CHAPTER 24

SPAN および RSPAN の設定

この章では、Catalyst 3550 スイッチにスイッチド ポート アナライザ（SPAN）およびリモート SPAN（RSPAN）を設定する方法について説明します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

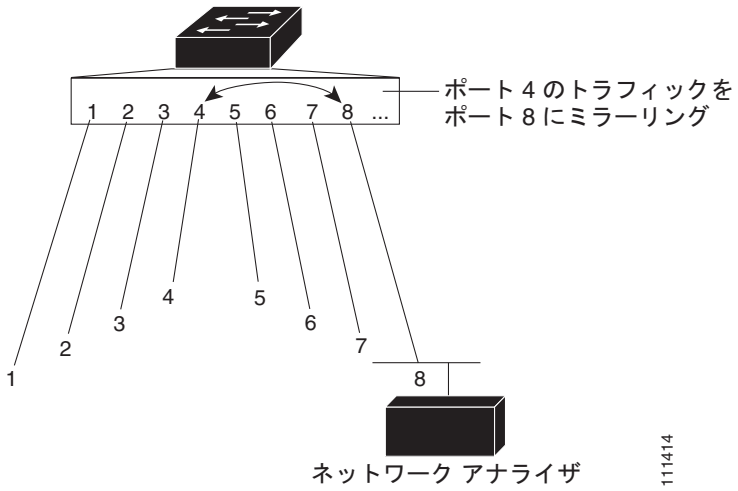
この章の内容は、次のとおりです。

SPAN および RSPAN の概要

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN を使用して、SwitchProbe デバイスまたは他のリモート モニタリング（RMON）プローブまたはセキュリティ デバイスに接続されているスイッチ上の別のポートにトラフィックのコピーを送信します。SPAN は、分析のために、送信元ポートで受信または送信したトラフィック（あるいは両方）や 1 つ以上の送信元ポートまたは送信元 VLAN で受信したトラフィックを宛先ポートにミラーリングします。

たとえば、図 24-1 の場合、ポート 4（送信元ポート）上のすべてのトラフィックがポート 8（宛先ポート）にミラーリングされます。ポート 8 のネットワーク アナライザは、ポート 4 に物理的には接続されていませんが、ポート 4 からのすべてのネットワーク トラフィックを受信します。

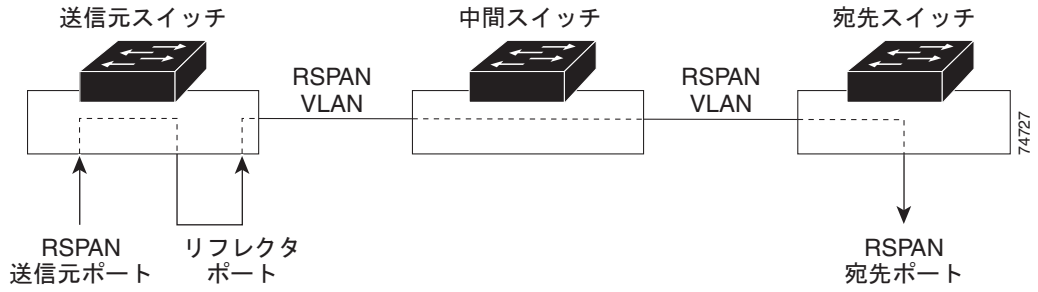
図 24-1　　SPAN の設定例



SPAN を使用してモニタできるのは、送信元ポートに入るトラフィックまたは送信元 VLANs に出入りするトラフィックだけです。受信送信元ポートまたは送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされるトラフィックはモニタされません。ただし、送信元 VLAN で受信され、別の VLAN にルーティングされるトラフィックはモニタされます。

RSPAN は、ネットワーク内の複数のスイッチのリモート モニタリングをイネーブルにすることによって、SPAN を拡張します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元からの SPAN トラフィックは、リフレクタ ポートを介して RSPAN VLAN にコピーされたあと、トランク ポートを介して転送されます。トランク ポートは、RSPAN VLAN をモニタする RSPAN 宛先セッションに RSPAN VLAN を伝送します（図 24-2 を参照）。

図 24-2　　RSPAN の設定例



SPAN と RSPAN は、送信元ポートまたは送信元 VLAN 上でのネットワーク トラフィックのスイッチングに影響しません。送信元インターフェイスによって送受信されたパケットのコピーは、宛先インターフェイスに送信されます。

ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム（IDS）センサー装置を宛先ポートに接続すれば、IDS デバイスは TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを閉じることができます。

SPAN と RSPAN の概念および用語

ここでは、SPAN および RSPAN の設定に関連する概念および用語について説明します。

SPAN セッション

ローカル SPAN セッションは、宛先ポートと送信元ポートおよび送信元 VLAN を結び付けたものです。RSPAN セッションは、ネットワーク全体の送信元ポートおよび送信元 VLAN の RSPAN VLAN との関連付けです。宛先の送信元は RSPAN VLAN です。

モニタ対象のネットワーク トラフィックの送信元を指定するパラメータを使用して、SPAN セッションを設定します。SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- 一連のポート、または一定範囲のポートおよび VLAN で着信トラフィックをモニタできます。
- 単一ポートのトラフィックをモニタできます。複数のポートの発信トラフィックはモニタできません。
- VLAN の発信トラフィックはモニタできません。

別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。

SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、SPAN の宛先がオーバーサブスクライブ型の場合は（たとえば 100 Mbps ポートをモニタする 10 Mbps ポートなど）、パケットがドロップされるか、または消失する可能性があります。

ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。**show monitor session** *session_number* 特権 EXEC コマンド では、SPAN セッションの動作上のステータスが表示されます。

SPAN セッションは、システムの起動後に、宛先ポートが動作可能になるまでアクティブになりません。

トラフィック タイプ

SPAN セッションには、次のトラフィック タイプがあります。

- RX（受信）SPAN：受信（または入力）SPAN の役割は、スイッチが変更または処理を行う前に、VLAN または送信元インターフェイスが受信したすべてのパケットを、できるだけ多くモニタすることです。送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。1 つの SPAN セッションで、一連のまたは一定範囲の入力ポートまたは VLAN をモニタできます。

  タグ付きパケット（ISL（スイッチ間リンク）または IEEE 802.1Q）では、タギングは入力ポートで削除されます。宛先ポートでは、タギングがイネーブルの場合、パケットは ISL または 802.1Q ヘッダー付きで表示されます。タギングが指定されていない場合、パケットはネイティブ形式で表示されます。

  ルーティングが原因で変更されたパケットは、Rx SPAN 用に変更されることなくコピーされます。つまり、元のパケットがコピーされます。Quality of Service（QoS）が原因で変更されたパケット（たとえば、変更済み DiffServ コード ポイント（DSCP））は、Rx SPAN 用に変更されてコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、SPAN では無効です。実際の着信パケットがドロップされた場合でも、宛先ポートはパケットのコピーを受信します。これらの機能には、標準および拡張 IP 入力アクセス コントロール リスト（ACL）、ユニキャストおよび入力側 QoS ポリシング用の標準および拡張 IP 出力 ACL、VLAN マップ、入力側 QoS ポリシング、ポリシーベース ルーティング（PBR）などがあります。パケットのドロップを引き起こすスイッチ輻輳も、SPAN には影響しません。

- TX（送信）SPAN：送信（または出力）SPAN の役割は、スイッチによる変更および処理がすべて完了した後で、送信元インターフェイスが送信したすべてのパケットをできるだけ多くモニタすることです。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に提供されます。

  SPAN セッションあたり 1 つの出力送信元ポートのみが許可されます。VLAN のモニタは、出力方向ではサポートされません。

  ルーティングにより変更されたパケット（存続可能時間（TTL）または MAC アドレスによる変更など）は、宛先ポートでも変更されます。QoS が原因で変更されたパケットには、SPAN 送信元とは異なる DSCP（IP パケット）または CoS（IP 以外のパケット）が設定されることがあります。

  送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の重複されたコピーにも影響を与えることがあります。このような機能には、VLAN マップ、マルチキャスト パケットに対応する標準および拡張 IP 出力 ACL、出力側 QoS ポリシングがあります。出力 ACL の場合は、SPAN 送信元がパケットをドロップすると、SPAN の宛先もパケットをドロップします。出力側 QoS ポリシングの場合は、SPAN 送信元がパケットをドロップしても、SPAN 宛先はパケットをドロップするとは限りません。送信元ポートがオーバーサブスクライブ型である場合、宛先ポートは別のドロップ動作を行います。

- 両方：SPAN セッションで、受信パケットと送信パケットの両方について、1 つのポートをモニタすることもできます。

送信元ポート

送信元ポート（別名*監視対象ポート*）は、ネットワーク トラフィック分析のために監視するスイッチド ポートまたはルーテッド ポートです。単一のローカル SPAN セッションまたは RSPAN 送信元セッションでは、受信（Rx）、送信（Tx）、または双方向（both）などの送信元ポート トラフィックをモニタできます。ただし、VLAN では、受信トラフィックのみをモニタできます。スイッチは、任意の数の送信元ポート（スイッチで利用可能なポートの最大数まで）と任意の数の送信元着信 VLAN（サポートされている VLAN の最大数まで）をサポートしています。

送信元ポートの特性は、次のとおりです。

- すべてのポート タイプ（EtherChannel、ファスト イーサネット、ギガビット イーサネットなど）が可能です。
- 複数の SPAN セッションでモニタできます。
- 宛先ポートにすることはできません。
- モニタする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。EtherChannel の送信元に設定する場合、モニタする方向はグループ内のすべての物理ポートに適用されます。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- VLAN の SPAN 送信元では、ソース VLAN のすべてのアクティブ ポートが送信元ポートとして含まれます。

トランク ポートを、送信元ポートとして設定できます。デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。選択された VLAN のスイッチド ト

ラフィックだけが宛先ポートに送信されます。この機能は、宛先 SPAN ポートに転送されたトラフィックだけに影響し、通常のトラフィックのスイッチングには影響を与えません。この機能は、VLAN 送信元によるセッションでは許可されません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、発信元ポートと VLAN からのトラフィックのコピーを受け取る宛先ポート（*モニタリング ポート*とも呼ばれる）が必要です。

宛先ポートには、次の特性があります。

- 送信元ポートと同じスイッチ上にある必要があります（ローカル SPAN セッションの場合）。
- 任意のイーサネット物理ポートにできます。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- 送信元ポートまたはリフレクタ ポートにすることはできません。
- EtherChannel グループまたは VLAN にすることはできません。
- EtherChannel グループが SPAN の送信元として指定された場合でも、EtherChannel グループに割り当てられる物理ポートにすることができます。ポートは、SPAN 宛先ポートとして設定されている間は、グループから削除されます。
- ポートは SPAN セッションに必要なトラフィック以外は送信しません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- SPAN セッションがアクティブなときは、スパニングツリーに参加しません。
- 宛先ポートである場合、レイヤ 2 プロトロル（Cisco Discovery Protocol（CDP）、VLAN トランク プロトコル（VTP）、ダイナミック トランキング プロトコル（DTP）、スパニングツリー プロトコル（STP）、ポート集約プロトコル（PAgP）、および Link Aggregation Control Protocol（LACP））のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- 宛先ポートでアドレス学習が行われません。

リフレクタ ポート

リフレクタ ポートは、RSPAN VLAN 上のパケットをコピーするメカニズムです。リフレクタ ポートは、参加している SPAN 送信元セッションからのトラフィックのみを転送します。リフレクタ ポートとして設定されたポートに接続されているすべてのデバイスでは、RSPAN 送信元セッションがディセーブルになるまで、接続が失われたままです。

リフレクタ ポートには、次の特性があります。

- ループバックに設定されたポートです。
- EtherChannel グループに属している可能性はなく、トランクではなく、プロトコル フィルタリングを実行できません。
- EtherChannel グループが SPAN の送信元として指定されている場合でも、EtherChannel グループに割り当てられる物理ポートにすることができます。ポートは、リフレクタ ポートとして設定されている間は、グループから削除されます。

- リフレクタ ポートとして使用されるポートは、SPAN の送信元または宛先にすることができず、一度に複数のセッションのリフレクタ ポートにすることもできません。
- すべての VLAN から認識されません。
- リフレクタ ポート上のループバックされたトラフィックのネイティブ VLAN は RSPAN VLAN です。
- リフレクタ ポートはタグなしトラフィックをスイッチにループ バックします。その後、トラフィックは RSPAN VLAN に送られ、RSPAN VLAN を伝送するすべてのトランク ポートにフラッディングされます。
- リフレクタ ポートではスパニングツリーが自動的にディセーブルになります。

リフレクタ ポートの帯域幅が対応する送信元ポートおよび VLAN からのトラフィック ボリュームに対して不十分である場合、過剰なパケットがドロップされます。10/100 ポートは 100 Mbps で動作します。ギガビット ポートは 1 Gbps で動作します。

VSPAN

VLAN ベースの SPAN（VSPAN）では、1 つまたは複数の VLAN のネットワーク トラフィックをモニタできます。VSPAN は、受信（Rx）トラフィックのみをモニタするように設定できます。これは、その VLAN のすべてのポートに適用されます。

VSPAN セッションでは、次の注意事項に従ってください。

- モニタ対象の VLAN 上のトラフィックだけが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN プルーニングと VLAN 許可リストは、SPAN モニタでは無効です。
- VSPAN がモニタリングするのはスイッチに入るトラフィックに限られ、VLAN 間でルーティングされるトラフィックはモニタリングしません。たとえば、VLAN が受信でモニタされ、マルチレイヤ スイッチが別の VLAN からのトラフィックをモニタ対象の VLAN にルーティングする場合、そのトラフィックはモニタ対象にはならず、SPAN 宛先ポート上で受信されません。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

SPAN トラフィック

ローカル SPAN を使用して、マルチキャスト パケットおよびブリッジ プロトコル データ ユニット（BPDU）パケット、CDP パケット、VTP パケット、DTP パケット、STP パケット、PagP パケット、および LACP パケットのすべてのネットワーク トラフィックをモニタできます。RSPAN を使用してレイヤ 2 プロトコルをモニタすることはできません。詳細については、「RSPAN 設定時の注意事項」（P.24-16）を参照してください。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。たとえば、送信元 a1 受信モニタおよび a2 受信/送信モニタから宛先ポート d1 まで、双方向（受信と送信の両方）SPAN セッションが設定されているとします。パケットが a1 からスイッチに入り、a2 へスイッチングされると、着信パケットおよび発信パケットの両方が宛先ポート d1 に送信されます。このため、両方のパケットは同じものになります（レイヤ 3 書き換えが行われた場合には、付加されたレイヤ 3 情報のため異なるパケットになります）。

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：入力 SPAN はルーテッド トラフィックを監視しません。VSPAN がモニタリングするのはスイッチに入るトラフィックに限られ、VLAN 間でルーティングされるトラフィックはモニタリングしません。たとえば、VLAN が受信でモニタされ、マルチレイヤ スイッチが別の VLAN からのトラフィックをモニタ対象の VLAN にルーティングする場合、そのトラフィックはモニタ対象にはならず、SPAN 宛先ポート上で受信されません。
- スパニングツリー プロトコル（STP）：宛先ポートまたはリフレクタ ポートの SPAN または RSPAN セッションがアクティブな間、宛先ポートまたはリフレクタ ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートまたはリフレクタ ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- Cisco Discovery Protocol（CDP）：SPAN 宛先ポートは、SPAN セッションがアクティブな間は CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VLAN トランキング プロトコル（VTP）：VTP を使用して、スイッチ間で RSPAN VLAN をプルーニングできます。
- VLAN およびトランキング：送信元ポート、宛先ポート、またはリフレクタ ポートの VLAN メンバーシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポート、またはリフレクタ ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、SPAN または RSPAN セッションをディセーブルにするまで反映されません。送信元ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。
- EtherChannel：EtherChannel グループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

  モニタ対象の EtherChannel グループにポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。ポートが EtherChannel グループ内の唯一のポートである場合、EtherChannel グループが SPAN から削除されます。

  EtherChannel グループに含まれる物理ポートを SPAN 送信元、宛先、またはリフレクタ ポートとして設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループ メンバのままですが、*down* または *standalone* 状態になります。

  EtherChannel グループに含まれる物理ポートが宛先ポートまたはリフレクタ ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポートリストから削除されます。
- QoS：入力のモニタリングの場合、入力 QoS 分類およびポリシングの後でパケットが転送されるため、SPAN 宛先ポートに送信されるパケットが SPAN 送信元ポートで実際に受信されるパケットとは異なる可能性があります。パケット DSCP が、受信パケットと同じではない可能性があります。

  出力のモニタでは、SPAN 送信元ポートの出力 QoS ポリシングがパケット分類を変更する可能性があるため、SPAN 宛先ポートに送信されたパケットは、SPAN 送信元ポートから送信されるパケットと同じではない可能性があります)。QoS ポリシングは、SPAN 宛先ポートで適用されません。

- マルチキャスト トラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集のパケットが 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト パケットの送信回数は反映されません。
- ポート セキュリティ：セキュア ポートを SPAN 宛先ポートにすることはできません。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。
- 802.1x：SPAN 宛先ポートまたはリフレクタ ポート上で 802.1x をイネーブルにできますが、SPAN 宛先またはリフレクタ ポートとしてこのポートを削除するまで、802.1x はディセーブルに設定されます。SPAN 送信元ポートでは 802.1x を有効にすることができます。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートで 802.1x をイネーブルにしないでください。

SPAN と RSPAN のセッション限度

スイッチ上で 1 つのローカル SPAN セッションまたは複数の RSPAN セッションを設定（および、NVRAM に保存）できます。スイッチごとに最大 2 つの SPAN または RSPAN セッションを設定（および NVRAM に保存）できます。SPAN、RSPAN 送信元、および RSPAN 宛先セッション間で 2 つのセッションを分離できます。セッションごとに、複数の送信元ポートまたは送信元 VLAN を設定できます。

SPAN および RSPAN のデフォルト設定

表 24-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 24-1　SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN ステート	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方（**both**）。追加の送信元ポートまたは VLAN では、受信（**rx**）トラフィックだけをモニタできます。
カプセル化タイプ（宛先ポート）	ネイティブ形式（カプセル化タイプ ヘッダーなし）
入力転送（宛先ポート）	ディセーブル

SPAN の設定

ここでは、スイッチに SPAN を設定する方法について説明します。内容は次のとおりです。

- 「フィルタリングする VLAN の指定」（P.24-15）

SPAN 設定時の注意事項

SPAN を設定するときには、次の注意事項に従ってください。

- SPAN セッションは、「SPAN と RSPAN のセッション限度」（P.24-8）に記載された限度内であれば、RSPAN セッションと共存できます。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- SPAN セッションごとに 1 つの宛先ポートのみを指定できます。同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- EtherChannel ポートを SPAN 送信元ポートにできますが、SPAN 宛先ポートにはできません。
- 802.1x ポートは SPAN 送信元ポートにすることができます。SPAN 宛先ポートまたはリフレクタ ポート上で 802.1x をイネーブルにできますが、SPAN 宛先またはリフレクタ ポートとしてこのポートを削除するまで、802.1x はディセーブルに設定されます。
- SPAN 送信元ポートの場合、単一ポートの送信トラフィックか、一連またはある範囲のポートまたは VLAN の受信トラフィックをモニタできます。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するトラフィックがモニタされるだけです。
- トランク ポートは、送信元ポートまたは宛先ポートです。SPAN 宛先ポートを経由する発信パケットは、設定されたカプセル化ヘッダーを伝送します（スイッチ間リンク（ISL）または IEEE 802.1Q）。カプセル化タイプが定義されていない場合、パケットはネイティブ形式で送信されます。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- 受信トラフィックの場合、1 つの SPAN セッションに、複数の送信元ポートおよび送信元 VLAN が混在できます。送信元 VLAN とフィルタ VLAN を SPAN セッションで混在させることはできません。送信元 VLAN、またはフィルタ VLAN を使用できますが、両方を同時に使用することはできません。
- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。
- SPAN 宛先ポートが VLAN スパニングツリーに参加することはありません。SPAN にはモニタ対象トラフィック内の BPDU が含まれるため、SPAN セッションのために SPAN 宛先ポートで受信されたスパニングツリー BPDU が SPAN 送信元ポートからコピーされます。
- SPAN がイネーブルの場合、設定の変更の結果は次のようになります。
  - 宛先ポートの VLAN 設定を変更する場合、SPAN がディセーブルになるまで変更が反映されません。
  - すべての送信元ポートまたは宛先ポートをディセーブルにする場合、送信元ポートと宛先ポートの両方がイネーブルになるまで、SPAN 機能は停止します。
  - 送信元が VLAN である場合、モニタ対象の VLAN との間でポートを移動すると、モニタ対象のポート数が変化します。

SPAN セッションの作成とモニタ対象ポートの指定

SPAN セッションを作成し、送信元（モニタ対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number* には、1 または 2 を指定します。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 （任意）[**,** | **-**]：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。追加の送信元ポートは、受信（rx）トラフィックだけをモニタリングします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。
ステップ 4	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q** | **isl**}]	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、宛先ポートを指定します。有効なインターフェイスは物理インターフェイスなどです。 （任意）発信パケットのカプセル化ヘッダーを指定します。指定しなかった場合は、パケットがネイティブ形式で送信されます。 • **isl**：ISL カプセル化を使用します。 • **dot1q**：IEEE 802.1Q カプセル化を使用します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、SPAN セッション 1 を設定し、送信元ポートから宛先ポートへのトラフィックをモニタする例を示します。まず、セッション 1 の既存の SPAN 設定を削除し、次に双方向トラフィックを送信元ポート 1 から宛先ポート 8 にミラーリングします。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet0/1
Switch(config)# monitor session 1 destination interface fastethernet0/8
encapsulation dot1q
Switch(config)# end
```

SPAN セッションの作成と入力トラフィックのイネーブル化

SPAN セッションを作成し、送信元ポートおよび宛先ポートを指定し、ネットワーク セキュリティ デバイス（Cisco IDS センサー装置など）用の宛先ポート上の入力トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number* には、1 または 2 を指定します。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 （任意）**[,** | **-]**：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。追加の送信元ポートは、受信（rx）トラフィックだけをモニタリングします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q** [**ingress vlan** *vlan id*] | **isl** [**ingress**]} | **ingress vlan** *vlan id*]	SPAN セッション、宛先ポート（モニタリング ポート）、パケット カプセル化、および入力 VLAN を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、宛先ポートを指定します。有効なインターフェイスは物理インターフェイスなどです。 （任意）SPAN 宛先ポート上で送信されるパケットのカプセル化を指定します。カプセル化タイプが指定されていない場合、すべての送信パケットはネイティブ形式（タグなし）で送信されます。 • タグなしのネイティブ VLAN パケットと、他のすべての **dot1q** タグ付き VLAN **tx** パケットを送信する場合は、**encapsulation dot1q** と入力します。 • ISL を使用してカプセル化されたすべての **tx** パケットを送信する場合は、**encapsulation isl** を入力します。 • （任意）ISL カプセル化を使用する場合、SPAN 宛先ポートの入力トラフィックの転送をイネーブルにするには、**ingress** を指定します。 （任意）ネイティブ（タグなし）および **dot1q** カプセル化の場合、*ingress vlan vlan id* を指定し、*vlan id* をネイティブ VLAN として入力転送をイネーブルにします。また、vlan id は、送信パケット用のネイティブ VLAN としても使用されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、IEEE 802.1Q カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 ingress vlan 5
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation
dot1q ingress vlan 5
```

次の例では、宛先ポートで入力トラフィック転送をディセーブルにする方法を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation
dot1q
```

SPAN セッションからのポートの削除

セッションの SPAN 送信元としてのポートを削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** *session_number* **source interface** *interface-id* **[,** | **-] [both** | **rx** | **tx]**	削除する送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 *session* には、1 または 2 を指定します。 *interface-id* には、モニタを中止する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 （任意）一連のインターフェイスまたはインターフェイス範囲を指定するには、**[,** | **-]** を使用します（設定されていない場合）。このオプションは、受信トラフィックのみをモニタする場合に有効です。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタ対象から外すトラフィックの方向（**both**、**rx**、または **tx**）を指定します。トラフィックの方向を指定しなかった場合、送信と受信の両方がディセーブルになります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SPAN セッションから送信元ポートまたは宛先ポートを削除する場合は、**no monitor session** *session_number* **source interface** *interface-id* グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。カプセル化タイプをデフォルト（ネイティブ）に戻すには、**encapsulation** キーワードなしで **monitor session** *session_number* **destination interface** *interface-id* を使用します。

次に、SPAN セッション 1 の SPAN 送信元としてのポートを削除する例を示します。

```
Switch(config)# no monitor session 1 source interface fastethernet0/1
Switch(config)# end
```

次に、双方向モニタリングが設定されていたポートで、受信トラフィックのモニタリングをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface fastethernet0/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

モニタリングする VLAN の指定

VLAN のモニタは、ポートのモニタリングと類似しています。特権 EXEC モードから、次の手順に従ってモニタする VLAN を指定します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number* には、1 または 2 を指定します。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	**monitor session** *session_number* **source vlan** *vlan-id* [**,** | **-**] **rx**	SPAN セッションおよび送信元 VLAN（モニタ対象ポート）を指定します。モニタリングできるのは、VLAN 上の受信（**rx**）トラフィックだけです *session_number* には、1 または 2 を指定します。 *vlan-id* の範囲は 1 ～ 4094 です。先行 0 は入力しないでください。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 4	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q** | **isl**}]	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、宛先ポートを指定します。有効なインターフェイスは物理インターフェイスなどです。 （任意）発信パケットのカプセル化ヘッダーを指定します。指定しなかった場合は、パケットがネイティブ形式で送信されます。 • **isl**：ISL カプセル化を使用します。 • **dot1q**：802.1Q カプセル化を使用します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SPAN セッションから 1 つ以上の送信元 VLAN または宛先ポートを削除する場合は、**no monitor session** *session_number* **source vlan** *vlan-id* **rx** グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination** interface *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定をすべてクリアし、VLAN 1 ～ 3 に所属するすべてのポート上で受信トラフィックをモニタリングする SPAN セッション 2 を設定し、宛先ポート 7 に送信する例を示します。この設定は次に、VLAN 10 に所属するすべてのポートで受信トラフィックをモニタリングするように変更されています。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/7
Switch(config)# monitor session 2 source vlan 10 rx
Switch(config)# end
```

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number* には、1 または 2 を指定します。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id* **rx**	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* には、1 または 2 を指定します。 *vlan-id* の範囲は 1 ～ 4094 です。先行 0 は入力しないでください。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination interface** *interface-id*	宛先ポート（モニタリング ポート）と SPAN セッションの特性を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、宛先ポートを指定します。有効なインターフェイスは物理インターフェイスなどです。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter** グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定をすべてクリアし、トランク ポート 4 上での受信したトラフィックをモニタリングする SPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 のトラフィックだけを、宛先ポート 8 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/4 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet0/8
Switch(config)# end
```

RSPAN の設定

ここでは、スイッチに RSPAN を設定する手順について説明します。内容は次のとおりです。

RSPAN 設定時の注意事項

RSPAN を設定するときには、次の注意事項に従ってください。

- 「SPAN 設定時の注意事項」（P.24-9）のすべての項目は RSPAN にも当てはまります。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力アクセス コントロール リスト（ACL）を適用して、特定のパケットを選択的にフィルタリングまたはモニタリングできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN セッションは、「SPAN と RSPAN のセッション限度」（P.24-8）に記載された限度内であれば、SPAN セッションと共存できます。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- ポートがリフレクタポートに指定されている間は、RSPAN 送信元ポートまたは RSPAN 宛先ポートとして指定できません。
- スイッチ ポートをリフレクタ ポートとして設定すると、通常のスイッチ ポートではなくなります。リフレクタ ポートを通過するトラフィックがループバックされるだけです。
- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。RSPAN VLAN 上のアクセス ポートは自動的にディセーブルになります。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
  - RSPAN VLAN ではアクセス ポートが設定されません。
  - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。

– 参加するすべてのスイッチで RSPAN がサポートされている。

（注）　RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークン リングおよび FDDI VLAN 専用）にすることはできません。

- RSPAN VLAN を作成してから、RSPAN 送信元または宛先セッションを設定します。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 未満の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラッディングが防止されます。
- RSPAN トラフィックは RSPAN VLAN のネットワーク上で伝送されるため、ミラーリングされたパケットの元の VLAN アソシエーションは失われます。したがって、RSPAN では、IDS デバイスからユーザが指定した単一 VLAN へのトラフィック転送だけをサポートしています。

RSPAN VLAN としての VLAN の設定

最初に、RSPAN セッションの RSPAN VLAN となる VLAN を新規に作成します。RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できます。拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のスイッチ、および中間スイッチに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

RSPAN VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**vlan** *vlan-id*	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ～ 1001 および 1006 ～ 4094 です。 （注）　RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN 専用）にすることはできません。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

次に、RSPAN VLAN 901 を作成する例を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の RSPAN 設定を削除します。 *session_number* には、1 または 2 を指定します。 すべての RSPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 （任意）[**,** | **-**]：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。追加の送信元ポートは、受信（**rx**）トラフィックだけをモニタリングします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。
ステップ 4	**monitor session** *session_number* **destination remote vlan** *vlan-id* **reflector-port** *interface*	RSPAN セッション、宛先リモート VLAN、およびリフレクタ ポートを指定します。 *session_number* には、1 または 2 を入力します。 *vlan-id* には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。（RSPAN VLAN の作成の詳細については、「イーサネット VLAN の作成または変更」（P.11-9）を参照してください）。 *interface* には、RSPAN トラフィックを RSPAN VLAN にフラッディングするインターフェイスを指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、セッション 1 の既存の RSPAN 設定をクリアし、複数の送信元インターフェイスをモニタする RSPAN セッション 1 を設定し、宛先 RSPAN VLAN およびリフレクタ ポートを設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet0/10 tx
Switch(config)# monitor session 1 source interface fastethernet0/2 rx
Switch(config)# monitor session 1 source interface fastethernet0/3 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
Switch(config)# monitor session 1 destination remote vlan 901 reflector-port
fastethernet0/1
Switch(config)# end
```

RSPAN 宛先セッションの作成

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 *session_number* には、1 または 2 を指定します。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 3	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q** | **isl**}]	RSPAN セッションおよび宛先インターフェイスを指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、宛先インターフェイスを指定します。 （任意）発信パケットのカプセル化ヘッダーを指定します。指定しなかった場合は、パケットがネイティブ形式で送信されます。 • **isl**：ISL カプセル化を使用します。 • **dot1q**：IEEE 802.1Q カプセル化を使用します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、VLAN 901 を送信元リモート VLAN に、ポート 5 を宛先インターフェイスに設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface fastethernet0/5
Switch(config)# end
```

RSPAN 宛先セッションの作成および入力トラフィックのイネーブル化

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN を指定し、ネットワーク セキュリティ デバイス（Cisco IDS センサー装置など）用の宛先ポート上の入力トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**monitor session** *session_number* **source remote vlan** *vlan-id*	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 *session_number* には、1 または 2 を指定します。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 3	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q** [**ingress vlan** *vlan id*] | **ISL** [**ingress**]} | **ingress vlan** *vlan id*]	RSPAN セッション、宛先ポート、パケット カプセル化、および入力側 VLAN を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、宛先ポートを指定します。有効なインターフェイスは物理インターフェイスなどです。 （任意）RSPAN 宛先ポート上で送信されるパケットのカプセル化を指定します。カプセル化タイプが指定されていない場合、すべての送信パケットはネイティブ形式（タグなし）で送信されます。 • タグなしのネイティブ VLAN パケットと、他のすべての **dot1q** タグ付き VLAN **tx** パケットを送信する場合は、**encapsulation dot1q** と入力します。 • ISL を使用してカプセル化されたすべての **tx** パケットを送信する場合は、**encapsulation isl** を入力します。 （任意）SPAN 宛先ポート上で入力トラフィックの転送をイネーブルにするか否かを指定します。 • ネイティブ（タグなし）および **dot1q** カプセル化の場合、*ingress vlan vlan id* を指定し、*vlan id* をネイティブ VLAN として入力転送をイネーブルにします。また、vlan id は、送信パケット用のネイティブ VLAN としても使用されます。 • ISL カプセル化を使用する場合、**ingress** を指定して入力転送をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、送信元リモート VLAN として VLAN 901 を設定し、802.1Q カプセル化をサポートするセキュリティ デバイスを使用して VLAN 5 上の入力トラフィック用の宛先ポートを設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface fastEthernet0/5 ingress vlan 5
Switch(config)# end
```

RSPAN セッションからのポートの削除

セッションの RSPAN 送信元としてのポートを削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	削除する RSPAN 送信元ポート（モニタ対象ポート）の特性を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、モニタを中止する送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 （任意）一連のインターフェイスまたはインターフェイス範囲を指定するには、**[,** | **-]** を使用します（設定されていない場合）。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 （任意）モニタ対象から外すトラフィックの方向（**both**、**rx**、または **tx**）を指定します。トラフィックの方向を指定しなかった場合、送信と受信の両方がディセーブルになります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、RSPAN セッション 1 の RSPAN 送信元としてのポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1
Switch(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1 rx
```

ポート 1 で受信するトラフィックのモニタリングはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

モニタリングする VLAN の指定

VLAN のモニタは、ポートのモニタリングと類似しています。特権 EXEC モードから、次の手順に従ってモニタする VLAN を指定します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number* には、1 または 2 を指定します。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	**monitor session** *session_number* **source vlan** *vlan-id* [**,** | **-**] **rx**	RSPAN セッションおよび送信元 VLAN（モニタ対象ポート）を指定します。モニタリングできるのは、VLAN 上の受信（**rx**）トラフィックだけです *session_number* には、1 または 2 を指定します。 *vlan-id* の範囲は 1 ～ 4094 です。先行 0 は入力しないでください。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 4	**monitor session** *session_number* **destination remote vlan** *vlan-id* **reflector port** *interface*	RSPAN セッション、宛先リモート VLAN、およびリフレクタ ポートを指定します。 *session_number* には、1 または 2 を入力します。 *vlan-id* には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。 *interface* には、RSPAN トラフィックを RSPAN VLAN にフラッディングするインターフェイスを指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN セッションから 1 つまたは複数の送信元 VLAN を削除するには、**no monitor session** *session_number* **source vlan** *vlan-id* **rx** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定をすべてクリアし、VLAN 1 ～ 3 に所属するすべてのポート上で受信トラフィックをモニタリングする RSPAN セッション 2 を設定し、リフレクタ ポート 7 を使用して宛先リモート VLAN 902 に送信する例を示します。この設定は次に、VLAN 10 に所属するすべてのポートで受信トラフィックをモニタリングするように変更されています。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination remote vlan 902 reflector-port
gigabitethernet0/7
Switch(config)# monitor session 2 source vlan 10 rx
Switch(config)# end
```

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number* には、1 または 2 を指定します。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id* **rx**	送信元ポート（モニタ対象ポート）と RSPAN セッションの特性を指定します。 *session_number* には、1 または 2 を指定します。 *interface-id* には、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	RSPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* には、1 または 2 を指定します。 *vlan-id* の範囲は 1 ～ 4094 です。先行 0 は入力しないでください。 （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* **reflector port** *interface*	RSPAN セッション、宛先リモート VLAN、およびリフレクタ ポートを指定します。 *session_number* には、1 または 2 を入力します。 *vlan-id* には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。 *interface* には、RSPAN トラフィックを RSPAN VLAN にフラッディングするインターフェイスを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*]	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session** *session_number* **filter vlan** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定をすべてクリアし、トランク ポート 4 上での受信したトラフィックをモニタリングする RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 のトラフィックだけを、ポート 8 をリフレクタ ポートとして宛先リモート VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/4 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902 reflector-port
gigabitethernet0/8
```

```
Switch(config)# end
```

SPAN および RSPAN のステータス表示

現在の SPAN または RSPAN 設定のステータスを表示するには、**show monitor** 特権 EXEC コマンドを使用します。

次に、SPAN 送信元セッション 1 に対する **show monitor** 特権 EXEC コマンドの出力例を示します。

```
Switch# show monitor session 1
Session 1
---------
Type              : Local Session
Source Ports      :
    RX Only       : None
    TX Only       : None
    Both          : Fa0/4
Source VLANs      :
    RX Only       : None
    TX Only       : None
    Both          : None
Source RSPAN VLAN : None
Destination Ports : Fa0/5
    Encapsulation: DOT1Q
          Ingress: Enabled, default VLAN = 5
Reflector Port    : None
Filter VLANs      : None
Dest RSPAN VLAN   : None
```