スイッチド ポート アナライザ

スイッチドポートアナライザ（SPAN）は、ネットワークトラフィックをモニタリング、分析、および障害対応するための強力なツールをネットワーク管理者に提供するシスコスイッチの機能です。この機能は、ライブ業務を中断することなく、データフローの優れた可視性を提供することで、ネットワークの正常性を維持し、セキュリティを確保し、パフォーマンスを最適化するのに不可欠です。

SPAN の概要

スイッチドポートアナライザ（SPAN）を使用すると、ネットワーク管理者は、トラフィックのコピーをデバイス上の別のポートに送信することにより、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分析できます。この宛て先ポートは、通常、ネットワークアナライザ、その他のモニタリングまたはセキュリティデバイスに接続されています。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指定された宛て先ポートにコピー（ミラーリング）して、解析します。SPAN の主な利点は、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通常のスイッチングには影響しません。

SPAN の仕組み

SPAN は、指定されたネットワークの場所から専用のモニタリングポートにトラフィックをミラーリングすることで動作します。次の段階では、SPAN の動作を説明します。

1. 送信元の特定：ネットワーク管理者は、トラフィックをミラーリングするための 1 つ以上の送信元ポートまたはVLANを設定します。これらの送信元には、スイッチに着信するトラフィック（入力）、スイッチから発信されるトラフィック（出力）、またはその両方を含めることができます。

（注） 送信元ポートに出入りするトラフィックや、送信元 VLAN に出入りするトラフィックが監視されます。送信元 VLAN にルーティングされるトラフィックはモニターできません。たとえば、着信トラフィックをモニターしている場合、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ーできません。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、モニターできます。

2. 接続先を指定：管理者は、スイッチで単一の宛て先ポートを指定します。ネットワークアナライザや侵入検知システムなどのモニタリングデバイスがこの宛て先ポートに接続します。

（注） 宛先ポートは SPAN 専用にする必要があります。SPAN セッションに必要なトラフィック以外、宛て先ポートが他のネットワーク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。

3. トラフィックミラーリング：スイッチは、設定済みの送信元ポートまたはVLANを通過するすべてのトラフィックを複製します。その後、これらの重複したパケットを指定された宛て先ポートに送信します。元のトラフィックは中断なしで意図したパスを継続します。
4. 分析とアクティブな使用：宛て先ポートに接続されているモニタリングデバイスは、ミラー済みトラフィックをキャプチャして分析します。これにより、ネットワークの動作、アプリケーションのパフォーマンス、および潜在的なセキュリティ脅威に関するインサイトが得られます。
5. トラフィック注入：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 宛て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 の概念および用語

ローカル SPAN

ローカル SPAN は 1 つのデバイス内の 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、同じデバイスまたはデバイス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。

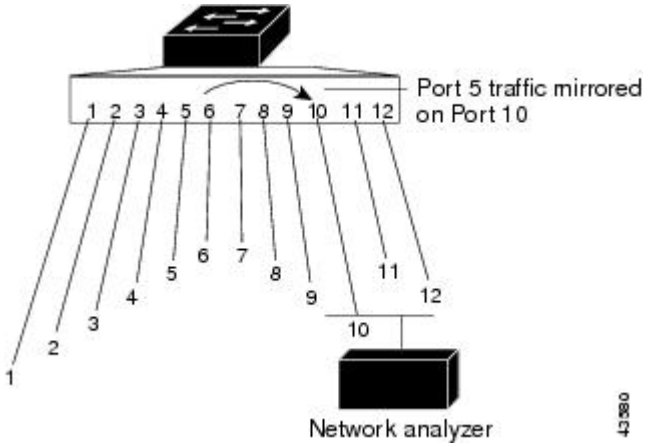
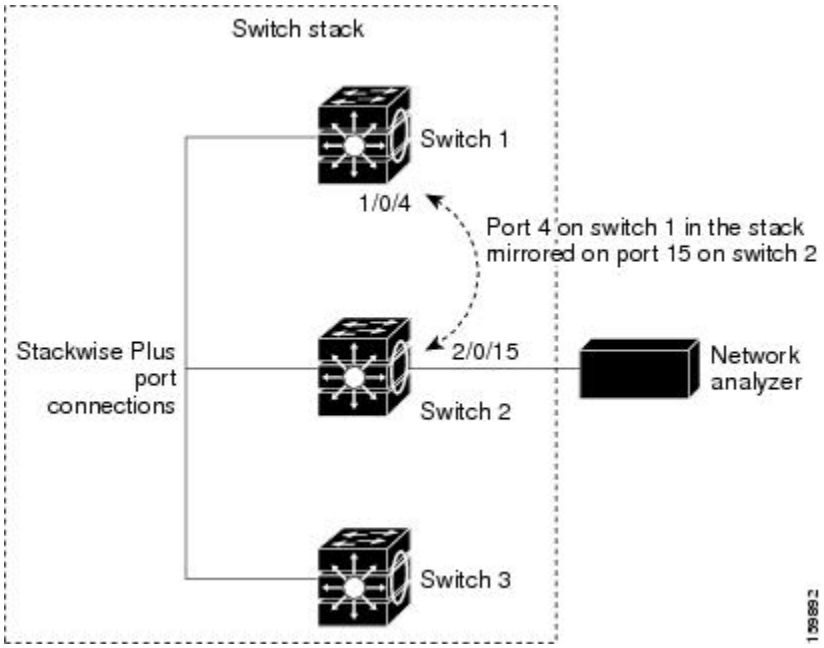


図 *1 :* 単一デバイスでのローカル *SPAN* の設定例

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 *2:* デバイス スタックでのローカル *SPAN* の設定例



SPAN セッション

SPAN セッションを使用すると、1 つまたは複数のポート上または VLAN 上でトラフィックをモニターし、そのモニターしたトラフィックを 1 つまたは複数の宛て先ポートに送信できます。ローカル SPAN セッションは、宛て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設定されている）を結び付けたものです。これらのセッションでは、指定された入力および出力パケットが収集され、宛て先ポートに誘導される SPAN データのストリームに形成されます。SPAN セッションの主な特性は次のとおりです。

- 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 セッションがデバイスの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをトラフィック監視するなど、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 が有効な場合、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）。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。
- 無効にされたポートで SPAN セッションを設定できます。ただし、SPAN セッションは、そのセッションの宛て先ポートと、少なくとも1つの送信元ポートまたは VLAN が有効になっている場合にのみアクティブになります。

モニター対象トラフィック

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。

- 受信（Rx）SPAN：受信（または入力）SPANは、デバイス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だけ多くモニタリングします。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。
  - Diffserv コード ポイント（DSCP）の変更など、ルーティングや Quality of Service（QoS）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 入力アクセス コントロール リスト（ACL）、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。
- 送信（Tx）SPAN：送信（または出力）SPAN は、デバイス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限り多くモニタリングします。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（存続可能時間（TTL）、MAC 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 をモニタすることもできます。これはデフォルトです。

デフォルトでは、ローカル SPAN セッションはカプセル化とともに送信元パケットを複製します。

- 送信元ポートと同じカプセル化設定（タグなし、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モニタされます。

したがって、ローカル SPAN セッションでは、タグなし、および IEEE 802.1Q タグ付きパケットが宛て先ポートに混在することがあります。

デバイスの輻輳により、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モニタ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。

- デバイス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、ポート A での RX モニター用とポート B での TX モニター用に双方向（RX と TX）SPAN セッションが設定されているとします。パケットがポート A からデバイスに入ってポート 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。

送信元ポート

送信元ポート（別名モニター側ポート）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モニターできます。

デバイスは、任意の数の送信元ポート（デバイスで使用可能なポートの最大数まで）および最大 1500 の送信元 VLAN 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。

- モニターする方向（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、トラフィックをモニターできます。
- 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。
- 宛先ポートにすることはできません。
- 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モニター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 トラフィックをモニターできます。VSPAN 内の SPAN 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モニターされます。

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モニターできます。

- 指定されたポートでは、モニター対象の 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、モニターされません。
- 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、モニター中の送信元に追加または削除されます。
- モニターできるのは、イーサネット VLAN だけです。
- セッションあたりの送信元 VLAN の数は 1,500 以下である必要があります。この制限は、受信（RX）および送信（TX）方向の合計です。

宛先ポート

各ローカル SPAN 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 パケットをユーザー（通常はネットワーク アナライザ）に送信する宛て先ポート（別名モニター側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- SPAN セッションには、セッションごとに 1 つの宛先ポートを設定できます。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）。
- 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デバイスまたはデバイススタックに存在している必要があります。
- 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。セキュアポートまたは送信元ポートにす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。
- 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、モニターされません。
- デバイスまたはデバイススタックの宛先ポートの最大数は 64 です。

ローカル SPAN の場合、宛て先ポートでの送信元パケットはデフォルトで元のカプセル化（タグなし、ISL、または IEEE802.1Q）で表示されます。したがって、ローカル SPAN セッションの出力に、タグなし、ISL、または IEEE802.1Q タグ付きパケットが混在することがあります。

SPAN 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 が監視するのはデバイス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 が受信モニターされ、デバイスが別の 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 セッションがアクティブな間、宛て先ポートは STP に参加しません。SPAN セッションが無効になると、宛て先ポートは 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。
- 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。
- 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できます。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することはできません。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監視では、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 ポートは、SPAN 宛先ポートには設定できません。
- 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。
- 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 を有効にできますが、SPAN宛先としてこのポートを削除するまで、IEEE 802.1x は無効に設定されます。

SPAN とデバイススタック

スイッチのスタックは 1 つの論理スイッチを表すため、ローカル SPAN の送信元ポートおよび宛先ポートは、スタック内の異なるスイッチである場合があります。したがって、スタック内でのスイッチの追加または削除は、ローカル SPAN セッションに影響を及ぼします。スイッチがスタックから削除されると、アクティブ セッションが非アクティブになります。また、スイッチがスタックに追加されると、非アクティブ セッションがアクティブになります。

SPAN の制約事項

SPAN セッションを設定する場合は、次の制限事項に従ってください。

- デバイスは、指定された送信元ポートまたは VLAN からのトラフィックをモニターおよびキャプチャするための送信元セッションとして指定された最大 8 セッションを含む、最大 66 モニタリングセッションをサポートします。
- 同じ SPAN セッション内に送信元ポートと送信元 VLAN を混在させないでください。
- 宛て先ポートを SPAN セッション内の送信元ポートにすることはできません。
- SPAN セッションには複数の宛て先ポートを設定できますが、デバイススタックは最大 64 個の宛て先ポートをサポートします。
- 10 Mbps のポートで 100 Mbps のポートをトラフィック監視するなど、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 送信元ポートまたは送信元 VLAN を複数の SPAN セッションの一部にすることはできません。
- SPAN セッションには 1 つの宛て先ポートしか設定できず、一意の宛て先ポートを使用する必要があります。
- EtherChannel グループを SPAN 宛て先ポートにすることはできません。
- EtherChannel メンバーを SPAN 送信元ポートにすることはできません。

SPAN の設定方法

SPAN は、指定されたネットワークの場所から専用のモニタリングポートにトラフィックをミラーリングすることで動作します。次の段階では、SPAN の動作を説明します。

1. 送信元の特定：ネットワーク管理者は、トラフィックをミラーリングするための 1 つ以上の送信元ポートまたはVLANを設定します。これらの送信元には、スイッチに着信するトラフィック（入力）、スイッチから発信されるトラフィック（出力）、またはその両方を含めることができます。

   送信元ポートに出入りするトラフィックや、送信元VLANに出入りするトラフィックが監視されます。送信元VLANにルーティングされるトラフィックはモニターできません。たとえば、着信トラフィックをモニターしている場合、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ーできません。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、モニターできます。

2. 接続先を指定：管理者は、スイッチで単一の宛て先ポートを指定します。ネットワークアナライザや侵入検知システムなどのモニタリングデバイスがこの宛て先ポートに接続します。

   宛先ポートは SPAN 専用にする必要があります。SPAN セッションに必要なトラフィック以外、宛て先ポートが他のネットワーク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。

3. トラフィックミラーリング：スイッチは、設定済みの送信元ポートまたはVLANを通過するすべてのトラフィックを複製します。その後、これらの重複したパケットを指定された宛て先ポートに送信します。元のトラフィックは中断なしで意図したパスを継続します。

4. 分析とアクティブな使用：宛て先ポートに接続されているモニタリングデバイスは、ミラー済みトラフィックをキャプチャして分析します。これにより、ネットワークの動作、アプリケーションのパフォーマンス、および潜在的なセキュリティ脅威に関するインサイトが得られます。

   トラフィック注入：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 宛て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。

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（監視側）ポートを指定するには、次の手順を実行します。

手順

ステップ 1 有効

例：

```
Device# configure terminal
```

特権 EXEC モードを有効にします。

ステップ 2 configure terminal

例：

```
Device# configure terminal
```

グローバル設定モードを開始します。

ステップ 3 **no monitor session** {*session_number* | **all** | **local** | **remote**}

例：

```
Device(config)# no monitor session all
```

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。
- **all**：すべての SPAN セッションを削除します。
- **local**：すべてのローカルセッションを削除します。
- **remote**：すべてのリモート SPAN セッションを削除します。

ステップ 4 **monitor session** session_number **source** {**interface** interface-id | **vlan** vlan-id} [**,** | **-**] [**both** | **rx** | **tx**]

例：

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
```

SPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。

- **session_number** の範囲は、1 ～ 66 です。
- interface-id には、モニタリング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。

（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の範囲を指定します。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）**both|rx|tx**：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：受信トラフィックと送信トラフィックの両方をモニターします。
  - rx：受信トラフィックをモニターします。
  - tx：送信トラフィックをモニターします。

（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。

ステップ 5 **monitor session** session_number **destination** {**interface** interface-id **[,** | **-]**

例：

```
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

SPAN セッションおよび宛先ポート（モニター側ポート）を指定します。設定変更が有効になると、ポートの LED がオレンジ色に変わります。LED は SPAN 宛先の設定を削除した後にのみ、元の状態（緑色）に戻ります。

- 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。
- **session_number** には、ステップ 4 で入力したセッション番号を指定します。
- **interface-id** には、宛て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の範囲を指定します。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 6 end

例：

```
Device(config)# end
```

特権 EXEC モードに戻ります。

ステップ 7 show running-config

例：

```
Device# show running-config
```

入力を確認します。

ステップ 8 copy running-config startup-config

例：

```
Device# 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 のコンフィギュレーション例

次のセクションに SPAN の設定例を示します。

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モニタする例を示します。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 にミラーリングします。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
Device(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。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet1/0/1
Device(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。

```
Device> enable
Device# configure terminal
Device(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。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に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、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source vlan 1 - 3 rx

Device(config)# monitor session 2 destination interface gigabitethernet1/0/2
Device(config)# monitor session 2 source vlan 10
Device(config)# end
```

次に、SPAN セッション 2 内の既存の設定を削除し、Gigabit Ethernet トランクポート 2 で受信トラフィックをモニターするように SPAN セッション 2 を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 2 destination interface gigabitethernet1/0/1
Device(config)# end
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。