(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-55200
(P2010-55200A)
(43)公開日　平成22年3月11日(2010.3.11)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 13/00	(2006.01)	G06F	13/00	510A	5K030
H04L 12/66	(2006.01)	H04L	12/66	Z	

審査請求 未請求　請求項の数 9　ＯＬ　（全 12 頁）

(21)出願番号　特願2008-217035 (P2008-217035)
(22)出願日　平成20年8月26日 (2008.8.26)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(71)出願人　504176911
国立大学法人大阪大学
大阪府吹田市山田丘１番１号
(74)代理人　100083552
弁理士　秋田　収喜
(74)代理人　100103746
弁理士　近野　恵一
(74)代理人　100119703
弁理士　井上　雅夫
(72)発明者　八木　毅
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】サーバ明示選択型リバースプロキシー装置、そのデータ中継方法、およびそのプログラム

(57)【要約】
【課題】リバースプロキシー装置経由の通信において送信ユーザが宛先ｗｅｂサーバを明示的に指定した通信を実現する。
【解決手段】リバースプロキシー装置は識別子変換手段と転送手段を備える。識別子変換手段が、第一のネットワークから受信したハイパーテキスト転送プロトコルデータに記述されたホスト識別子とディレクトリ識別子を含んで構成される宛先統一資源位置指定子４－１に対して、ディレクトリ識別子の内容に応じて宛先ホスト識別子を特定し、ホスト識別子を、特定した宛先ホストに変換すると共に、前記宛先統一資源位置指定子に記述されたディレクトリ識別子を、該ディレクトリ識別子の内容の一部を削除したディレクトリ識別子に変換する。転送手段が、ホスト識別子とディレクトリ識別子が変換された宛先統一資源位置指定子４－２が記述されたハイパーテキスト転送プロトコルを第二のネットワークに転送する。
【選択図】図４

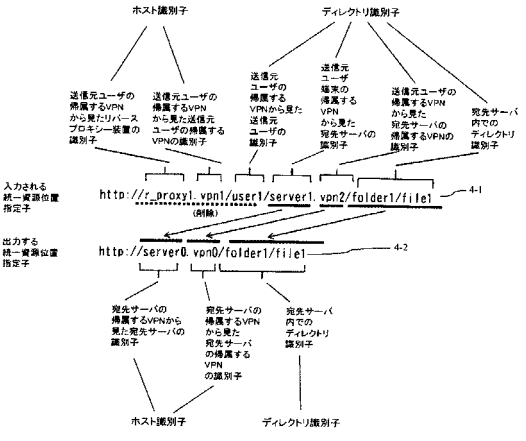

図4　リバースプロキシー装置における宛先統一資源位置指定子の変換処理例

【特許請求の範囲】
【請求項１】
第一のネットワークおよび第二のネットワークの間で、ハイパーテキスト転送プロトコルデータの中継を行うリバースプロキシー装置であって、
第一のネットワークから受信したハイパーテキスト転送プロトコルデータに記述された、ホスト識別子とディレクトリ識別子を含んで構成される宛先統一資源位置指定子に対して、ディレクトリ識別子の内容に応じて宛先ホスト識別子を特定し、前記宛先統一資源位置指定子に記述されたホスト識別子を、特定した宛先ホストに変換すると共に、前記宛先統一資源位置指定子に記述されたディレクトリ識別子を、該ディレクトリ識別子の内容の一部を削除したディレクトリ識別子に変換する識別子変換手段と、
ホスト識別子とディレクトリ識別子が変換された宛先統一資源位置指定子が記述されたハイパーテキスト転送プロトコルを、第二のネットワークに転送する転送手段と、
を有することを特徴とするリバースプロキシー装置。
【請求項２】
請求項１に記載のリバースプロキシー装置において、
前記識別子変換手段は、ディレクトリ識別子の一部の領域を、宛先ホストの識別部と解釈して変換することを特徴とするリバースプロキシー装置。
【請求項３】
請求項１または２に記載のリバースプロキシー装置において、
ディレクトリ識別子の一部の領域を、ユーザ識別子の識別部と解釈して予め決められたユーザ識別子を有しない場合に、転送先のホストへのハイパーテキスト転送プロトコルデータの中継を行わないことを特徴とするリバースプロキシー装置。
【請求項４】
請求項３に記載のリバースプロキシー装置において、
送信元ユーザのユーザ識別子と宛先ネットワークの識別子の組と、その組に対応する転送または廃棄のいずれかの処理内容を登録する認証テーブルと、
ハイパーテキスト転送プロトコルデータの転送または廃棄の判断を行う認証手段と、
を備え、
前記認証手段は、受信したハイパーテキスト転送プロトコルデータのディレクトリ識別子に記述されたユーザ識別子と宛先ネットワークの識別子から、前記認証テーブルを参照して、転送または廃棄の判断を行う、
ことを特徴とするリバースプロキシー装置。
【請求項５】
請求項１ないし４のうちのいずれか１項に記載のリバースプロキシー装置において、
第一のネットワークを収容する第一のネットワークインタフェースと第二のネットワークを収容する第二のネットワークインタフェースとアドレス解決手段とを有し、
第一のネットワークインタフェースは、第一のネットワークで定義される統一資源位置指定子のホスト識別子、第一のネットワークで定義されるインターネットプロトコルアドレスが付与され、
第二のネットワークインタフェースは、第二のネットワークで定義される統一資源位置指定子のホスト識別子、第二のネットワークで定義されるインターネットプロトコルアドレスが付与され、
前記識別子変換手段は、第一のネットワークインタフェースからハイパーテキスト転送プロトコルデータを受信すると、第一のネットワークで定義される宛先統一資源位置指定子のディレクトリ識別子の一部から、第二のネットワークで定義される宛先統一資源位置指定子のホスト識別子を生成し、第一のネットワークで定義される宛先統一資源位置指定子のディレクトリ識別子の一部を削除して、第二のネットワークで定義される宛先統一資源位置指定子のディレクトリ識別子を生成し、これらを用いて、第一のネットワークで定義される宛先統一資源位置指定子を、第二のネットワークで定義される宛先統一資源位置指定子に変換し、

前記アドレス解決手段は、ハイパーテキスト転送プロトコルデータを第二のネットワークインタフェースから第二のネットワークに送信する場合は、第二のネットワークで定義される宛先統一資源位置指定子のホスト識別子から、第二のネットワークで定義される宛先インターネットプロトコルアドレスを解決し、ハイパーテキスト転送プロトコルデータを第一のネットワークインタフェースから第一のネットワークに送信する場合は、第一のネットワークで定義される宛先統一資源位置指定子のホスト識別子から、第一のネットワークで定義される宛先インターネットプロトコルアドレスを解決する、

ことを特徴とするリバースプロキシー装置。

【請求項６】

請求項５に記載のリバースプロキシー装置において、

第一のネットワークで定義されるホスト識別子と第二のネットワークで定義されるホスト識別子の対応関係を登録する変換テーブルを備え、

前記識別子変換手段は、第一のネットワークから受信したハイパーテキスト転送プロトコルデータの宛先統一資源位置指定子のディレクトリ識別子に記述された第一のネットワークで定義されるホスト識別子から、前記変換テーブルを参照して、第二のネットワークで定義されるホスト識別子を得て、これを宛先ホスト識別子とする、

ことを特徴とするリバースプロキシー装置。

【請求項７】

請求項１ないし６のうちのいずれか１項に記載のリバースプロキシー装置において、

変換後のディレクトリ識別子は、受信したハイパーテキスト転送プロトコルデータの宛先統一資源位置指定子のディレクトリ識別子に記述された宛先ホスト内でのディレクトリ識別子であることを特徴とするリバースプロキシー装置。

【請求項８】

第一のネットワークおよび第二のネットワークの間で、ハイパーテキスト転送プロトコルデータの中継を行うリバースプロキシー装置におけるデータ中継方法であって、

前記リバースプロキシー装置は、識別子変換手段と転送手段とを備え、

前記識別子変換手段が、第一のネットワークから受信したハイパーテキスト転送プロトコルデータに記述された、ホスト識別子とディレクトリ識別子を含んで構成される宛先統一資源位置指定子に対して、ディレクトリ識別子の内容に応じて宛先ホスト識別子を特定し、前記宛先統一資源位置指定子に記述されたホスト識別子を、特定した宛先ホストに変換すると共に、前記宛先統一資源位置指定子に記述されたディレクトリ識別子を、該ディレクトリ識別子の内容の一部を削除したディレクトリ識別子に変換し、

前記転送手段が、ホスト識別子とディレクトリ識別子が変換された宛先統一資源位置指定子が記述されたハイパーテキスト転送プロトコルを、第二のネットワークに転送する、

ことを特徴とするデータ中継方法。

【請求項９】

請求項１ないし７のうちいずれか１項に記載のリバースプロキシー装置として、コンピュータを機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ＷＷＷ（World Wide Web）に代表されるようなハイパーテキスト転送プロトコルデータでデータ通信を行うインターネット通信技術を構成する技術である。特に、インターネット通信分野のうち、企業内に閉じたイントラネットから、企業外のＶＰＮ（Virtual Private Network）にセキュアにアクセスするためのＶＰＮ通信分野に属する。

【背景技術】

【０００２】

従来のリバースプロキシー装置は、ユーザとｗｅｂサーバ間でのハイパーテキスト転送プロトコルデータによる中継装置に位置づけられ、主としてａｐａｃｈｅやｓｑｕｉｄと呼ばれるプログラムを用いて実現されている。例えば、ユーザを配置した企業のイント

ラネット（第一のネットワーク）と、Ｗｅｂサーバを配置したアプリケーションサービスプロバイダのネットワーク（第二のネットワーク）を相互接続するために有効である。このようなネットワーク構成において、ユーザは、宛先統一資源位置指定子のホスト識別子にリバースプロキシー装置の識別子を記述して、リバースプロキシー装置宛にデータを送信する。リバースプロキシー装置は、自宛のホスト識別子を、実際のｗｅｂサーバのホスト識別子に変換して、データをｗｅｂサーバ宛に転送する。この際、データ中継毎に異なるｗｅｂサーバのホスト識別子に変換してデータ転送することで、複数のｗｅｂサーバ間での負荷分散が可能となる。

【０００３】

リバースプロキシー装置について記載された文献としては、例えば非特許文献１、特許文献１がある。

【０００４】

【非特許文献１】負荷分散制御アルゴリズムの性能評価と適用領域、Performance Evaluation of a Load Balancing Routing Algorithm for a Cache Server Array、巳波弘佳、熊谷和則、能上慎也、阿部威郎、電子情報通信学会技術研究報告、ＮＳ、ネットワークシステム、IEICE technical report、Ｖｏｌ．１０１、Ｎｏ．８、（２００１０４１２）、ｐｐ．１５－２０、ＮＳ２００１－３

【特許文献１】特開２００３－０５０７５６号公報（リバースプロキシネットワーク通信方式及び内部ネットワーク装置）

【発明の開示】

【発明が解決しようとする課題】

【０００５】

従来のリバースプロキシー装置では、転送先のｗｅｂサーバを複数指定することが可能であった。しかし、ユーザは、リバースプロキシー装置経由でハイパーテキスト転送プロトコルデータの中継を行う場合、リバースプロキシー装置の識別子をホスト識別子とした統一資源位置指定子を宛先として指定することしかできないため、これらのｗｅｂサーバを明示的に指定できなかった。このため、同様のコンテンツを有したｗｅｂサーバ間での負荷分散は行えても、Ｗｅｂサーバ毎に異なるコンテンツを配備して、要求されるコンテンツに応じて、Ｗｅｂサーバを選択することができなかった。そこで、本発明では、リバースプロキシー装置経由の通信において、送信ユーザが宛先ｗｅｂサーバを明示的に指定した通信を実現することを解決すべき課題とする。

【課題を解決するための手段】

【０００６】

本明細書において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。

【０００７】

請求項１の発明では、リバースプロキシー装置が、宛先統一資源位置指定子の変換の際に、ディレクトリ識別子の内容に応じて異なるホスト識別子を特定し変換し、ディレクトリ識別子の内容の一部を削除して、ディレクトリ識別子を再構成することで変換することを特徴とする。

【０００８】

また、請求項２の発明では、リバースプロキシー装置が、さらに、宛先統一資源位置指定子の変換の際に、ディレクトリ識別子の一部の領域を、宛先ホストの識別部と解釈して変換することを特徴とする。

【０００９】

一方、請求項３の発明では、リバースプロキシー装置が、ディレクトリ識別子の一部の領域を、ユーザ識別子の識別部と解釈して予め決められたユーザ識別子を有しない場合に、転送先のホストへのハイパーテキスト転送プロトコルデータの中継を行わないことを特徴とする。

【００１０】

請求項４の発明では、送信元ユーザのユーザ識別子と宛先ネットワークの識別子の組と、その組に対応する転送または廃棄のいずれかの処理内容を登録する認証テーブルと、ハイパーテキスト転送プロトコルデータの転送または廃棄の判断を行う認証手段と、を備え、前記認証手段は、受信したハイパーテキスト転送プロトコルデータのディレクトリ識別子に記述されたユーザ識別子と宛先ネットワークの識別子から、前記認証テーブルを参照して、転送または廃棄の判断を行う、ことを特徴とする。

【００１１】

さらに、請求項５の発明では、リバースプロキシー装置が、それぞれ、統一資源位置指定子とインターネットプロトコルアドレスの体系が異なる２つのネットワークを収容するインタフェース機能を有することを特徴とする。

【００１２】

請求項６の発明では、第一のネットワークで定義されるホスト識別子と第二のネットワークで定義されるホスト識別子の対応関係を登録する変換テーブルを備え、前記識別子変換手段は、第一のネットワークから受信したハイパーテキスト転送プロトコルデータの宛先統一資源位置指定子のディレクトリ識別子に記述された第一のネットワークで定義されるホスト識別子から、前記変換テーブルを参照して、第二のネットワークで定義されるホスト識別子を得て、これを宛先ホスト識別子とする、ことを特徴とする。

【００１３】

請求項７の発明では、変換後のディレクトリ識別子は、受信したハイパーテキスト転送プロトコルデータの宛先統一資源位置指定子のディレクトリ識別子に記述された宛先ホスト内でのディレクトリ識別子であることを特徴とする。

【００１４】

さらに、請求項８の発明は、請求項１の発明の内容を実現するデータ中継方法であり、請求項９の発明は、請求項１ないし７のうちいずれか１項に記載のリバースプロキシー装置として、コンピュータを機能させるためのプログラムである。

【発明の効果】

【００１５】

本発明により、単一のリバースプロキシー装置において、送信ユーザが宛先ｗｅｂサーバを明示的に指定して転送することが可能となる。

【発明を実施するための最良の形態】

【００１６】

本発明の構成例について説明する。

【００１７】

図１は、本発明のネットワーク構成を示す。１－１はネットワーク、１－２はＶＰＮ＃１、１－３はＶＰＮ＃２である。１－５は本発明の実施形態のサーバ明示選択型リバースプロキシー装置である。１－６はユーザ＃１（より正確にはユーザ＃１の端末）、１－７はユーザ＃２（より正確にはユーザ＃２の端末）である。１－８はプロキシー装置＃１、１－９はプロキシー装置＃２、１－１０はサーバ端末＃１、１－１１はサーバ端末＃２である。

【００１８】

この構成では、ネットワーク１－１がＶＰＮ＃１とＶＰＮ＃２で構成される。ＶＰＮ＃１はユーザ＃１およびユーザ＃２を収容する。また、ＶＰＮ＃１は中継装置として、プロキシー装置＃１を有する。ＶＰＮ＃２はサーバ端末＃１およびサーバ端末＃２を収容する。また、ＶＰＮ＃２は中継装置として、プロキシー装置＃２を有する。ＶＰＮ＃１とＶＰＮ＃２は、サーバ明示選択型リバースプロキシー装置１－５を介して接続される。サーバ明示選択型リバースプロキシー装置１－５は、ＶＰＮインタフェース＃１でＶＰＮ＃１を収容し、ＶＰＮインタフェース＃２でＶＰＮ＃２を収容する。

【００１９】

図２は、ＶＰＮ＃１から見たネーム体系を示す。ＶＰＮ＃１には、ｖｐｎ１、ＶＰＮ＃２には、ｖｐｎ２、ユーザ＃１には、ｕｓｅｒ１、ユーザ＃２には、ｕｓｅｒ２、サーバ

端末＃１には、ｓｅｒｖｅｒ１、サーバ端末＃２には、ｓｅｒｖｅｒ２、プロキシー装置＃１には、ｐｒｏｘｙ１、プロキシー装置＃２には、ｐｒｏｘｙ２、サーバ明示選択型リバースプロキシー装置１－５にはｒ＿ｐｒｏｘｙ１とネームを付与する。

【００２０】

図３は、ＶＰＮ＃２から見たネーム体系を示す。ＶＰＮ＃１には、ｖｐｎ１、ＶＰＮ＃２には、ｖｐｎ０、サーバ端末＃１には、ｓｅｒｖｅｒ０、サーバ端末＃２には、ｓｅｒｖｅｒ１、プロキシー装置＃２には、ｐｒｏｘｙ０、サーバ明示選択型リバースプロキシー装置１－５にはｒ＿ｐｒｏｘｙ０とネームを付与する。ここで、ＶＰＮ＃１から見たネーム体系とＶＰＮ＃２から見たネーム体系は、異なることに注意する必要がある。

【００２１】

図４は、サーバ明示選択型リバースプロキシー装置における宛先統一資源位置指定子の変換処理例である。この図は、上部に示す入力前の宛先統一資源位置指定子４－１と下部に示す出力後の宛先統一資源位置指定子４－２で構成される。

【００２２】

宛先統一資源位置指定子はアクセス手段識別子、ホスト識別子、ディレクトリ識別子で構成される。

【００２３】

入力前の宛先統一資源位置指定子４－１において、ホスト識別子は、送信元ユーザの帰属するＶＰＮから見たサーバ明示選択型リバースプロキシー装置の識別子、送信元ユーザの帰属するＶＰＮの識別子で構成され、ディレクトリ識別子は、送信元ユーザの帰属するＶＰＮから見た送信元ユーザの識別子、送信元ユーザの帰属するＶＰＮから見た宛先サーバの識別子、送信元ユーザの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子、宛先サーバ内でのディレクトリ識別子で構成される。

【００２４】

この例では、入力前の宛先統一資源位置指定子４－１において、アクセス手段識別子として、ｈｔｔｐ、送信元ユーザの帰属するＶＰＮから見たサーバ明示選択型リバースプロキシー装置の識別子として、ｒ＿ｐｒｏｘｙ１、送信元ユーザの帰属するＶＰＮの識別子としてｖｐｎ１、送信元ユーザの帰属するＶＰＮから見た送信元ユーザの識別子として、ｕｓｅｒ１、送信元ユーザの帰属するＶＰＮから見た宛先サーバの識別子として、ｓｅｒｖｅｒ１、送信元ユーザの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子として、ｖｐｎ２、宛先サーバ内でのディレクトリ識別子として、ｆｏｌｄｅｒ１／ｆｉｌｅ１、が指定されている。

【００２５】

また、出力後の宛先統一資源位置指定子４－２において、ホスト識別子は、宛先サーバの帰属するＶＰＮから見た宛先サーバの識別子、宛先サーバの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子から構成され、ディレクトリ識別子は、宛先サーバ内でのディレクトリ識別子で構成される。

【００２６】

この例では、出力後の宛先統一資源位置指定子４－２において、アクセス手段識別子として、ｈｔｔｐ、宛先サーバの帰属するＶＰＮから見た宛先サーバの識別子として、ｓｅｒｖｅｒ０、宛先サーバの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子として、ｖｐｎ０、宛先サーバ内でのディレクトリ識別子として、ｆｏｌｄｅｒ１／ｆｉｌｅ１、が指定されている。

【００２７】

図５に、変換テーブル５－１を示す。この変換テーブル５－１では、変換前としての送信元ユーザの帰属するＶＰＮから見た宛先サーバの識別子と送信元ユーザの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子の組から、変換後としての宛先サーバの帰属するＶＰＮから見た宛先サーバの識別子と宛先サーバの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子の組が導かれる。

【００２８】

例えば、変換前のｓｅｒｖｅｒ１．ｖｐｎ２からは、変換後のｓｅｒｖｅｒ０．ｖｐｎ０が、変換前のｓｅｒｖｅｒ２．ｖｐｎ２からは、変換後のｓｅｒｖｅｒ１．ｖｐｎ０が導かれる。ここで「．」は識別子同士の境界点を示す記号である。

【００２９】

図６に、認証テーブル６－１を示す。この認証テーブル６－１では、送信元ユーザの帰属するＶＰＮから見た送信元ユーザの識別子と送信元ユーザの帰属するＶＰＮから見た宛先ＶＰＮの識別子の組から、データ処理内容として「転送」あるいは「廃棄」が導かれる。

【００３０】

例えば、ｕｓｅｒ１とｖｐｎ２の組からは「転送」が、ｕｓｅｒ２とｖｐｎ２の組からは「廃棄」が、が導かれる。

【００３１】

図７に、本発明の実施形態のサーバ明示選択型リバースプロキシー装置１－５のシステム構成図を示す。

【００３２】

７－１は、受信したハイパーテキスト転送プロトコルデータのディレクトリ識別子に記述されたユーザ識別子と宛先ネットワークの識別子から、認証テーブル６－１を参照して、転送または廃棄の判断を行う認証手段である。７－２は、ＶＰＮ＃１から受信したハイパーテキスト転送プロトコルデータに記述された、ホスト識別子とディレクトリ識別子を含んで構成される宛先統一資源位置指定子に対して、ディレクトリ識別子の内容に応じて宛先ホスト識別子を特定し、前記宛先統一資源位置指定子に記述されたホスト識別子を、特定した宛先ホストに変換すると共に、前記宛先統一資源位置指定子に記述されたディレクトリ識別子を、該ディレクトリ識別子の内容の一部を削除したディレクトリ識別子に変換する識別子変換手段である。７－３は、アドレス解決を行うアドレス解決手段である。７－４は、ホスト識別子とディレクトリ識別子が変換された宛先統一資源位置指定子が記述されたハイパーテキスト転送プロトコルを、ＶＰＮ＃２に転送する転送手段である。

【００３３】

６－１は、図６に示す認証テーブルである。認証テーブル６－１には、送信元ユーザのユーザ識別子と宛先ネットワークの識別子の組と、その組に対応する転送または廃棄のいずれかの処理内容が登録される。５－１は、図５に示す変換テーブルである。変換テーブルには、ＶＰＮ＃１で定義されるホスト識別子とＶＰＮ＃２で定義されるホスト識別子の対応関係が登録される。

【００３４】

識別子変換手段７－２は、ＶＰＮ＃１から受信したハイパーテキスト転送プロトコルデータの宛先統一資源位置指定子のディレクトリ識別子に記述されたＶＰＮ＃１で定義されるホスト識別子から、変換テーブル５－１を参照して、ＶＰＮ＃２で定義されるホスト識別子を得て、これを宛先ホスト識別子とする。

【００３５】

アドレス解決手段７－３は、ハイパーテキスト転送プロトコルデータをＶＰＮインタフェース＃２からＶＰＮ＃２に送信する場合は、図示していないＶＰＮ＃２におけるＤＮＳ（Domain Name System）サーバを用いて、ＶＰＮ＃２で定義される宛先統一資源位置指定子のホスト識別子から、ＶＰＮ＃２で定義される宛先インターネットプロトコルアドレスを解決し、ハイパーテキスト転送プロトコルデータをＶＰＮインタフェース＃１からＶＰＮ＃１に送信する場合は、図示していないＶＰＮ＃１におけるＤＮＳサーバを用いて、ＶＰＮ＃１で定義される宛先統一資源位置指定子のホスト識別子から、ＶＰＮ＃１で定義される宛先インターネットプロトコルアドレスを解決する。なお、本実施形態ではＤＮＳサーバを用いてアドレス解決を行っているが、その他の方法を用いてもよい。

【００３６】

上述の構成における動作例について説明する。

【００３７】

ここでは、図１において、ユーザ＃１から、サーバ端末＃１のｆｏｌｄｅｒ１／ｆｉｌｅ１へハイパーテキスト転送プロトコルレイヤでアクセスする例について説明する。

【００３８】

ユーザ＃１は、図４に示す宛先統一資源位置指定子ｈｔｔｐ：／／ｒ＿ｐｒｏｘｙ１．ｖｐｎ１／ｕｓｅｒ１／ｓｅｒｖｅｒ１．ｖｐｎ２／ｆｏｌｄｅｒ１／ｆｉｌｅ１を付与したハイパーテキスト転送プロトコルデータを送信する。この際、プロキシーとして、プロキシー装置（ｐｒｏｘｙ１）が付与されていたとすると、送信データはプロキシー装置＃１へ到達する。

【００３９】

プロキシー装置＃１は、受信したハイパーテキスト転送プロトコルデータの宛先統一資源位置指定子を参照し、宛先のホスト識別子として、サーバ明示選択型リバースプロキシー装置１－５のホスト識別子ｒ＿ｐｒｏｘｙ１を特定するため、これをサーバ明示選択型リバースプロキシー装置１－５へ転送する。

【００４０】

サーバ明示選択型リバースプロキシー装置１－５は、基本的にはリバースプロキシーと同様に動作する。ただし以下の説明については、リバースプロキシーとは異なる動作を行う。

【００４１】

サーバ明示選択型リバースプロキシー装置１－５は、ＶＰＮインタフェース＃１において、ハイパーテキスト転送プロトコルデータを受信すると、認証手段７－１が、図６の認証テーブルに基づいて、宛先統一資源位置指定子ｈｔｔｐ：／／ｒ＿ｐｒｏｘｙ１．ｖｐｎ１／ｕｓｅｒ１／ｓｅｒｖｅｒ１．ｖｐｎ２／ｆｏｌｄｅｒ１／ｆｉｌｅ１において、送信元ユーザの帰属するＶＰＮから見た送信元ユーザの識別子ｕｓｅｒ１と送信元ユーザの帰属するＶＰＮから見た宛先ＶＰＮの識別子ｖｐｎ２から、データ処理内容としての「転送」を導く。

【００４２】

仮に、送信元ユーザの帰属するＶＰＮから見た送信元ユーザの識別子がｕｓｅｒ２で送信元ユーザの帰属するＶＰＮから見た宛先ＶＰＮの識別子がｖｐｎ２であった場合は、データ処理内容として「廃棄」が導かれるため、該当データが廃棄されて処理がここで終わる。

【００４３】

ここでは、データ処理内容として「転送」が導かれたので、該当データの転送処理を行う。具体的には、識別子変換手段７－２が、図５の変換テーブル５－１を参照し、送信元ユーザの帰属するＶＰＮから見た宛先サーバの識別子ｓｅｒｖｅｒ１と送信元ユーザの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子ｖｐｎ２の組から、変換後としての宛先サーバの帰属するＶＰＮから見た宛先サーバの識別子ｓｅｒｖｅｒ０と宛先サーバの帰属するＶＰＮから見た宛先サーバの帰属するＶＰＮの識別子ｖｐｎ０の組を導く。

【００４４】

この結果から、図４に示すように、宛先統一資源位置指定子をｈｔｔｐ：／／ｒ＿ｐｒｏｘｙ１．ｖｐｎ１／ｕｓｅｒ１／ｓｅｒｖｅｒ１．ｖｐｎ２／ｆｏｌｄｅｒ１／ｆｉｌｅ１からｈｔｔｐ：／／ｓｅｒｖｅｒ０．ｖｐｎ０／ｆｏｌｄｅｒ１／ｆｉｌｅ１へ変換する。

【００４５】

この後、アドレス解決手段７－３が、ＶＰＮ＃２で定義される宛先統一資源位置指定子のホスト識別子（ｓｅｒｖｅｒ０．ｖｐｎ０）から、ＶＰＮ＃２で定義される宛先インターネットプロトコルアドレスを解決し、転送手段７－４が、変換後の宛先統一資源位置指定子を付与したハイパーテキスト転送プロトコルデータをＶＰＮインタフェース＃２から送信する。

【００４６】

最終的には、変換後の宛先統一資源位置指定子のホスト識別子ｓｅｒｖｅｒ０に従って、該当データがＶＰＮ＃２内のサーバ端末＃１へ転送される。サーバ端末＃１は、宛先統一資源位置指定子のディレクトリ識別子ｆｏｌｄｅｒ１／ｆｉｌｅ１を参照して、該当データを抽出し、返送する。

【００４７】

サーバ端末＃１からユーザ＃１へ向けての返送データは、サーバ明示選択型リバースプロキシー装置１－５が、リバースプロキシー装置と同様に動作することで、従来通りのシーケンスで転送される。この場合、アドレス解決手段７－３が、ＶＰＮ＃１で定義される宛先統一資源位置指定子のホスト識別子から、ＶＰＮ＃１で定義される宛先インターネットプロトコルアドレスを解決することはいうまでもない。

【００４８】

この結果、ユーザ＃１から、サーバ端末＃１のｆｏｌｄｅｒ１／ｆｉｌｅ１へハイパーテキスト転送プロトコルレイヤでアクセスできることになる。

【００４９】

上述のように、本発明の実施形態によれば、単一のリバースプロキシー装置において、送信ユーザが宛先ｗｅｂサーバを明示的に指定して転送することが可能となる。このため、第一のネットワークにユーザを配置し、第二のネットワークに異なるコンテンツを有したｗｅｂサーバを用意してサービス提供を行うことが可能となる。ここで、第一のネットワークと第二のネットワークは異なるホスト識別子およびアドレスで運用されていても良い。

【００５０】

この結果として、第一のネットワークを企業のイントラネットと位置付けてユーザを配置し、第二のネットワークをアプリケーションサービスプロバイダのネットワークと位置づけてｗｅｂサーバを配置した上で、第一のネットワークと第二のネットワークを本発明のリバースプロキシー装置のみを介して相互接続した場合に、第一のネットワーク内では、第二のネットワーク内でのｗｅｂサーバの増設等にかかわらず、リバースプロキシー装置宛の統一資源位置指定子におけるホスト識別子とアドレスのみ管理しておけば良いという効果が得られ、一方で、第二のネットワーク内では、第一のネットワークに影響を与えることなくｗｅｂサーバの増設が行えるという効果が得られる。

【００５１】

本発明の実施形態のサーバ明示選択型リバースプロキシー装置は、コンピュータとプログラムで構成することができる。また、そのプログラムの一部または全部をハードウェアで構成してもよい。

【００５２】

以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【図面の簡単な説明】

【００５３】

【図１】本発明の実施形態のネットワーク構成例を示している。

【図２】本発明の実施形態の、一方のＶＰＮから見たネーム体系例を示している。

【図３】本発明の実施形態の、もう一方のＶＰＮから見たネーム体系例を示している。

【図４】本発明の実施形態の宛先統一資源位置指定子の変換処理例を示している。

【図５】本発明の実施形態の変換テーブル例を示している。

【図６】本発明の実施形態の認証テーブル例を示している。

【図７】本発明の実施形態のサーバ明示選択型リバースプロキシー装置のシステム構成図である。

【符号の説明】

【００５４】

１－１　ネットワーク

１－２　ＶＰＮ＃１
１－３　ＶＰＮ＃２
１－５　サーバ明示選択型リバースプロキシー装置
１－６　ユーザ＃１
１－７　ユーザ＃２
１－８　プロキシー装置＃１
１－９　プロキシー装置＃２
１－１０　サーバ端末＃１
１－１１　サーバ端末＃２
４－１　入力前の統一資源位置指定子
４－２　出力後の統一資源位置指定子
５－１　変換テーブル
６－１　認証テーブル
７－１　認証手段
７－２　識別子変換手段
７－３　アドレス解決手段
７－４　転送手段

【図１】

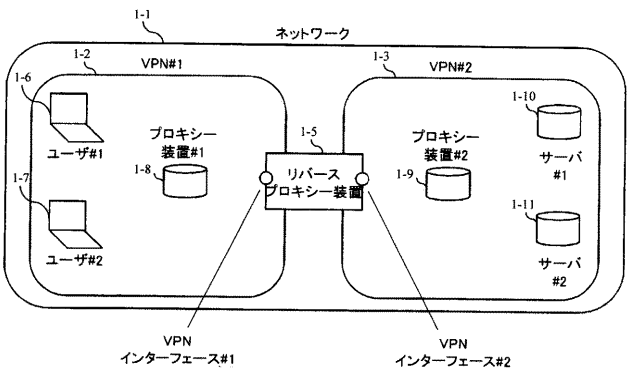

図1　ネットワーク構成

【図２】

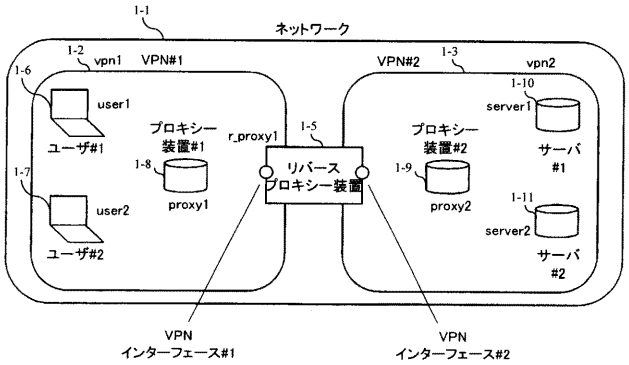

図2　VPN#1から見たネーム体系

【図３】

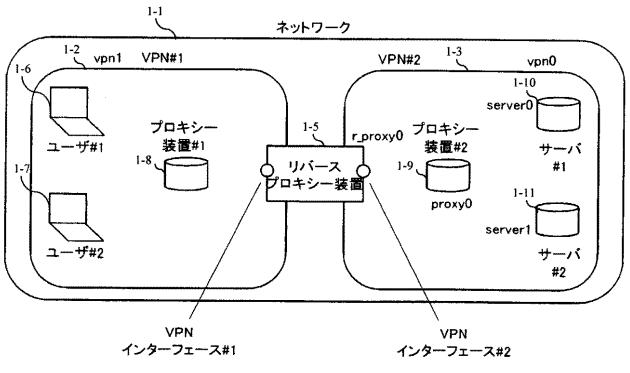

図3　VPN#2から見たネーム体系

【図４】

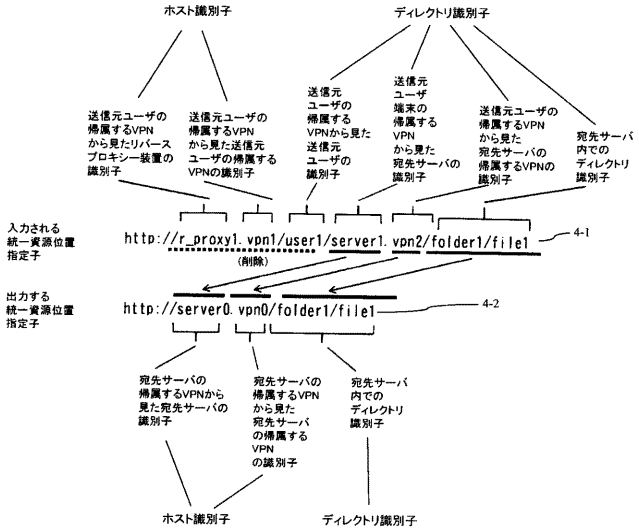

図4 リバースプロキシー装置における宛先統一資源位置指定子の変換処理例

【図５】

5-1

変換前	変換後
server1.vpn2	server0.vpn0
server2.vpn2	server1.vpn0

図5 変換テーブル

【図６】

6-1

送信元ユーザ	宛先VPN	データ処理内容
user1	vpn2	転送
user2	vpn2	廃棄

図6 認証テーブル

【図７】

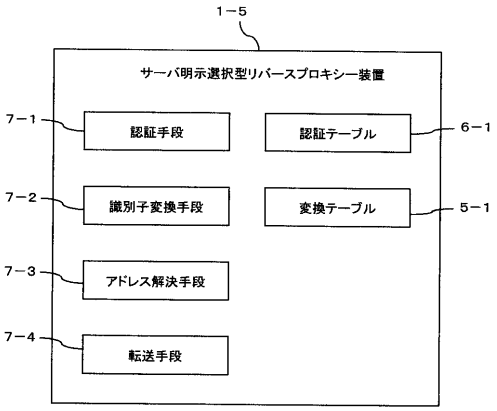

図7 サーバ明示選択型リバースプロキシー装置のシステム構成図

フロントページの続き

(72)発明者　村山　純一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　桑原　健
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　近藤　努
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　今瀬　真
大阪府吹田市山田丘１番１号　国立大学法人大阪大学内
(72)発明者　大崎　博之
大阪府吹田市山田丘１番１号　国立大学法人大阪大学内

Ｆターム(参考) 5K030 HD03　HD09