CHAPTER 30

SPAN および RSPAN の設定

この章では、Catalyst 3750-E または 3560-E スイッチに Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）を設定する方法について説明します。特に明記しないかぎり、*スイッチ*という用語は Catalyst 3750-E または 3560-E スタンドアロン スイッチおよび Catalyst 3750-E スイッチ スタックを意味します。

（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、このリリースのコマンド リファレンスを参照してください。

SPAN および RSPAN の概要

ポートまたは VLAN（バーチャル LAN）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 または RSPAN を使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタリング デバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用して監視できるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックは監視できません。たとえば、着信トラフィックを監視している場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックは監視できません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、監視できます。

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 Intrusion Detection System（IDS; 侵入検知システム）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。

ここでは、次の概要について説明します。

ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチまたはスイッチ スタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。たとえば、図 30-1 の場合、ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされます。ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 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 30-1　　単一スイッチでのローカル SPAN の設定例

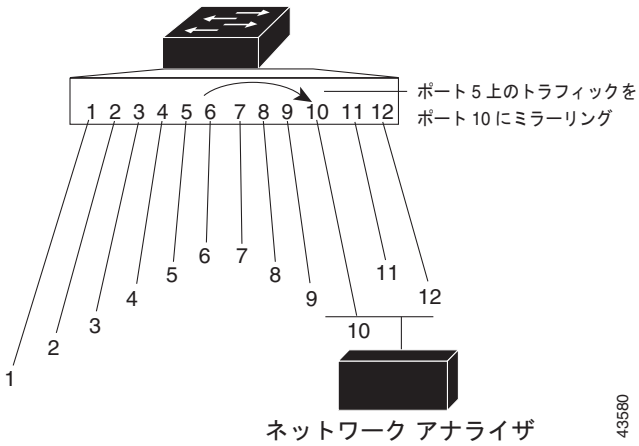
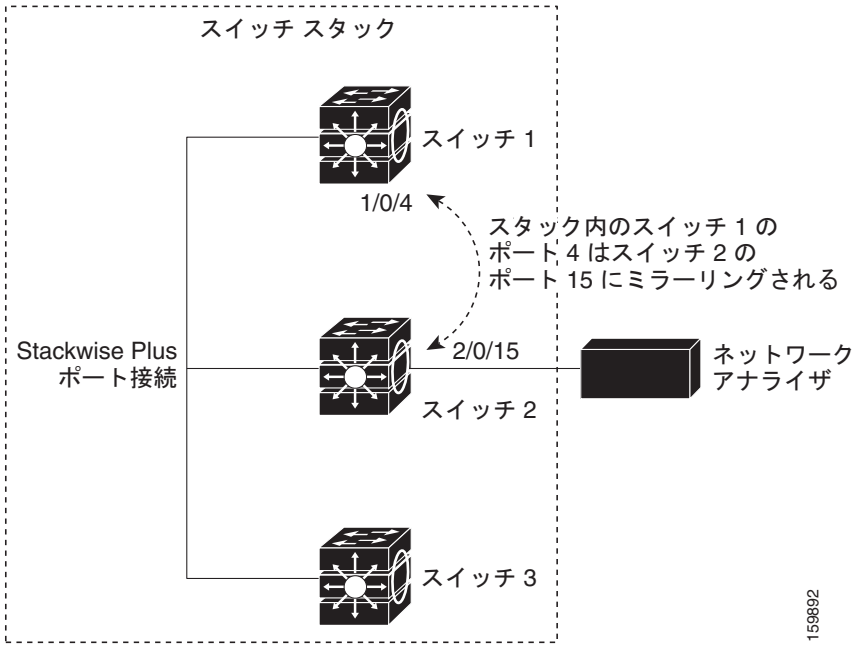


図 30-2 に、送信元ポートおよび宛先ポートが異なるスタック メンバー上にある場合の、スイッチ スタックのローカル SPAN の例を示します。

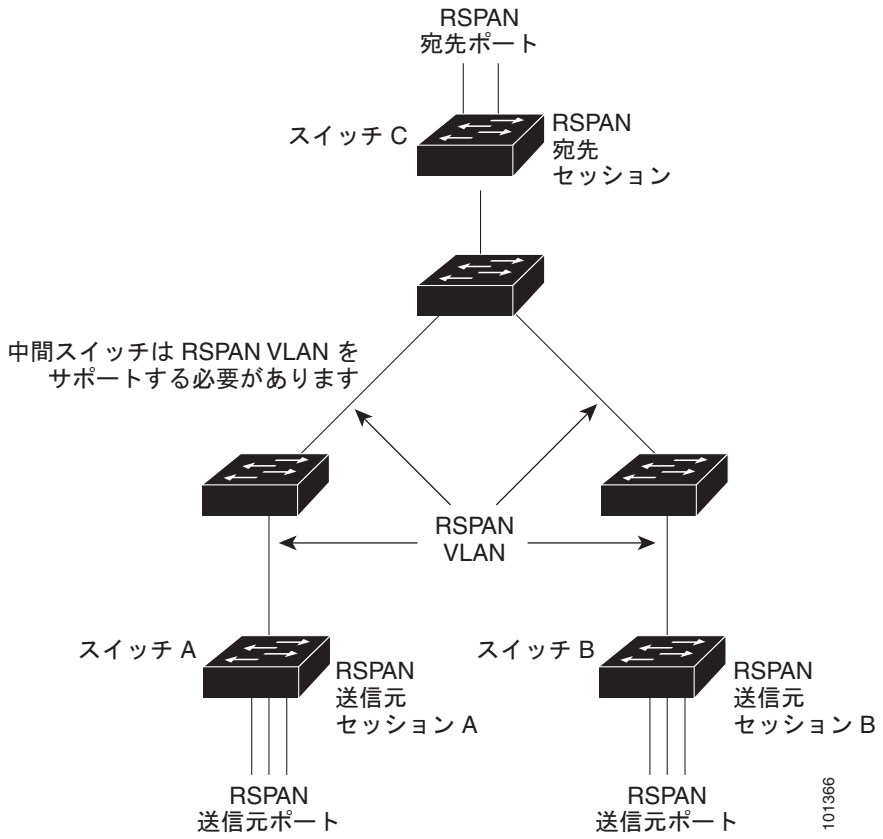
図 30-2　スイッチ スタックでのローカル SPAN の設定例



リモート SPAN

RSPAN は、異なるスイッチ（または異なるスイッチ スタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートしているので、ネットワーク上で複数のスイッチをリモートで監視できます。図 30-3 に、スイッチ A とスイッチ B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、参加するすべてのスイッチにおける当該 RSPAN セッション専用としてユーザ指定された RSPAN VLAN 上で伝送されます。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN を監視する宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。図中のスイッチ C のように、宛先は常に物理ポートになります。

図 30-3　RSPAN の設定例



SPAN と RSPAN の概念および用語

SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート上、あるいは 1 つまたは複数の VLAN 上でトラフィックを監視し、その監視したトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。ローカル SPAN には、送信元セッションおよび宛先セッションが個別に設定されません。ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタギングを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットを解析のためにユーザにコピーすることです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN 送信元セッションと宛先セッションを分離する中継スイッチを配置することもできます。これらのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要求に応答する必要があります（「RSPAN VLAN」（P.30-9）を参照）。

SPAN セッションでのトラフィックのモニタリングには、次のような制約があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- Catalyst 3560E-12D スイッチ以外のスイッチは、最大 2 つのローカル SPAN または RSPAN 送信元セッションをサポートします。
  - 同じスイッチまたはスイッチスタック内でローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチまたはスイッチスタックは、合計 66 個の送信元および RSPAN 宛先セッションをサポートします。
  - 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 送信元セッションを 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。
- Catalyst 3560E-12D スイッチは 1 つの送信元セッションだけ（ローカル SPAN または RSPAN 送信元セッションのいずれか）をサポートしますが、これはセッション 1 でなければなりません。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。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのスイッチ スタックに設定できる宛先ポートは最大で 64 個です。
- 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、10 Mb/s のポートで 100 Mb/s のポートを監視するなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。したがって、多数のポートまたは VLAN を監視すると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上では、SPAN セッションを設定できますが、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かぎり、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。

– 同じスイッチまたはスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

監視対象トラフィック

SPAN セッションは、次のトラフィック タイプを監視できます。

- RX（受信）SPAN：受信（または入力）SPAN の役割は、送信元インターフェイスまたは VLAN が受信したすべてのパケットを、スイッチが変更または処理を行う前にできるだけ多く監視することです。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。

  Differentiated Services Code Point（DSCP）の変更など、ルーティングや QoS（Quality of Service）が原因で変更されたパケットは、変更される前にコピーされます。

  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、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。パケットをドロップする可能性のある機能は、標準および拡張 IP 入力 Access Control List（ACL; アクセス コントロール リスト）、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- 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あとで、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監視することです。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用意されます。

  ルーティングが原因で変更されたパケット（Time to Live（TTL; 存続可能時間）、Media Access Control（MAC; メディア アクセス コントロール）アドレス、QoS 値の変更など）は、宛先ポートで（変更されて）コピーされます。

  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 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 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、ポートまたは VLAN を監視することもできます。これがデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。通常、SPAN は Cisco Discovery Protocol（CDP）、VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）、Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）などの Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）パケットおよびレイヤ 2 プロトコルを監視しません。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートの場合と同じカプセル化設定（タグなし、Inter Switch Link（ISL; スイッチ間リンク）、または IEEE 802.1Q）を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットが監視されます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タグなし、ISL、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットがドロップされることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因で監視されないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチの輻輳が原因でドロップされた出力パケットは、出力 SPAN からもドロップされます。

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、双方向（受信と送信の両方）SPAN セッションが、ポート A では受信モニタに、ポート B では送信モニタに設定されているとします。パケットがポート A からスイッチに入ってポート B にスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。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、パケット変更のため異なるパケットになります）。

ソース 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。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向で監視できます。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 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。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数は最大 2 つ（ローカルまたは RSPAN）であり、Catalyst 3560E-12D スイッチは送信元ポートまたは VLAN で 1 つのセッションだけ（ローカルまたは RSPAN）サポートします。単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- スイッチ上の複数の SPAN セッションで監視できます。Catalyst 3560E-12D スイッチでは、1 つの SPAN セッションでだけを監視できます。
- 監視する方向（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。
- すべてのポート タイプ（EtherChannel、ギガビット イーサネットなど）が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックを監視できます。
- アクセス ポート、トランク ポート、ルーテッド ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにはできません。
- 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。
- 単一セッション内で複数の送信元ポートを監視することが可能です。

送信元 VLAN

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 トラフィックを監視できます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートで監視されます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向で監視できます。
- 指定されたポートでは、監視対象の 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、監視されません。
- 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、監視中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN は、使用できません。
- 監視できるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとして監視する場合、デフォルトでは、トランク上でアクティブなすべての VLAN が監視されます。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 トラフィックの監視対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートだけです。
- VLAN フィルタリングはポートベース セッションにだけ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN だけが監視されます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにだけ作用し、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。

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、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名 *モニタ側ポート*）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチまたはスイッチスタックに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションだけを実行するスイッチまたはスイッチ スタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにはできません。
- 送信元ポートにはできません。
- EtherChannel グループまたは VLAN にはできません。
- 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）。
- アクティブな場合、着信トラフィックはディセーブルになります。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。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィックの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。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）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、監視されません。

- スイッチまたはスイッチスタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化について次のとおり動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、ISL、または IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

宛先ポート グループ

（注）　ここでは、Catalyst 3560E-12D スイッチに限定して説明します。

Catalyst 3560E-12D スイッチは、同じ*宛先ポート グループ*に属している宛先ポートを通してだけ、SPAN および RSPAN トラフィックを送信できます。RSPAN 宛先セッションを設定する場合、宛先ポート グループ（a、b、または c）を指定する必要があります。宛先ポート グループの詳細については、「SPAN 設定時の注意事項」（P.30-13）を参照してください。

宛先ポートが 1 つしかないローカル SPAN セッションでは、宛先ポート グループを指定する必要はありません。セッションに 2 つめの宛先ポートを追加する場合、そのポートは既存の宛先ポートと同じ宛先ポート グループに属していなければなりません。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には次の特殊な特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上だけです。
- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）に対して可視である VLAN 1 ～ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲（1006 ～ 4094）内の RSPAN VLAN ID を割り当てる場合は、すべての中継スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN を監視したり、ユーザにトラフィックを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

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：SPAN はルーテッド トラフィックを監視しません。VSPAN が監視するのはスイッチに出入りす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監視しません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは 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。
- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは 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。
- VTP：VTP を使用すると、スイッチ間で RSPAN VLAN のプルーニングが可能です。
- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバ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、宛先ポートの VLAN メンバシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートの VLAN メンバ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 グループは、送信元ポートとして設定できますが、SPAN 宛先ポートとしては設定できません。グループが SPAN 送信元として設定されている場合、グループ全体が監視されます。

  監視対象の EtherChannel グループに物理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。監視対象の 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。

  EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータは監視されます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先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 メンバーのままですが、*inactive* または *suspended* ステートになります。

  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 グループおよび監視対象ポート リストから削除されます。
- マルチキャスト トラフィックを監視できます。出力ポートおよび入力ポートのモニタリングでは、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。
- プライベート VLAN ポートを SPAN 宛先ポートにはできません。
- セキュア ポートを SPAN 宛先ポートにはできません。

  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、出力を監視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、出力を監視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。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

  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、出力を監視しているポートで IEEE 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、出力を監視しているポートで IEEE 802.1x をイネーブルにしないでください。

SPAN/RSPAN およびスイッチ スタック

スイッチ スタックは 1 つの論理スイッチとして扱われるため、ローカル SPAN 送信元ポートおよび宛先ポートをスタック内の異なるスイッチに設定できます。したがって、スタックにスイッチを追加または削除すると、ローカル SPAN セッションや、RSPAN 送信元または宛先セッションに影響が及ぶことがあります。スタックからスイッチを削除すると、アクティブ セッションが非アクティブになることがあります。スタックにスイッチを追加すると、非アクティブ セッションがアクティブになることがあります。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

フローベース SPAN の概要

送信元ポートで監視されるトラフィックに Access Control List（ACL; アクセス コントロール リスト）を適用するフローベース SPAN（FSPAN）またはフローベース RSPAN（FRSPAN）を使用して、SPAN または RSPAN で監視するネットワーク トラフィックのタイプを制御できます。FSPAN ACL は、IPv4、IPv6、および監視される非 IP トラフィックをフィルタリングするように設定できます。

インターフェイスを通して ACL を SPAN セッションに適用します。ACL は SPAN セッション内のすべてのインターフェイスで監視されるすべてのトラフィックに適用されます。この ACL によって許可されるパケットは、SPAN 宛先ポートにコピーされます。ほかのパケットは SPAN 宛先ポートにコピーされません。

元のトラフィックは継続して転送され、接続している任意のポート、VLAN、およびルータ ACL が適用されます。FSPAN ACL は転送の決定に影響を与えることはありません。同様に、ポート、VLAN、およびルータ ACL は、トラフィックのモニタリングに影響を与えません。セキュリティ入力 ACL がパケットを拒否したために転送されない場合でも、FSPAN ACL が許可すると、パケットは SPAN 宛先ポートにコピーされます。しかし、セキュリティ出力 ACL がパケットを拒否したために転送されない場合、パケットは SPAN 宛先ポートにコピーされません。ただし、セキュリティ出力 ACL がパケットの送信を許可した場合だけ、パケットは、FSPAN ACL が許可した場合 SPAN 宛先ポートにコピーされます。これは RSPAN セッションについてもあてはまります。

SPAN セッションには、次の 3 つのタイプの FSPAN ACL を接続できます。

- IPv4 FSPAN ACL：IPv4 パケットだけをフィルタリングします。
- IPv6 FSPAN ACL：IPv6 パケットだけをフィルタリングします。
- MAC FSPAN ACL：IP パケットだけをフィルタリングします。

セキュリティ ACL は、スイッチ上の FSPAN ACL よりも高いプライオリティをもっています。FSPAN ACL が適用され、その後ハードウェア メモリに収まらないセキュリティ ACL を追加する場合、適用された FSPAN ACL は、セキュリティ ACL のスペースを確保するためにメモリから削除されます。この処理（*アンローディング*と呼ばれる）は、システム メッセージにより通知されます。メモリ内に常駐するスペースが確保できたら、スイッチ上のハードウェア メモリに FSPAN ACL が追加されます。この処理（*リローディング*と呼ばれる）は、システム メッセージにより通知されます。IPv4、IPv6、および MAC FSPAN ACL は、別個にアンロードまたはリロードできます。

スタックに設定された VLAN ベースの FSPAN セッションが 1 つまたは複数のスイッチ上のハードウェア メモリに収まらない場合、セッションはこれらのスイッチ上でアンロードされたものとして処理され、スイッチでの FSPAN ACL およびソーシングのためのトラフィックは、SPAN 宛先ポートにコピーされません。FSPAN ACL は継続して正しく適用され、トラフィックは FSPAN ACL がハードウェア メモリに収まるスイッチの SPAN 宛先ポートにコピーされます。

空の FSPAN ACL が接続されると、一部のハードウェア機能により、その ACL の SPAN 宛先ポートにすべてのトラフィックがコピーされます。十分なハードウェア リソースが使用できない場合、空の FSPAN ACL もアンロードされる可能性があります。

IPv4 および MAC FSPAN ACL は、すべてのフィーチャ セットでサポートされています。IPv6 FSPAN ACL は、拡張 IP サービス フィーチャ セットでだけサポートされています。

FSPAN および FRSPAN のためのスイッチ設定については、「FSPAN および FRSPAN の設定」（P.30-27）を参照してください。

SPAN および RSPAN の設定

SPAN および RSPAN のデフォルト設定

表 30-1　SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート（SPAN および RSPAN）	ディセーブル
監視する送信元ポート 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**）
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）
入力転送（宛先ポート）	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上で、すべての VLAN が監視対象
RSPAN VLAN	未設定

ローカル SPAN の設定

SPAN 設定時の注意事項

- 各スイッチ スタックにつき、最大 2 つの送信元セッションおよび 64 の RSPAN 宛先セッションを設定できます。*送信元セッション*は、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックを監視できます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートは送信元ポートにできません。同様に、送信元ポートも宛先ポートにできません。
- 同じ宛先ポートでは、2 つの SPAN セッションを設定できません。
- 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監視されるだけです。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、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は、送信元ポートまたは宛先ポートとして設定できますが、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。
- 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 ポートを監視している場合、このキーワードで指定された VLAN 上のトラフィックだけが監視されます。デフォルトでは、トランク ポート上のすべての VLAN が監視されます。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。
- 次の注意事項は、Catalyst 3560E-12D スイッチに適用されます。
  - 次のタイプのセッションで **monitor session** *session_number* **destination remote vlan** *vlan-id* **destination-port group** {**a** | **b** | **c**} グローバル コンフィギュレーション コマンドを入力し、RSPAN 送信元セッションの宛先ポート グループを指定する必要があります。
  - スイッチは、スイッチ ポートの設定に応じて、次の宛先ポート グループをサポートします。

    a：tengigabitethernet 0/1 ～ tengigabitethernet 0/4 *または* gigabitethernet 0/1 ～ gigabitethernet 0/8

    b：tengigabitethernet 0/5 ～ tengigabitethernet 0/8 *または* gigabitethernet 0/9 ～ gigabitethernet 0/16

    c：tengigabitethernet 0/9 ～ tengigabitethernet 0/12 *または* gigabitethernet 0/17 ～ gigabitethernet 0/24

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（監視対象）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* の範囲は、1 ～ 66 です。 • 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* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 *session_number* の範囲は、1 ～ 66 です。Catalyst 3560E-12D スイッチでこのコマンドを入力する場合、*session_number* には **1** だけを入力できます。 *interface-id* には、監視する送信元ポートまたは送信元 VLAN を指定します。 • 送信元 *interface-id* には、監視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。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 **（注）** 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 （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）監視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、SPAN は送信トラフィックと受信トラフィックの両方を監視します。 • **both**：送信トラフィックと受信トラフィックの両方を監視します。これがデフォルトです。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。 **（注）** **monitor session** *session_number* **source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}	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、ステップ 3 で入力したセッション番号を指定します。 **（注）** ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （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）送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、**encapsulation replicate** を入力します。これを選択しない場合、デフォルトでは、パケットがネイティブ形式（タグなし）で送信されます。 **（注）** **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
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*] **show running-config**	設定を確認します。
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 セッションを削除するには、**no monitor session** *session_number* 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。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-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。宛先インターフェイスの場合、このコマンドの **no** 形式では、encapsulation オプションは無視されます。

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックを監視する例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 へミラーリングします。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 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 gigabitethernet1/0/1
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 1 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 gigabitethernet1/0/1 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監視されます。

次に、SPAN セッション 2 の既存の SPAN 設定を削除し、VLAN 1 ～ 3 に属するすべてのポート上の受信トラフィックを監視するよう SPAN セッション 2 を設定し、宛先ポート Gigabit Ethernet 2 へ送信します。この設定は、VLAN 10 に属するすべてのポート上のすべてのトラフィックも監視するように変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定したあと、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置など）用に着信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。

着信トラフィックに関係しないキーワードの詳細については、「ローカル SPAN セッションの作成」（P.30-14）を参照してください。

	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。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケット カプセル化、および入力 VLAN とカプセル化を指定します。 *session_number* には、ステップ 3 で入力したセッション番号を指定します。Catalyst 3560E-12D スイッチでこのコマンドを入力する場合、*session_number* には **1** だけを入力できます。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （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。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。 （任意）送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、**encapsulation replicate** を入力します。これを選択しない場合、デフォルトでは、パケットがネイティブ形式（タグなし）で送信されます。 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** をキーワードと一緒に入力します。 • **dot1q vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 • **isl**：ISL カプセル化を使用して着信パケットを転送します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
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*] **show running-config**	設定を確認します。
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 セッションを削除するには、**no monitor session** *session_number* 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。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-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。宛先インターフェイスの場合、このコマンドの **no** 形式を使用すると、カプセル化および入力オプションは無視されます。

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックを監視するように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
replicate ingress dot1q vlan 6
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* の範囲は、1 ～ 66 です。 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*	送信元ポート（監視対象ポート）と SPAN セッションの特性を指定します。 *session_number* の範囲は、1 ～ 66 です。Catalyst 3560E-12D スイッチでこのコマンドを入力する場合、*session_number* には **1** だけを入力できます。 *interface-id* には、監視する送信元ポートを指定します。指定されたインターフェイスは、あらかじめトランク ポートとして設定されていなければなりません。
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、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* に指定できる範囲は、1 ～ 4094 です。 （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* [**,** | **-**] [**encapsulation replicate**]}	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、ステップ 3 で入力したセッション番号を指定します。 *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 （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）送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、**encapsulation replicate** を入力します。これを選択しない場合、デフォルトでは、パケットがネイティブ形式（タグなし）で送信されます。
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*] **show running-config**	設定を確認します。
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 を監視するには、**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 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックを監視するように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してだけトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end
```

RSPAN の設定

RSPAN 設定時の注意事項

- 「SPAN 設定時の注意事項」（P.30-13）のすべての項目は RSPAN にも当てはまります。
- RSPAN VLAN には特殊な特性があるので、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 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監視できます。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 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。
- 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 ポートにだけ設定されており、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（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 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。ただし、スイッチはセッション間にわたるトラフィックを監視しないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。
- 次の条件を満たすかぎり、任意の VLAN を RSPAN VLAN として設定できます。
  - 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。

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。
- 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 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、および中継スイッチに 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。有効範囲は 2 ～ 1001 および 1006 ～ 4094 です。 RSPAN VLAN は、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 Fiber Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）VLAN 専用）にできません。
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、監視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* の範囲は、1 ～ 66 です。 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* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	RSPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 *session_number* の範囲は、1 ～ 66 です。Catalyst 3560E-12D スイッチでこのコマンドを入力する場合、*session_number* には **1** だけを入力できます。 RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 • *interface-id* には、監視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。有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 （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）監視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。 • **both**：送信トラフィックと受信トラフィックの両方を監視します。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。

	コマンド	目的
ステップ 4	Catalyst 3560E-12D スイッチ以外のスイッチの場合： **monitor session** *session_number* **destination remote vlan** *vlan-id* Catalyst 3560E0-12D スイッチの場合： **monitor session** *session_number* **destination remote vlan** *vlan-id* **destination-port group** {**a** | **b** | **c**}	RSPAN セッション、宛先 RSPAN VLAN、および宛先ポート グループを指定します。 *session_number* には、ステップ 3 で指定した番号を入力します。 *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。 Catalyst 3560E-12D スイッチの場合、**destination-port group** {**a** | **b** | **c**} を入力し、RSPAN トラフィックを伝送するポートを指定します。
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*] **show running-config**	設定を確認します。
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 セッションを削除するには、**no monitor session** *session_number* 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。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-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。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number* **destination remote vlan** *vlan-id* コマンドを使用します。

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスを監視するように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

次に、Catalyst 3560E-12D スイッチで、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスを監視するように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901 destination-port group b
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 に制限するように RSPAN 送信元セッションを設定するには、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* の範囲は、1 ～ 66 です。 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*	送信元ポート（監視対象ポート）と SPAN セッションの特性を指定します。 *session_number* の範囲は、1 ～ 66 です。Catalyst 3560E-12D スイッチでこのコマンドを入力する場合、*session_number* には **1** だけを入力できます。 *interface-id* には、監視する送信元ポートを指定します。指定されたインターフェイスは、あらかじめトランク ポートとして設定されていなければなりません。
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、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* に指定できる範囲は、1 ～ 4094 です。 （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	Catalyst 3560E-12D スイッチ以外のスイッチの場合： **monitor session** *session_number* **destination remote vlan** *vlan-id* Catalyst 3560E0-12D スイッチの場合： **monitor session** *session_number* **destination remote vlan** *vlan-id* **destination-port group** {**a** | **b** | **c**}	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 *session_number* には、ステップ 3 で指定したセッション番号を入力します。 *vlan-id* には、宛先ポートに監視対象トラフィックを伝送する RSPAN VLAN を指定します。 Catalyst 3560E-12D スイッチの場合、**destination-port group** {**a** | **b** | **c**} を入力し、RSPAN トラフィックを伝送するポートを指定します。
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*] **show running-config**	設定を確認します。
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 を監視するには、**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 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックを監視するように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してだけトラフィックを宛先 RSPAN 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 gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

次に、Catalyst 3560E-12D スイッチで、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックを監視するように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してだけトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

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

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは別のスイッチまたはスイッチ スタック（送信元セッションが設定されていないスイッチまたはスイッチ スタック）に設定します。

このスイッチ上で RSPAN VLAN を定義し、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	**vlan** *vlan-id*	送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ～ 4 は不要です。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として識別します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**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* の範囲は、1 ～ 66 です。 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 6	**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* の範囲は、1 ～ 66 です。Catalyst 3560E-12D スイッチでこのコマンドを入力する場合、*session_number* には **1** だけを入力できます。 *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。

	コマンド	目的
ステップ 7	**monitor session** *session_number* **destination interface** *interface-id*	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、ステップ 6 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 10	**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 セッションを削除するには、**no monitor session** *session_number* 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。SPAN セッションから宛先ポートを削除するには、**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。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number* **source remote vlan** *vlan-id* コマンドを使用します。

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 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 gigabitethernet2/0/1
Switch(config)# end
```

RSPAN 宛先セッションの作成および着信トラフィックの設定

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し、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置など）用に着信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。

着信トラフィックに関係しないキーワードの詳細については、「RSPAN 宛先セッションの作成」（P.30-24）を参照してください。この手順は、RSPAN VLAN がすでに設定されていることを前提にしています。

	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。
ステップ 3	**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* の範囲は、1 ～ 66 です。Catalyst 3560E-12D スイッチでこのコマンドを入力する場合、*session_number* には **1** だけを入力できます。 *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**ingress** {**dot1q vlan** *vlan-id* **| isl | untagged vlan** *vlan-id* **| vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケット カプセル化、および着信 VLAN とカプセル化を指定します。 *session_number* には、ステップ 4 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 （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。 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** を追加のキーワードと一緒に入力します。 • **dot1q vlan** *vlan-id* : VLAN をデフォルトの VLAN として指定し、IEEE 802.1Q カプセル化を使用して着信パケットを転送します。 • **isl** : ISL カプセル化を使用して着信パケットを転送します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id* : VLAN をデフォルトの VLAN として指定し、タグなしのカプセル化を使用して着信パケットを転送します。
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*] **show running-config**	設定を確認します。
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 セッションを削除する場合は、**no monitor session** *session_number* 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。RSPAN セッションから宛先ポートを削除するには、**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。このコマンドの **no** 形式を使用すると、入力オプションは無視されます。

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
vlan 6
Switch(config)# end
```

FSPAN および FRSPAN の設定

FSPAN および FRSPAN 設定時の注意事項

- ACL は、一度に 1 つの SPAN または RSPAN にしか接続できません。
- FSPAN ACL が接続されていない場合、FSPAN はディセーブルで、すべてのトラフィックが SPAN 宛先ポートにコピーされます。
- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
  - SPAN セッションに空の FSPAN ACL を接続すると、パケットはフィルタリングされず、すべてのトラフィックが監視されます。
  - SPAN セッションに空ではない FSPAN ACL を少なくとも 1 つ接続し、ほかの 1 つまたは複数の FSPAN ACL を接続しなかった場合（たとえば、空ではない IPv4 ACL を接続し、IPv6 と MAC ACL を接続しなかった場合）、FSPAN は、接続されていない ACL によってフィルタリングされたと思われるトラフィックをブロックします。したがって、このトラフィックは監視されません。
- ポートベースの FSPAN セッションは、セッションに送信元ポートとして Catalyst 3750-E ポートだけが含まれている場合にかぎり、Catalyst 3750 スイッチを含むスタックで設定できます。セッションに送信元ポートとして Catalyst 3750 ポートが含まれている場合、FSPAN ACL コマンドは拒否されます。セッションに FSPAN ACL が設定されている場合、送信元ポートとして Catalyst 3750 ポートを含むコマンドは拒否されます。Catalyst 3750 ポートは、FSPAN セッション内の宛先ポートとして追加できます。
- VLAN ベースの FSPAN セッションは、Catalyst 3750 スイッチを含むスタックでは設定できません。
- FSPAN ACL は、ポート単位 VLAN 単位のセッションに適用できません。ポート単位 VLAN 単位のセッションは、最初にポートベースのセッションを設定し、次にセッションに特定の VLAN を設定することにより設定できます。次に例を示します。

```
Switch (config)# monitor session session_number source interface interface-id
Switch (config)# monitor session session_number filter vlan vlan-id
Switch (config)# monitor session session_number filter ip access-group
{access-list-number | name}
```

（注）　**filter vlan** および **filter ip access-group** の両方のコマンドを同時に設定できません。一方を設定すると、他方が拒否されます。

- EtherChannel は FSPAN セッションでサポートされていません。
- TCP フラグまたは **log** キーワードが付いている FSPAN ACL はサポートされていません。
- スイッチで拡張 IP サービス フィーチャ セットを稼動中に IPv6 FSPAN ACL を設定し、のちに異なるフィーチャ セットを稼動した場合、スイッチのリブート後、スイッチでの IPv6 FSPAN ACL 設定が失われる可能性があります。
- IPv6 FSPAN ACL は、IPv6 対応の SDM テンプレートでだけサポートされています。IPv6 対応の SDM テンプレートを稼動中に IPv6 FSPAN ACL を設定し、のちに非 IPv6 SDM テンプレートを設定してスイッチをリブートすると、IPv6 FSPAN ACL 設定が失われます。

FSPAN セッションの設定

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定し、セッションに FSPAN を設定するには、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* の範囲は、1 ～ 66 です。 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* | **vlan** *vlan-id*} [, | -] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、監視する送信元ポートまたは送信元 VLAN を指定します。 • 送信元 *interface-id* には、監視する送信元ポートを指定します。物理インターフェイスだけが有効です。 • *vlan-id* には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 **（注）** 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （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）監視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、SPAN は送信トラフィックと受信トラフィックの両方を監視します。 • **both**：送信トラフィックと受信トラフィックの両方を監視します。これがデフォルトです。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。 **（注）** **monitor session** *session_number* **source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}	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、ステップ 3 で入力したセッション番号を指定します。 **（注）** ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （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）送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、**encapsulation replicate** を入力します。これを選択しない場合、デフォルトでは、パケットがネイティブ形式（タグなし）で送信されます。 **（注）** **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 5	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*}	SPAN セッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 3 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • *name* には、トラフィックのフィルタリングに使用したい ACL の名前を指定します。
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*] **show running-config**	設定を確認します。
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。

FRSPAN セッションの設定

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定し、セッションに FRSPAN を設定するには、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* の範囲は、1 ～ 66 です。 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* | **vlan** *vlan-id*} [, | -] [**both** | **rx** | **tx**]	RSPAN セッションおよび送信元ポート（監視対象ポート）を指定します。 *session_number* の範囲は、1 ～ 66 です。 RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 • 送信元 *interface-id* には、監視する送信元ポートを指定します。物理インターフェイスだけが有効です。 • *vlan-id* には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （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）監視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。 • **both**：送信トラフィックと受信トラフィックの両方を監視します。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。
ステップ 4	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先 RSPAN VLAN を指定します。 • *session_number* には、ステップ 3 で指定した番号を入力します。 • *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。
ステップ 5	**vlan** *vlan-id*	VLAN サブモードを開始します。*vlan-id* には、監視する送信元 RSPAN VLAN を指定します。
ステップ 6	**remote-span**	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを示します。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 8	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*}	RSPAN セッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 • *session_number* には、ステップ 3 で入力したセッション番号を指定します。 • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • *name* には、トラフィックのフィルタリングに使用したい ACL の名前を指定します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 11	**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、RSPAN、FSPAN、および FRSPAN ステータスの表示

現在の SPAN、RSPAN、FSPAN、FRSPAN 設定を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。また、設定されたセッションを表示するには、**show running-config** 特権 EXEC コマンドを使用できます。