事前定義済みレコードによる Cisco IOS Flexible NetFlow の設定

このモジュールには、事前定義済みレコードを使用した Flexible NetFlow の設定に関する情報、およびその設定方法が記載されています。Flexible NetFlow 事前定義済みレコードの多くでは、以前の NetFlow にあった集約キャッシュと同じ、key および nonkey フィールドが使用されます。ただし、事前定義済み Flexible NetFlow レコードでは集約が実行されません。

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.33）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

事前定義済みレコードによる Flexible NetFlow 設定の前提条件

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。
- 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 IPv6 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。

事前定義済みレコードによる Flexible NetFlow の設定について

事前定義済みレコードで Flexible NetFlow を設定するには、その前に次の概念を理解しておく必要があります。

Flexible NetFlow の事前定義済みレコード

Flexible NetFlow の事前定義済みレコードは、以前の NetFlow の入力キャッシュと出力キャッシュ、および集約キャッシュに基づいています。以前の NetFlow の集約キャッシュと、対応する事前定義済み Flexible NetFlow レコードの違いは、事前定義済みレコードでは集約が実行されないことです。Flexible NetFlow の事前定義済みレコードは、ユーザ定義の（カスタム）レコードの関連付けと同じ方法で、Flexible NetFlow フロー モニタに関連付けられます。

Flexible NetFlow の事前定義済みレコードの利点

以前の NetFlow または集約キャッシュを持つ以前の NetFlow を使用していた場合は、Flexible NetFlow で使用可能な事前定義済みレコードを使用して Flexible NetFlow に移行すると、引き続き同じトラフィック データをキャプチャして分析できます。多くのユーザにとって、以前から存在していた Flexible NetFlow レコードは、トラフィック分析の要件のほとんどに適合しているはずです。

Flexible NetFlow の事前定義済みレコード「NetFlow Original」と「NetFlow IPv4 Original Input」

Flexible NetFlow の事前定義済みレコード「NetFlow original」と「NetFlow IPv4 original input」は、key フィールドと nonkey フィールドが同じであるため、入れ替えて使用することができます。事前定義済みレコード「NetFlow original」と「NetFlow IPv4 original input」の key および nonkey フィールドを、表 1 に示します。

表 1　事前定義済みレコード「NetFlow Original」と「NetFlow IPv4 Original Input」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	key	タイプ オブ サービス（ToS）フィールドの値。
IP Protocol	Key	IP プロトコル フィールドの値。
IPv4 Source Address	Key	IPv4 送信元アドレス。
IPv4 Destination Address	Key	IPv4 宛先アドレス。

表 1　事前定義済みレコード「NetFlow Original」と「NetFlow IPv4 Original Input」で使用される key および nonkey フィールド （続き）

フィールド	key または nonkey フィールド	定義
Transport Source Port	Key	トランスポート レイヤの送信元ポート フィールドの値。
Transport Destination Port	Key	トランスポート レイヤの宛先ポート フィールドの値。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Flow Sampler ID	Key	フロー サンプラの ID 番号（フロー サンプリングがイネーブルにされている場合）。
IP Source AS	Nonkey	送信元自律システム番号。
IP Destination AS	Nonkey	宛先自律システム番号。
IPv4 Next Hop Address	Nonkey	ネクスト ホップの IPv4 アドレス。
IPv4 Source Mask	Nonkey	IPv4 送信元アドレスのマスク。
IPv4 Destination Mask	Nonkey	IPv4 宛先アドレスのマスク。
TCP Flags	Nonkey	TCP フラグ フィールドの値。
Interface Output	Nonkey	トラフィックが送信されたインターフェイス。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「NetFlow IPv4 Original Output」

Flexible NetFlow の事前定義済みレコード「NetFlow IPv4 original output」は、Cisco IOS Release 12.3(11)T でリリースされた以前の NetFlow 出力 NetFlow アカウンティング機能をエミュレートするために使用されます。事前定義済みレコード「NetFlow IPv4 original output」の key および nonkey フィールドとカウンタを、表 2 に示します。

表 2　事前定義済みレコード「NetFlow IPv4 Original Output」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Protocol	Key	IP プロトコル フィールドの値。
IPv4 Source Address	Key	IPv4 送信元アドレス。
IPv4 Destination Address	Key	IPv4 宛先アドレス。

表 2　事前定義済みレコード「NetFlow IPv4 Original Output」で使用される key および nonkey フィールド （続き）

フィールド	key または nonkey フィールド	定義
Transport Source Port	Key	トランスポート レイヤの送信元ポート フィールドの値。
Transport Destination Port	Key	トランスポート レイヤの宛先ポート フィールドの値。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Sampler ID	Key	フロー サンプラの ID 番号（フロー サンプリングがイネーブルにされている場合）。
IP Source AS	Nonkey	送信元自律システム番号。
IP Destination AS	Nonkey	宛先自律システム番号。
IPv4 Next Hop Address	Nonkey	ネクスト ホップの IPv4 アドレス。
IPv4 Source Mask	Nonkey	IPv4 送信元アドレスのマスク。
IPv4 Destination Mask	Nonkey	IPv4 宛先アドレスのマスク。
TCP Flags	Nonkey	TCP フラグ フィールドの値。
Interface Input	Nonkey	トラフィックが受信されたインターフェイス。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 Original Input」

Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 original input」の key および nonkey フィールドとカウンタを、表 3 に示します。

表 3　Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 Original Input」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
Traffic Class	Key	トラフィック クラス フィールドの値。
Flow Label	Key	フロー ラベル。
Protocol	Key	プロトコル フィールドの値。
Extension Map	Key	拡張マップ ビットマップの値。
IP Source Address	Key	IP 送信元アドレス。
IP Destination Address	Key	IP 宛先アドレス。

表 3　Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 Original Input」で使用される key および nonkey フィールド （続き）

フィールド	key または nonkey フィールド	定義
Transport Source Port	Key	トランスポート レイヤの送信元ポート フィールドの値。
Transport Destination Port	Key	トランスポート レイヤの宛先ポート フィールドの値。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Flow Direction	Key	フローの方向。
Flow Sampler	Key	フロー サンプラの ID 番号（フロー サンプリングがイネーブルにされている場合）。
Routing Source AS	Nonkey	送信元自律システム番号。
Routing Destination AS	Nonkey	宛先自律システム番号。
Routing Next-hop Address	Nonkey	ネクスト ホップの IP アドレス。
IP Source Mask	Nonkey	IP 送信元アドレスのマスク。
IP Destination Mask	Nonkey	IP 宛先アドレスのマスク。
Transport TCP Flags	Nonkey	TCP フラグ フィールドの値。
Interface Output	Nonkey	トラフィックが送信されたインターフェイス。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Timestamp Sys-uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Timestamp Sys-uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 Original Output」

Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 original output」の key および nonkey フィールドとカウンタを、表 4 に示します。

表 4　Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 Original Output」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
Traffic Class	Key	トラフィック クラス フィールドの値。
Flow Label	Key	フロー ラベル。
Protocol	Key	プロトコル フィールドの値。
Extension Map	Key	拡張マップ ビットマップの値。

表 4　Flexible NetFlow の事前定義済みレコード「NetFlow IPv6 Original Output」で使用される key および nonkey フィールド （続き）

フィールド	key または nonkey フィールド	定義
IP Source Address	Key	IP 送信元アドレス。
IP Destination Address	Key	IP 宛先アドレス。
Transport Source Port	Key	トランスポート レイヤの送信元ポート フィールドの値。
Transport Destination Port	Key	トランスポート レイヤの宛先ポート フィールドの値。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローの方向。
Flow Sampler	Key	フロー サンプラの ID 番号（フロー サンプリングがイネーブルにされている場合）。
Routing Source AS	Nonkey	送信元自律システム番号。
Routing Destination AS	Nonkey	宛先自律システム番号。
Routing Next-hop Address	Nonkey	ネクスト ホップの IP アドレス。
IP Source Mask	Nonkey	IP 送信元アドレスのマスク。
IP Destination Mask	Nonkey	IP 宛先アドレスのマスク。
Transport TCP Flags	Nonkey	TCP フラグ フィールドの値。
Interface Input	Nonkey	トラフィックが受信されたインターフェイス。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Timestamp Sys-uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Timestamp Sys-uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Autonomous System」

Flexible NetFlow の事前定義済みレコード「autonomous system」では、自律システム間のトラフィック フロー データに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「autonomous system」では、以前の NetFlow の「autonomous system」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

（注）　この事前定義済みレコードは、IPv4 および IPv6 トラフィックの分析に使用できます。

Flexible NetFlow の事前定義済みレコード「autonomous system」で使用される key および nonkey フィールドを、表 5 に示します。

表 5　Flexible NetFlow の事前定義済みレコード「Autonomous System」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP Source AS	Key	送信元 IP アドレスの自律システム（ピアまたは起点）。
IP Destination AS	Key	宛先 IP アドレスの自律システム（ピアまたは起点）。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Autonomous System ToS」

Flexible NetFlow の事前定義済みレコード「autonomous system ToS」では、自律システム間および Type of Service（ToS; タイプ オブ サービス）トラフィック フロー データに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「autonomous system ToS」では、以前の NetFlow の「autonomous system ToS」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

（注）　この事前定義済みレコードは、IPv4 トラフィックの分析だけに使用できます。

ヒント　この事前定義済みレコードは、特に自律システム間のトラフィック フロー データに基づいてフローを生成するときに役立ちます。

Flexible NetFlow の事前定義済みレコード「autonomous system ToS」で使用される key および nonkey フィールドを、表 6 に示します。

表 6　Flexible NetFlow の事前定義済みレコード「Autonomous System ToS」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Source autonomous system	Key	送信元 IP アドレスの自律システム（ピアまたは起点）。
IP Destination autonomous system	Key	宛先 IP アドレスの自律システム（ピアまたは起点）。
Interface Input	Key	トラフィックが受信されたインターフェイス。

表 6　Flexible NetFlow の事前定義済みレコード「Autonomous System ToS」で使用される key および nonkey フィールド （続き）

フィールド	key または nonkey フィールド	定義
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible BGP の事前定義済みレコード「BGP Next-Hop」

Flexible NetFlow の事前定義済みレコード「BGP next-hop」では、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）のトラフィック フロー データに基づいてフローが作成されます。

（注）　この事前定義済みレコードは、IPv6 トラフィックの分析だけに使用できます。

Flexible NetFlow の事前定義済みレコード「BGP next-hop」で使用される key および nonkey フィールドを、表 7 に示します。

表 7　Flexible NetFlow の事前定義済みレコード「BGP Next-Hop」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
Routing Source AS	Key	送信元 IP アドレスの自律システム。
Routing Destination AS	Key	宛先 IP アドレスの自律システム。
Routing Next-hop Address IPv6 BGP	Key	BGP ネクスト ホップの IPv6 アドレス。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Timestamp Sys-uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Timestamp Sys-uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible BGP の事前定義済みレコード「BGP Next-Hop ToS」

Flexible NetFlow の事前定義済みレコード「BGP next-hop ToS」では、BGP および ToS のトラフィック フロー データに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「BGP next-hop ToS」では、以前の NetFlow の「BGP next-hop ToS」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

（注） この事前定義済みレコードは、IPv4 トラフィックの分析だけに使用できます。

Flexible NetFlow の事前定義済みレコード「BGP next-hop ToS」で使用される key および nonkey フィールドを、表 8 に示します。

表 8　Flexible BGP の事前定義済みレコード「BGP Next-Hop ToS」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Source autonomous system	Key	送信元 IP アドレスの自律システム（ピアまたは起点）。
IP Destination autonomous system	Key	宛先 IP アドレスの自律システム（ピアまたは起点）。
IPv4 Next Hop Address BGP	Key	BGP ネクスト ホップの IPv4 アドレス。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Destination Prefix」

Flexible NetFlow の事前定義済みレコード「destination prefix」では、宛先プレフィクスのトラフィック フロー データに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「destination prefix」では、以前の NetFlow の「destination prefix」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

（注） この事前定義済みレコードは、IPv4 および IPv6 トラフィックの分析に使用できます。

Flexible NetFlow の事前定義済みレコード「destination prefix」で使用される key および nonkey フィールドを、表 9 に示します。

表 9　Flexible NetFlow の事前定義済みレコード「Destination Prefix」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP Destination autonomous system	Key	宛先 IP アドレスの自律システム（ピアまたは起点）。
IPv4 or IPv6 Destination Prefix	Key	宛先 IP アドレスと宛先プレフィクス マスクの論理積。
IPv4 or IPv6 Destination Mask	Key	宛先プレフィクスのビット数。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Destination Prefix ToS」

Flexible NetFlow の事前定義済みレコード「destination prefix ToS」では、宛先プレフィクスおよび ToS のトラフィック フロー データに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「destination prefix ToS」では、以前の NetFlow の「destination prefix ToS」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

この事前定義済みレコードは、データをキャプチャし、それを使用して NetFlow 対応デバイスを通過するネットワーク トラフィックの宛先を調べる場合に、特に役立ちます。

（注） この事前定義済みレコードは、IPv4 トラフィックの分析だけに使用できます。

Flexible NetFlow の事前定義済みレコード「destination prefix ToS」で使用される key および nonkey フィールドを、表 10 に示します。

表 10　Flexible NetFlow の事前定義済みレコード「Destination Prefix ToS」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Destination autonomous system	Key	宛先 IP アドレスの自律システム（ピアまたは起点）。
IPv4 Destination Prefix	Key	宛先 IP アドレスと宛先プレフィクス マスクの論理積。
IPv4 Destination Mask	Key	宛先プレフィクスのビット数。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Prefix」

Flexible NetFlow の事前定義済みレコード「prefix」では、トラフィック フロー データの送信元と宛先のプレフィクスに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「prefix」では、以前の NetFlow の「prefix」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

（注） この事前定義済みレコードは、IPv4 および IPv6 トラフィックの分析に使用できます。IPv6 トラフィックの場合、最小プレフィクス マスク長は 0 ビットと見なされます。

Flexible NetFlow の事前定義済みレコード「prefix」で使用される key および nonkey フィールドを、表 11 に示します。

表 11　Flexible NetFlow の事前定義済みレコード「Prefix」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP Source autonomous system	Key	送信元 IP アドレスの自律システム(ピアまたは起点)。
IP Destination autonomous system	Key	宛先 IP アドレスの自律システム (ピアまたは起点)。
IPv4 or IPv6 Source Prefix	Key	送信元 IP アドレスと送信元プレフィクス マスクの論理積。または、集約されたフローが属す送信元 IP アドレスのプレフィクス。
IPv4 or IPv6 Source Mask	Key	送信元プレフィクスのビット数。
IPv4 or IPv6 Destination Prefix	Key	宛先 IP アドレスと宛先プレフィクス マスクの論理積。
IPv4 or IPv6 Destination Mask	Key	宛先プレフィクスのビット数。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間)。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間)。

Flexible NetFlow の事前定義済みレコード「Prefix Port」

Flexible NetFlow の事前定義済みレコード「prefix port」では、トラフィック フロー データの送信元および宛先のプレフィクスとポートに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「prefix port」では、以前の NetFlow の「prefix port」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

この事前定義済みレコードは、データをキャプチャし、それを使用して NetFlow 対応デバイスを通過するネットワーク トラフィックの送信元と宛先を調べる場合に、特に役立ちます。

（注） この事前定義済みレコードは、Pv4 トラフィックの分析だけに使用できます。

宛先の Flexible NetFlow の事前定義済みレコード「prefix port」で使用される key および nonkey フィールドを、表 12 に示します。

表 12　Flexible NetFlow の事前定義済みレコード「Prefix Port」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Protocol	Key	IP プロトコル フィールドの値。
IPv4 Source Prefix	Key	送信元 IP アドレスと送信元プレフィクス マスクの論理積。または、集約されたフローが属す送信元 IP アドレスのプレフィクス。
IPv4 Source Mask	Key	送信元プレフィクスのビット数。
IPv4 Destination Prefix	Key	宛先 IP アドレスと宛先プレフィクス マスクの論理積。
IPv4 Destination Mask	Key	宛先プレフィクスのビット数。
Transport Source Port	Key	トランスポート レイヤの送信元ポート フィールドの値。
Transport Destination Port	Key	トランスポート レイヤの宛先ポート フィールドの値。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Prefix ToS」

Flexible NetFlow の事前定義済みレコード「prefix ToS」では、トラフィック フロー データの送信元および宛先のプレフィクスと ToS に基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「prefix ToS」では、以前の NetFlow の「destination prefix ToS」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

この事前定義済みレコードは、データをキャプチャし、それを使用して NetFlow 対応デバイスを通過するネットワーク トラフィックの送信元と宛先を調べる場合に、特に役立ちます。

（注） この事前定義済みレコードは、IPv4 トラフィックの分析だけに使用できます。

Flexible NetFlow の事前定義済みレコード「prefix ToS」で使用される key および nonkey フィールドを、表 13 に示します。

表 13　Flexible NetFlow の事前定義済みレコード「Prefix ToS」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Source autonomous system	Key	送信元 IP アドレスの自律システム（ピアまたは起点）。
IP Destination autonomous system	Key	宛先 IP アドレスの自律システム（ピアまたは起点）。
IPv4 Source Prefix	Key	送信元 IP アドレスと送信元プレフィクス マスクの論理積。または、集約されたフローが属す送信元 IP アドレスのプレフィクス。
IPv4 Source Mask	Key	送信元プレフィクスのビット数。
IPv4 Destination Prefix	Key	宛先 IP アドレスと宛先プレフィクス マスクの論理積。
IPv4 Destination Mask	Key	宛先プレフィクスのビット数。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Interface Output	Key	トラフィックが送信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Protocol Port」

Flexible NetFlow の事前定義済みレコード「protocol port」では、トラフィック フロー データのプロトコルおよびポートに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「protocol port」では、以前の NetFlow の「protocol port」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

（注） この事前定義済みレコードは、IPv4 および IPv6 トラフィックの分析に使用できます。

Flexible NetFlow の事前定義済みレコード「protocol port」で使用される key および nonkey フィールドを、表 14 に示します。

表 14　Flexible NetFlow の事前定義済みレコード「Protocol Port」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP Protocol	Key	IP プロトコル フィールドの値。
Transport Source Port	Key	トランスポート レイヤの送信元ポート フィールドの値。
Transport Destination Port	Key	トランスポート レイヤの宛先ポート フィールドの値。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Protocol Port ToS」

Flexible NetFlow の事前定義済みレコード「protocol port ToS」では、トラフィック フロー データのプロトコル、ポート、および ToS 値に基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「protocol port ToS」では、以前の NetFlow の「protocol port ToS」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

この事前定義済みレコードは、データをキャプチャし、トラフィック タイプごとのネットワーク使用状況を調べる場合に、特に役立ちます。

（注） この事前定義済みレコードは、IPv4 トラフィックの分析だけに使用できます。

Flexible NetFlow の事前定義済みレコード「protocol port ToS」で使用される key および nonkey フィールドを、表 15 に示します。

表 15　Flexible NetFlow の事前定義済みレコード「Protocol Port ToS」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Protocol	Key	IP プロトコル フィールドの値。
Transport Source Port	Key	トランスポート レイヤの送信元ポート フィールドの値。
Transport Destination Port	Key	トランスポート レイヤの宛先ポート フィールドの値。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

Flexible NetFlow の事前定義済みレコード「Source Prefix」

Flexible NetFlow の事前定義済みレコード「source prefix」では、ネットワーク トラフィックの送信元プレフィクスに基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「source prefix」では、以前の NetFlow の「source prefix」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

（注） この事前定義済みレコードは、IPv4 および IPv6 トラフィックの分析に使用できます。

Flexible NetFlow の事前定義済みレコード「source prefix」で使用される key および nonkey フィールドを、表 16 に示します。

表 16　Flexible NetFlow の事前定義済みレコード「Source Prefix」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP Source autonomous system	Key	送信元 IP アドレスの自律システム(ピアまたは起点)。
IPv4 or IPv6 Source Prefix	Key	送信元 IP アドレスと送信元プレフィクス マスクの論理積。または、集約されたフローが属す送信元 IP アドレスのプレフィクス。
IPv4 or IPv6 Source Mask	Key	送信元プレフィクスのビット数。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間)。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間)。

Flexible NetFlow の事前定義済みレコード「Source Prefix ToS」

Flexible NetFlow の事前定義済みレコード「source prefix ToS」では、ネットワーク トラフィックの送信元プレフィクスおよび ToS 値に基づいてフローが作成されます。Flexible NetFlow の事前定義済みレコード「source prefix ToS」では、以前の NetFlow の「source prefix ToS」集約キャッシュと同じ、key および nonkey フィールドが使用されます。

この事前定義済みレコードは、データをキャプチャし、それを使用して NetFlow 対応デバイスを通過するネットワーク トラフィックの送信元を調べる場合に、特に役立ちます。

（注） この事前定義済みレコードは、IPv4 トラフィックの分析だけに使用できます。

Flexible NetFlow の事前定義済みレコード「source prefix ToS」で使用される key および nonkey フィールドを、表 17 に示します。

表 17　Flexible NetFlow の事前定義済みレコード「Source Prefix ToS」で使用される key および nonkey フィールド

フィールド	key または nonkey フィールド	定義
IP ToS	Key	ToS フィールドの値。
IP Source autonomous system	Key	送信元 IP アドレスの自律システム（ピアまたは起点）。
IPv4 Source Prefix	Key	送信元 IP アドレスと送信元プレフィクス マスクの論理積。または、集約されたフローが属す送信元 IP アドレスのプレフィクス。
IPv4 Source Mask	Key	送信元プレフィクスのビット数。
Interface Input	Key	トラフィックが受信されたインターフェイス。
Flow Direction	Key	フローが監視される方向。
Counter Bytes	Nonkey	フロー内で認識されたバイト数。
Counter Packets	Nonkey	フロー内で認識されたパケット数。
Time Stamp System Uptime First	Nonkey	最初のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。
Time Stamp System Uptime Last	Nonkey	最後のパケットが交換されたときのシステム稼動時間（ミリ秒単位。このデバイスが最初にブートしてからの時間）。

フロー モニタ用の事前定義済みレコードを使用した Flexible NetFlow の設定方法

この項のタスクは、フロー モニタ用の事前定義済みレコードを使用して Flexible NetFlow を設定する方法を示しています。

(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。

事前定義済みレコードを使用して Flexible NetFlow を設定およびイネーブルにするには、次のタスクを実行します。

- 「事前定義済みレコードを使用した IPv4 トラフィックのフロー モニタの設定」（P.20）（必須）
- 「事前定義済みレコードを使用した IPv6 トラフィックのフロー モニタの設定」（P.21）（必須）
- 「インターフェイスへの IPv4 フロー モニタの適用」（P.23）（必須）
- 「インターフェイスへの IPv6 フロー モニタの適用」（P.24）（必須）
- 「フロー モニタの現在のステータスの表示」（P.25）（任意）
- 「フロー モニタの設定の確認」（P.26）（任意）
- 「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.27）（任意）
- 「フロー モニタ キャッシュ内のデータの表示」（P.28）（任意）

事前定義済みレコードを使用した IPv4 トラフィックのフロー モニタの設定

フロー モニタ用の事前定義済みレコードを使用して IPv4 トラフィックのフロー 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。レコード フォーマットは、いずれかの事前定義済みレコードのフォーマットにできますが、高度なユーザは Flexible NetFlow のフロー 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、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。

制約事項

フロー モニタのレコード フォーマットを **record** コマンドで変更するには、その前にフロー モニタを適用してある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。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*

4. **description** *description*
5. **record** {**netflow-original** | **netflow ipv4** *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：** `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** *description* **例：** `Router(config-flow-monitor)# description Used for monitoring IPv4 traffic`	（任意）フロー モニタの説明を作成します。
ステップ 5	**record** {**netflow-original** | **netflow ipv4** *record* [**peer**]} **例：** `Router(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：** `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。

事前定義済みレコードを使用した IPv6 トラフィックのフロー モニタの設定

フロー モニタ用の事前定義済みレコードを使用して IPv6 トラフィックのフロー 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。レコード フォーマットは、いずれかの事前定義済みレコードのフォーマットにできますが、高度なユーザは Flexible NetFlow のフロー 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、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。

制約事項

フロー モニタのレコード フォーマットを **record** コマンドで変更するには、その前にフロー モニタを適用してある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。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record netflow 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：** `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-2`	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：** `Router(config-flow-monitor)# description Used for monitoring IPv6 traffic`	（任意）フロー モニタの説明を作成します。
ステップ 5	**record netflow ipv6** *record* [**peer**] **例：** `Router(config-flow-monitor)# record netflow ipv6 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：** `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。

インターフェイスへの IPv4 フロー モニタの適用

アクティブにする前に、IPv4 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 モニタをインターフェイスに適用して IPv4 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」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、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、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. **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。

	コマンドまたはアクション	目的
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。 • 同じインターフェイスで **ip flow monitor** *monitor-name* **input** および **ip flow monitor** *monitor-name* **output** コマンドを設定することで、入力と出力のトラフィック分析を同時に設定できます。入力と出力のトラフィック分析に、異なるフロー モニタを使用できます。
ステップ 5	**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。

インターフェイスへの IPv6 フロー モニタの適用

アクティブにする前に、IPv6 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 モニタをインターフェイスに適用して IPv4 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 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、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 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、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. **ipv6 flow monitor** *monitor-name* {**input** | **output**}
5. **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	**ipv6 flow monitor** *monitor-name* {**input** | **output**} **例：** `Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 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。 • 同じインターフェイスで **ipv6 flow monitor** *monitor-name* **input** および **ipv6 flow monitor** *monitor-name* **output** コマンドを設定することで、入力と出力のトラフィック分析を同時に設定できます。入力と出力のトラフィック分析に、異なるフロー モニタを使用できます。
ステップ 5	**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。

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。

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**

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

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 FLOW-MONITOR-1:
  Description:       Used for monitoring IPv4 traffic
  Flow Record:       netflow ipv4 original-input
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 196620 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs

Flow Monitor FLOW-MONITOR-2:
  Description:       Used for monitoring IPv6 traffic
  Flow Record:       netflow ipv6 original-input
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 278544 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
```

フロー モニタの設定の確認

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 running-config flow monitor**

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

Building configuration...

Current configuration:
!
flow monitor FLOW-MONITOR-1
 description Used for monitoring IPv4 traffic
 record netflow ipv4 original-input
!
flow monitor FLOW-MONITOR-2
 description Used for monitoring IPv6 traffic
 record netflow ipv6 original-input
!
end
```

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 *type number*

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
```

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:                                 4096
  Current entries:                               1
  High Watermark:                                2

  Flows added:                                   8
  Flows aged:                                    7
    - Active timeout    (  1800 secs)            0
    - Inactive timeout (    15 secs)             7
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0

IP DESTINATION AS:        0
IPV4 DESTINATION PREFIX:  172.16.10.0
```

```
IPV4 DESTINATION MASK:    /24
INTERFACE OUTPUT:         Et1/0
FLOW DIRECTION:           Input
counter bytes:            4292430
counter packets:          4305
timestamp first:          15853684
timestamp last:           15860868

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

Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                               6
  High Watermark:                                8

  Flows added:                                1048
  Flows aged:                                 1042
    - Active timeout   (  1800 secs)            11
    - Inactive timeout (    15 secs)          1031
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0

IPV6 FLOW LABEL:          0
IPV6 EXTENSION MAP:       0x00000040
IPV6 SOURCE ADDRESS:      2001:DB8:1:ABCD::1
IPV6 DESTINATION ADDRESS: 2001:DB8:4:ABCD::2
TRNS SOURCE PORT:         3000
TRNS DESTINATION PORT:    55
INTERFACE INPUT:          Et0/0
FLOW DIRECTION:           Input
FLOW SAMPLER ID:          0
IP PROTOCOL:              17
IP TOS:                   0x00
ip source as:             0
ip destination as:        0
ipv6 next hop address:    ::
ipv6 source mask:         /48
ipv6 destination mask:    /0
tcp flags:                0x00
interface output:         Null
counter bytes:            521192
counter packets:          9307
timestamp first:          9899684
timestamp last:           11660744
.
.
.
IPV6 FLOW LABEL:          0
IPV6 EXTENSION MAP:       0x00000000
IPV6 SOURCE ADDRESS:      FE80::A8AA:BBFF:FEBB:CC03
IPV6 DESTINATION ADDRESS: FF02::9
TRNS SOURCE PORT:         521
TRNS DESTINATION PORT:    521
INTERFACE INPUT:          Et0/0
FLOW DIRECTION:           Input
FLOW SAMPLER ID:          0
IP PROTOCOL:              17
IP TOS:                   0xE0
ip source as:             0
ip destination as:        0
ipv6 next hop address:    ::
ipv6 source mask:         /10
ipv6 destination mask:    /0
```

```
tcp flags:                  0x00
interface output:           Null
counter bytes:              92
counter packets:            1
timestamp first:            11653832
timestamp last:             11653832
```

事前定義済みレコードによる Flexible NetFlow の設定例

ここでは、次の設定例について説明します。

- 「IPv4 トラフィック用の Flexible NetFlow 事前定義済みレコードの設定：例」（P.30）
- 「IPv6 トラフィック用の Flexible NetFlow 事前定義済みレコードの設定：例」（P.30）

IPv4 トラフィック用の Flexible NetFlow 事前定義済みレコードの設定 : 例

次の例は、Flexible NetFlow の事前定義済みレコード「BGP ToS next-hop」を使用して、IPv4 トラフィックを監視するフロー モニタ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 monitor FLOW-MONITOR-1
 record netflow ipv4 bgp-nexthop-tos
 exit
!
ip cef
!
interface Ethernet 0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

IPv6 トラフィック用の Flexible NetFlow 事前定義済みレコードの設定 : 例

次の例は、Flexible NetFlow の事前定義済みレコード「source prefix」を使用して、IPv6 トラフィックを監視するフロー モニタ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 monitor FLOW-MONITOR-2
 record netflow ipv6 source-prefix
 exit

ip cef
ipv6 cef
!
interface Ethernet 0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 input
!
```

次の作業

Quality of Service（QoS）と帯域幅モニタリング、アプリケーションおよびユーザ フロー モニタリングとプロファイリング、セキュリティ分析など、特定の目的に対する Flexible NetFlow の高度な設定の詳細については、「Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors」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。

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 のカスタマイズ	「Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors」
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」
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 18 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 18 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 18　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。 • 「事前定義済みレコードによる Flexible NetFlow 設定の前提条件」（P.2） • 「事前定義済みレコードによる Flexible NetFlow の設定について」（P.2） • 「フロー モニタ用の事前定義済みレコードを使用した Flexible NetFlow の設定方法」（P.20） • 「事前定義済みレコードによる Flexible NetFlow の設定例」（P.30） 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 18　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。 • 「事前定義済みレコードを使用した IPv6 トラフィックのフロー モニタの設定」（P.21） • 「インターフェイスへの IPv6 フロー モニタの適用」（P.24） • 「IPv6 トラフィック用の Flexible NetFlow 事前定義済みレコードの設定：例」（P.30） 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**