# の導入ガイド Cisco Webex ハイブリッド メッセージ サービス

**初版**：2018 年 1 月 24 日

**最終更新**：2019 年 8 月 29 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/

© 2020 Cisco Systems, Inc. All rights reserved.

# 目 次


第 1 章 **Cisco Webex ハイブリッド メッセージ サービスの概要** 1

ハイブリッド メッセージ サービス コンポーネントとユーザ 1

ユーザ間のやり取り 4

導入モデル 9

導入機能の適用範囲 14

連絡先 16

ダイレクトメッセージング インターフェイス（1 対 1） 16

オフラインストレージ 17

グループメッセージング 18

プレゼンスの変換 19

ファイル転送 23

移行に関する考慮事項 24

メッセージフローとセキュリティ 26

ハイブリッド メッセージ サービス 接続 28

メッセージサービスのポート 29

第 2 章 **環境の準備 ハイブリッド メッセージ サービス** 31

ハイブリッド メッセージ サービス の要件 31

ユーザの管理 ハイブリッド メッセージ サービス 33

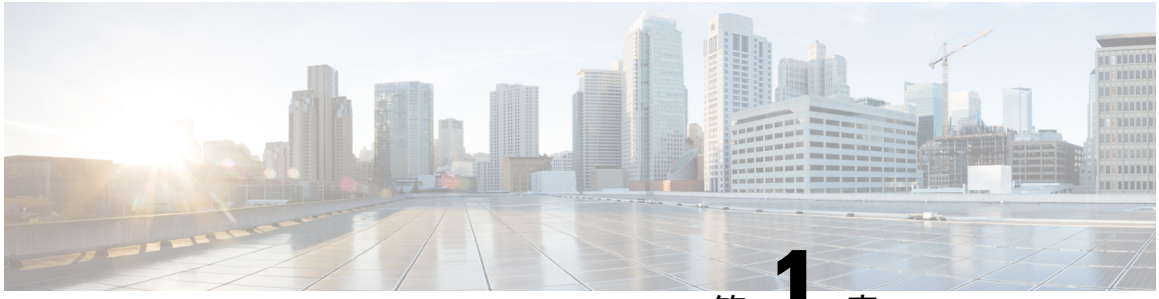
管理者招待メール送信の抑止 35

Cisco Webex ハイブリッド サービス に対する Expressway-C コネクタホストの前提条件の対処 35

第 3 章 **Cisco Webex ハイブリッド メッセージ サービスの導入** 41

Cisco Webex クラウドへの Expressway-C コネクタホストの登録 41
ハイブリッドサービスの認証局 44
メッセージ コネクタ用のアプリケーション アカウントの構成 45
IM およびプレゼンスサービス への接続の設定 45
起動 メッセージコネクタ 46
コネクタのステータスの確認 47
ユーザに対する ハイブリッド メッセージ サービス の有効化 47
Test ハイブリッド メッセージ サービス 48

第 4 章 ハイブリッド メッセージ サービスの管理 51
ハイブリッド メッセージ サービス Expressway 上のステータス 51
ハイ アベイラビリティとフェールオーバー 54
ユニファイド CM IM and Presence ノードへの接続の更新 55
ハイブリッド メッセージ サービスのトラブルシューティング 56



第 1 章

# Cisco Webex ハイブリッドメッセージサービスの概要

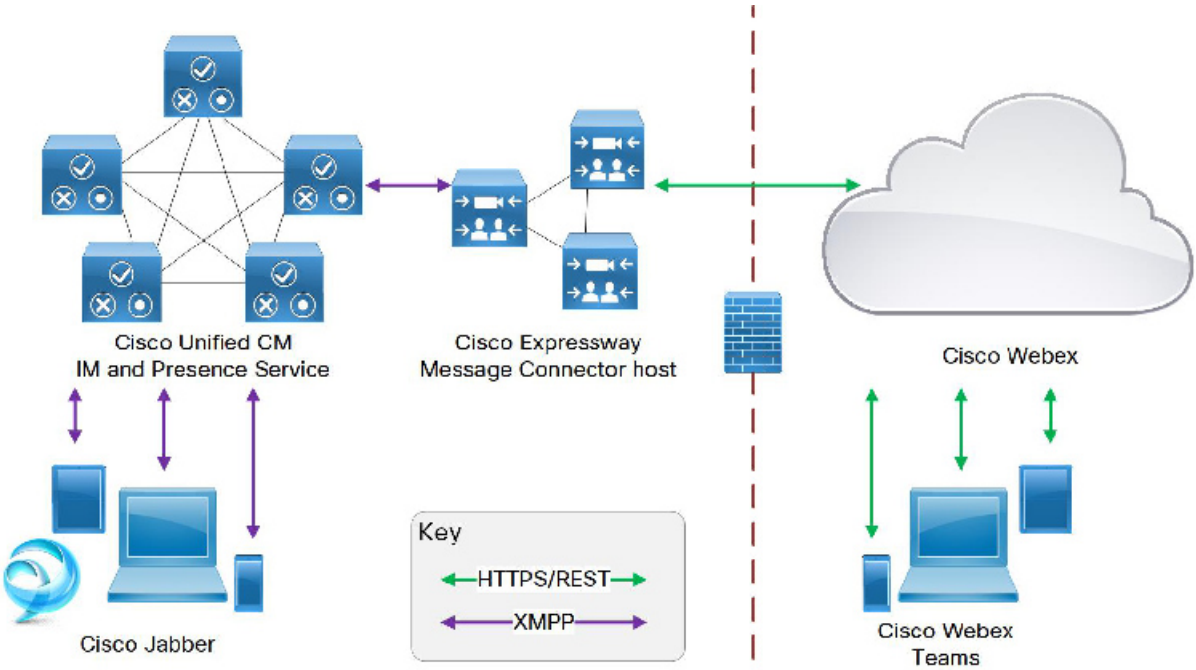

- ハイブリッド メッセージ サービス コンポーネントとユーザ （1 ページ）
- ユーザ間のやり取り （4 ページ）
- 導入モデル （9 ページ）
- 導入機能の適用範囲 （14 ページ）
- 連絡先 （16 ページ）
- ダイレクトメッセージング インターフェイス（1 対 1） （16 ページ）
- オフラインストレージ （17 ページ）
- グループメッセージング （18 ページ）
- プレゼンスの変換 （19 ページ）
- ファイル転送 （23 ページ）
- 移行に関する考慮事項 （24 ページ）
- メッセージフローとセキュリティ （26 ページ）
- ハイブリッド メッセージ サービス 接続 （28 ページ）
- メッセージサービスのポート （29 ページ）


## ハイブリッドメッセージサービスコンポーネントとユーザ

Cisco Webex ハイブリッド メッセージ サービス は Cisco Unified Communications Manager IM およびプレゼンスサービス （IM およびプレゼンスサービス ）を Cisco Webex に接続して、Cisco Webex Teams との相互運用を有効にします。

（注） この導入により、オンプレミスの *Jabber* 導入環境と Cisco Webex Teams ユーザ間の相互運用性が提供されます。これは、クラウドベースの *Jabber* 導入環境と Cisco Webex Teams ユーザ間の相互運用性とは異なります（この場合の導入について詳しくは、https://help.webex.com/article/nzx9su0を参照してください）。

図 *1:* ハイブリッド メッセージ サービス コンポーネント




図の左側は、Cisco Jabber と IM およびプレゼンスサービス のオンプレミス導入環境です。右側は、Cisco Webex 内のお客様の組織と、組織に属する Webex Teams ユーザです。この組織を管理するには、Cisco Webex Control Hub を使用します。

ハイブリッド メッセージ サービス は、これら 2 つのユーザグループ間の相互運用性を確立します。ハイブリッド メッセージ サービス を可能にするコンポーネントは、オンプレミスの Cisco Expressway インフラストラクチャでホストされた メッセージコネクタ と、Cisco Webex クラウドで実行されるメッセージサービスです。

### 相互運用性に影響するライセンスと利用資格の要素

- シスコでは、すべてのユーザがすでに Cisco Jabber のライセンスを取得しており、Jabber が Ciscoユニファイド コミュニケーション マネージャ IM and Presence に登録されていることを前提としています。
- 組織用に任意の Cisco Webex Teams オファーが購入済みである必要があります。これは Cisco Commerce Workspace を介して注文できます。

  また、組織の管理者権限が割り当てられていて、Cisco Webex Control Hub にアクセスできる必要もあります（注文プロセスの一環としてこの権限が付与されます）。

- すべての Jabber ユーザを 制御ハブ にインポートし、それらすべてのユーザに「Message Free」の利用資格を付与する必要があります。これにより、すべての Jabber ユーザが Webex Teams の基本的なメッセージング機能を使用できるようになります。

  この基本メッセージングに追加の有料ライセンス要件はありません。すべてのユーザにこの利用資格を付与すると、ハイブリッド メッセージ サービス が有効にされているユーザと、Jabber の利用資格のみを持つユーザとの間の相互運用性が向上します。

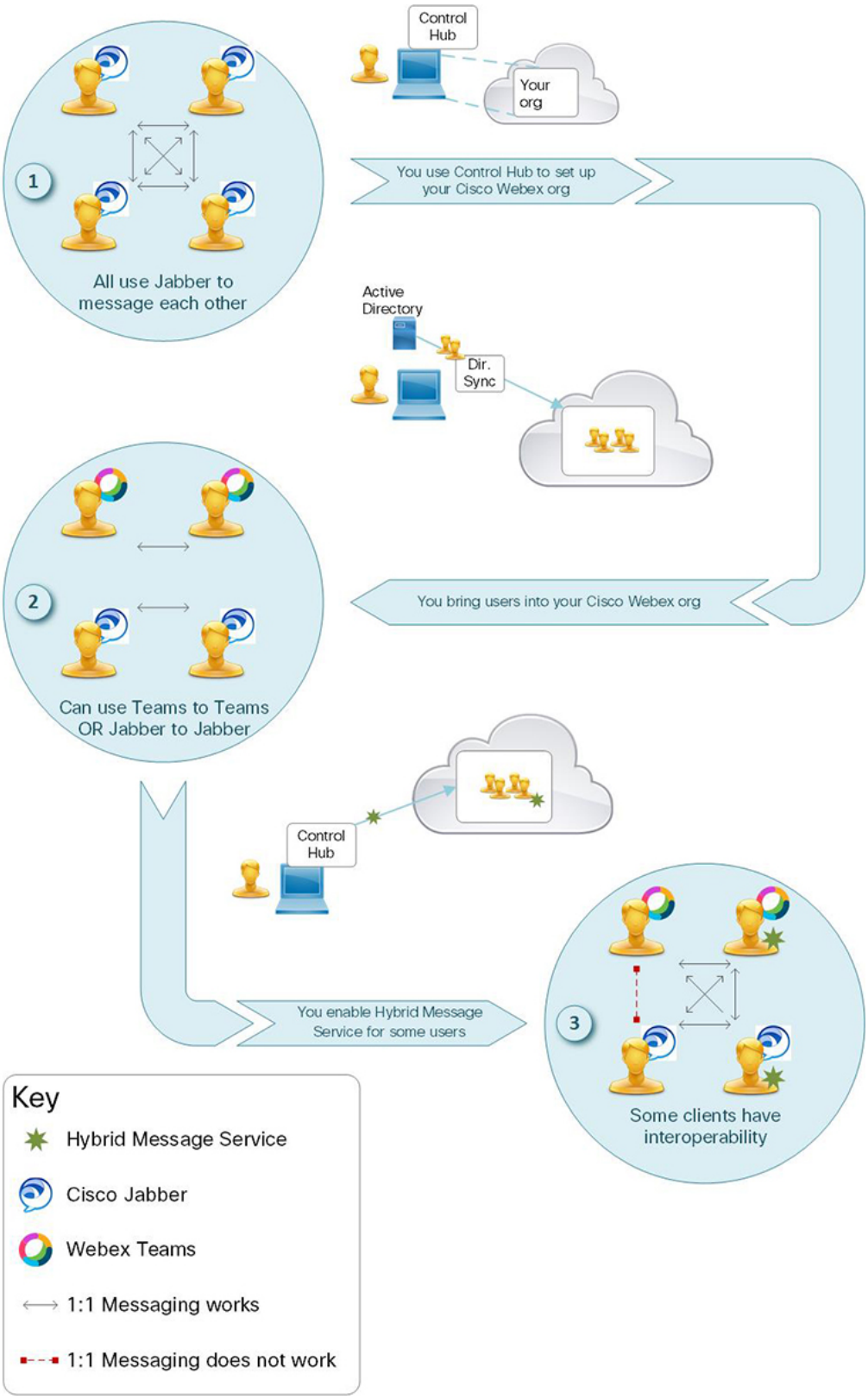
- ハイブリッド メッセージ サービス は、制御ハブ で同じ組織に属しているユーザ間でのみ機能します。このサービスを使用して、Webex Teams ユーザが組織外の Jabber ユーザと通信することはできません。

- ハイブリッド メッセージ サービス が有効にされているユーザは、Jabber または Webex Teams を使用して、組織内の他のすべてのユーザとチャットできます。受信者が Webex Teams または Jabber を使用しているかどうかは関係ありません。

- ハイブリッド メッセージ サービス が有効にされていないユーザは、Jabber を使用して組織内の他のすべてのユーザとチャットできます。Webex Teams を使用して、ハイブリッド メッセージ サービス が有効にされているユーザとチャットすることはできますが、メッセージは受信者の Jabber クライアントにコピーされません。

# ユーザ間のやり取り

図 *2:* 実装時のクライアント間の相互運用性


Control Hub
Your org
1
All use Jabber to message each other
You use Control Hub to set up your Cisco Webex org
Active Directory
Dir. Sync
2
Can use Teams to Teams OR Jabber to Jabber
You bring users into your Cisco Webex org
Control Hub
You enable Hybrid Message Service for some users
3
Some clients have interoperability
Key
Hybrid Message Service
Cisco Jabber
Webex Teams
1:1 Messaging works
1:1 Messaging does not work

次の図は、ハイブリッド メッセージ サービスを実装する際の対象ユーザの変化を示しています。実装を開始する時点で、すべてのユーザはCisco Jabber（図のポイント1）を使用しています。図に示されているタスクを行うと、ユーザの一部にハイブリッド メッセージ サービスが有効にされた状態になります（ポイント 3）。

この時点で、チャットメッセージを送信するには次の 4 つの方法があります。

- メッセージサービスを使用しないユーザが、Webex Teams を使用する
- メッセージサービスを使用しないユーザが、Cisco Jabber を使用する
- メッセージサービスを使用しているユーザが、Webex Teams を使用する
- メッセージサービスを使用しているユーザが、Cisco Jabber を使用する

受信者がチャットメッセージを受信するにも4つの方法があります。つまり、16通りのやり取りが考えられます。ただし有効なやり取りとして期待できるのは、同じクライアントの間（Jabber 間、または Webex Teams 間）でやり取りが行われる、このうち 8 つの方法です（ポイント 2）。残りの 8 つのシナリオのうち、次のように 3 つのケースは失敗するはずです。

図 *3 : 1* 対 *1* のメッセージングの場合の *8* つのシナリオ

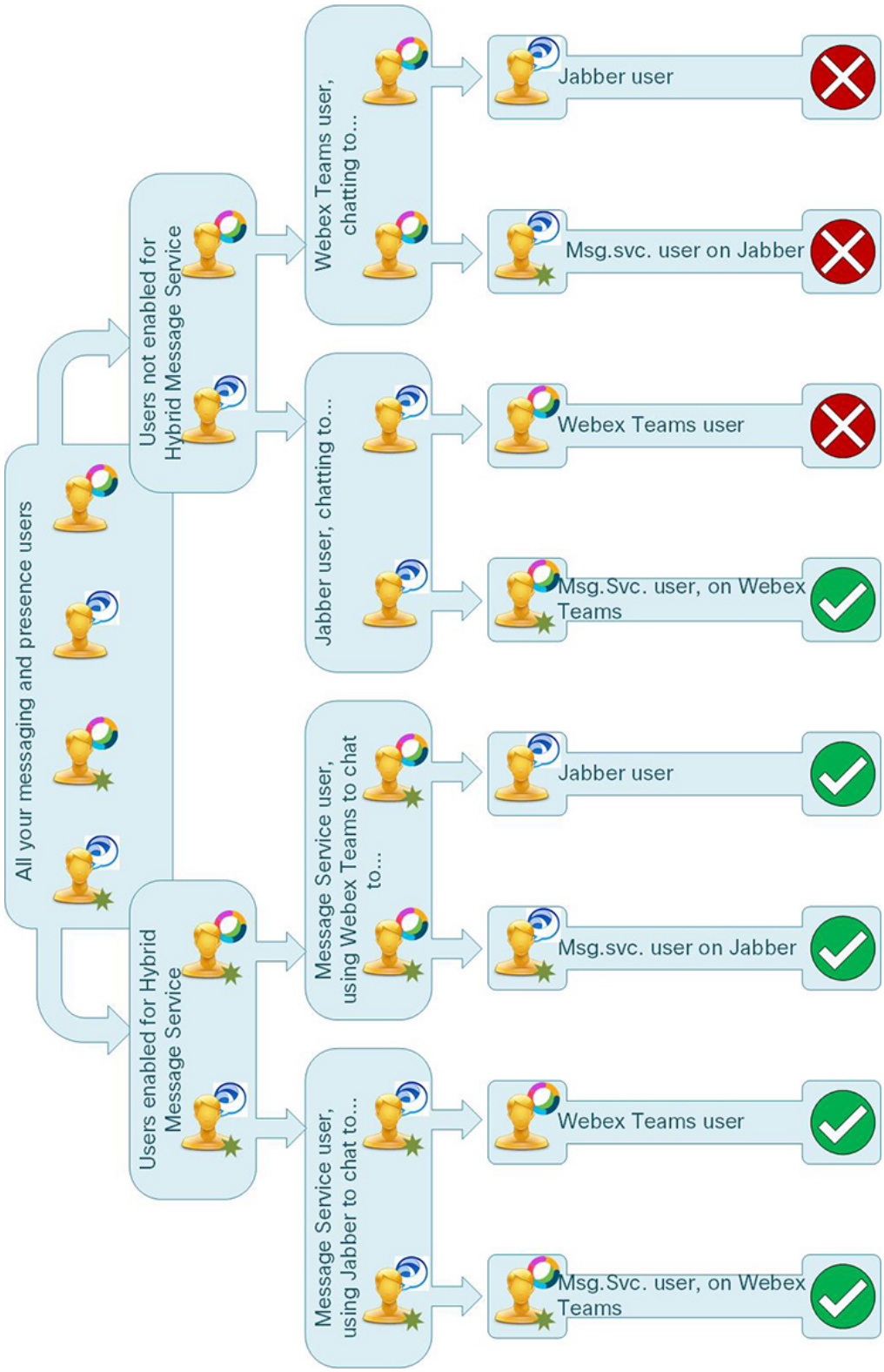
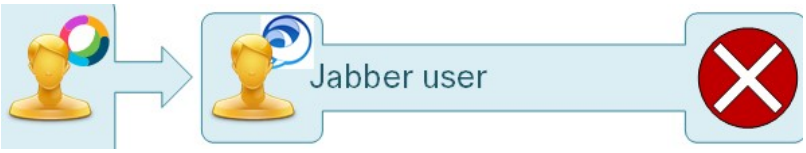


図 *4:* 予想される障害：***Webex Teams*** から ***Jabber*** へのメッセージング（いずれのユーザもハイブリッドメッセージサービスを使用していない場合）




送信者は Webex Teams を使用していますが、ハイブリッド メッセージ サービスが有効にされていません。送信者が Webex Teams を使用して、受信者と直接接続するためのスペースを開始します。受信者は Jabber を使用しているため、Webex Teams にメッセージが表示されません。

送信者のハイブリッド メッセージ サービスが有効になっていれば、Webex Teams のチャットメッセージが IM and Presence にコピーされて、Jabber アカウントから送信されます。しかし、送信者のハイブリッド メッセージ サービスは有効になっていないため、メッセージは IM and Presence にコピーされません。したがって、受信者が Webex Teams を使用しない限り、メッセージは受信者に表示されません。

図 *5:* 予想される障害：***Webex Teams*** からハイブリッド メッセージ サービスユーザの ***Jabber*** クライアンへのメッセージング

送信者は Webex Teams を使用していますが、ハイブリッド メッセージ サービスが有効にされていません。送信者が Webex Teams を使用して、受信者と直接接続するためのスペースを開始します。受信者のハイブリッド メッセージ サービスは有効になっていますが、Jabber を使用しているため、メッセージは表示されません。

これは予想された動作です。負荷を軽減するために、このサービスはこのように設計されています。その理由は、ハイブリッド メッセージ サービスが組織内の「早期導入者」に対して有効にされ、Webex Teams がプライマリチャット クライアントとして使用されることが想定されているためです。

図 *6:* 予想される障害：***Jabber*** から ***Webex Teams*** へのメッセージング（いずれのユーザもハイブリッドメッセージサービスを使用していない場合）

送信者は Jabber を使用しており、受信者の Jabber 連絡先とのチャットを開始します。受信者は Webex Teams を使用しているため、Jabber の会話が表示されません。受信者のハイブリッド メッセージ サービスが有効になっていないため、これらの Jabber メッセージはコピーされず、Webex Teams に送信されません。

受信者は、Jabber を使用しない限り、会話を認識できません。この場合、オフラインストレージが無効になっていると、受信者に会話が表示されることはありません。

# 導入モデル

## 導入モデルの選択

ハイブリッドメッセージサービスの導入方法を選択する際は、次の要因を考慮してください。

- スケール：サービスの提供対象となるIMおよびプレゼンスサービス ユーザの人数は何人ですか。その要件を満たすために、ノードまたはクラスタを追加してサービスのキャパシティを増やす必要はありますか。

  サポートされるメッセージサービスユーザの最大数は、小規模Expressswayでは5,000ユーザ、中規模 Expressway では 6,500 ユーザ、大規模 Expressway では 15,000 ユーザです。1 つのノードのキャパシティは冗長性を確保するために予約されるため、6 つの Expressway からなるクラスタでは最大75,000ユーザをサポートできます。メッセージサービスのキャパシティについては、https://help.webex.com/article/nv5p67gを参照してください。

- 可用性：サービスの可用性はどの程度重要ですか。障害発生時にもサービスが継続されるようにするために、冗長ノード/クラスタを導入する必要がありますか。

- 地域：ユーザが世界の各地に分散していると、複数のデータセンターを異なるタイムゾーンで運用することになります。コネクタホストの導入場所を選択する際は、遅延を考慮しなければならない場合があります。

- 各導入シナリオでは、次の点に注意してください。

  - 1 つの Expressway クラスタを構成するノードの数は、プライマリノードを含め、最大 6 つに制限されています。

  - 各 Expressway クラスタのプライマリノードを Cisco Webex に登録する必要があります。

  - Expressway クラスタを IM およびプレゼンスサービス クラスタに接続するには、該当する Expressway クラスタのプライマリノード上のパブリッシャの詳細を入力します。このアクションにより、IM およびプレゼンスサービス クラスタのすべてのノードで Expressway クラスタのすべてのノードが接続されます（わかりやすくするために、図にはプライマリとパブリッシャ間の接続のみが示されています）。

    すべての Expressway クラスタをすべての IM およびプレゼンスサービス クラスタに接続する必要はありません。確立する接続は、選択した導入モデルによって異なります。

    複数の Expressway コネクタクラスタを 1 つの IM およびプレゼンスサービス クラスタに関連付けないようにしてください（ただし、IM およびプレゼンスサービス クラスタはExpressway クラスタでサポート可能な数よりも多くのメッセージおよびPresence ユーザに対応することも可能です）。

    Expressway コネクタクラスタごとに複数の IM およびプレゼンスサービス クラスタを接続できます。

Expressway コネクタクラスタあたり、最大 5 つの IM およびプレゼンスサービス クラスタがサポートされます。

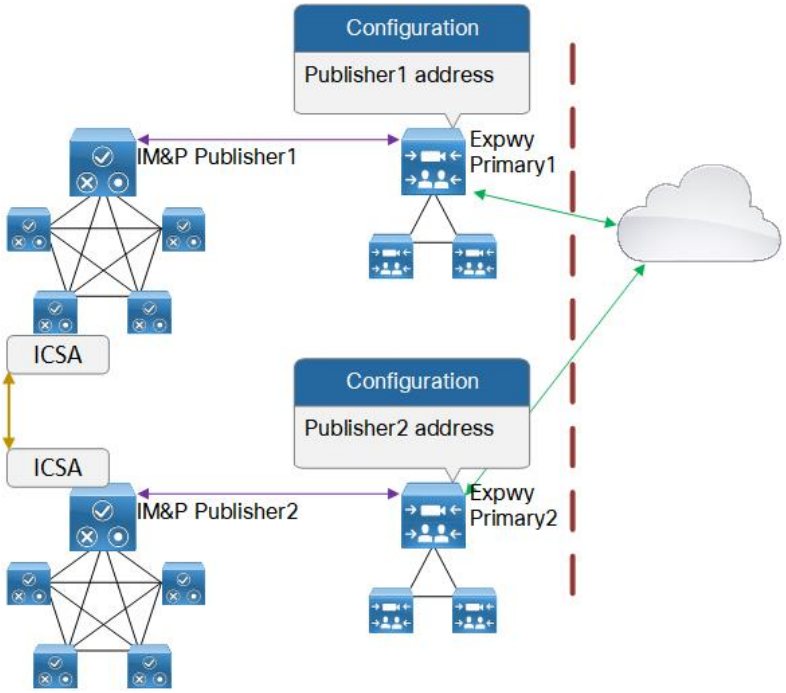
- 制御ハブ でリソースグループを使用して組織の地域を定義してから、それぞれ異なる場所を表すリソースグループに Expressway リソースを割り当てます。

  各リソースグループに割り当てるユーザのセットは、そのリソースグループの Expressway で対応するすべての IM およびプレゼンスサービス クラスタのユーザと一致している必要があります。

### 1 対 1 での Expressway コネクタクラスタと IM およびプレゼンスサービス クラスタの導入

この導入オプションで必要になる Expressway コネクタクラスタは、IM およびプレゼンスサービス クラスタごとに 1 つです。複数のサイトがある場合は、各データセンターで構成を繰り返します（次の 2 つの図を参照）。このオプションでは相互運用性に関して遅延が短くなりますが、データセンターの冗長性要件には対応していません。

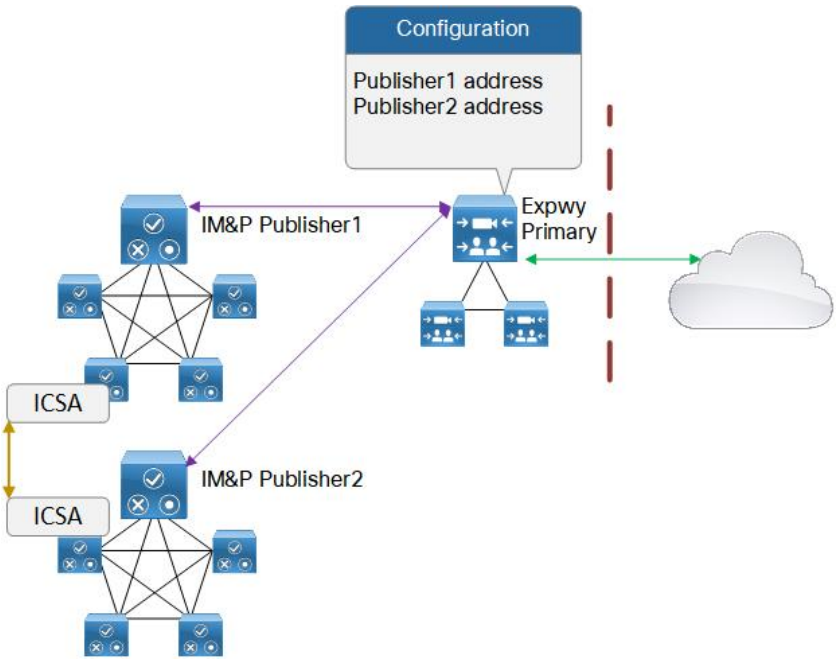
図 *7: 1* 対 *1* の *Expressway* と *IM* およびプレゼンスサービス クラスタ




### 1 対多の Expressway コネクタクラスタ IM およびプレゼンスサービス

この導入オプションで必要になる Expressway コネクタクラスタは、IM およびプレゼンスサービス 導入環境全体で 1 つです。このオプションは構成と管理をシンプルにしますが、多数のユーザがいる場合やユーザが地理的に分散されている場合、拡張性と遅延が問題になる可能性があります。

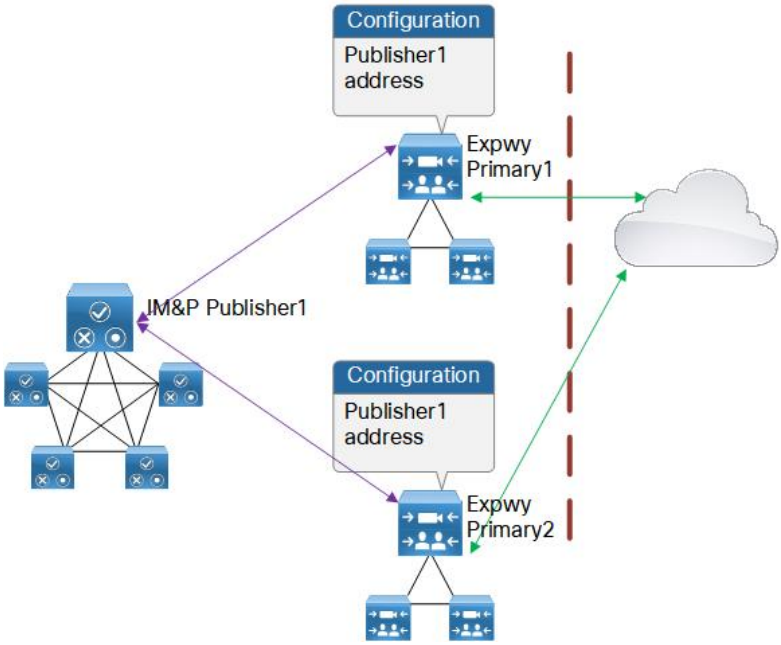
図 *8 : 1* 対多の *Expressway* コネクタクラスタ *IM* およびプレゼンスサービス




### メッシュ構成は推奨されません

冗長性が必要な場合は、次の導入例が適しています。ただし、IM およびプレゼンスサービス クラスタに接続する各 メッセージコネクタ クラスタでパフォーマンスに影響することが予想されます。そのため、1 つの IM およびプレゼンスサービス クラスタに複数の Expressway クラスタを接続しないことを推奨します。

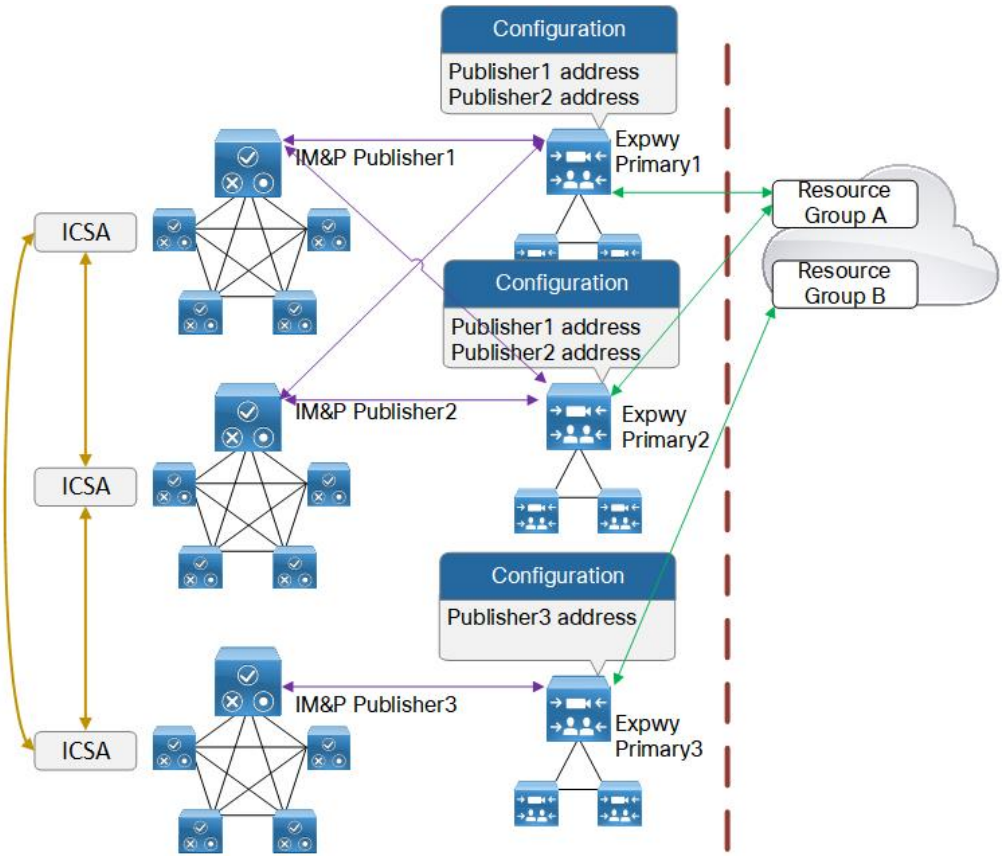
図 *9*：非推奨：*1* つの *IM* およびプレゼンスサービス クラスタに接続された複数の *Expressway* クラスタ




### 例：複数の IM およびプレゼンスサービス クラスタを使用した複数の Expressway クラスタの部分的メッシュ

データセンターの冗長性が遅延またはパフォーマンスよりも重要なためにメッシュ構成を避けられない場合は、最小限のメッシュ構成に抑えるようにしてください。例として、次の図は 2 つの IM およびプレゼンスサービス クラスタで構成された 2 つのメッシュ型 Expressway クラスタを示しています。2 つのデータセンターが地理的に近い場所にあり、サービス可用性の向上を優先してパフォーマンスへの影響を許容する場合は、この構成が役立ちます。

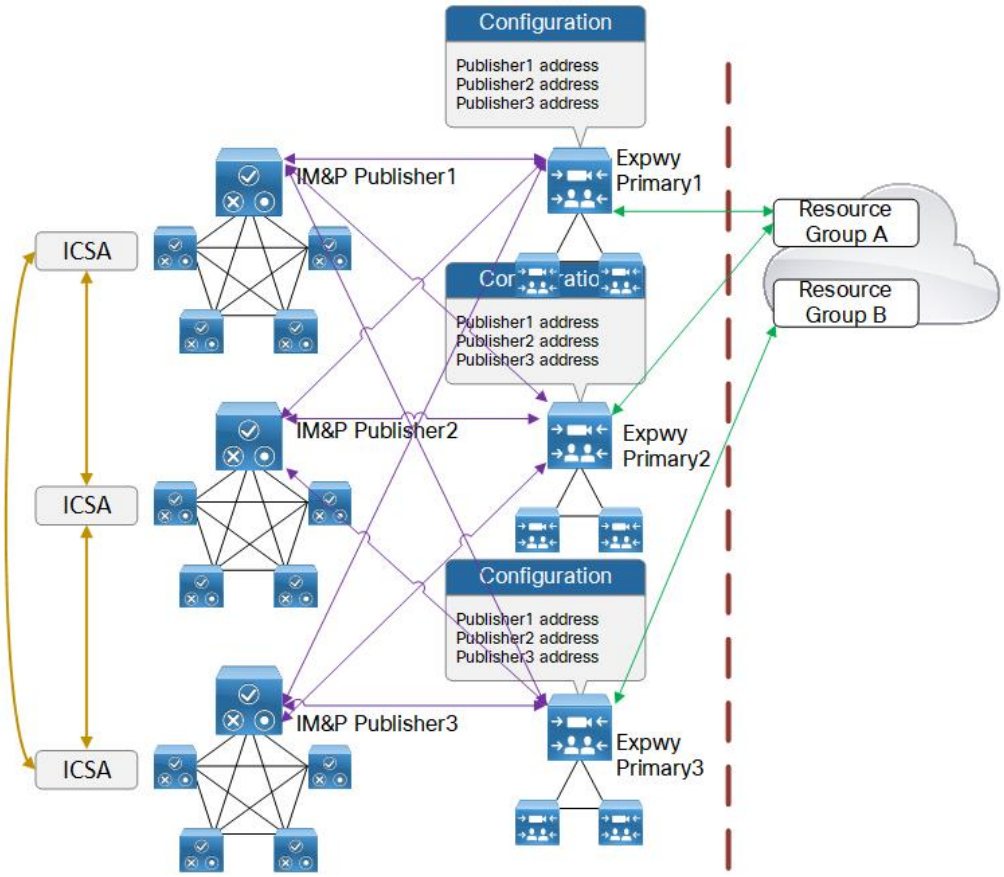
図 *10*：部分的メッシュ：複数の *IM* およびプレゼンスサービス クラスタに接続された複数の *Expressway* コネクタクラスタ




### 例：複数の IM およびプレゼンスサービス クラスタを使用した複数の Expressway クラスタのフルメッシュ

次の導入オプションは、データセンターに最大限の冗長性をもたらします。ただし、データセンターが地理的に分散されている場合、このオプションはパフォーマンスに非常に大きな影響を与え、ユーザエクスペリエンスに影響する遅延の問題が発生する可能性があります。「フルメッシュ」は使用しないことをお勧めします。この構成は有効ですが、大規模なテストは行っていません。

図 *11*：フルメッシュ：複数の *IM* およびプレゼンスサービス クラスタに接続された複数の *Expressway* コネクタクラスタ




# 導入機能の適用範囲

| 機能 | 説明 |
|---|---|
| インスタントメッセージングのコンプライアンス | ハイブリッド メッセージ サービス は、コンプライアンスに応じて構成された IM およびプレゼンスサービス で動作します。Webex Teams はコンプライアンスをサポートしておらず、ブロックされた Jabber ユーザでも Webex Teams から Webex Teams へのメッセージングが可能です。 |

| 機能 | 説明 |
|---|---|
| メッセージの暗号化 | オンプレミスと Cisco Webex 間でサポートされています（必須となっています）。<br>• IM およびプレゼンスサービス から Webex Teams へのメッセージは、メッセージコネクタによって暗号化されます。<br>• Webex Teams から IM およびプレゼンスサービス へのメッセージは、メッセージコネクタ によって復号されます。<br>• メッセージコネクタ は IM およびプレゼンスサービス ノードに TCP で接続します。これらの接続では、TLS はサポートされていません。 |
| 複数のオンプレミス ドメイン | メッセージコネクタ 複数の XMPP ドメインで機能します。 |
| 他のハイブリッドサービスとの共存 | メッセージコネクタは、Expressway ベースの他のハイブリッドサービス（Hybrid Call Service および Hybrid Calendar Service）と共存できます。共存によって、コネクタホストによって伝送される ハイブリッド メッセージ サービス ユーザの数が減ります。<br>共存とキャパシティの詳細については、https://help.webex.com/article/nv5p67gを参照してください。 |
| データセキュリティ/キー管理システム | ハイブリッド メッセージ サービス は Cisco Webex ハイブリッド データ セキュリティ との互換性があります。<br>通常は、ハイブリッド メッセージ サービス をセキュリティで保護するために Cisco Webex キー管理システム（KMS）を使用しますが、ハイブリッド メッセージ サービス で KMS のオンプレミスインスタンスを使用することもできます。<br>Cisco Webex ハイブリッド データ セキュリティ 導入の詳細については、https://www.cisco.com/go/hybrid-data-securityを参照してください。 |
| モバイルおよび Remote Access（MRA）との共存 | MRA に使用される Expressway クラスタにメッセージコネクタをインストールすることは推奨されません。これを行う場合は、ノードごとに最大 100 人のメッセージ サービス ユーザ、クラスタごとに最大 500 人のメッセージ サービス ユーザのみがサポートされます。 |

| 機能 | 説明 |
|---|---|
| 導入の規模 | 現在、ハイブリッド メッセージ サービス が有効にされた組織ごとに最大 75,000 人のユーザがサポートされます。<br><br>この制限は、組織内の、ハイブリッド メッセージ サービスを使用するユーザのサブセットに適用されます。これは、Webex Teams に対して有効にするユーザの数に影響しません。すべての Jabber ユーザを Cisco Webex にインポートしてください。<br><br>ハイブリッド メッセージ サービス のスケールと共存について詳しくは、https://help.webex.com/article/nv5p67gを参照してください。<br><br>Expressway コネクタクラスタごとに、最大 5 つの IM およびプレゼンスサービス クラスタを導入できます。<br><br>1 つの IM およびプレゼンスサービス クラスタで複数のコネクタクラスタを使用することは推奨されません。 |
| Jabber 導入環境と他のドメイン間の XMPP または SIP メッセージング フェデレーション | ハイブリッド メッセージ サービス は、IM およびプレゼンスサービス とサードパーティのメッセージプロバイダー間のドメイン間フェデレーションとは連動しません。<br><br>つまり、フェデレーションされた組織の連絡先が ハイブリッドメッセージサービスユーザにメッセージを送信した場合、メッセージは Jabber で表示されますが、Webex Teams では表示されません。 |
| IM およびプレゼンスサービスノードの高可用性とフェールオーバー | メッセージコネクタは、プレゼンス冗長グループの高可用性設定を認識します。メッセージコネクタは、フェールオーバー/フォールバック イベントに自動的に応答します。 |

# 連絡先

サポートされていません。Webex Teams には連絡先の概念がありません。メッセージコネクタは Jabber 連絡先に対し、何の操作も行いません。

# ダイレクトメッセージング インターフェイス（1 対 1）

- すべての ハイブリッド メッセージ サービス ユーザが Webex Teams を使用して、組織内のすべての Webex Teams ユーザにメッセージを送信できます。
- すべての ハイブリッド メッセージ サービス ユーザが Jabber を使用して、組織内のすべての Webex Teams ユーザにメッセージを送信できます。

- ハイブリッド メッセージ サービス の利用資格を持たない Webex Teams ユーザが、他のユーザの Jabber クライアントにメッセージを送信することはできません。
- 両者が ハイブリッド メッセージ サービス ユーザである場合、両方のクライアントでやり取りされた会話を完全に確認できます。
- 「入力中」ステータスがサポートされています。これは、片方のユーザが応答を入力している際に、ユーザインターフェイスでもう一方のユーザにインジケータが表示されることを意味します。
- 開封確認がサポートされています。これはユーザにとって、Jabber と Webex Teams 間で未読メッセージ数が同期されることを意味します。
- Webex Teams ユーザが 1 対 1 のスペースからメッセージを削除すると、Jabber ユーザには「ユーザ名が以前に投稿されたメッセージを削除するために Cisco Webex Teams を使用しました（Username used Cisco Webex Teams to delete a previously posted message）」という通知が表示されます。対応する Jabber メッセージは削除されません。
- プレーンテキストのみ。Webex Teams のマークダウンは Jabber のリッチテキストに変換されません。Jabber のリッチテキストは Webex Teams のマークダウンに変換されません。
- Teams 内のメッセージの編集はサポートされています。メッセージサービスのユーザが Teams 内のメッセージを編集すると、メッセージコネクタが編集後のメッセージを Unified CM IM and Presence に送信します。Jabber の受信者には、編集後のメッセージが新しいメッセージとして表示されますが、メッセージの元のバージョンは引き続き表示できます。

  Teams は、元のメッセージが Jabber で表示されなくなったとしても、元のメッセージを引き続き Jabber で表示できることをユーザに通知しません。

# オフラインストレージ

オフラインストレージは、ハイブリッド メッセージ サービス ユーザの 1 対 1 のメッセージングのやり取りに影響します。

ハイブリッド メッセージ サービス の利用資格を持つ Webex Teams ユーザが別の Webex Teams ユーザにメッセージを送信するときに想定される動作は、送信者の Jabber もそのメッセージを受信者の Jabber に送信することです。受信者が Jabber を使用していない場合、オフラインストレージの状態に応じて、次のいずれかの処理が行われます。

- IM およびプレゼンスサービス でオフラインストレージが有効にされている場合：メッセージは保存され、受信者が Jabber にサインインすると送信されます。
- IM およびプレゼンスサービス でオフラインストレージが有効にされていない場合：メッセージは廃棄されます。送信者が 12.5 より前のバージョンを使用している場合は、送信者に「メッセージを配信できませんでした（Message could not be delivered）」というエラーが表示されます。

この場合、送信者と受信者はWebex Teamsを使用しているため、どちらのユーザにもこのメッセージが配信されたと表示されることがあります。これは予期される動作ですが、ユーザを混乱させる可能性があります。

オフラインストレージは、 の [オフライン中の相手へのインスタントメッセージの送信を無効にする（Suppress Offline Instant Messaging）] 設定によって制御されます。IM およびプレゼンスサービス

（注） オフライン メッセージに関する既知の問題があります。メッセージサービスユーザが Webex Teams でオンラインに戻ると、保存されたメッセージは Webex Teams で再生されますが、順序が間違っている可能性があります。ユーザの Jabber クライアントでは、同じメッセージが順番に再生されます。

# グループメッセージング

サポートされていません。Webex Teams のスペースは、Jabber のグループチャットに変換されません。Jabber のグループ チャットは、Webex Teams のスペースに変換されません。

以下に、ユーザがグループメッセージングの相互運用性を試す際の既知の動作をリストします。通常、これらの動作は問題があることを示すわけではありませんが、これによりユーザの混乱を招く可能性があります。

- Jabber ユーザがグループチャットを作成するとき、または連絡先をグループチャットに招待するときは、ハイブリッド メッセージ サービス の利用資格を持つ Webex Teams ユーザを参照して選択できます。ただし、選択した連絡先をグループチャットに追加しようとしても、Webex Teams ユーザは追加されません。Jabber ユーザは、通常どおりグループチャットに追加されます。問題を示す UI フィードバックはありません。
- ハイブリッド メッセージ サービス の利用資格を持つ Jabber ユーザが Webex Teams の使用に切り替えると、他の Jabber ユーザとのグループチャットのすべてで、アクティブな名簿から直ちにそのユーザが削除されます。
- Webex Teams ユーザは、任意の Webex Teams のみのユーザまたは ハイブリッド メッセージ サービス ユーザを追加できます。Jabber を使用している ハイブリッド メッセージ サービス ユーザを追加した場合、そのユーザには Webex Teams スペースに追加されたことが示されません。この問題はスペース内の他のユーザだけが確認できます。該当するハイブリッド メッセージ サービス ユーザからの開封確認がないためです。
- ハイブリッド メッセージ サービス ユーザが Jabber を使用して常設グループチャットに参加した後、メッセージングのやり取りに Teams を使用するように切り替えた場合、Teams 内での [アクティブ（Active）] ステータスは、常設グループチャットで [応答可能（Available）] プレゼンスに変換されます。他の Jabber ユーザは、そのユーザが会話を追っているとみなす可能性があります。ただし、応答可能に見えるユーザが Jabber を開いていなければ、その常設チャットでの以降の投稿には気付きません。

# プレゼンスの変換

ハイブリッド メッセージ サービスは Jabber から Teams への移行を容易にするための過渡的な方策であることを前提として、プレゼンスの変換には最小限のアプローチを取っています。ハイブリッド メッセージ サービスの設計には、両方のクライアントを無期限で使用するユーザは考慮されていません。これは、Unified CM IM and Presence が構成されたプレゼンスを計算する方法により、Jabber ユーザに連絡先の予期しないプレゼンスステータスが表示される可能性があるためです。

### Webex Teams ユーザから見た Jabber クライアントのプレゼンス

プレゼンスは Cisco Jabber から Webex Teams に変換されません。

（注） この制限は、応答不可の動作に影響します。具体的には、ユーザが自分の Jabber プレゼンスを手動で「応答不可」から「応答可能」にリセットすると、対応する Teams のステータスが変更されません。通常、このアクションにより、ユーザがログインしているすべてのクライアント/デバイスのプレゼンスがリセットされるため、混乱を招きます。

### Jabber ユーザから見た Webex Teams クライアントのプレゼンス

Webex Teams から Cisco Jabber へのメッセージングは部分的にサポートされています。

#### 機能のしくみ

メッセージコネクタ は 10 分間隔で Cisco Webex をポーリングして、すべてのユーザのプレゼンスステータスをチェックします。この情報をデバイスプレゼンスとして Unified CM IM およびプレゼンスサービスに送信します（つまり、ステータスはユーザによって手動で変更されるのではなく、デバイスまたはクライアントによって推測されることを意味します）。

ハイブリッド メッセージ サービスのユーザが Teams または Jabber のいずれかを使用している場合、この手法による結果は予測可能ですが、移行のシナリオでは、ユーザが両方のクライアントを使用していることを想定しています。

ユーザが、デバイスプレゼンスを送信する複数のクライアントまたはデバイスを使用している場合、IM およびプレゼンスサービス はそのユーザの最新の更新を優先し、そのプレゼンスをすべての登録 Jabber ユーザに表示します。

ユーザが手動で Jabber ステータスを変更する場合は常に、IM およびプレゼンスサービス は手動プレゼンスを優先します。この場合、Teams または Jabber のどちらから送信されたかにかかわらず、デバイスプレゼンスは他の Jabber ユーザに表示されません。

次の表に、ハイブリッド メッセージ サービスのユーザがいる場合に Jabber ユーザに表示される可能性のあるプレゼンス状態のいくつかを記載します。お客様の環境で行われる可能性のあるやり取りのすべてを完全にテストすることはできないため、これは考えられるシナリオのベストエフォートによるマッピングです。

| 別の Jabber ユーザから見たユーザのプレゼンス | IM およびプレゼンスサービス によってプレゼンスが確立された方法 |
|---|---|
| **応対可**<br>連絡先のプレゼンスインジケータが緑色になります。 | • 連絡先は Jabber のみを使用しており、Jabber により、ユーザが**応答可能**であると判断されました。<br>• 連絡先は Jabber と Teams を使用しており、Jabber により、ユーザが**応答可能**であると判断されました。IM およびプレゼンスサービス は、同じユーザの Teams クライアントからのプレゼンスより後に、プレゼンス更新を受信しました。<br>• Jabber ユーザに、Teams のみを使用しているユーザのこのプレゼンスが表示されることはありません。 |
| [**応答可能** @ Cisco Webex Teams（Available @ Cisco Webex Teams）]<br>連絡先のプレゼンスインジケータが緑色になり、「@ Cisco Webex Teams」というテキストが表示されます。 | • 連絡先は Teams のみを使用しており、過去 10 分の間に Webex Teams で **[アクティブ（Active）]** な状態になりました。<br>• 連絡先は Jabber と Teams を使用しており、過去 10 分の間に Webex Teams で **[アクティブ（Active）]** な状態になりました。IM およびプレゼンスサービス は、同じユーザの Jabber クライアントからのデバイスプレゼンスの後に、Teams からのプレゼンス更新を受信しました。<br>• Jabber ユーザに、Jabber のみを使用しているユーザのこのプレゼンスが表示されることはありません。 |
| **[応答可能（Available）]** とカスタムメッセージ | • 連絡先は Jabber のみを使用しており、手動でプレゼンスのステータスを変更しました。<br>• 連絡先は Jabber と Teams を使用しており、Jabber で手動によりプレゼンスのステータスを変更しました。IM およびプレゼンスサービス は、同じユーザの Teams クライアントからのデバイスプレゼンスの更新よりも、Jabber から手動で編集されたプレゼンスを優先します。<br>• Jabber ユーザに、Teams のみを使用しているユーザのこのプレゼンスが表示されることはありません。 |
| **[退席中（Away）]**<br>連絡先のプレゼンスインジケータがオレンジ色になります。 | • 連絡先は Jabber のみを使用しており、Jabber により、ユーザが**退席中**であると判断されました。<br>• 連絡先は Jabber と Teams を使用しており、Jabber により、ユーザが**退席中**であると判断されました。IM およびプレゼンスサービス は、同じユーザの Teams クライアントからのプレゼンスより後に、プレゼンス更新を受信しました。 |

| 別の Jabber ユーザから見たユーザのプレゼンス | IM およびプレゼンスサービス によってプレゼンスが確立された方法 |
|---|---|
| | • Jabber ユーザに、Teams のみを使用しているユーザのこのプレゼンスが表示されることはありません。 |
| [**退席中** @ Cisco Webex Teams（Away @ Cisco Webex Teams）]<br><br>連絡先のプレゼンスインジケータがオレンジ色になり、「@ Cisco Webex Teams」というテキストが表示されます。 | • 連絡先は Teams のみを使用しており、最後に [アクティブ（Active）] の状態になってから 10 分以上経過していますが、24 時間は経過していません。Teams では、たとえば **[2 時間前にアクティブ（Active 2 hours ago）]**、**[昨日アクティブ（Active yesterday）]** として表示されます。<br><br>• 連絡先は Jabber と Teams を使用しており、Jabber で [応答可能（Available）] の状態になった後に、Webex Teams で [アクティブ（Active）] の状態になりました。IM およびプレゼンスサービスが Teams からデバイスプレゼンスを受信してから 10 分以上経過していますが、24 時間は経過していません。また、そのプレゼンス更新を受信したのは、同じユーザの Jabber クライアントからデバイスプレゼンスを受信した後です。<br><br>• 通常、Jabber ユーザに、Jabber のみを使用している他のユーザのこのプレゼンスが表示されることはありません。ハイブリッド メッセージサービスが有効にされているユーザは、実際には Teams を使用していなくても、そのプレゼンスは Teams を使用しているかのように構成されます。この場合、通常はユーザの Jabber プレゼンスが優先されますが、[退席中 @ Cisco Webex Teams（Away @ Cisco Webex Teams）] として示されることもあります。これに該当するのは、たとえば外出中のユーザのカレンダーが Cisco Webex と統合されている場合です。<br><br>• [退席中 @ Cisco Webex Teams（Away @ Cisco Webex Teams）] は、Webex Teams ではユーザが**不在**の状態であることを意味する場合もあります。Teams は、そのユーザのアバターに飛行機のオーバーレイを示します。<br><br>Teams での [不在（Out of Office）] ステータスは、ユーザカレンダーと統合すると表示されます。ユーザの Teams クライアントが予定表と統合されていなければ、Teams に [不在（Out of Office] ステータスは表示されません。<br><br>予定表で [不在（Out of Office）] がレポートされている間に Teams のユーザが Teams を使用すると、そのユーザの Teams ステータスが [アクティブ（Active）] に戻ります。これは、そのユーザの Jabber プレゼンスで [応答可能（Available）] に正しく変換されます。 |

| 別の Jabber ユーザから見たユーザのプレゼンス | IM およびプレゼンスサービス によってプレゼンスが確立された方法 |
|---|---|
| | • Teams ユーザは、ステータスを共有していません（Teams の設定で **[ステータスの表示（Show statuses）]** がオフになっています）。<br>Teams ユーザはステータスを非表示にすることができます。非表示にすると、他の Teams ユーザのステータスも表示されなくなります。Jabber ユーザには、これらのユーザが [退席中（Away）] として表示されます。<br>ユーザが [退席中（Away）] の状態になっている間、メッセージコネクタがユーザの XMPP セッションを破棄することはありません。ユーザがステータスを非表示にしている場合、そのユーザが過去 24 時間に Webex Teams を使用していなくても、ユーザのセッションは維持されます。 |
| **[退席中（Away）]** とカスタムメッセージ | • 連絡先は Jabber のみを使用しており、手動でプレゼンスのステータスを変更しました。<br>• 連絡先は Jabber と Teams を使用しており、Jabber で手動によりプレゼンスのステータスを変更しました。IM およびプレゼンスサービス は、同じユーザの Teams クライアントからのデバイスプレゼンスの更新よりも、Jabber から手動で編集されたプレゼンスを優先します。<br>• Jabber ユーザに、Teams のみを使用しているユーザのこのプレゼンスが表示されることはありません。 |
| **サイレント**<br>連絡先のプレゼンスインジケータが赤色になります。 | これはユーザレベルの設定です。つまり、ユーザがログインしているすべてのクライアント/デバイス（該当する場合は電話機を含む）に [着信拒否（Do Not Disturb）] のステータスがあります。<br>• 連絡先は Jabber を使用しており、手動でステータスを **[着信拒否（Do Not Disturb）]** に変更しました。<br>ユーザが Teams も使用している場合、メッセージコネクタは Jabber から Teams にプレゼンスを変換しないため、Teams プレゼンスには影響がありません。<br>また、IM およびプレゼンスサービス は常に、Teams からのデバイスプレゼンスよりも、Jabber からの手動 DND を優先します。<br>• 連絡先は Teams を使用しており、*30* 分～ *24* 時間の期間を設定して手動でステータスを **[着信拒否（Do Not Disturb）]** に変更しました。 |

| 別の Jabber ユーザから見たユーザのプレゼンス | IM およびプレゼンスサービス によってプレゼンスが確立された方法 |
|---|---|
| | Teams ユーザが [着信拒否（Do Not Disturb）] を有効にすると、Teams は他の Teams ユーザに対し、着信拒否しているユーザのアバターに三日月のオーバーレイを表示します。<br>• 連絡先は両方のクライアントを使用しており、*30* 分～ *24* 時間の期間を設定して手動でステータスを **[着信拒否（Do Not Disturb）]** に変更しました。<br>設定した期間が経過するまで、またはユーザが Teams でステータスを変更するまでは、両方のクライアントでこのステータスが維持されます。<br>両方のクライアントを使用しているユーザは、Jabber でプレゼンスを変更しても [着信拒否（Do Not Disturb）] ステータスをリセットできません（Teams を使用するか、Teams で着信拒否期間が経過するまで待つ必要があります）。これは、メッセージコネクタは Jabber から Teams にプレゼンスを変換しないためです。 |
| Offline<br>連絡先のプレゼンスインジケータが灰色になります。 | もう一方のユーザは、過去 24 時間以内に Webex Teams または Jabber を使用していません。メッセージコネクタ は、オフラインユーザの Webex Teams に対して保留にしていた XMPP セッションを破棄します。<br>特定の メッセージコネクタ ホストで非アクティブ状態になっているハイブリッド メッセージ サービス ユーザの数を確認するには、**[アプリケーション（Applications）]** > **[ハイブリッドサービス（Hybrid Services）]** > **[メッセージサービス（Message Services）]** > **[メッセージサービスのステータス（Message Service Status）]** に移動します。 |

Teams のステータスについては、次を参照してください。

- *Cisco Webex Teams* でのステータス（https://collaborationhelp.cisco.com/article/wghlt5）
- ステータスの共有を停止する（https://collaborationhelp.cisco.com/article/nkzs6wl）

# ファイル転送

- Webex Teams ユーザは Jabber ユーザとファイルを共有できます。Webex Teams で 1 対 1 のスペースにファイルが添付されると、Jabber ユーザにそのファイルへのリンクが表示されます。
- Webex Teams ユーザが 1 対 1 のスペースからファイルを削除した場合、Jabber ユーザにメッセージが表示されます。

- Jabber ユーザが Webex Teams ユーザにファイルを送信することはできません。

  Jabber ユーザが Webex Teams ユーザと通信している間、Jabber のファイル転送とスクリーンキャプチャのオプションは無効になります。

  ただし、IM およびプレゼンスサービス でマネージドファイル転送（MFT）が有効になっていると、これらの機能の Jabber オプションが使用可能であるように見えます。この場合、Jabber ユーザがファイルを送信しようとすると、Webex Teams ユーザは、Jabber からファイルが送信されたことの通知を受信します。

  ファイルが送信された時点で Teams ユーザが Jabber にログインしていない場合、そのユーザはファイルを受信しません。

  この動作は、受信者がオンプレミスの（IM and Presence に登録された）Jabber を使用しているか、Webex に登録された Jabber を使用しているかどうかにかかわらず、受信者に影響します。

# 移行に関する考慮事項

ハイブリッド メッセージ サービスを使用してユーザベースを Cisco Jabber から Webex Teams に段階的に移行する場合は、次の問題と問題軽減策を考慮すると、移行を計画する上で役立ちます。

- **管理者が生成する Webex Teams への参加招待**：ハイブリッド メッセージ サービスを機能させるための 1 つの要件は、CSV またはハイブリッド ディレクトリ サービスによってすべての Jabber ユーザを Cisco Webex にインポートすることです。ユーザをインポートすると、それらのユーザのすべてに Webex Teams の使用を開始するための招待が送信されますが、これが行われないようにすることをお勧めします。Control Hub で組織の SSO が有効にされている場合、ユーザをインポートする前に、電子メールによる招待の動作を抑制できます。https://help.webex.com/article/g5ey83を参照してください。

  残念ながら、組織の SSO が有効にされていない限り、これらの初期招待メールの送信を抑制することはできません。

  招待メールの送信を抑制すると、Webex Teams への予期しない早期アクセスの問題を軽減できます。

- **ユーザが生成する Webex Teams への参加招待**：Cisco Webex は通常、Cisco Webex にすでに追加されているユーザがまだ Teams を使用していない場合、それらのユーザに Teams の使用を開始するための招待を送信します。ハイブリッド メッセージ サービスを有効にすると、この「セルフサブスクライブ」動作は自動的に組織に対して無効になります。

  このように設計されている理由は、メッセージサービスのユーザが別の Jabber ユーザにメッセージを送信するたびに、Webex は Teams の使用を開始するよう受信者を招待する電子メールを生成するためです。この電子メールは、まだ Teams を使用していない Jabber ユーザにとってはスパムになります。

- **Webex Teams への予期しない早期アクセス**：ハイブリッド メッセージ サービスを機能させるための 1 つの要件は、CSV またはハイブリッド ディレクトリ サービスによってすべ

ての Jabber ユーザを Cisco Webex にインポートすることです。インポートしたユーザにまだ Webex Teams の使用を開始させたくないとしても、ユーザがディレクトリサービスと同期されていて、かつ SSO が有効にされている場合、Webex Teams クライアントの使用を防ぐ技術的な理由はありません。これは、ハイブリッド メッセージ サービスが有効にされていないユーザにとって相互運用性の問題につながる可能性があります。

次に例を示します。

- Teams で別のユーザと会話している ハイブリッド メッセージ サービス ユーザがその会話を Jabber で表示すると、自分側の会話しか表示されません。また、Jabber では会話相手が [オフライン（Offline）] として表示されます（ただし、Teams では [アクティブ（Active）] として表示されます）。
- 同じシナリオで、ハイブリッド メッセージ サービス ユーザが Jabber を使用して会話を続けようとすると、ユーザのメッセージは Teams 内の他のユーザに送信されますが、そのユーザからの応答は Jabber に返されません。

ユーザが技術的には Webex Teams を使用できるとしても、Jabber の使用を続けさせる必要がある移行計画に従う場合、クライアントがインストールされないようにするか、ユーザに潜在的な相互運用性の問題を知らせることをお勧めします。

- **ユーザの Jabber ID（JID）がユーザの Webex Teams UID と異なっている**：Teams UID はユーザの電子メールアドレスでなければなりませんが、Jabber ID は電子メールアドレスのように見えても、必ずしも電子メールアドレスである必要はありません。

  Webex Teams を使用する際は、ユーザを JID で検索しないでください。Jabber クライアントでユーザを検索するには、JID（または名前）を使用します。Webex Teams でユーザを検索するには、電子メールアドレス（または名前）を使用します。

- **オフラインメッセージの抑止**：ユーザが Webex Teams を使用して互いにチャットを開始する場合でも、ユーザは引き続き Cisco Jabber にアクセスできます。ユーザが両方のクライアントでオンラインになっている場合、ハイブリッド メッセージ サービスは両方のクライアントを使用してメッセージを配信しようとします。受信者が Jabber でオフラインになっている場合、送信者は IM およびプレゼンスサービス から混乱を招くオフラインメッセージを受信する可能性があります。

  この問題を軽減するには、次のようにします。

  1. Cisco Unified CM IM and Presence Administration にサインインして、**[メッセージング（Messaging）]** > **[設定（Settings）]** に移動します。
  2. **[オフライン中の相手へのインスタント メッセージの送信を無効にする（Suppress Offline Instant Messaging）]** チェックボックスをオフにしてから、**[保存（Save）]** をクリックします。

（注） オフライン メッセージに関する既知の問題があります。メッセージサービスユーザが Webex Teams でオンラインに戻ると、保存されたメッセージは Webex Teams で再生されますが、順序が間違っている可能性があります。ユーザの Jabber クライアントでは、同じメッセージが順番に再生されます。

# メッセージフローとセキュリティ

パブリックインターネット経由で送信されるインスタントメッセージはすべて、Cisco Webex クラウドに組み込まれているキー管理サービス（KMS）を使用して暗号化されます。インスタントメッセージのセキュリティを確保するために構成しなければならない設定はありません。

（注） ハイブリッド メッセージ サービス は、Cisco Webex ハイブリッド データ セキュリティ と呼ばれる、KMS のオンプレミスインスタンスでは機能しません。

### Cisco Jabber からのメッセージ Webex Teams

1. 送信者が Jabber クライアントからメッセージを送信します。メッセージは IM およびプレゼンスサービス にルーティングされて、そこから受信者の Jabber クライアントに送信されます。これが通常の IM およびプレゼンスサービス のフローです。このフローは必要に応じてセキュアにすることができます（このドキュメントの範囲外です）。
2. 受信者がデュアルユーザであり、ハイブリッド メッセージ サービス の利用資格を持っている場合、メッセージは Expressway 上の メッセージコネクタ にもルーティングされます。

   受信者が最近 Webex Teams でアクティブになっていない場合、メッセージは メッセージコネクタ にルーティングされません。処理リソースとメモリ リソースを節約するために、ユーザの非アクティブ状態が 24 時間以上続くと、ユーザは Webex Teams で応答しないとみなされるためです。

   IM およびプレゼンスサービス クラスタと、メッセージコネクタ をホストする Expressway クラスタとの間の接続を保護することを選択できます。
3. メッセージコネクタ は（クラウドベースのメッセージングサービスを介して）キー管理サービスと相互作用し、暗号キーを要求します。メッセージングサービスは、既存のスペースのキーを取得するか、新しいスペースの最初のメッセージ（「会話」または「ルーム」）である場合は新しいキーを取得して、メッセージコネクタ にそのキーを渡します。
4. メッセージコネクタ は必要に応じて Cisco Webex で新しい会話を確立し、暗号化されたメッセージをその会話に投稿します。

   この暗号化はオプションではなく、構成する必要はありません。

5. Cisco Webex がメッセージを受信者の Webex Teams クライアントに安全に送信します。このメカニズムの説明は、このドキュメントの範囲外です。

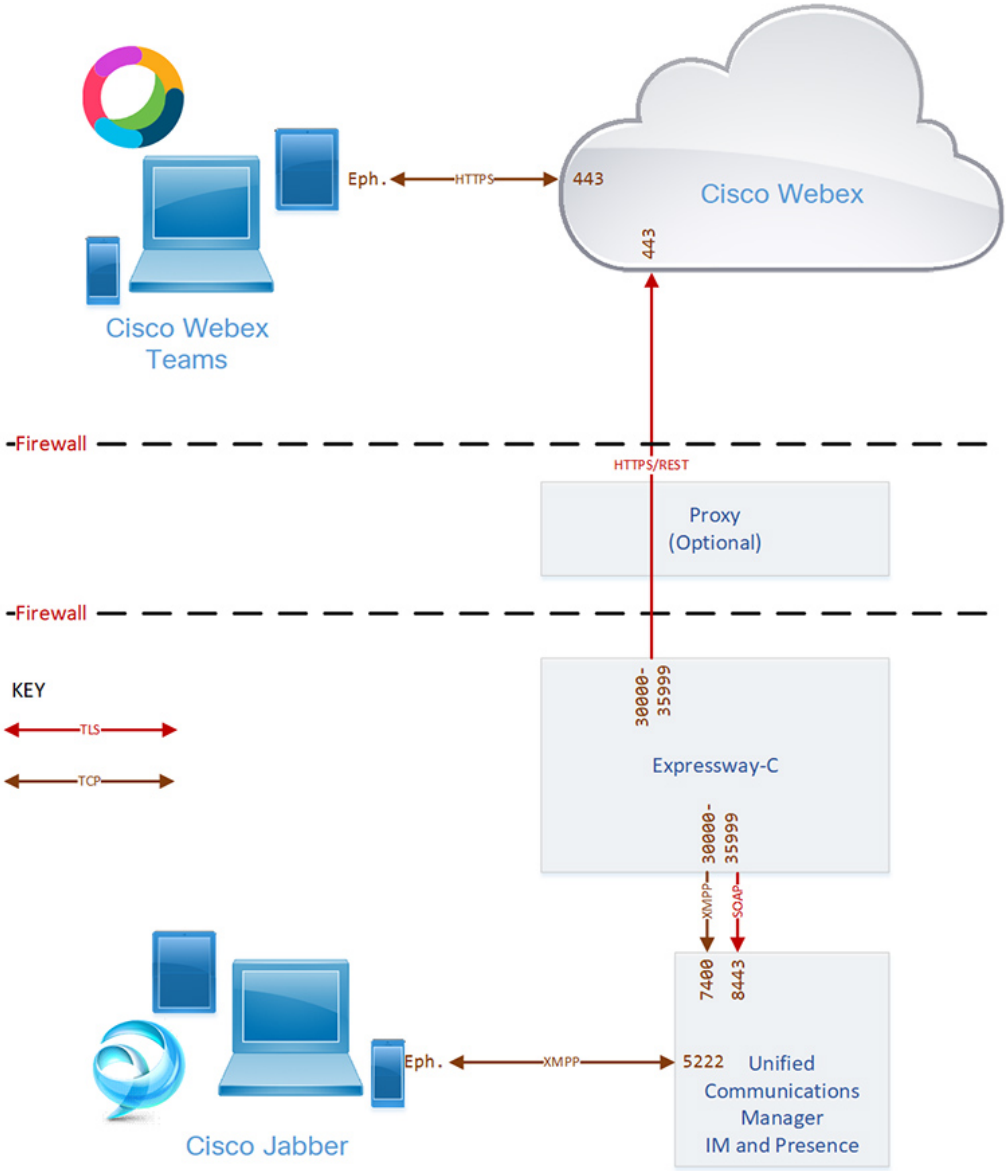
### Webex Teams から Cisco Jabber へのメッセージ

Webex Teams アプリが Cisco Webex に接続すると、Cisco Webex が自己認証を行うためにサーバ証明書を返します。ユーザがアクティブな間、この接続はアプリによって維持されます。アプリはキー管理サービスと連携して、各ユーザと各スペース（「会話」または「ルーム」）の暗号キーを動的に生成します。

1. 送信者は Webex Teams を使用して、受信者にメッセージを送信します。Webex Teams アプリがメッセージを暗号化してから Cisco Webex に送信します。Cisco Webex は暗号化されたメッセージを受信者の Webex Teams クライアントで使用できるようにします。これが通常の Webex Teams のメッセージフローです。このフローは常にセキュアですが、そのメカニズムの説明はこのドキュメントの範囲外です。
2. Cisco Webex が自身のメッセージングサービス データベースをチェックして、送信者と受信者に ハイブリッド メッセージ サービス の利用資格があるかどうかを確認します。また、受信者宛てのメッセージのルーティング先も確認します。
3. Cisco Webex クラウドが暗号化されたメッセージを メッセージコネクタ に送信します。
4. メッセージコネクタ は（クラウドベースのメッセージングサービスを介して）キー管理サービスと連携し、Webex Teams スペースの復号キーを要求します。
5. メッセージコネクタ がメッセージを復号してから IM およびプレゼンスサービス に送信します。
6. IM およびプレゼンスサービス が、受信者の Jabber クライアントへのメッセージのルーティングを試みます。
7. メッセージが既読になると、コネクタは開封確認を検出し、その開封確認を Cisco Webex に返します。これにより、メッセージング クライアント間でユーザの未読メッセージの一貫性が維持されます。

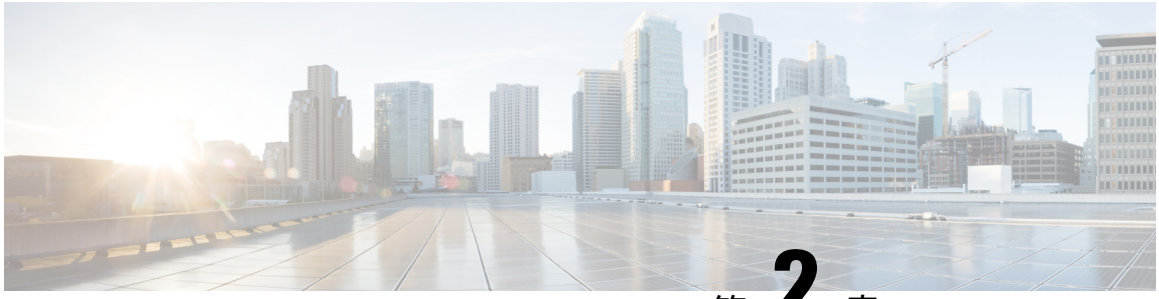
# ハイブリッド メッセージ サービス 接続

図 *12*：ハイブリッド メッセージ サービス 接続



# メッセージサービスのポート

| 目的 | Src. IP | Src. ポート | プロトコル | 宛先のIP | 宛先のポート |
|---|---|---|---|---|---|
| 基本メッセージング | Webex Teamsclients | エフェメラル | TCP | Cisco Webex hosts | 443 |
| 永続的な HTTPS 登録 | コネクタホスト Expressway | 30000-35999 | TLS | Cisco Webex hosts | 443 |
| XMPP（IM and Presence） | コネクタホスト Expressway | 30000-35999 | TCP | Unified CM IM and Presence パブリッシャ | 7400 |
| AXL クエリ（管理 XML レイヤ） | コネクタホスト Expressway | 30000-35999 | TCP | Unified CM IM and Presence パブリッシャ | 8443 |
| メッセージングとプレゼンス | Cisco Jabber クライアント | エフェメラル | TCP | Unified CM IM and Presence パブリッシャ | 5222 |



第 2 章

# 環境の準備 ハイブリッド メッセージ サービス


- ハイブリッド メッセージ サービス の要件 （31 ページ）
- ユーザの管理 ハイブリッド メッセージ サービス （33 ページ）
- 管理者招待メール送信の抑止 （35 ページ）
- Cisco Webex ハイブリッド サービス に対する Expressway-C コネクタホストの前提条件の対処 （35 ページ）


## ハイブリッド メッセージ サービス の要件

ハイブリッド メッセージ サービス を有効にするには、次の表に記載されているサポート対象の Cisco Presence ソフトウェアを使用する必要があります。Cisco Business Edition のすべてのパッケージには Cisco Unified Communications Manager と IM およびプレゼンスサービス が含まれています。適切なバージョンを使用していることを確認してください。

**表 *1 :* 必要な *Cisco* コンポーネント**

| 製品名 | Version |
|---|---|

| | |
|---|---|
| Cisco Unified Communications Manager および IM およびプレゼンスサービス （オンプレミスまたはサービスプロバイダーでホストされているもの） | 11.5(1)SU3 以降<br>• すべてのパブリッシャノードでAXLサービスが実行されている必要があります。また、HA 導入環境では、IM およびプレゼンスサービス クラスタ内のすべてのノードで AXL サービスを実行することをお勧めします。<br>• 複数の IM およびプレゼンスサービス クラスタを使用する場合は、それらのクラスタ間で Intercluster Sync AGENT （ICSA）を有効にする必要があります。<br>• IM およびプレゼンスサービス クラスタのいずれかが 10.5(2) よりも前のバージョンからアップグレードされている場合は、それらのクラスタに Cisco Options Package （COP ファイル）を適用して ハイブリッド メッセージ サービス 用に準備する必要があります。<br>*ciscocm.cup-CSCvi79393-v1.cop.sgn* ファイルとその適用手順は、https://software.cisco.com/download/home/286269517/type/282074312/release/UTILS から入手できます。<br>• IM およびプレゼンスサービス クラスタで Multiple Device Messaging（MDM）が有効にされている必要があります（この機能はデフォルトで有効にされています）。 |
| Cisco Jabber（任意のクライアント プラットフォーム） | 11.9 以降 |
| Cisco Webex Teams（任意のクライアント プラットフォーム） | |

Cisco Webex Control Hub を使用して組織を作成できるよう、Cisco Webex のライセンスを取得する必要があります。

**表 *2: Cisco Webex* ライセンス**

| 製品 | SKU |
|---|---|
| Cisco Webex | 任意のクラウドの有料オファー |

ハイブリッド メッセージ サービス を導入して管理するには、次のシステムを使用する必要があります。これらのシステムは、ハイブリッドメッセージサービスだけでなく、Webex Teams とハイブリッドサービスを導入する場合に一般に必要となります。

**表 *3:* サポートされるシステム**

| System | 必要となる理由 |
|---|---|

| | |
|---|---|
| 制御ハブ | Cisco Webex にログインして組織を作成してから、サービス、リソース、ユーザを管理するため。https://collaborationhelp.cisco.com/article/nkp3vu5を参照してください。 |
| Cisco Webex ハイブリッドディレクトリ サービス | （省略可）オンプレミスディレクトリのユーザ属性を 制御ハブ にマッピングして、ハイブリッドサービスを使用できるようにするため。「https://www.cisco.com/go/hybrid-services-directory」を参照してください |
| Cisco Unified CM Administration | 手動でユーザを作成するため、またはオンプレミスディレクトリを統合して IM およびプレゼンスサービス のユーザをプロビジョニングするため。 |
| Firewalls | コンポーネントシステム間のファイアウォールで必要なポートを開くため。 |

コネクタをホストするには、Expressway を導入する必要があります。Cisco Hosted Collaboration Solution を使用している組織は、社内に Cisco Expressway は必要ありません。代わりに、Hosted Collaboration Solution のパートナーが、その Cisco Webex ハイブリッド サービス オファーの一部としてクラウド内にそれを導入します。

**表 4 : *Cisco Expressway* の詳細**

| 要件 | Version |
|---|---|
| Cisco Expressway コネクタ ホスト | ソフトウェア イメージは software.cisco.com から無料でダウンロードできます。<br>コネクタ ホストには、最新リリース バージョンの Expressway をお勧めします。詳細については、*Cisco Webex* ハイブリッド サービスでサポートされる *Expressway* コネクタホスト（https://collaborationhelp.cisco.com/article/ruyceab）を参照してください。 |

# ユーザの管理 ハイブリッド メッセージ サービス

### オンプレミスの対象ユーザ

Jabber 導入環境を Cisco Webex に接続する前に、Jabber ユーザが次の場所に存在する場合があります。

- **Cisco Unified CM Administration**

  この要件は、Jabber のオンプレミス導入を行うことによってすでに満たされています。ユニファイド CM 内に存在しない Jabber ユーザは、互いにメッセージを交換できません。

  ユーザは手動で作成することも、LDAP ディレクトリと同期することもできます。

- （推奨）**LDAP ディレクトリ**

  LDAP ディレクトリを使用してユーザを管理する場合は、ユーザを Unified CM Administration に同期することをお勧めします。別の方法として、2 つの場所で手動同期によりユーザを管理することができます。

  https://www.cisco.com/c/en/us/support/unified-communications/unified-presence/tsd-products-support-series-home.html で、ご使用のバージョンの IM およびプレゼンスサービス のマニュアルを参照してください。

### クラウドベースの対象ユーザ

ハイブリッド メッセージ サービス を導入する一環として、Cisco Webex に組織内の対象ユーザが存在している必要があります。他のハイブリッドサービスまたは Cisco Webex Teams を導入している場合、Cisco Webex にはすでに組織とユーザが存在しているはずです。

最大限の相互運用性を得るために、すべての Jabber ユーザを Cisco Webex にインポートすることをお勧めします。これらのユーザに有料のサブスクリプションは必要ありませんが、Teams の「Message Free」の利用資格がなければなりません。ユーザをインポートする前に、**自動ライセンス割り当てテンプレート**を使用して、この利用資格を適用できます。

Jabber ユーザをインポートする前に、（Control Hub で）組織の SSO を有効にすることを推奨します（https://collaborationhelp.cisco.com/article/lfu88u を参照）。SSO 対応の組織では、インポートされた Jabber ユーザに Teams へのアクセスを許可しない場合、これらのユーザへの電子メール招待を抑止するオプションがあります（https://collaborationhelp.cisco.com/article/nqj88gt を参照）。

対象ユーザは、次の方法で管理できます。

- 制御ハブ で、手動でユーザを個別に入力する。
- 制御ハブ を使用して、ファイル（シスコ提供のテンプレートに基づく、カンマ区切り値ファイル）からユーザのリストをインポートする。

  制御ハブ を使用して、CSV ファイルを使用してエクスポート、編集、インポートを繰り返し、ユーザのサービス利用資格を一括で変更することもできます。

- （推奨）Cisco Webex の組織をオンプレミスディレクトリと同期する。このオプションは Cisco Webex ハイブリッド ディレクトリ サービス と呼ばれます。

  ユーザをインポートする前に、必ず「Message Free」の利用資格を自動ライセンス割り当てテンプレートに適用してください。

  「*Cisco Webex Control Hub* でユーザを追加し管理する方法 」（https://collaborationhelp.cisco.com/article/nj34yk2）を参照してください。

要約すると、ユーザの詳細は複数の場所で維持できますが、少なくとも Cisco Webex と Unified CM Administration には入力されている必要があります。あらゆる場所でユーザを一意に識別する属性は、ユーザの電子メールアドレスです。

オンプレミスとクラウドで対象ユーザをどのように作成するかに関係なく、**ユーザの電子メールアドレスはすべての場所で一致していることが必須**です。

# 管理者招待メール送信の抑止

メッセージサービス導入の一環として、すべての Jabber ユーザを Control Hub にインポートすることをお勧めします。このアクションにより通常は、インポートされた Jabber ユーザに対して Webex Teams の使用を開始するよう招待する電子メールメッセージが生成されます。Jabber ユーザで相互運用性の問題が発生する可能性があることから、すべての Jabber ユーザにではなく、一部のユーザだけに Webex Teams の使用を開始させたい場合もあります。したがって、これらの電子メールの送信を抑止することをお勧めします。

ユーザの一括インポートまたはディレクトリと Control Hub の同期を行う前に、次のタスクを実施する必要があります。

### 始める前に

Webex 組織の SSO を有効にします。https://collaborationhelp.cisco.com/article/lfu88uを参照してください。SSO が有効にされていない場合、招待メールの送信を抑止することはできません。その場合はこのタスクをスキップしますが、このプロセスの後の段階で自動招待メールが生成されることに注意してください。

### 手順

**ステップ 1** Control Hub（https://admin.webex.com/login）にサインインします。

**ステップ 2** **[設定（Settings）]** をクリックして、**[電子メール（Email）]** セクションを見つけます。

**ステップ 3** **[管理者招待メール送信の抑止（Suppress Admin Invite Emails）]** スイッチをスライドします。詳細については、https://collaborationhelp.cisco.com/article/nqj88gtを参照してください。

### 次のタスク

# CiscoWebexハイブリッドサービスに対するExpressway-Cコネクタホストの前提条件の対処

ハイブリッドサービス コネクタソフトウェアをホストする Cisco Webex クラウドに登録する前に、このチェックリストを使用して Cisco Webex ハイブリッド サービス 用の Expressway-C を準備してください。

### 始める前に

Expressway-C を Cisco Webex ハイブリッド サービス のホスティングコネクタ専用にすることをお勧めします。Expressway-C コネクタホストは他の目的でも使用できますが、その場合、サポートされるユーザの数が変わる可能性があります。

（注） ハイブリッドサービスの管理者として、オンプレミスの機器上で実行するソフトウェアに対する制御を維持します。また、物理的および電子的な攻撃からサーバを保護するために必要なすべてのセキュリティ対策を実行する責任もあります。

**手順**

**ステップ 1** Expressway を登録する前に、完全な組織管理者権限を取得し、その組織管理者のクレデンシャルを使用して Cisco Webex Control Hub（https://admin.webex.com）で顧客ビューにアクセスします。

**ステップ 2** 冗長性を考慮して、Expressway-C コネクタホストをクラスタに導入します。サポートされている Expressway のスケーラビリティに関する推奨事項に従います。

- 専用 Expressway-C 上の ハイブリッド メッセージ サービス の場合：
  - それぞれ最大 6 つのノードで構成された複数の Expressway-C クラスタで メッセージ コネクタ をホストできます。
  - メッセージコネクタ を複数の Cisco Unified Communications Manager IM およびプレゼンスサービス クラスタで使用することができます。

**ステップ 3** Expressway-C コネクタホストについては、次の要件に従います。

- サポートされる Expressway ソフトウェアイメージの最小バージョンをインストールします。詳細については、サポート バージョンの説明を参照してください。
- 『*Cisco Expressway Virtual Machine Installation Guide*』に従って、仮想 Expressway OVA ファイルをインスト—ルします。その後、その IP アドレスを参照してユーザインターフェイスにアクセスできます。マニュアルについては、cisco.com にある Cisco Expressway のインストールおよびアップグレードに関するガイドのリストを参照してください。

  （注） 仮想 Expressway のシリアル番号は、仮想マシンの MAC アドレスに基づきます。シリアル番号は、Expressway ライセンスを検証する際および Cisco Webex クラウドに登録された Expressway を識別するために使用されます。**VMware ツールを使用する際に Expressway の MAC アドレスを変更しないでください。変更すると、サービスを使用できなくなるおそれがあります。**

- リリースキー（Expressway シリーズキー）がなくても、 Cisco Webex ハイブリッド サービス 用に仮想 Expressway-C を使用できます。リリース キーに関するアラームが表示されることがあります。確認応答してインターフェイスから削除してかまいません。
- サポートされているブラウザで Expressway Web インターフェイスを使用します。（『Cisco Expressway Administrator Guide』を参照してください）。サポート対象外のブラウザでは、インターフェイスは機能することも機能しないこともあります。Expressway の Web インターフェイスを使用するには、JavaScript と Cookie を有効にする必要があります。

**ステップ 4** 初めて Expressway を実行する際に、Cisco Webex ハイブリッド サービス 用に構成できるよう、初期セットアップウィザードが表示されます。

**Cisco Webex ハイブリッドサービス**を選択します。これにより、リリースキーが不要になります。

**ステップ 5** Expressway-C コネクタホストで以下の要件が満たされていることを確認します。この確認は通常、インストール時に行います。詳細については、cisco.com の Cisco Expressway 設定ガイドのリストにある『*Cisco Expressway Basic Configuration Deployment Guide*』を参照してください。

- 基本的な IP 設定（**[システム（System）] > [ネットワーク インターフェイス（Network interfaces）] > [IP]**）
- システム名（**[システム（System）] > [管理設定（Administration settings）]**）
- DNS 設定（**[システム（System）] > [DNS]**）
- NTP 設定（**[システム（System）] > [時間（Time）]**）
- 管理者アカウントの新しいパスワード（**[ユーザ（Users）] > [管理者アカウント（Administrator accounts）]** で、**管理者**のユーザ(Admin user)をクリックし、[パスワードの変更（Change password）] をクリック）
- root アカウントの新しいパスワード（root として CLI にログオンし、passwd コマンドを実行）

**ステップ 6** Expressway-C を「cluster of one」として設定します。

- 現時点で追加のピアをインストールするつもりがなくても、Expressway をプライマリ ピアとして設定してから登録することをお勧めします。

  **注意** X8.11 およびそれ以降でクラスタの設定を変更する場合、**[システム（System）]> [クラスタリング（Clustering）]** ページからすべてのピア アドレスを削除すると、クラスタから削除するという指示が Expressway に伝わるため注意してください。**Expressway は次に再起動するときに初期設定にリセットされます。**すべてのピアを削除するが、Expressway の設定はそのまま残したい場合は、[クラスタリング（Clustering）] ページで Expressway のアドレスを残し、「cluster of one」でプライマリにします。

- 以下に最低限必要なクラスタ設定を示しますが、詳しくは『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』を参照してください。
  - H.323 プロトコルを有効にします。**[構成（Configuration）] > [プロトコル（Protocols）] > [H.323]** ページで、[H.323 モード（H.323 Mode）] をオンに設定します。

    Expressway で H.323 コールをサポートしていなくても、クラスタリングには H.323 モードが設定されている必要があります。

    （注） [サービス選択（Service Select）] ウィザードを使用してハイブリッドサービスの Expressway を構成した場合、[H.323] メニュー項目は表示されないことがあります。この問題を回避するには、Expressway コンソールにサインインして、コマンド `xconfig H323 Mode: "On"` を実行します。

- **[システム（System）] > [クラスタリング（Clustering）] > [クラスタ名（Cluster name）]** は FQDN にします。

  通常、この FQDN は DNS にある SRV レコードでマップされており、クラスタ ピアの A/AAAA レコードに解決されます。

- **[システム（System）] > [クラスタリング（Clustering）] > [設定プライマリ（Configuration primary）]** を 1 にします。

- **[システム（System）] > [クラスタリング（Clustering）] > [TLS検証モード（TLS verification mode）]** を、少なくとも 2 番目のピアを追加するまでは [許可（Permissive）] にします。

  クラスタ間通信を許可する前に、クラスタが互いの証明書を検証するようにする場合は、[強制（Enforce）] を選択します。

- **[システム（System）] > [クラスタリング（Clustering）] > [クラスタIPバージョン（Cluster IP version）]** をこの Expressway-C の IP アドレスのタイプと同じにします。

- **[システム（System）] > [クラスタリング（Clustering）] > [ピア1 IPアドレス（Peer 1 IP address）]** は、この Expressway の IP アドレスまたは FQDN にします。

  各ピアの FQDN は、TLS 検証を強制する場合、Expressway の証明書と一致する必要があります。

**注意** クラウドに正しく登録するために、Expressway-C に設定するホスト名は小文字のみにします。現時点で大文字はサポートされていません。

**ステップ 7** ファイアウォールに必要なポートをまだ開いていない場合は、開きます。

- Expressway-C と Cisco Webex クラウド間のトラフィックはすべて、HTTPS トラフィックまたはセキュア Web ソケットです。
- Expressway-C からのアウトバウンド トラフィックに対して TCP ポート 443 を開く必要があります。Expressway-C から要求されるクラウドドメインの詳細については、https://collaborationhelp.cisco.com/article/WBX000028782を参照してください。

**ステップ 8** 組織がインターネットのアクセスに HTTP プロキシを使用している場合は、その HTTP プロキシの詳細情報（アドレス、ポート）を取得します。Basic 認証を必要とする場合は、プロキシのユーザ名とパスワードも必要です。Expressway は、その他の方法でプロキシを認証できません。

- Ubuntu 12.04.5 で Squid 3.1.19 をテストし、確認しました。
- 認証ベースのプロキシはテストしていません。

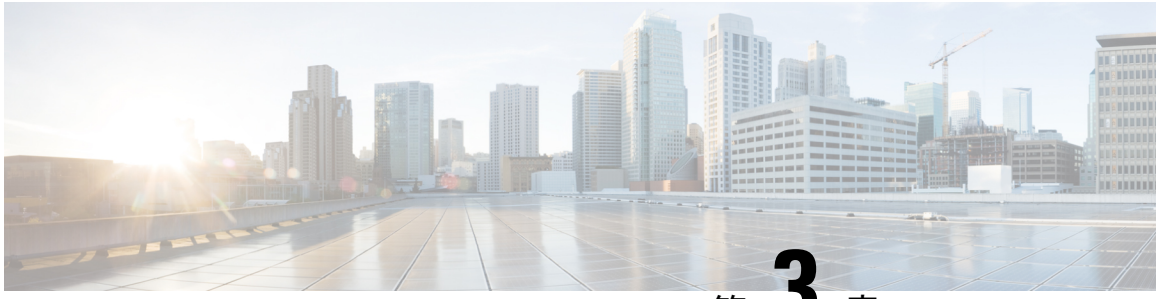
（注） 組織が TLS プロキシを使用している場合、Expressway-C は TLS プロキシを信頼する必要があります。プロキシの CA ルート証明書は、Expressway の信頼ストアにある必要があります。**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼できるCA証明書（Trusted CA certificate）]** で、証明書を追加する必要があるかどうか確認できます。

（注） コネクタホストクラスタ内のプライマリ Expressway に構成されているプロキシの詳細は、Expressway クラスタ全体で共有されます。クラスタ内のノードごとに異なるプロキシを構成することはできません。

**ステップ 9** 証明書の信頼に関する次のポイントを確認します。メインのセットアップ手順を開始する際に、セキュアな接続のタイプを選択できます。

- Cisco Webex ハイブリッド サービス には、Expressway-C と Cisco Webex 間のセキュアな接続が必要です。

  Cisco Webex にルート CA 証明書を管理させることができます。ただし、自分で管理する場合は、認証局と信頼チェーンを認識しておく必要があります。また、Expressway-C の信頼リストに変更を加える権限が付与されている必要もあります。



第 3 章

# Cisco Webex ハイブリッド メッセージ サービスの導入


- Cisco Webex クラウドへの Expressway-C コネクタホストの登録 （41 ページ）
- メッセージ コネクタ用のアプリケーション アカウントの構成 （45 ページ）
- IM およびプレゼンスサービス への接続の設定 （45 ページ）
- 起動 メッセージコネクタ （46 ページ）
- コネクタのステータスの確認 （47 ページ）
- ユーザに対する ハイブリッド メッセージ サービス の有効化 （47 ページ）
- Test ハイブリッド メッセージ サービス （48 ページ）


## Cisco Webex クラウドへの Expressway-C コネクタホストの登録

Cisco Webex ハイブリッド サービス は、Expressway-C でホストされているソフトウェアコネクタを使用して Cisco Webex を組織の環境に安全に接続します。この手順に従って、Expressway-C リソースをクラウドに登録します。

登録手順を完了すると、コネクタソフトウェアがオンプレミスの Expressway-C に自動的に導入されます。

### 始める前に

- Expressway-C がハイブリッドサービスにサポートされているバージョンで実行されていることを確認します。クラウドへの新規または既存の登録でサポートされているバージョンについては、ドキュメント「*Supported Versions of Expressway for Cisco Webex Hybrid Services Connectors*」（https://collaborationhelp.cisco.com/article/ruyceab）を参照してください。
- 他のブラウザタブで開いている、Expressway-Cインターフェイスとのすべての接続からサインアウトします。
- オンプレミス環境で発信トラフィックを代替処理している場合、最初に **[アプリケーション（Applications）] > ハイブリッド サービス > [コネクタプロキシ（Connector Proxy）]**

にプロキシサーバの詳細情報を入力してから、この手順を行う必要があります。正常に登録を行うには、こうすることが必要です。

### 手順

**ステップ 1** https://admin.webex.com の顧客ビューから **[サービス（Services）]** に移動して、次のいずれかを選択します。

- これが登録する最初のコネクタホストの場合、導入対象のハイブリッドサービスのカードで **[セットアップ（Set up）]** をクリックし、**[次へ（Next）]** をクリックします。
- 1 つ以上のコネクタホストをすでに登録している場合、導入対象のハイブリッドサービスのカードで **[すべて表示（View all）]** をクリックし、**[リソースの追加（Add Resource）]** をクリックします。

Expressway Web インターフェイスからの登録時に、Cisco Webex クラウドはすべての試行を拒否します。まず、Cisco Webex Control Hub を使用して Expressway を登録する必要があります。これは Control Hub がオンプレミスとクラウド間の信頼関係を確立して登録を完了するために、Expressway にトークンを渡す必要があるためです。

**ステップ 2** Expressway-C の登録方法を選択します。

- **新規の Expressways**：[完全修飾ドメイン名（FQDN）で新規 Expressway を登録する（Register a new Expressway with its Fully Qualified Domain Name (FQDN)）] を選択し、Expressway-C の IP アドレス、または完全修飾ドメイン名（FQDN）を入力します。Cisco Webex は該当する Expressway-C のレコードを作成して信頼を確立するので、[次へ（Next）] をクリックします。Cisco Webex Control Hub でリソースを識別するための表示名を入力することもできます。

  **注意** クラウドに正しく登録するために、Expressway-C に設定するホスト名は小文字のみにします。現時点で大文字はサポートされていません。

- **既存の Expressways**：[既存の Expressway クラスタを選択してこのサービスにリソースを追加（Select an existing Expressway cluster to add resources to this service）] を選択し、以前登録したノード、またはクラスタをドロップダウンから選択します。これは、1 つ以上のハイブリッド サービスの実行に使用できます。

**ヒント** クラスタを登録する場合は、プライマリ ピアを登録します。他のピアを登録する必要はありません。プライマリを登録すると自動的に登録されます。最初にあるノードをプライマリとしてセットアップする場合でも、その後の追加でシステムを再起動する必要はありません。

**ステップ 3** [次へ（Next）] をクリックし、新規登録の場合はリンクをクリックして Expressway-C を開きます。その後、サインインして [コネクタの管理（Connector Management）] ウィンドウをロードします。

**ステップ 4** Expressway-C 信頼リストの更新方法を決定します。

[ウェルカム（welcome）]ページのチェックボックスによって、必要なCA証明書をExpressway-C信頼リストに手動で追加するのか、それらの証明書を Cisco Webex に追加させるのかが決定されます。

次のいずれかのオプションを選択します。

- Cisco Webex によって必要な CA 証明書を Expressway-C 信頼リストに追加する場合は、このボックスをオンにします。

  登録すると、Cisco Webex クラウド証明書に署名した機関のルート証明書が自動的に Expressway-C にインストールされます。これは、Expressway-C が自動的に証明書を信頼し、セキュアな接続をセットアップできる必要があることを意味します。

  （注） または、[コネクタ管理（Connector Management）] ウィンドウを使用して、Cisco Webex クラウド CA ルート証明書を削除し、手動でルート証明書をインストールすることができます。

- Expressway-C信頼リストを手動で更新する場合は、このボックスをオフにします。手順については、Expressway-C オンラインヘルプを参照してください。

  注意 現時点で信頼リストに適切な CA 証明書がない場合は、登録すると証明書の信頼エラーが表示されます。ハイブリッドサービスの認証局 （44 ページ）を参照してください。

**ステップ 5** [登録する(Register)] をクリックします。Cisco Webex Control Hub にリダイレクトされたら、画面上のテキストを読んで、Cisco Webex が正しい Expressway-C を識別したことを確認します。

**ステップ 6** 情報を確認したら、**[許可（Allow）]** をクリックして、Expressway-C を Cisco Webex ハイブリッド サービス に登録します。

- 登録には、Expressway の設定内容および初めての登録かどうかによって最大 5 分かかる場合があります。
- Expressway-C が正常に登録されると、Expressway-C 上の Cisco Webex ハイブリッド サービス ウィンドウに、コネクタのダウンロードとインストールが表示されます。使用可能な新しいバージョンがある場合は、管理コネクタが自動的にアップグレードしてから、Expressway-C コネクタホスト用に選択された他のコネクタをインストールします。
- 各コネクタは、そのコネクタの設定と有効化に必要なインターフェイス ページをインストールします。

  このプロセスには数分かかる可能性があります。コネクタがインストールされると、Expressway-C コネクタホスト上の **[アプリケーション（Applications）] > ハイブリッド サービス** メニューに新しいメニュー項目が表示されます。

### トラブルシューティングのヒント

登録が失敗し、オンプレミス環境で発信トラフィックを代理的に処理する場合は、この手順の「はじめる前に」セクションを確認してください。登録プロセスがタイムアウトまたは失敗し

た場合（証明書エラーを修正する必要がある場合やプロキシの詳細を入力する必要がある場合など）は、Cisco Webex Control Hub で登録を再開できます。

# ハイブリッドサービスの認証局

次の表に、Cisco Webex ハイブリッド サービス を使用する場合にオンプレミスまたは既存の環境で信頼しなければならない認証局を記載します。

必要な証明書を Cisco Webex に管理させる場合は、手動で CA 証明書を Expressway-C 信頼リストに追加する必要はありません。

（注） Cisco Webex ホスト証明書の署名に使用する発行元は将来変更される可能性があります。その場合、以下の表の正確性は失われる可能性があります。CA 証明書を手動で管理している場合は、次に示すホストの現時点で有効な証明書に署名した証明書発行元の認証局の CA 証明書を追加する（および有効期限が切れていたり、失効している CA 証明書は削除する）必要があります。

| この CA が署名したクラウド ホスト | 発行元 CA | 信頼先 | 目的 |
|---|---|---|---|
| CDN | O = Baltimore、OU = CyberTrust、CN = Baltimore CyberTrust Root | Expressway-C | Expressway が信頼されたホストからコネクタをダウンロードするようにするため |
| 共通アイデンティティ サービス | O = VeriSign, Inc.、OU = Class 3 Public Primary Certification Authority | Cisco Directory Connector をホストしている Windows Server 2003 または Windows Server 2008<br>Expressway-C | Active Directory のユーザと Cisco Webex を同期し、Cisco Webex ハイブリッド サービス のユーザを認証する |
| Cisco Webex | O = The Go Daddy Group, Inc、OU = Go Daddy Class 2 Certification Authority | Expressway-C | |

### 関連トピック

Cisco Webex でサポートされている認証局

# メッセージコネクタ用のアプリケーションアカウントの構成

Cisco Unified Communications Manager IM およびプレゼンスサービス の AXL API にアクセスするための メッセージ コネクタ 用のアカウントを構成します。**メインの管理者アカウントではなく、独立した管理者アカウントを使用する必要があります。**このアカウントの詳細を覚えておいてください。後で、メッセージ コネクタ 構成に入力する必要があります。

### 手順

**ステップ 1** [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）]** に移動し、次のいずれかを選択します。

- [検索（Find）] をクリックし、Cisco Unified Communications ManagerIM およびプレゼンスサービス との通信にコネクタが使用する管理者アカウントをリストから選択します。
- **[新規追加（Add New）]** をクリックして、新しい アプリケーション ユーザ アカウントを作成します。

**ステップ 2** **標準 AXL API アクセス**ロールを割り当てたアカウントを構成します。

**ステップ 3** [保存(Save)] をクリックします。

# IM およびプレゼンスサービス への接続の設定

ハイブリッド メッセージ サービス を有効にするには、パブリッシャノードのサーバ情報を入力して、メッセージ コネクタ を IM およびプレゼンスサービス クラスタにリンクする必要があります。この手順では、IM およびプレゼンスサービス と Cisco Webex クラウド間のブリッジを作成し、コネクタを 2 つの間のブローカとして動作させます。

ハイブリッド メッセージ サービス 用に使用している各 Expressway クラスタで、プライマリノードにサインインして、次の構成を完了します。

### 始める前に

- メッセージ コネクタ用のアプリケーション アカウントの構成 （45 ページ）
- Expressway 上のコネクタは、ハイブリッド メッセージ サービスクラスタとクラウド間に耐障害性のある接続を維持します。必要なのは、パブリッシャを Expressway-C コネクタ構成に追加することだけです。クラスタ内で特定のノードがダウンした場合は、コネクタが別のサーバに移動します。

手順

ステップ 1 **[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [メッセージサービス（Message Service）] > [メッセージサービスの構成（Message Service Configuration）]** に移動します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 有効な Cisco AXL ウェブ サービスがある IM およびプレゼンスサービス パブリッシャ ノードのホスト名または IP アドレスを入力します。

コネクタは、AXL を使用して、パブリッシャにクエリを実行し、クラスタ内の他のノードを発見します。

ステップ 4 IM およびプレゼンスサービス パブリッシャ上に作成した メッセージコネクタ AXL アカウントのクレデンシャルを入力します。

（注） これは、メインの管理者アカウントである必要はありません。メッセージ コネクタ用のアカウントを明示的に作成する必要があります。

ステップ 5 （省略可）Expressway でパブリッシャノードからのサーバ証明書のチェックを省略する場合は、**[証明書の検証（Certificate validation）]** を **[無効（Disabled）]** に変更します。

証明書の検証が有効になっている場合（デフォルト）、IM およびプレゼンスサービス ノードからの tomcat 証明書は有効であり、Expressway が信頼する CA によって署名されている必要があります。自己署名証明書を使用している場合は、それを Expressway の *[*信頼できる *CA* 証明書（*Trusted CA certificate*）*]* リストにコピーします。

ステップ 6 **[追加（Add）]** をクリックして、コネクタの構成を Expressway-C に保存します。

ステップ 7 Expressway クラスタを 他の IM およびプレゼンスサービス クラスタに接続する必要がある場合は、このタスクを繰り返します。

次のタスク

起動 メッセージコネクタ （46 ページ）

# 起動 メッセージコネクタ

IM and Presence パブリッシャと AXL アカウントを設定してコネクタを構成した後、メッセージコネクタ を手動で有効にします。

手順

ステップ 1 Expressway-C から、**[アプリケーション（Applications）] > ハイブリッド サービス > [接続管理（Connector Management）]** と移動して、**[メッセージコネクタ（Message Connector）]** とクリックします。

ステップ 2 **[アクティブ(Active)]** ドロップダウン リストから **[有効(Enabled)]** を選択します。

ステップ 3 [Save] をクリックします。

コネクタが起動し、[コネクタの管理（Connector Management）] ウィンドウのステータスが [実行中（Running）] に変わります。

# コネクタのステータスの確認

ハイブリッド メッセージ サービス に対してユーザを有効にする前に、メッセージコネクタ が実行されていることを確認します。

手順

Expressway-C から、**[アプリケーション（Applications）] > ハイブリッド サービス > [メッセージサービス（Message Service）] > [メッセージサービスのステータス（Message Service Status）]** に移動します。[ステータス（Status）] の設定項目を確認します。

次のタスク

ユーザに対する ハイブリッド メッセージ サービス の有効化 （47 ページ）

# ユーザに対する ハイブリッド メッセージ サービス の有効化

ハイブリッド メッセージ サービス に対して Cisco Webex Teams ユーザを一度に 1 人つずつ有効にするには、次の手順を使用します。

一括 CSV テンプレートの使用や Cisco Directory Connector 経由の Active Directory 同期などの他の方法については、「*Ways to Add and Manage Users in Cisco Webex Control Hub*」（https://collaborationhelp.cisco.com/article/nj34yk2）を参照してください。

（注） 一括インポートまたはディレクトリ同期によってユーザをインポートする場合、送信元システムにユーザの電子メールアドレスが登録されている必要があります。Cisco Webex ユーザ ID にはユーザの電子メールアドレスをマッピングするため、ユーザが Cisco Webex Teams に使用するアドレスでなければなりません。

ユーザの電子メールアドレスが IM およびプレゼンスサービス になければ、メッセージコネクタ はそのユーザを検出できません。したがって、ハイブリッド メッセージ サービス はそのユーザに対して機能しません。

Cisco Directory Connector を使用して、選択した属性（たとえば、メール属性や userPrincipalName 属性など）を Cisco Webex UID にマッピングすることはできますが、**属性の値はユーザの電子メールアドレスであることが必須です。**

手順

**ステップ 1** https://admin.webex.com の顧客ビューから [ユーザ（Users）] に移動し、リストから特定のユーザを選択するか、検索を使用してリストを絞り込み、該当する行をクリックしてユーザの概要を表示します。

**ステップ 2** [編集（Edit）] をクリックし、少なくとも 1 つの有料サービスがユーザに割り当てられていることを [ライセンスコラボレーションサービス（Licensed Collaboration Services）] で確認します。必要な変更を加えて、[保存（Save）] をクリックします。

**ステップ 3** [コールサービス（Message Service）] をクリックし、設定を切り替えてオンにし、変更を保存します。

ユーザが Webex Teams から Cisco Jabber にメッセージを送信できるようになるまでに、最大 1 時間の遅延が発生します。

# Test ハイブリッド メッセージ サービス

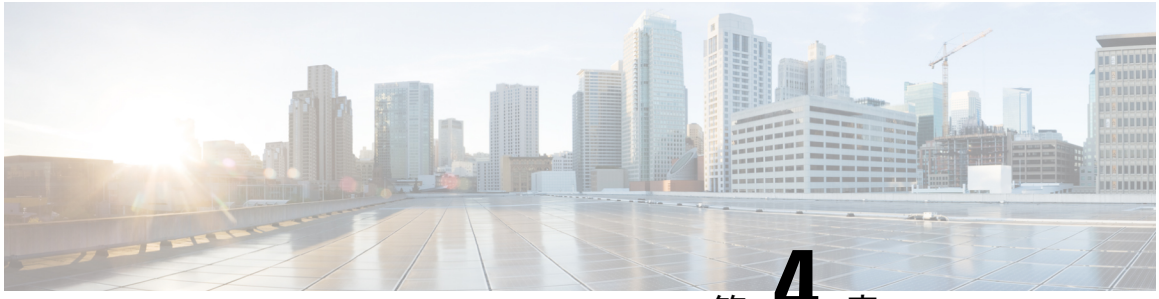
### 始める前に

ハイブリッド メッセージ サービス が有効にされている 2 人以上のユーザが必要です。ユーザのマシンに Cisco Jabber と Cisco Webex Teams がインストールされている必要があります。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | 一方のユーザが Webex Teams クライアントを開きます。 | この手順では、このユーザをユーザ A または Alice と呼びます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 2** | もう一方のユーザが Cisco Jabber クライアントを開きます。 | この手順では、このユーザをユーザ B または Bob と呼びます。 |
| **ステップ 3** | Alice の Webex Teams クライアントから Bob の Jabber クライアントにメッセージを送信します。 | |
| **ステップ 4** | メッセージが Bob の Jabber クライアントに到着して、Alice のステータスが [応答可能（Available）] として表示されることを確認します。 | |
| **ステップ 5** | Bob の Jabber クライアントから Alice の Webex Teams クライアントに応答します。 | |
| **ステップ 6** | Alice の Webex Teams クライアントに Bob が入力中であることが示されることを確認します。 | |
| **ステップ 7** | Alice の Jabber クライアントと Bob の Webex Teams クライアントでテストを繰り返します。 | |



第 4 章

# ハイブリッド メッセージ サービスの管理


- ハイブリッド メッセージ サービス Expressway 上のステータス （51 ページ）
- ハイ アベイラビリティとフェールオーバー （54 ページ）
- ユニファイド CM IM and Presence ノードへの接続の更新 （55 ページ）
- ハイブリッド メッセージ サービスのトラブルシューティング （56 ページ）


## ハイブリッドメッセージサービスExpressway上のステータス

各 Expressway コネクタホストは ハイブリッド メッセージ サービス 導入環境の一部を有効にして、その部分のステータス情報のみを表示します。特定の Expressway が問題の影響を受けている、または問題の原因となっていることが分かっている場合は、このことが役立ちます。

サービスステータスの全般的な概要を調べるには、制御ハブ で ハイブリッド メッセージ サービス 導入環境を開きます。

ステータス情報ページは、**[アプリケーション（Applications）]**>**[ハイブリッドサービス（Hybrid Services）]** > **[メッセージサービス（Message Service）]** > **[メッセージサービスのステータス（Message Service Status）]** にあります。表示される情報は、次のカテゴリに分類されます。

- への接続性 Cisco Webex
- ユーザおよびユーザ統計
- IM およびプレゼンスサービス インフラストラクチャへの接続

ステータスページとこの参照トピックは、ステータス項目がサービスに与える影響のレベルで順序付けられています。

### への接続性 Cisco Webex

このステータスが [動作中（Operational）] 以外として示されている場合、この Expressway と Cisco Webex の間に問題があります。問題は Expressway にある可能性（**[ステータス（Status）]**> **[アラーム（Alarms）]** を確認）、サービスにある可能性（status.ciscospark.com を確認）、またはこの 2 つの間のネットワークにある可能性があります（プロキシを使用している場合はプロ

キシを調べます。ファイアウォールがアウトバウンド HTTPS 接続を許可していることを確認します。また、ネットワーク診断ツールを使用してルートが存在するかどうかを確認します）。

### メッセージサービスの合計ユーザ数（Message Service User Totals）（この Expressway）

ステータスページのこの部分には、この Expressway クラスタに既知となっているユーザの合計数が示されます。この数値は、このコネクタホストクラスタ全体で共通しています。クラスタ内のすべてのノードは（パブリッシャアドレスとアカウントの詳細を入力した）ハイブリッド メッセージ サービス の構成を共有するためです。

[接続されている IM and Presence クラスタのユーザ数（Users from connected IM and Presence clusters）] には、直接接続されたインフラストラクチャからコネクタが収集するユーザの数が示されます。IM およびプレゼンスサービス これらのユーザは、この Expressway クラスタのプライマリノードで詳細を入力したパブリッシャを使用する IM and Presence クラスタを「ホーム」としています（つまり、このクラスタの「ローカル」ユーザです）。

この数値を区別する必要があるのは、コネクタがこれらのパブリッシャに対して AXL クエリを実行すると、パブリッシャが認識しているすべてのユーザの数が返されるためです。この数値には、クエリ対象のパブリッシャが認識する「クラスタ間」のユーザも含まれます。これは、ICSA（Intercluster Sync Agent）が複数の IM and Presence クラスタにわたって機能するためです。

この数値は、このコネクタホストクラスタを介してサービスを使用する可能性のある論理上の最大ユーザ数です。実際には、移行計画の一部として、それよりも少ないユーザを有効にすることになるはずです。

**[すべての IM and Presence クラスタ（ICSA）のユーザ数（Users from all IM and Presence clusters (ICSA)）]** には、コネクタ構成に追加したパブリッシャと（ICSA によって）同期されるすべての IM and Presence クラスタで認識されているユーザの数が示されます。この数値には、ローカルユーザの数（このセクションの上述の数値）が含まれます。したがって、この 2 つの数値を見ると、たとえば直接接続された IM and Presence クラスタをホームとするユーザ数が 300 で、複数の IM and Presence クラスタの間で同期されるユーザ数が 1000 の場合、1000 **のうちの** 300 がローカルユーザであると考えられます。

これらの数値間の関係を基に、メッセージサービス導入環境を検証またはトラブルシューティングすることができます。たとえば、同期されるユーザの数は 1000 のはずなのに合計がそれよりも少ない場合、Intercluster Sync Agent で問題が発生していることが考えられます。1 つのクラスタだけを使用している場合、またはすべての IM and Presence パブリッシャがこのコネクタ上に構成されている場合は、2 つの数値が同じになるはずです。両方の数値が 0 となっている場合、AXL クエリまたはメッセージコネクタの構成に問題があることを示している可能性があります。

[ハイブリッド メッセージ サービスが有効にされているユーザ数（Users Enabled for Hybrid Message Service）] には、 がこの特定の Expressway クラスタに割り当てている 対応のユーザの数が示されます。Cisco Webexハイブリッド メッセージ サービス 通常、この数値は [接続されている IM and Presence クラスタのユーザ数（Users from connected IM and Presence clusters）] よりも小さくなります。

制御ハブでユーザにメッセージサービスの利用資格を付与すると、クラウドはコネクタホストと通信して、それらのユーザについて認識しているコネクタを判別します。クラウドは判別したコネクタの間で均等になるようにユーザを割り当てます。

**[アクティブなメッセージサービスユーザ数（Active Message Service Users）]** には、現在ハイブリッド メッセージ サービス を使用している有効なユーザの数が示されます。ユーザがアクティブであるとみなされるのは、現時点までの 24 時間以内に Cisco Webex Teams を使用して Cisco Jabber に対するメッセージの読み取り/書き込みを行った場合です。この数値は、[ハイブリッド メッセージ サービスが有効にされているユーザ数（Users Enabled for Hybrid Message Service）] のパーセンテージとしても示されます。

**[24 時間以上アクティブになっていないユーザ数（Users not Active for 24 Hours or more）]** には、現在 ハイブリッド メッセージ サービス を使用していない有効なユーザの数が示されます。つまり、現時点までの 24 時間以内に Cisco Webex Teams を使用して Jabber に対するメッセージの読み取り/書き込みを行わなかったユーザの数です。コネクタはこの特性に基づき、非アクティブなユーザが保持するすべてのセッションを削除してパフォーマンスを向上させます。導入環境全体での一般的な使用状況では、（休日などで）非アクティブなユーザもある程度いると想定できますが、通常は非アクティブなユーザ数はアクティブなユーザ数より少ないはずです。この数値は、[ハイブリッドメッセージサービスが有効にされているユーザ数（Users Enabled for Hybrid Message Service）] のパーセンテージとしても示されます。

### メッセージサービスのステータス（Message Service Status）（IM and Presence ノード）

ステータスページのこのセクションでは、直接接続された IM and Presence ノードとのコネクタの関係に関する情報が提供されます。

IM and Presence パブリッシャ（構成時に入力したアドレス）ごとに、少なくとも 1 つのノード（それ自体）が検出されます。検出される可能性のあるノードは合計で最大 6 つです。

各 IM およびプレゼンスサービス クラスタの各ノードについて、次のステータス情報が表示されます。

- **[ノードバージョン（Node Version）]**は、その特定のノードから報告された IM およびプレゼンスサービス ソフトウェアバージョンです。
- **[ノードのステータス（Node Status）]** は、[動作中（Operational）] でなければなりません。[停止（Outage）] のステータスは、その IM およびプレゼンスサービス ノードまたはそのノードとの接続に問題があることを示します。
- **[証明書の検証（Certificate validation）]** は、このノードのパブリッシャに接続したときに選択した内容に応じて、オンまたはオフのいずれかになります。[オン（On）]（デフォルト）の場合、Expressway がこのノードによって提示された証明書を検証できなければ、ハイブリッド メッセージ サービス は機能しません。
- **[このノードのメッセージサービスユーザ数（Message Service Users from this Node）]** には、このコネクタに割り当てられていて、この IM およびプレゼンスサービス ノードをホームとしているハイブリッドメッセージサービス対応のユーザの数が示されます。ページの先頭近くに示される、メッセージサービスが有効にされているユーザの合計数には、このステータスページにリストされる各 IM およびプレゼンスサービス ノードが含まれています。

- **[アクティブなメッセージサービスユーザ数（Active Message Service Users）]** には、現在ハイブリッド メッセージ サービスを使用していて、この IM およびプレゼンスサービス ノードをホームとする有効なユーザの数が示されます。ページの先頭近くに示される、アクティブなメッセージサービスユーザの合計数には、このステータスページにリストされる各 IM およびプレゼンスサービス ノードが含まれています。
- **[24 時間以上アクティブになっていないユーザ数（Users not Active for 24 Hours or more）]** には、現在 ハイブリッド メッセージ サービスを使用していない、この IM およびプレゼンスサービス ノードをホームとしている有効なユーザの数が示されます。ページの先頭近くに示される、24 時間以上アクティブでないユーザの合計数には、このステータスページにリストされる各 IM およびプレゼンスサービス ノードが含まれています。

# ハイ アベイラビリティとフェールオーバー

### メッセージコネクタノードの制御された停止

メッセージコネクタをホストしている Expressway ノードでメンテナンスを開始する前に、Control Hub でノードをメンテナンスモードに切り替える必要があります。これにより、Cisco Webex によりそのノードからクラスタ内の残りのノードにユーザが移動されるので、メンテナンスを開始できます。

Cisco Webex は、Expressway 自体のメンテナンスモードを認識しません。このようにして Expressway のサービスを停止すると、Cisco Webex にはそのコネクタが制御外で停止したかのように見えます。

### プレゼンス冗長グループの高可用性設定

メッセージサービス コネクタは高可用性設定を認識します。したがって、IM and Presence ノードでの手動または自動フェールオーバーとフォールバックイベントに応答することができます。

グループのノードがメッセージサービスに参加しているときに、そのグループの高可用性設定（オンまたはオフのいずれか）を変更した場合、ノードに関連付けられている Expressway 上のコネクタを再起動する必要があります。

IM and Presence 構成について詳しくは、https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-im-presence-service/200958-IM-and-Presence-Server-High-Availability.htmlを参照してください。

### IM およびプレゼンスサービス ノードの制御された停止

IM およびプレゼンスサービス ノードのメンテナンスを開始する前に、そのノードでのセッションをプレゼンス冗長グループ内の他のノードに手動でフェールオーバーする必要があります。

プレゼンス冗長グループ内のいずれかの IM and Presence ノードに手動でフェールオーバーすると、ユーザセッションが送信元ノードからのそのノードに移行します。Expressway のメッセー

ジサービスのステータスページには、送信元ノードのステータスが [停止（Outage）] として報告されますが、ユーザはそのノードに割り当てられたままの状態で示されます。

メッセージコネクタがターゲット IM およびプレゼンスサービス ノードで新しいセッションを作成するときは、レート制限が適用されます。コネクタがユーザを他のノードに移行し始めるまでには最大 15 分かかる場合があります。その後、ターゲットノードが過負荷にならないレートで移行を進めます。たとえば、5,000 のユーザセッションがフェールオーバーする場合、制御された停止が開始されてからサービスが安定するまでには約 30 分かかることが見込まれます。

移行プロセスが完了するまで待機した後、IM およびプレゼンスサービス ノードでメンテナンスを開始できます。メンテナンスが完了したら、手動で元のノードにセッションをフォールバックできます。フォールバックの場合も、完了するまでには同様の待機時間が見込まれます。

### 制御外の停止

ハイブリッドメッセージサービスは、IM およびプレゼンスサービス ノードの予期しない障害に自動的に応答します。

制御された停止の場合と同じく、メッセージコネクタが残りの IM およびプレゼンスサービスノードで新しいセッションを作成するときに、レート制限が適用されます。コネクタがユーザを他のノードに移行し始めるまでには最大 15 分かかる場合があります。その後、ターゲットノードが過負荷にならないレートで移行を進めます。たとえば、5,000 のユーザセッションがフェールオーバーする場合、IM and Presence ノードのいずれかで予期しない障害が発生した後、サービスが安定するまでには約 30 分かかることが見込まれます。

このサービスは、他の制御外の停止に対して堅牢ではありません。こうした停止には以下が含まれますが、これらに限定されることはありません。

- Expressway の予期しない障害。
- メッセージコネクタの予期しない障害。
- ハイブリッド メッセージ サービスが依存する IM and Presence サービスの予期しない障害（XCP、AXL、プレゼンスエンジンなど）。

# ユニファイド CM IM and Presence ノードへの接続の更新

メッセージコネクタは IM and Presence パブリッシャに対する AXL コールを使用して、そのクラスタ内のノードを検出します。これは静的な設定であり、IM and Presence クラスタを変更した場合、メッセージコネクタは動的にその変更に適応しません。たとえば、ノードを追加または削除した場合です。

AXL サービスが IM and Presence ノードで実行されていないと、メッセージコネクタはそのノードを検出できません。したがって、導入環境で何らかの障害が発生した場合、メッセージコネクタが起動するまでノードが稼働状態に戻らなかったり、AXL サービスが再起動しなかったりする可能性があります。

メッセージコネクタがIM and Presenceノードの一部を検出していない場合は、メッセージコネクタを再起動して強制的に再検出させることができます。

手順

ステップ 1 メッセージコネクタ Expressway クラスタのプライマリピアにサインインし、**[アプリケーション（Applications）] > ハイブリッド サービス > [コネクタ管理（Connector Management）]** に移動します。

ステップ 2 **[メッセージコネクタ（Message Connector）]** をクリックします。

ステップ 3 **[アクティブ（Active）]** ドロップダウン リストから **[無効（Disabled）]** を選択します。

ステップ 4 [保存(Save)] をクリックします。

コネクタが停止します。

ステップ 5 **[アクティブ(Active)]**ドロップダウン リストから **[有効(Enabled)]**を選択します。

ステップ 6 [保存(Save)] をクリックします。

コネクタが起動して、ステータスが **[実行中（Running）]** に変わります。

# ハイブリッドメッセージサービスのトラブルシューティング

### Cisco Webex Status

すべてのユーザが問題の影響を受けている場合、最初に確認すべきことは ハイブリッド メッセージ サービス が動作しているかどうかです。

1. `https://status.ciscospark.com/` を参照します

   .

2. ステータスを確認するには、**[Webex ハイブリッドサービス（Webex Hybrid Services）** > **[メッセージサービス（Message Service）]** を展開します。

   ハイブリッド メッセージ サービス のステータスが [動作中（Operational）] でない場合、シスコがその修正を試みています。

### サービスのアクティベーション

`https://admin.webex.com` にサインインします。

- 組織の ハイブリッド メッセージ サービス カードはありますか。

### ユーザアクティベーション

制御ハブ で、ユーザのアクティベーションの問題がないか確認します。

1. `https://admin.webex.com` にサインインします。
2. [ユーザ（Users）] をクリックし、対象のユーザを見つけます。

   [ステータス（Status）] を基準にリストをソートできます。
3. ユーザ名(username)をクリックして、そのユーザの構成を開きます。

   **[メッセージサービス（Message Service）]** リンクがない場合は、ユーザを にオンボードする必要があります。ハイブリッド メッセージ サービス
4. **[メッセージサービス（Message Service）]** をクリックします。

   スライダはオン（右の位置）になっていなければなりません。表示されていない場合はオンにスライドして保存します。ユーザのステータスが数秒間 [保留中（Pending）] になってから [アクティブ（Active）] になります。
5. ユーザステータスが [エラー（Error）] の場合は、メッセージを確認します。また、**[履歴を表示（See history）]** をクリックして、このユーザのアクティベーションを妨げている問題に関する詳細情報を取得します。
6. アクティベーションを妨げている問題を修正してから、ユーザに戻って **[ユーザの再アクティブ化（Reactivate User）]** をクリックします。

   それでもユーザステータスが [アクティブ（Active）] にならない場合は、ケースをオープンする必要があります。

### コネクタのステータス

ハイブリッド メッセージ サービス がすべてのユーザまたはその大部分に対して機能していない場合、Expressway で メッセージコネクタ のステータスを確認する必要があります。

1. ハイブリッド メッセージ サービス 用に登録して構成したクラスタのプライマリピアにサインインします。
2. **[アプリケーション（Applications）]** > **[ハイブリッドサービス（Hybrid Services）]** > **[コネクタ管理（Connector Management）]** に移動します。
   - 管理コネクタは実行中ですか。
   - メッセージコネクタ は実行中ですか。
3. **[アプリケーション（Applications）]** > **[ハイブリッドサービス（Hybrid Services）]** > **[メッセージサービス（Message Service）]** > **[メッセージサービスのステータス（Message Service Status）]** に移動します。
4. ページで Expressway と構成済みの IM およびプレゼンスサービス ノードとの間にエラーがないかどうかを確認します。

ステータスは *[*動作中（*Operational*）*]* になっていなければなりません。ユーザがオンプレミスで割り当てられ、クラウドに登録されている必要があります。ユーザがハイブリッド メッセージ サービス を使用している場合は、ユーザの一部がアクティブなセッションを行っているはずです。

Expressway で IM およびプレゼンスサービス ノードの構成を確認します。

1. Expressway で、**[アプリケーション（Applications）] > [ハイブリッドサービス（Hybrid Services）] > [メッセージサービス（Message Service）] > [メッセージサービスの構成（Message Service Configuration）]** に移動します。
2. リストされているノードを確認します。**[アクティブ（Active）]** になっていないステータスエントリがあるかどうかを確認します。

（注） IM and Presence ノードがアップグレードされた後、Expressway で IM and Presence ノードのソフトウェアバージョンが正常に同期されていない場合に発生する既知の問題があります。メッセージコネクタではどのような目的でもバージョン情報が使用されないため、これは単なる表面的な問題です。IM and Presence バージョンを同期するには、メッセージコネクタを再起動します。この問題は、メッセージコネクタの今後のリリースで修正する予定です。

3. 該当するノードをすべて削除します。
4. 削除したノードを再作成します。必ずアドレス、ユーザ名およびパスワードを正しく入力してから、構成を保存してください。

   ステータスが改善されない場合は、おそらく IM およびプレゼンスサービス ノードに構成または接続の問題があります。

### IM およびプレゼンスサービス チェック

- 調査対象のユーザは、ハイブリッド メッセージ サービス で使用されているのと同じ IM およびプレゼンスサービス クラスタをホームとしていますか。
- メッセージ コネクタ アカウントに AXL ロールが割り当てられていますか。アカウントのユーザ名とパスワードは、メッセージ コネクタ で入力したものと同じですか。
- ユーザは、Control Hub で「重複メール ID」エラーによりエラー状態となっています。これらのユーザは、おそらく複数の IM and Presence クラスタをホームとしています。この状況は、ユーザを Active Directory から IM and Presence にインポートする方法によって発生する場合があります。ユーザが複数の IM and Presence クラスタをホームにすることはできません。IM and Presence のトラブルシュータを実行して、重複するユーザアカウントの有無を確認し、存在する場合は修正します。
- IM およびプレゼンスサービス ノードは Cisco AXL Web サービスを実行していますか。**[Cisco Unified IM and Presence サービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）]** に移動して確認します。

### ユーザごとのチェック項目

1 人または 2 人のユーザが問題の影響を受けている場合は、次の点を確認します。

- ユーザに ハイブリッド メッセージ サービス の利用資格はありますか。
- ユーザのアクティベーションが失敗したのは、これが初めてですか。Control Hub でユーザを表示し、ハイブリッドメッセージサービスを開いて **[ユーザの再アクティブ化（Reactivate User）]** をクリックします。
- IM and Presence の管理でユーザの電子メールアドレス（mailid）が設定されていますか。
- IM and Presence に設定されているユーザの電子メールアドレスは Cisco Webex Control Hub で設定されているものと一致していますか。
- ユーザの Jabber ID（JID）の後に指定した新しい Teams ユーザ名が「重複」していませんか。この状況は、Teams で JID を検索したことによって発生する場合があります。JID を検索すると、同じユーザの電子メールアドレスに基づくアカウントがすでに存在していても、Teams がその JID に基づく新しいスペースを作成する可能性があります。
- ハイブリッド ディレクトリ サービス を使用してユーザをインポートまたは同期しましたか。クラウド *UID* にマッピングした LDAP 属性にユーザの電子メールアドレスが含まれていることを確認します。

  たとえば、*UserPrincipalName* をクラウド *UID* にマッピングする場合、Active Directory では UserPrincipalName 属性にユーザの電子メールアドレスが含まれている必要があります。
- ユーザは Cisco Webex で適切な利用資格を与えられていますか。組織内の「Jabber のみ」のユーザには、Webex Teams を使用していなくても、Webex Teams で Message Free サービスを使用する資格が与えられていなければなりません。そうでないと、メッセージサービスのユーザが Teams を使用して送信したメッセージを受信できません。

  この状況が発生しないようにするには、すべてのユーザに Message Free 利用資格を割り当てることを推奨します。それには、ユーザをインポートする前に、Control Hub で自動ライセンス割り当てテンプレートを構成します。

  Control Hub 内に適切な利用資格を持っていないユーザが多数いる場合は、すべてのユーザを CSV ファイルにエクスポートして、その CSV ファイルからすべてのユーザを再インポートすることで、この状況を解決できます。この方法が有効なのは、CSV でユーザをインポートすると、自動的に Message Free 利用資格がユーザに適用されるためです。自動ライセンス割り当てテンプレートを使用していない限り、ハイブリッド ディレクトリ サービスを使用してユーザをインポートしても、この利用資格は自動的に適用されません。

  問題の影響を受けているユーザの数が少なければ、対象ユーザの利用資格が多種多様な場合は特に、手動で利用資格を適用することをお勧めします。
- メッセージサービスユーザが Jabber でメッセージを受信できませんか。メッセージサービスユーザが Teams 内でステータスを非表示にしている場合（[ステータスの表示（Show status）] 設定がオフになっている場合)、Jabber には、そのユーザのプレゼンスが [退席中（Away）] として反映されます。ただし、メッセージサービスはそのユーザに対して引き続き動作し、IM and Presence から Webex までメッセージを処理します。ユーザが Jabber だけを使用していても、メッセージの着信中に実際に Jabber クライアントを使用していな

ければ、クライアントにはメッセージが保持されないため、Jabber にメッセージが表示されないことがあります。IM and Presence でオフラインストレージを有効にすると、この問題が軽減される場合もありますが、このような問題の影響を受けているユーザは Teams で [ステータスの表示（Show status）] 設定をオンにすることをお勧めします。また、メッセージを保持する Teams を使用するという方法もあります。

### ハイブリッドサービスログ

（注） Expressway の [試験版（Experimental）] メニューはサポートされていません。また、文書化もされていません。

メッセージコネクタ がログに記録している内容を読むには、Expressway でハイブリッドサービスログを確認します。

1. /setaccess ページの URL を手動で入力します（例：`https://< IPAddressOrFQDN >/setaccess`）。
2. **[アクセス用パスワード（Access password）]** フィールドに値 `qwertsys` を入力し、**[アクセスの有効化（Enable access）]** をクリックします。

   これで、**[試験版（Experimental）]** メニューが表示されるようになります。
3. **[試験版（Experimental）]** > **[ハイブリッドサービスログ（Hybrid Services Log）]** > **[ハイブリッドサービスログ（Hybrid Services Log）]** をクリックします。
4. ログでエラー状態を調べます。

   繰り返される問題や永続的な問題が発生している場合は、ケースをオープンしてください。ログレベルを変更するか、または診断ログを取得してシスコに送信することをお勧めします（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]**）。