# ファイアウォール トラバーサル

ここでは、ファイアウォールを通過するための Expressway-C と Expressway-E の設定方法について説明します。



# ファイアウォール トラバーサルについて

ファイアウォールは、ネットワークに着信する IP トラフィックを制御することを目的としています。ファイアウォールは一般に、未承諾の着信要求をブロックします。つまり、ネットワーク外から発信されたすべてのコールが阻止されます。ただし、信頼できる特定の宛先への発信要求を許可したり、それらの宛先からの応答を許可するようにファイアウォールを設定できます。これが、すべてのファイアウォールのセキュアなトラバーサルを可能にするためにシスコの Expressway テクノロジーが用いている原則です。

## Expressway ソリューション

Expressway ソリューションは次のように構成されています。

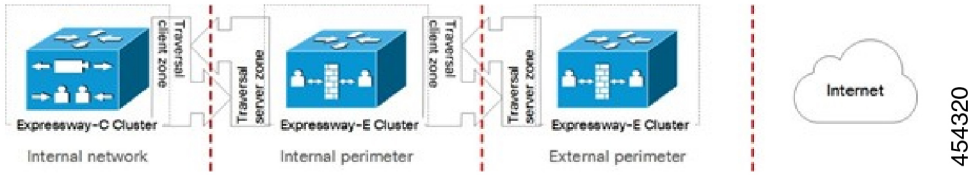
- ファイアウォール トラバーサル サーバとして機能し、パブリック ネットワーク上のファイアウォールの外側または DMZ 内にある Expressway-E。
- ファイアウォール トラバーサル クライアントとして機能し、プライベート ネットワーク内にある Expressway-C またはその他のトラバーサル対応のエンドポイント。

2つのシステムは連携して、2つの間のすべての接続が発信される環境を構築します。つまり、クライアントからサーバに確立されます。また、ファイアウォールを正常に通過することができます。

### チェーン接続されたファイアウォール トラバーサル

企業間の Expressway 展開では、ファイアウォール トラバーサル チェーンを設定できます。Expressway-E は、トラバーサル サーバとして機能するだけでなく、別の Expressway-E へのトラバーサル クライアントとしても機能します。

**図 *1 : 2* つのチェーン付き *Expressway-Es* の例**




たとえば、（図に示すように）2つの Expressway-E をチェーン化した場合、最初の Expressway-E は Expressway-C のトラバーサル サーバです。その最初の Expressway-E は、2番目の Expressway-E のトラバーサル クライアントでもあります。2 番目の Expressway-E は最初の Expressway-E のトラバーサル サーバです。

（注）

- トラバーサル チェーンは、Mobile & Remote Access の展開ではサポートされていません。
- この機能は、バージョン X8.10 の Cisco Expressway シリーズで正式に導入されました。ファイアウォール トラバーサルが導入されたため Cisco TelePresence VCS で可能になっています。

# 推奨事項と前提条件

（注）

Expressway-E と Expressway-C の両方で同じバージョンのソフトウェアを実行することを推奨します。

ファイアウォールが区別できないため、Expressway-E と Expressway-C に共有アドレスを使用しないでください。Expressway-E で IP アドレッシングにスタティック NAT を使用する場合は、Expressway-C 上の NAT が同じトラフィックの IP アドレスの解決を行わないことを確認します。Expressway-E と Expressway-C 間の共有 NAT アドレスはサポートされません。

# 動作の仕組み

トラバーサル クライアントは、トラバーサル サーバ上の指定ポートへの接続をファイアウォールを介して常に維持します。この接続は、クライアントがパケットを定期的にサーバへ送信することでアライブ状態が保持されます。トラバーサル サーバがトラバーサル クライアント宛の着信コールを受信すると、この既存の接続を使用して着信コール要求をクライアントに送信します。次に、クライアントはコール メディアまたは署名、あるいはその両方に必要なアウトバウンド接続を開始します。

この処理により、ファイアウォールの観点からはすべての接続がファイアウォール内部のトラバーサルクライアントからトラバーサル サーバに開始されることが保証されます。

ファイアウォール トラバーサルを正しく機能させるには、各クライアント システム用に Expressway-E 上で、Expressway-E に接続するクライアント システムごとに 1 つのトラバーサル サーバを設定する必要があります（これには、Expressway-E に直接登録するトラバーサル対応のエンドポイントは含まれません。これらの接続の設定値は別の方法で設定します）。同様に、各 Expressway クライアントには 1 つのトラバーサル クライアント ゾーンが必要です。これは、接続先のサーバごとに設定する必要があります。

クライアントとサーバ ゾーンの各ペアに設定するポートとプロトコルは同じである必要があります。各システムに必要な設定の概要については、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。Expressway-E は特定のポート上のクライアントからの接続をリッスンするため、Expressway-C でトラバーサル クライアント ゾーンを作成する前に、Expressway-E でトラバーサル サーバ ゾーンを作成することを推奨します。

トラバーサルクライアントとトラバーサルサーバは両方とも Cisco Expressway システムである必要があります（どちらにも Cisco VCS は使用できません）。

# エンドポイント トラバーサル テクノロジーの要件

ファイアウォールトラバーサルをサポートするための「遠端」（家庭やホテルなど）エンドポイントの要件の概要を以下に示します。

- H.323 の場合、エンドポイントで Assent、または H460.18 および H460.19 をサポートする必要があります。
- SIP の場合、エンドポイントは標準的な SIP のみをサポートする必要があります。
  - 登録メッセージで Expressway に対して「遠端」のファイアウォール ポートを開いたままにし、そのエンドポイントにメッセージを送信します。Expressway はファイアウォールの背後にあるエンドポイントからのメディアを待機してから、その同じポート上のエンドポイントにメディアを返します。つまり、エンドポイントは同じポートでのメディア転送や受信をサポートする必要がありません。
  - また、Expressway は SIP アウトバウンドもサポートしています。これは、登録メッセージ全体を使用するオーバーヘッドなしにファイアウォールを開いたままにする代替方法です。

- SIP エンドポイントと H.323 エンドポイントは Expressway-E に登録できます。または、SIP ポートや H.323 ポートを介して Expressway-E と通信できるようにローカル「DMZ」ファイアウォールで該当するポートを開いている場合、それらのエンドポイントは Expressway-E のみにコールを送信できます。

また、エンドポイントは ICE について を使用して、エンドポイント間のメディア通信に最適な（エンドポイントにとって最適な）パスを検出することもできます。メディアはエンドポイントからエンドポイントへと直接送信したり、エンドポイントから宛先のファイアウォールの外部 IP アドレスを経由して宛先のエンドポイントに送信したり、エンドポイントから TURN サーバを経由して宛先のエンドポイントに送信したりできます。

- Expressway がメディアを通過する必要がない場合（IPv4/IPv6 変換や SIP/H.323 変換の必要がないなど）、Expressway はコールの ICE をサポートします。通常これは、ICE をサポートできる 2 つのエンドポイントが Expressway-E クラスタと直接通信することを意味します。
- Expressway-E は独自の組み込み TURN サービスの設定を使用して ICE 対応のエンドポイントをサポートします。

# H.323 ファイアウォール トラバーサル プロトコル

Expressway は、H.323 用の 2 つの異なるファイアウォール トラバーサル プロトコルである Assent と H.460.18/H.460.19 をサポートします。

- Assent はシスコ独自のプロトコルです。
- H.460.18 と H.460.19 は ITU 標準規格で、署名およびメディアのファイアウォール トラバーサルにそれぞれプロトコルを定義します。これらの標準規格は、元の Assent プロトコルに基づいています。

トラバーサル サーバとトラバーサル クライアントが通信するには、同じプロトコルを使用する必要があります。2 つのプロトコルはそれぞれが別の範囲のポートを使用します。

# SIP ファイアウォール トラバーサル プロトコル

Expressway は、メディアの SIP ファイアウォール トラバーサル用の Assent プロトコルをサポートします。

クライアントからサーバへと確立された TCP/TLS 接続を通じてシグナリングが通過します。

# メディアの逆多重化

Expressway-E は、次のようなシナリオでメディアの逆多重化を使用します。

- Assent を使用するように設定されたトラバーサル ゾーンを通じて Expressway-C が送受信する H.323 または SIP のコール レッグ

- 逆多重化モードでH460.19を使用するように設定されたトラバーサルサーバゾーンを通じて Expressway-C が送受信する H.323 のコールレッグ。
- Expressway-E と Assent または H.460.19 対応のエンドポイント間の H.323 のコールレッグ。

Expressway-E は SIP エンドポイント（Assent または H.460.19 をサポートしないエンドポイント）が直接送受信するコール レッグに対して、または、トラバーサル サーバ ゾーンが逆多重化モードでH.460.19を使用するように設定されていない場合は、非逆多重化メディアを使用します。

Expressway-E のメディア逆多重化ポートは、一般的な範囲の**トラバーサル メディア ポート**から割り当てられます。これは、H.323 か SIP かに関係なく、すべての RTP/RTCP メディアに適用されます。

デフォルトのメディアトラバーサルポートの範囲は 36000 ～ 59999 です。Expressway-C では **[設定（Configuration）] > [ローカルゾーン（Local Zones）] > [トラバーサルサブゾーン（Traversal Subzone）]** で設定できます。大規模 Expressway システムでは、その範囲の最初の 12 ポート（デフォルトでは、36000 ～ 36011）は多重化トラフィック用に常に予約されています。Expressway-E はそれらのポートでリッスンします。大規模システムでは逆多重化リスニング ポートの範囲を明示的に設定することはできません。常にメディア ポート範囲内の最初の 6 ペアが使用されます。小規模/中規模のシステムでは、Expressway-E で多重化 RTP/RTCP トラフィックをリッスンする 2 つのポートを明示的に指定できます（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ポート（Ports）]**）。特定のペアのポートを設定しない場合（**[設定された逆多重化ポート**を使用する（Use configured demultiplexing ports）] が *[いいえ（No）]*）、Expressway-E はメディア トラバーサル ポート範囲内のポートの最初のペアでリッスンします（デフォルトでは 36000 と 36001）。

（注） **[設定済みの逆多重化ポートを使用（Use configured demultiplexing ports）]** 設定を変更するには、システムを再起動して変更を有効にする必要があります。

たとえば、Expressway-C と Expressway-E のペアを通じての企業内から自宅のエンドポイントへの SIP コールでは、発生する逆多重化のみが Expressway-C に対向する Expressway-E ポートで実行されます。

| **企業のエンドポイント** | ⟷ | **Expressway-C** | | ⟷ | **Expressway-E** | | ⟷ | **自宅のエンドポイント** |
|---|---|---|---|---|---|---|---|---|
| | | **非逆多重化** | **非逆多重化** | | **逆多重化** | **非逆多重化** | | |
| RTP ポート | | 36002 | 36004 | | 36000 | 36002 | | |
| RTCP ポート | | 36003 | 36005 | | 36001 | 36003 | | |

ただし、同じ Expressway-C/Expressway-E を通じた企業内から自宅の Assent 対応の H.323 エンドポイントへの H.323 コールは、Expressway-E の両側で逆多重化を実行します。

| 企業のエンドポイント | ⟷ | Expressway-C | | ⟷ | Expressway-E | | ⟷ | 自宅のエンドポイント |
|---|---|---|---|---|---|---|---|---|
| | | 非逆多重化 | 非逆多重化 | | 逆多重化 | 逆多重化 | | |
| RTP ポート | | 36002 | 36004 | | 36000 | 36000 | | |
| RTCP ポート | | 36003 | 36005 | | 36001 | 36001 | | |

Expressway-E で高度なネットワーキングを使用している場合も上記と同じポート番号を使用しますが、それらのポート番号は内部 IP アドレスと外部 IP アドレスに割り当てられます。

# ファイアウォール トラバーサルの設定の概要

ここでは、Expressway がトラバーサル サーバまたはトラバーサル クライアントとしてどのように機能するかの概要を示します。

## ファイアウォール トラバーサル クライアントとしての Expressway

Expressway は、VCS に登録された SIP エンドポイントと H.323 のエンドポイント、およびそれに隣接するシステムの代わりに、ファイアウォール トラバーサル クライアントとして機能します。ファイアウォール トラバーサル クライアントとして機能するには、ファイアウォール トラバーサル サーバとして機能するシステムに関する情報を使用して Expressway を設定する必要があります。

それには、Expressway クライアントのトラバーサルクライアント ゾーン（**[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]**）を追加し、トラバーサルサーバの詳細を使用してそのゾーンを設定します。詳細については、「トラバーサルクライアント ゾーンの設定」を参照してください。複数のトラバーサルサーバに接続する場合は、複数のトラバーサル クライアント ゾーンを作成できます。

### Expressway-C または Expressway-E？

- 通常、ファイアウォールトラバーサルクライアントとして Expressway-C を使用します。ただし、Expressway-E でもこの役割を果たします。
- Expressway クライアントが使用するファイアウォール トラバーサル サーバは Expressway-E でなければなりません。

# ファイアウォール トラバーサル サーバとしての Expressway

Expressway-E には、Expressway-C のすべての機能（ファイアウォール トラバーサル クライアントとしての機能を含む）が備わっています。ただし、その主要機能は、他のシスコのシステム用のファイアウォール トラバーサル サーバおよびそれに直接登録されたトラバーサル対応のエンドポイントとして機能できることです。また、TURN リレー サービスも ICE 対応のエンドポイントに提供します。

## トラバーサル サーバ ゾーンの設定

シスコのシステムのファイアウォールトラバーサルサーバとして機能する Expressway-E の場合は、Expressway-E でトラバーサルゾーンを作成し（**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]**）、トラバーサルクライアントの詳細を使用してそのゾーンを設定します。詳細については、トラバーサルサーバゾーンの設定を参照してください。

トラバーサル クライアントであるすべてのシステムに個別のトラバーサル サーバ ゾーンを作成する必要があります。

## その他のトラバーサル サーバ機能の設定

- Expressway-E をトラバーサル対応のエンドポイント（Cisco MXP エンドポイントや、ITU H.460.18 および H.460.19 標準規格をサポートするその他のエンドポイントなど）のファイアウォール トラバーサル サーバとして機能させる場合、追加の設定は必要ありません。詳細については、Expressway-E とトラバーサル エンドポイントとの通信の設定を参照してください。
- TURN リレーサービスを有効にし、ICE に関する詳細な情報を取得するには、ICE および TURN サービスについてを参照してください。
- Expressway-E が使用するデフォルトのポートを設定するには、ファイアウォール トラバーサル用のポートの設定を参照してください。

## ファイアウォール トラバーサルと高度なネットワーキング

高度なネットワーキングのオプション キーにより、Expressway-E の LAN 2 インターフェイスが有効になります（このオプションは Expressway-C では使用できません）。LAN 2 インターフェイスは、2 つの個別のネットワーク（内部 DMZ と 外部 DMZ）から構成される DMZ 内に Expressway-E があり、この 2 つのネットワーク間の直接通信を阻止するようにネットワークが構成されている場合に使用されます。

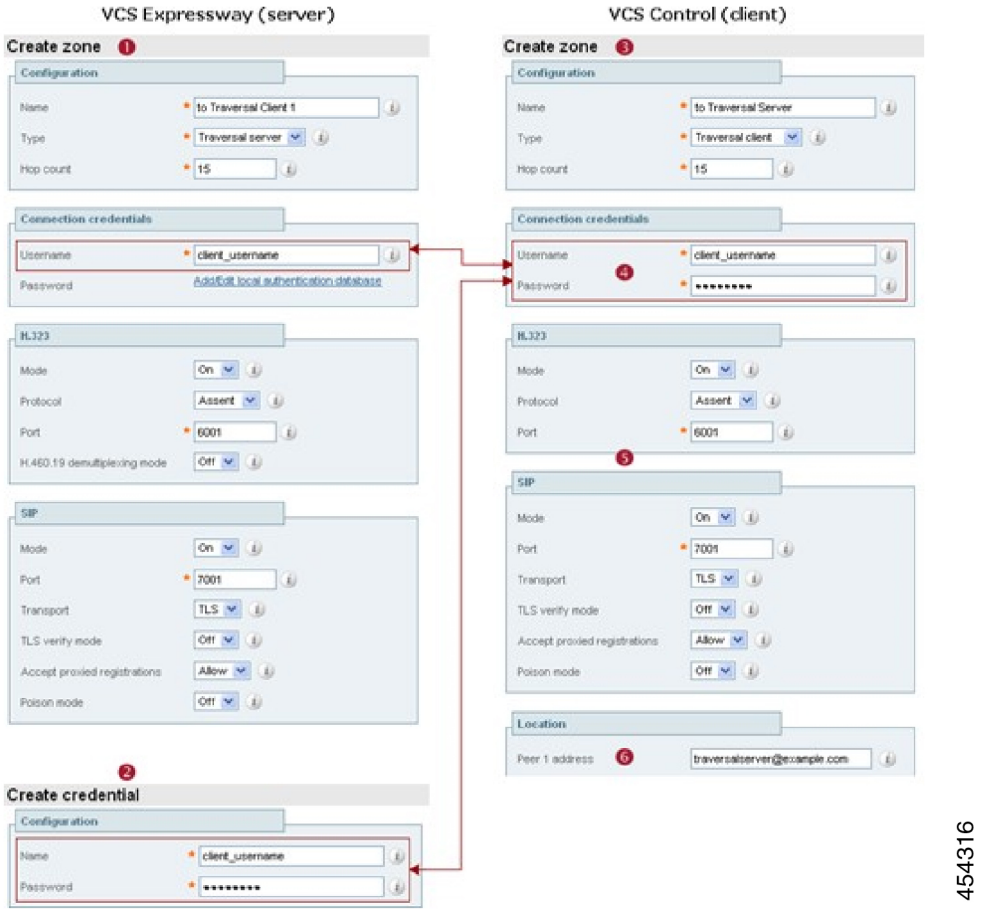
LAN 2 インターフェイスを有効にすると、2 つの個別の IP アドレス（DMZ 内のそれぞれのネットワークに 1 つずつ）を使用して Expressway を設定できます。そうすることで、Expressway は 2 つのネットワーク間でプロキシ サーバとして機能し、DMZ を構成する内部と外部のファイアウォール間でコールを渡すことができます。

高度なネットワーキングが有効になっていると、Expressway 上で設定された、ファイアウォール トラバーサルに関係するポートなどの全ポートが両方の IP アドレスに適用されます。IP アドレスごとにポートを個別に設定することはできません。

# トラバーサル クライアントとサーバの設定

トラバーサル クライアントとサーバを設定する基本的な手順は、次のとおりです。

| ステップ | 説明 |
|---|---|
| 1 | Expressway-E でトラバーサル サーバ ゾーンを作成します（これは、Expressway-C からの着信接続を表します）。**[ユーザ名（Username）]** フィールドに、Expressway-C の認証ユーザ名を入力します。 |
| 2 | Expressway-E で、Expressway-C の認証ユーザ名とパスワードをクレデンシャルとしてローカル認証データベースに追加します。 |
| 3 | Expressway-C でトラバーサル クライアント ゾーンを作成します（これは、Expressway-E への接続を表します）。 |
| 4 | Expressway-E で指定したものと同じ認証用の**ユーザ名**と**パスワード**を入力します。 |
| 5 | H.323 と SIP プロトコルのセクションのすべてのモードとポートを Expressway-E のトラバーサル サーバ ゾーンとまったく同じように設定します。 |
| 6 | Expressway-E の IP アドレスまたは FQDN を **[ピア 1 アドレス（Peer 1 address）]** フィールドに入力します。 |




# ファイアウォール トラバーサル用のポートの設定

（注） 具体的なポート情報は別のドキュメントに記載されています。Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

ポートはファイアウォール トラバーサル設定で重要な役割を果たします。接続が許可されるようにするには、正しいポートを Expressway-E、トラバーサル クライアントおよびファイアウォール上に設定する必要があります。

ポートは最初に Expressway-E 管理者が Expressway-E に設定します。次に、ファイアウォール管理者とトラバーサル クライアント管理者にそれらのポートが通知されます。管理者はサーバ上の特定のポートに接続するようにシステムを設定する必要があります。トラバーサル クライアント上で必要な唯一のポート設定は、発信接続に使用するポートの範囲です。ファイアウォー

ル管理者は、必要な場合にこれらのポートからの発信接続を許可するようにファイアウォールを設定できるよう、この情報を認識しておく必要があります。

「ポートの使用方法（Port usage）」ページ（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[ポートの使用方法（Port usage）]**）に Expressway でインバウンドとアウトバウンドの両方で使用されるすべての IP ポートを示します。ファイアウォールを適切に設定できるようにファイアウォール管理者に提供することができます。

高度なネットワーキングが有効になっていると、Expressway 上で設定された、ファイアウォール トラバーサルに関係するポートなどの全ポートが両方の IP アドレスに適用されます。IP アドレスごとにポートを個別に設定することはできません。

Expressway ソリューションは次のように機能します。

1. 各トラバーサル クライアントは Expressway-E の一意のポートへファイアウォールを介して接続します。
2. サーバは、接続を受けるポートと、クライアントが提供する認証クレデンシャルで各クライアントを識別します。
3. 接続が確立されるとクライアントはプローブを Expressway-E に定期的に送信し、接続を有効に維持します。
4. Expressway-E がクライアント宛の着信コールを受信すると、この最初の接続を使用して着信コール要求をクライアントに送信します。
5. 次にクライアントが、1 つ以上のアウトバウンド接続を開始します。これらの接続に使用される宛先ポートは、シグナリングやメディアごとに異なり、使用されているプロトコルによっても違います（詳細については以降の項を参照してください）。

# ファイアウォールの設定

Expressway のファイアウォール トラバーサルを正しく機能させるには、ファイアウォールを次のように設定する必要があります。

- クライアントから Expressway-E が使用するポートへの最初の発信トラフィックを許可する
- Expressway-E 上のこれらのポートから発信元のクライアントへのリターン トラフィックを許可する

（注） ファイアウォール上の H.323 および SIP プロトコルのサポートをすべてオフにすることをお勧めします。Expressway ソリューションでは不要なため、操作に支障をきたす可能性があります。

# トラバーサル サーバ ポートの設定

Expressway-E にはファイアウォール トラバーサルに使用する特定のリスニング ポートがあります。これらのポートへの接続を許可するように、ファイアウォールにルールを設定する必要があります。ほとんどの場合はデフォルトのポートを使用します。ただし、必要に応じて**「ポート（Ports）」**ページ（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ポート（Ports）]**）に移動して、これらのポートを変更することができます。

シグナリング用に設定可能なポートは次のとおりです。

- **H.323 Assent コール シグナリング ポート**
- **H.323 H.460.18 コール シグナリング ポート**

## RTP と RTCP のメディア逆多重化ポート

ポート設定のオプションは、アプライアンスまたは VM のタイプによって異なります。

- **小規模/中規模システム**：1 ペアの RTP と RTCP メディア逆多重化ポートを使用します。これらは、明示的に指定するか、トラバーサル メディア ポートの一般的な範囲の最初から割り当てることができます。
- **大規模システム**：6 つのペアの RTP と RTCP メディア逆多重化ポートを使用します。これらは常に、トラバーサル メディア ポート範囲の最初から割り当てられます。

# トラバーサル クライアントからの接続用のポートの設定

トラバーサル クライアントからの最初の接続に使用する H.323 ポートと SIP ポートを各トラバーサル サーバ ゾーンで指定します。トラバーサル サーバ ゾーンを Expressway-E に新たに設定するたびに、これらの接続にデフォルトのポート番号が割り当てられます。

- H.323 ポートは UDP/6001 から始まり、新たなトラバーサル サーバ ゾーンごとに 1 ずつ増えていきます。
- SHIP ポートは TCP/7001 から始まり、新たなトラバーサル サーバ ゾーンごとに 1 ずつ増えていきます。

これらのデフォルトのポートは必要に応じて変更できますが、各トラバーサル サーバ ゾーンで一意のポートであることを確認する必要があります。H.323 ポートと SIP ポートを Expressway-E に設定した後、対応するトラバーサル クライアントに一致するポートを設定する必要があります。

（注）

- MXP エンドポイントからの最初の接続に使用するデフォルトのポートは、標準 RAS メッセージに使用されるポートと同じ（UDP/1719）です。Expressway-E でこのポートを変更できますが、ほとんどのエンドポイントが UDP/1719 以外のポートへの接続をサポートしません。したがって、これはデフォルトのままにしておくことを推奨します。
- Expressway-E のトラバーサル サーバ ゾーンのそれぞれに設定された一意の SIP ポートと H.323 ポートそれぞれへのファイアウォールを通じたアウトバウンド接続を許可する必要があります。

コールシグナリングポートは **[設定（Configuration）]** > **[トラバーサル（Traversal）]** > **[ポート（Ports）]** で設定します。トラバーサルメディア ポートの範囲は **[設定（Configuration）]** > **[ローカル ゾーン（Local Zone）]** > **[サブゾーン（Subzone）]** で設定します。

Expressway-E に直接登録されているエンドポイントがない場合、Expressway-E がクラスタに含まれていなければ、UDP/1719 は必要ありません。したがって、Expressway-C と Expressway-E 間のファイアウォールを介してこのポートへのアウトバウンド接続を許可する必要はありません。

## TURN ポートの設定

Expressway-E を ICE 対応の SIP エンドポイントで使用できる ICE および TURN サービスについて（Traversal Using Relays around NAT）を提供することができます。

これらのサービスで使用するポートは **[設定（Configuration）]** > **[トラバーサル（Traversal）]** > **[TURN]** で設定できます。

各 SIP エンドポイントの ICE クライアントは、DNS 内の SRV レコードを使用するか、直接設定のいずれかによって、これらのポートを検出できる必要があります。

## パブリック インターネットへ接続するポートの設定

Expressway-E がパブリック インターネット上のエンドポイントに接続を試行する場合は、その接続が行われるエンドポイントのポートを正確に知ることはできません。使用するポートはエンドポイントによって決定され、パブリック インターネット上のエンドポイント上のサーバが見つかって初めて、Expressway-E に通知されるためです。これによって、Expressway-E が DMZ 内にある場合（Expressway-E とパブリック インターネット間にファイアウォールがある場合）は、そのエンドポイントのポートへの接続が許可されるルールを前もって指定することができないために問題が発生する場合があります。

ただし、ファイアウォール管理者がこれらのポートを介した接続を許可できるように、パブリック インターネット上のエンドポイントに送受信するコールに使用する Expressway-E 上のポートは指定できます。

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

# ファイアウォール トラバーサルと認証

Expressway-E では、認証されたクライアント システムのみがトラバーサル サーバとして使用できます。

最初の接続要求をトラバーサル クライアントから受け取ると、Expressway-E は、認証クレデンシャルを提供してそれ自体を認証するようクライアントに要求します。次に Expressway-E はクライアントのクレデンシャルを独自の認証データベースで検索します。一致が見つかると、Expressway-E はクライアントからの要求を受け入れます。

認証に使用する設定は、トラバーサル クライアントのタイプによって次のように異なります。

| トラバーサル クライアント | Expressway-E トラバーサル サーバ |
|---|---|
| **Expressway-C（または Expressway-E）**<br>Expressway クライアントは自身の**ユーザ名**と**パスワード**を提供します。これらは、**[接続認証情報（Connection credentials）]** セクションの **[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** > **[ゾーンの編集（Edit zone）]** を使用してトラバーサルクライアントゾーンで設定します。 | Expressway クライアントのトラバーサル サーバ ゾーンは、クライアントの認証**ユーザ名**を使用して設定する必要があります。これは、**[接続クレデンシャル（Connection credentials）]** セクションの **[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** > **[ゾーンの編集（Edit zone）]** を使用して Expressway-E で設定します。<br>また、Expressway-E の認証データベースに対応するクライアント ユーザ名とパスワードでのエントリが必要です。 |
| **エンドポイント**<br>エンドポイント クライアントはその**認証 ID** と**認証パスワード**を提供します。 | Expressway-E の認証データベースに対応するクライアント ユーザ名とパスワードでのエントリが必要です。 |

（注） Expressway-E がエンドポイントのデバイス認証を使用していないとしても、すべての Expressway トラバーサル クライアントを Expressway-E で認証する必要があります。

## 認証および NTP

H.323 をサポートするすべての Expressway のトラバーサル クライアントは Expressway-E で認証する必要があります。認証プロセスは、タイムスタンプを使用し、各システムが正確なシステム時刻を使用している必要があります。Expressway のシステム時刻はリモート NTP サーバによって提供されます。したがって、ファイアウォール トラバーサルが機能するには、関係するすべてのシステムを NTP サーバの詳細情報を使用して設定する必要があります。

# Expressway-E とトラバーサル エンドポイントとの通信の設定

トラバーサル対応の H.323 エンドポイントは Expressway-E に直接登録し、それをファイアウォール トラバーサルとして使用することができます。

**「ローカルで登録済みのエンドポイント（Locally registered endpoints）」**ページ（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ローカルで登録済みのエンドポイント（Locally registered endpoints）]**）を使用して、Expressway-E とトラバーサル対応のエンドポイント間の通信方法を設定できます。

次のオプションを使用できます。

| フィールド | 説明 |
|---|---|
| **H.323 Assent モード（H.323 Assent mode）** | ファイアウォール トラバーサルに Assent モードを使用する H.323 コールを許可するかどうかを決定します。 |
| **H.460.18 モード（H.460.18 mode）** | ファイアウォール トラバーサルに H.460.18/19 モードを使用する H.323 コールを許可するかどうかを決定します。 |
| **H.460.19 逆多重化モード（H.460.19 demux mode）** | Expressway-E がローカルで登録済みのエンドポイントからのコールに対して逆多重化モードで動作するかどうかを決定します。<br>*[オン（On）]*：すべてのコールにメディア逆多重化ポートを使用します。<br>*[オフ（Off）]*：各コールが個別のポート ペアをメディアに使用します。 |
| **H.323 優先（H.323 preference）** | エンドポイントが Assent と H.460.18 の両方をサポートしている場合に Expressway-E が使用するプロトコルを指定します。 |
| **UDP プローブの再試行間隔（UDP probe retry Interval）** | ローカルで登録済みのエンドポイントが UDP プローブを Expressway-E に送信する頻度（秒単位）です。 |
| **UDP プローブの再試行回数（UDP probe retry count）** | ローカルで登録済みのエンドポイントが Expressway-E への UDP プローブ送信を試行する回数です。 |
| **UDP プローブのキープアライブ間隔（UDP probe 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、ローカルで登録済みのエンドポイントが UDP プローブを Expressway-E に送信する間隔（秒単位）です。 |
| **TCP プローブの再試行間隔（UDP probe retry Interval）** | ローカルで登録済みのエンドポイントが TCP プローブを Expressway-E に送信する頻度（秒単位）です。 |

| フィールド | 説明 |
|---|---|
| **TCP プローブの再試行回数（UDP probe retry count）** | ローカルで登録済みのエンドポイントが Expressway-E への TCP プローブ送信を試行する回数です。 |
| **TCP プローブのキープアライブ間隔（UDP probe 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、ローカルで登録済みのエンドポイントが TCP プローブを Expressway-E に送信する間隔（秒単位）です。 |

# ICE および TURN サービスについて

## ICE について

ICE（Interactive Connectivity Establishment）は SIP クライアントの NAT トラバーサル用のメカニズムを提供します。ICE はプロトコルではなく、TURN（Traversal Using Relays around NAT）や STUN（Session Traversal Utilities for NAT）など、数多くの異なるテクノロジをまとめるフレームワークです。

これにより、NAT デバイスの背後に存在するエンドポイント（クライアント）がメディアを通過できるパスを検出し、それらのパスのそれぞれを経由してピアツーピア接続を確認してから最適なメディア接続パスを選択することができます。通常、使用できるパスは、NAT デバイスに設定されたインバウンド接続とアウトバウンド接続の制約事項によって異なります。このような動作については、RFC 4787 を参照してください。

ICE の使用例として、インターネットを経由した 2 人の在宅ワーカーの通信があります。2 つのエンドポイントが ICE を経由して通信できる場合、Expressway-E は（NAT デバイスがどのように設定されているかに応じて）シグナリングのみを取得する必要があり、メディアは取得しない（そのため、これは非トラバーサル コールとなる）場合があります。送信元の ICE クライアントが非 ICE クライアントをコールしようとすると、Expressway もメディアを取得するためにメディアのラッチングによる NAT トラバーサルが必要な従来の SIP コールにコールの設定プロセスが戻ります。

ICE の詳細については、RFC 5245 を参照してください。

## MRA 展開での ICE パススルー

X12.5 以降、Interactive Connectivity Establishment（ICE）パススルーがサポートされるようになっています。ICE パススルーにより、MRA 対応のエンドポイントが WAN および Cisco Expressway シリーズをバイパスして、エンドポイント間で直接メディアを渡すことができます。

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。

# TURN について

TURN サービスは、SIP クライアントが NAT デバイスの背後から UDP または TCP を介して通信できるようにする STUN ネットワーク プロトコルのリレー拡張機能です。

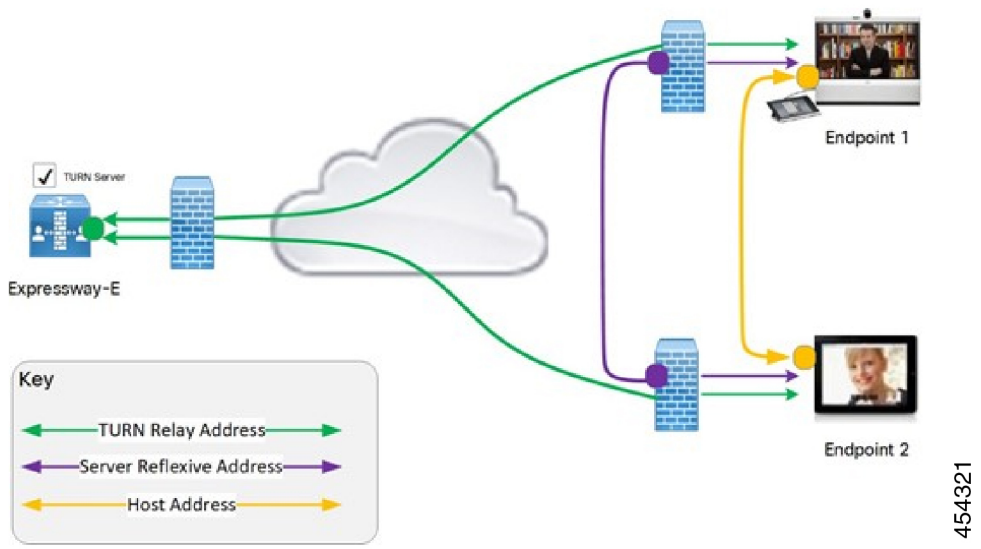
TURN の詳細については RFC 5766 を、基本の STUN プロトコルについては RFC 5389 を参照してください。

各 ICE クライアントはコールのメディア コンポーネントにリレーを割り当てるよう TURN サーバに要求します。各クライアント間のメディア ストリームの各コンポーネントに 1 つのリレーが必要です。

リレーが割り当てられると、各 ICE クライアントには、メディアの送受信が可能になる次の 3 つの潜在的な接続パス（アドレス）が備わります。

- NAT デバイスの背後にある（そのため、NAT の他方にあるエンドポイントからは到達できない）ホスト アドレス
- NAT デバイス上の公開形式でアクセス可能なアドレス
- TURN サーバ上のリレー アドレス

**図 *2 : ICE* メディアの接続パス**




次に、エンドポイントは ICE を通じて接続確認を実行して通信を行うかどうかを決定します。NAT デバイスがどのように設定されているかによっては、エンドポイントが NAT デバイス上の公開されているアドレス間で通信できることがありますが、そうでない場合は TURN サーバを介してメディアをリレーする必要があります。両方のエンドポイントが同じ NAT デバイスの背後にある場合は、内部ホストアドレスを使用して、その 2 つのエンドポイント間にメディアを直接送信できます。

メディア ルートを選択した後は、選択した接続パスに TURN サーバを経由するルートが含まれていなければ、TURN リレーの割り当ては解放されます。エンドポイントが選択した最終的なメディア通信パスに関係なく、シグナリングは常に Expressway 経由になります。

（注） TURN サーバは、一方または両方が企業の内部ファイアウォール内にある場合でも、任意の 2 つの ICE クライアント間でメディアを中継できます。

### 機能と制限事項

- X12.6.1 以降では、セキュリティ強化により、Expressway-E TURN サーバは汎用 STUN サーバとして動作しなくなり、認証されていない STUN バインディング要求を受け入れません。その結果、以下のシナリオが考えられます。
  - シナリオ A：（『*Cisco Expressway* および *Microsoft* インフラストラクチャ導入ガイド』*[英語]*で説明されているように）Microsoft との相互運用性の目的で TURN クライアントとして B2BUA を使用する場合、B2BUA は、サーバが動作しているかどうかを確認するために STUN バインディング要求を TURN サーバに送信することはありません。つまり、Expressway X12.6.1 以降では、到達可能でない TURN サーバの使用を B2BUA が試みた結果、**コールが失敗する可能性があります**。
  - シナリオ B：導入された CMS のバージョンによっては、CMS WebRTC ソリューションが Expressway-E 上の TURN サーバに対して STUN バインド要求を使用する場合があり、これにより障害が発生します。Meeting Server WebRTC を使用する場合は、Expressway バージョン X12.6.1 以降のソフトウェアをインストールする前に、CMS のバージョンと互換性があることを確認してください。バグ ID CSCvv01243 を参照してください。（Expressway-E TURN サーバの設定の詳細については、『Cisco Meeting Server 版 Cisco Expressway Web プロキシ導入ガイド』を参照してください）。
- 小規模または中規模システムでは、最大 1800 のリレー割り当てがサポートされます。通常、最大同時コール数の制限をサポートするにはこの数で十分ですが、ネットワーク トポロジと、コールに使用するメディア ストリーム コンポーネントの数によってはそうでない場合もあります。たとえば、コールの中にはデュオ ビデオを使用するものもあれば、音声のみを使用するものもあります。
- 大規模システムでは、最大 6000 のリレーがサポートされます。ポート多重化が有効になっている場合は、1 つの外部ポートでリレー容量のすべてを使用できます。ポート範囲が設定されている場合は、6 つの外部ポートにリレー容量が分配されます。ポート間で分配される場合、各ポートで処理できるリレー数は 1000 に制限されます。

  この制限は厳密に適用されるわけではありません。したがって、範囲内のポート アドレスごとに、6 つの A/AAAA エントリに同じアドレスを指定した DNS SRV レコードを作成することをお勧めします。このレコードを作成した上で、クライアントに Expressway-E TURN サーバの SRV レコードを設定します。TURN 多重化が有効にされている場合は、TURN 要求をリッスンする外部ポートにだけ SRV レコードを作成することをお勧めします。

- 大規模システムでは、ポートの範囲（デフォルトでは 3478 ～ 3483）で TURN 要求をリッスンする TURN サーバを設定できます。X8.11 以降、TURN 多重化が有効にされていると、Expressway-E はポート範囲の最初のポート（通常は UDP 3478）ですべての TURN 要求を受け入れます。Expressway は内部でこれらの要求をポート範囲に逆多重化します。TURN クライアントは設定済みの単一のポートで要求を送信する必要がありますが、大規模 Expressway-E TURN サーバの完全な容量を利用できます。

- X8.11 以降、Expressway-E は TCP ポート 443 で TURN 要求と Cisco Meeting Server 要求の両方をリッスンできます。Expressway-E は、ポート 443 経由で接続要求を受信すると、要求のタイプに応じて TURN サーバまたは Meeting Server Web プロキシに要求を転送します。したがって、外部ユーザは TURN サービスを使用することで、ファイアウォール ポリシーで制限された環境からでも Meeting Server スペースに参加できます。

  Web 管理者ポートがポート 443（**システム** > **管理設定**）でリッスンするように設定されている場合 、X12.7 以前の Expressway バージョンでは、443 から他の有効なポートに変更する必要があります。X12.7 から、Expressway が専用管理インターフェイスを唯一の管理インターフェイスとして使用するように設定されている場合は、これを行う必要があります。つまり、[**システム** > **管理設定**] ページで、**[専用管理インターフェイスのみを使用]** が *[はい]* に設定されます。

- 大規模システムでは、TCP 443 TURN サービスが有効で、TURN 多重機能も有効な場合 、6000 TCP TURN リレーがサポートされます。

- クラスタ化された Expressway：要求された TURN サーバのリレーが完全に割り当てられている場合、サーバは要求側のクライアントに対してクラスタ内の代替サーバの詳細情報で応答します（現在、使用可能なリソースが最大の TURN サーバ）。

- Expressway の TURN サービスは、単一のネットワーク インターフェイスまたはデュアル ネットワーク インターフェイスで（高度なネットワーキング オプションを介して）サポートされます。デュアル ネットワーク インターフェイスでは、TURN サーバは両方のインターフェイスでリッスンしますが、リレーは Expressway の外部に対向する LAN インターフェイスにのみ割り当てられます。

- Microsoft ICE（各種の標準規格に準拠していません）は Expressway-E の TURN サーバではサポートされていません。そのため、Microsoft Edge Server を通じて登録された Expressway と Microsoft クライアント間の通信を有効にするには、Microsoft 相互運用性サービスを使用する必要があります。

- TURN サーバは帯域幅要求をサポートしません。トラバーサル ゾーンの帯域幅制限は適用されません。

- Expressway-E の TURN サーバは TCP と UDP で TURN メディアをサポートします。サポートされているプロトコルの設定は、CLI コマンド **xConfiguration Traversal Server TURN ProtocolMode** を通じてのみ行えます。

- Expressway-E の TURN サーバは、TCP で UDP リレーをサポートします。

### 内部インターフェイスで送信される STUN パケット

Expressway は、外部 LAN インターフェイスを介して受信した STUN パケットを、常にパケット送信元アドレスとして外部 LAN IP アドレスを使用して送信します。通常、パケットは外部インターフェイスから送信されます。そのため、IP アドレスは通常は一致します。ただし、次の場合、Expressway は内部 LAN インターフェイスから STUN パケットを 送信します。

- TURN クライアントがリレーセッションを使用して、Expressway-E の内部 IP と同じサブネット内のデバイスにメッセージを送信する場合、または
- TURN クライアントがリレーセッションを使用して、Expressway-E の内部ゲートウェイ IP を使用するスタティックルートと一致するサブネット内のデバイスにメッセージを送信する場合。

この動作により、IP アドレスに不一致があるように見える場合がありますが、実際にはシステムは設計どおりに機能しています。

# TURN サービスの設定

TURN リレーサービスは、Expressway-E でのみ使用できます。(X8.11 以降は、TURN サービスの使用で TURN リレーオプションキーは不要です)。

**「TURN」**ページ（**[設定（Configuration）] > [トラバーサル（Traversal）] > [TURN]**）を使用して、Expressway-E の TURN 設定を構成します。Expressway-E を委任クレデンシャル チェック用に設定する場合は、**認証レルム**を介して、TURN サーバ 要求のクレデンシャル チェックが委任されるトラバーサル ゾーンも指定できます。

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 |
|---|---|---|
| **TURN サービス（TURN services）** | Expressway が TURN サービスをトラバーサル クライアントに提供するかどうかを決定します。 | **[TURNサービス（TURN services）]** がすでに *[オン（On）]* に設定されているときに、他の TURN 設定を変更する必要がある場合は、次の手順に従います。<br>1. **[TURNサービス（Turn services）]** を *[オフ（Off）]* に変更して **[保存（Save）]** します。<br>2. 必要に応じて TURN 設定を変更します。<br>3. **[TURNサービス（Turn services）]** を *[オン（On）]* に変更して **[保存（Save）]** します。<br><br>これは、他の TURN 設定を変更した場合、**TURN サービス**が再起動されるまでは、その変更が適用されないためです。 |
| **TCP 443 TURN サービス** | TURN サーバが TCP ポート 443 で TURN クライアントからの TCP 要求をリッスンする必要があるかどうかを指定します。次のオプションがあります。<br>• *[オン（On）]*：TURN サーバは TCP ポート 443 で TURN クライアントからの TCP 要求をリッスンし、設定済みのポートで UDP 要求をリッスンします。<br>• *[オフ（Off）]*：TURN サーバは TCP ポート 443 で TURN クライアントをリッスンしません。ただし、この設定は TURN 要求をリッスンするように設定されたポートには影響しません。 | この機能を有効にする前に、次のことを確認してください。<br>• **[TURNサービス（TURN services）]** が *[オン（On）]* に設定されていること。<br>• X12.7 以前は、Web 管理者ポートがポート 443 でリッスンするように設定されている場合（**[システム（System）] > [管理設定（Administration Settings）]**）、ポート 443 を他の有効なポートに変更する必要があります。X12.7 から、Expressway が専用管理インターフェイスを唯一の管理インターフェイスとして使用するように設定されている場合は、これを行う必要があります。つまり、[**システム > 管理設定**] ページで、**[専用管理インターフェイスのみを使用]** が *[はい]* に設定されます。 |

| フィールド | 説明 | 使用方法のヒント |
| --- | --- | --- |
| **TURN ポート多重化（TURN port multiplexing）** | 大規模システムで、Expressway TURN サーバの全容量を単一のリスニングポート上で有効にして、内部で要求をポート範囲に逆多重化します。<br>（注） このオプションは大規模システムでのみ使用できます。<br><br>オプションは次のいずれかです。<br>• *[オン（On）]*：<br>• Expressway は、ポート範囲ではなく、単一の設定可能な外部ポートでリッスンします。<br>• **[TCP443TURNサービス（TCP 443 TURN services）]** が *[オン（On）]* に設定されている場合、設定可能な外部ポートのみが UDP TURN 要求を多重化します。<br>（注） **[TCP 443 TURN サービス（TCP 443 TURN services）]** が *[オン（On）]* に設定されている場合、技術的な制約により、外部ポートは TCP TURN 要求を多重化しません。<br>• *[オフ（Off）]*：TURN サーバは、ポート範囲で TCP 要求と UDP 要求をリッスンします。 | この機能を有効にする前に、**[TURN サービス（TURN services）]** が *[オン（On）]* に設定されていることを確認してください。 |

| フィールド | 説明 | 使用方法のヒント |
|---|---|---|
| **TURN要求ポート（TURN requests port）** | TURN要求のリスニング ポート。デフォルト ポートは 3478 です。 | 大規模システムでは、このオプションは **[TURNポート多重化（TURN port multiplexing）]** が *[オン（On）]* に設定されている場合にのみ使用できます。<br><br>エンドポイントでTURNサービスを検出するには、**_turn._udp**. と **_turn._tcp** の DNS SRV レコードを作成する必要があります（必要に応じて、単一のポートでもポートの範囲でも可）。 |
| **TURN要求のポート範囲の開始（TURN requests port range start）** | **[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* の場合、このポートは大規模システム上の設定可能なポート範囲の最初のポートを表します。<br><br>デフォルトのポート範囲の開始は 3478 です。 | このオプションは、大規模システムで **[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* に設定されている場合にのみ使用できます。 |
| **TURN要求のポート範囲の終了（TURN requests port range end）** | **[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* の場合、このポートは大規模システム上の設定可能なポート範囲の上限ポートを表します。<br><br>デフォルトのポート範囲の終了は 3483 です。 | このオプションは、大規模システムで **[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* に設定されている場合にのみ使用できます。 |

| フィールド | 説明 | 使用方法のヒント |
|---|---|---|
| **委任クレデンシャル チェック（Delegated credential checking）** | TURN サーバ要求のクレデンシャル チェックをトラバーサル ゾーンを介して別の Expressway に委任できるかどうかを制御します。関連付けられている**認証レルム**によって、どのトラバーサル ゾーンが使用されるかが決まります。<br>*[オフ（Off）]*：認証チャレンジを実行する Expressway 上の該当するクレデンシャル チェックのメカニズム（ローカル データベースまたは LDAP を介して H.350 ディレクトリ）を使用します。<br>*[オン（On）]*：クレデンシャル チェックをトラバーサルクライアントに委任します。<br>デフォルトはオフです。 | 詳細については、「委任クレデンシャルチェック」を参照してください。 |
| **認証レルム（Authentication realm）** | 認証チャレンジでサーバが送信するレルム。 | クライアントのクレデンシャルがローカル認証データベースに保存されていることを確認します。 |
| **メディア ポート範囲の始端（Media port range start）** | TURN リレーの割り当てに使用するポート範囲の下限ポート。<br>デフォルトの TURN リレー メディア ポートの範囲は 24000 ～ 29999 です。 | |
| **メディア ポート範囲の末尾（Media port range end）** | TURN の割り当てに使用するポート範囲の上限ポート。 | |

### TURN サーバ ステータス

TURN サーバのステータスの概要が **[TURN]** ページの下部に表示されます。TURN サーバがアクティブになっていると、この概要には、アクティブな TURN クライアントの数とアクティブなリレーの数も表示されます。

アクティブなリレーのリンクをクリックして「TURN リレーの使用状況（TURN relay usage）」ページにアクセスします。このページには、Expressway 上で現在アクティブなすべての TURN リレーのリストが表示されます。また、アクセス許可、チャネル バインド、カウンタなどの TURN リレーの詳細も確認できます。