Cisco IOS XE Flexible NetFlow の概要

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 XE 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イネーブルに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。

このモジュールでは、Flexible NetFlow の概要、および Flexible NetFlow の高度な機能とサービスについて説明します。

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。

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 に関する制約事項」（P.2）
- 「Flexible NetFlow について」（P.2）
- 「関連情報」（P.13）
- 「参考資料」（P.14）

Flexible Netflow に関する制約事項

Flexible Netflow は、ASR 1000 シリーズ ルータの ESP（Embedded Services Processor）リソースに大きな影響を与えます。キャッシュ レコードのサイズおよび数に応じて、Flexible Netflow キャッシュで大量の ESP DRAM を消費する可能性があります。

Flexible Netflow または以前の NetFlow によって消費されるデータプレーン メモリの合計量は、ESP/FP のデータ プレーン DRAM 量の最大 25% に制限することをお勧めします。

データ プレーンメモリ使用量の許容サイズの設定方法については、「Getting Started with Configuring Cisco IOS XE Flexible NetFlow」モジュールを参照してください。

Flexible NetFlow について

ここでは、Flexible NetFlow の概要について説明します。

- 「NetFlow 一般的な使用方法」（P.2）
- 「以前の NetFlow および Flexible NetFlow でのフローの使用」（P.3）
- 「以前の NetFlow と Flexible NetFlow」（P.4）
- 「Flexible NetFlow のコンポーネント」（P.5）
- 「Flexible NetFlow でのセキュリティ監視」（P.12）
- 「以前の NetFlow と Flexible NetFlow の機能の比較」（P.12）

NetFlow 一般的な使用方法

一般的に、NetFlow は次のような、重要なカスタマー アプリケーションのいくつかで使用されます。

- ネットワークのモニタリング。NetFlow データでは、ほぼリアルタイムのさまざまなネットワークのモニタリング機能を利用できます。ネットワーク オペレータはフローベースの分析手法を使用して、個々のルータおよびスイッチに関連付けられたトラフィック パターンやネットワーク全体のトラフィック パターンを視覚化し（集約トラフィックまたはアプリケーションベースのビューの場合）、予防的な問題の検出、効率的なトラブルシューティング、迅速な問題解決を実現します。
- アプリケーションのモニタリングとプロファイリング。NetFlow のデータを利用すると、ネットワーク マネージャはネットワーク全体における、アプリケーション使用状況を時間ベースで詳細に調べることができます。この情報は、新しいサービスを計画および理解し、ネットワーク リソースおよびアプリケーション リソースを割り当て（たとえば、Web サーバのサイズ設定と VoIP の配置）、顧客の要求を迅速に満たすために使用されます。
- ユーザのモニタリングとプロファイリング。ネットワーク エンジニアは NetFlow データを使用すると、顧客やユーザによるネットワーク リソースおよびアプリケーション リソースの利用について詳しく理解できます。この情報を使用して、潜在的なセキュリティやポリシーの違反を検出して解決するために、アクセス、バックボーン、アプリケーション リソースを効率的に計画して割り当てることができます。
- ネットワーク プランニング。NetFlow を使用すると、長期間にわたってデータをキャプチャすることによって、ネットワークの成長を追跡して予測し、ルーティング デバイス、ポート、および高帯域幅のインターフェイスの数を増やすためのアップグレードを計画する機会が得られます。NetFlow サービス データによって、ピアリング、バックボーンのアップグレード、ルーティング ポリシーのネットワーク計画を最適化できます。NetFlow はネットワークのパフォーマンス、容量、および信頼性を最大化すると同時に、ネットワーク運用の総コストを最小限に抑えるために役

立ちます。NetFlow により、望ましくない WAN トラフィックが検出され、帯域幅と Quality of Service（QoS）が検証され、新しいネットワーク アプリケーションの分析が可能になります。NetFlow からは、ネットワークの運用コストを削減するための有用な情報が得られます。

- セキュリティの分析。NetFlow では、distributed Denial of Service（dDoS; 分散 DoS）攻撃、ウイルス、およびワームをリアルタイムで識別して分類します。ネットワークの動作が変化すると、Flexible NetFlow データに明らかな異常が表れます。このデータは、セキュリティ侵害の過程を調べ、再現するための貴重な科学捜査上のツールでもあります。
- 課金とアカウンティング。NetFlow データを使用すると細かい設定が可能な計測（たとえば、IP アドレス、パケット数やバイト数、タイム スタンプ、Type of Service（ToS; タイプ オブ サービス）、アプリケーション ポートなどの詳細を含むフロー データ）ができるため、非常に柔軟かつ詳細なリソース使用率のアカウンティングを実現できます。サービス プロバイダーは、時刻、帯域幅の使用率、アプリケーションの使用率、Quality of Service などに基づく課金のためにこの情報を使用できます。企業のお客様は、リソースの使用率に応じた部門別のチャージバックやコスト割り当てに、これらの情報を利用することがあります。
- NetFlow データのウェアハウジングとデータ マイニング。NetFlow データ（または派生したデータ）は後で予防的なマーケティングや顧客サービス プログラム（たとえば、社内または社外のユーザによって使用されるアプリケーションおよびサービスの検出や、向上したサービス、アドバタイジングなどのためのターゲット設定）のサポートのために取得および分析できるようにウェアハウジングできます。さらに、市場調査員は Flexible NetFlow データを使用して、エンタープライズおよびサービス プロバイダーに関する「誰が」、「どの」、「どこで」、「どのくらいの期間」という情報にアクセスできます。

以前の NetFlow および Flexible NetFlow でのフローの使用

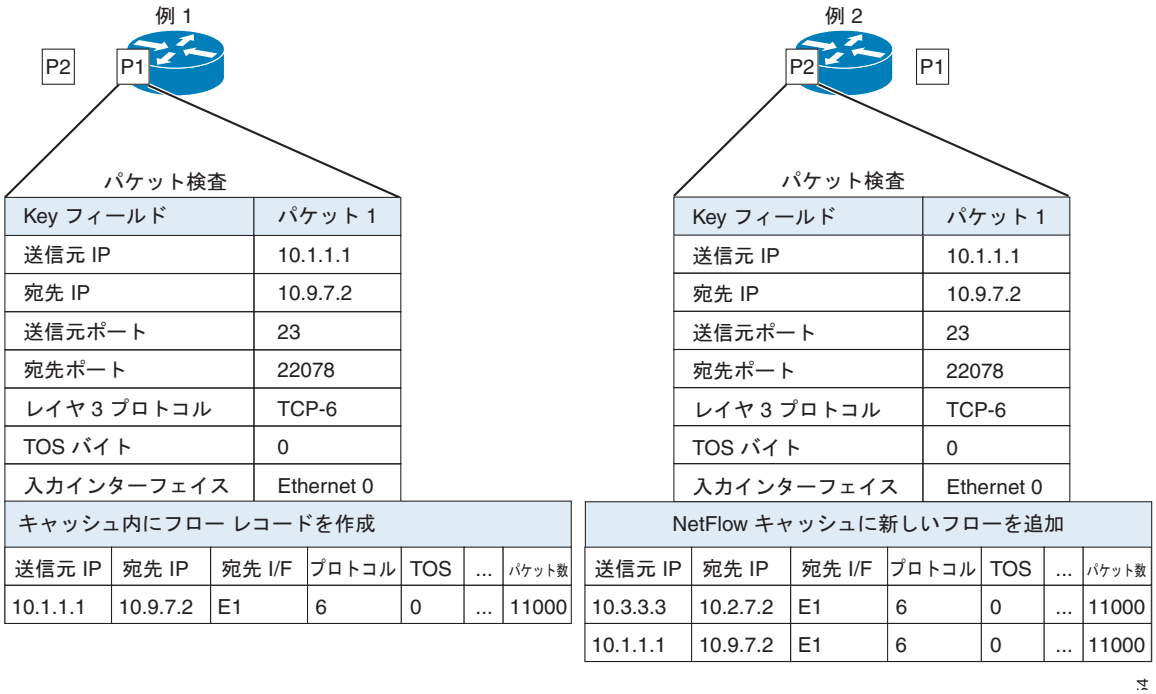
以前の NetFlow および Flexible NetFlow の両方でフローの概念を使用します。*フロー*は、特定の送信元と特定の宛先の間のパケットのストリームとして定義します。

以前の NetFlow および Flexible NetFlow の両方で、ネットワーク トラフィックの監視中にキャッシュ内にいつ新しいフローを作成する必要があるかを判断するための条件として、IP データグラムの key フィールドの値（IP 送信元アドレスまたは宛先アドレスおよび送信元または宛先のトランスポート プロトコル ポートなど）を使用します。データグラムの key フィールドのデータの値が既存のフローに関して一意である場合、新しいフローが作成されます。

以前の NetFlow および Flexible NetFlow の両方で、フローからキャプチャされるデータのフィールドを識別するための条件として、nonkey フィールドを使用します。フローには、nonkey フィールドの値からキャプチャされたデータが格納されます。

図 1 に、パケット インスペクションと、キャッシュ内のフロー レコードの作成のためのプロセスの例を示します。この例では、送信元と宛先の IP アドレスの key フィールドに異なる値があるため、2 つの固有のフローが作成されます。

図 1　パケットの検査



以前の NetFlow と Flexible NetFlow

以前の NetFlow は、フローの判定に固定 7 タプルの IP 情報を使用していました。Flexible NetFlow ではフローをユーザが定義できます。次に、Flexible NetFlow の利点を示します。

- スケーラビリティ、フロー情報の集約などの、大容量フロー認識。
- セキュリティの監視と dDoS の検出および識別のための拡張されたフロー インフラストラクチャ。
- フロー情報をネットワーク内の特定のサービスまたはオペレーションに適応させるパケットからの新しい情報。利用できるフロー情報は、Flexible NetFlow ユーザがカスタマイズ可能。
- Cisco の柔軟で拡張可能な NetFlow Version 9 エクスポート フォーマットの活用。
- IP アカウンティング、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ポリシー アカウンティング、永続的キャッシュなどの多数のアカウンティング機能を置換するために使用できる包括的な IP アカウンティング機能。

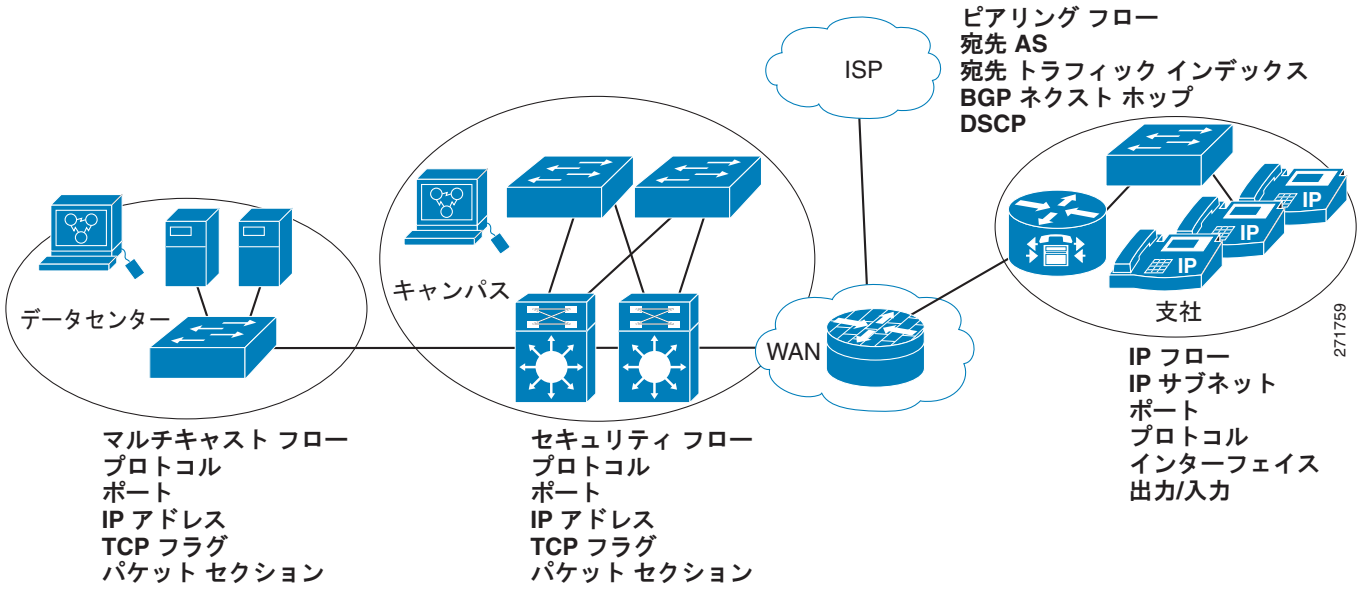
以前の NetFlow では、ネットワーク内のアクティビティを理解して、ネットワーク設計を最適化し、稼動コストを削減できます。Flexible NetFlow では、ネットワークの動作を、ネットワーク内で使用されるさまざまなサービスに合わせた特定のフロー情報とともに、より効率的に理解できます。次に、Flexible NetFlow 機能用の適用例を示します。

- Flexible NetFlow は Cisco NetFlow をセキュリティ監視ツールとして拡張します。たとえば、ユーザがネットワーク内で特定のタイプの攻撃を検索できるように、パケット長や MAC アドレスのために新しいフロー キーを定義することができます。
- Flexible NetFlow を使用すると、TCP アプリケーションまたは UDP アプリケーションをパケット内のサービス クラス（CoS）ごとに明確に追跡することによって、ホスト間で送信されるアプリケーション トラフィックの量を迅速に識別できます。

- サービス クラスごとに各ネクスト ホップの IP コア ネットワークおよびその宛先を入力するトラフィックのアカウンティング。この機能では、エッジ間のトラフィック マトリックスを構築できます。

図 2 に、Flexible NetFlow をネットワークに導入する方法の例を示します。

図 2　Flexible NetFlow の代表的な導入



Flexible NetFlow のコンポーネント

Flexible NetFlow は、いくつかのバリエーションで一緒に使用して、トラフィック分析およびデータ エクスポートに使用できるコンポーネントで構成されます。Flexible NetFlow のユーザ定義のフロー レコードおよびコンポーネントの構造では、最小限の数のコンフィギュレーション コマンドで、ネットワーキング デバイスでのトラフィック分析およびデータ エクスポートのためのさまざまなコンフィギュレーションの作成が容易になります。各フロー モニタに、フロー レコード、フロー エクスポータ、およびキャッシュ タイプの固有の組み合わせを設定できます。フロー エクスポータの宛先 IP アドレスなどのパラメータを変更する場合、フロー エクスポータを使用するすべてのフロー モニタに対して自動的に変更されます。同じフロー モニタを複数のフロー サンプラと組み合わると、さまざまなインターフェイス上でさまざまな速度の同じタイプのネットワーク トラフィックをサンプリングできます。ここでは、Flexible NetFlow コンポーネントのその他の情報を提供します。

- 「レコード」（P.6）
- 「フロー モニタ」（P.7）
- 「フロー エクスポータ」（P.9）
- 「フロー サンプラ」（P.11）

レコード

Flexible NetFlow では、key フィールドと nonkey フィールドの組み合わせが *レコード*と呼ばれます。Flexible NetFlow のレコードは Flexible NetFlow フロー モニタに割り当てられ、フロー データの格納に使用されるキャッシュが定義されます。Flexible NetFlow には、Flexible NetFlow の使用を開始する際に役立ついくつかの事前定義済みのレコードが含まれています。Flexible NetFlow の機能を完全に利用するには、次の項で説明するように、カスタマイズした独自のレコードを作成する必要があります。

- 「NetFlow の事前定義済みのレコード」（P.6）
- 「ユーザ定義レコード」（P.6）

NetFlow の事前定義済みのレコード

Flexible NetFlow には事前定義済みのレコードがいくつか含まれ、それを使用してネットワーク トラフィックの監視を開始できます。事前定義済みのレコードは、Flexible NetFlow を迅速に導入するために役立ち、ユーザ定義のフロー レコードよりも簡単に使用できます。ネットワーク モニタリングのニーズを満たす定義済みのレコードのリストから選択できます。Flexible NetFlow が改良されると、一般的なユーザ定義のフロー レコードを事前定義済みレコードとして使用でき、簡単に導入できるようになります。

事前定義済みレコードにより、エクスポートされるデータのために既存の NetFlow コレクタ コンフィギュレーションとの下位互換性が確保されます。事前定義済みレコードは、それぞれ固有の key および nonkey フィールドの組み合せを持ち、ルータで Flexible NetFlow をカスタマイズしなくても、ネットワーク内のさまざまなタイプのトラフィックを監視する、内蔵機能を提供します。

2 つの事前定義済みレコード（以前の NetFlow と以前の NetFlow の IPv4 出力）は機能的には同等で、以前の（入力）NetFlow の機能および出力 NetFlow アカウンティング機能をそれぞれエミュレートします。その他の Flexible NetFlow の事前定義済みレコードのいくつかは、以前の NetFlow で利用できる集約キャッシュ方式に基づきます。以前の NetFlow で利用できる集約キャッシュ方式に基づく Flexible NetFlow の事前定義済みレコードでは、集約を実行しません。代わりに、事前定義済みレコードによって各フローが個別に追跡されます。

Flexible NetFlow の事前定義済みレコードの詳細については、「Getting Started with Configuring Cisco IOS XE Flexible NetFlow」モジュールまたは「Configuring Cisco IOS XE Flexible NetFlow with Predefined Records」モジュールを参照してください。

ユーザ定義レコード

Flexible NetFlow では、key および nonkey フィールドを指定し、実際の要件に合わせてデータ収集をカスタマイズすることで、Flexible NetFlow フロー モニタ キャッシュ用の独自のレコードを定義できます。Flexible NetFlow フロー モニタ キャッシュに対して独自のレコードを定義する場合、*ユーザ定義レコード*と呼ばれます。nonkey フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。nonkey フィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、nonkey フィールドの値はフロー内の最初のパケットからのみ取得されます。Flexible NetFlow を使用すると、nonkey フィールドとして、フロー内のバイト数やパケット数などのカウンター値をキャプチャできます。

QoS や帯域幅の監視、アプリケーションおよびエンド ユーザのトラフィック プロファイリング、サービス拒絶（DoS）攻撃のセキュリティ監視などの用途のためにユーザ定義レコードを作成できます。また、Flexible NetFlow には以前の NetFlow をエミュレートするいくつかの事前定義済みレコードも含まれています。

Flexible NetFlow のユーザ定義レコードでは、ユーザが設定可能なサイズのパケットの連続するセクションを監視する機能を利用でき、key フィールドまたは nonkey フィールドとしてパケットのその他のフィールドや属性とともにフロー レコード内で使用します。セクションにはパケットのレイヤ 3 データが含まれる場合があります。

パケットのセクション フィールドでは、ユーザが Flexible NetFlow の事前定義済みレコードの対象外のパケット フィールドを監視できます。事前定義済みキーで収集されないパケット フィールドの分析機能によって、さらに詳細なトラフィック モニタリングが可能になるため、分散型 DoS 攻撃の調査に役立ち、URL モニタリングなど他のセキュリティ アプリケーションの実装が可能になります。

Flexible NetFlow では、事前定義済みタイプのユーザが設定可能なサイズのパケット セクションが提供されます。次の Flexible NetFlow コマンド（Flexible NetFlow フロー レコード コンフィギュレーション モードで使用される）をパケット セクションの事前定義済みタイプの設定に使用できます。

- **collect ipv4 section header size** *bytes*：各パケットの IPv4 ヘッダーの先頭から、*bytes* 引数で指定されたバイト数のキャプチャを開始します。
- **collect ipv4 section payload size** *bytes*：各パケットの IPv4 ヘッダーの直後からバイトのキャプチャを開始します。キャプチャされるバイト数は *bytes* 引数で指定されます。

bytes 値は、フロー レコードのこれらのフィールドのサイズ（バイト単位）です。対応するパケットのフラグメントが要求されたセクション サイズより小さい場合、Flexible NetFlow ではフロー レコード内の残りのセクション フィールドに 0 が挿入されます。パケット タイプが要求されたセクション タイプと一致しなかった場合、Flexible NetFlow はフロー レコード内のセクション フィールド全体を 0 で埋めます。

Flexible NetFlow では、ヘッダーおよびパケット セクションのタイプに新しいバージョン 9 エクスポート フォーマット フィールド タイプが追加されます。Flexible NetFlow は NetFlow コレクタに、対応するバージョン 9 エクスポート テンプレート フィールドで設定されたセクション サイズを通知します。ペイロード セクションには、対応する長さフィールドがあり、収集されるセクションの実際のサイズを収集するために使用できます。

フロー モニタ

フロー モニタは Flexible NetFlow のネットワーク トラフィックの監視を実行するコンポーネントで、インターフェイスに適用されます。フロー モニタは、ユーザ定義のレコードまたは事前定義済みレコード、オプションのフロー エクスポータ、およびフロー モニタが最初のインターフェイスに適用されるときに自動的に作成されるキャッシュで構成されます。フロー データはネットワーク トラフィックから収集され、フロー レコードの key フィールドおよび nonkey フィールドに基づいて監視プロセス中にフロー モニタ キャッシュに追加されます。

Flexible NetFlow は、同じトラフィックのさまざまなタイプの分析を実行するために使用できます。図 3 では、入力インターフェイス上の標準トラフィック分析のために設計されたレコードと、出力インターフェイス上のセキュリティ分析のために設計されたレコードを使用してパケット 1 が分析されます。

図 3　　2 つのフロー モニタを使用した同じトラフィックの分析例

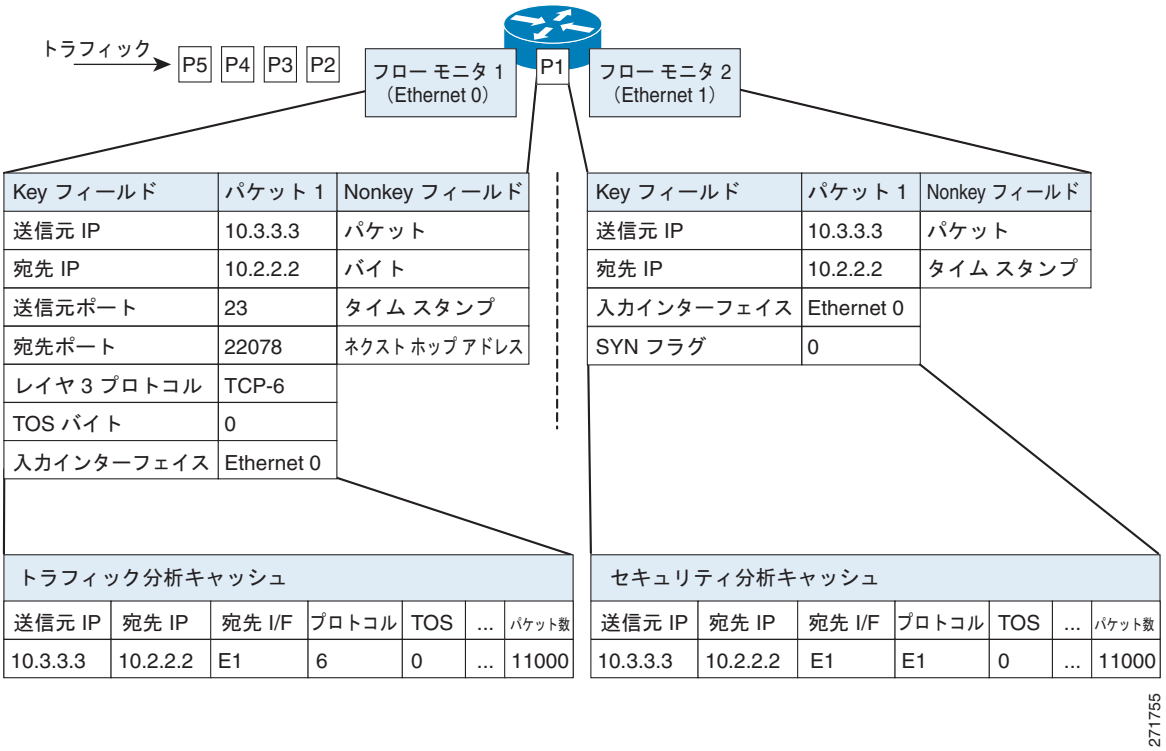
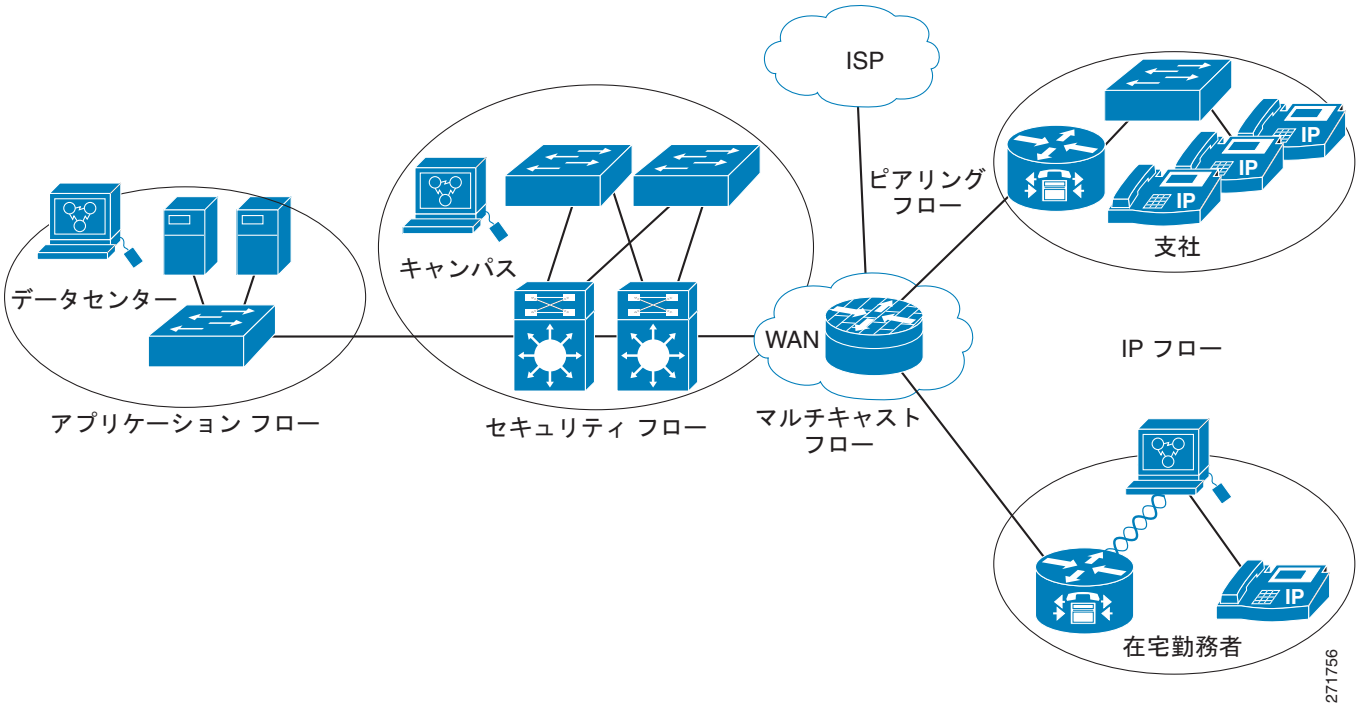


図 4 に、カスタム レコードを使用して複数のタイプのフロー モニタを適用するより複雑な方法の例を示します。

図 4　　カスタム レコードでの複数のタイプのフロー モニタの複雑な使用例



Normal

デフォルトのキャッシュ タイプは「normal」です。このモードでは、キャッシュ内のエントリが timeout active 設定と timeout inactive 設定に従って期限切れになります。キャッシュ エントリは、期限切れになるとキャッシュから削除され、設定されている何らかのエクスポータによってエクスポートされます。

フロー エクスポータ

フロー エクスポータでは、フロー モニタ キャッシュ内のデータをリモート システム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。フロー エクスポータは、コンフィギュレーションで別のエンティティとして作成されます。フロー エクスポータは、フロー モニタにデータ エクスポート機能を提供するためにフロー モニタに割り当てられます。複数のフロー エクスポータを作成して、1 つまたは複数のフロー モニタに適用すると、いくつかのエクスポート先を指定することができます。1 つのフロー エクスポータを作成し、いくつかのフロー モニタに適用することができます。

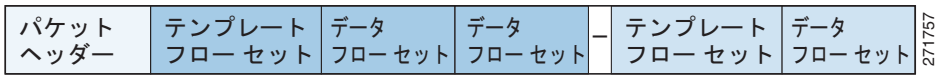
NetFlow データ エクスポート フォーマットのバージョン 9

NetFlow の基本出力はフロー レコードです。NetFlow が改良され、フロー レコードのいくつかのフォーマットが向上しました。NetFlow エクスポート フォーマットの最新の進化は、バージョン 9 と呼ばれます。NetFlow Version 9 エクスポート フォーマットの識別機能は、テンプレートがベースとなります。テンプレートにより、レコード フォーマットに対する拡張性の高い設計が可能になり、基本のフローレコード フォーマットを同時に変更しなくても NetFlow サービスを将来拡張できる機能が提供されます。テンプレートを使用すると、次のいくつかの利点があります。

- NetFlow のコレクタを提供したり、サービスを表示したりするアプリケーションを作成するサードパーティ ビジネス パートナーは、新規の NetFlow 機能が追加されるたびにアプリケーションを再コンパイルする必要はありません。代わりに、既知のテンプレート フォーマットを記述する外部のデータ ファイルを使用することができます。
- 新規機能は、現在の導入環境を損ねることなく、NetFlow に迅速に追加できます。
- バージョン 9 フォーマットは新しいプロトコルや開発中のプロトコルに適応できるため、NetFlow はこれらのプロトコルに対して「将来的に対応」します。

バージョン 9 のエクスポート フォーマットは、パケット ヘッダーとそれに続く 1 つ以上のテンプレート フロー セットまたはデータ フロー セットで構成されています。テンプレート フロー セットでは、将来のデータ フロー セットに表示されるフィールドの説明が提供されます。このようなデータ フロー セットは、後で同じエクスポート パケットまたは後続のエクスポート パケットで発生する可能性があります。テンプレート フロー セットおよびデータ フロー セットは、図 5 に示すように、1 つのエクスポート パケット内で混在できます。

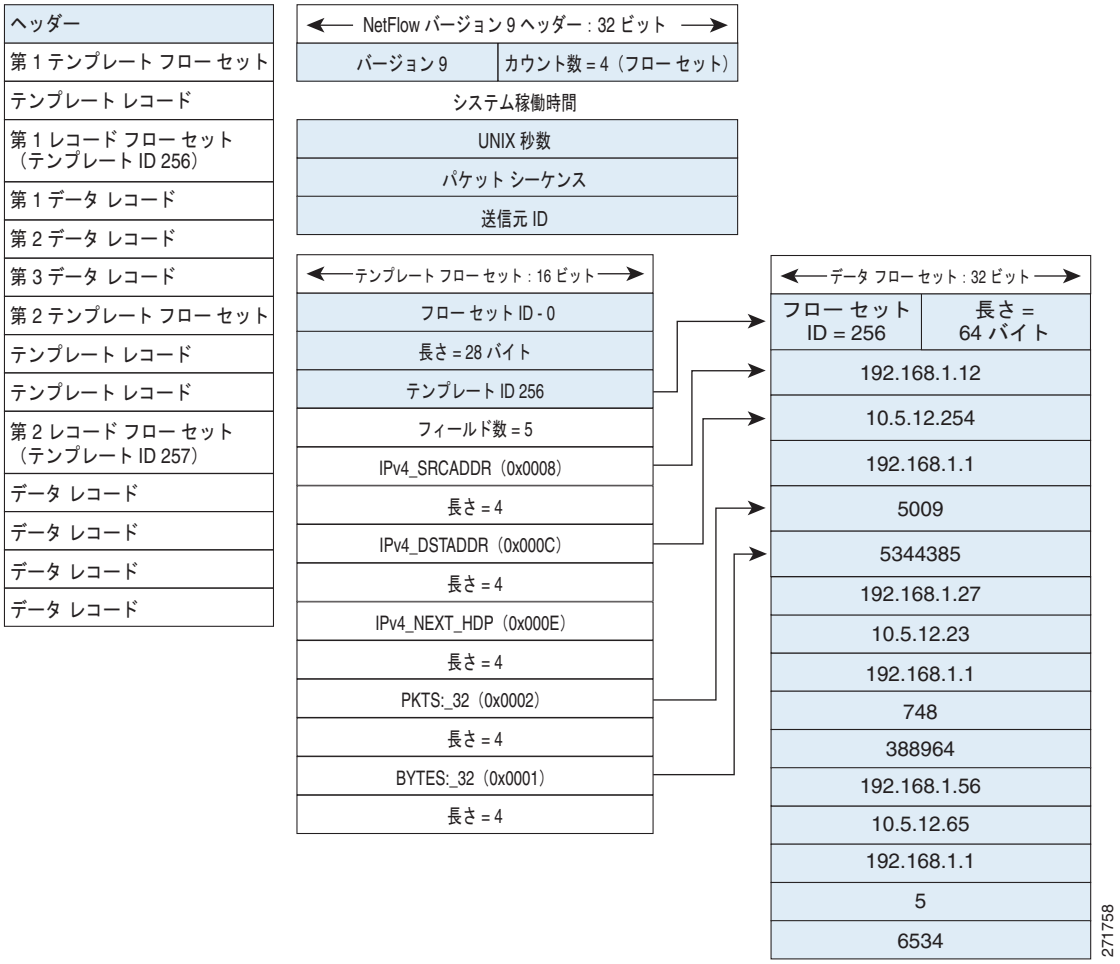
図 5　　バージョン 9 エクスポート パケット



NetFlow Version 9 では、送信されるデータを NetFlow コレクタが理解できるように、テンプレート データを定期的にエクスポートします。また、テンプレートのデータ フロー セットもエクスポートします。Flexible NetFlow の主な利点は、ユーザがフロー レコードを設定すると、バージョン 9 テンプレートに効率的に変換され、コレクタに転送されることです。図 6 に、ヘッダー、テンプレート フロー セットおよびデータ フロー セットを含めて、NetFlow Version 9 エクスポート フォーマットの詳細な例を示します。

（注） NetFlow Version 5 エクスポート フォーマットは、Flexible NetFlow データに対して制限された情報を提供する固定エクスポート フォーマットです。これが Flexible NetFlow でバージョン 9 エクスポート フォーマットが使用される理由です。

図 6　NetFlow Version 9 エクスポート フォーマットの詳細例



バージョン 9 エクスポート フォーマットの詳細については、ホワイト ペーパー『*Cisco IOS NetFlow Version 9 Flow-Record Format*』を参照してください。次の URL から入手できます。
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml

フロー サンプラ

フロー サンプラは分析されるパケット数を制限し、Flexible NetFlow によってトラフィックを監視するためにネットワーク デバイスで生じる負荷を軽減するために使用されます。サンプリングは確定的に行うことも、ランダムに行うこともできます。2 ～ 32,768 パケットの範囲から 1 パケットの割合でサンプリング レートを設定できます。たとえば、サンプリングレートを 2 分の 1 にすると、50% のパケットがネットワーク デバイスでの分析で処理されます。

フロー サンプラは、Flexible NetFlow フロー サンプリングを実装するためにフロー モニタとともにインターフェイスに適用されます。パケットはサンプラによって指定されたレートで分析され、フロー モニタに関連付けられたフロー レコードと比較されます。分析されるパケットがフロー レコードによって指定された条件を満たす場合、フロー モニタ キャッシュに追加されます。

Flexible NetFlow でのセキュリティ監視

Flexible NetFlow をネットワーク攻撃検出ツールとして IP ヘッダーのすべての部分および均等なパケット セクションを追跡する機能とともに使用して、この情報をフローに特徴付けることができます。セキュリティ監視システムでは Flexible NetFlow データを分析でき、ネットワーク上の問題を見つけた場合に、特定の情報を追跡して攻撃パターンまたはワーム伝播の詳細を識別するように設定される仮想バケットまたは仮想キャッシュを作成できます。特定の情報を入力フィルタリング（たとえば、特定の宛先へのすべてのフローのフィルタリング）と組み合わせて動的にキャッシュを作成する機能を備えた Flexible NetFlow は、強度なセキュリティ監視ツールです。

宛先サーバへのオープンな TCP 要求をフラッディングする（たとえば、SYN フラッド攻撃）ために TCP フラグが使用される場合、1 つの共通タイプの攻撃が発生します。攻撃デバイスは TCP SYN のストリームを特定の宛先アドレスに送信しますが、TCP スリーウェイ ハンドシェイクの一部として、サーバ SYN-ACK に応答して ACK を送信することはありません。セキュリティ検出サーバに必要なフロー情報では、宛先のアドレスまたはサブセット、TCP フラグ、パケット数などの 3 つの key フィールドの追跡が要求されます。セキュリティ検出サーバでは一般的な Flexible NetFlow 情報が監視され、このデータによって、Flexible NetFlow でルータのコンフィギュレーションに新しいフローを動的に作成することで、この特定の攻撃の詳細ビューがトリガーされます。新しいフロー モニタには Flexible NetFlow キャッシュに表示されるトラフィックを制限するための入力フィルタリングと、TCP ベースの攻撃を診断するための特定の情報の追跡が含まれます。この場合、ユーザはサーバの宛先アドレスまたはサブネットへのすべてのフロー情報をフィルタリングして、セキュリティ検出サーバでの評価のために必要な情報量を制限できます。セキュリティ検出サーバでこの攻撃を理解したと判断された場合、別のフロー モニタをプログラミングして、パケット内の署名を詳細に確認するペイロード情報またはパケットのセクションを収集してエクスポートします。この例は、Flexible NetFlow をセキュリティ インシデントの検出に使用できる多数の方法の 1 つにすぎません。

以前の NetFlow と Flexible NetFlow の機能の比較

表 1 では、以前の NetFlow と Flexible NetFlow の機能ごとの比較を示します。

表 1　以前の NetFlow と Flexible NetFlow の機能ごとの比較

機能	Original NetFlow	Flexible NetFlow	説明
NetFlow データ キャプチャ	サポートされる	サポートされる	データ キャプチャは Flexible NetFlow の事前定義済みレコードおよびユーザ定義レコードで使用できます。Flexible NetFlow には、以前の NetFlow のトラフィック分析機能をエミュレートするいくつかの事前定義済みキーがあります。
NetFlow データ エクスポート	サポートされる	サポートされる	フロー エクスポータは Flexible NetFlow フロー モニタ キャッシュからリモート システムにデータをエクスポートします。
NetFlow BGP ネクストホップ サポート	サポートされる	サポートされる	Flexible NetFlow レコードの事前定義済みキーおよびユーザ定義キーで使用できます。
ランダム パケット サンプリング NetFlow	サポートされる	サポートされる	Flexible NetFlow サンプリングで使用できます。

表 1　以前の NetFlow と Flexible NetFlow の機能ごとの比較（続き）

機能	Original NetFlow	Flexible NetFlow	説明
NetFlow v9 エクスポート フォーマット	サポートされる	サポートされる	Flexible NetFlow エクスポータで使用できます。
NetFlow サブインターフェイス サポート	サポートされる	サポートされる	Flexible NetFlow モニタはサブインターフェイスに割り当てることができます。
NetFlow 複数エクスポート先	サポートされる	サポートされる	Flexible NetFlow エクスポータで使用できます。
NetFlow ToS ベース ルータ集約	サポートされる	サポートされる	Flexible NetFlow レコードの事前定義済みレコードおよびユーザ定義レコードで使用できます。
NetFlow ルータベース集約の最小プレフィクス マスク	サポートされる	サポートされる	事前定義済みレコードおよびユーザ定義レコードで使用できます。
NetFlow 入力フィルタ	サポートされる	サポートなし	—
NetFlow MIB	サポートされる	サポートなし	—
出力 NetFlow アカウンティング	サポートされる	サポートされる	Flexible NetFlow モニタを使用すると、インターフェイスおよびサブネット上の出力トラフィックを監視できます。

関連情報

以前の NetFlow トラフィック分析およびデータ エクスポートをエミュレートする Flexible NetFlow の基本コンフィギュレーションを実装するには、「Getting Started with Configuring Cisco IOS XE Flexible NetFlow」モジュールを参照してください。その他の Flexible NetFlow コンフィギュレーションを実装するには、「関連資料」（P.14）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」
ネットワークでの Flexible NetFlow のカスタマイズ	「Customizing Cisco IOS XE 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 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*』

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