(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4584998号
(P4584998)
(45)発行日　平成22年11月24日(2010.11.24)　(24)登録日　平成22年9月10日(2010.9.10)

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

請求項の数 51　(全 21 頁)

(21)出願番号　特願2007-519144(P2007-519144)
(86)(22)出願日　平成16年6月30日(2004.6.30)
(65)公表番号　特表2008-505527(P2008-505527A)
(43)公表日　平成20年2月21日(2008.2.21)
(86)国際出願番号　PCT/SE2004/001065
(87)国際公開番号　WO2006/004461
(87)国際公開日　平成18年1月12日(2006.1.12)
審査請求日　平成19年1月24日(2007.1.24)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン(パブル)
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】仮想プライベートネットワーク構成方法及びシステム

(57)【特許請求の範囲】
【請求項１】
通信ネットワーク（１）内のマルチドメイン仮想プライベートネットワーク（２２Ａ－Ｃ）－ＶＰＮの構成方法であって、前記通信ネットワーク（１）は、互いに相互接続される少なくとも２つのドメイン（１０Ａ－Ｅ）を有し、これによって、カスタマーは、前記少なくとも２つのドメイン（１０Ａ－Ｅ）のエッジノード（１４、１４’）でＶＰＮ（２２Ａ－Ｃ）と接続される方法であって、
第１ドメイン（１０Ｅ）の第１エッジノード（１４’）を、前記第１ドメイン（１０Ｅ）で現在利用可能でない第１ＶＰＮ（２２Ａ）に接続するための接続リクエストを開始する工程と、
前記少なくとも２つのドメインの、各ドメインで利用可能なＶＰＮの少なくともＶＰＮアイデンティティを備えるドメインＶＰＮ情報を提供する工程（２４、６２）と、
前記第１ＶＰＮ（２２Ａ）のアイデンティティと、前記第１ドメインとは異なる前記少なくとも２つのドメインの第２ドメインのＶＰＮアイデンティティとをマッチングする工程と、
前記マッチングする工程の出力に基づいて、前記第１エッジノード（１４’）を備えるように前記第１ＶＰＮ（２２Ａ）を構成する構成工程と
を備えることを特徴とする方法。
【請求項２】
前記マッチングする工程は、

前記第１ドメイン（１０Ｅ）から隣接ドメイン（１０Ｂ－Ｄ）への前記第１ＶＰＮの存在についての情報リクエストを送信する工程（３２）と、
前記情報リクエストと、前記第１ドメイン（１０Ｅ）とは異なるドメインで提供されたドメインＶＰＮ情報とを比較する工程と
を備えることを特徴とする請求項１に記載の方法。
【請求項３】
前記マッチングする工程は、
前記第１ドメイン（１０Ｅ）から、１つ、いくつかあるいはすべてのドメイン（１０Ｂ－Ｄ）への前記第１ＶＰＮ（２２Ａ）の存在についての情報リクエストを送信する工程（３２）と、
前記情報リクエストと、前記第１ドメイン（１０Ｅ）とは異なるドメインで提供されたドメインＶＰＮ情報とを比較する比較工程と
を備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記マッチングする工程は、
マッチ（一致）が検出される場合、応答確認へ前記第１ドメイン（１０Ｅ）へ返信する工程を備える
ことを特徴とする請求項２または３に記載の方法。
【請求項５】
前記マッチングする工程は、
一致が検出されない場合、前記第１ＶＰＮの存在についての前記情報リクエストを更なる隣接ドメインへ転送する工程を備える
ことを特徴とする請求項２または４に記載の方法。
【請求項６】
前記応答確認は、更に、
第１ＶＰＮ（２２Ａ）が利用可能であるドメインのドメインＩＤと、
第１ＶＰＮ（２２Ａ）が利用可能であるエッジノード（１４）のエッジノードＩＤと、
前記第１ＶＰＮ（２２Ａ）が利用可能である前記ドメインへ到達するためにどのドメインを通過しなければならないかについての情報と、
前記第１ＶＰＮ（２２Ａ）が利用可能である前記エッジノードへのルーティング情報と
の内の少なくとも１つを示すデータを有する
ことを特徴とする請求項４に記載の方法。
【請求項７】
前記マッチングする工程は、
前記ドメインＶＰＮ情報を、少なくとも１つのＶＰＮアイデンティティを備える処理されたＶＰＮ情報にするように処理する工程と、
前記処理されたＶＰＮ情報を隣接ドメイン間で送信する送信工程（２８）と、
前記第１ＶＰＮ（２２Ａ）の前記アイデンティティと、前記送信された処理されたＶＰＮ情報とを比較する比較工程と
を備えることを特徴とする請求項１に記載の方法。
【請求項８】
前記マッチングする工程は、
前記ドメインＶＰＮ情報を、少なくとも１つのＶＰＮアイデンティティを備える処理されたＶＰＮ情報にするように処理する工程と、
１つ、いくつかあるいはすべてのドメインに前記処理されたＶＰＮ情報を送信する送信工程（２８）と、
前記第１ＶＰＮ（２２Ａ）の前記アイデンティティと、前記送信された処理されたＶＰＮ情報とを比較する工程と

を備えることを特徴とする請求項１に記載の方法。
【請求項９】
前記マッチングする工程は、
前記比較する工程の前に、前記送信された処理されたＶＰＮ情報を更に処理する工程を更に備える
ことを特徴とする請求項７または８に記載の方法。
【請求項１０】
前記他のドメインへの送信対象の前記処理されたＶＰＮ情報は、更に、隣接ドメインから受信する処理されたＶＰＮ情報を備える
ことを特徴とする請求項７または９に記載の方法。
【請求項１１】
前記処理する工程は、他のドメインから送信される前記処理されたＶＰＮ情報あるいは、それから派生する情報に関する通過情報の追加を含んでいる
ことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記処理されたＶＰＮ情報は、更に、
異なるＶＰＮ（２２Ａ－Ｃ）が利用可能なドメイン（１０Ａ－Ｅ）のドメインＩＤと、
異なるＶＰＮ（２２Ａ－Ｃ）が利用可能であるエッジノード（１４、１４’）のエッジノードＩＤと、
異なるＶＰＮ（２２Ａ－Ｃ）が利用可能である前記ドメイン（１０Ａ－Ｅ）へ到達するためにどのドメイン（１０Ａ－Ｅ）を通過しなければならないかについての情報と、
異なるＶＰＮ（２２Ａ－Ｃ）が利用可能である前記エッジノード（１４、１４’）へのルーティング情報と
の内の少なくとも１つを有する
ことを特徴とする請求項７乃至１１のいずれか１項に記載の方法。
【請求項１３】
前記送信する送信工程は、定期的に実行される
ことを特徴とする請求項７乃至１２のいずれか１項に記載の方法。
【請求項１４】
前記送信する送信工程は、ドメインＶＰＮ情報の変更の応答として実行される
ことを特徴とする請求項７乃至１２のいずれか１項に記載の方法。
【請求項１５】
前記送信する送信工程は、前記接続リクエストの応答として実行される
ことを特徴とする請求項７または１４に記載の方法。
【請求項１６】
前記ドメインＶＰＮ情報は、更に、各前記エッジノード（１４、１４’）と、関係するＶＰＮ（２２Ａ－Ｃ）に接続されているカスタマーのカスタマーアイデンティティを備える
ことを特徴とする請求項１乃至１５のいずれか１項に記載の方法。
【請求項１７】
前記ドメインＶＰＮ情報は、更に、前記ＶＰＮ（２２Ａ－Ｃ）のプロパティを備える
ことを特徴とする請求項１乃至１６のいずれか１項に記載の方法。
【請求項１８】
前記ＶＰＮの前記プロパティは、
サービス品質のプロパティ、
暗号プロパティ
透過性レイヤプロパティ
トンネリングプロパティ及び
トポロジープロパティ

の内の少なくとも１つを備える
ことを特徴とする請求項１７に記載の方法。
【請求項１９】
前記提供する工程は、同一ドメインのエッジノードからドメインＶＰＮデータを収集することを含む
ことを特徴とする請求項１乃至１８のいずれか１項に記載の方法。
【請求項２０】
前記ドメインＶＰＮデータを収集することは、少なくとも１つのドメインに集中させる方法で実行される
ことを特徴とする請求項１９に記載の方法。
【請求項２１】
前記ドメインＶＰＮデータを収集することは、少なくとも１つのドメインに分散させる方法で実行される
ことを特徴とする請求項１９に記載の方法。
【請求項２２】
前記ドメインＶＰＮデータを収集することは、プッシュメカニズムによって実行される
ことを特徴とする請求項１９乃至２１のいずれか１項に記載の方法。
【請求項２３】
前記ドメインＶＰＮデータを収集することは、プルメカニズムによって実行される
ことを特徴とする請求項１９乃至２１のいずれか１項に記載の方法。
【請求項２４】
通信ネットワーク（１）であって、
境界ノード（１８）間の接続によって相互に接続される少なくとも２つのドメイン（１０Ａ－Ｅ）と、
前記通信ネットワーク（１）内の仮想プライベートネットワーク（２２Ａ－Ｃ）－ＶＰＮを制御する手段と、
前記ＶＰＮ（２２Ａ－Ｃ）によって接続されるエッジノード（１４、１４’）と、これによって、前記ＶＰＮ（２２Ａ－Ｃ）のカスタマーサイト（２０）は、前記エッジノード（１４、１４’）に接続され、
第１ドメイン（１０Ｅ）で現在利用可能でない第１ＶＰＮ（２２Ａ）と、前記第１ドメイン（１０Ｅ）の第１エッジノード（１４’）とを接続するための接続リクエストを開始する手段と、
前記少なくとも２つのドメイン（１０Ａ－Ｅ）で利用可能なＶＰＮの少なくともＶＰＮアイデンティティを有するドメインＶＰＮ情報を提供するための手段（４１）を備える、前記少なくとも２つのドメイン（１０Ａ－Ｅ）のそれぞれにおけるＶＰＮ制御ノード（４３）と、
前記第１ＶＰＮのアイデンティティと、前記第１ドメイン（１０Ｅ）とは異なる前記少なくとも２つのドメイン（１０Ａ－Ｅ）の第２ドメイン（１０Ａ－Ｄ）のＶＰＮアイデンティティとをマッチングする手段と、
前記マッチングする手段の出力に基づいて、前記第１エッジノード（１４’）を備えるように前記第１ＶＰＮ（２２Ａ）を構成する手段と
を備えることを特徴とする通信ネットワーク。
【請求項２５】
前記ＶＰＮ制御ノード（４３）は、少なくとも１つのドメイン（１０Ａ－Ｅ）の集中化ノードである
ことを特徴とする請求項２４に記載の通信ネットワーク。
【請求項２６】
前記ＶＰＮ制御ノード（４３）は、少なくとも１つのドメイン（１０Ａ－Ｅ）の分散ノードである
ことを特徴とする請求項２４または２５に記載の通信ネットワーク。

【請求項２７】
前記分散ノードである前記ＶＰＮ制御ノード（４３）の少なくとも一部は、境界ノード（１８）と論理的に接続されており、これにより、前記分散ノードであるＶＰＮ制御ノード（４３）と前記境界ノード（１８）を介して接続されるドメイン間の接続が、該境界ノード（１８）を介して達成される
ことを特徴とする請求項２６に記載の通信ネットワーク。
【請求項２８】
前記ＶＰＮ制御ノード（４３）は、ＶＰＮ情報用の記憶装置（５４）を備える
ことを特徴とする請求項２４乃至２７のいずれか１項に記載の通信ネットワーク。
【請求項２９】
前記マッチングする手段は、すべてのドメインに分散されていて、分散されている部分は、
特定のＶＰＮの存在についての情報リクエストを、隣接ドメインに対して送受信するリクエスト処理手段と、
受信される情報リクエストと、提供された自身の所有するドメインのドメインＶＰＮ情報とを比較する手段とを備え、
これによって、前記リクエスト処理手段は、更に、一致が検出される場合に、応答確認を返信するように構成されている
ことを特徴とする請求項２４乃至２８のいずれか１項に記載の通信ネットワーク。
【請求項３０】
前記マッチングする手段は、すべてのドメイン（１０Ａ－Ｅ）に分散されていて、分散されている部分は、
特定のＶＰＮの存在についての情報リクエストを、１つ、いくつかあるいはすべての隣接ドメインに対して送受信するリクエスト処理手段と、
受信される情報リクエストと、提供された自身の所有するドメインのドメインＶＰＮ情報とを比較する手段とを備え、
これによって、前記リクエスト処理手段は、更に、一致が検出される場合に、応答確認を返信するように構成されている
ことを特徴とする請求項２４乃至２８のいずれか１項に記載の通信ネットワーク。
【請求項３１】
前記リクエスト処理手段は、更に、一致が検出されない場合、情報リクエストを更なる隣接ドメインへ転送するように構成されている
ことを特徴とする請求項２９または３０に記載の通信ネットワーク。
【請求項３２】
前記ＶＰＮ制御ノード（４３）は、更に、
前記記憶装置（５４）に接続され、前記ＶＰＮ情報を、処理されたＶＰＮ情報にするように処理する第１プロセッサ（５０）と、
前記第１プロセッサ（５０）に接続され、前記処理されたＶＰＮ情報を他のドメインへ送信する手段と
を備えることを特徴とする請求項２４乃至２８のいずれか１項に記載の通信ネットワーク。
【請求項３３】
前記ＶＰＮ制御ノード（４３）は、更に、
処理されたＶＰＮ情報を他のドメインから受信する手段と、
前記受信する手段と前記記憶装置（５４）に接続され、前記受信された前記処理されたＶＰＮ情報を処理する第２プロセッサ（５６）とを備え、
これによって、前記処理された前記受信された前記処理されたＶＰＮ情報は、前記記憶装置（５４）に記憶される
ことを特徴とする請求項３２に記載の通信ネットワーク。
【請求項３４】

少なくとも１つのドメイン（１０Ａ－Ｅ）の前記ＶＰＮ制御ノード（４３）は、同一のドメインのエッジノードからドメインＶＰＮ情報を収集する手段（４１）を備える
ことを特徴とする請求項２４乃至３３のいずれか１項に記載の通信ネットワーク。
【請求項３５】
少なくとも２つのドメイン（１０Ａ－Ｅ）を有し、かつマルチドメイン仮想プライベートネットワーク（２２Ａ－Ｃ）－ＶＰＮをサポートする通信ネットワーク（１）の第１ドメインのＶＰＮ制御ノード（４３）であって、前記少なくとも２つのドメイン（１０Ａ－Ｅ）のエッジノード（１４、１４’）で前記ＶＰＮ（２２Ａ－Ｃ）にカスタマーが接続されている、ＶＰＮ制御ノード（４３）であって、
第１ドメイン（１０Ｅ）の第１エッジノード（１４’）を、前記第１ドメイン（１０Ｅ）で現在利用可能でない第１ＶＰＮ（２２Ａ）に接続するための接続リクエストを開始する手段と、
前記少なくとも２つのドメインの、各ドメインで利用可能なＶＰＮの少なくともＶＰＮアイデンティティを備えるドメインＶＰＮ情報を提供する手段（５２、６２）と、
前記第１ＶＰＮのアイデンティティと、前記第１ドメインとは異なる前記少なくとも２つのドメインの第２ドメインのＶＰＮアイデンティティとをマッチングする手段と、
前記マッチングする手段の出力に基づいて、前記第１エッジノード（１４’）を備えるように前記第１ＶＰＮ（２２Ａ）を構成する構成手段と
を備えることを特徴とするＶＰＮ制御ノード。
【請求項３６】
前記第１ドメインのＶＰＮ接続のための構成マシーン（４６）を更に備える
ことを特徴とする請求項３５に記載のＶＰＮ制御ノード。
【請求項３７】
前記第１ドメインに関係するドメイン間ＶＰＮ接続のための構成マシーン（６０）を更に備える
ことを特徴とする請求項３５または３６のいずれか１項に記載のＶＰＮ制御ノード。
【請求項３８】
前記ＶＰＮ制御ノード（４３）は、集中化ノードである
ことを特徴とする請求項３５乃至３７のいずれか１項に記載のＶＰＮ制御ノード。
【請求項３９】
境界ノードを介して、他のドメインのＶＰＮ制御ノードと通信する手段を更に備える
ことを特徴とする請求項３８に記載のＶＰＮ制御ノード。
【請求項４０】
他のドメインのＶＰＮ制御ノードとの専用ＶＰＮ制御信号接続（４７）によって、通信する手段を更に備える
ことを特徴とする請求項３８に記載のＶＰＮ制御ノード。
【請求項４１】
前記ＶＰＮ制御ノードは、分散ノードである
ことを特徴とする請求項３５乃至３７のいずれか１項に記載のＶＰＮ制御ノード。
【請求項４２】
前記分散ノードである前記ＶＰＮ制御ノード（４３）の少なくとも一部は、境界ノード（１８）と論理的に接続されており、これを介して、近隣ドメインとのデータ通信が発生する
ことを特徴とする請求項４１に記載のＶＰＮ制御ノード。
【請求項４３】
前記ＶＰＮ制御ノード（４３）は、ＶＰＮ情報用の記憶装置（５４）を備える
ことを特徴とする請求項３５乃至４２のいずれか１項に記載のＶＰＮ制御ノード。
【請求項４４】
前記ＶＰＮ情報用の記憶装置（５４）は、集中化されている
ことを特徴とする請求項４３に記載のＶＰＮ制御ノード。

【請求項４５】
前記ＶＰＮ情報用の記憶装置（５４）は、分散されている
ことを特徴とする請求項４３に記載のＶＰＮ制御ノード。
【請求項４６】
他のドメインとの間で、ドメインＶＰＮ情報を通信する手段を更に備える
ことを特徴とする請求項３５乃至４５のいずれか１項に記載のＶＰＮ制御ノード。
【請求項４７】
ＶＰＮリクエストを受信する手段を更に備え、これによって、前記マッチングする手段は、一致が検出される場合に、応答確認を送信する手段を備える
ことを特徴とする請求項３５乃至４５のいずれか１項に記載のＶＰＮ制御ノード。
【請求項４８】
前記マッチングする手段によって一致が検出されない場合、ＶＰＮリクエストを他のドメインに転送する手段を更に備える
ことを特徴とする請求項４７に記載のＶＰＮ制御ノード。
【請求項４９】
同一ドメインのエッジノードからドメインＶＰＮ情報を収集する手段（４１）を更に備える
ことを特徴とする請求項３５乃至４５のいずれか１項に記載のＶＰＮ制御ノード。
【請求項５０】
前記ドメインＶＰＮ情報を収集する手段（４１）は、プッシュメカニズムに従って動作するように構成されている
ことを特徴とする請求項４９に記載のＶＰＮ制御ノード。
【請求項５１】
前記ドメインＶＰＮ情報を収集する手段（４１）は、プルメカニズムに従って動作するように構成されている
ことを特徴とする請求項４９に記載のＶＰＮ制御ノード。
【発明の詳細な説明】
【技術分野】
【０００１】
技術分野
本発明は、一般的には、通信システムの仮想プライベートネットワークに関するものであり、より詳しくは、マルチドメイン通信システムの仮想プライベートネットワークの構成（コンフィグレーション：configuration）に関するものである。
【０００２】
背景
仮想プライベートネットワーク（ＶＰＮ）は、パブリック（公衆）あるいはプライベート（専用）通信ネットワークを利用して、プライベート通信を管理する。伝統的には、広範囲ネットワークを構築することを望んでいる企業あるいは他のカスタマー（取引先（customer））は、各ノード間に自身が所有する専用線を提供して、接続性を提供しなければならない。しかしながら、このようなソリューションは、一般的には費用がかかりかつ柔軟性に欠ける。最近では、ＶＰＮの概念が急速に発展している。ＶＰＮは、通信ネットワークが多くのカスタマー間で共有されるが、各カスタマーの通信は仮想的に分けられているソリューションを提案している。ＶＰＮ技術は、たいていは、トンネリングの概念に基づいている。ネットワークトンネリングは、論理的なネットワーク接続の確立及び維持を意味するものである。この接続においては、パケットは、いくつかの他の基本あるいは搬送プロトコル内にカプセル化される。次に、それらは、ＶＰＮクライアントとサーバ間を送信され、最終的には、受信側で、逆カプセル化される。認証及びカプセル化は、セキュリティの提供を支援する。
【０００３】
ネットワークノードの数がＶＰＮの成長を早めさせる傾向になっており、それが、大規

模でかつ複雑なネットワーク構造及びトポロジーを生み出す結果となっている。このことは、ある程度は、ＶＰＮ上のトラフィックの増加の要因となり、また、ある程度は、ＶＰＮがますます広い地理的エリアを包囲することが要求される要因となっている。あらゆる地域でノードを有するＶＰＮを提供する通信ネットワークが、今日存在している。しかしながら、ノードはますます多くなり、送信対象のトラフィックもますます増え、更には、ＶＰＮの構成もますます複雑になっている。

【０００４】

従来より、ＶＰＮはネットワークオペレータと取引先間の協定（アグリーメント：agreement）に従って生成されている。ノードの位置、サービスの品質及び他の状態が取り決められていて、かつネットワークオペレータのプログラマーは、手動で、あるいは構成支援ツールを用いることによって構成をセットアップする。通信ネットワークがますます複雑になると、このような構成はますます複雑となり、また時間がかかる。また、取引先が自身のＶＰＮを変更したい場合には、処理全体を繰り返さなければならない。

【０００５】

ネットワーク内でＶＰＮをセットアップする場合、様々な技術を使用することもできる。各技術は、それ自身に利点と欠点を併せ持ち、かつ独自のＶＰＮの構成方法を持っている。このように、ＶＰＮ技術とは独立している、汎用的なＶＰＮアーキテクチャは存在していない。

【０００６】

要約

従来技術のソリューションの一般的な問題は、通信ネットワークが、大規模地理的通信範囲及び大量トラフィックの少なくとも一方を有する仮想プライベートネットワークを提供することはかなり複雑になることである。更なる問題は、新規のＶＰＮの構成あるいは既に存在しているＶＰＮの変更は複雑であり、かつ時間がかかることである。更なる問題は、より小範囲の地理的領域を包囲（カバー）するネットワークオペレータの通信リソースは、広範囲ＶＰＮ用に一般的には利用することができないことである。

【０００７】

本発明の一般的な目的は、ＶＰＮの構成方法、及び提供システム及び適切な装置を改良することである。本発明の更なる目的は、２つ以上のネットワークドメインを利用するＶＰＮを構成する方法を提供することである。本発明の別の更なる目的は、実際に使用されるＶＰＮ技術とは基本的には独立しているＶＰＮを構成する方法を提供することである。本発明の別の更なる目的は、ＶＰＮの自動構成を行う方法を提供することである。

【０００８】

上述の目的は、特許請求の範囲に従う方法及び装置によって達成される。一般的には言えば、ドメインのＶＰＮについての情報が提供される。ＶＰＮの構成用のリクエストと、他の接続されているドメインの提供された情報とを比較することによって、一致を検出することができる。そして、再構成は、比較結果に基づいて実行することができる。ドメインＶＰＮ情報の提供は、様々な方法で実行することができる。これには、例えば、集中化あるいは分散化方法によるデータの収集によるもの、あるいは記憶されたデータを検索することによるものがある。分散されたＶＰＮ制御ノードは、特定の実施形態では、ドメインの境界ノードにローカライズされている。ドメインＶＰＮ情報は、特定の実施形態では、ドメインのエッジノードから収集される。これは、エッジノードからブロードキャストされた情報を受動的に抽出し、エッジノード群あるいはそれらの組み合わせからのドメインＶＰＮ情報を受信することによって実行することができる。この収集は、ＶＰＮ構成リクエストのような外部イベントによって起動することができる。この提供されたドメインＶＰＮ情報は、一実施形態では、ドメインオペレータ間のＳＬＡによって与えられる制限下で、他のドメインに配信される。別の実施形態では、これに代えて、ＶＰＮ構成リクエストは、異なるドメインに配信される。こうして、マッチング（比較）は、リクエストを発信しているドメインから離れた様々な位置で実行することができる。

【０００９】

本発明の１つの重要か効果は、異なるドメインのオペレータが協調動作することができる単純かつ適切なプラットホームを提供することである。ドメインＶＰＮ情報は、マルチドメインシステムの本質的なすべてのドメインにおけるＶＰＮ構成をサポートするために利用することができる。更には、同時に、一実施形態では、実際の情報は、オペレータ間の様々な協定によって制限されているマルチドメインシステムを介して配信される。

【００１０】

詳細説明

一般的なＶＰＮプロバイダアーキテクチャ１の実施形態を図１に示す。このＶＰＮプロバイダアーキテクチャでは、５つのＶＰＮプロバイダドメイン１０Ａ－Ｅが存在し、これらはすべて、ドメイン間データ接続１２Ａ－Ｇによって互いに接続されている。１つのオペレータは、１つ以上のこれらのドメイン１０Ａ－Ｅを制御することができる。あるいは、これらは、別々のオペレータによって制御することができる。ドメイン１０－Ｅ間の関係、即ち、ドメイン間データ接続１２Ａ－Ｇの制御は、典型的には、介在するオペレータ間のアグリーメント（協定）、例えば、ＶＰＮサービスレベルアグリーメント（ＳＬＡ）に従って調整される。各ＶＰＮプロバイダドメイン１０Ａは、ＶＰＮエッジ（edge）ノード１４とコアノード１６を備えている。これは、ＶＰＮ　ａｗａｒｅ（認識できる）あるいはＶＰＮ　ｕｎａｗａｒｅ（認識できない）とすることができる。また、これらのうちのいくつかものだけに、ここでは参照番号を付している。ＶＰＮエッジノード１４は、アーキテクチャ１内の様々なＶＰＮと、様々なカスタマーのカスタマーサイト２０とが、これを介して接続されるノードである。ＶＰＮ　ｕｎａｗａｒｅ　ノード１６は、ドメインの中間ノードであり、また、ＶＰＮエッジノード１４間でメッセージ及びデータを転送するためだけに使用される。カスタマーは、通信用に使用されるＶＰＮ　ｕｎａｗａｒｅノードを認識しない。重要なことは、ＶＰＮエッジノード１４で開始し、終了することである。ドメインで接続されるＶＰＮは、実際の通信が１つあるいはいくつかのＶＰＮ　ｕｎａｗａｒｅノード１６を介して発生するとしても、ＶＰＮエッジノード１４間を直線で示すことができる。本発明の以下の開示では、ＶＰＮ　ｕｎａｗａｒｅノードの存在は通常は無視される。これは、本発明に従う基本処理ステップは、ＶＰＮ　ｕｎａｗａｒｅノード１６の存否は直接には依存しないからである。しかしながら、実際の実装環境では、ＶＰＮ　ｕｎａｗａｒｅノードの類は、実際の接続性を提供するために使用される。

【００１１】

ＶＰＮプロバイダドメイン１０Ａ－Ｅは、ＶＰＮ境界（border）ノード１８を介してデータプレーンに接続される。即ち、ドメイン間データ接続１２Ａ－Ｇは、ＶＰＮ境界ノード１８で開始し、終了する。ＶＰＮ境界ノード１８は、同時にＶＰＮエッジノード１４として動作してもしなくても良い。カスタマーサイト２０は、ＶＰＮエッジノード１４の１つに接続される。そして、同一カスタマーのカスタマーサイト２０は、ＶＰＮ２２Ａ－ＣによってＶＰＮプロバイダドメイン１０Ａ－Ｅを介して接続することができる。１つのカスタマーは、異なるＶＰＮ２２Ａ－Ｃに接続されているカスタマーサイト２０を持つことができる。また、２つ以上のカスタマーサイト２０は、同一のＶＰＮエッジノード１４に接続することができるが、他のカスタマーサイト２０の存在と、他のカスタマーサイト２０に接続されているＶＰＮの存在を認識できない。

【００１２】

本実施形態では、３つのＶＰＮ２２Ａ－Ｃが示されている。しかしながら、当業者であれば、実システム内でのＶＰＮの数は通常はもっと多いものであることを理解している。破線で示される第１ＶＰＮ２２Ａは、３つのドメイン１０Ａ、１０Ｃ、１０Ｄに渡って展開されていて、かつこれらのすべてのドメインのカスタマーサイト２０と接続している。点線で示される第２ＶＰＮ２２Ｂは、本実施形態のすべてのドメイン１０Ａ－Ｅに渡って展開されている。そして、一点鎖線で示される第３ＶＰＮ２２Ｃは、ドメイン１０Ｂのカスタマーサイト２０だけに接続している。各カスタマーサイト２０は、他のカスタマーのカスタマーサイト２０の存在と、自身に接続されているＶＰＮ以外のＶＰＮの存在を認識できない。このような状況では、ＶＰＮのプライバシー特徴は保護されているものの、こ

れらのすべては、同一の基本通信リソースを共有している。このことは、本発明が好適に動作する状況となる。

【００１３】

ここで、新規のカスタマーサイト２０’がドメイン１０ＥのＶＰＮエッジノード１４’に接続されたとする。カスタマーサイト２０’をＶＰＮ２２Ｂに接続したい場合は、その処理はおそらく比較的単純となる。これは、ＶＰＮ２２Ｂが既にドメイン１０Ｅに存在しているからである。従来技術に従う手動あるいは自動ＶＰＮ再構成処理を利用することもできるし、それらを合わせ持ったものを利用することもできる。しかしながら、新規のカスタマーサイト２０’をＶＰＮ２２Ａあるいは２２Ｃに接続したい場合、状況はより複雑となる。従来技術では、ドメイン間ＶＰＮ構成処理は通常は存在しない。

【００１４】

本発明の基本的な概念は、３つのアクティビティに基づいている。その１つは、ドメインＶＰＮ情報の提供に関するものである。この情報は、各ドメインで利用可能なＶＰＮの、自身で最も基本となる形式のＶＰＮアイデンティティを備えている。別の１つは、接続する特定のＶＰＮの検索（サーチ）に関するものである。これは、換言すれば、リクエストされたＶＰＮと、提供されたドメインＶＰＮ情報とマッチング（照合）することである。いくつかの実施形態では、このマッチング処理は、ドメインＶＰＮ情報、あるいはそのドメインＶＰＮ情報から派生する情報を他のドメインへ送信することを含んでいる。他の実施形態では、これに代えて、あるＶＰＮに対するリクエストがドメイン間を送信される。最後の１つは、ＶＰＮの実際の再構成に関するものである。本発明の基本的な新規な概念は、主に、２つの第１段階（ステージ）に関与している。

【００１５】

図２Ａは、ドメインＶＰＮ情報を提供する初期フェーズの実施形態を示している。各ＶＰＮエッジノード１４は、自身が所有する既存のＶＰＮ構成を反映する情報を記憶している。この構成は、少なくとも、どのＶＰＮが、特定のＶＰＮエッジノード１４でカスタマーサイトに接続されているかに関するものである。特定の実施形態では、ＶＰＮエッジノード１４は、どのカスタマーがＶＰＮエッジノード１４に接続されていて、かつ既存のＶＰＮとカスタマーサイト２０間の関係についての情報も持っている。いくつかの実施形態では、例えば、ＶＰＮアドレス空間及びアドレスタイプ（ローカルあるいはグローバル）と、帯域幅、遅延及びジッターのような仕様によって特定されるＶＰＮ品質のサービスクラス、及びＶＰＮセットアップ、即ち、トンネルあるいはフィルタの使用の少なくとも１つのような情報が提供される。暗号プロパティ、透過性レイヤプロパティ、トンネリングプロパティ及びトポロジープロパティのような情報も含めることができる。また、ＶＰＮ境界ノード１８は、自身が属するＶＰＮプロバイダドメインのアイデンティティについての情報を記憶している。

【００１６】

本発明の一実施形態に従えば、各ＶＰＮエッジノード１４に記憶されているドメインＶＰＮ情報あるいはその少なくとも一部は、同一ドメイン１０Ａ－Ｅの各境界ノード１８によって収集される。これについては、図２Ａでは矢印として視覚化されていて、それらの内の一部は参照番号２４が付与されている。このような方法で、所有するドメインについての、収集されたドメインノード情報は、各ドメイン１０Ａ－Ｅの各ＶＰＮ境界ノード１８で利用可能である。通信に対する１つの構成としては、ＢＧＰ（境界ゲートウェイプロトコル（Border Gateway Protocol））に類似する通信プロトコルを使用することであり、これは、どこで情報を必要としているかについての特別な知識なしに、ドメインに渡って情報を配信する。次に、境界ノードは、すべての必要な情報をピックアップすることができる。この例には、ドメインＶＰＮ情報を配信するためのプッシュメカニズムがある。

【００１７】

図２Ｂは、ドメインＶＰＮ情報を提供する別の実施形態を示していて、ここでは、この情報は、１つのドメイン１０Ｃに集約されている。ＶＰＮ境界ノード１８が、エッジノード１４が同一ドメイン１０Ｃに存在していることについての情報を記憶している場合、Ｖ

ＰＮ境界ノード１８は、単に、リクエスト２３を任意のＶＰＮエッジノード１４に行うことで、自身のドメインノード情報２４を返信することができる。リクエストする情報の最も単純な形式では、リクエスト自身をＶＰＮエッジノード１４があるＶＰＮに関係しているかどうかの問い合わせにすることができる。これは、例えば、ドメイン相互接続によって受信される。このような場合には、応答確認メッセージには任意の情報を含まないが、特定のＶＰＮエッジノードにおける特定のＶＰＮの情報を潜在的に送信することになる。この例には、ドメインＶＰＮ情報を配信するためのプッシュメカニズムがある。

【００１８】

ドメインノード情報は、異なるタイミングで収集することもできる。１つの構成は、利用可能な情報が常に更新されていることを保証するために、境界ノードに、このような情報を継続的にあるいは少なくとも定期的に収集することである。このような実施形態では、この情報は、境界ノード、あるいは、境界ノードから検索可能な場所にある任意の他のノードに記憶されることが好ましく、これについては以下で説明される実施形態を参照されたい。別の構成は、情報収集がいくつかのイベントによって起動されることである。このイベントは、例えば、エッジノードからのブロードキャスティングメッセージとすることができ、これには、なんらかの変更が存在すること、あるいは上述の特定のＶＰＮを検出するリクエストがある。すべてのエッジノードが、ドメインのどの境界ノードが利用可能であるかについての知識を持っている場合、この情報も、このような変更が発生する場合にすべての境界ノードに直接送信することができる。あるＶＰＮを検出するためのリクエストによって起動されることで情報が検索される場合、収集された情報はそのＶＰＮに制限されても良く、また、後に使用するために必要であるとしても記憶されなくても良い。

【００１９】

図２Ｃは、ドメインＶＰＮ情報が集中的に収集される実施形態を示している。異なるエッジノード１４によって提供されるすべてのドメインＶＰＮ情報を記憶するために、記憶装置５４が提供される。このようなドメインＶＰＮ情報を使用する機能は、中央の記憶装置５４からこの情報を検索することができる。

【００２０】

図２Ｄは、ドメインＶＰＮデータの集中収集に基づいている別の実施形態を示している。ここで、リクエスト２３あるいは他の外部信号は、記憶装置５４へのＶＰＮデータ２４の提供を初期化することができる。このリクエスト２３は、記憶装置５４自身から発せられる必要はない。

【００２１】

ドメインノード間でのドメインＶＰＮ情報を収集するための別の構成としては、データ記憶装置からデータを取得することによって、ドメインＶＰＮ情報が提供されても良い。この記憶されたデータは、例えば、上述の処理に従って従前に収集されたデータの結果とすることができる。あるいは、この記憶されたデータは、外部から提供されるものとすることができる。

【００２２】

上述の実施形態では、ドメインのデータの提供は、それに直接関係のある境界ノードあるいはノードによって実行される。このような状況は、図３Ａでも示される。ここで、マルチドメインシステムの１つのドメイン１０Ａがより詳細に示される。境界ノード１８は、データ接続１２Ａ及び１２Ｂによる他のドメインとのデータトラフィックを担当する。この境界ノード１８は、特定の実施形態では、境界ノード１８のプロセッサのソフトウェア機能による、ドメインＶＰＮ情報を収集する手段４１を備える。このドメインＶＰＮ情報は、記憶装置５４に記憶することができる。ドメインに関するドメインＶＰＮ情報を処理するためのＶＰＮ制御ノード４３は、全体として、特定の実施形態では、各境界ノード１８に分散されたローカルの手段４１として実現される。

【００２３】

図３Ｂでは、別の特定の実施形態が示されている。ここでも、境界ノード１８は、ドメ

インＶＰＮ情報に関係する機能エンティティ４１を備えている。但し、分散されたＶＰＮ制御ノード４３は、この特定の実施形態では、境界ノード１８に配置されるあるいはそれに接続されている、ドメインＶＰＮ情報を提供するための手段４１と、中央データベース５４を備えている。この中央データベース５４には、実際に更新されたＶＰＮ情報と、かつ好ましくは履歴ＶＰＮ情報が記憶される。

【００２４】

図３Ｃでは、更に別の特定の実施形態が示される。ここでは、ＶＰＮ制御ノード４３は中央に配置され、かつドメインＶＰＮ情報を提供する手段４１と、基本的には同一位置に提供される中央データベース５４を備えている。境界ノード１８は、この特定の実施形態では、単に、ＶＰＮ制御ノードと近隣ドメイン間の通信４５を処理するために使用される。実際のデータトラフィックに関係するシグナリングの制御に関わる境界ノード１８の機能は、ＶＰＮ構成に関係する制御メッセージの信号処理を行うようにも利用することができる。

【００２５】

図３Ｄでは、システム内の境界ノードから仮想的に分けられているＶＰＮ制御ノード４３を有する実施形態が示されている。ＶＰＮ制御ノード４３は、このような実施形態では、専用のＶＰＮ制御信号接続４７によって他のドメインのＶＰＮ制御ノードに接続されていて、自身で所有するハイレベルネットワークを生成する。

【００２６】

本発明の特定の実施形態では、提供されているドメインＶＰＮ情報は、システム内、即ち、異なるドメイン間で転送することができる。これについては、図４で示される。第１ステップは、各ドメインのＶＰＮ情報の提供である。これは、各ドメインのＶＰＮ制御ノード４３によって実行される。但し、ＶＰＮ制御ノード４３の構成は、異なるドメイン間で異ならせることができる。図４では、ドメイン１０Ａは、図３Ａに示される例と同様のＶＰＮ制御ノード４３を有している。ドメイン１０Ｃは、図３Ｂに示される例と同様のＶＰＮ制御ノード４３を有している。そして、ドメイン１０Ｂ、１０Ｄ及び１０Ｅは、図３Ｃに示される例と同様のＶＰＮ制御ノード４３を有している。異なるドメイン間のトラフィックを調整する各ＳＬＡに従えば、各ＶＰＮ制御ノード４３において利用可能なドメインＶＰＮ情報の少なくとも一部は、本実施形態では、近隣ドメインの反作用（counteracting）ＶＰＮ制御ノードに送信される。矢印２８は、ドメイン間の情報転送を示している。ＳＬＡは、利用可能な情報をどの程度近隣ドメインに対して利用可能にすべきであるかについての協定を行うことができる。一般的には、ＶＰＮ制御ノードは、利用可能なドメイン内ＶＰＮ情報を、コンパイルされたあるいは処理された、近隣ドメインに転送するのに適切なＶＰＮ情報にするように処理する。ドメイン同士が密接に関係している場合、例えば、同一のオペレータに属している場合、ＳＬＡは、ドメインＶＰＮ情報の交換時には全体として透過性を持たせることができる。他の場合には、ＶＰＮ制御ノード４３間を送信される、処理された情報２８をコンパイルされたＶＰＮ情報にするように処理することで、個々のドメインＶＰＮについてのかなり基本的なことだけしか明らかにならないようにすることができる。本実施形態における、ドメイン間接続１２Ａ－Ｇを介して送信されなければならない最低限の情報は、その情報を送信する境界ノード以外の別の場所で利用可能なＶＰＮのアイデンティティである。

【００２７】

ドメイン間接続１２Ａ－Ｇで送信される情報２８は、受信側ＶＰＮ制御ノードにおいて、全体として利用可能なＶＰＮ情報の状況の更新を引き起こすものである。このＶＰＮ制御ノードは、ここでも、例えば、どんなＶＰＮがドメイン間接続を介して利用可能であるかの情報を持っている。より完全な情報が利用可能である場合には、ＶＰＮ制御ノードは、例えば、これらの異なるＶＰＮのうちのどのＶＰＮで、エッジノードアイデンティティが利用可能であるか、ＶＰＭ品質のサービス等を判定することができる。こうして得られるＶＰＮ情報は、ここでは、近隣ドメインのプロパティとなる。また、ＳＬＡによって許可されている場合には、このＶＰＮ情報は、そのドメインのアクティビティに対して使用

することができる。ＶＰＮ制御ノード４３の記憶装置５４に記憶されている情報は、近隣ドメインから受信される情報、あるいはその処理されたもの、その受信される情報を追加、削除あるいは変更したものと同一とすることができる。例えば、この情報には、どのドメインから発信されているかの指示をラベルとして付加することができる。

【００２８】

この情報配信は、多くの連続ステップで継続することができる。いくつかの場合には、最初の送信と同様に、別のドメインに転送される前に、更なる情報の変更を適用する。最終的には、全体ＶＰＮプロバイダアーキテクチャ１におけるすべてのＶＰＮ制御ノードは、システム内で利用可能なすべてのドメインＶＰＮ情報の処理された形式のものを少なくとも持っている。各ＶＰＮ制御ノードでは、この情報は、使用対象の関係するドメイン間接続に対して有効となるＳＬＡに従って処理されても良い。

【００２９】

別の実施形態では、ドメイン間の情報配信は、ブロードキャストプッシュ方法で実行することができる。ドメインＶＰＮ情報は、近隣ドメインに制限されずに、システム全体の他のドメインの他のＶＰＮ制御ノードの１つ、いくつかあるいはすべてに直接送信される。これは、他の実施形態のように、チェイン（in a chain）でドメインＶＰＮ情報は転送されずに、単に、システムに渡ってブロードキャストされることを意味する。このような直接リクエスト転送の可用性は、ドメインＳＬＡによって調整することができる。

【００３０】

ドメインＶＰＮ情報の交換は、様々なタイミングで実行することができる。１つの構成は、利用可能な情報が常に更新されることを保証するために、このような情報を継続的にあるいは少なくとも定期的に交換する。このような実施形態では、この情報は、そのＶＰＮ制御ノード、あるいは、ＶＰＮ制御ノードから検索可能な場所にある任意の他のノードに記憶されることが好ましい。換言すれば、この構成は、データ配信用の典型的なプッシュメカニズムである。

【００３１】

別の構成には、いくつかのイベントによって起動される情報交換がある。このイベントは、例えば、なんらかの変更がドメインで発生すること、あるいは、以下で説明するような、特定のＶＰＮを検出するためのリクエストが発行されることである。換言すれば、この構成は、データ配信用に起動されたプッシュメカニズムとして説明することができる。

【００３２】

あるＶＰＮを検出するためのリクエストによって起動されることで情報が交換される場合、この交換される情報は、そのＶＰＮに制限されても良く、また、後に使用するために必要であるとしても記憶されなくても良い。この例には、データ配信用のプルメカニズムがある。

【００３３】

ここで、エッジノード１４’への新規のカスタマーサイト２０’の接続が、あるＶＰＮへ接続しようとすることを想定する。特定の実施形態では、この接続は、「プラグ－アンド－プレイ」処理を開始することになる。この処理は、自動的に、適切なＶＰＮを検出し、調整されたＶＰＮ構成をどのようにして配置するかを少なくとも示唆するものである。この制御ノード４３は、新規のカスタマーサイト２０’が接続されていることを特定し、かつどのＶＰＮが意図されているかを調査する。

【００３４】

ＶＰＮ制御ノード４３がＶＰＮ接続リクエストを開始する場合、それは、リクエストされたＶＰＮと、自身のドメイン間接続を介して利用可能なＶＰＮについての、記憶されている情報とを比較する。これらが一致する場合、一致することについての情報と、好ましくは、どのドメインにＶＰＮが存在し、かつどのドメイン間接続を介して、ＶＰＮが到達可能であるかについての情報を利用可能である。一実施形態では、利用可能である場合には、リクエストされたＶＰＮに接続されているエッジノードに到達するための経路が、リクエストしているＶＰＮ制御ノードに返信される。図４では、リクエストされたＶＰＮは

、図１のＶＰＮ２２Ａである。ドメイン１０ＥのＶＰＮ制御ノード４３は、２つの異なる経路に従って、境界ノード１８：１を介してＶＰＮ２２Ａが利用可能であることについての情報を持っている。ＶＰＮ２２Ａへ到達するための１つの構成は、ドメイン間接続１２Ｄ、ドメイン１０Ｂ、かつドメイン間接続１２Ａを経由するものである。ここでは、ＶＰＮ２２Ａは、ドメイン１０Ａに存在する。ＶＰＮ２２Ａへ到達するための別の構成は、ドメイン間接続１２Ｄ、ドメイン１０Ｂ、及びドメイン間接続１２Ｃを経由するものである。ここでは、ＶＰＮ２２Ａは、ドメイン１０Ｃに存在する。但し、ドメイン１０ＥのＶＰＮ制御ノード４３は、別の境界ノード１０を介するＶＰＮ２２Ａについての情報も持っている。ここで、リクエストされたＶＰＮ２２Ａは、ドメイン間接続１２Ｅを介して到達可能である。これは、ＶＰＮ２２Ａがドメイン１０Ｃで利用可能であるからである。そして、リクエストされたＶＰＮ２２Ａは、ドメイン間接続１２Ｇを介して到達可能である。これは、ＶＰＮ２２Ａがドメイン１０Ｄでも利用可能であるからである。

【００３５】

ＶＰＮ制御ノード４３は、リクエストされたＶＰＮを検出するために必要な情報をすべて持っている。この例では、ドメイン間接続１２Ｅを介する経路が使用するためには最も単純に見えるが、利用可能な品質のサービスレベルが、それについての決定を変更することができる。

【００３６】

この特定実施形態では、提供されたドメインＶＰＮ情報は、システム１全体のすべてのＶＰＮ制御ノード４３に配信される。この方法では、適切なＶＰＮを検出するためのリクエストは、「ホーム」ドメインのＶＰＮ制御ノード４３に直接出力することができる。ＶＰＮ情報の提供及び交換は、継続的に、定期的にあるいはリクエスト自身によって起動される前に指示することができる。

【００３７】

本発明の別の特定の実施形態が、図５に示される。ここで、初期のドメイン内ＶＰＮ情報の提供は、直前に実行される。但し、特定の実施形態では、ドメインＶＰＮ情報は、処理された形式でさえも、任意の近隣ドメインに向けてもたらせることはない。このことは、ＶＰＮ制御ノード４３が自身のドメインＶＰＮについての情報だけを持っていることを意味する。ＶＰＮ制御ノード４３が、自身が所有するドメイン１０ＥのＶＰＮ制御ノード４３の接続リクエストを開始する場合、自身が所有するデータベースで容易に利用可能な所有のドメインのＶＰＮについての情報だけを持つことになる。但し、ＶＰＮ制御ノード４３は、どのドメインが接続されているかを知っていて、また、ドメイン間接続１２Ａ－Ｇを介してそのリクエストを近隣ドメインに転送する。これについては、矢印３２によって示される。ドメイン間接続を介してこのようなリクエストを受信するＶＰＮ制御ノード４３は、自身が所有するデータベースを調査して、処理対象の任意のデータが存在するかを確認する。存在しない場合、ドメイン間接続を介する新規の転送が、リクエストされたＶＰＮについての情報が到達するまで発生する。そして、この情報は、オリジナルのドメイン１０ＥのＶＰＮ制御ノードへ返信されることになる。

【００３８】

特定の実施形態は、システム１全体が、単一のＶＰＮ制御ノード４３毎に更新されなければならないことがないという利点を持っている。但し、代わりに、ＶＰＮの検出は、なにかしらより複雑になることになる。

【００３９】

別の実施形態では、ＶＰＮ接続リクエストは、近隣ドメインに制限されない、システム全体の他のドメインの１つ、いくつかあるいは他のＶＰＮ制御ノードに直接送信される。このことは、他の実施形態のように、チェインでリクエストは転送されずに、単にシステム全体に渡ってブロードキャストされることを意味する。このような直接リクエスト転送の可用性は、ドメインＳＬＡによって調整することができる。

【００４０】

図６Ａは、本発明に従う、比較的一般的なＶＰＮ制御ノード４３の特定の実施形態のブ

ロック図である。ＶＰＮ制御ノード４３は、ドメインＶＰＮ情報を提供するための手段５２を備えている。この情報は、接続６２によってドメインの他のノードによって提供されても良い。メイン制御通信インタフェース４０は、他のドメインとの通信のために提供される。このインタフェース４０は、ドメイン内接続６２と一緒に構成されても良い。リクエストされたＶＰＮのアイデンティティがドメインＶＰＮ情報と一致（マッチ）するかを調査するマッチングユニット４９が提供される。ＶＰＮリクエストは、別のドメイン、あるいは所有のドメインの他のノードから受信することができる。あるいはＶＰＮ接続リクエストは、ＶＰＮ制御リクエストはＶＰＮ制御ノードで開始することができる。外部ＶＰＮ処理セクション４４は、ドメイン間ＶＰＮ構成を処理することを担当する。内部ＶＰＮ処理セクション４１は、所有のドメインの内部接続を構成するための機能を持っている。

【００４１】

図６Ｂは、本発明に従うＶＰＮ制御ノード４３の別の特定の実施形態のブロック図を示している。所有するドメインに関するドメインＶＰＮ情報は、内部ＶＰＮ処理セクション４１によって提供される。この内部ドメインＶＰＮ情報は、この特定の実施形態では、データメモリ５２に記憶されている。この情報は、この特定の実施形態では、矢印６２で示されるように、ドメインの他のノードとの通信によって提供される。他の実施形態では、この情報は、別の方法で取得することができる。内部ドメインＶＰＮ情報は、外部ＶＰＮ処理セクション４４内の総合ＶＰＮ情報データベース５４にも転送される。内部ＶＰＮ処理セクション４１も、内部構成マシーン４６を備えていて、これは、所有するドメインの内部接続を構成するための機能を持っている。内部ＶＰＮ処理セクション４１は、内部ドメインＶＰＮ情報と、データベース５４からの情報が提供される。つまり、内部ドメインに関する通信は内部ＶＰＮ処理セクション４１と外部ＶＰＮ処理セクション４４間の接続４２を介して実行される。

【００４２】

ＶＰＮ制御ノード４３は、ドメイン間接続を介する、他のドメインとのメイン制御通信インタフェース４０を持っている。他のドメインからのドメインＶＰＮ情報は、このインタフェース４０によって受信され、入力処理ユニット５６が、受信したデータから有用な情報を抽出し、この抽出した情報を入力データベース５８に記憶する。この入力データベース５８では、どのドメインから外部データが受信されたかのような追加の情報も記憶される。この入力データベース５８は、適切な場合に、総合ＶＰＮ情報データベース５４を更新する。外部ＶＰＮ処理セクション４４も、外部構成マシーン６０を備えていて、これは、ドメインに対して関連するドメイン関接続の一部を構成するための機能を持っている。この機能は、以下でより詳細に説明する。

【００４３】

外部ＶＰＮ処理セクション４４も、情報を他のドメインに提供する。所有するドメイン及び他のドメインの少なくとも一方に関連するドメインＶＰＮ情報は、データベース５４から抽出され、出力データ処理ユニット５０に提供される。取得された情報は、異なる近隣ドメインと関係するＳＬＡに従って処理され、出力データベース４８に記憶される。これによって、このＳＬＡは、どの情報が、異なる近隣ドメインに配信可能であるかを判定する。密接な関係を有するドメインオペレータは、情報交換をより透過にすることを許可しても良い。これに対して、関連しないオペレータに属するドメインは、より制限のある情報交換を適用することができる。適切な場合に、ＶＰＮについての情報は、インタフェース４０に送信される。

【００４４】

リクエストされたＶＰＮのアイデンティティがドメインＶＰＮ情報とマッチするかを調査するマッチングユニット４９が提供される。このＶＰＮリクエストは、別のドメインから、あるいは所有するドメインの別のノードから受信することができる。あるいは、ＶＰＮ接続リクエストをＶＰＮ制御ノード自身内で開始することができる。リクエストされたＶＰＮとＶＰＮ制御ノードのＶＰＮ情報がマッチ（一致）する場合、ドメイン間ＶＰＮの再構成を実行しなければならない。これについての実現は、様々な方法で実行することが

できる。典型的には、従来より知られている処理を使用する。例示する実施形態の１つを以下で説明する。ここでは、図４に示されるものと同様に、すべてのＶＰＮ情報がシステム全体に渡って配信されるものと想定する。

【００４５】

ユーザに対するＶＰＮ接続リクエストのマッチング後は、すべてのドメインのすべてのＶＰＮ制御ノードが、システム内でＶＰＮを検出するためのＶＰＮデータベースを持っている。各ドメインデータベースでは、ドメインに存在しない各ＶＰＮ　ＩＤに対する「ネクストホップ（nexthop）」情報が存在していて、これは、このＶＰＮ　ＩＤを検出することができる近隣ドメインＩＤを指摘する。近隣ドメインでは、このＶＰＮ　ＩＤに対して既に構成されているＶＰＮ、あるいはＶＰＮ　ＩＤを検出するための新規の「ネクストホップ」情報が存在する。ドメインの異なるデータベースでは、「ＶＰＮルーティングテーブル」として解釈することができる。これは、既に構成されているＶＰＮを検出する方法を示すものである。各「ネクストホップ」情報に対しては、異なるポリシールールが関連付けられて存在していても良い。このポリシールールによって、各ドメインのＶＰＮ制御ノードは、１つあるいはいくつかの「ネクストホップ」ドメインに対してＶＰＮ接続をセットアップすることを選択することができる。

【００４６】

図７に示される例は、ドメイン間ＶＰＮの構成をどのようにして自動化することができるかを示している。ドメイン１０Ｅの新規のカスタマーサイト２０’は、ＶＰＮ２２Ａに接続されても良い。ＶＰＮトンネルが、内側ドメインと、ドメイン間の両方に対するＶＰＮ接続に対して使用されると想定する。これは、以下のステップが採用される。

【００４７】

ドメイン１０ＥのＶＰＮ制御ノードは、いくつかの方法で、ＶＰＮ　２２Ａに接続するためのリクエストをカスタマーから取得する。ドメイン１０ＥのＶＰＮデータベースは、ＶＰＮ２２がドメイン１０Ｅに存在しないことを示しているので、ドメイン１０ＥのＶＰＮ制御ノードは、カスタマーサイト２０’を、ドメイン１０ＥのＶＰＮ２２Ａに直接接続することはできない。但し、接続リクエストと、他のドメインから発信されるＶＰＮ情報間ではマッチ（一致）が検出される。このデータベースは、ＶＰＮ２２Ａが、ドメイン１０Ａ、１０Ｃ及び１０Ｄで現在構成されていてかつ動作している「ネクストホップ」１０Ｂ、１０Ｃ及び１０Ｄで検出できることを示している。

【００４８】

ドメイン１０ＥのＶＰＮ制御ノードは、「ネクストホップ」１０Ｂだけを介してＶＰＮをセットアップすることを選択する。これは、カスタマーサイト２０’が接続されているエッジノード１４’から、リンク１２Ｄを介してドメイン１０Ｂに接続されている境界ノード１８：１への、ＶＰＮ２２Ａに対するＶＰＮトンネル７１をセットアップする。ドメイン１０ＥのＶＰＮ制御ノードは、ドメイン１０ＢのＶＰＮ制御ノードとの通信を開始し、かつリンク１２Ｄを介する境界ノード１８：２への、ＶＰＮ２２Ａに対するＶＰＮトンネル７２をセットアップする。ＶＰＮ２２Ａはドメイン１０Ｂに存在しないので、ドメイン１０ＢのＶＰＮ制御ノードは、自身のＶＰＮデータベースをチェックし、ＶＰＮ２２Ａが「ネクストホップ」１０Ａ及び１０Ｃを検出することができることを確認する。

【００４９】

ドメイン１０ＢのＶＰＮ制御ノードは、「ネクストホップ」１０Ａだけを介してＶＰＮをセットアップすることを選択する。これは、リンク１２Ｄを介してドメイン１０Ｂに接続される境界ノード１８：２から、リンク１２Ａを介してドメイン１０Ａに接続される境界ノード１８：３への、ＶＰＮ２２Ａに対するＶＰＮトランジット（通過）トンネル７３をセットアップする。ドメイン１０ＢのＶＰＮ制御ノードは、ドメイン１０Ａの制御ノードとの通信を開始し、リンク１２Ａを介する境界ノード１８：４へのＶＰＮトンネル７４をセットアップする。ＶＰＮ２２Ａがドメイン１０Ａに存在するので、ドメイン１０ＡのＶＰＮ制御ノードは、リンク１２Ａを介してドメイン１０Ｂに接続される境界ノードから、ＶＰＮ２２Ａへ接続されている境界ノード１８：５への内部トンネル７５をセットアッ

プすることができる。
【００５０】
各ステップの後、更新されたＶＰＮデータベースは、ＶＰＮ情報を次の回の収集のために利用可能となる。
【００５１】
本発明に従う方法の実施形態の基本ステップは、図８に示される。この処理は、ステップ２００で開始する。ステップ２１０で、接続リクエストが開始される。このリクエストは、第１ドメインで現在利用可能でないＶＰＮへ、第１ドメインの第１エッジノードを接続することに関するものである。ステップ２１２で、ドメインノード情報が収集される。ステップ２１４で、第１ＶＰＮのアイデンティティが、収集されたノード情報のＶＰＮアイデンティティとマッチングされる。このマッチングステップの結果に基づいて、ステップ２１６で、第１ＶＰＮは、第１エッジノードを備えるように構成される。この処理は、ステップ２９９で終了する。
【００５２】
上述の実施形態は、本発明のいくつかの例として理解されるべきである。様々な変形、組み合わせ及び変更の実施形態が、本発明の範囲から逸脱しないで実現できることが当業者には理解されるべきである。特に、様々な実施形態における異なる部分のソリューションが、技術的に可能な他の構成と組み合わせることができる。特に、プル／プッシュ、ドメイン内／間、ブロードキャスト／近隣通信、及び情報／リクエストの任意の組み合わせを適用することが可能である。ここで、本発明の範囲は、添付の請求項によって定義される。
【図面の簡単な説明】
【００５３】
【図１】仮想プライベートネットワークを提供するマルチドメイン通信ネットワークを示す図である。
【図２Ａ】本発明の実施形態に従うＶＰＮ情報収集を示す図である。
【図２Ｂ】本発明の他の実施形態に従うＶＰＮ情報収集を示す図である。
【図２Ｃ】本発明の他の実施形態に従うＶＰＮ情報収集を示す図である。
【図２Ｄ】本発明の他の実施形態に従うＶＰＮ情報収集を示す図である。
【図３Ａ】本発明のドメインのＶＰＮ制御ノード構成に従う実施形態を示す図である。
【図３Ｂ】本発明のドメインのＶＰＮ制御ノード構成に従う実施形態を示す図である。
【図３Ｃ】本発明のドメインのＶＰＮ制御ノード構成に従う実施形態を示す図である。
【図３Ｄ】本発明のドメインのＶＰＮ制御ノード構成に従う実施形態を示す図である。
【図４】本発明の実施形態に従うＶＰＮ情報転送及び接続リクエストを示す図である。
【図５】本発明の別の実施形態に従うＶＰＮ情報転送及び接続リクエストを示す図である。
【図６Ａ】本発明に従う一般的なＶＰＮ制御ノードの実施形態を示すブロック図である。
【図６Ｂ】本発明に従う一般的なＶＰＮ制御ノードの別の実施形態を示すブロック図である。
【図７】本発明の一実施形態に従うＶＰＮ構成を示す図である。
【図８】本発明に従う方法の実施形態の主要なステップを示すフロー図である。

【図１】

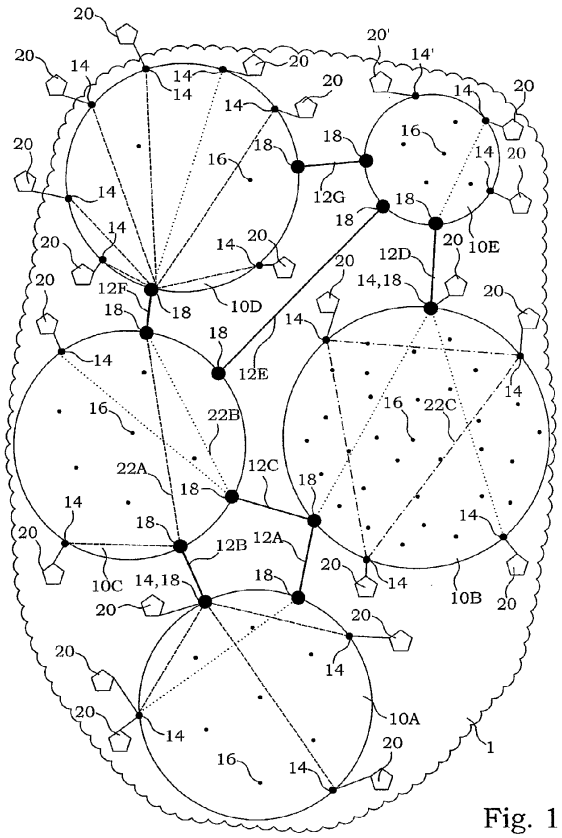

Fig. 1

【図２Ａ】

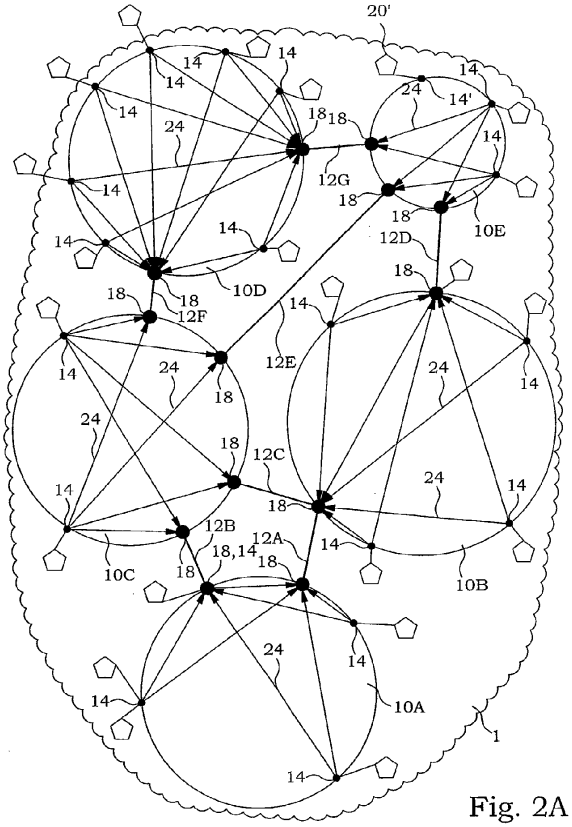

Fig. 2A

【図２Ｂ】

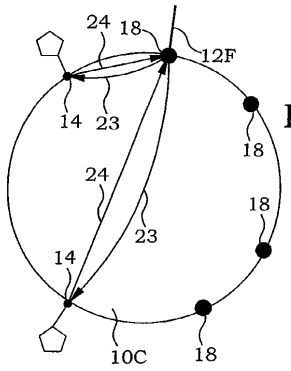

Fig. 2B

【図２Ｄ】

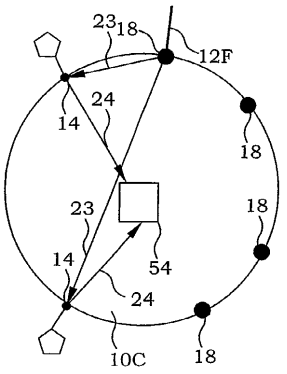

Fig. 2D

【図２Ｃ】

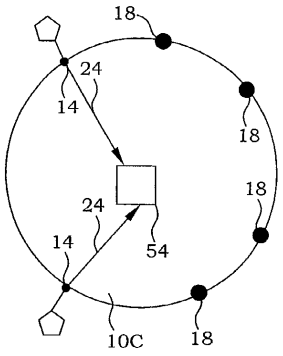

Fig. 2C

【図３Ａ】

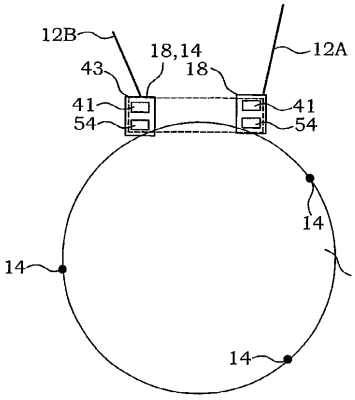

Fig. 3A

【図３Ｂ】

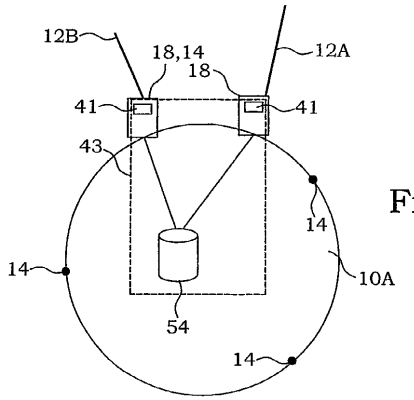

Fig. 3B

【図３Ｃ】

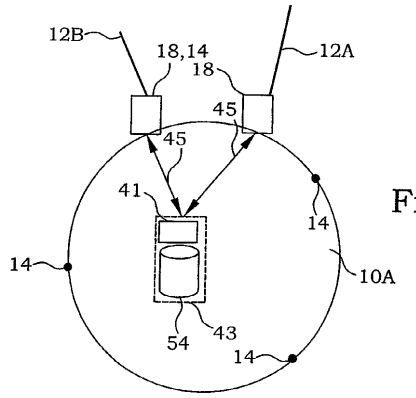

Fig. 3C

【図３Ｄ】

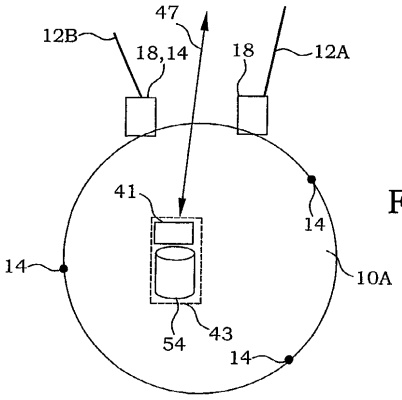

Fig. 3D

【図４】

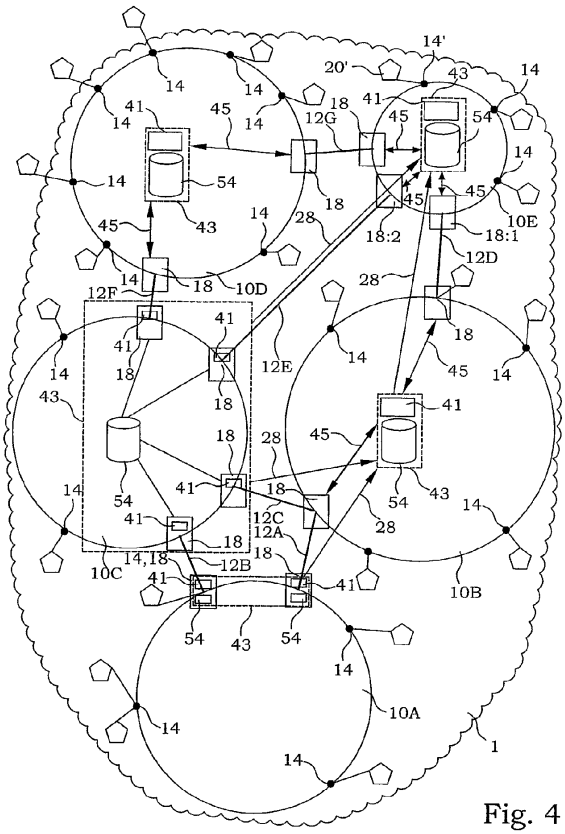

Fig. 4

【図５】

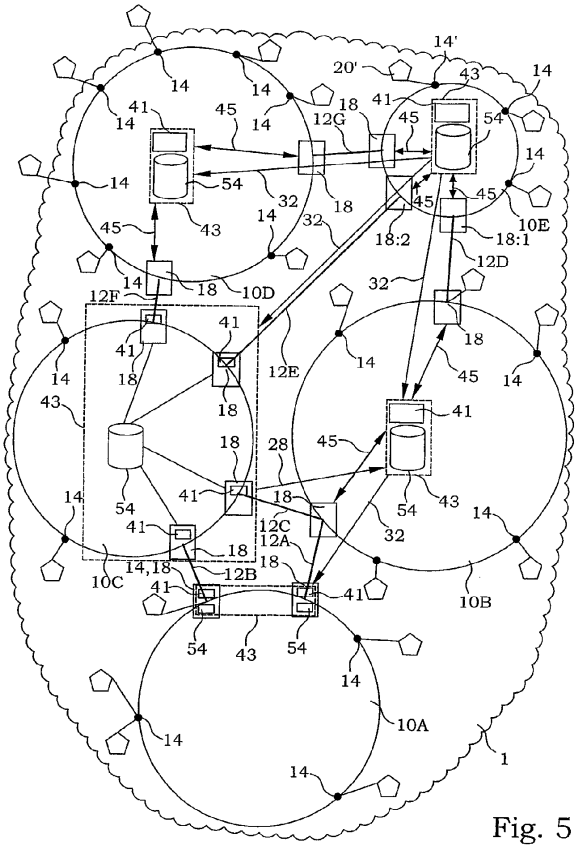

Fig. 5

【図６Ａ】

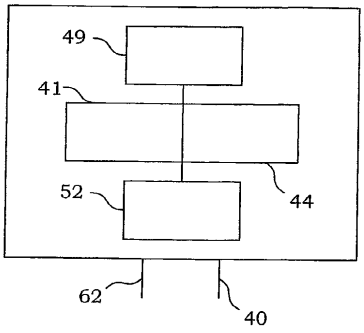

Fig. 6A

【図６Ｂ】

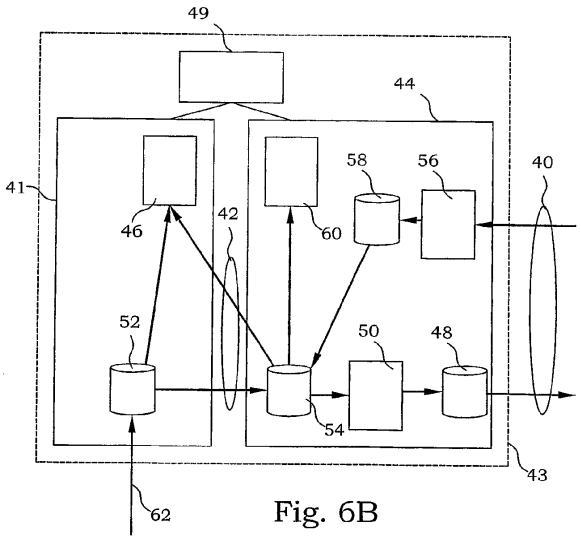

Fig. 6B

【図７】

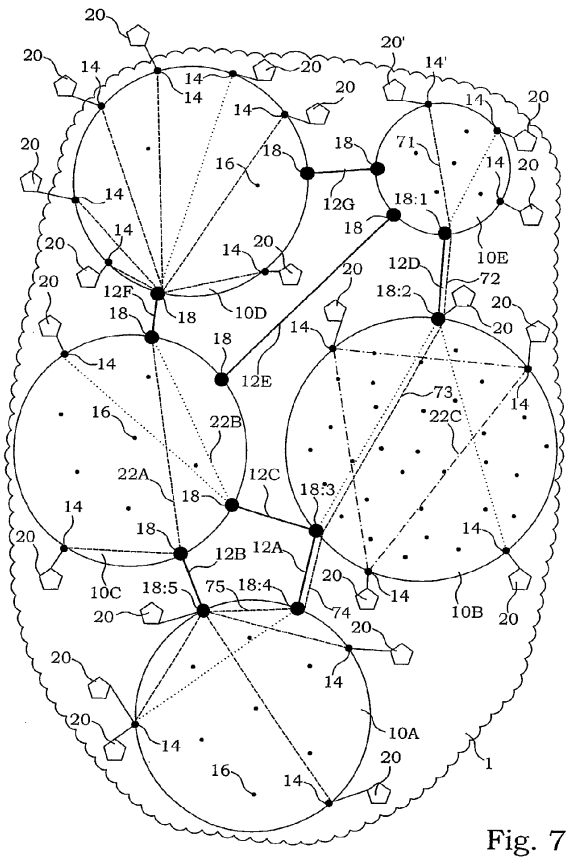

Fig. 7

【図８】

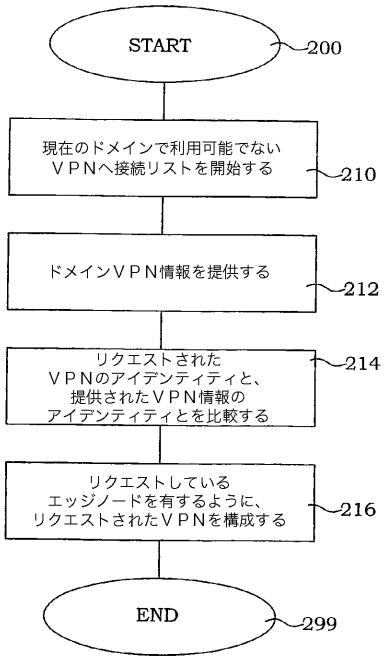

Fig. 8

フロントページの続き

(72)発明者　フリンタ，　クリストフェル
スウェーデン国　　ストックホルム　エス－１１８　６３，　スケルドガタン　４
(72)発明者　モングス，　ヤン－エリク
スウェーデン国　ソルナ　エス－１７０　７２，　ビェールンスティゲン　３６
(72)発明者　ヴェストベリ，　ラーシュ
スウェーデン国　エンチェピング　エス－７４５　９６，　ロングトラ

審査官　齋藤　浩兵

(56)参考文献　特開２００２－３３５２７４（ＪＰ，Ａ）
特開２００４－１５８９７１（ＪＰ，Ａ）
特開２００１－３２６６９３（ＪＰ，Ａ）
岡山聖彦 他，階層型ＶＰＮのためのＬＤＡＰサーバを用いた経路制御手法，情報処理学会論文誌　第４５巻　第１号，２００４年１１月　５日，p.46～55
岡山聖彦 他，代理ゲートウェイを用いたＳＯＣＫＳベースの階層的ＶＰＮ構成法，情報処理学会論文誌　第４２巻　第１２号，２００１年１２月１５日，p.2860～2868

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　12/56