(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4658098号
(P4658098)
(45)発行日　平成23年3月23日(2011.3.23)　(24)登録日　平成23年1月7日(2011.1.7)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　200Z
H04L 12/22 (2006.01)　H04L 12/22

請求項の数 10　(全 26 頁)

(21)出願番号　特願2007-199499 (P2007-199499)
(22)出願日　平成19年7月31日 (2007.7.31)
(65)公開番号　特開2008-154204 (P2008-154204A)
(43)公開日　平成20年7月3日 (2008.7.3)
審査請求日　平成21年7月14日 (2009.7.14)
(31)優先権主張番号　特願2006-314299 (P2006-314299)
(32)優先日　平成18年11月21日 (2006.11.21)
(33)優先権主張国　日本国(JP)

(73)特許権者　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　100123788
弁理士　宮崎　昭夫
(72)発明者　入野　仁志
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
(72)発明者　片山　勝
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

審査官　安藤　一道

最終頁に続く

(54)【発明の名称】フロー情報制限装置および方法

(57)【特許請求の範囲】
【請求項１】
複数の端末を相互に接続するネットワーク上に配置され、該ネットワークにおけるトラフィックを計測する測定用端末に測定用ネットワークを介して接続されるフロー情報制限装置であって、
同一の属性を持つパケットの集合を同一の通信のフローとし、該フロー毎に、前記パケットのヘッダ情報に基づいてフロー情報を生成するフロー情報生成部と、
前記フロー情報生成部で生成したフロー情報を一時的に格納する管理用バッファを備え、該管理用バッファからフロー情報を読み出して出力するフロー情報数制限部と、
前記フロー情報数制限部から出力されたフロー情報をパケット化して前記測定用ネットワーク上に送出するフロー情報送信部と、を有し、
前記フロー情報数制限部は、前記管理用バッファに格納されているフロー情報の数が予め設定された上限値を超えると、該格納されているフロー情報を、非集約フロー情報と前記トラフィックの計測における重要性が該非集約フロー情報より低い集約候補とに分け、該集約候補とされたフロー情報を集約して、前記管理用バッファに保持されているフロー情報の数が一定数以下になるように制御する、フロー情報制限装置。
【請求項２】
前記フロー情報は、前記トラフィックの計測に必要な計測情報を含み、
前記フロー情報数制限部は、前記管理用バッファに格納されているフロー情報を前記計測情報の量または統計値の大小関係に基づいて順位付けして並び替え、該並び替えたフロ

ー情報のうちの、上位のフロー情報を前記非集約フロー情報とし、下位のフロー情報を前記集約候補とする、請求項１に記載のフロー情報制限装置。
【請求項３】
前記フロー情報数制限部は、前記フロー情報を集約する条件に含まれる比較項目を段階的に変更する、請求項１または２に記載のフロー情報制限装置。
【請求項４】
前記フロー情報数制限部は、前記フロー情報生成部が行うフロー情報の生成に用いられるパケットの属性に対応する項目と外部入力された該項目の優先順位とを保持し、該優先順位が最下位の項目を前記フロー情報の生成の項目から削除する処理を繰り返して前記比較項目を段階的に変更する、請求項３に記載のフロー情報制限装置。
【請求項５】
前記フロー情報生成部は、前記管理用バッファに格納されているフロー情報に対して、外部入力された項目の優先順位の順序に基づき、該フロー情報が保持する項目毎に大小比較を繰り返してフロー情報間の大小を判定し、該判定結果を検索用索引として保持し、該検索用索引を参照して前記フロー情報の生成を行う、請求項１から４のいずれか１項に記載のフロー情報制限装置。
【請求項６】
前記フロー情報数制限部は、前記管理用バッファに格納されているフロー情報に対して、外部入力された項目の優先順位の順序に基づき、該フロー情報が保持する項目毎に大小比較を繰り返してフロー情報間の大小を判定し、該判定結果を検索用索引として保持し、該検索用索引を参照して前記フロー情報の集約を行う、請求項１から４のいずれか１項に記載のフロー情報制限装置。
【請求項７】
前記フロー情報数制限部は、前記フロー情報生成部が生成したフロー情報の総数から並び替え後に上位に位置する非集約となるフロー情報の数である非集約数を減算した値である集約候補数と、前記上限値から前記非集約数を減算した値である集約結果数と、フロー情報制限時の集約条件の各項目毎のフロー数とを含む情報の履歴を記録し、該履歴に基づいて、次回の集約時における前記検索用索引の作成に用いられる初期項目数を推測する、請求項６に記載のフロー情報制限装置。
【請求項８】
前記検索用索引が、優先度が上位の項目の葉を優先度が下位の項目の根とする二分木のデータ構造を有する、請求項５から７のいずれか１項に記載のフロー情報制限装置。
【請求項９】
前記フロー情報生成部は、前記ヘッダ情報を構成する、前記通信に使用されたプロトコル、ソースアドレス、宛先アドレス、ソースポートおよび宛先ポートの各項目が合致するパケットの集合をフローとし、該フローの情報として、該各項目に関する情報を含むフロー情報を生成し、
前記フロー情報数制限部は、前記各項目の組み合わせからなる、集約する条件に含まれる比較項目の異なる複数の集約条件の範囲において、集約条件を変更して前記集約候補とされたフロー情報を集約する、請求項３に記載のフロー情報制限装置。
【請求項１０】
複数の端末を相互に接続するネットワーク上に配置され、該ネットワークにおけるトラフィックを計測する測定用端末に測定用ネットワークを介して接続される通信装置において行われるフロー情報制限方法であって、
同一の属性を持つパケットの集合を同一の通信のフローとし、該フロー毎に、前記パケットのヘッダ情報に基づいてフロー情報を生成する第１のステップと、
前記第１のステップで生成したフロー情報を一時的に管理用バッファに格納し、該管理用バッファからフロー情報を読み出す第２のステップと、
前記第２のステップで出力したフロー情報をパケット化して前記測定用ネットワーク上に送出する第３のステップと、を含み、

前記第２のステップは、前記管理用バッファに格納されているフロー情報の数が予め設定された上限値を超えると、該格納されているフロー情報を、非集約フロー情報と前記トラフィックの計測における重要性が該非集約フロー情報より低い集約候補とに分け、該集約候補とされたフロー情報を集約して、前記管理用バッファに保持されているフロー情報の数が一定数以下になるように制御するステップを含む、フロー情報制限方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、インターネットなどに代表されるオープンなネットワーク環境上で使用されるネットワーク装置に関し、特に、ネットワーク上のトラフィックを測定するための情報（フロー情報）を収集することの可能な、ノードなどに代表される情報通信機器に関する。

【背景技術】

【０００２】

インターネットで使用されるＩＰ（Internet Protocol）では、プロトコル、ソースＩＰアドレス、宛先ＩＰアドレスの情報が管理され、また一部のトランスポートプロトコルでは、ソースポートや宛先ポートの情報が管理される。これらのプロトコルを使用して伝送されるパケットは、それぞれのプロトコルで管理されている情報を含む。そのようなパケットが持つ情報に基づいて、通信の種別を分類する方法がフロー計測である。

【０００３】

フロー計測では、同一の属性のパケット、例えばプロトコル、ソースＩＰアドレス、宛先ＩＰアドレス、ソースポートおよび宛先ポートの各情報について同じ情報を持つパケットを同一の通信に属するパケットと見なす。同一の通信に属するパケットの集合をフローと呼ぶ。フローのデータ量やパケット量を計測することで、複数の地点間で複数の通信サービスを監視することができ、通信量が異常に多い地点間や通信サービスを特定したり、通信傾向を把握したりすることができる。

【０００４】

インターネットは、経路制御を行う複数のルータを含む複数のネットワークを相互に接続することで構築されており、送信元から送出されたパケットはいくつかのルータを経由して送信先に到達する。ルータは、パケットのＩＰヘッダや、場合によっては、トランスポートレイヤーのヘッダを参照してパケットの転送を行うので、フローの分類を行う機器として適している。ルータを通過したパケットのフロー情報を他の機器に通知する技術として、NetFlow（非特許文献１参照）やIPFIX（IP Flow Information eXport）がある。

【０００５】

フロー情報を特定のフォーマットに従ってパケット化した計測用パケットをルータからネットワーク上の計測用端末に送信することで、そのノードの通信内容を把握することができる。しかし、非特許文献２によると、DDoSと呼ばれる、ソースアドレスを分散させて大量のデータを送り続ける攻撃トラフィックや、ポートスキャンと呼ばれる、対象のホストの全ポートへの接続を試みてサービス状態及び脆弱性を検出する攻撃トラフィック等が発生したときに、フロー数が急激に増大する。

【０００６】

また、非特許文献３によると、フロー情報の通知を行うIPFIXにおいては、トランスポートプロトコルとして、輻輳制御のないUDP（Use Datagram Protocol）と輻輳制御のあるTCP（Transmission Control Protocol）やSCTP（Stream Control Transmission Protocol）を使用することができる。フローの送受信装置が輻輳制御機能のないUDPを利用して送信を行う場合、フロー数が急激に増大すると、それに伴ってルータなどのフロー送信装置から計測用端末に送信されるパケットも増大し、その結果、フロー送信装置と計測用端末の間の計測用ネットワークにおいて輻輳が発生する可能性がある。

【０００７】

一方、フローの送受信装置が輻輳制御機能を持つTCPやSCTPを利用して送信を行う場合

は、フロー数が急激に増大しても、輻輳は発生しない。しかし、フロー送信装置において、輻輳制御機能によって送信できるフロー情報数が限定されるため、生成されるフロー情報数に対して送信されるフロー情報数が少なくなり、内部の送信バッファが溢れる場合がある。この結果、送信された情報は先に生成したフロー情報に限られ、観測したトラフィック全体の情報が送信できなくなる。

【非特許文献１】[平成１８年９月８日閲覧　インターネット]B. Claise. Cisco Systems NetFlow Services Export Version 9. RFC 3954 (Informational), October 2004.http://www.ietf.org/rfc/rfc3954.txt

【非特許文献２】Cristian Eatan, Ken Keys, David Moore, George Varghese:"Building a better netflow", ACM SIGCOMM Computer Communication Review, 34, Issue 4, pp. 245-256 (2004)

【非特許文献３】B. Claise. IPFIX Protocol Specification. Internet Draft, June 2006. HYPERLINK "http://tools.ietf.org/id/draft-ietf-ipfix-protocol-22.txt" http://tools.ietf.org/id/draft-ietf-ipfix-protocol-22.txt(２２版)

【発明の開示】

【発明が解決しようとする課題】

【０００８】

上述したように、NetFlow（非特許文献１参照）やIPFIXのフロー技術を採用する通信システムにおいては、攻撃トラフィックによりフローが増大した場合に、計測用ネットワークにおける通信に輻輳が発生する、または、輻輳は発生しないが、観測したトラフィック全体の情報が送信できないために不正確な情報送信が発生する、といった問題が生じる。以下に、この問題を具体的に説明する。

【０００９】

図２０に、計測用ネットワークを含むインターネットを通じてパケットによる通信を行う情報通信システムを示す。図２０において、インターネット１０は、パケット転送を行う複数のノード１２～１４、１１１を含む複数のネットワーク同士を相互に接続したものである。ノード１２～１４、１１１は相互に通信可能に接続されている。ノード１１１には、計測用端末２０および端末３０が接続されている。ノード１２には端末１４が接続され、ノード１３には端末４２が接続され、ノード１４には端末４３が接続されている。

【００１０】

計測用端末２０および端末３０、４１～４３のそれぞれは、通信機能を備えたコンピュータシステムである。コンピュータシステムの主要部は、プログラムなどを蓄積する記憶装置、キーボードやマウスなどの入力装置、ＣＲＴやＬＣＤなどの表示装置、外部との通信を行うモデムなどの通信装置、プリンタなどの出力装置および入力装置からの入力を受け付けて通信装置、出力装置、表示装置の動作を制御する制御装置からなる。端末４１～４３はクライアント端末であり、端末３０はクライアントに通信サービスを提供するサーバであり、サーバークライアント間で通信が行われる。

【００１１】

端末４１～４３は、ウィルスやワームに感染したり、第三者による不正な制御が行われたりする場合がある。そのような場合、端末４１～４３は、端末３０に対するネットワーク攻撃を行う。複数の端末が同時にネットワーク攻撃を開始した場合は、ソースアドレスが分散する。また、単一の端末がネットワーク攻撃を行った場合も、ソースアドレスの詐称によりソースアドレスが分散する場合がある。ノードには、このようにソースアドレスが分散した大量のデータが到達し、異常なトラフィックが発生する。

【００１２】

加えて、IPスキャンやポートスキャンなどの攻撃に準ずる行動、ウィルスやワーム等の感染活動などでは、ノードの存在とは無関係に宛先アドレスを分散させて通信が行われて、異常なトラフィックが発生する場合がある。この場合も、ソースアドレスは詐称などにより分散する場合がある。

【００１３】

上記のような攻撃等によってインターネット１０全体における通信量が増大し、端末３０宛のトラフィックなど、ノード１１１がゲートウェイとなるネットワーク上を流れるトラフィックが増大する。このトラフィックの増大は、ノード１１１における、計測用ネットワークにおける通信に輻輳が発生したり、観測したトラフィック全体の情報が送信できなかったりする、といった以下のような問題を引き起こす。

【００１４】

ノード１１１は、フロー情報をパケット化した計測用パケットを計測用端末２０に送信する。輻輳制御を行わないUDPをトランスポートプロトコルとして用いる場合は、ノード１１１上で観測されるフロー数が増えると、それに伴って計測用パケットの送信量も増大する。このため、ノード１１１と計測用端末２０の間の計測用ネットワークにおいて輻輳が発生し、攻撃の二次被害が発生する。

【００１５】

ノード１１１と端末３０の間やノード１１１とインターネット１０の間の通常の通信に利用する回線が異常状態になった場合に、異常性のあるトラフィックを発見するために、計測用端末２０が配置されている。しかし、フローの急激な増大により、ノード１１１と計測用端末２０の間の通信において輻輳が発生すると、計測用パケットのロスが高まり、計測用端末２０にて十分な計測を行うことが困難になる。加えて、他の通信が行われている場合には、その通信に悪影響を及ぼす場合がある。場合によっては、計測用端末２０が資源不足状態に陥る場合がある。

【００１６】

また、計測用端末２０が複数台のノードからフロー情報を受信するようなシステムを構築した場合には、輻輳の被害はさらに大きくなる。

【００１７】

一方、輻輳制御機能を持つTCPやSCTPをトランスプロトコルとして利用した場合は、ノード１１１と計測用端末２０の間の通信において輻輳は発生しない。しかし、輻輳制御機能によりノード１１１の出力フロー数が制限されるため、上記異常時に観測されたフロー数に対してノード１１１が出力できるフロー数が少なくなる場合がある。このように出力フロー数に比べて入力フロー数が多くなると、ノード１１１の内部バッファが破綻して計測情報の一部が欠落し、ノード１１１は、計測したトラフィック全体の情報を計測用端末２０へ正確に送信できない。

【００１８】

本発明の目的は、上記問題を解決し、トラフィック全体の計測情報を保持したまま、送信するフロー情報の数を制限することのできるフロー情報制限装置を提供することにある。

【課題を解決するための手段】

【００１９】

上記目的を達成するため、本発明のフロー情報制限装置は、複数の端末を相互に接続するネットワーク上に配置され、該ネットワークにおけるトラフィックを計測する測定用端末に測定用ネットワークを介して接続されるフロー情報制限装置であって、同一の属性を持つパケットの集合を同一の通信のフローとし、該フロー毎に、前記パケットのヘッダ情報に基づいてフロー情報を生成するフロー情報生成部と、前記フロー情報生成部で生成したフロー情報を一時的に格納する管理用バッファを備え、該管理用バッファからフロー情報を読み出して出力するフロー情報数制限部と、前記フロー情報数制限部から出力されたフロー情報をパケット化して前記測定用ネットワーク上に送出するフロー情報送信部と、を有し、前記フロー情報数制限部は、前記管理用バッファに格納されているフロー情報の数が予め設定された上限値を超えると、該格納されているフロー情報を、非集約フロー情報と前記トラフィックの計測における重要性が該非集約フロー情報より低い集約候補とに分け、該集約候補とされたフロー情報を集約して、前記管理用バッファに保持されているフロー情報の数が一定数以下になるように制御する、ことを特徴とする。

【００２０】

上記の構成においては、攻撃トラフィックによりフローが増大し、それに伴ってフロー情報生成部によって生成されるフロー情報の数が増大するが、フロー情報数制限部が、フロー情報生成部から入力されるフロー情報の数が増大すると、現在、格納しているフロー情報を集約する。このフロー情報の集約により、フロー情報送信部には、一定数以下のフロー情報しか供給されない。したがって、フロー情報送信部が、計測用ネットワーク上に送出するフロー情報の数も一定数以下に制限される。

【００２１】

また、フロー情報送信部には、一定数以下のフロー情報しか供給されないので、フロー情報送信部内のバッファが溢れてフロー情報が欠落することもない。したがって、トランスポートプロトコルに輻輳制御機能のあるTCPやSCTPを用いた場合に生じていた、フロー情報送信部内のバッファの破綻によるフロー情報の欠落のために、観測したトラフィック全体の情報を正確に送信できない、といった問題も生じない。

【発明の効果】

【００２２】

本発明によれば、フローの増大に関係なく、計測用ネットワーク上には、一定数以下のフロー情報しか送信されないので、トランスポートプロトコルに輻輳制御機能のないUDPを用いた場合において発生していた計測用ネットワークにおける通信の輻輳を抑制することができる。

【００２３】

また、トランスポートプロトコルに輻輳制御機能のあるTCPやSCTPを用いた場合に生じていた、フロー情報送信部内のバッファの破綻によるフロー情報の欠落を抑制することができるので、観測したトラフィック全体の情報を正確に測定用端末に送信することができる。

【発明を実施するための最良の形態】

【００２４】

次に、本発明の実施形態について図面を参照して説明する。

【００２５】

図１は、本発明が適用される情報通信システムの一例を示す図である。この情報通信システムは、ノード１１１に代えてノード１１を設けた以外は、図２０に示したシステムと同様のものである。インターネット１０は、パケット転送を行う複数のノード１１～１４を含む複数のネットワーク同士を相互に接続したものである。ノード１１～１４は相互に通信可能に接続されている。ノード１１には、計測用端末２０および端末３０が接続されている。

【００２６】

この情報通信システムでは、ノード１１がフロー情報集約機能を備えたフロー情報処理部２００を有しており、この点が、図２０に示した情報通信システムと異なる。

【００２７】

図２に、本発明のフロー情報制限装置の一実施形態であるノード１１のフロー情報処理部２００の構成を示す。図２を参照すると、フロー情報処理部２００は、計測用ネットワークインタフェース２０１、フロー生成機能部２０２、フロー情報数制限機能部２０３、フロー送信機能部２０４および出力用ネットワークインタフェース２０５を有する。

【００２８】

計測用ネットワークインタフェース２０１は、各端末からインターネット１００を通じて到達するパケットをそれぞれ収集する複数のネットワークインタフェースからなる。計測用ネットワークインタフェース２０１で収集されたパケットはフロー生成機能部２０２に供給される。

【００２９】

フロー生成機能部２０２は、NetFlow、IPFIX等のフロー通知プロトコルを利用する既存の送信機器が備えているフロー生成機能部であって、計測用ネットワークインタフェース２０１を通じて収集されたパケットのヘッダ情報に基づいてフロー情報を生成する。具体

的には、フロー生成機能部２０２は、プロトコル、ソースＩＰアドレス、宛先ＩＰアドレス、ソースポートおよび宛先ポートなど、パケットのヘッダに含まれる情報、または経路情報などのパケットのヘッダから判断される情報が同一のパケットを同一の通信に属するパケットと見なして、そのパケットの集合であるフローについての情報（フロー情報）を生成する。このフロー情報の生成では、フロー化するための条件に基づく時間情報の更新などの処理も行われる。一般的にフロー情報は、プロトコル、ソースＩＰアドレス、宛先ＩＰアドレス、ソースポートおよび宛先ポートの各情報を含む場合が多い。フロー生成機能部２０２で生成されたフロー情報は、フロー情報数制限機能部２０３に供給される。

【００３０】

フロー情報数制限機能部２０３は、フロー生成機能部２０２から入力されるフロー情報を一時的に格納して管理するための管理用バッファ部を備え、該管理用バッファ部からフロー情報を読み出してフロー送信機能部２０４へ供給する。管理用バッファ部にて管理するフロー情報の数の上限値が予め設定されており、フロー情報数制限機能部２０３は、フロー生成機能部２０２から一定時間あたりに供給されるフロー情報の数が増大して、管理用バッファ部に格納されて管理されているフロー情報の数が上限値を超えると、管理用バッファ部に格納されているフロー情報群を集約候補と非集約フロー情報とに分け、集約候補について集約処理を行う。上限値は、計測用ネットワークの通信能力（ノード１１と計測用端末２０の間のネットワークの通信能力）、フロー送信機能部２０４の処理能力および管理用バッファ部からの読み出し速度などを考慮し、管理用バッファ部やフロー送信機能部２０４の内部バッファが破綻せず、計測用ネットワークの通信に輻輳が生じないような値とされる。集約候補のトラフィックの計測における重要性は、非集約フロー情報より低い。

【００３１】

フロー送信機能部２０４は、NetFlow、IPFIX等のフロー通知プロトコルを利用する既存の送信機器が備えているフロー送信機能部であって、フロー情報数制限機能部２０３から供給されたフロー情報を一時的に格納するための内部バッファを備え、内部バッファから読み出したフロー情報を適切なサイズにパケット化して計測用パケットを生成し、該計測用パケットに専用のヘッダを付与して出力用ネットワークインタフェース２０５からネットワーク上に送出する。出力用ネットワークインタフェース２０５から送出された計測用パケットは、計測用端末２０に供給される。計測用ネットワークインタフェース２０１と出力用ネットワークインタフェース２０５は物理的に同じものであってもよい。

【００３２】

フロー生成機能部２０２が生成したフロー情報を格納するバッファ、フロー情報制限機能部２０３が管理するための管理用バッファ部、フロー送信機能部２０４がフロー情報を一時的に格納するためのバッファはその記憶領域の一部または全体がそれぞれ独立していても共有されていてもよい。

【００３３】

次に、ノード１１の動作を具体的に説明する。

【００３４】

ノード１１では、フロー情報数制限機能部２０３が、フロー生成機能部２０２から入力されるフロー情報の数に関係なく、フロー送信機能部２０４に対して、一定数以下のフロー情報しか送信しないので、ノード１１から計測用端末２０へ送信される計測用パケットの量も一定数以下に制限される。

【００３５】

図３に、フロー情報数制限機能部２０３にて管理される管理用バッファの構造の一例を示す。管理用バッファは、フロー生成機能部２０２から入力されるフロー情報が計測目的に応じた順位付けに基づいて並び替えられて格納されるバッファＢ１と、フロー生成条件の各項目の組み合わせからなる、集約する条件に含まれる比較項目の異なる複数の集約条件のそれぞれに対応して設けられたバッファＢ２～Ｂ７とを有する。

【００３６】

バッファＢ１は、非集約Ｂ１－１と集約候補Ｂ１－２とからなる。バッファＢ１に格納されるフロー情報は、フロー生成機能部２０２でのフロー情報の生成において用いた、同一の通信に属するパケットを識別するための条件（フロー生成条件）を満たすフロー情報である。ここでは、フロー生成条件は、プロトコル、ソースＩＰアドレス、宛先ＩＰアドレス、ソースポートおよび宛先ポートの５つの項目に関する条件とされている。

【００３７】

なお、フロー生成条件は、上記の５つの項目に限定されるものではない。マックアドレス、ＩＰアドレス、ポート番号などを始めとしたパケットヘッダに基づく情報、または、それら情報から判断されるネクストホップやＡＳ番号などを始とした経路制御に関する情報などを、フロー生成条件として利用することができる。同様に、集約済みの情報を管理するバッファも元の条件を削除して作成されるため、図３中のバッファＢ２～Ｂ７に例示する条件に限定されるものではない。

【００３８】

NetFlow、IPFIXといったフロー情報を他の機器に通知するためのプロトコルを用いた場合、計測用端末２０に対しては、観測されたトラフィックのフロー情報と、そのフロー情報のフォーマットを定義するためのデータ構造定義情報（テンプレートと呼ばれる）が送られる。

【００３９】

図４に、フロー情報およびデータ構造定義情報の一例を示す。この定義情報によれば、定義情報・フロー情報共通の４バイトのヘッダの後に、定義情報用の４バイトのヘッダが続き、その後に、フロー情報を構成する項目が列挙される。

【００４０】

定義情報・フロー情報共通の４バイトのヘッダでは、SetIDと呼ばれるＩＤが２バイトで示され、次の２バイトで情報の長さが示される。SetIDは、通常の定義情報か、後述するオプション用定義情報か、それら定義情報に対応するフロー情報・オプション情報かを区別するために用いられる。NetFlowの場合は、０が通常の定義情報に対応し、１がオプション情報に対応し、２５６以上の値がフロー情報・オプション情報に対応する。IPFIXの場合は、２が通常の定義情報に対応し、３がオプション情報に対応し、２５６以上の値がフロー情報・オプション情報に対応する。

【００４１】

定義情報・フロー情報共通の４バイトのヘッダに続く通常の定義情報用のヘッダは、２バイトのテンプレートＩＤと２バイトのフィールドカウントで構成される。２バイトのテンプレートＩＤは、どのフロー情報のデータ構造を定義するかを示すためのものであり、対応するフロー情報のSetIDと同一になる。フィールドカウントは、これに続く項目数を示す。

【００４２】

フィールド情報を構成する各項目は４バイトごとに１つの情報を表す。４バイトのうちの前半の２バイトは項目のＩＤを表し、後半の２バイトは項目のサイズ（バイト数）を表す。図４に示した例では、フィールド情報を構成する項目が１２個あり、それぞれの項目のＩＤおよびバイト数が示されている。例えば、最初の項目では、IPv4のソースアドレスを示すsourceIPv4Address（ID：８番）が４バイトであることが示され、次の項目では、IPv4の宛先アドレスを示すdestinationIPv4Address（ID：１２番）が４バイトであることが示されている。このように各項目によりフロー情報のデータ構造が定義されている。

【００４３】

図４に示したフィールド情報を構成する各項目の全てがフロー生成条件として利用されるわけではない。例えば、パケット量やバイト量を示すカウンタ（図４中のpacketDeltaCount（ID：２番）、octetDeltaCount(ID：１番)）や時間情報（図４中のflowStartSysUpTime（ID：２２番、flowEndSysUpTime（ID：２１番））は、フロー生成条件として利用することはできない。これ以外の項目についても、必ずしも全てフロー生成条件として利用するわけではなく、IPFIXの場合、別のオプション情報によって明示的にフロー生成条件

となる項目が通知される。なお、NetFlowでは、そのような通知機能はないため、機器実装依存となる。IPFIXの場合、フロー生成条件となる項目はフローキーと呼ばれている。

【００４４】

図５に、オプション情報による通知方法を模式的に示す。オプション情報を示す場合、オプションデータ構造定義情報とオプション情報の関係は、通常のフローデータ構造定義情報とフロー情報の関係と同じである。但し、オプション情報には、スコープと呼ばれる情報の範囲を示す情報が付与される。

【００４５】

オプションデータ構造定義情報は、フィールドカウントに続いて、２バイトのスコープフィールドカウントが付与され、その後に項目が列挙される。項目のうち最初のスコープフィールドカウントが付与された数がスコープになる。図５に示した例では、TemplateID（上述のテンプレートＩＤと用途は同じ）がスコープとなる。また、フロー生成条件を示すflowKeyIndicatorが定義される。

【００４６】

オプションデータ構造定義情報に従ってオプション情報のフォーマットが作成され、オプション情報として具体的な値が設定される。例えば、図４に示したフロー情報に対するオプション情報を示すためには、TemplateIDに対応する値は２５６になる。flowKeyIndicatorは、６４bitのビットマップになっており、１bitずつ１項目がフロー生成条件として利用することができるかを示す。つまり、flowKeyIndicatorは、先頭から最大６４個の項目に関して、フロー生成条件として利用しているか否かを示す情報を設定することができる。

【００４７】

図４に示した定義情報のうち、sourceIPv4Address、destinationIPv4Address、protocolIdentifier、sourceTransportPort、destinationTransportPortがフロー生成条件である場合、それぞれ先頭から１番目、２番目、６番目、７番目、８番目に位置するため、flowKeyIndicatorのデータは１bit目、２bit目、６bit目、７bit目、８bit目がそれぞれ１になる。

【００４８】

これらのフロー情報通知用プロトコルを用いる場合、利用者は、送信したいフロー情報に含める項目のＩＤとサイズを指定することになる。本実施形態では、さらに、フロー生成条件に用いる条件に対して、利用者によって設定された優先順位を付与する。この優先順位の低いものから条件を削除することで新しい条件を作成する。

【００４９】

図６および図７に、条件優先度を付与した定義情報およびそれにより展開されて使用される条件の一例を示す。

【００５０】

図６に示す例では、sourceIPv4Address、destinationIPv4Address、protocolIdentifier、sourceTransportPort、destinationTransportPortの５つの項目に対して条件の優先順位として異なる値が与えられている。この優先順位に従えば、削減数が０の場合、削減数が１の場合、削減数が２の場合、削減数が３の場合、削減数が４の場合のそれぞれで１つの条件の組が生成されるので、最大で５つの条件の組が生成されることになる。

【００５１】

複数の項目に対して同じ優先順位が与えられた場合は、同一優先順位の項目は排他的に利用される。図７に示す例では、sourceIPv4AddressおよびdestinationIPv4Addressの項目の優先順位が２とされ、protocolIdentifierの項目の優先順位が１とされ、sourceTransportPortおよびdestinationTransportPortの項目の優先順位が４とされている。この優先順位に従えば、削減数が０の場合に１つの条件の組が生成され、削減数が１の場合に２つの条件の組が生成され、削減数が２の場合に１つの条件の組が生成され、削減数が３の場合に２つの条件の組が生成され、削減数が４の場合に１つの条件の組が生成されるので、最大で７つの条件の組が生成されることになる。

【００５２】
これら優先順位に関する外部入力を受け付けるために、フロー情報処理部２００を図８に示すような構成としてもよい。図８に示すフロー情報処理部２００は、図２に示した構成に加えて制御部２０６を備える。フロー生成機能部２０２、フロー情報数制限機能部２０３およびフロー送信機能部２０４のそれぞれは、制御部２０６との間で情報を送受信する。定義情報の入力形式は、図９に示すようなｃｖｓ（カンマ区切りテキスト）やスペース・タブ区切りテキストであてもよく、また、図１０に示すような、ＸＭＬなどの記述言語を用いたものであってもよい。図１０に示す例は、ＩＥＴＦに提案されている”Configuration Data Model for IPFIX and PSAMP”（http://tools.ietf.org/wg/ipfix/draft-muenz-ipfix-configuration-01.txt（５月１５日入手））の記述方式に、flowKeyPrecedenceという条件の優先順位を示す要素を独自に追加したものである。

【００５３】
フロー生成機能部２０２で生成された情報は、フロー情報数制限機能部２０３に供給され、そこで、フロー送信機能部２０４に送信される前に、フロー集約条件において削除された項目がテンプレートから削除されるか、または、flowKeyIndicatorのビットマップから除外される。これらは全て、異なるテンプレートとして扱う必要があるため、フロー送信機能部２０４で異なったテンプレートＩＤが付与されて出力用ネットワークインタフェース２０５経由で送信される。このように、フロー情報数制限機能部が、フロー生成機能部が行うフロー情報の生成に用いられるパケットの属性に対応する項目と外部入力された該項目の優先順位とを保持し、該優先順位が最下位の項目をフロー情報の生成の項目から削除する処理を繰り返して行うことで、比較項目を段階的に変更する。

【００５４】
計測目的に応じた並び替えでは、例えば、計測目的がDoS等の攻撃により通信されるデータ量が増大したトラフィックの検出である場合は、フロー情報に含まれているデータ量の大小関係に基づいてフロー情報を並び替える。計測目的がTCP SYN DoS等の攻撃に関するトラフィックの検出である場合は、フロー情報に含まれているSYN等のメッセージの数の大小関係に基づいてフロー情報を並び替える。計測目的が複数の項目からなる場合は、フロー情報に含まれている、それぞれの項目のデータの数に対して、優先順位や重み付けを行った上で、フロー情報を並び替える。さらにそれらの値の標準偏差・分散値などの統計値も並び替えの指標として利用できる。並び替えの方法も目的に応じて降順、昇順を切り替えることが可能である。

【００５５】
非集約Ｂ１－１には、外部から与えられた非集約数に基づき、並び替えが行われたフロー情報群の上位非集約数個のフロー情報が非集約フロー情報として格納され、集約候補Ｂ１－２には、並び替えが行われたフロー情報群の非集約フロー情報以外のフロー情報が集約候補として格納される。図３中、非集約Ｂ１－１および集約候補Ｂ１－２に格納された情報フローは、図面に向かって左側に行くほど順位が低く、右側ほど順位が高くなっている。

【００５６】
バッファＢ２には、フロー生成条件のうちの、プロトコル、ソースアドレス、宛先アドレスおよび宛先ポートの４つの項目（集約条件）が合致するフロー情報を集約した集約済みフロー情報群が格納される。バッファＢ３には、フロー生成条件のうちの、プロトコル、ソースアドレス、宛先アドレスおよびソースポートの４つの項目（集約条件）が合致するフロー情報を集約した集約済みフロー情報群が格納される。

【００５７】
バッファＢ４には、フロー生成条件のうちの、プロトコル、ソースアドレスおよび宛先アドレスの３つの項目（集約条件）が合致するフロー情報を集約した集約済みフロー情報群が格納される。バッファＢ５には、フロー生成条件のうちの、プロトコルおよび宛先アドレスの２つの項目（集約条件）が合致するフロー情報を集約した集約済みフロー情報群が格納される。バッファＢ６には、フロー生成条件のうちの、プロトコルおよびソースア

ドレスの２つの項目（集約条件）が合致するフロー情報を集約した集約済みフロー情報群が格納される。バッファＢ７には、フロー生成条件のうちのプロトコル（集約条件）が合致するフロー情報を集約した集約済みフロー情報群が格納される。

【００５８】

集約条件は、条件を構成する項目が多い方から、バッファＢ２、Ｂ３、Ｂ４、Ｂ５、Ｂ６、Ｂ７の順番となっている。図３中では、図面に向かって上側ほど、条件を構成する項目が多くなっており、下側ほど、条件を構成する項目が少なくなっている。

【００５９】

管理用バッファ部に格納されて管理されているフロー情報の数が上限値以下である場合は、フロー情報数制限機能部２０３は、バッファＢ１からフロー情報を順次読み出してフロー送信機能部２０４に供給する。管理用バッファ部に格納されて管理されているフロー情報の数が上限値を超えた場合は、フロー情報数制限機能部２０３は、バッファＢ１に格納されているフロー情報に対して計測目的に応じた並び替えを行い、上位のフロー情報を非集約Ｂ１－１に格納し、下位のフロー情報を集約候補Ｂ１－２に格納する。そして、集約候補Ｂ１－２に格納したフロー情報（集約候補）に対して、フロー情報集約処理を実行する。非集約Ｂ１－１に格納したフロー情報は、集約されることなく、順次読み出されて、フロー送信機能部２０４に供給される。

【００６０】

なお、ここでは、管理されているフロー情報の数が上限値を超えた場合にバッファＢ１に格納されているフロー情報の並び替えを行うようになっているが、挿入ソート等のアルゴリズムを用いて、フロー生成機能部２０２から供給されるフロー情報を並び替えた状態でバッファＢ１に格納するようにしてもよい。

【００６１】

次に、フロー情報数制限機能部２０３にて行われるフロー情報集約処理について具体的に説明する。図１１に、そのフロー情報集約処理の一手順を示す。

【００６２】

まず、管理用バッファ部に格納されて管理されているフロー情報の数が上限値を超えたか否かを判断する（ステップＳ１）。この判断は、一定時間おき、または、フロー生成機能部２０２からフロー情報が入力されるたびに行われる。

【００６３】

管理されているフロー情報の数が上限値を超えた場合は、バッファＢ１に格納されているフロー情報の並び替えを行って集約候補と非集約フロー情報に分ける（ステップＳ２）。次に、集約候補のうちの順位の一番低いフロー情報を集約対象として抽出する（ステップＳ３）。次に、初期集約条件を設定する（ステップＳ４）。初期集約条件は、フロー生成条件より１つ項目の少ない条件であり、具体的には、図３に示したバッファＢ２に関する集約条件である。次に、検索対象バッファとして集約条件に対応するバッファを設定する（ステップＳ５）。図３に示したバッファＢ２に関する集約条件が設定された場合は、バッファＢ２が検索対象バッファとなる。

【００６４】

次に、検索対象バッファ内に、集約対象と設定された集約条件の全項目が一致する集約済みフロー情報があるか否かを判定する（ステップＳ６）。集約条件の全項目が一致する集約済みフロー情報がある場合は、集約対象をその集約済みフロー情報と集約して現在設定されている集約条件に対応するバッファに格納する（ステップＳ７）。検索時に集約条件の全項目が一致する集約済みフロー情報が複数検索された場合は、それら全ての集約済みフロー情報と集約対象とを集約する。

【００６５】

ステップＳ６で集約条件の全項目が一致する集約済みフロー情報がないと判断された場合は、ステップＳ５で設定した対象バッファが集約候補Ｂ１－２であるか否かを判断する（ステップＳ８）。対象バッファが集約候補Ｂ１－２でない場合は、検索対象バッファとして現在より１つ上位のバッファ（条件を構成する項目が多いバッファ）を設定し（ステ

ップＳ９）、ステップＳ６に移行する。

【００６６】

ステップＳ８で対象バッファが集約候補Ｂ１－２であると判断した場合は、現在設定されている集約条件が、条件を構成する項目が最も少ない条件であるか否かを判断する（ステップＳ１０）。集約条件が、条件を構成する項目が最も少ない条件でない場合は、集約条件を現在よりも項目が１つ少ない条件に変更し（ステップＳ１１）、ステップＳ５に移行する。集約条件が、条件を構成する項目が最も少ない条件である場合は、集約対象を、条件を構成する項目が最も少ない条件のバッファに格納する（ステップＳ１２）。

【００６７】

以上のフロー情報集約処理を、図３に示した管理用バッファを例に、具体的に説明する。

【００６８】

ステップＳ２で、上位のフロー情報を非集約Ｂ１－１に格納し、下位のフロー情報を集約候補Ｂ１－２に格納した後、ステップＳ３で、集約候補Ｂ１－２に格納したフロー情報のうちから順位の一番低いフロー情報を集約対象として抽出する。図３中、集約候補Ｂ１－２内の、最も左側に位置するフロー情報が集約対象となる。

【００６９】

次に、ステップＳ４で、初期集約条件として、フロー生成条件に比べて、条件を構成する項目が１つ少ない条件（バッファＢ２の集約条件）が設定される。すなわち、初期集約条件として、フロー生成条件のうちの、プロトコル、ソースアドレス、宛先アドレスおよび宛先ポートの４つの項目が設定される。次に、ステップＳ５で、検索対象バッファとして、設定された集約条件に対応するバッファを設定し、ステップＳ６で、そのバッファを検索する。この段階では、ステップＳ４で設定した初期集約条件に対応するバッファＢ２内に、集約対象と初期集約条件の全項目が一致する集約済みフロー情報があるか否かの判定が行われる。図１２に、バッファＢ２内の左から４番目の集約済みフロー情報が、集約対象と一致する状態が示されている。この場合、集約対象は、その４番目の集約済みフロー情報に集約される。なお、集約対象は、集約候補Ｂ１－２から削除される。

【００７０】

ステップＳ６での判定で「該当フロー無し」となった場合は、ステップＳ８で、検索対象バッファが集約候補Ｂ１－２であるか否か判断される。検索対象バッファが集約候補Ｂ１－２でない場合は、ステップＳ８で現在より１つ上位のバッファを検索対象バッファに設定し、ステップＳ６に移行して該当フローがあるか否かを判断する。図１３に、集約候補Ｂ１－２内の左から５番目のフロー情報が、集約対象と一致する状態が示されている。この場合、集約対象および５番目のフロー情報が集約されて集約済みフロー情報としてバッファＢ２に格納される。なお、集約対象および５番目のフロー情報は、集約候補Ｂ１－２から削除される。なお、上位のバッファの検索において、集約対象と合致するフロー情報が複数存在する場合がある。そのような場合は、それら複数のフロー情報のすべてを集約対象と集約する。

【００７１】

ステップＳ６での判定で「該当フロー無し」となり、ステップＳ８での判定で対象バッファが集約候補であると判断された場合は、ステップＳ１０で、集約条件が、条件を構成する項目が最も少ない条件（バッファＢ７に対応する集約条件）であるかが判断される。集約条件が、条件を構成する項目が最も少ない条件でない場合は、ステップＳ１１で、集約条件を現在より１つ項目の少ない条件に変更し、ステップＳ５に移行して、その変更した集約条件に対応するバッファを検索対象バッファに設定する。例えば、バッファＢ２の集約条件が初期集約条件として設定された場合において、バッファＢ２内に検索対象と集約条件の一致する集約済みフロー情報がなく、かつ、集約候補Ｂ１－２にも検索対象と集約条件の一致するフロー情報がない場合は、集約条件は、現在より１つ項目の少ない条件であるバッファＢ３の集約条件に変更され、集約対象バッファはバッファＢ３に設定される。そして、変更された集約条件で、バッファＢ３内の検索が行われる。図１４に、バッ

ファＢ３に対する検索の状態が示されている。この例では、バッファＢ３には、集約対象と集約条件の一致する集約済みフロー情報はないため、ステップＳ６での判断は「該当フロー無し」となる。

【００７２】

ステップＳ６～Ｓ９のループで、ステップＳ４またはステップＳ１１で設定した集約条件で、対象となるバッファの条件を段階的に変更する。また、ステップＳ５～Ｓ１１のループで、集約条件を段階的に変更する。この対象バッファおよび集約条件の段階的な変更により、集約に伴うフロー情報の欠落量を最小限にし、計測対象であるトラフィックにおける重要な情報を保持することが可能となっている。

【００７３】

また、この集約処理によれば、集約条件の項目数が必要以上に少なくならずに、集約対象を集約することができ、集約した分だけフロー情報の数が減少する。なお、図３、図１２～図１４に示したバッファの構成の例、図１１に示したアルゴリズムの例では、複数のバッファを移動して処理を行っているが、バッファ自体は１つでバッファ内の各フロー情報に集約の条件を示すIDを記録して識別する方法もある。全て集約の条件を構成する項目が異なる場合は、基本的にフロー送信機能部で創出されるテンプレートが異なることになり、その際、テンプレートIDが異なる。したがって、集約の条件を示すIDはテンプレートIDに相当する値を使えば良い。また、同様に集約され使わなくなったフロー情報は、バッファから削除する方法と、実際には削除せず、情報が無効である特別な有意のIDを付与して参照しない方法とがある。

【００７４】

図１１に示した集約処理の変形例として、ステップＳ２とＳ３の間で、初期のフロー情報の集約を行うことも考えられる。フロー情報は、フロー生成・集約条件として使われる項目が同じ値であっても、フローの終了によって別のフローとして数えられることがある。例えば、次のような２つの条件がある。

【００７５】

一つは、ＴＣＰなどのコネクション型プロトコルを用いる場合で、終了を示すメッセージ（ＴＣＰであれば、FIN、RSTなど）を観測した場合に、フローの終了として見なされる。もう１つは、一定時間毎にデータ送信を行うために、タイムアウト時間が設けられている場合で、このタイムアウト時間を越えたフローは一旦終了して、フロー生成・集約条件として使われる項目が同じ値の別のフロー情報として数えられる。タイムアウト時間としては、ＵＤＰなどのコネクションレス型プロトコル用の非継続時間（最終パケットからの経過時間）とＴＣＰなどのコネクション型プロトコル用の継続時間（開始パケットからの経過時間）の２種類がある。これらの条件によって、フロー生成・集約条件として使われる項目が同じ値であっても、別々のフローとして分断される可能性がある。

【００７６】

フロー集約条件を必要以上に小さくせずに、フロー情報をできる限り保持することを目的とする場合、集約条件削減の処理を行う前に、メッセージやタイムアウトによって分断されたフローの集約を行うことで、集約条件削減の処理を行う必要がなくなる場合がある。この場合は、フロー集約による情報の損失を最小限にとどめることができる。

【００７７】

なお、図１１に示した集約処理の、集約条件の段階的な変化の処理過程において、あらかじめ集約条件の項目が排他的である場合は、その項目についての検索は行わない。例えば、バッファＢ２の集約条件（プロトコル、ソースアドレス、宛先アドレスおよび宛先ポート）とバッファＢ３の集約条件（プロトコル、ソースアドレス、宛先アドレスおよびソースポート）は、項目数が同じであり、排他的である。したがって、バッファＢ３に対応する集約条件での検索処理においてバッファＢ２の検索はスキップすることが望ましい。

【００７８】

また、ステップＳ４で設定する初期集約条件は、プロトコル、ソースアドレス、宛先アドレスおよびソースポートの４つの項目に限定されるものでは当然ない。タイムアウトに

よって分断されたフローの集約を行う場合は、条件や優先度から導出される削減数０（フロー生成条件と同一）の条件を構成する項目となり、タイムアウトによって分断されたフローの集約を行わない場合は、削減数１の条件を構成する項目となる。

【００７９】

以上が基本的な条件削減方法である。この条件削減方法における処理の高速化を行うために、検索用のインデックス（索引）を作成することが考えられる。検索用インデックスを利用することで、検索回数を削減することができる。

【００８０】

検索用インデックスの作成には、例えば二分木のアルゴリズムを用いることができる。バランスの取れた二分木によれば、Log2Nの速度で検索を行うことが可能である。複数の項目毎に情報を持つフロー情報を二分木に保持する場合、２つの二分木の構築方法が考えられる。一般に、二分木の構築方法では、既に格納済みの要素の値と新規に挿入する要素の値を比較し、その大小関係によって格納位置を決定する。

【００８１】

第１の構築方法は、複数項目のうち、優先順位が上位の項目から大小比較を行う方法である。この第１の構築方法では、結果として複数項目の優先順位が上位の項目から値を上位の桁にマッピングしていき、１つの値に変換して、その値を大小比較する。

【００８２】

図１５は、第１の構築方法によって作成される検索用インデックスを説明するための図である。図１５に示す例では、フロー情報Ａ～Ｅに関する項目として、protocolIdentifier（優先順位は１）、destinationTransportPort（優先順位は２）、sourceIPv4Address（優先順位は３）、destinationIPv4Address（優先順位は４）、sourceTransportPort（優先順位は５）の５つの項目が与えられている。フロー情報Ａ～Ｅの間には、優先順位は設定されていない。これら項目に基づいて、検索用インデックスが以下の手順で作成される。

【００８３】

まず、Ａのフローをインデックスに追加する。このＡは１つめのフローとなるので、根として設定される。

【００８４】

次に、Ｂのフローをインデックスに追加する。そして、ＡおよびＢの各フローの項目の大小関係を優先順位の高い項目から順番に比較する。第１優先順位のprotocolIdentifierおよび第２優先順位のdestinationTransportPortの項目は、ＡおよびＢのフロー間で同じである。第３優先順位のsourceIPv4Addressの項目について、Ａのフローにおける値「10.0.0.1」よりＢのフローにおける値「10.0.0.2」の方が大きい。よって、Ａに代えてＢを根とし、Ａは左側の葉とされる。

【００８５】

次に、Ｃのフローをインデックスに追加する。そして、ＢおよびＣの各フローの項目の大小関係を優先順位の高い項目から順番に比較する。第１優先順位のprotocolIdentifierの項目について、Ｂのフローにおける値「６」よりＣのフローにおける値「１７」の方が大きい。よって、Ｃは右側の葉とされる。

【００８６】

次に、Ｄのフローをインデックスに追加する。そして、ＢおよびＤの各フローの項目の大小関係を優先順位の高い項目から順番に比較する。第１優先順位のprotocolIdentifierの項目について、Ｂのフローにおける値「６」よりＤのフローにおける値「１７」の方が大きい。よって、Ｄは右側の配置となる。ここで、右側には既にＣが存在するので、このＣとＤの各フローの項目の大小関係を優先順位の高い項目から順番に比較する。第２優先順位のdestinationTransportPortの項目について、Ｄのフローにおける値「10.0.0.1」よりＣのフローにおける値「192.168.0.1」の方が大きい。よって、ＤはＣの左側の葉とされる。

【００８７】

最後に、Ｅのフローをインデックスに追加する。そして、ＢおよびＥの各フローの項目の大小関係を優先順位の高い項目から順番に比較する。第１優先順位のprotocolIdentifierの項目について、Ｅのフローにおける値「１」よりＢのフローにおける値「６」の方が大きい。よって、Ｅは左側の配置となる。ここで、左側には既にＡが存在するので、このＡとＥの各フローの項目の大小関係を優先順位の高い項目から順番に比較する。第１優先順位のprotocolIdentifierの項目について、Ｅのフローにおける値「１」よりＡのフローにおける値「６」の方が大きい。よって、Ｅは、Ａの左側の葉とされる。

【００８８】

第２の構築方法は、最上位の項目から二分木を作成し、それ以下の項目は、上位の項目の葉を根とする方法である。図１６に、第２の構築方法によって作成される検索用インデックスを説明するための図である。図１６に示す例においても、フロー情報Ａ～Ｅに関する項目として、図１５に示した例と同様の優先順位を有する５つの項目が与えられており、これら項目に基づいて、検索用インデックスが以下の手順で作成される。

【００８９】

まず、Ａのフローをインデックスに追加する。ツリーの頂点となるポインタとして第１優先順位のprotocolIdentifierの要素（値：6）が追加され、このツリーの頂点となるポインタはその要素を指す。さらにその要素は、第２優先順位を指すポインタを保有する。同様にして、第２優先順位のdestinationTransportPortの要素（値：192.168.0.1）、第３優先順位のsourceIPv4Addresの要素（値：10.0.0.1）、第４優先順位のdestinationIPv4Addressの要素（値：80）、第５優先順位のsourceTransportPortの要素（値：23456）が追加され、そのツリーの下に要素番号（値：Ａ）を示す要素が追加される。

【００９０】

次に、Ｂのフローを追加する。第１優先順位のprotocolIdentifierの要素（値：6）、第２優先順位のdestinationTransportPortの要素（値：192.168.0.1）は、Ａのフローと同じであるため、Ａと同じツリーの要素をたどる。第３優先順位のsourceIPv4Addresの要素（値：10.0.0.2）は、既存の要素の「10.0.0.1」の右側の葉とされる。これ以降の優先順位の要素は、Ａのフローと同様の手順で、右側の葉とされた要素に追加され、そのツリーの下に要素番号（値：Ｂ）を示す要素が追加される。

【００９１】

次に、Ｃのフローを追加する。第１優先順位のprotocolIdentifierの要素（値：１７）は既存の要素（値：６）より大きいため、右側の葉とされる。これ以降の優先順位の要素は、Ａのフローと同様の手順で、右側の葉とされた要素に追加され、そのツリーの下に要素番号（値：Ｃ）を示す要素が追加される。

【００９２】

次に、Ｄのフローを追加する。第１優先順位のprotocolIdentifierの要素（値：１７）は、Ｃのフローと同じであるため、Ｃと同じツリーの要素をたどる。第２優先順位のdestinationTransportPortの要素（値：10.0.0.1）は、既存の要素（値：192.168.0.1）より小さいため、左側の葉とされる。これ以降の優先順位の要素は、Ａのフローと同様の手順で、左側の葉とされた要素に追加され、そのツリーの下に要素番号（値：Ｄ）を示す要素が追加される。

【００９３】

最後に、Ｅのフローを追加する。第１優先順位のprotocolIdentifierの要素（値：１）は既存の要素（値：６）より小さいため、左側の葉とされる。これ以降の優先順位の要素は、Ａのフローと同様の手順で、左側の葉とされた要素に追加され、そのツリーの下に要素番号（値：Ｅ）を示す要素が追加される。

【００９４】

上述した第１および第２の構築方法には、以下のような特徴がある。

【００９５】

第１の構築方法によれば、ツリー構造が単純で、ツリーが深くならずに済み、かつ、バランス（平衡木）を作成することができる。しかし、条件を構成する項目を削減して新た

な条件を作成する場合に、再度、ツリー構造を作り直す必要がある。

【００９６】

一方、第２の構築方法によれば、ツリーが深くなるが、重複する優先順位が存在しない限り、一度ツリー構造を作成すれば、条件を削減しても、一部の葉を集約することが可能であるので、再度ツリー構造を作り直す必要はない。また、例えば特定のポートを除外するといった、項目毎に情報の取り扱い方を変更することができる。ただし、第２の構築方法は、優先順位が重複する場合には適用することができない。

【００９７】

上述した第１または第２の構築方法によりインデックスを作成して保持し、フロー情報の生成および集約の際にその保持しているインデックスを参照して条件の削減を行うことで、生成および集約の処理の効率化を行うことが可能である。

【００９８】

具体的には、フロー生成機能部は、管理用バッファに格納されているフロー情報に対して、外部入力された項目の優先順位の順序に基づき、フロー情報が保持する項目毎に大小比較を繰り返してフロー情報間の大小を判定し、その結果を検索用索引として保持し、該検索用索引を参照してフロー情報の生成を行う。これにより、フロー情報の生成の際の条件（項目の組み合わせ）の比較回数を削減することができ、結果として、処理の効率化を図ることができる。

【００９９】

また、フロー情報数制限機能部は、管理用バッファに格納されているフロー情報に対して、外部入力された項目の優先順位の順序に基づき、フロー情報が保持する項目毎に大小比較を繰り返してフロー情報間の大小を判定し、その結果を検索用索引として保持し、該検索用索引を参照してフロー情報の集約を行う。これにより、フロー情報の集約の際の条件（項目の組み合わせ）の比較回数を削減することができ、結果として、処理の効率化を図ることができる。

【０１００】

なお、第１の構築方法において、条件毎にツリー構造を作り直す場合の効率低下を最小限に抑制する方法として、過去の同一条件の集約候補数と条件毎のフロー情報保持数を持つ方法がある。

【０１０１】

この方法では、フロー情報数制限機能部が、既に保持している上限値と非集約数を用いて算出される集約候補数と集約結果数及び、フロー情報制限時の集約条件の各項目毎のフロー数の履歴を記録し、次回以降の集約時にその記録情報に基づいて、検索用インデックスの作成時に用いる初期項目数を推測することで、検索用インデックスの作成回数を削減する。

【０１０２】

ここで、上限値は、最終的にフロー情報数制限機能部がフロー送信機能部に渡すフロー情報の数（外部から与えられるか、もしくは管理用バッファの容量から内部的に決定される）である。非集約数は、並び替え後に上位に位置する非集約となるフロー情報の数（外部から与えられる）である。集約候補数は、フロー生成機能部が生成したフロー情報の総数から非集約数を減算した値である。集約結果数は、集約した結果の値、即ち上限値から非集約数を減算した値である。

【０１０３】

以下、フロー情報数制限機能部による初期項目数の推測の処理を具体的に説明する。

【０１０４】

フロー情報数制限機能部は、各回毎に、生成されたフロー情報の総数から非集約数を減算して求められる集約候補数、上限値から非集約数を減算して求められる集約結果数、及び集約に用いた条件（フローキー）のうちの各情報の項目（Information Element）のそれぞれに関して、フロー情報の数を保持する。図１７に、フロー情報数制限機能部が保持する情報の一例を示す。図１７に示す例では、集約候補数、集約結果数、protocolIdenti

fier（優先順位は１）、destinationTransportPort（優先順位は２）、sourceIPv4Address（優先順位は３）、destinationIPv4Address（優先順位は４）、sourceTransportPort（優先順位は５）といった各項目の情報について、過去５回分の情報が記録される。

【０１０５】

例えば、直前の１回の情報を参照すると、集約候補数が１２００３４とされ、集約結果数が２００００とされる。そして、その集約結果数の内訳として、集約条件が第１優先順位までの項目を含んだ条件であるprotocolIdentifierのみ（図６の削減数４の条件）を用いて集約された結果のフロー数が４とされ、集約条件が第２優先順位までの項目を含んだ条件（図６の削減数３の条件）を用いて集約された結果のフロー数が６４４２とされ、集約条件が第３優先順位までの項目を含んだ条件（図６の削減数２の条件）を用いて集約された結果のフロー数が１２３２１とされ、集約条件が第４優先順位までの項目を含んだ条件（図６の削減数１の条件）を用いて集約された結果のフロー数が１２３３とされ、集約条件が第５優先順位までの項目を含んだ条件（図６の削減数０の条件）を用いて集約された結果のフロー数が０とされる。

【０１０６】

フロー数が０となった集約は結果的に必要のない集約とみなす。つまり、直前の１回の集約は、第５優先順位までの項目を含んだ条件を省略し、第４優先順位までの項目を含んだ条件からインデックスの作成を開始する。これにより、処理数が減り、処理速度が向上する。

【０１０７】

フロー情報数制限機能部では、過去の記録から集約を省略できる場合を判定する。図１７に示した例では、直前の１回、３回、５回において、第５優先順位までの項目を含んだ条件を用いた場合にフロー数が０となっている。そして、１回、３回、５回における集約時の集約候補数はそれぞれ、１２００３４、９３８９８、１０８２７０となっている。これらの情報を参照すると、集約結果数が２０００個である場合で、集約対象となるフロー情報数が、省略可能な状態の最小値である９３８９８個以上である場合は、第４優先順位までの項目を含んだ条件（すなわち、protocolIdentifier、protocolIdentifier、destinationTransportPort、destinationIPv4Addressの項目の組み合わせ）からインデックスを作り始めればよいと推測できる。この場合、第５優先順位までの項目を含んだ条件によるインデックスを作成する必要がなくなるので、その分、全体の処理を速くすることができる。

【０１０８】

以下、集約の一例を説明する。図１８に、ポートを集約する例を示す。図１８において、ＡおよびＢは、プロトコル、ソースアドレス、宛先アドレス、ソースポートおよび宛先ポートの５つの項目の条件（フロー生成条件）で生成されたフロー情報であり、Ｃは、これらフロー情報Ａ、Ｂを、そのフロー生成条件の各項目を集約条件として集約した集約済みフロー情報であり、この例ではソースポートが集約条件を構成する項目から削除されている。「SA」はソースアドレスであり、「DA」は宛先アドレスであり、「SAMask」および「DAMask」はネットマスクであり、「SP」はソースポートであり、「DP」は宛先ポートであり、「Packets」はパケット数であり、「octets」はバイト数であり、「First」はフローの開始時間であり、「Last」はフローの終了時間である。

【０１０９】

集約済みフロー情報Ｃでは、ソースポート「SP」の値は「０」とされ、パケット数「Packets」およびバイト数「octets」はそれぞれ、フロー情報Ａ、Ｂの対応する値を加算したものとされる。また、開始時間「First」および終了時間「Last」は、フロー情報Ａ、Ｂの対応する時間の和集合となる範囲に設定される。この例では、フロー情報Ａの開始時間「First」および終了時間「Last」はそれぞれ「134598098987」および「134598100384」とされ、フロー情報Ｂの開始時間「First」および終了時間「Last」はそれぞれ「134598098222」および「134598100001」とされているので、集約済みフロー情報Ｃの開始時間「First」および終了時間「Last」はそれぞれ「134598098222」および「134598100384」

とされる。このように、フロー情報Ａ、Ｂについて、ソースポート「SP」、パケット数「Packets」、バイト数「octets」、開始時間「First」および終了時間「Last」を集約することで集約済みフロー情報Ｃを得る。なお、この例では、フロー情報Ａ、Ｂでソースポートに共通項がないため、集約済みフロー情報Ｃでは、ソースポートを「０」としたが、複数のフローを集約する場合は、各フロー情報のうちデータ量など監視項目における任意の量が最も多かったフローの集約項目の値を代表値として利用してもよく、ソースポートの例においては最もデータ量の多かったソースポート番号を設定してもよい。また、フローの先頭パケットの情報を代表値として利用してもよいし、集約を行ったことを示す情報を追加してもよい。集約条件を構成する項目を削減した際に、テンプレートから該当するフィールド情報を構成する項目を削除する方式と、テンプレートからは削除せずにフローキーから削除する方式が考えられる。前者の場合は、削除された項目は送信されないため、内部的にどのような値を持っていても構わない。後者の場合は、削除された項目の代表値が送信される。なお、IPFIXプロトコルの規定によると、フローキーとして用いなかった項目は、最初に観測された値を使うことを推奨している。

【０１１０】

図１９に、アドレスを集約する例を示す。図１９において、ＡおよびＢは、プロトコル、ソースアドレス、宛先アドレス、ソースポートおよび宛先ポートの５つの項目の条件（フロー生成条件）で生成されたフロー情報であり、Ｃは、これらフロー情報Ａ、Ｂを、そのフロー生成条件のうちの、プロトコル、ソースアドレスおよび宛先アドレスの３つの項目を集約条件として集約した集約済みフロー情報である。

【０１１１】

集約済みフロー情報Ｃでは、図１８に示した場合と同様に、ソースポート「SP」の値は「０」とされ、パケット数「Packets」およびバイト数「octets」はそれぞれ、フロー情報Ａ、Ｂの対応する値を加算したものとされ、開始時間「First」および終了時間「Last」は、フロー情報Ａ、Ｂの対応する時間の和集合となる範囲に設定される。アドレスは、フロー情報Ａ、Ｂの対応するアドレスの値を積集合により得られる新たな値とされる。この例では、フロー情報Ａの宛先アドレス「192.168.0.2」とフロー情報Ｂの宛先アドレス「192.168.0.254」の積集合により、新たな宛先アドレス「192.168.0.0」を得る。このアドレス値の変更に伴い、ネットマスク「SAMask」も「24」に変更される。上記のテンプレートから削除する方式の場合は、集約条件を構成する項目から削除された項目に関する情報は送信されないため、上記同様に内部的にどのような値を持っていても構わない。フローキーから除外する方式の場合は、ここで例示しているIPv4環境下においては、SAMaskが３２ビット以外の場合は、送出する項目はアドレスを示す項目（sourceIPv4Address）ではなく、プリフィックスを示す項目（sourceIPv4Prefix）に変更して表現しなければならない。プリフィックスに変更しないのであれば、代表値を用いるべきであり、積集合をとる前の代表値（上記の通りプロトコル規定によると先頭パケットの値が好ましい。）を用いることになる。また、この場合は、SAMaskもホストアドレスを示す３２が用いられることになる。

【０１１２】

なお、本方式において、一定数以下に制限する場合に、削減数が最も多い状態における集約条件を構成する項目が取りうる値の総数が上限値として一定数以下に制限できることを保障する最低値となる。

【０１１３】

以上説明した本発明によれば、攻撃トラフィックによりフローが増大し、それに伴ってフロー生成機能部によって生成されるフロー情報の数が増大するが、フロー情報数制限機能部が、フロー生成機能部から入力されるフロー情報の数が増大すると、現在、格納しているフロー情報の一部（集約候補）を集約する。このフロー情報の集約により、フロー送信機能部に供給されるフロー情報の一定時間あたりの数が一定数以下に制限される。したがって、フロー送信機能部が、計測用ネットワーク上に送出するフロー情報の一定時間あたりの数も一定数以下に制限される。このように、フローの増大に関係なく、計測用ネッ

トワーク上には、一定数以下のフロー情報しか送信されないので、トランスポートプロトコルに輻輳制御機能のないＵＤＰを用いた場合において発生していた計測用ネットワークにおける通信の輻輳を抑制することができる。

【０１１４】

加えて、トラフィックの計測において重要な情報を含むフロー情報は、集約の対象から除外され、重要でないフロー情報を集約するようになっているので、計測目的において、トラフィックを特徴付けるフロー情報は保持される。

【０１１５】

さらに、集約する条件に含まれる比較項目が段階的に変更されるので、必要以上に項目が少ない条件で集約されることがなく、集約後のフロー情報における情報の損失を必要最小限に抑えることができる。

【０１１６】

また、フロー送信機能部には、一定数以下のフロー情報しか供給されないので、フロー送信機能部の内部バッファが溢れてフロー情報が欠落することもない。したがって、トランスポートプロトコルに輻輳制御機能のあるＴＣＰやＳＣＴＰを用いた場合に生じていた、フロー送信機能部の内部バッファの破綻によるフロー情報の欠落のために、観測したトラフィック全体の情報を正確に送信できない、といった問題も生じない。このように、トランスポートプロトコルに輻輳制御機能のあるＴＣＰやＳＣＴＰを用いた場合に生じていた、フロー送信機能部の内部バッファの破綻によるフロー情報の欠落を抑制することができるので、観測したトラフィック全体の情報を正確に測定用端末に送信することができる。

【０１１７】

以上説明した本実施形態のフロー情報制限装置（ノード）は、本発明の一例であり、その構成および動作は、本発明の趣旨を逸脱しない範囲で適宜に変更することができる。

【０１１８】

また、フロー生成機能部、フロー情報数制限機能部およびフロー送信機能部の各機能部における処理は、コンピュータシステムを構成する制御装置が記憶装置に格納されたプログラムを実行することで実現することが可能である。プログラムは、ＣＤ－ＲＯＭやＤＶＤなどのディスク型の記録媒体を通じて提供されてもよく、また、インターネットを通じて必要なプログラムをダウンロードすることで提供されてもよい。

【０１１９】

また、フローの生成条件および集約条件の項目の一例として、プロトコル、ソースＩＰアドレス、宛先ＩＰアドレス、ソースポートおよび宛先ポートの５つの項目を挙げたが、本発明はこれに限定されるものではない。フローの生成条件および集約条件の項目は、ヘッダ情報に基づいた情報を含むならば、これら以外の他の項目を含むものであっても、これら項目を含まないものであってもよい。ヘッダ情報に基づく情報とは、ヘッダそのものに含まれていなくても、ヘッダ情報から判断される情報も含まれる。一例としては、経路制御情報などもヘッダ情報に基づく情報に含まれる。また、ヘッダ情報は、ネットワーク層、トランスポート層に限定されず、それより下位及び上位のプロトコルも含む。また、フローの生成条件および集約条件の項目の数は、フローの生成および集約が可能な範囲で適宜に設定することができる。

【図面の簡単な説明】

【０１２０】

【図１】本発明が適用される情報通信システムの一例を示すブロック図である。

【図２】本発明のフロー情報制限装置の一実施形態であるノードの構成を示すブロック図である。

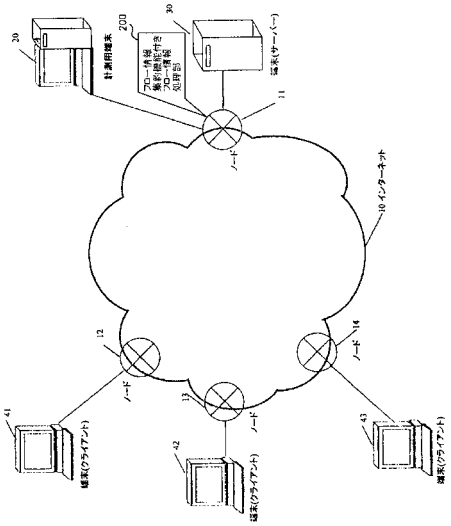
【図３】図２に示すフロー情報数制限機能部にて管理される管理用バッファの構造の一例を示す模式図である。

【図４】フロー情報およびデータ構造定義情報を説明するための図である。

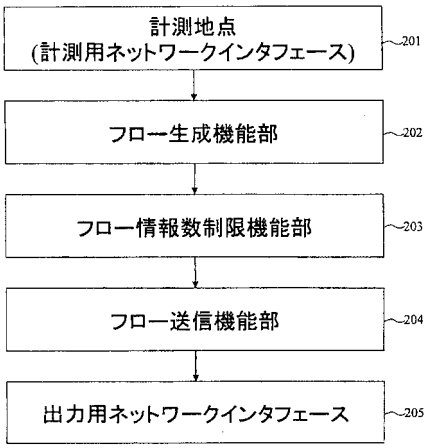
【図５】オプション情報による通知方法を説明するための図である。

【図６】条件優先度を付与した定義情報およびそれにより展開されて使用される条件の一例を示す模式図である。
【図７】条件優先度を付与した定義情報およびそれにより展開されて使用される条件の別の例を示す模式図である。
【図８】優先順位に関する外部入力を受け付けることのできるフロー情報処理部の構成を示すブロック図である。
【図９】定義情報の入力形式を説明するための図である。
【図１０】定義情報の別の入力形式を説明するための図である。
【図１１】図２に示すフロー情報数制限機能部にて行われるフロー情報集約処理の一手順を示すフローチャートである。
【図１２】図２に示すフロー情報数制限機能部によるフロー情報の集約の一例を示す模式図である。
【図１３】図２に示すフロー情報数制限機能部によるフロー情報の集約の別の例を示す模式図である。
【図１４】図２に示すフロー情報数制限機能部によるフロー情報の集約の他の例を示す模式図である。
【図１５】検索用インデックスの作成手順を説明するための図である。
【図１６】検索用インデックスの別の作成手順を説明するための図である。
【図１７】条件毎にツリー構造を作り直す場合の効率低下を抑制する方法を説明するための図である。
【図１８】ポートを集約する例を示す模式図である。
【図１９】アドレスを集約する例を示す模式図である。
【図２０】計測用ネットワークを含む情報通信システムの一般的な構成を示すブロック図である。
【符号の説明】
【０１２１】
１０　インターネット
１１～１４　ノード
２０　計測用端末
３０、４１～４３　端末
２００　フロー情報処理部
２０１　計測用ネットワークインタフェース
２０２　フロー生成機能部
２０３　フロー情報数制限機能部
２０４　フロー送信機能部
２０５　出力用ネットワークインタフェース

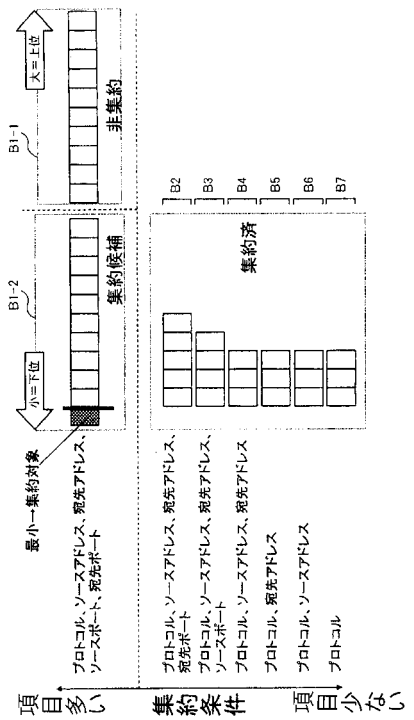
【図１】



【図２】



【図３】



【図４】

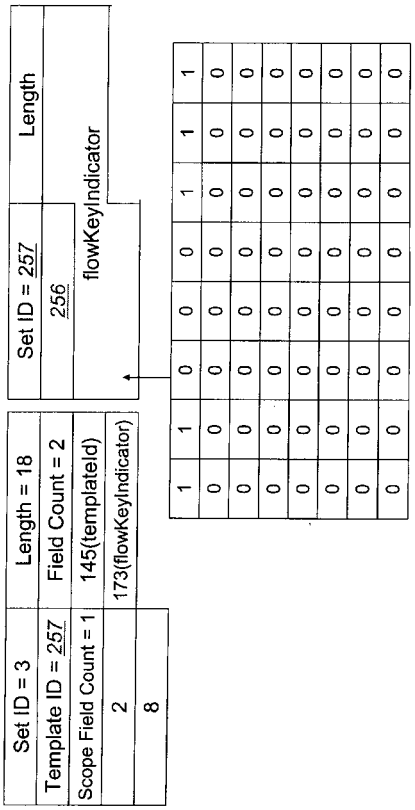
・フロー情報

Set ID = 256	Length = 44
sourceIPv4Address (例:192.168.0.1)	
destinationIPv4Address (例: 192.168.0.2)	
sourceIPv4PrefixLength	destinationIPv4PrefixLength
ipClassOfService	protocolIdentifier
sourceTransPort	destinationTransPort
packetDeltaCount	
octetDeltaCount	
flowStartSysUpTime	
flowEndSysUpTime	

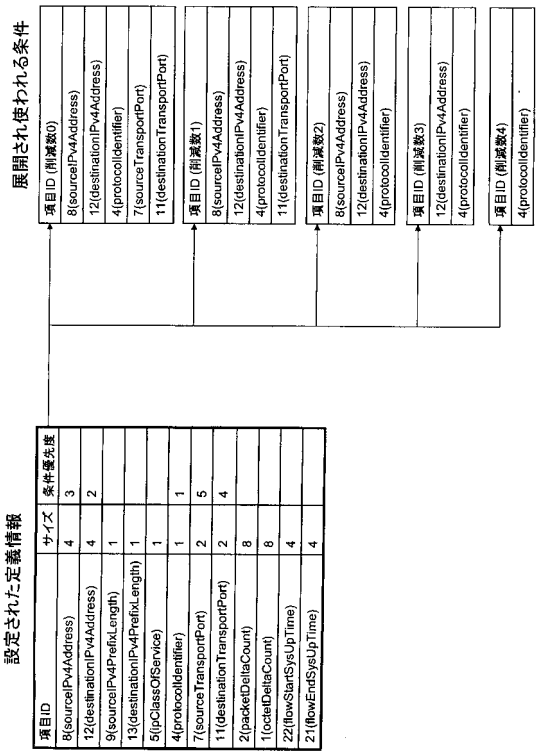
・データ構造定義情報

Set ID = 2	Length = 56
Template ID = 256	Field Count = 12
8(sourceIPv4Address)	4
12(destinationIPv4Address)	4
9(sourceIPv4PrefixLength)	1
13(destinationIPv4PrefixLength)	1
5(ipClassOfService)	1
4(protocolIdentifier)	1
7(sourceTransportPort)	2
11(destinationTransportPort)	2
2(packetDeltaCount)	8
1(octetDeltaCount)	8
22(flowStartSysUpTime)	4
21(flowEndSysUpTime)	4

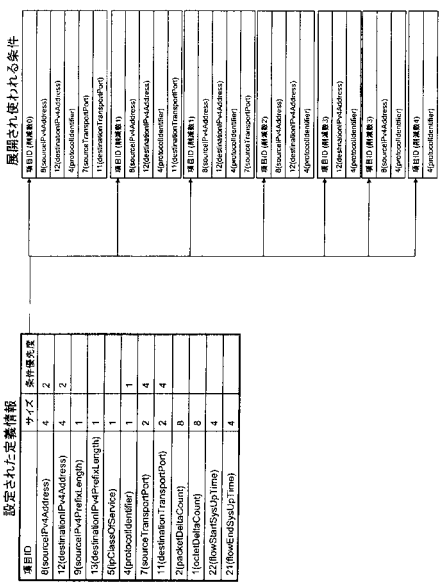
【図５】


・オプションデータ構造定義情報
・オプション情報
Set ID = 3
Length = 18
Template ID = 257
Field Count = 2
Scope Field Count = 1
145(templateId)
2
173(flowKeyIndicator)
8
Set ID = 257
Length
256
flowKeyIndicator

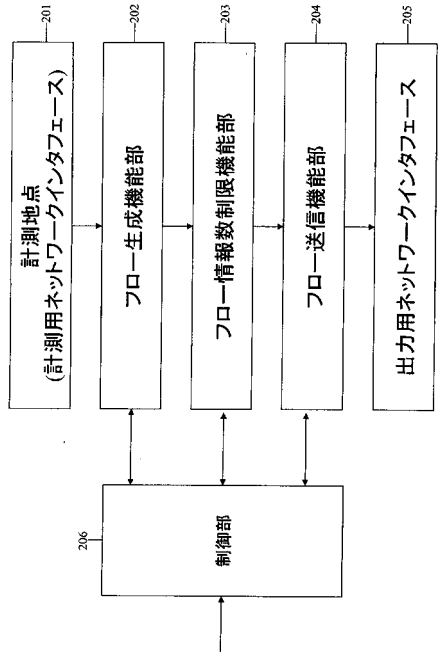
【図６】


設定された定義情報
展開され使われる条件
項目ID
サイズ
条件優先度
8(sourceIPv4Address)
12(destinationIPv4Address)
9(sourceIPv4PrefixLength)
13(destinationIPv4PrefixLength)
5(ipClassOfService)
4(protocolIdentifier)
7(sourceTransportPort)
11(destinationTransportPort)
2(packetDeltaCount)
1(octetDeltaCount)
22(flowStartSysUpTime)
21(flowEndSysUpTime)
項目ID (削減数0)
項目ID (削減数1)
項目ID (削減数2)
項目ID (削減数3)
項目ID (削減数4)

【図７】


設定された定義情報
展開され使われる条件
項目ID
サイズ
条件優先度

【図８】


計測地点
(計測用ネットワークインタフェース)
フロー生成機能部
フロー情報数制限機能部
フロー送信機能部
出力用ネットワークインタフェース
制御部
201
202
203
204
205
206

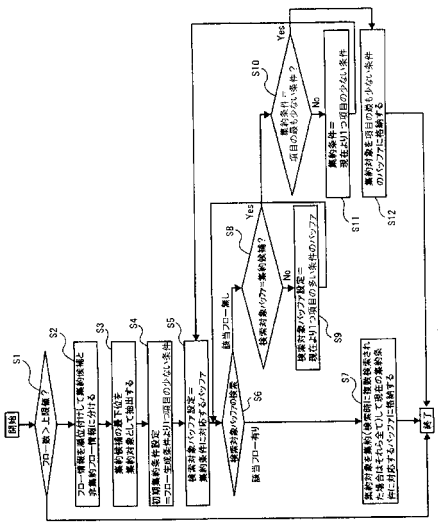
【図９】

8,4,3
12,4,2
9,1
13,1
5,1
4,1,1
7,2,5
11,2,4
2,8
1,8
22,4
21,4

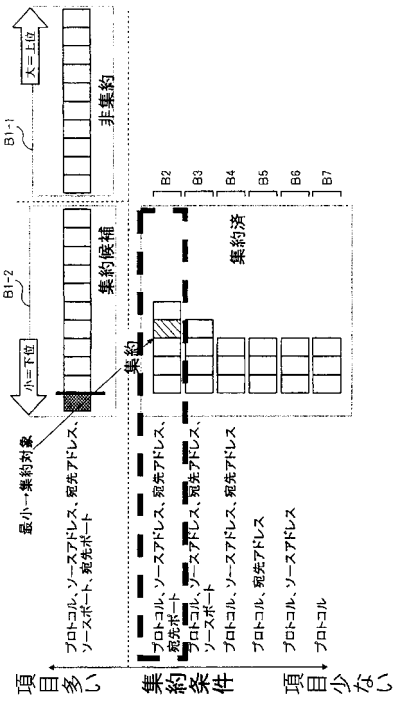
【図１０】

```
<meteringProcess id="1">
    <flowMetering>
      <rule>
        <templateId>256</templateId>
        <flowKey>
          <fieldName>sourceIPv4Address</fieldName>
          <flowKeyPrecedence>3</flowKeyPrecedence>
        </flowKey>
        <flowKey>
          <fieldName>destinationIPv4Address</fieldName>
          <flowKeyPrecedence>2</flowKeyPrecedence>
        </flowKey>
        <nonFlowKey>
          <fieldName>sourceIPv4Prefix</fieldName>
        </nonFlowKey>
        <nonFlowKey>
          <fieldName>destinationIPv4Prefix</fieldName>
        </nonFlowKey>
        <nonFlowKey>
          <fieldName>ipClassOfService</fieldName>
        </nonFlowKey>
        <flowKey>
          <fieldName>protocolIdentifier</fieldName>
          <flowKeyPrecedence>1</flowKeyPrecedence>
        </flowKey>
        <flowKey>
          <fieldName>sourceTransportPort</fieldName>
          <flowKeyPrecedence>5</flowKeyPrecedence>
        </flowKey>
        <flowKey>
          <fieldName>destinationTransportPort</fieldName>
          <flowKeyPrecedence>4</flowKeyPrecedence>
        </flowKey>
        <nonFlowKey>
          <fieldName>packetDeltaCount</fieldName>
          <fieldLength>8</fieldLength>
        </nonFlowKey>
        <nonFlowKey>
          <fieldName>octetDeltaCount</fieldName>
          <fieldLength>8</fieldLength>
        </nonFlowKey>
        <nonFlowKey>
          <fieldName>flowStartSeconds</fieldName>
        </nonFlowKey>
        <nonFlowKey>
          <fieldName>flowEndSeconds</fieldName>
        </nonFlowKey>
      </rule>
    </flowMetering>
    <next>
      <exportingProcessId>1</exportingProcessId>
    </next>
</meteringProcess>
```

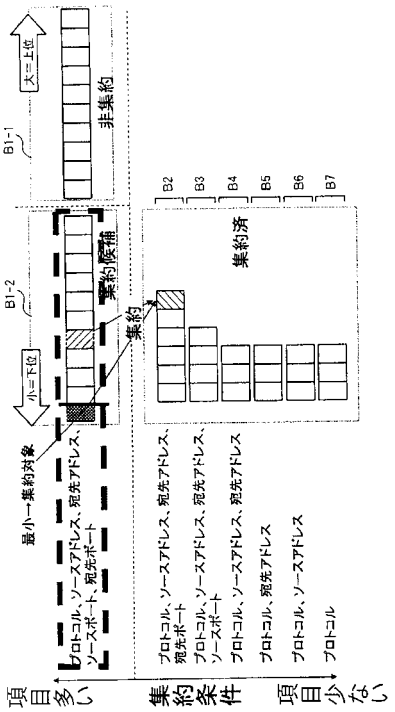
【図１１】



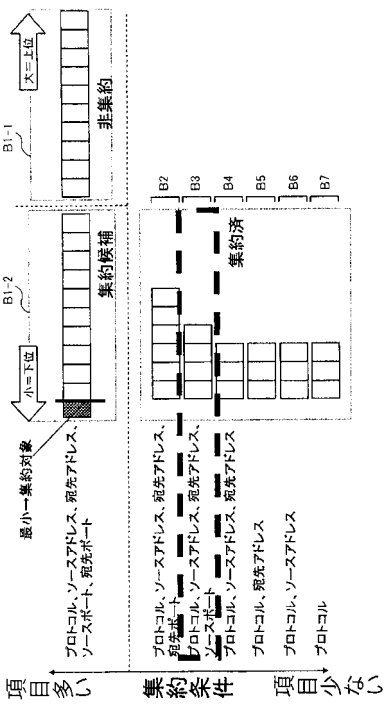
【図１２】



【図１３】

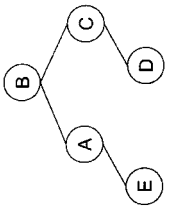


【図１４】



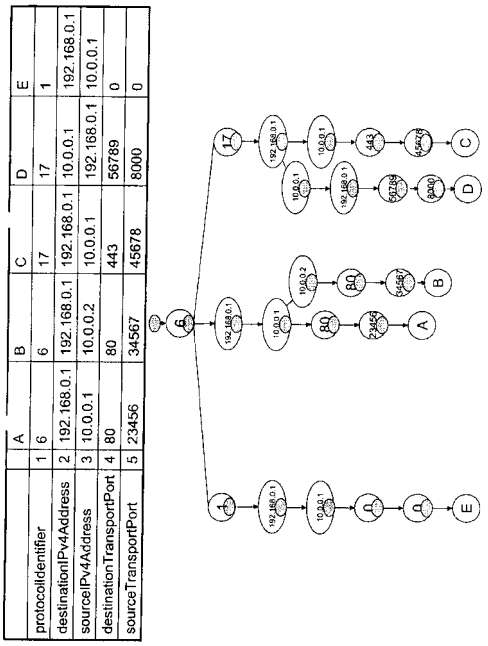
【図１５】

	A	B	C	D	E
protocolIdentifier	6	6	17	17	1
destinationIPv4Address	192.168.0.1	192.168.0.1	192.168.0.1	10.0.0.1	192.168.0.1
sourceIPv4Address	10.0.0.1	10.0.0.2	10.0.0.1	192.168.0.1	10.0.0.1
destinationTransportPort	80	80	443	56789	0
sourceTransportPort	23456	34567	45678	8000	0



【図１６】

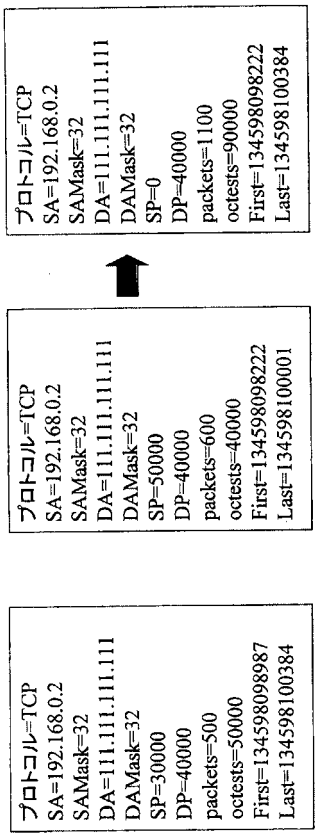
	A	B	C	D	E
protocolIdentifier	1 6	6	17	17	1
destinationIPv4Address	2 192.168.0.1	192.168.0.1	192.168.0.1	10.0.0.1	192.168.0.1
sourceIPv4Address	3 10.0.0.1	10.0.0.2	10.0.0.1	192.168.0.1	10.0.0.1
destinationTransportPort	4 80	80	443	56789	0
sourceTransportPort	5 23456	34567	45678	8000	0



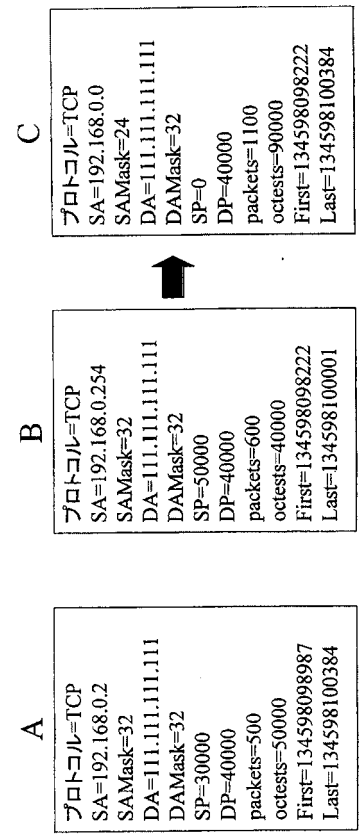
【図１７】

履歴番号	1	2	3	4	5
集約対象数	120034	250219	38984	40000	108270
集約結果数	20000	20000	20000	20000	20000
protocolIdentifier	14	0	4	4	4
destinationIPv4Address	26442	23	5656	278	7131
sourceIPv4Address	312321	1111	11223	879	10342
destinationTransportPort	41233	8765	3117	7728	2523
sourceTransportPort	50	10101	0	11111	0

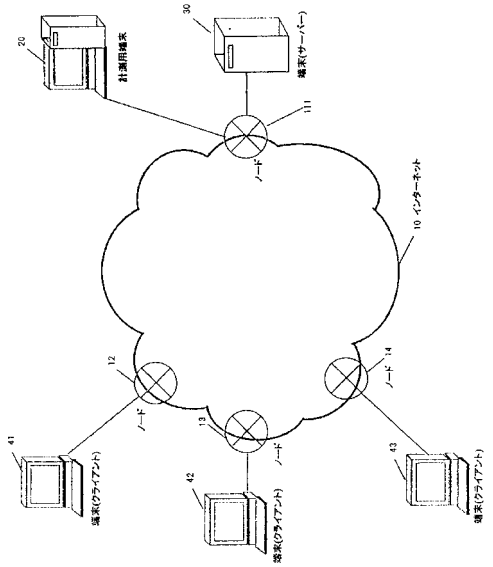
【図１８】



【図１９】



【図２０】



フロントページの続き

(56)参考文献 特開２００６－５０４４２（ＪＰ，Ａ）
国際公開第０２／１３４８６（WO，Ａ１）
特開２００１－２５７７２２（ＪＰ，Ａ）
入野仁志、片山勝，パケット特性を用いたフローアカウンティング手法の提案，２００６年電子情報通信学会総合大会，日本，社団法人電子情報通信学会，２００６年　3月　8日，B-7-119，p.215

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５６
Ｈ０４Ｌ　１２／２２