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

特許第6499276号
(P6499276)

(45)発行日　平成31年4月10日(2019.4.10)　(24)登録日　平成31年3月22日(2019.3.22)

(51)Int.Cl.　　F I
*H04L 12/749 (2013.01)*　　H04L 12/749
*H04L 12/70 (2013.01)*　　H04L 12/70　D

請求項の数 15　(全 36 頁)

(21)出願番号　特願2017-513782(P2017-513782)
(86)(22)出願日　平成27年9月18日(2015.9.18)
(65)公表番号　特表2017-529789(P2017-529789A)
(43)公表日　平成29年10月5日(2017.10.5)
(86)国際出願番号　PCT/US2015/051027
(87)国際公開番号　WO2016/044769
(87)国際公開日　平成28年3月24日(2016.3.24)
審査請求日　平成29年3月10日(2017.3.10)
(31)優先権主張番号　14/491,758
(32)優先日　平成26年9月19日(2014.9.19)
(33)優先権主張国　米国(US)

(73)特許権者　507303550
アマゾン・テクノロジーズ・インコーポレーテッド
アメリカ合衆国・９８１０８－１２２６・ワシントン州・シアトル・ピイオーボックス・８１２２６
(74)代理人　100098394
弁理士　山川　茂樹
(74)代理人　100064621
弁理士　山川　政樹
(72)発明者　ミラー，ケヴィン・クリストファー
アメリカ合衆国・９８１０９－５２１０・ワシントン州・シアトル・テリー　アヴェニュ　ノース・４１０

最終頁に続く

(54)【発明の名称】分離仮想ネットワークのためのプライベートエイリアスエンドポイント

(57)【特許請求の範囲】
【請求項１】
方法であって、
プロバイダネットワークのトンネリング手段で、第１のプライベートエイリアスエンドポイント（ＰＡＥ）が、クライアントの代わりに前記プロバイダネットワーク内に確立された第１の分離仮想ネットワーク（ＩＶＮ）で生じるトラフィックのためのルーティングターゲットとして指定されたと判断するステップであって、前記トラフィックが前記プロバイダネットワークに実装された特定の公にアクセス可能なサービスに送達されるステップと、
前記トンネリング手段で、前記第１のＩＶＮの第１の計算インスタンスから前記特定の公にアクセス可能なサービスの公に宣伝されたネットワークアドレスに向けられるベースラインパケットを受信するステップと、
前記トンネリング手段によって、（ａ）前記ベースラインパケットのコンテンツ、及び（ｂ）ソースＩＶＮとしての前記第１のＩＶＮの表示を備えるカプセル化パケットを前記特定のサービスの第１のノードに送信するステップと、
を含む、方法。
【請求項２】
前記カプセル化パケットがＩＰｖ６（インターネットプロトコルのバージョン６）に従ってフォーマットされ、前記ベースラインパケットがＩＰｖ４（前記インターネットプロトコルのバージョン４）に従ってフォーマットされる、請求項１に記載の方法。

【請求項３】
前記特定のサービスが複数のオブジェクトに対する複数の操作タイプをサポートし、
前記クライアントから前記第１のＩＶＮの構成マネージャで、前記第１のＰＡＥに第１のアクセス制御方針を適用する要求を受信するステップであって、前記第１のアクセス制御方針が、前記第１のＰＡＥを使用し、ルーティングターゲットとして提出される要求に関して、（ａ）前記複数の操作タイプの許可された操作タイプ、（ｂ）前記複数の操作タイプの禁止された操作タイプ、（ｃ）前記複数の操作タイプの内の特定の操作タイプが許可される時間間隔、または（ｄ）前記複数の操作タイプの内の特定の操作タイプが許可される前記複数のオブジェクトの内の特定のオブジェクトの内の１つまたは複数を示すステップと、
前記ベースラインパケットに示される特定の要求に従って第１の操作を実行する前に、前記第１の操作が前記第１のアクセス制御方針によって許可されることを検証するステップと、
をさらに含む、請求項１に記載の方法。
【請求項４】
前記第１のＩＶＮで生じる追加のトラフィックのルーティングターゲットとして第２のＰＡＥを指定することをさらに含み、前記追加のトラフィックが異なるサービスに送達される、請求項１に記載の方法。
【請求項５】
前記第１の計算インスタンスが前記クライアントの要求で該第１の計算インスタンスに割り当てられた特定のプライベートＩＰアドレスを有し、
前記クライアントの代わりに第２のＩＶＮを確立することであって、前記第２のＩＶＮが第２の計算インスタンスを含む、第２のＩＶＮを確立するステップと、
前記クライアントの要求で、前記第２の計算インスタンスに前記特定のプライベートＩＰアドレスを割り当てるステップと、
前記第２のＩＶＮで生じ、前記特定のサービスに向けられるトラフィックを送るために使用される第２のＰＡＥを確立するステップと、
前記トンネリング手段によって生成されるカプセル化ヘッダの調査に基づいて前記特定のサービスの特定のノードで、前記特定のノードで受信される特定のベースラインパケットが、前記特定のプライベートＩＰアドレスが割り当てられた前記第１の計算インスタンスで生成されたのか、それとも前記特定のプライベートＩＰアドレスが割り当てられた前記第２の計算インスタンスで生成されたのかを判断するステップと、
をさらに含む、請求項１に記載の方法。
【請求項６】
前記トンネリング手段において、（ａ）前記ベースラインパケットの前記コンテンツ、及び（ｂ）前記ソースＩＶＮとしての前記第１のＩＶＮの表示、を備えるカプセル化パケットを生成するステップをさらに含む、請求項１の方法。
【請求項７】
前記カプセル化パケットが、前記第１のＰＡＥの識別子の表現を含んだヘッダを含む、請求項１に記載の方法。
【請求項８】
プログラムインタフェースを介して前記プロバイダネットワークの構成マネージャで、前記第１のＰＡＥを生成する要求を前記クライアントから受信するステップと、
前記要求に応えて前記構成マネージャによって、前記第１のＰＡＥを表すメタデータエントリを記憶するステップと、
をさらに含む、請求項１に記載の方法。
【請求項９】
プログラムインタフェースを介して前記プロバイダネットワークの構成マネージャで、ＰＡＥを使用するアクセスのために異なるサービスを登録する要求を受信するステップと、

前記要求に応えて前記構成マネージャによって、特定のサービスが特定のＰＡＥとの関連付けのために前記クライアントによって選択できるサービスの集合体に前記異なるサービスを追加するステップと、
をさらに含む、請求項１に記載の方法。
【請求項１０】
前記異なるサービスが、前記プロバイダネットワークのリソースのセットを使用し、前記プロバイダネットワークの異なるクライアントによって実装され、
前記異なるサービスに向けられるベースラインパケットから引き出されるカプセル化パケットのコンテンツを抽出するように構成された特定のフロントエンドノードを含んだ、前記異なるサービスのために１つまたは複数のフロントエンドノードを確立するステップ、
をさらに含む、請求項９に記載の方法。
【請求項１１】
システムであって、
１つまたは複数のメモリを含んだ１つまたは複数のコンピュータシステムであって、前記１つまたは複数のメモリが、実行時に前記システムに、
クライアントの代わりにプロバイダネットワーク内に確立された第１の分離仮想ネットワーク（ＩＶＮ）からプロバイダネットワークに実装された特定のサービスに向けられるトラフィックのルーティングターゲットとしての第１のプライベートエイリアスエンドポイント（ＰＡＥ）の指定に従って、前記第１のＩＶＮの第１の計算インスタンスで生成されたベースラインパケットを前記プロバイダネットワークに実装された前記特定のサービスで受信させ、前記ベースラインパケットが前記特定のサービスのパブリックＩＰ（インターネットプロトコル）アドレスをその宛先アドレスとして示し、
選択されたトンネリングプロトコルに従って、（ａ）前記ベースラインパケットのコンテンツの少なくとも一部分、及び（ｂ）ソースＩＶＮとして前記第１のＩＶＮを示すヘッダ構成要素を備える第１のカプセル化パケットを生成させ、
前記特定のサービスの第１のノードに前記第１のカプセル化パケットを送信させる
前記システム。
【請求項１２】
前記第１のカプセル化パケットがＩＰｖ６（前記インターネットプロトコルのバージョン６）に従ってフォーマットされ、前記ベースラインパケットがＩＰｖ４（前記インターネットプロトコルのバージョン４）に従ってフォーマットされる、請求項１１に記載のシステム。
【請求項１３】
前記１つまたは複数のメモリが、実行時、前記システムに、
第１のＩＶＮとは異なるサービスに向けられるトラフィックのルーティングターゲットとして第２のＰＡＥの指定に従って、前記第１のＩＶＮの第２の計算インスタンスで生成される第２のベースラインパケットの表現を受信させ、前記第２のベースラインパケットが前記異なるサービスのパブリックＩＰアドレスをその宛先アドレスとして示し、
前記選択されたトンネリングプロトコルに従って、（ａ）前記第２のベースラインパケットのコンテンツの少なくとも一部分、及び（ｂ）ソースＩＶＮとして前記第１のＩＶＮを示すヘッダ構成要素を備える第２のカプセル化パケットを生成させ、
前記異なるサービスの異なるノードに前記第２のカプセル化パケットを送信させる、
請求項１１に記載のシステム。
【請求項１４】
前記第１のカプセル化パケットが前記第１の計算インスタンスのプライベートＩＰアドレスの表示を含み、前記１つまたは複数のメモリが、実行時に前記システムに、
前記クライアントに代わって確立された第２のＩＶＮから前記特定のサービスに向けられるトラフィックのルーティングターゲットとしての第２のＰＡＥの指定に従って、前記第２のＩＶＮの第２の計算インスタンスで生成された第２のベースラインパケットの表

現を受信させ、前記第２のベースラインパケットが前記特定のサービスの前記パブリックＩＰアドレスをその宛先アドレスとして示し、
前記選択されたトンネリングプロトコルに従って、（ａ）前記第２のベースラインパケットのコンテンツの少なくとも一部分、（ｂ）ソースＩＶＮとして前記第２のＩＶＮを示すヘッダ構成要素、及び（ｃ）前記プライベートＩＰアドレスの表示を備える第２のカプセル化パケットを生成させ、
前記特定のサービスの前記第１のノードに前記第２のカプセル化パケットを送信させ、前記特定のサービスの前記第１のノードが、前記第２のカプセル化パケットの調査に基づき、前記第２のベースラインパケットが前記第１の計算インスタンスで生成されたのか、それとも前記第２の計算インスタンスで生成されたのかを判断するように構成される、請求項１１に記載のシステム。
【請求項１５】
前記第１のカプセル化パケットが、前記第１のＰＡＥの識別子の表現を含んだヘッダを含む、請求項１１に記載のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
多くの企業及び他の組織は、多数のコンピューティングシステムをその動作をサポートするために相互接続するコンピュータネットワークを操作し、例えばコンピューティングシステムは（例えばローカルネットワークの一部として）同一場所に配置されているか、または代わりに（例えば、１つまたは複数のプライベート中間ネットワークもしくはパブリック中間ネットワークを介して接続される）複数の異なる地理的な位置に位置している。例えば、単一の組織によって及び単一の組織に代わって運営されるプライベートデータセンタ、及びカスタマにコンピューティングリソースを提供するための事業としてエンティティによって運営されるパブリックデータセンタ等、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するデータセンタが一般的になっている。
【０００２】
いくつかのプロバイダは、プロバイダのカスタマが係るデータセンタに位置するリソースを使用し、論理的に分離されたネットワークを作成することを許している。例えば、カスタマはプロバイダによって管理されるホストで実装される仮想化されたサーバ及び／または他のリソースのいくつかのセットを割り当てられてよく、カスタマはリソースのネットワーキング構成に関して相当な柔軟性を与えられてよい。カスタマは、例えばサーバに対するＩＰ（インターネットプロトコル）アドレスを選択するか、好みのサブネットを定義する等を行ってよい。プロバイダのリソースを使用し、実装される係るカスタマ構成可能なネットワークは、「分離仮想ネットワーク」または「仮想プライベートクラウド」を含むさまざまな名前で呼ばれることがある。いくつかの状況では、カスタマは、例えば分離仮想ネットワークの外のリソースに関してアドレスの一意性について懸念する必要なく、分離仮想ネットワークの中のいくつかのリソースにプライベートＩＰアドレス（つまり、分離仮想ネットワークの外で可視ではないまたは宣伝されないアドレス）を割り当ててよい。プロバイダは係る環境での高レベルのセキュリティ、ネットワーク分離、及び可用性をサポートし、カスタマが分離仮想ネットワークでビジネスに不可欠なアプリケーションを実行し、カスタマによって所有される構内で達成可能なサービスの質に類似する（またはさらに高い）サービスの質を経験できるようにする。
【０００３】
分離仮想ネットワークをサポートする少なくともいくつかのプロバイダは、ストレージサービス、データベースサービス等のさまざまな他のサービスを実装してもよい。これらの他のサービスのいくつかは、公衆インターネットからアクセス可能となるように設計されてよい‐例えば、公に宣伝されたＩＰアドレスまたは対応するＵＲＩ（ユニフォームリソースアイデンティファイア）のセットが、クライアントが係るサービスのリソースにアクセスするためにセットアップされてよい。少なくともいくつかの環境では、潜在的にセ

キュリティを弱めずに、または相当なコストを生じさせずにどちらかでこのようにすることは、きわめて安全な分離仮想ネットワークの中から係る公に宣伝されたサービスにアクセスすることを希望するカスタマにとって容易ではないことがある。

【０００４】

実施形態はいくつかの実施形態及び例示的な図面について例として本明細書に説明されているが、当業者は、実施形態が説明される実施形態または図面に制限されないことを認識する。図面及び図面に対する発明を実施するための形態が開示される特定な形式に実施形態を制限することを目的するのではなく、逆に、意図は添付される特許請求の範囲により定められる精神及び範囲に入るすべての変更形態、同等物、及び代替策をカバーすることであることが理解されるべきである。本明細書で使用される見出しは構成上の目的のためだけであり、本明細書または特許請求の範囲の範囲を制限するために使用されることを意図されていない。本願を通して使用されるように、単語「ｍａｙ（～してよい）」は、強制的な意味（つまり、しなければならないを意味する）よりもむしろ、許可の意味（つまり、する可能性を有することを意味する）で使用される。同様に、単語「ｉｎｃｌｕｄｅ（含む）」、「ｉｎｃｌｕｄｉｎｇ（含んだ）」、及び「ｉｎｃｌｕｄｅｓ（含む）」は、を含むがこれに限定されるものではないことを意味する。

【図面の簡単な説明】

【０００５】

【図１】少なくともいくつかの実施形態に従って、プライベートエイリアスエンドポイント（ＰＡＥ）が、プロバイダネットワークの分離仮想ネットワーク（ＩＶＮ）と１つまたは複数の公にアクセス可能なサービスとの間のネットワークトラフィックのルーティングを、ＩＶＮでパブリックＩＰアドレスを割り当てることなく、及びカスタマネットワークを横断することなく可能にするために確立されてよい、実施例のシステム環境を示す図である。

【図２】少なくともいくつかの実施形態に従って、分離仮想ネットワークの計算インスタンスで生じるパケットを、公にアクセス可能なサービスの宛先に向けることに関与する実施例の構成要素を示す図である。

【図３ａ】少なくともいくつかの実施形態に従って、分離仮想ネットワークの計算インスタンスで生じるパケットを処理してよい代替のサービス側構成要素のそれぞれの実施例を示す図である。

【図３ｂ】少なくともいくつかの実施形態に従って、分離仮想ネットワークの計算インスタンスで生じるパケットを処理してよい代替のサービス側構成要素のそれぞれの実施例を示す図である。

【図４】少なくともいくつかの実施形態に従って、計算インスタンスで生じるベースラインパケットのためのカプセル化フォーマットの実施例を示す図である。

【図５】少なくともいくつかの実施形態に従って、ＰＡＥ構成要求及びＰＡＥ構成応答の実施例を示す図である。

【図６】少なくともいくつかの実施形態に従って、ＰＡＥ構成データベースコンテンツの実施例を示す図である。

【図７】少なくともいくつかの実施形態に従って、同じプライベートＩＰアドレスを有する計算インスタンスからサービスで受信される要求を区別するためのＩＶＮ識別子及びＰＡＥ識別子の使用の実施例を示す図である。

【図８】少なくともいくつかの実施形態に従って、ＰＡＥを構成するために実行されてよい操作の態様を示す流れ図である。

【図９】少なくともいくつかの実施形態に従って、計算インスタンスから公にアクセス可能なサービスにパケットを送信するためのトンネリングプロトコルの使用を示す流れ図である。

【図１０】少なくともいくつかの実施形態で使用されてよい実施例のコンピューティング装置を示すブロック図である。

【発明を実施するための形態】

【０００６】
プロバイダネットワークでプライベートエイリアスエンドポイント（ＰＡＥ）をサポートするための方法及び装置の多様な実施形態が説明される。インターネット及び／または他のネットワークを介してクライアントの分散されたセットにアクセス可能な（多様なタイプのマルチテナント及び／またはシングルテナントのクラウドベースのコンピューティングサービスもしくはストレージサービス等の）１つまたは複数のサービスを提供するために企業または公共部門の組織等のエンティティによってセットアップされるネットワークは、本明細書ではプロバイダネットワークと称されることがある。また、少なくともいくつかのプロバイダネットワークは「パブリッククラウド」環境と呼ばれることもある。所与のプロバイダネットワークは、プロバイダによって提供されるインフラ及びサービスを実装する、構成する、及び分散するために必要とされる、物理コンピュータサーバ及び／または仮想化されたコンピュータサーバ、ストレージデバイス、ネットワーキング装置等の集合体等の多様なリソースプールをホストする多数のデータセンタを含んでよい。少なくともいくつかの実施形態では、プロバイダネットワークで実装される仮想コンピューティングサービスは、クライアントがクライアントのアプリケーションのために（本明細書では「コンピュータインスタンス」または単に「インスタンス」と呼ばれることがある）１台または複数のゲスト仮想機械を活用できるようにしてよく、１つまたは複数の計算インスタンスは大きな一群のインスタンスホストの内のインスタンスホストで実行されている。大きいプロバイダネットワークの中で、いくつかのデータセンタは他とは異なる都市、州、または国に位置してよく、いくつかの実施形態では、所与のアプリケーションに配分されるリソースは、所望されるレベルの可用性、障害耐性、及び性能を達成するためにいくつかの係る場所の間で分散されてよい。

【０００７】
少なくともいくつかの実施形態では、プロバイダネットワークは、カスタマがプロバイダのデータセンタでの「分離仮想ネットワーク」（ＩＶＮ）の確立を要求できるようにしてよい。（いくつかの環境では「仮想プライベートクラウド」つまりＶＰＣと呼ばれることもある）ＩＶＮは、カスタマがネットワーキング構成に関して相当な制御を与えられる、プロバイダネットワークの論理的に分離された部分でコンピューティングリソース及び／または他のリソースの集合体を含んでよい。いくつかの実施形態では、例えば、カスタマは、多様な計算インスタンス等のＩＶＮリソースのために使用されるＩＰ（インターネットプロトコル）アドレスの範囲を選択し、ＩＶＮの中でのサブネットの作成、及びＩＶＮのためのルートテーブル等の構成を管理してよい。いくつかの実施形態でのＩＶＮの中のデバイスの少なくともいくつかの場合、ＩＰアドレスは少なくともデフォルトによってＩＶＮの外では可視ではないことがある。ＢＧＢ（ボーダゲートウェイプロトコル）または他の類似したプロトコルを介して公衆インターネット上で直接的にまたは間接的に宣伝された結果として公衆インターネットからアクセス可能である「パブリック」ＩＰアドレスとは対照的に、係るＩＰアドレスは本明細書では「プライベート」ＩＰアドレスと呼ばれることがある。プライベートアドレスの使用は、クライアントが例えばインターネットから発する潜在的な攻撃からクライアントのアプリケーションを保護できるようにしてよい。ＩＶＮサポートは、いくつかの実施形態ではプロバイダネットワークのより一般的な仮想コンピューティングサービス（ＶＣＳ）の特徴の１つであってよい。例えば、ＶＣＳは、ＩＶＮの一部ではなく、（インスタンスが配分されるクライアントよりもむしろ）ＶＣＳが、必要とされるネットワーキング構成の多くまたはすべてを実行するコンピュータインスタンスの予約または配分をサポートしてもよい。

【０００８】
１つまたは複数のストレージサービスまたはデータベースサービス等のプロバイダネットワークで実装されるサービスの少なくともいくつかは公にアクセス可能であってよい。すなわち、サービスにアクセスするために使用できるＩＰアドレス（または対応するホスト名／ＵＲＩ）のなんらかのセットは公に宣伝されることがあり、したがってクライアントは、インターネットに対する接続性を有するデバイスから係るサービスに対するサービ

ス要求を提出できてよい。例えば、「ＳｖｃＸ」と名付けられるストレージサービスは、［https://SvcX.<providername>.com］等の公に宣伝されたＵＲＩを介してクライアントによってアクセス可能であってよく、係るサーバのＩＰアドレスは１つまたは複数のドメインネームサービス（ＤＮＳ）サーバから入手されてよい。

【０００９】

クライアントの代わりにＩＶＮの中で実行されるいくつかのアプリケーションは、係る公にアクセス可能なサービスへのアクセスを必要とすることがある。例えば、ＩＶＮ内のクライアントの計算インスタンスで実行中のｅ－コマースアプリケーションは、データを読み取るまたはプロバイダネットワークの公にアクセス可能なストレージサービスに書き込む必要がある場合がある。公にアクセス可能なサービスに対する接続性を確立するある方法は、ＩＶＮの中のリソースに１つまたは複数のパブリックＩＰアドレスを割り当てること（及び／またはＩＶＮにインターネットでアクセス可能なゲートウェイをセットアップすること）を伴ってよく、このことはＩＶＮクライアントの分離要件及びセキュリティ要件にいくぶん反する慣行である場合がある。ＩＶＮで実行中の計算インスタンスと公にアクセス可能なサービスのリソースとの間で接続性を確立する別の方法は、ＩＶＮとカスタマネットワークとの間でＶＰＮ（仮想プライベートネットワーク）を最初に確立し、次にカスタマネットワークを介してＩＶＮから公にアクセス可能なサービスに間接的にトラフィックを送信することであってよい。ただし、少なくともいくつかの環境では、係るＶＰＮをベースにした接続性はきわめて高価であり、トラフィックに使用される間接的な経路は必ずしも（エンドツーエンド待ち時間に関して）クライアントアプリケーションの要件を満たすほど十分早くない可能性がある。

【００１０】

したがって、ＩＶＮリソースと少なくともいくつかの公にアクセス可能なサービスとの間での効率的な接続性を容易にするために、いくつかの実施形態では、プロバイダネットワーク事業者はＩＶＮのためのプライベートエイリアスエンドポイントの確立をサポートしてよい。名前が暗示するように、ＰＡＥは公にアクセス可能なサービスを表す「仮想」エンドポイントとしての機能を果たしてよく、ＰＡＥは、その使用がＩＶＮの中の任意のエンティティへのパブリックネットワークアドレスの割当てを必要としない「個人用」であってよい。また、ＰＡＥは、いくつかの環境では「仮想プライベートエンドポイント」と呼ばれることもある。少なくともいくつかの実施形態では、ＰＡＥは、クライアントの代わりにセットアップされたＩＶＮの中で実行中のアプリケーションが、例えば、公衆インターネットにＩＶＮをさらす必要なく、及びプロバイダネットワークの外のネットワークリンクを横断することなくプロバイダネットワークの中の他の場所に実装される公にアクセス可能なサービスにサービス要求を送信（及び公にアクセス可能なサービスから応答を受信）できるようにしてよい。トンネリングプロトコルは、公にアクセス可能なサービスが実装されるプロバイダネットワークの部分への伝送のためのＩＶＮで生じるトラフィックのパケットをカプセル化するために、以下に説明されるように使用されてよい。ＩＶＮで実行中のクライアントアプリケーションも、クライアントサービス要求を実装する公にアクセス可能なサービスのリソースも、多様な実施形態で必ずしもトンネリングプロトコルの使用を認識させられる必要はない。すなわち、係る実施形態では、クライアントアプリケーションに対する、またはサービスリソースでクライアント要求にサービスを提供することに関与する論理に対する変更は必要とされないことがある。

【００１１】

少なくとも１つの実施形態では、ＰＡＥの確立は、クライアントによって実行されるＩＶＮネットワーキング構成の他の態様に通常必要とされるステップの種類に使用しやすさにおいて非常に類似するＩＶＮ構成のいくつかの追加のステップをクライアントが実行することを伴ってよい。クライアントは、例えば、プログラム管理／処理インタフェース（例えば、コンソールまたはアプリケーションプログラミングインタフェース（ＡＰＩ））を介してＩＶＮのためのＰＡＥの作成を要求し、次いでユーザフレンドリなサービス名によって識別される選択されたサービスにＰＡＥを関連付けてよい。クライアントは、次い

で、宛先がいくつかの実施形態では公にアクセス可能なサービスの任意のノードまたはリソースであるトラフィックのターゲットとして、例えばＩＶＮの１つまたは複数のサブネットのためにセットアップされたルートテーブルでＰＡＥを指定してよい。いくつかの実施態様では、（サービス名「Ｓｖｃ１」のような）一般的なエイリアスはルートテーブルの宛先としてサービスを示すために使用されてよく、ＰＡＥに割り当てられた識別子はターゲットとして示されてよい。係る実施態様では、クライアントは、宛先を指定するときにサービスのいずれのＩＰアドレスを特定する必要はないことがある。少なくともいくつかの実施形態では、クライアントは、例えばＩＶＮの外で実装されるいくつかの異なるサービスへのアクセスを可能にするために、所与のＩＶＮでいくつかの異なるＰＡＥをセットアップしてよい。

【００１２】

ＰＡＥが特定のＩＶＮからのサービス向けのトラフィックのターゲットとして構成され、示された後、ＩＶＮの計算インスタンス（計算インスタンスがプライベートＩＰアドレスを割り当てられ、パブリックＩＰアドレスは割り当てられない）で実行中のクライアントアプリケーションはサービスに要求を、係る要求がインターネットで接続されるデバイスから発行されるのと同様に発行してよい。経てば、ＤＮＳ要求はサービスのパブリックＩＰアドレスを入手するために計算インスタンスから（例えばプロバイダネットワークのＤＮＳサーバに）発行されてよい。アプリケーションは、サービスのパブリックＩＰアドレスを宛先として、インスタンスのプライベートＩＰアドレスをソースとする１つまたは複数のベースラインパケットに、オペレーティングシステムまたは計算インスタンスの他の構成要素によって変換されてよいウェブサービスＡＰＩ（またはサービスによってサポートされる任意の類似するプログラムインタフェース）を使用し、サービス要求を提出してよい。

【００１３】

上述されたように、計算インスタンスはインスタンスホストで実行中のゲスト仮想機械として実装されてよい。少なくともいくつかの実施形態では、インスタンスホストは、ハイパーバイザ及び／または（多くの場合「ｄｏｍ－０」つまりドメインゼロインスタンスと称される）特権をもつオペレーティングシステムインスタンス等、仮想化管理ソフトウェアスタックの多様な構成要素を含んでよい。（本明細書ではＶＭＣと呼ばれることがある）係る仮想化管理構成要素は、ゲスト仮想機械で発行されるリソース要求を、ハードウェアリソースで実行される物理的な操作に変換することを担ってよい。一実施形態では、インスタンスホストで実行中のＶＭＣは計算インスタンスから発行されるベースラインパケットを妨害してよく、ＶＭＣは、ベースラインパケットが、インスタンス化されたホストがアタッチされる物理ネットワーク上での伝送のためにどのようにして変換される必要があるのか（または変換されるかどうか）を判断することを担ってよい。いくつかの実施態様では、ＶＭＣは、サービスに向けられたトラフィックのためのターゲットとしてのＰＡＥの選択を示すＩＶＮメタデータレコードにアクセスできてよく、サービスのパブリックＩＰアドレスのリストにアクセスできてもよい。したがって、ＶＭＣは、妨害されたベースラインパケットがＰＡＥと関連付けられたサービスに送信されると判断できてよい。

【００１４】

少なくともいくつかの実施形態では、（ＩＶＮが構成される仮想コンピューティングサービス、及びＰＡＥに割り当てられた宛先サービスを含んだ）多様なサービスは、プロバイダネットワークのそれぞれの論理的に別個の部分に割り当てられてよい。所与のサービスの対の間のトラフィックは、ソースサービスから宛先サービスに到達するために（ボーダネットワークと呼ばれることもある）ブリッジネットワークを横断する必要がある場合がある。また、係るブリッジネットワークは、まさにソースサービスネットワーク及び宛先サービスネットワークがプロバイダネットワークのサブネットと見なされてよいのと同様に、プロバイダネットワークの特殊目的サブネットと見なされてもよい。名前が暗示するように、ブリッジネットワークは、プロバイダネットワークの多様な論理的に別個の部分の間の中間ネットワーク（及び、いくつかの場合には、プロバイダネットワークと外部

ネットワークとの間の手段）として機能してよい。ＶＭＣは、宛先サービスに達するために横断されなければならないブリッジネットワークへ直接アクセスできないことがあり、したがって係るブリッジネットワークへパケットを送ることができる手段の使用を必要とすることがある。その結果、少なくともいくつかの実施形態では、ＶＭＣは、例えば、パケットの第１のカプセル化されたバージョンでトンネリング手段にベースラインパケットのコンテンツを送達してよい。この第１のカプセル化パケットは、次いでトンネリング手段によって選択されたトンネリングプロトコルに従って変換されてよく、パケットの第２のカプセル化バージョンはブリッジネットワーク経路またはトンネルを介して宛先サービスのノードに送信されてよい。さまざまな異なるカプセル化手法のいずれかが、多様な実施形態でのカプセル化のどちらの段階にも使用されてよい。カプセル化技法のいくつかの特定の例は以下にさらに詳細に説明される。

【００１５】

一実施形態では、トンネリング手段によって追加される１つまたは複数のヘッダはソースＩＶＮの符号化もしくは表示及び／または宛先サービスと関連付けられたＰＡＥを含んでよい。一実施態様では、例えば、トンネリングプロトコルは、ＩＰｖ６アドレスビットのいくつかがＩＶＮ識別子及び／またはＰＡＥ識別子を符号化するために使用されるＩＰｖ６互換パケットフォーマットの中でのＩＰｖ４ベースラインパケットのカプセル化を伴ってよい。宛先サービスでは、（例えば、サービス要求、及びソース計算インスタンスのプライベートＩＰアドレスを含んだ）ベースラインパケットのコンテンツが、ＩＶＮ及び／またはＰＡＥの識別子とともにカプセル化されたバージョンから抽出されてよい。いくつかの実施形態では、ＩＶＮ識別子またはＰＡＥの識別子は、以下にさらに詳細に説明されるように、同じプライベートＩＰアドレスが割り当てられた可能性のある（異なるＩＶＮでの）ソース計算インスタンスを区別する際に役立つことがある。ベースラインパケット本体に示される要求された操作が実行されてよく、応答は、例えば逆方向での類似したタイプのトンネリング技法及びカプセル化技法を使用し、ソースインスタンスでの要求側アプリケーションに返されてよい。

【００１６】

クライアントは、例えば上述された管理プログラムインタフェースの種類を使用し、少なくともいくつかの実施形態でＰＡＥにアクセス制御方針を適用できてよい。アクセス制御方針は、例えば、許可される（または禁止される）操作またはサービス要求のタイプ、操作が許可される／禁止されるオブジェクト（例えば、ストレージ関連サービスでのファイルまたはディレクトリ）、方針が適用する期間（例えば、作業日の特定の時間）、方針が適用する本人（例えば、特定のユーザーまたはグループ）等を示してよい。係る方針がＰＡＥに割り当てられるいくつかの実施形態では、サービスでのカプセル化パケットから抽出される要求は、要求が適用可能な方針に違反していないことを確実にするために確認されてよい。他の実施形態では、潜在的な方針違反は、宛先サービスで確認される代わりに、または宛先サービスで確認されることに加えてＩＶＮ側で確認されてよい‐例えば、ＶＭＣは、要求が使用されるＰＡＥと関連付けられた方針に違反すると判断される場合、要求の送信をアボートしてよい。

【００１７】

一実施形態では、ＰＡＥは、ＩＶＮと、プロバイダネットワークによって実装されるサービスとの間で単にパケットを送るためだけではなく、ＩＶＮと、プロバイダネットワークの他の場所で実装されるサードパーティサービスとの間でパケットを送るためにも使用されてよい。係る実施形態では、サードパーティ（例えば、プロバイダネットワークの仮想コンピューティングサービスの別のカスタマ）は、プロバイダネットワークリソースのなんらかのセットを使用し、サービスをセットアップし、サービスにアクセスできるパブリックＩＰアドレスを宣伝してよい。サードパーティプロバイダは、例えばプロバイダネットワークの構成マネージャに要求を提出することによってＰＡＥアクセスのためにサードパーティプロバイダのサービスを登録してよい。構成マネージャは、候補サードパーティサービスが、ＰＡＥがターゲットとして示されるルートを介するアクセスをサポートで

きることを検証してよい。例えば、構成マネージャは、いくつかの実施形態では、サードパーティサービスに（インテリジェントロードバランサ等の）トンネリングプロトコルを実装できるフロントエンドノードの割当てを開始してよい。他の実施形態では、サードパーティサービス事業者がトンネリングプロトコルを実装することを目的とするノードをすでにセットアップしている場合、係るノードの能力が検証されてよい。サードパーティサービスが登録され、トンネリングプロトコルに従ってパケットを抽出し（カプセル開放を行い）、カプセル化できるフロントエンドノードがセットアップされた後に、クライアントはサードパーティサービスにアクセスするようにクライアントのＩＶＮのＰＡＥを構成してよい。例えば、サードパーティサービスでの名前またはエイリアス（例えば、「ＴｈｉｒｄＰａｒｔｙＳｖｃ１」）は、プログラムインタフェースを使用してクライアントによってＰＡＥと関連付けることができるサービス宛先オプションのリスト（例えば、ＰＡＥサポートのためにすでに構成されている公にアクセス可能なサービスを表す「ＳｔｏｒａｇｅＳｖｃ１」、「ＤＢＳｖｃ１」等）に追加されてよい。

【００１８】

例のシステム環境

図１は、少なくともいくつかの実施形態に従って、プライベートエイリアスエンドポイント（ＰＡＥ）がプロバイダネットワークの分離仮想ネットワーク（ＩＶＮ）と１つまたは複数の公にアクセス可能なサービスとの間のネットワークトラフィックのルーティングを、ＩＶＮでのパブリックＩＰアドレスを割り当てることなく、及びカスタマネットワークを横断することなく可能にするために確立されてよい、実施例のシステム環境を示す。示されるように、システム１００は、仮想コンピューティングサービス（ＶＣＳ）及び公にアクセス可能なサービスＳｖｃ１（つまり、そのクライアントが公に宣伝されたＩＰアドレスまたはＵＲＩを介して要求を提出できるようにするサービス）を含んだ複数のサービスが実装されるプロバイダネットワーク１０２を含む。公にアクセス可能なサービスＳｖｃ１は、例えば任意の大きさに作られたストレージオブジェクトへウェブサービスベースのアクセスを提供するストレージサービス、非リレーショナルデータベースサービス、リレーショナルデータベースサービス、通知サービス、メッセージ待ち行列サービス、またはさまざまな他のタイプのサービスのいずれかを含んでよい。これらのサービスのそれぞれは、例えば独自の管理層または制御プレーンと、プロバイダネットワークの論理的に別々の部分を集合的に形成する、複数のホスト、ストレージデバイス、及び他のコンピューティング設備を含んでよい。例えば図１では、ＶＣＳのリソースはＶＣＳネットワーク１０４の中に位置する。一方、Ｓｖｃ１のリソースはＳｖｃ１ネットワーク１７０の中に位置する。

【００１９】

ＶＣＳネットワーク１０４の中で、ＩＶＮ１１０Ａ及びＩＶＮ１１０Ｂ等のいくつかの異なる分離仮想ネットワーク（ＩＶＮ）１１０が多様なクライアントの代わりに確立されてよい。その代わりに所与のＩＶＮ１１０が確立されるクライアントは、ＩＶＮのネットワーキング構成に関して相当な柔軟性を与えられてよい‐例えば、クライアントは、ＩＰアドレスがＩＶＮの外での使用で他と重複しないことを確実にする必要なく多様な計算インスタンス１１２に所望されるＩＰアドレスを割り当て、サブネットをセットアップし、ルートテーブルをポピュレートする等してよい。示されるように、各ＩＶＮは、ＩＶＮ１１０ＡのＩＨ　１３０Ａ及び１３０Ｂ、並びにＩＶＭ１１０ＢのＩＨ　１３０Ｍ及び１３０Ｎ等の複数のインスタンスホスト（ＩＨ）１３０を含んでよい。１つまたは複数の計算インスタンス（ＣＩ）１１２は、ＩＨ　１３０ＡでのＣＨ　１１２Ａ、ＩＨ　１３０ＢでのＣＩ　１１２Ｂ、ＩＨ　１３０ＭでのＣＩ　１１２Ｋ、及びＩＨ　１３０ＮでのＣＩ　１１２Ｌ等の各ＩＨ　１３０でインスタンス化されてよい。計算インスタンスのそれぞれは１つまたは複数のクライアントアプリケーションまたはアプリケーションサブコンポーネントに使用されてよい。

【００２０】

図１に示される実施形態では、サービスＳｖｃ１は少なくとも２つの層のリソース、つ

まり入信サービス要求を受信し、アウトバウンドサービス応答を送信するように構成される（ロードバランサ及び／または要求ルータ等の）フロントエンド（ＦＥ）ノード１７１、並びにサービス要求を遂行するためのサービスの論理が実装されるバックエンド（ＢＥ）ノード１７３を含む。ＦＥノード１７１Ａ、１７１Ｂ、及び１７１Ｃ等のＦＥノードの少なくともいくつかはそれらに割り当てられたパブリックＩＰアドレスを有し、このようにして例えば公衆インターネット１３９のデバイスに、及びネットワーク１８５等のカスタマ所有のネットワークでインターネットに接続されたデバイスにＳｖｃ１を公にアクセス可能にしてよい。

【００２１】

示される実施形態では、例えばＳｖｃ１関係のパケットが（公衆インターネットから直接的にアクセスできないプライベートＩＰアドレスを有する）ＣＩ１１０Ａと、Ｓｖｃ１ネットワーク１７０との間で、ＣＩ１１０Ａがそれに割り当てられるパブリックＩＰアドレスを有する必要なく、及びトラフィックがカスタマ所有ネットワーク１８５または公衆インターネット１３９のリンクを通過することを必要とせずに流れることができるようにするために、プライベートエイリアスエンドポイント（ＰＡＥ）１５０がＩＶＮ１１０Ａで確立されている。以下にさらに詳細に説明されるように、ＩＶＮ１１０Ａのためのルートテーブルエントリは、（ＣＩ１１０Ａが構成されるサブネットを含んだ）ＩＶＮ１１０Ａの１つまたは複数のサブネットで生じ、Ｓｖｃ１に向かうことになっているトラフィックがＰＡＥ１５０をターゲットとする必要があることを示すためにいくつかの実施形態でセットアップされてよい。Ｓｖｃ１のパブリックＩＰアドレスのリスト等の他のメタデータだけではなくこのルートテーブルエントリも、少なくともいくつかの実施形態でＩＶＮ１１０Ａのインスタンスホスト１３０のそれぞれで実行中の仮想化管理構成要素（ＶＭＣ）（例えば、ハイパーバイザ構成要素）が利用できてよい。ＩＶＮ構成マネージャ１０６は、クライアントがＰＡＥの作成、ＰＡＥとの特定のサービスの関連付け、ＩＶＮのためのルートテーブルエントリの作成または修正等を要求できるようにする（アプリケーションプログラミングインタフェース（ＡＰＩ）、ウェブベースコンソール、コマンドラインツール、またはグラフィックユーザーインタフェース等の）１つまたは複数のプログラムインタフェースを実装してよい。

【００２２】

インスタンスホスト１３０ＡでのＶＭＣは、ＣＩ１１２Ａで生成され、Ｓｖｃ１に向けられたサービス要求を含むアウトバウンドベースラインネットワークパケットを妨害してよい。（いくつかのサービス要求及びその関連付けられた要求パラメータが複数のパケットを必要とする可能性があることに留意されたい。提示を簡略にするために、サービス要求は以下の説明ではベースラインパケットに収まると仮定される。係るサービス要求の本明細書に説明されるトンネリング技法は、多様な実施形態でパケット境界を渡るサービス要求に使用されてもよい。サービス要求は、ＨＴＴＰ（ハイパーテキスト転送プロトコル）、ＨＴＴＰｓ（セキュアＨＴＴＰ）、ＸＭＬ（拡張マークアップ言語）等のＳｖｃ１によってサポートされている任意の適切なインタフェースに従ってフォーマットされてよい。ベースラインパケットはソースとしてＣＩのプライベートＩＰアドレスを、宛先としてＳｖｃ１のパブリックＩＰアドレスを示してよい。ＶＭＣは、示される実施形態では第１のカプセル化プロトコルに従ってベースラインパケットから第１のカプセル化パケットを生成してよい。第１のカプセル化パケットの中で、いくつかの実施態様では、ベースラインパケットは本体に含まれてよい。一方、第１のカプセル化プロトコルの１つまたは複数の追加のヘッダは、パケットがＰＡＥトラフィックを含む旨の表示を（他の情報の中で）含んでよい。第１のカプセル化パケットは、ＰＡＥトラフィック１６２のための破線矢印によって示されるように、インスタンスホスト１１２Ａから、示されている実施形態では一群のトンネリング手段１４０の内のＴＩ　１４２Ａ等のトンネリング手段（ＴＩ）に送信されてよい。（ＴＩ１４２Ａ、１４２Ｂ等のＴＩとしてセットアップされる複数のコンピューティング装置を含んでよいＴＩ群１４０は、ＶＣＳネットワーク１０４と、Ｓｖｃ１のネットワーク１７０を含んだ、プロバイダネットワークのさまざまな他の論理的に分

けられたネットワークとの間でトラフィックが流れることができるように確立された可能性がある。トンネリング手段は、いくつかの実施形態ではネットワーク関係の処理のために最適化された特殊目的コンピューティング装置を含んでよい。他の実施形態では、トンネリング手段は汎用コンピューティング装置での実行のプロセスまたはスレッドを含んでよい。

【００２３】

少なくともいくつかの実施形態では、第１のカプセル化パケットを受信すると、ＴＩ１４２ＡはＶＭＣによって追加されたヘッダだけではなくベースラインパケットのコンテンツも抽出してよい。一実施形態では、ＴＩ１４２Ａはそれぞれベースラインパケットの送信元アドレス及び宛先アドレスとは異なる送信元アドレス及び宛先アドレスを生成するために特定のトンネリングプロトコルと関連付けられたマッピングデータベースを活用してよい。例えば、一実施態様では、ベースラインパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスは、ＩＰｖ４（インターネットプロトコルのバージョン４）に従ってフォーマットされてよく、ＴＩ１４２Ａはそれらを、内部ブリッジネットワーク１６０を介してＳｖｃ１ネットワーク１７０に送信される第２のカプセル化パケットのためのより長いＩＰｖ６（インターネットプロトコルバージョン６）アドレスで置き換えてよい。内部ブリッジネットワーク１６０は、例えば仮想コンピューティングサービスから公にアクセス可能なサービスに向けられるトラフィック用等、プロバイダネットワークでの相互サービストラフィック用の経路として使用されてよい。いくつかの実施形態では、内部ブリッジネットワーク１６０はボーダネットワークと呼ばれてよく、公衆インターネットと仮想コンピューティングサービスとの間を流れるトラフィックに使用されてもよい。

【００２４】

一実施態様では、ＴＩ１４２Ａで、ベースラインパケットの送信元ＩＰアドレスは、アウトバウンド第２カプセル化パケットで使用される対応する送信元アドレスを探すためにマッピングデータベースでキーとして使用されてよい。同様に、ベースラインパケットの宛先ＩＰアドレスは、係る実施態様でアウトバウンド第２カプセル化パケットで使用される対応する宛先アドレスを探すためにマッピングデータベースでキーとして使用されてよい。少なくともいくつかの実施形態では、第２のカプセル化パケットの送信元アドレス及び宛先アドレスにより多くの数のビットを使用することによって、ＴＩ１４２ＡはソースＩＶＮ（例えば、ＣＩ１１２Ａで生じるパケットの場合ＩＶＮ１１０Ａ）の識別子、及び第２のカプセル化パケットでのＰＡＥ（例えばＰＡＥ１５０）の識別子の符号化を含むことができてよい。いくつかの実施形態では、ＰＡＥ及び／またはＩＶＮの識別子は第１のカプセル化パケットでＶＭＣによって追加されたヘッダに含まれてよく、ＴＩ１４２は係るヘッダから識別子を入手してよい。他の実施形態では、マッピングデータベースから、への、入手される送信元アドレス及び宛先アドレスはＩＶＮ及び／またはＰＡＥの符号化された識別子を含んでよい。

【００２５】

ＴＩ１４２Ａで生成された第２のカプセル化パケットは、ブリッジネットワーク１６０を介して宛先サービスＳｖｃ１のフロントエンドノード１７１（例えば１７１Ａ）に送信されてよい。フロントエンドノード１７１は、ルーティングのために使用されるソースＩＶＮ（例えばＩＶＮ　１１０Ａ）の識別子及び／またはＰＡＥ（例えばＰＡＥ１５０）の識別子だけではなく、（ソースＣＩプライベートＩＰアドレスを含んだ）ベースラインパケットのコンテンツも抽出するためにトンネリングプロトコルに従って脱カプセル化を実行できてよい。少なくともいくつかの実施形態では、ＰＡＥ及び／またはソースＩＶＮの識別によって、Ｓｖｃ１ノードは、以下にさらに詳細に説明されるように、異なる計算インスタンスからのサービス要求と同じソースプライベートＩＰアドレスを区別できるようになる。ベースラインパケットに示されるサービス要求は、処理のためにバックエンドノード１７３（例えば１７３Ａ）に渡されてよい。要求が処理された後、ベースライン応答パケットがバックエンドノードで生成され、トンネリングプロトコルに従ってカプセル化され、要求のソース（ＣＩ１１２Ａ）に向かって逆方向で送信して戻されてよい。ＴＩ１

４２Ａ（例えばＴＩ１４２Ａまたは異なるＴＩのどちらか）は、内部ブリッジネットワーク１６０を介してカプセル化された応答を受信し、第１のカプセル化プロトコルを使用し、修正されたカプセル化バージョンを生成し、ＩＨ１３０ＡのＶＭＣに修正されたカプセル化バージョンを送信してよい。ＶＭＣはベースライン応答パケットを抽出し、ソースＣＩ１１２Ａにベースライン応答パケットを提供してよい。

【００２６】

２つの異なるカプセル化プロトコルが上述されているが、いくつかの実施形態では、単一のカプセル化プロトコルだけが、計算インスタンスと公にアクセス可能なサービスとの間のトラフィックを容易にするために必要とされることがあるか、または使用されることがあることに留意されたい。例えば、１つの係る実施形態では、ＶＭＣは内部ブリッジネットワーク上でトラフィックに使用されるトンネリングプロトコルを実装できてよく、したがってＶＭＣ自体がトンネリング手段の機能を果たしてよい。係る実施形態では、ＶＭＣは、宛先としてＰＡＥ１５０と関連付けられた公にアクセス可能なサービスでパケットを妨害し、ソースＩＶＮ及び／またはＰＡＥの符号化を含むカプセル化されたパケットを生成し、ブリッジネットワークデバイスにカプセル化されたパケットを送信してよい。

【００２７】

Ｓｖｃ１に向けられるトラフィックのためのルートテーブルエントリでのターゲットとしてＰＡＥを使用することによって、クライアントはＩＶＮとＳｖｃ１との間のルーティングトラフィックに向かう、ともに図１に示される他の２つの接近を回避できてよい。１つの接近では、その代わりにＩＶＮ１１０Ｂがセットアップされるクライアントは、そのＩＶＮのためにインターネットゲートウェイ１８２を確立する、及び／またはＣＩ１１２Ｋ等のそのインスタンスの１つに（公衆インターネットからアクセスできる）パブリックＩＰアドレスを割り当てることを決定してよい。係る状況では、ＣＩ１１２Ｋで生成されたＳｖｃ１要求を含んだベースラインパケットは、例えばインターネットゲートウェイ（ＩＧＷ）トラフィックのために示される経路１６３に類似する経路を介して、上述されたトンネリングプロトコルの種類を使用することなくＳｖｃ１ノード（例えばＦＥノード１７１Ｂ）に送信されてよい。いくつかの場合、パブリックＩＰアドレスで生じるトラフィックに使用される経路は公衆インターネットのリンク１３９を含んでよい。インターネットゲートウェイ手法を使用することに優るＰＡＥ手法を使用することの１つの潜在的な優位点は、ＩＶＮ１１０Ｂが（パブリックＩＰアドレスが割り当てられる必要がない）ＩＶＮ１１０Ａよりも公衆インターネットからの攻撃に（パブリックＩＰアドレスを露呈することのおかげで）より脆弱性がある場合がある点である。

【００２８】

ＰＡＥの使用に対する第２の代替策で、クライアントは、ＩＶＮ１１０Ｂとカスタマ所有ネットワーク１８５との間に安全な接続性を提供するためにＶＰＮ（仮想プライベートネットワーク）ゲートウェイ１８３を確立してよい。ＣＩ１１２Ｌ等のインスタンスからＳｖｃ１に向けられるパケットは、最初にカスタマ所有ネットワーク１８５に送信され、次いで（例えば公衆インターネットリンク１３９を介して）（ＦＥノード１７１Ｃ等の）Ｓｖｃ１ノードに送信されてよい。確立されたＶＰＮゲートウェイ１８５を有する１１０Ｂ等のＩＶＮがパブリックＩＰアドレスを活用する必要がなく、セットアップされたインターネットゲートウェイ１８２を有する必要がなく、ＶＰＮゲートウェイだけを使用するクライアントはそれによって上述されたセキュリティの脆弱性を回避し得ることに留意されたい。しかしながら、多くの場合、プロバイダネットワークの中で（例えば、ＩＶＮの中のインスタンスで）生じ、プロバイダネットワークの中の宛先（例えばＳｖｃ１ノード）をターゲットとするトラフィックのための外部ネットワークに対してＶＰＮ接続を使用することはいくつかの点で非効率的であることがある。例えば、少なくともいくつかの実施形態では、ＰＡＥ方式と比較して、より高い待ち時間に遭遇することがあり、より低いスループットが持続可能であることがあり、及び／またはＶＰＮ手法が使用される場合、より高いコストが生じることがある。それぞれ上述された３つの代替ルーティング手法（つまりＰＡＥを使用するルーティング、パブリックＩＰアドレスを送信元ＩＰアドレスと

して使用するルーティング、及びＶＰＮを使用するルーティング）に対応する３つの別々のＦＥノード１７１Ａ、１７１Ｂ、及び１７１Ｃが図１に示されるが、少なくともいくつかの実施形態では、任意の所与のＦＥノードは代替策のいずれかを使用し送信されるトラフィックを処理できてよい。したがって、３つのＦＥノードの図は、ＦＥノードのそれぞれのセットが異なる接続性代替策に必要とされることを暗示することを意図していない。

【００２９】

一実施形態では、仮想コンピューティングサービスは、ＩＶＮの計算インスタンスで実行中のアプリケーションからＰＡＥを使用し、公にアクセス可能なサービスにアクセスするために呼び出すことができるＡＰＩのセットを露呈するサービス接続性ライブラリ（ＳＣＬ）を提供してよい。係る状況では、アプリケーションはターゲットサービスＳｖｃ１を示すＡＰＩ呼出しを発行してよく、サービス要求のコンテンツはＡＰＩ呼出しのパラメータによって示される。ＳＣＬは、アプリケーションがＳｖｃ１にサービス要求を提供する意図があると判断してよく、Ｓｖｃ１にサービス要求を送信するために必要な適切なカプセル化の実装を開始してよい。したがって、アプリケーションがベースラインパケットの生成を開始する従来の手法を使用する代わりに、サービス要求からパケットを作成する作業はＳＣＬによって扱われてよい。いくつかの係る実施形態では、アプリケーションは、ターゲットサービスの特定のパブリックＰアドレスを入手する必要さえない。例えば、サービス要求の宛先は、特定のネットワークアドレス別よりむしろサービス名別で示されてよい。一実施形態では、アプリケーションがＡＰＩ呼出しのサービスの特定のターゲットパブリックアドレスを示すとしても、ＳＣＬは（ＳＣＬによって選択される実際の宛先がサービス要求に適切に応答できる限り）ターゲットサービスの異なるパブリックＩＰアドレスまたはプライベートＩＰアドレスにサービス要求のカプセル化バージョンを送信してよい。

【００３０】

パケットの流れの実施例

図２は、少なくともいくつかの実施形態に従って、分離仮想ネットワークの計算インスタンスで生じるパケットを、公にアクセス可能なサービスの宛先に向けることに関与する実施例の構成要素を示す。示されるように、ＩＶＮ２１０のインスタンスホスト２３０は、インスタンス１１２Ａ及び１１２Ｂ等の複数の計算インスタンス１１２を含んでよい。各インスタンス１１２は、ゲスト仮想機械で実行中のそれぞれのオペレーティングシステムインスタンスを含んでよい。クライアントアプリケーションの１つまたは複数の構成要素は、計算インスタンス１１２Ａでのアプリケーションプロセス２２０Ａ及び計算インスタンス１１２Ｂでのアプリケーションプロセス２２０Ｂ等の各計算インスタンスで実行されてよい。計算インスタンスと（ネットワークトラフィックに使用されるネットワークインタフェースカード、つまりＮＩＣ等の）インスタンスホストのハードウェア構成要素との間の対話は、ＶＭＣ２４０等の１つまたは複数の仮想化管理構成要素（ＶＭＣ）によって管理されてよい。ＶＭＣは、例えば、ハイパーバイザ及び／または（ドメインゼロつまりｄｏｍ０オペレーティングシステムインスタンスと呼ばれることもある）特権オペレーティングシステムインスタンスを含んでよい。

【００３１】

アプリケーションの少なくともいくつかは、示される実施形態ではＩＶＮの外で実装される１つまたは複数のサービスへのアクセスを必要とすることがある（例えば、ＩＶＮの外で実装される１つまたは複数のサービスにサービス要求を提出してよく、ＩＶＮの外で実装される１つまたは複数のサービスからサービス応答を受信してよい）。例えば、アプリケーションプロセス２２０Ｂは公にアクセス可能なサービスＳｖｃ１へのアクセスを必要とすることがある。したがって、図２で「１」と名前を付けられた矢印によって示されるように、ＤＮＳクエリー２０４は計算インスタンスから、Ｓｖｃ１のＩＰアドレスを要求するＤＮＳサーバ２５２（例えば、ＩＶＮ２１０が実装される仮想コンピューティングサービスネットワークの中からアクセス可能なＤＮＳサーバ）に提出されてよい。ＤＮＳサーバ２５２は、「２」と名前が付けられた矢印によって示されるように、Ｓｖｃ１によ

って露呈されるか、または宣伝されるパブリックＩＰアドレス２０５を提供してよい。少なくともいくつかの実施形態では、アプリケーションがしばらくＳｖｃ１と対話していない場合、ＤＮＳルックアップを実行しさえすればよい。すなわち、Ｓｖｃ１のアドレスがいったん入手されると、アドレスは、ＤＮＳサーバ２５２との追加の対話なしに、インスタンス１１２Ｂによって長期間（例えば、アドレスが有効である限り）使用されてよい。

【００３２】

Ｓｖｃ１に向けられるサービス要求は、示される実施形態ではインスタンス１１２Ｂで生成されるベースラインパケット２５０の本体に含まれ、Ｓｖｃ１に向かう伝搬のために計算インスタンスのネットワーキングスタックに送信されてよい。ベースラインパケット２５０は、その送信元アドレスとしてインスタンス１１２Ｂのプライベートアドレスを、宛先としてＳｖｃ１のパブリックＩＰアドレスを示してよい。他のネットワークパケットと同様に、ベースラインパケットは、「３」と名前を付けられた矢印によって示されるように、（物理ネットワーク伝送を担ってよい）ＶＭＣ２４０によって妨害されてよい。

【００３３】

ＶＭＣ２４０は、ルートテーブル２３５及びＳｖｃ１パブリックＩＰアドレスのリスト２３６等、示される実施形態ではＰＡＥ関係のメタデータ及び他のＩＶＮメタデータにアクセスできてよい。ルートテーブル２３５は、多様な宛先向けであるパケットを送るために使用される必要のあるターゲットを示すエントリを含んでよい‐例えば、Ｎ１．Ｎ２．Ｎ３．＊．の範囲の宛先アドレスの付いたパケットの場合、ターゲットＫ．Ｌ．Ｍ．Ｎが使用される必要がある。Ｓｖｃ１の任意のノード向けのパケットのルートテーブルは図２に示される実施例で作成され、プライベートエイリアスエンドポイントＰＡＥ－１はターゲットとして示される。ベースラインパケット２５０に示される宛先及びそれが利用できるＰＡＥ関係メタデータの分析に基づいて、ＶＭＣ２４０は示される実施形態では第１のカプセル化パケット２５１を生成してよい。パケット２５１の本体は（そのソース及び宛先の情報を含んだ）ベースラインパケット２５０のコンテンツを組み込んでよい。一方、追加のヘッダ２６０は、ＶＭＣとトンネリング手段２４２との間の通信に使用される第１のカプセル化プロトコルＰに従ってＶＭＣ２４０によって生成されてよい。カプセル化パケット２５１は、「４」と名前が付けられた矢印によって示されるように、ＶＭＣ２４０から特定のトンネリング手段２４２に送信されてよい。少なくともいくつかの実施形態では、ＰＩヘッダ２６０は、ベースラインパケットがＰＡＥ１と関連付けられる、及び／またはＩＶＮ２１０で生じる旨の表示を含んでよい。ＶＭＣ２４０とトンネリング手段２４２の間の経路はそれ自体いくつかのホップを含んでよく、例えば多様なホップのためのターゲットは図２に示されないルートテーブルエントリに基づいて選択されていることに留意されたい。

【００３４】

トンネリング手段２４２は、カプセル化パケット２５１に含まれるベースラインパケット２５０のＰＩヘッダ２６０及び／またはソースヘッダ／宛先ヘッダを調べてよい。第２のカプセル化プロトコルＰ２（本明細書ではトンネリングプロトコルとも呼ばれる）のマッピングデータベース２６２を使用し、トンネリング手段２４２は、１つまたは複数のＰ２ヘッダ２６１及びベースラインパケット２５０を含んだ第２のカプセル化パケット２５５を生成してよい。ベースラインパケットの送信元アドレス及び宛先アドレスは、パケット２５５に使用される新しいソースヘッダ及びパケットヘッダを識別するために、いくつかの実施形態ではマッピングデータベース２６２へのインデックスとして使用されてよい。いくつかの実施態様では、プロトコルＰ２に従って、ＩＰｖ４ベースラインパケット２５０は、例えばＳＩＩＴ（ステートレスＩＰ／ＩＣＭＰ（インターネットプロトコル／インターネットコントロールメッセージプロトコル）変換）または類似するＩＰｖ４－ＩＰｖ６ヘッダ変換機構を使用し、ＩＰｖ６互換パケット２５５の中でカプセル化されてよい。他の実施形態では、プロバイダネットワークの特許カプセル化プロトコルがカプセル化パケット２５５を生成するために使用されてよい。いくつかの実施形態では、ＩＰｖ６を

使用する代わりに、ＴＣＰオプションヘッダ等の追加のＩＰｖ４ヘッダがトンネリング手段によって使用されてよいか、またはＵＤＰ（ユーザーデータグラムプロトコル）カプセル化が（例えば、ＵＤＰメッセージの中にベースラインパケットコンテンツを取り込むことによって）使用されてよい。いくつかの実施形態でＰ１ヘッダ２６０及びＰ２ヘッダ２６１の中に含まれてよい情報の種類の実施例は図４に示され、以下に説明される。カプセル化パケット２５５は、トンネリング手段２４２から、Ｓｖｃ２ノードに達するために横断される適切なブリッジネットワーク１６０のデバイスに送信されてよい。

【００３５】

図３ａ及び図３ｂは、少なくともいくつかの実施形態に従って、分離仮想ネットワークの計算インスタンスで生じるパケットを処理してよいサービス側構成要素のそれぞれの実施例を示す図である。上述されたように、いくつかの実施形態では、少なくとも２つのタイプのサービスが、ＰＡＥが構成されているＩＶＮからのクライアントアクセスをサポートしてよい。第１のタイプのサービスはプロバイダネットワーク事業者によって実装されてよい。一方、第２のタイプはプロバイダネットワークのカスタマ等のサードパーティによって実装されるサービスを含んでよい。図３ａに示されるプロバイダネットワーク実装サービス３７６等の第１のタイプのサービスの場合、フロントエンドノード３７４はトンネリング手段２４２によって使用されるカプセル化プロトコルＰ２に精通して（つまり、実装できて）よい。すなわち、プロトコルＰ２に従ってフォーマットされるパケット２５５を受信すると、サービス３７６のフロントエンドノード３７４はベースラインパケットコンテンツを抽出し、処理のためにバックエンドノード３７４に送信できる対応する内部要求３５０を生成できてよい。いくつかの場合、プロバイダネットワークによって実装されるサービスは、例えばＨＴＴＰ（ハイパーテキスト転送プロトコル）に従ってフォーマットされたサービス要求をサポートしてよく、フロントエンドノードは、ベースラインパケットが生成されたソースＩＶＮの識別子、及び／またはベースラインパケットを送るために使用されるＰＡＥを示すベースライン要求に１つまたは複数のＸ－Ｆｏｒｗａｒｄｅｄ－Ｆｏｒヘッダを追加してよい。要求された操作がバックエンドノードで実行された後、例えば応答経路で類似したカプセル化技法を使用し、要求側計算インスタンスに応答が送り返されてよい。例えば、サービス３７６のＰ２精通フロントエンドノード３７４は、ベースライン応答の少なくとも一部分を含んだＰ２準拠のカプセル化パケットを生成し、ブリッジネットワーク１６０を介してパケットを、同様にＰ１準拠カプセル化パケットを生成し、適切なＶＭＣ２４０にパケットを送信してよいトンネリング手段２４２に送信してよい。ＶＭＣ２４０は、Ｐ１準拠パケットからベースライン応答を抽出し、１１２Ｂ等のソース計算インスタンスに応答を提供してよい。

【００３６】

プロバイダネットワーク事業者によって実装されるサービスのノードとは対照的に、（図３ｂに示されるサードパーティサービス３７８等の）少なくともいくつかのサードパーティサービスは、プロトコルＰ２に従って生成されるカプセル化パケット２５５からベースラインパケットを抽出できるノードを含まないことがある。いくつかの場合、例えば、Ｐ２の詳細はサードパーティサービス事業者が利用できないことがあるか、または係る事業者はＰ２準拠のサービスノードを構築するためのリソースまたは専門知識を有さないことがある。したがって、少なくともいくつかの実装態様では、ＰＡＥベースのルーティングのために係るサードパーティサービスを登録する要求に応えて、または登録後要求に応えて、プロバイダネットワークの構成または制御プレーンは１つまたは複数のサービス側Ｐ２精通手段３７０を確立してよい。係るサービス側手段３７０はカプセル化パケット２５５からベースラインパケット２５０を抽出し、サードパーティサービス３７８のフロントエンドノード３７５にベースラインパケットを送信してよい。フロントエンドノード３７５は次いでベースラインパケット２５０を、特許サードパーティフォーマット、ＨＴＴＰで、またはサービス３７８のバックエンドノード３８０によって予想される他のインタフェースに従って生成されてよい内部要求３５２に変換してよい。内部要求３５２に対応する操作は、次いでバックエンドノードで遂行されてよく、応答は、手段３７０でのカプ

セル化の後に、要求が生じた計算インスタンスに逆方向で送信されてよい。

【００３７】

カプセル化フォーマット

図４は、少なくともいくつかの実施形態に従って、計算インスタンスで生じるベースラインパケットのためのカプセル化フォーマットの実施例を示す。示されるように、ベースラインパケット４０２は、示される実施形態で送信元ＩＰバージョン４アドレス及び宛先ＩＰバージョン４アドレスを示してよい。例えば、分離仮想ネットワークの中で、（ＩＶＮの外で宣伝されていない）プライベートＩＰアドレス「１０．０．１．２」がクライアントによって計算インスタンス１１２に割り当てられてよく、このプライベートＩＰアドレスはベースラインパケット４０２で送信元アドレスとして示されてよい。パブリックＩＰバージョン４アドレス「１７６．３２．１０１．２５」は、計算インスタンスからアクセスされる特定の公にアクセス可能なサービスＳｖｃ１のアドレスに対するＤＮＳクエリーに応えてＤＮＳサーバによって提供された可能性がある。サービスのこのパブリックアドレスはベースラインパケット４０２の宛先として示されてよい。例えば、計算インスタンスでのソースポートとしてポート４３２１、及び宛先サービスポートとしてポート８０等、ＴＣＰポート番号もベースラインパケットに示されてよい。ベースラインパケット４０２のペイロードまたは本体部分は、サービス要求のパラメータだけではなくストレージサービスに向けられた読取り要求または書込み要求等、送信中のサービス要求のタイプも示してよい。

【００３８】

ベースラインパケット４０２は、示される実施形態でトンネリング手段との通信のために使用される第１のカプセル化プロトコルＰ１に従ってインスタンスのホストで仮想化管理構成要素（例えば、ＶＭＣ－ｘ）によってカプセル化されてよい。Ｐ１互換パケット４０４で、ベースラインパケットは本体に含まれてよく、１つまたは複数のＰ１ヘッダが追加されてよい。ＶＭＣの識別子はソースとして示されてよく、トンネル中間群はいくつかの実装態様で宛先として示されてよい。例えばベースラインパケットが生成されたソースＩＶＮを識別する、及び／または宛先としてＳｖｃ１を指定するルートテーブルエントリに示されたＰＡＥを示す他のＰ１特有のヘッダは、パケット４０４でいくつかの実施形態に含まれてよい。Ｐ１互換フォーマットは少なくともいくつかの実施形態での多様なヘッダフィールドにＩＰバージョン４フォーマットを使用してよい。

【００３９】

トンネリング手段で、Ｐ１互換パケット４０４は示される実施形態でそのＰ１ヘッダを取り去られてよく、ヘッダの異なるセットは宛先サービスへのブリッジネットワークを横切る通信のために使用されるトンネリングプロトコルＰ２に従って追加されてよい。示される実施形態では、トンネリング手段によって生成されるＰ２互換パケット４０６は、ＩＰｖ６ソースフィールド及び宛先フィールドを含んでよい。ＩＰｖ６で送信元アドレスに使用可能な１２８ビットの内の３２ビットのサブセットは、いくつかの実施形態でソース計算インスタンスのプライベートＩＰｖ４アドレスを示すために使用されてよい。同様に、ＩＰｖ６で宛先アドレスに使用可能な１２８ビットの内の３２ビットサブセットは宛先サービスのＩＰｖ４パブリックアドレスを示すために使用されてよい。例えば、パケット４０６の送信元アドレスの低位ビットは、送信元ＩＰＶ４アドレス１０．０．１．２の代替表現である０Ａ００：０１０２であり、パケット４０６の宛先アドレスの低位ビットは、ＩＰｖ４宛先アドレス１７６．３２．１０１．２５の代替表現であるＢ０２０：６５７Ｄである。

【００４０】

一実施態様では、図４に示されるアドレス構造４０８に示されるように、ＩＰｖ６で使用可能な１２８アドレスビットは、トンネリングプロトコルＰ２に従って以下の通り使用されてよい。最低位の３２ビット（ビット０～３１）は送信元ＩＰｖ４アドレスまたは宛先ＩＰｖ４アドレスに使用されてよく、ビット４０～７１はＰＡＥ識別子を示すために使用されてよく、ビット８０～１２７は、ソースＩＶＮまたは宛先サービスが実装されてい

るプロバイダネットワーク場所またはデータセンタに配分される４８ビットのＩＰｖ６接頭辞に使用されてよい。ＰＡＥ識別子用にとっておかれた３２ビットの内の２４ビット（例えば、より高位の２４ビット）は、示される実装態様ではソースＩＶＮ識別子を示してよい。このようにして、少なくともいくつかの実施形態では、ＩＶＮ識別子はＰＡＥ識別子の中に埋め込まれ、したがってＰＡＥ識別子から抽出可能であってよい。ソースＩＶＮ識別子、ＰＡＥ識別子、または両方を表すための他の符号化技法は異なる実装態様で使用されてよい。例えば、ＰＡＥを一意で識別するために必要とされるビットの数の将来の考えられる増加に対応するために、ビット３１～３９及びビット７２～８０等のいくつかの数のビットが将来の使用のために確保されてよい（ＲＦＵ）。Ｐ２互換カプセル化パケットアドレスを示されるように構造化する（例えば、最下位の３２ビットはＩＰｖ４送信元アドレス／宛先アドレスを符号化するために使用される）１つの優位点は、少なくともいくつかのロードバランサが、それらが、１２８ビットの内のＩＰｖ４部分だけが宛先として示されるならば選択されるだろう係るＩＰｖ６互換パケットを受信するときに同じ宛先を選択してよい点である。他の手法は、例えばビットの異なるサブセットがＩＶＮ識別子及び／またはＰＡＥ識別子を示すために使用される異なる実施形態でＩＰｖ６互換アドレス構造を区分化するために使用されてよい。

【００４１】

少なくともいくつかの実施形態に従って、トンネリングプロトコルは、例えば別個のトンネリング手段群を必要とすることなくソース計算インスタンスが実行するインスタンスホストで実装されてよい。係る実施形態では、図４に示される２ステップのカプセル化が、ＶＭＣで、及び／またはインスタンスホストで実行中の異なるサービス接続性構成要素で実装される単一論理ステップに結合されてよい。ＶＭＣ及び／またはサービス接続性構成要素は、係る実施形態でのソース計算インスタンスと宛先サービスとの間のトンネリング手段と見なされてよい。

【００４２】

ＰＡＥ構成

図５は、少なくともいくつかの実施形態に従って、ＰＡＥ構成要求及びＰＡＥ構成応答の実施例を示す。示されるように、プロバイダネットワークの構成マネージャ５９２は、ＡＰＩ、ウェブベースのコンソール、カスタムＧＵＩまたはコマンドラインツール等の１つまたは複数のプログラムインタフェース５５０を実装してよい。クライアント５０２は、係るインタフェースを使用し、例えば要求中のパラメータとしてＩＶＮ識別子を示す指定されたＩＶＮのプライベートエイリアスエンドポイントを作成するために「Ｃｒｅａｔｅ－ＰＡＥ－Ｉｎ－ＩＶＮ」要求５０５を提出してよい。それに応じて、構成マネージャ５９２はその構成データベースで要求されたＰＡＥのために１つまたは複数のエントリを生成し、記憶し、新規に作成されたＰＡＥの識別子を応答５０７で提供してよい。いくつかの実施形態では、１つまたは複数のＰＡＥは、ＩＶＮがクライアントのために確立された時点でＩＶＮのために自動的にセットアップされてよく、係る状況では、明確なＰＡＥ作成要求は必要とされないことがある。

【００４３】

クライアント５０２は、ＰＡＥ作成後に、ＰＡＥを使用しトラフィックが送られる特定のサービスを示す「Ａｓｓｉｇｎ－Ｓｅｒｖｉｃｅ－ｔｏ－ＰＡＥ」要求５０９を構成マネージャ５９２に提出してよい。いくつかの実装態様では、ＰＡＥ識別子及びサービス識別子は係る要求でパラメータとして供給されてよい。それに応じて、構成マネージャ５９２はＰＡＥに関してその構成メタデータを更新してよく、サービス割当ての肯定応答５１１を提供した。いくつかの実施形態では、プログラムインタフェース５５０は、構成されているＰＡとの関連付けのために１つがその中から選択できる登録サービス名のリストを（例えば、ドロップダウンメニューに）提供してよい。

【００４４】

多様なタイプのアクセス制御方針は、例えば方針及びＰＡＥを指定する「Ａｓｓｉｇｎ－Ｐｏｌｉｃｙ－ｔｏ－ＰＡＥ」要求５１３に応えて、いくつかの実施形態でＰＡＥに割

り当てられてよい。適用可能な方針の例は図６に示され、以下に説明される。構成マネージャ５９２は示される方針の表示及び方針のＰＡＥとの関連付けを記憶し、関連付けの肯定応答５１５をクライアントに提供してよい。少なくともいくつかの実施形態では、方針の関連付けはＰＡＥのために要求されてよいが、方針の実際の施行は（ａ）ＰＡＥに割り当てられるサービス、（ｎ）方針を指向するためにＰＡＥに割り当てられるサービスによって呼び出すことができる、プロバイダネットワークの許可及び認証サービス等の異なるサービス、または（ｃ）サービス要求がＰＡＥに従ってそこから送られるインスタンスホストのＶＭＣでの内の１つまたは複数で実行されてよい。いくつかの実施形態では、方針の表示は、例えば肯定応答５１５がクライアントに提供される前に、ＰＡＥに割り当てられたサービスの制御プレーン構成要素に構成マネージャによって送信されてよい。

【００４５】

プロバイダネットワークのクライアントは、いくつかの実施形態でＰＡＥ支援ルーティングのためのサービスを登録する要求５１７を提出してもよい。例えば、サードパーティサービス（つまり、プロバイダネットワーク事業者によって直接的に管理されないサービス）が、プロバイダネットワークのリソースのなんらかのセットを使用し確立されてよく、係るサードパーティサービスの事業者は、パブリックＩＰアドレスがＩＶＮによって使用される必要なく、ＩＶＮの中からサービスへのアクセスを可能にすることを希望することがある。係る状況では、サービス構成の詳細（例えば、サービスのフロントエンドノードのアドレス）を提供する「Ｒｅｇｉｓｔｅｒ－Ｓｅｒｖｉｃｅ－Ｆｏｒ－ＰＡＥ」要求がクライアント５０２によって提出されてよい。少なくともいくつかの実装態様では、ＰＡＥを確立することを担う構成マネージャとは異なる構成マネージャがサービスを登録することを担ってよく、プログラムインタフェースの異なるセットがサービス登録要求に使用されてよい。サービス登録要求に応えて、構成マネージャは、例えば、サービスを受け入れ、クライアントに応答５１９で登録された名前または登録されたサービスの識別子を提供する前に、登録されることが提案されたサービスがＰＡＥ互換性の特定の基準を満たすことを検証するために１つまたは複数のバリデーション操作を実行してよい。例えば、一実施態様では、サービスのフロントエンド構成要素は、それがプロバイダネットワークのカプセル化プロトコルを使用するトンネリング手段によって生成される要求を受信できることを確認するためにクエリーを行われてよい、または試験されてよい。

【００４６】

いくつかの実施形態では、追加構成要求のタイプが図５に示されるものを超えてサポートされてよい。例えば、（図３ｂのＰ２精通手段３７０等の）サービス側トンネリング手段を構成する要求は、いくつかの実施形態でサードパーティサービスをセットアップしたクライアントによって提出されてよい。一実施形態では、クライアントは異なるサービスにＰＡＥを割り当てし直す、または追加のタイプの構成要求を使用し、ＰＡＥに複数のサービスを割り当てることができてよい。いくつかの実施態様では、図５に示されるすべてのタイプの構成要求がサポートされてよいわけではない。上述されたように、クライアントは（例えば、同じＩＶＮの中から異なるサービスにアクセスするための）所与のＩＶＮと関連付けられた複数のＰＡＥを確立してよく、複数のＩＶＮを有するクライアントはそれぞれの係るＩＶＮで１つまたは複数のＰＡＥをセットアップしてよい。

【００４７】

図６は、少なくともいくつかの実施形態に従って、ＰＡＥ構成データベースコンテンツの実施例を示す。構成マネージャ５９２を活用して２つのＰＡＥが確立された特定のＩＶＮ（ＩＶＮ－ｊ）の構成データベースが示される。ＰＡＥ６０４Ａは、サービス識別子フィールド６０６Ａに示されるサービス「ＳｔｏｒａｇｅＳｖｃ１」（プロバイダネットワークで実装されたストレージサービス）を割り当てられる。一方、ＰＡＥ６０４Ａはサービス識別子フィールド６０６Ｂに示されるサービス「ＤＢＳｖｃ１」（プロバイダネットワークで実装されるデータベースサービス）を割り当てられる。ＰＡＥ６０４Ａはそれに割り当てられたアクセス方針６０８Ａを有する。一方、ＰＡＥ６０４Ｂは２つのアクセス方針６０８Ｂ及び６０８Ｃを有する。

【００４８】
アクセス方針６０８Ａは、示される実施例では範囲ＣＩ－ＩＰ－ａｄｄｒｅｓｓ－ｒａｎｇｅ６１０ＡのＩＰアドレスを有する計算インスタンスからまたは計算インスタンスに向けられるＳｔｏｒａｇｅＳｖｃ１トラフィックに適用する。いくつかの実施形態では、方針が適用するトラフィックを示すためにＩＰアドレスを使用する代わりに、計算インスタンスのインスタンス名または他の識別データが使用されてよい。アドレス範囲６１０Ａから要求が許可される操作タイプのリスト（例えば、読取り対書込み）は、方針６０８Ａのｏｐｅｒａｔｉｏｎ－ｔｙｐｅｓ－ｐｅｒｍｉｔｔｅｄフィールド６１２Ａに示されてよく、それらの操作を向けることができるサービスＳｔｏｒａｇｅＳｖｃ１のオブジェクト（例えば、ディレクトリ「／ｘｙｚ」に記憶されるオブジェクト）はオブジェクトリスト６１４Ａに示される。示される例では、方針６０８Ａが適用される時間範囲（例えば、各作業日の特定の時間、または週の特定の日）は、適用可能な時間範囲フィールド６１６Ａに示されてよい。本人（例えば、ユーザーまたはグループの識別子）のリスト６１８Ａも、そのサービス要求が方針６０８Ａに示される規則によって管理されるエンティティを示す、方針６０８Ａについて関連付けられてよい。

【００４９】
ＰＡＥ６０４Ｂのために施行されるアクセス方針６０８Ｂ及び６０８Ｃのそれぞれは、方針の規則が適用される計算インスタンスを示す、そのそれぞれのＣＩ－ＩＰ‐ａｄｒｅｓｓ範囲６１０を示してよい。６０８Ｂ等のいくつかの方針では、例えば、許可される操作のタイプの代わりに、または許可される操作のタイプに加えて、禁止される操作のタイプが（例えば、ｏｐｅｒａｔｉｏｎ－ｔｙｐｅｓ－ｐｒｏｈｉｂｉｔｅｄフィールド６１３に）示されてよい。オブジェクトリスト６１４Ｂに「＊」で示されるように、フィールド６１３に示される操作は、ｐｒｉｎｃｉｐａｌｓ－ｌｉｓｔ６１８Ｂに示される本人について示される例でＤＢＳｖｃ１のすべてのオブジェクトについて禁止されてよい。示されるように、方針に含むことができるエントリのすべてのタイプが方針ごとに指定される必要があるわけではない‐例えば、方針６０８Ｂは適用可能な時間範囲を含まない。一方、方針６０８Ｃは本人リストを含まない。方針に含まれないエントリのタイプについてはデフォルト値が使用されてよい‐例えば、終日が適用可能な時間範囲となると仮定されてよく、方針規則は、特定の本人が示されない場合すべての本人に適用されてよい。示される例では、フィールド６１２Ｂは、適用可能な時間範囲６１６Ｃの間にフィールド６１４Ｃにリストされるオブジェクトに関して許可される操作タイプを示してよい。

【００５０】
いくつかの実施形態では、特定のアクセス方針が所与のＰＡＥのためにクライアントによって指定されない場合、プロバイダネットワークは対応するサービスに提出されるサービス要求に適用される規則を決定するためになんらかのデフォルトのセットを適用してよい。デフォルトはいくつかの実装態様ではサービスごとに異なることがある。上述されたように、いくつかの実施形態では、ＰＡＥが割り当てられているサービスは（サービス自体のノードで、またはアイデンティティ及び許可管理サービス等のプロバイダネットワークの別のサービスに要求を提出することによって）方針を施行することを担ってよい。いくつかのサービスに対するサービス要求は、要求がサービスに到達した後に要求されている操作のタイプを決定することだけが可能であるように暗号化されてよく、その結果、アクセス方針はサービス端部に適用されなければならないことがある。係る場合、方針は、方針がクライアント（例えば、ＩＶＮ構成マネージャ）によって示される構成マネージャによってサービスに（例えば、制御プレーンまたはサービスの管理構成要素に）通信されてよい。他の実施形態では、方針の規則の少なくともいくつかは要求者端部（例えば、ＩＶＮ端部）で施行されてよい‐例えば、対応するユーザが適用可能な方針の本人リストに示され、示される本人についてすべての書込みが禁止されている場合、ＶＭＣは計算インスタンスから発行される書込み要求を拒否することができてよい。

【００５１】
再利用されるプライベートＩＰアドレスからの要求の区別

クライアントはＩＶＮネットワーク構成で与えられる柔軟性を使用して、例えば、同じアドレスが他の場所で（例えば、他のＩＶＮでまたは公衆インターネットで）使用中であるかどうかを考慮することなく、上述されたようにいくつかの実施形態でＩＶＮ計算インスタンスに対し、その好みのプライベートＩＰアドレスを割り当ててよい。いくつかの場合、クライアントは異なるＩＶＮのインスタンスに同じＩＰアドレスを割り当ててよい。（例えば、そこからの要求がサービスで受け取られるソースの正確な記録のため等の）いくつかの理由から、たとえ同じ送信元ＩＰアドレスが要求で示されることがあっても、サービスが異なるＩＶＮからの要求を区別できることが役立つ場合がある。

【００５２】

図７は、少なくともいくつかの実施形態に従って、同じプライベートＩＰアドレスを有する計算インスタンスからサービスで受信される要求を区別するためのＩＶＮ識別子及びＰＡＥ識別子の使用の例を示す。示されるように、それぞれのＩＶＮ７０２Ａ及び７０２ＢはクライアントＣ１によってセットアップされてよく、ＩＶＮ７０２Ａはクライアントの組織のエンジニアリング部による使用のためにセットアップされ、ＩＶＮ７０２Ｂは組織のマーケティング部による使用のためにセットアップされる。両方の組織とも、示される例で同じ公にアクセス可能なストレージサービス「ＳｔｏｒａｇｅＳｖｃ１」に記憶されるオブジェクトにアクセスする必要がある場合がある。ＰＡＥ７５０Ａは、ＩＶＮ７０２ＡからＳｔｏｒａｇｅＳｖｃ１にアクセスするために確立されてよく、ＰＡＥ７５０ＢはＩＶＮ７０２ＢからＳｔｏｒａｇｅＳｖｃ１にアクセスするために確立されてよい。

【００５３】

クライアントＣ１は（例えば、故意にまたは偶然に）同じプライベートＩＰアドレス１０．４．５．６をＩＶＮ７０２Ａの計算インスタンス７１０Ａに、及びＩＶＮ７０２Ｂの計算インスタンス７１０Ｋに割り当ててよい。ＳｔｏｒａｇｅＳｖｃ１に向けられるサービス要求は、両方の計算インスタンス７１０Ａと７１０Ｋで生成されてよい。上述されたプロバイダネットワークのトンネリング手段で実装されてよいカプセル化プロトコルに従って、ＳｔｏｒａｇｅＳｖｃ１のオブジェクトＸを読み取る、ＩＶＮ７０２Ａからの要求を示すカプセル化サービス要求パケット７７４Ａは、フロントエンドノード７７１に送信されてよい。カプセル化パケット７７４Ａは要求の元のソースとしてプライベートＩＰアドレス１０．４．５．６を示してよく、要求を送るために使用されるＩＶＮ識別子７０２Ａ及びＰＡＥ７５０Ａの符号化を含んでもよい。同様に、サービスのオブジェクトＹを読み取る要求を示すカプセル化パケット７７４Ｂは、フロントエンドノード７７１で受信されてよい。また、パケット７７４Ｂは、ソースインスタンスのプライベートＩＰアドレス（パケット７７４Ａに示されるものと同一の１０．４．５．６）、ソースＩＶＮ（７０２Ｂ）、及び示される実施形態でその要求を送るために使用されるＰＡＥ７５０Ｂも示してよい。

【００５４】

フロントエンドノード７７１（及び／または要求された作業が実行されるバックエンドノード７７３）は、パケット７７４Ａ及び７７４Ｂに示される送信元ＩＰアドレスが同一であっても、受信されたパケットに含まれるＩＶＮ及び／またはＰＡＥ識別情報を使用して要求のソースを区別できてよい。したがって、Ｘを読み取る要求が受信されたか、または処理されたタイムスタンプＴ１、要求側計算インスタンスのプライベートＩＰアドレス１０．４．５．６、ＩＶＮ７０２Ａ及びＰＡＥ７５０Ａの識別子を示すログレコード７３３Ａが（ＦＥノードまたはＢＥノードのどちらかによって）生成されてよい。受信または処理のタイムスタンプＴ２、送信元ＩＰアドレス１０．４．５．６、並びにＩＶＮ７０２Ｂ及びＰＡＥ７５０Ｂの識別子を示す類似するログレコード７３３ＢはＹを読み取る要求のために生成されてよい。いくつかの実施形態では、要求のソースの曖昧さをなくすためにはどちらか１つで十分である場合があるので、ＩＶＮの識別子または識別子ＰＡＥだけがログレコードに（またはカプセル化パケット）に含まれてよい。

【００５５】

トンネリング手段が上述されたようにカプセル化パケット７７４のソースヘッダの中に

ＩＶＮ識別子またはＰＡＥ識別子を取り込む実施形態では、異なるＩＶＮからのトラフィックが、（フロントエンドノード７７１及び／またはバックエンドノード７７３等の）サービス側ノードが必ずしもソースヘッダのコンテンツを解析できない可能性がある状況でも曖昧さをなくしてよいことに留意されたい。例えば、サードパーティサービスがＰＡＥベースのルーティングを使用するために登録され、ＩＰｖ６がカプセル化のために使用されている場合、サードパーティサービスのノードは、ＩＰｖ６ヘッダのどの特定のビットがソースＩＶＮ情報またはソースＰＡＥ情報を符号化するために使用されるのかを認識していないことがある。ただし、ＩＶＮ７０２Ａからのパケット Ｐ１のためのＩＰｖ６ソースヘッダはＩＶＮ７０２Ｂからのパケット Ｐ２のためのＩＰｖ６ソースヘッダとは異なるため、サードパーティサービスノードは、ＩＶＮ識別子及び／またはＰＡＥ識別子に関する詳細がサードパーティサービスノードで確かめられない場合にも、Ｐ１及びＰ２が異なるソースからであることを少なくとも判断できるだろう。言うまでもなく、サードパーティサービスノードが図６に示される方針に類似するアクセス制御方針を実装することを担い、アクセス制御方針が特定のＩＶＮまたは特定のＰＡＥと関連付けられる場合、サードパーティサービスノードはＩＶＮ／ＰＡＥ識別子を入手する必要がある場合がある。

【００５６】

プライベートエイリアスエンドポイントのための方法

図８は、少なくともいくつかの実施形態に従って、ＰＡＥを構成するために実行されてよい操作の態様を示す流れ図である。要素８０１に示されるように、１つまたは複数の分離仮想ネットワークは、例えば仮想コンピューティングサービスのリソースを使用し、プロバイダネットワークでクライアントＣ１の代わりにセットアップされてよい。各ＩＶＮは、クライアントが（サブネットセットアップ、ＩＰアドレス割当て等の）内部ネットワーキング構成選択を行うことができる計算インスタンス等のリソースのなんらかのセットを含んでよい。例えば、クライアントは、所与のプライベートＩＰアドレスがＩＶＮの外のリソースに関して一意であることを確認する必要なく、プライベートＩＰアドレス（ＩＶＮの外で宣伝されないアドレス）を計算インスタンスの仮想ネットワークインタフェースに割り当ててよい。クライアントが２つの異なるＩＶＮ、ＩＶＮ１及びＩＶＮ２で同じプライベートＩＰアドレス「ａ．ｂ．ｃ．ｄ」を使用することを希望する場合、そのアドレスは、例えばＩＶＮ１の計算インスタンスＣＩ１及びＩＶＮ２の異なる計算インスタンスＣＩ１に割り当てられてよい。ＩＰアドレスの一意性は少なくともいくつかの実施形態では所与のＩＶＮの中でまだ必要とされることがある‐例えば、同じＩＰアドレスは、同じＩＶＮの中で起動される２つのインスタンスに割当て可能ではないことがある‐ことに留意されたい。

【００５７】

示される実施形態では、仮想コンピューティングサービスは、クライアントが、ＩＶＮと関連付けられたプライベートエンドポイントエイリアス（ＰＡＥ）を使用し、公にアクセス可能なサービス（例えば、プロバイダネットワーク事業者によって実装されるストレージサービスまたはデータベースサービス、及び／またはプロバイダネットワークの他のカスタマによって実装されるサードパーティサービス）にプライベートＩＰアドレスを有するＩＶＮ計算インスタンスからサービス要求を提出できるようにしてよい。要素８０４に示されるように、ＣＩの代わりにＩＶＮ１のために確立された特定のＰＡＥ（ＰＡＥ１）を表すメタデータレコードは、例えば仮想コンピューティングサービスの構成マネージャ構成要素またはプロバイダネットワークによって作成され、記憶されてよい。少なくともいくつかの実施態様では、ＰＡＥ１が作成されるときに（例えば、Ｃ１からのプログラム要求に応えて）、ＰＡＥ１は任意の特定のサービスに関連付けられるか、または結び付けられる必要はない。ＩＶＮ１と関連付けられるルートテーブルの中で、ＰＡＥ１は、例えば、要素８０７に示されるように、選択されたサービスがＰＡＥ１に割り当てられる別個の構成ステップの後に最終的に、ＩＶＮ１の中で生じ、プロバイダネットワークの他の場所で（つまり、ＩＶＮ１の外で）実装される選択されたサービスに向けられるネットワークトラフィックのルートターゲットとして示されてよい。

【００５８】
少なくともいくつかの実施形態では、いくつかのサービスが、例えば、プロバイダネットワーク事業者が、ＩＶＮ端部でプライベートＩＰアドレスを有するインスタンスと、サービス端部でパブリックＩＰアドレスを有するサービスノードとの間でパケットを伝送するために使用されるカプセル化プロトコルを実装するために必要とされることがある（トンネリング手段等の）構成要素をセットアップし、試験した／検証した後に、ＰＡＥサポートに登録された可能性がある。また、サービスのパブリックＩＰアドレスは、いくつかの実施形態では、トンネリング手段及び／またはＩＶＮのインスタンスホストでの仮想化管理構成要素にアクセス可能な構成データベースの中で検証され（必要に応じて更新）される必要がある場合がある。少なくとも一実施形態で、クライアントＣ１が使用可能なプログラムインタフェースは、クライアントが、ＰＡＥ１にサービスＳｖｃ１を割り当てるとき（要素８０７）に係る登録されるセットの中からサービスを選択できるようにしてよい‐すなわち、クライアントは事前に承認されたサービスをそのＩＶＮのためにセットアップされたＰＡＥに関連付けることを許されるにすぎないことがある。一実装態様では、ＰＡＥ１等のＰＡＥとＳｖｃ１等のサービスとの間の関連付けは、ＰＡＥの「サービス」属性の値を設定することによってＩＶＮ構成データベースの中で表されてよい。

【００５９】
１つまたは複数のアクセス方針は、いくつかの実施形態でＰＡＥ１等の所与のＰＡＥと関連付けられてよい（要素８１０）。アクセス方針は、例えば、ＰＡＥ１を使用し、許可されるもしくは禁止される操作またはサービス要求のタイプ、ＰＡＥ１を介してアクセスが与えられるオブジェクトタイプ、方針規則が適用する本人（例えば、ユーザーまたはグループ）、方針規則が適用する期間等を示してよい。いくつかの実施形態では、クライアントＣ１は、例えばプログラムインタフェースを使用し、ＰＡＥ１に対する好みのアクセス方針を示してよい。デフォルトアクセス方針は、クライアントが方針を示さない場合、ＰＡＥに対しいくつかの実装態様で適用されてよい。また、方針はいくつかの実装態様ではＰＡＥの属性として表されてもよい。複数の方針を所与のＰＡＥに割り当てることができるいくつかの実施形態では、構成マネージャは異なる方針間の矛盾を検出することを担ってよい。例えば、ある方針は特定のオブジェクトに対する特定のタイプの操作を許してよい。一方、別の方針はそのタイプの操作を禁止してよい。いくつかの実施態様では、構成マネージャは、クライアントが矛盾する方針の中で優先順位を付けるまたは矛盾を取り除くことを要求してよい。他の実施形態では、構成マネージャはいくつかのデフォルトの優先順位で（例えば、最も最近に適用された方針がデフォルトでより古い方針を無効にする）指定された方針を単に適用してよく、矛盾は相応して解決されてよい。

【００６０】
宛先がＳｖｃ１であるトラフィックのターゲットとしてのＰＡＥ１を示すルートテーブルエントリは、（例えば、プログラムインタフェースを使用して提出された要求を介してＣ１によって）作成され、示される実施形態ではＩＶＮ１の１つまたは複数のサブネットにアタッチされてよい（要素８１３）。ルートテーブルエントリのためのソース及び宛先として特定のＩＰアドレス範囲を指定する代わりに、サービスの登録名が宛先として示されてよく、ＰＡＥ１が作成されたときにＰＡＥ１に割り当てられた名前または識別子がターゲットとして示されてよく、このようにしてクライアントＣ１の観点からＩＶＮ１とＳｖｃ１との間のルート管理を大幅に簡略化する。ルートテーブルエントリがアタッチされた後、サブネットのインスタンスとＳｖｃ１との間のトラフィックの流れが始まってよい。

【００６１】
少なくともいくつかの実施形態では、１つまたは複数のＰＡＥ（例えば、ＰＡＥ１）に割り当てられたサービス（例えば、Ｓｖｃ１）と関連付けられたパブリックＩＰアドレスのセットは経時的に変化する可能性がある。Ｓｖｃ１等の登録されたサービスの制御プレーンまたは管理構成要素、及び／または仮想コンピューティングサービスの構成マネージャは、係るアドレスが示される実施形態で使用されてよい構成要素に、パブリックＩＰア

ドレスのリスト及び／または他のＰＡＥ関係の構成情報に対する更新を伝搬することを担ってよい（要素８１６）。係る更新は、例えば上述された種類のカプセル化プロトコルが実装されるトンネリング手段からアクセス可能な構成データベース、及び／またはＩＶＮインスタンスホストの仮想化管理構成要素からアクセス可能なデータベースに対して行われてよい。

【００６２】

図９は、少なくともいくつかの実施形態に従って、計算インスタンスから公にアクセス可能なサービスにパケットを送信するためのトンネリングプロトコルの使用を示す流れ図である。要素９０１に示されるように、アクセスされるサービスＳｖｃ１パブリックＩＰアドレス「Ａｄｄｒ１」は、ＰＡＥ（ＰＡＥ１）がＳｖｃ１への／からのトラフィックのために確立されたＩＶＮ（ＩＶＮ１）で実装される計算インスタンスＣＩ１で（例えば、ＤＮＳクエリーを使用し）決定されてよい。計算インスタンスＣＩ１で、本体がサービス要求ＳＲ１の少なくとも一部分を示すベースラインパケットＢＰ１が生成されてよい（要素９０４）。ＣＩ１のプライベートＩＰアドレスはＢＰ１の送信元アドレスとして示されてよく、Ａｄｄｒ１は宛先として示されてよい。ＢＰ１は、例えばＣＩ１にアタッチされる仮想ネットワークインタフェースを使用し、ＣＩ１からＡｄｄｒ１に向かって送信されてよい。

【００６３】

示される実施形態では、ベースラインパケットＢＰ１は、ＣＩ１が実行するインスタンスホストで、ハイパーバイザまたは特権をもつドメインオペレーティングシステム等の仮想化管理構成要素（ＶＭＣ）によって妨害されることがある（要素９０７）。ＶＭＣは、例えば（仮想ネットワークインタフェース等の）仮想化されたリソースとインスタンスホストの（物理ネットワークインタフェースカード等の）ハードウェア構成要素との間で手段としての機能を果たしてよい。ＶＭＣは、ＢＰ１の宛先アドレス及び／またはＣＩ１からＳｖｃ１へのトラフィックがＰＡＥにターゲットとされる必要があることを示すルートテーブルエントリ等のＰＡＥ構成情報の１つまたは複数の要素を分析してよい。少なくとも一実施形態では、ＶＭＣはＳｖｃ１のパブリックＩＰアドレスのリストでＡｄｄｒ１を探してもよいか、または代わりに探すことができてよい。構成情報の調査に基づいて、ＶＭＣは、ＢＰ１から引き出される第１のカプセル化パケットＥＰ１が、例えばブリッジネットワークを介してＡｄｄｒ１に向かう追加の伝送のためにトンネリング手段に向かって送信されると判断できてよい（要素９１０）。トンネリング手段は、例えば、内部ブリッジネットワークを介して、（ＣＩ１等の）仮想コンピューティングサービスのノードと、（Ｓｖｃ１等の）公にアクセス可能なサービスのノードとの間でトラフィックを送るためにセットアップされたマルチノード群の内の１つのノードであってよい。第１のカプセル化パケットＥＰ１は、いくつかの実施形態で仮想コンピューティングサービスの多様な構成要素の中でのルーティングのために使用される第１のカプセル化プロトコルＰ１に従ってフォーマットされてよい。ＥＰ１の中で、（ＢＰ１のソースヘッダ及び宛先ヘッダを含んだ）ＢＰ１は本体構成要素の中で組み込まれてよく、１つまたは複数のＰ１ヘッダはいくつかの実施態様ではＶＭＣによって追加されてよい。ＥＰ１の追加されたヘッダは、例えばソースとしてＶＭＣ（またはＶＭＣが実行するインスタンスホスト）を、及び宛先としてトンネル群（または特定のトンネリング手段）を示してよい。一実施態様では、ＩＶＮ１及び／またはＰＡＥ１の識別子は、ＥＰ１ヘッダに含まれてもよい。いくつかの実施形態では、ＥＰ１ヘッダは必ずしもＰＡＥ１の識別子を示さないことがあるが、ＥＰ１がＰＡＥと関連付けられたパケットであることを示すフィールドを含んでもよい。

【００６４】

ＥＰ１は、最終的には、例えば仮想コンピューティングサービスのネットワークの１つまたは複数のホップを横切った後、示される実施形態でトンネリング手段に達してよい。トンネリング手段で、ＢＰ１は抽出されてよく、ＥＰ１ヘッダのコンテンツは調べられてよい。ＢＰ１の送信元アドレス及び宛先アドレス（つまり、ＣＩ１のプライベートＩＰアドレス及びＳｖｃ１アドレスＡｄｄｒ１）は、第２のカプセル化パケットＥＰ２で指定さ

れる、トンネリングプロトコルＰ２のマッピングデータベースで対応する送信元アドレス及び宛先アドレスを探すために使用されてよい（要素９１３）。いくつかの実施形態では、ベースラインパケットＢｐ１（及び／またはＥＰ）はＩＰｖ４に従ってフォーマットされてよい。一方、トンネリングプロトコルで使用される送信元アドレス及び宛先アドレスは、例えばＳＩＩＴまたは類似するＩＰｖ４－ＩＰｖ６変換プロトコルを使用し、ＩＰｖ６に従ってフォーマットされてよい。他の実施形態では、トンネリングプロトコルは専有であってよく、例えば、ＩＰｖ６様式のアドレスは必ずしも使用される必要はない、ＩＰｖ６アドレスがトンネリングプロトコルのために使用されないいくつかの実施形態で、ベースラインパケットのカプセル化は、ＴＣＰオプションヘッダ等の追加のＩＰｖ４ヘッダを使用し、実行されてよい。少なくとも１つの実施形態では、（例えば、ＵＤＰメッセージの中にベースラインパケットを取り込むことによって）ＵＤＰ（ユーザーデータグラムプロトコル）カプセル化が使用されてよい。ＥＰ１ヘッダは示される実施形態ではトンネリング手段でＥＰ２ヘッダによって削除され、置換されてよい。図４に示されるように、いくつかの実施形態では、１つまたは複数のＥＰ２ヘッダはそれぞれ（ａ）（例えば、３２ビットのＢＰ１送信元ＩＰアドレスを符号化するために１２８ビットのＥＰ２送信元アドレスヘッダの内の３２ビットを使用し、３２ビットのＢｐ１宛先ＩＰアドレスを符号化するために１２８ビットのＥＰ２宛先アドレスフィールドの内の３２ビットを使用する）ＢＰ１送信元アドレス及び宛先アドレス、及び／または（ｂ）ソースＩＶＮ（ＩＶＮ１）及びルーティングのために使用されるＰＡＥ（ＰＡＥ１）の識別子を示すまたは符号化してよい。いくつかの実装態様では、ＩＰ２ヘッダに含まれてよいＰＡＥ識別子は、それ自体対応するＩＶＮの識別子の符号化を含んでよく、したがってＰＡＥ識別子は、要求が受信されたＩＶＮ及びＰＡＥの両方ともを決定するためにサービスで使用可能であってよい。少なくとも１つの実施態様では、ＢＰ１宛先アドレスは、ＢＰ１宛先アドレスが使用されるのか、それともＥＰ２宛先アドレスが使用されるのかに関係なく、ロードバランサが同じサービスフロントエンドノードに所与のパケットを送るように（例えば最低３２ビットで）、それぞれＥＰ２ソースヘッダ及び宛先ヘッダの中に含まれてよい。

【００６５】

ＥＰ２は、例えばプロバイダネットワークの中で確立されたブリッジネットワークの選択された経路を介して、トンネリング手段からＳｖｃ１のフロントエンドノードに送信されてよい（要素９１６）。いくつかの実施形態では、ＥＰ２は、プロバイダネットワーク事業者によって管理される及び／または所有されるプライベートネットワークリンクだけを使用し、Ｓｖｃ１に達してよい。他の実施形態では、ＥＰ２のために使用される経路はパブリックネットワークリンクを含んでよい（例えば、パケットはプロバイダネットワークの外のネットワークデバイスを通過してよい、またはプロバイダネットワーク事業者以外のエンティティによって管理されてよい／所有されてよい）。Ｓｖｃ１のフロントエンドノードで、サービス要求ＳＲ１を示すＢＰ１コンテンツが抽出されてよい（要素９１９）。さらに、ソースインスタンスＣＩ１の一意の識別は、例えば同じＩＰアドレスが、他のＩＶＮの他のインスタンスに割り当てられるようにＣＩ１に割り当てられるとしても、ＥＰ２ヘッダを使用し、サービスで可能であってよい。例えば、１つまたは複数のＥＰ２ヘッダから抽出されてよいＢＰ１のコンテンツを送るために使用されるソースＩＶＮ及び／またはＰＡＥの識別子は、各ＩＶＮが特定のプライベートＩＰアドレスを有する単一のインスタンスだけを含んでよい実施形態では、係るインスタンスからのサービス要求の曖昧さをなくすために使用されてよい。少なくともいくつかの実施形態では、サービス要求ＳＲ１は、ＰＡＥと関連付けられた１つまたは複数のアクセス制御方針に従ってサービス側で確証されてよい。アクセス許可がチェックされた後、要求された操作が、例えばサービスＳｖｃ１のバックエンドノードで実行されてよい。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タイプの要求に応答が生成されてよく、応答は逆の順序で同じプロトコルを使用し、ＣＩ１に向かって逆方向で送信されてよい。例えば、コンテンツがバックエンドサービスノードで生成されるベースライン応答は、サービスのフロントエンドノードでトンネリングプロトコルＰ２に従ってフォーマットされ、仮想コンピューティ

ングサービスのトンネリング手段にブリッジネットワークを横切って送信されてよい。トンネリング手段で、応答は抽出され、第１のカプセル化プロトコルＰ１に従ってフォーマットされ、ＣＩ１が実行するインスタンスホストでＶＭＣに渡されてよい。ＶＭＣはベースライン応答を抽出し、ＣＩ１に応答を提供してよい。

【００６６】

多様な実施形態では、図８及び図９の流れ図に示される操作以外の操作は、プライベートエイリアスエンドポイントをサポートするための技法の少なくともいくつかを実装するために使用されてよいことに留意されたい。示される操作のいくつかはいくつかの実施形態では実装されないことがあり、図８もしくは図９に示されるのとは異なる順序でもしくは異なる構成要素で、または順次的よりむしろ並行して実装されてよい。少なくとも１つの実施形態で、トンネリング手段及びＶＭＣについて説明される機能性は例えば結合されてよい‐例えば、パケットを、別個の手段による追加のカプセル化なしに選択された経路を介してサービスに送信できるようにするトンネリングプロトコルがＶＭＣで実装されてよい。別の実施形態では、ベースラインパケットは、ＶＭＣによってカプセル化されずに、計算インスタンスから、または非仮想化コンピューティング装置からトンネリング手段に送信されてよい。

【００６７】

使用事例

分離仮想ネットワークの計算インスタンスから公にアクセス可能なサービスへ向けられたトラフィックのルーティングターゲットとしての機能を果たすためにプライベートエイリアスエンドポイントを確立する上述された技法はさまざまな状況で役に立ってよい。より多くの分散型アプリケーションがプロバイダネットワーク環境に移動され、ネットワークをベースにした攻撃者の複雑化が増すにつれ、公衆インターネットで生じるネットワーク侵入からクライアントアプリケーションを守り、分離する必要性も高まっている。分離仮想ネットワークは、クライアントが公衆インターネットに対して宣伝されないか、または公衆インターネットからアクセスできない計算インスタンスにプライベートＩＰアドレスを割り当てることを可能にするが、要求が係るインスタンスからのパブリックＩＰアドレスで生じることを期待するサービスにアクセスすることは問題を呈することもある。プライベートエイリアスエンドポイントは、潜在的なセキュリティの妥協を必要とせず、ＶＰＮ接続を介した要求の非効率的な／高価なルーティングなしに係るサービス要求を送信できるようにしてよい。

【００６８】

本開示の実施形態は、以下の条項を考慮して説明できる。

１．システムであって、

プロバイダネットワークの構成マネージャと、

インスタンスホストの仮想化構成要素（ＶＭＣ）であって、クライアントの代わりに確立された第１の分離仮想ネットワーク（ＩＶＮ）の第１の計算インスタンスが前記インスタンスホストでインスタンス化され、前記第１の計算インスタンスが前記クライアントによって選択されたプライベートネットワークアドレスを有する、前記仮想化管理構成要素（ＶＭＣ）と、

トンネリング手段と、

を備え、

前記構成マネージャが、前記第１のＩＶＮで生じ、特定のサービスに向けられるパケットのルーティングターゲットとして第１のプライベートエイリアスエンドポイント（ＰＡＥ）の指定を表す第１のメタデータエントリを記憶するように構成され、前記パケットが公に宣伝されたネットワークアドレスを送信元アドレスとして示すことなく前記特定のサービスに送達され、

前記ＶＭＣが前記第１のメタデータエントリの調査に少なくとも部分的に基づいて、前記ＶＭＣで妨害されたベースラインパケットから引き出される第１のカプセル化パケットを前記トンネリング手段に送信するように構成され、前記ベースラインパケットが前記第

１の計算インスタンスで生成され、前記特定のサービスの公に宣伝されたネットワークアドレスに向けられ、
前記トンネリング手段が、
トンネリングプロトコルに従って、前記第１のカプセル化パケットから第２のカプセル化パケットを生成するように構成され、前記第２のカプセル化パケットが前記第１のＩＶＮをソースＩＶＮとして示すヘッダ構成要素を含み、
前記特定のサービスの１つまたは複数のノードの内の第１のノードに前記第２のカプセル化パケットを送信するように構成され、前記第１のノードが（ａ）前記第２のカプセル化パケットから、前記第１のＩＶＮの識別子及び前記プライベートネットワークアドレスを決定する、及び（ｂ）前記ベースラインパケットに示されるサービス要求を遂行するために１つまたは複数の操作を開始するように構成される、
前記システム。
【００６９】
２．前記第２のカプセル化パケットがＩＰｖ６（インターネットプロトコルのバージョン６）に従ってフォーマットされ、前記ベースラインパケットがＩＰｖ４（前記インターネットプロトコルのバージョン４）に従ってフォーマットされる、条項１に記載のシステム。
【００７０】
３．前記特定のサービスが複数のオブジェクトに対する複数の操作タイプをサポートし、（ａ）前記特定のサービスの前記第１のノードまたは（ｂ）前記ＶＭＣの内の１つまたは複数が、
前記１つまたは複数の操作の前に、前記サービス要求が前記第１のＰＡＥに割り当てられた第１のアクセス制御方針に準拠しているかどうかの判断を開始するように構成され、前記第１のアクセス制御方針が、前記第１のＰＡＥをルーティングターゲットとして使用し、提出された要求に関して、（ａ）前記複数の操作タイプの許可された操作タイプ、（ｂ）前記複数の操作タイプの禁止された操作タイプ、（ｃ）前記複数の操作タイプの内の特定の操作タイプが許可される時間間隔、または（ｄ）前記複数の操作タイプの内の特定の操作タイプが許可される前記複数のオブジェクトの特定のオブジェクトの内の１つまたは複数を示す、
条項１に記載のシステム。
【００７１】
４．前記構成マネージャが、
前記第１のＩＶＮで生じる追加のパケットのルーティングターゲットとして第２のＰＡＥを指定するようにさらに構成され、前記追加のパケットが異なるサービスに送達される、
条項１に記載のシステム。
【００７２】
５．前記構成マネージャが、
前記クライアントの要求で、前記クライアントの第２のＩＶＮで確立された第２の計算インスタンスに前記プライベートネットワークアドレスを割り当て、
前記第２のＩＶＮで生じ、前記特定のサービスに向けられるトラフィックを送るために使用される第２のＰＡＥを確立する
ようにさらに構成され、
前記サービスの前記第１のノードが、
前記トンネリング手段によって生成される特定のカプセル化ヘッダの調査に基づいて、前記第１のノードで抽出された特定のベースラインパケットが前記第１の計算インスタンスで生成されたのか、それとも前記第２の計算インスタンスで生成されたのかを判断するように構成される、
条項１に記載のシステム。
【００７３】

６．方法であって、
プロバイダネットワークのトンネリング手段で、第１のプライベートエイリアスエンドポイント（ＰＡＥ）が、クライアントの代わりに確立された第１の分離仮想ネットワーク（ＩＶＮ）で生じるトラフィックのためのルーティングターゲットとして指定されたと判断することであって、前記トラフィックが特定の公にアクセス可能なサービスに送達される、判断することと、
前記トンネリング手段で、前記第１のＩＶＮの第１の計算インスタンスから前記特定の公にアクセス可能なサービスの公に宣伝されたネットワークアドレスに向けられるベースラインパケットを受信することと、
前記トンネリング手段によって、（ａ）前記ベースラインパケットのコンテンツ、及び（ｂ）ソースＩＶＮとしての前記第１のＩＶＮの表示を備えるカプセル化パケットを前記特定のサービスの第１のノードに送信することと、
を含む、前記方法。
【００７４】
７．前記カプセル化パケットがＩＰｖ６（インターネットプロトコルのバージョン６）に従ってフォーマットされ、前記ベースラインパケットがＩＰｖ４（前記インターネットプロトコルのバージョン４）に従ってフォーマットされる、条項６に記載の方法。
【００７５】
８．前記特定のサービスが複数のオブジェクトに対する複数の操作タイプをサポートし、
前記クライアントから前記第１のＩＶＮの構成マネージャで、前記第１のＰＡＥに第１のアクセス制御方針を適用する要求を受信することであって、前記第１のアクセス制御方針が、前記第１のＰＡＥを使用し、ルーティングターゲットとして提出される要求に関して、（ａ）前記複数の操作タイプの許可された操作タイプ、（ｂ）前記複数の操作タイプの禁止された操作タイプ、（ｃ）前記複数の操作タイプの内の特定の操作タイプが許可される時間間隔、または（ｄ）前記複数の操作タイプの内の特定の操作タイプが許可される前記複数のオブジェクトの内の特定のオブジェクトの内の１つまたは複数を示す、受信することと、
前記ベースラインパケットに示される特定の要求に従って第１の操作を実行する前に、前記第１の操作が前記第１のアクセス制御方針によって許可されることを検証することと、
をさらに含む、条項６に記載の方法。
【００７６】
９．前記第１のＩＶＮで生じる追加のトラフィックのルーティングターゲットとして第２のＰＡＥを指定することをさらに含み、前記追加のトラフィックが異なるサービスに送達される、条項６に記載の方法。
【００７７】
１０．前記第１の計算インスタンスが前記クライアントの要求で該第１の計算インスタンスに割り当てられた特定のプライベートＩＰアドレスを有し、
前記クライアントの代わりに第２のＩＶＮを確立することであって、前記第２のＩＶＮが第２の計算インスタンスを含む、第２のＩＶＮを確立することと、
前記クライアントの要求で、前記第２の計算インスタンスに前記特定のプライベートＩＰアドレスを割り当てることと、
前記第２のＩＶＮで生じ、前記特定のサービスに向けられるトラフィックを送るために使用される第２のＰＡＥを確立することと、
前記トンネリング手段によって生成されるカプセル化ヘッダの調査に基づいて前記特定のサービスの特定のノードで、前記特定のノードで受信される特定のベースラインパケットが、前記特定のプライベートＩＰアドレスが割り当てられた前記第１の計算インスタンスで生成されたのか、それとも前記特定のプライベートＩＰアドレスが割り当てられた前記第２の計算インスタンスで生成されたのかを判断することと、

をさらに含む、条項６に記載の方法。
【００７８】
１１．前記カプセル化パケットが、前記プロバイダネットワークで実装された特許トンネリングプロトコルに従ってフォーマットされる、条項６に記載の方法。
【００７９】
１２．前記カプセル化パケットが、前記第１のＰＡＥの識別子の表現を含んだヘッダを含む、条項６に記載の方法。
【００８０】
１３．プログラムインタフェースを介して前記プロバイダネットワークの構成マネージャで、前記第１のＰＡＥを生成する要求を前記クライアントから受信することと、
前記要求に応えて前記構成マネージャによって、前記第１のＰＡＥを表すメタデータエントリを記憶することと、
をさらに含む、条項６に記載の方法。
【００８１】
１４．プログラムインタフェースを介して前記プロバイダネットワークの構成マネージャで、ＰＡＥを使用するアクセスのために異なるサービスを登録する要求を受信することと、
前記要求に応えて前記構成マネージャによって、特定のサービスが特定のＰＡＥとの関連付けのために前記クライアントによって選択できるサービスの集合体に前記異なるサービスを追加することと、
をさらに含む、条項６に記載の方法。
【００８２】
１５．前記異なるサービスが、前記プロバイダネットワークのリソースのセットを使用し、前記プロバイダネットワークの異なるクライアントによって実装され、
前記異なるサービスに向けられるベースラインパケットから引き出されるカプセル化パケットのコンテンツを抽出するように構成された特定のフロントエンドノードを含んだ、前記異なるサービスのために１つまたは複数のフロントエンドノードを確立すること、
をさらに含む、条項１４に記載の方法。
【００８３】
１６．１つまたは複数のプロセッサでの実行時、プロバイダネットワークのトンネリング手段を実装するプログラム命令を記憶する非一過性のコンピュータアクセス可能記憶媒体であって、前記トンネリング手段が、
クライアントの代わりに前記プロバイダネットワークで確立された第１の分離仮想ネットワーク（ＩＶＮ）から特定のサービスに向けられるトラフィックのルーティングターゲットとしての第１のプライベートエイリアスエンドポイント（ＰＡＥ）の指定に従って、前記第１のＩＶＮの第１の計算インスタンスで生成されたベースラインパケットを受信するように構成され、前記ベースラインパケットが前記特定のサービスのパブリックＩＰ（インターネットプロトコル）アドレスをその宛先アドレスとして示し、
選択されたトンネリングプロトコルに従って、（ａ）前記ベースラインパケットのコンテンツの少なくとも一部分、及び（ｂ）ソースＩＶＮとして前記第１のＩＶＮを示すヘッダ構成要素を備えるカプセル化パケットを生成し、
前記特定のサービスの第１のノードに前記カプセル化パケットを送信する
ように構成される、前記非一過性のコンピュータアクセス可能記憶媒体。
【００８４】
１７．前記カプセル化パケットがＩＰｖ６（前記インターネットプロトコルのバージョン６）に従ってフォーマットされ、前記ベースラインパケットがＩＰｖ４（前記インターネットプロトコルのバージョン４）に従ってフォーマットされる、条項１６に記載の非一過性のコンピュータアクセス可能記憶媒体。
【００８５】
１８．前記トンネリング手段が、

第１のＩＶＮとは異なるサービスに向けられるトラフィックのルーティングターゲットとして第２のＰＡＥの指定に従って、前記第１のＩＶＮの第２の計算インスタンスで生成される第２のベースラインパケットの表現を受信するようにさらに構成され、前記第２のベースラインパケットが前記異なるサービスのパブリックＩＰアドレスをその宛先アドレスとして示し、

前記選択されたトンネリングプロトコルに従って、（ａ）前記第２のベースラインパケットのコンテンツの少なくとも一部分、及び（ｂ）ソースＩＶＮとして前記第１のＩＶＮを示すヘッダ構成要素を備える第２のカプセル化パケットを生成し、

前記異なるサービスの異なるノードに前記第２のカプセル化パケットを送信する

ようにさらに構成される、条項１６に記載の非一過性のコンピュータアクセス可能記憶媒体。

【００８６】

１９．前記第１のカプセル化パケットが、前記第１の計算インスタンスのプライベートＩＰアドレスの表示を含み、前記トンネリング手段が、

前記クライアントに代わって確立された第２のＩＶＮから前記特定のサービスに向けられるトラフィックのルーティングターゲットとしての第２のＰＡＥの指定に従って、前記第２のＩＶＮの第２の計算インスタンスで生成された第２のベースラインパケットの表現を受信するようにさらに構成され、前記第２のベースラインパケットが前記特定のサービスの前記パブリックＩＰアドレスをその宛先アドレスとして示し、

前記選択されたトンネリングプロトコルに従って、（ａ）前記第２のベースラインパケットのコンテンツの少なくとも一部分、（ｂ）ソースＩＶＮとして前記第２のＩＶＮを示すヘッダ構成要素、及び（ｃ）前記プライベートＩＰアドレスの表示を備える第２のカプセル化パケットを生成するようにさらに構成され、

前記特定のサービスの前記第１のノードに前記第２のカプセル化パケットを送信するようにさらに構成され、前記特定のサービスの前記第１のノードが、前記第２のカプセル化パケットの調査に基づき、前記第２のベースラインパケットが前記第１の計算インスタンスで生成されたのか、それとも前記第２の計算インスタンスで生成されたのかを判断するように構成される、

条項１６に記載の非一過性のコンピュータアクセス可能記憶媒体。

【００８７】

２０．前記カプセル化パケットが、前記第１のＰＡＥの識別子の表現を含んだヘッダを備える、条項１６に記載の非一過性のコンピュータアクセス可能記憶媒体。

【００８８】

例示的なコンピュータシステム

少なくともいくつかの実施形態では、構成マネージャ、ＶＭＣ、トンネリング手段、公にアクセス可能なサービスのノード等のプライベートエイリアスエンドポイントをサポートするために使用される構成要素の内の１つまたは複数を実装するサーバは、１つもしくは複数のコンピュータアクセス可能媒体を含むまたは１つもしくは複数のコンピュータアクセス可能媒体にアクセスするように構成される汎用コンピュータシステムを含んでよい。図１０は、係る汎用コンピューティング装置９０００を示す。示される実施形態では、コンピューティング装置９０００は、入力／出力（Ｉ／Ｏ）インタフェース９０３０を介して（不揮発性メモリモジュール及び揮発性メモリモジュールの両方を含んでよい）システムメモリ９０２０に結合される１つまたは複数のプロセッサ９０１０を含む。コンピューティング装置９０００は、Ｉ／Ｏインタフェース９０３０に結合されるネットワークインタフェース９０４０をさらに含む。

【００８９】

多様な実施形態では、コンピューティング装置９０００は、１つのプロセッサ９０１０を含んだユニプロセッサシステム、またはいくつかのプロセッサ９０１０（例えば、２、４、８、または別の適切な数）を含んだマルチプロセッサシステムであってよい。プロセッサ９０１０は、命令を実行できる任意の適切なプロセッサであってよい。例えば、多様

な実施形態では、プロセッサ９０１０は、ｘ８６、ＰｏｗｅｒＰｃ、ＳＰＡＲＣ、もしくはＭＩＰＳ　ＩＳＡ、または任意の他の適切なＩＳＡ等のさまざまな命令セットアーキテクチャ（ＩＳＡ）のいずれかを実装する汎用プロセッサまたは組み込みプロセッサであってよい。マルチプロセッサシステムでは、プロセッサ９０１０のそれぞれは、一般に同じＩＳＡを実装してよいが、必ずしも実装しなくてもよい。いくつかの実施態様では、グラフィックスプロセシングユニット（ＧＰＵ）が、従来のプロセッサの代わりに、または従来のプロセッサに加えて使用されてよい。

【００９０】

システムメモリ９０２０は、プロセッサ（複数可）９０１０によってアクセス可能な命令及びデータを記憶するように構成されてよい。少なくともいくつかの実施形態では、システムメモリ９０２０は揮発性部分と不揮発性部分の両方を含んでよい。他の実施形態では、揮発性メモリだけが使用されてよい。多様な実施形態では、システムメモリ９０２０の揮発性部分はスタティックランダムアクセスメモリ（ＳＲＡＭ）、同期ダイナミックＲＡＭ、または任意の他のタイプのメモリ等、任意の適切なメモリ技術を使用し、実装されてよい。（例えば、１つまたは複数のＮＶＤＩＭＭを含んでよい）システムメモリの不揮発性部分の場合、いくつかの実施形態では、ＮＡＮＤフラッシュデバイスを含んだフラッシュベースのメモリデバイスが使用されてよい。少なくともいくつかの実施形態では、システムメモリの不揮発性部分は、スーパーキャパシタまたは他の電力貯蔵装置（例えば電池）等の電源を含んでよい。多様な実施形態では、メムリスタベース抵抗ランダムアクセスメモリ（ＲｅＲＡＭ）、３次元ＮＡＮＤ技術、強誘電体ＲＡＭ、磁気抵抗ＲＡＭ（ＭＲＡＭ）、または多様なタイプの相変化メモリ（ＰＣＭ）のいずれかがシステムメモリの少なくとも不揮発性部分に使用されてよい。示される実施形態では、上述されたそれらの方法、技法、及びデータ等の１つまたは複数の所望される機能を実装するプログラム命令及びデータが、コード９０２５及びデータ９０２６としてシステムメモリ９０２０の中に記憶されて示される。

【００９１】

一実施形態では、Ｉ／Ｏインタフェース９０３０は、プロセッサ９０１０、システムメモリ９０２０、及びネットワークインタフェース９０４０または多様なタイプの永続記憶装置及び／または揮発性記憶装置等の他の周辺インタフェースを含んだ、デバイスの中の任意の周辺装置との間でＩ／Ｏトラフィックを調整するように構成されてよい。いくつかの実施形態では、Ｉ／Ｏインタフェース９０３０は、１つの構成要素（例えば、システムメモリ９０２０）から別の構成要素（例えば、プロセッサ９０１０）による使用に適したフォーマットに変換するために任意の必要なプロトコル、タイミング、または他のデータ変換を実行してよい。いくつかの実施形態では、Ｉ／Ｏインタフェース９０３０は、例えばペリフェラルコンポーネントインターコネクタ（ＰＣＩ）バス規格またはユニバーサルシリアルバス（ＵＳＢ）規格の変形等の多様な周辺バスを通してアタッチされたデバイスのためのサポートを含んでよい。いくつかの実施形態では、Ｉ／Ｏインタフェース９０３０の機能は、例えば、ノースブリッジ及びサウスブリッジ等の２つ以上の別々の構成要素に分割されてよい。また、いくつかの実施形態では、システムメモリ９０２０へのインタフェース等のＩ／Ｏインタフェース９０３０の機能性のいくつかまたはすべてはプロセッサ９０１０の中に直接的に組み込まれてよい。

【００９２】

ネットワークインタフェース９０４０は、コンピューティング装置９０００と、例えば図１から図９に示される他のコンピュータシステムまたはデバイス等、１つまたは複数のネットワーク９０５０にアタッチされた他のデバイス９０６０との間でデータを交換できるように構成されてよい。多様な実施形態では、ネットワークインタフェース９０４０は、例えばイーサネット（登録商標）ネットワークのタイプ等の任意の適切な有線汎用データネットワークまたは無線汎用データネットワークを介する通信をサポートしてよい。さらに、ネットワークインタフェース９０４０は、アナログ音声ネットワークまたはデジタルファイバ通信ネットワーク等の電気通信／電話ネットワークを介して、ファイバチャネ

ルＳＡＮ等のストレージエリアネットワークを介して、または任意の他の適切なタイプのネットワーク及び／またはプロトコルを介して通信をサポートしてよい。

【００９３】

いくつかの実施形態では、システムメモリ９０２０は、対応する方法及び装置の実施形態を実施するための図１から図９について上述されたようにプログラム命令及びデータを記憶するように構成されたコンピュータアクセス可能媒体の一実施形態であってよい。しかしながら、他の実施形態では、プログラム命令及び／またはデータは、異なるタイプのコンピュータアクセス可能媒体で受信、送信、または記憶されてよい。一般的に言えば、コンピュータアクセス可能媒体は、例えばＩ／Ｏインタフェース９０３０を介してコンピューティング装置９０００に結合されるディスクまたはＤＶＤ／ＣＤ等、磁気媒体または光媒体等の非一過性の記憶媒体またはメモリ媒体を含んでよい。また、非一過性のコンピュータアクセス可能記憶媒体は、システムメモリ９０２０または別のタイプのメモリとしてコンピューティング装置９０００のいくつかの実施形態に含まれてよいＲＡＭ（例えば、ＳＤＲＡＭ、ＤＤＲ　ＳＤＲＡＭ、ＲＤＲＡＭ、ＳＲＡＭ等）等の任意の揮発性媒体または不揮発性媒体を含んでもよい。さらに、コンピュータアクセス媒体は伝送媒体、またはネットワークインタフェース９０４０を介して実施され得るように、ネットワーク及び／もしくは無線リンク等の通信媒体を介して伝達される電気信号、電磁信号、もしくはデジタル信号等の伝送信号を含んでよい。図１０に示されるもののような複数のコンピューティング装置の部分またはすべては、多様な実施形態で説明された機能性を実装するために使用されてよい。例えば、さまざまな異なるデバイス及びサーバで実行中のソフトウェア構成要素は機能性を提供するために協調してよい。いくつかの実施形態では、説明される機能性の部分は、汎用コンピュータシステムを使用して実装されることに加えて、または実装される代わりに、ストレージデバイス、ネットワークデバイス、または特殊目的コンピュータシステムを使用し、実装されてよい。本明細書で使用される用語「コンピューティング装置」は、少なくともすべてのこれらのタイプのデバイスを指し、これらのタイプのデバイスに制限されない。

【００９４】

結論

多様な実施形態は、コンピュータアクセス可能媒体に対して上記説明に従って実施される命令及び／またはデータを受信すること、送信すること、または記憶することをさらに含んでよい。一般的に言えば、コンピュータアクセス可能媒体は、例えば、ディスクもしくはＤＶＤ／ＣＤ－ＲＯＭ等、磁気媒体もしくは光媒体、ＲＡＭ（例えば、ＳＤＲＡＭ、ＤＤＲ、ＲＤＲＡＭ、ＳＲＡＭ等の）ＲＡＭ、ＲＯＭ等の揮発性媒体若しくは不揮発性媒体等の記憶媒体またはメモリ媒体、並びに伝送媒体またはネットワーク及び／もしくは無線リンク等の通信媒体を介して伝達される電気信号、電磁信号またはデジタル信号等の伝送信号を含んでよい。

【００９５】

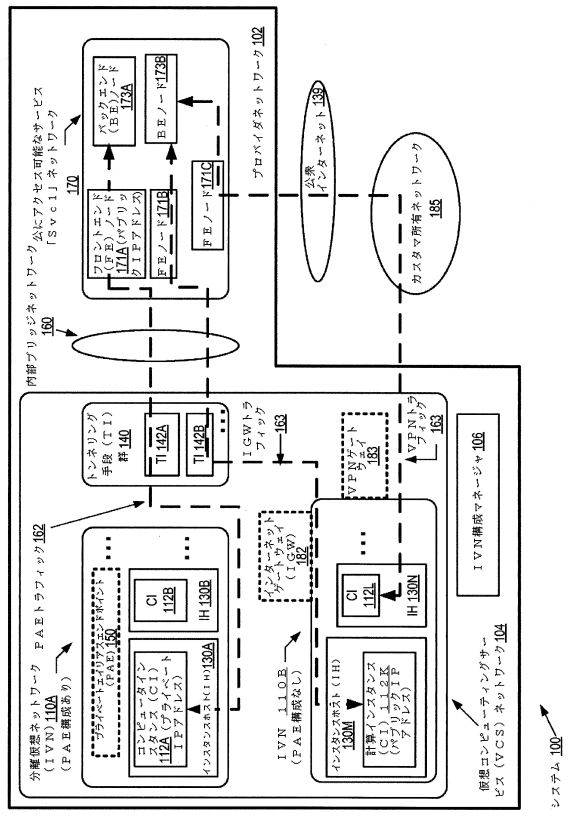
図に示され、本明細書に説明される多様な方法は方法の例示的な実施形態を表している。方法はソフトウェア、ハードウェア、またはその組合せで実装されてよい。方法の順序は変更されてよく、多様な要素が追加され、並べ替えられ、結合され、省略され、修正される等してよい。

【００９６】

多様な変更形態及び変更は、本開示の利益を有する当業者に明らかになるように行われてよい。すべての係る変更形態及び変更を、したがって制限的な意味よりむしろ例示的な意味で考慮される上記説明を包含することが意図される。

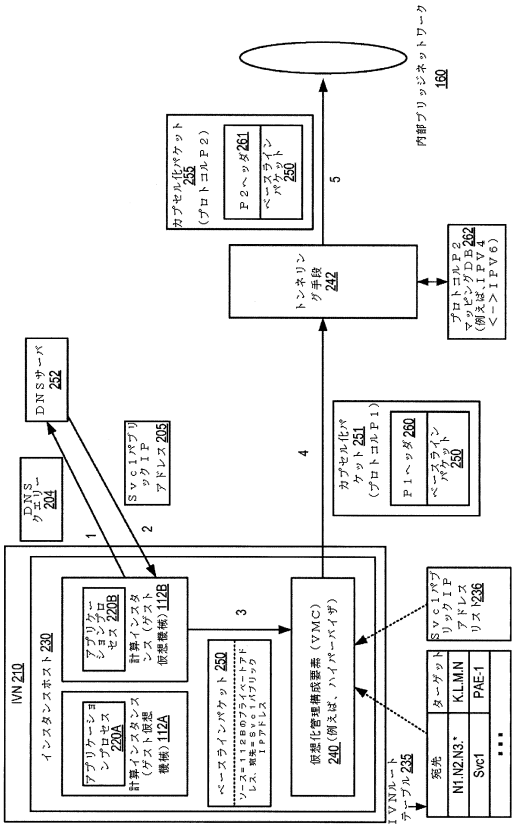
【図１】

図１



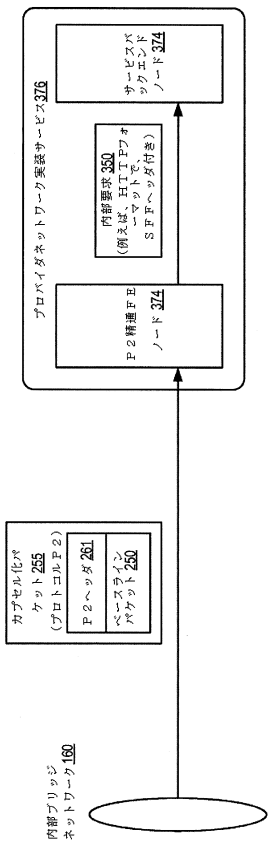

【図２】

図２



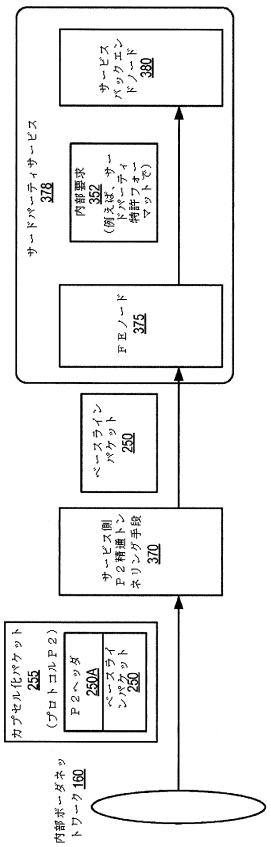

【図３ａ】

図３ａ




【図３ｂ】

図３ｂ



【図４】

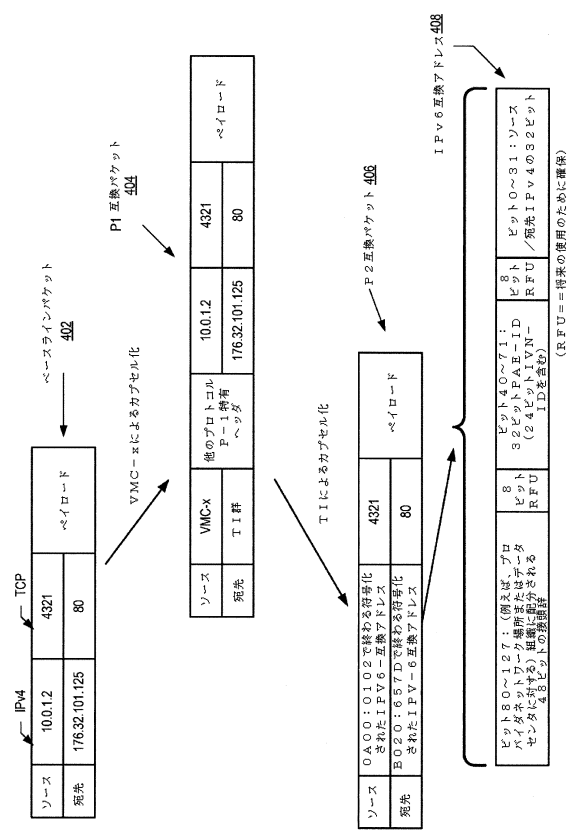


図４
ベースラインパケット
402
P1 互換パケット
404
VMC－xによるカプセル化
TIによるカプセル化
P2互換パケット 406
IPv6互換アドレス408
ソース
宛先
IP4
TCP
10.0.1.2
176.32.101.125
4321
80
ペイロード
VMC-x
TI群
他のプロトコル P－1待有 ヘッダ
ビット0～31：ソース／宛先IPv4の32ビット
8ビット RFU
ビット40～71：32ビットPAE－ID（24ビットIVN－IDを含む）
ビット80～127：（例えば、プロバイダネットワーク場所またはデータセンタに対する）組織に配分される48ビットの識別子
（RFU＝＝将来の使用のために確保）

【図５】

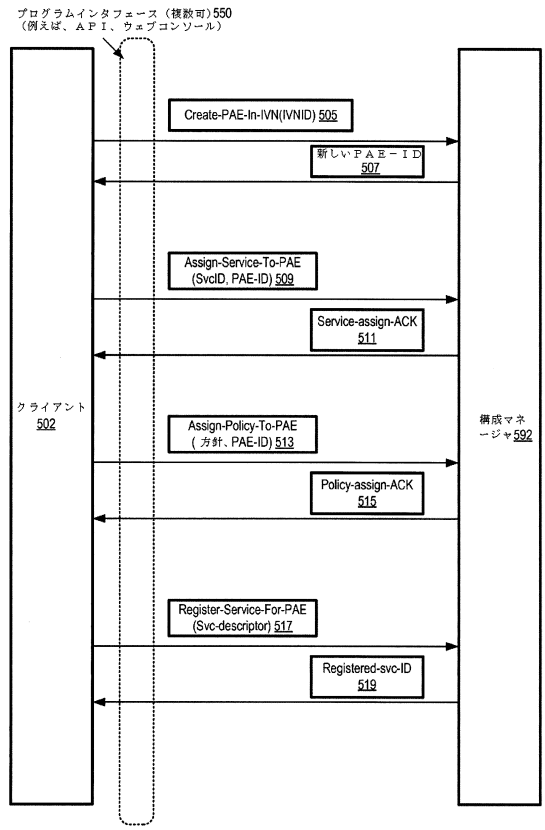


図５
プログラムインタフェース（複数可）550
（例えば、API、ウェブコンソール）
クライアント 502
構成マネージャ 592
Create-PAE-In-IVN(IVNID) 505
新しいPAE－ID 507
Assign-Service-To-PAE (SvcID, PAE-ID) 509
Service-assign-ACK 511
Assign-Policy-To-PAE (方針、PAE-ID) 513
Policy-assign-ACK 515
Register-Service-For-PAE (Svc-descriptor) 517
Registered-svc-ID 519

【図６】

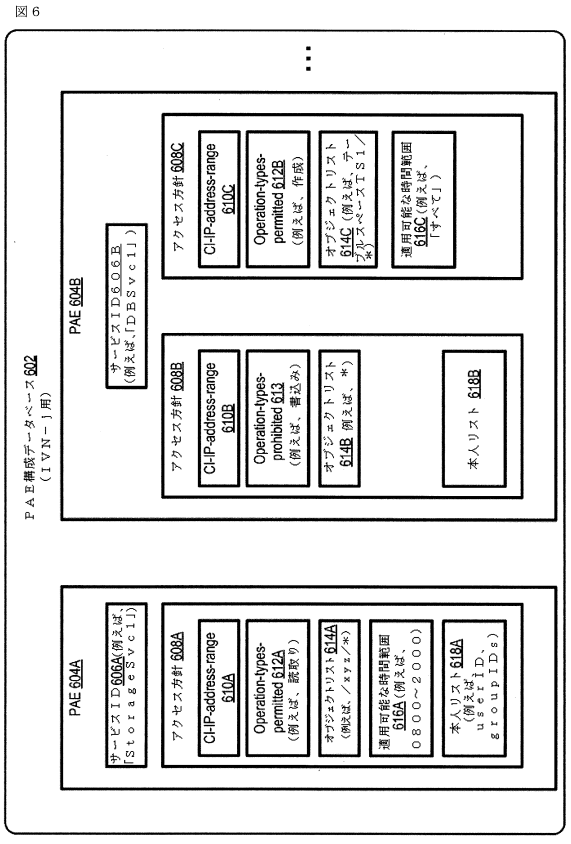


図６
PAE構成データベース 602
（IVN－1用）
PAE 604A
サービスID 606A（例えば、「StorageSvc1」）
アクセス方針 608A
CI-IP-address-range 610A
Operation-types-permitted 612A（例えば、読取り）
オブジェクトリスト 614A（例えば、／メッセージ）
適用可能な時間範囲 616A（例えば、0800～2000）
本人リスト 618A（例えば、userID、groupIDs）
PAE 604B
サービスID 606B（例えば、「DBSvc1」）
アクセス方針 608B
CI-IP-address-range 610B
Operation-types-prohibited 613（例えば、書込み）
オブジェクトリスト 614B（例えば、＊）
本人リスト 618B
アクセス方針 608C
CI-IP-address-range 610C
Operation-types-permitted 612B（例えば、作成）
オブジェクトリスト 614C（例えば、テーブスペースTS1／＊）
適用可能な時間範囲 616C（例えば、「すべて」）

【図７】

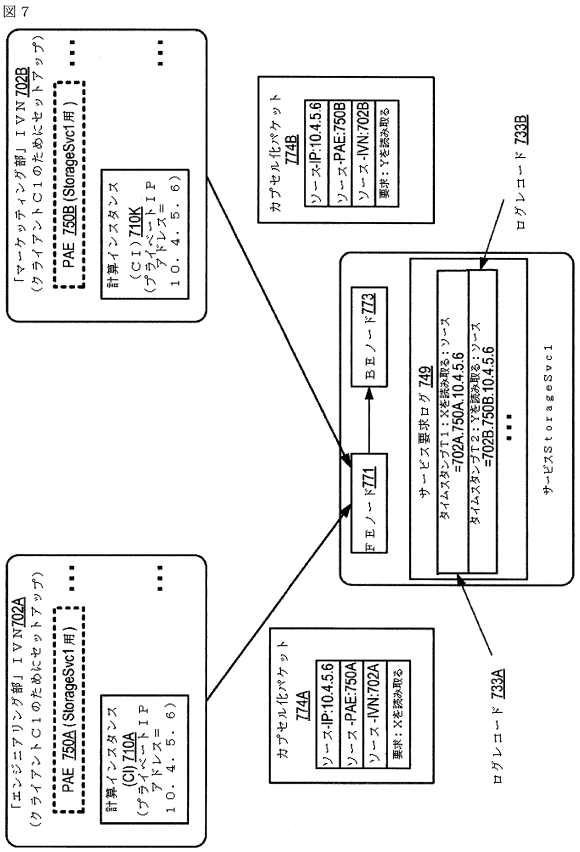
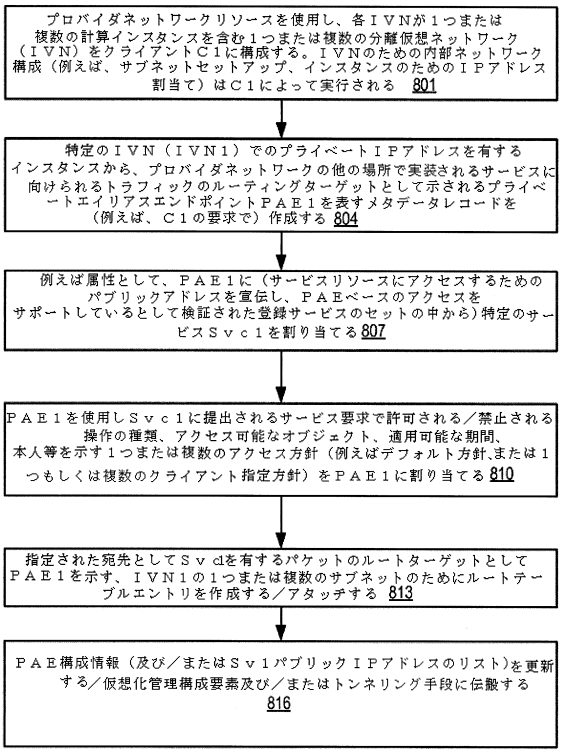


図７
「エンジニアリング部」IVN 702A
（クライアントC1のためにセットアップ）
PAE 750A (StorageSvc1用)
計算インスタンス (CI) 710A（プライベートIPアドレス＝10.4.5.6）
「マーケッティング部」IVN 702B
（クライアントC1のためにセットアップ）
PAE 750B (StorageSvc1用)
計算インスタンス（CI）710K（プライベートIPアドレス＝10.4.5.6）
カプセル化パケット 774A
ソース-IP:10.4.5.6
ソース-PAE:750A
ソース-IVN:702A
要求：Xを読み取る
カプセル化パケット 774B
ソース-IP:10.4.5.6
ソース-PAE:750B
ソース-IVN:702B
要求：Yを読み取る
FEノード 771
BEノード 773
サービス要求ログ 749
タイムスタンプT1：Xを読み取る：ソース＝702A.750A.10.4.5.6
タイムスタンプT2：Yを読み取る：ソース＝702B.750B.10.4.5.6
ログレコード 733A
ログレコード 733B
サービスStorageSvc1

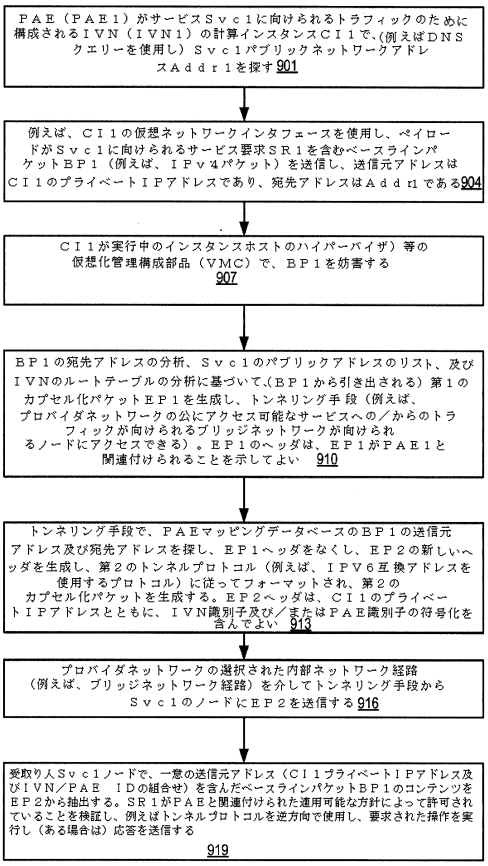
【図８】

図８



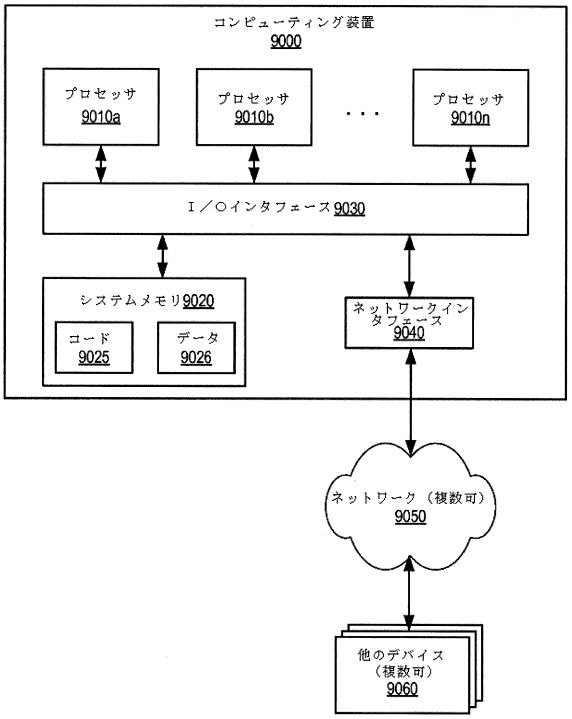

【図９】

図９




【図１０】

図１０



フロントページの続き

(72)発明者　シーン，リチャード・アレクサンダー
アメリカ合衆国・９８１０９－５２１０・ワシントン州・シアトル・テリー　アヴェニュ　ノース・４１０
(72)発明者　ローレンス，ダグラス・スチュワート
アメリカ合衆国・９８１０９－５２１０・ワシントン州・シアトル・テリー　アヴェニュ　ノース・４１０
(72)発明者　オウェイス，マルワン・サラー・エルーディン
アメリカ合衆国・９８１０９－５２１０・ワシントン州・シアトル・テリー　アヴェニュ　ノース・４１０
(72)発明者　ディッキンソン，アンドリュー・ブルース
アメリカ合衆国・９８１０９－５２１０・ワシントン州・シアトル・テリー　アヴェニュ　ノース・４１０

審査官　野元　久道

(56)参考文献　米国特許出願公開第２０１４／０００６６３８（ＵＳ，Ａ１）
米国特許出願公開第２０１１／０７５６６７（ＵＳ，Ａ１）
国際公開第２０１２／１７００１６（ＷＯ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／７４９
Ｈ０４Ｌ　１２／７０