# NetFlow の設定

この章では、Cisco NX-OS デバイス上で NetFlow 機能を設定する方法について説明します。

この章は、次の内容で構成されています。


- NetFlow について （1 ページ）
- NetFlow の前提条件 （5 ページ）
- NetFlow に関する注意事項および制約事項 （5 ページ）
- NetFlow の構成 （10 ページ）
- NetFlow 構成の確認 （22 ページ）
- NetFlow のモニタリング （22 ページ）
- NetFlow の表示例 （22 ページ）
- NetFlow の構成例 （23 ページ）


## NetFlow について

NetFlow は入力 IP パケットについてパケット フローを識別し、各パケット フローに基づいて統計情報を提供します。NetFlow のためにパケットやネットワーキング デバイスを変更する必要はありません。

NetFlow ではフローを使用して、アカウンティング、ネットワーク モニタリング、およびネットワーク プランニングに関連する統計情報を提供します。フローは送信元インターフェイス（VLAN 向け）に届く単方向のパケット ストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。フローを作成するには、フロー レコードを使用して、フロー固有のキーを定義します。

Cisco NX-OS は、ネットワーク異常とセキュリティ問題の高度な検出を有効にする Flexible NetFlow 機能をサポートします。フレクシブル NetFlow 機能を使用すると、大量の定義済みフィールドの集合からキーを選択することで、そのアプリケーションに最適なフロー レコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。フローは、設定したエクスポート レコード バージョンに基づいて、関係のある他のフィールドを集めることもあります。フローは NetFlow キャッシュに格納されます。

フロー用に NetFlow が収集したデータをエクスポートするには、フロー エクスポータを使用し、このデータを Cisco Stealthwatch などのリモート NetFlow コレクタにエクスポートします。Cisco NX-OS は次の状況で、NetFlow エクスポート用のユーザ データグラム プロトコル（UDP）データグラムの一部としてフローをエクスポートします。

- フローはフロータイムアウト値に従って定期的にエクスポートされます。設定されていない場合、デフォルトは 10 秒です。
- ユーザがフローの強制的エクスポートを行った。

フロー レコードによってフロー用に収集するデータのサイズが決まります。フローモニタで、フロー レコードおよびフロー エクスポータを NetFlow キャッシュ情報と結合します。

Cisco NX-OS は NetFlow 統計を集計し、インターフェイスまたはサブインターフェイス上のすべてのパケットを分析します。

# デュアルレイヤ NetFlow の実装

他の Cisco Nexus プラットフォームとは異なり、Cisco Nexus 9000 シリーズ スイッチは、NetFlow 処理を次の 2 つのレイヤに分離します。

- 第 1 レイヤは、ラインレート トラフィックのパケット単位の可視性をサポートします。パケットをサンプリングして統計的に分析する必要はありません。代わりに、パケットをライン レートで処理および集約できます。
- 2 番目のレイヤは、大規模なフローの収集を可能にします。フローを失うことなく何十万ものフローを維持でき、定期的に外部コレクタにエクスポートします。

# フロー レコード

フロー レコードでは、パケットを識別するために NetFlow で使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フローレコードを定義できます。Cisco NX-OS は、様々なキーセットをサポートしています。フローレコードでは、フロー単位で収集するカウンタのタイプも定義します。32 ビットまたは 64 ビットのパケット カウンタまたはバイト カウンタを設定できます。

キー フィールドは、**match** キーワードで指定されます。対象フィールドとカウンタは **collect** キーワードで指定されます。

Cisco NX-OS では、フロー レコードの作成時に次の match フィールドをデフォルトとして使用できます。

- match interface input
- match flow direction

# フロー エクスポータ

フローエクスポータでは、NetFlowエクスポートパケットに関して、ネットワーク層およびトランスポート層の詳細を指定します。フロー エクスポータで設定できる情報は次のとおりです。

- エクスポート宛先 IP アドレス
- 送信元インターフェイス
- UDP ポート番号（NetFlow コレクタが NetFlow パケットをリスニングするところ）：デフォルト値は 9995 です。

（注） NetFlow エクスポート パケットでは、送信元インターフェイスに割り当てられた IP アドレスを使用します。送信元インターフェイスを設定しない場合、フローエクスポータはエクスポートする予定のフローをドロップします。[Netflowエクスポータの送信元インターフェイスと接続先 IP は、同じ VRF を使用する必要があります。（The Netflow Exporter source interface and destination IP must use the same VRF.）]

Cisco NX-OS は、タイムアウトが発生するたびにデータを NetFlow コレクタへエクスポートします。キャッシュをフラッシュし、フローを強制的にエクスポートするには、フラッシュキャッシュ タイムアウトを設定できます（**flow timeout** コマンドを使用）。

# エクスポート形式

Cisco NX-OS は、バージョン 9 のエクスポート形式をサポートします。この形式は、古いバージョン5のエクスポート形式よりも効率的なネットワーク使用率をサポートし、IPv6およびレイヤ 2 フィールドをサポートします。さらに、バージョン 9 エクスポート形式は、NetFlow コレクタで完全な 32 ビット SNMP ifIndex 値をサポートします。

# レイヤ 2 NetFlow キー

フレクシブル NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。レイヤ 2 のキーは次のとおりです。

- 送信元および宛先 MAC アドレス
- 送信元 VLAN ID
- イーサネット フレームのイーサネット タイプ

受信方向については、次のインターフェイスに対してレイヤ 2 NetFlow を適用できます。

- アクセス モードのスイッチ ポート

- トランク モードのスイッチ ポート
- レイヤ 2 のポート チャネル

（注） Layer 2 NetFlow を VLAN、送信インターフェイス、またはレイヤ 3 インターフェイス（VLAN インターフェイスなど）に適用できます。

## フロー モニタ

フロー モニタは、フロー レコードおよびフロー エクスポータを参照します。フロー モニタはインターフェイスに適用します。

## NetFlow 出力インターフェイス

FM-E および FM-E2 モジュールを搭載した Cisco Nexus 9300-FX/FX3 および Cisco Nexus 9500 プラットフォーム スイッチの NetFlow 出力インターフェイスには、次の機能があります。

- **show flow cache** コマンドの NetFlow は `output_if_id` を表示し、出力インターフェイスを 9700-EX ライン カードを備えた Cisco Nexus 9300-FX および 9500 プラットフォーム スイッチのコレクタにエクスポートします。
- Cisco Nexus 9300-FX/FX3 プラットフォーム スイッチの NetFlow 出力インターフェイスは、IPv4 と IPv6 の両方のトラフィック フローをサポートします。Cisco Nexus 9500 プラットフォーム スイッチの NetFlow 出力インターフェイスは、IPv4 トラフィック フローでのみサポートされ、IPv6 トラフィック フローではサポートされません。
- **show flow cache** コマンドは、`output_if_id` を `0x0` またこの機能は、コントロール プレーン トラフィックや ICMP 要求/応答メッセージなど、スイッチ宛てのトラフィック以外のトラフィックでもサポートされます。
- NetFlow は、宛先インターフェイスとしてネクストホップを持つ IPv4/IPv6 着信トラフィック フローのコレクタへの出力インターフェイスのエクスポートをサポートします。`InputInt` および `OutputInt` の NetFlow エクスポート形式は、NetFlow コレクタで完全な 32 ビット SNMP `ifIndex` 値をサポートします。
- NetFlow 出力インターフェイスは、MPLS、VXLAN、GRE などのトンネル トラフィック フローではサポートされません。
- NetFlow 出力インターフェイスの例の詳細については、NetFlow の表示例 （22 ページ）を参照してください。

# 高可用性

Cisco NX-OS は NetFlow のステートフル リスタートをサポートします。リブート後、Cisco NX-OS は実行コンフィギュレーションを適用します。

フローキャッシュは再起動で保持されず、再起動中にソフトウェアに送信されるパケットは処理されません。

# NetFlow の前提条件

NetFlow の前提条件は、次のとおりです。

- 使用しているデバイスで必要とされるリソースを正しく理解していること。NetFlow はメモリと CPU リソースを消費するからです。

# NetFlow に関する注意事項および制約事項

（注） スケールの情報については、リリース特定の『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。

NetFlow に関する構成の注意事項および制約事項は、次のとおりです。

- Cisco Nexus 9300-FX プラットフォーム スイッチに対して、レイヤ 2 NetFlow に対してすでに設定されているポート チャネルにメンバを追加すると、NetFlow の設定が削除され、ポート チャネルのレイヤ 2 設定が追加されます。
- NetFlow はトンネル インターフェイスではサポートされていません。
- NetFlowは、CPU で送信されるパケットではサポートされません。
- 入力 NetFlow のみがサポートされます。出力 NetFlow はサポートされていません。
- フローキャッシュは、レイヤ2、IPv4、IPv6などのフロータイプごとにクリアできます。フロー モニタごとにクリアすることはできません。
- Nexus 9000 スイッチでは、NetFlow は ICMP フロー情報を収集してコレクタに送信します。ICMP タイプとコードはパケットに本質的に含まれます。NetFlow またはフローエクスポート レコード内の ICMP パケットは、TCP や UDP などの従来の送信元および宛先ポートを使用しません。代わりに、エクスポータは ICMP タイプとコードを SPORT（送信元ポート）や DPORT（宛先ポート）などのフィールドにエンコードすることがよくあります。次に例を示します。
  - ICMP Echo Request: SPORT=2048, DPORT=0
  - ICMP Echo Reply: SPORT=0, DPORT=0

    - ICMP Time Exceeded: SPORT=2816, DPORT=0

- フロー収集は ARP トラフィックに対して実行されません。
- NetFlowデータエクスポート（NDE）では、送信元インターフェイスを設定する必要があります。送信元インターフェイスを設定しない場合、フローエクスポータはエクスポートする予定のフローをドロップします。
- レイヤ 2 スイッチド フロー モニタは、レイヤ 2 インターフェイスにのみ適用されます。IP および IPv6 フロー モニタは、VLAN、SVI、レイヤ 3 ルーテッド インターフェイス、またはサブインターフェイスに適用できます。
- レイヤ 2 インターフェイスをレイヤ 3 インターフェイスへ変更するか、レイヤ 3 インターフェイスをレイヤ2インターフェイスへ変更すると、ソフトウェアで、インターフェイスからレイヤ 2 の NetFlow 設定が削除されます。
- 同じフロー モニタを VLAN およびレイヤ 3 インターフェイス（物理レイヤ 3 インターフェイス、SVI インターフェイス、またはレイヤ 3 サブインターフェイスなど）と共有することはできません。ACL は異なるため共有できないため、VLAN とレイヤ 3 インターフェイスを区別する必要があります。これらは 2 つの異なるプロファイルとして扱う必要があります。
- ロールバック中、ハードウェアでプログラムされているレコードを変更しようとすると、ロールバックは失敗します。
- NetFlow 機能の制限は次のとおりです。
    - MPLS/VXLAN データパスの NetFlow はサポートされていません
    - NetFlow は、ループバックおよびスイッチ管理インターフェイスではサポートされません。
- VXLAN 環境の NetFlow には、次のガイドラインと制限事項が適用されます。
    - NetFlow は、VXLAN VTEP の SVI および非アップリンク L3 インターフェイスでサポートされます。これには L3VNI SVI は含まれません。
    - NetFlow は、VXLAN VTEP のアップリンク インターフェイスではサポートされません。
    - マルチサイト境界ゲートウェイでの NetFlow はサポートされていません。
    - VXLAN ファブリックを介して到達可能な NetFlow コレクタがサポートされています。
- Cisco NX-OS リリース 9.2(1) 以降：
    - FEX レイヤ 3 ポートの NetFlow は Cisco Nexus 9300 EX と 9300 FX プラットフォーム スイッチでサポートされています。
    - Cisco Nexus 9300-EX プラットフォーム スイッチで NetFlow CE がサポートされています。

（注） すべての EX タイプのプラットフォームス イッチ（Cisco Nexus 9700-EX ライン カードを含む）では、CE NetFlow は非 IPv4 および IPv6 トラフィック フローの CE フローレコードのみをキャプチャします。FX および FX2 タイプのプラットフォーム スイッチとライン カードでは、 **mac packet-classify** がインターフェイスに適用されている限り、IP フローの CE フロー データをキャプチャできます。

- Cisco NX-OS リリース 9.2(2) 以降、Cisco Nexus 9300-FX スイッチは NetFlow データ エクスポート（NDE）の OUTPUT_SNMP フィールドの収集をサポートしています。他の Cisco Nexus 9000 プラットフォーム スイッチまたは Cisco Nexus ライン カードは、OUTPUT_SNMP フィールドの収集をサポートしていません。
- Cisco NX-OS リリース9.2(2) 以降では、NetFlow はCisco Nexus 9700-EX ライン カードと FM-E モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。
- NetFlow は、Cisco Nexus 92348GC-X プラットフォーム スイッチではサポートされていません。
- Cisco Nexus 9300-EX プラットフォーム スイッチの場合、VLAN または SVI に適用されたフロー モニタは、スイッチド トラフィックとルーテッド トラフィックの両方のフローを収集できます。Cisco Nexus 9300-FX プラットフォーム スイッチの場合、NetFlow VLAN はスイッチド トラフィックに対してのみサポートされ、NetFlow SVI はルーテッド トラフィックに対してのみサポートされます。
- Cisco Nexus 9300-EX プラットフォーム スイッチは、同じインターフェイスで NetFlow と SPAN を同時にサポートします。この機能は、SPAN および sFlow の代わりに使用できます。
- Cisco Nexus 9300-EX/FX プラットフォーム スイッチ、および EX/FX モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、SPAN と sFlow の両方を同時に有効にすることはできません。一方がアクティブな場合、もう一方は有効にできません。ただし、Cisco Nexus 9300-EX/FX/FX2 および EX モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、NetFlow と SPAN の両方を同時に有効にすることができ、sFlow と SPAN を使用する代わりに実行可能です。

（注） Cisco Nexus 9300-FX2 プラットフォーム スイッチは、sFlow と SPAN の共存をサポートします。

- Cisco Nexus 9300-EX プラットフォーム スイッチでは、同じフロー モニタを VLAN と SVI に同時に接続することはできません。

- Cisco Nexus 9300-EX プラットフォーム スイッチには専用の TCAM があり、カービングは必要ありません。
- ing-netflow リージョンの TCAM カービング設定は、FX ライン カードでは実行できます。EX ライン カードでは、デフォルトの ing-netflow リージョン TCAM カービングが 1024 であり、それ以外の場合は設定できません。EX および FX ライン カードのポートの場合、ing-netflow リージョンの推奨最大値は 1024 です。
- ToS フィールドは、Cisco Nexus 9300-EX プラットフォーム スイッチではエクスポートされません。
- IP ToS に基づくレコード一致は、IPv6 フロー モニタではサポートされません。ToS 値は、トラフィックが保持する値に関係なく、コレクタで 0x0 として収集されます。

  この制限は、次のプラットフォーム スイッチ ファミリに適用されます。

  - Cisco Nexus 9300-EX
  - Cisco Nexus 9300-FX
  - Cisco Nexus 9300-FX2
  - Cisco Nexus 9300-FX3
  - Cisco Nexus 9300-GX
  - EX または FX ライン カード搭載の Cisco Nexus 9500

- 次の注意事項は、EX および FX ライン カード搭載のすべての Cisco Nexus 9500 プラットフォーム スイッチに適用されます。

  FX ポートがすでに適用されている NetFlow 設定のトランクである場合、EX ポートをトランクとして設定しても、サポートされていない EX NetFlow 設定は FX ポート トランクから削除されません。たとえば、3 つ以上の異なる IPv4 フロー モニタを FX ポート トランクに適用し、EX ポートが同じトランクに追加された場合、EX ポートの制限のみであるため、2 つのモニタを超えるトランクの設定は自動的に削除されません。この設定では、EX トランク ポートの 2 つのモニタを超えるフローはレポートされないため、EX ポートと FX ポートの両方が同じトランクに存在する可能性があるモジュラ スイッチでは、プロトコルごとに 2 つのモニタ（v4/v6/CE）のみを使用することを推奨します。

-
- **record netflow ipv4 original-input**、**record netflow ipv4 original-output**、および **record netflow layer2-switched input** コマンドは、Cisco NX-OS リリース 9.3(1) ではサポートされていません。
- Cisco NX-OS リリース 9.3(3) 以降、NetFlow に関する次の無停止インサービス ソフトウェア アップグレード（ND ISSU）の制限がすべての Cisco Nexus 9000 シリーズ スイッチに適用されます。

  - ND ISSU の実行中、2 分間のエクスポート損失が予想されます。

- ND ISSU 中は、管理インターフェイスの送信元ポートを持つエクスポータはサポートされません。エクスポート損失は、管理インターフェイスが起動するまで予想されます。

- Cisco NX-OS リリース 9.3(3) 以降、入力 NetFlow は Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース9.3（4）以降では、次のRTP / NetFlowモニタリング制限が存在します。

  RTP モニタリング機能は、スイッチのすべてのインターフェイスで RTP フローのモニタをイネーブルにし、**show flow rtp detail** コマンド出力で報告します。RTP フローは、16384 ー32767 の範囲内の送信元ポートを持つ UDP フローです。RTP モニタリングがイネーブルになっているスイッチインターフェイスにNetFlowモニタが接続されている場合、そのインターフェイス上のすべてのトラフィック/フロー（RTP フローを含む）が **show flow cache** コマンドの出力で報告されます。RTP フローは、**show flow rtp detail** コマンドの出力に表示されなくなります。接続されたモニタが削除されると、RTP フローが **show flow rtp detail** コマンド出力で再度報告されます。

  この制限は、次のスイッチに影響します。

  - Cisco Nexus 9336C-FX2
  - Cisco Nexus 93240YC-FX2
  - Cisco Nexus 9348GC-FXP
  - Cisco Nexus 93180YC-FX
  - Cisco Nexus 93108TC-FX
  - Cisco Nexus 9316D-GX
  - Cisco Nexus 93600CD-GX
  - Cisco Nexus 9364C-GX
  - 9636C-RX ライン カードを搭載した Cisco Nexus 9504、9508 および 9516 スイッチ

- FM-E、FM-E2、および FM-E3 モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチおよびCisco Nexus 9300-FX/FX3 スイッチは、NetFlow 出力インターフェイスには機能をサポートします。ただし、9300-EX および 9500-EX プラットフォーム スイッチの出力インターフェイスはサポートされません。
- NetFlow は、EX、FX、および GX 混合シャーシの Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。EX、FX、およびGX混合シャーシのCisco Nexus 9500プラットフォーム スイッチでは、SPAN を NetFlow と同時に使用できます。Cisco Nexus 9500-GX プラットフォーム スイッチは、sFlow 機能を組み合わせた SPAN をサポートしていません。
- Cisco Nexus 3232C および 3264Q スイッチは、NetFlow をサポートしていません。

- Cisco NX-OS リリース 10.1(2) 以降、Netflow は N9K-X9716D-GX ライン カードでサポートされます。
- この機能をサポートするプラットフォームでのみ NetFlow を有効にします。
- **match ip tos** コマンドはフロー レコード設定オプションにありますが、機能はサポートされていません。
- Cisco NX-OS リリース 10.2(1)F 以降、レイヤ 2 インターフェイス上のレイヤ 3 NetFlow は、Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-FX3、9300-GX、および 9300-GX2 プラットフォーム、9500-EX LC および 9500-FX LC でサポートされます。注意事項と制約事項は次のとおりです。
  - レイヤ 3 フロー モニタまたはレイヤ 2 フロー モニタのいずれかをレイヤ 2 インターフェイスに接続できます（両方は接続できません）。
  - フローモニタがすでにレイヤ3インターフェイスに接続されている場合、同じフローモニタをレイヤ 2 インターフェイスに接続することはできません。
  - レイヤ 3 フロー モニタがレイヤ 2 インターフェイスに適用されている場合、**mac-packet-classify** コマンドはサポートされません。

（注） 確認済みの NetFlow のスケール数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

# NetFlow の構成

NetFlow を設定する手順は、次のとおりです。

手順

**ステップ 1** NetFlow 機能を有効化します。

**ステップ 2** フローにキーおよびフィールドを指定することによって、フロー レコードを定義します。

**ステップ 3** エクスポート フォーマット、プロトコル、宛先、およびその他のパラメータを指定することによって、任意でフロー エクスポータを定義します。

**ステップ 4** フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを定義します。

**ステップ 5** 送信元インターフェイス、サブインターフェイス、または VLAN インターフェイスにフロー モニタを適用します。

# NetFlow 機能の有効化

フローを設定するには、先に NetFlow をグローバルで有効しておく必要があります。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | グローバル設定モードを開始します。 |
| ステップ 2 | [**no**] **feature netflow**<br>例：<br>`switch(config)# feature netflow` | NetFlow 機能を有効にします。デフォルトではディセーブルになっています。<br>（注）<br>N9K-T2 EoR を搭載した Cisco Nexus 9500 プラットフォーム スイッチは、NetFlow をサポートしていません。 |
| ステップ 3 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

# フロー レコードの作成

フロー レコードを作成し、照合するためのキー、および収集するための非キー フィールドをフロー内に追加します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | 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 | **flow record** *name*<br>例：<br>`switch(config)# flow record Test`<br>`switch(config-flow-record)#` | フロー レコードを作成し、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。フロー レコード名には最大 63 文字の英数字を入力できます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | （任意） **description** *string*<br>例：<br>`switch(config-flow-record)# description IPv4Flow` | 最大 63 文字で、フロー レコードの説明を示します。 |
| ステップ 4 | （任意） **match** *type*<br>例：<br>`switch(config-flow-record)# match transport destination-port` | 一致キーを指定します。詳細については、match パラメータの指定 （12 ページ）を参照してください。<br>（注）<br>レイヤ4ポートデータをエクスポートするには、**match transport destination-port** および **match ip protocol** コマンドが必要です。 |
| ステップ 5 | （任意） **collect** *type*<br>例：<br>`switch(config-flow-record)# collect counter packets` | コレクションフィールドを指定します。詳細については、collect パラメータの指定 （13 ページ）を参照してください。 |
| ステップ 6 | （任意） **show flow record** [*name*] [*record-name*] {**netflow-original** \| **netflow protocol-port** \| **netflow** {**ipv4** \| **ipv6**} {**original-input** \| **original-output**}}<br>例：<br>`switch(config-flow-record)# show flow record netflow protocol-port` | NetFlow のフロー レコード情報を表示します。フロー レコード名には最大 63 文字の英数字を入力できます。 |
| ステップ 7 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config-flow-record)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

## match パラメータの指定

フロー レコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

| コマンド | 目的 |
|---|---|
| **match datalink** {**mac source-address** \| **mac destination-address** \| **ethertype** \| **vlan**}<br>**例:**<br>`switch(config-flow-record)# match datalink ethertype` | レイヤ 2 属性をキーとして指定します。 |

| コマンド | 目的 |
| --- | --- |
| **match ip** {**protocol** \| **tos**}<br>**例:**<br>`switch(config-flow-record)# match ip protocol` | IP プロトコルまたは ToS フィールドをキーとして指定します。<br>（注）<br>レイヤ 4 ポートデータをエクスポートするには、**match transport destination-port** および **match ip protocol** コマンドが必要です。<br>データは **show hardware flow ip** コマンドの出力に収集されて表示されますが、両方のコマンドを設定するまで収集とエクスポートは行われません。 |
| **match ipv4** {**destination address** \| **source address**}<br>**例:**<br>`switch(config-flow-record)# match ipv4 destination address` | IPv4 送信元または宛先アドレスをキーとして指定します。 |
| **match ipv6** {**destination address** \| **source address** \| **flow-label** \| **options**}<br>**例:**<br>`switch(config-flow-record)# match ipv6 flow-label` | IPv6 キーを指定します。 |
| **match transport** {**destination-port** \| **source-port**}<br>**例:**<br>`switch(config-flow-record)# match transport destination-port` | トランスポート送信元または宛先ポートをキーとして指定します。<br>（注）<br>レイヤ 4 ポートデータをエクスポートするには、**match transport destination-port** および **match ip protocol** コマンドが必要です。<br>データは **show hardware flow ip** コマンドの出力に収集されて表示されますが、両方のコマンドを設定するまで収集とエクスポートは行われません。 |

## collect パラメータの指定

フロー レコードごとに、次の collect パラメータを 1 つ以上設定する必要があります。

| コマンド | 目的 |
|---|---|
| **collect counter** {**bytes** \| **packets**} [**long**]<br>**例:**<br>`switch(config-flow-record)# collect counter packets` | フローからパケットベースまたはバイト カウンタを収集します。任意で、64 ビット カウンタを使用することを指定できます。 |
| **collect ip version**<br>**例:**<br>`switch(config-flow-record)# collect ip version` | フローの IP バージョンを収集します。 |
| **collect timestamp sys-uptime** {**first** \| **last**}<br>**例:**<br>`switch(config-flow-record)# collect timestamp sys-uptime last` | フローの先頭または最終パケットに関するシステム稼働時間を収集します。 |
| **collect transport tcp flags**<br>**例:**<br>`switch(config-flow-record)# collect transport tcp flags` | フローのパケットに対応する TCP トランスポート層フラグを収集します。 |

# フロー エクスポータの作成

フロー エクスポータの設定では、フローに対するエクスポート パラメータを定義し、リモート NetFlow Collector への到達可能性情報を指定します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | 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 | **flow exporter** *name*<br>例：<br>`switch(config)# flow exporter flow-exporter-one`<br>`switch(config-flow-exporter)#` | フローエクスポータを作成し、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。フロー エクスポータ名を最大 63 文字の英数字で入力できます。 |
| ステップ 3 | **destination** {*ipv4-address* \| *ipv6-address*} [**use-vrf** *name*]<br>例： | このフロー エクスポータの宛先 IPv4 または IPv6 アドレスを設定します。任意で、NetFlow Collector に到達するために使用する VRF を設定できます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `switch(config-flow-exporter)# destination 192.0.2.1` | VRF 名には最大 32 文字の英数字を入力できます。 |
| ステップ 4 | **source** *interface-type name/port*<br>例：<br>`switch(config-flow-exporter)# source ethernet 2/1` | 設定された宛先で NetFlow Collector に到達するために使用するインターフェイスを指定します。 |
| ステップ 5 | （任意） **description** *string*<br>例：<br>`switch(config-flow-exporter)# description exportversion9` | このフローエクスポータについて説明します。説明には最大 63 文字の英数字を入力できます。 |
| ステップ 6 | （任意） **dscp** *value*<br>例：<br>`switch(config-flow-exporter)# dscp 0` | DSCP（DiffServ コードポイント）値を指定します。範囲は 0 ～ 63 です。 |
| ステップ 7 | （任意） **transport udp** *port*<br>例：<br>`switch(config-flow-exporter)# transport udp 200` | NetFlow Collector に到達するために使用する UDP ポートを指定します。範囲は 0 ～ 65535 です。<br>（注）<br>UDP ポートを指定しない場合は、9995 がデフォルトとして選択されます。 |
| ステップ 8 | **version 9**<br>例：<br>`switch(config-flow-exporter)# version 9`<br>`switch(config-flow-exporter-version-9)#` | NetFlow エクスポート バージョンを指定します。フローエクスポータのバージョン 9 コンフィギュレーション サブモードを開始するには、バージョン 9 を選択します。 |
| ステップ 9 | （任意） **option** {**exporter-stats** \| **interface-table**} **timeout** *seconds*<br>例：<br>`switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200` | フローエクスポータの統計情報再送信タイマーを設定します。値の範囲は 1 ～ 86400 秒です。 |
| ステップ 10 | （任意） **template data timeout** *seconds*<br>例：<br>`switch(config-flow-exporter-version-9)# template data timeout 1200` | テンプレートデータ再送信タイマーを設定します。値の範囲は 1 ～ 86400 秒です。 |
| ステップ 11 | （任意） **copy running-config startup-config**<br>例： | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `switch(config-flow-exporter-version-9)# copy running-config startup-config` | |

# フロー モニタの作成

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。1 つのモニタに属しているすべてのフローは、様々なフィールド上で照合するために関連するフロー レコードを使用します。データは指定されたフローエクスポータにエクスポートされます。

## 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | 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 | **flow monitor** *name*<br>例：<br>`switch(config)# flow monitor flow-monitor-one`<br>`switch(config-flow-monitor)#` | フロー モニタを作成し、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。フロー モニタ名を最大 63 文字の英数字で入力できます。 |
| ステップ 3 | （任意） **description** *string*<br>例：<br>`switch(config-flow-monitor)# description IPv4Monitor` | このフローモニタについて説明します。説明には最大 63 文字の英数字を入力できます。 |
| ステップ 4 | （任意） **exporter** *name*<br>例：<br>`switch(config-flow-monitor)# export v9` | フロー エクスポータとこのフロー モニタを関連付けます。エクスポータ名には最大 63 文字の英数字を入力できます。 |
| ステップ 5 | **record** *name* [**netflow-original** \| **netflow protocol-port** \| **netflow** {**ipv4** \| **ipv6**} {**original-input** \| **original-output**}]<br>例：<br>`switch(config-flow-monitor)# record IPv4Flow` | フロー レコードを指定したフロー モニタと関連付けます。レコード名には最大 63 文字の英数字を入力できます。<br>（注）<br>**record netflow ipv4 original-input**、**record netflow ipv4 original-output**、**record netflow layer2-switched input** は、Cisco NX-OS リリース 9.3(1) ではサポートされていません。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config-flow-monitor)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

# インターフェイスへのフロー モニタの適用

フローモニタは入力インターフェイスに適用できます。出力NetFlowはサポートされていません。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | 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 | **interface vlan** *vlan-id*<br>例：<br>`switch(config)# interface vlan 10`<br>`switch(config-if)#` | VLANインターフェイスを設定し、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 3 | **ip flow monitor** {**ipv4** \| **ipv6** \| **layer-2-switched**} **input**<br>例：<br>`switch(config-if)# ip flow monitor ipv4 input` | 入力パケットのインターフェイスに、IPv4、IPv&、またはレイヤ 2 スイッチフロー モニタを関連付けます。 |
| ステップ 4 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config-if)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

# VLAN 上でのブリッジ型 NetFlow の設定

VLAN のレイヤ 2 スイッチド パケットでレイヤ 3 データを収集するために、VLAN にフローモニタを適用できます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **vlan configuration** *vlan-id*<br>例：<br>`switch(config)# vlan configuration 30`<br>`switch(config-vlan-config)#` | VLAN コンフィギュレーション モードを開始します。VLAN ID の範囲は 1 ～ 3967 または 4048 ～ 4093 です。<br>（注）<br>VLAN コンフィギュレーション モードでは、作成とは無関係に VLAN を設定できます。これは、VTP クライアントのサポートに必要です。 |
| ステップ 3 | {**ip** \| **ipv6**} **flow monitor** *name*<br>例：<br>`switch(config-vlan-config)# ip flow monitor testmonitor` | 入力パケットのフロー モニタを VLAN に関連付けます。フロー モニタ名を最大 63 文字の英数字で入力できます。 |
| ステップ 4 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config-vlan-config)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

# レイヤ 2 NetFlow キーの設定

フレクシブル NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | 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 2 | **flow record** *name*<br>例：<br>`switch(config)# flow record L2_record`<br>`switch(config-flow-record)#` | 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。フローレコードの設定の詳細については、フローレコードの作成 （11 ページ） を参照してください。 |
| ステップ 3 | **match datalink** {**mac source-address** \| **mac destination-address** \| **ethertype** \| **vlan**}<br>例：<br>`switch(config-flow-record)# match datalink ethertype` | レイヤ 2 属性をキーとして指定します。 |
| ステップ 4 | **exit**<br>例：<br>`switch(config-flow-record)# exit`<br>`switch(config)#` | フローレコードコンフィギュレーション モードを終了します。 |
| ステップ 5 | **interface** {**ethernet** *slot/port* \| **port-channel** *number*}<br>例：<br>`switch(config)# interface Ethernet 6/3`<br>`switch(config-if#)` | インターフェイス設定モードを開始します。インターフェイスタイプは、物理的なイーサネットポートまたはポートチャネルを指定できます。 |
| ステップ 6 | **switchport**<br>例：<br>`switch(config-if)# switchport` | インターフェイスをレイヤ 2 の物理インターフェイスに変更します。スイッチポートの設定に関する詳細については、「Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド」を参照してください。 |
| ステップ 7 | **mac packet-classify**<br>例：<br>`switch(config-if)# mac packet-classify` | パケットの MAC 分類を強制します。<br>このコマンドの使用に関する詳細については、「Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド」を参照してください）。<br>（注）<br>フローを検出するためにこのコマンドを使用する必要があります。 |
| ステップ 8 | **layer2-switched flow monitor** *flow-name* **input**<br>例： | フローモニタをスイッチポートの入力パケットに関連付けます。フローモニタ名を最大 63 文字の英数字で入力できます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `switch(config-if)# layer2-switched flow monitor L2_monitor input` | |
| ステップ 9 | （任意） **show flow record netflow layer2-switched input**<br>例：<br>`switch(config-if)# show flow record netflow layer2-switched input` | レイヤ 2 NetFlow のデフォルト レコードの情報を表示します。 |
| ステップ 10 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config-if)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

# レイヤ 2 インターフェイスでのレイヤ 3 NetFlow の設定

レイヤ 2 インターフェイスでレイヤ 3 フロー情報をキャプチャするために、レイヤ 2 インターフェイスでレイヤ 3 フロー モニタを定義できます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | 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 | **flow record** *name*<br>例：<br>`switch(config)# flow record L3_record`<br>`switch(config-flow-record)#` | 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。フロー レコードの設定の詳細については、フロー レコードの作成 （11 ページ） を参照してください。 |
| ステップ 3 | **interface** {**ethernet** *slot/port* \| **port-channel** *number*}<br>例：<br>`switch(config)# interface Ethernet 6/3`<br>`switch(config-if#)` | インターフェイス設定モードを開始します。インターフェイス タイプは、物理的なイーサネット ポートまたはポート チャネルを指定できます。 |
| ステップ 4 | **switchport**<br>例：<br>`switch(config-if)# switchport` | インターフェイスをレイヤ2モードに変更します。スイッチ ポートの設定に関する詳細については、「Cisco Nexus 9000 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | シリーズ NX-OS レイヤ 2 スイッチング設定ガイド」を参照してください。 |
| ステップ 5 | **ip flow monitor** *flow-name* **input**<br>例：<br>`switch(config-if)# ip flow monitor v41 input` | フロー モニタをスイッチ ポートの入力パケットに関連付けます。フロー モニタ名を最大 63 文字の英数字で入力できます。 |
| ステップ 6 | **ipv6 flow monitor** *flow-name* **input**<br>例：<br>`switch(config-if)# ipv6 flow monitor v61 input` | IPv6 フロー モニタをスイッチ ポートの入力パケットに関連付けます。フロー モニタ名を最大 63 文字の英数字で入力できます。 |
| ステップ 7 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config-if)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

# NetFlow タイムアウトの設定

任意で、システム内のすべてのフローに適用されるグローバルな NetFlow タイムアウトを設定できます。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`switch(config)#` | 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 | **flow timeout** *seconds*<br>例：<br>`switch(config)# flow timeout 30` | フラッシュ タイムアウト値を秒単位で設定します。範囲は 5 ～ 60 秒です。デフォルト値は 10 秒です。 |
| ステップ 3 | （任意） **copy running-config startup-config**<br>例：<br>`switch(config)# copy running-config startup-config` | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

# NetFlow 構成の確認

NetFlow 構成を表示するには、次のタスクのうちのいずれかを実行します。

| コマンド | 目的 |
|---|---|
| **show flow cache** [**ipv4** \| **ipv6** \| **ce**] | NetFlow IP フローに関する情報を表示します。<br>（注）<br>このコマンドは、EOR スイッチでは有効ではないように見え、フローは表示されません。EOR スイッチでこのコマンドを表示するには、 **attach mod** *x* コマンドを使用してモジュールにアタッチします。または、**slot** *x***quoted "show flow cache"** コマンドを使用してこのコマンドをチェックします。ここで、*x* は入力 NetFlow のモジュール番号です。 |
| **show flow exporter** [*name*] | NetFlow のフロー エクスポータ情報と統計情報を表示します。フロー エクスポータ名を最大 63 文字の英数字で入力できます。 |
| **show flow interface** [*interface-type slot/port*] | NetFlow インターフェイスに関する情報を表示します。 |
| **show flow record** [*name*] | NetFlow のフロー レコード情報を表示します。フロー レコード名には最大 63 文字の英数字を入力できます。 |
| **show flow record netflow layer2-switched input** | レイヤ 2 NetFlow 構成の情報を表示します。 |
| **show running-config netflow** | 現在デバイスにある NetFlow 設定を表示します。 |

# NetFlow のモニタリング

NetFlow の統計情報を表示するには、**show flow exporter** コマンドを使用します。NetFlow エクスポータの統計情報を消去するには、**clear flow exporter** コマンドを使用します。

# NetFlow の表示例

IPv4 の **show flow cache** コマンドの出力には、次のように表示されます。

```
show flow cache
IPV4 Entries
SIP          DIP         BD ID  S-Port  D-Port Protocol Byte Count  Packet Count  TCP
FLAGS  TOS  if_id      output_if_id  flowStart flowEnd
10.10.30.4   30.33.1.2   1480   30000   17998  17       683751850   471553        0x0
      0x0  0x90105c8  0x1a005000    14096494  14153835
30.33.1.2    10.10.39.4  4145   30000   18998  17       43858456    30164         0x0
      0x0  0x1a005000 0x1a006600    14096477  14099491
10.10.29.4   30.33.1.2   1479   30000   17998  17       683751850   471553        0x0
      0x0  0x90105c7  0x1a005000    14096476  14153817
10.10.7.4    30.33.1.2   1457   30000   17998  17       683753300   471554        0x0
      0x0  0x90105b1  0x1a005000    14096481  14153822
30.33.1.2    10.10.42.4  4145   30000   18998  17       95289344    65536         0x0
      0x0  0x1a005000 0x1a006600    14112551  14119151
10.10.49.4   30.33.1.2   1499   30000   17998  17       683753300   471554        0x0
      0x0  0x90105db  0x1a005000    14096486  14153827
```

# NetFlow の構成例

この例では、IPv4 に対してNetFlow エクスポータを構成する方法を示します。

```
feature netflow
flow exporter ee
 destination 171.70.242.48 use-vrf management
 source mgmt0
 version 9
  template data timeout 20
flow record rr
 match ipv4 source address
 match ipv4 destination address
 collect counter bytes
 collect counter packets
flow monitor foo
 record rr
 exporter ee
interface Ethernet2/45
 ip flow monitor foo input
 ip address 10.20.1.1/24
 no shutdown
```

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。