MSDP の設定

MSDP を使用した複数の PIM-SM ドメインの相互接続の前提条件

MSDP を設定する前に、すべての MSDP ピアのアドレスが Border Gateway Protocol（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

ここでは、MSDP を使用した複数の PIM-SM ドメインの相互接続について説明します。

MSDP を使用した複数の PIM-SM ドメインの相互接続の利点

- ランデブー ポイント(RP)が動的にドメイン外のアクティブな送信元を検出できます。
- 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、より管理しやすいアプローチが導入されます。

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 は、他の PIM ドメイン内のマルチキャスト送信元を検出することを目的としています。MSDP の主な利点は、（一般的な共有ツリーではなく）ドメイン間ソース ツリーを PIM-SM ドメインで使用できるようにし、複数の PIM-SM ドメインを相互接続する複雑性を軽減することです。MSDP がネットワークで設定されている場合、RP は他のドメイン内の RP と送信元情報を交換します。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。RP は、そのドメイン内の共有ツリーのルートであり、アクティブ 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ため、これを行うことができます。PIM-SM ドメイン外の新しい送信元を（共有ツリーの送信元からのマルチキャストパケットの到着によって）ラスト ホップ デバイスが認識すると、その送信元に加入要求を送信してドメイン間ソース ツリーに参加できます。

（注） RP に特定グループの共有ツリーがないか、発信インターフェイス リストがヌルの共有ツリーがある場合は、別のドメインの発信元に加入要求を送信しません。

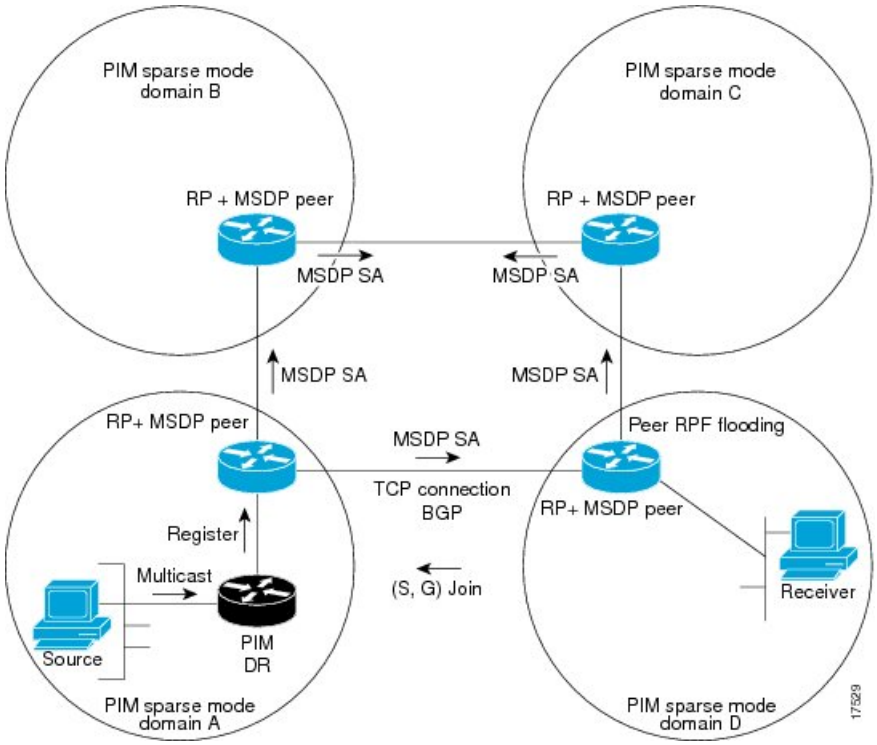
MSDP がイネーブルになっている場合、PIM-SM ドメインの RP は、他のドメインの MSDP 対応デバイスとの MSDP ピアリング関係を維持します。このピアリング関係は TCP 接続を通じて発生します。交換されるのは主にマルチキャスト グループを送信する送信元のリストです。MSDP はピアリング接続に TCP（ポート 639）を使用します。BGP と同様に、ポイントツーポイント TCP ピアリングを使用する場合は、各ピアを明示的に設定する必要があります。さらに、RP 間の TCP 接続は基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送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、ドメイン間動作を行うための BGP または Multiprotocol BGP（MBGP）によって異なります。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 ピア間の MSDP の動作を示します。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。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

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 指定デバイス（DR）が送信元を RP に登録すると、その RP が Source-Active（SA）メッセージをすべての MSDP ピアに送信します。

（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。これは、発信元 RP に登録されているすべての発信元を含んでいる定期的な SA メッセージの場合とは異なります。これらの SA メッセージは MSDP 制御パケットであるため、アクティブな送信元からのカプセル化されたデータを含んでいません。

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 PIM-SM ドメイン B および C 内の RP の場合など）、RP は複数の MSDP ピアからの 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、MBGP が最初に確認されてからユニキャスト BGP が確認されます。そのネクストホップ ネイバーが発信元の RPF ピアです。RPF ピアへのインターフェイス以外のインターフェイスにある発信元から受信した

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須ではありません。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 （26 ページ）」を参照してください。
- （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 （25 ページ）の項を参照してください。

1. SA メッセージを受信した RP は、グループの (*, G) 送信インターフェイス リストにインターフェイスが存在するかどうかを確認することによって、そのドメイン内にアドバタイズされたグループのメンバが存在す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（S, G）加入要求を送信元に送信します。その結果、ドメイン間ソース ツリーのブランチが自律システムの RP との境界に構築されます。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. 発信元 RP は、送信元がグループにパケットを送信し続ける限り、60 秒ごとに（S, G）ステートに関する SA メッセージを定期的に送信し続けます。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、発信元 RP 10.5.4.3 から (172.16.5.4, 228.1.2.3) に対する SA メッセージを受信したとします。RP は mroute テーブルを確認し、グループ 228.1.2.3 にアクティブなメンバが存在しないことを検出すると、SA メッセージを 10.5.4.3 のダウンストリームにあるピアに渡します。次に、ドメイン内のホストが加入要求をグループ 228.1.2.3 の RP に送信した場合、その 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、デバイスは (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対象のソフトウェア 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

MSDP メッセージには4つの基本タイプがあり、それぞれが固有の Type、Length、および Value（TLV）データ フォーマットでエンコードされています。

SA メッセージ

SA メッセージを使用して、ドメイン内のアクティブなソースをアドバタイズします。また、これらの SA メッセージには送信元によって送信された最初のマルチキャスト データ パケットが含まれていることがあります。

SA メッセージには、発信元 RP の IPアドレスと、アドバタイズされる 1 つ以上の（S, G）ペアが含まれています。また、SA メッセージにカプセル化されたデータ パケットが含まれていることがあります。

（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要求メッセージを使用して、特定のグループにアクティブなソースのリストを要求します。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。グループ内のすべてのアクティブなソースが発信元の RP によって再アドバタイズされるまで待つ代わりに、SA 要求メッセージを使用してアクティブなソースのリストを要求すると、加入遅延を短縮できます。

（注） SA 要求メッセージの詳細については、MSDP ピアへの送信元情報の要求 （31 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答する MSDP ピアによって送信されます。SA 応答メッセージには、発信元の RP の IP アドレスと、キャッシュに保存されている発信元 RP のドメイン内のアクティブなソースの 1 つ以上の（S, G）ペアが含まれています。

（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 （32 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 60 秒ごとに送信され、MSDP セッションをアクティブに保ちます。キープアライブ メッセージまたは SA メッセージを 75 秒間受信しなかった場合、MSDP セッションがリセットされます。

（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 （24 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）。ローカル送信元は、RP に直接接続された送信元であるか、または RP に登録済みのファーストホップ DR です。RP は、PIM-SM ドメイン内のローカル送信元（つまり、RP に登録しているローカル送信元）に対してのみ SA メッセージを発信します。

（注） ローカル送信元は、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、送信元が他の MSDP ピアに対する RP によるアドバタイズメントの候補であることを示します。

送信元がローカルの PIM-SM ドメインにある場合、RP で (S, G) ステートが作成されます。登録メッセージを受信するか、または直接接続された送信元から最初の (S, G) パケットが到着することによって、新しい送信元は RP によって検出されます。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、送信元に戻るベスト パスにある MSDP RPF ピアからのみ受け入れられます。他の MSDP ピアから到着する同じ SA メッセージは無視する必要があり、そうしないと SA ループが発生する可能性があります。到着した SA メッセージの MSDP RPF ピアを確定的に選択するには、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配信しません。MSDP は、SA RPF チェック機能に関する MSDP トポロジの最良近似として (M)BGP ルーティング データを使用することで、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。わずかな例外（MSDP メッシュ グループ内のデフォルトの MSDP ピアおよび MSDP ピア）を除き、MSDP ピアは一般的に (M)BGP ピアでもあります。

RPF チェック ルールが SA メッセージに適用される仕組み

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 ピアリングに依存します。

- 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 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 ピアであり、唯一の単一の MSDP ピアまたはデフォルトの MSDP ピアが設定されている状況の場合。
- 送信側の MSDP ピアがメッシュ グループのメンバーである場合。
- 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

RPF チェックに適用するルールをソフトウェアが決定する仕組み

ソフトウェアは、次のロジックを使用して、RPF チェックに適用される 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 ネイバーを見つけます。
  - 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 ルール選択の影響は次のとおりです。デバイスで MSDP ピアの設定に使用される IP アドレスは、同じデバイスで (M)BGP ピアの設定に使用される IP アドレスと一致する必要があります。

MSDP における 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 における 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. 前の検索が成功した（つまり、ベスト パスが見つかった）場合、ピアは、このベスト パスに対する BGP ネイバーのアドレスを判別します。このアドレスは、BGP 更新メッセージでピアにパスを送信した BGP ネイバーのアドレスです。

（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ので、ネクストホップアドレスは通常、シスコにパスを送信した BGP ピアのアドレスと同じではありません。

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 と必ずしも同じとは限りません。

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。

MSDP に対する RPF チェック ルール 1 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。通常、2 つのデバイス間に i(M)BGP ピア接続がある場合は、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 パスによって記述されないため、アドレスは同じである必要があります。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ではネクストホップ アドレスがアップデートされないため、ピアは (M)BGP トポロジ（MSDP トポロジ）の記述にネクスト ホップ アドレスを当てにすることができません。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 i(M)BGP と MSDP の両方のピア アドレスに同じアドレスが使用されるように、MSDP ピア アドレスの設定時は注意を払う必要があります。

MSDP における 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 における 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. 前の検索が成功した（つまり、ベストパスが見つかった）場合、ピアはパスを調べます。RP へのベスト 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。同じでない場合は失敗します。

MSDP に対する RPF チェック ルール 2 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。通常、2 つのデバイス間に e(M)BGP ピア接続がある場合は、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 における 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. 前の検索が成功した（つまり、SA メッセージを発信した RP へのベスト パスが見つかった）場合、ピアは、SA メッセージを送信した MSDP ピアへのベスト パスの BGP MRIB を検索します。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

次の手順は、MSDP ピアが SA メッセージを処理するときに実行されます。

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) エントリが見つかり、その発信インターフェイスのリストがヌルでない場合は、SA メッセージでアドバタイズされる送信元用の PIM-SM ドメインにアクティブな受信者がいます。
2. その後、MSDP ピアは、アドバタイズされた送信元用に (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 メッセージが受信された MSDP ピア。
   - このデバイスと同じ MSDP メッシュ グループにある MSDP ピア（ピアがメッシュ グループのメンバーである場合）。

（注） SA メッセージは、デバイスの 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。下位の IP アドレス ピアは、TCP 接続のオープンにおいてアクティブな役割を果たします。上位の IP アドレス ピアは、もう一方が接続を行うまで 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を 75 秒間受信しなかった場合、TCP 接続がリセットされます。

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 に従って開発された、MSDP MD5 パスワード認証機能は、MSDP ピア間の TCP 接続上で送信された各セグメントを検証するために使用されます。**ip msdp password peer** コマンドは、2 つの MSDP ピア間で 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** コマンドが設定されている場合、デバイスは SA キャッシュに保存された SA メッセージの数をピアごとに維持し、そのピアに設定された SA メッセージの制限に達した場合は、ピアからの新しいメッセージを無視します。

MSDP 対応デバイスをサービス妨害（DoS）攻撃から保護する手段として、**ip msdp sa-limit** コマンドが導入されました。デバイスですべての MSDP ピアリングに対する 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

ip msdp keepalive コマンドは、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ために使用します。

MSDP のピアリング セッションが確立されると、接続の各サイドでキープアライブ 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* 引数は、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。MSDP キープアライブ メッセージがピアに送信され、タイマーが期限切れになったときにリセットされると、キープアライブ タイマーは *keepalive-interval* 引数の値にリセットされます。キープアライブ タイマーは、MSDP ピアリング セッションがクローズすると削除されます。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 ピアリング接続がクローズすると削除されます。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、接続再試行間隔と呼ばれます。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。変更設定された接続再試行間隔は、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。

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推移的な自律システムの場合で、特に自律システムがマルチホームでないときは、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。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のピアを定義することで、BGP でのこの依存関係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。

スイッチが BGP や MBGP をサポートしていない場合は、**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。その代わり、このスイッチのすべての SA メッセージを受け入れることができるデフォルトの MSDP ピアを（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）定義します。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。スイッチで MSDP ピアによる BGP または MBGP ピアリングが行われない場合は、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、スイッチでは常にそのピアからのすべての SA メッセージが受信されます。

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。その代わりに、SA メッセージは 1 つのピアからだけ受け入れられます。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。もちろん、デフォルトのピアが両方とも同じ SAメッセージを送信することがこの基本的な前提となっています。

下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。この図では、デバイス 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（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 はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で BGP も MBGP も実行していません。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、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A だけまたはデバイス C だけから SA メッセージを受け入れます。デバイス A が設定内の最初のデフォルト ピアである場合、デ

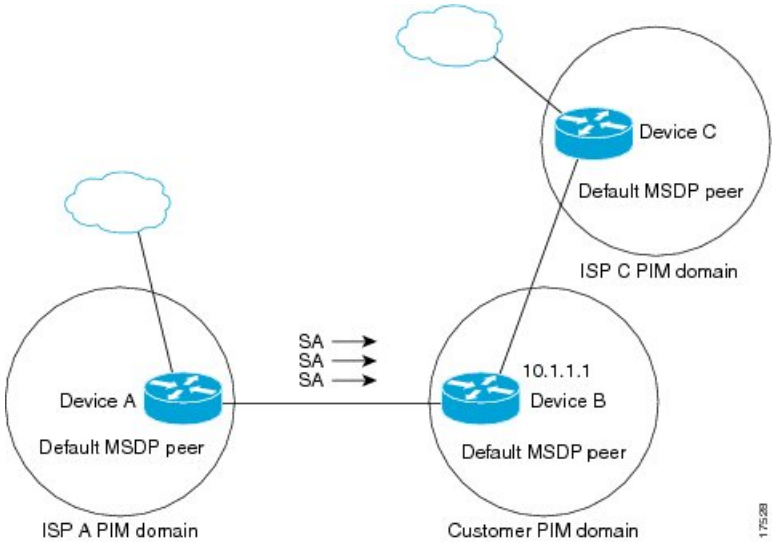
バイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのデバイス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。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *2 :* デフォルト *MSDP* ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。デバイス A が設定内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス 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 リストを使用しない動作です。

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（このピアにデバイスが接続されていて、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。

SA メッセージでアドバタイズされるソースを制御するには、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 メッセージでローカル ソースをアドバタイズしないように RP を設定できます。この場合もデバイスは通常の方法で他の MSDP ピアからの SA メッセージを転送します。ローカル ソースの SA メッセージは発信しません。
- 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（またはそれらのその組み合わせ）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イネーブル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 （27 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、デバイスがピアへ転送する SA メッセージを次のように制御できます。

- 指定した MSDP ピアへ転送したすべての発信 SAメッセージをフィルタリングするには、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します。
- 指定した MSDP ピアへ転送した発信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストで許可されている（S, G）ペアに一致する MSDP ピアへの SA メッセージだけを転送するようにデバイスを設定します。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。
- 指定した MSDP へ転送した発信 SA メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに定義された基準に一致する SA メッセージだけを転送するようにデバイスを設定します。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。
- 指定したピアからの発信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージが1 つ以上の MSDP ピアに送信されていても、それらの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します。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。この場合、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 リストを作成することによって、MSDP ピアからデバイスが受信する送信元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。

- 指定した 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には、指定した 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します。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアに一致する 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します。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。
- 指定したピアからの着信 SA 要求メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに指定された基準に一致する SA メッセージだけを受信するようにデバイスを設定します。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。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアと、ルートマップに定義された基準の両方に基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアと、ルート マップに定義された基準の両方に一致する着信 SA メッセージだけを受信するようにデバイスを設定します。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。
- 指定したピアからの着信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージがすでに1 つ以上の MSDP ピア全体に送信されている可能性がある場合でも、それらの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します。
- 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。この場合、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、したがってリモート 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

1 つ以上の指定した MSDP ピアに SA 要求メッセージを送信するように非キャッシュ デバイスを設定できます。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対象のソフトウェア 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、デバイス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。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するには、SA 要求フィルタを作成します。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。

- 指定した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するには、指定した MSDP ピアからのすべての SA 要求を無視するようにデバイスを設定します。
- 指定したピアからの SA 要求メッセージのサブセットを標準アクセス リストに定義されたグループに基づいてフィルタリングするには、標準アクセス リストに定義されたグループに一致する 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します。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 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。

始める前に

- 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、デフォルトの MSDP ピア、および MSDP メッシュ グループの場合を除き、すべての MSDP ピアは MSDP に設定される前に BGP を実行するように設定する必要があります。

手順

	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 モードを有効にします。 • 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*] 例： `Device(config)# ip msdp peer 192.168.1.2 connect-source loopback0`	MSDP をイネーブルにし、DNS 名または IP アドレスで指定される 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、通常は 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 （25 ページ）またはMSDP メッシュ グループの設定 （26 ページ）を参照してください。 • **connect-source** キーワードを指定した場合、指定されたローカルインターフェイスの *type* と *number* の値で示されるプライマリアドレスは TCP 接続の送信元 IP アドレスとして使用されます。リモートドメイン内のデバイスとのピアを確立している境界上の MSDP ピアの場合は特に、**connect-source** キーワードを推奨します。
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。

	コマンドまたはアクション	目的
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、そのすべての設定が終了するまではどのピアもアクティブにしない場合は、それぞれのピアをシャットダウンし、ピアごとに設定して、後からそれぞれのピアを起動することができます。その MSDP ピアの設定を失うことなく、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 ピアをシャットダウンすると、TCP 接続が終了します。**no ip msdp shutdown** コマンドを（指定したピアに対して）使用し、ピアを起動するまではこの接続は再開されません。

始める前に

MSDP が動作していて、MSDP ピアを設定する必要があります。

手順

	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 モードを有効にします。 • 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。	--

	コマンドまたはアクション	目的
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

	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 モードを有効にします。 • 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 接続の 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 ピアの間で MD5 認証に使用されるパスワードやキーを設定または変更した場合、パスワードの設定後にローカル デバイスの既存のセッションは切断されません。新しいパスワードまたは変更されたパスワードをアクティブにするには、手動でセッションを切断する必要があります。

	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。
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 ピア用のパスワードが設定されているが、MSDP ピアには設定されていない場合、デバイスがそれらの間でMSDP 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または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 パスワードが有効かどうか、およびキープアライブメッセージが MSDP ピアで受信されるかどうかを確認します。

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

デバイスが指定された 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、このオプションの（しかし強く推奨されます）タスクを実行します。この作業を実行することで、MSDP 対応デバイスを分散型サービス妨害（DoS）攻撃から保護します。

（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

	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 モードを有効にします。 • 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。
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：	（任意）MSDP ピアのステータスを表示します。

	コマンドまたはアクション	目的
	`Device# show ip msdp summary`	（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 セッションのダウンを検出するまでに 75 秒かかる場合があります。冗長 MSDP ピアが設定されたネットワーク環境では、保持時間間隔を短縮すると、MSDP ピアの障害発生時に MSDP ピアの再コンバージェンス時間を短縮できます。

（注） コマンドのデフォルトは RFC 3618、*Multicast Source Discovery Protocol* に従うため、**ip msdp keepalive** コマンドのデフォルトを変更しないことを推奨します。デフォルトの変更が必要なネットワーク環境の場合は、MSDP ピアリングセッションの終了時の *keepalive-interval* と *hold-time-interval*の両方の引数に同じ時刻値を設定する必要があります。

手順

	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 モードを有効にします。 • 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。

	コマンドまたはアクション	目的
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 MSDP ピアが待機する間隔を調整するには、次のオプション タスクを実行します。取引フロアのネットワーク環境など、SA メッセージの高速リカバリが必要なネットワーク環境では、接続再試行間隔をデフォルト値の 30 秒未満の時間値に減らすことができます。

手順

	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 モードを有効にします。 • 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。

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。

始める前に

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

	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 モードを有効にします。 • 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

	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 モードを有効にします。 • 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 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 グループに参加しているデバイス上のすべての MSDP ピアは、そのグループ内の他のすべての MSDP ピアと完全にメッシュ構造になっ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す、また、**ip msdp mesh-group** コマンドを使用して、その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

	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 モードを有効にします。 • 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送信元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。
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

	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 モードを有効にします。 • 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 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

	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 モードを有効にします。 • 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

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

手順

	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 モードを有効にします。 • 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 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 ピアへの送信元情報の要求

デバイスが MSDP ピアから送信元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） シスコの以前のソフトウェア リリースでは 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、明示的にイネーブルまたはディセーブルにすることはできないため、この作業はほとんど必要ありません。

手順

	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 モードを有効にします。 • 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-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

	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 モードを有効にします。 • 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。

	コマンドまたはアクション	目的
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。

RP アドレス以外の発信元アドレスの設定

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により、発信元 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 アドレスが発信元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。

始める前に

MSDP がイネーブルになり、MSDP ピアが設定されます。MSDP ピアの設定の詳細については、MSDP ピアの設定 （18 ページ）を参照してください。

手順

	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 モードを有効にします。 • 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 originator-id** *type number* 例： `Device(config)# ip msdp originator-id ethernet 1`	発信元デバイス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。
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

ステップ 1 **enable**

例：

```
Device# enable
```

特権 EXEC モードを有効にします。

- 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* 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。**ip msdp cache-sa-state** コマンドは、このコマンドによって出力が生成されるように設定する必要があります。

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、統計情報または 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

	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 モードを有効にします。 • 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が消去されます。 • 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。

始める前に

- SNMP および MSDP は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。
- MSDP 確立の通知は、シスコの MSDP MIB の実装ではサポートされていません。

手順

	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 モードを有効にします。 • 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、トラップと通知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

ここでは、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設定例を紹介します。

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
!
```

例：デフォルト MSDP ピアの設定

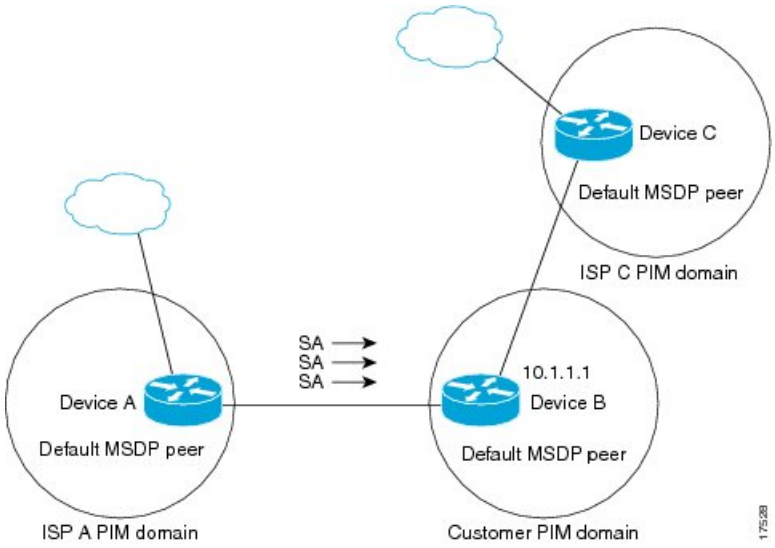
下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。この図では、デバイス B を所有するカスタマーが 2 つの ISP を介してインターネットに接続されています。一方の ISP はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で (M)BGP を実行していません。カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A 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

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *3*：デフォルト *MSDP* ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。デバイス A が設定ファイル内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス 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 リストを使用しない動作です。

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（このピアにデバイスが接続されていて、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、図に示されているデバイス A およびデバイス 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、図に示すカスタマーのような、デフォルト ピアリングを使用している複数のカスタマーがいる可能性があります。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。

デバイス 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
```

デバイス 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
```

マルチキャスト送信元検出プロトコルに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)* の「IP マルチキャスト ルーティング コマンド」の項を参照してください。

Multicast Source Discovery Protocol の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	Multicast Source Discovery Protocol	MSDP は複数の PIM-SM ドメインを接続するメカニズムです。MSDP は、他の PIM ドメイン内のマルチキャスト送信元を検出することを目的としています。MSDP の主な利点は、（一般的な共有ツリーではなく）ドメイン間ソース ツリーを PIM-SM ドメインで使用できるようにし、複数の PIM-SM ドメインを相互接続する複雑性を軽減することです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。