

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2010-16517
(P2010-16517A)

(43) 公開日 平成22年1月21日(2010.1.21)

(51) Int.Cl. F I テーマコード(参考)
H04L 12/56 (2006.01) H04L 12/56 100C 5K030

審査請求 未請求 請求項の数 6 O L (全 11 頁)

(21) 出願番号	特願2008-173174 (P2008-173174)	(71) 出願人	000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22) 出願日	平成20年7月2日(2008.7.2)	(71) 出願人	504132272 国立大学法人京都大学 京都府京都市左京区吉田本町36番地1
		(74) 代理人	100102587 弁理士 渡邊 昌幸
		(72) 発明者	亀井 聡 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	川原 亮一 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

最終頁に続く

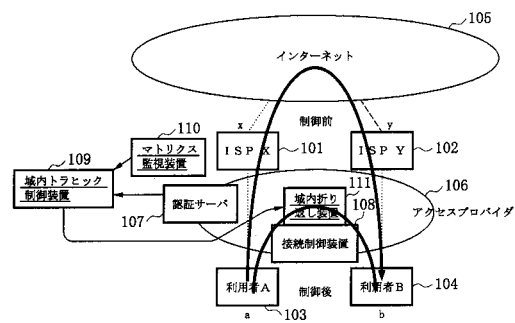
(54) 【発明の名称】 P2P型トラフィック制御システムおよび制御方法

(57) 【要約】

【課題】 アクセスプロバイダの中で冗長な経路を除き通信量を減少してコストを削減する。

【解決手段】 域内トラフィック制御装置109は、同一アクセスプロバイダの域内で閉じたユーザ間の通信は、アクセスプロバイダ経由でインターネット105に転送することなく、アクセスプロバイダ域内106に直接折り返して通信するように制御する。具体的には、域内トラフィック制御装置109がマトリクス監視装置110から通信元および通信先のフロー情報の一覧を取得し、認証サーバ107から払い出しアドレスの情報を受け取り、照合処理を実施し、通信元、通信先ともに一致するフローを制御対象トラフィックとし、認証サーバ107から変換前アドレスを得て、上記フロー情報および変換前アドレスの各情報を元に当該トラフィックを域内折り返し装置111へルーティングするようにアドレス変換指示を接続制御装置108に送り、域内通信を実施する。

【選択図】 図6



【特許請求の範囲】**【請求項 1】**

利用者がアクセスプロバイダから付与されたグローバルアドレスで発アドレス、着アドレスおよび通信量の組情報を保持するマトリクス監視装置と、

アクセスしてきた利用者端末ごとに、プライベートアドレスとグローバルアドレスの組情報を保持する認証サーバと、

指定された通信に対して、アクセスプロバイダ域内で折り返しを実施する域内折り返し装置と、

該マトリクス監視装置から発アドレスおよび着アドレスのフロー情報の一覧を受け取り、該認証サーバから払い出しグローバルアドレスおよびプライベートアドレスの情報を受け取り、前者の発アドレスおよび着アドレスが両方とも後者のグローバルアドレスに含まれるか否かの照合処理を実施し、発アドレス、着アドレスともに含まれるフローを制御対象トラヒックとし、該認証サーバから受け取ったプライベートアドレスを元に、当該トラヒックを域内折り返し装置ヘルテイングするようにアドレス変換指示を接続制御装置に送出する域内トラヒック制御装置と

を有することを特徴とする P 2 P 型トラヒック制御システム。

【請求項 2】

請求項 1 に記載の P 2 P 型トラヒック制御システムにおいて、

前記マトリクス監視装置は、アクセスプロバイダの利用者端末相互が、インターネットと通信している状態をそれぞれ監視する装置であり、通信元のポート番号と通信先のポート番号と通信量の組を保持することを特徴とする P 2 P 型トラヒック制御システム。

【請求項 3】

請求項 1 に記載の P 2 P 型トラヒック制御システムにおいて、

前記域内トラヒック制御装置は、前記マトリクス監視装置から発アドレスおよび着アドレス、ならびに通信量の一覧を受け取り、前記認証サーバから払い出しグローバルアドレスおよびプライベートアドレスの情報を受け取り、前者の発アドレスおよび着アドレスが両方とも後者のグローバルアドレスに含まれるか否かの照合処理を実施し、発アドレス、着アドレスともに含まれるフローのうち、通信量が予め定めた通信量の閾値より大きいもののみ、制御対象トラヒックとし、該認証サーバから受け取ったプライベートアドレスを元に、当該トラヒックを域内折り返し装置ヘルテイングするようにアドレス変換指示を接続制御装置に送出することを特徴とする P 2 P 型トラヒック制御システム。

【請求項 4】

インターネットへのネットワーク接続サービスを運用する際に、コンピュータの制御により、上位への接続回線を複数切り換えるサービスを提供する P 2 P 型トラヒック制御方法において、

域内トラヒック制御装置は、マトリクス監視装置から通信元および通信先のフロー情報の一覧を取得し、

認証サーバから払い出しアドレスの情報を受け取り、前記フロー情報と該払い出しアドレス情報との照合処理を実施し、

通信元、通信先ともに一致するフローを制御対象トラヒックとし、該認証サーバから変換前アドレスを得て、該フロー情報および該変換前アドレスの各情報を元に当該トラヒックを域内折り返し装置ヘルテイングするようにアドレス変換指示を接続制御装置に送り、

該接続制御装置および域内折り返し装置は、域内通信を実施することを特徴とする P 2 P 型トラヒック制御方法。

【請求項 5】

請求項 4 に記載の P 2 P 型トラヒック制御方法において、

域内トラヒック制御装置は、マトリクス監視装置から開始アドレスと宛先アドレスを取得するとともに、認証サーバから変換後アドレスを取得して、

取得した両方の変換後アドレスの照合を行い、前者の発アドレスと着アドレスとが両方

10

20

30

40

50

とも後者の変換後アドレスに含まれている場合には、同一域内同士の通信であると判別し、

これらを全てアクセスプロバイダ域内で折り返し通信に指定することを特徴とする P 2 P 型トラヒック制御方法。

【請求項 6】

請求項 4 に記載の P 2 P 型トラヒック制御方法において、

域内トラヒック制御装置は、マトリクス監視装置から発アドレスと着アドレスと通信量を取得するとともに、認証サーバから変換後アドレスを取得し、

取得した両方の変換後アドレスの照合を行い、前者の発アドレスと着アドレスとが両方とも後者の変換後アドレスに含まれており、かつ取得した前記通信量を判別して、通信量が予め定めた通信量の閾値より大きい場合にのみ、アクセスプロバイダ域内で折り返し通信に指定することを特徴とする P 2 P 型トラヒック制御方法。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、インターネット等へのネットワーク接続サービスを運用するに際して、上位への接続回線を複数切り換えるサービスを提供するシステムにおいて、トラヒック流量を削減するための P 2 P 型トラヒック制御システムおよび制御方法に関する。

【背景技術】

【0002】

インターネット等へのネットワーク接続サービスにおいては、アクセスプロバイダと呼ばれる利用者の足周りのアクセス回線とインターネットへの接続回線の橋渡しを行うサービスを提供する事業者が、ブロードバンド化や無線・ユビキタス化の進行に伴って登場している。

20

アクセスプロバイダ事業者は、各種アクセス回線により当該サービス事業者に接続された利用者に対して、契約や認証 ID 等により決定される上位のインターネットサービスプロバイダへの接続を提供する。すなわち、アクセスプロバイダは、電話回線や ISDN 回線、ADSL 回線、光ファイバー回線、データ通信専用回線等を通じて、顧客である企業や家庭のコンピュータをインターネットに接続する。

その他に、アクセスプロバイダの付加的サービスとして、メールアドレスやホームページ開設用のディスクスペースを貸し出したり、オリジナルのコンテンツを提供したりしている。

30

【0003】

図 1 は、アクセスプロバイダの接続形態を示す図である。

図 1 において、101、102 はインターネットサービスプロバイダのルータまたは網接続装置 (ISP X, ISP Y)、103, 105 は利用者端末 (利用者 A, B)、104 はインターネット、106 はアクセスプロバイダ域である。

利用者 A 端末 103 はプロバイダのルータ (ISP X) 101 に、利用者 B 端末 104 はプロバイダの別のルータ (ISP Y) 102 にそれぞれ接続され、各プロバイダのルータ 101, 102 からそれぞれインターネット 105 に接続する。

40

主要な通信がインターネット 105 側から利用者端末 (利用者 X, 利用者 Y) 103, 104 に一方的に流れる場合においては、この形態で特に問題は発生しない。

図 2 は、非効率になる P 2 P 折り返し通信を示す図である。

図 2 から明らかなように、利用者 A 端末 103 から利用者 B 端末 104 宛に通信を行いたい場合には、利用者 A 端末 103 から所属のプロバイダのルータ 101 を経由してインターネット 105 に接続してもらい、利用者 B が所属する別のプロバイダのルータ 102 を経由して、アクセスプロバイダ域 106 内に戻り、利用者 B 端末 104 に接続される (太線矢印参照)。

【0004】

しかしながら、近年 P 2 P と呼ばれる利用者間で頻繁に大量のデータをやりとりする

50

通信形態が増加している。また、一方では、アクセスプロバイダが広域的にサービスを提供する例も出てきており、一つのアクセスプロバイダの中で直接通信をする形態も、今後は増加が見込まれる。

この場合、従来技術においては、図2に示すように、通信は各プロバイダのルータ（例えば、101）を経由してインターネット105に出て行った後に、再び別のプロバイダのルータ（例えば、102）を介してアクセスプロバイダ域106内に戻って来ることになり、アクセスプロバイダ域106内の通信、上位のアクセスプロバイダの通信ともに増加することになるため、ネットワークの利用効率が悪化する。

なお、トラフィックに関する様々な情報を収集するための技術やプロトコルが従来より提案されている（非特許文献1参照）。

10

【0005】

【非特許文献1】“トラフィック管理技術とその比較”（<http://itpro.nikkeibp.co.jp/article/COLUMN/20070202/260432/>）

【発明の開示】

【発明が解決しようとする課題】

【0006】

このように、近年、P2Pと呼ばれる大量データのやりとりを行う通信形態が増加しているが、これらの大量のデータのやりとりでは、利用者端末は各プロバイダのルータを介してインターネットに出て行った後に、再び別のプロバイダのルータを介してアクセスプロバイダ域の中に戻って来ることになり、その別のプロバイダのルータから宛先の利用者端末にデータが送られる。

20

従って、アクセスプロバイダの中の通信、および上位プロバイダの通信ともに増加することになるため、ネットワークの利用効率が悪化するという問題があった。

【0007】

（目的）

本発明の目的は、上述の問題点を解決し、アクセスプロバイダの中で冗長な経路を取り通信の量を減らし、コストを削減することが可能なP2P型トラフィック制御システムおよび制御方法を提供することにある。

【課題を解決するための手段】

30

【0008】

上記目的を達成するため、本発明のP2P型トラフィック制御システムは、同一アクセスプロバイダの域内で閉じたユーザ間の通信は、アクセスプロバイダのルータ経由でインターネットに転送することなく、アクセスプロバイダ域内に直接折り返して通信するように制御することにより、無駄なトラフィックを削減し、効率的な域内通信を行う。

すなわち、本発明では、プロバイダのルータに加えて、域内トラフィックの折り返し装置と、通信元および通信先のフロー情報を収集するマトリクス監視装置を用いてトラフィックを制御し、通信量を抑制する。

また、本発明のトラフィック制御方法は、域内トラフィック制御装置がマトリクス監視装置から通信元および通信先のフロー情報の一覧を取得し、認証サーバから払い出しアドレスの情報を受け取り、照合処理を実施し、通信元、通信先ともに一致するフローを制御対象トラフィックとし、認証サーバから変換前アドレスを得て、上記フロー情報および変換前アドレスの各情報を元に当該トラフィックを域内折り返し装置へルーティングするようにアドレス変換指示を接続制御装置に送り、域内通信を実施する。

40

また、本発明のトラフィック制御方法は、アクセスプロバイダに振り分けることなく域内で折り返すべき通信を特定する場合に、a)同一域内の通信、b)同一域内の通信で、かつ通信量の多い通信とに分けて、両方とも域内で折り返すべき通信と特定する方法を採用するか、あるいは、後者のみを域内で折り返すべき通信と特定する方法を採用するか、を予め決定する。

【発明の効果】

50

【 0 0 0 9 】

本発明によれば、通信開始時に一つの共通の認証サーバにプライベートアドレスを用いてアクセスする利用者端末が、同一域内に属することを判別でき、域内トラヒック制御装置は同一域内で折り返すべき通信を特定することができるので、アクセスプロバイダの中で冗長な経路を除いて通信の量を減らし、コストを削減することが可能となる。

【 発明を実施するための最良の形態 】

【 0 0 1 0 】

まず、本発明の特徴点を挙げる。

1) 同一域内に属する利用者端末は、通信開始時に一つの共通の認証サーバにプライベートアドレスを用いてアクセスし、その後、当該認証サーバにより各々自分のアクセスプロバイダへ振り分けられ、振り分けられた先のアクセスプロバイダでグローバルアドレスが付与される。従って、同一の認証サーバにアクセスした利用者端末は、同一域内に属することが判明される。

10

2) 認証サーバは、自分にアクセスしたきた利用者端末ごとに、そのプライベートアドレスと、当該利用者端末がアクセスプロバイダから付与されたグローバルアドレスの組の情報(以下、情報1と記す)を保持する。

3) マトリクス監視装置は、インターネットを監視し、発アドレス(グローバルアドレス)、着アドレス(グローバルアドレス)、通信量の組(以下、情報2と記す)を保持する。

。なお、これらのアドレスは、グローバルアドレスであるため、この時点では、各発アドレスと着アドレスの組が同一域内に属するか否かは判別できない。

20

【 0 0 1 1 】

4) 域内トラヒック制御装置が、情報1と情報2を収集する。これら情報1と情報2に含まれるグローバルアドレスを比較し、情報2の発アドレスと着アドレスとが両方とも情報1に含まれていれば、同一域内同士の通信であることが判別できる(上記1)より判別)。

5) 域内トラヒック監視装置は、上記4)により、アクセスプロバイダに振り分けることなく、域内で折り返すべき通信を特定する。すなわち、同一域内の通信あるいは同一域内の通信で、かつ通信量の多い通信を特定する。これらの特定した通信を、域内トラヒック折り返し装置に通知することにより、折り返し通信を実現する。

30

【 0 0 1 2 】

以下、図面に従って、本発明の一実施形態を説明する。

本発明を詳細に説明するため、まず既存のアクセスプロバイダの接続技術を説明する。

図3は、従来のアクセスプロバイダ接続手順を示す説明図である。

図3において、図1および図2に用いた101~106の記号・番号は全く同じであり、さらアクセスプロバイダ106には、認証サーバ107および接続制御装置108が追加されている。

利用者端末103, 104が、それぞれプロバイダのルータ101, 102に接続して、インターネットサービスを利用している状態であって、利用者端末103, 104には、それぞれ内部管理用のアドレス(プライベートアドレス、v6アドレス、回線番号等)a, bが付与されている。

40

【 0 0 1 3 】

各ホスト(103)は、認証サーバ107に問い合わせ(ステップ1)、利用者端末A103, B104の接続先プロバイダ情報(この場合、プロバイダのルータ101または102の情報)を得る。接続制御装置108は、得られた情報に従って(ステップ2)、各プロバイダのサーバトンネルやルーティング等の手段で転送を行う(ステップ3)。その後、プロバイダのルータ101, 102からIPアドレスx, yがそれぞれ払い出されて(ステップ4)、接続制御装置108に付与され、接続が行われる流れとなる。

実際に集い出されたアドレスx, yの情報は、認証サーバ107において記録される場合と、記録されない場合とがあるが、本実施形態では認証サーバ107において記録され

50

る場合を対象とする。

【0014】

図4は、本発明の一実施形態に係るP2P型トラヒック制御装置の構成要素を示す図である。

図4において、図1～図3で用いた101～108の記号・番号に加えて、新たに域内トラヒック制御装置109と、マトリクス監視装置110と、域内折り返し装置111とを設ける。以下、新たに設けられた装置について説明する。

トラヒックマトリクス監視装置110は、アクセスプロバイダの利用者が、インターネットと通信している状態をそれぞれ監視する装置であり、通信元のアドレス（場合によっては、ポート番号）と通信先のアドレス（場合によっては、ポート番号）と通信量の組を保持する。これらは、通常、フローデータと呼ばれる量であり、*slow*, *netflow*等、ネットワーク管理のためにこのようなデータを測定する装置は、既に存在している（非特許文献1参照）。

10

【0015】

域内トラヒックの折り返し装置111は、技術的には既存のプロバイダのルータ101, 102が保持しているものと同一である。異なる点としては、アクセスプロバイダ域106内にのみ接続回線を持っており、インターネット105側の回線は保持していないことになる。

域内トラヒックの折り返し装置111は、ネットワークの構成によっては必要としない（アドレスの付替のみで直接通信が成される等）場合もあるが、そのような条件が成り立たない汎用的な条件でも通信可能となるように設けられる。

20

具体的には、ユーザ間でのプライベートアドレスでの直接通信はできないように設定されているサービスが存在する。その場合、ISP接続装置経由の通信しか許されないように設定されているため、疑似的にISP接続装置（もどき）として網内折り返し装置を設けてやることで、通信可能になる。

域内トラヒック制御装置109は、本発明の中心となる装置であって、この装置の処理動作は図5および図7で詳細に説明する。

【0016】

図5は、本発明の域内トラヒック制御装置の処理動作を示すフローチャートである。

域内トラヒック制御装置109は、まずトラヒックマトリクス監視装置110からフロー情報（通信元、通信先）の一覧を取得する（ステップ201, 202）。ここで、開始/宛先アドレスと記載されている『開始』は、『選択元』の意味であり、また、ここでのアドレスはグローバルアドレスを意味する。この一例では、マトリクス監視装置110の一覧として、例えば、通信元xはp、通信先yはq、通信量は5M、等が保存されており、このうち、域内トラヒック制御装置109に宛先アドレスy=qが取得される。マトリクス監視装置110が格納している一覧情報は、このように通信元アドレス（グローバルアドレス）、通信先アドレス（グローバルアドレス）、通信量の組情報（情報2）である。

30

【0017】

認証サーバ107が格納している一覧情報は、認証サーバにアクセスしてきた利用者端末（103, 104等）のプライベートアドレスと、その利用者がISPから付与されたグローバルアドレス（払い出しIP）の組情報（情報1）である。

40

次に、域内トラヒック制御装置109は、認証サーバ107から払い出しアドレスの情報（情報1）を受け取る（ステップ203a）。例えば、変換後アドレス一覧としてyを受け取る。なお、変換後のアドレスは、プライベートアドレスを意味する。これを受け取った後、変換後のアドレスとマトリクス監視装置110から取得したアドレスとの照合を実施する（ステップ203）。通信元、通信先とも一致するフローを制御対象トラヒック（域内フロー）とする（ステップ204）。すなわち、情報1と情報2に含まれるグローバルアドレスを比較して、情報2の発アドレスと着アドレスとが両方とも情報1に含まれていれば、同一域内同士の通信であると判別できる。

50

次に、認証サーバ107から変換前アドレスを取得する(ステップ203a)。照合の結果、一致した変換後アドレス情報および変換前アドレス情報を元に、当該トラヒックを域内折り返し装置111へルーティングするよう、アドレス変換指示を接続制御装置108へ送出する(ステップ205, 206)。これにより、域内通信が実施される。

【0018】

なお、アクセスプロバイダ域内で折り返し通信にする、と特定する場合、2つの方法がある。その1つは、a)『同一域内の通信』の場合であり、他の1つは、b)『同一域内の通信で、かつ通信量の多い通信』の場合である。

上記a)の場合には、図5において、域内トラヒック制御装置109がマトリクス監視装置110から開始アドレスと宛先アドレス(グローバルアドレス)(情報2)を取得するとともに、認証サーバ107から変換後アドレス(グローバルアドレス)(情報1)を取得して、取得した両方の変換後アドレスとの照合を行い、情報2の発アドレスと着アドレスとが両方とも情報1に含まれている場合には、同一域内同士の通信であることが判別でき、これらを全てアクセスプロバイダ域内で折り返し通信にする。

また、上記b)の場合には、図5において、域内トラヒック制御装置109がマトリクス監視装置110から情報2の発アドレスと着アドレスと通信量を取得するとともに、認証サーバ107から変換後アドレス(情報1)を取得し、情報1と情報2に含まれるグローバルアドレスを比較し、情報2の発アドレスと着アドレスとが両方とも情報1に含まれており、かつ情報2の中の通信量が予め定めた通信量の閾値より大きい場合、つまり通信量の多い通信の場合にのみ、アクセスプロバイダ域内で折り返し通信にする。

後者の場合は、同一域内通信が比較的多い場合に有効である。

【0019】

図6は、本発明の一実施例に係る域内トラヒック制御装置の処理動作の説明図である。

域内トラヒック制御装置109は、マトリクス監視装置110と認証サーバ107が保存しているデータを取得した後、域内で折り返すべき通信を特定する。特定したならば、域内で折り返すべき通信を域内折り返し装置111に通知する。制御前には、インターネット105を経由して折り返していたが、制御後には、域内折り返し装置111の制御により、アクセスプロバイダ106内において利用者端末103から利用者端末104に域内折り返しが実施される(太線矢印参照)。

【0020】

図7は、本発明の一実施例に係るマトリクス監視装置、域内トラヒック制御装置および認証サーバの詳細フローチャートである。

マトリクス監視装置110は、インターネット105を監視し、通信フロー全体、具体的には発アドレス(グローバルアドレス) $address_{s_1} \sim address_{s_6}$ と着アドレス(グローバルアドレス) $address_{d_1} \sim address_{d_6}$ 、通信量 $bw_1 \sim bw_6$ の組(情報2)を保持している。

認証サーバ107は、自分にアクセスしてきた利用者端末ごとに、そのプライベートアドレス a, b, \dots と、当該利用者端末がプロバイダのサーバから付与されたグローバルアドレス x, y, \dots の組の情報(情報1)を保持している。

【0021】

今、同一域内に属する利用者端末が、通信開始時に一つの共通の認証サーバ107にプライベートアドレスを用いてアクセスすると、その後、当該認証サーバ107により各々自分のプロバイダへ振り分けられ、振り分けられた先のプロバイダでグローバルアドレスを付与される。

域内トラヒック制御装置109は、マトリクス監視装置110からアドレス情報(グローバルアドレス)を受け取る(ステップ1)。次に、認証サーバ107から払い出しアドレス情報(グローバルアドレス)を受け取る(ステップ2)。照合処理を実施し、合致アドレス(図7の斜線下線部)を得る(ステップ3)。制御対象トラヒック(発アドレス s_{rc} / 着アドレス d_{st} ととも一致)を確定する(ステップ4)。すなわち、『一致』とは、マトリクス監視装置110のデータにも認証サーバ107のデータにも、両方に含まれ

10

20

30

40

50

るアドレスであることを意味する。換言すれば、情報 2 の発アドレスと着アドレスとが両方とも情報 1 に含まれているとき、同一域内同士の通信であると判別できる。

次に、認証サーバ 107 から変換前アドレス（プライベートアドレス）を受け取る（ステップ 5）。接続制御装置 108 に対して、当該トラヒックの制御指示を行う（ステップ 6）。域内トラヒック折り返し装置 111 は、照合結果が一致した制御対象トラヒック（address_s : private-address_Z）に対して、域内通信を実施する（ステップ 7）。

【図面の簡単な説明】

【0022】

【図 1】アクセスプロバイダの接続形態を示す図である。

10

【図 2】非効率になる P2P 折り返し通信を示す図である。

【図 3】従来のアクセスプロバイダ接続方法を示す図である。

【図 4】本発明の一実施形態に係る P2P 型トラヒック制御装置の構成図である。

【図 5】本発明の一実施形態に係る P2P 型トラヒック制御手順を示すフローチャートである。

【図 6】本発明の一実施例に係る P2P 型トラヒック制御装置の処理動作説明図である。

【図 7】本発明の一実施例に係る詳細な制御手順を示すフローチャートである。

【符号の説明】

【0023】

101, 102 プロバイダのルータ（または網接続装置）

20

103, 104 利用者端末

105 インターネット

106 アクセスプロバイダ

107 認証サーバ

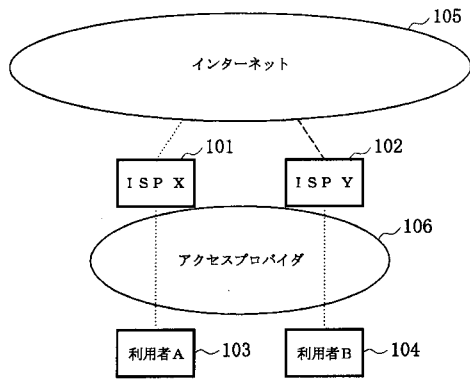
108 接続制御装置

109 域内トラヒック制御装置

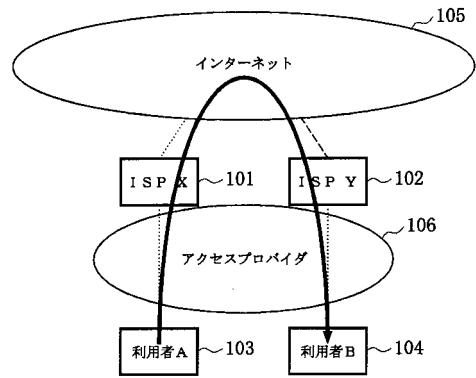
110 マトリクス監視装置

111 域内折り返し装置

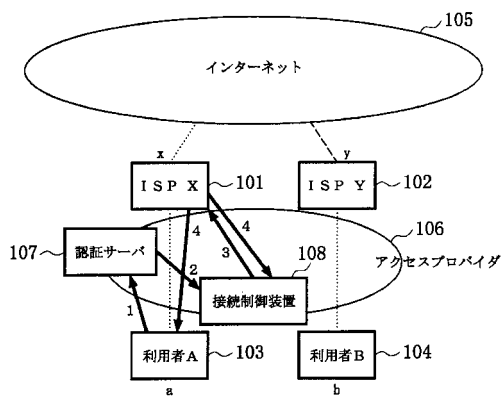
【 図 1 】



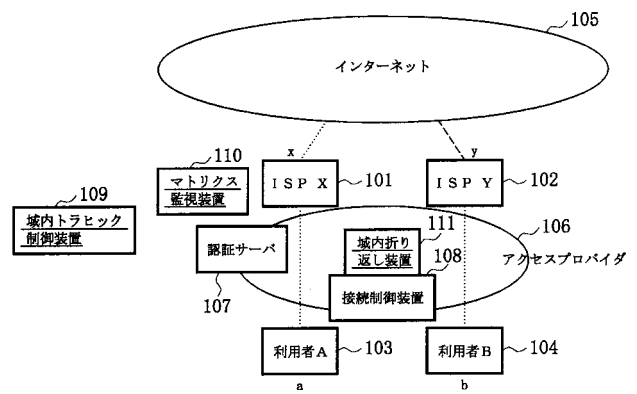
【 図 2 】



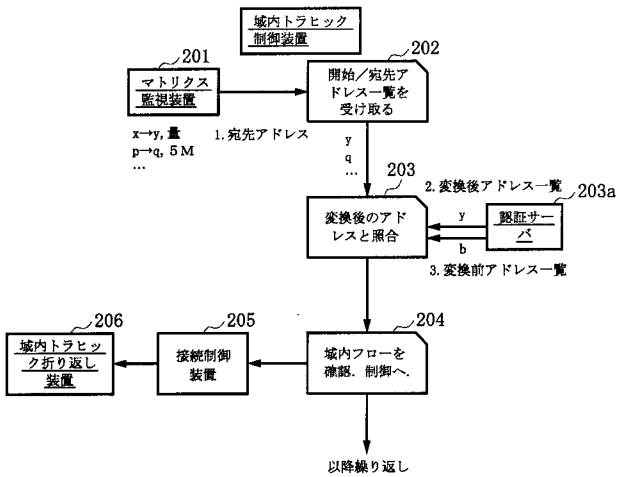
【 図 3 】



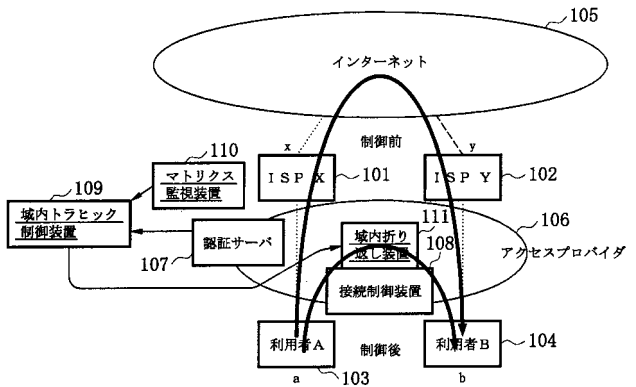
【 図 4 】



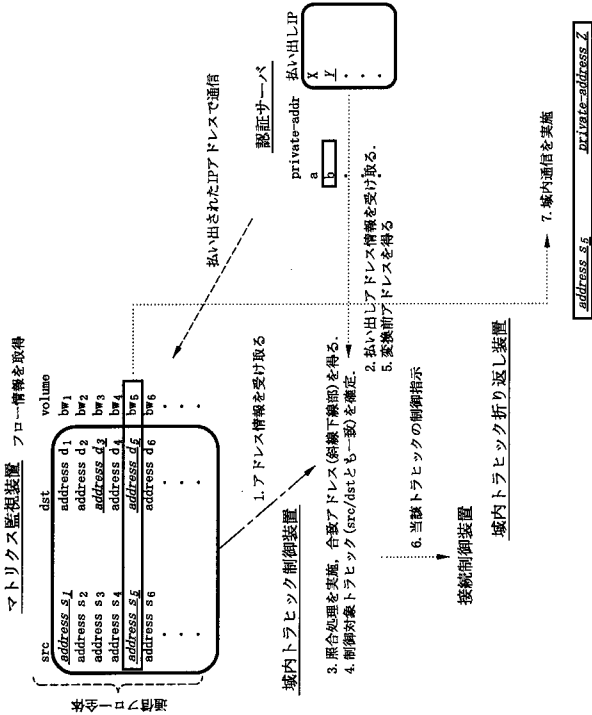
【 図 5 】



【 図 6 】



【 図 7 】



フロントページの続き

(72)発明者 笠原 正治

京都府京都市左京区吉田本町 国立大学法人京都大学大学院情報学研究科内

(72)発明者 高橋 豊

京都府京都市左京区吉田本町 国立大学法人京都大学大学院情報学研究科内

Fターム(参考) 5K030 GA03 GA08 GA14 HA08 HB28 HC01 HD03 HD09 JA07 JA10
KA04 KA05 LB08 LC01 MA04 MA13 MB09 MC08