(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-541997
(P2024-541997A)
(43)公表日　令和6年11月13日(2024.11.13)

(51)国際特許分類　FI
H04L 41/0803(2022.01)　H04L 41/0803
H04L 41/40 (2022.01)　H04L 41/40
H04L 61/2503(2022.01)　H04L 61/2503

審査請求　未請求　予備審査請求　有　（全72頁）

(21)出願番号　特願2024-525440(P2024-525440)
(86)(22)出願日　令和4年6月23日(2022.6.23)
(85)翻訳文提出日　令和6年6月7日(2024.6.7)
(86)国際出願番号　PCT/US2022/034751
(87)国際公開番号　WO2023/075868
(87)国際公開日　令和5年5月4日(2023.5.4)
(31)優先権主張番号　17/515,087
(32)優先日　令和3年10月29日(2021.10.29)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国 ９４０６５ カリフォルニア州 レッドウッド ショアーズ，メール ストップ ５オーピー７ オラクル パークウェイ ５００
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　クリーガー－スティックレス，ルーカス・マイケル
アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイシ
最終頁に続く

(54)【発明の名称】　プライベートネットワーク間での外部エンドポイントのトランスペアレントなマウント

(57)【要約】
顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間の安全なプライベートネットワーク接続を提供する、クラウドサービスプロバイダインフラストラクチャ（ＣＳＰＩ）内のセキュアプライベートネットワーク接続システム（ＳＮＣＳ）が記載される。外部リソースへの安全なアクセスは、ＳＮＣＳによって、クラウド内の顧客の仮想クラウドネットワーク（ＶＣＮ）内の外部リソースの外部リソース表現（すなわち、コンピューティングインスタンス）を作成し、外部リソース表現の仮想ネットワークインターフェイスカードを作成することによって可能にされる。ＳＮＣＳを使用して、顧客は、顧客が入り組んだサイト間ネットワーキングをセットアップすることを必要とせずに、そのオンプレミスルーティング構成に変更を加えることなく、または、外部リソースの構成に何ら変更を加えることなく、ＶＮＩＣに割り当てられている仮想ＩＰアドレスに接続することによって、そのＶＣＮ内からそのオンプレミスネットワーク内に存在する外部リソースに安全にアクセスすることができる。

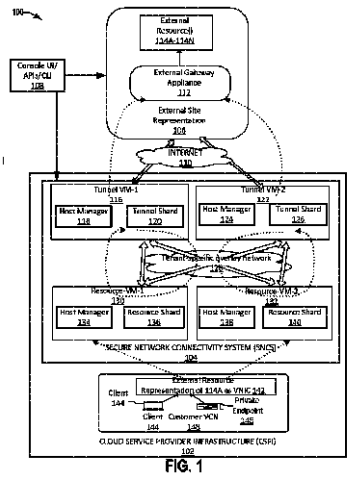

FIG. 1

【特許請求の範囲】
【請求項１】
方法であって、
クラウドサービスプロバイダにおいて実装されるセキュアネットワーク接続システムが、前記クラウドサービスプロバイダの顧客に関連付けられているオンプレミスネットワークと前記顧客のために前記クラウドサービスプロバイダによってホストされている仮想クラウドネットワーク（ＶＣＮ）との間の安全なプライベートネットワーク接続を可能にするためのセキュアネットワーク接続サービスを提供することを含み、前記セキュアネットワーク接続システムは、１つまたは複数のコンピューティングノードのセットを含む仮想オーバーレイネットワークを備え、前記方法は、
前記セキュアネットワーク接続システムが、前記オンプレミスネットワーク内に存在する外部リソースを、前記仮想クラウドネットワーク内の外部エンドポイントとして登録することをさらに含み、前記外部エンドポイントは、前記仮想クラウドネットワーク内のインターネットプロトコル（ＩＰ）アドレスによって識別され、前記方法は、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの１つのコンピューティングノードが、前記仮想クラウドネットワーク内の前記外部エンドポイントの外部リソース表現を作成することをさらに含み、前記外部リソース表現を作成することは、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの前記コンピューティングノードが、仮想ネットワークインターフェイスカード（ＶＮＩＣ）を作成することと、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの前記コンピューティングノードが、前記外部エンドポイントに関連付けられている前記インターネットプロトコル（ＩＰ）アドレスを前記仮想ネットワークインターフェイスカード（ＶＮＩＣ）に割り当てることと、を含み、前記方法はさらに、
前記セキュアネットワーク接続システム内の前記コンピューティングノードが、前記顧客に関連付けられている前記オンプレミスネットワーク内に存在する前記外部リソースに記憶されている情報をクエリするための要求を受信することと、
前記セキュアネットワーク接続システム内の前記コンピューティングノードが、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカードと、前記オンプレミスネットワーク内に存在する前記外部リソースとの間の接続を確立することと、
前記セキュアネットワーク接続システム内の前記コンピューティングノードが、確立された前記接続を介して前記外部リソースに前記要求を送信することと、
前記セキュアネットワーク接続システム内の前記コンピューティングノードが、確立された前記接続を介して前記要求に対応する結果を得ることと、を含む、方法。
【請求項２】
前記セキュアネットワーク接続システムが、外部ゲートウェイ機器を提供することをさらに含み、前記外部ゲートウェイ機器は、前記オンプレミスネットワーク内に存在する前記外部リソースと、前記セキュアネットワーク接続システムを備える前記１つまたは複数のコンピューティングノードのセットとの間のセキュアプライベートネットワーク接続を確立するように構成されている、請求項１に記載の方法。
【請求項３】
前記外部ゲートウェイ機器は、前記セキュアネットワーク接続システムのユーザによって前記顧客に関連付けられている前記オンプレミスネットワーク内に構成されている、請求項２に記載の方法。
【請求項４】
前記外部ゲートウェイ機器は、前記オンプレミスネットワーク内に存在する前記外部リソースと、前記セキュアネットワーク接続システムを備える前記１つまたは複数のコンピ

ューティングノードのセットとの間のセキュア仮想プライベートネットワーク（ＶＰＮ）接続を確立するように構成されている、請求項２または請求項３に記載の方法。
【請求項５】
前記コンピューティングノードが、確立された前記接続を介して前記オンプレミスネットワーク内に存在する前記外部リソースに前記要求を送信することは、
前記コンピューティングノードが、前記仮想ネットワークインターフェイスカードに関連付けられている前記ＩＰアドレスを、前記オンプレミスネットワーク内の前記外部リソースに関連付けられる物理ＩＰアドレスに変換することと、
前記コンピューティングノードが、前記外部リソースに関連付けられる前記物理ＩＰアドレスに前記要求を送信することと、を含む、請求項１～請求項４のいずれか１項に記載の方法。
【請求項６】
前記コンコンピューティングノードが、前記オンプレミスネットワーク内に存在する前記外部リソースへの前記接続を確立することは、前記コンコンピューティングノードが、前記仮想ネットワークインターフェイスカードを介して外部ゲートウェイ機器への接続を確立すること含む、請求項２～請求項４のいずれか１項に記載の方法。
【請求項７】
前記セキュアネットワーク接続システムが、前記顧客に関連付けられている前記オンプレミスネットワークの外部サイト表現の作成を可能にすることをさらに含み、前記外部サイト表現は、前記オンプレミスネットワークの論理表現であり、外部サイト識別子および顧客識別子によって識別される、請求項１～請求項６のいずれか１項に記載の方法。
【請求項８】
前記外部リソースは、前記外部サイト表現内に登録される、請求項７に記載の方法。
【請求項９】
前記コンピューティングノードは、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカードと、前記外部サイト表現内に存在する前記外部リソースとの間の前記接続を確立するように構成されている、請求項７または請求項８に記載の方法。
【請求項１０】
前記仮想ネットワークインターフェイスカードは、完全修飾ドメイン名、および、前記顧客に関連付けられている前記仮想クラウドネットワーク内のクラウド識別子によって識別される、請求項１～請求項９のいずれか１項に記載の方法。
【請求項１１】
前記外部リソースは、前記オンプレミスネットワーク内に存在するデータベース、アプリケーション、または計算インスタンスである、請求項１～請求項１０のいずれか１項に記載の方法。
【請求項１２】
クラウドサービスプロバイダにおいて実装され、前記クラウドサービスプロバイダの顧客に関連付けられているオンプレミスネットワークと前記顧客のために前記クラウドサービスプロバイダによってホストされている仮想クラウドネットワーク（ＶＣＮ）との間の安全なプライベートネットワーク接続を可能にするためのセキュアネットワーク接続システムであって、前記セキュアネットワーク接続システムは、１つまたは複数のコンピューティングノードのセットを含む仮想オーバーレイネットワークを備え、前記コンピューティングノードのセットのうちのコンピューティングノードは、
メモリと、
処理を実施するように構成されている１つまたは複数のプロセッサと、を備え、当該処理は、
前記セキュアネットワーク接続システムが、前記オンプレミスネットワーク内に存在する外部リソースを、前記仮想クラウドネットワーク内の外部エンドポイントとして登録することを含み、前記外部エンドポイントは、前記仮想クラウドネットワーク内のインター

ネットプロトコル（ＩＰ）アドレスによって識別され、前記処理はさらに、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの１つのコンピューティングノードが、前記仮想クラウドネットワーク内の前記外部エンドポイントの外部リソース表現を作成することを含み、前記外部リソース表現を作成することは、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの前記コンピューティングノードが、仮想ネットワークインターフェイスカード（ＶＮＩＣ）を作成することと、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの前記コンピューティングノードが、前記外部エンドポイントに関連付けられている前記インターネットプロトコル（ＩＰ）アドレスを前記仮想ネットワークインターフェイスカード（ＶＮＩＣ）に割り当てることと、を含み、前記処理はさらに、
前記顧客に関連付けられている前記オンプレミスネットワーク内に存在する前記外部リソースに記憶されている情報をクエリするための要求を受信することと、
前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカードと、前記オンプレミスネットワーク内に存在する前記外部リソースとの間の接続を確立することと、
確立された前記接続を介して前記外部リソースに前記要求を送信することと、
確立された前記接続を介して前記要求に対応する結果を得ることと、を含む、セキュアネットワーク接続システム。
【請求項１３】
外部ゲートウェイ機器を提供することをさらに含み、前記外部ゲートウェイ機器は、前記オンプレミスネットワーク内に存在する前記外部リソースと、前記セキュアネットワーク接続システムを備える前記１つまたは複数のコンピューティングノードのセットとの間のセキュアプライベートネットワーク接続を確立するように構成されており、前記外部ゲートウェイ機器は、前記セキュアネットワーク接続システムのユーザによって前記顧客に関連付けられている前記オンプレミスネットワーク内に構成されている、請求項１２に記載のシステム。
【請求項１４】
前記外部ゲートウェイ機器は、前記オンプレミスネットワーク内に存在する前記外部リソースと、前記セキュアネットワーク接続システムを備える前記１つまたは複数のコンピューティングノードのセットとの間のセキュア仮想プライベートネットワーク（ＶＰＮ）接続を確立するように構成されている、請求項１３に記載のシステム。
【請求項１５】
確立された前記接続を介して前記オンプレミスネットワーク内に存在する前記外部リソースに前記要求を送信することは、
前記仮想ネットワークインターフェイスカードに関連付けられている前記ＩＰアドレスを、前記オンプレミスネットワーク内の前記外部リソースに関連付けられる物理ＩＰアドレスに変換することと、
前記外部リソースに関連付けられる前記物理ＩＰアドレスに前記要求を送信することと、を含む、請求項１２～請求項１４のいずれか１項に記載のシステム。
【請求項１６】
前記オンプレミスネットワーク内に存在する前記外部リソースへの前記接続を確立することは、前記仮想ネットワークインターフェイスカードを介して前記外部ゲートウェイ機器への前記接続を確立することを含む、請求項１３～請求項１４のいずれか１項に記載のシステム。
【請求項１７】
プログラムコードを記憶している非一時的コンピュータ可読媒体であって、前記プログラムコードは、複数の動作を実行するための１つまたは複数の処理デバイスによって実行

可能であり、前記複数の動作は、
セキュアネットワーク接続システムが、前記オンプレミスネットワーク内に存在する外部リソースを、前記仮想クラウドネットワーク内の外部エンドポイントとして登録することを含み、前記外部エンドポイントは、前記仮想クラウドネットワーク内のインターネットプロトコル（ＩＰ）アドレスによって識別され、前記複数の動作は、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの１つのコンピューティングノードが、前記仮想クラウドネットワーク内の前記外部エンドポイントの外部リソース表現を作成することをさらに含み、前記外部リソース表現を作成することは、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの前記コンピューティングノードが、仮想ネットワークインターフェイスカード（ＶＮＩＣ）を作成することと、
前記セキュアネットワーク接続システム内の前記１つまたは複数のコンピューティングノードのセットのうちの前記コンピューティングノードが、前記外部エンドポイントに関連付けられている前記インターネットプロトコル（ＩＰ）アドレスを前記仮想ネットワークインターフェイスカード（ＶＮＩＣ）に割り当てることと、を含み、前記複数の動作はさらに、
前記顧客に関連付けられている前記オンプレミスネットワーク内に存在する前記外部リソースに記憶されている情報をクエリするための要求を受信することと、
前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカードと、前記オンプレミスネットワーク内に存在する前記外部リソースとの間の接続を確立することと、
確立された前記接続を介して前記外部リソースに前記要求を送信することと、
確立された前記接続を介して前記要求に対応する結果を得ることと、をさらに含む、非一時的コンピュータ可読媒体。
【請求項１８】
前記顧客に関連付けられている前記オンプレミスネットワークの外部サイト表現の作成を可能にすることをさらに含み、前記外部サイト表現は、前記オンプレミスネットワークの論理表現であり、外部サイト識別子および顧客識別子によって識別される、請求項１７に記載の非一時的コンピュータ可読媒体。
【請求項１９】
前記仮想ネットワークインターフェイスカードは、完全修飾ドメイン名、および、前記顧客に関連付けられている前記仮想クラウドネットワーク内のクラウド識別子によって識別される、請求項１７または請求項１８に記載の非一時的コンピュータ可読媒体。
【請求項２０】
前記外部リソースは、前記オンプレミスネットワーク内に存在するデータベース、アプリケーション、または計算インスタンスである、請求項１７～請求項１９のいずれか１項に記載の非一時的コンピュータ可読媒体。
【請求項２１】
コンピュータプログラム命令を含むコンピュータプログラム製品であって、前記コンピュータプログラム命令は、プロセッサによって実行されると、前記プロセッサに、
オンプレミスネットワーク内に存在する外部リソースを、仮想クラウドネットワーク内の外部エンドポイントとして登録することを行わせ、前記外部エンドポイントは、前記仮想クラウドネットワーク内のインターネットプロトコル（ＩＰ）アドレスによって識別され、前記コンピュータプログラム命令は、前記プロセッサによって実行されると、前記プロセッサにさらに、
前記仮想クラウドネットワーク内の前記外部エンドポイントの外部リソース表現を作成することを行わせ、前記外部リソース表現を作成するための動作は、
仮想ネットワークインターフェイスカード（ＶＮＩＣ）を作成する動作と、
前記外部エンドポイントに関連付けられている前記インターネットプロトコル（ＩＰ

）アドレスを前記仮想ネットワークインターフェイスカード（ＶＮＩＣ）に割り当てる動作と、を含み、前記コンピュータプログラム命令は、前記プロセッサによって実行されると、前記プロセッサにさらに、
前記顧客に関連付けられている前記オンプレミスネットワーク内に存在する前記外部リソースに記憶されている情報をクエリするための要求を受信することと、
前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカードと、前記オンプレミスネットワーク内に存在する前記外部リソースとの間の接続を確立することと、
確立された前記接続を介して前記外部リソースに前記要求を送信することと、
前記確立された接続を介して前記要求に対応する結果を得ることと、を行わせる、コンピュータプログラム製品。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願への相互参照

本出願は、２０２１年１０月２９日付けで出願された「Transparent Mounting of External Endpoints between Private Networks」と題する米国非仮特許出願第17/515,087号のＰＣＴ出願であり、米国特許法第１１９条（ｅ）項に基づくその利益および優先権を主張するものであり、その内容は、参照によりその全体があらゆる目的のために本明細書に組み込まれる。

【０００２】

本出願は、２０２１年１０月２９日付けで出願された「Secure Bi-Directional Network Connectivity System between Private Networks」と題する米国特許出願第17/515,093号に関連し、その内容は、参照によりあらゆる目的のために本明細書に組み込まれる。

【０００３】

技術分野

本開示は、概して、クラウドベースのサービスに関する。より詳細には、ただし決して限定することなく、本開示は、顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間の安全なプライベートネットワーク接続が確立されることを可能にする改善された機能を含むクラウドインフラストラクチャ内のセキュアプライベートネットワーク接続サービスを記載する。

【背景技術】

【０００４】

背景

クラウドベースのサービスに対する需要は、急速に増大し続けている。クラウドサービスという用語は、一般的に、クラウドサービスプロバイダによって提供されるシステムおよびインフラストラクチャ（クラウドインフラストラクチャ）を使用して要求に応じて（例えば、サブスクリプションモデルを介して）ユーザまたは顧客に利用可能にされるサービスを指すために使用される。典型的には、クラウドサービスプロバイダのインフラストラクチャを構成するサーバおよびシステムは、顧客自身のオンプレミスサーバおよびシステムとは別個のものである。したがって、顧客は、サービスのための別個のハードウェアおよびソフトウェアリソースを購入する必要なしに、クラウドサービスプロバイダによって提供されるクラウドサービスを利用することができる。サービス型ソフトウェア（ＳａａＳ）、サービス型プラットフォーム（ＰａａＳ）、サービス型インフラストラクチャ（ＩａａＳ）などを含む様々な異なるタイプのクラウドサービスが存在する。

【０００５】

クラウドサービスによって提供される多数の利点を活用するために、企業には、オンプレミスアプリケーションおよびデータを企業のローカルデータセンタから公衆クラウドインフラストラクチャへと移動させることを要求されることが多い。このプロセスは、典型

的には、企業が、企業のオンプレミスデータセンタとクラウドインフラストラクチャとの間の安全な接続を確立するために、サイト間ネットワーク接続をセットアップすることを必要とする。異なるネットワーク間のネットワークトラフィックを処理するための高性能で、スケーラブルな、かつ高可用性のサイト間ネットワーク接続を構成することは、特に、企業のオンプレミスアプリケーションおよびデータが複数の異なるネットワークにわたってスケーリングするときに、企業にとって複雑で時間のかかるタスクになり得る。

【発明の概要】

【０００６】

簡潔な概要

本開示は、概して、クラウドベースのサービスに関する。より詳細には、ただし決して限定することなく、本開示は、顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間の安全なプライベートネットワーク接続が確立されることを可能にする改善された機能を含むクラウドインフラストラクチャ内のセキュアプライベートネットワーク接続サービスを記載する。

【課題を解決するための手段】

【０００７】

ある実施形態において、クラウドサービスプロバイダ内のセキュアネットワーク接続システム（ＳＮＣＳ）が提供される。ＳＮＣＳは、クラウドサービスプロバイダの顧客に関連付けられているオンプレミスネットワークと顧客のためにクラウドサービスプロバイダによってホストされている仮想クラウドネットワーク（ＶＣＮ）との間の安全なプライベートネットワーク接続を可能にするためのセキュアネットワーク接続サービスを実行する。ＳＮＣＳは、コンピューティングノードのセットを含む仮想オーバーレイネットワークを備える。

【０００８】

ある実施態様において、また、ＳＮＣＳによって提供されるセキュア接続サービスの一部として、ＳＮＣＳは、オンプレミスネットワーク内に存在する外部リソースを、仮想クラウドネットワーク内の外部エンドポイントとして登録する。外部エンドポイントは、仮想クラウドネットワーク内のインターネットプロトコル（ＩＰ）アドレスによって識別される。次いで、ＳＮＣＳ内のコンピューティングノードは、仮想クラウドネットワーク内の外部エンドポイントの外部リソース表現を作成する。ある実施態様において、外部リソース表現を作成することは、仮想ネットワークインターフェイスカード（ＶＮＩＣ）を作成することと、外部エンドポイントに関連付けられているインターネットプロトコル（ＩＰ）アドレスをＶＮＩＣに割り当てることとを含む。コンピューティングノードは、顧客に関連付けられているオンプレミスネットワーク内に存在する外部リソースに記憶されている情報をクエリするための要求を受信し、仮想クラウドネットワーク内の外部リソース表現向けに作成されたＶＮＩＣと、オンプレミスネットワーク内に存在する外部リソースとの間の接続を確立する。コンピューティングノードは、確立された接続を介して外部リソースに要求を送信し、確立された接続を介して要求に対応する結果を得る。

【０００９】

ある例において、ＳＮＣＳは、外部ゲートウェイ機器を提供する。外部ゲートウェイ機器は、オンプレミスネットワーク内に存在する外部リソースと、セキュアネットワーク接続システムを備える１つまたは複数のコンピューティングノードのセットとの間のセキュアプライベートネットワーク接続を確立するように構成されている。ある例において、外部ゲートウェイ機器は、セキュアネットワーク接続システムのユーザによって顧客に関連付けられているオンプレミスネットワーク内に構成されている。ある例において、外部ゲートウェイ機器は、オンプレミスネットワーク内に存在する外部リソースと、セキュアネットワーク接続システムを備える１つまたは複数のコンピューティングノードのセットとの間のセキュア仮想プライベートネットワーク（ＶＰＮ）接続を確立するように構成されている。

【００１０】

ある例において、ＳＮＣＳ内のコンピューティングノードは、ＶＮＩＣに関連付けられているＩＰアドレスを、オンプレミスネットワーク内の外部リソースに関連付けられる物理ＩＰアドレスに変換し、外部リソースに関連付けられる物理ＩＰアドレスに要求を送信するように構成されている。ある例において、コンピューティングノードは、ＶＮＩＣを介して外部ゲートウェイ機器への接続を確立するように構成されている。

【００１１】

ある例において、ＳＮＣＳは、顧客に関連付けられているオンプレミスネットワークの外部サイト表現の作成するように構成されている。外部サイト表現は、オンプレミスネットワークの論理表現であり、外部サイト識別子および顧客識別子によって識別される。ある例において、外部リソースは、外部サイト表現内の外部エンドポイントとして登録される。ある例において、コンピューティングノードは、仮想クラウドネットワーク内の外部リソース表現向けに作成されたＶＮＩＣと、外部サイト表現内に存在する外部リソースとの間の接続を確立するように構成されている。

【００１２】

ある例において、ＶＮＩＣは、完全修飾ドメイン名、および、顧客に関連付けられている仮想クラウドネットワーク内のクラウド識別子によって識別される。ある例において、外部リソースは、オンプレミスネットワーク内に存在するデータベース、アプリケーション、または計算インスタンスである。

【００１３】

方法、システム、１つまたは複数のプロセッサによって実行可能なプログラム、コード、または命令を記憶している非一時的コンピュータ可読記憶媒体などを含む、様々な実施形態が本明細書に記載されている。これらの例示的な実施形態は、本開示を限定または定義するためではなく、その理解を補助するための例を提供するために言及されている。追加の実施形態が、詳細な説明において論じられており、さらに他の説明が、そこで与えられる。

【図面の簡単な説明】

【００１４】

【図１】ある実施形態による、クラウドサービスプロバイダインフラストラクチャ（ＣＳＰＩ）内のセキュアプライベートネットワーク接続サービスを含む分散環境を示す図である。

【図２】ある実施形態による、ＣＳＰＩによってホストされる顧客の仮想クラウドネットワークから顧客のオンプレミスネットワーク内に存在する顧客の外部リソースへの安全なプライベートネットワーク接続を提供するための、図１に示すシステムおよびサブシステムによって実施される動作の追加の詳細を示す図である。

【図３】ある実施形態による、顧客の外部サイト表現内の複数の外部リソースを、ＣＳＰＩによってホストされる顧客の仮想クラウドネットワーク内の複数の仮想ネットワークインターフェイスカードとして表現することができる例を示す図である。

【図４】ある実施形態による、安全なプライベートネットワーク接続を提供するための、図１に示すシステムおよびサブシステムによって実施されるプロセスの例を示す図である。

【図５】ある実施形態による、顧客の仮想クラウドネットワーク内の外部リソース表現と顧客のオンプレミスネットワーク内に存在する外部リソースとの間のネットワークパケットの流れを示すフローチャートである。

【図６】ある実施形態によるクラウドサービスプロバイダインフラストラクチャによってホストされる仮想またはオーバーレイクラウドネットワークを示す分散環境の高レベル図である。

【図７】ある実施形態によるＣＳＰＩ内の物理ネットワーク内の物理構成要素の単純化されたアーキテクチャ図である。

【図８】ある実施形態による、ホストマシンが複数のネットワーク仮想化デバイス（ＮＶＤ）に接続されているＣＳＰＩ内の例示的な構成を示す図である。

【図９】ある実施形態によるマルチテナンシ機能をサポートするためにＩ／Ｏ仮想化を提供するためのホストマシンとＮＶＤとの間の接続を示す図である。
【図１０】ある実施形態によるＣＳＰＩによって提供される物理ネットワークの単純化されたブロック図である。
【図１１】少なくとも１つの実施形態による、クラウドインフラストラクチャをサービスシステムとして実装するための１つのパターンを示すブロック図である。
【図１２】少なくとも１つの実施形態による、クラウドインフラストラクチャをサービスシステムとして実装するための別のパターンを示すブロック図である。
【図１３】少なくとも１つの実施形態による、クラウドインフラストラクチャをサービスシステムとして実装するための別のパターンを示すブロック図である。
【図１４】少なくとも１つの実施形態による、クラウドインフラストラクチャをサービスシステムとして実装するための別のパターンを示すブロック図である。
【図１５】少なくとも１つの実施形態による、例示的なコンピュータシステムを示すブロック図である。
【発明を実施するための形態】
【００１５】
詳細な説明
以下の記載において、説明を目的として、ある実施形態の完全な理解を提供するために、具体的な詳細が記載される。しかしながら、様々な実施形態は、これらの特定の詳細なしに実施され得ることが明らかであろう。図面および説明は、限定であるようには意図されていない。「例示的な」という語は本明細書においては、「例、事例、または実例としての役割を果たす」ことを意味するように使用される。「例示的」であるとして本明細書において記載されている任意の実施形態または設計は、必ずしも、他の実施形態または設計よりも好ましいかまたは有利であるものとして解釈されるべきではない。
【００１６】
本開示は、概して、クラウドベースのサービスに関する。より詳細には、ただし限定ではなく、顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間の安全なプライベートネットワーク接続を提供する改善された機能を含むクラウドサービスプロバイダインフラストラクチャ（ＣＳＰＩ）内のセキュアプライベートネットワーク接続サービスが記載される。
【００１７】
クラウドインフラストラクチャは、物理アンダーレイネットワークの上で作動し、企業のオンプレミスネットワークから安全にアクセス可能である柔軟なオーバーレイ仮想ネットワークにおいて高性能な計算、記憶、およびネットワーク機能を提供することができる。クラウドインフラストラクチャは、企業が、そのオンプレミスワークロードを管理するのと同じように、そのクラウドベースのワークロードを管理することを可能にする。したがって、企業は、そのオンプレミスネットワークと同じ制御、分離、セキュリティ、および予測可能性能によって、クラウドのすべての恩恵を得ることができる。企業は、クラウドによって提供される計算、メモリ、およびネットワーキングリソースを使用して、それ自体のネットワークを構築することができる。例えば、顧客は、クラウドによって提供されるリソースを使用して、仮想クラウドネットワーク（ＶＣＮ）として参照される１つまたは複数のカスタマイズ可能なプライベートネットワークを構築することができる。顧客は、これらの顧客ＶＣＮ上で、計算インスタンスなどの１つまたは複数の顧客リソースを展開することができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどの形態をとることができる。したがって、クラウドは、企業（顧客）が多様なアプリケーションおよびサービスを可用性の高いホスト環境内で構築し、実行することを可能にするインフラストラクチャ、および、補完クラウドサービスのセットを提供する。
【００１８】
クラウドインフラストラクチャによって提供される多数の利点を活用するために、多くの企業は、オンプレミスアプリケーションおよびデータの、企業のローカルデータセンタ

から公衆クラウドインフラストラクチャへの移動を実施する。ワークロードを企業のローカル（すなわち、オンプレミス）データセンタからクラウドへと移動させることは、複雑で困難なプロセスであり得る。クラウド移動中に遭遇する一般的な課題は、企業によって、実施する移動のタイプ、動かす必要があるリソースのタイプ、および、リソース間のデータ依存関係を識別することを含む。ワークロードを移動している間、一部のリソース（例えば、データベース、アプリケーションなど）は、クラウドに首尾よく移動することが可能になるまで、一定期間にわたってオンプレミスデータセンタに留まる必要がある場合がある。あるリソース（例えば、ビジネスに不可欠なリソース、データ可搬性制約を有するリソースまたは厳密な地理的要件を有するリソース）は、セキュリティ上の理由に起因してクラウドに移動されず、オンプレミスデータセンタに留まるリソースとして識別される場合がある。企業が、クラウド内のそのＶＣＮからそのようなオンプレミスリソースに安全にアクセスすることを可能にするためには、顧客（企業）のオンプレミスデータセンタと当該顧客のＶＣＮとの間に安全なプライベートネットワーク接続が確立される必要がある。安全なサイト間ネットワーク接続をセットアップすることは、企業にとって複雑で時間のかかるタスクであり得る。これは、典型的には、複数の構成パラメータをセットアップし、サイト間ネットワーク接続のＶＰＮ構成要素（例えば、顧客ゲートウェイデバイス、目標ゲートウェイデバイス）をセットアップすることなど、サイト間ネットワーク（例えば、ＶＰＮ）接続をセットアップするために、企業のユーザ（例えば、管理者）による、ネットワークポリシレベルの管理を必要とする。

【００１９】

付加的に、サイト間ネットワーク接続を使用してそのＶＣＮからそのオンプレミスデータセンタ内に存在するリモート資産（例えば、データベースまたはアプリケーションなどのオンプレミスリソース）にアクセスするために、企業のユーザは、顧客のＶＣＮから当該顧客の外部環境内のリモート資産に到達することができるように経路広告およびネットワークアドレス変換を実施するようにゲートウェイデバイスを手動で構成することのような、追加のタスクを実施する必要がある。ユーザはまた、トラフィック（例えば、ネットワークパケット）が顧客のＶＣＮからリモート資産に達するために、リモート資産を手動で構成すること、サイト間ＶＰＮ接続によって使用される経路を含むように経路テーブルを構成すること、経路テーブルが自動的にサイト間ＶＰＮ経路を伝播するようにルート伝播を可能にすること、セキュリティ規則を更新すること、などを行う必要もある。

【００２０】

ある実施形態において、企業のオンプレミス環境内に存在する外部リソースとクラウド内に存在する企業のリソースとの間の安全なプライベートネットワーク接続を提供する改善された機能を含むクラウドサービスプロバイダインフラストラクチャ（ＣＳＰＩ）内のセキュアプライベートネットワーク接続サービスが記載される。セキュアプライベートネットワーク接続サービスは、クラウドサービスプロバイダインフラストラクチャ（ＣＳＰＩ）内のセキュアネットワーク接続システム（ＳＮＣＳ）を使用して実施される。本開示に記載されているＳＮＣＳは、従来のクラウドベースのネットワーク接続サービスにまさるいくつかの技術的利点および／または改善を提供する。ＳＮＣＳは、顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間に安全なプライベートネットワーク接続が確立することを可能にするように構成されているネットワーク要素およびコンピューティングノードのロバストなインフラストラクチャを実装することによって、顧客のオンプレミス環境とＣＳＰＩとの間のネットワークトラフィックを処理するための高性能で、スケーラブルな、かつ高可用性のサイト間ネットワーク接続を提供する。ＳＮＣＳによって提供されるサービスを使用することによって、企業のユーザは、そのオンプレミスネットワークとクラウドとの間の入り組んだサイト間ネットワークを設定することなく、その外部リソースに何ら変更を行うことなく、または、サイト間接続によって使用される経路を構成することなく、クラウドからそのオンプレミス外部リソースに安全にアクセスすることができる。

【００２１】

ここで図面を参照すると、図１は、ある実施形態による、クラウドサービスプロバイダインフラストラクチャ（ＣＳＰＩ）内のセキュアプライベートネットワーク接続サービスを含む分散環境１００を示す。分散環境１００は、１つまたは複数の通信ネットワークを介して互いに通信可能に結合されている複数のシステムを含む。これらの通信ネットワークは、公衆およびプライベートネットワークを含み得る。図１に示す分散環境１００は、例示に過ぎず、特許請求される実施形態の範囲を不当に限定するようには意図されていない。多くの変形、代替、および修正が可能である。例えば、いくつかの他の実施形態において、図１に示す分散環境は、図１に示されているよりも多いもしくは少ないシステムもしくは構成要素を有してもよく、２つ以上のシステムを組み合わせてもよく、または、システムの異なる構成もしくは配置を有し得る。

【００２２】

図１に示す例に示すように、分散環境１００は、顧客が加入することができるサービスおよびリソースを提供するＣＳＰＩ１０２を備える。ある実施形態において、ＣＳＰＩ１０２は、顧客のオンプレミスネットワークとＣＳＰＩ１０２によってホストされる顧客のＶＣＮとの間の安全なプライベートネットワークを提供する機能を含むセキュアプライベートネットワーク接続サービスを提供する。図１に示す例において、セキュアプライベートネットワーク接続サービスは、ＣＳＰＩ１０２内のセキュアネットワーク接続システム（ＳＮＣＳ）１０４によって実施することができる。ＳＮＣＳ１０４は、付加的に、ＣＳＰＩ１０２の顧客が、顧客のＶＣＮ内から顧客のオンプレミスネットワーク内に存在する外部リソースに安全にアクセスすることを可能にする機能を含む。外部リソースへの安全なアクセスは、ＳＮＣＳ１０４によって、顧客のＶＣＮ内の外部リソースの外部リソース表現を作成することによって可能にされる。ある実施態様において、当該外部リソースの外部リソース表現を作成することは、顧客のＶＣＮ内の外部リソースの仮想ネットワークインターフェイスカード（ＶＮＩＣ）を作成することを含む。ＶＮＩＣは、ＩＰアドレス、ホスト名（例えば、完全修飾ドメイン名（ＦＱＤＮ））、および、ＶＣＮ内のクラウド識別子によって識別される。ＣＳＰＩの顧客は、ＶＮＩＣに割り当てられているＩＰアドレスに接続することによって、そのＶＣＮ内からそのオンプレミスネットワーク内に存在する外部リソースに安全にアクセスすることができる。ＳＮＣＳ１０４は、ＣＳＰＩ１０２の顧客が、顧客が入り組んだサイト間ネットワーキングをセットアップすることを必要とせずに、そのオンプレミスルーティング構成に何ら変更を加えることなく、または、外部リソースの構成に何ら変更を加えることなく、そのオンプレミスネットワーク内に存在する外部リソースに安全にアクセスすることを可能にする。

【００２３】

ある手法において、ＳＮＣＳ１０４は、多段階接続プロセスを使用して顧客のＶＣＮから顧客のオンプレミスネットワーク内に存在する外部リソースに安全にアクセスすることを可能にする。接続プロセスの第１の段階において、顧客に関連付けられているユーザ（例えば、管理者）が、顧客のオンプレミスネットワークの「外部サイト表現」１０６を作成することができる。例えば、ユーザは、外部サイト表現１０６を作成するために、ユーザデバイスによって実行されるアプリケーションのコンソールユーザインターフェイス（ＵＩ）１０８を介して、ＡＰＩを介して、または、ユーザのデバイスによって実行されるコマンドラインインターフェイス（ＣＬＩ）を介して、ＳＮＣＳ１０４とインタラクトすることができる。外部サイト表現（例えば、１０６）は、顧客の外部サイト（例えば、オンプレミスネットワーク／オンプレミスデータセンタ）の論理または仮想表現を表すことができ、外部サイト識別子およびテナント（顧客）識別子によって識別される。例として外部サイト表現１０６は、顧客のオンプレミスネットワークの一部分およびオンプレミスネットワーク内に存在する１つまたは複数の外部リソースのサブセットを論理的に表す高レベルコンテナリソースを表すことができる。

【００２４】

ＣＳＰＩ１０２による外部サイト表現１０６の登録に成功すると、接続プロセスの第２の段階において、ユーザは、外部サイト表現１０６内で外部ゲートウェイ機器１１２を構

成することができる。外部ゲートウェイ機器１１２は、顧客の外部サイト表現１０６から公衆ネットワーク（例えば、インターネット１１０）にわたってＳＮＣＳ１０４への安全なプライベートネットワーク接続が確立されることを可能にする。ある実施形態において、外部ゲートウェイ機器１１２は、ユーザがＳＮＣＳ１０４によって提供されるセキュアプライベート接続サービスに加入するときに、ＳＮＣＳ１０４によって提供されるダウンロードパッケージの一部としてユーザによってダウンロードされるソフトウェアアプリケーションであり得る。ある実施態様において、外部ゲートウェイ機器１１２は、ユーザによって、コンソールＵＩ１０８を介して顧客外部サイト表現１０６内にインストールされる仮想マシン（ＶＭ）であり得る。外部ゲートウェイ機器１１２をインストールした後、ユーザは、それに対して機器を登録しようとしている外部サイト識別子およびテナント識別子（顧客アカウント）をＳＮＣＳ１０４に提供することによって、ＳＮＣＳ１０４によって機器を登録することができる。

【００２５】

外部ゲートウェイ機器１１２のインストールおよび登録に成功すると、ＳＮＣＳ１０４が、外部ゲートウェイ機器１１２を認証し、顧客のテナント特有のオーバーレイネットワーク１２８のセットアップを指揮することができる。テナント特有のオーバーレイネットワーク１２８は、ＳＮＣＳによって提供されるサービスに加入している各テナント（顧客）のためにＳＮＣＳ１０４によって物理ネットワークの上に構築される仮想オーバーレイネットワークを表すことができる。テナント特有のオーバーレイネットワーク１２８は、顧客の外部サイト表現１０６とＣＳＰＩ内の顧客のＶＣＮ１４８との間に安全なプライベートネットワーク接続を確立するために使用される。図１に示す実施形態に示すように、テナント特有のオーバーレイネットワーク１２８は、１つまたは複数のトンネルホスト（本明細書においてはトンネル仮想マシンとしても参照される）、トンネルＶＭ－１　１１６およびトンネルＶＭ－２　１２２のセット、ならびに、１つまたは複数のリソースホスト（本明細書においてはリソース仮想マシンとしても参照される）、リソースＶＭ－１　１３０およびリソースＶＭ－２　１３２のセットを含むコンピューティングノードの分散された水平方向にスケーラブルなフリートを含み得る。ホスト（例えば、トンネルホストまたはリソースホスト）は、テナント特有のオーバーレイネットワーク１２８内で互いに相互接続されているコンテナ（本明細書においてはシャードとしても参照される）のセットから構成され得る。トンネルＶＭ１１６および１２２は、テナントごとのトンネルシャードを実行するために使用される。例えば、図１に示すように、トンネルＶＭ－１　１１６は、ＣＳＰＩの特定のテナント／顧客のトンネルシャード１２０を実行するために使用され、トンネルＶＭ－２　１２２は、トンネルシャード１２６を実行するために使用される。各トンネルシャード１２０または１２６は、顧客の外部サイト表現１０６への安全な接続を提供する役割を担う。リソースＶＭ１３０および１３２のセットは、テナントリソースシャードごとに実行するために使用することができる。例えば、図１に示すように、リソースＶＭ－１　１３０は、そのテナント／顧客のリソースシャード１３６を実行するために使用され、リソースＶＭ－２　１３２は、リソースシャード１４０を作動させるために使用される。リソースシャードは、顧客のＶＣＮからトラフィックを受信し、それを外部サイト表現内の顧客の外部リソースに転送するために使用することができる。顧客の外部サイト表現１０６と顧客のＶＣＮ１４８との間の安全な接続を提供するために図１に示すトンネルシャードおよびリソースシャードによって実施される動作の追加の詳細は、図１に詳細に記載されている。

【００２６】

各トンネルＶＭ（１１６、１２２）およびリソースＶＭ（１３０、１３２）は、付加的に、それぞれホストマネージャ（１１８、１３４）によって構成される。ホストマネージャ（１１８、１３４）は、トンネルＶＭおよびリソースＶＭ上で実行するプロセスを表す。ホストマネージャ（１１８または１３４）は、トンネルおよびリソースシャードを作成するために使用されるＡＰＩを実装することができる。ある実施態様において、ホストマネージャ（１１８、１３４）は、ステートレスとすることができ、ユーザから（ＡＰＩ１

０８を介して）作成されるべきシャードのタイプ（トンネルまたはリソースシャード）およびシャードのある構成に関する命令を受信することによって、命令モードにおいて（すなわち、ホストマネージャが実施するための一連のコマンドとして）動作することができる。ホストマネージャは、付加的に、トンネルシャードおよびリソースシャードのステータスを収集および監視する役割を担うことができる。

【００２７】

ＳＮＣＳ１０４が上述したようにテナント特有のオーバーレイネットワーク１２８を顧客向けにセットアップした後、接続プロセスの第３の段階において、ユーザは、そのオンプレミス／外部リソース１１４Ａ～１１４Ｎのサブセットを、外部サイト表現１０６内に登録する。「外部リソース」（例えば、１１４Ａ）は、顧客がそのＶＣＮ内から安全なプライベートネットワーク接続を可能にすることを意図する顧客のオンプレミスネットワーク内に存在するオンプレミスリソース（例えば、データベース、コンピューティングインスタンス、アプリケーションなど）を表すことができる。例えば、ユーザは（コンソールＵＩ１０８を介して）そのＶＣＮ１４８からの安全なプライベートネットワーク接続を可能にされるべき外部リソース（例えば、１１４Ａ）を識別し、コンソールＵＩ１０８を使用して（またはＡＰＩを介して）外部リソースをそのＶＣＮ内の外部エンドポイントとして登録する。外部リソースの登録の一部として、ユーザは、ＳＮＣＳによって提供されるコンソールＵＩまたはＡＰＩを介して外部リソースに関連付けられているオンプレミス物理ＩＰアドレス、外部リソースがアクセス可能であるポート番号、および、外部リソースのホスト名（または完全修飾ドメイン名（ＦＱＤＮ））などの外部リソースに関連する構成情報を提供する。ユーザはまた、外部リソースの外部エンドポイントが作成されるべきである顧客のＶＣＮ内のサブネットも選択する。ＳＮＣＳは、構成情報を受信し、外部リソースの外部エンドポイントを顧客のＶＣＮ内に作成する。外部エンドポイントは、顧客のＶＣＮ内のＩＰアドレス、ポート番号およびＦＱＤＮ（ホスト名）によって識別される。

【００２８】

次いで、ＳＮＣＳ１０４が、（制御プレーンＡＰＩを介して）外部エンドポイントの外部リソース表現を顧客のＶＣＮ内に作成する。ある実施態様において、外部リソース表現の作成は、ＶＮＩＣを作成することと、外部エンドポイントに関連付けられているＩＰアドレスをＶＮＩＣに割り当てることとを含む。次いで、ＳＮＣＳは、（制御プレーンＡＰＩを介して）ＶＮＩＣを（ワーカインターフェイスを介して）リソースシャードに論理的に接続（attach）することが可能であるリソースＶＭ上でリソースシャードを作成する。

【００２９】

顧客に関連付けられているユーザは、顧客のＶＣＮ１４８内のクライアントアプリケーション１４４またはプライベートエンドポイント１４６を介して、そのＶＣＮ内から任意の他のネイティブリソースに接続しているかのように、ＶＮＩＣ１４２のＩＰアドレスを介して顧客のリモートサイト内に位置するオンプレミス外部リソース１１４Ａにアクセスすることができる。例えば、外部リソース１１４Ａが外部サイト表現１０６内のデータベースを表す場合、ユーザは、データベース内に記憶されているメタデータに関する情報を得るために、クライアントアプリケーション１４４（ＣＳＰＩによって提供されるデータカタログサービスであり得る）を介して、クエリを提出することができる。クライアントアプリケーション１４４は、クエリを受信し、クエリに対応するネットワークパケットを、顧客のＶＣＮ内のＶＣＮ１４２に割り当てられているＩＰアドレスに送信する。次いで、ネットワークパケットは、それぞれリソースＶＭ１３０および１３２内で作動しているリソースシャード（１３６または１４０）によって受信される。リソースシャードは、外部サイト表現１０６内の登録された外部リソース１１４Ａへの接続を開始する。ある実施態様において、リソースシャード（１３６、１４０）は、外部リソースに関連付けられている外部エンドポイントのＩＰを、その現実の／物理オンプレミスＩＰアドレスに変換し、トンネルシャードを介して外部ゲートウェイ機器１１２にトラフィック（ネットワーク

パケット）をルーティングする機能を含む。外部ゲートウェイ機器１１２は、トンネルシャードからネットワークパケットを受信し、次いで、パケットを外部サイト表現１０６内の外部リソース１１４Ａにルーティングする。顧客のＶＣＮから登録された外部リソース１１４Ａへの安全な接続を確立するためにＳＮＣＳ１０４によって実装される、テナント特有のオーバーレイネットワーク１２８内のリソースシャードおよびトンネルシャードのサブシステムによって実施される動作の追加の詳細は、図２に詳細に論じられている。

【００３０】

図２は、ある実施形態による、ＣＳＰＩによってホストされる顧客のＶＣＮから顧客のオンプレミスネットワーク内に存在する顧客の外部リソースへの安全なプライベートネットワーク接続を提供するための、図１に示すシステムおよびサブシステムによって実施される動作の追加の詳細を示す。図２に示すシステムおよびサブシステムは、コンピューティングシステム、ハードウェア、またはそれらの組合せの１つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）を使用して実装することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。図２に示す分散環境２００は、例示に過ぎず、特許請求される実施形態の範囲を不当に限定するようには意図されていない。多くの変形、代替、および修正が可能である。例えば、いくつかの他の実施形態において、図２に示す分散環境は、図２に示されているよりも多いもしくは少ないシステムもしくは構成要素を有してもよく、２つ以上のシステムを組み合わせてもよく、または、システムの異なる構成もしくは配置を有し得る。

【００３１】

図１において以前に説明したように、顧客のオンプレミスネットワークとＣＳＰＩ１０２によってホストされる顧客のＶＣＮとの間の安全なプライベートネットワーク接続を提供するためにＳＮＣＳ１０４によって実施される接続プロセスの一部として、顧客に関連付けられているユーザ（例えば、管理者）は、顧客のオンプレミスネットワークの「外部サイト表現」１０６を作成し、次いで、外部サイト表現１０６内で外部ゲートウェイ機器１１２を構成する。外部ゲートウェイ機器１１２の登録に成功すると、外部ゲートウェイ機器１１２は、公衆ネットワーク（例えば、インターネット１１０）を介したＳＮＣＳ１０４への仮想プライベートネットワーク（ＶＰＮ）接続（本明細書においてはＶＰＮトンネルとしても参照される）を確立する。ＶＰＮ接続は、顧客の外部サイト表現１０６と顧客のＶＣＮ１４８との間の暗号化接続である。ある実施態様において、ＶＰＮ接続は、セキュアトンネリングプロトコル（例えば、ｏｐｅｎＶＰＮプロトコル）を利用して、インターネット１１０を介したＳＮＣＳ１０４への安全なプライベートネットワーク接続を確立する。外部ゲートウェイ機器１１２が外部サイト表現１０６内にインストールされると、外部ゲートウェイ機器１１２内で作動しているエージェント２０４は、外部ゲートウェイ機器１１２に関連付けられているコンパートメント識別子および構成ファイル内の外部サイト表現識別子などの情報をＳＮＣＳ１０４に渡すことによって、ＳＮＣＳ１０４によってそれ自体をアクティブ化するためのブートストラッププロセスを開始する。エージェント２０４がそれ自体をブートストラップすると、エージェントは、登録およびアクティブ化プロセスを開始するＳＮＣＳの制御プレーンと通信する。アクティブ化プロセス中、制御プレーンは、ＶＰＮサーバへの安全なトンネル接続を確立するためにゲートウェイ機器によって必要とされるすべての必要な情報（例えば、証明書、公衆ＩＤなど）を返信する。次いで、外部ゲートウェイ機器内で作動しているエージェント２０４は、ＳＮＣＳに設置されているＶＰＮサーバへの安全なＶＰＮトンネル接続を開くＶＰＮクライアントプログラムを実行することによって、ＳＮＣＳ１０４への安全なＶＰＮ接続を確立する。安全なトンネルは、ＳＮＣＳ１０４内のトンネルＶＭ（例えば、１１６）上に配置されているトンネルシャード（例えば、１２０）上で終端する。

【００３２】

図１に示す特定の実施態様において、外部ゲートウェイ機器１１２は、複数のトンネルシャード、すなわち、それぞれトンネルシャード１　１２０およびトンネルシャード２

１２６内で作動する２つの異なるＶＰＮサーバ、すなわち、ＶＰＮサーバ１　２２４およびＶＰＮサーバ２　２２６上で終端するトンネルを確立するように各々が構成されている２つのＶＰＮクライアント、すなわち、ＶＰＮクライアント１　２０６およびＶＰＮクライアント２　２０８を有して構成されている。図２に示す実施態様において、外部ゲートウェイ機器１１２のすべての物理的な設置の結果として、２つのトンネルが確立され、したがって、１つのトンネルが故障した場合、トラフィック（すなわち、ネットワークパケット）は、自動的に第２のトンネルを介してルーティングすることができる。図２に示す特定の実施態様は２つのトンネルを示しているが、他の実施態様において、ＳＮＣＳ１０４は、外部ゲートウェイ機器１１２のすべての物理的な設置のために３つ以上の冗長なトンネルを実装するように構成されてもよく、または、単に外部ゲートウェイ機器１１２の設置を受けて単一のトンネルを実装し得る。

【００３３】

ある実施形態において、外部ゲートウェイ機器１１２は、ボーダーゲートウェイプロトコル（ＢＧＰ）などの標準的な外部ゲートウェイプロトコルを使用して、トンネルシャード１２０および１２６とのＢＧＰピアリングセッションを確立する。ＢＧＰを使用して、外部ゲートウェイ機器１１２は、外部ゲートウェイ機器１１２内に実装されている公衆インターフェイス２２０を介して、トンネルシャードとルーティングおよび到達可能性情報を交換する。ＢＧＰピアリングセッションに必要とされる構成情報の一部として、外部ゲートウェイ機器１１２は、トンネルシャードによって受信されるそのローカル経路テーブル２１２（本明細書においてはルーティング情報ベース（ＲＩＢ）としても参照される）にオンプレミスＩＰアドレスを注入する。トンネルシャードは、適切な経路フィルタリングポリシを適用した後、ルーティング情報をそのローカル経路テーブル（２２８および２３６）にインポートする。経路フィルタリングは、欠陥のある外部ゲートウェイ機器１１２が任意の経路をトンネルシャードに注入しないことを保証することが好ましい。ある例において、外部ゲートウェイ機器１１２は、付加的に、ルーティングマネージャ２１４を備える。ルーティングマネージャ２１４は、ルーティングスイート（例えば、Ｑｕａｇｇａ）の一部であるオープンソースルーティングマネージャ（例えば、Ｚｅｂｒａ）を使用して実装され得る。ＢＧＰピアリングセッションが、経路を学習し、それをその経路テーブル２１２にインポートすると、ＢＧＰピアリングセッションは、最良経路計算を実施し、ルーティングマネージャ２１４を使用して、最良の経路をローカルカーネルに追加する。

【００３４】

トンネルシャード（例えば、１２０、１２６）は、１つまたは複数のコンテナのセットから構成され得る。ある実施態様において、トンネルシャード（１２０または１２６）は、トンネルシャードが、外部ゲートウェイ機器１１２と、テナント特有のオーバーレイネットワーク１２８の一部である他のシャード（例えば、リソースシャード１３６および１４０）の両方と通信することを可能にする様々なネットワークインターフェイスをセットアップするために使用することができるシェルコンテナを備え得る。図２に示す実施形態において、トンネルシャード内のシェルコンテナネット内に実装されるネットワークインターフェイスは、外部サイトインターフェイス（ｅｓｉ）、トンネルインターフェイスおよびシャードバックエンドインターフェイスを含み得る。例えば、トンネルシャード１　１２０内に実装されるネットワークインターフェイスは、トンネルインターフェイス２１６、外部サイトインターフェイス２２２およびシャードバックエンドインターフェイス２３４を含む。同様に、トンネルシャード２　１２６内に実装されるネットワークインターフェイスは、トンネルインターフェイス２１８、外部サイトインターフェイス２２３およびシャードバックエンドインターフェイス２３５を含む。トンネルシャード（例えば、１２０または１２６）は、付加的に、外部ゲートウェイ機器１１２内で作動するＶＰＮクライアント（２０６、２０８）へのＶＰＮトンネルを確立するために使用されるＶＰＮサーバ（２２４、２２６）から構成される。外部サイトインターフェイス（２２２、２２３）は、ＶＰＮクライアントがその上で作動する外部ゲートウェイ機器１１２にとって既知で

あり、トンネルシャードへのトンネルを確立するために使用される公衆ＩＰによって識別することができる。ＶＰＮクライアント（例えば、２０６、２０８）がＶＰＮサーバ（２２４、２２６）に接続すると、トンネルインターフェイス（２１６、２１８）が作成され、トンネルシャードの事前構成されたＶＰＮサブネット内に配置される。

【００３５】

ある実施態様において、各トンネルシャード（例えば、１２０、１２６）は、ボーダーゲートウェイプロトコル（ＢＧＰ）を利用して、外部ゲートウェイ機器とトンネルシャードとの間のＢＧＰピアリングセッションおよびトンネルシャードとリソースシャードとの間のＢＧＰピアリングセッションを確立することができる。ＢＧＰピアリングセッションは、シャードバックエンドインターフェイス（２３４、２３５）を介してリソースシャードとルーティングおよび到達可能性情報を交換し、外部サイトインターフェイス（２２２、２２３）を介して外部サイト表現１０６とルーティングおよび到達可能性情報を交換するために使用される。ＢＧＰピアリングセッションに必要とされる構成情報の一部として、テナント特有のオーバーレイネットワーク１２８を識別するＩＰアドレスが、それぞれトンネルシャード１２０、１２６内に実装されている経路テーブル２２８、２３６（すなわち、ルーティング情報ベース（ＲＩＢ））に追加される。ある実施態様において、クラスレスドメイン間ルーティング（ＣＩＤＲ）技法が、ＩＰアドレスをテナント特有のオーバーレイネットワークに割り振るために使用され得る。経路テーブル（２２８、２３６）は、リソースシャード（１３６、１４０）および外部サイト表現１０６などの特定のネットワーク宛先への経路を列挙する。いくつかの事例において、経路テーブル（２２８、２３６）はまた、それらの経路に関連付けられるメトリック（距離）も列挙する。リソースシャードとのＢＧＰピアリングセッションが確立されると、経路テーブル内の経路は、リソースシャードへと伝搬される。図２に示すように各トンネルシャード（１２０、１２６）は、付加的に、ルーティングマネージャ（２２８、２４０）を備える。ルーティングマネージャ（２２８または２４０）は、外部ゲートウェイ機器１１２内に実装されているルーティングマネージャ（２１４）と同様に実装され得る。ＢＧＰが経路を学習し、それらの経路をトンネルシャード内の経路テーブルにインポートすると、ＢＧＰは、最良経路計算を実施し、ルーティングマネージャを使用して、最良の経路を外部サイト表現１０６およびリソースシャード１３６、１４０にプッシュする。

【００３６】

リソースシャード（１３６、１４０）は、コンテナのセットから構成され得る。ある実施態様において、リソースシャード（１３６、１４０）は、トンネルシャード（１１６、１２６）との仮想トンネルエンドポイントＶＴＥＰ（２４２、２４３）をセットアップするために使用することができるシェルコンテナを備えることができる。各リソースシャード（１３６、１４０）は、ＢＧＰを使用して、トンネルシャードとのピアリングセッションを確立し、仮想トンネルエンドポイント（２４２、２４３）を介してトンネルシャードとルーティングおよび到達可能性情報を交換することができる。リソースシャード（１３６、１４０）は、付加的に、トンネルシャード内に実装されているルーティングマネージャ（２３２または２４０）と同じ機能を実施するように構成されているルーティングマネージャ（２５０、２６０）を備える。各リソースシャード（１３６、１４０）は、付加的に、プロキシサーバ（２４４、２５４）を含む。プロキシサーバ（２４４または２５４）は、顧客のＶＣＮ１４８内のクライアントアプリケーション１４４またはプライベートエンドポイント１４６からの接続を受け入れ、外部サイト表現内の外部リソースへの新たな接続を開始するように構成することができる。

【００３７】

ある実施態様において、すべての登録された外部エンドポイント（すなわち、外部サイト表現内の外部リソースに対応する）について、一意のプロキシサーバコンテナが立ち上げられ、リソースシャードに接続される。外部リソースを登録すると（例えば、図１に記載されている接続プロセスの第３の段階の一部として）、ユーザは、外部リソースのＩＰアドレス、外部リソースのポート番号、および外部リソースの名前などの構成情報をＳＮ

ＣＳ１０４に提供することができる。この構成情報は、プロキシサーバ内にプロビジョンされ、顧客のＶＣＮ内のクライアントアプリケーション１４４またはプライベートエンドポイント１４６（例えば、サービス）によって、外部リソースに接続するために使用される。外部リソースがＳＮＣＳによって顧客のＶＣＮ内の外部エンドポイントとして首尾よく登録されると、ＳＮＣＳ１０４は、（制御プレーンＡＰＩを介して）ＶＮＩＣを作成し、外部エンドポイントに関連付けられているＩＰアドレスをＶＮＩＣに割り当てる。

【００３８】

図２に示す例において、登録された外部エンドポイント（すなわち、外部サイト表現内の外部リソース）は、外部サイト表現１０６内に存在する外部データベース２０２を表す。プロキシサーバ（２４４、２５４）は、登録された外部エンドポイント２０２向けに作成されているＶＮＩＣに割り当てられているＩＰアドレスをリスンする。これによって、外部サイト表現内の他の登録された外部リソースにアクセスするために同じＶＮＩＣ　ＩＰが使用され得ないことが保証される。顧客のＶＣＮ内で作動しているクライアントアプリケーション１４４またはプライベートエンドポイント１４６が、外部データベース２０２内に記憶されている情報を得るためのクエリを受信すると、クライアントアプリケーションは、顧客のＶＣＮ内のＶＮＩＣ　ＩＰにネットワークパケットを送信する。ネットワークパケットは、リソースシャード（１３６、１４０）に接続されているワーカＶＮＩＣ（２５１、２５２）によって受信される。ワーカＶＮＩＣは、ＶＮＩＣのＩＰアドレスを有して構成されており、それによって、プロキシサーバ（２４４、２５４）を介して外部サイト表現内の登録された外部リソースへの接続を開始する。プロキシサーバ（２４４、２５４）は、ＶＮＩＣ１４２に割り当てられたＩＰアドレスを外部サイト表現１０６内の外部リソース１１４Ａの現実のＩＰアドレスに変換するためのネットワークアドレス変換（ＮＡＴ）を実施する。プロキシサーバ（２４４、２５４）を使用するリソースシャード（例えば１３６、１４０）は、トンネルシャード（１２０、１２６）を介した外部ゲートウェイ機器１１２への接続を開始する。外部ゲートウェイ機器１１２は、トンネルシャード（１２０、１２６）からネットワークパケットを受信し、次いで、パケットを外部サイト表現１０６内の登録された外部リソース１１４Ａにルーティングする。プロキシサーバ（２４４、２５４）は、付加的に、外部リソースへのネットワークトラフィックをトンネルシャードにわたって負荷平衡させる機能を含む。ある実施形態において、プロキシサーバ（２４４、２５４）は、複数のクライアントアプリケーションからの接続を、外部サイト表現に向けた単一の接続に多重化するように構成することができる。

【００３９】

図２に示す実施態様において、顧客のＶＣＮ１４８からのプライベート接続を要求する登録された各外部エンドポイントは、本明細書においては顧客のＶＣＮ１４８内の「ＳＶＮＩＣ」としても参照される、サービスＶＮＩＣとして実装され得る。ＳＶＮＩＣ２５４は、ＣＳＰＩ１０２によって、仮想クラウドネットワーク間のトラフィックを処理し、送信するために複数のＶＮＩＣ（例えば、サービスＶＮＩＣ２５４）をホストすることが可能であるＣＳＰＩ１０２によって実施される水平方向にスケーラブルなサービスを表すことができるサービス型ＶＮＩＣ（ＶＮＩＣａａＳ）システム（図２には示さず）を使用して実装することができる。具体的には、ＶＮＩＣａａＳは、ＶＮＩＣがサービス（すなわち、ＳＶＮＩＣ２５４）として表現または使用されることを可能にする仮想ネットワーキング特徴である。ＶＮＩＣａａＳは、特定のＳｍａｒｔＮＩＣ、または、ＶＮＩＣをホストするための仮想ネットワーク内の計算インスタンスのホストを必要とすることなく、ＶＮＩＣの機能を提供する。登録されたエンドポイントをＳＶＮＩＣとして表現するために使用される技法は、「Techniques for high performant virtual routing capabilities」と題する米国特許出願第１７／１７５，５７３号に詳細に記載されている。米国特許出願第１７／１７５，５７３号に記載されている技法は例として意図されているに過ぎず、限定であるようには意図されていない。代替的な実施形態において、登録されたエンドポイントを表現し、仮想クラウドネットワーク間のトラフィックを処理および送信するために、様々な他の技法も使用され得る。ＳＶＮＩＣ（例えば、２５４）は、すべて

の登録された外部エンドポイント（例えば、データベース２０２）向けに作成されるため、ＳＶＮＩＣごとに柔軟な数のワーカを構成することができる。特定の実施態様において、すべてのＳＶＮＩＣ（例えば、２５４）が、異なるリソースシャード（例えば、１３６、１４０）に接続されている２つのワーカＶＮＩＣ（例えば、２５１、２５２）に関連付けられ得る。ワーカＶＮＩＣは、リソースシャードに入れられ、ＳＶＮＩＣ　ＩＰによって構成される。

【００４０】

図２に示す特定の実施態様において、単一の外部ゲートウェイ機器１１２が、外部サイト表現１０６内にインストールされており、ＳＮＣＳ１０４によって実装されるトンネルフリート上に配置される必要がある合計２つのトンネルシャードをもたらす２つのトンネルを確立するように構成されている。この実施態様において説明されているような固定数のトンネルシャードについて、すべてのリソースシャードは、ＢＧＰピアの固定セットを、それらのピアの静的アドレス解決プロトコル（例えばＡＲＰ）エントリとともに用いて事前構成することができる。ある手法において、トンネルシャード上のＢＧＰコンテナは、ＢＧＰが入来する接続を受け入れることができる場所からＩＰアドレスのＣＩＤＲブロックを指定することができる「ダイナミックＢＧＰピア」を用いて構成することができる。このＣＩＤＲブロックは、テナント特有のオーバーレイネットワークのＣＩＤＲに設定することができ、したがって、リソースシャードが成長／縮小するにつれて、トンネルシャード上のＢＧＰピアも、適切に変化する。リソースシャードの観点から、この時点で、すべてのリソースシャードは２つのＢＧＰピアリング接続を有し、ＢＧＰピアの各々が同じＣＩＤＲ経路を、外部サイト表現から学習するオンプレミスネットワークに伝搬するため、すべてのリソースシャードが、オンプレミスネットワークに向けた２つのコストの等しい経路を有する。同様に、外部ゲートウェイの観点から、外部ゲートウェイ機器１１２は、ＳＮＣＳ１０４に向けた２つのトンネルを確立し、トンネルシャードは、テナント特有のオーバーレイネットワークの経路を外部ゲートウェイ機器１１２に広告し、次いで、外部ゲートウェイ機器は、テナント特有のオーバーレイネットワークへの適切な経路をインストールする。

【００４１】

ＳＮＣＳ１０４によって実装される本開示の新規の改善されたアーキテクチャを使用して、企業のユーザ（例えば、管理者）が明示的に外部リソースを構成し、経路を公告し、またはサイト間ネットワーク接続をセットアップする必要なしに、クラウド内の顧客のＶＣＮから顧客の外部サイト表現内の外部リソースへの安全なプライベートネットワーク接続を達成することができる。記載されているように、安全なプライベートネットワーク接続は、ＳＮＣＳによって、顧客の外部サイト表現と顧客のＶＣＮとの間の暗号化接続を使用して、および、顧客向けにテナント特有のオーバーレイネットワークをセットアップする前に外部ゲートウェイ機器を認証することによって、確立される。ＳＮＣＳ１０４は、ＳＮＣＳ１０４によって提供されるサービスを使用する各テナント／顧客のためのネットワーク要素およびコンピューティングノードのロバストなインフラストラクチャ（すなわち、テナント特有のオーバーレイネットワーク１２８）を実装することによって、顧客のオンプレミス環境とＣＳＰＩとの間のネットワークトラフィックを処理するための高性能、スケーラブル、かつ高可用性のサイト間ネットワーク接続を提供する。テナント特有のオーバーレイネットワーク１２８内のトンネルホストは、顧客の外部サイト表現１０６への安全な接続を提供するために使用され、リソースホストは、顧客のＶＣＮからトラフィックを受信し、それを顧客の外部サイト表現に転送するために使用される。テナント特有のオーバーレイネットワークによって実装されるネットワーク要素およびコンピューティングノードのロバストなインフラストラクチャを使用することによって、企業のユーザは、そのＶＣＮ内の任意の他のネイティブリソースに接続しているかのように、クラウドからその外部リソースに安全にアクセスすることができる。企業のユーザは、そのオンプレミスネットワークとクラウドとの間の入り組んだサイト間ネットワークを設定することなく、その外部リソースに何ら変更を行うことなく、かつ、サイト間接続によって使用され

る経路を構成することなく、その外部リソースにアクセスすることができる。

【００４２】

図２に示す実施形態において、ＳＮＣＳ１０４は、顧客のオンプレミスネットワーク内に存在する単一の外部リソース（すなわち、データベース２０２）と顧客のＶＣＮ内に存在する外部リソースの表現（すなわち、ＳＶＮＩＣ２５４）との間に安全なプライベートネットワーク接続を確立するために使用された。代替的な手法においては、顧客は、当該顧客のオンプレミスネットワーク内に存在する複数の外部リソースと当該顧客のＶＣＮ内に存在するこれらのリソースの表現との間に安全なプライベートネットワーク接続を確立するために、ＳＮＣＳ１０４によって提供されるサービスを利用し得る。図３は、ある実施形態による、顧客の外部サイト表現内の複数の外部リソースを、ＣＳＰＩによってホストされる顧客のＶＣＮ内の複数のＳＶＮＩＣとして表現することができる例を示す。図３に示す実施態様において、ＳＶＮＩＣ－Ａ３０６およびＳＶＮＩＣ－Ｂ３０８が、顧客のＶＣＮ３０２内の２つの外部リソース表現ＳＶＮＩＣ－Ａ３０６およびＳＶＮＩＣ－Ｂ３０８は、顧客のオンプレミスネットワーク内の２つの登録された外部エンドポイント（すなわち、顧客の外部サイト表現内の外部リソース１１４Ａ、１１４Ｂ）に対応する。この例において、ＳＶＮＩＣ－Ａ３０６は、ワーカＶＮＩＣのワーカＡ３１０に関連付けられ、ＳＶＮＩＣ－Ｂ３０８は、ワーカＶＮＩＣのワーカＢ３１２に関連付けられる。ワーカＶＮＩＣのワーカＡ３１０は、ＳＶＮＩＣ－Ａ３０６に対応するＩＰアドレス（５０．０．０．１０）を有して構成されており、２つの異なるリソースシャード３１８および３２０内に存在する。ワーカＶＮＩＣのワーカＢ３１０は、ＳＶＮＩＣ－Ｂ３０８に対応するＩＰアドレス（５０．０．０．２０）を有して構成されており、同じく２つの異なるリソースシャード３１８および３２０内に存在する。リソースシャード３１８および３２０は、図２において記載されているテナント特有のオーバーレイネットワーク１２８と同様のテナント特有のオーバーレイネットワーク内に存在し得る。

【００４３】

この例において、単一の経路テーブルがリソースシャード（３１８または３２０）内に実装される場合、リソースシャードがネットワークパケットを特定のワーカＶＮＩＣ（例えば、ワーカＡ３１０またはワーカＢ３１２）から送出しようとするときに、経路検索障害に遭遇する場合がある。これは、リソースシャード（３１８または３２０）が経路検索を行うときに、顧客のＶＣＮ３０２内のクライアントアプリケーション３０４が戻り経路のためにＳＶＮＩＣ－Ｂ３０８のｐｉｎｇを試行する場合に、最初に一致した経路をピックアップし、ワーカＡ３１０からパケットを送出しようとするためである。これは、最終的に、逆経路フィルタリングに起因して失敗することになる。これを回避するために、ある手法においては、各リソースシャード（３１８および３２０）が、ＳＶＮＩＣごとのルーティングテーブルを有して実装される。例えば、リソースシャード３１８は、ＳＶＮＩＣ－Ａの経路テーブル３１４ＡおよびＳＶＮＩＣ－Ｂの経路テーブル３１６Ａを有して実装され得る。同様に、リソースシャード３２０は、ＳＶＮＩＣ－Ａの経路テーブル３１４ＢおよびＳＶＮＩＣ－Ｂの経路テーブル３１６Ｂを有して実装され得る。ルーティングテーブルは、ネットワークパケットのソースＩＰアドレス（５０．０．０．２０または５０．０．０．１０）に基づいて、リソースシャードが適切なテーブル内で経路検索を実施することができるポリシベースの方式を使用することができる。

【００４４】

図４は、ある実施形態による、安全なプライベートネットワーク接続を提供するための、図１に示すシステムおよびサブシステムによって実施されるプロセスの例を示す。図４に示す処理は、それぞれのシステム、ハードウェア、またはそれらの組合せの１つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）内で実施することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。図４に提示されており、下記に説明されるプロセス４００は、例示的であり、非限定的であるように意図され

ている。図４は、特定のシーケンスまたは順序において行われる様々な処理ステップを示しているが、これは限定であるようには意図されていない。ある代替的な実施形態において、ステップは、何らかの異なる順序で実施されてもよく、または、一部のステップはまた、並列に実施され得る。図１に示す実施形態などのある実施形態において、図４に示す処理は、テナント特有のオーバーレイネットワーク１２８を備えるコンピューティングノード（例えば、１１６、１２２、１３０および１３２）によって実施され得る。ある実施形態において、テナント特有のオーバーレイネットワーク内で、処理は、テナント特有のオーバーレイネットワーク内のリソース仮想マシン（１３０または１３２）などの１つまたは複数のコンピューティングノードによって実施され得る。

【００４５】

図４に示す処理は、顧客に関連付けられているユーザ（例えば、管理者）が、顧客のオンプレミスネットワークの外部サイト表現（例えば、１０６）を作成しており、外部サイト表現１０６内の外部ゲートウェイ機器（例えば、１１２）を構成していると仮定する。図４に示す処理は、ＳＮＣＳ１０４が外部ゲートウェイ機器１１２を認証しており、顧客のためのコンピューティングノードの分散された水平方向にスケーラブルなフリートを含むテナント特有のオーバーレイネットワーク（例えば、１２８）を構成／確立しているとさらに仮定する。図１において記載されているように、１つまたは複数のコンピューティングノードのセットは、リソースホスト（すなわち、リソース仮想マシン１３０、１３２）およびトンネルホスト（すなわち、トンネル仮想マシン１１６、１２２）を含む。

【００４６】

図４に示す処理は、ブロック４０２において、ＳＮＣＳ１０４が、コンピューティングノードの分散された水平方向にスケーラブルなフリートを含むテナント特有のオーバーレイネットワーク（例えば、１２８）を実行するときに開始することができる。テナント特有のオーバーレイネットワークは、顧客の外部サイト表現とＣＳＰＩ内の顧客のＶＣＮ（例えば、１４８）との間に安全なプライベートネットワーク接続を確立するために使用される。

【００４７】

ブロック４０４において、ＳＮＣＳは（制御プレーンＡＰＩを介して）、顧客のオンプレミスネットワーク内に存在する外部リソースを、顧客のＶＣＮ内の外部エンドポイントとして登録する。外部エンドポイントは、顧客のＶＣＮ内のＩＰアドレスによって識別される。前述したように、外部リソースは、顧客がそのＶＣＮ内からの安全なプライベートネットワーク接続を可能にすることを意図する外部サイト表現１０６内のデータベース、コンピューティングインスタンス、またはアプリケーションを表すことができる。外部リソースの登録の一部として、ＳＮＣＳのユーザは、コンソールＵＩまたはＡＰＩを介して外部リソースに関連付けられているオンプレミス物理ＩＰアドレス、外部リソースがアクセス可能であるポート番号、および、外部リソースのホスト名（または完全修飾ドメイン名（ＦＱＤＮ））などの外部リソースに関連する構成情報を提供する。ユーザはまた、外部リソースの外部エンドポイントが作成されるべきである顧客のＶＣＮ内のサブネットも選択する。構成情報に基づいて、ＳＮＣＳは、外部リソースの外部エンドポイントを顧客のＶＣＮ内に作成する。外部エンドポイントは、顧客のＶＣＮ内のＩＰアドレス、ポート番号およびＦＱＤＮ（ホスト名）によって識別される。

【００４８】

ブロック４０６において、ＳＮＣＳ内のコンピューティングノード（例えば、リソースＶＭ１３０またはリソースＶＭ１３２）が、顧客のＶＣＮ内の外部エンドポイントの外部リソース表現を作成する。ある実施態様において、外部リソース表現の作成は、ブロック４０８において、コンピューティングノードによって、ＶＮＩＣを作成することと、ブロック４１０において、外部エンドポイントのＩＰアドレスをＶＮＩＣに割り当てることとを含む。

【００４９】

ブロック４１２において、コンピューティングノードは、オンプレミスネットワーク内

に存在する外部リソースに記憶されている情報をクエリするための要求を受信する。例えば、図１において記載されているように、ユーザは、外部リソース（例えば、１１４Ａ）内に記憶されているメタデータに関する情報を得るために、クライアントアプリケーション（例えば、１４４）を介して、クエリを提出することができる。クライアントアプリケーションは、当該クエリを受信し、当該クエリに対応するネットワークパケットを、顧客のＶＣＮ内のＶＮＩＣ１４２に割り当てられているＩＰアドレスに送信する。次いで、ネットワークパケットは、リソースＶＭ内で作動しているリソースシャード（１３６または１４０）によって受信される。

【００５０】

ブロック４１４において、コンピューティングノード（すなわち、リソースシャード１３６または１４０）は、ＶＮＩＣからトンネルシャード（例えば、１２０または１２６）を介して外部サイト表現１０６内の登録された外部リソース１１４Ａへの接続を確立する。特定の実施態様において、リソースシャード（１３６または１４０）は、ＶＮＩＣ１４２に割り当てられているＩＰアドレスを、外部サイト表現内に存在する外部リソース１１４Ａの現実のＩＰアドレスに変換する機能を含む。具体的には、図２に関連して記載されているように、リソースシャード（１３６または１４０）内のプロキシサーバ（２４４または２５４）が、ＶＮＩＣ１４２に割り当てられているＩＰアドレスを、外部サイト表現１０６内にインストールされている外部リソース１１４Ａの現実のＩＰアドレスに変換するためのネットワークアドレス変換（ＮＡＴ）を実施する機能を有して構成されている。プロキシサーバ（２４４または２５４）を使用して、リソースシャード（１３６または１４０）は、トンネルシャード（１２０または１２６）を介して外部ゲートウェイ機器１１２への接続を開始し、トンネルシャードは、外部サイト表現１０６内の登録された外部リソース１１４Ａへの接続を開始する。ＶＮＩＣに割り当てられているＩＰアドレスを外部リソースの現実のＩＰアドレスに変換するためのネットワークアドレス変換（ＮＡＴ）を実施するためにプロキシサーバによって実施される動作の追加の詳細は、図５に詳細に記載されている。

【００５１】

ブロック４１６において、コンピューティングノードが、ブロック４１０において確立された接続を介して外部サイト表現内に存在する外部リソースに要求を送信する。ブロック４１８において、コンピューティングノードが、確立された接続を介して要求に対応する結果を得る。次いで、結果は、顧客のＶＣＮ内の外部リソース表現に関連付けられているＶＮＩＣを介して顧客のＶＣＮ内のクライアントアプリケーションに送信される。例えば、外部リソースが外部サイト表現内で作動するデータベースである場合、結果は、データベース内の１つまたは複数のテーブル内に格納された情報を含み得る。

【００５２】

図５は、ある実施形態による、顧客の仮想クラウドネットワーク内の外部リソース表現と顧客のオンプレミスネットワーク内に存在する外部リソースとの間のネットワークパケットの流れを示すフローチャートである。図５に示す処理は、それぞれのシステム、ハードウェア、またはそれらの組合せの１つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）内で実施することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。図５に提示されており、下記に説明されるプロセス５００は、例示的であり、非限定的であるように意図されている。図５は、特定のシーケンスまたは順序において行われる様々な処理ステップを示しているが、これは限定であるようには意図されていない。ある代替的な実施形態において、ステップは、何らかの異なる順序で実施されてもよく、または、一部のステップはまた、並列に実施され得る。図２に示す実施形態などのある実施形態において、図５に示す処理は、テナント特有のオーバーレイネットワーク１２８を備えるコンピューティングノード（例えば、１１６、１２２、１３０および１３２）によって実施され得る。

【００５３】

図５に示す処理は、ブロック５０２において、顧客のＶＣＮ内のクライアントアプリケーション（例えば、１４４）が、顧客のオンプレミスネットワーク（すなわち、顧客の外部サイト表現１０６）内に存在する外部リソース（例えば、２０２）に関連付けられている情報に対するクエリを受信するときに開始することができる。例えば、クエリは、クライアントアプリケーションを介して、顧客に関連付けられているユーザから受信され得る。ブロック５０２において実施される処理の一部として、クライアントアプリケーション１４４は、クエリに対応するネットワークパケットを、顧客のＶＣＮ内のＶＮＩＣに割り当てられているＩＰアドレスに送信することによって、外部リソース表現に関連付けられるＶＮＩＣ（例えば、２０６）への接続を開始する。

【００５４】

ブロック５０４において、クライアントアプリケーションが、クエリに対応するネットワークパケットを、ＳＮＣＳ内のリソースＶＭ内で作動しているリソースシャード（１３６または１４０）に送信する。具体的には、図２に示すように、ネットワークパケットは、リソースシャード（１３６、１４０）に接続されているワーカＶＮＩＣ（２５１、２５２）によって受信することができる。リソースシャード（１３６、１４０）内のプロキシサーバ（２４４、２５４）は、ＶＮＩＣに割り当てられているＩＰアドレスを外部サイト表現１０６内の外部リソース１１４Ａの現実のＩＰアドレスに変換するためのネットワークアドレス変換（ＮＡＴ）を実施し、トンネルシャード（１２０、１２６）を介して外部ゲートウェイ機器１１２への接続を開始する。

【００５５】

ブロック５０６において、リソースシャードが、ネットワークパケットをトンネルシャード（１２０、１２６）に送信する。ブロック５０６において実施される処理の一部として、トンネルシャードは、パケットを外部サイト表現１０６内の外部ゲートウェイ機器１１２に送信する前に、リソースシャードから受信されるネットワークパケットを暗号化することができる。

【００５６】

ブロック５０８において、トンネルシャードが、顧客の外部サイト表現内に存在する外部ゲートウェイ機器１１２にネットワークパケットを送信する。ブロック５０８において実施される処理の一部として、外部ゲートウェイ機器１１２は、ネットワークパケットを外部サイト表現（例えば、１０６）内の外部リソース（例えば、２０２）に送信する前に、ネットワークパケットを解読する。

【００５７】

ブロック５１０において、外部ゲートウェイ機器１１２が、顧客の外部サイト表現内に存在する外部リソース（例えば、２０２）にネットワークパケットを送信／ルーティングする。外部リソースは、クエリに対応するネットワークパケットを受信し、クエリに対応する応答ネットワークパケットを生成する。次いで、応答ネットワークパケットは、外部リソースによってクライアントアプリケーションに返送することができる。例えば、応答ネットワークパケットフローの一部として、クエリに対する応答に対応するネットワークパケットが、外部リソースから外部ゲートウェイ機器に送信される。外部ゲートウェイ機器は、ネットワークパケットを暗号化し、暗号化ネットワークパケットをトンネルシャードに送信する。トンネルシャードは、暗号化パケットを受信し、リソースシャードにパケットを送信する。リソースシャードは、ネットワークパケットを解読し、外部リソースに割り当てられた現実のＩＰアドレスを、顧客のＶＣＮ内の外部リソース表現に関連付けられるＶＮＩＣのＩＰアドレスに変換するための逆ネットワークアドレス変換（ＮＡＴ）を実施する。次いで、リソースシャードは、応答ネットワークパケットをＶＮＩＣに送信し、ＶＮＩＣは、次いで、顧客のＶＣＮ１４８内の要求しているクライアントアプリケーション１４４に応答パケットを送信する。

【００５８】

例示的な仮想ネットワーキングアーキテクチャ

クラウドサービスという用語は、一般的に、クラウドサービスプロバイダ（ＣＳＰ）に

よって、ＣＳＰによって提供されるシステムおよびインフラストラクチャ（クラウドインフラストラクチャ）を使用して要求に応じて（例えば、サブスクリプションモデルを介して）ユーザまたは顧客に利用可能にされるサービスを指すために使用される。典型的には、ＣＳＰのインフラストラクチャを構成するサーバおよびシステムは、顧客自身のオンプレミスサーバおよびシステムとは別個のものである。したがって、顧客は、サービスのための別個のハードウェアおよびソフトウェアリソースを購入する必要なしに、ＣＳＰによって提供されるクラウドサービスを利用することができる。クラウドサービスは、顧客がサービスの提供に使用されるインフラストラクチャの獲得に投資を行う必要なしに、アプリケーションおよびコンピューティングリソースへの容易でスケーラブルなアクセスを、加入している顧客に提供するように設計されている。

【００５９】

様々なタイプのクラウドサービスを供給するいくつかのクラウドサービスプロバイダが存在する。サービス型ソフトウェア（ＳａａＳ）、サービス型プラットフォーム（ＰａａＳ）、サービス型インフラストラクチャ（ＩａａＳ）などを含む様々な異なるタイプまたはモデルのクラウドサービスが存在する。

【００６０】

顧客は、ＣＳＰによって提供される１つまたは複数のクラウドサービスに加入することができる。顧客は、個人、組織、企業などのような任意のエンティティとすることができる。顧客がＣＳＰによって提供されるサービスに加入または登録すると、その顧客のテナンシまたはアカウントが作成される。顧客は、その後、このアカウントを介して、アカウントに関連付けられる、加入した１つまたは複数のクラウドリソースにアクセスすることができる。

【００６１】

上記で言及したように、サービス型インフラストラクチャ（ＩａａＳ）は、１つの特定のタイプのクラウドコンピューティングサービスである。ＩａａＳモデルにおいて、ＣＳＰは、顧客によって、自身のカスタマイズ可能なネットワークを構築し、顧客リソースを展開するために使用することができるインフラストラクチャ（クラウドサービスプロバイダインフラストラクチャまたはＣＳＰＩとして参照される）を提供する。したがって、顧客のリソースおよびネットワークは、ＣＳＰによって提供されるインフラストラクチャによって、分散環境においてホストされる。これは、顧客のリソースおよびネットワークが顧客によって提供されるインフラストラクチャによってホストされる従来のコンピューティングとは異なる。

【００６２】

ＣＳＰＩは、基盤ネットワークまたはアンダーレイネットワークとしても参照される、物理ネットワークを形成する様々なホストマシン、メモリリソース、およびネットワークリソースを含む、相互接続された高性能の計算リソースを含み得る。ＣＳＰＩ内のリソースは、１つまたは複数の地理的領域にわたって地理的に分散され得る１つまたは複数のデータセンタにわたって分散され得る。これらの物理リソースによって、仮想化ソフトウェアを実行して、仮想化分散環境を提供することができる。仮想化は、物理ネットワークの上にオーバーレイネットワーク（ソフトウェアベースのネットワーク、ソフトウェア定義ネットワーク、または仮想ネットワークとしても知られる）を作成する。ＣＳＰＩ物理ネットワークは、物理ネットワークの上に１つまたは複数のオーバーレイまたは仮想ネットワークを作成するための下層基盤を提供する。物理ネットワーク（または基盤ネットワークまたはアンダーレイネットワーク）は、物理スイッチ、ルータ、コンピュータおよびホストマシンなどのような、物理ネットワークデバイスを含む。オーバーレイネットワークは、物理基盤ネットワークの上で作動する論理（または仮想）ネットワークである。所与の物理ネットワークは、１つまたは複数のオーバーレイネットワークをサポートすることができる。オーバーレイネットワークは、典型的には、カプセル化技法を使用して、異なるオーバーレイネットワークに属するトラフィックを区別する。仮想またはオーバーレイネットワークは、仮想クラウドネットワーク（ＶＣＮ）としても参照される。仮想ネット

ワークは、物理ネットワークの上で作動することができるネットワーク抽象化の層を作成するためのソフトウェア仮想化技術（例えば、ハイパーバイザ、ネットワーク仮想化デバイス（ＮＶＤ）によって実装される仮想化機能（例えば、ｓｍａｒｔＮＩＣ）、トップオブラック（ＴＯＲ）スイッチ、ＮＶＤによって実施される１つまたは複数の機能を実装するスマートＴＯＲ、および他のメカニズム）を使用して実装される。仮想ネットワークは、ピアツーピアネットワーク、ＩＰネットワークなどを含む、多くの形態をとることができる。仮想ネットワークは、典型的には、レイヤ３　ＩＰネットワークまたはレイヤ２　ＶＬＡＮのいずれかである。この仮想またはオーバーレイネットワーキング方法は、仮想またはオーバーレイレイヤ３ネットワーキングとして参照されることが多い。仮想ネットワークのために展開されるプロトコルの例は、ＩＰ－ｉｎ－ＩＰ（または一般ルーティングカプセル化（ＧＲＥ））、仮想拡張可能ＬＡＮ（ＶＸＬＡＮ－ＩＥＴＦ　ＲＦＣ７３４８）、仮想プライベートネットワーク（ＶＡＮ）（例えば、ＭＰＬＳレイヤ３仮想プライベートネットワーク（ＲＦＣ４３６４））、ＶＭｗａｒｅのＮＳＸ、ＧＥＮＥＶＥ（一般ネットワーク仮想化カプセル化）などを含む。

【００６３】

ＩａａＳの場合、ＣＳＰによって提供されるインフラストラクチャ（ＣＳＰＩ）は、公衆ネットワーク（例えば、インターネット）を介して仮想化コンピューティングリソースを提供するように構成することができる。ＩａａＳモデルにおいて、クラウドコンピューティングサービスプロバイダは、インフラストラクチャ構成要素（例えば、サーバ、記憶デバイス、ネットワークノード（例えば、ハードウェア）、展開ソフトウェア、プラットフォーム仮想化（例えば、ハイパーバイザ層）など）をホストすることができる。いくつかの事例において、ＩａａＳプロバイダはまた、それらのインフラストラクチャ構成要素に付随させるための様々なサービス（例えば、請求、監視、ログ記録、セキュリティ、負荷平衡およびクラスタリングなど）を供給することもできる。したがって、これらのサービスはポリシ駆動であり得るため、ＩａａＳユーザは、アプリケーション可用性およびパフォーマンスを維持するために負荷平衡を駆動するためのポリシを実装することが可能であり得る。ＣＳＰＩは、顧客が多様なアプリケーションおよびサービスを可用性の高いホスト分散環境内で構築し、実行することを可能にするインフラストラクチャ、および、補完クラウドサービスのセットを提供する。ＣＳＰＩは、顧客のオンプレミスネットワークなどの様々なネットワーク接続されたロケーションから安全にアクセス可能である柔軟な仮想ネットワーク内で、高性能の計算リソースおよび機能ならびに記憶容量を供給する。顧客がＣＳＰによって提供されるＩａａＳサービスに加入または登録するとき、その顧客向けに作成されるテナンシは、顧客がそのクラウドリソースを作成、編成、および管理することができる、ＣＳＰＩ内の安全で隔離された区分である。

【００６４】

顧客は、ＣＳＰＩによって提供される計算、メモリ、およびネットワーキングリソースを使用して、自身の仮想ネットワークを構築することができる。これらの仮想ネットワーク上に、計算インスタンスなどの１つまたは複数の顧客リソースまたはワークロードを展開することができる。例えば、顧客は、ＣＳＰＩによって提供されるリソースを使用して、仮想クラウドネットワーク（ＶＣＮ）として参照される１つまたは複数のカスタマイズ可能なプライベート仮想ネットワークを構築することができる。顧客は、顧客ＶＣＮ上で、計算インスタンスなどの１つまたは複数の顧客リソースを展開することができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどの形態をとることができる。したがって、ＣＳＰＩは、顧客が多様なアプリケーションおよびサービスを可用性の高い仮想ホスト環境内で構築し、実行することを可能にするインフラストラクチャ、および、補完クラウドサービスのセットを提供する。顧客は、ＣＳＰＩによって提供される下層物理リソースを管理せず、制御しないが、オペレーティングシステム、ストレージ、および展開されているアプリケーションを制御することができ、場合によっては、ネットワーキング構成要素（例えば、ファイアウォール）の選択を制限付きで制御することができる。

【００６５】

ＣＳＰは、顧客およびネットワーク管理者が、ＣＳＰＩリソースを使用してクラウド内で展開されるリソースを構成、アクセス、および管理することを可能にするコンソールを提供することができる。ある実施形態において、コンソールは、ＣＳＰＩにアクセスおよび管理するために使用することができるウェブベースのユーザインターフェイスを提供する。いくつかの実施態様において、コンソールは、ＣＳＰによって提供されるウェブベースのアプリケーションである。

【００６６】

ＣＳＰＩは、シングルテナンシまたはマルチテナンシアーキテクチャをサポートすることができる。シングルテナンシアーキテクチャにおいて、ソフトウェア（例えば、アプリケーション、データベース）またはハードウェア構成要素（例えば、ホストマシンまたはサーバ）は、単一の顧客またはテナントにサービスする。マルチテナンシアーキテクチャにおいて、ソフトウェアまたはハードウェア構成要素は、複数の顧客またはテナントにサービスする。したがって、マルチテナンシアーキテクチャにおいて、ＣＳＰＩリソースは、複数の顧客またはテナント間で共有される。マルチテナンシ状況において、各テナントのデータが分離され、他のテナントに見えないままであることを保証するために、予防措置がとられ、ＣＳＰＩ内に安全対策が導入される。

【００６７】

物理ネットワークにおいて、ネットワークエンドポイント（「エンドポイント」）は、物理ネットワークに接続されており、接続されているネットワークと往復して通信するコンピューティングデバイスまたはシステムを指す。物理ネットワーク内のネットワークエンドポイントは、ローカルエリアネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、または他のタイプの物理ネットワークに接続され得る。物理ネットワーク内の従来のエンドポイントの例は、モデム、ハブ、ブリッジ、スイッチ、ルータ、および他のネットワーキングデバイス、物理コンピュータ（またはホストマシン）などを含む。物理ネットワーク内の各物理デバイスは、デバイスと通信するために使用することができる固定ネットワークアドレスを有する。この固定ネットワークアドレスは、レイヤ２アドレス（例えば、ＭＡＣアドレス）、固定レイヤ３アドレス（例えば、ＩＰアドレス）などとすることができる。仮想化環境または下層ネットワークにおいて、エンドポイントは、物理ネットワークの構成要素によってホストされる（例えば、物理ホストマシンによってホストされる）仮想マシンなどの様々な仮想エンドポイントを含み得る。仮想ネットワーク内のこれらのエンドポイントは、オーバーレイレイヤ２アドレス（例えば、オーバーレイＭＡＣアドレス）およびオーバーレイレイヤ３アドレス（例えば、オーバーレイＩＰアドレス）などのオーバーレイアドレスによってアドレス指定される。ネットワークオーバーレイは、ネットワークマネージャが、ソフトウェア管理を使用して（例えば、仮想ネットワークの制御プレーンを実装するソフトウェアを介して）ネットワークエンドポイントに関連付けられるオーバーレイアドレスを転々と移動することを可能にすることによって、柔軟性を可能にする。したがって、物理ネットワークとは異なり、仮想ネットワークにおいて、オーバーレイアドレス（例えば、オーバーレイＩＰアドレス）は、ネットワーク管理ソフトウェアを使用して１つのエンドポイントから別のエンドポイントへと移動させることができる。仮想ネットワークは物理ネットワークの上に構築されるため、仮想ネットワーク内の構成要素間の通信は、仮想ネットワークと、下層の物理ネットワークの両方を含む。そのような通信を促進するために、ＣＳＰＩの構成要素は、仮想ネットワーク内のオーバーレイアドレスを基盤ネットワーク内の実際の物理アドレスにマッピングし、および、その逆を行うマッピングを学習し、記憶するように構成されている。このとき、これらのマッピングは、通信を促進するために使用される。仮想ネットワーク内のルーティングを促進するために、顧客トラフィックがカプセル化される。

【００６８】

したがって、物理アドレス（例えば、物理ＩＰアドレス）は、物理ネットワーク内の構成要素に関連付けられ、オーバーレイアドレス（例えば、オーバーレイＩＰアドレス）は、仮想またはオーバーレイネットワーク内のエンティティに関連付けられる。物理ＩＰア

ドレスは、基盤または物理ネットワーク内の物理デバイス（例えば、ネットワークデバイス）に関連付けられるＩＰアドレスである。例えば、各ＮＶＤは、関連付けられる物理ＩＰアドレスを有する。オーバーレイＩＰアドレスは、顧客の仮想クラウドネットワーク（ＶＣＮ）内の計算インスタンスなどの、オーバーレイネットワーク内のエンティティに関連付けられるオーバーレイアドレスである。各々がそれ自体のプライベートＶＣＮを有する２つの異なる顧客またはテナントが、可能性として、互いを一切知ることなく、そのＶＣＮ内で同じオーバーレイＩＰアドレスを使用することができる。物理ＩＰアドレスとオーバーレイＩＰアドレスは両方とも、現実のＩＰアドレスのタイプである。これらは、仮想ＩＰアドレスとは別個のものである。仮想ＩＰアドレスは、典型的には、複数の現実のＩＰアドレスを表すかまたはこれにマッピングする単一のＩＰアドレスである。仮想ＩＰアドレスは、仮想ＩＰアドレスと複数の現実のＩＰアドレスとの間の１対多マッピングを提供する。例えば、ロードバランサが、複数のサーバ（各サーバはそれ自体の現実のＩＰアドレスを有する）にマッピングするかまたはこれを表すためにＶＩＰを使用することができる。

【００６９】

クラウドインフラストラクチャまたはＣＳＰＩは、世界中の１つまたは複数の領域内で、１つまたは複数のデータセンタ内で物理的にホストされる。ＣＳＰＩは、物理または基盤ネットワーク内の構成要素、および、物理ネットワーク構成要素の上に構築される仮想ネットワーク内にある仮想化構成要素（例えば、仮想ネットワーク、計算インスタンス、仮想マシンなど）を含み得る。ある実施形態において、ＣＳＰＩは、レルム、リージョンおよび可用性ドメインに編成され、ホストされる。リージョンは、典型的には、１つまたは複数のデータセンタを含む局所的な地理的エリアである。リージョンは、一般的に、互いに独立しており、例えば、国またはさらには大陸をまたいで大きい距離によって分離することができる。例えば、第１のリージョンは、オーストラリア内にあってもよく、別のリージョンは日本内にあってもよく、さらに別のリージョンはインド内にあり得る、などである。ＣＳＰＩリソースは、複数のリージョンの間で分割され、結果、各リージョンは、ＣＳＰＩリソースのそれ自体の独立したサブセットを有する。各リージョンは、計算リソース（例えば、ベアメタルサーバ、仮想マシン、コンテナおよび関連するインフラストラクチャなど）、ストレージリソース（例えば、ブロックボリュームストレージ、ファイルストレージ、オブジェクトストレージ、アーカイブストレージ）、ネットワーキングリソース（例えば、仮想クラウドネットワーク（ＶＣＮ）、負荷平衡リソース、オンプレミスネットワークへの接続）、データベースリソース、エッジネットワーキングリソース（例えば、ＤＮＳ）、ならびにアクセス管理および監視リソースなどのような、基幹インフラストラクチャサービスおよびリソースのセットを提供することができる。各リージョンは、一般的に、それをレルム内の他のリージョンに接続する複数の経路を有する。

【００７０】

近傍のリソースを使用することは、離れたリソースを使用するよりも高速であるため、一般的に、アプリケーションは、最も頻繁に使用されるリージョンにおいて展開される（すなわち、そのリージョンに関連付けられるインフラストラクチャ上に展開される）。アプリケーションはまた、大規模な気象系または地震などのリージョン規模の危険性を軽減すること、法域、税領域、および他の事業または社会的基準に関する変動する要件を満たすことなどのための冗長性などの様々な理由から、異なるリージョンにおいて展開することもできる。

【００７１】

リージョン内のデータセンタは、さらに、可用性ドメイン（ＡＤ）に編成および細分化することもできる。可用性ドメインは、リージョン内に位置する１つまたは複数のデータセンタに対応することができる。リージョンは、１つまたは複数の可用性ドメインから構成することができる。そのような分散環境において、ＣＳＰＩリソースは、仮想クラウドネットワーク（ＶＣＮ）など、領域特有であるか、または、計算インスタンスなど、可用性ドメイン特有であるかのいずれかである。

【００７２】
リージョン内のＡＤは、互いから分離されており、耐障害性であり、同時に機能しなくなる可能性が非常に低いように構成されている。これは、あるリージョン内の１つのＡＤにおける障害が、同じリージョン内の他のＡＤの可用性に影響を及ぼす可能性が低くなるように、ＡＤが、ネットワーキング、物理ケーブル、ケーブル経路、ケーブル入口点などのような重大なインフラストラクチャリソースを共有しないことによって達成される。同じリージョン内のＡＤは、低レイテンシ高帯域幅ネットワークによって互いに接続することができ、これによって、他のネットワーク（例えば、インターネット、顧客のオンプレミスネットワークなど）への高可用性接続を提供し、高可用性と災害復旧の両方のために複数のＡＤ内に複製システムを構築することが可能になる。クラウドサービスは、複数のＡＤを使用して、高可用性を保証し、リソース障害に対して保護する。ＩａａＳによって提供されるインフラストラクチャが増加すると、より多くのリージョンおよびＡＤが、容量を付加して追加される。可用性ドメイン間のトラフィックは、通常、暗号化される。
【００７３】
ある実施形態において、リージョンはレルムにグループ化される。レルムは、複数のリージョンの論理的集合である。レルムは、互いに分離されており、一切のデータを共有しない。同じレルム内のリージョンは、互いに通信することができるが、異なるレルム内のリージョンは、互いに通信することができない。ＣＳＰを有する顧客のテナンシおよびアカウントは、単一のレルム内に存在し、そのレルムに属する１つまたは複数のリージョンにわたって分散することができる。典型的には、顧客がＩａａＳサービスに加入すると、レルム内の顧客が指定するリージョン（「ホーム」リージョンとして参照される）内に、その顧客のテナンシおよびアカウントが作成される。顧客は、顧客のテナンシを、レルム内の１つまたは複数の他の領域にまたがって拡張することができる。顧客は、顧客のテナンシが存在するレルム内にないリージョンにアクセスすることはできない。
【００７４】
ＩａａＳプロバイダは、複数のレルムを提供することができ、各レルムは、顧客またはユーザの特定のセットに供される。例えば、商業レルムは、商業顧客に対して提供され得る。別の例として、特定の国のためのレルムが、その国の中の顧客に対して提供され得る。さらに別の例として、政府レルムが、政府に対して提供され得る、などである。例えば、政府レルムは、特定の政府に対して供されてもよく、商業レルムよりも高められたセキュリティレベルを有し得る。例えば、Ｏｒａｃｌｅクラウドインフラストラクチャ（ＯＣＩ）は、現在、商業リージョンの１つのレルム、および、政府クラウドリージョンの２つのレルム（例えば、ＦｅｄＲＡＭＰ認可およびＩＬ５認可）を提供している。
【００７５】
ある実施形態において、ＡＤは、１つまたは複数のフォールトドメインに細分化することができる。フォールトドメインは、アンチアフィニティを提供するためのＡＤ内のインフラストラクチャリソースのグループ分けである。フォールトドメインは、インスタンスが単一のＡＤ内の同じ物理ハードウェア上にないように、計算インスタンスを分散させることを可能にする。これは、アンチアフィニティとして知られている。フォールトドメインは、単一の障害点を共有するハードウェア構成要素（コンピュータ、スイッチなど）のセットを指す。計算プールは、複数のフォールトドメインに論理的に分割される。これに起因して、１つのフォールトドメインに影響を及ぼすハードウェア障害または計算ハードウェアメンテナンスイベントは、他のフォールトドメイン内のインスタンスに影響を及ぼさない。実施形態に応じて、各ＡＤのフォールトドメインの数は変化し得る。例えば、ある実施形態において、各ＡＤは、３つのフォールトドメインを含む。フォールトドメインは、ＡＤ内の論理データセンタとして作用する。
【００７６】
顧客がＩａａＳサービスに加入すると、ＣＳＰＩからのリソースが顧客にプロビジョンされ、顧客のテナンシに関連付けられる。顧客は、これらのプロビジョンされたリソースを使用して、プライベートネットワークを構築し、これらのネットワーク上にリソースを

展開することができる。ＣＳＰＩによってクラウド内でホストされる顧客ネットワークは、仮想クラウドネットワーク（ＶＣＮ）として参照される。顧客は、顧客に割り振られたＣＳＰＩリソースを使用して１つまたは複数の仮想クラウドネットワーク（ＶＣＮ）をセットアップすることができる。ＶＣＮは、仮想またはソフトウェア定義のプライベートネットワークである。顧客のＶＣＮ内に展開される顧客リソースは、計算インスタンス（例えば、仮想マシン、ベアメタルインスタンス）および他のリソースを含み得る。これらの計算インスタンスは、アプリケーション、ロードバランサ、データベースなどのような様々な顧客ワークロードを表すことができる。ＶＣＮ上に展開される計算インスタンスは、インターネットなどの公衆ネットワーク上の公衆アクセス可能エンドポイント（「公衆エンドポイント」）、同じＶＣＮまたは他のＶＣＮ（例えば、顧客の他のＶＣＮ、または顧客に属しないＶＣＮ）内の他のインスタンス、顧客のオンプレミスデータセンタまたはネットワーク、ならびに、サービスエンドポイントおよび他のタイプのエンドポイントと通信することができる。

【００７７】

ＣＳＰは、ＣＳＰＩを使用して様々なサービスを提供することができる。いくつかの事例において、ＣＳＰＩの顧客自身が、サービスプロバイダのように作用し、ＣＳＰＩリソースを使用してサービスを提供し得る。サービスプロバイダは、識別情報（例えば、ＩＰアドレス、ＤＮＳ名およびポート）によって特徴付けられるサービスエンドポイントを暴露することができる。顧客のリソース（例えば、計算インスタンス）は、その特定のサービスのためにサービスによって暴露されるサービスエンドポイントにアクセスすることによって、特定のサービスを消費することができる。これらのサービスエンドポイントは、一般的には、インターネットなどの公衆通信ネットワークを介してエンドポイントに関連付けられる公衆ＩＰアドレスを使用して、ユーザによってパブリックにアクセス可能であるエンドポイントである。パブリックにアクセス可能であるネットワークエンドポイントは、公衆エンドポイントとして参照されることもある。

【００７８】

ある実施形態において、サービスプロバイダは、そのサービスのためのエンドポイント（サービスエンドポイントとして参照されることがある）を介してサービスを暴露することができる。次いで、サービスの顧客は、このサービスエンドポイントを使用して、サービスにアクセスすることができる。ある実施態様において、サービスのために提供されるサービスエンドポイントは、そのサービスを消費することを意図する複数の顧客によってアクセスすることができる。他の実施態様において、専用サービスエンドポイントが顧客のために提供されてもよく、結果、その顧客のみが、その専用サービスエンドポイントを使用してサービスにアクセスすることができる。

【００７９】

ある実施形態において、ＶＣＮが作成されると、ＶＣＮは、ＶＣＮに割り当てられる一定範囲のプライベートオーバーレイＩＰアドレス（例えば、１０．０／１６）である、プライベートオーバーレイクラスレスドメイン間ルーティング（ＣＩＤＲ）アドレス空間に関連付けられる。ＶＣＮは、関連付けられるサブネット、経路テーブル、およびゲートウェイを含む。ＶＣＮは、単一のリージョン内に存在するが、リージョンの可用性ドメインの１つまたは複数またはすべてにまたがることができる。ゲートウェイは、ＶＣＮ向けに構成されており、ＶＣＮへの、および、ＶＣＮからＶＣＮの外側の１つまたは複数のネットワークへのトラフィックの通信を可能にする仮想インターフェイスである。１つまたは複数の異なるタイプのゲートウェイが、異なるタイプのエンドポイントへの、および、そこからの通信を可能にするために、ＶＣＮ向けに構成され得る。

【００８０】

ＶＣＮは、１つまたは複数のサブネットなどの１つまたは複数のサブネットワークに細分化することができる。したがって、サブネットは、ＶＣＮ内に作成することができる構成単位または下位区分である。ＶＣＮは、１つまたは複数のサブネットを有することができる。ＶＣＮ内の各サブネットは、そのＶＣＮ内の他のサブネットと重なり合わず、ＶＣ

Ｎのアドレス空間内のアドレス空間サブセットを表す、連続した範囲のオーバーレイＩＰアドレス（例えば、１０．０．０．０／２４および１０．０．１．０／２４）に関連付けられる。

【００８１】

各計算インスタンスは、計算インスタンスがＶＣＮのサブネットに参加することを可能にする仮想ネットワークインターフェイスカード（ＶＮＩＣ）に関連付けられる。ＶＮＩＣは、物理ネットワークインターフェイスカード（ＮＩＣ）の論理的表現である。概して、ＶＮＩＣは、エンティティ（例えば、計算インスタンス、サービス）と仮想ネットワークとの間のインターフェイスである。ＶＮＩＣは、サブネット内に存在し、１つまたは複数の関連付けられるＩＰアドレスを有し、セキュリティ規則またはポリシに関連付けられる。ＶＮＩＣは、スイッチ上のレイヤ２ポートと等価である。ＶＮＩＣは、計算インスタンスおよびＶＣＮ内のサブネットに接続される。計算インスタンスに関連付けられるＶＮＩＣは、計算インスタンスが、ＶＣＮのサブネットの一部であることを可能にし、計算インスタンスが、計算インスタンスと同じサブネット上にあるエンドポイント、ＶＣＮ内の異なるサブネット内のエンドポイント、または、ＶＣＮの外側のエンドポイントと通信する（例えば、パケットを送受信する）ことを可能にする。したがって、計算インスタンスに関連付けられるＶＮＩＣは、計算インスタンスがＶＣＮの内側および外側のエンドポイントとどのように接続するかを決定する。計算インスタンスが作成され、ＶＣＮ内のサブネットに追加されると、計算インスタンスのＶＮＩＣが作成され、その計算インスタンスに関連付けられる。計算インスタンスのセットを含むサブネットについて、サブネットは、計算インスタンスのセットに対応するＶＮＩＣを含み、各ＶＮＩＣが、コンピュータインスタンスのセット中の計算インスタンスに接続される。

【００８２】

各計算インスタンスは、計算インスタンスに関連付けられるＶＮＩＣを介して、プライベートオーバーレイＩＰアドレスを割り当てられる。このプライベートオーバーレイＩＰアドレスは、計算インスタンスが作成され、計算インスタンスへのおよびそこからのトラフィックをルーティングするために使用されるときに、計算インスタンスに関連付けられるＶＮＩＣに割り当てられる。所与のサブネット内のすべてのＶＮＩＣが、同じ経路テーブル、セキュリティリスト、およびＤＨＣＰオプションを使用する。上述したように、ＶＣＮ内の各サブネットは、そのＶＣＮ内の他のサブネットと重なり合わず、ＶＣＮのアドレス空間内のアドレス空間サブセットを表す、連続した範囲のオーバーレイＩＰアドレス（例えば、１０．０．０．０／２４および１０．０．１．０／２４）に関連付けられる。ＶＣＮの特定のサブネット上のＶＮＩＣについて、ＶＮＩＣに割り当てられるプライベートオーバーレイＩＰアドレスは、サブネットに割り振られる連続した範囲のオーバーレイＩＰアドレスからのアドレスである。

【００８３】

ある実施形態において、計算インスタンスは、任意選択的に、プライベートオーバーレイＩＰアドレスに加えて、例えば、公衆サブネット内にある場合には１つまたは複数の公衆ＩＰアドレスなどの、追加のオーバーレイＩＰアドレスを割り当てられ得る。これらの複数のアドレスは、同じＶＮＩＣ上で、または、計算インスタンスに関連付けられる複数のＶＮＩＣにわたって、割り当てられる。しかしながら、各インスタンスは、インスタンス立ち上げ中に作成され、インスタンスに割り当てられているオーバーレイプライベートＩＰアドレスに関連付けられる一次ＶＮＩＣを有し、この一次ＶＮＩＣは、削除することができない。二次ＶＮＩＣとして参照される追加のＶＮＩＣを、一次ＶＮＩＣと同じ可用性ドメイン内の既存のインスタンスに追加することができる。すべてのＶＮＩＣが、インスタンスと同じ可用性ドメイン内にある。二次ＶＮＩＣは、一次ＶＮＩＣと同じＶＣＮ内のサブネット内、または、同じＶＣＮもしくは異なるＶＣＮのいずれかの中にある異なるサブネット内にあり得る。

【００８４】

計算インスタンスは、任意選択的に、公衆サブネット内にある場合には公衆ＩＰアドレ

スを割り当てられ得る。サブネットは、サブネットが作成されるときに、公衆サブネットまたはプライベートサブネットのいずれかとして設計することができる。プライベートサブネットとは、サブネット内のリソース（例えば、計算インスタンス）および関連付けられるＶＮＩＣが公衆オーバーレイＩＰアドレスを有することができないことを意味する。公衆サブネットとは、サブネット内のリソースおよび関連付けられるＶＮＩＣが公衆ＩＰアドレスを有することができることを意味する。顧客は、単一の可用性ドメイン内に、または、リージョンもしくはレルム内の複数の可用性ドメインにまたがって存在するように、サブネットを指定することができる。

【００８５】

上述したように、ＶＣＮは、１つまたは複数のサブネットに細分化することができる。ある実施形態において、ＶＣＮ向けに構成された仮想ルータ（ＶＲ）（ＶＣＮ　ＶＲまたは単にＶＲとして参照される）が、ＶＣＮのサブネット間の通信を可能にする。ＶＣＮ内のサブネットについて、ＶＲは、サブネット（すなわち、そのサブネット上の計算インスタンス）が、ＶＣＮ内の他のサブネット上のエンドポイントおよびＶＣＮの外側の他のエンドポイントと通信することを可能にする、そのサブネットの論理ゲートウェイを表す。ＶＣＮ　ＶＲは、ＶＣＮ内のＶＮＩＣと、ＶＣＮに関連付けられる仮想ゲートウェイ（「ゲートウェイ」）との間でトラフィックをルーティングするように構成されている論理エンティティである。ゲートウェイは、図６に関してさらに下記に説明される。ＶＣＮ　ＶＲは、レイヤ３／ＩＰレイヤ概念である。１つの実施形態において、ＶＣＮに対して１つのＶＣＮ　ＶＲが存在し、ＶＣＮ　ＶＲは、可能性として、ＩＰアドレスによってアドレス指定される無限数のポートを有し、ＶＣＮの各サブネットに対して１つのポートがある。このように、ＶＣＮ　ＶＲは、ＶＣＮ　ＶＲが接続される、ＶＣＮ内の各サブネットに対する異なるＩＰアドレスを有する。ＶＲはまた、ＶＣＮ向けに構成されている様々なゲートウェイにも接続されている。ある実施形態において、サブネットのオーバーレイＩＰアドレス範囲からのあるオーバーレイＩＰアドレスは、そのサブネットのＶＣＮ　ＶＲのポートのために予約される。例えば、それぞれ関連付けられるアドレス範囲１０．０／１６および１０．１／１６を有する２つのサブネットを有するＶＣＮを考察する。アドレス範囲１０．０／１６を有するＶＣＮ内の第１のサブネットについて、この範囲からのアドレスは、そのサブネットのＶＣＮ　ＶＲのポートのために予約される。いくつかの事例において、その範囲からの第１のＩＰアドレスが、ＶＣＮ　ＶＲのために予約され得る。例えば、オーバーレイＩＰアドレス範囲１０．０／１６を有するサブネットについて、ＩＰアドレス１０．０．０．１が、そのサブネットのＶＣＮ　ＶＲのポートのために予約され得る。アドレス範囲１０．１／１６を有する同じＶＣＮ内の第２のサブネットについて、ＶＣＮ　ＶＲは、ＩＰアドレス１０．１．０．１を有するその第２のサブネットのポートを有し得る。ＶＣＮ　ＶＲは、ＶＣＮ内のサブネットの各々に対して異なるＩＰアドレスを有する。

【００８６】

いくつかの他の実施形態において、ＶＣＮ内の各サブネットは、ＶＲに関連付けられる予約されたまたはデフォルトのＩＰアドレスを使用してサブネットによってアドレス指定可能であるそれ自体の関連付けられるＶＲを有することができる。予約されたまたはデフォルトのＩＰアドレスは、例えば、そのサブネットに関連付けられるＩＰアドレスの範囲からの第１のＩＰアドレスであり得る。サブネット内のＶＮＩＣは、このデフォルトのまたは予約されたＩＰアドレスを使用して、サブネットに関連付けられるＶＲと通信する（例えば、パケットを送受信する）ことができる。そのような実施形態において、ＶＲは、そのサブネットの進入／退出ポイントである。ＶＣＮ内のサブネットに関連付けられるＶＲは、ＶＣＮ内の他のサブネットに関連付けられる他のＶＲと通信することができる。ＶＲはまた、ＶＣＮに関連付けられるゲートウェイとも通信することができる。サブネットのＶＲ機能は、サブネット内のＶＮＩＣのＶＮＩＣ機能を実行している１つまたは複数のＮＶＤ上で作動しているか、または、それによって実行される。

【００８７】

経路テーブル、セキュリティ規則、およびＤＨＣＰオプションは、ＶＣＮ向けに構成することができる。経路テーブルは、ＶＣＮの仮想経路テーブルであり、ＶＣＮ内のサブネットからのトラフィックを、ゲートウェイまたは特別に構成されたインスタンスによって、ＶＣＮの外側の宛先にルーティングするための規則を含む。ＶＣＮの経路テーブルは、パケットがＶＣＮへと、および、そこからどのように転送／ルーティングされるかを制御するためにカスタマイズすることができる。ＤＨＣＰオプションは、インスタンスが起動するときにインスタンスに自動的に提供される構成情報を指す。

【００８８】

ＶＣＮ向けに構成されているセキュリティ規則は、ＶＣＮに対するオーバーレイファイアウォール規則を表す。セキュリティ規則は、進入および脱出規則を含むことができ、ＶＣＮ内のインスタンスに入ることおよび出ることを許容されるトラフィックのタイプを（プロトコルおよびポートに基づいて）指定することができる。顧客は、所与の規則がステートフルであるかまたはステートレスであるかを選択することができる。例えば、顧客は、ソースＣＩＤＲ０．０．０．０／０および宛先ＴＣＰポート２２を有するステートフル進入規則をセットアップすることによって、任意の場所からのＳＳＨトラフィックがインスタンスのセットに入来することを可能にすることができる。セキュリティ規則は、ネットワークセキュリティグループまたはセキュリティリストを使用して実施することができる。ネットワークセキュリティグループは、そのグループ内のリソースのみに適用されるセキュリティ規則のセットから成る。他方、セキュリティリストは、セキュリティリストを使用する任意のサブネット内のすべてのリソースに適用される規則を含む。ＶＣＮには、デフォルトのセキュリティ規則を有するデフォルトのセキュリティリストを提供することができる。ＶＣＮ向けに構成されているＤＨＣＰオプションは、インスタンスが起動するときにＶＣＮ内のインスタンスに自動的に提供される構成情報を提供する。

【００８９】

ある実施形態において、ＶＣＮの構成情報は、ＶＣＮ制御プレーンによって決定され、記憶される。ＶＣＮの構成情報は、例えば、ＶＣＮに関連付けられるアドレス範囲、ＶＣＮ内のサブネットおよび関連する情報、ＶＣＮに関連付けられる１つまたは複数のＶＲ、ＶＣＮ内の計算インスタンスおよび関連付けられるＶＮＩＣ、ＶＣＮに関連付けられる様々な仮想化ネットワーク機能（例えば、ＶＮＩＣ、ＶＲ、ゲートウェイ）を実行するＮＶＤ、ＶＣＮの状態情報、および他のＶＣＮ関連情報に関する情報を含み得る。ある実施形態において、ＶＣＮ配布サービスは、ＶＣＮ制御プレーンによって記憶されている構成情報またはその一部分をＮＶＤに発行する。配布された情報は、ＶＣＮ内の計算インスタンスへと、および、そこからパケットを転送するために、ＮＶＤによって記憶され、使用される情報（例えば、転送テーブル、ルーティングテーブルなど）を更新するために使用することができる。

【００９０】

ある実施形態において、ＶＣＮおよびサブネットの作成は、ＶＣＮ制御プレーン（ＣＰ）によってハンドリングされ、計算インスタンスの立ち上げは、計算制御プレーンによってハンドリングされる。計算制御プレーンは、計算インスタンスの物理リソースを割り振る役割を担い、次いで、ＶＮＩＣを作成して計算インスタンスに接続するために、ＶＣＮ制御プレーンを呼び出す。ＶＣＮ　ＣＰはまた、パケット転送およびルーティング機能を実施するように構成されているＶＣＮデータプレーンにＶＣＮデータマッピングを送る。ある実施形態において、ＶＣＮ　ＣＰは、ＶＣＮデータプレーンに更新を提供する役割を担う配布サービスを提供する。ＶＣＮ制御プレーンの例は、図１１、図１２、図１３、および図１４にも示されており（参照符号１１１６、１２１６、１３１６、および１４１６参照）、下記に説明される。

【００９１】

顧客は、ＣＳＰＩによってホストされるリソースを使用して１つまたは複数のＶＣＮを作成することができる。顧客ＶＣＮ上に展開される計算インスタンスは、複数の異なるエンドポイントと通信することができる。これらのエンドポイントは、ＣＳＰＩによってホ

ストされるエンドポイントおよびＣＳＰＩの外側のエンドポイントを含み得る。
【００９２】
ＣＳＰＩを使用してクラウドベースのサービスを実施するための様々な異なるアーキテクチャが、図６、図７、図８、図９、図１０、図１１、図１２、図１３、および図１５に示されており、下記に説明される。図６は、ある実施形態によるＣＳＰＩによってホストされるオーバーレイまたは顧客ＶＣＮを示す分散環境６００の高レベル図である。図６に示す分散環境は、オーバーレイネットワーク内の複数の構成要素を含む。図６に示す分散環境６００は、例示に過ぎず、特許請求される実施形態の範囲を不当に限定するようには意図されていない。多くの変形、代替、および修正が可能である。例えば、いくつかの実施態様において、図６に示す分散環境は、図１に示されているよりも多いもしくは少ないシステムもしくは構成要素を有してもよく、２つ以上のシステムを組み合わせてもよく、または、システムの異なる構成もしくは配置を有し得る。
【００９３】
図６に示す例に示すように、分散環境６００は、顧客が加入し、その仮想クラウドネットワーク（ＶＣＮ）を構築するために使用することができるサービスおよびリソースを提供するＣＳＰＩ６０１を備える。ある実施形態において、ＣＳＰＩ６０１は、加入している顧客にＩａａＳサービスを供給する。ＣＳＰＩ６０１内のデータセンタは、１つまたは複数のリージョンに編成することができる。１つの例示的なリージョンである「リージョンＵＳ」６０２が、図６に示されている。顧客は、リージョン６０２の顧客ＶＣＮ６０４を構成している。顧客は、ＶＣＮ６０４上に様々な計算インスタンスを展開することができ、ここで、計算インスタンスは、仮想マシンまたはベアメタルインスタンスを含み得る。インスタンスの例は、アプリケーション、データベース、ロードバランサなどを含む。
【００９４】
図６に示す実施形態において、顧客ＶＣＮ６０４は、２つのサブネット、すなわち「サブネット１」および「サブネット２」を含み、各サブネットが、それ自体のＣＩＤＲ　ＩＰアドレス範囲を有する。図６において、サブネット１のオーバーレイＩＰアドレス範囲は１０．０／１６であり、サブネット２のアドレス範囲は１０．１／１６である。ＶＣＮ仮想ルータ６０５は、ＶＣＮ６０４のサブネット間の、および、ＶＣＮの外側の他のエンドポイントとの通信を可能にする、ＶＣＮの論理ゲートウェイを表す。ＶＣＮ　ＶＲ６０５は、ＶＣＮ６０４内のＶＮＩＣと、ＶＣＮ６０４に関連付けられるゲートウェイとの間でトラフィックをルーティングするように構成されている。ＶＣＮ　ＶＲ６０５は、ＶＣＮ６０４の各サブネットのポートを提供する。例えば、ＶＲ６０５は、サブネット１のＩＰアドレス１０．０．０．１を有するポート、および、サブネット２のＩＰアドレス１０．１．０．１を有するポートを提供することができる。
【００９５】
複数の計算インスタンスが、各サブネット上に展開されてもよく、ここで、計算インスタンスは、仮想マシンインスタンスおよび／またはベアメタルインスタンスとすることができる。サブネット内の計算インスタンスは、ＣＳＰＩ６０１内の１つまたは複数のホストマシンによってホストすることができる。計算インスタンスは、計算インスタンスに関連付けられるＶＮＩＣを介してサブネットに参加する。例えば、図６に示すように、計算インスタンスＣ１は、計算インスタンスに関連付けられるＶＮＩＣを介する、サブネット１の一部である。同様に、計算インスタンスＣ２は、Ｃ２に関連付けられるＶＮＩＣを介する、サブネット１の一部である。同様に、仮想マシンインスタンスまたはベアメタルインスタンスであり得る複数の計算インスタンスが、サブネット１の一部であり得る。その関連付けられるＶＮＩＣを介して、各計算インスタンスは、プライベートオーバーレイＩＰアドレスおよびＭＡＣアドレスを割り当てられる。例えば、図６において、計算インスタンスＣ１は、１０．０．０．２のオーバーレイＩＰアドレスおよびＭ１のＭＡＣアドレスを有し、一方、計算インスタンスＣ２は、１０．０．０．３のプライベートオーバーレイＩＰアドレスおよびＭ２のＭＡＣアドレスを有する。計算インスタンスＣ１およびＣ２を含む、サブネット１内の各計算インスタンスは、サブネット１のＶＣＮ　ＶＲ６０５の

ポートのＩＰアドレスである、ＩＰアドレス１０．０．０．１を使用するＶＣＮ　ＶＲ６０５までのデフォルトの経路を有する。

【００９６】

サブネット２は、仮想マシンインスタンスおよび／またはベアメタルインスタンスを含む、複数の計算インスタンスをその上に展開され得る。例えば、図６に示すように、計算インスタンスＤ１およびＤ２は、それぞれの計算インスタンスに関連付けられるＶＮＩＣを介する、サブネット２の一部である。図６に示す実施形態おいて、計算インスタンスＤ１は、１０．１．０．２のオーバーレイＩＰアドレスおよびＭＭ１のＭＡＣアドレスを有し、一方、計算インスタンスＤ２は、１０．１．０．３のプライベートオーバーレイＩＰアドレスおよびＭＭ２のＭＡＣアドレスを有する。計算インスタンスＤ１およびＤ２を含む、サブネット２内の各計算インスタンスは、サブネット２のＶＣＮ　ＶＲ６０５のポートのＩＰアドレスである、ＩＰアドレス１０．１．０．１を使用するＶＣＮ　ＶＲ６０５までのデフォルトの経路を有する。

【００９７】

ＶＣＮ　Ａ６０４はまた、１つまたは複数のロードバランサを含み得る。例えば、ロードバランサは、サブネットのために提供されてもよく、サブネット上の複数の計算インスタンスにわたってトラフィックを負荷平衡させるように構成され得る。ロードバランサはまた、ＶＣＮ内のサブネットにわたってトラフィックを負荷平衡させるために提供され得る。

【００９８】

ＶＣＮ６０４上に展開される特定の計算インスタンスは、様々な異なるエンドポイントと通信することができる。これらのエンドポイントは、ＣＳＰＩ７００によってホストされるエンドポイントおよびＣＳＰＩ７００の外側のエンドポイントを含み得る。ＣＳＰＩ６０１によってホストされるエンドポイントは、特定の計算インスタンスと同じサブネット上のエンドポイント（例えば、サブネット１内の２つの計算インスタンス間の通信）、異なるサブネット上の、ただし同じＶＣＮ内のエンドポイント（例えば、サブネット１内の計算インスタンスとサブネット２内の計算インスタンスとの間の通信）、同じリージョン内の異なるＶＣＮ内のエンドポイント（例えば、サブネット１内の計算インスタンスと同じリージョン６０６または６１０内のＶＣＮ内のエンドポイントとの間の通信、サブネット１内の計算インスタンスと同じリージョン内のサービスネットワーク６１０内のエンドポイントとの間の通信）、または、異なるリージョン内のＶＣＮ内のエンドポイント（例えば、サブネット１内の計算インスタンスと異なるリージョン６０８内のＶＣＮ内のエンドポイントとの間の通信）を含み得る。ＣＳＰＩ６０１によってホストされるサブネット内の計算インスタンスはまた、ＣＳＰＩ６０１によってホストされない（すなわち、ＣＳＰＩ６０１の外側にある）エンドポイントとも通信し得る。これらの外側エンドポイントは、顧客のオンプレミスネットワーク６１６内のエンドポイント、他のリモートクラウドホストネットワーク６１８内のエンドポイント、インターネットなどの公衆ネットワークを介してアクセス可能な公衆エンドポイント６１４、および他のエンドポイントを含む。

【００９９】

同じサブネット上の計算インスタンス間の通信は、ソース計算インスタンスおよび宛先計算インスタンスに関連付けられるＶＮＩＣを使用して促進される。例えば、サブネット１内の計算インスタンスＣ１は、サブネット１内の計算インスタンスＣ２にパケットを送ることを所望し得る。ソース計算インスタンスに由来し、その宛先が同じサブネット内の別の計算インスタンスであるパケットについて、パケットは、最初に、ソース計算インスタンスに関連付けられるＶＮＩＣによって処理される。ソース計算インスタンスに関連付けられるＶＮＩＣによって実施される処理は、パケットヘッダからパケットの宛先情報を決定すること、ソース計算インスタンスに関連付けられるＶＮＩＣ向けに構成されている任意のポリシ（例えば、セキュリティリスト）を識別すること、パケットの次のホップを決定すること、必要に応じて任意のカプセル化／カプセル化解除機能を実施すること、お

よび、次いで、パケットのその意図される宛先への通信を促進することを目標としてパケットを次のホップに転送／ルーティングすることを含み得る。宛先計算インスタンスがソース計算インスタンスと同じサブネット内にあるとき、ソース計算インスタンスに関連付けられるＶＮＩＣは、宛先計算インスタンスに関連付けられるＶＮＩＣを識別し、パケットを処理のためにそのＶＮＩＣに転送するように構成されている。このとき、宛先計算インスタンスに関連付けられるＶＮＩＣが実行され、パケットを宛先計算インスタンスに転送する。

【０１００】

パケットがサブネット内の計算インスタンスから同じＶＣＮ内の異なるサブネット内のエンドポイントに通信されるようにするために、ソースおよび宛先計算インスタンスに関連付けられるＶＮＩＣおよびＶＣＮ　ＶＲによって通信が促進される。例えば、図６のサブネット１内の計算インスタンスＣ１が、サブネット２内の計算インスタンスＤ１にパケットを送ることを所望する場合、パケットは、最初に、計算インスタンスＣ１に関連付けられるＶＮＩＣによって処理される。計算インスタンスＣ１に関連付けられるＶＮＩＣは、ＶＣＮ　ＶＲのデフォルトの経路またはポート１０．０．０．１を使用して、パケットをＶＣＮ　ＶＲ６０５にルーティングするように構成されている。ＶＣＮ　ＶＲ６０５は、ポート１０．１．０．１を使用してパケットをサブネット２にルーティングするように構成されている。次いで、パケットは、Ｄ１に関連付けられるＶＮＩＣによって受信および処理され、ＶＮＩＣは、パケットを計算インスタンスＤ１に転送する。

【０１０１】

パケットがＶＣＮ６０４内の計算インスタンスからＶＣＮ６０４の外側にあるエンドポイントに通信されるようにするために、ソース計算インスタンスに関連付けられるＶＮＩＣ、ＶＣＮ　ＶＲ６０５、およびＶＣＮ６０４に関連付けられるゲートウェイによって通信が促進される。１つまたは複数のタイプのゲートウェイが、ＶＣＮ６０４に関連付けられ得る。ゲートウェイは、ＶＣＮと別のエンドポイントとの間のインターフェイスであり、ここで、別のエンドポイントは、ＶＣＮの外部にある。ゲートウェイは、レイヤ３／ＩＰレイヤ概念であり、ＶＣＮがＶＣＮの外側のエンドポイントと通信することを可能にする。したがって、ゲートウェイは、ＶＣＮと他のＶＣＮまたはネットワークとの間のトラフィックフローを促進する。様々な異なるタイプのゲートウェイが、異なるタイプのエンドポイントとの異なるタイプの通信を促進するために、ＶＣＮ向けに構成され得る。ゲートウェイに応じて、通信は、公衆ネットワーク（例えば、インターネット）またはプライベートネットワークを介するものであり得る。様々な通信プロトコルがこれらの通信に使用され得る。

【０１０２】

例えば、計算インスタンスＣ１は、ＶＣＮ６０４の外側のエンドポイントと通信することを所望し得る。パケットは、最初に、ソース計算インスタンスＣ１に関連付けられるＶＮＩＣによって処理され得る。ＶＮＩＣ処理は、パケットの宛先がＣ１のサブネット１の外側にあると判定する。Ｃ１に関連付けられるＶＮＩＣは、ＶＣＮ６０４のＶＣＮ　ＶＲ６０５にパケットを転送することができる。次いで、ＶＣＮ　ＶＲ６０５は、パケットを処理し、処理の一部として、パケットの宛先に基づいて、ＶＣＮ６０４に関連付けられる特定のゲートウェイを、パケットの次のホップとして決定する。次いで、ＶＣＮ　ＶＲ６０５は、特定の識別されたゲートウェイにパケットを転送することができる。例えば、宛先が顧客のオンプレミスネットワーク内のエンドポイントである場合、パケットは、ＶＣＮ　ＶＲ６０５によって、ＶＣＮ６０４向けに構成されている動的ルーティングゲートウェイ（ＤＲＧ）ゲートウェイ６２２に転送することができる。次いで、パケットは、パケットの、最終的な意図される宛先への通信を促進するために、ゲートウェイから次のホップへと転送することができる。

【０１０３】

様々な異なるタイプのゲートウェイが、ＶＣＮ向けに構成され得る。ＶＣＮ向けに構成することができるゲートウェイの例が、図６に示されており、下記に説明される。ＶＣＮ

に関連付けられるゲートウェイの例はまた、図１１、図１２、図１３、および図１４にも示されており（例えば、参照符号１１３４、１１３６、１１３８、１２３４、１２３６、１２３８、１３３４、１３３６、１３３８、１４３４、１４３６、および１４３８によって参照されるゲートウェイ）、下記に説明される。図６に示す実施形態に示すように、動的ルーティングゲートウェイ（ＤＲＧ）６２２は、顧客ＶＣＮ６０４に追加することができるか、または、それに関連付けることができ、顧客ＶＣＮ６０４と別のエンドポイントとの間のプライベートネットワークトラフィック通信のための経路を提供し、ここで、別のエンドポイントは、顧客のオンプレミスネットワーク６１６、ＣＳＰＩ６０１の異なるリージョン内のＶＣＮ６０８、または、ＣＳＰＩ６０１によってホストされない他のリモートクラウドネットワーク６１８とすることができる。顧客オンプレミスネットワーク６１６は、顧客のリソースを使用して構築されている顧客ネットワークまたは顧客データセンタであり得る。顧客オンプレミスネットワーク６１６へのアクセスは、一般的に、非常に制限されている。顧客オンプレミスネットワーク６１６とＣＳＰＩ６０１によってクラウド内で展開またはホストされている１つまたは複数のＶＣＮ６０４の両方を有する顧客について、顧客は、そのオンプレミスネットワーク６１６およびそのクラウドベースのＶＣＮ６０４が、互いに通信することが可能であることを所望し得る。これによって、顧客が、ＣＳＰＩ６０１によってホストされる顧客のＶＣＮ６０４およびそのオンプレミスネットワーク６１６を包含する拡張ハイブリッド環境を構築することが可能になる。ＤＲＧ６２２が、この通信を可能にする。そのような通信を可能にするために、通信チャネル６２４がセットアップされ、ここで、チャネルの１つのエンドポイントは顧客オンプレミスネットワーク６１６であり、他方のエンドポイントはＣＳＰＩ６０１であり、顧客ＶＣＮ６０４に接続されている。通信チャネル６２４は、インターネットなどの公衆通信ネットワークまたはプライベート通信ネットワークを介するものとすることができる。インターネットなどの公衆通信ネットワークを介したＩＰｓｅｃ　ＶＰＮ技術、公衆ネットワークの代わりにプライベートネットワークを使用するＯｒａｃｌｅのFastConnect技術などの、様々な異なる通信プロトコルが使用され得る。通信チャネル６２４の１つのエンドポイントを形成する顧客オンプレミスネットワーク６１６内のデバイスまたは設備は、図６に示すＣＰＥ６２６などの、顧客構内設備（ＣＰＥ）として参照される。ＣＳＰＩ６０１側では、エンドポイントは、ＤＲＧ６２２を実行するホストマシンであり得る。

【０１０４】

ある実施形態において、リモートピアリング接続（ＲＰＣ）をＤＲＧに追加することができ、これによって、顧客が、１つのＶＣＮを異なるリージョン内の別のＶＣＮとピアリングすることが可能になる。そのようなＲＰＣを使用して、顧客ＶＣＮ６０４は、ＤＲＧ６２２を使用して別のリージョン内のＶＣＮ６０８と接続することができる。ＤＲＧ６２２はまた、Ｍｉｃｒｏｓｏｆｔ　Ａｚｕｒｅクラウド、Ａｍａｚｏｎ　ＡＷＳクラウドなどのような、ＣＳＰＩ６０１によってホストされていない、他のリモートクラウドネットワーク６１８と通信するために使用することもできる。

【０１０５】

図６に示すように、インターネットゲートウェイ（ＩＧＷ）６２０は、ＶＣＮ６０４上の計算インスタンスがインターネットなどの公衆ネットワークを介してアクセス可能な公衆エンドポイント６１４と通信することを可能にするように、顧客ＶＣＮ６０４向けに構成することができる。ＩＧＷ６２０は、インターネットなどの公衆ネットワークにＶＣＮを接続するゲートウェイである。ＩＧＷ６２０は、ＶＣＮ６０４などのＶＣＮ内の公衆サブネット（ここで、公衆サブネット内のリソースは公衆オーバーレイＩＰアドレスを有する）が、インターネットなどの公衆ネットワーク６１４上の公衆エンドポイント６１２に直接的にアクセスすることを可能にする。ＩＧＷ６２０を使用して、ＶＣＮ６０４内のサブネットまたはインターネットからの接続を開始することができる。

【０１０６】

ネットワークアドレス変換（ＮＡＴ）ゲートウェイ６２８は、顧客のＶＣＮ６０４向けに構成することができ、専用公衆オーバーレイＩＰアドレスを有しない顧客のＶＣＮ内の

クラウドリソースが、インターネットにアクセスすることを可能にし、それらのリソースを直接入来インターネット接続（例えば、Ｌ４～Ｌ７接続）に暴露することなく、これを行う。これによって、ＶＣＮ６０４内のプライベートサブネット１などの、ＶＣＮ内のプライベートサブネットが、インターネット上の公衆エンドポイントへのプライベートアクセスを有することが可能になる。ＮＡＴゲートウェイにおいて、接続は、インターネットからプライベートサブネットへとではなく、プライベートサブネットから公衆インターネットへとのみ開始することができる。

【０１０７】

ある実施形態において、サービスゲートウェイ（ＳＧＷ）６２６は、顧客ＶＣＮ６０４向けに構成することができ、ＶＣＮ６０４とサービスネットワーク６１０内のサポートされているサービスエンドポイントとの間のプライベートネットワークトラフィックのための経路を提供する。ある実施形態において、サービスネットワーク６１０は、ＣＳＰによって提供することができ、様々なサービスを提供することができる。そのようなサービスネットワークの一例は、顧客によって使用することができる様々なサービスを提供するＯｒａｃｌｅのサービスネットワークである。例えば、顧客ＶＣＮ６０４のプライベートサブネット内の計算インスタンス（例えば、データベースシステム）は、公衆ＩＰアドレスまたはインターネットへのアクセスを必要とすることなく、データをサービスエンドポイント（例えば、オブジェクトストレージ）にバックアップすることができる。ある実施形態において、ＶＣＮは、１つのみのＳＧＷを有することができ、接続は、サービスネットワーク６１０からではなく、ＶＣＮ内のサブネットからのみ開始することができる。ＶＣＮが別のＶＣＮとピアリングされる場合、他のＶＣＮ内のリソースは、ＳＧＷにアクセスすることができない。FastConnectまたはVPN ConnectによってＶＣＮに接続されるオンプレミスネットワーク内のリソースもまた、そのＶＣＮ向けに構成されているサービスゲートウェイを使用することができる。

【０１０８】

ある実施態様において、ＳＧＷ６２６は、関心のあるサービスまたはサービスグループのすべてのリージョン公衆ＩＰアドレス範囲を表す文字列である、サービスクラスレスドメイン間ルーティング（ＣＩＤＲ）ラベルの概念を使用する。顧客は、ＳＧＷおよび関連する経路規則を、サービスへのトラフィックを制御するように構成するときに、サービスＣＩＤＲラベルを使用する。顧客は、任意選択的に、サービスの公衆ＩＰアドレスが将来的に変化する場合にセキュリティ規則を構成するときに、それらのセキュリティ規則を調整することを必要とすることなく、サービスＣＩＤＲラベルを利用することができる。

【０１０９】

ローカルピアリングゲートウェイ（ＬＰＧ）６３２は、顧客ＶＣＮ６０４に追加することができるゲートウェイであり、ＶＣＮ６０４が同じリージョン内の別のＶＣＮとピアリングすることを可能にする。ピアリングとは、トラフィックがインターネットなどの公衆ネットワークをトラバースすることなく、または、顧客のオンプレミスネットワーク６１６を通じてトラフィックをルーティングすることなく、ＶＣＮがプライベートＩＰアドレスを使用して通信することを意味する。好ましい実施形態において、ＶＣＮは、それが確立する各ピアリングのための別個のＬＰＧを有する。ローカルピアリングまたはＶＣＮピアリングは、異なるアプリケーションまたはインフラストラクチャ管理機能の間にネットワーク接続を確立するために使用される一般的な慣行である。

【０１１０】

サービスネットワーク６１０内のサービスのプロバイダなどのサービスプロバイダは、異なるアクセスモデルを使用してサービスへのアクセスを提供することができる。公衆アクセスモデルによれば、サービスは、インターネットなどの公衆ネットワークを介して顧客ＶＣＮ内の計算インスタンスによってパブリックにアクセス可能である公衆エンドポイントとして暴露されてもよく、または、ＳＧＷ６２６を介してプライベートにアクセス可能であり得る。特定のプライベートアクセスモデルによれば、サービスは、顧客のＶＣＮ内のプライベートサブネット内のプライベートＩＰエンドポイントとしてアクセス可能に

される。これは、プライベートエンドポイント（ＰＥ）アクセスとして参照され、サービスプロバイダが、顧客のプライベートネットワーク内のインスタンスとしてそれらのサービスを暴露することを可能にする。プライベートエンドポイントリソースは、顧客のＶＣＮ内のサービスを表す。各ＰＥは、顧客のＶＣＮ内の顧客によって選択されるサブネット内のＶＮＩＣ（１つまたは複数のプライベートＩＰを有するＰＥ－ＶＮＩＣとして参照される）として現れる。したがって、ＰＥは、ＶＮＩＣを使用してプライベート顧客ＶＣＮサブネット内にサービスを提示するための方法を提供する。エンドポイントはＶＮＩＣとして暴露されるため、ルーティング規則、セキュリティリストなどのようなＶＮＩＣに関連付けられるすべての特徴が、この時点でＰＥ　ＶＮＩＣにとって利用可能にされる。

【０１１１】

サービスプロバイダは、ＰＥを通じたアクセスを可能にするために、そのサービスを登録することができる。プロバイダは、ポリシをサービスに関連付けることができ、それによって、サービスの可視性が顧客テナンシに制約される。プロバイダは、特にマルチテナントサービスについて、単一の仮想ＩＰアドレス（ＶＩＰ）の下で複数のサービスを登録することができる。同じサービスを表す複数のそのようなプライベートエンドポイント（複数のＶＣＮ内の）が存在し得る。

【０１１２】

このとき、プライベートサブネット内の計算インスタンスは、ＰＥ　ＶＮＩＣのプライベートＩＰアドレスまたはサービスＤＮＳ名を使用して、サービスにアクセスすることができる。顧客ＶＣＮ内の計算インスタンスは、顧客ＶＣＮ内のＰＥのプライベートＩＰアドレスにトラフィックを送ることによって、サービスにアクセスすることができる。プライベートアクセスゲートウェイ（ＰＡＧＷ）６３０は、顧客サブネットプライベートエンドポイントからの／へのすべてのトラフィックの侵入／退出ポイントとして作用するサービスプロバイダＶＣＮ（例えば、サービスネットワーク６１０内のＶＣＮ）に接続することができるゲートウェイリソースである。ＰＡＧＷ６３０は、プロバイダが、その内部ＩＰアドレスリソースを利用することなくＰＥ接続の数をスケーリングすることを可能にする。プロバイダは、単一のＶＣＮ内に登録されている任意の数のサービスに対して、１つのＰＡＧＷを構成することのみを必要とする。プロバイダは、サービスを、１または複数の顧客の複数のＶＣＮ内のプライベートエンドポイントとして表すことができる。顧客の観点から、ＰＥ　ＶＮＩＣは、顧客のインスタンスに接続される代わりに、顧客がインタラクトすることを所望するサービスに接続されるように見える。プライベートエンドポイントに宛てられたトラフィックは、ＰＡＧＷ６３０を介してサービスへとルーティングされる。これらは、顧客－サービスプライベート接続（Ｃ２Ｓ接続）として参照される。

【０１１３】

ＰＥ概念はまた、トラフィックがFastConnect/IPsecリンクおよび顧客ＶＣＮ内のプライベートエンドポイントを通じて流れることを可能にすることによって、サービスのためのプライベートアクセスを顧客のオンプレミスネットワークおよびデータセンタへと拡張するために使用することもできる。サービスのためのプライベートアクセスはまた、トラフィックがＬＰＧ６３２と顧客のＶＣＮ内のＰＥとの間を流れることを可能にすることによって、顧客のピアリングされたＶＣＮへと拡張することもできる。

【０１１４】

顧客は、ＶＣＮにおけるルーティングをサブネットレベルで制御することができ、したがって、顧客は、ＶＣＮ６０４などの顧客のＶＣＮのいずれのサブネットが各ゲートウェイを使用するかを指定することができる。トラフィックが特定のゲートウェイを通じてＶＣＮを出ることを可能にされるか否かを判断するために、ＶＣＮの経路テーブルが使用される。例えば、特定の事例において、顧客ＶＣＮ６０４内の公衆サブネットの経路テーブルは、ＩＧＷ６２０を通じて非ローカルトラフィックを送ることができる。同じ顧客ＶＣＮ６０４内のプライベートサブネットの経路テーブルが、ＳＧＷ６２６を通じてＣＳＰサービスに宛てられたトラフィックを送ることができる。すべての残りのトラフィックは、ＮＡＴゲートウェイ６２８を介して送ることができる。経路テーブルは、ＶＣＮから出る

トラフィックのみを制御する。

【０１１５】

着信接続を介して、ゲートウェイを介してＶＣＮに入来するトラフィックを制御するために、ＶＣＮに関連付けられるセキュリティリストが使用される。サブネット内のすべてのリソースが、同じ経路テーブルおよびセキュリティリストを使用する。セキュリティリストは、ＶＣＮのサブネット内のインスタンスに入ることおよび出ることを可能にされる特定のタイプのトラフィックを制御するために使用することができる。セキュリティリスト規則は、進入（着信）および退出（発信）規則を含み得る。例えば、進入規則は、許容されるソースアドレス範囲を指定することができ、一方、退出規則は、許容される宛先アドレス範囲を指定することができる。セキュリティ規則は、特定のプロトコル（例えば、TCP、ICMP）、特定のポート（例えば、ＳＳＨのための２２、Windows（登録商標）RDPのための３３８９）などを指定することができる。ある実施態様において、インスタンスのオペレーティングシステムは、セキュリティリスト規則と整合されているそれ自体のファイアウォール規則を執行することができる。規則は、ステートフル（例えば、接続が追跡され、応答が、応答トラフィックに対する明示的なセキュリティリスト規則なしに、自動的に許可される）であってもよく、または、ステートレスであり得る。

【０１１６】

顧客ＶＣＮからの（すなわち、ＶＣＮ６０４上に展開されているリソースまたは計算インスタンスによる）アクセスは、公衆アクセス、プライベートアクセス、または専用アクセスとしてカテゴライズすることができる。公衆アクセスは、公衆ＩＰアドレスまたはＮＡＴが公衆エンドポイントにアクセスするために使用されるアクセスモデルを指す。プライベートアクセスは、プライベートＩＰアドレスを有するＶＣＮ６０４内の顧客ワークロード（例えば、プライベートサブネット内のリソース）が、インターネットなどの公衆ネットワークをトラバースすることなく、サービスにアクセスすることを可能にする。ある実施形態において、ＣＳＰＩ６０１は、プライベートＩＰアドレスを有する顧客ＶＣＮワークロードが、サービスゲートウェイを使用してサービス（の公衆サービスエンドポイント）にアクセスすることを可能にする。したがって、サービスゲートウェイは、顧客のＶＣＮと顧客のプライベートネットワークの外側に存在するサービスのエンドポイントとの間の仮想リンクを確立することによって、プライベートアクセスモデルを供給する。

【０１１７】

付加的に、ＣＳＰＩは、顧客オンプレミスインスタンスがFastConnect接続を使用して、インターネットなどの公衆ネットワークをトラバースすることなく顧客ＶＣＮ内の１つまたは複数のサービスにアクセスすることができるFastConnect公衆ピアリングなどの技術を使用して、専用公衆アクセスを供給することができる。ＣＳＰＩはまた、プライベートＩＰアドレスを有する顧客オンプレミスインスタンスがFastConnect接続を使用して顧客のＶＣＮワークロードにアクセスすることができるFastConnectプライベートピアリングを使用して専用プライベートアクセスを供給することもできる。FastConnectは、顧客のオンプレミスネットワークをＣＳＰＩおよびそのサービスに接続するための、公衆インターネットを使用することに代わるネットワーク接続である。FastConnectは、インターネットベースの接続と比較して、より高い帯域幅オプションおよびより信頼性が高く一貫したネットワーキング体験を有する、専用のプライベート接続を作成するための容易、弾性的かつ経済的な方法を提供する。

【０１１８】

図６および上記の付随する説明は、例示的な仮想ネットワークにおける様々な仮想化構成要素を記載している。上述したように、仮想ネットワークは、下層の物理または基盤ネットワーク上に構築される。図７は、ある実施形態による、仮想ネットワークの下層を提供するＣＳＰＩ７００内の物理ネットワーク内の物理構成要素の単純化されたアーキテクチャ図を示す。図示のように、ＣＳＰＩ７００は、クラウドサービスプロバイダ（ＣＳＰ）によって提供される構成要素およびリソース（例えば、計算、メモリ、およびネットワーキングリソース）を含む分散環境を提供する。これらの構成要素およびリソースは、加

入顧客、すなわち、ＣＳＰによって提供される１つまたは複数のサービスに加入している顧客にクラウドサービス（例えば、ＩａａＳサービス）を提供するために使用される。顧客が加入しているサービスに基づいて、ＣＳＰＩ７００のリソース（例えば、計算、メモリ、およびネットワーキングリソース）のサブセットが顧客にプロビジョンされる。その後、顧客は、ＣＳＰＩ７００によって提供される物理計算、メモリ、およびネットワーキングリソースを使用して、自身のクラウドベースの（すなわち、ＣＳＰＩによってホストされる）カスタマイズ可能なプライベート仮想ネットワークを構築することができる。前に示したように、これらの顧客ネットワークは、仮想クラウドネットワーク（ＶＣＮ）として参照される。顧客は、これらの顧客ＶＣＮ上で、計算インスタンスなどの１つまたは複数の顧客リソースを展開することができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどの形態とすることができる。ＣＳＰＩ７００は、顧客が多様なアプリケーションおよびサービスを可用性の高いホスト環境内で構築し、実行することを可能にするインフラストラクチャ、および、補完クラウドサービスのセットを提供する。

【０１１９】

図７に示す例示的な実施形態において、ＣＳＰＩ７００の物理構成要素は、１つまたは複数の物理ホストマシンまたは物理サーバ（例えば、７０２、７０６、７０８）、ネットワーク仮想化デバイス（ＮＶＤ）（例えば、７１０、７１２）、トップオブラック（ＴＯＲ）スイッチ（例えば、７１４、７１６）、および物理ネットワーク（例えば、７１８）、ならびに物理ネットワーク７１８内のスイッチを含む。物理ホストマシンまたはサーバは、ＶＣＮの１つまたは複数のサブネットに参加する様々な計算インスタンスをホストし、実行することができる。計算インスタンスは、仮想マシンインスタンスまたはベアメタルインスタンスを含み得る。例えば、図６に示す様々な計算インスタンスが、図７に示す物理ホストマシンによってホストされ得る。ＶＣＮ内の仮想マシン計算インスタンスは、１つホストマシンによって実行されてもよく、または、複数の異なるホストマシンによって実行され得る。物理ホストマシンはまた、仮想ホストマシン、コンテナベースのホストまたは機能などをホストすることもできる。図６に示すＶＮＩＣおよびＶＣＮ　ＶＲが、図７に示すＮＶＤによって実行され得る。図６に示すゲートウェイが、図７に示すホストマシンおよび／またはＮＶＤによって実行され得る。

【０１２０】

ホストマシンまたはサーバは、ホストマシン上で仮想化環境を作成し、イネーブルするハイパーバイザ（仮想マシンモニタまたはＶＭＭとしても参照される）を実行することができる。仮想化または仮想化環境は、クラウドベースのコンピューティングを促進する。１つまたは複数の計算インスタンスは、ホストマシン上で、そのホストマシン上のハイパーバイザによって作成、実行、および管理することができる。ホストマシン上のハイパーバイザは、ホストマシンの物理コンピューティングリソース（例えば、計算、メモリ、およびネットワーキングリソース）が、ホストマシンによって実行される様々な計算インスタンス間で共有されることを可能にする。

【０１２１】

例えば、図７に示すように、ホストマシン７０２および７０８は、それぞれハイパーバイザ７６０および７６６を実行する。これらのハイパーバイザは、ソフトウェア、ファームウェア、もしくはハードウェア、またはそれらの組合せを使用して実装され得る。典型的には、ハイパーバイザは、ホストマシンのハードウェアプロセッサ上で作動する、ホストマシンのオペレーティングシステム（ＯＳ）の上にあるプロセスまたはソフトウェア層である。ハイパーバイザは、ホストマシンの物理コンピューティングリソース（例えば、プロセッサ／コア、メモリリソース、ネットワーキングリソースなどの処理リソース）が、ホストマシンによって実行される様々な仮想マシン計算インスタンス間で共有されることを可能にすることによって、仮想化環境を提供する。例えば、図７において、ハイパーバイザ７６０は、ホストマシン７０２のＯＳの上にあることができ、ホストマシン７０２のコンピューティングリソース（例えば、処理、メモリ、およびネットワーキングリソース）がホストマシン７０２によって実行される計算インスタンス（例えば、仮想マシン）

間で共有されることを可能にする。仮想マシンは、ホストマシンのＯＳと同じであってもよく、または、異なってもよい、それ自体のオペレーティングシステム（ゲストオペレーティングシステムとして参照される）を有することができる。ホストマシンによって実行される仮想マシンのオペレーティングシステムは、同じホストマシンによって実行される別の仮想マシンのオペレーティングシステムと同じであってもよく、または異なってもよい。したがって、ハイパーバイザは、複数のオペレーティングシステムが、ホストマシンの同じコンピューティングリソースを共有しながら、互いに並行して実行されることを可能にする。図７に示すホストマシンは、同じまたは異なるタイプのハイパーバイザを有し得る。

【０１２２】

計算インスタンスは、仮想マシンインスタンスまたはベアメタルインスタンスとすることができる。図７において、ホストマシン７０２上の計算インスタンス７６８およびホストマシン７０８上の計算インスタンス７７４は、仮想マシンインスタンスの例である。ホストマシン７０６は、顧客に提供されるベアメタルインスタンスの一例である。

【０１２３】

ある事例において、ホストマシン全体が、単一の顧客にプロビジョンされてもよく、そのホストマシンによってホストされる１つまたは複数の計算インスタンス（仮想マシンまたはベアメタルインスタンスのいずれか）のすべてが、その同じ顧客に属する。他の事例において、ホストマシンは、複数の顧客（すなわち、複数のテナント）間で共有され得る。そのようなマルチテナンシシナリオにおいて、ホストマシンは、異なる顧客に属するホスト仮想マシン計算インスタンスをホストし得る。これらの計算インスタンスは、異なる顧客の異なるＶＣＮのメンバであり得る。ある実施形態において、ベアメタル計算インスタンスは、ハイパーバイザを用いずにベアメタルサーバによってホストされる。ベアメタル計算インスタンスがプロビジョンされるとき、単一の顧客またはテナントが、ベアメタルインスタンスをホストするホストマシンの物理ＣＰＵ、メモリ、およびネットワークインターフェイスの制御を維持し、ホストマシンは、他の顧客またはテナントと共有されない。

【０１２４】

前述したように、ＶＣＮの一部である各計算インスタンスは、計算インスタンスがＶＣＮのサブネットのメンバになることを可能にするＶＮＩＣに関連付けられる。計算インスタンスに関連付けられるＶＮＩＣは、計算インスタンスへのおよびそこからのパケットまたはフレームの通信を促進する。計算インスタンスが作成されると、ＶＮＩＣが計算インスタンスに関連付けられる。ある実施形態において、ホストマシンによって実行される計算インスタンスについて、その計算インスタンスに関連付けられるＶＮＩＣは、ホストマシンに接続されているＮＶＤによって実行される。例えば、図７において、ホストマシン７０２は、ＶＮＩＣ７７６に関連付けられる仮想マシン計算インスタンス７６８を実行し、ＶＮＩＣ７７６は、ホストマシン７０２に接続されているＮＶＤ７１０によって実行される。別の例として、ホストマシン７０６によってホストされるベアメタルインスタンス７７２は、ホストマシン７０６に接続されているＮＶＤ７１２によって実行されるＶＮＩＣ７８０に関連付けられる。さらに別の例として、ＶＮＩＣ７８４は、ホストマシン７０８によって実行される計算インスタンス７７４に関連付けられ、ＶＮＩＣ７８４は、ホストマシン７０８に接続されているＮＶＤ７１２によって実行される。

【０１２５】

ホストマシンによってホストされる計算インスタンスについて、そのホストマシンに接続されているＮＶＤはまた、計算インスタンスがそのメンバであるＶＣＮに対応するＶＣＮ　ＶＲも実行する。例えば、図７に示す実施形態において、ＮＶＤ７１０は、計算インスタンス７６８がそのメンバであるＶＣＮに対応するＶＣＮ　ＶＲ７７７を実行する。ＮＶＤ７１２はまた、ホストマシン７０６および７０８によってホストされる計算インスタンスに対応するＶＣＮに対応する１つまたは複数のＶＣＮ　ＶＲ７８３も実行することができる。

【０１２６】
ホストマシンは、ホストマシンが他のデバイスに接続されることを可能にする１つまたは複数のネットワークインターフェイスカード（ＮＩＣ）を含み得る。ホストマシン上のＮＩＣは、ホストマシンが別のデバイスに通信可能に接続されることを可能にする１つまたは複数のポートを提供することができる。例えば、ホストマシンは、ホストマシンおよびＮＶＤ上に設けられた１つまたは複数のポート（またはインターフェイス）を使用してＮＶＤに接続され得る。ホストマシンはまた、別のホストマシンなどの他のデバイスにも接続され得る。
【０１２７】
例えば、図７において、ホストマシン７０２は、ホストマシン７０２のＮＩＣ７３２によって提供されるポート７３４の間およびＮＶＤ７１０のポート７３６の間に延在するリンク７２０を使用して、ＮＶＤ７１０に接続されている。ホストマシン７０６は、ホストマシン７０６のＮＩＣ７４４によって提供されるポート７４６の間およびＮＶＤ７１２のポート７４８の間に延在するリンク７２４を使用して、ＮＶＤ７１２に接続されている。ホストマシン７０８は、ホストマシン７０８のＮＩＣ７５０によって提供されるポート７５２の間およびＮＶＤ７１２のポート７５４の間に延在するリンク７２６を使用して、ＮＶＤ７１２に接続されている。
【０１２８】
次いで、ＮＶＤは、通信リンクを介してトップオブラック（ＴＯＲ）スイッチに接続されており、ＴＯＲスイッチは、物理ネットワーク７１８（スイッチファブリックとしても参照される）に接続されている。ある実施形態において、ホストマシンとＮＶＤとの間、および、ＮＶＤとＴＯＲスイッチとの間のリンクは、イーサネット（登録商標）リンクである。例えば、図７において、ＮＶＤ７１０および７１２は、それぞれリンク７２８および７３０を使用して、１１２６個のＴＯＲスイッチ７１４および７１６に接続されている。ある実施形態において、リンク７２０、７２４、７２６、７２８、および７３０は、イーサネット（登録商標）リンクである。ＴＯＲに接続されているホストマシンおよびＮＶＤの集合は、ラックとして参照されることがある。
【０１２９】
物理ネットワーク７１８は、ＴＯＲスイッチが互いに通信することを可能にする通信ファブリックを提供する。物理ネットワーク７１８は、多階層構成ネットワークとすることができる。ある実施態様において、物理ネットワーク７１８は、スイッチの多階層構成Ｃｌｏｓネットワークであり、ＴＯＲスイッチ７１４および７１６は、多階層構成マルチノード物理スイッチングネットワーク７１８のリーフレベルノードを表す。限定ではないが、２階層ネットワーク、３階層ネットワーク、４階層ネットワーク、５階層ネットワーク、および一般的に「ｎ」階層構成ネットワークを含む、異なるＣｌｏｓネットワーク構成が可能である。Ｃｌｏｓネットワークの一例が、図１０に示されており、下記に説明される。
【０１３０】
１対１構成、多対１構成、１対多構成などのような、ホストマシンとＮＶＤとの間の様々な異なる接続構成が可能である。１対１構成実施態様においては、各ホストマシンが、それ自体の別個のＮＶＤに接続される。例えば、図７において、ホストマシン７０２は、ホストマシン７０２のＮＩＣ７３２を介してＮＶＤ７１０に接続される。多対１構成においては、複数のホストマシンが１つのＮＶＤに接続される。例えば、図７において、ホストマシン７０６および７０８は、それぞれＮＩＣ７４４および７５０を介して、同じＮＶＤ７１２に接続される。
【０１３１】
１対多構成においては、１つのホストマシンが複数のＮＶＤに接続される。図８は、ホストマシンが複数のＮＶＤに接続されているＣＳＰＩ８００内の例を示す。図８に示すように、ホストマシン８０２は、複数のポート８０６および８０８を含むネットワークインターフェイスカード（ＮＩＣ）８０４を備える。ホストマシン８００は、ポート８０６お

よびリンク８２０を介して第１のＮＶＤ８１０に接続されており、ポート８０８およびリンク８２２を介して第２のＮＶＤ８１２に接続されている。ポート８０６および８０８は、イーサネット（登録商標）ポートであってもよく、ホストマシン８０２とＮＶＤ８１０および８１２との間のリンク８２０および８２２は、イーサネット（登録商標）リンクであり得る。次いで、ＮＶＤ８１０は、第１のＴＯＲスイッチ８１４に接続されており、ＮＶＤ８１２は、第２のＴＯＲスイッチ８１６に接続されている。ＮＶＤ８１０および８１２とＴＯＲスイッチ８１４および８１６との間のリンクは、イーサネット（登録商標）リンクであり得る。ＴＯＲスイッチ８１４および８１６は、多階層構成物理ネットワーク８１８内の階層０スイッチングデバイスを表す。

【０１３２】

図８に示す配置構成は、物理スイッチネットワーク８１８からホストマシン８０２への、および、ホストマシン８０２から物理スイッチネットワーク８１８への２つの別個の物理ネットワーク経路、すなわち、ＴＯＲスイッチ８１４－ＮＶＤ８１０－ホストマシン８０２とトラバースする第１の経路、および、ＴＯＲスイッチ８１６－ＮＶＤ８１２－ホストマシン８０２とトラバースする第２の経路を提供する。これら別個の経路は、ホストマシン８０２の向上した可用性（高可用性として参照される）を提供する。経路（例えば、経路の１つのリンクが故障した）またはデバイス（例えば、特定のＮＶＤが機能していない）の１つに問題がある場合、他の経路が、ホストマシン８０２への／からの通信に使用され得る。

【０１３３】

図８に示す構成において、ホストマシンは、ホストマシンのＮＩＣによって提供される２つの異なるポートを使用して２つの異なるＮＶＤに接続されている。他の実施形態において、ホストマシンは、ホストマシンの複数のＮＶＤへの接続を可能にする複数のＮＩＣを含み得る。

【０１３４】

図７に戻って参照すると、ＮＶＤは、１つまたは複数のネットワークおよび／またはストレージ仮想化機能を実施する物理デバイスまたは構成要素である。ＮＶＤは、１つまたは複数の処理装置（例えば、ＣＰＵ、ネットワークプロセッシングユニット（ＮＰＵ）、ＦＰＧＡ、パケット処理パイプラインなど）、キャッシュを含むメモリ、およびポートを有する任意のデバイスであり得る。様々な仮想化機能が、ＮＶＤの１つまたは複数の処理装置によって実行されるソフトウェア／ファームウェアによって実施され得る。

【０１３５】

ＮＶＤは、様々な異なる形態で実装され得る。例えば、ある実施形態において、ＮＶＤは、プロセッサが基板に内蔵されているｓｍａｒｔＮＩＣまたはインテリジェントＮＩＣとして参照されるインターフェイスカードとして実装される。ｓｍａｒｔＮＩＣは、ホストマシン上のＮＩＣとは別個のデバイスである。図７において、ＮＶＤ７１０および７１２は、それぞれホストマシン７０２、ならびにホストマシン７０６および７０８に接続されるｓｍａｒｔＮＩＣとして実装され得る。

【０１３６】

しかしながら、ｓｍａｒｔＮＩＣは、ＮＶＤ実施態様の一例に過ぎない。様々な他の実施態様が可能である。例えば、いくつかの他の実施態様において、ＮＶＤまたはＮＶＤによって実施される１つまたは複数の機能は、１つもしくは複数のホストマシン、１つもしくは複数のＴＯＲスイッチ、およびＣＳＰＩ７００の他の構成要素に組み込まれてもよく、またはそれによって実施され得る。例えば、ＮＶＤは、ホストマシン内に具現化されてもよく、ここで、ＮＶＤによって実施される機能は、ホストマシンによって実施される。別の例として、ＮＶＤは、ＴＯＲスイッチの一部であってもよく、または、ＴＯＲスイッチが、ＴＯＲスイッチが公衆クラウドに使用される様々な複雑なパケット変換を実施することを可能にするＮＶＤによって実施される機能を実施するように構成され得る。ＮＶＤの機能を実施するＴＯＲは、スマートＴＯＲとして参照されることがある。ベアメタル（ＢＭ）インスタンスではなく仮想マシン（ＶＭ）インスタンスが顧客に供給されるさらに

他の実施態様においては、ＮＶＤによって実施される機能は、ホストマシンのハイパーバイザの内側で実装され得る。いくつかの他の実施態様において、ＮＶＤの機能の一部は、ホストマシンのフリート上で作動する集中型サービスにオフロードされ得る。

【０１３７】

図７に示すようにｓｍａｒｔＮＩＣとして実装されるときなどの、ある実施形態において、ＮＶＤは、１つまたは複数のホストマシンおよび１つまたは複数のＴＯＲスイッチに接続されることを可能にする複数の物理ポートを備え得る。ＮＶＤ上のポートは、ホスト側ポート（「サウスポート」としても参照される）またはネットワーク側もしくはＴＯＲ側ポート（「ノースポート」としても参照される）として分類することができる。ＮＶＤのホスト側ポートは、ＮＶＤをホストマシンに接続するために使用されるポートである。図７におけるホスト側ポートの例は、ＮＶＤ７１０上のポート７３６、ならびに、ＮＶＤ７１２上のポート７４８および７５４を含む。ＮＶＤのネットワーク側ポートは、ＮＶＤをＴＯＲスイッチに接続するために使用されるポートである。図７におけるネットワーク側ポートの例は、ＮＶＤ７１０上のポート７５６、ならびに、ＮＶＤ７１２上のポート７５８を含む。図７に示すように、ＮＶＤ７１０は、ＮＶＤ７１０のポート７５６からＴＯＲスイッチ７１４へと延在するリンク７２８を使用してＴＯＲスイッチ７１４に接続されている。同様に、ＮＶＤ７１２は、ＮＶＤ７１２のポート７５８からＴＯＲスイッチ７１６へと延在するリンク７３０を使用してＴＯＲスイッチ７１６に接続されている。

【０１３８】

ＮＶＤは、ホスト側ポートを介してホストマシンからのパケットおよびフレーム（例えば、ホストマシンによってホストされる計算インスタンスによって生成されるパケットおよびフレーム）を受信し、必要なパケット処理を実施した後、パケットおよびフレームを、ＮＶＤのネットワーク側ポートを介してＴＯＲスイッチに転送することができる。ＮＶＤは、ＮＶＤのネットワーク側ポートを介してＴＯＲスイッチからのパケットおよびフレームを受信することができ、必要なパケット処理を実施した後、パケットおよびフレームを、ＮＶＤのホスト側ポートを介してホストマシンに転送することができる。

【０１３９】

ある実施形態において、複数のポートおよびＮＶＤとＴＯＲスイッチとの間の関連付けられるリンクが存在し得る。これらのポートおよびリンクは、集約されて、複数のポートまたはリンクのリンクアグリゲータグループ（ＬＡＧとして参照される）を形成することができる。リンク集約は、２つのエンドポイント間の（例えば、ＮＶＤとＴＯＲスイッチとの間の）複数の物理リンクが単一の論理リンクとして扱われることを可能にする。所与のＬＡＧ内のすべての物理リンクは、同じ速度で全二重モードにおいて動作し得る。ＬＡＧは、２つのエンドポイント間の接続の帯域幅および信頼性を増大させるのを助ける。ＬＡＧ内の物理リンクのうちの１つが故障した場合、トラフィックは、ＬＡＧ内の他の物理リンクのうちの１つに、動的かつトランスペアレントに再割り当てされる。集約された物理リンクは、各個々のリンクよりも高い帯域幅を送達する。ＬＡＧに関連付けられる複数のポートは、単一の論理ポートとして扱われる。トラフィックは、ＬＡＧの複数の物理リンクにわたって負荷平衡させることができる。１つまたは複数のＬＡＧは、２つのエンドポイントの間で構成することができる。２つのエンドポイントは、ＮＶＤとＴＯＲスイッチとの間、ホストマシンとＮＶＤとの間などであり得る。

【０１４０】

ＮＶＤは、ネットワーク仮想化機能を実装または実施する。これらの機能は、ＮＶＤによって実行されるソフトウェア／ファームウェアによって実施される。ネットワーク仮想化機能の例は、限定ではないが、パケットカプセル化およびカプセル化解除機能、ＶＣＮネットワークを作成するための機能、ＶＣＮセキュリティリスト（ファイアウォール）機能などのネットワークポリシを実装するための機能、ＶＣＮ内の計算インスタンスへの、および、そこからのパケットのルーティングおよび転送を促進する機能などを含む。ある実施形態において、パケットが受信されると、ＮＶＤは、パケットを処理し、パケットがどのように転送またはルーティングされるかを決定するためのパケット処理パイプライン

を実行するように構成されている。このパケット処理パイプラインの一部として、ＮＶＤは、ＶＣＮ内の計算インスタンスに関連付けられるＶＮＩＣを実行すること、ＶＣＮに関連付けられる仮想ルータ（ＶＲ）を実行すること、仮想ネットワーク内での転送またはルーティングを促進するためのパケットのカプセル化およびカプセル化解除、あるゲートウェイ（例えば、ローカルピアリングゲートウェイ）の実行、セキュリティリスト、ネットワークセキュリティグループ、ネットワークアドレス変換（ＮＡＴ）機能（例えば、ホストごとの公衆ＩＰのプライベートＩＰへの変換）の実装、スロットル機能、および他の機能などの、オーバーレイネットワークに関連付けられる１つまたは複数の仮想機能を実行することができる。

【０１４１】

ある実施形態において、ＮＶＤ内のパケット処理データ経路は、各々が一連のパケット変換ステージから構成されている複数のパケットパイプラインを含み得る。ある実施態様において、パケットが受信されると、パケットは、解析されて、単一のパイプラインに分類される。次いで、パケットは、ＮＶＤのインターフェイス上でパケットがドロップされるかまたは送出されるまで、１つのステージから別のステージへと線形的に処理される。これらのステージは、基本機能パケット処理構築ブロック（例えば、ヘッダの検証、スロットルの執行、新たなレイヤ２ヘッダの挿入、Ｌ４ファイアウォールの執行、ＶＣＮカプセル化／カプセル化解除など）を提供し、結果、既存のステージを構成することによって新たなパイプラインを構築することができ、新たなステージを作成し、それらを既存のパイプラインに挿入することによって、新たな機能を追加することができる。

【０１４２】

ＮＶＤは、ＶＣＮの制御プレーンおよびデータプレーンに対応する制御プレーン機能とデータプレーン機能の両方を実施することができる。ＶＣＮ制御プレーンの例は、図１１、図１２、図１３、および図１４にも示されており（参照符号１１１６、１２１６、１３１６、および１４１６参照）、下記に説明される。ＶＣＮデータプレーンの例は、図１１、図１２、図１３、および図１４にも示されており（参照符号１１１８、１２１８、１３１８、および１４１８参照）、下記に説明される。制御プレーン機能は、データがどのように転送されるべきであるかを制御するネットワークの構成（例えば、経路および経路テーブルのセットアップ、ＶＮＩＣの構成など）に使用される機能を含む。ある実施形態において、すべてのオーバーレイ－基板マッピングを中心的に計算し、それらをＮＶＤおよびＤＲＧ、ＳＧＷ、ＩＧＷなどのような様々なゲートウェイなどの仮想ネットワークエッジデバイスに発行するＶＣＮ制御プレーンが提供される。ファイアウォール規則もまた、同じメカニズムを使用して発行することができる。ある実施形態において、ＮＶＤは、そのＮＶＤに関連するマッピングのみを得る。データプレーン機能は、制御プレーンを使用してセットアップされる構成に基づくパケットの実際のルーティング／転送のための機能を含む。ＶＣＮデータプレーンは、顧客のネットワークパケットを、それらが基盤ネットワークをトラバースする前にカプセル化することによって実装される。カプセル化／カプセル化解除機能は、ＮＶＤ上で実装される。ある実施形態において、ＮＶＤは、ホストマシンを出入りするすべてのネットワークパケットをインターセプトし、ネットワーク仮想化機能を実施するように構成されている。

【０１４３】

上記で示したように、ＮＶＤは、ＶＮＩＣおよびＶＣＮ　ＶＲを含む様々な仮想化機能を実行する。ＮＶＤは、ＶＮＩＣに接続されている１つまたは複数のホストマシンによってホストされる計算インスタンスに関連付けられるＶＮＩＣを実行することができる。例えば、図７に示すように、ＮＶＤ７１０は、ＮＶＤ７１０に接続されているホストマシン７０２によってホストされる計算インスタンス７６８に関連付けられるＶＮＩＣ７７６の機能を実行する。別の例として、ＮＶＤ７１２は、ホストマシン７０６によってホストされるベアメタル計算インスタンス７７２に関連付けられるＶＮＩＣ７８０を実行し、ホストマシン７０８によってホストされる計算インスタンス７７４に関連付けられるＶＮＩＣ７８４を実行する。ホストマシンは、異なる顧客に属する異なるＶＣＮに属する計算イン

スタンスをホストすることができ、ホストマシンに接続されているＮＶＤは、計算インスタンスに対応するＶＮＩＣを実行する（すなわち、ＶＮＩＣ関連機能を実行する）ことができる。

【０１４４】

ＮＶＤはまた、計算インスタンスのＶＣＮに対応するＶＣＮ仮想ルータも実行する。例えば、図７に示す実施形態において、ＮＶＤ７１０は、計算インスタンス７６８が属するＶＣＮに対応するＶＣＮ　ＶＲ７７７を実行する。ＮＶＤ７１２は、ホストマシン７０６および７０８によってホストされる計算インスタンスが属する１つまたは複数のＶＣＮに対応する１つまたは複数のＶＣＮ　ＶＲ７８３を実行する。ある実施形態において、そのＶＣＮに対応するＶＣＮ　ＶＲは、そのＶＣＮに属する少なくとも１つの計算インスタンスをホストするホストマシンに接続されているすべてのＮＶＤによって実行される。ホストマシンが、異なるＶＣＮに属する計算インスタンスをホストする場合、そのホストマシンに接続されているＮＶＤは、それらの異なるＶＣＮに対応するＶＣＮ　ＶＲを実行することができる。

【０１４５】

ＶＮＩＣおよびＶＣＮ　ＶＲに加えて、ＮＶＤは、様々なソフトウェア（例えば、デーモン）を実行し、ＮＶＤによって実施される様々なネットワーク仮想化機能を促進する１つまたは複数のハードウェア構成要素を含み得る。単純化を目的として、これらの様々な構成要素は、図７に示す「パケット処理構成要素」としてともにグループ化される。例えば、ＮＶＤ７１０は、パケット処理構成要素７８６を備え、ＮＶＤ７１２は、パケット処理構成要素７８８を備える。例えば、ＮＶＤのパケット処理構成要素は、ＮＶＤのポートおよびハードウェアインターフェイスとインタラクトして、ＮＶＤによって受信され、ＮＶＤを使用して受信され通信されるすべてのパケットを監視し、ネットワーク情報を記憶するように構成されているパケットプロセッサを含み得る。ネットワーク情報は、例えば、ＮＶＤによってフロー情報ごとに（例えば、フロー統計ごとに）ハンドリングされる異なるネットワークフローを識別するネットワークフロー情報を含み得る。ある実施形態において、ネットワークフロー情報は、ＶＮＩＣごとに記憶され得る。パケットプロセッサは、パケットごとの操作を実施するとともに、ステートフルＮＡＴおよびＬ４ファイアウォール（ＦＷ）を実装し得る。別の例として、パケット処理構成要素は、ＮＶＤによって記憶されている情報を、１つまたは複数の異なる複製目標ストアに複製するように構成されている複製エージェントを含み得る。さらに別の例として、パケット処理構成要素は、ＮＶＤのログ記録機能を実施するように構成されているログ記録エージェントを含み得る。パケット処理構成要素はまた、ＮＶＤの性能および健全性を監視し、また、場合によっては、ＮＶＤに接続されている他の構成要素の状態および健全性も監視するためのソフトウェアも含み得る。

【０１４６】

図６は、ＶＣＮ、ＶＣＮ内のサブネット、サブネット上に展開されている計算インスタンス、計算インスタンスに関連付けられるＶＮＩＣ、ＶＣＮのためのＶＲ、および、ＶＣＮ向けに構成されているゲートウェイのセットを含む例示的な仮想またはオーバーレイネットワークの構成要素を示す。図６に示すオーバーレイ構成要素は、図７に示す物理構成要素のうちの１つまたは複数によって実行またはホストされ得る。例えば、ＶＣＮ内の計算インスタンスは、図７に示す１つまたは複数のホストマシンによって実行またはホストされ得る。ホストマシンによってホストされる計算インスタンスについて、その計算インスタンスに関連付けられるＶＮＩＣは、典型的には、そのホストマシンに接続されているＮＶＤによって実行される（すなわち、ＶＮＩＣ機能は、そのホストマシンに接続されているＮＶＤによって提供される）。ＶＣＮのＶＣＮ　ＶＲ機能は、そのＶＣＮの一部である計算インスタンスをホストまたは実行するホストマシンに接続されているすべてのＮＶＤによって実行される。ＶＣＮに関連付けられるゲートウェイは、１つまたは複数の異なるタイプのＮＶＤによって実行され得る。例えば、あるゲートウェイは、ｓｍａｒｔＮＩＣによって実行されてもよく、一方、他のゲートウェイは、１つまたは複数のホストマシ

ンまたはＮＶＤの他の実施態様によって実行され得る。
【０１４７】
上述したように、顧客ＶＣＮ内の計算インスタンスは、様々な異なるエンドポイントと通信することができ、ここで、エンドポイントは、ソース計算インスタンスと同じサブネット内にあることができ、ソース計算インスタンスと異なるサブネット内であるが、同じＶＣＮ内にあることができ、または、エンドポイントは、ソース計算インスタンスのＶＣＮの外側にあることができる。これらの通信は、計算インスタンスに関連付けられるＶＮＩＣ、ＶＣＮ ＶＲ、およびＶＣＮに関連付けられるゲートウェイを使用して促進される。
【０１４８】
ＶＣＮ内の同じサブネット上の２つの計算インスタンス間の通信について、通信は、ソースおよび宛先計算インスタンスに関連付けられるＶＮＩＣを使用して促進される。ソースおよび宛先計算インスタンスは、同じホストマシンによってホストされてもよく、または、異なるホストマシンによってホストされ得る。ソース計算インスタンスに由来するパケットは、ソース計算インスタンスをホストするホストマシンから、そのホストマシンに接続されているＮＶＤへと転送することができる。ＮＶＤ上で、パケットは、ソース計算インスタンスに関連付けられるＶＮＩＣの実行を含み得る、パケット処理パイプラインを使用して処理される。パケットの宛先エンドポイントは同じサブネット内にあるため、ソース計算インスタンスに関連付けられるＶＮＩＣが実行される結果として、パケットが、宛先計算インスタンスに関連付けられるＶＮＩＣを実行するＮＶＤに転送され、その後、ＮＶＤは、パケットを処理し、宛先計算インスタンスに転送する。ソースおよび宛先計算インスタンスに関連付けられるＶＮＩＣは、同じＮＶＤ上で実行されてもよく（例えば、ソース計算インスタンスと宛先計算インスタンスの両方が同じホストマシンによってホストされるとき）、または、異なるＮＶＤ上で実行され得る（例えば、ソースおよび宛先計算インスタンスが異なるＮＶＤに接続されている異なるホストマシンによってホストされるとき）。ＶＮＩＣは、ＮＶＤによって記憶されているルーティング／転送テーブルを使用して、パケットの次のホップを決定することができる。
【０１４９】
パケットがサブネット内の計算インスタンスから同じＶＣＮ内の異なるサブネット内のエンドポイントに通信されるようにするために、ソース計算インスタンスに由来するパケットは、ソース計算インスタンスをホストするホストマシンからそのホストマシンに接続されているＮＶＤに通信される。ＮＶＤ上で、パケットは、１つまたは複数のＶＮＩＣの実行を含み得るパケット処理パイプラインおよびＶＣＮに関連付けられるＶＲを使用して処理される。例えば、パケット処理パイプラインの一部として、ＮＶＤは、ソース計算インスタンスに関連付けられるＶＮＩＣに対応する機能を実行するかまたは呼び出す（ＶＮＩＣの実行としても参照される）。ＶＮＩＣによって実施される機能は、パケット上のＶＬＡＮタグを見ることを含み得る。パケット宛先はサブネットの外側にあるため、ＶＣＮ ＶＲ機能は、ＮＶＤによって次に呼び出され、実行される。次いで、ＶＣＮ ＶＲは、宛先計算インスタンスに関連付けられるＶＮＩＣを実行するＮＶＤにパケットをルーティングする。次いで、宛先計算インスタンスに関連付けられるＶＮＩＣは、パケットを処理し、宛先計算インスタンスに転送する。ソースおよび宛先計算インスタンスに関連付けられるＶＮＩＣは、同じＮＶＤ上で実行されてもよく（例えば、ソース計算インスタンスと宛先計算インスタンスの両方が同じホストマシンによってホストされるとき）、または、異なるＮＶＤ上で実行され得る（例えば、ソースおよび宛先計算インスタンスが異なるＮＶＤに接続されている異なるホストマシンによってホストされるとき）。
【０１５０】
パケットの宛先がソース計算インスタンスのＶＣＮの外側にある場合、ソース計算インスタンスに由来するパケットは、ソース計算インスタンスをホストするホストマシンからそのホストマシンに接続されているＮＶＤに通信される。ＮＶＤは、ソース計算インスタンスに関連付けられるＶＮＩＣを実行する。パケットの宛先エンドポイントはＶＣＮの外側にあるため、パケットは、その後、そのＶＣＮのＶＣＮ ＶＲによって処理される。Ｎ

ＶＤは、ＶＣＮ　ＶＲ機能を呼び出し、その結果として、パケットは、ＶＣＮに関連付けられる適切なゲートウェイを実行するＮＶＤに転送される。例えば、宛先が顧客のオンプレミスネットワーク内のエンドポイントである場合、パケットは、ＶＣＮ　ＶＲによって、ＶＣＮ向けに構成されているＤＲＧゲートウェイを実行するＮＶＤに転送することができる。ＶＣＮ　ＶＲは、ソース計算インスタンスに関連付けられるＶＮＩＣを実行しているＮＶＤと同じＮＶＤ上で、または、異なるＮＶＤによって実行され得る。ゲートウェイは、ＮＶＤによって実行されてもよく、ＮＶＤは、ｓｍａｒｔＮＩＣ、ホストマシン、または他のＮＶＤ実施態様であり得る。次いで、パケットは、ゲートウェイによって処理され、パケットの、最終的な意図される宛先への通信を促進する次のホップへと転送されることができる。例えば、図７に示す実施形態において、計算インスタンス７６８に由来するパケットは、ホストマシン７０２からリンク７２０を介して（ＮＩＣ７３２を使用して）ＮＶＤ７１０へと通信することができる。ＮＶＤ７１０上で、ＶＮＩＣ７７６が、これがソース計算インスタンス７６８に関連付けられるＶＮＩＣであるため、呼び出される。ＶＮＩＣ７７６は、パケット内のカプセル化情報を調べ、パケットのその意図される宛先エンドポイントへの通信を促進することを目標としてパケットを転送する次のホップを決定し、次いで、決定された次のホップにパケットを転送するように構成されている。

【０１５１】

ＶＣＮ上に展開される特定の計算インスタンスは、様々な異なるエンドポイントと通信することができる。これらのエンドポイントは、ＣＳＰＩ７００によってホストされるエンドポイントおよびＣＳＰＩ７００の外側のエンドポイントを含み得る。ＣＳＰＩ７００によってホストされるエンドポイントは、同じＶＣＮまたは他のＶＣＮ内のインスタンスを含んでもよく、ＶＣＮは、顧客のＶＣＮであってもよく、または、顧客に属しないＶＣＮであり得る。ＣＳＰＩ７００によってホストされるエンドポイント間の通信は、物理ネットワーク７１８を介して実施され得る。計算インスタンスはまた、ＣＳＰＩ７００によってホストされないか、または、ＣＳＰＩ７００の外側にあるエンドポイントとも通信し得る。これらのエンドポイントの例は、顧客オンプレミスネットワークもしくはデータセンタ内のエンドポイント、または、インターネットなどの公衆ネットワークを介してアクセス可能な公衆エンドポイントを含む。ＣＳＰＩ７００の外側のエンドポイントとの通信は、様々な通信プロトコルを使用して、公衆ネットワーク（例えば、インターネット）（図７には示さず）またはプライベートネットワーク（図７には示さず）を介して実施され得る。

【０１５２】

図７に示すＣＳＰＩ７００のアーキテクチャは、例示に過ぎず、限定であるようには意図されていない。代替的な実施形態において、変形、代替、および修正が可能である。例えば、いくつかの他の実施形態において、ＣＳＰＩ７００は、図７に示されているよりも多いもしくは少ないシステムもしくは構成要素を有してもよく、２つ以上のシステムを組み合わせてもよく、または、システムの異なる構成もしくは配置を有し得る。図７に示すシステム、サブシステム、および他の構成要素は、それぞれのシステム、ハードウェアの使用、またはそれらの組合せの１つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）内で実施することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。

【０１５３】

図９は、ある実施形態によるマルチテナンシ機能をサポートするためにＩ／Ｏ仮想化を提供するためのホストマシンとＮＶＤとの間の接続を示す。図９に示すように、ホストマシン９０２は、仮想化環境を提供するハイパーバイザ９０４を実行する。ホストマシン９０２は、２つの仮想マシンインスタンス、すなわち、顧客／テナント＃１に属するＶＭ１９０６および顧客／テナント＃２に属するＶＭ２　９０８を実行する。ホストマシン９０２は、リンク９１４を介してＮＶＤ９１２に接続されている物理ＮＩＣ９１０を備える。計算インスタンスの各々は、ＮＶＤ９１２によって実行されるＶＮＩＣに接続される。図

９の実施形態において、ＶＭ１　９０６は、ＶＮＩＣ－ＶＭ１　９２０に接続され、ＶＭ２　９０８は、ＶＮＩＣ－ＶＭ２　９２２に接続される。

【０１５４】

図９に示すように、ＮＩＣ９１０は、２つの論理ＮＩＣ、すなわち、論理ＮＩＣ　Ａ９１６および論理ＮＩＣ　Ｂ９１８を含む。各仮想マシンは、それ自体の論理ＮＩＣに接続され、それと協働するように構成されている。例えば、ＶＭ１　９０６は、論理ＮＩＣ　Ａ９１６に接続され、ＶＭ２　９０８は、論理ＮＩＣ　Ｂ９１８に接続される。ホストマシン９０２は複数のテナントによって共有される１つのみの物理ＮＩＣ９１０を備えるが、論理ＮＩＣに起因して、各テナントの仮想マシンは、それらがそれら自体のホストマシンおよびＮＩＣを有すると考える。

【０１５５】

ある実施形態において、各論理ＮＩＣは、それ自体のＶＬＡＮ　ＩＤを割り当てられる。したがって、特定のＶＬＡＮ　ＩＤがテナント＃１の論理ＮＩＣ　Ａ９１６に割り当てられ、別個のＶＬＡＮ　ＩＤが、テナント＃２の論理ＮＩＣ　Ｂ９１８に割り当てられる。ＶＭ１　９０６からパケットが通信されるとき、テナント＃１に割り当てられているタグが、ハイパーバイザによってパケットに割り当てられ、次いで、パケットは、ホストマシン９０２からリンク９１４を介してＮＶＤ９１２に通信される。同様に、ＶＭ２　９０８からパケットが通信されるとき、テナント＃２に割り当てられているタグが、ハイパーバイザによってパケットに割り当てられ、次いで、パケットは、ホストマシン９０２からリンク９１４を介してＮＶＤ９１２に通信される。したがって、ホストマシン９０２からＮＶＤ９１２に通信されるパケット９２４は、特定のテナントおよび関連付けられるＶＭを識別する、関連付けられるタグ９２６を有する。ＮＶＤ上で、ホストマシン９０２から受信されるパケット９２４について、パケットに関連付けられるタグ９２６は、パケットがＶＮＩＣ－ＶＭ１　９２０によって処理されるべきであるか、または、ＶＮＩＣ－ＶＭ２　９２２によって処理されるべきであるかを判定するために使用される。次いで、パケットは、対応するＶＮＩＣによって処理される。図９に示す構成は、各テナントの計算インスタンスが、それらがそれら自体のホストマシンおよびＮＩＣを所有すると考えることを可能にする。図９に示すセットアップは、マルチテナンシをサポートするためのＩ／Ｏ仮想化を提供する。

【０１５６】

図１０は、ある実施形態による物理ネットワーク１０００の単純化されたブロック図を示す。図１０に示す実施形態は、Ｃｌｏｓネットワークとして構造化される。Ｃｌｏｓネットワークは、高い二分帯域幅および最大のリソース利用を維持しながら接続冗長性を提供するように設計されている特定のタイプのネットワークトポロジである。Ｃｌｏｓネットワークは、ノンブロッキング、マルチステージまたは多階層構成スイッチングネットワークのタイプであり、ステージまたは階層の数は、２、３、４、５などとすることができる。図１０に示す実施形態は、階層１、２、および３を備える３階層構成ネットワークである。ＴＯＲスイッチ１００４は、Ｃｌｏｓネットワーク内の階層０スイッチを表す。１つまたは複数のＮＶＤが、ＴＯＲスイッチに接続されている。階層０スイッチは、物理ネットワークのエッジデバイスとしても参照される。階層０スイッチは、リーフスイッチとしても参照される階層１スイッチに接続されている。図１０に示す実施形態においては、「ｎ」個の階層０ＴＯＲスイッチから成るセットが「ｎ」個の階層１スイッチから成るセットに接続され、ともにポッドを形成する。ポッド内の各階層０スイッチは、ポッド内のすべての階層１スイッチに相互接続されるが、ポッド間のスイッチの接続はない。ある実施態様において、２つのポッドがブロックとして参照される。各ブロックは、「ｎ」個の階層２スイッチ（スパインスイッチとして参照されることがある）から成るセットによってサービスされるか、または、それに接続される。物理ネットワークトポロジ内には、いくつかのブロックが存在し得る。次いで、階層２スイッチは、「ｎ」個の階層３スイッチ（スーパースパインスイッチとして参照されることがある）に接続されている。物理ネットワーク１０００を介したパケットの通信は、典型的には、１つまたは複数のレイヤ３通

信プロトコルを使用して実施される。典型的には、ＴＯＲレイヤを除く物理ネットワークのすべてのレイヤは、ｎウェイ冗長であり、したがって、高可用性を可能にする。物理ネットワークのスケーリングを可能にするように物理ネットワーク内のスイッチの互いに対する可視性を制御するために、ポッドおよびブロックに対してポリシを指定することができる。

【０１５７】

Ｃｌｏｓネットワークの特徴は、１つの階層０スイッチから別の階層０スイッチに（または階層０スイッチに接続されているＮＶＤから階層０スイッチに接続されている別のＮＶＤに）達するための最大ホップカウントが固定であることである。例えば、３階層構成Ｃｌｏｓネットワークにおいては、パケットが１つのＮＶＤから別のＮＶＤに達するために最大７ホップが必要とされ、ここで、ソースおよび目標ＮＶＤはＣｌｏｓネットワークのリーフ階層に接続されている。同様に、４階層構成Ｃｌｏｓネットワークにおいては、パケットが１つのＮＶＤから別のＮＶＤに達するために最大９ホップが必要とされ、ここで、ソースおよび目標ＮＶＤはＣｌｏｓネットワークのリーフ階層に接続されている。したがって、Ｃｌｏｓネットワークアーキテクチャは、ネットワーク全体を通じて一貫したレイテンシを維持し、これは、データセンタ内および間の通信に重要である。Ｃｌｏｓトポロジは水平方向にスケーリングし、コスト効率的である。ネットワークの帯域幅／スループット容量は、様々な階層により多くのスイッチ（例えば、より多くのリーフおよびスパインスイッチ）を追加することによって、および、隣接する階層のスイッチ間のリンクの数を増大させることによって、容易に増大することができる。

【０１５８】

ある実施形態において、ＣＳＰＩ内の各リソースは、クラウド識別子（ＣＩＤ）と呼ばれる一意の識別子を割り当てられる。この識別子は、リソースの情報の一部として含まれ、例えば、コンソールを介してまたはＡＰＩを通じてリソースを管理するために使用することができる。ＣＩＤの例示的な構文は、以下のとおりである。

【０１５９】

ocid1.〈RESOURCE TYPE〉.〈REALM〉.[REGION][.FUTURE USE].〈UNIQUE ID〉

ここで、

ocid1：ＣＩＤのバージョンを指示する文字列。

resource type：リソースのタイプ（例えば、インスタンス、ボリューム、ＶＣＮ、サブネット、ユーザ、グループなど）。

realm：リソースがその中にあるレルム。例示的な値は、商業レルムの「c1」、政府クラウドレルムの「c2」、または、連邦政府クラウドレルムの「c3」などである。各レルムが、それ自体のドメイン名を有することができる。

region：リソースがその中にあるリージョン。リージョンがリソースに適用可能でない場合、この部分はブランクになり得る。

future use：将来の使用のために予約済み。

unique ID：ＩＤの一意の部分。フォーマットは、リソースまたはサービスのタイプに応じて変化し得る。

【０１６０】

図１１は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの例示的なパターンを示すブロック図１１００である。サービスオペレータ１１０２は、仮想クラウドネットワーク（ＶＣＮ）１１０６およびセキュアホストサブネット１１０８を含み得るセキュアホストテナンシ１１０４に通信可能に結合することができる。いくつかの例において、サービスオペレータ１１０２は、Microsoft Windows Mobile（登録商標）などのソフトウェア、および／または、ｉＯＳ、Windows Phone、Android、BlackBerry 8、Ｐａｌｍ ＯＳなどのような様々なモバイルオペレーティングシステムを作動させており、インターネット、電子メール、ショートメッセージサービス（ＳＭＳ）、Blackberry（登録商標）、または他の通信プロトコルを有効化されているポータブル手持

ち式デバイス（例えば、iPhone（登録商標）、携帯電話機、iPad（登録商標）、コンピューティングタブレット、個人情報端末（ＰＤＡ））またはウェアラブルデバイス（例えば、Google（登録商標）Glassヘッドマウントディスプレイ）であり得る、１つまたは複数のクライアントコンピューティングデバイスを使用し得る。代替的に、クライアントコンピューティングデバイスは、例として、様々なバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、および／またはLinux（登録商標）オペレーティングシステムを作動させているパーソナルコンピュータおよび／またはラップトップを含む汎用パーソナルコンピュータとすることができる。クライアントコンピューティングデバイスは、限定ではないが、例えば、Google Chrome OSなどの様々なGNU/Linuxオペレーティングシステムを含む、様々な市販のUNIX（登録商標）またはUNIXのようなオペレーティングシステムのいずれかを作動させるワークステーションコンピュータとすることができる。代替的に、または、加えて、クライアントコンピューティングデバイスは、ＶＣＮ１１０６および／またはインターネットにアクセスすることができる、ネットワークを介して通信することが可能な、シンクライアントコンピュータ、インターネット接続可能ゲーミングシステム（例えば、Kinect（登録商標）ジェスチャ入力デバイスを有するかまたは有しないMicrosoft（登録商標）Xboxゲーミングコンソール）、および／またはパーソナルメッセージングデバイスなどの、任意の他の電子デバイスであり得る。

【０１６１】

ＶＣＮ１１０６は、ローカルピアリングゲートウェイ（ＬＰＧ）１１１０を含むことができ、これは、セキュアシェル（ＳＳＨ）ＶＣＮ１１１２に含まれるＬＰＧ１１１０を介してＳＳＨ ＶＣＮ１１１２に通信可能に結合することができる。ＳＳＨ ＶＣＮ１１１２は、ＳＳＨサブネット１１１４を含むことができ、ＳＳＨ ＶＣＮ１１１２は、制御プレーンＶＣＮ１１１６に含まれるＬＰＧ１１１０を介して制御プレーンＶＣＮ１１１６に通信可能に結合することができる。また、ＳＳＨ ＶＣＮ１１１２は、ＬＰＧ１１１０を介してデータプレーンＶＣＮ１１１８に通信可能に結合することもできる。制御プレーンＶＣＮ１１１６およびデータプレーンＶＣＮ１１１８は、ＩａａＳプロバイダが所有および／または運用することができるサービステナンシ１１１９に含まれ得る。

【０１６２】

制御プレーンＶＣＮ１１１６は、周縁ネットワーク（例えば、企業イントラネットと外部ネットワークとの間の企業ネットワークの部分）として作用する制御プレーン非武装地帯（ＤＭＺ）階層１１２０を含み得る。ＤＭＺベースのサーバは、役割を制限され得、違反を含まれたままにするのを助け得る。付加的に、ＤＭＺ階層１１２０は、１つまたは複数のロードバランサ（ＬＢ）サブネット１１２２、アプリサブネット１１２６を含み得る制御プレーンアプリ階層１１２４、データベース（ＤＢ）サブネット１１３０（例えば、フロントエンドＤＢサブネットおよび／またはバックエンドＤＢサブネット）を含み得る制御プレーンデータ階層１１２８を含み得る。制御プレーンＤＭＺ階層１１２０に含まれるＬＢサブネット１１２２は、制御プレーンアプリ階層１１２４に含まれるアプリサブネット１１２６および制御プレーンＶＣＮ１１１６に含まれ得るインターネットゲートウェイ１１３４に通信可能に結合することができ、アプリサブネット１１２６は、制御プレーンデータ階層１１２８に含まれるＤＢサブネット１１３０ならびにサービスゲートウェイ１１３６およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ１１３８に通信可能に結合することができる。制御プレーンＶＣＮ１１１６は、サービスゲートウェイ１１３６およびＮＡＴゲートウェイ１１３８を含み得る。

【０１６３】

制御プレーンＶＣＮ１１１６は、アプリサブネット１１２６を含み得るデータプレーンミラーアプリ階層１１４０を含み得る。データプレーンミラーアプリ階層１１４０に含まれるアプリサブネット１１２６は、計算インスタンス１１４４を実行することができる仮想ネットワークインターフェイスコントローラ（ＶＮＩＣ）１１４２を含み得る。計算インスタンス１１４４は、データプレーンミラーアプリ階層１１４０のアプリサブネット１

１２６を、データプレーンアプリ階層１１４６に含まれ得るアプリサブネット１１２６に通信可能に結合することができる。

【０１６４】

データプレーンＶＣＮ１１１８は、データプレーンアプリ階層１１４６と、データプレーンＤＭＺ階層１１４８と、データプレーンデータ階層１１５０とを含み得る。データプレーンＤＭＺ階層１１４８は、データプレーンアプリ階層１１４６のアプリサブネット１１２６およびデータプレーンＶＣＮ１１１８のインターネットゲートウェイ１１３４に通信可能に結合することができるＬＢサブネット１１２２を含み得る。アプリサブネット１１２６は、データプレーンＶＣＮ１１１８のサービスゲートウェイ１１３６およびデータプレーンＶＣＮ１１１８のＮＡＴゲートウェイ１１３８に通信可能に結合することができる。データプレーンデータ階層１１５０もまた、データプレーンアプリ階層１１４６のアプリサブネット１１２６に通信可能に結合することができるＤＢサブネット１１３０を含み得る。

【０１６５】

制御プレーンＶＣＮ１１１６およびデータプレーンＶＣＮ１１１８のインターネットゲートウェイ１１３４は、公衆インターネット１１５４に通信可能に結合することができるメタデータ管理サービス１１５２に通信可能に結合することができる。公衆インターネット１１５４は、制御プレーンＶＣＮ１１１６およびデータプレーンＶＣＮ１１１８のＮＡＴゲートウェイ１１３８に通信可能に結合することができる。制御プレーンＶＣＮ１１１６およびデータプレーンＶＣＮ１１１８のサービスゲートウェイ１１３６は、クラウドサービス１１５６に通信可能に結合することができる。

【０１６６】

いくつかの例において、制御プレーンＶＣＮ１１１６またはデータプレーンＶＣＮ１１１８のサービスゲートウェイ１１３６は、公衆インターネット１１５４を経由することなく、クラウドサービス１１５６に対するアプリケーションプログラミングインターフェイス（ＡＰＩ）呼を行うことができる。サービスゲートウェイ１１３６からクラウドサービス１１５６へのＡＰＩ呼は、一方向であり、すなわち、サービスゲートウェイ１１３６は、クラウドサービス１１５６に対するＡＰＩ呼を行うことができ、クラウドサービス１１５６は、要求されたデータをサービスゲートウェイ１１３６に送ることができる。しかし、クラウドサービス１１５６は、サービスゲートウェイ１１３６に対するＡＰＩ呼を開始することができない。

【０１６７】

いくつかの例において、セキュアホストテナンシ１１０４は、サービステナンシ１１１９に直接的に接続することができ、これは、他の様態では分離され得る。セキュアホストサブネット１１０８は、他の様態では分離されているシステムを介して双方向通信を可能にすることができるＬＰＧ１１１０を通じてＳＳＨサブネット１１１４と通信することができる。セキュアホストサブネット１１０８をＳＳＨサブネット１１１４に接続することによって、セキュアホストサブネット１１０８は、サービステナンシ１１１９内の他のエンティティにアクセスすることができるようになる。

【０１６８】

制御プレーンＶＣＮ１１１６は、サービステナンシ１１１９のユーザが、所望のリソースをセットアップまたは他の様態でプロビジョンすることを可能にすることができる。制御プレーンＶＣＮ１１１６においてプロビジョンされる所望のリソースは、データプレーンＶＣＮ１１１８内に展開されるか、または、他の様態で使用され得る。いくつかの例において、制御プレーンＶＣＮ１１１６は、データプレーンＶＣＮ１１１８から分離することができ、制御プレーンＶＣＮ１１１６のデータプレーンミラーアプリ階層１１４０は、データプレーンミラーアプリ階層１１４０およびデータプレーンアプリ階層１１４６内に包含され得るＶＮＩＣ１１４２を介して、データプレーンＶＣＮ１１１８のデータプレーンアプリ階層１１４６と通信することができる。

【０１６９】

いくつかの例において、システムのユーザまたは顧客は、公衆インターネット１１５４を通じて、要求、例えば、作成、読み出し、更新、または削除（ＣＲＵＤ）動作を行うことができ、公衆インターネットは、メタデータ管理サービス１１５２に要求を通信することができる。メタデータ管理サービス１１５２は、インターネットゲートウェイ１１３４を通じて制御プレーンＶＣＮ１１１６に要求を通信することができる。要求は、制御プレーンＤＭＺ階層１１２０内に包含されるＬＢサブネット１１２２によって受信することができる。ＬＢサブネット１１２２は、要求が有効であることを判定することができ、この判定に応答して、ＬＢサブネット１１２２は、制御プレーンアプリ階層１１２４内に包含されるアプリサブネット１１２６に要求を送信することができる。要求が、検証され、公衆インターネット１１５４に対する呼を必要とする場合、公衆インターネット１１５４に対する呼を行うことができるＮＡＴゲートウェイ１１３８に、公衆インターネット１１５４に対する呼を送信することができる。要求によって記憶されることを所望され得るメモリを、ＤＢサブネット１１３０内に記憶することができる。

【０１７０】

いくつかの例において、データプレーンミラーアプリ階層１１４０は、制御プレーンＶＣＮ１１１６とデータプレーンＶＣＮ１１１８との間の直接通信を促進することができる。例えば、構成に対する変更、更新、または他の適切な修正が、データプレーンＶＣＮ１１１８内に包含されるリソースに加えられることが所望され得る。ＶＮＩＣ１１４２を介して、制御プレーンＶＣＮ１１１６は、データプレーンＶＣＮ１１１８と直接通信することができ、以て、データプレーンＶＣＮ１１１８内に包含されるリソースに対して、構成の変更、更新、または他の適切な修正を実行することができる。

【０１７１】

いくつかの実施形態において、制御プレーンＶＣＮ１１１６およびデータプレーンＶＣＮ１１１８は、サービステナンシ１１１９に含めることができる。この場合、システムのユーザまたは顧客は、制御プレーンＶＣＮ１１１６またはデータプレーンＶＣＮ１１１８のいずれかを所有しなくてもよく、または、運営しなくてもよい。代わりに、ＩａａＳプロバイダが、制御プレーンＶＣＮ１１１６およびデータプレーンＶＣＮ１１１８を所有または運営することができ、これらは両方とも、サービステナンシ１１１９に含めることができる。この実施形態は、ユーザまたは顧客が他のユーザ、または他の顧客のリソースと干渉するのを防止することができるネットワークの分離を可能にすることができる。また、この実施形態は、システムのユーザまたは顧客が、記憶に関して所望のレベルの脅威防止を有しない場合がある公衆インターネット１１５４に依拠する必要なしに、データベースをプライベートに記憶することを可能にすることができる。

【０１７２】

他の実施形態において、制御プレーンＶＣＮ１１１６内に包含されるＬＢサブネット１１２２は、サービスゲートウェイ１１３６からの信号を受信するように構成することができる。この実施形態において、制御プレーンＶＣＮ１１１６およびデータプレーンＶＣＮ１１１８は、公衆インターネット１１５４にコールする必要なく、ＩａａＳプロバイダの顧客によってコールされるように構成することができる。ＩａａＳプロバイダの顧客は、顧客が使用するデータベースがＩａａＳプロバイダによって制御され得、公衆インターネット１１５４から分離することができるサービステナンシ１１１９に記憶することができるため、この実施形態を所望し得る。

【０１７３】

図１２は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別の例示的なパターンを示すブロック図１２００である。サービスオペレータ１２０２（例えば、図１１のサービスオペレータ１１０２）は、仮想クラウドネットワーク（ＶＣＮ）１２０６（例えば、図１１のＶＣＮ１１０６）およびセキュアホストサブネット１２０８（例えば、図１１のセキュアホストサブネット１１０８）を含み得るセキュアホストテナンシ１２０４（例えば、図１１のセキュアホストテナンシ１１０４）に通信可能に結合することができる。ＶＣＮ１２０６は、ローカルピアリングゲートウェイ（ＬＰＧ）１２１０（例えば

、図１１のＬＰＧ１１１０）を含むことができ、これは、セキュアシェル（ＳＳＨ）ＶＣＮ１２１２に含まれるＬＰＧ１１１０を介してセキュアシェル（ＳＳＨ）ＶＣＮ１２１２（例えば、図１１のＳＳＨ　ＶＣＮ１１１２）に通信可能に結合することができる。ＳＳＨ　ＶＣＮ１２１２は、ＳＳＨサブネット１２１４（例えば、図１１のＳＳＨサブネット１１１４）を含むことができ、ＳＳＨ　ＶＣＮ１２１２は、制御プレーンＶＣＮ１２１６に含まれるＬＰＧ１２１０を介して制御プレーンＶＣＮ１２１６（例えば、図１１の制御プレーンＶＣＮ１１１６）に通信可能に結合することができる。制御プレーンＶＣＮ１２１６は、サービステナンシ１２１９（例えば、図１１のサービステナンシ１１１９）に含めることができ、データプレーンＶＣＮ１２１８（例えば、図１１のデータプレーンＶＣＮ１１１８）は、システムのユーザまたは顧客によって所有または運営され得る顧客テナンシ１２２１に含めることができる。

【０１７４】

制御プレーンＶＣＮ１２１６は、ＬＢサブネット１２２２（例えば、図１１のＬＢサブネット１１２２）を含み得る制御プレーンＤＭＺ階層１２２０（例えば、図１１の制御プレーンＤＭＺ階層１１２０）と、アプリサブネット１２２６（例えば、図１１のアプリサブネット１１２６）を含み得る制御プレーンアプリ階層１２２４（例えば、図１１の制御プレーンアプリ階層１１２４）と、データベース（ＤＢ）サブネット１２３０（例えば、図１１のＤＢサブネット１１３０と同様の）を含み得る制御プレーンデータ階層１２２８（例えば、図１１の制御プレーンデータ階層１１２８）とを含み得る。制御プレーンＤＭＺ階層１２２０に含まれるＬＢサブネット１２２２は、制御プレーンアプリ階層１２２４に含まれるアプリサブネット１２２６および制御プレーンＶＣＮ１２１６に含まれ得るインターネットゲートウェイ１２３４（例えば、図１１のインターネットゲートウェイ１１３４）に通信可能に結合することができ、アプリサブネット１２２６は、制御プレーンデータ階層１２２８に含まれるＤＢサブネット１２３０ならびにサービスゲートウェイ１２３６（例えば、図１１のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ１２３８（例えば、図１１のＮＡＴゲートウェイ１１３８）に通信可能に結合することができる。制御プレーンＶＣＮ１２１６は、サービスゲートウェイ１２３６およびＮＡＴゲートウェイ１２３８を含み得る。

【０１７５】

制御プレーンＶＣＮ１２１６は、アプリサブネット１２２６を含み得るデータプレーンミラーアプリ階層１２４０（例えば、図１１のデータプレーンミラーアプリ階層１１４０）を含み得る。データプレーンミラーアプリ階層１２４０に含まれるアプリサブネット１２２６は、コンピュータインスタンス１２４４（例えば、図１１のコンピュータインスタンス１１４４と同様の）を実行することができる仮想ネットワークインターフェイスコントローラ（ＶＮＩＣ）１２４２（例えば、１１４２のＶＮＩＣ）を含み得る。コンピュータインスタンス１２４４は、データプレーンミラーアプリ階層１２４０内に包含されているＶＮＩＣ１２４２およびデータプレーンアプリ階層１２４６内に包含されているＶＮＩＣ１２４２を介して、データプレーンミラーアプリ階層１２４０のアプリサブネット１２２６と、データプレーンアプリ階層１２４６（例えば、図１１のデータプレーンアプリ階層１１４６）内に包含され得るアプリサブネット１２２６との間の通信を促進することができる。

【０１７６】

制御プレーンＶＣＮ１２１６内に包含されているインターネットゲートウェイ１２３４は、公衆インターネット１２５４（例えば、図１１の公衆インターネット１１５４）に通信可能に結合することができるメタデータ管理サービス１２５２（例えば、図１１のメタデータ管理サービス１１５２）に通信可能に結合することができる。公衆インターネット１２５４は、制御プレーンＶＣＮ１２１６内に包含されているＮＡＴゲートウェイ１２３８に通信可能に結合することができる。制御プレーンＶＣＮ１２１６内に包含されているサービスゲートウェイ１２３６は、クラウドサービス１２５６（例えば、図１１のクラウドサービス１１５６）に通信可能に結合することができる。

【０１７７】
いくつかの例において、データプレーンＶＣＮ１２１８は、顧客テナンシ１２２１に含めることができる。この場合、ＩａａＳプロバイダが、各顧客について制御プレーンＶＣＮ１２１６を提供することができ、ＩａａＳプロバイダは、各顧客について、サービステナンシ１２１９内に包含される固有の計算インスタンス１２４４をセットアップすることができる。各計算インスタンス１２４４は、サービステナンシ１２１９内に包含されている制御プレーンＶＣＮ１２１６と、顧客テナンシ１２２１内に包含されているデータプレーンＶＣＮ１２１８との間の通信を可能にすることができる。計算インスタンス１２４４は、サービステナンシ１２１９内に包含されている制御プレーンＶＣＮ１２１６内にプロビジョンされるリソースが、顧客テナンシ１２２１内に包含されているデータプレーンＶＣＮ１２１８内で展開されるか、または、他の様態で使用されることを可能にすることができる。

【０１７８】
他の例において、ＩａａＳプロバイダの顧客は、顧客テナンシ１２２１内に常駐するデータベースを有することができる。この例において、制御プレーンＶＣＮ１２１６は、アプリサブネット１２２６を含み得るデータプレーンミラーアプリ階層１２４０を含み得る。データプレーンミラーアプリ階層１２４０は、データプレーンＶＣＮ１２１８内に存在することができるが、データプレーンミラーアプリ階層１２４０は、データプレーンＶＣＮ１２１８内に常駐しなくてもよい。すなわち、データプレーンミラーアプリ階層１２４０は、顧客テナンシ１２２１にアクセスすることができるが、データプレーンミラーアプリ階層１２４０は、データプレーンＶＣＮ１２１８内に存在しなくてもよく、または、ＩａａＳプロバイダの顧客によって所有もしくは運営されなくてもよい。データプレーンミラーアプリ階層１２４０は、データプレーンＶＣＮ１２１８に対して呼を行うように構成することができるが、制御プレーンＶＣＮ１２１６内に包含されている任意のエンティティにも呼を行うように構成されなくてもよい。顧客は、制御プレーンＶＣＮ１２１６内にプロビジョンされているデータプレーンＶＣＮ１２１８内のリソースを展開するかまたは他の様態で使用することを所望する場合があり、データプレーンミラーアプリ階層１２４０は、顧客が所望するリソースの展開または他の使用を促進することができる。

【０１７９】
いくつかの例において、ＩａａＳプロバイダの顧客は、データプレーンＶＣＮ１２１８にフィルタを適用することができる。この実施形態において、顧客は、データプレーンＶＣＮ１２１８がアクセスすることができるものを決定することができ、顧客は、データプレーンＶＣＮ１２１８からの公衆インターネット１２５４へのアクセスを制約することができる。ＩａａＳプロバイダは、データプレーンＶＣＮ１２１８の任意の外部ネットワークまたはデータベースに対するアクセスにフィルタを適用するか、または、他の様態で制御することが可能でなくてもよい。顧客による、顧客テナンシ１２２１内に包含されているデータプレーンＶＣＮ１２１８に対するフィルタの適用および制御は、データプレーンＶＣＮ１２１８を他の顧客および公衆インターネット１２５４から分離することを助けることができる。

【０１８０】
いくつかの実施形態において、クラウドサービス１２５６は、公衆インターネット１２５４、制御プレーンＶＣＮ１２１６、またはデータプレーンＶＣＮ１２１８上に存在しない場合があるサービスにアクセスするために、サービスゲートウェイ１２３６によってコールすることができる。クラウドサービス１２５６と制御プレーンＶＣＮ１２１６またはデータプレーンＶＣＮ１２１８との間の接続は、ライブまたは連続的でなくてもよい。クラウドサービス１２５６は、ＩａａＳプロバイダが所有または運営する異なるネットワーク上に存在し得る。クラウドサービス１２５６は、サービスゲートウェイ１２３６から呼を受信するように構成することができ、公衆インターネット１２５４からの呼は受信しないように構成することができる。いくつかのクラウドサービス１２５６は、他のクラウドサービス１２５６から分離され得、制御プレーンＶＣＮ１２１６は、制御プレーンＶＣＮ

１２１６と同じリージョンにない場合があるクラウドサービス１２５６から分離され得る。例えば、制御プレーンＶＣＮ１２１６は「リージョン１」に位置する場合があり、クラウドサービス「展開１１」は、リージョン１および「リージョン２」に位置する場合がある。展開１１に対する呼がリージョン１に位置する制御プレーンＶＣＮ１２１６内に包含されているサービスゲートウェイ１２３６によって行われた場合、呼は、リージョン１の展開１１に送信され得る。この例において、制御プレーンＶＣＮ１２１６またはリージョン１の展開１１は、リージョン２の展開１１に通信可能に結合されなくてもよく、または、他の様態でこれと通信しなくてもよい。

【０１８１】

図１３は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別の例示的なパターンを示すブロック図１３００である。サービスオペレータ１３０２（例えば、図１１のサービスオペレータ１１０２）は、仮想クラウドネットワーク（ＶＣＮ）１３０６（例えば、図１１のＶＣＮ１１０６）およびセキュアホストサブネット１３０８（例えば、図１１のセキュアホストサブネット１１０８）を含み得るセキュアホストテナンシ１３０４（例えば、図１１のセキュアホストテナンシ１１０４）に通信可能に結合することができる。ＶＣＮ１３０６は、ＬＰＧ１３１０（例えば、図１１のＬＰＧ１１１０）を含むことができ、これは、ＳＳＨ　ＶＣＮ１３１２に含まれるＬＰＧ１３１０を介してＳＳＨ　ＶＣＮ１３１２（例えば、図１１のＳＳＨ　ＶＣＮ１１１２）に通信可能に結合することができる。ＳＳＨ　ＶＣＮ１３１２は、ＳＳＨサブネット１３１４（例えば、図１１のＳＳＨサブネット１１１４）を含むことができ、ＳＳＨ　ＶＣＮ１３１２は、制御プレーンＶＣＮ１３１６に含まれるＬＰＧ１３１０を介して制御プレーンＶＣＮ１３１６（例えば、図１１の制御プレーンＶＣＮ１１１６）に通信可能に結合することができ、データプレーンＶＣＮ１３１８に含まれるＬＰＧ１３１０を介してデータプレーンＶＣＮ１３１８（例えば、図１１のデータプレーンＶＣＮ１１１８）に通信可能に結合することができる。制御プレーンＶＣＮ１３１６およびデータプレーンＶＣＮ１３１８は、サービステナンシ１３１９（例えば、図１１のサービステナンシ１１１９）に含めることができる。

【０１８２】

制御プレーンＶＣＮ１３１６は、ロードバランサ（ＬＢ）サブネット１３２２（例えば、図１１のＬＢサブネット１１２２）を含み得る制御プレーンＤＭＺ階層１３２０（例えば、図１１の制御プレーンＤＭＺ階層１１２０）と、アプリサブネット１３２６（例えば、図１１のアプリサブネット１１２６と同様の）を含み得る制御プレーンアプリ階層１３２４（例えば、図１１の制御プレーンアプリ階層１１２４）と、ＤＢサブネット１３３０を含み得る制御プレーンデータ階層１３２８（例えば、図１１の制御プレーンデータ階層１１２８）とを含み得る。制御プレーンＤＭＺ階層１３２０に含まれるＬＢサブネット１３２２は、制御プレーンアプリ階層１３２４に含まれるアプリサブネット１３２６および制御プレーンＶＣＮ１３１６に含まれ得るインターネットゲートウェイ１３３４（例えば、図１１のインターネットゲートウェイ１１３４）に通信可能に結合することができ、アプリサブネット１３２６は、制御プレーンデータ階層１３２８に含まれるＤＢサブネット１３３０ならびにサービスゲートウェイ１３３６（例えば、図１１のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ１３３８（例えば、図１１のＮＡＴゲートウェイ１１３８）に通信可能に結合することができる。制御プレーンＶＣＮ１３１６は、サービスゲートウェイ１３３６およびＮＡＴゲートウェイ１３３８を含み得る。

【０１８３】

データプレーンＶＣＮ１３１８は、データプレーンアプリ階層１３４６（例えば、図１１のデータプレーンアプリ階層１１４６）と、データプレーンＤＭＺ階層１３４８（例えば、図１１のデータプレーンＤＭＺ階層１１４８）と、データプレーンデータ階層１３５０（例えば、図１１のデータプレーンデータ階層１１５０）とを含み得る。データプレーンＤＭＺ階層１３４８は、データプレーンアプリ階層１３４６の信頼できるアプリサブネット１３６０および信頼できないアプリサブネット１３６２ならびにデータプレーンＶＣ

Ｎ１３１８内に包含されているインターネットゲートウェイ１３３４に通信可能に結合することができるＬＢサブネット１３２２を含み得る。信頼できるアプリサブネット１３６０は、データプレーンＶＣＮ１３１８内に包含されているサービスゲートウェイ１３３６、データプレーンＶＣＮ１３１８内に包含されているＮＡＴゲートウェイ１３３８、およびデータプレーンデータ階層１３５０内に包含されているＤＢサブネット１３３０に通信可能に結合することができる。信頼できないアプリサブネット１３６２は、データプレーンＶＣＮ１３１８内に包含されているサービスゲートウェイ１３３６およびデータプレーンデータ階層１３５０内に包含されているＤＢサブネット１３３０に通信可能に結合することができる。データプレーンデータ階層１３５０は、データプレーンＶＣＮ１３１８内に包含されているサービスゲートウェイ１３３６に通信可能に結合することができるＤＢサブネット１３３０を含み得る。

【０１８４】

信頼できないアプリサブネット１３６２は、テナント仮想マシン（ＶＭ）１３６６（１）～（Ｎ）に通信可能に結合することができる１つまたは複数のＶＮＩＣ１３６４（１）～（Ｎ）を含み得る。各テナントＶＭ１３６６（１）～（Ｎ）は、それぞれの顧客テナンシ１３７０（１）～（Ｎ）内に包含され得るそれぞれのコンテナイグレスＶＣＮ１３６８（１）～（Ｎ）内に包含され得るそれぞれのアプリサブネット１３６７（１）～（Ｎ）に通信可能に結合することができる。それぞれの二次ＶＮＩＣ１３７２（１）～（Ｎ）が、データプレーンＶＣＮ１３１８内に包含されている信頼できないアプリサブネット１３６２とコンテナイグレスＶＣＮ１３６８（１）～（Ｎ）内に包含されているアプリサブネットとの間の通信を促進することができる。各コンテナイグレスＶＣＮ１３６８（１）～（Ｎ）は、公衆インターネット１３５４（例えば、図１１の公衆インターネット１１５４）に通信可能に結合することができるＮＡＴゲートウェイ１３３８を含み得る。

【０１８５】

制御プレーンＶＣＮ１３１６内に包含されているインターネットゲートウェイ１３３４およびデータプレーンＶＣＮ１３１８内に包含されているインターネットゲートウェイ１３３４は、公衆インターネット１３５４に通信可能に結合することができるメタデータ管理サービス１３５２（例えば、図１１のメタデータ管理サービス１１５２）に通信可能に結合することができる。公衆インターネット１３５４は、制御プレーンＶＣＮ１３１６内に包含されているＮＡＴゲートウェイ１３３８およびデータプレーンＶＣＮ１３１８内に包含されているＮＡＴゲートウェイ１３３８に通信可能に結合することができる。制御プレーンＶＣＮ１３１６内に包含されているサービスゲートウェイ１３３６およびデータプレーンＶＣＮ１３１８内に包含されているサービスゲートウェイ１３３６は、クラウドサービス１３５６に通信可能に結合することができる。

【０１８６】

いくつかの実施形態において、データプレーンＶＣＮ１３１８は、顧客テナンシ１３７０と統合することができる。この統合は、コードを実行するときにサポートを所望し得る事例などのいくつかの事例において、ＩａａＳプロバイダの顧客にとって有用であるかまたは望ましい可能性がある。顧客は、破壊的であり得るか、他の顧客リソースと通信し得るか、または、他の様態で望ましくない影響を引き起こし得る、実行のためのコードを提供し得る。これに応答して、ＩａａＳプロバイダは、顧客によってＩａａＳプロバイダに与えられたコードを実行すべきか否かを判定することができる。

【０１８７】

いくつかの例において、ＩａａＳプロバイダの顧客は、一時的なネットワークアクセスをＩａａＳプロバイダに許可し、データプレーン階層アプリ１３４６に付随する機能を要求することができる。機能を実行するためのコードは、ＶＭ１３６６（１）～（Ｎ）内で実行することができ、コードは、データプレーンＶＣＮ１３１８上のそれ以外の場所で実行するように構成されなくてもよい。各ＶＭ１３６６（１）～（Ｎ）は、１つの顧客テナンシ１３７０に接続することができる。ＶＭ１３６６（１）～（Ｎ）内に包含されているそれぞれのコンテナ１３７１（１）～（Ｎ）が、コードを実行するように構成され得る。

この場合、二重の分離（例えば、コンテナ１３７１（１）～（Ｎ）がコードを実行し、ここで、コンテナ１３７１（１）～（Ｎ）が、少なくとも、信頼できないアプリサブネット１３６２内に包含されているＶＭ１３６６（１）～（Ｎ）内に包含され得る）が存在し得、これは、正しくないかまたは他の様態で望ましくないコードがＩａａＳプロバイダのネットワークを損傷すること、または、異なる顧客のネットワークを損傷することを防止するのを助けることができる。コンテナ１３７１（１）～（Ｎ）は、顧客テナンシ１３７０に通信可能に結合することができ、顧客テナンシ１３７０からデータを送信または受信するように構成することができる。コンテナ１３７１（１）～（Ｎ）は、データプレーンＶＣＮ１３１８内のいかなる他のエンティティからのデータを送信または受信するように構成されなくてもよい。コードの実行が完了すると、ＩａａＳプロバイダは、コンテナ１３７１（１）～（Ｎ）を停止させるかまたは他の様態で破棄することができる。

【０１８８】

いくつかの実施形態において、信頼できるアプリサブネット１３６０は、ＩａａＳプロバイダが所有または運用し得るコードを実行することができる。この実施形態において、信頼できるアプリサブネット１３６０は、ＤＢサブネット１３３０に通信可能に結合することができ、ＤＢサブネット１３３０におけるＣＲＵＤ動作を実行するように構成することができる。信頼できないアプリサブネット１３６２は、ＤＢサブネット１３３０に通信可能に結合することができるが、この実施形態においては、信頼できないアプリサブネットは、ＤＢサブネット１３３０における読み出し動作を実行するように構成することができる。各顧客のＶＭ１３６６（１）～（Ｎ）内に包含され得、顧客からのコードを実行し得るコンテナ１３７１（１）～（Ｎ）は、ＤＢサブネット１３３０と通信可能に結合されなくてもよい。

【０１８９】

他の実施形態において、制御プレーンＶＣＮ１３１６およびデータプレーンＶＣＮ１３１８は、直接的に通信可能に結合されなくてもよい。この実施形態において、制御プレーンＶＣＮ１３１６とデータプレーンＶＣＮ１３１８との間には直接通信が存在しなくてもよい。しかしながら、通信は、少なくとも１つの方法を通じて間接的に行うことができる。制御プレーンＶＣＮ１３１６とデータプレーンＶＣＮ１３１８との間の通信を促進することができるＬＰＧ１３１０が、ＩａａＳプロバイダによって確立され得る。別の例において、制御プレーンＶＣＮ１３１６またはデータプレーンＶＣＮ１３１８が、サービスゲートウェイ１３３６を介してクラウドサービス１３５６に対する呼を行うことができる。例えば、制御プレーンＶＣＮ１３１６からクラウドサービス１３５６に対する呼は、データプレーンＶＣＮ１３１８と通信することができるサービスに対する要求を含み得る。

【０１９０】

図１４は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別の例示的なパターンを示すブロック図１４００である。サービスオペレータ１４０２（例えば、図１１のサービスオペレータ１１０２）は、仮想クラウドネットワーク（ＶＣＮ）１４０６（例えば、図１１のＶＣＮ１１０６）およびセキュアホストサブネット１４０８（例えば、図１１のセキュアホストサブネット１１０８）を含み得るセキュアホストテナンシ１４０４（例えば、図１１のセキュアホストテナンシ１１０４）に通信可能に結合することができる。ＶＣＮ１４０６は、ＬＰＧ１４１０（例えば、図１１のＬＰＧ１１１０）を含むことができ、これは、ＳＳＨ　ＶＣＮ１４１２に含まれるＬＰＧ１４１０を介してＳＳＨ　ＶＣＮ１４１２（例えば、図１１のＳＳＨ　ＶＣＮ１１１２）に通信可能に結合することができる。ＳＳＨ　ＶＣＮ１４１２は、ＳＳＨサブネット１４１４（例えば、図１１のＳＳＨサブネット１１１４）を含むことができ、ＳＳＨ　ＶＣＮ１４１２は、制御プレーンＶＣＮ１４１６に含まれるＬＰＧ１４１０を介して制御プレーンＶＣＮ１４１６（例えば、図１１の制御プレーンＶＣＮ１１１６）に通信可能に結合することができ、データプレーンＶＣＮ１４１８に含まれるＬＰＧ１４１０を介してデータプレーンＶＣＮ１４１８（例えば、図１１のデータプレーンＶＣＮ１１１８）に通信可能に結合することができる。制御プレーンＶＣＮ１４１６およびデータプレーンＶＣＮ１４１８は、サービステナンシ

１４１９（例えば、図１１のサービステナンシ１１１９）に含めることができる。
【０１９１】
制御プレーンＶＣＮ１４１６は、ＬＢサブネット１４２２（例えば、図１１のＬＢサブネット１１２２）を含み得る制御プレーンＤＭＺ階層１４２０（例えば、図１１の制御プレーンＤＭＺ階層１１２０）と、アプリサブネット１４２６（例えば、図１１のアプリサブネット１１２６）を含み得る制御プレーンアプリ階層１４２４（例えば、図１１の制御プレーンアプリ階層１１２４）と、ＤＢサブネット１４３０（例えば、図１３のＤＢサブネット１３３０）を含み得る制御プレーンデータ階層１４２８（例えば、図１１の制御プレーンデータ階層１１２８）とを含み得る。制御プレーンＤＭＺ階層１４２０に含まれるＬＢサブネット１４２２は、制御プレーンアプリ階層１４２４に含まれるアプリサブネット１４２６および制御プレーンＶＣＮ１４１６に含まれ得るインターネットゲートウェイ１４３４（例えば、図１１のインターネットゲートウェイ１１３４）に通信可能に結合することができ、アプリサブネット１４２６は、制御プレーンデータ階層１４２８に含まれるＤＢサブネット１４３０ならびにサービスゲートウェイ１４３６（例えば、図１１のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ１４３８（例えば、図１１のＮＡＴゲートウェイ１１３８）に通信可能に結合することができる。制御プレーンＶＣＮ１４１６は、サービスゲートウェイ１４３６およびＮＡＴゲートウェイ１４３８を含み得る。
【０１９２】
データプレーンＶＣＮ１４１８は、データプレーンアプリ階層１４４６（例えば、図１１のデータプレーンアプリ階層１１４６）と、データプレーンＤＭＺ階層１４４８（例えば、図１１のデータプレーンＤＭＺ階層１１４８）と、データプレーンデータ階層１４５０（例えば、図１１のデータプレーンデータ階層１１５０）とを含み得る。データプレーンＤＭＺ階層１４４８は、データプレーンアプリ階層１４４６の信頼できるアプリサブネット１４６０（例えば、図１３の信頼できるアプリサブネット１３６０）および信頼できないアプリサブネット１４６２（例えば、図１３の信頼できないアプリサブネット１３６２）ならびにデータプレーンＶＣＮ１４１８内に包含されているインターネットゲートウェイ１４３４に通信可能に結合することができるＬＢサブネット１４２２を含み得る。信頼できるアプリサブネット１４６０は、データプレーンＶＣＮ１４１８内に包含されているサービスゲートウェイ１４３６、データプレーンＶＣＮ１４１８内に包含されているＮＡＴゲートウェイ１４３８、およびデータプレーンデータ階層１４５０内に包含されているＤＢサブネット１４３０に通信可能に結合することができる。信頼できないアプリサブネット１４６２は、データプレーンＶＣＮ１４１８内に包含されているサービスゲートウェイ１４３６およびデータプレーンデータ階層１４５０内に包含されているＤＢサブネット１４３０に通信可能に結合することができる。データプレーンデータ階層１４５０は、データプレーンＶＣＮ１４１８内に包含されているサービスゲートウェイ１４３６に通信可能に結合することができるＤＢサブネット１４３０を含み得る。
【０１９３】
信頼できないアプリサブネット１４６２は、信頼できないアプリサブネット１４６２内に存在するテナント仮想マシン（ＶＭ）１４６６（１）～（Ｎ）に通信可能に結合することができる一次ＶＮＩＣ１４６４（１）～（Ｎ）を含み得る。各テナントＶＭ１４６６（１）～（Ｎ）は、それぞれのコンテナ１４６７（１）～（Ｎ）内のコードを実行することができ、コンテナイグレスＶＣＮ１４６８内に包含され得るデータプレーンアプリ階層１４４６内に包含され得るアプリサブネット１４２６に通信可能に結合することができる。それぞれの二次ＶＮＩＣ１４７２（１）～（Ｎ）が、データプレーンＶＣＮ１４１８内に包含されている信頼できないアプリサブネット１４６２とコンテナイグレスＶＣＮ１４６８内に包含されているアプリサブネットとの間の通信を促進することができる。コンテナイグレスＶＣＮは、公衆インターネット１４５４（例えば、図１１の公衆インターネット１１５４）に通信可能に結合することができるＮＡＴゲートウェイ１４３８を含み得る。
【０１９４】

制御プレーンＶＣＮ１４１６内に包含されているインターネットゲートウェイ１４３４およびデータプレーンＶＣＮ１４１８内に包含されているインターネットゲートウェイ１４３４は、公衆インターネット１４５４に通信可能に結合することができるメタデータ管理サービス１４５２（例えば、図１１のメタデータ管理サービス１１５２）に通信可能に結合することができる。公衆インターネット１４５４は、制御プレーンＶＣＮ１４１６内に包含されているＮＡＴゲートウェイ１４３８およびデータプレーンＶＣＮ１４１８内に包含されているＮＡＴゲートウェイ１４３８に通信可能に結合することができる。制御プレーンＶＣＮ１４１６内に包含されているサービスゲートウェイ１４３６およびデータプレーンＶＣＮ１４１８内に包含されているサービスゲートウェイ１４３６は、クラウドサービス１４５６に通信可能に結合することができる。

【０１９５】

いくつかの例において、図１４のブロック図１４００のアーキテクチャによって示されているパターンは、図１３のブロック図１３００のアーキテクチャによって示されているパターンの例外と考えることができ、ＩａａＳプロバイダが顧客と直接的に通信することができない場合（例えば、切り離されたリージョン）に、ＩａａＳプロバイダの顧客にとっては望ましい場合がある。各顧客のＶＭ１４６６（１）～（Ｎ）内に包含されているそれぞれのコンテナ１４６７（１）～（Ｎ）は、顧客によってリアルタイムにアクセスすることができる。コンテナ１４６７（１）～（Ｎ）は、コンテナイグレスＶＣＮ１４６８内に包含され得るデータプレーンアプリ階層１４４６のアプリサブネット１４２６内に包含されているそれぞれの二次ＶＮＩＣ１４７２（１）～（Ｎ）に対する呼を行うように構成することができる。二次ＶＮＩＣ１４７２（１）～（Ｎ）は、ＮＡＴゲートウェイ１４３８に呼を送信することができ、ＮＡＴゲートウェイ１４３８は、公衆インターネット１４５４に呼を送信することができる。この例において、顧客によってリアルタイムにアクセスすることができるコンテナ１４６７（１）～（Ｎ）は、制御プレーンＶＣＮ１４１６から分離することができ、データプレーンＶＣＮ１４１８内に包含されている他のエンティティから分離することができる。コンテナ１４６７（１）～（Ｎ）はまた、他の顧客のリソースからも分離することができる。

【０１９６】

他の例において、顧客は、コンテナ１４６７（１）～（Ｎ）を使用してクラウドサービス１４５６をコールすることができる。この例において、顧客は、クラウドサービス１４５６からのサービスを要求するコードを、コンテナ１４６７（１）～（Ｎ）内で実行することができる。コンテナ１４６７（１）～（Ｎ）は、この要求を二次ＶＮＩＣ１４７２（１）～（Ｎ）に送信することができ、二次ＶＮＩＣ１４７２（１）～（Ｎ）は、ＮＡＴゲートウェイに要求を送信することができ、ＮＡＴゲートウェイは、公衆インターネット１４５４に要求を送信することができる。公衆インターネット１４５４は、インターネットゲートウェイ１４３４を介して、制御プレーンＶＣＮ１４１６内に包含されているＬＢサブネット１４２２に要求を送信することができる。要求が有効であるという判定に応答して、ＬＢサブネットは、アプリサブネット１４２６に要求を送信することができ、アプリサブネット１４２６は、サービスゲートウェイ１４３６を介してクラウドサービス１４５６に要求を送信することができる。

【０１９７】

図面に示されているＩａａＳアーキテクチャ１１００、１２００、１３００、１４００は、図示されている以外の構成要素を有し得ることが理解されるべきである。さらに、図面に示されている実施形態は、本開示の実施形態を組み込むことができるクラウドインフラストラクチャシステムの一部の例に過ぎない。いくつかの他の実施形態において、ＩａａＳシステムは、図示されているよりも多いもしくは少ない構成要素を有してもよく、２つ以上の構成要素を組み合わせてもよく、または、構成要素の異なる構成もしくは配置を有し得る。

【０１９８】

ある実施形態において、本明細書に記載されているＩａａＳシステムは、セルフサービ

スで、サブスクリプションに基づいて、弾性的にスケーリング可能に、信頼可能に、高度に利用可能に、および安全に顧客に送達されるアプリケーション、ミドルウェア、およびデータベースサービス供給物のスイートを含み得る。そのようなＩａａＳの一例は、本譲受人によって提供されるOracleインフラストラクチャ（ＯＣＩ）である。

【０１９９】

図１５は、様々な実施形態を実装することができる例示的なコンピュータシステム１５００を示す。システム１５００は、上述したコンピュータシステムのいずれかを実装するために使用することができる。図面に示すように、コンピュータシステム１５００は、バスサブシステム１５０２を介して複数の周辺サブシステムと通信する処理装置１５０４を含む。これらの周辺サブシステムは、処理加速ユニット１５０６、Ｉ／Ｏサブシステム１５０８、記憶サブシステム１５１８および通信サブシステム１５２４を含み得る。記憶サブシステム１５１８は、有形コンピュータ可読記憶媒体１５２２およびシステムメモリ１５１０を含む。

【０２００】

バスサブシステム１５０２は、コンピュータシステム１５００の様々な構成要素およびサブシステムを意図したように互いに通信させるためのメカニズムを提供する。バスサブシステム１５０２は、単一のバスとして概略的に示されているが、バスサブシステムの代替的な実施形態は、複数のバスを利用し得る。バスサブシステム１５０２は、メモリバスまたはメモリコントローラ、周辺機器用バス、および、様々なバスアーキテクチャのうちのいずれかを使用するローカルバスを含む、いくつかのタイプのバス構造のいずれかであり得る。例えば、このようなアーキテクチャは、業界標準アーキテクチャ（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（ＭＣＡ）バス、拡張ＩＳＡ（ＥＩＳＡ）バス、ビデオ電子機器標準規格化協会（ＶＥＳＡ）ローカルバス、および、ＩＥＥＥ　Ｐ１３８６．１規格に従って製造されたメザニン（Mezzanine）バスとして実装され得る周辺構成要素相互接続（ＰＣＩ）バスを含み得る。

【０２０１】

１つまたは複数の集積回路（例えば、従来のマイクロプロセッサまたはマイクロコントローラ）として実装することができる処理装置１５０４は、コンピュータシステム１５００の動作を制御する。１つまたは複数のプロセッサが、処理装置１５０４に含まれ得る。これらのプロセッサは、シングルコアまたはマルチコアプロセッサを含み得る。ある実施形態において、処理装置１５０４は、各処理装置に含まれるシングルまたはマルチコアプロセッサを有する１つまたは複数の独立した処理装置１５３２および／または１５３４として実装され得る。他の実施形態において、処理装置１５０４はまた、２つのデュアルコアプロセッサを単一のチップに集積することによって形成されるクアッドコア処理装置としても実装され得る。

【０２０２】

様々な実施形態において、処理装置１５０４は、プログラムコードに応答して様々なプログラムを実行することができ、複数の同時に実行されているプログラムまたはプロセスを維持することができる。任意の所与の時点において、実行されるプログラムコードの一部または全部が、プロセッサ１５０４および／または記憶サブシステム１５１８内に存在することができる。適切なプログラミングを通じて、プロセッサ１５０４は、上述した様々な機能を提供することができる。コンピュータシステム１５００は、付加的に、デジタル信号プロセッサ（ＤＳＰ）、専用プロセッサなどを含み得る処理加速ユニット１５０６を含み得る。

【０２０３】

Ｉ／Ｏサブシステム１５０８は、ユーザインターフェイス入力デバイスおよびユーザインターフェイス出力デバイスを含み得る。ユーザインターフェイス入力デバイスは、キーボード、マウスまたはトラックボール、タッチパッドまたはディスプレイに組み込まれたタッチスクリーンなどのポインティングデバイス、スクロールホイール、クリックホイール、ダイヤル、ボタン、スイッチ、キーパッド、音声コマンド認識システムを有する音響

入力デバイス、マイクロフォン、および他のタイプの入力デバイスを含み得る。ユーザインターフェイス入力デバイスは、例えば、ユーザが、ジェスチャおよび音声指示を使用してナチュラルユーザインターフェイスを通じて、Microsoft Xbox（登録商標）３６０ゲームコントローラなどの入力デバイスを制御し、それとインタラクトすることを可能にするMicrosoft Kinect（登録商標）運動センサなどの運動検知および／またはジェスチャ認識デバイスを含み得る。ユーザインターフェイス入力デバイスはまた、ユーザから眼球活動（例えば、写真を撮っている、および／または、メニュー選択を行っている間の「まばたき」）を検出し、そのアイジェスチャを入力デバイス（例えば、Google（登録商標） Glass）への入力として変換するGoogle（登録商標） Glassまばたき検出器などのアイジェスチャ認識デバイスも含み得る。付加的に、ユーザインターフェイス入力デバイスは、ユーザが、音声コマンドを通じて音声認識システム（例えば、Siri（登録商標）ナビゲータ）とインタラクトすることを可能にする音声認識検知デバイスを含み得る。

【０２０４】

ユーザインターフェイス入力デバイスはまた、限定ではないが、三次元（３Ｄ）マウス、ジョイスティックまたはポインティングスティック、ゲームパッドおよびグラフィックタブレット、ならびに、スピーカ、デジタルカメラ、デジタルカムコーダ、ポータブルメディアプレーヤ、ウェブカメラ、画像スキャナ、指紋スキャナ、バーコードリーダ３Ｄスキャナ、３Ｄプリンタ、レーザ測距器、および視線追跡デバイスなどの音響／視覚デバイスも含み得る。付加的に、ユーザインターフェイス入力デバイスは、例えば、コンピュータ断層撮影、磁気共鳴イメージング、位置（position）放出断層撮影、医用超音波検査デバイスなどの医療撮像入力デバイスを含み得る。ユーザインターフェイス入力デバイスはまた、例えば、ＭＩＤＩキーボード、デジタル楽器などのような音響入力デバイスも含み得る。

【０２０５】

ユーザインターフェイス出力デバイスは、ディスプレイサブシステム、表示灯、または音響出力デバイスなどの非視覚的表示を含み得る。ディスプレイサブシステムは、陰極線管（ＣＲＴ）、液晶ディスプレイ（ＬＤＣ）またはプラズマディスプレイを使用するものなどのフラットパネルデバイス、投影デバイス、タッチスクリーンなどであり得る。一般に、「出力デバイス」という用語の使用は、コンピューティングデバイス１５００からユーザまたは他のコンピュータに情報を出力するためのすべての可能なタイプのデバイスおよびメカニズムを含むことを意図している。例えば、ユーザインターフェイス出力デバイスは、限定ではないが、モニタ、プリンタ、スピーカ、ヘッドフォン、自動車ナビゲーションシステム、プロッタ、音声出力デバイス、およびモデムなどの、テキスト、グラフィックおよび音響／ビデオ情報を視覚的に伝達する様々なディスプレイデバイスを含み得る。

【０２０６】

コンピュータシステム１５００は、目下のところシステムメモリ１５１０内に位置するものとして示されている、ソフトウェア要素を含む記憶サブシステム１５１８を備えることができる。システムメモリ１５１０は、処理装置１５０４上にロード可能かつ実行可能であるプログラム命令、および、これらのプログラムの実行中に生成されるデータを記憶することができる。

【０２０７】

コンピュータシステム１５００の構成およびタイプに応じて、システムメモリ１５１０は、揮発性（ランダムアクセスメモリ（ＲＡＭ）など）および／または不揮発性（読み出し専用メモリ（ＲＯＭ）、フラッシュメモリなど）であり得る。ＲＡＭは、典型的には、処理装置１５０４にとって直ちにアクセス可能であり、ならびに／または、処理装置１５０４によって現在動作および実行されているデータおよび／またはプログラムモジュールを包含する。いくつかの実施態様において、システムメモリ１５１０は、スタティックランダムアクセスメモリ（ＳＲＡＭ）またはダイナミックランダムアクセスメモリ（ＤＲＡ

Ｍ）などの、複数の異なるタイプのメモリを含み得る。いくつかの実施態様において、起動中などにコンピュータシステム１５００内の要素間で情報を転送するのを助ける基本ルーチンを包含する基本入出力システム（ＢＩＯＳ）が、典型的には、ＲＯＭ内に記憶され得る。限定ではなく例として、システムメモリ１５１０はまた、クライアントアプリケーション、ウェブブラウザ、中間層アプリケーション、リレーショナルデータベース管理システム（ＲＤＢＭＳ）などを含み得るアプリケーションプログラム１５１２、プログラムデータ１５１４、およびオペレーティングシステム１５１６も例示する。例として、オペレーティングシステム１５１６は、様々なバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、ならびに／または、様々な市販のUNIX（登録商標）もしくはUNIX系オペレーティングシステム（限定ではないが、様々なGNU/Linuxオペレーティングシステム、Google Chrome(登録商標）OSなど）、ならびに／または、iOS、Windows（登録商標）Phone、Android（登録商標）OS、BlackBerry（登録商標）15 OS、およびPalm（登録商標）OSオペレーティングシステムなどのモバイルオペレーティングシステムを含み得る。

【０２０８】

記憶サブシステム１５１８はまた、いくつかの実施形態の機能を提供する基本プログラミングおよびデータ構造を記憶するための有形コンピュータ可読記憶媒体も提供することができる。プロセッサによって実行されると、上述した機能を提供するソフトウェア（プログラム、コードモジュール、命令）が、記憶サブシステム１５１８に記憶され得る。これらのソフトウェアモジュールまたは命令は、処理装置１５０４によって実行され得る。記憶サブシステム１５１８はまた、本開示に従って使用されるデータを記憶するためのリポジトリも提供することができる。

【０２０９】

記憶サブシステム１５００はまた、コンピュータ可読記憶媒体１５２２にさらに接続することができるコンピュータ可読記憶媒体リーダ１５２０も含み得る。システムメモリ１５１０とともに、および、任意選択的にシステムメモリ１５１０と組み合わせて、コンピュータ可読記憶媒体１５２２は、コンピュータ可読情報を一時的に、および／または、より持続的に含み、記憶し、送信し、および抽出するための記憶媒体に加えて、遠隔、ローカル、固定、および／または取り外し可能な記憶デバイスを包括的に表わし得る。

【０２１０】

コードまたはコードの部分を包含するコンピュータ可読記憶媒体１５２２はまた、限定ではないが、情報を記憶および／または送信するための任意の方法または技術において実装される揮発性および不揮発性、取り外し可能および取り外し不能媒体などの、記憶媒体および通信媒体を含む、当該技術分野において知られているかまたは使用されている任意の適切な媒体を含み得る。これは、ＲＡＭ、ＲＯＭ、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）もしくは他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気的記憶デバイス、または、他の有形コンピュータ可読媒体などの有形コンピュータ可読記憶媒体を含み得る。これはまた、データ信号、データ送信、または、所望の情報を送信するために使用することができ、コンピューティングシステム１５００によってアクセスすることができる任意の他の媒体などの非有形コンピュータ可読媒体も含み得る。

【０２１１】

例として、コンピュータ可読記憶媒体１５２２は、取り外し不能不揮発性磁気媒体から読み出すかまたはこれに書き込むハードディスクドライブ、取り外し可能不揮発性磁気ディスクから読み出すかまたはこれに書き込む磁気ディスクドライブ、および、ＣＤ ＲＯＭ、ＤＶＤ、およびＢｌｕ－ｒａｙ（登録商標）ディスクまたは他の光媒体などの取り外し可能不揮発性光ディスクから読み出すかまたはこれに書き込む光ディスクドライブを含み得る。コンピュータ可読記憶媒体１５２２は、限定ではないが、Ｚｉｐ（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（ＵＳＢ）フラッシュデバ

イス、セキュアデジタル（ＳＤ）カード、ＤＶＤディスク、デジタルビデオテープなどを含み得る。コンピュータ可読記憶媒体１５２２はまた、フラッシュメモリベースのＳＳＤ、企業フラッシュドライブ、ソリッドステートＲＯＭなどのような不揮発性メモリに基づくソリッドステートドライブ（ＳＳＤ）、ソリッドステートＲＡＭ、ダイナミックＲＡＭ、スタティックＲＡＭなどの揮発性メモリに基づくＳＳＤ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（ＭＲＡＭ）ＳＳＤ、およびＤＲＡＭとフラッシュメモリベースのＳＳＤとの組合せを使用するハイブリッドＳＳＤも含み得る。ディスクドライブおよびそれらの関連コンピュータ可読媒体は、コンピュータシステム１５００に、コンピュータ可読命令、データ構造体、プログラムモジュールおよび他のデータの不揮発性記憶を提供することができる。

【０２１２】

通信サブシステム１５２４は、他のコンピュータシステムおよびネットワークに対するインターフェイスを提供する。通信サブシステム１５２４は、他のシステムからデータを受信し、コンピュータシステム１５００から他のシステムにデータを送信するためのインターフェイスとしての役割を果たす。例えば、通信サブシステム１５２４は、コンピュータシステム１５００が、インターネットを介して１つまたは複数のデバイスに接続することを可能にすることができる。いくつかの実施形態において、通信サブシステム１５２４は、ワイヤレス音声および／もしくはデータネットワーク（例えば、携帯電話技術、３Ｇ、４ＧまたはＥＤＧＥ（グローバル進化型高速データレート）、ＷｉＦｉ（ＩＥＥＥ８０２．１１ファミリ規格、もしくは他のモバイル通信技術などの先進的なデータネットワーク技術、またはそれらの任意の組合せを使用する）にアクセスするための無線周波数（ＲＦ）トランシーバ構成要素、全地球測位システム（ＧＰＳ）レシーバ構成要素、ならびに／または他の構成要素を含み得る。いくつかの実施形態において、通信サブシステム１５２４は、ワイヤレスインターフェイスに加えてまたはその代わりに有線ネットワーク接続（例えば、イーサネット（登録商標））を提供することができる。

【０２１３】

いくつかの実施形態において、通信サブシステム１５２４はまた、コンピュータシステム１５００を使用することができる１または複数のユーザに代わりに、構造化および／または非構造化データフィード１５２６、イベントストリーム１５２８、イベント更新１５３０などの形態の入力通信を受信することもできる。

【０２１４】

例として、通信サブシステム１５２４は、Ｔｗｉｔｔｅｒ（登録商標）フィード、Ｆａｃｅｂｏｏｋ（登録商標）更新、リッチサイトサマリ（ＲＳＳ）フィードなどのウェブフィード、および／または１つもしくは複数のサードパーティ情報源からのリアルタイム更新などの、ソーシャルネットワークおよび／または他の通信サービスのユーザからデータフィード１５２６をリアルタイムに受信するように構成することができる。

【０２１５】

付加的に、通信サブシステム１５２４はまた、本質的に明確な終わりがない連続的または無制限であり得る、リアルタイムイベントのイベントストリーム１５２８および／またはイベント更新１５３０を含み得る、連続データストリームの形態のデータを受信するように構成することもできる。連続データを生成するアプリケーションの例は、例えば、センサデータアプリケーション、ファイナンシャルティッカー、ネットワーク性能測定ツール（例えば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通監視などを含み得る。

【０２１６】

通信サブシステム１５２４はまた、コンピュータシステム１５００に結合されている１つまたは複数のストリーミングデータ源コンピュータと通信することができる１つまたは複数のデータベースに、構造化および／または非構造化データフィード１５２６、イベントストリーム１５２８、イベント更新１５３０などを出力するように構成することもできる。

【０２１７】
コンピュータシステム１５００は、手持ち式ポータブルデバイス（例えば、ｉＰｈｏｎｅ（登録商標）携帯電話、ｉＰａｄ（登録商標）コンピューティングタブレット、ＰＤＡ）、ウェアラブルデバイス（例えば、Ｇｏｏｇｌｅ　Ｇｌａｓｓ（登録商標）ヘッドマウントディスプレイ）、ＰＣ、ワークステーション、メインフレーム、キオスク、サーバラック、または任意の他のデータ処理システムを含む、様々なタイプのうちの１つとすることができる。
【０２１８】
コンピュータおよびネットワークの絶えず変化する性質のために、図面に示されているコンピュータデバイス１５００の説明は、特定の例としてのみ意図されている。図面に示されるシステムよりも多いまたは少ない構成要素を有する、多くの他の構成が可能である。例えば、カスタム化ハードウェアもまた使用されてもよく、および／または、特定の要素が、ハードウェア、ファームウェア、ソフトウェア（アプレットを含む）、または組合せにおいて実装され得る。さらに、ネットワーク入出力デバイスなどの他のコンピューティングデバイスへの接続が利用され得る。本開示および本明細書において提供されている教示に基づいて、当業者には、様々な実施形態を実装するための他の様式および／または方法が明らかであろう。
【０２１９】
実施形態は、プロセッサによって実行されると、プロセッサに、本開示に記載の方法のいずれかを実施させるコンピュータプログラム命令を含むコンピュータプログラム製品を使用することによって実装することができる。
【０２２０】
特定の実施形態が説明されたが、様々な修正、改変、代替的な構成、および均等物も、本開示の範囲内に包含される。実施形態は、ある特定のデータ処理環境内での動作に限定されず、複数のデータ処理環境内で自由に動作することができる。付加的に、実施形態は特定の系列のトランザクションおよびステップを使用して説明されているが、本開示の範囲は、記載されている系列のトランザクションおよびステップには限定されないことは、当業者に明らかであろう。上述した実施形態の様々な特徴および態様は、個別にまたは連帯して使用され得る。
【０２２１】
さらに、実施形態は、ハードウェアとソフトウェアとの特定の組合せを使用して説明されているが、ハードウェアとソフトウェアとの他の組合せも、本開示の範囲内にあることは認識されたい。実施形態は、ハードウェア内でのみ、もしくはソフトウェア内でのみ、またはそれらの組合せを使用して実装され得る。本明細書に記載されている様々なプロセスは、同じプロセッサ上で、または、任意の組合せにおける複数の異なるプロセッサ上で実装することができる。したがって、構成要素またはモジュールが特定の動作を実施するように構成されているものとして説明されている場合、そのような構成は、例えば、動作を実施するように電子回路を設計することによって、動作を実施するようにプログラム可能電子回路（マイクロプロセッサなど）をプログラムすることによって、またはその任意の組合せによって、そのような構成を達成することができる。プロセスは、限定ではないが、プロセス間通信のための従来の技法を含む様々な技法を使用して通信することができ、プロセスの異なる対が、異なる技法を使用してもよく、または、プロセスの同じ対が、異なる時点において異なる技法を使用し得る。
【０２２２】
したがって、本明細書および図面は、限定的な意味ではなく、例示的な意味において考慮されるべきである。しかしながら、特許請求の範囲に記載されているより広い思想および範囲から逸脱することなく、追加、差し引き、削除、および他の修正および変更をそれに行うことができることは明らかであろう。したがって、特定の開示実施形態が説明されているが、これらは、限定であるようには意図されていない。様々な修正および均等物が、添付の特許請求項の範囲内にある。

【０２２３】
本開示の実施形態を説明する文脈における（特に、以下の特許請求の範囲の文脈における）「a」および「an」ならびに「the」という用語および同様の指示対象の使用は、本明細書において別様に指示されていない限り、または、文脈と明確に矛盾しない限り、単数および複数の両方をカバーするように解釈されるべきである。「備える（comprising）」、「有する（having）」、「含む（including）」および「包含する（containing）」という用語は、特に言及されていない限り、オープンエンドな用語（すなわち、「限定ではないが、……を含む」を意味する）として解釈されるべきである。「接続されている」という用語は、何かが介在する場合であっても、部分的にまたは全体が中に包含されているか、取り付けられているか、またはともに接合されているものとして解釈されるべきである。本明細書における値の範囲の記述は、本明細書において別様に指示されておらず、各別個の値が本明細書において個別に記述されているかのように本明細書に組み込まれていない限り、その範囲内に入る各別個の値を個別に参照する簡潔な方法としての役割を果たすように意図されているに過ぎない。本明細書に記載されているすべての方法は、本明細書において別様に指示されていない限り、または、文脈と明確に矛盾しない限り、任意の適切な順序において実施することができる。本明細書において与えられているあらゆる例、または例示の文言（例えば、「～のような（such as）」）は、より良好に実施形態の理解を助けるようにのみ意図されており、別途主張されない限り、本開示の範囲に限定を課すものではない。本明細書におけるいかなる文言も、任意の特許請求されていない要素を、本開示の実践に必須であるとして指示しているものとして解釈されるべきではない。

【０２２４】
「Ｘ、ＹまたはＺのうちの少なくとも１つ」という語句などの離接的な文言は、別途具体的に述べられない限り、アイテム、項目などが、Ｘ、Ｙ、もしくはＺのいずれか、または、それらの任意の組合せ（例えば、Ｘ、Ｙ、および／またはＺ）であり得ることを提示するために、一般的に使用されるような文脈内で理解されるように意図されている。したがって、そのような離接的な文言は、概して、ある実施形態が、Ｘのうちの少なくとも１つ、Ｙのうちの少なくとも１つ、またはＺのうちの少なくともが各々提示されることを要求することを暗示するようには意図されておらず、暗示すべきでもない。

【０２２５】
本開示を実行するための、知られている最良の形態を含む、本開示の好ましい実施形態が、本明細書において記載されている。それらの好ましい実施形態の変形例が、上記の説明を読めば、当業者に明らかになり得る。当業者であれば、そのような変形例を適切であるとして利用することが可能であるはずであり、本開示は、具体的に本明細書に記載されているものとは別様に実践され得る。したがって、本開示は、適用法令によって許可されるものとしての、本明細書に添付の特許請求の範囲に挙げられている主題のすべての修正形態および等価形態を含む。その上、本明細書において別途指示しない限り、すべての可能な変形における上述した要素の任意の組合せが、本開示によって包含される。

【０２２６】
本明細書において引用されている、刊行物、特許出願、および特許を含む、すべての参考文献は、各参考文献が参照により組み込まれるように個々にかつ具体的に指示され、かつその全体が本明細書において記載されている場合と同じ程度まで、参照により本明細書に組み込まれる。

【０２２７】
上記の明細書において、本開示の態様は、その特定の実施形態を参照して説明されているが、本開示はそれに限定されないことが、当業者には認識されよう。上述した開示の様々な特徴および態様は、個別にまたは連帯して使用され得る。さらに、実施形態は、本明細書のより広い思想および範囲から逸脱することなく、本明細書に記載されているものを超えて、任意の数の環境および用途において利用することができる。したがって、本明細書および図面は、限定ではなく、例示的なものとして考慮されるべきである。

【図面】

【図１】

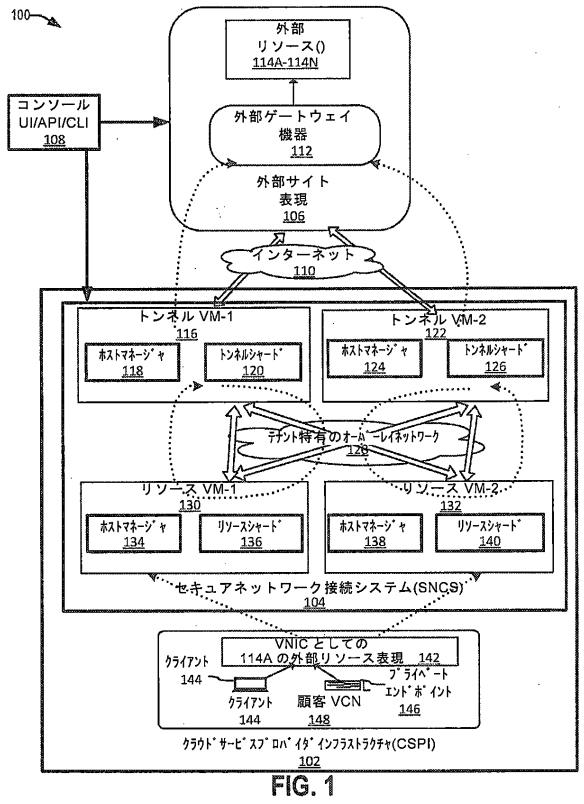

FIG. 1

【図２】

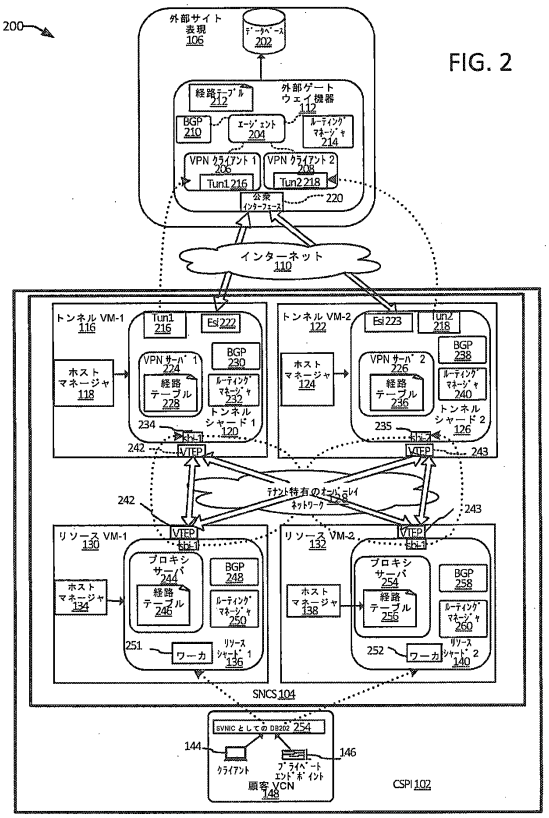

FIG. 2

【図３】

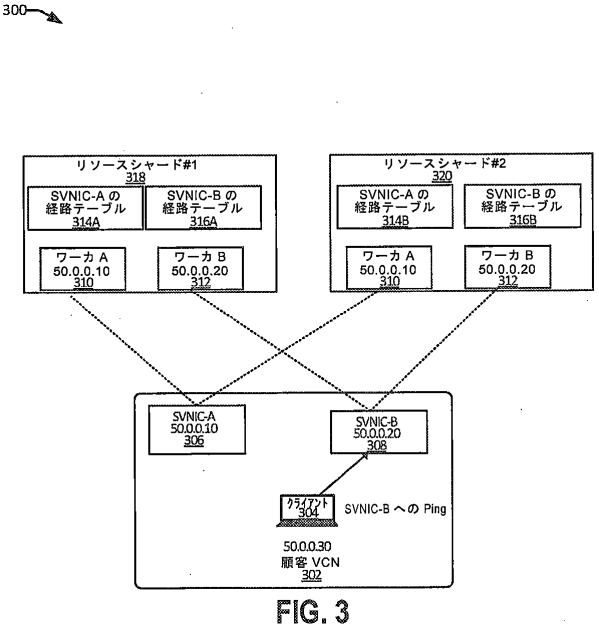

FIG. 3

【図４】

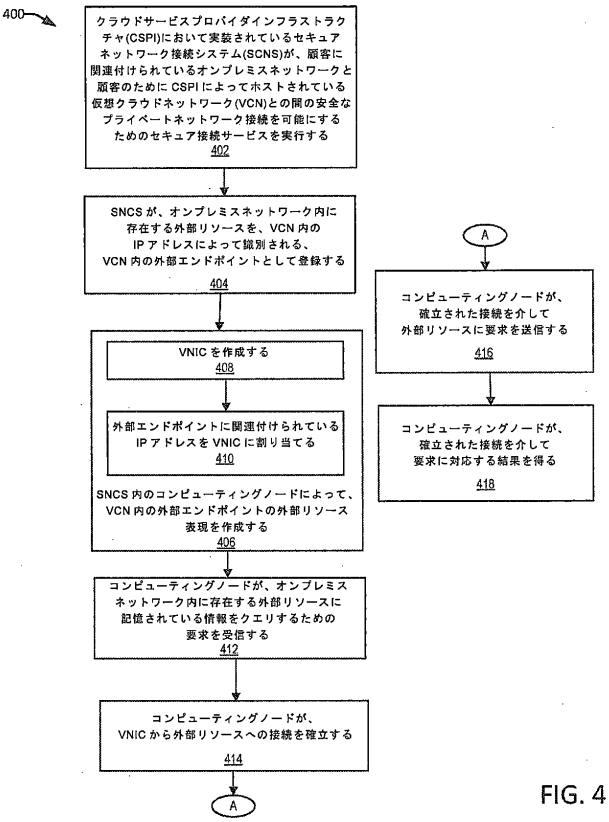

FIG. 4

【図５】

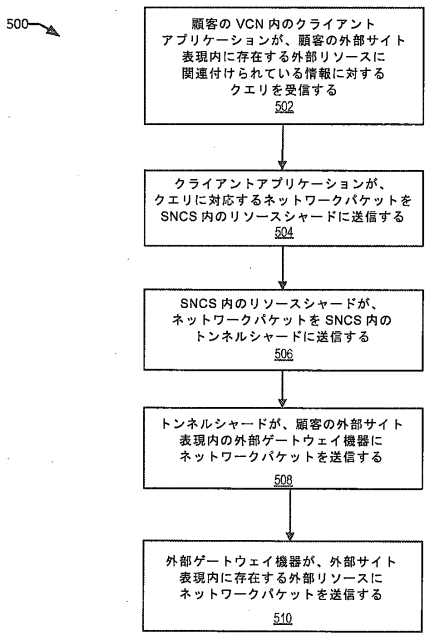

FIG. 5

【図６】

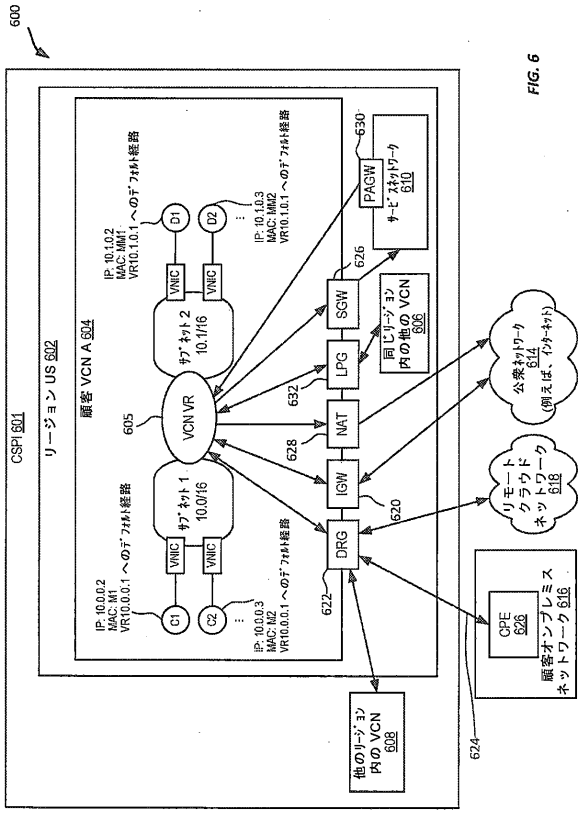

FIG. 6

【図７】

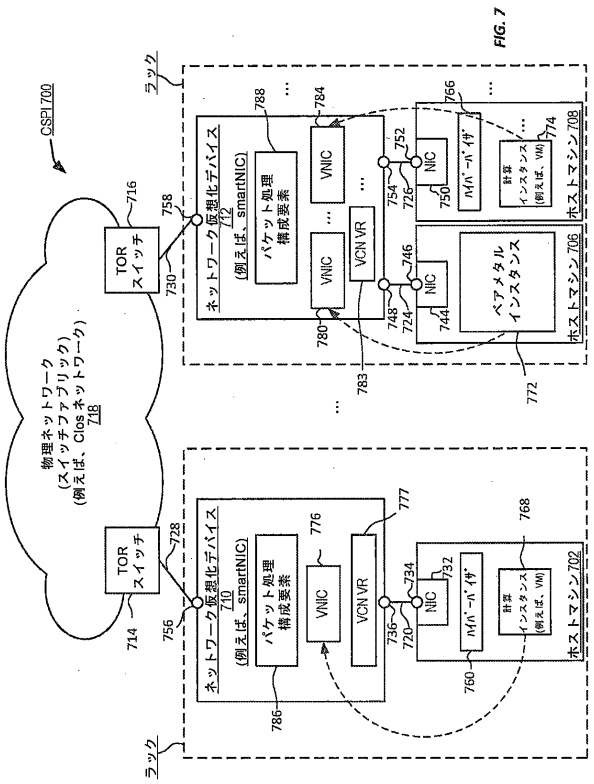

FIG. 7

【図８】

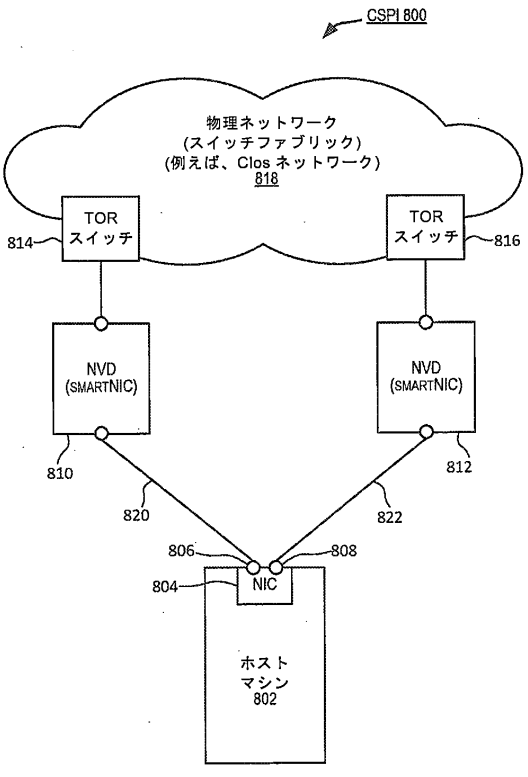

FIG. 8

【図９】

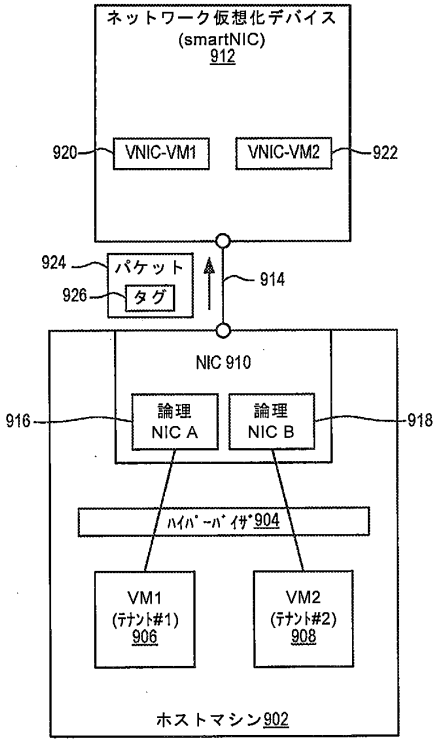

FIG. 9

【図１０】

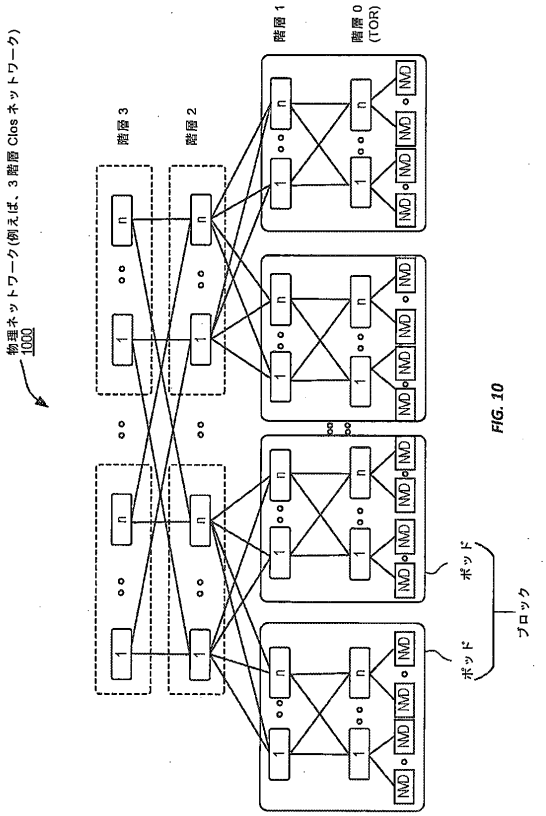

FIG. 10

【図１１】

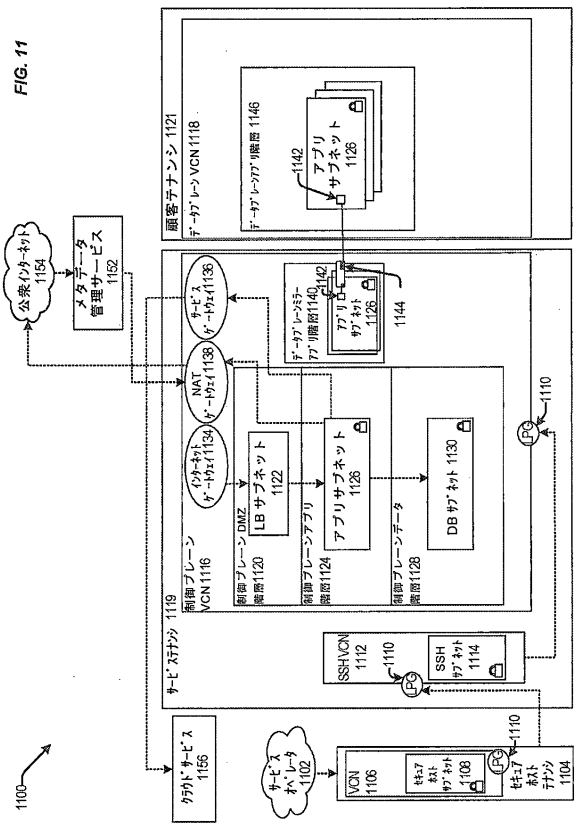

FIG. 11

【図１２】

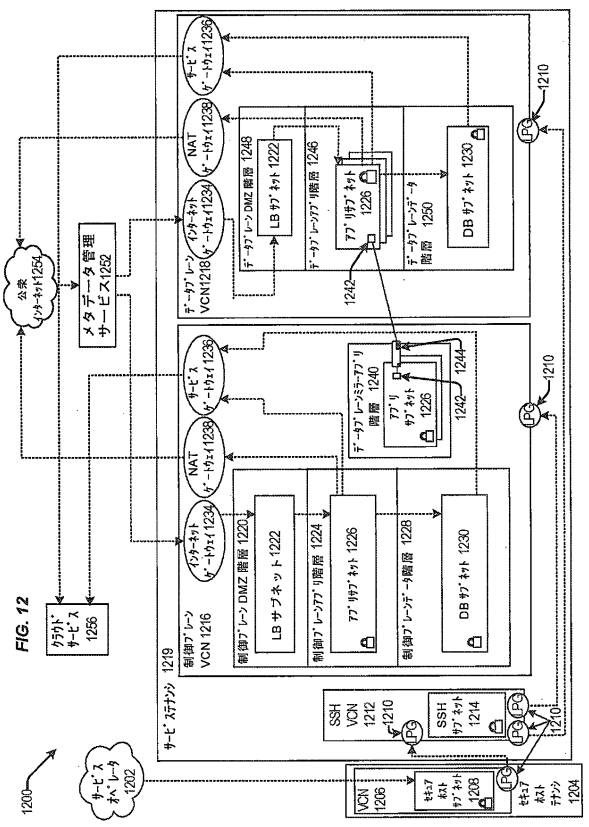

FIG. 12

【図１３】

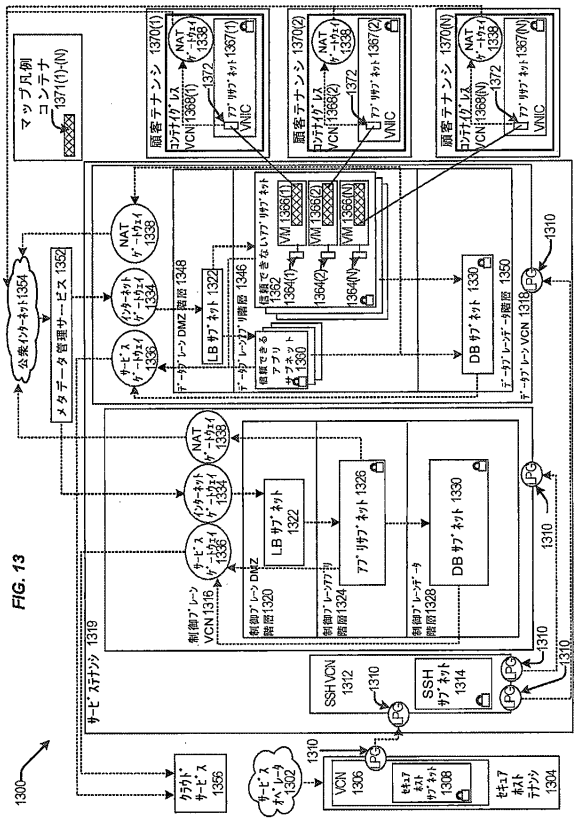

FIG. 13

【図１４】

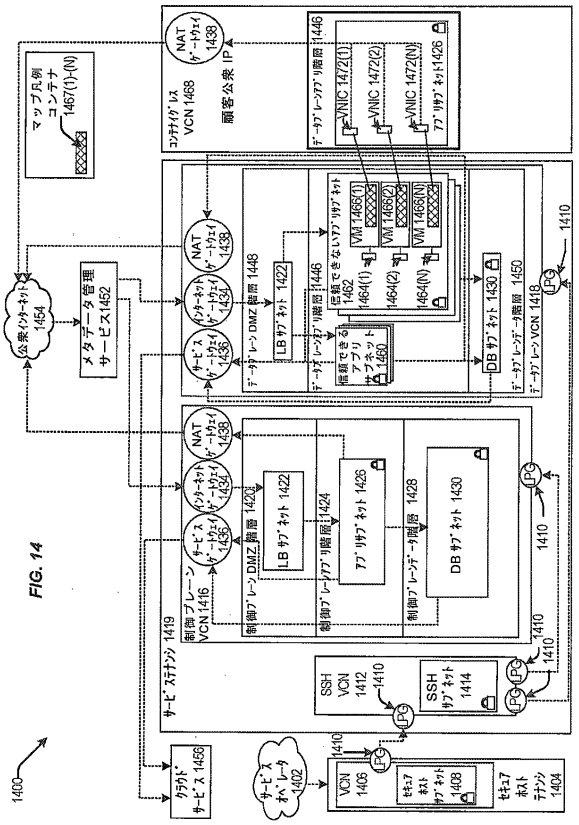

FIG. 14

【図１５】

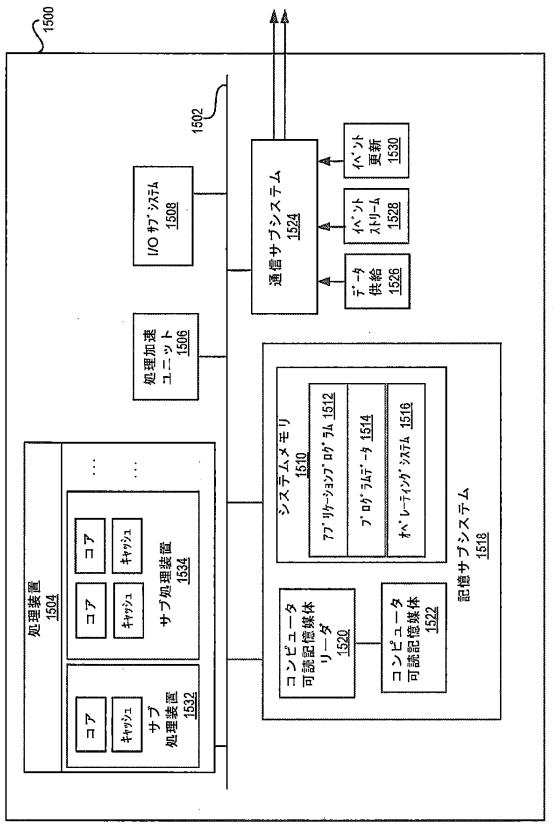

FIG. 15

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/034751

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/40 H04L45/00 G06F9/455
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/382471 A1 (JANAKIRAMAN RAJAGOPALAN [US] ET AL) 3 December 2020 (2020-12-03) paragraph [0001] - paragraph [0075]; figures 1-4	1-21
X	US 2018/062920 A1 (SRINIVASAN ARAVIND [US] ET AL) 1 March 2018 (2018-03-01) paragraph [0002] - paragraph [0046]	1-21
X	US 2019/222559 A1 (WANG NAN [CN] ET AL) 18 July 2019 (2019-07-18) paragraph [0001] - paragraph [0031]	1,12,17, 21

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

* Special categories of cited documents :

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

Date of the actual completion of the international search	Date of mailing of the international search report
15 September 2022	23/09/2022
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Veshi, Erzim

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/034751

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020382471 A1	03-12-2020	NONE	
US 2018062920 A1	01-03-2018	US 2018062920 A1	01-03-2018
		US 2018063074 A1	01-03-2018
		US 2018063077 A1	01-03-2018
		US 2018063743 A1	01-03-2018
		US 2018069924 A1	08-03-2018
US 2019222559 A1	18-07-2019	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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

（特許庁注：以下のものは登録商標）

１．ＷＩＮＤＯＷＳ ＰＨＯＮＥ

２．ｉＯＳ

ョン

(72)発明者 カルケラ，アビマン・ヤシュパラ

アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション

(72)発明者 シャー，ドゥワニッシュ・プラムテシュ

アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション

(72)発明者 ペイ，グアンホン

アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション

(72)発明者 マグウィルク，クレイトン・マシュー

アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション

(72)発明者 ケインカー，ポール・ジェイムズ

アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション