



## MSDP の設定

この章では、IE 3000 スイッチに Multicast Source Discovery Protocol (MSDP) を設定する手順について説明します。MSDP により、複数の Protocol-Independent Multicast Sparse-Mode (PIM-SM; Protocol-Independent Multicast sparse (疎) モード) ドメインが接続されます。

このソフトウェア リリースでは、MSDP と密接に連携する Multicast Border Gateway Protocol (MBGP) がサポートされていないため、MSDP は完全にはサポートされていません。ただし、MBGP が動作していない場合は、MSDP と連携して動作するデフォルト ピアを作成できます。

この機能を使用するには、スイッチが IP サービス イメージを実行している必要があります。



(注)

この章で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2』を参照してください。

この章で説明する内容は、次のとおりです。

- 「MSDP の概要」(P.50-1)
- 「MSDP の設定」(P.50-3)
- 「MSDP のモニタおよびメンテナンス」(P.50-18)

## MSDP の概要

MSDP を使用すると、さまざまなドメイン内のすべての Rendezvous Point (RP; ランデブー ポイント) に、グループのマルチキャスト送信元を通知できます。各 PIM-SM ドメインは独自の RP を使用し、他のドメインの RP には依存しません。RP は Transmission Control Protocol (TCP; 伝送制御プロトコル) を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応装置と MSDP ピアリング関係にあります。このピアリング関係は、TCP 接続を介して確立されます。この関係では、主に、マルチキャストグループの送信元のリストが交換されます。RP 間の TCP 接続は、基本的なルーティングシステムによって実現されます。受信側の RP では、送信元リストを使用して送信元パスを確立します。

このトポロジの目的は、ドメインが他のドメイン内のマルチキャスト送信元を検出できるようにすることです。レシーバーが配置されているドメインをマルチキャスト送信元が対象としている場合、マルチキャスト データは PIM-SM の通常の送信元ツリー構築メカニズムを通じて配信されます。MSDP は、グループの送信元をアナウンスする場合にも使用します。このアナウンスは、ドメインの RP で発信する必要があります。

MSDP のドメイン間の動作は、Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) または MBGP に大きく依存します。ドメイン内の RP (グローバル グループの送信元をインターネットにアナウンスするための RP) で、MSDP を実行することを推奨します。

## MSDP の動作

図 50-1 に、2 つの MSDP ピア間での MSDP の動作を示します。Protocol Independent Multicast (PIM) では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP を使用します。MSDP が設定されている場合、次のシーケンスが発生します。

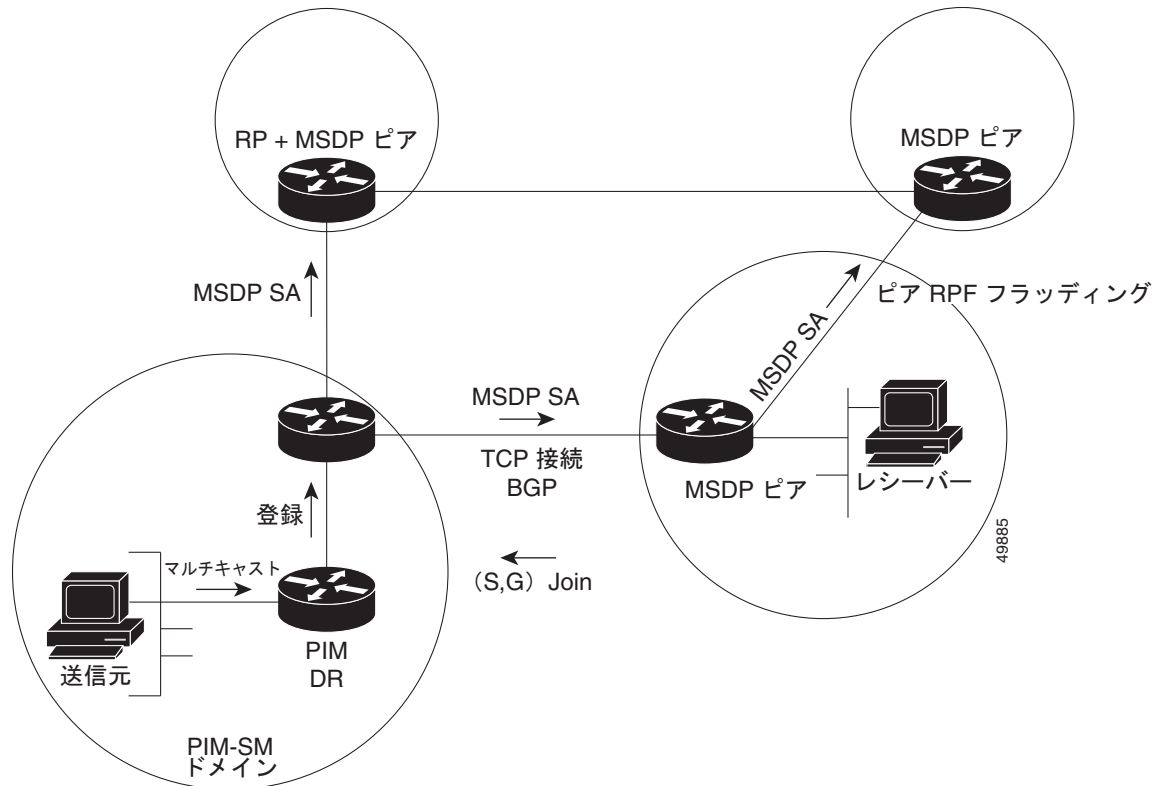
送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続されたファーストホップ ルータ (指定ルータまたは RP) が PIM 登録メッセージを RP に送信します。RP は、この登録メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active (SA) メッセージもすべての MSDP ピアに転送されます。送信元、送信元の送信先グループ、および RP のアドレスまたは送信元 ID (RP アドレスとして使用されるインターフェイスの IP アドレス) が設定されている場合は、SA メッセージによってこれらが識別されます。

各 MSDP ピアは SA メッセージを発信元 RP から受信および転送し、ピア Reverse-Path Flooding (RPF) を実現します。MSDP 装置は、BGP または MBGP ルーティング テーブルを調べ、SA メッセージの発信元 RP へのネクストホップであるピアを検出します。このようなピアは、Reverse-Path Forwarding (RPF) ピアと呼びます。MSDP 装置は、RPF ピア以外のすべての MSDP ピアにメッセージを転送します。BGP および MBGP がサポートされていない場合に MSDP ピアを設定する方法については、「デフォルトの MSDP ピアの設定」(P.50-4) を参照してください。

MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージを廃棄します。それ以外の場合、MSDP ピアは、すべての MSDP ピアにメッセージを転送します。

ドメインの RP は、MSDP ピアからの SA メッセージを受信します。SA メッセージに記述されたグループの Join 要求を RP が受信し、空でない出力インターフェイス リストに (\*,G) エントリが存在する場合、そのグループはドメインの対象となり、RP は (S,G) Join を送信元にトリガーします。(S,G) Join が送信元の Designated Router (DR; 指定ルータ) に到達すると、送信元ツリーのブランチが送信元からリモート ドメイン内の RP に構築されます。この結果、マルチキャスト トラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバーへと送信できます。

図 50-1 RP ピア間での MSDP の動作



## MSDP の利点

MSDP には、次のような利点があります。

- 共有のマルチキャスト分散ツリーが分割されるので、共有ツリーがドメインに対してローカルになるように設定できます。ローカルメンバーはローカルツリーに加わります。共有ツリーへの Join メッセージをドメイン外に送信する必要はありません。
- PIM sparse (疎) モードドメインは独自の RP だけに依存するため、他のドメインの RP に対する依存度は低くなります。このため、送信元の情報がドメイン外部に漏れないようにすることができ、セキュリティが高まります。
- レシーバーだけが配置されているドメインは、グループメンバーシップをグローバルにアダプタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャストルーティングテーブルステートが必要ないので、メモリを節約できます。

## MSDP の設定

ここでは、次の設定情報について説明します。

- 「MSDP のデフォルト設定」(P.50-4)
- 「デフォルトの MSDP ピアの設定」(P.50-4) (必須)
- 「Source-Active ステートのキャッシング」(P.50-6) (任意)

- 「MSDP ピアからの送信元情報の要求」 (P.50-8) (任意)
- 「スイッチから発信される送信元情報の制御」 (P.50-8) (任意)
- 「スイッチから転送される送信元情報の制御」 (P.50-11) (任意)
- 「スイッチで受信される送信元情報の制御」 (P.50-13) (任意)
- 「MSDP メッシュ グループの設定」 (P.50-15) (任意)
- 「MSDP ピアのシャットダウン」 (P.50-15) (任意)
- 「MSDP への境界 PIM dense (密) モード領域の追加」 (P.50-16) (任意)
- 「RP アドレス以外の発信元アドレスの設定」 (P.50-17) (任意)

## MSDP のデフォルト設定

MSDP はイネーブルになっておらず、デフォルトの MSDP ピアは存在しません。

## デフォルトの MSDP ピアの設定

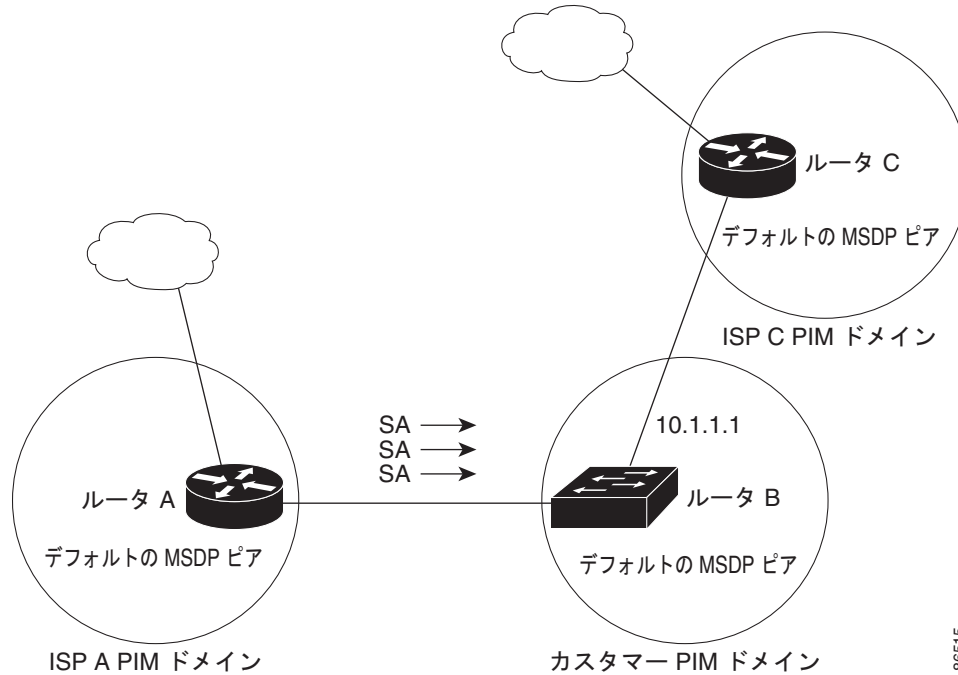
このソフトウェア リリースでは、BGP および MBGP がサポートされていないため、`ip msdp peer` グローバル コンフィギュレーション コマンドを使用して、ローカル スイッチに MSDP ピアを設定できません。代わりに、(`ip msdp default-peer` グローバル コンフィギュレーション コマンドを使用して) デフォルトの MSDP ピアを定義します。このピアでは、スイッチのすべての SA メッセージを受信します。デフォルトの MSDP ピアには、事前に設定済みの MSDP ピアを使用する必要があります。MSDP ピアによる BGP または MBGP ピアリングをスイッチが行わない場合、デフォルトの MSDP ピアを設定します。単一の MSDP ピアが設定されている場合、スイッチはそのピアから常にすべての SA メッセージを受信します。

図 50-2 に、デフォルトの MSDP ピアを使用したネットワークの例を示します。図 50-2 では、スイッチ B を所有するカスタマーが、2 つの Internet Service Provider (ISP; インターネット サービス プロバイダー) に接続されています。一方の ISP はルータ A、もう一方の ISP はルータ C を所有しています。これらの ISP 間では、BGP または MBGP は動作していません。ISP のドメイン内、または他のドメイン内の送信元を学習するために、カスタマー サイトのスイッチ B はルータ A をデフォルトの MSDP ピアとして識別します。スイッチ B は、ルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、受信するのはルータ A またはルータ C のどちらか一方の SA メッセージだけです。コンフィギュレーション ファイルでルータ A が最初に記述されている場合、ルータ A が動作していると、ルータ A が使用されます。ルータ A が動作していない場合にだけ、スイッチ B はルータ C からの SA メッセージを受信します。これが、プレフィクス リストを指定しない場合のデフォルトの動作です。

プレフィクス リストを指定すると、ピアはリスト内のプレフィクスに対してだけデフォルトピアになります。プレフィクス リストが各デフォルトピアに関連付けられている場合は、複数のアクティブなデフォルトピアを設定できます。プレフィクス リストを指定しなくても、複数のデフォルトピアを設定することは可能です。ただし、最初のピアにルータが接続されていて、このピアが動作している限り、アクティブなデフォルトピアになるのは最初のピアだけです。最初に設定したピアに障害が発生したり、このピアへの接続に障害が発生した場合、2 番めに設定したピアがアクティブなデフォルトピアになります。以降、アクティブなデフォルトピアに障害が発生すると、そのピアの次に設定したピアがアクティブなデフォルトピアになります。

ISP は通常、プレフィクス リストを使用して、カスタマーのルータから受信するプレフィクスを定義します。

図 50-2 デフォルトの MSDP ピア ネットワーク



デフォルトの MSDP ピアを指定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>ip msdp default-peer ip-address   name [prefix-list list]</code>	<p>すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。</p> <ul style="list-style-type: none"> <li><code>ip-address   name</code> には、MSDP デフォルト ピアの IP アドレスまたは Domain Name System (DNS; ドメイン ネーム システム) サーバ名を入力します。</li> <li>(任意) <code>prefix-list list</code> には、リストされたプレフィクスに対してだけデフォルト ピアとなるピアを指定するリスト名を入力します。プレフィクス リストが各デフォルト ピアに関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。</li> </ul> <p><b>prefix-list</b> キーワードを指定して複数の <code>ip msdp default-peer</code> コマンドを入力すると、すべてのデフォルト ピアが複数の RP プレフィクスに対して同時に使用されます。この構文は通常、スタブ サイトクラウドに接続されたサービス プロバイダークラウドで使用されます。</p> <p><b>prefix-list</b> キーワードを指定せずに複数の <code>ip msdp default-peer</code> コマンドを入力すると、すべての SA メッセージが単一のアクティブ ピアで受信されます。このピアに障害が発生した場合、このピアの次に設定したデフォルト ピアがすべての SA メッセージを受信します。この構文は通常、スタブ サイトで使用されます。</p>

	コマンド	目的
ステップ 3	<code>ip prefix-list name [description string]   seq number {permit   deny} network length</code>	(任意) ステップ 2 で指定した名前を使用し、プレフィクスリストを作成します。  <ul style="list-style-type: none"> <li>• (任意) <code>description string</code> には、このプレフィクスリストの説明を最大 80 文字で入力します。</li> <li>• <code>seq number</code> には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ~ 4294967294 です。</li> <li>• <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。</li> <li>• <code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。</li> <li>• <code>network length</code> には、許可または拒否されるネットワーク マスクのネットワーク番号および長さ (ビット単位) を指定します。</li> </ul>
ステップ 4	<code>ip msdp description {peer-name   peer-address} text</code>	(任意) 指定したピアを設定内または <code>show</code> コマンド出力内で識別しやすいように、そのピアの説明を設定します。  デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

デフォルト ピアを削除するには、`no ip msdp default-peer ip-address | name` グローバル コンフィギュレーション コマンドを使用します。

次に、[図 50-2](#) のルータ A とルータ C の設定の一部の例を示します。これらの各 ISP には、([図 50-2](#) のカスタマーと同様に) BGP または MBGP 以外のデフォルトのピアリングを使用する複数のカスタマーが存在します。この場合、これら 2 つの ISP の設定は類似したものになります。つまり、これらの ISP では、対応するプレフィクスリストで SA が許可されている場合、デフォルトピアからの SA だけを受信します。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

## Source-Active ステートのキャッシング

デフォルトでは、スイッチが受信した SA メッセージの送信元とグループのペアはキャッシュされません。スイッチは、MSDP SA 情報を転送するとき、この情報をメモリに格納しません。このため、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、そのメンバーは、次の SA メッセージから送信元についての情報を取得するまで待機する必要があります。この遅延は加入遅延と呼ばれます。

メモリを消費して送信元情報の遅延を短縮するには、SA メッセージをキャッシュするようにスイッチを設定します。

送信元とグループのペアのキャッシングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ip msdp cache-sa-state [list access-list-number]</b>	送信元とグループのペアのキャッシングをイネーブルにします (SA ステートを作成します)。これらのペアのうち、アクセス リストを通過したペアがキャッシュされます。 <b>list access-list-number</b> の範囲は 100 ~ 199 です。
ステップ 3	<b>access-list access-list-number {deny   permit} protocol source source-wildcard destination destination-wildcard</b>	必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。 <ul style="list-style-type: none"> <li><b>access-list-number</b> の範囲は 100 ~ 199 です。ステップ 2 で指定した数値と同じ値を入力します。</li> <li><b>deny</b> キーワードは、条件が一致した場合にアクセスを拒否します。<b>permit</b> キーワードは、条件が一致した場合にアクセスを許可します。</li> <li><b>protocol</b> には、プロトコル名として <b>ip</b> を入力します。</li> <li><b>source</b> には、パケットの送信元となるネットワークまたはホストの番号を入力します。</li> <li><b>source-wildcard</b> には、送信元に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> <li><b>destination</b> には、パケットの送信先となるネットワークまたはホストの番号を入力します。</li> <li><b>destination-wildcard</b> には、宛先に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> </ul> アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) 設定をコンフィギュレーション ファイルに保存します。



(注)

このコマンドの代わりに、**ip msdp sa-request** グローバル コンフィギュレーション コマンドも使用できます。**ip msdp sa-request** コマンドを使用すると、グループの新しいメンバーがアクティブになったときに、SA 要求メッセージがスイッチから MSDP ピアに送信されます。詳細については、次の項を参照してください。

デフォルト設定 (SA ステートが作成されていない状態) に戻すには、**no ip msdp cache-sa-state** グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.0.0/16 の範囲内にある、グループ 224.2.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

## MSDP ピアからの送信元情報の要求

ローカル RP は、SA 要求を送信し、特定グループのすべてのアクティブな送信元に対する応答をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャストトラフィックを受信する必要がある場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは、次の定期的な SA メッセージの受信を待機する必要があります。

グループの送信元である接続済み PIM sparse (疎) モードドメイン内にあるアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合、新しいメンバーがグループに加入したときに、指定した MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。ピアは、SA キャッシュ内の情報で応答します。ピアにキャッシュが設定されていない場合は、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバーがグループに加入し、マルチキャストトラフィックを受信する必要がある場合に、MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp sa-request {ip-address   name}</code>	指定した MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定します。  <i>ip-address   name</i> には、グループの新しいメンバーがアクティブになるときにローカルスイッチが SA メッセージを要求する MSDP ピアの IP アドレスまたは名前を入力します。  SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、`no ip msdp sa-request {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定する例を示します。

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

## スイッチから発信される送信元情報の制御

スイッチから発信される次のマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元 (送信元に基づく)
- 送信元情報のレシーバー (要求元の認識に基づく)

詳細については、「[送信元の再配布](#)」(P.50-9) および「[Source-Active 要求メッセージのフィルタリング](#)」(P.50-10) を参照してください。



## 送信元の再配布

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に *A* フラグが設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA にアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元をさらに制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <b>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</b>	<p>SA メッセージにアドバタイズされる、マルチキャスト ルーティング テーブル内の (S,G) エントリを設定します。</p> <p>デフォルトでは、ローカル ドメイン内の送信元だけがアドバタイズされます。</p> <ul style="list-style-type: none"> <li>• (任意) <b>list access-list-name</b> には、IP 標準アクセス リストまたは IP 拡張アクセス リストの名前または番号を入力します。標準アクセス リストの範囲は 1 ~ 99、拡張リストの範囲は 100 ~ 199 です。アクセス リストでは、アドバタイズされるローカルの送信元とその送信先となるグループを制御します。</li> <li>• (任意) <b>asn aspath-access-list-number</b> には、1 ~ 199 の範囲の IP 標準アクセス リスト番号または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、<b>ip as-path access-list</b> コマンドでも設定する必要があります。</li> <li>• (任意) <b>route-map map</b> には、1 ~ 199 の範囲の IP 標準アクセス リスト番号または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、<b>ip as-path access-list</b> コマンドでも設定する必要があります。</li> </ul> <p>アドバタイズされる (S,G) ペアは、アクセス リストまたは自律システム パス アクセス リストによって決まります。</p>

	コマンド	目的
ステップ 3	<pre>access-list access-list-number {deny   permit} source [source-wildcard]</pre> <p>または</p> <pre>access-list access-list-number {deny   permit} protocol source source-wildcard destination destination-wildcard</pre>	<p>必要な数だけこのコマンドを繰り返し、IP 標準アクセス リストを作成します。</p> <p>または</p> <p>必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。</p> <ul style="list-style-type: none"> <li>• <i>access-list-number</i> では、標準アクセス リストの範囲は 1 ~ 99、拡張リストの範囲は 100 ~ 199 です。ステップ 2 で指定した数値と同じ値を入力します。</li> <li>• <b>deny</b> キーワードは、条件が一致した場合にアクセスを拒否します。<b>permit</b> キーワードは、条件が一致した場合にアクセスを許可します。</li> <li>• <i>protocol</i> には、プロトコル名として <b>ip</b> を入力します。</li> <li>• <i>source</i> には、パケットの送信元となるネットワークまたはホストの番号を入力します。</li> <li>• <i>source-wildcard</i> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> <li>• <i>destination</i> には、パケットの送信先となるネットワークまたはホストの番号を入力します。</li> <li>• <i>destination-wildcard</i> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> </ul> <p>アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。</p>
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) 設定をコンフィギュレーション ファイルに保存します。

フィルタを削除するには、**no ip msdp redistribute** グローバル コンフィギュレーション コマンドを使用します。

## Source-Active 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシュしているスイッチだけが SA 要求に応答します。デフォルトでは、このようなスイッチは、MSDP ピアからのすべての SA 要求メッセージを受け入れ、アクティブな送信元の IP アドレスを提供します。

ただし、MSDP ピアからの SA 要求をすべて無視するようにスイッチを設定できます。また、標準アクセス リストに記述されたグループのピアからの SA 要求メッセージだけを受け入れることもできます。アクセス リストでグループが通過すると、そのグループのピアからの SA 要求メッセージが受信されます。他のグループのピアからのメッセージは、すべて無視されます。

これらの方法のいずれかを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp filter-sa-request ip-address   name</code>  または <code>ip msdp filter-sa-request {ip-address   name} list access-list-number</code>	指定した MSDP ピアからの SA 要求メッセージをすべてフィルタリングします。  または 指定した MSDP ピアからの SA 要求メッセージを、標準アクセス リストを通過したグループに対してフィルタリングします。アクセス リストには、マルチキャスト グループ アドレスが記述されています。 <code>access-list-number</code> の範囲は 1 ~ 99 です。
ステップ 3	<code>access-list access-list-number {deny   permit} source [source-wildcard]</code>	必要な数だけこのコマンドを繰り返し、IP 標準アクセス リストを作成します。  <ul style="list-style-type: none"> <li>• <code>access-list-number</code> の範囲は 1 ~ 99 です。</li> <li>• <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。</li> <li>• <code>source</code> には、パケットの送信元となるネットワークまたはホストの番号を入力します。</li> <li>• (任意) <code>source-wildcard</code> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> </ul> アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、`no ip msdp filter-sa-request {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.2.2 にある MSDP ピアからの SA 要求メッセージをフィルタリングするようにスイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージは、アクセス リスト 1 を通過して受信され、それ以外のメッセージはすべて無視されます。

```
Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1
Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

## スイッチから転送される送信元情報の制御

デフォルトでは、スイッチが受信したすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングしたり、Time To Live (TTL; 存続可能時間) 値を設定することで、発信メッセージがピアに転送されないようにすることができます。以降の項では、この方法について説明します。

## フィルタの使用

フィルタを作成すると、次のいずれかの処理を実行できます。

- 送信元とグループのペアをすべてフィルタリングする
- 特定の送信元とグループのペアだけが通過するように IP 拡張アクセス リストを指定する
- ルート マップの一致基準に基づいてフィルタリングする

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp sa-filter out ip-address   name</code> または <code>ip msdp sa-filter out {ip-address   name} list access-list-number</code>  または <code>ip msdp sa-filter out {ip-address   name} route-map map-tag</code>	指定した MSDP ピアへの SA メッセージをすべてフィルタリングします。 または IP 拡張アクセス リストを通過した SA メッセージだけを、指定したピアに渡します。 <code>access-list-number</code> (拡張アクセス リスト番号) の範囲は 100 ~ 199 です。  <b>list</b> と <b>route-map</b> の両方のキーワードを使用すると、すべての条件が <b>true</b> である場合に、発信 SA メッセージ内のすべての (S,G) ペアが通過します。 または ルート マップ <code>map-tag</code> 内の一致基準を満たしている SA メッセージだけを、指定した MSDP ピアに渡します。  すべての一致基準が <b>true</b> であり、ルート マップに <b>permit</b> を指定している場合、ルートはフィルタを通過します。 <b>deny</b> を指定していると、ルートはフィルタリングされます。
ステップ 3	<code>access-list access-list-number {deny   permit} protocol source source-wildcard destination destination-wildcard</code>	(任意) 必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。  <ul style="list-style-type: none"> <li>• <code>access-list-number</code> には、ステップ 2 で指定した番号を入力します。</li> <li>• <b>deny</b> キーワードは、条件が一致した場合にアクセスを拒否します。<b>permit</b> キーワードは、条件が一致した場合にアクセスを許可します。</li> <li>• <code>protocol</code> には、プロトコル名として <b>ip</b> を入力します。</li> <li>• <code>source</code> には、パケットの送信元となるネットワークまたはホストの番号を入力します。</li> <li>• <code>source-wildcard</code> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> <li>• <code>destination</code> には、パケットの送信先となるネットワークまたはホストの番号を入力します。</li> <li>• <code>destination-wildcard</code> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> </ul> アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

フィルタを削除するには、`no ip msdp sa-filter out {ip-address | name} [list access-list-number] [route-map map-tag]` グローバル コンフィギュレーション コマンドを使用します。

次に、アクセス リスト 100 を通過した (S,G) ペアだけが SA メッセージに格納され、`switch.cisco.com` という名前のピアに転送されるように設定する例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

## SA メッセージで送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が `ttl` 引数以上であるマルチキャスト パケットだけを、指定した MSDP ピアに送信します。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの送信時に TTL を 8 より大きく設定する必要があります。

TTL スレッシュホールドを確立するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp ttl-threshold {ip-address   name} ttl</code>	指定した MSDP ピアへの最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 <ul style="list-style-type: none"> <li><code>ip-address   name</code> には、TTL の制限を適用する MSDP ピアの IP アドレスまたは名前を入力します。</li> <li><code>ttl</code> には、TTL 値を入力します。デフォルトは 0 です。この場合、TTL がなくなるまで、すべてのマルチキャスト データ パケットがピアに転送されます。指定できる範囲は 0 ~ 255 です。</li> </ul>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、`no ip msdp ttl-threshold {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

## スイッチで受信される送信元情報の制御

デフォルトでは、スイッチは、MSDP の RPF ピアが送信したすべての SA メッセージを受信します。ただし、着信 SA メッセージをフィルタリングすることで、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信しないようにスイッチを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージをフィルタリングする
- 特定の送信元とグループのペアが通過するように IP 拡張アクセス リストを指定する

- ルート マップの一致基準に基づいてフィルタリングする
- フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ip msdp sa-filter in</b> <i>ip-address</i>   <i>name</i> または <b>ip msdp sa-filter in</b> { <i>ip-address</i>   <i>name</i> } <b>list</b> <i>access-list-number</i>  または <b>ip msdp sa-filter in</b> { <i>ip-address</i>   <i>name</i> } <b>route-map</b> <i>map-tag</i>	指定した MSDP ピアからの SA メッセージをすべてフィルタリングします。 または IP 拡張アクセス リストを通過した SA メッセージだけを、指定されたピアから受信します。 <i>access-list-number</i> (拡張アクセス リスト番号) の範囲は 100 ~ 199 です。 <b>list</b> と <b>route-map</b> の両方のキーワードを使用すると、すべての条件が <b>true</b> である場合に、着信 SA メッセージ内のすべての (S,G) ペアが通過します。 または ルート マップ <i>map-tag</i> 内の一致条件を満たしている SA メッセージだけを、指定した MSDP ピアから受信します。 すべての一致基準が <b>true</b> であり、ルート マップに <b>permit</b> を指定している場合、ルートはフィルタを通過します。 <b>deny</b> を指定していると、ルートはフィルタリングされます。
ステップ 3	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>protocol source source-wildcard destination destination-wildcard</i>	(任意) 必要な数だけこのコマンドを繰り返し、IP 拡張アクセス リストを作成します。 <ul style="list-style-type: none"> <li><i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。</li> <li><b>deny</b> キーワードは、条件が一致した場合にアクセスを拒否します。<b>permit</b> キーワードは、条件が一致した場合にアクセスを許可します。</li> <li><i>protocol</i> には、プロトコル名として <b>ip</b> を入力します。</li> <li><i>source</i> には、パケットの送信元となるネットワークまたはホストの番号を入力します。</li> <li><i>source-wildcard</i> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> <li><i>destination</i> には、パケットの送信先となるネットワークまたはホストの番号を入力します。</li> <li><i>destination-wildcard</i> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を指定します。</li> </ul> アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) 設定をコンフィギュレーション ファイルに保存します。

フィルタを削除するには、**no ip msdp sa-filter in** *{ip-address | name}* [**list access-list-number**] [**route-map map-tag**] グローバル コンフィギュレーション コマンドを使用します。

次に、*switch.cisco.com* という名前のピアからの SA メッセージをすべてフィルタリングする例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```

## MSDP メッシュ グループの設定

MSDP メッシュ グループは、フル メッシュ構造の MSDP 相互接続ができる MSDP スピーカーのグループです。メッシュ グループ内のピアから受信された SA メッセージは、同じメッシュ グループ内の他のピアに転送されません。このため、SA メッセージのフラディングが削減され、ピア RPF フラディングが簡素化されます。ドメイン内に複数の RP が存在する場合は、**ip msdp mesh-group** グローバル コンフィギュレーション コマンドを使用します。特に、ドメイン全体に SA メッセージを送信する場合に使用します。単一のスイッチに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ip msdp mesh-group name</b> <i>{ip-address   name}</i>	MSDP メッシュ グループを設定し、そのメッシュ グループに属する MSDP ピアを指定します。  デフォルトでは、MSDP ピアはメッシュ グループに属しません。 <ul style="list-style-type: none"> <li><i>name</i> には、メッシュ グループの名前を入力します。</li> <li><i>ip-address   name</i> には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。</li> </ul>
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(任意) 設定をコンフィギュレーション ファイルに保存します。
ステップ 6		グループ内の MSDP ピアごとに、この手順を繰り返します。

メッシュ グループから MSDP ピアを削除するには、**no ip msdp mesh-group name** *{ip-address | name}* グローバル コンフィギュレーション コマンドを使用します。

## MSDP ピアのシャットダウン

複数の MSDP コマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンして設定することにより、あとで起動できます。ピアをシャットダウンすると、TCP 接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDP セッションをシャットダウンすることもできます。

ピアをシャットダウンするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp shutdown {peer-name   peer address}</code>	設定情報を保持したまま、指定した MSDP ピアを管理上のシャットダウン状態にします。  <i>peer-name   peer address</i> には、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

ピアを再起動するには、`no ip msdp shutdown {peer-name | peer address}` グローバル コンフィギュレーション コマンドを使用します。これにより、TCP 接続が再確立されます。

## MSDP への境界 PIM dense (密) モード領域の追加

PIM sparse (疎) モード領域と dense (密) モード領域の境界となるスイッチに MSDP を設定できます。デフォルトでは、dense (密) モード領域のアクティブな送信元は MSDP に参加しません。



(注) `ip msdp border sa-address` グローバル コンフィギュレーション コマンドを使用することは推奨できません。dense (密) モードドメイン内の送信元を sparse (疎) モードドメインの RP にプロキシ登録するように sparse (疎) モードドメイン内の境界ルータを設定し、MSDP の標準的な手順を使用してこれらの送信元をアドバタイズするように sparse (疎) モードドメインを設定してください。

dense (密) モード領域内でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp border sa-address interface-id</code>	dense (密) モード領域内のアクティブな送信元に関する SA メッセージを送信するように、dense (密) モード領域と sparse (疎) モード領域の境界スイッチを設定します。  <i>interface-id</i> には、SA メッセージ内の RP アドレスとして使用される、IP アドレスが取得されるインターフェイスを指定します。  インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 3	<code>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</code>	SA メッセージにアドバタイズされる、マルチキャストルーティングテーブル内の (S,G) エントリを設定します。  詳細については、「送信元の再配布」(P.50-9) を参照してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。



**ip msdp originator-id** グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスによって RP アドレスが決まります。

デフォルト設定 (dense (密) モード領域のアクティブな送信元が MSDP に参加しない設定) に戻すには、**no ip msdp border sa-address interface-id** グローバル コンフィギュレーション コマンドを使用します。

## RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュ グループ内の複数のスイッチ上で、論理 RP を設定する場合。
- PIM sparse (疎) モード ドメインと dense (密) モード ドメインの境界スイッチがある場合。サイトの dense (密) モード ドメインの境界となるスイッチがあり、sparse (疎) モードがその外部で使用されている場合は、dense (密) モードの送信元を外部に通知する必要があります。このスイッチは RP ではないので、SA メッセージで使用される RP アドレスを含みません。したがって、このコマンドによりインターフェイスのアドレスを指定して、RP アドレスが取得されます。

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ip msdp originator-id interface-id</b>	発信元装置のインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。  <i>interface-id</i> には、ローカル スイッチのインターフェイスを指定します。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(任意) 設定をコンフィギュレーション ファイルに保存します。

**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスによって RP アドレスが決まります。

この方法で RP アドレスが取得されないようにするには、**no ip msdp originator-id interface-id** グローバル コンフィギュレーション コマンドを使用します。

## MSDP のモニタおよびメンテナンス

MSDP SA メッセージ、ピア、ステート、またはピア ステータスをモニタするには、表 50-1 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 50-1 MSDP のモニタおよびメンテナンスのためのコマンド

コマンド	目的
<code>debug ip msdp [peer-address   name] [detail] [routes]</code>	MSDP アクティビティをデバッグします。
<code>debug ip msdp resets</code>	MSDP ピアがリセットされた原因をデバッグします。
<code>show ip msdp count [autonomous-system-number]</code>	SA メッセージに格納され、各自律システムから発信された送信元およびグループの数を表示します。このコマンドによって出力を生成するには、 <code>ip msdp cache-sa-state</code> コマンドを設定する必要があります。
<code>show ip msdp peer [peer-address   name]</code>	MSDP ピアに関する詳細情報を表示します。
<code>show ip msdp sa-cache [group-address   source-address   group-name   source-name] [autonomous-system-number]</code>	MSDP ピアから学習した (S,G) ステートを表示します。
<code>show ip msdp summary</code>	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、または SA キャッシュ エントリを消去するには、表 50-2 に示す各特権 EXEC コマンドを使用します。

表 50-2 MSDP 接続、統計情報、または SA キャッシュ エントリを消去するためのコマンド

コマンド	目的
<code>clear ip msdp peer peer-address   name</code>	指定した MSDP ピアへの TCP 接続を消去し、すべての MSDP メッセージカウンタをリセットします。
<code>clear ip msdp statistics [peer-address   name]</code>	セッションをリセットせずに、特定の MSDP ピアまたはすべての MSDP ピアの統計カウンタをクリアします。
<code>clear ip msdp sa-cache [group-address   name]</code>	すべてのエントリの SA キャッシュ エントリ、特定グループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリを消去します。