(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年8 月12 日 (12.08.2004)

PCT

(10) 国際公開番号
WO 2004/068805 A1

(51) 国際特許分類[7]: H04L 12/56

(21) 国際出願番号: PCT/JP2004/000818

(22) 国際出願日: 2004 年1 月29 日 (29.01.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-23157 2003 年1 月31 日 (31.01.2003) JP
特願2003-121656 2003 年4 月25 日 (25.04.2003) JP
特願2003-306563 2003 年8 月29 日 (29.08.2003) JP

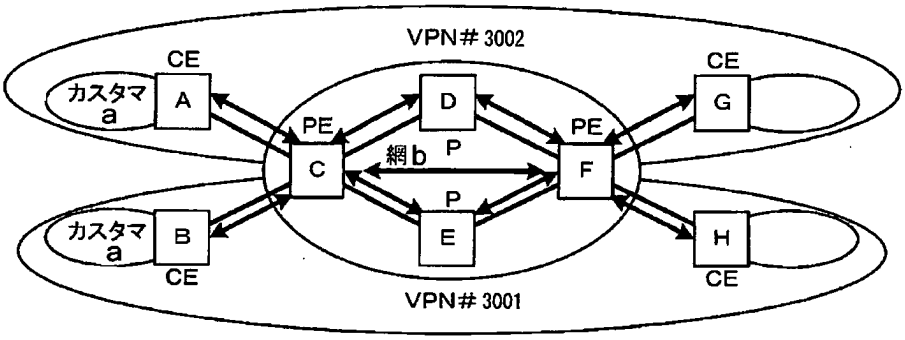
(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒100-8116 東京都千代田区 大手町二丁目３番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 武田 知典 (TAKEDA,Tomonori) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９−１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 井上 一郎 (INOUE,Ichiro) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９−１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 小島 久史 (KOJIMA,Hisashi) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９−１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 清水 香里 (SHIMIZU,Kaori) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９−１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 松浦 伸昭 (MATSUURA,Nobuaki) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９−１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

[続葉有]

(54) Title: VPN COMMUNICATION CONTROL DEVICE, COMMUNICATION CONTROL METHOD IN VPN, AND VIRTUAL DEDICATED NETWORK MANAGEMENT DEVICE

(54) 発明の名称: ＶＰＮ通信制御装置、ＶＰＮにおける通信制御方法、仮想専用網管理装置



a...CUSTOMER
b...NETWORK

(57) Abstract: Link information in a common DB is classified for each VPN associated with the link information. A VPNID which is information for identifying the VPN is assigned to each link information. Link information of the same VPNID is extracted from the link information to which the VPNID of the common DB is assigned, and stored in the corresponding VPNDB. With this configuration, it is possible to provide the network information in the VPN provider and the network information of the customer network to a customer while maintaining a high scalability, thereby enabling easy realization of a path design of the customer.

(57) 要約: 共通DB中のリンク情報を当該リンク情報が関わるVPN毎に分類して分類された各リンク情報にそれぞれVPNを識別する情報であるVPNIDを付与し、共通DBのVPNIDが付与されたリンク情報から同一VPNIDのリンク情報を抜き出して該当するVPNDBに格納する。このような構成によって高いスケーラビリティを実現しながら、VPNプロバイダ内部のネットワーク情報とカスタマ網のネットワーク情報とを、カスタマに提供することで、カスタマのパス設計を容易に実現可能とする。

WO 2004/068805 A1

(74) 代理人: 志賀 正武 (SHIGA,Masatake); 〒104-8453 東京都 中央区 八重洲２丁目３番１号 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

ＶＰＮ通信制御装置、ＶＰＮにおける通信制御方法、仮想専用網管理装置

技術分野

本発明は、ＶＰＮ(Virtual Private Network)に利用する。特に、カスタマからのパス設定要求を契機にカスタマエッジ装置間にパスを設定する網内エッジ装置に関する。

また本発明は、カスタマごとに異なるネットワーク情報を提供し、カスタマの要求を契機にカスタマエッジ装置間にパスを設定するＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）における通信制御方法、およびそれを実現するための通信制御装置とそのプログラム、およびそれを記録した記録媒体に関する。

さらに本発明は、仮想専用網におけるデータ転送装置間のリンクに関するリンク帯域情報を含む仮想網情報を管理し、インターネット接続業者などに仮想網情報を提供する仮想専用網管理装置に関する。

背景技術

カスタマからのパス設定要求を契機にカスタマ装置間にパスを設定する従来のＶＰＮ技術としては、網内エッジ装置間でＢＧＰ(Border Gateway Protocol:例えば「A Border Gateway Protocol4(BGP-4)RFC1771」,IETF,[online],1995年3月掲載,[2003年7月検索],インターネット<URL:http://www.ietf.org/rfc/rfc1771.txt?number=1771> 参照)の拡張を実行し、カスタマエッジ装置の情報にＣｏｍｍｕｎｉｔｙを付与した情報をＢＧＰで交換し、網内エッジ装置で、Ｃｏｍｍｕｎｉｔｙにより、情報を選択して、同一ＶＰＮに属するカスタマエッジ装置を持つ網内エッジ装置間にトンネルを生成して、ＶＰＮ毎に異なるカスタマ網の経路情報を提供するものがある（例えば「GVPN:GeneralizedProvIDer-provisioned Port-based VPNs using BGP and GMPLS draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-03.txt」,IETF,[online],2003年3月掲載,[2003年7月検索],イン

ターネット<URL:http://www.ietf.org/internet-drafts/draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-03.txt> 参照)。

さらに、集中サーバを設けておき、集中サーバから情報を限定的に交換することで、カスタマ毎に異なる情報を提供するものがある（例えば「StarNet Optical VPN」,Tellium,[online],不明,[2003年7月検索],インターネット<URL:http://www.tellium.com/applications/optical_VPN.html> 参照)。

しかしながら、ＢＧＰを用いる方式では、ＶＰＮプロバイダ内部のネットワーク情報を提供することはできない。このため、カスタマは、ＶＰＮプロバイダ内部のネットワークの空きリソース情報などが分からず、どのカスタマエッジ装置間にパスが設定可能か分からないため、パスの設計が困難であるという課題がある。

また、集中サーバを用いる方法では、スケーラビリティが悪く、また集中サーバがダウンした場合、ネットワーク全体が影響を受けてしまう。

従来技術上の課題としてはさらに、複数のＶＰＮ（仮想専用網：Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）を提供する仮想網提供網において、これらの仮想網情報を管理する仮想専用網管理装置としては、ＶＰＮ毎の仮想網情報をデータベースに分割して格納・管理し、個々のＶＰＮを管理する各々のカスタマ装置にこの仮想網情報を提供するものが知られている（例えば、特開２００２－２５２６３１号公報（請求項１、段落〔００１５〕〔００１７〕参照)。この仮想専用網管理装置によれば、仮想網情報はＶＰＮ毎に分割して管理されるから、データベースに格納された１つのＶＰＮに関する仮想網情報を、他のＶＰＮを管理するカスタマ装置に漏洩しないように提供することができ、仮想網情報の機密性の向上を図ることができる。

しかしながら、ＶＰＮを提供する仮想網提供網を管理する従来の仮想専用網管理装置では、機密性を向上させて仮想網情報を提供することはできるが、仮想網提供網内のＶＰＮにおけるデータ転送経路のリンク帯域を表す情報については、このデータ転送経路が運用中に変更される可能性があるため、ＶＰＮを管理するカスタマ装置に正確なリンク帯域を表す情報を提供することができないという課題があった。

また、以上で述べた従来の BGP を用いる方式ならびに仮想専用網管理装置では、カスタマにとって不要な情報の提供を省略して、リソース契約中の条件に必要な情報だけを明示して提示することはできない。さらにパスサービスを提供するプロバイダにとっても、不必要な詳細な情報を提供してしまう弊害を回避する効果を実現することができないという課題があった。

発明の開示

本発明は、このような背景に行われたものであって、高いスケーラビリティを実現しながら、ＶＰＮプロバイダ内部のネットワーク情報とカスタマ網のネットワーク情報とを、カスタマに提供することで、カスタマのパス設計を容易に実現可能とするＶＰＮ通信制御装置を提供することを目的とする。

本発明の他の目的は、ＶＰＮプロバイダ内部のネットワーク情報を、カスタマに提供することで、カスタマのパス設計を容易に実現可能とし、そのためにＶＰＮにおける通信制御方法、およびそれを実現するための通信制御装置、およびそのプログラムとそれを記録した記録媒体を提供することにある。

本発明のさらに他の目的は、仮想網提供網内のＶＰＮにおけるデータ転送経路に関わらず、カスタマ装置に正確なリンク帯域を表す情報を提供することができる仮想専用網管理装置、仮想専用網提供システム、仮想専用網管理プログラム及び該プログラムを記録した記録媒体を提供することにある。

本発明では、網内でＯＳＰＦ(Open Shortest Path First)など詳細なリンク情報を交換できる方式を用い、さらに、各カスタマが利用可能なリンクを識別し、各カスタマが利用可能なリンク情報のみ、カスタマに提供することで、カスタマ毎に異なるオプティカルＶＰＮプロバイダ内部のネットワーク情報を提供する。また、カスタマエッジ装置間にトンネルを生成し、このトンネルを利用してプロバイダがカスタマ網のネットワーク情報の交換を中継する。

これにより、カスタマはＶＰＮプロバイダ内部のネットワーク情報とカスタマ網のネットワーク情報を取得できるため、この情報を利用してパス設計が可能となる。

すなわち、本発明は、カスタマ毎に異なるネットワーク情報を提供し、カスタ

マのパス設定要求を契機に網内エッジ装置間にパスを設定するＶＰＮに設けられ、パス設定に用いる共通データベース（以下ＤＢと記す）と、この共通ＤＢにリンク情報を設定するリンク情報設定手段と、このリンク情報を他装置と自装置との間で交換するリンク情報交換手段と、このリンク情報交換に用いる制御情報の転送経路を決定する経路計算手段とを備えた網内エッジ装置としてのＶＰＮ通信制御装置である。

ここで、本発明の特徴とするところは、ＶＰＮ毎に異なるＤＢであるＶＰＮＤＢを生成するＶＰＮＤＢ生成手段と、前記共通ＤＢ中のリンク情報を当該リンク情報が関わるＶＰＮ毎に分類して分類された各リンク情報にそれぞれＶＰＮを識別する情報であるＶＰＮＩＤを付与するＶＰＮＩＤ設定手段と、前記共通ＤＢのＶＰＮＩＤが付与されたリンク情報から同一ＶＰＮＩＤのリンク情報を抜き出して該当するＶＰＮＤＢに格納するフィルタ手段とを備えたところにある。

これにより、共通ＤＢの他に、ＶＰＮ毎のリンク情報を格納したＶＰＮＤＢを持つことができる。したがって、カスタマは、ＶＰＮ毎のＤＢを用いて自己が属するＶＰＮに関するリンク情報を得ることができる。このときに、ＶＰＮＤＢは共通ＤＢのリンク情報に基づき生成されるので、ネットワーク全体のリンク状態情報をＶＰＮＤＢに反映させることができ、結果的に、カスタマはＶＰＮプロバイダ内部のネットワーク情報とカスタマ網のネットワーク情報とを取得できることになり、この情報を利用してパス設計が可能となる。

また、他網内エッジ装置と前記リンク情報を交換するためのトンネルを生成するトンネル生成手段を備えることができる。

これにより、ＶＰＮＤＢを持っている他網内エッジ装置から効率よくリンク情報の提供を受けることができる。

また、前記共通ＤＢの一部に前記ＶＰＮＤＢを備え、それぞれのＤＢの記録内容を識別するための識別情報を付与する手段を備えることができる。

これにより、共通ＤＢとＶＰＮＤＢとでメモリを分ける必要はなく、メモリを有効利用することができる。

また、前記経路計算手段に基づき決定された制御情報の転送経路を用いて他装置間で前記リンク情報を交換する手段を備えることができる。

これにより、ＶＰＮＤＢを持っている他網内エッジ装置との間の経路を臨機応変に設定可能であり、自網内エッジ装置が必要とするリンク情報を柔軟に取得することができる。

また、自装置内のＶＰＮＤＢがいずれのＶＰＮに関するＶＰＮＤＢであるかを他装置に通知する手段と、他装置の要求に応じて自装置内のＶＰＮＤＢの記録内容を当該他装置に転送する手段とを備えることができる。

これにより、各網内エッジ装置で不必要なＶＰＮＤＢを持つ必要がなく、リソースを有効利用することができる。

また、自装置がフィルタリング実施を行なう装置であるときには前記フィルタ手段によるフィルタリングを実施すると共に他装置に対して前記トンネル設定手段によりトンネルを設定する手段と、他装置が前記フィルタ手段によるフィルタリングを実施しているときには当該他装置に対して前記トンネル設定手段によりトンネルを設定する手段とを備えることができる。

これにより、フィルタ手段によるフィルタリングを各網内エッジ装置が同時に行なう必要がなくリソースを有効利用することができる。

このときに、自装置を識別する情報である自装置ＩＤとＶＰＮＩＤとを加算した値のハッシュ値が他装置を識別する情報である他装置ＩＤと前記ＶＰＮＩＤを加算した値のハッシュ値よりも大きいときには自装置がフィルタリングを実施する装置であると決定する手段を備えることができる。

このようにして、網内エッジ装置のいずれかにフィルタリングを実施させることにより、リソースを有効利用することができる。

また、カスタマエッジ装置から受信したリンク情報が自装置宛であるときにはカスタマ経路フラグをセットする手段と、前記カスタマ経路フラグがセットされたリンク情報を抽出するカスタマリンク情報抽出手段とを備え、このカスタマリンク情報抽出手段によって抽出されたリンク情報を他網内エッジ装置に転送するときには前記カスタマ経路フラグをそのまま付与して転送し、このカスタマリンク情報抽出手段によって抽出されたリンク情報をカスタマエッジ装置に転送するときには前記カスタマ経路フラグを削除して転送する手段を備えることができる。

このようにして、カスタマエッジ装置から受信したリンク情報とそれ以外のリ

ンク情報とをカスタマ経路フラグを用いて区別することにより、例えば、他網内エッジ装置またはカスタマエッジ装置から特定のカスタマ網に関するリンク情報の提供要求があったときに、これに応じることができる。カスタマ経路フラグを用いない場合には、ＶＰＮＩＤによるリンク情報の識別のみであるため、当該リンク情報がいずれのカスタマ網内の情報であるか、あるいは、プロバイダ網内の情報であるかを明確に区別することが困難であり、該当するＶＰＮＩＤを持つ全てのリンク情報を他網内エッジ装置またはカスタマエッジ装置に対して転送することになる。これにより、網内エッジ装置間または網内エッジ装置とカスタマエッジ装置との間で交換する情報に不必要な情報が含まれる場合があるが、カスタマ経路フラグを用いることにより、真に必要な情報を選択して情報交換することができ、交換する情報量を減らすことができる。

また、カスタマエッジ装置からパス設定要求を受けて当該パス設定のためのリソースを確保すると共に当該パス設定要求に基づく次網内装置にパス設定要求を転送するシグナリング手段を備えることができる。これにより、通信経路を確保した通信を行なうことができる。

本発明の他の観点は、本発明の網内エッジ装置を備えたネットワークであって、前記フィルタ手段を備えた網内エッジ装置を唯一備えたことを特徴とするネットワークである。このように、フィルタ手段を備える網内エッジ装置を限定することにより、リソースを有効に利用することができる。

本発明の他の観点は、情報処理装置にインストールすることにより、その情報処理装置に、カスタマ毎に異なるネットワーク情報を提供し、カスタマのパス設定要求を契機に網内エッジ装置間にパスを設定するＶＰＮに設けられ、パス設定に用いる共通ＤＢに相応する機能と、この共通ＤＢにリンク情報を設定するリンク情報設定機能と、このリンク情報を他装置と自装置との間で交換するリンク情報交換機能と、このリンク情報交換に用いる制御情報の転送経路を決定する経路計算機能とを備えた網内エッジ装置としてのＶＰＮ通信制御装置に相応する機能を実現させるプログラムである。

ここで、本発明の特徴とするところは、ＶＰＮ毎に異なるＤＢであるＶＰＮＤＢに相応する機能を生成するＶＰＮＤＢ生成機能と、前記共通ＤＢ中のリンク情

報を当該リンク情報が関わるＶＰＮ毎に分類して分類された各リンク情報にそれぞれＶＰＮを識別する情報であるＶＰＮＩＤを付与するＶＰＮＩＤ設定機能と、前記共通ＤＢのＶＰＮＩＤが付与されたリンク情報から同一ＶＰＮＩＤのリンク情報を抜き出して該当するＶＰＮＤＢに格納するフィルタ機能とを実現させるところにある。

また、他網内エッジ装置と前記リンク情報を交換するためのトンネルを生成するトンネル生成機能を実現させることができる。

また、前記共通ＤＢに相応する機能の一部に前記ＶＰＮＤＢに相応する機能を実現させ、それぞれのＤＢの記録内容を識別するための識別情報を付与する機能を実現させることができる。

また、前記経路計算機能に基づき決定された制御情報の転送経路を用いて他装置間で前記リンク情報を交換する機能を実現させることができる。

また、自装置内のＶＰＮＤＢがいずれのＶＰＮに関するＶＰＮＤＢであるかを他装置に通知する機能と、他装置の要求に応じて自装置内のＶＰＮＤＢの記録内容を当該他装置に転送する機能とを実現させることができる。

また、自装置がフィルタリング実施を行なう装置であるときには前記フィルタ機能によるフィルタリングを実施すると共に他装置に対して前記トンネル設定機能によりトンネルを設定する機能と、他装置が前記フィルタ機能によるフィルタリングを実施しているときには当該他装置に対して前記トンネル設定機能によりトンネルを設定する機能とを実現させることができる。

このときに、自装置を識別する情報である自装置ＩＤとＶＰＮＩＤとを加算した値のハッシュ値が他装置を識別する情報である他装置ＩＤと前記ＶＰＮＩＤを加算した値のハッシュ値よりも大きいときには自装置がフィルタリングを実施する装置であると決定する機能を実現させることができる。

また、カスタマエッジ装置から受信したリンク情報が自装置宛であるときにはカスタマ経路フラグをセットする機能と、前記カスタマ経路フラグがセットされたリンク情報を抽出するカスタマリンク情報抽出機能とを実現させ、このカスタマリンク情報抽出機能によって抽出されたリンク情報を他網内エッジ装置に転送するときには前記カスタマ経路フラグをそのまま付与して転送し、このカスタマ

リンク情報抽出機能によって抽出されたリンク情報をカスタマエッジ装置に転送するときには前記カスタマ経路フラグを削除して転送する機能を実現させることができる。

また、カスタマエッジ装置からパス設定要求を受けて当該パス設定のためのリソースを確保すると共に当該パス設定要求に基づく次網内装置にパス設定要求を転送するシグナリング機能を実現させることができる。

本発明のさらに他の観点は、本発明のプログラムが記録された前記情報処理装置読み取り可能な記録媒体である。本発明のプログラムは本発明の記録媒体に記録されることにより、前記情報処理装置は、この記録媒体を用いて本発明のプログラムをインストールすることができる。あるいは、本発明のプログラムを保持するサーバからネットワークを介して直接前記情報処理装置に本発明のプログラムをインストールすることもできる。

これにより、汎用の情報処理装置を用いて、高いスケーラビリティを実現しながら、ＶＰＮプロバイダ内部のネットワーク情報とカスタマ網のネットワーク情報とを、カスタマに提供することで、カスタマのパス設計を容易に実現可能とすることができるＶＰＮ通信制御装置を実現することができる。

上記目的を達成するため、本発明に係るＶＰＮにおける通信制御装置は、カスタマごとに異なるネットワーク情報を提供し、カスタマのパス設定要求を契機にカスタマエッジ装置間にパスを設定するため、網内エッジ装置に、装置間で詳細なリンク情報を交換するリンク情報交換手段と、ＶＰＮ　ＩＤを設定するＶＰＮ　ＩＤ設定手段と、他装置から送られたリンク情報にＶＰＮ　ＩＤを付与するＶＰＮ　ＩＤ付与手段と、ＶＰＮ　ＩＤが一致するリンク情報のみ抜き出すフィルタ手段とを設けることを特徴とする。

また、前記通信制御装置は、リンク情報交換手段として、ＧＭＰＬＳ（Ｇｅｎｅｒａｌｉｚｅｄ　Ｍｕｌｔｉｐｒｏｔｏｃｏｌ　Ｌａｂｅｌ　Ｓｗｉｔｃｈｉｎｇ）拡張ＯＳＰＦを用いることを特徴とする。

また、前記通信制御装置は、リンク情報に複数のＶＰＮ　ＩＤを付与することを特徴とする。

また、前記通信制御装置は、ＶＰＮごとのリンクアドレスおよびノードアドレスを設定するＶＰＮアドレス設定手段と、全ＶＰＮに共通のリンクアドレスおよびノードアドレスをＶＰＮごとのリンクアドレスおよびノードアドレスに変換するアドレス変換手段を追加し、備えることを特徴とする。

通信制御装置を動作させるための通信制御方法は、網内エッジ装置はカスタマエッジ装置からリンク情報を渡されると、他ノードとリンク情報を交換し、ＶＰＮ　ＩＤを付与し、網内のリンク情報を保持し、カスタマエッジ装置に対して、該リンク情報をフィルタリングして、カスタマがＶＰＮ設定に必要な情報のみ提示することを特徴とする。

本発明では、網内でＯＳＰＦ（Ｏｐｅｎ　Ｓｈｏｒｔｅｓｔ　Ｐａｔｈ　Ｆｉｒｓｔ）など、詳細なリンク情報を交換できる方式を用い、更に、各カスタマが利用可能なリンクを識別し、各カスタマが利用可能なリンク情報のみ、カスタマに提供することで、カスタマごとに異なるＶＰＮプロバイダ内部のネットワーク情報を提供する。カスタマはＶＰＮプロバイダ内部のネットワーク情報が取得できるため、この情報を利用して、パス設定が可能となる。

本願発明は、仮想専用網を個別管理するカスタマ装置に管理情報を提供するとともに、前記仮想専用網を提供する仮想網提供網を統括管理する仮想専用網管理装置において、前記仮想網提供網内のデータ転送経路からなる仮想経路を、仮想リンク帯域に対応させて登録する仮想経路登録手段と、前記仮想経路登録手段により登録された仮想経路に対応するデータ転送経路からなる対応経路を決定する経路決定手段と、前記経路決定手段により決定された対応経路に、前記仮想リンク帯域を割当てる仮想リンク帯域割当手段と、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報を、前記カスタマ装置に提供する仮想リンク帯域情報提供手段とを備えた構成を有している。この構成により、仮想専用網に関する予め決められた仮想経路を登録し、登録された仮想経路と対応する対応経路に仮想リンク帯域を割当てるため、仮想網提供網内のＶＰＮにおけるデータ転送経路に関わらず、カスタマ装置に正確なリンク帯域を表す情報を提供することができる。

本願発明ではさらに、前記仮想網提供網内のデータ転送経路の経路変更を検出

する経路変更検出手段を備え、該経路変更検出手段が経路変更を検出した場合には、前記経路決定手段が、前記仮想経路登録手段により登録された仮想経路に対応する対応経路を、前記経路変更検出手段により経路変更が検出されたデータ転送経路に基づいて決定し、前記仮想リンク帯域割当手段が、前記経路決定手段により決定された対応経路に、前記仮想リンク帯域を割当て、前記仮想リンク帯域情報提供手段が、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報を、前記カスタマ装置に提供する構成を有している。この構成により、仮想網提供網内のデータ転送経路の経路変更を検出するため、仮想専用網の運用中に経路変更がなされても、カスタマ装置に正確なリンク帯域を表す情報を提供することができる。

本願発明ではさらに、前記経路変更検出手段は、前記データ転送経路を構成するリンクの削除に応じて、前記仮想網提供網内のデータ転送経路の経路変更を検出する構成を有している。この構成により、リンクの削除に応じて、仮想網提供網内のデータ転送経路の経路変更を検出するため、仮想専用網の運用中に経路変更がなされても、カスタマ装置に正確なリンク帯域を表す情報を提供することができる。

本願発明ではさらに、前記経路変更検出手段は、前記データ転送経路を構成するリンクの追加に応じて、前記仮想網提供網内のデータ転送経路の経路変更を検出する構成を有している。この構成により、リンクの追加に応じて、仮想網提供網内のデータ転送経路の経路変更を検出するため、仮想専用網の運用中に経路変更がなされても、カスタマ装置に正確なリンク帯域を表す情報を提供することができる。

本願発明ではさらに、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報を自己の画面に表示する表示手段を備えた構成を有している。この構成により、仮想リンク帯域に関する情報を自己の画面に表示するため、カスタマ装置に提供した仮想リンク帯域に関する情報をネットワーク管理者などに確認させることができる。

本願発明ではさらに、前記仮想網提供網内のデータ転送経路におけるコネクションを確立させるための使用帯域情報を受信する使用帯域情報受信手段を備え、

前記仮想リンク帯域割当手段が、前記使用帯域情報受信手段により受信された使用帯域情報を前記対応経路に割当て、前記仮想リンク帯域情報提供手段が、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報および使用帯域情報を、前記カスタマ装置に提供する構成を有している。この構成により、仮想リンク帯域情報および使用帯域情報をカスタマ装置に提供するため、カスタマ装置が使用帯域を把握しながら確実にコネクションを確立させることができる。

本願発明ではさらに、仮想専用網管理装置と、該仮想専用網管理装置に対し管理情報を要求するカスタマ装置とを備えた仮想専用網提供システムであって、前記仮想専用網管理装置が、前記カスタマ装置に仮想リンク帯域に関する情報を提供する構成を有している。この構成により、仮想専用網に関する予め決められた仮想経路を登録し、登録された仮想経路と対応する対応経路に仮想リンク帯域を割当てるため、仮想網提供網内のＶＰＮにおけるデータ転送経路に関わらず、カスタマ装置に正確なリンク帯域を表す情報を提供することができる。

本願発明ではさらに、前記仮想網提供網内のデータ転送経路におけるコネクションを確立させるための使用帯域情報を送信するカスタマ装置と、前記カスタマ装置により送信された使用帯域情報を受信する仮想専用網管理装置とを備えた仮想専用網提供システムであって、前記仮想専用網管理装置が、前記使用帯域情報を前記仮想リンク帯域と共に、前記対応経路に割当て、該割当てた仮想リンク帯域に関する情報および使用帯域情報を前記カスタマ装置に提供する構成を有している。この構成により、仮想リンク帯域情報および使用帯域情報をカスタマ装置に提供するため、カスタマ装置が使用帯域を把握しながら確実にコネクションを確立させることができる。

さらに本願発明は、コンピュータに、それぞれ対応する仮想専用網管理装置における各手段の処理を実行させるための仮想専用網管理プログラムである。

さらに本願発明は、仮想専用網管理プログラムを記録した記録媒体である。

図面の簡単な説明

図１は、ネットワーク構成を示す図である。

図２はリンク情報保持および交換を示す図である。

図３は、ＰＥの構成を示す図である。

図４は、ＰＥにおけるリンク情報の交換の一連の流れを示す図である。

図５は、ＶＰＮＤＢ交換手段を備えたＰＥの構成を示す図である。

図６は、唯一のＰＥでフィルタ手段を実施する際の情報交換の流れを示す図である。

図７は、唯一のＰＥでフィルタ手段を実施する際のトンネル生成の自動化を示す図である。

図８は、カスタマリンク情報抽出手段を備えたＰＥの構成を示す図である。

図９は、カスタマリンク情報抽出手段を備えた際のＰＥにおけるリンク情報の交換を示す図である。

図１０は、シグナリング手段を備えたＰＥの構成を示す図である。

図１１は、シグナリング手段を備えた際のＰＥにおけるパス設定手順を示す図である。

図１２は、ＶＰＮのリンク情報の受け渡しを示す図である。

図１３は、網内エッジ装置の構成を示す図である。

図１４は、網内エッジ装置におけるリンク情報交換の一連の流れを示す図である。

図１５は、アドレス変換が可能な網内エッジ装置の構成を示す図である。

図１６は、アドレス変換が可能な場合の、網内エッジ装置におけるリンク情報交換の一連の流れを示す図である。

図１７は、本発明の第３の実施の形態に係る仮想専用網提供システムのシステム構成図である。

図１８は、本発明の第３の実施の形態に係る仮想専用網管理装置のブロック図である。

図１９Ａ１～１９Ｃ２は、各ＶＰＮに関する仮想リンク帯域情報を提供するイメージの一例を示す図である。

図２０は、本発明の第３の実施の形態に係る仮想専用網管理装置の処理の流れを示すフローチャートである。

図２１は、本発明の第４の実施の形態に係る仮想専用網提供システムのシステム構成図である。

図２２は、本発明の第４の実施の形態に係る仮想専用網管理装置のブロック図である。

図２３A～２３B は、本発明の第４の実施の形態に係る仮想専用網管理装置の処理の流れを示すフローチャートである。

図２４は、本発明の第５の実施の形態に係る仮想専用網提供システムのシステム構成図である。

図２５は、本発明の第５の実施の形態に係る仮想専用網管理装置のブロック図である。

図２６Ａ１～２６Ｃ２は、各ＶＰＮに関する仮想リンク帯域情報および残余帯域情報を提供するイメージの一例を示す図である。

図２７は、本発明の第５の実施の形態に係る仮想専用網管理装置の処理の流れを示すフローチャートである。

発明を実施するための最良の形態

次に、本発明の第１の実施の形態について図面を参照して説明する。

図１は、ネットワーク構成を示す図である。図中、ＰＥ(Provider Edge)とは網内エッジ装置、Ｐとは網内装置、ＣＥ(CustomerEdge)とはカスタマエッジ装置をそれぞれ意味する。また、実施例の文中でも網内エッジ装置、網内装置、カスタマエッジ装置をそれぞれＰＥ、Ｐ、ＣＥと表記する。ＰＥは、少なくても一つのＣＥと接続されており、一方、ＰＥは、ＣＥとは接続されない。Ｐ－ＰＥ間、Ｐ－Ｐ間、ＰＥ－ＰＥ間およびＣＥ－ＰＥ間はデータリンクならびに制御リンクにより接続されている。

データリンクは、主データを転送し、制御リンクは、制御情報を転送する。ＰＥ－ＰＥ間は、制御リンクのみによって接続される場合もある。このような制御リンクをトンネルと呼ぶ。また、網内の各データリンクは、どのＶＰＮが使用可能かを示す識別子が付与されている。

図２は、リンク情報の保持および交換を示す図である。ＰＥでは、ＶＰＮ毎に

異なる情報を格納するＶＰＮＤＢ１０と網内の情報のみを格納する共通ＤＢ９を持つ。共通ＤＢ９の情報の中から、ＶＰＮＩＤが付与された情報のみ、ＶＰＮＤＢ１０に渡される。また、ＶＰＮＤＢ１０の情報は、制御リンクにより接続されているＣＥおよびＰＥと情報の同期をとっている。これにより、各ＣＥに、ＣＥが属するＶＰＮのネットワーク情報のみを通知することができる。

ここでＣＥ－ＢおよびH、ＰＥ－ＣおよびＦは契約ＤＢ（データベース）であるＶＰＮ＃１ＤＢによって情報交換を行っている。ＣＥ－ＡおよびG，ＰＥ－ＣおよびＦは契約ＤＢであるＶＰＮ＃２ＤＢによって情報交換を行っている。図中のその他の構成、すなわち網内エッジ装置ＰＥおよび網内装置Ｐ－ＤおよびＥでは共通ＤＢによって情報交換を行っている。

図２に示すＰＥにおいては特に図示されていないが、該当ＶＰＮＩＤを有するリンク情報を抽出した後、複数のデータリンクを仮想リンクに対応づける（集約する）仮想専用網仮装置の機能を有していても良い。このようにリンク情報を抽出（集約）する機能を設けることで、リソース契約に従って、カスタマに通知する情報を柔軟に設定することが可能である。このようにすることで、カスタマにとって不要な情報の提供を省略して、リソース契約中の条件に必要な情報だけを明示して提示することができる。さらにパスサービスを提供するプロバイダにとっても、不必要に詳細な情報を提供してしまう弊害を回避する効果を実現することができる。

図３は、ＰＥの構成を示すものである。図中、共通ＤＢ３００９とは網内のＰＥ、Ｐと情報交換を行うためのＤＢ、ＶＰＮ＃１ＤＢ、ＶＰＮ＃２ＤＢなど、ＶＰＮ毎に持つＶＰＮＤＢ３０１０とは、当該ＶＰＮに所属するＣＥおよびＰＥの当該ＶＰＮのＶＰＮＤＢ３０１０と情報交換を行なうためのＤＢである。

共通ＤＢ３００９中の隣接データリンク情報ＤＢとは、このＰＥを一つの端点とするデータリンクの内、対向装置がＰもしくはＰＥであるものに関する各種情報を格納する。例えば、図１の例では、ＰＥ（Ｃ）の共通ＤＢ３００９中の隣接データリンクとして、データリンクＣ－Ｄ、データリンクＣ－Ｅが相当する。データリンクに関する各種情報として、装置ＩＤとは、この装置の装置を識別するための情報、リンクＩＦ（インタフェース）ＩＤとは、このリンクのこの装置に

おけるＩＦを識別するための情報、対向装置ＩＤとは、このリンクの対向装置を識別するための情報、対向リンクＩＦＩＤとは、このリンクの対向装置におけるリンクのＩＦを識別するための情報、ＶＰＮＩＤとはこのリンクがどのＶＰＮに属するかを示す識別情報、帯域とは、このリンクの帯域、残帯域とは、このリンクの残りの使用可能帯域をそれぞれ意味する。この他、シーケンスナンバーや廃棄までの時間などを持つ。

共通ＤＢ３００９中のデータリンク情報ＤＢとは、共通ＤＢ３００９中の隣接データリンク情報ＤＢに含まれるデータリンク情報、および共通ＤＢ９中の隣接制御リンク情報ＤＢに含まれる制御リンクを通して、他の装置より、リンク情報交換手段６により取得したデータリンク情報により構成される。

共通ＤＢ９中の隣接制御リンク情報ＤＢとは、このＰＥを一つの端点とする制御リンクの内、対向装置がＰもしくはＰＥであり、かつ、トンネル生成手段３００５により生成されていない、もしくは、対向装置との間に隣接データリンクがあるものに関する各種情報を格納する。

例えば、図１の例では、ＰＥ（Ｃ）の共通ＤＢ９中の隣接制御リンクとして、制御リンクＣ－Ｄ、制御リンクＣ－Ｅが相当する。制御リンクに関する各種情報として、装置ＩＤとは、この装置を識別するための情報、リンクＩＦＩＤとは、このリンクのこの装置におけるＩＦを識別するための情報、対向装置ＩＤとは、このリンクの対向装置を識別するための情報、対向リンクＩＦＩＤとは、このリンクの対向装置におけるリンクのＩＦを識別するための情報、ＶＰＮＩＤとはこのリンクがどのＶＰＮに属するかを示す識別情報をそれぞれ意味する。この他、シーケンスナンバーや廃棄までの時間などを持つ。

共通ＤＢ３００９中の制御リンク情報ＤＢとは、共通ＤＢ３００９中の隣接制御リンク情報ＤＢに含まれる制御リンク情報および共通ＤＢ３００９中の隣接制御リンク情報ＤＢに含まれる制御リンクを通して、他の装置より、リンク情報交換手段３００６により取得した制御リンク情報により構成される。

経路情報ＤＢとは、共通ＤＢ３００９中の制御リンク情報ＤＢを利用して、各装置ＩＤやリンクＩＦＩＤを宛先とした情報を転送するにはどの制御リンクから送出すればよいかを示しており、宛先と送出先ＩＦＩＤを持つ。

ＶＰＮＤＢ３０１０は、共通ＤＢ３００９と同様、隣接データリンク情報ＤＢ、データリンク情報ＤＢ、隣接制御リンク情報ＤＢ、制御リンク情報ＤＢ、経路情報ＤＢからなる。

ＶＰＮＤＢ１０中の隣接データリンクＤＢは、このＰＥを一つの端点とするデータリンクの内、対向装置がこのＶＰＮに属するＣＥであるものに関する各種情報を格納する。図１の例では、ＰＥ（Ｃ）のＶＰＮ＃１のＶＰＮＤＢ３０１０中の隣接データリンクとして、データリンクＣ－Ｂが相当する。各種情報としては、ＶＰＮＩＤがないことを除き、共通ＤＢ３００９中のデータリンク情報と同一である。

ＶＰＮＤＢ３０１０中のデータリンク情報ＤＢは、このＶＰＮＤＢ３０１０中の隣接データリンク情報ＤＢに含まれるデータリンク情報、およびこのＰＥの共通ＤＢ３００９中のデータリンク情報ＤＢの中からこのＶＰＮＩＤを持つリンク情報をフィルタ手段３００３により抽出したデータリンク情報、およびこのＶＰＮＤＢ３０１０中の隣接制御リンク情報ＤＢに含まれる制御リンクを通して、他の装置より、リンク情報交換手段３００６により取得した制御リンク情報により構成される。

ＶＰＮＤＢ３０１０中の隣接制御リンク情報ＤＢは、このＰＥを一つの端点とする制御リンクの内、対向装置がＣＥであるもの、およびトンネル生成手段３００５により生成され、かつ、対向装置がＶＰＮＤＢ３０１０を持つＰＥであるものに関する各種情報を格納する。図１の例では、ＶＰＮ＃１のＶＰＮＤＢ３０１０中の隣接制御リンクとして、制御リンクＣ－Ｂ、Ｃ－Ｆが相当する。ここで、各種情報としては、共通ＤＢ３００９中の隣接制御リンク情報ＤＢと同一である。

ＶＰＮＤＢ３０１０中の制御リンク情報ＤＢは、このＶＰＮＤＢ３０１０中の隣接制御リンク情報ＤＢに含まれる制御リンク情報、およびこのＶＰＮＤＢ３０１０中の隣接制御リンク情報ＤＢに含まれる制御リンクを通して、他の装置より、リンク情報交換手段３００６により取得した制御リンク情報により構成される。

ＶＰＮＤＢ３０１０中の経路情報ＤＢは、このＶＰＮＤＢ３０１０中の制御リンク情報ＤＢを利用して、各装置ＩＤやリンクＩＦＩＤを宛先として情報転送するにはどの制御リンクから送出すればよいかを示しており、宛先と送出先ＩＦＩ

Ｄを持つ。

リンク情報設定手段１は、共通ＤＢ３００９、ＶＰＮＤＢ３０１０中の隣接データリンク情報ＤＢ、隣接制御リンク情報ＤＢに含まれるリンク情報の装置ＩＤ、リンクＩＦＩＤ、対向装置ＩＤ、対向ＩＦＩＤを設定する。

ＶＰＮＩＤ設定手段３００２は、共通ＤＢ３００９中の隣接データリンク情報ＤＢに含まれるＶＰＮＩＤを設定する。

フィルタ手段３００３は、共通ＤＢ３００９のデータリンク情報ＤＢのデータリンク情報の内、特定のＶＰＮＩＤを持つものを抽出し、該当するＶＰＮＤＢ３０１０に注入する。

リンク情報交換手段３００６は、データリンク情報ＤＢおよび制御リンクＤＢに含まれるリンク情報について、隣接制御リンク情報ＤＢに含まれる制御リンクの対向装置ＩＤを持つ全対向装置と情報を交換し、情報を同期させる。すなわち、対向装置と同一のリンク集合を持つように情報の同期を行なう。

パケット転送手段３００８は、経路情報ＤＢを参照し、パケットを転送する。

なお、Ｐは、図３の内、共通ＤＢ３００９、リンク情報設定手段３００１、ＶＰＮＩＤ設定手段３００２、リンク情報交換手段３００６、経路計算手段３００７、パケット転送手段３００８を持つ。

図４は、ＰＥにおけるリンク情報の交換の一連の流れを示すものである。まず、ＶＰＮＤＢ生成手段３００４により、ＶＰＮＤＢ３０１０が生成される。なお、どのＰＥにどのＶＰＮＤＢ３０１０を生成するかは契約などに基づく。次に、リンク情報設定手段３００１により、共通ＤＢ３００９、ＶＰＮＤＢ３０１０中の隣接リンク情報ＤＢ、隣接制御リンクＤＢに含まれる装置ＩＤ、リンクＩＦＩＤ、対向装置ＩＤ、対向リンクＩＦＩＤを設定する。次に、ＶＰＮＩＤ設定手段３００２により、共通ＤＢ３００９の隣接データリンク情報ＤＢのＶＰＮＩＤが設定される。続いて、トンネル生成手段３００５により、トンネルを生成し、ＶＰＮＤＢ１０中の制御リンク情報ＤＢに格納する。ただし、経路情報ＤＢが生成される前には、トンネルが確立されず、始めは設定がされているだけの状態である。

この後、リンク情報交換手段３００６により、隣接制御リンク情報ＤＢに含まれる全ての対向装置に対し、リンク情報を送出すると同時に、対向装置から、リ

ンク情報を受け取る。このとき、受け取ったリンク情報が、自ノード宛ではない場合、トンネルを通っている情報であるため、経路情報ＤＢに基づき、パケット転送手段３００８により、さらに転送を行なう。一方、受け取ったリンク情報が自ノード宛である場合、受け取ったリンク情報が、共通ＤＢ３００９に含まれる隣接制御リンクから取得された場合、共通データリンク情報ＤＢに格納すると同時に、さらにリンク情報のＶＰＮＩＤのＶＰＮＤＢ３０１０があるかどうかの確認を行なう。このＶＰＮＩＤのＶＰＮＤＢ３０１０がある場合、フィルタ手段３００３により、ＶＰＮＤＢ３０１０に情報を渡す。一方、受け取ったリンク情報がその他のデータリンク情報もしくは制御リンク情報である場合は、該当するデータリンク情報ＤＢもしくは制御リンク情報ＤＢに情報を格納する。

さらに、経路計算手段３００７により、経路情報ＤＢの更新を行なう。経路情報の更新により、トンネルが確立される場合がある。なお、ＶＰＮＤＢ生成手段３００４および共通ＤＢ３００９とＶＰＮＤＢ３０１０と個別のＤＢを持つ代わりに、単一のＤＢの中でＩＤを付与し、ＩＤに基づいて選択的に情報を選択する手段を備える方法も考えられる。

また、トンネル生成手段３００５によりトンネルを生成し、トンネルを利用して情報を交換する代わりに、直接接続されていない装置間でも情報交換を実現する手段を備える方法も考えられる。

次に、図５を用いて、ＰＥにどのＶＰＮに関するＶＰＮＤＢ３０１０が存在するかを他のＰＥに通知するＶＰＮＤＢ交換手段３０１１を備えることにより、自動的にどのＰＥとトンネルを生成するべきかを取得できる方法について述べる。図５では、図３と比較して、ＰＥにおいて、ＶＰＮＤＢ交換手段３０１１、対向ＰＥＤＢが追加されている。

ＶＰＮＤＢ交換手段３０１１は、他の全ＰＥと情報の交換を行い、どのＰＥにどのＶＰＮＤＢ３０１０が存在しているかを取得し、取得した情報からあるＶＰＮのＶＰＮＤＢ３０１０を持つＰＥの装置ＩＤを、このＶＰＮＤＢ３０１０中の対向ＰＥＤＢに格納する。例えば、サーバを設けておき、各ＰＥはサーバと情報交換を行なうことで実現できる。

また、フィルタ手段３００３により、共通ＤＢ３００９から、特定のＶＰＮＩ

Ｄを持つデータリンク情報を抽出し、ＶＰＮＤＢ３０１０中のデータリンク情報ＤＢに注入する処理を、唯一のＰＥでのみ実施することもあり得る。このとき、フィルタ手段３００３を実施するかＰＥが、ＶＰＮ毎に異なっていても構わない。このときの情報交換の流れを図６に示す。

このように、フィルタ手段３００３を実施するＰＥが網内に唯一である場合に、ＶＰＮＤＢ交換手段３０１１により、トンネルの設定を自動化することができる。このときの手順を図７に示す。図７に示すように、ＶＰＮＤＢ交換手段３０１１により、どのＰＥにどのＶＰＮＤＢ３０１０が存在するかを全ＰＥで共有する。また、このとき、どのＰＥでフィルタ手段３００３を実施するかを決定する。例えば、装置ＩＤ＋ＶＰＮＩＤの値のハッシュ値をとり、最も大きな値を持つＰＥが、フィルタ手段３００３を実施するものとする。

トンネル生成手段３００５は、自ＰＥがフィルタ手段３００３を実施している場合は、全ＰＥに対し、また、自ＰＥがフィルタ手段３００３を実施していない場合はフィルタ手段３００３を実施するＰＥに対してのみ、トンネルを生成する。これにより、あるＶＰＮのＶＰＮＤＢ１０が存在するＰＥ間には、フィルタ手段３００３を行なうＰＥを頂点としてスター状のトンネルが形成され、全ＰＥの接続性が確保され、全ＰＥのＶＰＮＤＢ３０１０が同一のリンク情報を保持可能となる。

図８は、カスタマリンク情報抽出手段３０１２を備えたＰＥの構成を示すものである。ＶＰＮ毎のＤＢ中のリンク情報ＤＢの内、ＣＥから渡されたリンク情報のみ抽出するカスタマリンク情報抽出手段３０１２を持ち、ＰＥまたは他ＣＥに対しては、カスタマリンク情報抽出手段３０１２によって抽出された情報のみ交換を行なうことにより、情報交換量を削減することを可能とする。なお、このとき、全ＰＥにおいてフィルタ手段３を実施しているものとする。

図８は、図３と比較して、カスタマリンク情報抽出手段３０１２と、ＶＰＮＤＢ３０１０中の、データリンク情報、隣接データリンク情報、制御リンク情報、隣接制御リンク情報に、カスタマ経路フラグが追加されている。

隣接データリンク情報ＤＢ、隣接制御リンク情報ＤＢ中のカスタマ経路フラグは、対向装置ＩＤがＣＥである場合、フラグがセットされる。データリンク情報

ＤＢ、制御リンク情報ＤＢ中のカスタマ経路フラグは、リンク情報交換手段３００６によって情報を受け取った制御リンクの対向装置がＣＥである場合に、フラグがセットされる。

カスタマリンク情報抽出手段３０１２は、カスタマフラグがセットされたデータリンク情報および制御リンク情報を抽出する。リンク情報交換手段３００６は、交換する対向装置がＣＥである場合、ＶＰＮＤＢ３０１０中のカスタマ経路フラグがセットされたデータリンク情報と全制御リンク情報を交換する。ただし、ＰＥから送信する際はカスタマ経路フラグのエントリを削除し、ＰＥで受信した際はカスタマ経路フラグをセットする。また、交換する対向装置がＰＥである場合、カスタマリンク情報抽出手段３０１２により得られたカスタマ経路フラグがセットされたデータリンク情報および制御リンク情報をカスタマ経路フラグをセットしたまま交換する。

図９は、カスタマリンク情報抽出手段３０１２を備えた際のＰＥにおけるリンク情報の交換を示すものである。ＶＰＮＤＢ３０１０の隣接データリンク情報ＤＢと隣接制御リンク情報ＤＢ中のカスタマ経路フラグはあらかじめ設定しておく。リンク情報交換手段３００６は、前述したように動作する。

図１０は、シグナリング手段３０１３を備えたＰＥの構成を示す図である。図３００３と比較して、シグナリング手段３０１３が追加される。シグナリング手段３０１３は、ＣＥからパス設定要求を受け、データリンクリソースを確保し、パス設定要求に含まれる次の転送先のＰもしくはＰＥにパス設定要求を転送する。

パス設定要求には、経由すべきホップ情報と確保すべき帯域が含まれている。ここでホップ情報とは、データリンクＩＦＩＤである場合もあれば、装置ＩＤである場合もある。シグナリング手段３０１３は、ＣＥからパス設定要求を受け取ると、ＣＥが属するＶＰＮのＶＰＮＤＢ３０１０上のデータリンク情報ＤＢを参照し、宛先として指定されているＣＥに隣接するＰＥを検索する。そして、パス設定要求に含まれる経由すべきホップ情報の中から、自装置から検索されたＰＥまでの経路を抜き出す。この経路情報と、パス設定要求に含まれる確保すべき帯域と、ＶＰＮＩＤを含む新たなパス設定要求を生成する。新たなパス設定要求は、ＰＥ間にパスを設定する。

新たなパス設定要求は、共通ＤＢ３００９の経路情報ＤＢを利用して転送される。まず、経由すべきデータリンクＩＦＩＤから次に転送すべき装置を抜き出し、自装置からこの装置に、このＶＰＮが要求されている帯域が十分に確保できるか、共通ＤＢ３００９の隣接データリンク情報ＤＢを検索して確認する。十分に確保できる場合、次に転送すべき装置の送出先ＩＦＩＤを、共通ＤＢ９の経路情報ＤＢから検索し、パス設定要求を転送する。

ＰＥ間にパスが張られた場合、ＰＥは宛先として指定されたＣＥに接続されたＰＥに対して、元のパス設定要求を送る。宛先として指定されたＣＥに接続されたＰＥは、パス設定要求を受け取ると、ＣＥに対してパス設定要求を転送する。

なお、データリンク情報の帯域の値が変更された場合、リンク情報交換手段３００６により、対向装置とリンク情報の同期を行なう。

図１１は、シグナリング手段３０１３を備えた際のパス設定手順を示す図である。パス設定が成功した場合、リンク情報交換手段３００６により、情報の更新を行なう。

本発明は、汎用の情報処理装置にインストールすることにより、その情報処理装置に本発明のＶＰＮ通信制御装置に相応する機能を実現させるプログラムとして実現することができる。このプログラムは、記録媒体に記録されて情報処理装置にインストールされ、あるいは通信回線を介して情報処理装置にインストールされることにより当該情報処理装置に、リンク情報設定手段３００１、ＶＰＮＩＤ設定手段３００２、フィルタ手段３００３、ＶＰＮＤＢ生成手段３００４、トンネル生成手段３００５、リンク情報交換手段３００６、経路計算手段３００７、パケット転送手段３００８、共通ＤＢ３００９、ＶＰＮＤＢ３０１０、ＶＰＮＤＢ交換手段３０１１、カスタマリンク情報抽出手段３０１２、シグナリング手段３０１３にそれぞれ相応する機能を実現させることができる。

さらに本発明の第２の実施の形態について図面を参照して説明する。

図１２は、ネットワーク構成装置間でのリンク情報の受け渡しを示す図である。図中、ＰＥ（Ｐｒｏｖｉｄｅｒ　Ｅｄｇｅ）は網内エッジ装置、Ｐは網内装置、ＣＥ（Ｃｕｓｔｏｍｅｒ　Ｅｄｇｅ）はカスタマエッジ装置を意味する。網内エ

ッジ装置は、少なくても１つのカスタマエッジ装置と接続されており、一方、網内装置は、カスタマエッジ装置とは接続されない。

リンク情報Ｌ１、Ｌ２は、カスタマエッジ装置Ａ、Ｂから網内エッジ装置Ｃに渡されると、カスタマエッジ装置に属するリンク情報Ｌ３に基づき、網内エッジ装置ＣにおいてＶＰＮ　ＩＤが付与される（ＶＰＮ＃１、ＶＰＮ＃２等）。また、網内装置のリンク情報についても、ＶＰＮ　ＩＤを設定しておく。網内では、ＶＰＮ　ＩＤが付与されたリンク情報が交換される。一方、リンク情報Ｌ３は、網内エッジ装置Ｃ、ＦからカスタマエッジＡ、Ｂ、Ｇ、Ｈに渡される際、カスタマエッジ装置Ａ、Ｂ、Ｇ、ＨのＶＰＮ　ＩＤに一致するＶＰＮ　ＩＤをもつリンク情報のみ抜き出され、網内エッジ装置Ｃ、Ｆに渡される。なお、ここで図１に示すＶＰＮ＃１、ＶＰＮ＃２は、それぞれ特定のリンク情報の属する範囲を表わしたものである。

図１３は、網内エッジ装置Ｃ、Ｆの構成を示すものである。

隣接リンク情報ＤＢ２０８は該網内エッジ装置Ｃ、Ｆに接続されるリンクの各種情報を保持するＤＢである。ここで、各種情報として、装置ＩＤはカスタマエッジ装置、網内エッジ装置、網内装置のＩＤ、リンクＩＦ（Ｉｎｔｅｒｆａｃｅ）ＩＤはカスタマエッジ装置、網内エッジ装置、網内装置におけるリンクのＩＦＩＤ、対向装置ＩＤは該リンクの対向装置のＩＤ、対向リンクＩＦ　ＩＤは該リンクの対向装置におけるリンクのＩＦ　ＩＤ、ＶＰＮ　ＩＤは該リンクがどのＶＰＮに属するかを示す識別子、帯域は該リンクの帯域、残帯域は該リンクの残りの使用可能帯域を意味する。この他、シーケンスナンバーや廃棄までの時間などをもつ。

例えば、図１２におけるカスタマエッジ装置Ａと網内エッジ装置Ｃ間のリンクを対象とした場合、網内エッジ装置Ｃにおいて、装置ＩＤはＣ、リンクＩＦ　ＩＤはＣＡ－１、対向装置ＩＤはＡ、対向リンクＩＦ　ＩＤはＡＣ－１、ＶＰＮ　ＩＤはＶＰＮ＃２、帯域は１０Ｍｂｐｓ、残帯域は９０Ｍｂｐｓのようなデータとなる。

なお、カスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈから送られる通常のリンク情報Ｌ１．Ｌ２には、ＶＰＮ　ＩＤは付与されていない。

ＣＥ　ＤＢ２０９とは、隣接リンク情報ＤＢ２０８に含まれる一つないし複数のリンクにより、該網内エッジ装置Ｃ、Ｆがカスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈと接続されている場合、このカスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈの各種情報を保持するＤＢである。ここで、各種情報として、ＣＥ装置ＩＤはカスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈの装置ＩＤ、ＶＰＮ　ＩＤはこのカスタマエッジ装置Ａ、Ｂ、Ｇ、ＨがどのＶＰＮに属するかを示す識別子を意味する。

例えば、図１におけるカスタマエッジ装置Ａを対象とした場合、ＣＥ装置ＩＤはＡ、ＶＰＮ　ＩＤはＶＰＮ＃２のようなデータとなる。

トポロジーＤＢ２１０とは、リンク情報交換手段２０４により取得した、ネットワーク全体のリンク情報を保持するＤＢである。ここで、各リンク情報は、隣接リンク情報ＤＢ２０８に含まれるリンク情報と同じく、装置ＩＤ、リンクＩＦ　ＩＤ、対向装置ＩＤ、対向リンクＩＦ　ＩＤ、ＶＰＮ　ＩＤ、帯域、残帯域、その他を情報としてもつ。

なお、隣接リンク情報ＤＢ２０８中のリンク情報は、トポロジーＤＢ２１０に全て含まれる形態もあれば、隣接リンク情報ＤＢ２０８中のリンク情報は、トポロジーＤＢ２１０に全く含まれない形態もある。いずれの形態においても、該装置におけるリンク情報の全集合を全リンク集合と呼ぶこととする。

例えば、図１においては、Ａ－Ｃ、Ｂ－Ｃ、Ｃ－Ｄ、Ｃ－Ｅ、Ｄ－Ｆ、Ｅ－Ｆ、Ｆ－Ｇ、Ｆ－Ｈの全てのリンクに関するリンク情報の全集合を全リンク集合と呼ぶ。

リンク情報設定手段２０１とは、隣接リンク情報ＤＢ２０８に含まれるリンク情報の装置ＩＤ、リンクＩＦ　ＩＤを設定する。

ＶＰＮ　ＩＤ設定手段２０３とは、隣接リンク情報ＤＢ２０８に含まれるＶＰＮ　ＩＤを設定する。

ＶＰＮ　ＩＤ付与手段２０５とは、カスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈから送られたリンク情報に対して実行され、ＣＥ　ＤＢ２０９を参照し、該当するＣＥ装置ＩＤをもつエントリのＶＰＮ　ＩＤを抜き出し、リンク情報に対して、このＶＰＮ　ＩＤを付与する。

フィルタ手段２０６とは、カスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈにリンク情報を

送る際に実行され、ＣＥ　ＤＢ２０９から該カスタマエッジ装置Ａ、Ｂ、Ｇ、ＨのＣＥ装置ＩＤをもつエントリのＶＰＮ　ＩＤを抜き出し、全リンク集合から、このＶＰＮ　ＩＤをもつリンク情報のみ選択する。

隣接リンク情報交換手段２０２とは、隣接リンク情報ＤＢ２０８に含まれるリンク情報について、対向装置と情報の交換を行い、対向装置ＩＤ、対向リンクＩＦ　ＩＤを取得し、隣接リンク情報ＤＢ２０８に値を設定する。

リンク情報交換手段２０４とは、全リンク集合を、隣接リンク情報ＤＢ２０８に含まれる対向装置ＩＤをもつ全ての対向装置と交換し、情報を同期させる。すなわち、対向装置と同一の全リンク集合をもつように情報の同期を行う。ただし、対向装置がカスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈである場合、カスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈから送られたリンク情報については、ＶＰＮ　ＩＤ付与手段２０５を用い、ＶＰＮ　ＩＤを付与した後、トポロジーＤＢ２１０に保管する。一方、カスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈにリンク情報を送る場合には、フィルタ手段２０６により得たリンク情報についてのみ、ＶＰＮ　ＩＤを取り除いた後、カスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈに送出し、情報の同期をとる。

パス設定手段２０７は、カスタマからのパス設定要求を受け付ける。パス設定要求には、送信元カスタマエッジ装置ＩＤ、宛先カスタマエッジ装置ＩＤ、経由すべき経路上の装置ＩＤのリスト、帯域が含まれる。これに加え、経由すべきリンクのＩＦ　ＩＤが含まれる場合もある。リンクのＩＦ　ＩＤが含まれる場合は、装置間で利用すべきリンクも指定されるが、リンクのＩＦ　ＩＤが含まれない場合、各装置でどのリンクを用いるかおのおの決定する。

パス設定要求を受け取ると、パス設定中にリンクＩＦ　ＩＤが含まれる場合は、該当するリンクを、含まれない場合は、経由すべき経路上の装置ＩＤのリストから次の装置を割り出し、この情報から適切なリンクを、隣接リンク情報ＤＢ２０８から選択するとともに、パス設定要求を、パス設定要求中に含まれる情報に従って、隣接リンク情報ＤＢ２０８に含まれる対向装置に転送する。ただし、このとき、パス設定要求中に含まれる帯域が確保されない場合、対向装置にはパス設定要求を転送せず、パス設定要求が送られてきた経路を逆向きに、帯域が確保できない旨のエラー情報を送信する。

パス設定要求は、最終的に宛先カスタマエッジ装置まで到達すると、成功した旨を含む情報を、同じ経路を逆戻りに送る。この情報を受け取ると、各装置は、パス設定要求中に含まれる情報に従って、隣接リンク情報ＤＢ２０８中の該リンクのエントリの帯域の値が変更される。

リンク情報の帯域の値が変更された場合、リンク情報交換手段２０４により、対向装置とリンク情報の同期を行う。

なお、網内装置Ｄ、Ｅは、図２の中で、ＣＥ　ＤＢ２０９、フィルタ手段２０６、ＶＰＮ　ＩＤ付与手段２０５を除いた手段とＤＢをもつ構成となる。

図１４は、リンク情報の交換の一連の流れを示すフローチャートである。

図１における網内エッジ装置Ｃを例にとり説明する。なお、リンク情報交換以前に、ＣＥ　ＤＢ２０９の構築が行われているものとする。

（ステップＳ１）まず、リンク情報設定手段２０１により、隣接リンク情報ＤＢ２０８の装置ＩＤ、リンクＩＦ　ＩＤが設定される。

例えば、装置ＩＤとして、リンクＩＦ　ＩＤとして、ＣＡ－１、ＣＢ－１、ＣＤ－１、ＣＥ－１が設定される。

（ステップＳ２）次に、ＶＰＮ　ＩＤ設定手段２０３により、隣接リンク情報ＤＢ２０８のＶＰＮ　ＩＤが設定される。例えば、リンクＩＦ　ＩＤ＝ＣＡ－１に対してＶＰＮ　ＩＤとしてＶＰＮ＃２、リンクＩＦ　ＩＤ＝ＣＢ－１に対してＶＰＮ　ＩＤとしてＶＰＮ＃１、リンクＩＦ　ＩＤ＝ＣＤ－１に対してＶＰＮ　ＩＤとしてＶＰＮ＃２、リンクＩＦ　ＩＤ＝ＣＥ－１に対してＶＰＮ　ＩＤとしてＶＰＮ＃１が設定される。

（ステップＳ３）続いて、隣接リンク情報交換手段２０２により、隣接リンク情報ＤＢ２０８の対向装置ＩＤ、対向リンクＩＦ　ＩＤを設定する。

例えば、

リンクＩＦ　ＩＤ＝ＣＡ－１に対して対向装置ＩＤとしてＡ、対向リンクＩＦ　ＩＤとしてＡＣ－１、

リンクＩＦ　ＩＤ＝ＣＢ－１に対して対向装置ＩＤとしてＢ、対向リンクＩＦ　ＩＤとしてＢＣ－１、

リンクＩＦ　ＩＤ＝ＣＤ－１に対して対向装置ＩＤとしてＤ、対向リンクＩＦ

ＩＤとしてＤＣ－１、

リンクＩＦ　ＩＤ＝ＣＥ－１に対して対向装置ＩＤとしてＥ、対向リンクＩＦ　ＩＤとしてＥＣ－１、

が設定される。

（ステップＳ４）この後、リンク情報交換手段２０４により、隣接リンク情報ＤＢ２０８に含まれる全ての対向装置に対して、全リンク情報を送出すると同時に、対向装置から、全リンク情報を受け取る。この時、対向装置がＣＥ　ＤＢ２０９に含まれている場合（ステップＳ４１、Ｓ４２）、送出情報に関してはフィルタ手段２０６を、受取情報に関してはＶＰＮ　ＩＤ付与手段２０５を用い（ステップＳ４３、Ｓ４４）、情報を加工した後、それぞれ送出／受取を行う（ステップＳ４５、Ｓ４６）。

例えば、図１における、Ａ－Ｃ、Ｂ－Ｃ、Ｃ－Ｄ、Ｃ－Ｅ、Ｄ－Ｆ、Ｅ－Ｆ、Ｆ－Ｇ、Ｆ－Ｈの全てのリンクに関する上記のようなデータを送受することとなる。

（ステップＳ５）この後、カスタマ側からパス設定要求があった場合、パス設定手段２０７で処理を行い、パス設定が成功した場合、隣接リンク情報ＤＢ２０８を更新し、更新したリンク情報を、リンク情報交換手段２０４により、対向装置に対して送出する。

例えば、カスタマエッジ装置Ａから送信元カスタマエッジ装置ＩＤ＝Ａ、宛先カスタマエッジ装置ＩＤ＝Ｇ、経由経路＝（Ｃ、Ｄ、Ｆ）、帯域＝１０Ｍでパス設定要求が行われた場合、パス設定要求は装置Ｃ、Ｄ、Ｆを経由して、装置Ｇに至るとともに、パス設定要求が成功した旨を含む情報が装置Ｇから、Ｆ、Ｄ、Ｃを経由して装置Ａに送られ、装置Ａ、Ｃにおける隣接リンク情報ＤＢ２０８のリンクＡＣ－１の残帯域が１０Ｍ減少して更新され、更新したリンク情報が、リンク情報交換手段２０４により、伝播される。リンクＣＤ－１、ＤＦ－１、ＦＧ－１についても同様である。

なお、本願発明における図１３のリンク情報交換手段２０４としては、ＯＳＰＦ、もしくは、ＧＭＰＬＳ拡張ＯＳＰＦを用いることも可能である。

また、図１３の隣接リンク情報ＤＢ２０８のＶＰＮ　ＩＤに対して、複数の値

をもつことも可能である。ＶＰＮ　ＩＤを複数もつ場合、フィルタ手段２０６で、同一のリンク情報が異なるＶＰＮ　ＩＤをもつカスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈに対して選択されるため、同一リンク情報を異なるカスタマに提供可能となる。

次に、図１５を用いて、図１３に示した網内エッジ装置に対して、ＶＰＮごとのリンクアドレスおよびノードアドレスを設定するＶＰＮアドレス設定手段４０６と、全ＶＰＮに共通のリンクアドレスおよびノードアドレスをＶＰＮごとのリンクアドレスおよびノードアドレスに変換するアドレス変換手段４０８を追加することにより、ＶＰＮごとに独立のアドレス設計を可能とする方法について述べる。

図１５では、隣接リンク情報ＤＢ４１０において、ＶＰＮ装置ＩＤ、ＶＰＮリンクＩＦ　ＩＤ、ＶＰＮ対向装置ＩＤ、ＶＰＮ対向リンクＩＦ　ＩＤが追加される。ここで、ＶＰＮ装置ＩＤとは、装置ＩＤのＶＰＮごとの値、ＶＰＮリンクＩＦ　ＩＤとは、リンクＩＦ　ＩＤのＶＰＮごとの値、ＶＰＮ対向装置ＩＤとは、装置ＩＤのＶＰＮごとの値、ＶＰＮ対向リンクＩＦ　ＩＤとは、対向リンクＩＦ　ＩＤのＶＰＮごとの値を、それぞれ意味する。

ＶＰＮアドレス設定手段４０６では、隣接リンク情報ＤＢ４１０のＶＰＮ装置ＩＤ、ＶＰＮリンクＩＦ　ＩＤを設定する。

リンク情報交換手段４０４では、カスタマエッジ装置Ａ、Ｂ、Ｇ、Ｈにリンク情報を送出する際、アドレス変換手段４０８において、リンク情報の、①装置ＩＤをＶＰＮ装置ＩＤに、②リンクＩＦ　ＩＤをＶＰＮリンクＩＦ　ＩＤに、③対向装置ＩＤをＶＰＮ対向装置ＩＤに、④対向リンクＩＦ　ＩＤをＶＰＮ対向リンクＩＦ　ＩＤに、それぞれ変換し、ＶＰＮ装置ＩＤ、ＶＰＮリンクＩＦ　ＩＤ、ＶＰＮ対向装置ＩＤ、ＶＰＮ対向リンクＩＦ　ＩＤ、ＶＰＮ　ＩＤを削除した後、送出する。

また、隣接リンク情報交換手段４０２において、対向装置ＩＤ、対向リンクＩＦ　ＩＤに加え、ＶＰＮ対向装置ＩＤ、ＶＰＮ対向リンクＩＦ　ＩＤを取得し、隣接リンク情報ＤＢ４１０に値を設定する。ただし、ＣＥからのリンク情報に対しては、ＶＰＮ対向装置ＩＤ、ＶＰＮ対向リンクＩＦ　ＩＤは付与されていないため、ＶＰＮ対向装置ＩＤとして対向装置ＩＤ、ＶＰＮ対向リンクＩＦ　ＩＤと

して対向リンクＩＦ　ＩＤの値を用いる。

図１６は、アドレス変換手段が可能な場合の、網内エッジ装置におけるリンク情報交換の一連の流れを示すフローチャートである。

図１２における網内エッジ装置Ｃを例にとり、説明する。なお、リンク情報交換以前に、ＣＥ　ＤＢ４１１の構築が行われているものとする。

（ステップＳ１１）まず、リンク情報設定手段４０１により、隣接リンク情報ＤＢ４１０の装置ＩＤ、リンクＩＦ　ＩＤが設定される。

例えば、装置ＩＤとしてＣ、リンクＩＦ　ＩＤとして、ＣＡ－１、ＣＢ－１、ＣＤ－１、ＣＥ－１が設定される。

（ステップＳ１２）次に、ＶＰＮ　ＩＤ設定手段４０３により、隣接リンク情報ＤＢ４１０のＶＰＮ　ＩＤが設定される。

例えば、リンクＩＦ　ＩＤ＝ＣＡ－１に対して、ＶＰＮ　ＩＤとしてＶＰＮ＃２、リンクＩＦ　ＩＤ＝ＣＢ－１に対して、ＶＰＮ　ＩＤとしてＶＰＮ＃１、リンクＩＦ　ＩＤ＝ＣＤ－１に対して、ＶＰＮ　ＩＤとしてＶＰＮ＃２、リンクＩＦ　ＩＤ＝ＣＥ－１に対して、ＶＰＮ　ＩＤとしてＶＰＮ＃１が設定される。

（ステップＳ１３）続いて、ＶＰＮアドレス設定手段４０６により、隣接リンク情報ＤＢ４１０に、ＶＰＮ装置ＩＤ、ＶＰＮリンクＩＦ　ＩＤが追加される。

例えば、装置Ｃに対して、装置ＩＤ　Ｃ、リンクＩＦ　ＩＤ　ＣＡ－１、対向装置ＩＤ　Ａ、対向リンクＩＦ　ＩＤ　ＡＣ－１に対して、ＶＰＮ装置ＩＤ　ＶＰＮ２－Ｃ、ＶＰＮリンクＩＦ　ＩＤ　ＶＰＮ２－ＣＡ－１、装置ＩＤ　Ｃ、リンクＩＦ　ＩＤ　ＣＢ－１、対向装置ＩＤ　Ｂ、対向リンクＩＦ　ＩＤ　ＢＣ－１に対して、ＶＰＮ装置ＩＤ　ＶＰＮ１－Ｃ、ＶＰＮリンクＩＦ　ＩＤ　ＶＰＮ１－ＣＢ－１、装置ＩＤ　Ｃ、リンクＩＦ　ＩＤ　ＣＤ－１、対向装置ＩＤ　Ｄ、対向リンクＩＦ　ＩＤ　ＤＣ－１に対して、ＶＰＮ装置ＩＤ　ＶＰＮ２－Ｃ、ＶＰＮリンクＩＦ　ＩＤ　ＶＰＮ２－ＣＤ－１、装置ＩＤ　Ｃ、リンクＩＦ　ＩＤ　ＣＥ－１、対向装置ＩＤ　Ｅ、対向リンクＩＦ　ＩＤ　ＥＣ－１に対して、ＶＰＮ装置ＩＤ　ＶＰＮ１－Ｃ、ＶＰＮリンクＩＦ　ＩＤ　ＶＰＮ１－ＣＥ－１がそれぞれ付与される。

（ステップＳ１４）続いて、隣接リンク情報交換手段４０２により、隣接リン

ク情報ＤＢ４１０の対向装置ＩＤ、対向リンクＩＦ　ＩＤ、ＶＰＮ対向装置ＩＤ、ＶＰＮ対向リンクＩＦ　ＩＤを設定する。

例えば、

リンクＩＦ　ＩＤ＝ＣＡ－１に対して対向装置ＩＤとしてA、対向リンクＩＦ　ＩＤとしてＡＣ－１、ＶＰＮ対向装置ＩＤとしてA、ＶＰＮ対向リンクＩＦ　ＩＤとしてＡＣ－１、

リンクＩＦ　ＩＤ＝ＣＢ－１に対して対向装置ＩＤとしてB、対向リンクＩＦ　ＩＤとしてＢＣ－１、ＶＰＮ対向装置ＩＤとしてB、ＶＰＮ対向リンクＩＦ　ＩＤとしてＢＣ－１、

リンクＩＦ　ＩＤ＝ＣＤ－１に対して対向装置ＩＤとしてD、対向リンクＩＦ　ＩＤとしてＤＣ－１、ＶＰＮ対向装置ＩＤとしてＶＰＮ２－Ｄ、ＶＰＮ対向リンクＩＦ　ＩＤとしてＶＰＮ２－ＤＣ－１、

リンクＩＦ　ＩＤ＝ＣＥ－１に対して対向装置ＩＤとしてE、対向リンクＩＦ　ＩＤとしてＥＣ－１、ＶＰＮ対向装置ＩＤとしてＶＰＮ１－Ｅ、ＶＰＮ対向リンクＩＦ　ＩＤとしてＶＰＮ１－ＥＣ－１

が設定される。

（ステップＳ１５）この後、リンク情報交換手段４０４により、隣接リンク情報ＤＢ４１０に含まれる全ての対向装置に対して、全リンク情報を送出すると同時に、対向装置から、全リンク情報を受け取る。この時、対向装置がＣＥ　ＤＢ４１１に含まれている場合（ステップＳ５１、Ｓ５２）、送出情報に関しては、フィルタ手段４０７およびアドレス変換手段４０８を（ステップＳ５３、Ｓ５５）、受取情報に関してはＶＰＮ　ＩＤ付与手段４０５を用い（ステップＳ５４、Ｓ５６）、情報を加工した後、それぞれ送出／受取を行う（ステップＳ５６、Ｓ５７）。

例えば、図１２における、Ａ－Ｃ、Ｂ－Ｃ、Ｃ－Ｄ、Ｃ－Ｅ、Ｄ－Ｆ、Ｅ－Ｆ、Ｆ－Ｇ、Ｆ－Ｈの全てのリンクに関する上記のようなデータを送受することとなる。

また、例えば、カスタマAに送信される情報は、

装置ＩＤとしてＶＰＮ２－Ｃ、

リンクＩＦ　ＩＤ　ＶＰＮ２－ＣＡ－１、対向装置ＩＤ　ＶＰＮ２－Ａ、対向

リンクＩＦ　ＩＤ　ＶＰＮ２－ＡＣ－１、

リンクＩＦ　ＩＤ　ＶＰＮ２－ＣＤ－１、対向装置ＩＤ　ＶＰＮ２－Ｄ、対向リンクＩＦ　ＩＤ　ＶＰＮ２－ＤＣ－１

のようになる。

（ステップＳ１６）この後、カスタマ側からパス設定要求があった場合、パス設定手段４０９で処理を行い、パス設定が成功した場合、隣接リンク情報ＤＢ４１０を更新し、更新したリンク情報を、リンク情報交換手段４０４により、対向装置に対して送出する。

例えば、カスタマエッジ装置Ａから送信元カスタマエッジ装置ＩＤ＝Ａ、宛先カスタマエッジ装置ＩＤ＝Ｇ、経由経路＝（ＶＰＮ２－Ｃ、ＶＰＮ２－Ｄ、ＶＰＮ２－Ｆ）、帯域１０Ｍでパス設定要求が行われた場合、パス設定要求は装置Ｃ、Ｄ、Ｆを経由して、装置Ｇに至るとともに、パス設定要求が成功した旨を含む情報が装置Ｇから、Ｆ、Ｄ、Ｃを経由して装置Ａに送られ、装置Ａ、Ｃにおける隣接リンク情報ＤＢのリンクＶＰＮ２－ＡＣ－１の残帯域が１０Ｍ減少して更新され、更新したリンク情報が、リンク情報交換手段により、伝播される。リンクＶＰＮ２－ＣＤ－１、ＶＰＮ２－ＤＦ－１、ＶＰＮ２－ＦＧ－１についても同様である。

上述の実施形態において、その処理を行うプログラムをアプリケーションソフトとして、ＣＤ－ＲＯＭ等の記録媒体に格納しておいてもよい。このようにすれば、ＣＤ－ＲＯＭ等の可搬型記録媒体にプログラム等を格納して売買したり、携帯することができるようになる。

以下、図面を参照して、本発明の実施の形態について詳細に説明する。図１７は、本発明の第３の実施の形態に係る仮想専用網提供システムのシステム構成図である。以下、仮想専用網をＶＰＮと表す。

図１７に示すように、ＶＰＮ提供システム１０００は、仮想専用網管理装置２１００、ＶＰＮを提供する仮想網提供網２０４０、ＶＰＮ２０１０、ＶＰＮ２０２０、およびＶＰＮ２０３０を含むように構成される。例えば、ＶＰＮ２０１０、ＶＰＮ２０２０、およびＶＰＮ２０３０は、インターネット接続業者（ＩＳＰ：

Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）などに提供されるネットワークである。

仮想網提供網２０４０は、データ転送装置２０４１～２０４５、およびリンク４１４２，４１４４，４２４３，４３４４，４４４５を含むように構成される。なお、データ転送装置２０４１～２０４５は、ルータやハブ（ＨＵＢ）、ＯＸＣ（光クロスコネクト：Ｏｐｔｉｃａｌ　Ｃｒｏｓｓ－ｃｏｎｎｅｃｔ）などを含む通信装置である。リンク４１４２，４１４４，４２４３，４３４４，４４４５は、１つのデータ転送装置と他のデータ転送装置とを接続する光ファイバを含むが、本発明によれば、有線、無線を問わない。

ＶＰＮ２０１０は、仮想網提供網２０４０、データ転送装置２０１１～２０１３、およびカスタマ装置２０１９を含むように構成される。なお、カスタマ装置２０１９は、ＶＰＮを管理するための装置であり、仮想網提供網２０４０が含まないＶＰＮ内のデータ転送装置に具備されていてもよい。

ＶＰＮ２０２０は、仮想網提供網２０４０、データ転送装置２０２１，２０２２、およびカスタマ装置２０２９を含むように構成される。また、ＶＰＮ２０３０は、仮想網提供網２０４０、データ転送装置２０３１，２０３２、およびカスタマ装置２０３９を含むように構成される。

なお、各カスタマ装置２０１９，２０２９，２０３９は、それぞれのＶＰＮ２０１０，２０２０，２０３０内のデータ転送装置２０１１～２０１３，２０２１，２０２２，２０３１，２０３２と接続されるようにしてもよく、また、図示しないＶＰＮを管理するための管理ネットワークと接続されるようにしてもよい。

図２は、本発明の第３の実施の形態に係る仮想専用網管理装置のブロック図である。図１８に示すように、仮想専用網管理装置２１００は、リンク帯域格納手段２１１０、仮想経路登録手段２１２０、経路決定手段２１３０、仮想リンク帯域割当手段２１５０、仮想リンク帯域情報提供手段２１６０、および表示手段２１７０を含むように構成される。

リンク帯域格納手段２１１０は、仮想専用網を提供する仮想網提供網２０４０内のデータ転送装置２０４１～２０４５間のリンク４１４２，４１４４，４２４３，４３４４，４４４５に関するリンク帯域を表すリンク帯域情報を格納するよ

うになっている。ここで、リンク帯域格納手段２１１０が格納するリンク帯域情報の一例を表１に示す。なお、リンク帯域格納手段２１１０は、リンク帯域情報を仮想専用網管理装置２１００が有するハードディスクなどを含む記憶手段に格納してもよい。

表１

データ転送装置間のリンク	リンク帯域
リンク4142	100
リンク4243	100
リンク4144	100
リンク4344	100
リンク4445	200

表１に示したように、例えば、リンク４４４５は、リンク帯域が２００Ｍｂｉｔ／ｓであることを示している。なお、２００Ｍｂｉｔ／ｓは、１秒間に２００メガビットのデータ量が使用可能であることを表している。

仮想経路登録手段２１２０は、仮想網提供網２０４０内の仮想専用網に関する予め決められたデータ転送経路からなる仮想経路と、仮想リンク帯域とを登録するようになっている。なお、仮想経路は、実在する経路または仮想の経路からなる。例えば、仮想経路登録手段２１２０には、ＶＰＮを運用するＩＳＰなどとの契約に応じて、仮想網提供網２０４０を管理するネットワーク管理者から、仮想経路と、この仮想経路に対応する帯域の上限となる仮想リンク帯域とに関する仮想経路情報が入力され、仮想経路登録手段２１２０は、入力された仮想経路情報を登録するようになっている。

ここで、仮想経路登録手段２１２０が登録する仮想経路情報の一例を表２に示す。表２に示したように、ＶＰＮ２０１０の仮想経路は、データ転送装置２０４１とデータ転送装置２０４２との間のリンク、および、データ転送装置２０４２とデータ転送装置２０４３の間のリンクによって構成され、それぞれの仮想リンク帯域は１０Ｍｂｉｔ／ｓである。また、ＶＰＮ２０２０の仮想経路は、データ転送装置２０４１とデータ転送装置２０４５との間のリンクによって構成され、仮想リンク帯域は１０Ｍｂｉｔ／ｓである。なお、データ転送装置２０４１とデータ転送装置２０４５との間のリンク、および、データ転送装置２０４３とデー

タ転送装置２０４５との間のリンクは、実在しない仮想の経路からなる。

表２

ＶＰＮ	仮想経路	仮想経路(名称)	仮想リンク帯域
ＶＰＮ１０	データ転送装置2041とデータ点装置2042と間のリンク	V2011	10
	データ転送装置2042とデータ点装置2043と間のリンク	V2012	10
ＶＰＮ２０	データ転送装置2041とデータ点装置2045と間のリンク	V2021	10
ＶＰＮ３０	データ転送装置2043とデータ点装置2042と間のリンク	V2032	10

なお、以降、表２に示したように、データ転送装置２０４１とデータ転送装置２０４２との間のリンクを表す仮想経路を仮想経路Ｖ２０１１、データ転送装置２０４２とデータ転送装置２０４３との間のリンクを表す仮想経路を仮想経路Ｖ２０１２、データ転送装置２０４１とデータ転送装置２０４５との間のリンクを表す仮想経路を仮想経路Ｖ２０２１、データ転送装置２０４３とデータ転送装置２０４５との間のリンクを表す仮想経路を仮想経路Ｖ２０３１としてそれぞれ表す。

経路決定手段２１３０は、仮想経路登録手段２１２０によって登録された仮想経路を一つずつ選択し、選択された仮想経路と対応するデータ転送経路からなる対応経路を決定し、決定された対応経路に関する情報を仮想リンク帯域割当手段２１５０に出力するようになっている。

ここで、経路決定手段２１３０が決定する対応経路の１例を表３に示す。

表３

ＶＰＮ	仮想経路	対応経路
ＶＰＮ１０	V2011	リンク4142
	V2012	リンク4243
ＶＰＮ２０	V2021	リンク4144およびリンク4445
ＶＰＮ３０	V2032	リンク4344およびリンク4445

例えば、経路決定手段２１３０は、仮想経路を一つずつ選択し、選択された仮想経路の端のデータ転送装置と、もう一方のデータ転送装置とに対応する最短のデータ転送経路を、公知のＣＳＰＦ（Ｃｏｎｓｔｒａｉｎｔ　Ｓｈｏｒｔｅｓｔ　Ｐａｔｈ　Ｆｉｒｓｔ）などを用いて算出し、算出されたデータ転送経路を対応経路として決定するようになっている。

本実施の形態では、経路決定手段２１３０は、ＶＰＮ２０２０の仮想経路、すなわち、仮想経路Ｖ２０２１を選択したとき、最短のデータ転送経路となるリンク４１４４およびリンク４４４５を対応経路として決定するようになっている。

仮想リンク帯域割当手段２１５０は、経路決定手段２１３０によって出力された対応経路情報が入力されたとき、仮想経路登録手段２１２０から仮想リンク帯域を取得し、取得された仮想リンク帯域を対応経路に割当て、割当てた仮想リンク帯域に関する仮想リンク帯域情報を仮想リンク帯域情報提供手段２１６０に出力するようになっている。また、仮想リンク帯域割当手段２１５０は、仮想リンク帯域情報を表示手段２１７０に出力するようにしてもよい。

ここで、仮想リンク帯域割当手段２１５０が割当てた仮想リンク帯域に関する仮想リンク帯域情報の一例を表４に示す。

表４

仮想経路	対応経路	仮想リンク帯域
V2011	リンク4142	10
V2012	リンク4243	10
V2021	リンク4144およびリンク4445	10
V2032	リンク4344およびリンク4445	10

例えば、仮想リンク帯域割当手段２１５０は、仮想経路Ｖ２０２１について、表２に示した仮想経路情報と対応する仮想リンク帯域、１０Ｍｂｉｔ／ｓをリンク４１４４およびリンク４４４５に割当てるようになっている。

なお、対応経路に含まれるリンクについて、仮想リンク帯域の合計が、仮に、表１に示した帯域を超えていたとき、仮想リンク帯域割当手段２１５０は、異常の旨をネットワーク管理者に通知するようにしてもよい。

仮想リンク帯域情報提供手段２１６０には、仮想リンク帯域割当手段２１５０によって出力された仮想リンク帯域情報が入力され、仮想リンク帯域情報提供手段２１６０は、入力された仮想リンク帯域情報をカスタマ装置２０１９，２０２９，２０３９に提供するようになっている。例えば、仮想リンク帯域情報提供手段２１６０は、仮想リンク帯域情報をＷｅｂサーバなどに格納し、カスタマ装置２０１９，２０２９，２０３９は、格納された仮想リンク帯域情報を、仮想網提供網２０４０経由または管理ネットワーク経由でダウンロードするようにしてもよい。

仮想リンク帯域情報提供手段２１６０が、ＶＰＮ２０１０を管理するカスタマ装置２０１９に仮想リンク帯域情報を提供するイメージの一例を図１９Ａ１に示す。また、仮想リンク帯域情報提供手段２１６０が、ＶＰＮ２０２０を管理するカスタマ装置２０２９に仮想リンク帯域情報を提供するイメージの一例を図１９Ｂ１に示す。また、仮想リンク帯域情報提供手段２１６０が、ＶＰＮ２０３０を管理するカスタマ装置２０３９に仮想リンク帯域情報を提供するイメージの一例を図１９Ｃ１に示す。

例えば、図１９Ｂ１に示したように、仮想経路Ｖ２０２１は、仮想リンク帯域が１０Ｍｂｉｔ／ｓであることを示している。また、仮想リンク帯域情報提供手段２１６０は、例えば、仮想網提供網４０を含むデータ転送装置４１と、仮想網提供網２０４０を含まないデータ転送装置２１との間のリンク帯域情報を提供するようにしてもよい。

表示手段２１７０には、仮想リンク帯域割当手段２１５０によって出力された仮想リンク帯域情報が入力され、表示手段２１７０は、入力された仮想リンク帯域情報を自己の画面に表示するようになっている。表示手段２１７０がＶＰＮ１０に関する仮想リンク帯域情報を表示するイメージの一例を図１９Ａ１に示す。表示手段２１７０がＶＰＮ２０２０に関する仮想リンク帯域情報を表示するイメージの一例を図１９Ｂ１に示す。また、表示手段２１７０がＶＰＮ２０３０に関する仮想リンク帯域情報を表示するイメージの一例を図１９Ｃ１に示す。

また、表示手段２１７０がＶＰＮ１０に関する対応経路の仮想リンク帯域情報を表示するイメージの一例を図１９Ａ２に示す。また、表示手段２１７０がＶＰ

Ｎ２０２０に関する対応経路の仮想リンク帯域情報を表示するイメージの一例を図１９Ｂ２に示す。また、表示手段２１７０がＶＰＮ２０３０に関する対応経路の仮想リンク帯域情報を表示するイメージの一例を図１９Ｃ２に示す。例えば、図１９Ｂ２に示したように、データ転送装置２０４１とデータ転送装置２０４４との間のリンクは、仮想リンク帯域が１０Ｍｂｉｔ／ｓであり、データ転送装置２０４４とデータ転送装置２０４５との間が仮想リンク帯域が１０Ｍｂｉｔ／ｓであることを示している。

以下、本発明の第３の実施の形態に係る仮想専用網管理装置の処理について、図面を参照して説明する。図２０は、本発明の第３の実施の形態に係る仮想専用網管理装置の処理の流れを示すフローチャートである。まず、仮想網提供網２０４０内の仮想専用網に関する予め決められたデータ転送経路からなる仮想経路と仮想リンク帯域とが、仮想経路登録手段２１２０によって登録される（ステップＳ１０１）。次に、仮想経路登録手段２１２０によって登録された仮想経路に対応するデータ転送経路からなる対応経路は、経路決定手段２１３０によって決定され（ステップＳ１０２）、対応経路に対応する仮想リンク帯域は、仮想リンク帯域割当手段２１５０によって割当てられ（ステップＳ１０３）、割当てられた仮想リンク帯域に関する仮想リンク帯域情報が、仮想リンク帯域情報提供手段２１６０によって各カスタマ装置２０１９，２０２９，２０３９に提供される（ステップＳ１０４）。

以上説明したように、本発明の第３の実施の形態に係る仮想専用網管理装置２１００および仮想専用網提供システム１０００は、仮想専用網に関する予め決められた仮想経路を登録し、登録された仮想経路に対応する対応経路に仮想リンク帯域を割当てるため、仮想網提供網２０４０内のＶＰＮ２０１０，２０２０，２０３０におけるデータ転送経路に関わらず、カスタマ装置２０１９，２０２９，２０３９に正確な仮想リンク帯域を表す情報を提供することができる。また、仮想リンク帯域に関する情報を自己の画面に表示するため、カスタマ装置２０１９，２０２９，２０３９に提供した仮想リンク帯域に関する情報をネットワーク管理者などに確認させることができる。

図２１は、本発明の第４の実施の形態に係る仮想専用網提供システムのシステ

ム構成図である。以下、仮想専用網をＶＰＮと表す。

図２０に示すように、ＶＰＮ提供システム２０００は、仮想専用網管理装置２２００、ＶＰＮを提供する仮想網提供網２０４０、ＶＰＮ２０１０、ＶＰＮ２０２０、およびＶＰＮ２０３０を含むように構成される。例えば、ＶＰＮ２０１０、ＶＰＮ２０２０、およびＶＰＮ２０３０は、インターネット接続業者などに提供されるネットワークである。なお、本発明の第４の実施の形態に係るＶＰＮ提供システム２０００を構成する要素のうち、図１７に示した本発明の第３の実施の形態に係るＶＰＮ提供システム１０００を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

図２２は、本発明の第４の実施の形態に係る仮想専用網管理装置のブロック構成図である。図２２に示すように、仮想専用網管理装置２２００は、リンク帯域格納手段２１１０、仮想経路登録手段２１２０、経路決定手段２２３０、仮想リンク帯域割当手段２１５０、仮想リンク帯域情報提供手段２１６０、および経路変更検出手段２２８０を含むように構成される。なお、本発明の第４の実施の形態に係る仮想専用網管理装置２２００のうち、図１８に示した本発明の第３の実施の形態に係る仮想専用網管理装置２１００を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

ここで、リンク帯域格納手段２１１０は、表１に示したリンク帯域情報を格納するようになっている。また、仮想経路登録手段２１２０は、表２に示したように各ＶＰＮ２０１０，２０２０，２０３０に対応する仮想経路と、仮想リンク帯域とを登録するようになっている。

経路変更検出手段２２８０は、リンク削除検出手段２２８１およびリンク追加検出手段２２８２を含むように構成され、仮想網提供網２０４０内のデータ転送経路の経路変更を検出するようになっている。

リンク削除検出手段２２８１は、仮想網提供網２０４０内のデータ転送装置２０４１～２０４５間のリンク４１４２，４１４４，４２４３，４３４４，４４４５の削除に応じて、仮想網提供網２０４０内のデータ転送経路の経路変更を検出し、検出された経路変更に関する経路変更情報を経路決定手段２２３０に出力するようになっている。例えば、リンク４１４４が削除されたとき、リンク削除検

出手段２２８１は、リンク４１４４の削除に応じて仮想網提供網２０４０内のデータ転送経路の経路変更を検出するようになっている。

リンク追加検出手段２２８２は、仮想網提供網２０４０内のデータ転送装置２０４１～２０４５間のリンクの追加に応じて、仮想網提供網２０４０内のデータ転送経路の経路変更を検出し、検出された経路変更に関する経路変更情報を経路決定手段２２３０に出力するようになっている。例えば、上述したように、削除されたリンク４１４４が再度追加されたとき、リンク追加検出手段２２８２は、リンク４１４４の追加に応じて仮想網提供網２０４０内のデータ転送経路の経路変更を検出するようになっている。

経路決定手段２２３０には、経路変更検出手段２２８０によって出力された経路変更情報が入力され、経路決定手段２２３０は、入力された経路変更情報に応じて、仮想経路登録手段２１２０によって登録された仮想経路に対応する対応経路を決定し、決定された対応経路に関する対応経路情報を仮想リンク帯域割当手段２１５０に出力するようになっている。

例えば、リンク４１４４が削除されたとき、経路決定手段２２３０は、仮想経路に対応する仮想網提供網２０４０内の最短のデータ転送経路に基づいて、表３に示すような対応経路から表５に示すような対応経路を変更して決定するようになっている。ＶＰＮ２０２０の仮想経路Ｖ２０２１に対応する対応経路は、リンク４１４２，４２４３，４３４４，４４４５によって構成される。

表５

ＶＰＮ	仮想経路	対応経路
ＶＰＮ１０	V2011	リンク4142
	V2012	リンク4243
ＶＰＮ２０	V2021	リンク4144，リンク4142，リンク4344，およびリンク4445
ＶＰＮ３０	V2032	リンク4344，およびリンク4445

また、例えば、リンク４１４４が追加されたとき、経路決定手段２２３０は、仮想経路に対応する仮想網提供網２０４０内の最短のデータ転送経路に基づいて、表５に示すような対応経路から表３に示すような対応経路に変更して決定するよ

うになっている。

以下、本発明の第４の実施の形態に係る仮想専用網管理装置の処理について、図面を参照して説明する。図２３Ａおよび２３Ｂは、本発明の第４の実施の形態に係る仮想専用網管理装置の処理の流れを示すフローチャートである。なお、本発明の第４の実施の形態に係る仮想専用網管理装置２２００の処理のうち、図２０に示した本発明の第３の実施の形態に係る仮想専用網管理装置２１００の処理と同一のものには同一符号を付し、それぞれの説明を省略する。以下、本発明の第２の実施の形態に係る仮想専用網管理装置の処理について、リンクが削除された場合とリンクが追加された場合とに分けて説明する。

図２３Ａに示すように、仮想網提供網２０４０内のデータ転送装置２０４１～２０４５間のリンク４１４２，４１４４，４２４３，４３４４，４４４５の削除に応じて、仮想網提供網２０４０内のデータ転送経路の経路変更が、経路変更検出手段２２８０によって検出された場合、処理は、ステップ２０２からステップ２０３へ進み、経路変更が検出されない場合、処理は終了する（ステップＳ２０１）。例えば、ＶＰＮ２０２０に対応するリンク４１４４が削除されたとき、経路変更がリンク削除検出手段２２８１によって検出される（ステップＳ２０２）。

経路変更情報に応じて仮想経路登録手段２１２０によって登録された仮想経路に対応する対応経路が、経路決定手段２２３０によって決定される（ステップＳ２０３）。例えば、ＶＰＮ２０２０に対応するリンク４１４４が削除されたとき、表３に示すような対応経路から表５に示すような対応経路に変更され決定される。

対応経路に対応する仮想リンク帯域は、仮想リンク帯域割当手段２１５０によって割当てられ（ステップＳ１０３）、割当てられた仮想リンク帯域に関する仮想リンク帯域情報が、仮想リンク帯域情報提供手段２１６０によって各カスタマ装置２０１９，２０２９，２０３９に提供される（ステップＳ１０４）。ここで、仮想リンク帯域情報提供手段２１６０が、ＶＰＮ２０２０を管理するカスタマ装置２０２９に仮想リンク帯域情報を提供するイメージの一例は、図１９Ｂ１に示される。

図２３Ｂに示すように、例えば、ＶＰＮ２０２０に対応するリンク４１４４が追加されたとき、経路変更がリンク追加検出手段２８２によって検出される（ス

テップＳ２０４)。経路変更情報に応じて仮想経路登録手段２１２０によって登録された仮想経路に対応する対応経路が、経路決定手段２２３０によって決定される（ステップＳ２０３)。例えば、ＶＰＮ２０２０に対応するリンク４１４４が追加されたとき、表５に示すような対応経路から表３に示すような対応経路に変更され決定される。ここで、仮想リンク帯域情報提供手段２１６０が、ＶＰＮ２０２０を管理するカスタマ装置２０２９に仮想リンク帯域情報を提供するイメージの一例は、図１９Ｂ１に示される。

以上説明したように、本発明の第４の実施の形態に係る仮想専用網管理装置２２００および仮想専用網提供システム２０００は、仮想網提供網２０４０内のデータ転送経路の経路変更を検出するため、仮想専用網の運用中に経路変更がなされても、カスタマ装置２０１９，２０２９，２０３９に正確な仮想リンク帯域を表す情報を提供することができる。また、リンク４１４２，４１４４，４２４３，４３４４，４４４５の削除に応じて、仮想網提供網２０４０内のデータ転送経路の経路変更を検出するため、仮想専用網の運用中に経路変更がなされても、カスタマ装置２０１９，２０２９，２０３９に正確にリンク帯域を表す情報を提供することができる。また、リンクの追加に応じて、仮想網提供網２０４０内のデータ転送経路の経路変更を検出するため、仮想専用網の運用中に経路変更がなされても、カスタマ装置２０１９，２０２９，２０３９に正確なリンク帯域を表す情報を提供することができる。

図２４は、本発明の第５の実施の形態に係る仮想専用網提供システムのシステム構成図である。以下、仮想専用網をＶＰＮと表す。

図２４に示すように、ＶＰＮ提供システム３０００は、仮想専用網管理装置２３００、ＶＰＮを提供する仮想網提供網２０４０、ＶＰＮ２０１０、ＶＰＮ２０２０、およびＶＰＮ２０３０を含むように構成される。例えば、ＶＰＮ２０１０、ＶＰＮ２０２０、およびＶＰＮ２０３０は、インターネット接続業者などに提供されるネットワークである。なお、本発明の第５の実施の形態に係るＶＰＮ提供システム３０００を構成する要素のうち、図１７に示した本発明の第３の実施の形態に係るＶＰＮ提供システム１０００を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

図２５は、本発明の第５の実施の形態に係る仮想専用網管理装置のブロック構成図である。図２５に示すように、仮想専用網管理装置２３００は、リンク帯域格納手段２１１０、仮想経路登録手段２１２０、経路決定手段２１３０、仮想リンク帯域割当手段２３５０、仮想リンク帯域情報提供手段２３６０、表示手段２３７０および使用帯域情報受信手段２３９０を含むように構成される。なお、本発明の第５の実施の形態に係る仮想専用網管理装置２３００のうち、図１８に示した本発明の第３の実施の形態に係る仮想専用網管理装置２１００を構成する要素と同一の要素には同一の符号を付し、それぞれの説明を省略する。

使用帯域情報受信手段２３９０は、コネクションを確立させるための使用帯域情報を受信し、受信された使用帯域情報を仮想リンク帯域割当手段２３５０に出力するようになっている。

なお、使用帯域情報は、コネクションを確立させるために使用する帯域とコネクションが経由する仮想経路とを含む情報である。また、使用帯域情報受信手段２３９０は、使用帯域情報をカスタマ装置２０１９，２０２９，２０３９から受信してもよいし、ＶＰＮ２０１０，２０２０，２０３０内のデータ転送装置２０１１～２０１３，２０２１，２０２２，２０３１，２０３２から受信してもよい。

仮想リンク帯域割当手段２３５０には、経路決定手段２１３０によって出力された対応経路情報が入力され、仮想リンク帯域割当手段２３５０は、仮想経路登録手段２１２０から仮想リンク帯域を取得し、当該取得した仮想リンク帯域を対応経路に割当てるようになっている。また、仮想リンク帯域割当手段２３５０には、使用帯域情報受信手段２３９０によって出力された使用帯域情報が入力され、仮想リンク帯域割当手段２３５０は、当該使用帯域情報に含まれる仮想経路を抽出し、仮想経路から経路決定手段２１３０によって出力された対応経路を抽出し、対応経路に対して、使用帯域情報に含まれる使用帯域を割当てるようになっている。また、使用帯域が仮想リンク帯域を超えているか否かを判断し、使用帯域が仮想リンク帯域を超えたときには、コネクションの確率を拒否するようにしてもよい。

例えば、ＶＰＮ１０には、リンク４１４２およびリンク４２４３を経由し、２Ｍｂｉｔ／ｓを使用するコネクションが確立しているとした場合、仮想リンク帯

域割当手段２３５０は、2Ｍｂｉｔ／ｓを割当てる。また、ＶＰＮ２０２０には、リンク４１４４およびリンク４４４５を経由し、３Ｍｂｉｔ／ｓを使用するコネクションが確立しているとした場合、仮想リンク帯域割当手段２３５０は、３Ｍｂｉｔ／ｓを割当てる。ここで、仮想リンク帯域割当手段２３５０が割当てた仮想リンク帯域情報および使用帯域情報の一例を表６に示す。

表６

仮想経路	対応経路	仮想リンク帯域	使用帯域
V2011	リンク4142	１０	2
V2012	リンク4243	１０	2
V2021	リンク4144, およびリンク4445	１０	3
V2031	リンク4344, およびリンク4445	１０	1

仮想リンク帯域情報提供手段２３６０には、仮想リンク帯域割当手段２３５０によって出力された仮想リンク帯域情報および使用帯域情報が入力され、仮想リンク帯域情報提供手段２３６０は、入力された仮想リンク帯域情報および使用帯域情報をカスタマ装置２０１９，２０２９，２０３９に提供するようになっている。

仮想リンク帯域情報提供手段２３６０が、ＶＰＮ２０１０を管理するカスタマ装置２０１９に仮想リンク帯域情報および残余帯域情報を提供するイメージの一例を図２６Ａ１に示す。なお、残余帯域情報とは、仮想リンク帯域から使用帯域情報を差し引いた帯域を表す情報である。また、ＶＰＮ２０２０を管理するカスタマ装置２０２９に仮想リンク帯域情報および残余帯域情報を提供するイメージの一例を図２６Ｂ１に示す。また、ＶＰＮ２０３０を管理するカスタマ装置２０３９に仮想リンク帯域情報および残余帯域情報を提供するイメージの一例を図２６Ｃ１に示す。なお、括弧内の数値は、仮想リンク帯域を表す。例えば、図２６Ｂ１に示したように、仮想経路Ｖ２０２１は、仮想リンク帯域が１０Ｍｂｉｔ／ｓ、残余帯域が７Ｍｂｉｔ／ｓであることを示している。

表示手段２３７０には、仮想リンク帯域割当手段２３５０によって出力された仮想リンク帯域情報および使用帯域情報が入力され、表示手段２３７０は、入力

された仮想リンク帯域情報および使用帯域情報を自己の画面に表示するようになっている。

表示手段２３７０がＶＰＮ１０に関する仮想リンク帯域情報および残余帯域情報を表示するイメージの一例を図２６Ａ１に示す。また、ＶＰＮ２０２０に関する仮想リンク帯域情報および残余帯域情報を表示するイメージの一例を図２６Ｂ１に示す。また、ＶＰＮ３０に関する仮想リンク帯域情報および残余帯域情報を表示するイメージの一例を図２６Ｃ１に示す。

また、表示手段２３７０は、対応経路に関する仮想リンク帯域情報および残余帯域情報を自己の画面に表示するようにしてもよい。ＶＰＮ２０１０に関する対応経路の仮想リンク帯域情報および残余帯域情報を表示するイメージの一例を図２６Ａ２に示す。また、ＶＰＮ２０２０に関する対応経路の仮想リンク帯域情報および残余帯域情報を表示するイメージの一例を図２６Ｂ２に示す。また、ＶＰＮ２０３０に関する対応経路の仮想リンク帯域情報および残余帯域情報を表示するイメージの一例を図２６Ｃ２に示す。

例えば、図２６Ｂ２に示したように、データ転送装置２０４１とデータ転送装置２０４４との間のリンクは、仮想リンク帯域が１０Ｍｂｉｔ／ｓ、残余帯域が７Ｍｂｉｔ／ｓであり、データ転送装置２０４４とデータ転送装置２０４５との間のリンクは、仮想リンク帯域が１０Ｍｂｉｔ／ｓ、残余帯域が７Ｍｂｉｔ／ｓであることを示している。

以下、本発明の第５の実施の形態に係る仮想専用網管理装置の処理について、図面を参照して説明する。図２７は、本発明の第５の実施の形態に係る仮想専用網管理装置の処理の流れを示すフローチャートである。なお、本発明の第５の実施の形態に係る仮想専用網管理装置２３００の処理のうち、図２０に示した本発明の第３の実施の形態に係る仮想専用網管理装置２１００の処理と同一のものには同一符号を付し、それぞれの説明を省略する。また、ステップ１０１からステップ１０３までの処理は実施済みとして説明する。

まず、カスタマ装置２０１９，２０２９，２０３９などから送信された、コネクションを確立させるための使用帯域情報は、使用帯域情報受信手段２３９０によって受信され（ステップＳ３０１）、使用帯域は、仮想リンク帯域割当手段２３

５０によって対応経路に仮想リンク帯域と共に割当てられる(ステップＳ３０２)。

次に、割当てられた仮想リンク帯域情報および使用帯域情報は、仮想リンク帯域情報提供手段２３６０によって各カスタマ装置２０１９，２０２９，２０３９に、図２６Ａ１，２６Ｂ１，２６Ｃ１に示したイメージで提供される（ステップＳ３０３)。

以上説明したように、本発明の第５の実施の形態に係る仮想専用網管理装置２３００および仮想専用網提供システム３０００は、仮想リンク帯域情報および使用帯域情報をカスタマ装置２０１９，２０２９，２０３９に提供するため、カスタマ装置２０１９，２０２９，２０３９が使用帯域を把握しながら確実にコネクションを確立させることができる。

また、仮想専用網管理装置２１００，２２００，２３００が有するリンク帯域格納手段２１１０、仮想経路登録手段２１２０、経路決定手段２１３０，２２３０、仮想リンク帯域割当手段２１５０，２３５０、仮想リンク帯域情報提供手段２１６０，２３６０、表示手段２１７０，２３７０、経路変更検出手段２２８０、リンク削除検出手段２２８１、リンク追加検出手段２２８２、および使用帯域情報受信手段２３９０は、個々の処理を実行するための要素であり、実際には、仮想専用網管理装置２１００，２２００，２３００は、これらの処理を実行するソフトウェアを組み込んだコンピュータによってそれぞれ構成される。このソフトウェアは、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピィーディスク、ハードディスク等)、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等)、半導体メモリなどの記憶媒体に格納して頒布することもできる。

産業上の利用の可能性

本発明によれば、高いスケーラビリティを実現しながら、ＶＰＮプロバイダ内部のネットワーク情報とカスタマ網のネットワーク情報とを、カスタマに提供することで、カスタマのパス設計を容易に実現可能とすることができる。

また、アドレス変換が可能となることから、カスタマごとに独立のアドレス設

計が可能となる。これは、実際には１つしか存在しない装置ＩＤやリンクＩＦ　ＩＤを、仮想的にＶＰＮごとに変えることができるため、カスタマ網内の装置やリンクＩＦ　ＩＤとアドレス重複が発生しても、網内装置や網内エッジ装置の装置ＩＤにＶＰＮごとに異なるアドレスを振ることで、アドレス重複を解決することができる。

また、本発明の仮想専用網管理装置および仮想専用網提供システムによれば、ＶＰＮに関する予め決められた仮想経路を登録し、登録された仮想経路に対応する対応経路に仮想リンク帯域を割当てるため、仮想網提供網内のＶＰＮにおけるデータ転送経路に関わらず、カスタマ装置に正確なリンク帯域を表す情報を提供することができる。

また，本発明によれば、カスタマにとって不要な情報の提供を省略して、リソース契約中の条件に必要な情報だけを明示して提示することができる。さらにパスサービスを提供するプロバイダにとっても、不必要な詳細な情報を提供してしまう弊害を回避する効果を実現することができる

請求の範囲

1．カスタマ毎に異なるネットワーク情報を提供し、カスタマのパス設定要求を契機に網内エッジ装置間にパスを設定するＶＰＮに設けられ、パス設定に用いる共通データベース（以下ＤＢと記す）と、この共通ＤＢにリンク情報を設定するリンク情報設定手段と、このリンク情報を他装置と自装置との間で交換するリンク情報交換手段と、このリンク情報交換に用いる制御情報の転送経路を決定する経路計算手段とを備えた網内エッジ装置としてのＶＰＮ通信制御装置において、

ＶＰＮ毎に異なるＤＢであるＶＰＮＤＢを生成するＶＰＮＤＢ生成手段と、

前記共通ＤＢ中のリンク情報を当該リンク情報が関わるＶＰＮ毎に分類して分類された各リンク情報にそれぞれＶＰＮを識別する情報であるＶＰＮＩＤを付与するＶＰＮＩＤ設定手段と、

前記共通ＤＢのＶＰＮＩＤが付与されたリンク情報から同一ＶＰＮＩＤのリンク情報を抜き出して該当するＶＰＮＤＢに格納するフィルタ手段と

を備えたことを特徴とするＶＰＮ通信制御装置。

2．他網内エッジ装置と前記リンク情報を交換するためのトンネルを生成するトンネル生成手段を備えた請求項１記載のＶＰＮ通信制御装置。

3．前記共通ＤＢの一部に前記ＶＰＮＤＢを備え、それぞれのＤＢの記録内容を識別するための識別情報を付与する手段を備えた請求項１記載のＶＰＮ通信制御装置。

4．前記経路計算手段に基づき決定された制御情報の転送経路を用いて他装置間で前記リンク情報を交換する手段を備えた請求項１記載のＶＰＮ通信制御装置。

5．自装置内のＶＰＮＤＢがいずれのＶＰＮに関するＶＰＮＤＢであるかを他装置に通知する手段と、

他装置の要求に応じて自装置内のＶＰＮＤＢの記録内容を当該他装置に転送する手段と

を備えた請求項１記載のＶＰＮ通信制御装置。

６．自装置がフィルタリング実施を行なう装置であるときには前記フィルタ手段によるフィルタリングを実施すると共に他装置に対して前記トンネル設定手段によりトンネルを設定する手段と、

他装置が前記フィルタ手段によるフィルタリングを実施しているときには当該他装置に対して前記トンネル設定手段によりトンネルを設定する手段と

を備えた請求項１記載のＶＰＮ通信制御装置。

７．自装置を識別する情報である自装置ＩＤとＶＰＮＩＤとを加算した値のハッシュ値が他装置を識別する情報である他装置ＩＤと前記ＶＰＮＩＤを加算した値のハッシュ値よりも大きいときには自装置がフィルタリングを実施する装置であると決定する手段を備えた請求項６記載のＶＰＮ通信制御装置。

８．カスタマエッジ装置から受信したリンク情報が自装置宛であるときにはカスタマ経路フラグをセットする手段と、

前記カスタマ経路フラグがセットされたリンク情報を抽出するカスタマリンク情報抽出手段と

を備え、

このカスタマリンク情報抽出手段によって抽出されたリンク情報を他網内エッジ装置に転送するときには前記カスタマ経路フラグをそのまま付与して転送し、このカスタマリンク情報抽出手段によって抽出されたリンク情報をカスタマエッジ装置に転送するときには前記カスタマ経路フラグを削除して転送する手段を備えた

請求項１記載のＶＰＮ通信制御装置。

９．カスタマエッジ装置からパス設定要求を受けて当該パス設定のためのリソースを確保すると共に当該パス設定要求に基づく次網内装置にパス設定要求を転送するシグナリング手段を備えた請求項１記載のＶＰＮ通信制御装置。

１０．請求項６または７記載のＶＰＮ通信制御装置を備えたネットワークであって、

前記フィルタ手段を備えた網内エッジ装置を唯一備えたことを特徴とするネットワーク。

１１．情報処理装置にインストールすることにより、その情報処理装置に、

カスタマ毎に異なるネットワーク情報を提供し、カスタマのパス設定要求を契機に網内エッジ装置間にパスを設定するＶＰＮに設けられ、パス設定に用いる共通ＤＢに相応する機能と、この共通ＤＢにリンク情報を設定するリンク情報設定機能と、このリンク情報を他装置と自装置との間で交換するリンク情報交換機能と、このリンク情報交換に用いる制御情報の転送経路を決定する経路計算機能とを備えた網内エッジ装置としてのＶＰＮ通信制御装置に相応する機能を実現させるプログラムにおいて、

ＶＰＮ毎に異なるＤＢであるＶＰＮＤＢに相応する機能を生成するＶＰＮＤＢ生成機能と、

前記共通ＤＢ中のリンク情報を当該リンク情報が関わるＶＰＮ毎に分類して分類された各リンク情報にそれぞれＶＰＮを識別する情報であるＶＰＮＩＤを付与するＶＰＮＩＤ設定機能と、

前記共通ＤＢのＶＰＮＩＤが付与されたリンク情報から同一ＶＰＮＩＤのリンク情報を抜き出して該当するＶＰＮＤＢに格納するフィルタ機能と

を実現させることを特徴とするプログラム。

１２．他網内エッジ装置と前記リンク情報を交換するためのトンネルを生成するトンネル生成機能を実現させる請求項１１記載のプログラム。

１３．前記共通ＤＢに相応する機能の一部に前記ＶＰＮＤＢに相応する機能を実現させ、それぞれのＤＢの記録内容を識別するための識別情報を付与する機能を実現させる請求項１１記載のプログラム。

１４．前記経路計算機能に基づき決定された制御情報の転送経路を用いて他装置間で前記リンク情報を交換する機能を実現させる請求項１１記載のプログラム。

１５．自装置内のＶＰＮＤＢがいずれのＶＰＮに関するＶＰＮＤＢであるかを他装置に通知する機能と、

他装置の要求に応じて自装置内のＶＰＮＤＢの記録内容を当該他装置に転送する機能と

を実現させる請求項１１記載のプログラム。

１６．自装置がフィルタリング実施を行なう装置であるときには前記フィルタ機能によるフィルタリングを実施すると共に他装置に対して前記トンネル設定機能によりトンネルを設定する機能と、

他装置が前記フィルタ機能によるフィルタリングを実施しているときには当該他装置に対して前記トンネル設定機能によりトンネルを設定する機能と

を実現させる請求項１１記載のプログラム。

１７．　自装置を識別する情報である自装置ＩＤとＶＰＮＩＤとを加算した値のハッシュ値が他装置を識別する情報である他装置ＩＤと前記ＶＰＮＩＤを加算した値のハッシュ値よりも大きいときには自装置がフィルタリングを実施する装置であると決定する機能を実現させる請求項１６記載のプログラム。

１８．カスタマエッジ装置から受信したリンク情報が自装置宛であるときにはカスタマ経路フラグをセットする機能と、

前記カスタマ経路フラグがセットされたリンク情報を抽出するカスタマリンク情報抽出機能と

を実現させ、

このカスタマリンク情報抽出機能によって抽出されたリンク情報を他網内エッジ装置に転送するときには前記カスタマ経路フラグをそのまま付与して転送し、

このカスタマリンク情報抽出機能によって抽出されたリンク情報をカスタマエッジ装置に転送するときには前記カスタマ経路フラグを削除して転送する機能を実現させる

請求項１１記載のプログラム。

１９．カスタマエッジ装置からパス設定要求を受けて当該パス設定のためのリソースを確保すると共に当該パス設定要求に基づく次網内装置にパス設定要求を転送するシグナリング機能を実現させる請求項１１記載のプログラム。

２０．請求項１１ないし１９のいずれかに記載のプログラムが記録された前記情報処理装置読み取り可能な記録媒体。

２１．カスタマエッジ装置から網内エッジ装置にリンク情報を渡すことで、カスタマごとに異なるネットワーク情報を提供し、カスタマのパス設定要求を契機にカスタマエッジ装置間にパスを設定するＶＰＮにおける通信制御装置であって、該網内エッジ装置に、装置間で詳細なリンク情報を交換するリンク情報交換手段と、ＶＰＮ　ＩＤを設定するＶＰＮ　ＩＤ設定手段と、他装置から送られたリンク情報にＶＰＮ　ＩＤを付与するＶＰＮ　ＩＤ付与手段と、ＶＰＮ　ＩＤが一致するリンク情報のみ抜き出すフィルタ手段とを設けることを特徴とする通信制御装置。

２２．請求項２１記載の通信制御装置において、前記リンク情報交換手段として、ＧＭＰＬＳ拡張ＯＳＰＦを用いることを特徴とする通信制御装置。

２３．請求項２１記載の通信制御装置において、前記リンク情報にカスタマに対応した複数のＶＰＮ　ＩＤを付与することを特徴とする通信制御装置。

２４．請求項２１記載の通信制御装置において、前記各手段に加え、ＶＰＮごとのリンクアドレスおよびノードアドレスを設定するＶＰＮアドレス設定手段と、

全ＶＰＮに共通のリンクアドレスおよびノードアドレスをＶＰＮごとのリンクアドレスおよびノードアドレスに変換するアドレス変換手段を追加して、備えることを特徴とする通信制御装置。

２５．カスタマごとに異なるネットワーク情報を提供し、カスタマのパス設定要求を契機にカスタマエッジ装置間にパスを設定するＶＰＮにおける通信制御方法において、網内エッジ装置はカスタマエッジ装置からリンク情報を渡されると、他ノードとリンク情報を交換し、ＶＰＮ　ＩＤを付与し、網内のリンク情報を保持し、カスタマエッジ装置に対して、該リンク情報をフィルタリングして、カスタマがＶＰＮ設定に必要な情報のみ提示することを特徴とする通信制御方法。

２６．通信制御装置を、網内エッジ装置に、装置間で詳細なリンク情報を交換するリンク情報交換手段と、ＶＰＮ　ＩＤを設定するＶＰＮ　ＩＤ設定手段と、他装置から送られたリンク情報にＶＰＮ　ＩＤを付与するＶＰＮ　ＩＤ付与手段と、ＶＰＮ　ＩＤが一致するリンク情報のみ抜き出すフィルタ手段として機能させるためのＶＰＮにおける通信制御用プログラム。

２７．請求項２６記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

２８．仮想専用網を個別管理するカスタマ装置に管理情報を提供するとともに、前記仮想専用網を提供する仮想網提供網を統括管理する仮想専用網管理装置において、前記仮想網提供網内のデータ転送経路からなる仮想経路を、仮想リンク帯域に対応させて登録する仮想経路登録手段と、前記仮想経路登録手段により登録された仮想経路に対応するデータ転送経路からなる対応経路を決定する経路決定手段と、前記経路決定手段により決定された対応経路に、前記仮想リンク帯域を割当てる仮想リンク帯域割当手段と、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報を、前記カスタマ装置に提供する仮想リンク帯域情報提供手段と、を備えたことを特徴とする仮想専用網管理装置。

２９．前記仮想専用網管理装置は、さらに、前記仮想網提供網内のデータ転送経路の経路変更を検出する経路変更検出手段を備え、該経路変更検出手段が経路変更を検出した場合には、前記経路決定手段が、前記仮想経路登録手段により登録された仮想経路に対応する対応経路を、前記経路変更検出手段により経路変更が検出されたデータ転送経路に基づいて決定し、前記仮想リンク帯域割当手段が、前記経路決定手段により決定された対応経路に、前記仮想リンク帯域を割当て、前記仮想リンク帯域情報提供手段が、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報を、前記カスタマ装置に提供する、ことを特徴とする請求項２８に記載の仮想専用網管理装置。

３０．前記経路変更検出手段は、前記データ転送経路を構成するリンクの削除に応じて、前記仮想網提供網内のデータ転送経路の経路変更を検出する、ことを特徴とする請求項２９に記載の仮想専用網管理装置。

３１．前記経路変更検出手段は、前記データ転送経路を構成するリンクの追加に応じて、前記仮想網提供網内のデータ転送経路の経路変更を検出する、ことを特徴とする請求項２または請求項３０に記載の仮想専用網管理装置。

３２．前記仮想専用網管理装置は、さらに、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報を自己の画面に表示する表示手段、を備えたことを特徴とする請求項２８に記載の仮想専用網管理装置。

３３．前記仮想専用網管理装置は、さらに、前記仮想網提供網内のデータ転送経路におけるコネクションを確立させるための使用帯域情報を受信する使用帯域情報受信手段を備え、前記仮想リンク帯域割当手段が、前記使用帯域情報受信手段により受信された使用帯域情報を前記対応経路に割当て、前記仮想リンク帯域情報提供手段が、前記仮想リンク帯域割当手段により割当てられた仮想リンク帯域に関する情報および使用帯域情報を、前記カスタマ装置に提供する、ことを特徴

とする請求項２８に記載の仮想専用網管理装置。

３４．請求項２８に記載の仮想専用網管理装置と、該仮想専用。網管理装置に対し管理情報を要求するカスタマ装置とを備え、前記仮想専用網管理装置が、前記カスタマ装置に仮想リンク帯域に関する情報を提供する、ことを特徴とする仮想専用網提供システム。

３５．前記仮想網提供網内のデータ転送経路におけるコネクションを確立させるための使用帯域情報を送信するカスタマ装置と、前記カスタマ装置により送信された使用帯域情報を受信する請求項３３に記載の仮想専用網管理装置とを備え、前記仮想専用網管理装置が、前記使用帯域情報を前記仮想リンク帯域と共に、前記対応経路に割当て、該割当てた仮想リンク帯域に関する情報および使用帯域情報を前記カスタマ装置に提供する、ことを特徴とする仮想専用網提供システム。

３６．仮想専用網を個別管理するカスタマ装置に管理情報を提供するとともに、前記仮想専用網を提供する仮想網提供網を統括管理するための処理をコンピュータに実行させるためのプログラムであって、前記仮想網提供網内のデータ転送経路からなる仮想経路を、仮想リンク帯域に対応させて登録するための処理と、前記仮想経路に対応するデータ転送経路からなる対応経路を決定するための処理と、前記対応経路に前記仮想リンク帯域を割当てるための処理と、前記割当てられた仮想リンク帯域に関する情報を、前記カスタマ装置に提供するための処理と、をコンピュータに実行させる仮想専用網管理プログラム。

３７．前記仮想専用網管理プログラムが、さらに、前記仮想網提供網内のデータ転送経路の経路変更を検出するための処理と、前記経路変更を検出した場合には、前記登録された仮想経路に対応する対応経路を、前記経路変更が検出されたデータ転送経路に基づいて決定するための処理と、前記決定された対応経路に、前記仮想リンク帯域を割当てるための処理と、前記割当てられた仮想リンク帯域に関する情報を、前記カスタマ装置に提供するための処理とを、コンピュータに実行

させる請求項３６に記載の仮想専用網管理プログラム。

３８．前記仮想専用網管理プログラムが、さらに、前記割当てられた仮想リンク帯域に関する情報を自己の画面に表示するための処理をコンピュータに実行させる請求項３６に記載の仮想専用網管理プログラム。

３９．前記仮想専用網管理プログラムが、さらに、前記仮想網提供網内のデータ転送経路におけるコネクションを確立させるための使用帯域情報を受信するための処理と、前記受信された使用帯域情報を前記対応経路に割当てるための処理と、前記割当てられた仮想リンク帯域に関する情報および使用帯域情報を、前記カスタマ装置に提供するための処理と、を実行させる請求項３６に記載の仮想専用網管理プログラム。

４０．請求項３６乃至請求項３９の何れかに記載の仮想専用網管理プログラムを記録した記録媒体。

FIG. 1

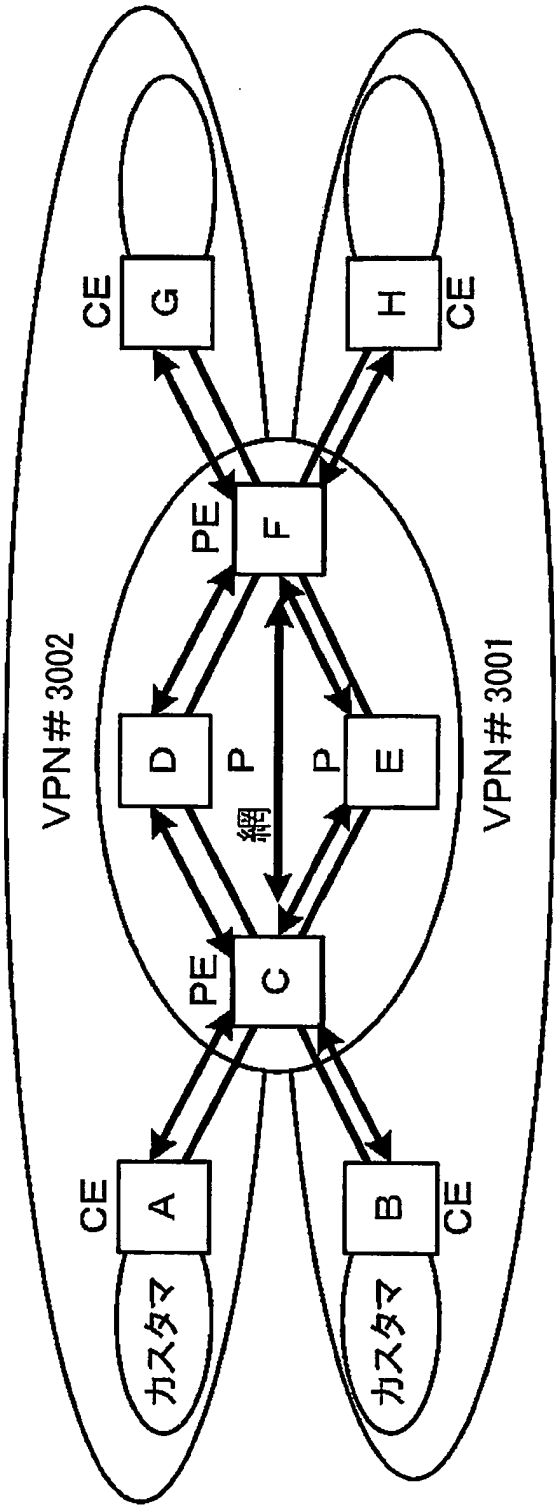


FIG. 2

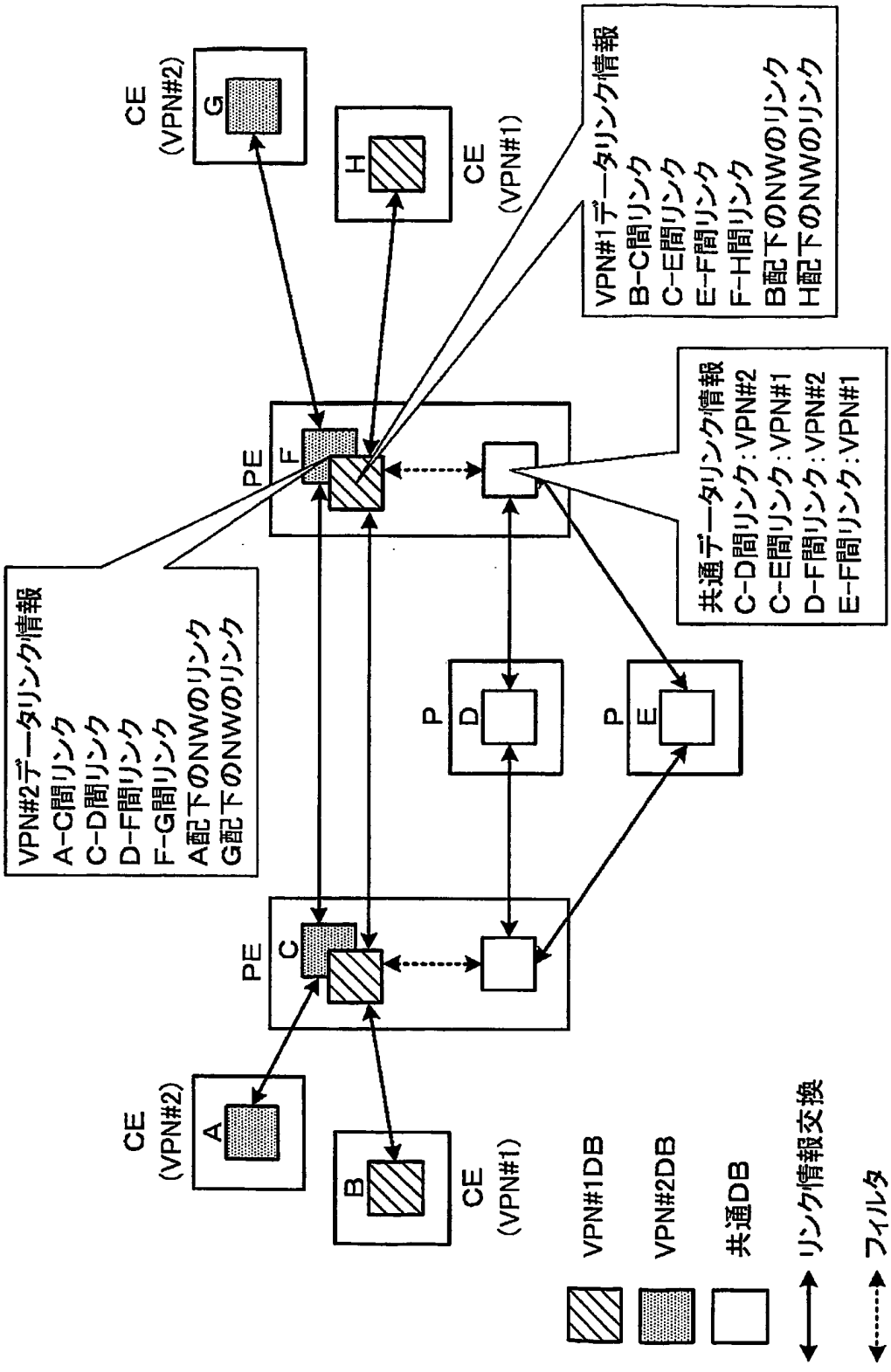

CE
(VPN#2)
A
CE
(VPN#1)
B
PE
C
P
D
P
E
PE
F
CE
(VPN#2)
G
CE
(VPN#1)
H
VPN#2データリンク情報
A-C間リンク
C-D間リンク
D-F間リンク
F-G間リンク
A配下のNWのリンク
G配下のNWのリンク
VPN#1データリンク情報
B-C間リンク
C-E間リンク
E-F間リンク
F-H間リンク
B配下のNWのリンク
H配下のNWのリンク
共通データリンク情報
C-D間リンク:VPN#2
C-E間リンク:VPN#1
D-F間リンク:VPN#2
E-F間リンク:VPN#1
VPN#1DB
VPN#2DB
共通DB
リンク情報交換
フィルタ

FIG. 3

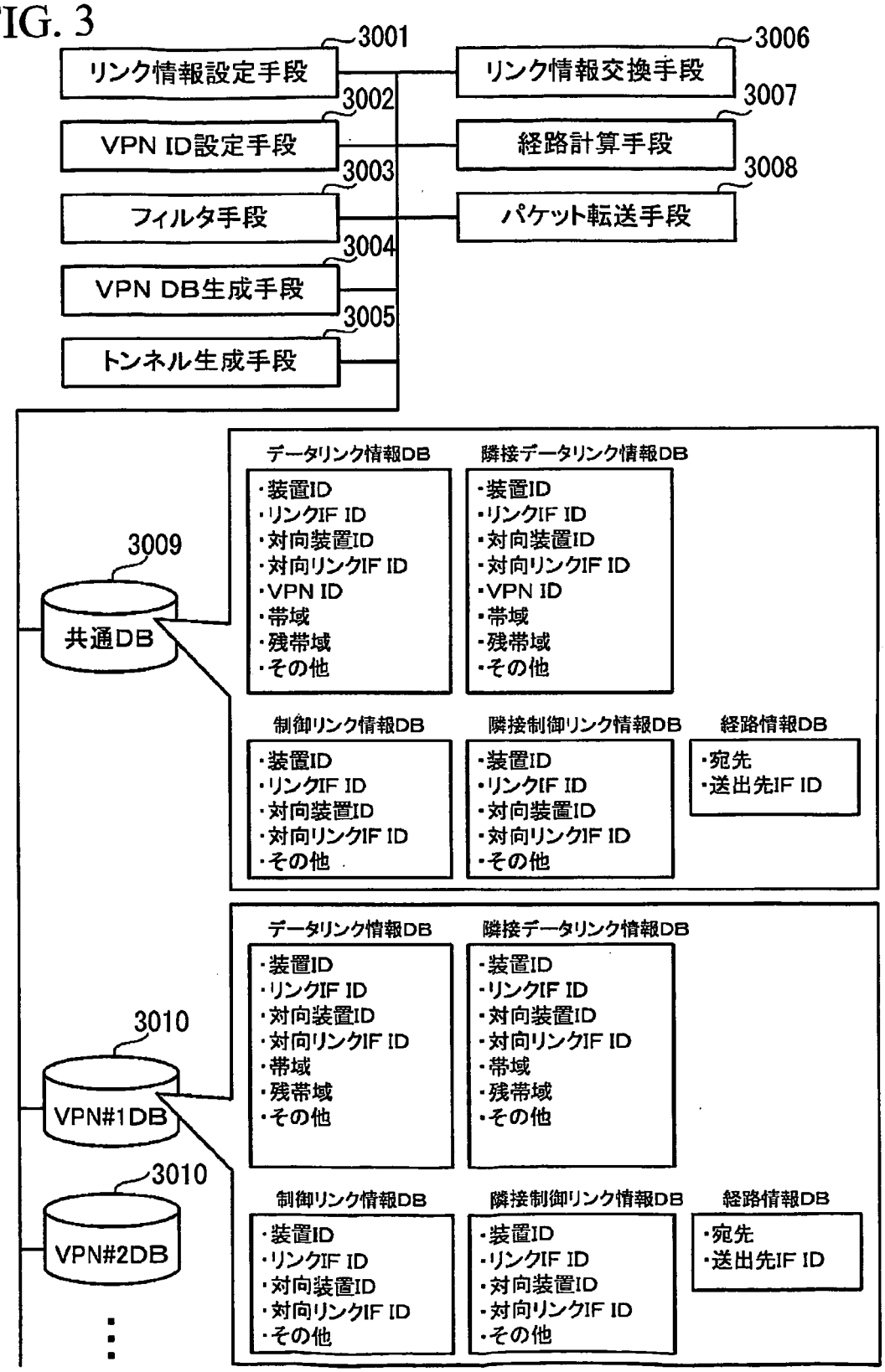

3001
リンク情報設定手段
3006
リンク情報交換手段
3002
VPN ID設定手段
3007
経路計算手段
3003
フィルタ手段
3008
パケット転送手段
3004
VPN DB生成手段
3005
トンネル生成手段
3009
共通DB
データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
隣接データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
隣接制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
経路情報DB
・宛先
・送出先IF ID
3010
VPN#1DB
3010
VPN#2DB
データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・帯域
・残帯域
・その他
隣接データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・帯域
・残帯域
・その他
制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
隣接制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
経路情報DB
・宛先
・送出先IF ID

FIG. 4

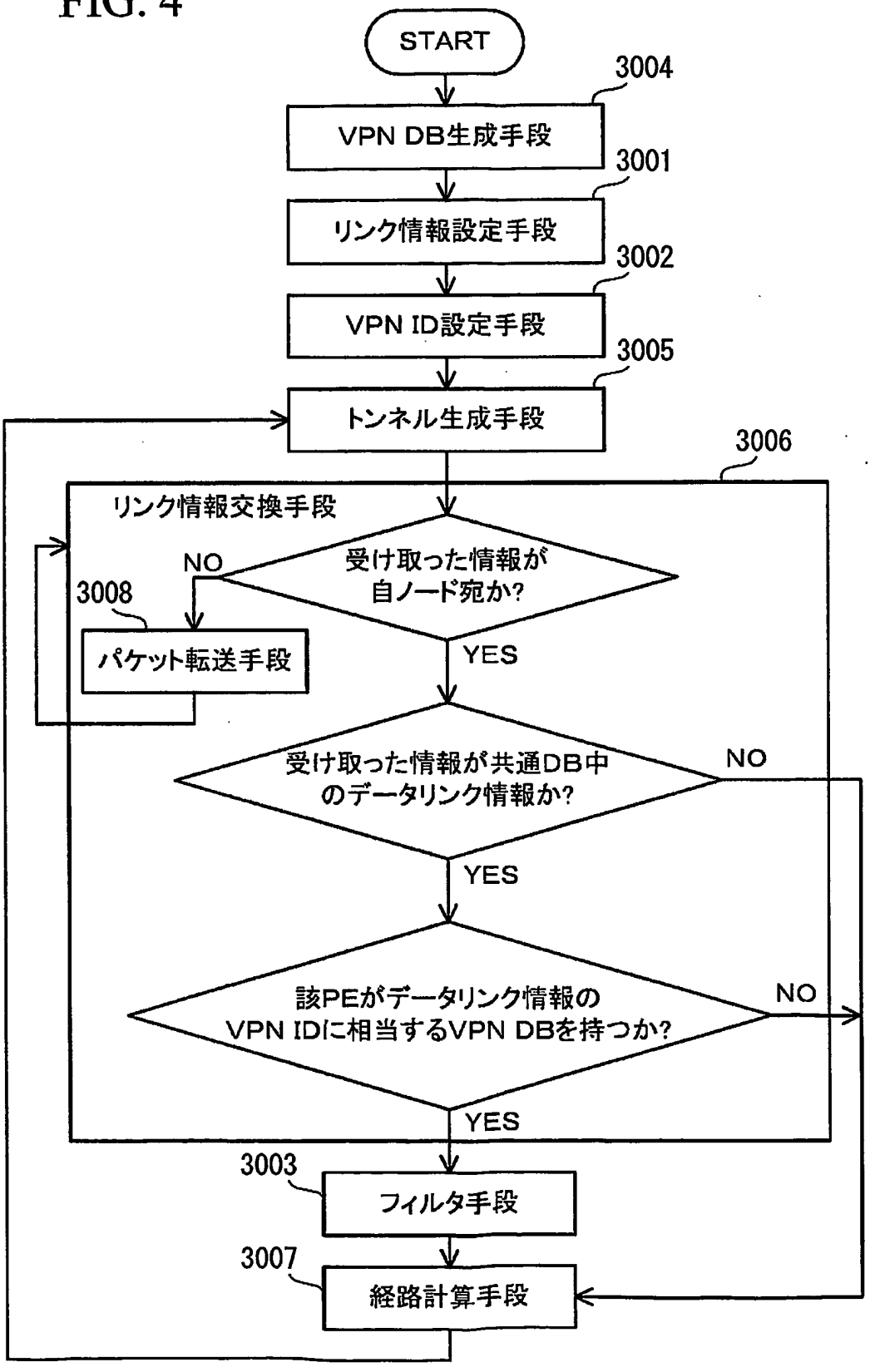

START
3004
VPN DB生成手段
3001
リンク情報設定手段
3002
VPN ID設定手段
3005
トンネル生成手段
3006
リンク情報交換手段
受け取った情報が
自ノード宛か?
NO
3008
パケット転送手段
YES
受け取った情報が共通DB中
のデータリンク情報か?
NO
YES
該PEがデータリンク情報の
VPN IDに相当するVPN DBを持つか?
NO
YES
3003
フィルタ手段
3007
経路計算手段

FIG. 5

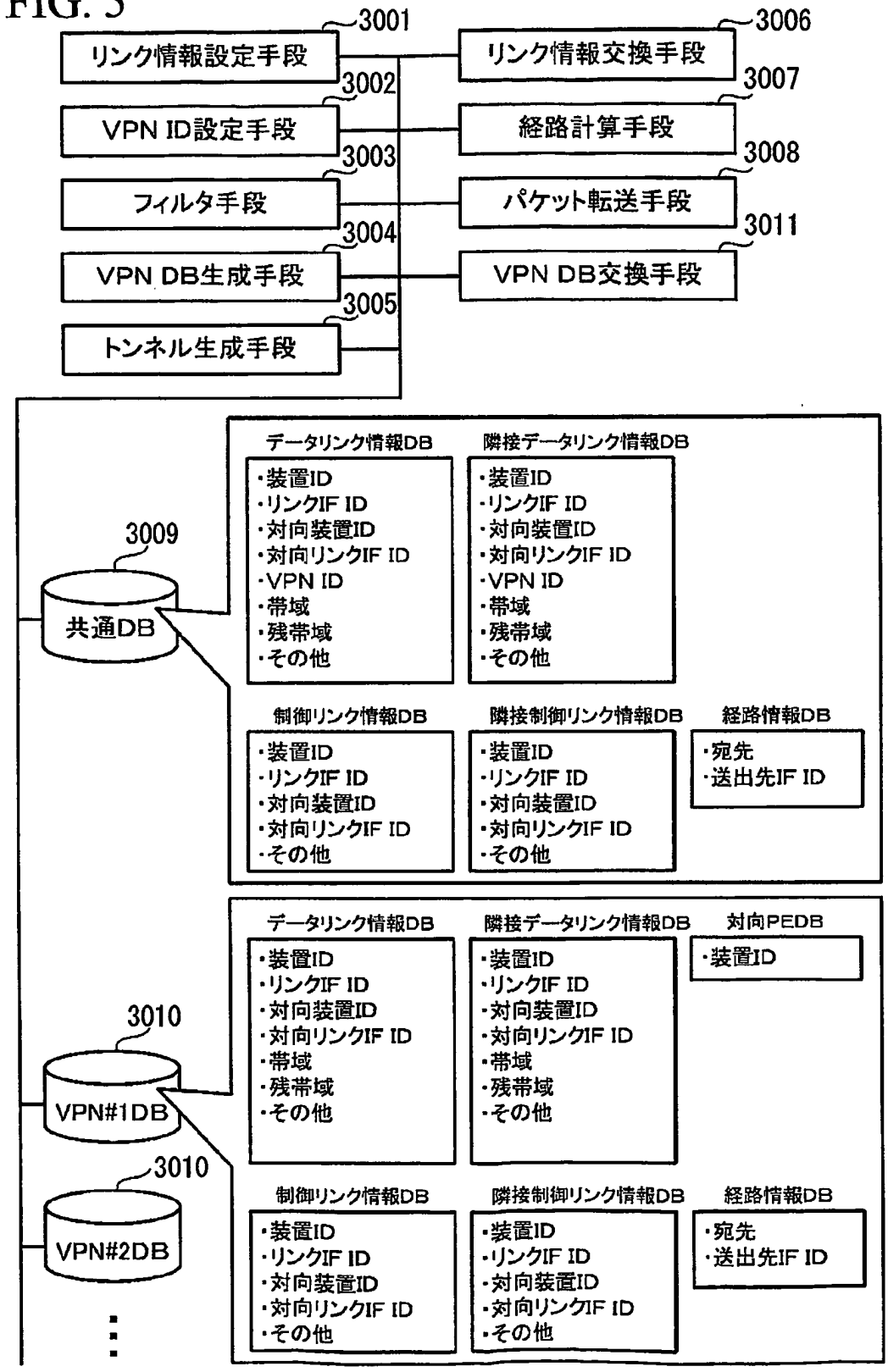

3001
リンク情報設定手段
3002
VPN ID設定手段
3003
フィルタ手段
3004
VPN DB生成手段
3005
トンネル生成手段
3006
リンク情報交換手段
3007
経路計算手段
3008
パケット転送手段
3011
VPN DB交換手段
3009
共通DB
データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
隣接データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
隣接制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
経路情報DB
・宛先
・送出先IF ID
3010
VPN#1DB
データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・帯域
・残帯域
・その他
隣接データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・帯域
・残帯域
・その他
対向PEDB
・装置ID
3010
VPN#2DB
制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
隣接制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
経路情報DB
・宛先
・送出先IF ID

FIG. 6

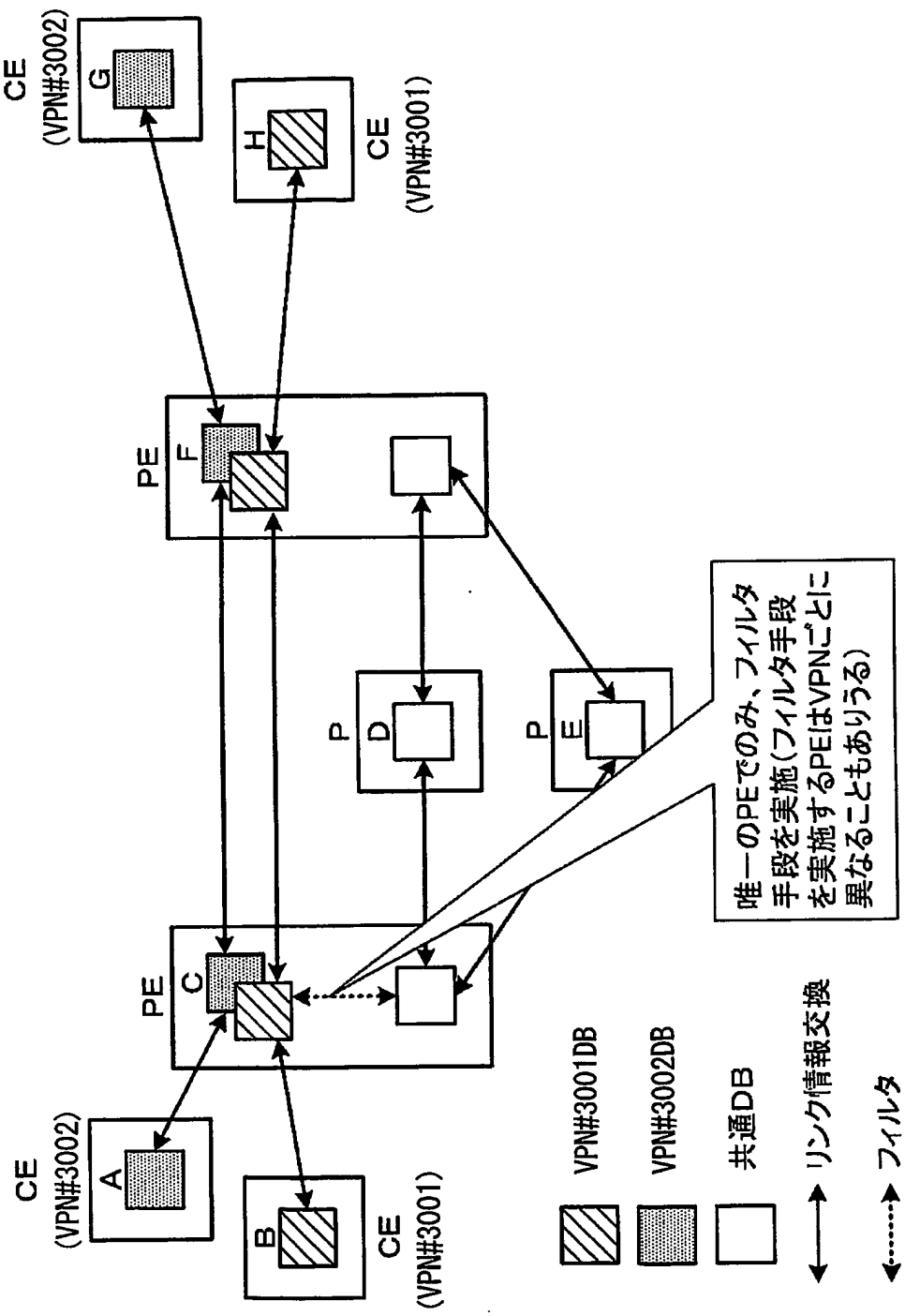

CE
(VPN#3002)
G
H
CE
(VPN#3001)
PE
F
P
D
P
E
PE
C
CE
(VPN#3002)
A
B
CE
(VPN#3001)
唯一のPEでのみ、フィルタ手段を実施(フィルタ手段を実施するPEはVPNごとに異なることもありうる)
VPN#3001DB
VPN#3002DB
共通DB
リンク情報交換
フィルタ

FIG. 7

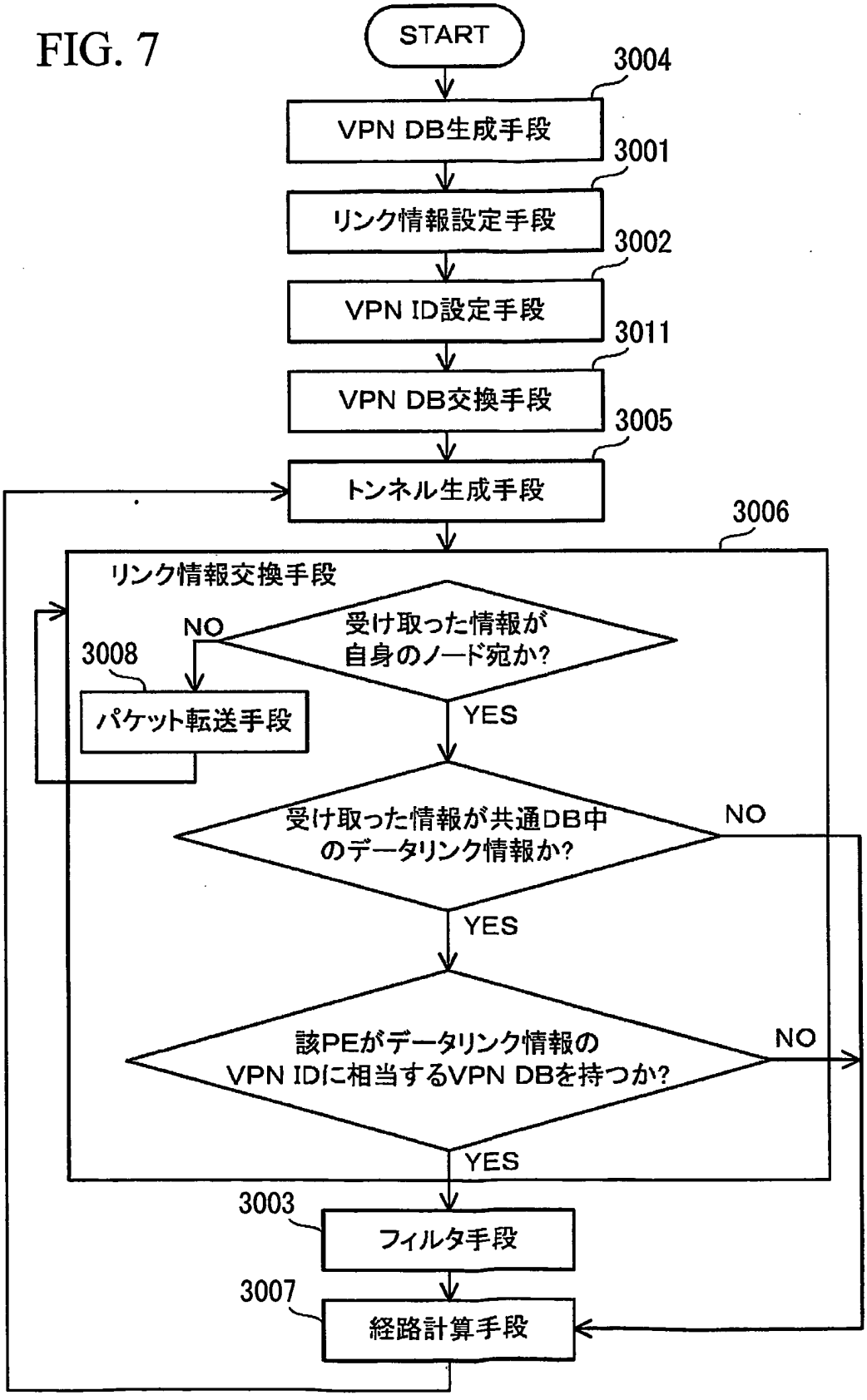

START
3004
VPN DB生成手段
3001
リンク情報設定手段
3002
VPN ID設定手段
3011
VPN DB交換手段
3005
トンネル生成手段
3006
リンク情報交換手段
NO
受け取った情報が
自身のノード宛か?
3008
パケット転送手段
YES
受け取った情報が共通DB中
のデータリンク情報か?
NO
YES
該PEがデータリンク情報の
VPN IDに相当するVPN DBを持つか?
NO
YES
3003
フィルタ手段
3007
経路計算手段

FIG. 8

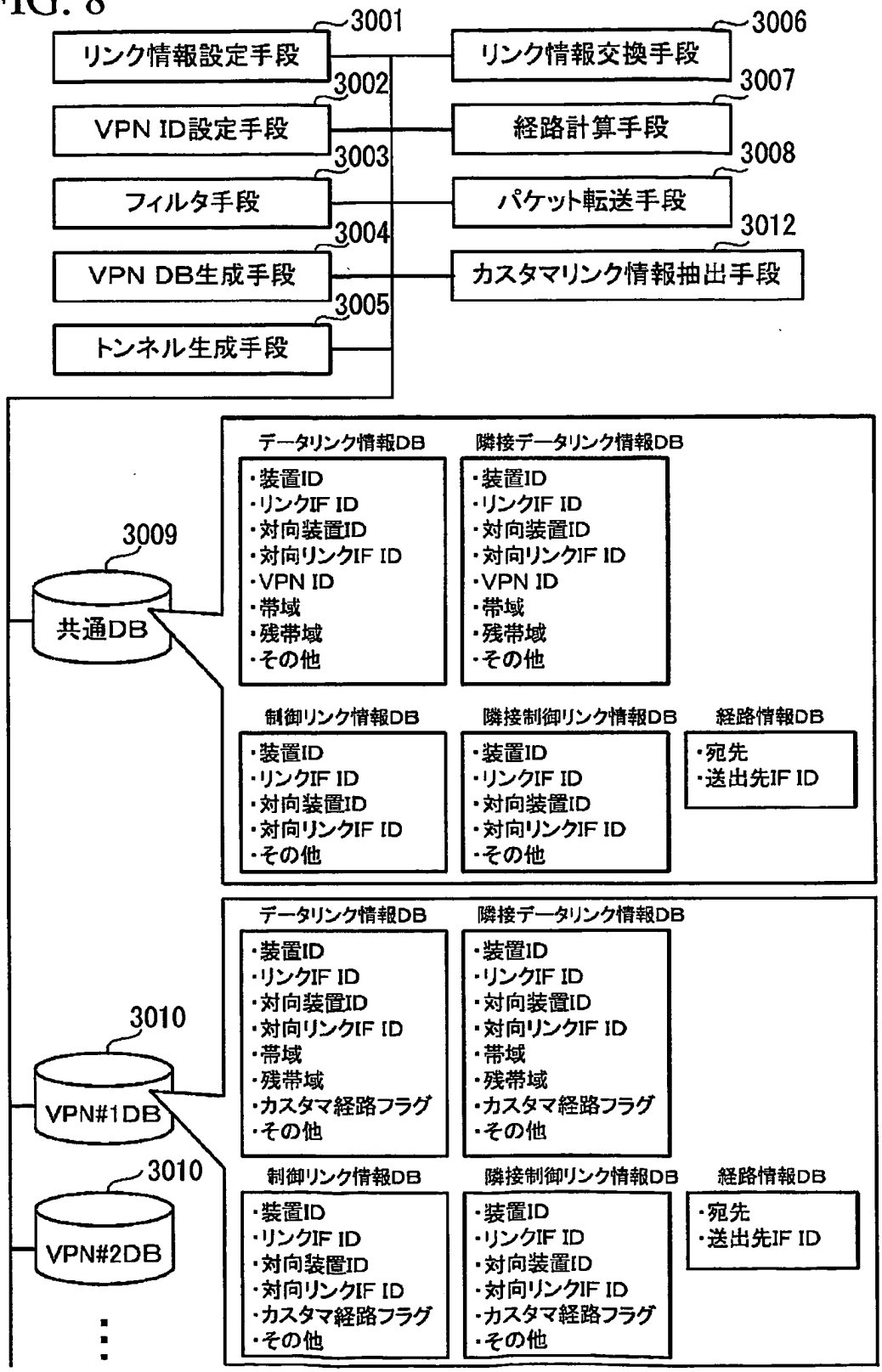

3001
リンク情報設定手段
3006
リンク情報交換手段
3002
VPN ID設定手段
3007
経路計算手段
3003
フィルタ手段
3008
パケット転送手段
3004
VPN DB生成手段
3012
カスタマリンク情報抽出手段
3005
トンネル生成手段
3009
共通DB
データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
隣接データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
隣接制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
経路情報DB
・宛先
・送出先IF ID
3010
VPN#1DB
データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・帯域
・残帯域
・カスタマ経路フラグ
・その他
隣接データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・帯域
・残帯域
・カスタマ経路フラグ
・その他
3010
VPN#2DB
制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・カスタマ経路フラグ
・その他
隣接制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・カスタマ経路フラグ
・その他
経路情報DB
・宛先
・送出先IF ID

FIG. 9

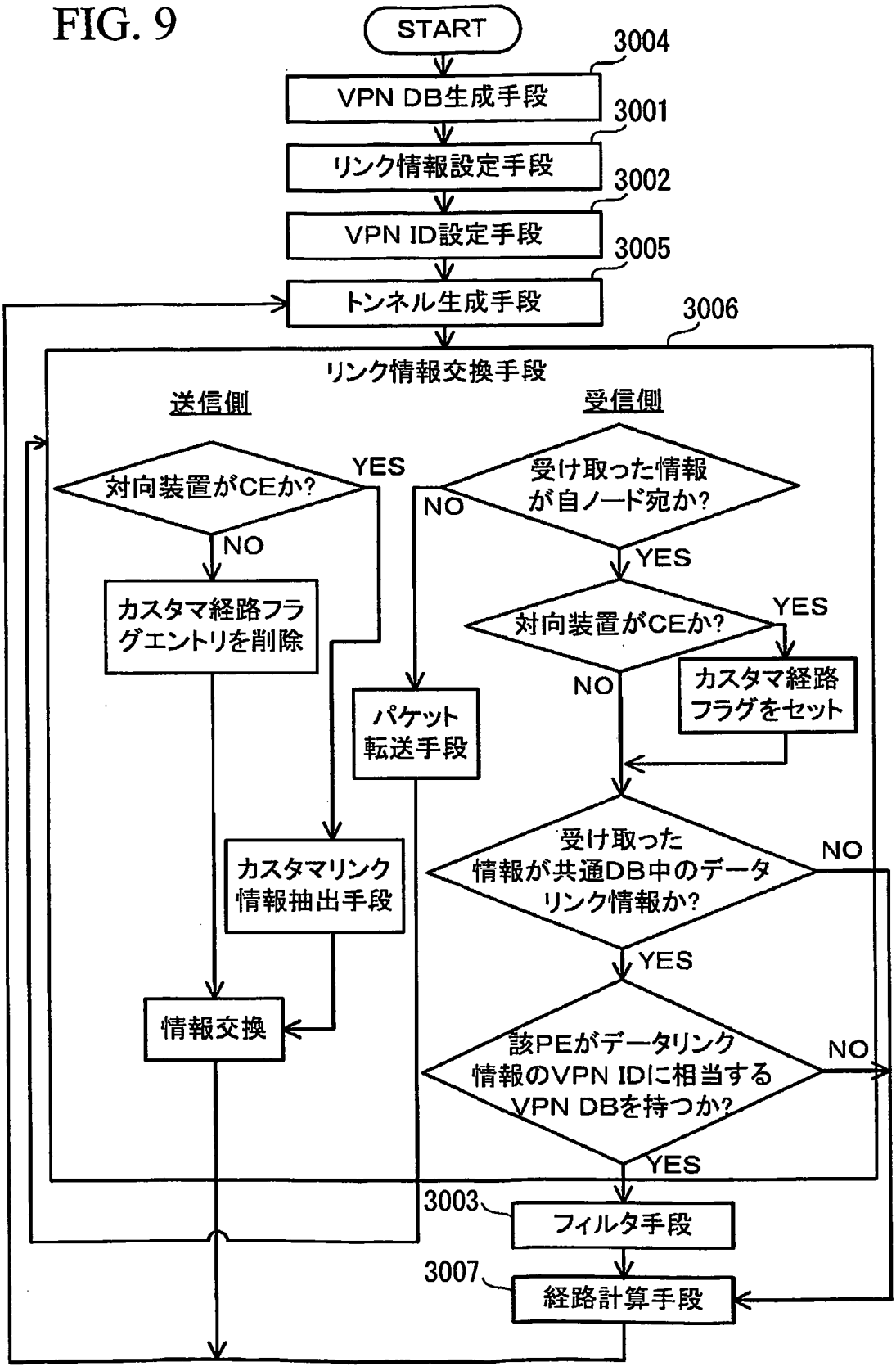

START
3004
VPN DB生成手段
3001
リンク情報設定手段
3002
VPN ID設定手段
3005
トンネル生成手段
3006
リンク情報交換手段
送信側
受信側
対向装置がCEか?
YES
NO
カスタマ経路フラグエントリを削除
受け取った情報が自ノード宛か?
NO
YES
対向装置がCEか?
YES
NO
カスタマ経路フラグをセット
パケット転送手段
カスタマリンク情報抽出手段
受け取った情報が共通DB中のデータリンク情報か?
NO
YES
情報交換
該PEがデータリンク情報のVPN IDに相当するVPN DBを持つか?
NO
YES
3003
フィルタ手段
3007
経路計算手段

FIG. 10

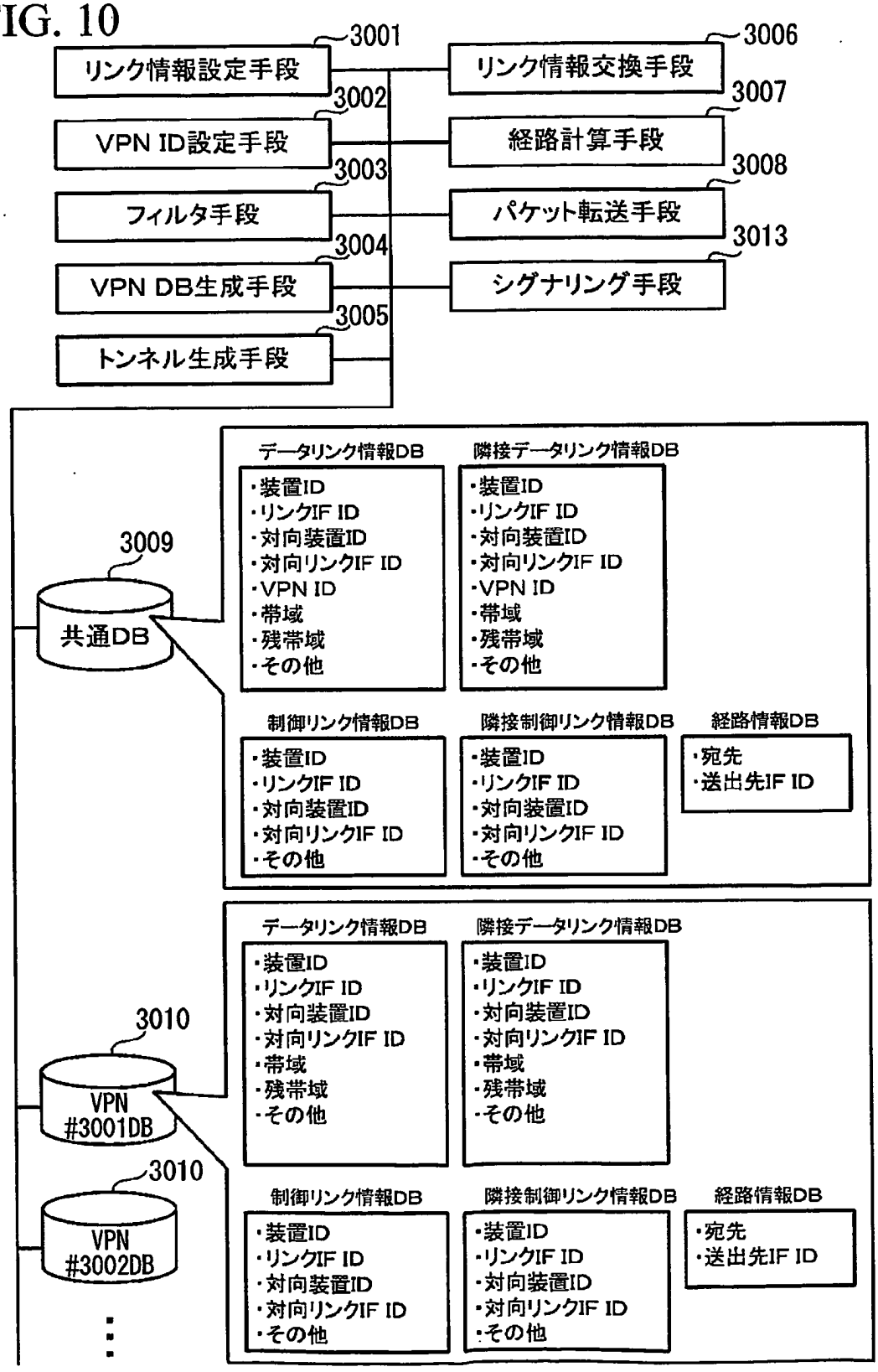

3001
リンク情報設定手段
3002
VPN ID設定手段
3003
フィルタ手段
3004
VPN DB生成手段
3005
トンネル生成手段
3006
リンク情報交換手段
3007
経路計算手段
3008
パケット転送手段
3013
シグナリング手段
3009
共通DB
データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
隣接データリンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
隣接制御リンク情報DB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・その他
経路情報DB
・宛先
・送出先IF ID
3010
VPN #3001DB
3010
VPN #3002DB

FIG. 11

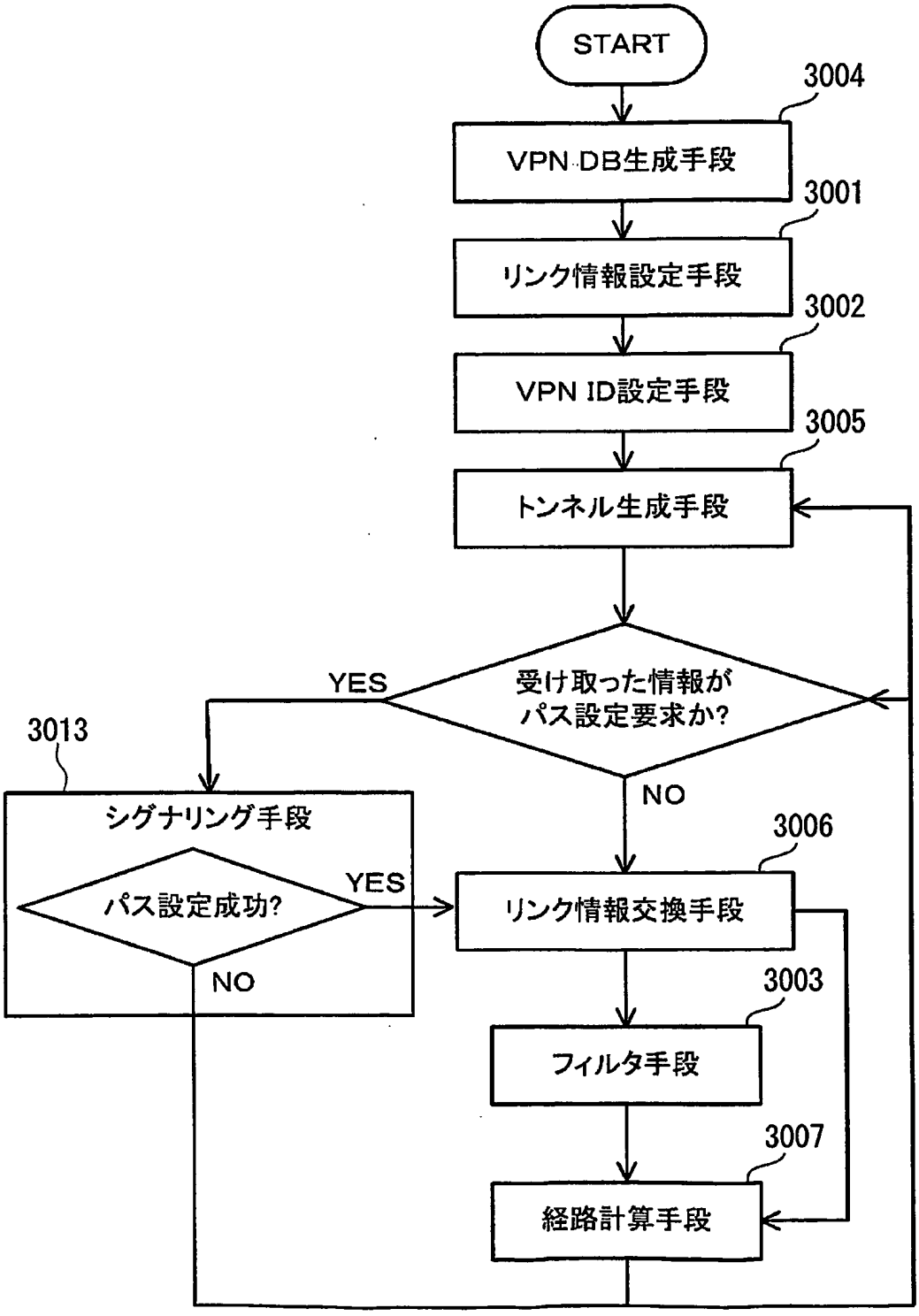

START
3004
VPN DB生成手段
3001
リンク情報設定手段
3002
VPN ID設定手段
3005
トンネル生成手段
受け取った情報が
パス設定要求か?
YES
NO
3013
シグナリング手段
パス設定成功?
YES
NO
3006
リンク情報交換手段
3003
フィルタ手段
3007
経路計算手段

FIG. 12

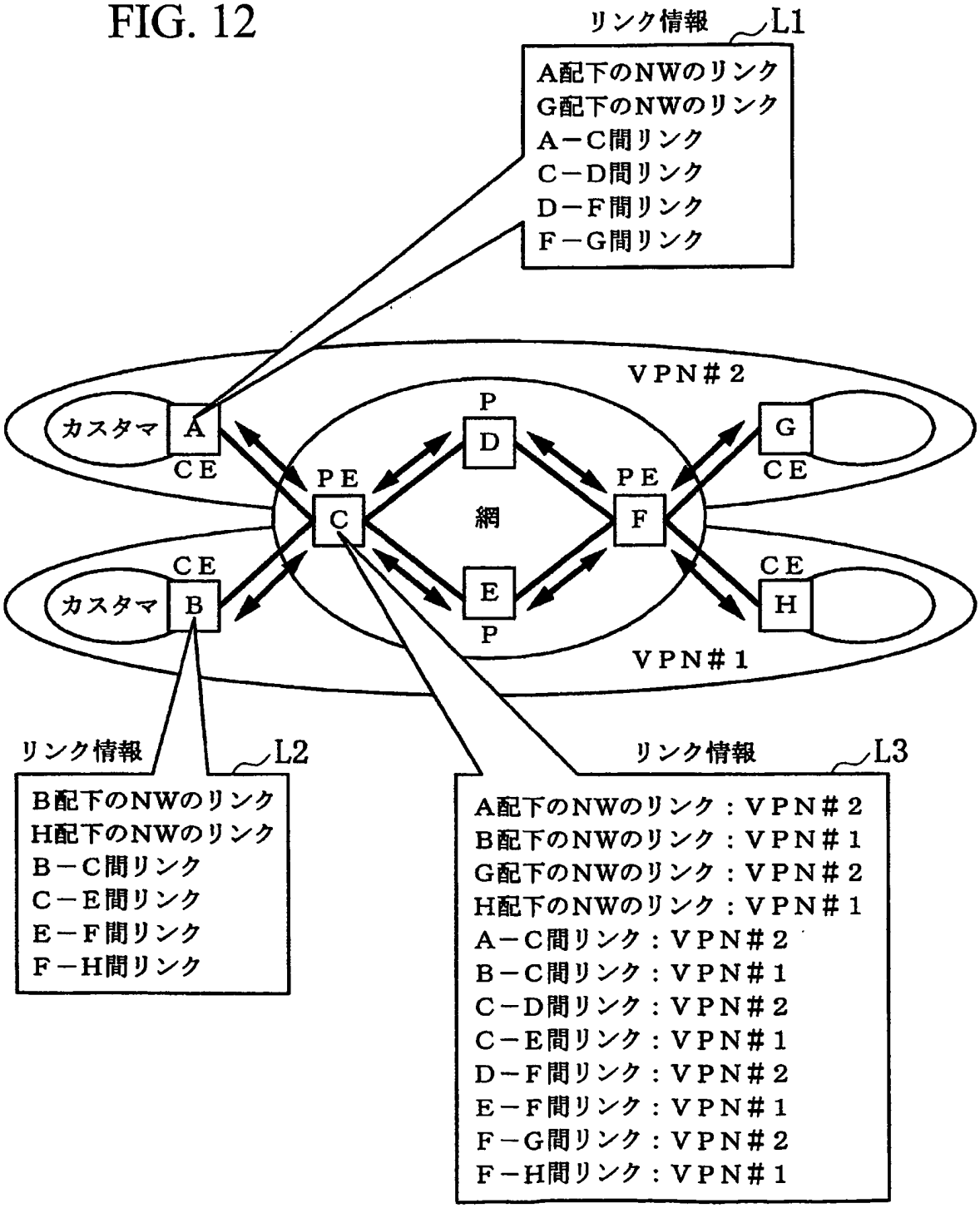

リンク情報
L1
A配下のNWのリンク
G配下のNWのリンク
A－C間リンク
C－D間リンク
D－F間リンク
F－G間リンク
VPN#2
カスタマ
A
CE
P
D
G
CE
PE
C
網
PE
F
CE
カスタマ
B
E
P
CE
H
VPN#1
リンク情報
L2
B配下のNWのリンク
H配下のNWのリンク
B－C間リンク
C－E間リンク
E－F間リンク
F－H間リンク
リンク情報
L3
A配下のNWのリンク：VPN#2
B配下のNWのリンク：VPN#1
G配下のNWのリンク：VPN#2
H配下のNWのリンク：VPN#1
A－C間リンク：VPN#2
B－C間リンク：VPN#1
C－D間リンク：VPN#2
C－E間リンク：VPN#1
D－F間リンク：VPN#2
E－F間リンク：VPN#1
F－G間リンク：VPN#2
F－H間リンク：VPN#1

FIG. 13

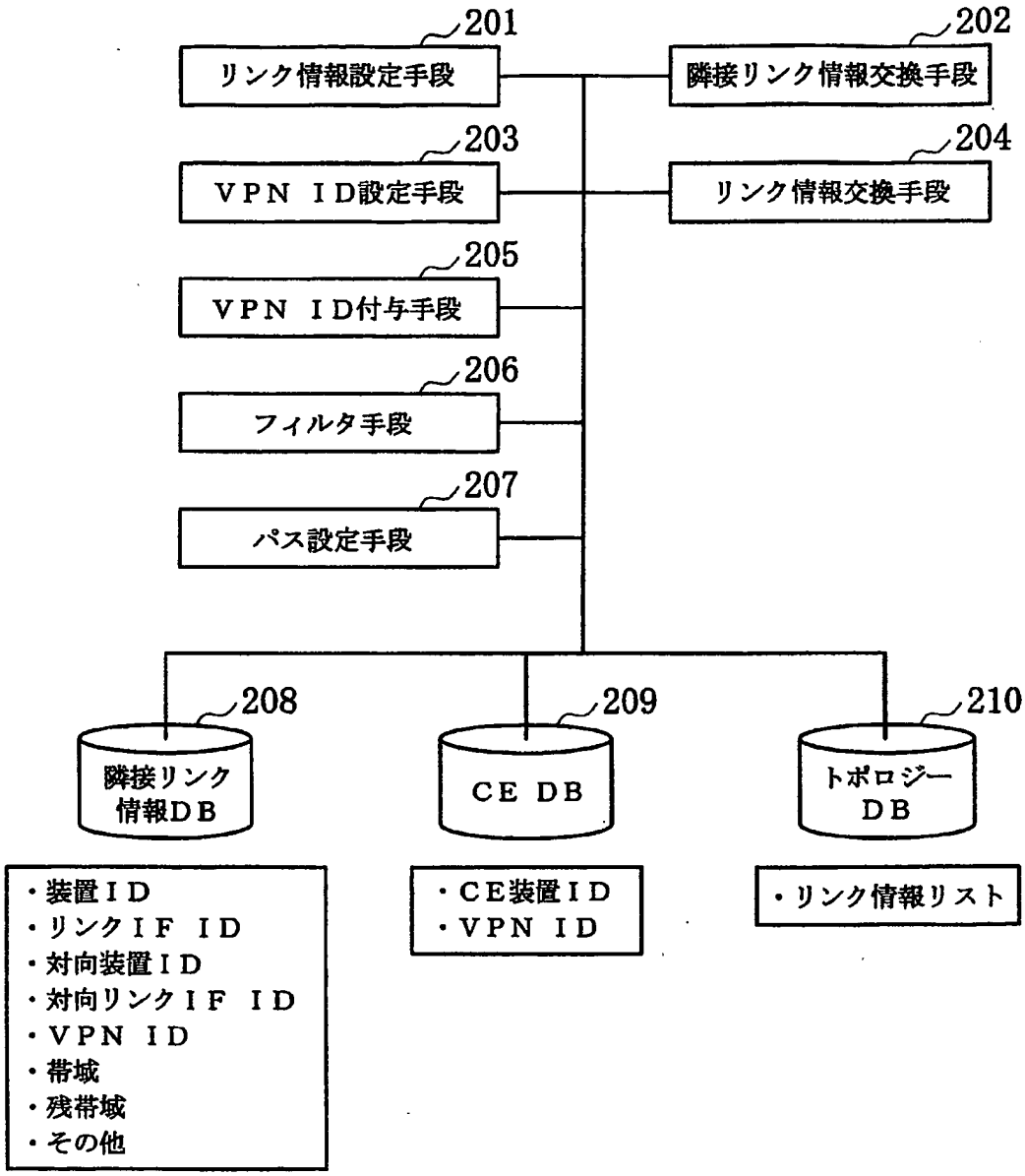

201
リンク情報設定手段
202
隣接リンク情報交換手段
203
VPN ID設定手段
204
リンク情報交換手段
205
VPN ID付与手段
206
フィルタ手段
207
パス設定手段
208
隣接リンク情報DB
209
CE DB
210
トポロジーDB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
・CE装置ID
・VPN ID
・リンク情報リスト

FIG. 14

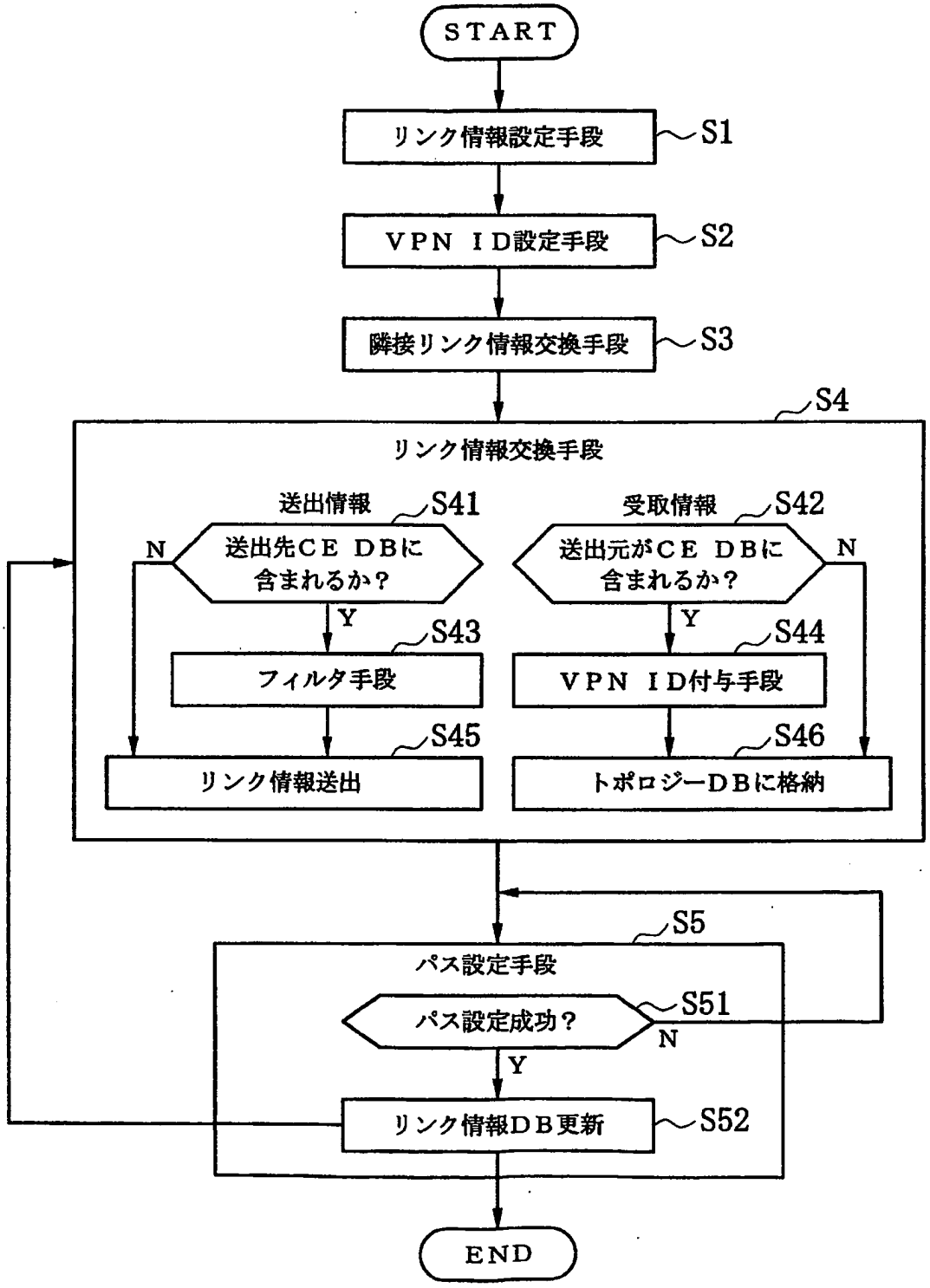

START
リンク情報設定手段
S1
VPN ID設定手段
S2
隣接リンク情報交換手段
S3
S4
リンク情報交換手段
送出情報
S41
送出先CE DBに含まれるか？
N
Y
S43
フィルタ手段
S45
リンク情報送出
受取情報
S42
送出元がCE DBに含まれるか？
N
Y
S44
VPN ID付与手段
S46
トポロジーDBに格納
S5
パス設定手段
パス設定成功？
S51
N
Y
リンク情報DB更新
S52
END

FIG. 15

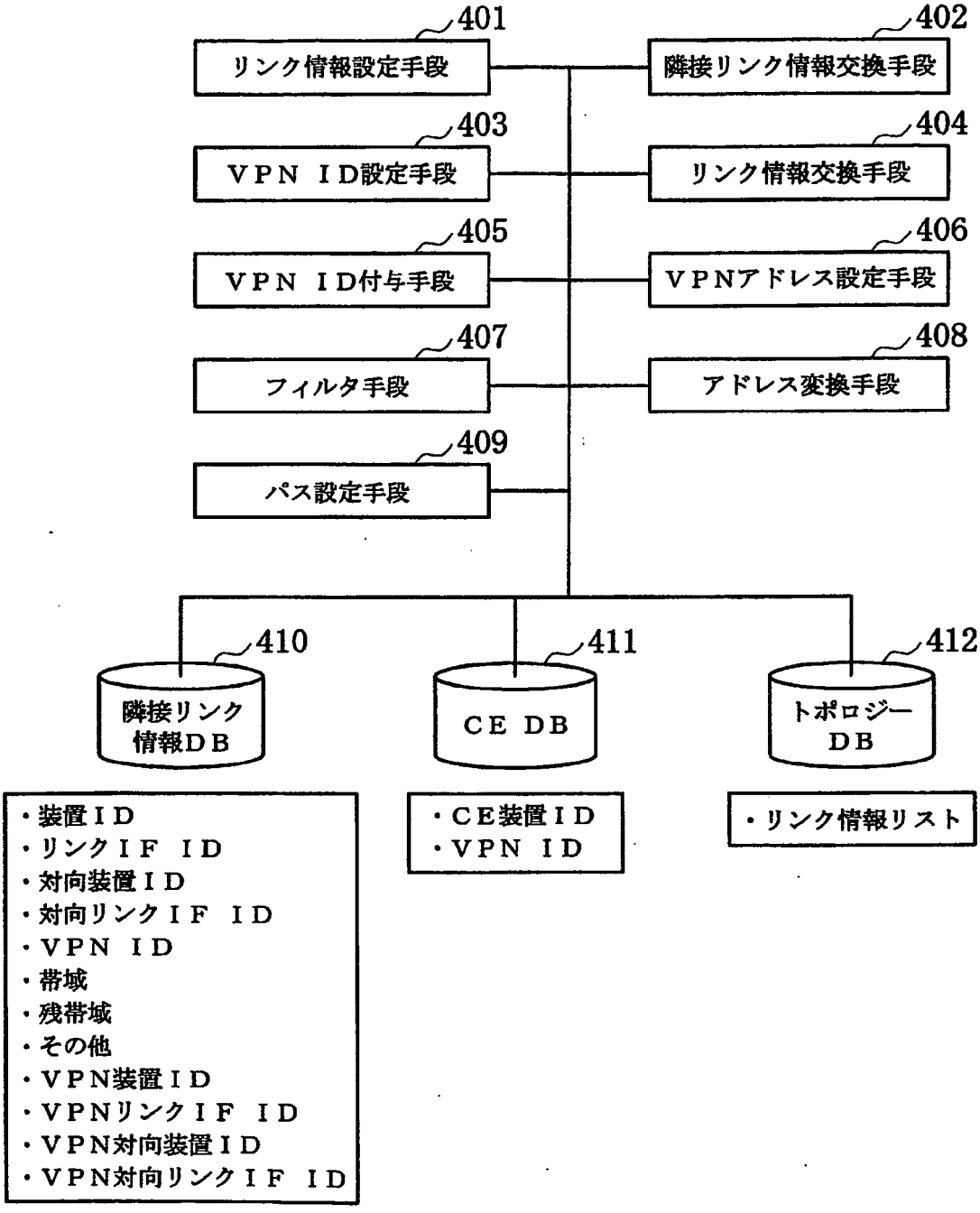

401
リンク情報設定手段
402
隣接リンク情報交換手段
403
VPN ID設定手段
404
リンク情報交換手段
405
VPN ID付与手段
406
VPNアドレス設定手段
407
フィルタ手段
408
アドレス変換手段
409
パス設定手段
410
隣接リンク情報DB
411
CE DB
412
トポロジーDB
・装置ID
・リンクIF ID
・対向装置ID
・対向リンクIF ID
・VPN ID
・帯域
・残帯域
・その他
・VPN装置ID
・VPNリンクIF ID
・VPN対向装置ID
・VPN対向リンクIF ID
・CE装置ID
・VPN ID
・リンク情報リスト

FIG. 16

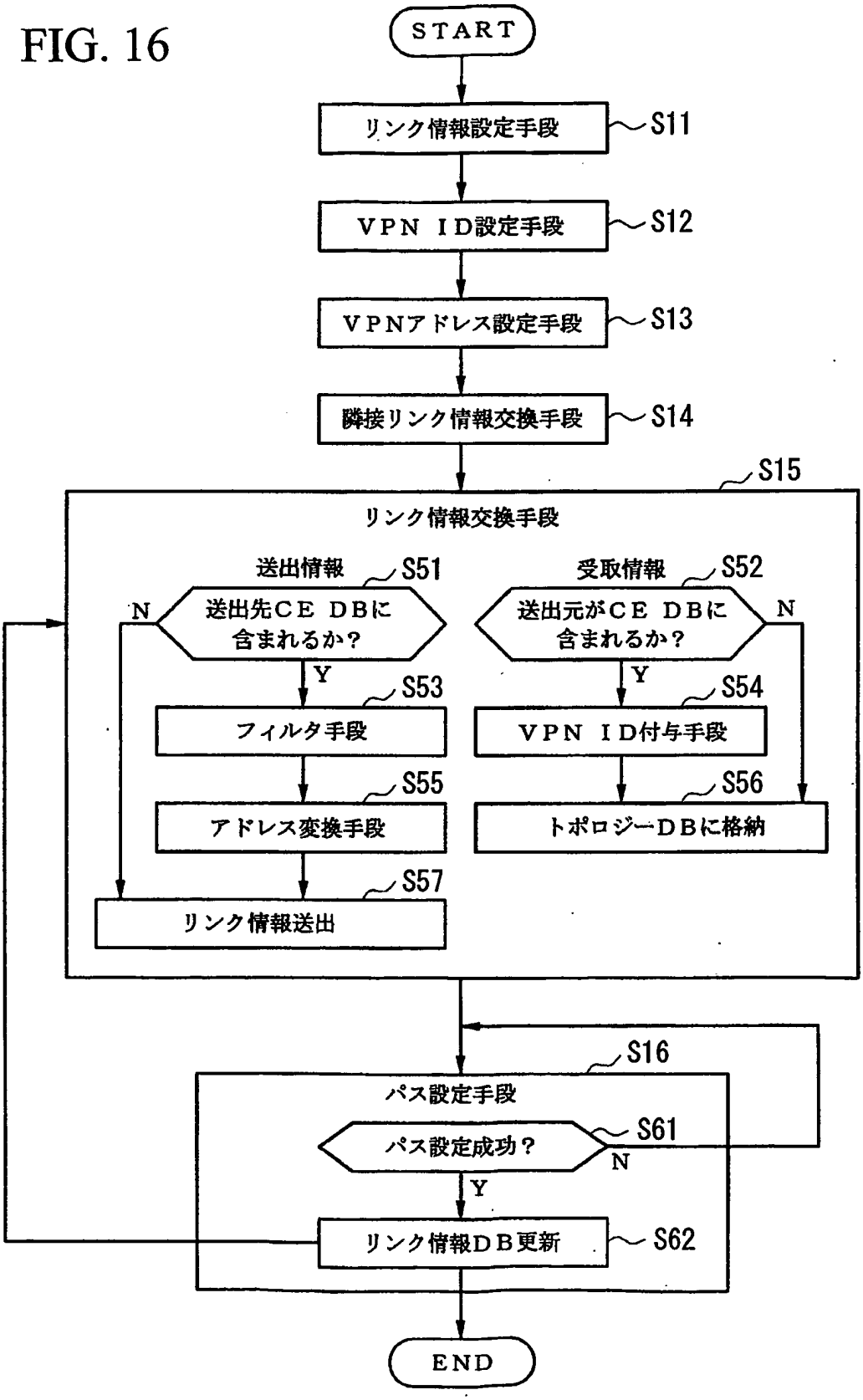

START
リンク情報設定手段
S11
VPN ID設定手段
S12
VPNアドレス設定手段
S13
隣接リンク情報交換手段
S14
S15
リンク情報交換手段
送出情報
S51
送出先CE DBに含まれるか？
N
Y
S53
フィルタ手段
S55
アドレス変換手段
S57
リンク情報送出
受取情報
S52
送出元がCE DBに含まれるか？
N
Y
S54
VPN ID付与手段
S56
トポロジーDBに格納
S16
パス設定手段
パス設定成功？
S61
N
Y
リンク情報DB更新
S62
END

FIG. 17

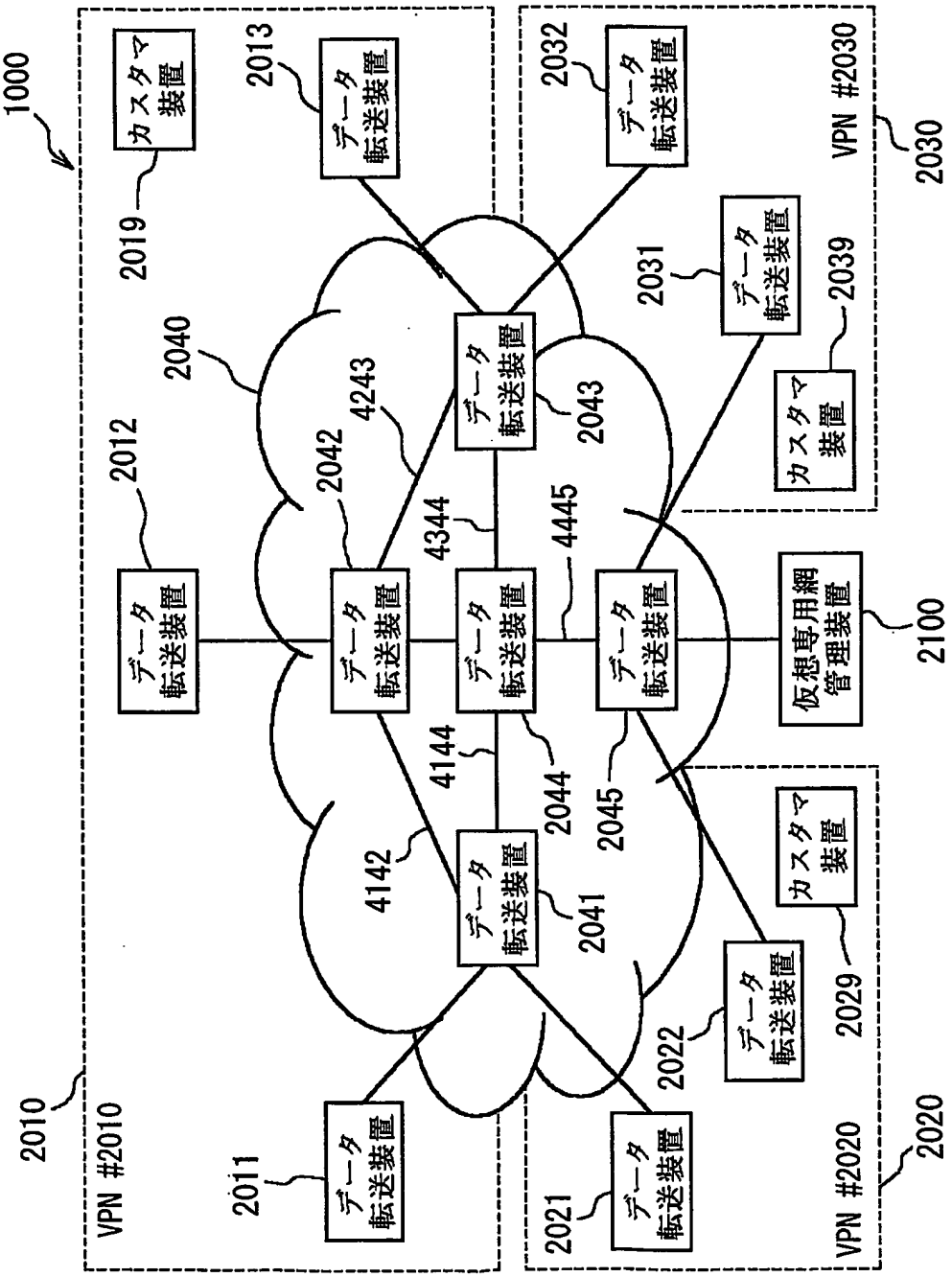

1000
2010
VPN #2010
2011
2012
2013
2019
2020
VPN #2020
2021
2022
2029
2030
VPN #2030
2031
2032
2039
2040
2041
2042
2043
2044
2045
2100
4142
4144
4243
4344
4445
データ転送装置
カスタマ装置
仮想専用網管理装置

FIG. 18

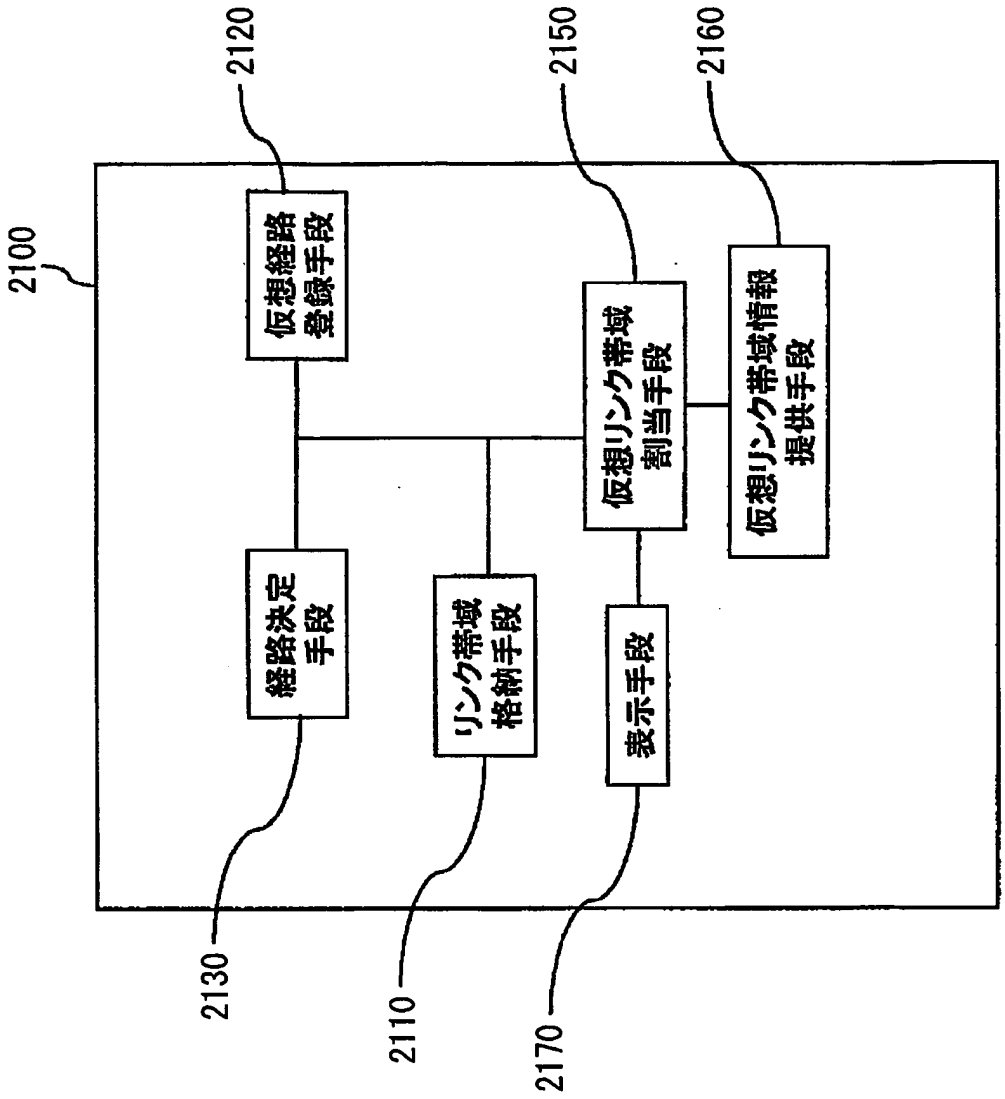
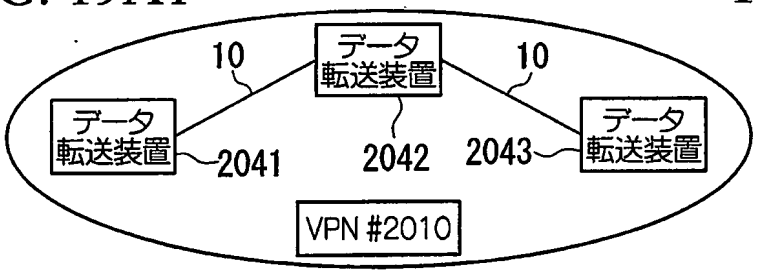
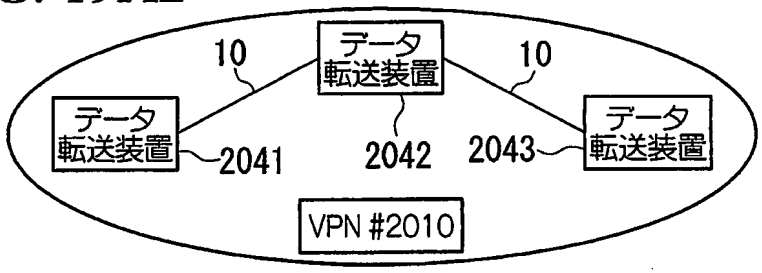

2100
2120
仮想経路登録手段
2150
仮想リンク帯域割当手段
2160
仮想リンク帯域情報提供手段
経路決定手段
リンク帯域格納手段
表示手段
2130
2110
2170

FIG. 19A1



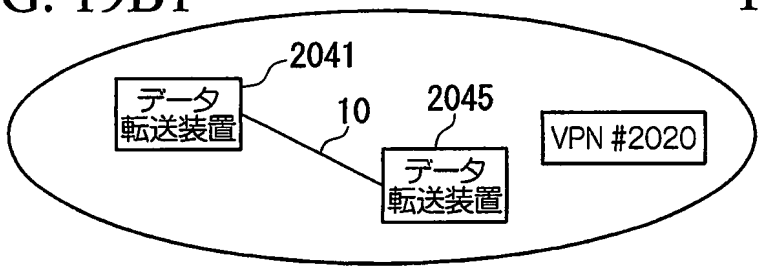
仮想リンク帯域をカスタマ装置に提供するイメージ

FIG. 19A2



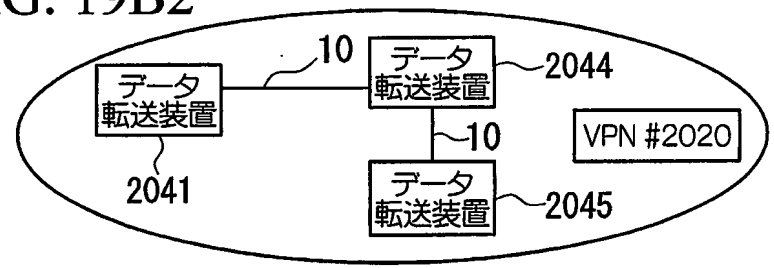
リンク帯域を表示するイメージ

FIG. 19B1



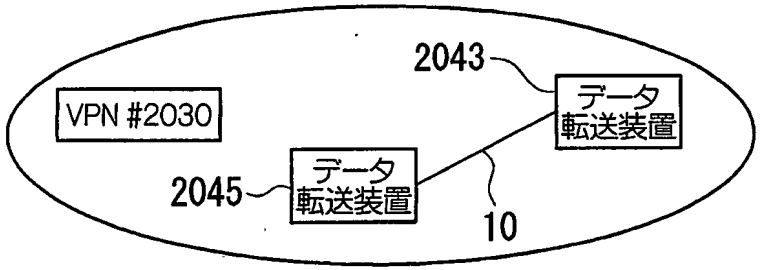
仮想リンク帯域をカスタマ装置に提供するイメージ

FIG. 19B2



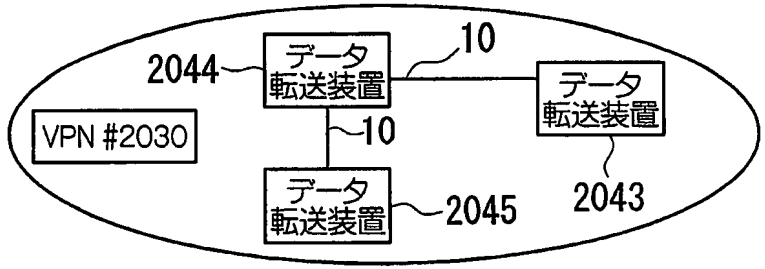
リンク帯域を表示するイメージ

FIG. 19C1



仮想リンク帯域をカスタマ装置に提供するイメージ

FIG. 19C2



リンク帯域を表示するイメージ

FIG. 20

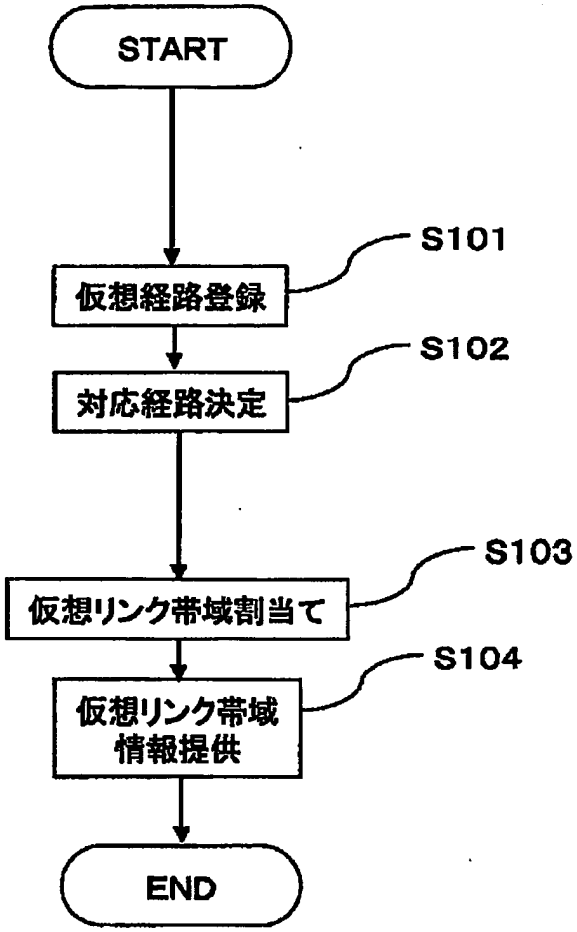

START
S101
仮想経路登録
S102
対応経路決定
S103
仮想リンク帯域割当て
S104
仮想リンク帯域
情報提供
END

FIG. 21

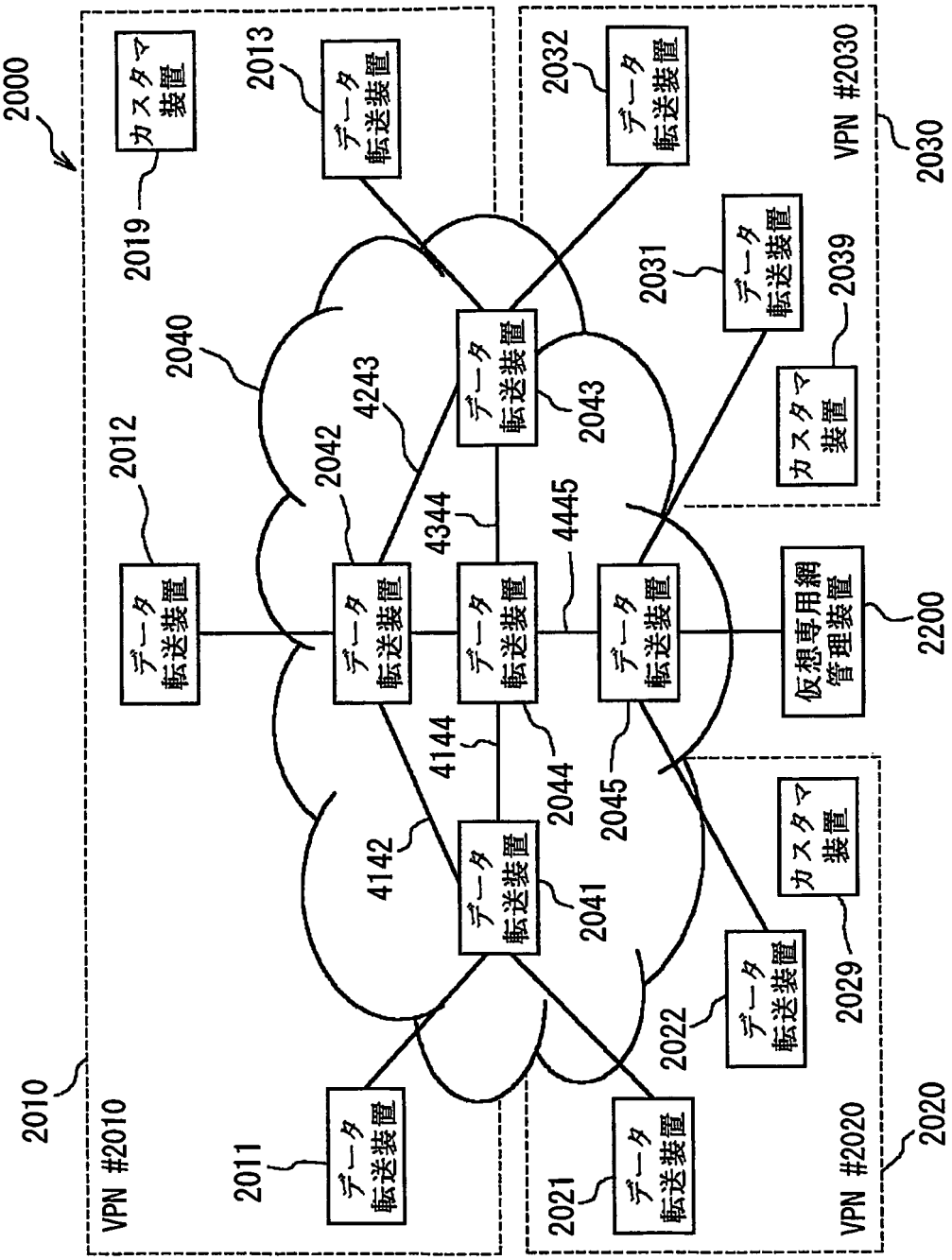

2000
2010
VPN #2010
2020
VPN #2020
2030
VPN #2030
2040
2200
仮想専用網管理装置
データ転送装置
カスタマ装置
2011
2012
2013
2019
2021
2022
2029
2031
2032
2039
2041
2042
2043
2044
2045
4142
4144
4243
4344
4445

FIG. 22

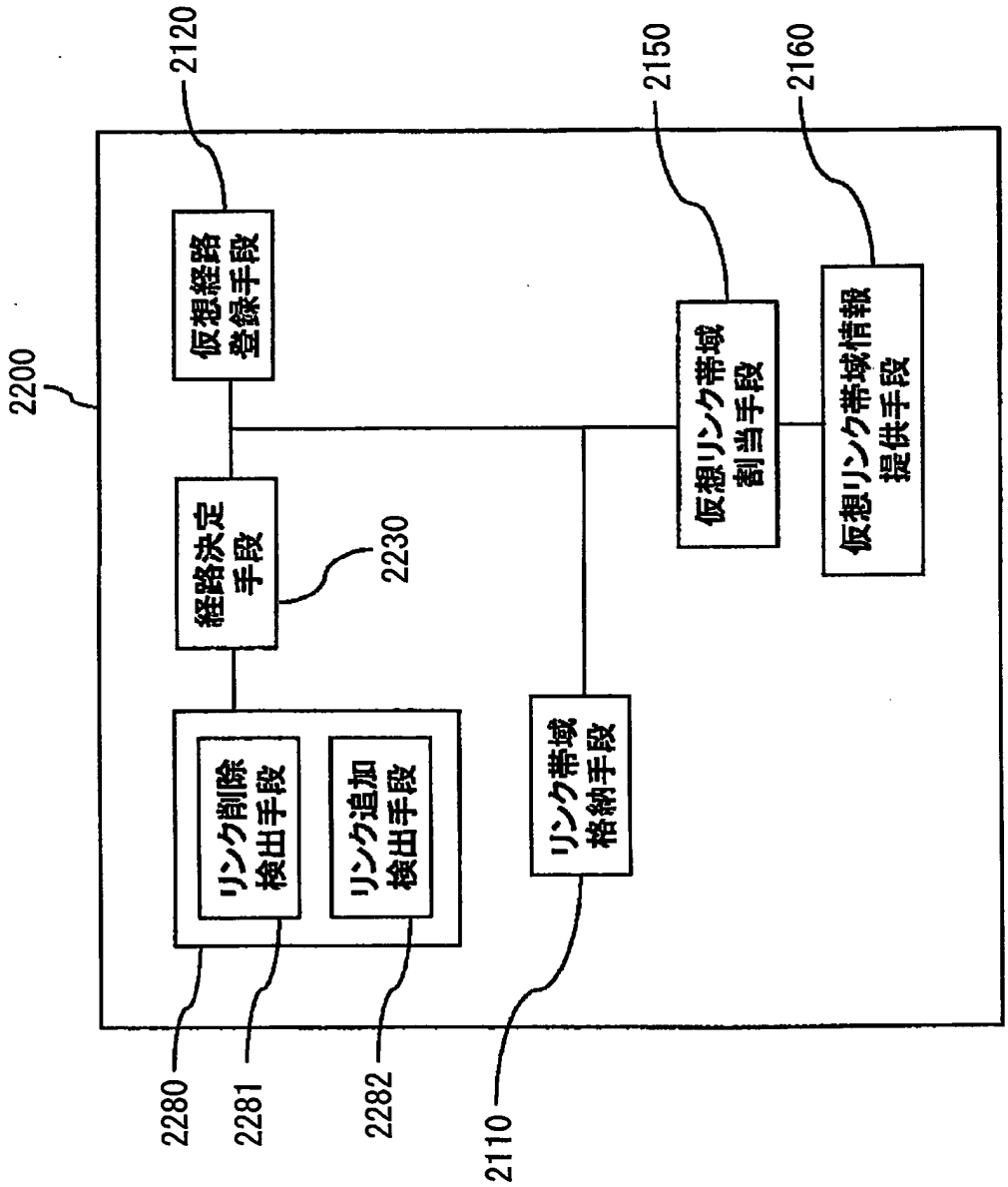

2200
2120
仮想経路登録手段
経路決定手段
2230
リンク削除検出手段
リンク追加検出手段
2280
2281
2282
リンク帯域格納手段
2110
2150
仮想リンク帯域割当手段
2160
仮想リンク帯域情報提供手段

FIG. 23A

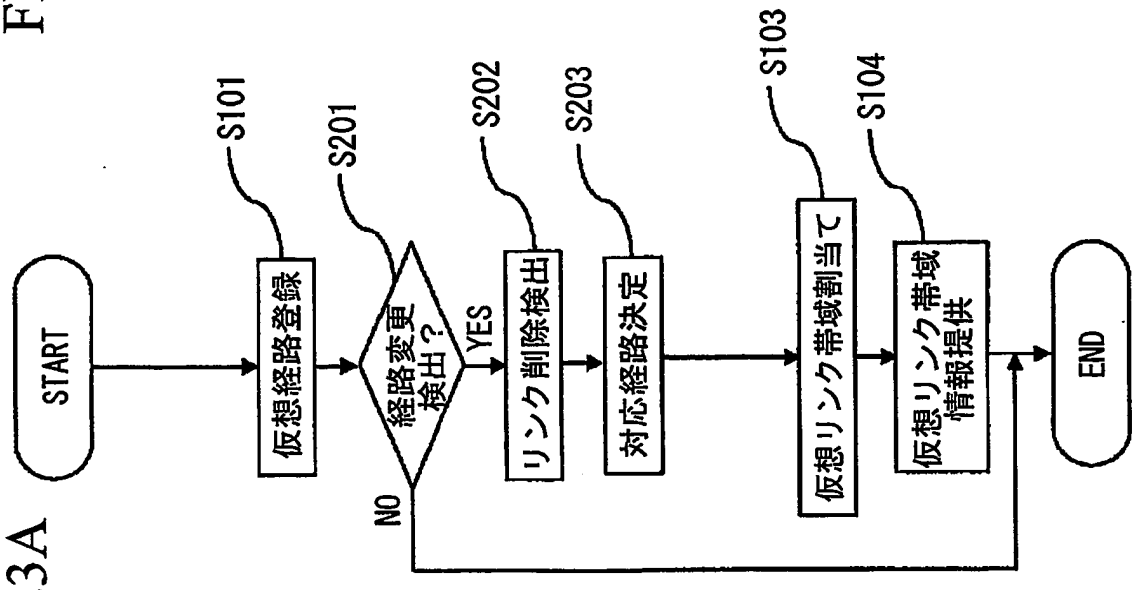


FIG. 23B

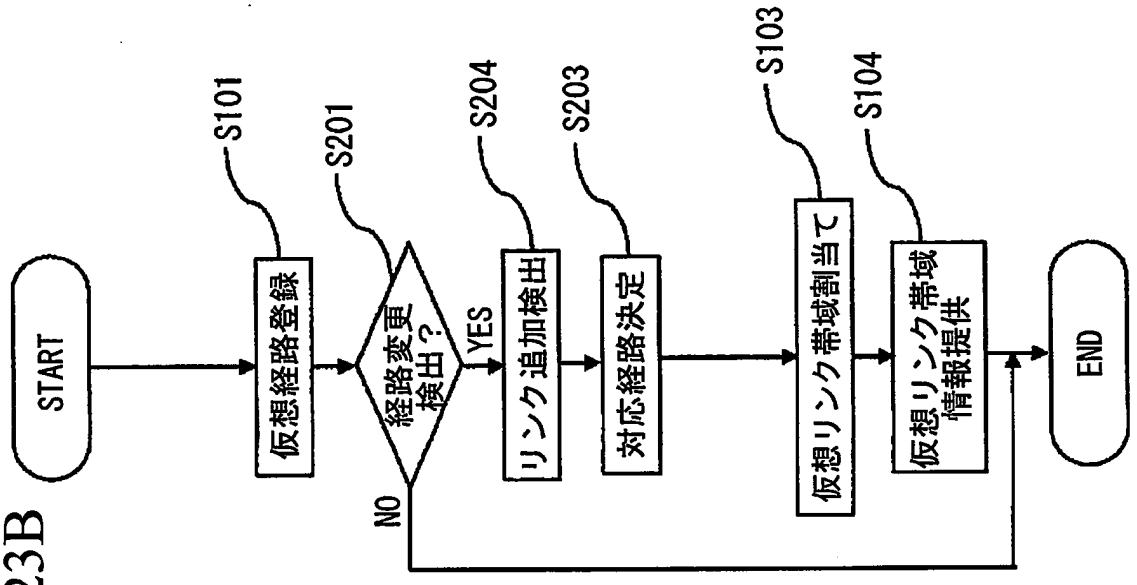


FIG. 24

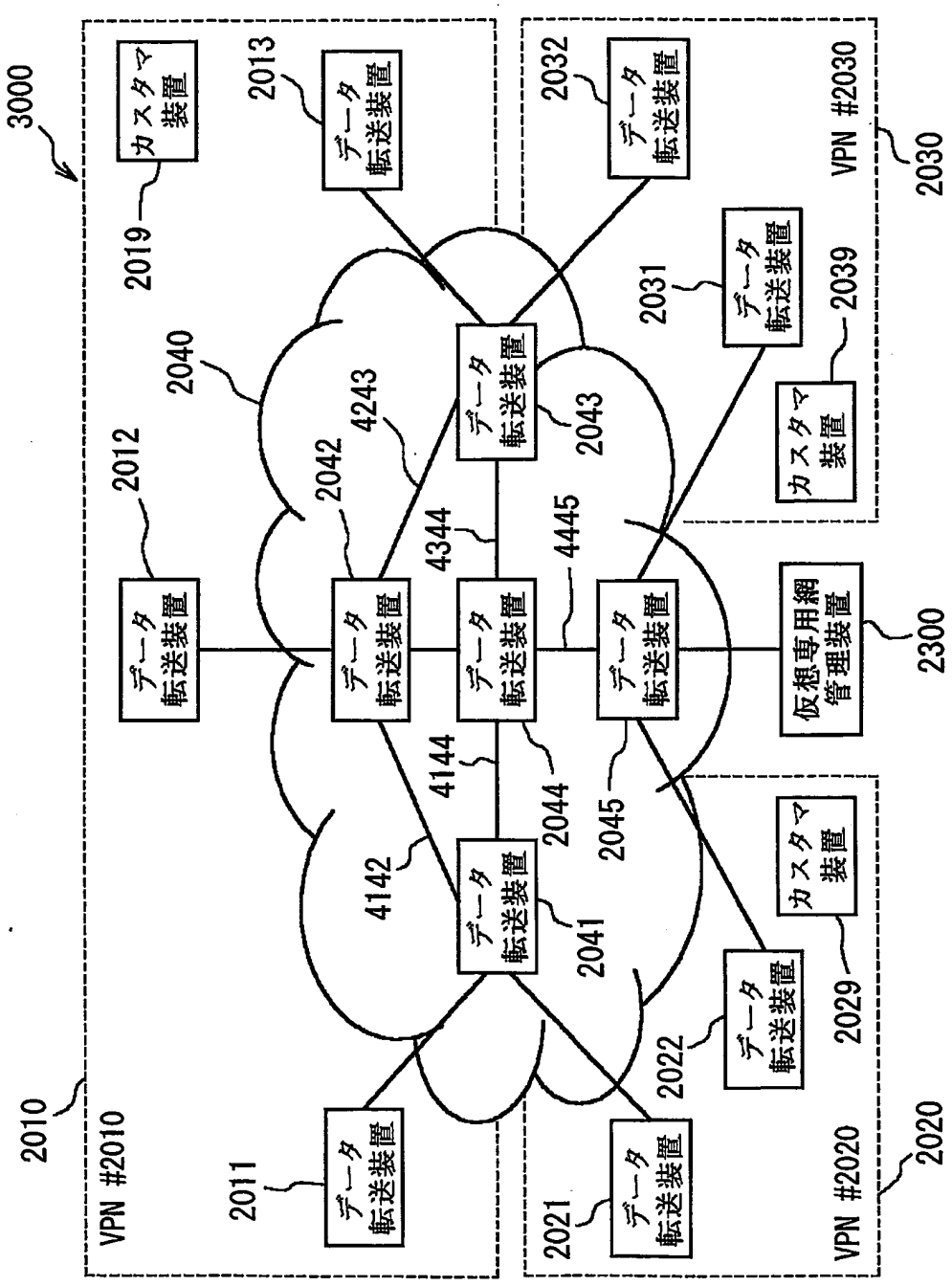

3000
2010
VPN #2010
2020
VPN #2020
2030
VPN #2030
データ転送装置
カスタマ装置
仮想専用網管理装置
2300
2011
2012
2013
2019
2021
2022
2029
2031
2032
2039
2040
2041
2042
2043
2044
2045
4142
4144
4243
4344
4445

FIG. 25

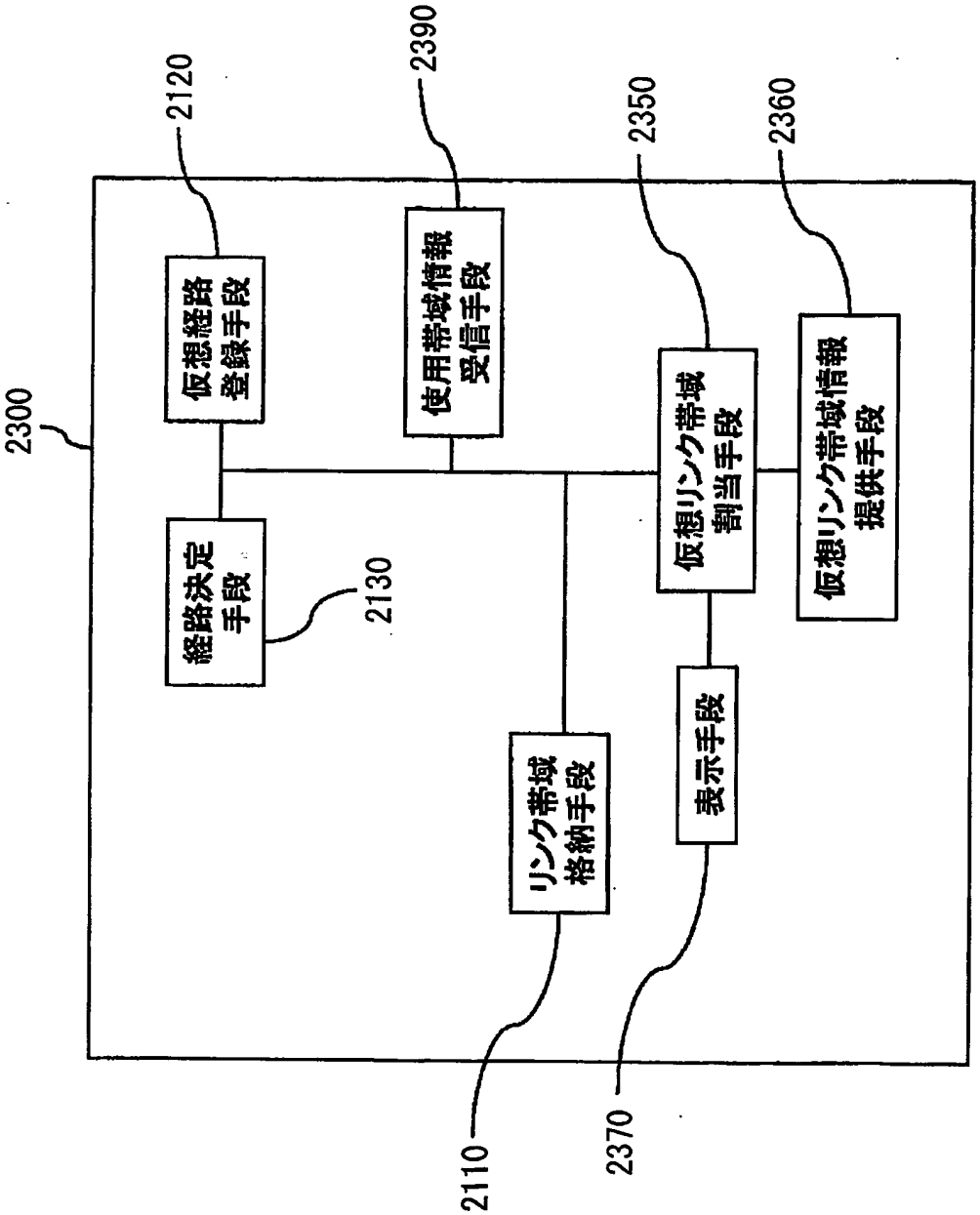
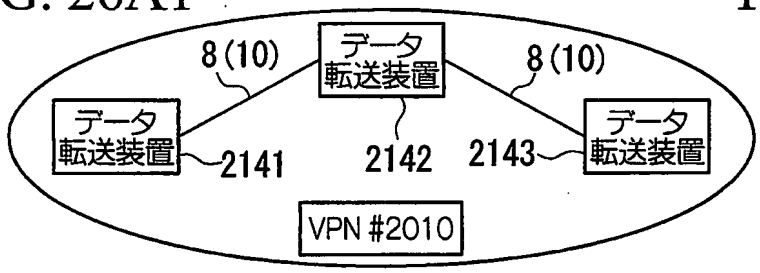
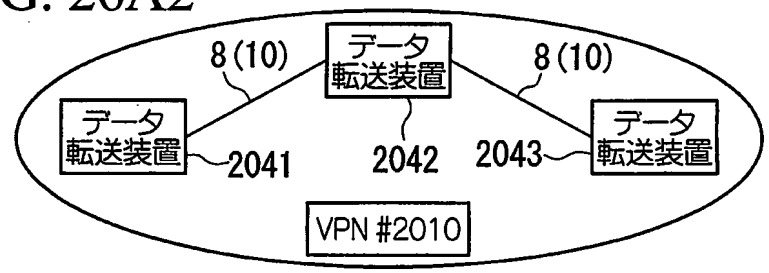

2300
2120
仮想経路登録手段
2390
使用帯域情報受信手段
2350
仮想リンク帯域割当手段
2360
仮想リンク帯域情報提供手段
経路決定手段
2130
リンク帯域格納手段
表示手段
2110
2370

FIG. 26A1



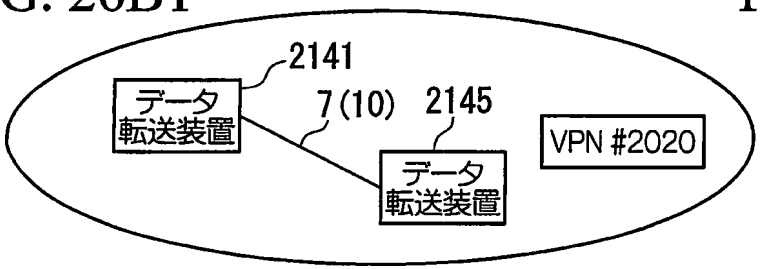
仮想リンク帯域をカスタマ装置に提供するイメージ

FIG. 26A2



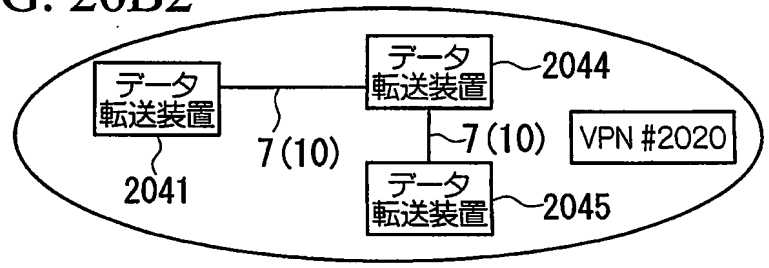
リンク帯域を表示するイメージ

FIG. 26B1



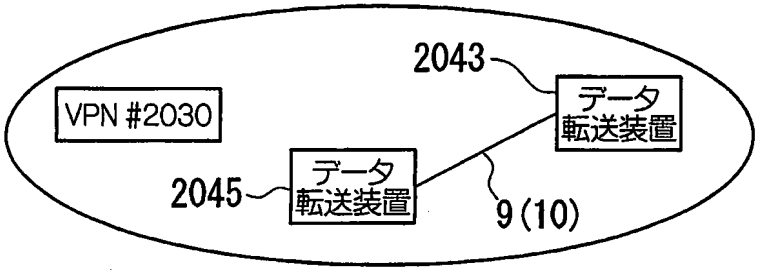
仮想リンク帯域をカスタマ装置に提供するイメージ

FIG. 26B2



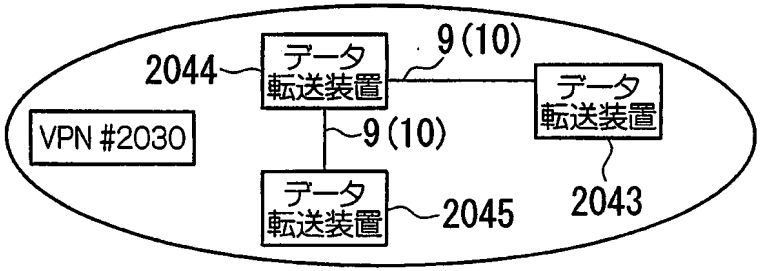
リンク帯域を表示するイメージ

FIG. 26C1



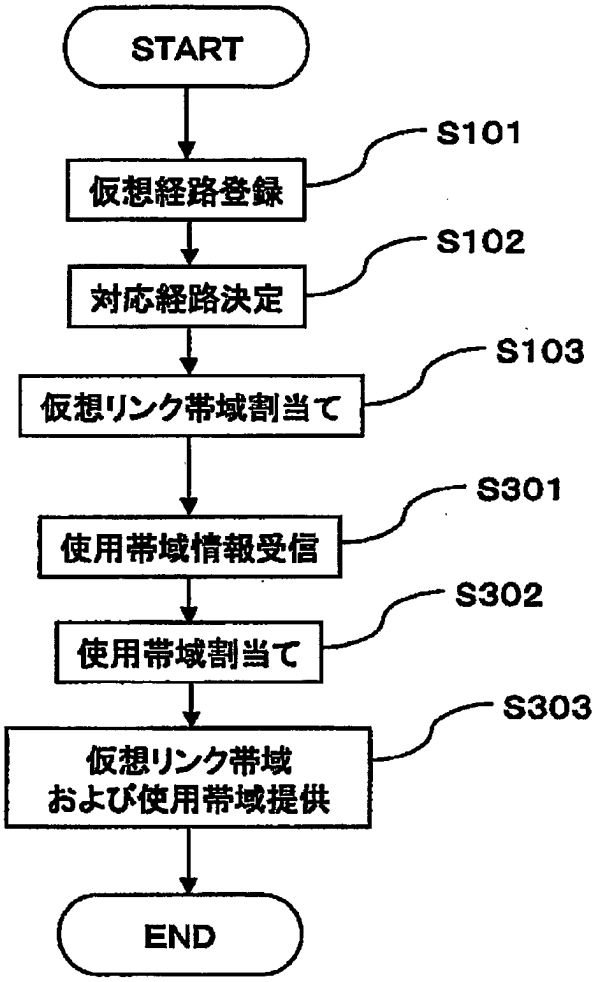
仮想リンク帯域をカスタマ装置に提供するイメージ

FIG. 26C2



リンク帯域を表示するイメージ

FIG. 27


START
S101
仮想経路登録
S102
対応経路決定
S103
仮想リンク帯域割当て
S301
使用帯域情報受信
S302
使用帯域割当て
S303
仮想リンク帯域
および使用帯域提供
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/000818

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-244508 A (Nippon Telegraph And Telephone Corp.), 08 September, 2000 (08.09.00), Fig. 1 (Family: none)	1-40
A	JP 2002-281084 A (NTT Communications Kabushiki Kaisha), 27 September, 2002 (27.09.02), Fig. 1 (Family: none)	1-40
A	JP 2002-044141 A (Fujitsu Ltd.), 08 February, 2002 (08.02.02), Fig. 1 (Family: none)	1-40

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 April, 2004 (26.04.04)	18 May, 2004 (18.05.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　PCT／JP2004／000818

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷ H04L12／56

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷ H04L12／56

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996年
日本国公開実用新案公報　1971－2004年
日本国登録実用新案公報　1994－2004年
日本国実用新案登録公報　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP　2000－244508　A（日本電信電話株式会社）、2000．09．08、図1（ファミリー無し）	1～40
A	JP　2002－281084　A（エヌ・ティ・ティ・コミュニケーションズ株式会社）、2002．09．27、図1（ファミリー無し）	1～40
A	JP　2002－044141　A（富士通株式会社）、2002．02．08、図1（ファミリー無し）	1～40

☐ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
26．04．2004	18.5.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5X	8124
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	石井　研一 電話番号　03－3581－1101　内線　3596		

様式PCT／ISA／210（第2ページ）（2004年1月）