(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4189076号
(P4189076)
(45)発行日　平成20年12月3日(2008.12.3)　(24)登録日　平成20年9月19日(2008.9.19)

(51)Int.Cl.　F I
G06F 11/20 (2006.01)　G06F 11/20 310E

請求項の数 2　(全 18 頁)

(21)出願番号　特願平11-83935
(22)出願日　平成11年3月26日(1999.3.26)
(65)公開番号　特開2000-276455(P2000-276455A)
(43)公開日　平成12年10月6日(2000.10.6)
審査請求日　平成16年9月24日(2004.9.24)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100070437
弁理士　河井　将次

最終頁に続く

(54)【発明の名称】耐障害コンピュータシステム

(57)【特許請求の範囲】
【請求項１】
クライアント計算機、及び当該クライアント計算機からの要求を処理する複数のサーバ計算機の各々がワイドエリアネットワークを介して相互接続され、前記クライアント計算機から、前記複数のサーバ計算機に共通のテイクオーバされる仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットが送出されることにより、サーバ計算機間のサービスの引き継ぎが行われる耐障害コンピュータシステムにおいて、
前記複数のサーバ計算機のそれぞれについて、前記仮想ネットワークアドレスと当該サーバ計算機に固有の実ネットワークアドレスと当該サーバ計算機において当該仮想ネットワークアドレスが有効であるかを示すフラグ情報とを対応付けた対応情報が登録され、いずれか１つの対応情報におけるフラグ情報によって前記仮想ネットワークアドレスが有効であることが示されるネットワークアドレス対応情報登録手段と、前記クライアント計算機から前記仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを受け取った場合に、当該ネットワークトレーラを、前記複数のサーバ計算機のそれぞれについて前記ネットワークアドレス対応情報登録手段に登録されている対応情報によって示される実ネットワークアドレスのうち、前記フラグ情報によって前記仮想ネットワークアドレスが有効であることが示されているサーバ計算機に固有の実ネットワークアドレス宛ての新たなネットワークトレーラに梱包する梱包手段と、前記新たなネットワークトレーラを含む通信パケットを前記仮想ネットワークアドレスが有効状態にあるサーバ計算機に送信する送信手段とを備えたゲートウェイを具備すると共に、

前記クライアント計算機は、前記仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを前記ゲートウェイに送信するように経路情報が設定された経路情報登録手段と、前記経路情報登録手段に設定されている経路情報に基づき、前記仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを前記ゲートウェイに送信する送信手段とを備え、

前記サーバ計算機は、前記ゲートウェイの梱包手段により前記クライアント計算機からのネットワークトレーラが梱包された、自身に固有の実ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを受け取った場合に、前記梱包されたネットワークトレーラを開封し、自身に固有の実ネットワークアドレス以外宛てのネットワークトレーラを含む通信パケットを受け取った場合には、当該パケットを破棄するフィルタドライバ手段と、自身に関する前記仮想ネットワークアドレスの状態を前記ゲートウェイに通知することによって、当該仮想ネットワークアドレスの状態を前記複数のサーバ計算機のそれぞれについて前記ネットワークアドレス対応情報登録手段に登録されている前記対応情報の前記フラグ情報に反映させる通知手段とを備えていることを特徴とする耐障害コンピュータシステム。

【請求項２】

前記梱包手段は、前記クライアント計算機からのネットワークトレーラを梱包する際に、当該トレーラを所定サイズ以下に分割する分割手段、当該トレーラを圧縮する圧縮手段、及び当該トレーラを暗号化する暗号化手段のうちの少なくとも１つを含み、

前記フィルタドライバ手段は、前記分割手段により分割された前記ネットワークトレーラを結合する結合手段、前記圧縮手段により圧縮された前記ネットワークトレーラを解凍する解凍手段、及び前記暗号化手段により暗号化された前記ネットワークトレーラを復号する復号手段のうち、前記梱包手段に含まれている前記少なくとも１つの手段に対応する手段を含むことを特徴とする請求項１記載の耐障害コンピュータシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、クライアント計算機、及び当該クライアント計算機からの要求を処理する複数のサーバ計算機の各々がワイドエリアネットワーク（ＷＡＮ）を介して相互接続されたコンピュータシステムに係り、特に遠隔地に分散配置されたサーバ計算機間のサービスの引き継ぎに好適な耐障害コンピュータシステムに関する。

【０００２】

【従来の技術】

従来から、複数のサーバ計算機（ノード）をネットワークで結合し、あるサーバ計算機で障害が発生しても、障害で停止したサービスを他のサーバ計算機が引き継ぐことにより、システム全体として可用性を維持できるようにしたクラスタ型の耐障害コンピュータシステム（高可用性システム）が種々開発されている。

【０００３】

この種のコンピュータシステムは、大別して、バックアップを兼ねた複数のサーバ計算機が近接して配置されたシステムと、地震や火災といった災害発生時のバックアップを考慮して、複数のサーバ計算機が例えば東京と大阪のように遠く離れた場所に配置されたシステムとに分類される。

【０００４】

複数のサーバ計算機が近接配置されたシステムでは、各サーバ計算機は同一のローカルエリアネットワーク（ＬＡＮ）に接続されるのが一般的である。この場合、各サーバ計算機のネットワークアドレス（インターネットアドレス）としてのＩＰ（Internet Protocol）アドレスのネットワーク部の内容は共通である。

【０００５】

一方、複数のサーバ計算機が互いに遠く離れた場所に配置されたシステムでは、各サーバ計算機は、公衆回線網等のＷＡＮにより結合された、それぞれ異なるＬＡＮに接続される

のが一般的である。この場合、各サーバ計算機のＩＰアドレスのネットワーク部の内容は異なる。

【０００６】

さて、耐障害コンピュータシステムでは、クライアント計算機に対してサービスを提供するサーバ計算機が（障害発生等で）切り替わった場合に、クライアント計算機でサービスを継続して受けることができるような仕組みが必要となる。

【０００７】

例えば、近接配置されたサーバ計算機間でサービスの引き継ぎを行うには、ＩＰアドレスを切り替える仕組み、またはクライアント計算機のアプリケーションプログラムにより接続するサーバ計算機を切り替える仕組みが必要となる。一方、遠く離れたサーバ計算機間でサービスの引き継ぎを行うには、クライアント計算機のアプリケーションプログラムにより接続するサーバ計算機を切り替える仕組みが必要となる。

【０００８】

【発明が解決しようとする課題】

上記したように、従来の耐障害コンピュータシステムにおいて、遠く離れたサーバ計算機間でサービスの引き継ぎを行うには、クライアント計算機のアプリケーションプログラムにより接続するサーバ計算機を切り替える必要があった。

【０００９】

しかし、クライアント計算機のアプリケーションプログラムにより接続するサーバ計算機を切り替えるには、アプリケーションプログラムを改造しなければならないという問題があった。

【００１０】

本発明は上記事情を考慮してなされたものでその目的は、遠く離れたサーバ計算機間のサービスの引き継ぎが、近接配置されたサーバ計算機間で引き継ぐ場合と同様にネットワークアドレスの切り替えにより実現できる耐障害コンピュータシステムを提供することにある。

【００１１】

【課題を解決するための手段】

本発明は、クライアント計算機、及び当該クライアント計算機からの要求を処理する複数のサーバ計算機の各々がＷＡＮ（ワイドエリアネットワーク）を介して相互接続され、クライアント計算機から、各サーバ計算機に共通のテイクオーバされる仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットが送出されることにより、サーバ計算機間のサービスの引き継ぎが行われる耐障害コンピュータシステムにおいて、次の各手段を備えたゲートウェイ、即ち上記仮想ネットワークアドレスと当該アドレスが有効状態に設定されているサーバ計算機に固有の実ネットワークアドレスとの対応情報が登録されるネットワークアドレス対応情報登録手段と、クライアント計算機から上記仮想ネットワークアドレス宛ての（つまり仮想ネットワークアドレスを宛先ネットワークアドレスとする）ネットワークトレーラを含む通信パケットを受け取った場合に、当該ネットワークトレーラを、上記ネットワークアドレス対応情報登録手段に登録されている、仮想ネットワークアドレスが有効状態にあるサーバ計算機に固有の実ネットワークアドレス宛ての新たなネットワークトレーラに梱包する梱包手段と、上記新たなネットワークトレーラを含む通信パケットを仮想ネットワークアドレスが有効状態にあるサーバ計算機に送信する送信手段とを備えたゲートウェイを設けると共に、上記クライアント計算機には、上記仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを上記ゲートウェイに送信するように経路情報が設定された経路情報登録手段を持たせ、上記サーバ計算機には、ゲートウェイの梱包手段によりクライアント計算機からのネットワークトレーラが梱包された、自身に固有の実ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを受け取った場合に、当該梱包されたネットワークトレーラを開封し、自身に固有の実ネットワークアドレス以外宛てのネットワークトレーラを含む通信パケットを受け取った場合には、当該パケットを破棄するフィルタドライバ手段と、自身に関する仮想

ネットワークアドレスの状態を上記ゲートウェイに通知してネットワークアドレス対応情報登録手段の登録内容に反映させる通知手段とを持たせたことを特徴とする。

【００１２】

このような構成において、クライアント計算機は、サーバ計算機からサービスの提供を受けようとする場合、（クライアント計算機にサービスを提供するサーバ計算機に共通の）仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを、経路情報登録手段に設定されている経路情報に従って、（宛先ハードウェアアドレスとしてゲートウェイのハードウェアアドレスを用いることで）ゲートウェイ経由となるように送信する。これにより、クライアント計算機からの仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットは、全てゲートウェイで受信される。

【００１３】

ゲートウェイは、受信パケット中のネットワークトレーラが仮想ネットワークアドレス宛ての場合、当該ネットワークトレーラを、ネットワークアドレス対応情報登録手段により当該仮想ネットワークアドレスが有効状態に設定されていることが示されているサーバ計算機の実ネットワークアドレス（つまり、サーバ計算機の外から見えて、当該サーバ計算機が特定できる実ネットワークアドレス）宛ての新たなネットワークトレーラに梱包して、そのサーバ計算機に送信する。

【００１４】

サーバ計算機は、ゲートウェイで処理されたクライアント計算機からのネットワークトレーラが梱包された新たなネットワークトレーラを含む通信パケットを受信すると、梱包されたネットワークトレーラを開封する。これによりサーバ計算機、即ち仮想ネットワークアドレスが有効状態にあるサーバ計算機では、クライアント計算機からの仮想ネットワークアドレス宛てのネットワークトレーラが処理可能となる。

【００１５】

以上により、クライアント計算機は、現在サービスを提供可能なサーバ計算機を何ら意識することなく、単に各サーバ計算機に共通のテイクオーバされる仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットをゲートウェイに送信するだけで、遠く離れた（具体的には、異なるＬＡＮに接続された）サーバ計算機間でも、近接配置された（具体的には、同一ＬＡＮに接続された）サーバ計算機間でのサービスの引き継ぎと同様に、ネットワークアドレスの切り替えが可能となり、クライアント計算機は、アプリケーションプログラムの改造を必要とせずに、遠く離れたサーバ計算機からのサービスを継続して受けることができる。

【００１６】

ここで、テイクオーバされる仮想ネットワークアドレスが共通に割り当てられている各サーバ計算機に、当該仮想ネットワークアドレスが外（そのサーバ計算機が接続されているローカルなネットワーク上の他のノード）から見えない（認識できない）ようにする機能を持たせるとよい。このようにすると、仮想ネットワークアドレスがサーバ計算機のハードウェアアドレスと誤って対応付けられる不具合を防止できる。この機能は、例えば米国AT&Tベル研究所で開発されたUNIX、或いは米国マイクロソフト社のWindows NTを用いたサーバ計算機には、予め用意されている。

【００１７】

また、サーバ計算機が、自身に固有の実ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを受け取った場合に、そのネットワークトレーラに、クライアント計算機からのネットワークトレーラが梱包されているか否かが、当該サーバ計算機のフィルタドライバ手段により容易に判別可能なように、ゲートウェイの梱包手段によるネットワークトレーラの梱包時に、新たなネットワークトレーラに特定の宛先ポート番号を付加する構成を適用するとよい。

【００１８】

この構成では、サーバ計算機のフィルタドライバ手段は、自身に固有の実ネットワークアドレス宛てのネットワークトレーラを含む通信パケットを受け取った場合、宛先ポート番

号が上記特定のポート番号であるか否かにより、そのネットワークトレーラにクライアント計算機からのネットワークトレーラが梱包されているか否かを判別することができ、特定のポート番号の場合にのみ、クライアント計算機からのネットワークトレーラを開封（復元）する処理を行えばよい。

【００１９】

また本発明は、仮想ネットワークアドレスが有効状態に設定されるサーバ計算機が複数存在することを許すようにし、ゲートウェイの梱包手段では、クライアント計算機からの仮想ネットワークアドレス宛てのネットワークトレーラを新たなネットワークトレーラに梱包する際に設定する、当該新たなネットワークトレーラの宛先ネットワークアドレスを、クライアント計算機に固有のネットワークアドレス、つまりクライアント計算機からの仮想ネットワークアドレス宛てのネットワークトレーラに設定されている送信元ネットワークアドレスをもとに決定するようにしたことをも特徴とする。

【００２０】

このような構成においては、仮想ネットワークアドレスが設定されているサーバ計算機、即ちサービスを提供する計算機として指定されたサーバ計算機が同時に複数存在する場合でも、通信パケット中の送信元計算機に関する情報、つまりサービス提供の要求元のクライアント計算機に関する情報をもとに、当該複数のサーバ計算機のうちの１つだけが、実際にサービスを提供するサーバ計算機として要求元のクライアント計算機と通信を行うことで、負荷分散を図ることが可能となる。ここで、仮想ネットワークアドレス宛てのネットワークトレーラに設定されている送信元ネットワークアドレスに基づいて、サービスを提供するサーバ計算機を決定する代わりに、各サーバ計算機の負荷状態に応じて、サービスを提供するサーバ計算機を決定するようにしても構わない。

【００２１】

また本発明は、クライアント計算機からのネットワークトレーラを新たなネットワークトレーラに梱包することで、当該新たなネットワークトレーラが規定サイズを超える場合に対処するために、上記梱包手段に、上記クライアント計算機からのトレーラを所定サイズ以下に分割する分割手段を持たせる一方、上記フィルタドライバ手段に、上記分割手段により分割されたネットワークトレーラを結合する結合手段を持たせたことをも特徴とする。

【００２２】

この他に、上記梱包手段に、クライアント計算機からのネットワークトレーラを圧縮する圧縮手段を持たせる一方、上記フィルタドライバ手段に、上記圧縮手段により圧縮されたネットワークトレーラを解凍する解凍手段を持たせるようにしても、上記分割手段及び結合手段を適用した場合と同様の効果を得ることが可能である。また秘匿性を実現するために、上記梱包手段に、クライアント計算機からのネットワークトレーラを暗号化する暗号化手段を持たせる一方、上記フィルタドライバ手段に、上記暗号化手段により暗号化されたネットワークトレーラを復号する復号手段を持たせるようにしてもよい。更に、上記梱包手段に、上記の分割手段、圧縮手段及び暗号化手段のうちの少なくとも２つを持たせる一方、上記フィルタドライバ手段に、上記の結合手段、解凍手段及び復号手段のうちの対応する少なくとも２つの手段を持たせるならば、なおよい。

【００２３】

【発明の実施の形態】

以下、本発明の実施の形態につき図面を参照して説明する。

【００２４】

図１は本発明の一実施形態に係る耐障害コンピュータシステムの構成を示すブロック図である。

【００２５】

図１において、１１Ａ，１１Ｂ，１１Ｃはイーサネット等により構成されるＬＡＮ（ローカルエリアネットワーク）である。ＬＡＮ１１Ａ，１１Ｂには、それぞれサーバ計算機（以下、サーバと称する）１２Ａ，１２Ｂが接続され、ＬＡＮ１１Ｃにはサーバ１２Ａ，１

２Ｂからのサービスを受けるクライアント計算機（以下、クライアントと称する）１２Ｃが接続されている。また、ＬＡＮ１１Ｃには、少なくともプロトコル変換機能を有するゲートウェイ１３も接続されている。各ＬＡＮ１１Ａ，１１Ｂ，１１Ｃは、それぞれルータ１４Ａ，１４Ｂ，１４Ｃを介して公衆回線網等のＷＡＮ（ワイドエリアネットワーク）１５に接続されている。ここでは、サーバ１２Ａ，１２Ｂ及びゲートウェイ１３間の通信にＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）と呼ばれる通信プロトコル（ＴＣＰ／ＩＰプロトコル）を適用するものとする。

【００２６】

図２はＬＡＮ１１Ａ～１１Ｃを介して転送される通信パケット（イーサネットトレーラ）の概略フォーマットを示す。

【００２７】

同図に示すように、通信パケット２０は、宛先ＭＡＣ（Media Access Control）アドレス２１１及び送信元ＭＡＣアドレス２１２を含むヘッダ部（イーサネットヘッダ）２１と、当該パケット（イーサネットトレーラ）２０のデータ部（イーサネットデータ部）をなすＩＰトレーラ２２とを有している。

【００２８】

ＩＰトレーラ２２は、宛先ＩＰアドレス２３１及び送信元ＩＰアドレス２３２を含むヘッダ部（ＩＰヘッダ）２３と、当該ＩＰトレーラ２２のデータ部（ＩＰデータ部）をなすＵＤＰ（User Diagram Protocol）トレーラ２４とを有している。ＵＤＰトレーラ２４は、宛先ポート番号２５１及び送信元ポート番号２５２を含むヘッダ部（ＵＤＰヘッダ）２５と、データ部（ＵＤＰデータ部）２６とを有している。

【００２９】

さて、図１中のサーバ１２Ａ，１２Ｂは、それぞれ当該サーバ１２Ａ，１２Ｂに固有のネットワークアドレス（実ネットワークアドレス）としてのＩＰアドレス（実ＩＰアドレス）ＩＰＡ，ＩＰＢ（１種類とは限らない）に加えて、当該サーバ１２Ａ，１２Ｂに共通のテイクオーバするネットワークアドレス（仮想ネットワークアドレス）としてのＩＰアドレス（仮想ＩＰアドレス）ＩＰＳを持つ。サーバ１２Ａ，１２Ｂは、ＩＰＳがＬＡＮ１１Ａ，１１Ｂ上の他のノードから見えない（認識できない）ようにする機能を有する。

【００３０】

サーバ１２Ａ，１２Ｂは、図３に示すように、特定アプリケーションプログラム（以下、特定アプリケーションと称する）１２１と、インタフェース層１２２、インターネット層（ネットワーク層）１２３及びトランスポート層１２４の処理を司る通信ドライバ１２５と、一般的なアプリケーションプログラム（以下、一般アプリケーションと称する）１２６と、フィルタドライバ１２７とを備えている。

【００３１】

特定アプリケーション１２１は、自身のＩＰＳがＯＮ（有効）／ＯＦＦ（無効）いずれの状態に設定されているかをゲートウェイ１３に通知して当該ゲートウェイ１３内のＩＰアドレス対応テーブル１３１の内容を更新させるＯＮ／ＯＦＦ通知機能１２１ａを有している。ＩＰＳは、サーバ１２Ａ及び１２Ｂのいずれか一方においてのみ有効（ＯＮ）状態に設定される。但し、クライアント１２Ｃからは、ＩＰアドレスＩＰＳがＯＮ状態に設定されているサーバとＯＦＦ状態に設定されているサーバとを識別できず、単にＩＰアドレスＩＰＳを持つ１つのサーバ（サービスを提供するサーバ）が存在するように見えるだけである。

【００３２】

フィルタドライバ１２７は、インタフェース層１２２とインターネット層１２３との間に位置しており、当該インタフェース層１２２及びインターネット層１２３に相当する処理機能を有する。本実施形態においてフィルタドライバ１２７は、インタフェース層１２２から送られるＩＰトレーラ（ネットワークトレーラ）２３の宛先ＩＰアドレス２４（図２参照）をチェックし、自身の実ＩＰアドレス宛てでない場合には当該ＩＰトレーラ２３を破棄するフィルタリング機能を持つ。フィルタドライバ１２７はまた、宛先ＩＰアドレス

２４が自身の実ＩＰアドレス宛ての場合には、ＩＰトレーラ２３からＵＤＰトレーラ２７を取り出して宛先ポート番号２７２をチェックし、その宛先ポート番号２７２に応じて、当該ＩＰトレーラ２３または後述するようにＵＤＰトレーラ２７のデータ部２７４に設定（梱包）されている（クライアントからの）ＩＰトレーラをインターネット層１２３に渡す機能を持つ。

【００３３】

図１中のクライアント１２Ｃは、ＩＰアドレスＩＰＳ宛てのパケット（２０）を全てゲートウェイ１３宛てに送信する（投げ入れる）ように構成されている。そのため、クライアント１２Ｃのルーティング・テーブル１２０には、ＩＰＳと対をなすハードウェアアドレス（物理アドレス）としてのＭＡＣアドレスとして、ゲートウェイ１３に固有のＭＡＣアドレスＭＡＣＧが設定される。

【００３４】

ゲートウェイ１３は、図４に示すように、ＩＰアドレス対応テーブル１３１と、インタフェース層１３２、インターネット層１３３及びトランスポート層１３４の処理を司る通信ドライバ１３５と、ゲートウェイプログラム１３６とを備えている。なお図４では、ＬＡＮ１１Ｃとのインタフェース（ネットワークインタフェース）は省略されている。

【００３５】

ＩＰアドレス対応テーブル１３１には、仮想ＩＰアドレスＩＰＳと、当該ＩＰＳが割り当てられているサーバ（ここではサーバ１２Ａ，１２Ｂ）に固有の（外から見える）実ＩＰアドレス（ここではサーバ１２Ａ，１２Ｂの実ＩＰアドレスＩＰＡ，ＩＰＢ）と、ＩＰＳがそのサーバでＯＮ状態に設定されているか否かを示すフラグ情報との対応を組にした情報が登録される。ここでは、サーバ１２Ａまたは１２ＢからのＩＰＳのＯＮ通知により、対応するＩＰＡまたはＩＰＢと組をなすフラグ情報がＯＮされ、他のサーバの実ＩＰアドレス（ＩＰＢまたはＩＰＡ）がＯＦＦされるようになっている。この他に、ＩＰＡ及びＩＰＢとそれぞれ組をなすフラグ情報がいずれもＯＦＦの場合にのみ、サーバ１２Ａまたは１２ＢからのＩＰＳのＯＮ通知に応じて、対応するＩＰＡまたはＩＰＢと組をなすフラグ情報がＯＮされるものであっても構わない。この場合、各サーバ１２Ａ，１２Ｂは、ゲートウェイ１３に問い合わせてＩＰアドレス対応テーブル１３１の状態を確認してから、ＩＰＳのＯＮ通知を出すようにするとよい。

【００３６】

通信ドライバ１３５は、ゲートウェイ１３で受信された通信パケット２０をインタフェース層１３２で受け取った場合に、そのＩＰトレーラ２２をインターネット層１３３ではなくてゲートウェイプログラム１３６に渡すように構成されている。

【００３７】

また通信ドライバ１３５は、トランスポート層１３４からインターネット層１３３にＵＤＰトレーラ２７が渡された場合に、そのＵＤＰトレーラ２７がデータ部に設定され、宛先ＩＰアドレス部に、ＩＰアドレス対応テーブル１３１内でＯＮ状態にあるＩＰＳに対応して登録されている実ＩＰアドレスが設定されたＩＰトレーラ２３を生成してインタフェース層１３２に渡す機能を有する。通信ドライバ１３５は更に、ゲートウェイプログラム１３６からインターネット層１３３にＩＰトレーラ２３が渡された場合、そのＩＰトレーラ２３をそのままインタフェース層１３２に渡す機能も有する。

【００３８】

ゲートウェイプログラム１３６は、インタフェース層１３２からＩＰトレーラ２３を渡された場合、その宛先ＩＰアドレス２４をチェックし、ＩＰＳ以外の場合には当該ＩＰトレーラ２３をそのままインターネット層１２３に渡し、ＩＰＳの場合には、当該ＩＰトレーラ２３をそのままデータとしてトランスポート層１３４に渡す機能を有する。

【００３９】

次に、図１のシステムの動作を、サーバ１２Ａ，１２Ｂのうちのサーバ１２ＡにおいてＩＰアドレスＩＰＳがＯＮされている状態で、クライアント１２ＣがＩＰＳ宛ての通信パケット２０（＝Ｄ）を送信する場合を例に、図５乃至図９を参照して説明する。

【００４０】
まずクライアント１２Ｃは、図５に示す、ＩＰアドレスＩＰＳ宛てのパケット２０（＝Ｄ）を作成する。ここで、クライアント１２Ｃ内のルーティング・テーブル１２０には、ＩＰＳ宛てのパケット２０（＝Ｄ）はゲートウェイ１３経由で通信するように設定されている。したがって、ＩＰＳ宛てのパケット２０のイーサネットヘッダ２１中の宛先ＭＡＣアドレス２１１にはゲートウェイ１３のＭＡＣアドレスＭＡＣＧが用いられる。また、送信元ＭＡＣアドレス２１２にはクライアント１２ＣのＭＡＣアドレスＭＡＣＣが用いられる。更に、ＩＰＳ宛てのパケット２０（＝Ｄ）のイーサネットデータ部をなすＩＰトレーラ２２（＝Ｅ）の（ＩＰヘッダ２３中の）宛先ＩＰアドレス２３１にはＩＰＳが、送信元ＩＰアドレス２３２にはクライアント１２ＣのＩＰアドレスＩＰＣが、それぞれ用いられる。

【００４１】
クライアント１２Ｃは作成した図５に示すパケット２０（＝Ｄ）をＬＡＮ１１Ｃ上に送出する。このＬＡＮ１１Ｃ上のパケット２０（＝Ｄ）は、当該パケット２０（＝Ｄ）におけるイーサネットヘッダ２１の宛先ＭＡＣアドレス２１１の情報ＭＡＣＧにより、ゲートウェイ１３で受信される。

【００４２】
ゲートウェイ１３で受信されたパケット２０（＝Ｄ）は、図５に示すように通信ドライバ１３５によりインタフェース層１３２の処理に供されて、当該パケット２０（＝Ｄ）からＩＰトレーラ２２（＝Ｅ）が取り出される。このＩＰトレーラ２２（＝Ｅ）は、インターネット層１３３ではなくて、ゲートウェイプログラム１３６に渡される（図４及び図５のステップＳ１）。

【００４３】
ゲートウェイ１３では、ゲートウェイプログラム１３６により以下の処理が行われる。
まず、ＩＰトレーラ２２（＝Ｅ）のＩＰヘッダ２３中の宛先ＩＰアドレス２３１がチェックされる（図５ステップＳ２１）。もし、宛先ＩＰアドレス２３１がＩＰＳ以外であるならば、（パケット受信時における従来のインタフェース層での処理と同様に）ＩＰトレーラ２２をそのままインターネット層１３３に渡す（図４及び図５のステップＳ２）。

【００４４】
これに対し、宛先ＩＰアドレス２３１が本実施形態のようにＩＰＳに一致するならば、ＩＰアドレス対応テーブル１３１を対象にＩＰＳがＯＮ状態にあるサーバの実ＩＰアドレス（この例ではサーバ１２ＡのＩＰＡ）を検索して新たな宛先ＩＰアドレスを取得する（図５ステップＳ２２）。続いて、パケット受信時における従来のインターネット層１３３での処理と同様に、ＩＰトレーラ２２（＝Ｅ）に対する処理を行って（図５ステップＳ２３）、そのＩＰトレーラ２２（＝Ｅ）をデータＦとして、先に検索した新たな宛先ＩＰアドレス（ここではＩＰＡ）及び送信元ＩＰアドレスとしての自身のＩＰアドレスＩＰＧと共にトランスポート層１３４に渡す（図４及び図６のステップＳ３）。

【００４５】
トランスポート層１３４では、ゲートウェイプログラム１３６から渡されたデータＦ、つまりＩＰトレーラ２２（＝Ｅ）を、図６に示すようにＵＤＰトレーラ２４（＝Ｈ）のＵＤＰデータ部２６に設定（梱包）する。このとき、ＵＤＰトレーラ２４（＝Ｈ）のＵＤＰヘッダ２５の宛先ポート番号２５１には、ＩＰＳ切り替え処理のための専用のポート番号αが設定される。このＵＤＰトレーラ２４（＝Ｈ）は、先にゲートウェイプログラム１３６から渡された宛先ＩＰアドレス（ＩＰＡ）及び送信元ＩＰアドレス（ＩＰＧ）と共に、トランスポート層１３４からインターネット層１３３に渡される（図４及び図６のステップＳ４）。

【００４６】
インターネット層１３３では、トランスポート層１３４からＵＤＰトレーラ２４（＝Ｈ）並びに宛先ＩＰアドレス（ＩＰＡ）及び送信元ＩＰアドレス（ＩＰＧ）を渡されると、そのＵＤＰトレーラ２４（＝Ｈ）がＩＰデータ部２４に設定された、図６に示す新たなＩＰ

トレーラ２２（＝Ｉ）、即ちクライアント１２ＣからのＩＰトレーラ２２（＝Ｅ）が梱包されている新たなＩＰトレーラ２２（＝Ｉ）を作成する。

【００４７】

ここで、新たなＩＰトレーラ２２（＝Ｉ）のＩＰヘッダ２３に設定される宛先ＩＰアドレスには、ＩＰＳに対応してＩＰアドレス対応テーブル１３１に登録されている実ＩＰアドレスのうち、フラグ情報がＯＮの実ＩＰアドレスが用いられる。この例では、該当する実ＩＰアドレスはＩＰＡであり、当該ＩＰＡ、即ちＩＰＳがＯＮ状態にあるサーバ１２Ａの実ＩＰアドレスＩＰＡが用いられる。また、新たなＩＰトレーラ２２（＝Ｉ）のＩＰヘッダ２３に設定される送信元ＩＰアドレスには、ゲートウェイ１３の実ＩＰアドレスＩＰＧが用いられる。これら宛先ＩＰアドレスＩＰＡ及び送信元ＩＰアドレスＩＰＧは、ゲートウェイプログラム１３６からトランスポート層１３４を介して渡されたものである。

【００４８】

作成されたＩＰトレーラ２２（＝Ｉ）は、インターネット層１３３からインタフェース層１３２に渡される（図４及び図７のステップＳ５）。

インタフェース層１３２では、インターネット層１３３からＩＰトレーラ２２（＝Ｉ）を渡されると、図７に示すように、そのＩＰトレーラ２２（＝Ｉ）がイーサネットデータ部に設定された新たなパケット（イーサネットトレーラ）２０（＝Ｊ）を作成する。このパケット２０（＝Ｊ）のイーサネットヘッダ２１には、宛先ＭＡＣアドレス２１１として宛先ＩＰアドレスのサーバのＭＡＣアドレス、即ちサーバ１２ＡのＭＡＣアドレスＭＡＣＡが、送信元ＭＡＣアドレス２１２としてクライアント１２ＣのＭＡＣアドレスＭＡＣＣが、それぞれ用いられる。

【００４９】

ゲートウェイ１３のインタフェース層１３２で作成されたパケット２０（＝Ｊ）は、当該インタフェース層１３２から図示せぬネットワークインタフェースを介してＬＡＮ１１Ｃ上に送出される（図４及び図７のステップＳ６）。このＬＡＮ１１Ｃ上のパケット２０（＝Ｊ）は、ルータ１４Ｃ、ＷＡＮ１５、ルータ１４Ａを介してＬＡＮ１１Ａに送出され、当該パケット２０（＝Ｊ）におけるイーサネットヘッダ２１の宛先ＭＡＣアドレス２１１の情報ＭＡＣＡにより、サーバ１２Ａで受信される。

【００５０】

サーバ１２Ａで受信されたパケット２０（＝Ｊ）は、通信ドライバ１２５によりインタフェース層１２２の処理に供されて、図８に示すように、当該パケット２０（＝Ｊ）からＩＰトレーラ２２が取り出される。このＩＰトレーラ２２は、図６及び図７中のＩ、つまりゲートウェイ１３により新たに作成された、クライアント１２ＣからのＩＰトレーラ２２（＝Ｅ）が梱包されているＩＰトレーラ２２（＝Ｉ）に一致する。このＩＰトレーラ２２（＝Ｉ）は、フィルタドライバ１２７に渡される（図３及び図８のステップＳ１１）。

【００５１】

これによりフィルタドライバ１２７では、以下の処理が行われる。

まず、ＩＰトレーラ２２（＝Ｉ）のＩＰヘッダ２３中の宛先ＩＰアドレスがチェックされる（図８ステップ３１）。もし、宛先ＩＰアドレスがＩＰＡ以外であるならば、ＩＰトレーラ２２（＝Ｉ）（を含む受信パケット）を破棄する（図８Ｓ３２）。これに対し、宛先ＩＰアドレスが本実施形態のようにＩＰＡに一致するならば、ＩＰトレーラ２２（＝Ｉ）からＩＰデータ部の内容、即ちＵＤＰトレーラ２４を取り出す（図８ステップＳ３３）。ここで取り出されるＵＤＰトレーラ２４は、図６中のＨに一致する。このようにフィルタドライバ１２７では、まずインターネット層１２３に相当する処理が行われる。

【００５２】

さて、上記ステップＳ３３でＵＤＰトレーラ２４が取り出されると、フィルタドライバ１２７では、トランスポート層１２４に相当する処理が行われる。

まず、ＵＤＰトレーラ２４（＝Ｈ）におけるＵＤＰヘッダ２５の宛先ポート番号２５１がチェックされる（図９ステップＳ３４）。もし、宛先ポート番号２５１がα以外であるならば、インタフェース層１２２から渡されたＩＰトレーラ２２（＝Ｉ）を（インタフェー

ス層１２２における従来のＩＰＡ宛てのパケットの受信時と同様に）インターネット層１２３に渡す（図３及び図９のＳ１２）。これに対し、宛先ポート番号２５１が本実施形態のようにαに一致するならば、ＵＤＰトレーラ２４（＝Ｈ）からＵＤＰデータ部２６の内容を取り出す（図９ステップＳ３５）。

【００５３】

ステップＳ３５でＵＤＰトレーラ２４（＝Ｈ）から取り出されたＵＤＰデータ部２６の内容は、データＦであり、クライアント１２Ｃからの送信パケット２０（＝Ｄ）中のＩＰトレーラ２２（＝Ｅ）に一致する。つまり、ＩＰトレーラ２２（＝Ｅ）が復元（開封）される。

フィルタドライバ１２７は、復元したＩＰトレーラ２２（＝Ｅ）をインターネット層１２３に渡す（図３及び図９のステップＳ１２）。

【００５４】

インターネット層１２３では、フィルタドライバ１２７からＩＰトレーラ２２を渡されると、従来インタフェース層１２２からＩＰトレーラ２２を渡された場合と同様に、ＩＰトレーラ２２（＝Ｅ）に対する処理を行って、そのデータ部の内容、即ちＵＤＰトレーラ２４を取り出し、トランスポート層１２４に渡す（図３ステップＳ１３）。

【００５５】

トランスポート層１２４では、インターネット層１２３からＵＤＰトレーラ２４を渡されると、当該ＵＤＰトレーラ２４のＵＤＰデータ部２６に設定されているデータを、ＵＤＰヘッダ２５の宛先ポート番号２５１で特定される一般アプリケーション１２６に渡す（図３ステップＳ１４）。

以上により、ＷＡＮ環境におけるＩＰアドレステイクオーバが実現される。

【００５６】

さて、サーバ１２Ａは、クライアント１２ＣからのＩＰトレーラ２２（＝Ｅ）、つまりリクエストを受け取ると、そのリクエストに応じてクライアント１２Ｃへのパケット送信（応答）を行う。このサーバ１２Ａからクライアント１２Ｃへの応答は、従来と同様に行われる。ここで、送信元ＩＰアドレスとしてＩＰＡ（実ＩＰアドレス）またはＩＰＳ（仮想ＩＰアドレス）のいずれを用いることも可能である。但し、クライアント１２Ｃ側に、当該クライアント１２Ｃが認識しているＩＰＳとサーバ１２Ａからの応答パケット中の送信元ＩＰアドレスとの一致をチェックする機能を持たせている場合、ＩＰＡは使用できない。

【００５７】

なお、前記実施形態では、ＷＡＮ１５とＬＡＮ１１ＣとがルータＲ１４Ｃにより接続されているものとして説明したが、本発明は、図１０に示すような、ゲートウェイ１３をルータとして兼用するシステムにも適用可能である。この図１０のシステムでクライアント１２ＣからＩＰＳ宛てのパケットを送信する場合も、前記実施形態で述べたのと同一手順が利用できる。

【００５８】

ここで、クライアント１２ＣからＩＰＳ宛てのパケットを送信する場合のデータの経路を、図１のシステムと図１０のシステムのそれぞれについて図１１に対比して示す。

【００５９】

この他にも本発明は、その要旨を逸脱しない範囲で種々変形して実施することができる。以下に、幾つかの変形例を列挙する。

［変形例１］

変形例１は、前記ステップＳ３でＩＰトレーラ２２（＝Ｅ）をそのままデータＦとする処理に代えて、当該ＩＰトレーラ２２（＝Ｅ）を分割、例えば２分割し、それぞれデータＦ１，Ｆ２として、トランスポート層１３４に渡す処理を適用したものである。この変形例１では、前記ステップＳ５でのＩＰトレーラ２２（＝Ｅ）の復元処理に代えて、上記分割したデータ（Ｆ１，Ｆ２）を結合して元のデータ（Ｅ）を復元する処理が必要となる。この変形例１は、ＩＰトレーラ２２のサイズが、ＵＤＰトレーラ２４のＵＤＰデータ部２６

のサイズより大きい場合に適している。

【００６０】

［変形例２］

変形例２は、前記ステップＳ３でＩＰトレーラ２２（＝Ｅ）をそのままデータＦとする処理に代えて、当該ＩＰトレーラ２２（＝Ｅ）を圧縮してトランスポート層１３４に渡す処理を適用したものである。この変形例２では、前記ステップＳ５でのＩＰトレーラ２２（＝Ｅ）の復元処理に代えて、上記圧縮したデータを解凍して元のデータ（Ｅ）を復元する処理が必要となる。この変形例２も、ＩＰトレーラ２２のサイズが、ＵＤＰトレーラ２４のＵＤＰデータ部２６のサイズより大きい場合に適している。

【００６１】

［変形例３］

変形例３は、前記ステップＳ３でＩＰトレーラ２２（＝Ｅ）をそのままデータＦとする処理に代えて、当該ＩＰトレーラ２２（＝Ｅ）を暗号化してトランスポート層１３４に渡す処理を適用したものである。この変形例２では、前記ステップＳ５でのＩＰトレーラ２２（＝Ｅ）の復元処理に代えて、上記暗号化したデータを復号して元のデータ（Ｅ）を復元する処理が必要となる。

【００６２】

［変形例４］

変形例４は、上記変形例１乃至変形例３の処理の少なくとも２つを組み合わせたものである。

【００６３】

［変形例５］

変形例５は、ゲートウェイ１３からサーバへのパケット送信に適用する専用プロトコルとしてＵＤＰに代えてＴＣＰを適用したものである。ここでは、ＵＤＰトレーラの代わりにＴＣＰトレーラを適用することになる。

【００６４】

［変形例６］

変形例６は、ゲートウェイ１３でクライアントからのＩＰＳ宛てのパケットを受け取った場合に、そのクライアントのＩＰアドレス（送信元ＩＰアドレス）の奇数（ｏｄｄ）／偶数（ｅｖｅｎ）、更に具体的に述べるならば当該ＩＰアドレスのホストアドレス部の奇数／偶数により、送信先サーバ（先の例であればＩＰＳがＯＮのサーバ）をＩＰアドレスがＩＰＡのサーバ１２Ａとするか、ＩＰＢのサーバ１２Ｂとするかを決定するようにしたものである。但し、該当するサーバがダウンしている場合には、送信元ＩＰアドレスの奇数／偶数に無関係に、もう一方のサーバに決定される。したがって、変形例６では、ＩＰアドレス対応テーブル１３１において、ＩＰＳ（仮想ＩＰアドレス）及び実ＩＰアドレスと組をなすフラグ情報は、当該実ＩＰアドレスが割り当てられているサーバでＩＰＳがＯＮ設定されているか否かというよりも、当該サーバが動作可能であるか或いはダウンしているかを示すようにするとよい。勿論、サーバが動作可能な場合に、そのサーバではＩＰＳがＯＮ設定され、ダウンしている場合に、そのサーバではＩＰＳがＯＦＦ設定されていると見なすこともできる。ここでは、サーバ１２Ａ，１２Ｂは動作状態にある場合に定期的にゲートウェイ１３にＯＮ通知を行い、ゲートウェイ１３では同一サーバから一定期間以上ＯＮ通知がない場合に、該当するフラグ情報をＯＦＦする方法を適用するのが、最も簡単でよい。また、ゲートウェイ１３から各サーバ１２Ａ，１２Ｂに定期的に問い合わせを行い、応答の有無に応じて該当するフラグ情報をＯＮ／ＯＦＦ設定するようにしても構わない。

【００６５】

以下、ゲートウェイ１３でクライアントからのパケットを受け取った場合の、ゲートウェイプログラム１３６に従う変形例６の処理手順について、図１２のフローチャートを参照して説明する。

【００６６】

まず、受信パケットのＩＰトレーラ２２が取り出されて、ＩＰヘッダ２３中の宛先ＩＰアドレス２３１がチェックされる（ステップＳ４１）。もし、宛先ＩＰアドレス２３１がＩＰＳ以外であるならば、前記実施形態と同様に、ＩＰトレーラ２２をそのままインターネット層１３３に渡す処理（ステップＳ２）に進む。

【００６７】

これに対し、宛先ＩＰアドレス２３１がＩＰＳに一致するならば、上記ＩＰヘッダ２３中の送信元ＩＰアドレス２３２が奇数または偶数のいずれであるかがチェックされる（ステップＳ４２）。

【００６８】

上記ＩＰアドレスが例えば奇数であり、且つＩＰアドレス対応テーブル１３１中のＩＰＡと組をなすフラグ情報がＯＮ状態にあるならば、即ちＩＰＡが割り当てられているサーバ１２Ａがダウンしていないならば、新たな宛先ＩＰアドレスとしてＩＰＡを選択する（ステップＳ４３，Ｓ４４）。この場合、クライアント１２ＣからのＩＰトレーラ２２（リクエスト）はサーバ１２Ａで処理される。これに対し、上記ＩＰアドレスが奇数であっても、ＩＰアドレス対応テーブル１３１中のＩＰＡと組をなすフラグ情報がＯＦＦ状態にあるならば、即ちＩＰＡが割り当てられているサーバ１２Ａがダウンしているならば、サーバ１２Ｂに割り当てられているＩＰＢを選択する（ステップＳ４３，Ｓ４５）。

【００６９】

一方、上記ＩＰアドレスが偶数であり、且つＩＰアドレス対応テーブル１３１中のＩＰＢと組をなすフラグ情報がＯＮ状態にあるならば、即ちＩＰＢが割り当てられているサーバ１２Ｂがダウンしていないならば、新たな宛先ＩＰアドレスとしてＩＰＢを選択する（ステップＳ４７，Ｓ４５）。この場合、クライアント１２ＣからのＩＰトレーラ２２（リクエスト）はサーバ１２Ｂで処理される。これに対し、上記ＩＰアドレスが偶数であっても、ＩＰアドレス対応テーブル１３１中のＩＰＢと組をなすフラグ情報がＯＦＦ状態にあるならば、即ちＩＰＢが割り当てられているサーバ１２Ｂがダウンしているならば、サーバ１２Ａに割り当てられているＩＰＡを選択する（ステップＳ４７，Ｓ４４）。

【００７０】

以上のようにして新たな宛先ＩＰアドレスとしての実ＩＰアドレスを選択した後の処理は前記実施形態におけるステップＳ２３と同様であり、受信パケットのＩＰトレーラ２２（ここではＥ）の処理が行われる（ステップＳ４６）。

【００７１】

このように、サーバ１２Ａ及び１２Ｂの両方に有効な仮想ＩＰアドレスＩＰＳが設定されていたとしても、クライアント１２ＣからのＩＰＳ宛ての（パケット２０中の）ＩＰトレーラ２２は、そのクライアント１２Ｃに割り当てられているＩＰアドレスＩＰＣが奇数または偶数のいずれであるかにより、サーバ１２Ａまたは１２Ｂの一方でのみ処理され、そのサーバとクライアント１２Ｃとの間でのみ通信が行われる。つまり、サーバ１２Ａ，１２Ｂのいずれか一方のみが要求元のクライアント１２Ｃにサービスを提供するという、ＷＡＮ環境におけるＩＰアドレステイクオーバが実現される。。

【００７２】

したがって、クライアント１２Ｃと同様のクライアントが複数存在し、各クライアントに設定されているＩＰアドレスが偶数アドレス、奇数アドレスほぼ同数の場合には、全クライアントの半数はサーバ１２Ａからサービスの提供を受け、残りの半数はサーバ１２Ｂからサービスの提供を受けることができ、負荷分散（ロードバランス）が図られる。

【００７３】

なお、サーバの数が３台以上の場合には、その数をＮとすると、ＩＰＳ宛てのパケット２０の送信元ＩＰアドレス２３２がＮ・ｎ＋（ｉ－１）（但し、ｎ＝０，１，２…）のときに、ｉ番目（ｉ＝１～Ｎ）のサーバのＩＰアドレスを選択することにより、Ｎ台のサーバ間で負荷分散を図ることができる。

【００７４】

この他に、ゲートウェイ１３が各サーバに負荷状態を定期的に問い合わせることで、或い

は各サーバがゲートウェイ１３に自身の負荷状態を定期的に通知することで、各サーバの負荷状態を把握し、その負荷状態に応じてクライアントからのリクエストを処理するサーバを決定することによっても、サーバ間の負荷分散を図ることができる。

【００７５】

【発明の効果】

以上詳述したように本発明によれば、テイクオーバされる仮想ネットワークアドレス宛てのネットワークトレーラを含む通信パケットは、クライアント計算機から全てゲートウェイに送られる構成とし、当該ゲートウェイでは、そのネットワークトレーラを、自身の持つネットワークアドレス対応情報登録手段により示されている、上記仮想ネットワークアドレスが有効なサーバ計算機に固有の実ネットワークアドレス宛ての新たなネットワークトレーラに梱包して送信し、サーバ計算機では、自身に関する仮想ネットワークアドレスの状態をゲートウェイに通知してネットワークアドレス対応情報登録手段の登録内容に反映させる一方、ゲートウェイにより送信された、クライアント計算機からのネットワークトレーラが梱包されたネットワークトレーラを受信した場合には、梱包されたネットワークトレーラを開封する構成としたので、ＷＡＮ環境で接続されている遠く離れて配置されたサーバ計算機間でも、近接配置されたサーバ計算機間と同様にネットワークアドレスの切り替えによりサービスの引き継きが実現できる。

【００７６】

また本発明によれば、クライアント計算機からの仮想ネットワークアドレス宛てのネットワークトレーラを、ゲートウェイにおいて新たなネットワークトレーラに梱包する際に設定する、当該新たなネットワークトレーラの宛先ネットワークアドレスを、クライアント計算機に固有のネットワークアドレス、または各サーバ計算機の負荷状態に基づいて切り替えるようにしたので、負荷分散も実現できる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る耐障害コンピュータシステム。

【図２】同実施形態で適用される通信パケットの概略フォーマットを示す図。

【図３】図１中のサーバ１２Ａ，１２Ｂの構成を示すブロック図。

【図４】図１中のゲートウェイ１３の構成を示すブロック図。

【図５】図１のシステムの動作を、サーバ１２ＡにおいてＩＰアドレスＩＰＳがＯＮされている状態で、クライアント１２ＣがＩＰＳ宛ての通信パケット２０（＝Ｄ）を送信する場合を例に説明するための第１の動作説明図。

【図６】図１のシステムの動作を、サーバ１２ＡにおいてＩＰアドレスＩＰＳがＯＮされている状態で、クライアント１２ＣがＩＰＳ宛ての通信パケット２０（＝Ｄ）を送信する場合を例に説明するための第２の動作説明図。

【図７】図１のシステムの動作を、サーバ１２ＡにおいてＩＰアドレスＩＰＳがＯＮされている状態で、クライアント１２ＣがＩＰＳ宛ての通信パケット２０（＝Ｄ）を送信する場合を例に説明するための第３の動作説明図。

【図８】図１のシステムの動作を、サーバ１２ＡにおいてＩＰアドレスＩＰＳがＯＮされている状態で、クライアント１２ＣがＩＰＳ宛ての通信パケット２０（＝Ｄ）を送信する場合を例に説明するための第４の動作説明図。

【図９】図１のシステムの動作を、サーバ１２ＡにおいてＩＰアドレスＩＰＳがＯＮされている状態で、クライアント１２ＣがＩＰＳ宛ての通信パケット２０（＝Ｄ）を送信する場合を例に説明するための第５の動作説明図。

【図１０】図１のシステムの変形例を示すブロック図。

【図１１】クライアント１２ＣからＩＰＳ宛てのパケットを送信する場合のデータの経路を、図１のシステムと図１０のシステムのそれぞれについて対比して示す図。

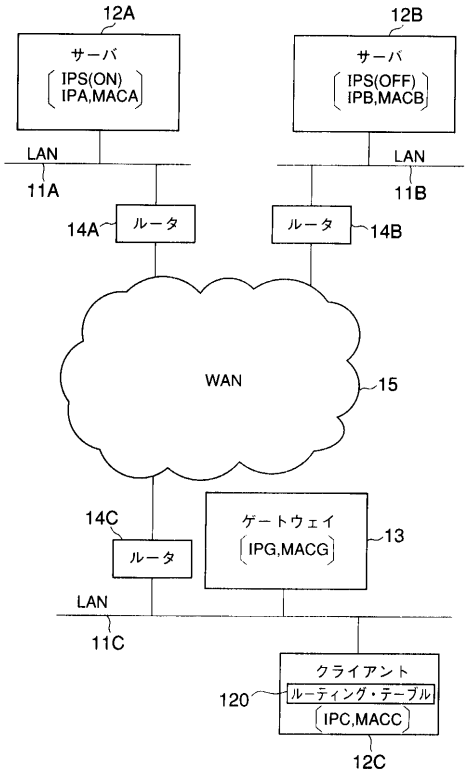
【図１２】ゲートウェイ１３でクライアントからのパケットを受け取った場合の、ゲートウェイプログラム１３６に従う処理手順の変形例を説明するためのフローチャート。

【符号の説明】

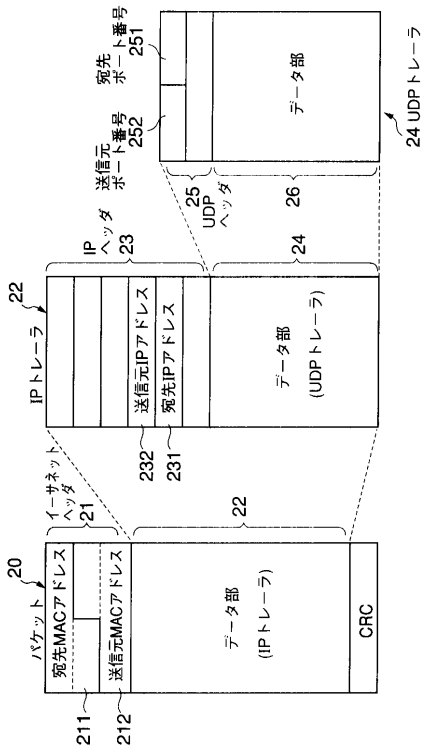
１１Ａ，１１Ｂ，１１Ｃ…ＬＡＮ

１２Ａ，１２Ｂ…サーバ（サーバ計算機）
１２Ｃ…クライアント（クライアント計算機）
１３…ゲートウェイ（梱包手段）
１４Ａ，１４Ｂ，１４Ｃ…ルータ
１２０…ルーティング・テーブル（経路情報登録手段）
１２１…特定アプリケーション（通知手段）
１２５…通信ドライバ
１２７…フィルタドライバ
１３１…ＩＰアドレス対応テーブル（ネットワークアドレス対応情報登録手段）
１３５…通信ドライバ（梱包手段）
１３６…ゲートウェイプログラム（梱包手段）

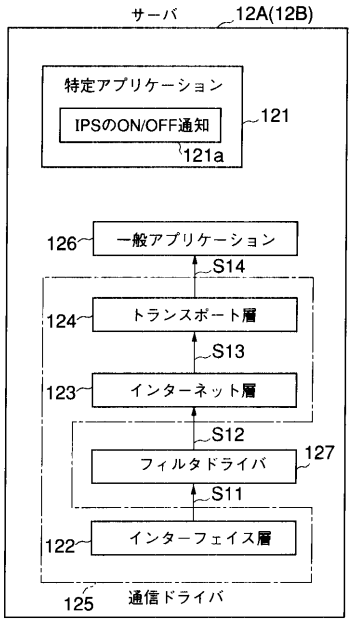
【図１】



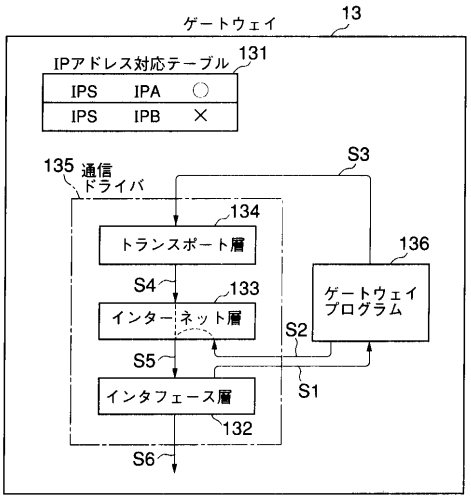
【図２】



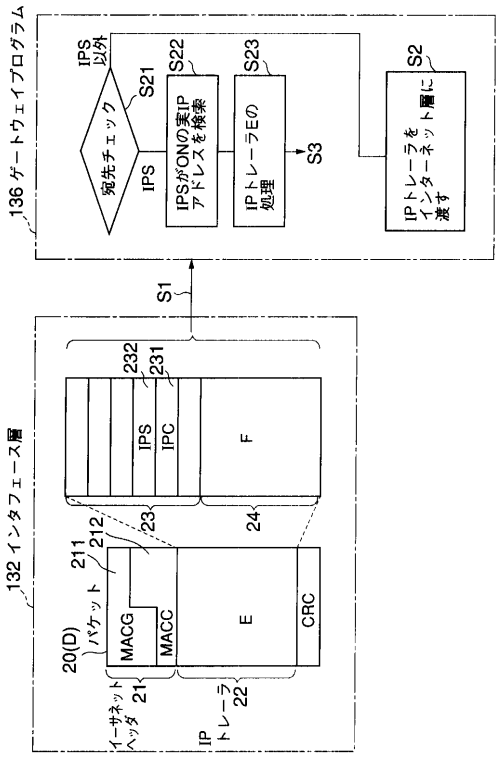
【図３】


サーバ
12A(12B)
特定アプリケーション
IPSのON/OFF通知
121
121a
126
一般アプリケーション
S14
124
トランスポート層
S13
123
インターネット層
S12
フィルタドライバ
127
S11
122
インターフェイス層
125
通信ドライバ

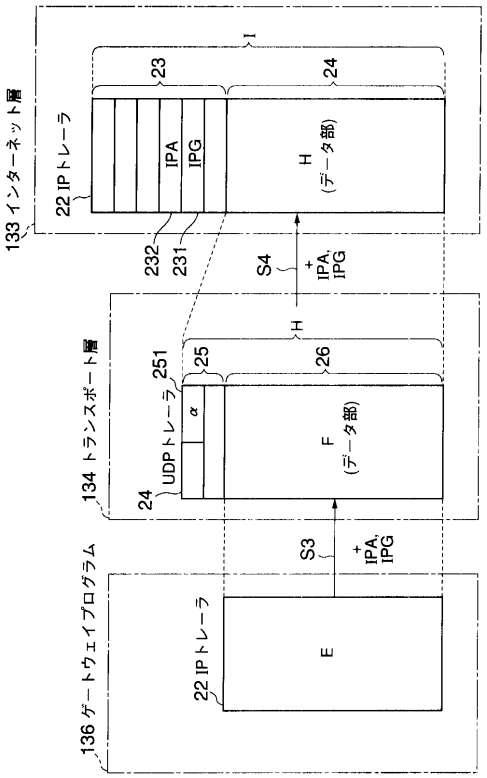
【図４】


ゲートウェイ
13
IPアドレス対応テーブル
131
IPS IPA ○
IPS IPB ×
135
通信ドライバ
S3
134
トランスポート層
136
ゲートウェイプログラム
S4
133
インターネット層
S2
S5
S1
インタフェース層
132
S6

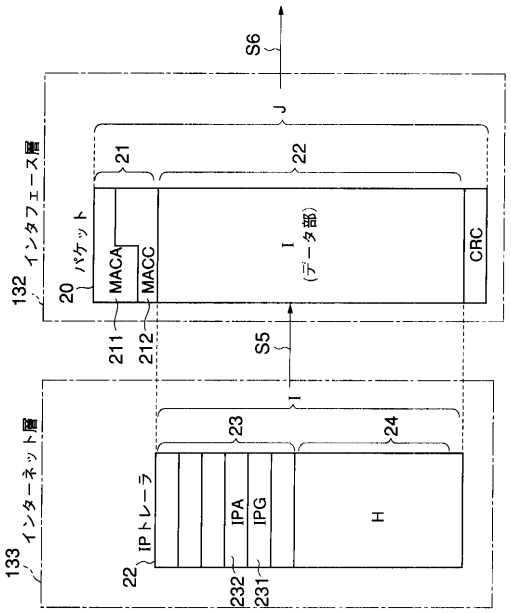
【図５】


136 ゲートウェイプログラム
IPS以外
宛先チェック
IPS
S21
S22
IPSがONの実IPアドレスを検索
S23
IPトレーラEの処理
S3
S2
IPトレーラをインターネット層に渡す
S1
132 インタフェース層
232
231
IPS
IPC
F
212
211
23
24
20(D)
パケット
MACG
MACC
E
CRC
イーサネットヘッダ
21
IPトレーラ
22

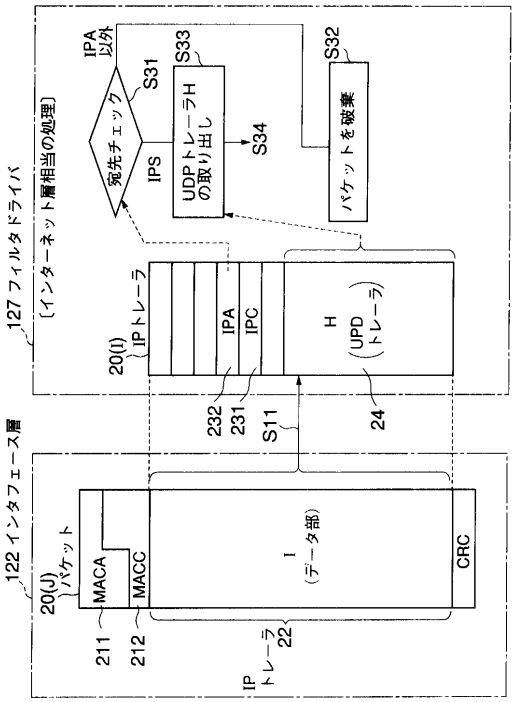
【図６】


133 インターネット層
22 IPトレーラ
23
24
IPA
IPG
H
(データ部)
232
231
S4
+IPA,IPG
134 トランスポート層
251
25
26
UDPトレーラ
α
F
(データ部)
24
S3
136 ゲートウェイプログラム
22 IPトレーラ
E

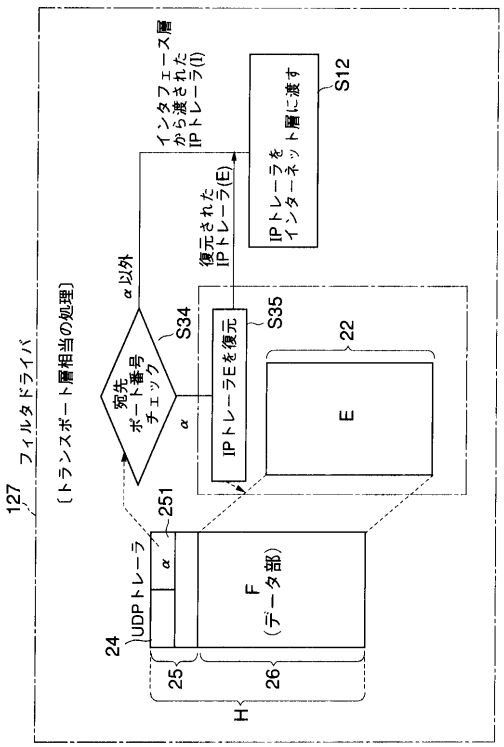
【図７】


S6
J
インタフェース層
132
20
パケット
21
22
MACA
MACC
I
(データ部)
CRC
211
212
S5
I
インターネット層
133
23
24
IPトレーラ
IPA
IPG
H
22
232
231

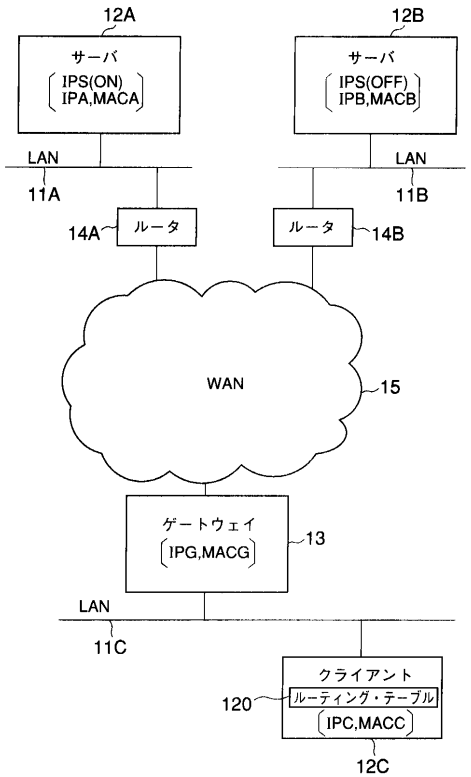
【図８】


127 フィルタドライバ
〔インターネット層相当の処理〕
IPA以外
S31
宛先チェック
IPS
S33
UDPトレーラHの取り出し
S34
S32
パケットを破棄
20(I)
IPトレーラ
IPA
IPC
H
(UPD トレーラ)
232
231
S11
24
122 インタフェース層
20(J)
パケット
MACA
MACC
I
(データ部)
CRC
211
212
IP トレーラ
22

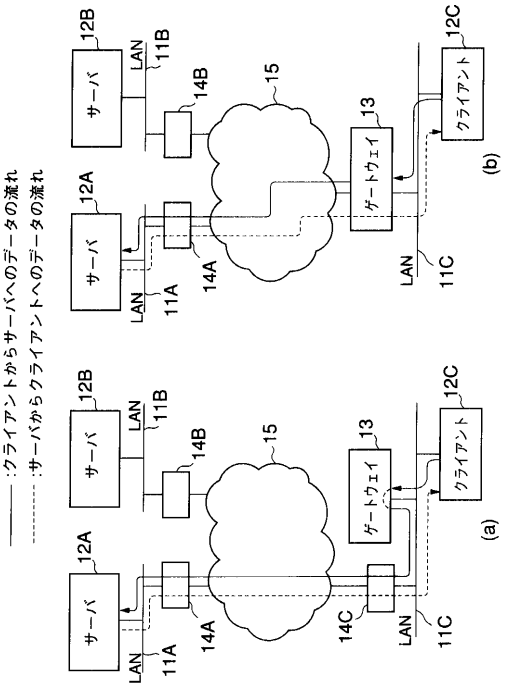
【図９】


127 フィルタドライバ
〔トランスポート層相当の処理〕
インタフェース層
から送された
IPトレーラ(I)
S12
IPトレーラを
インターネット層に渡す
復元された
IPトレーラ(E)
α以外
S34
宛先
ポート番号
チェック
α
S35
IPトレーラEを復元
22
E
251
UDPトレーラ
α
F
(データ部)
24
25
26
H

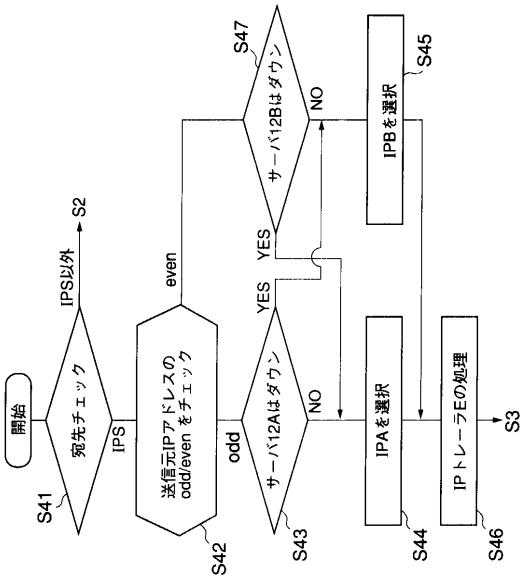
【図１０】


12A
サーバ
IPS(ON)
IPA,MACA
12B
サーバ
IPS(OFF)
IPB,MACB
LAN
11A
LAN
11B
14A
ルータ
ルータ
14B
WAN
15
ゲートウェイ
IPG,MACG
13
LAN
11C
クライアント
ルーティング・テーブル
IPC,MACC
120
12C

【図１１】


——：クライアントからサーバへのデータの流れ
------：サーバからクライアントへのデータの流れ
12A
12B
12C
サーバ
LAN
11A
11B
11C
14A
14B
14C
15
ゲートウェイ
13
クライアント
(a)
(b)

【図１２】


開始
S41
宛先チェック
IPS
IPS以外
S2
送信元IPアドレスの
odd/even をチェック
S42
odd
even
サーバ12Aはダウン
S43
YES
NO
サーバ12Bはダウン
S47
IPAを選択
S44
IPBを選択
S45
IPトレーラEの処理
S46
S3

フロントページの続き

(72)発明者　渡邊　誠
東京都府中市東芝町１番地　株式会社東芝府中工場内

審査官　▲高▼橋　正▲徳▼

(56)参考文献　特開平１０－２２４３７８（ＪＰ，Ａ）
特開平０６－２０５０１４（ＪＰ，Ａ）
特開平１０－２００５７８（ＪＰ，Ａ）
特開平０９－１４８９９３（ＪＰ，Ａ）
特開平１０－０９３６５５（ＪＰ，Ａ）
特開平０６－３３７８２４（ＪＰ，Ａ）
特開平１０－１０５４２４（ＪＰ，Ａ）
特開平０９－０３４８１４（ＪＰ，Ａ）
特開平０６－１８７２７６（ＪＰ，Ａ）
特開平１１－０５５３２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F11/16-11/20,
G06F15/16-15/177,
G06F13/00