(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5078025号
(P5078025)
(45)発行日　平成24年11月21日(2012.11.21)　(24)登録日　平成24年9月7日(2012.9.7)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　100C

請求項の数 6　(全 11 頁)

(21)出願番号　特願2008-173174(P2008-173174)
(22)出願日　平成20年7月2日(2008.7.2)
(65)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)
審査請求日　平成23年5月24日(2011.5.24)

(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
(73)特許権者　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　100121669
弁理士　本山　泰
(74)代理人　100127535
弁理士　豊田　義元
(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

最終頁に続く

(54)【発明の名称】Ｐ２Ｐ型トラヒック制御システムおよび制御方法

(57)【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Ｐ２Ｐ型トラヒック制御システム。
【請求項２】
請求項１に記載のＰ２Ｐ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Ｐ２Ｐ型トラヒック制御システム。
【請求項３】
請求項１に記載のＰ２Ｐ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出することを特徴とするＰ２Ｐ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Ｐ２Ｐ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、
該フロー情報の通信元アドレスと通信先アドレスの両方が、該払い出しアドレス情報に含まれてい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、
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Ｐ２Ｐ型トラヒック制御方法。
【請求項５】
請求項４に記載のＰ２Ｐ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Ｐ２Ｐ型トラヒック制御方法。
【請求項６】
請求項４に記載のＰ２Ｐ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Ｐ２Ｐ型トラヒック制御方法。

【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Ｐ２Ｐ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。
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。
【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（ＩＳＰＸ，ＩＳＰＹ）、１０３，１０５は利用者端末（利用者Ａ，Ｂ）、１０５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（ＩＳＰＸ）１０１に、利用者Ｂ端末１０４はプロバイダの別のルータ（ＩＳＰＹ）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。
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Ｐ２Ｐ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Ｐ２Ｐと呼ばれる利用者の間で頻繁に大量のデータをやりとりする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、従来の技術においては、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）。
【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。

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型トラヒ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】

【０００８】

上記目的を達成するため、本発明のＰ２Ｐ型トラヒ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、無駄なトラヒックを削減し、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、域内トラヒ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ヒックを制御し、通信量を抑制する。

また、本発明のトラヒック制御方法は、域内トラヒ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、該フロー情報の通信元アドレスと通信先アドレスの両方が、該払い出しアドレス情報に含まれているフローを制御対象トラヒックとし、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ヒ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。

また、本発明のトラヒック制御方法は、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】

【０００９】

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】

【００１０】

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。

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。

【００１１】

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。

【００１２】

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。

【００１３】

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へ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、ｓｆｌｏｗ，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）。

【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。
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。

【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。
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、通信先ともに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。
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～ａｄｄｒｅｓｓ　s_6と着アドレス（グローバルアドレス）ａｄｄｒｅｓｓ　d_1～ａｄｄｒｅｓｓ　s_6、通信量bw_1～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，・・・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，・・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、その後に、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ｓｒｃ／着アドレスｄｓｔ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_5：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。

【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。

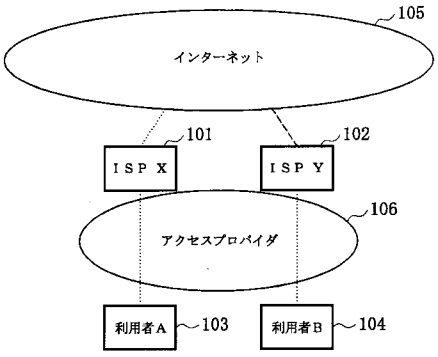
【図５】本発明の一実施形態に係るＰ２Ｐ型トラヒック制御手順を示すフローチャートである。

【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。

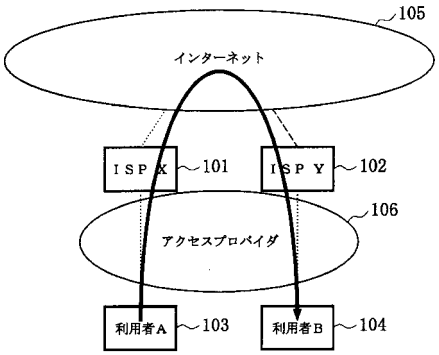
【図７】本発明の一実施例に係る詳細な制御手順を示すフローチャートである。

【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）
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

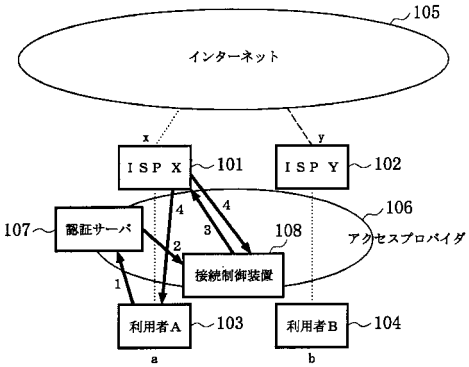
【図１】



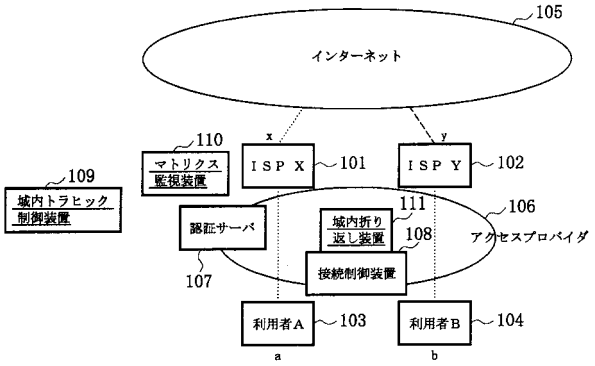
【図２】



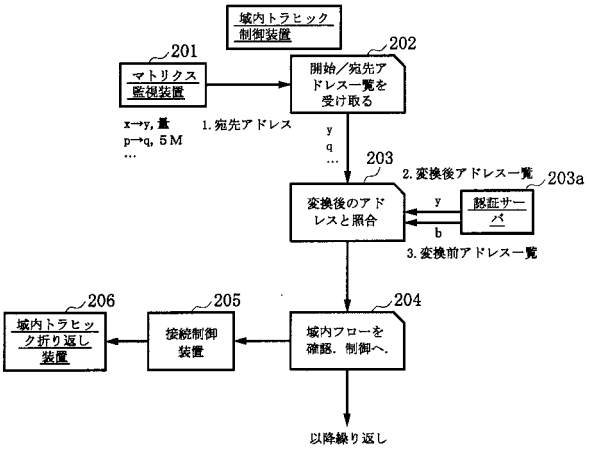
【図３】


105
インターネット
x
y
ＩＳＰ Ｘ
101
ＩＳＰ Ｙ
102
106
アクセスプロバイダ
107
認証サーバ
108
接続制御装置
1
2
3
4
4
利用者Ａ
103
利用者Ｂ
104
a
b

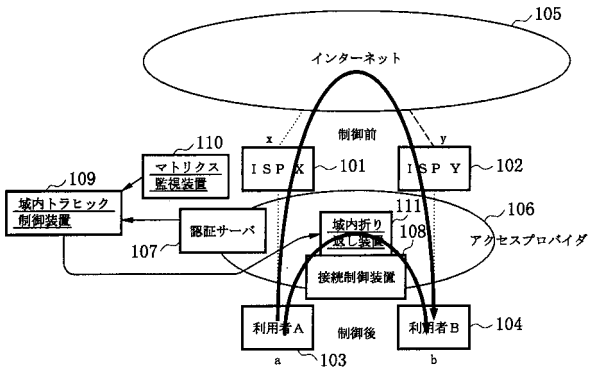
【図４】


105
インターネット
110
マトリクス監視装置
109
域内トラヒック制御装置
x
y
ＩＳＰ Ｘ
101
ＩＳＰ Ｙ
102
111
域内折り返し装置
106
アクセスプロバイダ
認証サーバ
107
108
接続制御装置
利用者Ａ
103
利用者Ｂ
104
a
b

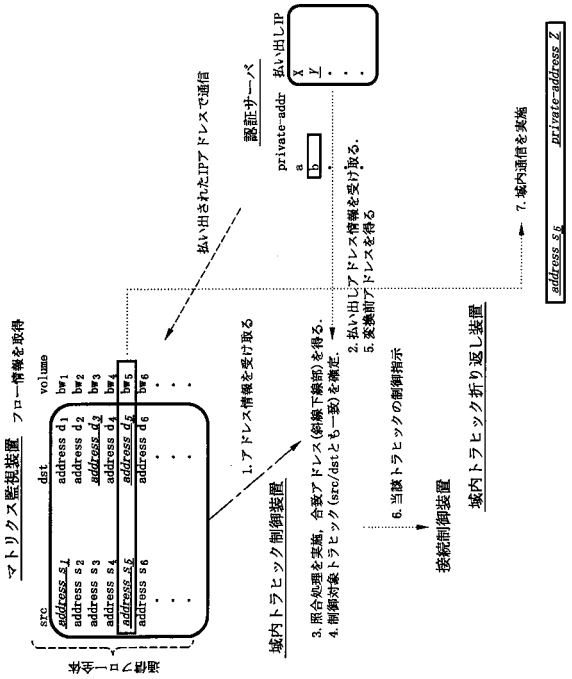
【図５】


域内トラヒック制御装置
201
マトリクス監視装置
x→y, 量
p→q, 5M
…
1. 宛先アドレス
202
開始／宛先アドレス一覧を受け取る
y
q
…
203
2. 変換後アドレス一覧
203a
変換後のアドレスと照合
y
b
認証サーバ
3. 変換前アドレス一覧
204
域内フローを確認．制御へ．
205
接続制御装置
206
域内トラヒック折り返し装置
以降繰り返し

【図６】


105
インターネット
制御前
110
マトリクス監視装置
109
域内トラヒック制御装置
x
y
ＩＳＰ Ｘ
101
ＩＳＰ Ｙ
102
111
域内折り返し装置
106
アクセスプロバイダ
認証サーバ
107
108
接続制御装置
利用者Ａ
103
制御後
利用者Ｂ
104
a
b

【図７】


マトリクス監視装置
フロー情報を取得
src
dst
volume
address s1
address s2
address s3
address s4
address s5
address s6
address d1
address d2
address d3
address d4
address d5
address d6
bw1
bw2
bw3
bw4
bw5
bw6
制御フロー全体
払い出されたIPアドレスで通信
認証サーバ
払い出しIP
private-addr
a
b
X
Y
1. アドレス情報を受け取る
域内トラヒック制御装置
3. 照合処理を実施，合致アドレス(斜線下線部)を得る．
4. 制御対象トラヒック(src/dstとも一致)を確定．
2. 払い出しアドレス情報を受け取る．
5. 変換前アドレスを得る
6. 当該トラヒックの制御指示
接続制御装置
域内トラヒック折り返し装置
7. 域内通信を実施
address_Sg
private-address_Z

フロントページの続き

(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
(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

審査官　浦口　幸宏

(56)参考文献　特開２００３－３３８８３２（ＪＰ，Ａ）
特開２００４－２２８７９９（ＪＰ，Ａ）
特開２００３－２５９４２２（ＪＰ，Ａ）

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