



# NetFlow

NetFlow システムは、以下を実行するネットワーク トラフィックのモニタリングおよびレポートのソリューションです。

- Nexus 9000 シリーズ スイッチを通過するパケットフローを識別、分類、および記録する
- IP およびレイヤ 2 パケット データの詳細なフローベースの統計情報を提供する
- は、ネットワーク トラフィックやデバイスを直接変更することなく、アカウンティング、ネットワーク パフォーマンス、およびセキュリティ分析の高度な機能をサポートします。

NetFlow は、パケットまたは、ネットワーキング デバイスへの変更を必要としません。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。フレキシブル 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。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。

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 エクスポートを使用し、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) 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。フローは NetFlow キャッシュに格納されます。フロー モニタで、フローレコードおよびフロー エクスポートを NetFlow キャッシュ情報と結合します。

- [NetFlow の基礎 \(2 ページ\)](#)

- 入力 NetFlow (7 ページ)
- 出力 NetFlow (15 ページ)
- NetFlow を有効にするための全般的な手順 (18 ページ)
- 入力 NetFlow のための追加の手順 (24 ページ)
- 出力 NetFlow に関する追加の手順 (28 ページ)
- ドロップ レポート (29 ページ)
- ドロップされたフローの通知 (32 ページ)

## NetFlow の基礎

### 主要コンポーネント

表 1: NetFlow の主要なコンポーネント

タイプ	定義
フロー レコード	<p>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。</p> <p>キー フィールドは、<b>match</b> 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<b>collect</b> キーワードで指定されます。</p> <p>Cisco NX-OS では、フロー レコードの作成時に次の <b>match</b> フィールドをデフォルトとして使用できます。</p> <ul style="list-style-type: none"> <li>• match interface input</li> <li>• match flow direction</li> </ul>
フロー モニタ	<p>フロー モニタは、フロー レコードおよびフロー エクスポートを参照します。フロー モニタはインターフェイスに適用します。</p>

タイプ	定義
フロー エクスポート	<p>フローエクスポートでは、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。フローエクスポートで設定できる情報は次のとおりです。</p> <ul style="list-style-type: none"><li>• エクスポート宛先 IP アドレス</li><li>• 送信元インターフェイス</li><li>• 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。</li></ul> <p>（注）</p> <p>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、フローエクスポートはエクスポートする予定のフローをドロップします。[Netflow エクスポート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.）]</p> <p>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（<b>flow timeout</b> コマンドを使用）。</p>

タイプ	定義
レイヤ 2 NetFlow キー	<p data-bbox="943 296 1481 472">フレキシブル 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。</p> <ul data-bbox="976 493 1481 672" style="list-style-type: none"><li data-bbox="976 493 1388 525">• 送信元および宛先 MAC アドレス</li><li data-bbox="976 546 1193 577">• 送信元 VLAN ID</li><li data-bbox="976 598 1481 672">• イーサネットフレームのイーサネットタイプ</li></ul> <p data-bbox="943 703 1481 777">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。</p> <ul data-bbox="976 798 1404 945" style="list-style-type: none"><li data-bbox="976 798 1404 829">• アクセスモードのスイッチポート</li><li data-bbox="976 850 1404 882">• トランクモードのスイッチポート</li><li data-bbox="976 903 1323 934">• レイヤ 2 のポートチャネル</li></ul> <p data-bbox="943 976 1481 1155">(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。</p>

タイプ	定義
NetFlow 出力インターフェイス	<p>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。</p> <ul style="list-style-type: none"><li>• <b>show flow cache</b> コマンドの NetFlow は <code>output_if_id</code> を表示し、出力インターフェイスを コレクタにエクスポートします。</li><li>• Cisco Nexus 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。ただし、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。</li><li>• <b>show flow cache</b> コマンドは、<code>output_if_id</code> を 0x0 として表示します。ただし、Cisco NX-OS リリース 10.3(3)F 以降では、宛先 IP アドレスが解決できない、またはルーティング テーブルに登録されていない、または受信したパケットが制御パケットであった場合に限り、<b>show flow cache</b> コマンドは <code>output_if_id</code> を 0x0 として表示します。</li><li>• 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 <code>ifIndex</code> 値をサポートします。</li><li>• 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。</li><li>• NetFlow 出力インターフェイスの例の詳細については、NetFlow のディスプレイ例を参照してください。</li></ul>



- (注) 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。



- (注) 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。

### アーキテクチャ

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。

### 種類

Cisco NX-OS リリース 10.4 (1) F 以降、NetFlow は次の 2 種類の構成で構成されます：

表 2: NetFlow のタイプ

タイプ	定義
入力 NetFlow	入力 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。入力 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。

タイプ	定義
出力 NetFlow	出力 NetFlow は発信 IP パケットとレイヤ 2 フローについてパケット フローを識別し、これらのパケット フローに基づいて統計情報を提供します。Cisco Nexus Cloudscale 9000 スイッチでは、出力 NetFlow は入力パイプラインと入力 TCAM カービング <code>egr-netflow</code> を使用して、スイッチから出力されるフロー情報を記録します。フロー レコード、フロー エクスポート、およびフロー モニターの NetFlow の全てのパラメータと制限は、出力 NetFlow に適用できます。

## 入力 NetFlow

### 注意事項と制約事項



(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。

### 一般的な制限事項

- 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。
- フロー収集は ARP トラフィックに対して実行されません。
- 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。
- 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。
- NetFlow およびフローテレメトリは、N9K-C9364C-H1 プラットフォームの SFP+ ポート、Ethernet1/65、および Ethernet1/66 ではサポートされていません。
- Cisco Nexus 3232C および 3264Q スイッチは、NetFlow をサポートしていません。
- MPLS/VXLAN データパスの NetFlow はサポートされていません
- `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。

- フローは CFLOW パケットの入力 (0) フィールドで識別されます。

### ICMP および非 TCP/UDP フロー

- 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来含まれています。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、エクスポートは 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

### 構成と使用に関する注意事項

- 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。
- 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、フローエクスポート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 およびレイヤ 3 インターフェイスの制限事項

- 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、その逆へ変更すると、ソフトウェアで、インターフェイスからレイヤ 2 の NetFlow 構成が削除されます。
- 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。
- VLAN インターフェイスとレイヤ 3 インターフェイスは異なる ACL を使用するため、2 つの異なるプロファイルとして扱う必要があります。
- ロールバック中に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、ロールバックは失敗します。

### リリース固有のガイドライン

- Cisco NX-OS リリース 9.2(1)



- FEX レイヤ 3 ポートの NetFlow は Cisco Nexus 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 NX-OS* リリース 9.2(2)
  - 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。
- *Cisco NX-OS* リリース 9.3(1)
  - **record netflow ipv4 original-input**、**record netflow ipv4 original-output**、および **record netflow layer2-switched input** コマンドはサポートされていません。
  - NetFlow **output\_if\_id** は 9300-FX スイッチでサポートされています。
- *Cisco NX-OS* リリース 9.3(3)
  - NetFlow に関する次の無停止インサースervice 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ト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。
  - 入力 Netflow は Cisco Nexus 9300-GX プラットフォーム スイッチではサポートされません。
  - NetFlow **output\_if\_id** は 9300-FX3 スイッチでサポートされています。
- *Cisco NX-OS* リリース 9.3 (4)
  - 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、16384～32767 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
  - 9736C-FX ライン カードを搭載した Cisco Nexus 9504、9508 および 9516 スイッチ
- *Cisco NX-OS* リリース 10.1(2)
    - Netflow は N9K-X9716D-GX ライン カードでサポートされています。
    - 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。
  - 入力 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 NX-OS* リリース 10.3(3)F
    - NetFlow Output\_if\_id は Cisco 9300-FX2、9300-GX、および 9300-GX2 スイッチおよび 9500-GX ライン カードでサポートされます。
      - ユニキャスト フローには、output\_if\_id が 0x0 と表示されている場合は、宛先 IP が解決されていないか、ルーティング テーブルまたは ARP テーブルで使用できないことを意味します。
      - コントロール プレーン宛ての受信パケットの output\_if\_id は 0x0 として表示されます。このようなトラフィックの例としては、ルーティング プロトコルまたは ICMP パケットがあります。
      - Cisco Nexus 9500 ライン カードの IPv6 フローの場合、output\_if\_id はハードウェアの制限によりサポート対象外と表示されます。
      - データプレーン マルチキャスト トラフィックの output\_if\_id は、0x0 として表示されます。
  - *Cisco NX-OS* リリース 10.4(1)F
    - 入力 NetFlow は N9K-C9332D-H2R スイッチでサポートされています。ドロップフローは、デフォルトではサポートされていません。ドロップフローを有効にするには、**hardware flow-table collect-drop-reason** コマンドを構成します。

- *Cisco NX-OS* リリース 10.4(2)F

- MPLS パケットの入力 NetFlow は、Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、9300-GX2、および 9500-FX/GX スイッチでサポートされています。この機能により、Nexus スイッチは MPLS パケットから IPv4 または IPv6 フロー情報をキャプチャし、フロー情報をコレクタに送信できます。NetFlow は、最大 8 つの MPLS スタック ラベルを持つパケットの情報をキャプチャし、2 つのラベルを持つ IPoMPLS および EoMPLS パケットや MPLS-VPN パケットなどの MPLS パケットのキャプチャをサポートします。show flow cache は、MPLS-VPN カプセル化ノードの出力インターフェイスを 0x0 と表示します。NetFlow 出力インターフェイスは、中継ノードまたは P ノードで MPLS-VPN をサポートします。この機能には、次の制限があります。

- ハードウェア ASIC の制限により、NetFlow は MPLS ラベルなどの MPLS 関連パラメータをキャプチャできません。
- 中継ノードまたは P ノードでは、同じレイヤ 2 送信元ポートと宛先ポートを持ち IP アドレスが重複している MPLS VPN は、MPLS-VPN ネットワーク内の単一のフローとして報告されます。
- 入力 NetFlow は N9K-C93400LD-H1 スイッチでサポートされます。ドロップフローは、デフォルトではサポートされていません。ドロップフローを有効にするには、**hardware flow-table collect-drop-reason** コマンドを構成します。

- *Cisco NX-OS* リリース 10.6(2)F

Nexus 9300-SG2 スイッチは、ドロップされたフローの通知機能をサポートします。

## VXLAN 環境の制限事項

- OIF（出力インターフェイス）を含む VXLAN トラフィックの NetFlow がサポートされています。内部フローの詳細をキャプチャするには、VXLAN トランジットノードで feature nv overlay コマンドを有効にする必要があります。そうでない場合、NetFlow は外部ヘッダー情報のみをキャプチャします。
- VXLAN カプセル化ノードの OIF は 0x0 と表示されます。
- 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。

## プラットフォームでの制限

- 入力 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。

- 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-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
- *Cisco Nexus 9300-FX* プラットフォーム スイッチ
  - 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。
  - レイヤ 2 NetFlow に対してすでに構成されているポート チャネルにメンバを追加すると、NetFlow の構成が削除され、レイヤ 2 設定が追加されます。
- 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-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-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。
- 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。これは、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。
- NetFlow は、EX および FX 混在シャーシを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。EX および FX 混在シャーシの 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。
- 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、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。

### 前提条件

- 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。

## 入力 NetFlow の構成

### 手順

- 
- ステップ 1 [NetFlow 機能を有効にします。](#)
  - 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 エクスポートを定義します。](#)
  - ステップ 4 [フロー レコードおよびフロー エクスポートに基づいて、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。](#)
- 

### 入力 NetFlow の構成例

この例では、IPv4 に対して出力 NetFlow エクスポート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
```

## 入力 NetFlow 検証コマンド

入力 NetFlow 検証コマンドは、

- デバイスの入力 NetFlow 機能のステータスと構成を表示します。

- フロー、インターフェイス、エクスポート、およびレコードに関する詳細情報を提供し、
- 管理者が NetFlow の動作をトラブルシューティングおよび検証するのに役立つ診断コマンドです。

入力 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
<b>show flow cache</b> [ipv4   ipv6   ce]	入力 NetFlow IP フローに関する情報を表示します。  (注) このコマンドは、EOR スイッチでは有効ではないように見なされ、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、 <b>attach mod x</b> 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、 <b>slot x</b> 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、 <i>x</i> は入力 NetFlow のモジュール番号です。
<b>show flow exporter</b> [name]	入力 NetFlow のフロー エクスポート情報と統計情報を表示します。フロー エクスポート名を最大 63 文字の英数字で入力できます。
<b>show flow interface</b> [interface-type slot/port]	入力 NetFlow インターフェイスに関する情報を表示します。
<b>show flow record</b> [name]	入力 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。
<b>show flow record netflow layer2-switched input</b>	レイヤ 2 入力 NetFlow 構成の情報を表示します。
<b>show running-config netflow</b>	現在デバイスにある NetFlow 設定を表示します。

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 エクスポート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。

### 入力 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

```

## 出力 NetFlow

### 注意事項と制約事項



(注) 検証済みの NetFlow のスケール数については、『[Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド](#)』を参照してください。

- インターフェイスで入力 NetFlow と出力 NetFlow の両方が有効になっている場合、入力 NetFlow は出力 NetFlow よりも優先され、フロー情報は入力方向に生成されます。
- フローは CFLOW パケットの出力 (1) フィールドで識別されます。
- 出力 NetFlow と機能分析は共存できますが、分析フィルタにヒットしたトラフィックフローは、分析で設定されたコレクタにのみエクスポートされます。
- モジュラ型 Cisco Nexus 9500 シャーシでは、トラフィックは異なるラインカードで送受信されます。出力 NetFlow がトラフィックの発信インターフェイスで有効で、トラフィックの着信インターフェイスで有効になっていない場合、出力フロー情報は入力インターフェイスのラインカードでキャプチャされ、出力インターフェイスではキャプチャされません。
- L2 インターフェイスに複数の SVI および sub\_interface がある場合、出力 NetFlow に対する入力インターフェイス (if\_id) の導出が正しくなくてもかまいません。
- 出力 NetFlow は、IPv4 およびレイヤ 2 トラフィックでのみサポートされます。出力 NetFlow は、IPv6 およびマルチキャスト トラフィックをサポートしません。
- 出力 NetFlow は、次をサポートしていません。
  - vrf-id
  - 発信制御プレーン トラフィックの記録
  - 出力インターフェイス (NetFlow OIF)
  - MPLS ネットワーク

- Cisco NX-OSリリース 10.6(2)F 以降、Nexus 9300-SG2 スイッチは、ドロップされたフローの通知機能をサポートします。

#### 前提条件

1. 出力 NetFlow TCAM リージョンで Nexus 9000 スイッチを構成します。
2. 出力 NetFlow TCAM カービング後にスイッチをリロードします。
3. スイッチがオンラインになったら、**ip flow monitor <> output or layer2-switched flow monitor <> output** コマンドを使用して、インターフェイスの任意の L2 または L3 インターフェイスで出力 NetFlow を有効にします。

## 出力 NetFlow の構成

### 手順

ステップ 1 NetFlow 機能を有効にします。

ステップ 2 egr-netflow TCAM カービングを実行し、スイッチをリロードします。

a) **configure terminal**

例：

```
switch# configure terminal
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。

b) **[no] hardware access-list tcam region egr-netflow {0 | 512}**

例：

```
switch(config)# hardware access-list tcam region egr-netflow 512
```

出力 NetFlow TCAM カービングを有効にします。デフォルトは無効です。egr-netflow TCAM カービングの場合、サポートされている値は 0 と 512 です。

c) **copy running-config startup-config**

例：

```
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。

d) **reload**

例：

```
switch(config)# reload
This command will reboot the system. (y/n)? [n] y
```

スイッチをリロードします。



- ステップ3** 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4** 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、フロー エクスポートを定義します。
- ステップ5** フロー レコードおよびフロー エクスポートに基づいて、フロー モニタを定義します。
- ステップ6** 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。

## 出力 NetFlow の構成例

この例では、IPv4 に対して出力 NetFlow エクスポート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 output
 ip address 10.20.1.1/24
 no shutdown
```

## 出力 NetFlow 検証コマンド

出力 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
<b>show flow cache [ipv4   ce] [output]</b>	出力 NetFlow IP フローに関する情報を表示します。
<b>show running-config netflow</b>	現在デバイスにある出力 NetFlow 構成を表示します。

### 出力 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。

```
switch(config-if-range)# show flow cache
NOTE: Only 10k flows are displayed in XML output
Egress 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      Profile    Ing-VRF
130.1.1.2    162.1.1.1    4119      60      893      6      161082
171          0x0        0x0        0x1a002600  0x1a002800  716994
732532      4 : NF    21
130.1.1.2    162.1.1.1    4151      60      11013     6      61230
65          0x0        0x0        0x1a006600  0x1a006800  715951
728074      4 : NF    38
130.1.1.2    162.1.1.1    4145      60      3441      6      162966
173          0x0        0x0        0x1a005a00  0x1a005c00  713085
727941      4 : NF    35

```

## NetFlow を有効にするための全般的な手順

次のセクションでは、有効にする場合に入力 NetFlow と出力 NetFlow の両方に共通する手順をリストします。

### NetFlow 機能を有効にします。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	<b>[no] feature netflow</b> 例： 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。  (注) 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) <b>copy running-config startup-config</b> 例： 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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	<b>flow record name</b> 例 : <pre>switch(config)# flow record Test switch(config-flow-record)#</pre>	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。
ステップ 3	(任意) <b>description string</b> 例 : <pre>switch(config-flow-record)# description IPv4Flow</pre>	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) <b>match type</b> 例 : <pre>switch(config-flow-record)# match transport destination-port</pre>	一致キーを指定します。詳細については、 <a href="#">match パラメータの指定 (19 ページ)</a> を参照してください。 (注) レイヤ 4 ポートデータをエクスポートするには、 <b>match transport destination-port</b> および <b>match ip protocol</b> コマンドが必要です。
ステップ 5	(任意) <b>collect type</b> 例 : <pre>switch(config-flow-record)# collect counter packets</pre>	コレクションフィールドを指定します。詳細については、 <a href="#">collect パラメータの指定 (21 ページ)</a> を参照してください。
ステップ 6	(任意) <b>show flow record [name] [record-name] {netflow-original   netflow protocol-port   netflow {ipv4   ipv6} {original-input   original-output}}</b> 例 : <pre>switch(config-flow-record)# show flow record netflow protocol-port</pre>	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) <b>copy running-config startup-config</b> 例 : <pre>switch(config-flow-record)# copy running-config startup-config</pre>	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
<b>match datalink {mac source-address   mac destination-address   ethertype   vlan}</b>  <b>例:</b>  <pre>switch(config-flow-record)# match datalink ethertype</pre>	レイヤ2属性をキーとして指定します。
<b>match ip {protocol   tos}</b>  <b>例:</b>  <pre>switch(config-flow-record)# match ip protocol</pre>	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。  (注) レイヤ4ポートデータをエクスポートするには、 <b>match transport destination-port</b> および <b>match ip protocol</b> コマンドが必要です。  データは <b>show hardware flow ip</b> 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。
<b>match ipv4 {destination address   source address}</b>  <b>例:</b>  <pre>switch(config-flow-record)# match ipv4 destination address</pre>	IPv4 送信元または宛先アドレスをキーとして指定します。
<b>match ipv6 {destination address   source address   flow-label   options}</b>  <b>例:</b>  <pre>switch(config-flow-record)# match ipv6 flow-label</pre>	IPv6 キーを指定します。
<b>match transport {destination-port   source-port}</b>  <b>例:</b>  <pre>switch(config-flow-record)# match transport destination-port</pre>	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。  (注) レイヤ4ポートデータをエクスポートするには、 <b>match transport destination-port</b> および <b>match ip protocol</b> コマンドが必要です。  データは <b>show hardware flow ip</b> 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

Cisco/NX-OS NetFlow では、「収集パラメータ」はフロー レコード内で指定する構成オプションで、エクスポートおよび分析のためにネットワーク フローからキャプチャされるフィールドまたはメトリックを示します。

フロー レコードごとに、次の collect パラメータを 1 つ以上構成する必要があります：

コマンド	目的
<b>collect counter {bytes   packets} [long]</b> 例： <pre>switch(config-flow-record)# collect counter packets</pre>	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。
<b>collect ip version</b> 例： <pre>switch(config-flow-record)# collect ip version</pre>	フローの IP バージョンを収集します。
<b>collect timestamp sys-uptime {first   last}</b> 例： <pre>switch(config-flow-record)# collect timestamp sys-uptime last</pre>	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。
<b>collect transport tcp flags</b> 例： <pre>switch(config-flow-record)# collect transport tcp flags</pre>	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 エクスポートの作成

フロー エクスポートの設定では、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	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	<b>flow exporter name</b> 例：	フロー エクスポートを作成し、フロー エクスポート 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
	<code>switch(config)# flow exporter flow-exporter-one</code> <code>switch(config-flow-exporter)#</code>	フロー エクスポート名を最大 63 文字の英数字で入力できます。
ステップ 3	<b>destination</b> { <i>ipv4-address</i>   <i>ipv6-address</i> } [ <i>use-vrf name</i> ]  例 : <code>switch(config-flow-exporter)# destination 192.0.2.1</code>	このフロー エクスポートの宛先 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。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	<b>source interface-type name/port</b>  例 : <code>switch(config-flow-exporter)# source ethernet 2/1</code>	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) <b>description string</b>  例 : <code>switch(config-flow-exporter)# description exportversion9</code>	このフロー エクスポート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) <b>dscp value</b>  例 : <code>switch(config-flow-exporter)# dscp 0</code>	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) <b>transport udp port</b>  例 : <code>switch(config-flow-exporter)# transport udp 200</code>	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。  (注) 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	<b>version 9</b>  例 : <code>switch(config-flow-exporter)# version 9</code> <code>switch(config-flow-exporter-version-9)#</code>	NetFlow エクスポートバージョンを指定します。フロー エクスポートのバージョン 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) <b>option {exporter-stats   interface-table} timeout seconds</b>  例 : <code>switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200</code>	フロー エクスポート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) <b>template data timeout seconds</b>  例 : <code>switch(config-flow-exporter-version-9)# template data timeout 1200</code>	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。

	コマンドまたはアクション	目的
ステップ 11	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config-flow-exporter-version-9)# copy running-config startup-config</pre>	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 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 エクスポート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ト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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	<b>flow monitor name</b> 例 : <pre>switch(config)# flow monitor flow-monitor-one switch(config-flow-monitor)#</pre>	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) <b>description string</b> 例 : <pre>switch(config-flow-monitor)# description IPv4Monitor</pre>	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) <b>exporter name</b> 例 : <pre>switch(config-flow-monitor)# export v9</pre>	フロー エクスポートとこのフロー モニタを関連付けます。エクスポート名には最大 63 文字の英数字を入力できます。
ステップ 5	<b>record name [netflow-original   netflow protocol-port   netflow {ipv4   ipv6} {original-input   original-output}]</b> 例 : <pre>switch(config-flow-monitor)# record IPv4Flow</pre>	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。 (注) <b>record netflow ipv4 original-input、record netflow ipv4 original-output、record netflow layer2-switched input</b> 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) <b>copy running-config startup-config</b> 例 : <pre>switch(config-flow-monitor)# copy running-config startup-config</pre>	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 モニタはインターフェイスに適用できます。入力の代わりに 出力 キーワードを使用して、出力方向にフロー 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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>interface vlan <i>vlan-id</i></b> 例 : <pre>switch(config)# interface vlan 10 switch(config-if)#</pre>	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	<b>ip flow monitor {ipv4   ipv6   layer-2-switched} input</b> 例 : <pre>switch(config-if)# ip flow monitor ipv4 input</pre>	入力パケットのインターフェイスに、IPv4、IPv6、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) <b>copy running-config startup-config</b> 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	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。

## 入力 NetFlow のための追加の手順

次のセクションでは、入力 NetFlow に適用できるその他のさまざまな手順を示します。

## VLAN 上でのブリッジ型 NetFlow の構成

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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>vlan configuration <i>vlan-id</i></b> 例 : <pre>switch(config)# vlan configuration 30 switch(config-vlan-config)#</pre>	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。 (注) 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	<b>{ip   ipv6} flow monitor <i>name</i></b> 例 : <pre>switch(config-vlan-config)# ip flow monitor testmonitor</pre>	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) <b>copy running-config startup-config</b> 例 : <pre>switch(config-vlan-config)# copy running-config startup-config</pre>	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 キーの構成

フレキシブル 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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	<b>flow record <i>name</i></b> 例 :	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

	コマンドまたはアクション	目的
	<pre>switch(config)# flow record L2_record switch(config-flow-record)#</pre>	ては、 <a href="#">フローレコードの作成（18 ページ）</a> を参照してください。
ステップ 3	<b>match datalink {mac source-address   mac destination-address   ethertype   vlan}</b>  例 : <pre>switch(config-flow-record)# match datalink ethertype</pre>	レイヤ 2 属性をキーとして指定します。
ステップ 4	<b>exit</b>  例 : <pre>switch(config-flow-record)# exit switch(config)#</pre>	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	<b>interface {ethernet slot/port   port-channel number}</b>  例 : <pre>switch(config)# interface Ethernet 6/3 switch(config-if#)</pre>	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	<b>switchport</b>  例 : <pre>switch(config-if)# switchport</pre>	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、「 <a href="#">Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド</a> 」を参照してください。
ステップ 7	<b>mac packet-classify</b>  例 : <pre>switch(config-if)# mac packet-classify</pre>	パケットの MAC 分類を強制します。  このコマンドの使用に関する詳細については、「 <a href="#">Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド</a> 」を参照してください。  (注) 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	<b>layer2-switched flow monitor flow-name input</b>  例 : <pre>switch(config-if)# layer2-switched flow monitor L2_monitor input</pre>	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 9	(任意) <b>show flow record netflow layer2-switched input</b>  例 : <pre>switch(config-if)# show flow record netflow layer2-switched input</pre>	レイヤ 2 NetFlow のデフォルトレコードの情報を表示します。

	コマンドまたはアクション	目的
ステップ 10	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	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 の構成

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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	<b>flow record name</b> 例 : <pre>switch(config)# flow record L3_record switch(config-flow-record)#</pre>	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 レコードの構成の詳細については、 <a href="#">フロー レコードの作成 (18 ページ)</a> を参照してください。
ステップ 3	<b>interface {ethernet slot/port   port-channel number}</b> 例 : <pre>switch(config)# interface Ethernet 6/3 switch(config-if#)</pre>	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	<b>switchport</b> 例 : <pre>switch(config-if)# switchport</pre>	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、「 <a href="#">Cisco Nexus 9000 シリーズ NX-OS レイヤ2 スイッチング設定ガイド</a> 」を参照してください。
ステップ 5	<b>ip flow monitor flow-name input</b> 例 : <pre>switch(config-if)# ip flow monitor v4l input</pre>	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	<b>ipv6 flow monitor flow-name input</b> 例 : <pre>switch(config-if)# ipv6 flow monitor v6l input</pre>	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。

	コマンドまたはアクション	目的
ステップ 7	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	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 タイムアウトの構成

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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>flow timeout seconds</b> 例 : <pre>switch(config)# flow timeout 30</pre>	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) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

## 出力 NetFlow に関する追加の手順

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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成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	<b>flow record <i>name</i></b> 例 : <pre>switch(config)# flow record L3_record switch(config-flow-record)#</pre>	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、 <a href="#">フロー レコードの作成 (18 ページ)</a> を参照してください。
ステップ 3	<b>interface {<i>ethernet slot/port</i>   <i>port-channel number</i>}</b> 例 : <pre>switch(config)# interface Ethernet 6/3 switch(config-if#)</pre>	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	<b>switchport</b> 例 : <pre>switch(config-if)# switchport</pre>	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 ポートの構成に関する詳細については、『 <a href="#">Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング構成ガイド</a> 』を参照してください。
ステップ 5	<b>ip flow monitor <i>flow-name</i> input   output</b> 例 : <pre>switch(config-if)# ip flow monitor v4l input  switch(config-if)# layer2-switched flow monitor v4l output</pre>	または <b>layer2-switched flow monitor <i>flow-name</i> input   output</b> IPv4 フロー モニタをスイッチ ポートの入力または出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	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	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。

## ドロップ レポート

Cisco NX-OS 10.5 (2) 以降、ユーザーはドロップ レポートと呼ばれる新しいトラブルシューティング機能を利用できます。これは、単一フローでの断続的なパケット損失や輻輳などのトラブルシューティングを迅速に絞り込むために使用できます。この機能は、Cisco Nexus 9300-FX3/GX/GX2/HX および 9300 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。この機能は、次のドロップをサポートします：

- ポリサー ドロップ
- 転送ドロップ
- IDS ドロップ
- バッファドロップ
- RPF ドロップ

### 注意事項と制約事項

このドロップ レポートには、次のガイドラインと制約事項があります。

- 機能 NetFlow は、ユーザーがドロップ レポート機能を構成すると自動的に有効になります。
- 指定された送信元および宛先 IP に一致する最大 10 のフローがサポートされます。指定された送信元および宛先 IP を持つ別のフローをキャプチャするには、フィルタをクリアして再適用し、レポートキャプチャを再開する必要があります。
- ドロップ レポート フィルタは 10 分間アクティブなままになります。
- 機能分析がすでに構成されている場合、ドロップ レポート機能はサポートされません。
- 一度にサポートされるのは、2 タプル (sip/dip) とベストエフォートの 5 タプルを含む 1 つの一意のフローのみです。
- この機能は、ISSU、ISSD、およびリロードをサポートしていません。

## ドロップ レポートを構成

この機能を構成するには、drop-report モードを開始します。

### 手順の概要

1. **drop-report**
2. **start**
3. **filter {ipv4 [src-ip | dst-ip] | ipv6 [src-ip | dst-ip]}**
4. **report**
5. **clear**
6. **stop**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>drop-report</b> 例 : <pre>switch# drop-report switch(drop-report)#</pre>	ドロップレポート モードを開始します。
ステップ 2	<b>start</b> 例 : <pre>sswitch(drop-report)# start Feature netflow enabled by drop report tool</pre>	ドロップレポートにより、機能 NetFlow が有効になります。

	コマンドまたはアクション	目的
ステップ 3	<b>filter {ipv4 [src-ip   dst-ip]   ipv6 [src-ip   dst-ip]}</b>  例 : <pre>switch(drop-report)# filter ipv6 src-ip 100::1 dst-ip 200::2 switch(drop-report)# filter ipv4 src-ip 192.168.1.2 dst-ip 192.168.1.1</pre>	アクセス コントロール リスト (ACL) にパラメータを割り当てるようにフィルタを構成します。
ステップ 4	<b>report</b>  例 : <pre>switch(drop-report)# report</pre>	ドロップ情報を表示します。
ステップ 5	<b>clear</b>  例 : <pre>switch(drop-report)# clear CS drop filter removed</pre>	ACL を削除し、録音を停止します。
ステップ 6	<b>stop</b>  例 : <pre>switch(drop-report)# stop</pre>	ドロップ レポート機能を削除します。

## ドロップ レポート構成の確認

drop-report の結果を表示するには、次のコマンドを使用します：

インターネット ユーザに商品やサービスを提供する IPv4

```
switch# drop-report
switch(drop-report)# start
Feature netflow enabled by drop report tool
switch(drop-report)# filter ipv4 src-ip 10.0.0.9 dst-ip 10.0.0.10
switch(drop-report)# report
Filter Status: Applied    Filter Type   : IPv4
Dst IP: 10.0.0.10 Src IP: 10.0.0.9 Protocol:  Dst Port:   Src Port:
```

```
IPV4 Entries
SIP          DIP          BDIId SrcP  DstP  Prot  Byte Count      Packet Count
  Ing Interface  Fwd Rpf Pol  Ids Acl Buf
10.0.0.9      10.0.0.10      4112 49280 3784  17    70              1
  Ethernet1/8    0    0    0    0    0    0
```

```
Fwd: Forward Drop Rpf:RPF Fail Pol:Policer Drop Ids: Ids Drop Acl: Acl Drop Buf: Buffer
Drop
```

IPv6 の場合

```
switch(drop-report)# report
Filter Status: Applied    Filter Type   : IPv6
Dst IPv6: 2000:1::130:1:33:10 Src IPv6: 2000:1::22:1:1:10 Protocol:  Dst Port:   Src Port:
```

```
IPV6 Entries
SIP          DIP          BDIId SrcP  DstP  Prot  Byte Count      Packet
Count      Ing Interface  Fwd Rpf Pol  Ids Acl Buf
```

```

2000:1::22:1:1:10 2000:1::130:1:33:10 4100 300 400 17 76494000 69540
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 306 400 17 77632500 70575
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 303 400 17 76320200 69382
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 304 400 17 77745800 70678
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 308 400 17 77867900 70789
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 301 400 17 76458800 69508
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 307 400 17 77558800 70508
Ethernet1/1 1 0 0 1 1 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 309 400 17 77943800 70858
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 302 400 17 76373000 69430
Ethernet1/1 0 0 0 0 0 0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 305 400 17 77706200 70642
Ethernet1/1 0 0 0 0 0 0

Fwd: Forward Drop Rpf:RPF Fail Pol:Policer Drop Ids: Ids Drop Acl: Acl Drop Buf: Buffer
Drop

switch(drop-report)# clear
CS drop filter removed

switch(drop-report)# report
Filter Status: No Filter Applied

```

## ドロップされたフローの通知

ドロップされたフローの通知は、

- ネットワーク管理者が、転送の問題またはキューのバッファスペース不足が原因でドロップされたパケットをキャプチャできます。
- 設定されたドロップイベントに応じてドロップパケットをCPUにコピーすることによって実現されます。そして、
- フローの詳細とドロップの理由を示す v9 形式でのコレクタへのエクスポートします。このため、パケット損失の原因の特定に役立ちます。



(注) 設定可能なタイマーに基づくエクスポート制限は 64K です。



## ドロップされたフローの通知の設定

ドロップされたフローの通知を設定するには、次の手順を実行します。

### 手順

**ステップ 1** NetFlow 機能を有効にします。

**ステップ 2** **flow event export-interval** <interval> コマンドを使用して、イベントのエクスポート間隔を有効化し、データがエクスポートされる割合を指定します。export-interval の範囲は 0 ～ 60 秒で、デフォルト値は 10 秒です。

例：

```
switch(config)# flow event export-interval 50
```

**ステップ 3** フロー エクスポートを作成します。

**ステップ 4** **events transport udp** <udp-port> コマンドを使用して、イベントデータのエクスポートのための UDP ポートを設定します。UDP ポートの範囲は 1 ～ 65535 です。

例：

```
switch(config-flow-exporter)# events transport udp 9001
```

**ステップ 5** フロー レコードを作成します。

**ステップ 6** フロー モニターを作成します。

**ステップ 7** **flow event** <event\_name> コマンドを使用してキャプチャするイベントを設定します。

例：

```
switch(config-flow-monitor)# flow event ee
```

- a) **capture buffer-drops**、**capture fwd-drops**、**capture acl-drops**の各コマンド、または3つすべてのイベントコンフィギュレーションコマンドを使用して、モニターする必要があるパケットドロップを定義します。

例：

```
switch(config-flow-event)# capture buffer-drops
```

```
switch(config-flow-event)# capture acl-drops
```

```
switch(config-flow-event)# capture fwd-drops
```

**ステップ 8** **flow system config** コマンドをグローバル コンフィギュレーション モードで入力して、システム レベルのフロー イベント設定を定義します。

例：

```
switch(config-flow-event)# flow system config
```

- a) **monitor** <mon\_name> **input** コマンドを入力して、既存の NetFlow モニターをシステムの入力トラフィックに関連付けます。

例：

```
switch(config-flow-system)# monitor mon_ipv4 input
```

- b) **event <event\_name>** コマンドを入力して、事前に設定されたイベント定義をシステム全体のフローイベント設定に適用します。

例：

```
switch(config-flow-system)# event ee
```

## ドロップされたフローの通知の設定例

ドロップされたフローの通知の完全な設定を表示する例を次に示します。

```
switch(config)# feature netflow switch(config)# flow event export-interval 50
switch(config)# flow exporter exp_2 switch(config-flow-exporter)# destination 50.50.50.53
switch(config-flow-exporter)# transport udp 9996 switch(config-flow-exporter)# source
Ethernet1/7 switch(config-flow-exporter)# events transport udp 9001
switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)# flow
record rec_ipv4 switch(config-flow-record)# match ipv4 source address
switch(config-flow-record)# match ipv4 destination address switch(config-flow-record)#
match ip protocol switch(config-flow-record)# match ip tos switch(config-flow-record)#
match transport source-port switch(config-flow-record)# match transport destination-port
switch(config-flow-record)# flow monitor mon_ipv4 switch(config-flow-monitor)# record
rec_ipv4 switch(config-flow-monitor)# exporter exp_2 switch(config-flow-monitor)# flow
event ee switch(config-flow-event)# capture buffer-drops switch(config-flow-event)#
capture acl-drops switch(config-flow-event)# capture fwd-drops switch(config-flow-event)#
flow system config switch(config-flow-system)# monitor mon_ipv4 input
switch(config-flow-system)# event ee switch(config-flow-system)#
```

## ドロップされたフロー通知の確認コマンド

目的に基づいて、表で説明されているドロップされたフロー通知の設定用 **show** コマンドを使用してください。

表 3: ドロップされたフロー通知の確認コマンド

コマンド	目的
<b>show flow event</b>	ドロップイベントに関する情報を表示します。
<b>show flow event cache [ipv4   ipv6]</b>	ドロップされたフローに関する情報を表示します。
<b>show flow system</b>	システム構成に関する情報を表示します。
<b>show flow event export-interval</b>	ドロップされたフローがエクスポートされる間隔を表示します。

## 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。

## 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。