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

特許第4253569号
(P4253569)

(45)発行日　平成21年4月15日(2009.4.15)　(24)登録日　平成21年1月30日(2009.1.30)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	100Z
H04W 40/34	(2009.01)	H04L	12/56	B
G09C 1/00	(2006.01)	H04L	12/56	100D
		G09C	1/00	640E

請求項の数 9　(全 25 頁)

(21)出願番号　特願2003-403971 (P2003-403971)
(22)出願日　平成15年12月3日 (2003.12.3)
(65)公開番号　特開2005-167646 (P2005-167646A)
(43)公開日　平成17年6月23日 (2005.6.23)
審査請求日　平成18年6月7日 (2006.6.7)

(73)特許権者　000153465
株式会社日立コミュニケーションテクノロジー
東京都品川区南大井六丁目２６番３号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　吉内　英也
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
(72)発明者　秋山　秀洋
東京都品川区南大井六丁目２６番３号　株式会社日立コミュニケーションテクノロジー内

最終頁に続く

(54)【発明の名称】接続制御システム、接続制御装置、及び接続管理装置

(57)【特許請求の範囲】

【請求項１】

通信網を介して第一の端末と接続された第一のゲートウェイ、第二の端末と接続された第二のゲートウェイ及び第三のゲートウェイと接続可能な接続管理装置であって、

上記通信網に接続可能な送受信部と、

上記送受信部と接続されたＣＰＵとを備え、

上記送受信部で上記第一の端末から上記第二の端末への接続要求を受信した場合に、上記上記ＣＰＵは、上記第一の端末から上記第二の端末への接続が可能かどうかを判定し、上記判定の結果、上記接続が上記第一ゲートウェイから上記第二のゲートウェイへ直接不可能な場合には、上記第二の端末と接続可能で、上記第一の端末と上記第二の端末間において経由する上記第１のゲートウェイ、上記第二のゲートウェイ及び上記第三のゲートウェイそれぞれを特定するアドレスを生成し、

該生成されたアドレスを含むデータを上記送受信部を介して上記第一の端末へ送信し、

上記第三のゲートウェイを介して第一の端末と第二の端末間の接続を開始するために、上記第一のゲートウェイ及び上記第三のゲートウェイに前記生成したアドレスを含むアドレス登録要求を上記送受信部を介して送信し、

前記第１の端末から前記接続が終了した旨の通知を前記送受信部を介して受信した場合、前記アドレス登録要求に含まれるアドレスの削除要求を前記第一のゲートウェイ及び前記第三のゲートウェイに上記送受信部を介して送信することを特徴とする接続管理装置。

【請求項２】

さらに、前記ＣＰＵに接続される記憶装置を備え、
上記記憶装置には、上記第一の端末から上記第二の端末への接続が可能かどうかを判定するデータベースが格納されており、
上記ＣＰＵは、上記データベースを用いて上記判定を行うことを特徴とする請求項１記載の接続管理装置。
【請求項３】
上記判定の結果、上記接続が不可能な場合には、
上記ＣＰＵはさらに、上記第一の端末から上記第二の端末への通信可能な通信経路を検索し、
上記検索の結果、上記通信経路が存在する場合に、上記アドレスを生成することを特徴とする請求項１記載の接続管理装置。
【請求項４】
上記判定の結果、上記接続が不可能な場合には、上記第一の端末にその旨を通知し、さらに上記第一の端末から要求があった後に、上記アドレスを生成することを特徴とする請求項１または２いずれか記載の接続管理装置。
【請求項５】
上記判定の結果、上記接続が可能な場合には、
上記ＣＰＵはさらに、
上記第一の端末を認証するプログラムを上記記憶装置から読み出して実行し、
上記第一の端末の認証に成功した後に、上記アドレスを生成することを特徴とする請求項２または３いずれかに記載の接続管理装置。
【請求項６】
通信網を介して第一の端末と接続された第一のゲートウェイ、第二の端末と接続された第二のゲートウェイ及び第三のゲートウェイと接続可能な接続制御システムであって、
上記通信網と接続された送受信部、上記送受信部と接続されたＣＰＵをそれぞれ備えた接続制御装置及びアドレス生成装置を備え、
上記接続制御装置では、
上記接続制御装置の送受信部で、上記第一の端末から上記第二の端末への接続要求を受付けた場合に、
上記接続制御装置のＣＰＵが、上記第一の端末から上記第二の端末への接続が可能かどうかを判定し、
上記判定の結果、上記接続が上記第一ゲートウェイから上記第二のゲートウェイへ直接不可能な場合には、
上記接続制御装置の送受信部から、上記第二の端末と上記第三のゲートウェイを介して接続可能なアドレスの生成依頼を上記アドレス生成装置に送信し、
上記アドレス生成装置では、
上記アドレス生成装置の送受信部で、上記アドレスの生成依頼を受信し、
上記アドレス生成装置のＣＰＵが前記第一の端末と第二の端末間を経由する前記第１のゲートウェイ、第二のゲートウェイ及び第三のゲートウェイそれぞれを特定するアドレスを生成し、
上記アドレス生成装置の送受信部から、該アドレスを含むデータを上記第一の端末へ送信し、
上記第三のゲートウェイを介して第一の端末と第二の端末間の接続を開始するために、上記アドレス生成装置の送受信部から、上記第一のゲートウェイ及び上記第三のゲートウェイに前記生成したアドレスを含むアドレス登録要求を送信し、
前記第１の端末から前記接続が終了した旨の通知を上記アドレス生成装置の送受信部が受信した場合、前記アドレス登録要求に含まれるアドレスの削除要求を前記第一のゲートウェイ及び前記第三のゲートウェイに上記アドレス生成装置の送受信部から送信する
ことを特徴とする接続制御システム。
【請求項７】

上記接続制御装置での判定の結果、上記接続が不可能な場合には、
上記接続制御装置のＣＰＵはさらに、上記第一の端末から上記第二の端末への通信可能な通信経路を検索し、
上記検索の結果、上記通信経路が存在した場合には、
上記接続制御装置の送受信部から、上記第二の端末と接続可能なアドレスの生成依頼を上記アドレス生成装置に送信することを特徴とする請求項６記載の接続制御システム。
【請求項８】
上記接続制御装置における判定の結果、上記接続が不可能な場合には、
上記接続制御装置が第一の端末にその旨を通知し、
さらに上記第一の端末から要求があった後に、
上記アドレス生成装置が上記アドレスを生成することを特徴とする請求項６または７記載の接続制御システム。
【請求項９】
上記通信網に接続された送受信部と、上記送受信部に接続され、さらに相互に接続されたＣＰＵ及びメモリを備えた認証装置をさらに備え、
上記接続制御装置における判定の結果、上記接続が可能な場合には、
上記認証装置のＣＰＵは、上記第一の端末の認証を実行し、
さらに上記認証装置が上記第一の端末の認証に成功した後に、
上記アドレス生成装置が、上記アドレスを生成することを特徴とする請求項６乃至８のいずれかに記載の接続制御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信網を介して複数の通信端末と相互接続されている接続制御システム、これを構成する接続制御装置、接続管理装置、この接続管理装置の動作プログラムに関する。
【背景技術】
【０００２】
通信網が拡大し、業務への適用が進む中、企業機密などの秘密情報を保護する目的で、接続に制限を設ける技術が開発されている。このような技術のうちで代表的なものは ＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）である。ＶＰＮにはＭＰＬＳ（（Ｍｕｌｔｉ Ｐｒｏｔｏｃｏｌ Ｌａｂｅｌ Ｓｗｉｔｃｈｉｎｇ）、ＩＰＳｅｃ（ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ＳＥＣｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）、Ｌ２ＴＰ（Ｌａｙｅｒ２ Ｔｕｎｎｅｌｉｎｇ Ｐｒｏｔｏｃｏｌ）等様々な技術を用いた実現方式が存在するが、基本動作は通信網に接続制限を設け、接続が許可されている通信網間に対してのみ通信を許可するというものである。接続許可はシステム構築時に接続許可データベースに接続を許可する接続元ネットワークと接続先ネットワークの対応を登録することで与えられる。多くの場合、接続許可を得るためには接続元端末と接続先端末が接続元ネットワーク、接続先ネットワークにそれぞれ属しているだけでは不十分であり、さらにユーザ認証、端末認証等の認証処理を必要とする。
【０００３】
例えば、特許文献１には複数のＩＳＰ（Ｉｎｔｅｒｎｅｔ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ）間にまたがるリモートＶＰＮの統一的管理方法が記載されているが、このような場合にも認証処理を必要とする。
【０００４】
【特許文献１】特開２００３－８６０７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、前記の特許文献の接続制御方法では、接続元と接続先のISPが相互接続を許可

していない場合など、接続元端末が接続許可のないネットワークに属する場合に通信できないという問題点がある。特に、移動体端末のように頻繁にネットワーク間を移動する端末では、自身が所属するネットワークが変化した場合に目的の端末と通信できなくなる可能性があるという問題が発生する。
本発明の目的は、接続に制限のあるネットワークにおいて、接続元端末または接続先端末の移動などにより接続元端末から接続先端末への接続が不可能となった場合に、接続元端末に対して接続先端末と通信が可能なアドレスを割り当てることにより、接続許可のない端末間の通信を実現することにある。
【課題を解決するための手段】
【０００６】
本発明における接続制御システムは、ネットワーク間または端末間の通信を制御し、接続許可判定を行う接続制御装置。接続要求を発した利用者を認証する認証装置を備える。接続許可のないネットワークに属する端末からの接続要求が到着した場合、接続制御システムは端末に対して接続ができない旨を通知する。さらに、端末が接続制御システムに対し、通信を可能にするための通信経路の検索と、通信の際に使用するアドレスの割当を要求した場合、接続制御システムは自システムが管理するネットワーク内で、迂回路通信経路を検索する。次に接続要求を発した端末の認証をした後、認証された端末に対して、接続許可のあるネットワークと接続可能なアドレスを割り当てることで前記問題を解決する。
【発明の効果】
【０００７】
本発明の接続制御システムは接続不可能な端末間の通信において、接続許可のあるネットワークの連結による迂回路を設定し、認証を経ることで接続許可のないネットワーク間の通信を可能にする。このような処理を行うことにより、頻繁にネットワークを移動する移動体端末同士の通信の利便性を向上させる。
【発明を実施するための最良の形態】
【０００８】
本発明における接続制御システムの構成を図１に示す。該システムにおいてネットワーク１（１）に属する端末１（１０）、ネットワーク２（２）に属する端末２（２０）、ネットワーク３（３）に属する端末３（３０）、ネットワーク４（４）に属する端末４（４０）は、ＬＡＮ（５００１０）によりゲートウェイ１（１５）、ゲートウェイ２（２５）、ゲートウェイ３（３５）、ゲートウェイ４（４５）と接続し、これらを通じて、接続制御システム（５）に接続している。接続制御システム（５）は、端末間の通信を制御する接続制御装置（５２）、利用者の認証を行う認証装置（５４）、迂回路接続の際に必要となる接続用アドレスを生成するアドレス管理装置（５６）を備える。ここで、ネットワーク１（１）からネットワーク３（３）への通信は許可されていない。しかし、ネットワーク１（１）からネットワーク２（２）、ネットワーク２（２）からネットワーク３（３）への通信はそれぞれ許可されている。
【０００９】
次に、接続制御システム（５）を構成する個々の要素の機能ブロックを示す。図２はゲートウェイ１（１５）の構成である。接続制御装置が端末の接続を制御するために、接続制御装置と接続した図１中の他のゲートウェイ２～４（２５、３５、４５）も同様の構成を持つ。
ゲートウェイ１（１５）は、ネットワークインターフェース(５００００)を通じて外部と通信を行う。ゲートウェイ１（１５）はさらにＣＰＵ（５０００２）、ハードディスク（５０００４）、メモリ（５０００８）を備え、これらはバス（５０００６）により相互にデータを送受信する。これらのハードウェア構成において、ゲートウェイ１（１５）は端末からのパケットを受信して、宛先アドレスへ送信するパケット送受信部（１１０）をネットワークインターフェース（５００００）に、接続を許可された端末の実アドレス（１２０１０）を登録するアドレス登録テーブル（１２０）、迂回路接続の際に使用する迂回

路アドレス（１３０１０）と実アドレス（１３０２０）の組を登録する迂回路アドレス登録テーブル（１３０）、通信状態を監視する通信監視タイマ（１４０）をメモリ（５０００８）上に備える。

【００１０】

実アドレスは端末のネットワークインターフェースに割り当てられているアドレスであり、接続元端末と接続先端末の通信が許可されている場合はこのアドレスを用いて通信を行う。迂回路接続とは接続元端末と接続先端末の通信ができない場合に、接続許可のあるネットワークを経由した通信経路を迂回路として用いることで端末間の接続を制御することを指す。迂回路アドレスは迂回路接続において通信を行う場合にアドレス管理装置が端末に割り当てるアドレスである。

図３は接続制御装置（５２）の構成である。接続制御装置（５２）は外部と通信するためのネットワークインターフェース（５００００）と、ＣＰＵ（５０００２）、ハードディスク（５０００４）、バス（５０００６）、メモリ（５０００８）を基本ハード構成として備える。さらに、接続制御装置（５２）は端末からのパケットを受信、あるいは送信するためのパケット送受信部（５２０）、接続制御システム（５）内の他の装置に処理を依頼するためのメッセージを送信したり、他の装置の処理結果をメッセージとして受信するためのメッセージ送受信部（５２２）をネットワークインターフェース（５００００）に、端末からの接続要求に対して送信元端末のアドレスと送信先端末のアドレスから接続許可を判定するための情報を含む接続許可データベース（５２４）をハードディスク（５０００４）に、接続制御対象のユーザの状態を管理するユーザ状態管理部（５２６）、通信状態を監視する通信監視タイマ（５２８）をメモリ（５０００８）上で動作する接続制御プログラム（５２０００）の接続制御機能（５２００２）の一部として備える。ここで、メッセージとはシステム内の各装置間で交換されるパケットを指す。

【００１１】

図４は接続許可データベース（５２４）の詳細である。接続許可データベース（５２４）は接続が許可されているネットワーク間の関係を保持するものであり、接続元ネットワーク（５２４２）、接続先ネットワーク（５２４４）と、迂回路として使用可能かどうかを示す迂回路判定フラグ（５２４６）を含む。迂回路判定フラグ（５２４６）が真の時は、この通信路を迂回路として用いることが可能である。

【００１２】

図５はユーザ状態管理部（５２６）の詳細である。図５では一つのデータレコードのみ例示している。ユーザ状態管理部は接続制御中のユーザの状態を管理する機能ブロックであり、ユーザ名（５２６０）、端末アドレス（５２６１）、接続元ネットワーク（５２６２）、接続先ネットワーク（５２６４）、迂回路判定フラグ（５２６６）、認証判定フラグ（５２６８）、迂回路アドレス１（５２７０）、迂回路アドレスＮ（５２７２）を含む。迂回路判定フラグ（５２６６）　は、対象ユーザが迂回路を使用中の場合に真となる。認証判定フラグ（５２６８）は、接続元ネットワークから接続先ネットワークへ通信する際のユーザ認証が完了済の場合に真となる。

【００１３】

図６は認証装置（５４）の構成である。認証装置（５４）は外部と通信するためのネットワークインターフェース（５００００）と、ＣＰＵ（５０００２）、ハードディスク（５０００４）、バス（５０００６）、メモリ（５０００８）を基本ハード構成として備える。さらに、認証装置（５４）はメッセージ送受信部（５４０）をネットワークインターフェース（５００００）に、認証データベース（５４２）をハードディスク（５０００４）上に備え、メモリ（５０００８）上で動作する認証プログラム（５４０００）の認証機能（５４００２）の一部として通信監視タイマ（５４４）を備える。

【００１４】

図７は認証データベース（５４２）の詳細である。図７では一つのデータレコードのみ例示している。迂回路接続を行う場合には複数の通信経路を経由して通信を行うが、その際認証は個々の通信経路ごとに行なう。認証データベース（５４２）は認証対象のユーザ

名（５４２０）、接続元ネットワーク（５４２２）、接続先ネットワーク（５４２４）、パスワード（５４２６）を含む。

【００１５】

図８はアドレス管理装置（５６）の構成である。アドレス管理装置（５６）は外部と通信するためのネットワークインターフェース（５００００）と、ＣＰＵ（５０００２）、ハードディスク（５０００４）、バス（５０００６）、メモリ（５０００８）を基本ハード構成として備える。さらに、アドレス管理装置（５６）はメッセージ送受信部（５６０）をネットワークインターフェース（５００００）に、迂回路接続に用いるアドレスを生成するアドレス生成部（５６２）、アドレス生成時に必要な情報を管理するネットワーク情報管理部（５６４）、通信状態を監視する通信監視タイマ（５６６）をメモリ（５０００８）上で動作するアドレス管理プログラム（５６０００）の接続制御機能（５６００２）の一部として備える。

【００１６】

図９はネットワーク情報管理部（５６４）の詳細である。本発明における接続制御システムでは、通信プロトコルにＩＰｖ６を想定している。従って、迂回路用のアドレス生成にはネットワークを識別する識別子（５６４０）とネットワーク内で用いられているネットワーク接頭辞（５６４２）が必要である。ＩＰｖ４を用いる場合には、アドレスの生成にはネットワーク接頭辞（５６４２）は必要ない。代わりに、ネットワーク内の端末のアドレスを管理し、未使用のアドレスを迂回路用のアドレスとして用いる必要がある。ＩＰｖ４におけるネットワーク情報管理部（５６４）を図２６に示す。ネットワーク情報管理部（５６４）はネットワーク識別子（５６４０）とアドレス管理データベース（５６４４）を備える。

【００１７】

次に、該システムの動作をシーケンスを用いて詳述する。図１０は接続制御システム（５）の基本シーケンスを示している。また、このシーケンスで用いられるパケットの内容を図１９に示す。前述したように、接続制御システム（５）においてはネットワーク１（１）からネットワーク２（２）、ネットワーク２（２）からネットワーク３（３）、ネットワーク３（３）からネットワーク４（４）、への接続が許可されており、全ての接続が迂回路として使用可能であるものと仮定し、ネットワーク１（１）に属する端末１（１０）がネットワーク２（２）に属する端末２（２０）と通信する場合を考える。通信を始めるにあたり、端末１（１０）はネットワーク１（１）からネットワーク２（２）への接続要求（１０００）をゲートウェイ１（１５）を通じて送信する。以後特別な記述がない限り端末から接続制御装置（５２）への通信はゲートウェイを経由するものとする。接続要求（１０００）の内容を図１９に示す。接続要求（１０００）は送信元ＩＰ（２３００）、宛先ＩＰ（２３０２）、パケット種別（接続要求）（２３０４）、接続元ネットワーク（２３０６）、接続先ネットワーク（２３０８）、ユーザ名（２３１０）を情報として含む。接続要求（１０００）を受信した接続制御装置（５２）は、要求された接続が許可されているかどうかを接続許可データベース（５２４）に問い合わせる。接続許可データベース（５２４）は接続要求（１０００）の接続元ネットワーク（２３０６）とデータベース中の接続元ネットワーク（５２４２）、接続要求（１０００）の接続先ネットワーク（２３０８）とデータベース中の接続先ネットワーク（５２４４）を比較し、要求された接続が許可されているかどうかを判定する。次に接続制御装置（５２）はユーザ状態管理部（５２６）に、該ユーザの認証が完了しているかどうかを問い合わせる。ユーザ状態管理部（５２６）に該ユーザのエントリが存在しない場合には、接続制御装置（５２）は該ユーザのエントリを生成し、端末１（１０）に認証要求（１００３）を送信する。図１９に認証要求（１００３）の内容を示す。認証要求（１００３）は送信元ＩＰ（２７００）、宛先ＩＰ（２７０２）、パケット種別（認証要求）（２７０４）、接続元ネットワーク（２７０６）、接続先ネットワーク（２７０８）、ユーザ名（２７１０）を情報として含む。該ユーザのエントリが存在する場合には、ユーザ状態管理部（５２６）はエントリの認証判定フラグ（５２６８）を調べ、偽の場合には端末１（１０）に認証要求（１００３）

を送信する。端末１（１０）はこれを受け、認証情報（１００６）を接続制御装置（５２）に送信する。認証情報（１００６）の内容を図１９に示す。認証情報（１００６）は送信元ＩＰ（２５００）、宛先ＩＰ（２５０２）、パケット種別（認証情報）（２５０４）、接続元ネットワーク（２５０６）、接続先ネットワーク（２５０８）、ユーザ名（２５１０）、パスワード（２５１２）を含む。認証情報（１００６）を受信した接続制御装置（５２）は、認証装置（５４）に認証依頼（１００９）を送信して認証を依頼する。認証依頼（１００９）の内容を図１９に示す。認証依頼（１００９）はメッセージ種別（認証依頼）（４３００）、接続元ネットワーク（４３０２）、接続先ネットワーク（４３０４）、ユーザ名（４３０６）、パスワード（４３０８）を含む。認証依頼（１００９）中の接続元ネットワーク（４３０２）、接続先ネットワーク（４３０４）、ユーザ名（４３０６）、パスワード（４３０８）の値は、認証情報（１００６）の接続元ネットワーク（２５０６）、接続先ネットワーク（２５０８）、ユーザ名（２５１０）、パスワード（２５１２）から取得する。認証依頼（１００９）を受信した認証装置（５４）は、認証の成否を認証データベース（５４２）に問い合わせる。認証装置（５４）は認証依頼（１００９）中の接続元ネットワーク（４３０２）、接続先ネットワーク（４３０４）、ユーザ名（４３０６）を用いて認証データベース（５４２）から対応するデータレコードを検索し、認証依頼（１００９）中のパスワード（４３０８）とデータレコード中のパスワード（５４２６）を比較する。パスワードが一致する場合には認証の完了を接続制御装置（５２）に通知する。これは認証完了（１０１２）を送信することで行われる。認証完了（１０１２）を受けた接続制御装置（５２）は、認証完了通知（１０１５）を端末１（１０）に送信する。この時点で認証が完了するため、接続制御装置（５２）はユーザ状態管理部（５２６）の認証要求（１００３）を送信したユーザの認証判定フラグ（５２６８）を真に、迂回路判定フラグ（５２６６）を偽に設定する。認証が完了した後に、接続制御装置（５２）はゲートウェイ１（１５）に認証が完了したユーザのアドレス登録（１０１６）を行う。アドレス登録（１０１６）の内容を図１９に示す。アドレス登録（１０１６）は送信元ＩＰ（５０００）、宛先ＩＰ（５００２）、パケット種別（アドレス登録）（５００４）、実アドレス（５００６）を含む。ゲートウェイ１（１５）は実アドレス（５００６）をアドレス登録テーブル（１２０）に登録する。

【００１８】

ユーザ状態管理部（５２６）内のユーザ状態を更新した後、接続制御装置（５２）は接続許可通知（１０１８）を端末１（１０）に送信する。図１９に接続許可通知（１０１８）の内容を示す。接続許可通知（１０１８）は送信元ＩＰ（３３００）、宛先ＩＰ（３３０２）、パケット種別（接続許可通知）（３３０４）、接続元ネットワーク（３３０６）、接続先ネットワーク（３３０８）、ユーザ名（３３１０）を情報として含む。接続許可通知（１０１８）を受信した端末１（１０）はこの時点で端末２（２０）との通信が可能になり、ゲートウェイ１（１５）、ゲートウェイ２（２５）を経由して端末２との通信を開始する（１０２１）。

端末１（１０）は通信を終了する際に接続制御装置（５２）に対して接続終了（１０２４）を送信する。接続終了（１０２４）を受信した接続制御装置（５２）は、ユーザ状態管理部（５２６）の該接続終了（１０２４）を送信したユーザに対応するエントリを削除し、端末１（１０）に接続終了確認（１０２７）を送信する。最後に接続管理装置（５２）はゲートウェイ１（１５）にアドレス削除（１０３０）を送信する。アドレス削除（１０３０）の内容を図１９に示す。アドレス削除（１０３０）は送信元ＩＰ（５１００）、宛先ＩＰ（５１０２）、パケット種別（アドレス削除）（５１０４）、実アドレス（５１０６）を含む。ゲートウェイ１（１５）は実アドレス（５１０６）をアドレス登録テーブル（１２０）から削除する。以後端末１（１０）が接続制御装置（５２）を経由して端末２（２０）と通信するには、再度接続要求（１０００）を送信して認証を経なければならない。以上で通常の接続処理が完了する。

【００１９】

次に、接続許可のないネットワーク間の通信について考える。図１２はネットワーク１

（１）からネットワーク３（３）への通信を要求した場合の処理である。図１においてネットワーク２（２）に属していた端末２（２０）がネットワーク１（１）に移動して（９）端末１（１０）となり、ネットワーク３（３）に属する端末３（３０）と通信する場合がこれに相当する。

【００２０】

本発明におけるシステムでは迂回路を用いた通信を行うことで、接続許可のないネットワーク間では接続できないという問題を解決する。迂回路は接続許可がないネットワーク間の通信を実現するための通信経路である。図１において、ネットワーク１（１）からネットワーク３（３）への接続許可は存在しないが、ネットワーク１（１）からネットワーク２（２）、ネットワーク２（２）からネットワーク３（３）への接続許可は存在する。そこで、ネットワーク（１）からネットワーク（３）への通信を、ネットワーク２（２）を経由する迂回路を経ることで実現する。この時、接続許可を満たすアドレスを端末が持つことが必要となる。端末１がネットワーク１（１）からネットワーク２（２）を経由してネットワーク３（３）に属する端末３（３０）と通信するには、ネットワーク２（２）からネットワーク（３）へ通信する必要があるが、接続許可を満たすためには端末１（１０）がネットワーク２（２）におけるアドレスを持つ必要がある。ところが端末１（１０）の持つアドレスはネットワーク（１）に属するため、そのままではネットワーク２（２）からネットワーク３（３）へ通信できない。そこで、アドレス管理装置（５６）は端末１（１０）に迂回路アドレスとしてネットワーク２（２）でのアドレスを付与する。ネットワーク２（２）における通信用のアドレスを端末に割り当てることで、ネットワーク２（２）を経由した、すなわち迂回路を用いた通信が可能になる。

【００２１】

図１１に迂回路を用いた通信シーケンスを示す。また、このシーケンスで用いられるパケットの内容を図２０、図２１に示す。端末１（１０）は接続制御装置（５２）に接続要求（１２００）を送信する。接続要求（１２００）を受信した接続制御装置（５２）は、要求された接続が許可されているかどうかを接続許可データベース（５２４）に問い合わせる。ネットワーク１（１）からネットワーク３（３）への通信は許可されていないため、接続制御装置（５２）は接続不許可通知（１２０３）を端末１（１０）に送信する。接続不許可通知（１２０３）の内容を図２０に示す。接続不許可通知（１２０３）は送信元ＩＰ（３５００）、宛先ＩＰ（３５０２）、パケット種別（接続許可通知）（３５０４）、接続元ネットワーク（３５０６）、接続先ネットワーク（３５０８）、ユーザ名（３５１０）を情報として含む。接続不許可通知（１２０３）を受信した端末（１０）はネットワーク１（１）からネットワーク３（３）へ直接接続できないことを知り、接続制御装置（５２）に迂回路による接続を要求するため、迂回路接続要求（１２０６）を送信する。迂回路接続要求の内容を図２０に示す。迂回路接続要求（１２０６）は送信元ＩＰ（２４００）、宛先ＩＰ（２４０２）、パケット種別（迂回路接続要求）（２４０４）、接続元ネットワーク（２４０６）、接続先ネットワーク（２４０８）、ユーザ名（２４１０）を情報として含む。この例では接続元ネットワーク（２４０６）にネットワーク１（１）、接続先ネットワークにネットワーク３（３）を指定する。迂回路接続要求（１２０６）を受信した接続制御装置（５２）は要求された迂回路が存在するかどうかを接続許可データベース（５２４）に問い合わせる。接続許可データベース（５２４）は迂回路接続要求（１２００）の接続元ネットワーク（２４０６）と接続先ネットワーク（２４０８）　を用いて迂回路を検索する。接続許可データベース（５２４）は、接続元ネットワークから接続先ネットワークを結ぶ経路が、自身が管理する接続許可のあるネットワークの連結で構築できる場合に迂回可能と判断する。ネットワークの連結とは、ある接続許可１の接続先ネットワークと別の接続許可２の接続元ネットワークが一致する場合に、接続許可１の接続元ネットワークを接続元ネットワークに、接続許可２の接続先ネットワークを接続先ネットワークにした新しい接続許可３を生成することを指す。例えば、ネットワーク１（１）からネットワーク３（３）については、接続許可データベース中の接続許可のうちネットワーク１（１）からネットワーク２（２）、ネットワーク２（２）からネットワーク３

（３）という経路が存在し、ネットワークの連結による迂回が可能である。可能と判断したら、接続制御装置（５２）はユーザ状態管理部（５２６）に、迂回路接続要求（１２０６）を送信したユーザの認証が完了しているかどうかを問い合わせる。この時点ではユーザ状態管理部（５２６）には該ユーザのエントリはまだ生成されていないので、接続制御装置（５２）は該ユーザのエントリを生成し、端末１（１０）に迂回路認証要求（１２０９）を送信する。図２０に迂回路認証要求（１２０９）の内容を示す。迂回路認証要求（１２０９）　は送信元ＩＰ（２８００）、宛先ＩＰ（２８０２）、パケット種別（迂回路認証要求）　（２８０４）、接続元ネットワーク（２８０６）、経由ネットワーク１（２８０８）、経由ネットワークＮ（２８１０）、接続先ネットワーク（２８１２）、ユーザ名（２８１４）を情報として含む。ＮはＮ番目の経由ネットワークを表わす。この例ではネットワーク２（２）を経由するので、接続元ネットワーク（２８０６）にネットワーク１（１）、経由ネットワーク１（２８０８）にネットワーク２（２）、接続先ネットワーク（２８１２）にネットワーク３（３）を指定する。ネットワークの指定には各ネットワークが識別できる情報を用いる。例えば各ネットワークに属するゲートウェイのアドレスや、アドレス管理装置（５６）のネットワーク情報管理部（５６４）が持つネットワーク識別子（５６４０）等がこれに相当する。迂回路認証要求（１２０９）を受信した端末１（１０）は迂回路認証情報（１２１２）を接続制御装置（５２）に送信する。迂回路認証情報（１２１２）は経由する全ての迂回路に必要な認証情報を含む必要がある。迂回路認証情報（１２１２）の内容を図２０に示す。迂回路認証情報（１２１２）は送信元ＩＰ（２６００）、宛先ＩＰ（２６０２）、パケット種別（迂回路認証情報）　（２６０４）、接続元ネットワーク（２６０６）、経由ネットワーク１（２６０８）、経由ネットワークＮ（２６１０）、接続先ネットワーク（２６１２）、ユーザ名（２６１４）、パスワード１（２６１６）、パスワードＮ＋１（２６１８）を含む。パスワードＩは経由ネットワークＩ－１から経由ネットワークＩへ接続する際に必要なパスワードを表す。経由ネットワーク０は接続元ネットワーク（２６０８）、経由ネットワークＮ＋１は接続先ネットワーク（２６１０）に対応する。迂回路認証情報（１２１２）を受信した接続制御装置（５２）は、認証装置（５４）に迂回路認証依頼（１２１５）を送信して認証を依頼する。迂回路認証依頼（１２１５）の内容を図２０に示す。迂回路認証依頼（１２１５）　はメッセージ種別（迂回路認証依頼）（４４００）、接続元ネットワーク（４４０２）、経由ネットワーク１（４４０４）、経由ネットワークＮ（４４０６）、接続先ネットワーク（４４０８）、ユーザ名（４４１０）、パスワード１（４４１２）、パスワードＮ＋１（４４１４）を含む。経由ネットワークとパスワードの添字の関係は迂回路認証情報（１２１２）と同様である。迂回路認証依頼（１２１５）を受信した認証装置（５４）は、認証の成否を認証データベース（５４２）に問い合わせる。認証装置（５４）は迂回路認証依頼（１２１５）中の全てのパスワードに対して経由ネットワークＩ－１、経由ネットワークＩ、ユーザ名（４４１０）、パスワードＩを、認証データベース（５４２）の接続元ネットワーク（５４２２）、接続先ネットワーク（５４２４）、ユーザ名（５４２０）、パスワード（５４２６）とそれぞれ比較し、全てのパスワードに対してデータレコードが存在する場合に認証の完了を接続制御装置（５２）に通知する。これは迂回路認証完了（１２１８）を送信することで行われる。迂回路認証完了（１２１８）の内容を図２０に示す。迂回路認証完了（１２１８）はメッセージ種別（迂回路認証完了）（３９００）、接続元ネットワーク（３９０２）、経由ネットワーク１（３９０４）、経由ネットワークＮ（３９０６）、接続先ネットワーク（３９０８）、ユーザ名（３９１０）を情報として含む。迂回路認証完了（１２１８）を受けた接続制御装置（５２）は、迂回路認証完了通知（１２２１）を端末１（１０）に送信する。迂回路認証完了通知（１２２１）の内容を図２１に示す。迂回路認証完了通知（１２２１）は送信元ＩＰ（３０００）、宛先ＩＰ（３００２）、パケット種別（迂回路認証完了通知）　（３００４）、接続元ネットワーク（３００６）、経由ネットワーク１（３００８）、経由ネットワークＮ（３０１０）、接続先ネットワーク（３０１２）、ユーザ名（３０１４）を情報として含む。この時点で認証が完了するため、接続制御装置（５２）はユーザ状態管理部（５２６）の該ユーザの認証判定フラ

グ（５２６８）と迂回路判定フラグ（５２６６）を真に設定する。先述したように、迂回路接続の際にはそれぞれの経由ネットワークに対して端末の迂回路アドレスを生成する必要がある。接続制御装置（５２）は迂回路アドレスの生成をアドレス管理装置（５６）に依頼する。この処理はアドレス生成依頼（１２２４）をアドレス管理装置（５６）に送信することで行う。アドレス生成依頼（１２２４）の内容を図２１に示す。アドレス生成依頼（１２２４）はメッセージ種別（アドレス生成依頼）（４５００）、端末ＭＡＣアドレス（４５０２）、経由ネットワーク１（４５０４）、経由ネットワークＮ（４５０６）を情報として含む。端末のＭＡＣアドレスは、ユーザ状態管理部（５２６）の端末アドレス（５２６１）から抽出可能であり、アドレス生成を依頼する際にアドレス管理装置（５６）にこれを送信する。アドレス生成依頼（１２２４）を受信したアドレス管理装置（５６）はアドレス生成処理を行う。アドレスの生成は受信したアドレス生成依頼（１２２４）中の端末ＭＡＣアドレス（４５０２）と、経由ネットワークＩのゲートウェイのアドレスから検出したネットワークプレフィックスネットワーク接頭辞（５６４２）を用いて行う。ＩＰｖ４の場合はアドレス管理データベース（５６４４）を検索して未使用のアドレスを生成アドレスとして用いる。アドレス管理装置（５６）は生成したアドレスをアドレス生成完了（１２２７）を用いて接続制御装置（５２）に通知する。アドレス生成完了（１２２７）の内容を図２１に示す。アドレス生成完了（１２２７）はメッセージ種別（アドレス生成完了）（４２００）、端末ＭＡＣアドレス（４２０２）、生成アドレス１（４２０４）、生成アドレスＮ（４２０６）を情報として含む。生成アドレスＩはアドレス生成依頼（１２２４）の経由ネットワークＩに対応したアドレスである。アドレス生成完了（１２２７）を受信した接続制御装置（５２）はアドレスをユーザ状態管理部（５２６）の迂回路アドレスに登録する。ここではネットワーク２（２）用の迂回路アドレスを迂回路アドレス１（５２７０）として登録する。次に、アドレス生成通知（１２３０）を端末１（１０）に送信して生成したアドレスを通知する。アドレス生成通知（１２３０）の内容を図２１に示す。アドレス生成通知（１２３０）は送信元ＩＰ（３７００）、宛先ＩＰ（３７０２）、パケット種別（アドレス生成通知）（３７０４）、端末アドレス（３７０６）、生成アドレス１（３７０８）、生成アドレスＮ（３７１０）を情報として含む。端末１（１０）はネットワーク２（２）用のアドレスを受信し、以降の通信に用いる。この処理については後述する。端末１（１０）へのアドレスの通知を終えた接続制御装置（５２）は、迂回路接続を可能にするために通信路上に存在するゲートウェイに対してアドレスの登録を行う。通信路に存在するゲートウェイにはゲートウェイ１（１５）、ゲートウェイ２（２５）、ゲートウェイ３（３５）があるが、ここではゲートウェイ１（１５）に接続許可のために必要なアドレスの登録、ゲートウェイ２（２５）に迂回路通信のために必要なアドレスの登録をそれぞれ行う。接続制御装置（５２）はゲートウェイ１（１５）にアドレス登録（１２３１）を送信する。ここで登録するアドレスは端末１（１０）のアドレスであり、これはユーザ状態管理部（５２６）の端末アドレス（５２６１）に格納されている。次に接続制御装置（５２）は迂回路アドレス登録（１２３２）をゲートウェイ２（２５）に送信する。図２１に迂回路アドレス登録（１２３２）の内容を示す。迂回路アドレス登録（１２３２）は送信元ＩＰ（５２００）、宛先ＩＰ（５２０２）、パケット種別（迂回路アドレス登録）（５２０４）、迂回路アドレス（５２０６）、実アドレス（５２０８）を情報として含む。迂回路アドレス（５２０６）は接続先ネットワークに存在する端末が迂回路ネットワークに後続のパケットを送信するために必要なアドレスであり、この例ではネットワーク２（２）に対して生成したアドレスが該当する。実アドレス（５２０８）は経由ネットワークに存在するゲートウェイが後続のパケットを転送するために必要なアドレスであり、一つ前の経由ネットワークに対して生成したアドレスが該当する。つまり、ネットワークＩを経由する場合、迂回路アドレスにはネットワークＩに対して生成したアドレス、実アドレスにはネットワークＩ－１に対して生成したアドレスが該当する。なお、ネットワーク１は端末が属するネットワークである。ここでは迂回路アドレス（５２０６）にネットワーク２（２）用のアドレスを指定する。これはユーザ状態管理部（５２６）の迂回路アドレス１（５２７０）に格納されている。実アドレス（５２０８

）
には端末１（１０）のアドレスを指定する。これはユーザ状態管理部（５２６）の端末アドレス（５２６１）に格納されている。必要なアドレスの登録を終えた接続制御装置（５２）は、端末１（１０）に迂回路接続許可通知（１２３３）を送信する。迂回路接続許可通知（１２３３）の内容を図２１に示す。迂回路接続許可通知（１２３３）は送信元ＩＰ（３４００）、宛先ＩＰ（３４０２）、パケット種別（迂回路接続許可通知）（３４０４）、接続元ネットワーク（３４０６）、経由ネットワーク１（３４０８）、経由ネットワークＮ（３４１０）、接続先ネットワーク（３４１２）、ユーザ名（３４１４）を情報として含む。迂回路接続許可通知（１２３３）を受信した端末はゲートウェイ１（１５）、ゲートウェイ２（２５）、ゲートウェイ３（３５）を経由して端末３（３０）との通信を行う（１２３６）。

【００２２】

端末１（１０）は通信を終了する際に接続制御装置（５２）に対して接続終了（１２３９）を送信する。接続終了（１２３９）を受信した接続制御装置（５２）は、ユーザ状態管理部（５２６）の該接続終了（１２３９）を送信したユーザに対応するエントリを削除し、端末１（１０）に接続終了確認（１２４２）を送信する。最後に接続管理装置（５２）はゲートウェイに登録したアドレスを削除するために、ゲートウェイ１（１５）にアドレス削除（１２４５）を送信する。アドレス削除（１２４５）の内容は、図１９に示したアドレス削除（１０３０）の内容と同様である。ゲートウェイ１（１５）は実アドレス（５１０６）をアドレス登録テーブル（１２０）から削除し、以後端末１（１０）が接続制御装置（５２）を経由して端末３（３０）と迂回路接続による通信をするには、再度迂回路接続要求（１２０６）を送信して認証を経なければならない。次に接続制御装置（５２）はゲートウェイ２（２５）に迂回路アドレス削除（１２４８）を送信する。迂回路アドレス削除（１２４８）の内容を図２１に示す。迂回路アドレス削除（１２４８）は送信元ＩＰ（５３００）、宛先ＩＰ（５３０２）、パケット種別（迂回路アドレス削除）（５３０４）、迂回路アドレス（５３０６）、実アドレス（５３０８）を情報として含む。以上で迂回路接続処理が完了する。

【００２３】

次に、各機能ブロックの動作をフローチャートを用いて詳述する。
図１２は接続制御装置（５２）のフローチャートである。接続制御装置（５２）はシステム起動時に処理を開始して（１３００）メッセージ／パケット受信ループに入る（１３０１）。受信したメッセージが接続要求（１０００）の場合（１３０２）、接続制御装置（５２）は接続処理（１３２４）を行う。接続処理（１３２４）については後述する。受信したメッセージが迂回路接続要求（１２０６）の場合（１３０４）、接続制御装置（５２）は迂回路接続処理（１３２６）を行う。迂回路接続処理（１３２６）については後述する。認証情報（１００６）を受信した場合（１３０６）、接続制御装置（５２）は認証装置（５４）に認証を依頼する（１３２８）。迂回路認証情報（１２１２）を受信した場合（１３０８）、接続制御装置（５２）は認証装置（５４）に迂回路認証を依頼する（１３３０）。認証失敗を受信した場合（１３１０）、接続制御装置（５２）は端末に認証失敗を通知する（１３３２）。認証失敗は認証装置（５４）が認証に失敗したことを接続制御装置（５２）に通知するメッセージである。迂回路認証失敗を受信した場合（１３１２）、接続制御装置（５２）は端末に迂回路認証失敗を通知する（１３３４）。迂回路認証失敗は認証装置（５４）が迂回路認証に失敗したことを接続制御装置（５２）に通知するメッセージである。迂回路認証失敗の内容を図２２に示す。迂回路認証失敗はメッセージ種別（迂回路認証失敗）（４１００）、接続元ネットワーク（４１０２）、経由ネットワーク１（４１０４）、経由ネットワークＮ（４１０６）、接続先ネットワーク（４１０８）、ユーザ名（４１１０）を情報として含む。接続制御装置は端末に迂回路認証失敗通知を送信する。迂回路認証失敗通知の内容を図２２に示す。迂回路認証失敗通知は送信元ＩＰ（３２００）、宛先ＩＰ（３２０２）、パケット種別（迂回路認証失敗通知）（３２０４）、接続元ネットワーク（３２０６）、経由ネットワーク１（３２０８）、経由ネットワ

ークＮ（３２１０）、接続先ネットワーク（３２１２）、ユーザ名（３２１４）を情報として含む。認証完了（１０１２）を受信した場合（１３１４）、接続制御装置（５２）は認証完了通知（１０１５）を端末に送信して認証完了を通知し（１３３６）、ゲートウェイにアドレス登録（１０３０）を送信してアドレス登録テーブル（１２０）に端末のアドレスを登録し（１３３８）、接続許可通知（１０１８）を端末に送信して通信を開始させる（１３４０）。迂回路認証完了（１２１８）を受信した場合（１３１６）、接続制御装置（５２）は迂回路認証完了通知（１２２１）を端末に送信して迂回路認証完了を通知し（１３４２）、アドレス管理装置にアドレス生成依頼（１２２４）を送信してアドレスの生成を依頼する（１３４４）。アドレス生成完了（１２２７）を受信した場合（１３１８）、接続制御装置（５２）はアドレス生成通知（１２３０）を端末に送信し（１３４６）、端末のアドレスと生成した迂回路アドレスをアドレス登録（１２３１）、迂回路アドレス登録（１２３２）によりゲートウェイに登録し（１３４８）、迂回路接続許可通知（１２３３）を端末に送信する（１３５０）。端末から接続終了（１２３９）を受信した場合（１３２０）、接続制御装置（５２）は接続終了確認（１２４２）を端末に送信し（１３５２）、アドレス削除（１２４５）、迂回路アドレス削除（１２４８）によりゲートウェイから該当するアドレスを削除する（１３５４）。パケット／メッセージ受信ループはシステム停止時に停止して（１３２２）、接続制御装置（５２）は終了する（１３９９）。

【００２４】

次に接続処理の様子を図１３に示す。接続処理が開始すると（１４００）、最初に要求された接続が許可されているかどうかを把握するために、接続許可データベース（５２４）を検索する（１４０２）。対応するデータレコードが接続許可データベース（５２４）に存在しなければ、接続制御装置（５２）は接続不許可通知（１２０３）を端末に送信して（１４２０）接続処理を終了する（１４９９）。データレコードが存在する場合はユーザ状態管理部（５２６）を検索して認証が完了しているかどうかを調べる（１４０４）。認証が完了していない場合は認証要求（１００３）を端末に送信して（１４２２）接続処理を終了する（１４９９）。認証が完了している場合は接続許可通知（１０１８）を送信して（１４０６）接続処理を終了する（１４９９）。

【００２５】

次に迂回路接続処理の様子を図１４に示す。迂回路接続処理が開始すると（１５００）、最初に要求された迂回路が存在するかどうかを把握するために、接続許可データベース（５２４）を検索する（１５０２）。迂回路が接続許可データベース（５２４）から算出できない場合、接続制御装置（５２）は迂回路接続不許可通知を端末に送信して（１５２０）接続処理を終了する（１５９９）。迂回路接続不許可通知の内容を図２２に示す。迂回路接続不許可通知は送信元ＩＰ（３６００）、宛先ＩＰ（３６０２）、パケット種別（迂回路接続許可通知）（３６０４）、接続元ネットワーク（３６０６）、接続先ネットワーク（３６０８）、ユーザ名（３６１０）を情報として含む。迂回路が存在する場合はユーザ状態管理部（５２６）を検索して認証が完了しているかどうかを調べる（１５０４）。認証が完了していない場合は迂回路認証要求（１２０９）を端末に送信して（１５２２）接続処理を終了する（１５９９）。認証が完了している場合はアドレスが生成済であるかどうかをユーザ状態管理部（５２６）に問い合わせる。アドレス生成判定は迂回路判定フラグ（５２６６）が真の場合に迂回路アドレス１（５２７０）が存在するかどうかによって行う。アドレスが未生成の場合、接続制御装置（５２）はアドレス管理装置（５６）にアドレス生成依頼（１２２４）を送信する（１５２４）。アドレスが生成済の場合は端末にアドレス生成通知（１２３０）を送信してアドレスの通知を行い（１５０８）、迂回路接続許可通知（１２３３）を送信して（１５１０）迂回路接続処理を終了する（１５９９）。

【００２６】

図１５は認証装置（５４）のフローチャートである。認証装置（５４）はシステム起動時に処理を開始して（１６００）メッセージ受信ループに入る（１６０１）。受信したメッセージが認証依頼（１００９）の場合（１６０２）、認証装置（５４）は認証処理を行

う（１６２０）。認証処理については後述する。受信したメッセージが迂回路認証依頼（１２１５）の場合（１６０４）、認証装置（５４）は迂回路認証処理を行う（１６２２）。メッセージ受信ループはシステム停止時に停止して（１６０６）、認証装置は終了する（１６９９）。

【００２７】

次に認証処理の様子を図１６に示す。認証処理が開始すると（１７００）、最初に認証情報中のユーザ名が認証データベース（５４２）に存在するか検索する（１７０２）。ユーザ名が存在しない場合、認証装置（５４）は認証失敗を接続制御装置（５２）に送信して（１７２０）処理を終了する（１７９９）。ユーザ名が存在する場合はパスワードが正当かどうかを検索する（１７０４）。パスワードが不正な場合は認証装置（５４）は認証失敗を接続制御装置（５２）に送信して（１７２２）処理を終了する（１７９９）。パスワードが正当な場合は認証装置（５４）は認証完了（１０１２）を接続制御装置（５２）に送信して（１７０６）処理を終了する（１７９９）。

【００２８】

次に迂回路認証処理の様子を図１７に示す。迂回路認証処理が開始すると（１８００）、最初に認証情報中のユーザ名が認証データベース（５４２）に存在するか検索する（１８０２）。ユーザ名が存在しない場合、認証装置（５４）は迂回路認証失敗を接続制御装置（５２）に送信して（１８２０）処理を終了する（１８９９）。ユーザ名が存在する場合はパスワードが正当かどうかを検索する（１８０４）。迂回路認証に必要な全てのパスワードが正当な場合にのみパスワードが正当であるとみなす。パスワードが不正な場合は認証装置（５４）は迂回路認証失敗を接続制御装置（５２）に送信して（１８２２）処理を終了する（１８９９）。パスワードが正当な場合は認証装置（５４）は迂回路認証完了（１２１８）を接続制御装置（５２）に送信して（１８０６）処理を終了する（１８９９）。

【００２９】

図１８はアドレス管理装置（５６）のフローチャートである。アドレス管理装置（５６）はシステム起動時に処理を開始して（１９００）メッセージ受信ループに入る（１９０１）。アドレス管理装置はアドレス生成依頼（１２２４）を受信すると（１９０２）、メッセージ中の端末ＭＡＣアドレス（４５０２）、経由ネットワーク１（４５０４）、経由ネットワークＮ（４５０６）から迂回路接続用のアドレスを生成し（１９０４）、アドレス生成完了（１２２７）を接続制御装置（５２）に送信する（１９０６）。メッセージ受信ループはシステム停止時に停止して（１９０８）、アドレス管理装置は終了する（１９９９）。

【００３０】

次に、端末１（１０）が端末３（３０）に対して通信を行う際のパケット処理について説明する。図２７は端末１（１０）が端末３（３０）に通信する際のシーケンスである。図１１において端末１（１０）がアドレス生成通知（１２３０）を受信した時点で、端末１（１０）は迂回路ネットワーク１であるネットワーク２（２）用のアドレスを保持する。端末１（１０）が最初に保持するアドレスをＨｏｓｔ１と記述し、ネットワーク２（２）用の迂回路アドレスをＨｏｓｔ１－２と記述する。アドレス登録（１２３１）をゲートウェイ１（１５）が受信すると、ゲートウェイ１（１５）のアドレス登録テーブル（１２０）にはＨｏｓｔ１が登録され、端末１（１０）がゲートウェイ１（１５）経由で通信することが可能になる。ゲートウェイ２（２５）が迂回路アドレス登録（１２３２）を受信すると、ゲートウェイ２（２５）の迂回路アドレス登録テーブル（１３０）には迂回路アドレス（１３０１０）として　Ｈｏｓｔ１－２、実アドレス（１３０２０）としてＨｏｓｔ１が登録される。これらの情報は迂回路接続において、端末３から端末１へのパケットを送信する際に必要となる。端末１（１０）が迂回路接続許可通知（１２３３）を受信すると、端末１（１０）は通信がゲートウェイ１、２、３を経由して送信されることを知る。端末１（１０）は端末３（３０）へパケットを以下の手順で送信する。端末１（１０）は最初にゲートウェイ１（１５）にパケット（５４９８）を送信する（５４９９）。端末

１（１０）がゲートウェイ１（１５）に送信するパケット（５４９８）はパケットの真の始点（５４０８）、真の終点（５４１０）、トンネル通信の始点（５４００）、トンネル通信の終点（５４０２）、迂回ヘッダ１（５４０４）、迂回ヘッダ２（５４０６）とペイロード（５４１２）を含む。端末１（１０）から端末３（３０）への通信は最初にゲートウェイ１（１５）を経由するので、トンネル通信の始点にＨｏｓｔ１（５４５０）、終点にＧＷ１（５４５２）を指定する。ＧＷ１はゲートウェイ１（１５）のアドレスであり、これは迂回路接続許可通知（１２３３）の接続元ネットワーク（３４０６）に含まれている。接続許可を満たすために、パケットはゲートウェイ２（２５）、ゲートウェイ３（３５）を経由しなければならない。これを実現するため、端末１（１０）はパケット中に２つの迂回ヘッダを挿入する。迂回ヘッダは送信元と送信先を対にして指定する。ここではゲートウェイ１（１５）からゲートウェイ２（２５）への迂回ヘッダ（５４５４）、ゲートウェイ２（２５）からゲートウェイ３（３５）への迂回ヘッダ（５４５６）をそれぞれ指定する。パケットの真の終点には端末３（３０）のアドレスである　Ｈｏｓｔ３を指定するが、ここで問題となるのは真の始点である。端末３がパケットを受信した時、パケットを返信する際にはネットワーク３（３）から接続許可のあるネットワークに対してのみ返信が可能である。そこで、真の始点にはネットワーク２用の迂回アドレスＨｏｓｔ１－２を指定する。迂回アドレスは終点に対して必ず接続許可があるように算出されているため、真の始点に迂回アドレスを指定することで端末３（３０）からのパケット返送が可能になる。ペイロード（５４１２）には端末３（３０）へ送信したいデータ（５４６２）を含める。端末１からのパケット（５４９８）を受信したゲートウェイ１（１５）は以下の手順でパケットを処理する。トンネル通信の始点（５４００）と終点（５４０２）から、トンネル通信の終点が自分自身であることを把握してこれらを取り除く。次にゲートウェイ１（１５）は迂回ヘッダの検索を行う。端末１（１０）がゲートウェイ１（１５）に送信したパケット（５４９８）にはゲートウェイ１（１５）からゲートウェイ２（２５）への迂回を要求する迂回ヘッダ１（５４０４）が存在するので、トンネル通信の始点をＧＷ１に（５５５０）、終点をＧＷ２に指定し（５５５２）、迂回ヘッダを一つ取り除いてゲートウェイ２からゲートウェイ３への迂回ヘッダのみを指定する（５５５４）。真の始点（５５０６）、真の終点（５５０８）、ペイロード（５５１０）は元のパケットのデータをそのままコピーする（５５５６、５５５８、５５６０）。以上の処理を経てゲートウェイ１（１５）はゲートウェイ２（２５）にパケット（５５９８）を送信する（５５９９）。このパケットを受信したゲートウェイ２（２５）はゲートウェイ１（１５）と同様の処理を行い、ゲートウェイ３（３５）にパケット（５６９８））を送信する（５６９９）。トンネル通信の始点はＧＷ２（５６５０）、終点はＧＷ３（５６５２）、真の始点はＨｏｓｔ１－２（５６５４）、真の終点はＨｏｓｔ３（５６５６）である。ペイロード（５６５８）は変化しない。このパケットを受信したゲートウェイ３（３５）はパケットを解析し、迂回ヘッダが存在しないことを知る。従って、ゲートウェイ３（３５）はゲートウェイ２（２５）から受信したパケットをトンネル化せずに通常の通信として処理する。パケットの真の終点はＨｏｓｔ３であるため、ゲートウェイ３（３５）は図２６に示すパケットを構築する。パケットの始点はＨｏｓｔ１－２（５７５０）、終点はＨｏｓｔ３（５７５２）である。ペイロード（５７５４）は変化しない。このようにして構築したパケット（５７９８）が端末３（３０）に到達する（５７９９）。

次に端末３（３０）から端末１（１０）へのパケットの返送について説明する。端末３が把握しているパケットの送信元は、ゲートウェイ３（３５）から受信したパケット（５７９８）の始点（５７００）で指定されたＨｏｓｔ１－２（５７５０）である。この情報を元にして端末３（３０）は端末１（１０）へのパケット（５８９８）を構築する。端末３（３０）はパケットを真の始点をＨｏｓｔ３（５８５４）、真の終点をＨｏｓｔ１－２（５８５６）に設定し、トンネルの始点をＨｏｓｔ３（５８５０）、トンネルの終点をＧＷ３（５８５２）に設定する。このパケットを受信したゲートウェイ３（３５）は（５８９９）、パケットの真の終点がＨｏｓｔ１－２であることから、ゲートウェイ１（１５）に送信する（５９９９）パケット（５９９８）パケットを構築する。真の始点（５９０４）

、真の終点（５９０６）、ペイロード（５９０８）は変化しない。トンネルの始点はＧＷ３（５９５０）、トンネルの終点はＧＷ２（５９５２）に設定される。このパケットを受信したゲートウェイ２（２５）はネットワーク２（２）の中でパケットの転送先を検索するが、Ｈｏｓｔ１－２は端末１（１０）がネットワーク２（２）内で用いる仮想的なアドレスのため、パケットの転送先は存在しない。そこでゲートウェイ２（２５）は迂回路アドレス登録テーブル（１３０）を検索し、該当する迂回路が存在しないかどうか調べる。ゲートウェイ２（２５）の迂回路アドレス登録テーブル（１３０）には迂回路アドレス（１３０１０）としてＨｏｓｔ１－２、実アドレス（１３０２０）としてＨｏｓｔ１が登録されているので、ゲートウェイ２（２５）はパケットをゲートウェイ１（１５）に送信する。以上の情報を元にゲートウェイ２（２５）はパケット（６０９８）をゲートウェイ１（１５）に送信する（６０９９）。トンネルの始点（６０５０）はＧＷ２、トンネルの終点はＧＷ１（６０５２）に設定される。真の始点はＨｏｓｔ３のまま変化しない（６０５４）が、真の終点は迂回路アドレス登録テーブル（１３０）から抽出した実アドレス（１３０２０）であるＨｏｓｔ１に変化する（６０５６）。ゲートウェイ２（２５）からのパケット（６０９８）を受信したゲートウェイ１（１５）はパケットの終点がＨｏｓｔ１であることを知り、パケット（６１９８）を構築して端末１（１０）に送信する（６１９９）。このパケットは始点がＨｏｓｔ３（６１５０）、終点がＨｏｓｔ１（６１５２）に設定されている。以上の処理を経て端末３（３０）から端末１（１０）にパケットが返送される。

【００３１】

次に、接続制御システムを一つの接続管理装置（６）として実現した場合の構成を図２３に示す。接続管理装置（６）はネットワークインターフェース（５００００）とバス（５０００６）、メモリ（５０００８）を最低限備える。接続管理装置（６）の構成については図２５で詳述する。接続管理装置（６）はメモリ（５０００８）上で動作する接続管理プログラム（６００００）の機能として接続制御機能（６００００２）、認証機能（６００００４）、アドレス管理機能（６００００６）を備える。各機能は接続制御装置（５２）、認証装置（５４）、アドレス管理装置（５６）と同等の機能を提供し、処理シーケンスは図１０、図１１と同様である。

次に、図２４を用いてシステムのハードウェア構成を示す。図１で示したように、接続制御システム（５）は接続制御装置（５２）、認証装置（５４）とアドレス管理装置（５６）から成る。これらの装置はそれぞれネットワークインターフェース（５００００）を備え、ＬＡＮ（５００１０）によって相互に通信を行う。各装置はそのほかにＣＰＵ（５０００２）、ハードディスク（５００００４）、メモリ（５０００８）を備え、これらは装置内のバス（５０００６）によって相互にデータを送受信する。各装置のメモリ（５０００００８）にはそれぞれの装置の機能を実現するプログラムが格納されている。接続制御装置（５２）のメモリ（５０００８）上では接続制御プログラム（５２０００）が動作、このプログラムは接続制御機能（５２００２）を備える。同様に、認証装置（５４）のメモリ（５０００８）上では認証機能（５４００２）を備えた認証プログラム（５４０００）が、アドレス管理装置（５６）のメモリ（５０００８）上ではアドレス管理機能（５６０００２）を備えたアドレス管理プログラム（５６０００）が動作する。これらの装置の実現形態としては、各装置に個別のコンピュータを割り当てるほかに、ブレードサーバのように複数のコンピュータを単一の筐体として扱える形で実現することもできる。また、単一のコンピュータに全ての機能を実装することも可能である。図２５に単一のハードウェアでの接続管理装置（６）の実装を示す。接続管理装置（６）は図２４の各装置と同様にネットワークインターフェース（５００００）を備え、ＬＡＮ（５００１０）によって外部の端末、ゲートウェイと相互に通信を行う。接続管理装置（６）はさらにＣＰＵ（５０００２）、ハードディスク（５００００４）、メモリ（５０００８）を備え、これらは装置内のバス（５０００６）によって相互にデータを送受信する。メモリ（５０００８）上では接続管理装置（６）の機能を備えた接続管理プログラム（６００００）が動作する。接続管理プログラム（６００００）は接続制御機能（６００００２）、認証機能（６００００４）、

アドレス管理機能（６０００６）を備え、これらの機能ブロックは接続制御装置（５２）、認証装置（５４）、アドレス管理装置（５６）と同じ機能を有し、処理シーケンスは図１０、図１１と同様である。

【００３２】

次に、アプリケーションの実例をいくつか挙げる。図２８はＶＰＮサーバ（７０）を用いてシステムを構築した例である。一般的なＶＰＮサーバ（７０）は通信において送信元ネットワークと送信先ネットワークの対として接続許可を管理し、接続許可がありかつユーザ認証が完了した端末からの通信のみを許可、管理するサーバである。これは接続制御装置（５２）と認証装置（５４）の機能を併せ持った装置とみなすことができる。

【００３３】

図２８に接続制御システム（５）にＶＰＮサーバ（７０）を適用した様子を示す。ＶＰＮサーバ（７０）とアドレス管理装置（５６）が連携することで、図１０、図１１に示した接続制御を行うことが可能である。

【００３４】

図２９はＴＶ会議システム（７）に接続制御システム（５）を連携させた実装例である。ＴＶ会議システム（７）はＴＶ会議サーバ（７２）と、ＩＥＴＦで標準化が進められているＳＩＰ(Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ)による呼制御を行うＳＩＰサーバ（７６）、ＴＶ会議参加者の状態を管理するプレゼンスサーバ（７４）から成る。ＴＶ会議サーバ（７２）は会議開始時にプレゼンスサーバ（７４）に参加者の状態を問い合わせ、参加者が現在端末を立ち上げているか、現在どのネットワークに属しているか等の情報を得る。このとき、端末の属するネットワークによっては会議サーバ（７２）から端末へ通信できない可能性が発生する。このような場合に、会議サーバ（７２）やＳＩＰサーバ（７６）が接続制御システムを用いて端末への通信到達性を確保することが考えられる。ＴＶ会議システム（７）と接続制御システム（５）を単一のシステムとして実装することも可能であり、その場合、たとえばＳＩＰサーバ（７６）が接続制御装置（５２）の機能を取り込む形の実装が考えられる。

【００３５】

上述のような接続管理機能は下記のようなプログラムで実現される。

通信網を介して第一及び第二の端末と接続され、
上記通信網と接続された送受信部と、
上記送受信部と接続されたＣＰＵを備えたサーバにおいて実行可能なプログラムであって、
送受信部が上記第一の端末から上記第二の端末への接続要求を受付けるステップと、
上記ＣＰＵが上記第一の端末から上記第二の端末への接続が可能かどうかを判定するステップと、
上記判定の結果、上記接続が不可能な場合には、上記ＣＰＵが、上記第二の端末と接続可能なアドレスを生成するステップと、
上記送受信部が該アドレスを含むデータを上記第一の端末へ送信するステップを有する接続制御方法を上記サーバに実行させるプログラム。

【図面の簡単な説明】

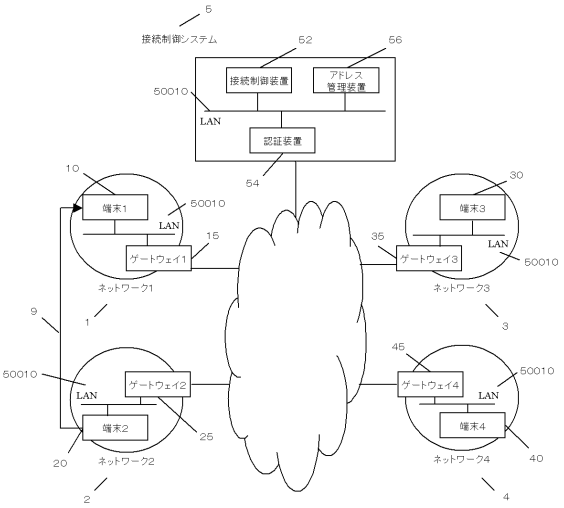
【００３６】

【図１】システムの全体構成を示す図。
【図２】ゲートウェイの機能ブロック図。
【図３】接続制御装置の機能ブロック図。
【図４】接続許可データベースの機能ブロック図。
【図５】ユーザ状態管理部の機能ブロック図。
【図６】認証装置の機能ブロック図。
【図７】認証データベースの機能ブロック図。
【図８】アドレス管理装置の機能ブロック図。
【図９】ネットワーク情報管理部の機能ブロック図。

【図１０】迂回路を使用しない場合のシーケンス図。
【図１１】迂回路を使用する場合のシーケンス図。
【図１２】接続制御装置のフローチャート。
【図１３】接続処理のフローチャート。
【図１４】迂回路接続処理のフローチャート。
【図１５】認証装置のフローチャート。
【図１６】認証処理のフローチャート。
【図１７】迂回路認証処理のフローチャート。
【図１８】アドレス管理装置のフローチャート。
【図１９】接続要求等のパケットフォーマットの図。
【図２０】接続不許可通知等のパケットフォーマットの図。
【図２１】迂回路認証完了通知等のパケットフォーマットの図。
【図２２】迂回路認証失敗通知等のパケットフォーマットの図。
【図２３】接続管理装置によるシステム構築例の図。
【図２４】接続制御装置等のハードウェア構成を表すブロック図。
【図２５】接続管理装置のハードウェア構成を表すブロック図。
【図２６】ＩＰｖ４適用時のネットワーク情報管理部の詳細を表すブロック図。
【図２７】通信時のパケット処理詳細図。
【図２８】ＶＰＮサーバによる接続制御システムの実現例の図。
【図２９】ＴＶ会議システムと接続制御システムの連携例の図。
【符号の説明】
【００３７】
１　ネットワーク１
２　ネットワーク２
３　ネットワーク３
４　ネットワーク４
５　接続制御システム
１０　端末１
１５　ゲートウェイ１
２０　端末２
２５　ゲートウェイ２
３０　端末３
３５　ゲートウェイ３
４０　端末４
４５　ゲートウェイ４
５２　接続制御装置
５４　認証装置
５６　アドレス管理装置。

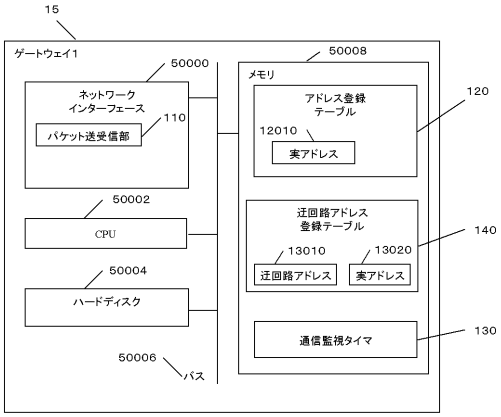
【図１】

図1



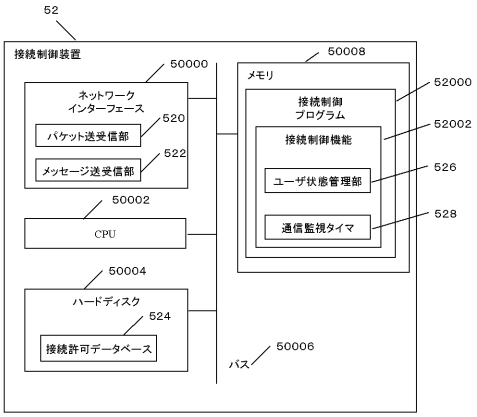
【図２】

図2



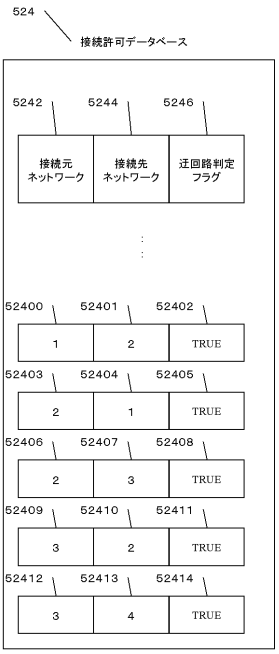
【図３】

図3



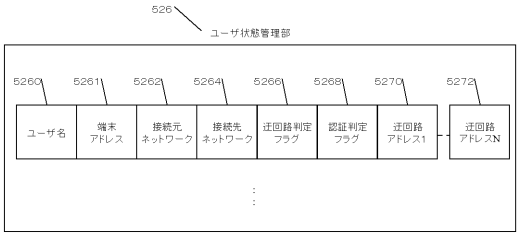
【図４】

図4



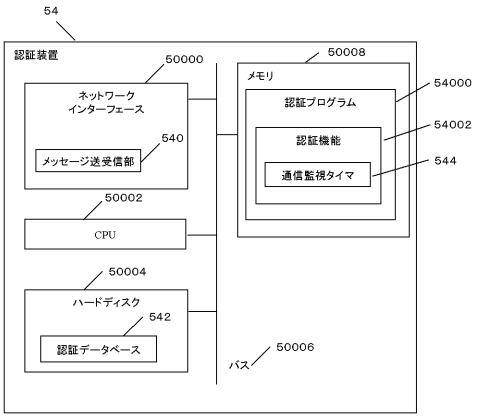
【図５】

図5



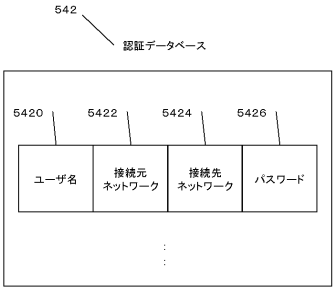
【図６】

図6



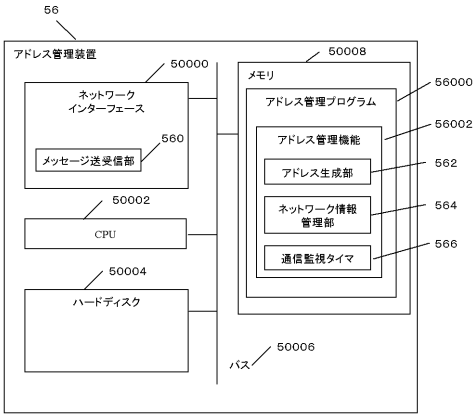
【図７】

図7



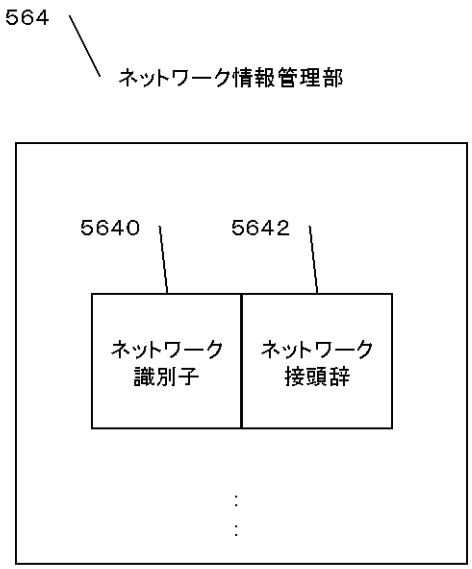
【図８】

図8



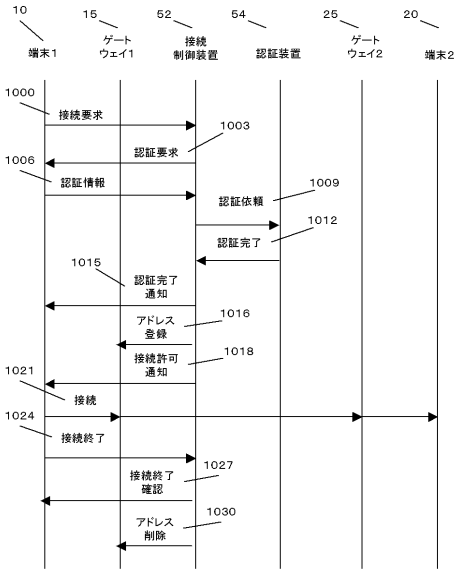
【図９】

図9



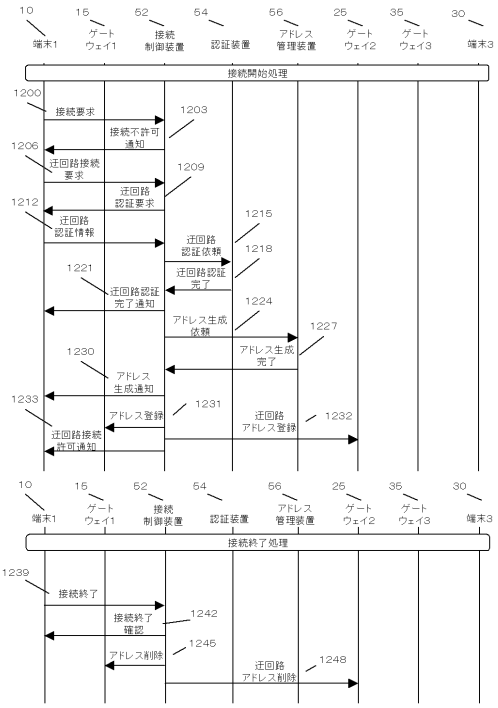
【図１０】

図10



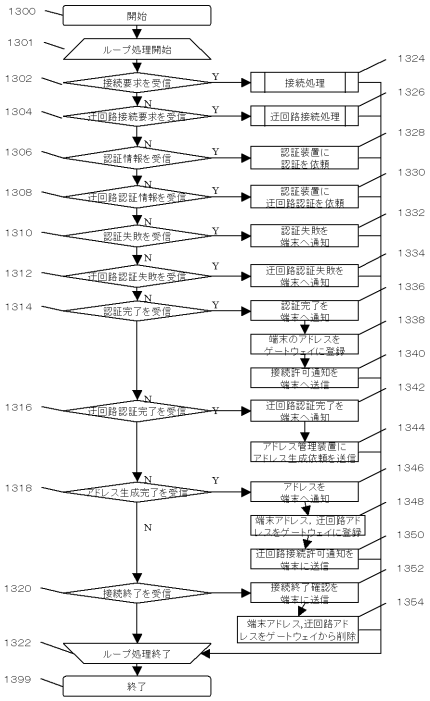
【図１１】

図11



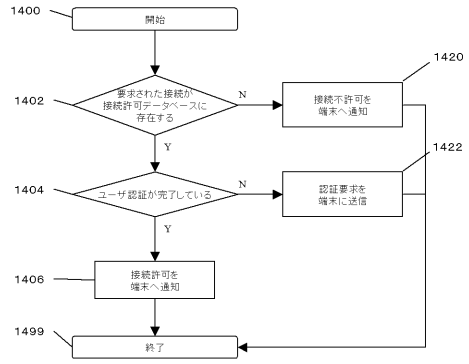
【図１２】

図12



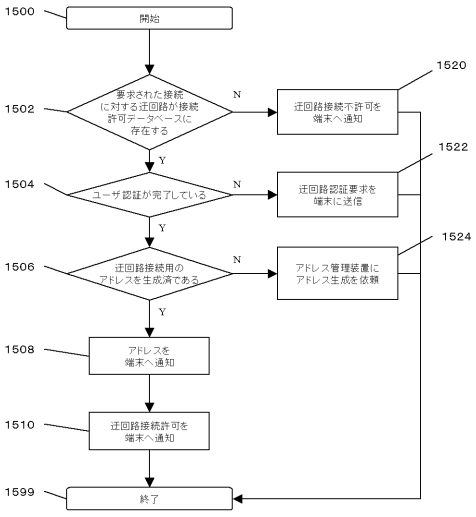
【図１３】

図13



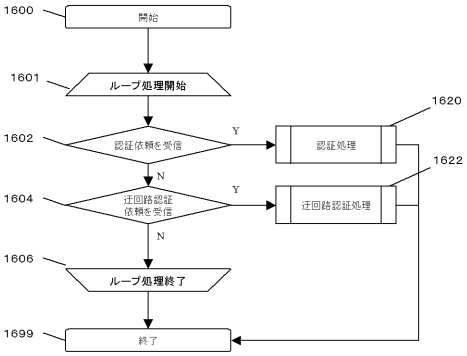
【図１４】

図14



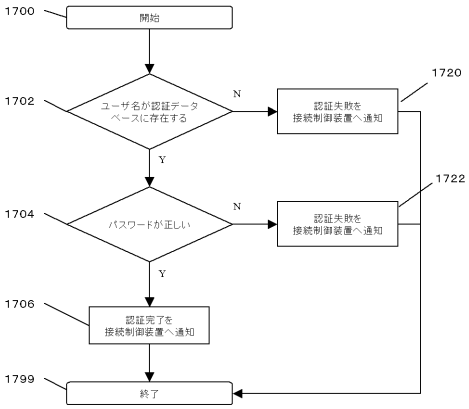
【図１５】

図15



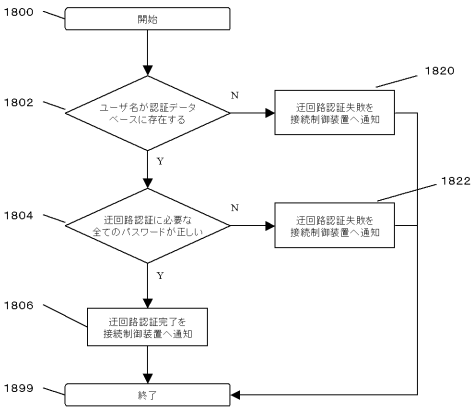
【図１６】

図16



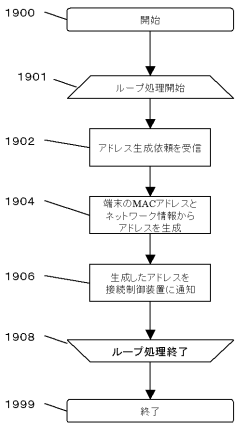
【図１７】

図17



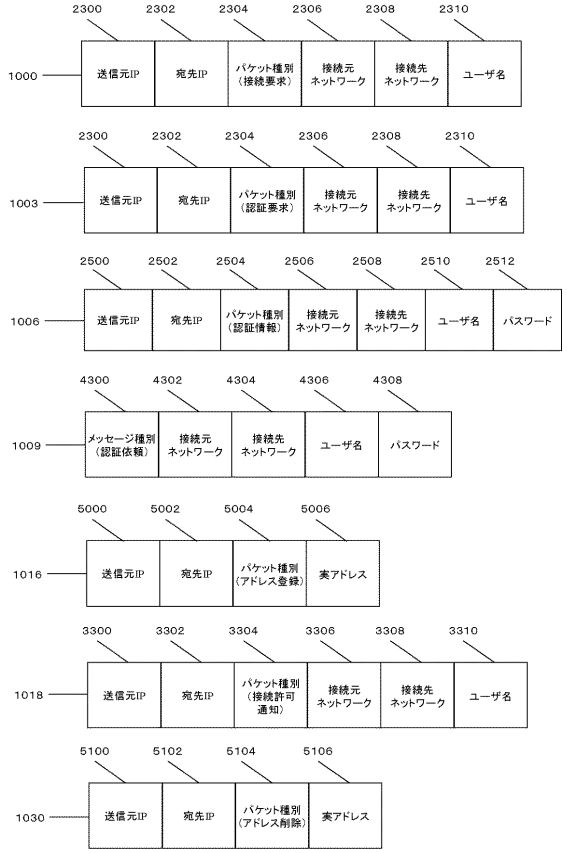
【図１８】

図18



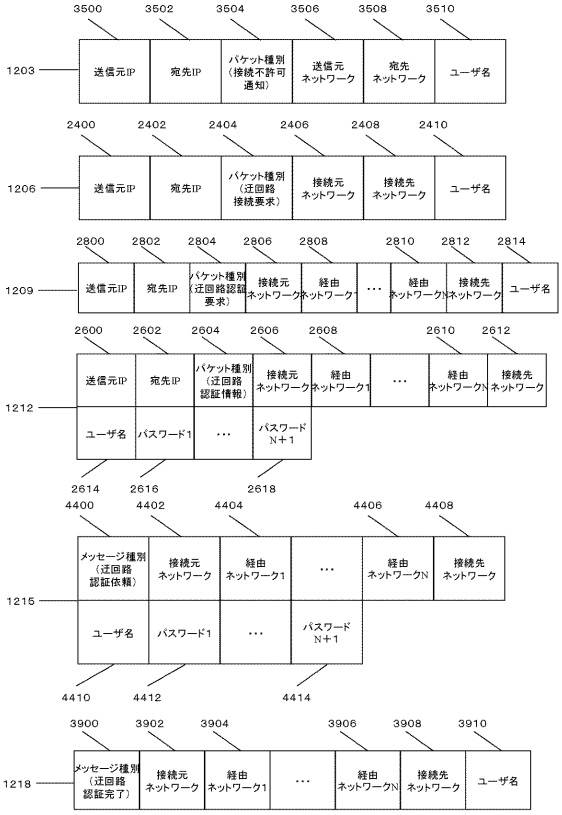
【図１９】

図19



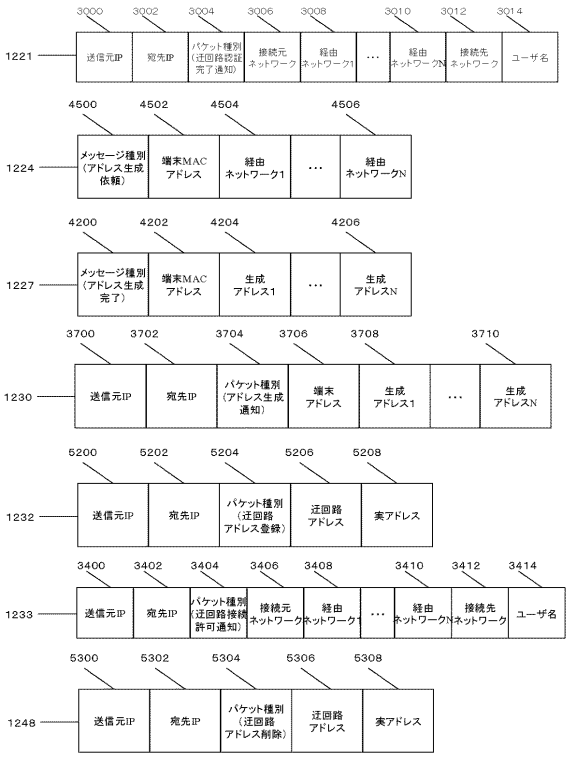
【図２０】

図20



【図２１】

図21

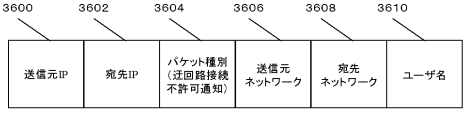


【図２２】

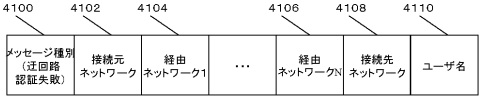
図22

迂回路認証失敗通知

迂回路接続不許可通知

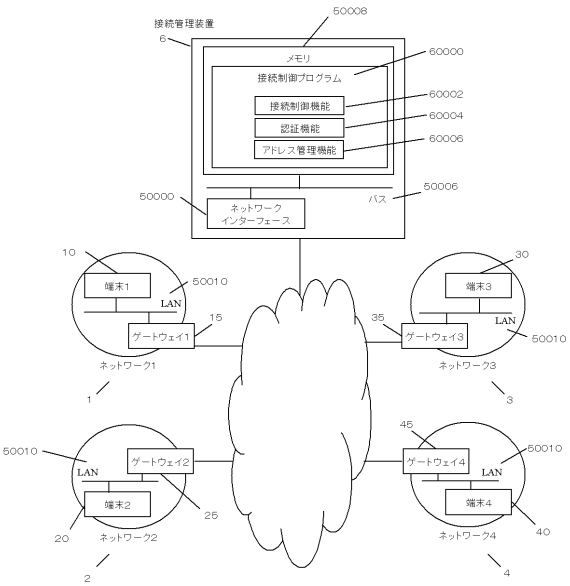


迂回路認証失敗



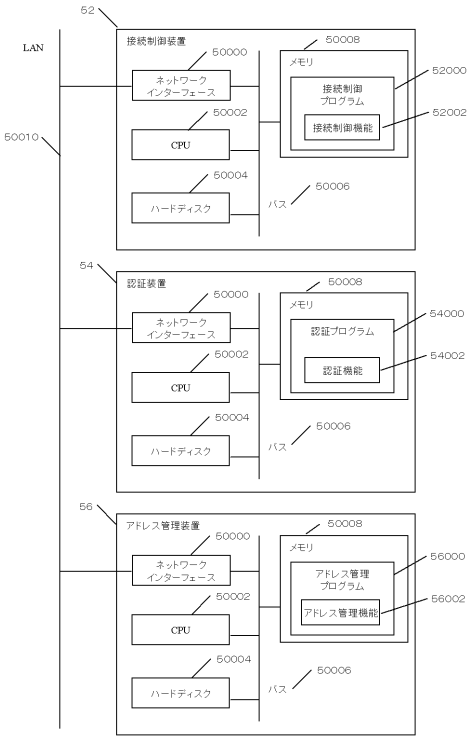
【図２３】

図23



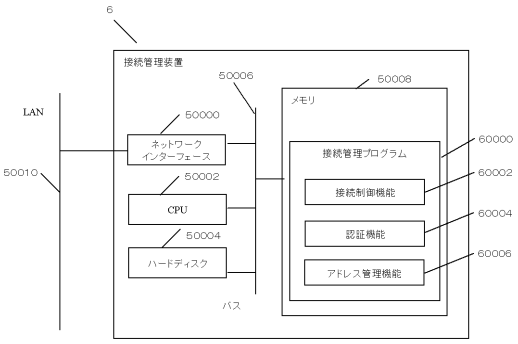
【図２４】

図24



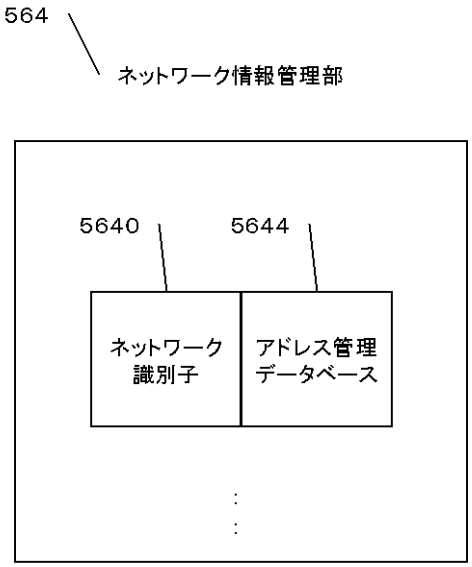
【図２５】

図25



【図２６】

図26



【図２７】

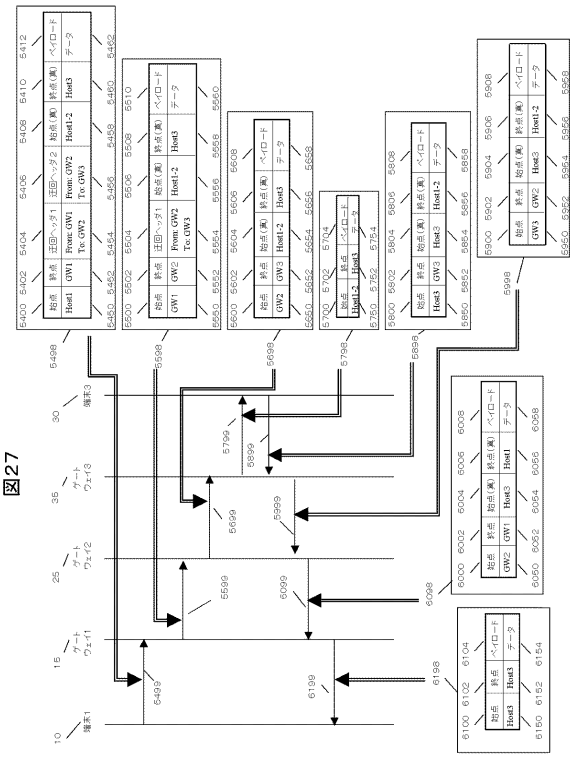
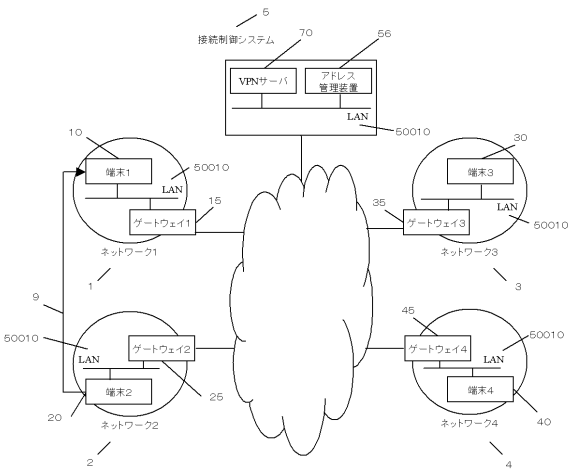


図27

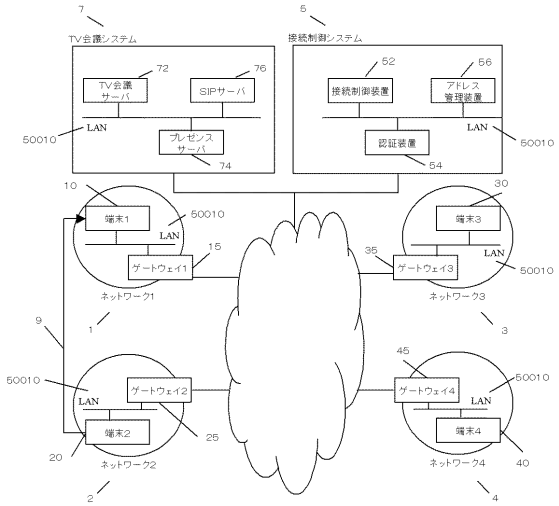
【図２８】

図28



【図２９】

図29



フロントページの続き

(72)発明者　吉澤　政洋
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
(72)発明者　武田　幸子
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

審査官　吉田　隆之

(56)参考文献　特開平１１－３５５２７２（ＪＰ，Ａ）
特開２００２－３１４５８７（ＪＰ，Ａ）
特開平１１－０３２０５８（ＪＰ，Ａ）
特開２００１－３５２３３７（ＪＰ，Ａ）
特開２００１－０５３７９１（ＪＰ，Ａ）
特開２００１－３３３１１４（ＪＰ，Ａ）
特開平０９－１２１２２３（ＪＰ，Ａ）
特開２００１－０４５０５８（ＪＰ，Ａ）
特開平１０－３２７１９１（ＪＰ，Ａ）
白崎　博生，ファイアウォールの作り方１３，ＵＮＩＸ　ＭＡＧＡＺＩＮＥ，株式会社アスキー，１９９８年１２月　１日，第13巻　第12号，p.38～p.50
ずばり、社内ＬＡＮの核心に迫ってみよう！　管理者に学ぶプロキシサーバ再入門，ＮＥＴＷＯＲＫ　ＭＡＧＡＺＩＮＥ　第６巻　第７号，日本，株式会社アスキー，２００１年　７月　１日，第6巻，p.154～p.157
中沢　功次　Koji　Nakazawa，次世代ネットワークサービスＩＰ－ＶＰＮ　Next Generation Network Service IP-VPN，ＮＥＣ技報　第５２巻　第８号　NEC TECHNICAL JOURNAL，日本電気株式会社　NEC Corporation，１９９９年　８月２５日，第52巻，p.62～p.65

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５６
Ｇ０９Ｃ　１／００
Ｈ０４Ｗ　４０／３４