(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-193628
(P2008-193628A)
(43)公開日　平成20年8月21日(2008.8.21)

(51)Int.Cl.	F I		テーマコード（参考）
H04L 12/56 (2006.01)	H04L	12/56　400Z	5K030

審査請求 有　請求項の数 7　ＯＬ　（全 13 頁）

(21)出願番号　特願2007-28730(P2007-28730)
(22)出願日　平成19年2月8日(2007.2.8)

（特許庁注：以下のものは登録商標）
１．ＥＴＨＥＲＮＥＴ

（出願人による申告）国等の委託研究の成果に係わる特許出願（平成１８年度、総務省、「次世代バックボーンに関する研究開発」、産業活力再生特別措置法３０条の適用を受けるもの）

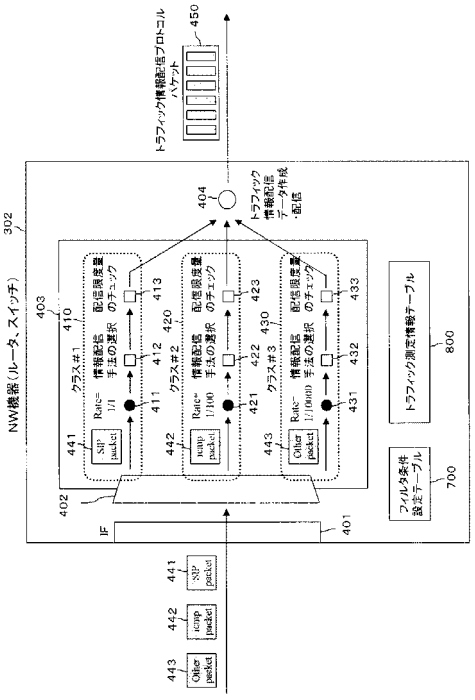
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100083552
弁理士　秋田　収喜
(74)代理人　100103746
弁理士　近野　恵一
(74)代理人　100119703
弁理士　井上　雅夫
(72)発明者　小林　淳史
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5K030 GA13 GA14 GA15 HA08 HD03 JA10 KA05 LC11 MA04 MB09 MC07 MC08

(54)【発明の名称】トラフィック情報の配信及び収集方法

(57)【要約】
【課題】クラスに応じて抽出するパケット長や配信方法を変更可能とすることで、より効率的なトラフィックの配信を可能とする。
【解決手段】NW機器３０２は、分類手段４０２とクラス別処理手段４０３とトラフィック情報配信データ作成配信手段４０４とを有する。分類手段４０２が、受信したパケットを各クラスに分類する。クラス別処理手段４０３が、各クラスに定められたトラフィック情報の配信手法に基づいて、パケットの一部を抽出するパケット抽出手法又はフローを集約するフロー集約手法のいずれかの配信手法を選択する。トラフィック情報配信データ作成配信手段４０４が、クラス別処理手段４０３で選択された配信手法による各トラフィック情報により構成されたトラフィック情報配信プロトコルパケット４５０を作成し、トラフィック情報収集機器に配信する。また、クラス別処理手段４０３は各クラス毎にサンプリングや配信限度量のチェックも行う。
【選択図】図４

図4



【特許請求の範囲】
【請求項１】
トラフィック情報をトラフィック情報収集機器に配信するトラフィック情報配信機器におけるトラフィック情報配信方法であって、
前記トラフィック情報配信機器は、分類手段とクラス別処理手段とトラフィック情報配信データ作成配信手段とを有し、
前記分類手段が、受信したパケットを各クラスに分類し、
前記クラス別処理手段が、前記分類手段により各クラスに分類されたパケットに対して、各クラスに定められたトラフィック情報の配信手法に基づいて、パケットの一部を抽出するパケット抽出手法又はフローを集約するフロー集約手法のいずれかの配信手法を選択し、
前記トラフィック情報配信データ作成配信手段が、前記クラス別処理手段で選択された配信手法による各トラフィック情報により構成されたトラフィック情報配信パケットを作成し、該トラフィック情報配信パケットを前記トラフィック情報収集機器に配信する
ことを特徴とするトラフィック情報配信方法。
【請求項２】
請求項１に記載のトラフィック情報配信方法であって、
前記クラス別処理手段が、前記分類手段により各クラスに分類されたパケットに対して、各クラスに定められた配信限度量に基づいて、限度量が超過している場合には、当該トラフィック情報の配信を停止し、限度量を下回った際に、当該トラフィック情報の配信を開始することを特徴とするトラフィック情報配信方法。
【請求項３】
請求項１又は２に記載のトラフィック情報配信方法であって、
前記クラス別処理手段が、前記分類手段により各クラスに分類されたパケットに対して、各クラスに定められたサンプリングレート及び／又はサンプリングアルゴリズムに基づいてパケットサンプリングを行うことを特徴とするトラフィック情報配信方法。
【請求項４】
請求項１ないし３のいずれか１項に記載のトラフィック情報配信方法であって、
前記トラフィック情報配信機器はフィルタ条件設定テーブルを有し、
前記フィルタ条件設定テーブルは、パケットのヘッダに関わる情報である宛先アドレス、送信元アドレス、プロトコル、宛先ポート番号、送信元ポート番号、ＴＣＰフラグ、ＴＯＳ、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、ラベル、ＩＰバージョン、パケットＬｅｎｇｔｈ、および、ＮＷ機器が当該パケットをルーティングするための特性情報である受信ＩＦ情報、送信先ＩＦ情報、Ｎｅｘｔ－ＨｏｐアドレスＢＧＰ　Ｎｅｘｔ－Ｈｏｐアドレス、ＰｅｅｒｉｎｇＡＳ番号、ＯｒｉｇｉｎＡＳ番号、ＢＧＰ　Ｃｏｍｍｕｎｉｔｙのうちの１以上に対応してフィルタ条件識別子とクラス識別子が設定されたものであり、
前記分類手段が、前記フィルタ条件設定テーブルに基づいて、受信したパケットを各クラスに分類する
ことを特徴とするトラフィック情報配信方法。
【請求項５】
請求項４に記載のトラフィック情報配信方法であって、
前記トラフィック情報配信機器はトラフィック測定情報テーブルを有し、
前記トラフィック測定情報テーブルは、前記クラス識別子に対応して、トラフィック配信方法、サンプリングレート、サンプリングアルゴリズム、配信量の限度量の１以上が設定されたものであり、
前記クラス別処理手段が、前記トラフィック測定情報テーブルに基づいて、クラス別の処理を行う
ことを特徴とするトラフィック情報配信方法。
【請求項６】

請求項５に記載のトラフィック情報配信方法であって、
前記トラフィック情報配信データ作成配信手段が、前記トラフィック情報配信パケットの各トラフィック情報に、前記フィルタ条件識別子及び／又は前記クラス識別子を付加することを特徴とするトラフィック情報配信方法。
【請求項７】
請求項６に記載のトラフィック情報配信方法によってトラフィック情報の配信を行う前記トラフィック情報配信機器から、トラフィック情報を収集するトラフィック情報収集機器におけるトラフィック情報収集方法であって、
前記トラフィック情報収集機器が、前記トラフィック情報配信機器から収集した各トラフィック情報に付加されたクラス識別子及び／又はフィルタ条件識別子をもとに、トラフィック分析装置群の中から適切なトラフィック分析装置に対して、トラフィック情報を振り分けることを特徴とするトラフィック情報収集方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、インターネットに代表されるネットワーク上を流れるトラフィックをモニタする際に、大容量化したネットワーク上のトラフィックを効率的にモニタする手法に関し、特に、トラフィック情報の配信及び収集方法に関する。
【背景技術】
【０００２】
大規模、大容量化したネットワークでは、膨大なトラフィックを全てモニタすることができない。そのため、パケットをサンプリングすることにより、全体のトラフィック量を推定する手法が採用されている。この場合、トラフィック量の大容量化に応じて、サンプリングレートを小さくする必要性があるが、トラフィック量が小さい異常トラフィックについては、検出不可能となることも考えられ、効率的なトラフィック・モニタ手法が必要とされている。
【０００３】
従来のフロー統計配信プロトコル（ｓＦｌｏｗ（非特許文献２参照），ＮｅｔＦｌｏｗ（非特許文献１参照））は、ＮＷ機器（Network機器）のＩＦ（Interface）上で受信する全てのパケットを対象にサンプリングが行われている。また、フロー統計配信プロトコルのひとつであるＩＰＦＩＸプロトコル（非特許文献３参照）では、フィルタ条件とサンプリングを組み合わせることでより柔軟なトラフィック測定を可能としているが、情報の配信方法については、一律同じ方式が適用される。このため、あるアプリケーションの分析により、より詳細なトラフィック情報の配信が必要な場合には、そのほかのトラフィックについてもより詳細なトラフィック情報の配信が必要となり、全体の情報転送量が大きくなるという問題がある。
【０００４】
このような状況の中で、より柔軟にトラフィックを抽出する手法として、一次的に異常と検知されたトラフィックを抽出して、大容量のトラフィックから埋もれないようにする機能や、フロー条件をもとにより柔軟にフロー統計を実施する機能が考案されている（特許文献１参照）。
【０００５】
しかし、サンプリングの前に特定のパケットをフィルタリングすることやサンプリング前にパケットを分類する案などは考案されているが、分類されたクラス単位にトラフィックの配信方法まで設定可能とするような機能は、現状存在しない。また、クラス化された際に、特定のクラスにトラフィックが集中することで、他のクラスのトラフィック情報が配信されなくなるという問題も解決されていない。
【０００６】
【特許文献１】特開２００６－１６４０３８号公報、「ＤｏＳ攻撃あるいはＤＤｏＳ攻撃に対処する方法、ネットワーク装置、および分析装置」、日本電信電話株式会社

【非特許文献１】RFC3954,“Cisco Systems NetFlow Services Export Version9”, October 2004
【非特許文献２】RFC3176,“InMon Corporation's sFlow:A Method for Monitoring Traffic in Switched and Routed Networks”, September 2001
【非特許文献３】draft-ietf-ipfix-Protocol-24.txt,“Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information”, November 2006
【発明の開示】
【発明が解決しようとする課題】
【０００７】
ＤＤｏＳ攻撃トラフィックなどの異常トラフィックを検知する目的から、ネットワーク上に流れているトラフィックをモニタするフロー統計配信プロトコル（ｓＦｌｏｗ，ｎｅｔＦｌｏｗ，ＩＰＦＩＸ）に注目が集まっている。しかし、ネットワーク上に流れるトラフィック量は、年々増加傾向にあり、トラフィックをモニタする手法もサンプリング間隔を上げるだけでは、複雑化するトラフィックの傾向を把握することが困難となっている。
【０００８】
近年、ＮＷ機器が実装するフィルタ機能（アクセスリスト機能）を用いることで、トラフィックを選択し、サンプリングを行うことによって、大容量のトラフィックの中から抽出したいパケットのみに絞り込み、サンプリングレートを大きくすることによって、特定パケットに注力して監視する機能が提案されている（特許文献１、非特許文献３）。この機能は、フィルタリングにより分類したクラス単位にサンプリングレートを設定することが示されているが、ボットネットなどに代表される不正トラフィックは、より巧妙となっており、サンプリングレートを大きくして、ボリュームベースで異常を検知することは難しい状況となっている。
【０００９】
近年の不正トラフィックについては、パケットのアプリケーション（ペイロード）部分まで分析をしないと異常を検知できないといった問題があり、年々トラフィックが増加していく中で、トラフィック抽出手法のスケーラビリティを維持しつつ、重要なトラフィックに対してアプリケーション部分の情報をどう抽出していくのかが課題となっている。
【００１０】
現在、パケットのフィルタリング処理、サンプリング処理、パケットのコピー、フロー集約情報のカウンタ処理等は、ハードウェア化されているため、より高速化されている。しかし、トラフィック情報配信プロトコルのパケット作成処理などは、ＮＷ機器（ルータ、スイッチ等）のメインＣＰＵのソフトウェア上で実行される場合が多く、配信処理のボトルネックとなっている場合が多い。図１は、配信するパケット情報の切り出しサイズを２５６ｂｙｔｅとした場合（図１の△参照）と６４ｂｙｔｅとした場合（図１の◆参照）のルータの負荷状況の様子である。横軸は配信トラフィック情報（Ｋｐｐｓ）であり、縦軸はＣＰＵ使用率％である。配信量を小さくした方が、よりルータの負担が少ない結果となっている。
【００１１】
従来の技術においては、あるパケットのペイロード部分の分析のために配信する切り取りパケット長を長くした場合、分析においては、その情報が不要なパケットも同じパケット長で配信されることになり非常に非効率である。このため、クラスに応じて抽出するパケット長や配信方法を変更可能とすることで、より効率的なトラフィックの配信が可能となる。
【００１２】
また、通常は、トラフィック量が小さいため、当該クラスのサンプリングを大きくした場合においても、急激にトラフィック量が増える場合などがある。その場合には、ＮＷ機器のＣＰＵが負荷状態となり、他のクラスのトラフィックを配信できなくなることやＮＷ機器のそのほかの機能へも影響がでるといった問題がある。本機能では、クラス毎に配信するトラフィックデータの最大限度量を規定しておくことで、これらの問題の発生を回避

する。
【００１３】
また、各アプリケーションによって分析に有効なパケットサイズが変わってくるため（図２にアプリケーション毎に有効なパケットサイズの一例を示す。）、クラス単位に配信方法が変更できることは有益である。
【課題を解決するための手段】
【００１４】
本明細書において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。
【００１５】
第１の発明は、トラフィック情報をトラフィック情報収集機器に配信するトラフィック情報配信機器におけるトラフィック情報配信方法であって、前記トラフィック情報配信機器は、分類手段とクラス別処理手段とトラフィック情報配信データ作成配信手段とを有し、前記分類手段が、受信したパケットを各クラスに分類し、前記クラス別処理手段が、前記分類手段により各クラスに分類されたパケットに対して、各クラスに定められたトラフィック情報の配信手法に基づいて、パケットの一部を抽出するパケット抽出手法又はフローを集約するフロー集約手法のいずれかの配信手法を選択し、前記トラフィック情報配信データ作成配信手段が、前記クラス別処理手段で選択された配信手法による各トラフィック情報により構成されたトラフィック情報配信パケットを作成し、該トラフィック情報配信パケットを前記トラフィック情報収集機器に配信するトラフィック情報配信方法である。
【００１６】
第２の発明は、第１の発明のトラフィック情報配信方法であって、前記クラス別処理手段が、前記分類手段により各クラスに分類されたパケットに対して、各クラスに定められた配信限度量に基づいて、限度量が超過している場合には、当該トラフィック情報の配信を停止し、限度量を下回った際に、当該トラフィック情報の配信を開始するトラフィック情報配信方法である。
【００１７】
第３の発明は、第１又は第２のトラフィック情報配信方法であって、前記クラス別処理手段が、前記分類手段により各クラスに分類されたパケットに対して、各クラスに定められたサンプリングレート及び／又はサンプリングアルゴリズムに基づいてパケットサンプリングを行うトラフィック情報配信方法である。
【００１８】
第４の発明は、第１～第３の発明のトラフィック情報配信方法であって、前記トラフィック情報配信機器はフィルタ条件設定テーブルを有し、前記フィルタ条件設定テーブルは、パケットのヘッダに関わる情報である宛先アドレス、送信元アドレス、プロトコル、宛先ポート番号、送信元ポート番号、ＴＣＰフラグ、ＴＯＳ、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、ラベル、ＩＰバージョン、パケットＬｅｎｇｔｈ、および、ＮＷ機器が当該パケットをルーティングするための特性情報である受信ＩＦ情報、送信先ＩＦ情報、Ｎｅｘｔ－ＨｏｐアドレスＢＧＰ　Ｎｅｘｔ－ＨｏｐアドレスＰｅｅｒｉｎｇＡＳ番号、ＯｒｉｇｉｎＡＳ番号、ＢＧＰ　Ｃｏｍｍｕｎｉｔｙのうちの１以上に対応してフィルタ条件識別子とクラス識別子が設定されたものであり、前記分類手段が、前記フィルタ条件設定テーブルに基づいて、受信したパケットを各クラスに分類するトラフィック情報配信方法である。
【００１９】
第５の発明は、第４の発明のトラフィック情報配信方法であって、前記トラフィック情報配信機器はトラフィック測定情報テーブルを有し、前記トラフィック測定情報テーブルは、前記クラス識別子に対応して、トラフィック配信方法、サンプリングレート、サンプリングアルゴリズム、配信量の限度量の１以上が設定されたものであり、前記クラス別処理手段が、前記トラフィック測定情報テーブルに基づいて、クラス別の処理を行うトラフ

ィック情報配信方法である。

【００２０】

第６の発明は、第５の発明のトラフィック情報配信方法であって、前記トラフィック情報配信データ作成配信手段が、前記トラフィック情報配信パケットの各トラフィック情報に、前記フィルタ条件識別子及び／又は前記クラス識別子を付加するトラフィック情報配信方法である。

【００２１】

第７の発明は、第６の発明のトラフィック情報配信方法によってトラフィック情報の配信を行う前記トラフィック情報配信機器から、トラフィック情報を収集するトラフィック情報収集機器におけるトラフィック情報収集方法であって、前記トラフィック情報収集機器が、前記トラフィック情報配信機器から収集した各トラフィック情報に付加されたクラス識別子及び／又はフィルタ条件識別子をもとに、トラフィック分析装置群の中から適切なトラフィック分析装置に対して、トラフィック情報を振り分けるトラフィック情報収集方法である。

【発明の効果】

【００２２】

本発明により、クラスに応じて抽出するパケット長や配信方法を変更可能とすることで、より効率的なトラフィックの配信が可能となる。また、クラス毎に配信するトラフィックデータの最大限度量を規定しておくことで、ＮＷ機器のＣＰＵが負荷状態となり、他のクラスのトラフィックを配信できなくなることやＮＷ機器のそのほかの機能へも影響がでるといった問題の発生を回避することができる。また、クラス毎にサンプリングレートやサンプリングプロトコルを変更することができる。

【発明を実施するための最良の形態】

【００２３】

本発明の実施形態は、サンプリングの前に、パケットを分類し、ある特定のトラフィックについては、例えば、サンプリングレートを大きくして、アプリケーションのペイロード部分を含むパケット情報を監視・分析し、それ以外のトラフィックについては、より集約を行った上で、トラフィック情報を配信することを可能とするより効率な測定を行うものである。また、これにより、大規模ネットワークでのトラフィック測定というスケーラビリティを維持しつつ、より詳細なトラフィック監視・分析が可能となる。すなわち、本実施形態は、複数のフィルタ条件をもとに、ＮＷ機器（ルータ、スイッチ）などで受信されるＩＰパケットを、複数のクラスに分類し、分類したクラス単位にサンプリングレート、サンプリングアルゴリズム、トラフィック情報収集機器への情報配信方法、配信限度量を定義することで、パケットのアプリケーション毎のトラフィック分析方法に応じたトラフィック情報配信方法を可能とする。この機能は、ＮＷ機器（ルータ、スイッチ）などに実装されることを想定している。

【００２４】

以下、本発明の実施の形態を図面を用いて詳細に説明する。

図３に全体概要図を示す。図３において、３０１はネットワークであり、３０２はネットワーク３０１上に配置されたＮＷ機器である。図では４個のＮＷ機器３０２－１～３０２－４が配置されているが、何個でもよい。３０３はトラフィック情報を収集するトラフィック情報収集機器である。３０４はトラフィック分析装置群である。図では、トラフィック分析装置群３０４は、異常パケットの収集・分析装置３１１、Unroutable／未使用アドレストラフィック分析装置３１２、Signature分析装置３１３、TCP status分析・ICMP分析装置３１４、VoIP品質分析装置３１５、Protocol Analyzer３１６から構成されているが、これは一例であり、これらの一部の分析装置だけで構成してもよいし、これら以外の分析装置を含んでいてもよい。また、これらの分析装置は一般に使用されている装置を使用すればよいので、その詳細な説明は省略する。

【００２５】

ＮＷ機器３０２は階層的フロー統計機能を有する。階層的フロー統計機能とは、クラス

に分類し重要度などの用途に応じたフロー統計を行う機能である。ネットワーク３０１上を流れるパケットが入力されると、ＮＷ機器３０２は、サンプリング前に各クラスに分類し、各クラス毎に処理して、トラフィック情報配信データを作成し、フロー配信プロトコルを用いて、トラフィック情報配信データをトラフィック情報収集機器３０３に配信する。ＮＷ機器３０２は、典型的にはルータやスイッチ等であるが、トラフィック情報配信機能に注目すれば、トラフィック情報配信機器ということができる。

【００２６】

トラフィック情報収集機器３０３は、ネットワーク３０１上のＮＷ機器３０２－１～３０２－４から受信したトラフィック情報配信データをクラス単位／フィルタ条件単位に振り分けてトラフィック分析装置群３０４のそれぞれの分析装置３１１～３１６に配信する。

【００２７】

トラフィック分析装置群３０４のそれぞれの分析装置３１１～３１６はトラフィック情報収集機器３０３から振り分け配信されたトラフィック情報を使用してそれぞれの分析を行う。

【００２８】

図４に本機能をもつＮＷ機器３０２の構成図を示す。４０１はＩＦであり、ＩＦ４０１をとおしてパケット４４１～４４３がＮＷ機器３０２に流入する。

【００２９】

４０２はトラフィックをフィルタ条件に従いクラスに分類する分類手段である。分類手段４０２は、フィルタ条件設定テーブル７００に基づいて、受信したパケットを階層的に各クラスに分類する。なお、フィルタ条件テーブル７００については、図７を用いて後述する。

【００３０】

４０３は分類手段４０２でクラスに分類されたパケットを各クラス毎に処理するクラス別処理手段である。クラス別処理手段４０３は、トラフィック測定情報テーブル８００に基づいて、クラス別の処理を行う。なお、トラフィック測定情報テーブル８００については、図８を用いて後述する。

【００３１】

図４では、受信したＳＩＰパケット４４１、ｉｃｍｐパケット４４２、Ｏｔｈｅｒパケット（その他のパケット）４４３を、分類手段４０２が、それぞれクラス＃１、クラス＃２、クラス＃３に分類する例を示している。

【００３２】

クラス別処理手段４０３は、クラス＃１に分類されたＳＩＰパケット４４１に対して、４１０で示すように、Ｒａｔｅ＝１／１でサンプリングし（４１１）、情報配信手法の選択を行い（４１２）、配信限度量のチェックを行う（４１３）。また、クラス別処理手段４０３は、クラス＃２に分類されたｉｃｍｐパケット４４２に対して、４２０で示すように、Ｒａｔｅ＝１／１００でサンプリングし（４２１）、情報配信手法の選択を行い（４２２）、配信限度量のチェックを行う（４２３）。また、クラス別処理手段４０３は、クラス＃３に分類されたＯｔｈｅｒパケット４４３に対して、４３０で示すように、Ｒａｔｅ＝１／１００００でサンプリングし（４３１）、情報配信手法の選択を行い（４３２）、配信限度量のチェックを行う（４３３）。図４では、分類手段４０２が３つのクラスに分類し、クラス別処理手段４０３は３のクラス毎に処理しているが、一般的には、分類手段４０２が、受信したパケットを複数のクラスに分類し、クラス別処理手段４０３が、分類手段４０２により複数のクラスに分類されたパケットに対して、各クラス毎の処理、例えば、トラフィック情報の配信手法に基づいて、パケットの一部を抽出するパケット抽出手法又はフローを集約するフロー集約手法のいずれかの配信手法の選択を行えばよい。

【００３３】

４０４はクラス別処理手段４０３からのデータに基づいて、トラフィック情報配信データを作成し、トラフィック情報配信プロトコル・パケット４５０をトラフィック情報収集

機器３０３に配信するトラフィック情報配信データ作成配信手段である。トラフィック情報配信プロトコル・パケット４５０は、トラフィック情報配信プロトコルにより、トラフィック情報を配信するトラフィック情報配信パケットである。すなわち、トラフィック情報配信データ作成配信手段４０４は、クラス別処理手段４０３で選択された配信手法による各トラフィック情報により構成されたトラフィック情報配信パケットを作成し、そのトラフィック情報配信パケットをトラフィック情報収集機器３０３に配信する。

【００３４】

以下、ＮＷ機器３０２のクラス別処理手段４０３の処理について更に詳細に説明する。

サンプリング４１１、４２１、４３１においては、例えば、サンプリングレートは、Ｍ個のパケットの通過でＮ個のパケットを抽出する場合には、Ｎ／Ｍをレートとする。サンプリングアルゴリズムについては、ランダムにサンプリングするのか、規則的に抽出するのか、時間周期でパケットをサンプリングするのかが選択できるものとする。

【００３５】

情報配信手法の選択４１２、４２２、４３２においては、トラフィック情報収集機器への情報配信方法は、大きく２つに分けられる。１つは、パケットのある部分を切り出してそれをコピーして配信する方法（以下、これをパケット抽出手法と呼ぶ。）であり、もう一つは、フロー識別情報（ＩＰヘッダに含まれる送信元／宛先ＩＰアドレス、送信元／宛先ポート番号、プロトコル）単位にパケット数、バイト数を集約して配信する方法（以下、これをフロー集約手法と呼ぶ。）になる。

【００３６】

パケット抽出手法においては、その配信方法に関するパラメータをクラス単位に指定可能とする。以下に指定可能とするパラメータを示す。

・パケットコピー開始ヘッダ情報：抽出したパケットの中で、配信するためのコピー開始箇所の情報としてヘッダ種別（Ｅｔｈｅｒｎｅｔヘッダ，ＩＰヘッダ，ＵＤＰ，ＴＣＰヘッダ）を指定する。

・オフセット情報：上記ヘッダ種別からパケットの切り出し開始部分を示すオフセット値（ｂｙｔｅ）である。

・抽出最大長：パケットの切り出し開始部分からコピー可能な最大長（ｂｙｔｅ）である。

【００３７】

フロー集約手法においても、その配信方法に関するパラメータをクラス単位に指定可能とする。以下に指定可能とするパラメータを示す。

・フローキー情報：前述したフロー識別情報をキー情報として集約する以外にＩＰ／ＵＤＰ／ＴＣＰヘッダ、Ｅｔｈｅｒｎｅｔヘッダ、Ｌａｂｅｌヘッダの各属性情報や受信／出力ＩＦ番号、パケット・ルーティング特性情報（Ｎｅｘｔ－Ｈｏｐ，ＢＧＰ Ｎｅｘｔ－ｈｏｐ，ｏｒｉｇｉｎＡＳ，ｐｅｅｒＡＳなど）を指定可能とする。このキー情報をもとに、フロー・エントリ情報が作成され、以降、同一のキー情報をもつパケットを抽出した際は、このエントリの集計属性情報に対して積算処理される。抽出したパケットの中で、該当するフロー・エントリがない場合には、新規に作成される。

・集計属性情報：フローキーをもとに集約する際に、集約すべき属性情報を指定する。例えば、パケット数、パケットＬｅｎｇｔｈの総計（総Ｂｙｔｅ数）などが該当する。

・タイムアウト情報：ある識別情報をもとに集約をしていた際に、ある周期内で、その識別情報に関する集計属性情報に変化がない場合に、このフロー・エントリ情報を削除して、トラフィック情報収集機器にこの情報を配信することを定めたタイムアウト値（秒）である。

【００３８】

以上のように情報配信手法の選択４１２、４２２、４３２により、クラス単位に定めたトラフィック情報の配信方法によって、各クラスのトラフィック情報は、トラフィック情報収集機器３０３に配信されるが、特定のクラスのトラフィック量が増えることによって、他のクラスの情報が配信されなくなるという状況を回避するため、クラス単位に配信量

の限度量を定めておき、配信限度量のチェック４１３、４２３、４３３により配信限度量のチェックが行われる。この限度量は、パケット抽出手法においては、ｐｐｓ（packets per second）を単位とし、フロー集約手法においては、ｆｐｓ（flow records per second）を単位とする。

【００３９】

トラフィック情報配信データ作成配信手段４０４が、これらのトラフィック情報をトラフィック情報収集機器３０３に配信する際には、各クラスの識別子及び該当したフィルタ条件識別子をトラフィック情報に付加して配信する。配信するためのプロトコルとしては、ＩＰＦＩＸ，ｓＦｌｏｗ，ＮｅｔＦｌｏｗなどのトラフィック情報配信プロトコルが適用される。パケット抽出手法にて抽出されたトラフィック情報はパケット情報として、フロー集約手法として選択された情報はフローレコード情報として、トラフィック情報配信プロトコルのパケットに格納される。各クラスを示すクラス識別子及びフィルタ条件識別子は、各トラフィック情報に付加される。

【００４０】

図５に、このようにして作成されたトラフィック情報配信プロトコル・パケット４５０の構成を示す。５０１はトラフィック情報配信プロトコル・パケットのヘッダであり、５０２－１～５０２－Ｎはトラフィック情報＃１～＃Ｎである。トラフィック情報＃１（５０２－１）はフロー集約手法の場合のトラフィック情報である。５１０はトラフィック情報＃１のヘッダであり、５１１はフローキー情報であり、５１２は集計属性情報であり、５１３はクラス識別子であり、５１４はフィルタ条件識別子である。ヘッダ５１０にサンプリングレート、サンプリングアルゴリズムが記述される。フローキー情報５１１と集計属性情報５１２がフローレコード情報である。一方、トラフィック情報＃Ｎ－１（５０２－Ｎ－１）はパケット抽出手法の場合のトラフィック情報である。５２０はトラフィック情報＃Ｎ－１のヘッダであり、５２１はパケットコピー情報であり、５２２は関連属性情報であり、５２３はクラス識別子であり、５２４はフィルタ条件識別子である。パケットコピー情報５２１がパケット情報である。

【００４１】

トラフィック情報収集機器３０３では、各トラフィック情報に付加された各クラスを示すクラス識別子５１３、５２３及びフィルタ条件識別子５１４、５２４により、受信したトラフィック情報のクラス及びフィルタ条件の識別が可能となり、トラフィック分析をする際にトラフィック分析装置群３０４に対して情報の振り分けが可能となる。

【００４２】

これにより、重要なパケットについては、サンプリングレートを大きくした上で、パケット抽出手法にてアプリケーションのペイロードも含む情報をトラフィック情報収集機器３０３に配信することが可能となり、トラフィック分析装置群３０４では、パケットのアプリケーション部分も含めたトラフィックの分析を行うことが可能となる。また、全体的なトラフィック動向を測ることを目的としているクラスに対しては、サンプリングレートを小さくした上で、ＯｒｉｇｉｎＡＳ単位の集約など粒度の荒いフロー集約手法にてトラフィック情報収集機器３０３に配信することが可能となり、スケーラビリティを維持することが可能となる。

【実施例】

【００４３】

ここで、図６のようなあるプロバイダのネットワークをもとに階層的フロー統計手法の適用方法を示す。図６は、あるプロバイダの概念図である。図６において、６０１はこのプロバイダのＮＷ（Network）であり、６０２はＮＷ６０１に接続されたマスユーザアクセス網であり、６０３はＮＷ６０１に接続された重要顧客のアクセス網である。６０４は外部ＮＷ＃１であり、ルータ＃１（６０６）を介してＮＷ６０１に接続されている。６０５は外部ＮＷ＃２であり、ルータ＃２（６０７）を介してＮＷ６０１に接続されている。

【００４４】

このプロバイダは、以下のようなアドレスの設定方針のＮＷ６０１をもっているものと

する。
・マスユーザアクセス網６０２として、お客さま用のアドレスとして、アドレスブロック１９２．０．２．０／２６をもつ。
・重要顧客のアクセス網６０３として、このお客さま用のアドレスとして、アドレスブロック１９２．０．２．６４／２６をもつ。
・ＮＷ６０１網内のリンクアドレスとして、アドレスブロック１９２．０．２．１２８／２６をもつ
・プロバイダの基幹サーバとして、ＤＮＳサーバ６０８とＳＩＰサーバ６１０がそれぞれ、１９２．０．２．２００、１９２．０．２．２１０のアドレスをもつ。

【００４５】
ここで、外部ＮＷ＃１（６０４）とルータ＃１（６０６）を結ぶルータ＃１（６０６）のＩＦで階層的フロー統計手法を適用させた場合の例を示す。

【００４６】
ルータ＃１（６０６）では、パケットをクラスわけするためのフィルタ条件設定テーブルとクラス毎のトラフィック測定情報テーブルをもつ。図７にフィルタ条件設定テーブルと図８にトラフィック測定情報テーブルを示す。

【００４７】
図７のフィルタ条件設定テーブル７００において、７０１はフィルタ条件識別子を、７０２は宛先ＩＰアドレス帯域を、７０３は送信元ＩＰアドレス帯域を、７０４はプロトコルを、７０５は宛先ポート番号を、７０６は送信元ポート番号を、７０７はＴＣＰ Ｆｌａｇｓを、７０８はクラス識別子を、それぞれ設定する欄である。

【００４８】
図７のフィルタ条件設定テーブルにおいては、宛先ＩＰアドレス帯域、送信元ＩＰアドレス帯域、プロトコル、宛先ポート番号、送信元ポート番号、ＴＣＰ Ｆｌａｇｓを設定可能とする例を示しているが、一般には、パケットのヘッダに関わる情報（宛先アドレス、送信元アドレス、プロトコル、宛先ポート番号、送信元ポート番号、ＴＣＰフラグ、ＴＯＳ、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、ラベル、ＩＰバージョン、パケットＬｅｎｇｔｈ）やＮＷ機器が当該パケットをルーティングするための特性情報（受信ＩＦ情報、送信先ＩＦ情報、Ｎｅｘｔ－ＨｏｐアドレスＢＧＰ Ｎｅｘｔ－Ｈｏｐアドレス、ＰｅｅｒｉｎｇＡＳ番号、ＯｒｉｇｉｎＡＳ番号、ＢＧＰ Ｃｏｍｍｕｎｉｔｙ）を設定可能としてもよい。すなわち、フィルタ条件設定テーブルは、これらのうちの１以上に対応してフィルタ条件識別子とクラス識別子が設定されたものでもよい。

【００４９】
図８のトラフィック測定情報テーブルにおいて、８０１はクラス識別子を、８０２はサンプリングアルゴリズムを、８０３はサンプリングレートを、８０４はトラフィック配信方法を、８０５はパケットコピー開始箇所情報を、８０６はオフセット情報を、８０７は抽出最大長を、８０８は関連属性情報を、８０９はフローキー情報を、８１０は集計属性情報を、８１１はタイムアウト情報を、８１２は配信量の限度量を、それぞれ設定する欄である。トラフィック配信方法８０４においてパケット抽出手法を設定した場合は、パケットコピー開始箇所情報８０５、オフセット情報８０６、抽出最大長８０７、関連属性情報８０８を設定する。一方、トラフィック配信方法８０４においてフロー集計手法を設定した場合は、フローキー情報８０９、集計属性情報８１０、タイムアウト情報８１１を設定する。

【００５０】
図７のフィルタ条件設定テーブル７００では、フィルタ条件識別子１～４までは、Ｐｒｉｖａｔｅアドレスを使用しているなどの本来あってはならないパケットが外部ＮＷから流入した場合を想定しており、これをクラス１としている。以降は、重要なサーバへの監視をサーバ単位にクラス２、３とし、最終的に外部ＮＷ＃２に流れていくトラフィックについては、クラス7として設定している。パケットを受信した際は、フィルタ条件識別子の若番（小さい番号）から順次検索されるものとして、条件に合致した箇所でそのパケッ

トのクラスが確定する。

【００５１】

すなわち、分類手段４０２は、図７のフィルタ条件設定テーブル７００に基づいて、本来あってはならないパケットについてはフィルタ条件識別子１～４、クラス識別子１とし、宛先がＤＮＳサーバ６０８（１９２．０．２．２００）であるパケットについてはフィルタ条件識別子５、クラス識別子２とし、宛先がＳＩＰサーバ６１０（１９２．０．２．２１０）であるパケットについてはフィルタ条件識別子６、クラス識別子３とし、宛先が重要顧客のアクセス網６０３（１９２．０．２．６４／２６）であるパケットについてはフィルタ条件識別子７、クラス識別子４とし、宛先がマスユーザアクセス網６０２（１９２．０．２．０／２６）であるパケットについてはフィルタ条件識別子８、クラス識別子５とし、宛先がＮＷ網６０１（１９２．０．２．１２８／２６）であるパケットについてはフィルタ条件識別子９、クラス識別子６とし、それ以外のパケットについてはフィルタ条件識別子１０、クラス識別子７とする。

【００５２】

クラスが決定したパケットは、クラス単位に設定されたトラフィック測定情報テーブル８００にそって、トラフィック情報として集計される。

【００５３】

例えば、ＳＩＰサーバ６１０に向けのトラフィック（クラス識別子３）については、ＳＤＰの部分まで分析可能なように抽出するコピーパケット部分の長さを多くしている（抽出最大長：７５０ｂｙｔｅ）。また、これに対して外部ＮＷ＃２（６０５）に流れ出るトラフィック（クラス識別子７）は、それほど詳細な分析は必要ないため、ピアリングするＡＳ番号単位にトラフィックを集計するように設定されている（フローキー情報：ＰｅｅｒｉｎｇＡＳ）。

【００５４】

上記のように外部ＮＷ＃１（６０４）からルータ＃１（６０６）に受信したパケットは、フィルタ条件設定テーブル７００をもとにクラスわけされ、トラフィック測定情報テーブル８００の設定内容に従い、トラフィック情報として成形されて、トラフィック情報配信プロトコルのパケット４５０に格納される。

【００５５】

トラフィック情報収集機器３０３では、クラス識別子、フィルタ条件識別子をもとに特定の分析装置に振り分けを行う。例えば、ＳＩＰパケット（フィルタ条件識別子６、クラス識別子３）に対しては、ＳＩＰプロトコル用の分析装置に振り分け配信される。

【００５６】

以上説明した実施形態のＮＷ機器の各手段は、記憶装置に記憶されたプログラムをＣＰＵが処理することにより実現される。また、そのプログラムの一部または全部をハードウェアで構成してもよい。また、ＮＷ機器の各テーブルは記憶装置に記憶される。

【００５７】

以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【図面の簡単な説明】

【００５８】

【図１】ルータの負荷状況を示す図である。

【図２】アプリケーション毎に有効なパケットサイズの一例を示す表である。

【図３】本発明の実施形態の全体概要図である。

【図４】本発明の実施形態のＮＷ機器（トラフィック情報配信機器）の構成図である。

【図５】本発明の実施形態により作成されたトラフィック情報配信プロトコル・パケットである。

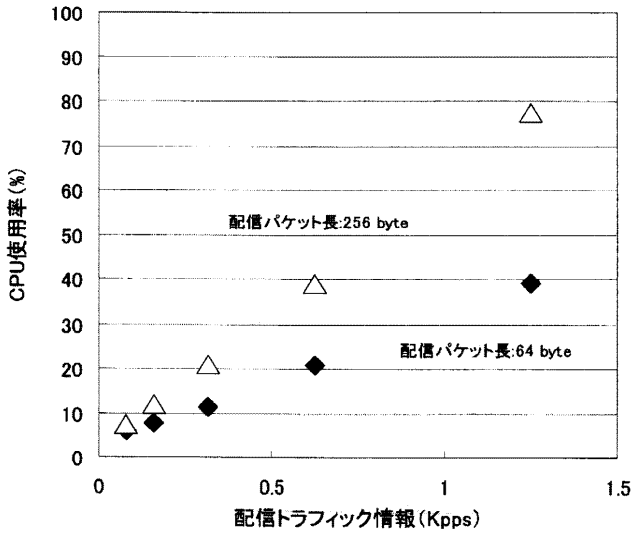
【図６】本発明の実施例のプロバイダの概念図である。

【図７】本発明の実施例のフィルタ条件設定テーブルである。

【図８】本発明の実施例のトラフィック測定情報テーブルである。
【符号の説明】
【００５９】
３０１…ネットワーク、３０２…ＮＷ機器（トラフィック情報配信機器）、３０３…トラフィック情報収集機器、３０４…トラフィック分析装置群、４０１…ＩＦ、４０２…分類手段、４０３…クラス別処理手段、４０４…トラフィック情報配信データ作成配信手段、４４１…ＳＩＰパケット、４４２…ｉｃｍｐパケット、４４３…Ｏｔｈｅｒパケット、４１０、４２０、４３０…クラス＃１、クラス＃２、クラス＃３に分類されたパケットの処理、４１１、４２１、４３１…サンプリング、４１２、４２２、４３２…情報配信手法の選択、４１３、４２３、４３３…配信限度量のチェック、４５０…トラフィック情報配信プロトコル・パケット、５０１…トラフィック情報配信プロトコル・パケットのヘッダ、５０２－１～５０２－Ｎ…トラフィック情報＃１～＃Ｎ、５１０…トラフィック情報＃１のヘッダ、５１１…フローキー情報、５１２…集計属性情報、５１３…クラス識別子、５１４…フィルタ条件識別子、５２０…トラフィック情報＃Ｎ－１のヘッダ、５２１…パケットコピー情報、５２２…関連属性情報、５２３…クラス識別子、５２４…フィルタ条件識別子、６０１…プロバイダのＮＷ、６０２…マスユーザアクセス網、６０３…重要顧客のアクセス網、６０４…外部ＮＷ＃１、６０５…外部ＮＷ＃２、６０６…ルータ＃１、６０７…ルータ＃２、６０８…ＤＮＳサーバ、６１０…ＳＩＰサーバ、７００…フィルタ条件設定テーブル、８００…トラフィック測定情報テーブル

【図１】

図1



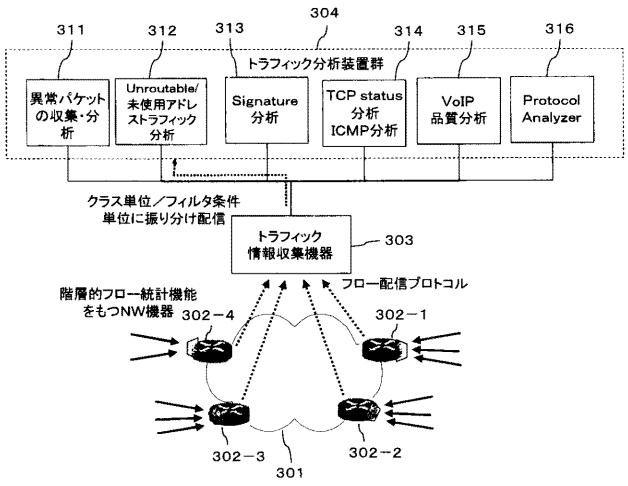
【図２】

図2

	モニタするポイント	Size
HTTP	・Request ・URL ・User-Agent	User-Agent までは、512byte 程度は必要。
DNS	・query URI ・response code	通常 200byte 程度。 512 byte あれば十分。
IRC/Convert chanel	・制御コマンドらしきものの形跡	Signature そのものは、非常に複雑。ものによって、フルキャプチャ程度のものが必要。
VoIP	・RTP ・SIP Call-ID ・Via ・Contact	・RTP 300byte ・SIP は、SDP の一部まで含めると 750byte は必要。

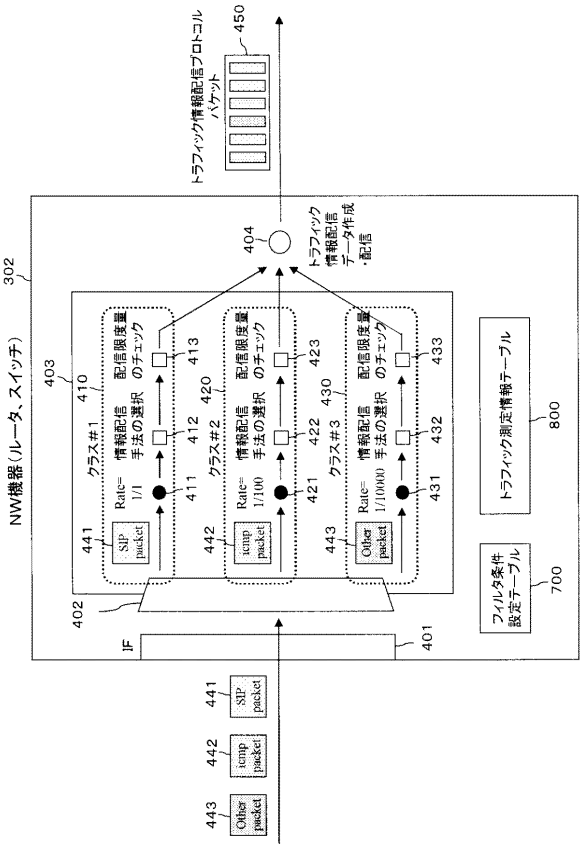
【図３】

図3



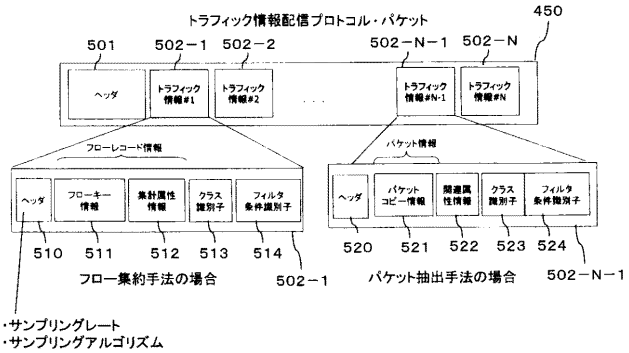
【図４】

図4



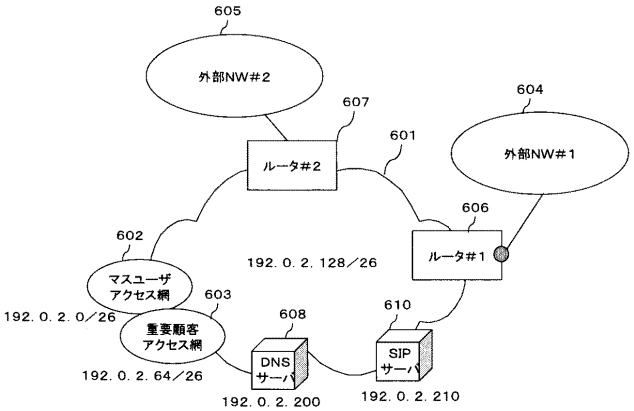
【図５】

図5



【図６】

図6



【図７】

図7

700

フィルタ条件設定テーブル

フィルタ条件識別子	宛先IPアドレス帯域	送信元IPアドレス帯域	プロトコル	宛先ポート番号	送信元ポート番号	TCP Flags	クラス識別子
1	any	192.168.0.0/24	any	any	any	any	1
2	any	172.16.0.0/12	any	any	any	any	1
3	any	10.0.0.0/8	any	any	any	any	1
4	any	any	TCP	any	any	000000	1
5	192.0.2.200	any	any	any	any	any	2
6	192.0.2.210	any	any	any	any	any	3
7	192.0.2.64/26	any	any	any	any	any	4
8	192.0.2.0/26	any	any	any	any	any	5
9	192.0.2.128/26	any	any	any	any	any	6
10	any	any	any	any	any	any	7

701 702 703 704 705 706 707 708

【図８】

図8

800

トラフィック測定情報テーブル

クラス識別子	サンプリングアルゴリズム	サンプリングレート	トラフィック配信方法	パケットコピー開始箇所情報	オフセット情報	抽出最大長	関連属性情報	フローキー情報	集計属性情報	タイムアウト情報	配信量の限度量
1	なし	–	パケット抽出手法	IPヘッダ	0	1000byte	・受信時刻 ・Nexthop	–	–	–	4000 pps
2	ランダム	1/100	パケット抽出手法	IPヘッダ	0	400byte	・受信時刻 ・Nexthop	–	–	–	4000 pps
3	ランダム	1/10	パケット抽出手法	IPヘッダ	100byte	750byte	・受信時刻 ・Nexthop	–	–	–	1000 pps
4	なし	–	フロー集計手法	–	–	–		・送信元IPアドレス ・宛先IPアドレス ・プロトコル ・送信元ポート番号 ・宛先ポート番号	・Byte量 ・パケット数 ・フロー開始時間 ・フロー終了時間	30秒	10000 fps
5	ランダム	1/100	フロー集計手法	–	–	–		・送信元IPアドレス ・宛先IPアドレス ・プロトコル ・送信元ポート番号 ・宛先ポート番号	・Byte量 ・パケット数	30秒	1000 fps
6	システム	1/100	フロー集計手法	–	–	–		・送信元IPアドレス ・宛先IPアドレス ・プロトコル ・送信元ポート番号 ・宛先ポート番号	・Byte量 ・パケット数	30秒	1000 fps
7	ランダム	1/10000	フロー集計手法	–	–	–		・PeeringAS	・Byte量 ・パケット数	60秒	10000 fps

801 802 803 804 805 806 807 808 809 810 811 812