



Flexible NetFlow フロー サンプリングの使用

このドキュメントには、Flexible NetFlow のトラフィック分析による CPU オーバーヘッドを軽減するためのサンプリングの設定について、およびその方法に関する説明が記載されています。

NetFlow は、ルータを通過するパケットの統計情報が得られるシスコテクノロジーです。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 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。

- [機能情報の確認, 1 ページ](#)
- [Flexible NetFlow フロー サンプリングを使用するための前提条件, 2 ページ](#)
- [Flexible NetFlow フロー サンプリングを使用するための制約事項, 2 ページ](#)
- [Flexible NetFlow フロー サンプリングについて, 2 ページ](#)
- [Flexible NetFlow フロー サンプリングの設定方法, 2 ページ](#)
- [Flexible NetFlow フロー サンプリングの設定例, 7 ページ](#)
- [その他の関連資料, 9 ページ](#)
- [Flexible NetFlow フロー サンプリングの機能情報, 10 ページ](#)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、『[Bug Search Tool](#)』および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を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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シスコ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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Flexible NetFlow フロー サンプリングを使用するための前提条件

- ネットワーキング デバイスで、Flexible NetFlow がサポートされたシスコ リリースが稼働していること。

Flexible NetFlow フロー サンプリングを使用するための制約事項

Flexible NetFlow フロー サンプリングについて

フロー サンプラ

フロー サンプラは、ルータのコンフィギュレーションで別のコンポーネントとして作成されます。フロー サンプラは、分析用に選択されるパケットの数を制限することで、Flexible NetFlow を実行しているデバイス上の負荷を減らすために使用されます。

フロー サンプリングでは、ルータのパフォーマンスに対するモニタリング精度が交換されます。サンプラをフロー モニタに適用すると、フロー モニタが分析する必要のあるパケット数が減少するため、ルータでフロー モニタを実行するためのオーバーヘッド負荷が低下します。フロー モニタで分析されるパケット数が減少すると、フロー モニタのキャッシュに格納される情報の精度が、それに応じて低下します。

ip flow monitor コマンドを使用してインターフェイスに適用する場合、サンプラとフロー モニタを組み合わせます。

Flexible NetFlow フロー サンプリングの設定方法

フロー サンプリングを使用すると、分析対象のパケット数が減少し、Flexible NetFlow によるトラフィック分析の CPU オーバーヘッドが軽減されます。



(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。

フロー モニタの設定

サンプラはフローモニタと連携してインターフェイスに適用されます。サンプリングをイネーブルにするには、フローモニタを作成して、分析するトラフィックタイプを設定する必要があります。フローモニタを設定するには、次の必須作業を実行します。

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。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 Flexible NetFlow フローレコードコンフィギュレーションモードで **collect** および **match** コマンドを使用して独自のレコードフォーマットを作成することもできます。



(注) 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor *monitor-name***
4. **description *description***
5. **record {*record-name* | netflow-original | netflow {ipv4 | ipv6} record [peer]}**
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： Device> enable	特権 EXEC モードをイネーブルにします。 ・パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# 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： Device(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 description 例： Device(config-flow-monitor)# description Used for basic 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 ipv6} record [peer]} 例： Device(config-flow-monitor)# record netflow ipv4 original-input	フロー モニタのレコードを指定します。
ステップ 6	end 例： Device(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 サンプリングの設定およびイネーブル化

フロー サンプラを設定してイネーブルにするには、次の必須作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sampler** *sampler-name*
4. **description** *description*
5. **mode** {*deterministic* | *random*} **1 out-of** *window-size*
6. **exit**
7. **interface** *type number*
8. {*ip* | *ipv6*} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**}
9. **end**
10. **show sampler sampler-name**

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： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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	sampler <i>sampler-name</i> 例： Device(config)# sampler SAMPLER-1	サンプラを作成し、サンプラ コンフィギュレーション モードを開始します。 • このコマンドでは、既存のサンプラを変更することもできます。
ステップ 4	description <i>description</i> 例： Device(config-sampler)# description Sample at 50%	(任意) フロー サンプラの説明を作成します。
ステップ 5	mode { <i>deterministic</i> <i>random</i> } 1 out-of <i>window-size</i> 例： Device(config-sampler)# mode random 1 out-of 2	サンプラ モードおよびフロー サンプラのウィンドウ サイズを指定します。 • 引数 <i>window-size</i> の範囲は、2 ~ 32,768 です。

	コマンドまたはアクション	目的
ステップ 6	exit 例： <code>Device(config-sampler)# exit</code>	サンプラ コンフィギュレーション モードを終了し、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 7	interface <i>type number</i> 例： <code>Device(config)# interface GigabitEthernet 0/0/0</code>	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 8	{ip ipv6} flow monitor <i>monitor-name</i> [[sampler] sampler-name] {input output} 例： <code>Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input</code>	作成したフロー モニタおよびフロー サンプラをインターフェイスに割り当て、サンプリングをイネーブルにします。
ステップ 9	end 例： <code>Device(config-if)# end</code>	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。
ステップ 10	show sampler sampler-name 例： <code>Device# show sampler SAMPLER-1</code>	設定済みでイネーブル化したフロー サンプラのステータスおよび統計情報を表示します。

フロー サンプラ設定のステータスと統計情報の表示

設定済みでイネーブル化したフロー サンプラのステータスおよび統計情報を表示するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **show sampler sampler-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）。

例：

```
Device> enable
Device#
```

ステップ 2 show sampler sampler-name

show sampler コマンドでは、指定するサンプラの現在のステータスを表示します。

例：

```
Device# 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
```

Flexible NetFlow フロー サンプリングの設定例

例：IPv4 トラフィックのランダムサンプラの設定およびイネーブル化

次に、IPv4 出力トラフィックのランダム サンプリングを設定し、イネーブルにする方法の例を示します。

この例は、グローバル コンフィギュレーション モードで開始します。

```
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
record v4_r1
exit
!
```

例：フロー モニタがすでにイネーブルの場合にフロー モニタにサンプラを追加する

```
sampler SAMPLER-1
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 output
!
```

次に、IPv4 入力トラフィックのランダム サンプリングを設定し、イネーブルにする方法の例を示します。

この例は、グローバル コンフィギュレーション モードで開始します。

```
!
flow record v4_r1
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exit
!
sampler SAMPLER-1
 mode random 1 out-of 2
 exit
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

例：フロー モニタがすでにイネーブルの場合にフロー モニタにサンプラを追加する

次の例では、サンプラなしでインターフェイスでイネーブルになっているフロー モニタにサンプラを追加する場合の動作を示します。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フロー モニタをサンプラと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```


例：フロー モニタからのサンプラの削除

次に、サンプラのキーワードおよび引数なしで再び **ip flow monitor** コマンドを入力して、インターフェイス上のフロー モニタからサンプラを削除する場合の動作の例を示します。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in sampled mode and cannot be
enabled in full mode.
```

次の例では、サンプラなしでイネーブルにできるように、サンプラと一緒にイネーブルになっているフロー モニタをインターフェイスから削除する方法を示します。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

その他の関連資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『 Cisco IOS Master Command List, All Releases 』
Flexible NetFlow の概念情報および設定作業	『 <i>Flexible NetFlow</i> コンフィギュレーション ガイド』
Flexible NetFlow コマンド	『 <i>Cisco IOS Flexible NetFlow Command Reference</i> 』

標準/RFC

標準	タイトル
この機能によりサポートされる新規または変更された標準/RFC はありません。	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、シスコソフトウェアリリース、およびフィチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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 フロー サンプリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコ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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1 : Flexible NetFlow フロー サンプリングの機能情報

機能名	リリース	機能情報
Flexible NetFlow : ランダム サンプリング	12.2(50)SY 12.4(20)T Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2SE	フロー サンプラは、ルータのコンフィギュレーションで別のコンポーネントとして作成されます。フロー サンプラは、分析用に選択されるパケットの数を制限することで、Flexible NetFlow を実行しているデバイス上の負荷を減らすために使用されます。サンプラでは、ランダムまたは確定的サンプリング手法（モード）を使用します。 次のコマンドが導入または変更されました。 clear sampler 、 debug sampler 、 mode 、 record 、 sampler 、 show sampler

