CHAPTER 48

Flexible NetFlow の設定

NetFlow は、ネットワーク モニタリング、ユーザのモニタリングとプロファイリング、ネットワーク プランニング、セキュリティの分析、課金とアカウンティング、データ ウェアハウジングとデータ マイニングのためにカスタマー アプリケーションで使用されるモニタ機能です。アップリンク ポートで Flexible NetFlow を使用すれば、ユーザ定義フローのモニタリング、フロー統計情報の収集、フロー単位のポリシングの実行が可能です。Flexible NetFlow は、フロー統計情報を収集してコレクタ デバイスにエクスポートします。

（注） Flexible NetFlow は、IP ベースまたは IP サービス フィーチャ セットを実行しネットワーク サービス モジュールが装備されている Catalyst 3750-X スイッチおよび 3560-X スイッチだけでサポートされます。NPE または LAN ベース イメージを実行しているスイッチではサポートされません。

Flexible NetFlow の詳細については、『NetFlow Configuration Guide』を参照してください。
http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/12_4t/fnf_12_4t_book.html

コマンドの詳細については、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

http://www.cisco.com/en/US/docs/ios/fnetflow/command/reference/fnf_book.html

（注） コマンド リファレンスに記載されているすべての Flexible NetFlow コマンドがスイッチで使用できるわけではありません。サポートされていないコマンドは、表示されないか、入力するとエラー メッセージが生成されます。

Flexible NetFlow の概要

Flexible NetFlow では、トラフィックが処理され、パケットはフローに分類されます。新しいフローは NetFlow テーブルに挿入され、統計情報は自動的に更新されます。入力および出力 NetFlow モニタの両方を設定する必要があります。ネットワーク サービス モジュールにより、方向ごとにインターフェイスあたり 1 個のモニタをサポートします。

Flexible NetFlow には次のコンポーネントがあります。

- *レコード*は、データの保存に使用されるキャッシュを定義するため、Flexible NetFlow モニタをモニタリングするために割り当てられるキーおよび非キー フィールドの組み合わせです。
- *フロー モニタ*はインターフェイスに適用され、ネットワーク トラフィックをモニタリングします。フロー モニタには、ユーザ定義のレコード、オプションのフロー エクスポータ、およびモニタが最初のインターフェイスに適用されるときに自動的に作成されるキャッシュで構成されます。スイッチは、設定に従って期限切れになる通常のキャッシュをサポートします。

- フロー エクスポータでは、フロー モニタ キャッシュ内のデータをリモート システム（たとえば、NetFlow コレクタを実行するサーバ）にエクスポートします。
- フロー サンプラは、分析するパケット数を制限することで、トラフィックをモニタするために Flexible NetFlow によってネットワーキング デバイスで生じる負荷を軽減します。

単方向フロー（宛先または送信元アドレス ベースのフロー）を設定でき、フロー エージングも設定できます。次の機能は、ネットワーク サービス モジュールでサポートされます。

- レイヤ 2 スイッチング（非ルーティング）トラフィック、レイヤ 3 IPv4 および IPv6 トラフィック、レイヤ 4 TCP、IGMP、および ICMP トラフィックの統計情報収集を設定できます。
- NetFlow カウント、メンテナンス、トラブルシューティング（デバッグ コマンド）。
- NetFlow 分析は、ネットワーク サービス モジュール上の物理インターフェイスを通るトラフィックに対して実行されます。スイッチは、転送判断を実行した後、出力（発信）トラフィックを処理します。プライベート VLAN または保護ポートを設定することで、ローカルでスイッチングされるか、サービス モジュール ポートを通じたルーテッド トラフィックを強制できます。

次の NetFlow の特性はサポートされていません。

- Netflow-5 プロトコル
- あらかじめ定義されたフロー レコード
- ISL
- ポリシーベースの NetFlow
- Cisco TrustSec モニタリング

Catalyst 3750-X および 3560-X に取り付けることができる他のモジュールは 1 ギガビットおよび 10 ギガビット アップリンク インターフェイスを搭載していますが、NetFlow はネットワーク サービス モジュールだけでサポートされます。

Flexible NetFlow の設定

次に、Flexible NetFlow のいくつかの基本的な設定を示します。

- 「カスタマイズしたフロー レコードの設定」（P.48-2）
- 「フロー エクスポータの設定」（P.48-5）
- 「カスタマイズしたフロー モニタの設定」（P.48-6）
- 「インターフェイスへのフロー モニタの適用」（P.48-8）
- 「フロー サンプリングの設定およびイネーブル化」（P.48-9）

Flexible NetFlow の詳細については、『*Cisco IOS Flexible NetFlow Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/12_4t/fnf_12_4t_book.html

コマンドの詳細については、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

http://www.cisco.com/en/US/docs/ios/fnetflow/command/reference/fnf_book.html

カスタマイズしたフロー レコードの設定

フロー レコードの次のキー フィールドを**照合**できます。

- IPv4 または IPv6 宛先アドレス

- 直接接続されたホストの MAC アドレスを示す、インターフェイスで受信または送信されるトラフィックのレイヤ 2 送信元と宛先アドレスおよび VLAN を識別するデータリンク フィールド。サービス クラス（CoS）および Ethertype データリンク ヘッダー フィールドも使用できます。
- アプリケーションのタイプ（ICMP、IGMP、または TCP トラフィック）を識別するトランスポート フィールドの送信元および宛先ポート。

フローレコードの次のキー フィールドを**収集**できます。

- 合計バイト数、エクスポータによって送信されるまたはフローまたはパケット（**exporter**）、または 64 ビット カウンタのバイト数またはパケット数（**long**）。
- 最初のパケットの送信時間または最新（**最後**）のパケットが見つかった時間からのシステム稼働時間に基づくタイムスタンプ。
- 入力または出力インターフェイスの SNMP インデックス。サービス モジュールに出入りするトラフィックのインターフェイスは、スイッチの転送キャッシュに基づいています。このフィールドは、一般にデータ リンク、IPv4 および IPv6 アドレスとともに使用され、直接接続されたホストの実際のファースト ホップのインターフェイスを提供します。
  - 値 0 は、インターフェイス情報がキャッシュにないことを意味します。
  - 一部の NetFlow コレクタでは、フロー レコードにこの情報が必要です。

詳細については、『*Cisco IOS Flexible NetFlow Configuration Guide*』および『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

特権 EXEC モードから、カスタマイズしたフロー レコードを設定する手順は、次のとおりです。

	コマンド	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	**flow record** *record-name*	フロー レコードを作成し、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。このコマンドを使用して既存のフロー レコードを変更することもできます。
ステップ 3	**description** *description*	（任意）フロー レコードの説明を作成します。
ステップ 4	**match** {**ipv4** | **ipv6**} {**destination** | **source**} **address** または **match datalink** {**destination-vlan-id** | **dot1q** | **ethertype** | **mac** | **source-vlan-id**} または **match transport** {**icmp** | **igmp**| **source-port** | **tcp** | **udp**}	フロー レコードの key フィールドを設定します。 詳細については、『*Cisco IOS Flexible NetFlow Configuration Guide*』および『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。
ステップ 5	追加ファイルをレコードに設定するには、ステップ 4 を繰り返します。	
ステップ 6	**collect counter** {**bytes** [**exported** | **long**] **flows** [**exported**] | **packets**} [**exported** | **long**] または **collect timestamp sys-uptime** {**first** | **last**} または **collect interface** {**input** | **output**} **snmp**	フローの 1 つ以上の送信元フィールドを、カウンタ フィールド、タイムスタンプ フィールド、またはインターフェイス フィールドに設定します。 詳細については、『*Cisco IOS Flexible NetFlow Configuration Guide*』および『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

	コマンド	目的
ステップ 7	必要に応じてステップ 6 を繰り返し、レコードの追加のフィールドを設定します。	
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config flow record**	（任意）設定されたフロー レコードを表示します。
ステップ 10	**show flow record**	（任意）フロー レコードのステータスを表示します。
ステップ 11	**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。

次に、フロー レコードを設定する例を示します。

```
Switch(config)# flow record
Switch(config-flow-record)# description record to monitor network traffic
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# collect counter packets
Switch(config-flow-record)# collect counter bytes
Switch(config-flow-record)# end
```

次の例では、**show flow record** コマンドの出力を示します。

```
Switch# show flow record
flow record L2L4ipv4:
  Description:        User defined
  No. of users:       1
  Total field space:  56 bytes
  Fields:
    match datalink dot1q priority
    match datalink mac source-address
    match datalink mac destination-address
    match ipv4 tos
    match ipv4 ttl
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    collect interface input snmp
    collect interface output snmp
    collect counter flows
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

flow record L2L4ipv6:
  Description:        User defined
  No. of users:       1
  Total field space:  81 bytes
  Fields:
    match datalink mac source-address
    match datalink mac destination-address
    match ipv6 traffic-class
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match ipv6 fragmentation flags
    match transport source-port
    match transport destination-port
    match transport icmp ipv6 type
    match transport icmp ipv6 code
```

```
collect interface input snmp
collect interface output snmp
collect counter flows
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

フロー エクスポータの設定

NetFlow エクスポータを設定するには、特権 EXEC モードで次の手順を実行します。Flexible NetFlow フロー エクスポータの設定の詳細については、『*Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters*』を参照してください。

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cfg_de_fnflow_exprts.html

（注）　任意の **export-protocol** フロー エクスポータ コンフィギュレーション コマンドは、エクスポータで使用される NetFlow エクスポート プロトコルを指定します。スイッチは **netflow-v9** だけをサポートします。CLI ヘルプに記載されていますが、**netflow-5** はサポートされません。

	コマンド	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	**flow exporter** *exporter-name*	フロー エクスポータを作成し、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。このコマンドを使用して既存のフロー エクスポータを変更することもできます。
ステップ 3	**description** *description*	（任意）コンフィギュレーションおよび **show flow exporter** コマンドの出力に表示されるエクスポータの説明を設定します。
ステップ 4	**destination** {*hostname* | *ip-address*} [**vrf** *vrf-name*]	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	**dscp** *dscp*	（任意）エクスポータによって送信されるデータグラムの Differentiated Services Code Point（DSCP; 差別化サービス コード ポイント）パラメータを設定します。DSCP の範囲は 0 ～ 63 です。デフォルトは 0 です。
ステップ 6	**source** *interface-id*	（任意）エクスポータで、エクスポートされたデータグラムの送信元 IP アドレスとして IP アドレスを使用するローカル インターフェイスを指定します。
ステップ 7	**option** {**exporter-stats** | **interface-table** | **sampler-table**} [**timeout** *seconds*]	（任意）エクスポータのオプション データ パラメータを設定します。3 つのオプションを同時に設定できます。 タイムアウトの範囲は 1 ～ 86400 秒です。デフォルト値は 600 です。
ステップ 8	**template data timeout** *seconds*	（任意）タイムアウトに基づいてテンプレートの再送信を設定します。指定できる範囲は 1 ～ 86400 秒です（86400 秒は 24 時間）。デフォルト値は 600 です。
ステップ 9	**transport udp** *udp-port*	エクスポートされるデータグラムを宛先システムが待機する UDP ポートを指定します。*udp-port* の範囲は 1 ～ 65536 です。
ステップ 10	**ttl** *seconds*	（任意）エクスポータによって送信されるデータグラムの存続可能時間（TTL）値を設定します。指定できる範囲は 1 ～ 255 秒です。デフォルトは 255 です。

	コマンド	目的
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show running-config flow exporter** *exporter-name*	（任意）設定済みのフロー エクスポータを確認します。
ステップ 13	**show flow exporter** *exporter-name*	（任意）フロー エクスポータのステータスを表示します。
ステップ 14	**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。

次に、フロー エクスポータを設定する例を示します。

```
Switch(config)# flow exporter QoS-Collector
Switch(config-flow-exporter)# description QoS Collector Bldg 19
Switch(config-flow-exporter)# destination 172.20.244.28
Switch(config-flow-exporter)# source vlan 1
Switch(config-flow-exporter)# dscp 3
Switch(config-flow-exporter)# transport udp 2055
Switch(config-flow-exporter)# end
```

次の例では、**show flow exporter** コマンドの出力を示します。

```
Switch# show flow exporter EXPORTER-1
Flow Exporter QoS-Collector:
  Description:              QoS Collector Bldg 19
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 172.20.244.28
    Source IP address:      10.30.0.234
    Source Interface:       Vlan1
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            62401
    DSCP:                   0x3
    TTL:                    255
    Output Features:        Not Used
```

カスタマイズしたフロー モニタの設定

特権 EXEC モードから、次の手順に従って NetFlow モニタを設定します。

	コマンド	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	**flow monitor** *monitor -name*	フロー モニタを作成し、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。このコマンドを使用して既存のフロー モニタを変更することもできます。
ステップ 3	**description** ***description***	（任意）フロー モニタの説明を設定します。
ステップ 4	**record** *record-name*	フロー モニタのレコードを指定します。

	コマンド	目的
ステップ 5	**cache** {**timeout active** *seconds* | **type normal**}	（任意）フロー モニタ キャッシュ パラメータ（タイムアウト値、キャッシュ エントリ数、キャッシュ タイプなど）を変更します。 • **timeout active** *seconds*：アクティブフロー タイムアウトを設定します。これは、トラフィック分析の細かさを定義します。指定できる範囲は 1 ～ 604800 秒です。デフォルト値は 1800 です。一般的な値は 60 または 300 秒です。推奨値については、『*Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters*』を参照してください。 • **type normal**：フロー キャッシュからの通常のフロー削除を設定します。 **（注）** コマンドラインのヘルプには記載されていますが、**entries** キーワードとタイムアウト **inactive** および **update** はサポートされません。
ステップ 6	フロー モニタの追加キャッシュ パラメータを設定するには、ステップ 5 を繰り返します。	
ステップ 7	**exporter** *exporter-name*	（任意）事前に作成されたエクスポータの名前を指定します。
ステップ 8	追加エクスポータを設定するには、ステップ 5 を繰り返します。	
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show running-config flow monitor** *monitor -name*	（任意）フロー モニタの設定を確認します。
ステップ 11	**show flow monitor** *monitor -name*	（任意）フロー モニタの現在のステータスが表示されます。
ステップ 12	**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。

次に、フロー モニタを設定する例を示します。

```
Switch(config)# flow monitor FLOW-MONITOR-1
Switch(config-flow-monitor)# Used for ipv4 traffic analysis
Switch(config-flow-monitor)# record FLOW-RECORD-1
Switch(config-flow-monitor)# cache timeout active 300
Switch(config-flow-monitor)# cache type normal
Switch(config-flow-monitor)# exporter EXPORTER-1
Switch(config-flow-monitor)# exit
```

次の例では、**show flow monitor** コマンドの出力を示します。

```
Switch# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic ipv4 traffic analysis
  Flow Record:       FLOW-RECORD-1
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:              normal (Platform cache)
    Status:            allocated
    Size:              Unknown
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs    1800 secs
    Update Timeout:    1800 secs
```

インターフェイスへのフロー モニタの適用

特権 EXEC モードから、次の手順に従ってインターフェイスに NetFlow モニタを適用します。

	コマンド	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	**interface** *interface-id*	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。Flexible NetFlow は、サービス モジュールの 1 ギガビットまたは 10 ギガビット イーサネット インターフェイスのみでサポートされます。 **（注）** ポート チャネル インターフェイスには NetFlow モニタを接続できません。サービス モジュールの両方のインターフェイスが EtherChannel の一部である場合、両方の物理インターフェイスにモニタを接続する必要があります。
ステップ 3	{**ip** | **ipv6**} **flow monitor** *monitor -name* [**layer2-switched** | **multicast** | **sampler** | **unicast**] {**input** | **output**}	着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。 • **ip**：IPv4 IP アドレスに一致するレコードを入力します。 • **ipv6**：IPv6 IP アドレスに一致するレコードを入力します。 **（注）** このキーワードは、デュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートがスイッチに設定されている場合にだけ表示されます。 • **layer2-switched**：（任意）レイヤ 2 スイッチド トラフィックにフロー モニタを適用します。 • **multicast**：（任意）マルチキャスト トラフィックにフロー モニタを適用します。 • **sampler**：（任意）サンプラにフロー モニタを適用します。 • **unicast**：（任意）ユニキャスト トラフィックにフロー モニタを適用します。 • **input**：入力トラフィックにフロー モニタを適用します。 • **output**：出力トラフィックにフロー モニタを適用します。
ステップ 4	**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 5	フロー モニタの追加キャッシュ パラメータを設定するには、ステップ 2 および 3 を繰り返します。	
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show flow interface** *interface-id*	（任意）Flexible NetFlow がインターフェイスに設定されていることを確認します。
ステップ 8	**show flow monitor name** *monitor -name* **cache**	（任意）フロー モニタ キャッシュ内のデータを表示します。
ステップ 9	**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。

次に、フロー モニタをインターフェイスに適用する例を示します。

```
Switch(config)# interface gigabitethernet 1/1/2
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

```
Switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
Switch(config-if)# end
```

次の例では、**show flow interface** コマンドの出力を示します。

```
Switch# show flow interface gigabitethernet 1/1/2

Interface Gigabit Ethernet1/1/2
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          FLOW-MONITOR-2
        direction:        Input
        traffic(ipv6):    on
```

フロー サンプリングの設定およびイネーブル化

特権 EXEC モードから、フロー サンプリングをイネーブル化および設定する手順は、次のとおりです。

	コマンド	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	**sampler** *sampler -name*	フロー モニタを作成し、Flexible NetFlow サンプラ コンフィギュレーション モードを開始します。このコマンドを使用して既存のサンプラを変更することもできます。
ステップ 3	**description** ***description***	（任意）サンプラの説明を設定します。
ステップ 4	**mode random 1 out-of** *window-size*	パケットを選択するモードとウィンドウ サイズを指定します。ウィンドウ サイズの範囲は 2 ～ 32768 です。 **（注）** CLI ヘルプには記載されていますが、**mode deterministic** キーワードはサポートされません。
ステップ 5	**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	**interface** *interface-id*	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。Flexible NetFlow は、サービス モジュールの 1 ギガビットまたは 10 ギガビット イーサネット インターフェイスのみでサポートされます。
ステップ 7	{**ip**| **ipv6**} **flow monitor** *monitor-name* **sampler** *sampler-name* {**input** | **output**}	トラフィックを分析するためにインターフェイスに割り当てることで、作成済みの IPv4 または IPv6 フロー モニタをアクティブにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show sampler** *sampler -name*	（任意）フロー サンプラの現在のステータスが表示されます。
ステップ 10	**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。

次に、フロー サンプラを設定してイネーブルにする方法を示します。

```
Switch(config)# sampler SAMPLER-1
Switch(config-sampler)# description Sample at 50
Switch(config-sampler)# mode random 1 out-of 2
Switch(config-sampler)# exit
Switch(config)# interface gigabitethernet 1/1/2
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLE-1 input
```

次の例では、**show sampler** コマンドの出力を示します。

```
Switch# show sampler SAMPLER-1
```

```
Sampler SAMPLER-1:
  ID:             2
  Description:    Sample at 50%
  Type:           random
  Rate:           1 out of 2
  Samples:        2482
  Requests:       4964
  Users (1):
    flow monitor FLOW-MONITOR-1 (ip,Et0/0,I  2482 out of 4964
```