登録制御

登録について

Expressway を H.323 ゲートキーパーまたは SIP レジストラとして使用するエンドポイントでは、そのエンドポイントを最初に Expressway に登録する必要があります。Expressway は、次のメカニズムを使用して登録を許可するデバイスを制御するように設定できます。

- エンドポイントが提供するユーザ名とパスワードに基づくデバイス認証プロセスです。
- 許可リストと拒否リストについてを使用した登録制限ポリシーの設定、または Expressway に登録できるエイリアスと登録できないエイリアスを指定するための外部ポリシーサービスです。
- サブゾーンメンバーシップ ルールとサブドメイン登録ポリシーを指定した、IP アドレスおよびサブネット範囲に基づく制限です。

これらのメカニズムは併用できます。たとえば、社内ディレクトリからエンドポイントの ID を確認するために認証を使用し、これらの認証済みのエンドポイントのうちのどれが特定の Expressway に登録できるかを制御するために登録制限を使用できます。

また、次のようなプロトコル固有の一部の動作も制御できます。

- H.323 登録に対する **[登録競合モード（Registration conflict mode）]** 設定と **[自動検出（Auto discover）]** 設定
- **[SIP 登録プロキシ モード（SIP registration proxy mode）]**（SIP 登録用）

クラスタ内のピア間での登録の管理方法に関する特定の情報については、「ピア間での登録の共有」の項を参照してください。

ユニファイドコミュニケーション導入環境では、SIP デバイスのエンドポイント登録は Unified CM により行われることがあります。このシナリオでは、Expressway が Unified CM 登録にセ

キュアなファイアウォールトラバーサルと回線側サポートを提供します。ドメイン設定時は、ドメインに登録とプロビジョニングのサービス提供元を Cisco Unified Communications Manager と Expressway から選択できます。

登録する Expressway の検出

エンドポイントを Expressway に登録する前に、登録できる、または登録が必要な Expressway を特定する必要があります。エンドポイントでこの設定を行いますが、プロセスは SIP と H.323 で異なります。

（注） たとえば、[MRA] を選択すると、**[登録（Registration）]** タブを無効にしても、Expressway E はデバイスを登録します。

MCU、ゲートウェイ、コンテンツサーバの登録

ゲートウェイ、MCU、コンテンツ サーバなどの H.323 システムも Expressway に登録できます。これらは、ローカルに登録されたサービスと呼ばれます。これらのシステムは、登録時に Expressway に提供する独自のプレフィックスを使用して設定されます。これにより、Expressway はそのプレフィックスで始まるすべてのコールを必要に応じてゲートウェイ、MCU、またはコンテンツ サーバにルーティングすることを認識します。また、これらのプレフィックスは登録の制御にも使用できます。

SIP デバイスはプレフィックスを登録できません。ダイヤル プランで SIP デバイスには特定のプレフィックスを介して到達するように指定している場合は、使用するプレフィックスと等しいパターン マッチを使用して、検索ルールを関連付けたネイバー ゾーンとしてデバイスを追加する必要があります。

登録制限ポリシーの設定

「登録設定（Registration configuration）」ページ（**[設定（Configuration）]** > **[登録（Registration）]** > **[設定（Configuration）]**）を使用して、Expressway による登録の管理方法を制御します。

[制限ポリシー（Restriction policy）] オプションは、Expressway に登録できるエンドポイントの決定時に使用するポリシーを指定します。次のオプションがあります。

- *[なし（None）]*：どのエンドポイントも登録できます。
- *[許可リスト（Allow List）]*：[許可リスト（Allow List）] 内のエントリに一致するエイリアスを持つエンドポイントのみが登録できます。
- *[拒否リスト（Deny List）]*：[拒否リスト（Deny List）] のエントリに一致しない限り、すべてのエンドポイントが登録できます。

- *[*ポリシーサービス（*Policy service*）*]*：外部ポリシーサービスで許可された詳細を使用して登録するエンドポイントのみが登録できます。

デフォルトは [なし（None）] です。

また、*[*許可リスト（*Allow List*）*]* または *[*拒否リスト（*Deny List*）*]* を使用する場合は、適切な [登録許可リスト（Registration Allow List）] の設定 または [登録拒否リスト（Registration Deny List）] の設定 の設定ページに移動してリストを作成する必要があります。

すべての登録制限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登録ポリシーの設定を参照してください。

エイリアスの登録

デバイス登録プロセス（必要な場合）が完了した後、エンドポイントはそのエイリアスを Expressway に登録しようと試みます。

H.323

登録時に H.323 エンドポイントは次のうちの 1 つ以上を Expressway に提供します。

- 1 つ以上の H.323 ID
- 1 つ以上の E.164 エイリアス
- 1 つ以上の URI

登録済みの他のエンドポイントのユーザは、これらのエイリアスのいずれかをダイヤルすることでそのエンドポイントをコールできます。

- URI を使用して H.323 エンドポイントを登録することを推奨します。これにより、SIP エンドポイントは標準として URI を使用して登録されるため、SIP と H.323 間のインターワーキングが促進されます。
- 機密情報を公開するエイリアスは使用しないでください。H.323 の特性上、コールセットアップ情報は暗号化されていない形式で交換されます。

SIP

登録時に SIP エンドポイントは、連絡先アドレス（IP アドレス）と論理アドレス（レコードのアドレス）を Expressway に提供します。論理アドレスは、そのエンドポイントのエイリアスと見なされ、一般的に URI の形式をとります。

H.350 ディレクトリの認証と登録

Expressway が H.350 ディレクトリ サービスを使用して登録要求を認証する場合、**[登録用エイリアスの送信元（Source of aliases for registration）]** の設定を使用して、エンドポイントによ

る登録の試行を許可するエイリアスを特定します。詳細については、「「LDAP 経由の H.350 ディレクトリ サービス ルックアップの使用」」を参照してください。

既存のエイリアスを使用した登録の試行

エンドポイントは、システムにすでに登録されているエイリアスを使用して Expressway に登録しようとする場合があります。これをどのように管理するかは、Expressway がどのように設定されているかと、エンドポイントが SIP か H.323 かによって異なります。

- **H.323**：H.323 エンドポイントは、別の IP アドレスから Expressway にすでに登録されているエイリアスを使用して Expressway に登録しようとする可能性があります。この場合に Expressway の動作を制御するには、「H.323」ページ（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）で **[登録競合モード（Registration conflict mode）]** を設定します。
- **SIP**：SIP エンドポイントには、別の IP アドレスからすでに使用されているエイリアスを使用した登録が常に許可されます。このエイリアス宛のコールを受信すると、そのエイリアスを使用して登録されているすべてのエンドポイントが同時にコールされます。この SIP 機能は「「フォーキング」」と呼ばれます。

登録のブロック

[登録拒否リスト（Registration Deny List）] の設定 を使用するように Expressway を設定している場合は、登録をブロックするオプションがあります。このオプションはそのエンドポイントが使用するすべてのエイリアスを [拒否リスト（Deny List）] に追加します。

既存の登録の削除

制限ポリシーはアクティブになると、その時点以降のすべての登録要求を制御します。ただし、既存の登録は、新しいリストがブロックしても、そのまま残ります。したがって、制限ポリシーを実装した後は、既存の不要な登録すべてを手動で削除することを推奨します。

登録を手動で削除するには、**[ステータス（Status）]** > **[登録（Registrations）]** > **[デバイスごと（By device）]** に移動し、削除する登録を選択して **[登録解除（Unregister）]** をクリックします。

登録されているデバイスがアクティブ コールに参加しており、その登録を削除した（または期限が切れた）場合、コールへの影響はプロトコルによって次のように異なります。

- **H.323**：コールが停止します。
- **SIP**：デフォルトでは、コールは有効な状態のままになります。SIP の動作は変更できますが、CLI で `xConfiguration SIP Registration Call Remove` コマンドを使用する必要があります。

再登録

すべてのエンドポイントは定期的に Expressway に再登録し、登録を有効状態に維持する必要があります。手動で登録を削除しない場合は、エンドポイントが再登録をしようとした時点で

削除されますが、これは、エンドポイントが使用しているプロトコルによって次のように異なります。

- H.323 エンドポイントは「「軽量の」」再登録を使用することがあります。これには、最初の登録で提供されたすべてのエイリアスは含まれておらず、再登録が制限ポリシーによってフィルタリングされない可能性があります。この場合、登録は登録タイムアウト期間の終了時に期限切れにならないため、手動で削除する必要があります。
- SIP の再登録には、最初の登録と同じ情報が含まれるため、制限ポリシーによってフィルタリングされます。つまり、リストがアクティブになった後にすべての SIP アプリケーションが登録タイムアウト期間の終了時点で表示されなくなります。

再登録の頻度は、[SIP]（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[SIP]**）の **[登録制御（Registration controls）]** の設定と、[H.323]（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）の **[存続時間（Time to live）]** の設定で決まります。

（注） 登録の存続時間を短縮しすぎると、登録要求が Expressway へ大量に送り付けられるリスクがあり、パフォーマンスに重大な影響を及ぼします。この影響はエンドポイントの数に比例します。したがって、パフォーマンスを良好に保つ必要性に対して、不定期に発生するフェールオーバーの必要性とのバランスをとることが必要です。

許可リストと拒否リストについて

エンドポイントが Expressway への登録を試行するときに、エイリアスのリストを提供します。Expressway が提供する登録を許可するエンドポイントを制御するための方法の 1 つは、**[制限ポリシー（Restriction policy）]** ページ（「登録制限ポリシーの設定」）を *[許可リスト（Allow List）]* または *[拒否リスト（Deny List）]* に設定してから、必要に応じて [許可リスト（Allow List）] か [拒否リスト（Deny List）] のエンドポイントのエイリアスのいずれかを含めることです。各リストには、最大で 2,500 のエントリを含めることができます。

エンドポイントが登録を試行すると、エイリアスのそれぞれが関連リストのパターンと比較され、一致するかどうかが確認されます。登録を許可または拒否するために [許可リスト（Allow List）] または [拒否リスト（Deny List）] に表示されるエイリアスは 1 つのみである必要があります。

たとえば、**[制限ポリシー（Restriction policy）]** が *[Deny List（拒否リスト）]* に設定されており、エンドポイントが 3 つのエイリアスを使用して登録しようとした場合にそのうちの 1 つが [Deny List（拒否リスト）] のパターンに一致していれば、そのエンドポイントの登録は拒否されます。同様に、**[制限ポリシー（Restriction policy）]** が *[Allow List（許可リスト）]* に設定されている場合にそれらすべてのエイリアスを使用した登録が許可されるには、エンドポイントのエイリアスの 1 つのみが [Allow List（許可リスト）] のパターンに一致する必要があります。

[許可リスト（Allow List）] と [拒否リスト（Deny List）] は相互に排他的です。使用できるのは常にどちらか 1 つです。また、サブゾーン レベルでも登録を制御できます。各サブゾーンの

登録ポリシーは、サブゾーン メンバーシップ ルールを介して割り当てられた登録を許可または拒否するように設定できます。

[登録許可リスト（Registration Allow List）] の設定

「登録許可リスト（Registration Allow List）」ページ（**[設定（Configuration）] > [登録（Registration）] > [Allow List（許可リスト）]**）には、Expressway への登録が許可されるエンドポイントのエイリアスとエイリアスパターンが表示されます。登録を許可するには、[許可リスト（Allow List）] のエントリにエンドポイントのエイリアスの 1 つが一致している必要があります。

[許可リスト（Allow List）] を使用するには、「登録制限ポリシーの設定」ページにある *[Allow List（許可リスト）]* の **[制限ポリシー（Restriction policy）]** を選択する必要があります。

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
説明 （Description）	エントリの任意の自由形式の説明。	
パターン タイプ（Pattern type）	**[パターン文字列（Pattern string）]** とエイリアスを一致させる方法。 次のオプションがあります。 *[完全一致（Exact）]*：エイリアスはパターン文字列に正確に一致する必要があります。 *[プレフィックス（Prefix）]*：エイリアスはパターン文字列で開始される必要があります。 *[サフィックス（Suffix）]*：エイリアスはパターン文字列で終了する必要があります。 *[正規表現（Regex）]*：パターン文字列は正規表現です。	パターンが特定のエイリアスに一致するかどうかは、[パターンの確認（Check pattern）] ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [パターンの確認（Check pattern）]**）を使用してテストできます。
パターン文字列（Pattern string）	エイリアスと比較するパターン。	

[登録拒否リスト（Registration Deny List）] の設定

「登録拒否リスト（Registration Deny List）」ページ（**[設定（Configuration）] > [登録（Registration）] > [Deny List（拒否リスト）]**）は、Expressway への登録が許可されないエンドポイントのエイリアスとエイリアスパターンが表示されます。登録を拒否するには、[拒否リスト（Deny List）] のエントリにエンドポイントのエイリアスの 1 つのみが一致している必要があります。

[拒否リスト（Deny List）] を使用するには、登録制限ポリシーの設定ページにある *[Deny List（拒否リスト）]* の **[制限ポリシー（Restriction policy）]** を選択する必要があります。

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
説明 （Description）	エントリの任意の自由形式の説明。	
パターン タイプ（Pattern type）	**[パターン文字列（Pattern string）]** とエイリアスを一致させる方法。 次のオプションがあります。 *[完全一致（Exact）]*：エイリアスはパターン文字列に正確に一致する必要があります。 *[プレフィックス（Prefix）]*：エイリアスはパターン文字列で開始される必要があります。 *[サフィックス（Suffix）]*：エイリアスはパターン文字列で終了する必要があります。 *[正規表現（Regex）]*：パターン文字列は正規表現です。	パターンが特定のエイリアスに一致するかどうかは、[パターンの確認（Check pattern）] ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[パターンの確認（Check pattern）]**）を使用してテストできます。
パターン文字列（Pattern string）	エイリアスと比較するパターン。	

外部サービスを使用するための登録ポリシーの設定

すべての登録制限ポリシーの決定を外部サービスを参照するように登録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）]** > **[登録（Registration）]** > **[設定（Configuration）]** に移動します。

ステップ 2 *[ポリシー サービス（Policy service）]* の **[制限ポリシー（Restriction policy）]** を選択します。

ステップ 3 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
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 *HTTPS* 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）	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。
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 **:<port>** 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。「ポリシーサーバのステータスと復元力」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。	

フィールド	説明（Description）	使用方法のヒント
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、「ポリシーサービスのデフォルト CPL」を参照してください。

ステップ 4 [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、登録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。

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。