.6.1.4.1.9.9.809.1.2.4.3	CiscoWebExCommSysRes	通知とともに送付されるシステムリソース名。 これは命名されたシステムリソースが事前に定義された警告レベル以上であることを示します。 0. cwCommTtoalCPUUsage 1. cwCommMemUsage 2. cwCommMemSwapUsage 3. オープンファイルデスクリプタ（MIB データなし） 4. cwCommSocketUsage 5. cwCommDiskTotal の 1 つ
cwCommNotificationResValue	.1.3.6.1.4.1.9.9.809.1.2.4.4	Unsigned32	通知付きシステムリソース割合使用値。
cwCommNotificationSeqNum	.1.3.6.1.4.1.9.9.809.1.2.4.5	Counter32	通知順にトラックするシーケンス番号。

第 10 章

共通の PC システム要件

ブラウザとオペレーティングシステムに共通の Cisco WebEx Meeting Server (CWMS) システム要件 管理者 PC と生産性向上ツールのユーザー PC は同一です。

クライアントおよびブラウザ要件

- JavaScript およびクッキーが有効
- Java 6、Java 7 または Java 8 （Java をサポートする Web ブラウザ）対応
- Cisco WebEx プラグインが有効です (Chrome 32 以降または Firefox 27 以降)
- Safari のプラグインが有効
- Active X が有効で、Microsoft Internet Explorer がブロックされていない（推奨）

（注） Google と Mozilla のポリシーが変更したため、Chrome 32 および Firefox 27 から、これらのブラウザを使用するとき、ユーザーは手動で WebEx プラグインを有効化することで、[25]WebEx ミーティングに参加するか、または WebEx 録画を再生する必要があります。 詳細については、https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htmを参照してください。

クライアントが指定されたバージョンの Chrome または Firefox 以外のブラウザーを使用し、Java を有効にしている場合、Cisco WebEx Meetings アプリケーションは初めてクライアントがミーティングを開始または参加するときに、自動的にクライアントのシステムにダウンロードされます。 Java バージョンの最新版をインストールするように、すべてのクライアントに指示することをお勧めします。

TLS 要件

すべてのユーザーのコンピュータで [インターネット設定] を TLS 暗号化を使用するように設定します。 たとえば、Windows PC で、[コントロール パネル] > [インターネット オプション] >

25 *このポリシーにより影響を受ける Chrome と Firefox の正確なバージョンは、このマニュアルの発行時点で確定していませんでした。

[詳細設定] > [セキュリティ] > [TLS 1.1 を使用する] および [TLS 1.2 を使用する] を選択します。互換性を最大限にするには、この両方のオプションを選択することをお勧めします。 （[TLS 1.0 を使用する] はバージョン 2.7 以降ではサポートされていません。）

ユーザーがゲスト（たとえば、社外の人）に対するミーティングを主催する場合は、そのゲストがミーティングに参加する前に、各自が使用するコンピュータのオペレーティングシステムおよびブラウザーが TLS 設定と一致するように手動で更新するよう知らせる必要があります。 これらのシステムを変更しない場合、互換性の問題が発生します。 ミーティングの招待にこれらの手順を含めることをお勧めします。 管理サイトで [設定] >> [メール] > > [テンプレート] の順に選択して、適切な招待状を編集することで、これを行うことができます。

SSL および TLS 要件

すべてのユーザーのコンピュータで、インターネット設定を SSL および TLS 暗号化に設定する。たとえば、Windows PC で、

- [コントロール パネル] > > [インターネット オプション] >> [詳細設定] >> [セキュリティ]、> [TLS 3.0 を使用する] の順に選択します。 互換性を最大限にするには、このオプションを選択することをお勧めします。
- 最大のご改正を得るために、[コントロール パネル] > [インターネット オプション] > [詳細設定] > [セキュリティ] > [TLS 1.0 を使用する] および [TLS 1.2 を使用する] を選択します。

ユーザーがゲスト（たとえば、社外の人）に対するミーティングを主催する場合は、そのゲストがミーティングに参加する前に、各自が使用するコンピュータのオペレーティングシステムおよびブラウザーが SSL または TLS 設定と一致するように手動で更新するよう知らせる必要があります。 これらの手順を実施しないと、互換性の問題が発生します。 ミーティングの招待にこれらの手順を含めることをお勧めします。 手順を招待状に含めるには、管理サイトで [設定] >> [メール] > > [テンプレート] の順に選択して適切な招待状を見つけ、適切に編集することによって行えます。

- Windows のオペレーティングシステム要件，212 ページ
- MACのオペレーティングシステム要件，216 ページ
- モバイルデバイスのオペレーティングシステム要件，216 ページ
- Citrix XenDesktop および XenApp の対応，217 ページ
- Cisco WebEx Meetings アプリケーションおよび生産性向上ツール互換性マトリクス，217 ページ
- 主催者ライセンスについて，220 ページ

Windows のオペレーティングシステム要件

対応する Windows オペレーティングシステム

- Windows Vista（32 ビット/64 ビット）

- Windows 7（32 ビット/64 ビット）
- Windows 8（32 ビット/64 ビット）
- Windows 8.1（32 ビット/64 ビット）
- Windows 10（32 ビット/64 ビット）（CWMS 2.6MR1 and higher 以降）
- Edge（Windows 10 のみ）20.10240.16384.0 から 38.14393.00

（注） Windows 10 Anniversary Update とも呼ばれる Microsoft Windows 10 Redstone 1（バージョン 1607）へのサポートが CWMS version 2.7 で追加されました。

Windows ハードウェアの最低必要要件

Intel Core2 Duo または AMD CPU 2.XX GHz 以降のプロセッサ

最低でも 2 GB 以上の RAM を推奨します。

サポート済みの Windows ブラウザ

- Internet Explorer： 8 - 11.103.14393.0

  IE 11 は Windows 7 SP1 と Windows 8.1 でテストされました

- Mozilla Firefox： 10—50

  Mozilla Firefox： 34 - 37、 バージョン 2.5MR4 でテスト済み

  の Firefox リリーススケジュールを参照してください。 https://wiki.mozilla.org/RapidRelease/Calendar

- Google Chrome： 23 - 54.0.2840.99

  Google Chrome： 39 - 42、 バージョン 2.5MR4 でテスト済み

  のChrome リリーススケジュールを参照してください。 http://www.chromium.org/developers/calendar

Microsoft Outlook 連携

- Microsoft Outlook 2007 SP2 以降
- Microsoft outlook 2010（32ビットおよび64ビット版のすべてのサービスパック）
- Microsoft Outlook 2013
- Microsoft Outlook 2016 （CWMS 2.6MR1）

下表はMicrosoft Outlookのどのバージョンがどのバージョンのオペレーティングシステムでサポートされているかを示します。

Microsoft Outlook のバージョン（クライアント/Exchange サーバー）	Vista	Windows 7	Windows 8（デスクトップモードのみ）	Windows 10
Outlook 2007/ Exchange 2007	はい	はい	いいえ	いいえ
Outlook 2010/ Exchange 2007	はい	はい	はい	はい
Outlook 2010/ Exchange 2010	はい	はい	はい	はい
Outlook 2013/ Exchange 2010	いいえ	はい	はい	はい
Outlook 2010/ Exchange 365 Hosted	いいえ	はい	はい	はい
Outlook 2013/ Exchange 2013	いいえ	はい	はい	はい
Outlook 2013/ Exchange 365 Hosted	いいえ	はい	はい	はい
Outlook 2016/ Exchange 365 Hosted	いいえ	はい	はい	はい
Outlook 2010/ Exchange 2016	いいえ	はい	はい	Y - window 7,8,10 サポート
Outlook 2013/ Exchange 2016	いいえ	はい	はい	Y - window 7,8,10 サポート
Outlook 2016/ Exchange 2016	いいえ	はい	はい	Y - window 7,8,10 サポート
Outlook 2016/ Exchange 2010	いいえ	はい	はい	Y - window 7,8,10 サポート
Outlook 2016/ Exchange 2013	いいえ	はい	はい	Y - window 7,8,10 サポート

サポートされているインスタントメッセンジャークライアント

インスタントメッセンジャーのバージョン	Windows XP SP3	Windows 7	Windows 8
Communicator 2007	はい	はい	はい
Communicator 2007 R2	はい	はい	はい
Lync 2010（32 ビット版）	いいえ	はい	はい
Lync 2013（32 ビット版）	いいえ	はい	はい

Windows と Cisco Jabber の連携

- Cisco Jabber for Windows 9.2.6
- Cisco Jabber for Windows 9.6.1
- Cisco Jabber for Windows 9.7
- Cisco Jabber for Windows 10.5
- Cisco Jabber for Windows 11.0
- Cisco Jabber for Windows 11.5 （CWMS 2.6MR1）
- Cisco Jabber for Windows 11.6
- Cisco WebEx Meetings Server システムと LDAP/ アクティブディレクトリとの統合をサポートしています。

制約事項 Windows 9.2.6 の Jabber は、Cisco WebEx Meetings Server 1.5 およびそれ以降の SAML 2.0 シングルサインオン（SSO）に構成されるサイトとの統合をサポートします。 Windows の Jabber のそれ以前のバージョンは、シングルサインオンをサポートしません。

すべての Cisco Jabber バージョンまたはプラットフォームは、Cisco WebEx Meetings Server との統合をサポートしているとは限りません。 (たとえば、クラウドベースの Jabber および WebEx Communicator。) Cisco WebEx Meetings Server との統合に関する情報については、http://www.cisco.com/en/US/products/ps12511/tsd_products_support_series_home.html で Cisco Jabber for Windows ドキュメントを参照してください。

MACのオペレーティングシステム要件

対応 Mac OS

- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- OS X 10.11 El Capitan (CWMS 2.6MR1)
- OS X 10.12 Sierra (CWMS 2.7MR2)

Mac ハードウェアの必要要件

2.0 GHz 以上の CPU

最低でも 512 MB 以上の RAM を推奨します。

サポートされている Mac ブラウザ

- Apple Safari: 6—9.1.3
- Google Chrome： 23— 53.0.2743.116

  のChrome リリーススケジュールを参照してください。 http://www.chromium.org/developers/calendar
- Mozilla Firefox： 10—48.1

Mac インテグレーション用 Cisco Jabber

以下の Cisco Jabber for Mac 統合は、SAML 2.0 シングルサインオン (SSO) または LDAP/アクティブディレクトリに構成された Cisco WebEx Meetings Server サイトに対応しています。

- Cisco Jabber for Mac 11.6 は Cisco WebEx Meetings Server リリース 2.6 以降に対応します
- Cisco Jabber for Mac 10.5 は Cisco WebEx Meetings Server リリース 2.5 以降に対応します
- Cisco Jabber for Mac 9.6 は Cisco WebEx Meetings Server リリース 2.0 以降に対応します

モバイルデバイスのオペレーティングシステム要件

Cisco WebEx アプリケーションを iOS または Android に手動でダウンロードし、WebEx モバイル機能が有効になった後、ユーザーはアプリケーションを使用してミーティングに出席または開始できます。 また、ユーザーはブラウザを使用することで、モバイル端末で Cisco WebEx にアクセスできますが、同じ最適なユーザーエクスペリエンスを提供できない可能性があります。

Cisco WebEx Meeting Server バージョン 2.0 以降は以下をサポートします。

- iOS 6.0 およびそれ以降の Apple iPhones および iPads
- Android 2.1 およびそれ以降の Android モバイル端末
- iPhones および Android 9.6 以降に対応した Jabber

（注） モバイル端末で録画を再生できません。 Android モバイル端末を使用してミーティングを開始した場合、ミーティングの録画を開始および管理できます。 iOS モバイル端末を使用してミーティングを開始した場合、iOS 端末上でミーティングの録画を開始または管理できません。

Citrix XenDesktop および XenApp の対応

Cisco Webex Meeting Server は主催者のオペレーティングシステムと仮想オペレーティングシステムの両方が Windows 7 または Windows 8 である Citrix XenDesktop 7.6 に対応します（主催者のオペレーティングシステムはエンドユーザーのコンピュータにインストールされています）。 仮想オペレーティングシステムはサーバーが送信したオペレーティングシステムです。）

既知の問題や限定事項が

- 仮想デスクトップ環境の設計上の制限により、ビデオの送信はスムーズに機能しない場合があります。 さらに、ミーティング中にビデオを送る時、フレームレートが低くなり、ユーザーエクスペリエンスが最適ではない場合があります。
- 仮想デスクトップ環境ではビデオファイルの一部は共有できません。
- Mac OS 使用時に、ウェブカメラとマイク（外付けまたは内蔵のいずれか）は認識されずミーティング中利用できない場合があります。
- Remote Access および Access Anywhere には対応していません。OS の再起動後、Citrix プラットフォームにより Remote Access および Access Anywhere エージェントが自動的に削除されてしまうためです。
- 生産性向上ツールのユーザーは、ワンクリックミーティングを開始したり、Outlook からスケジュールされたミーティングを開始できません。

Cisco WebEx Meetings アプリケーションおよび生産性向上ツール互換性マトリクス

この表は Cisco WebEx Meetings Server の各リリースに対する WebEx Meetings アプリケーションおよび生産性向上ツールのダウンロードのビルド番号を記載しています。

Cisco WebEx Meetings Server FAQ	ISO 番号	Cisco WebEx 生産性向上ツール	Cisco WebEx Meetings アプリケーション
1.5 MR3	1.5.1.323	2.80.501.321	27.32.151.321
1.5 MR4	1.5.1.402/1.5.1.400	2.80.501.401	27.32.151.401
1.5 MR5	1.5.1.503	2.80.501.503	27.32.151.503 (Windows) orion1.5.MR3.FCS.0.0.503 (Mac)
2.0[26]	2.0.1.2	2.82.0.1713	27.32.200.1713
2.0 MR1	2.0.1.107	2.82.0.1713	27.32.200.1713
2.0 MR2	2.0.1.205	2.82.0.1713	27.32.200.1713
2.0 MR3	2.0.1.302	2.82.1.302	27.32.200.302
2.0 MR4	2.0.1.407	2.82.1.407	27.32.200.407 orion2.0.MR4.0.0.407 (MAC OS)
2.0MR5。	2.0.1.507	2.82.1.507	27.32.201.507 (Windows) orion2.0.MR5.0.0.507 (Mac)
2.0MR6。	2.0.1.611	2.82.1.606	27.32.200.606 (Windows) orion2.0.MR6.0.0.606 (Mac)
2.0MR7。	2.0.1.707	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)
2.0MR8。	2.0.1.809	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)
2.0MR8 セキュリティパッチ 1	2.0.1.839	2.82.1.839	27.32.201.839 (Windows) orion2.0.MR8.0.0.839 (Mac)
2.0MR9。	2.0.1.918	2.82.1.910	27.32.201.910 (Windows) orion2.0.MR9.0.0.910 (Mac)

Cisco WebEx Meetings Server FAQ	ISO 番号	Cisco WebEx 生産性向上ツール	Cisco WebEx Meetings アプリケーション
2.5	2.5.1.29	2.82.500.2353	29.9.2.10085 (Windows と Mac)
2.5MR1。	2.5.1.132	2.82.500.3339	29.11.3.4858 (Windows と Mac)
2.5MR2。	2.5.1.227	2.82.501.10002	29.12.0.10076 (Windows と Mac)
2.5MR3。	2.5.1.3009	2.82.501.10008	29.12.0.10076 (Windows と Mac)
2.5MR4。	2.5.1.4378	2.82.502.8	29.13.11.10173 (Windows と Mac)
2.5MR5。	2.5.1.5033	2.82.502.9	29.13.12.10182 (Windows と Mac)
2.5MR6。	2.5.1.6139	2.82.502.11	29.13.41.30001 (Windows と Mac)
2.6	2.6.1.39	2.82.502.1078	30.1.0.20002 (Windows と Mac)
2.6MR1。	2.6.1.1099	2.82.6501.1082	30.5.2.10002 (Windows と Mac)
2.6MR2。	2.6.1.2097	2.82.6520.1083	30.6.4.10003 (Windows と Mac)
2.6MR3。	2.6.1.3096	2.82.6520.1090	30.10.1.10008 (Windows と Mac)
2.7	2.7.1.12	2.82.7000.1150	31.4.0.41 (Windows と Mac)
2.7MR1。	2.7.1.1073	2.82.7000.1159	31.5.20.63 (Windows と Mac)
2.7MR2。	2.7.1.2048 [27]	2.82.7000.1161	31.8.0.167 (Windows と Mac)
2.8	2.8.1.12 (保留。 バージョン 2.8.1.17 を使用のこと。)	該当せず	該当せず

Cisco WebEx Meetings Server FAQ	ISO 番号	Cisco WebEx 生産性向上ツール	Cisco WebEx Meetings アプリケーション
2.8	2.8.1.17	2.82.7000.1174	31.11.6.9

[26] 利用できません。
[27] 2.7MR2 ソフトウェアの更新は現在、Cisco WebEx Meetings Server リリース 2.7.1.12 または 2.7.1.1073 以降を実行中のシステムのみを対象としています。

主催者ライセンスについて

本製品の**ホストベースライセンス**は、ミーティングを**主催**する各ユーザーに対し購入する必要があります。または手動で割り当てられたライセンスです。 ユーザーが他の人の代理で、ミーティングに出席またはミーティングをスケジュールした場合、主催者ライセンスは消費されません。報告目的でライセンス使用の計算は毎月行われます (たとえば、1 月 1 日 ～ 31 日に 1 回、2 月 1 日 ～ 28 日に 1 回など)。

（注） 前のバージョンからバージョン 2.5 以降にアップグレードするとき、元のシステムにあったすべてのライセンスは、割り当てられていたユーザーから解放されます。 ユーザーはミーティングを主催するか、または手動でライセンスを割り当てることで、ライセンスを再取得できます。 これはマルチデータセンター (MDC) システムをインストールする際にも当てはまります。主催者ライセンスはMDC システムと結合しているデータセンター上で失われます。 これらのライセンスは、結合後に MDC システムで再ホストできます。

[レポート] ページから、使用されるライセンス数を提供するレポートを要求できます。 さらに、ライセンス使用傾向を示すPDF サマリーレポートを確認することをお勧めします。 全体のライセンス傾向を見ることにより、社内におけるこのシステムの使用の増加に合わせて今後のライセンス使用を効率的に計画することができます。

第 11 章

Cisco Unified Communications Manager (CUCM) の統合

Cisco WebEx Meetings Server は、以下のリリースの Cisco Unified Communications Manager と互換性があります。

- 11.5(1)SU1
- 11.0(1a)
- 10.5.2
- 10.5
- 10.0
- 9.1
- 9.0

（注） TLS 1.0 の CWMS 2.7 以降のサポートが除去されました（CSCuu40706）。 TLS 1.2 のサポートは、CUCM バージョン 10.5 以降に導入されました。

- Session Manager Edition (SME) 統合に対応しています。, 221 ページ
- オーディオエンドポイント互換性, 222 ページ

Session Manager Edition (SME) 統合に対応しています。

CWMS は Session Manager Edition (SME) をサポートします。

Unified MP ユーザーはUnified MP ミーティングをスケジュールするとき、Web会議プロバイダーとして、Cisco WebEx を選択できます。 Cisco WebEx 統合は Cisco Unified MP 6.0.2 以降で利用できます。 音声会議とビデオ会議が Unified MP により提供されます。 ミーティングに参加させるため、音声とビデオのダイヤルイン情報を WebEx ユーザーに提供する必要があります。または、

WebEx ユーザーはミーティングに参加するために、WebEx のダイヤルアウト機能を利用できます。

オーディオエンドポイント互換性

Cisco Unified Communications Manager に接続するどの基準ベースの音声エンドポイントを使用しても、WebEx ミーティングに参加できます。 サポートされている音声エンドポイントには、Cisco IP 電話、Telepresence エンドポイント、および携帯電話と固定電話などの PSTN 端末が含まれます。 多くの音声エンドポイントは、音声とビデオの接続をサポートしています。 ただし、サポートされているのは、Cisco WebEx Meetings Server への音声接続のみです。

組織外部からのユーザーの PSTN 端末による WebEx ミーティングへの参加を許可するには、会社が Cisco サービス連携ルーター（ISR）などのアナログ- VoIP 変換ゲートウェイを展開する必要があります。 下記の IP電話は、Cisco WebEx Meetings Server でテスト済みです。

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator
- ライフサイズ・ビデオ電話
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20。
- EX 60
- EX 90

その他の Cisco Unified IT-互換のエンドポイントも通常通り動作するはずです。 各モデルに対する Cisco Unified Communications Manager と Device Packs によってサポートされる Cisco Unified IP Phones の一覧については、「Cisco Unified IP Phone Feature および Cisco Unified Communications Manager Device Pack Compatibility Matrix 」を参照してください。