



## ダイヤルプランとコール処理

- コールルーティングプロセス (1 ページ)
- Cisco VCS のディレクトリサービスについて (4 ページ)
- ホップ カウントの設定 (4 ページ)
- ダイヤルプランの設定 (6 ページ)
- トランスフォーメーションと検索ルールについて (7 ページ)
- 検索とトランスフォーメーションの例 (18 ページ)
- Kari の法律の 911 コール (Expressway をコール制御および PSTN ゲートウェイとして使用) (32 ページ)
- 外部サービスを使用するための検索ルールの設定 (40 ページ)
- コールポリシーについて (43 ページ)
- サポートされているアドレス形式 (52 ページ)
- IP アドレスによるダイヤリング (54 ページ)
- URI ダイヤリングについて (56 ページ)
- ENUM ダイヤリングについて (66 ページ)
- ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定 (74 ページ)
- コールルーティングとシグナリングの設定 (74 ページ)
- コールの識別 (76 ページ)
- コールの切断 (77 ページ)

## コールルーティングプロセス

Expressway の機能の 1 つに適切な宛先へのコールのルーティングがあります。これは、指定されたターゲットエイリアスを見つけるために着信検索要求を処理することで行われます。これらの検索要求は次の場所から送信されます。

- ローカルで登録済みのエンドポイント
- ネイバー、トラバーサルクライアント、トラバーサルサーバなどのネイバーシステム
- パブリックインターネットのエンドポイント

コールの宛先の特定には多くの手順があり、これらの手順の一部にはエイリアスの変換や他のエイリアスへのコールのリダイレクトが含まれています。

エイリアスを元の形式から別の形式に変換し、その後で元のエイリアスに戻す場合に循環参照を避けるには、**ダイヤリングプラン**をセットアップする前にプロセスを理解していることが重要です。Expressway は循環参照を検出できます。循環参照を特定すると、VCS は検索のそのブランチを終了させ、「「ポリシーのループを検出しました (policy loop detected) 」」というエラーメッセージを返します。

### Expressway によるコールの宛先の決定方法

次に、宛先のエンドポイントを見つけようとするときに Expressway が従うプロセスについて説明します。

1. 発信者がエンドポイントに宛先エンドポイントのエイリアスまたはアドレスを入力します。このエイリアスまたはアドレスは、**サポートされているアドレス形式**をとることができます。
2. 宛先アドレスは、Expressway で受け取られます  
(アドレスは、登録済みのエンドポイントから Expressway へ直接送られるか、または導入の他のコール処理インフラストラクチャの結果として間接的に送られることもあります)。
3. エイリアスには、すべての**検索前トランスフォーメーション**についてが適用されます。
4. すべての**コールポリシーの設定**が(変換後の)エイリアスに適用されます。その結果、1つ以上の新しいターゲットエイリアスとなった場合、その新しいエイリアスを検索前のトランスフォーメーションと照合してチェックすることからプロセスが再開されます。
5. すべてのユーザポリシー (**FindMe** が有効になっている場合) がエイリアスに適用されます。エイリアスが1つ以上の新しいエイリアスを解決する FindMe ID である場合、検索前のトランスフォーメーションとコールポリシーと照合して結果のすべてのエイリアスを確認することからプロセスが再開されます。
6. 次に、Expressway は検索ルールに従ってエイリアスを検索します。



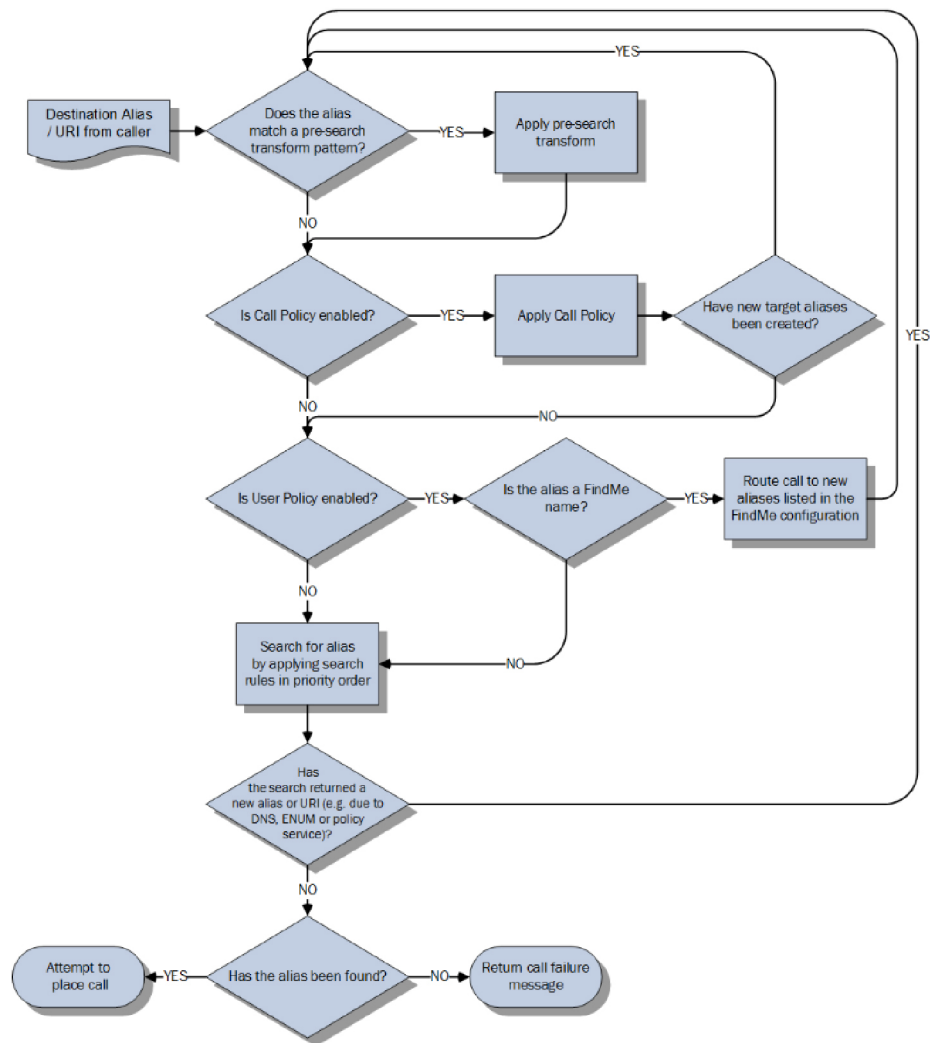
(注) Expressway は意図的に H.323 ロケーション要求から読み取った最初の宛先エイリアスのみを検索します。稀に、これによってコールが予想どおりにルーティングされないことがあります。

- マッチングルールで、クエリを**ターゲット**に送信する前に、ゾーントランスフォーメーションをエイリアスに適用する場合があります。[**ターゲット (Target)**]には、次のいずれかのタイプを指定できます。
  - **ローカルゾーン** : Expressway に登録されたエンドポイントとデバイス。
  - **ネイバーゾーン** : Expressway の設定済みの外部ネイバーゾーンの1つ、あるいは DNS または ENUM のルックアップゾーン。

- **ポリシー サービス**：外部サービスやアプリケーション。サービスは、コールをルーティングする必要があるゾーンを指定するか、または新しい宛先エイリアスを指定するなどの CPL を返します。

7. 検索で新しいURIまたはエイリアスが返された場合（DNSまたはENUMのルックアップ、あるいはポリシーサービスからの応答などのため）、プロセスは再開され、検索前トランスフォーメーションに照合して新しいURIを確認し、コールポリシーとユーザポリシーを適用してから、新しいExpressway検索を実行します。
8. ローカルゾーン内、外部ゾーンの1つでエイリアスが検出された、またはポリシーサービスによってルーティング先が返された場合、Expresswayはコールを発信しようとします。
9. エイリアスが検出されなかった場合は、コールが失敗したことを通知するメッセージで応答します。

図 1: コールルーティングのフローチャート



453646

## Cisco VCS のディレクトリサービスについて

### ホップカウントの設定

各検索要求には、その検索を開始したシステムによってホップカウント値が割り当てられます。要求が別のネイバーゲートキーパーまたはプロキシに転送されるたびに、ホップカウント値は1ずつ減っていきます。ホップカウントが0に達すると、要求はそれ以上は転送されず、検索は失敗します。

ローカル Expressway によって開始された検索要求では、要求に割り当てるホップカウントをゾーンごとに設定できます。ゾーンのホップカウントは、ローカル Expressway から開始され、そのゾーンに送信されたすべての検索要求に適用されます。

別のゾーンから受信した検索要求には、ホップカウントがすでに割り当てられています。その要求をさらにネイバースゾーンに転送すると、2つの値（元のホップカウントとそのゾーン用に設定されたホップカウント）のどちらか小さいほうが使用されます。

H.323 では、ホップカウントは検索要求のみに適用されます。SIP では、ホップカウントはゾーンに送信されたすべての要求に適用されます（要求の [Max-Forwards] フィールドに影響します）。

ホップカウント値には、1 ~ 255 を指定できます。デフォルトは 15 です。



- (注) ホップカウントを必要以上に高く設定すると、ネットワークにループを発生させるリスクがあります。このような場合、検索要求は、ホップカウントが0に到達するまでネットワークに送信され、リソースを不必要に消費します。これは、[コールルーティングとシグナリングの設定](#)を [オン (On)] に設定することによって防ぐことができます。

URI または ENUM によるダイヤリングでは、使用するホップカウントは、宛先エンドポイント（または関連付けられた DNS あるいは中間の SIP プロキシまたはゲートキーパー）を介して検出された、関連 DNS ゾーンまたは ENUM ゾーンに対するものです。

## ゾーンのホップカウントの設定

ホップカウントはゾーンごとに設定します。



- 重要** ネットワークが複雑な場合は、デフォルトのホップカウントが環境に対して低すぎる可能性があります。これにより、適切に設定された導入で予期しないコールエラーが発生する可能性があります。長いコールパスが予想される場合は、ホップカウントを増やすことを検討してください。

その他のゾーンオプションの詳細については、「[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。

- ステップ 1** [ゾーン (Zones)] ページ ([設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)]) に移動します。
- ステップ 2** 設定するゾーンの名前をクリックします。[ゾーンの編集 (Edit zone)] ページが表示されます。
- ステップ 3** [設定 (Configuration)] セクションの [ホップカウント (Hop count)] フィールドに、このゾーンに使用するホップカウント値を入力します。

## ダイヤルプランの設定

「ダイヤルプランの設定 (Dial plan configuration)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [設定 (Configuration)]) を使用して、特定のコールシナリオでの Expressway によるコールルーティング方法を設定します。

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 (Description)	使用方法のヒント
不明 IP アドレスへのコール (Calls to unknown IP addresses)	<p>Expressway またはそのネイバーの 1 つの登録されていないシステムに Expressway がコールを試行する方法を決定します。</p> <p>[直接 (Direct)] : Expressway がネイバーを照会することなく、エンドポイントが不明な IP アドレスにコールできます。端部がローカルシステムに直接登録されていたかのように、コールセットアップが実行されます。</p> <p>[間接 (Indirect)] : 不明な IP アドレスへのコールを受信すると、Expressway はネイバーにそのリモートアドレスを照会し、許可されれば、ネイバーを通じてコールをルーティングします。</p> <p>[オフ (Off)] : Expressway に直接登録されたエンドポイントが Expressway に直接登録されたシステムの IP アドレスのみをコールする可能性があります。</p> <p>デフォルトは [間接 (Indirect)] です。</p>	<p>この設定は、ゾーントランスフォーメーションの前、かつ検索前のトランスフォーメーション、コールポリシーまたはユーザポリシーのルールの適用後にコールの宛先アドレスに適用されます。</p> <p>コール制御に加えて、SIP デバイスへのプロビジョニングメッセージとプレゼンスメッセージは IP アドレスにルーティングされるため、この設定はこれらのメッセージの動作も決定します。</p> <p>詳細については、<a href="#">IP アドレスによるダイヤリング</a>を参照してください。</p>
フォールバックエイリアス (Fallback alias)	<p>Expressway の IP アドレスまたはドメイン名が指定されていても、コールエイリアスが指定されていないコールの場合に、着信メッセージを発信するエイリアス。</p>	<p>フォールバックエイリアスが設定されていない場合、エイリアスを指定しないコールは切断されます。詳細については、以下を参照してください。</p>

## フォールバックエイリアスについて

Expressway は、それ自体宛でも、エイリアスが指定されていないコールを受信できます。これは、次の理由のいずれかで発生することがあります。

- 発信者が Expressway の IP アドレスを直接ダイヤルした

- 発信者がプレフィックスとしてエイリアスを指定することなく、Expresswayに属するドメイン名（設定されている SIP ドメイン、または Expressway の IP アドレスを示す SRV レコードがあるドメインのいずれか）をダイヤルした

通常、このようなコールは切断されます。ただし、[フォールバック エイリアス (Fallback alias)] が指定されている場合、これらのコールはそのエイリアスにルーティングされます。



- (注) ユーザがコールの発信先のエイリアスや IP アドレスを入力することを許可しないエンドポイントもあります。

### 使用例

フォールバックエイリアスを受付係として設定し、エイリアスを指定しないすべてのコールに個別に応答して、適切にリダイレクトすることができます。

たとえば、ある会社のドメインが **example.com** だとします。受付のエンドポイントのエイリアスは **reception@example.com** です。Expressway をフォールバック エイリアス、**reception@example.com** で設定します。つまり、**example.com** に直接行われたコール（つまり、エイリアスによるプレフィックスなし）はすべて **reception@example.com** に転送され、受付係がコールに応答して適切に転送されます。

## トランスフォーメーションと検索ルールについて

Expressway は、コールルーティングプロセスの一環として、トランスフォーメーションと検索ルールを使用するように設定できます。

### トランスフォーメーション

トランスフォーメーションを使用して、特定の条件に一致した場合に検索要求内のエイリアスを変更します。プレフィックス、サフィックス、または文字列全体を削除または置換したり、正規表現を使用して、エイリアスを変換できます。

このトランスフォーメーションは、ルーティングプロセスの2つのポイントで、検索前のトランスフォーメーションとゾーントランスフォーメーションとしてエイリアスに適用できます。

- **検索前トランスフォーメーション**は、コールポリシーまたはユーザポリシーが適用される前と検索プロセスが実行される前に適用されます（詳細については、[検索前トランスフォーメーションについて](#)を参照してください）。
- **ゾーントランスフォーメーション**は、検索プロセス時に、必要に応じて個別の検索ルールによって適用されます。検索ルールがエイリアスと一致すると、検索要求がターゲットゾーンまたはポリシーサービスに送信される前に、それを使用してターゲットエイリアスを変更できます（詳細については、[検索とゾーン変換プロセス](#)を参照してください）。

## 検索ルール

検索ルールを使用して、適切なターゲットゾーン（ローカルゾーンを含む）またはポリシーサービスに着信検索要求を送信します。

Expressway の検索ルールは詳細な設定が可能です。次の操作を実行できます。

- 特定のゾーンまたはポリシーサービスへの検索をフィルタリングするエイリアス、IP アドレス、およびパターン マッチの定義。
- ルールを適用したり、一致が検出された後にプライオリティが下位の検索ルールの適用を中止するためのプライオリティの定義。これにより、送信する可能性がある検索要求の数を削減し、検索プロセスをスピードアップします。
- プロトコル（SIP または H.323）やクエリのソース（ローカルゾーンまたはサブゾーンの特定のゾーン）に応じた異なるルールのセットアップをします。
- 標準ベースの SIP または Microsoft SIP など、特定のタイプのトラフィックにのみ一致するルールのセットアップをします。
- 特定の検索ルールを **認証された要求** のみに適用可能にすることによる、未認証デバイスが使用できる宛先またはネットワーク サービスの範囲の制限します。
- クエリがターゲットゾーンまたはポリシーサービスに送信される前にエイリアスを変更するためのゾーントランスフォーメーションの使用します。



- (注) 複数の検索ルールが同じターゲットゾーンまたはポリシーサービスを参照できます。つまり、ゾーンまたはポリシー サービスごとに異なる検索条件とゾーン トランスフォーメーションを指定できます。

Expressway は、指定されたエイリアスを検出するためにゾーンを検索するときに着信コールの プロトコル（SIP または H.323）を使用します。検索が失敗すると、Expressway はその検索元と **[インターワーキング モード (Interworking mode)]** (**[設定 (Configuration)]**) > **[プロトコル (Protocols)]** > **[インターワーキング (Interworking)]** に応じて代替プロトコルを使用し、同じゾーンを再度検索することがあります。

- 要求をネイバーシステムから受け取っており、**[インターワーキングモード (Interworking mode)]** が **[登録済みのみ (Registered only)]** に設定されている場合、Expressway は両方のプロトコルを使用してローカルゾーンを検索します。また、その他のゾーンにはネイティブのプロトコルのみを使用して検索します（エンドポイントの一方がローカルに登録されている場合にのみコールをインターワーキングするため）。
- **[インターワーキング モード (Interworking mode)]** が **[オン (On)]** に設定されているか、または要求がローカルに登録されているエンドポイントから発信されたものである場合、Expressway は両方のプロトコルを使用して、ローカルゾーンとすべての外部ゾーンを検索します。



## 検索前トランスフォーメーションについて

検索前トランスフォーメーション機能では、着信検索要求のエイリアスを変更できます。トランスフォーメーションは、コールポリシーまたはユーザポリシーの適用前で、検索が実行される前に Expressway によって適用されます。

各検索前トランスフォーメーションはエイリアスを比較する文字列と、その文字列に一致する場合にエイリアスに加える変更を定義します。エイリアスが変換されると、そのエイリアスは変更された状態を維持し、その新しいエイリアスに対してその後のすべてのコール処理が適用されます。



(注) 1つの検索で一致できる変換は1つのみです。

### クラスタ化システム

クラスタ内のすべてのピアは、検索前トランスフォーメーションを含めて同じに設定する必要があります。各 Expressway は、任意のピアからの検索要求を Expressway 自体のローカルゾーンから着信したものとして処理し、要求受信時には検索前トランスフォーメーションを再度適用することはありません。

### 変換が適用されるのはいつか

- これは、ローカルに登録されたエンドポイント、ネイバー、トラバーサルクライアントおよびトラバーサルサーバのゾーン、ならびにパブリックインターネット上のエンドポイントから受信した着信検索要求すべてに適用されます。
- ピアから受信した要求に適用されません。これらは同じように設定されています。したがって、すでに同じ変換が適用されています。
- Expressway に登録されているエンドポイントから受信した GRQ メッセージまたは RRQ メッセージには適用されません。これらのメッセージに表示されるエイリアスには、エンドポイントが登録されます。

### 検索前トランスフォーメーションのプロセス

最大100の検索前トランスフォーメーションを設定できます。各トランスフォーメーションには、1～65534の一意のプライオリティを付ける必要があります。

1. すべての着信エイリアスは、1に最も近いプライオリティのものから順に各トランスフォーメーションと比較されます。一致した場合、変換がエイリアスに適用され、それ以上の検索前チェックと新しいエイリアスの変換は実行されません（検索ごとに1つの変換のみを一致させることができます）。残りのコールルーティングプロセスには新しいエイリアスが使用されます。
2. これ以降のエイリアスのトランスフォーメーションは残りの検索プロセス中に実行される場合があります。これは、**コールポリシー**（管理者ポリシーとも呼ばれる）またはユーザ

ポリシー（**FindMe** が有効になっている場合）の結果によります。この場合、検索前トランスフォーメーションが新しいエイリアスに再度適用されます。

既存のトランスフォーメーションと同じプライオリティの新しい検索前トランスフォーメーションを追加する場合、それよりも下位のプライオリティ（大きい数値を持つ）のすべてのトランスフォーメーションには1ずつ増えるプライオリティがあり、新しいトランスフォーメーションは指定したプライオリティで追加されます。または、すべての優先順位を下に移動する「スロット」が不十分な場合にエラーメッセージが表示されます。

## 検索前トランスフォーメーションの設定

「トランスフォーメーション (Transforms)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [トランスフォーメーション (Transformation)]) には Expressway に現在設定されているすべての[検索前トランスフォーメーションについてのリスト](#)が表示されます。これは、トランスフォーメーションの作成、編集、削除、有効化および無効化に使用します。

エイリアスは、パターンの [タイプ (Type)] で指定した方法でエイリアスが [パターン (Pattern)] と一致する場合にトランスフォーメーションが検出されるまで、[プライオリティ (Priority)] の順序で各トランスフォーメーションと比較されます。次に、エイリアスは、検索が（ローカルに、または外部ゾーンに対して）実行される前に [パターン動作 (Pattern behavior)] と [置換文字列 (Replace string)] のルールに従って変換されます。

エイリアスは変換された後は変更された状態が維持され、それ以降のすべてのコール処理は新しいエイリアスに適用されます。



(注) 変換はすべての[ユニファイドコミュニケーション](#)メッセージにも適用されます。

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 (Description)	使用方法のヒント
優先度	トランスフォーメーションのプライオリティ。プライオリティは1～65534の範囲であり、1が最も高いプライオリティになります。トランスフォーメーションはプライオリティ順に適用されるため、プライオリティは各トランスフォーメーションに一意である必要があります。	
説明 (Description)	トランスフォーメーションの任意の自由形式の説明。	リストのトランスフォーメーション上にマウスポインタを置くと、ツールチップとして説明が表示されます。

フィールド	説明 (Description)	使用方法のヒント
<p>パターンタイプ (Pattern type)</p>	<p>適用するルールで、パターン文字列をどのようにエイリアスと照合するか。次のオプションがあります。</p> <p><i>Exact</i> : 文字列全体がエイリアスと1文字も違うことなく完全に一致する必要があります。</p> <p><i>Prefix</i> : 文字列がエイリアスの先頭に表示される必要があります。</p> <p><i>Suffix</i> : 文字列がエイリアスの末尾に表示される必要があります。</p> <p>[正規表現 (Regex) ] : 文字列を正規表現として処理します。</p>	<p>パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、[パターンの確認 (Check pattern) ] ツール ([メンテナンス (Maintenance) ] &gt; [ツール (Tools) ] &gt; [パターンの確認 (Check pattern) ]) を使用してテストできます。</p>
<p>パターン文字列 (Pattern string)</p>	<p>エイリアスを比較するパターンを指定します。</p>	<p>Expressway には、特定の設定要素との照合に使用できる、事前に設定された一連の <b>パターンマッチング変数</b> が備わっています。</p>
<p>パターン動作 (Pattern behavior)</p>	<p>エイリアスの一致部分の変更方法を指定します。オプションは次のとおりです。</p> <p>[除去 (Strip) ] : 一致するプレフィックスまたはサフィックスが削除されます。</p> <p>[置換 (Replace) ] : エイリアスの一致部分が [置換文字列 (Replace string) ] のテキストで置き換えられます。</p> <p>[プレフィックスの追加 (Add Prefix) ] : エイリアスの前に [追加テキスト (Additional text) ] の値を追加します。</p> <p>[サフィックスの追加 (Add Suffix) ] : エイリアスの後ろに [追加テキスト (Additional text) ] を追加します。</p>	
<p>文字列の置換 (Replace string)</p>	<p>パターンに一致するエイリアスの部分を置き換える文字列</p>	<p>[パターン動作 (Pattern behavior) ] が [置換 (Replace) ] の場合にのみ適用されます。</p> <p>正規表現を使用できます。</p>

フィールド	説明 (Description)	使用方法のヒント
追加テキスト (Additional text)	プレフィックスまたはサフィックスとして追加する文字列。	[パターン動作 (Pattern behavior)] が [プレフィックスの追加 (Add Prefix)] または [サフィックスの追加 (Add Suffix)] の場合にのみ適用されます。
状態 (State)	トランスフォーメーション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。

設定するトランスフォームをクリックします (または[新規 (New)] をクリックして新しいトランスフォーメーションを作成するか、[削除 (Delete)] をクリックしてトランスフォーメーションを削除します)。

## 検索とゾーン変換プロセス

検索とゾーントランスフォーメーションのプロセスは、すべての[検索前トランスフォーメーション](#)について、[コールポリシー](#)について、および[ユーザポリシー](#)が適用された後に適用されます。

そのプロセスは次のとおりです。

- Expressway はプライオリティの順序で適用され (プライオリティ 1 のすべてのルールが最初に処理されてから、プライオリティ 2 以降のルールが処理されます)、指定したエアリアスがクエリの [ソース (Source)] ルールの [モード (Mode)] に基づいてルールの条件に一致しているかどうかを確認します。
- 照合が成功すると、関連付けられたゾーントランスフォーメーションがエアリアスに適用されます ([モード (Mode)] が [エイリアスパターンマッチ (Alias pattern match)] で、[パターン動作 (Pattern behavior)] が [置換 (Replace)] または [除去 (Strip)] の場合)。
- 検索ルールのターゲットのゾーンまたはポリシーサービスは、着信コール要求と同じプロトコル (SIP または H.323) を使用して (ゾーントランスフォーメーションが適用されている場合は変更されたエアリアスを使用して) 照会されます。



(注) 同じプライオリティ レベルの複数のルールで多くの照合に成功した場合、該当するすべてのターゲットが照会されます。

- エイリアスが検出された場合、コールはそのゾーンに転送されます。エイリアスが複数のゾーンで検出された場合、最初に応答したゾーンにコールが転送されます。

- ネイティブの protokol を使用してエイリアスが検出されない場合は、[インターワーキングモード (interworking mode)] SIP および H.323 のインターワーキングの設定に応じてインターワーキングしている protokol を使用してクエリが繰り返されます。
  - 検索で新しい URI またはエイリアスが返された場合 (ENUM ルックアップやポリシーサービスの応答などによる)、**コールルーティングプロセス**が再度開始されます。
4. エイリアスが検出されなかった場合、プライオリティが次に高い検索ルールが次のことが発生するまで、適用されます (ステップ 1 に戻ります)。
- エイリアスが検出されるか、または
  - 特定の条件を満たす検索ルールに関連付けられたすべてのターゲットゾーンまたはポリシーサービスが照会された、あるいは
  - 正常な一致がある検索ルールの **[正常に一致する場合 (On successful match)]** が **[検索の停止 (Stop searching)]** に設定されている



- (注) 正常な一致 (エイリアスが検索ルール条件に一致する場合) と検出するエイリアス (ターゲットゾーンに送信されたクエリに成功した場合) との違い。[検索の停止 (Stop searching)] オプションは、ネットワークのシグナリングインフラストラクチャの制御を向上させます。たとえば、特定のドメインの検索を常に特定のゾーンにルーティングしなければならない場合、このオプションを使用すると、検索プロセスの効率が向上し、Expressway がほかのゾーンを不必要に検索しなくなります。

## 検索ルールの設定

「検索ルール (Search rules)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)]) を使用して、Expressway による適切なターゲットゾーン (ローカルゾーンを含む) またはポリシーサービスへの着信検索要求のルーティング方法を設定します。

このページには、現在設定されているすべての検索ルールが表示されるため、ルールの作成、編集、削除、および有効化と無効化が行えます。列の見出しをクリックすると、**ターゲット別** または **プライオリティ別** にリストを並べ替えることができます。検索ルール上にマウスポインタを置くと、ルールの説明 (定義されている場合) がツールチップとして表示されます。

また、既存の検索ルールは、[アクション (Actions)] 列の [クローン (Clone)] をクリックすると、コピーしてから編集することもできます。

最大 2000 の検索ルールを設定できます。プライオリティ 1 の検索ルールが最初に適用され、次にプライオリティ 2 のすべての検索ルールが適用されます。

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 (Description)	使用方法のヒント
ルール名 (Rule Name)	検索ルールの記述名。	
説明 (Description)	検索ルールの任意の自由形式の説明。	リストのルールの上にマウス ポインタを置いた場合に説明がツールチップとして表示されます。
優先度	他の検索ルールのプライオリティと比較したときに、このルールを適用する検索プロセスの順序。プライオリティ1のすべてのルールが最初に適用され、次にプライオリティ2のすべてのルールが適用されます。複数のルールに同じプライオリティを割り当てることができます。この場合、照合するターゲットゾーンは同時に照会されます。デフォルトは100です。	デフォルト設定では、すべてのエイリアスについてローカルゾーンが最初に検索されます。ローカルでエイリアスが検出されなかった場合、すべてのネイバー、トラバースルクライアントおよびトラバースルサーバが検索されます。エイリアスが検出されなかった場合は、DNSゾーンとENUMゾーンに要求が送信されます。
プロトコル (Protocol)	ルールを適用するソースプロトコル。オプションは[いずれか (Any)]、[H.323]または[SIP]です。	
トラフィックタイプ (Traffic type)	このルールを適用するソーストラフィックタイプ。オプションは次のとおりです。 [いずれか (Any)] : ルールではトラフィックタイプを検査しません。 [標準 (Standard)] : ルールはトラフィックが標準ベースのSIPの場合に適用されます。 [いずれかの Microsoft (Any Microsoft)] : ルールはトラフィックがMicrosoft SIPまたはMicrosoft SIP-SIMPLEの場合に適用されます。 [Microsoft SIP] : ルールはトラフィックがMicrosoft SIPの場合に適用されます。 [Microsoft IM および Presence (Microsoft IM and Presence)] : ルールはトラフィックがMicrosoft SIP-SIMPLEの場合に適用されます。	このオプションにより、異なるタイプのコールをその処理に最適なインフラストラクチャにルーティングできます。  たとえば、2つの検索ルールを使用して、標準のSIPをUnified CMのネイバーゾーンヘルレーティングし、任意のMicrosoft SIPをCisco Meeting Serverのネイバーゾーンヘルレーティングできます。

フィールド	説明 (Description)	使用方法のヒント
ソース (Source)	このルールを適用する要求のソース。 [いずれか (Any) ]: ローカル登録されたデバイス、ネイバーまたはトラバーサルゾーン、および登録されていないデバイス。 [All Zones]: ローカルに登録されたデバイスとネイバーまたはトラバーサルゾーン。 [ローカルゾーン (Local Zone) ]: ローカル登録されたデバイスのみ。 [指定 (Named) ]: ルールを適用する特定のソースゾーンまたはサブゾーン。	指定ソースは、特定のサブゾーンとゾーンのダイヤルプランポリシーとして適用する検索ルールの機能を作成します。
ソース名 (Source name)	ルールを適用する特定のソースゾーンまたはサブゾーン。デフォルトゾーン、デフォルトサブゾーン、あるいはその他の設定済みのゾーンまたはサブゾーンを選択します。	[ソース (Source) ]が [指定 (Named) ]に設定されている場合にのみ適用されます。
要求に認証が必要 (Request must be authenticated)	検索ルールを認証された検索要求にのみ適用するかどうかを指定します。	これを Expressway の <a href="#">認証ポリシー</a> と併用して、認証されていないデバイスが使用可能な一連のサービスを制限できます。
モード (Mode)	エイリアスを検索ルールに適用するかどうかをテストするための方法。 [エイリアスパターンマッチ (Alias pattern match) ]: エイリアスは、指定された [パターンタイプ (Pattern type) ]と [パターン文字列 (Pattern string) ]に一致する必要があります。 [任意のエイリアス (Any alias) ]: (IP アドレスでない限り) どのエイリアスでもかまいません。 [任意の IP アドレス (Any IP Address) ]: エイリアスは IP アドレスである必要があります。	

フィールド	説明 (Description)	使用方法のヒント
パターンタイプ (Pattern type)	<p>適用するルールで、パターン文字列をどのようにエイリアスと照合するか。次のオプションがあります。</p> <p>[完全一致 (Exact) ]: 文字列全体がエイリアスと1文字も違うことなく完全に一致する必要があります。</p> <p>[プレフィックス (Prefix) ]: 文字列がエイリアスの先頭に表示される必要があります。</p> <p>Suffix: 文字列がエイリアスの末尾に表示される必要があります。</p> <p>[正規表現 (Regex) ]: 文字列を正規表現として処理します。</p>	<p>[モード (Mode) ]が [エイリアスパターンマッチ (Alias Pattern Match) ]である場合にのみ適用されます。</p> <p>パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、[パターンの確認 (Check pattern) ]ツール ([メンテナンス (Maintenance) ]&gt; [ツール (Tools) ]&gt; [パターンの確認 (Check pattern) ]) を使用してテストできます。</p>
パターン文字列 (Pattern string)	<p>エイリアスと比較するパターン。</p>	<p>[モード (Mode) ]が [エイリアスパターンマッチ (Alias Pattern Match) ]である場合にのみ適用されます。</p> <p>Expressway には、特定の設定要素との照合に使用できる、事前に設定された一連の <a href="#">パターンマッチング変数</a> が備わっています。</p>
パターン動作 (Pattern behavior)	<p>ターゲットゾーンまたはポリシーサービスに送信する前に、エイリアスの一致した部分を変更するかどうかを決定します。</p> <p>Leave: エイリアスは変更されません。</p> <p>Strip: 一致するプレフィックスまたはサフィックスをエイリアスから削除します。</p> <p>Replace: エイリアスの一致部分が [置換文字列 (Replace string) ] のテキストで置き換えられます。</p>	<p>[モード (Mode) ]が [エイリアスパターンマッチ (Alias Pattern Match) ]である場合にのみ適用されます。</p> <p>検索ルールの適用前にエイリアスを変換する場合は、<a href="#">検索前トランスフォーメーションについて</a> を使用します。</p>
文字列の置換 (Replace string)	<p>パターンに一致するエイリアスの部分を置き換える文字列</p>	<p>[パターン動作 (Pattern behavior) ]が [置換 (Replace) ]の場合にのみ適用されます。</p> <p>正規表現を使用できます。</p>



フィールド	説明 (Description)	使用方法のヒント
正常に一致する場合 (On successful match)	<p>エイリアスが検索ルールに一致する場合の進行中の検索動作を制御します。</p> <p><i>Continue</i> : エイリアスが特定したエンドポイントが検出されるまで、残りの検索ルールを (プライオリティ順に) 適用します。</p> <p><i>Stop</i> : エイリアスで特定されたエンドポイントがターゲットゾーンで検出されない場合でも、これ以上は検索ルールを適用しません。</p>	<p>[停止 (Stop)] を選択した場合、このルールと同じプライオリティのルールは適用されます。</p>
ターゲット (Target)	<p>エイリアスが検索ルールと一致するかどうかを照会するゾーンまたはポリシー サービス。</p>	<p>検索ルールのターゲットとして使用するよう外部外部サービスを使用するための検索ルールの設定を設定できます。たとえば、外部サービスや TelePresence Conductor などのアプリケーションをコールアウトするために使用できます。サービスは、検索プロセスをもう一度開始する新しい宛先エイリアスを指定するなど、一部の CPL を返します。</p>
状態 (State)	<p>検索ルールが有効になっているかどうかを示します。</p>	<p>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。</p>

設定するルールをクリックします (または[新規 (New)] をクリックして新しいルールを作成するか、[削除 (Delete)] をクリックしてルールを削除します)。

#### 検索ルールを設定を支援する便利なツール

- エンドポイントに実際に発信せずに、指定したエイリアスにより特定したエンドポイント Expressway が検出できるかどうかは、[検索 (Locate)] ツール ([メンテナンス (Maintenance)] > [ツール (Tools)] > [検索 (Locate)]) でテストできます。
- パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、[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。

## 検索とトランスフォーメーションの例

検索前のトランスフォーメーションと検索ルールは別々にも一緒にも使用できます。また、[任意のエイリアス (Any alias)] モードと [エイリアスパターンマッチ (Alias pattern match)] モードの組み合わせを使用する複数の検索ルールを定義することも、各ルールに同じプライオリティや別のプライオリティを適用することもできます。これによって、ターゲットゾーンをいつどのような場合に照会するか、およびトランスフォーメーションを適用するかどうかを決定する際に柔軟に対応できるようになります。

ここでは、導入環境における特定の使用例を解決するために検索前トランスフォーメーションや検索ルールをどのように使用できるかについて次の例を示します。

### ゾーンへのクエリの変換なしのフィルタリング

特定の条件に一致するエイリアスのみを照会するように、ゾーンに送信する検索要求をフィルタリングできます。たとえば、地域の営業オフィスのすべてのエンドポイントがサフィックスの @sales.example.com を使用してローカルの Cisco VCS に登録されているとします。この場合は、本社の Expressway にはサフィックスの @sales.example.com を持つエイリアスに対する検索要求を受信したときのみ、営業オフィスの VCS を照会することが適切です。別の検索要求をこの特定の VCS に送信するとリソースを不必要に消費することになります。また、このパターンに一致するエイリアスに対する検索要求を別のゾーンに送信してもリソースが無駄になります（これらのエイリアスに適用される、プライオリティの低い検索ルールも定義されている場合があります）。その場合、[正常に一致する場合 (On successful match)] を [停止 (Stop)] に設定すると、Expressway はそれ以上の（プライオリティの低い）検索ルールを適用しません。

上記の例を実現するには、本社の Expressway で営業オフィスの VCS を表すゾーンを作成し、「検索ルールの作成 (Create search rule)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) から関連する検索ルールを次のようにセットアップします。

フィールド	値
ルール名 (Rule Name)	地域営業オフィス (Regional sales office)
説明 (Description)	サフィックスが @sales.example.com のエイリアスをコールする (Calls to aliases with a suffix of @sales.example.com)
優先度	100
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)

フィールド	値
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	サフィックス (Suffix)
パターン文字列 (Pattern string)	@sales.example.com
パターン動作 (Pattern behavior)	変更なし (Leave)
正常に一致する場合 (On successful match)	停止 (Stop)
ターゲット (Target)	営業オフィス (Sales office)
状態 (State)	有効 (Enabled)

## 常に元のエイリアス（変換なし）でゾーンを照会する

元のエイリアスを使用して検索要求が送信されるようにゾーンを設定するには、「検索ルールの作成 (Create search rule)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) に [任意のエイリアス (Any alias)] のモードを使用してそのゾーンに検索ルールをセットアップします。

フィールド	値
ルール名 Rule Name)	常に元のエイリアスを使用して照会する (Always query with original alias)
説明 (Description)	元のエイリアスを使用して検索要求を送信する (Send search requests using the original alias)
優先度	100
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	任意のエイリアス (Any alias)
正常に一致する場合 (On successful match)	続行 (Continue)
ターゲット (Target)	本社 (Head office)
状態 (State)	有効 (Enabled)

## 変換されたエイリアスに関するゾーンの照会



- (注) エイリアスモードではエイリアス変換がサポートされません。受信した異なるエイリアスを使用してゾーンを常に照会する場合は、モードを [エイリアスのパターン マッチ (Alias pattern match)] にして正規表現と組み合わせて使用する必要があります。

ユーザが **name@example.com** の形式のエイリアスをダイヤルしたときに、Expressway が代わりに **name@example.co.uk** についてゾーンを照会するようにダイヤルプランを設定できます。

これを行うには、[検索ルールの作成 (Create search rule)] ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) から検索ルールを次のようにセットアップします。

フィールド	値
ルール名 (Rule Name)	example.co.uk へ変換 (Transform to example.co.uk)
説明 (Description)	example.com から example.co.uk へ変換 (Transform example.com to example.co.uk)
優先度	100
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターン マッチ (Alias pattern match)
パターン タイプ (Pattern type)	サフィックス (Suffix)
パターン文字列 (Pattern string)	example.com
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	example.co.uk
正常に一致する場合 (On successful match)	続行 (Continue)

フィールド	値
転送先ゾーン (Target zone)	本社 (Head office)
状態 (State)	有効 (Enabled)

## 元のエイリアスと変換後のエイリアスに関するゾーンの照会

変換後のエイリアスをゾーンに照会すると同時に元のエイリアスをゾーンに照会できます。これを行うには、適用するトランスフォーメーションの詳細とともに、[モード (Mode)] を [任意のエイリアス (Any alias)] に設定した検索ルールを1つと、[モード (Mode)] を [エイリアスのパターンマッチ (Alias pattern match)] に設定した検索ルールをもう1つ作成します。両方の検索に同じプライオリティ レベルを指定する必要があります。

たとえば、完全な URI と名前のみ (ドメインを除いた URI) の両方をネイバーゾーンに照会することができます。これを行うには、ローカル Expressway で「検索ルールの作成 (Create search rule)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) から2つの検索ルールを次のようにセットアップします。

### ルール #1

フィールド	値
ルール名 (Rule Name)	海外オフィス - 元のエイリアス (Overseas office - original alias)
説明 (Description)	元のエイリアスを持つ海外オフィスの照会 (Query overseas office with the original alias)
優先度	100
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	任意のエイリアス (Any alias)
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	海外オフィス (Overseas office)

フィールド	値
状態 (State)	有効 (Enabled)

## ルール #2

フィールド	値
ルール名 (Rule Name)	海外オフィス - ドメインの除去 (Overseas office - strip domain)
説明 (Description)	ドメインを除去した海外オフィスの照会 (Query overseas office)
優先度	100
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	サフィックス (Suffix)
パターン文字列 (Pattern string)	@example.com
パターン動作 (Pattern behavior)	除去 (Strip)
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	海外オフィス (Overseas office)
状態 (State)	有効 (Enabled)

## 複数の変換後のエイリアスに関するゾーンの照会

ゾーンに対して設定された検索ルールのプライオリティ順にゾーンが照会されます。

同じゾーンに複数の検索ルールを設定できます。たとえば、照合するプライオリティとパターン文字列は同じにし、置換文字列は異なるものをそれぞれに設定できます。この場合、Expressway は新しいエイリアスのそれぞれについて、そのゾーンを同時に照会します (トランスフォー

メーションによって重複するエイリアスが作成された場合は、検索要求が送信される前にそれらは削除されます)。新しいエイリアスのいずれかがそのゾーンで検出されると、コールはそのゾーンに転送されます。コールが転送されるエイリアスは、制御システムによって決定されます。

たとえば、ユーザが **name@example.com** 形式のエイリアスをダイヤルしたときに Expressway が **name@example.co.uk** と **name@example.net** の両方について同時にゾーンに照会するようにダイヤルプランを設定できます。

これを行うには、「検索ルールの作成 (Create search rule)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) から 2 つの検索ルールを次のようにセットアップします。

#### ルール #1

フィールド	値
ルール名 (Rule Name)	example.co.uk へ変換 (Transform to example.co.uk)
説明 (Description)	example.com から example.co.uk へ変換 (Transform example.com to example.co.uk)
優先度	100
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	サフィックス (Suffix)
パターン文字列 (Pattern string)	example.com
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	example.co.uk
正常に一致する場合 (On successful match)	続行 (Continue)

フィールド	値
転送先ゾーン (Target zone)	本社 (Head office)
状態 (State)	有効 (Enabled)

## ルール #2

フィールド	値
ルール名 (Rule Name)	example.net へ変換 (Transform to example.net)
説明 (Description)	example.net example.com へ変換
優先度	100
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	サフィックス (Suffix)
パターン文字列 (Pattern string)	example.com
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	example.net
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	本社 (Head office)
状態 (State)	有効 (Enabled)



## H.323 番号へのダイヤリングでの @domain の除去

SIP エンドポイントは URI の形式（たとえば **name@domain**）でのみコールを作成できます。発信者がコールの実行時にドメインを指定しない場合、SIP エンドポイントは自動的に自身のドメインをダイヤルされた番号に追加します。つまり、SIP エンドポイントから **123** をダイヤルすると、**123@domain** が検索されます。ダイヤルする H.323 エンドポイントが **123** と登録されている場合、Expressway はエアリアスの **123@domain** を見つけることができずにコールは失敗します。

1 つの番号を使用して登録した SIP エンドポイントと H.323 エンドポイントの両方が含まれている導入環境の場合、次の**検索前トランスフォーメーション**と**ローカルゾーン**の**検索ルール**をセットアップする必要があります。これらの両方によって、ユーザは SIP エンドポイントと H.323 エンドポイントの両方から、H.323 E.164 番号のみを使用して登録した H.323 エンドポイントにコールできます。

### 検索前トランスフォーメーション

「トランスフォーメーションの作成 (Create transforms)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [トランスフォーメーション (Transforms)] > [新規 (New)]) で、次のようにセットアップします。

フィールド	値
優先度	1
説明 (Description)	数字のみのダイヤル文字列を使用し @domain を追加 (Take any number-only dial string and append @domain)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	(\d+)
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1@domain
状態 (State)	有効 (Enabled)

この検索前トランスフォーメーションでは、数字のみのダイヤル文字列 (**123** など) を使用して、導入環境内のエンドポイントの AOR と URI に使用したドメインを追加します。これによって、SIP エンドポイントと H.323 エンドポイントが発信したコールが同じ URI になるようにします。

## ローカルゾーンの検索ルール

「検索ルールの作成 (Create search rule)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) で2つの新しい検索ルールを次のように作成します。

### ルール #1

フィールド	値
ルール名 (Rule Name)	H.323 番号をダイヤル (Dialing H.323 numbers)
説明 (Description)	number@domain 形式のエイリアスを番号に変換 (Transform aliases in format number@domain to number)
優先度	50
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	(\d+)@domain
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	ローカルゾーン (Local Zone)
状態 (State)	有効 (Enabled)

## ルール #2

フィールド	値
ルール名 (Rule Name)	H.323 番号をダイヤル (Dialing H.323 numbers)
説明 (Description)	エイリアスを変換せずに number@domain をコール (Place calls to number@domain with no alias transform)
優先度	60
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	(\d+)@domain
パターン動作 (Pattern behavior)	変更なし (Leave)
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	ローカルゾーン (Local Zone)
状態 (State)	有効 (Enabled)

これらの検索ルールによって、E.164 番号と完全な URI の両方が確実に検索されるため、エンドポイントが H.323 番号 (**123**) で登録されているか、完全な URI (**123@domain**) で登録されているかに関係なくエンドポイントに到達できます。

- 最初の検索ルールの形式は **number@domain** で、これらが **number** の形式に変換されます。
- エイリアスを実際に **number@domain** の形式で登録したエンドポイントにも確実に到達させるには、プライオリティが低い 2 番目の検索ルールでエイリアスを変換せずに **number@domain** をコールします。

## 英数字の H.323 ID のダイヤル文字列の変換

次に、H.323 番号へのダイヤリングでの @domain の除去に基づく例を示します。この例は数字のみのダイヤル文字列を考慮したのですが、H.323 ID は完全に数字のみである必要はありません。これらの ID には英数字（英字と数字）を含めることができます。

この例は、上記の例と同じモデルに従っています。つまり、[検索前トランスフォーメーション](#)と[ローカルゾーンの検索ルール](#)を使用して、エンドポイントが H.323 ID で登録されているか、完全な URI で登録されているかにかかわらず到達できるようにしています。ただし、英数字をサポートする別の正規表現を使用しています。

### 検索前トランスフォーメーション

「トランスフォーメーションの作成 (Create transforms)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [トランスフォーメーション (Transforms)] > [新規 (New)]) で、次のようにセットアップします。

フィールド	値
優先度	1
説明 (Description)	英数字のダイヤル文字列に @domain を追加 (Append @domain to any alphanumeric dial string)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	([^\@]*)
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1@domain
状態 (State)	有効 (Enabled)

この検索前の変換は英数字のダイヤル文字列 (123abc) を使用し、導入環境に使用されているドメインを追加することで、SIP のエンドポイントと H.323 のエンドポイントによって行われたコールが同じ URI になることを保証します。

### ローカルゾーンの検索ルール

「検索ルールの作成 (Create search rule)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) で 2 つの新しい検索ルールを次のように作成します。

## ルール #1

フィールド	値
ルール名 (Rule Name)	H.323 文字列をダイヤル (Dialing H.323 strings)
説明 (Description)	string@domain 形式のエイリアスを文字列に変換 (Transform aliases in format string@domain to string)
優先度	40
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	(.+@domain
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	ローカルゾーン (Local Zone)
状態 (State)	有効 (Enabled)

## ルール #2

フィールド	値
ルール名 (Rule Name)	ドメインを使用した H.323 文字列をダイヤル (Dialing H.323 strings with domain)
説明 (Description)	エイリアスを変換せずに string@domain をコール (Place calls to string@domain with no alias transform)

フィールド	値
優先度	50
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターン マッチ (Alias pattern match)
パターン タイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	(.+)@domain
パターン動作 (Pattern behavior)	変更なし (Leave)
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	ローカルゾーン (Local Zone)
状態 (State)	有効 (Enabled)

これらの検索ルールによって、E.164 番号と完全な URI の両方が確実に検索されるため、エンドポイントが H.323 ID (**123abc**) で登録されているか、完全な URI (**123abc@domain**) で登録されているかに関係なくエンドポイントに到達できます。

- 最初の検索ルールでは **string@domain** 形式のエイリアスを取り、それらを **string** の形式に変換します。
- エイリアスを実際に **string@domain** の形式で登録したエンドポイントにも確実に到達させるには、プライオリティが低い 2 番目の検索ルールでエイリアスを変換せずに **string@domain** をコールします。

## 既知のゾーンから着信した場合にのみ IP アドレスへのコールを許可

エイリアスへのコールの他に、指定した IP アドレスにコールを発信することができます。このようなコールを適切なターゲットゾーンまで通過させるには、**[モード (Mode)]** を **[任意の IP アドレス (Any IP address)]** に設定した検索ルールをセットアップする必要があります。セキュリティを強化するには、ルールの **[ソース (Source)]** オプションを **[すべてのゾーン (All zones)]** に設定する必要があります。これにより、設定済みのゾーンまたはローカルゾーンの

いずれかからクエリが発信されている場合、そのクエリはターゲットゾーンにのみ送信されます。

上記に示した例を実現するには、「検索ルールの作成 (Create search rule)」ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) から検索ルールを次のようにセットアップします。

フィールド	値
ルール名 (Rule Name)	既知のゾーンからの IP アドレス (IP addresses from known zones)
説明 (Description)	既知のゾーンからの IP アドレスへのコールのみを許可 (Allow calls to IP addresses only from a known zone)
優先度	100
ソース (Source)	全ゾーン (All zones)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	任意の IP アドレス
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	海外オフィス (Overseas office)
状態 (State)	有効 (Enabled)

## Microsoft SIP コールを Cisco Meeting Server へ転送する

Cisco Meeting Server を使用して Microsoft ユーザがスペース内で会議できるようにする場合、次のような検索ルールを使用して、このタイプの着信コールをミーティングサーバのネイバーゾーンへ転送します。

フィールド	値
ルール名 (Rule Name)	すべて Meeting Server にルーティング (Route all to Meeting Server)
説明 (Description)	すべてのインバウンド MS トラフィックを Meeting Server に送信 (Send all inbound MS traffic to Meeting Server)
優先度	100

フィールド	値
プロトコル (Protocol)	SIP
トラフィックのタイプ (Traffic type)	いずれかの Microsoft (Any Microsoft)
ソース (Source)	任意 (Any)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	任意のエイリアス (Any alias)
正常に一致する場合 (On successful match)	停止 (Stop)
ターゲット (Target)	Cisco Meeting Server
状態 (State)	有効 (Enabled)

## Kari の法律の 911 コール (Expressway をコール制御および PSTN ゲートウェイとして使用)

このセクションでは、Cisco Expressway 経由で直接 911 緊急コールをサポートするダイヤルプランを設定するための推奨事項を提供します。Federal Communications Commission によって義務付けされた「Kari の法律」は、米国内の直通 911 コールをサポートするため、複数回線電話システム (MLTS) を必要とします。つまり、緊急電話をかける人は、プレフィックスやその他の追加の数字をダイヤルする必要もありません。



(注) Expressway は、リッチメディアセッション (RMS) ライセンスを消費せずに 933 および 988 通話をサポートします。これは 911 通話に似ています。

- 933 電話番号：933 サービスは、E911 通話フローをテストするために使用されます。エンドユーザーが 933 にダイヤルすると、E911 データベースに保存されている電話番号とアドレスが再生されます。
- 988 番号：988 サービスは、RMS ライセンスなしで通話を自死防止ホットラインにルーティングするために使用されます。



## Kari の法律が Expressway に適用される時期

Kari の法律は、音声扱います。この法律は、次のすべての条件が適用される場合に、**米国の Expressway 導入に適用**されます。

- Expressway は、呼制御を管理し、緊急コールを Expressway-C に直接登録するエンドポイントを管理しています。
- ゲートウェイは、PSTN コールを有効にする Expressway で設定されます。
- 展開用の PSTN 通話機能には、911 の緊急コールが含まれます。
- 関係するエンドポイントは、PSTN 番号をダイヤルして基本的な音声通話を発信できます。

## はじめる前に

- Cisco Expressway バージョン X12.5.7 以降が必要です。
- 北米番号計画 (INGP) に関する情報を保持している必要があります。
- X12.5.7 から、コールを開始する前に少なくとも 1 つの RMS ライセンスをインストールする通常の要件は、直接 911 コールには適用されません。
- 料金の不正なリスクを最小限に抑えるために、送信元設定には「任意の」ワイルドカードを使用しないようにしてください。
- また、プレフィックスなしで 911 コールをルーティングするように PSTN ゲートウェイを設定する必要があります。
- エンドポイントとは異なる場所にゲートウェイが地理的に広がる導入の場合は、911 コールの実際のルーティング要件と、発信者が自分の場所とは異なる場所の緊急エージェントに接続している可能性があります。

## 検索ルールの設定

[検索ルールの作成 (Create search rule)] ページ ([設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] > [新規 (New)]) で、必要な検索ルールを作成します。このセクションでは、次の導入タイプの例を示します。

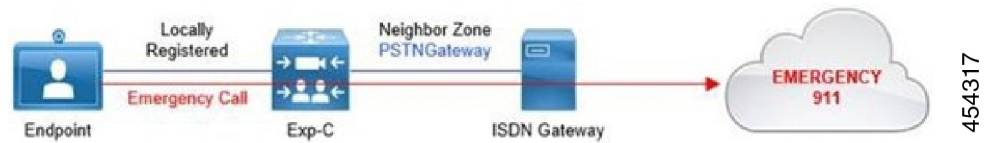
1. スタンドアロン PSTN ゲートウェイ (冗長性なし)
2. 複数の PSTN ゲートウェイ。

## 例 1 : スタンドアロンゲートウェイの検索ルール

これらのルール例は、次のことを前提にしています。

## 例 1 : スタンドアロンゲートウェイの検索ルール

- PSTN コール用の ISDN ゲートウェイは、Expressway 上でネイバゾーン（「PSTNGateway」という名前）として設定されます。
- 911 の緊急コールは、Expressway-C にローカルに登録されている SIP ユーザエージェントまたは H.323 エンドポイントからのみ許可されます。



## 例 1 : ルール #1

フィールド	値
ルール名 (Rule Name)	緊急コール - 911
説明 (Description)	PSTNGateway 経由で 911 緊急コールのルーティング
優先度	1
プロトコル (Protocol)	任意 (Any)
ソース (Source)	ローカルゾーン (Local Zone)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	911 (911@%localdomains%)
パターン動作 (Pattern behavior)	変更なし (Leave)
正常に一致する場合 (On successful match)	停止 (Stop)

フィールド	値
転送先ゾーン (Target zone)	PSTNGateway
状態 (State)	有効

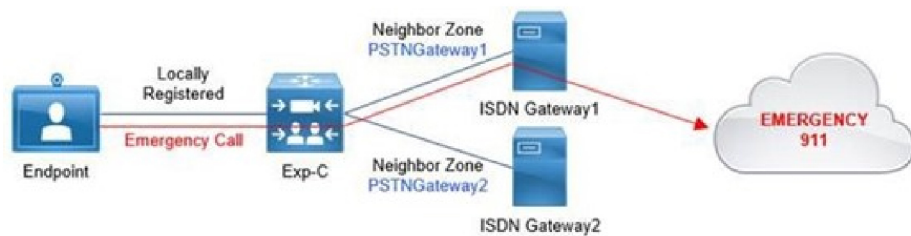
## 例1: ルール #2

フィールド	値
ルール名 (Rule Name)	緊急コール - プレフィックス 00 と 911
説明 (Description)	PSTNGateway 経由で 911 緊急コールのルーティング
優先度	2
プロトコル (Protocol)	任意 (Any)
ソース (Source)	ローカルゾーン (Local Zone)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	00(911 911@%localdomains%)
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1
正常に一致する場合 (On successful match)	停止 (Stop)
転送先ゾーン (Target zone)	PSTNGateway
状態 (State)	有効

## 例 2 : 複数のゲートウェイの検索ルール

これらのルール例は、次のことを前提にしています。

- PSTN コール用の2つの ISDN ゲートウェイを、冗長性を確保するためにライブネットワークで使用できます。
- 各ゲートウェイは、ネイバゾーン（「PSTNGateway1」と「PSTNGateway2」という名前）として Expressway 上で設定されます。
- 911 の緊急コールは、Expressway-C にローカルに登録されている SIP ユーザーエージェントまたは H.323 エンドポイントからのみ許可されます。



454318

ここで、ルールは、プライマリゲートウェイに対して一致に成功した場合 = 「続行」、.backup one に対して *On successful match* = 「停止」を指定します。

### 例 2 : ルール #1

フィールド	値
ルール名 (Rule Name)	緊急コール - PSTNGateway1 経由の 911
説明 (Description)	PSTNGateway 経由で 911 緊急コールのルーティング
優先度	1
プロトコル (Protocol)	任意 (Any)
ソース (Source)	ローカルゾーン (Local Zone)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)

フィールド	値
パターン文字列 (Pattern string)	911 (911@%localdomains%)
パターン動作 (Pattern behavior)	変更なし (Leave)
正常に一致する場合 (On successful match)	続行 (Continue)
転送先ゾーン (Target zone)	PSTNGateway1
状態 (State)	有効

## 例 2 : ルール #2

フィールド	値
ルール名 (Rule Name)	緊急コール - PSTNGateway2 経由の 911
説明 (Description)	PSTNGateway 経由で 911 緊急コールのルーティング
優先度	2
プロトコル (Protocol)	任意 (Any)
ソース (Source)	ローカルゾーン (Local Zone)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターン マッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	911 (911@%localdomains%)
パターン動作 (Pattern behavior)	変更なし (Leave)

## 例 2 : 複数のゲートウェイの検索ルール

フィールド	値
正常に一致する場合 (On successful match)	停止 (Stop)
転送先ゾーン (Target zone)	PSTNGateway2
状態 (State)	有効

## 例 2 : ルール #3

フィールド	値
ルール名 (Rule Name)	緊急コール - PSTNGateway1 経由のプレフィックス 00 で 911
説明 (Description)	PSTNGateway 経由で 911 緊急コールのルーティング
優先度	3
プロトコル (Protocol)	任意 (Any)
ソース (Source)	ローカルゾーン (Local Zone)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	00(911 911@%localdomains%)
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1
正常に一致する場合 (On successful match)	続行 (Continue)

フィールド	値
転送先ゾーン (Target zone)	PSTNGateway1
状態 (State)	有効

## 例2：ルール #4

フィールド	値
ルール名 (Rule Name)	緊急コール - PSTNGateway2 経由のプレフィックス 00 で 911
説明 (Description)	PSTNGateway 経由で 911 緊急コールのルーティング
優先度	4
プロトコル (Protocol)	任意 (Any)
ソース (Source)	ローカルゾーン (Local Zone)
要求に認証が必要 (Request must be authenticated)	いいえ (No)
モード (Mode)	エイリアスのパターンマッチ (Alias pattern match)
パターンタイプ (Pattern type)	正規表現 (Regex)
パターン文字列 (Pattern string)	00(911 911@%localdomains%)
パターン動作 (Pattern behavior)	置換 (Replace)
文字列の置換 (Replace string)	\1
正常に一致する場合 (On successful match)	停止 (Stop)
転送先ゾーン (Target zone)	PSTNGateway2
状態 (State)	有効

## 外部サービスを使用するための検索ルールの設定

検索ルール（ダイヤルプラン）に外部ポリシー サービスを使用するよう Expressway を設定する設定手順は以下のステップに分かれます。

- 検索ルールで使用するポリシー サービスを設定します。
- ポリシー サービスに検索を指定するための関連の検索ルールを設定します。

### 検索ルールが使用するポリシーサービスの構成

ステップ 1 [設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [ポリシー サービス (Policy services)] 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 コールポリシーの場合と同じようにサーバアドレスと接続プロトコルを設定します。

ステップ 4 「ポリシー サービスの作成 (Create policy service)」 ページのフィールドを次のように設定します。

フィールド	説明 (Description)	使用方法のヒント
名前 (Name)	ポリシー サービスの名前。	
説明 (Description)	オプションの自由形式のポリシー サービスの説明。	リストのポリシー サービスの上にマウスポインタを置いた場合に説明がツールチップとして表示されます。
プロトコル (Protocol)	ポリシー サービスに接続するために使用するプロトコル。 デフォルトは <i>HTTPS</i> です。	ポリシー サービス サーバと通信を行う場合、Expressway は HTTP から HTTPS へのリダイレクトを自動的にサポートします。
証明書検証モード (Certificate verification mode)	HTTPS を使用して接続すると、この設定は、ポリシー サーバが提示する証明書を検証するかどうかを制御します。 設定が [オン (On)] の場合、Expressway で HTTPS を使用してポリシー サーバに接続するには、Expressway にそのサーバのサーバ証明書を承認するルート CA 証明書がロードされている必要があります。また、証明書のサブジェクトの共通名またはサブジェクト代替名は次の [サーバアドレス (Server address)] フィールドの 1 つに一致する必要があります。	Expressway のルート CA 証明書は ([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)]) を選択してロードします。



フィールド	説明 (Description)	使用方法のヒント
HTTPS 証明書失効リスト (CRL) による確認 (HTTPS certificate revocation list (CRL) checking)	CRL による確認で証明書を保護する場合は、このオプションを有効にし、手動で CRL ファイルをロードするか、または、自動 CRL 更新を有効にします。	[メンテナンス (Maintenance)] > [セキュリティ (Security)] > [CRL 管理 (CRL management)] に移動して、Expressway が CRL ファイルを更新する方法を設定します。
サーバアドレス 1 ~ 3 (Server address 1 - 3)	サービスをホストしているサーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。アドレスに <b>:&lt;port&gt;</b> を追加することでポートを指定できます。	FQDN を指定する場合は、Expressway に FQDN を解決できる適切な DNS 設定が指定されていることを確認します。  復元力のために、最大 3 つのアドレスを指定できます。
パス (Path)	サーバのサービスの URL を入力します。	
ステータスパス (Status path)	[ステータスパス (Status path)] は、Expressway がリモートサービスのステータスを取得できる場所からのパスを特定します。  デフォルトはステータス (status) です。	ポリシーサーバは戻りステータス情報を提供する必要があります。「 <a href="#">ポリシーサーバのステータスと復元力</a> 」を参照してください。
ユーザ名 (Username)	サービスにログインし、問い合わせするために Expressway が使用するユーザ名。	
パスワード (Password)	サービスにログインし、問い合わせをするために Expressway が使用するパスワード。	プレーンテキストの最大長は 30 文字です (後で暗号化されます)。
デフォルト CPL (Default CPL)	これは、サービスが使用できない場合に Expressway が使用するフォールバック CPL です。	デフォルト CPL を、たとえば、応答サービスまたは録音メッセージにリダイレクトするように変更できます。  詳細については、「 <a href="#">ポリシーサービスのデフォルト CPL</a> 」を参照してください。

ステップ 5 [ポリシー サービスの作成 (Create policy service)] をクリックします。

## ポリシーサービスに検索を指定するための検索ルールの構成

Expressway は、指定したパターンに一致するすべての検索をポリシー サービス サーバに指定します。

最初のエイリアスでは一致し、次にポリシーサーバがコールをルーティングしたエイリアスについては一致しない、または拒否を返信しないように検索ルールを設定する必要があります。

- ステップ1 [設定 (Configuration)] > [ダイヤルプラン (Dial plan)] > [検索ルール (Search rules)] 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 外部ポリシーサーバに指定する検索に応じて、「検索ルールの作成 (Create search rule)」ページのフィールドを設定します。

この例は、.meet で終わっているエイリアスへのコールを外部ポリシーサーバに転送する方法を示しています。

フィールド	値
ルール名 (Rule Name)	ルールを説明する短い名前。
説明 (Description)	フリー形式のルールの説明。
優先度	必要に応じて、10 など。
プロトコル (Protocol)	必要に応じて、[すべて (Any)] などにします。
ソース (Source)	必要に応じて、[すべて (Any)] などにします。
要求に認証が必要 (Request must be authenticated)	この設定は認証ポリシーに従って設定します。
モード (Mode)	必要に応じて、[エイリアスのパターンの一致 (Alias pattern match)] などにします。
パターンタイプ (Pattern type)	必要に応じて、[正規表現 (Regex)] などにします。
パターン文字列 (Pattern string)	必要に応じて、「.*\meet@example.com」などにします。
パターン動作 (Pattern behavior)	必要に応じて、[許可 (Leave)] などにします。
正常に一致する場合 (On successful match)	必要に応じて入力 (注) [停止 (Stop)] が選択された場合、Expressway は元のエイリアスに対して、それ以上検索ルールを処理しませんが、新しいエイリアスが CPL で返される場合は、完全なコール処理シーケンスが再起動されます。
ターゲット (Target)	前の手順で作成したポリシーサービスを選択します。
状態 (State)	有効 (Enabled)

ポリシーサーバにすべての検索を転送するには、どちらもポリシーサービスを対象とする2つの検索ルールを設定できます。

- [モード (Mode)] を [任意のエイリアス (Any alias)] に設定した最初の検索ルール。
- [モード (Mode)] を [すべての IP アドレス (Any IP address)] に設定した 2 番目の検索ルール。

ステップ 4 [検索ルールの作成 (Create search rule)] をクリックします。

## コールポリシーについて

許可するコール、拒否するコール、および別の宛先に転送するコールを制御するルールをセットアップできます。これらのルールをコールポリシー（または管理者ポリシー）と呼びます。

コールポリシーが有効になっており、設定されている場合は、コールが行われるたびに、Expresswayはそのコールの送信元と宛先に基づいて次のことを決定するためにポリシーを実行します。

- 元の宛先へのコールのプロキシ経由での送信します。
- 別の宛先または別の一連の宛先へのコールの転送します。
- 着信を拒否します。



(注) 有効になっている場合、Expressway を通過するすべてのコールにコールポリシーが実行されます。

次の操作を実行する必要があります。

- コールポリシーを使用し、Expressway を介してコールを送受信できる発信者を決定する
- [登録制限ポリシー](#)を使用し、Expressway に登録できるエイリアス、または登録できないエイリアスを決定する

## コールポリシーの設定

「[コールポリシーの設定 \(Call Policy configuration\)](#)」ページ ([[設定 \(Configuration\)](#)] > >[[コールポリシー \(Call Policy\)](#)] > [[設定 \(Configuration\)](#)]) を使用して Expressway の [コールポリシーについて](#) モードを設定し、ローカルポリシーファイルをアップロードします。

## コールポリシーモード

コールポリシーモードは、コールポリシーの設定を Expressway が取得する場所を制御します。次のオプションがあります。

- [ローカル CPL (Local CPL) ]: ローカルで定義したコール ポリシーを使用します。
- [ポリシー サービス (Policy service) ]: 外部ポリシー サービスを使用します。
- [オフ (Off) ]: コール ポリシーを使用しません。

次に、これらのオプションを詳しく説明します。

#### ローカル CPL (Local CPL)

[ローカル CPL (Local CPL) ] オプションでは Expressway 上でローカルに設定されたコール ポリシーを使用します。[ローカル CPL (Local CPL) ] を選択した場合は、次のいずれかを実行する必要があります。

- コールポリシールールページで ([設定 (Configuration) ] > [コールポリシー (Call Policy) ] > [ルール (Rules) ]) ページで、[Web インターフェイスを使用したコール ポリシー ルールの設定](#)します。



(注) これにより、指定したコールのみを許可または拒否できます。

- [CPL スクリプトを使用したコール ポリシーの設定](#)を行います。このファイルには CPL スクリプトが含まれています。ただし、CPL スクリプトの作成は複雑であるため、代わりに外部ポリシーサービスを使用することを推奨します。

コール ポリシーの指定に一度に使用できるのは、これらの 2 つの方法のいずれかのみです。CPL スクリプトがアップロードされている場合は、そのスクリプトが優先されるため、「**コール ポリシー ルール (Call Policy rules)**」ページを使用できません。このページを使用するには、アップロードされている CPL スクリプトを最初に削除する必要があります。

[ローカル CPL (Local CPL) ] が有効になっていても、ポリシーが設定されていないか、またはアップロードされていない場合は、デフォルトのポリシーが適用されます。これにより、送信元や宛先に関係なく、すべてのコールが許可されます。

すべてのコールポリシーの決定を外部サービスに照会する場合は、[ポリシー サービス (Policy service) ] オプションを使用します。このオプションを選択すると、外部サービスの接続の詳細情報を指定できる一連の設定フィールドが新たに表示されます。[外部サービスを使用するためのコール ポリシーの設定](#)を参照してください。

## Web インターフェイスを使用したコール ポリシー ルールの設定

「**コールポリシー ルール (Call Policy rules)**」ページ ([設定 (Configuration) ] > [コールポリシー (Call Policy) ] > [ルール (Rules) ]) には、現在導入されている (CPL ファイル経由でアップロードされたのではなく) Web で設定されたコールポリシー ルールのリストが表示されます。また、このページでは、ルールを作成、編集、削除できます。このページには基本的なコールポリシールールをセットアップするメカニズムが備わっており、CPL スクリプトを作成したりアップロードしたりする必要はありません。

CPL ファイルがすでに導入されている場合は、[コールポリシーールール (Call Policy rules)] ページを使用してコールポリシーを設定できません。この場合は、「コールポリシーの設定 (Call Policy configuration)」ページ ([設定 (Configuration)] > [コールポリシー (Call Policy)] > [設定 (Configuration)]) の [アップロード済みのファイルの削除 (Delete uploaded file)] オプションを使用します。このオプションでCPLスクリプトを使用して導入された既存のポリシーを削除して「コールポリシーールール (Call Policy rules)」ページを使用できるようにし、コールポリシーを設定します。

各ルールで、特定の送信元から特定の宛先エイリアスへのコールに実行するアクションを指定します。複数のルールがある場合は、それらのルールを適用するプライオリティ順に並べ替えることもできます。

コールポリシーールールが設定されていない場合は、デフォルトのポリシーで送信元や宛先に関係なく、すべてのコールが許可されます。

設定するルールをクリックします (または[新規 (New)] をクリックして新しいルールを作成するか、[削除 (Delete)] をクリックして選択したルールを削除します)。

各ルールの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 (Description)	使用方法のヒント
送信元のタイプ (Source type)	このフィールドでは、コールの送信元をゾーンまたは送信元アドレスの2つのタイプから選択できます。この選択は、ルールの設定に使用するそのほかのフィールドに影響します。	異なる送信元のタイプを使用してルールの組み合わせを設定できます。コールポリシーを実装するため、または電話料金の詐欺行為から会議リソースを保護するために、これらを定義し、順序付けます。
発信側ゾーン (Originating Zone)	[送信元のタイプ (Source type)] が [ゾーン (Zone)] に設定されたルールに対してのみ表示されます。  ドロップダウンには、この Expressway に設定されたすべてのゾーンが表示されるため、このルールによって検査されたコールの送信元を選択できます。  ルールは、選択されたゾーンから発信されるすべてのコールを検査します。	

フィールド	説明 (Description)	使用方法のヒント
ルールの適用先 (Rule applies to)	<p>[送信元のタイプ (Source type)] が [送信元アドレス (From address)] に設定されたルールに対してのみ表示されます。</p> <p>このフィールドでは、ルールが認証済みの発信者または非認証の発信者からのコールを検査するかどうかを選択できます。</p> <p>認証済みの発信者は次のデバイスです。</p> <ul style="list-style-type: none"> <li>Expressway にローカルに登録され、認証されている、または</li> <li>ネイバーに登録され、認証されてから、ローカル Expressway に認証されている</li> </ul>	<p>詳細については、「<a href="#">デバイス認証について</a>」を参照してください。</p>
送信元パターン (Source pattern)	<p>[送信元のタイプ (Source type)] が [送信元アドレス (From address)] に設定されたルールに対してのみ表示されます。</p> <p>ルールは、このフィールドへの入力値と、発信側エンドポイントが自身を特定するために使用する送信元アドレスの一致を試みます。</p> <p>このフィールドが空白の場合、ポリシールールは、選択した発信者のタイプ (認証済みまたは非認証) からのすべての着信コールに適用されます。</p>	<p>より一般的なルール用のパターンを使用する、または明示的に特定の発信者を許可または拒否する必要がある場合には1つのエイリアス用のパターンを使用することができます。</p> <p>このフィールドは、<a href="#">正規表現</a>をサポートします。</p>
宛先パターン (Destination pattern)	<p>すべてのルールに必要です。</p> <p>ルールは、このフィールドへの入力値と、着信コールからの宛先アドレスの一致を試みます。</p>	<p>より一般的なルール用のパターンを使用する、または明示的に特定の宛先を許可または拒否する必要がある場合には1つのエイリアス用のパターンを使用することができます。</p> <p>このフィールドは、<a href="#">正規表現</a>をサポートします。</p>

フィールド	説明 (Description)	使用方法のヒント
アクション (Action)	<p>検査したコールが、送信元と宛先に指定したものと一致したときの、ルール動作を定義します。[許可 (Allow)] または [却下 (Reject)] を選択できます。</p> <p>[許可 (Allow)] : 送信元アドレスまたは発信側ゾーンがルールのソースパラメータと一致した場合、およびコールの宛先がルールの宛先パターンに一致した場合、Expressway はコールを処理し続けます。</p> <p>[却下 (Reject)] : 送信元アドレスまたは発信側ゾーンがルールのソースパラメータと一致した場合、およびコールの宛先がルールの宛先パターンに一致した場合、Expressway はコールを拒否します。</p>	
並べ替え (Rearrange)	<p>このフィールドは、通話ポリシールールのリストでのみ表示されます ([通話ポリシールール (Call Policy rules)] ページ)。</p> <p>ルールの順序を変更し、相対的な優先順位を変更するには、↑ および ↓ アイコンをクリックします。</p>	<p>各ルールは、コールに一致するまで、上から順に着信コールの詳細と比較されます。</p> <p>ルールが一致すると、ルールのアクションがコールに適用されます。</p>

## CPL スクリプトを使用したコールポリシーの設定

高度なコールポリシーを設定するには、CPL スクリプトを使用します。これを行うには、まず、CPL スクリプトをテキストファイルとして作成して保存し、その後で Expressway にアップロードします。ただし、CPL スクリプトの記述は複雑なため、代わりに外部ポリシーサービスを使用することを推奨します。

Expressway でサポートされている CPL 構文とコマンドについては、「[CPL リファレンス](#)」のセクションを参照してください。

### 既存の CPL スクリプトの表示

XML ベースの CPL スクリプトとして現在導入されているコールポリシーを表示するには、[コールポリシーの設定](#) ページ ([設定 (Configuration)] > [コールポリシー (Call Policy)] > [設定 (Configuration)]) に移動し、[コールポリシーファイルの表示 (Show Call Policy file)] をクリックします。

- CPL スクリプトを使用するようにコールポリシーを設定した場合は、アップロードしたスクリプトが表示されます。

- 「コール ポリシー ルール (Call Policy rules)」 ページでコール ポリシーを設定した場合は、CPL バージョンのコール ポリシー ルールが表示されます。
- 「コール ポリシー モード (Call Policy mode)」 が [オン (On)] になっていてもポリシーが設定されていない場合は、すべてのコールを許可するデフォルトの CPL スクリプトが表示されます。

コール ポリシーのバックアップ コピーを取得するファイルを表示したり、コール ポリシーが [コール ポリシー ルール (Call Policy rules)] ページを使用して設定されている場合は、この CPL ファイルのコピーを取得し、より高度な CPL スクリプトを作成するための開始点として使用できます。

コール ポリシーを「コール ポリシー ルール (Call Policy rules)」 ページを使用して設定した後に、CPL ファイルをダウンロードした後に編集せずに Expressway へアップロードした場合は、Expressway がそのファイルを認識して、各ルールを「コール ポリシー ルール (Call Policy rules)」 ページに自動的に追加します。

## CPL XSD ファイルについて

CPL スクリプトは Expressway によってサポートされている形式である必要があります。「コール ポリシーの設定 (Call Policy configuration)」 ページでは、Expressway へアップロードしたスクリプトの確認に使用する XML スキーマをダウンロードできます。XSD ファイルを使用して、CPL スクリプトが有効であることを事前に確認できます。2つのダウンロードオプションから選択できます。

- [CPL XSD ファイルの表示 (Show CPL XSD file)] : CPL スクリプトが使用する XML スキーマをブラウザに表示します。
- [CPL 拡張 XSD ファイルの表示 (Show CPL Extensions XSD file)] : Expressway がサポートする追加の CPL 要素に使用する XML スキーマをブラウザに表示します。

## CPL スクリプトのアップロード

CPL スクリプトの Expressway ポールは 5 秒ごとに変更されます。そのため、Expressway はほぼ即時にアップロードされた CPL スクリプトの使用を開始します。CPL スクリプトはコマンドライン インターフェイスを使用してアップロードできません。新しい CPL ファイルをアップロードするには、次の手順を実行します。

- 
- ステップ 1 [設定 (Configuration)] > [コールポリシー (Call Policy)] > [設定 (Configuration)] に移動します。
  - ステップ 2 [ポリシー ファイル (Policy files)] セクションの [新しいコール ポリシー ファイルの選択 (Select the new Call Policy file)] フィールドで、ファイル名を入力するか、アップロードする CPL スクリプトを参照します。
  - ステップ 3 [ファイルのアップロード (Upload file)] をクリックします。
-



## 既存の CPL スクリプトの削除

CPL スクリプトがすでにアップロードされている場合は [アップロード済みのファイルの削除 (Delete uploaded file)] ボタンが表示されます。ファイルを削除するには、そのボタンをクリックします。

## 外部サービスを使用するためのコールポリシーの設定

すべてのポリシー決定を外部サービスに委託するようコールポリシーを設定するには、次の手順を実行します。

ステップ1 [設定 (Configuration)] > [コールポリシー (Call Policy)] > [設定 (Configuration)] に移動します。

ステップ2 [コールポリシーモード (Call Policy mode)] に [ポリシーサービス (Policy service)] を選択します。

ステップ3 フィールドの設定は以下のとおりです。

フィールド	説明 (Description)	使用方法のヒント
プロトコル (Protocol)	ポリシーサービスに接続するために使用するプロトコル。 デフォルトは <i>HTTPS</i> です。	ポリシーサービスサーバと通信を行う場合、Expressway は HTTP から HTTPS へのリダイレクトを自動的にサポートします。
証明書検証モード (Certificate verification mode)	HTTPS を使用して接続すると、この設定は、ポリシーサーバが提示する証明書を検証するかどうかを制御します。 設定が [オン (On)] の場合、Expressway で HTTPS を使用してポリシーサーバに接続するには、Expressway にそのサーバのサーバ証明書を承認するルート CA 証明書がロードされている必要があります。また、証明書のサブジェクトの共通名またはサブジェクト代替名は次の [サーバアドレス (Server address)] フィールドの 1 つに一致する必要があります。	Expressway のルート CA 証明書は ([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)]) を選択してロードします。
HTTPS 証明書失効リスト (CRL) による確認 (HTTPS certificate revocation list (CRL) checking)	CRL による確認で証明書を保護する場合は、このオプションを有効にし、手動で CRL ファイルをロードするか、または、自動 CRL 更新を有効にします。	[メンテナンス (Maintenance)] > [セキュリティ (Security)] > [CRL 管理 (CRL management)] に移動して、Expressway が CRL ファイルを更新する方法を設定します。

フィールド	説明 (Description)	使用方法のヒント
サーバアドレス 1 ~ 3 (Server address 1 - 3)	サービスをホストしているサーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。アドレスに <b>:&lt;port&gt;</b> を追加することでポートを指定できます。	FQDN を指定する場合は、Expressway に FQDN を解決できる適切な DNS 設定が指定されていることを確認します。  復元力のために、最大 3 つのアドレスを指定できます。
パス (Path)	サーバのサービスの URL を入力します。	
ステータスパス (Status path)	[ステータスパス (Status path)] は、Expressway がリモートサービスのステータスを取得できる場所からのパスを特定します。  デフォルトはステータス (status) です。	ポリシーサーバは戻りステータス情報を提供する必要があります。「 <a href="#">ポリシーサーバのステータスと復元力</a> 」を参照してください。
ユーザ名 (Username)	サービスにログインし、問い合わせするために Expressway が使用するユーザ名。	
パスワード (Password)	サービスにログインし、問い合わせをするために Expressway が使用するパスワード。	プレーンテキストの最大長は 30 文字です (後で暗号化されます)。
デフォルト CPL (Default CPL)	これは、サービスが使用できない場合に Expressway が使用するフォールバック CPL です。	デフォルト CPL を、たとえば、応答サービスまたは録音メッセージにリダイレクトするように変更できます。  詳細については、「 <a href="#">ポリシーサービスのデフォルト CPL</a> 」を参照してください。

ステップ 4 フィールドの設定は以下のとおりです。

フィールド	説明 (Description)	使用方法のヒント
プロトコル (Protocol)	ポリシーサービスに接続するために使用するプロトコル。  デフォルトは <i>HTTPS</i> です。	ポリシー サービス サーバと通信を行う場合、Expressway は HTTP から HTTPS へのリダイレクトを自動的にサポートします。

フィールド	説明 (Description)	使用方法のヒント
証明書検証モード (Certificate verification mode)	<p>HTTPS を使用して接続すると、この設定は、ポリシーサーバが提示する証明書を検証するかどうかを制御します。</p> <p>設定が [オン (On)] の場合、Expressway で HTTPS を使用してポリシーサーバに接続するには、Expressway にそのサーバのサーバ証明書を承認するルート CA 証明書がロードされている必要があります。また、証明書のサブジェクトの共通名またはサブジェクト代替名は次の [サーバアドレス (Server address)] フィールドの 1 つに一致する必要があります。</p>	Expressway のルート CA 証明書は ([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)]) を選択してロードします。
HTTPS 証明書失効リスト (CRL) による確認 (HTTPS certificate revocation list (CRL) checking)	CRL による確認で証明書を保護する場合は、このオプションを有効にし、手動で CRL ファイルをロードするか、または、自動 CRL 更新を有効にします。	[メンテナンス (Maintenance)] > [セキュリティ (Security)] > [CRL 管理 (CRL management)] に移動して、Expressway が CRL ファイルを更新する方法を設定します。
サーバアドレス 1 ~ 3 (Server address 1 - 3)	サービスをホストしているサーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。アドレスに <b>:&lt;port&gt;</b> を追加することでポートを指定できます。	<p>FQDN を指定する場合は、Expressway に FQDN を解決できる適切な DNS 設定が指定されていることを確認します。</p> <p>復元力のために、最大 3 つのアドレスを指定できます。</p>
パス (Path)	サーバのサービスの URL を入力します。	
ステータスパス (Status path)	<p>[ステータスパス (Status path)] は、Expressway がリモートサービスのステータスを取得できる場所からのパスを特定します。</p> <p>デフォルトはステータス (status) です。</p>	ポリシーサーバは戻りステータス情報を提供する必要があります。「 <a href="#">ポリシーサーバのステータスと復元力</a> 」を参照してください。
ユーザ名 (Username)	サービスにログインし、問い合わせするために Expressway が使用するユーザ名。	
パスワード (Password)	サービスにログインし、問い合わせをするために Expressway が使用するパスワード。	プレーンテキストの最大長は 30 文字です (後で暗号化されます)。

フィールド	説明 (Description)	使用方法のヒント
デフォルト CPL (Default CPL)	これは、サービスが使用できない場合に Expressway が使用するフォールバック CPL です。	デフォルト CPL を、たとえば、応答サービスまたは録音メッセージにリダイレクトするように変更できます。  詳細については、「 <a href="#">ポリシーサービスのデフォルト CPL</a> 」を参照してください。

ステップ 5 [保存 (Save)] をクリックします。

Expressway はポリシー サービス サーバに接続し、コール ポリシーの決定に必要なサービスを使用して開始する必要があります。

接続の問題は、このページに報告されます。このページの下部の[ステータス (Status)] エリアを確認し、追加の情報メッセージを[サーバアドレス (Server address)] フィールドと照合します。

## サポートされているアドレス形式

発信者のエンドポイントを使用して入力する宛先アドレスにはさまざまな形式を使用できますが、これは、宛先エンドポイントを見つけようとしたときに Expressway が従う特定のプロセスに影響します。Expressway でサポートされるアドレス形式は次のとおりです。

- IP アドレス。例：10.44.10.1 または 3ffe:80ee:3706::10:35
- H.323 ID、例えば john.smith または john.smith@example.com



(注) H.323 ID は URI 形式で使用できます。

- E.164 エイリアス。例：441189876432 または 6432
- URI。例：john.smith@example.com
- ENUM。例：441189876432 または 6432

これらのアドレス形式それぞれをサポートするには、Expressway での設定が必要な場合があります。次の表に、それらの設定要件を示します。

## IP アドレスによるダイヤリング

宛先エンドポイントがシステムに登録されていない場合は、IP アドレスによるダイヤリングが必要です。詳細については、[IP アドレスによるダイヤリング](#)の項を参照してください。

## H.323 ID または E.164 エイリアスによるダイヤリング

H.323 ID または E.164 エイリアスを使用してコールするための特別な設定は不要です。

Expressway は通常の [コールルーティングプロセス](#) に従い、トランスフォーメーションを適用してから、検索ルールに従ってローカルゾーンと外部ゾーンでエイリアスを検索します。



- (注) SIP エンドポイントは常に、UIR の形式の AOR を使用して登録されます。インターワーキングを容易にするように、H.323 エンドポイントも必ず URI の形式の H.323 ID を使用して登録することを推奨します。

## H.323 または SIP URI によるダイヤリング

ユーザが URI ダイヤリングを使用してコールを発信するときは、通常 **name@example.com** をダイヤルします。

宛先エンドポイントがローカルに登録されている、またはネイバーシステムに登録されている場合は、コールを発信するために必要な特別な設定はありません。Expressway は通常の [コールルーティングプロセス](#) に従い、トランスフォーメーションを適用してから、検索ルールに従ってローカルゾーンと外部ゾーンでエイリアスを検索します。

宛先エンドポイントがローカルに登録されていない場合、URI ダイヤリングは DNS を使用して宛先エンドポイントを見つけます。DNS を介して URI ダイヤリングをサポートするには、1 つ以上の DNS サーバと 1 つ以上の DNS ゾーンを使用して Expressway を設定する必要があります。

DNS を介した URI ダイヤリング（アウトバウンドとインバウンドの両方）をサポートする Expressway の設定方法の詳細については、[URI ダイヤリングについての項](#)を参照してください。

## ENUM によるダイヤリング

ENUM ダイヤリングでは、そのエンドポイントが異なる形式のエイリアスを使用して登録されていても、E.164 番号（電話番号）にダイヤリングした発信者がエンドポイントに接続できます。E.164 番号が DNS システムによって URI に変換された後に、URI ダイヤリングのルールによりコールが発信されます。

ENUM ダイヤリング機能を使用すると、URI ダイヤリングの柔軟性は保ちながら、コールするために使用するのは番号だけというシンプルさが得られます。これは、発信者がテンキーを使用しているダイヤリングに限られている場合は特に重要です。

Expressway で ENUM ダイヤリングをサポートするには、1 つ以上の DNS サーバと適切な ENUM ゾーンを使用して設定する必要があります。

ENUM ダイヤリング（アウトバウンドとインバウンドの両方）をサポートする Expressway の設定方法の詳細については、「[ENUM ダイヤリングについて](#)」の項を参照してください。

# IP アドレスによるダイヤリング

宛先エンドポイントがシステムに登録されていない場合は、IPアドレスによるダイヤリングが必要です。

宛先エンドポイントが登録されている場合は、IPアドレスを使用してコールすることも可能ですが、エンドポイントがプライベートネット上にあるか、またはファイアウォールの背後にある場合は失敗する場合があります。このため、AOR や H.323 ID など、別のアドレス形式を介して登録されたエンドポイントにコールを発信することを推奨します。同様に、ネットワーク外の発信者が IP アドレスを使用してネットワーク内のエンドポイントと通信しないようにしてください。

## 既知の IP アドレスへのコール

IP アドレスがローカルに登録されたエンドポイントである場合、または Expressway で設定されているいずれかのサブゾーンメンバーシップルールの IP アドレス範囲内にある場合、Expressway はその IP アドレスを「既知」のものとして見なします。

SIP ユーザ エージェント（および H.323 エンドポイント）は、メンバーシップルールに基づき、デフォルトのサブゾーンまたはカスタマイズされたサブゾーンに登録します。インターワーキングのタイミングは、コールフローによって異なります。

SIP IP ダイアルは、常に UDP として扱われるなど、Expressway 上で期待される動作になります。Expressway サーバは次のとおりです。

1. デフォルト サブゾーンからカスタム Subzone1 へのコール -> SIP 間ネイティブ コールに進みます。Subzone1 で登録されているユニットが SIP UDP として登録されていない場合、ネイティブプロトコルは失敗するため、サーバがインターワーキングを行うまでに遅延が発生します。
2. Subzone1 からデフォルト サブゾーンへのコール -> ただちに SIP-to-H.323 インターワーキング コールにフォールバックします。
3. Subzone1 から Subzone1 へのコール -> SIP 間ネイティブ コールに進みます。Subzone1 で登録されているユニットが SIP UDP として登録されていない場合、ネイティブプロトコルは失敗するため、サーバがインターワーキングを行うまでに遅延が発生します。
4. Subzone1 から Subzone2 へのコール -> SIP 間ネイティブ コールに進みます。Subzone2 で登録されているユニットが SIP UDP として登録されていない場合、ネイティブプロトコルは失敗するため、サーバがインターワーキングを行うまでに遅延が発生します。
5. デフォルト サブゾーンからデフォルト サブゾーンへのコール -> ただちに SIP-to-H.323 インターワーキング コールにフォールバックします。

## 不明 IP アドレスへのコール (Calls to unknown IP addresses)

Expressway は IP アドレスによるダイヤリングをサポートしていますが、Expressway がローカルではない IP アドレスにコールを発信することが望ましくない場合もあります。Expressway

の代わりにネイバーにコールを発信させたり、そのようなコールをまったく許可しないようにすることもできます。[不明 IP アドレスへのコール (Calls to unknown IP addresses)] の設定 (「ダイヤルプランの設定」ページ) で、ローカルネットワークがなく、Expressway またはそのネイバーの 1 つに登録されていない IP アドレスに発信されたコールを Expressway がどのように処理するかを設定します。

Expressway は既知の IP アドレスに常にコールを発信しようとします (ローカルゾーンに [任意の IP アドレス (Any IP Address)] の検索ルールがある場合)。

ほかのすべての IP アドレスは「不明」と見なし、[不明 IP アドレスへのコール (Calls to Unknown IP addresses)] の設定に従って Expressway が処理します。

- [直接 (Direct)] : Expressway は、ネイバーに照会することなく、不明 IP アドレスにコールを直接発信しようとします。
- [間接 (Indirect)] : Expressway は通常の検索プロセスに従ってネイバーに、つまり、[任意の IP アドレス (Any IP Address)] モードの検索ルールのターゲットであるゾーンに検索要求を転送します。一致が検出され、ネイバーの設定でその IP アドレスへのコールが許可されている場合は、Expressway はコールをそのネイバーに渡して完了します。これがデフォルトの設定です。
- [オフ (Off)] : Expressway はネイバーのいずれにも直接的にも間接的にもコールを発信しようとしません。

この設定は、ゾーントランスフォーメーションの前、かつ検索前のトランスフォーメーション、コールポリシーまたはユーザポリシーのルールの適用後にコールの宛先アドレスに適用されます。



- (注) コールの制御のほかに、SIP デバイスのプロビジョニングメッセージとプレゼンスメッセージは IP アドレスにルーティングされることから、この設定ではそれらのメッセージの動作も決定します。

### 未登録エンドポイントへのコール発信

登録されていないエンドポイントとは、H.323 ゲートキーパーまたは SIP レジストラに登録されていないデバイスのことです。ほとんどのコールは、このようなシステムに登録されているエンドポイント間で行われますが、未登録エンドポイントへコールを発信する必要がある場合があります。未登録エンドポイントにコールする方法は次の 2 つです。

- URI をダイヤルする。これには、URI ダイヤリングをサポートするようにローカル Expressway を設定し、未登録のエンドポイントの IP アドレスを解決するその URI の DNS レコードが存在している必要があります。
- IP アドレスをダイヤルする。

### ファイアウォールを通過するための推奨設定

ファイアウォールトラバーサルのために Expressway-E が Expressway-C と隣接している場合、通常は、[不明な IP アドレスへのコール (Calls to unknown IP addresses)] を Expressway-C では [間接 (Indirect)] に、Expressway-E では [直接 (Direct)] に設定する必要があります。ファイアウォール内の発信者がファイアウォール外の IP アドレス コールの発信を試みると、次のようにルーティングされます。

1. コールはエンドポイントから、そのエンドポイントが登録されている Expressway-C に進みます。
2. コールされた IP アドレスがその Expressway に登録されておらず、[不明な IP アドレスへのコール (Calls to unknown IP addresses)] の設定が [間接 (Indirect)] であるため、Expressway はコールを直接発信できません。代わりに、この Expressway は隣接する Expressway-E を照会し、そのシステムが Expressway-C の代わりにコールを発信できるかどうかを確認します。トラバーサルサーバゾーンに対して検索ルールを [任意の IP アドレス (Any IP Address)] に設定する必要があります。
3. Expressway-E がコールを受信すると、[不明な IP アドレスへのコール (Calls to unknown IP addresses)] 設定が [直接 (Direct)] であるため、そのコールはコールされた IP アドレスに直接発信されます。

## URI ダイヤリングについて

URI アドレスの形式は通常、**name@example.com** です。ここで、**name** はエイリアス、**example.com** はドメインです。

URI ダイヤリングは DNS を利用して、さまざまなシステムに登録されているエンドポイントを互いに見つけ出せるようにし、コールし合えるようにします。DNS がない場合、エンドポイントを互いに見つけ出せるようにするには、同じシステムまたは隣接するシステムにエンドポイントを登録する必要があります。

## DNS を使用しない URI ダイヤリング

DNS を使用しない場合、URI ダイヤリングを使用してローカルに登録されたエンドポイントが行ったコールは、宛先エンドポイントもローカルに登録されている場合、またはネイバーシステムを介してアクセスできる場合にのみ、発信されます。これらのエンドポイントは、DNS クエリではなく、[検索とゾーン変換プロセス](#)を使用して見つけることができます。

DNS を使用せずにネットワークから URI ダイヤリングを使用する場合、ネットワーク内のすべてのシステムが互いに、直接または間接的ではなく、ネイバー関係で接続されていることを確認する必要があります。これによって、エンドポイントの URI を検索することで、いずれかのシステムがそのシステム自体または他のシステムに登録されているエンドポイントを確実に見つけられるようになります。

これは、システムの数が増えても十分に拡張されません。また、特に実用的でもありません。つまり、ネットワーク内のエンドポイントは、2つのシステム間にネイバー関係がなければ、



そのネットワーク外のシステムに登録されているエンドポイントにはダイヤルできません（別の会社へのコールの発信など）。

DNS ゾーンと DNS サーバがローカル Expressway 上に設定されていない場合、ローカルに登録されていないエンドポイントまたはネイバー システムへのコールは、ローカル Expressway が DNS を介した URI ダイヤリング用に設定された別の Expressway に（直接または間接的に）隣接していれば、発信されます。この場合、そのネイバーゾーンを参照する検索ルールによってピックアップされた URI でダイヤリングされたコールは、そのネイバーを経由し、DNS ルックアップが実行されます。

この設定は、すべての URI ダイヤリングを Expressway-E などの特定の 1 つのシステムを介して実行する場合に役に立ちます。

ネットワーク内での URI ダイヤリングの一環として DNS を使用しない場合は、特別な設定は不要です。エンドポイントが URI 形式のエイリアスを使用して登録され、コールがその URI に対して実行されたときに、Expressway がローカルゾーンとネイバーにその URI について照会します。

Expressway に DNS が設定されておらず、ネットワークに H.323 エンドポイントが含まれている場合、これらのエンドポイントに URI ダイヤリングを使用して到達するには、次のいずれかが必要です。

- H.323 の登録で使用される形式に URI を変換するために適切なトランスフォーメーションを作成する。たとえば、H.323 エンドポイントをエイリアスを使用して登録し、**alias@domain.com** に対して着信コールを実行するという導入方法があります。この場合はローカル トランスフォーメーションを設定して **@domain** を除去し、ローカルで **alias** を検索します。これを実行する方法の例については、[H.323 番号へのダイヤリングでの @domain の除去](#) を参照してください。

SIP エンドポイントは常に URI 形式の AOR で登録されるため、特別な設定は不要です。

## DNS を使用した URI ダイヤリング

URI ダイヤリングの一環として DNS を使用することで、不明なシステムに登録されている可能性がある場合でも、エンドポイントを検出できます。Expressway は DNS ルックアップを使用して URI アドレス内のドメインを見つけ、そのドメインにエイリアスを照会します。詳細については、[DNS を使用した URI の解決プロセス](#)のセクションを参照してください。

DNS を介した URI ダイヤリングは、発信コールと着信コールに別々に有効にできます。

### 発信コール

URI ダイヤリングを使用し、DNS を介して Expressway がエンドポイントを見つけられるようにするには、次の手順を実行します。

- 少なくとも 1 つの DNS ゾーンと関連する検索ルールを設定します。
- 少なくとも 1 つの DNS サーバを設定します。

この詳細については、[発信コールでの DNS を介した URI ダイヤリング](#)のセクションを参照してください。

### 着信コール

Expresswayに登録されているエンドポイントで、ローカルに登録されていないエンドポイントからのコールを URI ダイヤリングを使用し、DNS を介して受信できるようにするには、次の手順を実行します。

- すべてのエンドポイントが AOR (SIP) または URI 形式の H.323 ID で登録されていることを確認する
- 使用するプロトコルとトランスポートタイプとに応じて適切な DNS レコードを設定する

この詳細については、[着信コールでの DNS を介した URI ダイヤリング](#)のセクションを参照してください。

### ファイアウォールトラバーサルコール

URI を使用したコールをファイアウォールを通じて送受信できるようにシステムを設定するには、[URI ダイヤリングとファイアウォールトラバーサル](#)のセクションを参照してください。

## DNS を使用した URI の解決プロセス

Expressway が DNS システムを使用して宛先 URI アドレスを見つけようとする場合の一般的なプロセスは次のとおりです。

### H.323

1. Expressway は URI 内のドメインに関する SRV レコードについて DNS サーバにクエリを送信します (複数の DNS サーバを Expressway に設定している場合、クエリはすべてのサーバに同時に送信されますが、すべての応答は Expressway が使用している SRV レコードで最も関連性の高いもののみを使用して優先順位付けが行われます)。使用可能な場合、この SRV レコードは、デバイス自体や、そのドメインに権限を持つ H.323 ゲートキーパーに関する情報 (FQDN やリスニングポートなど) を返します。
  - URI アドレスのドメインの部分が H.323 ロケーション SRV レコード (`_h323ls` の部分) を使用して正常に解決された場合、Expressway は返された名前レコードごとに A/AAAA レコードクエリを送信します。これらは1つ以上の IP アドレスに解決され、Expressway がそれらの IP アドレスへの完全 URI の LRQ をプライオリティ順に送信します。
  - URI アドレスのドメインの部分が H.323 コールシグナリング SRV レコード (`_h323cs` の部分) を使用して解決された場合、Expressway は返された名前レコードごとに A/AAAA レコードクエリを送信します。これらは1つ以上の IP アドレスに解決され、Expressway がこれらのレコードで返された IP アドレスへプライオリティ順にコールをルーティングします (例外として、`user@example.com:1719` など元のダイヤル文字列

にポートが指定されていない場合があります。この場合、返されるアドレスで完全 URI アドレスが LRQ を介して照会されます)。

2. 関連する SRV レコードが見つからなかった場合は、次のようになります。

- 照会する DNS ゾーンの [アドレス レコードを含める (Include address record)] の設定が [オン (On)] の場合、システムは URI 内のドメインの A レコードまたは AAAA レコードの検索にフォールバックします。このようなレコードが検出された場合、コールはその IP アドレスにルーティングされ、検索が終了します。



(注) このドメイン内で検出された A レコードと AAAA レコードが SIP または H.323 をサポートするシステム以外のものである場合でも、Expressway はこのゾーンにコールを転送するため、コールは失敗します。そのため、デフォルト設定の [オフ (Off)] を使用することを推奨します。

- 照会する DNS ゾーンの [アドレス レコードを含める (Include address record)] の設定が [オフ (Off)] の場合、Expressway は A レコードも AAAA レコードも照会しません。その代わりに検索を続行して、残りの下位のゾーンを照会します。

## SIP

Expressway は、RFC 3263 で説明されているように、SIP 解決プロセスをサポートします。次に、Expressway がこのプロセスを実装する例を示します。

1. Expressway が URI のドメインについての NAPTR クエリを送信します。可能な場合は、そのドメインとの通信に使用する SRV レコードとトランスポート プロトコルの優先順位付けされたリストがこのクエリの結果セットに示されます。NAPTR レコードがこのドメイン名のドメインネームシステム (DNS) に提示されていない場合、Expressway は、NAPTR クエリから返されたかのように、どのドメインの `_sips._tcp.<domain>`、`_sip._tcp.<domain>` and `_sip._udp.<domain>` のデフォルトリストを使用します。
  - Expressway は NAPTR レコードのルックアップから返された結果それぞれに SRV クエリを送信します。返された A/AAAA レコードが優先順位付けられたリストが構築されます。
  - Expressway は、SRV レコードルックアップによって返された名前ごとに A/AAAA レコードクエリを送信します。

上記の手順によって、ターゲット ドメインとの通信に使用される IP アドレス、ポート、およびトランスポート プロトコルのツリーが構築されます。このツリーは NAPTR レコードのプライオリティ、次に SRV レコードのプライオリティによってさらに分割されます。場所のツリーを使用すると、検索プロセスが最初の場所で停止し、ターゲットの宛先と通信したことを示す応答が返されます。

2. 検索プロセスが関連する SRV レコードを返さない場合は次のようになります。

- 照会する DNS ゾーンの [アドレス レコードを含める (Include address record)] の設定が [オン (On)] の場合、システムは URI 内のドメインの A レコードまたは AAAA レコードの検索にフォールバックします。このようなレコードが検出された場合、コールはその IP アドレスにルーティングされ、検索が終了します。



(注) このドメイン内で検出された A レコードと AAAA レコードが SIP または H.323 をサポートするシステム以外のものである場合でも、Expressway はこのゾーンにコールを転送するため、コールは失敗します。そのため、デフォルト設定の [オフ (Off)] を使用することを推奨します。

- 照会する DNS ゾーンの [アドレス レコードを含める (Include address record)] の設定が [オフ (Off)] の場合、Expressway は A レコードも AAAA レコードも照会しません。その代わりに検索を続行して、残りの下位のゾーンを照会します。

## 発信コールでの DNS を介した URI ダイヤリング

ユーザが URI ダイヤリングを使用してコールを発信すると、通常は **name@example.com** の形式でエンドポイントからアドレスをダイヤルします。次に、Expressway に登録されたエンドポイントから URI をダイヤルした場合、またはネイバー システムからクエリとして URI アドレスを受信した場合に従うプロセスを示します。

1. Expressway は [検索ルールの設定](#) をチェックし、それらのルールの [モード (Mode)] が次のいずれかに設定されているかどうかを確認します。
  - [任意のエイリアス (Any alias)] または
  - URI アドレスに一致するパターンの [エイリアスパターンマッチ (Alias pattern match)]
2. 関連付けられたターゲットゾーンで URI がプライオリティ順に照会されます。
  - ターゲットゾーンのいずれかが DNS ゾーンである場合、Expressway は DNS ルックアップを通じてエンドポイントを見つけます。これは、Expressway に設定されている DNS サーバにドメインの場所を [DNS を使用した URI の解決プロセス](#) に従って照会することで実行されます。URI アドレスのドメインの部分が正常に解決されると、それらのアドレスに要求が転送されます。
  - ターゲットゾーンのいずれかがネイバー、トラバーサルクライアント、またはトラバーサルサーバである場合、URI についてそれらのゾーンが照会されます。そのシステムが DNS を介して URI ダイヤリングをサポートする場合、コール自体をルーティングする場合があります。

## DNS ゾーンの追加と設定

DNS を介して URI ダイヤリングを有効にするには、1 つ以上の DNS ゾーンを設定する必要があります。手順は次のとおりです。

**ステップ 1** [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] へ移動します。

**ステップ 2** [新規 (New)] をクリックします。[ゾーンの作成 (Create zone)] ページが表示されます。

**ステップ 3** ゾーンの名前を入力し、[タイプ (Type)] として [DNS] を選択します。

**ステップ 4** DNS ゾーンを次のように設定します。

フィールド	ガイドライン
ホップカウント (Hop count)	<p>DNS を介し、URI を使用してダイヤリングすると、使用されるホップ カウントは、UIR アドレスに一致する検索ルールに関連付けられた DNS ゾーンに対して設定されたものになります (これがコールに現在関連付けられているホップ カウントよりも少ない場合)。</p> <p>URI アドレスが DNS ゾーンと一致しない場合、ネイバーにクエリが送信されます。この場合、使用するホップ カウントは、ネイバーゾーンに対して設定されたものになります (コールに現在関連付けられているホップ カウントよりも小さい場合)。</p>
H.323 と SIP modes	[H.323] セクションと [SIP] セクションでは、コールが SIP または H.323 の SRV ルックアップを使用して見つかるかどうかに基づき、このゾーンを介して見つかったシステムとエンドポイントへのコールをフィルタリングすることができます。
アドレスレコードを含める (Include address record)	<p>この設定によって、このゾーンを介してダイヤルされたエイリアスについての NAPTR (SIP) レコードまたは SRV (SIP と H.323) レコードが検出されなかった場合、Expressway はプライオリティが低いゾーンの照会に移る前に、A および AAAA の DNS レコードを照会します。</p> <p>デフォルト設定の [オフ (Off)] を使用することを推奨します。つまり、Expressway は A レコードと AAAA レコードは照会せず、その代わりに検索を続行して残りのプライオリティが低いゾーンを検索します。これは、NAPTR レコードや SRV レコードとは異なり、A/AAAA レコードが関連する SIP メッセージまたは H.323 メッセージ (LRQ、Setup など) を処理できるシステムを示す保証がないためです。システムが、http メッセージを処理する Web サーバであったり、メール メッセージを処理するメール サーバであったりする可能性があります。システムが A/AAAA ルックアップをしている場合にこの設定が [オン (On)] になっていると、Expressway はその宛先にシグナリングを送信することになり、検索プロセスを続行しません。システムが SIP や H.323 をサポートしない場合、コールは失敗します。</p>
ゾーン プロファイル (Zone profile)	ほとんどの導入環境について、この設定は [デフォルト (Default)] のままにする必要があります。

ステップ5 [ゾーンの作成 (Create zone)] をクリックします。

## DNS ゾーンの設定

ローカル Expressway で DNS を使用し、ネットワーク外のエンドポイントを見つける場合は、次の手順を実行します。

- [ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定](#) (DNS クエリに Expressway が使用するもの)
- DNS ゾーンを作成し、DNS クエリをトリガーするエイリアスを定義するために [パターン文字列 (Pattern string)] フィールドと [パターンタイプ (Pattern type)] フィールドを使用する、関連付けられた検索ルールをセットアップする

たとえば、次のように設定します。

- [パターン文字列 (Pattern string)] に `.*@.*`、[パターンタイプ (Pattern type)] に [正規表現 (Regex)] を設定し、通常の URI アドレスの形式のすべてのエイリアスを DNS に照会する
- [パターン文字列 (Pattern string)] に `(?!.*@example.com$).*`、[パターンタイプ (Pattern type)] に [正規表現 (Regex)] を設定し、ドメイン `example.com` 以外の通常の URI アドレスの形式のすべてのエイリアスを DNS に照会する

さらに詳細なフィルタをセットアップするには、同じ DNS ゾーンをターゲットとする検索ルールを追加して設定します。プロトコル (SIP または H.323) に基づいてフィルタリングしたり、異なるホップカウントを使用したりしない限り、ルールごとに新しい DNS ゾーンを作成する必要はありません。



- (注) DNS ゾーンに対して [モード (Mode)] を [任意のエイリアス (Any alias)] に設定した検索ルールは設定しないでください。このような検索ルールは、ローカルに登録されているものや、URI アドレスの形式でないものも含めてすべてのエイリアスについて DNS が常に照会されることとなります。

## 着信コールでの DNS を介した URI ダイヤリング

### DNS レコードタイプ

URI ダイヤリングを使用し、DNS を介して行われたコール (および登録などのその他のメッセージ) を受信するための Expressway の機能は、Expressway がホストしている各ドメインに DNS レコードがあるかないかに依存します。

これらのレコードには、次のようなさまざまなタイプがあります。

- Expressway の IPv4 アドレスを提供する A レコード

- Expressway の IPv6 アドレスを提供する AAAA レコード
- 特定のプロトコルやトランスポート タイプについて照会される Expressway の FQDN やそのポートを指定するサービス (SRV) レコード
- SIP ドメインの SRV レコードやトランスポートの設定を指定する NAPTR レコード

ホストしているドメインと、Expressway で有効になっているプロトコルおよびトランスポートタイプの組み合わせごとに SRV レコードまたは NAPTR レコードを指定する必要があります。

### 着信コールプロセス

URI ダイヤリングを使用し、DNS を介して着信コールが実行された場合、発信側のシステムは上述の DNS レコードルックアップのいずれかを使用して Expressway を検出しています。

Expressway は、ダイヤルされた `user@example.com` 形式の URI を含む要求を受信します。これは、デフォルトゾーンから着信したように見えます。この場合、Expressway は通常の [コールルーティングプロセス](#) に従って、検索前トランスフォーメーション、コールポリシーと FindMe ポリシーを適用した後、ローカルゾーンとその他の設定済みのゾーンを検索ルールのプライオリティ順に検索して、URI を検索します。

### SRV レコードの形式

SRV レコードの形式は [RFC 2782](#) により、次のように定義されます。

**`_Service._Proto.Name TTL Class SRV Priority Weight Port Target`**

Expressway では、次のようになります。

- **`_Service`** と **`_Proto`** は異なり、使用するプロトコルとトランスポートタイプに依存します。
- **`Name`** は、Expressway がホストしている URI 内のドメイン (**`example.com`**) です。
- **`Port`** はその特定のサービスとプロトコルの組み合わせをリッスンするように設定された Expressway 上の IP ポートです。
- **`Target`** は、Expressway の FQDN です。

## H.323 SRV レコードの設定

『[ITU 仕様書 : H.323](#)』の「Annex O」に、DNS を使用してゲートキーパーとエンドポイントを見つけ、H.323 URL エイリアスを解決する手順が定義されています。また、H.323 URL で使用するパラメータも定義されています。

Expressway はこの付録で定義されている SRV レコードのロケーション、コール、および登録のサービス タイプをサポートします。

### ロケーションサービスの SRV レコード

コールを Expressway にルーティングするゲートキーパーには、ロケーションレコードが必要です。Expressway がホストするドメインごとにロケーションサービスの SRV レコードを次のように設定する必要があります。

- **\_Service** は **\_h323ls**
- **\_Proto** は **\_udp**
- **Port** は、**[設定 (Configuration)] > [プロトコル (Protocols)] > [H.323]** で登録 UDP ポートとして設定したポート番号。

#### コール シグナリングの SRV レコード

コール シグナリングの SRV レコード（および A/AAAA レコード）は、LRQ と LCF を交換するロケーショントランザクションに参加できない未登録のエンドポイントによって主に使用されます。Expressway がホストするドメインごとにコール シグナリングの SRV レコードを次のように設定する必要があります。

- **\_Service** は **\_h323cs**
- **\_Proto** は **\_tcp**
- **Port** は、**[設定 (Configuration)] > [プロトコル (Protocols)] > [H.323]** > として設定したポート番号。

#### 登録サービスの SRV レコード

登録レコードは、Expressway の登録を試行するデバイスが使用します。Expressway がホストするドメインごとに登録サービスの SRV レコードを次のように設定する必要があります。

- **\_Service** は **\_h323rs**
- **\_Proto** は **\_udp**
- **Port** は、**[設定 (Configuration)] > [プロトコル (Protocols)] > [H.323]** で登録 UDP ポートとして設定したポート番号。

## SIP SRV レコードの設定

[RFC 3263](#) に、SIP URI を通信する次のホップの IP アドレス、ポート、トランスポートプロトコルに解決するために使用する DNS のプロシージャが示されています。

SIP URI ダイヤリングを使用して Expressway に接続できるようにするには、Expressway で有効になっている SIP トランスポートプロトコル（UDP、TCP、または TLS）ごとに SRV レコードを次のように設定する必要があります。

- **\_Service** および **\_Proto** の有効な組み合わせは次のとおりです。
  - **\_sips.\_tcp**
  - **\_sip.\_tcp**
  - **\_sip.\_udp**（推奨されていません）
- **Port** はその特定のトランスポートプロトコル用のポートとして **[設定 (Configuration)] > [プロトコル (Protocols)] > [SIP]** で設定した IP ポート番号



**\_sip.\_udp** は、ビデオストリームの SIP メッセージが大きすぎて（ストリームベースでなく）パケットベースの転送では伝送できないため、推奨されません。UDP は、通常、オーディオ専用デバイスに使用されます。また、UDP は TCP や TLS よりもスパムが多発する傾向があります。

## DNS レコードの設定例

ドメイン名を持つ企業は、**example.com** 次の形式の URI アドレスを使用して H.323 および SIP の着信コールを有効にしたいと考えています。**user@example.com** ドメインをホストしている Expressway には、FQDN **expressway.example.com** があります。

通常、DNS レコードは次のようになります。

- **\_h323ls.\_udp.example.com** リターンの SRV レコード **expressway.example.com**
- **\_h323cs.\_tcp.example.com** リターンの SRV レコード **expressway.example.com**
- **\_h323rs.\_tcp.example.com** リターンの SRV レコード **expressway.example.com**
- **example.com** リターンの NAPTR レコード
  - **\_sip.\_tcp.example.com** および
  - **\_sips.\_tcp.example.com**
- **\_sip.\_tcp.example.com** リターンの SRV レコード **expressway.example.com**
- **\_sips.\_tcp.example.com** リターンの SRV レコード **expressway.example.com**
- Expressway の IPv4 アドレスを返す **expressway.example.com** レコード。
- Expressway の IPv6 アドレスを返す **expressway.example.com AAAA** レコード。

DNS レコードの追加方法は、使用している DNS サーバのタイプによって異なります。2 つの共通 DNS サーバをセットアップする手順については、「DNS 設定」の項を参照してください。

URI ダイヤリングを使用してローカルに登録された H.323 エンドポイントに到達するには、次のいずれかを実行します。

- URI 形式のアドレスを使用して H.323 エンドポイントを Expressway に登録する
- H.323 の登録で使用される形式に URI を変換するために適切なトランスフォーメーションを作成する。たとえば、H.323 エンドポイントをエイリアスを使用して登録し、**alias@domain.com** に対して着信コールを実行するという導入方法があります。この場合はローカルトランスフォーメーションを設定して **@domain** を除去し、ローカルで **alias** を検索します。これを実行する方法の例については、[H.323 番号へのダイヤリングでの @domain の除去](#) を参照してください。

SIP エンドポイントは常に URI 形式の AOR で登録されるため、特別な設定は不要です。

Expressway をを見つけるために複数のメカニズムが使用されていた可能性があります。

**user@<IP\_address>** に発信されたコールを **user@example.com** の既存の登録にルーティングできるようにすることができます。この場合は、[検索前トランスフォーメーションについて](#) を設定

して着信 URI からサフィックスの IP\_address を除去して **example.com** のサフィックスで置き換えます。

## URI ダイヤリングとファイアウォールトラバース

DNS を介した URI ダイヤリングをファイアウォールトラバースと一緒に使用する場合、DNS ゾーンを Expressway-E とパブリック ネットワークの Expressway のみに設定する必要があります。ファイアウォールの背後にある Expressway には DNS ゾーンを設定しないでください。これにより、Expressway に登録されているエンドポイントからの発信 URI コールが Expressway-E を通じてルーティングされるようになります。

さらに、着信コールの DNS レコードは、その企業の権限のあるプロキシとして Expressway-E のアドレスを使用して設定する必要があります（詳細については、「DNS 設定例」の項を参照してください）。これにより、URI ダイヤリングを使用して処理された着信コールが Expressway-E を通じて企業内に入るため、ファイアウォールのトラバースが成功するようになります。

## ENUM ダイヤリングについて

ENUM ダイヤリングでは、そのエンドポイントが異なる形式のエイリアスを使用して登録されていても、E.164 番号（電話番号）にダイヤリングした発信者がエンドポイントに接続できます。

ENUM ダイヤリングを使用し、E.164 番号をダイヤルすると、DNS に保存された情報を使用して URI に変換されます。次に Expressway が返された URI に基づいてエンドポイントを検索しようとしています。

ENUM ダイヤリング機能を使用すると、URI ダイヤリングの柔軟性は保ちながら、コールするために使用するのは番号だけというシンプルさが得られます。これは、発信者がテンキーを使用してのダイヤリングに限られている場合は特に重要です。

Expressway 上の ENUM ゾーンを設定できるため、Expressway は発信 ENUM ダイヤリングをサポートします。ENUM ゾーンを照会することによって、ENUM ドメインにダイヤルされ、その後で DNS を使用して照会される E.164 番号の Expressway による変換がトリガーされます。



---

(注) ENUM ダイヤリングは照会される ENUM ドメインの関連する DNS NAPTR レコードの有無に依存します。これは、そのドメインの管理者が担当します。

---

## ENUM ダイヤリング プロセス

Expressway が ENUM を使用してエンドポイントを見つけようとする場合の一般的なプロセスは次のようになります。

1. ユーザがエンドポイントから E.164 番号をダイヤルします。

2. Expressway が E.164 番号を ENUM ドメインに次のように変換します。
  1. 数字を反転し、ドットで区切ります。
  2. E.164 番号の NAPTR レコードをホストするドメインの名前がサフィックスとして追加されます。
3. 次に、結果の ENUM ドメインを DNS に照会します。
4. その ENUM ドメインの NAPTR レコードがある場合は、1 つ（場合によっては複数）の H.323/SIP URI への番号の変換方法が示されます。
5. Expressway が再度検索を開始しますが、ここでは、変換した URI を [発信コールでの DNS を介した URI ダイヤリング](#)に従って検索します。



---

(注) これは、まったく新しい検索と見なすことができるため、検索前トランスフォーメーションとコールポリシーが適用されます。

---

## ENUM ダイヤルの有効化

ENUM ダイヤリングは着信コールと発信コールに別々に有効にできます。

### 発信コール

ENUM を使用するエンドポイントへの発信コールを可能にするには、次の手順を実行する必要があります。

- 少なくとも 1 つの ENUM ゾーンを設定する、および
- 少なくとも 1 つの DNS サーバを設定します。

この詳細については、[発信コールの ENUM ダイヤリング](#)のセクションを参照してください。

### 着信コール

企業内のエンドポイントが ENUM ダイヤリングを介して他のエンドポイントからの着信コールを受信できるようにするには、エンドポイントの E.164 番号を SIP/H.323 URI にマッピングする DNS NAPTR レコードを設定する必要があります。これを実行する方法については、[着信コールの ENUM ダイヤリング](#)セクションを参照してください。



---

(注) ENUM ゾーンと DNS サーバがローカル Expressway 上に設定されていない場合も、ローカル Expressway が ENUM ダイヤリングに適切に設定された別の Expressway と隣接していれば、ENUM ダイヤリングを使用して発信されたコールは処理されます。ENUM ダイヤリングされたコールはネイバーを経由します。この設定は、自社からのすべての ENUM ダイヤリングを特定の 1 つのシステム上に設定する場合に便利です。

---

## 発信コールの ENUM ダイヤリング

ローカルエンドポイントを ENUM を使用して別のエンドポイントに Expressway を介してダイヤルできるようにするには、次の条件を満たす必要があります。

- 着信側のエンドポイントの E.164 番号を URI にマッピングするために使用できる NAPTR レコードが NDS に存在する必要があります。このレコードを提供する役割は着信側のエンドポイントが属する企業の管理者が担い、企業内のエンドポイントを ENUM ダイヤリングを介して接続可能にする場合にのみ、そのレコードを使用可能にします。
- ローカル Expressway 上に [ENUM ダイヤリングのゾーンと検索ルールの設定](#)する必要があります。この ENUM ゾーンには、着信側のエンドポイントの NAPTR レコードを保持しているドメインと同じ DNS サフィックスが必要です。
- NAPTR レコード（および、必要な場合は結果の URI）を照会できる、少なくとも 1 つ以上の [ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定](#)のアドレスを使用してローカル Expressway を設定する必要があります。

ENUM プロセスが 1 つまたは複数の URI が返された後、[発信コールでの DNS を介した URI ダイヤリング](#)に従って、これらの URI のそれぞれについての新しい検索が開始されます。URI がローカルに登録されたエンドポイントに属している場合は、それ以上の設定は不要です。ただし、少なくとも 1 つの URI がローカルに登録されていない場合、DNS ルックアップを使用してそれらの URI を検索するのであれば、DNS ゾーンを設定する必要もあります。

### コール処理

Expressway はこのプロセスに従って ENUM (E.164) 番号を検索します。

1. Expressway は、ダイヤルされたとおりに受信した E.164 番号の検索を開始します。これは通常の [コールルーティングプロセス](#)に従います。
2. 検索前トランスフォーメーションを適用した後、Expressway は [検索ルールの設定](#) をチェックして、それらのルールのいずれかが、次のいずれかの **モード** で設定されていることを確認します。
  - [任意のエイリアス (*Any alias*) ] または
  - E.164 番号に一致するパターンによる [エイリアス パターン マッチ (*Alias pattern match*) ]
3. 一致する検索ルールに関連付けられたターゲットゾーンがルールのプライオリティ順に照会されます。
  - ターゲットゾーンがネイバーゾーンである場合、ネイバーで E.164 番号が照会されます。ネイバーが ENUM ダイヤリングをサポートする場合、コール自体をルーティングできます。
  - ターゲットゾーンが ENUM ゾーンである場合、Expressway は ENUM を通じてエンドポイントを検出しようとします。Expressway に設定されている各 ENUM ゾーンを照会する限り、E.164 番号が次のように ENUM ドメインに変換されます。

1. 数字を反転し、ドットで区切ります。
  2. ENUM ゾーンに設定された **DNS サフィックス**が追加されます。
4. 次に、結果の ENUM ドメインを DNS に照会します。
  5. DNS サーバがその ENUM ドメインで変換後の E.164 番号（反転され、ドットで区切られた後の番号）に一致する NAPTR レコードを検出した場合、関連付けられた URI を Expressway に返します。
  6. その後、Expressway はその URI の新しい検索を開始します（既存のホップ カウントは維持されます）。検索プロセス（検索前トランスフォーメーションを適用してからローカルゾーンと外部ゾーンをプライオリティ順に検索）の開始時に Expressway が起動します。SIP/H.323 URI を検索しているこの時点から、[URI ダイヤリングについてのプロセス](#)に進みます。

この例では Example Corp の Fred をコールします。Fred のエンドポイントは実際には URI の **fred@example.com** を使用して登録されていますが、もっと簡単に Fred と接続するために、Fred のシステム管理者がこのエイリアスを Fred の E.164 番号である **+44123456789** にマッピングする DNS NAPTR レコードを設定しました。

**example.com** の NAPTR レコードが **e164.arpa** の DNS ドメインを使用することを分かっています。

1. ローカル Expressway に、**e164.arpa** の **DNS サフィックス** を使用して、2 つのゾーンに 1 つの 2 つのゾーンを作成します。
2. **[パターン マッチ モード (Pattern match mode)]** を **[任意のエイリアス (Any alias)]** に、また、**[ターゲット (Target)]** を ENUM ゾーンに設定した検索ルールを設定します。つまり、検索されるエイリアスの形式に関係なく、常に ENUM が照会されます。
3. エンドポイントから **44123456789** をダイヤルします。
4. Expressway が **44123456789** の登録の検索を開始します。また、**[任意のエイリアス (Any alias)]** の検索ルールは ENUM ゾーンを照会することを意味します。



(注) 最初に他のプライオリティの高い検索が番号に一致する可能性があります。

5. 照会するゾーンが ENUM ゾーンであるため、Expressway が自動的にトリガーされ、番号を次のように ENUM ドメインに変換します。
  1. 数字を反転し、ドットで区切って **9.8.7.6.5.4.3.2.1.4.4** にします。
  2. ENUM ゾーン **e164.arpa** に設定された **DNS サフィックス** が追加されます。この結果、**9.8.7.6.5.4.3.2.1.4.4.e164.arpa** のドメインが変換されます。
6. 次に DNS で ENUM ドメインを照会します。

7. DNS サーバがドメインを検出し、関連付けられた NAPTR レコードの情報を返します。これは、ダイヤルした E.164 番号が **fred@example.com** の SIPURI にマップされていることを Expressway に通知します。
8. Expressway はその後、**fred@example.com** のこの時間に関する別の検索を開始します。この時点から URI ダイヤリングプロセスに進み、コールは Fred のエンドポイントに転送されます。

## ENUM ダイヤリングのゾーンと検索ルールの設定

ENUM ダイヤリングをサポートするには、リモートエンドポイントで使用する各 ENUM サービス用の ENUM ゾーンと関連する検索ルールを設定する必要があります。

### ENUM ゾーン追加と設定



- (注)
- ENUM ゾーンは Expressway 上にいくつでも設定できます。エンドポイントが使用する各 DNS サフィックスに少なくとも 1 つの ENUM ゾーンを設定する必要があります。
  - 通常の検索ルールのパターンマッチングと優先順位付けのルールが ENUM ゾーンに適用されます。
  - また、NAPTR レコードの検索時に使用する [ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定](#) 必要もあります。

ENUM ゾーンをセットアップするには、次の手順を実行します。

ステップ 1 [設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)] へ移動します。

ステップ 2 [新規 (New)] をクリックします。[ゾーンの作成 (Create zone)] ページが表示されます。

ステップ 3 ゾーンの名前を入力し、[タイプ (Type)] として [ENUM] を選択します。

ステップ 4 ENUM ゾーンを次のように設定します。

フィールド	ガイドライン
ホップカウント (Hop count)	ほかのゾーンタイプのホップカウントと同じ方法で、ENUM ゾーンに指定した <a href="#">ホップカウントの設定</a> を適用します。DNS ルックアップで戻されたエイリアスの新しい検索プロセスを Expressway が開始した時点で現在適用可能なホップカウントが維持されます。
DNS サフィックス (DNS suffix)	ENUM のホスト名を作成するための変換後の E.164 番号に追加するサフィックス。これは NAPTR レコードを照会する (ドメインネームスペース内の) DNS ゾーンを表します。

フィールド	ガイドライン
<b>H.323 モード (H.323 Mode)</b>	このゾーンを H.323 レコードでルックアップするかどうかを制御します。
<b>SIP モード (SIP mode)</b>	このゾーンを SIP レコードでルックアップするかどうかを制御します。

ステップ 5 [ゾーンの作成 (Create zone)] をクリックします。

## ENUM ゾーンの検索ルールの設定

ローカルに登録されたエンドポイントが Expressway を介して ENUM コールをできるようにするには、少なくとも次の情報を使用して ENUM ゾーンと関連する検索ルールを設定する必要があります。

- **e164.arpa** の DNS サフィックス (この 2 つのドメインは、この 2 つのドメインの 1 つで指定されます)。
- **[モード (Mode)]** が **[任意のエイリアス (Anyalias)]** に設定された関連する検索ルール。

これにより、ENUM だけでなく、常にすべてのタイプのエイリアスが DNS で照会されることとなります。また、ダイヤルされる企業が **e164.arpa** ドメインを使用している場合にのみ、ENUM ダイヤリングが成功することも意味します。ENUM ダイヤリングが確実に成功するには、企業内の発信者がダイヤルするエンドポイントの NAPTR レコードを保持しているドメインごとに ENUM ゾーンを設定する必要があります。

各 ENUM に送信するクエリをフィルタリングする検索ルールを次のように設定します。

- **[モード (Mode)]** に **[エイリアス パターン マッチ (Alias pattern match)]** を使用する
- **[パターン文字列 (Pattern string)]** フィールドと **[パターンタイプ (Pattern type)]** フィールドを使用して ENUM ルックアップをトリガーするドメインごとにエイリアスを定義する

たとえば、自社のネットワークからエンドポイントの E.164 番号が **44** で始まる英国内のリモートオフィスへの ENUM ダイヤリングを有効にすることができます。これを行うには、Expressway 上に ENUM ゾーンと、それに関連付ける検索ルールを次のように設定します。

- **[モード (Mode)]** を **[エイリアス パターン マッチ (Alias pattern match)]** に設定する
- **[パターン文字列 (Pattern string)]** **44**
- **[パターンタイプ (Pattern type)]** を **[プレフィックス (Prefix)]** に設定する

これにより、**44** で始まる番号を誰かがダイヤルした場合にのみ、ENUM クエリがそのゾーンに送信されるようになります。

## ENUM ゾーンのトランスフォーメーションの設定

他のゾーンと同じ方法で、ENUMゾーン用のトランスフォーメーションを設定できます（詳細については、[検索とゾーン変換プロセス](#)の項を参照してください）。

ENUM ゾーンのトランスフォーメーションは、番号が ENUM ドメインに変換される前に適用されます。

たとえば、自社のネットワークからプレフィックスに8と、その後リモートのエンドポイントの E.164 番号の最後の4桁を使用してリモートサイトのエンドポイントへの ENUM ダイヤリングを有効にすることができます。これを行うには、Expressway 上に ENUM ゾーンと、それに関連付ける検索ルールを次のように設定します。

- [モード (Mode) ] を [エイリアスパターンマッチ (Alias pattern match) ] に設定する
- [パターン文字列 (Pattern string) ] 8(\d{4})
- [パターンタイプ (Pattern type) ] を [正規表現 (Regex) ] にする
- [パターン動作 (Pattern behavior) ] を [置換 (Replace) ] にする
- [置換文字列 (Replace string) ] 44123123(\1)

この設定により、ENUM ドメインに変換され、DNS を介して照会された文字列は (44123123xxxx) になります。

発信 ENUM ダイヤリングを正しく設定したことを確認するには、[検索ツール](#) ([メンテナンス (Maintenance) ] > [ツール (Tools) ] > [検索 (Locate) ]) を使用して E.164 エイリアスの解決を試行します。

## 着信コールの ENUM ダイヤリング

ENUM ダイヤリングを使用してローカルに登録したエンドポイントに到達するようにするには、エンドポイントの E.164 番号を UIR にマッピングする DNS NAPTR レコードを設定する必要があります。このレコードは、ENUM ダイヤリングを使用して到達しようとしているシステムが検出できる、適切な DNS ドメインに配置する必要があります。

### ENUM の DNS ドメインについて

ENUM が E.164 番号と URI との間でマッピングを行うには、NAPTR レコードの有無に依存します。

[RFC 3761](#) は、ENUM の標準規格を定義する一連のドキュメントの一部であり、NAPTR レコードが公共の ENUM 導入環境として検出されるべき ENUM ドメインは **e164.arpa** であると明示しています。ただし、このドメインを使用するには、適切な国の規制機関によって E.164 番号が割り当てられている必要があります。すべての国が ENUM に参加しているわけではないため、NAPTR レコードに代替ドメインを使用することができます。このドメインは会社のネットワーク内に存在するか (ENUM を社内で使用する場合)、または <http://www.e164.org> などの公共の ENUM データベースを使用することも可能です。



## DNS NAPTR レコードの設定

ENUM は RFC 2915 に定義されているように、NAPTR レコードの有無に依存します。これらのレコードを使用して、E.164 番号から H.323 や SIP URI が取得されます。

Expressway がサポートするレコード形式は次のとおりです。

### order preference flag service regex replacement

値は次のとおりです。

- **order** および **preference** を選択して、NAPTR レコードが処理される順序を決定します。最下位のレコードが最初に処理され、照合順の場合は最下位の優先度を持つレコードが最初に処理されます。
- **flag** によってこのレコード内の他のフィールドの解釈が決まります。値 **u**（これが終端ルールであることを示す）のみが現在サポートされており、必須となっています。
- **service** はこのレコードが E.164 から H.323 または SIP の URI 変換を記述するためのものであることを示します。その値は、**E2U+h323** or **E2U+SIP** のいずれかである必要があります。
- **regex** は指定された E.164 番号から H.323 または SIP URI への変換を記述する正規表現です。
- **replacement** は、Expressway で現在使用されていないので、. (句点) に設定する必要があります。

ENUM の非終端ルールは現在 Expressway ではサポートされていません。これらの詳細については、『RFC 3761』の 2.4.1 項を参照してください。

たとえば、次のレコードがあります。

**IN NAPTR 10 100 "u" "E2U+h323" "!(.\*)\$!h323:\1@example.com!"**を使用して無効にすることができます。

この例は次のように解釈されます。

- **10** は **order**
- **100** は **preference**
- **u** は **flag**
- **E2U+h323** はこのレコードが H.323 URI 用であるとしています。
- **!(.\*)\$!h323:\1@example.com!** は変換について説明します。
  - **!** はフィールド区切り文字
  - 最初のフィールドが変換する文字列であることを表します。この例では、**!(.\*)\$** は E.164 番号全体を表します。

- 2 番目のフィールドは生成される H.323 URI を表します。この例では、**h323:1@example.com** が E.164 番号が **@example.com** と連結されることを示しています。たとえば、**1234** は **1234@example.com** にマッピングされます。
- 置換フィールドが使用されていないことを示します。

## ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定

DNS サーバは次のように ENUM ダイヤリングと URI ダイヤリングをサポートする必要があります。

- **ENUM ダイヤリング** : E.164 番号を URI にマッピングする NAPTR レコードを照会する
- **URI ダイヤリング** : ローカルに登録されていないか、またはネイバー システムを介してアクセスできないエンドポイントをルックアップする

DNS サーバ (DNS クエリに Expressway が使用するもの) を設定するには、次の手順を実行します。

**ステップ 1** [DNS] ページ ([システム (System)] > [DNS]) に移動します。

**ステップ 2** [アドレス 1 (Address 1)] フィールドから [アドレス 5 (Address 5)] フィールドに、ドメインの検出を試行する際に Expressway を照会する最大 5 台の DNS サーバの IP アドレスを入力します。これらのフィールドには FQDN ではなく、IP アドレスを使用する必要があります。

## コール ルーティングとシグナリングの設定

「コールルーティング (Call routing)」ページ ([設定 (Configuration)] > [コールルーティング (Call routing)]) を使用して、Expressway のコールルーティングとシグナリングの機能を設定します。

### コール シグナリングの最適化

コールは、シグナリングとメディアの 2 つのコンポーネントから構成されています。トラバーサル コールの場合、Expressway は常にメディアとシグナリングの両方を処理します。非トラバーサル コール場合は、Expressway はメディアを処理しません。またシグナリングの処理は必要な場合も不要な場合もあります。

[**コールシグナリングの最適化 (Call signaling optimization)**] の設定では、コールがセットアップされた後にコールシグナリングパスから Expressway がそれ自体を (可能な場合は) 削除するかどうかを指定します。この設定のオプションは次のとおりです。

- [オフ (*Off*)] : Expressway は常にコールシグナリングを処理します。
  - コールは RMS コールライセンス、または Expressway 上の登録済みコールライセンスのいずれかを消費します。
- [オン (*On*)] : Expressway はコールが次のいずれかである場合にコールシグナリングを処理します。
  - トラバーサルコール
  - コールポリシーまたは FindMe によって次のように変更された H.323 コール
    - コールが複数のエイリアスに解決される
    - コールの送信元エイリアスが関連付けられた FindMe ID を表示するように変更された
    - FindMe に「応答なし」または「ビジー」のデバイスが設定されていない
  - コール内のいずれかのエンドポイントがローカルに登録されている
  - 着信トランスポートプロトコル (UDP、TCP、TLS) が発信プロトコルと異なっている場合の SIP コール

その他の場合はすべて、Expressway はコールがセットアップされた後にコールシグナリングパスからそれ自体を削除します。Expressway はそのようなコールについてはコールライセンスを消費しません。また、コールシグナリングパスが簡略化されます。この設定は、ディレクトリ Expressway で使用する場合の[階層化ダイヤルプラン](#)に役立ちます。そのような導入環境では、ディレクトリ Expressway を使用してエンドポイントをロックアップして検出します。また、どのエンドポイントもその Expressway に登録させません。

## コールループ検出モード

ダイヤルプランまたは隣接するネットワークのダイヤルプランは、シグナリングループが発生することを想定して設定できます。この例は[構造化ダイヤルプラン](#)であり、すべてのシステムがメッシュ内にまとめて隣接化されています。このような設定では、[ホップカウントの設定](#)の設定が大きすぎると、ホップカウントが 0 に到達するまで単一の検索要求がネットワークに繰り返し送信されることがあり、リソースを不必要に消費します。

Expressway はネットワーク内のループを検出し、そのような検索を [**コールループ検出モード (Call loop detection mode)**] の設定で終了させて、ネットワークリソースを節約することができます。この設定のオプションは次のとおりです。

- [オン (On) ] : Expressway はループを含んでいる検索のブランチを実行せず、レベル2の「ループを検出 (loop detected) 」 イベントとして記録します。次の条件のすべてを満たしている場合、2つの検索がループしていると見なされます。
  - 同じコールタグがある
  - 同じ宛先エイリアス宛である
  - 同じプロトコルを使用している
  - 同じゾーンから発信されている
- [オフ (Off) ] : Expressway は検索ループを検出せず、検索ループは失敗します。この設定は高度な導入にのみ使用することを推奨します。

## コールの識別

Expressway を通過する各コールにはコール ID とコール シリアル番号が割り当てられます。また、まだ行われていない場合には、コール タグも割り当てられます。

### コール ID

Expressway は現在進行中の各コールに異なるコール ID を割り当てます。コール ID 番号は1から始まり、そのシステムで許可されるコールの最大数までになります。

コールが発信されるたびに、Expressway はそのコールに使用可能な最も小さいコール ID 番号を割り当てます。たとえば、すでにコール ID が1の進行中のコールがある場合、次のコールにはコール ID 2が割り当てられます。コール1が切断されると、発信される3番目のコールにはコール ID 1が割り当てられます。

したがって、コール ID は一意の識別子ではありません。同時に進行中の2つのコールが同じコール ID を持つことはありませんが、時間の経過とともに、同じコール ID が複数のコールに割り当てられます。




---

(注) Expressway の Web インターフェイスにはコール ID は表示されません。

---

### コール シリアル番号

Expressway は、通過するすべてのコールに一意のコール シリアル番号を割り当てます。Expressway 上の2つのコールが同じコール シリアル番号を持つことはありません。複数の Expressway 間を通過する単一のコールは、システムごとに異なるコール シリアル番号によって識別されます。

## コールタグ

コールタグは、多くの Expressway を通過するコールの追跡に使用されます。Expressway がコールを受信すると、そのコールにコールタグがすでに割り当てられているかどうかを確認します。割り当てられている場合は Expressway は既存のタグを使用します。割り当てられていない場合はそのコールに新しいコールタグを割り当てます。このコールタグは、コールが転送されるときにそのコールの詳細情報に組み込まれます。複数の Expressway 間を通過する単一のコールには、(すでの通過したものも含め) Expressway に着信するたびに異なるコールシリアル番号が割り当てられますが、コールタグを使用することで同じコールであると識別できます。これは、リモート syslog サーバを使用してネットワーク内の多くの Expressway のイベントを照合している場合に特に役に立ちます。

また、コールタグは、ネットワーク内のループの識別にも役立ちます。自動コールルーティングとシングナリングの設定の一部として使用されているため、単一のコールタグに関連するすべてのイベントをイベントログで検索することができます。クエリをネイバーゾーンに送信し、元の Expressway に再度ルーティングされる前に1つ以上のシステムを通過する場合にループが発生します。この場合、発信クエリと着信クエリは異なるコールシリアル番号を持ち、さらに、(トランスフォーメーションが割り当てられたかどうかに応じて)異なる宛先エイリアス宛となる場合があります。ただし、この場合もそのコールのコールタグは同じです。



- 
- (注) Expressway または TelePresence Conductor ではないシステムをコールが通過する場合は、コールタグの情報は失われます。
- 

## CLIでのコールの識別

CLI を使用してコールを制御するには、コール ID かコールシリアル番号のいずれかを使用してコールを参照する必要があります。これらは、次のコマンドを使用して取得できます。

### xStatus Calls

このコマンドは、現在進行中の各コールの詳細情報をコール ID 順に返します。各エントリの 2 番目の行にはコールシリアル番号が表示され、3 番目の行にはコールタグが表示されます。

## コールの切断

### Web インターフェイスを使用したコールの切断



- 
- (注) Expressway がクラスタの一部である場合は、コールが関連付けられているピアにログインし、コールを切断できるようにする必要があります。
-

Web インターフェイスを使用して既存の1つ以上のコールを切断するには、次の手順を実行します。

- 
- ステップ1 「コール (Calls)」 ページ ([ステータス (Status)] > [コール (Calls)]) に移動します。
- ステップ2 コールシリアル番号やコールタグなどのコールの詳細情報を確認するには、[表示 (View)] をクリックします。ブラウザの [戻る (back)] ボタンをクリックして「コール (Calls)」 ページに戻ります。
- ステップ3 終了するコールの横にあるボックスをオンにし、[切断 (Disconnect)] をクリックします。
- 

## CLI を使用したコールの切断

CLI を使用して既存のコールを終了するには、まずコール ID 番号か、またはコールのシリアル番号を取得する必要があります (コールの識別を参照してください)。次に、必要に応じて次のコマンドのいずれかを使用します。

- **xCommand DisconnectCall Call: <ID number>**
- **xCommand DisconnectCall CallSerialNumber: <serial number>**

切断するコールの参照にコール ID 番号を使用するほうが簡単ですが、その間にそのコールが切断され、コール ID が新しいコールに割り当てられているというリスクがあります。そのため、Expressway では、より長くても一意のコール シリアル番号を使用してコールを照会することもできます。



(注) コールを切断すると、そのコール シリアル番号のコールのみが切断されます。コール タグが同じでコール シリアル番号が異なる他のコールは影響されない場合があります。

---

## SIP コールの切断時の制限

コールの切断は、プロトコルの動作の違いにより、H.323 コールと SIP コールでは異なる方法で動作します。

H.323 コールでインターワーキングしているコールでは、**Disconnect** コマンドでコールが実際に切断されます。

SIP コールでは、**Disconnect** コマンドによって Expressway はそのコールに使用したすべてのリソースを解放します。これで、コールは Expressway 上で切断されたように見えます。ただし、この時点でも、エンドポイントはコール中であると見なします。SIP コールはピアツーピアであり、Expressway は SIP プロキシであるため、エンドポイントに権限がありません。Expressway 上のリソースを解放すると、次にエンドポイントから Expressway へのシグナリングが発生した場合は、Expressway は「「481 コール/トランザクションは存在しません (481 Call/Transaction Does Not Exist)」」と応答してエンドポイントがコールをクリアします。



- 
- (注) SIP セッションタイマーをサポートするエンドポイント ([RFC 4028](#) を参照) にはコールリフレッシュタイマーがあり、切断されたコール (エンドポイント間でのシグナリングの消失) を検出することができます。エンドポイントは、次のセッションタイマーメッセージの交換後にリソースを解放します。
-





## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。