メンテナンス

ここでは、**[設定（Configuration）]>[メンテナンス（Maintenance）]** メニューのオプションについて説明します。

メンテナンスモードを有効にする

メンテナンス モードは通常、アップグレードが必要な場合やクラスタの一部である Expressway ピアの動作を停止する場合に使用します。これにより、他のクラスタピアは通常どおりに動作し続けますが、メンテナンス モードのピアはアップグレードまたは処理が行われます。ピアをメンテナンス モードにすると、それ以降は制御された方法で登録を中止したりコールのそのピアでの管理を中止できます。

ピアがメンテナンス モードになっている間にアラームが発生します。**「リソース使用状況（Resource usage）」** ページ（**[ステータス（Status）]>[システム（System）]>[リソース使用状況（Resource usage）]**）をモニタし、そのピアで現在処理されている登録とコールの数を確認します。

ピアがメンテナンスモードの場合、そのワークロードは他のクラスタノードによって処理されます。したがって、大規模なマルチテナント導入または MRA 導入の場合、他のノードの過負荷を回避するために、一度に 1 つのピアでのみメンテナンスモードを有効にすることをお勧めします。

アクティブコールおよび登録への影響

標準 Expressway セッション（MRA ではない）

- 新しいコールや登録は、クラスタ内の別のピアによって処理されます。
- 既存の登録は期限が切れると別のピアに登録されます（エンドポイントの設定とDNS SRV レコードのセットアップに関する詳細については、『*Expressway* クラスタ作成および保守導入ガイド』を参照してください）。
- 既存のコールはコールが終了するまで継続します。

Unified CM MRA セッション

Expresswayは、新しいコールまたはプロキシ（MRA）トラフィックの受け入れを停止します。既存のコールとチャット セッションは影響を受けません。

ユーザがセッションを正常に終了すると、システムは、特定のタイプのトラフィックを処理していない時点に到達し、そのサービスをシャットダウンします。

Expresswayがメンテナンスモード中、ユーザが新しいコールを発信または新しいチャットセッションを開始しようとすると、クライアントはサービス利用不可応答を受信し、他のピアを使用するように選択できます（可能な場合）。このフェールオーバーの動作はクライアントによって異なりますが、クラスタ内に実行中のピアがある場合、クライアントの再起動により、接続の問題を解決する必要があります。

[ユニファイドコミュニケーションのステータス（Unified Communications status）]ページには、MRA サービスが影響を受けるすべての場所（メンテナンスモード）が示されます。

メンテナンスモードを有効にするプロセス

1. 該当するピアにログインします。
2. 「メンテナンス モード（**Maintenance mode**）」ページ（**[メンテナンス（Maintenance）]**> **[メンテナンス モード（Maintenance mode）]**）に移動します。
3. **[メンテナンス モード（Maintenance mode）]** を *[オン（On）]* に設定します。
4. 確認ダイアログボックスで **[保存（Save）]** をクリックし、**[OK]** をクリックします。

（注） ピアが再起動すると、メンテナンス モードは自動的に無効になります。

手動でコールまたは登録を削除する方法

自動的にクリアしないコールまたは登録を手動で削除するには

- **[ステータス（Status）] > [コール（Calls）]** に移動して、**[すべて選択（Select all）]** をクリックし、**[切断（Disconnect）]** をクリックします（SIP コールがすぐに切断されない場合があります）。
- デバイスによる **[ステータス（Status）] > [登録（Registrations）] > [デバイスで（By device）]** に移動し、**[すべて選択（Select all）]**をクリックしてから **[登録解除（Registration）]** をクリックします。

Conference Factory の登録を終了できます。他のピアには独自の Conference Factory 登録があるため（有効になっている場合）、これはコールのソースにはならず、削除されても別のピアにロールオーバーされません。

Expressway への SSH アクセスの有効化

パスワードベースのログインを必要とすることなく安全にアクセスできるように、Expressway へのアクセスに SSH を有効にすることができます。これは一般に、モニタリングとロギングの効率を高めることを目的としています。この方法でアクセスする Expressway ごとにこの手順を繰り返す必要があります。

⚠

注意 公開キーを許可するには、root アクセスを使用します。セキュリティ上のリスクを増大させたり、サポートされていない設定をしたりしないように注意が必要です。`root` の使用は避けてください。

手順

ステップ 1 SSH を使用して `root` としてログインします。

ステップ 2 `.ssh` ディレクトリがまだない場合は、`mkdir /tandberg/.ssh` と入力して、このディレクトリを作成します。

ステップ 3 `/tandberg/.ssh` に公開キーをコピーします。

ステップ 4 `authorized_keys` ファイルに `cat /tandberg/.ssh/id_rsa.pub >> /tandberg/.ssh/authorized_keys` を使用して公開キーを追加します。

id_rsa.pub は、公開キーの名前で置き換えてください。自分のキーをほかの場所に配置しないでください。アップグレード時に失われる可能性があります（`authorized_keys` ファイルが維持されません）。

ステップ 5 ログオフし、自分のキーを使用して SSH アクセスをテストします。

自分のキーで Expressway にアクセスできない場合は、`root` として接続し、`/etc/init.d/sshd restart` を使用して SSH デーモンを再起動します。

Expressway ソフトウェアのアップグレード

ここでは、Expressway ソフトウェアコンポーネントの新しいリリースを既存のシステムにインストールする方法について説明します。コンポーネントのアップグレードは、次の 2 つの方法のいずれかで実行できます。

- **Web インターフェイスの使用 - [メンテナンス（Maintenance ）] > [アップグレード（Upgrade）]** ページを使用した推奨される方法。手順の詳細については、該当するソフトウェアのリリースノートを参照してください。
- **セキュアコピー**（SCP/PSCP）の使用 - 代替方法。この方法は、ネットワーク接続が遅い、または不安定であるなど、特定の場合に役立ちます。

ダウングレードのサポートなし

以前のバージョンへのダウングレードはサポートされていません。

セキュア コピー（SCP/PSCP）を使用したアップグレード

オプションで、このプロセスを使用して、SCP や PSCP（PuTTY無料パッケージの一部）などのセキュアコピープログラムを使用してアップグレードし、ソフトウェアイメージを含むファイルをシステムに転送します。

はじめる前に

このプロセスでは、ソフトウェアイメージファイルを、システムが期待するファイル名に手動で名前を変更する必要があります。デフォルト名（*s42700xXX_XX_XX.tar.gz* と同様）でファイルをアップロードし、アップグレードを開始（インストール）する準備ができている場合にのみ名前を変更することをお勧めします。これにより、プロセスの制御が向上し、続行する前にファイルサイズを確認できます。

ソフトウェアのバージョンによっては、*release-key* ファイルのインストールが必要な場合があります。

手順

ステップ 1 ソフトウェアイメージファイルをアップロードします。

- **システムプラットフォーム**コンポーネント の場合は、システムの /tmp フォルダにアップロードします。例：*scp s42700x12_5_7.tar.gz root@10.0.0.1:/tmp/s42700x12_5_7.tar.gz*
- 他のコンポーネントについては、ファイル名と拡張子を変更しないままシステムの */tmp/pkgs/new/* フォルダにアップロードします。例：*scp root@10.0.0.1:/tmp/pkgs/new/vcs-lang-es-es_8.1_amd64.tlp*

ステップ 2 ファイルのアップロードが完了するまで待ち、ファイルサイズを確認します。デフォルトの */tmp* での */tmp/tandgz-image.tar.gz* ファイルエントリ は 0 バイトです。

ステップ 3 アップグレードを開始する準備ができたら、ファイルの名前を */tmp/tandgz-image.tar.gz* の必要なファイル名に変更（または移動）します（アップグレードプロセスが開始されます）。

例：*mv /tmp/s42700x12_5_7.tar.gz /tmp/tandgz-image.tar.gz*

ステップ 4 プロンプトが表示されたら、root パスワードを入力します。ソフトウェアのインストールが自動的に開始され、SSH/ コンソールで「ソフトウェアアップグレード進行中」と表示されます。

ステップ 5 ソフトウェアが完全にインストールされ、「 のアップグレードが完了するまで待ちます! 新しいソフトウェアは次の再起動時」に使用されます。

ステップ 6 再起動する前に行われた設定変更は、**システムの再起動時に失われるため**、システムをすぐに再起動することをお勧めします 。

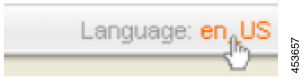
ファームウェアのアップグレード（物理アプライアンスのみ）

このセクションの説明は、Expressway が物理アプライアンス上に導入されていて、何らかの理由でファームウェアをアップグレードする必要がある場合に適用されます。

アップグレードを行うには、Cisco Host Upgrade Utility（HUU）を使用します。これは、UCS C シリーズ サーバ上のファームウェア コンポーネントをアップグレードするためのシスコの専用ツールです。HUU の使用方法について詳しくは、Cisco UCS C シリーズ ラック サーバ ドキュメント ページに用意されている最新の『*Cisco HostUpgrade* ユーティリティ ユーザ ガイド』を参照してください。

言語設定

「言語（Language）」ページ（**[メンテナンス（Maintenance）] > [言語（Language）]**）で、Web ユーザインターフェイスに表示されるテキストに使用する言語を制御します。

 453657	また、「**言語（Language）**」ページには、すべてのページの下部にある**[言語（Language）]** リンクをクリックしても移動することができます。

言語の変更

デフォルトの言語と、個々のブラウザで使用する言語の両方を設定できます。

フィールド	説明	使用方法のヒント
システムのデフォルト言語（**System default language**）	Web インターフェイスで使用されるデフォルト言語。	これは管理者セッションとユーザ（FindMe）セッションに適用されます。インストールされた言語パッケージのセットから選択できます。
このブラウザ（**This browser**）	現在のクライアント マシンの現在のブラウザで使用する言語。これは、システムのデフォルト言語か特定の代替言語のいずれかを使用するように設定できます。	この設定はクライアント コンピュータで現在使用しているブラウザに適用されます。別のブラウザまたは別のコンピュータを使用している Expressway ユーザ インターフェイスにアクセスすると、別の言語が設定されている場合があります。

言語パックのインストール

新しい言語パックをインストールしたり、既存の言語パックの更新バージョンをインストールしたりできます。

言語パックは Expressway ソフトウェア ファイルを取得したときと同じ cisco.com のエリアからダウンロードできます。使用可能なすべての言語が 1 つの言語パックの zip ファイルに含まれています。ソフトウェア リリースと一致する、適切な言語パック バージョンをダウンロードします。

言語パックをダウンロードした後に、ファイルを解凍して一連の .tlp ファイルを抽出します。サポートされている言語ごとに 1 つのファイルがあります。

使用可能な言語のリストについては、使用しているソフトウェア バージョンの関連リリース ノートを参照してください。

（注）

- 英語（en_us）はデフォルトでインストールされ、常に使用できるようになっています。
- 独自の言語パッケージは作成できません。言語パックはシスコからのみ取得できます。
- Expressway ソフトウェアの最新バージョンにアップグレードすると、「「Language pack mismatch」」のアラームが表示されます。関連付けられた言語パックの最新バージョンをインストールし、すべてのテキストが選択した言語で使用できることを確認する必要がある場合があります。

.tlp の言語パッケージ ファイルをインストールするには、次の手順を実行します。

手順

ステップ 1 **[メンテナンス（Maintenance）] > [言語（Language）]** に移動します。

ステップ 2 **[参照（Browse）]** をクリックし、アップロードする **.tlp** 言語パッケージをクリックします。

ステップ 3 [Install] をクリックします。

選択した言語パックが検証され、アップロードされます。これには数秒かかることがあります。

ステップ 4 別の言語をインストールするには、ステップ 2 と 3 を繰り返します。

言語パッケージの削除

言語パッケージを削除するには、次の手順を実行します。

手順

ステップ 1 **「言語（Language）」**ページ（**[メンテナンス（Maintenance）] > [言語（Language）]**）に移動します。

ステップ 2 インストールされた言語パックのリストから、削除する言語パッケージを選択します。

ステップ 3 [Remove] をクリックします。

ステップ 4 確認を求めるメッセージが表示された場合は、**[はい（Yes）]** をクリックします。

選択した言語パックが削除されます。これには数秒かかることがあります。

Expressway データのバックアップと復元

「バックアップと復元（Backup and restore）」ページ（**[メンテナンス（Maintenance）] > [バックアップと復元（Backup and restore）]**）を使用して、Expressway データのバックアップファイルを作成し、Expressway を以前保存した設定に復元します。

バックアップ ファイルを作成するタイミング

バックアップを定期的に作成し、さらに次の状況でも常に作成することをお勧めします。

- アップグレードを実行する前
- システムの復元を実行する前
- デモ環境およびテスト環境（既知の設定に Expressway を復元できるようにする場合）

バックアップ内容

バックアップ ファイルに保存されるデータは次のとおりです。

- ブートス トラップ キー（X8.11 以降）
- システム構成時の設定
- クラスタリング設定
- ローカル認証データ（リモートで管理するアカウントの Active Directory クレデンシャルではありません）。
  - ユーザ アカウントとパスワードの詳細
  - サーバ セキュリティ証明書と秘密キー
- コールの詳細レコード（Expressway の CDR サービスが有効になっている場合）

バックアップ ファイルには、ログ ファイルは含まれません。

バックアップと復元の手順の詳細については、「システム バックアップの作成および以前のバックアップの復元」を参照してください。

クラスタ化システム

クラスタ内のピアのバックアップと復元の詳細については、次を参照してください。

クラスタのアップグレード、バックアップ、および復元

システム バックアップの作成

はじめる前に

- バックアップファイルは常に暗号化されるようになっています（X8.11 以降）。バックアップ ファイルにはブートストラップ キー、認証データ、およびその他の機密情報が含まれるためです。
- バックアップを復元できるシステムは、**そのバックアップを作成したソフトウェアと同じバージョンを実行しているシステム**に限られます。
- ある Expressway でバックアップを作成し、別の Expressway でこのバックアップを復元することができます。たとえば、元のシステムが失敗した場合などです。復元するには、古いシステムで使用していたのと同じオプション キーを新しいシステムにインストールする必要があります。

  別の Expressway で実行したバックアップを復元しようとすると警告メッセージが表示されますが、続行できます。

（FIPS140-2 暗号化モードを使用している場合）FIPS 非準拠システムで作成されたバックアップを FIPS モードで稼動するシステム上で復元することはできません。FIPS 準拠システムのバックアップを FIPS 非準拠システム上で復元することはできます。

- Expressway 間のデータをコピーするためにバックアップを使用しないでください。使用すると、システム固有情報（IP アドレスなど）が重複します。
- バックアップ ファイルには機密情報が含まれるため、テクニカル サポートを受ける場合にこの情報をシスコに送らないでください。代わりにスナップショットと診断ファイルを使用します。

パスワード

- バックアップすべてパスワードで保護されている必要があります。
- 以前のバックアップを復元する際、そのバックアップの作成後に管理者アカウントのパスワードが変更されている場合は、復元後最初にログインするときに、古いパスワードを入力する必要があります。
- Active Directory のクレデンシャルは、システムのバックアップ ファイルに含まれて**いません**。NTLM のデバイス認証を使用する場合は、Active Directory のパスワードを入力して復元後に Active Directory ドメインに再参加する必要があります。
- バックアップと復元するためには、緊急アカウントのパスワードを標準的な管理者アカウント パスワードと同じように処理します。

プロセス

Expressway システム データのバックアップを作成するには、次の手順を実行します。

手順

ステップ 1 **[メンテナンス（Maintenance）] > [バックアップと復元（Backup and Restore）]** に移動します。

ステップ 2 [暗号化パスワード（Encryption password）] に、バックアップ ファイルの暗号化に使用するパスワードを入力します。

注意 バックアップファイルを復元する際は、このパスワードが必要になります。

ステップ 3 [システム バックアップ ファイルの作成（Create system backup file）] をクリックします。

ステップ 4 バックアップ ファイルが作成されるまで待機します。これには数分かかることがあります。ファイルが準備されている間は、このページから移動しないでください。

ステップ 5 バックアップ ファイルが作成されると、ファイルを保存するように求められます。デフォルトのファイル名では次の形式が使用されます：**<software version><hardware serial number><date><time>_backup.tar.enc** Internet Explorer を使用している場合、デフォルトのファ

イル拡張子は **.tar.gz.gz** となります。（ファイル名の拡張子がこのように異なっても運用上の影響はありません。サポート対象のブラウザを使用してバックアップ ファイルを作成し、復元できます。）

ステップ 6 セキュアな場所にバックアップ ファイルを保存します。

以前のバックアップの復元

はじめる前に

⚠

注意 CE1100 またはそれ以前のアプライアンスのバックアップから CE1200 アプライアンスに Expressway-E を復元する場合、CE1200 アプライアンスは Expressway-C として復元される場合があります。この問題が発生するのは、CE1100 または以前のアプライアンスでサービス セットアップ ウィザードを使用してタイプを Expressway-C に変更した後、ウィザードをスキップして設定を完全に完了しなかった場合です。この問題を回避するには、アプライアンスをバックアップする前に、サービス セットアップ ウィザードを実行してタイプを Expressway-E に変更し、ウィザードを完了するようにしてください。

- 復元するバックアップ ファイルのパスワードが必要です。
- 別の Expressway からバックアップファイルを復元する場合は、復元元のシステムに存在しているのと同じライセンスキーを適用する必要があります。
- 復元を実行する前に、Expressway ユニットのサービスを停止の状態にすることを推奨します。
- 復元プロセスには、元のソフトウェアバージョンに戻す**初期設定へのリセット**が含まれます。その後、**バックアップの作成時に実行していたのと同じソフトウェアバージョン**へのアップグレードを行います。
- バックアップが古い場合（希望するバージョンよりも以前のバージョンで作成されていた場合）は、復元後に次の追加手順を実行する必要があります。
  1. ソフトウェア バージョンを必要な最新バージョンにアップグレードします。
  2. バックアップの作成後に加えられたすべての設定変更を手動でやり直します。
- （FIPS140-2 暗号化モードを使用している場合）FIPS 非準拠システムで作成されたバックアップを FIPS モードで稼動するシステム上で復元することはできません。FIPS 準拠システムのバックアップを FIPS 非準拠システム上で復元することはできます。
- システムがクラスタの一部である場合には Expressway にデータを復元できません。クラスタから最初に削除する必要があります。詳細については、クラスタのアップグレード、バックアップ、および復元を参照してください。

パスワード

- バックアップはパスワードで保護されている必要があります。
- 以前のバックアップを復元する際、そのバックアップの作成後に管理者アカウントのパスワードが変更されている場合は、復元後最初にログインするときに、古いパスワードを入力する必要があります。
- Active Directory のクレデンシャルは、システムのバックアップ ファイルに含まれて**いません**。NTLM のデバイス認証を使用する場合は、Active Directory のパスワードを入力して復元後に Active Directory ドメインに再参加する必要があります。
- バックアップと復元するためには、緊急アカウントのパスワードを標準的な管理者アカウント パスワードと同じように処理します。

プロセス

Expressway を以前の設定のシステム データに復元するには、次の手順を実行します。

手順

ステップ 1 最初に、「デフォルト設定の復元（初期設定へのリセット）」の手順に従って初期設定にリセットします。これにより、設定データが削除され、システムが元の状態に戻ります。システムを最初にセットアップしてからアップグレードしている場合は、リセットしても現在のソフトウェア バージョンが維持されます。

ステップ 2 バックアップの作成時に実行していたのと同じソフトウェア バージョンにシステムをアップグレードします。

- スタンドアロン システムについては、「アップグレード手順」を参照してください。
- クラスタ化システムの場合は、『*Expressway Cluster Creation and Maintenance Deployment Guide*』を参照してください。

ステップ 3 これで次のようにバックアップからシステムを復元することができます。

1. **[メンテナンス（Maintenance）]** > **[バックアップと復元（Backup and Restore）]** に移動します。
2. **[復元（Restore）]** セクションで **[参照（Browse）]** をクリックし、復元するバックアップ ファイルを選択します。
3. **[復号パスワード（Decryption password）]** フィールドに、バックアップ ファイルの作成に使用したパスワードを入力します。
4. [システム バックアップ ファイルのアップロード（Upload system backup file）] をクリックします。

5. Expressway がファイルを確認した後、「**復元の確認（Restore confirmation）**」ページが表示されます。
   - バックアップ ファイルが無効である場合、または誤った復号パスワードが入力された場合は、**[バックアップと復元（Backup and restore）]** の上部にエラー メッセージが表示されます。
   - 現在のソフトウェア バージョンとコール数と登録数が表示されます。
6. 表示される警告メッセージを確認してから続行します。
7. 復元を続行するには、**[システムの復元を続行する（Continue with system restore）]** をクリックします。

   これにより、システムが再起動するため、アクティブ コールがないことを確認します。
8. システムの再起動後、「**ログイン（Login）**」ページが表示されます。

ステップ 4 バックアップ ファイルが古い場合のみ、この手順が適用されます。つまり、バックアップの作成後にソフトウェアバージョンがアップグレードされた場合、システム設定が変更された場合です。この場合、次のように計算します。

1. システムを再びアップグレードします。この場合は、システムに必要なソフトウェア バージョンにアップグレードします。
2. バックアップ後に加えた設定変更をやり直します（復元したシステムでその変更がまだ必要な場合）。

パターンの効果の確認

[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）]**）では、Expressway に設定するパターンまたはトランスフォーメーションで期待した結果を得られるかどうかをテストできます。

次の設定時にパターンを使用できます。

- トランスフォーメーションで何らかの検索を実行する前に変換するエイリアスを指定する
- 検索ルールで検索するエイリアスに基づいて検索をフィルタリングし、検索をゾーンに送信する前にエイリアスを変換する

このツールを使用するには、次の手順を実行します。

手順

ステップ 1 トランスフォーメーションに対してテストする **[エイリアス（Alias）]** を入力します。

ステップ 2 **[パターン（Pattern）]** セクションで、テストする **[パターン文字列（Pattern string）]** の **[パターン タイプ（Pattern type）]** と **[パターン動作（Pattern behavior）]** の組み合わせを入力します。

- **[パターン動作（Pattern behavior）]** に *[置換（Replace）]* を選択した場合は、**[置換文字列（Replace string）]** も入力する必要があります。
- **[パターン動作（Pattern behavior）]** に *[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）]* を選択した場合は、**[パターン文字列（Pattern string）]** の前または後ろに追加する **[追加テキスト（Additional text）]** 文字列も入力する必要があります。
- 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パターン マッチング変数が備わっています。

ステップ 3 **[パターンの確認（Check pattern）]** をクリックし、エイリアスがパターンと一致するかどうかをテストします。

[結果（Result）] セクションに、エイリアスがパターンと一致するかどうかが示され、結果のエイリアス（該当する場合はトランスフォーメーションの効果も含む）が表示されます。

エイリアスの検出

[検索（Locate）] ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[検索（Locate）]**）では、Expressway が指定したエイリアスで識別されたエンドポイントを、指定した「ホップ」回数以内に、そのエンドポイントに実際にコールを発信することなく検出できるかどうかをテストできます。

このツールは、ダイヤル プランやネットワーク導入の問題を診断する際に役立ちます。

手順

ステップ 1 検索する **[エイリアス（Alias）]** を入力します。

ステップ 2 検索の **[ホップ カウント（Hop count）]** を入力します。

ステップ 3 検索を開始するために使用する **[プロトコル（Protocol）]** として *[H.323]* または *[SIP]* のいずれかを選択します。検索プロセス時に検索がインターワーキングされる可能性がありますが、Expressway は常にネイティブ プロトコルを最初に使用して検索ルールと関連付けられた同じプライオリティのターゲット ゾーンとポリシー サービスを検索してから、代替プロトコルを使用して、それらのゾーンを再度検索します。

ステップ 4 検索要求をシミュレーションする **[ソース（Source）]** を選択します。*[デフォルトゾーン（Default Zone）]*（不明なリモート システム）、*[デフォルトサブゾーン（Default Subzone）]*（ローカルに登録されたエンドポイント）、またはそのほかの設定済みのゾーンまたはサブゾーンから選択します。

ステップ 5 要求を **[認証済み（Authenticated）]** として処理するかどうかを選択します（認証されたメッセージのみに適用するように検索ルールを制限できます）。

ステップ 6 任意で、[送信元エイリアス（Source alias）] を入力することができます。通常、これは、送信元エイリアスに依存するルールがある CPL をルーティング プロセスで使用している場合にのみ関係します（値が指定されていない場合は、デフォルトのエイリアスの `xcom-locate` が使用されます）。

ステップ 7 **[検索（Locate）]** をクリックして検索を開始します。

ステータス バーに **[検索しています...（Searching...）]** と表示され、その後に **[検索が完了しました（Search completed）]** と表示されます。結果には、検索したゾーンのリスト、適用したトランスフォーメーションとコール ポリシー、検出された場合はエイリアスが存在するゾーンが含まれます。

検索プロセスは、選択した **[送信元ゾーン（Source zone）]** から Expressway がコール要求を受信したかのように実行されます。詳細については、「コールルーティングプロセス」の項を参照してください。

ポートの使用

[メンテナンス（Maintenance）] > **[ツール（Tools）]** > **[ポートの使用状況（Port usage）]** メニューのページは、Expressway で設定されたすべての IP ポートが表形式で表示されます。

これらのページに表示される情報は、その特定の Expressway に固有のもので、Expressway の設定、インストールされたオプション キー、および有効になっている機能によって異なります。

情報はページのどの列ででも並べ替えることができ、IP ポート別や IP アドレス別にリストをソートできます。

各ページには **[CSV にエクスポート（Export to CSV）]** オプションがあります。これによって、スプレッドシート アプリケーションで開くのに適した CSV（カンマ区切り値）形式のファイルに情報を保存できます。

IP ポートは IPv4 アドレスおよび IPv6 アドレス用に個別に設定できません。また、2 つの LAN インターフェイスのそれぞれに設定することもできません。つまり、これは、IP ポートを特定のサービス（SIP、UDP など）用に設定した後は、Expressway 上のそのサービスのすべての IP アドレスに適用されます。これらのページの表にはすべての IP ポートとすべての IP アドレスのリストが表示されるため、Expressway の設定によっては、単一の IP ポートが最大 4 回リストに表示される場合があります。

ポート情報は次のページに分割されています。

- ローカル インバウンド ポート
- ローカル アウトバウンド ポート
- リモート リスニング ポート

また、Expressway-E では、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 ポートも **[設定（Configuration）]** > **[トラバーサル（Traversal）]** > **[ポート（Ports）]** で設定できます。

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。

ローカル インバウンド ポート

「ローカル インバウンド ポート（Local inbound ports）」ページ（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[ポートの使用状況（Port usage）]** > **[ローカルインバウンド ポート（Local inbound ports）]**）には、ほかのシステムからインバウンド通信を受信するために使用する Expressway 上のリスニング IP ポートが表示されます。

このページのリストに表示された各ポートについては、Expressway とインバウント通信の送信元の間にファイアウォールがある場合、そのファイアウォールは次を許可する必要があります。

- インバウンド通信の送信元から Expressway 上の IP ポートへの着信トラフィック
- その同じ Expressway IP ポートからインバウンド通信の送信元に返すリターン トラフィック

（注） このファイアウォールの設定は、この Expressway がトラバーサルクライアントまたはトラバーサルサーバの場合、Expressway ファイアウォールトラバーサルが正しく機能するために特に重要です。

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。

ローカル アウトバウンド ポート

「ローカル アウトバウンド ポート（Local outbound ports）」ページ（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[ポートの使用状況（Port usage）]** > **[ローカル アウトバウンドポート（Local outbound ports）]**）には、ほかのシステムへのアウトバウンド通信を送信するために使用する Expressway 上の送信元 IP ポートが表示されます。

このページにリストされた各ポートについては、Expressway とアウトバウント通信の宛先の間にファイアウォールがある場合、そのファイアウォールは次を許可する必要があります。

- Expressway の IP ポートからアウトバウンド通信の宛先へのアウトバウンドトラフィック
- その宛先から同じ Expressway IP ポートへのリターントラフィック

（注） このファイアウォールの設定は、このExpresswayがトラバーサルクライアントまたはトラバーサルサーバの場合、Expresswayファイアウォールトラバーサルが正しく機能するために特に重要です。

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。

リモート リスニング ポート

「リモート リスニング ポート（Remote listening ports）」ページ（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ポートの使用状況（Port usage）] > [リモートリスニングポート（Remote Listening ports）]**）には、Expressway と通信するリモートシステムの宛先 IP アドレスと IP ポートが表示されます。

ファイアウォールは、このページのリストに表示された IP アドレスと IP ポートで識別されたローカル Expressway からリモート デバイスへのトラフィックを許可するように設定する必要があります。

（注） このリストに表示されていない、Expresswayがメディアやシグナリングを送信する他のリモートデバイスもありますが、これらのデバイスがExpresswayからのトラフィックを受信するポートは宛先デバイスの設定によって決まります。そのため、それらのポートはこのリストに表示できません。[ローカル アウトバウンド ポート] ページにリストされているすべてのポートを開いている場合、Expressway はすべてのリモート ポートと通信できます。こらのリモート システムとポートにファイアウォール上で開く IP ポートを制限する場合は、このページの情報のみが必要です。

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。

再起動、リブート、およびシャットダウン

「再起動オプション（Restart options）」ページ（**[メンテナンス（Maintenance）]>[再起動オプション（Restart options）]**）を使用すると、ハードウェアに物理的にアクセスすることなく、Expressway を再起動、リブート、またはシャットダウンできます。

注意 ユニットの前面の赤のALM LEDがオンになっている間はExpresswayを再起動、リブート、またはシャットダウンしないでください。これは、ハードウェア障害を示しています。シスコのカスタマー サポート担当者に連絡してください。

再起動

再起動機能は Expressway アプリケーション ソフトウェアをシャットダウンして再起動しますが、オペレーティング システムやハードウェアのシャットダウンおよび再起動は行いません。再起動には約 3 分かかります。

通常、何らかの設定変更を有効にしたり、クラスタに対してシステムを追加または削除する場合に再起動が必要です。このような場合はシステム アラームが発生し、システムが再起動されるまではそのままです。

Expressway がクラスタの一部であり、クラスタ内の他のピアも再起動を必要としている場合は、各ピアが再起動するまで次のピアの再起動を待つことを推奨します。

リブート

リブート機能は Expressway アプリケーション ソフトウェア、オペレーティング システム、およびハードウェアをシャットダウンし、再起動します。リブートには約 5 分かかります。

リブートは、通常はソフトウェア アップグレードの後にのみ必要で、アップグレード プロセスの一部として実行されます。予期しないシステム エラーを解決しようとしているときにも、リブートが必要になる場合があります。

シャットダウン

シャットダウンは、通常、メンテナンスまたは再配置の前にユニットのプラグを抜く場合に必要になります。プラグを抜く前にシステムをシャットダウンする必要があります。特に、通常運用時のシステムへの電源を取り外す場合に、制御されていないシャットダウンは避けてください。

アクティブ コールへの影響

これらの再起動オプションのいずれかによって、すべてのアクティブ コールが終了されます。（Expressway がクラスタの一部である場合は、Expressway がシグナリングを取得しているコールのみが終了されます）。

そのため、**[システム ステータス（System status）]** には現在のコールの数が表示されるため、システムを再起動する前にそれらの数を確認できます。システムをすぐに再起動しない場合は、再起動前にこのページを更新し、コールの現在のステータスを確認してください。

[Mobile & Remote Access] が有効になっている場合、現在プロビジョニングされているセッションの数が表示されます（Expressway-C のみ）。

Web インターフェイスを使用した再起動、リブート、およびシャットダウン

Web インターフェイスを使用して Expressway を再起動するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]** > **[再起動オプション（Restart options）]** に移動します。
2. 現在実行されているコールの数を確認します。
3. 必要に応じて **[再起動（Restart）]**、**[リブート（Reboot）]**、または **[シャットダウン（Shutdown）]** をクリックし、アクションを確認します。

場合によっては、これらのオプションのうち 1 つのみ（たとえば **[再起動（Restart）]** など）を使用できます。これは、通常、アラームまたはバナーメッセージ内のリンクに従った後で「**再起動オプション（Restart options**）」ページにアクセスすると発生します。

- 再起動またはリブート：**[再起動しています（Restarting）] または [リブートしています（Rebooting）]** ページが表示され、オレンジ色のバーで進捗状況が示されます。

  システムが正常に再起動またはリブートされると、「**ログイン（Login**）」ページが表示されます。

- シャットダウン：[シャットダウン中（Shutting down）] ページが表示されます。

  このページは、システムが正常にシャットダウンした後もそのまま表示されますが、このページを更新しようとしたり、Expressway へアクセスしようとしても失敗します。