(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2011-501623
(P2011-501623A)
(43)公表日　平成23年1月6日(2011.1.6)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	***(2006.01)***	H04L	12/56	B	5K030
H04L 12/66	***(2006.01)***	H04L	12/66	A	

審査請求 未請求　予備審査請求 未請求　（全 26 頁）

(21)出願番号　特願2010-531285 (P2010-531285)
(86)(22)出願日　平成20年10月24日 (2008.10.24)
(85)翻訳文提出日　平成22年6月22日 (2010.6.22)
(86)国際出願番号　PCT/US2008/081186
(87)国際公開番号　WO2009/055717
(87)国際公開日　平成21年4月30日 (2009.4.30)
(31)優先権主張番号　60/982,388
(32)優先日　平成19年10月24日 (2007.10.24)
(33)優先権主張国　米国 (US)

(71)出願人　510114675
ドイチユ，ジヨナサン・ピーター
アメリカ合衆国、カリフオルニア・９２８８６、ヨーバ・リンダ、ラ・コンセツタ・ドライブ・４０４１
(71)出願人　510114686
サン，ダニー・テ－アン
アメリカ合衆国、カリフオルニア・９２６８８、ランチヨ・サンタ・マルガリータ、ビスタ・バランカ・１０
(74)代理人　110001173
特許業務法人川口國際特許事務所

最終頁に続く

(54)【発明の名称】仮想ＩＰアドレスを割り当てるための中央ステーションのための種々の方法および装置

(57)【要約】
仮想ＩＰアドレスを割り当てるための中央ステーションのための方法、装置、システムを説明する。デバイスサービスマネージャサーバ（ＤＳＭ）は、２つ以上のデバイスサービスコントローラ（ＤＳＣ）と協働するように構成されたネットワークアクセスモジュールを有する。ＤＳＭは、各ＤＳＣが常駐するローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのための通信をプロキシするために、ネットワークデバイスに仮想ＩＰアドレスを割り当てて指定するための中央管理ステーションとしての機能を果たす。ＤＳＭは、割り当てられたＶＩＰアドレスに関連付けられた通信がルーティングされているＬＡＮ上のネットワークデバイスから外側に位置する。ＤＳＭは、ＤＳＭのレジストリ内に記憶されている対応するＤＳＣおよびネットワークデバイスの情報に基づいて、仮想ＩＰアドレスを各ＤＳＣに割り当てて、割り当てられた仮想ＩＰアドレスからＬＡＮ上の宛先ネットワークデバイスまでのルートを確立する。

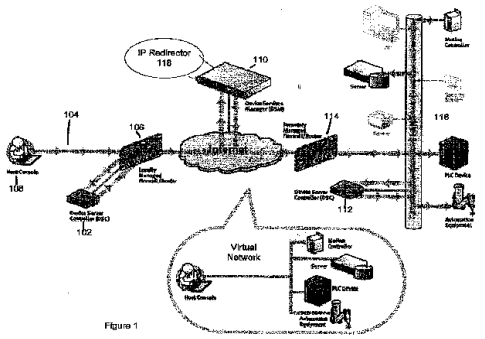

Figure 1

【特許請求の範囲】
【請求項１】
２つ以上のデバイスサービスコントローラ（ＤＳＣ）と協働するように構成されたネットワークアクセスモジュールを有するデバイスサービスマネージャサーバ（ＤＳＭ）を備え、ＤＳＭが、各ＤＳＣが常駐するローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのための通信をプロキシするために、ネットワークデバイスに仮想ＩＰアドレスを割り当てて指定するための中央管理ステーションとしての機能を果たし、ＤＳＭが、割り当てられたＶＩＰアドレスに関連付けられた通信がルーティングされているＬＡＮ上のネットワークデバイスから外側に位置し、ＤＳＭが、ＤＳＭのレジストリ内に記憶されている対応するＤＳＣおよびネットワークデバイスの情報に基づいて、第１の仮想ＩＰアドレスを第１のＤＳＣ割り当てて、第１の仮想ＩＰアドレスから宛先ネットワークデバイスまでのルートを確立する、装置。
【請求項２】
ＤＳＭ内のネットワークアクセスモジュールが、１）各ＤＳＣの固有識別子とＤＳＣに割り当てられたローカルネットワークからの仮想ＩＰアドレスとの組を作成し、また２）宛先ネットワークデバイスの実ＩＰアドレスと第２のローカルエリアネットワーク上の宛先ＤＳＣの固有識別子との組を作成するように構成され、ＤＳＭがこれらの組をＤＳＭのレジストリにおいて記憶する、請求項１に記載の装置。
【請求項３】
ＤＳＭが、ＤＳＭのレジストリ内に、少なくとも各ＤＳＣおよびローカルエリアネットワーク上で、ローカルエリアネットワークのユーザにより可視であるものと指定される、ネットワークデバイスの実ＩＰアドレス、仮想ＩＰアドレス、デバイスへのルートを記憶する仮想ＩＰアドレスルーティングテーブルを有し、ＤＳＭが、仮想ＩＰアドレスルーティングテーブル内の情報を使用して、ＤＳＭによって割り当てられた仮想ＩＰアドレスを所与のＤＳＣに関連付けられた実ＩＰアドレスにマッピングしてルートを確立する、請求項１に記載の装置。
【請求項４】
ＤＳＣの固有の識別子が、各ＤＳＣに関連付けられた固有ＩＤまたはＤＳＣに割り当てられたＭＡＣアドレスとすることができ、ネットワークデバイスが、高域エリアネットワーク上のＤＳＭの位置に対してローカルエリアネットワーク上のファイアウォールの背後に位置する、請求項２に記載の装置。
【請求項５】
ＤＳＭのネットワークアクセスモジュールが、第１のＤＳＣにどの仮想ＩＰアドレスがローカルネットワーク内で利用可能であるかを発見し、それらの仮想ＩＰアドレスをＤＳＭ内のアソシエーションマネージャに報告するように命令するために、コードでスクリプト化され、ＤＳＣがローカル自動アドレスサーバを使用してＶＩＰアドレスを取得し、その後、ＶＩＰアドレスをＤＳＭ内のアソシエーションマネージャにコピーする、請求項１に記載の装置。
【請求項６】
ネットワークアクセスモジュールが、ＤＳＣにＤＨＣＰを使用してＤＳＣによってＤＳＭに対して予め識別されたＶＩＰアドレスのプールからＶＩＰアドレスをピックアップするように命令し、ネットワークアクセスモジュールが、実ＩＰアドレスを割り当てられたＶＩＰアドレスとマッピングしてＤＳＭのレジストリ内にそのアソシエーションを記憶することができるように、ＶＩＰルーティングテーブル内のルーティング情報を自動的に更新する、請求項３に記載の装置。
【請求項７】
アソシエーションの組が、接続がアクティブである間記憶されており、その後、組を必要とする新規のアクティブな接続に置換されるまで記憶された組のキューに配置され、使用頻度が最も低い順に上書きされる、請求項６に記載の装置。
【請求項８】

ＤＳＭ内のネットワークアクセスマネージャが、仮想ＩＰアドレスを指すドメインネームを設定するために、動的ＤＮＳを介するアドレスマッピングサービスを使用してドメインネームからリモート対象デバイスへのルートを確立し、第１のＤＳＣに割り当てられた仮想ＩＰアドレスとその固有ＩＤの指定された組を第２のＤＳＣに割り当てられたＩＰアドレスとドメインネームに関連付けられたその固有ＩＤとの組にマッピングする、請求項１に記載の装置。

【請求項９】

ＤＳＭ内のネットワークアクセスマネージャが、ドメインネームサーバと協働して、ＤＮＳ内の１つ以上のアドレス記録を更新し、ドメインネームからＩＰアドレスへの転換を自動的に行うことができ、ＤＮＳがＤＳＭによって通信可能に接続され、動作され、各アクティブな接続に対して仮想ＩＰアドレスを作成する、請求項１に記載の装置。

【請求項１０】

ＤＳＭ内のネットワークアクセスマネージャがドメインネームサーバと協働し、ＤＮＳがＤＮＳのクエリが発生した時にのみ仮想ＩＰアドレスを割り当てる必要があり、第１のＤＳＣがそのＬＡＮ内で利用可能なＶＩＰアドレスのプールを予め割り当てて、その後、ＶＩＰアドレスのプールをＤＳＭに送信し、ＤＳＭが、必要に応じて、プールからＶＩＰアドレスエントリを割り当てて使用する、請求項１に記載の装置。

【請求項１１】

第１のＤＳＣが、そのＬＡＮ内で利用可能なＶＩＰアドレスのプールを予め割り当てて、その後、ＶＩＰアドレスのプールをＤＳＭに送信し、ＤＳＭが、仮想ＩＰアドレスを割り当てるために、未知のパブリックＩＰアドレスからの要求に対して使用されるＶＩＰアドレスの小さいプールと、ＤＳＣに登録されている知られているＩＰアドレスからの要求に対して使用されるＶＩＰアドレスの大きいプールとの２つのプールを維持する、請求項１に記載の装置。

【請求項１２】

ＤＳＭ内のネットワークアクセスモジュールが各ＤＳＣ内のネットワークマニホールドと協働して各ＤＳＣに対する仮想ＩＰアドレスを設定し、その後、任意の対象デバイス上の任意のポートへのＴＣＰ／ＩＰ接続を処理することができ、ネットワークマニホールドがＤＳＣが常駐するＬＡＮのためにＶＩＰアドレスプールを管理するように構成される、請求項１に記載の装置。

【請求項１３】

各デバイスサービスコントローラ（ＤＳＣ）が常駐し、第１のＤＳＣが第１のローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのために通信をプロキシするようなＬＡＮ上で２つ以上のＤＳＣと協働するステップと、

第１のＤＳＣに、各ＤＳＣが常駐するＬＡＮから外側に位置するデバイスから利用可能なローカル仮想ＩＰアドレスを取得するように命令するステップと、

第１のＤＳＣが常駐する第１のローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのための通信をプロキシするために、仮想ＩＰアドレスをネットワークデバイスに割り当てて指定するステップと、

第２のＤＳＣに、各ＤＳＣが常駐するＬＡＮから外側に位置するデバイスから利用可能なローカル仮想ＩＰアドレスを取得するように命令するステップと、

第２のＤＳＣが常駐する第２のローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのための通信をプロキシするために、仮想ＩＰアドレスをネットワークデバイスに割り当てて指定するステップと、

第１のＤＳＣに割り当てられた仮想ＩＰアドレスとデバイス内の第１のＤＳＣに関するある固有の識別情報との第１の組を記憶するステップと、

第２のＤＳＣに割り当てられた仮想ＩＰアドレスとデバイス内の第２のＤＳＣに関するある固有の識別情報との第２の組を記憶するステップと、

デバイス内に記憶されている情報の記憶された組に基づいて、割り当てられた仮想ＩＰアドレスから所与のＤＳＣに関連付けられたＬＡＮ上の宛先ネットワークデバイスまでの

ルートを確立するステップとを含む、方法。
【請求項１４】
１）各ＤＳＣの固有識別子とＤＳＣに割り当てられたローカルネットワークの仮想ＩＰアドレスとの組、２）ホストＤＳＣコントローラの固有識別子と、第１のローカルエリアネットワーク上のＤＳＣの固有識別子に関連付けられたホストコンソールネットワークデバイスの実ＩＰアドレスとの組、および３）宛先ネットワークデバイスの実ＩＰアドレスと第２のローカルエリアネットワーク上の宛先ＤＳＣの固有識別子との組を作成するステップと、
これらの組をデバイスのレジストリ内に記憶するステップと、
これらの記憶された組をマッピングして、第１のＤＳＣから宛先ネットワークデバイスまでのルートを確立するステップとをさらに含む、請求項１３に記載の方法。
【請求項１５】
ローカルネットワーク内で利用可能な仮想ＩＰアドレスの２つ以上のプールであって、未知のパブリックＩＰアドレスからの要求に対して使用されるＶＩＰアドレスの小さいプールとＤＳＣに登録されている知られているＩＰアドレスからの要求に対して使用されるＶＩＰアドレスの大きいプールとを作成するステップをさらに含む、請求項１４に記載の方法。
【請求項１６】
２つ以上のデバイスサービスコントローラ（ＤＳＣ）と通信を確立し、各ＤＳＣが常駐するローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのための通信をプロキシするために、ネットワークデバイスに仮想ＩＰアドレスを割り当てて指定するための中央管理ステーションとしての機能を果たすように構成されたネットワークアクセスモジュールを有するデバイスサービスマネージャサーバ（ＤＳＭ）であって、割り当てられたＶＩＰアドレスに関連付けられた通信がルーティングされているＬＡＮ上のネットワークデバイスから外側に位置するＤＳＭと、
２つ以上のＤＳＣのうちの第１のＤＳＣであって、ＤＳＭが第１のＤＳＣに第１のＤＳＣが常駐するローカルエリアネットワーク内の利用可能なローカル仮想ＩＰアドレスを取得し、これらの利用可能なローカル仮想ＩＰアドレスをＤＳＭに報告するように命令し、ＤＳＭが、ＤＳＭのレジストリ内に記憶されている対応するＤＳＣおよびネットワークデバイスの情報に基づいて、第１の仮想ＩＰアドレスを第１のＤＳＣに割り当てて、第１のＤＳＣに割り当てられた第１の仮想ＩＰアドレスから宛先ネットワークデバイスまでのルートを確立するような第１のＤＳＣとを備える、システム。
【請求項１７】
ＤＳＭ内のネットワークアクセスモジュールが、１）各ＤＳＣの固有識別子とＤＳＣに割り当てられたローカルネットワークの仮想ＩＰアドレスとの組、２）ホストＤＳＣコントローラの固有識別子と、第１のローカルエリアネットワーク上のＤＳＣの固有識別子に関連付けられたホストコンソールネットワークデバイスの実ＩＰアドレスとの組、および３）宛先ネットワークデバイスの実ＩＰアドレスと第２のローカルエリアネットワーク上の宛先ＤＳＣの固有識別子との組を作成するように構成され、ＤＳＭがこれらの組をＤＳＭのレジストリ内に記憶し、ネットワークデバイスが高域エリアネットワーク上のＤＳＭの位置に対してローカルエリアネットワーク上のファイアウォールの背後に位置する、請求項１６に記載のシステム。
【請求項１８】
ＤＳＣが、ローカル自動アドレスサーバを使用してＶＩＰアドレスを取得し、その後、ＶＩＰアドレスをＤＳＭ内のアソシエーションマネージャにコピーし、アソシエーションマネージャがＤＳＭ内のＶＩＰルーティングテーブルを更新する、請求項１６に記載のシステム。
【請求項１９】
ネットワークアクセスモジュールが、ＤＳＣにＤＨＣＰを使用してＤＳＣによってＤＳＭに対して予め識別されたＶＩＰアドレスのプールからＶＩＰアドレスをピックアップす

るように命令し、ネットワークアクセスモジュールが、実ＩＰアドレスを割り当てられたＶＩＰアドレスとマッピングしてＤＳＭのレジストリ内にそのアソシエーションを記憶することができるように、ＶＩＰルーティングテーブル内のルーティング情報を自動的に更新し、アソシエーションの組が、接続がアクティブである間記憶されており、その後、組を必要とする新規のアクティブな接続に置換されるまで記憶された組のキューに配置され、使用頻度が最も低い順に上書きされる、請求項１６に記載のシステム。

【請求項２０】

ドメインネームサーバ（ＤＮＳ）をさらに備え、ＤＳＭ内のネットワークアクセスマネージャがＤＮＳと協働し、ＤＮＳがＤＮＳのクエリが発生した時にのみ仮想ＩＰアドレスを割り当てる必要があり、第１のＤＳＣがそのＬＡＮ内で利用可能なＶＩＰアドレスのプールを予め割り当てて、その後、ＶＩＰアドレスのプールをＤＳＭに送信し、ＤＳＭが、必要に応じて、プールからＶＩＰアドレスエントリを割り当てて使用する、請求項１６に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本出願は、米国特許出願シリアル番号第６０／９８２，３８８号、２００７年１０月２４日出願、「Ｍｅａｎｓ ｏｆ ｐｒｏｖｉｄｉｎｇ ｖｉｒｔｕａｌ ＩＰ ａｄｄｒｅｓｓ ｔｏ ａｕｔｏｍａｔｉｃａｌｌｙ ａｃｃｅｓｓ ｒｅｍｏｔｅ ｎｅｔｗｏｒｋ ｄｅｖｉｃｅｓ」の優先権を主張するものである。

【０００２】

著作権

本願の開示の一部は、著作権保護対象の素材を含む。著作権所有者は、ソフトウェアエンジンおよびそのモジュールのいずれかによる複製再生に対して、それが特許商標局の特許ファイルまたは記録内で見られる時には異議はないが、それ以外の場合には、如何なる形であれ全ての著作権の権利を有する。

【０００３】

本発明の実施形態は、概して、ネットワークデバイスに関する。より詳細には、本発明の一実施形態の一態様は、仮想インターネットプロトコル（ＩＰ）アドレスの自動割り当てのための中央管理ステーションに関する。

【背景技術】

【０００４】

インターネットは、あるネットワーク上のデバイスが同じネットワークまたはリモートネットワーク上にあり得る他のデバイスと自動的に通信できるように、ＴＣＰ／ＩＰプロトコルスイートを共同で使用するネットワークの大きな集合である。このような各デバイスは、各々のアクティブなネットワークインタフェースに対してＩＰアドレスが割り当てられており、このＩＰアドレスによりネットワークインフラのコンポーネントが宛先のデバイス間のトラフィックを自動的にルーティングすることができる。

【０００５】

このような各ネットワークインタフェースは、ＩＰアドレスの複数のブロックがローカルネットワークの外側で利用可能である必要のないインタフェース上で使用するために確保されていても、インターネット全体にわたって固有のＩＰアドレスを割り当てられることが一般的に必要である。このようなプライベートアドレスは、ローカルネットワーク上のデバイスからのトラフィックがリモートネットワーク上のルーティング不可能なアドレスを有するネットワークインタフェースに到達できるようにルート（すなわち、ネットワークインフラデバイス群を通るパス）を確立することができないため、「ルーティング不可能な」アドレスとも呼ばれる。インターネットが普及したので、この技術によりプライベートアドレスを繰り返し再使用することができるようになり、このことが公的にアクセス可能なＩＰアドレスの不足しつつある状況を緩和するのに役立っている。しかし、管理者がルーティング可能なアドレスを持たないリモートデバイスにアクセスできる代替の機

構を求めたために、この技術はより複雑なものとなった。
【０００６】
インターネットが普及し、セキュリティ脅威が増大したため、ネットワーク管理者はさらに、ネットワーク管理者が要求通りに許可されるアクセスまたは拒否されるアクセスの特定のアドレスとポートの組み合わせを指定することができるようなネットワークフィルタリングデバイスまたはアプリケーションを開発および展開することによって、管理制御の下で特定のデバイスへのアクセスの制限しようとしてきた。これら２つの技術は、一緒になってインターネットの普及および安定を確保するのに役立つが、そのことでより一層複雑になり、管理者はその管理制御の範囲外のネットワーク上のネットワークデバイスにシームレスにアクセスすることを望むことができない。
【０００７】
この問題に対処するための１つの既存の機構は、ローカルネットワークデバイスに専用クライアントソフトウェアをインストールすることを含む。このソフトウェアにより、ローカルネットワークデバイスは「仮想プライベートネットワーク（ＶＰＮ）」の一部として機能することができ、ローカルデバイスはリモートネットワークのメンバであるかのように機能することができる。このようなＶＰＮシステムを使用すると、ローカルホストはリモートネットワーク上のＩＰアドレスが割り当てられ、リモートネットワーク上のホストに対する（ｔｏ　ａｎｄ　ｆｒｏｍ）全てのトラフィックがＶＰＮシステムによって自動的にルーティングされる。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
この技術は有効であるが、アプローチには複数の欠点がある。ＶＰＮシステムは、まず、リモートネットワークの管理者によって設定されなければならない。設定されると、ＶＰＮシステムにアクセスを望む各々の外部デバイスに特殊なソフトウェアがインストールされなければならない（インストールされない場合、システムは、例えば、ウェブブラウザインタフェース経由で制限されたアクセスのみを提供することができる）。さらに、適切なセキュリティ証明書がリモート管理者によって作成され、ローカル管理者またはユーザによって配布され維持されなければならない。これらは全て、操作に関与する当事者全員に重要な管理上の負担をかけるものである。最後の欠点は、ローカルホストがＶＰＮアクセスを許可されると、通常は、リモートネットワーク上の全てのデバイスにアクセスするのを防ぐために追加のフィルタリングステップが行われなければ、全てのデバイスにアクセスしてしまう。これは、リモート管理者に望まれない場合もある。
【０００９】
ルーティング不可能なアドレスの問題を克服する別の技術は、いわゆる「ネットワークアドレス変換（ＮＡＴ）」を実行することである。このＮＡＴは、ネットワークのアドレス／ポートの組み合わせをルーティング可能なアドレスからルーティング不可能なアドレスに自動的にマッピングする境界ルータの複雑な再構成を含む。この技術により、１つの公的にルーティング可能なＩＰアドレスを使用することでルーティング不可能なアドレスを有する複数のデバイスにアクセスすることができるが、システムはより複雑になる。ＮＡＴ対応のネットワークは、一般には、特定のポート／アドレスの組み合わせから特定のデバイスへのマッピングが予め構成されていなければ、着信接続できない。また、このマッピングはデフォルト設定のアドレス／ポートの組または非標準的なアドレス／ポートの組み合わせの使用を試みるソフトウェアと競合する場合がある。
【００１０】
これらの課題を考えると、専用のホストソフトウェアを使用せずに、またリモートネットワークのネットワーク管理者がソリューションを設定、維持、または操作するための特権を必要とせずに、ルーティング不可能なアドレスを使用してリモートデバイスに簡単に、かつ自動的にアクセスできるようにする機構が必要である。このようなシステムが生成され展開されるとすると、主な課題は、システムにより使用するための適切なローカル仮

想ＩＰアドレスを自動的に生成し、割り当て、維持できる能力ということになる。
【課題を解決するための手段】
【００１１】
仮想ＩＰアドレスを割り当てる中央ステーションのための方法、装置、システムを説明する。デバイスサービスマネージャサーバ（ＤＳＭ）は、２つ以上のデバイスサービスコントローラ（ＤＳＣ）と協働するように構成されたネットワークアクセスモジュールを有する。ＤＳＭは、各ＤＳＣが常駐するローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのための通信をプロキシするために、ネットワークデバイスに仮想ＩＰアドレスを割り当てて指定するための中央管理ステーションとしての機能を果たす。ＤＳＭは、割り当てられたＶＩＰアドレスに関連付けられた通信がルーティングされているＬＡＮ上のネットワークデバイスから外側に位置する。ＤＳＭは、ＤＳＭのレジストリ内に記憶されている対応するＤＳＣおよびネットワークデバイスの情報に基づいて、仮想ＩＰアドレスを各ＤＳＣに割り当てて、割り当てられた仮想ＩＰアドレスからＬＡＮ上の宛先ネットワークデバイスまでのルートを確立する。
【００１２】
図面は本発明の実施形態を参照したものである。
【図面の簡単な説明】
【００１３】
【図１】ファイアウォールにより保護されたネットワーク内のネットワークデバイスに対してアクセスするシステムの一実施形態を示すブロック図である。
【図２ａ】第１のファイアウォールにより保護された第１のドメインおよび第２のファイアウォールにより保護された第２のドメインの外部にデバイスサービスマネージャを配置するシステムの一実施形態を示すブロック図である。
【図２ｂ】ＤＳＭに対して自身の認証を行い、ＤＳＭへの発信ＴＣＰ／ＩＰストリーム接続を確立し、その後、確立されたＴＣＰ／ＩＰストリーム接続上で将来の双方向通信に対して接続をオープンに保つことにより、ＤＳＭへの直接通信トンネルを提供するように構成されたコンジットマネージャを各々が有するＤＳＣを備えたシステムの一実施形態を示すブロック図である。
【図３】中央ＤＳＭとファイアウォールにより保護されたネットワーク内のネットワークデバイスに対してアクセスするローカルＤＳＣとを有するシステムの一実施形態を示すブロック図である。
【図４】ＤＳＣ内のコンジットマネージャの一実施形態の状態図である。
【図５】分散システムの自動化集中型管理の一実施形態のブロック図である。
【図６】ＤＳＭの一実施形態の例を示すブロック図である。
【図７】ＤＳＣの一実施形態の例を示すブロック図である。
【図８】ＤＳＣ内の実行可能な起動ファイルを介して構成情報をＤＳＣに配布するＤＳＭの一実施形態を示すブロック図である。
【図９】仮想ＩＰアドレスの割り当てを自動化するＤＳＭの一実施形態を示すブロック図である。
【図１０】仮想ＩＰアドレスを取得してＤＳＭに報告するネットワークマニホールドの一実施形態を示すフロー図である。
【図１１】ローカルネットワーク内で利用可能な仮想ＩＰアドレスの２つ以上のプールを作成するＤＳＭを示す図である。
【発明を実施するための形態】
【００１４】
本発明は、さまざまな変更や代替の形態が可能であるが、本発明の特定の実施形態が図面に例として示されており、これについて本明細書内で詳細に説明する。本発明は、開示された特別な形態に限定されるものではないと理解されるべきであるが、一方で、本発明は、本発明の精神およびその範囲内にある全ての変更、等価物、代替形態を含めるものとする。

【００１５】
以下の説明では、本発明を十分に理解できるように、多くの特定の詳細事項、例えば、特定のデータ信号、指定コンポーネント、接続、ネットワークなどの実施例が説明されている。しかしながら、本発明はこれらの特定の詳細事項がなくても実施可能であることは当業者には明らかである。他に、本発明を不必要に分かりにくくするのを避けるために、知られているコンポーネントまたは方法は詳細に説明されず、ブロック図で説明される。また、第１のネットワークなどのように特定の番号参照がなされてもよい。しかしながら、特定の番号参照は、文字通りの順番として解釈すべきではなく、第１のネットワークは第２のネットワークと異なるものであると解釈すべきである。したがって、説明される特定の詳細事項は単なる例にすぎない。特定の詳細事項は変わる場合があるが、それでも本発明の精神および範囲内にあるように考慮される。
【００１６】
概して、２つ以上のリモートデバイスに仮想ＩＰアドレスを割り当てて指定する中央システムを提供するための種々の方法および装置を説明する。デバイスサービスマネージャサーバ（ＤＳＭ）は、２つ以上のデバイスサービスコントローラ（ＤＳＣ）との通信を確立するように構成されたネットワークアクセスモジュールを有し得る。ＤＳＭは、各ＤＳＣが常駐するローカルエリアネットワーク（ＬＡＮ）上のネットワークデバイスのための通信をプロキシするために、ネットワークデバイスに仮想ＩＰアドレスを割り当てて指定するための中央管理ステーションとしての機能を果たす。ＤＳＭは、割り当てられたＶＩＰアドレスに関連付けられた通信がルーティングされているＬＡＮ上のネットワークデバイスから外側に位置する。ＤＳＭは、各ＤＳＣに、ＤＳＣが常駐するローカルエリアネットワーク内の利用可能なローカル仮想ＩＰアドレスを取得するように命令する。ＤＳＣは、次に、これらの利用可能なローカル仮想ＩＰアドレスをＤＳＭに報告する。ＤＳＭは、ＤＳＭのレジストリ内に記憶されている対応するＤＳＣおよびネットワークデバイスの情報に基づいて、仮想ＩＰアドレスを所与のＤＳＣに割り当てて、第１のＤＳＣに割り当てられた仮想ＩＰアドレスから宛先ネットワークデバイスまでのルートを確立する。
【００１７】
ＤＳＭ内のネットワークアクセスモジュールは、１）各ＤＳＣの固有識別子とＤＳＣに割り当てられたローカルネットワークの仮想ＩＰアドレスとの組、２）ホストＤＳＣコントローラの固有識別子と、第１のローカルエリアネットワーク上のＤＳＣの固有識別子に関連付けられたホストコンソールネットワークデバイスの実ＩＰアドレスとの組、および３）宛先ネットワークデバイスの実ＩＰアドレスと第２のローカルエリアネットワーク上の宛先ＤＳＣの固有識別子との組の例を作成するように構成され得る。ＤＳＭはこれらの組をＤＳＭのレジストリ内に記憶する。
【００１８】
図１は、ファイアウォールにより保護されたネットワーク内のネットワークデバイスに対してアクセスするシステムの一実施形態を示すブロック図である。
【００１９】
第１のネットワーク１０４上の第１のデバイスサービスコントローラ１０２（ＤＳＣ）は、第１のファイアウォール１０６により保護されている。第１のネットワーク１０４は、第１のＤＳＣ１０２に関連付けられたホストコンソール１０８を含んでもよい。ホストコンソール１０８は、第２のファイアウォール１１４により保護されている第２のネットワーク１１６内の機器のサブセットを制御および管理する。第２のネットワーク１１６は、第１のネットワーク１０４およびホストコントローラ１０８からのインターネット上に位置する。第１のネットワーク１０４上の第１のデバイスサービスコントローラ１０２と第２のネットワーク１１６上の第２のデバイスサービスコントローラ１１２とは、インターネット上に位置するデバイスサービスマネージャサーバ（ＤＳＭ）１１０と協働して、ファイアウォール１０６、１１４を介して第２のネットワーク１１６上の機器の一部への高度に安全なリモートアクセスを提供する。デバイスサービスマネージャサーバ１１０は、ファイアウォール１０６、１１４を介して、各デバイスサービスコントローラとの直接

通信トンネル経由でマシン間の通信を実行するコードを含むＩＰリダイレクタプログラム１１８を有する。第２のネットワーク１１６内の機器のサブセットは、例えば、サーバ、ＰＬＣデバイス、動作コントローラ、自動化装置、プリンタ、セキュリティシステム、パーソナルコンピュータを含むことができる。

【００２０】

動作時に、ユーザはホストコンソール１０８から、ホストコントローラモードで動作しているローカルＤＳＣ、すなわち第１のＤＳＣ上の指定ポートへの接続をオープンにする。このローカルＤＳＣは、接続を承認し、対象デバイスへの接続が確立するまで接続を保留状態に保つ。このローカルＤＳＣは、次に、制御ＤＳＭ１１０への接続を開始し、ＤＳＭ１１０は対応する管理されたデバイスのＩＰアドレスおよびポートにその接続をマッピングする。ローカルＤＳＣは、ＤＳＭ１１０に対して自身の認証を成功させるためにその識別情報を送信する。対象デバイスに関与する関連ＤＳＣ、すなわち、第２のＤＳＣ１１２は、定期的にＤＳＭ１１０との安全なトンネルをオープンにし、保留中の接続があるか否かを判断する。保留中の接続がある場合、ＤＳＭ１１０は、ＤＳＭ１１０へのプロキシ接続を開始するようにＤＳＣに命令し、そのプロキシ接続に保留中の接続のトラフィックを通過させる。ファイアウォールの背後にあるローカルＤＳＣは、保留中の接続がある場合、ＤＳＭ１１０との直接通信トンネルをオープンに保つ。

【００２１】

第１のＤＳＣ１０２とＤＳＭ１１０との間の直接通信トンネルと第２のＤＳＣ１１２とＤＳＭ１１０との間の直接通信トンネルとが結合して、ファイアウォールにより保護されているネットワークの外側のデバイスからファイアウォールにより保護されているネットワーク内にある機器の安全なアクセスおよび管理を可能にすると同時に、ネットワークのＩＴポリシーおよびネットワークファイアウォールのインテグリティを維持することができる。第１のＤＳＣ１０２および第２のＤＳＣ１１２に対する接続点は、直接通信トンネルを介する通信のセキュリティを強化するために、ＤＳＣ１０２、１１２は各ファイアウォール１０６、１１４の背後に配置されるので、ネットワーク外部のデバイスに対して各ネットワークの外側で公的に公開されない。ローカルＤＳＣがＤＳＭ１１０に対して認証を成功させると、ＤＳＣはすぐに、関与しているＤＳＣに対して可視であると指定されたネットワーク内の任意のデバイス、例えば、ＰＬＣデバイスに対する安全なアクセスを開始することができる。指定された可視デバイスは、公開される第２のネットワーク１１６のユーザにより認証されたデバイスである。

【００２２】

上述したように、関連する可視デバイスは、ドメインの所有者によって仮想デバイスネットワークＶＤＮに対して可視である／公開されることを認証されたデバイスである（すなわち、ＶＤＮは、可視であると認証された第１および第２のネットワーク１０４、１１６内の機器を含む）。ＶＤＮに対して情報が可視的に公開されていると認証されている第２のネットワーク内の機器のサブセットの例には、サーバ、ＰＬＣデバイス、動作コントローラ、自動化装置が含まれるが、プリンタ、セキュリティシステム、パーソナルコンピュータはＶＤＮに対して可視であることがユーザによって認証されていない。

【００２３】

ローカルＤＳＣは、そのネットワーク内のコンポーネントを発見し、ドメインの所有者にグラフィックユーザインタフェースで提示して、所有者が情報を可視／公開を望むのはどのネットワークコンポーネントであるかを尋ねる。ローカルＤＳＣは、この情報を収集し、この情報を記憶し、ＬＡＮ上のネットワークデバイスの公開情報をＤＳＭに送信する。この情報は、ＤＳＣのネットワーク内のＤＳＣの識別子およびＩＰアドレス、各コンポーネントのＩＰアドレス、名前、機能、サポートされるプロトコルなどを含むことができる。

【００２４】

図６は、ＤＳＭの実施形態の一例を示すブロック図である。ＤＳＭ１１０は、ＤＳＭ６１０内のトンネルマネージャを含むＩＰリダイレクタ６１８、ユーザインタフェース、レ

ジストリを含むデータベース６２０、アソシエーションマネージャ、ポリシーマネージャ、複製マネージャなどのコンポーネントおよび他の同様のコンポーネントを含むことができる。

【００２５】

図７は、ＤＳＣの実施形態の一例を示すブロック図である。ＤＳＣ７０２は、アソシエーションマネージャ、コンジットマネージャ７２４、トンネルマネージャ、ネットワークマニホールド７２６のコンポーネントを含むアクセスサブシステムなどのコンポーネントを含むことができる。ＤＳＣはさらに、レジストリを含むローカルデータベース７２８、ディスカバリマネージャ７３０、デバイス構成マネージャ、デバイス監視マネージャ、デバイス構成エンジン７４３を含む自動化サブシステム、ユーザインタフェース、電源７３２、ドライブポート７３４、他の同様のコンポーネントを含むことができる。

【００２６】

図９は、仮想ＩＰアドレスの割り当てを自動化するＤＳＭの一実施形態のブロック図である。ＤＳＭ９１０は、ネットワークアクセスマネージャとトンネルマネージャとを含むネットワークアクセスモジュールを有する。これらは、２つ以上のデバイスサービスコントローラ（ＤＳＣ）と協働して、各ＤＳＣ９０２、９１２が常駐するローカルエリアネットワーク上のネットワークデバイスのための通信をプロキシするためにネットワークデバイスに仮想ＩＰアドレスを割り当てて指定するための中央管理ステーションとして機能するように構成されている。ＤＳＭ９１０は、ＶＩＰアドレスに関連付けられた通信がルーティングされているＬＡＮ上のネットワークデバイスから外側に配置される。したがって、ＤＳＭ９１０は、中央ＤＳＭ９１０からのこれらの仮想ＩＰアドレスの構成および割り当てを自動化し、そのためにユーザは仮想アドレスを機能させるのにホスト側では何もする必要がない。ＤＳＭ９１０は、仮想ＩＰアドレスを所与のＤＳＣに割り当てて、ＤＳＭのレジストリ９２２内に記憶された対応するＤＳＣおよびネットワークデバイス情報に基づいて、割り当てられた仮想ＩＰアドレスから宛先のネットワークデバイスへのルートを確立する。ネットワークデバイスは、高域エリアネットワーク上のＤＳＭ９１０の位置に対してローカルネットワーク上のローカルファイアウォール９１４などのファイアウォールの背後に配置され得る。

【００２７】

ＤＳＭ９１０上で、ＶＤＮ管理者は手動で仮想ＩＰアドレスの組（すなわち、ホストコントローラＤＳＣのＩＤと割り当てられたローカル仮想ＩＰアドレス）を指定して、宛先デバイス（すなわち、対応するデバイスコントローラＤＳＣのＩＤと割り当てられたローカル仮想ＩＰアドレスの組）へのルーティングを行うことができる。あるいは、ＤＳＣはどの仮想ＩＰアドレスがそのローカルネットワーク内で利用可能であるかを発見して、それらのＩＰアドレスをＤＳＭ９１０に報告することができる。ＤＳＭ９１０内のネットワークアクセスモジュールは、１）各ＤＳＣの固有識別子（ＩＤ）とＤＳＣに関連付けられたローカルネットアークの仮想ＩＰアドレスとの組を作成する。また、ＤＳＭ９１０内のネットワークアクセスモジュールは、２）ホストＤＳＣコントローラの固有識別子と第１のローカルエリアネットワーク上のＤＳＣに固有識別子に関連付けられたホストコンソールネットワークデバイスの実ＩＰアドレスとの組と、３）宛先ネットワークデバイスの実ＩＰアドレスと第２のローカルエリアネットワーク上の宛先ＤＳＣの固有識別子との組を作成する。次に、ＤＳＭ９１０内のネットワークアクセスモジュールは、ＤＳＭのレジストリ９２２内に、ＤＳＮ９１０のＶＩＰルーティングテーブル内のこれらの組を記憶する。組は、ローカルネットワークの仮想ＩＰアドレスとそのローカルネットワークのＤＳＣの固有識別子との組とすることもでき、また他にローカルネットワーク上のネットワークデバイスとそのローカルネットワークに関連付けられた仮想ＩＰアドレスとの組とすることも可能である。このルーティング情報は、パケットのヘッダ部の既存のパケットルーティング情報のトップに追加される。

【００２８】

ＤＳＭ９１０は、アプリケーションが対象ポートを変更する必要がない、または異なる

ポートを使用するように再構成される必要もないので、ドメインネームシステム９３８などの自動アドレスマッピングサービスと統合されてもよい。管理者は仮想ＩＰアドレス（ＶＩＰ）を指すドメインネームを設定するだけでよく、ユーザアプリケーションは全く変わらない。

【００２９】

ＶＩＰルーティングテーブル９２２はさらに、ＶＩＰアドレス、ＶＩＰアドレスと固有ＩＤとの組、デバイスへのルート、および同様の情報を記憶することもできる。また、仮想ＩＰアドレスルーティングテーブル９２２は少なくとも、１）各ＤＳＣの実ＩＰアドレスとローカルエリアネットワークのユーザによって可視であると指定されたローカルエリアネットワーク上のネットワークデバイス（ＤＳＣに登録される）、２）ＤＳＣの仮想ＩＰアドレスとＤＳＣに登録されているネットワークデバイス、３）デバイスへの接続ルート、４）ＤＳＣの全ての公開情報とそれらの関連の可視ネットワークコンポーネント、５）接続終端ポイント、現在の接続、ホスト情報、同様の情報、を記憶することができる。仮想ＩＰアドレスルーティングテーブル９２２は、ＤＳＭ９１０のレジストリの一部を形成する。次に、ＤＳＭ－ＤＳＣシステムは、この記憶された情報を使用して、ＤＳＭ９１０によって割り当てられた仮想ＩＰアドレスを各ＤＳＣに関連付けられた、または各ＤＳＣの背後の実ＩＰアドレスにマッピングして、発信元のネットワークデバイスと宛先デバイスとの間のルートを確立することができる。概して、ＤＳＭ９１０は、実アドレスがＮＡＴされているか否かに関係なく、仮想ＩＰアドレスから実ＩＰアドレスへのマッピングを自動化する。ＤＳＣデバイスは自身と任意の関連ネットワークデバイスとの両方をＤＳＭレジストリ９２２に登録し、定期的にその情報を更新するように構成されていることに留意されたい。また、ローカルＤＳＣ９１２は、ＤＳＭ９１０からのトラフィックを受信し、その後、実際に第１のネットワークデバイス９５３などの宛先の対象デバイスの関連する実ＩＰアドレスにトラフィックをルーティングする。

【００３０】

ＤＳＭ９１０内の組作成のためのＤＳＣの固有識別子は、各ＤＳＣにハードコードされた固有ＩＤ、ＤＳＣに割り当てられたＭＡＣアドレス、またはＤＳＣに割り当てられた実ＩＰアドレスとしてもよい。しかしながら、ＤＳＣに割り当てられたＭＡＣアドレスまたは実ＩＰアドレスは、将来的に変化する可能性があり、したがって、固有ＩＤ以上の管理が必要となる。

【００３１】

ＤＳＭ９１０のネットワークアクセスモジュールは、ホストＤＳＣコントローラ９０２にどの仮想ＩＰアドレスがそのローカルネットワーク内で利用可能であるかを見つけ、これらのＶＩＰアドレスをＤＳＭ９１０内のアソシエーションマネージャに報告するように命令するためにスクリプト化されたコードを有する。ＤＳＣ９０２は、ローカル自動アドレスサーバ９４０（例えば、ＤＨＣＰ）を使用して、ＶＩＰアドレスを取得し、その後、ＶＩＰアドレスをＤＳＭ９１０内のアソシエーションマネージャにコピーすることができる。

【００３２】

図１０は、ＤＳＣ内の仮想ＩＰアドレスを取得しＤＳＭへ報告するネットワークマニホールドの一実施形態にフロー図である。

【００３３】

図９、図１０では、ブロック１０４４の動作で、ＤＳＣがまずＤＳＭと通信し、その後、定期的に以下ように行う時に、ＤＳＭは自動的に、例えば、ＤＨＣＰを使用して、ホストＤＳＣコントローラ９０２のネットワークマニホールドにローカルＶＩＰアドレスを取得するように命令する。次に、ＤＳＣ９０２のネットワークマニホールドは、１）接続が発生する都度、または２）ブロック１０４５における効率性のために、ＶＩＰアドレスをピックアップするのにローカル自動アドレスサーバ９４０を使用して、ＤＳＣ９０２よりＤＳＭ９１０に対してこのローカルＬＡＮ内の利用可能なＶＩＰであると予め識別されたＶＩＰアドレスのプールからＶＩＰアドレスをピックアップする。ブロック１０４６では

、ＤＳＣのネットワークマニホールドは、ローカル自動アドレスサーバ９４０（例えば、ＤＨＣＰ）を使用して、ＶＩＰアドレスを取得し、その後、ＶＩＰアドレスをＤＳＭ９１０にコピーする。ＤＳＭ９１０は中央ＤＳＭ９１０からのこれらの仮想ＩＰアドレスの構成を自動化し、そのために、ユーザはこれらの仮想ＩＰアドレスを機能させるのにホスト側では何もする必要がない。ネットワークアクセスモジュールは、次に、ＶＩＰルーティングテーブル９２２内のルーティング情報を更新して、実ＩＰアドレスを割り当てられたＶＩＰアドレスと相関させ／マッピングし、ＤＳＭレジストリ９２２内のアソシエーション、場合によっては、ドメインネームをＶＩＰアドレスに関連付けるドメインネームサーバ９３８内のアソシエーションを記憶することができる。

【００３４】

一実施形態では、アソシエーションはＶＩＰルーティングテーブル９２２内に永久的に記憶される。一実施形態では、アソシエーションの組は、接続がアクティブである間、ＶＩＰルーティングテーブル９２２内に一時的に記憶されており、その後、組を必要とする新規のアクティブな接続に置換されるまで記憶された組、例えば、１００個の記憶された組のキューに配置され、使用頻度が最も低い順に上書きされる。

【００３５】

上述したように、ホストＤＳＣ９０２はＤＳＭ９１０に問い合わせを行うことができる、または直接ＤＮＳ９３８に問い合わせを行うことができる。ホストＤＳＣ９０２は、ＤＮＳ９３８に正確な仮想ＩＰアドレスを問い合わせることができる、またはＶＩＰルーティングテーブル９２２に問い合わせることにより正確な仮想ＩＰアドレスを取得することができる。ホストＤＳＣ９０２は、ＤＳＣに割り当てられた新規のＶＩＰアドレスに接続する。クエリを受信する際に、ＤＳＣ９１０内のネットワークアクセスマネージャは、自動アドレスマッピングサービス９３８（すなわち、動的ＤＮＳ）を介して、ドメインネームからリモート対象デバイスへのルートを確立することができる。自動マッピングサーバ９３８は、仮想ＩＰアドレスを指すドメインネームを設定して、トラフィックを発信元のネットワークデバイス（すなわち、ホストコントローラＤＳＣのＩＤと割り当てられたローカル仮想ＩＰアドレスとの組）から宛先デバイス（すなわち、対応するデバイスコントローラＤＳＣのＩＤと割り当てられたローカル仮想ＩＰアドレスとの組）にマッピングする。したがって、ＤＳＭ９１０は、第１のＤＳＣ９０２に割り当てられた仮想ＩＰアドレスとその固有ＩＤの指定された組を第２のＤＳＣ９１２に割り当てられた仮想ＩＰアドレスとドメインネームに関連付けられたその固有ＩＤとの組にマッピングする。ＤＳＭ９１０内のネットワークアクセスマネージャは、ドメインネームサーバと協働して、任意にＤＮＳ９３８内の１つ以上のアドレス記録を更新し、ドメインネームからＩＰアドレスへの転換を自動的に行うことができる。一実施形態では、インターネット上のコンピューティングデバイスを識別するために、ドメインネームは数字のＩＰアドレスにマッピングされる英数字の名前とすることができる。したがって、発信元のネットワークデバイスは、宛先デバイスに向かうトラフィックのドメインネームを入力するだけでもよい。

【００３６】

ＤＮＳ９３８が接続され、ＤＳＭ９１０によって動作され、各々のアクティブな接続のために仮想ＩＰアドレスを作成する。複数のデバイスからの個々のポートを１つのパブリックＩＰアドレスに転送するのではなく、各ＤＳＣ９０２、９１２内のネットワークマニホールドと協働するＤＳＭ９１０内のネットワークアクセスモジュールが各リンクおよび各ＤＳＣ宛ての仮想ＩＰアドレスを設定するので、任意の対象デバイス上の任意のポートへのＴＣＰ／ＩＰ接続を処理することができる。アプリケーションはそれらの対象とするポートを変更する必要もなく、異なるポートを使用するように構成される必要もないので、このソリューションは容易にドメインネームシステムに統合される。仮想ＩＰアドレスを指すドメインネームを設定するだけでよく、ユーザアプリケーションは全く変更されない。

【００３７】

動作上、ＤＮＳサーバ９３８は、ＤＮＳのクエリが発生した時に仮想ＩＰアドレスを割

り当てる必要となるだけである。各ＤＳＣ９０２、９１２は、そのＬＡＮ内で利用可能なＶＩＰアドレスのプールを予め割り当てて、その後、ＶＩＰアドレスのこのプールをＤＳＭ９１０に送信する。ＤＳＭ９１０は、必要に応じて、プールから自由にＶＩＰアドレスエントリを割り当てて使用する。ＤＳＣが必要とする情報は単に、プールからＶＩＰアドレスを割り当てるか再要求するかである。

【００３８】

明らかなＤｏＳ攻撃を防ぐために、ＤＳＭ９１０は仮想ＩＰアドレスを割り当てるために２つのプールを維持する。ＶＩＰアドレスの小さいプールは、未知のパブリックＩＰアドレスからの要求に対して使用され、ＶＩＰアドレスの大きいプールは、ＤＳＣに登録されている知られているＩＰアドレスからの要求に対して使用される。接続が確立されると、接続の開始点のパブリックＩＰアドレスは自動ホワイトリストプール内に配置され、その後、長いタイムアウトを有することができる。

【００３９】

ホワイトリスト内のエントリはさらに、接続が終了した後、ホワイトリストプールからエントリを自動的に削除する指数関数的減衰のタイマを有することができる。

【００４０】

図１１は、ローカルネットワーク内で利用可能な仮想ＩＰアドレスの２つ以上のプールを作成するＤＳＭの図である。

【００４１】

図１１では、ブロック１１５０の動作で、ＤＳＭ内のネットワークアクセスモジュールは、ＤＮＳのクエリ時に、仮想ＩＰアドレスがホストＤＳＣに割り当てられているか否かを確認するためにチェックする。

【００４２】

はいの場合、つまり仮想ＩＰアドレスが現在ホストＤＳＣに割り当てられている場合、ネットワークアクセスモジュールは仮想ＩＰアドレスをホストＤＳＣに送信する。

【００４３】

いいえの場合、つまり仮想ＩＰアドレスが現在ホストＤＳＣに割り当てられていない場合、ブロック１１５４で、ネットワークアクセスモジュールは、クエリがパブリックＩＰアドレスからのものであるか、またはクエリがＤＮＳクエリのホワイトリストからのものであるかをチェックする。

【００４４】

はいである場合、つまりクエリが登録されているパブリックＩＰアドレスまたはホワイトリストからのものである場合、ネットワークアクセスモジュールは、ホストＤＳＣの利用可能ＩＰアドレスの大きいプールから仮想ＩＰアドレスを割り当てる。

【００４５】

いいえである場合、つまりクエリが知られているパブリックＩＰアドレスまたはホワイトリストからのものでない場合、ネットワークアクセスモジュールは、ホストＤＳＣの利用可能ＩＰアドレスの小さいプールから仮想ＩＰアドレスを割り当てる。

【００４６】

ここで、仮想ＩＰアドレスがホストＤＳＣに割り当てられる。

【００４７】

ブロック１１５６で、ＤＳＭのネットワークアクセスモジュールは、クエリに応答して仮想ＩＰアドレスを送信する。

【００４８】

図９では、ＤＳＭ９１０内のネットワークアクセスモジュールは、ＤＳＣからのトンネル要求時に、要求のパブリックＩＰアドレスをホワイトリストに追加し、その後、そのパブリックＩＰアドレスをトンネルディスパッチャに送信する。

【００４９】

介在するファイアウォールまたはＮＡＴデバイス側にネットワーク管理者の介入は必要なく、またホストデバイスにこのモードを使用するための構成変更の必要もないが、ネッ

トワーク管理者は所望のＤＮＳドメイン（すなわち、ローカルネットワーク）のサブドメインを作成し、その後、そのサブドメインをＤＳＭ９１０に委譲するか、またはＤＳＭ９１０が動的ＤＮＳを更新できるようにする必要があることに留意されたい。

【００５０】

図７では、上述したように、各ＤＳＣ７０２は、ＤＨＣＰ経由のＩＰアドレスの１つ以上のプール、ポートマネージメント、ＤＨＣＰサーバを管理維持するように構成されたネットワークマニホールド７２６を有する。ＤＳＣ７０２内のネットワークマニホールド７２６は、ＤＨＣＰサーバと、仮想ＩＰアドレスのコレクションを維持するための仮想ＩＰプールマネージャと、ポートのプールを維持するためのポートプールマネージャとからなる。　ＤＳＣ７０２内のネットワークマニホールド７２６は、ＩＰアドレスをドメインネームにマッピングする時に、ＤＳＭ９１０によって使用するための仮想ＩＰアドレスのプールを維持するのに関与する。

【００５１】

ＤＳＣ７０２内のネットワークマニホールド７２６は、その動作のために複数の値を維持する：

ｐｏｏｌ．ｍａｘは、ＤＳＣ７０２が一度に保存するＩＰアドレスの最大数（自身を除いて）を示し、

ｐｏｏｌ．ｌｏｗｍａｒｋは、（ｐｏｏｌ．ｍａｘに達しない限り）常に保存しているＩＰアドレス数を示し、

ｐｏｏｌ．ｉｎｕｓｅは、現在使用中のＩＰアドレス数を示す。

【００５２】

ＤＳＣ７０２内のネットワークマニホールド７２６は、ＤＳＭ内のネットワークアクセスモジュールと通信して、プールインユースの合計を得る。さらに、ＤＳＣ７０２内のネットワークマニホールド７２６は、終了のために使用中の各ＩＰアドレスの使用量をＤＳＭに問い合わせることができなければならない。

【００５３】

ＤＳＣ７０２は、宛先に関する追加の情報は必要としない。実際に、ＤＳＣ７０２は、トンネルの最終の宛先に関する情報を持たない。

【００５４】

ＤＳＣ７０２内のトンネルマネージャ７２５は、ネットワークマニホールド７２６および多重（ＭＵＸ）およびＤｅＭＵＸモードの両方の他の内部プロセスと通信して、トンネルトラフィックを案内する。ＭＵＸモードにより、ＤＳＣの関連ネットワークデバイスは他のドメイン内の別のＤＳＣの関連ネットワークデバイスと通信できる。ＤＥＭＵＸモードは、トンネリングされたトラフィックをＤＳＭからローカルドメイン内の関連ネットワークデバイスにリダイレクトする。ＭＵＸモードは、２つの関連プログラムを有することができる。ポートＭＵＸは、ローカルポート（ｔｃｐ／ｕｄｐ）をＤＳＭ９１０へトンネリングする。仮想ＩＰＭＵＸは、仮想ＩＰアドレスへのトラフィックをＤＳＭ９１０へトンネリングする。

【００５５】

トンネルＭＵＸマネージャ７２５は、ローカルＬＡＮからＤＳＣ上での接続（ＴＣＰ／ＵＤＰ）を承認する。Ｎｅｔｆｉｌｔｅｒ／ＩＰテーブルを使用することによって、ＤＳＣ上の全ての仮想インタフェースが１つのトンネルＭＵＸマネージャデーモンにリダイレクトされることができる。

【００５６】

次に、ＭＵＸマネージャは、Ｎｅｔｆｉｌｔｅｒインタフェースに目的の宛先の問い合わせを行って仮想ＩＰを決定することができる。ＤＳＭトンネルマネージャへの接続時に、ＭＵＸマネージャは仮想宛先ＩＰ、仮想宛先ポート番号、ローカルＤＳＣのＤＮＡのＩＤを送信することができる。

【００５７】

この情報に基づいて、ＤＳＭはパケットが実際に進む意図があるかを決定し、その後、

接続をプロキシすることができる。

【００５８】

ＭＵＸＴＣＰトンネルハンドラは、いくつかの初期ヘッダをＤＳＭに送信する。その後、ｔｃｐ＿ｒｅｌａｙ３と同じ機能を実行する。

【００５９】

トンネルＤＥＭＵＸマネージャのタスクは非常に単純である。接続を受信し、認証を行う時に、トンネルＤＥＭＵＸマネージャは初期ヘッダ情報を読み出して、パケットタイプと宛先とを決定する。トンネルＤＥＭＵＸマネージャは、次に、実際の中継タスクを実行するために、ｔｃｐ＿ｒｅｌａｙエージェントかｕｄｐ＿ｒｅｌａｙエージェントのいずれかを生成する。

【００６０】

このようにして、ＤＳＭ９１０は、統合されたファイアウォールと顧客ＮＡＴルータとの背後で動作する各ＤＳＣの複数の関連デバイスのためのプロキシアクセスポイントとして機能する。

【００６１】

図６では、ＤＳＭ６１０のグラフィックユーザインタフェース６５１も、ＤＳＭの管理者が個々のデバイスのアソシエーションを指定するように構成されている。このアソシエーションは、既存のデバイス構成と特定の発見されたＤＳＣデバイスとの組として定義される。デバイスがＤＳＭのレジストリ６２０内で関連付けられると、ＤＳＭ６１０は適切な構成変更を加えることができ、ＤＳＭ６１０のＩＰリダイレクタモジュール６１８内で維持されているアクセスルールのプリセットセットによりネットワーク機器のＤＳＣへのプロキシ接続の転送を開始する。

【００６２】

検出されたＤＳＣが発見され登録されると、グラフィックユーザインタフェース６５１のデバイス監視サービスビュー内に適切なアイコンが現れ得る。その後、ユーザは各々の登録されたデバイスを以前作成構成された記録と関連付けることができる。これが行われれば、さらなるデバイス設定（検索記録のディスカバリを含む）がＤＳＣデバイスに自動的にダウンロードされることができる。次に、これらの設定に基づいて、ＤＳＣは追加のネットワークデバイスを発見してトラフィックを通過させるのを開始する。

【００６３】

ＤＳＭ６１０内のユーザデータ複製マネージャ６４５は、データがＤＳＣからＤＳＭに複製される機構を提供する。ＤＳＭ６１０内のユーザデータ複製マネージャ６４５は、ＤＳＣの構成記録を含むデバイス構成ファイルのローカルコピーを生成する。ＤＳＣはＳＳＨで実装された安全な通信チャネルを使用してデバイス構成ファイルのローカルコピーを中央レジストリ６２０からフェッチし、その後、ＤＳＣはデバイス構成ファイルのそのローカルに記憶されたコピーを更新する。したがって、シャドウ構成レジストリがリモート管理されたＤＳＣデバイス上で維持される。次に、ＤＳＣは更新が完了したことをＤＳＭ６１０に信号で伝え、ＤＳＭ６１０がＤＳＭ６１０の中央レジストリ６２０内のリモート構成のＤＳＣの状態を更新する。

【００６４】

図２ａは、第１のファイアウォールにより保護された第１のドメインおよび第２のファイアウォールにより保護された第２のドメインの外部にデバイスサービスマネージャサーバを配置するシステムの一実施形態を示すブロック図である。

【００６５】

各ＤＳＣ２０２、２１２は、ハードウェア論理およびソフトウェアを使用して、１）ホストコントローラ（第１のファイアウォール２０６の範囲外に配置されるＤＳＭ２１０に対してホストコントローラと第１のドメイン２０４内の関連デバイスとの接続を確立する）、２）デバイスコントローラ（ＤＳＭ１１０から第２のファイアウォール２１４により保護されている第２のドメイン２１６内の個々のリモート対象デバイスへの着信接続を受信および管理する）の両方として機能するように構成される。ドメインはファイアウォー

ルにより分割された任意のネットワークまたはさまざまなサブネットとすることができることに留意されたい。ＤＳＣは、ローカルドメインの範囲外に配置される親ＤＳＭに対する自身と関連デバイスとの両方の接続をプロキシすることができることになる。各ＤＳＣは、保留中のＴＣＰ接続が待機中であるか否かを確認すべくＤＳＭに確認するために定期的にアウトバウンド通信を送信するように構成され得る。

【００６６】

一実施形態では、第１のＤＳＣ２０２および第２のＤＳＣ２１２は、ＤＳＭ２１０に対して自身の認証を行い、ＤＳＭ２１０への発信ＴＣＰ／ＩＰストリーム接続を確立することによりＤＳＭ２１０への直接ネットワーク通信トンネルを提供するためのコンジットマネージャを有する。ＤＳＣは、発信ＴＣＰ／ＩＰストリーム接続における将来の双方向通信に対してその接続をオープンに保つ。確立され、認証された双方向通信のＴＣＰ／ＩＰストリーム接続は、直接ネットワーク通信トンネルまたはコンジットトンネルとして知られている場合がある。ＤＳＭ２１０のＩＰリダイレクタは、第１のＤＳＣ２０２への第１の確立されたＴＣＰ／ＩＰストリーム接続にルーティングされたパケットを送信し、第２のＤＳＣ２１２への第２の確立されたＴＣＰ／ＩＰストリーム接続にルーティングされたパケットを送信する。ＤＳＭ２１０のＩＰリダイレクタは、第１のファイアウォール２０６の背後にある第１のドメイン２０４内のネットワークコンポーネントのパケットを第１のＤＳＣ２０２への第１の確立されたＴＣＰ／ＩＰストリーム接続にルーティングする。また、ＤＳＭ２１０のＩＰリダイレクタは、第２のファイアウォール２１４の背後にある第２のドメイン２１６内のネットワークコンポーネントのパケットを第２のＤＳＣ２１２への第２の確立されたＴＣＰ／ＩＰストリーム接続にルーティングする。ＴＣＰ／ＩＰは双方向ストリームのプロトコルであるため、ＤＳＭ２１０はルーティングされたパケットをオープンな通信コンジットトンネルに送信し、各ＤＳＣ２０２、２１２からのトラフィックを受信することができることに留意されたい。

【００６７】

ホストコンソール２０８と第２のネットワーク内の機器のサブセットとは、ＶＤＮの一部を形成する。ＶＤＮでは、ホストコンソール２０８は、第２のＤＳＣ２１２がローカルファイアウォールおよび／または顧客ＮＡＴルータを介してアウトバウンドを横断することにより第２のネットワーク内のサブセットを制御管理して、リモートネットワーク上の機器のサブセットにアクセスする。ホストコンソール２０８は、ＶＤＮを制御するＤＳＭ２１０に対して単一のアウトバウンド接続を確立する。このことにより、双方向通信が可能になり、そのアウトバウンド接続をオープンに維持する。ＤＳＣを介してＤＳＭ２１０と協働するＶＤＮは、インターネットの任意の２点間の専用ＴＣＰ／ＩＰ接続を生成することができる。

【００６８】

図２ｂは、ＤＳＭに対して自身の認証を行い、ＤＳＭへの発信ＴＣＰ／ＩＰストリーム接続を確立し、その後、確立されたＴＣＰ／ＩＰストリーム接続上で将来の双方向通信に対して接続をオープンに保つことにより、ＤＡＭへの直接通信トンネルを提供するように構成されたコンジットマネージャを各々が有するＤＳＣを有するシステムの一実施形態を示すブロック図である。ホストコンソール２０８ｂは、ローカルＤＳＣ経由のリモートＤＳＣ２１２ｂとＤＳＭ２１０ｂとに接続する。ローカルＤＳＣとリモートＤＳＣ２１２ｂは共に、双方向通信のために、自身とＤＳＭ２１０ｂとの間の直接通信トンネルをオープンに保つことができる。直接ＴＣＰ通信トンネルは、ＤＳＭ２１０ｂに対してオープンに保たれる双方向ＴＣＰ／ＩＰストリーム接続／ＴＣＰセッションである。その後、着信接続のトラフィックはこのセッションを介して中継される。リモートＤＳＣ２１２ｂ内のコンジットマネージャは、証明書ベースのＳＳＨ（セキュアシェル）暗号化プロトコルを使用して、直接ＴＣＰ通信トンネル経由で、ホストコンソール２０８ｂと動作コントローラなどの宛先の対象デバイスとの間の安全なエンドツーエンド通信を確実なものとすることができる。トラフィックが通信された後、ＴＣＰセッションは閉鎖され得る。このように、直接ＴＣＰ通信トンネルはＳＳＨを介して実装され得る。

【００６９】
一実施形態では、直接ＴＣＰ通信トンネルは、単純なＴＣＰポートフォワーダとすることもできる。プログラムは、ローカルＴＣＰポートをリスンするだけで、受信された全てのデータがリモートホスト、ＤＳＭに送信された状態になる。直接ＴＣＰ通信トンネルにより、ユーザは、リモートデバイスがサーバへのインバウンドＴＣＰ／ＩＰ接続をできないようにするファイアウォールをバイパスすることができる。
【００７０】
また、リモートＤＳＣは、トラフィックのヘッダを復号し、そのトラフィックを対象ネットワークコンポーネントに転送することによって、その関連するローカルネットワーク上でトラフィックを直接通信トンネルからネットワークコンポーネントに逆多重化している。ＴＣＰパケットヘッダ情報は、一般に、データ送信元のソースポートとパケットを受信する対象宛先ポートとの両方を識別する。
【００７１】
図５は、分散システムの自動化集中型管理の一実施形態のブロック図である。
【００７２】
システムの中核は、ＤＳＭ５１０である。デバイスサービスマネージャは、ＤＳＣ５０２、５１２、５１３、５１５の一群を管理する。ＤＳＭ５１０は、高域エリアネットワーク上のＤＳＭ５１０の位置に対して高域エリアネットワーク上のファイアウォール５０６、５１４、５１７、５１９などのファイアウォールの背後にあるＤＳＣ５０２、５１２、５１３、５１５のうち２つ以上と協働するように構成されているＩＰリダイレクタモジュール５１８を有することができる。ＤＳＭ５１０は、ＤＳＣ５０２、５１２、５１３、５１５に構成情報を自動配布するための中央管理ステーションとして機能する。ＤＳＣ内のドライブポートを介してアップロードされた実行可能な起動ファイルは、ＤＳＣおよびそのＤＳＣと同じネットワーク上のネットワークデバイスのための構成情報を集めるためにスクリプト化され、ＤＳＭ５１０によるプロンプトなしで、初期構成ファイルをＤＳＭ５１０に送信する。ＤＳＭ５１０は、ＤＳＣのためにＤＳＭのレジストリ内にデバイス構成ファイルのマスターコピーを作成する。
【００７３】
各ＤＳＣ５０２、５１２、５１３、５１５とＤＳＭ５１０とは協働して、異なるドメイン内の関連デバイス間のエンドツーエンドアクセスを提供する。ＤＳＭ５１０は、関与しているＤＳＣ５０２、５１２、５１３、５１５のためにプロキシ接続ポイントとして機能する。ＤＳＭ１１０は、ユーザホストと宛先デバイスとの間の接続を中継する専用の機器である。
【００７４】
各ＤＳＣ５０２、５１２、５１３、５１５は、関与しているＬＡＮ上の低コストのプレゼンスポイントとして機能する。各５０２、５１２、５１３、５１５は、同時にホストコントローラ（ホストシステムから接続を発信する）とデバイスコントローラ（個々のリモートデバイスへの着信接続を受信および管理する）との両方の機能を果たすことができる。各５０２、５１２、５１３、５１５は、ローカルＬＡＮの範囲外に位置する親ＤＳＭ５１０に対する自身とその関連ネットワークデバイスとの両方の接続をプロキシするように構成されている。
【００７５】
リモートネットワークに対して、新規にインストールされたＤＳＣは新規にインストールされたコンピュータのように機能する。リモートネットワーク上のデバイスにアクセスするためには、ＤＳＣはＶＤＮを制御するＤＳＭへの１つのアウトバウンド接続を確立しなければならないだけである。アウトバウンド接続は、ホストコントローラの機能を果たすＤＳＣとＤＳＭとの間のコンジット通信リンクである。この接続が確立されると、システム構成、コマンド、ネットワークトラフィックが全て暗号化されたチャネルを通過することができる。ＤＳＣがＤＳＭに対する認証に成功すると、ＤＳＣは即座に予め認証されている機器の個々の構成要素への安全なアクセスを提案する。

【００７６】
図８は、ＤＳＣ８１０内のドライブポート８３４を介してアップロードされた実行可能な起動ファイルを介して、第１のＤＳＣ８０２などのＤＳＣに構成情報を配布するＤＳＭの一実施形態を示すブロック図である。ＤＳＭ８１０の管理者は、起動ファイルを作成し、この実行可能な起動ファイルのコピーをサムドライブに組み込む。実行可能な起動ファイルを搭載したサムドライブは、ＤＳＣデバイス８０２が一緒になって標準装備となっている。ＤＳＣ８０２内の実行可能起動ファイルはコードでスクリプト化されて、少なくとも、１）個々のＤＳＣデバイスの固有ＩＤを決定する、２）ＤＳＣの現在のＩＰアドレスを決定する、３）高域エリアネットワーク上のＤＳＭのＩＰアドレスを提供する、４）ＤＳＭ８１０との通信を開始するためにコードをアクティブにする。

【００７７】
ＤＳＣデバイス８０２は、ドライブポート８３４を介してサムドライブから起動ファイルをアップロードし、起動ファイルのコンテンツを使用して、ＳＳＨを介したＤＳＣ８０２とＤＳＭ８１０との間の安全な通信チャネルを自動的に生成し、ＤＳＭ８１０にＷＡＮ上のそのＩＰアドレスで接続する。ＤＳＣ８０２は、次に、固有ＩＤ、デバイスＭＡＣアドレス、および／または、可能であれば関連ＤＮＳエントリを使用してＤＳＭ８１０に対して自身の認証を行う。ＤＳＭ８１０は、次に、ＤＳＭ８１０内で維持されている参照テーブル内の認証情報を調べる。

【００７８】
図７では、上述したように、ＤＳＣ７０２内のデバイス構成エンジン７４３が、ＤＳＭによるプロンプトなしで、安全な通信チャネルを介して、例えば、安全なプロトコル、暗号化電子メール、または同様の方法を介して、少なくとも個々のＤＳＣデバイスの固有ＩＤとＤＳＣの現在のＩＰアドレス情報とを有する初期構成ファイルをＤＳＭ（個々のデバイスがデバイスＩＤ、デバイスＭＡＣアドレス、および／または、可能であれば関連ＤＮＳエントリによって識別されている）に送信する。

【００７９】
図６では、ＤＳＭのＩＰリダイレクタモジュール６１８がこの構成情報を受信する。ＤＳＭ６１０は、この構成情報およびさらなる情報を有するデバイス構成／複製ファイルを作成し、ＤＳＭのレジストリ６２０内にデバイス構成ファイルのマスターコピーを作成するためのユーザデータ複製マネージャモジュール６４５を有する。ユーザデータ複製マネージャモジュール６４５は、次に、ＤＳＣがＤＳＭ６１０に登録されるのに応答して、または所与のＤＳＣがシステムリセットを実行するのに応答して、この構成情報を適切なＤＳＣに配布する。また、ＤＳＭ６１０は、起動コールに応答して、ファームウェア、ソフトウェアパッチなどの更新を送信することができることに留意されたい。

【００８０】
図７では、ＤＳＣ７０２は、既存のネットワーク内で展開されるスタンドアロン型デバイスとすることができる。展開は、単にＤＳＣの電力接続部および電源供給回路への電源に物理的にプラグインすること、Ｅｔｈｅｒｎｅｔ（登録商標）ネットワーク接続にプラグインすること、提供されたサムドライブをドライブポート７３４に挿入すること（すなわち、ＵＳＢフラッシュドライブをＵＳＢポートに挿入すること）からなる。それだけである。このように、ＤＳＣ７０２はスタンドアロン型デバイスであり、既存のネットワーク内の別のホストデバイス上にクライアントソフトウェアがインストールされる必要もなく、またエンドユーザからネットワーク構成設定が要求されることなく、既存のネットワークに接続してＤＳＣを既存のネットワーク上に完全にインストールすることができる。したがって、多くの企業のＩＴ部門が未承認のサードパーティアプリケーションがシステム上にインストールされるのを許可しないのを避けることができる。この時、ＤＳＣ７０２は既存のネットワーク上に常駐し、ＬＡＮへの通信を仲介する。ネットワーキング知識は必要ではなく、このリモートデバイスへのアクセスが自動的に構成される。ＤＳＣを既存のネットワーク上に完全にインストールするのに、エンドユーザの構成またはソフトウェアのインストールが必要でない。

【００８１】
各ＤＳＣ７０２内に常駐する自動ディスカバリプレゼンスマネージャプログラム７３０は、既存のＬＡＮ上のネットワーク機器を発見し、ローカルネットワーク上のプレゼンスの瞬間ポイントを確立する。ディスカバリプレゼンスマネージャプログラム７３０は、ポーリング技術を使用してネットワーク上の関連デバイスを発見する。ディスカバリプレゼンスマネージャプログラム７３０は、ネットワークのユーザに、ファイアウォールによって保護されているネットワーク機器の発見された構成要素が少なくともＤＳＭによるリモートアクセスに対して可視であるか否かを尋ねるためにグラフィカルユーザインタフェース（ＧＵＩ）７４９を有する。次に、ＤＳＣデバイス７０２は、安全なチャネルを介して、指定された可視ネットワークデバイス情報を有する初期構成ファイルを収集し、中央管理ＤＳＭに送信し、ＤＳＭはローカルＤＳＣおよび任意の関連ネットワークデバイスの両方をＤＳＭがホストする識別レジストリに自動的に登録する。この情報は、その後、動的ＤＮＳ、ＬＤＡＰ、ＤＨＣＰおよび関連ウェブベースディレクトリサービスアプリケーションインタフェースを介して利用可能になる。一実施形態では、自動ディスカバリサービス７３０は、ＤＳＭがマスター構成ファイルのコピーおよび任意のファームウェアやソフトウェアの更新を返信するまで、既存ＬＡＮ上のネットワーク機器を発見するために待機する。

【００８２】
グラフィックユーザインタフェース７４９は、ＤＳＭ管理者が各関連ＤＳＣに対して自動化デバイスディスカバリを構成するように構成されている。ＳＮＭＰｖ１、ＳＮＭＰｖ２、または別のプロトコルのいずれかを検索機構として指定する複数の個々の走査記録が作成される場合がある。自動化デバイスディスカバリがアクティベートされると、走査記録が適切なＤＳＣへコピーされ、それらを使用して付属するネットワークデバイスに対してローカルＬＡＮの定期的走査を開始する。

【００８３】
デバイスが発見されると、ＤＳＣはディスカバリ記録を作成する。このディスカバリ記録は、最低限、発見されたデバイスのＩＰアドレス、発見されたネットワークデバイスを配置するのに使用されるディスカバリプロトコル、発見するＤＳＣの識別子を含む。得られるディスカバリ記録は、ＤＳＭのアソシエーションコンポーネント、構成コンポーネント、監視サービスコンポーネントにより使用するために、ＤＳＭに戻って複製される。そのような各ディスカバリ記録は固有ＩＤが割り当てられ、その固有ＩＤにより管理者は個々の構成や発見されたデバイスを曖昧に指すことを避けることができる。ＤＳＭは、次に、ＤＳＭのレジストリ７２８内に記憶するために、ＤＳＣのローカルコピーを返信する。

【００８４】
このように、２つ以上のＤＳＣの各ＤＳＣ７０２はローカル登録オーソリティとしての機能を果たし、既存のローカルＬＡＮ上の関連ネットワークデバイスからの登録要求を承認し、ローカルＬＡＮ上の関連デバイスに対してポーリングを行う。ＤＳＣ７０２は、関連ネットワークデバイスのレジストリ７２８を維持し、自動的にＤＳＣ７０２自身と関連デバイスとの両方を親ＤＳＭレジストリに登録することができる。各ＤＳＣ７０２はこのデータを親ＤＳＭに提供する。各ＤＳＣ７０２は、ポーリング技術を使用して発見された関連デバイスを登録することによってデバイスディスカバリおよびディレクトリサービスに関与する。

【００８５】
図６では、ＤＳＭ６１０は、高域エリアネットワークを介するＤＳＣの分散システムの集中管理とこれらのＤＳＣ間のプロキシ通信を行う。管理者は、ＤＳＭ６１０のＧＵＩ６５１を使用して、特定の発見されたデバイスと既存のデバイス構成とのアソシエーションの組を作成することを含む追加情報、永続的状態情報などを有する初期構成ファイルから中央レジストリ６２０内に完全なデバイス構成記録を作成する。中央構成レジストリ６２０は構成情報を記憶し、ユーザデータ複製マネージャはＤＳＭ６１０内に記憶されたデバイス構成ファイルのマスターコピーを作成する。

【００８６】
図３は、ファイアウォールによって保護されているネットワーク内のネットワークデバイスに対してアクセスするために、中央ＤＳＭとローカルＤＳＣとを有するシステムの一実施形態のブロック図である。仮想デバイスネットワークは、ＤＳＭ３１０とＤＳＣ３０２、３１２と各ＤＳＣに関連付けられたネットワークデバイスとによって形成される。図３内のＶＤＮは、ここで説明する以外は、図１、図２ａ、図２ｂの上述の説明と同様に動作する。ＩＰリダイレクタは、ＤＳＣおよびＤＳＭの両方に常駐する部分を有し得る。
【００８７】
図７では、ＩＰリダイレクタは、アクセスサブシステムとデバイス管理サブシステムとレジストリとを含むことができる。ＤＳＣ内のコンジットマネージャ７２４は、ローカルＤＳＣプロセスに、ＤＳＭへのＳＳＨセッションが完全に確立されたことを通知する。コンジットのＳＳＨシェルセッションは、ＤＳＭ内のＩＰリダイレクタのプログラムの一部に付加される。ＩＰリダイレクタプログラムは、次に、定期的ビーコンパケットを送信する。ＤＳＣはこのパケットを使用することができ確実に直接通信トンネルが確立されアクティブになる。一部の小さなプロトコル機能が存在して、ＤＳＣ／ＤＳＭ１１０は帯域幅／レイテンシの推定を実行することができる。ＳＳＨのＴＣＰポート転送機能が使用されて、全ての他の制御およびＤＳＭとＤＳＣとの間のトンネルデータを渡すことができる。また、コンジットマネージャ７２４は、ＤＳＭからリスンすることができる「リモート」ポートのネゴシエーションを行うこともできる。
【００８８】
図４は、ＤＳＣ内のコンジットマネージャの一実施形態の状態図である。コンジットマネージャは、直接ＴＣＰ通信トンネルを開始および停止し、この直接ＴＣＰ通信トンネルがいつ待機状態であるかまたは突然中断されるかなどを判断するコードを含む。ブロック４０２では、保留中のＴＣＰ接続の要求が到着すると、コンジットマネージャがＤＳＭとの任意のＳＳＨトンネルがすでに確立されているかをチェックする。まだ確立されていない場合、ブロック４０４で、コンジットマネージャが完全な、または部分的なＳＳＨセッションを確立する。ブロック４０６で、コンジットマネージャは、それぞれの同一性を確認することによって、ＤＳＭとＤＳＣとの認証のネゴシエーションを行う。
【００８９】
ＳＳＨセッションが完全に確立され、発信点に関与するＤＳＣの同一性がＤＳＭと共に認証されると、ブロック４０８で、トラフィックは直接通信トンネル内の両方向への通過が許可される。
【００９０】
トンネルがすでに確立されている場合、ブロック４１０で、ＤＳＣはソケットをリダイレクトし、トンネルタイマをリフレッシュする。
【００９１】
図６では、ＤＳＭ６１０は、ソフトウェア内で実装される複数のルーチン、ロジック、またはその両方の組み合わせからなるＩＰリダイレクタプログラムを有する。ＤＳＣは、ＩＰリダイレクタプログラムの一部を含むこともできる。ＩＰリダイレクタプログラムは、ＤＳＣのコンジットマネージャなどのＤＳＣ内の一部を含むことができ、基本の安全なネットワーク通信を提供し、ＤＳＣとＤＳＭとの間のコンジットトンネルとＤＳＣ内のトンネルマネージャとを管理するためにスクリプト化されたコードを有する。
【００９２】
ＤＳＭ６１０内のＩＰリダイレクタのトンネルマネージャ６２４部は、ＤＳＭとＤＥＭＵＸモードで動作するＤＳＣとの間、およびＤＳＭとＭＵＸモードで動作するＤＳＣとの間の安全な多重ＴＣＰセッションを提供するためにスクリプト化されたコードを有する。
【００９３】
上述のプロセスは、所与のプログラミング言語で書かれたソフトウェアコード、ハードウェア論理コンポーネント、他の電気回路、または両方の組み合わせで実装され得る。
【００９４】

したがって、一実施形態では、上述のアルゴリズムを容易にするのに使用されるソフトウェアは、マシン可読媒体上で具現化されることができる。マシン可読媒体は、マシン（例えば、コンピュータ）に可読の形態で情報を提供（例えば、記憶および／または伝送）する任意の機構を含む。例えば、マシン可読媒体は、リードオンリメモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリデバイス、デジタルビデオディスク（ＤＶＤ）、ＥＰＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、磁気カードもしくは光カード、または電子命令を記憶するのに適した任意のタイプの媒体を含む。

【００９５】

詳細な上述の内容の一部は、コンピュータメモリ内のデータビットの動作のアルゴリズムおよび象徴的表現で示されている。これらのアルゴリズムおよび表現は、データ処理技術の分野の当業者が最も効率的に仕事の内容を他の当業者に伝達するのに使用する手段である。アルゴリズムとは、ここでは、一般に、望ましい結果につながるステップの首尾一貫したシーケンスであると考えられる。ステップは、物理量の物理操作を必要とするステップである。通常、必ずしもではないが、これらの量は、記憶、転送、結合、比較、その他の操作が可能な電気または磁気信号の形態をとる。これらの信号を、ビット、値、要素、記号、文字、用語、数字などとして参照することは、主に、一般的な使い方であるとの理由から、時には便利であることが証明されている。これらのアルゴリズムは、多数のさまざまなソフトウェアプログラミング言語で書かれ得る。また、アルゴリズムは、ソフトウェア内のコード行、ソフトウェア内の構成された論理ゲート、またはその組み合わせを使用して実装され得る。

【００９６】

しかしながら、これらの用語および同様の用語は全て、適切な物理量に関連付けられるべきであり、これらの量に適用された単に便利なラベルにすぎないことに留意すべきである。上述した内容から明らかであるように、特に言及しない限り、明細書全体にわたって、「処理」、「コンピューティング」、「計算」、「判断」、または「表示」などの用語を使用した説明は、コンピュータシステムのレジスタまたはメモリ内の物理（電子）量として表されるデータを操作し、コンピュータシステムのメモリもしくはレジスタ、または他の情報記憶デバイス、伝送デバイスもしくは表示デバイス内の物理量として同様に表される他のデータに変換する、コンピュータシステムまたは同様の電子コンピューティングデバイスの動作およびプロセスを指すものであると考えられる。

【００９７】

一実施形態では、ロジックは、Ｂｏｏｌｅａｎ　Ｌｏｇｉｃの規則に従う電子回路、命令のパターンを含むソフトウェア、またはその両方の組み合わせからなる。

【００９８】

本発明のいくつかの特定の実施形態が示されているが、本発明はこれらの実施形態に限定されるものではない。例えば、電子ハードウェアコンポーネントによって実行されるほとんどの機能はソフトウェアエミュレーションによって再現される場合がある。したがって、これらの同じ機能を達成するために書かれたソフトウェアプログラムは、入出力回路内のハードウェアコンポーネントの機能性をエミュレートすることができる。本発明は、本明細書内で説明されている特定の実施形態に限定されないが、添付の請求項の範囲によってのみ限定されると理解されるべきである。

【図１】

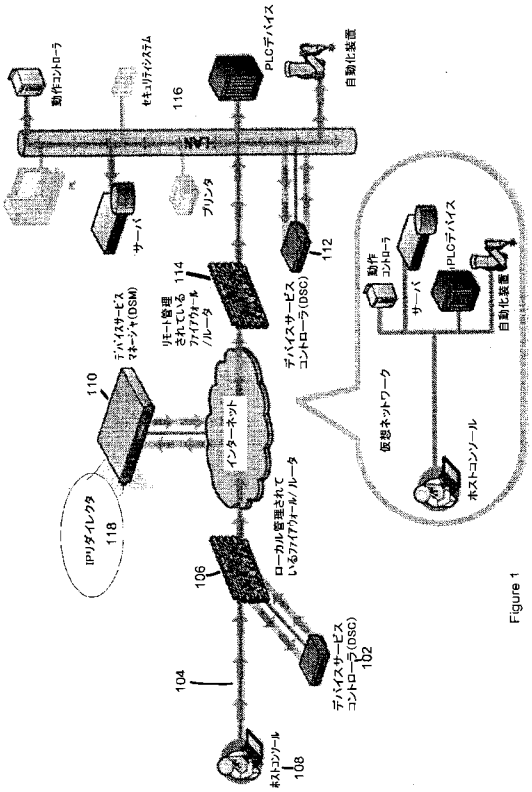

Figure 1

【図２ａ】

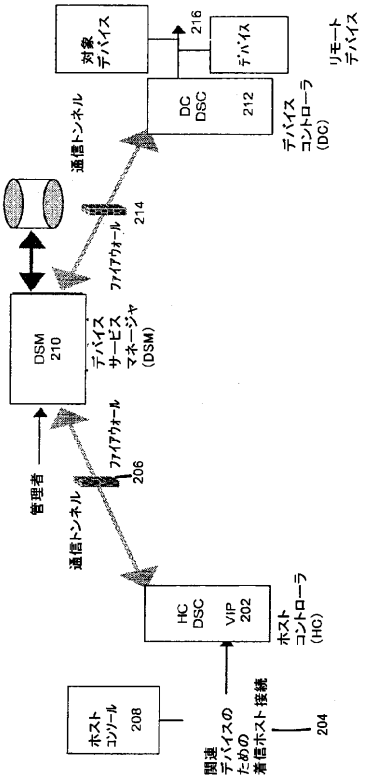

Figure 2a

【図２ｂ】

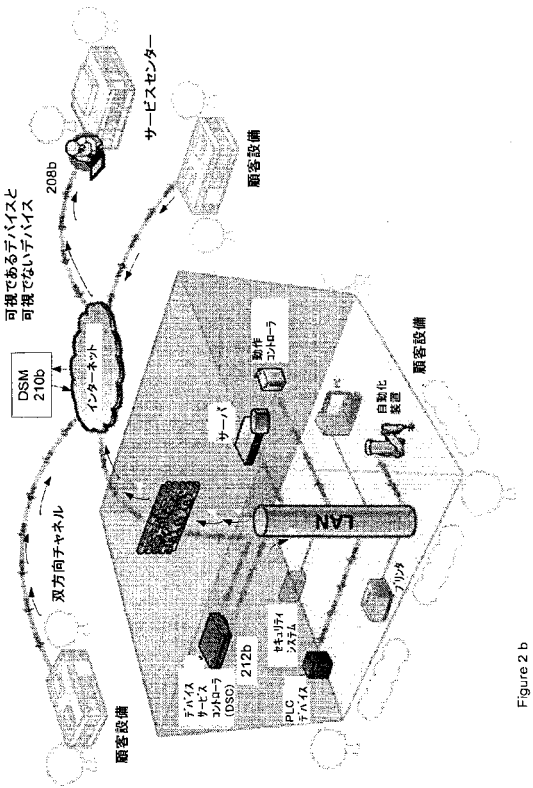

Figure 2 b

【図３】

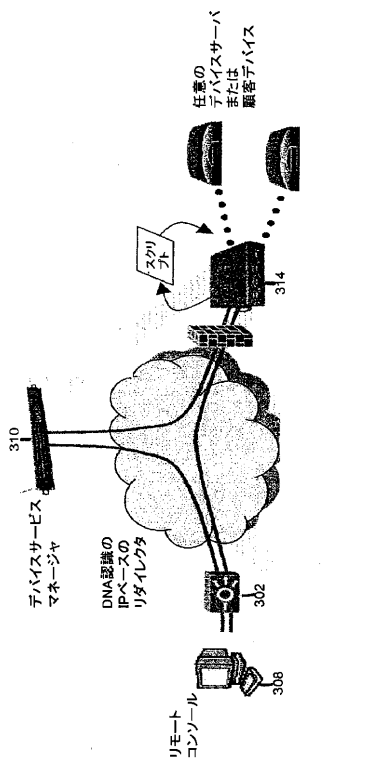

Figure 3

【図４】

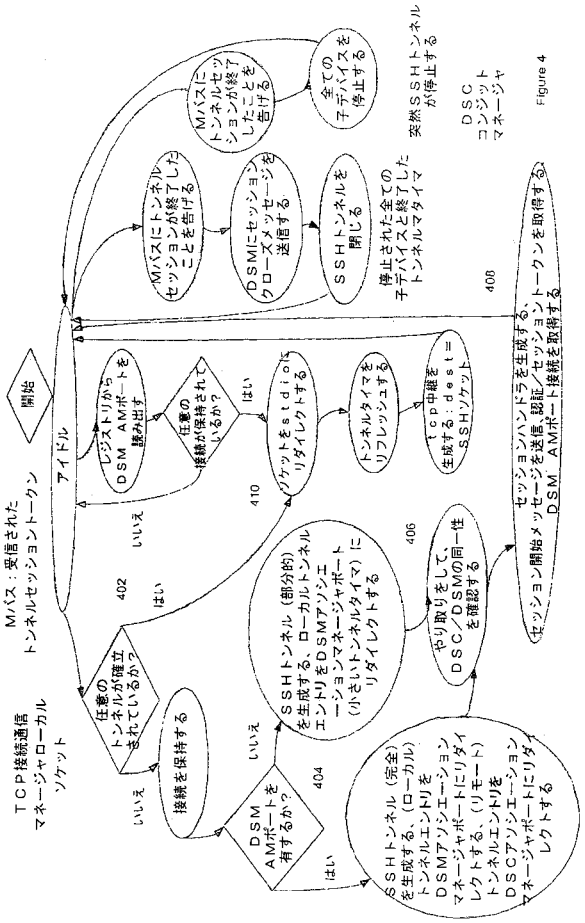

Figure 4

【図５】

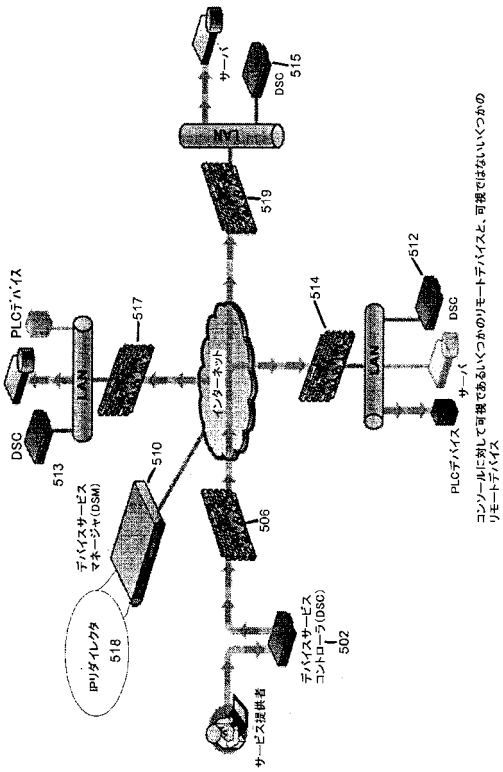

Figure 5

【図６】

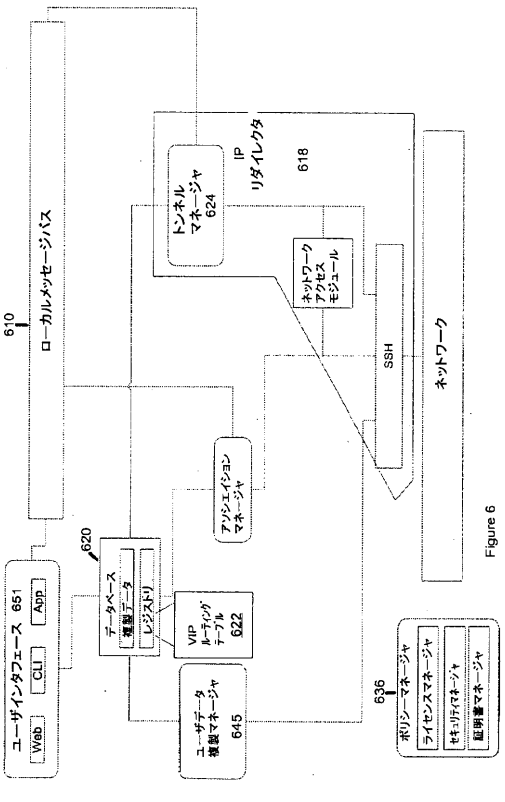

Figure 6

【図７】

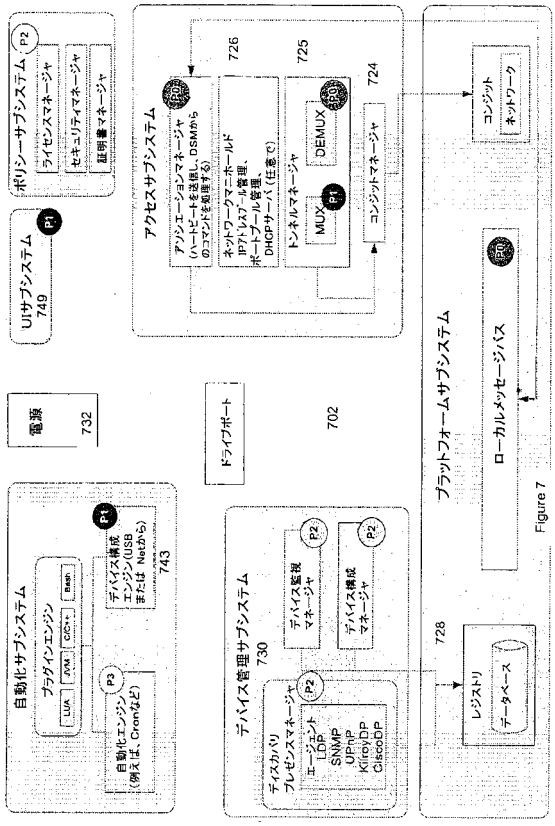

Figure 7

【図８】

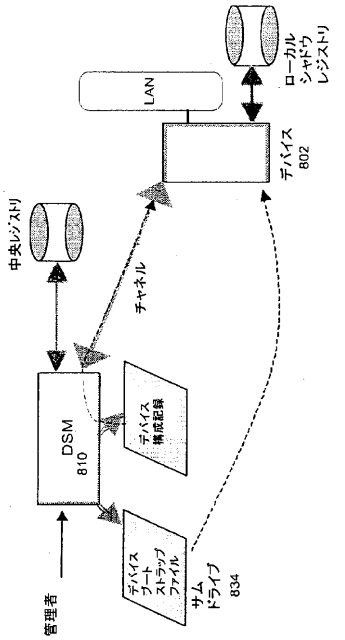

Figure 8

【図９】

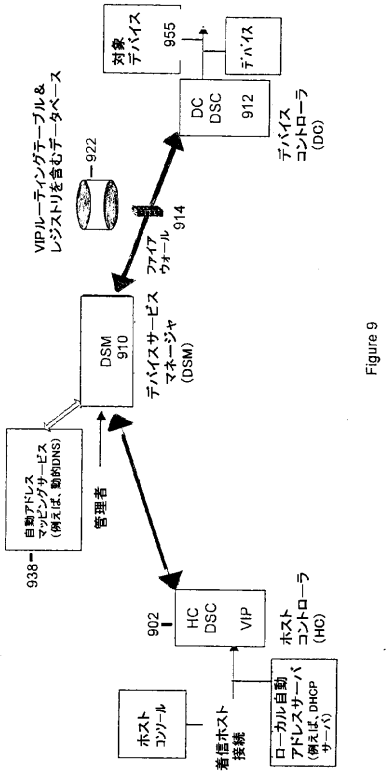

Figure 9

【図１０】

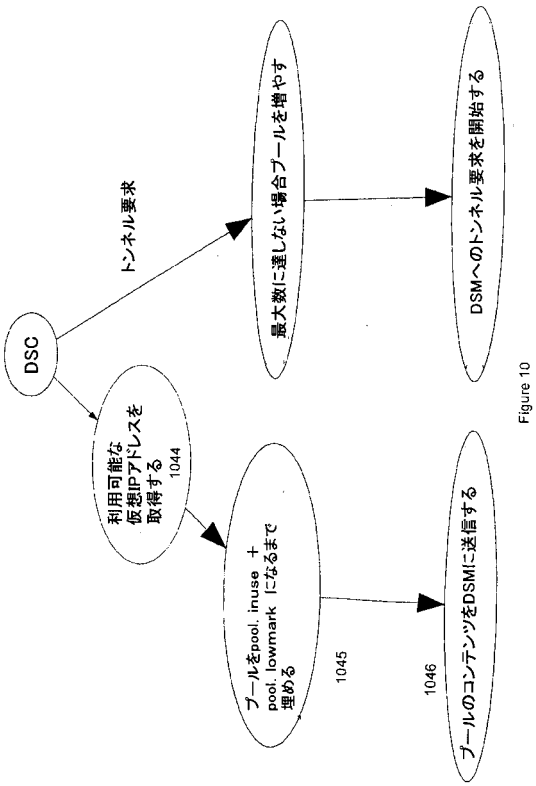

Figure 10

【図１１】

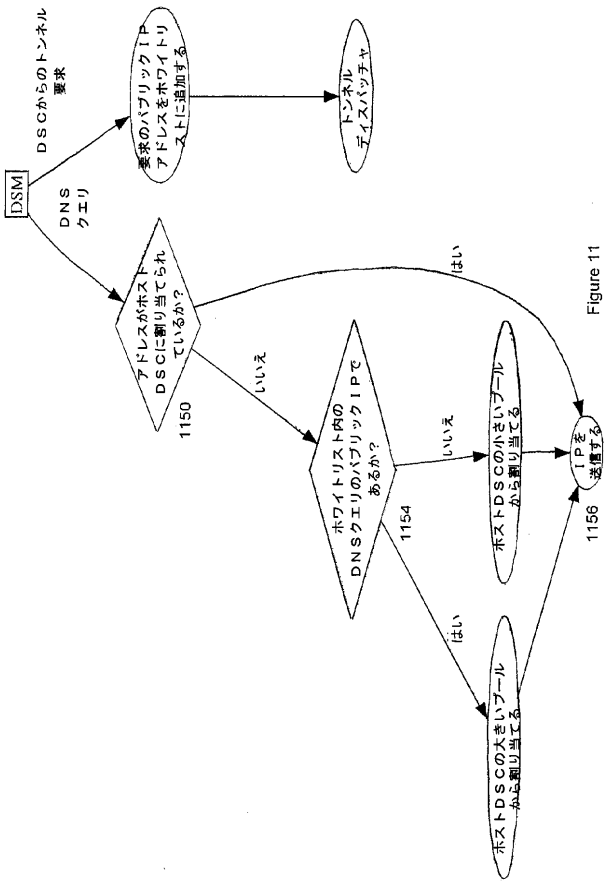

Figure 11

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/081186

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 13/00 (2008.04)
USPC - 709/227
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)
IPC(8) - G06F 13/00 (2008.04)
USPC - 709/227

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,631,416 B2 (BENDINELLI et al) 07 October 2003 (07.10.2003) Entire Document.	1-20
A	US 6,850,982 B1 (SIEGEL) 01 February 2005 (01.02.2005) Entire Document.	1-20
A	US 2002/0124090 A1 (POIER et al) 05 September 2002 (05.09.2002) Entire Document.	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* 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
10 December 2008	04 MAR 2009
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ドイチユ，ジヨナサン・ピーター
アメリカ合衆国、カリフオルニア・９２８８６、ヨーバ・リンダ、ラ・コンセツタ・ドライブ・４０４１
(72)発明者 サン，ダニー・テーアン
アメリカ合衆国、カリフオルニア・９２６８８、ランチヨ・サンタ・マルガリータ、ビスタ・バランカ・１０

Ｆターム(参考) 5K030 HA08 HC01 HC13 HD09 LB05