追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用

ここでは、NetFlow フィルタリングまたはサンプリングを使用して、追跡するネットワーク トラフィックを選択する方法について説明します。ここで説明する NetFlow 入力フィルタリング機能およびランダム サンプル NetFlow 機能により、トラフィックの特定のサブセットからデータを収集できます。

- NetFlow 入力フィルタ機能では、NetFlow で処理するためのフローを選択するフィルタを作成することにより、トラフィックの特定のサブセットに関する NetFlow データが得られます。たとえば、特定のホスト グループからのフローを選択できます。
- ランダム サンプル NetFlow 機能では、連続した *n* 個のパケット（*n* はユーザが設定可能なパラメータ）ごとにランダムに選択される 1 個のパケットだけを処理することにより、Cisco ルータ内のトラフィックのサブセットに関する NetFlow データが得られます。

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 アプリケーションであり、ネットワーク アカウンティングおよびセキュリティの新たな主要テクノロジーになりつつあります。

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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用の機能情報」（P.22）を参照してください。

プラットフォーム サポートと Cisco ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

内容

追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用の前提条件

NetFlow 入力フィルタの前提条件

NetFlow 入力フィルタ機能を設定する前に、次の作業を実行しておく必要があります。

- IP ルーティング用にルータを設定する。
- ルータおよび、NetFlow 入力フィルタをイネーブルにするインターフェイスで Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）スイッチングまたは distributed CEF（dCEF; 分散 CEF）スイッチングを設定する（高速スイッチングはサポートされていません）。
- トラフィック クラスを作成し、NetFlow サンプラ マップを定義する。

（注） NetFlow 入力フィルタ機能は、バージョン 5 およびバージョン 9 の NetFlow エクスポート フォーマットでサポートされています。

ランダム サンプル NetFlow の前提条件

ランダム サンプル NetFlow 機能を設定する前に、次の作業を実行しておく必要があります。

- IP ルーティング用にルータを設定する。
- ルータおよび、ランダム サンプル NetFlow をイネーブルにするインターフェイスでシスコ エクスプレス フォワーディング（CEF）スイッチングまたは分散 CEF（dCEF）スイッチングを設定する（高速スイッチングはサポートされていません）。
- NetFlow データをエクスポートする場合は、NetFlow バージョン 5 またはバージョン 9 データ エクスポートを設定する（設定しなかった場合、NetFlow データは、キャッシュ内で表示できますが、エクスポートされません）。
- サンプラ オプション テンプレートを使用する場合、または NetFlow サンプラ ID を表示する場合は、NetFlow バージョン 9 を設定する。

追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用に関する制約事項

NetFlow 入力フィルタの制約事項

Cisco 7500 プラットフォームの場合、NetFlow 入力フィルタ機能は、分散モードでしかサポートされていません。

ランダム サンプル NetFlow の制約事項

フル NetFlow がインターフェイス上でイネーブルになっている場合、フル NetFlow がランダム サンプル NetFlow よりも優先されます（したがって、ランダム サンプル NetFlow は無効になります）。つまり、インターフェイス上でランダム サンプル NetFlow をイネーブルにする前に、そのインターフェイス上のフル NetFlow をディセーブルにする必要があります。

物理インターフェイス上でランダム サンプル NetFlow をイネーブルにしても、サブインターフェイス上でランダム サンプル NetFlow が自動的にイネーブルになることはありません。サブインターフェイス上で明示的に設定する必要があります。また、ランダム サンプル NetFlow を物理インターフェイス（またはサブインターフェイス）上でディセーブルにしても、フル NetFlow がイネーブルになることはありません。この制約事項は、フル NetFlow への移行によって物理インターフェイス（またはサブインターフェイス）に過剰な負荷がかかるのを防いでいます。フル NetFlow が必要な場合は、明示的にイネーブルにする必要があります。

ランダム サンプル NetFlow をバージョン 5 データ エクスポートでイネーブルにすると、サンプラ オプション テンプレートはエクスポートされず、サンプラ ID がバージョン 5 レコード パッド フィールドの最後のバイトの下位 3 ビットにエクスポートされます。サンプラ オプション テンプレートを使用する場合、または NetFlow サンプラ ID を表示する場合は、NetFlow バージョン 9 を使用します。

追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用について

ロードマップ：追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用

表 1 に、対象となるトラフィックを選択するための関連情報と設定手順へのリンクを示します。

表 1　ロードマップ：サンプリングとフィルタリングを使用した追跡するネットワーク トラフィックの選択

対象となるトラフィック	関連情報と設定手順へのリンク
クラスベースのトラフィック分析とモニタを目的とした NetFlow トラフィックの特定のサブセット（ネットワーク上またはネットワーク外のトラフィックなど）	関連情報： • 「NetFlow トラフィックのフィルタリングとサンプリング」（P.4） • 「NetFlow 入力フィルタ：フロー分類」（P.6） • 「NetFlow 入力フィルタの前提条件」（P.2） • 「NetFlow 入力フィルタの制約事項」（P.3） 設定手順： • 「NetFlow データ エクスポートの影響を軽減する NetFlow 入力フィルタの設定」（P.7）
トラフィック エンジニアリングまたは容量プランニングを目的としたネットワーク トラフィックの統計的なサンプリング	関連情報： • 「NetFlow トラフィックのフィルタリングとサンプリング」（P.4） • 「ランダム サンプル NetFlow：サンプリング モード」（P.7） • 「ランダム サンプル NetFlow の前提条件」（P.2） • 「ランダム サンプル NetFlow の制約事項」（P.3） 設定手順： • 「NetFlow データ エクスポートの影響を軽減する NetFlow 入力フィルタの設定」（P.7）

NetFlow トラフィックのフィルタリングとサンプリング

NetFlow では、Cisco ルータにおいてフロー単位の非常に細かいトラフィック統計情報が提供されます。フローとは、同じサブインターフェイス上でルータに到着し、送信元と宛先の IP アドレス、レイヤ 4 プロトコル、送信元と宛先の TCP/UDP ポート、および IP ヘッダー内の Type of Service（ToS; タイプ オブ サービス）バイトが同一である単方向のパケットのストリームです。ルータにより NetFlow 統計情報が NetFlow キャッシュに蓄積され、蓄積された情報は、外部デバイス（Cisco Networking Service（CNS）NetFlow Collection Engine など）にエクスポートしてさらに処理できます。

フル NetFlow では、イネーブルのサブインターフェイスに入ってくるすべてのトラフィックが記録されます。しかし、場合によっては、このトラフィックのサブセットに関してだけ、NetFlow データを収集することがあります。ランダム サンプル NetFlow 機能および NetFlow 入力フィルタ機能では、NetFlow で処理するために、着信トラフィックを関係のあるトラフィックだけに制限できます。ランダム サンプル NetFlow では、連続した *n* 個のパケットごとにランダムに選択された 1 個のパケットだけを処理することにより、Cisco ルータ内のトラフィックのサブセットが NetFlow データとして提供されます。NetFlow 入力フィルタ機能では、ユーザが定義した特定のトラフィックのサブセットに関してだけ NetFlow データを収集できます。

（注）　ランダム サンプル NetFlow は、サンプル NetFlow よりも統計的に正確です。NetFlow でパケットをサンプリングする機能は、サンプル NetFlow 機能によって最初に提供されました。サンプル NetFlow 機能で使用される方法論は、*決定論的な*サンプリングです。この方法では、インターフェイスごとに毎回 *n* 番めのパケットが NetFlow で処理するために選択されます。たとえば、サンプリング レートを 100 パケットごとに 1 つとして設定すると、1 番め、101 番め、201 番め、301 番めと続くパケットがサン

プル NetFlow によってサンプリングされます。サンプル NetFlow では、ランダムなサンプリングはできません。そのため、トラフィックが一定のパターンで到着する場合は、統計情報が不正確になる可能性があります。

（注） ランダム サンプル NetFlow アルゴリズムは、入力フィルタリングの後に適用されます。

表 2 に、NetFlow 入力フィルタ機能と NetFlow ランダム サンプル機能の比較を示します。

表 2 NetFlow 入力フィルタ機能とランダム サンプル NetFlow 機能の比較

比較カテゴリ	NetFlow 入力フィルタ機能	ランダム サンプル NetFlow 機能
簡単な説明	この機能では、NetFlow データをトラフィックの特定のサブセットにだけ基づいて収集できます。フィルタを作成して NetFlow で処理するフローを選択することにより実行します。たとえば、特定のホスト グループからのフローを選択できます。また、この機能では、選択されたフローに対してさまざまなサンプリング レートを選択することもできます。	この機能では、連続した *n* 個のパケット（*n* はユーザが設定可能なパラメータ）ごとにランダムに選択される 1 個のパケットだけを処理することにより、Cisco ルータ内のトラフィックのサブセットが NetFlow データとして提供されます。パケットは、到着時にサンプリングされます（これらのパケットに対して NetFlow キャッシュ エントリが作成される前）。
主な用途	この機能は、クラスベースのトラフィック分析およびネットワーク上またはネットワーク外のトラフィックのモニタに使用できます。	この機能は、トラフィック エンジニアリングや容量プランニング、およびフル NetFlow でなくてもネットワーク トラフィックの正確なビューが得られるアプリケーションに使用できます。
エクスポート フォーマットのサポート	この機能は、バージョン 5 およびバージョン 9 の NetFlow エクスポート フォーマットでサポートされています。	この機能は、バージョン 5 およびバージョン 9 の NetFlow エクスポート フォーマットでサポートされています。
Cisco IOS Release のサポート	12.3(4)T	12.3(2)T、12.2(18)S、および 12.0(26)S
サブインターフェイスのサポート	物理インターフェイス単位でだけでなく、サブインターフェイス単位でも NetFlow 入力フィルタを設定できます。 サブインターフェイスごとに複数のフィルタを選択し、すべてのフィルタを同時に実行できます。	物理インターフェイス単位でだけでなく、サブインターフェイス単位でもランダム サンプル NetFlow 機能を設定できます。 トラフィックは、ランダム サンプル NetFlow が設定されているサブインターフェイス上でだけ収集されます。フル NetFlow の場合と同様に、ランダム サンプル NetFlow を物理インターフェイス上でイネーブルにしても、サブインターフェイス上のランダム サンプル NetFlow が自動でイネーブルになることはありません。サブインターフェイス上で明示的に設定する必要があります。

表 2　NetFlow 入力フィルタ機能とランダム サンプル NetFlow 機能の比較（続き）

比較カテゴリ	NetFlow 入力フィルタ機能	ランダム サンプル NetFlow 機能
メモリへの影響	この機能には、追加のメモリは必要ありません。フローの本数が大幅に減少するため、フル NetFlow よりも小さい NetFlow キャッシュを使用できます。この機能では、設定した NetFlow サンプラごとに少量のメモリが必要になります。	この機能では、フローの本数が大幅に減少するため、フル NetFlow よりも小さい NetFlow キャッシュを使用できます。この機能では、設定した NetFlow サンプラごとに少量のメモリが必要になります。
パフォーマンス上の影響	分類されたトラフィックのアカウンティングによって、処理およびエクスポートの対象となるフローの本数が減少するので、ルータのリソースが節約されます。節約される帯域幅の量は、使用状況とクラス マップ基準に依存します。 ただし、ポリシーに設定されたクラス マップの数と複雑さによっては、パフォーマンスが低下する可能性もあります。	統計的なトラフィックのサンプリングによって、価値のある NetFlow データが得られるとともに、ルータ リソースの消費が大幅に削減されます（特に CPU リソース）。 この機能により、NetFlow データ エクスポートがインターフェイス トラフィックに与える影響が大幅に減少します。たとえば、100 パケットごとに 1 つのサンプリング レートでは、NetFlow データのエクスポートが約 50% 減少します。

NetFlow 入力フィルタ：フロー分類

NetFlow 入力フィルタ機能では、送信元と宛先の IP アドレス、レイヤ 4 プロトコルとポート番号、着信インターフェイス、MAC アドレス、IP Precedence、DSCP 値、レイヤ 2 情報（フレームリレー DE ビットやイーサネット 802.1p ビットなど）、および Network-Based Application Recognition（NBAR）情報に基づいてパケットを分類できます。パケットは、上記の基準に基づいて分類（フィルタリング）され、サブインターフェイス上でフロー アカウンティングが適用されます。

フィルタリング メカニズムでは、フローの分類に Modular QoS Command-Line Interface（MQC）が使用されます。サブインターフェイスごとに複数のフィルタをマッチング サンプラとともに作成できます。たとえば、サブインターフェイス トラフィックをタイプ オブ サービス（ToS）値または宛先プレフィクス（あるいは両方）に基づいて複数のクラスに分割できます。高プライオリティのクラスには高いレートを使用し、低プライオリティのクラスには低いレートを使用して、クラスごとに異なるレートでサンプリングを設定することもできます。

MQC には、帯域幅の速度やキューイング管理などの多くのポリシー（アクション）があります。これらのポリシーは、サブインターフェイスに適用されているクラス マップ内の基準にパケットが一致した場合に限り、適用されます。クラス マップは、match 句とその評価方法に関する指示のセットを保管しており、ポリシーのフィルタとして働きます。ポリシーは、パケットの内容が match 句を満たしている場合に限り適用されます。NetFlow 入力フィルタ機能では、NetFlow アカウンティングが MQC インフラストラクチャに追加されます。つまり、パケットが match 句を満たしている場合に限り、フロー アカウンティングがパケットに対して実行されます。

2 種類のフィルタを使用できます。

- ACL ベースのフローマスク フィルタ
- フィルタのフィールド（送信元 IP アドレス、宛先 IP アドレス、送信元アプリケーション ポート、宛先アプリケーション ポート、ポート プロトコル、ToS ビット、および TCP フラグ）

ランダム サンプル NetFlow：サンプリング モード

サンプリング モードでは、NetFlow で処理するためのトラフィックのサブセットを選択するアルゴリズムが使用されます。ランダム サンプル NetFlow 機能で使用されるランダム サンプリング モードでは、連続した *n* 個のパケットにつき *平均的に* 1 つのパケットが NetFlow の処理用に選択されるように、着信パケットがランダムに選択されます。たとえば、サンプリング レートを 100 パケットごとに 1 つとして設定すると、NetFlow によって 5 番めのパケットがサンプリングされ、その後に、120 番め、199 番め、302 番めというようにサンプリングされる可能性があります。この設定例では、全トラフィックの 1% に対する NetFlow データが得られます。*n* の値はパラメータであり、1 ～ 65535 パケットの範囲内で設定できます。

ランダム サンプル NetFlow：NetFlow サンプラ

NetFlow サンプラ マップにより、NetFlow サンプリングの特性（サンプリング レートや NetFlow サンプラ名など）のセットが定義されます。各 NetFlow サンプラ マップは、物理インターフェイスだけでなく、1 つ以上のサブインターフェイスにも適用できます。最大で 8 つの NetFlow サンプラ マップを定義できます。

たとえば、ランダム サンプリング モードと 100 パケットにつき 1 つのサンプリング レートを特性として持つ mysampler1 という名前の NetFlow サンプラ マップを作成できます。この NetFlow サンプラ マップは、任意の数のサブインターフェイスに適用できます。適用された各サブインターフェイスでは、mysampler1 を参照して NetFlow サンプリングが実行されます。これらのサブインターフェイスからのトラフィックは（サンプリングの観点から）マージされます。これにより、サブインターフェイス単位の NetFlow サンプリングよりもさらに強い「ランダム性」が導入されますが、統計的には、関係する各サブインターフェイスに同じ 100 パケットにつき 1 つのサンプリング レートが与えられます。

ランダム サンプル NetFlow におけるサンプリングは、NetFlow サンプラによって行われます。NetFlow サンプラは、物理インターフェイスまたはサブインターフェイスに適用されている NetFlow サンプラ マップのインスタンスとして定義されます。物理インターフェイス上でフル NetFlow が設定されると、その物理インターフェイスのすべてのサブインターフェイス上でランダム サンプル NetFlow がフル NetFlow に上書きされます。

NetFlow フィルタリングまたはサンプリングの設定方法

- 「NetFlow データ エクスポートの影響を軽減する NetFlow 入力フィルタの設定」（P.7）
- 「NetFlow データ エクスポートの影響を軽減するランダム サンプル NetFlow の設定」（P.13）

（注） ランダム サンプル NetFlow アルゴリズムを適用する前に、入力フィルタリングを設定する必要があります。

NetFlow データ エクスポートの影響を軽減する NetFlow 入力フィルタの設定

NetFlow 入力フィルタを設定するには、次の作業を実行します。NetFlow 入力フィルタを設定することにより、NetFlow データ エクスポートの影響が軽減されます。

- 「NetFlow 入力フィルタリング用のポリシー マップのクラス マップの作成」（P.8）（必須）
- 「NetFlow 入力フィルタリング用のポリシー マップのサンプラ マップの作成」（P.10）（必須）

- 「NetFlow サンプリング アクションが含まれているクラスベースのポリシーの作成」（P.11）（必須）
- 「NetFlow サンプリング アクションが含まれているポリシーのインターフェイスへの適用」（P.12）（必須）

NetFlow 入力フィルタリング用のポリシー マップのクラス マップの作成

NetFlow 入力フィルタリング用のポリシー マップのクラス マップを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all** | **match-any**]
4. **match access-group** *access-group*
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。 • 必要に応じて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。

	コマンドまたはアクション	目的
ステップ 3	**class-map** *class-map-name* [**match-all** | **match-any**] **例：** `Router(config)# class-map my_high_importance_class`	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。 • *class-map-name* 引数は、クラス マップ用のクラスの名前です。名前には最大 40 文字までの英数字を指定できます。クラス名は、クラス マップに対して、およびポリシー マップ内でクラスのポリシーを設定するために使用されます。 • **match-all | match-any** キーワードは、複数の一致基準が存在するときのパケットの評価方法を決定します。パケットは、クラスのメンバーとして見なされるために、すべての一致基準（**match-all**）または一致基準の 1 つだけ（**match-any**）のいずれかを満たす必要があります。 **class-map** コマンドを入力すると、クラス マップ コンフィギュレーション モードがイネーブルになります。このモードでは、match コマンドの 1 つを入力して、このクラスの一致基準を設定できます。
ステップ 4	**match access-group** *access-group* **例：** `Router(config-cmap)# match access-group 101`	指定した Access Control List（ACL; アクセス コントロール リスト）に基づいて、クラス マップの一致基準を設定します。 • *access-group* 引数は、パケットがこのクラスに属するかどうかを判定するための一致基準として使用される番号付き ACL です。ACL 番号の範囲は、1 ～ 2699 です。
ステップ 5	**end** **例：** `Router(config-cmap)# end`	現在の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。

NetFlow 入力フィルタリング用のポリシー マップのサンプラ マップの作成

NetFlow 入力フィルタリング用のポリシー マップのサンプラ マップを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random** *one-out-of* **packet-interval**
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。 • 必要に応じて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-sampler-map** *sampler-map-name* **例：** `Router(config)# flow-sampler-map my_high_sampling`	統計的なサンプリングの NetFlow エクスポート フロー サンプラ マップを定義します。 • *sampler-map-name* 引数は、定義されるフロー サンプラ マップの名前です。 **flow-sampler-map** コマンドを入力すると、フロー サンプラ コンフィギュレーション モードがイネーブルになります。
ステップ 4	**mode random** *one-out-of* **packet-interval** **例：** `Router(config-sampler-map)# mode random one-out-of 100`	統計的なサンプリングの NetFlow エクスポート ランダム サンプリング モードとパケット間隔を指定します。 • **random** キーワードは、サンプリングにランダム サンプリング モードを使用することを指定します。 • *one-out-of* **packet-interval** の引数とキーワードのペアは、サンプリングを行うパケット間隔（*n* パケットごとに 1 つ）を指定します。*n* には、1 ～ 65535（パケット）を指定できます。
ステップ 5	**end** **例：** `Router(config-sampler-map)# end`	現在の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。

NetFlow サンプリング アクションが含まれているクラスベースのポリシーの作成

NetFlow サンプリング アクションが含まれているクラスベースのポリシーを作成するには、次の手順を実行します。

1 つのクラスには、1 つの NetFlow 入力フィルタ サンプラしか割り当てられません。続けて NetFlow 入力フィルタ サンプラをクラスに割り当てると、前のサンプラは上書きされます。NetFlow サンプラ マップを削除すると、対応するポリシー マップの NetFlow 入力フィルタ サンプラも削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **netflow-sampler** *map-name*
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。 • 必要に応じて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	**policy-map** *policy-map-name* **例：** `Router(config)# policy-map mypolicymap`	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。 • *policy-map-name* 引数は、ポリシー マップの名前です。名前には最大 40 文字までの英数字を指定できます。 **policy-map** コマンドを入力すると、Quality of Service（QoS）ポリシー マップ コンフィギュレーション モードがイネーブルになります。このモードでは、指定したポリシー マップのクラス ポリシーを設定または変更できます。

	コマンドまたはアクション	目的
ステップ 4	**class** {*class-name* | **class-default**} **例：** `Router(config-pmap)# class my_high_importance_class`	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。 • *class-name* 引数は、ポリシーを設定または変更するクラスの名前です。 • **class-default** キーワードは、デフォルト クラスのポリシーを設定または変更できるようにデフォルト クラスを指定します。 **class** コマンドを入力すると、QoS ポリシー マップ クラス コンフィギュレーション モードがイネーブルになります。
ステップ 5	**netflow-sampler** *sampler-map-name* **例：** `Router(config-pmap-c)# netflow-sampler high_sampling`	NetFlow 入力フィルタ サンプラをイネーブルにします。 • *sampler-map-name* 引数は、クラスに適用する NetFlow サンプラ マップの名前です。 1 つのクラスには、1 つの NetFlow 入力フィルタ サンプラしか割り当てられません。同じクラスに NetFlow 入力フィルタ サンプラをもう 1 つ割り当てると、前のものは上書きされます。
ステップ 6	**end** **例：** `Router(config-pmap-c)# end`	現在の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。

NetFlow サンプリング アクションが含まれているポリシーのインターフェイスへの適用

NetFlow サンプリング アクションが含まれているポリシーをインターフェイスに適用するには、次の手順を実行します。

サービス ポリシーを **policy-map** コマンドで定義した後、インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用して、定義したサービス ポリシーを 1 つ以上のインターフェイスに付加します。それにより、それらのインターフェイスのサービス ポリシーが指定されます。同じサービス ポリシーを複数のインターフェイスに割り当てられますが、各インターフェイスに付加できるのは、1 つのサービス ポリシーだけです。このサービス ポリシーは、入力方向にだけ適用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **service-policy** {**input** | **output**} *policy-map-name*
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。 • 必要に応じて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** *interface-type interface-number* **例：** `Router(config)# interface POS 1/0`	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	**service-policy** {**input** | **output**} *policy-map-name* **例：** `Router(config-if)# service-policy input mypolicymap`	インターフェイスまたは Virtual Circuit（VC; 仮想回線）のサービス ポリシーとして使用されるポリシー マップを入力のインターフェイスまたは VC（あるいは出力のインターフェイスまたは VC）に付加します。 • **input** キーワードは、指定されたポリシー マップを入力インターフェイスまたは入力 VC に付加します。 • **output** キーワードは、指定されたポリシー マップを出力インターフェイスまたは出力 VC に付加します。 • *policy-map-name* は、付加されるサービス ポリシー マップ（**policy-map** コマンドを使用して作成される）の名前です。名前には最大 40 文字までの英数字を指定できます。
ステップ 5	**end** **例：** `Router(config-if)# end`	現在の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。

トラブルシューティングのヒント

debug flow-sampler class-based コマンドを使用して、NetFlow 入力フィルタのデバッグ出力を表示します。

NetFlow データ エクスポートの影響を軽減するランダム サンプル NetFlow の設定

ランダム サンプル NetFlow 機能を設定し、その設定を確認するには、次の手順を実行します。

- 「NetFlow サンプラ マップの定義」（P.14）（必須）
- 「インターフェイスへの NetFlow サンプラ マップの適用」（P.14）（必須）

- 「ランダム サンプル NetFlow の設定の確認」（P.15）（任意）

NetFlow サンプラ マップの定義

NetFlow サンプラ マップを定義するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random one-out-of** *sampling-rate*
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。 • 必要に応じて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-sampler-map** *sampler-map-name* **例：** `Router(config)# flow-sampler-map mysampler1`	NetFlow サンプラ マップを定義し、フロー サンプラ マップ コンフィギュレーション モードを開始します。 • *sampler-map-name* 引数は、定義される NetFlow サンプラ マップの名前です。
ステップ 4	**mode random one-out-of** *sampling-rate* **例：** `Router(config-sampler)# mode random one-out-of 100`	ランダム モードをイネーブルにし、NetFlow サンプラのサンプリング レートを指定します。 • **random** キーワードは、サンプリングにランダム モードを使用することを指定します。 • **one-out-of** *sampling-rate* のキーワードと引数のペアは、サンプリングを行うサンプリング レート（*n* パケットごとに 1 つ）を指定します。*n* には、1 ～ 65535（パケット）を指定できます。
ステップ 5	**end** **例：** `Router(config-sampler)# end`	現在の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。

インターフェイスへの NetFlow サンプラ マップの適用

NetFlow サンプラ マップをインターフェイスに適用するには、次の作業を実行します。

NetFlow サンプラ マップを物理インターフェイス（またはサブインターフェイス）に適用して、NetFlow サンプラを作成できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **flow-sampler** *sampler-map-name*
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。 • 必要に応じて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** *interface-type interface-number* **例：** `Router(config)# ethernet 1/0.2`	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	**flow-sampler** *sampler-map-name* **例：** `Router(config-if)# flow-sampler mysampler1`	NetFlow サンプラ マップをインターフェイスに適用して、NetFlow サンプラを作成します。 • *sampler-map-name* 引数は、インターフェイスに適用する NetFlow サンプラ マップの名前です。
ステップ 5	**end** **例：** `Router(config-if)# end`	現在の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。

ランダム サンプル NetFlow の設定の確認

ランダム サンプル NetFlow 機能の設定を確認するには、次の手順を実行します。

手順の概要

1. **show flow-sampler**
2. **show ip cache verbose flow**
3. **show ip flow export template**

手順の詳細

ステップ 1　show flow-sampler

このコマンドを使用して、1 つまたはすべてのランダム サンプル NetFlow サンプラの属性（モード、サンプリング レート、サンプリングされたパケットの数など）を表示し、サンプラの設定を確認します。次に例を示します。

```
Router# show flow-sampler

Sampler : mysampler1, id : 1, packets matched : 10, mode : random sampling mode
  sampling interval is : 100

 Sampler : myflowsampler2, id : 2, packets matched : 5, mode : random sampling mode
  sampling interval is : 200
```

特定の NetFlow サンプラの属性を確認するには、**show flow-sampler** *sampler-map-name* コマンドを使用します。たとえば、mysampler1 という名前の NetFlow サンプラに対しては次のように入力します。

```
Router# show flow-sampler mysampler1

Sampler : mysampler1, id : 1, packets matched : 0, mode : random sampling mode
  sampling interval is : 100
```

ステップ 2　show ip cache verbose flow

このコマンドを使用して、ランダム サンプル NetFlow が設定されているときのヘッダー内の追加の NetFlow フィールドを表示します。次に例を示します。

```
Router# show ip cache verbose flow
...
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active

BGP: BGP NextHop
Et1/0          8.8.8.8         Et0/0*         9.9.9.9         01 00  10       3
0000 /8  302                   0800 /8  300   3.3.3.3               100     0.1
BGP: 2.2.2.2         Sampler: 1  Class: 1  FFlags: 01
```

この例では、サンプラ、クラス ID、および一般的なフラグが設定されているときの **show ip cache verbose flow** コマンドの NetFlow 出力を示しています。フローに関して表示される情報は、そのフローに設定されているフラグによって異なります。フローがサンプラによってキャプチャされた場合は、出力にサンプラ ID が表示されます。フローが MQC によってマーク付けられた場合は、表示にクラス ID が含まれます。一般的なフラグが設定されている場合は、出力にそれらのフラグが含まれます。

show ip cache verbose flow コマンドの出力で表示される可能性のある NetFlow フラグ（FFlags）は、次のとおりです。

- FFlags: 01（#define FLOW_FLAGS_OUTPUT 0x0001）：入力フロー
- FFlags: 02（#define FLOW_FLAGS_DROP 0x0002）：廃棄されたフロー（ACL による廃棄など）
- FFlags: 04（#define FLOW_FLAGS_MPLS 0x0004）：MPLS フロー
- FFlags: 08（#define FLOW_FLAGS_IPV6 0x0008）：IPv6 フロー
- FFlags: 10（#define FLOW_FLAGS_RSVD 0x0010）：予備

IPv6 と RSVD の FFlags はあまり使用されません。FFlags がゼロの場合、その行は出力から省略されます。複数のフラグが定義されている場合は（論理和がとられる）、フラグの両方のセットが 16 進数形式で表示されます。

ステップ 3　show ip flow export template

このコマンドを使用して、テンプレート固有の設定に関して NetFlow データ エクスポートの統計情報（テンプレート タイムアウトやリフレッシュ レートなど）を表示します。次に例を示します。

```
Router# show ip flow export template

Template Options Flag = 0
   Total number of Templates added = 0
   Total active Templates = 0
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 0
   Option Templates added = 0
   Template ager polls = 0
   Option Template ager polls = 0
Main cache version 9 export is enabled
 Template export information
   Template timeout = 30
   Template refresh rate = 20
 Option export information
   Option timeout = 30
   Option refresh rate = 20
```

トラブルシューティングのヒント

debug flow-sampler コマンドを使用して、ランダム サンプル NetFlow 機能のデバッグ出力を表示します。

NetFlow フィルタリングおよびサンプリングの設定例

例：NetFlow データ エクスポートの影響を軽減する NetFlow 入力フィルタの設定

例：NetFlow 入力フィルタリング用のポリシー マップのクラス マップの作成

NetFlow 入力フィルタリング用のポリシー マップのクラス マップを作成する例を示します。この例では、my_high_importance_class および my_medium_importance_class という名前のクラス マップが作成されます。

```
configure terminal
!
```

```
class-map my_high_importance_class
 match access-group 101
 exit
!
class-map my_medium_importance_class
 match access-group 102
 end
```

例：NetFlow 入力フィルタリング用のポリシー マップのサンプラ マップの作成

NetFlow 入力フィルタリング用のポリシー マップのサンプラ マップを作成する例を示します。次の例では、NetFlow 入力フィルタリング用のポリシー マップとともに使用するために、my_high_sampling、my_medium_sampling、および my_low_sampling という名前のサンプラ マップが作成されます。

```
configure terminal
!
flow-sampler-map my_high_sampling
 mode random one-out-of 1
 exit
!
flow-sampler-map my_medium_sampling
 mode random one-out-of 100
 exit
!
flow-sampler-map my_low_sampling
 mode random one-out-of 1000
 end
```

例：NetFlow サンプリング アクションが含まれているポリシーの作成

3 つの NetFlow サンプリング アクションが含まれているクラスベースのポリシーを作成する例を示します。この例では、サンプリング アクション my_high_sampling がクラス my_high_importance_class に適用され、サンプリング アクション my_medium_sampling がクラス my_medium_importance_class に適用され、サンプリング アクション my_low_sampling がデフォルト クラスに適用されます。

```
configure terminal
!
policy-map mypolicymap
 class my_high_importance_class
 netflow sampler my_high_sampling
 exit
!
class my_medium_importance_class
 netflow-sampler my_medium_sampling
 exit
!
class class-default
 netflow-sampler my_low_sampling
end
```

例：インターフェイスへのポリシーの適用

NetFlow サンプリング アクションが含まれているポリシーをインターフェイスに適用する例を示します。この例では、mypolicymap という名前のポリシーがインターフェイス POS1/0 に付加され、さらにインターフェイス ATM2/0 にも付加されます。

```
configure terminal
!
```

```
interface POS1/0
 service-policy input mypolicymap
 exit
!
interface ATM2/0
 service-policy input mypolicymap
 end
```

例：NetFlow データ エクスポートの影響を軽減するランダム サンプル NetFlow の設定

- 「例：NetFlow サンプラ マップの定義」（P.19）
- 「例：インターフェイスへの NetFlow サンプラ マップの適用」（P.19）

例：NetFlow サンプラ マップの定義

mysampler1 という名前の NetFlow サンプラ マップを定義する例を示します。

```
configure terminal
!
flow-sampler-map mysampler1
 mode random one-out-of 100
 end
```

例：インターフェイスへの NetFlow サンプラ マップの適用

CEF スイッチングをイネーブルにし、mysampler1 という名前の NetFlow サンプラ マップをイーサネット インターフェイス 1 に適用して、そのインターフェイス上に NetFlow サンプラを作成する例を示します。

```
configure terminal
!
ip cef
!
interface ethernet 1/0
 flow-sampler mysampler1
 end
```

その他の参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
NetFlow コマンド	『*Cisco IOS NetFlow Command Reference*』
Cisco IOS NetFlow の概要	「*Cisco IOS NetFlow Overview*」
『*Cisco IOS NetFlow コンフィギュレーション ガイド*』に記載されている機能のリスト	「*Cisco IOS NetFlow Features Roadmap*」

関連項目	参照先
NetFlow および NetFlow データ エクスポートの設定に必要な作業の最小限の情報	「*Getting Started with Configuring NetFlow and NetFlow Data Export*」
ネットワーク トラフィック データをキャプチャし、エクスポートするための NetFlow の設定作業	『*Configuring NetFlow and NetFlow Data Export*』
MPLS 認識 NetFlow の設定作業	「*Configuring MPLS Aware NetFlow*」
MPLS 出力 NetFlow アカウンティングの設定作業	「*Configuring MPLS Egress NetFlow Accounting and Analysis*」
ランダム サンプル NetFlow の設定作業	「*Using NetFlow Filtering or Sampling to Select the Network Traffic to Track*」
NetFlow 集約キャッシュの設定作業	『*Configuring NetFlow Aggregation Caches*』
NetFlow BGP ネクスト ホップ サポートの設定作業	「*Configuring NetFlow BGP Next Hop Support for Accounting and Analysis*」
NetFlow マルチキャスト サポートの設定作業	「*Configuring NetFlow Multicast Accounting*」
NetFlow を使用したネットワーク脅威の検出と分析の作業	「*Detecting and Analyzing Network Threats With NetFlow*」
NetFlow の SCTP を使用した信頼性のあるエクスポートの設定作業	「*NetFlow Reliable Export With SCTP*」
NetFlow レイヤ 2 およびセキュリティ モニタリング エクスポートの設定作業	「*NetFlow Layer 2 and Security Monitoring Exports*」
SNMP NetFlow MIB の設定作業	「*Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data*」
NetFlow MIB およびトップ トーカー機能の設定作業	「*Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands*」
CNS NetFlow Collection Engine のインストール、開始、および設定に関する情報	*Cisco CNS NetFlow Collection Engine のマニュアル*

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	—

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 セットの MIB の場所を検索し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
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

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。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

追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用の機能情報

表 3 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。

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、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、フィーチャ 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 3 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。

表 3　追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用の機能情報

機能名	リリース	機能情報
NetFlow 入力フィルタ	12.3(4)T、 12.2(25)S 12.2(27)SBC 15.0(1)S	NetFlow 入力フィルタ機能では、NetFlow で処理するためのフローを選択するフィルタを作成することにより、トラフィックの特定のサブセットに関する NetFlow データが得られます。たとえば、特定のホスト グループからのフローを選択できます。また、この機能では、選択されたフローに対してさまざまなサンプリング レートを選択することもできます。NetFlow 入力フィルタ機能は、たとえば、クラスベースのトラフィック分析や、ネットワーク上またはネットワーク外のトラフィックのモニタに使用します。 この機能に関する詳細については、次の各項を参照してください。 • 「ロードマップ：追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用」（P.3） • 「NetFlow トラフィックのフィルタリングとサンプリング」（P.4） • 「NetFlow 入力フィルタ：フロー分類」（P.6） • 「NetFlow データ エクスポートの影響を軽減する NetFlow 入力フィルタの設定」（P.7） この機能により、**netflow-sampler** コマンドおよび **debug flow-sampler** コマンドが導入または変更されました。

表 3　追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用の機能情報

機能名	リリース	機能情報
ランダム サンプル NetFlow	12.3(4)T、 12.2(18)S、 12.0(26)S、 12.2(27)SBC 12.2(33)SRC	ランダム サンプル NetFlow では、連続した *n* 個のパケット（*n* はユーザが設定可能なパラメータ）ごとにランダムに選択される 1 個のパケットだけを処理することにより、Cisco ルータ内のトラフィックのサブセットに関する NetFlow データが得られます。パケットは、到着時にサンプリングされます（これらのパケットに対して NetFlow キャッシュ エントリが作成される前）。統計的なトラフィックのサンプリングによって、価値のある NetFlow データが得られるとともに、ルータ リソースの消費が大幅に削減されます（特に CPU リソース）。ランダム サンプル NetFlow の主な用途は、トラフィック エンジニアリング、容量プランニング、およびフル NetFlow でなくてもネットワーク トラフィックの正確なビューが得られるアプリケーションです。 Cisco IOS Release 12.2(33)SRC では、この機能は IPv6 ユニキャストおよび IPv4 マルチキャスト機能をサポートするように拡張されています。 この機能に関する詳細については、次の各項を参照してください。 • 「ロードマップ：追跡するネットワーク トラフィックを選択するための NetFlow フィルタリングまたはサンプリングの使用」（P.3） • 「NetFlow トラフィックのフィルタリングとサンプリング」（P.4） • 「ランダム サンプル NetFlow：サンプリング モード」（P.7） • 「ランダム サンプル NetFlow：NetFlow サンプラ」（P.7） • 「NetFlow データ エクスポートの影響を軽減するランダム サンプル NetFlow の設定」（P.13） この機能により、**debug flow-sampler**、**flow-sampler**、**flow-sampler-map**、**mode**（**フロー サンプラ マップ コンフィギュレーション**）、および **show flow-sampler** の各コマンドが導入されました。 この機能により、**ip flow-export** コマンドが変更されました。

用語集

ACL：Access Control List（ACL; アクセス コントロール リスト）。ルータによって保持されるユーザおよびユーザ グループの参加者リストです。このリストは、多数のサービスについてルータに対するアクセスまたはルータからのアクセスを制御するために使用されます。

BGP：ボーダー ゲートウェイ プロトコル。Exterior Gateway Protocol（EGP）に代わるドメイン間ルーティング プロトコル。BGP システムは到着可能性情報を他の BGP システムと交換します。RFC 1163 によって定義されています。

BGP ネクスト ホップ：特定の宛先に到達するために使用されるネクスト ホップの IP アドレス。

CEF：Cisco Express Forwarding。大規模で動的なトラフィック パターンを使用してネットワークのパフォーマンスと拡張性を最適化する、レイヤ 3 IP スイッチング テクノロジー。

dCEF：分散型シスコ エクスプレス フォワーディング。CEF スイッチングの一種であり、ライン カード（Versatile Interface Processor（VIP）ライン カードなど）に Forwarding Information Base（FIB; 転送情報ベース）と隣接テーブルの同一コピーが保持されます。ラインカードは、ポート アダプタ間でエクスプレス フォワーディングを実行します。これにより、ルート スイッチ プロセッサがスイッチング動作から解放されます。

MQC：Modular QoS Command-Line Interface（MQC）。トラフィック ポリスを作成し、それらをインターフェイスに付加することができる CLI 構造です。1 つのトラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の QoS 機能が含まれます。トラフィック ポリシー内にある QoS 機能により、分類後のトラフィックの処理方法が決定されます。

NBAR：Network-Based Application Recognition。Cisco IOS ソフトウェアの分類エンジンです。Transmission Control Protocol（TCP; 伝送制御プロトコル）または User Datagram Protocol（UDP; ユーザ データグラム プロトコル）のポート番号を動的に割り当てる Web ベースのアプリケーションやクライアント/サーバ アプリケーションなど、多種多様なアプリケーションを認識します。アプリケーションが認識された後は、そのアプリケーションの特定のサービスをネットワークで使用できます。NBAR は、Cisco Content Networking アーキテクチャの重要な要素であり、QoS 機能と連動して、ネットワーク帯域幅の効率的な利用を可能にします。

NetFlow：フロー単位の情報を保持する Cisco IOS セキュリティおよびアカウンティング機能。

NetFlow v9：NetFlow エクスポート フォーマットのバージョン 9。ネットワーク ノードからコレクタに NetFlow レコードを送信するための柔軟で拡張可能な手段です。NetFlow バージョン 9 には定義可能なレコード タイプが用意されています。また、自己記述型で、NetFlow Collection Engine の設定を容易にします。

NetFlow サンプラ：少なくとも 1 つの物理インターフェイスまたはサブインターフェイスに適用されている NetFlow サンプラ マップ内で定義された特性のセット。

NetFlow サンプラ マップ：NetFlow サンプリング用の特性（サンプリング レートなど）のセットの定義。

ToS：Type of Service（ToS; タイプ オブ サービス）。特定のデータグラムに必要な Quality of Service を示す、IP ヘッダーの 2 番めのバイトです。

高速スイッチング：ルート キャッシュを使用して、ルータを介したパケット交換を促進するシスコの機能。

フロー：任意の送信元と宛先の間の単方向のパケットのストリーム。送信元と宛先は、ネットワークレイヤの IP アドレスとトランスポートレイヤの送信元および宛先のポート番号によってそれぞれ定義されます。