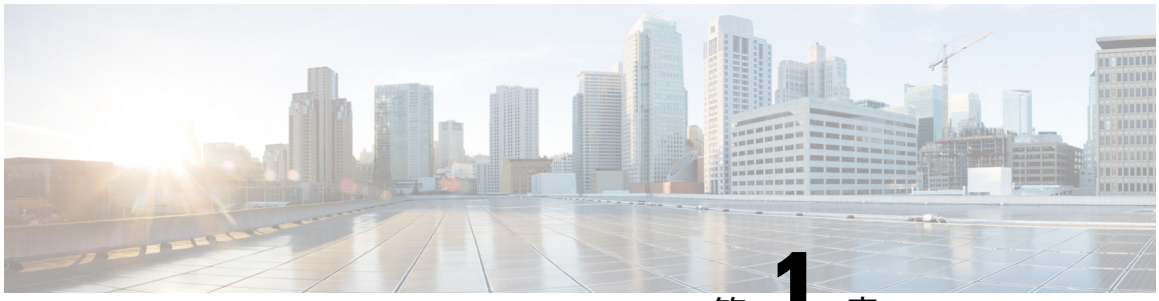
Cisco Catalyst IE3x00 高耐久性、IE3400 Heavy Duty、ESS3300 シリーズ スイッチ ネットワーク管理設定ガイド

最終更新：2024 年 9 月 9 日

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
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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/**）をご確認ください。本書は、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。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。



第 1 章

組み込みパケットキャプチャの設定

組み込みパケット キャプチャの概要

組み込みパケットキャプチャ（EPC）は、ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャし、パケットをローカルで分析するか、オフライン分析を行うために、パケットを保存してエクスポートできるようにするオンボードパケットキャプチャファシリティです。キャプチャされたデータは .pcap ファイル形式で保存され、Wireshark などの標準的なパケット分析ツールを使用して分析できます。この機能は、パケットの形式に関する情報を収集することによって、トラブルシューティングを容易にします。また、アプリケーションの分析とセキュリティも容易にします。

組み込みパケットキャプチャ（EPC）は、パケットのトレースとトラブルシューティングに役立つ組み込みシステム管理機能を提供します。ネットワーク管理者は、キャプチャバッファサイズおよびキャプチャする各パケットの最大バイト数を定義する場合があります。パケット キャプチャ レートは、詳細な管理制御を使用してスロットリングできます。たとえば、アクセス コントロール リストを使用してキャプチャ対象パケットをフィルタリングするオプションや、最大パケット キャプチャ レートまたはサンプリング間隔の指定などの詳細な定義を行うオプションが利用できます。

（注） パケットキャプチャは、物理インターフェイス上の入力方向でのみサポートされています。ACL フィルタは、EPC を設定する前に設定する必要があります。

組み込みパケットキャプチャの設定

組み込みパケットキャプチャを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。
ステップ 2	**monitor capture** *capture-name* **access-list** *access-list-name*	アクセスリストをパケットキャプチャのコアフィルタとして指定し、モニターキャプチャを設定します。
ステップ 3	**monitor capture** *capture-name* **limit duration** *seconds*	モニターキャプチャの制限を設定します。
ステップ 4	**monitor capture** *capture-name* **interface** *interface-name* **in**	接続ポイントおよびパケットフロー方向を指定して、モニターキャプチャを設定します。
ステップ 5	**monitor capture** *capture-name* **buffer circular size** *bytes*	パケットデータをキャプチャするようにバッファを設定します。サイズは最大100 MBです。
ステップ 6	**monitor capture** *capture-name* **start**	トラフィック トレース ポイントでパケットデータのバッファへのキャプチャを開始します。
ステップ 7	**monitor capture** *capture-name* **export** *file-location/file-name*	キャプチャされたデータを分析用にエクスポートします。
ステップ 8	**monitor capture** *capture-name* **stop**	トラフィック トレース ポイントでパケットデータのキャプチャを停止します。
ステップ 9	**monitor capture** *capture-name* **clear**	キャプチャされたバッファデータをクリアします。
ステップ 10	**end**	特権 EXEC モードを終了します。

例

キャプチャされたデータのモニタリングとメンテナンス

キャプチャされたパケットデータのモニタリングとメンテナンスを行うには、次の作業を実行します。キャプチャ バッファの詳細とキャプチャ ポイントの詳細を表示します。

手順

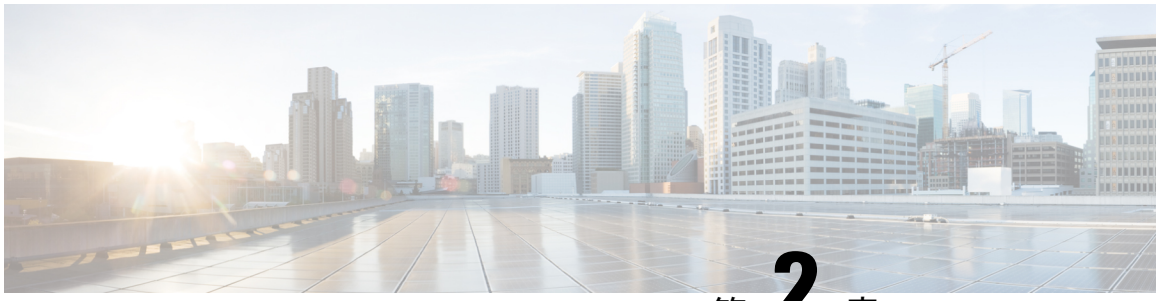
	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。
ステップ 2	**show monitor capture** *capture-buffer-name* **buffer dump**	（任意）キャプチャされたパケットの 16 進数ダンプおよびそのメタデータを表示します。

	コマンドまたはアクション	目的
ステップ 3	**show monitor capture** *capture-buffer-name* **parameter**	（任意）キャプチャを指定するために使用されたコマンドのリストを表示します。
ステップ 4	**debug epc capture-point**	（任意）パケットキャプチャポイントのデバッグを有効にします。
ステップ 5	**debug epc provision**	（任意）パケット キャプチャ プロビジョニングのデバッグを有効にします。
ステップ 6	**exit**	特権 EXEC モードを終了します。

例

機能の履歴

機能名	リリース	機能情報
組み込みパケット キャプチャ	Cisco IOS XE 16.11.1	Cisco Catalyst IE 3200、3300、3400、およびCiscoエンベデッドサービス 3300 シリーズ スイッチでの初期サポート



第 2 章

Cisco TrustSec フィールドの Flexible NetFlow エクスポート

Flexible NetFlow の Cisco TrustSec フィールド

Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、Flexible Netflow（FNF）フローレコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニタ、トラブルシューティング、および特定を支援します。

（注） Flexible NetFlow レコード、および IP パケットの Cisco TrustSec フィールドの記録は、IPv4 パケットでのみ機能します。IPv6 パケットは、Cisco TrustSec フィールドのキャプチャをサポートしていません。

Flexible Netflow（FNF）フローレコード内の Cisco TrustSec フィールド、送信元セキュリティグループタグ（SGT）および宛先セキュリティグループタグ（DGT）は、管理者によるフローとアイデンティティ情報の関連付けに役立ちます。ネットワーク エンジニアは、これにより、顧客のネットワーク リソースおよびアプリケーション リソースの利用について詳しく理解できます。この情報を使用して、潜在的なセキュリティやポリシーの違反を検出して解決するために、アクセスおよびアプリケーション リソースを効率的に計画して割り当てることができます。

Cisco TrustSec フィールドは入力 FNF およびユニキャスト/マルチキャスト トラフィックでサポートされています。

次のテーブルに、Cisco TrustSec 用の NetFlow V9 の企業固有フィールド タイプを示します。これは、Cisco TrustSec の送信元/宛先ソース グループ タグの FNF テンプレートで使用されます。

ID	説明
CTS_SRC_GROUP_TAG	Cisco Trusted Security 送信元グループ タグ
CTS_DST_GROUP_TAG	Cisco Trusted Security 宛先グループ タグ

FNF フロー レコードで既存の一致するフィールドに加えて、Cisco TrustSec フィールドが設定されます。次の設定を使用して、Cisco TrustSec フローオブジェクトを非キーフィールドとして FNF フローレコードに追加し、パケットの送信元と宛先のセキュリティグループタグを設定します。

collect flow cts {source | destination} group-tag コマンドは、非キーフィールドとして Cisco TrustSec フィールドを指定するため、フローレコードで設定されます。非キー フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。

フロー レコードは、フロー モニタ下で設定され、フロー モニタはインターフェイスに適用されます。FNF データをエクスポートするには、フローエクスポータを設定し、フローモニター以下に追加する必要があります。

フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **match ipv4 protocol**
5. **match ipv4 source address**
6. **match ipv4 destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **collect flow cts source group-tag**
10. **collect flow cts destination group-tag**
11. **collect counter packets**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow record** *record-name* 例： `Device(config)# flow record cts-record-ipv4`	Flexible Netflow（FNF）フロー レコードを作成するか、または既存の FNF フロー レコードを変更して、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
ステップ 4	**match ipv4 protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	（オプション）フローレコードのキーフィールドとして IPv4 プロトコルを設定します。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
ステップ 5	**match ipv4 source address** 例： `Device(config-flow-record)# match ipv4 source address`	（任意）IPv4 送信元アドレスをフローレコードのキーフィールドとして設定します。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
ステップ 6	**match ipv4 destination address** 例： `Device(config-flow-record)# match ipv4 destination address`	（任意）IPv4宛先アドレスをフローレコードのキーフィールドとして設定します。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
ステップ 7	**match transport source-port** 例： `Device(config-flow-record)# match transport source-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート送信元ポートを設定します。

	コマンドまたはアクション	目的
ステップ 8	**match transport destination-port** 例： `Device(config-flow-record)# match transport destination-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート宛先ポートを設定します。
ステップ 9	**collect flow cts source group-tag** 例： `Device(config-flow-record)# collect flow cts source group-tag`	（オプション）FNF フローレコード内の Cisco TrustSec 送信元セキュリティグループタグ（SGT）を非キーフィールドとして設定します。
ステップ 10	**collect flow cts destination group-tag** 例： `Device(config-flow-record)# collect flow cts destination group-tag`	（オプション）FNF フローレコード内の Cisco TrustSec 宛先セキュリティグループタグ（DGT）を非キーフィールドとして設定します。
ステップ 11	**collect counter packets** 例： `Device(config-flow-record)# collect counter packets`	（オプション）フローで確認されるパケット数を非キー フィールドとして設定し、フローから合計パケット数を収集します。
ステップ 12	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フロー エクスポータの設定

フローエクスポータごとに、1つの宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポータを設定してフロー モニターに割り当てる必要があります。

始める前に

フロー レコードを作成していることを確認します。詳細については、「フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定」の項および「フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**

3. **flow exporter** *exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow exporter** *exporter-name* 例： `Device(config)# flow exporter EXPORTER-1`	フローエクスポータを作成するか、または既存のフロー エクスポータを変更して、Flexible NetFlow フロー エクスポータ コンフィギュレーション モードを開始します。
ステップ 4	**destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*] 例： `Device(config-flow-exporter)# destination 172.16.10.2`	エクスポータの宛先システムの IP アドレスまたはホスト名を指定します。
ステップ 5	**end** 例： `Device(config-flow-exporter)# end`	Flexible NetFlow フロー エクスポータ コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

フロー モニタの設定

始める前に

フロー エクスポータをデータ エクスポート用のフロー モニタに追加するには、フロー エクスポータを作成していることを確認します。詳細については、「フローエクスポータの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**

3. **flow monitor** *monitor-name*
4. **record** *record-name*
5. **exporter** *exporter-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor FLOW-MONITOR-1`	フロー モニタを作成するか、または既存のフロー モニタを変更して、Flexible NetFlow フロー モニタ コンフィギュレーション モードを開始します。
ステップ 4	**record** *record-name* 例： `Device(config-flow-monitor)# record cts-record-ipv4`	フロー モニターのレコードを指定します。
ステップ 5	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter EXPORTER-1`	フロー モニタのエクスポータを指定します。
ステップ 6	**end** 例： `Device(config-flow-monitor)# end`	Flexible NetFlow フロー モニタ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイスへのフロー モニタの適用

フロー モニタをアクティベートするには、フロー モニタを 1 つ以上のインターフェイスに適用する必要があります。

始める前に

フロー モニタを作成していることを確認します。詳細については、「フロー モニタの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow monitor** *monitor-name* **input**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface Gi1/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip flow monitor** *monitor-name* **input** 例： `Device (config-if)# ip flow monitor FLOW-MONITOR-1 input`	作成済みのフローモニタを、トラフィックの分析対象となるインターフェイスに割り当てることで、そのフロー モニタをアクティブにします。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの確認

手順の概要

1. **enable**
2. **show flow record** *record-name*
3. **show flow exporter** *exporter-name*
4. **show flow monitor** *monitor-name*
5. **show flow monitor** *monitor-name* **cache**
6. **show flow interface** *type number*

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show flow record *record-name*

指定した Flexible Netflow（FNF）フロー レコードの詳細を表示します。

例：

```
Device> show flow record cts-recordipv4

flow record cts-recordipv4:
  Description:        User defined
  No. of users:       1
  Total field space:  30 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface output
    collect flow direction
    collect flow cts source group-tag
    collect flow cts destination group-tag
```

```
    collect counter packets
```

ステップ 3 **show flow exporter** *exporter-name*

指定した FNF フロー エクスポータの現在のステータスを表示します。

例：

```
Device> show flow exporter EXPORTER-1

Flow Exporter EXPORTER-1:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 100.100.100.1
    Source IP address:      3.3.3.2
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            65252
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

ステップ 4 **show flow monitor** *monitor-name*

指定した FNF フロー モニタのステータスと統計情報を表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       User defined
  Flow Record:       cts-recordipv4
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:                 normal (Platform cache)
    Status:               allocated
    Size:                 200000 entries
    Inactive Timeout:     60 secs
    Active Timeout:       1800 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
    Trans end aging:      off
```

ステップ 5 **show flow monitor** *monitor-name* **cache**

指定した FNF フロー モニタ キャッシュのコンテンツを表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1 cache
```

```
  Cache type:                               Normal
  Cache size:                               4096
  Current entries:                          2
  High Watermark:                           2

  Flows added:                              6
  Flows aged:                               4
    - Active timeout      (1800 secs)       0
    - Inactive timeout    (15 secs)         4
    - Event aged                            0
    - Watermark aged                        0
    - Emergency aged                        0

  IPV4 SOURCE ADDRESS:                      10.1.0.1
  IPV4 DESTINATION ADDRESS:                 172.16.2.0
  TRNS SOURCE PORT:                         58817
  TRNS DESTINATION PORT:                    23
  FLOW DIRECTION:                           Input
  IP PROTOCOL:                              6
  SOURCE GROUP TAG:                         100
  DESTINATION GROUP TAG:                    200
  counter packets:                          10

  IPV4 SOURCE ADDRESS:                      172.16.2.0
  IPV4 DESTINATION ADDRESS:                 10.1.0.1
  TRNS SOURCE PORT:                         23
  TRNS DESTINATION PORT:                    58817
  FLOW DIRECTION:                           Output
  IP PROTOCOL:                              6
  SOURCE GROUP TAG:                         200
  DESTINATION GROUP TAG:                    100
  counter packets:                          8
```

ステップ 6 **show flow interface** *type number*

指定したインターフェイスに適用されるFNFフローモニタの詳細を表示します。フローモニタがインターフェイスに適用されない場合、出力は空になります。

例：

```
Device>  show flow interface Gi1/1

Interface GigabitEthernet1/1
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
```

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定例

例：フローレコードの非キーフィールドとしてのCiscoTrustSecフィールドの設定

次の例は、Cisco TrustSec フロー オブジェクトを、IPv4 Flexible NetFlow フロー レコードの非キー フィールドとして設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# end
```

例：フロー エクスポータの設定

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# end
```

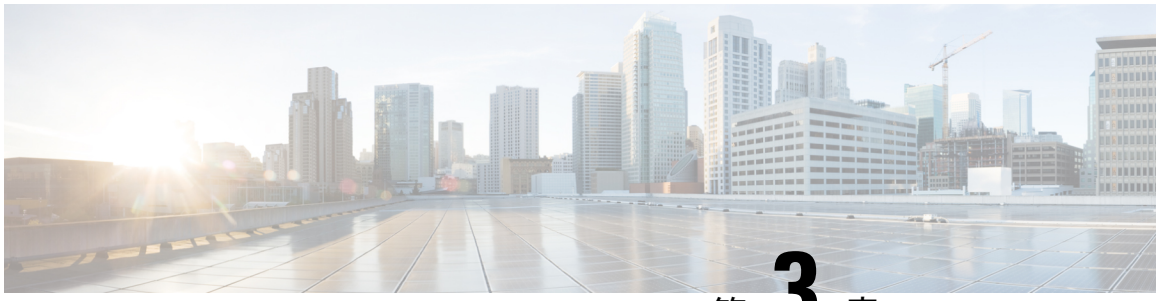
例：フロー モニタの設定

```
Device> enable
Device# configure terminal
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record cts-record-ipv4
Device(config-flow-monitor)# exporter EXPORTER-1
Device(config-flow-monitor)# end
```

例：インターフェイス上のフロー モニタの適用

次の例は、トラフィックを分析するインターフェイスにIPv4フローモニタを適用することで、このフロー モニタをアクティベートする方法を示します。IPv6 フローモニターをアクティベートするには、 **ip** キーワードを **ipv6** キーワードと置き換えます。

```
Device> enable
Device# configure terminal
Device(config)# interface Gi1/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# end
```



第 3 章

SNMP の設定

SNMP の前提条件

サポートされている SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1：RFC1157 に規定された SNMP（完全インターネット標準）。
- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティ ベースの管理およびセキュリティ フレームワークをコミュニティ ストリング ベースの管理フレームワークに置き換えたものです。次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定された SNMP バージョン 2（ドラフト版インターネット標準）
  - SNMPv2C：RFC 1901 に規定された SNMPv2 のコミュニティ ストリング ベースの管理フレームワーク（試験版インターネット プロトコル）
- SNMPv3：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベース プロトコルです。SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
  - メッセージの完全性：パケットが伝送中に改ざんされないようにします。
  - 認証：有効な送信元からのメッセージであるかどうかを判別します。

- 暗号化：パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。

（注） 暗号化を選択するには、 **priv** キーワードを入力します。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索機能が組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索機能は、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラー コードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュリティ方式が決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

次の表では、この特性を識別し、セキュリティ モデルとセキュリティ レベルの異なる組み合わせを比較します。

表 *1 : SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	未対応	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	未対応	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	ユーザー名	未対応	ユーザ名の照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
SNMPv3	authNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	未対応	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv	MD5 または SHA	データ暗号規格（DES）または Advanced Encryption Standard（AES）	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。 次の暗号化アルゴリズムで、User-based Security Model（USM）を指定できます。 • CBC-DES（DES-56）規格に基づく認証に加えた DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP の制約事項

バージョンの制約事項

- SNMPv1 は informs をサポートしていません。

SNMP に関する情報

ここでは、SNMP の概要について説明します。

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージ フォーマットを提供するアプリケーションレイヤプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース（MIB）で構成されます。SNMP マネージャは、Cisco Prime Infrastructure などのネットワーク管理システム（NMS）に統合できます。エージェントと MIB はネットワークデバイス上に存在します。デバイスに SNMP を設定するには、マネージャとエージェントの間の関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、次の表に示す動作を実行します。

表 *2 : SNMP* の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[1]
get-bulk-request[2]	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

[1] この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
[2] get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

（注） パフォーマンスに関連する問題を回避するために、SNMP マネージャで **ciscoFlashFileDate** MIB オブジェクトをクエリから除外することを推奨します。これは、 **ciscoFlashFileDate** オブジェクトが MIB で公開されていても、製品ではサポートされていないためです。

SNMP エージェント機能

SNMP エージェントは、1 つ以上の SNMP マネージャから要求を受信できます。すべての要求に、NMS の IP アドレス、NMS がエージェントをポーリングした回数、およびポーリングのタイムスタンプが含まれます。この情報は、IPv4 サーバーと IPv6 サーバーの両方で追跡できます。

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

※ **show snmp stats hosts** コマンドを使用してキュー内の SNMP マネージャ要求のリストを表示し、 **clear snmp stats hosts** コマンドを使用してキューをクリアします。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリートポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がデバイスにアクセスするには、NMS 上のコミュニティストリング定義がデバイス上の 3 つのコミュニティストリング定義の少なくとも 1 つと一致しなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- 読み取り専用（RO）：コミュニティ ストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。

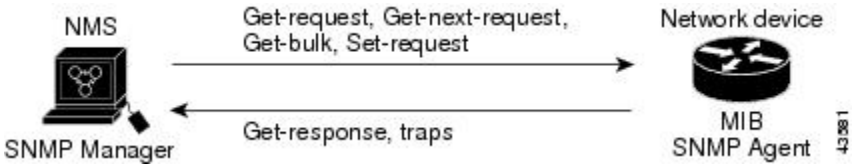
- 読み取り-書き込み（RW）：MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンドデバイスがメンバデバイスとSNMPアプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドデバイス上で最初に設定されたRWおよびROコミュニティストリングにメンバデバイス番号（@esN、N はデバイス番号）を追加し、これらのストリングをメンバデバイスに伝播します。

SNMP MIB 変数アクセス

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。Cisco Prime Infrastructure ソフトウェアは、デバイス MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

次の図に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから次の形式で送信される MIB 関連のクエリに応答します。 *get-request*、 *get-next-request*にダウンロードすると、 *set-request* 形式のファイル名を付けてファイルを保存します。

図 *1 : SNMP* ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、デバイスからSNMPマネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード traps はトラップ、情報、またはその両方を表します。※ **snmp-server host** コマンドを使用して、トラップまたはインフォームのどちらとして SNMP 通知を送信するかを指定します。

（注） SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかが送信側にわからないからです。情報要求の場合、受信したSNMPマネージャはSNMP応答プロトコル データ ユニット（PDU）でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、デバイスおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は1回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMPマネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはデバイスのメモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

SNMP エージェントの IF-MIB モジュールがリブート後すぐに起動されます。さまざまな物理インターフェイス ドライバが IF-MIB モジュールの登録を初期化されているように、「インデックス番号をください」と示します。IF-MIB モジュールが先着順で使用可能な次の ifIndex 番号を割り当てます。つまり、1 つのリブートから他のリブートへのドライバの初期化順序のマイナーな違いが、同じ物理インターフェイスにリブートを行う以前のものとは別のインデックス番号を取得する可能性があるということです（インデックス持続が有効化されていない限り）。

SNMP および Syslog Over IPv6

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。Syslog over IPv6 は、このトランスポートのアドレス データ タイプをサポートします。

Simple Network Management Protocol (SNMP) と syslog over IPv6 は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

Over IPv6 をサポートするため、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザー データグラム プロトコル（UDP）SNMP ソケットを開く

- ※ *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む SNMP over IPv6 の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の 「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、syslog over IPv6 については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の 「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル[3]
SNMP トラップ レシーバ	未設定
SNMP トラップ	TCP接続のトラップ（tty）以外は、イネーブルではありません。
SNMP バージョン	バージョン キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを指定しない場合、デフォルトは **noauth** (noAuthNoPriv) セキュリティレベルです。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

[3] これは、デバイスが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

デバイスでは、SNMP UDP ポート 161 および 162 を開き、SNMP エージェントを有効にするために、次のいずれかのグローバル コンフィギュレーション コマンドを設定する必要があります。 **snmp-server host**、または **snmp-server user**、または **snmp-server community**、または **snmp-server manager**に従って構成設定を変更します。

SNMP *group* は、SNMP ユーザーを SNMP ビューに対応付けるテーブルです。SNMP *user* は、SNMP グループのメンバーです。SNMP ホストは、トラップ動作の受信先です。SNMP エンジン ID は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP グループを設定するときには、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。 **snmp-server host** グローバル コンフィギュレーション コマンドがユーザーの通知ビューを自動生成し、そのユー

ザーに関連付けられているグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。

- リモートユーザを設定する場合は、ユーザが存在するデバイスのリモートSNMPエージェントに対応するIPアドレスまたはポート番号を指定します。
- 特定のエージェントにリモートユーザーを設定する前に、SNMP エンジン ID を設定します。設定には、 **snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションを指定して使用します。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシー ダイジェストが算出されます。先にリモートエンジンIDを設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカルユーザーがリモートホストと関連付けられていない場合、デバイスは **auth**（authNoPriv）および **priv** （authPriv）の認証レベルのインフォームを送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。（コマンド ラインで入力された）ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5またはSHAセキュリティ ダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は、SNMPv3 ユーザーのセキュリティダイジェストが無効となり、 **snmp-server user** *username* グローバル コンフィギュレーション コマンドを使用して、SNMP ユーザーを再設定する必要があります。エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要があります。
- SNMP サーバーホストをデフォルトの UDP ポート（162）で設定すると、 **show running-config** コマンドの出力にUDPポート値が表示されません。デフォルト以外のUDPポート値を **snmp-server host** {*host-addr*} *community-string* **udp-port** *value* コマンドを使用して指定する場合は、UDPポート番号が **show running-config** コマンド出力に表示されます。これを自動または手動で実行するように **snmp-server host** コマンドを、デフォルトのUDPポート162を使用しても使用しなくても設定できます。ただし、両方を同時に設定することはできません。

  正しい例を次に示します。

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community

Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community udp-port 162
```

  次の例は正しくありません。

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community
Device(config)# snmp-server host 10.10.10.10 community udp-port 162

Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community udp-port 162
Device(config)# snmp-server host 10.10.10.10 community
```

SNMP の設定方法

ここでは、SNMP の設定方法について説明します。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がデバイスにアクセスするには、NMS 上のコミュニティストリング定義がデバイス上の 3 つのコミュニティストリング定義の少なくとも 1 つと一致しなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- 読み取り専用（RO）：コミュニティ ストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。
- 読み取り-書き込み（RW）：MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンドデバイスがメンバデバイスと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドデバイス上で最初に設定された RW および RO コミュニティストリングにメンバデバイス番号（@esN、N はデバイス番号）を追加し、これらのストリングをメンバデバイスに伝播します。

SNMP グループおよびユーザの設定

デバイスのローカルまたはリモート SNMP サーバエンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

デバイス上の SNMP グループとユーザを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}
4. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
5. **snmp-server user** *username group-name* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*] } [*priv* {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]
6. **end**

7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*} 例： `Device(config)# snmp-server engineID local 1234`	SNMP のローカル コピーまたはリモート コピーに名前を設定します。 • *engineid-string* は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。手順例では、123400000000000000000000 のエンジン ID を設定します。 • ※ **remote**を選択した場合、SNMP のリモートコピーが置かれているデバイスの *ip-address* を指定し、任意でリモートデバイスのユーザーデータグラムプロトコル（UDP）ポートを指定します。デフォルトは 162 です。
ステップ 4	**snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*] 例： `Device(config)# snmp-server group public v2c access lmnop`	リモート デバイス上で新しい SNMP グループを設定します。 ※ *group-name* には、グループの名前を指定します。 次のいずれかのセキュリティ モデルを指定します。 • **v1** は、最も安全性の低いセキュリティ モデルです。 • **v2c** は、2 番目に安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を伝送できます。

	コマンドまたはアクション	目的
		• **v3**最も安全な場合には、次の認証レベルの 1 つを選択する必要があります。 **auth**：Message Digest 5（MD5）およびセキュアハッシュアルゴリズム（SHA）によるパケット認証を可能にします。 **noauth**：noAuthNoPriv セキュリティ レベルを可能にします。キーワードを指定しなかった場合、これがデフォルトです。 **priv**：データ暗号規格（DES）によるパケット暗号化（プライバシーともいう）を可能にします。 （任意） **read** *readview* とともに、エージェントの内容のみを表示できるビュー名を表す文字列（64 文字以内）を入力します。 （任意） **write** *writeview* とともに、データを入力し、エージェントの内容を設定できるビュー名を表す文字列（64 文字以内）を入力します。 （任意） **notify** *notifyview* とともに、通知、インフォーム、またはトラップを指定するビュー名を表す文字列（64 文字以内）を入力します。 （任意） **access** *access-list* とともに、アクセスリスト名の文字列（64 文字以内）を入力します。
ステップ 5	**snmp-server user** *username group-name* {**remote** *host* [**udp-port** *port*] } {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*] } [*priv* {**des** | **3des** | **aes** {**128** | **192** | **256**} } *priv-password*] 例： `Device(config)# snmp-server user Pat public v2c`	SNMP グループに対して新規ユーザを追加します。 The *username* は、エージェントに接続する、ホスト上のユーザーの名前です。 *group-name* は、ユーザーが対応付けられるグループの名前です。 Enter **remote** を入力して、ユーザーが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルトは 162 です。 SNMP バージョン番号（**v1**、 **v2c**、または **v3**を押します）。永続タイマーとして**v3**を入力した場合は、次の追加オプションがあります。 • **encrypted** は、パスワードを暗号化形式で表示するように指定します。このキーワードは、 **v3** キーワードを指定した場合のみ使用できます。

	コマンドまたはアクション	目的
		• **auth** は認証レベル設定セッションであり、HMAC-MD5-96 (**md5**) または HMAC-SHA-96 (**sha**）認証レベルを使用できます。 *auth-password* パスワード文字列 が必要です。（64 文字以下）。 永続タイマーとして**v3** を入力すると、次のキーワードを使用して（64文字以下）、プライベート（**priv**）暗号化アルゴリズムおよびパスワード文字列 *priv-password* を設定することもできます。 • **priv** は、ユーザベース セキュリティ モデル（USM）を指定します。 • **des** 56 ビット DES アルゴリズムを使用する場合に指定します。 • **3des** 168 ビット DES アルゴリズムを使用する場合に指定します。 • **aes** DES アルゴリズムを使用する場合に指定します。128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化のいずれかを選択する必要があります。 （任意） **access** *access-list* とともに、アクセスリスト名の文字列（64 文字以内）を入力します。
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。

SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、デバイスから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード traps はトラップ、情報、またはその両方を表します。※ **snmp-server host** コマンドを使用して、トラップまたはインフォームのどちらとして SNMP 通知を送信するかを指定します。

（注） SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかが送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答プロトコル データ ユニット（PDU）でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、デバイスおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはデバイスのメモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム接点およびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server contact** *text*
4. **snmp-server location** *text*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server contact** *text* 例： `Device(config)# snmp-server contact Dial System Operator at beeper 21555`	システムの連絡先文字列を設定します。
ステップ 4	**snmp-server location** *text* 例： `Device(config)# snmp-server location Building 3/Room 222`	システムの場所を表す文字列を設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**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。

SNMP を通して使用する TFTP サーバの制限

SNMP を介したコンフィギュレーション ファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定されたサーバに限定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server tftp-server-list** *access-list-number*
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server tftp-server-list** *access-list-number* 例： `Device(config)# snmp-server tftp-server-list 44`	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リストのサーバに限定します。 ※ *access-list-number*には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセスリスト番号を入力します。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 44 permit 10.1.1.2`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 ※ *access-list-number*には、ステップ 3 で指定したアクセスリスト番号を入力します。 **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 ※ *source*には、デバイスにアクセスできる TFTP サーバーの IP アドレスを入力します。 （任意） *source-wildcard*には、送信元に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**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。

SNMP エージェントのディセーブル化

[**no snmp-server** グローバル コンフィギュレーション コマンドは、デバイス上で実行している SNMP エージェントのすべてのバージョン（バージョン 1、バージョン 2C、バージョン 3）を無効にして、SNMP プロセスをシャットダウンします。グローバル コンフィギュレーション モードで、 **snmp-server host**、または **snmp-server user**、または **snmp-server community**、または **snmp-server manager**のいずれかのコマンドを入力して、SNMP エージェントのすべてのバージョンを再度有効にします。特に SNMP をイネーブルにするために指定された Cisco IOS コマンドはありません。

SNMP エージェントをディセーブルにするには、次の手順を実行します。

始める前に

SNMP エージェントをディセーブルにする前にイネーブルにする必要があります。SNMP エージェントは、デバイスに入力された最初の **snmp-server** グローバル コンフィギュレーション コマンドによって有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **no snmp-server**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no snmp-server** 例： `Device(config)# no snmp-server`	SNMP エージェント動作をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**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。

SNMP の例

次に、SNMP の全バージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、デバイスはトラップを送信しません。

```
Device(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。デバイスはさらに、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に

VTP トラップを送信します。コミュニティストリング *public* は、トラップとともに送信されます。

```
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps vtp
Device(config)# snmp-server host 192.180.1.27 version 2c public
Device(config)# snmp-server host 192.180.1.111 version 1 public
Device(config)# snmp-server host 192.180.1.33 public
```

次に、 *comaccess* コミュニティストリングを使用するアクセスリスト 4 のメンバーに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証失敗トラップは、SNMPv2C がコミュニティストリング *cisco.com* を使用してホスト cisco.com に送信します。 *public*をクリックします。

```
Device(config)# snmp-server community comaccess ro 4
Device(config)# snmp-server enable traps snmp authentication
Device(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com*に送信する例を示します。コミュニティストリングは制限されます。1 行目で、デバイスはすでにイネーブルになっているトラップ以外に、エンティティ MIB トラップを送信できるようになります。2行目はこれらのトラップの宛先を指定し、 **snmp-server** ホスト *cisco.com*に対する以前の ホストコマンドを無効にします。

```
Device(config)# snmp-server enable traps entity
Device(config)# snmp-server host cisco.com restricted entity
```

次の例では、すべてのトラップをホスト *myhost.cisco.com* myhost.cisco.com に送信するようにコミュニティストリング *public*を使用して、デバイスをイネーブルにする方法を示します。

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

次の例では、ユーザーがグローバル コンフィギュレーション モードを開始したときに、ユーザーをリモートホストに関連付け、 **auth**（authNoPriv）認証レベルインフォームを送信する方法を示しています。

```
Device(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Device(config)# snmp-server group authgroup v3 auth
Device(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Device(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Device(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Device(config)# snmp-server enable traps
Device(config)# snmp-server inform retries 0
```

次に、SNMPエージェントにポーリングされたSNMPマネージャのエントリを表示する例を示します。

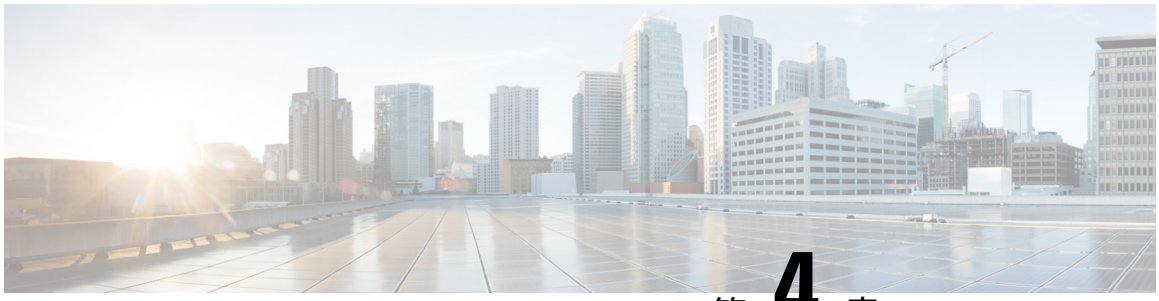
```
Device# show snmp stats host
Request Count                  Last Timestamp              Address
2                               00:00:01 ago               3.3.3.3
1                               1w2d ago                   2.2.2.2
```

SNMP ステータスのモニタリング

不正なコミュニティ ストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、 **show snmp** 特権 EXEC コマンドを使用します。また、次の表にリストされたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。

表 *3 : SNMP* 情報を表示するためのコマンド

コマンド	目的
show snmp	SNMP 統計情報を表示します。
	デバイスに設定されているローカル SNMP エンジンおよびモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示し
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を す。 （注） このコマンドは、 **auth** | **noauth** | **priv** モードの SNM 報を表示する際に使用する必要があります。この情 **running-config** 出力には表示されません。



第 4 章

SPAN および RSPAN の設定

SPAN および RSPAN の前提条件

SPAN

- SPAN トラフィックを特定の VLAN に制限するには、 **filter vlan** キーワードを使用します。トランク ポートをモニターしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニターされます。デフォルトでは、トランク ポート上のすべての VLAN がモニターされます。

RSPAN

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。

SPAN および RSPAN の制約事項

SPAN

SPAN の制約事項は次のとおりです。

- 各デバイスで 66 のセッションを設定できます。最大 2 つの送信元セッションを設定できます。残りのセッションは、RSPAN宛先セッションとして設定できます。送信元セッショ

ンは、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。

- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたはVLAN、一定範囲のポートまたはVLANのトラフィックを監視できます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 送信元ポートは、1 つのモニターセッションでのみ使用できます。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- デバイスポートを SPAN 宛先ポートとして設定すると、通常のデバイスポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、 **no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、 **encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。
- 無効のポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN が有効になってからです。
- 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。

SPAN セッションのトラフィック監視には次の制約事項があります。

- 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。
- Wireshark は、出力スパンがアクティブな場合は出力パケットをキャプチャしません。
- 同じデバイスまたはデバイススタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。デバイスまたはデバイススタックは、合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- SPAN セッションが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 または RSPAN が有効の場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。多数のポートまたは VLAN を監視すると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- デバイスは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じデバイスまたはデバイススタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。
- デバイスで DHCP スヌーピングが有効になっている場合、SPAN セッションは Dynamic Host Configuration Protocol（DHCP）入力パケットのみをキャプチャします。

RSPAN

RSPAN の制約事項は次のとおりです。

- IE31xx、IE3x00、および ESS3300 プラットフォームは、ハードウェアの制限により、1 つの RSPAN セッションのみをサポートします。
- 処理チップのハードウェア制限により、制御パケットとデータトラフィックを区別できません。したがって、ミラーリングを有効にすると、制御パケットを含むすべてのパケットがミラーリングされます。

⚠

注意 RSPAN機能は、実稼働ネットワークに影響を与える可能性があるため、慎重に使用してください。

- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのデバイスで VLAN RSPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN を設定できるトランクインターフェイスは 1 つだけです。複数のトランクインターフェイスでリモート VLAN を設定しようとすると、次のようなエラーが表示されます。

```
Switch(config-if)#do sh vlan id 2508

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2508 VLAN2508                         active    Gi1/1, Gi1/2          >>>>>>>>>>>>
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2508 enet  102508     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Enabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch(config-if)#exit
Switch(config)#mon sess 1 destination remote vlan 2508
% Platform cannot support remote-span mirroring on VLAN with more than one member
ports.
```

（注） 4 バイトの RSPAN VLAN ID の追加によって発生する RSPAN の受信インターフェイスでのエラーを防ぐために、MTU サイズをモニター対象最大パケットサイズよりも 4 バイト大きい値に設定することが推奨されます。

- プラットフォームは、複数のメンバーポートを含むポートチャネルに関連付けられた VLAN での RSPAN ミラーリングをサポートしません。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、デバイスはスパンされたトラフィックを監視しないため、デバイスの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラッディングが防止されます。
- RSPAN VLAN をネイティブ VLAN として設定しないことをお勧めします。
- SPAN と RSPAN は同時に動作できます。
- ERSPAN は、IOx の CV に対して内部的にのみ機能します。独立した機能としてはサポートされていません。
- IOx で CV が有効になっている場合、SPAN および RSPAN はサポートされません。
- IOx の CV の有効化後に SPAN/RSPAN が設定された場合、またはその逆の場合は、最新の設定が適用されます。

SPAN および RSPAN について

ここでは、SPAN および RSPAN について説明します。

SPAN および RSPAN

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

SPAN を使用してモニターできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックは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。

ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム（IDS）センサー装置を宛先ポートに接続した場合、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

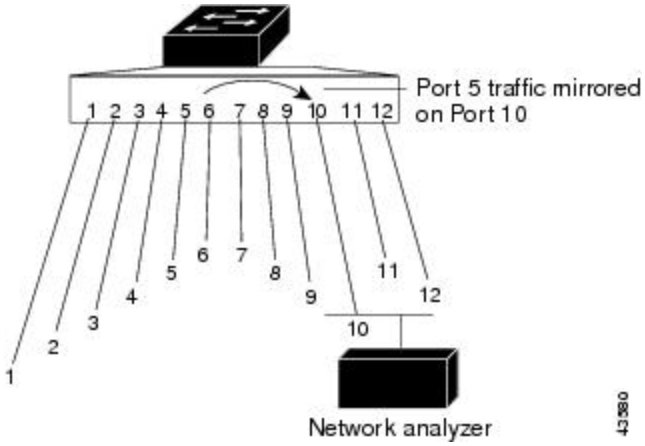
ローカル SPAN は 1 つのデバイス内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元VLAN、および宛先ポートは、同じデバイスまたはデバイススタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは1つまたは複数のVLANからのトラフィックを解析するために宛先ポートへコピーします。

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートおよび宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、1 つ以上の送信元ポートからのトラフィックを、解析のため宛先ポートにコピーします。

図 *2*：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。



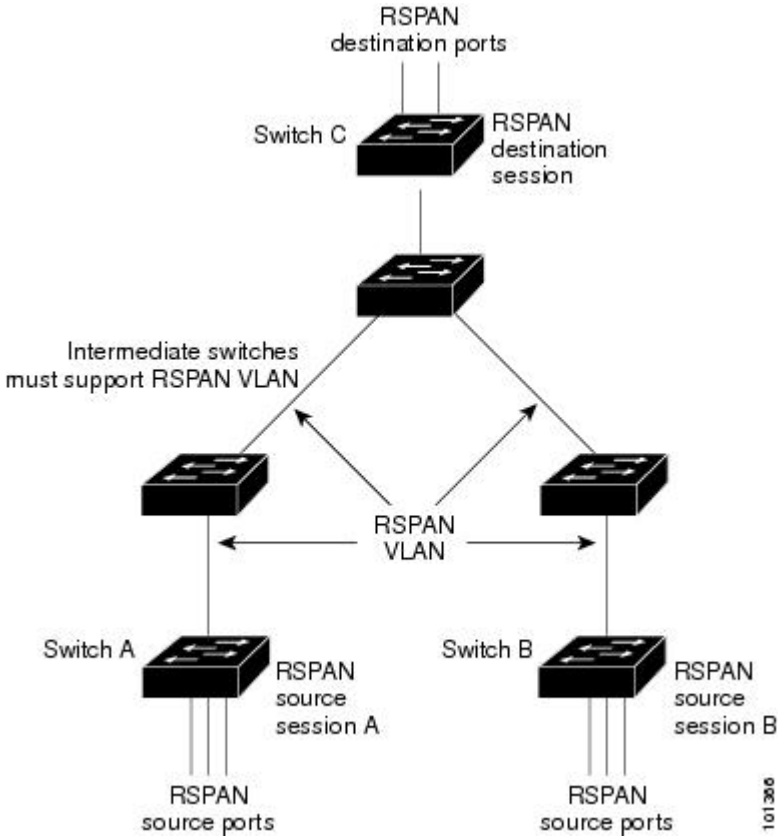
リモート SPAN

RSPAN は、異なるデバイス（または異なるデバイススタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートしているので、ネットワーク上で複数のデバイスをリモート監視できます。

図 *3 : RSPAN* の設定例

下の図にデバイス A とデバイス B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザーが指定した 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デバイスの RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランクポートを介して、RSPAN VLAN を監視する宛先セッションに転送されます。各 RSPAN 送信元デバイスには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。図中のデバ

イス C のように、宛先は常に物理ポートになります。



SPAN と RSPAN の概念および用語

SPAN セッション

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

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

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

VLANに関連付けます。宛先セッションはRSPAN VLANトラフィックをすべて収集し、RSPAN宛先ポートに送信します。

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

RSPAN宛先セッションはRSPAN VLAN上で受信されたすべてのパケットを取得し、VLANのタギングを除去し、宛先ポートに送ります。セッションは、（レイヤ2制御パケットを除く）すべての RSPAN VLAN パケットのコピーを分析のためにユーザーに提供します。

SPAN セッションでのトラフィックのモニターには、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。
- 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 または RSPAN が有効の場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。したがって、多数のポートまたは VLAN をモニターすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上にSPANセッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- デバイスは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じデバイスまたはデバイススタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

モニタ対象トラフィック

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。

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

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（デバイスで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートしています。

単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 送信元ポートは、1 つのモニターセッションでのみ使用できます。
- 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 または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニターされます。

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。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニターできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニターする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニターされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニター対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLAN フィルタリングはポートベース セッションにのみ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN のみがモニターされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザー（通常はネットワーク アナライザ）に送信する宛先ポート（別名モニター側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- 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。RSPAN セッションの場合は、RSPAN 宛先セッションを含むデバイス上にあります。RSPAN 送信元セッションのみを実行するデバイスまたはデバイススタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。

（注） SPAN の宛先ポートに QoS が設定されている場合、QoS はただちに有効になります。

- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。

- 送信元ポートにすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、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 および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化で次のように動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、これらのパケットに元のカプセル化が使用されます（タグなし、ISL、またはIEEE 802.1Q)。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、 **encapsulation replicate** が有効になっているローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合、元の VLAN ID を保持したまま RSPAN VLAN ID がパケットに挿入されます。

RSPAN VLAN

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

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

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

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

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッド トラフィックを監視しません。VSPAN は、 で受信または送信されるトラフィックのみをモニターし、VLAN間でルーティングされるトラフィックはモニターされません。たとえば、VLAN が受信モニターされ、 が別の VLAN からモニタリング対象 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ーされず、SPAN 宛先ポートで受信されません。

- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションが無効になると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。

- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。

- VTP：VTP を使用すると、 間で RSPAN VLAN のプルーニングが可能です。

- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバ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。 SPAN 宛先ポートとしては設定できません。グループが SPAN 送信元として設定されている場合、グループ全体が監視されます。

  監視対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。監視対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。

  EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータは監視されます。ただし、EtherChannel グ

ループに含まれる物理ポートをSPAN宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループ メンバのままですが、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。

  SPAN セッションでは、入力転送が宛先ポートで有効の場合、出力を監視しているポートでポート セキュリティを有効にしないでください。RSPAN 送信元セッションでは、出力を監視しているポートでポート セキュリティを有効にしないでください。
- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x を有効にできますが、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 セッションでは、入力転送が宛先ポートで有効の場合、出力を監視しているポートで IEEE 802.1x を有効にしないでください。RSPAN 送信元セッションでは、出力を監視しているポートで IEEE 802.1x を有効にしないでください。

SPAN と RSPAN とデバイス スタック

※ のスタックが 1 つの論理 を表すため、ローカル SPAN の送信元ポートと宛先ポートはスタック内で異なる に存在することがあります。したがって、 のスタック内での追加または削除は、RSPAN の送信元セッションまたは宛先セッションだけではなく、ローカル SPAN セッションにも影響を及ぼします。アクティブなセッションは、 がスタックから削除された場合に非アクティブになる可能性があり、非アクティブなセッションは、 がスタックに追加された場合にアクティブになる可能性があります。

フローベースの SPAN

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

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

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

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

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

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

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

SPAN および RSPAN のデフォルト設定

表 *4 : SPAN* および *RSPAN* のデフォルト設定

機能	デフォルト設定
SPAN のステート（SPAN および RSPAN）	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィック（**both**）の両方。
カプセル化タイプ（宛先ポート）	ネイティブ形式（タグなしパケット）
入力転送（宛先ポート）	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

SPAN および RSPAN の設定

SPAN および RSPAN の設定

SPAN 設定時の注意事項

- 送信元ポートまたは宛先ポート または VLAN を SPAN セッションから削除するには、 **no monitor session** *session_number* **source interface** *interface-id* {**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、 **encapsulation** オプションは、コマンドの × 形式で無視されます。
- トランクポート上のすべての VLAN をモニターするには、 **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。

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたはモニターできます。RSPAN 送信元 内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数の に分散させることができます。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
  - すべての で、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加しているすべての が RSPAN をサポートしている。

FSPAN および FRSPAN 設定時の注意事項

- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
- SPAN セッションに空ではない FSPAN ACL を少なくとも 1 つ接続し、ほかの 1 つまたは複数の FSPAN ACL を接続しなかった場合（たとえば、空ではない IPv4 ACL を接続し、IPv6 と MAC ACL を接続しなかった場合）、FSPAN は、接続されていない ACL によって

フィルタリングされたと思われるトラフィックをブロックします。したがって、このトラフィックは監視されません。

SPAN および RSPAN の設定方法

ここでは、SPAN および RSPAN の設定方法について説明します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**][**ingress**{**vlan** *vlan-id*}] }
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 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*に指定できる範囲は 1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。

	コマンドまたはアクション	目的
		• **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* } [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 1 source interface gigabitethernet1/1`	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*に指定できる範囲は 1 ～ 66 です。 • ※ *interface-id*には、モニター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。 • （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。 • （オプション） **both** | **rx** | **tx**：モニター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監視します。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックをモニタします。 （注） ※ **monitor session** *session_number* **source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンドまたはアクション	目的
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | -] [**encapsulation replicate**][**ingress**{**vlan** *vlan-id*}] } 例： `Device(config)# monitor session 1 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10`	（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。 • ※ *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。 •（オプション） **encapsulation replicate** 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。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** 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します。 • **vlan** *vlan-id*—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。 （注） ※ **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 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。

	コマンドまたはアクション	目的
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。

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定した後、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress**{**vlan** *vlan-id*}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 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*に指定できる範囲は 1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。

	コマンドまたはアクション	目的
		• **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* } [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 2 source gigabitethernet1/1 rx`	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。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress**{**vlan** *vlan-id*}]} 例： `Device(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10`	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 • ※ *session_number*には、ステップ 4 で入力したセッション番号を指定します。 • ※ *interface-id*には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**,** | **-**]：一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。 • （オプション） **encapsulation replicate** 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。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** 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します。 • **vlan** *vlan-id*—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
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。

フィルタリングする VLAN の指定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]
6. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**][**ingress**{**vlan** *vlan-id*}]}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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*に指定できる範囲は 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* } [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 2 source interface gigabitethernet1/2 rx`	送信元ポート（モニター対象ポート）と SPAN セッションの特性を指定します。 • ※ *session_number*に指定できる範囲は 1 ～ 66 です。 • ※ *interface-id*には、モニターする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例： `Device(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • ※ *session_number*には、ステップ 4 で指定したセッション番号を入力します。 • ※ *vlan-id*に指定できる範囲は 1 ～ 4094 です。 • （任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して、VLAN 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	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**][**ingress**{**vlan** *vlan-id*}]} 例： `Device(config)# monitor session 2 destination interface gigabitethernet1/1 ingress vlan 6`	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 • ※ *session_number*には、ステップ 4 で入力したセッション番号を指定します。 • ※ *interface-id*には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定す

	コマンドまたはアクション	目的
		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。 • （オプション） **encapsulation replicate** 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。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** 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します。 • **vlan** *vlan-id*—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**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。

RSPAN VLAN としての VLAN の設定

新しい VLAN を作成し、RSPAN セッション用の RSPAN VLAN になるように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **remote-span**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 100`	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーションモードを開始します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN 専用）にすることはできません。
ステップ 4	**remote-span** 例： `Device(config-vlan)# remote-span`	VLAN を RSPAN VLAN として設定します。
ステップ 5	**end** 例： `Device(config-vlan)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**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。

次のタスク

RSPAN に参加するすべてのデバイスに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つのデバイスに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のデバイスに伝播するように設定できます。拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のデバイス、および中間デバイスに RSPAN VLAN を設定する必要があります。

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

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

SPAN セッションから送信元ポートまたは VLAN を削除するには、 **no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、 **no monitor session** *session_number* **destination remote vlan** *vlan-id* コマンドを使用します。

RSPAN 送信元セッションの作成

RSPAN送信元セッションを作成および開始し、モニター対象の送信元および宛先RSPAN VLANを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination remote vlan** *vlan-id*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 1`	セッションに対する既存の SPAN 設定を削除します。 • ※ *session_number*に指定できる範囲は 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* } [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 1 source interface gigabitethernet1/1 tx`	RSPAN 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*に指定できる範囲は 1 ～ 66 です。 • RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 • ※ *interface-id*には、モニター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。 • 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送信元ポートと送信元 VLAN を併用することはできません。

	コマンドまたはアクション	目的
		• （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。 • （オプション） **both**	**rx**	**tx**：モニター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監視します。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックをモニタします。
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Device(config)# monitor session 1 destination remote vlan 100`	RSPAN セッション、宛先 RSPAN VLAN、および宛先ポート グループを指定します。 • ※ *session_number*には、ステップ 4 で定義した番号を入力します。 • ※ *vlan-id*には、モニターする送信元 RSPAN VLAN を指定します。
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。

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]
6. **monitor session** *session_number* **destination remote vlan** *vlan-id*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number*	**all**	**local**	**remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • ※ *session_number*に指定できる範囲は 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* } [**,**	**-**] [**both**	**rx**	**tx**] 例：	送信元ポート（モニター対象ポート）と SPAN セッションの特性を指定します。

	コマンドまたはアクション	目的
	`Device(config)# monitor session 2 source interface gigabitethernet1/2 rx`	• ※ *session_number*に指定できる範囲は 1 ～ 66 です。 • ※ *interface-id*には、モニターする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。 • （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。 • （オプション） **both** | **rx** | **tx** : モニター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監視します。 • **rx** : 受信トラフィックを監視します。 • **tx** : 送信トラフィックをモニタします。
ステップ 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例 : `Device(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • ※ *session_number*には、ステップ 4 で指定したセッション番号を入力します。 • ※ *vlan-id*に指定できる範囲は 1 ～ 4094 です。 • （オプション） **,**|**-** 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 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	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例 : `Device(config)# monitor session 2 destination remote vlan 902`	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 • ※ *session_number*には、ステップ 4 で指定したセッション番号を入力します。

	コマンドまたはアクション	目的
		• ※*vlan-id*には、宛先ポートにモニタリング対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**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。

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは、別のデバイスまたはデバイススタック（送信元セッションが設定されていないデバイスまたはデバイススタック）に設定します。

このデバイス上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **remote-span**
5. **exit**
6. **no monitor session** {*session_number* | **all** | **local** | **remote**}
7. **monitor session** *session_number* **source remote vlan** *vlan-id*
8. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**][**ingress**{**vlan** *vlan-id*}] }
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 901`	送信元デバイスで作成された RSPAN VLAN の VLAN ID を指定し、VLAN コンフィギュレーション モードを開始します。 両方のデバイスが VTP に参加し、RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 3 ～ 5 は不要です。
ステップ 4	**remote-span** 例： `Device(config-vlan)# remote-span`	VLAN を RSPAN VLAN として識別します。
ステップ 5	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 1`	セッションに対する既存の SPAN 設定を削除します。 • ※ *session_number*に指定できる範囲は 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。

	コマンドまたはアクション	目的
ステップ 7	**monitor session** *session_number* **source remote vlan** *vlan-id* 例： `Device(config)# monitor session 1 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • ※ *session_number*に指定できる範囲は 1 ～ 66 です。 • ※ *vlan-id*には、モニターする送信元 RSPAN VLAN を指定します。
ステップ 8	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**][**ingress**{**vlan** *vlan-id*}] } 例： `Device(config)# monitor session 1 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10`	RSPAN セッションと宛先インターフェイスを指定します。 • ※ *session_number*には、ステップ 7 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。 • ※ *interface-id*には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • （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。 • （オプション） **encapsulation replicate** 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。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** 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します。 • **vlan** *vlan-id*—デフォルトの VLAN として指定した VLAN で、タグなしのカプセル化タイプで着信パケットを受け入れます。 • ※ **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**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。

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source remote vlan** *vlan-id*
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress**{**vlan** *vlan-id*}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • ※ *session_number*に指定できる範囲は 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 remote vlan** *vlan-id* 例： `Device(config)# monitor session 2 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • ※ *session_number*に指定できる範囲は 1 ～ 66 です。 • ※ *vlan-id*には、モニターする送信元 RSPAN VLAN を指定します。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress**{**vlan** *vlan-id*}]} 例： `Device(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10`	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 • ※ *session_number*には、ステップ 5 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。 • ※ *interface-id*には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • コマンドラインのヘルプ文字列には表示されますが、 **encapsulation replicate** は RSPAN ではサポートされません。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。

	コマンドまたはアクション	目的
		• （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。 • Enter **ingress** を追加のキーワードと一緒に入力することで、宛先ポートでの着信トラフィックの転送を有効にして、カプセル化タイプを指定できます。 • **vlan** *vlan-id*—デフォルトの VLAN として指定した VLAN で、タグなしのカプセル化タイプで着信パケットを転送します。
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。

FSPAN セッションの設定

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定し、セッションに FSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**vlan** *vlan-id*}]}

6. **monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number*	**all**	**local**	**remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • ※ *session_number*に指定できる範囲は 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* } [**,**	-] [**both**	**rx**	**tx**] 例： `Device(config)# monitor session 2 source interface gigabitethernet1/1`	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*に指定できる範囲は 1 ～ 66 です。 • ※ *interface-id*には、モニター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。 • （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。

	コマンドまたはアクション	目的
		• （オプション） [**both** | **rx** | **tx**]：モニター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モニターします。 • **both**：送信トラフィックと受信トラフィックの両方を監視します。これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。 （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* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**vlan** *vlan-id*}]} 例： `Device(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 50`	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 • ※ *session_number*には、ステップ 4 で入力したセッション番号を指定します。 • ※ **destination**には、次のパラメータを指定します。 • ※ *interface-id*には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • （任意）**,** | **-**] 一連のインターフェイスまたはインターフェイス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。 • （オプション） **encapsulation replicate** 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。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** 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します。

	コマンドまたはアクション	目的
		• **vlan** *vlan-id*—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。 （注） ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 ※ **monitor session** *session_number* **destination** コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 6	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Device(config)# monitor session 2 filter ipv6 access-group 4`	SPAN セッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。 • ※ *session_number*には、ステップ 4 で入力したセッション番号を指定します。 • ※ *access-list-number*には、トラフィックのフィルタリングに使用する ACL 番号を指定します。 • ※ *name*には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**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。

FRSPAN セッションの設定

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定し、セッションに FRSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination remote vlan** *vlan-id*
6. **vlan** *vlan-id*
7. **remote-span**
8. **exit**
9. **monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*}
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session** {*session_number*	**all**	**local**	**remote**} 例： `Device(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • ※ *session_number*に指定できる範囲は 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。

	コマンドまたはアクション	目的
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* } [**,** | **-**] [**both** | **rx** | **tx**] 例： `Device(config)# monitor session 2 source interface gigabitethernet1/1`	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*に指定できる範囲は 1 ～ 66 です。 • ※ *interface-id*には、モニター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、モニターする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたはVLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）**,** | **-**]：一連のインターフェイスまたはインターフェイス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。 • （オプション） [**both** | **rx** | **tx**]：モニター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モニターします。 • **both**：送信トラフィックと受信トラフィックの両方を監視します。これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。 （注） ※ **monitor session** *session_number* **source** コマンドを複数回使用すると、複数の送信元ポートを設定できます。

	コマンドまたはアクション	目的
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Device(config)# monitor session 2 destination remote vlan 5`	RSPAN セッションと宛先 RSPAN VLAN を指定します。 • ※ *session_number*には、ステップ 4 で定義した番号を入力します。 • ※ *vlan-id*には、モニタリングする宛先 RSPAN VLAN を指定します。
ステップ 6	**vlan** *vlan-id* 例： `Device(config)# vlan 10`	VLAN コンフィギュレーション モードを開始します。※ *vlan-id*には、モニターする送信元 RSPAN VLAN を指定します。
ステップ 7	**remote-span** 例： `Device(config-vlan)# remote-span`	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを指定します。
ステップ 8	**exit** 例： `Device(config-vlan)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Device(config)# monitor session 2 filter ip access-group 7`	RSPAN セッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 • ※ *session_number*には、ステップ 4 で入力したセッション番号を指定します。 • ※ *access-list-number*には、トラフィックのフィルタリングに使用する ACL 番号を指定します。 • ※ *name*には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 12	**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 および RSPAN 動作のモニタリング

次の表で、SPAN および RSPAN 動作の設定と結果を表示して動作をモニタするために使用するコマンドについて説明します。

表 *5 : SPAN* および *RSPAN* 動作のモニタリング

コマンド	目的
show monitor	現在の SPAN、RSPA 示します。

SPAN および RSPAN の設定例

次のセクションに SPAN および RSPAN の設定例を示します

例：ローカル SPAN の設定

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 gigabitethernet1/1
Device(config)# monitor session 1 destination interface gigabitethernet1/2
encapsulation replicate ingress vlan 7
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 gigabitethernet1/1
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 gigabitethernet1/1 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 gigabitethernet1/2
Device(config)# monitor session 2 source vlan 10
Device(config)# end
```

次に、SPANセッション2の既存の設定を削除し、ギガビットイーサネット ソース送信元ポート1上で受信される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、その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の宛先ギガビット イーサネット ポート 2 に送信し、デフォルト入力 VLAN として VLAN 6 を使用した入力転送をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source gigabitethernet0/1 rx
Device(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
 replicate ingress vlan 6
Device(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニターするように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination interface gigabitethernet1/1 ingress vlan
 10
Device(config)# end
```

例：RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# vlan 901
Device(config-vlan)# remote span
Device(config-vlan)# end
```

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

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/1 tx
Device(config)# monitor session 1 source interface gigabitethernet1/2 rx
Device(config)# monitor session 1 source interface port-channel 2
Device(config)# monitor session 1 destination remote vlan 901
Device(config)# end
```

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

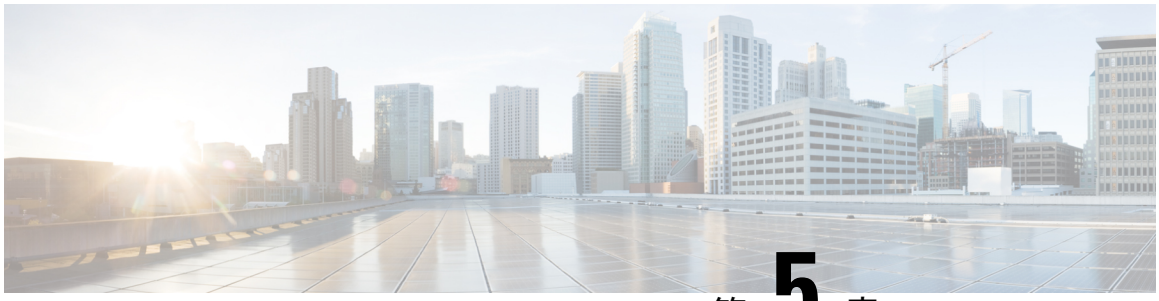
```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination remote vlan 902
Device(config)# end
```

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 source remote vlan 901
Device(config)# monitor session 1 destination interface gigabitethernet2/1 ingress vlan
 10
Device(config)# end
```

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

```
Device> enable
Device# configure terminal
Device(config)# monitor session 2 source remote vlan 901
Device(config)# monitor session 2 destination interface gigabitethernet1/2 ingress vlan 6
Device(config)# end
```



第 5 章

産業資産検出の設定

産業資産検出に関する情報

産業資産検出（IAD）機能を使用すると、直接接続されたエンドデバイスの詳細を表示できます。IAD は、Common Industrial Protocol（CIP）や Profinet などの産業用プロトコルに含まれる検出メッセージを使用して、これらの詳細を検出します。IE スイッチは CIP および Profinet デバイスと同じプロトコルメッセージを使用しているため、エンドデバイスへの影響はありません。エンドデバイスは正常に応答します。

産業用ネットワークには、制御プロセスの自動化に使用されるプログラマブル ロジック コントローラ（PLC）やインテリジェント電子機器（IED）などのエンドデバイスが含まれます。これらのデバイスは、CIP や Profinet などのプロトコルを実行してエンドデバイスをモニター、制御、および管理する、 遠隔監視制御・情報取得（SCADA）アプリケーションに接続されます。一元化された CIP/Profinet コントローラは、ブロードキャスト検出によってデバイス情報を収集し、デバイス インベントリ データベースを維持します。ただし、この情報には、オペレータがエンドデバイスを物理的に見つけて追跡するのに役立つ、スイッチ、インターフェイス、ロケーション、VLAN などのエンドデバイスのレイヤ 2 ネットワーク接続情報は含まれません。

IAD 検出により、詳細なロケーションおよびレイヤ 2 接続情報をエンドデバイスから収集できます。このデバイス情報は、スイッチ上のローカルデータベースで処理および維持されます。CIP/Profinet 検出によって収集された情報は、IP デバイストラッキング情報と組み合わせて、エンドデバイスに関する詳細情報を提供できます。

産業資産検出動作

IADが有効になっている場合、IEスイッチが起動した後、IADは事前に定義された時間待機してから、有効になっている産業用プロトコルに検出メッセージを送信します。その後、通知は定期的に送信されます。この間隔は、 **iad refresh-interval** コマンドを使用して設定できます。コマンドで設定するIPアドレスが含まれていることを確認します。IADの任意またはすべてのプロトコル（CIP、Profinet、IP Device Tracking（IPDT）、Cisco Discovery Protocol（CDP）、およびLink Layer Discovery Protocol（LLDP））の検出を有効または無効にできます。

インターフェイスがダウンし、復旧すると、データベースは自動的に更新されます。リンクフラップイベントが発生すると、IADは通知を送信し、 事前に定義された時間間隔を待機してから次の検出メッセージを送信します。これは、過剰な検出メッセージの送信を回避するのに役立ちます。

CIP、Profinet、IPDT、またはCDPとLLDPを介して受信したデバイス情報は照合され、ローカルデータベースに保存されます。ネットワーク内の各アクセススイッチは、独自のIADデータベースを維持します。ローカルデータベースは、設定可能なタイマー値に基づいて動的に更新されます。IAD検出の一部としてエンドデバイスに関して収集される情報には、次のものが含まれます。

- インターフェイス ステータス
- IP-Address
- MAC アドレス
- シリアル番号
- デバイス PID
- ベンダー
- デバイスタイプ
- ソフトウェアのバージョン
- プロトコル
- タイムスタンプ

出力結果は、エンドデバイスが設定されているネットワークによって異なります。

注意事項と制約事項

- IADは、IE3200、IE3300、およびIE3400/IE3400Hプラットフォームでのみサポートされます。
- CIP/Profinetでは、エンドデバイスがアクセスポートを介して接続され、スイッチ間のピアリンクがトランクポートを介して接続されていることが前提となっています。トランク

インターフェイスで検出されたエンドデバイスは、ローカルデータベースに追加されません。

- インターフェイスがダウンすると、そのインターフェイスに関連するすべてのレコードが削除されます。インターフェイスが再稼働すると、検出メッセージが開始され、レコードが収集されます。
- CIP および Profinet 検出メッセージの場合、スイッチ仮想インターフェイス（SVI）VLAN インターフェイスに IP アドレスを割り当てる必要があります。同じ VLAN が Profinet または CIP デバイスに使用されます。
- 最大 100 個のレコードを IAD データベースに保存できます。インターフェイスで受信されるレコードの数に制限はありません。
- SNMP および YANG はサポートされていません。

デフォルト設定

IAD はデフォルトで無効になっています。

IAD が有効になっている場合のデフォルト設定は次のとおりです。

- 検出メッセージが、CIP および Profinet に対して送信されます。IPDT も有効になっています。プロトコルサブシステムが、対応するディスカバリメッセージを送信し、レコードを収集します。
- レコードが CDP および LLDP から受信されます。
- プロトコル通知を送信してローカルデータベースを更新するデフォルトの更新間隔は 6 時間です。

産業資産検出の設定

始める前に

IAD に対して有効にするプロトコルがスイッチレベルで有効になっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	`configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`iad enable [cdp | cip | ipdt | lldp | profinet]`	指定されたプロトコルの IAD を有効にします。

	コマンドまたはアクション	目的
		プロトコルが指定されていない場合、IADはすべてのプロトコルに対して有効になります。
ステップ3	`iad refresh-interval` *interval*	CIP/Profinet検出パケットが送信されるレートを指定します（秒単位）。 範囲は60～86400です。デフォルトは21,600（6時間）です。

例

次に、CIPおよびProfinetのIADを設定し、更新間隔を3時間に設定する例を示します。

```
IE3400_IAD#config t
IE3400_IAD(config)#iad enable cip
IE3400_IAD(config)#iad enable profinet
IE3400_IAD(config)#iad refresh-interval 10800
```

産業資産検出情報の確認

IADインベントリと設定ステータスを表示するには、次のコマンドを使用します。

コマンド	説明

show iad inventory [all | interface | protocol]	IADデバイスインベントリを表示します。
	• all：表形式のすべてのデバイスレコード
	• interface：インターフェイスでレコードをフィルタリングします
	• protocol：次のプロトコルでレコードをフィルタリングします
	  • cdp
	  • cip
	  • ipdt
	  • lldp
	  • profinet

show iad status	現在のIAD設定ステータスを表示します。

次に、IADステータスを確認する例を示します。

```
IE3400#show iad status
IAD Information:
Status : Enabled
Send/Receive Notification to CDP : Enabled
Send/Receive Notification to CIP : Enabled
Send/Receive Notification to IPDT : Enabled
Send/Receive Notification to LLDP : Enabled
Send/Receive Notification to PROFINET : Enabled
Last discovery sent for CIP/Profinet : 14:41:47 UTC Wed Nov 15 2023
IAD Records Refresh Interval Rate : 10 secs
```

次に、IAD インベントリを確認する例を示します。

```
IE3400#show iad inventory all
Capability codes:
    (R) Router, (B) Source Route Bridge, (T) Telephone, (H) Host
    (C) DOCSIS Cable Device (W) WLAN Access Point (P) Repeater
    (G) Trans Bridge, (F) Switch, (I) IGMP, (E) Phone, (S) Station
    (D) Remote, (A) CVTA, (M) Two-port Mac Relay, (O) Other
Interface  Status      IP-Address        Mac Addr        Serial No    Device PID
Vendor          Device Type  SW ver       Protocol      Last Reported Time
---------- ------ ---------------   -----------------   -----------  ---------------
---------- ------------ ------------ ------------- --------------------
Gi2/5      UP     10.76.29.205      0C:75:BD:C8:68:29   Unknown      IE-3400-8P2S
Unknown    B,R          17.14.202310 CDP,LLDP      16:39:56 UTC Tue Nov 21 2023
Gi2/2      UP     Unknown           AC:64:17:65:D4:A9   Unknown      ET200MP
SIEMENS A  IO           Unknown      PROFINET      16:39:49 UTC Tue Nov 21 2023
Gi1/7      UP     29.29.29.60       38:4B:24:6A:A6:48   Unknown      SCALANCE XC-200
SIEMENS A  IO           Unknown      PROFINET      16:39:49 UTC Tue Nov 21 2023
Gi1/6      UP     192.168.1.8       00:00:BC:D1:2E:DB   8467751      1756-EN2T/C
Rockwell   EtherNet/IP  Unknown      CIP           16:39:48 UTC Tue Nov 21 2023
Gi2/8      UP     192.168.1.30      A4:53:0E:91:E9:61   1049749832   IE-3400H-24T-E
Cisco Sys  Switch       Unknown      CIP           16:39:48 UTC Tue Nov 21 2023
Gi2/4      UP     192.168.1.10      00:29:C2:3C:09:8B   943458688    IE-3200-8T2S
Cisco Sys  Switch       Unknown      CIP           16:39:48 UTC Tue Nov 21 2023
Gi2/3      UP     Unknown           D0:EC:35:58:53:04   Unknown      IE-3400-8T2S
Unknown    R,F,I        17.13.202310 CDP           16:39:53 UTC Tue Nov 21 2023

Total entries displayed : 7
```

産業資産検出の機能履歴

機能名	リリース	説明
産業資産検出（IAD）	Cisco IOS XE 17.14.1	IE3200、IE3300、および IE3400/IE3400H シリーズ スイッチの初期リリース

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。