Cisco IOS Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズ

このドキュメントには、Flexible NetFlow フロー レコードおよびフロー モニタについて、およびそのカスタマイズ方法に関する説明が記載されています。「Getting Started with Configuring Cisco IOS Flexible NetFlow」モジュールおよび「Configuring Cisco IOS Flexible NetFlow with Predefined Records」モジュールに示されたタスクおよび設定例が、実際のトラフィック分析要件に適合しない場合は、このドキュメントに記載された情報と説明を使用して Flexible NetFlow をカスタマイズし、実際のトラフィック分析要件に合わせてください。

NetFlow は、ルータを流れるパケットの統計情報が得られる、Cisco IOS 技術の 1 つです。NetFlow は、IP ネットワークから実際の IP データを取得するための標準規格です。NetFlow を利用すると、ネットワークとセキュリティの監視、ネットワーク計画、トラフィック分析、および IP アカウンティングをサポートするためのデータが得られます。

Flexible NetFlow は、実際の要件に合わせてトラフィック分析パラメータをカスタマイズする機能を追加することで、以前の NetFlow よりも改善されています。Flexible NetFlow では、トラフィック分析のための非常に複雑な構成を作成したり、再利用可能な構成コンポーネントを使用してデータをエクスポートすることが容易になります。

機能情報の検索

このモジュールに記載されている機能の一部が、ご使用のソフトウェア リリースでサポートされていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「Flexible NetFlow の機能情報」（P.22）を参照してください。

プラットフォームのサポート、ならびに Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズの前提条件

Flexible NetFlow を設定するには、次の前提条件を満たしている必要があります。

- 「Cisco IOS Flexible NetFlow Overview」モジュールに記載された内容をよく理解していること。
- 『*Cisco IOS Flexible NetFlow Command Reference*』で次のコマンドに定義された、Flexible NetFlow の key フィールドをよく理解していること。
  - **match flow**
  - **match interface**
  - **match {ipv4 | ipv6}**
  - **match routing**
  - **match transport**
- 『*Cisco IOS Flexible NetFlow Command Reference*』で次のコマンドに定義された、Flexible NetFlow の nonkey フィールドをよく理解していること。
  - **collect counter**
  - **collect flow**
  - **collect interface**
  - **collect {ipv4 | ipv6}**
  - **collect routing**
  - **collect timestamp sys-uptime**
  - **collect transport**
- ネットワーク デバイスで、Flexible NetFlow がサポートされた Cisco IOS リリースが稼動していること。Flexible NetFlow をサポートした Cisco IOS ソフトウェア リリースのリストについては、「Cisco IOS Flexible NetFlow Features Roadmap」を参照してください。

IPv4 トラフィック

- ネットワーク デバイスが、IPv4 ルーティング用に設定されていること。
- シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングのいずれかが、使用中のルータおよび Flexible NetFlow をイネーブルにするすべてのインターフェイスでイネーブルにされていること。

IPv6 トラフィック

- ネットワーク デバイスが、IPv6 ルーティング用に設定されていること。
- シスコ エクスプレス フォワーディング IPv6 または分散型シスコ エクスプレス フォワーディングのいずれかが、使用中のルータおよび Flexible NetFlow をイネーブルにするすべてのインターフェイスでイネーブルにされていること。

Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズについて

Flexible NetFlow フロー レコードおよびフロー モニタをカスタマイズするには、次の概念を理解しておく必要があります。

- 「分析に使用するトラフィックの識別基準」（P.3）

分析に使用するトラフィックの識別基準

事前定義済みの Flexible NetFlow レコードが実際のトラフィック要件に適合しない場合は、Flexible NetFlow の **collect** および **match** コマンドを使用して、ユーザ定義（カスタム）レコードを作成できます。カスタム レコードを作成するには、その前に key および nonkey フィールドに使用する基準を決定する必要があります。

ネットワーク攻撃検出用のカスタム レコードを作成する場合は、適切な key および nonkey フィールドをレコードに含めることで、ルータが攻撃の分析と対処に必要なフローを作成し、データをキャプチャする必要があります。たとえば、SYN フラッド攻撃はよくある DoS（サービス拒絶）攻撃で、宛先ホストへの TCP 要求のフラッディング開始に TCP フラグが使用されます。通常の TCP 接続が開始されると、宛先ホストは SYN（同期/開始）パケットを送信元ホストから受信し、SYN ACK（同期確認応答）を返送します。その後、宛先ホストは SYN ACK に対する ACK（確認応答）を受け取ってから、接続を確立する必要があります。これは、「TCP 3 ウェイ ハンドシェイク」と呼ばれます。宛先ホストは SYN ACK に対する ACK を待つ間、宛先ホスト上の有限サイズの接続キューが接続を監視し、接続完了を待ちます。通常、ACK は SYN ACK から数ミリ秒後に到着するため、このキューはすぐに空になります。TCP SYN 攻撃ではこの設計を悪用し、攻撃側の送信元ホストがランダムな送信元アドレスを持つ TCP SYN パケットを発生して、攻撃を受けるホストに送信します。攻撃を受けた宛先ホストは、ランダムな送信元アドレスに SYN ACK を返送し、接続キューにエントリを追加します。この SYN ACK の宛先は不正または存在しないホストであるため、TCP 3 ウェイ ハンドシェイクの最後の部分が完了することはなく、接続キューのエントリは、通常は 1 分間程度のタイマーが期限切れとなるまで残ります。送信元ホストが、ランダムな IP アドレスからの偽の TCP SYN パケットを急速に大量発生することで、接続キューがいっぱいになり、正規ユーザに対する TCP サービス（電子メール、ファイル転送、WWW など）が拒絶されることがあります。

この種の DoS 攻撃に対するセキュリティ監視レコードに必要な情報には、次の key および nonkey フィールドが含まれます。

- key フィールド：
  - 宛先 IP アドレスまたは宛先 IP サブネット
  - TCP フラグ
  - パケット数

- nonkey フィールド
  - 宛先 IP アドレス
  - 送信元 IP アドレス
  - インターフェイスの入力および出力

ヒント 多くのユーザは、DoS 攻撃の詳細な Flexible NetFlow 表示がトリガーされるよう、これらの key および nonkey フィールドを使用して、一般的な Flexible NetFlow モニタを設定しています。

Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズ方法

ここに示すタスクは、次のことを行うための方法を示しています。

- Flexible NetFlow フロー レコードのカスタマイズ。
- Flexible NetFlow フロー モニタのカスタマイズ。
- Flexible NetFlow のイネーブル化。

（注） これらのタスクでは、そのタスクで使用される Flexible NetFlow コマンドに必要なキーワードと引数だけが示されています。これらの Flexible NetFlow コマンドで使用可能なその他のキーワードと引数については、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

Flexible NetFlow フロー レコードおよびフロー モニタをカスタマイズし、Flexible NetFlow をイネーブルにするには、次のタスクを実行します。

- 「カスタム フロー レコードの設定」（P.4）（必須）
- 「フロー レコードの現在のステータスの表示」（P.6）（任意）
- 「フロー レコードの設定確認」（P.7）（任意）
- 「カスタム フロー モニタの作成」（P.8）（必須）
- 「フロー モニタの現在のステータスの表示」（P.11）（任意）
- 「フロー モニタの設定確認」（P.11）（任意）
- 「インターフェイスへのフロー モニタの適用」（P.12）（必須）
- 「インターフェイスで Flexible NetFlow がイネーブル化されていることの確認」（P.13）（任意）
- 「フロー モニタ キャッシュ内のデータの表示」（P.14）（任意）

カスタム フロー レコードの設定

カスタム フロー レコードは、特定の目的でトラフィック データを分析するために使用されます。カスタム フロー レコードには、key フィールドとして使用する最低 1 つの **match** 基準が必要で、通常は nonkey フィールドとして使用する最低 1 つの **collect** 基準が必要です。

カスタム フロー レコードには、数百の順列と組み合せが存在します。このタスクでは、可能な順列と組み合せの 1 つを作成するための手順を示します。このタスクの手順を必要に応じて変更すると、実際の要件に合ったカスタム フロー レコードを作成できます。

カスタム フロー レコードを作成するには、次のタスクを実行します。

- 「IPv4 または IPv6 トラフィック用のカスタム フロー レコードの設定」

IPv4 または IPv6 トラフィック用のカスタム フロー レコードの設定

このタスクでは、IPv4 または IPv6 トラフィック用のカスタム フロー レコードの作成に使用する手順を示します。これは、IPv4 または IPv6 トラフィックから特定のデータを収集するために使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *descrription*
5. **match** {**ipv4** | **ipv6**} {**destination** | **source**} {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}
6. 必要に応じてステップ 5 を繰り返し、レコードのその他の key フィールドを設定します。
7. **collect** {**ipv4** | **ipv6**} **source** {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}
8. 必要に応じてステップ 7 を繰り返し、レコードのその他の nonkey フィールドを設定します。
9. **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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(config)# flow record FLOW-RECORD-1`	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。 • このコマンドでは、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 4	**description** *description* **例：** `Router(config-flow-record)# description Used for basic traffic analysis`	（任意）フロー レコードの説明を作成します。

	コマンドまたはアクション	目的
ステップ 5	**match** {**ipv4** | **ipv6**} {**destination** | **source**} {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]} **例：** `Router(config-flow-record)# match ipv4 destination address`	フロー レコードの key フィールドを設定します。 **（注）** この例では、レコードの key フィールドとして、IPv4 宛先アドレスを設定します。**match ipv4** コマンドで使用可能なその他の key フィールド、および key フィールドの設定に使用可能なその他の **match** コマンドについては、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。
ステップ 6	必要に応じてステップ 5 を繰り返し、レコードのその他の key フィールドを設定します。	—
ステップ 7	**collect** {**ipv4** | **ipv6**} **source** {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]} **例：** `Router(config-flow-record)# collect ipv4 source address`	レコードの nonkey フィールドとして、1 つ以上の IPv4 送信元フィールドを設定します。 **（注）** この例では、レコードの nonkey フィールドとして、IPv4 送信元アドレスを設定します。nonkey フィールドの設定に使用可能なその他の **collect** コマンドについては、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。
ステップ 8	必要に応じてステップ 7 を繰り返し、レコードのその他の nonkey フィールドを設定します。	—
ステップ 9	**end** **例：** `Router(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 レコードの現在のステータスの表示

フロー レコードの現在のステータスを表示するには、次の任意タスクを実行します。

手順の概要

1. **enable**
2. **show flow record**

手順の詳細

ステップ 1 **enable**

enable コマンドによって、特権 EXEC モードを開始します（プロンプトが表示されたらパスワードを入力します）。

```
Router> enable

Router#
```

ステップ 2 **show flow record**

show flow record コマンドでは、指定したフロー モニタの現在のステータスが表示されます。

```
Router# show flow record
```

```
flow record FLOW-RECORD-2:
  Description:        Used for basic IPv6 traffic analysis
  No. of users:       1
  Total field space:  53 bytes
  Fields:
    match ipv6 destination address
    collect ipv6 protocol
    collect ipv6 source address
    collect transport source-port
    collect transport destination-port
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

flow record FLOW-RECORD-1:
  Description:        Used for basic IPv4 traffic analysis
  No. of users:       1
  Total field space:  29 bytes
  Fields:
    match ipv4 destination address
    collect ipv4 protocol
    collect ipv4 source address
    collect transport source-port
    collect transport destination-port
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

フロー レコードの設定確認

入力したコンフィギュレーション コマンドを確認するには、次の任意タスクを実行します。

手順の概要

1. **enable**
2. **show running-config flow record**

手順の詳細

ステップ 1 **enable**

enable コマンドによって、特権 EXEC モードを開始します（プロンプトが表示されたらパスワードを入力します）。

```
Router> enable

Router#
```

ステップ 2 **show running-config flow record**

show running-config flow record コマンドでは、指定したフロー モニタのコンフィギュレーション コマンドが表示されます。

```
Router# show running-config flow record

Current configuration:
```

```
!
flow record FLOW-RECORD-2
 description Used for basic IPv6 traffic analysis
 match ipv6 destination address
 collect ipv6 protocol
 collect ipv6 source address
 collect transport source-port
 collect transport destination-port
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
flow record FLOW-RECORD-1
 description Used for basic IPv4 traffic analysis
 match ipv4 destination address
 collect ipv4 protocol
 collect ipv4 source address
 collect transport source-port
 collect transport destination-port
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

カスタム フロー モニタの作成

カスタム フロー モニタを作成するには、次の必須タスクを実行します。

フロー モニタ

各フロー モニタは、それに関連付けられた個別のキャッシュを持っています。各フロー モニタには、キャッシュ エントリの内容とレイアウトを定義するためのレコードが必要です。このレコード形式は、事前定義済みの形式の 1 つにすることも、高度なユーザが **flow record** コマンドを使用してカスタム形式を作成することもできます。このタスクでは、「カスタム フロー レコードの設定」（P.4）で作成したレコードを使用します。

前提条件

Flexible NetFlow の定義済みレコードではなく、カスタム レコードを使用する場合は、このタスクを実行する前にカスタム レコードを作成しておく必要があります。カスタム フロー レコードについて、およびその作成方法については、「カスタム フロー レコードの設定」（P.4）を参照してください。

データのエクスポートのため、フロー モニタにフロー エクスポータを追加する場合は、このタスクを終了する前にエクスポータを作成しておく必要があります。フロー エクスポータについて、およびその作成方法については、「Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters」モジュールを参照してください。

制約事項

フロー モニタで **record** コマンドのパラメータを変更するには、その前に **no ip flow monitor** コマンドを使用して、適用されたすべてのインターフェイスからフロー モニタを削除しておく必要があります。**ip flow monitor** 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *string*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **cache** {**entries** *number* | **timeout** {**active** *seconds* | **inactive** *seconds* | **update** *seconds*} | **type** {**immediate** | **normal** | **permanent**}}
7. 必要に応じてステップ 6 を繰り返し、このフロー モニタのキャッシュ パラメータの変更を終了します。
8. **statistics packet protocol**
9. **statistics packet size**
10. **exporter** *exporter-name*
11. **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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(config)# flow monitor FLOW-MONITOR-1`	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。 • このコマンドでは、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 4	**description** *string* **例：** `Router(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	（任意）フロー モニタの説明を作成します。

	コマンドまたはアクション	目的
ステップ 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **例：** `Router(config-flow-monitor)# record FLOW-RECORD-1`	フロー モニタのレコードを指定します。
ステップ 6	**cache** {**entries** *number* | **timeout** {**active** *seconds* | **inactive** *seconds*| **update** *seconds*} | **type** {**immediate** | **normal** | **permanent**}} **例：** `Router(config-flow-monitor)# cache entries 1000`	（任意）タイムアウト値、キャッシュのエントリ数、キャッシュ タイプなど、フロー モニタのキャッシュ パラメータを変更します。 • キャッシュ タイプが **immediate** に設定されている場合、**timeout** キーワードに関連付けられたキーワードの値は無効になります。
ステップ 7	必要に応じてステップ 6 を繰り返し、このフロー モニタのキャッシュ パラメータの変更を終了します。	—
ステップ 8	**statistics packet protocol** **例：** `Router(config-flow-monitor)# statistics packet protocol`	（任意）Flexible NetFlow モニタのプロトコル分散統計情報の収集をイネーブルにします。
ステップ 9	**statistics packet size** **例：** `Router(config-flow-monitor)# statistics packet size`	（任意）Flexible NetFlow モニタのサイズ分散統計情報の収集をイネーブルにします。
ステップ 10	**exporter** *exporter-name* **例：** `Router(config-flow-monitor)# exporter EXPORTER-1`	（任意）作成済みのエクスポータの名前を指定します。 • フロー エクスポータについて、およびその設定方法については、「Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters」モジュールを参照してください。
ステップ 11	**end** **例：** `Router(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。

フロー モニタの現在のステータスの表示

フロー モニタの現在のステータスを表示するには、次の任意タスクを実行します。

手順の概要

1. **enable**
2. **show flow monitor** *monitor-name*

手順の詳細

ステップ 1 **enable**

enable コマンドによって、特権 EXEC モードを開始します（プロンプトが表示されたらパスワードを入力します）。

```
Router> enable

Router#
```

ステップ 2 **show flow monitor** *monitor-name*

show flow monitor コマンドでは、指定したフロー モニタの現在のステータスが表示されます。

```
Router# 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
    Status:            allocated
    Size:              1000 entries / 50052 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
  Stats:
    protocol distribution
    size distribution
```

フロー モニタの設定確認

入力したコンフィギュレーション コマンドを確認するには、次の任意タスクを実行します。

手順の概要

1. **enable**
2. **show running-config flow monitor** *monitor-name*

手順の詳細

ステップ 1 **enable**

enable コマンドによって、特権 EXEC モードを開始します（プロンプトが表示されたらパスワードを入力します）。

```
Router> enable

Router#
```

ステップ 2　show running-config flow monitor

show running-config flow monitor コマンドでは、指定したフロー モニタのコンフィギュレーション コマンドが表示されます。

```
Router# show running-config flow monitor FLOW-MONITOR-1

Current configuration:
!
flow monitor FLOW-MONITOR-1
 description Used for basic ipv4 traffic analysis
 record FLOW-RECORD-1
 exporter EXPORTER-1
 cache entries 1000
 statistics packet protocol
 statistics packet size
!
```

インターフェイスへのフロー モニタの適用

アクティブにする前に、フロー モニタを最低 1 つのインターフェイスに適用する必要があります。フロー モニタをアクティブにするには、次の必須タスクを実行します。

制約事項

事前定義済みレコード「NetFlow original」、または「NetFlow IPv4 original input」あるいは「NetFlow IPv6 original input」をフロー モニタに指定して、以前の NetFlow をエミュレートする場合は、Flexible NetFlow フロー モニタを入力（受信）トラフィックの分析だけに使用できます。

事前定義済みレコード「NetFlow IPv4 original output」または「NetFlow IPv6 original output」をフロー モニタに指定して、出力 NetFlow アカウンティング機能をエミュレートする場合は、Flexible NetFlow フロー モニタを出力（発信）トラフィックの分析だけに使用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. {**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**}
5. ステップ 3 と 4 を繰り返し、トラフィックを監視するルータの他のすべてのインターフェイスでフロー モニタをアクティブにします。
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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(config)# interface ethernet 0/0`	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** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**} **例：** `Router(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	ステップ 3 と 4 を繰り返し、トラフィックを監視するルータの他のすべてのインターフェイスでフロー モニタをアクティブにします。	—
ステップ 6	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイスで Flexible NetFlow がイネーブル化されていることの確認

インターフェイスで Flexible NetFlow がイネーブルになっていることを確認するには、次の任意タスクを実行します。

手順の概要

1. **enable**
2. **show flow interface** [*type number*]

手順の詳細

ステップ 1 **enable**

enable コマンドによって、特権 EXEC モードを開始します（プロンプトが表示されたらパスワードを入力します）。

```
Router> enable

Router#
```

ステップ 2　show flow interface

show flow interface コマンドによって、インターフェイスで Flexible NetFlow がイネーブルになっていることが確認されます。

```
Router# show flow interface ethernet 0/0

Interface Ethernet0/0
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          FLOW-MONITOR-2
        direction:        Input
        traffic(ipv6):    on

Router# show flow interface ethernet 1/0

Interface Ethernet1/0
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      on
  FNF:  monitor:          FLOW-MONITOR-2
        direction:        Output
        traffic(ipv6):    on
```

フロー モニタ キャッシュ内のデータの表示

フロー モニタ キャッシュ内のデータを表示するには、次の任意タスクを実行します。

前提条件

フロー モニタ キャッシュ内のフローを表示するためには、NetFlow original レコードで定義された基準に適合するトラフィックを受信するインターフェイスに、入力フロー モニタを適用する必要があります。

手順の概要

1. **enable**
2. **show flow monitor name** *monitor-name* **cache format record**

手順の詳細

ステップ 1　enable

enable コマンドによって、特権 EXEC モードを開始します（プロンプトが表示されたらパスワードを入力します）。

```
Router> enable

Router#
```

ステップ 2　show flow monitor name *monitor-name* **cache format record**

show flow monitor name *monitor-name* **cache format record** コマンド ストリングでは、フロー モニタのキャッシュ内にあるステータス、統計情報、およびフロー データが表示されます。

```
Router# show flow monitor name FLOW-MONITOR-1 cache format record

Cache type:                               Normal
  Cache size:                               1000
  Current entries:                             4
  High Watermark:                              4

  Flows added:                               101
  Flows aged:                                 97
    - Active timeout   (  1800 secs)           3
    - Inactive timeout (    15 secs)          94
    - Event aged                               0
    - Watermark aged                           0
    - Emergency aged                           0

IPV4 DESTINATION ADDRESS:  172.16.10.5
ipv4 source address:       10.10.11.1
trns source port:          25
trns destination port:     25
counter bytes:             72840
counter packets:           1821
timestamp first:           21237828
timestamp last:            22086520
ip protocol:               6

IPV4 DESTINATION ADDRESS:  172.16.10.2
ipv4 source address:       10.10.10.2
trns source port:          20
trns destination port:     20
counter bytes:             3913860
counter packets:           7326
timestamp first:           21238788
timestamp last:            22088080
ip protocol:               6

IPV4 DESTINATION ADDRESS:  172.16.10.200
ipv4 source address:       192.168.67.6
trns source port:          0
trns destination port:     3073
counter bytes:             51072
counter packets:           1824
timestamp first:           21239228
timestamp last:            22087980
ip protocol:               1

Router# show flow monitor name FLOW-MONITOR-2 cache format record

Cache type:                               Normal
  Cache size:                               1000
  Current entries:                             2
  High Watermark:                              3

  Flows added:                                95
  Flows aged:                                 93
    - Active timeout   (  1800 secs)           0
    - Inactive timeout (    15 secs)          93
    - Event aged                               0
    - Watermark aged                           0
    - Emergency aged                           0

IPV6 DESTINATION ADDRESS:  2001:DB8:4:ABCD::2
ipv6 source address:       2001:DB8:1:ABCD::1
trns source port:          33572
trns destination port:     23
```

```
counter bytes:              19140
counter packets:            349
timestamp first:            2172704
timestamp last:             2198272
ip protocol:                6

IPV6 DESTINATION ADDRESS:   FF02::9
ipv6 source address:        FE80::A8AA:BBFF:FEBB:CC03
trns source port:           521
trns destination port:      521
counter bytes:              92
counter packets:            1
timestamp first:            2195672
timestamp last:             2195672
ip protocol:                17
```

Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズの設定例

ここでは、次の設定例について説明します。

可能なフローの数が制限された永久フロー レコード キャッシュの設定：例

次の例は、ルータのすべてのインターフェイスでの、タイプ オブ サービス（ToS）フィールド使用状況を監視するよう設計されています。この例は、**show flow monitor** コマンドを使用してルータ上の追加データをキャプチャし、分析に使用することを目的としているため、エクスポータは設定されません。

このサンプルは、グローバル コンフィギュレーション モードから開始します。

```
!
ip cef
!
flow record QOS_RECORD
 description UD: Flow Record to monitor the use of TOS within this router/network
 match interface input
 match interface output
 match ipv4 tos
 collect counter packets
 collect counter bytes
 exit
!
flow monitor QOS_MONITOR
 description UD: Flow Monitor which watches the limited combinations of interface and TOS
 record QOS_RECORD
 cache type permanent
 cache entries 8192   ! 2^5 (combos of interfaces) * 256 (values of TOS)
 exit
```

```
!
interface ethernet0/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface ethernet0/1
 ip flow monitor QOS_MONITOR input
 exit
!
interface ethernet0/2
 ip flow monitor QOS_MONITOR input
 exit
!
interface serial2/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface serial2/1
 ip flow monitor QOS_MONITOR input
!
```

show flow monitor コマンドの出力には、キャッシュの現在のステータスが表示されます。

```
Router# show flow monitor QOS_MONITOR cache

  Cache type:                           Permanent
  Cache size:                                8192
  Current entries:                              2
  High Watermark:                               2

  Flows added:                                  2
  Updates sent         (  1800 secs)            0
```

IPv6 トラフィック監視用のカスタム フロー レコード設定：例

次の例では、IPv6 トラフィック監視用のカスタム フロー レコード キャッシュを作成します。

このサンプルは、グローバル コンフィギュレーション モードから開始します。

```
!
ip cef
ipv6 cef
!
flow record FLOW-RECORD-2
 description Used for basic IPv6 traffic analysis
 match ipv6 destination address
 collect ipv6 protocol
 collect ipv6 source address
 collect transport source-port
 collect transport destination-port
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
flow monitor FLOW-MONITOR-2
 description Used for basic IPv6 traffic analysis
 record FLOW-RECORD-2
 cache entries 1000
 statistics packet protocol
 statistics packet size
!
```

```
interface Ethernet0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 input
!
interface Ethernet1/0
 ipv6 address 2001:DB8:3:ABCD::1/48
 ipv6 flow monitor FLOW-MONITOR-2 output
!
```

MAC および VLAN 統計情報監視用の Flexible NetFlow の設定：例

次の例は、MAC および VLAN 統計情報監視用に Flexible NetFlow を設定する方法を示しています。

このサンプルは、グローバル コンフィギュレーション モードから開始します。

```
!
 flow record LAYER-2-FIELDS-1
 match ipv4 source address
 match ipv4 destination address
 collect datalink dot1q vlan output
 collect datalink mac source address input
 collect datalink mac source address output
 collect datalink mac destination address input
 collect flow direction
 collect counter bytes
 collect counter packets
!
 exit
!
!
flow monitor FLOW-MONITOR-4
 record LAYER-2-FIELDS-1
 exit
!
ip cef
!
interface Ethernet0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

入力 VRF サポートのための Flexible NetFlow の設定：例

次の例では、Virtual Route Forwarding（VRF）ID を key フィールドとして収集するフロー レコードを持つ入力フロー モニタを適用することで、ルータの着信パケットからの VRF ID の収集を設定します。

このサンプルは、グローバル コンフィギュレーション モードから開始します。

```
!
flow record rm_1
match routing vrf input
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
```

```
!
interface Serial2/0
ip vrf forwarding green
ip address 172.16.2.2 255.255.255.252
ip flow monitor mm_1 output
!
end
```

ネットワーク ベースのアプリケーション認識のための Flexible NetFlow の設定：例

次の例では、アプリケーション名を key フィールドとして収集するフロー レコードを持つフロー モニタを適用することで、任意の 2 台の IP ホスト間で見られるアプリケーションごとに異なるフローを作成するために、Network Based Application Recognition（NBAR）を使用します。

このサンプルは、グローバル コンフィギュレーション モードから開始します。

```
!
flow record rm_1
match application name
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

次の作業

Flexible NetFlow に対してデータ エクスポートを設定する場合は、「Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters」モジュールを参照してください。

フロー サンプリングを設定して、トラフィック分析による CPU オーバーヘッドを軽減する場合は、「Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic」モジュールを参照してください。

Flexible NetFlow に対していずれかの事前定義済みレコードを設定する場合は、「Configuring Cisco IOS Flexible NetFlow with Predefined Records」モジュールを参照してください。

参考資料

ここでは、Flexible NetFlow に関する参考資料について説明します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Flexible NetFlow の概要	「Cisco IOS Flexible NetFlow Overview」
Flexible NetFlow の機能ロードマップ	「Cisco IOS Flexible NetFlow Features Roadmap」
Flexible NetFlow による以前の NetFlow のエミュレーション	「Getting Started with Configuring Cisco IOS Flexible NetFlow」
Flexible NetFlow データをエクスポートするためのフロー エクスポータの設定	「Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters」
Flexible NetFlow のトラフィック監視によるオーバーヘッド軽減のためのフロー サンプリング設定	「Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic」
事前定義済みレコードを使用した Flexible NetFlow の設定	「Configuring Cisco IOS Flexible NetFlow with Predefined Records」
Flexible NetFlow Top N Talkers を使用したネットワーク トラフィックの分析	「Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic」
Flexible NetFlow 用の IPv4 マルチキャスト統計情報サポートの設定	「Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow」
Flexible NetFlow のコンフィギュレーション コマンド	『*Cisco IOS Flexible NetFlow Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB の場所を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Flexible NetFlow の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1)、あるいは Cisco IOS Release 12.2(1) または 12.0(3)S 以降のリリースで導入または変更された機能だけが示されています。

ここに示されていないこの技術の機能の詳細については、「Cisco IOS Flexible NetFlow Features Roadmap」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS および Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　Flexible NetFlow の機能情報

機能名	リリース	機能情報
Flexible NetFlow	12.2(33)SRC 12.4(9)T	Flexible NetFlow が導入されました。 この機能のサポートは、Cisco 7200 シリーズ ルータ用として Cisco IOS Release 12.2(33)SRC で追加されました。 Flexible NetFlow 機能については、次の各項に説明があります。 • 「Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズの前提条件」（P.2） • 「Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズについて」（P.3） • 「Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズ方法」（P.4） • 「Flexible NetFlow フロー レコードおよびフロー モニタのカスタマイズの設定例」（P.16） 次のコマンドが導入または変更されました。**cache**（Flexible NetFlow）、**clear flow exporter**、**clear flow monitor**、**clear sampler**、**collect counter**、**collect flow**、**collect interface**、**collect ipv4**、**collect ipv4 destination**、**collect ipv4 fragmentation**、**collect ipv4 section**、**collect ipv4 source**、**collect ipv4 total-length**、**collect ipv4 ttl**、**collect routing**、**collect timestamp sys-uptime**、**collect transport**、**collect transport icmp ipv4**、**collect transport tcp**、**collect transport udp**、**debug flow exporter**、**debug flow monitor**、**debug flow record**、**debug sampler**、**description**（Flexible NetFlow）、**destination**、**dscp**（Flexible NetFlow）、**exporter**、**flow exporter**、**flow monitor**、**flow record**、**ip flow monitor**、**match flow**、**match interface**（Flexible NetFlow）、**match ipv4**、**match ipv4 destination**、**match ipv4 fragmentation**、**match ipv4 section**、**match ipv4 source**、**match ipv4 total-length**、**match ipv4 ttl**、**match routing**、**match transport**、**match transport icmp ipv4**、**match transport tcp**、**match transport udp**、**mode**（Flexible NetFlow）、**option**（Flexible NetFlow）、**record**、**sampler**、**show flow exporter**、**show flow interface**、**show flow monitor**、**show flow record**、**show sampler**、**source**（Flexible NetFlow）、**statistics packet**、**template data timeout**、**transport**（Flexible NetFlow）

表 1　Flexible NetFlow の機能情報 （続き）

機能名	リリース	機能情報
Flexible NetFlow—IPv4 Unicast Flows	12.2(33)SRC 12.4(9)T	Flexible NetFlow で IPv4 トラフィックを監視できます。 この機能のサポートは、Cisco 7200 シリーズ ルータ用として Cisco IOS Release 12.2(33)SRC で追加されました。 Flexible NetFlow : IPv4 Unicast Flows 機能については、次の各項に説明があります。 • 「IPv4 または IPv6 トラフィック用のカスタム フロー レコードの設定」（P.5） • 「インターフェイスへのフロー モニタの適用」（P.12） 次のコマンドが導入または変更されました。**collect routing**、**debug flow record**、**collect ipv4**、**collect ipv4 destination**、**collect ipv4 fragmentation**、**collect ipv4 section**、**collect ipv4 source**、**ip flow monitor**、**match ipv4**、**match ipv4 destination**、**match ipv4 fragmentation**、**match ipv4 section**、**match ipv4 source**、**match routing**、**record**、**show flow monitor**、**show flow record**
Flexible NetFlow—Layer 2 Fields	12.2(33)SRE 12.4(22)T	MAC アドレスや仮想 LAN（VLAN）ID などのレイヤ 2 フィールドの統計情報を、トラフィックから収集できます。 この機能のサポートは、Cisco 7200 および 7300 Network Processing Engine（NPE; ネットワーク処理エンジン）シリーズ ルータ用として、Cisco IOS Release 12.2(33)SRE で追加されました。 Flexible NetFlow—Layer 2 Fields 機能については、次の各項に説明があります。 • 「MAC および VLAN 統計情報監視用の Flexible NetFlow の設定：例」（P.18） 次のコマンドが導入または変更されました。 **collect datalink dot1q vlan**、**collect datalink mac**、**match datalink dot1q vlan**、**match datalink mac**

表 1　Flexible NetFlow の機能情報 （続き）

機能名	リリース	機能情報
Flexible NetFlow—IPv6 Unicast Flows	12.2(33)SRE 12.4(20)T	Flexible NetFlow で IPv6 トラフィックを監視できます。 この機能のサポートは、Cisco 7200 および 7300 Network Processing Engine（NPE; ネットワーク処理エンジン）シリーズ ルータ用として、Cisco IOS Release 12.2(33)SRE で追加されました。 Flexible NetFlow—IPv6 Unicast Flows 機能については、次の各項に説明があります。 • 「フロー レコードの現在のステータスの表示」（P.6） • 「インターフェイスへのフロー モニタの適用」（P.12） • 「IPv6 トラフィック監視用のカスタム フロー レコード設定：例」（P.17） 次のコマンドが導入または変更されました。**collect routing**、**debug flow record**、**match routing**、**record**、**show flow monitor**、**show flow record**、**collect ipv6**、**collect ipv6 destination**、**collect ipv6 extension map**、**collect ipv6 fragmentation**、**collect ipv6 hop-limit**、**collect ipv6 length**、**collect ipv6 section**、**collect ipv6 source**、**collect transport icmp ipv6**、**ipv6 flow monitor**、**match ipv6**、**match ipv6 destination**、**match ipv6 extension map**、**match ipv6 fragmentation**、**match ipv6 hop-limit**、**match ipv6 length**、**match ipv6 section**、**match ipv6 source**、**match transport icmp ipv6**
Flexible NetFlow—Ingress VRF Support	12.2(33)SRE 15.0(1)M	VRF ID を key または nonkey フィールドとして収集するフロー レコードを持つ入力フロー モニタを適用することで、ルータの着信パケットから Virtual Route Forwarding（VRF）ID を収集できます。 この機能のサポートは、Cisco 7200 および 7300 Network Processing Engine（NPE; ネットワーク処理エンジン）シリーズ ルータ用として、Cisco IOS Release 12.2(33)SRE で追加されました。 Flexible NetFlow—Ingress VRF Support 機能に関する情報は、次の項に記載されています。 • 「入力 VRF サポートのための Flexible NetFlow の設定：例」（P.18） 次のコマンドが導入または変更されました。**collect routing**、**match routing**、**option**（Flexible NetFlow）、**show flow monitor**

表 1　Flexible NetFlow の機能情報 （続き）

機能名	リリース	機能情報
Flexible NetFlow—NBAR Application Recognition	15.0(1)M	Network Based Application Recognition（NBAR）を使用すると、アプリケーション名を key または nonkey フィールドとして収集するフロー レコードを持つフロー モニタを適用することで、任意の 2 台の IP ホスト間で見られるアプリケーションごとに異なるフローの作成が可能になります。 NBAR Application Recognition 認識機能については、次の各項に説明があります。 • 「ネットワーク ベースのアプリケーション認識のための Flexible NetFlow の設定：例」（P.19） 次のコマンドが導入または変更されました。 **collect application name**、**match application name**、**option**（Flexible NetFlow）、**show flow monitor**