MSDPを使用しての複数のPIM-SMドメインの相互接続

このモジュールでは、Multicast Source Discovery Protocol（MSDP）を使用した複数の PIM-SM ドメインの相互接続に関連する作業について説明します。 作業では、MSDP のピア、メッシュ グループ、およびデフォルト ピアを設定する方法、フィルタを使用して MSDP のアクティビティを制御し、範囲を設定する方法、およびMSDPをモニタリングし、維持する方法を説明します。 MSDP を PIM-SM と併用することで、複数の PIM-SM ドメインを簡単に接続できます。

- 機能情報の確認，1 ページ
- MSDP を使用して複数の PIM-SM ドメインを相互接続する前提条件，2 ページ
- MSDP を使用して複数の PIM-SM ドメインを相互接続するための情報，2 ページ
- MSDP を使用して複数の PIM-SM ドメインを相互接続する方法，20 ページ
- MSDP を使用して複数の PIM-SM ドメインを相互接続する設定例，48 ページ
- その他の関連資料，51 ページ
- MSDP を使用して複数の PIM-SM ドメインを相互接続するための機能情報，53 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

MSDP を使用して複数の PIM-SM ドメインを相互接続する前提条件

MSDP を設定する前に、すべての MSDP ピアのアドレスがボーダー ゲートウェイ プロトコル（BGP）で認識されている必要があります。

MSDP を使用して複数の PIM-SM ドメインを相互接続するための情報

MSDP を使用して複数の PIM-SM ドメインを相互接続することの利点

- ランデブー ポイント（RP）でドメイン外のアクティブなソースを動的に検出できます。
- 複数のドメイン間でマルチキャスト配信ツリーを構築するためのさらに管理しやすいアプローチを導入できます。

複数の PIM-SM ドメインを相互接続するための MSDP の使用

MSDP は、複数の PIM-SM ドメインを接続するメカニズムです。 MSDP の目的は、他の PIM ドメイン内のマルチキャスト ソースを検出することです。 MSDP の主な利点は、PIM-SM ドメインで（共通の共有ツリーではなく）ドメイン間ソース ツリーを使用することで、複数の PIM-SM ドメインを簡単に相互接続できることです。 MSDP がネットワークで設定されている場合、RP は他のドメインの RP とソース情報を交換します。 RP は、レシーバがいるグループに送信するソースのドメイン間ソース ツリーに参加できます。 これができるのは、RP が、アクティブなレシーバが存在するドメイン内のすべてのポイントへのブランチがある、ドメイン内の共有ツリーのルートであるためです。 ラスト ホップ ルータは（共有ツリー下のソースからのマルチキャスト パケットの着信によって）PIM-SM ドメイン外の新しいソースを学習すると、ソースに加入を送信し、ドメイン間ソース ツリーに参加できます。

（注） RP に特定のグループの共有ツリーがないか、または RP の共有ツリーの発信インターフェイス リストが空の場合は、別のドメイン内のソースに加入を送信しません。

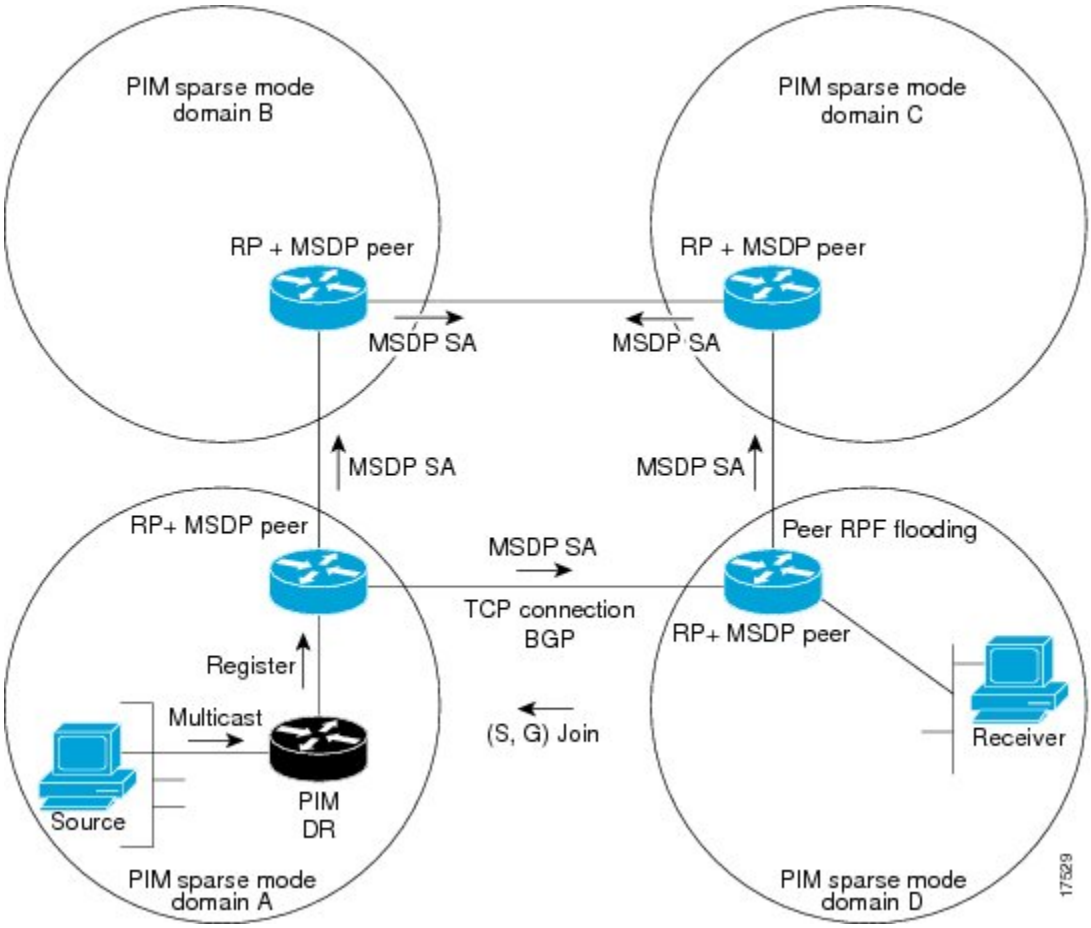
MSDP がイネーブルになっている場合、PIM-SM ドメインの RP は、他のドメインの MSDP 対応ルータとの MSDP ピアリング関係を維持します。 このピアリング関係は TCP 接続を通じて発生し、主にマルチキャスト グループに送信するソースのリストが交換されます。 MSDP は、ピアリング接続に TCP（ポート 639）を使用します。 BGP と同様に、ポイントツーポイント TCP ピアリングを使用することは、各ピアを明示的に設定する必要があることを意味します。 また、RP 間

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のパスが確立されます。 マルチキャスト ソースがレシーバがいるドメインの対象である場合、マルチキャスト データは PIM-SM で提供される通常のソース ツリー構築メカニズムを使用して配信されます。 MSDP は、グループを送信する送信元のアナウンスにも使用されます。 これらのアナウンスは、ドメインの RP で発信する必要があります。

（注） MSDP は、ドメイン間の動作に関して BGP またはマルチプロトコル BGP（MBGP）に依存しています。 グローバル マルチキャスト グループに送信する RP で MSDP を実行することを推奨します。

図に、2 つの MSDP ピア間で動作する MSDP を示します。 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 が使用されます。

図 *1*：*RP* ピア間で動作する *MSDP*



MSDP が実装されている場合、次のイベント シーケンスが発生します。

1 図に示すように、PIM 指定ルータ（DR）が RP にソースを登録すると、RP はその MSDP ピアすべてに Source-Active（SA）メッセージを送信します。

（注） DR は、（ソースがアクティブになると）カプセル化されたデータをソースごとに 1 回だけ RP に送信します。 ソースがタイムアウトした場合、ソースが再度アクティブになるとこのプロセスが実行されます。 この状況は、発信側の RP に登録されたすべてのソースを含む定期的な SA メッセージとは異なります。 これらの SA メッセージは MSDP の制御パケットで、そのため、アクティブなソースからのカプセル化されたデータは含まれません。

1. SA メッセージでは、ソース アドレス、ソースの送信先グループ、および RP のアドレスまたは発信者 ID が識別されます（設定されている場合）。
2. SA メッセージを受信する各 MSDP ピアは、発信者からのダウンストリームのすべてのピアに SA メッセージをフラッディングします。 場合によっては（図のように PIM-SM ドメイン B および C に RP がある場合など）、RP は複数の MSDP ピアから SA メッセージのコピーを受信することがあります。 ループが作成されないように、RP は BGP ネクスト ホップ データベースに問い合わせて、SA メッセージの発信者へのネクスト ホップを識別します。 MBGP とユニキャスト BGP の両方が設定されている場合、最初に MBGP がチェックされ、次にユニキャスト BGP がチェックされます。 そのネクスト ホップ ネイバーは発信者の RPF ピアです。 RPF ピアとのインターフェイス以外のインターフェイスの発信者から受信した SA メッセージはドロップされます。 そのため、SA メッセージ フラッディング プロセスはピア RPF フラッディングと呼ばれます。 ピア RPF フラッディング メカニズムにより、BGP または MBGP は MSDP とともに実行する必要があります。

（注） （M）BGP は、MSDP メッシュ グループのシナリオでは必要ありません。 MSDP メッシュ グループの詳細については、MSDP メッシュ グループの設定, （31 ページ）のセクションを参照してください。

（注） （M）BGP は、デフォルト MSDP ピアのシナリオまたは MSDP ピアが 1 つだけ設定されているシナリオでは必要ありません。 詳細については、デフォルトの MSDP ピアの設定, （30 ページ）のセクションを参照してください。

1. RP は SA メッセージを受信すると、グループ（*, G）の発信インターフェイス リストにインターフェイスがあるかどうかを確認して、アドバタイズされたグループのメンバがドメイン内にあるかどうかを確認します。 グループ メンバが存在しない場合、RP は何も実行しません。 グループ メンバが存在する場合、RP はソースに対して（S,G）加入を送信します。 その結果、RP へのドメイン間のブランチが自律システムの境界を越えて構築されます。 マルチキャスト パケットは、RP に着信すると、その共有ツリーを経由して RP のドメイン内のグループ メンバに転送されます。 メンバの DR は、標準的な PIM-SM 手順を使用してソースへのランデブー ポイント ツリー（RPT）に加入することもできます。
2. 発信側の RP は、ソースがグループにパケットを送信している限り、（S, G）ステートの定期的な SA メッセージを 60 秒ごとに送信し続けます。 RP は SA メッセージを受信すると、SA

メッセージをキャッシュします。 たとえば、RP が発信側の RP 10.5.4.3 から（172.16.5.4、228.1.2.3）の SA メッセージを受信するとします。 RP は mroute テーブルに問い合わせて、グループ 228.1.2.3 にアクティブ メンバがないことを検出するため、10.5.4.3 のダウンストリームのピアに SA メッセージを渡します。 ドメイン内のホストがグループ 228.1.2.3 の RP に加入を送信すると、RP はホストへのインターフェイスを（*, 224.1.2.3）エントリの発信インターフェイス リストに追加します。 RP は SA メッセージをキャッシュするため、ルータは (172.16.5.4, 228.1.2.3) のエントリを持ち、ホストが加入を要求するとすぐにソース ツリーに加入できます。

（注） 現行のすべてのサポートされているソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。 デフォルトでは、MSDP ピアが設定されると、**ip multicast cache-sa-state** コマンドが自動的に実行コンフィギュレーションに追加されます。

MSDP メッセージ タイプ

それぞれ独自のタイプ、長さ、値（TLV）データ形式で符号化された 4 つの基本的な MSDP メッセージ タイプがあります。

SA メッセージ

SA メッセージは、ドメイン内のアクティブなソースをアドバタイズするために使用されます。また、これらの SA メッセージには、ソースから送信された初期マルチキャスト データ パケットが含まれる場合があります。

SA メッセージには、発信側の RP の IP アドレスおよびアドバタイズされる 1 つまたは複数の（S, G）ペアが含まれます。 また、SA メッセージにはカプセル化されたデータ パケットが含まれることがあります。

（注） SA メッセージの詳細については、SA メッセージの発信、受信、および処理, （6 ページ）を参照してください。

SA 要求メッセージ

SA 要求メッセージは、特定のグループのアクティブなソースのリストを要求するために使用されます。 これらのメッセージは、SA キャッシュにアクティブな（S, G）ペアのリストを保持する MSDP SA キャッシュに送信されます。 参加遅延は、発信側の RP によって再度アドバタイズされるグループ内のすべてのアクティブなソースに対して最大 60 秒待機するのではなく、SA 要求メッセージを使用してグループのアクティブなソースのリストを要求することで低減できます。

（注） SA 要求メッセージの詳細については、MSDP ピアへのソース情報の要求, （37 ページ）を参照してください。

SA 応答メッセージ

SA 応答メッセージは、SA 要求メッセージに応じて MSDP ピアによって送信されます。 SA 応答メッセージには、発信側 RP の IP アドレス、およびキャッシュに格納されている発信側 RP のドメイン内のアクティブなソースの（S, G）ペアが 1 つまたは複数含まれます。

（注） SA 応答メッセージの詳細については、SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御, （39 ページ）を参照してください。

キープアライブ メッセージ

キープアライブ メッセージは、MSDP セッションをアクティブにしておくために 60 秒ごとに送信されます。 キープアライブ メッセージまたは SA メッセージが 75 秒間受信されない場合、MSDP セッションはリセットされます。

（注） キープアライブ メッセージの詳細については、MSDP キープアライブ インターバルおよび保留時間インターバルの調整, （27 ページ）を参照してください。

SA メッセージの発信、受信、および処理

ここでは SA メッセージの発信、受信、および処理について詳しく説明します。

SA メッセージの発信

SA メッセージは、ローカル PIM-SM ドメイン内で新しいソースがアクティブになると、RP によってトリガーされます（MSDP が設定されている場合）。 ローカル ソースは、RP に直接接続されているソース、または登録されているファースト ホップ DR です。 RP は、PIM-SM ドメイン内のローカル ソース、つまり RP に登録されているローカル ソースの SA メッセージだけを発信します。

（注） ローカル ソースは、RP の（S, G）mroute エントリに設定されている A フラグによって示されます（**show ip mroute** コマンドの出力で確認できます）。 このフラグは、ソースが、RP が他の MSDP ピアにアドバタイズする候補であることを示します。

ソースがローカル PIM-SM ドメイン内にある場合、RP に（S, G）ステートが作成されます。 新しいソースは、登録メッセージを受信するか、直接接続されているソースから最初の（S,G）パケットが着信することによって RP で検出されます。 ソースから送信された最初のマルチキャスト パケット（登録メッセージにカプセル化されるか、直接接続されているソースから受信します）は、最初の SA メッセージにカプセル化されます。

SA メッセージの受信

SA メッセージは、発信者への最良パスにある MSDP RPF ピアからに限り受け入れられます。 他の MSDP ピアから着信する同じ SA メッセージは無視する必要があり、無視しないと、SA ループが発生することがあります。 着信 SA メッセージの MSDP RPF ピアを選択するには、MSDP トポロジの知識が必要です。 ただし、MSDP はルーティング アップデートの形式でトポロジ情報を送信しません。 MSDP は、SA RPF チェック メカニズムに（M）BGP ルーティング データを MSDP トポロジの最適な近似データとして使用して、この情報を推測します。 したがって、MSDP トポロジは BGP ピア トポロジと同じ汎用トポロジに従う必要があります。 いくつかの例外（デフォルト MSDP ピア、MSDP メッシュ グループの MSDP ピアなど）を除いて、MSDP ピアは、一般に（M）BGP ピアにする必要があります。

RPF チェック ルールを SA メッセージに適用する方法

SA メッセージの RPF チェックに適用されるルールは、MSDP ピア間の BGP ピアリングによって異なります。

- ルール 1：送信側の MSDP ピアが Interior (M)BGP（i（M）BGP）ピアでもある場合に適用されます。
- ルール 2：送信側の MSDP ピアが Exterior（M）BGP（e（M）BGP）ピアでもある場合に適用されます。
- ルール 3：送信側の MSDP ピアが（M）BGP ピアでない場合に適用されます。

RPF チェックは次の場合は実行されません。

- 送信側の MSDP ピアが唯一の MSDP ピアである場合。これは、MSDP ピアが 1 つだけまたはデフォルト MSDP ピアだけが設定されている場合です。
- 送信側の MSDP ピアがメッシュ グループのメンバである場合。
- 送信側の MSDP ピアのアドレスが SA メッセージに含まれる RP アドレスである場合

ソフトウェアが RPF チェックに適用するルールを決定する方法

ソフトウェアは、次の論理で RPF チェックに適用する RPF ルールを決定します。

- 送信側の MSDP ピアと同じ IP アドレスを持つ（M）BGP ネイバーを検索します。
  - 一致した（M）BGP ネイバーが Internal BGP（iBGP）ピアである場合、ルール 1 を適用します。
  - 一致した（M）BGP ネイバーが External BGP（eBGP）ピアである場合、ルール 2 を適用します。
  - 一致するネイバーが見つからなかった場合、ルール 3 を適用します。

RPF チェックのルールの選択では、デバイスの MSDP ピアを設定するために使用される IP アドレスが同じデバイスの（M）BGP ピアを設定するために使用される IP アドレスと一致していることが前提になっています。

MSDP の SA メッセージの RPF チェックのルール 1

送信側の MSDP ピアが i（M）BGP ピアでもある場合、MSDP の RPF チェックのルール 1 が適用されます。 ルール 1 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP マルチキャスト ルーティング情報ベース（MRIB）を検索して SA メッセージを発信した RP への最適パスを探します。 MRIB でパスが検出されなかった場合、ピアはユニキャスト ルーティング情報ベース（URIB）を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 検索が成功した場合（最適パスが検出された場合）、ピアはこの最適パスの BGP ネイバーのアドレスを決定します。このアドレスは、ピアに BGP アップデート メッセージでパスを送信した BGP ネイバーのアドレスになります。

（注） BGP ネイバー アドレスは、パス内のネクスト ホップ アドレスと同じではありません。i（M）BGP ピアはパスのネクスト ホップ属性を更新しないため、ネクスト ホップ アドレスは通常、パスを送信した BGP ピアのアドレスと同じではありません。

（注） BGP ネイバー アドレスは、ピアにパスを送信したピアの BGP ID と同じでなくても構いません。

1. 送信側の MSDP ピアの IP アドレスが BGP ネイバー アドレス（ピアにパスを送信した BGP ピアのアドレス）と同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

RPF チェックのルール 1 の MSDP への影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。 一般に、2 台のデバイス間に i（M）BGP ピア接続がある場合は、必ず MSDP ピア接続を設定する必要があります。 つまり、遠端 MSDP ピア接続の IP アドレスは、遠端 i（M）BGP ピア接続と同じにする必要があります。 自律システム内の i（M）BGP ピア間の BGP トポロジは AS パスでは記述されないため、アドレスを同じにする必要があります。 別の i（M）BGP ピアへのアップデートの送信時に i（M）BGP ピアがパス内のネクスト ホップ アドレスをアップデートした場合、ピアはネクスト ホップ アドレスを使用して i（M）BGP トポロジ（したがって MSDP トポロジ）を表すことができます。ただし、i（M）BGP ピアのデフォルトの動作はネクストホップアドレスをアップデートしないため、ピアはネクスト ホップ アドレスを使用して（M）BGP トポロジ（MSDP トポロジ）を表すことはできません。 その代わりに、i（M）BGP ピアは、パスを送信した i（M）BGP ピアのアドレスを使用して、自律システム内の i（M）BGP トポロジ（MSDP トポロジ）を表します。

ヒント MSDP ピアを設定する場合は、i（M）BGP ピア アドレスと MSDP ピア アドレスの両方に同じアドレスが使用されるように注意する必要があります。

MSDP の SA メッセージの RPF チェックのルール 2

送信側の MSDP ピアが e（M）BGP ピアでもある場合、MSDP の RPF チェックのルール 2 が適用されます。 ルール 2 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。 MRIB でパスが検出されなかった場合、ピアは URIB を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 検索が成功した場合（最適パスが検出された場合）、ピアはパスを検査します。 RP への最適パス内の最初の自律システムが e（M）BGP ピア（送信側の MSDP ピアでもある）の自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

RPF チェックのルール 2 の MSDP への影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。 一般に、2 台のデバイス間に e（M）BGP ピア接続がある場合は、必ず MSDP ピア接続を設定する必要があります。 ルール 1 とは対照的に、遠端 MSDP ピア接続の IP アドレスは遠端 e（M）BGP ピア接続と同じである必要はありません。その理由は、2 つの e（M）BGP ピア間の BGP トポロジが AS パスで記述されないためです。

MSDP の SA メッセージの RPF チェックのルール 3

送信側の MSDP ピアが（M）BGP ピアではない場合、RPF チェックのルール 3 が適用されます。 ルール 3 が適用されると、RPF チェックは次のように行われます。

1 ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。 MRIB でパスが検出されなかった場合、ピアは URIB を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。

2 検索が成功した場合（つまり、SA メッセージを発信した RP への最適パスが検出された場合）、ピアは BGP MRIB を検索して SA メッセージを送信した MSDP ピアへの最適パスを探します。 MRIB でパスが検出されなかった場合、ピアは URIB を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。

（注） SA メッセージを送信した MSDP ピアの自律システムは発信元自律システムで、これは MSDP ピアへの AS パス内にある最後の自律システムです。

1 RP への最適パス内の最初の自律システムが送信側の MSDP ピアの自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

SA メッセージの処理

MSDP ピアは、SA メッセージを処理するたびに次の手順を実行します。

1 ピアは SA メッセージの（S, G）ペアのグループ アドレス G を使用して、mroute テーブル内の関連する（*, G）エントリを見つけます。 （*, G）エントリが検出され、発信インターフェイス リストが空でない場合、SA メッセージでアドバタイズされたソースのアクティブなレシーバが PIM-SM ドメインにあります。

2 MSDP ピアは、アドバタイズされたソースの（S, G）エントリを作成します。

3 (S, G) エントリがない場合、MSDP ピアはソース ツリーに加入するためにソースへの (S, G) 加入をただちにトリガーします。

4 ピアは SA メッセージをその他のすべての MSDP ピアにフラッディングします。ただし、次を除きます。

- SA メッセージを受信した MSDP ピア。
- このデバイスと同じ MSDP メッシュ グループ内の MSDP ピア（ピアがメッシュ グループのメンバである場合）。

（注） SA メッセージは、デバイス SA キャッシュにローカルに保存されます。

MSDP ピア

BGP と同様に、MSDP は他の MSDP ピアとのネイバー関係を確立します。 MSDP ピアは TCP ポート 639 を使用して接続します。 IP アドレスが小さい方のピアは、TCP 接続を開くアクティブなロールを担います。 IP アドレスが大きい方のピアは、他方が接続を確立するのを LISTEN ステートで待機します。 MSDP ピアは、60 秒ごとにキープアライブ メッセージを送信します。 データが着信すると、キープアライブ メッセージと同じ機能が実行され、セッションがタイムアウトにならないようにします。 キープアライブ メッセージまたはデータが 75 秒間受信されない場合、TCP 接続はリセットされます。

MSDP MD5 パスワード認証

MSDP MD5 パスワード認証機能は、2 つの MSDP ピア間の TCP 接続上で Message Digest 5（MD5）シグネチャの保護を提供するための拡張です。 この機能は、TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護することにより、追加のセキュリティを提供します。

MSDP MD5 パスワード認証の動作

RFC 2385 に準拠して開発された MSDP MD5 パスワード認証機能は、MSDP ピア間の TCP 接続で送信された各セグメントを確認するために使用されます。 **ip msdp password peer** コマンドは、2 つの MSDP ピア間の TCP 接続の MD5 認証をイネーブルにするために使用されます。 2 つの MSDP ピア間で MD5 認証がイネーブルになると、ピア間の TCP 接続で送信された各セグメントが確認されます。 どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。 MD5 認証を設定すると、Cisco IOS ソフトウェアにより、TCP 接続上で送信される各セグメントについて MD5 ダイジェストが生成され、検証されるようになります。

MSDP MD5 パスワード認証の利点

- TCP 接続ストリームに入り込むスプーフィングされた TCP セグメントの脅威に対して MSDP を保護します。
- 業界標準の MD5 アルゴリズムを使用して信頼性およびセキュリティを向上させます。

SA メッセージの制限

デバイスが特定の MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、**ip msdp sa-limit** コマンドを使用します。 **ip msdp sa-limit** コマンドを設定すると、そのピア用に設定された SA メッセージの制限に到達した場合、デバイスは SA キャッシュに格納されている SA メッセージのピアごとの数を維持し、ピアからの新規メッセージを無視します。

MSDP 対応デバイスをサービス拒否（DoS）攻撃から保護するための手段として、**ip msdp sa-limit** コマンドが導入されました。 デバイス上のすべての MSDP ピアリングに対して SA メッセージの制限を設定することを推奨します。 適度に低い SA 制限をスタブ MSDP リージョンとのピアリングに設定する必要があります（たとえば、さらにダウンストリーム ピアを持つが、インターネットの残りの部分で SA メッセージの中継として動作しないピアなど）。 インターネット上の SA メッセージの中継として動作するすべての MSDP ピアリングに高い SA 制限を設定する必要があります。

MSDP キープアライブ インターバルおよび保留時間インターバル

MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を調整するには、**ip msdp keepalive** コマンドを使用します。

MSDP ピアリング セッションが確立されると、接続の各側はキープアライブ メッセージを送信し、キープアライブ タイマーを設定します。 キープアライブ タイマーの期限が切れると、ローカル MSDP ピアはキープアライブ メッセージを送信し、キープアライブ タイマーを再開します。この間隔をキープアライブ インターバルといいます。 *keepalive-interval* 引数がキープアライブ メッセージの送信間隔を調整するために使用されます。キープアライブ タイマーは、ピアがアップ状態のときに *keepalive-interval* 引数に指定された値に設定されます。 キープアライブ タイマーは、MSDP キープアライブ メッセージがピアに送信されるたびに *keepalive-interval* 引数の値にリセットされ、タイマーの期限が切れるとリセットされます。 キープアライブ タイマーは、MSDP ピアリング セッションが終了したときに削除されます。 デフォルトでは、keepalive タイマーは 60 秒に設定されます。

（注） *keepalive-interval* 引数に指定される値は、*holdtime-interval* 引数に指定される値未満にしなければならず、また、1 秒以上に設定する必要があります。

保留時間タイマーは、MSDP ピアリング接続が確立されると *hold-time-interval* 引数の値に初期化され、MSDP キープアライブ メッセージが受信されると *hold-time-interval* 引数の値にリセットされます。 保留時間タイマーは、MSDP ピアリング接続が閉じられると削除されます。 デフォルトでは、保留時間インターバルは 75 秒に設定されています。

MSDP ピアが他のピアがダウンしたと宣言するまで他のピアからのキープアライブ メッセージを待機する間隔を調整するには、*hold-time-interval* 引数を使用します。

MSDP 接続再試行インターバル

ピアリングセッションがリセットされてからピアリングセッションの再確立が試行されるまですべての MSDP ピアが待機する間隔を調整できます。 この間隔は、接続再試行インターバルと呼ばれます。デフォルトでは、ピアリングセッションがリセットされてから他のピアとのピアリングセッションの再確立が試行されるまで MSDP ピアは 30 秒間待機します。 変更された設定済み接続再試行インターバルは、デバイス上のすべての MSDP ピアリング セッションに適用されます。

MSDP の IETF RFC 3618 準拠

MSDP の IETF RFC 3618 準拠機能が設定されている場合は、IETF RFC 3618 で定義されているピア RPF 転送ルールが MSDP ピアに適用されます。 IETF RFC 3618 では、MSDP が使用可能なインターネット全体で SA メッセージを転送するために使用されるピア RPF 転送ルールが規定されています。 データ パケットの転送時に使用される RPF チェックではパケットのソース アドレスをパケットを受信したインターフェイスと比較しますが、ピア RPF チェックでは SA メッセージで送信される RP アドレスをメッセージを受信した MSDP ピアと比較します。 MSDP メッシュ グループを使用されている場合を除き、SA メッセージのループを避けるために RP アドレスからの SA メッセージは 1 つの MSDP ピアからだけ受け入れます。

（注） RFC 3618 で定義されている MSDP ピア転送ルールの詳細については、RFC 3618『Multicast Source Discovery Protocol（MSDP）』を参照してください。

MSDP の RFC 3618 準拠の利点

- BGP ルート リフレクタ（RR）で MSDP を実行しなくても、BGP RR を使用できます。 この機能は、RR の負荷を軽減する必要があるサービス プロバイダーに役立ちます。
- リバース パス転送（RPF）のチェックに Interior Gateway Protocol（IGP）を使用でき、そのため（M）BGP なしでピアリングを実行できます。 この機能は、（M）BGP を実行せず、メッシュ グループが提供できるものより大規模なトポロジを必要とする企業に役立ちます。

（注） IGP ピアリングは直接接続された MSDP ピア間に常に存在する必要があります。そうしないと、RPF チェックは失敗します。

- 直接接続されていない自律システム（つまり、1 つまたは複数の自律システムがその間に存在する）のルータ間でピアリングを設定できます。 この機能は、連合設定および冗長性に役立ちます。

デフォルト MSDP ピア

ほとんどのシナリオでは、MSDP ピアは BGP ピアでもあります。 自律システムがスタブまたは非中継自律システムであり、特に自律システムがマルチホーム化されてない場合、中継自律システムに BGP を実行する理由は、ほとんどまたはまったくありません。 一般に、スタブ自律システムのスタティックなデフォルト ルート、および中継自律システムのスタブ プレフィックスに接続するスタティックなルートで十分です。 ただし、スタブ自律システムがマルチキャスト ドメインでもあり、RP が隣接ドメイン内の RP とピアリングする必要がある場合は、MSDP は BGP ネクスト ホップ データベースを使用してピア RPF チェックを行います。 **ip msdp default-peer** コマンドを

使用して、ピア RPF チェックを実行せずにすべての SA メッセージを受け入れるデフォルト ピアを定義することにより、この BGP への依存をディセーブルにできます。 デフォルトの MSDP ピアは、事前に設定しておく必要があります。

スタブ自律システムには、冗長性を実現するために複数の RP との MSDP ピアリングが必要な場合もあります。 たとえば、RPF チェック メカニズムがないため、SA メッセージは複数のデフォルト ピアから受け入れられません。 代わりに、SA メッセージは 1 つのピアからのみ受け入れられます。 そのピアに障害が発生した場合、SA メッセージは別のピアから受け入れられます。 ここでの基本的な前提は、両方のデフォルト ピアが同じ SA メッセージを送信していることです。

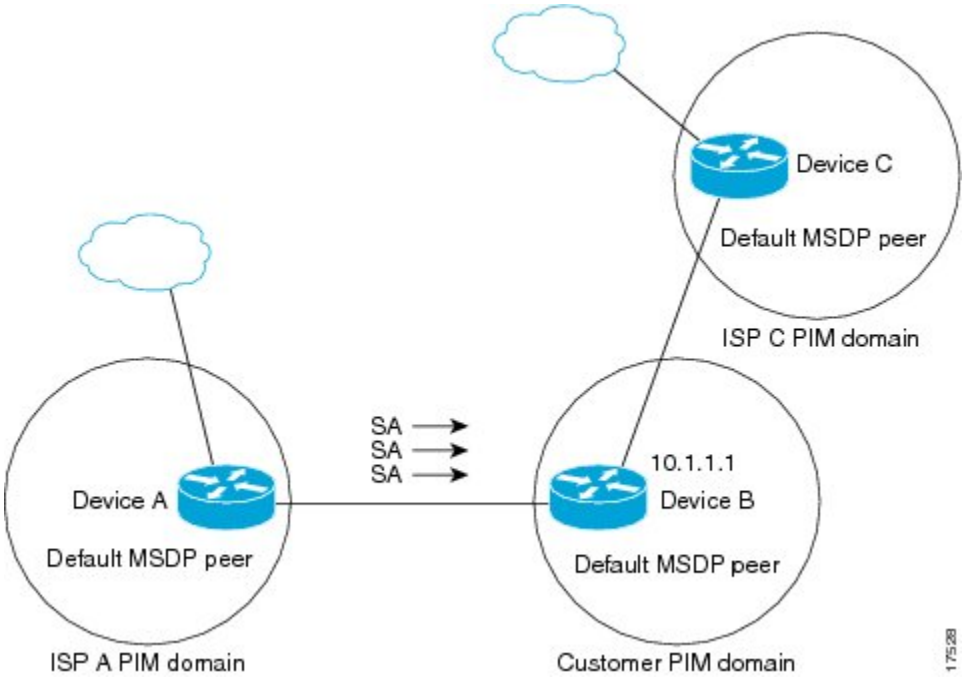
図に、デフォルト MSDP ピアが使用されるシナリオを示します。 この図では、ルータ B を所有するカスタマーが 2 つのインターネット サービス プロバイダー（ISP）を介してインターネットに接続されています。一方の ISP はルータ A を所有し、もう一方の ISP はルータ C を所有しています。 これらの ISP 間で、BGP または MBGP は動作していません。 カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、ルータ B はルータ A をデフォルト MSDP ピアとして識別します。 ルータ B はルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、ルータ A だけまたはルータ C だけから SA メッセージを受け入れます。 ルータ A が設定内の最初のデフォルト ピアである場合、ルータ A が稼働していればルータ A が使用されます。ルータ A が稼働していない場合に限り、ルータ B がルータ C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのルータから受け入れるプレフィックスを定義する場合もあります。 カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。 カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。 設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、

このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

図 *2*：デフォルト *MSDP* ピアのシナリオ



ルータ B はルータ A およびルータ C に SA をアドバタイズしますが、ルータ A またはルータ C だけを使用して SA メッセージを受け入れます。 ルータ A が設定内の最初のルータである場合、ルータ A が稼働していればルータ A が使用されます。 ルータ A が稼働していない場合に限り、ルータ B がルータ C から SA メッセージを受け入れます。 これは、プレフィックス リストがない場合の動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックスリストがそれぞれ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。 プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、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（このピアにルータが接続されていて、ピアがアクティブの場合に限ります）。 最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

MSDP メッシュ グループ

MSDP メッシュ グループは、MSDP によってフル メッシュ型に相互接続された MSDP スピーカーのグループです。 つまり、グループの各 MSDP ピアには、グループ内の他のすべての MSDP ピアとの MSDP ピアリング関係（MSDP 接続）が必要です。 MSDP メッシュ グループが MSDP ピアのグループ間に設定されている場合、SA メッセージのフラッディングが削減されます。 グループ内の MSDP ピアがグループ内の別の MSDP ピアから SA メッセージを受信すると、この SA メッ

セージはグループ内のその他のすべての MSDP ピアに送信されたとみなされるためです。その結果、受信側の MSDP ピアがグループ内の他の MSDP ピアに SA メッセージをフラッディングする必要はありません。

MSDP メッシュ グループの利点

- SA フラッディングの最適化：グループ内に複数のピアがある場合、SA フラッディングを最適化するために MSDP メッシュ グループは特に有用です。
- インターネットを通過する SA トラフィック量の削減：MSDP メッシュ グループを使用すると、SA メッセージは他のメッシュ グループ ピアにフラッディングされません。
- 着信 SA メッセージの RPF チェックの省略：MSDP メッシュ グループが設定されていると、メッシュ グループ ピアからの SA メッセージは常に受け入れられます。

SA 発信フィルタ

デフォルトでは、MSDP を実行するように設定されている RP は、それが RP であるすべてのローカル ソースの SA メッセージを発信します。そのため、RP に登録されているローカル ソースは SA メッセージでアドバタイズされますが、これが望ましくない場合もあります。たとえば、PIM-SM ドメイン内のソースがプライベート アドレス（たとえば、ネットワーク 10.0.0.0/8）を使用している場合、SA 発信フィルタを設定してこれらのアドレスがインターネット上の他の MSDP ピアにアドバタイズされないようにする必要があります。

どのソースが SA メッセージでアドバタイズされるかを制御するには、RP に SA 発信フィルタを設定します。SA 発信フィルタを作成すると、SA メッセージでアドバタイズされるソースを次のように制御できます。

- デバイスが SA メッセージのローカル ソースをアドバタイズしないように、RP を設定できます。デバイスは引き続き通常の方法で他の MSDP ピアからの SA メッセージを転送し、ローカル ソースの SA メッセージは送信しません。
- 拡張アクセス リストで定義されている（S, G）ペアと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- AS パス アクセス リストで定義されている AS パスと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- ルート マップで定義されている基準と一致するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- 拡張アクセス リスト、AS パス アクセス リスト、およびルート マップ、またはその組み合わせを含む SA 発信フィルタを設定します。この場合、ローカル ソースが SA メッセージでアドバタイズされる前に、すべての条件を満たしている必要があります。

MSDP での発信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは、受信したすべての SA メッセージをその MSDP ピアすべてに転送します。 ただし、発信フィルタ リストを作成することで、SA メッセージが MSDP ピアに転送されないようにすることができます。発信フィルタリストは、ローカルに発信されたか別の MSDP ピアから受信したかに関係なくすべての SA メッセージに適用されますが、SA 発信フィルタはローカルに発信された SA メッセージだけに適用されます。 ローカル デバイスから発信される MSDP SA メッセージのフィルタを有効にする方法の詳細については、ローカル ソースの RP によって発信された SA メッセージの制御, （33 ページ）を参照してください。

発信フィルタ リストを作成すると、デバイスがピアに転送する SA メッセージを次のように制御できます。

- MSDP ピアへの SA メッセージの転送を停止するようにデバイスを設定することにより、特定の MSDP ピアに転送されたすべての発信 SA メッセージをフィルタリングできます。
- 拡張アクセス リストで許可された（S, G）ペアと一致する SA メッセージだけを MSDP ピアに転送するようにデバイスを設定することにより、拡張アクセス リストで定義されている（S, G）ペアに基づいて、特定の MSDP ピアに転送された発信 SA メッセージのサブセットをフィルタリングできます。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- ルート マップで定義されている基準と一致する SA メッセージだけを転送するようにデバイスを設定することにより、ルートマップで定義されている一致基準に基づいて、特定の MSDP ピアに転送された発信 SA メッセージのサブセットをフィルタリングできます。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- SA メッセージが 1 つまたは複数の MSDP ピアに転送された後でも、発信元に基づいて発信 SA メッセージをフィルタリングするようにデバイスを設定することにより、SA メッセージに含まれる、アナウンスする RP アドレスに基づいて、特定のピアからの発信 SA メッセージのサブセットをフィルタリングできます。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む発信フィルタ リストを設定できます。 その場合、MSDP ピアで発信 SA メッセージを転送するにはすべての条件を満たしている必要があります。

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。 そのため、このタイプのフィルタを使用する場合は注意が必要です。 通常、発信フィルタ リストは、プライベート アドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用します。

MSDP での着信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは MSDP ピアからそのデバイスに送信されたすべての SA メッセージを受信します。 ただし、着信フィルタ リストを作成して、デバイスが MSDP ピアから受信するソース情報を制御できます。

着信フィルタ リストを作成すると、デバイスがピアから受信する着信 SA メッセージを次のように制御できます。

- 特定の MSDP ピアから送信されたすべての SA メッセージを無視するようにデバイスを設定することにより、特定の 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できます。
- 拡張アクセス リストで定義されている（S, G）ペアと一致する MSDP ピアからの SA メッセージだけを受信するようにデバイスを設定することにより、拡張アクセス リストで定義されている（S,G）ペアに基づいて、特定のピアからの着信 SA メッセージのサブセットをフィルタリングできます。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- ルート マップで定義されている基準と一致する SA メッセージだけを受信するようにデバイスを設定することにより、ルートマップで定義されている一致基準に基づいて、特定のピアからの着信 SA 要求メッセージのサブセットをフィルタリングできます。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 拡張アクセス リストで定義されている（S,G）ペアおよびルート マップで定義されている基準の両方と一致する着信 SA メッセージだけを受信するようにデバイスを設定することにより、拡張アクセス リストで定義されている（S,G）ペアおよびルート マップで定義されている一致基準の両方に基づいて、特定のピアからの着信 SA メッセージのサブセットをフィルタリングできます。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- SA メッセージが 1 つまたは複数の MSDP ピアに転送された後でも、発信元に基づいて着信 SA メッセージをフィルタリングするようにデバイスを設定することにより、SA メッセージに含まれる、アナウンスする RP アドレスに基づいて、特定のピアからの着信 SA メッセージのサブセットをフィルタリングできます。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む着信フィルタ リストを設定できます。 その場合、MSDP ピアで着信 SA メッセージを受信するにはすべての条件を満たしている必要があります。

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。 そのため、このタイプのフィルタを使用する場合は注意が必要です。 通常、着信フィルタ リストは、プライベートアドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用されます。

MSDP の TTL しきい値

存続可能時間（TTL）値を使用して、ドロップされる前にパケットが取得できるホップの数を制限できます。 特定の MSDP ピアに送信された、データがカプセル化された SA メッセージの TTL を指定するには、**ip multicast ttl-threshold** コマンドを使用します。 デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。

一般に、TTL しきい値の問題は、SA メッセージ内でソースの初期マルチキャスト パケットがカプセル化されることによって発生することがあります。マルチキャストパケットはユニキャスト SA メッセージ内部でカプセル化されるため（TTL は 255）、SA メッセージが MSDP ピアに送信されるときに TTL は減少しません。 さらに、マルチキャスト トラフィックおよびユニキャスト トラフィックは MSDP ピアへのまったく異なるパスと、その結果としてリモート PIM-SM ドメインへのまったく異なるパスに従うため、SA メッセージが通過するホップの総数は、通常のマルチキャスト パケットとは大きく異なります。 その結果、カプセル化されたパケットは TTL しきい値に違反することになります。 この問題を解決するには、**ip multicast ttl-threshold** コマンドを使用して、特定の MSDP ピアに送信された SA メッセージにカプセル化されているマルチキャスト パケットに関連付けられた TTL しきい値を設定します。 **ip msdp ttl-threshold** コマンドを使用すると、IP ヘッダーの TTL が *ttl-value* 引数に指定されている TTL 値未満であるマルチキャスト パケットが、ピアに送信される SA メッセージにカプセル化されないようにすることができます。

SA 要求メッセージ

非キャッシュ デバイスが 1 つ以上の特定の MSDP ピアに SA 要求メッセージを送信するように設定できます。

非キャッシュ RP に SA をキャッシュする MSDP ピアがある場合、非キャッシュ ピアが SA 要求メッセージを送信できるようにすると非キャッシュ ピアの参加遅延を低減できます。 ホストが特定のグループに対して加入を要求すると、非キャッシュ RP は SA 要求メッセージをキャッシュ ピアに送信します。 ピアがこの特定のグループのソース情報をキャッシュしている場合、SA 応答メッセージで要求側の RP に情報を送信します。 要求側の RP は SA 応答内の情報を使用しますが、他のピアにメッセージを転送しません。 非キャッシュ RP が SA 要求を受信すると、要求者にエラー メッセージを返します。

（注） 現行のすべてのサポートされているソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。 デフォルトでは、MSDP ピアが設定されると、設定済みコマンドが自動的に実行コンフィギュレーションに追加されます。

SA 要求フィルタ

デフォルトでは、デバイスはその MSDP ピアからのすべての発信 SA 要求メッセージを受け入れます。つまり、ルータはキャッシュされたソース情報を要求側の MSDP ピアに SA 応答メッセージで送信します。 SA 要求フィルタを作成すると、デバイスが特定のピアから受け入れる発信 SA 要求メッセージを制御できます。 SA 要求フィルタは、デバイスが MSDP ピアから受け入れる発信 SA 要求を次のように制御します。

- 特定の MSDP ピアからのすべての SA 要求メッセージを無視するようにデバイスを設定することにより、特定のピアからのすべての SA 要求メッセージをフィルタリングできます。
- 標準アクセス リストで定義されているグループと一致する MSDP ピアからの SA 要求メッセージだけを受け入れるようにデバイスを設定することにより、標準アクセス リストで定義されているグループに基づいて、特定のピアからの SA 要求メッセージのサブセットをフィルタリングできます。 その他のグループの指定されたピアからの SA 要求メッセージは無視されます。

MSDP MIB

MSDP MIB には、SNMP を介して MSDP スピーカーのリモート モニタリングを行う際に使用できる管理対象オブジェクトが規定されています。 MSDP MIB モジュールには、スカラ オブジェクトが 4 つとテーブルが 3 つあります。 このテーブルは、要求テーブル、ピア テーブル、および Source-Active（SA）キャッシュ テーブルです。 シスコの実装では、ピア テーブルと SA キャッシュ テーブルだけがサポートされています。 要求テーブルには、SA 要求の送信先のピアを決定するために使用される情報が含まれています。 ただし、Cisco IOS ソフトウェアで使用される MSDP 実装では、ピアへの SA 要求の送信はグループ アドレス（またはグループ アドレス マスク）に関連付けられていません。

（注） MSDP-MIB.my ファイルは、次の URL にある Cisco.com の Cisco MIB Web サイトからダウンロードできます。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml。

MSDP を使用して複数の PIM-SM ドメインを相互接続する方法

最初の作業は必須で、他の作業はすべて任意です。

MSDP ピアの設定

（注） MSDP ピアをイネーブルにすることで、MSDP は暗黙的にイネーブルになります。

はじめる前に

- IP マルチキャスト ルーティングをイネーブルにし、PIM-SM を設定する必要があります。
- 単一の MSDP ピア、デフォルト MSDP ピア、および MSDP メッシュ グループのシナリオを除いて、すべての MSDP ピアは、MSDP 用に設定する前に BGP を実行するように設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*]
4. **ip msdp description** {*peer-name*| *peer-address*} *text*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*]	MSDP をイネーブルにし、DNS 名または IP アドレスによって指定された MSDP ピアを設定します。 （注） MSDP ピアとして設定するように選択されたデバイスは、通常 BGP ネイバーでもあります。 そうでない場合は、デフォルトの MSDP ピアの設定, （30 ページ）またはMSDP メッシュ グループの設定, （31 ページ）を参照してください。

	コマンドまたはアクション	目的
	例： `Device(config)# ip msdp peer 192.168.1.2 connect-source loopback0`	• **connect-source** キーワードを指定した場合、指定したローカル インターフェイスの *type* および *number* の値のプライマリ アドレスは TCP 接続のソース IP アドレスとして使用されます。 特にリモート ドメイン内のデバイスとピアリングする境界上の MSDP ピアに対しては、**connect-source** キーワードが推奨されます。
ステップ 4	**ip msdp description** {*peer-name*| *peer-address*} *text* 例： `Device(config)# ip msdp description 192.168.1.2 router at customer a`	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピアのシャットダウン

MSDP ピアをシャットダウンするには、次の任意の作業を実行します。

複数の MSDP ピアを設定していて、すべてのピアの設定が完了するまでいずれのピアもアクティブにしない場合は、各ピアをシャット ダウンし、各ピアを設定した後で起動することができます。 MSDP ピアの設定を失わずに、MSDP セッションをシャットダウンすることもできます。

（注） MSDP ピアがシャット ダウンされると、TCP 接続は終了し、（指定されたピアに対して）**no ip msdp shutdown** コマンドを使用してピアを再起動するまで再開されません。

はじめる前に

MSDP を実行していること、および MSDP ピアを設定することが必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp shutdown** {*peer-name* | *peer-address*}
4. 別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp shutdown** {*peer-name* | *peer-address*} 例： `Device(config)# ip msdp shutdown 192.168.1.3`	指定された MSDP ピアを管理上シャットダウンします。
ステップ 4	別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。	--
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピア間の MSDP MD5 パスワード認証の設定

MSDP ピア間の MSDP Message Digest 5（MD5）パスワード認証を設定するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*
4. **exit**
5. **show ip msdp peer** [peer-address | peer-name]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string* 例： `Device(config)# ip msdp password peer 10.32.43.144 0 test`	2 つの MSDP ピア間の TCP 接続で MD5 パスワード暗号化をイネーブルにします。 （注） どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。 • 2 つの MSDP ピア間の MD5 認証で使用するパスワードやキーを設定または変更する場合、パスワードを設定した後、ローカル デバイスは既存のセッションを解放しません。 ローカル デバイスは、キープアライブ期間が期限切れになるまで新しいパスワードを使用してピアリング セッションを維持しようとします。 キープアライブ期間が期限切れになるまでにリモート デバイスでパスワードが入力または変更されなかった場合、セッションはタイムアウトし、MSDP セッションはリセットされます。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show ip msdp peer** [peer-address | peer-name] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドを使用して、MSDP ピアで MD5 パスワード認証がイネーブルになっているかどうかを確認します。

トラブルシューティングのヒント

デバイスに MSDP ピアのパスワードが設定されており、MSDP ピアに設定されていない場合、デバイスが MSDP ピアとの間にセッションを確立しようとすると、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

同様に、2 台のデバイスに異なるパスワードが設定されている場合、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

debug ip tcp transactions コマンドを使用すると、ステートの変更、再送、重複するパケットなどの重要な TCP トランザクションに関する情報が表示されます。 MSDP MD5 パスワード認証のモニタリングやトラブルシューティングでは、**debug ip tcp transactions** コマンドを使用して、MD5 パスワードがイネーブルになっていること、およびキープアライブ メッセージが MSDP ピアによって受信されたことを確認します。

SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージ数の制限によるサービス拒絶（DoS）攻撃の防止

デバイスが特定の MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、この任意の作業（ただし強く推奨されます）を実行します。 この作業を実行することで、分散型サービス拒否攻撃（DoS）から MSDP 対応デバイスを保護します。

（注） デバイス上のすべての MSDP ピアリングに対してこの作業を実行することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit*
4. 別の MSDP ピアの SA 制限を設定するには、ステップ 3 を繰り返します。
5. **exit**
6. **show ip msdp count** [*as-number*]
7. **show ip msdp peer** [*peer-address* | *peer-name*]
8. **show ip msdp summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit* 例： `Device(config)# ip msdp sa-limit 192.168.10.1 100`	SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージの数を制限します。
ステップ 4	別の MSDP ピアの SA 制限を設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ip msdp count** [*as-number*] 例： `Device# show ip msdp count`	（任意）MSDP SA メッセージ内で発信されたソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。

	コマンドまたはアクション	目的
ステップ 7	**show ip msdp peer** [*peer-address* | *peer-name*] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドの出力には、キャッシュに格納されている MSDP ピアから受信した SA メッセージの数が表示されます。
ステップ 8	**show ip msdp summary** 例： `Device# show ip msdp summary`	（任意）MSDP ピアのステータスを表示します。 （注） このコマンドの出力には、キャッシュに格納されている SA の数を表示するピアごとの「SA Count」フィールドが表示されます。

MSDP キープアライブ インターバルおよび保留時間インターバルの調整

MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を調整するには、次の任意の作業を実行します。 デフォルトでは、MSDP ピアが別の MSDP ピアとのピアリング セッションが停止したことを検出するために 75 秒かかる場合があります。 冗長 MSDP ピアがあるネットワーク環境では、保留時間インターバルを短くすると、MSDP ピアに障害が発生した場合に MSDP ピアの再コンバージェンス時間を短縮できます。

（注） **ip msdp keepalive** コマンドのデフォルト値は RFC 3618『*Multicast Source Discovery Protocol*』に準拠しているため、コマンドのデフォルト値を変更しないことを推奨します。 ネットワーク環境でデフォルト値を変更する必要がある場合は、MSDP ピアリング セッションの両端で *keepalive-interval* および *hold-time-interval* 引数に同じ時間値を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval*
4. 別の MSDP ピアのキープアライブ メッセージの間隔を調整するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval* 例： `Device(config)# ip msdp keepalive 10.1.1.3 40 55`	MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンとしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を設定します。
ステップ 4	別の MSDP ピアのキープアライブ メッセージの間隔を調整するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP 接続再試行インターバルの調整

ピアリングセッションがリセットされてからピアリングセッションの再確立が試行されるまですべての MSDP ピアが待機する間隔を調整するには、次の任意の作業を実行します。 SA メッセージの迅速なリカバリが必要なネットワーク環境（金融機関の取引フロアのネットワーク環境など）では、接続再試行インターバルをデフォルト値の 30 秒未満に短縮することが必要な場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp timer** *connection-retry-interval*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp timer** *connection-retry-interval* 例： `Device# ip msdp timer 45`	ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまで MSDP ピアが待機する間隔を設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP の IETF RFC 3618 準拠の設定

インターネット技術特別調査委員会（IETF）RFC 3618 の MSDP の仕様に準拠するように MSDP ピアを設定するには、次の任意作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp rpf rfc3618**
4. **end**
5. **show ip msdp rpf-peer** *rp-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip msdp rpf rfc3618** 例： `Router(config)# ip msdp rpf rfc3618`	IETF RFC 3618 で指定されているピア RPF 転送ルールに準拠するようにします。
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip msdp rpf-peer** *rp-address* 例： `Router# show ip msdp rpf-peer 192.168.1.5`	（任意）指定された RP から発信される SA メッセージをルータが受け入れる固有の MSDP ピア情報を表示します。

デフォルトの MSDP ピアの設定

デフォルト MSDP ピアを設定するには、次の任意の作業を実行します。

はじめる前に

デフォルト MSDP ピアは、事前に設定されている MSDP ピアでなければなりません。デフォルト MSDP ピアを設定する前に、まず MSDP ピアを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*] 例： `Device(config)# ip msdp default-peer 192.168.1.3`	すべての MSDP SA メッセージの受信元となるデフォルト ピアを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP メッシュ グループの設定

MSDP メッシュ グループを設定するには、次の任意の作業を実行します。

（注） デバイスごとに複数のメッシュ グループを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*}
4. MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*} 例： `Device(config)# ip msdp mesh-group peermesh`	MSDP メッシュ グループを設定し、MSDP ピアがそのメッシュ グループに属することを指定します。 （注） メッシュ グループに参加するデバイスのすべての MSDP ピアは、グループ内の他のすべての MSDP ピアと完全にメッシュ化されている必要があります。 各デバイスの各 MSDP ピアは、**ip msdp peer** コマンドを使用してピアとして設定する必要があり、また、**ip msdp mesh-group** コマンドを使用してメッシュ グループのメンバとしても設定する必要があります。
ステップ 4	MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ローカル ソースの RP によって発信された SA メッセージの制御

SA メッセージでアドバタイズされる登録ソースを制限するフィルタをイネーブルにして、RP によって発信された SA メッセージを制御するには、次の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*] 例： `Device(config)# ip msdp redistribute route-map customer-sources`	ローカル デバイスによって発信される MSDP SA メッセージのフィルタをイネーブルにします。 （注） **ip msdp redistribute** コマンドは、RP で認識されているが登録されていないソースをアドバタイズするために使用することもできます。 ただし、RP に登録されていないソースのアドバタイズメントは発信しないことを強く推奨します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

発信フィルタ リストを使用した SA メッセージの MSDP ピアへの転送の制御

発信フィルタ リストを設定して SA メッセージの MSDP ピアへの転送を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. 別の MSDP ピアの発信フィルタ リストを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter out 192.168.1.5 peerone`	発信 MSDP メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの発信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

着信フィルタ リストを使用した MSDP ピアからの SA メッセージの受信の制御

MSDP ピアからの着信 SA メッセージの受信を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. 別の MSDP ピアの着信フィルタ リストを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter in 192.168.1.3`	着信 MSDP SA メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの着信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TTL しきい値を使用した SA メッセージで送信されたマルチキャスト データの制限

存続可能時間（TTL）しきい値を設定して、SA メッセージで送信されるマルチキャスト データを制限するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value* 例： 例： `Device(config)# ip msdp ttl-threshold 192.168.1.5 8`	ローカル デバイスにより発信される MSDP メッセージの TTL 値を設定します。 • デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピアへのソース情報の要求

デバイスが MSDP ピアにソース情報を要求できるようにするには、次の任意の作業を実行します。

（注） SA キャッシングはデフォルトでイネーブルになっており、以前の Cisco ソフトウェア リリースでは明示的にイネーブルまたはディセーブルにすることができないため、この作業を実行する必要はほとんどありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-request** {*peer-address* | *peer-name*}
4. デバイスが別の MSDP キャッシュ ピアに SA 要求メッセージを送信するように指定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp sa-request** {*peer-address* | *peer-name*} 例： `Device(config)# ip msdp sa-request 192.168.10.1`	デバイスが指定された MSDP ピアに SA 要求メッセージを送信するように指定します。
ステップ 4	デバイスが別の MSDP キャッシュ ピアに SA 要求メッセージを送信するように指定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御

デバイスが MSDP ピアから受け入れる発信 SA 要求メッセージを制御するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]
4. 別の MSDP ピアの SA 要求フィルタを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*] 例： `Device(config)# ip msdp filter sa-request 172.31.2.2 list 1`	発信 SA 要求メッセージのフィルタをイネーブルにします。 （注） MSDP ピアには SA 要求フィルタを 1 つだけ設定できます。
ステップ 4	別の MSDP ピアの SA 要求フィルタを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

境界 PIM デンス モード リージョンの MSDP への包含

PIM デンス モード（PIM-DM）リージョンでアクティブなソースの SA メッセージを送信するように境界デバイスを設定するには、次の任意作業を実行します。

PIM-SM リージョンと PIM-DM リージョンの境界にデバイスを設定できます。 デフォルトでは、PIM-DM ドメインのソースは MSDP に含まれません。 PIM-DM ドメインでアクティブなソースの SA メッセージを送信するようにこの境界デバイスを設定できます。 その場合、**ip msdp redistribute** コマンドを設定してアドバタイズする PIM-DM ドメインのローカル ソースを制御することも非常に重要です。 このコマンドを設定しないと、PIM-DM ドメインのソースが送信を停止した後も長時間 (S, G) ステートのままになります。 設定の詳細については、ローカル ソースの RP によって発信された SA メッセージの制御, （33 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp border sa-address** *type number*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp border sa-address** *type number* 例： `Device(config)# ip msdp border sa-address gigabitethernet0/0/0`	PIM-DM ドメインでアクティブなソースの SA メッセージを発信するように、PIM-SM および PIM-DM ドメイン間の境界にデバイスを設定します。 • インターフェイスの IP アドレスは、SA メッセージの RP フィールドに示されるソース ID として使用されます。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RP アドレス以外のソース アドレスの設定

SA メッセージを発信する MSDP スピーカーがその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できるようにするには、次の任意の作業を実行します。

また、次のいずれかの理由から、発信 ID を変更できます。

- Anycast RP の MSDP メッシュ グループに複数のデバイスを設定する場合。
- デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にある場合。 デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にあり、PIM-DM ドメイン内のアクティブなソースをアドバタイズする場合は、SA メッセージ内の RP アドレスがソース デバイスのインターフェイスのアドレスとなるように設定します。

はじめる前に

MSDP がイネーブルであり、MSDP ピアが設定されている必要があります。 MSDP ピアの設定の詳細については、MSDP ピアの設定, （21 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp originator-id** *type number*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip msdp originator-id** *type number* 例： `Device(config)# ip msdp originator-id ethernet 1`	SA メッセージ内の RP アドレスをソース デバイスのインターフェイスのアドレスになるように設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP のモニタリング

MSDP の SA メッセージ、ピア、ステート、およびピアのステータスをモニタリングするには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
3. **debug ip msdp resets**
4. **show ip msdp count** [*as-number*]
5. **show ip msdp peer** [*peer-address* | *peer-name*]
6. **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]
7. **show ip msdp summary**

手順の詳細

ステップ 1 **enable**

例：

```
Device# enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]

このコマンドを使用して、MSDP アクティビティをデバッグします。

オプションの *peer-address* 引数または *peer-name* 引数を使用して、デバッグ イベントをログに記録するピアを指定します。

次に、**debug ip msdp** コマンドの出力例を示します。

例：

```
Device# debug ip msdp
MSDP debugging is on
Device#
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 192.168.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 192.168.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.250: Forward 32-byte SA to peer
```

ステップ 3 **debug ip msdp resets**

このコマンドを使用して、MSDP ピアのリセット理由をデバッグします。

例：

```
Device# debug ip msdp resets
```

ステップ 4 **show ip msdp count** [*as-number*]

このコマンドを使用して、MSDP SA メッセージ内で発信したソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。 何らかの出力を得るためには、このコマンドに **ip msdp cache-sa-state** コマンドを設定しておく必要があります。

次に、**show ip msdp count** コマンドの出力例を示します。

例：

```
Device# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
    192.168.4.4: 8
```

```
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 8
    ?: 8/8
```

ステップ 5 **show ip msdp peer** [*peer-address* | *peer-name*]

このコマンドを使用して、MSDP ピアに関する詳細情報を表示します。

オプションの *peer-address* 引数または *peer-name* 引数を使用して、特定のピアに関する情報を表示します。

次に、**show ip msdp peer** コマンドの出力例を示します。

例：

```
Device# show ip msdp peer 192.168.4.4
MSDP Peer 192.168.4.4 (?), AS 64512 (configured AS)
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (2.2.2.2)
    Uptime(Downtime): 00:07:55, Messages sent/received: 8/18
    Output messages discarded: 0
    Connection and counters cleared 00:08:55 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 8
  Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
```

ステップ 6 **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]

このコマンドを使用して、MSDP ピアから学習した (S, G) ステートを表示します。

次に、**show ip msdp sa-cache** コマンドの出力例を示します。

例：

```
Device# show ip msdp sa-cache
MSDP Source-Active Cache - 8 entries
(10.44.44.5, 239.232.1.0), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.1), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.2), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.3), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.4), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.5), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.6), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.7), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
```

ステップ 7 **show ip msdp summary**

このコマンドを使用して、MSDP ピアのステータスを表示します。

次に、**show ip msdp summary** コマンドの出力例を示します。

例：

```
Device# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
```

```
                                Downtime Count Count
192.168.4.4       4     Up      00:08:05 0     8     ?
```

MSDP 接続、統計情報、および SA キャッシュ エントリの消去

MSDP 接続、統計情報、および SA キャッシュ エントリを消去するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **clear ip msdp peer** [*peer-address* | *peer-name*]
3. **clear ip msdp statistics** [*peer-address* | peer-name]
4. **clear ip msdp sa-cache** [*group-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip msdp peer** [*peer-address* | *peer-name*] 例： `Device# clear ip msdp peer`	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 3	**clear ip msdp statistics** [*peer-address* | peer-name] 例： `Device# clear ip msdp statistics`	指定された MSDP ピアの統計情報カウンタをクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 4	**clear ip msdp sa-cache** [*group-address*] 例： `Device# clear ip msdp sa-cache`	SA キャッシュ エントリを消去します。 • **clear ip msdp sa-cache** コマンドにオプションの *group-address* 引数または *source-address* 引数を指定した場合、すべての SA キャッシュ エントリは消去されます。

	コマンドまたはアクション	目的
		• 特定のグループに関連付けられたすべてのSAキャッシュエントリを消去するには、オプションの *group-address* 引数を使用します。

MSDPの簡易ネットワーク管理プロトコル（SNMP）モニタリングのイネーブル化

MSDPの簡易ネットワーク管理プロトコル（SNMP）モニタリングをイネーブルにするには、次の任意の作業を実行します。

はじめる前に

- SNMP および MSDP がデバイスに設定されています。
- 各 PIM-SM ドメインには、MSDP スピーカーとして設定されているデバイスが必要です。 このデバイスは、SNMP と MSDP MIB がイネーブルに設定されている必要があります。

（注）
- すべての MSDP-MIB オブジェクトは読み取り専用として実装されます。
- 要求テーブルは、シスコの MSDP MIB の実装ではサポートされていません。
- msdpEstablished 通知は、シスコの MSDP MIB の実装ではサポートされていません。

手順の概要

1. **enable**
2. **snmp-server enable traps msdp**
3. **snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**snmp-server enable traps msdp** 例： `Device# snmp-server enable traps msdp`	SNMP で使用される MSDP 通知の送信をイネーブルにします。 （注） **snmp-server enable traps msdp** コマンドは、トラップと応答要求の両方をイネーブルにします。
ステップ 3	**snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp** 例： `Device# snmp-server host examplehost msdp`	MSDP トラップまたは応答要求の受信者（ホスト）を指定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

MSDP MIB 通知の結果とソフトウェアの出力を比較するには、適切なデバイスで **show ip msdp summary** コマンドおよび **show ip msdp peer** コマンドを使用します。 また、これらのコマンドの結果と SNMP GET 操作の結果を比較することもできます。 SA キャッシュ テーブル エントリを確認するには、**show ip msdp sa-cache** コマンドを使用します。 接続のローカル アドレス、ローカル ポート、リモート ポートなどのその他のトラブルシューティング情報は、**debug ip msdp** コマンドの出力を使用して取得できます。

MSDP を使用して複数の PIM-SM ドメインを相互接続する設定例

例：MSDP ピアの設定

次に、3 つの MSDP ピア間で MSDP ピアリング接続を確立する例を示します。

デバイス A

```
!
interface Loopback 0
 ip address 10.220.8.1 255.255.255.255
!
ip msdp peer 10.220.16.1 connect-source Loopback0
ip msdp peer 10.220.32.1 connect-source Loopback0
!
```

デバイス B

```
!
interface Loopback 0
 ip address 10.220.16.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect connect-source Loopback0
ip msdp peer 10.220.32.1 connect connect-source Loopback0
!
```

デバイス C

```
!
interface Loopback 0
 ip address 10.220.32.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect 10.220.8.1 connect-source Loopback0
ip msdp peer 10.220.16.1 connect 10.220.16.1 connect-source Loopback0
!
```

例：MSDP MD5 パスワード認証の設定

次に、2 つの MSDP ピア間の TCP 接続の MD5 パスワード認証をイネーブルにする例を示します。

デバイス A

```
!
ip msdp peer 10.3.32.154
ip msdp password peer 10.3.32.154 0 test
!
```

デバイス B

```
!
ip msdp peer 10.3.32.153
ip msdp password peer 10.3.32.153 0 test
!
```

MSDP の IETF RFC 3618 準拠の設定の例

次に、10.10.2.4 および 10.20.1.2 の MSDP ピアを IETF RFC 3618 で指定されているピア RPF 転送ルールに準拠するように設定する例を示します。

```
ip msdp peer 10.10.2.4
ip msdp peer 10.20.1.2
ip msdp rpf rfc3618
```

デフォルト MSDP ピアの設定の例

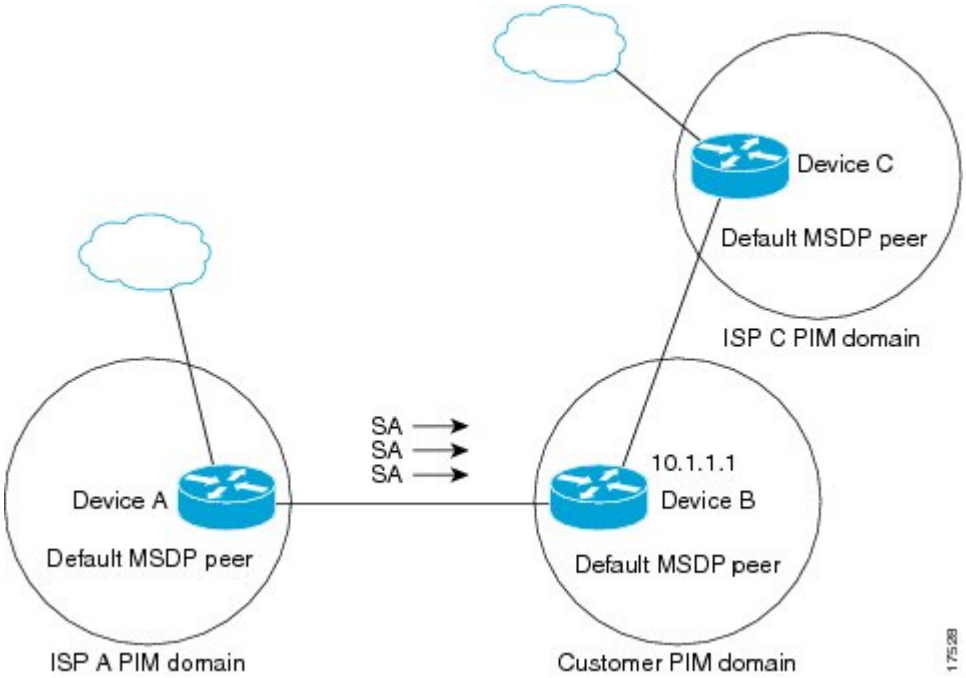
図に、デフォルト MSDP ピアが使用されるシナリオを示します。 この図では、ルータ B を所有するカスタマーが 2 つの ISP を介してインターネットに接続されています。一方の ISP はルータ A を所有し、もう一方の ISP はルータ C を所有しています。 これらの ISP 間で、（M）BGP は動作していません。 カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、ルータ B はルータ A をデフォルト MSDP ピアとして識別します。 ルータ B はルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、ルータ A だけまたはルータ C だけから SA メッセージを受け入れます。 ルータ A が設定内の最初のデフォルト ピアである場合、ルータ A が稼働していればルータ A が使用されます。 ルータ A が稼働していない場合に限り、ルータ B がルータ C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのルータから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。 カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。 設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、

このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

図 *3*：デフォルト *MSDP* ピアのシナリオ



ルータ B はルータ A およびルータ C に SA をアドバタイズしますが、ルータ A またはルータ C だけを使用して SA メッセージを受け入れます。 ルータ A が設定ファイル内の最初のルータである場合、ルータ A が稼働していればルータ A が使用されます。 ルータ A が稼働していない場合に限り、ルータ B がルータ C から SA メッセージを受け入れます。 これは、プレフィックス リストがない場合の動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックスリストがそれぞれ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。 プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、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（このピアにルータが接続されていて、ピアがアクティブの場合に限ります）。 最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

次に、図に示されているルータ A およびルータ C の部分的な設定例を示します。 これらの ISP にはそれぞれ、図に示すデフォルト ピアリングを使用するカスタマーのような複数のカスタマーがある場合があります。 そのようなカスタマーの設定は類似しています。 つまり、SA が対応するプレフィックス リストによって許可される場合、デフォルト ピアからの SA だけを受け入れます。

ルータ A の設定

```
ip msdp default-peer 10.1.1.1
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

ルータ C の設定

```
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

例：MSDP メッシュ グループの設定

次に、3 台のデバイスを MSDP メッシュ グループのフル メッシュ メンバになるように設定する例を示します。

デバイス A の設定

```
ip msdp peer 10.2.2.2
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.2.2.2
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス B の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス C の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.2.2.2
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.2.2.2
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2385	『Protection of BGP Sessions via the TCP MD5 Signature Option』
RFC 2858	『Multiprotocol Extensions for BGP-4』
RFC 3618	『Multicast Source Discovery Protocol』

MIB

MIB	MIB のリンク
MSDP-MIB.my	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MSDP を使用して複数の PIM-SM ドメインを相互接続するための機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*MSDP* を使用して複数の *PIM-SM* ドメインを相互接続するための機能情報

機能名	リリース	機能情報
Multicast Source Discovery Protocol（MSDP）	Cisco IOS XE Release 2.1 Cisco IOS Xe Release 3.5S	Multicast Source Discovery Protocol（MSDP）は、複数の PIM スパース モード（SM）ドメインを接続するためのメカニズムです。 MSDP を使用すると、さまざまなドメイン内のすべてのランデブー ポイント（RP）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 ドメインは自身の RP を使用するため、他のドメインの RP に依存する必要はありません。 RP は、MSDP を TCP 上で実行して他のドメインのマルチキャスト ソースを検出します。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。

機能名	リリース	機能情報
MSDP の IETF RFC 3618 準拠	Cisco IOS XE Release 2.1	MSDP の IETF RFC 3618 準拠機能は、IETF RFC 3618 仕様で規定されているピアと RPF 間の転送ルールに準拠するように MSDP を設定できるようにします。 MSDP の IETF RFC 3618 準拠機能をイネーブルにすると、SA メッセージのループを防止できます。 また、MSDP の IETF RFC 3618 準拠機能をイネーブルにすることで、BGP RR で MSDP を実行する必要がなくなり、RPF チェックに IGP を使用でき、直接接続されていない自律システムのルータ間で MSDP ピアリングが可能になります。 この機能により、**ip msdp rpf rfc3618** コマンドおよび **show ip msdp rpf-peer** コマンドが導入または変更されました。
MSDP MD5 パスワード認証	Cisco IOS XE Release 2.5	MSDP MD5 パスワード認証機能は、2 つの MSDP ピア間の TCP 接続上で MD5 シグネチャの保護を提供するための拡張です。 この機能は、TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護することにより、追加のセキュリティを提供します。 この機能により、**ip msdp password peer** コマンドおよび **show ip msdp peer** コマンドが導入または変更されました。