

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2025-506384
(P2025-506384A)

(43)公表日 令和7年3月11日(2025.3.11)

(51)国際特許分類
H 0 4 L 45/76 (2022.01)

F I
H 0 4 L 45/76

テーマコード (参考)
5 K 0 3 0

審査請求 未請求 予備審査請求 未請求 (全77頁)

(21)出願番号 (86)(22)出願日 (85)翻訳文提出日 (86)国際出願番号 (87)国際公開番号 (87)国際公開日 (31)優先権主張番号 (32)優先日 (33)優先権主張国・地域又は機関 (31)優先権主張番号 (32)優先日 (33)優先権主張国・地域又は機関 (31)優先権主張番号	特願2024-545931(P2024-545931) 令和5年2月1日(2023.2.1) 令和6年9月25日(2024.9.25) PCT/US2023/012084 WO2023/150143 令和5年8月10日(2023.8.10) 63/306,007 令和4年2月2日(2022.2.2) 米国(US) 63/306,918 令和4年2月4日(2022.2.4) 米国(US) 63/321,614	(71)出願人 (74)代理人 (72)発明者	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 9 4 0 6 5 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 5 0 0 110001195 弁理士法人深見特許事務所 カーニー, ルーク・フランシス アメリカ合衆国、9 4 0 6 5 カリフォ ルニア州、レッドウッド・シティ、オ ラクル・パークウェイ、5 0 0、オラク ル・インターナショナル・コーポレイシ ョン内
---	---	-------------------------------	--

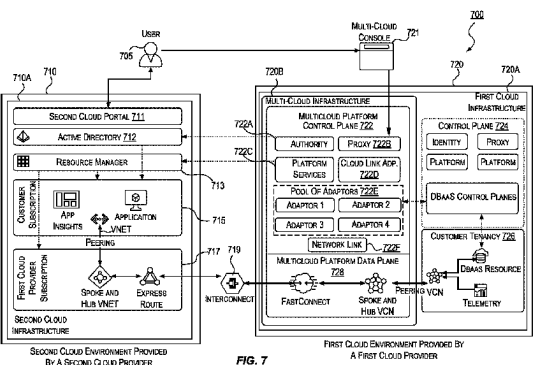
最終頁に続く

最終頁に続く

(54)【発明の名称】 マルチクラウド制御プレーンアーキテクチャ

(57)【要約】

第1のクラウドインフラストラクチャ内で提供されたサービスおよび／またはリソースが第2のクラウド環境のユーザによって利用されることを可能にする、(第1のクラウドサービスプロバイダによって提供された第1のクラウド環境に含まれている)第1のクラウドインフラストラクチャ内のマルチクラウド制御プレーン(MC CP)を提供するための技術が説明され、第2のクラウド環境は第1のクラウド環境と異なる。マルチクラウドインフラストラクチャは、第2のクラウドサービスプロバイダでのアカウントに関連付けられたユーザが、第2のクラウドインフラストラクチャから、1つまたは複数のクラウドサービスのセットからの第1のサービスを使用することを可能にする。マルチクラウドインフラストラクチャは、ユーザによって第1のサービスを使用することを可能にするために、第2のクラウドサービスプロバイダでのアカウントと第1のクラウドインフラストラクチャ内で作成されたテナンシとの間にリンクを作成する。



【特許請求の範囲】**【請求項 1】**

第 1 のクラウドサービスプロバイダによって提供された第 1 のクラウドインフラストラクチャを使用して、1 つまたは複数のクラウドサービスのセットを提供することと、

前記第 1 のクラウドインフラストラクチャ内で、第 2 のクラウドサービスプロバイダでのアカウントに関連付けられたユーザが、第 2 のクラウドインフラストラクチャから、前記 1 つまたは複数のクラウドサービスのセットからの第 1 のサービスを使用できるようにするマルチクラウドインフラストラクチャを提供することと、

前記ユーザによって前記第 1 のサービスを使用することを可能にするために、前記マルチクラウドインフラストラクチャを使用して、前記第 2 のクラウドサービスプロバイダでの前記アカウントと前記第 1 のクラウドインフラストラクチャ内で作成されたテナンシとの間にリンクを作成することを含む、方法。

10

【請求項 2】

前記第 1 のサービスは、前記第 1 のクラウドインフラストラクチャ内で作成された前記テナンシにデプロイされるデータベースリソースを作成して利用することに対応する、請求項 1 に記載の方法。

【請求項 3】

前記マルチクラウドインフラストラクチャは、クラウドリンクアダプタをホストするマルチクラウド制御プレーン、ネットワークリンクアダプタ、およびアダプタのプールを含み、これらの各々は、前記第 1 のクラウドサービスプロバイダによって提供された前記 1 つまたは複数のクラウドサービスのセット内の特定のサービスに対応する、請求項 1 に記載の方法。

20

【請求項 4】

前記マルチクラウドインフラストラクチャによって、前記第 1 のクラウドサービスプロバイダによって提供された前記第 1 のサービスを利用する要求を受信することをさらに含み、前記要求は、マルチクラウドコンソールから前記マルチクラウドインフラストラクチャに転送され、前記要求は、前記第 2 のクラウドインフラストラクチャ内の前記ユーザの前記アカウントに関連付けられたトークンを含む、請求項 1 に記載の方法。

【請求項 5】

前記マルチクラウドインフラストラクチャによって、前記トークンに基づいて前記第 1 のサービスを利用する前記要求の妥当性を確認することをさらに含み、前記妥当性を確認することは、前記第 2 のクラウドインフラストラクチャ内の前記ユーザに関連付けられたロールを決定することを含む、請求項 4 に記載の方法。

30

【請求項 6】

前記マルチクラウドインフラストラクチャによって、前記リンクに対応するメタデータ情報を格納するデータオブジェクトを生成することをさらに含み、前記メタデータ情報は、前記第 1 のクラウドインフラストラクチャ内に作成された前記テナンシに関連付けられた第 1 の識別子、および前記第 2 のクラウドサービスプロバイダでの前記アカウントに関連付けられた第 2 の識別子のマッピングを含む、請求項 5 に記載の方法。

【請求項 7】

妥当性確認の成功に回答して、前記マルチクラウドインフラストラクチャによって、前記データオブジェクトに関連付けられるリソースプリンシパルを生成することをさらに含む、請求項 6 に記載の方法。

40

【請求項 8】

アダプタのプールに含まれ、前記第 1 のサービスに対応する第 1 のアダプタは、前記リソースプリンシパルを利用して、前記第 1 のクラウドサービスプロバイダによって提供された前記第 1 のサービスを呼び出す、請求項 7 に記載の方法。

【請求項 9】

前記マルチクラウドインフラストラクチャによって、前記第 1 のクラウドインフラストラクチャ内の前記テナンシを、前記第 2 のクラウドインフラストラクチャ内の前記アカウ

50

ントを含んでいる顧客サブスクリプションに相互接続する通信リンクを生成することをさらに含み、前記第1のクラウドインフラストラクチャにデプロイされ、前記第1のサービスに対応するリソースの性能に関連付けられた指標情報は、前記通信リンクを介して、前記第1のクラウドインフラストラクチャから前記第2のクラウドインフラストラクチャに送信される、請求項1に記載の方法。

【請求項10】

前記第1のクラウドインフラストラクチャは前記第2のクラウドインフラストラクチャと異なる、請求項1に記載の方法。

【請求項11】

前記アダプタのプールは、
エクスデータクラウドサービスアダプタ、
自律的データベース共有アダプタ、
自律的データベース専用アダプタ、および
仮想マシンデータベースアダプタを含む、請求項3に記載の方法。

【請求項12】

前記マルチクラウドコンソールは、前記第2のクラウドサービスプロバイダのクラウドポータルに関連付けられたユーザインターフェイスに類似するインターフェイスを含む、請求項4に記載の方法。

【請求項13】

コンピュータ実行可能命令を格納する1つまたは複数のコンピュータ可読非一時的媒体であって、前記コンピュータ実行可能命令は、1つまたは複数のプロセッサによって実行された場合に、

第1のクラウドサービスプロバイダによって提供された第1のクラウドインフラストラクチャを使用して、1つまたは複数のクラウドサービスのセットを提供することと、

前記第1のクラウドインフラストラクチャ内で、第2のクラウドサービスプロバイダでのアカウントに関連付けられたユーザが、第2のクラウドインフラストラクチャから、前記1つまたは複数のクラウドサービスのセットからの第1のサービスを使用できるようにするマルチクラウドインフラストラクチャを提供することと、

前記ユーザによって前記第1のサービスを使用することを可能にするために、前記マルチクラウドインフラストラクチャを使用して、前記第2のクラウドサービスプロバイダでの前記アカウントと前記第1のクラウドインフラストラクチャ内で作成されたテナンシとの間にリンクを作成することとを引き起こす、コンピュータ実行可能命令を格納する1つまたは複数のコンピュータ可読非一時的媒体。

【請求項14】

前記第1のサービスは、前記第1のクラウドインフラストラクチャ内で作成された前記テナンシにデプロイされるデータベースリソースを作成して利用することに対応する、請求項13に記載のコンピュータ実行可能命令を格納する1つまたは複数のコンピュータ可読非一時的媒体。

【請求項15】

前記マルチクラウドインフラストラクチャは、クラウドリンクアダプタをホストするマルチクラウド制御プレーン、ネットワークリンクアダプタ、およびアダプタのプールを含み、これらの各々は、前記第1のクラウドサービスプロバイダによって提供された前記1つまたは複数のクラウドサービスのセット内の特定のサービスに対応する、請求項13に記載のコンピュータ実行可能命令を格納する1つまたは複数のコンピュータ可読非一時的媒体。

【請求項16】

1つまたは複数のプロセッサによって実行された場合に、

前記マルチクラウドインフラストラクチャによって、前記第1のクラウドサービスプロバイダによって提供された前記第1のサービスを利用する要求を受信することを引き起こす命令をさらに含み、前記要求は、マルチクラウドコンソールから前記マルチクラウドイ

10

20

30

40

50

ンフラストラクチャに転送され、前記要求は、前記第 2 のクラウドインフラストラクチャ内の前記ユーザの前記アカウントに関連付けられたトークンを含む、請求項 13 に記載のコンピュータ実行可能命令を格納する 1 つまたは複数のコンピュータ可読非一時的媒体。

【請求項 17】

1 つまたは複数のプロセッサによって実行された場合に、

前記マルチクラウドインフラストラクチャによって、前記トークンに基づいて前記第 1 のサービスを利用する前記要求の妥当性を確認することを引き起こす命令をさらに含み、前記妥当性を確認することは、前記第 2 のクラウドインフラストラクチャ内の前記ユーザに関連付けられたロールを決定することを含む、請求項 16 に記載のコンピュータ実行可能命令を格納する 1 つまたは複数のコンピュータ可読非一時的媒体。

10

【請求項 18】

1 つまたは複数のプロセッサによって実行された場合に、

前記マルチクラウドインフラストラクチャによって、前記リンクに対応するメタデータ情報を格納するデータオブジェクトを生成することを引き起こす命令をさらに含み、前記メタデータ情報は、前記第 1 のクラウドインフラストラクチャ内に作成された前記テナンシに関連付けられた第 1 の識別子、および前記第 2 のクラウドサービスプロバイダでの前記アカウントに関連付けられた第 2 の識別子のマッピングを含む、請求項 17 に記載のコンピュータ実行可能命令を格納する 1 つまたは複数のコンピュータ可読非一時的媒体。

【請求項 19】

1 つまたは複数のプロセッサによって実行された場合に、

妥当性確認の成功に応答して、前記マルチクラウドインフラストラクチャによって、前記データオブジェクトに関連付けられるリソースプリンシパルを生成することを引き起こす命令をさらに含み、アダプタのプールに含まれ、前記第 1 のサービスに対応する第 1 のアダプタは、前記リソースプリンシパルを利用して、前記第 1 のクラウドサービスプロバイダによって提供された前記第 1 のサービスを呼び出す、請求項 18 に記載のコンピュータ実行可能命令を格納する 1 つまたは複数のコンピュータ可読非一時的媒体。

20

【請求項 20】

1 つまたは複数のプロセッサと、

命令を含んでいるメモリとを備えているコンピューティングデバイスであって、前記命令は、前記 1 つまたは複数のプロセッサを使用して実行された場合に、前記コンピューティングデバイスに、少なくとも

30

第 1 のクラウドサービスプロバイダによって提供された第 1 のクラウドインフラストラクチャを使用して、1 つまたは複数のクラウドサービスのセットを提供することと、

前記第 1 のクラウドインフラストラクチャ内で、第 2 のクラウドサービスプロバイダでのアカウントに関連付けられたユーザが、第 2 のクラウドインフラストラクチャから、前記 1 つまたは複数のクラウドサービスのセットからの第 1 のサービスを使用できるようにするマルチクラウドインフラストラクチャを提供することと、

前記ユーザによって前記第 1 のサービスを使用することを可能にするために、前記マルチクラウドインフラストラクチャを使用して、前記第 2 のクラウドサービスプロバイダでの前記アカウントと前記第 1 のクラウドインフラストラクチャ内で作成されたテナンシとの間にリンクを作成することとを実行させる、コンピューティングデバイス。

40

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本出願は、以下の仮出願の各々の非仮出願であり、以下の仮出願の各々の利益を主張する。下に挙げられた仮出願の各々の内容全体は、あらゆる目的で、参照によって本明細書に組み込まれている。

(1) 2022 年 2 月 2 日に出願された米国特許仮出願第 63 / 306, 007 号、

(2) 2022 年 2 月 4 日に出願された米国特許仮出願第 63 / 306, 918 号、

50

(3) 2022年3月18日に出願された米国特許仮出願第63／321,614号、
(4) 2022年4月22日に出願された米国特許仮出願第63／333,965号、
(5) 2022年4月29日に出願された米国特許仮出願第63／336,811号、
(6) 2022年5月6日に出願された米国特許仮出願第63／339,297号、
(7) 2022年6月30日に出願された米国特許仮出願第63／357,541号、および

(8) 2022年7月13日に出願された米国特許仮出願第63／388,925号。

【0002】

分野

本開示は、クラウドアーキテクチャに関し、より詳細には、1つのクラウド環境のユーザが、他のクラウド環境によって提供されたサービスを使用できるように、2つのクラウド環境をリンクするための技術に関する。

【背景技術】

【0003】

背景

ここ数年、クラウドサービスの採用における劇的な増加が見られており、この傾向は増す一方である。さまざまなクラウド環境が、異なるクラウドサービスプロバイダ(CSP: cloud service providers)によって提供されており、各クラウド環境は、一連の1つまたは複数のクラウドサービスを提供する。クラウド環境によって提供される一連のクラウドサービスは、SaaS (Software-as-a-Service) サービス、IaaS (Infrastructure-as-a-Service) サービス、PaaS (Platform-as-a-Service) サービスなどを含むが、これらに限定されない、1つまたは複数の異なる種類のサービスを含んでよい。

【0004】

さまざまなクラウド環境が現在利用可能であるが、各クラウド環境は、閉じたエコシステムを加入している顧客に提供する。その結果、クラウド環境の顧客は、そのクラウド環境によって提供されたサービスを使用することに制限される。CSPによって提供されたクラウド環境に加入している顧客が、そのクラウド環境を介して、異なるCSPによって提供された異なるクラウド環境において提供されているサービスを使用するための簡単な方法はない。本明細書において説明された実施形態は、これらの問題および他の問題に対処する。

【発明の概要】

【課題を解決するための手段】

【0005】

概要

本開示は、一般に、改善されたクラウドアーキテクチャに関し、より詳細には、1つのクラウド環境のユーザが、別の異なるクラウド環境によって提供されたサービスを使用できるように、2つのクラウドをリンクするための技術に関する。本明細書では、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、または命令を格納する非一時的コンピュータ可読ストレージ媒体などを含む、さまざまな実施形態が説明される。一部の実施形態は、コンピュータプログラム／命令を含んでいる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されてよく、これらの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た場合に、プロセッサに、本開示において説明された方法のいずれかを実行させる。

【0006】

本開示の実施形態は、特定のクラウドネットワーク(例えば、Oracleクラウドインフラストラクチャ(OCI: Oracle Cloud Infrastructure))のサービスを他のクラウド上の(例えば、Microsoft Azure内の)ユーザに配信するための機能をプロビジョニングする、マルチクラウド制御プレーン(MCCP: multi-cloud control plane)フレームワークを提供する。MCCPフレームワークは、ユーザのネイティブなクラウド

ド環境のユーザ体験にできるだけ近いユーザ体験を提供しながら、（他のクラウド環境の）ユーザがクラウド環境のサービス（例えば、PaaSサービス）にアクセスすることを可能にする。MCCPの重要な課題は、顧客が、外部クラウド内のサービスの完全なデータプレーン機能を体験できるようになることである。

【0007】

本開示の1つの実施形態は、第1のクラウドサービスプロバイダによって提供された第1のクラウドインフラストラクチャを使用して、1つまたは複数のクラウドサービスのセットを提供することと、第1のクラウドインフラストラクチャ内で、第2のクラウドサービスプロバイダでのアカウントに関連付けられたユーザが、第2のクラウドインフラストラクチャから、1つまたは複数のクラウドサービスのセットからの第1のサービスを使用できるようにするマルチクラウドインフラストラクチャを提供することと、ユーザによって第1のサービスを使用することを可能にするために、マルチクラウドインフラストラクチャを使用して、第2のクラウドサービスプロバイダでのアカウントと第1のクラウドインフラストラクチャ内で作成されたテナンシとの間にリンクを作成することを含む方法を対象にする。

10

【0008】

本開示の態様は、1つまたは複数のデータプロセッサと、命令を含んでいる非一時的コンピュータ可読ストレージ媒体とを備えているコンピューティングデバイスを提供し、これらの命令は、1つまたは複数のデータプロセッサ上で実行された場合に、コンピューティングデバイスに、本明細書において開示された1つまたは複数の方法の一部またはすべてを実行させる。

20

【0009】

本開示の別の態様は、1つまたは複数のデータプロセッサに、本明細書において開示された1つまたは複数の方法の一部またはすべてを実行させるように構成された命令を含む、非一時的機械可読ストレージ媒体において有形に具現化された、コンピュータプログラム製品を提供する。

【0010】

前述の内容は、他の特徴および実施形態と共に、以下の明細書、特許請求の範囲、および添付の図面を参照するときに、さらに明らかになるであろう。

【0011】

本開示の特徴、実施形態、および利点は、添付の図面を参照して以下の詳細な説明が読まれるときに、よりよく理解される。

30

【図面の簡単な説明】

【0012】

【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によってホストされる仮想クラウドネットワーク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の図である。

【図2】ある実施形態による、CSP内の物理ネットワークにおける物理コンポーネントの簡略化されたアーキテクチャ図を示す図である。

【図3】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：network virtualization devices）に接続されるCSP内の例示的な配置を示す図である。

40

【図4】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のI/O仮想化を実現するための、ホストマシンとNVDの間の接続を示す図である。

【図5】ある実施形態による、CSPによって提供された物理ネットワークの簡略化されたブロック図を示す図である。

【図6】ある実施形態による、異なるクラウドサービスプロバイダ（CSP）によって提供された複数のクラウド環境を含んでいる分散環境の簡略化された高レベルの図であり、クラウド環境が、その特定のクラウド環境によって提供された1つまたは複数のクラウドサービスが他のクラウド環境の顧客によって使用されることを可能にする特殊なインフラ

50

ストラクチャを提供する特定のクラウド環境を含む。

【図 7】一部の実施形態による、マルチクラウド制御プレーン（MCCP）の例示的な高レベルのアーキテクチャを示す図である。

【図 8 A】一部の実施形態による、異なるクラウド環境内の 2 つのユーザアカウントをリンクするための例示的なプロセスを示す図である。

【図 8 B】一部の実施形態による、異なるクラウド環境内の 2 つのユーザアカウントをリンクするための例示的なプロセスを示す図である。

【図 9】一部の実施形態による、マルチクラウド制御プレーン（MCCP）のコンポーネントを示す例示的なシステム図を示す図である。

【図 10】一部の実施形態による、マルチクラウドインフラストラクチャによって受信された例示的な要求を示す図である。

【図 11】ある実施形態による、マルチクラウドインフラストラクチャによって実行されるステップを示す例示的なフローチャートを示す図である。

【図 12】少なくとも 1 つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための 1 つのパターンを示すブロック図である。

【図 13】少なくとも 1 つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを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、サービスシステムとしてクラウドインフラストラクチャを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、サービスシステムとしてクラウドインフラストラクチャを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 16】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】

【0013】

詳細な説明

以下の説明では、説明の目的で、ある実施形態を十分に理解できるように、特定の詳細が示されている。しかし、さまざまな実施形態が、それらの特定の詳細なしで実践されてよいということが明らかである。各図および説明は、限定となるよう意図されていない。

「例示的」という単語は、本明細書では「例、事例、または実例としての役割を果たす」ことを意味するために使用される。「例示的」として本明細書に記載されたすべて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、または有利であると解釈されるべきではない。

【0014】

本開示は、一般に、改善されたクラウドアーキテクチャに関し、より詳細には、1 つのクラウド環境のユーザが、別の異なるクラウド環境によって提供されたサービスを使用できるように、2 つのクラウドをリンクするための技術に関する。本明細書では、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、または命令を格納する非一時的コンピュータ可読ストレージ媒体などを含む、さまざまな実施形態が説明される。一部の実施形態は、コンピュータプログラム／命令を含んでいる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されてよく、これらの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た場合に、プロセッサに、本開示において説明された方法のいずれかを実行させる。

【0015】

本開示の実施形態は、特定のクラウドネットワーク（例えば、Oracle クラウドインフラストラクチャ（OCI））のサービスを他のクラウド上の（例えば、Microsoft Azure 内の）ユーザに配信するための機能をプロビジョニングする、マルチクラウド制御プレーン（MCCP）フレームワークを提供する。MCCP フレームワークは、ユーザのネイティブなクラウド環境のユーザ体験にできるだけ近いユーザ体験を提供しながら、（他のクラウド環境の）ユーザがクラウド環境のサービス（例えば、PaaS サービス）にア

10

20

30

40

50

クセスすることを可能にする。MCCPの重要な課題は、顧客が、外部クラウド内のサービスの完全なデータプレーン機能を体験できるようになることである。

【0016】

MCCPは、第2のクラウドインフラストラクチャのユーザ（例えば、Azureユーザ）が、ユーザにとって透過的な方法で、第1のクラウドインフラストラクチャ（例えば、OCI）によって提供されたリソース（例えば、データベースリソース）を利用できるようにする。特に、第1のクラウドインフラストラクチャによって提供されたサービスは、第2のクラウドインフラストラクチャにおける「ネイティブな」サービスのように見える。これによって、第2のクラウドインフラストラクチャの顧客が、第1のクラウドインフラストラクチャによって提供されたサービスにネイティブにアクセスできるようにする。図6～図11を参照して下で説明されるように、MCCPは、外部クラウドユーザ（例えば、第2のクラウドインフラストラクチャのユーザ）によって利用される第1のクラウドインフラストラクチャのリソースを公開する、第1のクラウドインフラストラクチャにおいて実行されるマイクロサービスの集合である。これらのマイクロサービスの各々は、第1のクラウドインフラストラクチャによって提供されたリソースとの通信を提供するプロキシとして機能する。

10

【0017】

クラウドネットワークの例

クラウドサービスという用語は、通常、クラウドサービスプロバイダ（CSP）によって、CSPによって提供された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）を使用しているユーザまたは顧客による利用をオンデマンドで（例えば、サブスクリプションモデルによって）可能にされるサービスのことを指すために使用される。通常、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のサーバおよびシステムから分離している。したがって、顧客は、サービスのための別々のハードウェアリソースおよびソフトウェアリソースを購入することを必要とせず、CSPによって提供された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、加入している顧客に、顧客が、サービスを提供するために使用されるインフラストラクチャの調達に投資することを必要としない、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拡張可能なアクセスを提供するように設計される。

20

【0018】

さまざまな種類のクラウドサービスを提供する、複数のクラウドサービスプロバイダが存在する。SaaS（Software-as-a-Service）、PaaS（Platform-as-a-Service）、IaaS（Infrastructure-as-a-Service）などを含む、クラウドサービスのさまざまな種類またはモデルが存在する。

30

【0019】

顧客は、CSPによって提供された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、企業などの任意の実体であることができる。顧客がCSPによって提供されたサービスに加入または登録するときに、その顧客のテナンシまたはアカウントが作成される。次に、顧客は、そのアカウントによって、アカウントに関連付けられた加入している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。

40

【0020】

前述したように、IaaS（infrastructure as a service）は、クラウドコンピューティングサービスの1つの特定の種類である。IaaSモデルでは、CSPは、顧客自身のカスタマイズ可能なネットワークを構築し、顧客のリソースをデプロイするために顧客によって使用され得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CSP I（cloud services provider infrastructure）と呼ばれる）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によって提供されたインフラストラクチャによって、分散環境内でホストされる。これは、顧客によって提供されたインフラストラクチャによって顧客のリソースおよびネットワークがホストされる従来のコンピューティングと異なっている。

50

【0021】

C S P I は、さまざまなホストマシン、メモリリソース、および基板ネットワークまたはアンダーレイネットワークとも呼ばれる物理ネットワークを形成するネットワークリソースを含む、相互接続された高性能な計算リソースを備えることができる。C S P I におけるリソースは、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ーにわたって分散されてよい。仮想化された分散環境を提供するために、これらの物理的リソースによって仮想化ソフトウェアが実行されてよい。この仮想化は、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ている）を作成する。C S P I 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または仮想ネットワークを物理ネットワークの上に作成するための基盤になる基礎を提供する。物理ネットワーク（または基板ネットワークもしくはアンダーレイネットワーク）は、物理的スイッチ、ルータ、コンピュータ、およびホストマシンなどの、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、物理基板ネットワークの上で動作する論理（または仮想）ネットワークである。特定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、通常、カプセル化技術を使用して、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。仮想ネットワーク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（V C N : virtual cloud network）とも呼ばれる。仮想ネットワークは、物理ネットワークの上で実行され得るネットワーク抽象化のレイヤを作成するために、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（N V D）（例えば、スマートN I C）、トップオブラック（T O R : top-of-rack）スイッチ、N V Dによって実行される1つまたは複数の機能を実施するスマートT O Rによって実施される仮想化機能、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、I P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、通常、レイヤ3 I Pネットワークまたはレイヤ2 V L A Nのいずれかである。仮想ネットワークまたはオーバーレイネットワークのこの方法は、多くの場合、仮想レイヤ3ネットワークまたはオーバーレイレイヤ3ネットワークと呼ばれる。仮想ネットワークのために開発されたプロトコルの例としては、I P - i n - I P（または汎用ルーティングカプセル化（G R E : Generic Routing Encapsulation））仮想拡張可能L A N（V X L A N（Virtual Extensible LAN）- I E T F R F C 7348）、仮想プライベートネットワーク（V P N : Virtual Private Networks）（例えば、M P L Sレイヤ3仮想プライベートネットワーク（R F C 4364））、V M w a r eのN S X、G E N E V E（Generic Network Virtualization Encapsulation：汎用ネットワーク仮想化カプセル化）などが挙げられる。

【0022】

I a a Sの場合、C S Pによって提供されたインフラストラクチャ（C S P I）は、パブリックネットワーク（例えば、インターネット）を経由して仮想化されたコンピューティングリソースを提供するように構成され得る。I a a Sモデルでは、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コンポーネント（例えば、サーバ、ストレージデバイス、ネットワークノード（例えば、ハードウェア）、デプロイメントソフトウェア、プラットフォーム仮想化（例えば、ハイパーバイザレイヤ）など）をホストすることができる。場合によっては、I a a Sプロバイダは、それらのインフラストラクチャコンポーネントに付随して生じるように、さまざまなサービス（例えば、請求書送付、監視、ロギング、セキュリティ、ロードバランシング、およびクラスタ化など）を提供してもよい。したがって、これらのサービスはポリシー主導であることができるため、I a a Sユーザは、ロードバランシングを駆動してアプリケーションの可用性および性能を維持するようにポリシーを実装することができてよい。C S P Iは、顧客が高度に利用可能なホストされた分散環境内で広範囲のアプリケーションおよびサービスを構築して実行できるようにする、インフラストラクチャおよび一連の補完するクラウドサービスを

10

20

30

40

50

提供する。C S P I は、顧客のオンプレミスネットワークからなど、さまざまなネットワーク化された場所から安全にアクセスできる柔軟な仮想ネットワーク内で、高性能な計算リソースおよび計算能力ならびにストレージ容量を提供する。顧客がC S P Iによって提供されたI a a Sサービスに加入または登録するときに、その顧客用に作成されるテナンシは、顧客が自分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、C S P I内の安全で分離されたパーティションである。

【0023】

顧客は、C S P Iによって提供された計算リソース、メモリリソース、およびネットワークリソースを使用して、自分自身の仮想ネットワークを構築することができる。計算インスタンスなどの1つまたは複数の顧客のリソースまたはワークロードが、これらの仮想ネットワークにデプロイされ得る。例えば、顧客は、C S P Iによって提供されたリソースを使用して、仮想クラウドネットワーク（V C N）と呼ばれる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、計算インスタンスなどの1つまたは複数の顧客のリソースを、顧客のV C Nにデプロイすることができる。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、C S P Iは、顧客が高度に利用可能なホストされた仮想環境内で広範囲のアプリケーションおよびサービスを構築して実行できるようにする、インフラストラクチャおよび一連の補完するクラウドサービスを提供する。顧客は、C S P Iによって提供された基盤になる物理的リソースを管理することも制御することもないが、オペレーティングシステム、ストレージ、デプロイされた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、選ばれたネットワークコンポーネント（例えば、ファイアウォール）を限定的に制御することができる。

【0024】

C S Pは、顧客およびネットワーク管理者が、C S P Iリソースを使用してクラウド内でデプロイされたリソースの構成、アクセス、および管理を行うことを可能にする、コンソールを提供してよい。ある実施形態では、このコンソールは、C S P Iにアクセスして管理するために使用され得るW e bベースのユーザインターフェイスを提供する。一部の実装では、コンソールは、C S Pによって提供されたW e bベースのアプリケーションである。

【0025】

C S P Iは、シングルテナンシアーキテクチャまたはマルチテナンシアーキテクチャをサポートしてよい。シングルテナンシアーキテクチャでは、ソフトウェアコンポーネント（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コンポーネント（例えば、ホストマシンまたはサーバ）が、単一の顧客またはテナントのために働く。マルチテナンシアーキテクチャでは、ソフトウェアコンポーネントまたはハードウェアコンポーネントは、複数の顧客またはテナントのために働く。したがって、マルチテナンシアーキテクチャでは、C S P Iリソースは、複数の顧客またはテナント間で共有される。マルチテナンシの状況では、各テナントのデータが分離され、他のテナントには見えないままであることを保証するために、予防策が取られ、C S P I内に予防手段が導入される。

【0026】

物理ネットワークでは、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、接続先のネットワークとの間で通信するコンピューティングデバイスまたはシステムのことを指す。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（L A N：Local Area Network）、広域ネットワーク（W A N：Wide Area Network）、または他の種類の物理ネットワークに接続されてよい。物理ネットワーク内の従来のエンドポイントの例としては、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クデバイス、物理コンピュータ（またはホストマシン）などが挙げられる。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され得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、M A Cアドレス）、固定レイヤ3アドレス（例

例えば、IPアドレス)などであることができる。仮想環境または仮想ネットワークでは、エンドポイントは、物理ネットワークのコンポーネント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、さまざまな仮想エンドポイントを含むことができる。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、ネットワーク管理者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によって)ネットワークエンドポイントに関連付けられたオーバーレイアドレス間を移動できるよう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、仮想ネットワークでは、ネットワーク管理ソフトウェアを使用して、オーバーレイアドレス(例えば、オーバーレイIPアドレス)が1つのエンドポイントから別のエンドポイントに移動され得る。仮想ネットワークが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コンポーネント間の通信は、仮想ネットワークおよび基盤になる物理ネットワークの両方を含む。そのような通信を容易にするために、CSPのコンポーネントは、仮想ネットワーク内のオーバーレイアドレスを基板ネットワーク内の実際の物理アドレスに、およびその逆に、マッピングするマッピングを学習して格納するように構成される。その後、これらのマッピングは、通信を容易にするために使用される。顧客トラフィックは、仮想ネットワーク内のルーティングを容易にするためにカプセル化される。

10

20

【0027】

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コンポーネントに関連付けられ、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、仮想ネットワークまたはオーバーレイネットワーク内の実体に関連付けられる。物理IPアドレスは、基板ネットワーク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)に関連付けられたIPアドレスである。例えば、各NVは、関連付けられた物理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に関連付けられるなど、オーバーレイネットワーク内の実体に関連付けられたオーバーレイアドレスである。自分自身のプライベートVCNを各々有する2つの異なる顧客またはテナントは、互いについての知識を何も持たずに、それらのVCN内で同じオーバーレイIPアドレスを使用できる可能性がある。物理IPアドレスおよびオーバーレイIPアドレスは、両方とも、実IPアドレスの種類である。これらのIPアドレスは、仮想IPアドレスとは別に存在する。仮想IPアドレスは、通常、複数の実IPアドレスを表すか、または複数の実IPアドレスにマッピングされる、単一のIPアドレスである。仮想IPアドレスは、仮想IPアドレスと複数の実IPアドレスの間の1対多のマッピングを提供する。例えば、ロードバランサは、VIPを使用して、複数のサーバにマッピングされるか、または複数のサーバを表してよく、各サーバは、それ自身の実IPアドレスを有する。

30

【0028】

クラウドインフラストラクチャまたはCSPは、世界中の1つまたは複数のリージョンの1つまたは複数のデータセンター内で、物理的にホストされる。CSPは、物理ネットワークまたは基板ネットワーク内のコンポーネント、および物理ネットワークのコンポーネントの上に構築された仮想ネットワーク内にある仮想コンポーネント(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)を含んでよい。ある実施形態では、CSPは、レルム、リージョン、および可用性ドメイン内で編成され、ホストされる。リージョンは、通常、1つまたは複数のデータセンターを含む局所的な地理的領域である。リージョンは、一般に、互いに独立しており、例えば、複数の国または大陸にわたる広大な距離によって分離され得る。例えば、第1のリージョンがオーストラリアにあってよく、別のリージョンが日本にあってよく、さらに別のリージョンがインドにあってよく、などである。各リージョンがCSPリソースのそのリージョン自体の独立したサブセ

40

50

ットを含むように、C S P Eリソースがリージョン間で分割される。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）、ネットワークリソース（例えば、仮想クラウドネットワーク（V C N）、ロードバランシングリソース、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、エッジネットワークリソース（例えば、D N S）、ならびにアクセス管理および監視リソースなどの、一連のコアインフラストラクチャサービスおよびリソースを提供してよい。各リージョンは、一般に、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。

【0029】

近くのリソースを使用することが、遠いリソースを使用することよりも高速であるため、一般にアプリケーションは、そのアプリケーションが最も頻繁に使用されるリージョン内でデプロイされる（すなわち、そのリージョンに関連付けられたインフラストラクチャにデプロイされる）。アプリケーションは、大きい気象系または地震などのリージョン全体のイベントのリスクを軽減すること、法律管轄区域、税領域に関する変化する要件、および他のビジネス上の基準または社会的基準を満たすことなどのための冗長性などの、さまざまな理由で、異なるリージョン内でデプロイされることも可能である。

【0030】

リージョン内のデータセンターは、可用性ドメイン（A D : availability domains）にさらに編成されて細分化され得る。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ーに対応してよい。リージョンは、1つまたは複数の可用性ドメインで構成され得る。そのような分散環境では、C S P Eリソースは、仮想クラウドネットワーク（V C N）など、リージョンに固有であるか、または計算インスタンスなど、可用性ドメインに固有である。

【0031】

リージョン内のA Dは、互いに分離され、故障耐性があり、同時に故障する可能性が極めて低くなるように構成される。これは、リージョン内の1つのA Dでの故障が同じリージョン内の他のA Dの可用性に影響を与える可能性が低くなるように、ネットワーク、物理ケーブル、ケーブル経路、ケーブルエントリポイントなどの重要なインフラストラクチャリソースを共有しないA Dによって実現される。同じリージョン内のA Dは、高可用性接続を他のネットワーク（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）に提供すること、ならびに高可用性および災害復旧の両方のために複数のA D内に複製されたシステムを構築することを可能にする、待ち時間の短い高帯域幅ネットワークによって互いに接続されてよい。クラウドサービスは、複数のA Dを使用して高可用性を保証し、リソースの故障に対して保護する。I a a Sプロバイダによって提供されたインフラストラクチャが増大するにつれて、追加の能力を有するより多くのリージョンおよびA Dが追加されてよい。可用性ドメイン間のトラフィックは、通常、暗号化される。

【0032】

ある実施形態では、リージョンは、レルムにグループ化される。レルムは、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、どのデータも共有しない。同じレルム内のリージョンは、互いに通信してよいが、異なるレルム内のリージョンは通信することができない。顧客のテナンシまたはアカウントは、C S Pと共に、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され得る。通常、顧客がI a a Sサービスに加入するときに、レルム内の顧客によって指定されたリージョン（「ホーム」リージョンと呼ばれる）内に、その顧客用のテナンシまたはアカウントが作成される。顧客は、レルム内の1つまたは複数の他のリージョンにわたって顧客のテナンシを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はないリージョンにアクセスすることができない。

【0033】

I a a S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

10

20

30

40

50

ユーザの特定のセットの要求に応じる。例えば、商用レームは、商業の顧客に提供されてよい。別の例として、レームは、ある国の中の顧客のために、その特定の国に提供されてよい。さらに別の例として、政府レームが政府などに提供されてよい。例えば、政府レームは、特定の政府の要求に応じてよく、商用レームより高度なセキュリティを有してよい。例えば、Oracleクラウドインフラストラクチャ（OCI）は、商用リージョンのためのレームおよび政府クラウドリージョンのための（例えば、FedRAMP認定およびIL5認定の）2つのレームを現在提供している。

【0034】

ある実施形態では、ADは、1つまたは複数の障害ドメインに細分化され得る。障害ドメインは、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である。障害ドメインは、複数の計算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存在しないように、計算インスタンスの分散を可能にする。この分散は、アンチアフィニティとして知られている。障害ドメインは、単一障害点を共有するハードウェアコンポーネント（コンピュータ、スイッチなど）のセットのことを指す。計算プールが、障害ドメインに論理的に分割される。そのため、1つの障害ドメインに影響を与えるハードウェア故障または計算ハードウェアの保守イベントが、他の障害ドメイン内のインスタンスに影響を与えない。実施形態に応じて、ADごとの障害ドメインの数は変わってよい。例えば、ある実施形態では、各ADは3つの障害ドメインを含む。障害ドメインは、AD内の論理データセンターとして機能する。

【0035】

顧客がIaaSサービスに加入するときに、CSPからのリソースが、顧客のためにプロビジョニングされ、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ニング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、リソースをこれらのネットワークにデプロイすることができる。CSPによってクラウド内でホストされている顧客のネットワークは、仮想クラウドネットワーク（VCN）と呼ばれる。顧客は、顧客に割り当てられているCSP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）を設定することができる。VCNは、仮想プライベートネットワークまたはソフトウェア定義プライベートネットワークである。顧客のVCN内でデプロイされている顧客のリソースは、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むことができる。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、さまざまな顧客のワークロードを表してよい。VCNにデプロイされた計算インスタンスは、インターネットなどのパブリックネットワークを経由してパブリックにアクセスできるエンドポイント（「パブリックエンドポイント」と、同じVCNまたは他のVCN（例えば、顧客の他のVCN、または顧客に属していないVCN）内の他のインスタンスと、顧客のオンプレミスのデータセンターまたはネットワークと、ならびにサービスエンドポイントおよび他の種類のエンドポイントと、通信することができる。

【0036】

CSPは、CSPを使用してさまざまなサービスを提供してよい。場合によっては、CSPの顧客は、自分自身がサービスプロバイダのように振る舞い、CSPリソースを使用してサービスを提供してよい。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DNSポート）によって特徴付けられたサービスエンドポイントを公開してよい。顧客のリソース（例えば、計算インスタンス）は、特定のサービスのためにサービスによって公開されたサービスエンドポイントにアクセスすることによって、その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、一般に、インターネットなどのパブリック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たパブリック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できるエンドポイントである。パブリックにアクセスできるネットワークエンドポイントは、パブリックエンドポイントと呼ばれることもある。

【0037】

ある実施形態では、サービスプロバイダは、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呼ばれることがある）を介してサービスを公開してよい。次に、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。ある実装では、サービスのために提供されたサービスエンドポイントは、そのサービスを消費しようとする複数の顧客によってアクセスされ得る。他の実装では、専用サービスエンドポイントが顧客に提供されてよく、その客のみが、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できるようにする。

【0038】

ある実施形態では、VCNが作成されるときに、そのVCNは、VCNに割り当てられているプライベートオーバーレイIPアドレスの範囲（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：Classless Inter-Domain Routing）アドレス空間に関連付けられる。VCNは、関連付けられたサブネット、ルートテーブル、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うちの1つまたは複数あるいはすべてに及ぶことができる。ゲートウェイは、VCNのために構成されている仮想インターフェイスであり、VCNとの間で、VCNの外側の1つまたは複数のエンドポイントへのトラフィックの通信を可能にする。異なる種類のエンドポイントとの間での通信を可能にするために、VCNのための1つまたは複数の異なる種類のゲートウェイが構成されてよい。

【0039】

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され得る。したがって、サブネットは、VCN内で作成され得る構成または細分化の単位である。VCNは、1つまたは複数のサブネットを含むことができる。VCN内の各サブネットは、そのVCN内の他のサブネットと重複しない、VCNのアドレス空間内のアドレス空間サブセットを表す、オーバーレイIPアドレスの連続的な範囲（例えば、10.0.0.0/24および10.0.1.0/24）に関連付けられる。

【0040】

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できるようにする仮想ネットワークインターフェイスカード（VNIC：virtual network interface card）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：Network Interface Card）の論理的表現である。一般に、VNICは、実体（例えば、計算インスタンス、サービス）と仮想ネットワークの間のインターフェイスである。VNICは、サブネットに存在し、1つまたは複数の関連付けられたIPアドレス、および関連付けられたセキュリティルールまたはセキュリティポリシーを有する。VNICは、スイッチ上のレイヤ2ポートと同等である。VNICは、計算インスタンスに接続され、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たVNICは、計算インスタンスが、VCNのサブネットの一部になることを可能にし、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と、VCN内の異なるサブネット内のエンドポイントと、またはVCNの外側のエンドポイントと、通信する（例えば、パケットを送信および受信する）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た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接続する方法を決定する。計算インスタンスのためのVNICは、計算インスタンスが作成されてVCN内のサブネットに追加されるときに、作成されて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んでいるサブネットの場合、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は、計算インスタンスのセット内の1つの計算インスタンスに接続される。

【0041】

各計算インスタンスには、計算インスタンスに関連付けられたVNICを介して、プライベートオーバーレイIPアドレスが割り当てられる。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るときに、計算インスタンスに関連付けられたVNICに割り当てられ、計算インスタンスとの間でトラフィックをルーティングする

ために使用される。特定のサブネット内のすべてのVNICは、同じルートテーブル、セキュリティリスト、およびDHCPオプションを使用する。前述したように、VCN内の各サブネットは、そのVCN内の他のサブネットと重複しない、VCNのアドレス空間内のアドレス空間サブセットを表す、オーバーレイIPアドレスの連続的な範囲（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の場合、VNICに割り当てられているプライベートオーバーレイIPアドレスは、このサブネットに割り当てられたオーバーレイIPアドレスの連続的な範囲からのアドレスである。

【0042】

ある実施形態では、計算インスタンスには、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、パブリックサブネット内である場合、1つまたは複数のパブリックIPアドレスなどの、追加のオーバーレイIPアドレスが割り当てられてよい。これらの複数のアドレスは、同じVNICに割り当てられるか、または計算インスタンスに関連付けられている複数のVNICにわたって割り当てられる。しかし、各インスタンスは、インスタンスの起動中に作成され、インスタンスに割り当てられたプライベートオーバーレイIPアドレスに関連付けられる、プライマリVNICを有し、このプライマリVNICは除去され得ない。セカンダリVNICと呼ばれる追加のVNICが、プライマリ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され得る。すべてのVNICは、インスタンスと同じ可用性ドメイン内にある。セカンダリVNICは、プライマリVNICと同じVCN内のサブネット内、または同じVCN内もしくは異なるVCN内のいずれかにある異なるサブネット内にあることができる。

【0043】

計算インスタンスがパブリックサブネット内にある場合、計算インスタンスには、任意選択的に、パブリックIPアドレスが割り当てられてよい。サブネットが作成されるときに、サブネットは、パブリック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指定され得る。プライベートサブネットは、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たVNICがパブリックオーバーレイIPアドレスを有することができないということを意味する。パブリックサブネットは、サブネット内のリソースおよび関連付けられたVNICがパブリックIPアドレスを有することができるということを意味する。顧客は、単一の可用性ドメイン内に存在するか、またはリージョン内もしくはレルム内の複数の可用性ドメインにわた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。

【0044】

前述したように、VCNは、1つまたは複数のサブネットに細分化されてよい。ある実施形態では、VCNのために構成された仮想ルータ（VR：Virtual Router）（VCN VRまたは単にVRと呼ばれる）が、VCNのサブネット間の通信を可能にする。VCN内のサブネットの場合、VRは、そのサブネットの論理ゲートウェイを表し、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と、およびVCNの外側の他のエンドポイントと、通信できるようにする。VCN VRは、VCN内のVNICとVCNに関連付けられた仮想ゲートウェイ（「ゲートウェイ」）の間のトラフィックをルーティングするように構成された論理的実体である。ゲートウェイは、図1に関して下でさらに説明される。VCN VRは、レイヤ3/IPレイヤの概念である。1つの実施形態では、1つのVCNに対して1つのVCN VRが存在し、VCN VRは、場合によっては、IPアドレスによってアドレス指定される無制限の数のポートを有し、VCNのサブネットごとに1つのポートがある。このようにして、VCN VRは、VCN VRが接続されたVCN内のサブネットごとに異なるIPアドレスを有する。VRは、VCNのために構成されたさまざまなゲートウェイにも接続される。ある実施形態では、サブネットのオーバーレイIPアドレス範囲からの特定のオーバーレイIPアドレスが、そのサブネットのVCN VRのポートのために予約されている。例えば、関連付けられたアドレス範囲10.0/16および10.1/16

をそれぞれ有する2つのサブネットを含んでいるVCNについて考える。アドレス範囲10.0/16を有するVCN内の第1のサブネットの場合、この範囲からのアドレスが、そのサブネットのVCN VRのポートのために予約されている。場合によっては、この範囲からの最初のIPアドレスが、VCN VRのために予約されてよい。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の場合、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てよい。アドレス範囲10.1/16を有する同じVCN内の第2のサブネットの場合、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てよい。VCN VRは、VCN内のサブネットの各々について、異なるIPアドレスを有する。

【0045】

一部の他の実施形態では、VCN内の各サブネットは、VRに関連付けられた予約されたIPアドレス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、それ自体に関連付けられたVRを含んでよい。予約されたIPアドレス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たIPアドレスの範囲からの最初のIPアドレスであってよい。サブネット内のVNICは、このデフォルトのIPアドレスまたは予約されたIPアドレスを使用して、サブネットに関連付けられたVRと通信する（例えば、パケットを送信および受信する）ことができる。そのような実施形態では、VRは、そのサブネットの入口／出口ポイントである。VCN内のサブネットに関連付けられたVRは、VCN内の他のサブネットに関連付けられた他のVRと通信することができる。VRは、VCNに関連付けられたゲートウェイと通信することもできる。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上で動作しているか、または1つまたは複数のNVDによって実行される。

【0046】

ルートテーブル、セキュリティルール、およびDHCPオプションが、VCNのために構成されてよい。ルートテーブルは、VCNの仮想ルートテーブルであり、ゲートウェイまたは特別に構成されたインスタンスを経由してVCN内のサブネットからVCNの外側の送信先ヘトラフィックをルーティングするためのルールを含む。VCNのルートテーブルは、VCNとの間でパケットが転送／ルーティングされる方法を制御するようにカスタマイズされ得る。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のことを指す。

【0047】

VCNのために構成されたセキュリティルールは、VCNのオーバーレイファイアウォールルールを表す。セキュリティルールは、入口ルールおよび出口ルールを含み、VCN内のインスタンスの内外に許可される（例えば、プロトコルおよびポートに基づく）トラフィックの種類を指定することができる。顧客は、特定のルール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、送信元CIDR0.0.0.0/0および送信先TCPポート22を含むステートフル入口ルールを設定することによって、任意の位置からインスタンスのセットへの着信SSHトラフィックを許可することができる。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、セキュリティルールが実装され得る。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当てはまるセキュリティルールのセットで構成される。一方、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当てはまるルールを含む。VCNは、デフォルトのセキュリティルールを含むデフォルトのセキュリティリストを備えてよい。VCNのために構成された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。

【0048】

ある実施形態では、VCNの構成情報は、VCN制御プレーンによって決定されて格納される。VCNの構成情報は、例えば、VCNに関連付けられたアドレス範囲に関する情

10

20

30

40

50

報、V C N内のサブネットおよび関連付けられた情報、V C Nに関連付けられた1つまたは複数のV R、V C N内の計算インスタンスおよび関連付けられたV N I C、V C Nに関連付けられたさまざまな仮想化ネットワーク機能を実行するN V D（例えば、V N I C、V R、ゲートウェイ）、V C Nの状態情報、ならびに他のV C Nに関連する情報を含んでよい。ある実施形態では、V C N配布サービスが、V C N制御プレーンまたはその一部によって格納された構成情報をN V Dに公開する。配布された情報は、パケットをV C N内の計算インスタンスとの間で転送するためにN V Dによって格納されて使用される情報（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されてよい。

【0049】

ある実施形態では、V C Nおよびサブネットの作成は、V C N制御プレーン（C P：C ontrol Plane）によって処理され、計算インスタンスの起動は、計算制御プレーンによって処理される。計算制御プレーンは、物理的リソースを計算インスタンスに割り当てる役割を担い、その後、V C N制御プレーンを呼び出してV N I Cを作成し、計算インスタンスに接続する。V C N C Pは、V C Nデータマッピングも、パケット転送およびルーティング機能を実行するように構成されたV C Nデータプレーンに送信する。ある実施形態では、V C N C Pは、更新をV C Nデータプレーンに提供する役割を担う配布サービスを提供する。V C N制御プレーンの例が、図6、図7、図8、および図9にも示されており（参照番号616、716、816、および916を参照）、下で説明される。

【0050】

顧客は、C S P Iによってホストされたリソースを使用して、1つまたは複数のV C Nを作成してよい。顧客のV C Nにデプロイされた計算インスタンスは、さまざまなエンドポイントと通信してよい。これらのエンドポイントは、C S P Iによってホストされているエンドポイント、およびC S P Iの外側のエンドポイントを含むことができる。

【0051】

C S P Iを使用してクラウドベースのサービスを実装するためのさまざまな異なるアーキテクチャが、図1、図2、図3、図4、図5、および図12～図16に示されており、下で説明される。図1は、ある実施形態によるC S P IによってホストされたオーバーレイV C Nまたは顧客のV C Nを示す分散環境100の高レベルの図である。図1に示された分散環境は、オーバーレイネットワーク内に複数のコンポーネントを含む。図1に示された分散環境100は、単に例であり、主張される実施形態の範囲を過度に限定するよう意図されていない。多くの変形、代替手段、および変更が可能である。例えば、一部の実装では、図1に示された分散環境は、図1に示されたシステムまたはコンポーネントより多いか、または少ないシステムまたはコンポーネントを含んでよく、2つ以上のサブシステムを組み合わせてよく、またはシステムの異なる構成もしくは配置を含んでよい。

【0052】

図1に示された例に示されているように、分散環境100は、顧客が加入し、自分の仮想クラウドネットワーク（V C N）を構築するために使用できるサービスおよびリソースを提供するC S P I 101を含む。ある実施形態では、C S P I 101は、I a a Sサービスを加入している顧客に提供する。C S P I 101内のデータセンターは、1つまたは複数のリージョンに編成されてよい。1つの例示的なリージョン「リージョンUS」102が、図1に示されている。顧客は、リージョン102に関して、Oracle International Corporationの顧客のV C Nを構成している。顧客は、さまざまな計算インスタンスをV C N 104にデプロイしてよく、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んでよい。インスタンスの例としては、アプリケーション、データベース、ロードバランサなどが挙げられる。

【0053】

図1に示された実施形態では、顧客のV C N 104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、各サブネットは、それ自体のC I D R I Pアドレス範囲を有する。図1では、サブネット1のオーバーレイI Pアドレス範囲が10.0/16であり、サブネット2のアドレス範囲が10.1/16である。V C N仮

10

20

30

40

50

想ルータ105は、VCN104のサブネット間および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 VR105は、VCN104内のVNICとVCN104に関連付けられたゲートウェイの間のトラフィックをルーティングするように構成される。VCN VR105は、VCN104のサブネットごとにポートを提供する。例えば、VR105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してよい。

【0054】

複数の計算インスタンスが各サブネットにデプロイされてよく、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であることができる。サブネット内の計算インスタンスは、CSP101内の1つまたは複数のホストマシンによってホストされてよい。計算インスタンスは、計算インスタンスに関連付けられたVNICを介してサブネットに参加する。例えば、図1に示されているように、計算インスタンスC1は、この計算インスタンスに関連付けられたVNICを介してサブネット1の一部になる。同様に、計算インスタンスC2は、C2に関連付けられたVNICを介してサブネット1の一部になる。同様の方法で、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ってよい複数の計算インスタンスが、サブネット1の一部になってよい。各計算インスタンスには、それに関連付けられたVNICを介して、プライベートオーバーレイIPアドレスおよびMACアドレスが割り当てられる。例えば、図1では、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 VR105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 VR105へのデフォルトのルートを有する。

【0055】

サブネット2には、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がデプロイされ得る。例えば、図1に示されているように、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たVNICを介してサブネット2の一部になる。図1に示された実施形態では、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 VR105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 VR105へのデフォルトのルートを有する。

【0056】

VCN A104は、1つまたは複数のロードバランサを含んでもよい。例えば、ロードバランサは、サブネットに提供されてよく、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ロードバランスするように構成されてよい。ロードバランサは、VCN内の複数のサブネットにわたってトラフィックをロードバランスするために提供されてもよい。

【0057】

VCN104にデプロイされた特定の計算インスタンスは、さまざまな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、CSP200によってホストされているエンドポイント、およびCSP200の外側のエンドポイントを含んでよい。CSP101によってホストされてい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）、

10

20

30

40

50

同じリージョン内の異なるV C N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106または110内のV C N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110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V C N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108内のV C N内のエンドポイントとの間の通信）を含んでよい。C S P I 101によってホストされたサブネット内の計算インスタンスは、C S P I 101によってホストされていない（すなわち、C S P I 101の外側にある）エンドポイントと通信してもよい。これらの外側のエンドポイントは、顧客のオンプレミスネットワーク116内のエンドポイント、他のリモートクラウドによってホストされたネットワーク118内のエンドポイント、インターネットなどのパブリックネットワークを介してアクセス可能なパブリックエンドポイント114、および他のエンドポイントを含む。

10

【0058】

同じサブネット上の計算インスタンス間の通信は、送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたV N I Cを使用して容易にされる。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にパケットを送信したいことがある。送信元計算インスタンスから発生し、送信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の場合、パケットは、送信元計算インスタンスに関連付けられたV N I Cによって最初に処理される。送信元計算インスタンスに関連付けられたV N I Cによって実行される処理は、パケットヘッダーからパケットの送信先情報を決定すること、送信元計算インスタンスに関連付けられたV N I Cのために構成された任意のポリシー（例えば、セキュリティリスト）を識別すること、パケットのネクストホップを決定すること、必要に応じて任意のパケットカプセル化／カプセル解除機能を実行すること、およびその後、意図された送信先とのパケットの通信を容易にすることを目的に、パケットをネクストホップに転送／ルーティングすることを含むことができる。送信先計算インスタンスが送信元計算インスタンスと同じサブネット内にある場合、送信元計算インスタンスに関連付けられたV N I Cは、送信先計算インスタンスに関連付けられたV N I Cを識別し、パケットを処理するためにそのV N I Cに転送するように構成される。次に、送信先計算インスタンスに関連付けられたV N I Cが実行され、パケットを送信先計算インスタンスに転送する。

20

30

【0059】

サブネット内の計算インスタンスから同じV C N内の異なるサブネット内のエンドポイントに伝達されるパケットの場合、この通信は、送信元および送信先計算インスタンスに関連付けられたV N I CならびにV C N V Rによって容易にされる。例えば、図1のサブネット1内の計算インスタンスC1が、パケットをサブネット2内の計算インスタンスD1に送信したい場合、このパケットは、計算インスタンスC1に関連付けられたV N I Cによって最初に処理される。計算インスタンスC1に関連付けられたV N I Cは、V C N V Rのデフォルトのルートまたはポート10.0.0.1を使用してパケットをV C N V R105にルーティングするように構成される。V C N V R105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る。次に、D1に関連付けられたV N I Cによってパケットが受信されて処理され、V N I Cは、パケットを計算インスタンスD1に転送する。

40

【0060】

V C N104内の計算インスタンスからV C N104の外側にあるエンドポイントに伝達されるパケットのために、送信元計算インスタンスに関連付けられたV N I C、V C N V R105、およびV C N104に関連付けられたゲートウェイによって、通信が容易にされる。1つまたは複数の種類のゲートウェイが、V C N104に関連付けられてよい。ゲートウェイは、V C Nと別のエンドポイントの間のインターフェイスであり、別のエンドポイントはV C Nの外側にある。ゲートウェイは、レイヤ3／I Pレイヤの概念であり、V C NがV C N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

50

ートウェイは、V C Nと他のV C Nまたはネットワークとの間のトラフィックフローを容易にする。さまざまな種類のゲートウェイが、さまざまな種類のエンドポイントとのさまざまな種類の通信を容易にするように、V C Nのために構成されてよい。ゲートウェイに応じて、通信は、パブリックネットワーク（例えば、インターネット）を経由するか、またはプライベートネットワークを経由してよい。さまざまな通信プロトコルが、これらの通信に使用されてよい。

【0061】

例えば、計算インスタンスC 1は、V C N 1 0 4の外側のエンドポイントと通信したいことがある。送信元計算インスタンスC 1に関連付けられたV N I Cによって、パケットが最初に処理されてよい。このV N I Cの処理は、パケットの送信先がC 1のサブネット1の外側にあるということを決断する。C 1に関連付けられたV N I Cは、パケットをV C N 1 0 4のV C N V R 1 0 5に転送してよい。次にV C N V R 1 0 5は、パケットを処理し、この処理の一部として、パケットの送信先に基づいて、パケットのネクストホップとして、V C N 1 0 4に関連付けられた特定のゲートウェイを決断する。その後、V C N V R 1 0 5は、パケットを特定の識別されたゲートウェイに転送してよい。例えば、送信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、V C N V R 1 0 5によってパケットが、V C N 1 0 4のために構成されたダイナミックルーティングゲートウェイ（D R G : Dynamic Routing Gateway）ゲートウェイ1 2 2に転送されてよい。次に、パケットは、最終的な意図された送信先へのパケットの伝達を容易にするために、ゲートウェイからネクストホップに転送されてよい。

【0062】

さまざまな種類のゲートウェイが、V C Nのために構成されてよい。V C Nのために構成され得るゲートウェイの例が、図1に示されており、下で説明される。V C Nに関連付けられたゲートウェイの例は、図1 2、図1 3、図1 4、および図1 5（例えば、参照番号1 2 3 4、1 2 3 6、1 2 3 8、1 3 3 4、1 3 3 6、1 3 3 8、1 4 3 4、1 4 3 6、1 4 3 8、1 5 3 4、1 5 3 6、および1 5 3 8によって参照されるゲートウェイ）にも示されており、下で説明される。図1に示された実施形態に示されているように、ダイナミックルーティングゲートウェイ（D R G）1 2 2は、顧客のV C N 1 0 4に追加されるか、または関連付けられてよく、顧客のV C N 1 0 4と別のエンドポイント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、この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1 1 6、C S P I 1 0 1の異なるリージョン内のV C N 1 0 8、またはC S P I 1 0 1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1 1 8であることができる。顧客のオンプレミスネットワーク1 1 6は、顧客のリソースを使用して構築された顧客のネットワークまたは顧客のデータセンターであってよい。顧客のオンプレミスネットワーク1 1 6へのアクセスは、通常、極めて制限される。顧客のオンプレミスネットワーク1 1 6、およびC S P I 1 0 1によってクラウド内でデプロイまたはホストされた1つまたは複数のV C N 1 0 4の両方を有する顧客の場合、顧客は、顧客のオンプレミスネットワーク1 1 6および顧客のクラウドベースのV C N 1 0 4が互いに通信できることを望むことがある。これによって、顧客が、C S P I 1 0 1によってホストされた顧客のV C N 1 0 4および顧客のオンプレミスネットワーク1 1 6を包含する拡張されたハイブリッド環境を構築することを可能にする。D R G 1 2 2は、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、通信チャンネル1 2 4が設定され、このチャンネルの1つのエンドポイントが、顧客のオンプレミスネットワーク1 1 6内にあり、他のエンドポイントが、C S P I 1 0 1内にあり、顧客のV C N 1 0 4に接続される。通信チャンネル1 2 4は、インターネットなどのパブリック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経由することができる。インターネットなどのパブリック通信ネットワークを経由するI P s e c V P N技術、パブリック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、さまざまな通信プロトコルが使用されてよい。通信チャンネル1 2 4の1つのエンドポイントを形成する顧客のオンプレミスネットワーク1 1 6内のデバイスまたは機器は、図1に示

されたCPE126などの、加入者宅内機器（CPE：customer premise equipment）と呼ばれる。CSP101側では、エンドポイントは、DRG122を実行するホストマシンであってよい。

【0063】

ある実施形態では、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を可能にする、リモートピアリング接続（RPC：Remote Peering Connection）がDRGに追加され得る。そのようなRPCを使用すると、顧客のVCN104は、DRG122を使用して、別のリージョン内のVCN108と接続することができる。DRG122は、Microsoft Azureクラウド、Amazon AWSクラウドなどの、CSP101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118と通信するために使用されてもよい。

10

【0064】

図1に示されているように、VCN104上の計算インスタンスが、インターネットなどのパブリックネットワークを経由してアクセス可能なパブリックエンドポイント114と通信することを可能にするインターネットゲートウェイ（IGW：Internet Gateway）120が、顧客のVCN104のために構成されてよい。IGW120は、VCNをインターネットなどのパブリックネットワークに接続するゲートウェイである。IGW120は、VCN104などのVCN内のパブリックサブネット（パブリックサブネット内のリソースは、パブリックオーバーレイIPアドレスを有する）の、インターネットなどのパブリックネットワーク114上のパブリックエンドポイント112への直接アクセスを可能にする。IGW120を使用して、VCN104内のサブネットから、またはインターネットから、接続が開始され得る。

20

【0065】

ネットワークアドレス変換（NAT：Network Address Translation）ゲートウェイ128が、顧客のVCN104のために構成され、専用パブリックオーバーレイIPアドレスを有さない顧客のVCN内のクラウドリソースのインターネットへのアクセスを可能にし、ネットワークアドレス変換ゲートウェイ128は、それらのリソースを直接着信インターネット接続（例えば、L4-L7接続）に公開せずに、そのようなアクセスを可能にする。これによって、VCN104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の、インターネット上のパブリックエンドポイントへのプライベートアクセスを可能にする。NATゲートウェイでは、プライベートサブネットからパブリックインターネットへの接続のみが開始されることが可能であり、インターネットからプライベートサブネットへの接続は開始され得ない。

30

【0066】

ある実施形態では、サービスゲートウェイ（SGW：Service Gateway）126が、顧客のVCN104のために構成されることが可能であり、VCN104とサービスネットワーク110内のサポートされているサービスエンドポイント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。ある実施形態では、サービスネットワーク110は、CSPによって提供されてよく、さまざまなサービスを提供してよい。そのようなサービスネットワークの例は、顧客によって使用され得るさまざまなサービスを提供するOracleのServices Networkである。例えば、顧客のVCN104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、パブリックIPアドレスもインターネットへのアクセスも必要とせずに、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。ある実施形態では、VCNは、1つのみのSGWを含むことができ、接続は、VCN内のサブネットのみから開始されることが可能であり、サービスネットワーク110からは開始され得ない。VCNが別のVCNとピアリングされた場合、通常、他のVCN内のリソースは、SGWにアクセスできない。FastConnectまたはVPN接続を使用してVCNに接続されているオンプレミスネットワーク内のリソースは、そのVCNのために構成されたサービスゲートウェイを使用することもできる。

40

50

【0067】

ある実装では、SGW126は、対象のサービスまたはサービスのグループのすべてのリージョンのパブリック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ルーティング（CIDR）ラベルの概念を使用する。顧客は、サービスへのトラフィックを制御するようにSGWおよび関連するルートルールを構成するときに、サービスCIDRラベルを使用する。顧客は、任意選択的に、セキュリティルールを構成するときに、サービスCIDRラベルを利用することができ、将来、サービスのパブリックIPアドレスが変化する場合に、それらのセキュリティルールを調整する必要がない。

【0068】

ローカルピアリングゲートウェイ（LPG：Local Peering Gateway）132は、顧客のVCN104に追加され得るゲートウェイであり、VCN104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。ピアリングは、トラフィックがインターネットなどのパブリックネットワークを横断せず、または顧客のオンプレミスネットワーク116を通してトラフィックをルーティングすることもなく、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。好ましい実施形態では、VCNは、確立するピアリングごとに別々のLPGを含む。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間で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方法である。

【0069】

サービスネットワーク110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、さまざまな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してよい。パブリック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パブリックネットワークを介して顧客の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、およびまたはSGW126を介してプライベートにアクセス可能であってよい、パブリックエンドポイントとして公開されてよい。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。このアクセスは、プライベートエンドポイント（PE：Private Endpoint）アクセスと呼ばれ、サービスプロバイダがサービスを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公開することを可能にする。プライベートエンドポイントのリソースは、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たサブネット内のVNIC（1つまたは複数のプライベートIPを有するPE-VNICと呼ばれる）として現れる。したがって、PEは、VNICを使用して、プライベートな顧客のVCNのサブネット内のサービスを提示するための方法を提供する。エンドポイントがVNICとして公開されるため、ルーティングルール、セキュリティリストなどの、VNICに関連付けられたすべての特徴は、PE-VNICに使用可能になっている。

【0070】

サービスプロバイダは、PEを介してアクセスを可能にするために、サービスを登録することができる。プロバイダは、サービスの可視性を顧客のテナンシに制限するポリシーを、サービスに関連付けることができる。プロバイダは、特にマルチテナントサービスの場合、単一の仮想IPアドレス（VIP：virtual IP address）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VCN内の）複数のそのようなプライベートエンドポイントが存在してよい。

【0071】

次に、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のDNS名を使用してサービスにアクセスすることができる。顧客のVCN内の計算インスタンスは、トラフィックを顧客のVCN内のPEのプライベートIPアドレスに送信することによって、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：Private Access Gateway）130は、サービスプロバイダのVCN（例えば、サービスネットワーク110内のVCN）に接

続され得るゲートウェイリソースであり、顧客のサブネットのプライベートエンドポイントとの間のすべてのトラフィックの入口／出口ポイントとして機能する。PAGW130は、プロバイダが内部のIPアドレスリソースを利用せずにPEの接続数をスケールリングすることを可能にする。プロバイダは、単一のVCN内で登録された任意の数のサービスに対して、1つのPAGWのみを構成する必要がある。プロバイダは、サービスを1人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。顧客の視点からは、PE VNICは、顧客のインスタンスに接続される代わりに、顧客が対話することを望むサービスに接続されているように見える。プライベートエンドポイントに行くトラフィックは、PAGW130を介してサービスにルーティングされる。これらは、顧客－サービス間プライベート接続（C2S（customer-to-service）接続）と呼ばれる。

10

【0072】

PEの概念は、トラフィックがFastConnect/IPsecリンクおよび顧客のVCN内のプライベートエンドポイントを通して流れることを可能にすることによって、サービス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ーに拡張するために使用されることも可能である。サービスのプライベートアクセスは、トラフィックがLPG132と顧客のVCN内のPE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に拡張されることも可能である。

【0073】

顧客は、サブネットレベルでVCN内のルーティングを制御することができ、そのため顧客は、VCN104などの顧客のVCN内のど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してVCNから外に出ることを許容されるかどうかを判定するために、VCNのルートテーブルが使用される。例えば、特定の例では、顧客のVCN104内のパブリックサブネットのルートテーブルは、IGW120を介して非ローカルトラフィックを送信してよい。同じ顧客のVCN104内のプライベートサブネットのルートテーブルは、SGW126を介してCSPサービスに行くトラフィックを送信してよい。すべての残りのトラフィックは、NATゲートウェイ128を介して送信されてよい。ルートテーブルは、VCNから出るトラフィックのみを制御する。

20

【0074】

VCNに関連付けられたセキュリティリストは、インバウンド接続を経由してゲートウェイを介してVCNに入るトラフィックを制御するために使用される。サブネット内のすべてのリソースは、同じルート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、およびインスタンスから出ることを許可された特定の種類のトラフィックを制御するために使用されてよい。セキュリティリストルールは、入口（インバウンド）ルールおよび出口（アウトバウンド）ルールを含んでよい。例えば、入口ルールは、許可された送信元アドレス範囲を指定してよく、一方、出口ルールは、許可された送信先アドレス範囲を指定してよい。セキュリティルールは、特定のプロトコル（例えば、TCP、ICMP）、特定のポート（例えば、SSHの場合は22、Windows RDPの場合は3389）などを指定してよい。ある実装では、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ルールと一致する、それ自体のファイアウォールルールを強制してよい。ルールは、ステートフル（例えば、接続が追跡され、応答トラフィックに関する明示的なセキュリティリストルールを使用しないで、応答が自動的に許可される）またはステートレスであってよい。

30

40

【0075】

顧客のVCNからの（すなわち、VCN104にデプロイされたリソースまたは計算インスタンスによる）アクセスは、パブリックアクセス、プライベートアクセス、または専用アクセスとして分類され得る。パブリックアクセスは、パブリックエンドポイントにアクセスするためにパブリックIPアドレスまたはNATが使用されるアクセスモデルのことを指す。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VCN104内

50

の顧客のワークロード（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パブリックネットワークを横断せずにサービスにアクセスすることを可能にする。ある実施形態では、C S P I 1 0 1 は、プライベートIPアドレスを有する顧客のV C Nのワークロードが、サービスゲートウェイを使用してサービス（のパブリック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V C N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パブリック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提供する。

【0076】

さらに、C S P I は、FastConnectパブリックピアリングなどの技術を使用して専用パブリックアクセスを提供してよく、このアクセスでは、顧客の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パブリックネットワークを横断せずに、顧客のV C N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。C S P I は、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提供してもよく、このアクセスでは、プライベートIPアドレスを有する顧客のオンプレミスインスタンスが、FastConnect接続を使用して顧客のV C Nのワークロードにアクセスすることができる。FastConnectは、顧客のオンプレミスネットワークをC S P I およびそのサービスに接続するための、パブリック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、インターネットに基づく接続と比較した場合に、より高い帯域幅の選択肢およびより信頼できる一貫性のあるネットワーク体験を伴う専用のプライベート接続を作成するための、容易で弾力性のある経済的な方法を提供する。

【0077】

図1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内のさまざまな仮想コンポーネントを説明する。前述したように、仮想ネットワークは、基盤になる物理ネットワークまたは基板ネットワークの上に構築される。図2は、ある実施形態に従って、仮想ネットワークのための基盤になるC S P I 2 0 0内の物理ネットワークにおける物理コンポーネントの簡略化されたアーキテクチャ図を示している。図に示されているように、C S P I 2 0 0 は、クラウドサービスプロバイダ（C S P）によって提供されたコンポーネントおよびリソース（例えば、計算リソース、メモリリソース、およびネットワークリソース）を含んでいる分散環境を提供する。これらのコンポーネントおよびリソースは、クラウドサービス（例えば、I a a S サービス）を、加入している顧客、すなわち、C S Pによって提供された1つまたは複数のサービスに加入している顧客に提供するために使用される。顧客が加入したサービスに基づいて、C S P I 2 0 0のリソース（例えば、計算リソース、メモリリソース、およびネットワークリソース）のサブセットが、顧客のためにプロビジョニングされる。次に、顧客は、C S P I 2 0 0によって提供された物理的な計算リソース、メモリリソース、およびネットワークリソースを使用して、自分自身のクラウドベースの（すなわち、C S P Iによってホストされた）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。すでに示されたように、これらの顧客のネットワークは、仮想クラウドネットワーク（V C N）と呼ばれる。顧客は、計算インスタンスなどの1つまたは複数の顧客のリソースを、これらの顧客のV C Nにデプロイすることができる。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であることができる。C S P I 2 0 0 は、顧客が高度に利用可能なホストされた環境内で広範囲のアプリケーションおよびサービスを構築して実行できるようにする、インフラストラクチャおよび一連の補完するクラウドサービスを提供する。

【0078】

図2に示された実施形態例では、C S P I 2 0 0の物理コンポーネントは、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、202、206、208）、ネットワーク仮想化デバイス（N V D）（例えば、210、212）、トップオブブラック（T O R）スイッチ（例えば、214、216）、ならびに物理ネットワーク（例えば、218

）、および物理ネットワーク 218 内のスイッチを含む。物理ホストマシンまたは物理サーバは、V C N の 1 つまたは複数のサブネットに参加するさまざまな計算インスタンスをホストし、実行してよい。計算インスタンスは、仮想マシンインスタンスおよびベアメタルインスタンスを含んでよい。例えば、図 1 に示されたさまざまな計算インスタンスは、図 2 に示された物理ホストマシンによってホストされてよい。V C N 内の仮想マシン計算インスタンスは、1 つのホストマシンによって、または複数の異なるホストマシンによって、実行されてよい。物理ホストマシンは、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してもよい。図 1 に示された V N I C および V C N V R は、図 2 に示された N V D によって実行されてよい。図 1 に示されたゲートウェイは、ホストマシンによって、および／または図 2 に示された N V D によって、実行されてよい。

10

【0079】

ホストマシンまたはサーバは、ホストマシン上の仮想環境を作成して有効化するハイパーバイザ（仮想マシンモニタまたは V M M (virtual machine monitor) と呼ばれる）を実行してよい。仮想化環境または仮想環境は、クラウドベースのコンピューティングを容易にする。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、1 つまたは複数の計算インスタンスが作成、実行、および管理されてよい。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的コンピューティングリソース（例えば、計算リソース、メモリリソース、およびネットワークリソース）が、ホストマシンによって実行されるさまざまな計算インスタンス間で共有されることを可能にする。

【0080】

20

例えば、図 2 に示されているように、ホストマシン 202 および 208 は、ハイパーバイザ 260 および 266 をそれぞれ実行する。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、またはハードウェア、あるいはこれらの組合せを使用して実装されてよい。通常、ハイパーバイザは、ホストマシンのオペレーティングシステム（O S : operating system）の上に存在するプロセスまたはソフトウェアレイヤであり、オペレーティングシステムは、ホストマシンのハードウェアプロセッサ上で実行される。ハイパーバイザは、ホストマシンの物理的コンピューティングリソース（例えば、プロセッサ／コアなどの処理リソース、メモリリソース、ネットワークリソース）が、ホストマシンによって実行されるさまざま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、仮想環境を提供する。例えば、図 2 では、ハイパーバイザ 260 は、ホストマシン 202 の O S の上に存在してよく、ホストマシン 202 のコンピューティングリソース（例えば、処理リソース、メモリリソース、およびネットワークリソース）が、ホストマシン 202 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 O S と同じであるか、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呼ばれる）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るか、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 2 に示されたホストマシンは、同じ種類または異なる種類のハイパーバイザを有してよい。

30

40

【0081】

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であることができる。図 2 では、ホストマシン 202 上の計算インスタンス 268 およびホストマシン 208 上の計算インスタンス 274 は、仮想マシンインスタンスの例である。ホストマシン 206 は、顧客に提供されているベアメタルインスタンスの例である。

【0082】

ある例では、ホストマシン全体が単一の顧客にプロビジョニングされてよく、そのホストマシンによってホストされた 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。他の例では、ホ

50

ストマシンは、複数の顧客（すなわち、複数のテナント）間で共有されてよい。そのようなマルチテナンシの状況では、ホストマシンは、異なる顧客に属する仮想マシン計算インスタンスをホストしてよい。これらの計算インスタンスは、異なる顧客の異なるV C Nのメンバーであってよい。ある実施形態では、ベアメタル計算インスタンスは、ハイパーバイザを有さない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ニングされる場合、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しているホストマシンの物理的C P U、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、ホストマシンが、他の顧客またはテナントと共有されない。

【0083】

前述のように、V C N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V C Nのサブネットのメンバーになることを可能にするV N I Cに関連付けられる。計算インスタンスに関連付けられたV N I Cは、計算インスタンスとの間のパケットまたはフレームの通信を容易にする。V N I Cは、計算インスタンスが作成されるときに、計算インスタンスに関連付けられる。ある実施形態では、ホストマシンによって実行される計算インスタンスの場合、その計算インスタンスに関連付けられたV N I Cが、ホストマシンに接続されたN V Dによって実行される。例えば、図2では、ホストマシン202が、V N I C 276に関連付けられている仮想マシン計算インスタンス268を実行し、V N I C 276が、ホストマシン202に接続されたN V D 210によって実行される。別の例として、ホストマシン206によってホストされたベアメタルインスタンス272が、ホストマシン206に接続されたN V D 212によって実行されるV N I C 280に関連付けられる。さらに別の例として、V N I C 284が、ホストマシン208によって実行される計算インスタンス274に関連付けられ、V N I C 284は、ホストマシン208に接続されたN V D 212によって実行される。

【0084】

ホストマシンによってホストされた計算インスタンスの場合、そのホストマシンに接続されたN V Dは、それらの計算インスタンスがメンバーであるV C Nに対応するV C N V Rも実行する。例えば、図2に示された実施形態では、N V D 210は、計算インスタンス268がメンバーであるV C Nに対応するV C N V R 277を実行する。N V D 212は、ホストマシン206および208によってホストされた計算インスタンスに対応するV C Nに対応する1つまたは複数のV C N V R 283を実行してもよい。

【0085】

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クード（N I C）を含んでよい。ホストマシン上のN I C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（またはインターフェイス）を提供してよい。例えば、ホストマシンは、ホストマシンおよびN V D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N V Dに接続されてよい。ホストマシンは、別のホストマシンなどの他のデバイスに接続されてもよい。

【0086】

例えば、図2では、ホストマシン202は、ホストマシン202のN I C 232によって提供されたポート234とN V D 210のポート236の間に延びるリンク220を使用して、N V D 210に接続される。ホストマシン206は、ホストマシン206のN I C 244によって提供されたポート246とN V D 212のポート248の間に延びるリンク224を使用して、N V D 212に接続される。ホストマシン208は、ホストマシン208のN I C 250によって提供されたポート252とN V D 212のポート254の間に延びるリンク226を使用して、N V D 212に接続される。

【0087】

次に、N V Dは、物理ネットワーク218に接続されている（スイッチファブリックとも呼ばれる）トップオブラック（T O R）スイッチへの通信リンクを介して接続される。ある実施形態では、ホストマシンとN V Dの間およびN V DとT O Rスイッチの間のリン

クは、イーサネット（登録商標）リンクである。例えば、図 2 では、リンク 2 2 8 および 2 3 0 を使用して、NVD 2 1 0 および 2 1 2 が TOR スイッチ 2 1 4 および 2 1 6 にそれぞれ接続される。ある実施形態では、リンク 2 2 0、2 2 4、2 2 6、2 2 8、および 2 3 0 は、イーサネットリンクである。TOR に接続されているホストマシンおよび NVD の集合は、ラックと呼ばれることがある。

【0088】

物理ネットワーク 2 1 8 は、TOR スイッチが互いに通信できるようにする通信ファブリックを提供する。物理ネットワーク 2 1 8 は、多層ネットワークであることができる。ある実装では、物理ネットワーク 2 1 8 は、スイッチの多層 Clos ネットワークであり、TOR スイッチ 2 1 4 および 2 1 6 は、多層のマルチノード物理スイッチングネットワーク 2 1 8 の葉レベルのノードを表す。2 層ネットワーク、3 層ネットワーク、4 層ネットワーク、5 層ネットワーク、および一般に、「n」層ネットワークを含むが、これらに限定されない、さまざまな Clos ネットワーク構成が可能である。Clos ネットワークの例が、図 5 に示されており、下で説明される。

【0089】

ホストマシンと NVD の間で、1 対 1 構成、多対 1 構成、1 対多構成などの、さまざまな接続構成が可能である。1 対 1 構成の実装では、各ホストマシンがそれ自体の別々の NVD に接続される。例えば、図 2 では、ホストマシン 2 0 2 が、ホストマシン 2 0 2 の NIC 2 3 2 を介して NVD 2 1 0 に接続される。多対 1 構成では、複数のホストマシンが 1 つの NVD に接続される。例えば、図 2 では、ホストマシン 2 0 6 および 2 0 8 が、NIC 2 4 4 および 2 5 0 を介して同じ NVD 2 1 2 にそれぞれ接続される。

【0090】

1 対多構成では、1 つのホストマシンが複数の NVD に接続される。図 3 は、ホストマシンが複数の NVD に接続される CSPI 3 0 0 内の例を示している。図 3 に示されているように、ホストマシン 3 0 2 は、複数のポート 3 0 6 および 3 0 8 を含むネットワークインターフェイスカード（NIC）3 0 4 を備える。ホストマシン 3 0 0 は、ポート 3 0 6 およびリンク 3 2 0 を介して第 1 の NVD 3 1 0 に接続され、ポート 3 0 8 およびリンク 3 2 2 を介して第 2 の NVD 3 1 2 に接続される。ポート 3 0 6 および 3 0 8 は、イーサネットポートであってよく、ホストマシン 3 0 2 と NVD 3 1 0 および 3 1 2 の間のリンク 3 2 0 および 3 2 2 は、イーサネットリンクであってよい。次に、NVD 3 1 0 が第 1 の TOR スイッチ 3 1 4 に接続され、NVD 3 1 2 が第 2 の TOR スイッチ 3 1 6 に接続される。NVD 3 1 0 および 3 1 2 と TOR スイッチ 3 1 4 および 3 1 6 の間のリンクは、イーサネットリンクであってよい。TOR スイッチ 3 1 4 および 3 1 6 は、多層物理ネットワーク 3 1 8 内の層 0 のスイッチングデバイスを表す。

【0091】

図 3 に示された配置は、TOR スイッチ 3 1 4 を横断して NVD 3 1 0 を通り、ホストマシン 3 0 2 に向かう第 1 の経路、および TOR スイッチ 3 1 6 を横断して NVD 3 1 2 を通り、ホストマシン 3 0 2 に向かう第 2 の経路という、物理スイッチネットワーク 3 1 8 とホストマシン 3 0 2 の間の 2 つの別々の物理ネットワーク経路を提供する。別々の経路が、ホストマシン 3 0 2 の改善された可用性（高可用性と呼ばれる）をもたらす。経路（例えば、経路のうちの 1 つのリンクが故障する）またはデバイス（例えば、特定の NVD が機能していない）のうちの 1 つに問題がある場合、他の経路がホストマシン 3 0 2 との間の通信に使用されてよい。

【0092】

図 3 に示された構成では、ホストマシンの NIC によって提供された 2 つの異なるポートを使用して、ホストマシンが 2 つの異なる NVD に接続される。他の実施形態では、ホストマシンは、複数の NVD へのホストマシンの接続を可能にする複数の NIC を含んでよい。

【0093】

再び図 2 を参照すると、NVD は、1 つまたは複数のネットワークおよび／またはスト

10

20

30

40

50

レージ仮想化機能を実行する物理デバイスまたはコンポーネントである。NVDは、1つまたは複数の処理ユニット（例えば、CPU、ネットワーク処理ユニット（NPU：Network Processing Units）、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ってよい。NVDの1つまたは複数の処理ユニット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、さまざまな仮想化機能が実行されてよい。

【0094】

NVDは、さまざまな形態で実装されてよい。例えば、ある実施形態では、NVDは、組み込みプロセッサを内蔵するスマートNICまたはインテリジェントNICと呼ばれるインターフェイスカードとして実装される。スマートNICは、ホストマシン上のNICとは別のデバイスである。図2では、NVD210および212は、ホストマシン202、ならびにホストマシン206および208にそれぞれ接続されたスマートNICとして実装されてよい。

【0095】

しかし、スマートNICは、NVDの実装の単に1つの例である。さまざまな他の実装が可能である。例えば、一部の他の実装では、NVDまたはNVDによって実行される1つまたは複数の機能は、1つまたは複数のホストマシン、1つまたは複数のTORスイッチ、およびCSP1200の他のコンポーネントに組み込まれるか、またはこれらによって実行されてよい。例えば、NVDはホストマシンにおいて具現化されてよく、NVDによって実行される機能がホストマシンによって実行される。別の例として、NVDはTORスイッチの一部であってよく、またはTORスイッチは、NVDによって実行される機能を実行するように構成されてよく、これによってTORスイッチは、パブリッククラウドに使用されるさまざまな複雑なパケット変換を実行できる。NVDの機能を実行するTORは、スマートTORと呼ばれることがある。ベアメタル（BM：bare metal）インスタンスではなく仮想マシン（VM：virtual machines）インスタンスが顧客に提供されるさらに他の実装では、NVDによって実行される機能が、ホストマシンのハイパーバイザの内部に実装されてよい。一部の他の実装では、NVDの機能の一部が、一連のホストマシン上で動作している集中型のサービスにオフロードされてよい。

【0096】

ある実施形態では、図2に示されているようなスマートNICとして実装されるなどの場合、NVDは、NVDが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てよい。NVD上のポートは、ホスト向きポート（「南ポート」とも呼ばれる）またはネットワーク向きまたはTOR向きポート（「北ポート」とも呼ばれる）として分類され得る。NVDのホスト向きポートは、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2のホスト向きポートの例は、NVD210上のポート236、ならびにNVD212上のポート248および254を含む。NVDのネットワーク向きポートは、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2のネットワーク向きポートの例は、NVD210上のポート256およびNVD212上のポート258を含む。図2に示されているように、NVD210は、NVD210のポート256からTORスイッチ214に延びるリンク228を使用してTORスイッチ214に接続される。同様に、NVD212は、NVD212のポート258からTORスイッチ216に延びるリンク230を使用してTORスイッチ216に接続される。

【0097】

NVDは、ホスト向きポートを介してホストマシンから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た計算インスタンスによって生成された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行した後に、それらのパケットおよびフレームを、NVDのネットワーク向きポートを介してTORスイッチに転送してよい。NVDは、NVDのネットワーク向きポートを介してTORスイッチからパケットおよびフレームを受信してよく、必要なパケット処理を実行した後に、それらのパケットおよび

フレームを、NVDのホスト向きポートを介してホストマシンに転送してよい。

【0098】

ある実施形態では、複数のポート、およびNVDとTORスイッチの間の関連付けられたリンクが存在してよい。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（link aggregator group）と呼ばれる）を形成してよい。リンクの集約は、2つのエンドポイント間（例えば、NVDとTORスイッチの間の）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。特定のLAG内のすべての物理リンクは、同じ速度で全二重モードで動作してよい。LAGは、帯域幅を増やし、2つのエンドポイント間の接続の信頼性を向上させるのに役立つ。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つに動的かつ透過的に再割り当てされる。集約された物理リンクは、個々のリンクより高い帯域幅を供給する。LAGに関連付けられた複数のポートが、単一の論理ポートとして扱われる。LAGの複数の物理リンクにわたってトラフィックがロードバランスされ得る。1つまたは複数のLAGが、2つのエンドポイント間に構成されてよい。2つのエンドポイントが、NVDとTORスイッチの間、ホストマシンとNVDの間などに存在してよい。

10

【0099】

NVDは、ネットワーク仮想化機能を実装または実行する。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行される。ネットワーク仮想化機能の例としては、パケットカプセル化およびカプセル解除機能、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ーを実施するための機能、VCN内の計算インスタンスとの間でのパケットのルーティングおよび転送を容易にする機能などが挙げられるが、これらに限定されない。ある実施形態では、パケットの受信時に、NVDは、パケットを処理して、パケットが転送されまたはルーティングされる方法を決定するために、パケット処理パイプラインを実行するように構成される。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たVNICを実行すること、VCNに関連付けられた仮想ルータ（VR）を実行すること、仮想ネットワーク内の転送またはルーティングを容易にするためのパケットのカプセル化およびカプセル解除、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の実施、ネットワークアドレス変換（NAT）機能（例えば、ホストごとのパブリックIPからプライベートIPへの変換）、帯域幅調整機能、ならびに他の機能などの、オーバーレイネットワークに関連付けられた1つまたは複数の仮想機能を実行してよい。

20

30

【0100】

ある実施形態では、NVD内のパケット処理データ経路は、一連のパケット変換段で各々構成された、複数のパケットパイプラインを備えてよい。ある実装では、パケットの受信時に、パケットが構文解析され、単一のパイプラインに分類される。次に、パケットは、パケットが除去されるか、またはNVDのインターフェイスを経由して送信されるまで、1段ずつ線形方式で処理される。これらの段は、既存の段を組み立てることによって新しいパイプラインが構築されることが可能になり、新しい段を作成して既存のパイプラインに挿入することによって、新しい機能が追加されることが可能になるように、基本機能的パケット処理構成要素（例えば、ヘッダーの妥当性確認、帯域幅調整の実施、新しいレイヤ2ヘッダーの挿入、L4ファイアウォールの実施、VCNカプセル化／カプセル解除など）を提供する。

40

【0101】

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およびデータプレーン機能の両方を実行してよい。VCN制御プレーンの例が、図12、図13、図14、および図15にも示されており（参照番号1216、1316、1416、および1516を参照）、下で説明される。VCNデータプレーンの例が、図12、図

50

13、図14、および図15に示されており（参照番号1218、1318、1418、および1518を参照）、下で説明される。制御プレーン機能は、データが転送される方法を制御するネットワークを構成する（例えば、ルートおよびルートテーブルを設定する、VNICを構成するなどの）ために使用される機能を含む。ある実施形態では、すべてのオーバーレイと基板の間のマッピングを中心的に計算し、それらのマッピングをNVDに、およびDRG、SGW、IGWなどのさまざまなゲートウェイのような仮想ネットワークエッジデバイスに公開する、VCN制御プレーンが提供される。同じメカニズムを使用して、ファイアウォールルールが公開されてもよい。ある実施形態では、NVDは、そのNVDに関連するマッピングのみを取得する。データプレーン機能は、制御プレーンを使用する構成設定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が基板ネットワークを横断する前に、それらのパケットをカプセル化することによって実施される。カプセル化／カプセル解除機能は、NVDで実施される。ある実施形態では、NVDは、ホストマシンに入るネットワークパケットおよびホストマシンから出るネットワークパケットをすべて傍受し、ネットワーク仮想化機能を実行するように構成される。

10

20

30

40

50

【0102】

上で示されたように、NVDは、VNICおよびVCN VRを含むさまざまな仮想化機能を実行する。NVDは、VNICに接続された1つまたは複数のホストマシンによってホストされた計算インスタンスに関連付けられているVNICを実行してよい。例えば、図2に示されているように、NVD210は、NVD210に接続されたホストマシン202によってホストされた計算インスタンス268に関連付けられているVNIC276の機能を実行する。別の例として、NVD212は、ホストマシン206によってホストされたベアメタル計算インスタンス272に関連付けられているVNIC280を実行し、ホストマシン208によってホストされた計算インスタンス274に関連付けられているVNIC284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してよく、ホストマシンに接続されたNVDは、計算インスタンスに対応するVNICを実行してよい（すなわち、VNICに関連する機能を実行してよい）。

【0103】

NVDは、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2に示された実施形態では、NVD210は、計算インスタンス268が属するVCNに対応するVCN VR277を実行する。NVD212は、ホストマシン206および208によってホストされた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 VR283を実行する。ある実施形態では、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たすべての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たNVDは、それらの異なるVCNに対応するVCN VRを実行してよい。

【0104】

VNICおよびVCN VRに加えて、NVDは、さまざまなソフトウェア（例えば、デーモン）を実行してよく、NVDによって実行されるさまざまなネットワーク仮想化機能を容易にする1つまたは複数のハードウェアコンポーネントを含んでよい。簡単に目的で、これらのさまざまなコンポーネントは、図2に示された「パケット処理コンポーネント」として一緒にグループ化される。例えば、NVD210はパケット処理コンポーネント286を備え、NVD212はパケット処理コンポーネント288を備える。例えば、NVDのパケット処理コンポーネントは、NVDのポートおよびハードウェアインターフェイスとやりとりして、NVDによって受信されたパケットおよびNVDを使用して伝達されたパケットをすべて監視し、ネットワーク情報を格納するように構成された、パケットプロセッサを含んでよい。ネットワーク情報は、例えば、NVDによって処理されるさまざまな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およびフローごとの

情報（例えば、フローごとの統計値）を含んでよい。ある実施形態では、ネットワークフロー情報は、VNICごとに格納されてよい。パケットプロセッサは、パケットごとの操作を実行することに加えて、ステートフルNATおよびL4ファイアウォール（FW：firewall）を実施してよい。別の例として、パケット処理コンポーネントは、NVDによって格納された情報を1つまたは複数の異なる複製ターゲットストアに複製するように構成された複製エージェントを含んでよい。さらに別の例として、パケット処理コンポーネントは、NVDのロギング機能を実行するように構成されたロギングエージェントを含んでよい。パケット処理コンポーネントは、NVDの性能および健全性を監視するためのソフトウェア、および場合によっては、NVDに接続された他のコンポーネントの状態および健全性を監視するソフトウェアも、含んでもよい。

10

【0105】

図1は、VCN、VCN内のサブネット、サブネットにデプロイされた計算インスタンス、計算インスタンスに関連付けられたVNIC、VCNのVR、およびVCNのために構成されたゲートウェイのセットを含む、例示的な仮想ネットワークまたはオーバーレイネットワークのコンポーネントを示している。図1に示されたオーバーレイコンポーネントは、図2に示された物理コンポーネントのうちの1つまたは複数によって実行またはホストされてよい。例えば、VCN内の計算インスタンスは、図2に示された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てよい。ホストマシンによってホストされた計算インスタンスの場合、その計算インスタンスに関連付けられたVNICは、通常、そのホストマシンに接続されたNVDによって実行される（すなわち、そのホストマシンに接続されたNVDによって、VNIC機能が提供される）。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しているか、または実行してい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に関連付けられたゲートウェイは、1つまたは複数の異なる種類のNVDによって実行されてよい。例えば、あるゲートウェイは、スマートNICによって実行されてよく、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の他の実装によって実行されてよい。

20

【0106】

前述したように、顧客のVCN内の計算インスタンスは、さまざまなエンドポイントと通信してよく、エンドポイントは、送信元計算インスタンスと同じサブネット内、または送信元計算インスタンスと同じVCN内の、異なるサブネット内にあることができ、あるいはエンドポイントは、送信元計算インスタンスのVCNの外側にある。これらの通信は、計算インスタンスに関連付けられたVNIC、VCN VR、およびVCNに関連付けられたゲートウェイを使用して容易にされる。

30

【0107】

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の場合、通信は、送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたVNICを使用して容易にされる。送信元計算インスタンスおよび送信先計算インスタンスは、同じホストマシンによって、または異なるホストマシンによってホストされてよい。送信元計算インスタンスから生じるパケットは、送信元計算インスタンスをホストしているホストマシンから、そのホストマシンに接続されたNVDに転送されてよい。NVDでは、パケット処理パイプラインを使用してパケットが処理され、パケット処理パイプラインは、送信元計算インスタンスに関連付けられたVNICの実行を含むことができる。パケットの送信先エンドポイントが同じサブネット内にあるため、送信元計算インスタンスに関連付けられたVNICの実行は、パケットが、送信先計算インスタンスに関連付けられたVNICを実行しているNVDに転送されることを引き起こし、次に、このVNICは、パケットを処理して、送信先計算インスタンスに転送する。送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたVNICは、同じNVD上（例えば、送信元計算インスタンスおよび送信先計算インスタンスが、両方とも同じホストマシンによってホストされる場合）、または異なるNVD上（例えば、送信元計算インスタンスおよび送信先計算イン

40

50

スタンスが、異なるNVDに接続された異なるホストマシンによってホストされる場合)で実行されてよい。VNICは、NVDによって格納されたルーティングテーブル／転送テーブルを使用して、パケットのネクストホップを決定してよい。

【0108】

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伝達されるパケットの場合、送信元計算インスタンスから生じるパケットは、送信元計算インスタンスをホストしているホストマシンから、そのホストマシンに接続されたNVDに伝達される。NVDでは、パケット処理パイプラインを使用してパケットが処理され、パケット処理パイプラインは、1つまたは複数のVNIC、およびVCNに関連付けられたVRの実行を含むことができる。例えば、パケット処理パイプラインの一部として、NVDは、送信元計算インスタンスに関連付けられたVNICに対応する機能を実行するか、または呼び出す(VNICを実行する、とも呼ばれる)。VNICによって実行される機能は、パケット上のVLANタグを調べることを含んでよい。パケットの送信先がサブネットの外側にあるため、VCN VR機能が次に呼び出され、NVDによって実行される。次に、VCN VRは、パケットを、送信先計算インスタンスに関連付けられたVNICを実行しているNVDにルーティングする。次に、送信先計算インスタンスに関連付けられたVNICがパケットを処理し、パケットを送信先計算インスタンスに転送する。送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたVNICは、同じNVD上(例えば、送信元計算インスタンスおよび送信先計算インスタンスが、両方とも同じホストマシンによってホストされる場合)、または異なるNVD上(例えば、送信元計算インスタンスおよび送信先計算インスタンスが、異なるNVDに接続された異なるホストマシンによってホストされる場合)で実行されてよい。

【0109】

パケットの送信先が、送信元計算インスタンスのVCNの外側である場合、送信元計算インスタンスから生じるパケットは、送信元計算インスタンスをホストしているホストマシンから、そのホストマシンに接続されたNVDに伝達される。NVDは、送信元計算インスタンスに関連付けられたVNICを実行する。パケットの送信先エンドポイントがVCNの外側にあるため、次にパケットは、そのVCNのVCN VRによって処理される。NVDは、VCN VR機能を呼び出し、パケットが、VCNに関連付けられた適切なゲートウェイを実行しているNVDに転送されることを引き起こしてよい。例えば、送信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のために構成されたDRGゲートウェイを実行しているNVDに転送されてよい。VCN VRは、送信元計算インスタンスに関連付けられた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、実行されてよい。ゲートウェイは、スマートNIC、ホストマシン、または他のNVDの実装であることができるNVDによって、実行されてよい。次に、パケットは、ゲートウェイによって処理され、意図された送信先エンドポイントへのパケットの伝達を容易にするネクストホップに転送される。例えば、図2に示された実施形態では、計算インスタンス268から生じるパケットは、リンク220を経由して(NIC232を使用して)ホストマシン202からNVD210に伝達されてよい。NVD210で、VNIC276が、送信元計算インスタンス268に関連付けられたVNICであるため、呼び出される。VNIC276は、パケット内のカプセル化された情報を調べ、意図された送信先エンドポイントへのパケットの伝達を容易にすることを目的に、パケットを転送するためのネクストホップを決定し、その後、パケットを決定されたネクストホップに転送するように構成される。

【0110】

VCNにデプロイされた計算インスタンスは、さまざまな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、CSP I200によってホストされているエンドポイント、およびCSP I200の外側のエンドポイントを含んでよい。CSP I200によってホストされたエンドポイントは、同じVCNまたは他のVCN内のインスタンスを含んでよく、これらのVCNは、顧客のVCNまたは顧客に属していないVCNであ

ってよい。C S P I 2 0 0によってホストされたエンドポイント間の通信は、物理ネットワーク218を経由して実行されてよい。計算インスタンスは、C S P I 2 0 0によってホストされていないか、またはC S P I 2 0 0の外側にある、エンドポイントと通信してもよい。これらのエンドポイントの例としては、顧客のオンプレミスネットワークまたはデータセンター内のエンドポイント、あるいはインターネットなどのパブリックネットワークを経由してアクセスできるパブリックエンドポイントが挙げられる。C S P I 2 0 0の外側のエンドポイントとの通信は、さまざまな通信プロトコルを使用して、パブリックネットワーク（例えば、インターネット）（図2に示されていない）またはプライベートネットワーク（図2に示されていない）を経由して実行されてよい。

【0111】

図2に示されたC S P I 2 0 0のアーキテクチャは、単に例であり、限定することを意図されていない。代替の実施形態では、変形、代替手段、および変更が可能である。例えば、一部の実装では、C S P I 2 0 0は、図2に示されたシステムまたはコンポーネントより多いか、または少ないシステムまたはコンポーネントを含んでよく、2つ以上のシステムを組み合わせるよく、またはシステムの異なる構成もしくは配置を含んでよい。図2に示されたシステム、サブシステム、および他のコンポーネントは、それぞれのシステムの1つまたは複数の処理ユニット（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）において、ハードウェアを使用して、またはこれらの組合せで実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。

【0112】

図4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のI/O仮想化を実現するための、ホストマシンとNVDの間の接続を示している。図4に示されているように、ホストマシン402は、仮想環境を提供するハイパーバイザ404を実行する。ホストマシン402は、顧客／テナント1番に属するVM1 406および顧客／テナント2番に属するVM2 408という2つの仮想マシンインスタンスを実行する。ホストマシン402は、リンク414を介してNVD412に接続されている物理NIC410を備える。計算インスタンスの各々は、NVD412によって実行されるVNICに接続される。図4の実施形態では、VM1 406はVNIC-VM1 420に接続され、VM2 408はVNIC-VM2 422に接続される。

【0113】

図4に示されているように、NIC410は、論理NIC A 416および論理NIC B 418という2つの論理NICを備えている。各仮想マシンは、それ自体の論理NICに接続され、その論理NICと共に機能するように構成される。例えば、VM1 406は論理NIC A 416に接続され、VM2 408は論理NIC B 418に接続される。ホストマシン402が、複数のテナントによって共有されている1つのみの物理NIC410を備えているとしても、論理NICに起因して、各テナントの仮想マシンは、自分のホストマシンおよびNICを有しているということを確認している。

【0114】

ある実施形態では、各論理NICがそれ自体の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番の論理NIC A 416に割り当てられ、別のVLAN IDが、テナント2番の論理NIC B 418に割り当てられる。パケットがVM1 406から伝達されるときに、テナント1番に割り当てられたタグが、ハイパーバイザによってパケットに取り付けられ、次に、パケットが、リンク414を経由してホストマシン402からNVD412に伝達される。同様の方法で、パケットがVM2 408から伝達されるときに、テナント2番に割り当てられたタグが、ハイパーバイザによってパケットに取り付けられ、次に、パケットが、リンク414を経由してホストマシン402からNVD412に伝達される。したがって、ホストマシン402からNVD412に伝達されたパケット424は、特定のテナントおよび関連付けられたVMを識別する関連付けられたタグ426を有する。NVDで、ホストマシン402から受信

されたパケット 4 2 4 に関して、パケットに関連付けられたタグ 4 2 6 が、パケットが V N I C - V M 1 4 2 0 によって処理されるべきか、または V N I C - V M 2 4 2 2 によって処理されるべきかを判定するために使用される。次に、パケットは、対応する V N I C によって処理される。図 4 に示された構成は、各テナントの計算インスタンスが、自分のホストマシンおよび N I C を所有しているということを確認できるようにする。図 4 に示された設定は、マルチテナンシ機能をサポートするための I / O 仮想化を可能にする。

【 0 1 1 5 】

図 5 は、ある実施形態による、物理ネットワーク 5 0 0 の簡略化されたブロック図を示している。図 5 に示された実施形態は、C l o s ネットワークとして構造化される。C l o s ネットワークは、高い 2 分割帯域幅および最大のリソース利用を維持しながら、接続冗長性をもたらすように設計された特定の種類ネットワークトポロジである。C l o s ネットワークは、ノンブロッキングの多段または多層スイッチングネットワークの一種であり、その段または層の数は、2 つ、3 つ、4 つ、5 つなどであることができる。図 5 に示された実施形態は、層 1、2、および 3 を含んでいる 3 層ネットワークである。T O R スイッチ 5 0 4 は、C l o s ネットワーク内の層 0 スイッチを表す。1 つまたは複数の N V D が T O R スイッチに接続される。層 0 スイッチは、物理ネットワークのエッジデバイスとも呼ばれる。層 0 スイッチは、リーフスイッチとも呼ばれる層 1 スイッチに接続される。図 5 に示された実施形態では、「n」個の層 0 T O R スイッチのセットが、「n」個の層 1 スイッチのセットに接続され、一緒にポッドを形成する。ポッド内の各層 0 スイッチは、ポッド内のすべての層 1 スイッチに相互接続されるが、ポッド間にスイッチの接続は存在しない。ある実装では、2 つのポッドはブロックと呼ばれる。各ブロックは、「n」個の層 2 スイッチ（スパインスイッチと呼ばれることがある）のセットによってサービスを提供されるか、またはそれらに接続される。物理ネットワークトポロジには、複数のブロックが存在することができる。次に、層 2 スイッチは、「n」個の層 3 スイッチ（スーパースパインスイッチと呼ばれることがある）に接続される。物理ネットワーク 5 0 0 を経由するパケットの通信は、通常、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行される。通常、T O R レイヤを除く物理ネットワークのすべてのレイヤは、n 方向の冗長性を有し、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で互いのスイッチの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ーが指定されてよい。

【 0 1 1 6 】

C l o s ネットワークの特徴は、1 つの層 0 スイッチから別の層 0 スイッチに（または層 0 スイッチに接続された N V D から層 0 スイッチに接続された別の N V D に）達するための最大ホップ数が固定されることである。例えば、3 層 C l o s ネットワークでは、パケットが 1 つの N V D から別の N V D に達するために、最大で 7 ホップが必要とされ、送信元 N V D およびターゲット N V D が、C l o s ネットワークのリーフ層に接続される。同様に、4 層 C l o s ネットワークでは、パケットが 1 つの N V D から別の N V D に達するために、最大で 9 ホップが必要とされ、送信元 N V D およびターゲット N V D が、C l o s ネットワークのリーフ層に接続される。したがって、C l o s 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性のある待ち時間を維持し、これは、データセンター内およびデータセンター間の通信にとって重要である。C l o s トポロジは、水平にスケーリングし、コスト効率が高い。より多くのスイッチ（例えば、より多くのリーフスイッチおよびスパインスイッチ）をさまざまな層に追加することによって、および隣接する層でスイッチ間のリンクの数を増やすことによって、ネットワークの帯域幅／スループット能力が容易に増やされ得る。

【 0 1 1 7 】

ある実施形態では、C S P I 内の各リソースに、クラウド識別子（C I D : Cloud Identifier）と呼ばれる一意の識別子が割り当てられる。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 A P I を介して、リソースを管

理するために使用され得る。C I D の例示的な構文は次のとおりである。

o c i d 1 . <リソースの種類> . <レルム> . [リージョン] [. 将来の使用] . <一意の I D >

ここで、

o c i d 1 : C I D のバージョンを示すリテラル列。

リソースの種類：リソースの種類（例えば、インスタンス、ボリューム、V C N、サブネット、ユーザ、グループなど）。

レルム：リソースが存在するレルム。例示的な値は、商用レルムの場合の「c 1」、政府クラウドレルムの場合の「c 2」、または連邦政府クラウドレルムの場合の「c 3」などである。各レルムは、それ自体のドメイン名を有してよい。

リージョン：リソースが存在するリージョン。リージョンをリソースに適用できない場合、この部分は空白であってよい。

将来の使用：将来の使用のために予約されている。

一意の I D : I D の一意の部分。この形式は、リソースまたはサービスの種類に応じて変わってよい。

【0118】

マルチクラウドの導入

図6は、ある実施形態による、異なるクラウドサービスプロバイダ（C S P）によって提供された複数のクラウド環境を含んでいる分散環境600の簡略化された高レベルの図を示し、クラウド環境が、その特定のクラウド環境によって提供された1つまたは複数のクラウドサービスが他のクラウド環境の顧客によって使用されることを可能にする特殊なインフラストラクチャを提供する特定のクラウド環境を含む。図6に示されているように、さまざまなクラウド環境（「クラウド」とも呼ばれる）が、異なるクラウドサービスプロバイダ（C S P）によって提供されてよく、各クラウド環境またはクラウドは、そのクラウド環境の1人または複数の顧客が加入することができる1つまたは複数のクラウドサービスを提供する。C S Pによって提供されたクラウド環境によって提供される一連のクラウドサービスは、S a a S（Software-as-a-Service）サービス、I a a S（Infrastructure-as-a-Service）サービス、P a a S（Platform-as-a-Service）サービス、D B a a S（Database-as-a-Service）などを含むが、これらに限定されない、1つまたは複数の異なる種類のクラウドサービスを含んでよい。さまざまなC S Pによって提供されたクラウド環境の例としては、Oracle Corporationによって提供されたOracle（登録商標）クラウドインフラストラクチャ（O C I）、Microsoft Corporationによって提供されたMicrosoft（登録商標）Azure、Google LLCによって提供されたGoogle Cloud（商標）、Amazon Corporationによって提供されたAmazon Web Services（A W S（登録商標））などが挙げられる。特定のクラウド環境によって提供されたクラウドサービスは、別のクラウド環境によって提供されたクラウドサービスのセットと異なってよい。

【0119】

標準的なクラウド環境では、C S Pは、そのクラウド環境によって顧客に提供されている1つまたは複数のクラウドサービスを提供するために使用されるクラウドサービスインフラストラクチャ（C S P I）を提供する。C S Pによって提供されたC S P Iは、計算リソース、メモリリソース、ネットワークリソース、クラウドサービスにアクセスするためのコンソールなどを含む、さまざまな種類のハードウェアリソースおよびソフトウェアリソースを含んでよい。C S Pによって提供されたクラウド環境の顧客は、そのクラウド環境によって提供されたクラウドサービスのうちの1つまたは複数に加入してよい。C S Pによって、さまざまなサブスクリプションモデルが顧客に提供されてよい。顧客がクラウド環境によって提供されたクラウドサービスに加入した後に、1人または複数のユーザが、加入している顧客に関連付けられてよく、これらのユーザは、顧客が加入したクラウドサービスを使用することができる。ある実装では、顧客が、特定のクラウド環境によって提供されたクラウドサービスに加入するときに、顧客のアカウントまたは顧客のテナン

10

20

30

40

50

シが、その顧客のために作成される。次に、1人または複数のユーザが、顧客のテナンシに関連付けられることが可能であり、その後、これらのユーザは、顧客のテナンシの下で顧客が加入したサービスを使用することができる。顧客が加入したサービス、顧客のテナンシに関連付けられたユーザなどに関する情報が、通常は、クラウド環境内に格納され、顧客のテナンシに関連付けられる。

【0120】

例えば、3つの異なるCSPによって提供された3つの異なるクラウド環境が、図6に示されている。これらのクラウド環境は、CSP Aによって提供されたクラウド環境A（クラウドA）610、CSP Bによって提供されたクラウド環境B（クラウドB）640、およびCSP Cによって提供されたクラウド環境C（クラウドC）660を含む。クラウドA 610は、CSP Aによって提供されたインフラストラクチャCSP I__A 612を含み、このインフラストラクチャは、クラウドA 610によって提供されたサービスのセット「サービスA」614を提供するために使用されてよい。1人または複数の顧客（例えば、顧客A1 616-1、顧客A2 616-2）は、クラウドA 610によって提供されたサービスA 614からの1つまたは複数のサービスに加入してよい。1人または複数のユーザ618-1は、顧客A1 616-1に関連付けられてよく、クラウドA 610内で顧客A1 616-1が加入したサービスを使用することができる。同様の方法で、1人または複数のユーザ618-2は、顧客A2 616-2に関連付けられてよく、クラウドA 610内で顧客A2 616-2が加入したサービスを使用することができる。さまざまな使用事例では、顧客A1 616-1が加入したサービスは、顧客A2 616-2が加入したサービスと異なってよい。

【0121】

図6に示されているように、クラウドB 640は、CSP Bによって提供されたインフラストラクチャCSP I__B 642を含み、このインフラストラクチャは、クラウドB 640によって提供されたサービスのセット「サービスB」644を提供するために使用されてよい。1人または複数の顧客（例えば、顧客B1 646-1）は、サービスB 644からの1つまたは複数のサービスに加入してよい。1人または複数のユーザ648-1は、顧客B1 646-1に関連付けられてよく、クラウドB 640内で顧客B1 646-1が加入したサービスを使用することができる。

【0122】

図6に示されているように、クラウドC 660は、CSP Cによって提供されたインフラストラクチャCSP I__C 662を含み、このインフラストラクチャは、クラウドC 660によって提供されたサービスのセット「サービスC」664を提供するために使用されてよい。1人または複数の顧客（例えば、顧客C1 666-1）は、サービスC 664からの1つまたは複数のサービスに加入してよい。1人または複数のユーザ668-1は、顧客C1 666-1に関連付けられてよく、クラウドC 660内で顧客C1 666-1が加入したサービスを使用することができる。サービスA 614、サービスB 644、およびサービスC 664が互いに異なることができるということに、注意すべきである。

【0123】

既存のクラウドの実装では、各クラウドは、閉じたエコシステムを加入している顧客および関連付けられたユーザに提供する。その結果、クラウド環境の顧客および関連付けられたユーザは、顧客が加入しているクラウドによって提供されたサービスを使用することに制限される。例えば、顧客B1 646-1およびそのユーザ648-1は、クラウドB 640によって提供されたサービスB 644を使用することに制限され、クラウドB 640内の自分のアカウントを使用して、クラウドA 610によって提供されたサービスA 614からのサービスまたはクラウドC 660によって提供されたサービスC 664からのサービスなどの、異なるクラウド環境からのサービスにアクセスすることができない。本明細書に記載された教示は、この制限を克服する。本開示において説明されているように、リンクが2つのクラウド環境間に作成されることを可能にし、それに

よって、第1のCSPによって提供された第1のクラウド環境によって提供されたサービスが、第2の異なるCSPによって提供された第2の異なるクラウド環境の顧客（および関連付けられたユーザ）によって、第2のクラウド環境内の顧客のアカウントを使用して、使用されることを可能にする、さまざまな技術が説明される。

【0124】

例えば、図6に示された実施形態では、CSP Aによって提供されたインフラストラクチャCSP I__A 612は、他のインフラストラクチャ620に加えて、クラウドAによって提供された1つまたは複数のサービス614が、クラウドB 640およびC 660などの他のクラウドの顧客および関連付けられたユーザによって、それらの他のクラウド内の顧客のアカウントを使用して、使用されることを可能にする、特殊なインフラストラクチャ622（マルチクラウド有効化インフラストラクチャ622またはMEI（multi-cloud enabling infrastructure）622あるいはマルチクラウドインフラストラクチャ622と呼ばれる）を含む。ある実装では、クラウドBおよびCの顧客は、クラウドA 610によって提供されたサービス614のうちの1つまたは複数を使用するために、クラウドAを使用して別々のアカウントを開く必要がない。クラウドB 640の顧客B1 646-1および関連付けられたユーザ648-1は、クラウドB 640内の顧客のアカウントまたはテナンシを使用して、クラウドA 610によって提供された1つまたは複数のサービス614を使用することができる。別の例として、クラウドC 660の顧客C1 666-1および関連付けられたユーザ668-1は、クラウドC 660内の顧客のアカウントまたはテナンシを使用して、クラウドA 610によって提供された1つまたは複数のサービス614を使用することができる。

10

20

【0125】

ある実装では、MEI 622は、クラウドA 610と他のクラウドの間にリンクが作成されることを可能にし、これらのリンクは、クラウドA 610によって提供されたサービスにアクセスして利用するために、他のクラウドの顧客および関連付けられたユーザによって使用され得る。これが、クラウドA 610とクラウドB 640の間に作成されたリンク670、およびクラウドA 610とクラウドC 660の間に作成されたリンク672として、図6に記号的に示されている。リンク670を介して、クラウドB 640の顧客は、クラウドA 610によって提供された1つまたは複数のサービス614にアクセスするか、またはサービス614を使用することができる。同様に、リンク672を介して、クラウドC 660の顧客は、クラウドA 610によって提供された1つまたは複数のサービス614にアクセスするか、またはサービス614を使用することができる。

30

【0126】

MEI 612が実装され得るさまざまな方法が存在する。ある実施形態では、MEI 612は、異なるクラウドとのリンクが確立されることを可能にするコンポーネントを含んでよい。例えば、図6では、MEI 622は、クラウドB 640とのリンク670を有効化する役割を担うインフラストラクチャコンポーネント624、およびクラウドC 660とのリンク672を有効化する役割を担うインフラストラクチャコンポーネント626を含む。同様の方法で、MEI 622は、他のクラウドとのリンクを有効化し、容易にする他のコンポーネントを含んでよい。一部の实装では、MEI 622のコンポーネントは、複数の異なるクラウドとのリンクを容易にしてもよい。

40

【0127】

1つのクラウドの顧客が、異なるクラウドによって提供されたクラウドサービスを使用したい理由、または使用することを望む理由は、複数ある。例として図6を使用すると、クラウドB 640の顧客B1 646-1がクラウドA 610によって提供されたクラウドサービス614を使用したい理由が複数ある。1つの使用事例の状況では、この理由は、クラウドA 610が、クラウドB 640によって提供されない機能を有するクラウドサービスを提供するために発生することがある。別の使用事例の状況として、クラウドAおよびBは、同様のサービスを提供することができるが、クラウドA 610によ

50

って提供されたサービスが、クラウド B 640 によって提供された対応するサービスより良い（例えば、より多くの特徴／機能、より高速など）ことがある。さらに別の使用事例の状況として、クラウド B 640 の顧客 B1 646-1 は、クラウド B 640 によって提供されたクラウドサービスより低価格でサービスが提供されるため、クラウド A 610 によって提供されたクラウドサービスを使用したいことがある。場合によっては、クラウド B 640 の顧客 B1 646-1 がクラウド A 610 によって提供されたクラウドサービスを使用したい、地理的制約または他の理由が存在することがある。例えば、クラウド A 610 は、クラウド B 640 によってサービス提供されていない所望のサービスを地理的領域内で提供することがあり、または特定のサービスが、顧客がサービスを望んでいる地理的領域内で、クラウド B 640 によって提供されていない。1つのクラウドの顧客が異なるクラウドによって提供されたサービスを使用したい理由に関して、複数の他の使用事例の状況も可能である。

10

【0128】

ある実施形態では、MEI622 は、クラウド A 610 と別のクラウドの間のリンクを作成し、このリンクを介して、他のクラウドの顧客に関連付けられたユーザが、シームレスな方法で、他のクラウド自体から、クラウド A 610 によって提供されたサービスにアクセスして使用できるようにするための能力を提供し、その機能を実行する。例えば、MEI622 は、クラウド B 640 の顧客 B1 646-1 に関連付けられたユーザ 648-1 が、シームレスな方法で、クラウド A 610 によって提供されたサービス A 614 からのサービスにアクセスできるようにする。ある実装では、クラウド B 640 内からユーザ 648-1 がアクセスできるユーザインターフェイス（例えば、コンソール）が提供されてよく、このユーザインターフェイスは、ユーザが、クラウド A 610 によって提供されたサービス 614 のリストを見ること、およびユーザ 648-1 がアクセスすることを望む特定のサービスを選択することを可能にする。ユーザの選択に応答して、MEI622 は、要求されたサービスへのアクセスを可能にするために、クラウド A と B の間のリンク 670 を確立する処理を実行する役割を担う。リンク 670 を設定するための処理が、MEI622 によって実質的に自動的に実行される。顧客 B1 646-1 または関連付けられたユーザ 648-1 は、クラウド A 610 と B 640 の間のリンク 670 の作成、維持、および使用を容易にするために必要とされるすべてのシステム、ネットワーク、または他の構成の変更を実行することに関して、心配することがない。クラウド間のリンクの作成において、ユーザにも顧客にも負担を与えない。本開示で説明された技術を使用して、高速で効率的な方法でリンクが作成される。

20

30

【0129】

MEI622 は、さまざまな技術を使用して、ユーザおよび顧客にとってシームレスなリンクの作成および使用を行い、このようにして、改善されたユーザ体験を提供することができる。ある実装では、MEI622 は、クラウド A 610 にサービスを要求する、およびクラウド A 610 からの要求されたサービスにアクセスするなどのために、顧客 B1 および関連付けられたユーザ 648-1 が対話するユーザインターフェイス（例えば、グラフィカルユーザインターフェイス GUI (graphical user interfaces) など）およびプロセスフローを、クラウド B 640 内で顧客／ユーザが体験するインターフェイスおよびプロセスフローに実質的に類似させる。このようにして、クラウド B 640 のインターフェイスおよびプロセスフローに慣れていることがある顧客またはユーザは、クラウド A 610 からのサービス 614 にアクセスするために、新しいインターフェイスおよびプロセスフローを学習する必要がない。MEI622 は、異なるクラウド環境のユーザに、異なるインターフェイスおよびプロセスフローを提示してよい。例えば、クラウド B のユーザインターフェイスおよびフローに実質的に類似しているユーザインターフェイスおよびプロセスフローの第 1 のセットが、クラウド B 640 からのユーザに提示されてよく、一方、クラウド C のユーザインターフェイスおよびフローに実質的に類似しているユーザインターフェイスおよびプロセスフローの異なるセットが、クラウド C 660 からクラウド A 610 にアクセスしているユーザに提示されてよい。これは、

40

50

他のクラウドからクラウド A 610 のサービス 614 にアクセスするためのユーザの体験を簡略化し、その結果、改善するために実行される。

【0130】

別の例として、各クラウド環境は、通常、セキュリティをクラウド環境に提供するように構成されたアイデンティティ管理システムを含む。アイデンティティ管理システムは、クラウド環境にデプロイされている、CSPによって提供されたリソース、および加入しているクラウドの顧客のリソースを含む、クラウド環境内のリソースを保護するように構成される。アイデンティティ管理システムによって実行される機能は、例えば、クラウドの加入している顧客および関連付けられたユーザに関連付けられたアイデンティティ認証情報（例えば、ユーザ名、パスワードなど）を管理すること、アイデンティティ認証情報を使用して、クラウド環境のために構成された許可／アクセスポリシーに基づいてクラウドリソースおよびサービスへのユーザのアクセスを規制すること、ならびに他の機能を含む。異なるクラウドは、異なるアイデンティティ管理システムおよび関連する技術を使用してよい。例えば、クラウド A 610 内のアイデンティティ管理システムおよび関連する手順は、クラウド B 640 内のアイデンティティ管理システムおよび関連する手順と完全に異なってよく、さらに、クラウド B 640 内のアイデンティティ管理システムおよび関連する手順は、クラウド C 660 内のアイデンティティ管理システムおよび関連する手順と完全に異なってよい。ある実装では、異なるクラウド環境間のアイデンティティ管理システムおよび関連する手順におけるこれらの違いにもかかわらず、本明細書に記載された技術は、第1のクラウドの顧客に関連付けられたユーザが、第1のクラウド内の顧客およびユーザに関連付けられた同じアイデンティティ認証情報を使用して、異なるクラウドによって提供されたクラウドサービスにアクセスすることを可能にする。

10

20

【0131】

例えば、図6に示された実施形態では、CSP Bによって提供されたクラウド B 640 は、アイデンティティ認証情報を、顧客 B1 646-1 および関連付けられたユーザ 648-1 などの加入している顧客および関連付けられたユーザに割り当てる（assigns）か、または割り当てる（allocates）、アイデンティティ管理システムを含んでよい。これらのアイデンティティ認証情報は、クラウド B 640 内の顧客 B1 646-1 のために作成されたテナンシに関連付けられる。ある実装では、クラウド A 610 によって提供された MEI 622 は、クラウド B の顧客 B1 646-1 に関連付けられたユーザ 648-1 が、クラウド B 640 内のユーザ 648-1 および顧客 B1 646-1 に関連付けられたアイデンティティ認証情報を使用してクラウド A 610 内のサービス A 614 からのサービスにアクセスすることを可能にする。これによって、単にクラウド A 610 内のサービス 614 にアクセスする目的で、ユーザ 648-1 がクラウド A 610 に固有の新しいアイデンティティ認証情報を作成する必要がないため、ユーザ 648-1 のユーザ体験を大幅に改善する。MEI 622 は、そのようなアクセスを容易にする。

30

【0132】

例として、クラウド B 640 の顧客 B1 は、クラウド A 610 によって提供されたサービスのセット 614 からの DBaaS（Database-as-a Service）などのサービスを使用することを選択してよい。そのような選択に回答して、MEI 622 は、顧客 B1 646-1 に関連付けられたユーザ 648-1 がクラウド A 610 によって提供された DBaaS サービスを使用できるようにするために、リンク 670 がクラウド A 610 とクラウド B 640 の間に自動的に作成されることを引き起こす。リンク 670 の自動的な設定は、MEI 622 によって容易にされる。リンク 670 が設定された後に、ユーザ 668-1 は、クラウド B 640 を介してクラウド A 610 内の DBaaS サービスを使用することができる。このサービスを使用することの一部として、ユーザ 668-1 は、クラウド B 640 を介して、データベースリソースを作成する要求をクラウド A 610 に送信することができる。それに応じて、CSP I__A 612 は、要求されたデータベースをクラウド A 610 内に作成してよい。ある実装では、作成されたデータベ

40

50

ースは、クラウド A 610 内で顧客 B 1 のために作成された仮想ネットワーク（例えば、仮想クラウドネットワークまたは VCN）内でプロビジョニングされてよく、クラウド B 640 を介してユーザ 668-1 によってアクセス可能である。次に、ユーザ 668-1 は、クラウド B 640 から、プロビジョニングされたデータベースを使用する要求をクラウド A 610 に送信してよい。これらの要求は、例えば、データをデータベースに書き込むこと、データベースに格納されたデータを更新すること、データベース内のデータを削除すること、データベースを削除すること、追加のデータベースを作成することなどの要求を含んでよい。一部の使用事例では、これらの要求は、クラウド B 640 を介してユーザ 668-1 から、またはクラウド B 640 によって提供されたサービス 644 から、生じてよい。このようにして、クラウド A 610 によって提供された MEI 622 は、異なる CSP によって提供された異なるクラウドの顧客に関連付けられたユーザが、クラウド A 610 によって提供されたサービスにシームレスにアクセスできるようにする。

10

【0133】

図 6 に示された分散環境 600 は、単に例であり、主張される実施形態の範囲を過度に限定するよう意図されていない。多くの変形、代替手段、および変更が可能である。例えば、代替の実施形態では、分散環境 600 は、より多くの、またはより少ない、クラウド環境を含んでよい。クラウド環境は、より多くの、またはより少ない、システムおよびコンポーネントを含んでもよく、あるいはシステムおよびコンポーネントの異なる構成または配置を有してよい。図 6 に示されたシステムおよびコンポーネントは、それぞれのシステムの 1 つまたは複数の処理ユニット（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）において、ハードウェアを使用して、またはこれらの組合せで実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。

20

【0134】

マルチクラウド制御プレーン（MCCP）

図 7 は、一部の実施形態による、マルチクラウド制御プレーン（MCCP）の高レベルのアーキテクチャを示している。図 7 に示されているように、高レベルのアーキテクチャ 700 は、第 1 のクラウドサービスプロバイダ（例えば、OCI）720 によって提供された第 1 のクラウド環境、および第 2 のクラウドサービスプロバイダ 710（すなわち、Azure）によって提供された第 2 のクラウド環境を含む。第 1 のクラウド環境 720 は、第 1 のクラウド環境 720 のユーザに複数のサービスを提供する第 1 のクラウドインフラストラクチャ 720A を含む。さらに、第 1 のクラウド環境 720 は、第 1 のクラウドインフラストラクチャ 720A（例えば、Oracle クラウドインフラストラクチャ（OCI））のサービスを他のクラウド環境（例えば、第 2 のクラウドインフラストラクチャ 710A）のユーザに配信する能力をプロビジョニングするマルチクラウドインフラストラクチャ 720B を含む。マルチクラウドインフラストラクチャ 720B は、クラウド環境間の単純な統合をもたらしながら、ユーザが、ユーザのネイティブなクラウド環境のユーザ体験にできるだけ近いユーザ体験を伴って、他のクラウド上のサービス（例えば、Oracle PaaS サービス）にアクセスすることを可能にする。

30

40

【0135】

第 2 のクラウドインフラストラクチャ 710A は、第 2 のクラウドポータル 711、アクティブディレクトリ 712、リソースマネージャ 713、顧客サブスクリプション 715、第 1 のクラウドプロバイダのサブスクリプション 717 を含む。第 2 のクラウドポータル 711 は、第 2 の環境 710 の顧客がログインし、クラウドのデプロイメントおよびインスタンスを管理することができる、集中型のアクセスポイントである。第 2 のクラウドポータルが、第 2 のクラウドインフラストラクチャによって提供された監視サービスおよび操作サービスの両方の選択肢を提供してよいということに注意する。アクティブディレクトリ 712 は、エンドユーザのアイデンティティおよびアクセス権限を管理する能力を管理者に提供する、第 2 のクラウドインフラストラクチャ 710A によって提供された

50

サービスである。そのサービスは、コアディレクトリ、アクセス管理、およびアイデンティティ保護を含んでよい。リソースマネージャ 7 1 3 は、第 2 のクラウドインフラストラクチャのデプロイメントおよび管理サービス、すなわち、顧客サブスクリプション 7 1 5 においてデプロイされるリソースに関する操作（例えば、作成、更新、削除など）を実行するための、ユーザに提供する管理レイヤである。顧客サブスクリプションが、顧客のアプリケーションがデプロイされて実行される仮想ネットワーク（VNET: virtual network）と呼ばれることもあるということに注意する。第 2 のクラウドインフラストラクチャ 7 1 0 A 内の第 1 のクラウドプロバイダ 7 1 7 のサブスクリプションは、第 2 のクラウドインフラストラクチャ 7 1 0 A と確立される（例えば、オンプレミスの場所から、外部クラウド環境からの）ネットワーク接続をプロビジョニングするエクスプレスルートならびにハブおよびスポーク VNET を含む。そのような接続が、パブリックインターネットを介してルーティングされなくてよく、それによって、さらなる信頼性、より速い速度、一貫性のある待ち時間、およびより高いセキュリティをユーザにもたらすということに注意する。

10

20

30

40

50

【0136】

第 1 のクラウドインフラストラクチャ 7 2 0 A は、制御プレーン 7 2 4、顧客のテナンシ 7 2 6、およびマルチクラウドインフラストラクチャ 7 2 0 B を含む。第 1 のクラウドインフラストラクチャ 7 2 0 A の制御プレーン 7 2 4 は、クラウド環境にわたって管理およびオーケストレーションを提供する第 1 のクラウド環境のネイティブな制御プレーンである。制御プレーン 7 2 4 では、構成ベースラインが設定され、ユーザおよびロールのアクセスがプロビジョニングされ、アプリケーションが存在するため、アプリケーションが関連するサービスと共に実行され得る。マルチクラウドインフラストラクチャ 7 2 0 B は、マルチクラウドプラットフォームデータプレーン 7 2 2、およびマルチクラウドプラットフォームデータプレーン 7 2 8 を含む。前述したように、マルチクラウドインフラストラクチャ 7 2 0 B は、クラウド環境間の単純な統合をもたらしながら、他のクラウド環境（例えば、第 2 のクラウド環境 7 1 0）のユーザが、ユーザのネイティブなクラウド環境（例えば、第 2 のクラウド環境 7 1 0）のユーザ体験にできるだけ近いユーザ体験を伴って、第 1 のクラウド環境によって提供されたサービスにアクセスするために、プロビジョニングする。

【0137】

図 7 の MCCP アーキテクチャは、第 2 のクラウドインフラストラクチャ 7 1 0 内で認証されたユーザが、マルチクラウドインフラストラクチャ 7 2 0 B を介して公開される第 1 のクラウドインフラストラクチャ 7 2 0 のリソースに対して制御プレーンの操作を実行することを許可する、マルチクラウドコンソール 7 2 1（第 2 のクラウドポータル 7 1 1 と異なる）をさらに含む。一部の実装では、図 7 に示されているように、マルチクラウドコンソール 7 2 1 に送信されたすべてのユーザ 7 0 5 の要求は、第 1 のクラウド環境に含まれているマルチクラウドインフラストラクチャに向けられる。ユーザ 7 0 5 が、第 1 のクラウドインフラストラクチャによって提供されたリソースに関する要求（例えば、CRUD 要求）をマルチクラウドコンソール 7 2 1 に直接送信できるということが理解される。マルチクラウドコンソール 7 2 1 は、第 2 のクラウドインフラストラクチャ内でローカルに使用される構文または形式に類似する構文または形式を有する要求を処理するように構成される。言い換えると、マルチクラウドコンソール 7 2 1 は、第 2 のクラウドインフラストラクチャ 7 1 0 A に含まれている第 2 のクラウドポータル 7 1 1 に類似するルックアンドフィールを有するだけでなく、類似する用語を使用する。一部の实装では、第 2 のクラウドコンソール 7 1 1 内で、ユーザをマルチクラウドコンソール 7 2 1 に向けるリンク（例えば、ウェブリンク）が提供されてよい。

【0138】

第 1 のクラウドインフラストラクチャ 7 2 0 A に含まれているマルチクラウドインフラストラクチャ 7 2 0 B は、権限モジュール 7 2 2 A、プロキシモジュール 7 2 2 B、プラットフォームサービスモジュール 7 2 2 C、クラウドリンクアダプタ 7 2 2 D、アダプタ

1、アダプタ2、アダプタ3、およびアダプタ4を含んでいるアダプタのプール722E、ならびにネットワークリンクアダプタ722Fなどの、複数のマイクロサービスを含む。アダプタのプール722Eは、エクサデータクラウドサービスアダプタ、自律的データベース共有アダプタ、自律的データベース専用アダプタ、および仮想マシンデータベースアダプタなどのアダプタを含むことができる。

【0139】

アダプタのプール722Eに含まれているアダプタの各々は、（第1のクラウドインフラストラクチャ720Aによって提供された）固有の基盤になるリソースのセットを、他のクラウド環境（例えば、第2のクラウド環境）のユーザに公開する役割を担う。特に、アダプタのプール722E内のアダプタの各々は、第1のクラウドインフラストラクチャ720Aによって提供された特定の製品またはリソースにマッピングされる。実際のリソースが、第1のクラウドインフラストラクチャのネイティブな制御プレーン724によって作成されるということに注意する。例えば、DBaaS（database as a service）に関して、制御プレーン724に含まれているDBaaS制御プレーンは、第1のクラウド環境の顧客のテナンシ726内のエクサデータベースリソースをインスタンス化するように構成される。

【0140】

マルチクラウドインフラストラクチャ720Bによって受信された着信要求は、認証およびアクセス制御を実行するために、権限モジュール722Aによって処理される。各要求は、第2のクラウドインフラストラクチャ内のユーザのアカウントに関連付けられたトークンを含む。権限モジュールは、このトークンを抽出し、アクティブディレクトリ712（すなわち、第2のクラウドインフラストラクチャ710Aのアイデンティティプロバイダシステム）と共に、トークンの妥当性を確認する。妥当性確認の成功時に、権限モジュール722Aは、ユーザに関連付けられたロール（すなわち、権限のセット）をチェックしてよい。ロールが、ロールに対して許可されている1つまたは複数のタスク／操作に関連付けられてよいということに注意する。1つの実施形態によれば、権限モジュール722Aは、MCCPへの着信要求を認証する役割、およびトークンに関連付けられたロールに基づいて、ユーザが要求された操作を実行することを許可されている場合に許可する役割を担う。一部の実装では、権限モジュール722Aは、サービスプラットフォーム（すなわち、第1のクラウドインフラストラクチャに関連付けられたSPLAT）のカスタム認証機能を利用することによって、前述の認証プロセスを実行してよい。SPLATは、着信要求を受け取って権限モジュール722Aに転送し、権限モジュール722Aは、着信要求をさらに構文解析して、許可決定を判定し、成功メッセージまたは失敗メッセージをSPLATに返す。成功時に、この要求がSPLATによってルーティングプロキシ722Bに渡され、一方、失敗時に、SPLATは、エラー応答を呼び出し元に直接返す。

【0141】

マルチクラウドインフラストラクチャ720Bに含まれているプロキシモジュール722B（ルーティングプロキシモジュールとも呼ばれる）は、マルチクラウドコンソール721から着信要求を受信し、この要求を、アダプタのプール722Eに含まれている特定のアダプタにルーティングするコンポーネントである。1つの実施形態によって、プロキシモジュール722Bは、第1のクラウドインフラストラクチャのサービスプラットフォーム（すなわち、SPLAT）から事前に認証された要求を受け取り、着信要求に含まれている経路情報に基づいて、この要求を適切なアダプタにルーティングする。一部の实装では、プロキシモジュール722Bは、（着信要求から）サービスのプロバイダに対応する識別子を抽出し、この要求を、アダプタのプール722E内の適切なアダプタにルーティングする。例えば、図10に示された例示的な要求を参照し、サービス1010がエクサデータベースインフラストラクチャサービスに対応するということに注意する。したがって、そのような要求は、アダプタのプール722Eに含まれているデータベースアダプタに転送される。

【0142】

マルチクラウドインフラストラクチャ720Bに含まれているクラウドリンクアダプタ722Dは、第1のクラウドインフラストラクチャによって提供されたリソースのライフサイクル操作を処理する役割を担う。クラウドリンクアダプタ722Dは、第2のクラウドインフラストラクチャのアクティブディレクトリテナント（および関連付けられたサブスクリプション）と第1のクラウドインフラストラクチャ内のユーザの対応するテナンシ／アカウントの間のマッピング（またはサインアッププロセスで作成される関係）を作成するように構成される。言い換えると、クラウドリンクアダプタ722Dは、第2のクラウドインフラストラクチャ内のユーザのアカウントに関連付けられた第2の識別子への、第1のクラウドインフラストラクチャ内のユーザのテナンシに関連付けられた第1の識別子のマッピングを生成する。

10

【0143】

一部の実装では、クラウドリンクアダプタ722Dは、外部のクラウド識別子（例えば、第2のクラウドインフラストラクチャ内のユーザのアカウントに関連付けられた第2の識別子）と（第1のクラウドインフラストラクチャ内のユーザのテナンシに関連付けられた）第1の識別子の間の変換を実行し、マルチクラウド制御プレーン722を通過する操作が、第1のクラウドインフラストラクチャ内の適切な基盤になるリソースにマッピングされることを可能にする。一部の実施形態では、クラウドリンクアダプタは、前述のマッピング情報を格納するために、データオブジェクトを生成する。さらに、クラウドリンクアダプタ722Dは、データオブジェクトに関連付けられているリソースプリンシパルも生成する。リソースプリンシパルには、要求に含まれているトークン（およびその関連付けられたロール）に基づいて1つまたは複数の許可が割り当てられる。第1のクラウドインフラストラクチャによって提供された下流のサービスへのアクセスは、リソースプリンシパルに基づいて、第2のクラウドインフラストラクチャからのユーザによって達成される。クラウドリンクアダプタ722Dは、データオブジェクトおよび関連付けられたリソースプリンシパルを、第1のクラウドインフラストラクチャ内のユーザのテナンシのルート区画に格納してよい。代替的または追加的に、クラウドリンクアダプタ722Dは、データオブジェクトおよびリソースプリンシパルを、マルチクラウドインフラストラクチャに含まれている他のアダプタによるシームレスなアクセスのために、マルチクラウドインフラストラクチャのプラットフォームサービスモジュール722Cにローカルに維持してもよい。

20

30

【0144】

ネットワークリンクモジュール（ネットワークアダプタとも呼ばれる）722Fは、（第2のクラウドインフラストラクチャ内の）顧客サブスクリプション715と（第1のクラウドインフラストラクチャ内の）対応する顧客のテナンシ／アカウント726の間のネットワークリンクを作成する役割を担う。一部の実施形態によって、ネットワークリンクモジュール722Fは、（プラットフォームサービスモジュール722Cから）トークンを取得し、（1）マルチクラウドプラットフォームデータプレーン728と顧客のテナンシ726の間の（第1のクラウド環境内の）第1のピアリング関係、および（2）第2のクラウドインフラストラクチャに含まれている顧客サブスクリプション715と第1のクラウドサービスプロバイダのサブスクリプション717の間の（第2のクラウド環境内の）第2のピアリング関係を作成する。

40

【0145】

ネットワークリンクモジュール722Fは、第1のクラウド環境と第2のクラウド環境の間のネットワーク接続を確立するようにも構成され、すなわち、ネットワークリンクモジュール722Fは、相互接続719を、2つのクラウド環境を通信可能に結合するように構成することができる。2つのクラウド環境間にネットワークリンクを形成すると、顧客のサブスクリプションにおいて（例えば、第2のクラウドインフラストラクチャのVNET内で）実行されるアプリケーションが、リソース（例えば、第1のクラウドインフラストラクチャの顧客のテナンシ726にデプロイされているエクサデータベースリソース

50

）にアクセスできるということが理解される。さらに、図 7 に示されているように、テナンシ 7 2 6 内で、遠隔測定機能が提供されている。そのような機能は、顧客のテナンシにデプロイされたリソースおよびそれらの各使用に関連する、ログ、指標、および他の性能パラメータを維持することに関連している。一部の実施形態によれば、MCCP は、第 1 のクラウド環境内の異なるリソースに関連付けられたログおよび指標をミラーリングし、指標、ログ、イベントなどを、さらなる処理のために、例えばダッシュボードに（例えば、第 2 のクラウド環境の顧客サブスクリプション 7 1 5 に含まれているアプリケーションインサイトモジュールに）公開する。

【0146】

一部の実施形態によって、マルチクラウドインフラストラクチャに含まれているプラットフォームサービスモジュール 7 2 2 C は、第 2 のクラウドインフラストラクチャに提供された第 1 のクラウドインフラストラクチャのサービスに関連付けられた認証情報を格納するように構成される。プラットフォームサービスモジュール 7 2 2 C は、アダプタが、第 1 のクラウドインフラストラクチャのネイティブな制御プレーン 7 2 4 と通信できるように、例えば、アダプタ 7 2 2 E のプールに含まれているさまざまなアダプタのトークン／リソースプリンシパルを提供する。一部の実施形態によって、プラットフォームサービスモジュール 7 2 2 C は、次のようなタスクを実行するために、さまざまなアダプタによって呼び出される API を公開する。

- ・（第 2 のクラウドインフラストラクチャによって発行された）最小限に範囲指定されたアクセストークンをアダプタに販売する。例えば、ネットワークアダプタ 7 2 2 F は、前述のネットワークピアリング操作を実行するために、アクセストークンを必要とする。

- ・下流のサービスを呼び出して第 1 のクラウドインフラストラクチャの顧客のテナンシにリソースを作成するためにアダプタが使用する、リソースプリンシパルを提供する。

- ・第 1 のクラウドインフラストラクチャから第 2 のクラウドインフラストラクチャへの可観測性データ（ログ、指標、イベント）の複製を引き起こす。

【0147】

前述したように、アダプタのプールは複数のアダプタを含み、それらのアダプタの各々は、第 1 のクラウドインフラストラクチャの固有の基盤になるリソースのセットを第 2 のクラウドインフラストラクチャのユーザに公開する役割を担い、すなわち、各アダプタは、第 1 のクラウド環境によって提供された特定の製品またはリソースにマッピングされる。例えば、エクサデータベースアダプタは、第 2 のクラウドインフラストラクチャのユーザがエクサデータベースリソースを作成して利用するための、プロキシとして機能する。エクサデータベースは、データベースを実行するためのインフラストラクチャを提供するハードウェアとソフトウェアの事前に構成された組合せである。一部の実施形態によって、エクサデータベースは、（a）エクサデータインフラストラクチャ（すなわち、ハードウェア）、（b）VM クラウドクラスタ、（c）コンテナデータベース、および（d）プラガブルデータベースという、リソースのスタックを備える。一部の実施形態によれば、マルチクラウドインフラストラクチャは、積み重ねられたインフラストラクチャのレベルの各々を分析する能力を（第 2 のクラウドインフラストラクチャのユーザに）提供する。さらに、MCCP は、ユーザが（マルチクラウドコンソール 7 2 1 を介して）ワークフローの作成コマンドを単に発行するための柔軟性を提供し、その後、MCCP は、スタックの各レベルで、個別のリソースの自動作成を実行する。図 7 に示されているように、アダプタのプール 7 2 2 F は、4 つの異なるアダプタを含んでいるが、これが MCCP アーキテクチャ 7 0 0 の範囲を全く制限していないということが、理解される。MCCP アーキテクチャは、他のアダプタ、例えば、クラウドサービスプロバイダの要求に基づいて、特定のクラウドサービスプロバイダによる使用を目的とする専用アダプタを含んでよい。

【0148】

図 8 A および図 8 B は、一部の実施形態による、異なるクラウド環境内の 2 つのユーザアカウントをリンクするための例示的なフロー図を示している。2 つのユーザアカウントは、第 1 のクラウドインフラストラクチャ内の第 1 のユーザアカウント（例えば、テナン

シ) および第2のクラウドインフラストラクチャ内の第2のユーザアカウントに対応してよい。図8Aは、2つのユーザアカウントをリンクするプロセスを示しており、最初に、ユーザのテナンシが第1のクラウドインフラストラクチャ内に作成され、次に、第2のクラウドインフラストラクチャ内のユーザのアカウントにリンクされる。図8Bは、2つのユーザアカウントをリンクするプロセスを示しており、第1のクラウドインフラストラクチャ内のユーザのテナンシがすでに作成されており、すなわち、テナンシがすでに存在する。

【0149】

図8Aは、システム管理者などの、顧客を表すユーザが、第1のクラウドインフラストラクチャにおいて提供されたサービスにサインアップするために、第2のクラウドインフラストラクチャから（第1のクラウドインフラストラクチャに含まれている）マルチクラウドインフラストラクチャへの呼び出しを行うときに実行される、データフローを示している。第2のクラウドインフラストラクチャのユーザが第1のクラウドインフラストラクチャ内でアカウントを開くため、および第1のクラウドインフラストラクチャ内のユーザのアカウントを第2のクラウドインフラストラクチャ内のユーザのアカウントにリンクするために、特殊なコンソール（本明細書では、マルチクラウドコンソールと呼ばれる）が提供されてよい。第1および第2のクラウドインフラストラクチャ内のアカウントをリンクすることによって、（第2のクラウドインフラストラクチャからの）ユーザが、第1のクラウドインフラストラクチャによって提供された1つまたは複数のサービスを利用できるようになるということに注意する。ある実装では、ユーザは、マルチクラウドコンソールを使用してサービスにサインアップする。サインアップに応答して、ユーザがマルチクラウドコンソールにログインできるようにするURLが、ユーザに送信されてよい。マルチクラウドコンソールは、第2のクラウドインフラストラクチャのUIおよびAPIに類似するUIおよびAPIを公開する。

【0150】

マルチクラウドコンソールは、第2のクラウドインフラストラクチャのユーザが、第1のクラウドインフラストラクチャ内でアカウントを開くこと、ならびに第1および第2のクラウドインフラストラクチャ内のユーザアカウントをさらにリンクすることを可能にする、ユーザ選択可能な選択肢を提供するさまざまなUI（例えば、GUI）を提供してよい。例えば、マルチクラウドコンソールは、ユーザが第1のクラウドインフラストラクチャ内でアカウント／テナンシを作成すること、および（第1のクラウドインフラストラクチャ内の）ユーザのアカウントを第2のクラウドインフラストラクチャ内のユーザのアカウントにリンクすることを可能にする、サインアップUIを提供してよい。サインアップ／リンク要求に応答して引き起こされた処理が完了した後に、それぞれのクラウドインフラストラクチャ内のユーザのアカウントが一緒にリンクされる。この処理の一部として、マルチクラウドコンソールは、ユーザ（例えば、システム管理者）が、第2のクラウドインフラストラクチャにログインし、（a）（第1のクラウドインフラストラクチャ内の）ユーザのアカウントの作成を要求すること、およびユーザのアカウントをリンクすること、または（b）ユーザが第1のクラウドインフラストラクチャ内ですでに保有しているアカウントの場合、ユーザの第1のクラウドインフラストラクチャのアカウントがユーザの第2のクラウドインフラストラクチャのアカウントにリンクされることを要求することを可能にする。

【0151】

したがって、ある使用事例では、次の2つの可能性がある。（a）ユーザが、第1のクラウドインフラストラクチャ内で既存のアカウントまたはテナンシをすでに保有しており、ユーザが、現在、マルチクラウドコンソールのサインアップUIを介して、ユーザのアカウント間にリンクが作成されることを要求している（この処理に関する詳細が、次に、図8Bを参照して説明される）、または（b）ユーザが、第1のクラウドインフラストラクチャ内の新しいアカウントの作成、および第2のクラウドインフラストラクチャ内のユーザのアカウントとの新たに作成されたアカウントのリンクの両方を要求する。この処理

に関する詳細が、次に、図 8 A を参照して説明される。アカウントのリンクは、ユーザが第 2 のクラウドを介して第 1 のクラウド内のリソースを使用することを可能にするということが、理解される。例えば、第 2 のクラウドを介して、ユーザは、第 1 のクラウド内でリソースが作成されるか、またはプロビジョニングされることを要求すること、第 1 のクラウド内のリソースを利用して管理すること、第 1 のクラウド内のリソースを削除することなどができる。

【0152】

図 8 A に示されているように、ステップ 1 で、第 1 のクラウドインフラストラクチャ内でユーザの新しいアカウントが作成され、第 2 のクラウドインフラストラクチャ内のユーザのアカウントにリンクされることを要求する、マルチクラウドコンソール（例えば、マルチクラウドコンソールのサインアップ UI）に提供されたユーザの入力に応答して、新しいアカウントを作成するために、マルチクラウドコンソールによって、（第 1 のクラウドインフラストラクチャ内の）アカウントサービスへの呼び出しが行われる。この呼び出しが、第 2 のクラウドインフラストラクチャによって生成されるトークンを含むということに注意する。第 2 のクラウドインフラストラクチャによって生成され、アカウントサービスへの呼び出しに含まれるトークンは、第 1 のクラウドインフラストラクチャ内で作成されたアカウントまたはテナンシが第 2 のクラウドインフラストラクチャ内のユーザのアカウントにリンクされることを可能にする。

【0153】

ステップ 2 で、ユーザの新しいアカウントを設定するための処理の一部として、アカウントサービスは、マルチクラウド制御プレーンに含まれている権限／プロキシモジュール（例えば、図 7 のマルチクラウドインフラストラクチャに含まれている権限モジュール 722 A）への呼び出しを行い、トークンの妥当性を確認してよい。権限／プロキシモジュールは、（図 7 を参照して前に説明されたように）トークンの妥当性を確認し、トークンの妥当性確認の成功時にのみ、さらに処理が継続してよい。トークンの妥当性確認の成功時に、アカウントサービスは、第 1 のクラウドインフラストラクチャ内のユーザの新しいアカウントを作成する。新しいアカウントを作成することの一部として、ネイティブユーザが作成され、新たに作成されたアカウントに関連付けられてよい。しかし、このネイティブユーザの認証情報が使用されないということに注意する。むしろ、第 1 のクラウドインフラストラクチャ内の（第 2 のクラウドインフラストラクチャからの）アカウントおよびそのリソースを管理するために、第 2 のクラウドインフラストラクチャ内のユーザのアイデンティティが使用される。

【0154】

第 1 のクラウドインフラストラクチャ内のアカウントサービスによって新しいアカウントが正常に作成された後に、ステップ 3 で、アカウントサービスは、（マルチクラウドインフラストラクチャに含まれている）クラウドリンクアダプタへの呼び出しを行い、第 2 のクラウドインフラストラクチャ内のユーザのアカウントと第 1 のクラウドインフラストラクチャ内の新たに作成されたアカウントの間のリンク（クラウドリンクとも呼ばれる）を作成する。ある実装では、クラウドリンクアダプタが、API をアカウントサービスに、およびマルチクラウドコンソールに公開する。これらの API は、アカウントのリンクを要求するために、アカウントサービスによって（または、マルチクラウドコンソールによって）呼び出されてよい。一部の实装では、リンクを要求する呼び出しが、ユーザによって行われず、むしろ、アカウントサービスによって開始されるため、ステップ 3 の呼び出しにトークンが含まれていないということに注意する。この場合、クラウドリンクアダプタは、アカウントサービスが、ステップ 1 で受信されたトークンを使用してアカウントを設定するための処理の一部として、ユーザに対して必要な認証をすでに実行しているということを信頼するため、別のトークンを必要とする別の認証を行わない。

【0155】

一部の实装では、2 つのアカウントをリンクするためにクラウドリンクアダプタによってステップ 3 で実行される処理は、以下を含む。

(a) クラウドリンクアダプタが、リンクされている2つのアカウントを識別するメタデータ情報を格納するためのデータオブジェクト（本明細書では、クラウドリンクリソースオブジェクトとも呼ばれる）を作成する。例えば、データオブジェクトは、第1のクラウドインフラストラクチャ内に作成されたテナンシ（すなわち、アカウント）に関連付けられた第1の識別子、および第2のクラウドサービスプロバイダを使用してユーザのアカウントに関連付けられた第2の識別子のマッピングを含んでいるメタデータ情報を格納する。

(b) クラウドリンクアダプタが、第1のクラウドインフラストラクチャ側でリソースを格納し、含むための新しい区画を作成し、ユーザは、この区画を、マルチクラウドコンソールを使用して管理することができる／管理する。一部の実装では、クラウドリンクリソースオブジェクトは、第1のクラウドインフラストラクチャ内の顧客のアカウントのルートに作成される。

(c) クラウドリンクアダプタが、第2のクラウドインフラストラクチャのユーザによって使用されるのが望ましいリソースに関して、新しいリソースプリンシパル（本明細書では、クラウドリンクリソースプリンシパルと呼ばれる）を作成する。

(d) クラウドリンクアダプタが、アクティブディレクトリ（例えば、図7に示されているような第2のクラウドインフラストラクチャのアクティブディレクトリ712）への第1のクラウドインフラストラクチャ内のドメインのリンクを容易にする1つまたは複数のフェデレーション設定を実行してよい。第1のクラウドインフラストラクチャおよび第2のクラウドインフラストラクチャのアカウントをフェデレートするプロセスは、第2のクラウドインフラストラクチャ内のユーザ／ユーザのグループが第1のクラウドインフラストラクチャ内で認証されること、および第1のクラウドインフラストラクチャからのユーザ／グループが第2のクラウドインフラストラクチャ内へ認証されることを可能にする。

【0156】

ある実装では、第2のクラウドインフラストラクチャのアカウントにおけるユーザの認証情報／トークンに基づいて、許可がクラウドリンクリソースプリンシパルに関連付けられる。ユーザが、マルチクラウドコンソールを使用して新しいアカウントを要求するか、または第1のクラウドインフラストラクチャ内のユーザのアカウントが第2のクラウドインフラストラクチャ内のユーザのアカウントにリンクされることを要求するときに、ユーザによって、リソースプリンシパルを設定することに対する同意が提供される。さらに、ステップ4に示されているように、ユーザが第2のクラウドインフラストラクチャから下流のサービス（例えば、第1のクラウドインフラストラクチャによって提供された1つまたは複数のサービス）を利用できるようにするために、クラウドリンクリソースプリンシパルが下流のサービスに送信される。

【0157】

図8Bを参照すると、第1のクラウドインフラストラクチャ内の既存のアカウントまたはテナンシを第2のクラウドインフラストラクチャ内のユーザのアカウントにリンクすることに関連する処理が示されている。図8Bに示されているように、ユーザは、マルチクラウドコンソールによって提供されたサインアップUIを介して、第1のクラウドインフラストラクチャおよび第2のクラウドインフラストラクチャ内のユーザのアカウントがリンクされることを要求する。それに応じて、ステップ1で、マルチクラウドコンソールがクラウドリンクアダプタへの呼び出しを行い、アカウントをリンクする。そのような呼び出しは、クラウドリンクアダプタによってサインアップUIに公開されたAPIのうちの1つを使用して行われてよい。ある実装では、ステップ1でクラウドリンクアダプタに渡される情報は、第2のクラウドインフラストラクチャ内のユーザのアカウントおよびさらに第1のクラウドインフラストラクチャ内のユーザのアカウントを識別する情報、第2のクラウドインフラストラクチャによって発行されたトークンなどを含む。

【0158】

ステップ2で、クラウドリンクアダプタは、マルチクラウドインフラストラクチャに含まれている権限／プロキシモジュールへの呼び出しを行い、ステップ1で受信されたト

10

20

30

40

50

クンを認証する。この認証の一部として、権限／プロキシモジュールは、要求を行っているユーザが、第2のクラウドインフラストラクチャ側でリンク要求を行うための十分な権限を持っているかどうかを判定する。この妥当性確認の一部として、第2のクラウドインフラストラクチャ側でのロールおよび許可設定がチェックされてよい。ユーザの妥当性確認が成功することに応答して、クラウドリンクアダプタは、ユーザのために前に作成されたデータオブジェクトから、ユーザによって利用されるのが望ましいリソースに関連付けられたリソースプリンシパルを取り出す。さらに、ステップ3に示されているように、ユーザが第2のクラウドインフラストラクチャから下流のサービス（例えば、第1のクラウドインフラストラクチャによって提供された1つまたは複数のサービス）を利用できるようにするために、クラウドリンクリソースプリンシパルが下流のサービスに送信される。

10

【0159】

図9は、一部の実施形態による、マルチクラウド制御プレーン（MCCP）のコンポーネントを示す例示的なシステム図を示している。MCCP900は、サービスプラットフォーム（SPLAT）910、ルーティングプロキシ915、クラウドリンクアダプタ920、データベースアダプタ925、ネットワークアダプタ930、およびMCCPプラットフォーム935を含む。図8Aおよび図8Bを参照して上で説明されたように、ユーザがサインアッププロセスを正常に完了すると、ユーザは、マルチクラウドコンソール905を利用して、第1のクラウドインフラストラクチャ内のユーザのテナンシにおけるリソースにアクセスするか、リソースを作成するか、または更新するためのコマンドを発行してよい。説明の目的で、以下では、ユーザがマルチクラウドコンソールを利用して、エクサデータベースリソースを作成する要求を発行する状況が説明されている。

20

【0160】

一部の実装では、ユーザが、マルチクラウドコンソール905にアクセスし、ログイン情報、例えば、第2のクラウドインフラストラクチャ内のユーザの認証情報を提供する。マルチクラウドコンソール905は、例えば、リソースの作成、リソースへのアクセス、リソースの更新などの、複数の選択肢を提供する。そのような選択肢は、マルチクラウドコンソール905内の選択可能なアイコン（例えば、ボタン）の形態でユーザに提供されてよい。ユーザが（例えば、リソースを作成するための）選択を実行すると、サービスプラットフォーム910へのAPI呼び出しが引き起こされる。サービスプラットフォーム910に対して行われる要求が、第1のクラウドインフラストラクチャに関するネイティブな呼び出しでないということが理解される。むしろ、この呼び出しは、第2のクラウドインフラストラクチャ内のユーザに関連付けられたトークンを含む許可ヘッダーを含んでいるREST型の呼び出しである。

30

【0161】

トークンを含んでいるREST呼び出しが、認証動作およびアクセス制御動作を実行するルーティングプロキシモジュール915にさらに転送される。一部の実施形態によれば、ルーティングプロキシモジュール915は、REST呼び出しに含まれているトークンを抽出することによって、認証動作を実行する。ルーティングプロキシモジュール915は、署名（要求に署名するために使用される）を、第2のクラウドインフラストラクチャの公開されている署名と比較することによって、トークンの妥当性を確認し、要求が第2のクラウドインフラストラクチャに関連付けられた有効な顧客から生じていることを保証する。さらに、ルーティングプロキシモジュール915は、ロール、すなわち、トークンに関連付けられた権限をチェックしてもよく、例えば、ロールがエクサデータDB管理者に対応するかどうかなどをチェックしてもよい。ロールに基づいて、ルーティングプロキシモジュール915は、要求をMCCPフレームワーク900に含まれている適切なアダプタにルーティングしてよい。

40

【0162】

1つの実施形態によれば、ルーティングプロキシモジュール915は、（トークンに関連付けられた）ロールを、公開されて（API仕様の一部として）アダプタの各々に割り当てられたロールの事前に構成されたリストと比較する。例えば、トークンに関連付けら

50

れたロールが「エクサデータDB管理者」に対応する場合、要求は、エクサデータベースを作成する要求として理解されてよく、したがって要求が、データベースアダプタ925に転送される。さらに、一部の実施形態によって、ルーティングプロキシモジュール915は、プロバイダID、要求されたリソースの種類などの、REST呼び出しに含まれている情報を分析してよく、分析された情報に基づいて、ルーティングプロキシモジュール915は、要求を適切なアダプタに転送してよい。

【0163】

一部の実装では、ルーティングプロキシモジュール915によって取得された要求は、リソースがデプロイされるべきである第1のクラウドインフラストラクチャ内のユーザのテナンシを識別する情報を含まなくてよい。したがって、ルーティングプロキシモジュール915は、クラウドリンクアダプタ920と通信し、第1のクラウドインフラストラクチャ内のユーザのテナンシへの、第2のクラウドインフラストラクチャ内のユーザのアカウントのマッピング情報を取得する。マッピング情報が存在する場合、ルーティングプロキシモジュール915は、第1のクラウドインフラストラクチャ内のユーザのテナンシに関する情報を取得し、この情報をデータベースアダプタ925に渡す。このようにして、データベースアダプタ925は、リソースが作成／デプロイされるべきである第1のクラウドインフラストラクチャ内のユーザのテナンシを認識する。しかし、クラウドリンクアダプタ920が、マッピング情報が存在しないということを決定した場合、ルーティングプロキシモジュール915は、データベースリソースを作成する要求に対する応答として、ユーザに返信される「許可されないアクセス」メッセージを単に発行してよい。

【0164】

一部の実装では、クラウドリンクアダプタ920が、リンクされている2つのアカウントを識別するメタデータ情報を格納するためのデータオブジェクト（本明細書では、クラウドリンクリソースオブジェクトと呼ばれる）を作成するということに注意する。例えば、データオブジェクトは、第1のクラウドインフラストラクチャ内のテナンシ（すなわち、アカウント）に関連付けられた第1の識別子、および第2のクラウドサービスプロバイダを使用してユーザのアカウントに関連付けられた第2の識別子のマッピングを含んでいるメタデータ情報を格納する。さらに、クラウドリンクアダプタ920が、第2のクラウドインフラストラクチャのユーザによって作成／管理されるのが望ましいリソース（例えば、データベース）に関して、リソースプリンシパル（本明細書では、クラウドリンクリソースプリンシパルと呼ばれる）も作成する。クラウドリンクアダプタ920は、データオブジェクトおよびリソースプリンシパルを、第1のクラウドインフラストラクチャ内のユーザのテナンシのルート区画内で維持してよい。一部の実施形態では、クラウドリンクアダプタ920は、MCCPプラットフォーム935内のデータオブジェクトおよび／またはリソースプリンシパルをローカルに維持してもよい。

【0165】

一部の実施形態では、データベースアダプタ925は、ネットワークアダプタ930と通信し（またはネットワークアダプタ930に指示し）、第2のクラウドインフラストラクチャ内のユーザのアカウントと第1のクラウドインフラストラクチャ内のユーザのテナンシの間のネットワークリンクを作成してよい。例えば、ネットワークアダプタ930は、第2のクラウドインフラストラクチャモジュール945内のネイティブなサービスから、ユーザに関連付けられたトークンを取得し、（1）MCCPのデータプレーンと第1のクラウドインフラストラクチャ内のユーザのテナンシの間の（第1のクラウド環境内の）第1のピアリング関係、および（2）第2のクラウドインフラストラクチャに含まれているユーザのアカウントと第1のクラウドプロバイダのサブスクリプションの間の（第2のクラウド環境内の）第2のピアリング関係を作成してよい。

【0166】

ネットワークアダプタ930は、第1のクラウドインフラストラクチャと第2のクラウドインフラストラクチャの間のネットワーク接続を確立するようにも構成され、すなわち、ネットワークアダプタ930は、2つのクラウド環境を通信可能に結合する相互接続（

例えば、図 7 の相互接続 7 1 9) を構成することができる。第 1 のクラウドインフラストラクチャ内のユーザのテナンシと第 2 のクラウドインフラストラクチャ内のユーザのアカウントの間にネットワークリンクを形成すると、ユーザのサブスクリプション／アカウントにおいて実行されるアプリケーションが、リソース、例えば、第 1 のクラウドインフラストラクチャのテナンシにデプロイされたエクサデータベースにアクセスできるということが、理解される。さらに、ピアリング関係の作成は、第 2 のクラウドインフラストラクチャ内で、例えば、第 2 のクラウドインフラストラクチャ内のユーザのサブスクリプションにおいて実行されるダッシュボードアプリケーションにおいて、アクセスできるように、指標、例えば、データベース使用量指標をプロビジョニングする。

【0167】

一部の実装では、データベースアダプタ 9 2 5 は、MCCP プラットフォーム 9 3 5 内でローカルに維持されているリソースプリンシパルを取得してよい。データベースアダプタ 9 2 5 は、(リソースプリンシパルを含んでいる) 要求を、第 1 のクラウドインフラストラクチャ 9 4 0 に含まれている 1 つまたは複数の下流のサービスに送信し、第 1 のクラウドインフラストラクチャ内のユーザのテナンシにリソースを作成してよい。言い換えると、第 1 のクラウドインフラストラクチャ 9 4 0 に含まれている下流のサービスは、アイデンティティを利用し、すなわち、要求されたリソース (例えば、第 1 のクラウドインフラストラクチャ内のユーザのテナンシにおけるエクサデータベース) を作成／デプロイするために MCCP プラットフォーム 9 3 5 から取得されたリソースプリンシパルを利用する。ユーザが、エクサデータベースを作成する要求を発行すると、ユーザは、MCCP 9 0 0 を断続的にポーリングし、要求の状態を取得してよい。第 1 のクラウドインフラストラクチャ 9 4 0 の下流のサービスが、第 1 のクラウドインフラストラクチャ内のユーザのテナンシにリソースを作成し、ネットワークアダプタ 9 3 0 がピアリング関係を確立すると、MCCP 9 0 0 は、要求の正常な完了に関してユーザに通知してよい。

【0168】

図 1 0 は、一部の実施形態による、マルチクラウドインフラストラクチャによって受信された例示的な要求を示している。詳細には、図 1 0 は、マルチクラウドコンソールからマルチクラウドインフラストラクチャによって受信された要求 1 0 0 0 を示している。要求 1 0 0 0 は、第 1 のクラウドインフラストラクチャ内のユーザのテナンシ内にリソースを作成することをマルチクラウドインフラストラクチャによって要求されたメタデータ情報を含む。このメタデータ情報は、(a) 第 2 のクラウドインフラストラクチャ内のユーザのサブスクリプション (例えば、アカウント) (およびリソースグループ情報) を識別する情報 1 0 0 5、(b) サービスのプロバイダを識別する情報 1 0 1 0、および (c) 第 2 のクラウドインフラストラクチャのユーザによって利用されるのが望ましいリソースの種類 1 0 1 5 を含んでよい。

【0169】

一部の実装では、要求 1 0 0 0 は、マルチクラウドインフラストラクチャのプロキシモジュール (例えば、図 7 のプロキシ 7 2 2 B) によって受信される。プロキシモジュールは、要求 (例えば、図 1 0 に示されているように、エクサデータベースを作成する要求) を受信すると、前述したように、第 2 のクラウドインフラストラクチャによって生成されたトークンに基づいてユーザの妥当性を確認してよい。妥当性確認の成功時に、一部の实装では、プロキシモジュールは、要求において取得された情報を、マルチクラウドインフラストラクチャに含まれているアダプタのプールに含まれている対応する (例えば、要求されたサービスに対応する) アダプタに渡す。例えば、図 1 0 の要求 1 0 0 0 は、プロキシモジュールによって、マルチクラウドインフラストラクチャに含まれているデータベースアダプタに向けられてよい。次に、データベースアダプタは、要求を受信すると、第 2 のクラウドインフラストラクチャ内のユーザのアカウントと第 1 のクラウドインフラストラクチャ内のユーザに関連付けられたテナンシの間のマッピングに関連するマッピング情報を取得するために、マルチクラウドインフラストラクチャのクラウドリンクアダプタへの呼び出しを行ってよい。

10

20

30

40

50

【0170】

マッピング情報が存在しない場合、クラウドリンクアダプタがユーザの要求1000を拒否するという事に注意する。これに対して、マッピング情報が存在する場合、クラウドリンクアダプタは、マッピング情報（およびリソースに関連付けられたリソースプリンシパル）をデータベースアダプタに提供し、その後、データベースアダプタは、要求を下流のサービス、例えばDBaaS（database-as-a-service）に発行して、この要求を実行する。

【0171】

図11は、ある実施形態による、マルチクラウドインフラストラクチャによって実行されるステップを示す例示的なフローチャートを示している。図11に示された処理は、それぞれのシステムの1つまたは複数の処理ユニット（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）、ハードウェア、またはこれらの組合せにおいて実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。図11に提示され、下で説明される方法は、例示的かつ非限定的であるよう意図されている。図11は、特定のシーケンスまたは順序で発生するさまざまな処理ステップを示しているが、これは、限定することを意図されていない。ある代替の実施形態では、これらのステップは、何らかの異なる順序で実行されてよく、または一部のステップは、並列に実行されてもよい。

【0172】

プロセスがステップ1105で開始し、ステップ1105で、第1のクラウドサービスプロバイダが、第1のクラウドインフラストラクチャを使用して1つまたは複数のクラウドサービスのセットを提供する。ステップ1110で、第1のクラウドインフラストラクチャ内でマルチクラウドインフラストラクチャが提供される。マルチクラウドインフラストラクチャは、第2のクラウドサービスプロバイダでのアカウントに関連付けられたユーザが、第2のクラウドインフラストラクチャから、1つまたは複数のクラウドサービスのセットからの第1のサービスを使用することを可能にする。言い換えると、マルチクラウドインフラストラクチャは、他のクラウドサービスプロバイダのユーザが、ユーザのネイティブなクラウド環境から、第1のクラウドインフラストラクチャによって提供された1つまたは複数のクラウドサービスを利用するためのゲートウェイを形成する。第1のサービスが、第1のクラウドインフラストラクチャに（例えば、第1のクラウドインフラストラクチャ内でユーザに関連付けられて作成されたテナンシに）デプロイされるデータベースリソースを作成して利用することに対応してよいということが理解される。

【0173】

次に、プロセスがステップ1115に移動し、ステップ1115で、ユーザが第1のサービスを使用できるようにするために、マルチクラウドインフラストラクチャが、第2のクラウドサービスプロバイダでの（ユーザの）アカウントと第1のクラウドインフラストラクチャ内に作成されたテナンシの間のリンクを作成する。一部の実装では、マルチクラウドインフラストラクチャは、リンクに対応するメタデータ情報を格納するデータオブジェクトを生成する。メタデータ情報は、第1のクラウドインフラストラクチャ内に作成されたテナンシに関連付けられた第1の識別子、および第2のクラウドサービスプロバイダでの（ユーザの）アカウントに関連付けられた第2の識別子のマッピングを含んでよい。

【0174】

クラウドインフラストラクチャの例

前述したように、IaaS（infrastructure as a service）は、クラウドコンピューティングの1つの特定の種類である。IaaSは、パブリックネットワーク（例えば、インターネット）を経由して仮想化されたコンピューティングリソースを提供するように構成され得る。IaaSモデルでは、クラウドコンピューティングプロバイダは、インフラストラクチャコンポーネント（例えば、サーバ、ストレージデバイス、ネットワークノード（例えば、ハードウェア）、デプロイメントソフトウェア、プラットフォーム仮想化（例えば、ハイパーバイザレイヤ）など）をホストすることができる。場合によっては、

IaaSプロバイダは、それらのインフラストラクチャコンポーネントに付随して生じるように、さまざまなサービス（例えば、請求書送付、監視、ロギング、セキュリティ、ロードバランシング、およびクラスタ化など）を提供してもよい。したがって、これらのサービスはポリシー主導であることができるため、IaaSユーザは、ロードバランシングを駆動してアプリケーションの可用性および性能を維持するようにポリシーを実装することができる。

【0175】

場合によっては、IaaSの顧客は、インターネットなどの広域ネットワーク（WAN）を介してリソースおよびサービスにアクセスしてよく、クラウドプロバイダのサービスを使用して、アプリケーションスタックの残りの要素をインストールすることができる。例えば、ユーザは、IaaSプラットフォームにログインして、仮想マシン（VM）を作成し、オペレーティングシステム（OS）を各VMにインストールし、データベースなどのミドルウェアをデプロイし、ワークロードおよびバックアップのためのストレージバケットを作成し、企業ソフトウェアをVMにインストールすることもできる。次に、顧客は、プロバイダのサービスを使用して、ネットワークトラフィックをバランス調整すること、アプリケーションの問題をトラブルシューティングすること、性能を監視すること、災害復旧を管理することなどを含む、さまざまな機能を実行することができる。

【0176】

ほとんどの場合、クラウドコンピューティングモデルは、クラウドプロバイダの参加を必要とする。クラウドプロバイダは、IaaSを提供する（例えば、提供する、貸し出す、販売する）ことを専門とするサードパーティサービスであってよいが、そうである必要はない。実体は、プライベートクラウドをデプロイし、インフラストラクチャサービスのそれ自身のプロバイダになることを選択してもよい。

【0177】

一部の例では、IaaSのデプロイメントは、新しいアプリケーションまたは新しいバージョンのアプリケーションを、準備されたアプリケーションサーバなどにつなぐプロセスである。このプロセスは、サーバを準備する（例えば、ライブラリ、デーモンなどをインストールする）プロセスを含んでもよい。このプロセスは、多くの場合、ハイパーバイザレイヤ（例えば、サーバ、ストレージ、ネットワークハードウェア、および仮想化）の下でクラウドプロバイダによって管理される。したがって、顧客は、（例えば、（例えば、オンデマンドでスピンアップされ得る）セルフサービス仮想マシンなどの上の）OS、ミドルウェア、および／またはアプリケーションのデプロイメントを処理する役割を担ってよい。

【0178】

一部の例では、IaaSのプロビジョニングは、コンピュータまたは仮想ホストを使用のために取得すること、および必要とされるライブラリまたはサービスをそれらのコンピュータまたは仮想ホストにインストールすることも、指してよい。ほとんどの場合、デプロイメントはプロビジョニングを含まず、プロビジョニングは、最初に行われる必要があることがある。

【0179】

場合によっては、IaaSのプロビジョニングには2つの異なる課題が存在する。第一に、何かが実行される前に、インフラストラクチャの初期セットをプロビジョニングするという最初の課題がある。第二に、すべてがプロビジョニングされた後に、既存のインフラストラクチャを発達させるという（例えば、新しいサービスを追加する、サービスを変更する、サービスを除去するなどの）課題がある。場合によっては、これらの2つの課題は、インフラストラクチャの構成が宣言的に定義されることを可能にすることによって対処されてよい。言い換えると、インフラストラクチャ（例えば、どのコンポーネントが必要とされるか、およびそれらのコンポーネントがどのように情報をやりとりするか）が、1つまたは複数の構成ファイルによって定義され得る。このようにして、インフラストラクチャのトポロジー全体（例えば、どのリソースがどのリソースに依存するか、およびそ

これらの各リソースがどのように連携するか)が、宣言的に記述され得る。場合によっては、トポロジーが定義された後に、構成ファイルに記述されたさまざまなコンポーネントを作成および／または管理するワークフローが生成され得る。

【0180】

一部の例では、インフラストラクチャは、多くの相互接続された要素を含んでよい。例えば、コアネットワークとしても知られている1つまたは複数の仮想プライベートクラウド(VPC: virtual private clouds)(例えば、構成可能な、および／または共有されたコンピューティングリソースの、場合によってはオンデマンドのプール)が存在してよい。一部の例では、ネットワークのセキュリティがどのように設定されるかを定義するためにプロビジョニングされた1つまたは複数のセキュリティグループルール、および1つまたは複数の仮想マシン(VM)が存在してもよい。ロードバランサ、データベースなどの他のインフラストラクチャ要素がプロビジョニングされてもよい。より多くのインフラストラクチャ要素が望まれ、かつ／または追加されるにつれて、インフラストラクチャが徐々に発達することができる。

【0181】

場合によっては、さまざまな仮想コンピューティング環境にわたってインフラストラクチャコードのデプロイメントを可能にするために、継続的デプロイメント技術が採用されてよい。さらに、説明された技術は、これらの環境内のインフラストラクチャ管理を可能にすることができる。一部の例では、サービスチームは、1つまたは複数の、ただし多くの場合は多数の、(例えば、さまざまな地理的位置にわたって、ときには世界全体にわたって)異なる実稼働環境にデプロイされるのが望ましいコードを記述する可能性がある。しかし、一部の例では、コードがデプロイされるインフラストラクチャは、最初に設定されなければならない。場合によっては、プロビジョニングが手動で行われることが可能であり、リソースをプロビジョニングするためにプロビジョニングツールが利用されてよく、かつ／またはインフラストラクチャがプロビジョニングされた後に、コードをデプロイするためにデプロイメントツールが利用されてよい。

【0182】

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は、仮想クラウドネットワーク(VCN)1206およびセキュアホストサブネット1208を含むことができるセキュアホストテナンシ1204に通信可能に結合され得る。一部の例では、サービスオペレータ1202は、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てよく、クライアントコンピューティングデバイスは、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などのさまざまなモバイルオペレーティングシステムを実行している、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: short message service)、Blackberry(登録商標)、または他の通信プロトコルが有効化されている、ポータブルハンドヘルドデバイス(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、パーソナルデジタルアシスタント(PDA: personal digital assistant))または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)であってよい。代替として、クライアントコンピューティングデバイスは、例として、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のさまざまなバージョンを実行し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コンピュータを含む、汎用パーソナルコンピュータであることができる。クライアントコンピューティングデバイスは、例えばGoogle Chrome OSなどの、さまざまなGNU/Linuxオペレーティングシステムを含むが、これらに限定されない、さまざまな市販されている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実行しているワークステーションコンピュータであることができる。代替または追加として、クライアントコンピューティングデバイスは、

V C N 1 2 0 6 にアクセスできるネットワークおよび／またはインターネットを経由して通信することができる、シンクライアントコンピュータ、インターネット対応のゲーミングシステム（例えば、Kinect（登録商標）ジェスチャー入力デバイスを含むか、または含まないMicrosoft Xboxゲーム機）、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ってよい。

【0183】

V C N 1 2 0 6 は、S S H V C N 1 2 1 2 に含まれているL P G 1 2 1 0 を介してセキュアシェル（S S H）V C N 1 2 1 2 に通信可能に結合され得る、ローカルピアリングゲートウェイ（L P G）1 2 1 0 を含むことができる。S S H V C N 1 2 1 2 はS S H サブネット1 2 1 4 を含むことができ、S S H V C N 1 2 1 2 は、制御プレーンV C N 1 2 1 6 に含まれているL P G 1 2 1 0 を介して、制御プレーンV C N 1 2 1 6 に通信可能に結合され得る。また、S S H V C N 1 2 1 2 は、L P G 1 2 1 0 を介して、データプレーンV C N 1 2 1 8 に通信可能に結合され得る。制御プレーンV C N 1 2 1 6 およびデータプレーンV C N 1 2 1 8 は、I a a S プロバイダによって所有および／または操作され得るサービステナンシ1 2 1 9 に含まれ得る。

10

【0184】

制御プレーンV C N 1 2 1 6 は、境界ネットワーク（例えば、企業イントラネットと外部ネットワークの間の企業ネットワークの一部）として機能する制御プレーン非武装ゾーン（D M Z : demilitarized zone）層1 2 2 0 を含むことができる。D M Z に基づくサーバは、制限された責任を有し、セキュリティ侵害を封じ込められた状態に保つのに役立つことができる。さらに、D M Z 層1 2 2 0 は、1 つまたは複数のロードバランサ（L B : load balancer）サブネット1 2 2 2 、アプリサブネット1 2 2 6 を含むことができる制御プレーンアプリ層1 2 2 4 、データベース（D B : database）サブネット1 2 3 0 （例えば、フロントエンドD B サブネットおよび／またはバックエンドD B サブネット）を含むことができる制御プレーンデータ層1 2 2 8 を含むことができる。制御プレーンD M Z 層1 2 2 0 に含まれているL B サブネット1 2 2 2 は、制御プレーンV C N 1 2 1 6 に含まれ得る制御プレーンアプリ層1 2 2 4 に含まれているアプリサブネット1 2 2 6 およびインターネットゲートウェイ1 2 3 4 に通信可能に結合されることが可能であり、アプリサブネット1 2 2 6 は、制御プレーンデータ層1 2 2 8 に含まれているD B サブネット1 2 3 0 ならびにサービスゲートウェイ1 2 3 6 およびネットワークアドレス変換（N A T）ゲートウェイ1 2 3 8 に通信可能に結合され得る。制御プレーンV C N 1 2 1 6 は、サービスゲートウェイ1 2 3 6 およびN A T ゲートウェイ1 2 3 8 を含むことができる。

20

30

【0185】

制御プレーンV C N 1 2 1 6 は、アプリサブネット1 2 2 6 を含むことができるデータプレーンミラーアプリ層1 2 4 0 を含むことができる。データプレーンミラーアプリ層1 2 4 0 に含まれているアプリサブネット1 2 2 6 は、計算インスタンス1 2 4 4 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（V N I C : virtual network interface controller）1 2 4 2 を含むことができる。計算インスタンス1 2 4 4 は、データプレーンミラーアプリ層1 2 4 0 のアプリサブネット1 2 2 6 を、データプレーンアプリ層1 2 4 6 に含まれ得るアプリサブネット1 2 2 6 に通信可能に結合することができる。

40

【0186】

データプレーンV C N 1 2 1 8 は、データプレーンアプリ層1 2 4 6 、データプレーンD M Z 層1 2 4 8 、およびデータプレーンデータ層1 2 5 0 を含むことができる。データプレーンD M Z 層1 2 4 8 は、データプレーンアプリ層1 2 4 6 のアプリサブネット1 2 2 6 およびデータプレーンV C N 1 2 1 8 のインターネットゲートウェイ1 2 3 4 に通信可能に結合され得るL B サブネット1 2 2 2 を含むことができる。アプリサブネット1 2 2 6 は、データプレーンV C N 1 2 1 8 のサービスゲートウェイ1 2 3 6 およびデータプレーンV C N 1 2 1 8 のN A T ゲートウェイ1 2 3 8 に通信可能に結合され得る。データ

50

プレーンデータ層 1 2 5 0 は、データプレーンアプリ層 1 2 4 6 のアプリサブネット 1 2 2 6 に通信可能に結合され得る DB サブネット 1 2 3 0 を含むこともできる。

【 0 1 8 7 】

制御プレーン V C N 1 2 1 6 の、およびデータプレーン V C N 1 2 1 8 のインターネットゲートウェイ 1 2 3 4 は、パブリックインターネット 1 2 5 4 に通信可能に結合され得るメタデータ管理サービス 1 2 5 2 に通信可能に結合され得る。パブリックインターネット 1 2 5 4 は、制御プレーン V C N 1 2 1 6 の、およびデータプレーン V C N 1 2 1 8 の N A T ゲートウェイ 1 2 3 8 に通信可能に結合され得る。制御プレーン V C N 1 2 1 6 の、およびデータプレーン V C N 1 2 1 8 のサービスゲートウェイ 1 2 3 6 は、クラウドサービス 1 2 5 6 に通信可能に結合され得る。

10

【 0 1 8 8 】

一部の例では、制御プレーン V C N 1 2 1 6 の、またはデータプレーン V C N 1 2 1 8 のサービスゲートウェイ 1 2 3 6 は、パブリックインターネット 1 2 5 4 を通らずに、クラウドサービス 1 2 5 6 へのアプリケーションプログラミングインターフェイス (A P I : application programming interface) 呼び出しを行うことができる。サービスゲートウェイ 1 2 3 6 からクラウドサービス 1 2 5 6 への A P I 呼び出しは、一方向であることができ、サービスゲートウェイ 1 2 3 6 は、クラウドサービス 1 2 5 6 への A P I 呼び出しを行うことができ、クラウドサービス 1 2 5 6 は、要求されたデータをサービスゲートウェイ 1 2 3 6 に送信することができる。しかし、クラウドサービス 1 2 5 6 は、サービスゲートウェイ 1 2 3 6 への A P I 呼び出しを開始しなくてよい。

20

【 0 1 8 9 】

一部の例では、セキュアホストテナンシ 1 2 0 4 は、サービステナンシ 1 2 1 9 に直接接続されることが可能であり、そうでなければ、分離されてよい。セキュアホストサブネット 1 2 0 8 は、 L P G 1 2 1 0 を介して S S H サブネット 1 2 1 4 と通信することができ、 L P G 1 2 1 0 は、そうしないと分離されたシステム上で、双方向通信を可能にすることができる。セキュアホストサブネット 1 2 0 8 を S S H サブネット 1 2 1 4 に接続することは、セキュアホストサブネット 1 2 0 8 に、サービステナンシ 1 2 1 9 内の他の実体へのアクセスを与えてよい。

【 0 1 9 0 】

制御プレーン V C N 1 2 1 6 は、サービステナンシ 1 2 1 9 のユーザが、望ましいリソースを設定するか、またはそうでなければ、プロビジョニングすることを可能にしてよい。制御プレーン V C N 1 2 1 6 内でプロビジョニングされた望ましいリソースは、データプレーン V C N 1 2 1 8 においてデプロイされるか、またはそうでなければ、使用されてよい。一部の例では、制御プレーン V C N 1 2 1 6 は、データプレーン V C N 1 2 1 8 から分離されることが可能であり、制御プレーン V C N 1 2 1 6 のデータプレーンミラーアプリ層 1 2 4 0 は、データプレーンミラーアプリ層 1 2 4 0 およびデータプレーンアプリ層 1 2 4 6 に含まれ得る V N I C 1 2 4 2 を介して、データプレーン V C N 1 2 1 8 のデータプレーンアプリ層 1 2 4 6 と通信することができる。

30

【 0 1 9 1 】

一部の例では、システムのユーザまたは顧客は、要求をメタデータ管理サービス 1 2 5 2 に伝達することができるパブリックインターネット 1 2 5 4 を介して、要求、例えば、作成、読み取り、更新、または削除 (C R U D : create, read, update, or delete) 操作を行うことができる。メタデータ管理サービス 1 2 5 2 は、インターネットゲートウェイ 1 2 3 4 を介して、要求を制御プレーン V C N 1 2 1 6 に伝達することができる。要求は、制御プレーン D M Z 層 1 2 2 0 に含まれている L B サブネット 1 2 2 2 によって受信され得る。L B サブネット 1 2 2 2 は、要求が有効であるということを決定してよく、この決定に応答して、L B サブネット 1 2 2 2 は、要求を、制御プレーンアプリ層 1 2 2 4 に含まれているアプリサブネット 1 2 2 6 に送信することができる。要求の妥当性が確認され、要求がパブリックインターネット 1 2 5 4 への呼び出しを必要とする場合、パブリックインターネット 1 2 5 4 への呼び出しが、パブリックインターネット 1 2 5 4 への

40

50

呼び出しを行うことができるNATゲートウェイ1238に送信されてよい。要求によって格納されるのが望ましいことがあるメモリが、DBサブネット1230内で格納される。

【0192】

一部の例では、データプレーンミラーアプリ層1240は、制御プレーンVCN1216とデータプレーンVCN1218の間の直接通信を容易にすることができる。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VCN1218に含まれているリソースに適用されるのが望ましいことがある。VNIC1242を介して、制御プレーンVCN1216は、データプレーンVCN1218に含まれているリソースと直接通信し、それによって、リソースの構成に対する変更、更新、または他の適切な修正を実行することができる。

10

【0193】

一部の実施形態では、制御プレーンVCN1216およびデータプレーンVCN1218は、サービステナンシ1219に含まれ得る。この場合、システムのユーザまたは顧客は、制御プレーンVCN1216またはデータプレーンVCN1218のいずれかを、所有することも、操作することも行わなくてよい。代わりに、IaaSプロバイダが、両方ともサービステナンシ1219に含まれ得る制御プレーンVCN1216およびデータプレーンVCN1218を所有するか、または操作してよい。この実施形態は、ユーザまたは顧客が他のユーザのリソースまたは他の顧客のリソースと情報をやりとりするのを防ぐことができる、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、格納のために、望ましいレベルのセキュリティを有さないことがあるパブリックインターネット1254に頼ることを必要とせずに、データベースをプライベートに格納することを可能にしてよい。

20

【0194】

他の実施形態では、制御プレーンVCN1216に含まれているLBサブネット1222は、サービスゲートウェイ1236から信号を受信するように構成され得る。この実施形態では、制御プレーンVCN1216およびデータプレーンVCN1218は、パブリックインターネット1254を呼び出さずに、IaaSプロバイダの顧客によって呼び出されるように構成されてよい。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ることがあり、パブリックインターネット1254から分離され得るサービステナンシ1219に格納されることがあるため、この実施形態を望むことがある。

30

【0195】

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12のサービスオペレータ1202）は、仮想クラウドネットワーク（VCN）1306（例えば、図12のVCN1206）およびセキュアホストサブネット1308（例えば、図12のセキュアホストサブネット1208）を含むことができるセキュアホストテナンシ1304（例えば、図12のセキュアホストテナンシ1204）に通信可能に結合され得る。VCN1306は、セキュアシェル（SSH）VCN1312に含まれているローカルピアリングゲートウェイ（LPG）1310を介してSSH VCN1312（例えば、図12のSSH VCN1212）に通信可能に結合され得る、LPG1310（例えば、図12のLPG1210）を含むことができる。SSH VCN1312はSSHサブネット1314（例えば、図12のSSHサブネット1214）を含むことができ、SSH VCN1312は、制御プレーンVCN1316に含まれているLPG1310を介して、制御プレーンVCN1316（例えば、図12の制御プレーンVCN1216）に通信可能に結合され得る。制御プレーンVCN1316は、サービステナンシ1319（例えば、図12のサービステナンシ1219）に含まれることが可能であり、データプレーンVCN1318（例えば、図12のデータプレーンVCN1218）は、システムのユーザまたは顧客によって所有または操作され得る顧客のテナンシ1321に含まれ

40

50

ることが可能である。

【0196】

制御プレーンVCN1316は、LBサブネット1322（例えば、図12のLBサブネット1222）を含むことができる制御プレーンDMZ層1320（例えば、図12の制御プレーンDMZ層1220）、アプリサブネット1326（例えば、図12のアプリサブネット1226）を含むことができる制御プレーンアプリ層1324（例えば、図12の制御プレーンアプリ層1224）、データベース（DB）サブネット1330（例えば、図12のデータベース（DB）サブネット1230に類似する）を含むことができる制御プレーンデータ層1328（例えば、図12の制御プレーンデータ層1228）を含むことができる。制御プレーンDMZ層1320に含まれているLBサブネット1322は、制御プレーンVCN1316に含まれ得る制御プレーンアプリ層1324に含まれているアプリサブネット1326およびインターネットゲートウェイ1334（例えば、図12のインターネットゲートウェイ1234）に通信可能に結合されることが可能であり、アプリサブネット1326は、制御プレーンデータ層1328に含まれている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12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12のNATゲートウェイ1238）に通信可能に結合され得る。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を含むことができる。

10

【0197】

制御プレーンVCN1316は、アプリサブネット1326を含むことができるデータプレーンミラーアプリ層1340（例えば、図12のデータプレーンミラーアプリ層1240）を含むことができる。データプレーンミラーアプリ層1340に含まれているアプリサブネット1326は、計算インスタンス1344（例えば、図12の計算インスタンス1244に類似する）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）1342（例えば、1242のVNIC）を含むことができる。計算インスタンス1344は、データプレーンミラーアプリ層1340に含まれているVNIC1342およびデータプレーンアプリ層1346に含まれているVNIC1342を介して、データプレーンミラーアプリ層1340のアプリサブネット1326とデータプレーンアプリ層1346（例えば、図12のデータプレーンアプリ層1246）に含まれ得るアプリサブネット1326の間の通信を容易にすることができる。

20

30

【0198】

制御プレーンVCN1316に含まれているインターネットゲートウェイ1334は、パブリックインターネット1354（例えば、図12のパブリックインターネット1254）に通信可能に結合され得るメタデータ管理サービス1352（例えば、図12のメタデータ管理サービス1252）に通信可能に結合され得る。パブリックインターネット1354は、制御プレーンVCN1316に含まれているNATゲートウェイ1338に通信可能に結合され得る。制御プレーンVCN1316に含ま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（例えば、図12のクラウドサービス1256）に通信可能に結合され得る。

40

【0199】

一部の例では、データプレーンVCN1318は、顧客のテナンシ1321に含まれ得る。この場合、IaaSプロバイダは、顧客ごとに制御プレーンVCN1316を提供してよく、IaaSプロバイダは、顧客ごとに、サービステナンシ1319に含まれている固有の計算インスタンス1344を設定してよい。各計算インスタンス1344は、サービステナンシ1319に含まれている制御プレーンVCN1316と顧客のテナンシ1321に含まれているデータプレーンVCN1318の間の通信を可能にしてよい。計算インスタンス1344は、サービステナンシ1319に含まれている制御プレーンVCN1316内でプロビジョニングされているリソースが、顧客のテナンシ1321に含まれているデータプレーンVCN1318においてデプロイされること、またはそうでなければ

50

、使用されることを可能にしてよい。

【0200】

他の例では、IaaSプロバイダの顧客は、顧客のテナンシ1321に存続するデータベースを保有してよい。この例では、制御プレーンVCN1316は、アプリサブネット1326を含むことができるデータプレーンミラーアプリ層1340を含むことができる。データプレーンミラーアプリ層1340は、データプレーンVCN1318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層1340は、データプレーンVCN1318に存続しなくてよい。すなわち、データプレーンミラーアプリ層1340は、顧客のテナンシ1321に対するアクセス権限を有してよいが、データプレーンミラーアプリ層1340は、データプレーンVCN1318に存在しなくてよく、IaaSプロバイダの顧客によって所有されることも操作されることもなくてよい。データプレーンミラーアプリ層1340は、データプレーンVCN1318への呼び出しを行うように構成されてよいが、制御プレーンVCN1316に含まれているいずれかの実体への呼び出しを行うように構成されなくてよい。顧客は、制御プレーンVCN1316内でプロビジョニングされているデータプレーンVCN1318内のリソースをデプロイすること、またはそうでなければ、使用することを望むことがあり、データプレーンミラーアプリ層1340は、顧客のリソースの望ましいデプロイメントまたは他の使用を容易にすることができる。

10

【0201】

一部の実施形態では、IaaSプロバイダの顧客は、フィルタをデータプレーンVCN1318に適用することができる。この実施形態では、顧客は、どのデータプレーンVCN1318がアクセスできるかを決定することができ、顧客は、データプレーンVCN1318からパブリックインターネット1354へのアクセスを制限してよい。IaaSプロバイダは、フィルタを適用すること、またはそうでなければ、任意の外部のネットワークまたはデータベースへのデータプレーンVCN1318のアクセスを制御することが、できなくてよい。顧客によってフィルタおよび制御を顧客のテナンシ1321に含まれているデータプレーンVCN1318に適用することは、他の顧客から、およびパブリックインターネット1354から、データプレーンVCN1318を分離するのに役立つことができる。

20

【0202】

一部の実施形態では、クラウドサービス1356は、パブリックインターネット1354、制御プレーンVCN1316、またはデータプレーンVCN1318に存在しないこと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1336によって呼び出され得る。クラウドサービス1356と制御プレーンVCN1316またはデータプレーンVCN1318との間の接続は、作動中であることも、継続的であることもなくてよい。クラウドサービス1356は、IaaSプロバイダによって所有または操作される異なるネットワークに存在してよい。クラウドサービス1356は、サービスゲートウェイ1336からの呼び出しを受信するように構成されてよく、パブリックインターネット1354からの呼び出しを受信しないように構成されてよい。一部のクラウドサービス1356は、他のクラウドサービス1356から分離されてよく、制御プレーンVCN1316は、制御プレーンVCN1316と同じリージョンに存在しないことがあるクラウドサービス1356から分離されてよい。例えば、制御プレーンVCN1316が「リージョン1」に位置することがあり、クラウドサービスの「デプロイメント12」がリージョン1および「リージョン2」に位置することがある。リージョン1に位置する制御プレーンVCN1316に含まれているサービスゲートウェイ1336によってデプロイメント12への呼び出しが行われる場合、この呼び出しは、リージョン1内のデプロイメント12に送信されてよい。この例では、制御プレーンVCN1316、またはリージョン1内のデプロイメント12は、リージョン2内のデプロイメント12に通信可能に結合されること、またはそうでなければ、リージョン2内のデプロイメント12と通信することがなくてよい。

30

40

【0203】

50

図 1 4 は、少なくとも 1 つの実施形態による、I a a S 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 1 4 0 0 である。サービスオペレータ 1 4 0 2 (例えば、図 1 2 のサービスオペレータ 1 2 0 2) は、仮想クラウドネットワーク (V C N) 1 4 0 6 (例えば、図 1 2 の V C N 1 2 0 6) およびセキュアホストサブネット 1 4 0 8 (例えば、図 1 2 のセキュアホストサブネット 1 2 0 8) を含むことができるセキュアホストテナンシ 1 4 0 4 (例えば、図 1 2 のセキュアホストテナンシ 1 2 0 4) に通信可能に結合され得る。V C N 1 4 0 6 は、S S H V C N 1 4 1 2 に含まれている L P G 1 4 1 0 を介して S S H V C N 1 4 1 2 (例えば、図 1 2 の S S H V C N 1 2 1 2) に通信可能に結合され得る、L P G 1 4 1 0 (例えば、図 1 2 の L P G 1 2 1 0) を含むことができる。S S H V C N 1 4 1 2 は S S H サブネット 1 4 1 4 (例えば、図 1 2 の S S H サブネット 1 2 1 4) を含むことができ、S S H V C N 1 4 1 2 は、制御プレーン V C N 1 4 1 6 に含まれている L P G 1 4 1 0 を介して制御プレーン V C N 1 4 1 6 (例えば、図 1 2 の制御プレーン V C N 1 2 1 6) に、およびデータプレーン V C N 1 4 1 8 に含まれている L P G 1 4 1 0 を介してデータプレーン V C N 1 4 1 8 (例えば、図 1 2 のデータプレーン 1 2 1 8) に、通信可能に結合され得る。制御プレーン V C N 1 4 1 6 およびデータプレーン V C N 1 4 1 8 は、サービステナンシ 1 4 1 9 (例えば、図 1 2 のサービステナンシ 1 2 1 9) に含まれ得る。

10

【 0 2 0 4 】

制御プレーン V C N 1 4 1 6 は、ロードバランサ (L B) サブネット 1 4 2 2 (例えば、図 1 2 の L B サブネット 1 2 2 2) を含むことができる制御プレーン D M Z 層 1 4 2 0 (例えば、図 1 2 の制御プレーン D M Z 層 1 2 2 0)、アプリサブネット 1 4 2 6 (例えば、図 1 2 のアプリサブネット 1 2 2 6 に類似する) を含むことができる制御プレーンアプリ層 1 4 2 4 (例えば、図 1 2 の制御プレーンアプリ層 1 2 2 4)、D B サブネット 1 4 3 0 を含むことができる制御プレーンデータ層 1 4 2 8 (例えば、図 1 2 の制御プレーンデータ層 1 2 2 8) を含むことができる。制御プレーン D M Z 層 1 4 2 0 に含まれている L B サブネット 1 4 2 2 は、制御プレーン V C N 1 4 1 6 に含まれ得る制御プレーンアプリ層 1 4 2 4 に含まれているアプリサブネット 1 4 2 6 に、およびインターネットゲートウェイ 1 4 3 4 (例えば、図 1 2 のインターネットゲートウェイ 1 2 3 4) に通信可能に結合されることが可能であり、アプリサブネット 1 4 2 6 は、制御プレーンデータ層 1 4 2 8 に含まれている D B サブネット 1 4 3 0 に、ならびにサービスゲートウェイ 1 4 3 6 (例えば、図 1 2 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 (N A T) ゲートウェイ 1 4 3 8 (例えば、図 1 2 の N A T ゲートウェイ 1 2 3 8) に通信可能に結合され得る。制御プレーン V C N 1 4 1 6 は、サービスゲートウェイ 1 4 3 6 および N A T ゲートウェイ 1 4 3 8 を含むことができる。

20

30

【 0 2 0 5 】

データプレーン V C N 1 4 1 8 は、データプレーンアプリ層 1 4 4 6 (例えば、図 1 2 のデータプレーンアプリ層 1 2 4 6)、データプレーン D M Z 層 1 4 4 8 (例えば、図 1 2 のデータプレーン D M Z 層 1 2 4 8)、およびデータプレーンデータ層 1 4 5 0 (例えば、図 1 2 のデータプレーンデータ層 1 2 5 0) を含むことができる。データプレーン D M Z 層 1 4 4 8 は、データプレーンアプリ層 1 4 4 6 の信頼できるアプリサブネット 1 4 6 0 および信頼できないアプリサブネット 1 4 6 2 ならびにデータプレーン V C N 1 4 1 8 に含まれているインターネットゲートウェイ 1 4 3 4 に通信可能に結合され得る L B サブネット 1 4 2 2 を含むことができる。信頼できるアプリサブネット 1 4 6 0 は、データプレーン V C N 1 4 1 8 に含まれているサービスゲートウェイ 1 4 3 6、データプレーン V C N 1 4 1 8 に含まれている N A T ゲートウェイ 1 4 3 8、およびデータプレーンデータ層 1 4 5 0 に含まれている D B サブネット 1 4 3 0 に、通信可能に結合され得る。信頼できないアプリサブネット 1 4 6 2 は、データプレーン V C N 1 4 1 8 に含まれているサービスゲートウェイ 1 4 3 6、およびデータプレーンデータ層 1 4 5 0 に含まれている D B サブネット 1 4 3 0 に、通信可能に結合され得る。データプレーンデータ層 1 4 5 0 は、データプレーン V C N 1 4 1 8 に含まれているサービスゲートウェイ 1 4 3 6 に通信可

40

50

能に結合され得るDBサブネット1430を含むことができる。

【0206】

信頼できないアプリサブネット1462は、テナント仮想マシン（VM）1466（1）～（N）に通信可能に結合され得る1つまたは複数のプライマリVNIC1464（1）～（N）を含むことができる。各テナントVM1466（1）～（N）は、それぞれの顧客のテナンシ1470（1）～（N）に含まれ得るそれぞれのコンテナ出口VCN1468（1）～（N）に含まれ得るそれぞれのアプリサブネット1467（1）～（N）に、通信可能に結合され得る。それぞれのセカンダリVNIC1472（1）～（N）は、データプレーンVCN1418に含まれている信頼できないアプリサブネット1462とコンテナ出口VCN1468（1）～（N）に含まれているアプリサブネットの間の通信を容易にすることができる。各コンテナ出口VCN1468（1）～（N）は、パブリックインターネット1454（例えば、図12のパブリックインターネット1254）に通信可能に結合され得るNATゲートウェイ1438を含むことができる。

10

【0207】

制御プレーンVCN1416に含まれており、データプレーンVCN1418に含まれているインターネットゲートウェイ1434は、パブリックインターネット1454に通信可能に結合され得るメタデータ管理サービス1452（例えば、図12のメタデータ管理システム1252）に通信可能に結合され得る。パブリックインターネット1454は、制御プレーンVCN1416に含まれており、データプレーンVCN1418に含まれているNATゲートウェイ1438に通信可能に結合され得る。制御プレーンVCN1416に含まれており、データプレーンVCN1418に含ま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に通信可能に結合され得る。

20

【0208】

一部の実施形態では、データプレーンVCN1418は、顧客のテナンシ1470と統合され得る。この統合は、コードを実行するときにサポートを望むことがある場合など、場合によっては、IaaSプロバイダの顧客にとって有用なまたは望ましいことであり得る。顧客は、破壊的であり得るコードを実行するために提供することがあり、他の顧客のリソースと通信することがあり、またはそうでなければ、望ましくない影響を引き起こすことがある。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るべきかどうかを判定してよい。

30

【0209】

一部の例では、IaaSプロバイダの顧客は、一時的なネットワークアクセス権限をIaaSプロバイダに付与し、データプレーンアプリ層1446に接続される機能を要求することができる。この機能を実行するためのコードは、VM1466（1）～（N）において実行されてよく、このコードは、データプレーンVCN1418上の他の場所で実行するように構成されなくてよい。各VM1466（1）～（N）は、1つの顧客のテナンシ1470に接続されてよい。VM1466（1）～（N）に含まれているそれぞれのコンテナ1471（1）～（N）は、コードを実行するように構成されてよい。この場合、二重の分離が存在することができ（例えば、コードを実行しているコンテナ1471（1）～（N）、コンテナ1471（1）～（N）は、信頼できないアプリサブネット1462に含まれている少なくともVM1466（1）～（N）に含まれてよい）、これは、正しくないか、またはそうでなければ、望ましくないコードが、IaaSプロバイダのネットワークに損傷を与えること、または異なる顧客のネットワークに損傷を与えることを防ぐのに役立つことができる。コンテナ1471（1）～（N）は、顧客のテナンシ1470に通信可能に結合されてよく、顧客のテナンシ1470との間でデータを送信または受信するように構成されてよい。コンテナ1471（1）～（N）は、データプレーンVCN1418内の任意の他の実体との間でデータを送信または受信するように構成されなくてよい。コードの実行の完了時に、IaaSプロバイダは、コンテナ1471（1）～（N）を強制終了するか、またはそうでなければ、破棄してよい。

40

【0210】

50

一部の実施形態では、信頼できるアプリサブネット1460は、IaaSプロバイダによって所有または操作され得るコードを実行してよい。この実施形態では、信頼できるアプリサブネット1460は、DBサブネット1430に通信可能に結合されてよく、DBサブネット1430内でCRUD操作を実行するように構成されてよい。信頼できないアプリサブネット1462は、DBサブネット1430に通信可能に結合されてよいが、この実施形態では、信頼できないアプリサブネットは、DBサブネット1430内で読み取り操作を実行するように構成されてよい。各顧客のVM1466(1)~(N)に含まれ得る、顧客からのコードを実行できるコンテナ1471(1)~(N)は、DBサブネット1430と通信可能に結合されなくてよい。

【0211】

他の実施形態では、制御プレーンVCN1416およびデータプレーンVCN1418は、直接、通信可能に結合されなくてよい。この実施形態では、制御プレーンVCN1416とデータプレーンVCN1418の間に、直接通信が存在しなくてよい。しかし、通信は、少なくとも1つの方法によって間接的に発生することができる。LPG1410は、IaaSプロバイダによって確立されてよく、制御プレーンVCN1416とデータプレーンVCN1418の間の通信を容易にすることができる。別の例では、制御プレーンVCN1416またはデータプレーンVCN1418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への呼び出しを行うことができる。例えば、制御プレーンVCN1416からクラウドサービス1456への呼び出しは、データプレーンVCN1418と通信することができるサービスに対する要求を含むことができる。

【0212】

図15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1500である。サービスオペレータ1502(例えば、図12のサービスオペレータ1202)は、仮想クラウドネットワーク(VCN)1506(例えば、図12のVCN1206)およびセキュアホストサブネット1508(例えば、図12のセキュアホストサブネット1208)を含むことができるセキュアホストテナンシ1504(例えば、図12のセキュアホストテナンシ1204)に通信可能に結合され得る。VCN1506は、SSH VCN1512に含まれているLPG1510を介してSSH VCN1512(例えば、図12のSSH VCN1212)に通信可能に結合され得る、LPG1510(例えば、図12のLPG1210)を含むことができる。SSH VCN1512はSSHサブネット1514(例えば、図12のSSHサブネット1214)を含むことができ、SSH VCN1512は、制御プレーンVCN1516に含まれているLPG1510を介して制御プレーンVCN1516(例えば、図12の制御プレーンVCN1216)に、およびデータプレーンVCN1518に含まれているLPG1510を介してデータプレーンVCN1518(例えば、図12のデータプレーン1218)に、通信可能に結合され得る。制御プレーンVCN1516およびデータプレーンVCN1518は、サービステナンシ1519(例えば、図12のサービステナンシ1219)に含まれ得る。

【0213】

制御プレーンVCN1516は、LBサブネット1522(例えば、図12のLBサブネット1222)を含むことができる制御プレーンDMZ層1520(例えば、図12の制御プレーンDMZ層1220)、アプリサブネット1526(例えば、図12のアプリサブネット1226)を含むことができる制御プレーンアプリ層1524(例えば、図12の制御プレーンアプリ層1224)、DBサブネット1530(例えば、図14のDBサブネット1430)を含むことができる制御プレーンデータ層1528(例えば、図12の制御プレーンデータ層1228)を含むことができる。制御プレーンDMZ層1520に含まれているLBサブネット1522は、制御プレーンVCN1516に含まれ得る制御プレーンアプリ層1524に含まれているアプリサブネット1526に、およびインターネットゲートウェイ1534(例えば、図12のインターネットゲートウェイ1234)に通信可能に結合されることが可能であり、アプリサブネット1526は、制御プレ

10

20

30

40

50

ーンデータ層 1 5 2 8 に含まれている DB サブネット 1 5 3 0 に、ならびにサービスゲートウェイ 1 5 3 6（例えば、図 1 2 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 1 5 3 8（例えば、図 1 2 の NAT ゲートウェイ 1 2 3 8）に通信可能に結合され得る。制御プレーン VCN 1 5 1 6 は、サービスゲートウェイ 1 5 3 6 および NAT ゲートウェイ 1 5 3 8 を含むことができる。

【0214】

データプレーン VCN 1 5 1 8 は、データプレーンアプリ層 1 5 4 6（例えば、図 1 2 のデータプレーンアプリ層 1 2 4 6）、データプレーン DMZ 層 1 5 4 8（例えば、図 1 2 のデータプレーン DMZ 層 1 2 4 8）、およびデータプレーンデータ層 1 5 5 0（例えば、図 1 2 のデータプレーンデータ層 1 2 5 0）を含むことができる。データプレーン DMZ 層 1 5 4 8 は、データプレーンアプリ層 1 5 4 6 の信頼できるアプリサブネット 1 5 6 0（例えば、図 1 4 の信頼できるアプリサブネット 1 4 6 0）および信頼できないアプリサブネット 1 5 6 2（例えば、図 1 4 の信頼できないアプリサブネット 1 4 6 2）ならびにデータプレーン VCN 1 5 1 8 に含まれているインターネットゲートウェイ 1 5 3 4 に通信可能に結合され得る LB サブネット 1 5 2 2 を含むことができる。信頼できるアプリサブネット 1 5 6 0 は、データプレーン VCN 1 5 1 8 に含まれているサービスゲートウェイ 1 5 3 6、データプレーン VCN 1 5 1 8 に含まれている NAT ゲートウェイ 1 5 3 8、およびデータプレーンデータ層 1 5 5 0 に含まれている DB サブネット 1 5 3 0 に、通信可能に結合され得る。信頼できないアプリサブネット 1 5 6 2 は、データプレーン VCN 1 5 1 8 に含まれているサービスゲートウェイ 1 5 3 6、およびデータプレーンデータ層 1 5 5 0 に含まれている DB サブネット 1 5 3 0 に、通信可能に結合され得る。データプレーンデータ層 1 5 5 0 は、データプレーン VCN 1 5 1 8 に含まれているサービスゲートウェイ 1 5 3 6 に通信可能に結合され得る DB サブネット 1 5 3 0 を含むことができる。

【0215】

信頼できないアプリサブネット 1 5 6 2 は、信頼できないアプリサブネット 1 5 6 2 内に存在するテナント仮想マシン（VM）1 5 6 6（1）～（N）に通信可能に結合され得るプライマリ VNIC 1 5 6 4（1）～（N）を含むことができる。各テナント VM 1 5 6 6（1）～（N）は、それぞれのコンテナ 1 5 6 7（1）～（N）内のコードを実行することができ、コンテナ出口 VCN 1 5 6 8 に含まれ得るデータプレーンアプリ層 1 5 4 6 に含まれ得るアプリサブネット 1 5 2 6 に、通信可能に結合され得る。それぞれのセカンダリ VNIC 1 5 7 2（1）～（N）は、データプレーン VCN 1 5 1 8 に含まれている信頼できないアプリサブネット 1 5 6 2 とコンテナ出口 VCN 1 5 6 8 に含まれているアプリサブネットの間の通信を容易にすることができる。コンテナ出口 VCN は、パブリックインターネット 1 5 5 4（例えば、図 1 2 のパブリックインターネット 1 2 5 4）に通信可能に結合され得る NAT ゲートウェイ 1 5 3 8 を含むことができる。

【0216】

制御プレーン VCN 1 5 1 6 に含まれており、データプレーン VCN 1 5 1 8 に含まれているインターネットゲートウェイ 1 5 3 4 は、パブリックインターネット 1 5 5 4 に通信可能に結合され得るメタデータ管理サービス 1 5 5 2（例えば、図 1 2 のメタデータ管理システム 1 2 5 2）に通信可能に結合され得る。パブリックインターネット 1 5 5 4 は、制御プレーン VCN 1 5 1 6 に含まれており、データプレーン VCN 1 5 1 8 に含まれている NAT ゲートウェイ 1 5 3 8 に通信可能に結合され得る。制御プレーン VCN 1 5 1 6 に含まれており、データプレーン VCN 1 5 1 8 に含まれているサービスゲートウェイ 1 5 3 6 は、クラウドサービス 1 5 5 6 に通信可能に結合され得る。

【0217】

一部の例では、図 1 5 のブロック図 1 5 0 0 のアーキテクチャによって示されたパターンは、図 1 4 のブロック図 1 4 0 0 のアーキテクチャによって示されたパターンの例外と見なされてよく、IaaS プロバイダが顧客（例えば、切断されたリージョン）と直接通信することができない場合、IaaS プロバイダの顧客にとって望ましいことがある。顧

10

20

30

40

50

客ごとにVM1566(1)～(N)に含まれているそれぞれのコンテナ1567(1)～(N)は、顧客によってリアルタイムにアクセスされ得る。コンテナ1567(1)～(N)は、コンテナ出口VCN1568に含まれ得るデータプレーンアプリ層1546のアプリサブネット1526に含まれているそれぞれのセカンダリVNIC1572(1)～(N)への呼び出しを行うように構成されてよい。セカンダリVNIC1572(1)～(N)は、呼び出しをNATゲートウェイ1538に送信することができ、NATゲートウェイ1538は、呼び出しをパブリックインターネット1554に送信してよい。この例では、顧客によってリアルタイムにアクセスされ得るコンテナ1567(1)～(N)が、制御プレーンVCN1516から分離されることが可能であり、データプレーンVCN1518に含まれている他の実体から分離され得る。コンテナ1567(1)～(N)は、他の顧客のリソースから分離されてもよい。

10

【0218】

他の例では、顧客は、コンテナ1567(1)～(N)を使用して、クラウドサービス1556を呼び出すことができる。この例では、顧客は、クラウドサービス1556に対してサービスを要求するコンテナ1567(1)～(N)内のコードを実行してよい。コンテナ1567(1)～(N)は、この要求をセカンダリVNIC1572(1)～(N)に送信することができ、セカンダリVNIC1572(1)～(N)は、この要求をNATゲートウェイに送信することができ、NATゲートウェイは、この要求をパブリックインターネット1554に送信することができる。パブリックインターネット1554は、この要求を、インターネットゲートウェイ1534を介して、制御プレーンVCN1516に含まれているLBサブネット1522に送信することができる。この要求が有効であるということを決断することに応答して、LBサブネットは、この要求をアプリサブネット1526に送信することができ、アプリサブネット1526は、サービスゲートウェイ1536を介して、この要求をクラウドサービス1556に送信することができる。

20

【0219】

図に示されているIaaSアーキテクチャ1200、1300、1400、1500が、示されているコンポーネント以外のコンポーネントを含んでよいということが、理解されるべきである。さらに、図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単に一部の例である。一部の他の実施形態では、IaaSシステムは、図に示されているコンポーネントより多いか、または少ないコンポーネントを含んでよく、2つ以上のコンポーネントを結合してよく、あるいはコンポーネントの異なる構成または配置を有してよい。

30

【0220】

ある実施形態では、本明細書に記載されたIaaSシステムは、セルフサービスの、サブスクリプションに基づく、弾力的に拡張可能な、信頼できる、高度に利用可能な、および安全な方法で顧客に配信される、一連のアプリケーション、ミドルウェア、およびデータベースサービスの提供を含んでよい。そのようなIaaSシステムの例は、本譲受人によって提供されるOracleクラウドインフラストラクチャ(OCI)である。

【0221】

図16は、さまざまな実施形態が実装され得る例示的なコンピュータシステム1600を示している。システム1600は、前述の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されてよい。図に示されているように、コンピュータシステム1600は、バスサブシステム1602を介して複数の周辺サブシステムと通信する処理ユニット1604を含んでいる。これらの周辺サブシステムは、処理加速ユニット1606、I/Oサブシステム1608、ストレージサブシステム1618、および通信サブシステム1624を含んでよい。ストレージサブシステム1618は、有形のコンピュータ可読ストレージ媒体1622およびシステムメモリ1610を含む。

40

【0222】

バスサブシステム1602は、コンピュータシステム1600のさまざまなコンポーネントおよびサブシステムに、意図されたとおりに互いに通信させるためのメカニズムを提

50

供する。バスサブシステム 1602 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の実施形態は、複数のバスを利用してよい。バスサブシステム 1602 は、メモリバスまたはメモリコントローラ、ペリフェラルバス、およびさまざまなバスアーキテクチャのいずれかを使用するローカルバスを含む、複数の種類のバス構造のいずれかであってよい。例えば、そのようなアーキテクチャは、ISA (Industry Standard Architecture) バス、MCA (Micro Channel Architecture) バス、EISA (Enhanced ISA) バス、VESA (Video Electronics Standards Association) ローカルバス、および IEEE P1386.1 規格で製造されたメザンバスとして実装され得る PCI (Peripheral Component Interconnect) バスを含んでよい。

【0223】

10

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）として実装され得る処理ユニット 1604 は、コンピュータシステム 1600 の動作を制御する。1つまたは複数のプロセッサが、処理ユニット 1604 に含まれてよい。これらのプロセッサは、シングルコアプロセッサまたはマルチコアプロセッサを含んでよい。ある実施形態では、処理ユニット 1604 は、1つまたは複数の独立した処理ユニット 1632 および／または 1634 として実装されてよく、シングルコアプロセッサまたはマルチコアプロセッサが各処理ユニットに含まれている。他の実施形態では、処理ユニット 1604 は、2つのデュアルコアプロセッサを単一のチップに統合することによって形成されたクアッドコア処理ユニットとして実装されてもよい。

【0224】

20

さまざまな実施形態では、処理ユニット 1604 は、プログラムコードに応じてさまざまなプログラムを実行することができ、複数の同時に実行するプログラムまたはプロセスを維持することができる。任意の特定の時間に、実行されるプログラムコードの一部またはすべてが、プロセッサ 1604 に、および／またはストレージサブシステム 1618 に存在することができる。適切なプログラミングによって、プロセッサ 1604 は、前述のさまざまな機能を提供することができる。コンピュータシステム 1600 は、デジタル信号プロセッサ (DSP: digital signal processor)、専用プロセッサ、および／または同様のものを含むことができる処理加速ユニット 1606 を、さらに含んでよい。

【0225】

30

I/O サブシステム 1608 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んでよい。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などのポインティングデバイス、ディスプレイに組み込まれたタッチパッドまたはタッチスクリーン、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備える音声入力デバイス、マイクロホン、および他の種類の入力デバイスを含んでよい。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、ジェスチャーおよび話されたコマンドを使用する自然なユーザインターフェイスを介して、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て情報をやりとりすることを可能にする、Microsoft Kinect (登録商標) モーションセンサなどの、動作検出デバイスおよび／またはジェスチャー認識デバイスを含んでよい。ユーザインターフェイス入力デバイスは、ユーザの目の活動（例えば、写真を撮っているとき、および／またはメニューを選択しているときの「まばたき」）を検出し、アイジェスチャーを入力デバイス（例えば、Google Glass (登録商標)）への入力として変換する Google Glass (登録商標) まばたき検出器などの、アイジェスチャー認識デバイスを含んでもよい。さらに、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介して音声認識システム（例えば、Siri (登録商標) ナビゲーター）とやりとりできるようにする音声認識検出デバイスを含んでよい。

40

【0226】

ユーザインターフェイス入力デバイスは、3次元 (3D: three dimensional) 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

50

ックタブレット、ならびにスピーカ、デジタルカメラ、デジタルビデオカメラ、ポータブルメディアプレーヤー、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、レーザ距離計、および視線追跡デバイスなどの、音声／視覚デバイスを含んでもよいが、これらに限定されない。さらに、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、磁気共鳴撮像、位置放出断層撮影、医用超音波検査デバイスなどの、医用画像入力デバイスを含んでよい。ユーザインターフェイス入力デバイスは、例えば、MIDIキーボード、デジタル楽器などの音声入力デバイスを含んでもよい。

【0227】

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、インジケータライト、または音声出力デバイスなどの視覚表示以外などを含んでよい。ディスプレイサブシステムは、ブラウン管（CRT：cathode ray tube）、液晶ディスプレイ（LCD：liquid crystal display）またはプラズマディスプレイを使用するフラットパネルデバイスなどのフラットパネルデバイス、投射デバイス、タッチスクリーンなどであってよい。一般に、「出力デバイス」という用語の使用は、情報をコンピュータシステム1600からユーザまたは他のコンピュータに出力するためのすべての可能性のある種類のデバイスおよびメカニズムを含むよう意図されている。例えば、ユーザインターフェイス出力デバイスは、モニタ、プリンタ、スピーカ、ヘッドホン、カーナビ、プロッター、音声出力デバイス、およびモデムなどの、テキスト情報、グラフィックス情報、および音声／ビデオ情報を視覚的に伝達するさまざまなディスプレイデバイスを含んでよいが、これらに

10

20

【0228】

コンピュータシステム1600は、システムメモリ1610内に現在あるように示されているソフトウェア要素を含む、ストレージサブシステム1618を備えてよい。システムメモリ1610は、処理ユニット1604で読み込み可能かつ実行可能なプログラム命令に加えて、これらのプログラムの実行中に生成されたデータを格納してよい。

【0229】

コンピュータシステム1600の構成および種類に応じて、システムメモリ1610は、揮発性（ランダムアクセスメモリ（RAM：random-access memory）など）および／または不揮発性（読み取り専用メモリ（ROM：read-only memory）、フラッシュメモリなど）であってよい。RAMは、通常、処理ユニット1604によって直ちにアクセス可能である、かつ／または現在操作されて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含む。一部の実装では、システムメモリ1610は、スタティックランダムアクセスメモリ（SRAM：static random-access memory）またはダイナミックランダムアクセスメモリ（DRAM：dynamic random-access memory）などの、複数の異なる種類のメモリを含んでよい。一部の实装では、起動中などにコンピュータシステム1600内の要素間で情報を転送するのに役立つ基本ルーチンを含んでいる基本入出力システム（BIOS：basic input/output system）が、通常はROMに格納されてよい。限定ではなく例として、システムメモリ1610は、クライアントアプリケーション、ウェブブラウザ、ミッドティアアプリケーション、リレーショナルデータベース管理システム（RDBMS：relational database management systems）などを含んでよいアプリケーションプログラム1612、プログラムデータ1614、およびオペレーティングシステム1616も示している。オペレーティングシステム1616の例としては、Microsoft Windows（登録商標）、Apple Macintosh（登録商標）、および／またはLinuxオペレーティングシステム、さまざまな市販されている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（さまざまなGNU/Linuxオペレーティングシステム、Google Chrome（登録商標）OSなどを含むが、これらに限定されない）、ならびに／あるいはiOS、Windows（登録商標）Phone、Android（登録商標）OS、BlackBerry（登録商標）16 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の、さまざまなバージ

30

40

50

ョンが挙げられ得る。

【0230】

ストレージサブシステム1618は、一部の実施形態の機能を提供する基本的なプログラミングおよびデータの構成を格納するための有形のコンピュータ可読ストレージ媒体を提供してもよい。プロセッサによって実行されたときに前述の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、ストレージサブシステム1618に格納されてよい。これらのソフトウェアモジュールまたは命令は、処理ユニット1604によって実行されてよい。ストレージサブシステム1618は、本開示に従って使用されるデータを格納するためのリポジトリを提供してもよい。

【0231】

ストレージサブシステム1600は、コンピュータ可読ストレージ媒体1622にさらに接続され得るコンピュータ可読ストレージ媒体リーダ1620を含んでもよい。システムメモリ1610と組み合わせて、一緒に、任意選択的に、コンピュータ可読ストレージ媒体1622は、リモートの、ローカルな、固定された、および／または取り外し可能なストレージ媒体に加えて、コンピュータ可読情報を一時的に、かつ／またはより永続的に含むため、格納するため、送信するため、および取り出すためのストレージ媒体を、包括的に表してよい。

【0232】

コードまたはコードの一部を含んでいるコンピュータ可読ストレージ媒体1622は、情報の格納および／または送信のために任意の方法または技術で実装された、揮発性および不揮発性の、取り外し可能および取り外し不可能な媒体などの、ただしこれらに限定されない、ストレージ媒体および通信媒体を含む、当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むこともできる。コンピュータ可読ストレージ媒体1622は、RAM、ROM、電子的消去可能プログラマブルROM（EEPROM：electronically erasable programmable ROM）、フラッシュメモリまたは他のメモリ技術、CD-ROM、デジタルバーサタイルディスク（DVD：digital versatile disk）、また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、または他の磁気ストレージデバイス、あるいは他の有形のコンピュータ可読媒体などの、有形のコンピュータ可読ストレージ媒体を含むことができる。コンピュータ可読ストレージ媒体1622は、所望の情報を送信するために使用されることが可能であり、コンピュータシステム1600によってアクセスされ得る、データ信号、データ送信、または任意の他の媒体などの非有形のコンピュータ可読媒体を含むこともできる。

【0233】

例として、コンピュータ可読ストレージ媒体1622は、取り外し不可能な不揮発性の磁気媒体から読み取るか、または磁気媒体に書き込むハードディスクドライブ、取り外し可能な不揮発性の磁気ディスクから読み取るか、または磁気ディスクに書き込む磁気ディスクドライブ、ならびにCD-ROM、DVD、およびブルーレイ（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な不揮発性の光ディスクから読み取るか、または光ディスクに書き込む光ディスクドライブを含んでよい。コンピュータ可読ストレージ媒体1622は、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：universal serial bus）フラッシュドライブ、セキュアデジタル（SD：secure digital）カード、DVDディスク、デジタルビデオテープなどを含んでよいが、これらに限定されない。コンピュータ可読ストレージ媒体1622は、フラッシュメモリベースのSSD、エンタープライズフラッシュドライブ、半導体ROMなどの、不揮発性メモリに基づく半導体ドライブ（SSD：solid-state drives）、半導体RAM、ダイナミックRAM、スタティックRAM、DRAMベースのSSD、磁気抵抗RAM（MRAM：magneto resistive RAM）SSDなどの、揮発性メモリに基づくSSD、およびDRAMとフラッシュメモリベースのSSDの組合せを使用するハイブリッドSSDを含んでもよい。ディスクドライブおよび関連するコンピュータ可読媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、およびコンピュータシステム1

10

20

30

40

50

600の他のデータの不揮発性ストレージを提供してよい。

【0234】

通信サブシステム1624は、他のコンピュータシステムおよびネットワークへのインターフェイスを提供する。通信サブシステム1624は、コンピュータシステム1600の他のシステムからデータを受信するため、および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機能する。例えば、通信サブシステム1624は、コンピュータシステム1600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できるようにしてよい。一部の実施形態では、通信サブシステム1624は、ワイヤレス音声および／またはデータネットワークにアクセスするための無線周波（RF：radio frequency）トランシーバのコンポーネント（例えば、携帯電話技術、3G、4G、もしくはEDGE（enhanced data rates for global evolution：エンハンスドデータレツフォグローバルエボリューション）などの高度なデータネットワーク技術、Wi-Fi（IEEE 802.11群規格、または他の移動体通信技術、あるいはこれらの任意の組合せを使用する）、全地球測位システム（GPS：global positioning system）レシーバのコンポーネント、および／または他のコンポーネントを含むことができる。一部の実施形態では、通信サブシステム1624は、ワイヤレスインターフェイスに加えて、またはワイヤレスインターフェイスの代わりに、有線ネットワーク接続（例えば、イーサネット）を提供することができる。

10

【0235】

一部の実施形態では、通信サブシステム1624は、コンピュータシステム1600を使用することがある1人または複数のユーザの代わりに、構造化および／または非構造化データフィード1626、イベントストリーム1628、イベント更新1630などの形態で入力通信を受信してもよい。

20

【0236】

例として、通信サブシステム1624は、Twitter（登録商標）フィード、Facebook（登録商標）の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、リッチサイトサマリー（RSS：Rich Site Summary）フィードなどのウェブフィード、ならびに／あるいは1つまたは複数のサードパーティの情報源からのリアルタイムの更新から、データフィード1626をリアルタイムに受信するように構成されてよい。

30

【0237】

さらに、通信サブシステム1624は、連続データストリームの形態でデータを受信するように構成されてもよく、連続データストリームは、明示的な末尾がなく、本質的に連続的であるか、または境界がなくてよいリアルタイムイベントのイベントストリーム1628および／またはイベント更新1630を含むことができる。連続データを生成するアプリケーションの例としては、例えば、センサデータアプリケーション、金融ティッカー、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が挙げられ得る。

【0238】

通信サブシステム1624は、構造化および／または非構造化データフィード1626、イベントストリーム1628、イベント更新1630などを、コンピュータシステム1600に結合された1つまたは複数のストリーミングデータソース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出力するように構成されてもよい。

40

【0239】

コンピュータシステム1600は、ハンドヘルド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、自動発券機、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、さまざまな種類のうちの1つであることができる。

50

【0240】

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、図に示されたコンピュータシステム1600の説明は、単に具体的な例となるよう意図されている。図に示されたシステムよりも多いか、または少ないコンポーネントを含んでいる多くの他の構成が可能である。例えば、カスタマイズされたハードウェアが使用されてもよく、かつ／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）、またはこれらの組合せにおいて実装されてよい。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採用されてよい。本明細書において提供された開示および教示に基づいて、当業者は、さまざまな実施形態を実施するための他の方法および／または方式を理解するであろう。

10

【0241】

特定の実施形態が説明されたが、さまざまな修正、変更、代替の構造、および同等のものも、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の動作に制限されず、複数のデータ処理環境内で自由に動作できる。さらに、特定の一連のトランザクションおよびステップを使用して実施形態が説明されたが、本開示の範囲が説明された一連のトランザクションおよびステップに限定されないということが、当業者にとって明らかであるはずである。前述の実施形態のさまざまな特徴および態様は、個別に、または一緒に使用されてよい。

【0242】

さらに、ハードウェアとソフトウェアの特定の組合せを使用して実施形態が説明されたが、ハードウェアとソフトウェアの他の組合せも本開示の範囲内にあるということが認識されるべきである。ハードウェアのみにおいて、またはソフトウェアのみにおいて、あるいはこれらの組合せを使用して、実施形態が実装されてよい。本明細書に記載されたさまざまなプロセスは、同じプロセッサまたは任意の組合せでの異なるプロセッサ上で実施され得る。したがって、コンポーネントまたはモジュールが、ある動作を実行するように構成されていると説明される場合、そのような構成は、例えば、この動作を実行するように電子回路を設計することによって、この動作を実行するようにプログラム可能な電子回路（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、あるいはこれらの任意の組合せによって、実現され得る。プロセスは、プロセス間通信のための従来技術を含むが、これらに限定されないさまざまな技術を使用して通信することができ、プロセスの異なる対は、異なる技術を使用してよく、またはプロセスの同じ対は、異なる時間に異なる技術を使用してよい。

20

30

【0243】

したがって、本明細書および図面は、限定を意味するのではなく、例示であると思なされるべきである。しかし、特許請求の範囲に示されるようなより広い思想および範囲から逸脱することなく、本明細書および図面に対して追加、削減、削除、ならびに他の修正および変更が行われてよいということが、明らかである。したがって、特定の開示の実施形態が説明されたが、これらは限定することを意図されていない。さまざまな変更および同等のものが、添付の特許請求の範囲内にある。

【0244】

開示された実施形態を説明する文脈における（特に、添付の特許請求の範囲の文脈における）「a」および「an」および「the」という用語ならびに同様の指示対象の使用は、本明細書において特に示されない限り、または文脈と明らかに矛盾しない限り、単数と複数の両方を対象にすると解釈されるべきである。「備えている」、「有している」、「含んでいる（including）」、および「含んでいる（containing）」という用語は、特に注記されない限り、無制限の（すなわち、「～を含むが、これに限定されない」ということを意味する）用語であると解釈されるべきである。「接続される」という用語は、介在する何かが存在する場合でも、内部に部分的に、または完全に含まれるか、接続されるか、あるいは一緒に接合されると解釈されるべきである。本明細書における値の範囲の列挙は、本明細書において特に示されない限り、単に、範囲に含まれる別々の各値を個別

40

50

に参照する簡単な方法として役立つよう意図されており、別々の各値は、本明細書において個別に列挙されたかのように、本明細書に組み込まれる。本明細書に記載されたすべての方法は、本明細書において特に示されない限り、または文脈と特に明確に矛盾しない限り、任意の適切な順序で実行され得る。本明細書において提供される、ありとあらゆる例、または例示的な言語（例えば、「など」）の使用は、単に、実施形態をより良く明らかにするよう意図されており、特に主張されない限り、本開示の範囲に限定を課さない。本明細書における言語は、いずれかの主張されない要素を、本開示の実践にとって不可欠であるとして示すと解釈されるべきでない。

【0245】

「X、Y、またはZのうちの少なくとも1つ」という語句などの選言的言語は、特に明確に述べられない限り、一般に、項目、条件などが、X、Y、またはZのいずれか、あるいはこれらの任意の組合せ（例えば、X、Y、および／またはZ）であってよいということを提示するために使用されると文脈内で理解されるよう意図されている。したがって、そのような選言的言語は、一般に、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1つが各々存在することを必要とするということを意味するよう意図されておらず、そのようなことを意味するべきでない。

【0246】

本明細書では、本開示を実行するための知られている最良のモードを含む、本開示の好ましい実施形態が説明される。前述の説明を読むときに、当業者にとって、そのような好ましい実施形態の変形が明らかになり得る。当業者は、必要に応じてそのような変形を採用することができるはずであり、本開示は、本明細書において詳細に説明されたような実践以外に実践されてよい。したがって、本開示は、適用可能な法律によって認可される、本明細書に添付されている特許請求の範囲において列挙された本主題のすべての変更および同等のものを含む。さらに、実施形態のすべての可能な変形における前述の要素の任意の組合せは、本明細書において特に示されない限り、本開示によって包含される。

【0247】

本明細書において引用された公表文献、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、参照によって組み込まれるように個別に詳細に示され、本明細書において全体として示された場合と同じ程度に、参照によって本明細書に組み込まれる。

【0248】

前述の明細書では、本明細書の特定の実施形態を参照して本開示の態様が説明されたが、当業者は、本開示がそれらに限定されないということを認識するであろう。前述の開示のさまざまな特徴および態様は、個別に、または一緒に使用されてよい。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た環境および応用を越えて、任意の数の環境および応用において利用され得る。したがって、本明細書および図面は、限定ではなく例示であると見なされるべきである。

10

20

30

40

50

【図面】
【図 1】

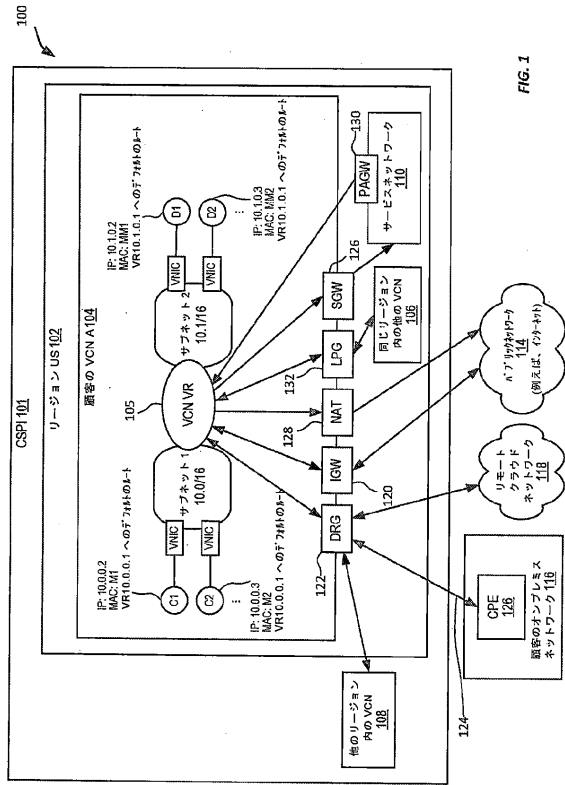


FIG. 1

【図 2】

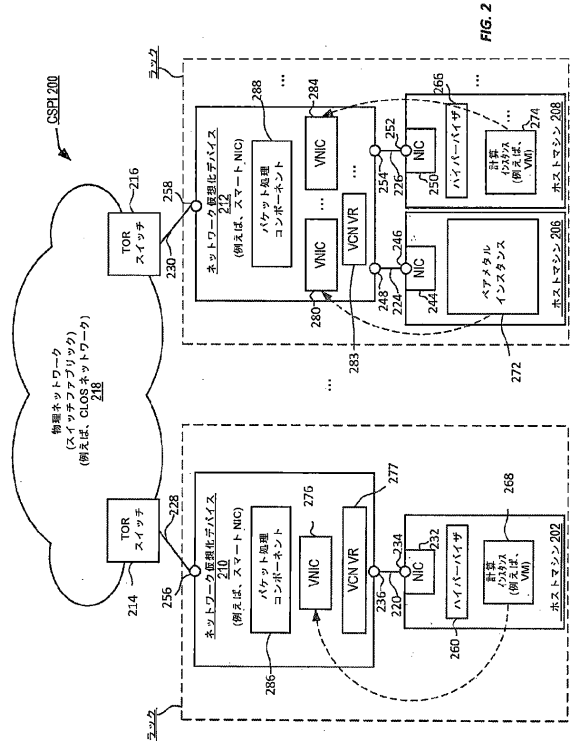


FIG. 2

【図 3】

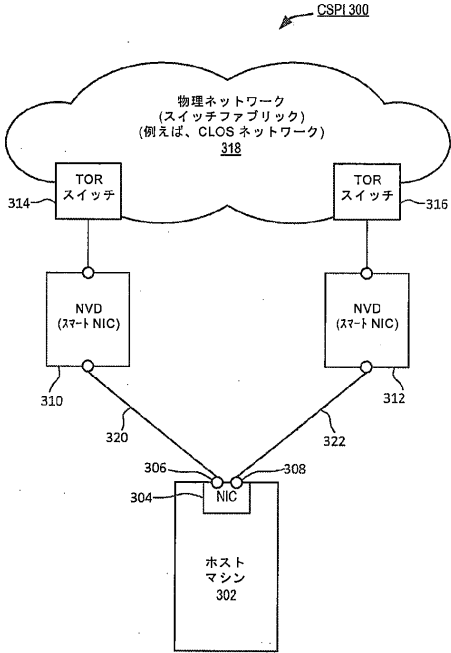


FIG. 3

【図 4】

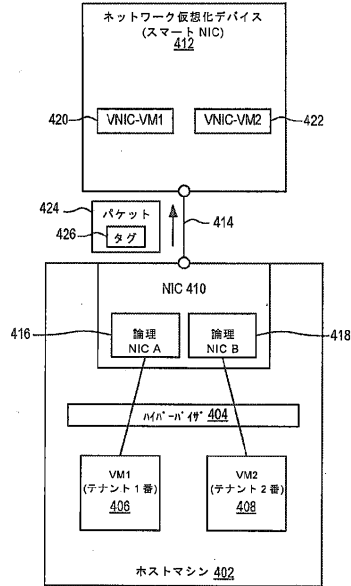


FIG. 4

10

20

30

40

50

【図 5】

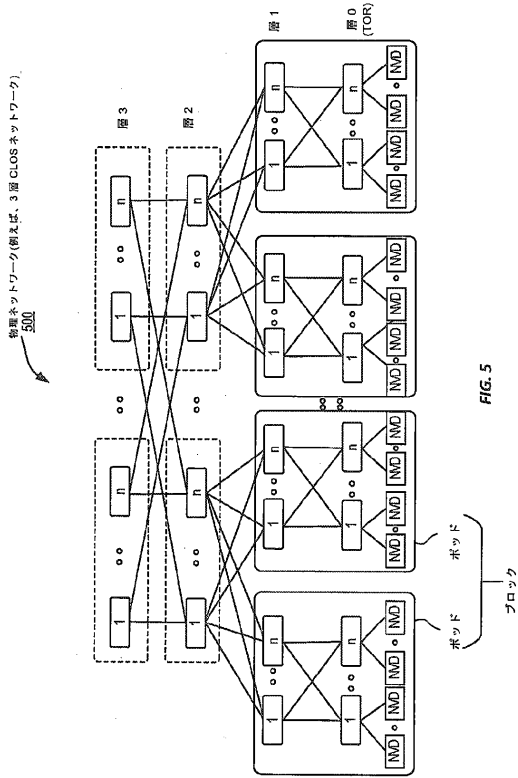


FIG. 5

【図 6】

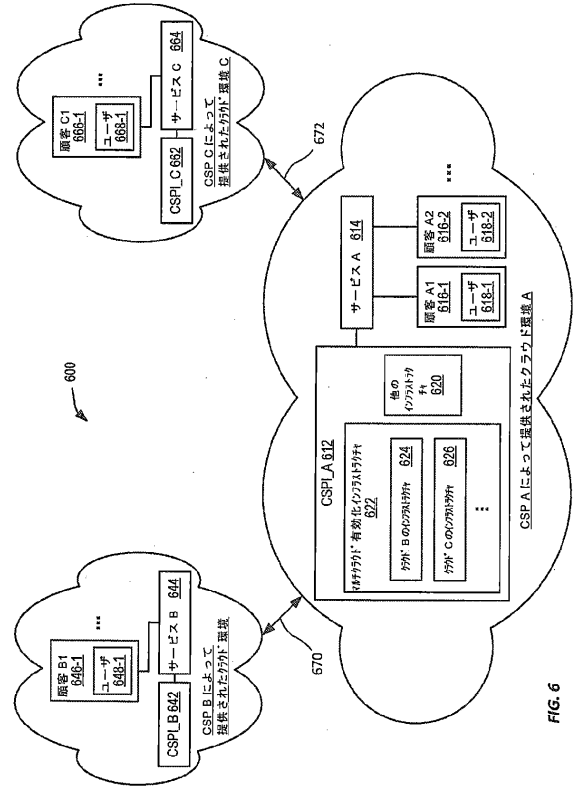


FIG. 6

【図 7】

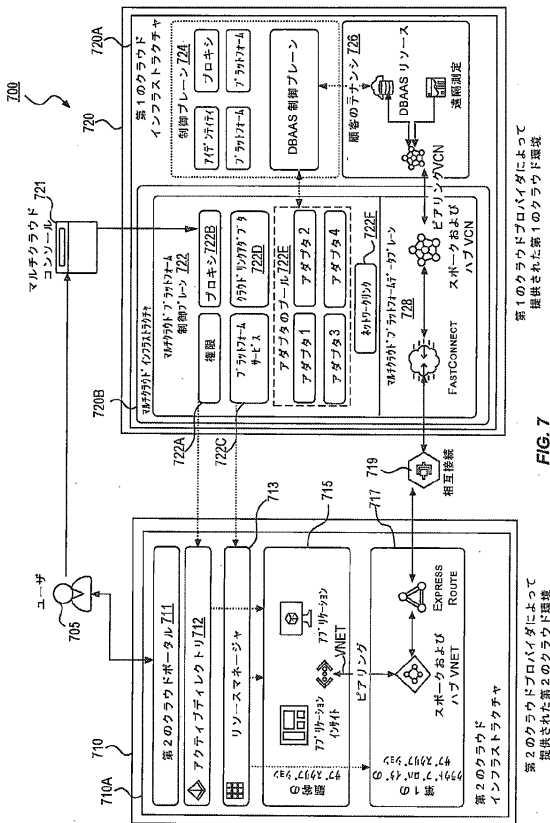


FIG. 7

【図 8 A】

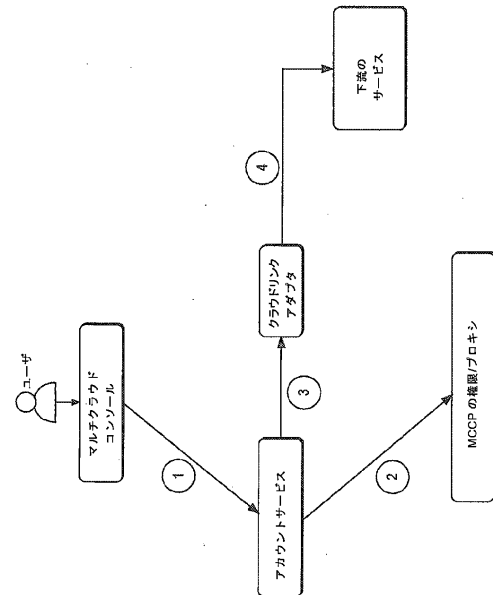


FIG. 8A

10

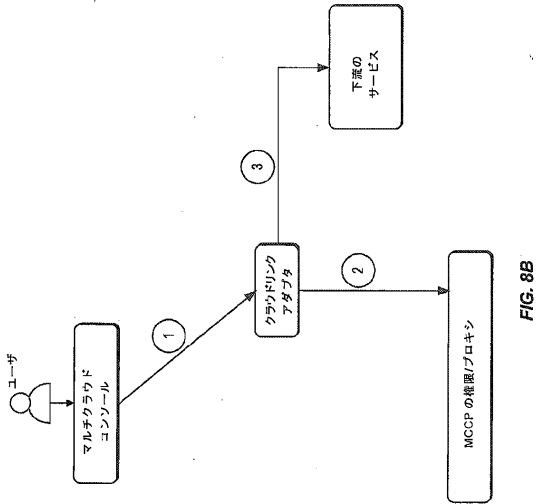
20

30

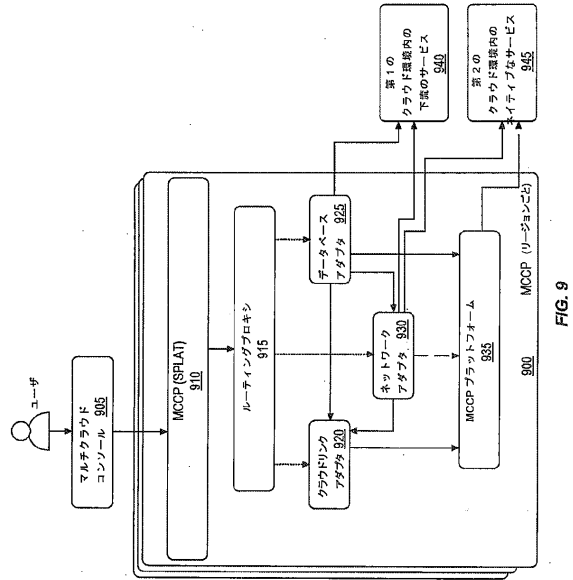
40

50

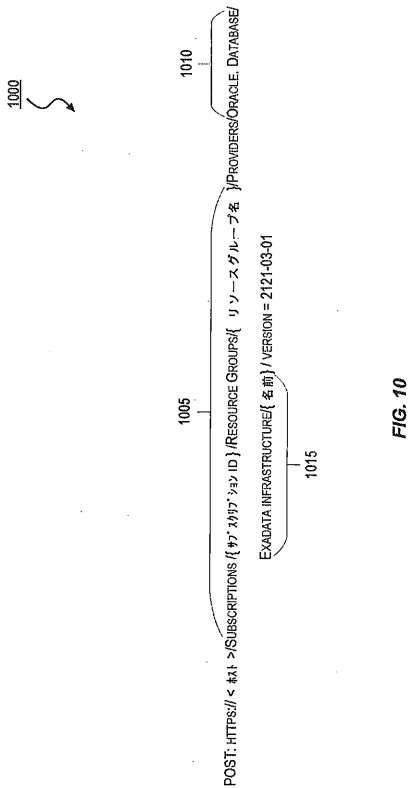
【図 8 B】



【図 9】



【図 10】



【図 11】

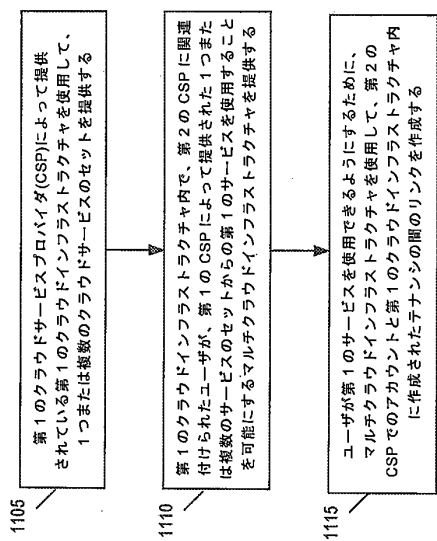
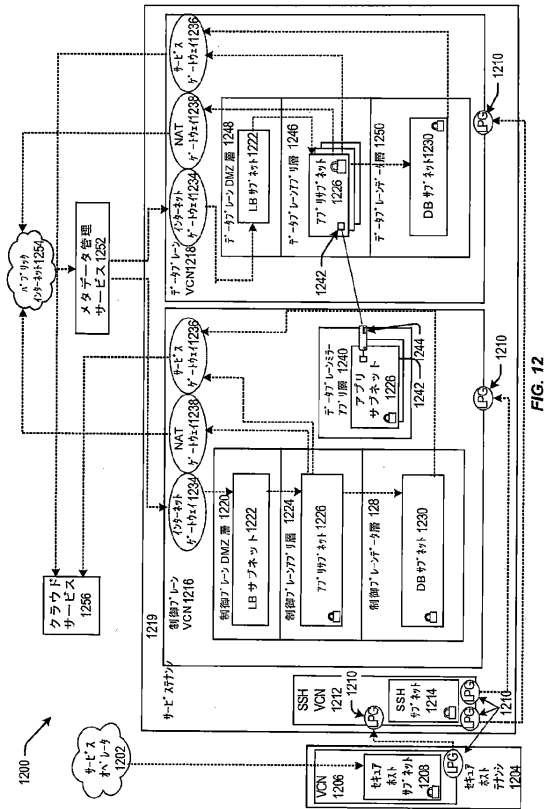
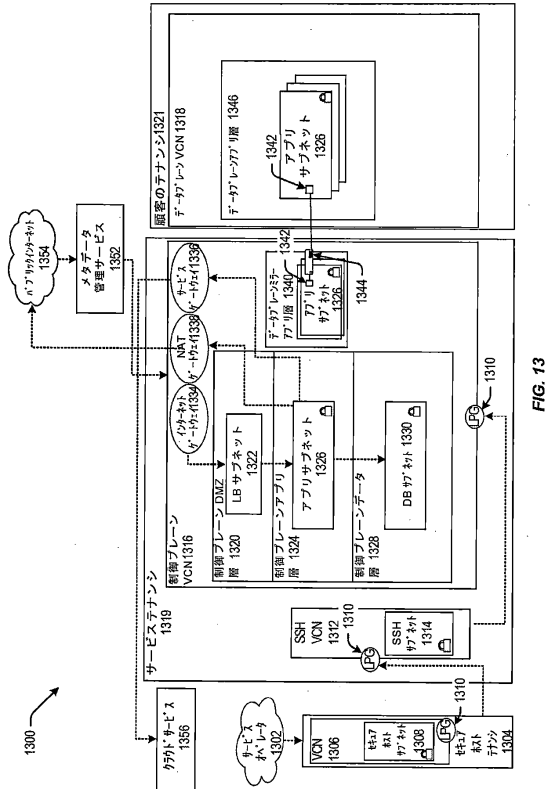


FIG. 11

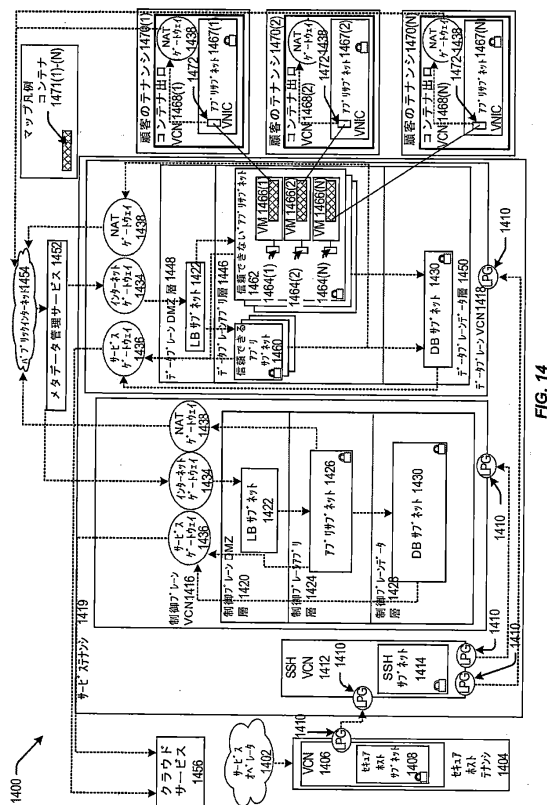
【図 12】



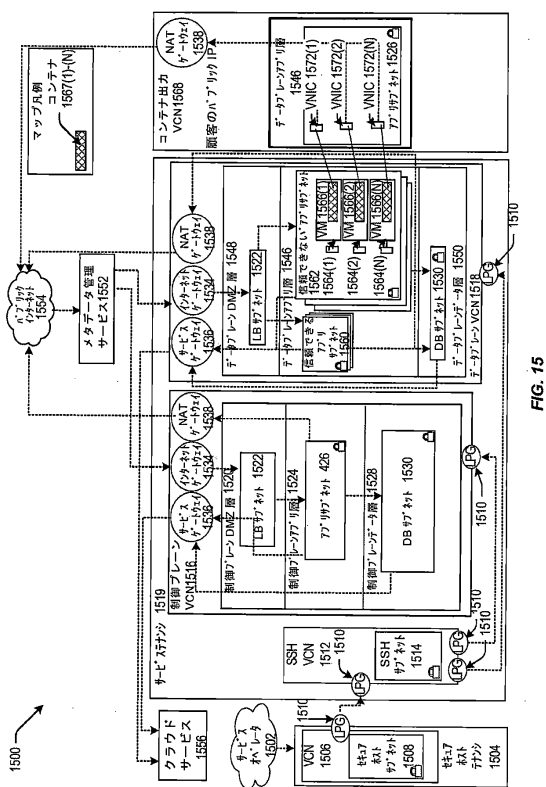
【圖 13】



【図 14】



【図 15】



【図 16】

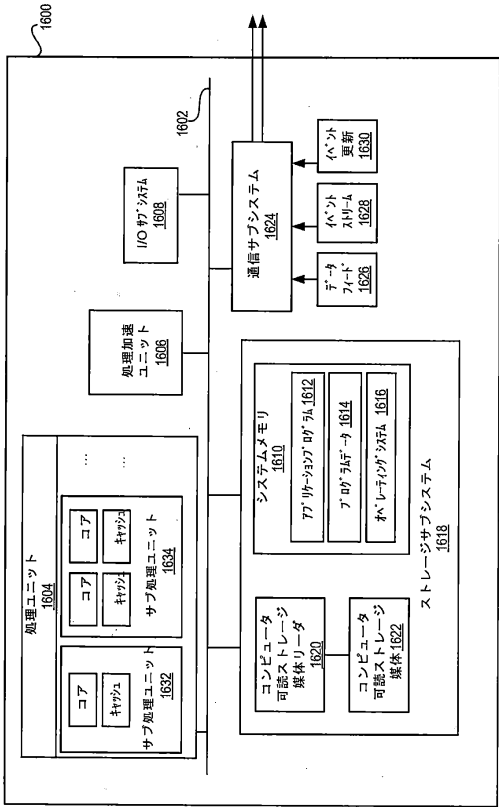


FIG. 16

10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2023/012084

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F9/50
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)
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	Rao Vinay: "Building Multi-Cloud Apps on Microsoft Azure and Oracle Cloud Infrastructure", 26 July 2019 (2019-07-26), pages 1-16, XP093038479, Retrieved from the Internet: URL:https://medium.com/oracledevs/from-azure-to-autonomous-an-enterprise-multi-cloud-journey-an-enterprise-multi-cloud-journey-cc070a28cb10 [retrieved on 2023-04-12] the whole document ----- -/--	1-20

☒ 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

13 April 2023

Date of mailing of the international search report

25/04/2023

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

Touloupis, Emmanuel

1

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

10

20

30

40

50

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2023/012084

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Chandrashekar Vinay Shivagange: "Oracle and Microsoft Interconnect Clouds to Accelerate Enterprise Cloud Adoption", , 5 June 2019 (2019-06-05), pages 1-4, XP093036732, Retrieved from the Internet: URL:https://blogs.oracle.com/cloud-infrast ructure/post/oracle-and-microsoft-intercon nect-clouds-to-accelerate-enterprise-cloud -adoption?source=post_page----- ----- [retrieved on 2023-03-31] the whole document -----	1-20

1

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

フロントページの続き

(32)優先日 令和4年3月18日(2022.3.18)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 63/333,965

(32)優先日 令和4年4月22日(2022.4.22)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 63/336,811

(32)優先日 令和4年4月29日(2022.4.29)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 63/339,297

(32)優先日 令和4年5月6日(2022.5.6)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 63/357,541

(32)優先日 令和4年6月30日(2022.6.30)

(33)優先権主張国・地域又は機関
米国(US)

(31)優先権主張番号 63/388,925

(32)優先日 令和4年7月13日(2022.7.13)

(33)優先権主張国・地域又は機関
米国(US)

(81)指定国・地域 AP(BW,CV,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,ME,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,CV,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,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

3. PALM OS

(72)発明者 レイナルト, ジョン

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

Fターム(参考) 5K030 HA08 HC13 HD07 KA01 LB05