(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5385403号
(P5385403)

(45)発行日　平成26年1月8日(2014.1.8)　(24)登録日　平成25年10月11日(2013.10.11)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	E
H04L 12/70	(2013.01)	H04L	12/70	D
G06Q 50/00	(2012.01)	G06F	17/60	

請求項の数 15　(全 62 頁)

(21)出願番号	特願2011-540820 (P2011-540820)
(86)(22)出願日	平成21年12月8日 (2009.12.8)
(65)公表番号	特表2012-511878 (P2012-511878A)
(43)公表日	平成24年5月24日 (2012.5.24)
(86)国際出願番号	PCT/US2009/067106
(87)国際公開番号	WO2010/068618
(87)国際公開日	平成22年6月17日 (2010.6.17)
審査請求日	平成23年6月9日 (2011.6.9)
(31)優先権主張番号	12/332,214
(32)優先日	平成20年12月10日 (2008.12.10)
(33)優先権主張国	米国(US)

(73)特許権者　506329306
アマゾン　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　８９５０７　ネバダ州　レノ　ピーオー　ボックス　８１０２
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　エリック　ジェイソン　ブランドウィン
アメリカ合衆国　９８１４４　ワシントン州　シアトル　１２　アベニュー　サウス　１２００　スイート　１２００

最終頁に続く

(54)【発明の名称】設定可能プライベートコンピュータネットワークへのアクセス提供

(57)【特許請求の範囲】

【請求項１】

プライベートコンピュータネットワークへのアクセスを提供するコンピュータ実装された方法であって、

複数のクライアントの使用のためにプライベートコンピュータネットワークを設定するため、前記複数のクライアントによる使用のためのプログラムによるインタフェースを提供する設定可能ネットワークサービス用のコンピューティングシステムの制御下において、

第１のクライアントによる利用のために第１のプライベートコンピュータネットワークを設定するため、前記プログラムによるインタフェースを介して、前記第１のクライアントによってプログラムによって提供される第１の情報を受信することであって、前記第１のプライベートコンピュータネットワークが、前記設定可能ネットワークサービスにより提供される複数のコンピューティングノードのグループを含み、前記複数のコンピューティングノードの各々が、前記第１のプライベートコンピュータネットワークで使用する前記第１の情報で特定された複数のネットワークアドレスの少なくとも１つに関連付けられるように設定されていることと、

前記第１のプライベートコンピュータネットワークから、ネットワークアクセス可能なリモート資源サービス内の名前空間に関連付けられたコンピューティング関連資源のサブセットへのアクセスを設定するための第２の情報を取得することであって、前記第２の情報が、前記リモート資源サービス内の前記名前空間に関連する識別子を含むことと、

前記複数のコンピューティングノードから、前記リモート資源サービスで提供される前記コンピューティング関連資源のサブセットへのアクセスを可能するように前記第１のプライベートコンピュータネットワークを自動的に設定することであって、前記設定が、前記コンピューティング関連資源のサブセットへアクセスするために、指示されたネットワークアドレスを介して前記リモート資源サービスに送信された通信が、前記名前空間の識別時に前記リモート資源サービスによって使用される前記識別子の指示を含むように変更される、前記識別子の前記リモート資源サービスを表す前記複数のネットワークアドレスの指示された１つとの関連付けを含むことと、

前記第１のクライアントの１つまたは複数のリモートコンピューティングシステムから前記第１のプライベートコンピュータネットワークへのアクセス利用可能状態を開始することと、

を含む方法。

【請求項２】

前記第１のプライベートコンピュータネットワークが、複数のコンピューティングシステムを含む前記第１のクライアントのリモートプライベートコンピュータネットワークの拡張となるように設定され、前記特定された複数のネットワークアドレスが、前記リモートプライベートコンピュータネットワークで使用される複数のプライベートネットワークアドレスのサブセットであって、かつ、前記第１のプライベートコンピュータネットワークの前記自動設定が、前記第１のクライアントの前記リモートプライベートコンピュータネットワークの前記複数のコンピューティングシステムと前記第１のプライベートコンピュータネットワークの前記複数のコンピューティングノードとの間のプライベートアクセスをさらに可能にする、請求項１に記載の方法。

【請求項３】

前記第１の情報が、前記第１のプライベートコンピュータネットワークの前記複数のコンピューティングノード間の通信を制御するように前記第１のプライベートコンピュータネットワークを設定する際に使用するために前記第１のクライアントによって特定される追加情報をさらに含み、かつ、前記方法が、前記特定された追加情報に従って前記複数のコンピューティングノード間の通信を許可および阻止するように前記第１のプライベートコンピュータネットワークを自動的に設定することをさらに含む、請求項１に記載の方法。

【請求項４】

前記第２の情報が、前記第１のクライアントが前記プログラムによるインタフェースを介して前記第２の情報をプログラムで提供することに少なくとも部分的に基づいて取得され、前記提供される第２の情報が、前記名前空間に対する前記関連した識別子を含み、コンピューティング関連資源の前記サブセットの少なくともいくつかが、前記第２の情報の提供前に、前記名前空間内の前記リモート資源サービスに存在し、かつ、前記方法が、前記リモート資源サービスから１つまたは複数の前記既存のコンピューティング関連資源にアクセスするために１つまたは複数の前記複数のコンピューティングノードから前記指示されたネットワークアドレスに送信された１つまたは複数の通信を取得することと、前記識別子の前記指示を含むように前記取得された１つまたは複数の通信の変更後、前記取得された１つまたは複数の通信を前記リモート資源に転送することを含む、請求項１に記載の方法。

【請求項５】

前記第２の情報に含まれた前記識別子の前記取得が、前記設定可能ネットワークサービスが前記第１のプライベートコンピュータネットワークで使用される前記名前空間を作成するため、前記リモート資源サービスと自動的にやりとりすることを含み、前記名前空間の前記作成が前記名前空間に対する前記識別子の決定を含み、かつ、前記方法が、前記リモート資源サービスから１つまたは複数の新規コンピューティング関連資源を作成するために前記複数のコンピューティングノードの１つまたは複数から前記指示されたネットワークアドレスに送信された１つまたは複数の通信を取得すること、および前記識別子の前

記指示を含むように前記取得された１つまたは複数の通信の変更後、前記取得された１つまたは複数の通信を前記リモート資源へ転送することをさらに含む、請求項１に記載の方法。

【請求項６】

前記リモート資源サービスが、１つまたは複数の公衆網を経由してアクセス可能であって、かつ、前記複数のコンピューティングノードから前記コンピューティング関連資源のサブセットへのアクセスを可能にするための、前記第１のプライベートコンピュータネットワークの前記設定が、前記設定可能ネットワークサービスの１つまたは複数のモジュールを、前記指示されたネットワークアドレスに送信された通信を前記１つまたは複数の公衆網を経由して前記リモート資源サービスへ転送するように設定することを含む、請求項１に記載の方法。

【請求項７】

前記第１のプライベートコンピュータネットワークから、前記リモート資源サービス内の別個の第２の名前空間に関連付けられたコンピューティング関連資源の別個の第２のサブセットへのアクセスを設定するための第３の情報を取得することであって、前記第３の情報が、前記リモート資源サービス内の前記第２の名前空間に関連付けられた別個の第２の識別子を含むことと、前記第１のプライベートコンピュータネットワークを、前記第２の識別子を前記複数のネットワークアドレスの第２の１つに関連付けることにより、前記複数のコンピューティングノードからコンピューティング関連資源の前記第２のサブセットへのアクセスを可能にするように自動設定して、コンピューティング関連資源の前記第２のサブセットにアクセスするため、前記第２のネットワークアドレスを介して前記リモート資源サービスに送信された通信が、前記第２の名前空間の識別時に前記リモート資源サービスによって使用される前記第２の識別子の指示を含むように変更されるようにすることをさらに含む、請求項１に記載の方法。

【請求項８】

前記リモート資源サービス内の前記名前空間に関連付けられた前記コンピューティング関連資源が、データストレージサービスおよびプログラム実行サービスおよび非同期メッセージ受渡しサービスの少なくとも１つのための資源を含み、かつ、

前記方法が、前記リモート資源サービスの制御下において、

前記コンピューティング関連資源のサブセットの少なくともいくつかにアクセスするための前記指示されたネットワークアドレスを経由して前記第１のプライベートコンピュータネットワークの前記複数のコンピューティングノードから送信された通信を受信するステップことであって、前記受信された通信が前記識別子の前記指示を含むことと、

前記指示された識別子に関連付けられた前記名前空間から前記コンピューティング関連資源の少なくともいくつかへのアクセスを提供することと、をさらに含む、

請求項１に記載の方法。

【請求項９】

前記複数のコンピューティングノードが、各々、前記設定可能ネットワークサービスの複数の物理コンピューティングシステムの１つ上でホストされる仮想マシンであって、かつ、前記第１のプライベートコンピュータネットワークの前記設定が、１つまたは複数の前記物理コンピューティングシステム上で実行する１つまたは複数の仮想マシン通信マネージャモジュールを、前記ホストされた仮想マシンのための通信を管理するように設定することを含む、請求項１に記載の方法。

【請求項１０】

前記複数のクライアントによって設定された前記プライベートコンピュータネットワークが、前記第１のプライベートコンピュータネットワークで使用のために特定された前記複数のネットワークアドレスの少なくとも１つと同一の前記１つまたは複数の別のクライアントによって特定された１つまたは複数のネットワークアドレスを持つ前記第１のクライアント以外の１つまたは複数のクライアント用の前記第１のプライベートコンピュータネットワーク以外の１つまたは複数の設定されたプライベートコンピュータネットワーク

を含み、かつ、前記設定可能ネットワークサービスが、それら同一のネットワークアドレスをさらに管理し、それら同一のネットワークアドレスの各々について、前記別のプライベートコンピュータネットワークの各々が、前記第１のプライベートコンピュータネットワーク用の前記ネットワークアドレスに対応するコンピューティングノードとは異なる前記ネットワークアドレスに対応するコンピューティングノードを持つようにする、請求項１に記載の方法。

【請求項１１】

前記第１のクライアントによる前記第１のプライベートコンピュータネットワークの前記設定が、前記第１のクライアントが前記第１のプライベートコンピュータネットワークで使用するように前記第１の情報で特定された前記複数のネットワークアドレスに対する任意のネットワークアドレスの選択することを許可することを含む、請求項１に記載の方法。

【請求項１２】

プライベートコンピュータネットワークへのアクセスを提供するように設定されたコンピューティングシステムであって、

１つまたは複数のメモリと、

リモートクライアントによる使用のために作成されたコンピュータネットワークを自動的に提供するように設定された設定可能ネットワークサービスマネージャモジュールと、を備え、前記設定可能ネットワークサービスマネージャモジュールが、複数のリモートクライアントの各々に対して、

前記クライアントによる使用のために作成されたコンピュータネットワークを設定するため、前記クライアントによってプログラムで提供される設定情報を受信することであって、前記設定情報が、前記クライアント用に前記作成されたコンピュータネットワークの一部として提供される複数のコンピューティングノードに関連付けられる複数のネットワークアドレスの指示を含むことと、

前記受信された設定情報に従って前記クライアント用に前記作成されたコンピュータネットワークの一部として提供される複数のコンピューティングノードを設定することであって、前記設定が、前記複数のネットワークアドレスの少なくとも１つの、前記複数のコンピューティングノードの各々への関連付けを含み、前記複数のコンピューティングノードが、クライアントのコンピュータネットワークで利用可能な複数のコンピューティングノードから選択されることと、

前記クライアント用に前記作成されたコンピュータネットワークからネットワークアクセス可能な資源サービスによって提供される１つまたは複数の資源へのアクセスを設定するための追加情報を取得することであって、前記追加情報が、前記資源サービスによって前記１つまたは複数の資源に関連付けられた識別子を含むことと、

前記クライアント用に前記作成されたコンピュータネットワークを、取得された前記追加情報に基づいて、前記複数のコンピューティングノードから前記資源サービスによって提供される前記１つまたは複数の資源へのアクセスを可能にして、前記１つまたは複数の資源にアクセスするために前記作成されたコンピュータネットワークから前記資源サービスに送信された通信が、前記資源サービスによる使用のための前記識別子の指示を含むように、自動的に設定することと、

前記クライアントに前記作成されたコンピュータネットワークの前記複数のコンピューティングノードへのアクセスを提供することと、を実行する、

コンピューティングシステム。

【請求項１３】

前記設定可能ネットワークサービスマネージャモジュールが、設定可能ネットワークサービスの一部であり、かつ、前記クライアントによる使用のために作成された前記コンピュータネットワークを設定するために、前記複数のリモートクライアントによって使用されるプログラムによるインタフェースを提供し、前記作成されたコンピュータネットワークでの使用が可能である前記複数のコンピューティングノードが、前記設定可能ネットワ

ークサービスによって提供され、前記複数のクライアントの少なくともいくつかの各々について、前記クライアントによりプログラムで提供される前記設定情報が、前記プログラムによるインタフェースを介して提供され、さらに、前記クライアントによる使用のために設定されている前記作成済みコンピュータネットワーク用のネットワークトポロジ情報を提供し、前記クライアントによる使用のために作成および設定された前記コンピュータネットワークが、前記クライアントのリモートプライベートコンピュータネットワークへのプライベートコンピュータネットワーク拡張であり、さらに前記提供されたネットワークトポロジ情報に従って設定され、前記作成済みコンピュータネットワークの前記自動設定がさらに、前記リモートプライベートコンピュータネットワークと前記プライベートコンピュータネットワーク拡張の前記複数のコンピューティングノードとの間のプライベートアクセスを可能にする、請求項１２に記載のコンピューティングシステム。

【請求項１４】

前記複数のクライアントの少なくともいくつかの各々について、前記クライアント用の前記作成済みコンピュータネットワーク用に設定されているアクセス先の前記１つまたは複数の資源を提供する前記ネットワークアクセス可能資源サービスが、前記作成済みコンピュータネットワークの一部でないリモート資源サービスであって、前記取得された追加情報に含まれる前記識別子が、前記リモート資源サービス内の前記クライアント用の名前空間に関連付けられた一意の識別子であって、前記クライアント用に前記作成済みコンピュータネットワークからアクセスされる前記１つまたは複数の資源が、前記クライアント用の前記関連した名前空間に格納され、かつ、前記識別子の前記指示を前記リモート資源サービスに送信された前記通信に含むための前記クライアント用の前記作成済みコンピュータネットワークの前記設定が、前記リモート資源サービスを表すための前記作成済みコンピュータネットワーク用の前記複数のネットワークアドレスの１つの割当て、および前記リモート資源サービスへ前記割当て済みネットワークアドレスを介して送信された前記通信が、前記関連した名前空間の識別時に前記リモート資源サービスでの使用のために前記識別子を含むように変更されるような方法での前記識別子の前記割当て済みネットワークアドレスとの関連付けを含む、請求項１２に記載のコンピューティングシステム。

【請求項１５】

前記設定可能ネットワークサービスマネージャモジュールが、リモートクライアントによる使用のために作成されたコンピュータネットワークを自動的に提供するための手段から構成されるコンピューティングシステムであって、前記設定可能ネットワークサービスマネージャモジュールが、前記複数のリモートクライアントの各々に対して、

前記クライアントによる使用のために作成されたコンピュータネットワークを設定するため、前記クライアントによりプログラムで提供される設定情報を受信することであって、前記設定情報が、前記クライアント用の前記作成済みコンピュータネットワークの一部として提供される複数のコンピューティングノードに関連付けるための複数のネットワークアドレスの指示を含むことと、

前記受信された設定情報に従って前記クライアント用の前記作成済みコンピュータネットワークの一部として提供される複数のコンピューティングノードを設定することであって、前記設定が、前記複数のネットワークアドレスの少なくとも１つの、前記複数のコンピューティングノードの各々との関連付けを含み、前記複数のコンピューティングノードが、クライアントのコンピュータネットワークで利用可能な複数のコンピューティングノードから選択されることと、

前記クライアント用の前記作成済みコンピュータネットワークから、ネットワークアクセス可能な資源サービスによって提供される１つまたは複数の資源へのアクセスを設定するための追加情報を取得することであって、前記追加情報が、前記資源サービスによって前記１つまたは複数の資源に関連付けられた識別子を含むことと、

前記クライアント用の前記作成済みコンピュータネットワークを前記複数のコンピューティングノードから、取得された前記追加情報に基づいて、前記資源サービスによって提供される前記１つまたは複数の資源へのアクセスを可能にして、前記１つまたは複数の資

源にアクセスするために前記作成済みプライベートネットワークから前記資源サービスに送信された通信が、前記資源サービスで使用される前記識別子の指示を含むようにするように、自動的に設定することと、
前記クライアントに前記作成済みコンピュータネットワークの前記複数のコンピューティングノードへのアクセスを提供することと、を実行する、
請求項１２に記載のコンピューティングシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
多数の企業およびその他の組織は、同一場所に配置されている（例えば、ローカルネットワークの一部として）か、またはその代わりに地理的に異なる複数の場所に配置されている（例えば、１つまたは複数のプライベートまたは公衆の中間ネットワークを経由して接続された）コンピューティングシステムなど、多くのコンピューティングシステムを相互接続して、それらの運用を支援するコンピュータネットワークを運営している。例えば、単一の組織によりその組織のために運営されているプライベートのデータセンタや、ビジネスとして顧客にコンピューティング資源を提供する団体によって運営されている公共データセンタなど、かなりの数の相互接続されたコンピューティングシステムを収容しているデータセンタが当たり前になってきている。公共データセンタの運営者の中には、ネットワークアクセス、電力、および種々の顧客が所有しているハードウェアのための安全な設置施設を提供するものもあれば、顧客が利用可能なハードウェア資源も含めて「完全なサービス」施設を提供するものもある。しかし、典型的なデータセンタの規模や範囲が拡大してくるにつれ、物理的なコンピューティング資源の提供、運営、および管理業務が次第に複雑になってきた。
【発明の概要】
【０００２】
コモディティハードウェア用の仮想化技術の出現によって、多様なニーズを持つ多数の顧客に大規模なコンピューティング資源の管理に関する恩恵がもたらされ、様々なコンピューティング資源が複数の顧客によって効果的かつ安全に共有できるようになった。例えば、ＶＭＷａｒｅ、ＸＥＮ、またはＵｓｅｒ－Ｍｏｄｅ　Ｌｉｎｕｘによって提供されるような仮想化技術は、各ユーザに単一の物理コンピューティングマシンでホストされる１つまたは複数の仮想マシンを提供し、かかる各仮想マシンは、各ユーザに当該ハードウェアコンピューティング資源を操作および管理しているのは自分だけであると錯覚させる別個の論理コンピューティングシステムとして動作するソフトウェアシミュレーションであり、同時に、種々の仮想マシン間にアプリケーションの隔離および安全性を提供することにより、単一の物理コンピューティングマシンが複数のユーザで共有できるようにする。さらに、仮想化技術の中には、複数の異なる物理コンピューティングシステムに渡る複数の仮想プロセッサを持つ単一の仮想マシンなど、１つまたは複数の物理資源に渡る仮想資源を提供できるものもある。
【図面の簡単な説明】
【０００３】
【図１Ａ】プライベートコンピュータネットワークを作成および設定するリモートクライアントに関わる相互関係の実施形態例を示すネットワーク図である。
【図１Ｂ】プライベートコンピュータネットワークを作成および設定するリモートクライアントに関わる相互関係の実施形態例を示すネットワーク図である
【図２】コンピュータネットワークをクライアントに提供するために使用する相互接続されたコンピューティングシステムの一実施形態例を示すネットワーク図である。
【図３】リモートクライアントが使用するコンピュータネットワークを提供するためのシステムの一実施形態の実行に適したコンピューティングシステムの例を示すブロック図である。
【図４Ａ】設定可能ネットワークマネージャ（Ｃｏｎｆｉｇｕｒａｂｌｅ　Ｎｅｔｗｏｒ

ｋ　Ｓｅｒｖｉｃｅ　Ｍａｎａｇｅｒ）ルーチンの一実施形態例の流れ図を示す。
【図４Ｂ】設定可能ネットワークマネージャ（Ｃｏｎｆｉｇｕｒａｂｌｅ　Ｎｅｔｗｏｒｋ　Ｓｅｒｖｉｃｅ　Ｍａｎａｇｅｒ）ルーチンの一実施形態例の流れ図を示す。
【図５】ノード通信マネージャ（Ｎｏｄｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｍａｎａｇｅｒ）ルーチンの一実施形態例の流れ図を示す。
【図６】外部通信マネージャ（Ｅｘｔｅｒｎａｌ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｍａｎａｇｅｒ）ルーチンの一実施形態例の流れ図を示す。
【図７】リモート資源サービスアクセス（Ｒｅｍｏｔｅ　Ｒｅｓｏｕｒｃｅ　Ｓｅｒｖｉｃｅ　Ａｃｃｅｓｓ）ルーチンの流れ図を示す。
【図８】ＶＰＮ作成実行（ＶＰＮ　Ｃｒｅａｔｉｏｎ　Ｆｕｌｆｉｌｍｅｎｔ）ルーチンの一実施形態例の流れ図を示す。
【発明を実施するための形態】
【０００４】
リモートユーザが利用可能な設定可能ネットワークサービスの制御下においてなど、ユーザにコンピュータネットワークへのアクセスを提供するための技術について説明する。少なくともいくつかの実施形態では、リモートユーザは、そのユーザが利用するコンピュータネットワークの作成および設定を行うため、公衆網を介して設定可能ネットワークサービスとやりとりすることができ、その設定されたコンピュータネットワークは、その設定可能ネットワークサービスにより提供され、かつその設定可能ネットワークサービスで保守されているか、そうでなければその制御下にある複数のコンピューティングノードを含んでいる。かかるコンピュータネットワークを設定すると、ユーザは１つまたは複数のリモート位置から、提供されるコンピュータネットワークのコンピューティングノード上でのプログラム実行などのために、設定可能ネットワークサービスによりユーザに対して提供されているコンピュータネットワークとやりとりできる。設定可能ネットワークサービスは、少なくともいくつかの実施形態で、有料サービスのこともあり、設定可能ネットワークサービスのユーザは、その設定可能ネットワークサービスによって提供される機能の少なくともいくつかに対して、設定可能ネットワークサービスの料金を支払う顧客となる。また、少なくともいくつかの実施形態では、説明した技術の一部または全ては、以降でさらに詳述するように、設定可能ネットワークサービスマネージャモジュールの実施形態によって自動的に実行され、オプションとして別の通信マネージャモジュールと連動して実行される。
【０００５】
少なくともいくつかの実施形態において、設定可能ネットワークサービスによって提供されるコンピュータネットワークの少なくともいくつかは、提供されるコンピュータネットワークがそのユーザのために作成および設定された設定可能ネットワークサービスのユーザによって（またはアクセスが明示的に設定された別のユーザによって）のみアクセス可能なプライベートコンピュータネットワークである。例えば、設定可能ネットワークサービスは、その設定可能ネットワークサービスのクライアントであるユーザに、クライアントの１つまたは複数のリモートコンピューティングシステムとその提供されるコンピュータネットワークとの間にＶＰＮ（仮想プライベートネットワーク）接続または別の安全な接続を可能にすることなどにより、そのクライアント用に提供されるコンピュータネットワークへの安全なプライベートアクセスを提供し、または、別のセキュリティおよび／または認証技術を使用して、クライアントが非公開かつ安全な方法でその提供されるコンピュータネットワークとリモートでやりとりできるようにする。また、少なくともいくつかの実施形態では、設定可能ネットワークサービスによって提供されるコンピュータネットワークの少なくともいくつかは、クライアントの既存のリモートプライベートコンピュータネットワーク（例えば、企業体であるクライアントのリモート企業ネットワーク）へのプライベートコンピュータネットワーク拡張としてなど、各々、クライアントの既存のコンピュータネットワークへの拡張としてクライアントによって作成および設定される。かかる実施形態では、既存のコンピュータネットワークと提供される新規のコンピュータ

ネットワーク拡張との間の安全なプライベートアクセスは、同様に、１つもしくは複数のＶＰＮ接続または別のプライベート接続を用いて可能にできる。設定可能ネットワークサービスの一実施形態によって提供されるコンピュータネットワークへのクライアントのアクセス確立に関しては、以下で詳述する。

【０００６】

設定可能ネットワークサービスのクライアントは、設定可能ネットワークサービスによって提供されるコンピュータネットワークを、種々の実施形態において種々の方法で作成および設定することができる。少なくともいくつかの実施形態では、設定可能ネットワークサービスは、設定可能ネットワークサービスによって提供されるコンピュータネットワークの作成、設定、および使用開始時に一部または全ての動作を実行するために、クライアントのコンピューティングシステムが、設定可能ネットワークサービスとプログラムでやりとりできるようにする１つまたは複数のＡＰＩ（アプリケーションプログラミングインタフェース）を提供し、他方、少なくともいくつかの実施形態では、設定可能ネットワークサービスのクライアントであるユーザは、かかるＡＰＩの使用によるかかる動作の実行に代わってまたは加えてかに関わらず、かかる動作の一部または全てを（例えば、ＧＵＩ（グラフィカルユーザインタフェース）、またはその設定可能ネットワークサービスによって提供される別のコンソールを介して）実行するために、設定可能ネットワークサービスと対話形式でやりとりできる。いくつかの実施形態では、ユーザが利用可能なＧＵＩは、代替としてユーザが利用可能な基礎となるＡＰＩに基づくことができ、他方、別の実施形態では、ＧＵＩを別の方法で実装できる。さらに、クライアントのコンピューティング装置と設定可能ネットワークサービスとの間のやりとりは、例えば設定可能ネットワークサービスのメッセージベースのＡＰＩに従って、クライアントのコンピューティング装置と設定可能ネットワークサービスとの間で送信された電子メッセージ（例えば、電子メールサービス）に少なくとも部分的に基づき得る。

【０００７】

例えば、少なくともいくつかの実施形態では、クライアントは、そのクライアント用に提供されるコンピュータネットワーク用の設定情報を指定するために設定可能ネットワークサービスの一実施形態とやりとりすることができ、その設定情報はオプションとして、次の限定的ではないリストの１つまたは複数のような、様々なタイプの情報を含む：つまり、提供されるコンピュータネットワークの複数のコンピューティングノードに割り当てる複数の特定されたネットワークアドレス、提供されるコンピュータネットワーク用に特定されたネットワークトポロジ情報、および提供されるコンピュータネットワーク用に特定されたネットワークアクセス制限である。複数の特定されたネットワークアドレスは、例えば、１つまたは複数のネットワークアドレスの範囲を含むことができ、提供されるコンピュータネットワークが、クライアントのリモートプライベートコンピュータネットワークへの拡張である場合は、リモートプライベートコンピュータネットワーク用に使用される仮想および／またはプライベートのネットワークアドレスのサブセットに対応し得る。特定されたネットワークトポロジ情報は、例えば、提供されるコンピュータネットワークの一部となり、かつ特定の指定済みネットワークアドレスを有するコンピューティングノードを管理するかまたは別の方法でそれらに関連付けられた１つまたは複数のネットワーキング装置（例えば、ルータ、スイッチなど）の特定、またはそうでなければ、提供されるコンピュータネットワークのサブネットもしくは提供されるコンピュータネットワークのコンピューティングノードの別のグループの特定などによって、グループにまとめられるか、また別の方法で共通の相互通信特性を共有する提供されるコンピュータネットワークのコンピューティングノードのサブセットを指示することができる。特定されたネットワークアクセス制限情報は、例えば、提供されるコンピュータネットワークのコンピューティングノードの１つまたは複数の各々について、提供されるコンピュータネットワークのコンピューティングノードが、提供されるコンピュータネットワークの外部にある任意のコンピューティングノードとの通信を許可されているか否か（または、提供されるコンピュータネットワークが既存の別のコンピュータネットワークへの拡張である場合に、

提供されるコンピュータネットワークのコンピューティングノードが、それが属するその別のコンピュータネットワークの外部にある任意のコンピューティングノードとの通信が許可されているか否か）を含めて、別のコンピューティングノードのどれがそのコンピューティングノードと相互接続できるか、および／またはそのコンピューティングノードとの間で許可されている通信のタイプを特定することができる。設定可能ネットワークサービスの実施形態によって提供されるコンピュータネットワークの作成および設定については、以下でさらに詳述する。

【０００８】

また、少なくともいくつかの実施形態では、クライアントにコンピュータネットワークを提供するために設定可能ネットワークサービスによって使用されるコンピューティングノードは、各々が１つまたは複数の物理コンピューティングシステム上でホストされる物理コンピューティングシステムおよび／または仮想マシンなど、種々の形態をとることができる。例えば、いくつかの実施形態では、設定可能ネットワークサービスは、１つまたは複数の地理的位置にある１つまたは複数のデータセンタなど、クライアントに提供されるコンピュータネットワークで利用可能になる設定可能ネットワークサービスによって提供される多数のコンピューティングノードを含むことができる。さらに、少なくともいくつかの実施形態では、設定可能ネットワークサービスで提供されるコンピューティングノードの一部または全ては、１つまたは複数の中間物理ネットワークで相互接続され、かつ、クライアントに提供されるコンピュータネットワークは、その中間物理ネットワークを基板ネットワークとして使用することによりその中間物理ネットワークの上に重ねられた仮想（または「論理」）ネットワークでもよい。その上、少なくともいくつかの実施形態では、少なくともいくつかのコンピューティングノードは、複数の顧客またはプログラム実行サービスの別のユーザのために複数のプログラムを実行するプログラム実行サービス（または「ＰＥＳ」）によって使用され得る。コンピューティングノードおよび基礎となるコンピュータネットワークに関する詳細については以下で述べられており、クライアントへの仮想ネットワークの提供およびプログラム実行サービスの提供の実施形態例に関する詳細については、２００６年3月３１日に出願された「Ｍａｎａｇｉｎｇ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｂｅｔｗｅｅｎ Ｃｏｍｐｕｔｉｎｇ Ｎｏｄｅｓ」という名称の米国特許出願番号第１１／３９４，５９５号（代理人整理番号１２０１３７．５２４）、２００６年3月３１日に出願された「Ｍａｎａｇｉｎｇ Ｅｘｅｃｕｔｉｏｎ ｏｆ Ｐｒｏｇｒａｍｓ ｂｙ Ｍｕｌｔｉｐｌｅ Ｃｏｍｐｕｔｉｎｇ Ｓｙｓｔｅｍｓ」という名称の米国特許出願番号第１１／３９５，４６３号（代理人整理番号１２０１３７．５２５）、２００７年3月２７日に出願された「Ｃｏｎｆｉｇｕｒｉｎｇ Ｉｎｔｅｒｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｂｅｔｗｅｅｎ Ｃｏｍｐｕｔｉｎｇ Ｎｏｄｅｓ」という名称の米国特許出願番号第１１／６９２，０３８号（代理人整理番号１２０１３７．５５４）、２００８年3月３１日に出願された「Ｃｏｎｆｉｇｕｒｉｎｇ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｂｅｔｗｅｅｎ Ｃｏｍｐｕｔｉｎｇ Ｎｏｄｅｓ」という名称の米国特許出願番号第１２／０６０，０７４号（代理人整理番号１２０１３７．５７６）、および２００７年6月１８日に出願された「Ｐｒｏｖｉｄｉｎｇ Ｅｎｈａｎｃｅｄ Ａｃｃｅｓｓ Ｔｏ Ｒｅｍｏｔｅ Ｓｅｒｖｉｃｅｓ」という名称の米国特許出願番号第１１／７６４，７３９号（代理人整理番号１２０１３７．５５５）に含まれており、その各々が全体の参照により本明細書に組み込まれる。

【０００９】

いくつかの実施形態において、クライアントは、例えばインターネットまたは別の公衆網を経由してアクセス可能であるか、またはそうでなければ提供されるコンピュータネットワークの外部にあってかつその一部でない、別のリモートネットワークアクセス可能サービスなど、提供されるコンピュータネットワークからリモートの１つまたは複数の別のネットワークアクセス可能サービスへのアクセスを提供するため、設定可能ネットワークサービスで提供されるコンピュータネットワークをさらに設定できる。かかるリモートサービスの少なくともいくつかは、いくつかの実施形態において、設定可能ネットワークサ

ービスと関連していてもよく（例えば、設定可能ネットワークサービスの運営者または関連団体による提供、設定可能ネットワークサービスによってその別のクライアントに提供されるコンピュータネットワーク経由など、設定可能ネットワークサービスの別のクライアントによる提供などによって）、かかるリモートサービスの少なくともいくつかは、いくつかの実施形態では、代わりに設定可能ネットワークサービスから独立していてもよい。かかる別のリモートサービスは、種々の実施形態で種々の形態をとることができ、これには、リモートコンピューティングシステムで使用するために１つまたは複数のタイプのコンピューティング関連資源へのネットワークアクセスを提供するサービス（例えば、格納されたデータ資源へのアクセスを提供するストレージサービス、メッセージキュー資源または別の格納されたメッセージ資源へのアクセスを提供するメッセージサービス、格納されたデータベース資源へのアクセスを提供するデータベースサービス、プログラム実行資源へのアクセスを提供するプログラム実行サービスなど）、または別の方法で情報または機能または他の役立つ資源へのアクセスを提供するサービス（例えば、株価情報資源または検索クエリ結果資源を提供するサービス、写真共有機能資源またはソーシャルネットワーキング能力資源を提供するサービスなど）などがある。いくつかの状況では、設定可能ネットワークサービスの一実施形態は、データセンタまたは別の地理的位置に複数のコンピューティングノードを提供することができ、さらに、これらのコンピューティングノードのサブセットを使用して、様々なクライアントに様々なコンピュータネットワークを（例えば、提供されるコンピュータネットワークの各々を、共通の基板ネットワークを共有する別個の仮想ネットワークとして）提供することができる、つまり、かかる状況では、１つのクライアントは、その地理的位置で別の提供されるコンピュータネットワークを使用して別のクライアントで提供される１つまたは複数のネットワークアクセス可能リモートサービスへのアクセスを提供するために、例えばそのクライアントが、それらのリモート資源が同一の地理的位置で別のコンピューティングノードによって物理的に提供されていることを認識することなく、提供されるコンピュータネットワークをそのクライアント用に設定することが可能である。

【００１０】

少なくともいくつかの実施形態では、クライアントは、特定の資源サービスへアクセス用の機構を含め、そのアクセス機構が、提供されるコンピュータネットワークに種々の機能を提供できるように、その提供されるコンピュータネットワークをそのクライアント用に設定できる。一具体例として、いくつかの実施形態では、複数の関連付けられた仮想ネットワークアドレスを持つ提供される仮想コンピュータネットワークは、特定のリモート資源サービスを表すために、それら仮想ネットワークアドレスの１つ（または複数）を割り当てて、提供されるコンピュータネットワークのコンピューティングノードまたは別の参加者が、その提供されるコンピュータネットワークにローカルな代表の割当てられたネットワークアドレスを利用して、提供されるコンピュータネットワークの外部にあるリモート資源サービスと通信できるようにする。このように、提供されるコンピュータネットワークの外部との通信を防ぐために（例えば、インターネットまたは１つもしくは複数の別の公衆網を通過するような通信を防ぐため）ネットワークアクセス制限を用いて設定された提供されるコンピュータネットワークでさえ、提供されるコンピュータネットワークの一部であるかかる設定されたアクセス機構を経由して、特定の外部リモート資源サービスへの通信が許可されるように設定できる。

【００１１】

さらに、少なくともいくつかの実施形態では、提供されるコンピュータサービスから、その提供されるコンピュータネットワークの設定されたアクセス機構を経由したリモート資源サービスへのかかる通信用に強化されたセキュリティを提供するために、種々の技術が使用できる。例えば、少なくともいくつかの実施形態では、特定のリモート資源サービスは、インターネットまたは別の公衆網を経由して（例えば、１つまたは複数の公衆網アドレスおよび関連したドメイン名を経由して）ユーザが利用できる公的アクセス可能なインタフェースを持つことができるが、例えば、特定のリモート資源サービスが設定可能ネ

ットワークサービスと同一の運営者によって提供されているか、そうでなければその設定可能ネットワークサービスに関連している場合など、コンピューティングノードを相互接続するために、その設定可能ネットワークサービスで使用される基板ネットワークから直接アクセス可能なインタフェースを実装することもできる。かかる直接アクセス可能なインタフェースが特定のリモート資源サービス用の基板ネットワーク上で実装されている場合、設定可能ネットワークサービスの１つまたは複数の提供されるコンピュータネットワークは各々、そのリモート資源サービスを対象とした通信を、そのリモート資源サービスのリモートから公的アクセス可能なインタフェースではなく、基板ネットワーク上に実装されたそのインタフェースへ向ける、そのリモート資源サービス用の設定されたアクセス機構を持つ。そのリモート資源サービスはそれゆえ、少なくともいくつかの実施形態および状況において、少なくともいくつかのクライアント要求のためにリモート資源サービスの機能の一部または全てを設定可能ネットワークサービスにローカルな方法で提供することを（例えば、そのローカル機能を実装するために、設定可能ネットワークサービスの１つまたは複数のコンピューティングノードが使用される場合）選択し、一方、別の実施形態および状況では、リモート資源サービスは、設定可能ネットワークサービスの基板ネットワークから、そのリモート資源サービスのリモート位置への１つまたは複数の公衆網を介した通信を安全な方法で管理することにより、かかるクライアント要求の少なくともいくつかに対して、一部または全ての機能を提供できる。あるいは、少なくともいくつかの実施形態において、設定可能ネットワークサービスは、設定可能ネットワークサービスから１つまたは複数の公衆網を介してそのリモート資源サービスのリモート位置への安全な通信を同様の方法で提供するために、例えば、そのリモート資源サービスにアクセス可能な方法での通信の暗号化および／または信頼できるソースからとしてのその通信の認証などにより、少なくともいくつかのリモート資源サービスに対して追加の動作を行うことができる。提供されるコンピュータネットワークからリモート資源のアクセスについては、以下でさらに詳述する。

【００１２】

また、少なくともかかる実施形態のいくつかでは、クライアント用に提供されるコンピュータネットワークは、ネットワークアクセス可能なリモート資源サービスで提供されるコンピューティング関連資源の特定のサブセット（例えば、そのクライアントに対応するサブセットなど）へのアクセスを受けるように設定できる。一例として、リモート資源サービスは、それ自身の提供される資源を、異なるアクセス権を持つ異なるグループに分割し、かつ別々に参照される別個の名前空間を使用することができ、異なる名前空間の異なる資源が同一のローカル名または別の識別子を持つことができるが、それらの名前空間に基づいて別々に参照されるようになり、特定の名前空間が特定のクライアントに対応する。そうである場合、クライアント用に提供されるコンピュータネットワークは、各々がそのリモート資源サービスの特定の名前空間に自動的に対応するように設定された特定のリモート資源サービスにアクセスするための１つまたは複数の機構を含むことができ、その提供されるコンピュータネットワークのコンピューティングノードは、設定されたアクセス機構を使用して、そのクライアントの特定の対応する名前空間内の資源にアクセスできるようになる。さらに、少なくともいくつかの実施形態では、提供されるコンピュータネットワークのコンピューティングノードは、設定された機構が対応する名前空間を認識していない可能性があり、コンピューティングノードは、名前空間のコンテキスト内において、対象とする資源の名前または別の識別子を指示するリモート資源サービスに対して、しかしその名前空間の実際の指示なしで、要求または別のメッセージを送信できるようになる。そうである場合、設定されたアクセス機構は、メッセージを自動的に変更または変換し、オプションとしてその変更または変換をそのメッセージを送信したコンピューティングノードに対して透過的にして、指示された名前または別の識別子が設定されたアクセス機構に対応する名前空間に関連付けられるようにする。

【００１３】

提供されるコンピュータネットワークの設定およびリモート資源サービスを表すアクセ

ス機構は、種々の方法で実行することができる。例えば、いくつかの状況では、クライアントは、リモート資源サービス内でそのクライアントの既存の名前空間（そのクライアントが特定の資源を事前に格納したかまたは別の方法で使用した名前空間など）を特定できる。あるいは、別の実施形態では、設定可能ネットワークサービスは、例えば、新規の名前空間を作成するためにリモート資源サービスとやりとりすることなどにより、その提供されるコンピュータネットワークからアクセスされる新規の資源用のリモート資源サービス内で新規の名前空間の使用を自動的に開始することができる。リモート資源サービスとのかかるやりとりは、そのクライアントが提供されるコンピュータネットワークを作成および設定している時、またはその代わりに後で（例えば、提供されるコンピュータネットワーク上のコンピューティングノードが設定されたアクセス機構を介してリモート資源サービスに初めてアクセスしようとする時）など、さまざまな時に実行され得る。さらに、少なくともいくつかの実施形態および状況では、設定可能ネットワークサービスは、提供されるコンピュータネットワークに関連付けられた一意の識別子を生成し、その識別子を使用して新規の名前空間を参照することができ、他方、別の実施形態では、リモート資源サービスは、作成された新規の名前空間のかかる識別子または別の指示を提供することができる。いずれの場合も、クライアントおよび提供されるコンピュータネットワークのコンピューティングノードは、オプションとして、新規で自動的に開始された名前空間および／またはその新規の名前空間を参照するために設定可能ネットワークサービスで使用された一意の識別子を認識しないことができる。また、いくつかの実施形態では、新規の名前空間を参照するためにその識別子が設定可能ネットワークサービスで使用されるか、または代わりに別の方法で行われることをそのクライアントが認識しているか否かに関わらず、そのクライアントは、設定可能ネットワークサービスによりそのクライアントに提供されるコンピュータネットワークに関連付けられる設定可能ネットワークサービスで使用される識別子を特定することができる。さらに、少なくともいくつかの実施形態では、クライアントに提供されるコンピュータネットワークに関連付けられた識別子は、そのクライアントが単一の提供されるコンピュータネットワークを有する場合など、そのクライアントに関連付けられた識別子のこともあるが、他方、別の実施形態では、提供されるコンピュータネットワークの識別子は、クライアントに固有のいずれの識別子とも異なる。名前空間の使用については、以降で詳述する。

【００１４】

さらに、少なくともいくつかのかかる実施形態において、クライアント用に提供されるコンピュータネットワークが特定のリモート資源サービスから資源にアクセスするために使用するアクセス機構は、例えば、通信が特定の位置から送信されたことを確認するためなど（例えば、その同一のクライアントでさえ別の位置から特定の資源にアクセスするのを防ぐため）、提供されるコンピュータネットワークから受信された通信の認証および確認時に、リモート資源サービスを支援するように設定することができる。例えば、少なくともいくつかのリモート資源サービスは、そのリモート資源サービスによって提供される資源の各々が、１つまたは複数の関連したアクセス制御インディケータ（例えば、名前または別のテキスト識別子、数値識別子、タグまたは別のアクセスキー、認証情報など）を持つことを許可または要求でき、リクエスタがそれらの関連したインディケータの全てを提供する場合に限り、かかる資源を外部のリクエスタがアクセスできるようになる。かかるリモート資源サービスに関して、クライアント用に提供されるコンピュータネットワークのコンピューティングノードで使用されるアクセス制御インディケータの１つは、そのリモート資源サービスでの、そのクライアント用の顧客識別子など、そのクライアントに対応する識別子であり得る。クライアント用の単一の顧客識別子が資源に関連付けられている場合に限り、そのクライアントは、同一の単一の顧客識別子を提供することによりそのクライアントの別のリモートコンピューティングシステムからその資源にアクセスすることが可能になる。例えば、かかる資源は、クライアントからの要求に応じて作成されるか、または別の方法でアクセスされて、そのクライアントに（例えば、一時的に）関連付けられる。

【００１５】
しかし、少なくともいくつかの実施形態では、クライアント用に提供されるコンピュータネットワークが特定のリモート資源サービスから資源にアクセスするために使用する設定されたアクセス機構は、１つまたは複数の別の追加のアクセス制御インディケータを含めるために、リモート資源サービスに送信される通信を変更するように設定できる。かかる別の追加のアクセス制御インディケータは、例えば、設定可能ネットワークサービスで自動的に生成される提供されるコンピュータネットワークに対応する識別子を含むことができ、さらに、少なくともいくつかの実施形態では、そのクライアントおよび／または提供されるコンピュータネットワークのコンピューティングノードは、使用される特定の追加のアクセス制御インディケータを認識しないか、またはかかる追加のアクセス制御インディケータのいずれの存在および使用を認識さえしない。１つまたは複数の追加のアクセス制御インディケータがそのクライアントに未知である場合、そのクライアントは、その資源へのアクセス要求でかかる資源に関連付けられた全てのインディケータを別の方法では提供しないため、そのクライアントは、その設定されたアクセス機構を経由して提供されるコンピュータネットワーク以外からは、それらの資源にアクセスすることができない。このため、前述のとおり、かかる追加のアクセス制御インディケータは、リモート資源サービスによって資源へのアクセス要求のソースまたは位置のインディケータとして使用でき、別の位置からの要求にはその資源へのアクセスが付与されないようになる。あるいは、例えば、その資源用の全てのアクセス制御インディケータが提供される場合に限り、その資源への書込みアクセスまたは変更アクセスを許可するが、別の状況ではその資源への読取りアクセスまたは他のアクセスが許可されるように資源を設定する場合や、そのクライアント固有の識別子が提供される場合にもう１つ別の位置からのクライアントによって要求される場合、アクセス制御インディケータのいずれも提供することなく誰かによって要求される場合など、別の位置からの要求には、かかる資源への別の異なるアクセスが付与される。さらに、かかる追加のアクセス制御インディケータは、自動生成されたランダムな英数字インディケータ、提供されるコンピュータネットワークに関連した実際の地理的位置の指示など、種々の形態をとることができる。

【００１６】
名前空間で使用するのと同様の方法で、提供されるコンピュータネットワークが１つまたは複数のかかる追加のアクセス制御インディケータを使用するようにするためのアクセス機構の設定は、種々の方法で実行することができる。例えば、いくつかの実施形態において、クライアントは、リモート資源サービスへの設定されたアクセス機構で使用するために、提供されるコンピュータネットワークに関連付けるべき１つまたは複数の追加のインディケータを特定することができる。また、別の実施形態では、設定可能ネットワークサービスは、提供されるコンピュータネットワーク用のリモート資源サービスへの設定されたアクセス機構用の１つまたは複数の新規の追加インディケータの使用を（例えば、提供されるコンピュータネットワークに関連付けられた一意の識別子の生成および使用などによって）自動的に開始することができ、そのリモート資源サービスからその設定されたアクセス機構を経由してアクセスされる新規の資源が、その提供されるコンピュータネットワークからのみアクセス可能になる。さらに、以降でさらに詳述するように、設定可能ネットワークサービスのいくつかの実施形態では、基板ネットワークを経由した通信の送信を容易にするためなど、提供されるコンピュータネットワークのコンピューティングノード間での通信を管理するために種々のモジュールを使用でき、そうである場合、名前空間識別子および／またはアクセス制御インディケータを含むように通信を自動的に変更すること、および／または１つまたは複数の公衆網を経由して特定のリモート資源サービスへ通信を転送する（オプションとして変更の後に）ことにより、１つまたは複数のかかるモジュールを特定のアクセス機構を実装するように設定できる。提供されるコンピュータネットワークからの位置に固有の通信を確認する際のリモート資源サービスの支援を含め、アクセス機構の実装については、以降でさらに詳述する。

【００１７】

少なくともいくつかの実施形態において、設定可能ネットワークサービスは、クライアントがその設定可能ネットワークサービスとプログラムでやりとりできるようにするＡＰＩを追加で提供して、その設定可能ネットワークサービスが、その設定可能ネットワークサービスによってクライアントに提供されるコンピュータネットワークへのクライアントのリモートアクセスの確立を容易にする動作を行うようにする。かかるリモートアクセス確立ＡＰＩは、種々の実施形態において種々の動作を実行でき、さらに、少なくともいくつかの実施形態において、クライアントのリモート位置から設定可能ネットワークサービスによってそのクライアント用に提供されるコンピュータネットワークへのＶＰＮ接続の確立時にクライアントを支援する。前述のように、状況によっては、クライアントは、設定可能ネットワークサービスの外部にリモートプライベートコンピュータネットワークを有することができ、その設定可能ネットワークサービスによって作成および提供されるコンピュータネットワークは、リモートプライベートネットワークへの拡張であるか、またはそうでない場合はそのリモートプライベートネットワークに接続され得る。別の状況では、クライアントは、１つまたは複数のリモートコンピューティングシステムを使用して、その設定可能ネットワークサービスにより提供されるコンピュータネットワークに対してアクセスし、やりとりすることができる。いずれの状況でも、そのクライアントは、少なくともいくつかの実施形態において、リモートプライベートネットワークまたは別のリモートコンピューティングシステムから、その設定可能ネットワークサービスによって提供されるコンピュータネットワークへのＶＰＮ接続または別の安全な接続を使用することができる。かかる実施形態において、設定可能ネットワークサービスにより提供されるリモートアクセス確立ＡＰＩは、その設定可能ネットワークサービスのクライアントによりプログラムで起動される際、その設定可能ネットワークサービスがそのクライアントに対して１つまたは複数の適切なネットワーク設定要素の提供を開始するようにして、そのクライアントのリモートプライベートネットワークまたは別のリモートコンピューティングシステムが、その設定可能ネットワークサービスによって提供されるコンピュータネットワークへのＶＰＮ接続または別の安全な接続を確立できるようにする。例えば、かかるネットワーク構成要素は、１つまたは複数のハードウェア装置（例えば、ルータまたは別のネットワーキング装置）、ソフトウェア構成要素、および／または一連の設定情報を含むことができる。

【００１８】

例えば、いくつかの実施形態において、クライアントによってリモートアクセス確立ＡＰＩを起動することにより、設定可能ネットワークサービスが、クライアントのリモート位置に配達される適切なルータ装置または別のハードウェアネットワーキング装置を購入するかまたは別の方法で入手するために、販売業者とやりとりし、さらに、その入手したネットワーキング装置用に適切に設定されたソフトウェアまたは別の設定情報がそのクライアントに送達されるようになり、これによって、その装置が、そのソフトウェアを使用してまたはその設定情報に基づいて設定されて、そのクライアントの１つまたは複数のリモートコンピューティングシステムに接続されると、その設定可能ネットワークによってそのクライアント用に提供されるコンピュータネットワークとの通信を開始する。このようにして、クライアントがネットワーキング装置、ソフトウェアおよび／または設定情報を受け取ると、そのクライアントは、例えば、受け取ったネットワーキング装置をリモートプライベートネットワークまたは別のリモートコンピューティングシステムに接続し、そのソフトウェアおよび／または設定情報を使用してその受け取ったネットワーキング装置を設定する。すると、その設定されたネットワーキング装置は、そのクライアント用に提供されるコンピュータネットワークと自動的に通信しＶＰＮ接続を確立し、提供されるコンピュータネットワークへのそのクライアントのプライベートで安全なアクセスを可能にする。別の状況では、設定されたネットワーキング装置は、そのクライアント用に提供されるコンピュータネットワークに特有の追加設定情報を取得するため、まず設定可能ネットワークサービスの設定されたコンピューティングシステムと自動的にやりとりし、その後、その提供されるコンピュータネットワークへのＶＰＮ接続を自動的に確立する。

【００１９】
かかる実施形態において、ネットワーキング装置をクライアントに提供するために利用される販売業者は、オンライン販売業者または設定可能ネットワークサービスを運営する同一の運営者によって運営されるかもしくは別の方法でその設定可能ネットワークサービスと提携している別の小売業者、またはその設定可能ネットワークサービスと無関係な第三者の販売業者など、種々の形態を取ることができる。使用されるハードウェア装置は、自動的に検出および／またはクライアントによって特定され得るなど、その設定可能ネットワークサービスによって提供されるコンピュータネットワークとの互換性および／またはそのクライアントが使用中のリモートコンピューティングシステムとの互換性に基づいて選択されることを含め、種々の実施形態において種々の方法で同様に選択することができる。さらに、いくつかの実施形態では、リモートアクセス確立ＡＰＩを最初に起動する時、または後で設定可能ネットワークサービスからのクエリ（例えば、クライアントが選択可能な複数の選択肢を指定するクエリ）に応じて、クライアントによって特定し得るなど、クライアントが選択可能な複数の選択肢を利用することができる。別の実施形態では、単一のタイプのネットワーキング装置または別のハードウェア装置が使用できる。さらに、設定されたソフトウェアおよび／または他の設定情報は、種々のソースからクライアントに提供でき（例えば、ネットワーキング装置を提供した同一の販売業者から、設定可能ネットワークサービスから直接、またはもう１つ別の団体から）、かつ種々の方法で提供できる（例えば、ソフトウェアおよび／または設定情報をクライアントへ電子的に送信する、ＤＶＤまたはＵＳＢメモリキーなどの物理装置の可読媒体上へソフトウェアおよび／または設定情報を格納し、その媒体をクライアントへ物理的に配達する、装置の事前設定などのように、ソフトウェアおよび／または設定情報をネットワーキング装置に格納してから、それらをクライアントに配達する）。さらに、いくつかの実施形態では、クライアントに提供される設定されたソフトウェアは、クライアントが既にリモート位置に有する１つまたは複数のコンピューティングシステムまたは別のハードウェア装置と一緒に使用する場合など、ＶＰＮ接続を確立するのに十分であり得る。

【００２０】
さらに、クライアントのための小売業者または別の第三者団体からのハードウェア装置の取得は、その装置の購入またはその代わりに別の方法での取得（例えば、リース、賃貸、一時的評価での取得など）など、種々の実施形態において種々の方法で実行でき、かつ、いくつかの実施形態では、その小売業者への支払提供およびその後の別途クライアントからの支払受取り（例えば、クライアントからの支払金額が小売業者への支払金額を超えて、未満、または同額で）を行うか、または別の方法でクライアントに小売業者に対して直接支払提供をさせる（例えば、設定可能ネットワークサービスが小売業者にクライアント用の支払情報を提供する、設定可能ネットワークサービスが支払情報取得のために小売業者にクライアントとの連絡または別の方法でのやりとりのための情報を提供する、小売業者に支払受取りのためクライアントから事前に取得した情報を使用させるなどの方法で）設定可能ネットワークサービスを含むことができる。さらに、いくつかの実施形態では、クライアントのために小売業者からハードウェア装置の取得を開始すると、小売業者からクライアントのリモート位置にハードウェア装置が直接配達されるが、他方、別の実施形態では、設定可能ネットワークサービスが最初にハードウェア装置の配達を受け、その後それをクライアントに配達するなど（例えば、適切なソフトウェアおよび／または設定情報を使用してハードウェア装置を設定した後、またはその代わりにハードウェア装置を受け取った時点と同じ形でクライアントに転送することにより）、別の方法で取得を実行することができる。種々の実施形態において設定可能ネットワークサービスによりクライアントのリモートアクセス確立ＡＰＩのプログラム起動を実行するための動作については、以降でさらに詳述する。

【００２１】
例示を目的として、特定のタイプのコンピューティングノード、ネットワーク、通信、および設定操作が実行される、いくつかの実施形態が以下で説明される。これらの例は、

例示を目的として提供され簡潔さのために単純化されており、また、独創的な技術は多岐にわたる別の状況で使用することが可能であり、そのうちのいくつかの状況について以下で説明する。例えば、いくつかの実施形態では、クライアントによるアクセスのために作成および設定されるコンピュータネットワークは、それらのクライアントの既存のプライベートコンピュータネットワークへのプライベートコンピュータネットワーク拡張であり、他方、別の実施形態では、作成および設定されるコンピュータネットワークは、別のコンピュータネットワークへの拡張ではない独立のネットワーク、および／または、ネットワークが作成および設定されるクライアントによってプライベートにはアクセスできない公衆のコンピュータネットワークでもよい。さらに、いくつかの実施形態では、設定可能ネットワークサービスによって提供されるコンピュータネットワークは、その設定可能ネットワークサービスで提供および制御されるコンピューティングノードを使用し、他方、別の実施形態では、提供されるコンピュータネットワークで使用される少なくともいくつかのかかるコンピューティングノードは、他者（例えば、第三者、クライアントなど）によって制御または保守され得るが、その設定可能ネットワークサービスで利用可能にできる。

【００２２】

図１Ａは、リモートクライアントがそのクライアントによる使用のためにコンピュータネットワークを作成および設定できるようにする設定可能ネットワークサービスの実施形態例を示すネットワーク図である。この例では、作成および設定されるコンピュータネットワークは、クライアントの既存のプライベートコンピュータネットワークへのプライベートネットワーク拡張であり、設定可能ネットワークサービス１０５は、１つまたは複数の公衆網１００を経由して（例えば、インターネットを経由して）クライアント（図示せず）にかかる機能を提供する。このため、リモートクライアントは、例えば、公衆網１００を経由してクラウドコンピューティング技術を使用するなど、設定可能ネットワークサービス（ＣＮＳ）１０５を使用して、それらのプライベートコンピュータネットワークの規模および／または能力を動的に変更できる。

【００２３】

具体的には、図１Ａの例では、多数のクライアント（図示せず）が、リモートで既存のクライアントプライベートネットワーク１３０への種々のプライベートコンピュータネットワーク拡張１２０を作成および設定するために公衆網１００を経由してマネージャモジュール１１０とやりとりしているが、コンピュータネットワーク拡張１２０のうちの少なくともいくつかは、公衆網１００を経由して（例えば、相互接続１００ａおよび１００ｂを介して確立されたＶＰＮ接続を経由して）１つまたは複数の対応するクライアントプライベートネットワーク１３０から安全なプライベートアクセスが可能になるように設定されている。この実施形態例では、マネージャモジュール１１０は、例えばＣＮＳ１０５の様々な別のモジュール（図示せず）ならびにＣＮＳ１０５によってプライベートコンピュータネットワーク拡張１２０を提供するために使用される種々のコンピューティングノードおよびネットワーキング装置（図示せず）と連携などして、ＣＮＳ１０５の機能をリモートクライアントに提供するのを支援する。少なくともいくつかの実施形態では、ＣＮＳマネージャモジュール１１０は、ＣＮＳ１０５の１つまたは複数のコンピューティングシステム（図示せず）上で実行することができ、リモートコンピューティングシステムがモジュール１１０とプログラムでやりとりして、クライアントのためにＣＮＳ１０５の一部または全ての機能にアクセスできるようにする１つまたは複数のＡＰＩを提供することができる（例えば、プライベートネットワーク拡張１２０の作成、設定、および／または使用の開始のため）。さらに、少なくともいくつかの実施形態において、クライアントはかかる動作の一部または全てを実行するために、代わりにモジュール１１０と手動でやりとりする（例えば、モジュール１１０によって提供されるユーザインタフェース経由で）ことができる。

【００２４】

例えば、公衆網１００は、インターネットなど、（おそらく個別の団体によって運営さ

れている）接続されたネットワークの公的にアクセス可能なネットワークでもよい。リモートクライアントプライベートネットワーク１３０の各々は、特権のないユーザには部分的または完全にアクセス不可能であって、かつクライアントのコンピューティングシステムおよび／または別のネットワーク装置を含む、企業または別のプライベートネットワーク（例えば、家庭、大学など）のような、１つまたは複数の既存のプライベートネットワークを含む。図示例では、提供されるネットワーク拡張１２０の各々は、複数のコンピューティングノード（図示せず）を含み、それらのうちの少なくともいくつかは、ＣＮＳ１０５によって提供されるか、またはそうでない場合はＣＮＳ１０５の制御下にあり、かつ提供されるネットワーク拡張１２０の各々は、それらが提供されるクライアントによって種々の方法で設定することができる。例示した実施形態におけるネットワーク拡張１２０の各々は、それを作成するクライアントによってのみアクセス可能なプライベートコンピュータネットワークの可能性があるが、別の実施形態では、ＣＮＳによりクライアントに対して提供される少なくともいくつかのコンピュータネットワークは、他の既存のコンピュータネットワークへの拡張ではない公的にアクセス可能および／または単独のコンピュータネットワークであり得る。同様に、この例では、提供されるコンピュータネットワーク１２０は、プライベートネットワークであるリモートクライアントコンピュータネットワーク１３０への拡張であるが、別の実施形態では、提供されるコンピュータネットワーク１２０は、プライベートネットワークではないクライアントコンピュータネットワーク１３０への拡張であり得る。

【００２５】

リモートクライアントプライベートコンピュータネットワーク１３０とクライアントに提供される対応するプライベートコンピュータネットワーク拡張１２０との間のプライベートアクセスは、例えば、公衆網１００を介した相互通信を安全でプライベートな方法で可能にするＶＰＮ接続または別の安全な接続をそれらの間に確立することなどにより、種々の方法で有効にされる。例えば、ＣＮＳ１０５でホストされる１つまたは複数のＶＰＮ機構（例えば、ソフトウェアおよび／またはハードウェアＶＰＮ機構）の自動設定などにより、ＣＮＳ１０５は、そのコンピューティングノードおよび別のコンピューティングシステム上で適切な設定を自動的に実行して、クライアントの特定のプライベートネットワーク拡張１２０へのＶＰＮアクセスを可能にでき、および／またはクライアントに適切な設定情報（例えば、認証情報、アクセスポイント、および／または他のパラメータ）を自動的に提供して、リモートクライアントプライベートネットワーク１３０上でホストされるＶＰＮ機構がＶＰＮアクセスを確立できるようにする。ＶＰＮアクセスが適切に有効にされかつ／または設定されると、ＶＰＮ接続がリモートクライアントプライベートネットワークとプライベートネットワーク拡張との間で、例えば、ＩＰｓｅｃ（インターネットプロトコルセキュリティ）または他の適切な通信技術を使用してクライアントにより開始されるなどして、確立される。例えば、いくつかの実施形態では、ＶＰＮ接続または別の安全な接続を、例えばＩＰｓｅｃに基づくＶＰＮなどの代わりに、データ送信用のＭＰＬＳ（マルチプロトコルラベルスイッチング）を使用するネットワークに対してまたはネットワークとの間に確立できる。例えば、ＣＮＳ１０５で提供される対応するリモートアクセス確立ＡＰＩのクライアント起動に応じてなど、安全な接続の有効化および確立については、別の箇所で詳述する。

【００２６】

また、例示した実施形態では、種々のネットワークアクセス可能なリモート資源サービス１４０は、リモートクライアントプライベートネットワーク１３０上のコンピューティングシステムを含め、公衆網１００を介してリモートコンピューティングシステムが利用可能である。資源サービス１４０は、例えば、資源サービス１４０の少なくともいくつかがリモートコンピューティングシステムに各種コンピューティング関連資源へのアクセスを提供するなど、種々の機能をリモートコンピューティングシステムに提供することができる。さらに、ＣＮＳ１０５で提供されるプライベートネットワーク拡張１２０の少なくともいくつかは、リモート資源サービス１４０の少なくともいくつかへのプライベートア

クセスまたは別の専用アクセスを提供するように設定することができるが、このとき、リモート資源サービス１４０との実際の通信は公衆網１００を経由して（例えば、相互接続１００ｂおよび１００ｃを経由して）生じるが、その提供されるアクセスは、オプションとして、プライベートネットワーク拡張１２０のコンピューティングノードには、プライベートネットワーク拡張１２０の一部である仮想接続１１５を経由してローカルに提供されているように見える。リモート資源サービスへのかかるプライベートアクセスまたは別の専用アクセスの確立および使用についての詳細は、別の箇所で詳述する。

【００２７】

前述のとおり、提供されるネットワーク拡張１２０の各々は、クライアントにより種々の方法で設定され得る。例えば、少なくともいくつかの実施形態では、ＣＮＳ１０５は、クライアントに提供されるネットワーク拡張での使用が可能な複数のコンピューティングノードを提供し、提供されるネットワーク拡張１２０の各々は、その提供されるネットワーク拡張の一部として専用に使用される複数のかかるコンピューティングノードをクライアントによって設定された数だけ含むことができる。具体的には、クライアントは、モジュール１１０とやりとりして、クライアント用に提供されるコンピュータネットワークに当初に含まれるコンピューティングノードの数を設定することができる（例えば、ＣＮＳ１０５で提供されるＡＰＩとの１つまたは複数のプログラムによるやりとりを通して）。また、少なくともいくつかのかかる実施形態では、提供されるコンピュータネットワークがクライアントによって既に使用されるようになった後などに（例えば、特定のコンピューティングノード上で特定プログラムの実行の開始または終了を指示することにより）、クライアントの提供されるコンピュータネットワークに対して、後で動的にコンピューティングノードの追加または除去を行うことができる（例えば、ＣＮＳ１０５で提供されるＡＰＩとの１つまたは複数のプログラムによるやりとりを通して）。さらに、ＣＮＳ１０５は、例えば、種々の性能特性（例えば、プロセッサ速度、利用可能なメモリ、利用可能なストレージ）および／または別の能力を持つコンピューティングノードなど、少なくともいくつかの実施形態において、複数の異なるタイプのコンピューティングノードを提供することができる。そうである場合、少なくともいくつかのかかる実施形態では、クライアントは、そのクライアント用に提供されるコンピュータネットワークに含めるコンピューティングノードのタイプを指定できる。

【００２８】

また、少なくともいくつかの実施形態では、クライアントは、モジュール１１０とやりとりして、そのクライアント用に提供されるコンピュータネットワーク用のネットワークアドレスを設定することができ（例えば、ＣＮＳ１０５で提供されるＡＰＩとの１つまたは複数のプログラムによるやりとりを通して）、提供されるコンピュータネットワークがクライアントによって既に使用されるようになった後などに、少なくともいくつかのかかる実施形態では、提供されるコンピュータネットワークに対して、後で動的にネットワークアドレスの追加、除去、または変更を行うことができる。例えば、設定中のある特定の提供されるコンピュータネットワークが既存のリモートクライアントコンピュータネットワークへの拡張である場合、クライアントは１つまたは複数のアドレス範囲（例えば、クラスレスインタードメインルーティング（ＣＩＤＲ）アドレスブロック）または既存のリモートクライアントコンピュータネットワークで使用されるネットワークアドレスのサブセットであるネットワークアドレスの別のグループを指定することができ、指定されたネットワークアドレスは提供されるコンピュータネットワークのコンピューティングノード用に使用されるようになる。かかる設定されたネットワークアドレスは、ある状況では、公衆網１００上のコンピューティングシステムから直接アドレス指定できない仮想またはプライベートのネットワークアドレスであり得（例えば、既存のリモートクライアントコンピュータネットワークおよび対応する提供されるネットワーク拡張が、クライアントコンピュータネットワークおよびその提供されるネットワーク拡張に対して、ネットワークアドレス変換技術および／または仮想ネットワーキング技術を使用する場合など）、他方、別の状況では、設定されたネットワークアドレスの少なくともいくつかは、公衆網１０

０上のコンピューティングシステムから直接アドレス可能な公衆網アドレスであり得る（例えば、インターネットルーティング可能な固定ＩＰアドレスまたは別の変わらないネットワークアドレスなど）。別の実施形態では、ＣＮＳ１０５は、例えば、ＣＮＳ１０５で使用可能なネットワークアドレスに基づいて、提供されるコンピュータネットワークに対応するリモートで既存のコンピュータネットワークで使用される関連したネットワークアドレスであるネットワークアドレス選択に基づいてなど、少なくともいくつかの提供されるコンピュータネットワーク拡張の少なくともいくつかのコンピューティングノードで使用するためのネットワークアドレスを自動的に選択することができる。さらに、例えば、基板ネットワーク上でのオーバーレイネットワークの使用などにより、ＣＮＳ１０５がクライアントに仮想ネットワークを提供する少なくともいくつかの実施形態では、たとえ複数のクライアントが各々の提供されるコンピュータネットワークに対して同一または重複するネットワークアドレスを指定しても、各クライアントはそれらの提供されるコンピュータネットワークで使用する任意のネットワークアドレスを指定することが許可されており、つまり、かかる実施形態では、ＣＮＳ１０５は、各クライアントについて別個にネットワークアドレスを管理するため、第１のクライアントは、その第１のクライアントの提供されるコンピュータネットワーク用のある特定の指定されたネットワークアドレスに関連付けられた第１のコンピューティングノードを持つことができ、他方、異なる第２のクライアントは、その第２のクライアントの提供されるコンピュータネットワーク用の同一の特定の指定されたネットワークアドレスに関連付けられた異なる第２のコンピューティングノードを持つことができる。提供されるコンピュータネットワーク用にネットワークアドレスが設定されるかまたは別の方法で決定されるとすぐに、ＣＮＳ１０５は、例えば、ランダムに、ＤＨＣＰ（動的ホスト設定プロトコル）またはネットワークアドレスを動的に割り当てる他の技術の使用などにより、提供されるコンピュータネットワーク用に選択された各種コンピューティングノードに対してネットワークアドレスを割り当てることができる。また、たとえ公衆網アドレスが特定のコンピュータネットワーク用に使用されていても、ＣＮＳ１０５は、例えば、別の箇所で詳述するとおり、特定のリモート資源サービス用のアクセス機構として動作するために特定の公衆網アドレスを使用するなど、それらの公衆網アドレスの１つまたは複数を別の方法で使用するためにマッピングすることができ、、その特定のコンピュータネットワークのコンピュータノードによってその特定の公衆網アドレスに送信される通信が、インターネットまたはその特定の公衆網アドレスが割り当てられた別のネットワーク上にあるもう１つ別のコンピューティングシステムではなく、対応するリモート資源サービスに転送されるようになる。図１Ｂは、提供されるコンピュータネットワーク内で通信をルーティングするために設定されたネットワークアドレスを使用する詳細な例を示している。

【００２９】

また、少なくともいくつかの実施形態において、クライアントは、モジュール１１０とやりとりして、そのクライアント用に提供されるコンピュータネットワーク用にネットワークトポロジ情報を設定することができ（例えば、ＣＮＳ１０５で提供されるＡＰＩとの１つまたは複数のプログラムによるやりとりを通して）、例えば、提供されるコンピュータネットワークがクライアントによって既に使用されるようになった後に、かかるネットワークトポロジ情報は、少なくともいくつかのかかる実施形態において提供されるコンピュータネットワーク用に後で動的に変更することができる。例えば、クライアントは、特定のタイプのネットワーキング装置（例えば、ルータ、スイッチなど）および／または提供されるコンピュータネットワークの一部となる別のネットワーク装置またはノード（例えば、ファイアウォール、プロキシ、ネットワークストレージ装置、プリンタなど）を特定することができ、かつ／または、グループにまとめられるか、または別の方法で共通の相互通信特性を共有する提供されるコンピュータネットワークのコンピューティングノードのサブセットを特定できる（例えば、相互通信がフィルタリングされていないか、かつ／または特定のネットワーキング装置に関連付けられたサブネットの一部であるコンピューティングノードの特定のサブセットなど）。また、提供されるコンピュータネットワー

ク用に特定された設定情報は、少なくともいくつかの実施形態において、ネットワーク装置および／またはコンピューティング装置グループ間のルーティング情報または別の相互接続情報を含む。さらに、少なくともいくつかの実施形態では、ＣＮＳ１０５は、複数の地理的位置で（例えば、複数の地理的に分散されたデータセンタで）利用可能なコンピューティングノードを提供することができ、提供されるコンピュータネットワーク用にクライアントによって特定される設定情報は、（例えば、提供されるコンピュータネットワークのコンピューティングノードを複数の地理的位置に設置することにより、それらのコンピューティングノード間に耐障害性を提供するために）提供されるコンピュータネットワークのコンピューティングノードが設置される１つまたは複数の地理的位置を追加で指示することができ、かつ／または、そうでない場合、１つまたは複数のかかる地理的位置を選択するためにＣＮＳ１０５で使用される、提供されるコンピュータネットワークのコンピューティングノードを相互運用する方法の優先または要件に関する情報（例えば、コンピューティングノード相互通信のための最小または最大のネットワーク待ち時間または帯域幅、コンピューティングノード間の最小または最大のネットワーク近接性、コンピューティングノード間の最小または最大の地理的近接性、かかる地理的位置全てで利用できない特定の資源または機能へのローカルアクセスを有すること、例えばクライアントのリモートコンピュータネットワークおよび／またはリモート資源サービスなど、別の外部コンピューティングシステムに関連して特定された位置を有すること、など）を提供できる。

【００３０】

別の箇所で詳述するとおり、少なくともいくつかの実施形態において、提供されるコンピュータネットワークのコンピューティングノード間の相互接続および相互通信は、ＣＮＳ１０５の基礎となる基板ネットワークを使用して管理され、そうである場合、設定されたネットワークトポロジ情報の一部または全ては、少なくともいくつかのかかる実施形態において基礎となる基板ネットワークおよびＣＮＳ１０５の対応するモジュールを使用してシミュレートすることができる。例えば、ＣＮＳ１０５で提供されるコンピューティングノードの各々は、その関連付けられたコンピューティングノードとの間での通信を管理するＣＮＳ１０５のノード通信マネージャモジュールと関連付けられ得る。そうである場合、ファイアウォール装置は、コンピューティングノード用の関連した通信マネージャを使用することによってシミュレートされ、１つまたは複数のシミュレートされたファイアウォール装置に合致する方法でコンピューティングノードとの間での通信を許可しないか、または別の方法で処理できる。かかるノード通信マネージャモジュールは、相互通信がコンピューティングノード間でどのように渡されるか、または渡されるか否かを制御すること、およびコンピューティングノードからの情報要求（例えば、ＡＲＰ（アドレス解決プロトコル）要求）に適切な応答情報で応答することにより、ルータおよびサブネットを同様にシミュレートすることができる。ＣＮＳ１０５の１つまたは複数の外部通信マネージャモジュールは、例えば、ファイアウォール装置の同様のシミュレートおよび特定されたネットワークアクセス制限の強化、ならびにリモート資源サービス用の設定されたアクセス機構およびリモートクライアントプライベートコンピュータネットワークへの安全な接続の管理など、ＣＮＳ１０５および外部コンピューティングシステムで提供されるコンピューティングノード間での通信を管理できる。別のタイプのネットワークトポロジ情報も同様にシミュレートすることができ、いくつかの実施形態におけるＣＮＳ１０５の種々のモジュール使用についての詳細は、以降で図２に関する説明および別の箇所で述べる。

【００３１】

さらに、少なくともいくつかの実施形態では、クライアントはモジュール１１０とやりとりして、クライアント用に提供されるコンピュータネットワークのために種々のネットワークアクセス制限情報を設定することができ（例えば、ＣＮＳ１０５で提供されるＡＰＩとの１つまたは複数のプログラムによるやりとりを通して）、かかるネットワークアクセス制限情報は、提供されるコンピュータネットワークがクライアントによって既に使用されるようになった後などに、少なくともいくつかのかかる実施形態において、提供されるコンピュータネットワーク用に後で動的に変更することができる。例えば、クライアン

トは、提供されるコンピュータネットワークのコンピューティングノードの一部または全てが、その提供されるコンピュータネットワークの別のコンピューティングノードおよび／または別の外部コンピューティングシステムとの通信が許可されるか否かおよびどのように許可されるかに関する情報を特定できるが、それは、次のうちの１つ以上に基づいて特定される：通信の方向（入力対出力）、通信のタイプ（例えば、テキスト用にＨＴＴＰ要求を許可するが画像では許可せず、ＦＴＰ要求は許可しないなど、含まれる内容のタイプおよび／または使用する通信プロトコルのタイプに基づいて）、別のコンピューティングシステムの位置（例えば、提供されるコンピュータネットワークの一部か、提供されるコンピュータネットワークに対応するリモートクライアントコンピュータネットワークの一部か、プライベートアクセスまたは別の専用アクセスが確立されているリモート資源サービスの一部か、提供されるコンピュータネットワークおよび任意の対応するリモートクライアントコンピュータネットワークの外部かどうか、など）、他のコンピューティングシステムのタイプなど。また、別の箇所で詳述するとおり、少なくともいくつかの実施形態では、提供されるコンピュータネットワークは、その提供されるコンピュータネットワークの一部またはそうでない場合はそのネットワークにローカルな設定されたアクセス機構などによって、１つまたは複数のリモート資源サービスへのプライベートアクセスまたは別の専用アクセスを提供するように設定できる。ネットワークトポロジ情報および別のルーティング情報と同様の方法で、ＣＮＳ１０５は、提供されるコンピュータネットワーク用のネットワークアクセス制限情報を用いて種々の方法で制限を実行することができる。いくつかの実施形態において提供されるコンピュータネットワーク用通信の管理についての詳細は、以降で図２に関する説明および別の箇所で述べる。

【００３２】

図１Ｂは、ＣＮＳ１０５によってクライアントに対し提供され得るコンピュータネットワーク例１２０ａ（または設定可能ネットワークサービスの別の実施形態）に関する詳細を図示しており、本例中において、提供されるコンピュータネットワーク１２０ａは、図１Ａのリモートプライベートコンピュータネットワーク１３０の１つのような、クライアントのリモートプライベートコンピュータネットワークへのプライベートネットワーク拡張である。本例において、提供されるコンピュータネットワーク１２０ａ用の種々の接続および通信経路は、設定可能ネットワークアクセス制限およびネットワークトポロジのタイプを説明するように概念的な方法で示されており、また、図２には、提供されるコンピュータネットワーク例１２０ａのような、提供されるコンピュータネットワークの作成に使用可能な基礎となる基板ネットワークおよび接続の一例に関する詳細が図示されている。

【００３３】

具体的には、図１Ｂでは、提供されるコンピュータネットワーク１２０ａは、第１の地理的位置１　１６０（例えば、地理的位置１にある第１のデータセンタなど）に配置されたＣＮＳ１０５によって提供される種々のコンピューティングノードを含み、その種々のコンピューティングノードは（例えば、異なるサブネットおよび／または関連した設定されたネットワーキング装置（図示せず）に対応するため）本例では論理グループ１６４、１６５および１６６に設定されている。本例では、それらのコンピューティングノードと別のコンピューティングシステムとの間の通信を制御するために単一の概念的仮想ルータ１６２が地理的位置１に示され、提供されるコンピュータネットワーク１２０ａは、実際には地理的位置１に複数の設定されたネットワーキング装置を持つこともあれば全く持たないこともあるが、生じる可能性のある各種の通信が図示されており、そして、コンピュータネットワーク１２０ａは、例えば、複数の物理的に相互接続されたルータまたは他のネットワーキング装置経由や、基礎となる基板ネットワークおよびその基礎となる基板ネットワークを介した通信を制御する関連したモジュールの使用など、地理的位置１において種々の方法で設定可能ネットワークサービスにより実装される可能性がある。本例では、仮想ルータ１６２は、設定されたネットワークトポロジ情報、リモート資源サービスへの設定されたプライベートアクセスまたは別の専用アクセス、および別の設定されたネッ

トワークアクセス制限情報を含め、提供されるコンピュータネットワーク１２０ａ用の設定された情報に従って動作し、例えば、提供されるコンピュータネットワーク１２０ａ内のネットワークアドレスに送信される通信を、提供されるコンピュータネットワーク１２０ａ上の対応する宛先コンピューティングノードへルーティングしたり、別の通信を、提供されるコンピュータネットワーク１２０ａの外部にある別のネットワークアドレスに適宜ルーティングしたりする。さらに、設定されたファイアウォール装置、設定されたネットワークトポロジ情報、または別の設定されたネットワークアクセス制限によって許可されていない通信は、仮想ルータ１６２によってブロックされるか、または別の方法で管理される。

【００３４】

本例において、コンピュータネットワーク１２０ａは、例のクライアント１用に提供され、クライアント１のリモートコンピュータネットワークへのネットワーク拡張である。クライアント１のリモートコンピュータネットワークは、第１リモート位置のサイトＡ１９０にある複数のコンピューティングシステム（図示せず）を含み、かつ、仮想ルータ１６２は、地理的位置１にある仮想通信リンク１７０を経由してそれら複数のコンピューティングシステムと通信するように設定される。例えば、別の箇所で詳述するとおり、提供されるコンピュータネットワーク１２０ａは、サイトＡ１９０にある複数のコンピューティングシステムへの１つまたは複数の設定されたＶＰＮ接続を含むことができ、通信リンク１７０は、１つまたは複数のかかるＶＰＮ接続に対応することができる。また、クライアント１のリモートコンピューティングネットワークは、図示されているオプションのサイトＢ１９２など、１つまたは複数の別の位置にあるコンピューティングシステムをオプションとして含むことができ、そうである場合、仮想ルータ１６２はさらに、サイトＢ１９２へのオプションの仮想通信リンク１７２経由（例えば、サイトＢに対して直接設定された１つまたは複数の別のＶＰＮ接続を介して）などで、別の位置にあるそれら別のコンピューティングシステムと通信するように設定できる。リモートコンピュータネットワークのリモートコンピューティングシステムに対して複数のＶＰＮ接続または別の安全な接続が使用されている場合、各接続は、（例えば、それらリモートコンピューティングシステムに対応するリモートコンピュータネットワークのネットワークアドレスのサブセットに対応することにより）リモートコンピューティングシステムのサブセットに対応して、通信が適切な接続にルーティングされるようにできる。別の実施形態では、複数のＶＰＮ接続または別の安全な接続は、１つまたは複数の位置にあるリモートコンピューティングシステムに対して使用できるが、複数の接続が冗長な代替手段の場合（例えば、負荷分散のための使用）などは、リモートコンピューティングシステムのいずれかへの通信を各々サポートできる。さらに、いくつかの実施形態では、クライアントのリモートコンピュータネットワークは、複数のサイトで複数のコンピューティングシステムを含むことができるが、リモートコンピューティングシステムへの単一のＶＰＮ接続または他の安全な接続のみが使用される場合があり、リモートコンピュータネットワークが通信の適切なサイトおよびコンピューティングシステムへのルーティングに責任を持つ。

【００３５】

また、提供されるコンピュータネットワーク１２０ａは、インターネット１９６または別の公衆網上で通常アクセス可能な提供されるコンピュータネットワーク１２０ａのコンピューティングノードと別の外部コンピューティングシステムとの間の通信を全部もしくは一部を許可するか、または通信を許可しないように設定することができる。少なくとも一部のかかる外部通信が許可される場合、仮想ルータ１６２は、例えば提供されるコンピュータネットワーク１２０ａ用のオプションの仮想境界ルータ１５５と接続して、提供されるコンピュータネットワーク１２０ａのオプションの仮想通信リンク１７８を経由して、それら外部の複数のコンピューティングシステムと通信するようにさらに設定できる。仮想境界ルータ１５５は、種々の方法で物理的に実装することができるが、例えば、ＣＮＳ１０５が地理的位置１において外部コンピューティングシステムとＣＮＳ１０５によって提供される種々のコンピューティングノードとの間の通信を管理する１つまたは複数の

実際のファイアウォール装置または境界ルータ装置（例えば、ＣＮＳ１０５のそれらのコンピューティングノードを使用するクライアントに対してＣＮＳ１０５によって提供される多数のコンピュータネットワークをサポートする実際の装置）を使用することや、（例えば、許可されていない通信が、提供されるコンピュータネットワーク１２０ａのコンピューティングノードによって基板ネットワークへ送信されるのを防ぐために）基礎となる基板ネットワークおよび基礎となる基板ネットワークを介した通信を制御する関連モジュールを使用することによる。さらに、仮想境界ルータ１５５は、例えば、サイトＡおよびサイトＢにあるリモートクライアントコンピュータネットワーク、１つまたは複数のリモート資源サービスなど、提供されるコンピュータネットワーク１２０ａの外部にある別のコンピューティングシステムへの別の通信を管理するのをさらに概念的に支援する。

【００３６】

さらに、提供されるコンピュータネットワーク１２０ａは、例えば、提供されるコンピュータネットワーク１２０ａの１つまたは複数のネットワークアドレスをそれらの１つまたは複数のリモート資源サービスを表すために割り当てたり、オプションとしてそれらの割当て済みネットワークアドレスに送信された通信に対して実行する特定の動作を設定したりすることにより、１つまたは複数のリモート資源サービスへのプライベートアクセスまたは別の専用アクセスを提供するように設定できる。本例では、仮想ルータ１６２は、提供されるコンピュータネットワーク１２０ａの仮想通信リンク１７４を経由してリモート資源サービス１９４へのローカルアクセスを提供するように設定されている。このため、例えば、提供されるコンピュータネットワーク１２０ａのコンピューティングノードの１つが、通信リンク１７４へマッピングされている提供されるコンピュータネットワーク１２０ａの特定のネットワークアドレスに通信を送信する場合、仮想ルータは、その通信を（例えば、インターネットまたは別の公衆網を経由して）提供されるコンピュータネットワーク１２０の外部にあるリモート資源サービス１９４に転送する。別の実施形態では、リモート資源サービス１９４は、ＣＮＳ１０５の一部であるかそうでない場合は地理的位置１にあるインタフェースを実装することができ、そうである場合、通信リンク１７４にマッピングされている提供されるコンピュータネットワーク１２０ａの特定のネットワークアドレスに送信された通信は、代わりに、処理のためリモート資源サービスのそのインタフェースに転送される。

【００３７】

また、仮想通信リンク１７４は、少なくともいくつかの実施形態において、例えば、リモート資源サービス１９４に転送される前に１つまたは複数の方法でそれらの通信を変更したり、そうでない場合は特定の方法でリモート資源サービス１９４にアクセスしたりするため、そのリンクを経由して送信された通信を種々の方法で管理するように設定することができる。例えば、例示した実施形態では、仮想通信リンク１７４は、リモート資源サービス１９４で提供されるコンピューティング関連資源のサブセットをその名前空間の一部にして、リモート資源サービス１９４内の特定の名前空間に対応するように設定することができる。従って、仮想通信リンク１７４は、例えば、特定の名前空間に関連付けられた名前または別の識別子を使用する通信の変更または変換、特定の名前空間の指示をサポートするリモート資源サービスの特定のインタフェースの使用などにより、特定の名前空間内の資源にアクセスするように設定できる。さらに、仮想通信リンク１７４が特定の名前空間に対応するように、またそうでない場合はリモート資源サービス１９４で提供される資源のサブセットに対応するように設定される場合、提供されるコンピュータネットワーク１２０ａは、同一のリモート資源サービス１９４にも対応するが、リモート資源サービス１９４に別の方法でアクセスするように設定された１つまたは複数の別の仮想通信リンクを含むようにオプションとしてさらに設定できる。例えば、提供されるコンピュータネットワーク１２０ａは、異なる第２の名前空間に対応する、どの特定の名前空間にも対応しない、通信リンク１７４用に使用された顧客識別子と異なるリモート資源サービス１９４の顧客識別子を使用するために、仮想通信リンク１７４とは異なる方法でリモート資源サービス１９４にアクセスするように設定された異なる仮想通信リンク１７６をオプシ

ョンとして含むことができる。本例では、仮想通信リンク１７４および１７６は、異なる識別子（例えば、異なる名前空間識別子）を使用するように設定されており、それらの識別子は、本例中ではリンク１７４および１７６に対してそれぞれＩＤ１およびＩＤ２として表される。このため、提供されるコンピュータネットワーク１２０ａのコンピューティングノードは、リモート資源１９４から異なるタイプの機能にアクセスすることが可能になる。さらに、ここでは図示していないが、提供されるコンピュータネットワーク１２０ａは、それら別のリモート資源サービスへの別の仮想通信リンクを使用して、１つまたは複数の別のリモート資源サービス（図示せず）にアクセスするように同様に設定できる。

【００３８】

リモート資源サービス１９４の特定の名前空間にアクセスするための仮想通信リンク１７４の設定に加えてまたはその代わりに、仮想通信リンクは、少なくともいくつかの実施形態において、リモート資源サービス１９４が通信の位置または別のソースを、提供されるコンピュータネットワーク１２０ａとして確認にするのを可能にするため、リモート資源サービス１９４に追加情報を提供するように設定できる。例えば、例示した実施形態において、仮想通信リンク１７４は、設定可能ネットワークサービスまたはリモート資源サービス１９４によりその提供されるコンピュータネットワーク１２０ａに関連付けられた１つまたは複数の特定の識別子または別のアクセス制御インディケータに対応するように設定されて、リモート資源サービス１９４によるそれらの資源へのアクセスの制限時に使用するため、仮想通信リンク１７４経由でアクセスされるリモート資源サービス１９４によって提供される新規または／および既存のコンピューティング関連リソースのサブセットが、アクセス制御インディケータに関連付けられるようになる。従って、仮想通信リンク１７４は、例えば、追加のインディケータを含むように通信を変更する、通信を変更することなく追加のインディケータを通信と一緒に送信する、かかる追加のインディケータを含むことをサポートするリモート資源サービスの特定のインタフェースを使用するなど、種々の方法で、提供されるコンピュータネットワーク１２０ａに関連付けられた指定済みの追加のインディケータを使用するように設定できる。さらに、仮想通信リンク１７４が１つまたは複数の追加のインディケータに対応するように設定された場合、提供されるコンピュータネットワーク１２０ａはオプションとして、同一のリモート資源サービス１９４にも対応するが別の方法でリモート資源サービス１９４にアクセスするように設定された、１つまたは複数の他の仮想通信リンクを含むようさらに設定できる。例えば、提供されるコンピュータネットワーク１２０ａは、追加のインディケータのいずれも使用することなくリモート資源サービス１９４にアクセスするため（例えば、そうでなければ公的に利用可能になるようなリモート資源サービス１９４への同一アクセスを提供するため）、仮想通信リンク１７４で使用されたものとは異なる１つまたは複数の別の追加のアクセス制御インディケータを使用するため、仮想通信リンク１７４用に使用された顧客識別子とは異なるリモート資源サービス１９４の顧客の識別子を使用するためなど、オプションとして別個の仮想通信リンク１７６を設定することができる。さらに、ここでは図示していないが、提供されるコンピュータネットワーク１２０ａは、同様に、例えば、仮想通信リンク１７４として１つまたは複数の追加のインディケータを使用するように設定されたかまたは別の方法で設定された別の仮想通信リンクなど、それら別のリモート資源サービスへの別の仮想通信リンクを使用する１つまたは複数の別のリモート資源サービス（図示せず）にアクセスするように同様に設定され得る。

【００３９】

例示した実施形態では、地理的位置１にあるＣＮＳ１０５のコンピューティングノードに加えて、提供されるコンピュータネットワーク１２０は、第２の地理的位置２　１８０に配置されているＣＮＳ１０５で提供されるコンピューティングノード１８４（例えば、地理的位置２にある異なる第２のデータセンタなど）をさらに含むことができる。それに応じて、仮想ルータ１６２は、地理的位置２で提供されるコンピュータネットワーク１２０ａの一部へのオプションの仮想通信リンク１６８を含むように設定できる。本例では、地理的位置２にある提供されるコンピュータネットワーク１２０ａの一部は、同様に、仮

想通信リンク１８８を経由した地理的位置１にある提供されるコンピュータネットワーク１２０の一部との通信を含め、コンピューティングノード１８４との間の通信を管理する概念的仮想ルータ１８２を用いて説明される。異なる地理的位置にあるＣＮＳ１０５のコンピューティングノード間のかかる通信は、インターネットまたは別の公衆網を介して（例えば、ＣＮＳ１０５でサポートされる暗号を使用する、安全なトンネルの一部として）通信を送信する、プライベートで安全な方法で（例えば、地理的位置間の専用回線を経由して）通信を送信するなど、種々の実施形態において種々の方法で処理される。さらに、ここでは図示していないが、地理的位置２における提供されるコンピュータネットワーク１２０ａの一部は、同様に、（例えば、地理的位置１へのいかなるＶＰＮ接続とも異なる１つまたは複数のＶＰＮ接続を経由した）リモートクライアントプライベートネットワーク、リモート資源サービス、インターネットなどへの、地理的位置１でその一部が図示されている、同一タイプの他の仮想通信リンクの一部または全てを含むことができる。

【００４０】

図１Ｂの提供されるコンピュータネットワーク１２０ａは、例示を目的として含まれていること、および、クライアント用にＣＮＳ１０５で提供される別のコンピュータネットワークは、あらゆるタイプの設定された通信リンクおよびネットワークトポロジ情報を含んではおらず、かつ／または、ここに示されていない別のタイプの設定された通信リンクおよびネットワークトポロジ情報を含む可能性があることを理解されよう。例えば、いくつかの実施形態および状況では、提供されるコンピュータネットワークは、コンピューティングノードに加えてまたはその代わりに、設定された装置および別の資源を含むことができ、そうである場合、かかる別の資源の各々に、オプションとして、その提供されるコンピュータネットワークのネットワークアドレスを割り当てることができる。さらに、図１Ｂに示されている概念的装置および通信リンクは、各種の基礎となる物理装置、接続およびモジュールを用いて実装することができる。また、ここでは図示していないが、クライアントは、提供されるコンピュータネットワークからか、またはその代わりに別のリモートコンピューティングシステムからかに関わらず、リモート資源サービスとの様々なタイプの別のやりとりを実行することができ、これには、資源使用のための加入／登録、種々の認証情報（例えば、ユーザＩＤ、パスワードなど）の受信／作成、提供されるコンピュータネットワーク（例えば、プライベートな企業ネットワークへのネットワーク拡張など）から後でアクセスされる（例えば、リモートのプライベートな企業ネットワークの一部である）別のリモートコンピューティングシステムからの資源および／または名前空間の作成などがある。

【００４１】

図２は、設定可能ネットワークサービスの一実施形態などによって、コンピュータネットワークの提供に使用するためのコンピューティングシステムの実施形態例を示すネットワーク図である。具体的には、本例では、多数の物理コンピューティングシステムがデータセンタ２００内の同一場所に配置され、かつ種々のネットワーキング装置および１つまたは複数の物理ネットワークを経由して相互接続されている。物理コンピューティングシステムおよび別の装置は、本例では設定可能ネットワークサービスによってクライアントに複数のコンピュータネットワークを提供するために、提供されるコンピュータネットワークの各々を仮想ネットワークとして確立および保守すること、および物理ネットワークを、仮想ネットワークがその上に重ねられている基板ネットワークとして使用することにより、使用される。例えば、図１Ｂの例に関して、データセンタ２００は、地理的位置１に配置することができ、例示された物理コンピューティングシステムは、提供されるコンピュータネットワーク１２０ａのコンピューティングノード１６４、１６５および１６６を提供するために使用できる。オーバーレイネットワークおよび基礎となる基板ネットワークの使用は、少なくともいくつかの実施形態において提供されるコンピュータネットワークのコンピューティングシステムにとって透過的である可能性がある。

【００４２】

このように、本例では、設定可能ネットワークサービスによって提供されるコンピュー

タネットワークが、基礎となる物理基板ネットワークを経由して通信を送信する仮想オーバーレイネットワークとして実装される。提供される仮想オーバーレイネットワークは、種々の実施形態において種々の方法で実装することができ、例えば、いくつかの実施形態では（例えば、仮想ネットワーク用の仮想ネットワーク情報を、物理基板ネットワークのネットワーキングプロトコル用に設定された通信に埋め込むことにより）通信をカプセル化することなく実装できる。説明に役立つ一例として、仮想ネットワークは、３２ビットのＩＰｖ４（インターネットプロトコルバージョン４）ネットワークアドレスを使用して実装され得、そしてそれらの３２ビットの仮想ネットワークアドレスは、その物理基板ネットワークで使用される１２８ビットのＩＰｖ６（インターネットプロトコルバージョン６）ネットワークアドレスの一部として埋め込まれ得る、これは、（例えば、ステートレスＩＰ／ＩＣＭＰトランスレーション（ＳＩＩＴ）を用いて）通信パケットまたは別のデータ通信のヘッダの再設定、または別の方法で、それらのデータ通信が設定された第１のネットワーキングプロトコルから、異なる第２のネットワーキングプロトコルに変換するための、かかるデータ通信の変更などにより行う。説明に役立つもう１つ別の例として、仮想ネットワークおよび基板ネットワークの両方を同一のネットワークアドレス指定プロトコル（例えば、ＩＰｖ４またはＩＰｖ６）を使用して実装することができ、通信は基板ネットワークを介して送信されるのに対し、仮想ネットワークアドレスを使用し、提供される仮想オーバーレイネットワークを経由して送信されたデータ通信は、基板ネットワークに対応する異なる物理ネットワークアドレスを使用するように変更できるが、基板ネットワークを出る時に通信データをその元の形式に復元できるように、元の仮想ネットワークアドレスを変更済みデータ通信に格納しているか、または別の方法で追跡している。別の実施形態では、少なくともいくつかのオーバーレイネットワークは、通信のカプセル化を使用して実装できる。

【００４３】

図２の図示例は、設定可能ネットワークサービスの実施形態で動作する複数の物理コンピューティングシステムを持つデータセンタ２００を含む。データセンタ２００は、データセンタ２００の外部にある１つまたは複数の公衆網２３５に接続されており、その公衆網２３５は、プライベートネットワーク２４０を経由して１つまたは複数のリモートコンピューティングシステム２４５ａ、各々が別の地理的位置に複数のコンピューティングシステムを持つ１つまたは複数のグローバルアクセス可能なデータセンタ２６０、および１つまたは複数の別のリモートコンピューティングシステム２４５ｂへのアクセスを提供する。公衆網２３５は、例えば、ネットワークのうちの公的アクセス可能なネットワークであって、インターネットなど、種々の異なる団体によっておそらく運営されている可能性があり、そして、プライベートネットワーク２４０は、例えば、プライベートネットワーク２４０の外部にあるコンピューティングシステムからは全体または一部がアクセス不能な企業ネットワークである。コンピューティングシステム２４５ｂの各々は、例えば、インターネットと（例えば、電話回線、ケーブルモデム、デジタル加入者回線（ＤＳＬ）などを経由して）直接接続するホームコンピューティングシステムであってもよい。

【００４４】

本例では、仮想の提供されるコンピュータネットワークの設定は、設定可能ネットワークサービスのマネージャモジュール２１０によって容易にされ、そして、設定可能ネットワークサービスの複数の別のモジュールは、例えば、基板ネットワークに出入りする通信を変更することにより物理基板ネットワークの端から、提供されるコンピュータネットワークの機能を実装するために使用される。具体的には、本例では、設定可能ネットワークサービスの複数のノード通信マネージャモジュールの各々は、例えば、以降でさらに詳述するように、図示したノード通信マネージャモジュール２０９ａ、２０９ｄ、および２５０など、関連付けられたコンピューティングノードとの間の通信を管理する。さらに、本例では、設定可能ネットワークサービスの外部通信マネージャモジュール２７０は、以降でさらに詳述するように、データセンタ２００内の物理コンピューティングシステムと外部コンピューティングシステムとの間の通信を管理する。本例では、単一の外部通信マネ

ージャモジュール２７０のみが図示されているが、モジュール２７０の機能は、冗長性および負荷分散などのために、複数の装置を使用して実装できることを理解されよう。

【００４５】

データセンタ２００は、多数の物理コンピューティングシステム２０５ａ～２０５ｄおよび２５５ａ～２５５ｎのほかに、関連したコンピューティングシステム２５５ａ～２５５ｎのために通信を管理する１つまたは複数の別のコンピューティングシステム（図示せず）上で実行するＣＮＳノード通信マネージャモジュール２５０、および１つまたは複数のコンピューティングシステム（図示せず）上で実行する設定可能ネットワークサービスのマネージャモジュール２１０を含む。本実施形態例において、物理コンピューティングシステム２０５ａ～２０５ｄの各々は、複数の仮想マシンコンピューティングノードをホストし、かつ、コンピューティングシステム２０５ａ上のＣＮＳ　ＶＭノード通信マネージャモジュール２０９ａおよび仮想マシン２０７ａ、ならびにコンピューティングシステム２０５ｄ上のＣＮＳ　ＶＭノード通信マネージャモジュール２０９ｄおよび仮想マシン２０７ｄなど、仮想マシン（ＶＭ）ノード通信マネージャモジュールも（例えば、物理コンピューティングシステム用の仮想マシンハイパーバイザモニタの一部として）含む。仮想マシンコンピューティングノードの各々は、設定可能ネットワークサービスによって、クライアントに提供されるコンピュータネットワークの異なるコンピューティングノードとして使用できる。物理コンピューティングシステム２５５ａ～２５５ｎは、本例ではいかなる仮想マシンも実行しないため、設定可能ネットワークサービスでクライアントに提供されるコンピュータネットワークの一部である異なるコンピューティングノードとして、各々動作することができる。別の実施形態では、データセンタにある物理コンピューティングシステムの全部が仮想マシンをホストするか、いずれもホストしない可能性がある。

【００４６】

本データセンタ例は、スイッチ２１５ａおよび２１５ｂ、エッジルータ２２５ａ～２５５ｃ、ならびにコアルータ２３０ａ～２３０ｃなど、複数の物理ネットワーキング装置をさらに含む。スイッチ２１５ａは、物理コンピューティングシステム２０５ａ～２０５ｃを含む物理ネットワークの一部であって、かつ、エッジルータ２２５ａに接続されている。スイッチ２１５ｂは、物理コンピューティングシステム２０５ｄ、２５５ａ～２５５ｎ、およびＣＮＳノード通信マネージャモジュール２５０およびＣＮＳシステムマネージャモジュール２１０を提供するコンピューティングシステムを含む異なる物理ネットワークの一部であって、かつ、エッジルータ２５５ｂに接続されている。スイッチ２１５ａ～２１５ｂで確立された物理ネットワークは、中間にある相互接続ネットワーク２２０を経由して相互に別のネットワーク（例えば、公衆網２３５）と交互に接続され、その相互接続ネットワーク２２０は、エッジルータ２２５ａ～２５５ｃおよびコアルータ２３０ａ～２３０ｃを含む。エッジルータ２２５ａ～２５５ｃは、２つ以上のネットワーク間のゲートウェイを提供する。例えば、エッジルータ２２５ａは、スイッチ２１５ａで確立された物理ネットワークと相互接続ネットワーク２２０との間のゲートウェイを提供する。エッジルータ２２５ｃは、相互接続ネットワーク２２０と公衆網２３５との間のゲートウェイを提供する。コアルータ２３０ａ～２３０ｃは、かかるデータ送信の特性（例えば、ソースおよび／または宛先の基板ネットワークアドレス、プロトコル識別子、など）および／または相互接続ネットワーク２２０自体の特性（例えば、物理ネットワークトポロジに基づく経路など）に基づき適宜パケットまたは他のデータ通信を転送することなどにより、相互接続ネットワーク２２０内での通信を管理する。

【００４７】

図示されたノード通信マネージャモジュールは、関連したコンピューティングノードとの間で送信された通信を管理する。例えば、ノード通信マネージャモジュール２０９ａは、関連した仮想マシンコンピューティングノード２０７ａを管理し、ノード通信マネージャモジュール２０９ｄは、関連した仮想マシンコンピューティングノード２０７ｄを管理し、そして、別のノード通信マネージャモジュールの各々は、同様に１グループの１つま

たは複数の別の関連したコンピューティングノードのために通信を管理する。図示されたノード通信マネージャモジュールは、コンピューティングノード間の通信を管理して、特定の仮想ネットワークが中間にある物理基板ネットワーク（例えば、相互接続ネットワーク２２０ならびにスイッチ２１５ａおよび２１５ｂに関連付けられた物理ネットワーク）の上に重なるようにすることができ、そして、かかる通信を管理するためにファイアウォールポリシおよび別のネットワークアクセス制限を実装できる。外部通信マネージャモジュール２７０は、例えば、かかる外部通信に関して、データセンタ２００内の基板ネットワーク上にオーバーレイネットワークをさらに実装するため、データセンタ２００に出入りする外部通信を管理する。外部通信マネージャモジュール２７０は、データセンタ２００の外部にあるリモート資源サービスへのプライベートアクセスまたは別の専用アクセスを許可する提供されるコンピュータネットワーク用の少なくともいくつかの設定されたアクセス機構、およびオプションとして外部リモートクライアントコンピュータネットワークへの少なくともいくつかのＶＰＮ接続を含め、ファイアウォールポリシおよび別のネットワークアクセス制限を実装するための処置をとることができるか、または代わりに、かかるＶＰＮ接続の設定可能ネットワークサービスの部分を実装する別のハードウェアおよび／またはソフトウェア（図示せず）と連携して動作することができる。

【００４８】

従って、説明に役立つ一例として、コンピューティングシステム２０５ａ上の１つの仮想マシンコンピューティングノード２０７ａは、ＩＰｖ４を仮想ネットワーク用の仮想ネットワークアドレスを表すために使用して、コンピューティングシステム２０５ｄ上の１つの仮想マシンコンピューティングノード２０７ｄ、およびコンピューティングシステム２５５ａ（およびオプションとして、このデータセンタ内または設定可能ネットワークサービスでも使用される１つまたは複数の別のデータセンタ２６０内の別のコンピューティングノード）とともに、クライアント用の特定の提供される仮想コンピュータネットワーク（例えば、図１Ｂの提供されるコンピュータネットワーク１２０ａ）の一部であってもよい。別の仮想マシンコンピューティングノード２０７ａ、仮想マシンコンピューティングノード２０７ｄ、およびコンピューティングシステム２５５ｄ～２５５ｎは（図示された別のコンピューティングノードと同様に）、現在、別のクライアントに提供中の別のコンピュータネットワークに割り当てられているか、現在は提供されるコンピュータネットワークに割り当てられておらずその設定可能ネットワークサービスで使用不能であるか、かつ／または同一の特定の提供される仮想コンピュータネットワークの一部でもある可能性がある。特定の提供される仮想コンピュータネットワークの一部である仮想マシンコンピューティングノード２０７ａ上でクライアント用に実行されているプログラムは、次に、出力通信（図示せず）を特定の提供される仮想コンピュータネットワークの仮想マシンコンピューティングノード２０７ｄへ向けることができるが、これは、その宛先仮想マシンコンピューティングノード２０７ｄに割り当てられたその提供される仮想コンピューティングネットワーク用の仮想ネットワークアドレスを指定することなどによって行う。ノード通信マネージャモジュール２０９ａは、その出力通信を受信し、そして、少なくともいくつかの実施形態では、送信仮想マシンコンピューティングノード２０７ｄおよび／または宛先仮想マシンコンピューティングノード２０７ｄに関する事前の設定された情報などに基づき、および／またはシステムマネージャモジュール２１０と（例えば、許可決定の取得、かかる情報の一部または全ての取得などのため）動的にやりとりすることにより、その出力通信の送信を許可するかどうかを決定する。

【００４９】

ノード通信マネージャモジュール２０９ａが、出力通信が許可されることを決定する（または、かかる許可決定を実行しない）場合、モジュール２０９ａは、その通信用の宛先仮想ネットワークアドレスに対応する実際の物理基板ネットワーク位置を決定する。本例では、相互接続ネットワークは、相互接続ネットワークを経由して接続されたコンピューティングノード用の実際のネットワークアドレスを表すためにＩＰｖ６を使用し、モジュール２０９ａは、出力通信のヘッダを再設定し、実際のＩＰｖ６の基板ネットワークアド

レスを使用してその出力通信がノード通信マネージャモジュール２０９ｄに向けられるようにする。ノード通信マネージャモジュール２０９ａは、例えば、システムマネージャモジュール２１０と動的にやりとりすることにより、宛先仮想コンピューティングノード２０７ｄの仮想ネットワークアドレス用に使用する実際のＩＰｖ６宛先ネットワークアドレスを決定できるか、または（例えば、アドレス解決プロトコル（ＡＲＰ）を使用した要求など、送信仮想マシンコンピューティングノード２０７ａからのその宛先仮想ネットワークアドレスに関する情報の事前の要求に応じて）その情報を事前に決定および保存しておくことができる。本例では、使用された実際のＩＰｖ６宛先ネットワークアドレスが仮想宛先ネットワークアドレスおよび追加情報を埋め込んで、カプセル化することなくオーバーレイネットワークを介して通信を送信できるようにする。

【００５０】

ノード通信マネージャモジュール２０９ｄは、相互接続ネットワーク２２０を経由して通信を受信する場合、実際のＩＰｖ６宛先ネットワークアドレスから仮想宛先ネットワークアドレスおよび追加情報を抽出して、どの仮想マシンコンピューティングノード２０７ｄにその通信が向けられているかを決定する。ノード通信マネージャモジュール２０９ｄは次に、オプションとして、通信が宛先仮想マシンコンピューティングノード２０７ｄに対して許可されているかどうかを決定するが、これは、例えば、実際のＩＰｖ６ソースネットワークアドレスから仮想ソースネットワークアドレスおよび追加情報を抽出すること、およびその仮想ソースネットワークアドレスを持つコンピューティングノードが、通信を転送したノード通信マネージャモジュールで実際に管理されていることを確認して、悪意のある送信者がソースネットワークアドレスになりすますのを防ぐことなどにより、行う。通信が許可される（または、ノード通信マネージャモジュール２０９ｄがかかる許可決定を実行しない）ことが決定している場合、そのモジュール２０９ｄはその後、例えば、送信仮想マシンコンピューティングノードの仮想ネットワークアドレスをソースネットワークアドレスとして使用し、宛先仮想マシンコンピューティングノードの仮想ネットワークアドレスを宛先ネットワークアドレスとして使用することなどにより、入力通信のヘッダを再設定し、仮想ネットワーク用の適切なＩＰｖ４ネットワークアドレスを使用して、その入力通信が宛先仮想マシンコンピューティングノード２０７ｄに向けられるようにする。入力通信のヘッダを再設定した後、モジュール２０９ｄは、次にその変更済み通信を宛先仮想マシンコンピューティングノードに転送する。少なくともいくつかの実施形態では、入力通信を宛先仮想マシンに転送する前に、モジュール２０９ｄは、安全に関する追加の手順を実行することもできる。例えば、モジュール２０９ｄは、（例えば、同一仮想ネットワークに属していること、および／またはその提供される仮想ネットワーク用に指定されたネットワークアクセス制限情報、同一顧客または別の団体に関連付けられていること、コンピューティングノードが相互通信を許可されている異なる団体に関連付けられていること、などに基づいて）送信仮想マシンコンピューティングノードが宛先仮想マシンと通信するのを許可されること、および／または、モジュール２０９ｄによって事前に取得された情報またはシステムマネージャモジュール２１０とのやりとりなどに基づいて、入力通信が許可されているタイプであることを確認できる。

【００５１】

送信仮想マシンコンピューティングノード２０７ａが代わりに（または追加で）、出力通信（図示せず）を、データセンタ２００の外部にある１つまたは複数の対象とする宛先コンピューティングシステムに向ける場合、通信マネージャモジュール２０９ａは、同様の方法でその出力通信を受信および処理する。対象とする外部の宛先コンピューティングシステムは、例えば、同一の特定の提供される仮想コンピュータネットワークの一部であるもう１つ別のコンピューティングノード（例えば、特定の提供されるコンピュータネットワークがその拡張であるリモート仮想クライアントコンピュータネットワーク上、または設定可能ネットワークサービスによって特定の仮想コンピュータネットワークの部分を提供するためにも使用されたもう１つ別のデータセンタ２６０においてなど）、リモート資源サービスのコンピューティングシステム、インターネット上で公的アクセス可能なコ

ンピューティングシステムなどでもよい。少なくともいくつかの実施形態および状況では、モジュール２０９ａは、出力通信の送信を許可するかどうかを最初に決定することができ、決定する場合、その通信用の宛先ネットワークアドレスに対応する実際の物理基板ネットワーク位置を決定する。本例では、決定された物理基板ネットワーク位置は、例えば、モジュール２７０が、別の方法ではノード通信マネージャモジュールに割り当てられていない全ての仮想および／または実際のネットワークアドレスに関連付けられている場合、外部通信マネージャモジュール２７０に対応する。モジュール２７０は、相互接続ネットワーク２２０を経由して通信を受信する場合、受信した通信から宛先ネットワークアドレスおよび追加情報を同様に抽出し、オプションとして、対象とする宛先に対して通信が許可されているか否かの決定を含め、その通信を転送するか否かおよびその方法を決定する。通信が許可されること（または、モジュール２７０がかかる許可決定を実行しないこと）が決定された場合、モジュール２７０は、次に入力通信のヘッダを再設定し、適切なＩＰｖ４の公衆網アドレス（または、公衆網２３５に適した別のネットワークアドレス）を使用してその通信が宛先に向けられるようにし、その後その変更済み通信を公衆網経由で転送する。

【００５２】

前述したとおり、こうして外部通信マネージャモジュール２７０は、例示した実施形態において、リモート資源サービス用の設定されたアクセス機構を経由してそれらリモート資源サービスに送信された出力通信を含め、提供されるコンピュータネットワークからの出力通信を処理する。出力通信が、特定の提供されるコンピュータネットワーク用の設定されたアクセス機構を経由してリモート資源サービスに送信されている場合、モジュール２７０および／または送信コンピューティングノードの関連するノード通信マネージャモジュールは、少なくともいくつかの実施形態および状況において追加の処置をとる。例えば、特定の提供される仮想コンピュータネットワークは、リモート資源サービスの特定の名前空間にマッピングされている特定のリモート資源サービス（例えば、１つまたは複数のコンピューティングシステム２４５ｂまたはもう１つ別のデータセンタ２６０にある１つまたは複数のコンピューティングシステムを経由して提供されるリモート資源サービスなど）用の設定されたアクセス機構を有することができ、そして、送信仮想マシンコンピューティングノード２０７ａは、その設定されたアクセス機構を経由して通信を送信できる。特定の提供されるコンピュータネットワーク用のそのリモート資源サービスに対する設定されたアクセス機構は、例えば、その設定されたアクセス機構を表すために割り当てられた特定の提供されるコンピュータネットワークの仮想ネットワークアドレスである可能性があり、そうである場合、その割り当てられた仮想ネットワークアドレスはモジュール２７０に関連付けられて、出力通信がモジュール２７０に向けられるようにすることができる。かかる出力通信を公衆網２３５経由でリモート資源サービスに転送する前に、モジュール２７０は使用されたアクセス機構用の設定を反映させるために、例えば、アクセス機構が対応する特定の名前空間を参照または別の方法で使用する出力通信の変更など、種々の処置をとる。かかる状況では、モジュール２７０は、アクセス機構のための名前空間および他の設定情報を、例えば、設定情報をローカルに保存する、システムマネージャモジュール２７０と連絡をとって設定情報を取得するなど、種々の方法で決定することができる。さらに、モジュール２７０は、特定の名前空間を種々の方法で使用するように通信を変更する方法および時を決定できるが、これは、事前に提供される設定可能ネットワークサービスに対応する設定情報（例えば、名前空間を示す１つまたは複数の特定のメッセージパラメータの指示、資源の指定または参照に使用される１つまたは複数の特定のメッセージパラメータの指示（オプションとして名前空間識別子を含む）、名前空間が示されるのを許可するかまたは別の方法で名前空間情報を使用するメッセージのタイプの指示、など）を有するリモート資源サービスなどによって行うことができる。

【００５３】

説明に役立つ特定の一例として、リモート資源サービスは、データストレージサービスを提供することができ、そして、出力通信は、（例えば、保存されたオブジェクトまたは

保存されたデータの別のグループを検索するため）特定のストレージ関連資源へのアクセス要求の可能性がある。そうである場合、特定のストレージ資源は、提供されるコンピュータネットワークの外部にあるコンピューティングシステム（例えば、クライアントのリモートプライベートコンピュータネットワーク上）の使用などにより、クライアントによって定義された名前空間の一部としてクライアントにより事前に作成されていた可能性がある。その同一の名前空間を使用するために特定の提供されるコンピュータネットワーク用のアクセス機構を設定することにより、提供されるコンピュータネットワークのコンピューティングノードは、クライアントの既存の保存された資源のアクセスおよび使用が可能になる。説明に役立つ一例として、クライアントのリモートプライベートコンピュータネットワークが企業ネットワークである場合、そのクライアントは異なるタイプのデータを保存するために異なる名前空間を使用することができ、例えば、デリケートな人事データを第１の名前空間に保存し、機密のソフトウェア開発ソフトウェアおよび他のデータを第２の名前空間に保存し、企業全体で一般に利用可能な他の企業データを第３の名前空間で保存する。設定可能ネットワークサービスの提供されるコンピュータネットワークは、その企業の特定のサブセット（例えば、人事部員）によってのみ使用される場合、特定の提供されるコンピュータネットワーク用のリモート資源サービスへのアクセス機構は、デリケートな人事データ用の第１の名前空間を使用するように設定できる。さらに、特定の提供されるコンピュータネットワークは、オプションとして、例えば、一般に利用可能な企業データ用の第３の名前空間を使用して、リモート資源サービスに対して設定された第２のアクセス機構を持つ（例えば、提供されるコンピュータネットワークの異なる割当て済み仮想ネットワークアドレスを使用して）ことができ、特定の提供されるコンピュータネットワークのコンピューティングノードが、異なるグループの資源にアクセスするため、特定の提供されるコンピュータネットワークの異なるローカル仮想ネットワークアドレスとやりとりできるようになる。

【００５４】

説明に役立つもう１つの例として、特定のコンピュータネットワーク用のリモート資源サービスへのアクセス機構は、代わりに、特定の提供されるコンピュータネットワークのコンピューティングノードのみが、それらのコンピューティングノードによって作成および使用されるストレージ資源へのアクセスを許可されるように設定できる。そうである場合、設定可能ネットワークサービスは、新規の名前空間を自動生成する（例えば、その情報を特定の提供されるコンピュータネットワークのコンピューティングノードに提供することなく）か、または、クライアントにより設定情報で指示される新規の名前空間を使用することにより、その特定の提供されるコンピュータネットワークで使用する新規の名前空間を決定することができ、そして、その新規の名前空間を使用するようにアクセス機構を設定できる。設定可能ネットワークサービスまたは特定の提供されるコンピュータネットワークのコンピューティングノードは、リモート資源サービス内に新規の名前空間を作成するため、リモート資源サービスに応じて、さらに初期の処置をとる必要がある。一旦新規の名前空間が利用可能になると、特定の提供されるコンピュータネットワークのコンピューティングノードは、リモート資源サービスとやりとりするために設定されたアクセス機構を同様に使用して、新規の名前空間の一部である新規の保存された資源の作成およびかかる保存された資源へのアクセスを行うことができ、そして、外部通信マネージャモジュール２７０は、同様にその新規の名前空間を使用するように出力通信を適宜変更するであろう。

【００５５】

特定のリモート資源サービス内の特定の名前空間に対応する設定されたアクセス機構を実装するために設定されていることに加えてまたはその代わりに、外部通信マネージャモジュール２７０は、いくつかの実施形態において、そのアクセス機構経由でそのリモート資源サービスに送信された一部または全ての通信に対するアクセス制御に関連した１つまたは複数の追加のインディケータを含むように設定でき、そして、送信仮想マシンコンピューティングノード２７０ａはかかる通信をその設定されたアクセス機構経由で送信でき

る。かかる出力通信を公衆網２３５経由でリモート資源サービスに転送する前に、モジュール２７０は、使用されたアクセス機構用の設定を反映するために種々の処置をとることができ、例えば、リモート資源サービスに固有の方法で通信のヘッダおよび／または本体を変更することにより、アクセス機構が対応する１つまたは複数の追加のインディケータを含むように（例えば、リモート資源サービスが１つまたは複数のアクセス制御インディケータのクライアント指定を許可する場合、送信仮想マシンコンピューティングノード２０７ａで指定された任意のインディケータの代わりまたは追加かを問わず、そのリモート資源サービスでサポートされる方法で１つまたは複数の追加のインディケータを含める）出力通信を変更することができる。かかる状況において、モジュール２７０は、情報をローカルに保存する、情報取得のためにシステムマネージャモジュールに連絡する、など、種々の方法でアクセス機構用の追加のインディケータを決定できる。また、モジュール２７０は、特定の追加のインディケータを種々の方法で使用するために通信を変更する方法と時を決定することができるが、これは、事前に提供される設定可能ネットワークサービスに対応する設定情報（例えば、かかるアクセス制御インディケータを示す１つまたは複数の特定のメッセージパラメータの指示、資源のアクセスに使用された１つまたは複数の特定のメッセージパラメータの指示（オプションとして１つまたは複数のかかるアクセス制御インディケータを含む）、１つまたは複数のかかるアクセス制御インディケータが指定できるかまたは別の方法でかかるアクセス制御インディケータを使用できるようにするメッセージのタイプの指示など）を有するリモート資源サービスなどによって行うことができる。

【００５６】

設定されたアクセス機構による名前空間使用に関して前に説明した例と同様の方法で、リモート資源サービスは、データストレージサービスを提供することができ、そして、出力通信は、（例えば、保存されたオブジェクトまたは保存されたデータの別のグループを検索するため）特定のストレージ関連資源へのアクセス要求の可能性がある。そうである場合、特定のストレージ資源は、送信仮想マシンコンピューティングノード２０７ａが属する提供されるコンピュータネットワークの１つのコンピューティングノードで事前に作成されているか、または現在の通信の一部として新規に作成またはアクセスされている可能性がある。いくつかの実施形態では、設定可能ネットワークサービスは、１つまたは複数の追加のインディケータをリモート資源サービス内での使用のために（例えば、それらを定義するために）指定するには、リモート資源サービスに応じて、さらに初期の処置をとる必要がある。別の箇所で詳述するとおり、送信仮想マシンコンピューティングノード２０７ａおよび関連するクライアントは、追加のインディケータの使用を認識していない可能性があるが、外部通信マネージャモジュール２７０は、それにもかかわらず関連したインディケータを使用するために出力通信を適宜変更するだろう。

【００５７】

さらに、前述したとおり、外部通信マネージャモジュール２７０は、例示した実施形態において、例えば、設定されたＶＰＮ接続経由で特定のリモートコンピュータネットワークに送信された出力通信など、提供されるコンピュータネットワークから、拡張が対応するリモートコンピュータネットワークへの出力通信を処理する。少なくともいくつかの実施形態では、設定可能ネットワークサービスは、クライアントが、データセンタ２００にリモートな位置から、データセンタ２００にあるクライアント用に提供されるコンピュータネットワークへのかかるＶＰＮ接続の確立をプログラムで開始できるようにするリモートアクセス確立ＡＰＩを提供し、例えば、クライアントがＶＰＮ接続の確立に使用するため、適切なハードウェア装置、ソフトウェアおよび／または設定情報がリモート位置に配達されるようにする。例えば、コンピューティングシステム２４５ｄの１つは、かかるハードウェア装置および／またはソフトウェアを販売または別の方法で提供するオンライン小売業者に連絡することができ、そうである場合、設定可能ネットワークサービスは、その小売業者によって提供される別個のＡＰＩを使用して、かかるハードウェア装置および／またはソフトウェアをクライアントに応じたリモート位置または別の指定位置へ配達す

る発注を（例えば、設定可能ネットワークサービスの提供されるＡＰＩ起動の一部としてクライアントによる指定、クライアント用の設定可能ネットワークサービスによって予め保存された情報、そのクライアント用に小売業者によって事前に保存された情報、などに基づいて）行うことができる。一旦かかるＶＰＮ接続または別の安全な接続が確立されて、クライアントが提供されるコンピュータネットワークにリモートアクセスできるようになると、モジュール２７０は、例えば、その安全な接続を使用して、その安全な接続が対応するリモート位置にある１つまたは複数の宛先コンピューティングシステム向けの出力通信を送信するなど、安全な接続をサポートするためにさらに処置をとることができる。

【００５８】

このように、図２に関して前述したとおり、少なくともいくつかの実施形態では、設定可能ネットワークサービスは、例えば、設定可能ネットワークサービスの種々のノード通信マネージャおよび設定可能ネットワークサービスの１つまたは複数の外部通信マネージャモジュールの使用など、基礎となる基板ネットワークを使用して、仮想コンピュータネットワークをオーバーレイネットワークとして実装することにより、クライアントに提供する。少なくともいくつかの実施形態では、１つまたは複数のシステムマネージャモジュールは、例えば、どのコンピューティングノードがどの提供される仮想ネットワークに属するかの追跡および／または管理、ならびに（例えば、特定の顧客または他の団体によって）特定の仮想ネットワーク用に使用されている仮想ネットワークアドレスに対応する実際の物理基板ネットワークアドレスに関する情報の提供などにより、コンピューティングノード間の通信の設定をさらに容易にすることができる。また、システムマネージャモジュールは、対象となる物理コンピューティングシステム上の仮想マシンコンピューティングノードおよび仮想マシンが関連付けられる提供される仮想ネットワークの指示を受信でき、その後、仮想マシンを仮想ネットワークに関連付けるために、対象とする物理コンピューティングシステム用の仮想マシンノード通信マネージャモジュールの設定を開始するか、または、（例えば、仮想マシンが最初に通信を開始または受信する時に）ノード通信マネージャモジュールが代わりにその設定を開始できる。

【００５９】

少なくともいくつかの実施形態において、許可されていない通信の検出および／または防止は、前述したとおり、少なくともいくつかは仮想ネットワークがその上に重ねられている１つまたは複数の中間基板ネットワークのトポロジに基づく。かかる実施形態では、基板ネットワークを介した通信用のかかるコンピューティングノード用に使用された物理ネットワークアドレスは、コンピューティングノードの仮想ネットワークアドレスの指示を含み、かつ、コンピューティングノードの関連したノード通信マネージャモジュール位置に対応する基板ネットワーク用の部分ネットワークアドレス（例えば、ノード通信マネージャモジュールが通信を管理する基板ネットワークのサブネットワークまたは別の部分）を含む。従って、悪意のあるユーザが、仮想ネットワークの一部であるコンピューティングノード用に有効な物理ネットワークアドレスを正しく設定するためには、その悪意のあるユーザは、コンピューティングノードが属する仮想ネットワークに関する情報にアクセスし、関連するノード通信マネージャモジュール用の部分ネットワークアドレスを決定するためにコンピューティングノードの物理基板ネットワーク位置のトポロジに関する情報にアクセスし、そして、物理ネットワークアドレスを設定するためにその情報を使用する方法を決定する必要があるだろう。設定された物理ネットワークアドレスの妥当性は、例えば、設定された物理ネットワークアドレスに埋め込まれた仮想アドレスが対応するコンピューティングノードを識別し、その識別されたコンピューティングノード位置が、部分ネットワークアドレスに対応する基板ネットワークの部分にあるコンピューティングノードの１つ（例えば、部分ネットワークアドレスが対応するノード通信マネージャモジュールによって管理されるコンピューティングノードの１つ）に対応することを確認するなど、種々の方法で確認できる。また、設定された物理ネットワークアドレスの妥当性は、（例えば、ソース物理ネットワークアドレスが有効であることを確認するため）宛先コンピューティングノード向けの入力通信を受信するノード通信マネージャモジュール、指示

された管理対象ノードの代わりにノード通信マネージャモジュールからとされるメッセージ（例えば、関心の対象とする宛先コンピューティングノード用の物理ネットワークアドレスを要求するメッセージ）を受信するマネージャモジュールなどによって、何度も確認される可能性がある。

【００６０】

図４、図５、および図６は、それぞれ、少なくともいくつかの実施形態におけるシステムマネージャモジュール２１０、ノード通信マネージャモジュール、および外部通信マネージャモジュール２７０の動作に関する詳細を示している。また、少なくともいくつかの実施形態で使用できるオーバーレイネットワークの実装に関する詳細については、２００８年3月３１日に出願された「Ｃｏｎｆｉｇｕｒｉｎｇ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｂｅｔｗｅｅｎ　Ｃｏｍｐｕｔｉｎｇ　Ｎｏｄｅｓ」という名称の米国特許出願番号第１２／０６０，０７４号（代理人整理番号１２０１３７．５７６）に含まれており、その全体の参照により本明細書に組み込まれる。

【００６１】

図３は、リモートクライアント用のコンピュータネットワークを提供するためのシステムの一実施形態の実行に適したコンピューティングシステム例を示すブロック図である。具体的には、図３は、設定可能ネットワークサービスの提供を支援する設定可能ネットワークサービスシステムマネージャモジュールの一実施形態の実行に適したサーバコンピューティングシステム３００と共に、種々のクライアントコンピューティングシステム３５０、ホストコンピューティングシステム３６０、および別のコンピューティングシステム３８０を示す。ここに示されていないが、いくつかの実施形態では、図示されたコンピューティングシステムの少なくともいくつか（例えば、サーバコンピューティングシステム３００および設定可能ネットワークサービスの一部であるホストコンピューティングシステム３６０の少なくともいくつか）は、図１Ｂおよび図２に関して詳述しているように、例えば、データセンタなど、同一場所に配置されているか、またはそうでない場合は関連付けられている。さらに、ここには示されていないが、例えば、種々のノード通信マネージャモジュールおよび１つまたは複数の外部通信マネージャモジュールなど、設定可能ネットワークサービスの種々の他のモジュールは、少なくともいくつかの実施形態では存在し使用されている可能性がある。

【００６２】

例示した実施形態において、サーバコンピューティングシステム３００は、ＣＰＵ３０５、各種入出力コンポーネント３１０、ストレージ３２０、およびメモリ３３０を含む設定要素を有する。図示した入出力コンポーネントは、ディスプレイ３１１、ネットワーク接続３１２、コンピュータ可読媒体ドライブ３１３、および別の入出力装置３１５（例えば、キーボード、マウス、スピーカなど）を含む。さらに、図示したクライアントコンピューティングシステム３５０は、ＣＰＵ３５１、入出力コンポーネント３５２、ストレージ３５４、およびメモリ３５７を含め、サーバコンピューティングシステム３００と同様の設定要素を持つ。別のコンピューティングシステム３６０および３８０の各々は、サーバコンピューティングシステム３００に関して図示された設定要素の一部または全てと同様の設定要素を含むが、かかる設定要素は、簡潔さのために本例では図示されていない。

【００６３】

設定可能ネットワークサービス（ＣＮＳ）マネージャモジュール３４０の一実施形態は、メモリ３３０内で実行し、コンピューティングシステム３５０、３６０、および３８０と１つまたは複数のネットワーク３９０（例えば、インターネットおよび／またはワールドワイドウェブ、プライベートセルラーネットワーク、設定可能ネットワークサービスで使用中のプライベート基板ネットワークなど）を経由してやりとりする。本実施形態例では、モジュール３４０は、設定可能ネットワークサービスの一部として種々のクライアント（図示せず）による使用のためのコンピュータネットワークの提供および管理に関連する機能を含み、クライアントはコンピュータシステム３５０を使用して、提供されるコンピュータネットワークの設定およびアクセスを行う。ホストコンピューティングシステム

３６０はまた、例えば、設定可能ネットワークサービスで提供されるコンピュータネットワーク用のコンピューティングノードの提供などにより、設定可能ネットワークサービスの提供を支援することができる。同様に、少なくともいくつかの実施形態では、別のコンピューティングシステムの少なくともいくつかもまた、設定可能ネットワークサービスの提供を支援することができ、例えば、提供されるコンピュータネットワークと外部リモートコンピューティングシステムとの間の相互通信を（例えば、ＶＰＮ接続または別のアクセス機構の実装などで）容易にすること、提供されるコンピュータネットワークがアクセスするように設定されたリモート資源サービスを提供すること、提供されるコンピュータネットワークのコンピューティングノード間の相互通信を（例えば、基板ネットワークの部分または通信を容易にする設定可能ネットワークサービスの他のインフラストラクチャの実装などで）容易にすること、などができる。

【００６４】

別のコンピューティングシステム３５０、３６０、および３８０は、モジュール３４０とのやりとりの一部として種々のソフトウェアを実行している可能性がある。例えば、クライアントコンピューティングシステム３５０の一部または全ての各々は、例えば、クライアントコンピューティングシステムのユーザが、設定可能ネットワークサービスのそのユーザまたは別のクライアントによる使用のために設定可能コンピュータネットワークの作成および設定を可能にするためなど、モジュール３４０とやりとりするために（例えば、ウェブブラウザまたは専用のクライアント側アプリケーションプログラムの一部として）メモリ３５７内でソフトウェアを実行している可能性がある。さらに、クライアントコンピューティングシステム３５０および／または別のコンピューティングシステム３８０の一部または全ての各々は、例えば、クライアント用のリモートネットワークの一部である複数のクライアントコンピューティングシステム３５０および／または別のコンピューティングシステム３８０を、クライアントのリモートネットワーク用に提供されるコンピュータネットワーク拡張の一部としてコンピューティングノードを提供する複数のホストコンピューティングシステム３６０に接続するＶＰＮ接続経由などで、クライアントの代わりに、そのクライアント用の設定可能ネットワークサービスで提供中のコンピュータネットワークとやりとりするため、メモリ３５７でソフトウェアを実行している可能性がある。また、クライアントコンピューティングシステム３５０の１つまたは複数のユーザは、別の箇所で詳述するとおり、様々な別のタイプの動作（例えば、設定可能ネットワークサービスでのクライアントのアカウントに関する管理機能、提供されるコンピュータネットワーク使用のモニタなど）を実行するためにモジュール３４０とやりとりすることができる。このほか、ホストコンピューティングシステム３６０および／または別のコンピューティングシステム３８０のいくつかは、設定可能ネットワークサービスの提供を支援するために、提供されるコンピュータネットワークのコンピューティングノード間で送信された通信の管理を支援するノード通信マネージャモジュールなどの、ソフトウェアモジュール（図示せず）を実行することができる。さらに、コンピューティングシステム３６０および３８０の別のいくつかは、種々のユーザが利用可能なリモート資源サービスの実行など、他の機能を実行することができる。情報３２２など、モジュール３４０および設定可能ネットワークサービスの機能に関する種々の情報は、ストレージ３２０にも保存されており、複数のクライアントのために、コンピュータネットワークの設定および／または提供に関する情報を含むことができる。

【００６５】

モジュール３４０がクライアント用にコンピュータネットワークを作成および設定するための１つまたは複数の要求（または他の指示）を受信すると、モジュール３４０は、別の箇所で詳述するとおり、種々の動作を実行することができる。かかる動作は、コンピュータネットワークの一部となる予定のホストコンピューティングシステム３６０からの１つまたは複数のコンピューティングノードの選択、そのコンピュータネットワークを提供するためのそれらホストコンピューティングシステムおよび／または別のコンピューティングシステムの設定、および提供されるコンピュータネットワークからクライアントのリ

モートコンピューティングシステム３５０またはリモートの別のコンピューティングシステム３８０へのアクセスの開始を含む。また、モジュール３４０は、例えば、クライアントからの要求に応じてまたは自動的に決定したとおり、提供中のコンピュータネットワークを管理するためにコンピューティングシステム３６０とさらにやりとりするが、これは、いくつかの状況における提供されるコンピュータネットワークの一部であるコンピューティングノード数の増減、提供されるコンピュータネットワーク用の設定されたネットワークトポロジの変更、提供されるコンピュータネットワークのコンピューティングノードを提供する特定のホストコンピューティングシステムの変更（例えば、提供されるコンピュータネットワークの１つまたは複数のコンピューティングノード上で実行中のプログラムの別のコンピューティングノードへの移行など）などのためである。さらに、モジュール３４０は、提供されるコンピュータネットワークの使用および動作を追跡するため、ホストコンピューティングシステム３６０の１つまたは複数のモニタ、またはそうでない場合はそれらとのやりとりを行うことができる。

【００６６】

コンピューティングシステム３００、３５０、３６０、および３８０は単に例示的であって、本発明の範囲を制限することを意図するものでないことを理解されよう。コンピューティングシステムおよび／またはコンピューティングノードは、各々代わりに複数のやりとりするコンピューティングシステムまたは装置を含んでもよく、そのコンピューティングシステム／ノードは、インターネットなどの１つまたは複数のネットワーク、ウェブ、またはプライベートネットワーク（例えば、モバイル通信ネットワークなど）経由を含めて、図示されていない別の装置に接続可能である。より一般的には、コンピューティングノードまたは別のコンピューティングシステムは、デスクトップまたは別のコンピュータ、データベースサーバ、ネットワークストレージ装置および別のネットワーク装置、ＰＤＡ、携帯電話、無線電話、ポケットベル、電子手帳、インターネット家電、テレビベースのシステム（例えば、セットトップボックスおよび／またはパーソナル／デジタルビデオレコーダを使用）、ならびに適切な通信能力を含む他の種々の消費者製品を含むがこれらに限定されることなく、やりとりし、説明したタイプの機能を実行できるハードウェアおよびソフトウェアの任意の組合せを含んでもよい。さらに、図示したモジュール３４０によって提供される機能は、いくつかの実施形態では、追加のモジュールに分散してもよく、また、モジュール３４０は、設定可能ネットワークサービスの複数のモジュールで提供されているとして別の箇所で説明されている機能（例えば、１つまたは複数のシステムマネージャモジュール、１つまたは複数のノード通信マネージャモジュール、および１つまたは複数の外部通信マネージャモジュール）を組み込むことができる。同様に、いくつかの実施形態では、モジュール３４０の一部の機能は提供されなくてもよく、さらに／または別の追加の機能が利用可能であってもよい。

【００６７】

種々のアイテムが、使用中にメモリ内またはストレージ上に格納されているとして例示されるが、これらのアイテムまたはそれらの部分は、メモリ管理およびデータ整合性の目的で、メモリと別のストレージ装置との間で転送可能であることも理解されよう。代替として、別の実施形態では、ソフトウェアモジュールおよび／またはシステムの一部もしくは全ては、別の装置上のメモリ内で実行し、コンピュータ間通信を経由して例示されたコンピューティングシステムと通信してもよい。さらに、いくつかの実施形態では、システムおよび／またはモジュールの一部もしくは全ては、特定用途向け集積回路（ＡＳＩＣ）、標準的な集積回路、コントローラ（例えば、適切な命令の実行、およびマイクロコントローラおよび／または組込コントローラを含む）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、結合プログラム可能論理回路（ＣＰＬＤ）などを含むがこれらに限定されることなく、少なくともいくつかはファームウェア内および／またはハードウェア内など、別の方法で実装または提供可能である。モジュール、システムおよびデータ構造の一部または全ても、ハードディスク、メモリ、ネットワーク、または適切なドライブもしくは適切な接続を介して読み取る携帯用媒体などの、コンピュータ可読媒体上に（例えば、

ソフトウェア命令または構造化データとして）格納することができる。システム、モジュールおよびデータ構造も、無線ベースおよび有線／ケーブルベースの媒体を含め、種々のコンピュータ可読伝送媒体上で生成されたデータ信号として（例えば、搬送波の一部または別のアナログまたはデジタル伝搬信号として）送信されることが可能で、種々の形態（例えば、単一または多重化アナログ信号の一部、または複数の不連続デジタルパケットまたはフレームとして）をとることができる。かかるコンピュータプログラム製品は、別の実施形態では別の形態をとることもできる。従って、本発明は、別のコンピュータシステム設定で実施してもよい。

【００６８】

図４Ａおよび図４Ｂは、設定可能ネットワークサービスマネージャ（Ｃｏｎｆｉｇｕｒａｂｌｅ　Ｎｅｔｗｏｒｋ　Ｓｅｒｖｉｃｅ　Ｍａｎａｇｅｒ）ルーチン４００の実施形態例の流れ図である。このルーチンは、例えば、図１Ａのシステムマネージャモジュール１１０、図２のシステムマネージャモジュール２１０、および／または図３のシステムマネージャモジュール３４０によって提供されることがあり、例えば、コンピュータネットワークをリモートクライアントに提供する設定可能ネットワークサービスの動作の管理を支援する。例示した実施形態では、ルーチン４００で作成および提供されるコンピュータネットワークの少なくともいくつかは、クライアントの既存のリモートネットワークへの拡張でもよく、他方、別の実施形態では、ルーチン４００で作成および提供されるネットワークは代わりに、別のネットワークの拡張ではない、クライアントによって使用される単独のネットワークでもよい。

【００６９】

例示した実施形態のルーチンは、ブロック４０５から始まり、ここで、クライアントからのメッセージまたは受信された別の情報の指示を受信する。少なくともいくつかの実施形態では、ルーチン４００がサポートする設定可能ネットワークサービスは、リモートクライアントがその設定可能ネットワークサービスとプログラムでやりとりできるようにする１つまたは複数のＡＰＩを提供し、そうである場合、ブロック４０５で受信された指示の一部または全ては、起動またはリモートクライアントのそれらＡＰＩとのプログラムでのやりとりによって作成された可能性があり、他方、別の実施形態および状況では、ブロック４０５で受信された指示の一部または全ては、代わりに、リモートクライアントまたは別のものによって別の方法で開始された可能性がある。

【００７０】

ブロック４０５の後、ルーチンはブロック４１０に進み、ブロック４０５で受信された指示が、要求しているクライアントのために提供される新規のコンピュータネットワークの作成（例えば、クライアントの既存のリモートネットワークへの拡張など）を開始するか否かを判定する。作成を開始する場合、ルーチンはブロック４１５に進み、クライアントのために、新規のコンピュータネットワーク拡張または別の新規のコンピュータネットワークを作成するための種々の動作を実行する。例えば、別の箇所で詳述するとおり、新規のコンピュータネットワークを作成するために受信された通信は、例えば、作成されたコンピュータネットワークの一部となる多数のコンピューティングノード、新規のコンピュータネットワークがもう１つ別のリモートネットワークへの拡張か否かの指示など、作成されるコンピュータネットワークに関連した種々の設定情報を含むことができる。ブロック４１５で取られる処置には、例えば、作成中の新規コンピュータネットワークでの使用のために設定可能ネットワークサービスから利用可能な特定のコンピューティングノードの選択、一意の識別子の生成および作成中の新規コンピュータネットワークへの関連付け、後で使用するための受信した任意の設定情報の保存などがある。別の箇所で詳述するとおり、かかるコンピューティングノードは、種々の実施形態において、例えば、選択されたコンピューティングノードの能力、選択されたコンピューティングノードのネットワーク位置（例えば、設定可能ネットワークサービスの基礎となる基板ネットワーク上、コンピュータネットワークの別のコンピューティングノードと相対的なネットワーク位置上など）、選択されたコンピューティングノードの地理的位置（例えば、地理的に分散され

た複数のデータセンタのうちの１つ内、コンピュータネットワークの別のコンピューティングノードと相対的な地理的位置上など）に基づき、またはランダムな方法などで、利用可能なコンピューティングノードのグループから種々の方法で選択することができる。さらに、ここでは図示していないが、ルーチンは、クライアントに新規コンピュータネットワーク用のの識別子または新規コンピュータネットワーク用の別の参照を提供して、クライアントが、新規コンピュータネットワークの追加の設定を実行する際に、その新規コンピュータネットワークを後で参照できるようにする。

【００７１】

ブロック４１５の後、または代わりにブロック４１０で、ブロック４０５で受信された指示が新規のコンピュータネットワークを作成しないと判定された場合、ルーチンはブロック４２０に進み、ブロック４０５で受信された指示がアクセス制限に関する情報または指示されたコンピュータネットワーク用の別のアクセス情報を含むか否かを判定する。例えば、ある状況では、クライアントは、新規のコンピュータネットワーク拡張およびその新規コンピュータネットワーク拡張用に指定された種々の設定情報の作成要求など、ブロック４０５に関して受信されて一緒に処理された１つあるいは複数の要求または別のメッセージを提供することができ、そうである場合、アクセス情報が提供される指示されたコンピュータネットワークは、ブロック４１５に関して作成されたばかりの新規コンピュータネットワーク拡張の可能性がある。別の状況および実施形態では、リモートクライアントは、例えば、新規のコンピュータネットワークを作成するための初期要求、その以前に作成されたコンピュータネットワーク用の各種の設定情報を後で指定するための１つまたは複数の別個の要求など、ブロック４０５に関して受信および処理された異なる通信を異なる時に代わりに提供することもできる。ブロック４２０で、アクセス情報がブロック４０５で受信されたと判定された場合、ルーチンはブロック４２２に進み、クライアントがリモートアクセス確立ＡＰＩを起動したか、またはそうでなければ、クライアントのリモート位置から指示されたコンピュータネットワークへのリモートアクセスの確立を要求したか否かを判定し、これは、例示した実施形態において、リモート位置にあるクライアントの１つまたは複数のリモートコンピューティングシステムから指示されたコンピュータネットワークへのＶＰＮ接続の作成を開始することにより実行される。そうである場合、ルーチンはブロック４２５に進み、リモートクライアントアクセスを確立するための処置をとるＶＰＮ作成実行（ＶＰＮ　Ｃｒｅａｔｉｏｎ　Ｆｕｌｆｉｌｌｍｅｎｔ）ルーチンを実行するが、かかるルーチンの一例は図８に関して詳述する。

【００７２】

ブロック４２５の後、または代わりにブロック４２２で、アクセス情報がリモートクライアント位置でのＶＰＮ接続の作成開始を指示していないと判定された場合、ルーチンはブロック４３０に進み、指示されたコンピュータネットワーク用に指定された別のアクセス制限情報を使用して、指示されたコンピュータネットワークのために許容アクセスを設定する。別の箇所で詳述するとおり、かかる設定情報は、コンピュータネットワークのコンピューティングノードのいずれかが、インターネットまたはそうでない場合はコンピュータネットワークの外部へのアクセスを許可されるか否か、およびオプションとしてコンピュータネットワーク（指示されたコンピュータネットワークがリモートコンピュータネットワークの外部にある場合、コンピュータネットワークのリモート部分を含む）のコンピューティングノード間の通信アクセスポリシを指定できるか否の制限を含むことができる。したがって、ブロック４３０では、別の箇所で詳述するとおり、ルーチンは、１つまたは複数の処置をとり、これには、例えば、コンピュータネットワークをサポートするノード通信マネージャモジュールおよび／または外部通信マネージャモジュールで使用するルーティング情報の設定（例えば、それらの通信マネージャモジュールに、設定する情報とともにメッセージを送信することによって）などが含まれる。また、ブロック４２５でリモートクライアント位置から提供されるコンピュータネットワークへのＶＰＮ接続を確立するための処置がとられた場合、ブロック４３０でとられた処置は、提供されるコンピュータネットワークのために、提供されるコンピュータネットワークまたはそうでない場

合は設定可能ネットワークサービスによってかかるＶＰＮ接続をサポートするための処置を追加で含むことができ、例えば、かかるＶＰＮ接続を受け取って、そのＶＰＮ接続用に暗号化された通信を解読するための適切な情報を使用するために、提供されるコンピュータネットワークを設定する。

【００７３】

ブロック４３０の後、または代わりにブロック４２０で、ブロック４０５での指示がアクセス情報を含まないと判定された場合、ルーチンは、ブロック４４０に進んで、ブロック４０５の指示が、例えば、１つまたは複数のネットワークアドレス範囲および／または別の形式で指定されたネットワークアドレスなど、指示されたコンピュータネットワーク用のネットワークアドレス情報を含むかどうかを判定する。アドレス情報を含む場合、ルーチンは、ブロック４４５に進み、指示されたコンピュータネットワークのコンピューティングノードで使用するため、指定されたネットワークアドレス情報を保存し、それらのコンピューティングノードが既に選択されているか、またはそうでなければ使用されている場合、さらに続けてそれらの指定済みネットワークアドレスを指示されたコンピュータネットワークのコンピューティングノードに関連付けることができる（例えば、ブロック４１５または／および４６２に関して）。指定済みネットワークアドレスとコンピュータネットワークのコンピューティングアドレスとの関連付けは、別の箇所で詳述するとおり、コンピュータネットワークをサポートするノード通信マネージャモジュールおよび／または外部通信マネージャモジュールによって使用されるルーティング情報の設定をさらに含むことができる。ブロック４４５の後、または代わりにブロック４４０で、ブロック４０５で受信された指示がネットワークアドレス情報を含んでいないと判定された場合、ルーチンは、ブロック４５５に進み、ブロック４０５で受信された指示が指示されたコンピュータネットワーク用のネットワークトポロジ情報を含むかどうかを判定する。ネットワークトポロジ情報を含む場合、ルーチンは、ブロック４５７に進んで、指示されたコンピュータネットワーク用のネットワークトポロジ情報を保存し、オプションとして続けて、その指示されたコンピュータネットワークをネットワークトポロジ情報に従って設定する。ネットワークトポロジ情報の設定は、別の箇所で詳述するとおり、例えば、指定されたトポロジ情報の一部である仮想ネットワーク装置の動作をシミュレートするために、コンピュータネットワークをサポートするノード通信マネージャモジュールおよび／または外部通信マネージャモジュールによって使用されるルーティング情報の設定を含むことができる。

【００７４】

ブロック４５７の後、または代わりにブロック４５５で、ブロック４０５の情報がネットワークトポロジ情報を含んでいないと判定された場合、ルーチンは、ブロック４６０に進み、例えば、指示されたコンピュータネットワークが指定された数のコンピューティングノードを含むように設定されているが、指定された数に満たないコンピューティングノードが選択されて使用されている場合などに、ブロック４０５の指示が、コンピューティングノードの指示されたコンピュータネットワークへの追加の指示を含むかどうかを判定する。さらに、いくつかの実施形態では、クライアントは、別の箇所で詳述するとおり、コンピュータネットワークの使用が継続している後であっても、コンピュータネットワークのコンピューティングノード数の変更および／またはコンピュータネットワーク用のそのネットワークトポロジ情報の変更を含め、設定可能ネットワークサービスで提供中の既存のコンピュータネットワークを種々の方法で変更できる。ブロック４６０で、指示が１つまたは複数のコンピューティングノードの追加であると判定された場合、ルーチンは、ブロック４６２に進み、設定可能ネットワークサービスの利用可能なコンピューティングノードのグループから、指示されたコンピュータネットワークに追加する１つまたは複数のコンピューティングノードを選択する。別の箇所で詳述するとおり、かかるコンピューティングノードは、種々の方法で選択することができる。ブロック４６４では、選択されたコンピューティングノードは、その後、前述と同等の方法（例えば、適切なネットワークアドレス情報をそれらの選択されたコンピューティングノードと関連付ける、コンピュ

ータネットワーク拡張用の任意の指定済みネットワークトポロジ情報および／または別のアクセス制限情報に従ってそれらの選択されたコンピューティングノードにアクセス権を設定する、など）で、コンピュータネットワークに追加される。

【００７５】

ブロック４６４の後、または代わりにブロック４６０で、ブロック４０５での指示がコンピューティングノードの追加でない場合、ルーチンは、ブロック４７０に進み、ブロック４０５での指示が、指示されたコンピューティングネットワーク用の設定されたアクセスの、指示されたリモート資源サーバへの追加か否かを判定する。そうである場合、ルーチンは、ブロック４７５に進み、指示されたリモート資源サービスをアクセスするために、指示されたコンピュータネットワーク用にアクセス機構を設定するが、これは、例えば、指示されたコンピュータネットワーク用の１つまたは複数のネットワークアドレスをそのリモート資源サービスにマッピングする、コンピュータネットワークをサポートするノード通信マネージャモジュールおよび／または外部通信マネージャモジュールで使用されるルーティング情報を設定する、そのアクセス機構を使用する通信用の外部通信マネージャモジュールによって行われる動作を設定する、などの方法で行われる。ルーチンは、その後、ブロック４７８に進み、ブロック４０５で指示されたか、またはそうでなければ設定可能ネットワークサービスで自動的に決定された場合、リモート資源サービスが、指示されたコンピュータネットワークからアクセス可能になる資源用の特定の名前空間を持ち、さらに／またはその資源で使用する指示されたコンピュータネットワーク用の１つまたは複数の追加のアクセス制御インディケータを持つか否かを判定し、そうである場合、ルーチンは、ブロック４８０に進み、その名前空間情報および／またはアクセス制御インディケータ情報を、リモート資源サービス用の設定されたアクセス機構と関連付ける。

【００７６】

ブロック４８０の後、または代わりに、ブロック４７８で名前空間および／もしくは追加のアクセス制御インディケータが使用されないと判定されたか、またはブロック４７０で、ブロック４０５での指示が指示されたリモート資源サービスへのアクセスを提供しないと判定された場合、ルーチンはブロック４９０に進み、オプションとして、１つまたは複数の指示された別の動作を適宜実行する。例えば、クライアント用に特定のコンピュータネットワークの設定を完了した後、ルーチンは、作成された新規のネットワーク拡張が属するリモートコンピュータネットワークなどの、リモート資源からのコンピュータネットワークへのアクセスを提供するための１つまたは複数の最後の手順をさらに実行してもよい。かかるアクセスの提供は、例えば、クライアントがコンピュータネットワークへアクセスできるようにするためのクライアントへの情報の提供（例えば、コンピュータネットワークへのＶＰＮ用の公的アクセス可能なネットワークアドレス）、リモートクライアントからの通信を受け付けるためのコンピュータネットワークの設定などを含むことができる。さらに、ルーチンは、適宜（例えば、定期的に、現在の状態が指定された閾値を超えたかまたは指定された条件の引き金を引いた場合）、さらに別の動作を実行できるが、これには、例えば、ネットワーク接続を確認するかまたは一部もしくは全てのコンピュータネットワーク用の一部もしくは全てのコンピュータノードの状態を確認する、リモートクライアントによる一部または全てのコンピュータネットワーク使用をモニタする、一部または全ての提供されるコンピュータネットワークによる内部の設定可能ネットワークサービス資源の使用をモニタする、設定可能ネットワークサービスでクライアントのアカウントを確立および保守する、クライアントからの自身のアカウントまたは自身の提供されるコンピュータネットワークに関する状態情報の要求に応答する、設定可能ネットワークサービスの使用に対するクライアントからの支払いを取得する、指示されたコンピュータネットワーク用のコンピューティングノードの数を減らす、指示されたコンピュータネットワークの一部である特定のコンピューティングノードを（例えば、１つまたは複数の実行プログラムを第１の地理的位置にあるコンピューティングノードから第２の地理的位置にある新しいコンピューティングノードに移動することにより）変更する、などがある。ブロック４９０の後、ルーチンはブロック４９５に進み、続行するかどうかを判定する（

例えば、終了するための明示的な指示が受信されるまで）。続行すると判定された場合、ルーチンはブロック４０５に戻り、続行しない場合は、ブロック４９９に進んで終了する。

【００７７】

図５は、ノード通信マネージャ（Ｎｏｄｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｍａｎａｇｅｒ）ルーチン５００の一実施形態例の流れ図である。このルーチンは、例えば、図２のＣＮＳノード通信マネージャモジュール２０９ａ、２０９ｄ、および２５０の実行によって提供される可能性があり、例えば、少なくともいくつかの実施形態において、提供されるコンピュータネットワークの関連したコンピューティングノード間での通信の制御などを目的とする。ルーチン５００は、少なくともいくつかの実施形態では、設定可能ネットワークサービスで提供されるコンピューティングノードの１つまたは複数と各々関連付けられた設定可能ネットワークサービスの多数のノード通信マネージャモジュールの各々によって実行される可能性があり、さらにノード通信マネージャモジュールの各々は、（例えば、別の仮想マシンコンピューティングノードが実行する物理ホストコンピューティングシステム用の仮想マシンモニタハイパーバイザの一部として、提供されるコンピュータネットワークの１つまたは複数のコンピューティングノード間での通信を制御するスタンドアロンのプロキシコンピューティングシステムまたは別のコンピューティングシステムとして、など）種々の方法によって提供される可能性がある。具体的には、例示した実施形態では、ノード通信マネージャモジュールは、設定可能ネットワークサービスにより設定可能ネットワークサービスの種々のコンピューティングノードの相互接続に使用される１つまたは複数の基礎となる物理基板ネットワークの上に重ねられた仮想ネットワークを使用して、クライアントへのコンピュータネットワークの提供を容易にするが、別の実施形態では、提供されるコンピュータネットワークは仮想ネットワークおよび／またはオーバーレイネットワーク以外の形をとることができる。さらに、別の箇所で詳述するとおり、ノード通信マネージャモジュールは、例示した実施形態では、例えば、シミュレートされた仮想または実在しないネットワーキング装置機能の実装、または存在しているかかるネットワーキング装置に一致する方法での通信の処理、などの方法により、提供されるコンピュータネットワーク用に指定されたネットワークトポロジ情報に従って機能を提供するが、別の実施形態では、提供されるコンピュータネットワーク用のネットワークトポロジ情報は、代わりに（例えば、ネットワークトポロジに対応する実際の物理ネットワーキング装置の使用など）別の方法で提供してもよい。

【００７８】

例示した実施形態のルーチンは、ブロック５０５から始まり、ここではノード通信または別のメッセージの指示が受信される。ルーチンは、ブロック５１０に進み、指示されたメッセージのタイプを判定し、それに応じて進む。具体的には、指示されたメッセージが、ルーチンが対応する通信マネージャモジュールに関連付けられた１つまたは複数の宛先コンピューティングノードを対象とした入力ノード通信であると判定された場合、ルーチンはブロック５１５に進み、入力ノード通信用に１つまたは複数の対象とする宛先コンピューティングノードを決定する。例えば、入力通信は、１つまたは複数の基礎となる基板ネットワークを経由して、ノード通信マネージャモジュールに向けられる可能性があり、さらに基板ネットワークを経由して送信された通信のヘッダまたは別の部分は、仮想の提供されるコンピュータネットワークの一部である宛先コンピューティングノードの仮想ネットワークアドレスに関する情報を含むことができるか、そうでなければ宛先コンピューティングノードを指示してもよい。以降でブロック５２５に関して説明するとおり、基板ネットワーク経由での入力通信の処理は、宛先コンピューティングノードが属する提供されるコンピュータネットワークに適した方法（例えば、宛先およびソースコンピューティングノード用に仮想ネットワークアドレスを使用するように通信のヘッダを再設定する方法など）での通信の変更を追加で含むことができる。

【００７９】

ブロック５１５の後、ルーチンはブロック５２０に進んで、入力通信が、対象とする宛

先コンピューティングノードに対して許容可能であることを確認する。別の箇所で詳述するとおり、入力通信は、許容可能か許容可能でないかを種々の方法で判定されるが、これには、例えば、指定された別のコンピューティングノード（例えば、同一の提供されるコンピュータネットワークの一部である別のコンピューティングノード）からの通信のみが許可されるよう、および／または（例えば、通信が、提供されるコンピュータネットワークのコンピューティングノードの１つからそれらのコンピューティングシステムに送信された別の通信への応答である場合に限り、別のコンピューティングシステムからの少なくともいくつかの通信に対して）指定されたタイプの通信のみが許可されるように、ファイアウォール機能または別のアクセス制御を提供する方法などがある。前述したとおり、通信が許容されるか否かの判定は、少なくともいくつかは、ルーチンが対応するノード通信マネージャモジュール用に事前に指定された設定情報に基づいて行われる可能性があり、例えば、宛先コンピューティングノードおよび／またはそれらの宛先コンピューティングノードが属する提供されるコンピュータネットワークに固有の方法で（例えば、宛先コンピューティングノードが属する提供されるコンピュータネットワーク用に指定されたネットワークトポロジ情報および／またはその提供されるコンピュータネットワーク用に指定された別のアクセス制限情報に基づいて）行われる。さらに、宛先コンピューティングノードが属する提供されるコンピュータネットワーク用にオーバーレイ仮想ネットワークが使用される実施形態では、入力通信の確認は、例えば、通信が送信者とされる人によって実際に送信されたことを確認する目的で、通信が最初の送信コンピューティングノードで送信された後、設定可能ネットワークサービスによって入力通信に含められるオーバーレイネットワークおよび／または基板ネットワークに関する情報に一部は基づいて行われる可能性がある。

【００８０】

入力通信が許容されると判定された場合、入力通信はブロック５２５で、例えば、ノード通信マネージャモジュールと宛先コンピューティングノードとの間の１つまたは複数の接続または通信リンクを経由して通信を転送することにより、１つまたは複数の通信用の宛先ノードに提供される。基礎となる基板ネットワークを経由して入力通信が送信された実施形態では、入力通信はまず、提供されるコンピュータネットワークと一致するように、例えば、提供されるコンピュータネットワークと一致する方法（例えば、宛先およびソースコンピューティングノード用に提供されるコンピュータネットワークに対応する仮想ネットワークアドレスの使用）で入力通信のヘッダを再設定することにより、変更される。また、ここでは図示していないが、ブロック５２０で通信が許容されないと判定された場合、ルーチンは、例えば、送信コンピューティングノードに対していかなる指示もない出力ノード通信をドロップする、エラーメッセージを送信コンピューティングノードに返す、出力通信を許容されるように変更しようと試みる、など、様々な処置をとることができる。

【００８１】

代わりにブロック５１０で、ブロック５０５で指示されたメッセージが、ルーチンが対応するノード通信マネージャモジュールによって管理される提供されるコンピュータネットワークの関連したコンピューティングノードからの出力ノード通信であると判定された場合、ルーチンは、代わりに５３０に進み、例えば、ブロック５２０に関して以前説明したのと同様の方法などで、出力通信が許容されるか否かをまず確認する。別の箇所で詳述するとおり、出力通信が許容されるか否かの判定は、送信コンピューティングノードが属する提供されるコンピュータネットワーク用に指定されたネットワークトポロジ情報および／またはその提供されるコンピュータネットワーク用に指定された別のアクセス制限情報などに基づき、種々の実施形態において種々の方法で行うことができる。例示した実施形態では、提供されるコンピュータネットワークは仮想オーバーレイネットワークであって、コンピューティングノード間の通信は、実際には１つまたは複数の基礎となる基板ネットワークを経由して送信される。このため、ブロック５３０の後、ルーチンは、ブロック５３５に進み、別の箇所で詳述するとおり、出力送信用の１つまたは複数の宛先コンピ

ューティングノードまたは別の宛先コンピューティングシステムに対応する１つまたは複数の基板宛先ネットワークアドレス（例えば、それらの宛先コンピューティングノード用の通信を管理する１つまたは複数のリモートノード通信マネージャモジュール、外部の宛先コンピューティングシステム用の通信を管理する外部通信マネージャモジュール、などに対する）を決定する。ルーチンはその後、ブロック５４０に進み、決定された基板宛先ネットワークアドレスを使用して、出力ノード通信を、対象とする宛先に転送する。ブロック５２５に関しての説明と同様の方法で、基礎となる基板ネットワーク経由でのノード通信の転送は、別の箇所で詳述するとおり、基板ネットワークに一致するように出力通信の変更を含むことができ、これは、例えば、基板ネットワークに一致する方法で出力通信のヘッダを再設定する（例えば、決定された基板宛先ネットワークアドレスを使用する、さらに／または宛先およびソースコンピューティングノード用の仮想ネットワークアドレスに関する情報を含める）ことにより行う。

【００８２】

代わりにブロック５１０で、ブロック５０５でもう１つ別のタイプの指示されたメッセージが受信されたと判定された場合、ルーチンは代わりにブロック５９０に進み、１つまたは複数の指示された動作を適宜実行する。例えば、別のタイプのメッセージは、図４の設定可能ネットワークサービスマネージャルーチン４００（例えば、ルーチン５００の本インスタンスに対応する１つまたは複数の提供されるコンピュータネットワーク用に、ルーチン５００によって使用されるルーティング情報または別の設定情報を指定するため）、別のノード通信マネージャルーチン（例えば、提供されるコンピュータネットワーク用の設定情報を伝播するため）などからの設定情報または別の管理メッセージを含む可能性がある。同様に、ある状況では、ルーチンはブロック５９０で、例えば、もう１つ別のノード通信マネージャモジュールまたは設定可能ネットワークサービスマネージャモジュールから情報を受信した後、かかる情報をピアツーピア方式で分散するために、提供されるコンピュータネットワーク用の設定情報を別のノード通信マネージャモジュールに送信するための動作を行うことができる。別の動作には、少なくともいくつかの実施形態および状況では、各種の管理またはハウスキーピング処理の動作を含むことができ、例えば、一部または全てのコンピュータネットワーク用の一部または全てのコンピューティングノードの状態を確認する、一部または全てのコンピュータネットワークのリモートクライアントによる使用をモニタする、一部または全ての提供されるコンピュータネットワークによる内部の設定可能ネットワークサービス資源の使用をモニタする、などがある。ブロック５２５、５４０、または５９０の後、ルーチンはブロック５９５に進み、続行するかどうかを判定する（例えば、終了する明示的な指示が受信されるまで）。続行すると判定された場合、ルーチンはブロック５０５に進み、続行しない場合は、ブロック５９９に進んで終了する。

【００８３】

このように、ルーチン５００は、設定可能ネットワークサービスによって提供されるコンピュータネットワークの一部であるコンピューティングノード間での様々なタイプの通信を管理する。ルーチンの本実施形態例では別個に示していないが、ルーチン５００は、例えば、通信のセッションまたは別の連続を開始するために、事前に送信された通信に対する１つまたは複数の応答を許可するように、少なくともいくつかの通信用に追加の設定を実行することができる。従って、例えば、提供されるコンピュータネットワークの特定のコンピューティングノードは、少なくともいくつかの別のコンピューティングシステム（例えば、外部のコンピューティングシステム）からの通信を受け入れないように設定することができるが、その通信が、最初はその特定のコンピューティングノードから送信された通信に対する応答である場合、それら別のコンピューティングシステムからの通信を許可することができる。そのため、ブロック５２０での判定はさらに、入力通信が、ブロック５３０～５４０に関して処理された以前の出力通信に対する応答かどうかに一部基づいてもよい。

【００８４】

図６は、外部通信マネージャ（Ｅｘｔｅｒｎａｌ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｍａｎａｇｅｒ）ルーチン６００の一実施形態の流れ図である。このルーチンは、例えば、図２の外部通信マネージャモジュール２７０の実行によって提供される可能性があり、例えば、データセンタまたは設定可能ネットワークサービスによって制御されるコンピューティングノードの別のグループに出入りする通信（例えば、その制御されたコンピューティングノードのグループとそれら制御されたコンピューティングノードの外部位置（例えば、クライアントのリモート位置、リモート資源サービス、およびインターネットまたは別の公衆網上の一般にアクセス可能な別の場所など）にある別のコンピューティングシステムとの間で）を管理する。別の箇所で詳述するとおり、例示した実施形態において１つまたは複数の外部通信マネージャモジュールは、例えば、クライアントによって自身の提供されるコンピュータネットワーク用に指定されたか、および／または設定可能ネットワークサービスによって自身の提供されるコンピュータネットワーク用に指定されたファイアウォールおよび別のアクセス制限情報に一致する方法で通信を処理するなど、提供されるコンピュータネットワーク用に指定されたアクセス制限情報および特定のリモート資源サービスのアクセス用に指定された設定情報に従って機能を提供する。さらに、例示した実施形態では、設定可能ネットワークサービスで提供されるコンピュータネットワークは、その設定可能ネットワークサービスで提供されるコンピューティングノードを相互接続する１つまたは複数の基礎となる物理基板ネットワークを使用する仮想オーバーレイネットワークであるが、別の実施形態では、提供されるコンピュータネットワークは、別の方法で（例えば、仮想ネットワークおよび／またはオーバーレイネットワークを使用せずに）実装してもよい。

【００８５】

例示した実施形態のルーチンは、ブロック６０５から始まり、ここで、提供されるコンピュータネットワークのコンピューティングノードとの間の通信またはもう１つ別のメッセージの指示を受信する。ブロック６０５の後、ルーチンはブロック６１０で、受信された指示されたメッセージのタイプを判定し、それに応じて進む。具体的には、指示されたメッセージが、設定可能ネットワークサービスによって制御されたコンピューティングノードへの着信であって、提供されるコンピュータネットワーク上の１つまたは複数の宛先コンピューティングノードを対象としている場合（例えば、そのクライアントのためにコンピュータネットワークが提供されるクライアントのリモート位置からＶＰＮ接続を経由して、インターネット経由で外部コンピューティングシステムから、など）、ルーチンはブロック６１５へ進む。ブロック６１５で、ルーチンはまず、入力通信がクライアントのＶＰＮ接続を経由して送信されたか否かを判定し、送信された場合はブロック６２０に進み、オプションとして通信の解読またはそうでなければ復号を行う（例えば、設定可能ネットワークサービスの別のソフトウェアがＶＰＮ接続を経由して受信された通信のかかる管理をまだ処理していない場合）。別の実施形態では、例えば、設定可能ネットワークサービスの別のソフトウェアおよび／またはハードウェアが、ブロック６０５で受信される前に、ＶＰＮ接続を経由して受信されたかかる通信を管理する場合、ブロック６１５および６２０は実行されない可能性がある。ブロック６２０の後、または代わりにブロック６１５で、入力通信がＶＰＮ接続を経由して受信されていないと判定された場合、ルーチンはブロック６２５に進む。

【００８６】

ブロック６２５～６２９は、図５のブロック５３０～５４０と同様の方法で実行される。具体的には、ブロック６２５で、ルーチンはまず、例えば、少なくともいくつかは宛先コンピューティングノードが属する提供されるコンピュータネットワーク用に指定されたネットワークトポロジ情報に基づき、さらに／またはその提供されるコンピュータネットワーク用の別のアクセス制限情報に基づいて、入力通信が許容可能であるか否かを確認する。通信が許容可能であると確認された場合、ルーチンはブロック６２７に進み、宛先コンピューティングノードに対応する１つまたは複数の宛先基板ネットワークアドレスを決定する。ブロック６２９で、ルーチンは次に、基板ネットワーク上の決定済み宛先ネット

ワークアドレスに通信を転送し、例えば、図５のブロック５１５～５２５に関して以前説明したとおり、最終的には１つまたは複数のノード通信マネージャモジュールで処理される。前述したとおり、通信がブロック６２５で許容可能であると確認されない場合、例えば、通信をドロップするなど、代わりに別の様々な処置が取られる。また、別の箇所で詳述するとおり、基板ネットワーク上での通信の転送は、その基板ネットワークと一致する１つまたは複数の方法での通信の変更を含むことができる。さらに、ここでは例示していないが、少なくともいくつかの実施形態では、ルーチンは、制御されたコンピューティングノードのグループへの入力（例えば、公衆網からプライベートネットワークへの）通信と一致する別の機能、例えば、ネットワークアドレス変換（ＮＡＴ）および／またはポートアドレス変換（ＰＡＴ）の提供、設定可能ネットワークサービス用の一般的なファイアウォールまたはプロキシまたは別のセキュリティ機能の提供など、を実行することができる。

【００８７】

代わりにブロック６１０で、指示されたメッセージが提供されるコンピュータネットワークのコンピューティングノードへの入力通信ではないが、代わりに、提供されるコンピュータネットワークのコンピューティングノードから内部の基板ネットワークを介して受信される通信であって、１つまたは複数の外部宛先コンピューティングシステムへの出力（例えば、クライアントのリモートコンピュータネットワークまたはクライアントの別のリモートコンピューティングシステムへのＶＰＮ接続経由、公的アクセス可能システムへのインターネット経由など）であると判定された場合、ルーチンはブロック６３０へ進む。ブロック６３０、６３５、および６４５は、図５のブロック５１５～５２５と同様の方法で実行される。具体的には、ブロック６３０で、ルーチンは、例えば、基板ネットワーク経由で受信した通信内の情報に基づいて、出力通信用に１つまたは複数のリモート位置にある１つまたは複数の指示された宛先コンピューティングシステムを決定する。ブロック６３５で、ルーチンは次に、前述と同様の方法で（例えば、送信コンピューティングノードが属する提供されるコンピュータネットワーク用に指定されたネットワークトポロジ情報および／またはアクセス制限情報を考慮して）、通信が許容可能か否かを判定する。ブロック６３５の後、ルーチンはブロック６４０に進み、出力通信が、例えば、クライアントのリモートコンピュータネットワークの一部として、ＶＰＮ接続を経由して１つまたは複数のリモートクライアントコンピューティングシステムへ送信されているか否かを判定する。ＶＰＮ接続の場合、ルーチンは、ブロック６４２に進み、オプションとして通信をＶＰＮ接続用に暗号化またはそうでなければ符号化し（例えば、設定可能ネットワークサービスの別のソフトウェアおよび／またはハードウェアがＶＰＮ接続経由で送信された通信のかかる管理を処理しない場合）、その後、ＶＰＮ接続経由で通信を決定済み宛先コンピューティングシステムに転送する。別の実施形態では、ＶＰＮ接続を保守する別個のソフトウェアおよび／またはハードウェアが代わりにかかる動作を実行することができる。代わりにブロック６４０で、出力通信がＶＰＮ接続経由で送信されていないと判定された場合、ルーチンは代わりにブロック６４５に進み、インターネットまたは別の公衆網を介して、通信を決定済み宛先コンピューティングシステムに転送する。前述したとおり、ルーチンは、基板ネットワーク経由で受信するかかる通信を、外部に転送される前に、例えば、通信が通る予定のコンピュータネットワークと一致する方法で出力通信のヘッダを再設定するなど、さらに変更することができる。また、ここでは例示していないが、少なくともいくつかの実施形態において、ルーチンは、制御されたコンピューティングノードのグループからの出力（例えば、プライベートから公衆網への）通信と一致する別の機能、例えば、ネットワークアドレス変換（ＮＡＴ）および／またはポートアドレス変換（ＰＡＴ）の提供、設定可能ネットワークサービス用の一般的なファイアウォールまたはプロキシまたは別のセキュリティ機能の提供など、を実行することができる。

【００８８】

代わりにブロック６１０で、指示されたメッセージが、提供されるコンピュータネットワーク上のコンピューティングノードからその提供されるコンピュータネットワーク用の

設定されたアクセス機構を持つリモート資源サービスへのアクセスであると判定された場合、ルーチンは代わりにブロック６５０に進み、リモート資源サービスアクセス（Ｒｅｍｏｔｅ　Ｒｅｓｏｕｒｃｅ　Ｓｅｒｖｉｃｅ　Ａｃｃｅｓｓ）ルーチンを実行するが、このルーチンの一実施形態例については図７に関して詳述する。そうでない場合、ルーチンはブロック６９０に進み、例えば、別の受信されたメッセージまたは受信された情報に応じて、１つまたは複数の指示された別の動作を適宜実行する。かかる指示された別の動作は、図５のブロック５９０に関して詳述したとおり、様々な形をとることができる。例えば、別のタイプのメッセージは、図４の設定可能ネットワークサービスマネージャモジュール４００から（例えば、１つまたは複数の提供されるコンピュータネットワーク用にルーチン６００で使用されるルーティング情報または別の設定情報を指定するため）、ノード通信マネージャルーチンから（例えば、提供されるコンピュータネットワーク用の設定情報を伝播するため）、などの設定情報または別の管理メッセージを含むことができる。同様にある状況では、ルーチンはブロック６９０で、例えば、別のノード通信マネージャモジュールまたは設定可能ネットワークサービスマネージャモジュールから情報を受信した後、ピアツーピア方式でかかる通信を分散するために、提供されるコンピュータネットワーク用の設定情報をノード通信マネージャに送信するための動作を行うことができる。別の動作も同様に、少なくともいくつかの実施形態および状況では、各種の管理またはハウスキーピング処理の動作を含むことができ、例えば、一部または全てのコンピュータネットワーク用の一部または全てのコンピューティングノードの状態を確認する、一部または全てのコンピュータネットワークのリモートクライアントによる使用をモニタする、一部または全ての提供されるコンピュータネットワークによる内部の設定可能ネットワークサービス資源の使用をモニタする、などがある。

【００８９】

ブロック６２９、６４２、６４５、６５０、または６９０の後、ルーチンはブロック６９５に進み、続行するか否かを判定する（例えば、終了するための明示的な指示が受信されるまで）。続行すると判定された場合、ルーチンはブロック６０５に戻り、続行しない場合は、ブロック６９９に進んで終了する。

【００９０】

このように、ルーチン６００は、設定可能ネットワークサービスによって提供されるコンピュータネットワークの一部であるコンピューティングノード間での様々なタイプの通信を管理する。このルーチンの本実施形態例には例示されていないが、ルーチン６００は、例えば、通信のセッションまたは別の連続を開始するために、以前に送信された通信に対する１つまたは複数の応答を許可するように、少なくともいくつかの通信用に追加の設定を実できることが理解されよう。従って、例えば、特定の提供されるコンピュータネットワークは、いかなる外部コンピューティングシステムも、そのコンピュータネットワークのコンピューティングノードへの通信を開始するのを防ぐように設定することができるが、かかる外部コンピューティングシステムが、最初はそのコンピュータネットワークのコンピューティングノードからその外部コンピューティングシステムへ送信された通信に応答するのを許可することができる。そのため、ブロック６２５での判定が、入力通信が、ブロック６３０～６４５に関して処理された以前の出力通信に対する応答であるか否かにさらに一部基づいてもよい。同様に、ブロック６５０に関して詳述したように、リモート資源サービスにアクセスするために開始された通信に対するリモート資源サービスからの応答は、ブロック６１５～６２９に関してのように、許容されるように設定できるか、または代わりに別の方法で設定できる。

【００９１】

図７は、リモート資源サービスアクセス（Ｒｅｍｏｔｅ　Ｒｅｓｏｕｒｃｅ　Ｓｅｒｖｉｃｅ　Ａｃｃｅｓｓ）ルーチン７００の一実施形態例の流れ図である。このルーチンは、図６のブロック６５０の実行によって開始される場合、例えば、図２の外部通信マネージャモジュール２７０の実行によって提供される可能性がある。ルーチンは、提供されるコンピュータネットワークのコンピューティングノードにより、リモート資源サービスに

対して行われた通信、具体的には、例えば、図４Ｂのブロック４７５～４８０に関連して、提供されるコンピュータネットワークが専用アクセスを提供するために事前に設定されたリモート資源サービスに対して行われた通信を管理する。別の箇所で詳述するとおり、少なくともいくつかの実施形態では、提供されるコンピュータネットワークは、特定のリモート資源サービスに対する専用アクセスを提供するように（例えば、リモート資源サービスを表すために、その提供されるコンピュータネットワーク上の１つまたは複数のネットワークアドレスを割り当てることにより）設定でき、基板物理ネットワークは、対応する通信を、外部通信を管理する外部通信マネージャモジュールに転送するように設定できる（外部通信マネージャモジュールを、それら転送された通信を適宜管理するように設定して）。

【００９２】

例示した実施形態では、ルーチンはブロック７０５から始まり、ここで、提供されるコンピュータネットワーク上のコンピューティングノードから、そのコンピュータネットワーク用に設定されたアクセス機構が提供されているリモート資源サービスへの通信の指示が、例えば、通信用に使用されたネットワークアドレスに基づいて、受信される。ルーチンは次にブロック７１０に進み、ここで、通信用に使用されたアクセス機構用に以前に指定された設定情報を検索する。ブロック７１５で、ルーチンはその後、例えば、検索した設定情報に基づいて、通信が対象とする宛先リモート資源サービスを決定する。

【００９３】

ブロック７１５の後、ルーチンは７２５に進み、図５のブロック５２０および５３０、ならびに図６のブロック６２５および６３５に関して説明したのと同様の方法で、通信が許容可能か否かを判定する。さらに、判定は、少なくともいくつかの状況および実施形態では、ある設定されたアクセス機構に関してあるタイプの通信のみを許可するため、使用されたアクセス機構用に検索された設定情報に基づいてさらに行われる可能性がある。通信が許容可能と判定された場合、ルーチンは次にブロック７３０に進み、オプションとして、使用されたアクセス機構用の以前の設定に基づく方法で通信を変更する。例えば、別の箇所で詳述するとおり、アクセス機構は、リモート資源サービスで使用された特定の名前空間に対応するためや、リモート資源サービスによる認証の目的で、通信を送信するコンピューティングノードの提供されるコンピュータネットワークに関する情報またはコンピューティングノードの位置に関する別の情報を含むため等に、通信を変更するように設定される可能性がある。

【００９４】

ルーチンはその後、ブロック７３５に進み、オプションとして、決定済みリモート資源サービスに固有の方法で、通信用に追加の認証関連動作を実行する。例えば、別の箇所で詳述するとおり、少なくともいくつかのリモート資源サービスは、設定可能ネットワークサービスに属しているか、またはそうでなければ、設定可能ネットワークサービスが、公衆網を介してリモート資源サービスと通信する未認証のリクエスタに提供されていない特権的な方法で、リモート資源サービスにアクセスするのを許可する可能性がある。そうであれば、ルーチンは、例えば、通信が信頼されるかまたはそうでなければ既知のリクエスタから送信されているとリモート資源サービスが判定できるようにする認証関連動作を実行できるが、これは、例えば、設定可能ネットワークサービスに対応する識別子を含むように通信を変更することによって（例えば、設定可能ネットワークサービスとリモート資源サービスとの間の事前のやりとりに基づき、変更済み通信の一部として識別子に基づくデジタル署名を含むこと等により）実行できる。

【００９５】

ブロック７３５の後、ルーチンは次にブロック７４５に進み、オプションとして、通信の暗号化またはそうでなければ決定済みリモート資源サービスへの安全な接続（例えば、特定の関連するリモート資源サービスとのＶＰＮ接続、リモート資源サービスへの専用プライベート回線または別の通信リンク、など）にアクセスし、通信を決定済みリモート資源サービスに転送する。転送中の通信は、例えば、インターネットまたは１つもしくは複

数の別の公衆網を介して送信することができるか、または代わりにいくつかの実施形態において、プライベート通信リンクまたは別の安全な接続を経由して送信することができる。ブロック７４５の後、ルーチンはブロック７９９に進んで終了する。

【００９６】

図８は、ＶＰＮ作成実行（ＶＰＮ　Ｃｒｅａｔｉｏｎ　Ｆｕｌｆｉｌｌｍｅｎｔ）ルーチン８００の流れ図である。ルーチンは、設定可能ネットワークサービスの実施形態によって提供されるリモートアクセス確立ＡＰＩのクライアント起動に起因する、図４Ａのブロック４２５の実行に基づいて開始される場合、例えば、設定可能ネットワークサービスマネージャモジュールの実行によって提供される。

【００９７】

例示した実施形態では、ルーチンはブロック８０５から始まり、ここで、クライアントのリモート位置（例えば、クライアントのリモートプライベートコンピュータネットワーク）からクライアント用の提供されるコンピュータネットワーク（例えば、クライアントのリモートプライベートコンピュータネットワーク用の設定可能ネットワークサービスによって提供されるネットワーク拡張）へのＶＰＮ接続を確立するためのクライアント要求の指示を受信する。少なくともいくつかの実施形態では、クライアントによるＶＰＮ接続の確立要求は、クライアントのリモート位置に提供される１つまたは複数の適切なネットワーキング装置および対応するソフトウェアおよび／または設定情報に関する注文の実行要求の一部であり、それによって、ＶＰＮ接続がリモートのクライアント位置にある１つまたは複数のコンピューティングシステムから設定可能ネットワークサービスによってクライアント用に提供されるコンピュータネットワークに対して確立できるようにする。少なくともいくつかのかかる実施形態では、リモートアクセス確立ＡＰＩの起動またはクライアントからの別の要求の開始の後、注文の実行は、クライアントによるいかなる追加の動作なしに、設定可能ネットワークサービスによって実行されるが、別の実施形態では、クライアントとのある追加のやりとりが、注文履行の一部として実行される（例えば、クライアントへのオプションの提示、クライアントからの追加情報の取得、クライアントからの支払い情報の取得、など）可能性がある。

【００９８】

ブロック８１５で、ルーチンは次に、要求の実現に使用するクライアントに関する種々の情報を取得するが、それらは、例えば、ブロック８０５で受信された要求で供給されたか、以前クライアントから受信され、設定可能ネットワークサービスでクライアントのアカウントから検索されたか、ならびに／またはそのクライアントおよび／もしくは１つまたは複数の外部ソースから動的に取得された情報などの可能性がある。取得された情報は、例えば、ネットワーキング装置および別のアイテムを物理的に配達可能なクライアントの地理的位置に関する情報、電子情報を電子的に配信可能な電子通信アドレス、クライアントがブロック８０５で受信された要求に関連する料金の支払いに利用する支払い情報、など、種々の形態をとる可能性がある。さらに、リモートクライアント位置とクライアント用に提供されるコンピュータネットワークとの間でＶＰＮ接続を設定するのを支援するために、ＶＰＮ接続開始のためにリモートクライアント位置から公的アクセス可能なネットワークアドレス（または対応する別の接続情報）、ＶＰＮ接続の確立先である提供されるコンピュータネットワークの識別に使用する一意の識別子または別の情報など、種々の情報が取得される可能性がある。

【００９９】

ブロック８１５の後、ルーチンはブロック８２５に進み、提供されるコンピュータネットワークへのＶＰＮ接続を確立するために、クライアントの１つまたは複数のリモートコンピューティングシステムで使用する１つまたは複数の適切なネットワーキング装置を決定する。別の箇所で詳述するとおり、適切なネットワーキング装置は、例えば、クライアント用に提供されるコンピュータネットワーク、クライアントのリモートコンピューティングシステム、および／または設定可能ネットワークサービス（例えば、設定可能ネットワークサービスの基板ネットワークまたは設定可能ネットワークサービスの別のインフラ

の一部として使用されたネットワーク装置に基づいて）に固有の情報などに基づき、種々の方法で決定することができる。さらに、適切なネットワーキング装置の決定は、例えば、設定可能ネットワークサービスにより自動的に決定され、かつ／または少なくともいくつかはクライアントからの情報に基づいて（例えば、ブロック８０５で受信された要求の一部としてクライアントによる選択に基づき、またはクライアントに提示された複数の選択肢からの選択など、別の方法でクライアントによる指定として）決定される、など、種々の実施形態において種々の方法で行われる可能性がある。

【０１００】

ブロック８２５の後、ルーチンはブロック８３５に進み、クライアント用に提供されるコンピュータネットワークに接続するネットワーキング装置の準備で使用するネットワーキング装置を決定するための設定情報を生成するが、別の実施形態では、ルーチンは、第三者の団体（例えば、ブロック８４５で連絡をとる同一の小売業者）に設定情報を生成するように指示することができる。少なくともいくつかの実施形態では、決定されたネットワーキング装置用の設定情報は、設定されたネットワーキング装置の設定を完了するため、（例えば、特定の提供されるコンピュータネットワークに固有の方法でネットワーキング装置を設定するために、設定可能ネットワークサービスから追加の情報を取得することにより）設定されたネットワーク装置に設定可能ネットワークサービスとの連絡を開始させることができる。また、少なくともいくつかの実施形態では、決定されたネットワーキング装置用の設定情報は、例えば、提供されるコンピュータネットワークへのＶＰＮ接続を確立するために、設定されたネットワーキング装置にクライアントの提供されるコンピュータネットワークとの連絡を開始させることができる。生成された設定情報は、いくつかの実施形態では、決定されたネットワーキング装置のタイプ、および／または決定されたネットワーキング装置によるＶＰＮ接続の確立先である提供されるコンピュータネットワークに固有の可能性があり、さらに、設定情報の生成は、事前に準備された設定情報の検索、および／または新規設定情報の動的作成（例えば、事前に準備された設定情報が任意のネットワーキング装置および／または任意の提供されるコンピュータネットワーク用である場合などに、例えば、決定されたネットワーキング装置および／または提供されるコンピュータネットワークに固有の方法で事前に準備された設定情報を変更することによって）を含む可能性がある。生成された設定情報は、同様に、例えば、ハードウェア装置上で実行される設定されたソフトウェア、リモート位置で人間のオペレータで使用されるテキストの指示として、など、種々の形態をとる可能性がある。

【０１０１】

ブロック８４５で、ルーチンは次に、クライアントの１つまたは複数のリモートコンピューティングシステムでの使用のために決定済みネットワーキング装置をリモートクライアント位置に供給するため、小売業者への発注を開始し、そして、例示される実施形態では、さらに、ネットワーキング装置での使用のために生成された設定情報のクライアントへの供給を開始する。かかる実施形態では、生成された設定情報は、例えば、発注の一部として設定情報を送信する、ブロック８３５で設定情報を生成するように事前に小売業者に指示する、など、種々の方法で小売業者に提供できる。別の箇所で詳述するとおり、生成された設定情報は、次の１つまたは複数の方法を含め、種々の方法でクライアントに供給でき、つまり、生成された設定情報を物理的にクライアントに配達される物理装置可読ストレージ媒体（例えば、ＣＤ、ＤＶＤ、ＵＳＢメモリキーなど）に格納する、クライアントへの配達前に、生成された設定情報でネットワーキング装置を設定する（例えば、小売業者が使用する発送センターで生成された設定情報をネットワーキング装置にロードする）、生成された設定情報をクライアントに電子的に送信する、などの方法である。別の実施形態では、ネットワーキング装置および／または設定情報は、例えば、ネットワーキング装置および生成された設定情報の一方または両方を小売業者よりはむしろ設定可能ネットワークサービスで直接供給させる、ネットワーキング装置の供給に第１の小売業者を利用し、生成された設定情報の供給に異なる第２の小売業者を利用する、小売業者ではない１つまたは複数の第三者の団体を利用する、など、別の方法でクライアントに提供でき

る。ブロック８４５の後、ルーチンはブロック８９９に進み、戻る。

【０１０２】

いくつかの実施形態では、前述したルーチンによって提供される機能は、より多数のルーチンに分割したり、より少数のルーチンに統合したり、などの代替方法で提供できることを理解されよう。同様に、いくつかの実施形態では、例示されるルーチンは、例えば、例示される別のルーチンの各々が、かかる機能を欠いていたり含んでいたりする場合や、提供される機能の量が変更される場合などでも、ほぼ説明どおりの機能を提供することができる。また、種々の動作が、特定の方法（例えば、連続して、または、並行して）および／または特定の順序で実行されていると説明されることがあるが、当技術分野に精通した人であれば、別の実施形態では、その動作は別の順序および別の方法で実行できることを理解されよう。当技術分野に精通した人であれば、前述したデータ構造が、例えば、単一のデータ構造を複数のデータ構造に分割したり、複数のデータ構造を単一のデータ構造に統合したり、などの別の方法で構造化できることも理解されよう。同様に、いくつかの実施形態では、例示されたデータ構造は、例えば、例示された別のデータ構造の各々がかかる情報を欠いていたり含んでいたりする場合や、格納される情報の量やタイプが変更される場合などでも、ほぼ説明どおりの情報を格納することができる。

【０１０３】

第１項。設定可能ネットワークサービスのコンピューティングシステムがプライベートコンピュータネットワークにアクセスを提供する方法であって、

リモートユーザが、前記リモートユーザのリモートプライベートコンピュータネットワークへのネットワーク拡張を作成および設定できるようにする、前記設定可能ネットワークサービス用のプログラムによるインタフェースを提供することであって、前記設定可能ネットワークサービスが、前記作成されたネットワーク拡張を前記リモートユーザに提供する際に使用される複数のコンピューティングシステムを含むことと、

前記設定可能ネットワークサービスの前記コンピューティングシステムの制御下において、かつ、複数のリモートユーザの各々に対して、

ローカルプライベートネットワーク拡張を、前記ユーザのリモートプライベートコンピュータネットワークに対して作成および設定するための前記提供されるプログラマティクインタフェースを経由して前記リモートユーザによりプログラムによって提供される設定情報を受信することであって、前記プライベートネットワーク拡張が前記設定可能ネットワークサービスにより提供され、かつ前記複数のコンピューティングシステムのサブセットを含み、前記受信された設定情報が前記プライベートネットワーク拡張用のユーザによって特定されたネットワークトポロジ情報および前記複数のコンピューティングシステムに割り当てられる前記プライベートコンピュータネットワークの複数のネットワークアドレスのユーザによって特定されたサブセットを含み、前記受信された設定情報が前記ユーザの前記プライベートコンピュータネットワークの外部にあって、かつ前記プライベートネットワーク拡張の複数のコンピューティングシステムからアクセス可能であるリモート資源サービスの指示をさらに含むことと、

前記ユーザの前記プライベートコンピュータネットワークと前記ユーザの前記プライベートネットワーク拡張の前記複数のコンピューティングシステムとの間にプライベートアクセスを提供するため、前記ユーザの前記プライベートネットワーク拡張を自動的に設定することであって、前記設定が、前記プライベートネットワーク拡張と前記ユーザの前記プライベートコンピュータネットワークとの間での仮想プライベートネットワーク接続の確立および前記プライベートネットワーク拡張内の通信を前記特定されたネットワークトポロジ情報に従ってルーティングされるようにする設定を含むことと、

前記指示されたリモート資源サービス内の新規名前空間を表すために、前記プライベートネットワーク拡張用に一意の識別子を自動的に生成することであって、前記リモート資源サービスが複数のユーザにコンピューティング関連資源を提供し、前記表された名前空間が前記プライベートネットワーク拡張からのみアクセス可能な前記リモート資源サービスによって提供される１つまたは複数のコンピューティング関連資源を含むことと、

前記表された名前空間内の前記リモート資源サービスによって提供される前記１つまたは複数のコンピューティング関連資源への前記プライベートネットワーク拡張の前記複数のコンピューティングシステムからのアクセスを可能にするために、前記ユーザの前記プライベートネットワーク拡張を自動的に設定することであって、前記設定が、前記リモート資源サービスを表すようにネットワークアドレスの前記ユーザにより特定されたサブセットの１つへの割当ておよび前記一意の識別子の前記割当てられたネットワークアドレスとの関連付けを含み、前記割当てられたネットワークアドレス経由で前記リモート資源サービスに送信された通信が、前記表された名前空間の識別のために前記リモート資源サービスで使用される前記一意の識別子を含むように変更されることと、

前記提供されるネットワーク拡張の前記複数のコンピューティングシステムと前記ユーザの前記プライベートコンピュータネットワークとの間に前記プライベートアクセスを提供することと、

を含む方法。

【０１０４】

第２項。前記複数のユーザのうちの１ユーザに対して、

前記１ユーザ用の前記プライベートネットワーク拡張の前記複数のコンピューティングシステムを異なる通信間特性を持つ異なるグループに分割するため、前記受信された設定情報内の前記ネットワークトポロジ情報がさらに１つまたは複数のネットワーク装置を特定し、

前記受信された設定情報が、前記１ユーザ用の前記プライベートネットワーク拡張の前記複数のコンピューティングシステムが、前記ユーザの前記プライベートコンピュータネットワークの前記複数のネットワークアドレスの一部でないネットワークアドレスを持つコンピューティングシステムへのアクセスを許可されない、という指示をさらに含み、かつ、

前記１ユーザの前記プライベートコンピュータネットワークからの前記１ユーザ用の前記プライベートネットワーク拡張への前記プライベートアクセスを提供するための前記１ユーザの前記プライベートネットワーク拡張の自動設定は、前記特定された１つまたは複数のネットワーク装置をシミュレートするための仮想装置の作成および、前記１ユーザの前記プライベートコンピュータネットワークと前記１ユーザの前記プライベートコンピュータネットワークの外部の任意のコンピューティングシステムとの間の通信を防ぐための１つまたは複数の実際のネットワーキング装置の設定を含む、

第１項に記載の方法。

【０１０５】

第３項。前記設定可能ネットワークサービスが、公衆網を介して前記リモートユーザにアクセス可能であって、かつクラウドコンピューティング技術を用いて前記ネットワーク拡張を提供する有料サービスである方法であって、かつ

前記複数のリモートユーザが、前記設定可能ネットワークサービスによって前記ユーザに対して提供されている前記作成されたネットワーク拡張用の前記設定可能ネットワークサービスに対して支払いを行う前記設定可能ネットワークサービスの顧客である、

第２項に記載の方法。

【０１０６】

第４項。プライベートコンピュータネットワークへのアクセスを提供するためのコンピュータに実装された方法であって、

複数のクライアントが、前記複数のクライアントによって使用されるプライベートコンピュータネットワークを設定するために使用されるプログラムによるインタフェースを提供する設定可能ネットワークサービス用のコンピューティングシステムの制御下において、

第１のクライアントによって使用される第１のプライベートコンピュータネットワークを設定するための前記プログラムによるインタフェースを用いて、前記第１のクライアントによってプログラムによって提供される第１の情報を受信することであって、前記第１

のプライベートコンピュータネットワークが、前記設定可能ネットワークサービスにより提供される複数のコンピューティングノードのグループを含み、前記複数のコンピューティングノードの各々が、前記第１のプライベートコンピュータネットワークで使用するために前記第１の情報に特定されている複数のネットワークアドレスのうちの少なくとも１つに関連付けられるように設定されていることと、

第１のプライベートコンピュータネットワークからネットワークアクセス可能なリモート資源サービス内の名前空間に関連付けられているコンピューティング関連資源のサブセットへのアクセスを設定するための第２の情報を取得することであって、前記第２の情報が、前記リモート資源サービス内の名前空間に関連付けられている識別子を含むことと、

前記複数のコンピューティングノードから前記リモート資源サービスによって提供されるコンピューティング関連資源の前記サブセットへのアクセスを可能にするように第１のプライベートコンピュータネットワークを自動的に設定することであって、前記設定が、前記識別子と前記リモート資源サービスを表す１つまたは複数の指示されたネットワークアドレスとの関連付けを含み、コンピューティング関連資源の前記サブセットをアクセスするために、前記指示されたネットワークアドレスを経由して前記リモート資源サービスに送信された通信が、前記名前空間を識別する際に前記リモート資源サービスによって使用される前記識別子の指示を含むように変更されることと、

前記第１のクライアントの１つまたは複数のリモートコンピューティングシステムから第１のプライベートコンピュータネットワークへのアクセス利用可能状態を開始することと、

を含む方法。

【０１０７】

第５項。前記第１のプライベートコンピュータネットワークが、複数のコンピューティングシステムを含む第１のクライアントのリモートプライベートコンピュータネットワークの拡張になるように設定されていて、前記特定された複数のネットワークアドレスが、前記リモートプライベートネットワークで使用される複数のプライベートネットワークアドレスのサブセットであって、第１のプライベートネットワークの前記自動設定が、前記第１のクライアントの前記リモートプライベートコンピュータネットワークの前記複数のコンピューティングシステムと前記第１のプライベートコンピュータネットワークの前記複数のコンピューティングノードとの間のプライベートアクセスをさらに可能にする、第４項に記載の方法。

【０１０８】

第６項。前記第１のクライアントの前記１つまたは複数のリモートコンピューティングシステムから前記第１のプライベートコンピュータネットワークへの前記アクセス利用可能状態の前記開始が、前記有効なプライベートアクセスを提供するための前記リモートプライベートコンピュータネットワークと前記第１のプライベートコンピュータネットワークとの安全な接続の確立を含む、第５項に記載の方法。

【０１０９】

第７項。前記第１のプライベートコンピュータネットワークが、前記設定可能ネットワークサービスによって提供される前記複数のコンピューティングノードと相互接続する前記設定可能ネットワークサービスの１つまたは複数の物理基板ネットワーク上に重なる仮想ネットワークとして前記設定可能ネットワークサービスによって提供される、第５項に記載の方法。

【０１１０】

第８項。前記第１の情報が、前記第１のプライベートコンピュータネットワークの前記複数のコンピューティングノード間での通信を制御するために前記第１のプライベートコンピュータネットワークの設定時に使用するために第１のクライアントによって特定される追加情報をさらに含み、かつ、前記方法が、前記特定された追加情報に従って前記複数のコンピューティングノード間の通信を許可および阻止するように第１のプライベートコンピュータネットワークの自動設定をさらに含む、第４項に記載の方法。

【０１１１】
第９項。前記特定された追加情報が、前記第１のプライベートコンピュータネットワークの一部である１つまたは複数のネットワーキング装置の少なくとも１つ、および共通の相互通信特性を共有する前記複数のコンピューティングノードの１つまたは複数のサブグループを指示するネットワークトポロジ情報を含む方法であって、前記ネットワークトポロジ情報が前記１つまたは複数のネットワーキング装置を指示する場合、前記第１のプライベートコンピュータネットワークの前記自動設定が、前記１つまたは複数のネットワーキング装置の存在をシミュレートするための前記設定可能ネットワークサービスの１つまたは複数のモジュールの設定を含む方法であって、前記ネットワークトポロジ情報が前記１つまたは複数のサブグループを指示する場合、前記第１のプライベートコンピュータネットワークの前記自動設定が、前記１つまたは複数のサブグループの存在をシミュレートするための前記設定可能ネットワークサービスの１つまたは複数のモジュールの設定を含む、第８項に記載の方法。
【０１１２】
第１０項。前記第１の情報が、前記第１のプライベートコンピュータネットワークの設定に使用するために第１のクライアントによって特定される追加情報をさらに含む方法であって、前記追加情報が、前記第１のプライベートネットワーク用の前記複数のコンピューティングノード数のうちの１つまたは複数、前記複数のコンピューティングノードの少なくともいくつかが配置されている１つまたは複数の地理的位置、および前記第１のプライベートコンピュータネットワークの前記複数のコンピューティングノードと前記第１のプライベートコンピュータネットワークの外部にある別のコンピューティングシステムとの間の通信を制御する１つまたは複数のネットワークアクセス制限を含み、前記方法が、前記特定された第１の情報に基づき第１のプライベートコンピュータネットワーク用に前記複数のコンピューティングノードの自動選択と、前記特定された追加情報に従って第１のプライベートコンピュータネットワークの自動設定をさらに含む、第４項に記載の方法。
【０１１３】
第１１項。第２の情報が、前記プログラムによるインタフェースを用いて前記第１のクライアントがプログラムで提供する前記第２の情報に少なくとも部分的に基づき取得され、前記提供される第２の情報が、前記名前空間用の前記関連付けられた識別子を含み、前記第２の情報の前記提供前に、コンピューティング関連資源の前記サブセットの少なくともいくつかが前記名前空間内の前記リモート資源サービスに存在し、前記方法が、前記リモート資源サービスから前記既存の少なくともいくつかのコンピューティング関連資源の１つまたは複数にアクセスするため、前記１つまたは複数のコンピューティングノードから前記指示されたネットワークアドレスに送信された１つまたは複数の通信の取得、および前記識別子の前記指示を含むために、前記取得した１つまたは複数の通信を変更後、前記取得した１つまたは複数の情報の前記リモート資源への転送をさらに含む、第４項に記載の方法。
【０１１４】
第１２項。前記第２の情報に含まれる前記識別子の前記取得が、前記設定可能ネットワークサービスが前記第１のプライベートコンピュータネットワーク用の名前空間を作成するために前記リモート資源サービスと自動的にやりとりすることを含み、前記名前空間の前記作成が前記名前空間用の前記識別子の決定を含む方法であって、前記方法が、１つまたは複数の新規コンピューティング関連資源を前記リモート資源サービスから作成するため、前記複数のコンピューティングノードの１つまたは複数から前記指示されたネットワークアドレスに送信された１つまたは複数の通信の取得、および前記識別子の指示を含むため、前記取得された１つまたは複数の通信の変更後、前記取得された１つまたは複数の通信の前記リモート資源への転送をさらに含む、第４項に記載の方法。
【０１１５】
第１３項。前記リモート資源サービスが、１つまたは複数の公衆網を経由してアクセス

可能であって、前記複数のコンピューティングノードからコンピューティング関連資源の前記サブセットへのアクセスを可能にするための第１のプライベートコンピュータネットワークの前記設定が、前記指示されたネットワークアドレスに送信された通信を前記１つまたは複数の公衆網を経由して前記リモート資源サービスに転送するように、前記設定可能ネットワークサービスの１つまたは複数のモジュールの設定を含む、第４項に記載の方法。

【０１１６】

第１４項。前記第１のプライベートコンピュータネットワークから、前記リモート資源サービス内の第２の別個の名前空間と関連付けられたコンピューティング関連資源の第２の別個のサブセットへのアクセスを設定するための第３の情報を取得し、前記第３の情報が、前記リモート資源サービス内の第２の名前空間と関連付けられた第２の別個の識別子を含み、かつ、前記第２の識別子を前記複数のネットワークアドレスの第２の１つに関連付けることにより、前記複数のコンピューティングノードからコンピューティング関連資源の第２のサブセットへのアクセスを可能にするため、前記第１のプライベートコンピュータネットワークを自動設定して、前記第２のネットワークアドレス経由で前記リモート資源サービスに送信された通信が、コンピューティング関連資源の第２のサブセットにアクセスするために、前記名前空間を識別するために前記リモート資源サービスで使用される前記第２の識別子の指示を含むように変更されるようにする、第４項に記載の方法。

【０１１７】

第１５項。前記リモート資源サービス内の前記名前空間に関連付けられた前記コンピューティング関連資源が、データストレージサービスおよびプログラム実行サービスおよび非同期メッセージ受渡しサービスの少なくとも１つに対する資源を含む方法であって、

前記方法がさらに、前記リモート資源サービスの制御下において、

コンピューティング関連資源のサブセットの少なくともいくつかにアクセスするために、前記指示されたネットワークアドレス経由で前記第１のプライベートコンピュータネットワークの前記複数のコンピューティングノードから送信された通信を受信することであって、前記受信された通信が前記識別子の前記指示を含むことと、

前記指示された識別子に関連付けられた前記名前空間から前記少なくともいくつかのコンピューティング関連資源へのアクセスを提供することと、を含む、

第４項に記載の方法。

【０１１８】

第１６項。前記複数のコンピューティングノードが、各々、前記設定可能ネットワークサービスの複数の物理コンピューティングシステムの１つをホストとした仮想マシンである方法であって、かつ前記第１のプライベートコンピュータネットワークの前記設定が、前記ホストされた仮想マシン用に通信を管理するように、１つまたは複数の前記物理コンピューティングシステム上で実行する１つまたは複数の仮想マシン通信マネージャモジュールの設定を含む、第４項に記載の方法。

【０１１９】

第１７項。

前記複数のクライアントによって設定された前記プライベートコンピュータネットワークが、第１のプライベートコンピュータネットワークで使用するために特定された前記複数のネットワークアドレスの少なくとも１つと同一である前記１つまたは複数の別のクライアントによって特定された１つまたは複数のネットワークアドレスを持つ前記第１のクライアント以外の１つまたは複数のクライアント用の前記第１のプライベートコンピュータネットワーク以外の１つまたは複数の設定されたプライベートコンピュータネットワークを含む方法であって、かつ、前記設定可能ネットワークサービスが、それら同一ネットワークアドレスが、それら同一ネットワークアドレスの各々について、前記別のプライベートコンピュータネットワークの各々が、前記第１のプライベートコンピュータネットワーク用の前記ネットワークアドレスに対応するコンピューティングノードと別個の前記ネットワークアドレスに対応するコンピューティングノードを持つように、さらに管理する、

第４項に記載の方法。
【０１２０】
第１８項。前記第１のクライアントによる前記第１のプライベートコンピュータネットワークの設定が、前記第１のプライベートコンピュータネットワークで使用される前記第１の情報で特定される前記複数のネットワークアドレス用に、前記第１のクライアントが任意のネットワークアドレスを選択することの許可を含む、第４項に記載の方法。
【０１２１】
第１９項。前記第１のクライアントにより前記プログラムによるインタフェースを用いてプログラムによって提供される前記第１の情報が、前記第１のクライアントのコンピューティング装置上に前記第１のクライアントに対して表示されるグラフィカルユーザインタフェースとの前記第１のクライアントの１つまたは複数のやりとりに基づいて受信される、第４項に記載の方法。
【０１２２】
第２０項。内容が、設定可能ネットワークサービスのコンピューティングシステムがプライベートコンピュータネットワークへのアクセスを提供できるようにするコンピュータ可読媒体であって、前記提供を実行する方法が、
設定可能ネットワークサービスの複数のリモート顧客の各々に対して、
前記顧客のリモートプライベートネットワーク用のネットワーク拡張を前記顧客用に作成を開始し、かつ前記顧客の前記作成されたネットワーク拡張用に設定情報を特定するために、前記リモート顧客によってプログラムで行われた１つまたは複数の要求を受信することであって、前記設定情報が、前記顧客の前記作成されたネットワーク拡張用のネットワークトポロジ情報を含むことと、
前記顧客の前記作成されたネットワーク拡張の一部として使用される複数のコンピューティングノードを自動選択することであって、前記複数のコンピューティングノードが、前記設定可能ネットワークサービスで提供される複数のコンピューティングノードのサブセットであって、かつ前記顧客によって特定された前記設定情報に少なくとも部分的に基づいて選択されることと、
前記顧客の前記作成済みネットワーク拡張への前記顧客のプライベートアクセスを提供するために、前記顧客の前記作成済みネットワーク拡張が前記複数のコンピューティングノードを使用するように自動設定されることであって、前記プライベートアクセスが、前記複数のコンピューティングノードと前記顧客の前記リモートプライベートネットワークの１つまたは複数のコンピューティングシステムとの間の相互通信を可能にし、前記相互通信が、前記顧客によって特定された前記ネットワークトポロジ情報に従い前記作成済みネットワーク拡張経由でルーティングされることと、
前記顧客の前記作成済みネットワーク拡張への前記顧客の前記プライベートアクセスの提供を開始することと、を含む方法である、
コンピュータ可読媒体。
【０１２３】
第２１項。前記設定可能ネットワークサービスが、要求を提供するために前記複数のリモート顧客によって使用されるプログラムによるインタフェースを提供し、前記複数の顧客の各々から受信された前記１つまたは複数の要求が、前記プログラムによるインタフェースを使用して提供され、かつ、前記１人または複数のリモート顧客の各々について、前記顧客によって特定された前記ネットワークトポロジ情報が、前記顧客用の前記作成済みネットワーク拡張で使用される複数のネットワークアドレスの指示を含み、前記複数のコンピューティングノードを使用するため、前記顧客用に前記作成済みネットワーク拡張の前記設定が、前記コンピューティングノードの前記指示されたネットワークアドレスの１つとの関連付けを含み、前記資源サービス用の前記アクセス機構が、前記資源サービスを表すために割当てられた前記作成済みネットワーク拡張用の前記複数のネットワークアドレスの１つを含む、第２０項に記載のコンピュータ可読媒体。
【０１２４】

第２２項。第１のネットワークアドレスが前記複数の顧客の少なくともいくつかの各々によって特定され、かつ、前記少なくともいくつかの顧客の前記作成済みネットワーク拡張の前記自動設定が、前記少なくともいくつかの顧客の前記作成済みネットワーク拡張用に区別した第１のネットワークアドレスの管理を含み、それら作成済みネットワーク拡張の各々が、前記第１のネットワークアドレスが割当てられた前記作成済みネットワーク拡張の一部である別個のコンピューティングノードを持つ、第２１項に記載のコンピュータ可読媒体。

【０１２５】

第２３項。前記複数のリモート顧客の少なくとも１人の各々について、前記１つまたは複数のプログラムで行われた要求が、前記顧客の、前記顧客に対して表示されたグラフィカルユーザインタフェースとの１つまたは複数のやりとりに基づいて受信され、かつ、前記複数のリモート顧客の少なくともう１人の各々について、前記１つまたは複数のプログラムで行われた要求が、前記設定可能ネットワークサービスのプログラムによるインタフェースをプログラムで起動する前記顧客のコンピューティング装置上で実行しているソフトウェアから受信される、第２０項に記載のコンピュータ可読媒体。

【０１２６】

第２４項。前記方法が、１人または複数の前記複数のリモート顧客の各々について、

前記顧客用の前記作成済みネットワーク拡張から、前記作成済みネットワーク拡張および前記顧客の前記プライベートネットワークの外部にある資源サービスによって提供される１つまたは複数のコンピューティング関連資源へのアクセスを設定するための情報を取得することであって、前記情報が前記１つまたは複数のコンピューティング資源が関連付けられた前記資源サービス内の名前空間の識別子を含むことと、

前記作成済みネットワーク拡張を、前記顧客用に前記作成済みネットワーク拡張の前記複数のコンピューティングノードから、前記資源サービスで提供される前記１つまたは複数のコンピューティング関連資源へアクセスできるように自動的に設定することであって、前記設定が、前記１つまたは複数のコンピューティング関連資源にアクセスするため、前記作成済みネットワーク拡張から前記アクセス機構経由で前記資源サービスに送信された通信が、前記資源サービスで使用される前記名前空間識別子の指示を含むように自動的に変更されるような方法で、前記名前空間識別子を前記資源サービス用のアクセス機構と関連付けることと、

をさらに含む、第２０項に記載のコンピュータ可読媒体。

【０１２７】

第２５項。前記コンピュータ可読媒体が、前記内容および前記内容を含む生成された格納済みデータ信号を含むデータ送信媒体を格納するコンピューティングシステムのメモリの少なくとも１つであって、かつ、前記内容が、実行時に前記コンピューティングシステムに前記方法を実行させる命令である、第２０項に記載のコンピュータ可読媒体。

【０１２８】

第２６項。プライベートコンピュータネットワークへのアクセスを提供するように設定されたコンピューティングシステムであって、

１つまたは複数のメモリと、

リモートクライアントによる使用のために作成されたコンピュータネットワークを自動的に提供するように設定された設定可能ネットワークサービスマネージャモジュールと、を備え、前記設定可能ネットワークサービスマネージャモジュールが、複数のリモートクライアントの各々に対して、

前記クライアントによって使用するために作成されたコンピュータネットワークを設定するため、前記クライアントによってプログラムで提供される設定情報を受信することであって、前記設定情報が、前記クライアント用の前記作成済みコンピュータネットワークの一部として提供される複数のコンピューティングノードに関連する複数のネットワークアドレスの指示を含むことと、

前記受信された設定情報に従って前記クライアント用に前記作成済みコンピュータネッ

トワークの一部として提供される複数のコンピューティングノードを作成することであって、前記設定が、前記複数のネットワークアドレスの少なくとも１つの前記複数のコンピューティングの各々への関連付けを含み、前記複数のコンピューティングノードが、クライアントのコンピュータネットワークで使用可能な複数のコンピューティングノードから選択されていることと、

前記クライアント用に前記作成済みコンピュータネットワークからネットワークアクセス可能資源サービスによって提供されている１つまたは複数の資源へのアクセスを設定するための追加情報を取得することであって、前記追加情報が前記資源サービスによって前記１つまたは複数の資源に関連付けられる識別子を含むことと、

前記複数のコンピューティングノードから、前記識別子に関連付けられるような方法で、前記資源サービスによって提供される前記１つまたは複数の資源へアクセスできるように、前記クライアント用の前記作成済みコンピュータネットワークを自動的に設定して、前記１つまたは複数の資源にアクセスするために、前記作成済みプライベートネットワークから前記資源サービスに送信された通信が、前記資源サービスで使用される前記識別子の指示を含むようにすることと、

前記クライアントに前記作成済みコンピュータネットワークの前記複数のコンピュータノードへのアクセスを提供することと、

を実行する、

コンピューティングシステム。

【０１２９】

第２７項。前記設定可能ネットワークサービスマネージャモジュールが設定可能ネットワークサービスの一部であって、前記クライアントによる使用のために作成された前記コンピュータネットワークを設定するために、前記複数のリモートクライアントによる使用のためのプログラムによるインタフェースを提供し、前記作成済みコンピュータネットワークで使用可能な前記複数のコンピューティングノードが前記設定可能ネットワークサービスにより提供され、かつ前記複数のクライアントの少なくともいくつかの各々について、前記クライアントによりプログラムで提供される前記設定情報が、プログラムによるインタフェースを利用して提供され、前記クライアントによる使用のために設定されている前記作成済みコンピュータネットワーク用のネットワークトポロジ情報をさらに提供し、前記クライアントによる使用のために作成および設定されている前記コンピュータネットワークが、前記クライアントのリモートプライベートコンピュータネットワークへのプライベートコンピュータネットワーク拡張であって、さらに前記提供されるネットワークトポロジ情報に従って設定され、かつ、前記作成されたコンピュータネットワークの前記自動設定が、前記リモートプライベートコンピュータネットワークと前記プライベートコンピュータネットワーク拡張の複数のコンピューティングノードとの間のプライベートアクセスをさらに可能にする、第２６項に記載のコンピューティングシステム。

【０１３０】

第２８項。前記複数のクライアントの少なくともいくつかの各々について、前記クライアント用の前記作成済みコンピュータネットワーク用に設定されているアクセス先の前記１つまたは複数の資源を提供する前記ネットワークアクセス可能資源サービスが、前記作成済みコンピュータネットワークの一部でないリモート資源サービスであって、前記取得された追加情報に含まれる前記識別子が、前記リモート資源サービス内の前記クライアント用の名前空間に関連付けられた一意の識別子であって、前記クライアント用に前記作成済みコンピュータネットワークからアクセスされる前記１つまたは複数の資源が、前記クライアント用の前記関連する名前空間に格納され、かつ、前記識別子の前記指示を前記リモート資源サービスに送信された前記通信に含むための前記クライアント用に前記作成済みコンピュータネットワークの前記設定は、前記リモート資源サービスを表すための前記作成済みコンピュータネットワーク用の前記複数のネットワークアドレスの１つの割当てと、前記リモート資源サービスへ前記割当て済みネットワークアドレスを用いて送信された通信が、前記関連した名前空間の識別時に前記リモート資源サービスによる使用のため

に前記識別子を含むように変更されるような方法での前記識別子の前記割当て済みネットワークアドレスとの関連付けを含む、第２６項に記載のコンピューティングシステム。

【０１３１】

第２９項。前記設定可能ネットワークサービスマネージャモジュールが、前記コンピューティングシステムによる実行用のソフトウェア命令を含む、第２６項に記載のコンピューティングシステム。

【０１３２】

第３０項。

前記設定可能ネットワークサービスマネージャモジュールが、リモートクライアントによる使用のために作成されたコンピュータネットワークを自動的に提供するための方法から設定されるコンピューティングシステムであって、前記設定可能ネットワークサービスマネージャモジュールが、前記複数のリモートクライアントの各々に対して、

前記クライアントによる使用のために作成されたコンピュータネットワークを設定するため、前記クライアントによりプログラムで提供される設定情報を受信することであって、前記設定情報が、前記クライアント用に前記作成済みコンピュータネットワークの一部として提供される複数のコンピューティングノードに関連付けるための複数のネットワークアドレスの指示を含むことと、

前記受信された設定情報に従って前記クライアント用に前記作成済みコンピュータネットワークの一部として提供される複数のコンピューティングノードを設定することであって、前記設定が、前記複数のネットワークアドレスの少なくとも１つの前記複数のコンピューティングノードの各々との関連付けを含み、前記複数のコンピューティングノードが、クライアントのコンピュータネットワークで利用可能な複数のコンピューティングノードから選択されることと、

前記クライアント用に前記作成されたコンピュータネットワークから、ネットワークアクセス可能な資源サービスで提供される１つまたは複数の資源へのアクセスを設定するための追加情報を取得することであって、前記追加情報が、前記資源サービスによって前記１つまたは複数の資源に関連付けられた識別子を含むことと、

前記複数のコンピューティングノードから、前記資源サービスによって提供される前記１つまたは複数の資源へのアクセスを、前記識別子に関連付けられるような方法で可能にして、前記１つまたは複数の資源にアクセスするために前記作成済みプライベートネットワークから前記資源サービスに送信された通信が、前記資源サービスで使用される前記識別子の指示を含むようにするように、前記クライアント用の前記作成済みコンピュータネットワークを自動的に設定することと、

前記クライアントに前記作成済みコンピュータネットワークの前記複数のコンピューティングノードへのアクセスを提供することと、

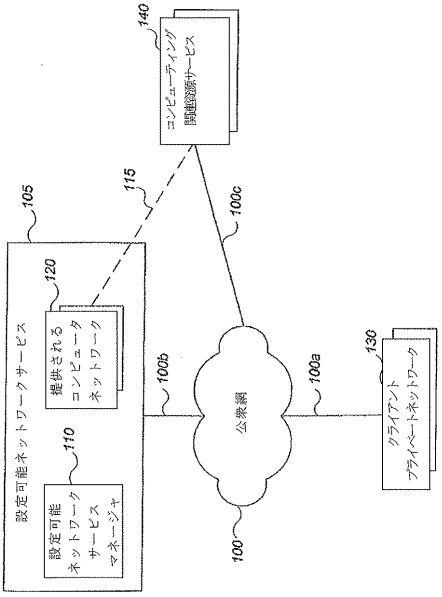
を実行する、

第２６項に記載のコンピューティングシステム。

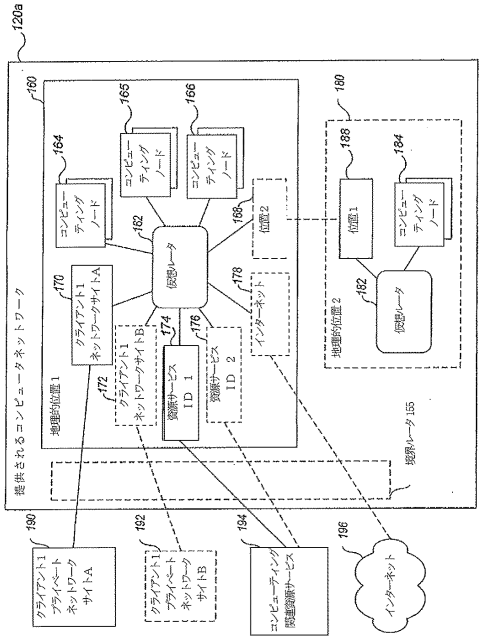
【０１３３】

前述の説明から、本明細書中に具体的な実施形態が例示の目的で記載されているが、本発明の精神および範囲から逸脱することなく種々の変更を行うことが可能であることが理解されよう。従って、本発明は、添付の特許請求の範囲および本明細書に列挙された要素によることを除いて、限定されるものではない。また、本発明のある態様がある請求項の形で以降に提示されているが、発明者は、本発明の種々の態様を利用可能ないかなる請求項の形でも考慮する。例えば、本発明の一部の態様のみがコンピュータ可読媒体で具体化されているとして現在列挙されているが、別の態様も同様にそのように具体化することが可能である。

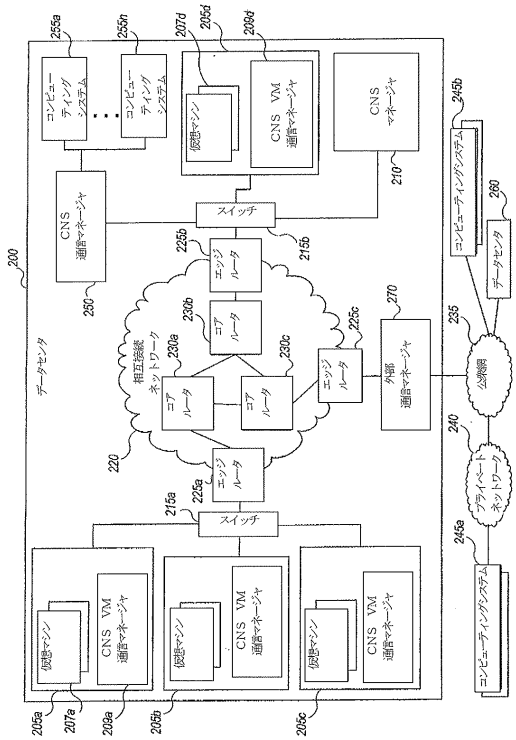
【図１Ａ】


140
コンピューティング関連資源サービス
105
115
100c
設定可能ネットワークサービス
120
提供されるコンピュータネットワーク
110
設定可能ネットワークサービスマネージャ
100b
100a
公衆網
130
クライアントプライベートネットワーク
100

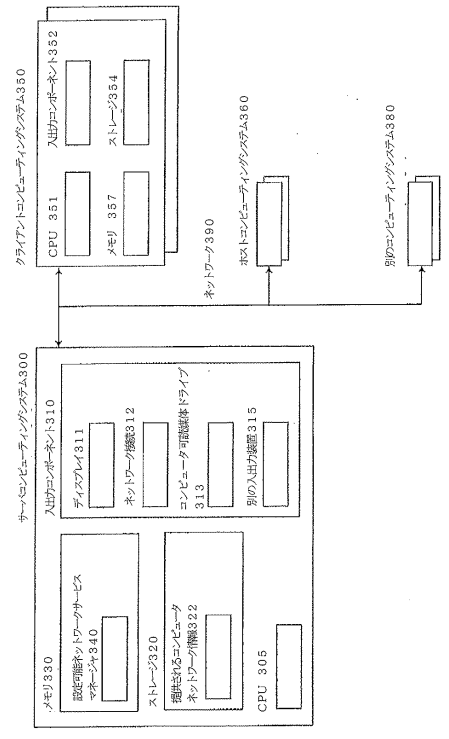
【図１Ｂ】


120a
160
提供されるコンピュータネットワーク
地理的位置1
164
コンピューティングノード
165
コンピューティングノード
166
コンピューティングノード
162
仮想ルータ
168
位置2
180
地理的位置2
188
位置1
184
コンピューティングノード
182
仮想ルータ
170
クライアント1ネットワークサイトA
172
クライアント1ネットワークサイトB
174
顧客サービスID 1
176
顧客サービスID 2
178
インターネット
境界ルータ155
190
クライアント1プライベートネットワークサイトA
192
クライアント1プライベートネットワークサイトB
194
コンピューティング関連資源サービス
196
インターネット

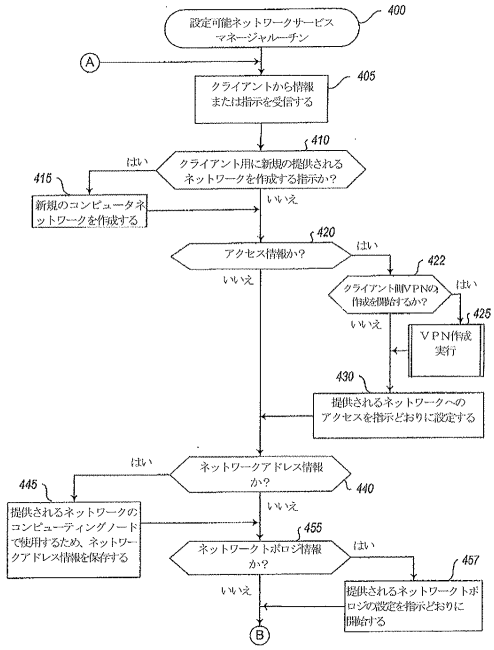
【図２】


データセンタ
200
コンピューティングシステム255a
コンピューティングシステム255n
仮想マシン207d
CNS VM通信マネージャ205d
208d
CNSマネージャ
210
CNS通信マネージャ250
スイッチ215b
エッジルータ225b
コアルータ230b
相互接続ネットワーク220
コアルータ230a
コアルータ230c
エッジルータ225c
外部通信マネージャ270
コンピューティングシステム245b
260
データセンタ
235
公衆網
240
プライベートネットワーク
スイッチ215a
エッジルータ225a
コンピューティングシステム245a
仮想マシン205a
CNS VM通信マネージャ207a
仮想マシン203a
CNS VM通信マネージャ205b
仮想マシン205c
CNS VM通信マネージャ

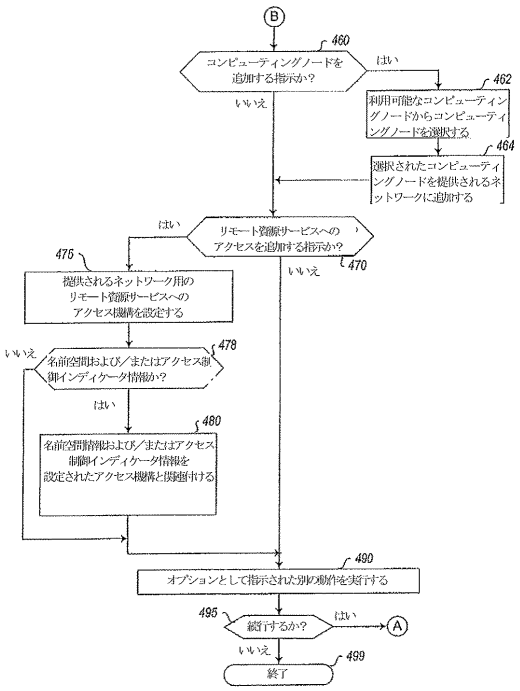
【図３】


クライアントコンピューティングシステム350
入出力コンポーネント352
CPU 351
メモリ 357
ストレージ354
ネットワーク390
ホストコンピューティングシステム360
別のコンピューティングシステム380
サーバコンピューティングシステム300
入出力コンポーネント310
ディスプレイ311
ネットワーク機器312
コンピュータ可読媒体ドライブ313
別の入出力装置315
メモリ330
設定可能ネットワークサービスマネージャ340
ストレージ320
通信されるコンピュータネットワーク情報322
CPU 305

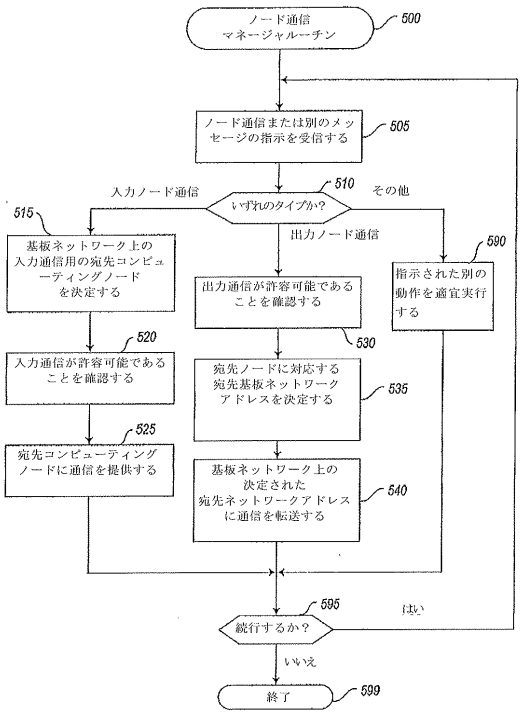
【図４Ａ】


設定可能ネットワークサービス
マネージャルーチン
400
A
クライアントから情報
または指示を受信する
405
クライアント用に新規の提供される
ネットワークを作成する指示か?
410
はい
新規のコンピュータネ
ットワークを作成する
415
いいえ
アクセス情報か?
420
はい
クライアント側VPNの
作成を開始するか?
422
はい
いいえ
VPN作成
実行
425
いいえ
提供されるネットワークへの
アクセスを指示どおりに設定する
430
ネットワークアドレス情報
か?
440
はい
提供されるネットワークの
コンピューティングノード
で使用するため、ネットワー
クアドレス情報を保存する
445
いいえ
ネットワークトポロジ情報
か?
455
はい
提供されるネットワークトポ
ロジの設定を指示どおりに
開始する
457
いいえ
B

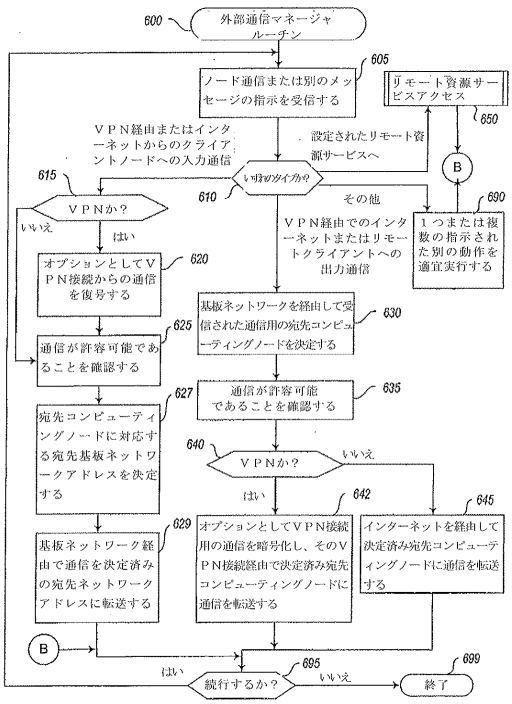
【図４Ｂ】


B
コンピューティングノードを
追加する指示か?
460
はい
利用可能なコンピューティン
グノードからコンピューティ
ングノードを選択する
462
選択されたコンピューティ
ングノードを提供されるネ
ットワークに追加する
464
いいえ
リモート資源サービスへの
アクセスを追加する指示か?
470
はい
提供されるネットワーク用の
リモート資源サービスへの
アクセス機構を設定する
475
いいえ
名前空間および/またはアクセス制
御インディケータ情報か?
478
いいえ
はい
名前空間情報および/またはアクセス
制御インディケータ情報を
設定されたアクセス機構と関連付ける
480
オプションとして指示された別の動作を実行する
490
続行するか?
495
はい
A
いいえ
終了
499

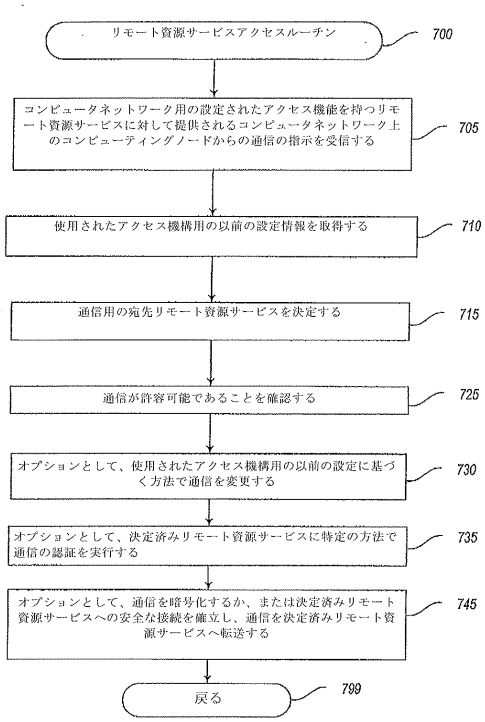
【図５】


ノード通信
マネージャルーチン
500
ノード通信または別のメッ
セージの指示を受信する
505
入力ノード通信
いずれのタイプか?
510
その他
出力ノード通信
515
基板ネットワーク上の
入力通信用の宛先コンピュ
ーティングノード
を決定する
指示された別の
動作を適宜実行
する
590
出力通信が許容可能である
ことを確認する
530
入力通信が許容可能であ
ることを確認する
520
宛先ノードに対応する
宛先基板ネットワーク
アドレスを決定する
535
宛先コンピューティング
ノードに通信を提供する
525
基板ネットワーク上の
決定された
宛先ネットワークアドレス
に通信を転送する
540
続行するか?
595
はい
いいえ
終了
599

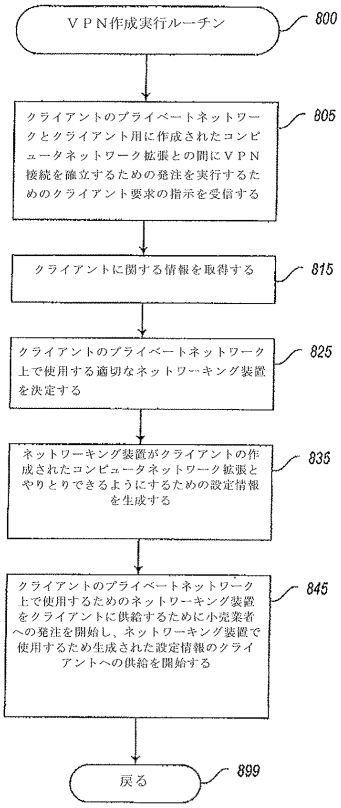
【図６】


600
外部通信マネージャ
ルーチン
ノード通信または別のメッ
セージの指示を受信する
605
リモート資源サー
ビスアクセス
650
VPN経由またはインタ
ーネットからのクライア
ントノードへの入力通信
設定されたリモート資
源サービスへ
B
いずれのタイプか?
610
615
その他
VPNか?
いいえ
はい
690
1つまたは複
数の指示され
た別の動作を
適宜実行する
VPN経由でのインタ
ーネットまたはリモー
トクライアントへの
出力通信
オプションとしてV
PN接続からの通信
を復号する
620
基板ネットワークを経由して受
信された通信用の宛先コンピュ
ーティングノードを決定する
630
通信が許容可能であ
ることを確認する
625
通信が許容可能
であることを確認する
635
宛先コンピューティ
ングノードに対応する宛先基板ネットワ
ークアドレスを決定
する
627
VPNか?
640
いいえ
はい
642
645
インターネットを経由して
決定済み宛先コンピューテ
ィングノードに通信を転送
する
オプションとしてVPN接続
用の通信を暗号化し、そのV
PN接続経由で決定済み宛先
コンピューティングノードに
通信を転送する
基板ネットワーク経
由で通信を決定済み
の宛先ネットワーク
アドレスに転送する
629
B
はい
695
699
続行するか?
いいえ
終了

【図７】


リモート資源サービスアクセスルーチン
700
コンピュータネットワーク用の設定されたアクセス機能を持つリモート資源サービスに対して提供されるコンピュータネットワーク上のコンピューティングノードからの通信の指示を受信する
705
使用されたアクセス機構用の以前の設定情報を取得する
710
通信用の宛先リモート資源サービスを決定する
715
通信が許容可能であることを確認する
725
オプションとして、使用されたアクセス機構用の以前の設定に基づく方法で通信を変更する
730
オプションとして、決定済みリモート資源サービスに特定の方法で通信の認証を実行する
735
オプションとして、通信を暗号化するか、または決定済みリモート資源サービスへの安全な接続を確立し、通信を決定済みリモート資源サービスへ転送する
745
戻る
799

【図８】


ＶＰＮ作成実行ルーチン
800
クライアントのプライベートネットワークとクライアント用に作成されたコンピュータネットワーク拡張との間にＶＰＮ接続を確立するための発注を実行するためのクライアント要求の指示を受信する
805
クライアントに関する情報を取得する
815
クライアントのプライベートネットワーク上で使用する適切なネットワーキング装置を決定する
825
ネットワーキング装置がクライアントの作成されたコンピュータネットワーク拡張とやりとりできるようにするための設定情報を生成する
835
クライアントのプライベートネットワーク上で使用するためのネットワーキング装置をクライアントに供給するために小売業者への発注を開始し、ネットワーキング装置で使用するため生成された設定情報のクライアントへの供給を開始する
845
戻る
899

フロントページの続き

(72)発明者 クラリッサ ローリー クック ブランドウィン
アメリカ合衆国 ９８１４４ ワシントン州 シアトル １２ アベニュー サウス １２００
スイート １２００
(72)発明者 ダニエル ティー. コーン
アメリカ合衆国 ９８１４４ ワシントン州 シアトル １２ アベニュー サウス １２００
スイート １２００
(72)発明者 アンドリュー ジェイ. ドーン
アメリカ合衆国 ９８１４４ ワシントン州 シアトル １２ アベニュー サウス １２００
スイート １２００
(72)発明者 カール ジェイ. モーゼス
アメリカ合衆国 ９８１４４ ワシントン州 シアトル １２ アベニュー サウス １２００
スイート １２００
(72)発明者 ステファン イー. シュミット
アメリカ合衆国 ９８１４４ ワシントン州 シアトル １２ アベニュー サウス １２００
スイート １２００

審査官 山田 倍司

(56)参考文献 米国特許出願公開第２００６／０２５３４５６（ＵＳ，Ａ１）
国際公開第２００７／１２６８３５（WO，Ａ２）
米国特許第７４５７８２４（ＵＳ，Ｂ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／００－１２／９５５