(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4628938号
(P4628938)
(45)発行日　平成23年2月9日(2011.2.9)　(24)登録日　平成22年11月19日(2010.11.19)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56 100Z
H04L 12/56 H

請求項の数 16　(全 30 頁)

(21)出願番号　特願2005-349268(P2005-349268)
(22)出願日　平成17年12月2日(2005.12.2)
(65)公開番号　特開2007-158594(P2007-158594A)
(43)公開日　平成19年6月21日(2007.6.21)
審査請求日　平成20年5月30日(2008.5.30)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　松田　哲史
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　玉木　宏治

(56)参考文献　特開２００５－２５２７６２（ＪＰ，Ａ）
特開２００４－２７４１２７（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】データ通信システム、端末装置およびＶＰＮ設定更新方法

(57)【特許請求の範囲】
【請求項１】
ＩＰネットワーク上に複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を構成可能とするデータ通信システムであって、
前記ＩＰネットワークに接続され、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うための所定情報を保持するエッジ装置と、
前記複数のＶＰＮのメンバーとなりうる端末装置と、
前記複数のＶＰＮおよび前記端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、
を備え、
前記エッジ装置は、ＶＰＮへの接続を要求する端末装置との論理的コネクションを確立した後、該端末装置が属するＶＰＮの情報をＶＰＮメンバー管理サーバから取得し、該ＶＰＮメンバー管理サーバから取得したＶＰＮの情報に基づいて該端末装置と該端末装置が接続を要求するＶＰＮとの接続設定処理を行うことを特徴とするデータ通信システム。
【請求項２】
前記エッジ装置は、
端末装置との間の論理的コネクションの識別子とラベル値のペアをキーとして、ＶＰＮ識別子、端末装置識別子およびＶＰＮ内ＩＰアドレスをデータとするデータベースと、
ＶＰＮ内ＩＰアドレスをキーとして、該ＩＰアドレスを使用している端末装置との間の論理的コネクションの識別子とラベル値のペアをデータとするデータベースと、

ＶＰＮ識別子をキーとして、そのＶＰＮへの接続に使用される端末装置との間の論理的コネクションの識別子とラベル値のペアのリストをデータとするデータベースと、
ＶＰＮ識別子をキーとして、そのＶＰＮに対応付けられるマルチキャストＩＰアドレスとサブネットアドレスをデータとするデータベースと、
マルチキャストＩＰアドレスをキーとして、そのマルチキャストＩＰアドレスに対応付けられるＶＰＮ識別子をデータとするデータベースと、
サブネットアドレスをキーとして、そのサブネットアドレスに対応付けられるＶＰＮ識別子をデータとするデータベースと、
を備え、
前記エッジ装置は、前記データベースに保持される情報に基づいて「ＶＰＮの作成または削除処理」、「ＶＰＮへのメンバーの追加または削除処理」、「ＶＰＮへの参加または離脱処理」、「ユニキャストＩＰパケットの転送処理」、および「ブロード／マルチキャストＩＰパケットの転送処理」のうちの少なくとも一つの処理を行うことを特徴とする請求項１に記載のデータ通信システム。
【請求項３】
前記ＶＰＮメンバー管理サーバは、前記エッジ装置から受信したＶＰＮ識別子と端末装置識別子を含むＶＰＮメンバー問合せ要求メッセージに対して、該ＶＰＮ識別子で指定されるＶＰＮに、該端末装置識別子で指定される端末装置が参加可能と判断した場合、当該参加を認める端末装置に割当てるＩＰアドレスと、ＶＰＮ上のブロードキャストまたはマルチキャストパケットを転送するときに使用するマルチキャストＩＰアドレスと、ＶＰＮに対応付けられるサブネットアドレスとを、前記ＶＰＮメンバー問合せ要求メッセージに対するＶＰＮメンバー問合せ応答メッセージにて通知することを特徴とする請求項１または２に記載のデータ通信システム。
【請求項４】
前記エッジ装置は、前記ＩＰネットワーク上にオーバーレイネットワークを構築し、自装置に接続した端末装置のＶＰＮへの参加が前記ＶＰＮメンバー管理サーバにより認められ、その結果、該端末装置にＩＰアドレスが割り当てられた場合、該割り当てられたＩＰアドレスをキーとして、自装置のＩＰアドレスをデータとするレコードを前記オーバーレイネットワーク上に登録し、前記オーバーレイネットワーク上に登録されたデータを検索する際には、ＤＨＴ（Ｄｉｓｔｒｉｂｕｔｅｄ　Ｈａｓｈ　Ｔａｂｌｅ）方式の検索機能を利用することを特徴とする請求項１～３のいずれか一つに記載のデータ通信システム。
【請求項５】
ＶＰＮへの参加が認められた端末装置に割り当てられたＩＰアドレスのサブネット部分が、ＶＰＮ識別子として用いられることを特徴とする請求項１～４のいずれか一つに記載のデータ通信システム。
【請求項６】
前記ＩＰネットワーク内で伝送されるＩＰパケットには、どのＶＰＮ上で送受信されるＩＰパケットかを識別可能とするためのラベルが付与されることを特徴とする請求項１～５のいずれか一つに記載のデータ通信システム。
【請求項７】
前記ＶＰＮメンバー管理サーバは、ＶＰＮに接続する端末装置の情報を分割して管理するための複数のＶＰＮメンバー管理サーバから構成され、
前記エッジ装置は、
前記ＶＰＮ識別子をキーとして、該ＶＰＮ識別子に関するデータを管理するＶＰＮメンバー管理サーバのＩＰアドレスを対応づけた情報が保持されるデータベースと、
前記データベースの情報を管理する情報管理手段と、
を備え、
前記情報管理手段は、端末装置からの要求に応じて該端末装置がメンバーとなっているＶＰＮの情報を取得する際に、該ＶＰＮの情報がどのＶＰＮメンバー管理サーバに登録されているかの判定処理を行うことを特徴とする請求項１～６のいずれか一つに記載のデー

タ通信システム。
【請求項８】
請求項１～７のいずれか一つに記載のデータ通信システムにおいて用いられる端末装置であって、
前記ＩＰネットワークにおけるＩＰ通信を実現するＩＰプロトコル処理を行うＩＰプロトコル処理部と、
前記エッジ装置との間で論理的コネクションを確立するための処理を行うトンネル通信処理部と、
論理的コネクションを識別する識別子およびＩＰパケットに付与するラベルのラベル値をＩＰ通信が可能な一つの仮想インタフェースとして扱う仮想インタフェース処理部と、
を備え、
前記仮想インタフェース処理部は、前記仮想インタフェース毎に複数の論理的コネクションが確立しているとみなしてＩＰ通信を行うことを特徴とする端末装置。
【請求項９】
複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が構成されるＩＰネットワーク上にオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うエッジ装置と、複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、が具備されるデータ通信システムに適用され、
前記オーバーレイネットワークを構築するネットワークに接続されているＶＰＮのいずれかに参加している端末装置からのエッジ装置との間の論理的コネクションおよび参加中のＶＰＮを介した新しいＶＰＮの生成指示に応じてＶＰＮの設定を更新する際に、
前記端末装置が、新たに作成を希望するＶＰＮを識別するためのＶＰＮ識別子を前記エッジ装置に通知する工程と、
前記エッジ装置が、前記論理的コネクションの識別子およびＩＰパケットの先頭に付与されているＶＰＮを識別するためのラベル値に基づいて前記端末装置の端末装置識別子を取得する工程と、
前記エッジ装置が、前記ＶＰＮ識別子および端末装置識別子を前記ＶＰＮメンバー管理サーバに通知する工程と、
前記ＶＰＮメンバー管理サーバが、前記ＶＰＮ識別子および端末装置識別子に基づいて新たに作成するＶＰＮについての情報（ＶＰＮ情報）および前記端末装置が当該ＶＰＮに接続するための情報（端末装置情報）を作成する工程と、
前記ＶＰＮメンバー管理サーバが、前記ＶＰＮ情報を自装置内のデータベースに登録する工程と、
前記ＶＰＮメンバー管理サーバが、前記端末装置情報をエッジ装置に通知する工程と、
を含むことを特徴とするＶＰＮ設定更新方法。
【請求項１０】
複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が構成されるＩＰネットワーク上にオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うエッジ装置と、複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、が具備されるデータ通信システムに適用され、
前記オーバーレイネットワークを構築するネットワークに接続されているＶＰＮのいずれかに参加している第１の端末装置からのエッジ装置との間の論理的コネクションを介した所定のＶＰＮに対する新しいメンバーの追加登録要求に応じてＶＰＮの設定を更新する際に、
前記第１の端末装置が、新たにメンバーとなる第２の端末装置を識別するための端末装置識別子およびメンバー登録先のＶＰＮを識別するためのＶＰＮ識別子を前記エッジ装置に通知する工程と、
前記エッジ装置が、前記第２の端末装置の端末装置識別子（第２の端末装置識別子）お

よびＶＰＮ識別子を前記ＶＰＮメンバー管理サーバに通知する工程と、
前記ＶＰＮメンバー管理サーバが、前記第２の端末装置識別子および前記ＶＰＮ識別子に基づいて新たにＶＰＮのメンバーとなる前記第２の端末装置を管理するための情報（端末装置管理情報）および前記第２の端末装置が前記ＶＰＮに接続するための情報（端末装置情報）を作成する工程と、
前記ＶＰＮメンバー管理サーバが、前記端末装置管理情報を自サーバ内のデータベースに登録する工程と、
前記ＶＰＮメンバー管理サーバが、端末装置用情報をエッジ装置に通知する工程と、
を含むことを特徴とするＶＰＮ設定更新方法。
【請求項１１】
複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が構成されるＩＰネットワーク上にオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うエッジ装置と、複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、が具備されるデータ通信システムに適用され、
前記オーバーレイネットワークを構築するネットワークに接続されているＶＰＮのいずれかに参加している端末装置からのエッジ装置との間の論理的コネクションおよび参加中のＶＰＮを介した既存ＶＰＮの削除指示に応じてＶＰＮの設定を更新する際に、
前記端末装置が、削除を要求するＶＰＮを識別するためのＶＰＮ識別子を前記エッジ装置に通知する工程と、
前記エッジ装置が、前記論理的コネクションの識別子およびＩＰパケットの先頭に付与されているＶＰＮを識別するためのラベル値、に基づいて前記端末装置の端末装置識別子を取得する工程と、
前記エッジ装置が、前記ＶＰＮ識別子および端末装置識別子を前記ＶＰＮメンバー管理サーバに通知する工程と、
前記ＶＰＮメンバー管理サーバが、前記ＶＰＮ識別子および端末装置識別子に基づいて削除するＶＰＮについての必要な情報（ＶＰＮ情報）を特定し、当該ＶＰＮ情報の自サーバ内データベースへの登録を解除する工程と、
を含むことを特徴とするＶＰＮ設定更新方法。
【請求項１２】
複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が構成されるＩＰネットワーク上にオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うエッジ装置と、複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、が具備されるデータ通信システムに適用され、
前記オーバーレイネットワークを構築するネットワークに接続されているＶＰＮのいずれかに参加している第１の端末装置からのエッジ装置との間の論理的コネクションを介した所定のＶＰＮに登録されているメンバーの登録削除要求に応じてＶＰＮの設定を更新する際に、
前記第１の端末装置が、メンバー登録から削除する第２の端末装置を識別するための端末装置識別子およびメンバー登録先のＶＰＮを識別するためのＶＰＮ識別子を前記エッジ装置に通知する工程と、
前記エッジ装置が、前記第２の端末装置の端末装置識別子（第２の端末装置識別子）およびＶＰＮ識別子を前記ＶＰＮメンバー管理サーバに通知する工程と、
前記ＶＰＮメンバー管理サーバが、前記第２の端末装置識別子およびＶＰＮ識別子に基づいて削除要求する前記第２の端末装置のＶＰＮ登録情報（端末装置管理情報）を特定し、当該端末装置管理情報の自サーバ内データベースへの登録を解除する工程と、
前記エッジ装置が、前記第２の端末装置がＶＰＮに参加するために登録されている情報を前記オーバーレイネットワーク上から削除する工程と、
を含むことを特徴とするＶＰＮ設定更新方法。

【請求項１３】
複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が構成されるＩＰネットワーク上にオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うエッジ装置と、該複数のＶＰＮのメンバーとして登録されている端末装置が属するデフォルトＶＰＮのＶＰＮ識別子に基づいて所定のＶＰＮへの接続を要求する端末装置の認証を行う認証サーバと、複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、が具備されるデータ通信システムに適用され、
前記オーバーレイネットワークを構築するネットワークに接続されているＶＰＮに対して、当該ＶＰＮのメンバーである端末装置が、当該ＶＰＮに参加するためにＶＰＮの設定を更新する際に、
メンバーとなっているＶＰＮに参加しようとする端末装置が、前記エッジ装置に対して当該端末装置の識別情報（端末装置識別子）を含んだ論理的コネクションの確立要求を行う工程と、
前記エッジ装置が、前記端末装置識別子を前記認証サーバに通知する工程と、
前記認証サーバが、認証処理が正常に終了した場合に、前記端末装置がメンバーとなっているＶＰＮを識別するためのＶＰＮ識別子を前記エッジ装置に対して通知する工程と、
前記ＶＰＮ識別子の通知を受けたエッジ装置が、当該ＶＰＮ識別子および前記端末装置識別子を前記ＶＰＮメンバー管理サーバに通知して当該ＶＰＮ識別子に対応するＶＰＮに参加するための情報の通知を要求する工程と、
を含むことを特徴とするＶＰＮ設定更新方法。
【請求項１４】
前記エッジ装置および前記端末装置が、ＶＰＮを識別するためのラベルを付与したＩＰパケットの送受信を前記論理的コネクション上で行うことを特徴とする請求項１３に記載のＶＰＮ設定更新方法。
【請求項１５】
複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が構成されるＩＰネットワーク上にオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うエッジ装置と、複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、が具備されるデータ通信システムに適用され、
前記オーバーレイネットワークを構築するネットワークに接続されているＶＰＮのいずれかに参加している端末装置からのエッジ装置との間の論理的コネクションを介した、参加中のＶＰＮと異なるＶＰＮへの参加要求に応じて、ＶＰＮの設定を更新する際に、
前記端末装置が、新たに参加するＶＰＮを識別するためのＶＰＮ識別子を前記エッジ装置に通知するＶＰＮ識別子通知工程と、
前記エッジ装置が、前記ＶＰＮ識別子に基づいて前記端末装置の端末装置識別子を取得する端末装置識別子取得工程と、
前記エッジ装置が、前記ＶＰＮ識別子通知工程および前記端末装置識別子取得工程において入手した、ＶＰＮ識別子および端末装置識別子を、前記ＶＰＮメンバー管理サーバに通知して当該ＶＰＮ識別子に対応するＶＰＮに参加するための情報の通知を要求する工程と、
を含むことを特徴とするＶＰＮ設定更新方法。
【請求項１６】
複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が構成されるＩＰネットワーク上にオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うエッジ装置と、複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、が具備されるデータ通信システムに適用され、
前記オーバーレイネットワークを構築するネットワークに接続されているＶＰＮのいず

れかに参加している端末装置からのエッジ装置との間の論理的コネクションを介した、参加中のＶＰＮからの離脱要求に応じて、ＶＰＮの設定を更新する際に、
前記端末装置が、離脱を希望するＶＰＮを識別するためのＶＰＮ識別子を前記エッジ装置に通知する工程と、
前記エッジ装置が、前記端末装置のＶＰＮに参加するために登録されている情報を前記オーバーレイネットワーク上から削除する工程と、
を含むことを特徴とするＶＰＮ設定更新方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を備え、一つの端末装置（データ通信端末装置）が同時に複数のＶＰＮに接続可能なネットワークに関するものであって、特に、端末装置がＶＰＮへの参加および離脱、などの処理を動的に行うデータ通信システムおよび、その端末装置ならびにＶＰＮ設定更新方法に関するものである。
【背景技術】
【０００２】
ＶＰＮとは、共有（公衆）ネットワークを仮想的な専用線として利用するために当該ネットワーク上に構築された私設通信網（プライベートネットワーク）または、その利用技術を示す用語である。近時、このＶＰＮを利用して、出張先などの遠隔地から自社のイントラネットなどへの接続を可能とするサービスが提供されており、コストのかかる専用線の代替になる新しいサービスとして、企業を中心として着実に浸透している。
【０００３】
ところで、遠隔地の端末装置が自社のイントラネットなどに接続するためには、ＶＰＮとして構成されたネットワークに端末装置が接続できなければならない。ここで、ＶＰＮを構成するための従来方式として、例えば、ＩＰＳｅｃを用いる方式や、ＭＰＬＳ／ＶＰＮ（下記、非特許文献１を参照）を用いる方式などがある。ただし、これらのいずれの方式を用いた場合でも、端末装置がＶＰＮに接続するためには、論理的なコネクション（例えば、ＩＰＳｅｃを用いる場合はＩＰＳｅｃトンネルモードＳｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ（以下「ＩＰｓｅｃ＿ＳＡ」と呼称）、ＭＰＬＳ／ＶＰＮの場合はＰｏｉｎｔ　ｔｏ　Ｐｏｉｎｔ　Ｐｒｏｔｏｃｏ　ｏｖｅｒ　Ｅｔｈｅｒｎｅｔ（登録商標）セッション（以下「ＰＰＰｏＥセッション」と呼称）を確立する相手となるエッジ装置を必要とする。このエッジ装置は、端末装置の認証情報に基づいて端末装置が接続しようとするＶＰＮを識別して当該ＶＰＮへの接続可否を決定するとともに、端末装置にＩＰアドレスを割り当てる機能を有し、このようなエッジ装置の機能に基づいて端末装置とＶＰＮとの接続が実現される。
【０００４】
【非特許文献１】ＩＥＴＦ　ＲＦＣ２５４７ｂｉｓ
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記従来技術にかかるＶＰＮ構成方式には、以下に示すような問題点がある。
【０００６】
［端末装置とＶＰＮとの接続に伴う種々の問題］
端末装置がＶＰＮに接続するためには、ＶＰＮを構成するエッジ装置には、以下に示すいずれかの要件を満たしている必要があった。
（ａ）端末装置と当該端末装置が接続を希望するＶＰＮとの間の接続を仲介するための必要な設定が予めエッジ装置に具備されている。
（ｂ）端末装置がエッジ装置に接続してきた時点で、エッジ装置とＶＰＮとの間の接続

を動的に確立する手段および手順が具備されている。

【０００７】

ここで、上記（ａ）の要件が満たされる場合、端末装置の接続対象となるＶＰＮの数が多くなるとエッジ装置への設定作業の手間が膨大になるといった問題点や、メモリ等のリソースが、使用されないＶＰＮのためにも消費されるといった問題点があった。また、動的にＶＰＮを生成／削除する機能をサポートする場合、生成／削除されるＶＰＮに関する情報を、全てのエッジ装置に対して設定する必要があり、エッジ装置間でやりとりされるメッセージ数が増加し、処理が繁雑になるという問題点があった。

【０００８】

一方、上記（ｂ）の要件が満たされる場合、端末装置がエッジ装置に接続してきた時点で、エッジ装置とＶＰＮとの間の接続を動的に確立するための機能は、ＩＰＳｅｃ方式にもＭＰＬＳ／ＶＰＮ方式にも標準の規定がない。そのため、独自の手順で上記機能を実現する必要がある。

【０００９】

例えば、ＩＰＳｅｃ方式を用いる場合、端末装置がエッジ装置に接続してきた時点で、エッジ装置とＶＰＮとの間の接続を動的に確立するためには、エッジ装置に対して当該ＶＰＮに接続するための設定を動的に行った上で、さらにエッジ装置自身がＶＰＮへの接続を動的に行う必要がある。この機能を実現するためには、例えばエッジ装置をＶＰＮに接続するための別のエッジ装置を設けておく必要がある。そして、エッジ装置は、目的のＶＰＮに接続するためにＩＰＳｅｃ＿ＳＡを確立する相手方となる相手方エッジ装置のＩＰアドレスを何らかの手段（例えば、設定データの読み出しを行う手段、外部データベースを検索する手段など）を用いて取得し、さらに、相手方エッジ装置との間にＩＰＳｅｃ＿ＳＡを確立するための複数往復（アグレッシブモードで３往復、メインモードで４．５往復）のメッセージのやりとりが必要となる。さらには、動的にＶＰＮを生成／削除する場合には、当該ＶＰＮを収容するエッジ装置を決定し、そのＶＰＮを実現するための設定を当該エッジ装置に行う必要がある。

【００１０】

一方、ＭＰＬＳ／ＶＰＮを使用する場合、端末装置がエッジ装置に接続してきた時点で、エッジ装置とＶＰＮとの間の接続を動的に確立するためには、エッジ装置に対して接続先のＶＰＮに対応するＶＲＦ（Ｖｉｒｔｕａｌ Ｒｏｕｔｉｎｇ Ｆｏｒｗａｒｄｉｎｇ）およびインタフェースの設定を行うとともに、他の全てのエッジ装置との間で、ＢＧＰ（Ｂｏｒｄｅｒ Ｇａｔｅｗａｙ Ｐｒｏｔｏｃｏｌ）によりＶＰＮ内のルーティング情報の交換を行う必要があり、全エッジ装置数に比例する数のメッセージ伝送が必要となる。

【００１１】

このように、ＩＰＳｅｃ方式やＭＰＬＳ／ＶＰＮ方式に基づいて動的なＶＰＮの生成／削除をサポートするためには、多くのメッセージ伝送が必要となり処理が繁雑になるという問題点があった。

【００１２】

［端末装置数増加に対するスケーラビリティの問題］

エッジ装置を含むＶＰＮ内でのルーティング情報伝播は、通常のＩＰルーティングプロトコル（例えば、ＲＩＰ（Ｒｏｕｔｉｎｇ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）や、ＯＳＰＦ（Ｏｐｅｎ Ｓｈｏｒｔｅｓｔ Ｐａｔｈ Ｆｉｒｓｔ）など）に基づいて行われる。ここで、端末装置が任意のエッジ装置経由で接続しても同一ＩＰアドレスでのＶＰＮ接続を可能とする場合、端末装置のＩＰアドレスが、ＶＰＮ内でエッジ装置に割当てられるサブネットアドレスに属さないケースが生じるのを防止するためには、エッジ装置は端末装置に割当てたホストアドレスをルーティングプロトコルで広告する必要がある。そして、ホストアドレスへのルーティング情報が、全てのエッジ装置と、ＶＰＮ内の全てのルータのルーティングテーブルに設定されることと、端末装置の接続／切断の度にルーティングプロトコルによりルーティング情報が変化したことがＶＰＮ全体に広告され

ることになるので、端末装置数増加に対するスケーラビリティが悪いという問題点があった。

【００１３】

なお、端末装置がモバイルＩＰの機能をサポートしている場合には、ＶＰＮ内にモバイルＩＰのホームエージェント（Ｈｏｍｅ　Ａｇｅｎｔ：ＨＡ）を設置し、エッジ装置から割当てられたＩＰアドレスを気付アドレス（Ｃａｒｅ　ｏｆ　Ａｄｄｒｅｓｓ：ＣｏＡ）として使用して通信することで、エッジ装置が端末装置のホストアドレスをルーティングプロトコルで広告しないようにする手法もある。しかしながら、この手法では、モバイルＩＰの使用が前提とされるので、当該ＶＰＮにアクセスする全ての端末装置がモバイルＩＰの機能を備えていなければならず、また、ホームエージェントを設置しなければならないという問題点があった。

【００１４】

本発明は、上記に鑑みてなされたものであって、ＩＰＳｅｃ方式やＭＰＬＳ／ＶＰＮ方式を使用する場合よりも簡潔な手順で、動的なＶＰＮの生成／削除を可能とするデータ通信システムおよび、その端末装置ならびにＶＰＮ設定更新方法を得ることを目的とする。

【００１５】

また、端末装置がモバイルＩＰをサポートすることなく、任意のエッジ装置経由でＶＰＮに接続した場合であっても、ＶＰＮ内にて同一ＩＰアドレスを使用して通信を行うことを可能とするデータ通信システムおよび、その端末装置ならびにＶＰＮ設定更新方法を得ることを目的とする。

【課題を解決するための手段】

【００１６】

上述した課題を解決し、目的を達成するために、本発明は、ＩＰネットワーク上に複数のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を構成可能とするデータ通信システムであって、ＶＰＮのメンバーとして登録されている端末装置が属するデフォルトＶＰＮのＶＰＮ識別子の情報を保持し、該デフォルトＶＰＮのＶＰＮ識別子に基づいて所定のＶＰＮへの接続を要求する端末装置の認証を行う認証サーバと、前記ＩＰネットワーク上にＤＨＴ（Ｄｉｓｔｒｉｂｕｔｅｄ　Ｈａｓｈ　Ｔａｂｌｅ）方式の検索機能を提供するオーバーレイネットワークを構築し、端末装置とＶＰＮとの接続処理およびＩＰパケットの転送処理を行うための所定情報を保持するエッジ装置と、前記複数のＶＰＮおよび該ＶＰＮのメンバーとなりうる端末装置を管理するための所定情報を保持するＶＰＮメンバー管理サーバと、を備え、前記エッジ装置は、ＶＰＮへの接続を要求する端末装置との論理的コネクションを確立した後、該端末装置が属するＶＰＮの情報をＶＰＮメンバー管理サーバから取得し、該ＶＰＮメンバー管理サーバから取得したＶＰＮの情報に基づいて該端末装置と該端末装置が接続を要求するＶＰＮとの接続設定処理を行うことを特徴とする。

【発明の効果】

【００１７】

この発明によれば、ＩＰネットワーク上にＤＨＴ方式の検索機能を提供するオーバーレイネットワークを構築するエッジ装置と、複数のＶＰＮおよびＶＰＮのメンバーとなりうる端末装置を管理するＶＰＮメンバー管理サーバとが具備され、エッジ装置は、ＶＰＮへの接続を要求する端末装置との論理的コネクションを確立した後に、ＶＰＮメンバー管理サーバから取得したＶＰＮの情報に基づいて端末装置と端末装置が接続を要求するＶＰＮとの接続設定処理を行うようにしているので、ＩＰＳｅｃ方式やＭＰＬＳ／ＶＰＮ方式を使用する場合よりも簡潔な手順で、動的なＶＰＮの生成／削除が可能となり、また、端末装置がモバイルＩＰをサポートすることなく、任意のエッジ装置経由でＶＰＮに接続した場合であっても、ＶＰＮ内にて同一ＩＰアドレスを使用した通信が可能となるという効果を奏する。

【発明を実施するための最良の形態】

【００１８】

以下に、本発明にかかるデータ通信システムおよびデータ通信方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態により本発明が限定されるものではない。

【００１９】

実施の形態１．

図１は、本発明の実施の形態１にかかるデータ通信システムを実現するネットワークの構成例を示す図であり、当該ネットワークは、エッジ装置間を接続するＩＰマルチキャストに対応したＩＰネットワークに接続する端末装置１－１，１－２，…，１－ｍと、上記ＩＰネットワークに接続され、オーバーレイネットワークを構築するエッジ装置２－１，２－２，…，２－ｎと、ＶＰＮ毎の各種情報を管理するＶＰＮメンバー管理サーバ３と、端末装置の認証を行う認証サーバ４と、を備えている。

【００２０】

ここで、本発明にかかるデータ通信システムを実現する本実施の形態のネットワークでは、ＩＰアドレスのサブネット部分でＶＰＮを識別することとする。このようにすれば、同じＶＰＮに属する端末装置を、同じサブネットに所属させることができるとともに、複数のＶＰＮをＩＰネットワーク上に同時に実現することができる。なお、サブネット部分のビット長は、必ずしも同一である必要はないが、処理の簡素化のためには、いずれのＶＰＮでも同一であることが好ましい。

【００２１】

また、当該ＩＰネットワークにおいて送受信を行うＩＰパケットには、どのＶＰＮ上で送受信するＩＰパケットかを識別可能にするためのラベルを付与することができる。なお、このようなラベルを付与することにより、端末装置（図１に示した端末装置１－１～１－ｍ）は、同時に複数のＶＰＮに接続することができる。

【００２２】

（端末装置１の構成）

つづいて、図２は、端末装置１（上記端末装置１－１～１－ｍに相当）の構成例を示す図であり、例えば、ＬｉｎｕｘをＯＳとするＰＣ（パーソナルコンピュータ）を用いることができる。図２に示したように、端末装置１は、ＩＰ通信モジュール１１、トンネル通信モジュール１２、仮想インタフェースドライバ１３、アプリケーション１４、データベース１５を備えている。

【００２３】

ＩＰ通信モジュール１１は、ＩＰネットワークを介して端末装置１およびエッジ装置２の間のＩＰ通信を実現するＩＰプロトコル処理を行う機能を提供し、例えば、Ｌｉｎｕｘに含まれるＩＰプロトコルスタックＳ／Ｗ（ソフトウェア）によって実現される。

【００２４】

また、トンネル通信モジュール１２は、端末装置とエッジ装置間の論理的コネクションを実現するための通信プロトコル処理を行う。例えば、ＩＰＳｅｃトンネルモードを通信プロトコルとして使用することで、論理的コネクションを実現する。ＩＰＳｅｃ＿ＳＡが表す論理的コネクション上で、ラベル付きのＩＰパケットを転送するときは、ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）のＲＦＣ３０３２に定義される、ＭＰＬＳのラベルフォーマットと同じラベルを付与したＩＰパケットを転送する。論理的コネクション上で転送されるラベル付きＩＰパケットが、ユーザトラフィックとなるＩＰパケットか、ＶＰＮに関する制御のためのＩＰパケットかは、ＩＰｖ４ヘッダのＰｒｏｔｏｃｏｌフィールド、もしくは、ＩＰｖ６ヘッダのＮｅｘｔ Ｈｅａｄｅｒフィールドの値を参照し、その値がＶＰＮに関する制御のためのＩＰパケットでないかどうかで判定する。

【００２５】

また、仮想インタフェースドライバ１３は、論理的コネクションの識別子およびラベル値を、ＩＰ通信モジュールに対してＩＰ通信が可能な一つのインタフェースとして見せかけるための機能（仮想インタフェース）を提供するもので、例えば、Ｌｉｎｕｘのデバイ

スドライバとして実現することが可能である。
【００２６】
また、アプリケーション１４は、例えば、Ｌｉｎｕｘ上で動作するアプリケーションで、ソケットインタフェースを用いたＶＰＮ上でのＩＰ通信、仮想インタフェースドライバが提供するＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍ Ｉｎｔｅｒｆａｃｅ）を利用したＶＰＮへの参加／離脱，ＶＰＮの生成／削除，ＶＰＮへのメンバー追加／削除を指示するための制御信号の送受信を行う機能、を実現する。
【００２７】
また、データベース１５は、「仮想インタフェースの識別子をキーとして、仮想インタフェースが使用するラベルの値をデータとするデータベース。」および「ラベルの値をキーとして、ラベルに対応付けられる仮想インタフェースの識別子をデータとするデータベース。」を管理する。そして、登録されているデータの検索機能を提供するＳ／Ｗとして実現される。
【００２８】
上述の構成をとる端末装置１は、通信者間での認証機能、秘匿機能、改竄防止機能を有する論理的コネクションを介して、エッジ装置（図１に示したエッジ装置２－１、…、２－ｎのいずれか）と接続する。そして、端末装置１は、当該論理的コネクションを介してＶＰＮへの参加などを行うための制御メッセージの送受信およびＩＰパケットの送受信を行う。
【００２９】
ここで、上記制御メッセージには、「ＶＰＮ参加要求ＭＳＧ（メッセージ）および応答ＭＳＧ」、「ＶＰＮ離脱要求ＭＳＧおよび応答ＭＳＧ」、「ＶＰＮ生成要求ＭＳＧおよび応答ＭＳＧ」、「ＶＰＮ削除要求ＭＳＧおよび応答ＭＳＧ」、「メンバー追加要求ＭＳＧおよび応答ＭＳＧ」、および「メンバー削除要求ＭＳＧおよび応答ＭＳＧ」がある。端末装置１は、これらのメッセージを使用して、ＶＰＮへの参加および離脱、ＶＰＮの生成および削除、ＶＰＮへのメンバー追加および削除、をエッジ装置（図１に示したエッジ装置２－１、…、２－ｎのいずれか）に対して要求する。
【００３０】
なお、端末装置１は、論理的コネクション上の各ラベル値を、ＩＰパケットが送受信可能な仮想インタフェースとして扱う。
【００３１】
（エッジ装置２の構成）
つづいて、図３は、エッジ装置２（上記エッジ装置２－１～２－ｎに相当）の構成例を示す図であり、例えば、ＬｉｎｕｘをＯＳとするＰＣを用いることができる。図３に示したように、エッジ装置２は、ＩＰ通信モジュール２１、データベース２５、ＤＨＴ検索モジュール２６、制御モジュール２７、トンネル通信モジュール１２を備えている。なお、トンネル通信モジュール１２は、上記端末装置１が備えているトンネル通信モジュールと同一である。
【００３２】
ＩＰ通信モジュール２１は、ＩＰネットワークを介して端末装置１およびエッジ装置２の間のＩＰ通信と、他のエッジ装置との間（上記エッジ装置２－１、２－２、…、２－ｎの間）のＩＰ通信と、エッジ装置２および認証サーバ４の間のＩＰ通信と、エッジ装置２－１、２－２、…、２－ｎおよびＶＰＮメンバー管理サーバ３の間のＩＰ通信を実現するＩＰプロトコル処理を行う機能を提供し、例えば、Ｌｉｎｕｘに含まれるＩＰプロトコルスタックＳ／Ｗによって実現される。
【００３３】
また、データベース２５は、エッジ装置２に存在するデータベースを管理する。そして、登録されているデータの検索機能を提供するＳ／Ｗとして実現さる。なお、データベース２５は、以下に示す６種類のデータベースを総括したものである。
【００３４】

「端末装置との間の論理的コネクションの識別子とラベル値のペアをキーとして、ＶＰＮ識別子と端末装置識別子とＶＰＮ内ＩＰアドレスをデータとするデータベース」、「ＶＰＮ内ＩＰアドレスをキーとして、そのＩＰアドレスを使用している端末装置との間の論理的コネクションの識別子とラベル値のペアをデータとするデータベース」、「ＶＰＮ識別子をキーとして、そのＶＰＮへの接続に使用される端末装置との間の論理的コネクションの識別子とラベル値のペアのリストをデータとするデータベース」、「ＶＰＮ識別子をキーとして、そのＶＰＮに対応付けられるマルチキャストＩＰアドレスとサブネットアドレスをデータとするデータベース」、「マルチキャストＩＰアドレスをキーとして、そのマルチキャストＩＰアドレスに対応付けられるＶＰＮ識別子をデータとするデータベース」、「サブネットアドレスをキーとして、そのサブネットアドレスに対応付けられるＶＰＮ識別子をデータとするデータベース」。

【００３５】

なお、上記の６つのデータベースは、必ずしもそれぞれが個別のデータベースとして記憶されている必要はなく、一つのデータベースが構成され、所定項目のデータをキーとして、上記６つのデータベースにおける各データ項目が抽出されるように構成されるものであってもよい。

【００３６】

また、ＤＨＴ検索モジュール２６は、例えば「Ｂｕｉｌｄｉｎｇ Ｐｅｅｒ－ｔｏ－Ｐｅｅｒ Ｓｙｓｔｅｍｓ Ｗｉｔｈ Ｃｈｏｒｄ, ａ Ｄｉｓｔｒｉｂｕｔｅｄ Ｌｏｏｋｕｐ Ｓｅｒｖｉｃｅ, Ｆ. Ｄａｂｅｋ, Ｅ. Ｂｒｕｎｓｋｉｌｌ, Ｍ. Ｋａａｓｈｏｅｋ, Ｄ. Ｋａｒｇｅｒ, Ｒ. Ｍｏｒｒｉｓ, Ｉ. Ｓｔｏｉｃａ ａｎｄ Ｈ. Ｂａｌａｋｒｉｓｈｎａｎ, Ｐｒｏｃｅｅｄｉｎｇ ｏｆ ｔｈｅ ８ｔｈ Ｗｏｒｋｓｈｏｐ ｏｎ Ｈｏｔ Ｔｏｐｉｃｓ ｏｎ Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍｓ, Ｍａｙ, ２００１」に示されるＣｈｏｒｄの実現方法例において述べられる、ＤＨＴ（Ｄｉｓｔｒｉｂｕｔｅｄ Ｈａｓｈ Ｔａｂｌｅ）検索方式を実現するモジュールであり、ある端末装置のＩＰアドレスが与えられたときに、その端末装置が論理的コネクションを確立しているエッジ装置を決定するための機能を提供する（以下「論理的コネクションを確立しているエッジ装置…」を単に「接続しているエッジ装置…」と表現する。）。

【００３７】

また、制御モジュール２７は、例えば、Ｓ／Ｗとして実現され、エッジ装置２を構成する他のモジュール（ＩＰ通信モジュール２１、トンネル通信モジュール１２、など）を制御する。

【００３８】

そして、ＩＰネットワークに接続したエッジ装置２は、他のエッジ装置と共にオーバーレイネットワークを構築し、当該ネットワークにおいて、例えば上述したＣｈｏｒｄの方式に従って、ＤＨＴ方式で検索を行う機能を提供する。

【００３９】

（ＶＰＮメンバー管理サーバ３の構成）

つづいて、図４に基づいてＶＰＮメンバー管理サーバ３を説明する。図４は、ＶＰＮメンバー管理サーバ３の構成例を示す図であり、例えば、ＬｉｎｕｘをＯＳとするＰＣを用いることができる。図４に示したように、ＶＰＮメンバー管理サーバ３は、ＩＰ通信モジュール３１、データベース３５、制御モジュール３７、ＤＨＴ検索モジュール２６を備えている。なお、ＤＨＴ検索モジュール２６は、上記エッジ装置２が備えているＤＨＴ検索モジュールと同一である。

【００４０】

ＩＰ通信モジュール３１は、ＩＰネットワークを介してエッジ装置２およびＶＰＮメンバー管理サーバ３の間のＩＰ通信を実現するＩＰプロトコル処理を行う機能を提供し、例えば、Ｌｉｎｕｘに含まれるＩＰプロトコルスタックＳ／Ｗによって実現される。

【００４１】

また、データベース３５は、ＶＰＮ識別子をキーとしてＶＰＮメンバー管理サーバ３に

存在するデータベースをＶＰＮ毎に管理する。そして、登録されているデータの検索機能を提供するＳ／Ｗとして実現する。なお、データベース３５が管理するデータベースは、「ＶＰＮ上のブロードキャスト／マルチキャストパケットを転送するときに使用するマルチキャストＩＰアドレス情報」、「ＶＰＮに対応付けられるサブネットアドレス情報」、「ＶＰＮメンバーとなりうる端末装置毎の情報（端末装置識別子および端末装置に割当てるＩＰアドレスの組のリスト）」であり、これをＶＰＮ情報データベースと呼ぶ。

【００４２】

また、制御モジュール３７は、例えば、Ｓ／Ｗとして実現され、ＶＰＮメンバー管理サーバ３を構成する他のモジュール（ＩＰ通信モジュール３１など）を制御する。

【００４３】

そして、ＶＰＮメンバー管理サーバ３は、ＶＰＮ識別子と端末装置識別子とを含むＶＰＮメンバー問合せ要求ＭＳＧを受信したときに、端末装置識別子で指定される端末装置がＶＰＮ識別子で指定されるＶＰＮに参加可能かどうかをチェックした結果と、参加可能な場合に端末装置に割当てるＩＰアドレスと、ＶＰＮ上のブロードキャスト／マルチキャストパケットを転送するときに使用するマルチキャストＩＰアドレスと、ＶＰＮに対応付けられるサブネットアドレスとを、ＶＰＮメンバー問合せ応答ＭＳＧで通知（返信）する。

【００４４】

（認証サーバ４の構成）

つづいて、図５は、認証サーバ４の構成例を示す図であり、例えば、ＬｉｎｕｘをＯＳとするＰＣを用いることができる。図５に示したように、認証サーバ４は、ＩＰ通信モジュール４１、データベース４５、制御モジュール４７を備えている。

【００４５】

ＩＰ通信モジュール４１は、ＩＰネットワークを介してエッジ装置２－１、２－２、…、２－ｎおよび認証サーバ４の間のＩＰ通信を実現するＩＰプロトコル処理を行う機能を提供し、例えば、Ｌｉｎｕｘに含まれるＩＰプロトコルスタックＳ／Ｗによって実現される。

【００４６】

また、データベース４５は、認証サーバ４に存在するデータベースを管理する。そして、登録されているデータの検索機能を提供するＳ／Ｗとして実現さる。なお、データベース４５は、「端末装置認証のために必要な秘密情報」、「端末装置が属するデフォルトＶＰＮのＶＰＮ識別子」を管理する。

【００４７】

また、制御モジュール４７は、例えば、Ｓ／Ｗとして実現され、認証サーバ４を構成する他のモジュール（ＩＰ通信モジュール４１など）を制御する。

【００４８】

そして、認証サーバ４は、認証要求ＭＳＧを受信した場合、当該認証要求ＭＳＧに含まれる端末装置識別子と端末装置認証に必要な情報とを元に端末装置の認証処理を行い、当該認証結果と、端末装置がデフォルトで属するＶＰＮのＶＰＮ識別子とを認証応答ＭＳＧで通知（返信）する。

【００４９】

（端末装置によるＶＰＮの作成）

つづいて、端末装置１－１が既存のＶＰＮとの接続を介して新しいＶＰＮを作成する動作の一例を図６に基づいて説明する。なお、図６は端末装置１－１がＶＰＮを作成する動作の一例を示すシーケンス図である。また、端末装置１－１とエッジ装置２－１との間で、論理的コネクションが確立済みとする。

【００５０】

端末装置１－１は、仮想インタフェース上で、新たに作成したいＶＰＮを示すＶＰＮ識別子を含むＶＰＮ生成要求ＭＳＧを、エッジ装置２－１に対して送信する（ステップＳ１）。

【００５１】

エッジ装置２－１は、端末装置１－１から受信したＶＰＮ生成要求ＭＳＧに含まれる論理的コネクションの識別子とラベル値のペアをキーとして、端末装置１－１の端末装置識別子をデータベース２５で検索する（ステップＳ２）。そして、エッジ装置２－１は、上記検索により取得した端末装置１－１の端末装置識別子および上記ＶＰＮ識別子を含むＶＰＮ作成要求ＭＳＧをＶＰＮメンバー管理サーバ３宛に送信する（ステップＳ３）。

【００５２】

ＶＰＮメンバー管理サーバ３は、受信したＶＰＮ作成要求ＭＳＧに含まれるＶＰＮ識別子が未登録の場合、以下に述べる処理を実行し、データベース３５（ＶＰＮ情報データベース）を更新する（ステップＳ４）。

【００５３】

ＶＰＮメンバー管理サーバ３は、「上記ＶＰＮ識別子に対応するＶＰＮ（新規作成するＶＰＮ）に割当てるサブネットアドレス（他のＶＰＮ識別子に割当済みのサブネットアドレスと重複しない値とする）」および「上記ＶＰＮ識別子に対応するＶＰＮ上のブロードキャスト／マルチキャストパケットを転送するときに使用するマルチキャストＩＰアドレス（他のＶＰＮ識別子に割当済みのマルチキャストＩＰアドレスと重複しない値とする）」を決定する。そして、ＶＰＮメンバー管理サーバ３は、上記データを、上記ＶＰＮ識別子をキーとして管理するデータベースとしてデータベース３５に追加する。さらに、ＶＰＮメンバー管理サーバ３は、データベース３５に含まれる「ＶＰＮメンバーとなりうる端末装置毎の端末装置識別子および端末装置に割当てるＩＰアドレスの組のリスト」に、「上記ＶＰＮ作成要求ＭＳＧで指定された端末装置識別子と、それに割当てるＩＰアドレスの組の情報」を追加する（以上、ステップＳ４）。

【００５４】

そして、ＶＰＮメンバー管理サーバ３は、ＶＰＮ作成応答ＭＳＧ（作成成功、端末装置に割当てるＩＰアドレス，ＶＰＮ上のブロードキャスト／マルチキャストパケットを転送するときに使用するマルチキャストＩＰアドレス，ＶＰＮに対応付けられるサブネットアドレスを含む）を、エッジ装置２－１へ送信する（ステップＳ５）。なお、ＶＰＮメンバー管理サーバ３は、上記エッジ装置２－１から受信したＶＰＮ作成要求ＭＳＧに含まれるＶＰＮ識別子が登録済みの場合、ＶＰＮの作成失敗を示すＶＰＮ作成応答ＭＳＧ（作成失敗）をエッジ装置２－１へ送信する。

【００５５】

ＶＰＮ作成の成功を示すＶＰＮ作成応答ＭＳＧを受信した場合、エッジ装置２－１は、端末装置１－１との論理的コネクション上で、このＶＰＮ内でパケットを転送する際にＩＰパケットの先頭に付けるラベルが使用するラベル値を決定する（ステップＳ６）。なお、当該ラベルの値は、論理的コネクション内で一意になる様に決める。

【００５６】

つぎに、エッジ装置２－１は、以下に述べる処理を実行し、データベース２５を更新する（ステップＳ７）。

【００５７】

エッジ装置２－１は、端末装置１－１との間の論理的コネクションの識別子とラベル値のペアをキーとして、ＶＰＮ識別子と端末装置識別子とＶＰＮ内ＩＰアドレスをデータベース２５に記録する。また、エッジ装置２－１は、ＶＰＮ内ＩＰアドレスをキーとして、端末装置１－１との間の論理的コネクションの識別子とラベル値のペアをデータベース２５に記録する。さらに、エッジ装置２－１は、ＶＰＮ識別子をキーとして、データベース２５を検索して得られる、端末装置との間の論理的コネクションの識別子とラベル値のペアのリストに、論理的コネクションの識別子とラベル値のペアを追加する。（データベース２５のリストを更新する）。なお、エッジ装置２－１は、ＶＰＮ識別子をキーとしたデータベース２５の検索の結果、端末装置との間の論理的コネクションの識別子とラベル値のペアのリストが得られない（指定のＶＰＮ識別子に対応するリストをデータベース２５に保持していない）場合は、ＶＰＮ識別子をキーとして空のリストをデータとするデータをデータベース２５に追加した上で（空のリストを新規作成した上で）、論理的コネクシ

ョンの識別子とラベル値のペアを追加する（以上、ステップＳ７）。
【００５８】
そして、エッジ装置２－１は、上記ＶＰＮ生成要求ＭＳＧに付与されていたものと同じラベルを付与したＶＰＮ生成応答ＭＳＧ（成功、端末装置１－１に割り当てたＩＰアドレスおよびラベル値を含む）を、論理的コネクション上で端末装置１－１に送信する（ステップＳ８）。
【００５９】
以下、エッジ装置２－１は、前述したＤＨＴ方式検索機能を提供するオーバーレイネットワーク上に端末装置１－１に割当てたＩＰアドレスをキーとして、自装置のＩＰアドレスをデータとするレコードを登録する（ステップＳ９）。また、新規作成したＶＰＮに端末装置１－１が接続する場合、エッジ装置２－１は、以下の処理を行う。
【００６０】
エッジ装置２－１は、「（新規作成したＶＰＮの）ＶＰＮ識別子をキーとした、マルチキャストＩＰアドレスおよびサブネットアドレス」のデータ、「マルチキャストＩＰアドレスをキーとした、ＶＰＮ識別子」のデータ、および「サブネットアドレスをキーとした、ＶＰＮ識別子」のデータをデータベース２５に記録する。そして、マルチキャストＩＰアドレス宛パケットを受信する様に、マルチキャストＩＰアドレスにＪＯＩＮする。
【００６１】
なお、エッジ装置２－１は、ＶＰＮメンバー管理サーバ３から、ＶＰＮ作成失敗を示すＶＰＮ作成応答ＭＳＧを受信した場合、その旨を示すＶＰＮ生成応答ＭＳＧ（失敗）を端末装置１－１に送信する。
【００６２】
端末装置１－１は、ＶＰＮ生成の成功を示すＶＰＮ生成応答ＭＳＧ（生成成功）を受信した場合、論理的コネクションの識別子とＶＰＮ生成応答ＭＳＧに示されるラベル値のペアを仮想インタフェースとして扱い、ＶＰＮ生成応答ＭＳＧに示されるＩＰアドレスを、その仮想インタフェースのＩＰアドレスとして設定する。つぎに、端末装置１－１は、仮想インタフェースを表す識別子を決定し、仮想インタフェース識別子とラベル値の対応付けを、データベース１５に記録する（ステップＳ１０）。
【００６３】
（端末装置によるＶＰＮへのメンバーの追加）
つづいて、端末装置１－１が既存のＶＰＮへメンバーを追加する動作の一例を図７に基づいて説明する。なお、図７は、既存のＶＰＮへメンバーを追加する動作の一例を示すシーケンス図である。また、端末装置１－１とエッジ装置２－１との間で、論理的コネクションが確立済みとする。
【００６４】
端末装置１－１は、仮想インタフェース上で、メンバーを追加したいＶＰＮを示すＶＰＮ識別子と追加したいメンバーを示す端末装置識別子とを含むメンバー追加要求ＭＳＧを、エッジ装置２－１に対して送信する（ステップＳ１１）。
【００６５】
エッジ装置２－１は、端末装置１－１から受信したメンバー追加要求ＭＳＧに含まれる論理的コネクションの識別子とラベル値のペアをキーとして、追加要求元の端末装置である端末装置１－１の端末装置識別子（以下「追加要求元端末装置識別子」と呼称）をデータベース２５で検索する（ステップＳ１２）。そして、エッジ装置２－１は、上記検索により取得した追加要求元端末装置識別子、上記メンバー追加要求ＭＳＧに含まれていた端末装置識別子（以下「追加対象端末装置識別子」と呼称）および上記ＶＰＮ識別子を含むＶＰＮメンバー追加要求ＭＳＧをＶＰＮメンバー管理サーバ３宛に送信する（ステップＳ１３）。
【００６６】
ＶＰＮメンバー管理サーバ３は、以下に述べる処理を実行し、データベース３５（ＶＰＮ情報データベース）を更新する（ステップＳ１４）。

【００６７】
ＶＰＮメンバー管理サーバ３は、エッジ装置２－１から受信したＶＰＮメンバー追加要求ＭＳＧに含まれるＶＰＮ識別子をキーとしてデータベース３５を検索する。当該検索結果である「ＶＰＮメンバーとなりうる端末装置毎の情報（端末装置アドレスおよび端末装置に割り当てるＩＰアドレスの組のリスト）」に上記追加対象端末装置識別子が未登録である場合、ＶＰＮメンバー管理サーバ３は、追加対象端末装置に割り当てるＩＰアドレスを決定する。さらに、ＶＰＮメンバー管理サーバ３は、当該ＩＰアドレスと上記追加対象端末装置識別子を、データベース３５に含まれる「ＶＰＮメンバーとなりうる端末装置毎の情報（端末装置アドレスおよび端末装置に割り当てるＩＰアドレスの組のリスト）」へ追加する（以上、ステップＳ１４）。

【００６８】
そして、ＶＰＮメンバー管理サーバ３は、ＶＰＮへのメンバー追加の成功を示すＶＰＮメンバー追加応答ＭＳＧ（追加成功）をエッジ装置２－１へ送信する（ステップＳ１５）。なお、上記追加対象端末装置識別子がＶＰＮ識別子をキーとして検索された「ＶＰＮメンバーとなりうる端末装置毎の情報」に登録済みである場合、ＶＰＮメンバー管理サーバ３は、ＶＰＮへのメンバー追加の失敗を示すＶＰＮメンバー追加応答ＭＳＧ（追加失敗）をエッジ装置２－１へ送信する。

【００６９】
エッジ装置２－１は、ＶＰＮメンバー管理サーバ３からＶＰＮメンバー追加応答ＭＳＧを受信すると、その結果（追加成功／追加失敗）をメンバー追加応答ＭＳＧに設定して端末装置１－１に通知する（ステップＳ１６）。

【００７０】
（端末装置によるＶＰＮの削除）
つづいて、端末装置１－１がＶＰＮとの接続を介して当該ＶＰＮとは異なる既存のＶＰＮを削除する動作の一例を図８に基づいて説明する。なお、図８は、端末装置１－１がＶＰＮを削除する動作の一例を示すシーケンス図である。また、端末装置１－１とエッジ装置２－１との間で、論理的コネクションが確立済みとする。

【００７１】
端末装置１－１は、仮想インタフェース上で、削除したいＶＰＮを示すＶＰＮ識別子を含むＶＰＮ削除要求ＭＳＧを、エッジ装置２－１に対して送信する（ステップＳ２１）。

【００７２】
エッジ装置２－１は、端末装置１－１から受信したＶＰＮ削除要求ＭＳＧに含まれる論理的コネクションの識別子とラベル値のペアをキーとして、削除要求元の端末装置である端末装置１－１の端末装置識別子をデータベース２５で検索する（ステップＳ２２）。そして、エッジ装置２－１は、上記検索により取得した端末装置識別子および上記ＶＰＮ削除要求ＭＳＧに含まれていたＶＰＮ識別子（以下「削除対象ＶＰＮ識別子」と呼称）を含むＶＰＮ消去要求ＭＳＧをＶＰＮメンバー管理サーバ３宛に送信する（ステップＳ２３）。

【００７３】
ＶＰＮメンバー管理サーバ３は、受信したＶＰＮ消去要求ＭＳＧに含まれる削除対象ＶＰＮ識別子が登録済み、かつ削除対象ＶＰＮ識別子をキーとしてデータベース３５（ＶＰＮ情報データベース）に登録されている「ＶＰＮメンバーとなりうる端末装置毎の端末装置識別子および端末装置に割当てるＩＰアドレスの組」のリストが空である場合、以下に述べる処理を実行し、データベース３５を更新する（ステップＳ２４）。

【００７４】
ＶＰＮメンバー管理サーバ３は、ＶＰＮに割当てるサブネットアドレスと、ＶＰＮ上のブロードキャスト／マルチキャストパケットを転送するときに使用するマルチキャストＩＰアドレスと、を解放する。また、ＶＰＮメンバー管理サーバ３は、上記削除対象ＶＰＮ識別子をキーとしてデータベース３５に登録されている「ＶＰＮ上のブロードキャスト／マルチキャストパケットを転送するときに使用するマルチキャストＩＰアドレス」、「Ｖ

ＰＮに割当てるサブネットアドレス」、および「ＶＰＮメンバーとなりうる端末装置毎の端末装置識別子および端末装置に割当てるＩＰアドレスの組のリスト」をデータベース３５から削除する（以上、ステップＳ２４）。

【００７５】

そして、ＶＰＮメンバー管理サーバ３は、ＶＰＮ消去応答ＭＳＧ（削除成功）を、エッジ装置２－１へ送信する（ステップＳ２５）。なお、ＶＰＮメンバー管理サーバ３は、「ＶＰＮメンバーとなりうる端末装置毎の端末装置識別子および端末装置に割当てるＩＰアドレスの組のリスト」が空でない場合は、エッジ装置２－１が指定したＶＰＮの削除失敗を示すＶＰＮ消去応答ＭＳＧ（削除失敗）をエッジ装置２－１へ送信する。

【００７６】

エッジ装置２－１は、ＶＰＮの削除動作が終了したことを示すＶＰＮ消去応答ＭＳＧ（削除成功／削除失敗）を受信すると、当該動作結果（削除成功／削除失敗）を示すＶＰＮ削除応答ＭＳＧを端末装置１－１に送信する（ステップＳ２６）。

【００７７】

（端末装置によるＶＰＮからのメンバーの削除）

つづいて、端末装置１－１が既存のＶＰＮからメンバー（端末装置１－ｍとする）を削除する動作の一例を図９に基づいて説明する。なお、図９は、既存のＶＰＮからメンバーを削除する動作の一例を示すシーケンス図である。また、端末装置１－１とエッジ装置２－１との間で、論理的コネクションが確立済みとする。

【００７８】

端末装置１－１は、仮想インタフェース上で、メンバーを削除したいＶＰＮを示すＶＰＮ識別子と削除したいメンバー（端末装置１－ｍ）を示す端末装置識別子とを含むメンバー削除要求ＭＳＧを、エッジ装置２－１に対して送信する（ステップＳ３１）。

【００７９】

エッジ装置２－１は、端末装置１－１から受信したメンバー削除要求ＭＳＧに含まれる論理的コネクションの識別子とラベル値のペアをキーとして、メンバー削除を要求した端末装置１－１の端末装置識別子をデータベース２５で検索する（ステップＳ３２）。そして、エッジ装置２－１は、上記検索により取得した端末装置１－１の端末装置識別子、上記メンバー削除要求ＭＳＧに含まれていた端末装置１－ｍ（メンバー削除対象の端末装置）の端末装置識別子、および上記ＶＰＮ識別子を含むＶＰＮメンバー削除要求ＭＳＧをＶＰＮメンバー管理サーバ３宛に送信する（ステップＳ３３）。

【００８０】

ＶＰＮメンバー管理サーバ３は、エッジ装置２－１から受信したＶＰＮメンバー削除要求ＭＳＧに含まれるＶＰＮ識別子をキーとしてデータベース３５（ＶＰＮ情報データベース）を検索する。当該検索結果である「ＶＰＮメンバーとなりうる端末装置毎の情報（端末装置アドレスおよび端末装置に割り当てるＩＰアドレスの組のリスト）」に端末装置１－ｍの端末装置識別子が登録済みである場合、ＶＰＮメンバー管理サーバ３は、端末装置１－ｍに割り当てたＩＰアドレスを開放する。さらに、ＶＰＮメンバー管理サーバ３は、当該ＩＰアドレスと上記端末装置１－ｍの端末装置識別子を、データベース３５に含まれる「ＶＰＮメンバーとなりうる端末装置毎の情報（端末装置アドレスおよび端末装置に割り当てるＩＰアドレスの組のリスト）」から削除する（ステップＳ３４）。

【００８１】

つぎに、ＶＰＮメンバー管理サーバ３は、端末装置１－ｍに割り当てられていたＩＰアドレスをキーとして、端末装置１－ｍが接続しているエッジ装置（エッジ装置２－ｎとする）のＩＰアドレスをオーバーレイネットワーク上で検索し（ステップＳ３５）、当該検索結果のＩＰアドレス（エッジ装置２－ｎ）宛に、端末装置１－ｍに割り当てられているＩＰアドレス情報を含んだ端末装置切断要求ＭＳＧを送信する（ステップＳ３６）。そして、ＶＰＮメンバー管理サーバ３は、ＶＰＮメンバー削除応答ＭＳＧ（削除成功）を、エッジ装置２－１へ送信する（ステップＳ３７）。

【００８２】

なお、エッジ装置２－１は、ＶＰＮメンバー削除応答ＭＳＧを受信するとその中で示される結果（削除成功／削除失敗）をメンバー削除応答ＭＳＧに設定し、端末装置１－１へ通知する（ステップＳ３８）。

【００８３】

エッジ装置２－ｎは、オーバーレイネットワーク上のレコードから、端末装置１－ｍに割当てられているＩＰアドレスをキーとするデータを削除する（ステップＳ３９）。

【００８４】

さらに、エッジ装置２－ｎは、以下に述べる処理を実行し、データベースを更新する（ステップＳ４０）。

【００８５】

エッジ装置２－ｎは、端末装置１－ｍに割当てられているＩＰアドレスをキーとしてデータベースを検索し、端末装置１－ｍとの間の論理的コネクションの識別子とラベル値のペアを取得し、当該論理的コネクションの識別子とラベル値のペアをキーとして端末装置１－ｍが接続しているＶＰＮのＶＰＮ識別子（以下「削除対象ＶＰＮ識別子」と呼称）を検索（取得）する。そして、当該削除対象ＶＰＮ識別子をキーとして検索した論理的コネクションの識別子とラベル値のペアをデータベースから削除する。また、エッジ装置２－ｎは、端末装置１－ｍに割当てられているＶＰＮ内ＩＰアドレスをキーとして検索した論理的コネクションの識別子とラベル値のペアをデータベースから削除する。また、エッジ装置２－ｎは、端末装置１－ｍとの論理的コネクションの識別子とラベル値のペアをキーとして検索したＶＰＮ識別子、端末装置識別子、およびＶＰＮ内ＩＰアドレスをデータベースから削除する。

【００８６】

また、上記端末装置１－ｍが、エッジ装置２－ｎに接続する端末装置の中で削除対象のＶＰＮに接続していた最後の端末装置である場合、エッジ装置２－ｎは、上記ステップＳ４０に続いて以下の処理を実行する。

【００８７】

エッジ装置２－ｎは、「ＶＰＮ識別子（削除対象ＶＰＮ識別子）」をキーとしてデータベースを検索して得た「マルチキャストＩＰアドレス」へのＪＯＩＮを停止する。また、削除対象ＶＰＮ識別子をキーとしてデータベースを検索して得た「サブネットアドレス」をキーとして、データベースに記録されている「ＶＰＮ識別子」を削除する。また、削除対象ＶＰＮ識別子をキーとしてデータベースを検索して得た「マルチキャストＩＰアドレス」をキーとして、データベースに記録されている「ＶＰＮ識別子」を削除する。さらに、「ＶＰＮ識別子」をキーとしてデータベースに記録されている「マルチキャストＩＰアドレス」と「サブネットアドレス」と、を削除する（以上、ステップＳ４０）。

【００８８】

さらに、エッジ装置２－ｎは、ラベル値を解放し、上記削除対象ＶＰＮ識別子を含み、論理的コネクション上で、ラベル値が指定するラベルを付与したＶＰＮ切断通知ＭＳＧを端末装置１－ｍへ送信する（ステップＳ４１）。なお、当該ＶＰＮ切断通知ＭＳＧにおいては、送信元ＩＰアドレスおよび宛先ＩＰアドレスに端末装置１－ｍのＩＰアドレスを設定する。

【００８９】

そして、端末装置１－ｍは、ＶＰＮ切断通知ＭＳＧを受信後、当該ＶＰＮ切断通知ＭＳＧを受信した仮想インタフェースを削除する（ステップＳ４２）。

【００９０】

（端末装置のエッジ装置への接続）

つづいて、端末装置１－２のデフォルトＶＰＮがＶＰＮメンバー管理サーバ３に登録済みの場合に、端末装置１－２がエッジ装置２－１へ接続する動作の一例を図１０に基づいて説明する。なお、図１０は、端末装置１－２がエッジ装置２－１へ接続する動作の一例を示すシーケンス図である。

【００９１】

端末装置１－２は、認証情報（端末装置識別子を含む）を含んだ論理的コネクションの確立要求をエッジ装置２－１宛に送信する（ステップＳ５１）。

【００９２】

エッジ装置２－１は、受信した上記論理的コネクション確立要求に含まれる認証情報を用いて認証要求ＭＳＧを作成して認証サーバ４宛に送信し、認証サーバ４からの応答（認証応答ＭＳＧ）を待つ（ステップＳ５２）。そして、エッジ装置２－１は、認証サーバ４からの認証応答ＭＳＧを受信し（ステップＳ５３）、その内容が認証成功の場合、認証応答ＭＳＧに含まれるＶＰＮ識別子と、上記論理的コネクション確立要求に含まれる端末装置識別子と、を用いて、ＶＰＮメンバー問合せ要求ＭＳＧを作成する。そして、エッジ装置２－１は、当該ＶＰＮメンバー問合せ要求ＭＳＧをＶＰＮメンバー管理サーバ３宛に送信することにより、端末装置１－２がＶＰＮ識別子に対応するＶＰＮに参加可能かどうかと、参加可能な場合に端末装置１－２に割当てるＩＰアドレスと、を問い合わせる（ステップＳ５４）。なお、上記認証応答ＭＳＧの内容が認証失敗の場合、エッジ装置２－１は、端末装置１－２との論理的コネクション確立を拒否する。

【００９３】

つぎに、エッジ装置２－１は、上記ＶＰＮメンバー問合せ要求ＭＳＧに対するＶＰＮメンバー問合せ応答ＭＳＧが、端末装置１－２のＶＰＮへの参加を許可するもの（端末装置に割り当てるＩＰアドレス、マルチキャストＩＰアドレス、ＶＰＮに対応付けられるサブネットアドレスを含むもの）であった場合、端末装置１－２との論理的コネクションを介してＶＰＮ内でパケットを転送する際にＩＰパケットの先頭に付けるラベルが使用するラベル値を例えば“０”（一番初めに参加するＶＰＮ用のラベルの値を固定する趣旨）に決定する（ステップＳ５６）。なお、当該ラベルの値は、論理的コネクション内で一意になる様に決定すればよい。また、エッジ装置２－１は、上記ＶＰＮメンバー問合せ応答ＭＳＧが、端末装置１－２のＶＰＮへの参加を拒否するものであった場合、端末装置１－２との論理的コネクション確立を拒否する。

【００９４】

つぎに、エッジ装置２－１は、以下に述べる処理を実行し、データベース２５を更新する（ステップＳ５７）。

【００９５】

エッジ装置２－１は、端末装置１－２との間の論理的コネクションの識別子とラベル値（＝０）のペアをキーとして、ＶＰＮ識別子、端末装置識別子、およびＶＰＮ内ＩＰアドレスをデータベース２５に記録する。また、エッジ装置２－１は、ＶＰＮ内ＩＰアドレスをキーとして、端末装置１－２との間の論理的コネクションの識別子とラベル値（＝０）のペア（データ）をデータベース２５に記録する。さらに、エッジ装置２－１は、ＶＰＮ識別子をキーとしてデータベース２５を検索して得られる、端末装置との間の論理的コネクションの識別子とラベル値のペアのリストに、論理的コネクションの識別子とラベル値（＝０）のペアを追加する（データベース２５のリストを更新する）。なお、エッジ装置２－１は、ＶＰＮ識別子をキーとしたデータベース２５の検索の結果、端末装置との間の論理的コネクションの識別子とラベル値のペアのリストが得られない（指定のＶＰＮ識別子に対応するリストをデータベース２５に保持していない）場合は、ＶＰＮ識別子をキーとする空のリストのデータをデータベース２５に追加した上で（空のリストを新規作成した上で）、論理的コネクションの識別子とラベル値（＝０）のペアを当該空のリストに追加する（以上、ステップＳ５７）。

【００９６】

そして、エッジ装置２－１は、上記ＶＰＮメンバー問合せ応答ＭＳＧに含まれる「端末装置１－２が使用するＩＰアドレス」を端末装置１－２との間の論理的コネクションを確立するためのメッセージシーケンスの中で、通知する（ステップＳ５８）。

【００９７】

また、エッジ装置２－１は、前述したＤＨＴ方式検索機能を提供するオーバーレイネットワーク上に、端末装置１－２に割当てたＩＰアドレスをキーとして、自装置のＩＰアド

レスをデータとするレコードを登録する（ステップＳ５９）。

【００９８】

なお、端末装置１－２が、エッジ装置２－１に接続する端末装置の中で、上記認証サーバ４から受信した認証応答ＭＳＧに含まれるＶＰＮ識別子に対応するＶＰＮに対して初めて接続するものである場合、エッジ装置２－１は、上記ステップＳ５９に続いて以下の処理を実行する。

【００９９】

エッジ装置２－１は、端末装置１－２が接続するＶＰＮの「ＶＰＮ識別子」をキーとして、上記ＶＰＮメンバー問合せ応答ＭＳＧに含まれる「マルチキャストＩＰアドレス」と「サブネットアドレス」と、をデータベースに記録する。また、「マルチキャストＩＰアドレス」をキーとして、「ＶＰＮ識別子」をデータベース２５に記録する。また、「サブネットアドレス」をキーとして、「ＶＰＮ識別子」をデータベース２５に記録する。そして、マルチキャストＩＰアドレス宛パケットを受信する様に、マルチキャストＩＰアドレスにＪＯＩＮする。

【０１００】

また、端末装置１－２は、論理的コネクションの識別子とラベル値（＝０）のペアを仮想インタフェースとして扱い、論理的コネクション確立手順の中で割当てられたＩＰアドレスを、その仮想インタフェースのＩＰアドレスとして設定する。そして、端末装置１－２は、仮想インタフェースを表す識別子を決定し、仮想インタフェース識別子とラベル値の対応付けを、データベース１５に記録する（ステップＳ６０）。

【０１０１】

（端末装置の既存のＶＰＮへの参加）

つづいて、端末装置１－２が既存のＶＰＮへ参加する動作の一例を図１１に基づいて説明する。なお、図１１は、端末装置１－２が既存のＶＰＮへ参加する動作の一例を示すシーケンス図である。また、端末装置１－２とエッジ装置２－１との間で、論理的コネクションが確立済みとする。

【０１０２】

端末装置１－２は、仮想インタフェース上で、新たに参加したいＶＰＮを示すＶＰＮ識別子を含むＶＰＮ参加要求ＭＳＧを、エッジ装置２－１に対して送信する（ステップＳ６１）。

【０１０３】

エッジ装置２－１は、端末装置１－２から受信したＶＰＮ参加要求ＭＳＧに含まれる論理的コネクションの識別子とラベル値のペアをキーとして、端末装置１－２の端末装置識別子をデータベース２５で検索する（ステップＳ６２）。

【０１０４】

つぎに、エッジ装置２－１は、ＶＰＮ参加要求ＭＳＧに含まれるＶＰＮ識別子と、上記検索で得た端末装置１－２の端末装置識別子を用いてＶＰＮメンバー問合せ要求ＭＳＧを作成し、ＶＰＮメンバー管理サーバ３宛に送信する（ステップＳ６３）。ＶＰＮメンバー管理サーバ３は、当該要求ＭＳＧに対するＶＰＮメンバー問合せ応答ＭＳＧを作成してエッジ装置２－１に送信する（ステップＳ６４）。エッジ装置２－１は、当該応答ＭＳＧの内容を確認し、端末装置１－２が上記ＶＰＮ識別子に対応するＶＰＮに参加可能かどうかを判断し、参加可能な場合は当該応答ＭＳＧに含まれている端末装置１－２に割当てるＩＰアドレスを取得する（ステップＳ６５）。なお、端末装置１－２がＶＰＮに参加できない場合、エッジ装置２－１は、上記ＶＰＮ参加要求ＭＳＧに付与されていたものと同じラベルを付与したＶＰＮ参加応答ＭＳＧ（参加拒否）を論理的コネクション上で端末装置１－２に送信し、端末装置１－２のＶＰＮ参加を拒否する。

【０１０５】

端末装置１－２のＶＰＮへの参加を許可する場合、エッジ装置２－１は、端末装置１－２との論理的コネクション介してＶＰＮ内でパケットを転送する際にＩＰパケットの先頭に付けるラベルが使用するラベル値を決定する（ステップＳ６６）。なお、当該ラベルの

値は、論理的コネクション内で一意になる様に決める。

【０１０６】

つぎに、エッジ装置２－１は、以下に述べる処理を実行し、データベース２５を更新する（ステップＳ６７）。

【０１０７】

エッジ装置２－１は、端末装置１－２との間の論理的コネクションの識別子とラベル値のペアをキーとして、ＶＰＮ識別子と端末装置識別子とＶＰＮ内ＩＰアドレスをデータベース２５に記録する。また、エッジ装置２－１は、ＶＰＮ内ＩＰアドレスをキーとして、端末装置１－２との間の論理的コネクションの識別子とラベル値のペアをデータベース２５に記録する。さらに、エッジ装置２－１は、ＶＰＮ識別子をキーとして、データベース２５を検索して得られる端末装置との間の論理的コネクションの識別子とラベル値のペアのリストに、論理的コネクションの識別子とラベル値のペアを追加する（データベース２５のリストを更新する）。なお、エッジ装置２－１は、ＶＰＮ識別子をキーとしたデータベース２５の検索の結果、端末装置との間の論理的コネクションの識別子とラベル値のペアのリストが得られない（指定のＶＰＮ識別子に対応するリストをデータベース２５に保持していない）場合は、ＶＰＮ識別子をキーとする空のリストのデータをデータベース２５に追加した上で（空のリストを新規作成した上で）、論理的コネクションの識別子とラベル値のペアを追加する（以上、ステップＳ６７）。

【０１０８】

また、エッジ装置２－１は、上記ＶＰＮ参加要求ＭＳＧに付与されていたものと同じラベルを付与したＶＰＮ参加応答ＭＳＧ（参加許可、端末装置１－２に割り当てたＩＰアドレスおよびラベル値を含む）を、論理的コネクション上で端末装置１－２に送信する（ステップＳ６８）。

【０１０９】

つぎに、エッジ装置２－１は、上述した「端末装置１－２のデフォルトＶＰＮがＶＰＮメンバー管理サーバ３に登録済みの場合に、端末装置１－２がエッジ装置２－１へ接続する動作」の場合などと同様に、オーバーレイネットワーク上に、端末装置に割当てたＩＰアドレスをキーとして、自装置のＩＰアドレスをデータとするレコードを登録する。

【０１１０】

なお、端末装置１－２が、エッジ装置２－１に接続する端末装置の中で、上記ＶＰＮに対して初めて接続するものである場合、エッジ装置２－１は、上記の処理に続いて以下の処理を実行する。

【０１１１】

エッジ装置２－１は、「（上記ＶＰＮの）ＶＰＮ識別子をキーとした、マルチキャストＩＰアドレスおよびサブネットアドレス」のデータ、「マルチキャストＩＰアドレスをキーとしたＶＰＮ識別子」のデータ、および「サブネットアドレスをキーとしたＶＰＮ識別子」のデータをデータベース２５に記録する。そして、エッジ装置２－１は、マルチキャストＩＰアドレス宛パケットを受信する様に、マルチキャストＩＰアドレスにＪＯＩＮする（以上、ステップＳ６９）。

【０１１２】

また、エッジ装置２－１との論理的コネクションを確立した端末装置１－２は、論理的コネクションの識別子とＶＰＮ参加応答ＭＳＧに示されるラベル値のペアを仮想インタフェースとして扱い、ＶＰＮ参加応答ＭＳＧに示されるＩＰアドレスを、その仮想インタフェースのＩＰアドレスとして設定する。つぎに、端末装置１－２は、仮想インタフェースを表す識別子を決定し、仮想インタフェース識別子とラベル値の対応付けを、データベース１５に記録する（ステップＳ７０）。

【０１１３】

（端末装置の参加中のＶＰＮからの離脱）

つづいて、端末装置１－２がＶＰＮから離脱する動作の一例を図１２に基づいて説明する。なお、図１２は、端末装置１－２がＶＰＮから離脱する動作の一例を示すシーケンス

図である。また、端末装置１－２とエッジ装置２－１との間で、論理的コネクションが確立済みとする。

【０１１４】

端末装置１－２は、仮想インタフェース上で、離脱したいＶＰＮを示すＶＰＮ識別子を含むＶＰＮ離脱要求ＭＳＧをエッジ装置２－１に対して送信する（ステップＳ７１）。

【０１１５】

ＶＰＮ離脱要求ＭＳＧを受信したエッジ装置２－１は、ＶＰＮ離脱要求ＭＳＧに示されるＶＰＮ識別子をキーとして、端末装置１－２との間の論理的コネクションの識別子とラベル値のペアのリストを、データベース２５で検索する（ステップＳ７２）。当該検索結果のリストにＶＰＮ離脱要求ＭＳＧを受信した論理的コネクションの識別子とラベル値のペアが含まれている場合、エッジ装置２－１は、端末装置１－２に割当てたＩＰアドレスをキーとしたレコードをオーバーレイネットワーク上から削除する（ステップＳ７３）。

【０１１６】

さらに、エッジ装置２－１は、以下に述べる処理を実行し、データベース２５を更新する（ステップＳ７４）。

【０１１７】

エッジ装置２－１は、「ＶＰＮ離脱要求ＭＳＧを受信した論理的コネクションの識別子とラベル値のペアをデータベース２５のリストから削除する処理」、「論理的コネクションの識別子とラベル値のペアをキーとしたデータベース２５の検索結果であるＶＰＮ内ＩＰアドレス、をキーとして記録されている、端末装置１－２との間の論理的コネクションの識別子とラベル値のペア（データ）をデータベース２５から削除する処理」、「論理的コネクションの識別子とラベル値のペアをキーとして記録されている、ＶＰＮ識別子と端末装置識別子とＶＰＮ内ＩＰアドレスをデータベース２５から削除する処理」、および「ラベル値の解放処理」を行う（以上、ステップＳ７４）。

【０１１８】

なお、上記検索結果のリストにＶＰＮ離脱要求ＭＳＧを受信した論理的コネクションの識別子とラベル値のペアが含まれていない場合は、その時点で処理を終了する。

【０１１９】

つぎに、エッジ装置２－１は、ＶＰＮ離脱要求ＭＳＧを受信した論理的コネクションの識別子とラベル値のペア上（端末装置１－２にとっての仮想インタフェース上）へＶＰＮ離脱応答ＭＳＧを送信する（ステップＳ７５）。そして、端末装置１－２は、ＶＰＮ離脱応答ＭＳＧを受信すると、受信した仮想インタフェースを削除する。

【０１２０】

（エッジ装置によるパケットの転送処理－ユニキャスト転送）

つづいて、端末装置１－２が送信したユニキャストＩＰアドレス宛パケットを、エッジ装置２－１が宛先端末装置（端末装置１－ｍとする）へ転送する動作の一例を図１３に基づいて説明する。なお、図１３は、端末装置１－２がユニキャストＩＰアドレス宛のパケットを送信する動作の一例を示すシーケンス図である。また、端末装置１－２とエッジ装置２－１との間で、論理的コネクションが確立済みとする。

【０１２１】

端末装置１－２は、ユニキャストの宛先アドレスを指定し、先頭に仮想インタフェースに対応するラベル値のラベルを付与したＩＰパケットを仮想インタフェース上で送信する（ステップＳ８１）。

【０１２２】

エッジ装置２－１は、宛先ＩＰアドレスがユニキャストＩＰアドレスである上記ＩＰパケットを端末装置１－２から受信すると、論理的コネクションの識別子とラベル値（＝０）のペアをキーとして、データベース２５でＶＰＮ識別子を検索し、さらに、検索により得たＶＰＮ識別子をキーとしてＶＰＮに対応付けられるサブネットアドレスをデータベース２５で検索する（ステップＳ８２）。

【０１２３】

エッジ装置２－１は、端末装置１－２から受信したＩＰパケットの宛先ＩＰアドレスが、上記検索により得られたサブネットアドレスに属する場合、ＩＰパケットの宛先ＩＰアドレスをキーとして、ＩＰパケットの送信先である端末装置１－ｍが接続するエッジ装置（エッジ装置２－ｎとする）のＩＰアドレスをオーバーレイネットワーク上で検索する（ステップＳ８３）。一方、受信したＩＰパケットの宛先ＩＰアドレスが、検索により得られたサブネットアドレスに属さない場合、エッジ装置２－１は、上記ＩＰパケットを廃棄する。また、オーバーレイネットワーク上でのエッジ装置２－ｎのＩＰアドレス検索に失敗した場合、エッジ装置２－１は、上記ＩＰパケットを廃棄する（相手側エッジ装置ＩＰアドレス検索処理１）。

【０１２４】

なお、エッジ装置２－１は、上記「相手側エッジ装置ＩＰアドレス検索処理１（ステップＳ８２およびＳ８３）」に代えて次の処理（相手側エッジ装置ＩＰアドレス検索処理２）を行うこととしてもよい。

【０１２５】

エッジ装置２－１は、宛先ＩＰアドレスがユニキャストＩＰアドレスである上記ＩＰパケットを端末装置１－２から受信すると、論理的コネクションの識別子とラベル値（＝０）のペアをキーとして、データベース２５でＶＰＮ識別子および端末装置１－２のＶＰＮ内ＩＰアドレスを検索し、さらに、検索により得たＶＰＮ識別子をキーとしてＶＰＮに対応付けられるサブネットアドレスをデータベース２５で検索する（上記ステップＳ８２の代替処理）。そして、エッジ装置２－１は、端末装置１－２から受信したＩＰパケットの宛先ＩＰアドレスが、上記検索により得られたサブネットアドレスに属し、かつ受信したＩＰパケットの送信元ＩＰアドレスが、上記検索により得られたＶＰＮ内ＩＰアドレスと一致する場合、ＩＰパケットの宛先ＩＰアドレスをキーとして、ＩＰパケットの送信先である端末装置１－ｍが接続するエッジ装置（エッジ装置２－ｎとする）のＩＰアドレスをオーバーレイネットワーク上で検索する。一方、ＩＰパケットの宛先ＩＰアドレスが、上記検索により得られたサブネットアドレスに属さない場合、または、受信したＩＰパケットの送信元ＩＰアドレスが、上記検索により得られたＶＰＮ内ＩＰアドレスと一致しない場合は、上記ＩＰパケットを廃棄する。また、オーバーレイネットワーク上でのエッジ装置２－ｎのＩＰアドレス検索に失敗した場合、エッジ装置２－１は、上記ＩＰパケットを廃棄する（相手側エッジ装置ＩＰアドレス検索処理２）。

【０１２６】

エッジ装置２－１は、上記「相手側エッジ装置ＩＰアドレス検索処理１」または「相手側エッジ装置ＩＰアドレス検索処理２」によりエッジ装置２－ｎのＩＰアドレスを取得後、端末装置１－２から受信した上記ＩＰパケットを当該ＩＰアドレス（エッジ装置２－ｎ）宛に、エッジ装置間トンネルで送信する（ステップＳ８４）。

【０１２７】

エッジ装置間トンネルでＩＰパケットを受信したエッジ装置２－ｎは、そのＩＰパケットの宛先アドレスに指定されるＩＰアドレスをキーとして、対応する論理的コネクションの識別子とラベル値のペアをデータベースで検索する（ステップＳ８５）。そして、エッジ装置２－ｎは、検索で得たラベル値のラベルを上記ＩＰパケットに付与し、同じく検索で得た論理的コネクション上へ送信する。なお、エッジ装置２－ｎは、論理的コネクションの識別子とラベル値のペアの検索に失敗した場合、上記ＩＰパケットを廃棄する。

【０１２８】

端末装置１－２が送信したＩＰパケットの宛先端末装置（端末装置１－ｍ）は、論理的コネクション上でラベルが付与されたＩＰパケットを受信したときには、付与されているラベルの値からどの仮想インタフェース上で受信したかを識別し、ラベルを外してＩＰパケットとして受信する（ステップＳ８６）。

【０１２９】

なお、上記エッジ装置間トンネルは、転送対象のＩＰパケットを、送信元ＩＰアドレスとして送信元エッジ装置（エッジ装置２－１）のＩＰアドレスを設定し、宛先ＩＰアドレ

スとして転送先エッジ装置（エッジ装置２－ｎ）のＩＰアドレスを設定したＩＰヘッダでカプセル化を施したＩＰｉｎＩＰカプセル化により実現する。

【０１３０】

（エッジ装置によるパケットの転送処理－ブロードキャスト／マルチキャスト転送）

つづいて、端末装置１－２が送信したブロードキャスト／マルチキャストＩＰアドレス宛パケットを、エッジ装置２－１が宛先端末装置へ転送する動作の一例を説明する。ここでは特に、図１４に基づいて、端末装置１－２がマルチキャストＩＰアドレスを設定したパケットを送信する動作について説明する。なお、図１４は、端末装置１－２がマルチキャストＩＰアドレス宛のパケットを送信する動作の一例を示すシーケンス図である。また、端末装置１－２とエッジ装置２－１との間で、論理的コネクションが確立済みとする。

【０１３１】

端末装置１－２は、ブロードキャスト／マルチキャストＩＰアドレスを宛先アドレスとして指定し、先頭に仮想インタフェースに対応するラベル値のラベルを付与したＩＰパケットを仮想インタフェース上で送信する（ステップＳ９１）。

【０１３２】

エッジ装置２－１は、宛先ＩＰアドレスがブロードキャスト／マルチキャストアドレスである上記ＩＰパケットを端末装置１－２から受信すると、論理的コネクションの識別子とラベル値（＝０）のペアをキーとして、データベース２５でＶＰＮ識別子を検索し、さらに、検索により得たＶＰＮ識別子をキーとして、マルチキャストＩＰアドレスをデータベース２５で検索する（ステップＳ９２）。

【０１３３】

エッジ装置２－１は、端末装置１－２から受信したＩＰパケットに、上記検索で得たマルチキャストＩＰアドレスを宛先とし、自ＩＰアドレスを送信元とするＩＰｉｎＩＰカプセル化を施して送信する（ステップＳ９３）。なお、エッジ装置２－１は、上記検索でマルチキャストＩＰアドレスを取得できなかった場合（検索に失敗した場合）、上記ＩＰパケットを廃棄する。

【０１３４】

マルチキャストＩＰアドレス宛でＩＰｉｎＩＰカプセル化された上記ＩＰパケットを受信したエッジ装置（相手側エッジ装置）は、マルチキャストＩＰアドレスをキーとしてＶＰＮ識別子をデータベースで検索し、さらに、当該検索で得たＶＰＮ識別子をキーとして、論理的コネクションの識別子とラベル値のペアのリストをデータベースで検索する（ステップＳ９４）。そして、相手側エッジ装置は、ＩＰｉｎＩＰカプセル化されているパケットの中のＩＰパケットを取り出し、上記検索で得られたリストに含まれる全ての論理的コネクションの識別子とラベル値のペア上（端末装置にとっての仮想インタフェース上）へ送信する。なお、相手側エッジ装置は、論理的コネクションの識別子とラベル値のペアの検索に失敗した場合、上記ＩＰパケットを廃棄する。

【０１３５】

端末装置１－２が送信したＩＰパケットの宛先端末装置は、論理的コネクション上でラベルが付与されたＩＰパケットを受信したときは、付与されているラベルの値からどの仮想インタフェース上で受信したかを識別し、ラベルを外してＩＰパケットとして受信する（ステップＳ９５～Ｓ９７）。

【０１３６】

このように、この実施の形態においては、あるＶＰＮに接続したい端末装置（ユーザ）がエッジ装置に接続してきたときに、エッジ装置がＶＰＮメンバー管理サーバにＶＰＮに関する情報を問い合わせるようにしているので、端末装置と当該端末装置が接続を希望するＶＰＮとの間の接続を仲介するための必要な設定が予めエッジ装置に具備されていなければならばいという制約を解除することできる。

【０１３７】

さらに、この実施の形態では、ラベル付けを行ったＩＰパケットを端末装置とエッジ装置とを接続する論理的コネクション上で転送することにより、１つの論理的コネクション

上にさらにラベルで区別される複数の論理的コネクションを多重化するようにした。また、端末装置からの要求で、ＶＰＮメンバー管理サーバへ、ＶＰＮの登録／削除とＶＰＮに属するメンバー（端末装置）の登録／削除を可能とすることにより、動的なＶＰＮ生成／削除を可能とした。これらの処理により、少ないメッセージのやり取りで、端末装置が動的にＶＰＮを生成／削除することができるとともに、端末装置がＶＰＮに動的に参加／離脱することができる。

【０１３８】

さらには、エッジ装置で構築されるＤＨＴ方式検索機能を有するオーバーレイネットワーク上で、各端末装置がどのエッジ装置に接続するかの情報を管理することにより、端末装置数とエッジ装置数に対してスケールする形で、端末装置が常に同じＩＰアドレスでＶＰＮに接続することを可能とした。すなわち、端末装置の接続／切断の度に、エッジ装置がルーティングプロトコルによりルーティング情報をＶＰＮ全体に広告する処理を不要とした。この処理により、端末装置数の増加に対するスケーラビリティの問題が解消されたＶＰＮを構築することができる。

【０１３９】

また、ＩＰアドレスのサブネット部分をＶＰＮ識別子として使用することで、同一ＶＰＮ内での通信かどうかの判定を簡易にした。この処理により、端末装置がモバイルＩＰをサポートすることなく、任意のエッジ装置経由でＶＰＮに接続した場合であっても、ＶＰＮ内にて同一ＩＰアドレスを使用して通信を行うことが可能となる。

【０１４０】

なお、この実施の形態では、各エッジ装置が、Ｃｈｏｒｄの方式に従ってＩＰネットワーク上にＤＨＴ方式の検索機能を提供するオーバーレイネットワークを構築する場合を一例として説明したが、Ｃｈｏｒｄの方式に限定されるものではなく、Ｃｈｏｒｄを改良または拡張した方式を用いてもよく、あるいはＤＨＴを用いるＣｈｏｒｄ以外の方式を用いてもよい。

【０１４１】

実施の形態２.

図１５は、本発明の実施の形態２にかかるデータ通信システムを実現するネットワークの構成例を示す図である。この実施の形態にかかるネットワークは、前述の実施の形態１にかかるネットワークと比較して、エッジ装置２－１～２－ｎに代えてエッジ装置２ａ－１～２ａ－ｎを備え、また、ＶＰＮメンバー管理サーバを複数備えることを特徴とする。このような構成のため、この実施の形態では、前述の実施の形態１と異なる処理について説明する。

【０１４２】

図１６は、本実施の形態のエッジ装置２ａ（図１５のエッジ装置２ａ－１～２ａ－ｎに相当）の構成例を示す図であり、例えば、ＬｉｎｕｘをＯＳとするＰＣを用いることができる。そして、エッジ装置２ａは、ＩＰ通信モジュール２１、データベース２５、ＤＨＴ検索モジュール２６、トンネル通信モジュール１２、ＶＰＮ識別子－ＶＰＮメンバー管理サーバ対応付けモジュール２８、制御モジュール２７ａを備えている。なお、前述した実施の形態１のエッジ装置２（図３参照）と同様の構成については、同一の符号を付してその説明を省略する。

【０１４３】

ＶＰＮ識別子－ＶＰＮメンバー管理サーバ対応付けモジュール２８は、ＶＰＮ識別子をキーとして、そのＶＰＮ識別子に関するデータを管理するＶＰＮメンバー管理サーバのＩＰアドレスをデータとするデータベースを管理し、ＶＰＮ識別子の入力に対して、そのＶＰＮ識別子に関するデータを管理するＶＰＮメンバー管理サーバのＩＰアドレスを出力として返送するデータベースソフトウェアとして実現される。

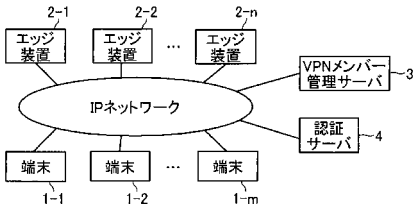
【０１４４】

また、制御モジュール２７ａは、例えば、Ｓ／Ｗとして実現され、エッジ装置２ａを構成する他のモジュール（ＩＰ通信モジュール２１、トンネル通信モジュール１２、など）

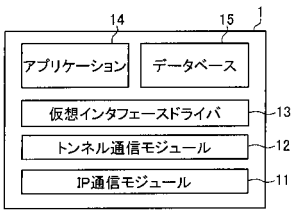
を制御する。
【０１４５】
そして、この実施の形態にかかるネットワークにおける処理は、エッジ装置２ａがＶＰＮメンバー管理サーバ３－１～３－ｘ（図１５参照）のいずれかと通信する場合、その前段階として必ずＶＰＮ識別子－ＶＰＮメンバー管理サーバ対応付けモジュール２８を呼び出して、どのＶＰＮメンバー管理サーバと通信するべきかの判定処理を行うことを特徴とする。なお、当該判定処理が追加された点を除いて、本実施の形態にかかるネットワークにおける処理は、前述の実施の形態１の処理と同様である。
【０１４６】
このように、この実施の形態においては、ＶＰＮメンバー管理サーバとの通信を行うにあたり、複数台存在するＶＰＮメンバー管理サーバのいずれと通信するかを判定することとし、動的なＶＰＮ生成／削除等の処理の負荷を分散させることとした。これにより、上述した実施の形態１の場合よりもさらに、ＶＰＮ数と端末装置数に対するスケーラビリティを向上させることができる。
【産業上の利用可能性】
【０１４７】
以上のように、本発明にかかるデータ通信システムは、複数のＶＰＮが構成されるＩＰネットワークに有用である。
【図面の簡単な説明】
【０１４８】
【図１】本発明の実施の形態１にかかるデータ通信システムを実現するネットワークの構成例を示す図である。
【図２】端末装置の構成例を示す図である。
【図３】エッジ装置の構成例を示す図である。
【図４】ＶＰＮメンバー管理サーバの構成例を示す図である。
【図５】認証サーバの構成例を示す図である。
【図６】端末装置がＶＰＮを作成する動作の一例を示すシーケンス図である。
【図７】既存のＶＰＮへメンバーを追加する動作の一例を示すシーケンス図である。
【図８】端末装置がＶＰＮを削除する動作の一例を示すシーケンス図である。
【図９】既存のＶＰＮからメンバーを削除する動作の一例を示すシーケンス図である。
【図１０】端末装置がエッジ装置へ接続する動作の一例を示すシーケンス図である。
【図１１】端末装置が既存のＶＰＮへ参加する動作の一例を示すシーケンス図である。
【図１２】端末装置がＶＰＮから離脱する動作の一例を示すシーケンス図である。
【図１３】端末装置がユニキャストＩＰアドレス宛のパケットを送信する動作の一例を示すシーケンス図である。
【図１４】端末装置がマルチキャストＩＰアドレス宛のパケットを送信する動作の一例を示すシーケンス図である。
【図１５】本発明の実施の形態２にかかるデータ通信システムを実現するネットワークの構成例を示す図である。
【図１６】エッジ装置の構成例を示す図である。
【符号の説明】
【０１４９】
１，１－１，１－２，１－ｍ　端末装置
２，２－１，２－２，２－ｎ，２ａ　エッジ装置
３，３－１，３－ｘ　ＶＰＮメンバー管理サーバ
４　認証サーバ
１１，２１，３１，４１　ＩＰ通信モジュール
１２　トンネル通信モジュール
１３　仮想インタフェースドライバ
１４　アプリケーション

１５，２５，３５，４５　データベース
２６　ＤＨＴ検索モジュール
２７，３７，４７，２７ａ　制御モジュール
２８　ＶＰＮ識別子－ＶＰＮメンバー管理サーバ対応付けモジュール

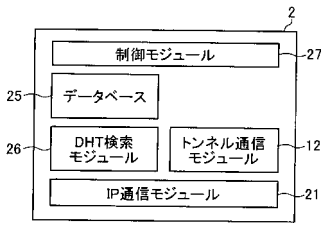
【図１】



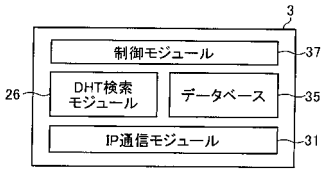
【図２】



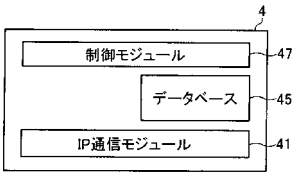
【図３】



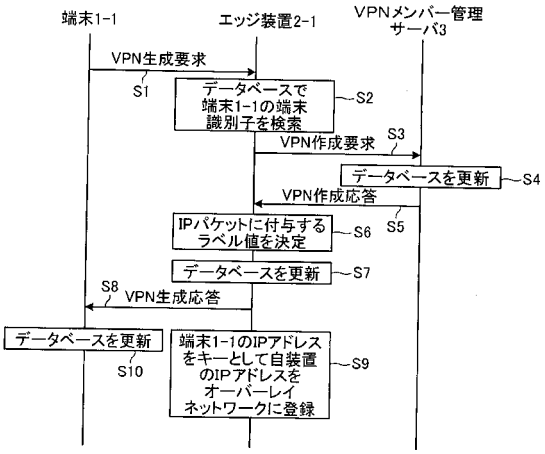
【図４】



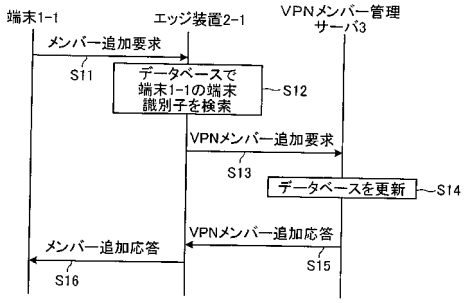
【図５】



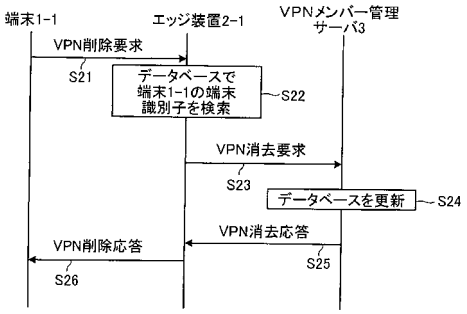
【図６】



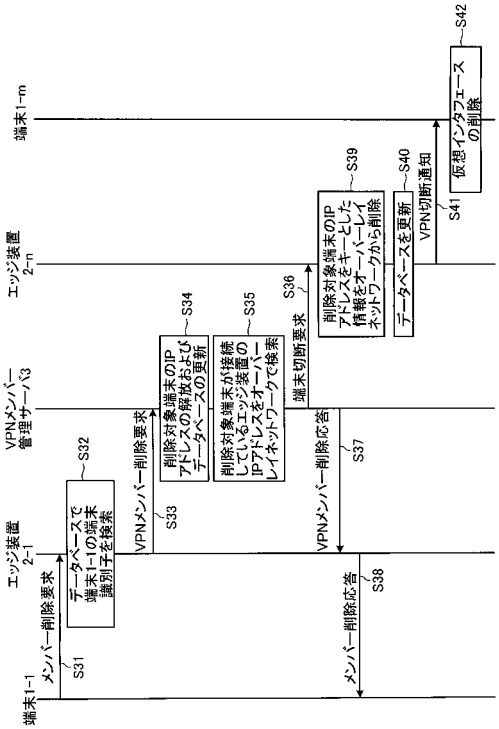
【図７】



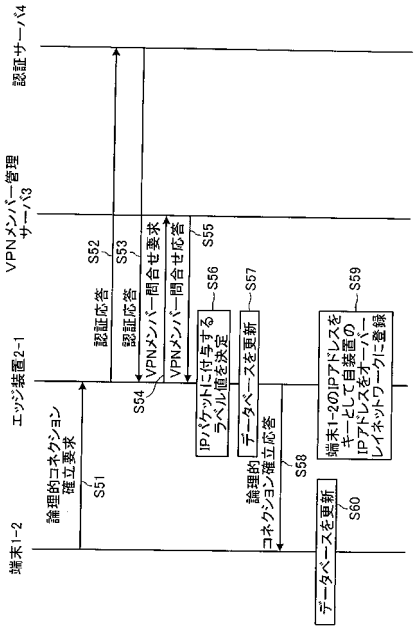
【図８】



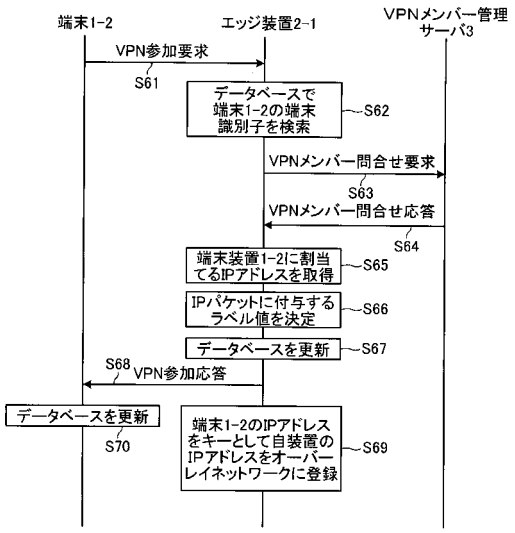
【図９】



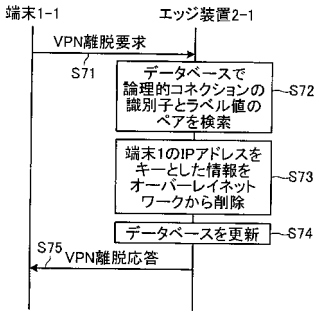
【図１０】



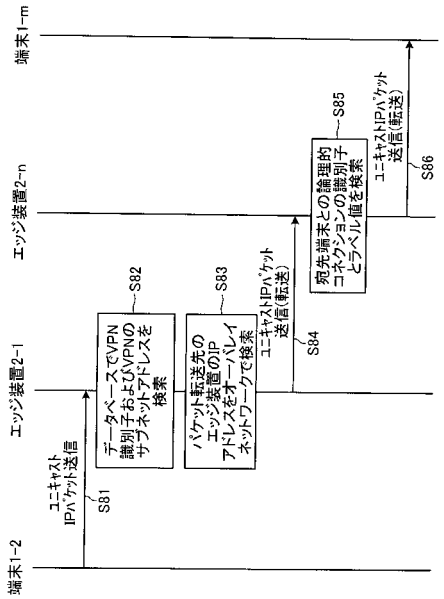
【図１１】



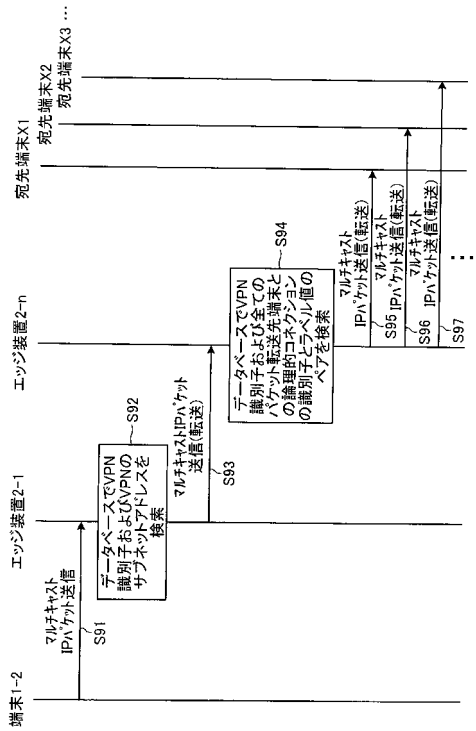
【図１２】



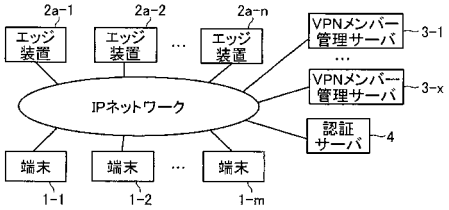
【図１３】



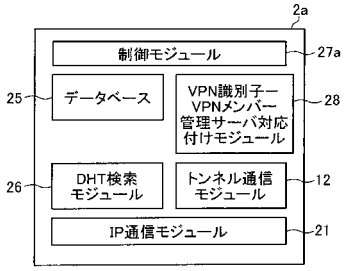
【図１４】



【図１５】


2a-1
2a-2
2a-n
エッジ装置
エッジ装置
エッジ装置
VPNメンバー管理サーバ
3-1
VPNメンバー管理サーバ
3-x
IPネットワーク
認証サーバ
4
端末
端末
端末
1-1
1-2
1-m

【図１６】


2a
制御モジュール
27a
データベース
25
VPN識別子ーVPNメンバー管理サーバ対応付けモジュール
28
DHT検索モジュール
26
トンネル通信モジュール
12
IP通信モジュール
21

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　１２／００－６６