



## マニュアル更新情報 : Catalyst 3560E-12D スイッチ

**【注意】** シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)) をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。  
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

2007年11月27日

この資料では、*集約スイッチ*と呼ばれる Catalyst 3560E -12D スイッチを設定する方法について説明します。Catalyst 3560E-12D スイッチ以外の Catalyst 3750-E スイッチおよび Catalyst 3560-E スイッチは、*デスクトップスイッチ*と呼ばれています。

この資料は、Catalyst 3750-E および 3560-E ソフトウェア マニュアルと併せてご利用ください（「[関連資料](#)」 [p.27] を参照）。

ここで説明する内容は、次のとおりです。

- [ソフトウェア コンフィギュレーション ガイド](#)、「[SPAN および RSPAN の設定](#)」の章の更新 (p.2)
- [ソフトウェア コンフィギュレーション ガイド](#)への「[ファン障害](#)」の追加 (p.17)
- [コマンド リファレンス](#)の `monitor session` コマンドに関する更新情報 (p.18)
- [コマンド リファレンス](#)の `show monitor session` コマンドに関する更新情報 (p.23)
- [コマンド リファレンス](#)への `system env fan-fail-action shut` コマンドの追加 (p.26)
- [関連資料](#) (p.27)
- [マニュアルの入手方法](#)、[テクニカル サポート](#)、および[セキュリティ ガイドライン](#) (p.28)

## ソフトウェア コンフィギュレーション ガイド、「SPAN および RSPAN の設定」の章の更新

ここでは、Catalyst 3560E-12D スイッチを**集約スイッチ**と呼び、Catalyst 3560E-12D スイッチ以外の Catalyst 3750-E スイッチと Catalyst 3560-E スイッチを**デスクトップスイッチ**と呼びます。

次の情報が変更または追加されました。

- 「SPAN と RSPAN の概念および用語」の更新 (p.2)
- 「送信元ポート」の更新 (p.3)
- 「宛先ポート グループ」の追加 (p.3)
- 「ローカル SPAN の設定」の更新 (p.3)
- 「RSPAN の設定」の更新 (p.10)

### 「SPAN と RSPAN の概念および用語」の更新

「SPAN セッション」における更新：

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。
- スイッチ (Catalyst 3560E-12D スイッチ以外) は最大 2 つのローカル SPAN 送信元セッションまたは 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 送信元セッションと RSPAN 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 の送信元セッションおよび RSPAN 宛先セッションをサポートします。
  - 個別の、または重複する SPAN 送信元ポートと VLAN のセットを使用して、2 つの個別の SPAN または RSPAN 送信元セッションを設定できます。スイッチド ポートとルーテッド ポートはどちらも、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 (ローカル SPAN または RSPAN 送信元セッションのどちらか) のみをサポートし、これがセッション 1 になります。スイッチド ポートとルーテッド 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 スタックに設定可能な宛先ポートは最大で 64 です。
- SPAN セッションがスイッチの通常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 のポートを監視するなど、オーバーサブスクライブの SPAN 宛先は、結果としてパケットの廃棄や消失を招くことがあります。
- ローカル 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 回は監視対象パケットとして)。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に SPAN セッションを設定することはできませんが、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することはできません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定することはできません。
  - 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 宛先セッションと RSPAN 送信元セッションを実行することはできません。

## 「送信元ポート」の更新

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最大ポート数まで）と任意の数の送信元 VLAN（サポートされている最大 VLAN 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）までで、Catalyst 3560E-12D が送信元ポートまたは VLAN でサポートするセッション（ローカルまたは RSPAN）は 1 つだけです。したがって、単一のセッションにポートと 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。

- 1つの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 スイッチ上では、1つの SPAN セッションでのみ送信元ポートを監視できます。
- 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、GigabitEthernet 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。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN に属していても、異なる VLAN に属していてもかまいません。
- 単一セッション内で複数の送信元ポートを監視できます。

## 「宛先ポートグループ」の追加

「宛先ポートグループ」は「宛先ポート」の後に追加されます。



(注)

ここでの説明は、Catalyst 3560E-12D スイッチのみに適用されます。

Catalyst 3560E-12D スイッチは、同じ *宛先ポートグループ* に属する宛先ポートのみを經由して SPAN および RSPAN トラフィックを送信します。RSPAN 宛先セッションを設定する場合は、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.4）を参照してください。

宛先ポートが 1 つのみのローカル 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。2 番目の宛先ポートをセッションに追加する場合、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所属させる必要があります。

## 「ローカル SPAN の設定」の更新

ここでは、次の設定情報について説明します。

- [SPAN 設定時の注意事項](#)（p.4）
- [ローカル SPAN セッションの作成](#)（p.5）
- [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](#)（p.7）
- [フィルタリングする VLAN の指定](#)（p.9）



## SPAN 設定時の注意事項



SPAN を設定するときには、次の注意事項に従ってください。

- スイッチ スタックごとに、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、送信元ポートと送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。
- 同じ宛先ポートを使用する 2 つの SPAN セッションを設定することはできません。
- 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、監視対象トラフィックのみが SPAN 宛先ポートを経由するようになります。
- SPAN コンフィギュレーション コマンドを入力しても、以前に設定した SPAN パラメータは削除されません。設定済みの 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）を搬送します。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を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 ポートを監視する場合に、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。
- Catalyst 3560E-12D スイッチでは、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。指定するには、セッション タイプに応じて、**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 コマンドを入力します。
- Catalyst 3560E-12D スイッチは、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	<code>configure terminal</code>	グローバル コンフィギュレーション モードに切り替えます。
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 設定を削除します。  <i>session_number</i> 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 <b>all</b> 、すべてのローカル セッションを削除する場合は <b>local</b> 、すべてのリモート SPAN セッションを削除する場合は <b>remote</b> をそれぞれ指定します。
ステップ 3	<code>monitor session session_number source {interface interface-id   vlan vlan-id} [, -] [both   rx   tx]</code>	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。  <i>session_number</i> 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、 <i>session_number</i> に入力できる値は <b>1</b> だけです。  <i>interface-id</i> 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。  <ul style="list-style-type: none"> <li>送信元 <i>interface-id</i> 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。有効なポートチャネル番号は 1 ～ 48 です。</li> <li><i>vlan-id</i> 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 を除く）。</li> </ul> <p> <b>(注)</b> 単一のセッションに、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 つのセッションで送信元ポートと送信元 VLAN を併用することはできません。</p> <p>(任意) [, -] 一連のインターフェイス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。</p> <p>(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。</p> <ul style="list-style-type: none"> <li><b>both</b> — 受信トラフィックと送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。</li> <li><b>rx</b> — 受信トラフィックを監視します。</li> <li><b>tx</b> — 送信トラフィックを監視します。</li> </ul> <p> <b>(注)</b> <code>monitor session session_number source</code> 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。</p>

	コマンド	目的
ステップ 4	<b>monitor session</b> <i>session_number</i> <b>destination</b> { <b>interface</b> <i>interface-id</i> [, -] [encapsulation replicate]}	<p>SPAN セッション、宛先ポート（モニタ側ポート）、および複数のポートを指定する場合は宛先ポート グループを指定します。</p> <p><i>session_number</i> 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。</p> <p> (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。</p> <p><i>interface-id</i> 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。</p> <p>(任意) [, -] 一連のインターフェイス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。</p> <p>(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、<b>encapsulation replicate</b> 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。</p> <p> (注) <b>monitor session session_number destination</b> 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。宛先ポートはすべて、同じ宛先ポート グループに属している必要があります。</p>
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show monitor</b> [session <i>session_number</i> ]  <b>show running-config</b>	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。

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。

次の例は、SPAN セッション 1 を設定し、宛先ポートへの送信元ポート トラフィックを監視する方法を示しています。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
```

次の例は、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する方法を示しています。

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

次の例は、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方法を示しています。

```
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。

次の例では、SPAN セッション 2 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監視するように SPAN セッション 2 を設定し、監視されたトラフィックを宛先ポート GigabitEthernet 2 に送信します。さらに、この設定を 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監視するように変更しています。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface 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てから、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 アプライアンスなど) 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.5) を参照してください。

	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 モードに切り替えます。
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 設定を削除します。
ステップ 3	<code>monitor session session_number source {interface interface-id   vlan vlan-id} [, -] [both   rx   tx]</code>	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	<b>monitor session</b> <i>session_number</i> <b>destination</b> { <b>interface</b> <i>interface-id</i> [, -] [ <b>encapsulation replicate</b> ] [ <b>ingress</b> { <b>dot1q</b> <b>vlan</b> <i>vlan-id</i>   <b>isl</b>   <b>untagged vlan</b> <i>vlan-id</i>   <b>vlan</b> <i>vlan-id</i> }]                 }	<p>SPAN セッション、宛先ポート、パケット カプセル化、入力 VLAN とカプセル化、および複数のポートが指定される場合には、宛先ポート グループを指定します。</p> <p><i>session_number</i> 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、<i>session_number</i> に入力できる値は 1 だけです。</p> <p><i>interface-id</i> 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。</p> <p>(任意) [, -] 一連のインターフェイスまたは一定範囲のインターフェイスを指定します。カンマまたはハイフンの前後に 1 つずつスペースを入力します。</p> <p>(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、<b>encapsulation replicate</b> 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。</p> <p>(任意) 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、<b>ingress</b> と次のキーワードを一緒に入力します。</p> <ul style="list-style-type: none"> <li>• <b>dot1q vlan</b> <i>vlan-id</i> — 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。</li> <li>• <b>isl</b> — ISL カプセル化を使用して着信パケットを転送します。</li> <li>• <b>untagged vlan</b> <i>vlan-id</i> または <b>vlan</b> <i>vlan-id</i> — 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。</li> </ul>
ステップ 5	<b>end</b>	特権 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> ]  <b>show running-config</b>	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。

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** オプションと **ingress** オプションは無視されます。



次の例では、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 で受信トラフィックを監視するように SPAN セッション 2 を設定しています。さらに、監視したトラフィックを送信元ポートと同じ出力カプセル化方式を使用して宛先ポート 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しています。

```
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トランク ポートおよび音声 VLAN ポート上の特定の VLAN のみに制限するには、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	<b>configure terminal</b>	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	セッションの既存の SPAN 設定を削除します。  <i>session_number</i> 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 <b>all</b> 、すべてのローカルセッションを削除する場合は <b>local</b> 、すべてのリモート SPAN セッションを削除する場合は <b>remote</b> をそれぞれ指定します。
ステップ 3	<b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i>	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。  <i>session_number</i> 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、 <i>session_number</i> に入力できる値は <b>1</b> だけです。  <i>interface-id</i> には、監視する送信元ポートを指定します。指定するインターフェイスは、事前にトランク 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	<b>monitor session</b> <i>session_number</i> <b>filter vlan</b> <i>vlan-id</i> [,   -]	SPAN 送信元トラフィックを特定の VLAN に制限します。  <i>session_number</i> 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。  <i>vlan-id</i> 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。

	コマンド	目的
ステップ 5	<b>monitor session</b> <i>session_number</i> <b>destination</b> { <b>interface</b> <i>interface-id</i> [, -] [ <b>encapsulation replicate</b> ]}	SPAN セッション、宛先ポート（モニタ側ポート）、および複数のポートを指定する場合は宛先ポートグループを指定します。  <i>session_number</i> 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。  <i>interface-id</i> 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一定範囲のインターフェイスを指定します。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、 <b>encapsulation replicate</b> 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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]  <b>show running-config</b>	設定を確認します。
ステップ 8	<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。

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。

次の例では、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 の受信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 VLAN 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信しています。

```
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」の更新

ここでは、「RSPAN の設定」以降の更新情報を説明します。

- [RSPAN 送信元セッションの作成 \(p.11\)](#)
- [フィルタリングする VLAN の指定 \(p.13\)](#)
- [RSPAN 宛先セッションの作成 \(p.14\)](#)
- [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 \(p.15\)](#)

## 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	<code>vlan vlan-id</code>	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 モードに切り替えます。  両方のスイッチが VTP に含まれ、RSPAN VLAN ID が 2 ~ 1005 の場合、RSPAN VLAN ID は VTP ネットワーク全体に伝播されるため、ステップ 2 ~ 4 は必要ありません。
ステップ 3	<code>remote-span</code>	VLAN を RSPAN VLAN として識別します。
ステップ 4	<code>no monitor session {session_number   all   local   remote}</code>	セッションの既存の RSPAN 設定を削除します。  <i>session_number</i> 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 <b>all</b> 、すべてのローカルセッションを削除する場合は <b>local</b> 、すべてのリモート SPAN セッションを削除する場合は <b>remote</b> をそれぞれ指定します。
ステップ 5	<code>monitor session session_number source {interface interface-id   vlan vlan-id} [, -] [both   rx   tx]</code>	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。  <i>session_number</i> 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、 <i>session_number</i> に入力できる値は 1 だけです。  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。  <ul style="list-style-type: none"> <li><i>interface-id</i> 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。有効なポートチャネル番号は 1 ~ 48 です。</li> <li><i>vlan-id</i> 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 を除く）。  単一のセッションに、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 つのセッションで送信元ポートと送信元 VLAN を併用することはできません。</li> </ul> (任意) [, -] 一連のインターフェイス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。  <ul style="list-style-type: none"> <li><b>both</b> — 受信トラフィックと送信トラフィックの両方を監視します。</li> <li><b>rx</b> — 受信トラフィックを監視します。</li> <li><b>tx</b> — 送信トラフィックを監視します。</li> </ul>

	コマンド	目的
ステップ 6	<p>Catalyst 3560E-12D スイッチ以外のスイッチ :</p> <pre>monitor session session_number destination remote vlan vlan-id</pre> <p>Catalyst 3560E0-12D スイッチ :</p> <pre>monitor session session_number destination remote vlan vlan-id destination-port group {a   b   c}</pre>	<p>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。</p> <p><i>session_number</i> には、ステップ 3 で定義した番号を入力します。</p> <p><i>vlan-id</i> には、監視する送信元 RSPAN VLAN を指定します。</p> <p>Catalyst 3560E-12D スイッチで、RSPAN トラフィックを伝送するポートを指定するには、<b>destination-port group {a   b   c}</b> を入力します。</p>
ステップ 7	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show monitor</b> [ <i>session session_number</i> ]	設定を確認します。
	<b>show running-config</b>	
ステップ 9	<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。

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** を使用します。

次の例では、セッション 1 の既存の 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 に設定しています。

```
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
```

次の例では、Catalyst 3560E-12D スイッチで、セッション 1 の既存の 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 に設定しています。

```
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	<b>configure terminal</b>	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	セッションの既存の RSPAN 設定を削除します。  <i>session_number</i> 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 <b>all</b> 、すべてのローカルセッションを削除する場合は <b>local</b> 、すべてのリモート SPAN セッションを削除する場合は <b>remote</b> をそれぞれ指定します。
ステップ 3	<b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i>	送信元ポート（監視対象ポート）と RSPAN セッションの特性を指定します。  <i>session_number</i> 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、 <i>session_number</i> に入力できる値は <b>1</b> だけです。  <i>interface-id</i> には、監視する送信元ポートを指定します。指定するインターフェイスは、事前にトランク 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	<b>monitor session</b> <i>session_number</i> <b>filter vlan</b> <i>vlan-id</i> [,   -]	RSPAN 送信元トラフィックを特定の VLAN に制限します。  <i>session_number</i> 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。  <i>vlan-id</i> 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：  <b>monitor session</b> <i>session_number</i> <b>destination remote vlan</b> <i>vlan-id</i>  Catalyst 3560E0-12D スイッチ：  <b>monitor session</b> <i>session_number</i> <b>destination remote vlan</b> <i>vlan-id</i> <b>destination-port group</b> { <b>a</b>   <b>b</b>   <b>c</b> }	RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。  <i>session_number</i> 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。  <i>vlan-id</i> 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 スイッチで、RSPAN トラフィックを伝送するポートを指定するには、 <b>destination-port group</b> { <b>a</b>   <b>b</b>   <b>c</b> } を入力します。
ステップ 6	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show monitor</b> [ <b>session</b> <i>session_number</i> ]  <b>show running-config</b>	設定を確認します。
ステップ 8	<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。

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。

次の例では、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 の受信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 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信しています。

```
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
```

次の例では、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 の受信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 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信しています。

```
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て、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	<code>configure terminal</code>	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	<code>vlan vlan-id</code>	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 モードに切り替えます。  両方のスイッチが VTP に含まれ、RSPAN VLAN ID が 2 ～ 1005 の場合、RSPAN VLAN ID は VTP ネットワーク全体に伝播されるため、ステップ 2 ～ 4 は必要ありません。
ステップ 3	<code>remote-span</code>	VLAN を RSPAN VLAN として識別します。
ステップ 4	<code>exit</code>	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	<code>no monitor session {session_number   all   local   remote}</code>	セッションの既存の RSPAN 設定を削除します。  <code>session_number</code> 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 <b>all</b> 、すべてのローカルセッションを削除する場合は <b>local</b> 、すべてのリモート SPAN セッションを削除する場合は <b>remote</b> をそれぞれ指定します。
ステップ 6	<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。  <code>session_number</code> 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、 <code>session_number</code> に入力できる値は 1 だけです。  <code>vlan-id</code> 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	<b>monitor session</b> <i>session_number</i> <b>destination interface</b> <i>interface-id</i>	RSPAN セッション、宛先インターフェイス、および宛先ポートグループを指定します。  <i>session_number</i> には、ステップ 6 で定義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。  <i>interface-id</i> 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ある必要があります。  <b>encapsulation replicate</b> は、コマンドラインのヘルプ文字列に表示されますが、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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 9	<b>show monitor</b> [ <i>session session_number</i> ]  <b>show running-config</b>	設定を確認します。
ステップ 10	<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。

RSPAN 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。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。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* を使用します。

次の例では、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 を設定する方法を示しています。

```
Switch(config)# monitor session 3 source remote vlan 901
Switch(config)# monitor session 3 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、さらに送信元 RSPAN VLAN および宛先ポートを指定したのち、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 アプライアンスなど) 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 \(p.14\)](#)」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	<b>configure terminal</b>	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	セッションの既存の SPAN 設定を削除します。
ステップ 3	<b>monitor session</b> <i>session_number</i> <b>source remote vlan</b> <i>vlan-id</i>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。  <i>session_number</i> 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、 <i>session_number</i> に入力できる値は <b>1</b> だけです。  <i>vlan-id</i> 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	<b>monitor session</b> <i>session_number</i> <b>destination</b> { <b>interface</b> <i>interface-id</i> [, -] <b>[ingress</b> { <b>dot1q</b> <i>vlan</i> <i>vlan-id</i>   <b>isl</b>   <b>untagged</b> <i>vlan</i> <i>vlan-id</i>   <b>vlan</b> <i>vlan-id</i> }}	<p>SPAN セッション、宛先ポート、パケット カプセル化、着信 VLAN とカプセル化、および宛先ポート グループを指定します。</p> <p><i>session_number</i> には、ステップ 4 で定義した番号を入力します。</p> <p>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。</p> <p><i>interface-id</i> 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ある必要があります。</p> <p><b>encapsulation replicate</b> は、コマンドラインのヘルプ文字列に表示されますが、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。</p> <p>(任意) [, -] 一連のインターフェイス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。</p> <p>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、<b>ingress</b> と次のキーワードを一緒に入力します。</p> <ul style="list-style-type: none"> <li>• <b>dot1q</b> <i>vlan</i> <i>vlan-id</i> — 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転送します。</li> <li>• <b>isl</b> — ISL カプセル化を使用して着信パケットを転送します。</li> <li>• <b>untagged</b> <i>vlan</i> <i>vlan-id</i> または <b>vlan</b> <i>vlan-id</i> — 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転送します。</li> </ul>
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show monitor</b> [ <i>session session_number</i> ]  <b>show running-config</b>	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。

RSPAN 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。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、**ingress** オプションは無視されます。

次の例では、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て、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しています。

```
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
```



## ソフトウェア コンフィギュレーション ガイドへの「ファン障害」の追加

この情報は、『*Catalyst 3750-E and 3560-E Switch Software Configuration Guide*』の「Troubleshooting」の章に追加されます。

### ファンの障害

Catalyst 3560E-12D スイッチでのみ、ファン障害機能がサポートされています。この機能を使用して、スイッチが過熱状態になるのを防ぐことができます。

デフォルトでは、この機能はディセーブルです。FRU（現場で交換可能なユニット）または電源モジュール内の 1 つ以上のファンが故障した場合、スイッチはシャットダウンせず、次のエラーメッセージが表示されます。

```
Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.
```

スイッチが過熱状態になり、シャットダウンする可能性があります。

ファン障害機能をイネーブルにするには、**system env fan-fail-action shut** 特権 EXEC コマンドを入力します。スイッチ内の 1 つ以上のファンが故障すると、スイッチは自動的にシャットダウンし、次のエラーメッセージが表示されます。

```
Faulty (FRU/PS) fans detected, shutting down system!
```

スイッチは、最初に障害を検出したファンをシャットダウンしたあと、2 番めのファン障害を検出すると、20 秒間待機してから、2 番めのファンをシャットダウンします。

スイッチを再起動するには、電源を入れ直す必要があります。

## コマンドリファレンスの monitor session コマンドに関する更新情報

### monitor session

新規の Switched Port Analyzer (SPAN; スイッチドポートアナライザ) セッションまたは Remote SPAN (RSPAN) 送信元/宛先セッションの開始、ネットワークセキュリティデバイス (Cisco IDS センサー アプライアンスなど) 用の宛先ポート上での入力トラフィックのイネーブル化、既存の SPAN または RSPAN セッションにおけるインターフェイスまたは VLAN の追加と削除、および SPAN 送信元トラフィックの特定 VLAN への制限を実行するには、スイッチ スタックまたはスタンドアロン スイッチ上で **monitor session** 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 または RSPAN セッションを削除したり、SPAN または RSPAN セッションからインターフェイスやフィルタを削除するには、このコマンドの **no** 形式を使用します。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。

すべての Catalyst 3750-E および 3560-E スイッチ :

```
monitor session session_number filter vlan vlan-id [, | -]
monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
no monitor session {session_number | all | local | remote}
no monitor session session_number filter vlan vlan-id [, | -]
no monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

Catalyst 3560E-12D スイッチ以外のスイッチ :

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id}]} | {remote vlan vlan-id}
no monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id}]} | {remote vlan vlan-id}
```

Catalyst 3560E-12D スイッチ :

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id}]} | {remote vlan vlan-id} destination-port group {a | b | c}
no monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | vlan vlan-id}]} | {remote vlan vlan-id} destination-port group {a | b | c}
```

#### シンタックスの説明

<i>session_number</i>	SPAN または RSPAN セッションで識別されるセッション番号を指定します。指定できる範囲は 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、 <i>session_number</i> に入力できる値は <b>1</b> だけです。
<b>destination</b>	SPAN または RSPAN の宛先を指定します。宛先は物理ポートである必要があります。
<b>interface interface-id</b>	SPAN または RSPAN セッションの宛先インターフェイスまたは送信元インターフェイスを指定します。有効なインターフェイスは物理ポート (タイプ、スタック メンバー、モジュール、ポート番号を含む) です。 <b>source interface</b> の場合は、 <b>port channel</b> も有効なインターフェイス タイプであり、指定できる値の範囲は 1 ~ 48 です。

<b>encapsulation replicate</b>	<p>(任意) 宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。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。</p> <p>これらのキーワードは、ローカル SPAN の場合のみ有効です。RSPAN の場合は、RSPAN VLAN ID が元の VLAN ID を上書きします。</p>
<b>ingress</b>	(任意) 入力トラフィックの転送をイネーブルにします。
<b>dot1q vlan vlan-id</b>	デフォルト VLAN として指定された VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受け入れます。
<b>isl</b>	ISL カプセル化を使用した入力転送を指定します。
<b>untagged vlan vlan-id</b>	デフォルト VLAN として指定された VLAN で、タグなしでカプセル化された着信パケットを受け入れます。
<b>vlan vlan-id</b>	<b>ingress</b> キーワードのみが使用されている場合は、入力トラフィック用のデフォルト VLAN を設定します。
<b>remote vlan vlan-id</b>	<p>RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は、2 ~ 1001 および 1006 ~ 4094 です。</p> <p>RSPAN VLAN として、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 用に予約済み) を指定することはできません。</p>
<b>,</b>	(任意) 一連のインターフェイスまたは VLAN を指定します。または、インターフェイスまたは VLAN の範囲を直前の範囲から分離します。カンマの前後に 1 つずつスペースを入力します。
<b>-</b>	(任意) インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後に 1 つずつスペースを入力します。
<b>filter vlan vlan-id</b>	トランク送信元ポートのフィルタとして VLAN のリストを指定し、SPAN 送信元トラフィックを特定の VLAN に制限します。vlan-id に指定できる範囲は、1 ~ 4094 です。
<b>source</b>	SPAN または RSPAN の送信元を指定します。送信元は、物理ポート、ポート チャネル、または VLAN のいずれかになります。
<b>both、rx、tx</b>	(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。
<b>source vlan vlan-id</b>	VLAN ID として SPAN 送信元インターフェイスを指定します。指定できる範囲は 1 ~ 4094 です。
<b>all、local、remote</b>	すべての SPAN および RSPAN セッション、すべてのローカル SPAN セッション、またはすべての RSPAN セッションを切断するには、それぞれ <b>all</b> 、 <b>local</b> 、または <b>remote</b> を <b>no monitor session</b> コマンドに指定します。
<b>destination-port group {a   b   c}</b>	<p>このオプションは、Catalyst 35600-E-12D 集約スイッチでのみサポートされます。</p> <p>RSPAN 送信元セッションを設定する場合は、宛先ポートが所属する宛先ポート グループを指定します。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>a</b> — tengigabitethernet 0/1 ~ tengigabitethernet 0/4 または gigabitethernet 0/1 ~ gigabitethernet 0/8</li> <li>• <b>b</b> — tengigabitethernet 0/5 ~ tengigabitethernet 0/8 または gigabitethernet 0/9 ~ gigabitethernet 0/16</li> <li>• <b>c</b> — tengigabitethernet 0/9 ~ tengigabitethernet 0/12 または gigabitethernet 0/17 ~ gigabitethernet 0/24</li> </ul>

## デフォルト

モニタセッションは設定されません。

送信元インターフェイスでは、デフォルトで、受信トラフィックと送信トラフィックの両方を監視します。

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では、すべての VLAN が監視されます。

ローカル SPAN 宛先ポートで **encapsulation replicate** が指定されていない場合、パケットはタグなしでカプセル化されたネイティブ形式で送信されます。

入力転送は、宛先ポートではディセーブルです。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更内容
12.2(35)SE2	このコマンドが追加されました。
12.2(40)EX	Catalyst 3560E-12D スイッチの場合のみ、 <b>destination-port group {a   b   c}</b> キーワードが追加されました。

## 使用上のガイドライン

送信元ポートまたは送信元 VLAN で入力または出力されるトラフィックは、SPAN または RSPAN を使用して監視できます。送信元ポートまたは送信元 VLAN にルーティングされたトラフィックは監視できません。

最大 2 つのローカル SPAN セッションと RSPAN セッションを組み合わせて設定できます。1 つのスイッチまたはスイッチスタック上では合計 66 の SPAN および RSPAN セッションを設定できます。

1 つのスイッチまたはスイッチスタックで最大 64 の宛先ポートを保持できます。

各セッションには複数の入力送信元ポート、出力送信元ポート、または VLAN を含めることができますが、単一のセッションで送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションには、複数の宛先ポートを含めることができます。

VLAN ベースの SPAN (VSPAN) を使用して単一または一連の VLAN 内のネットワークトラフィックを分析する場合は、送信元 VLAN 内のすべてのアクティブポートが SPAN または RSPAN セッションの送信元ポートになります。トランクポートは VSPAN の送信元ポートとして含まれ、監視対象の VLAN ID を持つパケットだけが宛先ポートに送信されます。

単一のポートまたは VLAN、一連のポートまたは VLAN、あるいは一定範囲のポートまたは VLAN 上のトラフィックを監視できます。一連の、または一定範囲のインターフェイスまたは VLAN を選択するには、[,|-] オプションを使用します。

一連の VLAN またはインターフェイスを指定する場合は、カンマの前後に 1 つずつスペースを入力する必要があります。一定範囲の VLAN またはインターフェイスを指定する場合は、ハイフン (-) の前後に 1 つずつスペースを入力する必要があります。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定できません。EtherChannel グループのメンバーである物理ポートは宛先ポートとして使用できますが、それが SPAN 宛先として指定されている間は、EtherChannel グループに参加できません。

プライベート VLAN ポートは、SPAN 宛先ポートとして設定できません。

ポートが EtherChannel に参加している間でも、個々のポートを監視することができます。また、**port-channel** 番号を RSPAN 送信元インターフェイスとして指定することで EtherChannel バンドル全体を監視できます。

宛先ポートとして使用されているポートを SPAN または RSPAN 送信元として指定することはできません。また、1 つのポートを一度に複数のセッションの宛先ポートとして指定することもできません。

SPAN または RSPAN 宛先ポートであるポートで IEEE 802.1x 認証をイネーブルにすることはできませんが、そのポートが SPAN 宛先として削除されるまで IEEE 802.1x 認証は使用できません。そのポートで IEEE 802.1x 認証を使用できない場合、スイッチはエラーメッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

VLAN フィルタリングとは、トランク送信元ポート上の選択した一連の VLAN のネットワークトラフィックを分析することです。デフォルトでは、トランク送信元ポート上のすべての VLAN が監視されます。トランク送信元ポートの SPAN トラフィックを指定した VLAN だけに制限するには、**monitor session session\_number filter vlan vlan-id** コマンドを使用します。

VLAN モニタリングと VLAN フィルタリングは相互に排他的です。VLAN が送信元である場合は、VLAN フィルタリングをイネーブルにすることはできません。VLAN フィルタリングが設定されている場合、VLAN を送信元として指定することはできません。

ネットワークセキュリティデバイスに対して入力トラフィック転送が有効である場合、宛先ポートはトラフィックをレイヤ 2 で転送します。

宛先トラフィックは、次の方法で動作するように設定できます。

- **monitor session session\_number destination interface interface-id** を、その他のキーワードを指定せずに入力した場合、出力カプセル化はタグなしで、入力転送はイネーブルになりません。
- **monitor session session\_number destination interface interface-id ingress** と入力した場合、出力カプセル化はタグなしになり、入力カプセル化は後続のキーワード (**dot1q**、**isl**、または **untagged**) に応じて決定されます。
- **monitor session session\_number destination interface interface-id encapsulation replicate** を、その他のキーワードを指定せずに入力した場合、出力カプセル化は送信元インターフェイスカプセル化を複製し、入力転送はイネーブルになりません（これは、ローカル SPAN のみに適用されます。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session session\_number destination interface interface-id encapsulation replicate ingress** と入力した場合、出力カプセル化は送信元インターフェイスカプセル化を複製し、入力カプセル化は後続のキーワード (**dot1q**、**isl**、または **untagged**) に応じて決定されます（これは、ローカル SPAN のみに適用されます。RSPAN はカプセル化の複製をサポートしていません）。
- Catalyst 3560E-12D スイッチは送信元セッションを 1 つだけサポートします（ローカル SPAN 送信元セッションまたは RSPAN 送信元セッションのどちらか）。
- Catalyst 3560E-12D スイッチでは、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。指定するには、**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ます。

**例** 次の例では、ローカル SPAN セッション 1 を作成し、スタックメンバー 1 の送信元ポート 1 とスタックメンバー 2 の宛先ポート 2 との間で送受信されるトラフィックを監視する方法を示しています。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/2
```

次の例では、既存のローカル SPAN セッションから宛先ポートを削除する方法を示しています。

```
Switch(config)# no monitor session 2 destination gigabitethernet1/0/2
```

次の例では、既存セッション内の SPAN トラフィックを特定の VLAN のみに制限する方法を示しています。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次の例では、複数の送信元インターフェイスを監視するように RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示しています。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

次の例では、Catalyst 3560E-12D スイッチ上で、複数の送信元インターフェイスを監視するように RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示しています。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900 destination-group b
Switch(config)# end
```

次の例では、監視対象トラフィックを受信するスイッチ内で RSPAN 宛先セッション 10 を設定する方法を示しています。

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ 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方法を示しています。出力トラフィックは送信元を複製します。また、入力トラフィックは、IEEE 802.1Q カプセル化を使用します。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
encapsulation dot1q ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 の入力トラフィック用の宛先ポートを設定する方法を示しています。出力トラフィックと入力トラフィックはタグなしになります。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
untagged vlan 5
```

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。スイッチの SPAN および RSPAN 設定を表示するには、**show running-config** 特権 EXEC コマンドを入力します。SPAN 情報は出力の終わり近くに現れます。

## 関連コマンド

コマンド	説明
<a href="#">remote-span</a>	vlan コンフィギュレーション モードで RSPAN VLAN を設定します。
<a href="#">show monitor</a>	SPAN および RSPAN セッション情報を表示します。
<a href="#">show running-config</a>	稼働設定を表示します。構文の詳細については、次のリンクを使用して、Cisco IOS Release 12.2 コマンドリファレンスのリスト ページを参照してください。 <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html">http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html</a> <b>Cisco IOS Commands Master List, Release 12.2</b> を選択して、コマンドに移動します。


# コマンドリファレンスの show monitor session コマンドに関する更新情報

## show monitor

スイッチ上のすべての Switched Port Analyzer (SPAN; スイッチドポートアナライザ) および Remote SPAN (RSPAN) セッションに関する情報を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。特定のセッション、すべてのセッション、すべてのローカルセッション、またはすべてのリモートセッションを表示するには、それぞれ該当するキーワードを指定してこのコマンドを実行します。

```
show monitor [session {session_number | all | local | range list | remote} [detail]] [| {begin | exclude | include} expression]
```

### シンタックスの説明

<b>session</b>	(任意) 指定された SPAN セッションに関する情報を表示します。
<i>session_number</i>	SPAN または RSPAN セッションの番号を指定します。指定できる範囲は 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、 <i>session_number</i> に入力できる値は <b>1</b> だけです。
<b>all</b>	すべての SPAN セッションを表示します。
<b>local</b>	ローカル SPAN セッションのみを表示します。
<b>range list</b>	一定範囲の SPAN セッションが表示されます。 <i>list</i> には有効なセッションの範囲で、単一のセッションまたはセッションの範囲を指定します。範囲の場合は、先頭と終わりの 2 つの番号を小さい方を先にしてハイフンで区切って指定します。カンマ区切りのパラメータの間、またはハイフン区切りの範囲にスペースを入力しないでください。
	 <b>(注)</b> このキーワードは、特権 EXEC モードでのみ使用可能です。
<b>remote</b>	リモート SPAN セッションのみを表示します。
<b>detail</b>	(任意) 指定されたセッションに関する詳細情報を表示します。
<b>begin</b>	<i>expression</i> と一致する行から表示を開始します。
<b>exclude</b>	<i>expression</i> と一致する行を表示から除外します。
<b>include</b>	指定した <i>expression</i> と一致する行を表示します。
<i>expression</i>	参照ポイントとして使用する出力内の文字列です。

### コマンドモード

ユーザ EXEC

### コマンド履歴

リリース	変更内容
12.2(35)SE2	このコマンドが追加されました。

### 使用上のガイドライン

文字列 (*expression*) では大文字と小文字が区別されます。たとえば、| **exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

**show monitor** コマンドと **show monitor session all** コマンドの出力は同じです。

例 次に、Catalyst 3560E-12D スイッチ以外のスイッチでの **show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Switch# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled

Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

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

```
Switch# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次に、入力トラフィック転送がイネーブルの場合の **show monitor session all** ユーザ EXEC コマンドの出力例を示します。

```
Switch# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```



次に、Catalyst 3560E-12D スイッチでの **show monitor** ユーザ EXEC コマンドの出力例を示します。宛先グループに関する情報は、RSPAN 送信元セッションがスイッチに設定されている場合にのみ表示されます。

```
Switch# show monitor
Session 1
-----
Type : Remote Source Session
Source Ports :
Both : Te0/7,Te0/10
Dest RSPAN VLAN : 900
Dest-port group : A = Te0/1-4, Gi0/1-8
```

関連コマンド

コマンド	説明
<a href="#">monitor session</a>	SPAN または RSPAN セッションを開始または変更します。

## コマンドリファレンスへの system env fan-fail-action shut コマンドの追加

**system env fan-fail-action shut** 特権 EXEC コマンドが『*Catalyst 3750-E and 3560-E Switch Command Reference*』に追加されました。

### system env fan-fail shutdown

1 つ以上のファンが故障したときにシャットダウンするように Catalyst 3560-E-12 スイッチを設定するには、**system env fan-fail-action shut** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**system env fan-fail-action shut**

**no system env fan-fail-action shut**

このコマンドは、Catalyst 3560E-12D スイッチでのみサポートされます。

#### シンタックスの説明

このコマンドには、引数またはキーワードはありません。

#### デフォルト

デフォルトでは、ファン障害機能はディセーブルです。Catalyst 3560E-12D スイッチは、FRU（現場で交換可能なユニット）または電源モジュール内の 1 つ以上のファンが故障してもシャットダウンしません。

#### コマンドモード

グローバル コンフィギュレーション

#### コマンド履歴

リリース	変更内容
12.2(40)EX	このコマンドが追加されました。

#### 使用上のガイドライン

ファン障害機能をイネーブルにするには、**system env fan-fail-action shut** グローバル コンフィギュレーション コマンドを入力します。1 つ以上のスイッチ ファンが故障した場合、Catalyst 3560E-12D スイッチは自動的にシャットダウンします。

この機能をディセーブルにし、デフォルト設定に戻すには、**no system env fan-fail-action shut** コマンドを入力します。

この機能の詳細については、「ソフトウェア コンフィギュレーション ガイドへの「ファン障害」の追加」(p.17) を参照してください。

#### 例

次の例は、ファン障害機能をイネーブルにする方法を示しています。

```
Switch# configure terminal
Switch(config)# system env fan-fail-action shut
Switch(config)# end
```

## 関連資料

マニュアルをご注文の際は、「[マニュアルの入手方法、テクニカル サポート、およびセキュリティガイドライン](#)」(p.28)に記載した URL で表示される Cisco.com および電話番号を利用して、DOC-xxxxxx= の形式で必要な文書をご指定ください。

スイッチの詳細については、Cisco.com で次のマニュアルを参照してください。

- 『*Catalyst 3750-E and Catalyst 3560-E Switch Hardware Installation Guide*』(発注はできませんが、Cisco.com から入手できます。)
- 『*Regulatory Compliance and Safety Information for the Catalyst 3750-E and Catalyst 3560-E Switch*』(Customer Order number DOC-7817569=)
- 『*Release Notes for the Catalyst 3750-E and Catalyst 3560-E Switch*』(発注はできませんが、Cisco.com から入手できます。)
- 『*Catalyst 3750-E and Catalyst 3560-E Switch Software Configuration Guide*』(発注はできませんが、Cisco.com から入手できます。)
- 『*Cisco Software Activation and Compatibility Document*』(発注はできませんが、Cisco.com から入手できます。)
- 『*Catalyst 3750-E and Catalyst 3560-E Switch Command Reference*』(発注はできませんが、Cisco.com から入手できます。)
- 『*Catalyst 3750-E and Catalyst 3560-E Switch System Message Guide*』(発注はできませんが、Cisco.com から入手できます。)
- 『*Installation Notes for the Catalyst 3750-E, Catalyst 3560-E, and RPS 2300 Power Supply Modules*』(Customer Order Number DOC-7817570=)
- 『*Installation Notes for the Catalyst 3750-E and Catalyst 3560-E Switch Fan Module*』(Customer Order Number DOC-7817571=)
- 『*Installation Notes for the Cisco TwinGig Converter Module*』(Customer Order Number DOC-7817572=)
- 『*Cisco Redundant Power System 2300 Hardware Installation Guide*』(Customer Order Number DOC-7817647=)
- 『*Cisco Redundant Power System 2300 Compatibility Matrix*』(発注はできませんが、Cisco.com から入手できます。)

## マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスと一般的なシスコのマニュアルに関する情報については、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。ここでは、シスコの新規および改訂版の技術マニュアルの一覧も表示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

### Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register/>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(0709R)

Copyright © 2007, Cisco Systems, Inc.  
All rights reserved.

お問い合わせは、購入された各代理店へご連絡ください。

シスコシステムズでは以下のURLで最新の日本語マニュアルを公開しております。  
本書とあわせてご利用ください。

**Cisco.com 日本語サイト**

[http://www.cisco.com/japanese/warp/public/3/jp/service/manual\\_j/](http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/)

日本語マニュアルの購入を希望される方は、以下のURLからお申し込みいただけます。

**シスコシステムズマニュアルセンター**

<http://www2.hipri.com/cisco/>

上記の両サイトで、日本語マニュアルの記述内容に関するご意見もお受けいたしますので、  
どうぞご利用ください。

なお、技術内容に関するご質問は、製品を購入された各代理店へお問い合わせください。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先 (シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-933-122 (通話料無料)、03-6670-2992 (携帯電話、PHS)

電話受付時間 : 平日 10:00 ~ 12:00、13:00 ~ 17:00