Cisco IOS XE Flexible NetFlow のフロー 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 のフロー レコードおよびフロー モニタのカスタマイズについて、およびその方法に関する説明が記載されています。「Getting Started with Configuring Cisco IOS XE Flexible NetFlow」モジュールおよび「Configuring Cisco IOS XE Flexible NetFlow with Predefined Records」モジュールのタスクおよび設定例がトラフィック分析要件に適していない場合は、このドキュメント内の情報および指示を使用して、トラフィック分析要件を満たすように Flexible NetFlow をカスタマイズできます。

NetFlow は、ルータを通過するパケットの統計情報が得られる Cisco IOS テクノロジーです。NetFlow は、IP ネットワークから IP 運用データを取得するための規格です。NetFlow は、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を提供します。

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

ご使用のソフトウェア リリースによっては、このモジュールに記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース 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の詳細、および各機能がサポートされているリリースのリストについては、「Flexible NetFlow の機能情報」（P.19）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

Flexible NetFlow のフロー レコードおよびフロー モニタをカスタマイズするための前提条件

Flexible NetFlow を設定する前に、次の前提条件を満たしておく必要があります。

- 「Cisco IOS XE 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。
- Flexible NetFlow の key フィールドについて、『*Cisco IOS Flexible NetFlow Command Reference*』で次のコマンドに定義されている内容をよく理解していること。
  - **match flow**
  - **match interface**
  - **match ipv4**
  - **match routing**
  - **match transport**
- Flexible NetFlow の nonkey フィールドについて、『*Cisco IOS Flexible NetFlow Command Reference*』で次のコマンドに定義されている内容をよく理解していること。
  - **collect counter**
  - **collect flow**
  - **collect interface**
  - **collect ipv4**
  - **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 XE 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。

Flexible NetFlow のフロー 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前に、次の概念を理解しておく必要があります。

- 「Flexible NetFlow の分析に使用されるトラフィックの識別基準」（P.3）

Flexible NetFlow の分析に使用されるトラフィックの識別基準

事前定義されている Flexible NetFlow レコードがトラフィック要件に適していない場合は、Flexible NetFlow **collect** コマンドおよび **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。カスタマイズしたレコードを作成する前に、key フィールドおよび nonkey フィールドに対して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、一般的な Denial of Service（DoS; サービス拒否）攻撃である SYN フラッド攻撃では、宛先ホストに対するオープン TCP 要求をフラッディングするために TCP フラグが使用されます。通常の TCP 接続が開始されると、宛先ホストは送信元ホストからの SYN（同期 / 開始）パケットを受信し、SYN ACK（同期応答確認）を返信します。宛先ホストは、接続を確立する前に、SYN ACK への ACK（応答確認）を受信する必要があります。これは、「TCP スリーウェイ ハンドシェイク」と呼ばれます。宛先ホストが SYN ACK への ACK を待機している間、宛先ホスト上のサイズが制限された接続キューは、完了するまで待機しながら、接続を記録します。ACK は SYN ACK の数ミリ秒後に到着すると予想されるため、このキューは通常、すぐに空になります。TCP SYN 攻撃ではこの設計を悪用し、攻撃元ホストでランダムな送信元アドレスを使用して被害ホストに対する TCP SYN パケットを生成します。被害を受けた宛先ホストは SYN ACK をランダムな送信元アドレスに返信し、接続キューにエントリが追加されます。SYN ACK は適切でないか、または存在していないホストを宛先にするため、TCP スリーウェイ ハンドシェイクの最後の部分が完了せず、エントリはタイマーが期限切れになるまで、通常は約 1 分間、接続キューに残ります。送信元ホストがランダムな IP アドレスから TCP SYN パケットを迅速に生成する場合、接続キューがいっぱいになる可能性があり、正当なユーザに対する TCP サービス（電子メール、ファイル転送、WWW など）が拒否されるおそれがあります。

このタイプの 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 フィールドおよび nonkey フィールドが含まれることがあります。

- key フィールド
  - 宛先 IP アドレスまたは宛先 IP サブセット
  - 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
  - インターフェイス入力および出力

ヒント ユーザの多くは、これらの key フィールドおよび nonkey フィールドを使用して、DoS 攻撃の詳細な Flexible NetFlow ビューをトリガーする一般的な Flexible NetFlow モニタを設定します。

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

この項のタスクでは、次の作業の実行方法について説明します。

- Flexible NetFlow フロー レコードをカスタマイズする。
- Flexible NetFlow フロー モニタをカスタマイズする。
- Flexible NetFlow をイネーブルにする。

（注） 次の作業では、これら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および引数のみについて説明します。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 のフロー レコードおよびフロー モニタをカスタマイズして、Flexible NetFlow をイネーブルにするには、次の作業を実行します。

- 「カスタマイズしたフロー 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 レコード設定の確認」（P.7）（任意）
- 「カスタマイズしたフロー 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.10）（任意）
- 「フロー モニタ設定の確認」（P.11）（任意）
- 「インターフェイスへのフロー モニタの適用」（P.11）（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.13）（任意）

カスタマイズしたフロー レコードの設定

カスタマイズしたフロー 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します。カスタマイズしたフロー レコードには、key フィールドとして使用する 1 つ以上の **match** 基準が必須で、通常は nonkey フィールドとして使用する 1 つ以上の **collect** 基準があります。

カスタマイズしたフロー レコードの順列は、数百もの可能性があります。このタスクでは、可能性のある順列の 1 つを作成するための手順について説明します。必要に応じてこれらのタスクの手順を変更し、要件に合わせてカスタマイズしたフロー レコードを作成します。

カスタマイズしたフロー レコードを設定するには、次のタスクを実行します。

- 「IPv4 トラフィックのカスタマイズしたフロー レコードの設定」

IPv4 トラフィックのカスタマイズしたフロー レコードの設定

このタスクでは、IPv4 トラフィックのカスタマイズしたフロー レコードを作成するために使用される手順を説明します。これは、IPv4 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 destination** {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}
6. 必要に応じてステップ 5 を繰り返し、レコードの追加 key フィールドを設定します。
7. **collect ipv4 source** {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}
8. 必要に応じてステップ 7 を繰り返し、レコードの追加 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。
ステップ 5	**match ipv4 destination** {**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、IPv4 宛先アドレスをレコードの key フィールドとして設定します。**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、レコードの追加 key フィールドを設定します。	—

	コマンドまたはアクション	目的
ステップ 7	**collect ipv4 source** {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]} **例：** `Router(config-flow-record)# collect ipv4 source address`	フロー内の 1 つ以上の IPv4 送信元フィールドをレコードの nonkey フィールドとして設定します。 **（注）** この例では、IPv4 送信元アドレスをレコードの nonkey フィールドとして設定します。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、レコードの追加 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、次のオプション作業を実行します。

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、指定するフロー モニタの現在のステータスを表示します。

```
Router# show flow record

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 レコード設定の確認

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、次のオプション作業を実行します。

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、指定するフロー モニタのコンフィギュレーション コマンドを表示します。

```
Router# show running-config flow record

Current configuration:
!
!
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
!
```

カスタマイズしたフロー モニタの作成

カスタマイズしたフロー モニタを設定するには、次の必須タスクを実行します。

フロー モニタ

各フロー モニタには、専用のキャッシュが割り当てられています。フロー モニタごとに、キャッシュ エントリの内容およびレイアウトを定義するレコードが必要です。これらのレコード フォーマットは、事前定義済みのレコード フォーマットのいずれかにすることもできますが、上級のユーザであれば **flow record** コマンドを使用して、カスタマイズしたフォーマットを作成することもできます。このタスクでは、「カスタマイズしたフロー 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 の事前定義済みレコードの代わりにカスタマイズしたレコードを使用する場合は、このタスクを実行する前に、カスタマイズしたレコードを作成する必要があります。カスタマイズしたフロー レコードの作成について、およびその方法については、「カスタマイズしたフロー レコードの設定」（P.4）を参照してください。

データをエクスポートするためにフロー エクスポータをフロー モニタに追加する場合は、このタスクを完了する前にエクスポータを作成する必要があります。フロー エクスポータの作成について、およびその方法については、「Configuring Data Export for Cisco IOS XE 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前に、**no ip flow monitor** コマンドを使用して、すべてのインターフェイスから適用済みのフロー モニタを削除する必要があります。**ip flow monitor** コマンドについては、『*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** *record* [**peer**]}
6. **cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**}*seconds* | **type** {**immediate** | **normal** | **permanent**}}
7. 必要に応じてステップ 6 を繰り返して、このフロー モニタのキャッシュ パラメータの変更を完了します。
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。
ステップ 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4**} *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** | **inactive** | **update**}*seconds* | **type** {**immediate** | **normal** | **permanent**}} **例：** `Router(config-flow-monitor)# cache entries 1000`	（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** キーワードに関連するキーワードの値は、キャッシュ タイプが **immediate** に設定されている場合には反映されません。
ステップ 7	必要に応じてステップ 6 を繰り返して、このフロー モニタのキャッシュ パラメータの変更を完了します。	—
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。

	コマンドまたはアクション	目的
ステップ 10	**exporter** *exporter-name* **例：** `Router(config-flow-monitor)# exporter EXPORTER-1`	（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。 • フロー エクスポータの設定およびその方法については、「Configuring Data Export for Cisco IOS XE 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、次のオプション作業を実行します。

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、指定するフロー モニタの現在のステータスを表示します。

```
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 モニタ設定の確認

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、次のオプション作業を実行します。

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 コマンドを表示します。

```
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

フロー モニタをアクティブ化する前に、1 つ以上のインターフェイスに適用する必要があります。フロー モニタをアクティブ化するには、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」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」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 flow monitor** *monitor-name* {**input** | **output**}
5. ステップ 3 および 4 を繰り返して、トラフィックを監視するルータの他のインターフェイスでフロー モニタをアクティブ化します。
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 fastethernet 0/0/0`	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 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 および 4 を繰り返して、トラフィックを監視するルータの他のインターフェイスでフロー モニタをアクティブ化します。	—
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、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、次のオプション作業を実行します。

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** *type number*

show flow interface コマンドでは、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します。

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

Interface FastEthernet0/0/0
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on


Router# show flow interface fastethernet 1/0/0

Interface FastEthernet1/0/0
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      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 キャッシュのデータを表示するには、次のオプション作業を実行します。

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** コマンド文字列では、フロー モニタのステータス、統計情報、およびキャッシュ内のフロー データを表示します。

```
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
```

Flexible NetFlow のフロー レコードおよびフロー モニタをカスタマイズする設定例

ここでは、次の設定例について説明します。

- 「例：数が制限されたフローで使用する永続的なフロー レコード キャッシュの設定」（P.15）
- 「例：入力 VRF サポートのための Flexible NetFlow の設定」（P.16）
- 「例：ネットワークベース アプリケーション認識のための Flexible NetFlow の設定」（P.16）

例：数が制限されたフローで使用する永続的なフロー レコード キャッシュの設定

次に、ルータのすべてのインターフェイス上の Type of Service（ToS; タイプ オブ サービス）フィールドを監視するための設定例を示します。この例は、**show flow monitor** コマンドを使用して、ルータで分析用の追加データを収集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ていません。

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。

```
!
!
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 fastethernet0/0/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface fastethernet0/1/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface fastethernet0/2/0
 ip flow monitor QOS_MONITOR input
 exit
!
```

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

show flow monitor コマンドでは、キャッシュの現在のステータスを表示します。

```
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
```

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

次に、key フィールドとして VRF ID を収集するフロー レコードがある入力フロー モニタを適用して、ルータで着信パケットから Virtual Routing and Forwarding（VRF）ID を収集するための設定例を示しています。

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 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 Serial2/0/0
ip vrf forwarding vrf1
ip address 172.16.2.2 255.255.255.252
ip flow monitor mm_1 output
!
end
```

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

次に、key フィールドとしてアプリケーション名を収集するフロー レコードがあるフロー モニタを適用し、Network-Based Application Recognition（NBAR; ネットワークベース アプリケーション認識）を使用して、2 台の IP ホスト間で表示されるアプリケーションごとに異なるフローを作成する例を示します。

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 FastEthernet0/0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

関連情報

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 XE 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 XE 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 に対して事前定義済みのレコードを設定する場合は、「Configuring Cisco IOS XE Flexible NetFlow with Predefined Records」モジュールを参照してください。

参考資料

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 XE Flexible NetFlow Overview」
Flexible NetFlow の機能ロードマップ	「Cisco IOS Flexible NetFlow Features Roadmap」
Flexible NetFlow での以前の NetFlow のエミュレート	「Getting Started with Configuring Cisco IOS XE 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 XE 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 XE 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 XE Flexible NetFlow with Predefined Records」
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、およびフィーチャ セットに対する MIB を特定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、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする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確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Flexible NetFlow の機能情報

機能名	リリース	機能情報
Flexible NetFlow	Cisco IOS XE リリース 3.1S	Flexible NetFlow が導入されました。 Flexible NetFlow 機能については、次の項で説明します。 • 「Flexible NetFlow のフロー レコードおよびフロー モニタをカスタマイズするための前提条件」（P.2） • 「Flexible NetFlow のフロー 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 のフロー 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 のフロー レコードおよびフロー モニタをカスタマイズする設定例」（P.15） 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 ユニキャスト フロー	Cisco IOS XE Release 3.1S	Flexible NetFlow での IPv4 トラフィックの監視をイネーブルにします。 Flexible NetFlow：IPv4 ユニキャスト フロー機能については、次の項で説明します。 • 「IPv4 トラフィックのカスタマイズしたフロー レコードの設定」（P.4） • 「インターフェイスへのフロー モニタの適用」（P.11） 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：入力 VRF サポート	Cisco IOS XE リリース 3.1S	key フィールドまたは nonkey フィールドとして VRF ID を収集するフロー レコードがある入力フロー モニタを適用して、ルータで着信パケットから Virtual Routing and Forwarding（VRF）ID を収集できるようにします。 Flexible NetFlow：入力 VRF サポート機能については、次の項で説明します。 • 「例：入力 VRF サポートのための Flexible NetFlow の設定」（P.16） 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**。
Flexible NetFlow：NBAR アプリケーション認識	Cisco IOS XE リリース 3.1S	Network-Based Application Recognition（NBAR; ネットワークベース アプリケーション認識）では、key フィールドまたは nonkey フィールドとしてアプリケーション名を収集するフロー レコードがあるフロー モニタを適用して、Network-Based Application Recognition（NBAR）を使用して、2 台の IP ホスト間で表示されるアプリケーションごとに異なるフローを作成できます。 NBAR アプリケーション認識機能については、次の項で説明します。 • 「例：ネットワークベース アプリケーション認識のための Flexible NetFlow の設定」（P.16） 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**。