ゾーンとネイバー

ここでは、Expressway でゾーンとネイバーを設定する方法について説明します（**[設定（Configuration）] > [ゾーン（Zones）]**）。

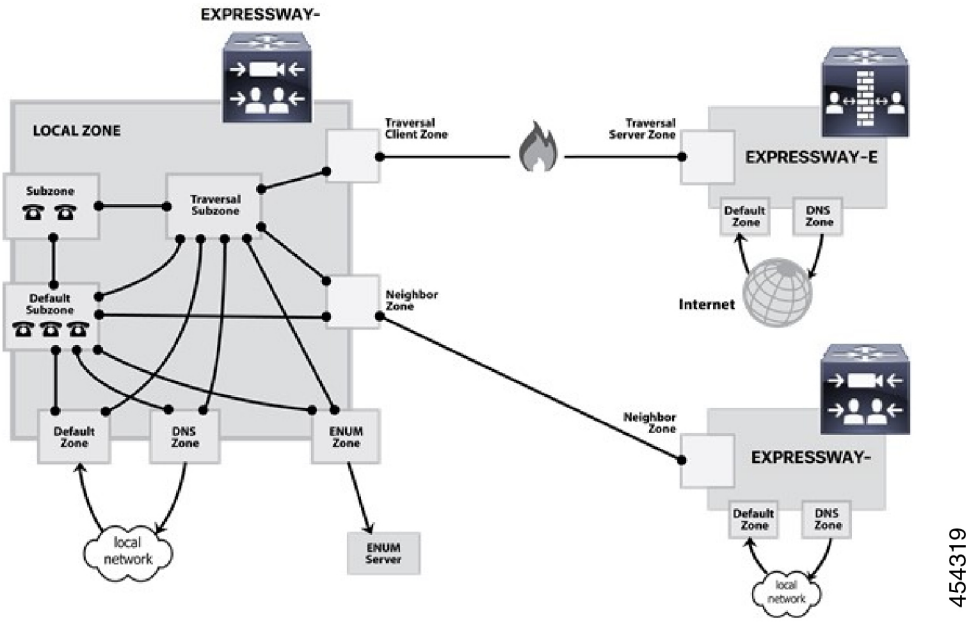
ビデオ ネットワークの基礎

このセクションでは、Expressway のビデオ通信ネットワークに関するさまざまな部分とその接続方法について概説します。

最も基本的な実装は、インターネットに接続する、1 つ以上のエンドポイントが登録された単一の Expressway です。企業の規模と複雑性に応じて、Expressway はエンドポイント ネットワーク、他の Expressway、および他のネットワーク インフラストラクチャ デバイスの一部となっており、Expressway とインターネットの間に 1 つ以上のファイアウォールがある場合があります。（そのような場合に、ネットワークの別の部分によって使用される、またはそれらの間で使用される帯域幅の量に制約を適用することができます。）

図は、Expressway の導入例に対応するさまざまなサブゾーンとゾーンを示しています。リンクによって接続されている複数のサブゾーンを設定する方法を示すために、ローカルゾーンの例として Expressway-C を使用しています。ローカル ゾーンは外部の Expressway およびインターネットと、特定のタイプのゾーンを通じて接続されています。

図 *1:* ネットワーク構成図の例



ダイヤル プランの構築

複数の Expressway の導入を開始するにあたっては、登録済みのエンドポイントについて相互に照会できるようにシステムをまとめて隣接させると便利です。開始する前に、ダイヤルプランの構築方法を検討してください。これによって、エンドポイントに割り当てるエイリアスや、Expressway を隣接させる方法が決定します。選択するソリューションは、システムの複雑性によって異なります。以降の項では、考えられるオプションのいくつかを説明します。

フラット ダイヤル プラン

最もシンプルなアプローチは、各エンドポイントに一意のエイリアスを割り当ててエンドポイントの登録を Expressway 間で分割することです。各 Expressway は、他のすべての Expressway でネイバー ゾーンとして設定されます。1 つの Expressway が、その Expressway に登録されていないエンドポイント宛のコールを受信すると、ロケーション要求を他のすべてのネイバー Expressway に送信します。

概念的にはシンプルですが、このタイプのフラット ダイヤル プランの拡張性はあまり高くありません。Expressway の追加や移動には、すべての Expressway の設定を変更する必要があり、1 回のコール試行が多数のロケーション要求を発生させる可能性があります。したがって、このオプションは、1 つまたは 2 つの Expressway とそのピアのみでの導入に最も適しています。

構造化ダイヤル プラン

構造化ダイヤルプランを使用して導入することもできます。このプランでは、登録するシステムに基づいてエンドポイントにエイリアスが割り当てられます。

E.164エイリアスを使用している場合、各Expresswayにはエリア コードが割り当てられます。Expresswaysをまとめて隣接させると、ネイバー ゾーンには対応するエリア コードで設定された検索ルールがプレフィックスとして割り当てられます（*[*エイリアス パターン マッチ（*Alias pattern match*）*]* の **[**モード（**Mode**）**]** および *[*プレフィックス（*Prefix*）*]* の **[**パターン タイプ（**Pattern type**）**]**）。そのネイバーは、そのプレフィックスで開始する番号へのコールのみを照会します。

ダイヤルプランに基づくURIでは、必要なドメイン名に一致するサフィックスを持つネイバーごとに検索ルールを設定することによって同様の動作を得ることができます。

エンドポイントをサブスクライバ番号（E.164 番号の最後の部分）のみで登録すると有効な場合があります。その場合、そのゾーンにクエリを送信する前にプレフィックスを除去するように検索ルールを設定できます。

構造化ダイヤルプランは、コールを試行するときに発行するクエリの数を最小限に抑えます。ただし、この場合も、導入環境内のすべての Expressway による完全に接続されたメッシュが必要です。階層型ダイヤル プランはこれを簡略にします。

階層型ダイヤル プラン

このタイプの構造では、1 つの Expressway をその導入環境の中央ディレクトリ Expressway として指定し、他のすべての Expressway をその中央ディレクトリ Expressway と隣接させます。

- ディレクトリ Expresswayは、近傍ゾーンとしての各 Expressway を、*[*エイリアスパターン マッチ（*Alias pattern match*）*]* の **[**モード（**Mode**）**]**と**パターン文字列**としてターゲット Expresswayのプレフィックス（構造化ダイヤルプランの場合）を持つ各ゾーンに対応する検索ルールを設定します。
- 各 Expressway には、近傍ゾーンとしてのディレクトリ Expressway が設定されています。また、*[*任意のエイリアス（*Any alias*）*]* の **[**モード（**Mode**）**]** を使用する検索ルールとディレクトリ Expressway の **[**ターゲット（**Target**）**]** を設定します。

導入環境でデバイス認証を使用していない場合は、すべての Expressway をお互いに隣接させる必要はありません。この時点で新しい Expressway を追加するには、その新しい Expressway とディレクトリ Expressway で設定を変更する必要があります。デバイス認証（下記を参照）を使用している場合は、Expressway を互いに隣接させなければならない場合があります。

この場合、ディレクトリ Expressway に障害が発生すると、通信が大幅に途絶される可能性があります。復元力を引き上げるためにクラスタリングの使用を検討してください。

階層型ダイヤル プラン（ディレクトリ Expressway）の導入とデバイス認証

階層型ダイヤルプラン内での認証ポリシーの設定方法に関する重要な情報については、「階層型ダイヤル プランと認証ポリシー」を参照してください。

ゾーンについて

ゾーンはエンドポイントの集合であり、1 つのシステムにすべて登録されているか、そうでない場合は ENUM や DNS ルックアップなどの特定の方法で見つかります。ゾーンには、次を含む多くの機能があります。

- コールをこれらのゾーンの間で使用できるかどうかに関するリンク経由での制御。
- ローカルサブゾーンと他のゾーンのエンドポイント間のコールの帯域幅の管理。
- ローカルに登録されていないエイリアスの検索。
- 認証ポリシーの設定による、そのゾーン内のエンドポイントが使用できるサービスの制御。
- そのゾーンで送受信する SIP コールのメディア暗号化ポリシーの設定と ICE メッセージング サポートの設定 機能の制御。

最大 1,000 のゾーンを設定できます。各ゾーンは、次のゾーン タイプのいずれかとして設定します。

- ネイバー ゾーンの設定：ローカル Expressway のネイバー システムへの接続
- トラバーサル クライアント ゾーンの設定：ローカル Expressway は接続されているシステムのトラバーサル クライアントであり、それら 2 つの間にはファイアウォールがあります。
- トラバーサル サーバ ゾーンの設定：ローカル Expressway は接続されているシステムのトラバーサル サーバであり、それら 2 つの間にはファイアウォールがあります。
- ENUM ゾーンの設定：ゾーンには、ENUM ルックアップで検出されたエンドポイントが含まれています。
- DNS ゾーンの設定：ゾーンには、ENUM ルックアップで検出されたエンドポイントが含まれています。
- [ユニファイドコミュニケーショントラバーサル（Unified Communications traversal）]：モバイルおよびリモートアクセスや Jabber Guest などのユニファイドコミュニケーション機能に使用するトラバーサルクライアントゾーンまたはトラバーサルサーバ ゾーン

また、Expressway には事前に設定されたデフォルト ゾーンの設定もあります。

- すべてのゾーン タイプに使用できる設定オプションについては、ゾーンの設定（デフォルト以外のゾーン）の項を参照してください。
- 検索ルールのターゲットとしてゾーンを含める方法については、検索ルールとゾーン トランスフォーメーション ルールの設定の項を参照してください。

自動的に生成されたネイバー ゾーン

Expressway は設定できない一部のネイバー ゾーンを自動的に生成します。

- システムがモバイルおよびリモート アクセス用に設定されている場合、Expressway-C は、自身と検出された各 Unified CM ノード間にネイバー ゾーンを自動的に生成します。
- Microsoft 相互運用性サービスが有効になっている場合、Expressway は「「To Microsoft destination via B2BUA」」というネイバー ゾーンを自動的に生成します。
- Unified CM 上で SIP OAuth モードが有効になっている場合、Expressway は、自身と検出された各 Unified CM ノード間に「「CEOAuth <Unified CM name>」」という名前のネイバー ゾーンを自動的に生成します。

ICE メッセージング サポートの設定

[ICE サポート（ICE support）] オプションはゾーン単位の設定であり、Expressway がそのゾーン内で SIP デバイスと送受信する ICE メッセージをサポートする方法を制御します。

この動作は、着信（入力）と発信（出力）ゾーンまたはサブゾーンの **[ICE サポート（ICE support）]** の設定によって異なります。設定の不一致（一方は *[オン（On）]*、もう一方は *[オフ（Off）]*）がある場合、Expressway はバック ツー バック ユーザ エージェント（B2BUA）を呼び出して、関連ホストと ICE ネゴシエーションを実行します。

すべてのゾーンはデフォルトで **[ICE サポート（ICE support）]** が *[オフ（Off）]* に設定されます。

B2BUA がホストと ICE ネゴシエーション を実行する際に TURN リレーの候補アドレスを提供することができます。これを行うには、TURN サーバのアドレスで設定する必要があります（**[アプリケーション（Applications）]** > **[B2BUA]** > **[B2BUA TURN サーバ（B2BUA TURN servers）]**）。

次のマトリックスで、たとえば、ゾーン A とゾーン B 間のコールを処理するときの **[ICE サポート（ICE support）]** 設定の考えられるさまざまな組み合わせでの Expressway 動作を示します。

ICE サポートの設定	**ゾーン A**	
	オフ（Off）	**オン（On）**

ゾーン B	**オフ**	標準的な Expressway のプロキシ動作。 B2BUA は通常は呼び出されません（ただし、メディア暗号化ポリシーについては下記の注を参照してください）。	B2BUA が呼び出されます。 B2BUA は、ゾーン A のホストへのメッセージ内に ICE 候補を組み込みます。
	オン	B2BUA が呼び出されます。 B2BUA は、ゾーン B のホストへのメッセージ内に ICE 候補を組み込みます。	標準的な Expressway のプロキシ動作。 B2BUA は通常は呼び出されません（ただし、メディア暗号化ポリシーについては下記の注を参照してください）。

ICE サポートと組み合わせた場合のメディア暗号化ポリシーの影響

Expressway は、メディア暗号化ポリシーの設定 （7 ページ）（自動以外の暗号化設定）を適用する必要がある場合は、B2BUA も呼び出します。次の表に、入力ゾーンと出力ゾーンの ICE サポートとメディア暗号化モードに依存する ICE ネゴシエーションの動作への影響を示します。

ICE サポート（ICE support）	**メディア暗号化モード（Media encryption mode）**	**B2BUA の呼び出し**	**ICE ネゴシエーションへの影響**
両方のゾーン = [オフ（Off）]	少なくとも 1 つのゾーンは、*[自動（Auto）]* **ではありません。**	○	B2BUA はどのホストとも ICE ネゴシエーションを実行しません。
両方のゾーン = [オン（On）]	少なくとも 1 つのゾーンは、*[自動（Auto）]* **ではありません。**	○	B2BUA は両方のホストと ICE ネゴシエーションを実行します。
両方のゾーン = [オン（On）]	両方のゾーン = [自動（Auto）]	なし	Expressway は ICE 対応のどのホストにも TURN リレーの候補アドレスを提供しません。 **（注）** 各ホストのデバイスはすでに TURN リレー候補アドレスを使用してプロビジョニングされている場合があります。

（注）

- B2BUA でルーティングされたコールは、コンポーネント タイプ *B2BUA* としてコール履歴で識別されます。
- 登録されたエンドポイントでコールを発信する場合を除き、暗号化 B2BUA を介してコールが実行される場合は、1 つの RMS コールライセンスが使用されます。
- B2BUA を介してルーティングが可能な同時発生コールは 100（大規模システムでは 500 コール）の制限があります。

メディア暗号化ポリシーの設定

メディア暗号化ポリシーの設定では、Expressway を通過する SIP コールのメディア暗号化機能を選択的に追加または削除できます。これにより、たとえば、パブリック インターネットから Expressway-E に発着信するすべてのトラフィックを暗号化し、プライベート ネットワーク内では暗号化を解除するようにシステムを設定できます。

- ポリシーはゾーン/サブゾーン単位で設定され、そのゾーン/サブゾーンのコールの発着信のレッグにのみ適用されます。
- 暗号化は、他のレッグが H.323 の場合でも、コールの SIP レッグに適用されます。

メディア暗号化ポリシーは、各ゾーンとサブゾーンの**[メディア暗号化モード（Media encryption mode）]**設定を通じて設定されます。ただし、結果のコールの暗号化ステータスもターゲット システム（エンドポイントや別の Expressway など）の暗号化ポリシーの設定によって異なります。

暗号化モードのオプションは次のとおりです。

- *[*強制暗号化（*Force encrypted*）*]*：ゾーン/サブゾーンで送受信するすべてのメディアが暗号化されます。暗号化を使用しないようにターゲット システム/エンドポイントを設定している場合は、コールは破棄されます。
- *[*強制暗号化解除（*Force unencrypted*）*]*：すべてのメディアの暗号化が解除されます。暗号化を使用するようにターゲットシステム/エンドポイントが設定されている場合は、コールが破棄される可能性があります。*[*ベストエフォート（*Best effort*）*]* を使用するように設定されている場合は、コールは暗号化されていないメディアにフォールバックします。
- *Best Effort*：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。
- *[*自動（*Auto*）*]*：特定のメディア暗号化ポリシーが Expressway によって適用されることはありません。メディア暗号化は、ターゲット システム/エンドポイントの要求にのみ依存します。これはデフォルト動作で、この機能が導入される前の Expressway の動作と同等です。

暗号化ポリシー（[自動（Auto）]以外の暗号化の設定）は、Expressway でホストされるバックツーバック ユーザ エージェント（B2BUA）を通じてルーティングされたコールに適用されます。

（注） メディア暗号化を使用するためにシステムを設定する際は、次のことを覚えておいてください。

- 暗号化モードが *[強制暗号化（Force encrypted）]* または *[強制暗号化解除（Force unencrypted）]* のゾーンは、SIP 専用ゾーンとして設定する必要があります（そのゾーンでは H.323 を無効にする必要があります）。
- 暗号化モードを *[強制暗号化（Force encrypted）]* または *[ベスト エフォート（Best effort）]* にする必要がある場合は、TLS 転送を有効にする必要があります。
- B2BUA を通じてルーティングしたコール コンポーネントは、コンポーネント タイプが B2BUA であるため、コール履歴の詳細情報で特定できます。
- B2BUA がメディアを利用する必要がある場合、各コールはトラバーサルコールとして分類され、したがって、両方のエンドポイントがシスコのインフラストラクチャに登録されている場合を除き、Rich Media Session（RMS）ライセンスが使用されます。
- Expressway ごとに同時発生ビデオコールは 100（大規模システムでは 500 ビデオコール）という制限があり、これにはメディア暗号化ポリシーを適用できます。
- B2BUA は、ICE メッセージング サポートの設定が有効になっている場合でも呼び出せます。

メディア暗号化用の B2BUA の設定

暗号化（および ICE サポート）に使用する B2BUA は、Microsoft 相互運用性に使用する B2BUA とは異なるインスタンスです。Microsoft 相互運用性サービス B2BUA は手動で設定して有効にする必要がありますが、暗号化に使用する B2BUA は暗号化ポリシーが適用されている場合は常に自動で有効になります。

ローカル ゾーンとサブゾーンについて

Expressway に登録されているすべてのデバイスの集合は、その**ローカル ゾーン**を構成します。

ローカル ゾーンは**サブゾーン**に分割されます。これには、自動的に作成された**デフォルトのサブゾーン**と、最大 1,000 個の手動設定が可能なサブゾーンが含まれます。

エンドポイントを Expressway に登録すると、そのエンドポイントはサブゾーンのメンバーシップ ルールに基づいて適切なサブゾーンに割り当てられます。これらのルールは各サブゾーンの IP アドレスまたはエイリアスのパターンマッチの範囲を指定します。エンドポイントの IP アドレスまたはエイリアスがメンバーシップ ルールのいずれにも一致しない場合は、デフォルト サブゾーンに割り当てられます。

ローカル ゾーンはネットワーク トポロジとは関係ない場合があり、複数のネットワーク セグメントを構成することがあります。また、Expressway には 2 つの特殊なタイプのサブゾーンがあります。

- トラバーサル サブゾーン。これは常に存在します。
- クラスタ ゾーン。これは常に存在しますが、Expressway がクラスタの一部の場合にのみ使用されます。

帯域幅管理

ローカル ゾーンのサブゾーンは帯域幅の管理に使用します。サブゾーンを設定した後に、帯域幅制限を次のコールに適用できます。

- サブゾーン内の 2 つのエンドポイント間の個々のコール。
- サブゾーン内のエンドポイントとそのサブゾーン外の別のエンドポイント間の個々のコール。
- サブゾーン内のエンドポイントで送受信するコールの総数。

サブゾーンの作成および設定方法、およびデフォルト サブゾーンとトラバーサル サブゾーンなどのサブゾーンに帯域幅制限を適用する方法の詳細については、帯域幅制御の項を参照してください。

登録、認証、およびメディア暗号化のポリシー

帯域幅管理の他に、Expressway の登録、認証、およびメディア暗号化のポリシーを制御するためにもサブゾーンを使用します。

これらの設定方法の詳細については、サブゾーンの設定を参照してください。

ローカル ゾーンの検索

Expressway の機能の 1 つは、ローカルに登録したエンドポイントまたは外部ゾーンから受信したコールを適切な宛先にルーティングすることです。コールは宛先エンドポイントのアドレスまたはエイリアスに基づいてルーティングされます。

Expressway はローカル ゾーンと設定された外部ゾーンの宛先のエンドポイントを検索します。検索するアドレスやエイリアスに基づいて、これらのゾーンを検索する順序にプライオリティを設定したり、各ゾーンに送信された検索要求をフィルタリングしたりできます。これにより、ローカル ゾーンや外部ゾーンに送信する検索要求の潜在的な数を削減し、検索プロセスの速度を速めることができます。

ローカル ゾーンの検索ルールの設定方法の詳細については、「検索ルールとゾーン トランスフォーメーション ルールの設定」の項を参照してください。

デフォルト ゾーンの設定

デフォルト ゾーンは、登録されていないか、または認識されておらず、ローカル ゾーンまたは既存の設定済みのゾーンのいずれかに属しているエンドポイントまたはその他のデバイスからの着信コールを表します。

Expressway には、デフォルト ゾーンおよびデフォルト ゾーンとトラバーサル サブゾーン間のデフォルト リンクが事前に設定されています。デフォルト ゾーンは削除できません。

デフォルト ゾーンの設定

デフォルト ゾーンを設定することによって、認識されていないシステムやエンドポイントからのコールを Expressway がどのように処理するかを制御できます。**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** に移動し、**[デフォルト ゾーン（DefaultZone）]** をクリックします。設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
認証ポリシー（Authentication policy）	**[認証ポリシー（Authentication policy）]** の設定で、Expressway がデフォルト ゾーンへの着信メッセージにどのように対処するかを制御します。	詳細については、「認証ポリシー」を参照してください。
メディア暗号化モード（Media encryption mode）	**[メディア暗号化モード（Media encryption mode）]** の設定では、デフォルト ゾーンを通過する SIP コール用のメディア暗号化機能を設定します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。

フィールド	説明	使用方法のヒント
デフォルト ゾーンで相互 TLS を有効にする（Enable Mutual TLS on Default Zone）	*[*オン（*On*）*]* で、MTLS（Mutual Transport Layer Security）がデフォルト ゾーンを通じた着信接続に適用されます。 *[*オフ（*Off*）*]* は、MTLS が TLS ポートへの接続に適用されていないことを意味します。専用 MTLS ポートへの接続がある場合、そのポートが **[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]** で有効にされていれば、MTLS は依然として適用されます。 デフォルト：[オフ（Off）]	この設定は、デフォルト ゾーンへの他の接続（H.323、SIP UDP、または SIP TCP）に影響しません。 （注） B2BUA はクライアント証明書の検査を実行できません。MTLS が TLS ポート 5061 で設定されているときに B2BUA を実行すると、コールは失敗します。TLS と MTLS をさまざまなポートで有効にすることを推奨します（**[プロトコル（Protocols）] > [SIP]** のページを使用）。 MTLS にポート 5061 を使用する必要がある場合、B2BUA の実行を避ける必要があります。そのためには、コール パスのすべてのゾーンで **[メディア暗号化モード（Media encryption mode）]** を *[*自動（*Auto*）*]* に切り替えます。

アクセスと帯域幅を管理するためのリンクとパイプの使用

認識されていないシステムやエンドポイントからのコールも、デフォルト ゾーンに関連付けられた「リンク」と「パイプ」を設定することで管理できます。たとえば、既定のリンクを削除して、認識されていないエンドポイントから着信コールが発信されないようにしたり、既定のリンクにパイプを適用したりすることで、認識されないエンドポイントからの着信コールに消費される帯域幅を制御できます。

デフォルト ゾーンのアクセス ルールの設定

デフォルト ゾーンのアクセス ルールを作成し（**[設定（Configuration）]> >[ゾーン（Zones）]> [デフォルト ゾーンのアクセス ルール（Default Zone access rules）]**）、デフォルト ゾーンを介して SIP TLS から Expressway への接続を許可する外部システムを制御します。

ルールごとに、パターンを指定し、外部システムから受信した証明書の CN（および SAN）と照合して比較します。次に、照合する証明書を提供するシステムへのアクセスを許可するか拒否するかを選択します。最大 10,000 のルールを設定できます。

表 *1:* デフォルトのゾーンアクセスルールパラメータ

フィールド	説明	使用方法のヒント
名前（Name）	ルールに割り当てられる名前。	
Description	ルールの任意の自由形式の説明	
優先度（Priority）	証明書名が複数のルールに一致する場合に適応するルールの順序を決定します。最も高いプライオリティ（1、2、3 の順）を持つルールが最初に適用されます。同じプライオリティの複数のルールが設定順序に適用されます。	
パターン タイプ（Pattern type）	**[パターン文字列（Pattern string）]** と証明書内に含まれる [サブジェクト共通名（Subject Common Name）] または [サブジェクト代替名（Subject Alternative Names）] を一致させる方法。 *[完全一致（Exact）]*：文字列全体が名前と 1 文字も違うことなく完全に一致する必要があります。 *[プレフィックス（Prefix）]*：文字列が名前の先頭に表示される必要があります。 *[サフィックス（Suffix）]*：文字列が名前の末尾に表示される必要があります。 *[正規表現（Regex）]*：文字列を正規表現として処理します。	パターンが特定の名前に一致するかどうかは、[パターンの確認（Check pattern）] ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [パターンの確認（Check pattern）]**）を使用してテストできます。
パターン文字列（Pattern string）	名前を比較するパターン。	
アクション（Action）	証明書がこのアクセス ルールに一致する場合に実行するアクション。 *[許可（Allow）]*：外部システムがデフォルト ゾーンを介して接続することを許可します。 *[拒否（Deny）]*：外部システムから受信した接続要求を拒否します。	

フィールド	説明	使用方法のヒント
状態（State）	ルールが有効になっているかどうかを示します。	この設定を使用して設定変更をテストしたり、特定のルールを一時的に無効にします。ルール リストには無効にしたルールが表示されますが、無視されます。

ゾーンの設定（デフォルト以外のゾーン）

[ゾーン（Zones）]ページ（**[設定（Configuration）]>[ゾーン（Zones）]>[ゾーン（Zones）]**）には、Expressway で設定したすべてのゾーンのリストが表示されます。このページで、ゾーンの作成、編集、および削除を行えます。リスト内のゾーンで、コールの数、使用される帯域幅、プロキシ経由の登録の数、プロトコルのステータス、検索ルールのステータスに関する情報が表示されます。

H.323 または SIP ステータス オプションは次のとおりです。

- *[オフ（Off）]*：ゾーンまたはシステムのどちらかでプロトコルが無効になっています。
- *[アクティブ（Active）]*：そのゾーンに対してプロトコルが有効になっており、1 つ以上の接続がアクティブになっています。複数の接続を設定し、それらの接続の一部が失敗した場合は、アクティブな接続数が表示されます。
- *[オン（On）]*：そのゾーンに対してプロトコルが有効になっていることを示します（アクティブな接続がないゾーン タイプ（たとえば、DNS ゾーンや ENUM ゾーンなど）の場合）。
- *[失敗（Failed）]*：そのゾーンに対してプロトコルが有効になっていますが、接続に失敗しました。
- *[チェック中（Checking）]*：そのゾーンに対してプロトコルが有効になっており、現在、システムが接続を確立しようとしています。

ローカル Expressway にゾーンを設定して、別のシステム（別の Expressway やゲートキーパーなど）と隣接させる、ファイアウォールを越えてトラバーサル サーバまたはトラバーサル クライアントへの接続を作成する、あるいは ENUM または DNS ルックアップを使用してエンドポイントを検出します。使用できるゾーン タイプは次のとおりです。

- ネイバー ゾーンの設定：ローカル Expressway をネイバーシステムに接続します。
- トラバーサル クライアント ゾーンの設定：ローカル Expressway をトラバーサルサーバに接続します。
- トラバーサル サーバ ゾーンの設定：ローカル Expressway-E をトラバーサルクライアントに接続します。

- ENUM ゾーンの設定：ローカル Expressway を介して ENUM ダイヤリングを有効にします。
- DNS ゾーンの設定：ローカル Expressway を有効にし、DNS ルックアップを使用してエンドポイントやその他のシステムを見つけます。
- [ユニファイドコミュニケーショントラバーサル（Unified Communications traversal）]：モバイルおよびリモートアクセスや Jabber Guest などのユニファイドコミュニケーション機能に使用するトラバーサルクライアントゾーンまたはトラバーサルサーバゾーン
- Webex ゾーンの設定: Cisco Collaboration Cloud で使用するための具体的に設定されている DNS ゾーンを有効にします。

ゾーン タイプは接続の特性を示し、使用できる設定オプションを決定します。トラバーサル サーバ ゾーン、トラバーサルクライアント、およびネイバーゾーンの場合、これは、IP アドレスやポートなど、ネイバーシステムに関する提供情報を示します。ゾーンとゾーンタイプの詳細については、ゾーンについてを参照してください。

また、Expresswayには事前に設定されたデフォルト ゾーンの設定もあります。デフォルト ゾーンは、登録されていないか、または認識されておらず、ローカル ゾーンまたは既存の設定済みのゾーンのいずれかに属しているエンドポイントまたはその他のデバイスからの着信コールを表します。

Expressway とネイバー システム間の接続は、同じ SIP トランスポート タイプを使用するように設定する必要があります。つまり、どちらも TLS を使用するように設定するか、どちらも TCP を使用するように設定する必要があります。トランスポート タイプの不一致による接続の失敗はイベント ログに記録されます。

ゾーンを作成した後は、通常、1 つ以上のゾーンポリシー検索ルールにターゲットを作成します（[設定（Configuration）]**[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]**）。これを行わないと、検索要求がそのゾーンに送信されません。

ネイバー ゾーンの設定

ネイバー ゾーンは別のシステム（VCS や Expressway など）に登録されたエンドポイントの集合であるか、SIP デバイス（Cisco Unified Communications Manager など）です。別のシステムまたはSIPデバイスはネイバーと呼ばれます。ネイバーは固有のエンタープライズネットワークの一部か別のネットワークの一部、あるいは、スタンドアロン システムである場合があります。

別のシステムとのネイバー関係は、ローカル Expressway にネイバー ゾーンとしてその別のシステムを追加することによって構築します。ネイバーゾーンでは次の操作を行うことができます。

- ネイバーに対するエンドポイントのクエリ
- 送信前の要求に対するトランスフォーメーションの適用
- ローカル Expressway とネイバー ゾーン間のコールに使用する帯域幅の制御

（注）

- ネイバー ゾーン関係の定義は一方向です。Expressway にシステムをネイバーとして追加しても、Expressway は自動的にそのシステムのネイバーにはなりません。
- 設定されたネイバーからのインバウンドコールはそのネイバーからの着信として識別されます。
- クラスタ ピアとして設定されたシステム（以前は代替と呼ばれていました）は相互にネイバーとして設定しないでください。

次の表に、ネイバー ゾーンの設定可能なオプションを記載します。

表 *2:* ネイバーゾーンの設定

フィールド	説明	使用方法のヒント
[設定（Configuration）] セクション：		
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[ネイバー（Neighbor）] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2つの値のうちの小さいほうが使用されます。
[H.323] セクション：		
モード（Mode）	ネイバー システムでH.323 コールを送受信するかどうかを決定します。	

フィールド	説明	使用方法のヒント
[ポート（Port）]	ローカル Expressway から発信された H.323 検索に使用するネイバー システムのポート。	これは、ネイバー システムでその H.323 UDP ポートで設定されたものと同じポート番号である必要があります。 ネイバーがゲートキーパーとして動作している Expressway の場合は、**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]** のページで設定されている **[登録 UDP ポート（Registration UDP port）]** の値と一致する必要があります。
SIP セクション：		
モード（Mode）	ネイバー システムで送受信する SIP コールを許可するかどうかを決定します。	
[ポート（Port）]	ローカル Expressway から発信された発信 SIP メッセージに使用するネイバー システムのポート。	これは、その SIP TCP、SIP TLS、または SIP UDP のリスニング ポート（使用する SIP **トランスポート** モードに依存）としてネイバー システムで設定されているものと同じポート番号である必要があります。
トランスポート（Transport）	ネイバー システムで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは、[TLS] です。	
TLS 検証モード（TLS verify mode）	TLS を使用して通信するときにネイバー システムに対して X.509 証明書チェックを Expressway が実行するかどうかを制御します。	ネイバー システムが別の Expressway である場合、両方のシステムが互いの証明書を確認できます（相互認証と呼ばれます）。詳細については、ネイバー システムの TLS 証明書の確認を参照してください。

フィールド	説明	使用方法のヒント
プロキシ経由の登録の許可（Accept proxied registrations）	このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。	この設定は、Expressway がレジストラとして機能するドメイン宛の登録要求にのみ適用されます。他のドメイン宛の要求の場合は、**[SIP 登録プロキシ モード（SIP registration proxy mode）]** の設定が適用されます。詳細については、登録要求のプロキシ経由での送信を参照してください。
メディア暗号化モード（Media encryption mode）	このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。
ICE パススルー サポート（ICE Passthrough support）	このゾーン内で Expressway が ICE パススルーをサポートする方法を制御します。	ICE パススルー サポートは ICE サポートよりも優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。 ICE パススルーの設定の詳細と必要なバージョンについては、Expressway 設定ガイドのページに用意されている『*Mobile and Remote Access Through Cisco Expressway guide*』を参照してください。

フィールド	説明	使用方法のヒント
マルチストリーム モード（Multistream mode）	Expressway B2BUA が発呼側間でマルチストリーム コールをネゴシエートすることを許可するかどうかを制御します。 *[オン（On）]*：Expressway は、発呼側がこのゾーンを通じてマルチストリームコールをネゴシエートし、セットアップすることを許可します。 *[オフ（Off）]*：Expressway はこのゾーンを通じてマルチストリーム ネゴシエーションを拒否します。発呼側は標準コールのネゴシエーションをフォールバックする必要があります。	この切り替えは、コールが B2BUA を通過しない場合はコールに影響しません。 発呼側双方にマルチストリーム機能がない場合、相互に正しく応答することが予測されるため、デフォルトは *[オン（On）]* になっています。ただし、発呼側間のマルチストリームの設定に問題がある場合、マルチストリーム モードを無効にして、発呼側が標準コールをネゴシエートできるかどうか確認することができます。 TelePresence Server の場合、標準コールは、TelePresence Server が、複数のストリームをエンドポイントに送信して独自の方法で処理する代わりに、複数の参加者から 1 つの「会議ストリーム」を構成してエンドポイントに送信することを意味します。
プリロードされた SIP ルートのサポート（Preloaded SIP routes support）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、有効にする必要があります。

フィールド	説明	使用方法のヒント
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新要求の送受信に SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション：		
認証ポリシー（Authentication policy）	Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。	H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。詳細 については、「認証ポリシー」を参照してください。
SIP 認証信頼モード（SIP authentication trust mode）	このゾーンからの認証された SIP メッセージ（P-Asserted-Identity ヘッダーを含んでいるもの）はこれ以上のチャレンジをせずに処理されるかどうかを制御します。	詳細については、「SIP 認証の信頼」を参照してください。
[ロケーション（Location）] セクション：		

フィールド	説明	使用方法のヒント
次の方法でピアを検索する（Look up peers by）	ピアをアドレスで検索するか、またはサービス（SRV）レコード ルックアップで検索するかを指定します。 • アドレス（デフォルト）を使用すると、最大6つのピアを追加できます。[保存（Save）] をクリックすると、Expresswayがアドレスの検索を行います。 • サービス レコードは、サービス ドメインに入るためのフィールドを生成します。[保存（Save）] をクリックすると、Expresswayは、入力されたドメインとそのゾーンで有効になっているプロトコルとトランスポートに基づいて、その DNS サーバにサービス レコードの照会を行います。 次にゾーン ページにアクセスすると、ピア アドレスが表示されているステータスが報告されます。プロトコル（SIP、SIPS、H323）、ピアが到達可能かどうか、およびピア アドレスの後にポートが表示されます。	**SRV レコード ルックアップに関する注記**： 有効なサービス ルックアップは次の 4 つです。 • _sip._udp.example.com. SIP over UDP（これは Expressway とそのゾーンではデフォルトで無効になっています） • _sip._tcp.example.com. SIP over TCP • _sips._tcp.example.com. SIP over TLS（セキュア SIP） • _h323._udp.example.com. H.323 over UDP（他のトランスポートはH.323 ではサポートされていません） SRV レコード ルックアップが設定されている所定のネイバー ゾーンでは、Expressway が登録できるピアの最大数はデフォルトで 15 に制限されます。 DNS サーバでルックアップを使用する場合は、ゾーンはゾーン ポートではなく、SRV レコードで指定されたポート経由で通信することに注意してください。ファイアウォールで、DNS 指定のポートを開いたままの状態にする必要があります。

フィールド	説明	使用方法のヒント
ピア 1 ～ ピア 2 アドレス（Peer 1 to Peer 6 address）	ネイバー システムの IP アドレスまたは FQDN。 次の場合に追加ピアのアドレスを入力します。 • ネイバーが Expressway クラスタ。この場合は、クラスタ内のすべてのピアを指定する必要があります。 • ネイバーの復元力がある Expressway 以外のシステム。この場合は、そのシステム内の復元力のあるすべての要素のアドレスを入力する必要があります。	Expressway クラスタへのコールは、そのネイバー クラスタ内でリソース使用率が最も低いピアにルーティングされます。詳細については、「Expressway クラスター間の隣接」を参照してください。 Expressway 以外のシステムに接続する場合、リソース使用率の情報が使用できないときは Expressway はラウンドロビン選択プロセスを使用して通信するピアを決定します。
[詳細]セクション：		
ゾーン プロファイル（Zone profile）	ゾーンの詳細な設定方法を決定します。 *[デフォルト（Default）]*：工場出荷時のデフォルト プロファイルを使用します。 *[カスタム（Custom）]*：各設定を個別に行うことができます。 または、事前設定されたプロファイルのいずれかを選択して、そのタイプのシステムへの接続に必要な適切な設定を自動的に使用します。オプションは次のとおりです。 • *Default* • *Custom* • *Cisco Unified Communications Manager（8.6 以前）* • *Cisco Unified Communications Manager（8.6.1 または 8.6.2）* • *Cisco Unified Communications Manager（9.x 以降）* • *Nortel Communication Server 1000* • インフラストラクチャ デバイス（通常は MCU などの非ゲートキーパー デバイスに使用）	詳細設定について詳しくは、ゾーンの設定：詳細設定を参照してください。 シスコのカスタマー サポートのアドバイスがあった場合に個別の詳細設定を行うには、カスタム プロファイルのみを使用してください。 *Cisco Unified Communications Manager* のプロファイルについて詳しくは、『Cisco Unified Communications Manager with Expressway Deployment Guide』を参照してください。

トラバーサル クライアント ゾーンの設定

ファイアウォールを通過するには、トラバーサル サーバ（通常は Expressway-E）を使用して Expressway を接続する必要があります。この場合、ローカル Expressway がトラバーサル クライアントとなるため、ローカル Expressway にトラバーサル クライアント ゾーンを作成してトラバーサル サーバとの接続を確立します。次に、トラバーサル サーバの対応するゾーンの詳細を使用してクライアント ゾーンを設定します（トラバーサル サーバも Expressway クライアント ゾーンの詳細情報を使用して設定する必要があります）。

トラバーサル サーバと隣接させた後は、次のことが可能になります。

- トラバーサル サーバとしてネイバーを使用する
- トラバーサル サーバに対してエンドポイントをクエリする
- トラバーサル サーバに送信する前にクエリへトランスフォーメーションを適用する
- ローカル Expressway とトラバーサル サーバ間のコールに使用する帯域幅を制御する

（注） NTP サーバは、トラバーサルゾーンで動作するように設定する必要があります。

詳細情報

ファイアウォールを通過するためにトラバーサルクライアントゾーンとトラバーサルサーバゾーンが連携する仕組みについて詳しくは、「ファイアウォールトラバーサルについて」を参照してください。

トラバーサル クライアント ゾーンの設定

次の表に、トラバーサル クライアント ゾーンの設計可能なオプションを記載します。

表 *3*: トラバーサル クライアント ゾーンの設定

フィールド	説明	使用方法のヒント
[設定（Configuration）] セクション：		
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[トラバーサル クライアント（Traversal client）] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。

フィールド	説明	使用方法のヒント
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2つの値のうちの小さいほうが使用されます。
[接続クレデンシャル（Connection credentials）] セクション		
[ユーザ名(Username)] と **[パスワード(Password)]**	トラバーサル クライアントは常に認証クレデンシャルを提供することによってトラバーサル サーバで認証される必要があります。各トラバーサル クライアント ゾーンは、トラバーサル サーバで認証を受けるために使用する**ユーザ名**と**パスワード**を指定する必要があります。	1 つ以上のサービス プロバイダに接続するために、それぞれ異なるクレデンシャルを使用して複数のトラバーサル クライアントを指定できます。
[H.323] セクション：		
モード（Mode）	トラバーサル サーバで H.323 コールを送受信するかどうかを決定します。	
[Protocol]	トラバーサルサーバへのコールに 2 つのファイアウォールトラバーサルプロトコル（*Assent* または *H.460.18*）のどちらを使用するかを指定します。	詳細については、「ファイアウォール トラバーサル用ポートの設定」を参照してください。
[ポート（Port）]	ローカル Expressway で送受信する H.323 コールに使用するトラバーサル サーバのポート。	H.323 を介してファイアウォール トラバーサルを動作するようにするには、トラバーサル サーバに、同じポート番号を使用してこの Expressway を表すために設定したトラバーサル サーバ ゾーンが必要です。
SIP セクション：		
モード（Mode）	トラバーサル サーバで SIP コールの送受信を許可するかどうかを決定します。	

フィールド	説明	使用方法のヒント
[ポート（Port）]	Expressway で送受信する SIP コールに使用するトラバーサル サーバのポート。 着信 SIP コールに使用するリスニング ポートとは異なっている必要があります。	SIP を介してファイアウォール トラバーサルを動作するようにするには、トラバーサル サーバに、同じトランスポート タイプとポート番号を使用してこの Expressway を表すために設定したトラバーサル サーバ ゾーンが必要です。
トランスポート（Transport）	トラバーサル サーバで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは、[TLS] です。	
TLS 検証モード（TLS verify mode）	TLS を使用して通信するときのこの Expressway とトラバーサル サーバ間での X.509 証明書チェックと相互認証を制御します。	詳細については、ネイバー システムの TLS 証明書の確認を参照してください。
プロキシ経由の登録の許可（Accept proxied registrations）	このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。	この設定は、Expressway がレジストラとして機能するドメイン宛の登録要求にのみ適用されます。他のドメイン宛の要求の場合は、**[SIP 登録プロキシ モード（SIP registration proxy mode）]** の設定が適用されます。詳細については、登録要求のプロキシ経由での送信を参照してください。
メディア暗号化モード（Media encryption mode）	このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。

フィールド	説明	使用方法のヒント
ICE パススルー サポート（ICE Passthrough support）	このゾーン内で Expressway が ICE パススルーをサポートする方法を制御します。	ICE パススルー サポートは ICE サポートよりも優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。 ICE パススルーの設定の詳細と必要なバージョンについては、Expressway 設定ガイドのページ に用意されている『*Mobile and Remote Access Through Cisco Expressway guide*』を参照してください。
マルチストリーム モード（Multistream mode）	Expressway B2BUA が発呼側間でマルチストリーム コールをネゴシエートすることを許可するかどうかを制御します。 *[オン（On）]*：Expressway は、発呼側がこのゾーンを通じてマルチストリームコールをネゴシエートし、セットアップすることを許可します。 *[オフ（Off）]*：Expressway はこのゾーンを通じてマルチストリームネゴシエーションを拒否します。発呼側は標準コールのネゴシエーションをフォールバックする必要があります。	この切り替えは、コールが B2BUA を通過しない場合はコールに影響しません。 発呼側双方にマルチストリーム機能がない場合、相互に正しく応答することが予測されるため、デフォルトは*[オン（On）]* になっています。ただし、発呼側間のマルチストリームの設定に問題がある場合、マルチストリーム モードを無効にして、発呼側が標準コールをネゴシエートできるかどうか確認することができます。 TelePresence Server の場合、標準コールは、TelePresence Server が、複数のストリームをエンドポイントに送信して独自の方法で処理する代わりに、複数の参加者から 1 つの「会議ストリーム」を構成してエンドポイントに送信することを意味します。
SIP Poison モード（SIP poison mode）	このゾーンを介して見つかったシステムに送信される SIP 要求が、この Expressway が再度受信したときには拒否されるように「「ポイズニング」」されるかどうかを決定します。	

フィールド	説明	使用方法のヒント
プリロードされた SIP ルートのサポート（**Preloaded SIP routes support**）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
SIP パラメータの保持（SIP parameter preservation）	Expressway の B2BUA がこのゾーンを介してルーティングされた SIP 要求内のパラメータを保持するか、書き直すかを決定します。	*[オン（On）]*は、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを保持します。 *[オフ（Off）]*は、必要に応じて、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを B2BUA が書き直すことを許可します。 デフォルト：[オフ（Off）]
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、有効にする必要があります。
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新要求の送受信に SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション：		

フィールド	説明	使用方法のヒント
認証ポリシー（Authentication policy）	Expresswayがこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。	詳細については、「認証ポリシー」を参照してください。
[クライアントの設定（Client settings）] セクション：		
再試行間隔（Retry Interval）	トラバーサル サーバへの接続の確立に失敗した試行を再度試す秒単位の間隔。	
[ロケーション（Location）] セクション：		
ピア 1 ～ ピア 2 アドレス（Peer 1 to Peer 6 address）	トラバーサル サーバの IP アドレスまたは FQDN。 トラバーサル サーバが Expressway-E のクラスタの場合は、そのすべてのピアを組み込む必要があります。	詳細については、「Expressway クラスター間の隣接」を参照してください。

トラバーサル サーバ ゾーンの設定

Expressway-E はトラバーサル サーバとして機能でき、トラバーサル クライアント（Expressway-C）に代わってファイアウォール トラバーサルを実装します。

ファイアウォール トラバーサルを動作させるには、トラバーサル サーバ（Expressway-E）に特殊なタイプの各トラバーサル クライアントとの双方向の関係が必要です。Expressway-E と Expressway-C 間にこの接続を作成するには、「トラバーサルクライアントとサーバの設定」を参照してください。ファイアウォールを通過するためにトラバーサル クライアント ゾーンとトラバーサル サーバ ゾーンが連携する仕組みについて詳しくは、ファイアウォール トラバーサルについてを参照してください。

（注） トラバーサル ゾーンを確実に機能させるには、NTP サーバと同期させる必要があります。

トラバーサル クライアントと隣接させた後は、次のことが可能になります。

- トラバーサルクライアントへファイアウォールトラバーサルサービスを提供する
- トラバーサルクライアントにエンドポイントを照会する

- トラバーサルクライアントに送信する前にクエリへトランスフォーメーションを適用する
- ローカル Expressway とトラバーサルクライアント間のコールに使用する帯域幅を制御する
- 接続アドレスなどのゾーンステータス情報を表示する

（注） ステータス情報に示されている接続アドレスは、トラバーサル サーバ ゾーンと送信元のデバイス間で NAT 要素により変換されていることがあります。

表 *4:* トラバーサルサーバ ゾーンの設定リファレンス

フィールド	説明	使用方法のヒント
[設定（Configuration）] セクション：		
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[トラバーサル サーバ（Traversal server）] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。
[接続クレデンシャル（Connection credentials）] セクション		

フィールド	説明	使用方法のヒント
ユーザ名（Username）	トラバーサル クライアントは常に認証クレデンシャルを提供することによってトラバーサル サーバで認証される必要があります。 認証ユーザ名はトラバーサル クライアントが Expressway-E に提供する必要がある名前です。（トラバーサル クライアント ゾーンに接続クレデンシャルの **[ユーザ名（Username）]** として設定されています。）	また、クライアントの認証ユーザ名とパスワードについては、Expressway-E のローカル認証データベースにエントリがある必要があります。エントリのリストを確認し、必要に応じて追加するには、**[ローカル認証データベース（Local authentication database）]** ページに移動します。次のいずれかを行います。 • **[ローカル認証データベースの追加/削除（Add/Edit local authentication database）]** リンクをクリックします • **[設定（Configuration）]** > **[認証（Authentication）]** > **[ローカル データベース（Local database）]** に移動します
[H.323] セクション：		
モード（Mode）	トラバーサル クライアントで H.323 コールを送受信するかどうかを決定します。	
[Protocol]	ファイアウォールまたはNAT の通過に使用するプロトコル（*Assent* または *H.460.18*）を指定します。	詳細については、「ファイアウォール トラバーサル用ポートの設定」を参照してください。
[ポート（Port）]	トラバーサル クライアントで送受信する H.323 コールに使用するローカル Expressway-E のポート。	
H.460.19 逆多重化モード（H.460.19 demultiplexing mode）	2 つ以上のコールで同じ 2 つのポートをメディアに使用するかどうかを決定します。 *[オン（On）]*：トラバーサル クライアントからのすべてのコールで同じ 2 つのポートをメディアに使用します。 *[オフ（Off）]*：トラバーサル クライアントからの各コールで個別のポート ペアをメディアに使用します。	
SIP セクション：		

フィールド	説明	使用方法のヒント
モード（Mode）	トラバーサル クライアントで SIP コールを送受信するかどうかを決定します。	
[ポート（Port）]	トラバーサル クライアントで送受信する SIP コールに使用するローカル Expressway-E のポート。	これは、着信 TCP、TLS、および UDP SIP コールに使用するリスニング ポート（通常は 5060 と 5061）とは異なる必要があります。
トランスポート（Transport）	トラバーサル クライアントで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは、[TLS] です。	
ユニファイド コミュニケーション サービス（Unified Communications services）	このトラバーサル ゾーンが Mobile & Remote Access などのユニファイド コミュニケーション サービスを提供するかどうかを制御します。	有効にした場合、このゾーンも有効にし、**[TLS 検証モード（TLS verify mode）]** を有効にした状態で TLS を使用する必要があります。 この設定は[ユニファイドコミュニケーション モード（Unified Communications mode）] が *[モバイルとリモート アクセス（Mobile & Remote Access）]* に設定されているときにのみ適用されます。
TLS 検証モード（TLS verify mode）とサブジェクト名（subject name）	この Expressway とトラバーサル クライアント間での X.509 証明書チェックと相互認証を制御します。 **[TLS 検証モード（TLS verify mode）]** が有効になっている場合は、**[TLS 検証サブジェクト名（TLS verify subject name）]** を指定する必要があります。これは、トラバーサル クライアントの X.509 証明書内で検索する証明書の所有者の名前です。	トラバーサル クライアントがクラスタ化されている場合、**[TLS 検証サブジェクト名（TLS verify subject name）]** はクラスタの FQDN である必要があります。 詳細については、ネイバー システムの TLS 証明書の確認を参照してください。
プロキシ経由の登録の許可（Accept proxied registrations）	このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。	この設定は、Expressway がレジストラとして機能するドメイン宛の登録要求にのみ適用されます。他のドメイン宛の要求の場合は、**[SIP 登録プロキシ モード（SIP Registration Proxy Mode）]** の設定が適用されます。詳細については、登録要求のプロキシ経由での送信を参照してください。

フィールド	説明	使用方法のヒント
メディア暗号化モード（Media encryption mode）	このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスでICEメッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。
ICE パススルー サポート（ICE Passthrough support）	このゾーン内で Expressway が ICE パススルーをサポートする方法を制御します。	ICE パススルー サポートは ICE サポートよりも優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。 ICE パススルーの設定の詳細と必要なバージョンについては、Expressway 設定ガイドのページ に用意されている『*Mobile and Remote Access Through Cisco Expressway guide*』を参照してください。
マルチストリーム モード（Multistream mode）	Expressway B2BUA が発呼側間でマルチストリーム コールをネゴシエートすることを許可するかどうかを制御します。 *[オン（On）]*：Expressway は、発呼側がこのゾーンを通じてマルチストリームコールをネゴシエートし、セットアップすることを許可します。 *[オフ（Off）]*：Expressway はこのゾーンを通じてマルチストリーム ネゴシエーションを拒否します。発呼側は標準コールのネゴシエーションをフォールバックする必要があります。	この切り替えは、コールが B2BUA を通過しない場合はコールに影響しません。 発呼側双方にマルチストリーム機能がない場合、相互に正しく応答することが予測されるため、デフォルトは*[オン（On）]* になっています。ただし、発呼側間のマルチストリームの設定に問題がある場合、マルチストリーム モードを無効にして、発呼側が標準コールをネゴシエートできるかどうか確認することができます。 TelePresence Server の場合、標準コールは、TelePresence Server が、複数のストリームをエンドポイントに送信して独自の方法で処理する代わりに、複数の参加者から 1 つの「会議ストリーム」を構成してエンドポイントに送信することを意味します。

フィールド	説明	使用方法のヒント
ポイズンモード（Poison mode）	このゾーンを介して見つかったシステムに送信される SIP 要求が、この Expressway が再度受信したときには拒否されるように「「ポイズニング」」されるかどうかを決定します。	
プリロードされた SIP ルートのサポート（Preloaded SIP routes support）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
SIP パラメータの保持（SIP parameter preservation）	Expressway の B2BUA がこのゾーンを介してルーティングされた SIP 要求内のパラメータを保持するか、書き直すかを決定します。	*[オン（On）]*は、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを保持します。 *[オフ（Off）]*は、必要に応じて、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを B2BUA が書き直すことを許可します。 デフォルト：[オフ（Off）]
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、有効にする必要があります。
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新要求の送受信に SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション：		

フィールド	説明	使用方法のヒント
認証ポリシー（Authentication policy）	Expresswayがこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。	詳細 については、「認証ポリシー」を参照してください。
[UDP/TCP プローブ（UDP / TCP probes）] セクション：		
UDP の再試行間隔（UDP retry interval）	キープ アライブ確認を受信していない場合にクライアントが UDP プローブを Expressway-E へ送信する頻度（秒単位）。	デフォルトの UDP および TCP プローブの再試行間隔はほとんどの場合に適しています。ただし、NAT バインドのタイムアウトに問題が発生した場合は、変更する必要がある場合があります。
UDP の再試行回数（UDP retry count）	コール セットアップ時にクライアントが UDP プローブの Expressway-E への送信を試行する回数。	
UDP のキープ アライブ間隔（UDP keep alive interval）	コールが確立した後に、ファイアウォールの NAT バインドを有効にしておくために、クライアントが UDP プローブを Expressway-E に送信する間隔（秒単位）。	
TCP の再試行間隔（TCP retry interval）	キープ アライブ確認を受信していない場合にトラバーサル クライアントが TCP プローブを Expressway-E へ送信する間隔（秒単位）。	
TCP の再試行回数（TCP retry count）	コール セットアップ時にクライアントが TCP プローブの Expressway-E への送信を試行する回数。	
TCP のキープ アライブ間隔（TCP keep alive interval）	コールが確立しているときに、ファイアウォールの NAT バインドを有効にしておくために、トラバーサル クライアントが TCP プローブを Expressway-E に送信する間隔（秒単位）。	

ENUM ゾーンの設定

ENUM ゾーンでは、ENUM ルックアップを使用してエンドポイントを見つけることができます。使用されている ENUM DNS サフィックスに基づき、またはエンドポイントのエイリアスのパターンマッチングにより、あるいはそれらの両方で、ENUM ゾーンに 1 つ以上の検索ルールを作成できます。

1 つ以上の ENUM ゾーンを設定した後で、次のことが可能になります。

- エンドグループのそのグループ宛のエイリアス検索要求にトランスフォーメーションを適用します。
- ローカル Expressway と ENUM エンドポイントの各グループ間でのコールに使用する帯域幅を制御します。

ENUM ゾーンの使用方法と設定方法の詳細については、「ENUM ダイヤリングについて」 セクションを参照してください。

次の表に、ENUM ゾーンの設定可能なオプションを記載します。

表 *5 : ENUM* ゾーン設定

フィールド	説明	使用方法のヒント
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[ENUM] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。
DNS サフィックス（DNS suffix）	このゾーンを照会する ENUM ドメインを作成するために変換された E.164 番号に追加するドメイン。	
H.323 モード（H.323 Mode）	このゾーンについて H.323 レコードをルックアップするかを決定します。	

フィールド	説明	使用方法のヒント
SIP モード（SIP mode）	このゾーンについて SIP レコードをルックアップするかどうかを決定します。	

DNS ゾーンの設定

DNS ゾーンでは、DNSルックアップを使用してエンドポイントを見つけることができます。エンドポイント エイリアスのパターン マッチングに基づいて DNS ゾーンに 1 つ以上の検索ルールを作成できます。

1 つ以上の DNS ゾーンを作成した後、そのエンドポイント グループ宛のエイリアス検索要求にトランスフォームを適用できます。ローカル Expressway と DNS エンドポイントの各グループ間でのコールに使用する帯域幅を制御することもできます。DNS ゾーンの設定および仕様の詳細については、URI ダイヤリングについてを参照してください。

次の表に、DNS ゾーンの設定可能なオプションを記載します。

表 *6 : DNS* ゾーン設定

フィールド	説明	使用方法のヒント
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[DNS] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップカウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。
[H.323] セクション		
H.323 モード（H.323 Mode）	このゾーンを介した DNS ルックアップを使用して見つかったシステムとエンドポイントに対する H.323 コールを許可するかどうかを決定します。	
SIP セクション		

フィールド	説明	使用方法のヒント
SIP モード（SIP mode）	このゾーンを介した DNS ルックアップを使用して見つかったシステムとエンドポイントに対する SIP コールを許可するかどうかを決定します。	
TLS 検証モード（TLS verify mode）とサブジェクト名（subject name）	DNS ルックアップにより返された宛先システム サーバに対して X.509 認証チェックを Expressway が実行するかどうかを制御します。 **[TLS 検証モード（TLS verify mode）]** が有効になっている場合は、**[TLS 検証サブジェクト名（TLS verify subject name）]** を指定する必要があります。これは、宛先システムのサーバの X.509 証明書内で検索する証明書の所有者の名前です。	この設定は、DNS ルックアップが必要なプロトコルとして TLS を指定している場合にのみ適用されます。TLS が不要であれば、設定は無視されます。詳細については、ネイバー システムの TLS 証明書の確認を参照してください。
TLS サブジェクト名の確認（TLS verify subject name）	宛先システムのサーバの X.509 証明書で検索する証明書の所有者の名前（SAN にあるサブジェクト代替名の属性に含まれている必要があります）。	
TLS 検証着信マッピング（TLS verify inbound mapping）	[着信TLSマッピング（Inbound TLS mapping）] を [オン（On）] に切り替えて、ピア証明書に TLS 検証サブジェクト名が含まれている場合に着信 TLS 接続をこのゾーンにマッピングします。受信した証明書に TLS検証サブジェクト名（共通名またはサブジェクト代替名）が含まれていない場合は、接続はこのゾーンにマッピングされません。	[着信 TLS マッピング（Inbound TLS mapping）] を [オフ（Off）] に切り替えて、Expressway が着信 TLS接続をこのゾーンにマッピングしようとしないようにします。
フォールバック トランスポート プロトコル（Fallback transport protocol）	DNS NAPTR レコードと SIP URI パラメータによって必要なトランスポート情報が得られないときに DNS ゾーンからの SIP コールに使用するトランスポートタイプ。 デフォルトは、*[UDP]* です（有効になっている場合）。	
メディア暗号化モード（Media encryption mode）	インターネットへの SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。

フィールド	説明	使用方法のヒント
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。
プリロードされた SIP ルートのサポート（Preloaded SIP routes support）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
DNS 要求の変更（Modify DNS request）	このゾーンからの発信 SIP コールをダイヤルした宛先内のドメインではなく、手動で指定した SIP ドメインにルーティングします。	このオプションは、コール サービス制御で使用することを主な目的としています。www.cisco.com/go/hybrid-services を参照してください。
検索対象のドメイン（Domain to search for）	発信 SIP URI のドメインを検索するのではなく、DNS にある完全修飾ドメイン名を入力します。元の SIP URI には影響しません。	
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、有効にする必要があります。
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新リクエストを送受信するための SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション		

フィールド	説明	使用方法のヒント
SIP 認証信頼モード（SIP authentication trust mode）	**[認証ポリシー（Authentication Policy）]** と一緒に使用して、このゾーンから受信した事前に認証された SIP メッセージ（P-Asserted-Identity ヘッダーが含まれているもの）が信頼できるかどうかを制御、さらに、Expressway 内で認証済みまたは未認証として処理するかどうかを制御します。 *[オン（On）]*：事前認証済みメッセージは追加のチャレンジなしに信頼され、その後、Expressway内では認証済みとして扱われます。未認証メッセージは、**[認証ポリシー（Authentication Policy）]** が *[クレデンシャルを確認する（Check credentials）]* に設定されている場合はチャレンジされます。 *[オフ（Off）]*：既存の認証済みインジケータ（P-Asserted-Identityヘッダー）はすべてメッセージから削除されます。ローカルドメインからのメッセージは、**[認証ポリシー（Authentication Policy）]** が *[クレデンシャルを確認する（Check credentials）]* に設定されている場合はチャレンジされます。	DNS ゾーンの場合、認証済みとして処理するには、**[認証ポリシー（Authentication Policy）]** を常に設定します。
[詳細]セクション		

フィールド	説明	使用方法のヒント
アドレスレコードを含める（**Include address record**）	NAPTR（SIP）レコードまたは SRV（SIP と H.323）レコードがこのゾーンを介してダイヤルされたエイリアスで検出されなかった場合は、プライオリティが下位のゾーンの照会に進む前に、Expressway が A および AAAA DNS レコードを照会するかどうかを決定します。SIP または H.323 をサポートするシステム以外で A および AAAA レコードが同じドメインにある場合は、Expressway は検索が成功したと認識し、コールがこのゾーンに転送されて、コールが失敗する場合があります。 *[オン（On）]*：Expressway は A または AAAA レコードを照会します。検出された場合、Expressway はプライオリティが下位のゾーンは照会しません。 *[オフ（Off）]*：（デフォルト）Expressway は A および AAAA レコードを照会しません。その代わりに、検索を続行し、プライオリティが下位の残りのゾーンを照会します。	
ゾーン プロファイル（**Zone profile**）	ゾーンの詳細な設定方法を決定します。 *[デフォルト（Default）]*：工場出荷時のデフォルトプロファイルを使用します。 *[カスタム（Custom）]*：各設定を個別に行うことができます。	詳細設定について詳しくは、ゾーンの設定：詳細設定を参照してください。 シスコのカスタマー サポートのアドバイスがあった場合に個別の詳細設定を行うには、カスタム プロファイルのみを使用してください。

Webex ゾーンの設定

Webex ゾーンは、Expressway-E から Cisco Webex に接続するために事前設定された DNS ゾーンです。このゾーンを使用して、Cisco Webex ハイブリッド コール サービスまたは Webex Meetings、あるいはその両方を有効にすることができます。

このようにすると、Expressway-E は、Expressway-C を使用せずに Cisco Unified Communications Manager に接続します。このシナリオではトラバーサルまたはファイアウォールは必要ありません。また Expressway-E は、Webex クラウドを Cisco Unified Communications Manager に直接接続します。テスト済み設定では、Cisco Unified Communications Manager と Expressway-E 間のネイバーゾーンで、インターネット上の標準の Webex Edge Audio を使用します。

このシナリオでは、インバウンド接続を内部ファイアウォールで開く必要があります。そのため、通常のデュアルファイアウォール設定を使用した標準規格の導入ではサポートされて**いません**。

Webex ゾーンを有効にするには、次の方法を実行します。

1. **[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** へ移動します。
2. [新規（New）] をクリックします。
3. **[タイプ（Type）]** ドロップダウンから *[Webex]* を選択します。

   Expressway は、Cisco Webex への正しい接続を保証する事前設定された名前と事前設定されたパラメータを使用して新しいゾーンを作成します。

（注） このタイプのゾーンを複数作成することはできません。また、ゾーンを有効化した後で、ゾーンの 1 つのインスタンスを変更することはできません。

設定の詳細については、ハイブリッド コール サービスのドキュメントを参照してください。

デフォルト設定を変更する方法

Webex ゾーンのメディア暗号化モードは 「[自動（Auto）]」 です 。Webex ゾーンは事前設定された DNS ゾーンなので、シナリオによっては 「[オン（On）]」 である必要がある場合は、代わりに DNS ゾーンを作成することをお勧めします。その後、Expressway Web インターフェイスを介して DNS ゾーンを変更 します（**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]**を設定し、**[メディア暗号化モード（Media encryption mode）]** を *[オン（On）]*に設定します）。同じ回避策を使用して、**[SIP 認証信頼モード（SIP authentication trust mode）]** を *[オン（On）]* に変更できます。

ゾーンの設定：詳細設定

次の表に、カスタム ゾーン プロファイルの詳細なゾーン設定オプションを記載します。これらの設定の一部は、特定のゾーン タイプのみに適用されます。

設定	説明	デフォルト	ゾーン タイプ
アドレスレコードを含める（Include address record）	NAPTR（SIP）レコードまたは SRV（SIP と H.323）レコードがこのゾーンを介してダイヤルされたエイリアスで検出されなかった場合は、プライオリティが下位のゾーンの照会に進む前に、Expressway が A および AAAA DNS レコードを照会するかどうかを決定します。SIP または H.323 をサポートするシステム以外で A および AAAA レコードが同じドメインにある場合は、Expressway は検索が成功したと認識し、コールがこのゾーンに転送されて、コールが失敗する場合があります。 *[オン（On）]*：Expressway は A または AAAA レコードを照会します。検出された場合、Expressway はプライオリティが下位のゾーンは照会しません。 *[オフ（Off）]*：Expresswayは A および AAAA レコードを照会しません。その代わりに、検索を続行し、プライオリティが下位の残りのゾーンを照会します。	オフ（Off）	DNS
ピア ステータスのモニタ（Monitor peer status）	Expressway がゾーンのピアのステータスをモニタするかどうかを指定します。有効になっている場合は、H.323 LRQ または SIP OPTIONS、あるいはその両方が定期的にピアに送信されます。ピアが応答しない場合は、そのピアを非アクティブとマークします。すべてのピアが応答しない場合は、ゾーンを非アクティブとします。	○	ネイバー（Neighbor）
コール シグナリング ルーティング モード（Call signaling routed mode）	このネイバーで送受信するコールのシグナリングを Expressway がどのように処理するかを指定します。 *[自動（Auto）]*：シグナリングは**[コールシグナリングの最適化（Call signaling optimization）]（[設定（Configuration）]>[コール ルーティング（Call routing）]）**の設定に従って行われます。 *[常時（Always）]*：シグナリングは**[コールシグナリングの最適化（Call signaling optimization）]**の設定に関係なく、のネイバーで送受信するコールに応じて行われます。 トラバーサル ゾーンまたは B2BUA を介したコールは常にシグナリングを取得します。	Auto	ネイバー（Neighbor）

設定	説明	デフォルト	ゾーン タイプ
H.323 検索に自動的に応答（Automatically respond to H.323 searches）	Expressway がこのゾーン宛の H.323 検索を受信したときの動作を決定します。 *[オフ（Off）]*：LRQ メッセージがゾーンに送信されます。 *[オン（On）]*：検索をゾーンに転送せずに自動的に応答します。	オフ（Off）	ネイバー（Neighbor）
SIP 検索に自動的に応答（Automatically respond to SIP searches）	Expressway が H.323 検索として発信された SIP 検索を受信したときの動作を決定します。 *[オフ（Off）]*：SIP OPTIONS または SIP INFO メッセージが送信されます。 *[オン（On）]*：検索に自動的に応答します。検索が転送されることはありません。 通常はこれをデフォルトの [オフ（Off）] のままにしてください。ただし、SIP OPTIONS メッセージオプションを許可しないシステムもあります。そのため、これらのゾーンについては、設定を [オン（On）] にする必要があります。これを [オン（On）] に変更した場合はパターン マッチも設定し、このゾーン内で実際にエンドポイントに一致する検索のみに応答するよう設定する必要もあります。これを行わないと、プライオリティが下位の他のゾーンの検索が続行され、サポートできない場合でも、このゾーンにコールが転送されます。	オフ	ネイバー（Neighbor） DNS

設定	説明	デフォルト	ゾーン タイプ
相互運用されるコール用に空の INVITE を送信（Send empty INVITE for interworked calls）	Expressway がこのゾーンを介して送信する SDP なしに SIP INVITE メッセージを生成するかどうかを決定します。SDP を使用していない INVITE は、宛先デバイスがコーデックの選択を開始するよう求められることを意味し、コールが H.323 からローカルにインターワーキングされていた場合に使用されます。 *[オン（On）]*：SDP なしの SIP INVITE が生成されます。 *[オフ（Off）]*：SIP INVITE が生成され、事前設定された SDP が挿入されてから INVITE が送信されます。 ほとんどの場合、このオプションは通常はデフォルトの [オン（On）] のままにしてください。ただし、一部のデバイスは SDP なしの INVITE を許可しません。そのため、これらのゾーンについてはこの設定を [オフ（Off）] にする必要があります。 （注） 事前に設定された SDP の設定は、CLI で `xConfiguration Zones Zone [1..1000] [Neighbor/DNS] Interworking SIP` コマンドを使用して設定できます。これらの設定値は、シスコ カスタマー サポートのアドバイスがあった場合にのみ、変更してください。		

設定	説明	デフォルト	ゾーン タイプ
SIP パラメータの保持（SIP parameter preservation）	Expressway の B2BUA がこのゾーンを介してルーティングされた SIP 要求内のパラメータを保持するか、書き直すかを決定します。 *[オン（On）]*は、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを保持します。 *[オフ（Off）]*は、必要に応じて、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを B2BUA が書き直すことを許可します。 デフォルト：[オフ（Off）]	オフ（Off）	ネイバー（Neighbor） DNS UC トラバーサル（UC Traversal） トラバーサル サーバ（Traversal Server） トラバーサル クライアント（Traversal Client）
SIP Poison モード（SIP poison mode）	*[オン（On）]*：このゾーンを介して見つかったシステムに送信される SIP 要求が、この Expressway が再度受信したときには拒否されるように「「ポイズニング」」されます。 *[オフ（Off）]*：このゾーンを介して送信され、Expressway が再度受信する SIP 要求は拒否されません。これらの要求は通常どおりに処理されます。	オフ	ネイバー（Neighbor）トラバーサル クライアント（Traversal client）トラバーサル サーバ（Traversal server）DNS
SIP 暗号化モード（SIP encryption mode）	Expressway がこのゾーンで暗号化された SIP コールを許可するかどうかを決定します。 *Auto*：セキュア SIP トランスポート（TLS）が使用されている場合、SIP コールが暗号化されます。 *[Microsoft]*：SIP コールは MS-SRTP を使用して暗号化されます。 *[オフ（Off）]*：SIP コールは暗号化されません。 通常はこのオプションをデフォルトの *[自動（Auto）]* のままにしてください。	自動（Auto）	ネイバー（Neighbor）

設定	説明	デフォルト	ゾーン タイプ
SIP REFER モード（SIP REFER mode）	SIP REFER 要求の処理方法を決定します。 *[転送（Forward）]*：SIP REFER 要求がターゲットに転送されます。 *[終了（Terminate）]*：SIP REFER 要求は Expressway によって終了されます。	転送（Forward）	ネイバー（Neighbor）
Meeting Server ロードバランシング（Meeting Server load balancing）	X8.11 以降、Cisco Expressway シリーズではコールブリッジ グループに含まれる Meeting Server 間のコールのロードバランシングに使用されるメカニズムがサポートされています。 Cisco Meeting Server がコール ブリッジ グループに含まれている場合、容量のないサーバ上のスペースに参加者が参加しようとすると、コールは別のサーバーに再ルーティングされます。ルーティング先のサーバは、元のコールの詳細を使用して SIP INVITE をコール制御層に送信します。これにより、参加者は別の Meeting Server 上の適切なスペースに参加できます。「「2 番目」」のサーバに容量があるが、別の Meeting Server にそれよりも多い容量がある場合は、2 番目のサーバはその Meeting Server に SIP INVITE を送信するよう求めます。 *[オン（On）]*：Expressway B2BUA は Meeting Server からの INVITE を処理します。Unified CM またはこの Expressway に登録されているエンドポイント、あるいは隣接する VCS または Expressway に登録されているエンドポイントに対してロードバランシングを有効にする必要があります。 *[オフ（Off）]*：Expressway B2BUA は p ではありません	オフ（Off）	ネイバー（Neighbor）
SIP マルチパート MIME 削除モード（SIP multipart MIME strip mode）	複数の MIME ストリッピングをこのゾーンからの要求上で実行するかどうかを制御します。 通常はこのオプションをデフォルトの [オフ（Off）] のままにしてください。	オフ（Off）	ネイバー（Neighbor）

設定	説明	デフォルト	ゾーン タイプ
SIP UPDATE 削除モード（SIP UPDATE strip mode）	Expressway がこのゾーンで送受信するすべての要求と応答の Allow ヘッダーから UPDATE メソッドを削除するかどうかを制御します。 通常はこのオプションをデフォルトの [オフ（Off）] のままにしてください。ただし、Allow ヘッダーの UPDATE メソッドをサポートしていないシステムもあります。そのため、これらのゾーンについては設定を [オン（On）] にする必要があります。	オフ（Off）	ネイバー（Neighbor）
相互接続 SIP 検索戦略（Interworking SIP Search Strategy）	H.323 コールとインターワーキングするときに Expressway が SIP エンドポイントをどのように検索するかを決定します。 *[オプション（Options）]*：Expressway は OPTIONS 要求を送信します。 *[情報（Info）]*：Expressway は INFO 要求を送信します。 通常はこのオプションをデフォルトの *[オプション（Options）]* のままにしてください。ただし、OPTIONS 要求に応答できないエンドポイントもあります。そのため、これらのエンドポイントについては *[情報（Info）]* に設定する必要があります。	オプション（Options）	ネイバー（Neighbor）
SIP UDP/BFCP フィルタ モード（SIP UDP/BFCP filter mode）	このゾーンに送信された INVITE 要求から UDP/BFCP をフィルタリングにより除去するかどうかを決定します。UDP/BFCP プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。 *[オン（On）]*：UDP/BFCP プロトコルを参照しているメディア回線が TCP/BFCP で置き換えられ、無効になります。 *[オフ（Off）]*：INVITE 要求は変更されません。	オフ	ネイバー（Neighbor） DNS

設定	説明	デフォルト	ゾーン タイプ
SIP UDP/IX フィルタ モード（SIP UDP/IX filter mode）	このゾーンに送信された INVITE 要求から UDP/UDT/IX または UDP/DTLS/UDT/IX をフィルタリングにより除去するかどうかを決定します。UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。 *[オン（On）]*：UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルを参照するメディア回線を RTP/AVP に置き換えて無効にします。 *[オフ（Off）]*：INVITE 要求は変更されません。 次の場合は **[SIP UDP/IX フィルタ モード（SIP UDP/IX filter mode）]** を *[オン（On）]* に設定することを推奨します。 • 外部ネットワークまたはシスコ以外のインフラストラクチャに接続されているネイバーゾーンを通じてルーティングされている Business-to-Business（B2B）コール • Unified CM 8.x 以前に内部的に接続されているコール（9.x 以降の場合は *[オフ（Off）]* に設定）	Cisco Unified Communications Manager で事前設定されたゾーンプロファイルでは *[オフ（Off）]*。 それ以外の場合は *[オン（On）]*。	ネイバー（Neighbor） DNS
SIP レコード ルート アドレス タイプ（SIP record route address type）	Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求のレコードルートまたはパスのヘッダーのホスト名を使用するかを制御します。 *[IP]*：Expressway の IP アドレスを使用します。 *[ホスト名（Hostname）]*：Expressway の**システム ホスト名**を使用します（空白の場合は、IP アドレスが使用されます）。	IP	ネイバー（Neighbor） DNS
SIP プロキシ - ヘッダー削除リストが必要（SIP Proxy-Require header strip list）	このゾーンから受信した SIP 要求の Proxy-Require ヘッダーを検索し、そのヘッダーから削除するオプション タグのカンマ区切りのリスト。	なし（None）	ネイバー（Neighbor）

ゾーンの設定：事前設定されたプロファイルの設定

次の表に、事前に設定されたプロファイルに自動的に適用される詳細なゾーン設定オプションを示します。

設定	Cisco Unified CM（9.x or 以降）	Cisco Unified CM（8.6.1 または 8.6.2）	Cisco Unified CM（8.6 以下）	Nortel Communication Server 1000	インフラストラクチャ デバイス	デフォルト
ピア ステータスのモニタ（Monitor peer status）	はい	はい	はい	はい	いいえ	はい
コール シグナリング ルーティング モード（Call signaling routed mode）	常に（Always）	常に（Always）	常に（Always）	自動（Auto）	常に（Always）	自動（Auto）
H.323 検索に自動的に応答（Automatically respond to H.323 searches）	消灯	消灯	消灯	オフ	オン	オフ
SIP 検索に自動的に応答（Automatically respond to SIP searches）	消灯	消灯	消灯	オフ	オン	オフ
相互運用されるコール用に空の INVITE を送信（Send empty INVITE for interworked calls）	オン	オン	オン	オン	オン	オン

設定	Cisco Unified CM（9.x or 以降）	Cisco Unified CM（8.6.1 または 8.6.2）	Cisco Unified CM（8.6 以下）	Nortel Communication Server 1000	インフラストラクチャデバイス	デフォルト
SIP パラメータの保持（SIP parameter preservation）	消灯	消灯	消灯	消灯	消灯	消灯
SIP Poison モード（SIP poison mode）	消灯	消灯	消灯	消灯	消灯	消灯
SIP 暗号化モード（SIP encryption mode）	自動（Auto）	自動（Auto）	自動（Auto）	自動（Auto）	自動（Auto）	自動（Auto）
SIP REFER モード（SIP REFER mode）	転送（Forward）	転送（Forward）	転送（Forward）	転送（Forward）	転送（Forward）	転送（Forward）
Meeting Server ロードバランシング（Meeting Server load balancing）	消灯	消灯	消灯	消灯	オフ	オン
SIP マルチパート MIME 削除モード（SIP multipart MIME strip mode）	消灯	消灯	消灯	消灯	消灯	消灯
SIP UPDATE 削除モード（SIP UPDATE strip mode）	消灯	消灯	オフ	オン	オフ	消灯

設定	Cisco Unified CM（9.x or 以降）	Cisco Unified CM（8.6.1 または 8.6.2）	Cisco Unified CM（8.6 以下）	Nortel Communication Server 1000	インフラストラクチャデバイス	デフォルト
相互接続 SIP 検索戦略（Interworking SIP Search Strategy）	オプション	オプション	オプション	オプション	オプション	オプション
SIP UDP/BFCP フィルタモード（SIP UDP/BFCP filter mode）	消灯	オフ	オン	オフ	消灯	消灯
SIP UDP/IX フィルタモード（SIP UDP/IX filter mode）	オフ	オン	オン	オン	オン	オフ
SIP レコードルートアドレス タイプ（SIP record route address type）	IP	IP	IP	IP	IP	IP
SIP プロキシ - ヘッダー削除リストが必要（SIP Proxy-Require header strip list）	<空白>	<空白>	<空白>	[illegible]	<空白>	<空白>

Expressway と Unified CM 間の SIP トランクの設定詳細：

「Expressway 設定ガイド」 ページに用意されている『*Cisco Expressway and CUCM via SIP Trunk Deployment Guide*』を参照してください。

ネイバー システムの TLS 証明書の確認

SIP TLS 接続が Expressway とネイバー システム間で確立されている場合、ネイバー システムの ID を確認するためにそのシステムの X.509 証明書を確認するように Expressway を設定できます。これを行うには、ゾーンの [TLS 検証モード（TLS verify mode）] を設定します。

TLS 検証モードが有効にされている場合、ゾーン設定の **[ピア アドレス（Peer address）]** フィールドに指定されたネイバー システムの FQDN または IP アドレスがそのシステムで提示された X.509 証明書に含まれる証明書の所有者名と照合するために使用されます。(名前は、証明書のサブジェクト代替名属性に含める必要があります。) 証明書自体も有効であり、信頼された認証局によって署名されている必要があります。

（注） トラバーサル サーバと DNS ゾーンでは、接続元のトラバーサル クライアントの FQDN または IP アドレスは設定されないため、必須の証明書の所有者の名前を個別に指定する必要があります。

ネイバー システムが別の Expressway であるか、またはトラバーサル クライアントとトラバーサル サーバの関係がある場合、互いの証明書を認証するように 2 つのシステムを設定できます。これは相互認証と呼ばれ、この場合は各 Expressway がクライアントとサーバの両方として機能します。そのため、各 Expressway の証明書がクライアントとしてもサーバとしても有効であることを確認する必要があります。

証明書の確認についての詳細、および Expressway のサーバ証明書のアップロードと信頼できる認証局のリストのアップロードの手順については、「セキュリティ証明書について」を参照してください。

着信コール専用のゾーンの設定

エイリアス検索要求を送信しないように（このゾーンからの着信コールのみを受信する場合など）ゾーンを設定するには、ターゲットとしてそのゾーンが必要な検索ルールを定義しないでください。

このシナリオでは、ゾーンを表示するときに、検索ルールが設定されていないことを示す警告を無視できます。