(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2015-53663
(P2015-53663A)
(43)公開日　平成27年3月19日(2015.3.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/46	(2006.01)	H04L	12/46	E	5K030
H04L 12/66	(2006.01)	H04L	12/46	V	5K033
H04L 12/70	(2013.01)	H04L	12/66	B	
		H04L	12/70	D	
		H04L	12/70	B	

審査請求 未請求　請求項の数 7　ＯＬ　（全 14 頁）

(21)出願番号　特願2013-186769 (P2013-186769)
(22)出願日　平成25年9月9日 (2013.9.9)

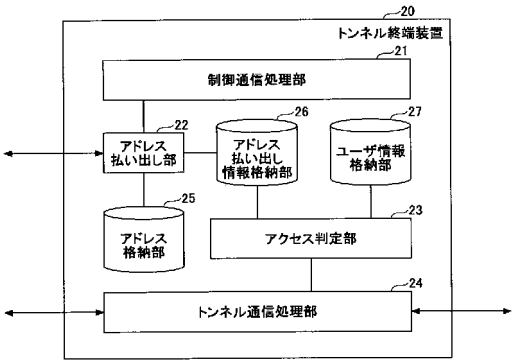
(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　波多　浩昭
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

最終頁に続く

(54)【発明の名称】アクセス制御装置、アクセス制御方法、及びプログラム

(57)【要約】
【課題】ＩＰアドレスのように変化しないアクセス元ユーザのＩＤを用いてアクセス制御を行う技術を提供する。
【解決手段】通信ネットワーク上におけるアクセス元装置からアクセス先装置へのアクセスを制御するアクセス制御装置において、前記アクセス元装置から送信元アドレスと宛先アドレスを設定したパケットを受信し、アドレスとＩＤとを対応付けて格納するアドレス情報格納手段から、前記送信元アドレスに対応する送信元ＩＤを取得する手段と、前記送信元ＩＤに基づいて、ＩＤ毎に接続先情報を格納したユーザ情報格納手段を参照することにより、前記パケットを前記宛先アドレスに転送するか否かを決定するアクセス判定手段とを備える。
【選択図】図８

トンネル終端装置20の機能構成図



【特許請求の範囲】
【請求項１】
通信ネットワーク上におけるアクセス元装置からアクセス先装置へのアクセスを制御するアクセス制御装置であって、
前記アクセス元装置から送信元アドレスと宛先アドレスを設定したパケットを受信し、アドレスとＩＤとを対応付けて格納するアドレス情報格納手段から、前記送信元アドレスに対応する送信元ＩＤを取得する手段と、
前記送信元ＩＤに基づいて、ＩＤ毎に接続先情報を格納したユーザ情報格納手段を参照することにより、前記パケットを前記宛先アドレスに転送するか否かを決定するアクセス判定手段と
を備えたことを特徴とするアクセス制御装置。
【請求項２】
前記ユーザ情報格納手段には、送信元ＩＤに対応するユーザの属性情報が格納されており、前記アクセス判定手段は、当該属性情報と前記接続先情報とを比較することにより、前記パケットを宛先アドレスに転送するか否かを決定する
ことを特徴とする請求項１に記載のアクセス制御装置。
【請求項３】
前記アクセス元装置から接続要求を受信したときに、アドレスを当該アクセス元装置に払い出し、当該アクセス元装置のＩＤと払い出したアドレスとを前記アドレス情報格納手段に格納するアドレス払い出し手段
を備えることを特徴とする請求項１又は２に記載のアクセス制御装置。
【請求項４】
前記アドレス払い出し手段は、前記アクセス元装置の認証がとれている場合にアドレスの払い出しを行う
ことを特徴とする請求項３に記載のアクセス制御装置。
【請求項５】
前記アクセス元装置と前記アクセス制御装置とはトンネル接続され、前記アクセス制御装置は前記パケットをトンネルから受信する
ことを特徴とする請求項１ないし４のうちいずれか１項に記載のアクセス制御装置。
【請求項６】
コンピュータを、請求項１ないし５のうちいずれか１項に記載のアクセス制御装置の各手段として機能させるためのプログラム。
【請求項７】
通信ネットワーク上におけるアクセス元装置からアクセス先装置へのアクセスを制御するアクセス制御装置が実行するアクセス制御方法であって、
前記アクセス元装置から送信元アドレスと宛先アドレスを設定したパケットを受信し、アドレスとＩＤとを対応付けて格納するアドレス情報格納手段から、前記送信元アドレスに対応する送信元ＩＤを取得するステップと、
前記送信元ＩＤに基づいて、ＩＤ毎に接続先情報を格納したユーザ情報格納手段を参照することにより、前記パケットを前記宛先アドレスに転送するか否かを決定するアクセス判定ステップと
を備えたことを特徴とするアクセス制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信ネットワーク上におけるアクセス元装置からアクセス先装置へのアクセスを制御するアクセス制御技術に関連するものである。
【背景技術】
【０００２】
有害なＷｅｂサイトへのアクセスを防止したり、着信端末への迷惑アクセスを防止する

等のために、ネットワーク上のサーバ等に、アクセスを許可するアクセス元端末のアドレスのリスト（ホワイトリスト）をポリシーとして登録しておき、ホワイトリストに登録されていないアドレスからの通信要求を拒否する従来技術がある（例えば特許文献１）。

【０００３】

このような従来技術によれば、例えば特定のアクセス元端末からの有害Ｗｅｂサイトへのアクセスを防止するといったことが可能となる。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００８－０４２６４２号公報

【特許文献２】特開２０１３－５１１０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかし、上記のようなアドレスに基づいたホワイトリストでは、例えば、アクセス元ユーザの年齢等のプロファイルに基づいたアクセス制限を行うことができない。また、アクセス元の識別のためにＩＰアドレスを用いる場合においては、ＩＰアドレスは接続の度に変化する可能性があるため、正確なアクセス制限ができなくなったり、ＩＰアドレスの変化に応じて、リストを更新する仕組みを設ける必要があるといった問題が生じる。

【０００６】

本発明は上記の点に鑑みてなされたものであり、ＩＰアドレスのように変化しないアクセス元ユーザのＩＤを用いてアクセス制御を行うことを可能とする技術を提供することを目的とする。

【課題を解決するための手段】

【０００７】

本発明の一実施形態によれば、通信ネットワーク上におけるアクセス元装置からアクセス先装置へのアクセスを制御するアクセス制御装置であって、

前記アクセス元装置から送信元アドレスと宛先アドレスを設定したパケットを受信し、アドレスとＩＤとを対応付けて格納するアドレス情報格納手段から、前記送信元アドレスに対応する送信元ＩＤを取得する手段と、

前記送信元ＩＤに基づいて、ＩＤ毎に接続先情報を格納したユーザ情報格納手段を参照することにより、前記パケットを前記宛先アドレスに転送するか否かを決定するアクセス判定手段とを備えたことを特徴とするアクセス制御装置が提供される。

【発明の効果】

【０００８】

本発明の一実施形態によれば、ＩＰアドレスのように変化しないアクセス元ユーザのＩＤを用いてアクセス制御を行うことを可能とする技術が提供される。

【図面の簡単な説明】

【０００９】

【図１】本発明の実施の形態に係る通信システムの構成図である。

【図２】トンネル接続の方式の概要を説明するための図である。

【図３】トンネル接続装置の機能を説明するための図である。

【図４】ＮＩＣ１のＲＡＷソケットからフレームを受信したときの動作を説明するための図である。

【図５】ＮＩＣ０のＲＡＷソケットからフレームを受信したときの動作について説明するための図である。

【図６】経路表に含まれるＩＰアドレス向けの通信の場合の動作を説明するための図である。

【図７】ＮＩＣ１のトンネルからＩＰパケットを受信したときの動作を説明するための図である。

【図８】トンネル終端装置２０の機能構成図である。
【図９】アドレス払い出し情報格納部２６に格納されるアドレス払い出し情報の例を示す図である。
【図１０】ユーザ情報格納部２７に格納されるユーザ情報の例を示す図である。
【図１１】システムの動作例を説明するための図である（アクセスが拒否される例）。
【図１２】システムの動作例を説明するための図である（アクセスが許容される例）。
【図１３】接続例を示す図である。
【発明を実施するための形態】
【００１０】
以下、図面を参照して本発明の実施の形態を説明する。なお、以下で説明する実施の形態は一例に過ぎず、本発明が適用される実施の形態は、以下の実施の形態に限られるわけではない。例えば、本実施の形態では、トンネル接続を用いた仮想ネットワークでのアクセス制限を対象とし、アクセス制御装置の例としてトンネル終端装置を用いて説明をしているが、本発明はこのような仮想ネットワークに限定されずに適用可能である。
【００１１】
（システム構成例）
図１に、本発明の実施の形態に係る通信システムの構成図を示す。図１に示すように、本実施の形態の通信システムは、トンネル接続装置１０、トンネル終端装置２０、トンネル接続装置３０、及び接続制御装置４０を有する。各装置はインターネット等のＩＰネットワークに接続されている。図１に示す例では、トンネル接続装置２０にユーザ端末５０（クライアント機器）が接続されている。また、トンネル接続装置３０には、Ｗｅｂサーバ５０が接続される。トンネル接続装置１０／トンネル接続装置３０とトンネル終端装置２０との間でトンネルを構築することにより、仮想ネットワークが構成される。なお、図１には、代表として、１つのトンネル終端装置２０、及び２つのトンネル接続装置１０、３０を示しているが、より多くのトンネル接続装置がトンネル終端装置２０に接続されてもよい。また、複数のトンネル終端装置が存在してもよい。また、トンネル接続装置１０の機能がソフトウェアによりユーザ端末５０に含まれる形態でもよく、トンネル接続装置３０の機能がソフトウェアによりＷｅｂサーバ６０に含まれる形態でもよい。
【００１２】
トンネル接続装置１０、３０は、トンネル終端装置２０とトンネル接続を行う装置である。トンネル終端装置２０は、トンネル接続装置１０、３０からのトンネル接続要求を待ち受け、トンネル接続装置１０、３０との間でトンネル接続を行う装置である。接続制御装置４０は、トンネル接続装置１０、３０とトンネル終端装置２０間でトンネル接続を行うための認証や設定情報の配布等の制御を行う装置である。
【００１３】
本実施の形態では、基本的に、特許文献２に記載されたＬ３モードでのトンネル接続を行うこととしている。ただし、本発明を適用できる接続の方式はこれに限られるわけではない。
【００１４】
図２を参照して、本実施の形態におけるトンネル接続の方式の概要について説明する。図２に示すように、本方式では、ネットワーク終端装置２０とネットワーク接続装置１０、３０との間がトンネル（ＩＰトンネル）で接続される。そして、トンネル接続装置１０とトンネル接続装置３０のそれぞれにＩＰアドレス（図２には、ＩＰ１、ＩＰ２が示されている）が配布される。当該ＩＰアドレスは、仮想ネットワークのＩＰアドレスであり、ＩＰ１はＷｅｂサーバ６０側からはユーザ端末５０のＩＰアドレスとして見え、ユーザ端末５０側からはＩＰ２がＷｅｂサーバ６０のアドレスとして見える。
【００１５】
トンネル接続装置１０、３０には、例えば、接続制御装置４０により、トンネル接続装置１０、３０が認証された場合に当該ＩＰアドレスが配布される。あるいは、接続制御装置４０による認証後に行われるトンネル接続装置１０、３０からトンネル終端装置２０へ

の接続要求に応じて、当該ＩＰアドレスがトンネル終端装置２０からトンネル接続装置１０、３０に配布される。本実施の形態は後者の例で説明している。パケットの転送の流れの概要は以下のとおりである。

【００１６】

図２において、ユーザ端末５０からＷｅｂサーバ６０宛（つまりＩＰ２宛て）に送出されたパケットは、トンネル接続装置１０において、そのソースアドレスがユーザ端末５０のＩＰアドレスからＩＰ１に変換され、カプセリングされてトンネル終端装置２０に送信される。トンネル終端装置２０では、カプセリングヘッダがトンネル２のものに変えられて、パケットがトンネル接続装置３０に転送される。トンネル接続装置３０は、トンネルのヘッダを取り除き、宛先のＩＰ２をＷｅｂサーバ６０のＩＰアドレスに変換したパケットをＷｅｂサーバ６０に送信する。

【００１７】

以下では、本実施の形態のトンネル接続装置１０の機能をより詳しく説明する。図３は、トンネル接続装置１０の機能構成を示す図である。これらの機能はソフトウェアにより実現される。なお、トンネル接続装置１０とトンネル接続装置３０は同じ構成であるので、以下では例としてトンネル接続装置１０について説明する。

【００１８】

図３に示すように、本実施の形態のトンネル接続装置１０はインタフェースを２つ持ち、図３では右側（ＮＩＣ１）方向にインターネット、もしくは宅内ルータへのネットワークが接続される。左側（ＮＩＣ０）方向にはＶＰＮ（トンネル）に接続したい端末が接続される。トンネル接続装置１０では、まず２つのインタフェースに対して、ＯＳの機能であるＲＡＷソケットをオープンしてｐｒｏｍｉｓｃｕｏｕｓモードで全てのＥｔｈｅｒｎｅｔ（登録商標）フレームを受信し、受信したフレームを他方のインタフェースに送信する。

【００１９】

更に、ＮＩＣ１は、インターネットもしくは宅内ルータからＩＰアドレスを割り当てられ、ＩＰホストとして動作する。そして、適切なトランスポートを選択してトンネル終端装置２０との間にコネクションを確立する。トランスポートは通信状態等によりＵＤＰ、ＴＣＰ、ＴＬＳなどが可能であるが、図３ではＵＤＰを例としている。そして、このトンネル終端装置２０との間のコネクションをトンネルとして使用する。

【００２０】

トンネル接続装置１０はトンネル終端装置２０との間にコネクションを確立すると、ＩＰアドレスとネットマスク、そしてトンネル終端装置２０を経由してルーティング可能な経路一覧（ＩＰアドレス一覧）を与えられる。本例では、これらの情報は、トンネル終端装置２０から与えられるが、接続制御装置４０から与えてもよい。図示するように、トンネル接続装置１０は、内部にＮＡＴもしくはＮＡＰＴテーブルを有する。なお、本質的にＮＡＰＴでもＮＡＴでも差異はないことから、以下ではＮＡＴの場合を例にとって説明する。

【００２１】

トンネル終端装置２０から与えられたＩＰアドレスはＮＡＴのソースアドレスとして使用される。また、図示するように、トンネル接続装置１０の内部には経路表が備えられ、与えられたＩＰアドレスの属するネットワークアドレス、及びトンネル終端装置２０を介してルーティング可能なネットワークアドレスが保存される。また、図示するように、トンネル接続装置１０は、ＭＡＣアドレステーブルを備え、これはパケット転送動作時に使用される。

【００２２】

図４を参照して、ＮＩＣ１（インターネット側）のＲＡＷソケットからＥｔｈｅｒｎｅｔ（登録商標）フレームを受信したときの動作について説明する。この場合は単にＥｔｈｅｒｎｅｔ（登録商標）ブリッジとして動作させるために、受信したＥｔｈｅｒｎｅｔ（登録商標）フレームには変更を加えず、ＮＩＣ０に出力する。これにより、ＮＩＣ０に接

続された端末は、本装置の有無にかかわらずインターネットからのフレームを受信できる。

【００２３】

次に、図５を参照して、ＮＩＣ０のＲＡＷソケットからＥｔｈｅｒｎｅｔ（登録商標）フレームを受信したときの動作について説明する。

【００２４】

まず、トンネル接続装置１０は、受信したフレームの発信元ＭＡＣアドレスをＭＡＣテーブルに記憶しておく。次に、そのＥｔｈｅｒｎｅｔ（登録商標）フレームがＩＰパケットであるなら、宛先ＩＰアドレスが経路表に含まれているものかどうかを判定し、含まれていない場合は、当該フレームをそのままＮＩＣ１側のＲＡＷソケットに送出する。これにより、経路表登録外のＩＰアドレス向けのＥｔｈｅｒｎｅｔ（登録商標）フレームは２つのＲＡＷソケット間を通過するので、ＮＩＣ０に接続された端末から見れば本装置は単なるＥｔｈｅｒｎｅｔ（登録商標）ブリッジとして見えて、本装置の介在有無にかかわらずインターネット上のホストへの接続が可能である。また、例えば、本装置を介しての宅内ルータとの非ＩＰパケットも通過できるので、本装置を介しながら接続端末に対してＤＨＣＰでＩＰアドレスを配布することも可能である。

【００２５】

経路表に含まれるＩＰアドレス向けの通信の場合の動作については、更に、図６を参照して説明する。まず、ＮＩＣ０にある端末はデフォルト経路にパケットを送出しようとして、デフォルトルータにＡＲＰ要求を発する（ステップ１０１）。この場合、本装置は非ＩＰパケットとしてＮＩＣ１へそのまま転送する。ＮＩＣ１側のデフォルトルータからＡＲＰ応答が返されると、本装置はそのままＮＩＣ０側へ転送し（ステップ１０２）、その後、ＮＩＣ０に接続された端末はＶＰＮ向けのＩＰパケットをデフォルトルータ向けのＭＡＣアドレスをあて先として発信する（ステップ１０３）。

【００２６】

トンネル接続装置１０は、宛先ＩＰアドレスが経路表に含まれるとの判定を行うと（ステップ１０４、図５での宛先ＩＰ判定）、発信元ＩＰアドレスをＮＡＴテーブルに記録して、パケットの発信元ＩＰアドレスを事前にトンネル終端装置２０から得たＩＰアドレスで書き換え、処理軽減のためのＥｔｈｅｒｎｅｔ（登録商標）ヘッダの切り落とし等の処理を行って、トンネル終端装置２０に送信する（ステップ１０５）。このように、トンネル接続装置１０とトンネル終端装置２０間はＩＰｉｎＩＰのトンネル通信となる。なお、図５等に示されるＶＮヘッダは仮想ＮＷヘッダであり、メタ情報等が記録されている。

【００２７】

次に、図７を参照して、ＮＩＣ１のトンネルからＩＰパケットを受信したときの動作を説明する。トンネル終端装置２０からの通信は、ＵＤＰソケットから受信される。受信されたパケットのＰＤＵにはＩＰパケットが格納されているので、このパケットの宛先ＩＰアドレスを、ＮＡＴテーブルの発信元ＩＰアドレスで置き換え、ＭＡＣテーブルに基づいて、宛先ＭＡＣアドレスを端末ＭＡＣアドレスに設定したＥｔｈｅｒｎｅｔ（登録商標）ヘッダを付加してＮＩＣ０側に送り出す。これにより、ＮＩＣ０に接続された端末は、トンネル終端装置２０側から発信されたパケットを受け取ることができる。

【００２８】

本実施の形態では、このようなトンネル接続装置１０、３０とトンネル接続を行うトンネル終端装置２０において、トンネル接続装置のＩＤでアクセスリストを設定し、ユーザプロファイルによってアクセス可能なサーバ群を選択することを可能としている。

【００２９】

なお、「ＩＤ」は、特定の形式に限定されない識別情報である。「ＩＤ」としては例えば番号、名前等がある。

【００３０】

（装置構成例）

図８に、本実施の形態に係るトンネル終端装置２０の機能構成図を示す。図８に示すよ

うに、トンネル終端装置２０は、制御通信処理部２１、アドレス払い出し部２２、アクセス判定部２３、トンネル通信処理部２４、アドレス格納部２５、アドレス払い出し情報格納部２６、ユーザ情報格納部２７を有する。

【００３１】

制御通信処理部２１は、接続制御装置４０等と制御情報の送受信を行う。アドレス払い出し部２２は、アドレス格納部２５に格納された払い出し可能なＩＰアドレスをトンネル接続装置からの要求に応じてトンネル接続装置に払い出す。

【００３２】

アクセス判定部２３は、アドレス払い出し情報格納部２６を参照することにより、トンネル接続装置から受信したパケットの送信元ＩＰアドレスと宛先ＩＰアドレスのそれぞれのＩＤを取得し、これらＩＤに基づいて、ユーザ情報格納部２７を参照することで、トンネル接続装置からのアクセスを許容するかどうかを判定する。

【００３３】

トンネル通信処理部２４は、トンネル接続装置との間でトンネル通信を行う。アドレス格納部２５には、払い出し用のＩＰアドレス群が格納される。このＩＰアドレス群は、例えば接続制御装置４０から与えられたものである。

【００３４】

図９は、アドレス払い出し情報格納部２６に格納される払い出し情報の例を示す図である。図９に示すように、アドレス払い出し情報格納部２６にはＩＰアドレスを払い出した先のトンネル接続装置のＩＤ（ユーザＩＤ）と、払い出したＩＰアドレスとが対応付けて格納される。

【００３５】

図１０は、ユーザ情報格納部２７に格納される情報の例を示す図である。本実施の形態では、ＩＤ毎に該当ユーザに許容する接続先（群）の情報がユーザ情報格納部２７に格納される。図１０に示す例では、ＩＤ１のユーザはＩＤ２にのみ接続でき、ＩＤ２のユーザは、どのＩＤにも接続できる。

【００３６】

本実施の形態に係るトンネル終端装置２０は、ＣＰＵ、記憶装置等からなるコンピュータ（コンピュータの構成を含む通信装置でもよい）に、トンネル終端装置２０の各機能部の機能を実現するためのプログラムを実行させることにより実現できる。当該プログラムは可搬メモリ等の記録媒体からコンピュータにインストールすることとしてもよいし、ネットワーク上のサーバからダウンロードすることとしてもよい。

【００３７】

なお、図８に示すトンネル終端装置２０において、アドレス格納部２５、アドレス払い出し情報格納部２６、ユーザ情報格納部２７のいずれか１つ又は複数又は全部は、別装置に備えられていてもよい。その場合、トンネル終端装置２０はネットワーク経由で当該格納部にアクセスし、必要な情報の取得／格納を行う。

【００３８】

（システムの動作例）

次に、図１１、図１２を参照して、本実施の形態に係るシステムの動作例を説明する。図１１、図１２に示す動作例は、トンネル接続装置１０（ユーザ端末５０）からトンネル接続装置３０（Ｗｅｂサーバ６０）へのアクセスを行う場合の動作例である。図１１は、アクセスが拒否される例を示し、図１２は、アクセスが許容される例を示す。

【００３９】

本動作の前提として、トンネル接続装置１０は、例えば、接続制御装置４０にＩＤ／パスワードを送信することで接続制御装置４０から認証され、その結果、トンネル接続装置１０のトンネル接続先であるトンネル終端装置２０のアドレス情報を取得しており、トンネル終端装置２０へのアクセスが可能になっているものとする。また、トンネル接続装置３０は接続制御装置４０による認証が済み、トンネル終端装置２０から既にＩＰアドレスが配布されており、トンネル接続装置３０とトンネル終端装置２０間でトンネル通信可能

であるとする。

【００４０】

図１１において、トンネル接続装置１０は、自身のＩＤを含むトンネル接続要求をトンネル終端装置２０に送信する（ステップ１）。トンネル接続要求を受信したトンネル終端装置２０において、アドレス払い出し部２２が、アドレス格納部２５から、払い出し可能なＩＰアドレス（ＩＰ１）を取り出し、当該ＩＰ１をトンネル接続装置１０に払い出す（ステップ２）。また、アドレス払い出し部２２は、払い出し先のトンネル接続装置１０のＩＤ１と、払い出したＩＰ１とをアドレス払い出し情報として、アドレス払い出し情報格納部２６に格納する（ステップ３）。

【００４１】

図９の例では、Ｗｅｂサーバ６０側のトンネル接続装置３０のＩＤがＩＤ３で、ＩＰアドレスはＩＰ３が払い出されているものとする。

【００４２】

ＩＰ１の払い出しを受けたトンネル接続装置１０は、送信元ＩＰアドレスをＩＰ１、宛先ＩＰアドレスをＩＰ３としたパケットをトンネルを介して送信する（ステップ４）。

【００４３】

パケットを受信したトンネル終端装置２０では、アクセス判定部２３が、アドレス払い出し情報格納部２６（図９）を参照することで、送信元ＩＰアドレスであるＩＰ１に対応するＩＤ１、及び宛先ＩＰアドレスであるＩＰ３に対応するＩＤ３を取得する（ステップ５）。そして、アクセス判定部２３は、ユーザ情報格納部２７（図１０）を参照することで、ＩＤ１に許容されている宛先のＩＤがＩＤ２であることを把握する。ここで、パケットの宛先であるＩＤ３はＩＤ２と異なるので、アクセス判定部２３はアクセスを拒否する。アクセスを拒否した場合、パケットは破棄される。

【００４４】

次に、アクセスが許容される場合の例を図１２を参照して説明する。図１２の例では、宛先のトンネル接続装置３０のＩＤがＩＤ２であり、ＩＰアドレスはＩＰ２が割り当てられているものとする。

【００４５】

図１２において、ステップ３までの処理は図１１と同じである。ステップ４において、トンネル接続装置１０は、送信元ＩＰアドレスをＩＰ１、宛先ＩＰアドレスをＩＰ２としたパケットをトンネルを介して送信する。

【００４６】

パケットを受信したトンネル終端装置２０では、アクセス判定部２３が、アドレス払い出し情報格納部２６（図９）を参照することで、送信元ＩＰアドレスであるＩＰ１に対応するＩＤ１、及び宛先ＩＰアドレスであるＩＰ２に対応するＩＤ２を取得する（ステップ５）。そして、アクセス判定部２３は、ユーザ情報格納部（図１０）を参照することで、ＩＤ１に許容されている宛先のＩＤがＩＤ２であることを把握する。ここで、パケットの宛先であるＩＤ２はＩＤ２と一致するので、アクセス判定部２３はアクセスを許容する。

【００４７】

トンネル終端装置２０のトンネル通信処理部２４は、パケットを宛先のＩＰ２に対応するトンネルに送り出す（ステップ７）。これにより、パケットはＷｅｂサーバ６０まで届けられる。このようにして、図１２の場合には、ユーザ端末５０はＷｅｂサーバ６０との通信が可能となる（ステップ８）。

【００４８】

上記のように、本実施の形態によれば、接続毎に変るＩＰアドレスではなく、接続毎に変らない装置もしくはユーザのＩＤでアクセスリスト（図１０のユーザ情報に相当）を設定でき、当該アクセスリストによって、アクセス先を選択できる。

【００４９】

本例では、アクセスリストとして、図１０に示すように簡単な例を示したが、例えば、ユーザのＩＤに対応付けて、ユーザの属性（年齢等のプロファイル）も設定し、アクセス

先のサイトの情報としてＩＤに対応付けて例えばある年齢以上のみアクセス可能といった情報の設定を行うこともできる。この場合、ＩＤに対応付けられた年齢と、サイトで許容できる年齢とを比較することで、アクセス許可／拒否を決定できる。

【００５０】

また、本例では、Ｗｅｂサーバ６０側にもトンネル接続装置３０を配置しているが、Ｗｅｂサーバ６０側にトンネル接続装置３０を配置しないこととしてもよい。その場合、Ｗｅｂサーバ６０にはＩＤとともに仮想ネットワークのアドレスを固定的に割り当て、仮想ネットワーク経由でアクセス可能としておけばよい。

【００５１】

また、本実施の形態の技術は、図１３に示すように利用することも可能である。図１３では、例として、特定のサイトを提供するＷｅｂサーバ６０と、有害サイトを提供するＷｅｂサーバ８０が示されており、Ｗｅｂサーバ６０にはトンネル接続装置３０が接続されて仮想ネットワークの通信が可能であり、Ｗｅｂサーバ８０はインターネットに接続されている。また、ユーザ端末５０はトンネル接続装置１０に接続されて仮想ネットワークの通信が可能であり、端末７０はインターネットに接続されている。

【００５２】

この場合、前述したトンネル接続装置の動作により、特定のサイトへのアクセスは、仮想ネットワーク経由でできるとともに、通常のインターネット経由でもできる。そして、ユーザ端末５０側では仮想ネットワークだけしか利用できないように制限をかける。この制限は、例えば、トンネル接続装置１０の宛先ＩＰ判定機能において、経路表に記載された仮想ネットワークのＩＰアドレスの宛先にのみパケットを送り出すようにすれば実現できる。また、トンネル終端装置２０においては、ユーザ情報（図１１）として、ユーザ端末５０のユーザはどのアドレス（仮想ネットワークのアドレス）にも接続可能としておく。このことは、トンネル終端装置２０が本実施の形態で説明したアクセス制限の機能を有しない場合も含む。このようにした場合、トンネル接続装置１０を有するユーザ端末５０からはインターネット上に存在する有害サイトへのアクセスはできず、その仮想ネットワークに加入しているサイトだけのアクセスが可能になる。このような方式は、例えば以下のような事例に適用することができる。

【００５３】

例えば、学校等の教育機関のサイトからなる仮想ネットワークを構成する。上述したとおり、それらのサイトは仮想ネットワークに加入しても、通常のインターネットからのアクセスも依然可能である。そして、端末側で、利用者が未成年である場合には保護者は仮想ネットワーク経由でのインターネットアクセスに限定するように設定する。これにより、仮想ネットワークに参加するユーザは許可されたサイトだけにアクセスできるホワイトリストインターネットが実現される。

【００５４】

本実施の形態では、トンネル終端装置２０の装置構成として図８の例を示したが、装置構成は図８に限られるわけではなく、本発明に係る技術を実施できる構成であればどのような構成でもよい。例えば、トンネル終端装置を、通信ネットワーク上におけるアクセス元装置からアクセス先装置へのアクセスを制御するアクセス制御装置として構成し、前記アクセス元装置から送信元アドレスと宛先アドレスを設定したパケットを受信し、アドレスとＩＤとを対応付けて格納するアドレス情報格納手段から、前記送信元アドレスに対応する送信元ＩＤを取得する手段と、前記送信元ＩＤに基づいて、ＩＤ毎に接続先情報を格納したユーザ情報格納手段を参照することにより、前記パケットを前記宛先アドレスに転送するか否かを決定するアクセス判定手段とを備えることとしてもよい。

【００５５】

前記ユーザ情報格納手段には、例えば送信元ＩＤに対応するユーザの属性情報が格納されており、前記アクセス判定手段は、当該属性情報と前記接続先情報とを比較することにより、前記パケットを宛先アドレスに転送するか否かを決定することができる。

【００５６】

前記アクセス制御装置は、前記アクセス元装置から接続要求を受信したときに、アドレスを当該アクセス元装置に払い出し、当該アクセス元装置のＩＤと払い出したアドレスとを前記アドレス情報格納手段に格納するアドレス払い出し手段を備えることとしてもよい。

【００５７】

前記アドレス払い出し手段は、例えば、前記アクセス元装置の認証がとれている場合にアドレスの払い出しを行う。また、前記アクセス元装置と前記アクセス制御装置とはトンネル接続され、前記アクセス制御装置は前記パケットをトンネルから受信するように構成されてもよい。

【００５８】

本発明は、上記の実施の形態に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

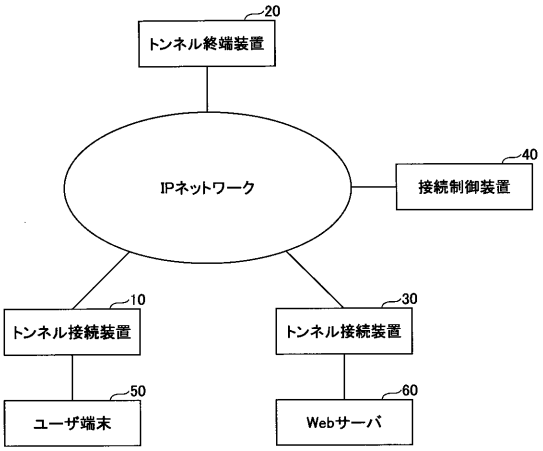
【符号の説明】

【００５９】

１０　トンネル接続装置
２０　トンネル終端装置
３０　トンネル接続装置
４０　接続制御装置
５０　ユーザ端末
６０、８０　Ｗｅｂサーバ
２１　制御通信処理部
２２　アドレス払い出し部
２３　アクセス判定部
２４　トンネル通信処理部
２５　アドレス格納部
２６　アドレス払い出し情報格納部
２７　ユーザ情報格納部

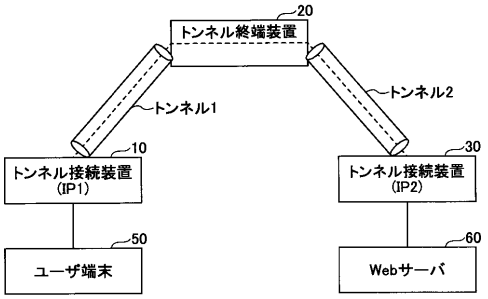
【図１】

本発明の実施の形態に係る通信システムの構成図



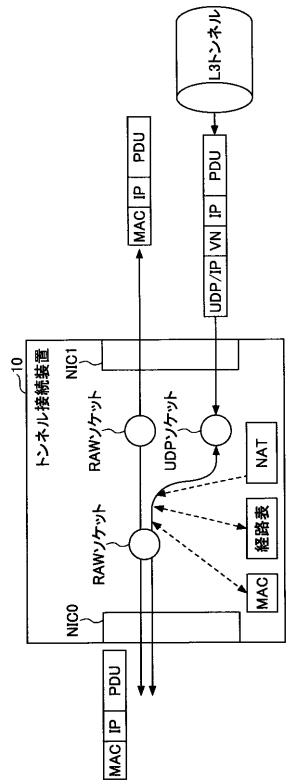
【図２】

トンネル接続の方式の概要を説明するための図



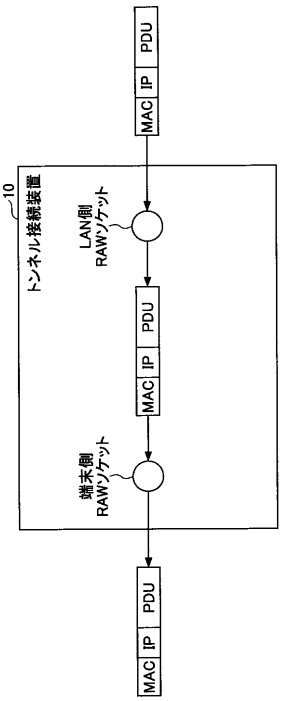
【図３】

トンネル接続装置の機能を説明するための図



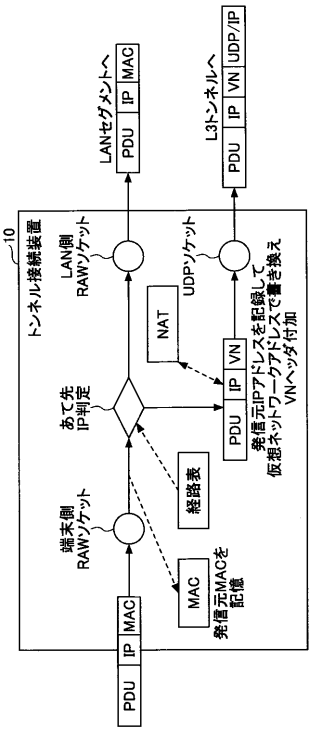
【図４】

NIC1のRAWソケットからフレームを受信したときの動作を説明するための図



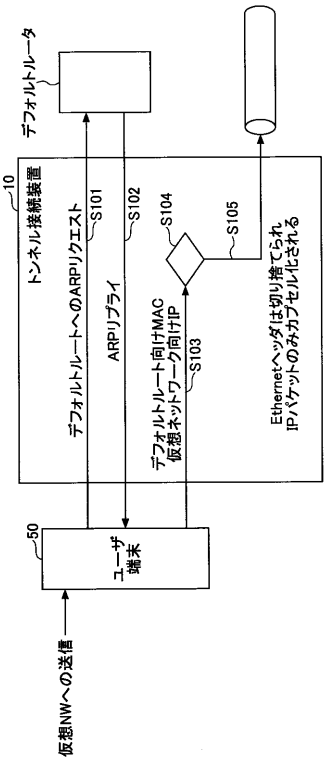
【図５】

NIC0のRAWソケットからフレームを受信したときの動作について説明するための図



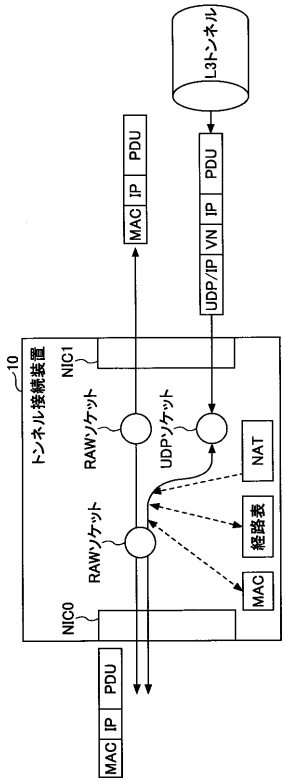
【図６】

経路表に含まれるIPアドレス向けの通信の場合の動作を説明するための図



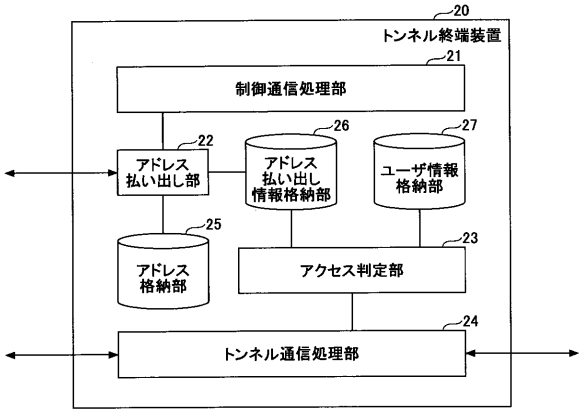
【図７】

NIC1のトンネルからIPパケットを受信したときの動作を説明するための図



【図８】

トンネル終端装置20の機能構成図



【図９】

アドレス払い出し情報格納部26に格納されるアドレス払い出し情報の例を示す図

ID	IPアドレス
ID1	IP1
ID2	IP2
ID3	IP3

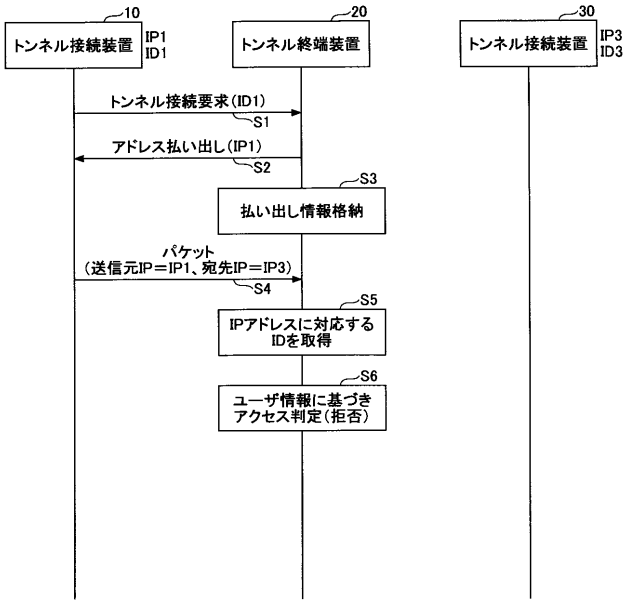
【図１０】

ユーザ情報格納部27に格納されるユーザ情報の例を示す図

ユーザID	接続先
ID1	ID2
ID2	ANY
ID3	ANY

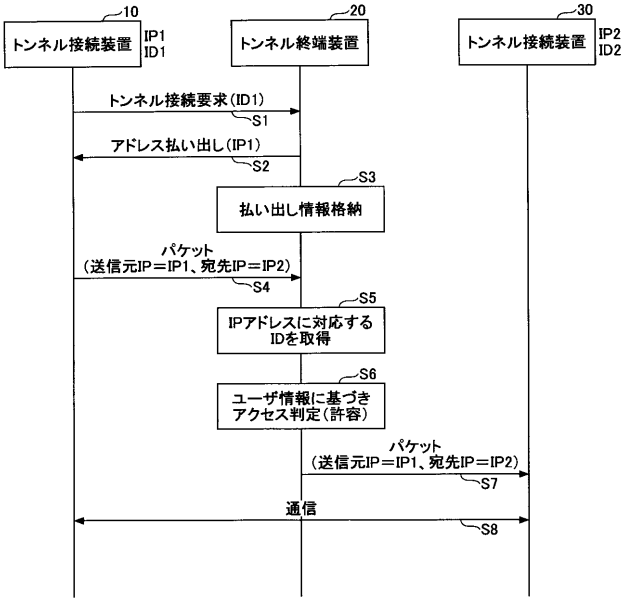
【図１１】

システムの動作例を説明するための図（アクセスが拒否される例）



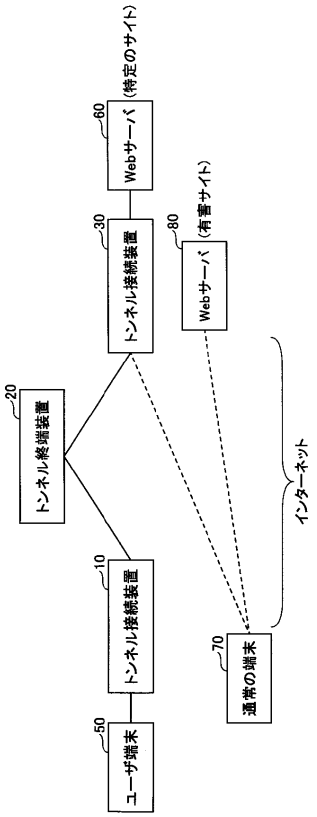
【図１２】

システムの動作例を説明するための図（アクセスが許容される例）



【図１３】

接続例を示す図



フロントページの続き

(72)発明者　上水流　由香
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

Ｆターム(参考) 5K030 GA15 HA08 HD03 HD06 HD09 JA11 KA05 LB20 MD09 MD10
5K033 AA08 CB08 DA06 DB12 DB18 EC03