(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4241760号
(P4241760)
(45)発行日　平成21年3月18日(2009.3.18)　(24)登録日　平成21年1月9日(2009.1.9)

(51)Int.Cl.　F I
G06F 9/50 (2006.01)　G06F 9/46 465D

請求項の数 6 (全 21 頁)

(21)出願番号　特願2006-138431(P2006-138431)
(22)出願日　平成18年5月18日(2006.5.18)
(62)分割の表示　特願2005-125850(P2005-125850)の分割
原出願日　平成17年4月25日(2005.4.25)
(65)公開番号　特開2006-309777(P2006-309777A)
(43)公開日　平成18年11月9日(2006.11.9)
審査請求日　平成20年4月22日(2008.4.22)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　湯本　一磨
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　川井　恵理
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
(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
最終頁に続く

(54)【発明の名称】負荷分散システム

(57)【特許請求の範囲】
【請求項１】
自ドメイン内の複数の端末と複数のサーバと他ドメインのパケット送信元に接続された負荷分散装置であって、
ペイロードを含むパケットを受信する送受信部と、
記憶装置と、
受信したパケットの送信元を前記ペイロードに記述された情報に基づいて判定する制御部とを有し、
上記記憶装置は、自ドメイン内の端末と該端末に関するセッション制御を行うサーバとの対応関係を記憶しており、
上記制御部の上記判定の結果、送信元が上記自ドメイン内の端末であると判定された場合には、上記複数のサーバのうち該端末に関するセッション制御を行うサーバを上記対応関係に基づいて決定し、該決定されたサーバのアドレスを上記送受信部を介して該端末に通知し、
上記制御部の上記判定の結果、送信元が上記他ドメインのパケット送信元であると判定された場合には、前記ペイロードに記述される情報により特定される自ドメイン内の端末に関するセッション制御を行うサーバに上記パケットを上記送受信部を介して送信し、
さらに、上記対応関係には有効期限が設定されており、該有効期限を過ぎた場合には、上記自ドメイン内の端末からの接続及び上記自ドメイン内の端末への接続を拒否することを特徴とする負荷分散装置。

【請求項２】
請求項１記載の負荷分散装置であって、
上記判定の結果、送信元が上記他ドメインのパケット送信元であると判定された場合には、上記対応関係を参照して前記ペイロードに記述される情報により特定される自ドメイン内の端末に関するセッション制御を行うサーバを検索し、検索された上記サーバに上記パケットを上記送受信部を介して送信することを特徴とする負荷分散装置。
【請求項３】
請求項１記載の負荷分散装置であって、
上記判定の結果、送信元が上記自ドメイン内の端末であると判定された場合には、上記対応関係を参照し、利用端末数が最も少ないサーバを該端末に関するセッション制御を行うサーバと決定することを特徴とする負荷分散装置。
【請求項４】
自ドメイン内の複数の端末と他ドメインのパケット送信元とに接続された負荷分散システムであって、
複数のサーバと負荷分散装置を備え、
該負荷分散装置は、
ペイロードを含むパケットを受信する送受信部と、
記憶装置と、
前記ペイロードに記述された情報に基づいて受信したパケットの送信元を判定する制御部を有し、
上記記憶装置は、上記自ドメイン内の複数の端末のアドレスと該端末に関するセッション制御を行うサーバの対応関係を記憶しており、
上記判定の結果、送信元が上記自ドメイン内の端末であると判定された場合には、上記複数のサーバのうち該端末に関するセッション制御を行うサーバを決定し、該決定されたサーバのアドレスを上記送受信部を介して該端末に通知し、
上記判定の結果、送信元が上記他ドメインのパケット送信元であると判定された場合には、前記ペイロードに記述される情報により特定される自ドメイン内の端末に関するセッション制御を行うサーバに上記パケットを上記送受信部を介して送信し、
さらに、上記対応関係には有効期限が設定されており、該有効期限を過ぎた場合には、上記負荷分散装置は上記自ドメイン内の端末からの接続及び上記自ドメイン内の端末への接続を拒否することを特徴とする負荷分散システム。
【請求項５】
請求項４記載の負荷分散システムであって、　上記負荷分散装置は、　上記判定の結果、送信元が上記他ドメインのパケット送信元であると判定された場合には、上記対応関係を参照して前記ペイロードに記述される情報により特定される自ドメイン内の端末に関するセッション制御を行うサーバを検索し、検索された上記サーバに上記パケットを上記送受信部を介して送信することを特徴とする負荷分散システム。
【請求項６】
請求項４記載の負荷分散システムであって、
上記負荷分散装置は、上記判定の結果、送信元が上記自ドメイン内の端末であると判定された場合には、上記対応関係を参照し、利用端末数が最も少ないサーバを該端末に関するセッション制御を行うサーバと決定することを特徴とする負荷分散システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セッション制御および管理を行う装置が、受信したメッセージの中継先を決定する技術に係わり、特に、複数のセッション制御装置に負荷を分散して通信処理を行う技術に関する。
【背景技術】
【０００２】

従来、負荷分散装置は、Webサーバに対するトラフィックを、同じ機能を持った複数台のWebサーバで分担することにより、膨大なトラフィックに対応させることを目的として発展してきた。現在では、Webサーバ以外にも、ルータ、メールサーバ、VPNゲートウェイなど、多様な機器やプロトコルを対象として広げつつ発展してきている。

【０００３】

その中には、SIPサーバを対象とした負荷分散を実現する装置も含まれており、SIP（Session Initiation Protocol）（非特許文献１参照）固有の仕様を考慮して、同一ダイアログのトラフィックを同じサーバに振り分ける機能を備えている。同一ダイアログのトラフィックを同じサーバに振り分ける機能（パーシステンス機能）の典型的な方式としては、SIPヘッダに含まれるCall-Idの値を参照し、この値が同一であるメッセージは同じサーバに振り分けるという方式が採られている。

【０００４】

また、暗号化通信への対応に関しても、SSL（Secure Socket Layer）を使ったHTTPS（Hypertext Transfer Protocol Security）による暗号化通信をサポートした装置なども存在する。

負荷分散装置の実現方法としては、負荷分散装置が振り分け先サーバのアドレスを端末に通知し、負荷分散装置が指定した振り分け先サーバに端末が再接続することを促す方法がある（例えば、特許文献１参照）。

【０００５】

【特許文献１】特開2002－334012

【非特許文献１】RFC 3261

【発明の開示】

【発明が解決しようとする課題】

【０００６】

従来の負荷分散装置では、IPパケットのペイロード部分に含まれる情報（例えばSIPメッセージのようなレイヤ７の情報、アプリケーション層の情報）を参照して振分け先を決定する場合には、一旦負荷分散装置において暗号化通信を終端し、復号化処理を行う必要がある。

本発明の第一の課題及び目的は、この復号化処理のために、負荷分散装置の処理負荷が増大して負荷分散の効果が薄れてしまったり、転送遅延が起きてしまうのを防ぐことである。

【０００７】

従来のリダイレクト通知を利用した負荷分散装置では、振り分け先を端末に通知するステップまでしか考慮されていないため、一旦通知した振り分け先を、端末が永久に使い続けてしまう場合がある。

本発明の第二の課題及び目的は、このように特定の振り分け先に対して長い間処理負荷が集中し、負荷分散という効果が薄れてしまうことを防ぐことである。

【０００８】

従来のリダイレクト通知を利用した負荷分散装置では、接続または処理のリクエストはリダイレクト通知に応対する機能を有する端末から送信されることを前提としていたため、リダイレクト通知に応対する機能を有さないサーバなど（例えば、一般的なSIPプロキシサーバ）からのリクエストには対応できない。

本発明の第三の課題及び目的は、このようにリダイレクト通知に応対する機能を有さないサーバからの接続または処理のリクエストに対応することである。

【０００９】

従来の負荷分散装置では、負荷分散装置によって振り分けられた振り分け先と端末が継続的なコネクションを確立している最中に、別の端末またはサーバからこの端末への接続要求があった場合、前記の継続的なコネクションを確立している振分け先とは異なる振分け先にこの接続要求を振り分けてしまう場合がある。

本発明の第四の課題及び目的は、一つの端末に応対するために複数の振分け先のリソース

が消費されてしまうことを防ぐことである。
【００１０】
従来の負荷分散装置では、端末やサーバが接続要求を負荷分散装置に送信することなく振分け先の一つに直接送信してしまった場合には、負荷分散装置がこの接続要求を検知することができず、その結果負荷分散装置が指示した通りに負荷が分散されない場合がある。
本発明の第五の課題及び目的は、負荷分散装置が割当てていない振分け先への接続を防ぐことである。
【課題を解決するための手段】
【００１１】
上記第一の課題に対する解決手段として、本発明の負荷分散装置は、受信したIPパケットの上位レイヤでの直前の送信元が端末か否かを判定し、直前の送信元が端末である場合には該端末に応対する振分け先を決定し、該端末に振分け先のアドレスを通知する（リダイレクト）。また、このとき端末はリダイレクトによって通知された振分け先へ上記IPパケットを再送信する。
【００１２】
上記第二の課題に対する解決手段として、本発明では、端末に応対する振分け先に有効期限を設け、この有効期限を過ぎた場合は、振分け先への上記端末の接続を拒否する。
【００１３】
上記第三の課題に対する解決手段として、本発明の負荷分散装置は、受信したIPパケットの上位レイヤでの直前の送信元がサーバか否かを判定し、直前の送信元がサーバである場合には、該IPパケットの送信先の端末に応対する振分け先に該IPパケットを送信する。
【００１４】
上記第四の課題に対する解決手段として、本発明の負荷分散装置は、振り分け先と端末が継続的なコネクションを確立している最中に、別の端末またはサーバからこの端末への別の接続要求があった場合、この別の接続要求を前記の継続的なコネクションを確立している振分け先へ送信する。
【００１５】
上記第五の課題に対する解決手段として、本発明では、負荷分散装置が割当てていない振分け先に端末やサーバが直接接続要求を送信した場合には、この接続要求を拒否する。
【発明の効果】
【００１６】
上記第一の課題に対する解決手段により、負荷分散装置は暗号化通信の終端、つまり復号化処理を行う必要がなくなる。これにより、負荷分散装置の処理を軽減でき、負荷分散装置本来の負荷分散が達成でき、負荷分散装置での復号化処理による転送遅延も防ぐことができる。
【００１７】
上記第二の課題に対する解決手段により、端末が一つの振分け先を永久に使い続けることがなくなる。これにより、特定の振分け先に長い間処理が集中することを防ぐことができ、負荷分散装置本来の負荷分散が達成できる。
【００１８】
上記第三の課題に対する解決手段により、リダイレクト通知に応対する機能を有しない送信元からの接続または処理の要求も各々の振分け先に振り分けることができる。これにより、リダイレクト通知に応対する機能を有しない送信元からの接続または処理の要求に関しても負荷分散を実現できる。
【００１９】
上記第四の課題に対する解決手段により、端末が継続的なコネクションを確立している振分け先のリソースを有効に利用でき、かつ一つの端末に応対するために複数の振分け先のリソースが消費されるのを防ぐことができる。
【００２０】

上記第五の課題に対する解決手段により、端末またはサーバが負荷分散装置が割当てていない振分け先へ勝手に接続するのを防ぐことができる。これにより、負荷分散装置本来の負荷分散が達成できる。

【実施例１】

【００２１】

図１は、本実施形態に係わるSIP負荷分散装置の一構成例を示す図である。本実施例では、SIPを例に挙げているが、その他のアプリケーションレイヤのプロトコル（他のセッション制御プロトコルなど）に適用してもよい。SIP負荷分散装置1は、CPU（10）、メモリ（16）、記憶装置（14）、ネットワークインターフェース（12）を備え、以降に詳しく説明する制御用プログラムが格納されている。SIP負荷分散装置が動作する際には、筐体内に設けられたメモリ上に制御プログラムが展開され、CPUで制御プログラムが実行される。記憶装置は筐体内部に実装される形態でも、外部記憶装置として別筐体で設置される形態でも、ネットワークで接続される形態でも構わない。

【００２２】

また、図１に示した負荷分散装置は、装置管理権限を持つユーザなどが負荷分散装置を操作するためのユーザインタフェースを備えていてもよい。ユーザインタフェースとしては、例えば、コマンド入力のためのキーボードや、ＧＵＩ入力のためのマウス、表示画面などを備えているとよい。

【００２３】

上記制御用プログラムの詳細を、図１の20から27に示すブロック構成図を用いて説明する。SIP負荷分散装置は、パケットの送受信を行うネットワークインターフェース12と、ＣＰＵ10とＨＤＤ(Hard Disc Drive)14と、メモリ16とからなる。メモリ16には、通信制御プログラム20、SIPスタックプログラム21、送信元判定プログラム22、リダイレクトプログラム23、ステートレスプロキシプログラム24、負荷分散管理プログラム25、負荷分散管理テーブル26、ロケーション制御プログラム27が格納されている。

【００２４】

通信制御プログラム20は、ネットワークインターフェース12を介して受信したパケットの解析と、パケットの送信を行う際に必要となるヘッダ情報の整形操作および送信を行う。SIPスタックプログラムは、受信パケットの内容がSIPメッセージだった場合にはメッセージ解析を行い、送信パケットの内容がSIPメッセージの場合にはSIPヘッダ情報の整形操作と通信制御プログラム20を通じた送信処理を行う。送信元判定プログラム22は、SIPメッセージを受信した際に直前のホップの送信元が自身が責任を負うドメイン内の端末7からであるか否かの判定を行う。リダイレクトプログラム25は、直前ホップの送信元が自身が責任を負うドメイン内の端末からであった場合に、負荷分散管理テーブル26から負荷分散管理プログラム25を通じてこの送信元端末に応対するSIPサーバ2のアドレスを取得し、取得したSIPサーバのアドレスを端末7に通知する。ロケーション制御プログラム27は、負荷分散管理プログラム25が端末7に対して応対するSIPサーバを新たに割り当て、負荷分散管理テーブル26に新規登録した際に、端末7と応対するSIPサーバ2の対応関係をロケーションDB(Data Base)3に通知して登録を促す。

【００２５】

ステートレスプロキシプログラム24は、直前ホップの送信元が自身が責任を負うドメイン内の端末以外からであった場合に、宛先端末7がオンライン時にどのSIPサーバ2に振り分けられているかを、負荷分散管理テーブル26から負荷分散管理プログラム25を通じて取得し、取得したSIPサーバにメッセージをステートレスプロキシとして中継する。

【００２６】

ここでステートレスプロキシとは、ダイアログの管理もトランザクションの管理も行わず、宛先解決した結果に従って単純に受信したメッセージを中継するプロキシのことをいう。従ってステートレスプロキシの場合、例えばあるリクエストメッセージの中継を行ったとしても、これに対するレスポンスメッセージの通信経路には含まれないことがある。これに対してトランザクションステートフルプロキシとは、リクエストとレスポンスの対

を管理し、必要に応じて再送制御などを行うプロキシをいう。更に、IP電話における発信時のリクエストから切断時のレスポンスまでのダイアログを管理し、状態遷移モデルに合致しないトラフィックを排除したり、通信ログを課金管理に活用したりするトランザクションステートフルプロキシをコールステートフルプロキシという。

【００２７】

負荷分散管理テーブル26は、端末7と応対するSIPサーバ2との対応関係を記憶して管理する。負荷分散管理プログラム25は、負荷分散管理テーブル26の情報を参照・更新する。ここで、負荷分散管理テーブル26はＨＤＤ14内に格納されていてもよい。

本実施例では、図１の20から27に示した各機能ブロックが、全てソフトウェア処理により実現するものと仮定しているが、機能ブロックそれぞれに対応するプロセッサや信号処理回路などを用いて、ハードウェア的に図１の構成を実現しても構わない。

【００２８】

図２は、本実施形態に係わるSIP負荷分散システムの一構成例を示す図である。SIP負荷分散システムは、ユーザA1およびユーザA1が所有する端末7aと、ユーザA1もしくはユーザA1とは別のユーザAnが所有する端末7nなど、複数の端末7が属するドメインA30と、ユーザBおよびユーザBが所有する端末8が属するドメインB35で構成される。ドメインBは、ドメインAと異なるドメインの存在を一例として示しているものであり、更に異なる複数のドメインを加えてネットワークシステムを構成してもよい。また、ドメインB内には端末8と、端末8を収容し、端末8のセッションを制御するSIPサーバb4とがネットワーク6で接続された構成を図示しているが、ドメインB内の構成もドメインA内の構成と同様に、複数台の端末と複数台のSIPサーバで構成される形態でも構わない。

【００２９】

本実施形態に係わるSIP負荷分散システムの特徴の一つは、ドメインA内の構成のように、複数台の端末7a～7nとの通信を複数台のSIPサーバ2a～2nで分担して対応させる際に、SIP負荷分散装置1が端末7からの問合せに対して、応対するSIPサーバ2のアドレスを通知する機能を有することにある。この時、当該ドメインに属するユーザおよび端末の情報を管理するロケーションDB3は、各SIPサーバ2a～2nが共通に利用する。また、SIP負荷分散装置1、SIPサーバ2a～2n、ロケーションDB3と、端末7a～7nはネットワーク5で接続されている。更に、ドメインAとドメインBも相互にネットワークで接続されているものとする。図２では、ロケーションDB3に対するアクセスが端末7や他ドメインの装置からも可能であるかのようにみえるかもしれないが、SIP負荷分散装置1およびSIPサーバ2a～2nのみからアクセスが可能なようにネットワークを分けてもよい。この場合、よりセキュリティが確保される。

【００３０】

図３は、本実施形態に係わるSIP負荷分散システムにおいて、端末7からのメッセージがSIP負荷分散装置1を通じてSIPサーバ2に振り分けられるまでのシーケンスの一例を示した図である。

【００３１】

本実施形態における端末7は、暗号化通信を行う場合には、事前にRFC3329で規定されているセキュリティ方式のネゴシエーションを行うものとする。よって、図３から図６ではセキュリティ方式のネゴシエーションが完了するまでは非暗号化（平文）通信を行うという前提でシーケンスおよびメッセージの例を示している。但し、本発明の効果を奏する限り、他の暗号化通信方式を適用してもよい。

【００３２】

また、図４に例示した端末からSIP負荷分散装置に送るメッセージ（F40）には、セキュリティ方式のネゴシエーション情報（Security-Clientヘッダ）を含まない一般的なREGISTER登録のリクエストメッセージを示しているが、F40のメッセージにセキュリティ方式のネゴシエーション情報が含まれていても構わない。

【００３３】

一方、図５に示したSIP負荷分散装置1から端末7へ応対するSIPサーバのアドレスを通知

するレスポンスメッセージ（F41）にはセキュリティ方式のネゴシェーション応答情報（Security-Serverヘッダ）を含まない302応答を使う。
これは、例えF40にセキュリティ方式のネゴシェーション情報が含まれていたとしても、負荷分散装置自体はこのネゴシェーションを行わないので、F41のメッセージにセキュリティ方式のネゴシエーション情報（Security-Serverヘッダ）は通常含めないからである。
但し、F41のメッセージでセキュリティ方式のネゴシエーション情報を含めてもよい。このとき、RFC3329の規定には反するが、302応答をF41として使ってもよい。あるいは、RFC3329の規定に従って、セキュリティ方式のネゴシェーション応答情報を指定可能な423応答もしくは429応答をF41として使ってもよい。

【００３４】
更に、本実施形態ではリダイレクト通知のメッセージとして302応答（F41）を用いる例を示しているが、端末との間のネットワークインターフェース仕様を統一すれば、300番台の他のレスポンスコードや、予約されていない独自のレスポンスコードを用いても構わない。

【００３５】
SIP負荷分散装置1には、管轄するドメインを代表するアドレスとして、バーチャルドメイン的なドメイン名（例：domainA.co.jp）を割り当てる。バーチャルドメイン的とは、実際に各メッセージを処理する各SIPサーバのアドレスの代わりにSIP負荷分散装置1のアドレスを公開するという意味である。端末7は利用開始時のREGISTERメッセージ（F40）を、このアドレス（すなわちSIP負荷分散装置）宛（50）に送信する。SIP負荷分散装置1は、送信元判定プログラム22により、受信したメッセージの直前ホップの送信元が端末7であると判定した場合、負荷分散管理プログラム25によって端末7に応対するSIPサーバ2を決定し、決定したSIPサーバのアドレスを302応答で端末7に通知する（F41）。この時のSIPサーバ2のアドレス通知方法としては、図５に示すように、Contactヘッダ（54）を利用する。

【００３６】
302応答（F41）を受信した端末は、302応答のContactヘッダで通知されたアドレス宛にメッセージを送りなおす（F42）。具体的なメッセージ内容は、図６に示すように、Request-Lineに302応答のContactヘッダで通知されたアドレスを指定する（56）。この時、ユーザもしくは端末に割り振られたSIP-URI（52、56）やコンタクトアドレス（53、59）の内容は、オリジナルのものと同一のままである。

【００３７】
図７は、本実施形態に係わるSIP負荷分散装置1の負荷分散管理テーブル26の一構成例を示した図である。
図７に示すように、負荷分散管理テーブル26では、例えば端末オンライン時のREGISTER登録（F40）を契機に割り当てたSIPサーバと端末の対応関係を記憶して管理する。具体的には、SIPサーバの割り当てを契機にリクエストメッセージのFromヘッダに指定されたユーザまたは端末のSIP-URIのエントリ（62）を追加し、当該SIP-URIに割り当てたSIPサーバのカラムにビットを立てる（60）。

【００３８】
一方、負荷分散管理プログラム25は、端末7に応対するSIPサーバを決定する際に、各SIPサーバの応対総数（64）を参照して、例えば応対数の少ないSIPサーバを新たに割り当てる。応対総数（64）からSIPサーバの負荷を推測できるので、応対総数（64）を参照してSIPサーバを割当てることによって、SIPサーバの負荷を反映した割り当てが実行でき、よりきめ細かな負荷分散が実現できる。

【００３９】
応対総数を簡便に集計する方法としては、割り当てたSIPサーバのカラムへの登録に数値カウントの「１」を用い、この数値カウントの総和を応対総数とすると良い。また、振り分け先（割り当て先）のSIPサーバを決定する際に、各SIPサーバ毎の性能を加味した重

み付けを行っても良い。各SIPサーバ毎の性能を加味した重み付けを行うことによって、それぞれのSIPサーバのスペック（例えば、CPU性能、メモリ容量など）に差がある場合には、そのスペックの差を反映した割当てが実行でき、よりきめ細かな負荷分散が実現できる。

【００４０】

F40のリクエストで端末7が希望する暗号化通信の方式が（例えばセキュリティネゴシエーションの情報として）示されている場合は、SIPサーバとの間で利用する暗号化通信の方式ごとに重み付けを行っても良い。暗号のエンコード／デコード処理にかかる負荷は暗号化通信の方式ごとに異なるため、暗号化通信の方式ごとに重み付けを行うことによって、暗号化通信の方式ごとの負荷の差を反映したSIPサーバの割り当てが実行でき、よりきめ細かな負荷分散が実現できる。

重み付けを行う場合は、重みによって決まる数値カウントをカラムへ登録すればよい。また、暗号化通信方式ごとに割り当てるSIPサーバを決めておいてもよい。暗号化の有無や暗号化通信方式の違いによってサービスや契約形態を分ける場合に、設備投資や管理が単純化できる。

【００４１】

図８は、本実施形態に係わるSIP負荷分散装置で割り当てたSIPサーバの利用有効期限を制御する方法の一例を示したシーケンス図である。

本実施形態に係わるSIP負荷分散装置では、端末7に割り当てたSIPサーバのアドレスを端末7に通知するのと同時に、この割り当てたSIPサーバの利用有効期限も端末7に通知する。例えば302応答のContactヘッダにexpiresパラメータ（図５、54）を含めて通知する。この時に通知する有効期限の値としては、システムとして許容する最長利用時間を通知する。この最長利用時間は、システムの置かれている場所、システムの使い方などに合わせて設定することができる。

【００４２】

このように有効期限を定めることによって、実質的にセッションが終了しているにも関わらず障害などの原因で端末からのセッション終了通知が送られてこない場合に、リソースを解放することができる。これにより、SIPサーバのリソースを無駄に使い続けるのを防ぐことができる。

【００４３】

一方、負荷分散管理テーブル26からのエントリの削除を行う際のシーケンスを、図８の後半に示す。端末がオフライン時に投げるREGISTER削除のメッセージ（F75）を契機に、SIPサーバ2がロケーション情報の削除を行う通常の処理（F76）に加え、SIP負荷分散装置2に対して負荷分散管理テーブル26の該当ユーザ（または端末）のエントリ削除を要求する命令を送る（F77）。SIP負荷分散装置2内部では、この命令を受けた負荷分散管理プログラム25が負荷分散管理テーブル26の該当エントリを削除する。このような処理を行うことにより、オンライン時に端末に対して割り当てたSIPサーバが、オフライン時には開放されることを負荷分散テーブル26で管理できるようになる。端末がオフライン時にREGISTER削除メッセージ（F76）を送らない場合は、REGISTERの有効期限が切れた時に、SIPサーバ2がエントリ削除要求を発行する。この有効期限切れの処理により、端末が一つの振分け先を永久に使い続けることがなくなる。これにより、特定の振分け先に長い間処理が集中することを防ぐことができ、負荷分散装置本来の負荷分散が達成できる。

【００４４】

上記の方法は、SIP負荷分散装置で有効期限のタイマ管理を行わない方法であるが、別の方法としては、SIP負荷分散装置で有効期限のタイマ管理を行っても良い。この時に、端末が割り当てられたSIPサーバを利用可能な期間を、REGISTER有効期限と一致させる必要がある。この際、REGISTER有効期限が延長される場合も考慮しなけらばならない。先ず、F41のリダイレクト通知で端末7に通知するSIPサーバの有効期限の値と同じ値を、REGISTER登録に対する成功応答（200ＯＫ（F45））で当該REGISTERの有効期限として端末7に通知する。また、負荷分散管理テーブル26には、図７の構成に加えて端末に対して割り当て

たSIPサーバの利用有効期限を管理するためのカラム（行）を追加する。

【００４５】

有効期限の設定の仕方としては、有効期限の時間（長さ）が一意に決まっている場合は、開始時刻の絶対時間を記録しておく形でも良いし、あらかじめ終了時刻を計算して記録しておく形でもよい。この場合、記録時に終了時刻を計算しておいて、検査時は現在時刻と比較するだけにするとより処理負荷が軽減される。さらに、有効期限を接続毎に可変とする場合は、終了時刻を記録しておいた方がよい。こうすることにより、有効期限が可変であっても検査処理の手順を統一化できる。さらに、SIPサーバ2側は、REGISTER削除（F75）の時だけでなく、REGISTER更新（F70）の際にも、SIP負荷分散装置に対して負荷分散管理テーブルの更新要求を発行する（F72）。この場合は、図８のF70からF73のシーケンスと同様のシーケンスとなる。

【００４６】

この方法では、SIP負荷分散装置でも有効期限のタイマ管理を行っているため、REGISTERの有効期限が切れた時に、SIPサーバ2からSIP負荷分散装置1へエントリ削除要求を送信する必要がなくなる。SIP負荷分散装置（負荷分散管理プログラム25と負荷分散管理テーブル26）で管理する有効期限が切れた時には、負荷分散管理プログラム25が負荷分散管理テーブル26の該当するエントリを削除する。

【００４７】

図９は、本実施形態に係わるSIP負荷分散システムにおいて、端末7がSIP負荷分散装置1に許可されていないSIPサーバ2を利用することを防止する方法の一例を示したシーケンス図である。

本実施形態のSIP負荷分散システムでは、全てのトラフィックをSIP負荷分散装置1が中継するモデルでは無く、端末に対して応対するSIPサーバ2を通知して誘導するモデルであるため、SIP負荷分散装置1が割り当てていないSIPサーバ2を端末7が勝手に利用してしまうと負荷分散の管理が成り立たなくなり、上手く負荷が分散されなくなる。本実施形態のSIP負荷分散システムでは、各SIPサーバ2のアドレスは原則公開せず、SIP負荷分散装置1のアドレスを公開する運用形態をとるが、一度SIP負荷分散装置1からリダイレクト通知（F41）を受けると、割り当てられたSIPサーバのアドレスはContactヘッダで通知（54）されるため、このSIPサーバのアドレスは端末の知る所となる。ここでアドレスが判明したSIPサーバを、一旦利用を終えた端末が、別の機会に、SIP負荷分散装置1を介さずに直接再利用してしまうと、上記のような問題が発生する。

そこで、本実施形態のSIP負荷分散システムでは、以下に説明するような直接通信防止方法を導入する。

【００４８】

図３に示したのと同様の手順で端末7がSIP負荷分散装置1にリクエストを送信してきた時（F40）に、SIP負荷分散装置1は応対するSIPサーバ2を決定し、割り当てたSIPサーバ2のアドレスを端末7に通知する（F41）が、この際SIP負荷分散装置1は各SIPサーバ2a～2nが共通で利用するロケーションDB3に端末7（またはユーザ）に割り当てたSIPサーバ2のアドレスを登録する（F80）。

【００４９】

ロケーション情報は、通常、ユーザまたは端末に付与するSIP-URI（92）と、端末7のコンタクトアドレス（94）としてFQDN（Fully Qualified Domain Name）またはIPアドレスなどの情報を登録管理する。これらの情報を固定設定して運用してもよいが、SIPシステムではREGISTER登録を契機に、ユーザまたは端末に付与するSIP-URI（いわゆるユーザネーム（U-Name））と、当該SIP-URIに割当てられたSIPサーバのコンタクトアドレスなどの情報を登録してもよい。本実施形態のSIP負荷分散システムでは、ロケーションDB3で管理するロケーションテーブル90を図10に示すような形で拡張する。従来のユーザアドレス単位で管理する情報に、新たに、振分け先の（応対する）SIPサーバ2のアドレスを追加する（96）。

【００５０】

この拡張ロケーションテーブル90の情報は、F80のステップの命令を受けた際に、SIP負荷分散装置1にリクエストを送ってきた端末（またはユーザ）のユーザネームと、振分け先のSIPサーバ2のアドレス情報を対にして登録する。一方、コンタクト情報などは、端末7からのREGISTER登録（F82）を振分け先のSIPサーバ2が受信し、受付処理する段階で追加登録する（F85）。

【００５１】

本実施形態のSIP負荷分散システムでは、図８のSIPサーバの利用有効期限に関する説明で述べたように、例えば、オンライン時のREGISTER登録からオフライン時のREGISTER削除までの期間を、割り当てたSIPサーバの利用有効期限とする場合、オンライン時に応対するSIPサーバを割り当てられた後は、利用有効期限内であればSIP負荷分散装置1を介さずに直接割り当てられたSIPサーバと通信することを想定している。この時に、各SIPサーバ2は端末1からのメッセージを直接受け取ることになるが、端末1からのメッセージを受けた時、例えば最初のREGISTER登録メッセージを受けた時（F80）などに、自身が応対しても良い端末か否かは、F85とF86のステップで拡張ロケーションテーブル90の情報を参照し、REGISTER登録メッセージを送ってきた端末に割り当てられているSIPサーバが自身か否かを確認する。ここでREGISTER登録メッセージを送ってきた端末に割り当てられているSIPサーバが自身であった場合には、コンタクトアドレスなどREGISTER登録メッセージから取得した情報を拡張ロケーションテーブル90に追加登録し（F87）、端末に応答を返す（F89）。一方、F85とF86のステップで拡張ロケーションテーブル90の情報を参照した際に、REGISTER登録メッセージを送ってきた端末に割り当てられているSIPサーバが無い、または割り当てられているSIPサーバが自身では無い場合には、F87のコンタクトアドレスの登録などは行わず、F89のステップでは端末にエラー応答（例えば、403 Forbiddenなど）を返す。このような手順を踏むことにより、本実施形態のSIP負荷分散システムでは、SIP負荷分散装置1が割り当てていないSIPサーバと端末との間の直接通信を防止する。

【００５２】

ちなみに、拡張ロケーションテーブル90の各エントリは、通常のロケーション情報を削除するタイミングと同様に、REGISTER登録の有効期限が切れたとき、または端末がREGISTER削除メッセージを送ってきたときに、SIPサーバがロケーションDB3に削除命令を送ってクリアする。

また、図９に示した端末からSIPサーバへのREGISTER登録シーケンス（F82からF89）は、セキュリティネゴシエーションを含まないREGISTER登録のシーケンスを例としているが、図３に示したようなセキュリティネゴシエーションを含むREGISTER登録シーケンスの場合には、F44のステップの後で、F85からF87のようなSIPサーバとロケーションDB3との間のシーケンスが走る。

【実施例２】

【００５３】

図１１は、本実施形態に係わるSIP負荷分散システムにおいて、他ドメインのSIPサーバ4を経由して自ドメインの端末7宛に送られてきたリクエストメッセージを扱う方法の一例を示した図である。

【００５４】

他ドメイン（ドメインB）35に属する端末8から、自ドメイン（ドメインA）に属する端末7宛に送られるリクエストメッセージは、最初に端末8が属するSIPサーバb4に送られる（F100）。SIPサーバb4は受信したリクエストメッセージを、宛先端末7が属するドメインのSIPサーバに中継するが、この時、本実施形態に係わるSIP負荷分散システムでは、ドメインAを管轄するSIPサーバの代表アドレス（例：domainA.co.jp）をSIP負荷分散装置1に割り当てて運用するため、SIPサーバb4が中継するリクエストメッセージはSIP負荷分散装置1に送られる（F101）。

【００５５】

他ドメインのSIPサーバb4から送られてきたリクエストメッセージを受信したSIP負荷分散装置1では、送信元判定プログラム22において、受信したリクエストメッセージの直前

の送信元が自ドメインの端末でないと判定されるため、ここで負荷分散管理プログラム25が負荷分散管理テーブル26を参照し、宛先端末の通信（セッション）管理を割り当てられているSIPサーバを調べ、そのSIPサーバにメッセージをステートレスに中継する（F102）。ここで述べている「ステートレスに」というのは、SIPについて規定しているRFC3261で定義されているステートレスプロキシの動作と同様の動作を指す。すなわち、SIP負荷分散装置1は以降の通信におけるセッションの状態遷移は管理せず、レスポンスメッセージを含め、以降のトランザクションがSIP負荷分散装置1を経由しなくても良いようにメッセージを中継する。具体的には、ViaヘッダやRecord-Routeヘッダなど、メッセージの通信経路が同じになるように、通常、SIPサーバがメッセージ中継時に付与するヘッダを付加せずに、受信したメッセージを中継する。このようにすることで、一度適切なSIPサーバにメッセージを中継した後は、SIP負荷分散装置1は当該セッションに係わる通信に関与せずに済むため、SIP負荷分散装置１は当該セッションの管理の処理負荷から開放される。

【００５６】

SIP負荷分散装置1からリクエストメッセージを中継されたSIPサーバa2（2b）は、ロケーション情報を参照し、宛先に指定されたユーザアドレスに対応するコンタクトアドレスを調べ、該コンタクトアドレス宛にメッセージを中継する（F103）。本実施形態に係わるSIPサーバでは、自身が応対する端末に関するロケーション情報をサーバ内部で登録管理することを想定しているため、ロケーション情報の参照に関わる装置間の通信はシーケンスに含めていないが、ロケーションDB3で管理している拡張ロケーションテーブル90を参照しても良い。ここで、自身が応対する端末に関するロケーション情報をサーバ内部で管理すると、SIPサーバとロケーションDBとの間の通信時間を削減できる効果が得られる。

【００５７】

一方、レスポンスメッセージは、リクエストメッセージに付与されたViaヘッダの情報に従い、F104、F105、F106の順に返信される。ここでリクエストメッセージの経路と違い、レスポンスメッセージがSIP負荷分散装置1を経由しないのは、リクエスト中継時にSIP負荷分散装置1がステートレスな中継を行ったため、ViaヘッダにSIP負荷分散装置1のアドレスを付加しないためである。また、以降の端末8と端末7との間の通信は、各SIPサーバがリクエスト中継時に付加したRecord-Routeヘッダの情報に基づいて生成するRouteセットの経路に従うため、その経路もレスポンスメッセージの通信経路と同様の通信経路となる（つまり、SIP負荷分散装置１は通過しない）。

【００５８】

図１２は、本実施形態に係わるSIP負荷分散装置1のパケット受信時の処理手順を示すフローチャートである。

ネットワークインターフェース12を通じてパケットを受信した通信制御プログラム20は、受信パケットがSIPメッセージか否かを調べる（ステップ110）。ここで受信パケットがSIPメッセージであった時は、SIPスタックプログラム21にてメッセージ解析を行い、送信元判定プログラム22において、メッセージの直前の送信元が自ドメイン内の端末か否かを調べる（ステップ111、ステップ112）。送信元が自ドメイン内の端末であった場合には、負荷分散管理プログラム25が負荷分散管理テーブル26を参照し、端末との通信に応対する適切なSIPサーバを決定する（ステップ113）。決定したSIPサーバの情報は、ロケーションDB3の対応するユーザアドレスの項に設定した後（ステップ114）、端末にリダイレクト通信プログラム23を用いて通知する（ステップ115）。

【００５９】

ステップ111、ステップ112の送信元処理において、メッセージの直前の送信元が自ドメイン内の端末以外、例えば、図１１に示したような他ドメインのSIPサーバであった場合は、負荷分散管理プログラム25が負荷分散管理テーブル26を参照し（ステップ120）、宛先端末との通信に応対しているSIPサーバを調べる（ステップ121）。ここで該当するSIPサーバが存在する場合には、ステートレスプロキシプログラム24を用いてメッセージを当該サーバに中継し（ステップ122）、該当するSIPサーバが無かった場合には、宛先端末がオフライン状態であると判定してエラー応答（例えば404 Not Found）を送信元に返す（

ステップ123）。

【００６０】

一方、ステップ110の受信パケット内容の判定において、受信パケットがSIPメッセージ以外であった場合には、通信制御プログラム20において、図８のF77に示したような負荷分散管理テーブル26のエントリ削除を要求する命令パケットであるか否かを判定し（ステップ125）、エントリ削除命令であった場合には、負荷分散制御プログラム25が負荷分散管理テーブル26の該当エントリを削除する（ステップ126）。

【００６１】

ステップ111の送信元判定には幾つかの方法が考えられる。一つの方法は、受信したリクエストメッセージのSIPヘッダ部に含まれるFromヘッダの情報52を参照する方法である。「@」マーク以降のドメイン部の内容が自ドメインと合致する場合には、自ドメイン内の端末から送られたメッセージと判定する。この判定を行うことにより、負荷分散装置が取るべき動作を決定することができる。例えば本実施例の場合は、メッセージの送信元が自ドメインの端末である場合、負荷分散装置はメッセージ送信元である端末に対して応対するSIPサーバのアドレスを通知し、一方、メッセージの送信元が他ドメインの端末・装置である場合、本発明の負荷分散装置は宛先端末に応対しているSIPサーバにメッセージをステートレス中継する。

【００６２】

同じく、受信したリクエストメッセージのSIPヘッダ部に含まれるFromヘッダの情報52を参照して判定する別の方法としては、Fromヘッダの情報52を同ドメインの加入者情報と比較しても良い。ここで比較する加入者情報とは、ユーザまたは端末に付与したSIP-URI、すなわちユーザアドレスを指す。この場合は、受信したリクエストメッセージのSIPヘッダ部に含まれるFromヘッダに指定されたSIP-URIと合致するユーザアドレスが、加入者情報に存在するか否かを検索する。検索した結果、合致すれば自ドメイン内の端末から送られたメッセージと判定する。このように判定することにより、ドメイン指定は正しいが、ユーザIDが不正な（例えば、無作為に設定された）アドレスであった場合、SIPサーバに振り分けを行う前にこれを検出して拒絶することが可能になる。つまり、不正なアドレスをもつメッセージによりSIPサーバに負荷がかかることを防止できる。

【００６３】

この加入者情報は、SIP負荷分散装置1内に持たせても良いし、ロケーションDBに持たせて参照しても良いし、加入者情報を管理する独立のDBサーバを設けて参照しても構わない。

または、自ドメイン内の端末に付与するIPアドレスの範囲が特定できる場合には、受信したリクエストメッセージのIPヘッダのソースアドレスが、この範囲に含まれるか否かで判定することもできる。この範囲は、例えば「133.144.0.1」から「133.144.0.255」までというようにIPアドレスの番号の範囲で指定してもよい。

【００６４】

このように、IPアドレスの範囲によって判定することにより、ドメインアドレスを使ったリクエストを送信できない端末にも対応できる。また、IPアドレスに対応する加入者情報とは関係なく割当てを行うことにより、加入者の登録／削除／サービス変更等に左右されずに割当てられるので、割当ての処理が軽減される。

【００６５】

更に別の方法としては、相互に接続する他ドメインのSIPサーバなどのアドレスリストを持ち、これと受信したリクエストメッセージのIPヘッダのソースアドレスとを比較することにより、他ドメインからの通信であるか否かを判定するという方法でも構わない。この判定方法により、他ドメインと相互接続するSIPサーバを限定することができる。さらに、その接続規制を負荷分散装置で行うことにより、SIPサーバに負担を掛けずに接続規制を行うことができる。

【実施例３】

【００６６】

図１３は、本実施形態に係わるSIP負荷分散システムにおいて、同一ドメイン内の端末間で通信を行う方法の一例を示した図である。
端末a1（7a）と端末aN（7n）は、それぞれ、図３と同様の手順でSIP負荷分散装置1から通知されたSIPサーバa1（2a）とSIPサーバaN（2n）との間で、継続的なコネクションを確立している。このような状況で端末a1から端末aNに送られるリクエストメッセージの流れを説明する。

【００６７】

端末a1が発行するリクエストメッセージは、先ず、端末a1との間で継続的なコネクションを確立しているSIPサーバa1に送られる（F130）。SIPサーバa1は、メッセージの宛先を参照することで、宛先が同一ドメインに属する端末であることを判別する。ここで、自身が応対している端末のロケーション情報を、メモリまたはローカルのハードディスク上でキャッシュ管理している場合は、キャッシュ上のロケーション情報に宛先端末の情報が存在するか調べる。キャッシュ上に宛先端末の情報が存在する場合は、そこに記録されているコンタクトアドレス宛にメッセージを中継する。一方、キャッシュ上に宛先端末の情報が存在しない場合には、ロケーションDB3で管理している拡張ロケーションテーブル90の情報を参照する（F132、F134）。宛先端末aN（7n）がオンラインであれば、該当端末との通信に応対し、セッションの管理を行っているSIPサーバの情報96が、該当端末のSIP-URI情報92と対で登録されている。よって、該当端末のSIP-URIに対応するSIPサーバの情報96を参照し、ここで得られたSIPサーバのアドレスにメッセージの中継を行う（F136）。最後に、メッセージを受信したSIPサーバaN（2n）は、SIPサーバa1（2a）と同様の手順で宛先の確認とロケーション情報の参照を行い、メッセージを端末aN（7n）に中継する。このように既存コネクションを利用することで、SIPサーバおよび端末のリソースの消費を抑制できる。また、既存コネクションを利用することで、新たな暗号化通信路を確立するための鍵交換や認証手順を省略でき、この場合さらにSIPサーバ、端末の負荷を削減できる。
SIPサーバが、自身が応対している端末のロケーション情報をキャッシュ管理していない場合は、最初からロケーションDB3で管理している拡張ロケーションテーブル90の情報を参照する。

【００６８】

ちなみに、拡張ロケーションテーブル90では端末のコンタクトアドレス情報94も登録・管理しているため、F132、F134の手順で拡張ロケーションテーブルを参照する際には宛先端末aN（7n）のコンタクトアドレスも判明する。よって、SIPサーバa1（2a）はSIPサーバaN（2n）を介さず、直接、宛先端末aN（7n）にメッセージを中継することも可能である。

【００６９】

しかしながら、端末aN（7n）とSIPサーバaN（2n）との間の継続的なコネクションが、認証手順を経て確立される通信路であって、また、送受信されるパケットが暗号化されるセキュアな通信路であるような場合、このコネクション上で送受信されるパケットは安全が保障されるものとして許容するが、他のコネクション上で送られるパケット（例えば、上記のようにSIPサーバa1から端末aNに直接中継されるパケット）は許容しないとしてもよい。このような場合には、安全が保障されている通信は、図１３で示したようにSIPサーバaNを経由する通信経路でパケットを中継することが望ましい。このように、安全が保障されていない他のコネクションのパケットを許容しないことで、安全が保障されているパケットとそれ以外のパケットを混同せずに転送することができる。
図１３に示したような中継処理を行うSIPサーバの装置構成図と動作フローを、それぞれ図１４と図１５で説明する。

【００７０】

図１４は、本実施形態に係わるSIPサーバ2の一構成例を示す図である。CPU10、メモリ16、記憶装置14、ネットワークインターフェース12を備える点は、図１に示したSIP負荷分散装置と同様である。記憶装置に格納されたSIPサーバの制御用プログラムは、動作時にメモリ上に展開され、CPUで実行される。記憶装置は筐体内部に実装されても、外部記憶

装置として別筐体で設置されても、ネットワークで接続されていも構わない。
また、装置管理権限を持つユーザがSIPサーバを操作するためのユーザインタフェースを備えていてもよい。ユーザインタフェースとしては、例えば、コマンド入力のためのキーボードや、ＧＵＩ入力のためのマウス、表示画面などを指す。

【００７１】

通信制御プログラム20とSIPスタックプログラム21も図１で示したプログラムと同様である。一方、簡略化して示しているが、140から149までがSIPプロキシプログラムを含むSIPサーバの主構成要素である。SIPプロキシプログラム140は中継先のアドレス解決プログラム144を含む。この中継先アドレス解決プログラムの詳細については、後に、図１５のフローチャートを用いて説明する。セッション管理テーブル142は、呼の状態遷移を管理する。ローカルロケーションテーブル146は、当該SIPサーバが応対する端末のSIP-URIとコンタクトアドレスなどのロケーション情報を管理する。セッション管理テーブル142と、ローカルロケーションテーブル146は、図14ではメモリ16上のテーブルとして描いているが、記憶装置14上に置かれるデータベーステーブルであっても構わない。また、ローカルロケーションテーブルをSIPサーバ内で保持する代わりに、外部のロケーションDBにロケーション情報を保持しておき、必要なときにこのDBにアクセスしてもよい。しかし、SIPメッセージの中継処理を高速に行うためには、自身が応対する端末のロケーション情報は、ローカルロケーションテーブル146のような形で自サーバ内に情報を保持しておく方が、常に外部のロケーションDB3を参照するよりも有利である。

【００７２】

アドレス解決プログラム144は、先ず、受信したメッセージの宛先情報を参照し、自身が管轄するドメイン内の端末宛のメッセージであるか（自ドメイン宛であるか）否かを調べる（ステップ150）。ここで宛先が自ドメインの端末であった場合は、アドレス解決プログラム144において、ローカルロケーションテーブル146を参照し、現在、自身が応対している端末であるか否か調べる（ステップ153）。ローカルロケーションテーブル146に情報がある場合は（ステップ154）、SIPスタックプログラム21が判明したコンタクトアドレス宛にメッセージを中継する（ステップ157）。一方、ローカルロケーションテーブル146に情報が存在しない場合には（ステップ154）、ロケーションDB制御プログラム148が、外部のロケーションDB3の情報を参照する（ステップ155）。他のSIPサーバが応対している場合を含めて、宛先端末がオンライン状態の場合は、ロケーションDB3にコンタクトアドレスが登録されていることとする。次に、ロケーションDB3検索の結果、コンタクトアドレスが解決した場合には（ステップ156）、メッセージを該コンタクトアドレス宛に中継する（ステップ157）。一方、ロケーションDB3にもコンタクトアドレスが登録されていない場合、または端末のアカウント（SIP-URI）自体が存在しない場合には、SIPスタックプログラム21はエラー応答を送信元に返信する（ステップ158）。

【００７３】

アドレス解決プログラム144が宛先ドメイン判定を行った際に、他ドメイン宛のメッセージであると判定した場合は（ステップ150）、DNSクライアントプログラム149がDNSサーバに問い合せを行う（ステップ151）。次にSIPスタックプログラム21は、アドレス解決した場合はメッセージを中継し（ステップ157）、解決しなかった場合はエラー応答を返す（ステップ158）。
ここではアドレス解決処理の手順に焦点を当てるため、アドレス解決とメッセージ中継またはエラー応答との間を直結して説明を簡略化しているが、実際のSIPサーバの動作では、認証処理や呼状態管理処理や固有のフィルタ処理などが、メッセージ中継またはエラー応答前に実施されることもある。

【実施例４】

【００７４】

図１６は、アプリケーションサーバを用いる場合におけるSIP負荷分散システムの一構成例を示す図である。プレゼンスサーバや会議サーバなどのアプリケーションサーバの設置例としては、SIP負荷分散装置1と同一ドメイン内に設置する例160と他ドメインに設置

する例162が考えられる。他ドメインに設置する場合162、アプリケーションサーバ発のSIPメッセージは、一旦、アプリケーションサーバ162と同一ドメイン内のSIPサーバ4に送られる。そのメッセージの宛先がドメインA内に属する端末宛であった場合は、SIPサーバ4経由でSIP負荷分散装置1に送られてくるので、この時のメッセージ送受信処理は図１１に示した実施例と同様である。一方、SIP負荷分散装置1と同一ドメイン内に設置されたアプリケーションサーバ160の場合は、これを端点（End Point）の端末とみなして端末2と同様に扱うか、それともサーバ2とは別のSIP負荷分散装置1配下のサーバとみなして、他ドメインのSIPサーバ4経由のメッセージを受信する場合と同様に扱うかで、SIP負荷分散装置1の動作が異なる。

【００７５】

端末2と同様に扱う場合、アプリケーションサーバ160には図３で説明した端末2と同様の動作が求められる。このように、アプリケーションサーバを端末と同様に扱うことによって、アプリケーションサーバ発のリクエストも負荷分散の対象として扱うことができる。

【００７６】

一方、他ドメインのSIPサーバ4と同様に扱う場合、SIP負荷分散装置1およびSIP負荷分散装置配下の複数台のSIPサーバ2と相互に接続するサーバのアドレスをアドレスリストとして保持し、SIP負荷分散装置1の送信元判定プログラム22がこのアドレスリストにアプリケーションサーバ160のアドレスも加えて管理制御すると良い。このように、アプリケーションサーバを他ドメインのSIPサーバと同様に扱うことによって、リダイレクト応答に対応する機能を有さないアプリケーションサーバ発のリクエストも負荷分散の対象として扱うことができる。

【００７７】

また、これまで説明したシステム構成図では、SIP負荷分散装置1と複数台のSIPサーバ2は、それぞれ独立した装置であるように描いているが、これらのサーバ装置をブレードサーバのような、同一筐体の装置を構成する各サーバブレードで動作させても構わない。更に、アプリケーションサーバ160のサーバモジュールもブレードサーバ内に同居させて、同一のブレードサーバ装置で動かしても構わない。このように、ブレードサーバ内に同居させることによって、統一的な監視制御を行える。また、サーバを一台一台並べる場合に比べて、省スペース化が実現できる。

【００７８】

以上、本実施例のSIP負荷分散装置を用いることにより、受信したリクエストメッセージの直前の送信元が自ドメインの端末だった場合には、負荷分散管理テーブルの情報に基づき応対するSIPサーバを決定し、リダイレクト応答を使って応対するSIPサーバのアドレスを通知するため、以降の端末からの通信（暗号化通信を含む）ではSIP負荷分散装置を介さず、且つ、適切なSIPサーバに負荷分散することができる。特に、応対するSIPサーバのアドレスを端末に通知した後は、SIP負荷分散装置は端末からの通信に介在する必要が無いため、暗号化通信を行う際にSIP負荷分散装置で暗号化通信を終端しなければならないメッセージ数が減り、SIP負荷分散装置がボトルネックとならないようにすることができる。

【００７９】

同様に、受信したリクエストメッセージの直前の送信元が自ドメインの端末以外だった場合にも、負荷分散管理テーブルを参照して宛先端末が接続しているSIPサーバを調べ、ステートレスプロキシとして当該SIPサーバにメッセージを中継するため、以降の通信ではSIP負荷分散装置を介さず、端末が継続的なコネクションを確立しているSIPサーバにメッセージを振り分けることができる。

【産業上の利用可能性】

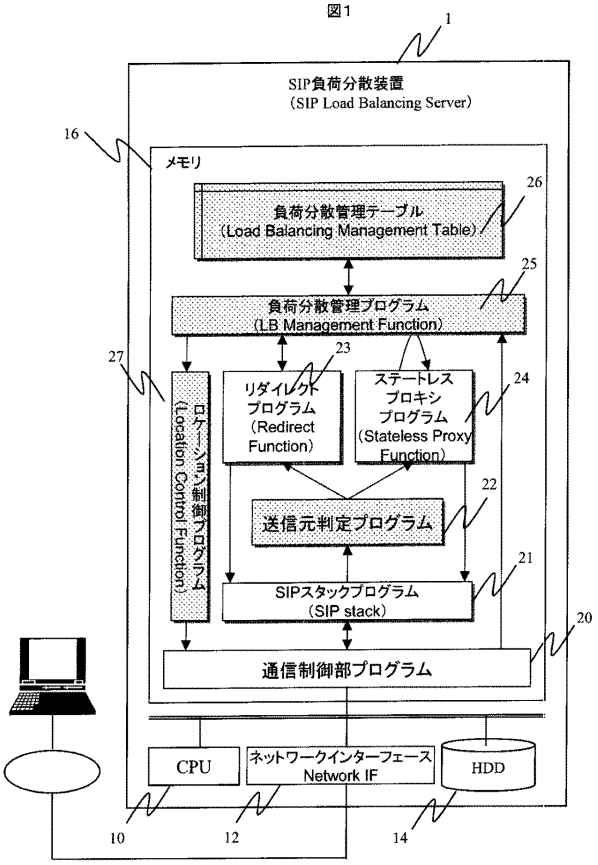
【００８０】

本発明の通信方法は、非暗号化通信においても同様にSIPサーバの負荷分散が実現できるため、暗号化通信と非暗号化通信が混在するSIPシステムにも適用できる。

【図面の簡単な説明】
【００８１】
【図１】SIP負荷分散装置の一構成例を示す図。
【図２】本発明の実施形態に係わるSIP負荷分散システムの一構成例を示す図。
【図３】端末を応対するSIPサーバに誘導する手順の一例を示すシーケンス図。
【図４】端末がSIP負荷分散装置に送るメッセージの一例を示す図。
【図５】応対するSIPサーバのアドレスを通知するリダイレクト応答のメッセージの一例を示す図。
【図６】端末が応対するSIPサーバに送るメッセージの一例を示す図。
【図７】負荷分散管理テーブルの一例を示すテーブル図。
【図８】SIP負荷分散装置で割り当てたSIPサーバの利用有効期限を制御する方法の一例を示すシーケンス図。
【図９】SIP負荷分散装置に許可されていないSIPサーバを端末が利用することを防止する方法の一例を示すシーケンス図。
【図１０】拡張ロケーションテーブルの一例を示すテーブル図。
【図１１】SIP負荷分散システムにおける、ドメインを跨るメッセージ送受信処理の一例を示す方式説明図。
【図１２】SIP負荷分散装置のパケット受信時の処理手順の一例を示すフローチャート。
【図１３】同一ドメイン内の端末間通信の一例を示す方式説明図。
【図１４】SIPサーバの一構成例を示す図。
【図１５】SIPサーバにおける中継先アドレス解決処理の一例を示すフローチャート。
【図１６】アプリケーションサーバを用いる場合におけるSIP負荷分散システムの一構成例を示す図。
【符号の説明】
【００８２】
１０．　CPU
１２．　ネットワークインターフェース
１４．　記憶装置
１６．　メモリ
２０．　通信制御部
２１．　SIPスタック部
２２．　送信元判定手段
２３．　リダイレクト機能
２４．　ステートレスプロキシ機能
２５．　負荷分散管理手段
２６．　負荷分散管理テーブル
２７．　ロケーション制御手段。

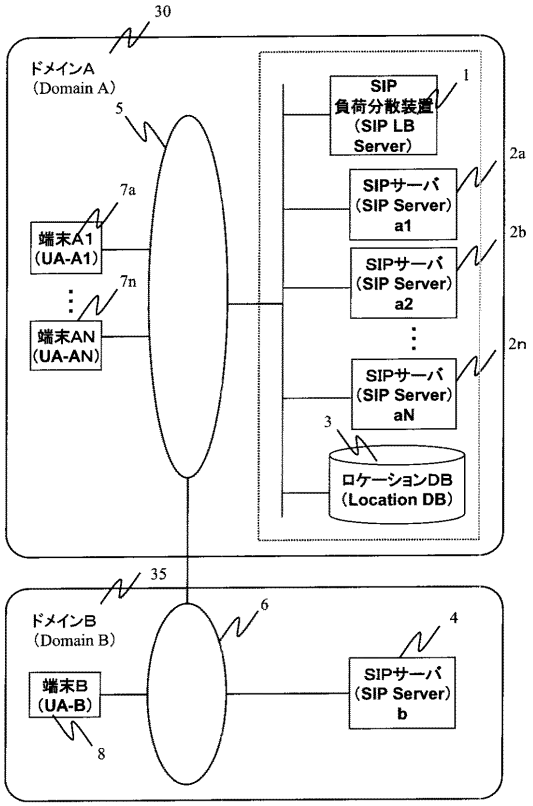
【図１】

図1



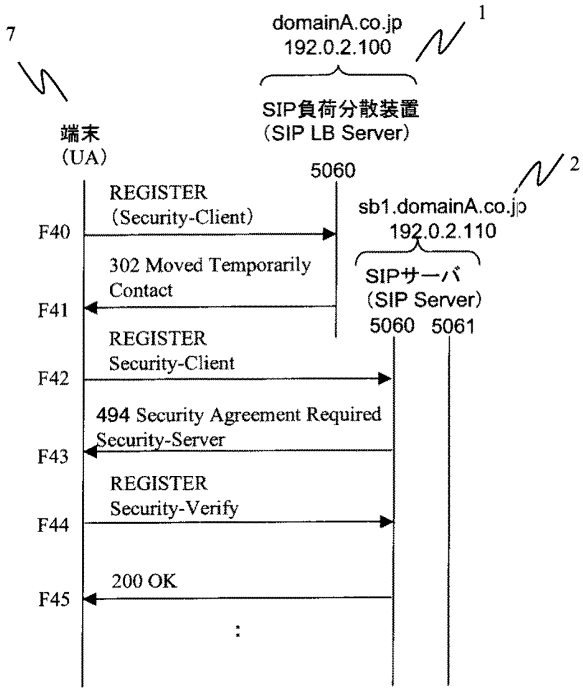
【図２】

図2



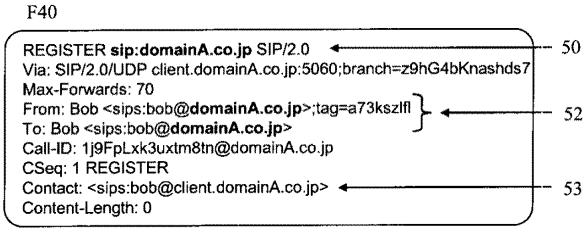
【図３】

図3



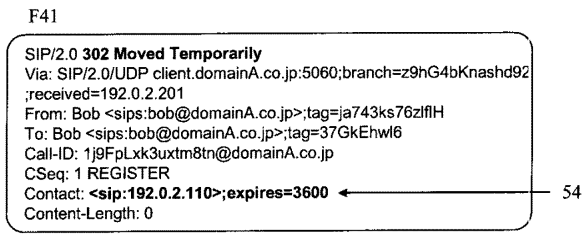
【図４】

図4



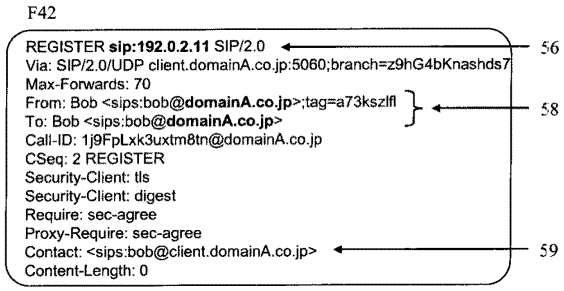
【図５】

図5



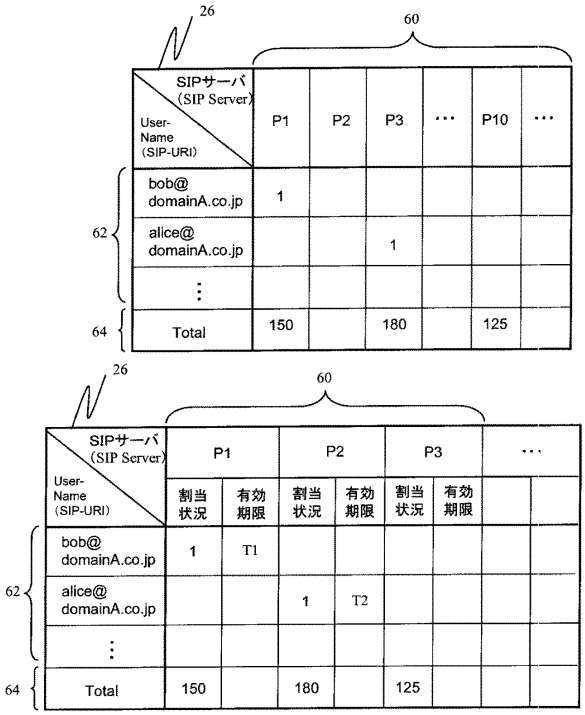
【図６】

図6



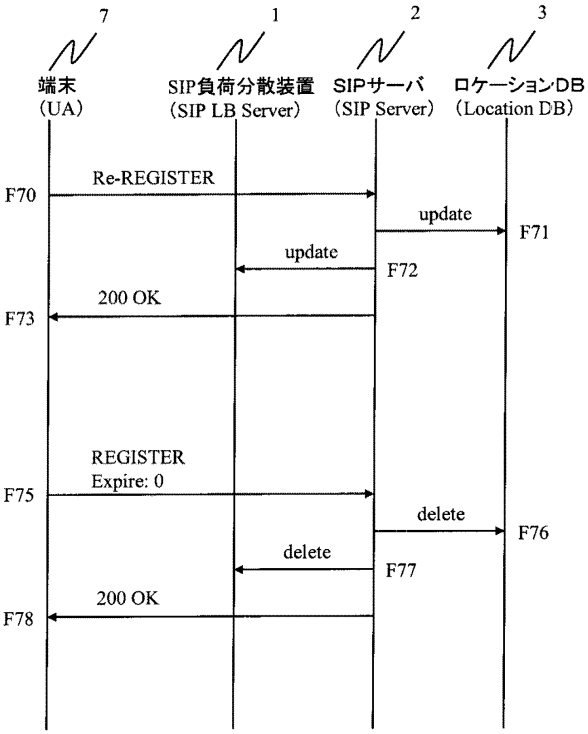
【図７】

図7



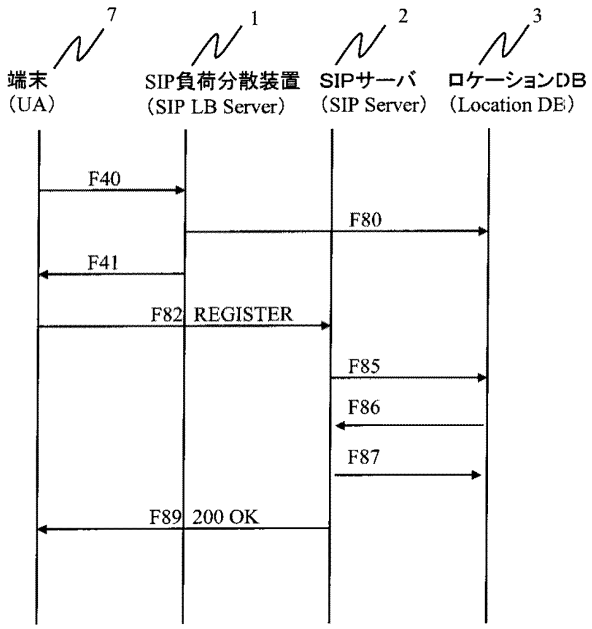
【図８】

図8



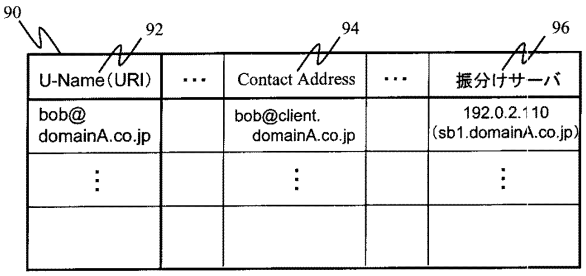
【図９】

図9



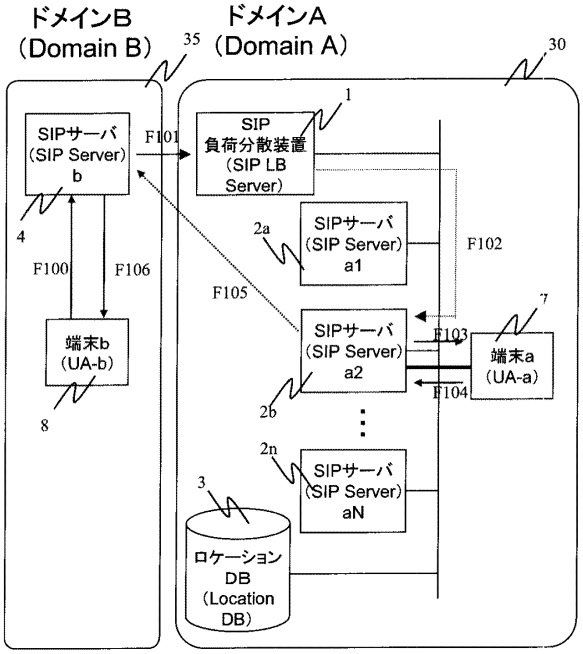
【図１０】

図10



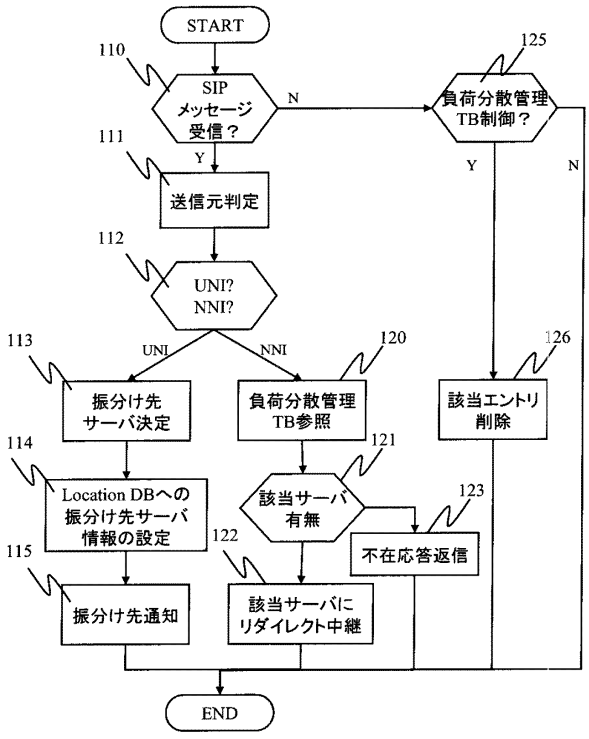
【図１１】

図11



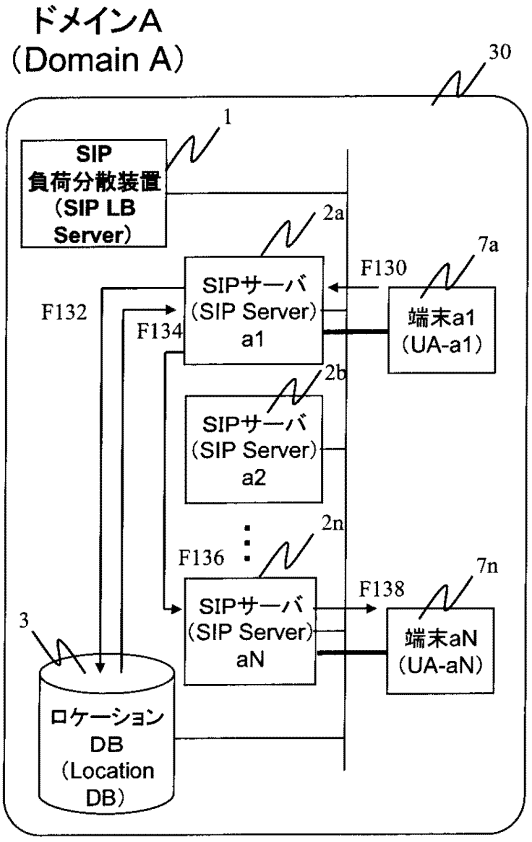
【図１２】

図12



【図１３】

図13



【図１４】

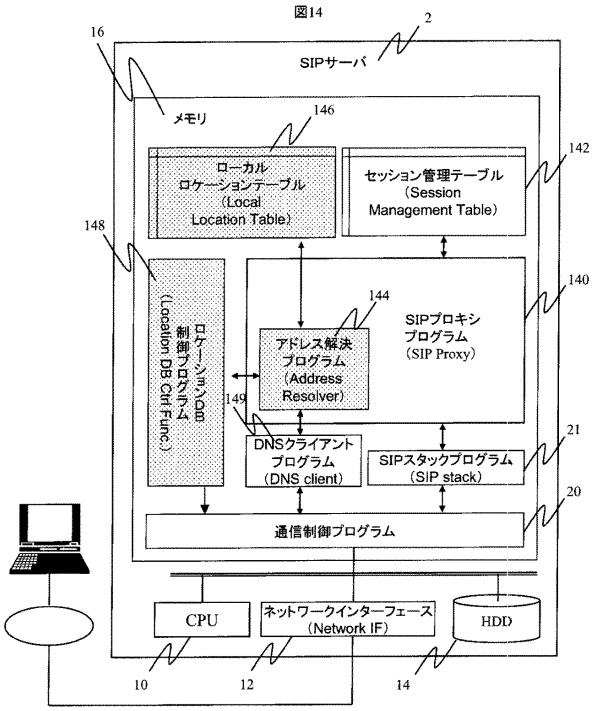


図14
SIPサーバ
メモリ
ローカル
ロケーションテーブル
(Local
Location Table)
セッション管理テーブル
(Session
Management Table)
ロケーションDB制御プログラム
(Location DB Ctrl Func.)
SIPプロキシ
プログラム
(SIP Proxy)
アドレス解決
プログラム
(Address
Resolver)
DNSクライアント
プログラム
(DNS client)
SIPスタックプログラム
(SIP stack)
通信制御プログラム
CPU
ネットワークインターフェース
(Network IF)
HDD

【図１５】

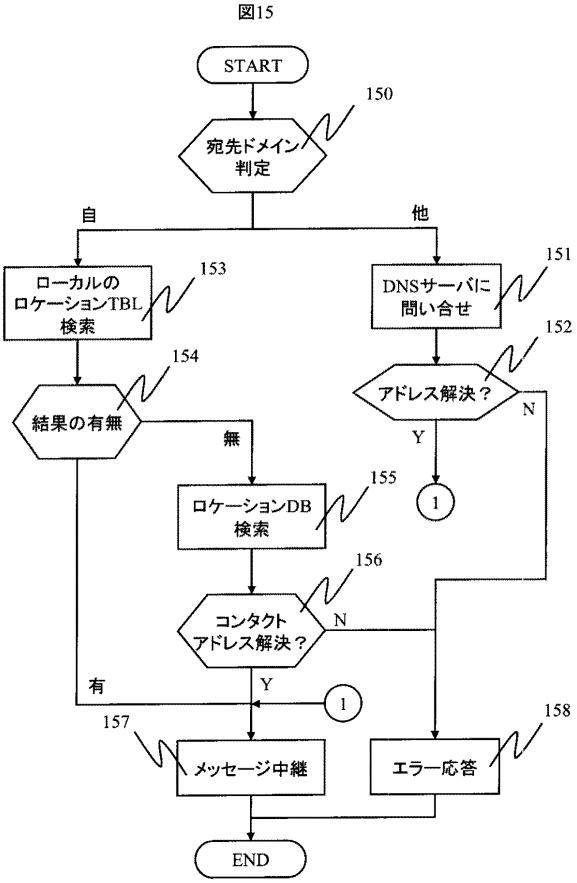


図15
START
宛先ドメイン
判定
自
他
ローカルの
ロケーションTBL
検索
DNSサーバに
問い合せ
結果の有無
無
有
アドレス解決？
Y
N
ロケーションDB
検索
コンタクト
アドレス解決？
メッセージ中継
エラー応答
END

【図１６】

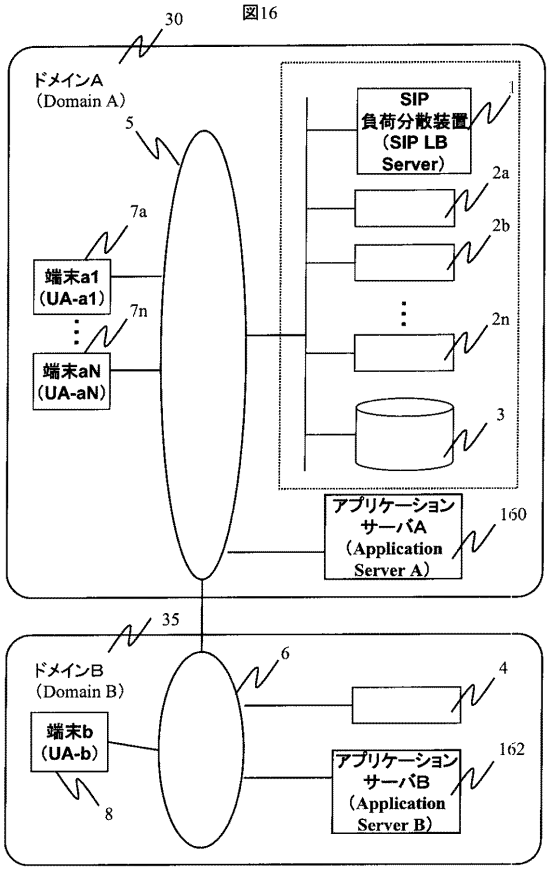


図16
ドメインA
(Domain A)
SIP
負荷分散装置
(SIP LB
Server)
端末a1
(UA-a1)
端末aN
(UA-aN)
アプリケーション
サーバA
(Application
Server A)
ドメインB
(Domain B)
端末b
(UA-b)
アプリケーション
サーバB
(Application
Server B)

フロントページの続き

審査官　鈴木　修治

(56)参考文献　特開２００２－３３４０１２（ＪＰ，Ａ）
山下克司，サーバー負荷分散装置を使いこなす▲１▼　ＳＳＬ暗号は先に復号化せよ　経路新設でレスポンス向上，日経コミュニケーション，日本，日経ＢＰ社，２００３年　６月　９日，第392号，pp.126－129
中村一貴、外２名，第３章　ＶｏＩＰのシグナリングプロトコル　ＳＩＰを用いたシグナリングの実際，Interface，日本，ＣＱ出版株式会社，２００３年　６月　１日，第29巻，第６号，pp.79－89
石井健一、外６名，異なる連携方式を用いたＷｅｂサービスアプリケーションの開発および評価，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００４年　２月２７日，第103巻，第690号，pp.107－112

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　９／４６　－　９／５４