(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4774357号
(P4774357)
(45)発行日　平成23年9月14日(2011.9.14)　(24)登録日　平成23年7月1日(2011.7.1)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　400Z

請求項の数 8　(全 38 頁)

(21)出願番号　特願2006-324200 (P2006-324200)
(22)出願日　平成18年11月30日 (2006.11.30)
(65)公開番号　特開2007-336512 (P2007-336512A)
(43)公開日　平成19年12月27日 (2007.12.27)
審査請求日　平成21年8月7日 (2009.8.7)
(31)優先権主張番号　特願2006-138661 (P2006-138661)
(32)優先日　平成18年5月18日 (2006.5.18)
(33)優先権主張国　日本国(JP)

(73)特許権者　504411166
アラクサラネットワークス株式会社
神奈川県川崎市幸区鹿島田８９０
(74)代理人　100075513
弁理士　後藤　政喜
(74)代理人　100114236
弁理士　藤井　正弘
(74)代理人　100120260
弁理士　飯田　雅昭
(72)発明者　正村　雄介
東京都国分寺市東恋ヶ窪一丁目２８０番地
株式会社日立製作所中央研究所内

最終頁に続く

(54)【発明の名称】統計情報収集システム及び統計情報収集装置

(57)【特許請求の範囲】
【請求項１】
演算処理をする第一プロセッサと、前記第一プロセッサに接続される第一記憶領域と、前記第一プロセッサに接続される第一インタフェースと、を備える統計情報収集装置と、
演算処理をする第二プロセッサと、前記第二プロセッサに接続される第二記憶領域と、前記第二プロセッサに接続され、前記統計情報収集装置に接続される第二インタフェースと、を備えるコレクタ装置と、を備え、
前記第一プロセッサは、パケットを受信し、前記受信パケットの統計情報として当該フローの帯域を収集し、前記収集された統計情報を前記コレクタ装置に送信する通信情報収集システムにおいて、
前記第一記憶領域には、前記受信パケットが属するフローを識別するためのフロー識別条件を含むフロー情報が格納され、
前記第一プロセッサは、
前記フロー識別条件によって識別されるフロー毎に、前記収集されたパケットの統計情報を分類し、
前記フロー毎に分類された統計情報を参照し、前記統計情報を前記コレクタ装置に送信する送信間隔を前記フロー毎に決定し、
前記フロー毎に分類された統計情報が分析された結果に基づいて、前記受信パケットのサンプリング間隔を決定し、
前記決定されたサンプリング間隔で、前記受信パケットをサンプリングし、

前記サンプリングされたパケットのヘッダ情報を前記統計情報として、前記コレクタ装置に送信することを特徴とする統計情報収集システム。

【請求項２】

前記第二プロセッサは、

前記第一プロセッサから統計情報を受信すると、前記フロー毎に分類された統計情報を分析し、

前記統計情報の分析結果を前記第一プロセッサに送信し、

前記第一プロセッサは、

前記統計情報の分析結果を受信すると、前記受信した分析結果に基づいて、前記受信パケットのサンプリング間隔を決定することを特徴とする請求項１に記載の統計情報収集システム。

【請求項３】

前記第一プロセッサは、

前記フロー毎に分類された統計情報を分析し、

前記統計情報の分析結果に基づいて、前記受信パケットのサンプリング間隔を決定することを特徴とする請求項１に記載の統計情報収集システム。

【請求項４】

前記フロー毎に分類された統計情報に関する閾値がフロー毎に設定され、

前記第一プロセッサは、

前記パケットを受信すると、前記受信パケットが属するフローに設定された閾値に基づいて、前記フロー毎に分類された統計情報を分析するか否かを判定することを特徴とする請求項１に記載の統計情報収集システム。

【請求項５】

前記フロー毎に分類された統計情報に関する閾値がフロー毎に設定され、

前記第二プロセッサは、

前記第一プロセッサから統計情報を受信すると、前記受信した統計情報のフローに設定された閾値に基づいて、前記フロー毎に分類された統計情報を分析するか否かを判定することを特徴とする請求項１に記載の統計情報収集システム。

【請求項６】

前記第一プロセッサは、

前記統計情報の分析結果及び前記フローの帯域のうち少なくとも一方に基づいて、前記フロー毎に分類された統計情報に関する閾値を更新することを特徴とする請求項４に記載の統計情報収集システム。

【請求項７】

前記第二プロセッサは、

前記統計情報の分析結果及び前記フローの帯域のうち少なくとも一方に基づいて、前記フロー毎に分類された統計情報に関する閾値を更新することを特徴とする請求項５に記載の統計情報収集システム。

【請求項８】

演算処理をするプロセッサと、前記プロセッサに接続される記憶領域と、コレクタ装置に接続され、前記プロセッサに接続されるインタフェースと、を備え、パケットを受信し、前記受信パケットの統計情報として当該フローの帯域を収集し、前記収集された統計情報を前記コレクタ装置に送信する統計情報収集装置において、

前記記憶領域には、前記受信パケットが属するフローを識別するためのフロー識別条件を含むフロー情報が格納され、

前記プロセッサは、

前記フロー識別条件によって識別されるフロー毎に、前記収集されたパケットの統計情報を分類し、

前記フロー毎に分類された統計情報が分析された結果に基づいて、前記受信パケットのサンプリング間隔を決定し、

前記決定されたサンプリング間隔で、前記受信パケットをサンプリングし、
前記サンプリングされたパケットのヘッダ情報を前記統計情報として、前記コレクタ装置に送信することを特徴とする統計情報収集装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、転送されるパケットのパケット数及びバイト数等の統計情報を収集する通信統計収集装置に関し、特にコレクタ装置に統計情報を送信する統計情報収集装置に関する。
【背景技術】
【０００２】
今日、インターネットは、重要な社会インフラとして定着している。そのため、従来のベストエフォート型のデータ通信だけでなく、通信品質が保証されなければならないデータが通信され始めている。例えば、通信品質が保証されなければならないデータには、音声及び動画並びに基幹業務のトランザクションデータ等がある。また、ADSL(Asymmetric Digital Subscriber Line)及びFTTH(Fiber To The Home)技術によってアクセス回線がブロードバンド化し、通信されるデータの容量も増大している。
【０００３】
このような背景から、通信事業者及びＩＳＰ(Internet Service Provider)にとって、ネットワーク内の通信の状態を把握するため、ネットワーク内で通信されるデータの容量の統計を収集し、収集された統計を分析することによってネットワークを監視する機能が必要とされる。
【０００４】
データの送信元、データの宛先、アプリケーション、及び品質レベル等によって分類されるデータ群（以下、フローという）毎に統計情報を収集する機能及びフロー毎の統計情報を分析する機能が、ネットワークを監視する機能の中でも特に要求される。
【０００５】
通信事業者及びＩＳＰは、フロー毎の統計情報を利用することによって、通信の品質保証サービスを提供する際に、通信の品質が保証されているか否かの状況を確認できる。また、フロー毎の統計情報を利用することによって、限られたネットワーク資源において通信されるデータの容量が増大しているので、ネットワーク資源を有効に活用するためのトラフィック・エンジニアリング（ＴＥ）を利用できる。
【０００６】
さらに、フロー毎の統計情報を利用することによって、顧客の需要を予測してネットワーク資源を事前に準備して、ユーザからの要求に対して、迅速にネットワーク資源を提供するプロビジョニングを実行できる。また、フロー毎の統計情報を利用することによって、ネットワークへの不正アタックを検出し、分析できる。また、フロー毎の統計情報を利用することによって、フロー毎に課金等を行える。
【０００７】
なお、統計情報を収集する機能は、ネットワーク上でパケットを転送するルータ及びスイッチ等のノード装置に備わる。
【０００８】
統計情報収集システムは、ネットワーク上に分散して配置される複数の統計情報収集装置と、これらの統計情報収集装置から送信される統計情報に基づいて、ネットワーク全体のトラフィックを分析するコレクタ装置と、を備える。
【０００９】
フロー毎の統計情報を収集する方法として、サンプリング型のフロー統計技術が知られている（非特許文献１参照）。非特許文献１に記載された統計情報収集システムでは、統計情報収集装置であるルータが、受信したパケットを複製し、複製したパケットを選択的にコレクタ装置に転送する。そして、コレクタ装置側は、転送されたパケットからフロー

を識別し、統計情報を収集し、分析する。

【００１０】

統計情報収集システムに備わる各ルータは、ネットワークの管理者によって予め設定されたサンプリングレートに従って、受信したパケットをサンプリングし、サンプリング処理が実行されたパケットの複製を予め規定されたカプセル化フォーマットでカプセル化して、コレクタ装置に転送する。

【００１１】

コレクタ装置は、ルータから転送されたパケットから複製されたパケットを抽出し、複製されたパケットのヘッダ情報と、必要に応じて追加されたフローを識別するための情報とに基づいて、フローを識別し、フロー毎の統計情報を更新する。

【００１２】

また、サンプリング型の統計情報収集システムの拡張として、フロー単位でサンプリングする技術が知られている（特許文献１参照）。非特許文献１に記載されたフロー統計技術は、ルータが受信したパケットの中から一定の割合でパケットをサンプリングするのに対して、特許文献１に記載されたフロー統計技術は、ルータが受信するパケットのヘッダ情報からフローを識別し、フロー毎に設定した割合でパケットをサンプリングする。

【特許文献１】特開２００６－５４０２号公報

【非特許文献１】IETF RFC3176 “ InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks"

【発明の開示】

【発明が解決しようとする課題】

【００１３】

非特許文献１に記載されたフロー統計技術は、ルータが受信するパケットのヘッダ情報と一部のデータ情報とをカプセル化して、コレクタ装置に送信する。従って、ルータがフローの統計情報を詳細に監視するためには、サンプリングレートを大きく設定して、頻繁にパケットをサンプリングし、コレクタ装置へ送信する必要がある。

【００１４】

しかし、サンプリングレートを大きくすると、ルータの処理負荷が増大する。またルータとコレクタ装置との間の通信量及びコレクタ装置の処理負荷が増大する。

【００１５】

従って、通信量の多いコアルータにおいて、フロー情報を精度よく収集することは困難である。また、通信量が比較的少ないルータにおいても、帯域の小さいフローを把握することは困難である。

【００１６】

特許文献１に記載されたフロー統計技術は、フロー単位にサンプリングするので、監視したいフローのみをサンプリングして、コレクタ装置へ送信する。従って、サンプリングするフローを限定することによって、ルータの処理負荷、ルータとコレクタ装置との間の通信量、及びコレクタ装置の処理負荷を軽減できる。

【００１７】

しかしながら、サンプリングされるフローの選択次第で、異常なトラフィックを検出できない場合、及び統計情報のトラフィック量を軽減できない場合がある。従って、特許文献１に記載された技術は、監視するフローを適切に選択することが困難である。

【課題を解決するための手段】

【００１８】

本発明の代表的な一形態によると、演算処理をする第一プロセッサと、前記第一プロセッサに接続される第一記憶領域と、前記第一プロセッサに接続される第一インタフェースと、を備える統計情報収集装置と、演算処理をする第二プロセッサと、前記第二プロセッサに接続される第二記憶領域と、前記第二プロセッサに接続され、前記統計情報収集装置に接続される第二インタフェースと、を備えるコレクタ装置と、を備え、前記第一プロセッサは、パケットを受信し、前記受信パケットの統計情報として当該フローの帯域を収集

し、前記収集された統計情報を前記コレクタ装置に送信する通信情報収集システムにおいて、前記第一記憶領域には、前記受信パケットが属するフローを識別するためのフロー識別条件を含むフロー情報が格納され、前記第一プロセッサは、前記フロー識別条件によって識別されるフロー毎に、前記収集されたパケットの統計情報を分類し、前記フロー毎に分類された統計情報を参照し、前記統計情報を前記コレクタ装置に送信する送信間隔を前記フロー毎に決定し、前記フロー毎に分類された統計情報が分析された結果に基づいて、前記受信パケットのサンプリング間隔を決定し、前記決定されたサンプリング間隔で、前記受信パケットをサンプリングし、前記サンプリングされたパケットのヘッダ情報を前記統計情報として、前記コレクタ装置に送信することを特徴とする。

【発明の効果】

【００１９】

本発明の一形態によると、コレクタ装置が受信する統計情報を、フローの帯域と種別に応じ、自動的に制御するため、統計情報収集装置とコレクタ装置との間の通信量削減、並びに統計情報収集装置及びコレクタ装置の処理負荷を低減し、統計情報の分析精度を向上させる。

【発明を実施するための最良の形態】

【００２０】

本発明の実施の形態を図面を用いて説明する。

【００２１】

（第一実施形態）

本発明の第一の実施の形態を図１から図８、及び図１５を用いて説明する。

【００２２】

図１は本発明の第一の実施の形態の通信統計情報収集システムを示すブロック図である。

【００２３】

統計情報収集システムは、ルータ１０１、サーバ１０２、端末１０３、及びコレクタ装置１０４を備える。これらの装置はネットワークを介して接続される。例えば、ネットワークは、ＩＳＰ（Internet Service Provider）によって提供される。また、ネットワークは、企業内ネットワークであってもよい。

【００２４】

具体的には、端末Ａ１０３、端末Ｂ１０３、及び端末Ｃ１０３は、ルータＡ１０１と接続される。サーバＡ１０２はルータＢ１０１と接続され、サーバＣ１０２はルータＣ１０１と接続される。コレクタ装置Ａ１０４は、ルータＡ１０１と接続される。また、ルータＡ１０１、ルータＢ１０１、及びルータＣ１０１は、各々接続される。

【００２５】

ルータ１０１は、ネットワーク内で通信される情報をその情報の宛先に転送する装置で、プロセッサ、記憶装置及び通信インタフェースを備える。また、ルータ１０１は、通信される情報の統計情報を収集し、収集した統計情報をコレクタ装置１０４に送信する。

【００２６】

図２は、本発明の第一の実施の形態のルータ１０１の機能ブロック図である。

【００２７】

ルータ１０１は、受信パケット処理部２０１、送信パケット処理部２０２、検索処理部２０３、サンプリングレート管理テーブル２０４、統計情報テーブル２０５、フローテーブル２０６、ルーティングテーブル２０７、及び制御部２０８を備える。

【００２８】

管理端末２０９は、制御部２０８に接続される。管理者は、管理端末２０９を介して受信パケット処理部２０１、送信パケット処理部２０２、及び検索処理部２０３に設定されている各種パラメータを変更できる。なお、管理端末２０９は、ネットワークを介して制御部２０８に接続されてもよい。

【００２９】

受信パケット処理部２０１は、入力ポートを介してパケットを受信する。受信パケット処理部２０１は、受信したパケットをバッファに蓄積し、蓄積されたパケットのヘッダ情報を検索処理部２０３に送信する。

【００３０】

検索処理部２０３は、受信パケット処理部２０１からヘッダ情報を受信すると、検索処理を実行し、検索処理の結果を受信パケット処理部２０１に送信する。なお、検索処理については、図６で詳細を説明する。

【００３１】

受信パケット処理部２０１は、検索処理部２０３から検索結果を受信すると、検索結果に含まれる出力ポートに基づいて、送信パケット処理部２０２へパケットを送信する。

【００３２】

また、受信パケット処理部２０１が受信する検索結果にパケットをサンプリングする指示が含まれる場合、受信パケット処理部２０１は、該当するパケットにカプセル化する指示、サンプリング処理に利用されたサンプリングレート、及びカプセル化ヘッダ情報を含め、カプセル化する指示、サンプリング処理に利用されたサンプリングレート、及びカプセル化ヘッダ情報が含められたパケットのヘッダ情報を該当する送信パケット処理部２０２に送信する。なお、サンプリング処理に利用されたサンプリングレート及びカプセル化ヘッダ情報は、受信パケット処理部２０１が受信する検索結果に含まれる。

【００３３】

送信パケット処理部２０２の動作を説明する。送信パケット処理部２０２は、受信パケット処理部２０１からパケット及び検索結果を受信すると、検索結果に含まれる出力ポートにパケットを送信する。

【００３４】

また、送信パケット処理部２０２が受信する検索結果にカプセル化の指示が含まれる場合、送信パケット処理部２０２は、検索結果に含まれるカプセル化ヘッダ情報からＩＰパケットを作成し、サンプリング処理が実行されたパケットをデータ部分に含め、コレクタ装置１０４に送信する。

【００３５】

送信パケット処理部２０２によってコレクタ装置１０４へ送信されるパケットのフォーマットの一例を図１５に示す。サンプル情報送信フォーマット１５０１は、ｓＦｌｏｗヘッダ１５０２、取得パラメータ１５０３、及びパケットデータ１５０４を含む。サンプル情報送信フォーマット１５０１は、ＵＤＰのデータグラムとして送信される。送信パケット処理部２０２は、受信パケット処理部２０１から受信した、サンプリング処理に利用されたサンプリングレートを取得パラメータ１５０３のｓａｍｐｌｉｎｇ　ｒａｔｅに設定する。

【００３６】

サンプリングレート管理テーブル２０４は、フローの帯域とフローの種別に対応したサンプリングレートを管理し、検索処理部２０３がサンプリングレート制御処理（図７）を実行する際、参照される。

【００３７】

統計情報テーブル２０５は、収集されたフロー毎の統計情報を管理する。フローテーブル２０６は、ルータが受信したパケットのフローを特定する条件となる情報、及びフローに実行される処理を示す情報を含む。ルーティングテーブル２０７は、送信元のＩＰアドレスと宛先のＩＰアドレスに対応する出力ポートとが登録される。

【００３８】

図３は、本発明の第一の実施の形態のフローテーブル２０６を示す図である。

【００３９】

フローテーブル２０６は、フロー識別条件３０２及び統計制御情報３０３を含む。フロー識別条件３０２は、送信元ＩＰアドレス３１１、宛先ＩＰアドレス３１２、上位プロトコル３１３、送信元ポート番号３１４、宛先ポート番号３１５、及びその他情報３１６を

含む。

【００４０】

送信元ＩＰアドレス３１１には、ルータ１０１が受信したパケットを送信した送信元のＩＰアドレスが登録される。宛先ＩＰアドレス３１２には、ルータ１０１が受信したパケットの宛先のＩＰアドレスが登録される。上位プロトコル３１３には、例えば、ＴＣＰ及びＵＤＰ等が登録される。

【００４１】

送信元ポート番号３１４には、ルータ１０１が受信したパケットを送信した送信元のポート番号が登録される。宛先ポート番号３１５には、ルータ１０１が受信したパケットの宛先のポート番号が登録される。

【００４２】

その他情報３１６には、例えば、パケットの入出力ポート番号、送信元のＭＡＣアドレス、宛先のＭＡＣアドレス、ＴＡＧプロトコルの識別子、ＶＬＡＮ（Ｖｉｒｔｕａｌ　ＬＡＮ）の識別子、優先度、ＴＯＳ、及びＴＣＰフラグの一部等が登録される。

【００４３】

統計制御情報３０３は、登録処理３２１、登録処理レート３２２、統計収集３２３、サンプル処理３２４、送信制御３２５、フロー種別３２６、サンプリングレート３２７、及びその他情報３２８を含む。

【００４４】

登録処理３２１には、フローテーブル２０６に新たにエントリが登録されるか否かの情報が登録される。登録処理３２１に「１」が登録されると、検索処理部２０３は、新たにエントリを登録する。一方、登録処理３２１に「０」が登録されると、検索処理部２０３は、エントリを登録しない。

【００４５】

登録処理レート３２２には、フローテーブル２０６に新たにエントリが登録される場合、エントリが登録される比率が登録される。登録処理レート３２２に「１／１」が登録される場合、検索処理部２０３は、必ずエントリを新たに追加する。また、登録処理３２１に「０」が登録されている場合、新たにエントリが登録されないので、登録処理レート３２２には、「－」が登録される。

【００４６】

なお、フローＩＤ「Ｆ１２」の登録処理レート３２２に「１／１」が登録される。フローＩＤ「Ｆ１２」は、いずれのフロー識別条件と一致せず、かつ上位プロトコル３１３がＴＣＰであれば、自動的にフローテーブル２０６に新たにエントリを追加する。

【００４７】

統計収集３２３には、統計情報が収集されるか否かの情報が登録される。統計収集３２３に「１」が登録される場合、該当するエントリの統計情報が収集される。一方、統計収集３２３に「０」が登録される場合、該当するエントリの統計情報は収集されない。

【００４８】

サンプル処理３２４には、サンプリング処理が実行されるか否かの情報が登録される。サンプリング処理は、サンプリングレートに従って、送信パケット処理部２０２がパケットを複製し、複製したパケットをコレクタ装置１０４に送信する処理である。

【００４９】

サンプル処理３２４に「１」が登録されると、サンプリング処理がサンプリングレート３２７に登録された値を利用して実行される。サンプル処理３２４に「０」が登録されると、サンプリング処理は実行されない。

【００５０】

送信制御３２５は、送信制御処理が実行されるか否かの情報が登録される。なお、送信制御処理は、サンプリングレート３２７に登録された値を変更する処理であるが、詳細については、図７で説明する。送信制御３２５に「１」が登録されると、送信制御処理が実行される。

【００５１】
フロー種別３２６には、フローの種別が登録される。例えば、フロー種別３２６には、「０」、「１」及び「２」のいずれかが登録される。「０」は未知フローを示す。フローテーブル２０６に新たに登録されるフローは未知フローである。また、「１」は分析済みフローを示す。安全と判定されたフローは、分析済みフローである。「２」は異常フローを示す。異常と判定されたフローは、異常フローである。
【００５２】
また、フロー種別３２６には、「３」以上の値が登録され、異常フローの異常の度合いを示すようにしてもよい。
【００５３】
コレクタ装置１０４がフロー毎の統計情報を参照して、フロー種別を決定し、決定されたフロー種別をルータ１０１に送信する。ルータ１０１は、コレクタ装置１０４からフロー種別３２６を受信すると、制御部２０８を介してフローテーブル２０６のフロー種別３２６に登録する。また、フロー種別３２６は、ルータ１０１が登録してもよいし、管理端末２０９を介して管理者が登録してもよい。
【００５４】
サンプリングレート３２７には、サンプリング処理が実行される割合が登録される。例えば、サンプリングレート３２７に「１／１０００」が登録されると、該当するフローの１０００パケットに１個の割合でサンプリング処理が実行される。
【００５５】
その他情報３２８には、例えば、サンプル開始条件及びサンプル終了条件等が登録される。
【００５６】
図４は、本発明の第一の実施の形態の統計情報テーブル２０５を示す図である。
【００５７】
統計情報テーブル２０５は、フローＩＤ３０１及び統計情報４０１を含む。
【００５８】
フローＩＤ３０１は、フローテーブル２０６のフローＩＤ３０１と共通のＩＤであってフロー識別条件３０２と統計情報４０１とを対応させる。共通のＩＤを用いてフロー識別条件３０２と統計情報４０１を対応させる方法の代わりに、ポインタを用いてフロー識別条件３０２と統計情報４０１とを対応させる方法、及びフローテーブル２０６と統計情報テーブル２０５とを一つのテーブルとし保持する方法等を用いてもよい。
【００５９】
統計情報４０１は、パケット数４１１、バイト数４１２、帯域（ｂｐｓ）４１３、帯域（ｐｐｓ）４１４、開始時刻４１５、閾値４１６、及びその他情報４１７を含む。
【００６０】
パケット数４１１には、ルータ１０１が受信したパケットの数が積算された値が登録される。フローＩＤ３０１に該当するパケットをルータ１０１が受信すると、パケット数４１１に１が加算される。
【００６１】
バイト数４１２には、ルータ１０１が受信したパケットに含まれるパケット長が積算された値が登録される。フローＩＤ３０１に該当するパケットをルータ１０１が受信すると、ルータ１０１は、受信したパケットのヘッダ情報に含まれるパケット長をバイト数４１２に加算する。
【００６２】
帯域（ｂｐｓ）４１３には、フローが専有する帯域（ｂｐｓ）が登録される。帯域（ｐｐｓ）４１４には、フローが専有する帯域（ｐｐｓ）が登録される。
【００６３】
開始時刻４１５には、パケット数４１１に１が登録された時刻が登録される。すなわち、ルータ１０１が最初にフローＩＤに該当するパケットを受信した時刻が登録される。

【００６４】
閾値４１６には、統計情報を分析するため、コレクタ装置１０４に統計情報を送信するか否かの条件である閾値が登録される。通常、閾値４１６には、パケット数４１１の閾値が登録される。パケット数４１１が閾値４１６に登録された値に達すると、ルータ１０１は、当該フローの統計情報をコレクタ装置１０４に送信する。そして、コレクタ装置１０４のフロー分析処理部８０５がフローの統計情報を分析する。
【００６５】
なお、閾値４１６には、バイト数４１２及び開始時刻４１５に関する閾値が登録されてもよい。
【００６６】
その他情報４１７には、フローＩＤに含まれない項目が出現した種類の数、ルータ１０１が最後にパケットを受信した時刻等が登録される。なお、出現した種類の数は、例えば、送信元ＩＰアドレスがフローテーブル２０６のフロー識別条件３０２に含まれる場合、宛先ＩＰアドレスが何種類出現したかを示す。
【００６７】
図５は、本発明の第一の実施の形態のサンプリングレート管理テーブル２０４を示す図である。
【００６８】
サンプリングレート管理テーブル２０４は、帯域（ｐｐｓ）５０１及びサンプリングレート５０２を含む。
【００６９】
帯域（ｐｐｓ）５０１は、統計情報テーブル２０５の帯域（ｐｐｓ）４１４に対応する。なお、帯域（ｐｐｓ）ではなく、統計情報テーブル２０５の帯域（ｂｐｓ）４１３に対応する帯域（ｂｐｓ）を用いてもよい。
【００７０】
サンプリングレート５０２は、フローテーブル２０６のフロー種別３２６毎にサンプリングレート３２７に登録される値が登録される。具体的には、サンプリングレート５０２は、分析済みフロー（０）５１１、未知フロー（１）５１２、及び異常フロー（２）５１３に対応するサンプリングレート３２７に登録される値を含む。
【００７１】
検索処理部２０３は、帯域及びフロー種別からフローテーブル２０６に適切なサンプリングレート３２７を登録するためにサンプリングレート管理テーブル２０４を参照する。
【００７２】
なお、サンプリングレート管理テーブル２０４は、管理端末２０９から制御部２０８を介して登録内容を変更できる。
【００７３】
図６は、本発明の第一の実施の形態の検索処理のフローチャートである。
【００７４】
検索処理部２０３は、受信パケット処理部２０１からヘッダ情報を受信する（ステップ６０１）。
【００７５】
検索処理部２０３は、ヘッダ情報を受信すると、フローテーブル２０６を検索する（ステップ６０２）。また、検索処理部２０３は、ヘッダ情報を受信すると、ルーティングテーブル２０７を検索する（ステップ６２１）。なお、ステップ６０２～ステップ６１１の処理とステップ６２１～ステップ６２２の処理は並行して実行される。
【００７６】
具体的には、ステップ６０２の処理では、検索処理部２０３は受信したヘッダ情報に含まれる送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、及び宛先ポート番号等に基づいて、フローテーブル２０６のフロー識別条件３０２を検索し、フローＩＤ３０１を特定する。

【００７７】
そして、検索処理部２０３は、特定したフローＩＤ３０１の統計制御情報３０３に基づいて、ステップ６０３～ステップ６１１の処理の統計処理を実行する。
【００７８】
まず、検索処理部２０３は、フローテーブル２０６を参照し、登録処理３２１に登録された情報を取得する（ステップ６０３）。
【００７９】
次に、検索処理部２０３は、新たにエントリを追加するか否かを判定する（ステップ６０４）。具体的には、ステップ６０３の処理で取得した登録処理３２１に登録された情報が「１」である場合、検索処理部２０３は、新たにエントリを追加すると判定し、ステップ６０５の処理に進む。一方、ステップ６０３の処理で取得した登録処理３２１に登録された情報が「０」である場合、検索処理部２０３は、新たにエントリを追加しないと判定し、ステップ６０６の処理に進む。
【００８０】
検索処理部２０３は、登録処理レート３２２に基づいて、フローテーブル２０６に新たにエントリを追加する（ステップ６０５）。
【００８１】
次に、検索処理部２０３は、フローテーブル２０６の統計収集３２３及びサンプル処理３２４を参照する（ステップ６０６）。その後、処理がステップ６０７の処理とステップ６１０の処理に分岐する。
【００８２】
検索処理部２０３は、フローテーブル２０６を参照して、統計収集処理を実行するか否かを判定する（ステップ６０７）。具体的には、検索処理部２０３は、統計収集３２３に登録された情報が「１」である場合、統計収集処理を実行すると判定し、ステップ６０８の処理に進む。一方、検索処理部２０３は、統計収集３２３に登録された情報が「１」以外である場合、統計収集処理を実行しないと判定し、統計処理を終了する。
【００８３】
ステップ６０７の処理で、統計収集処理を実行すると判定された場合、検索処理部２０３は、統計情報テーブル２０５を更新する（ステップ６０８）。
【００８４】
具体的には、検索処理部２０３は、特定したフローＩＤのパケット数４１１に１を加算し、バイト数４１２に受信したヘッダ情報に含まれるパケット長を加算する。そして、検索処理部２０３は、帯域（ｂｐｓ）４１３及び帯域（ｐｐｓ）４１４に測定された帯域（ｂｐｓ）及び帯域（ｐｐｓ）を登録する。
【００８５】
また、ステップ６０７の処理と並行して、検索処理部２０３は、フローテーブル２０６を参照して、サンプリング処理を実行するか否かを判定する（ステップ６１０）。具体的には、検索処理部２０３は、サンプル処理３２４に登録された情報が「１」以外である場合、サンプリング処理を実行しないと判定する。一方、検索処理部２０３は、サンプル処理３２４に登録された情報が「１」である場合、サンプリング処理を実行すると判定し、ステップ６１１の処理に進む。
【００８６】
ステップ６１０の処理で、サンプリング処理を実行すると判定された場合、検索処理部２０３は、サンプリングレート３２７に登録された値を利用して、サンプリング処理を実行する（ステップ６１１）。具体的には、検索処理部２０３は、受信パケット処理部２０１へ送信する検索結果にサンプリング処理を実行する指示を追加する。また、検索処理部２０３は、送信パケット処理部２０２がサンプリング処理を実行する際、パケットをカプセル化するヘッダ情報を検索結果に追加する。
【００８７】
検索処理部２０３は、ステップ６０１の処理でヘッダ情報を受信すると、ルーティング

テーブル２０７を検索する（ステップ６２１）。検索処理部２０３は、ルーティングテーブル２０７を検索して、出力ポートを取得する（ステップ６２２）。

【００８８】

そして、検索処理部２０３は、ステップ６２２の処理で取得した出力ポートの情報を検索結果に追加し、検索処理を完了する（ステップ６２３）。なお、ステップ６１１の処理で、サンプリング処理が実行された場合、検索処理部２０３は、サンプリング処理を実行する指示、サンプリング処理に利用されたサンプリングレート、及びカプセル化するヘッダ情報を検索結果に追加する。

【００８９】

検索処理が完了する（ステップ６２３）と、検索処理部２０３は、サンプリングレート制御処理を実行する（ステップ６２４）。なお、サンプリングレート制御処理については、図７で詳細を説明する。また、検索処理が完了する（ステップ６２３）と、検索処理部２０３は、受信パケット処理部２０１に検索結果を送信する（ステップ６２５）。

【００９０】

図７は、本発明の第一の実施の形態のサンプリングレート制御処理（ステップ６２４）のフローチャートである。

【００９１】

まず、検索処理部２０３は、フローテーブル２０６を参照して、送信制御３２５に登録される情報を取得する（ステップ７０１）。

【００９２】

次に、検索処理部２０３は、取得した送信制御３２５に登録される情報に基づいて、送信制御処理を実行するか否かを判定する（ステップ７０２）。具体的には、取得した送信制御３２５に登録される情報が「１」である場合、検索処理部２０３は、送信制御処理を実行すると判定し、ステップ７０３の処理に進む。一方、取得した送信制御３２５に登録される情報が「１」以外である場合、検索処理部２０３は、送信制御処理を実行しないと判定し、サンプリングレート制御処理を終了する。

【００９３】

送信制御処理を実行すると判定された場合、検索処理部２０３は、フローテーブル２０６のフロー種別３２６及び統計情報テーブル２０５の帯域（ｐｐｓ）４１４を取得する（ステップ７０３）。

【００９４】

そして、検索処理部２０３は、サンプリングレート管理テーブル２０４を参照して、取得したフロー種別３２６及び帯域（ｐｐｓ）４１４に対応するサンプリングレートを算出する（ステップ７０４）。

【００９５】

なお、帯域（ｐｐｓ）４１４が測定されていない場合、サンプリングレート管理テーブル２０４の帯域（ｐｐｓ）５０１の「Ｄｅｆａｕｌｔ」に対応するサンプリングレートを参照する。

【００９６】

ステップ７０４の処理で算出されたサンプリングレートの値をフローテーブル２０６の該当するフローＩＤ３０１のサンプリングレート３２７に登録する（ステップ７０５）。

【００９７】

フローテーブル２０６に新たなサンプリングレートが登録されると、サンプリング制御処理を終了する。

【００９８】

なお、本実施の形態では、検索処理部２０３がサンプリングレート管理テーブル２０４を参照して、サンプリングレートを算出したが、帯域及びフロー種別から計算式を用いてサンプリングレートを算出してもよい。

【００９９】

また、ルータ１０１の検索処理部２０３がサンプリングレートを動的に変更する例を説

明したが、コレクタ装置１０４がサンプリングレート３２７を動的に変更できる。コレクタ装置１０４がサンプリングレート３２７を変更する方法については、図８で詳細を説明する。また、管理者が管理端末２０９を介してサンプリングレートを手動で変更できる。

【０１００】

図８は、本発明の第一の実施の形態のコレクタ装置１０４の機能ブロック図である。

【０１０１】

コレクタ装置１０４は、パケット送受信処理部８０１、統計情報パケット解析処理部８０２、データベース管理部８０３、サンプリング設定処理部８０４、フロー分析処理部８０５、フロー情報表示処理部８０６、入出力処理部８０７、及びサンプリングレート管理テーブル２０４を備える。

【０１０２】

また、コレクタ装置１０４の入出力処理部８０７に、入出力装置（マウス８２１、キーボード８２２及びディスプレイ８２３）が接続される。また、端末計算機がネットワークを介してコレクタ装置１０４に接続され、その端末計算機に備わる入出力装置によって、入出力がなされてもよい。

【０１０３】

パケット送受信処理部８０１は、ルータ１０１から統計情報パケットを受信する。また、パケット送受信処理部８０１は、制御情報パケットを送信する。

【０１０４】

統計情報パケット解析処理部８０２は、統計情報パケットに含まれるサンプリング処理が実行されたパケットのヘッダ情報を抽出する。そして、統計情報パケット解析処理部８０２は、抽出されたヘッダ情報をデータベース管理部８０３へ送信する。

【０１０５】

データベース管理部８０３は、統計情報パケット解析処理部８０２から受信したヘッダ情報に基づいて、統計情報データベース８１１を更新する。また、データベース管理部８０３は、サンプリング処理が実行されたパケットが属するフローの帯域を測定する。そして、データベース管理部８０３は、サンプリングレート、フロー種別、及び測定されたフローの帯域をサンプリング設定処理部８０４に送信する。

【０１０６】

また、データベース管理部８０３は、サンプリング処理が実行されたパケットが属するフローが閾値に設定された条件を満たす場合、統計情報データベース８１１の該当するフローの情報をフロー分析処理部８０５に送信する。閾値に設定された条件は、フローのパケット数が所定の数以上になった場合、及びフローの帯域（ｂｐｓ又はｐｐｓ）が所定の値以上になった場合等である。

【０１０７】

データベース管理部８０３は、フロー分析処理部８０５から送信される統計情報データベース８１１を検索する条件に基づいて、統計情報データベース８１１を検索し、検索した結果をフロー分析処理部８０５に送信する。

【０１０８】

また、データベース管理部８０３は、フロー分析処理部８０５から分析結果を受信し、受信した分析結果に基づいて、統計情報データベース８１１のフロー種別を登録又は更新する。

【０１０９】

サンプリング設定処理部８０４は、サンプリングレート管理テーブル２０４を参照して、データベース管理部８０３から受信するサンプリングレート、フロー種別、及び帯域に基づいて、該当するフローのサンプリングレートを算出する。そして、サンプリング設定処理部８０４は、算出されたサンプリングレートをルータ１０１に制御情報パケットとして送信する指示を、パケット送受信処理部８０１に送信する。

【０１１０】

なお、マウス８２１又はキーボード８２２の入力装置を介して管理者が直接サンプリン

グレートを設定できる。コレクタ装置１０４は、設定されたサンプリングレートをルータ１０１に送信できる。

【０１１１】

フロー分析処理部８０５は、サンプリング処理が実行されたパケットが属する統計情報データベース８１１の情報をデータベース管理部８０３から受信する。そして、フロー分析処理部８０５は、受信した統計情報データベース８１１の情報に基づいて、該当するフローのフロー種別を分析する。フロー分析処理部８０５は、該当するフローのフロー種別を分析した結果をデータベース管理部８０３に送信する。

【０１１２】

なお、フロー分析処理部８０５は、必要であれば、該当するフローに関連する情報を統計情報データベース８１１から検索する条件をデータベース管理部８０３に送信する。

【０１１３】

フロー情報表示処理部８０６は、統計情報データベース８１１から統計情報を受信する。そして、フロー情報表示処理部８０６は、統計情報にソートを実行し、又は統計情報をグラフ化する。

【０１１４】

サンプリング設定処理部８０４がサンプリングレートを算出し、算出されたサンプリングレートをルータ１０１に送信することによって、コレクタ装置１０４がフローテーブル２０６に含まれるサンプリングレート３２７を変更する。

【０１１５】

サンプリング設定処理部８０４によって算出されたサンプリングレートを受信したルータ１０１は、制御部２０８及び検索処理部２０３を介してフローテーブル２０６のサンプリングレート３２７を更新する。フローテーブル２０６に更新するフローに該当するフローＩＤが含まれない場合、ルータ１０１は、新たにフローテーブル２０６にエントリを追加する。

【０１１６】

なお、コレクタ装置１０４がフローテーブル２０６のサンプリングレート３２７を更新する場合、ルータ１０１は、送信制御３２５を「０」とし、ルータ１０１によってサンプリングレートが変更されないようにする。

【０１１７】

（第二実施形態）

本発明の第二の実施の形態を図９～図１３、及び図１６を用いて説明する。なお、第一の実施の形態と同一の構成要素には、同一の符号を付し、説明を省略する。

【０１１８】

本実施の形態のルータ１０１は、第一の実施の形態のルータ１０１がフローの統計情報を分析する機能を備える。

【０１１９】

図９は、本発明の第二の実施の形態のルータ１０１の機能ブロック図である。

【０１２０】

ルータ１０１は、受信パケット処理部２０１、送信パケット処理部２０２、検索処理部２０３、トラフィック統計分析処理部９０１、サンプリングレート管理テーブル２０４、統計情報テーブル２０５、フローテーブル２０６、ルーティングテーブル２０７、アイテムセットテーブル９０２、閾値管理テーブル９０３、及び制御部２０８を備える。

【０１２１】

統計情報テーブル２０５は、検索処理部２０３及びトラフィック統計分析処理部９０１によって参照される。

【０１２２】

トラフィック統計分析処理部９０１は、トラフィック情報を構成する各項目を任意に組み合わせたアイテムセットテーブル９０２を生成し、アイテムセットテーブル９０２のエントリの統計情報を収集することによって特徴的なトラフィックを抽出する。

【０１２３】
アイテムセットテーブル９０２は、トラフィック情報を構成する各項目の任意の組み合わせを示す。なお、アイテムセットテーブル９０２は、図１０で詳細を説明する。閾値管理テーブル９０３は、統計情報テーブル２０５の閾値１２０６をフローの帯域及びフローの種別に応じて変更する場合に参照される。なお、閾値管理テーブル９０３は、図１２で詳細を説明する。
【０１２４】
図１０は、本発明の第二の実施の形態のアイテムセットテーブル９０２を示す図である。
【０１２５】
本実施の形態では、トラフィック情報を構成する項目は、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、及び宛先ポート番号の４種類である。なお、他にトラフィック情報を構成する項目として、例えば、送信元ＭＡＣアドレス、宛先ＭＡＣアドレス、ＶＬＡＮ－ＩＤ、プロトコル番号、優先度、ＴＯＳ、及びＴＣＰフラグ等を用いてもよい。
【０１２６】
アイテムセットテーブル９０２は、トラフィック情報を構成する項目を任意に組み合わせて生成された各テーブルを含む。
【０１２７】
本実施の形態では、アイテムセットテーブル９０２は、テーブルＡ１１０１、テーブルＢ１１０２、テーブルＣ１１０３、及びテーブルＤ１１０４を含む。テーブルＡ１１０１は、トラフィック情報を構成する項目が１項目である。テーブルＢ１１０２は、トラフィック情報を構成する項目が２項目である。テーブルＣ１１０３は、トラフィック情報を構成する項目が３項目である。テーブルＤ１１０４は、トラフィック情報を構成する項目が４項目である。
【０１２８】
なお、本実施の形態では、アイテムセットテーブル９０２に含まれるテーブルの数が４つの場合を説明したが、アイテムセットテーブル９０２は、少なくとも一つのテーブルを含み、トラフィック情報を構成する項目は４種類なので、アイテムセットテーブル９０２は最大４つのテーブルを含む。アイテムセットテーブル９０２に含まれる各テーブルは、エントリ番号１１１１及び項目１１１２を含む。
【０１２９】
エントリ番号１１１１は、アイテムセットテーブル９０２に含まれるエントリの一意な識別子である。項目１１１２は、種類１１２１及び値１１２２を含む。種類１１２１には、トラフィック情報を構成する項目が登録される。値１１２２には、種類１１２１に登録されたトラフィック情報を構成する項目の値が登録される。
【０１３０】
図１１は、本発明の第二の実施の形態の統計情報テーブル２０５を示す図である。
【０１３１】
統計情報テーブル２０５は、トラフィック統計分析処理部９０１及び検索処理部２０３によって参照される。
【０１３２】
統計情報テーブル２０５は、エントリ番号１１１１、パケット数１２０１、バイト数１２０２、帯域（ｂｐｓ）１２０３、帯域（ｐｐｓ）１２０４、開始時刻１２０５、閾値１２０６、及びその他情報１２０７を含む。
【０１３３】
エントリ番号１１１１は、アイテムセットテーブル９０２及びフローテーブル２０６のエントリ番号と共通の識別子であって、アイテムセットテーブル９０２と統計情報テーブル２０５とを対応させる。
【０１３４】

なお、本実施の形態では、トラフィック統計分析処理部９０１及び検索処理部２０３が一つの統計情報テーブル２０５を参照するが、トラフィック統計分析処理部９０１が参照する統計情報テーブルと検索処理部２０３が参照する統計情報テーブルとを互いに独立して保持してもよい。

【０１３５】

パケット数１２０１には、ルータ１０１が受信したパケットの数が積算された値が登録される。具体的には、エントリ番号１１１１に該当するパケットをルータ１０１が受信すると、ルータ１０１は、パケット数１２０１に１が加算される。

【０１３６】

バイト数１２０２には、ルータ１０１が受信したパケットに含まれるパケット長が積算された値が登録される。エントリ番号１１１１に該当するパケットをルータ１０１が受信すると、ルータ１０１は、受信したパケットのヘッダ情報に含まれるパケット長をバイト数１２０２に加算する。

【０１３７】

帯域（ｂｐｓ）１２０３には、該当するエントリ番号が専有する帯域（ｂｐｓ）が登録される。帯域（ｐｐｓ）１２０４には、該当するエントリ番号が専有する帯域（ｐｐｓ）が登録される。

【０１３８】

開始時刻１２０５には、パケット数１２０１に１が登録された時刻が登録される。すなわち、ルータ１０１が最初にフローＩＤに該当するパケットを受信した時刻が登録される。

【０１３９】

閾値１２０６には、統計テーブル作成部１００２がフロー分析部１００３に情報を送信する場合の条件が登録される。通常、閾値１２０６には、パケット数１２０１の閾値が登録される。パケット数１２０１が閾値１２０６に登録された値に達すると、統計テーブル作成部１００２がフロー分析部１００３に情報を送信する。

【０１４０】

なお、閾値１２０６には、バイト数１２０２及び開始時刻１２０５に関する閾値が登録されてもよい。

【０１４１】

その他情報１２０７には、アイテムセットテーブル９０２の項目１１０１に含まれない項目が出現した種類の数、ルータ１０１が最後にパケットを受信した時刻等が登録される。例えば、出現した種類の数は、送信元ＩＰアドレスがアイテムセットテーブル９０２に含まれる場合、アイテムセットテーブル９０２に含まれない項目である宛先ＩＰアドレスが出現した種類の数である。

【０１４２】

図１２は、本発明の第二の実施の形態の閾値管理テーブル９０３を示す図である。

【０１４３】

閾値管理テーブル９０３は、帯域（ｐｐｓ）１４０１及び閾値１４０２を含む。

【０１４４】

帯域（ｐｐｓ）１４０１は、統計情報テーブル２０５の帯域（ｐｐｓ）１２０４に対応する。なお、帯域はｐｐｓを用いたが、ｂｐｓを用いてもよい。

【０１４５】

閾値１４０２には、フロー種別毎に閾値の比率が登録される。統計情報テーブル２０５の閾値１２０６がパケット数１２０１の閾値である場合、アイテムセットテーブル９０２によって特定されるエントリ番号１１１１毎に定められた閾値に閾値１４０２に登録される比率を乗算した値が統計情報テーブル２０５の閾値１２０６に設定される。

【０１４６】

閾値管理テーブル９０３は、帯域及びフロー種別から統計情報テーブル２０５の閾値１２０６に適切な値を登録するために参照される。なお、閾値管理テーブル９０３は、管理

端末２０９から制御部２０８を介して変更できる。

【０１４７】

図１３は、本発明の第二の実施の形態のトラフィック統計分析処理部９０１の機能ブロック図である。

【０１４８】

トラフィック統計分析処理部９０１は、ヘッダ情報蓄積部１００１、統計テーブル作成部１００２、フロー分析部１００３、統計情報パケット生成部１００４、及び閾値設定部１００５を備える。

【０１４９】

ヘッダ情報蓄積部１００１は、受信パケット処理部２０１からヘッダ情報を受信し、受信したヘッダ情報を統計テーブル作成部１００２に送信する。

【０１５０】

統計テーブル作成部１００２は、受信したヘッダ情報に含まれるトラフィック情報を構成する項目（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、及び宛先ポート番号）の任意の組み合わせを生成する。そして、統計テーブル作成部１００２は、アイテムセットテーブル９０２を参照して、生成された組み合わせに一致するエントリを検索する。

【０１５１】

アイテムセットテーブル９０２に一致するエントリが存在する場合、統計テーブル作成部１００２は、一致するエントリのエントリ番号１１１１に基づいて、統計情報テーブル２０５の該当するパケット数１２０１、バイト数１２０２、帯域（ｂｐｓ）１２０３、帯域（ｐｐｓ）１２０４、開始時刻１２０５、及び閾値１２０６を更新する。

【０１５２】

一方、アイテムセットテーブル９０２に一致するエントリが存在しない場合、統計情報テーブル作成部１００２は、アイテムセットテーブル９０２及び統計情報テーブル２０５に新たに生成された組み合わせのエントリを追加する。

【０１５３】

アイテムセットテーブル９０２又は統計情報テーブル２０５に新たにエントリを追加できない場合、新たに追加するエントリが既登録のエントリに上書きされる。上書きされる既登録のエントリを選択する方法として、統計情報テーブル２０５のパケット数１２０１が少ないエントリを選択する方法、最後に更新された時刻が一番古いエントリを選択する方法、及びランダムにエントリを選択する方法等がある。

【０１５４】

新たにエントリを追加する場合に、生成されたトラフィック情報を構成する項目の組み合わせがアイテムセットテーブル９０２に登録される。統計情報テーブル２０５のパケット数１２０１に「１」が登録され、バイト数１２０２にはヘッダ情報に含まれるパケット長が登録される。また、帯域（ｂｐｓ）１２０３及び帯域（ｐｐｓ）１２０４には、ルータ１０１によって測定された帯域が登録される。

【０１５５】

開始時刻１２０５には、パケット数１２０１に１が登録された時刻が登録される。閾値４１６には、予め設定された値が登録される。なお、閾値４１６に登録される予め設定された値は、アイテムセットテーブル９０２の組み合わせ毎に設定され、制御部２０８を介して管理者が変更できる。

【０１５６】

統計テーブル作成部１００２が統計情報テーブル２０５のエントリを更新する方法を説明する。なお、図１の端末１からサーバ１へのパケットのフローを例に説明する。ここで、端末１のＩＰアドレスをＸ１、サーバ１のＩＰアドレスをＹ１、送信元ポート番号をＡ１、宛先ポート番号をＢ１とする。

【０１５７】

統計テーブル作成部１００２は、ヘッダ情報蓄積部１００１からヘッダ情報を受信する

と、テーブルＡ１１０１の種類１１２１及び値１１２２に各々送信元ＩＰアドレス及びＸ１を登録して、送信元ＩＰアドレスがＸ１となるエントリを登録する。同様に、統計テーブル作成部１００２は、宛先アドレスＹ１となるエントリ、送信元ポート番号がＡ１となるエントリ、及び宛先ポート番号がＢ１となるエントリをテーブルＡ１１０１に登録する。これによって、テーブルＡ１１０１が、更新又は新たに作成される。

【０１５８】

また、統計テーブル作成部１００２は、テーブルＢ１１０２の項目Ａ含まれる種類１１２１及び値１１２２に各々送信元ＩＰアドレス及びＸ１を登録して、項目Ｂに含まれる種類１１２１及び値１１２２に各々宛先ＩＰアドレス及びＹ１を登録して、送信元ＩＰアドレスがＸ１であって宛先ＩＰアドレスがＹ１となるエントリを登録する。同様に送信元ＩＰアドレスがＸ１であって送信元ポート番号がＡ１となるエントリ、送信元ＩＰアドレスがＸ１であって宛先ポート番号がＢ１となるエントリ、宛先ＩＰアドレスがＹ１であって送信元ポート番号がＡ１となるエントリ、宛先ＩＰアドレスがＹ１であって宛先ポート番号がＢ１となるエントリ、及び送信元ポート番号がＡ１であって宛先ポート番号がＢ１となるエントリをテーブルＢ１１０２に登録する。これによって、テーブルＢ１１０２は、更新又は新たに作成される。

【０１５９】

同様に、統計テーブル作成部１００２は、送信元ＩＰアドレスがＸ１であって宛先ＩＰアドレスがＹ１であって送信元ポート番号がＡ１となるエントリ、送信元ＩＰアドレスがＸ１であって宛先ＩＰアドレスがＹ１であって宛先ポート番号がＢ１となるエントリ、送信元ＩＰアドレスがＸ１であって送信ポート番号がＡ１であって宛先ポート番号がＢ１となるエントリ、及び宛先ＩＰアドレスがＹ１であって送信ポート番号Ａ１であって宛先ポート番号がＢ１となるエントリをテーブルＣ１１０３に登録する。これによって、テーブルＣ１１０３は、更新又は新たに作成される。

【０１６０】

同様に、統計テーブル作成部１００２は、送信元アドレスがＸ１であって宛先ＩＰアドレスがＹ１であって送信元ポート番号がＡ１であって宛先ポート番号がＢ１となるエントリをテーブルＤ１１０４に登録する。これによって、テーブルＤ１１０４は、更新又は新たに作成される。

【０１６１】

なお、本実施の形態では、統計テーブル作成部１００２は、全項目の組み合わせをアイテムセットテーブル９０２に登録したが、必要に応じて省略できる。

【０１６２】

例えば、送信元ＩＰアドレスＸ１と宛先ポート番号Ｂ１とのエントリのみをテーブルＢ１１０２に登録し、他の組み合わせがテーブルＢ１１０２に登録しない。なお、各テーブルに登録される組み合わせは、管理者が制御部２０８を介して設定する。

【０１６３】

また、統計テーブル作成部１００２は、アイテムセットテーブル９０２及び統計情報テーブル２０５を更新すると、統計情報テーブル２０５の閾値１２０６を参照して、フロー分析部１００３へ情報を送信するか否かを判定する。

【０１６４】

通常、統計テーブル作成部１００２は、統計情報テーブル２０５に含まれるパケット数１２０１と閾値１２０６とを比較する。具体的には、統計テーブル作成部１００２は、パケット数１２０１が閾値１２０６以上であると、アイテムセットテーブル９０２及び統計情報テーブル２０５の該当するエントリの情報をフロー分析部１００３に送信すると判定し、その情報をフロー分析部１００３に判定する。

【０１６５】

また、統計テーブル作成部１００２は、フロー分析部１００３に情報を送信すると同時に、統計情報テーブル２０５の該当するエントリ（パケット数１２０１、バイト数１２０２、開始時刻１２０５、及びその他情報１２０７）に「０」を登録する。なお、閾値１２

０６については、予め設定されている値が登録される。
【０１６６】
一方、統計テーブル作成部１００２は、パケット数１２０１が閾値１２０６未満であると、アイテムセットテーブル９０２及び統計情報テーブル２０５の該当するエントリの情報をフロー分析部１００３に送信しないと判定する。
【０１６７】
なお、閾値１２０６には、バイト数１２０２の閾値、開始時刻１２０５の閾値、又はその他情報１２０７の閾値が登録されてもよい。この場合、統計テーブル作成部１００２は、閾値１２０６に対応して、バイト数１２０２、開始時刻１２０５、又はその他情報１２０７を参照して、フロー分析部１００３に情報を送信するか否かを判定する。
【０１６８】
統計テーブル作成部１００２が開始時刻４１５を参照してフロー分析部１００３に情報を送信するか否かを判定する場合、現在時刻から開始時刻１２０５を引き、継続時間を算出する。そして、統計テーブル作成部１００２は、算出された継続時間と閾値１２０６とを比較する。算出された継続時間が閾値１２０６以上であれば、統計テーブル作成部１００２は、フロー分析部１００３に情報を送信すると判定する。一方、算出された継続時間が閾値１２０６未満であれば、統計テーブル作成部１００２は、フロー分析部１００３に情報を送信しないと判定する。
【０１６９】
なお、閾値１２０６が統計情報テーブル２０５に含まれるどの情報の閾値であるかについては、統計テーブル作成部１００２が保持し、制御部２０８から管理者が変更できる。
【０１７０】
なお、本実施の形態では、統計テーブル作成部１００２は、一つの閾値１２０６を参照するが、複数の閾値を参照するようにしてもよい。
【０１７１】
この場合、統計情報テーブル２０５は、複数の閾値を含む。統計テーブル作成部１００２は、複数の閾値のうち予め設定された数の閾値を満たすと、該当するエントリの情報をフロー分析部１００３に送信する。
【０１７２】
例えば、第一の閾値にはパケット数１２０１の閾値が登録され、第二の閾値には開始時刻１２０５に関する閾値が登録される。統計テーブル作成部１００２は、第一の閾値を満たし、かつ第二の閾値を満たす場合、該当するエントリの情報をフロー分析部１００３に送信する。また、統計テーブル作成部１００２は、第一の閾値及び第二の閾値の少なくとも一方を満たす場合にフロー分析部１００３へ送信してもよい。
【０１７３】
また、閾値１２０６が全てのエントリに共通の値である場合、すなわちフロー毎に閾値を設定しない場合、統計テーブル作成部１００２に全てのエントリに共通の閾値を保持し、統計情報テーブル２０５に閾値１２０６を保持しないようにして、使用するメモリ量を節約してもよい。
【０１７４】
フロー分析部１００３は、統計テーブル作成部１００２から送信されたアイテムセットテーブル９０２及び統計情報テーブル２０５の該当するエントリの情報に基づいて、トラフィックの帯域と種別を判定する。
【０１７５】
なお、フロー分析部１００３は、必要に応じてアイテムセットテーブル９０２及び統計情報テーブル２０５から他のエントリ情報を検索し、エントリの種別を分析する。
【０１７６】
フロー分析部１００３で分析した結果及び該当するエントリの統計情報は、統計情報パケット生成部１００４に送信される。なお、エントリの帯域、エントリの種別、及びエントリ番号１１１１は閾値設定部１００５にも送信される。また、フロー分析部１００３は

、エントリの種別に異常と分析すると、そのエントリの統計情報を制御部２０８に送信する。

【０１７７】

統計情報パケット生成部１００４は、フロー分析部１００３から受信した分析結果及び統計情報を送信フォーマットに整形し、ルータ１０１の受信パケット処理部２０１に送信する。

【０１７８】

統計情報パケット生成部１００４によって受信パケット処理部２０１へ送信される統計情報送信フォーマット１６０１の一例を図１６に示す。統計情報送信フォーマット１６０１は、ヘッダ情報１６０２及び統計情報１６０３を含む。統計情報送信フォーマット１６０１は、ＳＣＴＰ、ＴＣＰ、又はＵＤＰのデータグラムとして送信される。

【０１７９】

統計情報１６０３には、統計情報を収集するために利用されたサンプリングレートと、統計情報テーブル２０５で収集した統計情報と、アイテムセットテーブル９０２の項目１１０２が含まれる。なお、統計情報の送信先となるコレクタ装置１０４のアドレスは、管理者によって制御部２０８を介して、統計情報パケット生成部１００４に事前に設定される。

【０１８０】

閾値設定部１００５は、閾値管理テーブル９０３を参照して、フロー分析部１００３から受信したエントリの帯域及びエントリの種別に基づいて、次に統計テーブル作成部１００２からフロー分析部１００３へ送信する間隔を決定する閾値１２０６を算出する。具体的には、閾値設定部１００５は、閾値管理テーブル９０３を参照し、該当するエントリの帯域（ｐｐｓ）及び該当するエントリの種別に対応する比率を算出する。そして、閾値設定部１００５は、算出した比率を統計テーブル作成部１００２に送信する。

【０１８１】

統計テーブル作成部１００２は、該当するエントリの閾値１２０６に登録された値に受信した比率を乗算し、新しい閾値１２０６を算出する。算出した閾値を該当するエントリの閾値１２０６に登録する。

【０１８２】

次に、第一の実施の形態の受信パケット処理部２０１に追加した機能について説明する。

【０１８３】

本実施の形態の受信パケット処理部２０１は、パケットを受信する場合、ヘッダ情報を検索処理部２０３に送信すると同時に、トラフィック統計分析処理部９０１にもヘッダ情報を送信する。また、受信パケット処理部２０１は、トラフィック統計分析処理部９０１から受信した統計情報パケットを送信パケット処理部２０２に送信する。受信パケット処理部２０１の他の動作は、第一の実施の形態と同じである。

【０１８４】

本実施の形態の制御部２０８は、トラフィック統計分析処理部９０１のフロー分析部１００３から受信したエントリの種別が異常である旨の情報を検索処理部２０３に送信する。また、異常である旨の情報を受信した検索処理部２０３は、フローテーブル２０６に該当するエントリが存在するか検索し、該当するエントリが存在する場合、フロー種別３２６に異常フローと設定する。

【０１８５】

送信パケット処理部２０２、検索処理部２０３の他の動作は第一の実施の形態と同じである。

【０１８６】

（第三実施形態）

本発明の第三の実施の形態を図１４を用いて説明する。

【０１８７】

本発明の第三の実施の形態は、第二の実施の形態のトラフィックの統計を分析する機能をネットワーク制御装置１３０１に実装する。

【０１８８】

図１４は、本発明の第三の実施の形態のネットワーク制御装置１３０１の機能ブロック図である。

【０１８９】

ネットワーク制御装置１３０１は、ＣＰＵ（Central Processing Unit）１３０２、ワークメモリ１３０３、プログラムメモリ１３０４、統計情報データベース１３０５、通信インタフェース（通信Ｉ／Ｆ）１３０６、及び入出力装置１３０７を備える。また、これらは、各々バス１３０８によって接続される。

【０１９０】

パケット送受信処理部１３１１、統計情報パケット解析処理部１３１２、トラフィック統計分析処理部１３１３は、プログラムメモリ１３０４に格納される。ＣＰＵ１３０２は、プログラムメモリ１３０４に格納される各種プログラム等をワークメモリにロードし、実行する。

【０１９１】

パケット送受信処理部１３１１は、ＩＰパケットを送受信する。統計情報パケット解析処理部１３１２は、ルータ１０１から送信されたパケットに含まれるヘッダ情報を取得する。トラフィック統計分析処理部１３１３は、第二の実施の形態のトラフィック統計分析処理部９０１と同様の処理を実行する。トラフィック統計分析処理部１３１３は、第二の実施の形態のトラフィック統計分析処理部９０１は、統計情報パケット生成部１００４が生成したパケットを受信パケット処理部２０１に送信するのに対して、本実施の形態のトラフィック統計分析処理部１３１３は、統計情報パケット生成部１００４が生成したパケットをパケット送受信処理部１３１１に送信する点で異なる。

【０１９２】

統計情報データベース１３０５は、アイテムセットテーブル９０２及び統計情報テーブル２０５を含む。また、統計情報データベース１３０５は、トラフィック統計分析処理部１３１３によって参照される。

【０１９３】

ルータ１０１は、第一の実施の形態と同様の構成である。ルータ１０１によってサンプリング処理が実行されたパケットのヘッダ情報がネットワーク制御装置１３０１及びコレクタ装置１０４に送信される。

【０１９４】

なお、ルータ１０１を通過するパケットの数が少ない場合、パケットを複製して、複製されたパケットをネットワーク制御装置１３０１に送信するようにしてもよい。

【産業上の利用可能性】

【０１９５】

本発明は、ネットワークの運用管理に利用できる。特に、ネットワークに流れるトラフィックを詳細に管理する場合及び大規模のネットワークが適用される場合に効果的である。

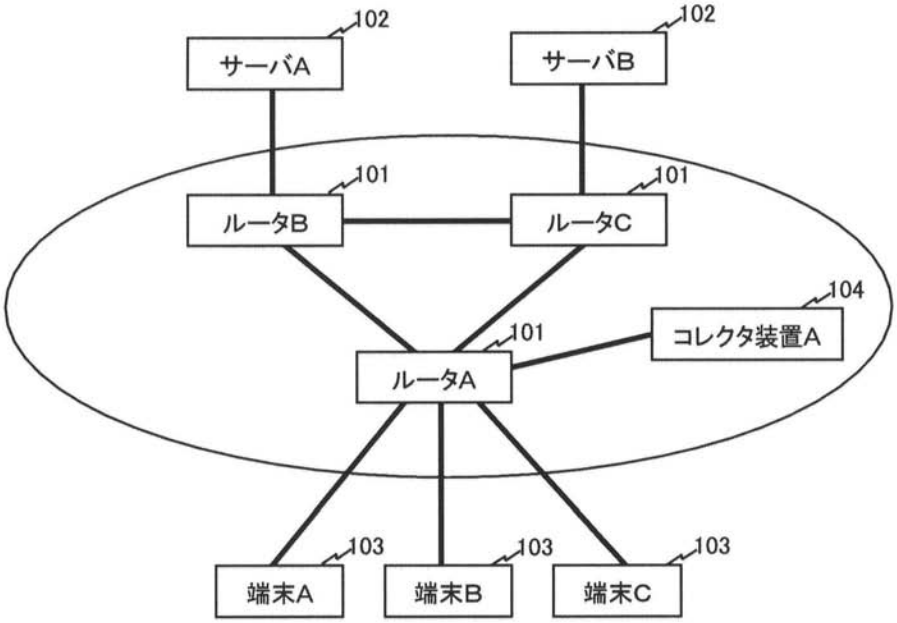
【図面の簡単な説明】

【０１９６】

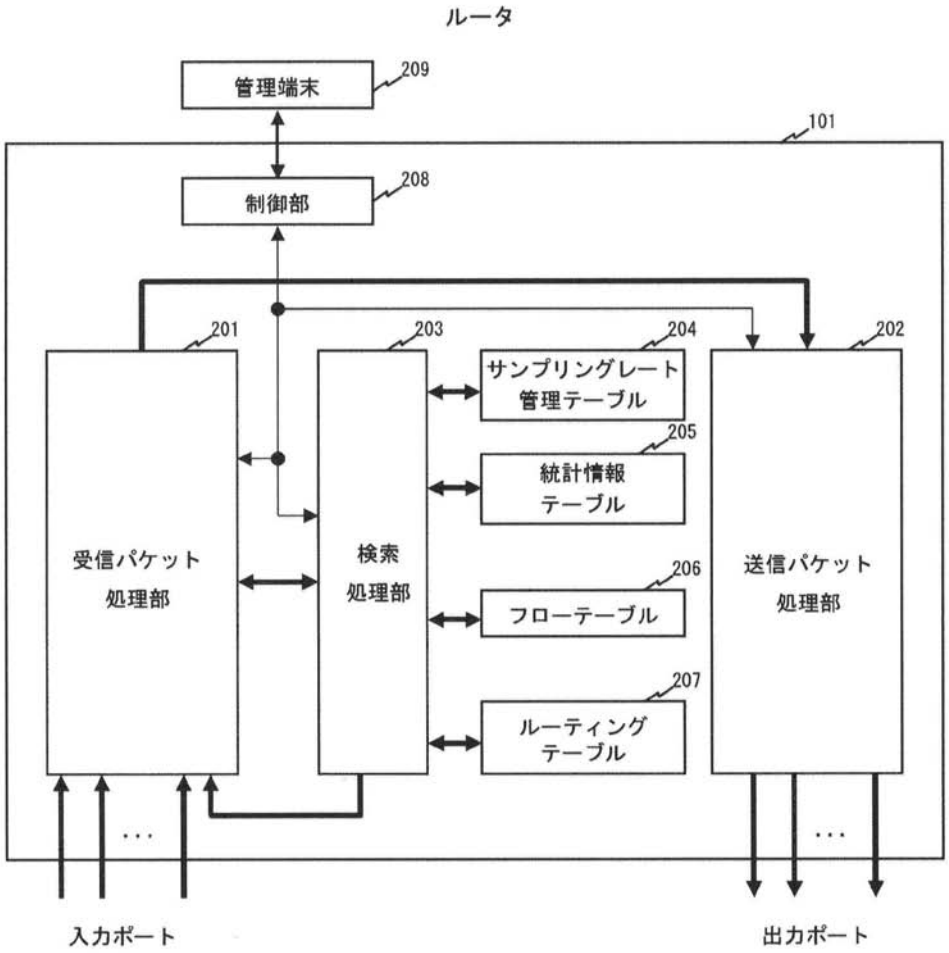
【図１】本発明の第一の実施の形態の通信統計情報収集システムを示す図である。
【図２】本発明の第一の実施の形態のルータの機能ブロック図である。
【図３】本発明の第一の実施の形態のフローテーブルを示す図である。
【図４】本発明の第一の実施の形態の統計情報テーブルを示す図である。
【図５】本発明の第一の実施の形態のサンプリングレート管理テーブルを示す図である。
【図６】本発明の第一の実施の形態の検索処理部の動作のフローチャートである。
【図７】本発明の第一の実施の形態のサンプリングレート制御処理のフローチャートである。

【図８】本発明の第一の実施の形態のコレクタ装置の機能ブロック図である。
【図９】本発明の第二の実施の形態のルータの機能ブロック図である。
【図１０】本発明の第二の実施の形態のアイテムセットテーブルを示す図である。
【図１１】本発明の第二の実施の形態の統計情報テーブルを示す図である。
【図１２】本発明の第二の実施の形態の閾値管理テーブルを示す図である。
【図１３】本発明の第二の実施の形態のトラフィック統計分析処理部の機能ブロック図である。
【図１４】本発明の第三の実施の形態の統計情報収集装置の機能ブロック図である。
【図１５】本発明の第一の実施の形態のサンプル情報送信フォーマットを示す図である。
【図１６】本発明の第二の実施の形態の統計情報送信フォーマットを示す図である。
【符号の説明】
【０１９７】
１０１　ルータ
１０２　サーバ
１０３　端末
１０４　コレクタ装置
２０１　受信パケット処理部
２０２　送信パケット処理部
２０３　検索処理部
２０４　サンプリングレート管理テーブル
２０５　統計情報テーブル
２０６　フローテーブル
２０７　ルーティングテーブル
２０８　制御部
２０９　管理端末
８０１　パケット送受信処理部
８０２　統計情報パケット解析処理部
８０３　データベース管理部
８０４　サンプリング設定処理部
８０５　フロー分析処理部
８０６　フロー情報表示処理部
８０７　入出力処理部
９０１　トラフィック統計分析処理部
９０２　アイテムセットテーブル
９０３　パケットカウントテーブル
１３０１　ネットワーク制御装置
１３０２　ＣＰＵ
１３０３　ワークメモリ
１３０４　プログラムメモリ
１３０５　統計情報データベース

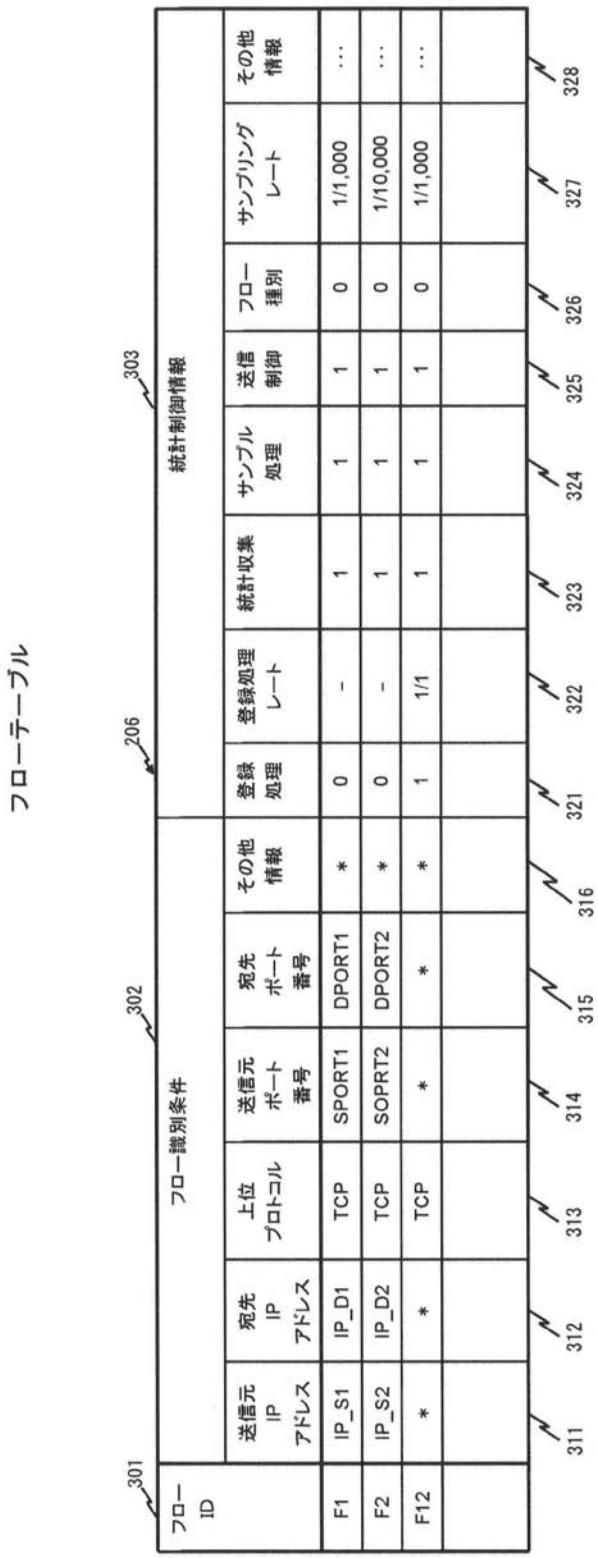
【図１】


102
サーバA
102
サーバB
101
ルータB
101
ルータC
104
コレクタ装置A
101
ルータA
103
端末A
103
端末B
103
端末C

【図２】

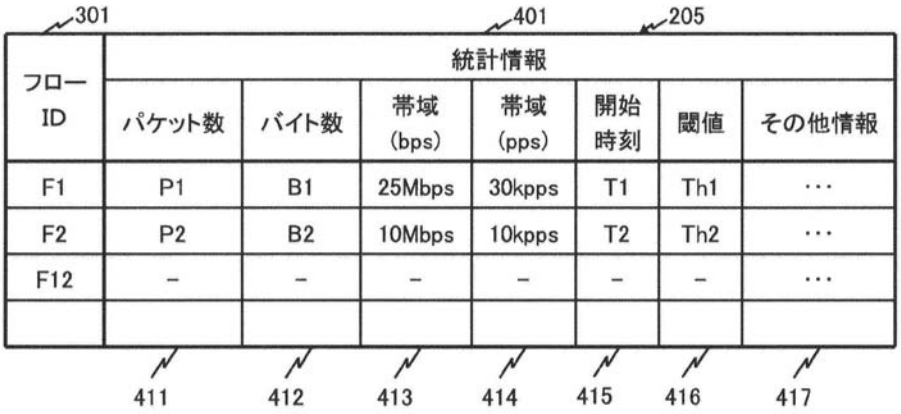

ルータ
管理端末
209
101
制御部
208
201
203
204
202
サンプリングレート
管理テーブル
205
統計情報
テーブル
受信パケット
処理部
検索
処理部
206
フローテーブル
送信パケット
処理部
207
ルーティング
テーブル
入力ポート
出力ポート

【図３】


フローテーブル
301
302
303
206
フロー識別条件
統計制御情報
フローID
送信元IPアドレス
宛先IPアドレス
上位プロトコル
送信元ポート番号
宛先ポート番号
その他情報
登録処理
登録処理レート
統計収集
サンプル処理
送信制御
フロー種別
サンプリングレート
その他情報
F1
IP_S1
IP_D1
TCP
SPORT1
DPORT1
*
0
-
1
1
1
0
1/1,000
…
F2
IP_S2
IP_D2
TCP
SOPRT2
DPORT2
*
0
-
1
1
1
0
1/10,000
…
F12
*
*
TCP
*
*
*
1
1/1
1
1
1
0
1/1,000
…
311
312
313
314
315
316
321
322
323
324
325
326
327
328

【図４】

統計情報テーブル

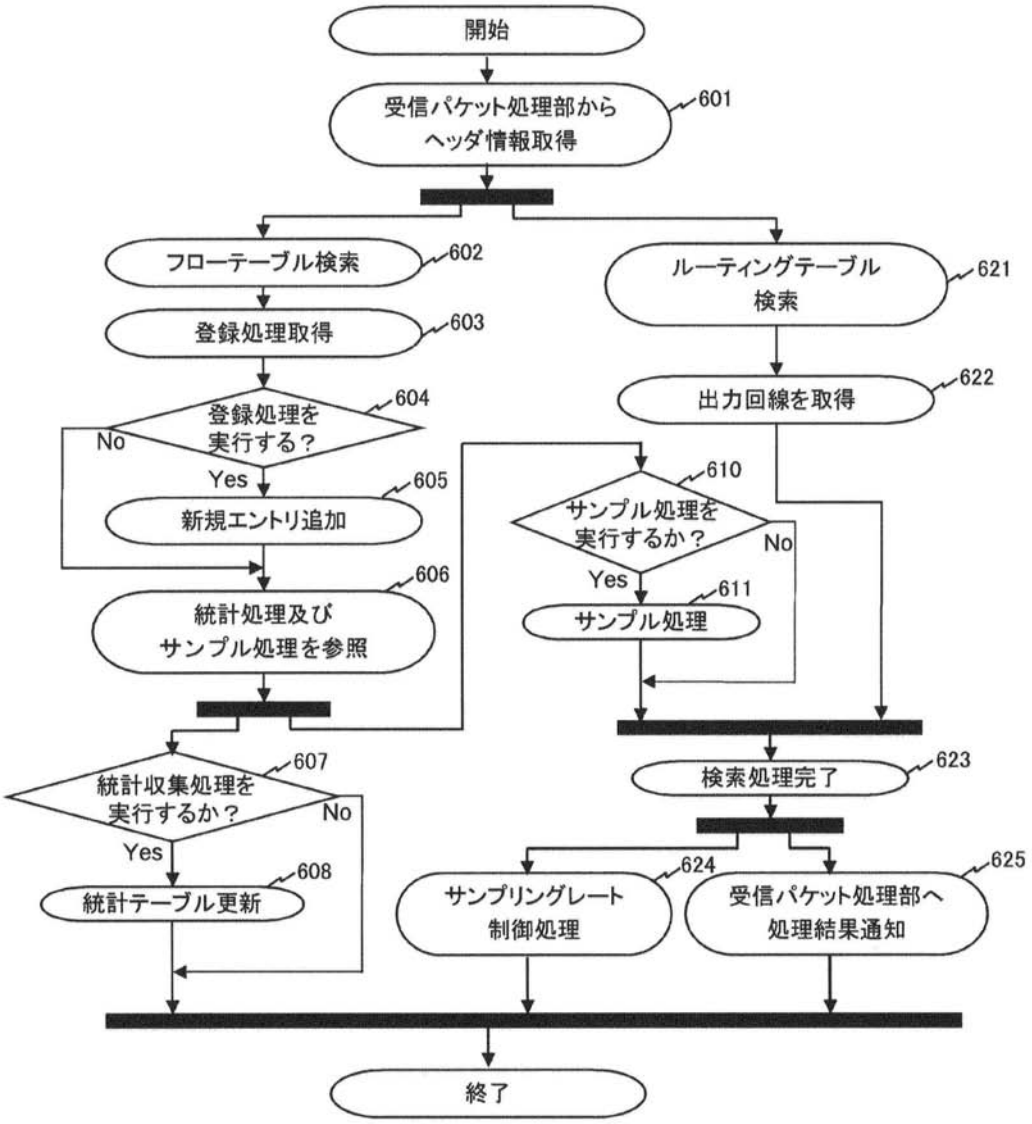

301
401
205
フローID
統計情報
パケット数
バイト数
帯域(bps)
帯域(pps)
開始時刻
閾値
その他情報
F1
P1
B1
25Mbps
30kpps
T1
Th1
・・・
F2
P2
B2
10Mbps
10kpps
T2
Th2
・・・
F12
－
－
－
－
－
－
・・・
411
412
413
414
415
416
417

【図５】

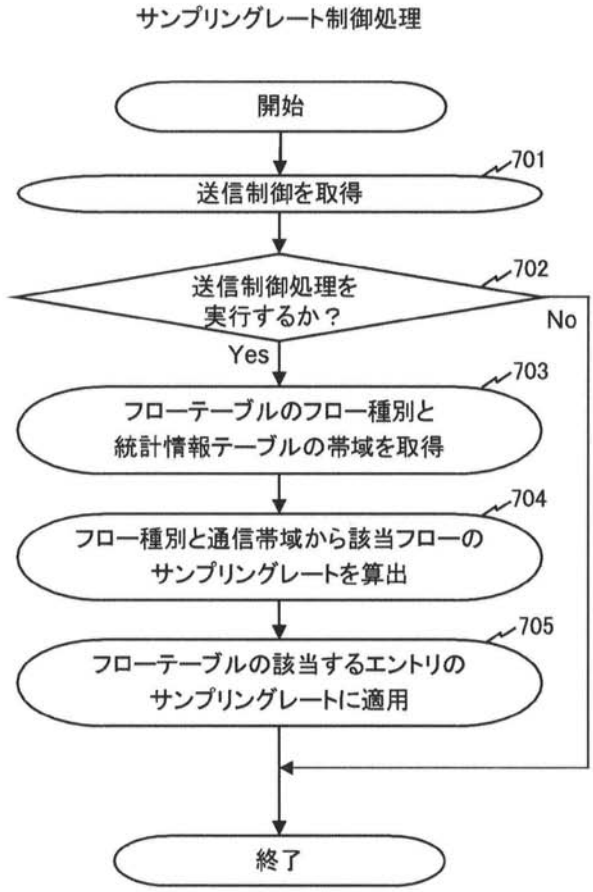
サンプリングレート管理テーブル

501	502		204
帯域 (pps)	サンプリングレート		
	分析済みフロー(0)	未知フロー(1)	異常フロー(2)
Default	1/10,000	1/1,000	1/100
～100	1/10,000	1/1,000	1/10
101～1,000	1/10,000	1/1,000	1/100
1,001～10,000	1/100,000	1/10,000	1/1,000
10,001～100,000	1/1,000,000	1/100,000	1/10,000
100,001～1,000,000	1/10,000,000	1/1,000,000	1/100,000
1,000,001～10,000,000	1/100,000,000	1/10,000,000	1/1,000,000
10,000,001～100,000,000	1/1,000,000,000	1/100,000,000	1/10,000,000
	511	512	513

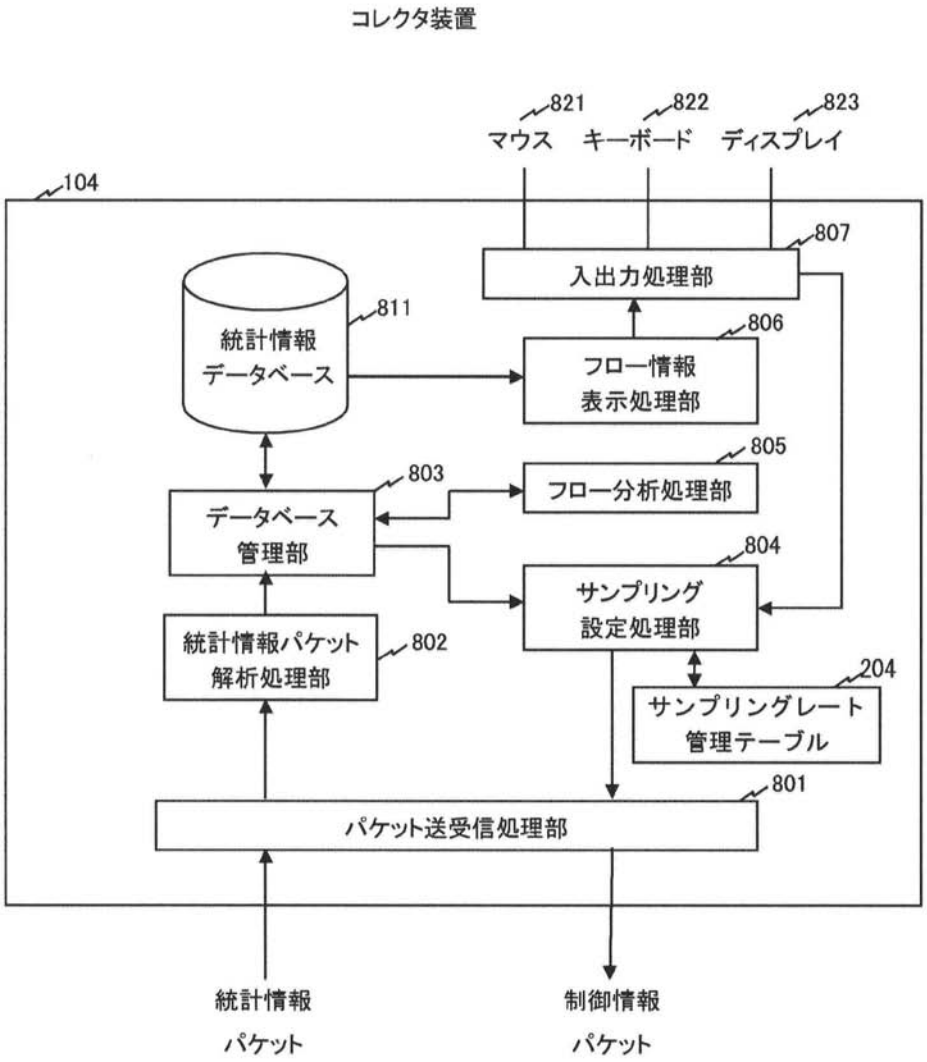
【図６】


開始
受信パケット処理部から
ヘッダ情報取得
601
フローテーブル検索
602
登録処理取得
603
登録処理を
実行する？
604
No
Yes
新規エントリ追加
605
統計処理及び
サンプル処理を参照
606
統計収集処理を
実行するか？
607
No
Yes
統計テーブル更新
608
ルーティングテーブル
検索
621
出力回線を取得
622
サンプル処理を
実行するか？
610
No
Yes
サンプル処理
611
検索処理完了
623
サンプリングレート
制御処理
624
受信パケット処理部へ
処理結果通知
625
終了

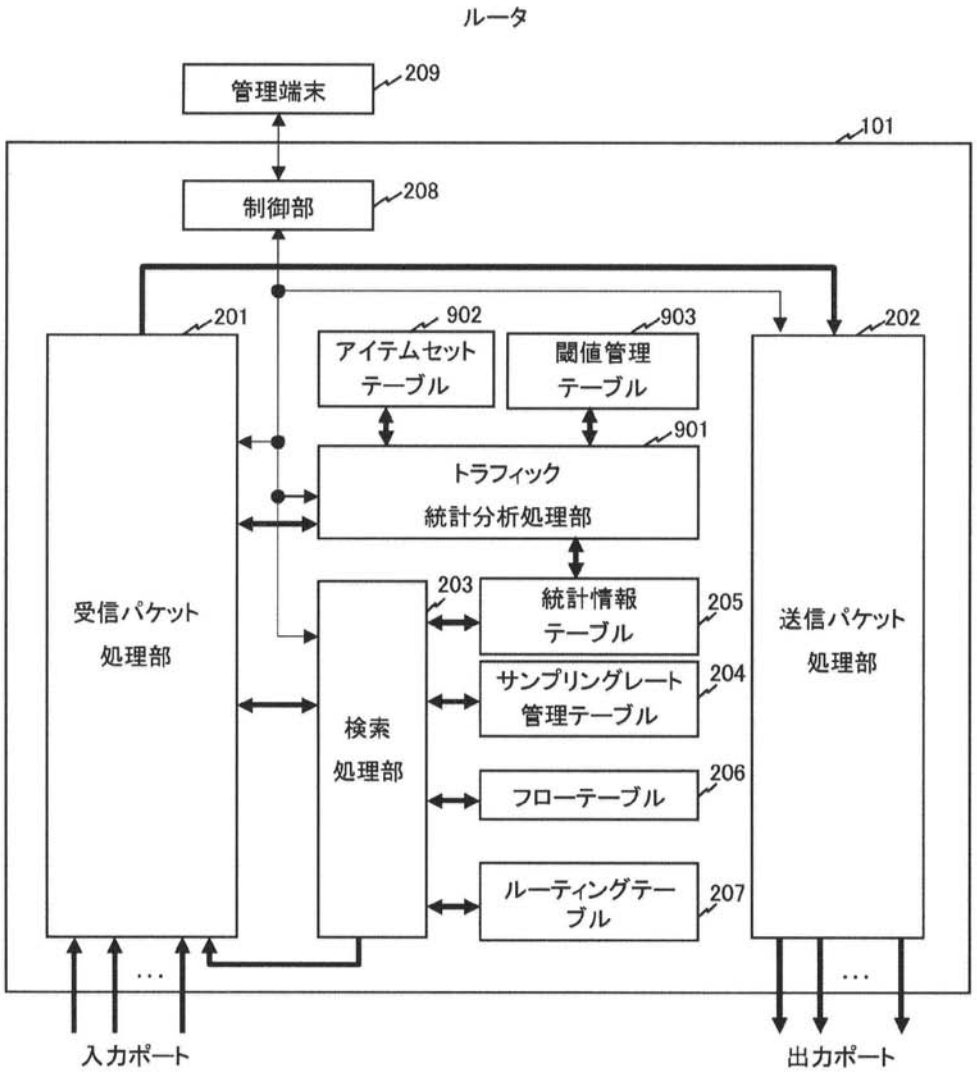
【図７】


サンプリングレート制御処理
開始
701
送信制御を取得
702
送信制御処理を
実行するか？
No
Yes
703
フローテーブルのフロー種別と
統計情報テーブルの帯域を取得
704
フロー種別と通信帯域から該当フローの
サンプリングレートを算出
705
フローテーブルの該当するエントリの
サンプリングレートに適用
終了

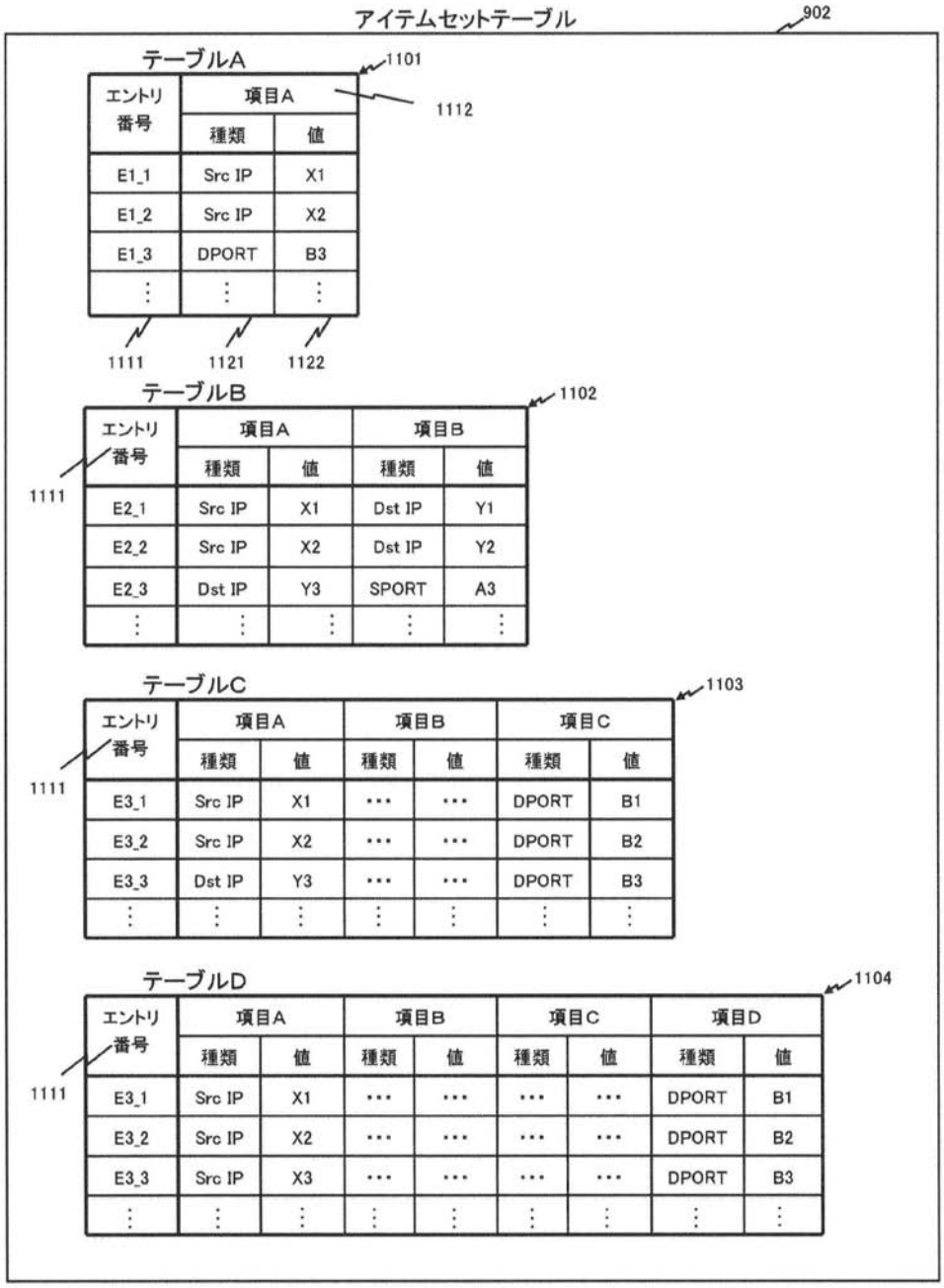
【図８】


コレクタ装置
821
マウス
822
キーボード
823
ディスプレイ
104
807
入出力処理部
811
統計情報
データベース
806
フロー情報
表示処理部
805
フロー分析処理部
803
データベース
管理部
804
サンプリング
設定処理部
統計情報パケット
解析処理部
802
204
サンプリングレート
管理テーブル
801
パケット送受信処理部
統計情報
パケット
制御情報
パケット

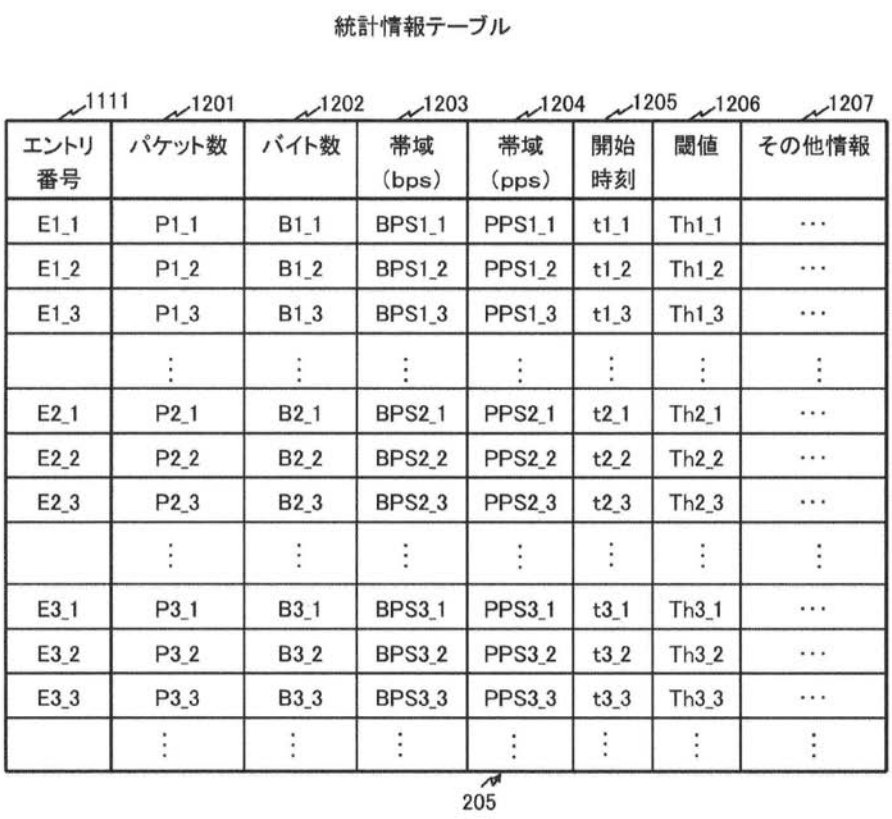
【図９】


ルータ
管理端末
209
101
制御部
208
201
902
アイテムセット
テーブル
903
閾値管理
テーブル
202
901
トラフィック
統計分析処理部
受信パケット
処理部
203
統計情報
テーブル
205
送信パケット
処理部
サンプリングレート
管理テーブル
204
検索
処理部
フローテーブル
206
ルーティングテー
ブル
207
入力ポート
出力ポート

【図１０】


アイテムセットテーブル
902
テーブルA
1101
1112
エントリ番号
項目A
種類
値
E1_1
Src IP
X1
E1_2
Src IP
X2
E1_3
DPORT
B3
1111
1121
1122
テーブルB
1102
項目B
Dst IP
Y1
E2_1
E2_2
Y2
E2_3
SPORT
A3
テーブルC
1103
項目C
DPORT
B1
B2
B3
E3_1
E3_2
E3_3
テーブルD
1104
項目D
X3

【図１１】

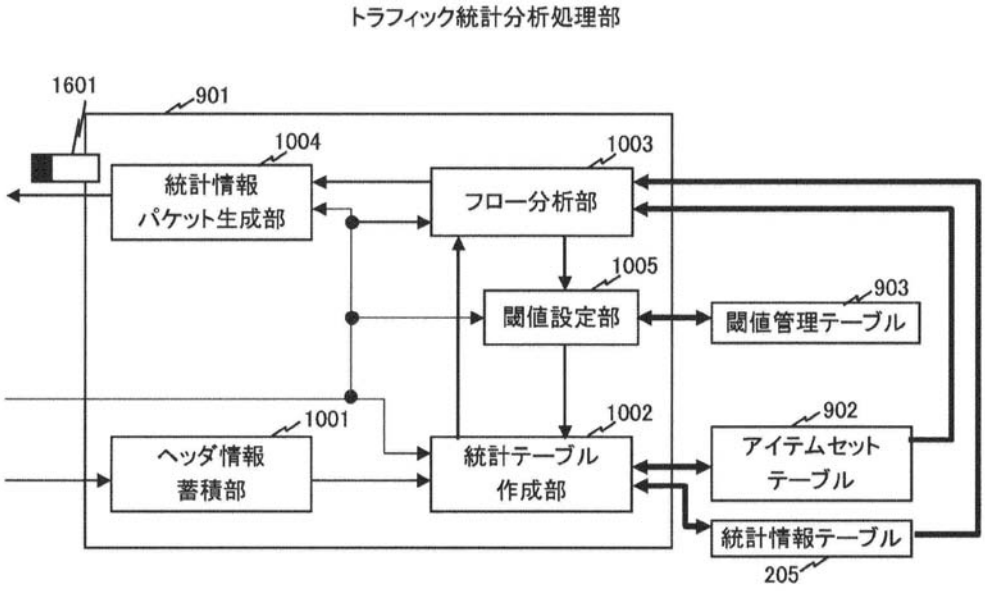

統計情報テーブル
1111
1201
1202
1203
1204
1205
1206
1207
エントリ番号
パケット数
バイト数
帯域（bps）
帯域（pps）
開始時刻
閾値
その他情報
E1_1 P1_1 B1_1 BPS1_1 PPS1_1 t1_1 Th1_1 …
E1_2 P1_2 B1_2 BPS1_2 PPS1_2 t1_2 Th1_2 …
E1_3 P1_3 B1_3 BPS1_3 PPS1_3 t1_3 Th1_3 …
E2_1 P2_1 B2_1 BPS2_1 PPS2_1 t2_1 Th2_1 …
E2_2 P2_2 B2_2 BPS2_2 PPS2_2 t2_2 Th2_2 …
E2_3 P2_3 B2_3 BPS2_3 PPS2_3 t2_3 Th2_3 …
E3_1 P3_1 B3_1 BPS3_1 PPS3_1 t3_1 Th3_1 …
E3_2 P3_2 B3_2 BPS3_2 PPS3_2 t3_2 Th3_2 …
E3_3 P3_3 B3_3 BPS3_3 PPS3_3 t3_3 Th3_3 …
205

【図１２】

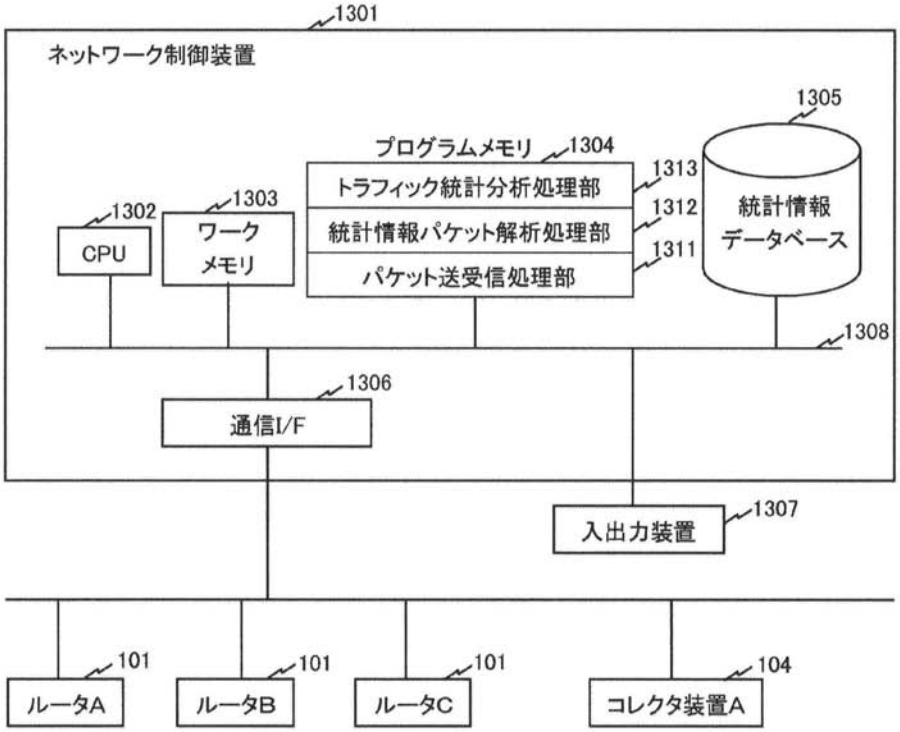
閾値管理テーブル

1401 帯域 (PPS)	1402 閾値(比率)		903
	分析済みフロー(0)	未知フロー(1)	異常フロー(2)
Default	10	1	1/10
～100	10	1	1/100
101～1,000	10	1	1/10
1,001～10,000	100	10	1
10,001～100,000	1,000	100	10
100,001～1,000,000	10,000	1,000	100
1,000,001～10,000,000	100,000	10,000	1,000
10,000,001～100,000,000	1,000,000	100,000	10,000
	1411	1412	1413

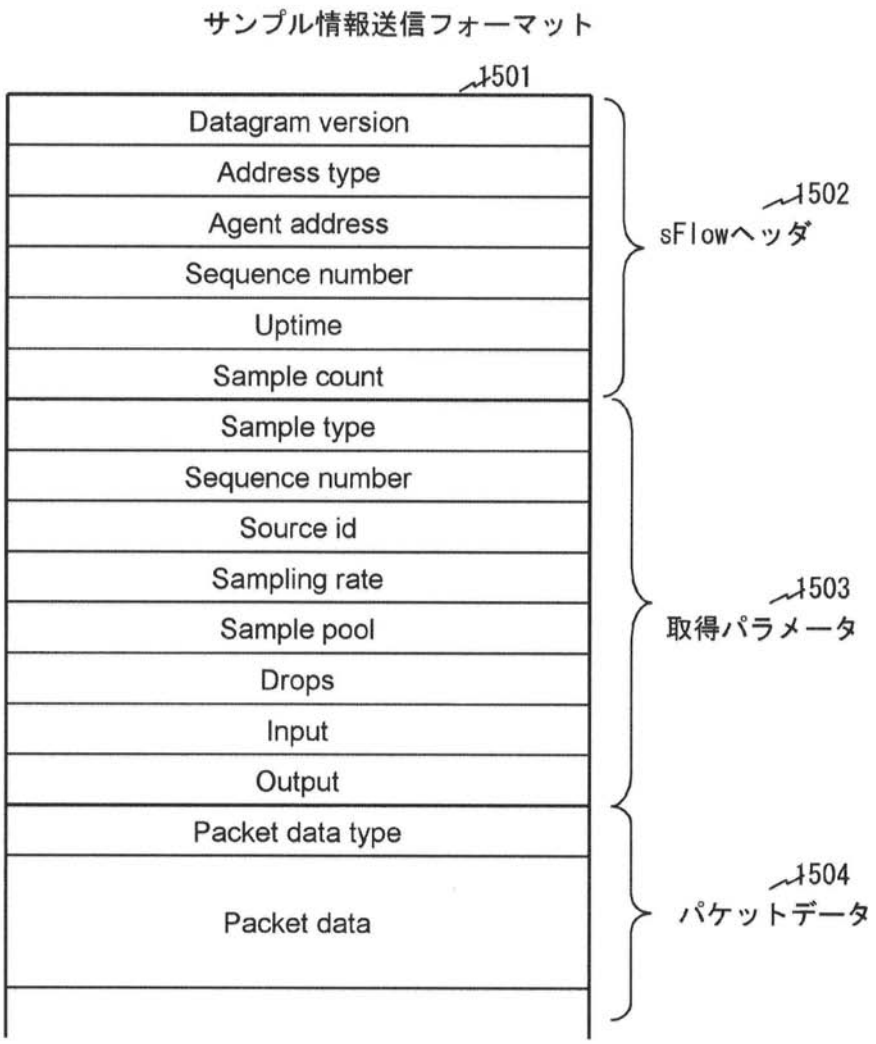
【図１３】


トラフィック統計分析処理部
1601
901
1004
統計情報
パケット生成部
1003
フロー分析部
1005
閾値設定部
903
閾値管理テーブル
1001
ヘッダ情報
蓄積部
1002
統計テーブル
作成部
902
アイテムセット
テーブル
統計情報テーブル
205

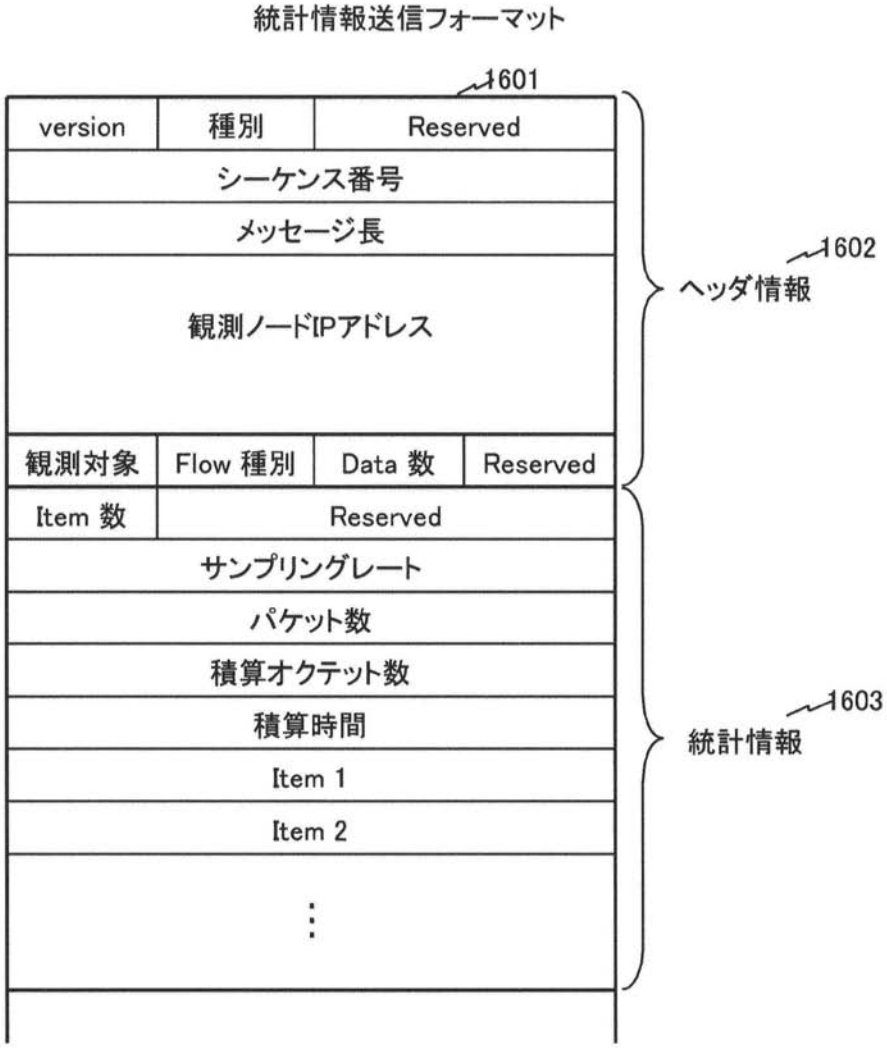
【図１４】


1301
ネットワーク制御装置
1305
プログラムメモリ
1304
1313
1312
1311
トラフィック統計分析処理部
統計情報パケット解析処理部
パケット送受信処理部
統計情報
データベース
1302
CPU
1303
ワーク
メモリ
1308
1306
通信I/F
1307
入出力装置
101
ルータA
101
ルータB
101
ルータC
104
コレクタ装置A

【図１５】


サンプル情報送信フォーマット
1501
Datagram version
Address type
Agent address
Sequence number
Uptime
Sample count
1502
sFlowヘッダ
Sample type
Sequence number
Source id
Sampling rate
Sample pool
Drops
Input
Output
1503
取得パラメータ
Packet data type
Packet data
1504
パケットデータ

【図１６】


統計情報送信フォーマット
1601
version
種別
Reserved
シーケンス番号
メッセージ長
観測ノードIPアドレス
観測対象
Flow 種別
Data 数
Reserved
Item 数
Reserved
サンプリングレート
パケット数
積算オクテット数
積算時間
Item 1
Item 2
1602
ヘッダ情報
1603
統計情報

フロントページの続き

(72)発明者　渡辺　義則
神奈川県川崎市幸区鹿島田８９０　新川崎三井ビル西棟　アラクサラネットワークス株式会社内
(72)発明者　柴田　剛志
東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所中央研究所内

審査官　安藤　一道

(56)参考文献　特開２００６－００５４０２（ＪＰ，Ａ）
特開２００１－２５７７２２（ＪＰ，Ａ）
特開２００５－０５１７３６（ＪＰ，Ａ）
特開２００６－０７９４８８（ＪＰ，Ａ）
特開２００１－１８６１２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５６