



## SPAN および RSPAN の設定

---

この章では、Catalyst 3550 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) を設定する方法について説明します。



(注)

---

ここで使用され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。

---

この章で説明する内容は、次のとおりです。

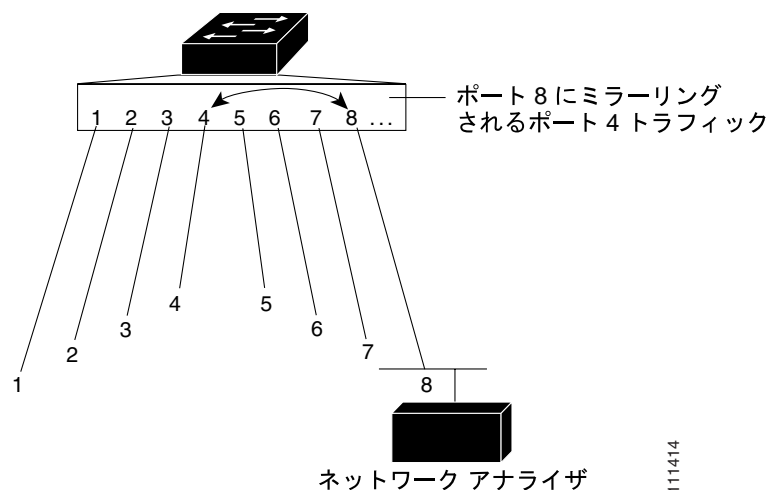
- [SPAN および RSPAN の概要 \(p.25-2\)](#)
- [SPAN の設定 \(p.25-9\)](#)
- [RSPAN の設定 \(p.25-16\)](#)
- [SPAN および RSPAN ステータスの表示 \(p.25-24\)](#)

## SPAN および RSPAN の概要

SPAN を使用すると、SwitchProbe デバイスまたはその他の Remote Monitoring (RMON) プロンプトやセキュリティ デバイスに接続されているスイッチの別のポートにトラフィックのコピーを送信することによって、ポートまたは VLAN (仮想 LAN) を通過するネットワーク トラフィックを分析できます。SPAN は、1 つの送信元ポートで送信や受信 (または送受信) したトラフィック、および 1 つまたは複数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分析するために宛先ポートにミラーリングします。

たとえば、[図 25-1](#) では、ポート 4 (送信元ポート) 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ています。ポート 8 のネットワーク アナライザは、ポート 4 に物理的に接続しなくても、ポート 4 からすべてのネットワーク トラフィックを受信します。

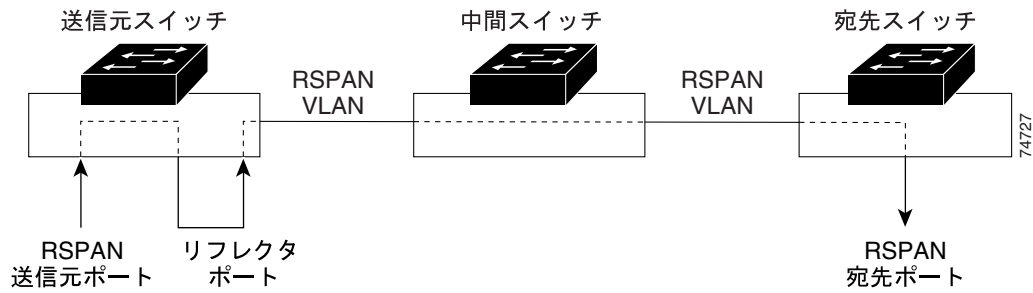
図 25-1 SPAN の設定例



SPAN でモニタ対象となるのは、送信元ポートに入出力するトラフィックまたは送信元 VLAN に入るトラフィックだけです。入力側送信元ポートまたは送信元 VLAN にルーティングされる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ているトラフィックはモニタしません。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モニタします。

RSPAN は、ネットワーク内の複数のスイッチのリモート モニタリング機能をイネーブルにして、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 ポートを経由して RSPAN VLAN にコピーされてから、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 を搬送します ([図 25-2](#) を参照)。

図 25-2 RSPAN 設定の例



SPAN および RSPAN は、送信元ポートまたは送信元 VLAN 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。

SPAN または RSPAN 宛先ポートを使用して、ネットワーク セキュリティ デバイスから送信されたトラフィックを転送できます。たとえば、Cisco Intrusion Detection System (IDS; 侵入検知システム) センサ装置を宛先ポートに接続した場合、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 セッションを停止させることができます。

## SPAN および RSPAN の概念と用語

ここでは、SPAN および RSPAN の設定に関連する概念と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、送信元ポートと宛先ポートおよび送信元 VLAN との対応付けです。RSPAN セッションは、送信元ポートおよびネットワーク上の送信元 VLAN と RSPAN VLAN との対応付けです。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 セッションを設定できます。SPAN セッションでのトラフィックのモニタには、次のような制限があります。

- 一連のまたは一定範囲のポートまたは VLAN 上の着信トラフィックをモニタできます。
- 単一のポートの発信トラフィックをモニタできます。複数ポートの発信トラフィックはモニタできません。
- VLAN 上の発信トラフィックはモニタできません。

個別のまたは重複する SPAN 送信元ポートと VLAN の集合を使用して、2 つの独立した SPAN または RSPAN セッションを設定できます。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 セッションは、スイッチの正常な動作を妨げません。ただし、SPAN の宛先がオーバーサブスクライブ型ポートである場合、たとえば 100 Mbps ポートをモニタする 10 Mbps ポートでは、パケットが廃棄されるか、または損失する可能性があります。

ディセーブルのポートでも SPAN セッションを設定できます。宛先ポートと、1 つまたは複数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。`show monitor session session_number` イネーブル EXEC コマンドを使用すると、SPAN セッションの動作ステータスが表示されます。

システムの電源投入後、宛先ポートが動作可能になるまで、SPAN セッションは非アクティブなままです。

## 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。

- 受信 (rx) SPAN 受信 (または入力) SPAN の目的は、スイッチが変更または処理を行う前に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できるかぎり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 セッションの宛先ポートに送信されます。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、タグgingは入力ポートで削除されます。宛先ポートでは、タグgingがイネーブルの場合、パケットは、ISL または IEEE 802.1Q ヘッダー付きで表示されます。タグgingが指定されていない場合は、パケットはネイティブのフォーマットで表示されます。

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; サービス品質) が原因で変更されたパケット (たとえば、変更済み Differentiated Services Code Point [DSCP]) は、rx SPAN 用に変更してコピーされます。

機能によっては受信処理中にパケットを廃棄することがありますが、この機能は SPAN には無効です。実際の着信パケットが廃棄された場合でも、宛先ポートはパケットのコピーを受信します。パケットを廃棄する可能性のある機能には、標準および拡張 IP 入力 Access Control List (ACL; アクセス制御リスト)、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などがあります。パケットの廃棄を引き起こすスイッチ輻輳も、SPAN には無効です。

- 送信 (tx) SPAN 送信 (または出力) SPAN の目的は、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできるかぎり多くモニタすることです。送信元から送信された各パケットのコピーは、その SPAN セッションに対応する宛先ポートに送信されます。コピーは、パケットの変更後送信されます。

1 つの SPAN セッションでは、出力側送信元ポートが 1 つだけ許可されます。出力方向では VLAN モニタはサポートされません。

ルーティングが原因で変更されたパケット (たとえば、Time to Live [TTL] または MAC [メディアアクセス制御] アドレス変更付き) は、宛先ポートでコピーされます。QoS が原因で変更されたパケットは、SPAN 送信元とは異なる DSCP (IP パケット) または Class of Service (CoS; サービスクラス) (非 IP パケット) を設定されることがあります。

送信処理中にパケットを廃棄する可能性のある機能は、SPAN 用のコピーにも影響を与えます。これらの機能には、VLAN マップ、マルチキャストパケットの標準および拡張 IP 出力 ACL、出力 QoS ポリシングなどがあります。出力 ACL の場合は、SPAN 送信元がパケットを廃棄すると、SPAN の宛先もパケットを廃棄します。出力側 QoS ポリシングの場合は、SPAN 送信元がパケットを廃棄しても、SPAN 宛先はパケットを廃棄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、宛先ポートは別の廃棄動作を行います。

- 双方向 (both) 1 つの SPAN セッションで、単一ポートの送信パケットと受信パケットを両方モニタできます。

## 送信元ポート

送信元ポート (別名 *モニタ対象ポート*) は、ネットワークトラフィック分析のためにモニタ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、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、受信トラフィックしかモニタできません。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入力側 VLAN (サポートされている VLAN の最大数まで) をサポートします。

送信元ポートには、次の特性があります。

- 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。
- 宛先ポートに指定することはできません。
- 各送信元ポートに、モニタする方向 (入力、出力、両方) 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 内であっても異なる VLAN 内であってもかまいません。
- VLAN SPAN 送信元の場合、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組み入れられます。

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すれば、特定の VLAN だけを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にできます。選択された VLAN のスイッチドトラフィックのみ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のみに作用し、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。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、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する宛先ポート (別名 *モニタ側ポート*) を設定する必要があります。

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になければなりません (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 ポートになることはできません。
- EtherChannel グループまたは VLAN にはできません。
- EtherChannel グループが SPAN 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た物理ポートに指定できます。ポートは、SPAN 宛先ポートとして設定されている間、グループから削除されます。
- このポートでは、SPAN セッションに必要なトラフィック以外の転送は行われません。
- 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。
- SPAN セッションがアクティブな間は、スパンニングツリーに参加しません。
- 宛先ポートである場合は、どのレイヤ 2 プロトコル (Cisco Discovery Protocol [CDP]、VLAN Trunk Protocol [VTP]、VLAN トランク プロトコル]、Dynamic Trunking Protocol [DTP]、Spanning-Tree Protocol [STP]、スパンニングツリー プロトコル]、Port Aggregation Protocol [PAgP]、または Link Aggregation Control Protocol [LACP]) にも参加しません。
- SPAN セッションの送信元 VLAN に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。
- 宛先ポートではアドレス学習は実行されません。

## リフレクタ ポート

リフレクタ ポートは、RSPAN VLAN にパケットをコピーするためのメカニズムで、所属している RSPAN 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ているポートに接続しているデバイスは、RSPAN 送信元セッションがディセーブルになるまで接続が切断されています。

リフレクタ ポートには、次の特性があります。

- ループバックを設定されたポートです。
- EtherChannel グループにはできません。トランキングは行わず、プロトコル フィルタリングも実行できません。
- EtherChannel グループが SPAN 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た物理ポートに指定できます。ポートは、リフレクタ ポートとして設定されている間、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 送信元または宛先ポートにすることはできません。また、ポートは、一度に複数のセッションでリフレクタ ポートにすることもできません。
- すべての VLAN に対して不可視です。
- リフレクタ ポートでのループバック トラフィック用のネイティブ 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。ループバックされたトラフィックは、RSPAN VLAN に入り、RSPAN VLAN を伝送するいずれか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、スパンニングツリーは自動的にディセーブルになります。

対応する送信元ポートおよび VLAN からのトラフィック量を処理できるだけの帯域幅がリフレクタ ポートにない場合は、超過パケットは廃棄されます。10/100 ポートは 100 Mbps で反映します。ギガビット ポートは 1 Gbps で反映します。

## VSPAN

VLAN-based 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。受信 (rx) トラフィックのみをモニタするように VSPAN を設定できますが、この場合、設定はその 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 上のトラフィックのみ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 ブルーニングと VLAN 許可リストは、SPAN モニタには無効です。
- VSPAN がモニタするのはスイッチに入るトラフィックに限られ、VLAN 間をルーティングするトラフィックはモニタしません。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とはならず、SPAN 宛先ポートで受信されません。
- 同じセッション内のフィルタ VLAN を VLAN 送信元と併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 を使用すると、マルチキャスト パケットおよび Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) パケットをはじめ、CDP、VTP、DTP、STP、PAgP、LACP パケットなど、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 では、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.25-16)を参照してください。

SPAN の設定によっては、同じ送信元パケットの複数のコピーが SPAN 宛先ポートに送信される場合があります。たとえば、送信元 a1 受信モニタおよび a2 送受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 のほかの機能との相互作用

SPAN は次の機能と相互作用します。

- ルーティング 入力 SPAN はルーティング トラフィックをモニタしません。VSPAN がモニタするのはスイッチに入るトラフィックに限られ、VLAN 間をルーティングするトラフィックはモニタしません。たとえば、VLAN が受信モニタされ、マルチレイヤ スイッチが別の VLAN からモニタ対象 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モニタされず、SPAN 宛先ポートで受信されません。
- STP 宛先ポートまたはリフレクタ ポートは、SPAN または RSPAN セッションがアクティブな間、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、これらのポートは STP に参加します。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 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。
- 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、宛先、およびリフレクタ ポートの VLAN メンバーシップまたはトランク設定は、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設定に対する変更は、SPAN または RSPAN セッションをディセーブルにするまでは有効になりません。送信元ポートの VLAN メンバーシップまたはトランク設定の変更はただちに有効になり、対応する SPAN セッションは、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に設定できますが、SPAN 宛先ポートには設定できません。グループを SPAN 送信元として設定すると、グループ全体がモニタ対象となります。

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

EtherChannel グループに属する物理ポートを、SPAN 送信元、宛先、またはリフレクタ ポートに設定した場合は、EtherChannel グループから削除されます。SPAN セッションからポートが削除されると、EtherChannel グループに復帰します。EtherChannel グループから削除されたポートはグループのメンバーに残りますが、ダウンまたはスタンダアロン状態になります。

EtherChannel グループに属す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、かつ EtherChannel グループが送信元である場合、ポートは EtherChannel グループおよびモニタ対象ポートのリストから削除されます。

- QoS 入力モニタの場合、SPAN 宛先ポートに送信されたパケットは、SPAN 送信元ポートで実際に受信したパケットと異なることがあります。パケットが入力側 QoS 分類およびポリシングのあとで転送されたためです。パケットの DSCP は、受信されたパケットと異なる場合があります。  
出力モニタの場合、SPAN 宛先ポートに送信されたパケットは、SPAN 送信元ポートに送信されたパケットと異なる場合があります。SPAN 送信元ポートでの出力側 QoS ポリシングによって、パケット分類が変更されることがあるためです。QoS ポリシングは、SPAN 宛先ポートでは適用されません。
- マルチキャストトラフィックをモニタできます。出力側および入力側ポートモニタの場合は、未編集パケットが 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が送信された回数は反映されません。
- ポートセキュリティ セキュアポートは SPAN 宛先ポートにはできません。  
SPAN セッションでは、宛先ポートで入力転送がイネーブルの場合、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どのポートでも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 SPAN 宛先ポートまたはリフレクタポートで IEEE 802.1X をイネーブルにできますが、SPAN 宛先ポートまたはリフレクタポートとして削除するまでは、IEEE 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、IEEE 802.1X をイネーブルにできます。  
SPAN セッションでは、宛先ポートで入力転送がイネーブルの場合、出力をモニタしているポートで 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、出力をモニタしているどのポートでも IEEE 802.1X をイネーブルにしないでください。

## SPAN および RSPAN のセッション限度

スイッチ上に、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 [不揮発性 RAM] に格納）できます。各スイッチでは、最大 2 つの SPAN または RSPAN セッションを設定（および NVRAM に格納）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割できます。セッションごとに送信元として、複数のポートまたは VLAN を設定できます。

## SPAN および RSPAN のデフォルト設定

表 25-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 25-1 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のトラフィック	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 フォーム (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。具体的な設定情報は次のとおりです。

- [SPAN 設定時の注意事項 \(p.25-9\)](#)
- [SPAN セッションの作成とモニタするポートの指定 \(p.25-10\)](#)
- [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 \(p.25-11\)](#)
- [SPAN セッションからのポートの削除 \(p.25-13\)](#)
- [モニタする VLAN の指定 \(p.25-14\)](#)
- [フィルタリングする VLAN の指定 \(p.25-15\)](#)

### SPAN 設定時の注意事項

SPAN の設定の際は、次の注意事項に従ってください。

- SPAN セッションは、「[SPAN および RSPAN のセッション限度](#)」(p.25-8)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。
- 宛先ポートは送信元ポートにできません。また、送信元ポートは宛先ポートにできません。
- 宛先ポートは SPAN セッションごとに 1 つしか設定できません。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 ポートは 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。
- IEEE 802.1X ポートは SPAN 送信元ポートにできます。SPAN 宛先ポートまたはリフレクタポートで IEEE 802.1X をイネーブルにできますが、SPAN 宛先ポートまたはリフレクタポートとして削除するまでは、IEEE 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は、1 つのポートの送信トラフィック、あるいは一連のまたは一定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 宛先ポートに設定すると、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のは、モニタ対象のトラフィックだけです。
- トランクポートは、送信元ポートにも宛先ポートにも設定できます。SPAN 宛先ポートを通過する送信パケットは、設定済みのカプセル化ヘッダー (ISL または IEEE 802.1Q のいずれか) を伝送します。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フォームで送信されます。
- ディセーブルに設定されているポートを送信元または宛先ポートにすることはできますが、SPAN 機能は、宛先ポートおよび 1 つ以上の送信元ポートまたは送信元 VLAN がイネーブルになるまでは起動しません。
- 受信トラフィックの場合、複数の送信元ポートと送信元 VLAN を 1 つの SPAN セッションで混在させることができます。送信元 VLAN とフィルタ VLAN を 1 つの 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 のどちらかを設定できますが、両方を同時に設定することはできません。
- `filter vlan` キーワードを使用すると、特定の VLAN に対して SPAN トラフィックを制限できます。モニタ対象がトランクポートの場合、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、トランクポートのすべての VLAN がモニタされます。
- SPAN 宛先ポートは、どの VLAN スパニングツリーにも参加しません。SPAN のモニタ対象トラフィックに BPDU が含まれているので、SPAN セッションの SPAN 宛先ポートで受信されたスパニングツリー BPDU は、SPAN 送信元ポートからのコピーです。
- SPAN がイネーブルのときに設定変更を行うと、次のような結果になります。
  - 宛先ポートの VLAN 設定を変更すると、SPAN がディセーブルになるまで変更は有効になりません。

- 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と、送信元ポートおよび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 である場合は、モニタされるポートの数は、モニタ対象の VLAN 間でポートを移動するに伴って変化します。

## SPAN セッションの作成とモニタするポートの指定

SPAN セッションを作成し、送信元 (モニタ対象) および宛先 (モニタ側) ポートを指定するには、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {session_number   all   local   remote}</code>	セッションの既存の SPAN 設定をクリアします。  <i>session_number</i> 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には <b>all</b> を、すべてのローカル セッションを削除するには <b>local</b> を、すべてのリモート SPAN セッションを削除するには <b>remote</b> を指定します。
ステップ 3	<code>monitor session session_number source interface interface-id [, -] [both   rx   tx]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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とポートチャネル論理インターフェイス ( <b>port-channel port-channel-number</b> ) があります。  (任意) [, -] 一連のまたは一定範囲のインターフェイスを指定します。カンマおよびハイフンの前後にはスペースを 1 つ入れます。  (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い場合、送信元インターフェイスは、送受信両方のトラフィックを送信します。追加の送信元ポートは、受信 (rx) トラフィックのみをモニタします。  <ul style="list-style-type: none"> <li>• <b>both</b> 送受信両方のトラフィックを送信します。</li> <li>• <b>rx</b> 受信トラフィックをモニタします。</li> <li>• <b>tx</b> 送信トラフィックをモニタします。</li> </ul>
ステップ 4	<code>monitor session session_number destination interface interface-id [encapsulation {dot1q   isl}]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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) 送信パケット用カプセル化ヘッダーを指定します。指定しない場合、パケットはネイティブ フォームで送信されます。  <ul style="list-style-type: none"> <li>• <b>isl</b> ISL カプセル化を使用します。</li> <li>• <b>dot1q</b> IEEE 802.1Q カプセル化を使用します。</li> </ul>
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。

	コマンド	目的
ステップ 6	<code>show monitor [session session_number]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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、宛先ポートで送信元ポートのトラフィックをモニタする手順を示します。最初に、セッション 1 の既存の SPAN 設定を消去し、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て送信元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 センサ装置など) 用の宛先ポートの入力トラフィックをイネーブルにするには、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {session_number   all   local   remote}</code>	セッションの既存の SPAN 設定をクリアします。  <i>session_number</i> 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には <b>all</b> を、すべてのローカル セッションを削除するには <b>local</b> を、すべてのリモート SPAN セッションを削除するには <b>remote</b> を指定します。
ステップ 3	<code>monitor session session_number source interface interface-id [,   -] [both   rx   tx]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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とポートチャネル論理インターフェイス ( <b>port-channel port-channel-number</b> ) があります。  (任意) [,   -] 一連のまたは一定範囲のインターフェイスを指定します。カンマおよびハイフンの前後にはスペースを 1 つ入れます。  (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い場合、送信元インターフェイスは、送受信両方のトラフィックを送信します。追加の送信元ポートは、受信 (rx) トラフィックのみをモニタします。  <ul style="list-style-type: none"> <li><b>both</b> 送受信両方のトラフィックを送信します。</li> <li><b>rx</b> 受信トラフィックをモニタします。</li> <li><b>tx</b> 送信トラフィックをモニタします。</li> </ul>

	コマンド	目的
ステップ 4	<b>monitor session</b> <i>session_number</i> <b>destination interface</b> <i>interface-id</i> <b>[encapsulation {dot1q [ingress vlan</b> <i>vlan id</i> ] <b>   isl [ingress]}   ingress vlan</b> <i>vlan id</i>	SPAN セッション、宛先ポート ( モニタ側ポート )、パケット カプセル化、および入力側 VLAN を指定します。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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定義されていない場合、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。  <ul style="list-style-type: none"> <li>• タグなしのネイティブ VLAN パケットと、ほかのすべての <b>dot1q</b> タグ付き VLAN tx パケットを送信する場合は、<b>encapsulation dot1q</b> を入力します。</li> <li>• ISL を使っ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、<b>encapsulation isl</b> を入力します。</li> <li>• ( 任意 ) <b>ingress</b> を指定して、ISL カプセル化を使用する際に、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します。</li> </ul> ( 任意 ) ネイティブ ( タグなし ) および dot1q カプセル化の場合、 <b>ingress vlan</b> <i>vlan id</i> を指定し、 <i>vlan id</i> 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 <i>vlan id</i> 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	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 6	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]	設定を確認します。
ステップ 7	<b>copy running-config startup-config</b>	( 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、IEEE 802.1Q カプセル化をサポートしていないセキュリティ デバイスを使用して、VLAN 5 の入力トラフィック用の宛先ポートを設定する例を示します。

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

次に、IEEE 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 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 destination interface fastethernet0/5 encapsulation dot1q ingress vlan 5
```

次に、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例を示します。

```
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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session <i>session_number</i></code> <code>source interface <i>interface-id</i> [,   -] [<i>both</i>   <i>rx</i>   <i>tx</i>]</code>	削除する送信元ポート ( モニタ対象ポート ) の特性と SPAN セッションを指定します。  <i>session</i> には、1 または 2 を指定します。  <i>interface-id</i> 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とポートチャネル論理インターフェイス ( <code>port-channel <i>port-channel-number</i></code> ) があります。  ( 任意 ) [,   -] 一連のまたは一定範囲のインターフェイスを指定します ( 設定済みの場合 )。このオプションは、受信トラフィックのみをモニタするときには有効です。カンマおよびハイフンの前後にはスペースを 1 つ入れます。  ( 任意 ) モニタを中止するトラフィックの方向 ( <code>both</code> 、 <code>rx</code> 、 <code>tx</code> ) を指定します。トラフィックの方向を指定しない場合、送受信両方のトラフィックがディセーブルになります。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show monitor [<i>session session_number</i>]</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	( 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には、`no monitor session session_number source interface interface-id` 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` キーワードを使用するのではなく、`monitor session session_number destination interface interface-id` を実行します。

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手順を示します。

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

次に、双方向モニタ用に設定された、ポートでの受信トラフィック モニタをディセーブルにする手順を示します。

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

ポート 1 での受信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。

## モニタする VLAN の指定

VLAN のモニタは、ポートのモニタと似ています。モニタする VLAN を指定するには、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {session_number   all   local   remote}</code>	セッションの既存の SPAN 設定をクリアします。  <i>session_number</i> 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には <code>all</code> を、すべてのローカル セッションを削除するには <code>local</code> を、すべてのリモート SPAN セッションを削除するには <code>remote</code> を指定します。
ステップ 3	<code>monitor session session_number source vlan vlan-id [, -] rx</code>	SPAN セッションおよび送信元 VLAN (モニタ対象 VLAN) を指定します。モニタできるのは、VLAN 上の受信 (rx) トラフィックだけです。  <i>session_number</i> には、1 または 2 を指定します。  <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。先頭に 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 (-) を使用して一定範囲の VLAN を指定します。カンマおよびハイフンの前後にはスペースを 1 つ入れます。
ステップ 4	<code>monitor session session_number destination interface interface-id [encapsulation {dot1q   isl}]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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) 送信パケット用カプセル化ヘッダーを指定します。指定しない場合、パケットはネイティブフォームで送信されます。  <ul style="list-style-type: none"> <li><code>isl</code> ISL カプセル化を使用します。</li> <li><code>dot1q</code> IEEE 802.1Q カプセル化を使用します。</li> </ul>
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show monitor [session session_number]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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 つまたは複数の送信元 VLAN または宛先ポートを削除するには、`no monitor session session_number source vlan vlan-id rx` 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 に既存の設定があれば消去し、VLAN 1 ~ 3 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するように 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。この例ではさらに、その設定を変更して、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するようにしています。

```
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

特定の VLAN に対する SPAN 送信元トラフィックを制限するには、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session { <i>session_number</i>   all   local   remote }</code>	セッションの既存の SPAN 設定をクリアします。  <i>session_number</i> 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には <code>all</code> を、すべてのローカル セッションを削除するには <code>local</code> を、すべてのリモート SPAN セッションを削除するには <code>remote</code> を指定します。
ステップ 3	<code>monitor session <i>session_number</i> source interface <i>interface-id</i> rx</code>	送信元ポート (モニタ対象ポート) および SPAN セッションの特性を指定します。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> には、モニタ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が、トランク ポートとして設定されている必要があります。
ステップ 4	<code>monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [,   -]</code>	特定の VLAN に対する SPAN 送信元トラフィックを制限します。  <i>session_number</i> には、1 または 2 を指定します。  <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。先頭に 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 (-) を使用して一定範囲の VLAN を指定します。カンマおよびハイフンの前後にはスペースを 1 つ入れます。
ステップ 5	<code>monitor session <i>session_number</i> destination interface <i>interface-id</i></code>	宛先ポート (モニタ側ポート) および SPAN セッションの特性を指定します。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show monitor [session <i>session_number</i>]</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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 に既存の設定があればクリアし、トランク ポート 4 での受信トラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ~ 5 および VLAN 9 のトラフィックのみを宛先ポート 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。具体的な設定情報は次のとおりです。

- RSPAN 設定時の注意事項 (p.25-16)
- RSPAN VLAN としての VLAN 設定 (p.25-17)
- RSPAN 送信元セッションの作成 (p.25-18)
- RSPAN 宛先セッションの作成 (p.25-19)
- RSPAN 宛先セッションの作成と入力トラフィックのイネーブル化 (p.25-20)
- RSPAN セッションからのポートの削除 (p.25-21)
- モニタする VLAN の指定 (p.25-22)
- フィルタリングする VLAN の指定 (p.25-23)

### RSPAN 設定時の注意事項

RSPAN の設定時は、次の注意事項に従ってください。

- RSPAN には、「SPAN 設定時の注意事項」(p.25-9) のすべての項目が当てはまります。
- RSPAN VLAN には特殊なプロパティがあるので、RSPAN VLAN として使用する VLAN をネットワーク上にいくつか確保しておき、これらの VLAN にはアクセスポートを割り当てないでください。
- RSPAN トラフィックに出力 ACL を適用して、特定の packets を選択してフィルタリングまたはモニタできます。これらの ACL は、RSPAN 送信元スイッチ内の RSPAN VLAN 上で指定します。
- RSPAN セッションは、「SPAN および RSPAN のセッション限度」(p.25-8) 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 の設定では、送信元ポートと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 リフレクタポートとして指定されているポートを、RSPAN 送信元ポートまたは RSPAN 宛先ポートにすることはできません。
- スイッチポートをリフレクタポートに設定すると、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のは、ループバックされたトラフィックだけです。
- RSPAN は BPDU パケット モニタリング、その他のレイヤ 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 に発生するのを防ぐため、参加しているすべてのスイッチで VLAN リモート SPAN 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 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組み込まれます。また、RSPAN VLAN を SPAN セッションの送信元にすることもできます。
- 任意の VLAN を RSPAN VLAN として設定するには、次の条件を満たす必要があります。
  - RSPAN VLAN に、アクセスポートが設定されていない。
  - 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が RSPAN をサポートしている。



**(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 VLAN および FDDI VLAN 専用) に設定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する必要があります。
- VTP および VTP プルーニングがイネーブルの場合、RSPAN トラフィックはトランクでプルーニングされ、ネットワーク上で VLAN ID が 1005 より小さい RSPAN トラフィックの不要なフラディングを防止できます。
- 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消失します。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のみをサポートします。

## RSPAN VLAN としての VLAN 設定

最初に、RSPAN セッション用の RSPAN VLAN にする 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 以下) 内で、ネットワークの VTP がイネーブルの場合、1 つのスイッチに RSPAN VLAN を作成して、それを VTP ドメイン内の他のスイッチに VTP から伝播させることができます。拡張範囲 VLAN (1006 以上) では、送信元と宛先スイッチの両方、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 トラフィックのフローを効率化するか、または RSPAN トラフィックを伝送する必要のないすべてのトランクから、RSPAN VLAN を手動で削除してください。

RSPAN VLAN を作成するには、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vlan vlan-id</code>	VLAN ID を入力して VLAN を作成し、VLAN コンフィギュレーション モードを開始します。または、既存の 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。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 VLAN および FDDI VLAN 専用) に設定することはできません。
ステップ 3	<code>remote-span</code>	RSPAN VLAN として VLAN を設定します。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(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 の特性を削除して標準の VLAN に戻すには、`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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session { <i>session_number</i>   all   local   remote }</code>	既存の RSPAN セッション設定をクリアします。  <i>session_number</i> 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には <code>all</code> を、すべてのローカル セッションを削除するには <code>local</code> を、すべてのリモート SPAN セッションを削除するには <code>remote</code> を指定します。
ステップ 3	<code>monitor session <i>session_number</i> source interface <i>interface-id</i> [,   -] [both   rx   tx]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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とポートチャネル論理インターフェイス ( <code>port-channel <i>port-channel-number</i></code> ) があります。  (任意) [,   -] 一連のまたは一定範囲のインターフェイスを指定します。カンマおよびハイフンの前後にはスペースを 1 つ入れます。  (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い場合、送信元インターフェイスは、送受信両方のトラフィックを送信します。追加の送信元ポートでは、受信 (rx) トラフィックのみをモニタできます。  <ul style="list-style-type: none"> <li>• <code>both</code> 送受信両方のトラフィックを送信します。</li> <li>• <code>rx</code> 受信トラフィックをモニタします。</li> <li>• <code>tx</code> 送信トラフィックをモニタします。</li> </ul>
ステップ 4	<code>monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i> reflector-port <i>interface</i></code>	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。  <i>session_number</i> には、1 または 2 を入力します。  <i>vlan-id</i> には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。(RSPAN VLAN の作成方法については、「イーサネット VLAN の作成または変更」[p.11-9] を参照)。  <i>interface</i> 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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show monitor [session <i>session_number</i>]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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ーするように 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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>monitor session session_number source remote vlan vlan-id</code>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。  <i>session_number</i> には、1 または 2 を指定します。  <i>vlan-id</i> には、モニターする送信元 RSPAN VLAN を指定します。
ステップ 3	<code>monitor session session_number destination interface interface-id [encapsulation {dot1q   isl}]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> には、宛先インターフェイスを指定します。  (任意) 送信パケット用カプセル化ヘッダーを指定します。指定しない場合、パケットはネイティブ フォームで送信されません。  <ul style="list-style-type: none"> <li><code>isl</code> ISL カプセル化を使用します。</li> <li><code>dot1q</code> IEEE 802.1Q カプセル化を使用します。</li> </ul>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show monitor [session session_number]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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と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て送信元 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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>monitor session session_number source remote vlan vlan-id</code>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。  <i>session_number</i> には、1 または 2 を指定します。  <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 3	<code>monitor session session_number destination interface interface-id [encapsulation {dot1q [ingress vlan vlan id]   ISL [ingress]}   ingress vlan vlan id]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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定義されていない場合、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。  <ul style="list-style-type: none"> <li>タグなしのネイティブ VLAN パケットと、ほかのすべての <code>dot1q</code> タグ付き VLAN tx パケットを送信する場合は、<code>encapsulation dot1q</code> を入力します。</li> <li>ISL を使っ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、<code>encapsulation isl</code> を入力します。</li> </ul> (任意) SPAN 宛先ポートで入力トラフィックに対して転送をイネーブルにするか否かを指定します。  <ul style="list-style-type: none"> <li>ネイティブ (タグなし) および <code>dot1q</code> カプセル化の場合、<code>ingress vlan vlan id</code> を指定し、<i>vlan id</i> 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 <i>vlan id</i> 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。</li> <li>ISL カプセル化を使用する場合、<code>ingress</code> を指定して入力転送をイネーブルにします。</li> </ul>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show monitor [session session_number]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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、IEEE 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 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、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session <i>session_number</i> source interface <i>interface-id</i> [,   -] [<i>both</i>   <i>rx</i>   <i>tx</i>]</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> 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とポートチャネル論理インターフェイス ( <code>port-channel <i>port-channel-number</i></code> ) があります。  (任意) [,   -] 一連のまたは一定範囲のインターフェイスを指定します (設定済みの場合)。カンマおよびハイフンの前後にはスペースを 1 つ入れます。  (任意) モニタを中止するトラフィックの方向 ( <code>both</code> 、 <code>rx</code> 、 <code>tx</code> ) を指定します。トラフィックの方向を指定しない場合、送受信両方のトラフィックがディセーブルになります。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show monitor [<i>session session_number</i>]</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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、双方向モニタ用に設定された、ポート 1 での受信トラフィック 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 での受信トラフィックのモニタはディセーブルになっていますが、このポートから送信されたトラフィックは引き続きモニタされます。

## モニタする VLAN の指定

VLAN のモニタは、ポートのモニタと似ています。モニタする VLAN を指定するには、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {<i>session_number</i>   all   local   remote}</code>	セッションの既存の SPAN 設定をクリアします。  <i>session_number</i> 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には <code>all</code> を、すべてのローカル セッションを削除するには <code>local</code> を、すべてのリモート SPAN セッションを削除するには <code>remote</code> を指定します。
ステップ 3	<code>monitor session <i>session_number</i> source vlan <i>vlan-id</i> [,   -] rx</code>	RSPAN セッションおよび送信元 VLAN (モニタ対象 VLAN) を指定します。モニタできるのは、VLAN 上の受信 (rx) トラフィックだけです。  <i>session_number</i> には、1 または 2 を指定します。  <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。先頭に 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 (-) を使用して一定範囲の VLAN を指定します。カンマおよびハイフンの前後にはスペースを 1 つ入れます。
ステップ 4	<code>monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i> reflector port <i>interface</i></code>	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。  <i>session_number</i> には、1 または 2 を入力します。  <i>vlan-id</i> には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。  <i>interface</i> 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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show monitor [session <i>session_number</i>]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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 に既存の設定があればクリアし、VLAN 1 ~ 3 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するように 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。この例ではさらに、その設定を変更して、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するようにしています。

```
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

特定の VLAN に対する RSPAN 送信元トラフィックを制限するには、イネーブル 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {<i>session_number</i>   all   local   remote}</code>	セッションの既存の SPAN 設定をクリアします。  <i>session_number</i> 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には <code>all</code> を、すべてのローカル セッションを削除するには <code>local</code> を、すべてのリモート SPAN セッションを削除するには <code>remote</code> を指定します。
ステップ 3	<code>monitor session <i>session_number</i> source interface <i>interface-id</i> rx</code>	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。  <i>session_number</i> には、1 または 2 を指定します。  <i>interface-id</i> には、モニタ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が、トランクポートとして設定されている必要があります。
ステップ 4	<code>monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]</code>	特定の VLAN に対する RSPAN 送信元トラフィックを制限します。  <i>session_number</i> には、1 または 2 を指定します。  <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。先頭に 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 (-) を使用して一定範囲の VLAN を指定します。カンマおよびハイフンの前後にはスペースを 1 つ入れます。
ステップ 5	<code>monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i> reflector port <i>interface</i></code>	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。  <i>session_number</i> には、1 または 2 を入力します。  <i>vlan-id</i> には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。  <i>interface</i> には、RSPAN トラフィックを RSPAN VLAN にフラッシュするインターフェイスを指定します。
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show monitor [session <i>session_number</i>]</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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 に既存の設定があればクリアし、トランク ポート 4 の受信したトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ~ 5 および VLAN 9 のトラフィックのみを、リフレクタポートとしてポート 8 を使用した宛先リモート 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 ステータスの表示

現在の SPAN または RSPAN 設定を表示するには、`show monitor` イネーブル EXEC コマンドを使用します。

次の例は、SPAN 送信元セッション 1 を示す `show monitor` イネーブル EXEC コマンドの出力です。

```
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
```