(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4361570号
(P4361570)

(45)発行日　平成21年11月11日(2009.11.11)　(24)登録日　平成21年8月21日(2009.8.21)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
H04L 12/56	(2006.01)	H04L	12/56	400Z
H04L 12/28	(2006.01)	H04L	12/28	200M
G06F 13/00	(2006.01)	G06F	13/00	353B

請求項の数 3　(全 17 頁)

(21)出願番号　特願2007-44902(P2007-44902)
(22)出願日　平成19年2月26日(2007.2.26)
(65)公開番号　特開2008-211415(P2008-211415A)
(43)公開日　平成20年9月11日(2008.9.11)
審査請求日　平成19年2月26日(2007.2.26)

(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)

(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　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　大倉　一浩
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　八木　毅
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

最終頁に続く

(54)【発明の名称】パケット制御命令管理方法

(57)【特許請求の範囲】

【請求項１】

パケットを疎通する複数の中継装置と、前記複数の中継装置の通過パケットを監視する複数の監視機能と、制御命令に従って前記中継装置を制御する複数の制御機能を含むネットワークにおいて、前記制御命令を管理するネットワーク管理機能を備えるネットワーク管理装置のパケット制御命令管理方法であって、

前記ネットワーク管理装置は、パケット情報受信手段と実行中制御命令特定手段と制御命令更新判定手段と判定結果出力手段とを有し、

前記パケット情報受信手段が、前記監視機能により通過パケットを監視される中継装置の識別子である中継装置識別子と、当該中継装置が収容する受信端末のアドレスである受信端末アドレスと、当該受信端末の受信パケット流量を含むパケット情報を、前記監視機能から受信するパケット情報受信ステップと、

前記実行中制御命令特定手段が、前記パケット情報に含まれる中継装置識別子を用いて、中継装置識別子と受信端末アドレスと制御命令を含むレコードを記録可能であり、中継装置識別子により、レコード検索可能なテーブルである制御命令テーブルを検索し、前記監視機能により流量変動が監視された通過パケットを疎通する中継装置と、当該中継装置が実行中の制御命令及び受信端末アドレスとを含む判定対象レコードを特定する実行中制御命令特定ステップと、

前記制御命令更新判定手段が、前記実行中制御命令特定ステップで特定された判定対象レコードの受信端末アドレスと前記パケット情報が通知する受信端末アドレスとを比較し

て一致する場合は、当該パケット情報が通知するパケット流量の値と所定のパケット流量閾値とを比較して当該受信端末アドレス毎にパケット制御の必要性を判定し、一致しない場合は、前記制御命令テーブルに新規レコードを生成し当該パケット情報が通知するパケット流量の値と所定のパケット流量閾値とを比較して当該受信端末アドレス毎にパケット制御の必要性を判定することにより、当該受信端末アドレス毎に制御命令の登録、解除及び変更を含む状態の更新判定を行う制御命令更新判定ステップと、

前記判定結果出力手段が、前記制御命令更新判定ステップ後、前記受信端末アドレス毎に前記更新判定の結果を出力する判定結果出力ステップと、

を備えることを特徴とするパケット制御命令管理方法。

【請求項２】

請求項１に記載のパケット制御命令管理方法であって、

前記制御命令テーブルは、中継装置識別子と受信端末アドレスと制御命令とフラグを含むレコードを記録可能であり、中継装置識別子と受信端末アドレスとにより、レコード検索可能なテーブルであり、

前記実行中制御命令特定手段は、前記実行中制御命令特定ステップにおいて、

特定した判定対象レコードについて、検索された旨のフラグ値である判定対象フラグ値を当該判定対象レコードの記録域に記録し、

前記制御命令更新判定手段は、前記制御命令更新判定ステップにおいて、

前記判定対象レコードが記録する受信端末アドレスの全てと、前記パケット情報が含む受信端末アドレスの全てとを比較する受信端末アドレス比較ステップを実施した結果、当該二つの受信端末アドレスが一致する場合、

当該受信端末アドレスを記録する当該判定対象レコードの記録域に、当該受信端末アドレス宛のパケット流量が前記監視機能により監視されている旨を示すフラグ値である監視フラグ値を記録する第一の状態更新ステップを実施し、当該第一の状態更新ステップを実施したうえで、当該パケット情報が含む当該受信端末アドレス宛のパケット流量の値が、所定のパケット流量閾値よりも大きいとき、当該判定対象レコードの記録域に閾値超過フラグ値を記録し、

前記受信端末アドレス比較ステップを実施した結果、前記二つの受信端末アドレスが一致せず、かつ前記パケット情報に含まれ前記制御命令テーブルに記録されていない受信端末アドレスが存在する場合、

当該制御命令テーブルに新たなレコードを追加し、当該レコードの記録域に当該パケット情報が含む中継装置識別子及び当該受信端末アドレス、並びに判定対象フラグ値、監視フラグ値及び新たなレコードを追加した旨のフラグ値である追加フラグ値を記録する第二の状態更新ステップを実施し、当該第二の状態更新ステップを実施したうえで、当該受信端末アドレス宛のパケット流量の値が、前記パケット流量閾値よりも大きいとき、当該レコードの記録域に閾値超過フラグ値を記録し、

前記制御命令出力手段は、前記制御命令出力ステップにおいて、

前記制御命令テーブルを検索し、判定対象フラグ値、監視フラグ値、閾値超過フラグ値、及び追加フラグ値に対する所定のフラグ値組合せである制御命令管理識別子に該当するレコードを特定し、当該レコードが記録する受信端末アドレスを当該制御命令管理識別子とともに出力する、

ことを特徴とするパケット制御命令管理方法。

【請求項３】

請求項２に記載のパケット制御命令管理方法であって、

前記パケット情報受信手段は、前記パケット情報受信ステップにおいて、

受信パケット流量の時系列波形変化情報である差分受信パケット流量を含むパケット情報を受信し、

前記制御命令更新判定手段は、前記制御命令更新判定ステップにおいて、

差分受信パケット流量に対する閾値である差分パケット流量閾値と前記パケット流量閾値を受信端末アドレス毎に記録した閾値テーブルを使用し、

前記受信端末アドレス比較ステップを実施した結果、
前記第一の状態更新手段又は第二の状態更新手段を実施したうえで、
当該受信端末アドレスに該当する閾値テーブルが記録するパケット流量閾値と差分パケット流量閾値を、前記パケット情報の当該受信端末アドレスに該当する受信パケット流量と差分受信パケット流量に対して各々比較し、
当該受信パケット流量の値が当該パケット流量閾値より大きいとき、当該受信端末アドレスを記録する前記判定対象レコードの記録域に閾値超過フラグ値を記録し、
当該差分受信パケット流量の値が当該差分パケット流量閾値より大きいとき、当該判定対象レコードの記録域に差分閾値超過閾値フラグ値を記録し、
前記制御命令出力手段は、前記制御命令出力ステップにおいて、
前記制御命令テーブルを検索し、判定対象フラグ値、監視フラグ値、閾値超過フラグ値、差分閾値超過フラグ値、及び追加フラグ値に対する所定のフラグ値組合せに該当するレコードを特定し、当該レコードが記録する受信端末アドレスを、当該フラグ値組合せの所定の識別子である制御命令管理識別子とともに出力する、
ことを特徴とするパケット制御命令管理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、パケットを疎通する複数の中継装置と、通過パケットを監視する複数の監視機能と、制御命令に従って中継装置を制御する複数の制御機能を含むネットワークにおいて、制御命令を管理するネットワーク管理機能を備えるネットワーク管理装置のパケット制御命令管理方法に関し、制御命令の設定、解除及び変更を含む状態の更新判定と管理を行い、複数の制御機能相互間での重複実行や、単一制御機能の重複実行を防止することで、制御機能の整合性を担保することができるパケット制御命令管理方法に関する。

【背景技術】

【０００２】

近年、ＤｏＳ（Denial of Service）攻撃やＤＤｏＳ（Distributed Denial of Service）攻撃、あるいは災害時トラヒック等の異常トラヒックを構成するパケットを制御する目的から、ＩＳＰ（Internet Service Provider）ネットワークの中継装置が疎通するパケットのヘッダ情報を含んだパケット疎通情報を監視し、パケットの送信先ＩＰアドレスである受信端末アドレスと通過パケット量を含んだ情報でなるパケット情報に基づいて、中継装置でパケット制御を行う機能の重要性が増している。

【０００３】

従来技術における監視機能として、ＩＤＳ（Intrusion Detection System）やＰｒｏｂｅ装置を利用し、受信端末を収容する中継装置の近傍で局所的に適用される周知技術が存在する。

【０００４】

また、非特許文献１及び非特許文献２には、ネットワーク全域を広域に監視する広域監視機能により異常トラヒック発生を推定した上で、受信端末アドレス単位での詳細監視を行う階層型監視機能も開示されている。

【０００５】

このように、従来技術として複数の監視機能が存在しており、目的に応じて異なる監視装置を使い分ける運用形態が考えられる。

【０００６】

一方、従来技術における制御機能として、ルータなどの中継装置を想定した場合、ＡＣＬ（Access ControI List）を使用した通過パケットの遮断制御やＱｏＳ（Quality of Service）制御などの公知なパケット制御が存在する。

【０００７】

この場合、当該ＩＳＰネットワークにおける異常パケットの流出地点に位置するＥｇｒｅｓｓ中継装置に対し、ＡＣＬを設定する単純な制御機能がある。また、ネットワーク内

に大量の異常パケットが流入することによる輻輳発生を防止するため、Ｅｇｒｅｓｓ中継装置に加えて、流入地点に位置するＩｎｇｒｅｓｓ中継装置に対して、ＡＣＬを同時設定する制御機能（以下、「遡り制御機能」と記載する）が非特許文献３において開示されている。

【０００８】

また、非特許文献４では、ＤＤｏＳ攻撃を構成するパケットのパケットヘッダ情報をより詳細に分析し、高精度に異常パケットを識別した上でパケット制御を実行することを目的とし、異常パケットを攻撃軽減装置に迂回する制御機能（以下、「迂回制御機能」と記載する）が開示されている。

【０００９】

制御機能から複数の中継装置に対して送信される制御コマンドの整合性を担保する従来技術として、特許文献１に開示されている技術が存在している。特許文献１の技術は、複数の中継装置が各々異なる制御コマンドの書式を解釈する装置形態を前提とし、制御機能が制御コマンドを送信する際、個々の中継装置が解釈可能な書式に変換する技術である。これにより、オペレータが制御コマンド書式の差異を意識することが不要となり、中継装置の管理コストと設定ミスを軽減するという課題を解決している。

【００１０】

【非特許文献１】廣川祐他、“次世代バックボーン向けトラヒック監視システムの開発”、２００６電子情報通信学会総合大会、ＢＳ－５－１１、Ｍａｒｃｈ．２００６

【非特許文献２】大倉一浩他、“階層型監視制御方式の設計”、２００６電子情報通信学会総合大会、Ｂ－７－７０、Ｓｅｐｔｅｍｂｅｒ．２００６

【非特許文献３】Hitoshi Fuji et al., “MovingFirewall: A Countermeasure against Distributed Denial of Service Attacks”, NTT Technical Review, Vol.1 No.5 Aug. 2003 (http://www.ntt.co.jp/tr/0308/files/ntr200308085.pdf)

【非特許文献４】八木毅他、“ＤＤｏＳ攻撃軽減装置の共有化のための網制御方式”、２００６電子情報通信学会総合大会、Ｂ－７－３３、Ｓｅｐｔｅｍｂｅｒ．２００６

【特許文献１】特開２０００－２４４５６７号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

上述のように、複数の監視機能と制御機能が従来技術として開示されており、多種多様な異常トラヒックの発生に対する適応性を高める為には、これら複数の機能を異常性の種類や程度に応じて、柔軟に使い分けることが重要である。このことを踏まえ、本発明は、図１に示すように、複数の中継装置、監視機能、及び制御命令により制御される制御機能を含むネットワークと、制御命令を管理するネットワーク管理機能からなる構成を前提としている。

【００１２】

図１に示す複数の監視機能と制御機能からなる構成を前提とした場合、特許文献１が開示する技術では、中継装置と制御機能の間で送受信される制御コマンドを矛盾なく生成、更新することは可能となるが、複数の制御機能間での重複実行を防止するなどの制御機能の動作に関する整合性を担保することは出来ない。

【００１３】

例えば、特定の受信端末アドレスを有するパケットに対して遡り制御機能が実行されている場合、異常パケットは当該ＩＳＰネットワークのＩｎｇｒｅｓｓ中継装置においてパケット制御されているため、同ネットワーク内に問題となる異常パケットは通過していない。この状態で、同受信端末アドレスを有するパケットに対して迂回制御機能を実行しても、迂回制御対象のパケットが存在しないため、本制御機能の効果は生まれない。

【００１４】

また、特定の受信端末アドレスを有するパケットに対して迂回制御機能を実行している場合であって、同パケットに対してＥｇｒｅｓｓ中継装置でパケット遮断制御を行う制御

機能を実行したとき、迂回制御機能によりパケットヘッダ情報の詳細分析を伴う高精度なパケット制御を実行する目的にもかかわらず、Ｅｇｒｅｓｓ中継装置において同受信端末アドレスを含んだ正規パケットが一律、遮断されるため、迂回制御機能の効果は生まれない。

【００１５】

更に、個々の制御機能の実行と解除の整合性を担保するために、制御機能の重複実行を防止する必要がある。

【００１６】

このように、複数の制御機能を使い分ける運用形態を想定した場合、各制御機能の実行状態を管理し、制御機能の新たな実行の設定、実行中の制御機能の解除、又はその種別の変更などの動作の更新処理における整合性を担保することが大きな課題となっている。

【００１７】

なお、図１において、ネットワーク管理機能を用いず、監視機能において本課題を解決する機能を具備する形態を考えた場合、複数の監視機能が存在することから、制御機能の実行状態を各監視機能がそれぞれ管理する必要が生じ、課題の解決が困難となる。従って、本発明では、ネットワーク管理機能が集中して制御機能の実行状態を管理する機能配備を採用している。

【００１８】

この発明は、従来技術では解決できない上述の課題を解消するためになされたものであって、複数の制御機能の実行状態の管理と更新処理の整合性を担保することで、オペレータの操作ミスを防止し、管理コストを低減することを目的としている。

【課題を解決するための手段】

【００１９】

上述する課題を解決し、目的を達成するため、請求項１に係る発明は、パケットを疎通する複数の中継装置と、前記複数の中継装置の制御命令に従って前記中継装置を制御する制御機能を含むネットワークにおいて、前記制御命令を管理するネットワーク管理機能を備えるネットワーク管理装置のパケット制御命令管理方法であって、ネットワーク管理装置はパケット情報受信手段、実行中制御命令特定手段、制御命令更新判定手段及び判定結果出力手段を有することを特徴としている。

【００２０】

そして、前記パケット情報受信手段が、前記監視機能により通過パケットを監視される中継装置の識別子である中継装置識別子と、当該中継装置が収容する受信端末のアドレスである受信端末アドレスと、当該受信端末の受信パケット流量を含むパケット情報を、前記監視機能から受信するパケット情報受信ステップと、前記実行中制御命令特定手段が、前記パケット情報に含まれる中継装置識別子を用いて、中継装置識別子と受信端末アドレスと制御命令を含むレコードを記録可能であり、中継装置識別子により、レコード検索可能なテーブルである制御命令テーブルを検索し、前記監視機能により流量変動が監視された通過パケットを疎通する中継装置と、当該中継装置が実行中の制御命令及び受信端末アドレスとを含む判定対象レコードを特定する実行中制御命令特定ステップと、前記制御命令更新判定手段が、前記実行中制御命令特定ステップで特定された判定対象レコードの受信端末アドレスと前記パケット情報が通知する受信端末アドレスとを比較して一致する場合は、当該パケット情報が通知するパケット流量の値と所定のパケット流量閾値とを比較して当該受信端末アドレス毎にパケット制御の必要性を判定し、一致しない場合は、前記制御命令テーブルに新規レコードを生成し当該パケット情報が通知するパケット流量の値と所定のパケット流量閾値とを比較して当該受信端末アドレス毎にパケット制御の必要性を判定することにより、当該受信端末アドレス毎に制御命令の登録、解除及び変更を含む状態の更新判定を行う制御命令更新判定ステップと、前記判定結果出力手段が、前記制御命令更新判定ステップ後、前記受信端末アドレス毎に前記更新判定の結果を出力する判定結果出力ステップと、を備えることを特徴とする。

【００２１】

また、請求項２の発明は、上記の発明において、前記制御命令テーブルは、中継装置識別子と受信端末アドレスと制御命令とフラグを含むレコードを記録可能であり、中継装置識別子と受信端末アドレスとにより、レコード検索可能なテーブルであり、前記実行中制御命令特定手段は、前記実行中制御命令特定ステップにおいて、特定した判定対象レコードについて、検索された旨のフラグ値である判定対象フラグ値を当該判定対象レコードの記録域に記録し、前記制御命令更新判定手段は、前記制御命令更新判定ステップにおいて、前記判定対象レコードが記録する受信端末アドレスの全てと、前記パケット情報が含む受信端末アドレスの全てとを比較する受信端末アドレス比較ステップを実施した結果、当該二つの受信端末アドレスが一致する場合、当該受信端末アドレスを記録する当該判定対象レコードの記録域に、当該受信端末アドレス宛のパケット流量が前記監視機能により監視されている旨を示すフラグ値である監視フラグ値を記録する第一の状態更新ステップを実施し、当該第一の状態更新ステップを実施したうえで、当該パケット情報が含む当該受信端末アドレス宛のパケット流量の値が、所定のパケット流量閾値よりも大きいとき、当該判定対象レコードの記録域に閾値超過フラグ値を記録し、前記受信端末アドレス比較ステップを実施した結果、前記二つの受信端末アドレスが一致せず、かつ前記パケット情報に含まれ前記制御命令テーブルに記録されていない受信端末アドレスが存在する場合、当該制御命令テーブルに新たなレコードを追加し、当該レコードの記録域に当該パケット情報が含む中継装置識別子及び当該受信端末アドレス、並びに判定対象フラグ値、監視フラグ値及び新たなレコードを追加した旨のフラグ値である追加フラグ値を記録する第二の状態更新ステップを実施し、当該第二の状態更新ステップを実施したうえで、当該受信端末アドレス宛のパケット流量の値が、前記パケット流量閾値よりも大きいとき、当該レコードの記録域に閾値超過フラグ値を記録し、前記制御命令出力手段は、前記制御命令出力ステップにおいて、前記制御命令テーブルを検索し、判定対象フラグ値、監視フラグ値、閾値超過フラグ値、及び追加フラグ値に対する所定のフラグ値組合せである制御命令管理識別子に該当するレコードを特定し、当該レコードが記録する受信端末アドレスを当該制御命令管理識別子とともに出力する、ことを特徴とする。

【００２２】

また、請求項３の発明は、請求項２の発明において、前記パケット情報受信手段は、前記パケット情報受信ステップにおいて、受信パケット流量の時系列波形変化情報である差分受信パケット流量を含むパケット情報を受信し、前記制御命令更新判定手段は、前記制御命令更新判定ステップにおいて、差分受信パケット流量に対する閾値である差分パケット流量閾値と前記パケット流量閾値を受信端末アドレス毎に記録した閾値テーブルを使用し、前記受信端末アドレス比較ステップを実施した結果、前記第一の状態更新手段又は第二の状態更新手段を実施したうえで、当該受信端末アドレスに該当する閾値テーブルが記録するパケット流量閾値と差分パケット流量閾値を、前記パケット情報の当該受信端末アドレスに該当する受信パケット流量と差分受信パケット流量に対して各々比較し、当該受信パケット流量の値が当該パケット流量閾値より大きいとき、当該受信端末アドレスを記録する前記判定対象レコードの記録域に閾値超過フラグ値を記録し、当該差分受信パケット流量の値が当該差分パケット流量閾値より大きいとき、当該判定対象レコードの記録域に差分閾値超過閾値フラグ値を記録し、前記制御命令出力手段は、前記制御命令出力ステップにおいて、前記制御命令テーブルを検索し、判定対象フラグ値、監視フラグ値、閾値超過フラグ値、差分閾値超過フラグ値、及び追加フラグ値に対する所定のフラグ値組合せに該当するレコードを特定し、当該レコードが記録する受信端末アドレスを、当該フラグ値組合せの所定の識別子である制御命令管理識別子とともに出力する、ことを特徴とする。

【発明の効果】

【００２３】

請求項１の発明によれば、複数の前記制御機能を使い分ける運用形態を想定した場合、各制御機能の実行状態を管理し、いずれかの制御機能の新たな実行の設定、実行中の制御機能の解除、又はその種別の変更などの動作の更新処理における整合性を担保することが

できるという効果を奏する。

【００２４】

請求項１の発明によれば、パケット情報を受信した後、監視機能により流量変動が監視された通過パケットを疎通する中継装置と、当該中継装置が実行中の制御命令及び受信端末アドレスとを、制御命令の実行状態に関する情報を管理する制御命令テーブルを用いて効率的に特定することを可能とし、実装上、容易に実現することができるという効果を奏する。

【００２５】

また、請求項２の発明によれば、前記制御命令テーブルのレコード情報及びそのフラグ値を用いることにより、前記受信端末アドレス毎に制御命令が実行中か否かの判定処理と、当該受信端末アドレス毎にパケット制御の必要性の判定処理とを、効率的に実行することを可能とし、実装上、容易に実現することができるという効果を奏する。

【００２６】

また、請求項２の発明によれば、前記受信端末アドレス毎に更新判定の結果を効率的に出力することを可能とし、実装上、容易に実現することができるという効果を奏する。

【００２７】

また、請求項３の発明によれば、差分受信パケット流量を含めた精度の高い制御命令更新処理を行うことを可能とし、あわせて、前記閾値テーブルにより受信端末アドレス毎にパケット流量閾値及び差分パケット流量閾値をあらかじめ設定することで、受信端末のパケット処理能力の差異を考慮した精度の高い制御命令更新処理を効率的に実行することを可能とし、実装上、容易に実現することができるという効果を奏する。

【００２８】

また、請求項３の発明によれば、差分受信パケット流量を含めた制御命令更新処理の更新判定の結果を効率的に出力することを可能とし、実装上、容易に実現することができるという効果を奏する。

【発明を実施するための最良の形態】

【００２９】

以下に添付図面を参照して、パケット制御命令管理方法の実施例１～２を詳細に説明する。

各実施例の説明に先立って、本発明の実施形態にかかるパケット制御命令管理方法の概要を図１により説明しておく。本実施形態は、複数の中継装置４－１～３、複数の監視機能２－１～２、制御命令に従って中継装置４－１～３を制御する複数の制御機能３－１～３を含むネットワークにおいて、制御命令を管理するネットワーク管理機能１を備えるネットワーク管理装置のパケット制御命令管理方法に関する。

【００３０】

ネットワーク管理機能１は、ネットワーク管理機能を備えるネットワーク管理装置により実現される。監視機能２－１～２は、それぞれ監視機能を備える監視装置により実現される。制御機能３－１～３は、それぞれ制御機能を備える制御装置により実現されるか、あるいは、その一部又は全部が前記ネットワーク管理装置の内部において実現されていてもよい。これらのネットワーク管理装置、監視装置、制御装置は、コンピュータと記憶装置に記憶されたプログラムで構成することができる。また、そのプログラムの一部または全部に代えてハードウェアを用いて構成してもよい。また、ネットワーク管理装置、監視装置、制御装置のそれぞれを複数の装置が連携して動作する装置として構成してもよい。また、それらの装置が他の機能を有していてもよい。

【００３１】

中継装置４－１～３は、監視機能２－１～２に対してパケット疎通情報（図１の（１））を定期的あるいは、監視機能２－１～２の要求に応じて送信する。パケット疎通情報は、ルータ等が汎用的に具備しており、公知の技術であるｓＦｌｏｗデータあるいはＮｅｔＦｌｏｗデータによって構成されてもよい。

【００３２】

監視機能２－１～２は、パケット疎通情報に基づいて異常トラヒックの分析を実行し、その結果としてパケット情報（図１の（２））をネットワーク管理機能１に送信する。パケット情報は、異常トラヒックを構成するパケットの送信先ＩＰアドレスである受信端末アドレスを含み、異常性を示す値として、受信パケット流量、あるいは、時系列的な受信パケット流量の変化量を示す差分受信パケット流量を含んだ情報で構成される。

【００３３】

ネットワーク管理機能１は、パケット情報を受信した後、内部テーブルである制御情報テーブルを使用して、受信端末アドレス毎に制御命令管理識別子を出力し、オペレータへのコンピュータ画面等を介した通知を行う。その後、オペレータが、通知された受信端末アドレスと制御命令管理識別子に対して、制御命令の送信判断を行い、その結果、制御機能３－１～３に対して制御命令（図１の（３））が送信される。

【００３４】

制御命令管理識別子は、制御機能３－１～３のいずれか一つの新規実行である「設定」、実行中の制御機能の停止である「解除」、実行中の制御機能の停止と他の制御機能の新規実行である「変更」と、実行中の制御機能は継続実行するがパケット情報のみをオペレータに通知する「情報通知」（又は「情報表示」）と、更新処理を実行しない「無処理」の識別子を含んだ情報で構成される。

【００３５】

オペレータは、受信端末アドレス毎に制御管理識別子を通知され、各制御管理識別子で指定された処理の実行をするか否かを判断する。その後、制御命令が送信された制御機能は、その制御処理を実行する為に中継装置４－１～３のいずれかに対して制御コマンド（図１の（４））を送信する。制御コマンドは、ＣＬＩ（Command Line Interface）等の汎用的にルータ等の中継装置が具備するＡＣＬエントリの登録、変更、削除機能等により実現されてもよい。

【実施例１】

【００３６】

実施例１では、請求項２の発明の実施例について、図２～６を用いて説明する。図２は、ネットワーク管理機能１の機能ブロック図であり、図３は制御命令テーブルの構成例である。図４は、パケット情報のメッセージ例であり、図５は本実施例のフローチャートである。図６は、ネットワーク管理機能１が受信したパケット情報に対して、パケット流量閾値を使用した制御命令管理識別子の評価要件を示す。

【００３７】

まず、図１に記載のネットワーク管理機能１の機能ブロックについて図２を用いて説明する。ネットワーク管理機能１は、監視機能送受信インターフェース１ｈ及び制御機能送受信インターフェース１１を備えている。これらは、ＬＡＮ（Local Area Network）あるいはＷＡＮ（Wide Area Network）インターフェースボードなどの通信デバイスであり、他の監視機能２２－１～２や制御機能３－１～３とのメッセージ送受信処理を行う。

【００３８】

監視機能通信部１ｆ，１ｇは、各々、監視機能２２－１，２からパケット情報を受信し、受信端末アドレス、受信パケット流量及び差分受信パケット流量などのパケット情報の構成情報を解釈し、監視機能選択部１ｄを介して、ネットワーク管理部１ｂにデータ送信する。

【００３９】

その後、ネットワーク管理部１ｂは、制御命令テーブル１ａのレコードに対して検索、参照、更新などの処理を行い、パケット受信情報と制御命令テーブル１ａのレコード情報から、受信端末アドレス毎に制御命令管理識別子を生成し、オペレータインターフェース１ｍを介してオペレータに通知する。制御命令テーブル１ａは、汎用的なＤＢ（DataBase）を用いて実現されても良いし、ハードディスク上のデータファイルにより実現されても良い。

【００４０】

オペレータは、オペレータインターフェースを介して、受信端末アドレス毎に通知される制御命令管理識別子に基づいて制御判断を行い、これに基づき、ネットワーク管理部１ｂは制御機能選択部１ｅを介して制御機能通信部１ｉ，ｊ，ｋのいずれかを選択し、制御命令が制御機能送受信インターフェース１１を介して、制御機能２３－１～３に送信される。

【００４１】

次に、制御命令テーブル１ａのレコード構成を、図３を用いて説明する。「レコード識別子」は、制御命令テーブルのレコード（行）を一意に特定する識別子である。「中継装置識別子」、「受信端末アドレス」及び「制御命令」は、制御命令を実行中の中継装置に該当する中継装置識別子と、制御命令の実行対象であるパケットの送信先ＩＰアドレスである受信端末アドレスと、その実行中の制御機能を各々示している。例えば、レコード識別子（０１ａ）のレコードは、中継装置識別子（ＥＲ１）の中継装置が疎通するパケットを対象にした制御命令が実行中であり、受信端末アドレス（１０．１．１．２）を送信先ＩＰアドレスに持つパケットに対して、制御機能１が実行中であることを示す。また、「フラグ」情報属性として、「判定対象」、「監視」、「閾値超過」及び「追加」が存在し、その用途は図５において後述するフローチャートで説明することとする。

【００４２】

尚、「制御命令管理識別子」は、制御命令テーブルの各レコードに対して、図５に記載するフローチャートの処理を実行した場合の、受信端末アドレス毎に判定される制御命令管理識別子を示している。例えば、レコード識別子（０１ａ）のレコードは、現在、受信端末アドレス１０．１．１．２のパケットに対して制御機能１を実行中であり、パケット情報を新たに受信した結果、受信パケット流量がパケット流量閾値を超えているため、閾値超過フラグが値１を持ち、制御機能１以外の制御機能を選択して異常トラヒックの対処をする事が可能である旨の制御命令管理識別子（変更）が付与されていることを示している。

【００４３】

続いて、監視機能２－１～２からネットワーク管理機能１が受けるパケット情報の情報属性を、図４を用いて説明する。情報属性として、「中継装置識別子」は、監視装置が通過パケットを監視しているＥｇｒｅｓｓ中継装置に該当する中継装置識別子を示す。「＃」は、異常トラヒック情報を一意に特定する識別番号であり、＃１の行は、受信端末アドレス（１０．１．１．２）への通過パケットが、受信パケット量（８００Ｍｂｐｓ）である旨の異常トラヒック情報を示している。このように、監視装置により異常性が特定された異常トラヒック情報が、受信端末アドレス毎にパケット情報を介して、ネットワーク管理機能１に通知される構成が示されている。

【００４４】

更に、図３の制御命令テーブルと図４のパケット情報を使用し、請求項２の発明の実施例のフローチャートを、図５を用いて説明する。ネットワーク管理機能１は、パケット情報（図４）を受信した後（Ｓ１０１）、パケット情報に含まれる中継装置識別子と受信端末アドレスを取得する（Ｓ１０２）。この際、受信端末アドレスは複数存在する場合があるため、これらを本フローチャートでは「Ａ」と標記する。パケット情報に含まれる中継装置識別子を用いて、制御命令テーブル（図３）を検索し（Ｓ１０３）、該当レコードの有無により分岐ステップ（Ｓ１０４）において分岐先が分かれる。

【００４５】

該当レコードが存在する場合、当該レコードを「判定対象レコード」とし、判定対象フラグを１に更新する。本フローチャートでは「Ｂ」と標記する。当該処理は，請求項に記載の実行中制御命令特定ステップに対応しており、これ以降の処理ステップ（Ｓ１０６～１１９）が制御命令更新判定ステップに対応する。尚、処理ステップ（Ｓ１２０）は、請求項に記載の制御命令出力ステップに対応している。また、図２のネットワーク管理部１ｂの機能を実現する手段が、請求項の実行中制御命令特定手段と制御命令更新判定手段と判定結果出力手段に対応し、図２の監視機能通信部１ｆ、１ｇの機能を実現する手段が、

請求項のパケット情報受信手段に対応する。ただし、これらは請求項を実施例に限定するものではない。

【００４６】

処理ステップ（Ｓ１０６～１０９）は、Ａの要素のいずれか一つの「ａ」と、Ｂの要素のいずれか一つの「ｂ」とを選択し、該当する受信端末アドレスを比較している。すなわち、Ａに未処理の受信端末が有るかどうかを判断し（Ｓ１０６）、有る場合は未処理の受信端末アドレスを選択する。本フローチャートでは選択した受信端末アドレスを「ａ」と表記する（Ｓ１０７）。ａに対し、未処理のレコードがＢに有るかどうかを判断し（Ｓ１０８）、有る場合は未処理のレコードの受信端末アドレスを選択する。本フローチャートでは選択した未処理のレコードの受信端末アドレスを「ｂ」と表記する（Ｓ１０９）。処理ステップ（Ｓ１０８）で、無い場合は処理ステップ（Ｓ１０６）に戻る。処理ステップ（Ｓ１０６）で、無い場合は処理ステップ（Ｓ１２０）に進む。

【００４７】

処理ステップ（Ｓ１１０）において、ａとｂの値が同じ場合は、パケット情報に含まれる受信端末アドレス（ａ）に対して、既に、いずれかの制御機能が実行され、制御命令テーブルに受信端末アドレス（ｂ）のレコードが存在している状態に該当する。このとき、処理ステップ（Ｓ１１２）により受信パケット流量とパケット流量閾値の評価を行い、閾値超過フラグの更新（Ｓ１１３）を実行する。処理ステップ（Ｓ１１０）において、ａとｂが一致しない場合は、制御命令テーブルに新規レコードを生成し、新規に制御機能を実行するか否かの判定を行うために、処理ステップ（Ｓ１１４，１１２，１１３）によりフラグ更新処理を実行する。すなわち、処理ステップ（Ｓ１１４）において、制御命令テーブルに新規レコードを生成する。本フローチャートでは新規レコードの受信端末アドレスを「ｂ」と表記する。ｂの判定対象フラグを１に更新し、ｂの監視フラグを１に更新し、ｂの追加フラグを１に更新する。その後、処理ステップ（Ｓ１１２～１１３）において、ａの受信パケット流量がパケット流量閾値以上である場合に、ｂの閾値超過フラグを１に更新する。

【００４８】

処理ステップ（Ｓ１１６～１１９）は、パケット情報で通知される中継装置識別子に該当するＥｇｒｅｓｓ中継装置に対して、制御命令が全く実行されていない場合に（Ｓ１０４の分岐先「Ｎ」）、制御命令テーブルに新規レコードを生成する処理（Ｓ１１４，１１２，１１３）を同様に実行する処理ステップである。

【００４９】

制御命令テーブルに対するフラグ更新処理が終了した時点で、処理ステップ（Ｓ１２０）により、フラグ値の組合せに対する所定の制御命令管理識別子を特定し、オペレータインターフェース部１ｍへの出力が実行される。すなわち、処理ステップ（Ｓ１２０）において、次の処理がなされる。閾値超過及び追加フラグが共に値１のレコードの受信端末アドレスを、「設定」とする。判定対象、監視及び閾値超過フラグの全てが値１、かつ、追加フラグが値０のレコードの受信端末アドレスを、「変更」とする。判定対象フラグが値１、かつ、監視及び追加フラグが共に値０のレコードの受信端末アドレスを、「解除」とする。判定対象及び監視フラグが共に値１、かつ、閾値超過及び追加フラグが共に値０のレコードの受信端末アドレスを、「情報表示」とする。追加フラグが値１、かつ、閾値超過フラグが値０のレコードの受信端末アドレスを、「無処理」とする。そして、この制御命令管理識別子をオペレータインターフェースへ出力する。

【００５０】

以上のフローチャート動作の整理として、図６に、パケット情報で通知される受信端末アドレスに対して、パケット流量閾値の評価を行い、制御命令識別子の割当処理を行う評価要件を示す。（ａ）は制御命令実行中の受信端末アドレスの評価要件であり、（ｂ）は制御命令が実行中でない受信端末アドレスの評価要件である。

【００５１】

（ａ）の場合、すなわち、制御命令が実行中の場合は、例えば、パケット情報で通知さ

れた一の受信端末アドレスが、パケット流量閾値以上の受信パケット流量を持つ場合は、制御命令管理識別子（変更）が割当られ、現在実行中の制御機能に変えて、新たな制御機能の実行判断の機会がオペレータに提供される。受信端末アドレスが、パケット流量閾値以下の受信パケット流量を持つ場合は、制御命令管理識別子（情報表示）が割当られ、パケット情報がオペレータに通知される。尚、制御命令が実行中であり、制御命令テーブルに登録済みの受信端末アドレスが、パケット情報で非通知の場合は、監視装置により当該受信端末アドレスに送信されるパケットの異常性の終了が検知されている状態であるため、制御命令管理識別子（解除）が割当られ、実行中の制御機能の停止判断の機会がオペレータに提供されることとなる。

【００５２】

（ｂ）の場合、すなわち、制御命令が実行中でない場合は、パケット情報で通知された一の受信端末アドレスが、パケット流量閾値以上の受信パケット流量を持つ場合は、制御命令管理識別子（設定）が割当られ、パケット流量閾値以下の受信パケット流量を持つ場合は、制御命令管理識別子（無処理）が割当られる。

【００５３】

制御命令管理識別子がオペレータインターフェースへ出力された後、オペレータは、受信端末アドレス毎に通知される制御命令管理識別子に基づいて制御判断を行い、これに基づき、ネットワーク管理部１ｂは制御機能選択部１ｅを介して制御機能通信部１ｉ，ｊ，ｋのいずれかを選択し、制御命令が制御機能送受信インターフェース１１を介して、制御機能３－１～３に送信される。同時に、ネットワーク管理部１ｂは制御命令テーブル１ａ（図３）の「制御命令」の欄に、その値（「制御機能１」等）を記述する。なお、図３の「制御未実行」は制御命令が未実行であることを示す。

【実施例２】

【００５４】

実施例２では、請求項３の発明の実施例について、図７～１２を用いて説明する。図７は、制御命令テーブルの構成例である。図８は、図２に記載の閾値テーブル１ｃの構成例であり、図９はパケット情報のメッセージ例であり、図１０及び１１は本実施例のフローチャートである。図１２は、本実施例において、ネットワーク管理機能が受信したパケット情報に対して、パケット流量閾値を使用した制御命令管理識別子の評価要件を示す。

【００５５】

実施例２は、実施例１に対し、異常性の判断要素としてパケット情報に差分受信パケット流量を付加し、これを所定の差分パケット流量閾値と比較している。これにより、受信端末アドレスに対する制御命令管理識別子の付与処理を、トラヒックの異常性に対して精度高く行うことを可能としている。また、所定の閾値であるパケット流量閾値と差分パケット流量閾値を、受信端末アドレス毎に予め設定することを可能とし、異常トラヒックから防御すべきサーバ等の処理能力を加味して、制御命令の更新判断を行うことを可能としている。

【００５６】

図７の制御命令テーブル例では、新たに「差分超過閾値」フラグが追加されている。本フラグは、図９のパケット情報のメッセージ例で新たに追加されたパケット情報の「差分受信パケット流量」に対する差分パケット流量閾値の評価結果を記録するフラグである。

【００５７】

図８は、図２に記載の閾値テーブル１ｃの構成例である。「受信端末アドレス」毎に予め、「パケット流量閾値」と「差分パケット流量閾値」を決定しておくことが可能となる。この際、受信端末アドレスは一のＩＰアドレス単位としてもよいし、図８に示すように、ネットワークアドレス単位に決定し設定してもよい。

【００５８】

図１０及び１１は、新たに追加した差分超過閾値フラグ、差分受信パケット流量及び差分パケット流量閾値に関する処理ステップが、Ｓ２１５、Ｓ２１９及びＳ２２０に記載されている。なお、Ｓ２１５及び２１９のフローチャートは、図１１に個別フローチャート

として記載されている。

【００５９】

図１０は、処理ステップ（Ｓ２１５，Ｓ２１９，Ｓ２２０）以外の処理ステップについては、実施例１の図５と同じであるので、処理ステップ（Ｓ２１５，Ｓ２１９，Ｓ２２０）についてのみ説明する。

【００６０】

処理ステップ（Ｓ２１５）と処理ステップ（Ｓ２１９）は同じ処理を行うステップであり、図１１に詳細が示されている。図１１において、ａの受信パケット流量ｌがパケット流量閾値以上かどうかを判断し（Ｓ３０１）、閾値以上の場合は、ｂの閾値超過フラグを１に更新する（Ｓ３０２）。ａの差分受信パケット流量が差分パケット流量閾値以上かどうかを判断し（Ｓ３０３）、閾値以上の場合は、ｂの差分閾値超過フラグを１に更新する（Ｓ３０４）。処理ステップ（Ｓ３０１）で閾値以上でない場合は、ａの差分受信パケットが差分パケット流量閾値以上かどうかを判断し（Ｓ３０５）、閾値以上の場合は、ｂの差分閾値超過フラグを１に更新する（Ｓ３０６）。

【００６１】

また、処理ステップ（Ｓ２２０）においては次のように処理を行う。閾値超過、差分閾値超過及び追加フラグが共に値１のレコードの受信端末アドレスを、「設定」とする。判定対象、監視及び閾値超過フラグの全てが値１、かつ、追加フラグが値０のレコードの受信端末アドレスを、「変更」とする。判定対象フラグが値１、かつ、監視及び追加フラグが共に値０のレコードの受信端末アドレスを、「解除」とする。判定対象及び監視フラグが共に値１、かつ、閾値超過及び追加フラグが共に値０のレコードの受信端末アドレスを、「情報表示」とする。追加フラグが値１、かつ、閾値フラグ及び差分閾値超過フラグが値０のレコードの受信端末アドレスを、「無処理」とする。そして、この制御命令管理識別子をオペレータインターフェース部１ｍへ出力する。

【００６２】

以上のフローチャートに記載した動作の整理として、パケット情報で通知される受信端末アドレスに対して、パケット流量閾値及び差分パケット流量閾値の評価を行い、制御命令識別子の割当処理を行う評価要件を図１２にまとめている。

【００６３】

図１２は、実施例１の図６の「制御命令管理識別子」の欄を、「差分パケット流量閾値の評価」が「閾値以上」と「閾値以下」で分けたものである。（ａ）は制御命令実行中の受信端末アドレスの評価要件であり、（ｂ）は制御命令が実行中でない受信端末アドレスの評価要件である。図１２（ａ）、すなわち、制御命令実行中の受信端末アドレスについては、図６（ａ）と同じである。一方、図１２（ｂ）、すなわち、制御命令が実行中でない受信端末アドレスについては、図６（ｂ）とは異なり、「パケット流量閾値が閾値以上」かつ「差分パケット流量閾値が閾値以上」の場合のみ、制御命令管理識別子（設定）が割当られ、それ以外の場合は、制御命令管理識別子（無処理）が割当られる。

【００６４】

実施例１と同様に、制御命令管理識別子がオペレータインターフェースへ出力された後、オペレータが、受信端末アドレス毎に通知される制御命令管理識別子に基づいて制御判断を行い、制御命令が制御機能３－１～３に送信され、同時に、制御命令テーブル１ａ（図７）の「制御命令」の欄に、その値（「制御機能１」等）が記述される。

【００６５】

以上、実施例１と実施例２に基づいて、本発明の実施例のネットワーク管理装置のパケット制御命令管理方法を詳細に説明したが、一般的には、次のようにパケット制御命令を管理する。まず、ネットワーク管理装置は、パケット情報受信手段と実行中制御命令特定手段と制御命令更新判定手段と判定結果出力手段とを有する。そして、前記パケット情報受信手段が、前記監視機能が通知するパケット情報を受信する。次に、前記実行中制御命令特定手段が、前記パケット情報に基づいて、前記監視装置により流量変動が監視された通過パケットを疎通する中継装置と、当該中継装置が実行中の制御命令及び受信端末アド

レスとを特定する。次に、前記制御命令更新判定手段が、特定された受信端末アドレスと前記パケット情報が通知する受信端末アドレスとを比較して受信端末アドレス毎に制御命令が実行中であるか否かを判定し、当該パケット情報が通知するパケット流量の値と所定のパケット流量閾値とを比較して当該受信端末アドレス毎にパケット制御の必要性を判定することにより、当該受信端末アドレス毎に制御命令の登録、解除及び変更を含む状態の更新判定を行う。そして、前記判定結果出力手段が、前記制御命令更新判定ステップ後、前記受信端末アドレス毎に前記更新判定の結果を出力する。

【００６６】

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】

【００６７】

【図１】本発明の実施形態のネットワークとネットワーク管理機能を示す図である。

【図２】本発明の実施形態のネットワーク管理機能の機能ブロック図である。

【図３】実施例１の制御命令テーブルの構成例である。

【図４】実施例１のパケット情報のメッセージ例である。

【図５】実施例１のフローチャートである。

【図６】実施例１の制御命令管理識別子の評価要件を示す図である。

【図７】実施例２の制御命令テーブルの構成例である。

【図８】実施例２の閾値テーブルの構成例である。

【図９】実施例２のパケット情報のメッセージ例である。

【図１０】実施例２のフローチャート（その１）である。

【図１１】実施例２のフローチャート（その２）である。

【図１２】実施例２の制御命令管理識別子の評価要件を示す図である。

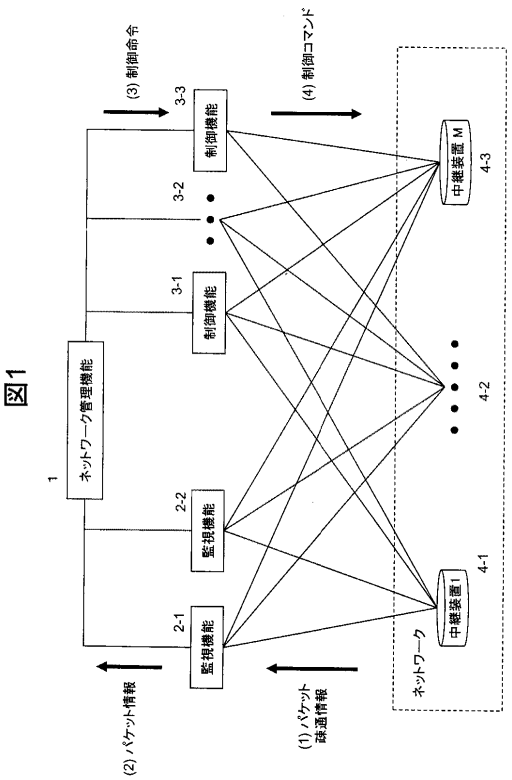
【符号の説明】

【００６８】

１…ネットワーク管理機能、１ａ…制御命令テーブル、１ｂ…ネットワーク管理部、１ｃ…閾値テーブル、１ｄ…監視機能選択部、１ｅ…制御機能選択部、１ｆ、１ｇ…監視機能通信部、１ｈ…監視機能送受信インターフェース、１ｉ、１ｊ、１ｋ…制御機能通信部、１ｌ…制御機能送受信インターフェース、１ｍ…オペレータインターフェース部、２－１～２、２２－１～２…監視機能、３－１～３、２３－１～３…制御機能、４－１～３…中継装置。

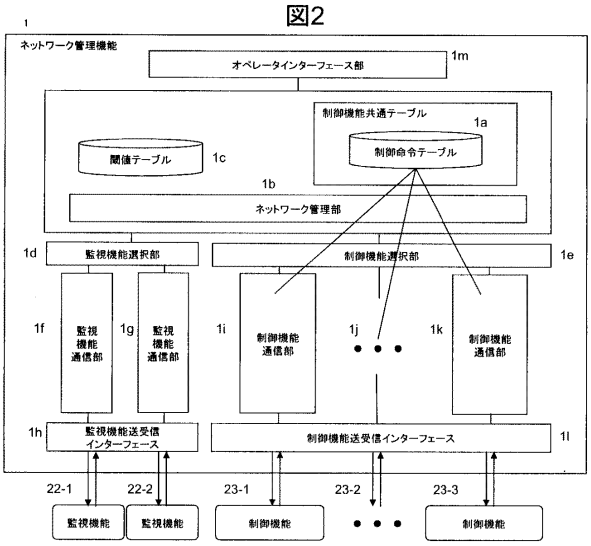
【図１】

図1



【図２】

図2



【図３】

図3

レコード識別子	中継装置識別子	受信端末アドレス	制御命令	フラグ				制御命令管理識別子
				判定対象	監視	閾値超過	追加	
…	ER0	…	…	0	0	0	0	…
01a	ER1	10.1.1.2	制御機能1	1	1	1	0	変更
01b	ER1	10.1.1.3	制御機能2	1	1	0	0	情報通知
01c	ER1	10.1.1.4	制御機能3	1	0	0	0	解除
01d	ER1	10.1.1.5	制御未実行	1	1	1	1	設定
01e	ER1	10.1.1.6	制御未実行	1	1	1	1	設定
01f	ER1	10.1.1.7	制御未実行	1	1	0	1	無処理

最新レコード

【図４】

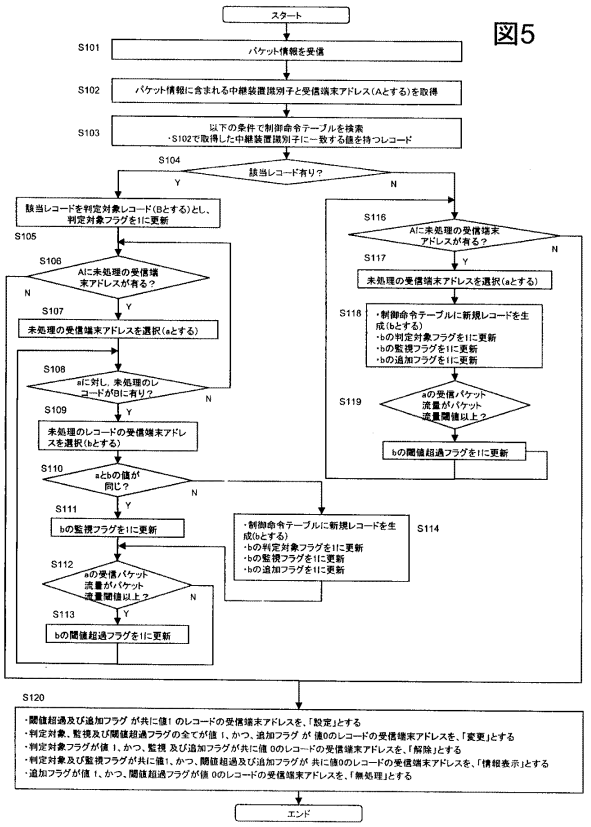
図4

「中継装置識別子」
・ER1

「#」,「受信端末アドレス」,「受信パケット流量」
・#1, 10.1.1.2, 800Mbps
・#2, 10.1.1.3, 100Mbps
・#3, 10.1.1.5, 800Mbps
・#4, 10.1.1.6, 800Mbps
・#5, 10.1.1.7, 100Mbps

【図５】

図5



【図６】

図6

(a) 制御命令実行中の受信端末アドレスの評価要件

			制御命令管理識別子
パケット情報で通知	パケット流量閾値の評価	閾値以上	「変更」
		閾値以下	「情報表示」
パケット情報で非通知		任意	「解除」

(b) 制御命令が実行中でない受信端末アドレスの評価要件

		制御命令管理識別子
パケット流量閾値の評価	閾値以上	「設定」
	閾値以下	「無処理」

【図７】

図7

レコード識別子	中継装置識別子	受信端末アドレス	制御命令	フラグ					制御命令管理識別子
				判定対象	監視	閾値超過	差分閾値超過	追加	
…	ER0	…	…	0	0	0	0	0	…
01a	ER1	10.1.1.2	制御機能1	1	1	1	0	0	変更
01b	ER1	10.1.1.3	制御機能2	1	1	0	0	0	情報通知
01c	ER1	10.1.1.4	制御機能3	1	0	0	0	0	解除
01d	ER1	10.1.1.5	制御未実行	1	1	1	1	1	設定
01e	ER1	10.1.1.6	制御未実行	1	1	1	0	1	無処理
01f	ER1	10.1.1.7	制御未実行	1	1	0	0	1	無処理

最新レコード

【図８】

図8

受信端末アドレス	パケット流量閾値	差分パケット流量閾値
10.1.1.0/24	500Mbps	300Mbps
10.1.2./24	1000Mbps	600Mbps
…	…	…

【図９】

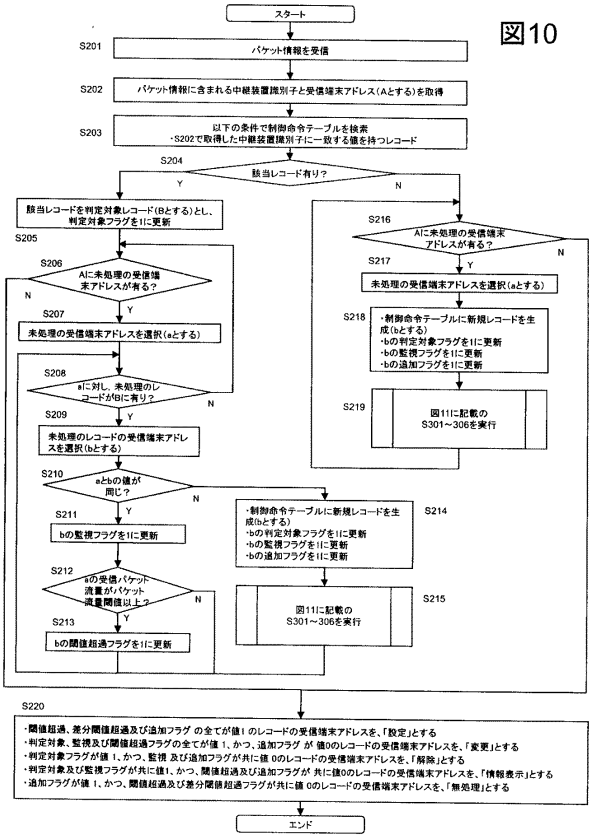
図9

「中継装置識別子」
・ER1

「#」,「受信端末アドレス」,「受信パケット流量」, 「差分受信パケット流量」
・#1, 10.1.1.2, 800Mbps, 100Mbps
・#2, 10.1.1.3, 100Mbps, 100Mbps
・#3, 10.1.1.5, 800Mbps, 500Mbps
・#4, 10.1.1.6, 800Mbps, 100Mbps
・#5, 10.1.1.7, 100Mbps, 100Mbps

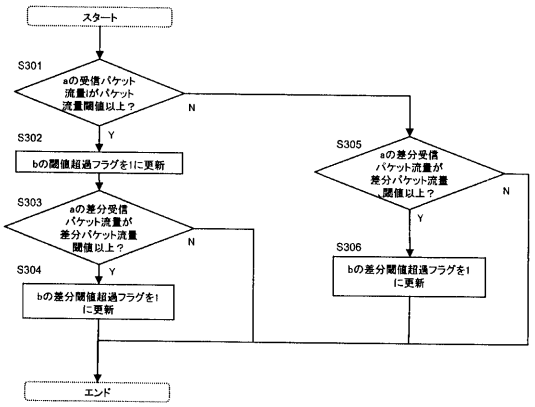
【図１０】

図10



【図１１】

図11



【図１２】

図12

(a) 制御命令実行中の受信端末アドレスの評価要件

			差分パケット流量閾値の評価	
			閾値以上	閾値以下
パケット情報で通知	パケット流量閾値の評価	閾値以上	「変更」	
		閾値以下	「情報表示」	
パケット情報で非通知		任意	「解除」	

(b) 制御命令が実行中でない受信端末アドレスの評価要件

		差分パケット流量閾値の評価	
		閾値以上	閾値以下
パケット流量閾値の評価	閾値以上	「設定」	
	閾値以下	「無処理」	

フロントページの続き

(72)発明者　田邉　正雄
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　村山　純一
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　玉木　宏治

(56)参考文献　八木　毅　他，DDoS攻撃軽減装置スクラビングボックス共用化のためのネットワーク制御方式の評価，電子情報通信学会技術研究報告（信学技報）　IN2006-131，２００６年１２月　７日

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　１２／００－６６
Ｇ０６Ｆ　　１３／００