

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号

特表2024-541998

(P2024-541998A)

(43)公表日 令和6年11月13日(2024.11.13)

(51)国際特許分類

H 0 4 L 41/0895(2022.01)

F I

H 0 4 L 41/0895

審査請求 未請求 予備審査請求 有 (全75頁)

(21)出願番号 特願2024-525442(P2024-525442)
(86)(22)出願日 令和4年6月23日(2022.6.23)
(85)翻訳文提出日 令和6年6月7日(2024.6.7)
(86)国際出願番号 PCT/US2022/034753
(87)国際公開番号 WO2023/075869
(87)国際公開日 令和5年5月4日(2023.5.4)
(31)優先権主張番号 17/515,093
(32)優先日 令和3年10月29日(2021.10.29)
(33)優先権主張国・地域又は機関 米国(US)
(81)指定国・地域 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA, RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR, GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC, 最終頁に続く

(71)出願人 502303739
オラクル・インターナショナル・コーポ
レイション
アメリカ合衆国 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
(74)代理人 110001195
弁理士法人深見特許事務所
(72)発明者 クリーガースティックレス, ルーカス
・マイケル
アメリカ合衆国、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
最終頁に続く

(54)【発明の名称】 プライベートネットワーク間のセキュア双方向ネットワーク接続システム

(57)【要約】

顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間の安全なプライベートネットワーク接続を提供する、クラウドサービスプロバイダインフラストラクチャ(CSPI)内のセキュアプライベートネットワーク接続サービス(SNCS)が記載される。SNCSは、企業のユーザ(例えば、管理者)が明示的に外部リソースを構成し、経路を公告し、またはサイト間ネットワーク接続をセットアップする必要なしに、顧客の外部サイト表現内に存在する外部リソースと、クラウド内の顧客のVCN内に存在するリソースおよびサービスとの間の安全なプライベート双方向ネットワーク接続を提供する。SNCSは、安全なサイト間ネットワーク接続を提供するために使用されるネットワーク要素およびコンピューティングノードのロバストなインフラストラクチャを実装することによって、顧客のオンプレミス環境とCSPIとの間のネットワークトラフィックを処理するための高性能で、スケーラブルな、かつ高可用性のサイト間ネットワーク接続を提供する。

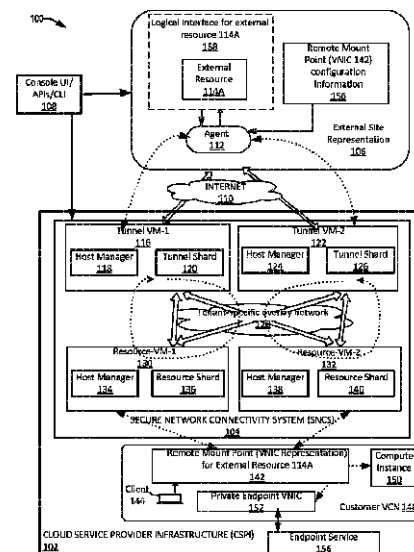


FIG. 1

【特許請求の範囲】

【請求項 1】

方法であって、

クラウドサービスプロバイダにおいて実装されているセキュアネットワーク接続システムが、前記クラウドサービスプロバイダの顧客に関連付けられているオンプレミスネットワークと前記顧客のために前記クラウドサービスプロバイダによってホストされている仮想クラウドネットワーク（VCN）との間の安全なプライベートネットワーク接続を可能にするためのセキュアネットワーク接続サービスを提供することを含み、前記セキュアネットワーク接続システムは、1つまたは複数のコンピューティングノードのセットを含む仮想オーバーレイネットワークを備え、前記方法はさらに、

10

前記セキュアネットワーク接続システムが、前記オンプレミスネットワーク内に存在する外部リソースを、前記仮想クラウドネットワーク内の外部エンドポイントとして登録することを含み、前記外部エンドポイントは、前記仮想クラウドネットワーク内のインターネットプロトコル（IP）アドレスによって識別され、前記方法はさらに、

前記セキュアネットワーク接続システム内の前記1つまたは複数のコンピューティングノードのセットのうちの第1のコンピューティングノードが、前記仮想クラウドネットワーク内の前記外部エンドポイントの外部リソース表現を作成することを含み、前記外部リソース表現を作成することは、

前記第1のコンピューティングノードが、仮想ネットワークインターフェイスカード（VNIC）を作成することと、

20

前記第1のコンピューティングノードが、前記外部エンドポイントに関連付けられている前記インターネットプロトコル（IP）アドレスを前記仮想ネットワークインターフェイスカード（VNIC）に割り当てることと、を含み、前記方法はさらに、

前記第1のコンピューティングノードが、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する構成情報を、前記顧客に関連付けられている前記オンプレミスネットワーク内に構成されているエージェントに送信することと、

前記セキュアネットワーク接続システム内の前記1つまたは複数のコンピューティングノードのセットのうちの第2のコンピューティングノードが、前記顧客に関連付けられている前記仮想クラウドネットワーク（VCN）内に存在するリソースに関連付けられている情報をクエリするための要求を受信することと、をさらに含み、前記クエリは、前記オンプレミスネットワーク内に存在する前記外部リソースによって送信され、前記外部リソースは、論理インターフェイスをプロビジョンされ、前記方法はさらに、

30

前記第2のコンピューティングノードが、前記オンプレミスネットワーク内に存在する前記外部リソースにプロビジョンされた前記論理インターフェイスと、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された仮想ネットワークインターフェイスカード（VNIC）との間の接続を確立することと、

前記第2のコンピューティングノードが、確立された前記接続を介して前記仮想クラウドネットワーク内に存在する前記リソースに前記要求を送信することと、

前記第2のコンピューティングノードが、前記確立された接続を介して前記要求に対応する結果を得ることと、を含む、方法。

40

【請求項 2】

前記オンプレミスネットワーク内の前記エージェントは、前記オンプレミスネットワーク内に存在する前記外部リソースと、前記セキュアネットワーク接続システムを備える前記1つまたは複数のコンピューティングノードのセットとの間のセキュア仮想プライベートネットワーク（VPN）接続を確立するように構成されている、請求項1に記載の方法。

【請求項 3】

前記エージェントは、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する前記構成情報に少なくとも部分的に基づいて、前記オンプレ

50

レミスネットワーク内に存在する前記外部リソースの前記論理インターフェイスをプロビジョンするように構成されている、請求項 1 または請求項 2 に記載の方法。

【請求項 4】

前記外部リソースの前記論理インターフェイスをプロビジョンすることは、前記エージェントが、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）の前記仮想インターネットプロトコル（IP）アドレスを前記論理インターフェイスに割り当てることを含む、請求項 3 に記載の方法。

【請求項 5】

前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する前記構成情報は、前記仮想ネットワークインターフェイスカード（VNIC）の前記仮想インターネットプロトコル（IP）アドレス、前記仮想ネットワークインターフェイスカード（VNIC）に関連付けられているコンピューティングインスタンスに関連付けられる完全修飾ドメイン名、および、前記顧客に関連付けられている前記仮想クラウドネットワークのクラウド識別子を含む、請求項 3 または請求項 4 に記載の方法。

【請求項 6】

前記第 2 のコンピューティングノードが、前記オンプレミスネットワーク内に存在する前記外部リソースにプロビジョンされた前記論理インターフェイスと、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカードとの間の前記接続を確立することは、前記オンプレミスネットワーク内に存在する前記エージェントを介して前記接続を確立することを含む、請求項 1 ～請求項 5 のいずれか 1 項に記載の方法。

【請求項 7】

前記第 2 のコンピューティングノードが、確立された前記接続を介して前記仮想クラウドネットワーク内に存在する前記リソースに前記要求を送信することは、

前記第 2 のコンピューティングノードが、前記外部リソースに関連付けられている前記物理 IP アドレスを、前記顧客に関連付けられている前記仮想クラウドネットワーク内の前記外部リソース表現の前記仮想ネットワークインターフェイスカードに関連付けられる前記仮想 IP アドレスに変換することと、

第 2 のコンピューティングノードが、前記仮想ネットワークインターフェイスカードに関連付けられる前記仮想 IP アドレスに前記要求を送信することと、を含む、請求項 1 ～請求項 6 のいずれか 1 項に記載の方法。

【請求項 8】

前記セキュアネットワーク接続システムが、前記顧客に関連付けられている前記オンプレミスネットワークの外部サイト表現の作成を可能にすることをさらに含み、前記外部サイト表現は、前記オンプレミスネットワークの論理表現であり、外部サイト識別子および顧客識別子によって識別される、請求項 1 ～請求項 7 のいずれか 1 項に記載の方法。

【請求項 9】

前記外部リソースは、前記外部サイト表現内に登録される、請求項 8 に記載の方法。

【請求項 10】

前記第 2 のコンピューティングノードが、前記外部サイト表現内に存在する前記外部リソースにプロビジョンされた前記論理インターフェイスと、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカードとの間の接続を確立することをさらに含む、請求項 9 に記載の方法。

【請求項 11】

前記外部リソースは、前記オンプレミスネットワーク内に存在するデータベース、アプリケーション、または計算インスタンスである、請求項 1 ～請求項 10 のいずれか 1 項に記載の方法。

【請求項 12】

クラウドサービスプロバイダにおいて実装される、前記クラウドサービスプロバイダの顧客に関連付けられているオンプレミスネットワークと前記顧客のために前記クラウドサ

10

20

30

40

50

ービスプロバイダによってホストされている仮想クラウドネットワーク（VCN）との間の安全なプライベートネットワーク接続を可能にするためのセキュアネットワーク接続システムであって、前記セキュアネットワーク接続システムは、1つまたは複数のコンピューティングノードのセットを含む仮想オーバーレイネットワークを備え、前記コンピューティングノードのセットのうちのコンピューティングノードは、

メモリと、

処理を実施するように構成されている1つまたは複数のプロセッサと、を備え、前記処理は、

前記セキュアネットワーク接続システムが、前記オンプレミスネットワーク内に存在する外部リソースを、前記仮想クラウドネットワーク内の外部エンドポイントとして登録することを含み、前記外部エンドポイントは、前記仮想クラウドネットワーク内のインターネットプロトコル（IP）アドレスによって識別され、前記処理はさらに、

10

前記セキュアネットワーク接続システム内の前記1つまたは複数のコンピューティングノードのセットのうちの第1のコンピューティングノードが、前記仮想クラウドネットワーク内の前記外部エンドポイントの外部リソース表現を作成することを含み、前記外部リソース表現を作成することは、

前記セキュアネットワーク接続システム内の前記1つまたは複数のコンピューティングノードのセットのうちの前記第1のコンピューティングノードが、仮想ネットワークインターフェイスカード（VNIC）を作成することと、

前記セキュアネットワーク接続システム内の前記1つまたは複数のコンピューティングノードのセットのうちの前記第1のコンピューティングノードが、前記外部エンドポイントに関連付けられている前記インターネットプロトコル（IP）アドレスを前記仮想ネットワークインターフェイスカード（VNIC）に割り当てることと、をさらに含み、前記処理はさらに、

20

前記セキュアネットワーク接続システム内の前記第1のコンピューティングノードが、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する構成情報を、前記顧客に関連付けられている前記オンプレミスネットワーク内に構成されているエージェントに送信することと、

前記セキュアネットワーク接続システム内の前記1つまたは複数のコンピューティングノードのセットのうちの第2のコンピューティングノードが、前記顧客に関連付けられている前記仮想クラウドネットワーク（VCN）内に存在するリソースに関連付けられている情報をクエリするための要求を受信することと、を含み、前記クエリは、前記オンプレミスネットワーク内に存在する前記外部リソースによって送信され、前記外部リソースは、論理インターフェイスをプロビジョンされ、前記処理はさらに、

30

前記セキュアネットワーク接続システム内の前記第2のコンピューティングノードが、前記オンプレミスネットワーク内に存在する前記外部リソースにプロビジョンされた前記論理インターフェイスと、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカード（VNIC）との間の接続を確立することと、

前記セキュアネットワーク接続システム内の前記第2のコンピューティングノードが、確立された前記接続を介して前記仮想クラウドネットワーク内に存在する前記リソースに前記要求を送信することと、

40

前記セキュアネットワーク接続システム内の前記第2のコンピューティングノードが、前記確立された接続を介して前記要求に対応する結果を得ることと、を含む、セキュアネットワーク接続システム。

【請求項13】

前記オンプレミスネットワーク内の前記エージェントは、前記オンプレミスネットワーク内に存在する前記外部リソースと、前記セキュアネットワーク接続システムを備える前記1つまたは複数のコンピューティングノードのセットとの間のセキュア仮想プライベートネットワーク（VPN）接続を確立するように構成されている、請求項12に記載のシ

50

ステム。

【請求項 1 4】

前記エージェントは、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する前記構成情報に少なくとも部分的に基づいて、前記オンプレミスネットワーク内に存在する前記外部リソースの前記論理インターフェイスをプロビジョンするように構成されている、請求項 1 2 または請求項 1 3 に記載のシステム。

【請求項 1 5】

前記外部リソースの前記論理インターフェイスをプロビジョンすることは、前記エージェントが、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）の前記仮想インターネットプロトコル（IP）アドレスを前記論理インターフェイスに割り当てることを含む、請求項 1 4 に記載のシステム。

10

【請求項 1 6】

前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する前記構成情報は、前記仮想ネットワークインターフェイスカード（VNIC）の前記仮想インターネットプロトコル（IP）アドレス、前記仮想ネットワークインターフェイスカード（VNIC）に関連付けられているコンピューティングインスタンスに関連付けられる完全修飾ドメイン名、および、前記顧客に関連付けられている前記仮想クラウドネットワークのクラウド識別子を含む、請求項 1 2 ～請求項 1 5 のいずれか 1 項に記載のシステム。

【請求項 1 7】

プログラムコードを記憶している非一時的コンピュータ可読媒体であって、前記プログラムコードは、1 つまたは複数の処理デバイスによって複数の動作を実施するために実行可能であり、前記複数の動作は、

20

前記オンプレミスネットワーク内に存在する外部リソースを、仮想クラウドネットワーク内の外部エンドポイントとして登録することを含み、前記外部エンドポイントは、前記仮想クラウドネットワーク内のインターネットプロトコル（IP）アドレスによって識別され、前記複数の動作はさらに、

前記仮想クラウドネットワーク内の前記外部エンドポイントの外部リソース表現を作成することを含み、前記外部リソース表現を作成することは、

仮想ネットワークインターフェイスカード（VNIC）を作成することと、

30

前記外部エンドポイントに関連付けられている前記インターネットプロトコル（IP）アドレスを前記仮想ネットワークインターフェイスカード（VNIC）に割り当てることと、を含み、前記複数の動作はさらに、

前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する構成情報を、前記顧客に関連付けられている前記オンプレミスネットワーク内に構成されているエージェントに送信することと、

前記顧客に関連付けられている前記仮想クラウドネットワーク（VCN）内に存在するリソースに関連付けられている情報をクエリするための要求を受信することと、を含み、前記クエリは、前記オンプレミスネットワーク内に存在する前記外部リソースによって送信され、前記外部リソースは、論理インターフェイスをプロビジョンされ、前記複数の動作はさらに、

40

前記オンプレミスネットワーク内に存在する前記外部リソースにプロビジョンされた前記論理インターフェイスと、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカード（VNIC）との間の接続を確立することと、

確立された前記接続を介して前記仮想クラウドネットワーク内に存在する前記リソースに前記要求を送信することと、

前記確立された接続を介して前記要求に対応する結果を得ることと、を含む、非一時的コンピュータ可読媒体。

【請求項 1 8】

50

前記エージェントは、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する前記構成情報に少なくとも部分的に基づいて、前記オンプレミスネットワーク内に存在する前記外部リソースの前記論理インターフェイスをプロビジョンするように構成されている、請求項１７に記載の非一時的コンピュータ可読媒体。

【請求項１９】

前記外部リソースの前記論理インターフェイスをプロビジョンすることは、前記エージェントが、前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）の前記仮想インターネットプロトコル（IP）アドレスを前記論理インターフェイスに割り当てることを含む、請求項１８に記載の非一時的コンピュータ可読媒体。

【請求項２０】

前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する前記構成情報は、前記仮想ネットワークインターフェイスカード（VNIC）の前記仮想インターネットプロトコル（IP）アドレス、前記仮想ネットワークインターフェイスカード（VNIC）に関連付けられているコンピューティングインスタンスに関連付けられる完全修飾ドメイン名、および、前記顧客に関連付けられている前記仮想クラウドネットワークのクラウド識別子を含む、請求項１７～請求項１９のいずれか１項に記載の非一時的コンピュータ可読媒体。

【請求項２１】

コンピュータプログラム命令を含むコンピュータプログラム製品であって、前記コンピュータプログラム命令は、プロセッサによって実行されると、前記プロセッサに、

前記オンプレミスネットワーク内に存在する外部リソースを、仮想クラウドネットワーク（VCN）内の外部エンドポイントとして登録することを行わせ、前記外部エンドポイントは、前記仮想クラウドネットワーク（VCN）内のインターネットプロトコル（IP）アドレスによって識別され、前記コンピュータプログラム命令は、プロセッサによって実行されると、前記プロセッサにさらに、

前記仮想クラウドネットワーク（VCN）内の前記外部エンドポイントの外部リソース表現を作成することをさらに行わせ、前記外部リソース表現を作成する動作は、

仮想ネットワークインターフェイスカード（VNIC）を作成する動作と、

前記外部エンドポイントに関連付けられている前記インターネットプロトコル（IP）アドレスを前記仮想ネットワークインターフェイスカード（VNIC）に割り当てる動作と、を含み、前記コンピュータプログラム命令は、プロセッサによって実行されると、前記プロセッサにさらに、

前記外部リソース表現の前記仮想ネットワークインターフェイスカード（VNIC）に対応する構成情報を、前記顧客に関連付けられている前記オンプレミスネットワーク内に構成されているエージェントに送信することと、

前記顧客に関連付けられている前記仮想クラウドネットワーク（VCN）内に存在するリソースに関連付けられている情報をクエリするための要求を受信することと、を行わせ、前記クエリは、前記オンプレミスネットワーク内に存在する前記外部リソースによって送信され、前記外部リソースは、論理インターフェイスをプロビジョンされ、前記コンピュータプログラム命令は、プロセッサによって実行されると、前記プロセッサにさらに、

前記オンプレミスネットワーク内に存在する前記外部リソースにプロビジョンされた前記論理インターフェイスと、前記仮想クラウドネットワーク内の前記外部リソース表現向けに作成された前記仮想ネットワークインターフェイスカード（VNIC）との間の接続を確立することと、

確立された前記接続を介して前記仮想クラウドネットワーク（VCN）内に存在する前記リソースに前記要求を送信することと、

前記確立された接続を介して前記要求に対応する結果を得ることと、を行わせる、コンピュータプログラム製品。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願への相互参照

本出願は、2021年10月29日付けで出願された「Secure Bi-Directional Network Connectivity System between Private Networks」と題する米国非仮特許出願第17/515,093号のPCT出願であり、米国特許法第119条(e)項に基づくその利益および優先権を主張するものであり、その内容は、参照によりその全体があらゆる目的のために本明細書に組み込まれる。

【0002】

本出願は、2021年10月29日付けで出願された「Transparent mounting of external endpoints between private networks」と題する米国特許出願第17/515,087号に関連し、その内容は、参照によりあらゆる目的のために本明細書に組み込まれる。

10

【0003】

技術分野

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

【背景技術】

20

【0004】

背景

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

30

【発明の概要】

【発明が解決しようとする課題】

【0005】

クラウドサービスによって提供される多数の利点を活用するために、企業には、オンプレミスアプリケーションおよびデータを企業のローカルデータセンタから公衆クラウドインフラストラクチャへと移動させることを要求されることが多い。このプロセスは、典型的には、企業が、企業のオンプレミスデータセンタとクラウドインフラストラクチャとの間の安全な接続を確立するために、サイト間ネットワーク接続をセットアップすることを必要とする。異なるネットワーク間のネットワークトラフィックを処理するための高性能で、スケーラブルな、かつ高可用性のサイト間ネットワーク接続を構成することは、特に、企業のオンプレミスアプリケーションおよびデータが複数の異なるネットワークにわたってスケーリングするときに、企業にとって複雑で時間のかかるタスクになり得る。

40

【0006】

簡潔な概要

本開示は、概して、クラウドベースのサービスに関する。より詳細には、ただし決して限定することなく、本開示は、顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間の安全なプライベート双方向ネットワーク接続を

50

確立する改善された機能を含むクラウドインフラストラクチャ内のセキュアプライベートネットワーク接続サービスを記載する。

【課題を解決するための手段】

【0007】

ある実施形態において、セキュアネットワーク接続システムが開示される。セキュアネットワーク接続サービスは、クラウドサービスプロバイダの顧客に関連付けられているオンプレミスネットワークと顧客のためにクラウドサービスプロバイダによってホストされている仮想クラウドネットワーク（VCN）との間の安全なプライベートネットワーク接続を可能にする。セキュアネットワーク接続システムは、1つまたは複数のコンピューティングノードのセットを含む仮想オーバーレイネットワークを備える。システムは、オンプレミスネットワーク内に存在する外部リソースを、仮想クラウドネットワーク内の外部エンドポイントとして登録する。外部エンドポイントは、仮想クラウドネットワーク内のインターネットプロトコル（IP）アドレスによって識別される。システム内のコンピューティングノードのセットのうちの第1のコンピューティングノードは、仮想クラウドネットワーク内の外部エンドポイントの外部リソース表現を作成する。外部リソース表現は、仮想ネットワークインターフェイスカード（VNIC）を作成し、外部エンドポイントに関連付けられているインターネットプロトコル（IP）アドレスをVNICに割り当てることによって作成される。次いで、第1のコンピューティングノードは、外部リソース表現のVNICに対応する構成情報を、顧客に関連付けられているオンプレミスネットワーク内に構成されているエージェントに送信する。

10

20

【0008】

ある例において、システム内のコンピューティングノードのセットのうちの第2のコンピューティングノードは、顧客に関連付けられているVCN内に存在するリソースに関連付けられている情報をクエリするための要求を受信する。クエリは、オンプレミスネットワーク内に存在する外部リソースによって送信される。ある実施態様において、外部リソースは、論理インターフェイスをプロビジョンされる。第2のコンピューティングノードは、オンプレミスネットワーク内に存在する外部リソースにプロビジョンされた論理インターフェイスと、仮想クラウドネットワーク内の外部リソース表現向けに作成されたVNICとの間の接続を確立する。第2のコンピューティングノードは、確立された接続を介して仮想クラウドネットワーク内に存在するリソースに要求を送信し、確立された接続を介して要求に対応する結果を得る。

30

【0009】

ある実施形態において、オンプレミスネットワーク内のエージェントは、オンプレミスネットワーク内に存在する外部リソースと、セキュアネットワーク接続システムを備える1つまたは複数のコンピューティングノードのセットとの間のセキュア仮想プライベートネットワーク（VPN）接続を確立するように構成されている。ある例において、エージェントは、外部リソース表現のVNICに対応する構成情報に少なくとも部分的に基づいて、オンプレミスネットワーク内に存在する外部リソースの論理インターフェイスをプロビジョンするように構成されている。ある例において、外部リソースの論理インターフェイスをプロビジョンすることは、エージェントによって、外部リソース表現の仮想ネットワークインターフェイスカード（VNIC）の仮想インターネットプロトコル（IP）アドレスを論理インターフェイスに割り当てることを含む。

40

【0010】

ある例において、外部リソース表現のVNICに対応する構成情報は、VNICの仮想インターネットプロトコル（IP）アドレス、VNICに関連付けられているコンピューティングインスタンスに関連付けられる完全修飾ドメイン名、および、顧客に関連付けられている仮想クラウドネットワークのクラウド識別子を含む。

【0011】

ある例において、第2のコンピューティングノードは、オンプレミスネットワーク内に存在するエージェントを介して、オンプレミスネットワーク内に存在する外部リソースに

50

プロビジョンされた論理インターフェイスと、仮想クラウドネットワーク内の外部リソース表現向けに作成された仮想ネットワークインターフェイスカードとの間の接続を確立する。

【0012】

ある例において、第2のコンピューティングノードは、確立された接続を介して仮想クラウドネットワーク内に存在するリソースに要求を送信する。このプロセスは、第2のコンピューティングノードによって、外部リソースに関連付けられている物理IPアドレスを、顧客に関連付けられている仮想クラウドネットワーク内の外部リソース表現のVNICに関連付けられる仮想IPアドレスに変換することと、VNICに関連付けられる仮想IPアドレスに要求を送信することを含む。

10

【0013】

ある例において、セキュアネットワーク接続システムは、顧客に関連付けられているオンプレミスネットワークの外部サイト表現の作成を可能にする。外部サイト表現は、オンプレミスネットワークの論理表現であり、外部サイト識別子および顧客識別子によって識別される。ある例において、外部リソースは、外部サイト表現内に登録される。

【0014】

ある例において、セキュアネットワーク接続システム内の第2のコンピューティングノードは、外部サイト表現内に存在する外部リソースにプロビジョンされた論理インターフェイスと、仮想クラウドネットワーク内の外部リソース表現向けに作成された仮想ネットワークインターフェイスカードとの間の接続を確立する。ある例において、外部リソースは、オンプレミスネットワーク内に存在するデータベース、アプリケーション、または計算インスタンスである。

20

【0015】

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

【図面の簡単な説明】

30

【0016】

【図1】ある実施形態による、クラウドサービスプロバイダインフラストラクチャ(CSPI)内のセキュアプライベートネットワーク接続サービスを含む分散環境100を示す図である。

【図2】ある実施形態による、顧客のオンプレミスネットワーク内に存在する顧客の外部リソースと顧客のVCN内に存在するリソースおよびサービスとの間の安全なプライベートネットワーク接続を提供するための、図1に示すシステムおよびサブシステムによって実施される動作の追加の詳細を示す図である。

【図3】ある実施形態による、安全なプライベートネットワーク接続を提供するための、図1に示すシステムおよびサブシステムによって実施されるプロセスの例を示す図である。

40

【図4】ある実施形態による、顧客のオンプレミスネットワーク内に存在する外部リソースと顧客の仮想クラウドネットワーク内の外部リソースとの間のネットワークパケットの流れを示すフローチャートである。

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

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

50

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

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

【図 9】ある実施形態によるマルチテナンシ機能をサポートするために I / O 仮想化を提供するためのホストマシンと N V D との間の接続を示す図である。

【図 10】ある実施形態による C S P I によって提供される物理ネットワークの単純化されたブロック図である。

【図 11】少なくとも 1 つの実施形態による、クラウドインフラストラクチャをサービスシステムとして実装するための 1 つのパターンを示すブロック図である。

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

【図 13】少なくとも 1 つの実施形態による、クラウドインフラストラクチャをサービスシステムとして実装するための別のパターンを示すブロック図である。

【図 14】少なくとも 1 つの実施形態による、クラウドインフラストラクチャをサービスシステムとして実装するための別のパターンを示すブロック図である。

【図 15】少なくとも 1 つの実施形態による、例示的なコンピュータシステムを示すブロック図である。

【発明を実施するための形態】

【0017】

詳細な説明

以下の記載において、説明を目的として、ある実施形態の完全な理解を提供するために、具体的な詳細が記載される。しかしながら、様々な実施形態は、これらの特定の詳細なしに実施され得ることが明らかであろう。図面および説明は、限定であるようには意図されていない。「例示的な」という語は本明細書においては、「例、事例、または実例としての役割を果たす」ことを意味するように使用される。「例示的」として本明細書において記載されている任意の実施形態または設計は、必ずしも、他の実施形態または設計よりも好ましいかまたは有利であるものとして解釈されるべきではない。

【0018】

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

【0019】

クラウドインフラストラクチャは、物理アンダーレイネットワークの上で作動し、企業のオンプレミスネットワークから安全にアクセス可能である柔軟なオーバーレイ仮想ネットワークにおいて高性能な計算、記憶、およびネットワーク機能を提供することができる。クラウドインフラストラクチャは、企業が、そのオンプレミスワークロードを管理すると同じように、そのクラウドベースのワークロードを管理することを可能にする。したがって、企業は、そのオンプレミスネットワークと同じ制御、分離、セキュリティ、および予測可能性能によって、クラウドのすべての恩恵を得ることができる。企業は、クラウドによって提供される計算、メモリ、およびネットワークリソースを使用して、それ自体のネットワークを構築することができる。例えば、顧客は、クラウドによって提供されるリソースを使用して、仮想クラウドネットワーク（V C N）として参照される 1 つまたは複数のカスタマイズ可能なプライベートネットワークを構築することができる。顧客は、これらの顧客 V C N 上で、計算インスタンスなどの 1 つまたは複数の顧客リソースを展開することができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどの形態をとることができる。したがって、クラウドは、企業（顧客）が多様なアプリケーションおよびサービスを可用性の高いホスト環境内で構築し、実行することを可能にする

10

20

30

40

50

インフラストラクチャ、および、補完クラウドサービスのセットを提供する。

【0020】

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

【0021】

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

【0022】

ある実施形態において、顧客のオンプレミス環境内に存在する外部リソースとクラウド内に存在する顧客のリソースとの間の安全なプライベート双方向ネットワーク接続を確立する改善された機能を含むクラウドサービスプロバイダインフラストラクチャ（CSP）内のセキュアプライベートネットワーク接続サービスが記載される。セキュアプライベートネットワーク接続サービスは、クラウドサービスプロバイダインフラストラクチャ（CSP）内のセキュアネットワーク接続システム（SNCS）を使用して実施される。本開示に記載されているSNCSは、従来のクラウドベースのネットワーク接続サービスにまさるいくつかの技術的利点および／または改善を提供する。SNCSによって実装される本開示の新規の改善されたアーキテクチャを使用して、企業のユーザ（例えば、管理者）が明示的に外部リソースを構成し、経路を公告し、またはサイト間ネットワーク接続をセットアップする必要なしに、顧客の外部サイト表現内に存在する外部リソースと、ク

クラウド内の顧客のVCN内に存在するリソースおよびサービスとの間の安全なプライベート双方向ネットワーク接続を達成することができる。SNCSは、安全なサイト間ネットワーク接続を提供するために使用されるネットワーク要素およびコンピューティングノードのロバストなインフラストラクチャを実装することによって、顧客のオンプレミス環境とCSP Iとの間のネットワークトラフィックを処理するための高性能で、スケーラブルな、かつ高可用性のサイト間ネットワーク接続を提供する。SNCSによって実装されるネットワーク要素およびコンピューティングノードのロバストなインフラストラクチャを使用することによって、企業のユーザは、そのVCN内の任意の他のネイティブリソースに接続しているかのように、クラウドからその外部リソースに安全にアクセスすることができる。付加的に、SNCSは、顧客のオンプレミスネットワーク内に存在する1つまたは複数の外部リソースが、顧客のVCN（すなわち、クラウド）内に存在するリソースおよびサービスに安全にリーチアウトし、アクセスすることができることを可能にする。企業のユーザ（例えば、管理者）が明示的に外部リソースを構成し、経路を公告し、またはサイト間ネットワーク接続をセットアップする必要なしに、顧客の外部サイト表現内の外部リソースと、クラウド内の顧客のVCN内に存在するリソースおよびサービスとの間の安全なプライベート双方向ネットワーク接続を達成することができる。

10

20

30

40

50

【0023】

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

【0024】

図1に示す例に示すように、分散環境100は、顧客が加入することができるサービスおよびリソースを提供するCSP I 102を備える。ある実施形態において、CSP I 102は、顧客のオンプレミスネットワークとCSP I 102によってホストされる顧客のVCNとの間の安全な双方向プライベートネットワークを提供する機能を含むセキュアプライベートネットワーク接続サービスを提供する。図1に示す例において、セキュアプライベートネットワーク接続サービスは、CSP I 102内のセキュアネットワーク接続システム（SNCS）104によって実施することができる。SNCS 104によって提供されるセキュアプライベートネットワーク接続サービスは、顧客のオンプレミスネットワーク内に存在する1つまたは複数のリソース（本明細書においては外部リソースまたはリモート資産としても参照される）が、顧客のVCN内に存在するリソースおよびサービスに安全にアクセスすることができることを可能にする。SNCS 104によって提供されるセキュアプライベートネットワーク接続サービスは、付加的に、顧客のVCN内のリソースおよびサービスが、顧客のオンプレミスネットワークに存在する外部リソースに安全にアクセスすることを可能にする。顧客は、顧客のVCN内に存在する任意の他のネイティブリソースに接続しているかのように、そのVCN内から外部リソースにアクセスすることができる。オンプレミス外部リソースと顧客のVCN（すなわち、クラウド）内に存在するリソースとの間の安全なアクセスは、顧客（例えば、企業のユーザ）がそのオンプレミスネットワークとクラウドとの間の入り組んだサイト間ネットワーク接続を設定することを必要とすることなく、顧客が、その外部リソースに何ら変更を行う必要なしに、または、顧客が、サイト間接続によって使用される経路を構成する必要なしに、可能にすることができる。顧客のオンプレミスネットワーク内に存在する外部リソースとクラウド内の顧客のリソースおよびサービスとの間の安全な双方向接続を可能にするためにSNCS

104によって実施される処理の追加の詳細は、下記により詳細に説明する。

【0025】

ある手法において、顧客のオンプレミスネットワーク内に存在する外部リソースとクラウド（例えば、顧客のVCN）内の顧客のリソースおよびサービスとの間の安全な双方向接続は、SNCS104によって、多段階プロセスを使用して達成される。第1の段階において、顧客に関連付けられているユーザ（例えば、管理者）が、顧客のオンプレミスネットワークの「外部サイト表現」106を作成することができる。例えば、ユーザは、外部サイト表現106を作成するために、ユーザデバイスによって実行されるアプリケーションのコンソールユーザインターフェイス（UI）108を介して、APIを介して、または、ユーザのデバイスによって実行されるコマンドラインインターフェイス（CLI）を介して、SNCS104と相互に作用することができる。外部サイト表現（例えば、106）は、顧客の外部サイト（例えば、オンプレミスネットワーク／オンプレミスデータセンタ）の論理または仮想表現を表すことができ、外部サイト識別子およびテナント（顧客）識別子によって識別することができる。例として外部サイト表現106は、顧客のオンプレミスネットワークの一部分およびオンプレミスネットワーク内に存在する1つまたは複数の外部リソースのサブセットを論理的に表す高レベルコンテナリソースを表すことができる。

10

【0026】

第2の段階において、ユーザが、エージェント112をダウンロードし、外部サイト表現106内にエージェント112をインストール／構成する。ある実施形態において、エージェント112は、ユーザがSNCS104によって提供されるセキュアプライベート接続サービスに加入するときに、SNCS104によって提供されるダウンロードパッケージの一部としてユーザによってダウンロードされるソフトウェアアプリケーションであり得る。エージェント112は、ユーザによって、コンソールUI108を介して外部サイト表現106内にインストールおよび構成され得る。

20

【0027】

第3の段階において、エージェント112を外部サイト表現106内にインストールするのに成功すると、SNCS104が、エージェント112を認証し、顧客のテナント特有のオーバーレイネットワーク128のセットアップを指揮する。テナント特有のオーバーレイネットワーク128は、SNCSによって提供されるサービスに加入している各テナント（顧客）のためにSNCS104によって物理ネットワークの上に構築される仮想オーバーレイネットワークを表すことができる。テナント特有のオーバーレイネットワーク128は、顧客の外部サイト表現106とCSP内の顧客のVCN148との間に安全なプライベートネットワーク接続を確立するために使用される。図1に示す実施形態に示すように、テナント特有のオーバーレイネットワーク128は、1つまたは複数のトンネルホスト（本明細書においてはトンネル仮想マシンとしても参照される）、トンネルVM-1 116およびトンネルVM-2 122のセット、ならびに、1つまたは複数のリソースホスト（本明細書においてはリソース仮想マシンとしても参照される）、リソースVM-1 130およびリソースVM-2 132のセットを含むコンピューティングノードの分散された水平方向にスケーラブルなフリートを含むことができる。ホスト（例えば、トンネルホストまたはリソースホスト）は、テナント特有のオーバーレイネットワーク128内で互いに相互接続されているコンテナ（本明細書においてはシャードとしても参照される）のセットから構成され得る。トンネルVM116および122は、テナントごとのトンネルシャードを実行するために使用される。例えば、図1に示すように、トンネルVM-1 116は、CSPの特定のテナント／顧客のトンネルシャード120を実行するために使用され、トンネルVM-2 122は、トンネルシャード126を実行するために使用される。各トンネルシャード120または126は、顧客の外部サイト表現106への安全な接続を提供する役割を担う。リソースVM130および132のセットは、テナントリソースシャードごとに実行するために使用することができる。例えば、図1に示すように、リソースVM-1 130は、そのテナント／顧客のリソースシャ

30

40

50

ード136を実行するために使用され、リソースVM-2 132は、リソースシャード140を作動させるために使用される。リソースシャードは、顧客のVCNからトラフィックを受信し、それを顧客の外部サイト表現に転送するために使用することができる。顧客の外部サイト表現106と顧客のVCN148との間の安全な接続を提供するために図1に示すトンネルシャードおよびリソースシャードによって実施される動作の追加の詳細は、図1に詳細に記載されている。

【0028】

各トンネルVM(116、122)およびリソースVM(130、132)は、付加的に、それぞれホストマネジャー(118、134)によって構成される。ホストマネジャー(118、134)は、トンネルVMおよびリソースVM上で実行するプロセスを表す。ホストマネジャー(118または134)は、トンネルおよびリソースシャードを作成するために使用されるAPIを実装することができる。ある実施態様において、ホストマネジャー(118、134)は、ステートレスとすることができ、ユーザから(API108を介して)作成されるべきシャードのタイプ(トンネルまたはリソースシャード)およびシャードのある構成に関する命令を受信することによって、命令モードにおいて(すなわち、ホストマネジャーが実施するための一連のコマンドとして)動作することができる。ホストマネジャーは、付加的に、トンネルシャードおよびリソースシャードのステータスを収集および監視する役割を担うことができる。

【0029】

SNCS104が上述したようにテナント特有のオーバーレイネットワーク128を顧客向けにセットアップした後、第4の段階において、ユーザは、オンプレミス資産(例えば、外部リソース114A)を、そのVCN内の外部エンドポイントとして、外部サイト表現106内に登録する。外部リソース114Aは、顧客が顧客のVCN内に存在するリソースおよびサービスとの安全な双方向接続を確立することを意図する顧客のオンプレミスネットワーク内に存在するデータベース、コンピューティングインスタンス、アプリケーションなどのようなオンプレミスリソースまたは資産を表すことができる。外部リソース114Aを登録するために、ユーザは(コンソールUI108を介して)そのVCN148からの安全なプライベートネットワーク接続を可能にされるべき外部リソース(例えば、114A)を識別し、コンソールUI108を使用して(またはAPIを介して)外部リソースをそのVCN内の外部エンドポイントとして登録する。外部リソースの登録の一部として、ユーザは、SNCSによって提供されるコンソールUIまたはAPIを介して外部リソースに関連付けられているオンプレミス物理IPアドレス、外部リソースがアクセス可能であるポート番号、および、外部リソースのホスト名(または完全修飾ドメイン名(FQDN))などの外部リソースに関連する構成情報を提供する。ユーザはまた、外部リソースの外部エンドポイントが作成されるべきである顧客のVCN内のサブネットも選択する。SNCSは、構成情報を受信し、外部リソースの外部エンドポイントを顧客のVCN内に作成する。外部エンドポイントは、顧客のVCN内のIPアドレス、ポート番号およびFQDN(ホスト名)によって識別される。

【0030】

次いで、第5の段階において、SNCS104が、(制御プレーンAPIを介して)外部エンドポイントの外部リソース表現を顧客のVCN内に作成する。ある実施態様において、外部リソース表現の作成は、リモートマウントポイントVNICを作成することと、外部エンドポイントに関連付けられているIPアドレスをVNICに割り当てることとを含む。次いで、SNCSは、(制御プレーンAPIを介して)VNICを(ワーカインターフェイスを介して)リソースシャードに論理的にアタッチすることが可能であるリソースVM上でリソースシャードを作成する。

【0031】

第6の段階において、エージェント112は、顧客のVCN148内で外部リソース表現114A向けに作成されたVNIC142に関連付けられる構成情報156をダウンロードして読み出し、構成情報156を登録された外部リソース114A上にコピーする。

構成情報は、例えば、VNICの仮想IPアドレス、VNICに関連付けられているコンピューティングインスタンスに関連付けられる完全修飾ドメイン名、および、顧客に関連付けられている仮想クラウドネットワークのクラウド識別子を含み得る。構成情報156を使用して、エージェント112は、外部リソース114Aの論理インターフェイス158を作成／プロビジョンする。論理インターフェイス158は、IPアドレスから成るソフトウェアエンティティを表すことができる。ある実施態様において、エージェント112によって論理インターフェイス158を作成またはプロビジョンすることは、エージェントによって、外部リソース表現向けに作成されたVNIC142に割り当てられた仮想IPアドレスを論理インターフェイス158に割り当ててることを含む。

【0032】

外部リソース114Aは、顧客のVCN内に存在する外部リソース表現のVNIC142に対応する仮想IPアドレスを割り当てられている論理インターフェイス158をプロビジョンされているため、この時点で、外部リソースは、顧客のVCNの一部になり、SNCS104によって提供されるセキュアプライベートネットワーク接続サービスを使用することによってクラウド内（例えば、顧客のVCN148内）にあるリソースおよびサービスに安全にアクセスすることが可能である。例えば、外部リソース114Aは、エージェント112を介してSNCS104内のトンネルホストへの接続を確立することによって、その論理インターフェイス158を介して、顧客のVCN148内の計算インスタンス150または顧客のVCN内のサービス152（例えば、ストリーミングサービスまたはオブジェクト記憶サービス）に安全に到達／アクセスすることができる。同様に、顧客のVCN148内のクライアントアプリケーションは、顧客のVCN148内の任意の他のネイティブリソースに接続しているかのように、外部リソースのVNIC表現142を使用して顧客のオンプレミスネットワーク内の外部リソース114Aに安全にアクセスするために、SNCS104によって提供されるサービスを使用することができる。このように、顧客のオンプレミスネットワーク内に存在する外部リソースとクラウド（例えば、顧客のVCN）内の顧客のリソースおよびサービスとの間の安全な双方向接続は、SNCS104によって達成される。

【0033】

図2は、ある実施形態による、顧客のオンプレミスネットワーク内に存在する顧客の外部リソースと顧客のVCN内に存在するリソースおよびサービスとの間の安全なプライベートネットワーク接続を提供するための、図1に示すシステムおよびサブシステムによって実施される動作の追加の詳細を示す。図2に示すシステムおよびサブシステムは、コンピューティングシステム、ハードウェア、またはそれらの組み合わせの1つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）を使用して実装することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。図2に示す分散環境200は、例示に過ぎず、特許請求される実施形態の範囲を不当に限定するようには意図されていない。多くの変形、代替、および修正が可能である。例えば、いくつかの他の実施形態において、図2に示す分散環境は、図2に示されているよりも多いもしくは少ないシステムもしくは構成要素を有してもよく、2つ以上のシステムを組み合わせてもよく、または、システムの異なる構成もしくは配置を有し得る。本発明者らは、図2において、大部分は発明1（IaaS272.1）に記載されているシステムアーキテクチャ（SNCS）に基づくシステムを記載している。下記の図2に関する説明を検討し、より明瞭にするために必要であれば、追加／編集されたい。

【0034】

図1において以前に説明したように、顧客のオンプレミスネットワークとCSP102によってホストされる顧客のVCNとの間の安全なプライベートネットワーク接続を提供するためにSNCS104によって実施される接続プロセスの一部として、顧客に関連付けられているユーザ（例えば、管理者）は、顧客のオンプレミスネットワークの「外部サイト表現」（例えば、106）を作成し、外部サイト表現内でエージェント（例えば、

10

20

30

40

50

112)を構成し、オンプレミス資産を外部サイト表現内に登録し、登録された外部リソースについて顧客のVCN内にリモートマウントポイント(本明細書においてはエンドポイントとしても参照される)を作成する。エージェント(例えば、112)を外部サイト表現内にインストールするのに成功すると、エージェント112は、公衆ネットワーク(例えば、インターネット110)を介したSNCS104への仮想プライベートネットワーク(VPN)接続(本明細書においてはVPNトンネルとしても参照される)を確立する。VPN接続は、顧客の外部サイト表現106と顧客のVCN148との間の暗号化接続である。ある実施態様において、VPN接続は、セキュアトンネリングプロトコル(例えば、レイヤ2トンネリングプロトコル(L2TP)プロトコル)を利用して、インターネット110を介したSNCS104への安全なプライベートネットワーク接続を確立する。エージェント112が外部サイト表現106内にインストールされると、エージェントは、エージェント112に関連付けられるコンパートメント識別子および構成ファイル内の外部サイト表現識別子などの情報をSNCS104に渡すことによって、SNCS104によってそれ自体をアクティブ化するためのブートストラッププロセスを開始する。エージェント112がそれ自体をブートストラップすると、エージェントは、登録およびアクティブ化プロセスを開始するSNCSの制御プレーンと通信する。アクティブ化プロセス中、制御プレーンは、VPNサーバへの安全なトンネル接続を確立するためにゲートウェイ機器によって必要とされるすべての必要な情報(例えば、証明書、公衆IDなど)を返信する。次いで、エージェント112は、SNCSに設置されているVPNサーバへの安全なVPNトンネル接続を開くVPNクライアントプログラムを実行することによって、SNCS104への安全なVPN接続を確立する。安全なトンネルは、SNCS104内のトンネルVM(例えば、116)上に配置されているトンネルシャード(例えば、120)上で終端する。

10

20

30

40

50

【0035】

図1に示す特定の実施態様において、エージェント112は、複数のトンネルシャード、すなわち、それぞれトンネルシャード1120およびトンネルシャード2126内で作動する2つの異なるVPNサーバ、すなわち、VPNサーバ1224およびVPNサーバ2226上で終端するトンネルを確立するように各々が構成されている2つのVPNクライアント、すなわち、VPNクライアント1206およびVPNクライアント2208を有して構成されている。図2に示す実施態様において、エージェント112のすべての物理的な設置の結果として、2つのトンネルが確立され、したがって、1つのトンネルが故障した場合、トラフィック(すなわち、ネットワークパケット)は、自動的に第2のトンネルを回してルーティングすることができる。図2に示す特定の実施態様は2つのトンネルを示しているが、他の実施態様において、SNCS104は、エージェント112のすべての物理的な設置のために3つ以上の冗長なトンネルを実装するように構成されてもよく、または、単にエージェント112の設置を受けて単一のトンネルを実装し得る。

【0036】

ある実施形態において、エージェント112は、ボーダーゲートウェイプロトコル(BGP)などの標準的な外部ゲートウェイプロトコルを使用して、トンネルシャード120および126とのBGPピアリングセッションを確立する。BGPを使用して、エージェント112は、エージェント112内に実装されている公衆インターフェイス220を介して、トンネルシャードとルーティングおよび到達可能性情報を交換する。BGPピアリングセッションに必要とされる構成情報の一部として、エージェント112は、トンネルシャードによって受信されるそのローカル経路テーブル212(本明細書においてはルーティング情報ベース(RIB)としても参照される)にそのオンプレミスIPアドレスを注入する。トンネルシャードは、適切な経路フィルタリングポリシーを適用した後、ルーティング情報をそのローカル経路テーブル(228および236)にインポートする。経路フィルタリングは、欠陥のあるエージェント112が任意の経路をトンネルシャードに注入しないことを保証することが好ましい。ある例において、エージェント112は、付加

的に、ルーティングマネジャー 2 1 4 を備える。ルーティングマネジャー 2 1 4 は、ルーティングスイート（例えば、Quagga）の一部であるオープンソースルーティングマネジャー（例えば、Zebra）を使用して実装され得る。BGPピアリングセッションが、経路を学習し、それをその経路テーブル 2 1 2 にインポートすると、BGPピアリングセッションは、最良経路計算を実施し、ルーティングマネジャー 2 1 4 を使用して、最良の経路をローカルカーネルに追加する。

【0037】

トンネルシャード（例えば、1 2 0、1 2 6）は、1 つまたは複数のコンテナのセットから構成され得る。ある実施態様において、トンネルシャード（1 2 0 または 1 2 6）は、トンネルシャードが、エージェント 1 1 2 と、テナント特有のオーバーレイネットワーク 1 2 8 の一部である他のシャード（例えば、リソースシャード 1 3 6 および 1 4 0）の両方と通信することを可能にする様々なネットワークインターフェイスをセットアップするために使用することができるシェルコンテナを備え得る。図 2 に示す実施形態において、トンネルシャード内のシェルコンテナネット内に実装されるネットワークインターフェイスは、外部サイトインターフェイス（e s i）、トンネルインターフェイスおよびシャードバックエンドインターフェイスを含み得る。例えば、トンネルシャード 1 1 2 0 内に実装されるネットワークインターフェイスは、トンネルインターフェイス 2 1 6、外部サイトインターフェイス 2 2 2 およびシャードバックエンドインターフェイス 2 3 4 を含む。同様に、トンネルシャード 2 1 2 6 内に実装されるネットワークインターフェイスは、トンネルインターフェイス 2 1 8、外部サイトインターフェイス 2 2 3 およびシャードバックエンドインターフェイス 2 3 5 を含む。トンネルシャード（例えば、1 2 0 または 1 2 6）は、付加的に、外部ゲートウェイ機器 1 1 2 内で作動する VPN クライアント（2 0 6、2 0 8）への VPN トンネルを確立するために使用される VPN サーバ（2 2 4、2 2 6）から構成される。外部サイトインターフェイス（2 2 2、2 2 3）は、VPN クライアントがその上で作動するエージェント 1 1 2 にとって既知であり、トンネルシャードへのトンネルを確立するために使用される公衆 IP によって識別することができる。VPN クライアント（例えば、2 0 6、2 0 8）が VPN サーバ（2 2 4、2 2 6）に接続すると、トンネルインターフェイス（2 1 6、2 1 8）が作成され、トンネルシャードの事前構成された VPN サブネット内に配置される。

【0038】

ある実施態様において、各トンネルシャード（例えば、1 2 0、1 2 6）は、ボーダーゲートウェイプロトコル（BGP）を利用して、外部ゲートウェイ機器とトンネルシャードとの間の BGPピアリングセッションおよびトンネルシャードとリソースシャードとの間の BGPピアリングセッションを確立することができる。BGPピアリングセッションは、シャードバックエンドインターフェイス（2 3 4、2 3 5）を介してリソースシャードとルーティングおよび到達可能性情報を交換し、外部サイトインターフェイス（2 2 2、2 2 3）を介して外部サイト表現 1 0 6 とルーティングおよび到達可能性情報を交換するために使用される。BGPピアリングセッションに必要とされる構成情報の一部として、テナント特有のオーバーレイネットワーク 1 2 8 を識別する IP アドレスが、それぞれトンネルシャード 1 2 0、1 2 6 内に実装されている経路テーブル 2 2 8、2 3 6（すなわち、ルーティング情報ベース（RIB））に追加される。ある実施態様において、クラスレスドメイン間ルーティング（CIDR）技法が、IP アドレスをテナント特有のオーバーレイネットワークに割り振るために使用され得る。経路テーブル（2 2 8、2 3 6）は、リソースシャード（1 3 6、1 4 0）および外部サイト表現 1 0 6 などの特定のネットワーク宛先への経路を列挙する。いくつかの事例において、経路テーブル（2 2 8、2 3 6）はまた、それらの経路に関連付けられるメトリック（距離）も列挙する。リソースシャードとの BGPピアリングセッションが確立されると、経路テーブル内の経路は、リソースシャードへと伝搬される。図 2 に示すように各トンネルシャード（1 2 0、1 2 6）は、付加的に、ルーティングマネジャー（2 2 8、2 4 0）を備える。ルーティングマネジャー（2 2 8 または 2 4 0）は、外部ゲートウェイ機器 1 1 2 内に実装されているル

ーティングマネジャー（２１４）と同様に実装され得る。ＢＧＰが経路を学習し、それらの経路をトンネルシャード内の経路テーブルにインポートすると、ＢＧＰは、最良経路計算を実施し、ルーティングマネジャーを使用して、最良の経路を外部サイト表現１０６およびリソースシャード１３６、１４０にプッシュする。

【００３９】

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

【００４０】

ある実施態様において、すべての登録された外部エンドポイント（すなわち、外部サイト表現内の外部リソースに対応する）について、一意のプロキシサーバコンテナが立ち上げられ、リソースシャードにアタッチされる。外部リソースを登録し、顧客のＶＣＮ内の登録された外部エンドポイントのリモートマウントポイントＶＮＩＣを作成するとき、ユーザは、外部リソースのＩＰアドレス、外部リソースのポート番号、および外部リソースの名前などの構成情報をＳＮＣＳ１０４に提供することができる。この構成情報は、プロキシサーバ内にプロビジョンされ、顧客のＶＣＮ内のクライアントアプリケーションによって、外部リソースに接続するために使用される。外部リソースがＳＮＣＳによって顧客のＶＣＮ内の外部エンドポイントとして首尾よく登録されると、ＳＮＣＳ１０４は、（制御プレーンＡＰＩを介して）ＶＮＩＣを作成し、外部エンドポイントに関連付けられているＩＰアドレスをＶＮＩＣに割り当てる。

【００４１】

図２に示す例において、登録された外部エンドポイント（すなわち、外部サイト表現内の外部リソース）は、外部サイト表現１０６内に存在するデータベース２０２を表す。プロキシサーバ（２４４、２５４）は、登録された外部エンドポイント２０２向けに作成されているＶＮＩＣ２０６に割り当てられている仮想ＩＰアドレスをリスンする。これによって、外部サイト表現内の他の登録された外部リソースにアクセスするために同じＶＮＩＣＩＰが使用され得ないことが保証される。顧客のＶＣＮ内で作動しているクライアントアプリケーション１４４が、外部データベース２０２内に記憶されている情報を得るためのクエリを受信すると、クライアントアプリケーションは、顧客のＶＣＮ内のＶＮＩＣＩＰにネットワークパケットを送信する。ネットワークパケットは、リソースシャード（１３６、１４０）にアタッチされているワーカＶＮＩＣ（２５１、２５２）によって受信される。ワーカＶＮＩＣは、ＶＮＩＣの仮想ＩＰアドレスを有して構成されており、それによって、プロキシサーバ（２４４、２５４）を介して外部サイト表現内の登録された外部リソースへの接続を開始する。プロキシサーバ（２４４、２５４）は、ＶＮＩＣ２０６に割り当てられた仮想ＩＰアドレスを外部サイト表現１０６内の外部リソース１１４Ａの現実の／物理ＩＰアドレスに変換するためのネットワークアドレス変換（ＮＡＴ）を実施する。プロキシサーバ（２４４、２５４）を使用するリソースシャード（例えば１３６、１４０）は、トンネルシャード（１２０、１２６）を介したエージェント１１２への接続を開始する。エージェント１１２は、トンネルシャード（１２０、１２６）からネットワ

ークパケットを受信し、次いで、パケットを外部サイト表現 106 内の登録された外部リソース（すなわち、データベース 202）にルーティングする。プロキシサーバ（244、254）は、付加的に、外部リソースへのネットワークトラフィックをトンネルシャードにわたって負荷平衡させる機能を含む。ある実施形態において、プロキシサーバ（244、254）は、複数のクライアントアプリケーションからの接続を、外部サイト表現に向けた単一の接続に多重化するように構成することができる。

【0042】

同様に、外部サイト表現 106 内に存在する登録された外部リソース（すなわち、データベース 202）は、顧客の VCN 内に存在するリソース（例えば、計算インスタンス 150）またはサービス（例えば、プライベートエンドポイント VNIC 152）にリーチアウトし、安全にアクセスすることができる。図 1 において前述したように、エージェント 112 は、外部リソース 202 の論理インターフェイス 204 を作成／プロビジョンする。外部リソース 114A の論理インターフェイス 158 を作成し、データベース 202 の VNIC 表現 206 の仮想 IP アドレスを論理インターフェイスに割り当てることによって、データベース 202（顧客のオンプレミスネットワーク内に存在する）は、SNCS 104 によって提供されるセキュアプライベートネットワーク接続サービスを使用して、顧客の VCN 148 内のプライベートエンドポイント VNIC 142 を介して顧客の VCN 148 内の計算インスタンス 150 またはサービス 156（例えば、CSP I 内のストリーミングサービスまたはオブジェクト記憶サービス）に安全にアクセスすることが可能である。例えば、図 2 に示す実施形態において、エージェント 112 は、顧客の VCN 内のリソース（例えば、150）に関連付けられている情報を要求するクエリをデータベース 202 から受信することができる。次いで、エージェント 112 は、クエリに対応するネットワークパケットをトンネルシャード（120、126）に送信する。次いで、トンネルシャードは、リソースシャード（136、140）への接続を開始する。リソースシャード（136、140）内のプロキシサーバ（244、254）は、外部サイト表現 106 内の外部リソースの現実の IP アドレスを顧客の VCN 内の外部リソース（例えば、データベース 202）の VNIC 表現 206 の仮想 IP アドレスに変換するためのネットワークアドレス変換（NAT）を実施する。次いで、リソースシャード（136、140）にアタッチされているワーカ VNIC（251、252）は、クエリに対応するネットワークパケットを顧客の VCN 内の要求しているリソース（例えば、150）に送信する顧客の VCN 内のデータベース 202 の VNIC 表現 206 への接続を開始する。このように、SNCS 104 は、顧客のオンプレミスネットワーク内に存在する外部リソース（例えば、データベース 202）と顧客の VCN（すなわち、クラウド）内のリソース（例えば、150）およびサービス（例えば、152）との間に安全なプライベート双方向ネットワーク接続が確立されることを保証する。

【0043】

ある実施態様において、顧客の VCN 148 からのプライベート接続を要求する登録された外部エンドポイントは、本明細書においては顧客の VCN 148 内の「SVNIC」としても参照される、サービス VNIC として実装され得る。SVNIC は、CSP I 102 によって、仮想クラウドネットワーク間のトラフィックを処理し、送信するために複数の VNIC（例えば、サービス VNIC 254）をホストすることが可能である CSP I 102 によって実施される水平方向にスケーラブルなサービスを表すことができるサービス型 VNIC（VNICaaS）システム（図 2 には示さず）を使用して実装することができる。具体的には、VNICaaS は、VNIC がサービス（すなわち、SVNIC）として表現または使用されることを可能にする仮想ネットワーキング特徴である。VNICaaS は、特定の SmartNIC、または、VNIC をホストするための仮想ネットワーク内の計算インスタンスのホストを必要とすることなく、VNIC の機能を提供する。登録されたエンドポイントを SVNIC として表現するために使用される技法は、「Techniques for high performant virtual routing capabilities」と題する米国特許出願第 17/175,573 号に詳細に記載されている。米国特許出願第 17/175,573 号に

10

20

30

40

50

記載されている技法は例として意図されているに過ぎず、限定であるようには意図されていない。代替的な実施形態において、登録されたエンドポイントを表現し、仮想クラウドネットワーク間のトラフィックを処理および送信するために、様々な他の技法も使用され得る。SVNICは、すべての登録された外部エンドポイント（例えば、データベース202）向けに作成されるため、SVNICごとに柔軟な数のワーカを構成することができる。特定の実施態様において、すべてのSVNICが、異なるリソースシャード（例えば、136、140）にアタッチされている2つのワーカVNIC（例えば、251、252）に関連付けられ得る。ワーカVNICは、リソースシャードに入れられ、SVNICIPによって構成される。

【0044】

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

【0045】

SNCS104によって実装される本開示の新規の改善されたアーキテクチャを使用して、企業のユーザ（例えば、管理者）が明示的に外部リソースを構成し、経路を公告し、またはサイト間ネットワーク接続をセットアップする必要なしに、顧客の外部サイト表現内の外部リソースと、クラウド内の顧客のVCN内に存在するリソースおよびサービスとの間の安全なプライベート双方向ネットワーク接続を達成することができる。記載されているように、安全なプライベート双方向ネットワーク接続は、SNCSによって、顧客の外部サイト表現と顧客のVCNとの間の暗号化接続を使用して、および、顧客向けにテナント特有のオーバーレイネットワークをセットアップする前にエージェントを認証することによって、確立される。SNCS104は、SNCS104によって提供されるサービスを使用する各テナント／顧客のためのネットワーク要素およびコンピューティングノードのロバストなインフラストラクチャ（すなわち、テナント特有のオーバーレイネットワーク128）を実装することによって、顧客のオンプレミス環境とCSPとの間のネットワークトラフィックを処理するための高性能で、スケーラブルな、かつ高可用性のサイト間ネットワーク接続を提供する。テナント特有のオーバーレイネットワーク128内のトンネルホストは、顧客の外部サイト表現106への安全な接続を提供するために使用され、リソースホストは、顧客のVCNからトラフィックを受信し、それを顧客の外部サイト表現に転送するために使用される。リソースホストは、付加的に、外部サイト表現内の外部リソースからトラフィックを受信し、それを顧客のVCN内に存在するリソースまたはサービスに転送することが可能である。テナント特有のオーバーレイネットワークによって実装されるネットワーク要素およびコンピューティングノードのロバストなインフラ

10

20

30

40

50

ストラクチャを使用することによって、企業は、そのVCN内の任意の他のネイティブリソースに接続しているかのように、クラウドからその外部リソースに安全にアクセスすることができる。企業のユーザは、そのオンプレミスネットワークとクラウドとの間の入り組んだサイト間ネットワークを設定することなく、その外部リソースに何ら変更を行うことなく、かつ、サイト間接続によって使用される経路を構成することなく、その外部リソースにアクセスすることができる。同様に、外部リソースの論理インターフェイスを作成し、論理インターフェイスを外部リソースのVNIC表現の仮想IPアドレスに関連付けることによって、外部リソース（顧客のオンプレミスネットワーク内に存在する）は、SNCS104によって提供されるセキュアプライベートネットワーク接続サービスを使用してクラウド内（例えば、顧客のVCN148内）にあるリソースおよびサービスに安全にアクセスすることが可能である。

10

【0046】

図3は、ある実施形態による、安全なプライベートネットワーク接続を提供するための、図1に示すシステムおよびサブシステムによって実施されるプロセスの例を示す。図3に示す処理は、それぞれのシステム、ハードウェア、またはそれらの組み合わせの1つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）内で実施することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。図3に提示されており、下記に説明されるプロセス300は、例示的であり、非限定的であるように意図されている。図3は、特定のシーケンスまたは順序において行われる様々な処理ステップを示しているが、これは限定であるようには意図されていない。ある代替的な実施形態において、ステップは、何らかの異なる順序で実施されてもよく、または、一部のステップはまた、並列に実施され得る。図1に示す実施形態などのある実施形態において、図3に示す処理は、テナント特有のオーバーレイネットワーク128を備えるコンピューティングノード（例えば、116、122、130および132）によって実施され得る。

20

【0047】

図3に示す処理は、顧客に関連付けられているユーザ（例えば、管理者）が、顧客のオンプレミスネットワークの外部サイト表現（例えば、106）を作成しており、外部サイト表現106内のエージェント（例えば、112）を構成していると仮定する。図4に示す処理は、SNCS104がエージェント112を認証しており、顧客のためのコンピューティングノードの分散された水平方向にスケーラブルなフリートを含むテナント特有のオーバーレイネットワーク（例えば、128）を構成／確立しているとさらに仮定する。図1において記載されているように、1つまたは複数のコンピューティングノードのセットは、リソースホスト（すなわち、リソース仮想マシン130、132）およびトンネルホスト（すなわち、トンネル仮想マシン116、122）を含む。

30

【0048】

図3に示す処理は、ブロック302において、SNCS104が、コンピューティングノードの分散された水平方向にスケーラブルなフリートを含むテナント特有のオーバーレイネットワーク（例えば、128）を実行するときに開始することができる。テナント特有のオーバーレイネットワークは、顧客の外部サイト表現とCSP内の顧客のVCN（例えば、148）との間に安全なプライベートネットワーク接続を確立するために使用される。

40

【0049】

ブロック304において、SNCSは（制御プレーンAPIを介して）、顧客のオンプレミスネットワーク内に存在する外部リソースを、顧客のVCN内の外部エンドポイントとして登録する。外部エンドポイントは、顧客のVCN内のIPアドレスによって識別される。前述したように、外部リソースは、顧客がそのVCN内からの安全な双方向プライベートネットワーク接続を可能にすることを意図する外部サイト表現106内のデータベース、コンピューティングインスタンス、またはアプリケーションを表すことができる。外部リソースの登録の一部として、SNCSのユーザは、コンソールUIまたはAPIを

50

介して外部リソースに関連付けられているオンプレミス物理IPアドレス、外部リソースがアクセス可能であるポート番号、および、外部リソースのホスト名（または完全修飾ドメイン名（FQDN））などの外部リソースに関連する構成情報を提供する。ユーザはまた、外部リソースの外部エンドポイントが作成されるべきである顧客のVCN内のサブネットも選択する。構成情報に基づいて、SNCSは、外部リソースの外部エンドポイントを顧客のVCN内に作成する。外部エンドポイントは、顧客のVCN内のIPアドレス、ポート番号およびFQDN（ホスト名）によって識別される。

【0050】

ブロック306において、SNCS内の第1のコンピューティングノード（例えば、リソースVM130またはリソースVM132）が、顧客のVCN内の外部エンドポイントの外部リソース表現を作成する。ある実施態様において、外部リソース表現の作成は、コンピューティングノードによって、VNICを作成することと、外部エンドポイントのIPアドレスをVNICに割り当てることを含む。

【0051】

ブロック308において、第1のコンピューティングノードが、顧客のVCN内の外部リソース表現向けに作成されたVNICに対応する構成情報を、オンプレミスネットワーク内に構成されているエージェント112に送信する。ブロック308において実施される処理の一部として、エージェント112は、構成情報をダウンロードし、オンプレミスネットワーク内に存在する登録された外部リソースにコピーする。前述したように、構成情報は、例えば、VNICの仮想IPアドレス、VNICに関連付けられているコンピューティングインスタンスに関連付けられる完全修飾ドメイン名、および、顧客に関連付けられている仮想クラウドネットワークのクラウド識別子を含み得る。構成情報を使用して、エージェント112は、外部リソース（例えば、114A）の論理インターフェイス（例えば、158）を作成／プロビジョンする。ある実施態様において、エージェント112によって論理インターフェイスを作成またはプロビジョンすることは、エージェントによって、外部リソース表現向けに作成されたVNIC142に割り当てられた仮想IPアドレスを外部リソース114A向けにプロビジョンされている論理インターフェイス158に割り当てることを含む。

【0052】

ブロック310において、第2のコンピューティングノード（例えば、トンネルVM116またはトンネルVM122）が、顧客のVCN内に存在するリソース（例えば、計算インスタンス150）に関連付けられている情報をクエリするための要求を受信する。ある例において、要求は、オンプレミスネットワーク内に存在する外部リソース（例えば、114A）によって、その論理インターフェイス158を介して送信される。例えば、顧客に関連付けられているユーザは、顧客のVCN内に存在する計算インスタンス150に関連付けられている情報をクエリするための要求を（UI108を介して）顧客のオンプレミスネットワーク内に存在する外部リソースに送信することができる。次いで、外部リソースは、オンプレミスネットワーク内に存在するエージェント112にクエリを送信することができる。エージェント112は、クエリ要求を受信し、クエリ要求に対応するネットワークパケットを、トンネルVM内で作動しているトンネルシャード（120または126）に送信する。

【0053】

ブロック312において、第2のコンピューティングノード（例えば、トンネルVM116またはトンネルVM122）が、リソースシャード（例えば、136または140）を介して、外部リソースにプロビジョンされた論理インターフェイスと、顧客のVCN内の外部リソース表現向けに作成されたVNICとの間の接続を確立する。特定の実施態様において、トンネルシャード（例えば、120または126）は、外部リソースに割り当てられた現実の／物理IPアドレスをVNIC142の仮想IPアドレスに変換し、リソースシャード（136または140）を介したVNIC142への接続を開始するための機能を含むことができる。次いで、リソースシャードは、顧客のVCN内のリソース（例

10

20

30

40

50

えば、150)への接続を開始する。

【0054】

ブロック314において、第2のコンピューティングノード（例えば、トンネルVM116またはトンネルVM122）が、ブロック410において確立された接続を介して顧客のVCN内に存在するリソースに要求を送信する。ブロック412において、第2のコンピューティングノードが、確立された接続を介して要求に対応する結果を得る。次いで、結果は、エージェント112を介して外部サイト表現内に存在する外部リソースに送信される。例えば、リソースが顧客のVCN内で作動するデータベースである場合、結果は、データベース内の1つまたは複数のテーブル内に格納された情報を含み得る。

【0055】

図4は、ある実施形態による、顧客のオンプレミスネットワーク内に存在する外部リソースと顧客の仮想クラウドネットワーク内の外部リソースの表現との間のネットワークパケットの流れを示すフローチャートである。図4に示す処理は、それぞれのシステム、ハードウェア、またはそれらの組み合わせの1つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）内で実施することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。図4に提示されており、下記に説明されるプロセス400は、例示的であり、非限定的であるように意図されている。図4は、特定のシーケンスまたは順序において行われる様々な処理ステップを示しているが、これは限定であるようには意図されていない。ある代替的な実施形態において、ステップは、何らかの異なる順序で実施されてもよく、または、一部のステップはまた、並列に実施され得る。図2に示す実施形態などのある実施形態において、図4に示す処理は、テナント特有のオーバーレイネットワーク128を備えるコンピューティングノード（例えば、116、122、130および132）によって実施され得る。

【0056】

図4に示す処理は、ブロック402において、顧客のオンプレミスネットワーク（すなわち、顧客の外部サイト表現106）内に存在する外部リソース（例えば、データベース202）が、顧客のVCN（例えば、148）内に存在するリソース（例えば、150）に関連付けられている情報に対するクエリを受信するときに開始することができる。前述したように、顧客に関連付けられているユーザは、顧客のVCN内に存在する計算インスタンス150に関連付けられている情報をクエリするための要求を（UI108を介して）顧客のオンプレミスネットワーク内に存在する外部リソースに送信することができる。次いで、外部リソースは、オンプレミスネットワーク内に存在するエージェント112にクエリを送信することができる。

【0057】

ブロック404において、エージェント112が、クエリを受信し、クエリに対応するネットワークパケットを、トンネルVM内で作動しているトンネルシャード（120または126）に送信する。ある例において、ブロック404において実施される処理の一部として、エージェント112は、ネットワークパケットをトンネルシャードに送信する前に、ネットワークパケットを暗号化することができる。

【0058】

ブロック406において、トンネルシャードが、暗号化ネットワークパケットを受信し、リソースVM内で作動しているリソースシャード（136、140）に暗号化ネットワークパケットを送信する。具体的には、図2に示すように、暗号化ネットワークパケットは、リソースシャード（136、140）にアタッチされているワーカVNIC（251、252）によって受信することができる。

【0059】

ブロック408において、リソースシャード（136、140）が、ネットワークパケットを解読し、外部リソースに割り当てられた物理IPアドレスを、顧客のVCN内の外部リソース表現に関連付けられるVNIC（例えば、206）の仮想IPアドレスに変換

10

20

30

40

50

するためのネットワークアドレス変換（NAT）を実施する。

【0060】

ブロック410において、リソースシャード（136、140）が、顧客のVCN内の外部リソース表現向けに作成されたVNICにネットワークパケットを送信する。

【0061】

ブロック412において、VNICが、クエリに対応するネットワークパケットを、顧客のVCNに存在するリソース（例えば、150）に送信する。

【0062】

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

【0063】

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

【0064】

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

【0065】

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

【0066】

ブロック508において、トンネルシャードが、顧客の外部サイト表現内に存在するエ

10

20

30

40

50

エージェント 112 にネットワークパケットを送信する。ブロック 508 において実施される処理の一部として、エージェント 112 は、ネットワークパケットを外部サイト表現（例えば、106）内の外部リソース（例えば、202）に送信する前に、ネットワークパケットを解読する。

【0067】

ブロック 510 において、エージェント 112 が、顧客の外部サイト表現内に存在する外部リソース（例えば、202）にネットワークパケットを送信する。外部リソースは、クエリに対応するネットワークパケットを受信し、クエリに対応する応答ネットワークパケットを生成する。次いで、応答ネットワークパケットは、外部リソースによってクライアントアプリケーションに返送することができる。例えば、応答ネットワークパケットフローの一部として、クエリに対する応答に対応するネットワークパケットが、外部リソースからエージェントに送信される。エージェントは、ネットワークパケットを暗号化し、暗号化ネットワークパケットをトンネルシャードに送信する。トンネルシャードは、暗号化パケットを受信し、リソースシャードにパケットを送信する。リソースシャードは、ネットワークパケットを解読し、外部リソースに割り当てられた物理／現実の IP アドレスを、顧客の VCN 内の外部リソース表現に関連付けられる VNIC の仮想 IP アドレスに変換するための逆ネットワークアドレス変換（NAT）を実施する。次いで、リソースシャードは、応答ネットワークパケットを VNIC に送信し、VNIC は、次いで、顧客の VCN 148 内の要求しているクライアントアプリケーション 144 に応答パケットを送信する。

【0068】

例示的な仮想ネットワーキングアーキテクチャ

クラウドサービスという用語は、一般的に、クラウドサービスプロバイダ（CSP）によって、CSP によって提供されるシステムおよびインフラストラクチャ（クラウドインフラストラクチャ）を使用して要求に応じて（例えば、サブスクリプションモデルを介して）ユーザまたは顧客に利用可能にされるサービスを指すために使用される。典型的には、CSP のインフラストラクチャを構成するサーバおよびシステムは、顧客自身のオンプレミスサーバおよびシステムとは別個のものである。したがって、顧客は、サービスのための別個のハードウェアおよびソフトウェアリソースを購入する必要なしに、CSP によって提供されるクラウドサービスを利用することができる。クラウドサービスは、顧客がサービスの提供に使用されるインフラストラクチャの獲得に投資を行う必要なしに、アプリケーションおよびコンピューティングリソースへの容易でスケーラブルなアクセスを、加入している顧客に提供するように設計されている。

【0069】

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

【0070】

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

【0071】

上記で言及したように、サービス型インフラストラクチャ（IaaS）は、1 つの特定のタイプのクラウドコンピューティングサービスである。IaaS モデルにおいて、CSP は、顧客によって、自身のカスタマイズ可能なネットワークを構築し、顧客リソースを展開するために使用することができるインフラストラクチャ（クラウドサービスプロバイ

ダイインフラストラクチャまたはC S P Iとして参照される)を提供する。したがって、顧客のリソースおよびネットワークは、C S Pによって提供されるインフラストラクチャによって、分散環境においてホストされる。これは、顧客のリソースおよびネットワークが顧客によって提供されるインフラストラクチャによってホストされる従来のコンピューティングとは異なる。

【0072】

C S P Iは、基盤ネットワークまたはアンダーレイネットワークとしても参照される、物理ネットワークを形成する様々なホストマシン、メモリリソース、およびネットワークリソースを含む、相互接続された高性能の計算リソースを含むことができる。C S P I内のリソースは、1つまたは複数の地理的領域にわたって地理的に分散され得る1つまたは複数のデータセンタにわたって分散され得る。これらの物理リソースによって、仮想化ソフトウェアを実行して、仮想化分散環境を提供することができる。仮想化は、物理ネットワークの上にオーバーレイネットワーク(ソフトウェアベースのネットワーク、ソフトウェア定義ネットワーク、または仮想ネットワークとしても知られる)を作成する。C S P I物理ネットワークは、物理ネットワークの上に1つまたは複数のオーバーレイまたは仮想ネットワークを作成するための下層基盤を提供する。物理ネットワーク(または基盤ネットワークまたはアンダーレイネットワーク)は、物理スイッチ、ルータ、コンピュータおよびホストマシンなどのような、物理ネットワークデバイスを含む。オーバーレイネットワークは、物理基盤ネットワークの上で作動する論理(または仮想)ネットワークである。所与の物理ネットワークは、1つまたは複数のオーバーレイネットワークをサポートすることができる。オーバーレイネットワークは、典型的には、カプセル化技法を使用して、異なるオーバーレイネットワークに属するトラフィックを区別する。仮想またはオーバーレイネットワークは、仮想クラウドネットワーク(V C N)としても参照される。仮想ネットワークは、物理ネットワークの上で作動することができるネットワーク抽象化の層を作成するためのソフトウェア仮想化技術(例えば、ハイパーバイザ、ネットワーク仮想化デバイス(N V D)によって実装される仮想化機能(例えば、smart N I C)、トップオブラック(T O R)スイッチ、N V Dによって実施される1つまたは複数の機能を実装するスマートT O R、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、典型的には、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。この仮想またはオーバーレイネットワークング方法は、仮想またはオーバーレイレイヤ3ネットワークングとして参照されることが多い。仮想ネットワークのために展開されるプロトコルの例は、I P - i n - I P(または一般ルーティングカプセル化(G R E))、仮想拡張可能L A N(V X L A N - I E T F R F C 7 3 4 8)、仮想プライベートネットワーク(V A N)(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 4 3 6 4))、V M w a r eのN S X、G E N E V E(一般ネットワーク仮想化カプセル化)などを含む。

【0073】

I a a Sの場合、C S Pによって提供されるインフラストラクチャ(C S P I)は、公衆ネットワーク(例えば、インターネット)を介して仮想化コンピューティングリソースを提供するように構成することができる。I a a Sモデルにおいて、クラウドコンピューティングサービスプロバイダは、インフラストラクチャ構成要素(例えば、サーバ、記憶デバイス、ネットワークノード(例えば、ハードウェア)、展開ソフトウェア、プラットフォーム仮想化(例えば、ハイパーバイザ層)など)をホストすることができる。いくつかの事例において、I a a Sプロバイダはまた、それらのインフラストラクチャ構成要素に付随させるための様々なサービス(例えば、請求、監視、ログ記録、セキュリティ、負荷平衡およびクラスタリングなど)を供給することもできる。したがって、これらのサービスはポリシ駆動であり得るため、I a a Sユーザは、アプリケーション可用性およびパフォーマンスを維持するために負荷平衡を駆動するためのポリシーを実装することが可能であり得る。C S P Iは、顧客が多様なアプリケーションおよびサービスを可用性の高いホ

スト分散環境内で構築し、実行することを可能にするインフラストラクチャ、および、補完クラウドサービスのセットを提供する。C S P Iは、顧客のオンプレミスネットワークなどの様々なネットワーク接続されたロケーションから安全にアクセス可能である柔軟な仮想ネットワーク内で、高性能の計算リソースおよび機能ならびに記憶容量を供給する。顧客がC S Pによって提供されるI a a Sサービスに加入または登録するとき、その顧客向けに作成されるテナンシは、顧客がそのクラウドリソースを作成、編成、および管理することができる、C S P I内の安全で隔離された区分である。

【0074】

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

【0075】

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展開されるリソースを構成、アクセス、および管理することを可能にするコンソールを提供することができる。ある実施形態において、コンソールは、C S P Iにアクセスおよび管理するために使用することができるウェブベースのユーザインターフェイスを提供する。いくつかの実施態様において、コンソールは、C S Pによって提供されるウェブベースのアプリケーションである。

【0076】

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

【0077】

物理ネットワークにおいて、ネットワークエンドポイント（「エンドポイント」）は、物理ネットワークに接続されており、接続されているネットワークと往復して通信するコンピューティングデバイスまたはシステムを指す。物理ネットワーク内のネットワークエンドポイントは、ローカルエリアネットワーク（L A N）、広域ネットワーク（W A N）、または他のタイプの物理ネットワークに接続され得る。物理ネットワーク内の従来のエンドポイントの例は、モデム、ハブ、ブリッジ、スイッチ、ルータ、および他のネットワーキングデバイス、物理コンピュータ（またはホストマシン）などを含む。物理ネットワーク内の各物理デバイスは、デバイスと通信するために使用することができる固定ネットワークアドレスを有する。この固定ネットワークアドレスは、レイヤ2アドレス（例えば、M A Cアドレス）、固定レイヤ3アドレス（例えば、I Pアドレス）などとなることが

できる。仮想化環境または下層ネットワークにおいて、エンドポイントは、物理ネットワークの構成要素によってホストされる（例えば、物理ホストマシンによってホストされる）仮想マシンなどの様々な仮想エンドポイントを含むことができる。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、ネットワークマネージャーが、ソフトウェア管理を使用して（例えば、仮想ネットワークの制御プレーンを実装するソフトウェアを介して）ネットワークエンドポイントに関連付けられるオーバーレイアドレスを転々と移動することを可能にすることによって、柔軟性を可能にする。したがって、物理ネットワークとは異なり、仮想ネットワークにおいて、オーバーレイアドレス（例えば、オーバーレイIPアドレス）は、ネットワーク管理ソフトウェアを使用して1つのエンドポイントから別のエンドポイントへと移動させることができる。仮想ネットワークは物理ネットワークの上に構築されるため、仮想ネットワーク内の構成要素間の通信は、仮想ネットワークと、下層の物理ネットワークの両方を含む。そのような通信を促進するために、CSPの構成要素は、仮想ネットワーク内のオーバーレイアドレスを基盤ネットワーク内の実際の物理アドレスにマッピングし、および、その逆を行うマッピングを学習し、記憶するように構成されている。このとき、これらのマッピングは、通信を促進するために使用される。仮想ネットワーク内のルーティングを促進するために、顧客トラフィックがカプセル化される。

10

20

30

40

50

【0078】

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

【0079】

クラウドインフラストラクチャまたはCSPは、世界中の1つまたは複数の領域内で、1つまたは複数のデータセンタ内で物理的にホストされる。CSPは、物理または基盤ネットワーク内の構成要素、および、物理ネットワーク構成要素の上に構築される仮想ネットワーク内にある仮想化構成要素（例えば、仮想ネットワーク、計算インスタンス、仮想マシンなど）を含むことができる。ある実施形態において、CSPは、レルム、リージョンおよび可用性ドメインに編成され、ホストされる。リージョンは、典型的には、1つまたは複数のデータセンタを含む局所的な地理的エリアである。リージョンは、一般的に、互いに独立しており、例えば、国またはさらには大陸をまたいで大きい距離によって分離することができる。例えば、第1のリージョンは、オーストラリア内にあってもよく、別のリージョンは日本内にあってもよく、さらに別のリージョンはインド内にあり得る、などである。CSPリソースは、複数のリージョンの間で分割され、結果、各リージョンは、CSPリソースのそれ自体の独立したサブセットを有する。各リージョンは

、計算リソース（例えば、ベアメタルサーバ、仮想マシン、コンテナおよび関連するインフラストラクチャなど）、ストレージリソース（例えば、ブロックボリュームストレージ、ファイルストレージ、オブジェクトストレージ、アーカイブストレージ）、ネットワーキングリソース（例えば、仮想クラウドネットワーク（VCN）、負荷平衡リソース、オンプレミスネットワークへの接続）、データベースリソース、エッジネットワーキングリソース（例えば、DNS）、ならびにアクセス管理および監視リソースなどのような、基幹インフラストラクチャサービスおよびリソースのセットを提供することができる。各リージョンは、一般的に、それをレルム内の他のリージョンに接続する複数の経路を有する。

【0080】

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

【0081】

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

【0082】

リージョン内のADは、互いから分離されており、耐障害性であり、同時に機能しなくなる可能性が非常に低いように構成されている。これは、あるリージョン内の1つのADにおける障害が、同じリージョン内の他のADの可用性に影響を及ぼす可能性が低くなるように、ADが、ネットワーキング、物理ケーブル、ケーブル経路、ケーブル入口点などのような重大なインフラストラクチャリソースを共有しないことによって達成される。同じリージョン内のADは、低レイテンシ高帯域幅ネットワークによって互いに接続することができ、これによって、他のネットワーク（例えば、インターネット、顧客のオンプレミスネットワークなど）への高可用性接続を提供し、高可用性と災害復旧の両方のために複数のAD内に複製システムを構築することが可能になる。クラウドサービスは、複数のADを使用して、高可用性を保証し、リソース障害に対して保護する。IaaSによって提供されるインフラストラクチャが増加すると、より多くのリージョンおよびADが、容量を付加して追加される。可用性ドメイン間のトラフィックは、通常、暗号化される。

【0083】

ある実施形態において、リージョンはレルムにグループ化される。レルムは、複数のリージョンの論理的集合である。レルムは、互いに分離されており、一切のデータを共有しない。同じレルム内のリージョンは、互いに通信することができるが、異なるレルム内のリージョンは、互いに通信することができない。CSPを有する顧客のテナンシおよびアカウントは、単一のレルム内に存在し、そのレルムに属する1つまたは複数のリージョンにわたって分散することができる。典型的には、顧客がIaaSサービスに加入すると、レルム内の顧客が指定するリージョン（「ホーム」リージョンとして参照される）内に、その顧客のテナンシおよびアカウントが作成される。顧客は、顧客のテナンシを、レルム内の1つまたは複数の他の領域にまたがって拡張することができる。顧客は、顧客のテナンシが存在するレルム内にはないリージョンにアクセスすることはできない。

【0084】

IaaSプロバイダは、複数のレルムを提供することができ、各レルムは、顧客または

10

20

30

40

50

ユーザの特定のセットに供される。例えば、商業レلمは、商業顧客に対して提供され得る。別の例として、特定の国のためのレلمが、その国の中の顧客に対して提供され得る。さらに別の例として、政府レلمが、政府に対して提供され得る、などである。例えば、政府レلمは、特定の政府に対して供されてもよく、商業レلمよりも高められたセキュリティレベルを有し得る。例えば、Oracleクラウドインフラストラクチャ（OCI）は、現在、商業リージョンの1つのレلم、および、政府クラウドリージョンの2つのレلم（例えば、FedRAMP認可およびIL5認可）を提供している。

【0085】

ある実施形態において、ADは、1つまたは複数のフォールトドメインに細分化することができる。フォールトドメインは、アンチアフィニティを提供するためのAD内のインフラストラクチャリソースのグループ分けである。フォールトドメインは、インスタンスが単一のAD内の同じ物理ハードウェア上にないように、計算インスタンスを分散させることを可能にする。これは、アンチアフィニティとして知られている。フォールトドメインは、単一の障害点を共有するハードウェア構成要素（コンピュータ、スイッチなど）のセットを指す。計算プールは、複数のフォールトドメインに論理的に分割される。これに起因して、1つのフォールトドメインに影響を及ぼすハードウェア障害または計算ハードウェアメンテナンスイベントは、他のフォールトドメイン内のインスタンスに影響を及ぼさない。実施形態に応じて、各ADのフォールトドメインの数は変化し得る。例えば、ある実施形態において、各ADは、3つのフォールトドメインを含む。フォールトドメインは、AD内の論理データセンタとして作用する。

【0086】

顧客がIaaSサービスに加入すると、CSPからのリソースが顧客にプロビジョンされ、顧客のテナンシに関連付けられる。顧客は、これらのプロビジョンされたリソースを使用して、プライベートネットワークを構築し、これらのネットワーク上にリソースを展開することができる。CSPによってクラウド内でホストされる顧客ネットワークは、仮想クラウドネットワーク（VCN）として参照される。顧客は、顧客に割り振られた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）をセットアップすることができる。VCNは、仮想またはソフトウェア定義のプライベートネットワークである。顧客のVCN内に展開される顧客リソースは、計算インスタンス（例えば、仮想マシン、ベアメタルインスタンス）および他のリソースを含むことができる。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ような様々な顧客ワークロードを表すことができる。VCN上に展開される計算インスタンスは、インターネットなどの公衆ネットワーク上の公衆アクセス可能エンドポイント（「公衆エンドポイント」）、同じVCNまたは他のVCN（例えば、顧客の他のVCN、または顧客に属しないVCN）内の他のインスタンス、顧客のオンプレミスデータセンタまたはネットワーク、ならびに、サービスエンドポイントおよび他のタイプのエンドポイントと通信することができる。

【0087】

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

【0088】

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

【0089】

ある実施形態において、VCNが作成されると、VCNは、VCNに割り当てられる一定範囲のプライベートオーバーレイIPアドレス（例えば、10.0/16）である、プライベートオーバーレイクラスレスドメイン間ルーティング（CIDR）アドレス空間に関連付けられる。VCNは、関連付けられるサブネット、経路テーブル、およびゲートウェイを含む。VCNは、単一のリージョン内に存在するが、リージョンの可用性ドメインの1つまたは複数またはすべてにまたがることができる。ゲートウェイは、VCN向けに構成されており、VCNへの、および、VCNからVCNの外側の1つまたは複数のネットワークへのトラフィックの通信を可能にする仮想インターフェイスである。1つまたは複数の異なるタイプのゲートウェイが、異なるタイプのエンドポイントへの、および、そこからの通信を可能にするために、VCN向けに構成され得る。

【0090】

VCNは、1つまたは複数のサブネットなどの1つまたは複数のサブネットワークに細分化することができる。したがって、サブネットは、VCN内に作成することができる構成単位または下位区分である。VCNは、1つまたは複数のサブネットを有することができる。VCN内の各サブネットは、そのVCN内の他のサブネットと重なり合わず、VCNのアドレス空間内のアドレス空間サブセットを表す、連続した範囲のオーバーレイIPアドレス（例えば、10.0.0.0/24および10.0.1.0/24）に関連付けられる。

【0091】

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

【0092】

各計算インスタンスは、計算インスタンスに関連付けられるVNICを介して、プライベートオーバーレイIPアドレスを割り当てられる。このプライベートオーバーレイIPアドレスは、計算インスタンスが作成され、計算インスタンスへのおよびそこからのトラ

10

20

30

40

50

フィックをルーティングするために使用されるときに、計算インスタンスに関連付けられる V N I C に割り当てられる。所与のサブネット内のすべての V N I C が、同じ経路テーブル、セキュリティリスト、および D H C P オプションを使用する。上述したように、V C N 内の各サブネットは、その V C N 内の他のサブネットと重なり合わず、V C N のアドレス空間内のアドレス空間サブセットを表す、連続した範囲のオーバーレイ IP アドレス（例えば、10.0.0.0 / 24 および 10.0.1.0 / 24）に関連付けられる。V C N の特定のサブネット上の V N I C について、V N I C に割り当てられるプライベートオーバーレイ IP アドレスは、サブネットに割り振られる連続した範囲のオーバーレイ IP アドレスからのアドレスである。

【0093】

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

【0094】

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

【0095】

上述したように、V C N は、1 つまたは複数のサブネットに細分化することができる。ある実施形態において、V C N 向けに構成された仮想ルータ（V R）（V C N V R または単に V R として参照される）が、V C N のサブネット間の通信を可能にする。V C N 内のサブネットについて、V R は、サブネット（すなわち、そのサブネット上の計算インスタンス）が、V C N 内の他のサブネット上のエンドポイントおよび V C N の外側の他のエンドポイントと通信することを可能にする、そのサブネットの論理ゲートウェイを表す。V C N V R は、V C N 内の V N I C と、V C N に関連付けられる仮想ゲートウェイ（「ゲートウェイ」）との間でトラフィックをルーティングするように構成されている論理エンティティである。ゲートウェイは、図 6 に関してさらに下記に説明される。V C N V R は、レイヤ 3 / IP レイヤ概念である。1 つの実施形態において、V C N に対して 1 つの V C N V R が存在し、V C N V R は、可能性として、IP アドレスによってアドレス指定される無限数のポートを有し、V C N の各サブネットに対して 1 つのポートがある。このように、V C N V R は、V C N V R がアタッチされる、V C N 内の各サブネットに対する異なる IP アドレスを有する。V R はまた、V C N 向けに構成されている様々なゲートウェイにも接続されている。ある実施形態において、サブネットのオーバーレイ IP アドレス範囲からのあるオーバーレイ IP アドレスは、そのサブネットの V C N V R のポートのために予約される。例えば、それぞれ関連付けられるアドレス範囲 10.0

／16および10.1/16を有する2つのサブネットを有するVCNを考察する。アドレス範囲10.0/16を有するVCN内の第1のサブネットについて、この範囲からのアドレスは、そのサブネットのVCN VRのポートのために予約される。いくつかの事例において、その範囲からの第1のIPアドレスが、VCN VRのために予約され得る。例えば、オーバーレイIPアドレス範囲10.0/16を有するサブネットについて、IPアドレス10.0.0.1が、そのサブネットのVCN VRのポートのために予約され得る。アドレス範囲10.1/16を有する同じVCN内の第2のサブネットについて、VCN VRは、IPアドレス10.1.0.1を有するその第2のサブネットのポートを有し得る。VCN VRは、VCN内のサブネットの各々に対して異なるIPアドレスを有する。

10

【0096】

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

20

【0097】

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

30

【0098】

VCN向けに構成されているセキュリティ規則は、VCNに対するオーバーレイファイアウォール規則を表す。セキュリティ規則は、進入および脱出規則を含むことができ、VCN内のインスタンスに入ることおよび出ることを許容されるトラフィックのタイプを（プロトコルおよびポートに基づいて）指定することができる。顧客は、所与の規則がステートフルであるかまたはステートレスであるかを選択することができる。例えば、顧客は、ソースCIDR0.0.0.0/0および宛先TCPポート22を有するステートフル進入規則をセットアップすることによって、任意の場所からのSSHトラフィックがインスタンスのセットに入来することを可能にすることができる。セキュリティ規則は、ネットワークセキュリティグループまたはセキュリティリストを使用して実施することができる。ネットワークセキュリティグループは、そのグループ内のリソースのみに適用されるセキュリティ規則のセットから成る。他方、セキュリティリストは、セキュリティリストを使用する任意のサブネット内のすべてのリソースに適用される規則を含む。VCNには、デフォルトのセキュリティ規則を有するデフォルトのセキュリティリストを提供することができる。VCN向けに構成されているDHCPオプションは、インスタンスが起動するときにVCN内のインスタンスに自動的に提供される構成情報を提供する。

40

【0099】

ある実施形態において、VCNの構成情報は、VCN制御プレーンによって決定され、記憶される。VCNの構成情報は、例えば、VCNに関連付けられるアドレス範囲、VC

50

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

【0100】

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

【0101】

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

【0102】

CSP Iを使用してクラウドベースのサービスを実施するための様々な異なるアーキテクチャが、図6、図7、図8、図9、図10、図11、図12、図13、および図15に示されており、下記に説明される。図6は、ある実施形態によるCSP Iによってホストされるオーバーレイまたは顧客VCNを示す分散環境600の高レベル図である。図6に示す分散環境は、オーバーレイネットワーク内の複数の構成要素を含む。図6に示す分散環境600は、例示に過ぎず、特許請求される実施形態の範囲を不当に限定するようには意図されていない。多くの変形、代替、および修正が可能である。例えば、いくつかの実施態様において、図6に示す分散環境は、図1に示されているよりも多いもしくは少ないシステムもしくは構成要素を有してもよく、2つ以上のシステムを組み合わせてもよく、または、システムの異なる構成もしくは配置を有し得る。

【0103】

図6に示す例に示すように、分散環境600は、顧客が加入し、その仮想クラウドネットワーク（VCN）を構築するために使用することができるサービスおよびリソースを提供するCSP I 601を備える。ある実施形態において、CSP I 601は、加入している顧客にIaaSサービスを供給する。CSP I 601内のデータセンタは、1つまたは複数のリージョンに編成することができる。1つの例示的なリージョンである「リージョンUS」602が、図6に示されている。顧客は、リージョン602の顧客VCN 604を構成している。顧客は、VCN 604上に様々な計算インスタンスを展開することができる。ここで、計算インスタンスは、仮想マシンまたはベアメタルインスタンスを含み得る。インスタンスの例は、アプリケーション、データベース、ロードバランサなどを含む。

【0104】

図6に示す実施形態において、顧客VCN 604は、2つのサブネット、すなわち「サブネット1」および「サブネット2」を含み、各サブネットが、それ自体のCIDR IPアドレス範囲を有する。図6において、サブネット1のオーバーレイIPアドレス範囲

10

20

30

40

50

は 10.0 / 16 であり、サブネット 2 のアドレス範囲は 10.1 / 16 である。VCN 仮想ルータ 605 は、VCN 604 のサブネット間の、および、VCN の外側の他のエンドポイントとの通信を可能にする、VCN の論理ゲートウェイを表す。VCN VR 605 は、VCN 604 内の VNIC と、VCN 604 に関連付けられるゲートウェイとの間でトラフィックをルーティングするように構成されている。VCN VR 605 は、VCN 604 の各サブネットのポートを提供する。例えば、VR 605 は、サブネット 1 の IP アドレス 10.0.0.1 を有するポート、および、サブネット 2 の IP アドレス 10.1.0.1 を有するポートを提供することができる。

【0105】

複数の計算インスタンスが、各サブネット上に展開されてもよく、ここで、計算インスタンスは、仮想マシンインスタンスおよび／またはベアメタルインスタンスとすることができる。サブネット内の計算インスタンスは、CSP 601 内の 1 つまたは複数のホストマシンによってホストすることができる。計算インスタンスは、計算インスタンスに関連付けられる VNIC を介してサブネットに参加する。例えば、図 6 に示すように、計算インスタンス C1 は、計算インスタンスに関連付けられる VNIC を介する、サブネット 1 の一部である。同様に、計算インスタンス C2 は、C2 に関連付けられる VNIC を介する、サブネット 1 の一部である。同様に、仮想マシンインスタンスまたはベアメタルインスタンスであり得る複数の計算インスタンスが、サブネット 1 の一部であり得る。その関連付けられる VNIC を介して、各計算インスタンスは、プライベートオーバーレイ IP アドレスおよび MAC アドレスを割り当てられる。例えば、図 6 において、計算インスタンス C1 は、10.0.0.2 のオーバーレイ IP アドレスおよび M1 の MAC アドレスを有し、一方、計算インスタンス C2 は、10.0.0.3 のプライベートオーバーレイ IP アドレスおよび M2 の MAC アドレスを有する。計算インスタンス C1 および C2 を含む、サブネット 1 内の各計算インスタンスは、サブネット 1 の VCN VR 605 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 VR 605 までのデフォルトの経路を有する。

【0106】

サブネット 2 は、仮想マシンインスタンスおよび／またはベアメタルインスタンスを含む、複数の計算インスタンスをその上に展開され得る。例えば、図 6 に示すように、計算インスタンス D1 および D2 は、それぞれの計算インスタンスに関連付けられる VNIC を介する、サブネット 2 の一部である。図 6 に示す実施形態において、計算インスタンス D1 は、10.1.0.2 のオーバーレイ IP アドレスおよび MM1 の MAC アドレスを有し、一方、計算インスタンス D2 は、10.1.0.3 のプライベートオーバーレイ IP アドレスおよび MM2 の MAC アドレスを有する。計算インスタンス D1 および D2 を含む、サブネット 2 内の各計算インスタンスは、サブネット 2 の VCN VR 605 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 VR 605 までのデフォルトの経路を有する。

【0107】

VCN A 604 はまた、1 つまたは複数のロードバランサを含むことができる。例えば、ロードバランサは、サブネットのために提供されてもよく、サブネット上の複数の計算インスタンスにわたってトラフィックを負荷平衡させるように構成され得る。ロードバランサはまた、VCN 内のサブネットにわたってトラフィックを負荷平衡させるために提供され得る。

【0108】

VCN 604 上に展開される特定の計算インスタンスは、様々な異なるエンドポイントと通信することができる。これらのエンドポイントは、CSP 700 によってホストされるエンドポイントおよび CSP 700 の外側のエンドポイントを含み得る。CSP 601 によってホストされるエンドポイントは、特定の計算インスタンスと同じサブネット上のエンドポイント（例えば、サブネット 1 内の 2 つの計算インスタンス間の通信）、異なるサブネット上の、ただし同じ VCN 内のエンドポイント（例えば、サブネット 1 内

の計算インスタンスとサブネット 2 内の計算インスタンスとの間の通信)、同じリージョン内の異なる 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 6 0 6 または 6 1 0 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 6 1 0 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 6 0 8 内の V C N 内のエンドポイントとの間の通信) を含み得る。C S P I 6 0 1 によってホストされるサブネット内の計算インスタンスはまた、C S P I 6 0 1 によってホストされない (すなわち、C S P I 6 0 1 の外側にある) エンドポイントとも通信し得る。これらの外側エンドポイントは、顧客のオンプレミスネットワーク 6 1 6 内のエンドポイント、他のリモートクラウドホストネットワーク 6 1 8 内のエンドポイント、インターネットなどの公衆ネットワークを介してアクセス可能な公衆エンドポイント 6 1 4、および他のエンドポイントを含む。

10

【0109】

同じサブネット上の計算インスタンス間の通信は、ソース計算インスタンスおよび宛先計算インスタンスに関連付けられる V N I C を使用して促進される。例えば、サブネット 1 内の計算インスタンス C 1 は、サブネット 1 内の計算インスタンス C 2 にパケットを送ることを所望し得る。ソース計算インスタンスに由来し、その宛先が同じサブネット内の別の計算インスタンスであるパケットについて、パケットは、最初に、ソース計算インスタンスに関連付けられる V N I C によって処理される。ソース計算インスタンスに関連付けられる V N I C によって実施される処理は、パケットヘッダからパケットの宛先情報を決定すること、ソース計算インスタンスに関連付けられる V N I C 向けに構成されている任意のポリシー (例えば、セキュリティリスト) を識別すること、パケットの次のホップを決定すること、必要に応じて任意のカプセル化／カプセル化解除機能を実施すること、および、次いで、パケットのその意図される宛先への通信を促進することを目標としてパケットを次のホップに転送／ルーティングすることを含むことができる。宛先計算インスタンスがソース計算インスタンスと同じサブネット内にあるとき、ソース計算インスタンスに関連付けられる V N I C は、宛先計算インスタンスに関連付けられる V N I C を識別し、パケットを処理のためにその V N I C に転送するように構成されている。このとき、宛先計算インスタンスに関連付けられる V N I C が実行され、パケットを宛先計算インスタンスに転送する。

20

30

【0110】

パケットが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通信されるようにするために、ソースおよび宛先計算インスタンスに関連付けられる V N I C および V C N V R によって通信が促進される。例えば、図 6 のサブネット 1 内の計算インスタンス C 1 が、サブネット 2 内の計算インスタンス D 1 にパケットを送ることを所望する場合、パケットは、最初に、計算インスタンス C 1 に関連付けられる V N I C によって処理される。計算インスタンス C 1 に関連付けられる V N I C は、V C N V R のデフォルトの経路またはポート 1 0 . 0 . 0 . 1 を使用して、パケットを V C N V R 6 0 5 にルーティングするように構成されている。V C N V R 6 0 5 は、ポート 1 0 . 1 . 0 . 1 を使用してパケットをサブネット 2 にルーティングするように構成されている。次いで、パケットは、D 1 に関連付けられる V N I C によって受信および処理され、V N I C は、パケットを計算インスタンス D 1 に転送する。

40

【0111】

パケットが V C N 6 0 4 内の計算インスタンスから V C N 6 0 4 の外側にあるエンドポイントに通信されるようにするために、ソース計算インスタンスに関連付けられる V N I C、V C N V R 6 0 5、および V C N 6 0 4 に関連付けられるゲートウェイによって通信が促進される。1 つまたは複数のタイプのゲートウェイが、V C N 6 0 4 に関連付けられ得る。ゲートウェイは、V C N と別のエンドポイントとの間のインターフェイスであり、ここで、別のエンドポイントは、V C N の外部にある。ゲートウェイは、レイヤ 3 / I

50

プレイヤ概念であり、VCNがVCNの外側のエンドポイントと通信することを可能にする。したがって、ゲートウェイは、VCNと他のVCNまたはネットワークとの間のトラフィックフローを促進する。様々な異なるタイプのゲートウェイが、異なるタイプのエンドポイントとの異なるタイプの通信を促進するために、VCN向けに構成され得る。ゲートウェイに応じて、通信は、公衆ネットワーク（例えば、インターネット）またはプライベートネットワークを介するものであり得る。様々な通信プロトコルがこれらの通信に使用され得る。

【0112】

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

【0113】

様々な異なるタイプのゲートウェイが、VCN向けに構成され得る。VCN向けに構成することができるゲートウェイの例が、図6に示されており、下記に説明される。VCNに関連付けられるゲートウェイの例はまた、図11、図12、図13、および図14にも示されており（例えば、参照符号1134、1136、1138、1234、1236、1238、1334、1336、1338、1434、1436、および1438によって参照されるゲートウェイ）、下記に説明される。図6に示す実施形態に示すように、動的ルーティングゲートウェイ（DRG）622は、顧客VCN604に追加することができるか、または、それに関連付けることができ、顧客VCN604と別のエンドポイントとの間のプライベートネットワークトラフィック通信のための経路を提供し、ここで、別のエンドポイントは、顧客のオンプレミスネットワーク616、CSP601の異なるリージョン内のVCN608、または、CSP601によってホストされない他のリモートクラウドネットワーク618とすることができる。顧客オンプレミスネットワーク616は、顧客のリソースを使用して構築されている顧客ネットワークまたは顧客データセンターであり得る。顧客オンプレミスネットワーク616へのアクセスは、一般的に、非常に制限されている。顧客オンプレミスネットワーク616とCSP601によってクラウド内で展開またはホストされている1つまたは複数のVCN604の両方を有する顧客について、顧客は、そのオンプレミスネットワーク616およびそのクラウドベースのVCN604が、互いに通信することが可能であることを所望し得る。これによって、顧客が、CSP601によってホストされる顧客のVCN604およびそのオンプレミスネットワーク616を包含する拡張ハイブリッド環境を構築することが可能になる。DRG622が、この通信を可能にする。そのような通信を可能にするために、通信チャネル624がセットアップされ、ここで、チャネルの1つのエンドポイントは顧客オンプレミスネットワーク616であり、他方のエンドポイントはCSP601であり、顧客VCN604に接続されている。通信チャネル624は、インターネットなどの公衆通信ネットワークまたはプライベート通信ネットワークを介するものとしてすることができる。インターネットなどの公衆通信ネットワークを介したIPsec VPN技術、公衆ネットワークの代わりにプライベートネットワークを使用するOracleのFastConnect技術などの、様々な異なる通信プロトコルが使用され得る。通信チャネル624の1つのエンドポイン

トを形成する顧客オンプレミスネットワーク 616 内のデバイスまたは設備は、図 6 に示す CPE 626 などの、顧客構内設備 (CPE) として参照される。CSP 601 側では、エンドポイントは、DRG 622 を実行するホストマシンであり得る。

【0114】

ある実施形態において、リモートピアリング接続 (RPC) を DRG に追加することができ、これによって、顧客が、1つのVCNを異なるリージョン内の別のVCNとピアリングすることが可能になる。そのようなRPCを使用して、顧客VCN 604は、DRG 622を使用して別のリージョン内のVCN 608と接続することができる。DRG 622はまた、Microsoft Azureクラウド、Amazon AWSクラウドなどのような、CSP 601によってホストされていない、他のリモートクラウドネットワーク 618と通信するために使用することもできる。

10

【0115】

図 6 に示すように、インターネットゲートウェイ (IGW) 620は、VCN 604上の計算インスタンスがインターネットなどの公衆ネットワークを介してアクセス可能な公衆エンドポイント 614と通信することを可能にするように、顧客VCN 604向けに構成することができる。IGW 620は、インターネットなどの公衆ネットワークにVCNを接続するゲートウェイである。IGW 620は、VCN 604などのVCN内の公衆サブネット (ここで、公衆サブネット内のリソースは公衆オーバーレイIPアドレスを有する) が、インターネットなどの公衆ネットワーク 614上の公衆エンドポイント 612に直接的にアクセスすることを可能にする。IGW 620を使用して、VCN 604内のサブネットまたはインターネットからの接続を開始することができる。

20

【0116】

ネットワークアドレス変換 (NAT) ゲートウェイ 628は、顧客のVCN 604向けに構成することができ、専用公衆オーバーレイIPアドレスを有しない顧客のVCN内のクラウドリソースが、インターネットにアクセスすることを可能にし、それらのリソースを直接入来インターネット接続 (例えば、L4~L7接続) に暴露することなく、これを行う。これによって、VCN 604内のプライベートサブネット 1などの、VCN内のプライベートサブネットが、インターネット上の公衆エンドポイントへのプライベートアクセスを有することが可能になる。NATゲートウェイにおいて、接続は、インターネットからプライベートサブネットへとではなく、プライベートサブネットから公衆インターネットへとのみ開始することができる。

30

【0117】

ある実施形態において、サービスゲートウェイ (SGW) 626は、顧客VCN 604向けに構成することができ、VCN 604とサービスネットワーク 610内のサポートされているサービスエンドポイントとの間のプライベートネットワークトラフィックのための経路を提供する。ある実施形態において、サービスネットワーク 610は、CSPによって提供することができ、様々なサービスを提供することができる。そのようなサービスネットワークの一例は、顧客によって使用することができる様々なサービスを提供するOracleのサービスネットワークである。例えば、顧客VCN 604のプライベートサブネット内の計算インスタンス (例えば、データベースシステム) は、公衆IPアドレスまたはインターネットへのアクセスを必要とすることなく、データをサービスエンドポイント (例えば、オブジェクトストレージ) にバックアップすることができる。ある実施形態において、VCNは、1つのみのSGWを有することができ、接続は、サービスネットワーク 610からではなく、VCN内のサブネットからのみ開始することができる。VCNが別のVCNとピアリングされる場合、他のVCN内のリソースは、SGWにアクセスすることができない。FastConnectまたはVPN ConnectによってVCNに接続されるオンプレミスネットワーク内のリソースもまた、そのVCN向けに構成されているサービスゲートウェイを使用することができる。

40

【0118】

ある実施形態において、SGW 626は、関心のあるサービスまたはサービスグループ

50

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

【0119】

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

【0120】

サービスネットワーク610内のサービスのプロバイダなどのサービスプロバイダは、異なるアクセスモデルを使用してサービスへのアクセスを提供することができる。公衆アクセスモデルによれば、サービスは、インターネットなどの公衆ネットワークを介して顧客VCN内の計算インスタンスによってパブリックにアクセス可能である公衆エンドポイントとして暴露されてもよく、または、SGW626を介してプライベートにアクセス可能であり得る。特定のプライベートアクセスモデルによれば、サービスは、顧客のVCN内のプライベートサブネット内のプライベートIPエンドポイントとしてアクセス可能にされる。これは、プライベートエンドポイント（PE）アクセスとして参照され、サービスプロバイダが、顧客のプライベートネットワーク内のインスタンスとしてそれらのサービスを暴露することを可能にする。プライベートエンドポイントリソースは、顧客のVCN内のサービスを表す。各PEは、顧客のVCN内の顧客によって選択されるサブネット内のVNIC（1つまたは複数のプライベートIPを有するPE-VNICとして参照される）として現れる。したがって、PEは、VNICを使用してプライベート顧客VCNサブネット内にサービスを提示するための方法を提供する。エンドポイントはVNICとして暴露されるため、ルーティング規則、セキュリティリストなどのようなVNICに関連付けられるすべての特徴が、この時点でPE VNICにとって利用可能にされる。

【0121】

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

【0122】

このとき、プライベートサブネット内の計算インスタンスは、PE VNICのプライベートIPアドレスまたはサービスDNS名を使用して、サービスにアクセスすることができる。顧客VCN内の計算インスタンスは、顧客VCN内のPEのプライベートIPアドレスにトラフィックを送ることによって、サービスにアクセスすることができる。プライベートアクセスゲートウェイ（PAGW）630は、顧客サブネットプライベートエンドポイントからの／へのすべてのトラフィックの侵入／退出ポイントとして作用するサービスプロバイダVCN（例えば、サービスネットワーク610内のVCN）にアタッチすることができるゲートウェイリソースである。PAGW630は、プロバイダが、その内部IPアドレスリソースを利用することなくPE接続の数をスケーリングすることを可能

にする。プロバイダは、単一のV C N内に登録されている任意の数のサービスに対して、1つのP A G Wを構成することのみを必要とする。プロバイダは、サービスを、1または複数の顧客の複数のV C N内のプライベートエンドポイントとして表すことができる。顧客の観点から、P E V N I Cは、顧客のインスタンスにアタッチされる代わりに、顧客が相互に作用することを所望するサービスにアタッチされるように見える。プライベートエンドポイントに宛てられたトラフィックは、P A G W 6 3 0を介してサービスへとルーティングされる。これらは、顧客-サービスプライベート接続（C 2 S接続）として参照される。

【0123】

P E概念はまた、トラフィックがFastConnect/IPsecリンクおよび顧客V C N内のプライベートエンドポイントを通じて流れることを可能にすることによって、サービスのためのプライベートアクセスを顧客のオンプレミスネットワークおよびデータセンタへと拡張するために使用することもできる。サービスのためのプライベートアクセスはまた、トラフィックがL P G 6 3 2と顧客のV C N内のP Eとの間を流れることを可能にすることによって、顧客のピアリングされたV C Nへと拡張することもできる。

【0124】

顧客は、V C Nにおけるルーティングをサブネットレベルで制御することができ、したがって、顧客は、V C N 6 0 4などの顧客のV C Nのいずれのサブネットが各ゲートウェイを使用するかを指定することができる。トラフィックが特定のゲートウェイを通じてV C Nを出ることを可能にされるか否かを判断するために、V C Nの経路テーブルが使用される。例えば、特定の事例において、顧客V C N 6 0 4内の公衆サブネットの経路テーブルは、I G W 6 2 0を通じて非ローカルトラフィックを送ることができる。同じ顧客V C N 6 0 4内のプライベートサブネットの経路テーブルが、S G W 6 2 6を通じてC S Pサービスに宛てられたトラフィックを送ることができる。すべての残りのトラフィックは、N A Tゲートウェイ6 2 8を介して送ることができる。経路テーブルは、V C Nから出るトラフィックのみを制御する。

【0125】

着信接続を介して、ゲートウェイを介してV C Nに入来するトラフィックを制御するために、V C Nに関連付けられるセキュリティリストが使用される。サブネット内のすべてのリソースが、同じ経路テーブルおよびセキュリティリストを使用する。セキュリティリストは、V C Nのサブネット内のインスタンスに入ることおよび出ることを可能にされる特定のタイプのトラフィックを制御するために使用することができる。セキュリティリスト規則は、進入（着信）および退出（発信）規則を含むことができる。例えば、進入規則は、許容されるソースアドレス範囲を指定することができ、一方、退出規則は、許容される宛先アドレス範囲を指定することができる。セキュリティ規則は、特定のプロトコル（例えば、T C P、I C M P）、特定のポート（例えば、S S Hのための2 2、Windows（登録商標）R D Pのための3 3 8 9）などを指定することができる。ある実施態様において、インスタンスのオペレーティングシステムは、セキュリティリスト規則と整合されているそれ自体のファイアウォール規則を執行することができる。規則は、ステートフル（例えば、接続が追跡され、応答が、応答トラフィックに対する明示的なセキュリティリスト規則なしに、自動的に許可される）であってもよく、または、ステートレスであり得る。

【0126】

顧客V C Nからの（すなわち、V C N 6 0 4上に展開されているリソースまたは計算インスタンスによる）アクセスは、公衆アクセス、プライベートアクセス、または専用アクセスとしてカテゴライズすることができる。公衆アクセスは、公衆I PアドレスまたはN A Tが公衆エンドポイントにアクセスするために使用されるアクセスモデルを指す。プライベートアクセスは、プライベートI Pアドレスを有するV C N 6 0 4内の顧客ワークロード（例えば、プライベートサブネット内のリソース）が、インターネットなどの公衆ネットワークをトラバースすることなく、サービスにアクセスすることを可能にする。ある

実施形態において、C S P I 6 0 1 は、プライベートIPアドレスを有する顧客V C Nワークロードが、サービスゲートウェイを使用してサービス（の公衆サービスエンドポイント）にアクセスすることを可能にする。したがって、サービスゲートウェイは、顧客の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エンドポイントとの間の仮想リンクを確立することによって、プライベートアクセスモデルを供給する。

【0127】

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

【0128】

図6および上記の付随する説明は、例示的な仮想ネットワークにおける様々な仮想化構成要素を記載している。上述したように、仮想ネットワークは、下層の物理または基盤ネットワーク上に構築される。図7は、ある実施形態による、仮想ネットワークの下層を提供するC S P I 7 0 0内の物理ネットワーク内の物理構成要素の単純化されたアーキテクチャ図を示す。図示のように、C S P I 7 0 0は、クラウドサービスプロバイダ（C S P）によって提供される構成要素およびリソース（例えば、計算、メモリ、およびネットワーキングリソース）を含む分散環境を提供する。これらの構成要素およびリソースは、加入顧客、すなわち、C S Pによって提供される1つまたは複数のサービスに加入している顧客にクラウドサービス（例えば、I a a Sサービス）を提供するために使用される。顧客が加入しているサービスに基づいて、C S P I 7 0 0のリソース（例えば、計算、メモリ、およびネットワーキングリソース）のサブセットが顧客にプロビジョンされる。その後、顧客は、C S P I 7 0 0によって提供される物理計算、メモリ、およびネットワーキングリソースを使用して、自身のクラウドベースの（すなわち、C S P Iによってホストされる）カスタマイズ可能なプライベート仮想ネットワークを構築することができる。前に示したように、これらの顧客ネットワークは、仮想クラウドネットワーク（V C N）として参照される。顧客は、これらの顧客V C N上で、計算インスタンスなどの1つまたは複数の顧客リソースを展開することができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどの形態とすることができる。C S P I 7 0 0は、顧客が多様なアプリケーションおよびサービスを可用性の高いホスト環境内で構築し、実行することを可能にするインフラストラクチャ、および、補完クラウドサービスのセットを提供する。

【0129】

図7に示す例示的な実施形態において、C S P I 7 0 0の物理構成要素は、1つまたは複数の物理ホストマシンまたは物理サーバ（例えば、702、706、708）、ネットワーク仮想化デバイス（N V D）（例えば、710、712）、トップオブラック（T O R）スイッチ（例えば、714、716）、および物理ネットワーク（例えば、718）、ならびに物理ネットワーク718内のスイッチを含む。物理ホストマシンまたはサーバは、V C Nの1つまたは複数のサブネットに参加する様々な計算インスタンスをホストし、実行することができる。計算インスタンスは、仮想マシンインスタンスまたはベアメタルインスタンスを含み得る。例えば、図6に示す様々な計算インスタンスが、図7に示す物理ホストマシンによってホストされ得る。V C N内の仮想マシン計算インスタンスは、1つホストマシンによって実行されてもよく、または、複数の異なるホストマシンによっ

て実行され得る。物理ホストマシンはまた、仮想ホストマシン、コンテナベースのホストまたは機能などをホストすることもできる。図 6 に示す V N I C および V C N V R が、図 7 に示す N V D によって実行され得る。図 6 に示すゲートウェイが、図 7 に示すホストマシンおよび／または N V D によって実行され得る。

【0130】

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

10

【0131】

例えば、図 7 に示すように、ホストマシン 702 および 708 は、それぞれハイパーバイザ 760 および 766 を実行する。これらのハイパーバイザは、ソフトウェア、ファームウェア、もしくはハードウェア、またはそれらの組み合わせを使用して実装され得る。典型的には、ハイパーバイザは、ホストマシンのハードウェアプロセッサ上で作動する、ホストマシンのオペレーティングシステム（O S）の上にあるプロセスまたはソフトウェア層である。ハイパーバイザは、ホストマシンの物理コンピューティングリソース（例えば、プロセッサ／コア、メモリリソース、ネットワークリソースなどの処理リソース）が、ホストマシンによって実行される様々な仮想マシン計算インスタンス間で共有されることを可能にすることによって、仮想化環境を提供する。例えば、図 7 において、ハイパーバイザ 760 は、ホストマシン 702 の O S の上にあることができ、ホストマシン 702 のコンピューティングリソース（例えば、処理、メモリ、およびネットワークリソース）がホストマシン 702 によって実行される計算インスタンス（例えば、仮想マシン）間で共有されることを可能にする。仮想マシンは、ホストマシンの O S と同じであってもよく、または、異なり得る、それ自体のオペレーティングシステム（ゲストオペレーティングシステムとして参照される）を有することができる。ホストマシンによって実行される仮想マシンのオペレーティングシステムは、同じホストマシンによって実行される別の仮想マシンのオペレーティングシステムと同じであってもよく、または異なり得る。したがって、ハイパーバイザは、複数のオペレーティングシステムが、ホストマシンの同じコンピューティングリソースを共有しながら、互いに並行して実行されることを可能にする。図 7 に示すホストマシンは、同じまたは異なるタイプのハイパーバイザを有し得る。

20

30

【0132】

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

40

【0133】

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

50

ルインスタンスをホストするホストマシンの物理CPU、メモリ、およびネットワークインターフェイスの制御を維持し、ホストマシンは、他の顧客またはテナントと共有されない。

【0134】

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

10

【0135】

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

20

【0136】

ホストマシンは、ホストマシンが他のデバイスに接続されることを可能にする1つまたは複数のネットワークインターフェイスカード(NIC)を含むことができる。ホストマシン上のNICは、ホストマシンが別のデバイスに通信可能に接続されることを可能にする1つまたは複数のポートを提供することができる。例えば、ホストマシンは、ホストマシンおよびNVD上に設けられた1つまたは複数のポート(またはインターフェイス)を使用してNVDに接続され得る。ホストマシンはまた、別のホストマシンなどの他のデバイスにも接続され得る。

30

【0137】

例えば、図7において、ホストマシン702は、ホストマシン702のNIC732によって提供されるポート734の間およびNVD710のポート736の間に延在するリンク720を使用して、NVD710に接続されている。ホストマシン706は、ホストマシン706のNIC744によって提供されるポート746の間およびNVD712のポート748の間に延在するリンク724を使用して、NVD712に接続されている。ホストマシン708は、ホストマシン708のNIC750によって提供されるポート752の間およびNVD712のポート754の間に延在するリンク726を使用して、NVD712に接続されている。

40

【0138】

次いで、NVDは、通信リンクを介してトップオブブラック(TOR)スイッチに接続されており、TORスイッチは、物理ネットワーク718(スイッチファブリックとしても参照される)に接続されている。ある実施形態において、ホストマシンとNVDとの間、および、NVDとTORスイッチとの間のリンクは、イーサネット(登録商標)リンクである。例えば、図7において、NVD710および712は、それぞれリンク728および730を使用して、1126個のTORスイッチ714および716に接続されている

50

。ある実施形態において、リンク 720、724、726、728、および 730 は、イーサネット（登録商標）リンクである。TOR に接続されているホストマシンおよび NV D の集合は、ラックとして参照されることがある。

【0139】

物理ネットワーク 718 は、TOR スイッチが互いに通信することを可能にする通信ファブリックを提供する。物理ネットワーク 718 は、多階層構成ネットワークとすることができる。ある実施態様において、物理ネットワーク 718 は、スイッチの多階層構成 Clos ネットワークであり、TOR スイッチ 714 および 716 は、多階層構成マルチノード物理スイッチングネットワーク 718 のリーフレベルノードを表す。限定ではないが、2 階層ネットワーク、3 階層ネットワーク、4 階層ネットワーク、5 階層ネットワーク、および一般的に「n」階層構成ネットワークを含む、異なる Clos ネットワーク構成が可能である。Clos ネットワークの一例が、図 10 に示されており、下記に説明される。

10

【0140】

1 対 1 構成、多対 1 構成、1 対多構成などのような、ホストマシンと NV D との間の様々な異なる接続構成が可能である。1 対 1 構成実施態様においては、各ホストマシンが、それ自体の別個の NV D に接続される。例えば、図 7 において、ホストマシン 702 は、ホストマシン 702 の NIC 732 を介して NV D 710 に接続される。多対 1 構成においては、複数のホストマシンが 1 つの NV D に接続される。例えば、図 7 において、ホストマシン 706 および 708 は、それぞれ NIC 744 および 750 を介して、同じ NV D 712 に接続される。

20

【0141】

1 対多構成においては、1 つのホストマシンが複数の NV D に接続される。図 8 は、ホストマシンが複数の NV D に接続されている C S P I 800 内の例を示す。図 8 に示すように、ホストマシン 802 は、複数のポート 806 および 808 を含むネットワークインターフェイスカード（NIC）804 を備える。ホストマシン 800 は、ポート 806 およびリンク 820 を介して第 1 の NV D 810 に接続されており、ポート 808 およびリンク 822 を介して第 2 の NV D 812 に接続されている。ポート 806 および 808 は、イーサネット（登録商標）ポートであってもよく、ホストマシン 802 と NV D 810 および 812 との間のリンク 820 および 822 は、イーサネット（登録商標）リンクであり得る。次いで、NV D 810 は、第 1 の TOR スイッチ 814 に接続されており、NV D 812 は、第 2 の TOR スイッチ 816 に接続されている。NV D 810 および 812 と TOR スイッチ 814 および 816 との間のリンクは、イーサネット（登録商標）リンクであり得る。TOR スイッチ 814 および 816 は、多階層構成物理ネットワーク 818 内の階層 0 スwitchングデバイスを表す。

30

【0142】

図 8 に示す配置構成は、物理スイッチネットワーク 818 からホストマシン 802 への、および、ホストマシン 802 から物理スイッチネットワーク 818 への 2 つの別個の物理ネットワーク経路、すなわち、TOR スイッチ 814 - NV D 810 - ホストマシン 802 とトラバースする第 1 の経路、および、TOR スイッチ 816 - NV D 812 - ホストマシン 802 とトラバースする第 2 の経路を提供する。これら別個の経路は、ホストマシン 802 の向上した可用性（高可用性として参照される）を提供する。経路（例えば、経路の 1 つのリンクが故障した）またはデバイス（例えば、特定の NV D が機能していない）の 1 つに問題がある場合、他の経路が、ホストマシン 802 への／からの通信に使用され得る。

40

【0143】

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

50

【0144】

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

【0145】

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

【0146】

しかしながら、smartNICは、NVD実施態様の一例に過ぎない。様々な他の実施態様が可能である。例えば、いくつかの他の実施態様において、NVDまたはNVDによって実施される1つまたは複数の機能は、1つもしくは複数のホストマシン、1つもしくは複数のTORスイッチ、およびCSP1700の他の構成要素に組み込まれてもよく、またはそれによって実施され得る。例えば、NVDは、ホストマシン内に具現化されてもよく、ここで、NVDによって実施される機能は、ホストマシンによって実施される。別の例として、NVDは、TORスイッチの一部であってもよく、または、TORスイッチが、TORスイッチが公衆クラウドに使用される様々な複雑なパケット変換を実施することを可能にするNVDによって実施される機能を実施するように構成され得る。NVDの機能を実施するTORは、スマートTORとして参照されることがある。ベアメタル（BM）インスタンスではなく仮想マシン（VM）インスタンスが顧客に供給されるさらに他の実施態様においては、NVDによって実施される機能は、ホストマシンのハイパーバイザの内側で実装され得る。いくつかの他の実施態様において、NVDの機能の一部は、ホストマシンのフリート上で作動する集中型サービスにオフロードされ得る。

【0147】

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

【0148】

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

ームを受信することができ、必要なパケット処理を実施した後、パケットおよびフレームを、NVDのホスト側ポートを介してホストマシンに転送することができる。

【0149】

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

10

【0150】

NVDは、ネットワーク仮想化機能を実装または実施する。これらの機能は、NVDによって実行されるソフトウェア／ファームウェアによって実施される。ネットワーク仮想化機能の例は、限定ではないが、パケットカプセル化およびカプセル化解除機能、VCNネットワークを作成するための機能、VCNセキュリティリスト（ファイアウォール）機能などのネットワークポリシーを実装するための機能、VCN内の計算インスタンスへの、および、そこからのパケットのルーティングおよび転送を促進する機能などを含む。ある実施形態において、パケットが受信されると、NVDは、パケットを処理し、パケットがどのように転送またはルーティングされるかを決定するためのパケット処理パイプラインを実行するように構成されている。このパケット処理パイプラインの一部として、NVDは、VCN内の計算インスタンスに関連付けられるVNICを実行すること、VCNに関連付けられる仮想ルータ（VR）を実行すること、仮想ネットワーク内での転送またはルーティングを促進するためのパケットのカプセル化およびカプセル化解除、あるゲートウェイ（例えば、ローカルピアリングゲートウェイ）の実行、セキュリティリスト、ネットワークセキュリティグループ、ネットワークアドレス変換（NAT）機能（例えば、ホストごとの公衆IPのプライベートIPへの変換）の実装、スロットル機能、および他の機能などの、オーバーレイネットワークに関連付けられる1つまたは複数の仮想機能を実行することができる。

20

30

【0151】

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

40

【0152】

NVDは、VCNの制御プレーンおよびデータプレーンに対応する制御プレーン機能とデータプレーン機能の両方を実施することができる。VCN制御プレーンの例は、図11、図12、図13、および図14にも示されており（参照符号1116、1216、13

50

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

10

20

30

40

50

【0153】

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

【0154】

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

【0155】

VNICおよびVCN VRに加えて、NVDは、様々なソフトウェア(例えば、デーモン)を実行し、NVDによって実施される様々なネットワーク仮想化機能を促進する1つまたは複数のハードウェア構成要素を含むことができる。単純化を目的として、これらの様々な構成要素は、図7に示す「パケット処理構成要素」としてともにグループ化される。例えば、NVD710は、パケット処理構成要素786を備え、NVD712は、パケット処理構成要素788を備える。例えば、NVDのパケット処理構成要素は、NVDのポートおよびハードウェアインターフェイスと相互に作用して、NVDによって受信され、NVDを使用して受信され通信されるすべてのパケットを監視し、ネットワーク情報を記憶するように構成されているパケットプロセッサを含み得る。ネットワーク情報は、

例えば、NVDによってフロー情報ごとに（例えば、フロー統計ごとに）ハンドリングされる異なるネットワークフローを識別するネットワークフロー情報を含み得る。ある実施形態において、ネットワークフロー情報は、VNICごとに記憶され得る。パケットプロセッサは、パケットごとの操作を実施するとともに、ステートフルNATおよびL4ファイアウォール（FW）を実装し得る。別の例として、パケット処理構成要素は、NVDによって記憶されている情報を、1つまたは複数の異なる複製目標ストアに複製するように構成されている複製エージェントを含み得る。さらに別の例として、パケット処理構成要素は、NVDのログ記録機能を実施するように構成されているログ記録エージェントを含み得る。パケット処理構成要素はまた、NVDの性能および健全性を監視し、また、場合によっては、NVDに接続されている他の構成要素の状態および健全性も監視するためのソフトウェアも含み得る。

10

【0156】

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

20

【0157】

上述したように、顧客VCN内の計算インスタンスは、様々な異なるエンドポイントと通信することができ、ここで、エンドポイントは、ソース計算インスタンスと同じサブネット内にあることができ、ソース計算インスタンスと異なるサブネット内であるが、同じVCN内にあることができ、または、エンドポイントは、ソース計算インスタンスのVCNの外側にあることができる。これらの通信は、計算インスタンスに関連付けられるVNIC、VCN VR、およびVCNに関連付けられるゲートウェイを使用して促進される。

30

【0158】

VCN内の同じサブネット上の2つの計算インスタンス間の通信について、通信は、ソースおよび宛先計算インスタンスに関連付けられるVNICを使用して促進される。ソースおよび宛先計算インスタンスは、同じホストマシンによってホストされてもよく、または、異なるホストマシンによってホストされ得る。ソース計算インスタンスに由来するパケットは、ソース計算インスタンスをホストするホストマシンから、そのホストマシンに接続されているNVDへと転送することができる。NVD上で、パケットは、ソース計算インスタンスに関連付けられるVNICの実行を含むことができる、パケット処理パイプラインを使用して処理される。パケットの宛先エンドポイントは同じサブネット内にあるため、ソース計算インスタンスに関連付けられるVNICが実行される結果として、パケットが、宛先計算インスタンスに関連付けられるVNICを実行するNVDに転送され、その後、NVDは、パケットを処理し、宛先計算インスタンスに転送する。ソースおよび宛先計算インスタンスに関連付けられるVNICは、同じNVD上で実行されてもよく（例えば、ソース計算インスタンスと宛先計算インスタンスの両方が同じホストマシンによってホストされるとき）、または、異なるNVD上で実行され得る（例えば、ソースおよび宛先計算インスタンスが異なるNVDに接続されている異なるホストマシンによってホ

40

50

ストされるとき)。VNICは、NVDによって記憶されているルーティング／転送テーブルを使用して、パケットの次のホップを決定することができる。

【0159】

パケットがサブネット内の計算インスタンスから同じVCN内の異なるサブネット内のエンドポイントに通信されるようにするために、ソース計算インスタンスに由来するパケットは、ソース計算インスタンスをホストするホストマシンからそのホストマシンに接続されているNVDに通信される。NVD上で、パケットは、1つまたは複数のVNICの実行を含むことができるパケット処理パイプラインおよびVCNに関連付けられるVRを使用して処理される。例えば、パケット処理パイプラインの一部として、NVDは、ソース計算インスタンスに関連付けられるVNICに対応する機能を実行するかまたは呼び出す（VNICの実行としても参照される）。VNICによって実施される機能は、パケット上のVLANTagを見ることを含むことができる。パケット宛先はサブネットの外側にあるため、VCN VR機能は、NVDによって次に呼び出され、実行される。次いで、VCN VRは、宛先計算インスタンスに関連付けられるVNICを実行するNVDにパケットをルーティングする。次いで、宛先計算インスタンスに関連付けられるVNICは、パケットを処理し、宛先計算インスタンスに転送する。ソースおよび宛先計算インスタンスに関連付けられるVNICは、同じNVD上で実行されてもよく（例えば、ソース計算インスタンスと宛先計算インスタンスの両方が同じホストマシンによってホストされるとき）、または、異なるNVD上で実行され得る（例えば、ソースおよび宛先計算インスタンスが異なるNVDに接続されている異なるホストマシンによってホストされるとき）。

10

20

【0160】

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

30

40

【0161】

VCN上に展開される特定の計算インスタンスは、様々な異なるエンドポイントと通信することができる。これらのエンドポイントは、CSP700によってホストされるエンドポイントおよびCSP700の外側のエンドポイントを含み得る。CSP700によってホストされるエンドポイントは、同じVCNまたは他のVCN内のインスタンスを含んでもよく、VCNは、顧客のVCNであってもよく、または、顧客に属しないVCNであり得る。CSP700によってホストされるエンドポイント間の通信は、物理ネ

50

ットワーク 718 を介して実施され得る。計算インスタンスはまた、C S P I 700 によってホストされないか、または、C S P I 700 の外側にあるエンドポイントとも通信し得る。これらのエンドポイントの例は、顧客オンプレミスネットワークもしくはデータセンタ内のエンドポイント、または、インターネットなどの公衆ネットワークを介してアクセス可能な公衆エンドポイントを含む。C S P I 700 の外側のエンドポイントとの通信は、様々な通信プロトコルを使用して、公衆ネットワーク（例えば、インターネット）（図 7 には示さず）またはプライベートネットワーク（図 7 には示さず）を介して実施され得る。

【0162】

図 7 に示す C S P I 700 のアーキテクチャは、例示に過ぎず、限定であるようには意図されていない。代替的な実施形態において、変形、代替、および修正が可能である。例えば、いくつかの他の実施形態において、C S P I 700 は、図 7 に示されているよりも多いもしくは少ないシステムもしくは構成要素を有してもよく、2 つ以上のシステムを組み合わせてもよく、または、システムの異なる構成もしくは配置を有し得る。図 7 に示すシステム、サブシステム、および他の構成要素は、それぞれのシステム、ハードウェアの使用、またはそれらの組み合わせの 1 つまたは複数の処理装置（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）内で実施することができる。ソフトウェアは、非一時的記憶媒体上に（例えば、メモリデバイス上に）記憶することができる。

【0163】

図 9 は、ある実施形態によるマルチテナンシ機能をサポートするために I / O 仮想化を提供するためのホストマシンと N V D との間の接続を示す。図 9 に示すように、ホストマシン 902 は、仮想化環境を提供するハイパーバイザ 904 を実行する。ホストマシン 902 は、2 つの仮想マシンインスタンス、すなわち、顧客／テナント # 1 に属する V M 1 906 および顧客／テナント # 2 に属する V M 2 908 を実行する。ホストマシン 902 は、リンク 914 を介して N V D 912 に接続されている物理 N I C 910 を備える。計算インスタンスの各々は、N V D 912 によって実行される V N I C にアタッチされる。図 9 の実施形態において、V M 1 906 は、V N I C - V M 1 920 にアタッチされ、V M 2 908 は、V N I C - V M 2 922 にアタッチされる。

【0164】

図 9 に示すように、N I C 910 は、2 つの論理 N I C、すなわち、論理 N I C A 916 および論理 N I C B 918 を含む。各仮想マシンは、それ自体の論理 N I C にアタッチされ、それと協働するように構成されている。例えば、V M 1 906 は、論理 N I C A 916 にアタッチされ、V M 2 908 は、論理 N I C B 918 にアタッチされる。ホストマシン 902 は複数のテナントによって共有される 1 つのみの物理 N I C 910 を備えるが、論理 N I C に起因して、各テナントの仮想マシンは、それらがそれら自体のホストマシンおよび N I C を有すると考える。

【0165】

ある実施形態において、各論理 N I C は、それ自体の V L A N I D を割り当てられる。したがって、特定の V L A N I D がテナント # 1 の論理 N I C A 916 に割り当てられ、別個の V L A N I D が、テナント # 2 の論理 N I C B 918 に割り当てられる。V M 1 906 からパケットが通信されるとき、テナント # 1 に割り当てられているタグが、ハイパーバイザによってパケットに割り当てられ、次いで、パケットは、ホストマシン 902 からリンク 914 を介して N V D 912 に通信される。同様に、V M 2 908 からパケットが通信されるとき、テナント # 2 に割り当てられているタグが、ハイパーバイザによってパケットに割り当てられ、次いで、パケットは、ホストマシン 902 からリンク 914 を介して N V D 912 に通信される。したがって、ホストマシン 902 から N V D 912 に通信されるパケット 924 は、特定のテナントおよび関連付けられる V M を識別する、関連付けられるタグ 926 を有する。N V D 上で、ホストマシン 902 から受信されるパケット 924 について、パケットに関連付けられるタグ 926 は、パケット

が V N I C - V M 1 9 2 0 によって処理されるべきであるか、または、V N I C - V M 2 9 2 2 によって処理されるべきであるかを判定するために使用される。次いで、パケットは、対応する V N I C によって処理される。図 9 に示す構成は、各テナントの計算インスタンスが、それらがそれら自体のホストマシンおよび N I C を所有すると考えることを可能にする。図 9 に示すセットアップは、マルチテナンシをサポートするための I / O 仮想化を提供する。

【0166】

図 10 は、ある実施形態による物理ネットワーク 1000 の単純化されたブロック図を示す。図 10 に示す実施形態は、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、高い二分帯域幅および最大のリソース利用を維持しながら接続冗長性を提供するように設計されている特定のタイプのネットワークトポロジである。C l o s ネットワークは、ノンブロッキング、マルチステージまたは多階層構成スイッチングネットワークのタイプであり、ステージまたは階層の数は、2、3、4、5 などとすることができる。図 10 に示す実施形態は、階層 1、2、および 3 を備える 3 階層構成ネットワークである。T O R スイッチ 1004 は、C l o s ネットワーク内の階層 0 スイッチを表す。1 つまたは複数の N V D が、T O R スイッチに接続されている。階層 0 スイッチは、物理ネットワークのエッジデバイスとしても参照される。階層 0 スイッチは、リーフスイッチとしても参照される階層 1 スイッチに接続されている。図 10 に示す実施形態においては、「n」個の階層 0 T O R スイッチから成るセットが「n」個の階層 1 スイッチから成るセットに接続され、ともにポッドを形成する。ポッド内の各階層 0 スイッチは、ポッド内のすべての階層 1 スイッチに相互接続されるが、ポッド間のスイッチの接続はない。ある実施形態様において、2 つのポッドがブロックとして参照される。各ブロックは、「n」個の階層 2 スイッチ（スパインスイッチと呼ばれることがある）から成るセットによってサービスされるか、または、それに接続される。物理ネットワークトポロジ内には、いくつかのブロックが存在し得る。次いで、階層 2 スイッチは、「n」個の階層 3 スイッチ（スーパースパインスイッチと呼ばれることがある）に接続されている。物理ネットワーク 1000 を介したパケットの通信は、典型的には、1 つまたは複数のレイヤ 3 通信プロトコルを使用して実施される。典型的には、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 ウェイ冗長であり、したがって、高可用性を可能にする。物理ネットワークのスケールアップを可能にするように物理ネットワーク内のスイッチの互いに対する可視性を制御するために、ポッドおよびブロックに対してポリシーを指定することができる。

【0167】

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

【0168】

ある実施形態において、C S P I 内の各リソースは、クラウド識別子（C I D）と呼ばれる一意の識別子を割り当てられる。この識別子は、リソースの情報の一部として含まれ、例えば、コンソールを介してまたは A P I を通じてリソースを管理するために使用する

ことができる。C I Dの例示的な構文は、以下のとおりである。

【0169】

ocid1. <RESOURCE TYPE> . <REALM> .[REGION][.FUTURE USE]. <UNIQUE ID>

ここで、

ocid1: C I Dのバージョンを指示する文字列。

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

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

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

future use: 将来の使用のために予約済み。

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

【0170】

図11は、少なくとも1つの実施形態による、I a a Sアーキテクチャの例示的なパターンを示すブロック図1100である。サービスオペレータ1102は、仮想クラウドネットワーク(V C N) 1106およびセキュアホストサブネット1108を含むことができるセキュアホストテナンシ1104に通信可能に結合され得る。いくつかの例において、サービスオペレータ1102は、Microsoft Windows Mobile (登録商標)などのソフトウェア、および／または、i O S、Windows Phone、Android、BlackBerry (登録商標) 8、Palm OSなどのような様々なモバイルオペレーティングシステムを作動させており、インターネット、電子メール、ショートメッセージサービス(S M S)、Blackberry (登録商標)、または他の通信プロトコルを有効化されているポータブル手持ち式デバイス(例えば、iPhone (登録商標)、携帯電話機、iPad (登録商標)、コンピューティングタブレット、個人情報端末(P D A))またはウェアラブルデバイス(例えば、Google (登録商標) Glassヘッドマウントディスプレイ)であり得、1つまたは複数のクライアントコンピューティングデバイスを使用し得る。代替的に、クライアントコンピューティングデバイスは、例として、様々なバージョンのMicrosoft Windows (登録商標)、Apple Macintosh (登録商標)、および／またはLinux (登録商標) オペレーティングシステムを作動させているパーソナルコンピュータおよび／またはラップトップを含む汎用パーソナルコンピュータとすることができる。クライアントコンピューティングデバイスは、限定ではないが、例えば、Google Chrome OSなどの様々なGNU/Linuxオペレーティングシステムを含む、様々な市販のUNIX (登録商標) またはUNIXのようなオペレーティングシステムのいずれかを作動させるワークステーションコンピュータとすることができる。代替的に、または、加えて、クライアントコンピューティングデバイスは、V C N 1106および／またはインターネットにアクセスすることができる、ネットワークを介して通信することが可能な、シンクライアントコンピュータ、インターネット接続可能ゲーミングシステム(例えば、Kinect (登録商標) ジェスチャ入力デバイスを有するかまたは有しないMicrosoft (登録商標) Xboxゲーミングコンソール)、および／またはパーソナルメッセージングデバイスなどの、任意の他の電子デバイスであり得る。

【0171】

V C N 1106は、ローカルピアリングゲートウェイ(L P G) 1110を含むことができ、これは、セキュアシェル(S S H) V C N 1112に含まれるL P G 1110を介してS S H V C N 1112に通信可能に結合され得る。S S H V C N 1112は、S S Hサブネット1114を含むことができ、S S H V C N 1112は、制御プレーンV C N 1116に含まれるL P G 1110を介して制御プレーンV C N 1116に通信可能

に結合され得る。また、SSH VCN 1112は、LPG 1110を介してデータプレーン VCN 1118に通信可能に結合することもできる。制御プレーン VCN 1116およびデータプレーン VCN 1118は、IaaSプロバイダが所有および／または運用することができるサービステナンシ 1119に含めることができる。

【0172】

制御プレーン VCN 1116は、周縁ネットワーク（例えば、企業イントラネットと外部ネットワークとの間の企業ネットワークの部分）として作用する制御プレーン非武装地帯（DMZ）階層 1120を含むことができる。DMZベースのサーバは、役割を制限され得、違反を含まれたままにするのを助け得る。付加的に、DMZ階層 1120は、1つまたは複数のロードバランサ（LB）サブネット 1122、アプリサブネット 1126を含むことができる制御プレーンアプリ階層 1124、データベース（DB）サブネット 1130（例えば、フロントエンドDBサブネットおよび／またはバックエンドDBサブネット）を含むことができる制御プレーンデータ階層 1128を含むことができる。制御プレーンDMZ階層 1120に含まれるLBサブネット 1122は、制御プレーンアプリ階層 1124に含まれるアプリサブネット 1126および制御プレーン VCN 1116に含まれ得るインターネットゲートウェイ 1134に通信可能に結合することができ、アプリサブネット 1126は、制御プレーンデータ階層 1128に含まれるDBサブネット 1130ならびにサービスゲートウェイ 1136およびネットワークアドレス変換（NAT）ゲートウェイ 1138に通信可能に結合され得る。制御プレーン VCN 1116は、サービスゲートウェイ 1136およびNATゲートウェイ 1138を含むことができる。

10

20

【0173】

制御プレーン VCN 1116は、アプリサブネット 1126を含むことができるデータプレーンミラーアプリ階層 1140を含むことができる。データプレーンミラーアプリ階層 1140に含まれるアプリサブネット 1126は、計算インスタンス 1144を実行することができる仮想ネットワークインターフェイスコントローラ（VNIC） 1142を含むことができる。計算インスタンス 1144は、データプレーンミラーアプリ階層 1140のアプリサブネット 1126を、データプレーンアプリ階層 1146に含まれ得るアプリサブネット 1126に通信可能に結合され得る。

【0174】

データプレーン VCN 1118は、データプレーンアプリ階層 1146と、データプレーンDMZ階層 1148と、データプレーンデータ階層 1150とを含むことができる。データプレーンDMZ階層 1148は、データプレーンアプリ階層 1146のアプリサブネット 1126およびデータプレーン VCN 1118のインターネットゲートウェイ 1134に通信可能に結合され得るLBサブネット 1122を含むことができる。アプリサブネット 1126は、データプレーン VCN 1118のサービスゲートウェイ 1136およびデータプレーン VCN 1118のNATゲートウェイ 1138に通信可能に結合され得る。データプレーンデータ階層 1150もまた、データプレーンアプリ階層 1146のアプリサブネット 1126に通信可能に結合され得るDBサブネット 1130を含むことができる。

30

【0175】

制御プレーン VCN 1116およびデータプレーン VCN 1118のインターネットゲートウェイ 1134は、公衆インターネット 1154に通信可能に結合され得るメタデータ管理サービス 1152に通信可能に結合され得る。公衆インターネット 1154は、制御プレーン VCN 1116およびデータプレーン VCN 1118のNATゲートウェイ 1138に通信可能に結合され得る。制御プレーン VCN 1116およびデータプレーン VCN 1118のサービスゲートウェイ 1136は、クラウドサービス 1156に通信可能に結合され得る。

40

【0176】

いくつかの例において、制御プレーン VCN 1116またはデータプレーン VCN 1118のサービスゲートウェイ 1136は、公衆インターネット 1154を経由することな

50

く、クラウドサービス 1156 に対するアプリケーションプログラミングインターフェイス (API) コールを行うことができる。サービスゲートウェイ 1136 からクラウドサービス 1156 への API コールは、一方向であり、すなわち、サービスゲートウェイ 1136 は、クラウドサービス 1156 に対する API コールを行うことができ、クラウドサービス 1156 は、要求されたデータをサービスゲートウェイ 1136 に送ることができる。しかし、クラウドサービス 1156 は、サービスゲートウェイ 1136 に対する API コールを開始することができない。

【0177】

いくつかの例において、セキュアホストテナンシ 1104 は、サービステナンシ 1119 に直接的に接続することができ、これは、他の様態では分離され得る。セキュアホストサブネット 1108 は、他の様態では分離されているシステムを介して双方向通信を可能にすることができる L P G 1110 を通じて S S H サブネット 1114 と通信することができる。セキュアホストサブネット 1108 を S S H サブネット 1114 に接続することによって、セキュアホストサブネット 1108 は、サービステナンシ 1119 内の他のエンティティにアクセスすることができるようになる。

10

【0178】

制御プレーン V C N 1116 は、サービステナンシ 1119 のユーザが、所望のリソースをセットアップまたは他の様態でプロビジョンすることを可能にすることができる。制御プレーン V C N 1116 においてプロビジョンされる所望のリソースは、データプレーン V C N 1118 内に展開されるか、または、他の様態で使用され得る。いくつかの例において、制御プレーン V C N 1116 は、データプレーン V C N 1118 から分離することができる。制御プレーン V C N 1116 のデータプレーンミラーアプリ階層 1140 は、データプレーンミラーアプリ階層 1140 およびデータプレーンアプリ階層 1146 内に含まれ得る V N I C 1142 を介して、データプレーン V C N 1118 のデータプレーンアプリ階層 1146 と通信することができる。

20

【0179】

いくつかの例において、システムのユーザまたは顧客は、公衆インターネット 1154 を通じて、要求、例えば、作成、読み出し、更新、または削除 (C R U D) 動作を行うことができる。公衆インターネットは、メタデータ管理サービス 1152 に要求を通信することができる。メタデータ管理サービス 1152 は、インターネットゲートウェイ 1134 を通じて制御プレーン V C N 1116 に要求を通信することができる。要求は、制御プレーン D M Z 階層 1120 内に含まれる L B サブネット 1122 によって受信することができる。L B サブネット 1122 は、要求が有効であることを判定することができる。この判定に応答して、L B サブネット 1122 は、制御プレーンアプリ階層 1124 内に含まれるアプリサブネット 1126 に要求を送信することができる。要求が、検証され、公衆インターネット 1154 に対するコールを必要とする場合、公衆インターネット 1154 に対するコールを行うことができる N A T ゲートウェイ 1138 に、公衆インターネット 1154 に対するコールを送信することができる。要求によって記憶されることを所望され得るメモリを、D B サブネット 1130 内に記憶することができる。

30

【0180】

いくつかの例において、データプレーンミラーアプリ階層 1140 は、制御プレーン V C N 1116 とデータプレーン V C N 1118 との間の直接通信を促進することができる。例えば、構成に対する変更、更新、または他の適切な修正が、データプレーン V C N 1118 内に含まれるリソースに加えられることが所望され得る。V N I C 1142 を介して、制御プレーン V C N 1116 は、データプレーン V C N 1118 と直接通信することができる。以て、データプレーン V C N 1118 内に含まれるリソースに対して、構成の変更、更新、または他の適切な修正を実行することができる。

40

【0181】

いくつかの実施形態において、制御プレーン V C N 1116 およびデータプレーン V C N 1118 は、サービステナンシ 1119 に含めることができる。この場合、システムの

50

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

【0182】

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

【0183】

図12は、少なくとも1つの実施形態による、IaaSアーキテクチャの別の例示的なパターンを示すブロック図1200である。サービスオペレータ1202（例えば、図11のサービスオペレータ1102）は、仮想クラウドネットワーク（VCN）1206（例えば、図11のVCN1106）およびセキュアホストサブネット1208（例えば、図11のセキュアホストサブネット1108）を含むことができるセキュアホストテナンシ1204（例えば、図11のセキュアホストテナンシ1104）に通信可能に結合され得る。VCN1206は、ローカルピアリングゲートウェイ（LPG）1210（例えば、図11のLPG1110）を含むことができ、これは、セキュアシェル（SSH）VCN1212に含まれるLPG1110を介してセキュアシェル（SSH）VCN1212（例えば、図11のSSH VCN1112）に通信可能に結合され得る。SSH VCN1212は、SSHサブネット1214（例えば、図11のSSHサブネット1114）を含むことができ、SSH VCN1212は、制御プレーンVCN1216に含まれるLPG1210を介して制御プレーンVCN1216（例えば、図11の制御プレーンVCN1116）に通信可能に結合され得る。制御プレーンVCN1216は、サービステナンシ1219（例えば、図11のサービステナンシ1119）に含めることができ、データプレーンVCN1218（例えば、図11のデータプレーンVCN1118）は、システムのユーザまたは顧客によって所有または運営され得る顧客テナンシ1221に含めることができる。

【0184】

制御プレーンVCN1216は、LBサブネット1222（例えば、図11のLBサブネット1122）を含むことができる制御プレーンDMZ階層1220（例えば、図11の制御プレーンDMZ階層1120）と、アプリサブネット1226（例えば、図11のアプリサブネット1126）を含むことができる制御プレーンアプリ階層1224（例えば、図11の制御プレーンアプリ階層1124）と、データベース（DB）サブネット1230（例えば、図11のDBサブネット1130と同様の）を含むことができる制御プレーンデータ階層1228（例えば、図11の制御プレーンデータ階層1128）とを含むことができる。制御プレーンDMZ階層1220に含まれるLBサブネット1222は、制御プレーンアプリ階層1224に含まれるアプリサブネット1226および制御プレーンVCN1216に含まれ得るインターネットゲートウェイ1234（例えば、図11のインターネットゲートウェイ1134）に通信可能に結合することができ、アプリサブネット1226は、制御プレーンデータ階層1228に含まれるDBサブネット1230

10

20

30

40

50

ならびにサービスゲートウェイ 1 2 3 6（例えば、図 1 1 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 2 3 8（例えば、図 1 1 の NAT ゲートウェイ 1 1 3 8）に通信可能に結合され得る。制御プレーン VCN 1 2 1 6 は、サービスゲートウェイ 1 2 3 6 および NAT ゲートウェイ 1 2 3 8 を含むことができる。

【0185】

制御プレーン VCN 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階層 1 2 4 0（例えば、図 1 1 のデータプレーンミラーアプリ階層 1 1 4 0）を含むことができる。データプレーンミラーアプリ階層 1 2 4 0 に含まれるアプリサブネット 1 2 2 6 は、コンピュータインスタンス 1 2 4 4（例えば、図 1 1 のコンピュータインスタンス 1 1 4 4 と同様の）を実行することができる仮想ネットワークインターフェイスコントローラ（VNIC）1 2 4 2（例えば、1 1 4 2 の VNIC）を含むことができる。コンピュータインスタンス 1 2 4 4 は、データプレーンミラーアプリ階層 1 2 4 0 内に包含されている VNIC 1 2 4 2 およびデータプレーンアプリ階層 1 2 4 6 内に包含されている VNIC 1 2 4 2 を介して、データプレーンミラーアプリ階層 1 2 4 0 のアプリサブネット 1 2 2 6 と、データプレーンアプリ階層 1 2 4 6（例えば、図 1 1 のデータプレーンアプリ階層 1 1 4 6）内に包含され得るアプリサブネット 1 2 2 6 との間の通信を促進することができる。

【0186】

制御プレーン VCN 1 2 1 6 内に包含されているインターネットゲートウェイ 1 2 3 4 は、公衆インターネット 1 2 5 4（例えば、図 1 1 の公衆インターネット 1 1 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（例えば、図 1 1 のメタデータ管理サービス 1 1 5 2）に通信可能に結合され得る。公衆インターネット 1 2 5 4 は、制御プレーン VCN 1 2 1 6 内に包含されている 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 2 1 6 内に包含されている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（例えば、図 1 1 のクラウドサービス 1 1 5 6）に通信可能に結合され得る。

【0187】

いくつかの例において、データプレーン VCN 1 2 1 8 は、顧客テナンシ 1 2 2 1 に含めることができる。この場合、IaaS プロバイダが、各顧客について制御プレーン VCN 1 2 1 6 を提供することができる。IaaS プロバイダは、各顧客について、サービステナンシ 1 2 1 9 内に包含される固有の計算インスタンス 1 2 4 4 をセットアップすることができる。各計算インスタンス 1 2 4 4 は、サービステナンシ 1 2 1 9 内に包含されている制御プレーン VCN 1 2 1 6 と、顧客テナンシ 1 2 2 1 内に包含されているデータプレーン VCN 1 2 1 8 との間の通信を可能にすることができる。計算インスタンス 1 2 4 4 は、サービステナンシ 1 2 1 9 内に包含されている制御プレーン VCN 1 2 1 6 内にプロビジョンされるリソースが、顧客テナンシ 1 2 2 1 内に包含されているデータプレーン VCN 1 2 1 8 内で展開されるか、または、他の状態で使用されることを可能にすることができる。

【0188】

他の例において、IaaS プロバイダの顧客は、顧客テナンシ 1 2 2 1 内に常駐するデータベースを有することができる。この例において、制御プレーン VCN 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階層 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階層 1 2 4 0 は、データプレーン VCN 1 2 1 8 内に存在することができるが、データプレーンミラーアプリ階層 1 2 4 0 は、データプレーン VCN 1 2 1 8 内に常駐しなくてもよい。すなわち、データプレーンミラーアプリ階層 1 2 4 0 は、顧客テナンシ 1 2 2 1 にアクセスすることができるが、データプレーンミラーアプリ階層 1 2 4 0 は、データプレーン VCN 1 2 1 8 内に存在しなくてもよく、または、IaaS プロバイダの顧客によって所有もしくは運営されなくてもよい。データプレーンミラーアプリ階層 1 2 4 0 は、データプレーン VCN 1 2 1 8 に対してコールを行うように構成することができるが、制御プレーン VCN 1 2 1 6 内に包含されて

いる任意のエンティティにもコールを行うように構成されなくてもよい。顧客は、制御プレーンV C N 1 2 1 6内にプロビジョンされているデータプレーンV C N 1 2 1 8内のリソースを展開するかまたは他の様態で使用するを所望する場合があります、データプレーンミラーアプリ階層1 2 4 0は、顧客が所望するリソースの展開または他の使用を促進することができる。

【0189】

いくつかの例において、I a a Sプロバイダの顧客は、データプレーンV C N 1 2 1 8にフィルタを適用することができる。この実施形態において、顧客は、データプレーンV C N 1 2 1 8がアクセスすることができるものを決定することができ、顧客は、データプレーンV C N 1 2 1 8からの公衆インターネット1 2 5 4へのアクセスを制約することができる。I a a Sプロバイダは、データプレーンV C N 1 2 1 8の任意の外部ネットワークまたはデータベースに対するアクセスにフィルタを適用するか、または、他の様態で制御することが可能でなくともよい。顧客による、顧客テナンシ1 2 2 1内に含まれているデータプレーンV C N 1 2 1 8に対するフィルタの適用および制御は、データプレーンV C N 1 2 1 8を他の顧客および公衆インターネット1 2 5 4から分離することを助けることができる。

【0190】

いくつかの実施形態において、クラウドサービス1 2 5 6は、公衆インターネット1 2 5 4、制御プレーンV C N 1 2 1 6、またはデータプレーンV C N 1 2 1 8上に存在しない場合があるサービスにアクセスするために、サービスゲートウェイ1 2 3 6によってコールすることができる。クラウドサービス1 2 5 6と制御プレーンV C N 1 2 1 6またはデータプレーンV C N 1 2 1 8との間の接続は、ライブまたは連続的でなくともよい。クラウドサービス1 2 5 6は、I a a Sプロバイダが所有または運営する異なるネットワーク上に存在し得る。クラウドサービス1 2 5 6は、サービスゲートウェイ1 2 3 6からコールを受信するように構成することができ、公衆インターネット1 2 5 4からのコールは受信しないように構成することができる。いくつかのクラウドサービス1 2 5 6は、他のクラウドサービス1 2 5 6から分離され得、制御プレーンV C N 1 2 1 6は、制御プレーンV C N 1 2 1 6と同じリージョンにない場合があるクラウドサービス1 2 5 6から分離され得る。例えば、制御プレーンV C N 1 2 1 6は「リージョン1」に位置する場合があります、クラウドサービス「展開1 1」は、リージョン1および「リージョン2」に位置する場合があります。展開1 1に対するコールがリージョン1に位置する制御プレーンV C N 1 2 1 6内に含まれているサービスゲートウェイ1 2 3 6によって行われた場合、コールは、リージョン1の展開1 1に送信され得る。この例において、制御プレーンV C N 1 2 1 6またはリージョン1の展開1 1は、リージョン2の展開1 1に通信可能に結合されなくともよく、または、他の様態でこれと通信しなくともよい。

【0191】

図1 3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 3 0 0である。サービスオペレータ1 3 0 2（例えば、図1 1のサービスオペレータ1 1 0 2）は、仮想クラウドネットワーク（V C N）1 3 0 6（例えば、図1 1のV C N 1 1 0 6）およびセキュアホストサブネット1 3 0 8（例えば、図1 1のセキュアホストサブネット1 1 0 8）を含むことができるセキュアホストテナンシ1 3 0 4（例えば、図1 1のセキュアホストテナンシ1 1 0 4）に通信可能に結合され得る。V C N 1 3 0 6は、L P G 1 3 1 0（例えば、図1 1のL P G 1 1 1 0）を含むことができ、これは、S S H V C N 1 3 1 2に含まれるL P G 1 3 1 0を介してS S H V C N 1 3 1 2（例えば、図1 1のS S H V C N 1 1 1 2）に通信可能に結合され得る。S S H V C N 1 3 1 2は、S S Hサブネット1 3 1 4（例えば、図1 1のS S Hサブネット1 1 1 4）を含むことができ、S S H V C N 1 3 1 2は、制御プレーンV C N 1 3 1 6に含まれるL P G 1 3 1 0を介して制御プレーンV C N 1 3 1 6（例えば、図1 1の制御プレーンV C N 1 1 1 6）に通信可能に結合することができ、データプレーンV C N 1 3 1 8に含まれるL P G 1 3 1 0を介してデータプレーンV C N 1 3 1 8（例えば、

図 1 1 のデータプレーン V C N 1 1 1 8) に通信可能に結合され得る。制御プレーン V C N 1 3 1 6 およびデータプレーン V C N 1 3 1 8 は、サービステナンシ 1 3 1 9 (例えば、図 1 1 のサービステナンシ 1 1 1 9) に含めることができる。

【0192】

制御プレーン V C N 1 3 1 6 は、ロードバランサ (L B) サブネット 1 3 2 2 (例えば、図 1 1 の L B サブネット 1 1 2 2) を含むことができる制御プレーン D M Z 階層 1 3 2 0 (例えば、図 1 1 の制御プレーン D M Z 階層 1 1 2 0) と、アプリサブネット 1 3 2 6 (例えば、図 1 1 のアプリサブネット 1 1 2 6 と同様の) を含むことができる制御プレーンアプリ階層 1 3 2 4 (例えば、図 1 1 の制御プレーンアプリ階層 1 1 2 4) と、D B サブネット 1 3 3 0 を含むことができる制御プレーンデータ階層 1 3 2 8 (例えば、図 1 1 の制御プレーンデータ階層 1 1 2 8) とを含むことができる。制御プレーン D M Z 階層 1 3 2 0 に含まれる L B サブネット 1 3 2 2 は、制御プレーンアプリ階層 1 3 2 4 に含まれるアプリサブネット 1 3 2 6 および制御プレーン V C N 1 3 1 6 に含まれ得るインターネットゲートウェイ 1 3 3 4 (例えば、図 1 1 のインターネットゲートウェイ 1 1 3 4) に通信可能に結合することができる。アプリサブネット 1 3 2 6 は、制御プレーンデータ階層 1 3 2 8 に含まれる D B サブネット 1 3 3 0 ならびにサービスゲートウェイ 1 3 3 6 (例えば、図 1 1 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 3 3 8 (例えば、図 1 1 の N A T ゲートウェイ 1 1 3 8) に通信可能に結合され得る。制御プレーン V C N 1 3 1 6 は、サービスゲートウェイ 1 3 3 6 および N A T ゲートウェイ 1 3 3 8 を含むことができる。

【0193】

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

【0194】

信頼できないアプリサブネット 1 3 6 2 は、テナント仮想マシン (V M) 1 3 6 6 (1) ~ (N) に通信可能に結合され得る 1 つまたは複数の V N I C 1 3 6 4 (1) ~ (N) を含むことができる。各テナント V M 1 3 6 6 (1) ~ (N) は、それぞれの顧客テナンシ 1 3 7 0 (1) ~ (N) 内に包含され得るそれぞれのコンテナイグレス V C N 1 3 6 8 (1) ~ (N) 内に包含され得るそれぞれのアプリサブネット 1 3 6 7 (1) ~ (N) に通信可能に結合され得る。それぞれの二次 V N I C 1 3 7 2 (1) ~ (N) が、データプレーン V C N 1 3 1 8 内に包含されている信頼できないアプリサブネット 1 3 6 2 とコンテナイグレス V C N 1 3 6 8 (1) ~ (N) 内に包含されているアプリサブネットとの間の通信を促進することができる。各コンテナイグレス V C N 1 3 6 8 (1) ~ (N) は、公衆インターネット 1 3 5 4 (例えば、図 1 1 の公衆インターネット 1 1 5 4) に通信可能に結合され得る N A T ゲートウェイ 1 3 3 8 を含むことができる。

【0195】

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

10

【0196】

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

【0197】

いくつかの例において、IaaSプロバイダの顧客は、一時的なネットワークアクセスをIaaSプロバイダに許可し、データプレーン階層アプリ1346に付随する機能を要求することができる。機能を実行するためのコードは、VM1366（1）～（N）内で実行することができ、コードは、データプレーンVCN1318上のそれ以外の場所で実行するように構成されなくてもよい。各VM1366（1）～（N）は、1つの顧客テナンシ1370に接続することができる。VM1366（1）～（N）内に包含されているそれぞれのコンテナ1371（1）～（N）が、コードを実行するように構成され得る。この場合、二重の分離（例えば、コンテナ1371（1）～（N）がコードを実行し、ここで、コンテナ1371（1）～（N）が、少なくとも、信頼できないアプリサブネット1362内に包含されているVM1366（1）～（N）内に包含され得る）が存在し得、これは、正しくないかまたは他の様態で望ましくないコードがIaaSプロバイダのネットワークを損傷すること、または、異なる顧客のネットワークを損傷することを防止するのを助けることができる。コンテナ1371（1）～（N）は、顧客テナンシ1370に通信可能に結合することができ、顧客テナンシ1370からデータを送信または受信するように構成することができる。コンテナ1371（1）～（N）は、データプレーンVCN1318内のいかなる他のエンティティからのデータを送信または受信するように構成されなくてもよい。コードの実行が完了すると、IaaSプロバイダは、コンテナ1371（1）～（N）を停止させるかまたは他の様態で破棄することができる。

20

30

【0198】

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

40

【0199】

50

他の実施形態において、制御プレーンV C N 1 3 1 6およびデータプレーンV C N 1 3 1 8は、直接的に通信可能に結合されなくてもよい。この実施形態において、制御プレーンV C N 1 3 1 6とデータプレーンV C N 1 3 1 8との間には直接通信が存在しなくてもよい。しかしながら、通信は、少なくとも1つの方法を通じて間接的に行うことができる。制御プレーンV C N 1 3 1 6とデータプレーンV C N 1 3 1 8との間の通信を促進することができるL P G 1 3 1 0が、I a a Sプロバイダによって確立され得る。別の例において、制御プレーンV C N 1 3 1 6またはデータプレーンV C N 1 3 1 8が、サービスゲートウェイ1 3 3 6を介してクラウドサービス1 3 5 6に対するコールを行うことができる。例えば、制御プレーンV C N 1 3 1 6からクラウドサービス1 3 5 6に対するコールは、データプレーンV C N 1 3 1 8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。

10

【0200】

図14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1400である。サービスオペレータ1402（例えば、図11のサービスオペレータ1102）は、仮想クラウドネットワーク（V C N）1406（例えば、図11のV C N 1106）およびセキュアホストサブネット1408（例えば、図11のセキュアホストサブネット1108）を含むことができるセキュアホストテナンシ1404（例えば、図11のセキュアホストテナンシ1104）に通信可能に結合され得る。V C N 1406は、L P G 1410（例えば、図11のL P G 1110）を含むことができ、これは、S S H V C N 1412に含まれるL P G 1410を介してS S H V C N 1412（例えば、図11のS S H V C N 1112）に通信可能に結合され得る。S S H V C N 1412は、S S Hサブネット1414（例えば、図11のS S Hサブネット1114）を含むことができ、S S H V C N 1412は、制御プレーンV C N 1416に含まれるL P G 1410を介して制御プレーンV C N 1416（例えば、図11の制御プレーンV C N 1116）に通信可能に結合することができ、データプレーンV C N 1418に含まれるL P G 1410を介してデータプレーンV C N 1418（例えば、図11のデータプレーンV C N 1118）に通信可能に結合され得る。制御プレーンV C N 1416およびデータプレーンV C N 1418は、サービステナンシ1419（例えば、図11のサービステナンシ1119）に含めることができる。

20

【0201】

制御プレーンV C N 1416は、L Bサブネット1422（例えば、図11のL Bサブネット1122）を含むことができる制御プレーンD M Z階層1420（例えば、図11の制御プレーンD M Z階層1120）と、アプリサブネット1426（例えば、図11のアプリサブネット1126）を含むことができる制御プレーンアプリ階層1424（例えば、図11の制御プレーンアプリ階層1124）と、D Bサブネット1430（例えば、図13のD Bサブネット1330）を含むことができる制御プレーンデータ階層1428（例えば、図11の制御プレーンデータ階層1128）とを含むことができる。制御プレーンD M Z階層1420に含まれるL Bサブネット1422は、制御プレーンアプリ階層1424に含まれるアプリサブネット1426および制御プレーンV C N 1416に含まれ得るインターネットゲートウェイ1434（例えば、図11のインターネットゲートウェイ1134）に通信可能に結合することができ、アプリサブネット1426は、制御プレーンデータ階層1428に含まれるD Bサブネット1430ならびにサービスゲートウェイ1436（例えば、図11のサービスゲートウェイ）およびネットワークアドレス変換（N A T）ゲートウェイ1438（例えば、図11のN A Tゲートウェイ1138）に通信可能に結合され得る。制御プレーンV C N 1416は、サービスゲートウェイ1436およびN A Tゲートウェイ1438を含むことができる。

30

40

【0202】

データプレーンV C N 1418は、データプレーンアプリ階層1446（例えば、図11のデータプレーンアプリ階層1146）と、データプレーンD M Z階層1448（例えば、図11のデータプレーンD M Z階層1148）と、データプレーンデータ階層145

50

0（例えば、図11のデータプレーンデータ階層1150）とを含むことができる。データプレーンDMZ階層1448は、データプレーンアプリ階層1446の信頼できるアプリサブネット1460（例えば、図13の信頼できるアプリサブネット1360）および信頼できないアプリサブネット1462（例えば、図13の信頼できないアプリサブネット1362）ならびにデータプレーンVCN1418内に包含されているインターネットゲートウェイ1434に通信可能に結合され得るLBサブネット1422を含むことができる。信頼できるアプリサブネット1460は、データプレーンVCN1418内に包含されているサービスゲートウェイ1436、データプレーンVCN1418内に包含されているNATゲートウェイ1438、およびデータプレーンデータ階層1450内に包含されているDBサブネット1430に通信可能に結合され得る。信頼できないアプリサブネット1462は、データプレーンVCN1418内に包含されているサービスゲートウェイ1436およびデータプレーンデータ階層1450内に包含されているDBサブネット1430に通信可能に結合され得る。データプレーンデータ階層1450は、データプレーンVCN1418内に包含されているサービスゲートウェイ1436に通信可能に結合され得るDBサブネット1430を含むことができる。

10

20

30

40

50

【0203】

信頼できないアプリサブネット1462は、信頼できないアプリサブネット1462内に存在するテナント仮想マシン（VM）1466（1）～（N）に通信可能に結合され得る一次VNIC1464（1）～（N）を含むことができる。各テナントVM1466（1）～（N）は、それぞれのコンテナ1467（1）～（N）内のコードを実行することができ、コンテナイグレスVCN1468内に包含され得るデータプレーンアプリ階層1446内に包含され得るアプリサブネット1426に通信可能に結合され得る。それぞれの二次VNIC1472（1）～（N）が、データプレーンVCN1418内に包含されている信頼できないアプリサブネット1462とコンテナイグレスVCN1468内に包含されているアプリサブネットとの間の通信を促進することができる。コンテナイグレスVCNは、公衆インターネット1454（例えば、図11の公衆インターネット1154）に通信可能に結合され得るNATゲートウェイ1438を含むことができる。

【0204】

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

【0205】

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

ット 1 4 5 4 にコールを送信することができる。この例において、顧客によってリアルタイムにアクセスすることができるコンテナ 1 4 6 7 (1) ~ (N) は、制御プレーン V C N 1 4 1 6 から分離することができ、データプレーン V C N 1 4 1 8 内に含まれている他のエンティティから分離することができる。コンテナ 1 4 6 7 (1) ~ (N) はまた、他の顧客のリソースからも分離することができる。

【0206】

他の例において、顧客は、コンテナ 1 4 6 7 (1) ~ (N) を使用してクラウドサービス 1 4 5 6 をコールすることができる。この例において、顧客は、クラウドサービス 1 4 5 6 からのサービスを要求するコードを、コンテナ 1 4 6 7 (1) ~ (N) 内で実行することができる。コンテナ 1 4 6 7 (1) ~ (N) は、この要求を二次 V N I C 1 4 7 2 (1) ~ (N) に送信することができ、二次 V N I C 1 4 7 2 (1) ~ (N) は、N A T ゲートウェイに要求を送信することができ、N A T ゲートウェイは、公衆インターネット 1 4 5 4 に要求を送信することができる。公衆インターネット 1 4 5 4 は、インターネットゲートウェイ 1 4 3 4 を介して、制御プレーン V C N 1 4 1 6 内に含まれている L B サブネット 1 4 2 2 に要求を送信することができる。要求が有効であるという判定に回答して、L B サブネットは、アプリサブネット 1 4 2 6 に要求を送信することができ、アプリサブネット 1 4 2 6 は、サービスゲートウェイ 1 4 3 6 を介してクラウドサービス 1 4 5 6 に要求を送信することができる。

【0207】

図面に示されている I a a S アーキテクチャ 1 1 0 0、1 2 0 0、1 3 0 0、1 4 0 0 は、図示されている以外の構成要素を有し得ることは理解されるべきである。さらに、図面に示されている実施形態は、本開示の実施形態を組み込むことができるクラウドインフラストラクチャシステムの一部の例に過ぎない。いくつかの他の実施形態において、I a a S システムは、図示されているよりも多いもしくは少ない構成要素を有してもよく、2 つ以上の構成要素を組み合わせてもよく、または、構成要素の異なる構成もしくは配置を有し得る。

【0208】

ある実施形態において、本明細書に記載されている I a a S システムは、セルフサービスで、サブスクリプションに基づいて、弾性的にスケーリング可能に、信頼可能に、高度に利用可能に、および安全に顧客に送達されるアプリケーション、ミドルウェア、およびデータベースサービス供給物のスイートを含み得る。そのような I a a S の一例は、本譲受人によって提供される Oracle インフラストラクチャ (O C I) である。

【0209】

図 1 5 は、様々な実施形態を実装することができる例示的なコンピュータシステム 1 5 0 0 を示す。システム 1 5 0 0 は、上述したコンピュータシステムのいずれかを実装するために使用することができる。図面に示すように、コンピュータシステム 1 5 0 0 は、バスサブシステム 1 5 0 2 を介して複数の周辺サブシステムと通信する処理装置 1 5 0 4 を含む。これらの周辺サブシステムは、処理加速ユニット 1 5 0 6、I / O サブシステム 1 5 0 8、記憶サブシステム 1 5 1 8 および通信サブシステム 1 5 2 4 を含み得る。記憶サブシステム 1 5 1 8 は、有形コンピュータ可読記憶媒体 1 5 2 2 およびシステムメモリ 1 5 1 0 を含む。

【0210】

バスサブシステム 1 5 0 2 は、コンピュータシステム 1 5 0 0 の様々な構成要素およびサブシステムを意図したように互いに通信させるためのメカニズムを提供する。バスサブシステム 1 5 0 2 は、単一のバスとして概略的に示されているが、バスサブシステムの代替的な実施形態は、複数のバスを利用し得る。バスサブシステム 1 5 0 2 は、メモリバスまたはメモリコントローラ、周辺機器用バス、および、様々なバスアーキテクチャのうちのいずれかを使用するローカルバスを含む、いくつかのタイプのバス構造のいずれかであり得る。例えば、このようなアーキテクチャは、業界標準アーキテクチャ (I S A) バス、マイクロチャネルアーキテクチャ (M C A) バス、拡張 I S A (E I S A) バス、ビデ

オ電子機器標準規格化協会（VESA）ローカルバス、および、IEEE P1386.1規格に従って製造されたMezzanineバスとして実装することができる周辺構成要素相互接続（PCI）バスを含み得る。

【0211】

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

10

【0212】

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

20

【0213】

I/Oサブシステム1508は、ユーザインターフェイス入力デバイスおよびユーザインターフェイス出力デバイスを含むことができる。ユーザインターフェイス入力デバイスは、キーボード、マウスまたはトラックボール、タッチパッドまたはディスプレイに組み込まれたタッチスクリーンなどのポインティングデバイス、スクロールホイール、クリックホイール、ダイヤル、ボタン、スイッチ、キーパッド、音声コマンド認識システムを有する音響入力デバイス、マイクロフォン、および他のタイプの入力デバイスを含み得る。ユーザインターフェイス入力デバイスは、例えば、ユーザが、ジェスチャおよび音声指示を使用してナチュラルユーザインターフェイスを通じて、Microsoft Xbox（登録商標）360ゲームコントローラなどの入力デバイスを制御し、それと相互に作用することを可能にするMicrosoft Kinect（登録商標）運動センサなどの運動検知および／またはジェスチャ認識デバイスを含み得る。ユーザインターフェイス入力デバイスはまた、ユーザから眼球活動（例えば、写真を撮っている、および／または、メニュー選択を行っている間の「まばたき」）を検出し、そのアイジェスチャを入力デバイス（例えば、Google 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認識デバイスも含み得る。付加的に、ユーザインターフェイス入力デバイスは、ユーザが、音声コマンドを通じて音声認識システム（例えば、Siri（登録商標）ナビゲータ）と相互に作用することを可能にする音声認識検知デバイスを含み得る。

30

40

【0214】

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

50

はまた、例えば、M I D I キーボード、デジタル楽器などのような音響入力デバイスも含み得る。

【0215】

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

10

【0216】

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

20

【0217】

コンピュータシステム1500の構成およびタイプに応じて、システムメモリ1510は、揮発性（ランダムアクセスメモリ（R A M）など）および／または不揮発性（読み出し専用メモリ（R O M）、フラッシュメモリなど）であり得る。R A Mは、典型的には、処理装置1504にとって直ちにアクセス可能であり、ならびに／または、処理装置1504によって現在動作および実行されているデータおよび／またはプログラムモジュールを包含する。いくつかの実施態様において、システムメモリ1510は、スタティックランダムアクセスメモリ（S R A M）またはダイナミックランダムアクセスメモリ（D R A M）などの、複数の異なるタイプのメモリを含み得る。いくつかの実施態様において、起動中などにコンピュータシステム1500内の要素間で情報を転送するのを助ける基本ルーチンを包含する基本入出力システム（B I O S）が、典型的には、R O M内に記憶され得る。限定ではなく例として、システムメモリ1510はまた、クライアントアプリケーション、ウェブブラウザ、中間層アプリケーション、リレーショナルデータベース管理システム（R D B M S）などを含み得るアプリケーションプログラム1512、プログラムデータ1514、およびオペレーティングシステム1516も例示する。例として、オペレーティングシステム1516は、様々なバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、ならびに／または、様々な市販のUNIX（登録商標）もしくはUNIX系オペレーティングシステム（限定ではないが、様々なGNU/Linuxオペレーティングシステム、Google Chrome（登録商標）OSなど）、ならびに／または、iOS、Windows（登録商標）Phone、Android（登録商標）OS、BlackBerry（登録商標）15 OS、およびPalm（登録商標）OSオペレーティングシステムなどのモバイルオペレーティングシステムを含み得る。

30

40

【0218】

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

50

【0219】

記憶サブシステム1500はまた、コンピュータ可読記憶媒体1522にさらに接続することができるコンピュータ可読記憶媒体リーダ1520も含むことができる。システムメモリ1510とともに、および、任意選択的にシステムメモリ1510と組み合わせて、コンピュータ可読記憶媒体1522は、コンピュータ可読情報を一時的および／またはより持続的に包含、記憶、送信、および抽出するための遠隔、ローカル、固定、および／または取り外し可能記憶デバイス+記憶媒体を包括的に表すことができる。

【0220】

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

【0221】

例として、コンピュータ可読記憶媒体1522は、取り外し不能不揮発性磁気媒体から読み出すかまたはこれに書き込むハードディスクドライブ、取り外し可能不揮発性磁気ディスクから読み出すかまたはこれに書き込む磁気ディスクドライブ、および、CDROM、DVD、およびBlu-ray（登録商標）ディスクまたは他の光媒体などの取り外し可能不揮発性光ディスクから読み出すかまたはこれに書き込む光ディスクドライブを含み得る。コンピュータ可読記憶媒体1522は、限定ではないが、Zip（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（USB）フラッシュデバイス、セキュアデジタル（SD）カード、DVDディスク、デジタルビデオテープなどを含み得る。コンピュータ可読記憶媒体1522はまた、フラッシュメモリベースのSSD、企業フラッシュドライブ、ソリッドステートROMなどのような不揮発性メモリに基づくソリッドステートドライブ（SSD）、ソリッドステートRAM、ダイナミックRAM、スタティックRAMなどの揮発性メモリに基づくSSD、DRAMベースのSSD、磁気抵抗RAM（MRAM）SSD、およびDRAMとフラッシュメモリベースのSSDとの組み合わせを使用するハイブリッドSSDも含み得る。ディスクドライブおよびそれらの関連コンピュータ可読媒体は、コンピュータシステム1500に、コンピュータ可読命令、データ構造体、プログラムモジュールおよび他のデータの非揮発性記憶を提供することができる。

【0222】

通信サブシステム1524は、他のコンピュータシステムおよびネットワークに対するインターフェイスを提供する。通信サブシステム1524は、他のシステムからデータを受信し、コンピュータシステム1500から他のシステムにデータを送信するためのインターフェイスとしての役割を果たす。例えば、通信サブシステム1524は、コンピュータシステム1500が、インターネットを介して1つまたは複数のデバイスに接続することを可能にすることができる。いくつかの実施形態において、通信サブシステム1524は、ワイヤレス音声および／もしくはデータネットワーク（例えば、携帯電話技術、3G、4GまたはEDGE（グローバル進化型高速データレート）、WiFi（登録商標）（IEEE 802.11ファミリ規格、もしくは他のモバイル通信技術などの先進的なデータネットワーク技術、またはそれらの任意の組み合わせを使用する）にアクセスするための無線周波数（RF）トランシーバ構成要素、全地球測位システム（GPS）レシーバ構

成要素、ならびに／または他の構成要素を含むことができる。いくつかの実施形態において、通信サブシステム 1524 は、ワイヤレスインターフェイスに加えてまたはその代わりに有線ネットワーク接続（例えば、イーサネット（登録商標））を提供することができる。

【0223】

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

【0224】

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

【0225】

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

【0226】

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

【0227】

コンピュータシステム 1500 は、手持ち式ポータブルデバイス（例えば、iPhone（登録商標）携帯電話、iPad（登録商標）コンピューティングタブレット、PDA）、ウェアラブルデバイス（例えば、Google Glass（登録商標）ヘッドマウントディスプレイ）、PC、ワークステーション、メインフレーム、キオスク、サーバラック、または任意の他のデータ処理システムを含む、様々なタイプのうちの 1 つとすることができる。

【0228】

コンピュータおよびネットワークの絶えず変化する性質のために、図面に示されているコンピュータデバイス 1500 の説明は、特定の例としてのみ意図されている。図面に示されるシステムよりも多いまたは少ない構成要素を有する、多くの他の構成が可能である。例えば、カスタム化ハードウェアもまた使用されてもよく、および／または、特定の要素が、ハードウェア、ファームウェア、ソフトウェア（アプレットを含む）、または組み合わせにおいて実装され得る。さらに、ネットワーク入出力デバイスなどの他のコンピューティングデバイスへの接続が利用され得る。本開示および本明細書において提供されている教示に基づいて、当業者は、様々な実施形態を実装するための他の様式および／または方法を理解するであろう。

【0229】

実施形態は、プロセッサによって実行されると、プロセッサに、本開示に記載の方法のいずれかを実施させるコンピュータプログラム命令を含むコンピュータプログラム製品を使用することによって実装することができる。

【0230】

特定の実施形態が説明されたが、様々な修正、改変、代替的な構成、および均等物も、本開示の範囲内に包含される。実施形態は、ある特定のデータ処理環境内での動作に限定されず、複数のデータ処理環境内で自由に動作することができる。付加的に、実施形態は特定の系列のランザクションおよびステップを使用して説明されているが、本開示の範囲は、記載されている系列のランザクションおよびステップには限定されないことは、当業者には明らかであろう。上述した実施形態の様々な特徴および態様は、個別にまたは連帯して使用され得る。

【0231】

さらに、実施形態は、ハードウェアとソフトウェアとの特定の組み合わせを使用して説明されているが、ハードウェアとソフトウェアとの他の組み合わせも、本開示の範囲内に
10
あることは認識されたい。実施形態は、ハードウェア内でのみ、もしくはソフトウェア内でのみ、またはそれらの組み合わせを使用して実装され得る。本明細書に記載されている様々なプロセスは、同じプロセッサ上で、または、任意の組み合わせにおける複数の異なるプロセッサ上で実装することができる。したがって、構成要素またはモジュールが特定の動作を実施するように構成されているものとして説明されている場合、そのような構成は、例えば、動作を実施するように電子回路を設計することによって、動作を実施するようにプログラム可能電子回路（マイクロプロセッサなど）をプログラムすることによって、またはその任意の組み合わせによって、そのような構成を達成することができる。プロセスは、限定ではないが、プロセス間通信のための従来の技法を含む様々な技法を使用して通信することができ、プロセスの異なる対が、異なる技法を使用してもよく、または、
20
プロセスの同じ対が、異なる時点において異なる技法を使用し得る。

【0232】

したがって、本明細書および図面は、限定的な意味ではなく、例示的な意味において考慮されるべきである。しかしながら、特許請求の範囲に記載されているより広い思想および範囲から逸脱することなく、追加、差し引き、削除、および他の修正および変更をそれに行うことができることは明らかであろう。したがって、特定の開示実施形態が説明されているが、これらは、限定であるようには意図されていない。様々な修正および均等物が、添付の特許請求項の範囲内にある。

【0233】

本開示の実施形態を説明する文脈における（特に、以下の特許請求の範囲の文脈における）「a」および「an」ならびに「the」という用語および同様の指示対象の使用は、本明細書において別様に指示されていない限り、または、文脈と明確に矛盾しない限り、単数および複数の両方をカバーするように解釈されるべきである。「備える（comprising）」、「有する（having）」、「含む（including）」および「包含する（containing）」という用語は、特に言及されていない限り、オープンエンドな用語（すなわち、「限定ではないが、……を含む」を意味する）として解釈されるべきである。「接続されている」という用語は、何かが介在する場合であっても、部分的にまたは全体が中に包含されているか、取り付けられているか、またはともに接合されているものとして解釈されるべきである。本明細書における値の範囲の記述は、本明細書において別様に指示され
30
おらず、各別個の値が本明細書において個別に記述されているかのように本明細書に組み込まれていない限り、その範囲内に入る各別個の値を個別に参照する簡潔な方法としての役割を果たすように意図されているに過ぎない。本明細書に記載されているすべての方法は、本明細書において別様に指示されていない限り、または、文脈と明確に矛盾しない限り、任意の適切な順序において実施することができる。本明細書において与えられているあらゆる例、または例示の文言（例えば、「～のような（such as）」）は、より良好に実施形態の理解を助けるようにのみ意図されており、別途主張されない限り、本開示の範囲に限定を課すものではない。本明細書におけるいかなる文言も、任意の特許請求されていない要素を、本開示の実践に必須であるとして指示しているものとして解釈されるべきではない。
40

【0234】

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

【0235】

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

10

【0236】

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

20

【0237】

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

30

40

50

【図面】

【図 1】

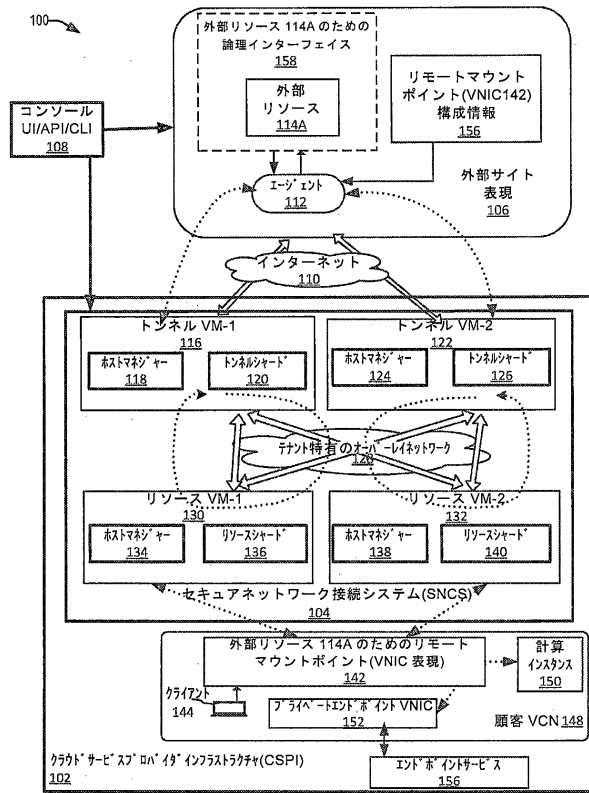


FIG. 1

【図 2】

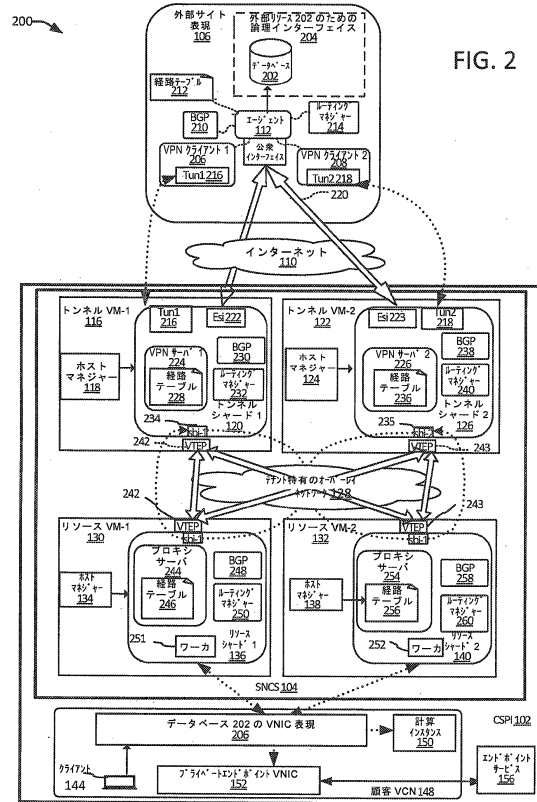


FIG. 2

【図 3】

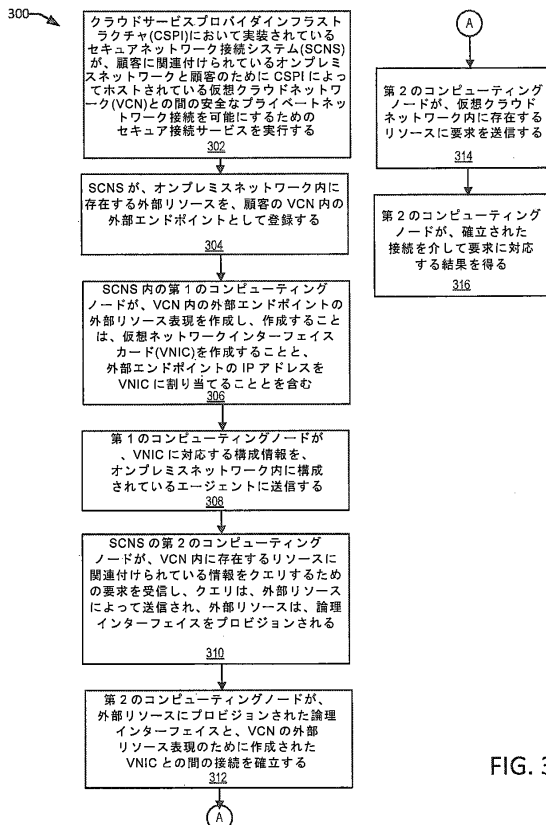


FIG. 3

【図 4】

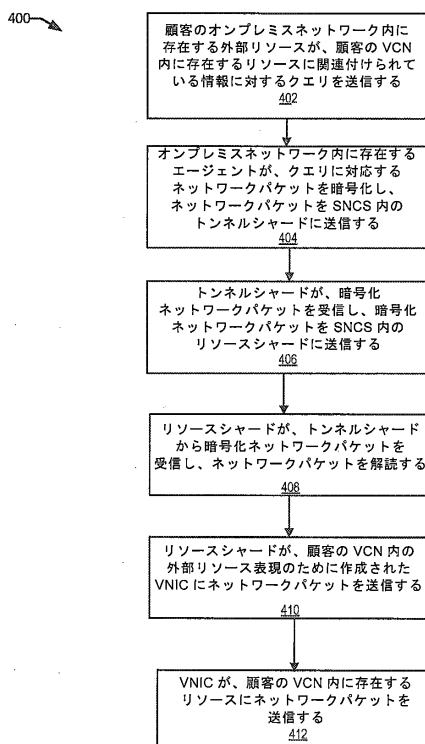


FIG. 4

【図 5】

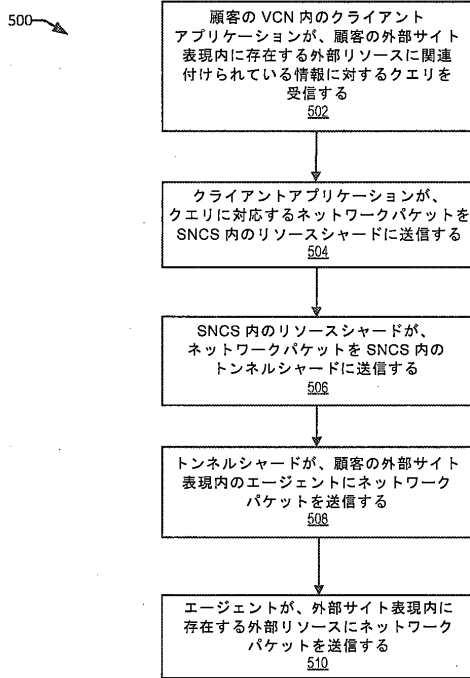


FIG. 5

【図 6】

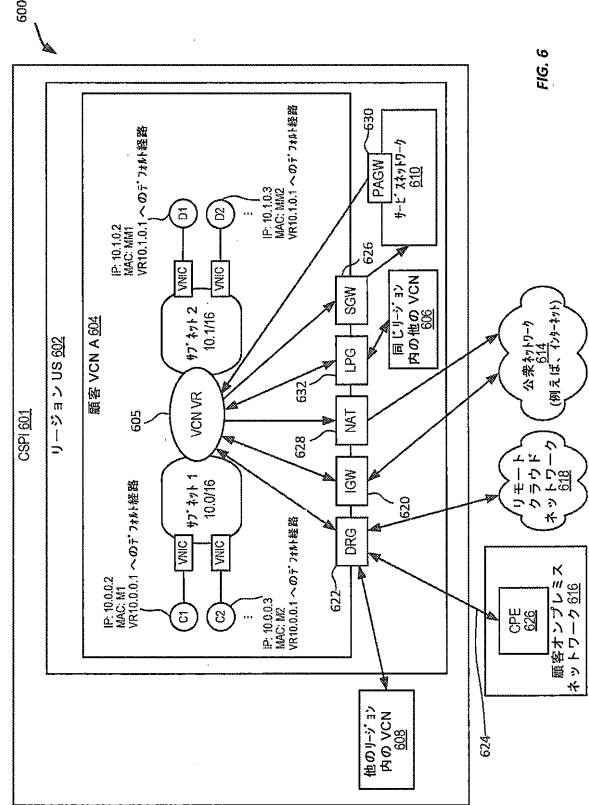


FIG. 6

【図 7】

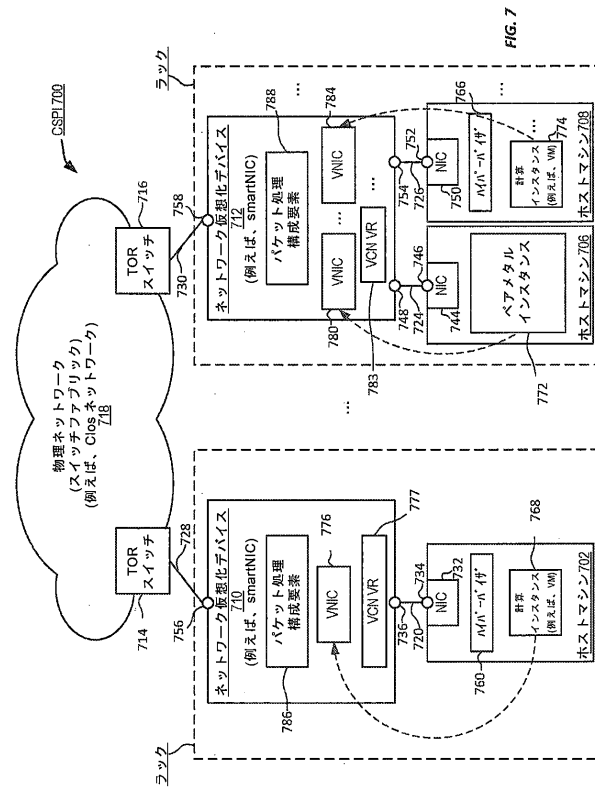


FIG. 7

【図 8】

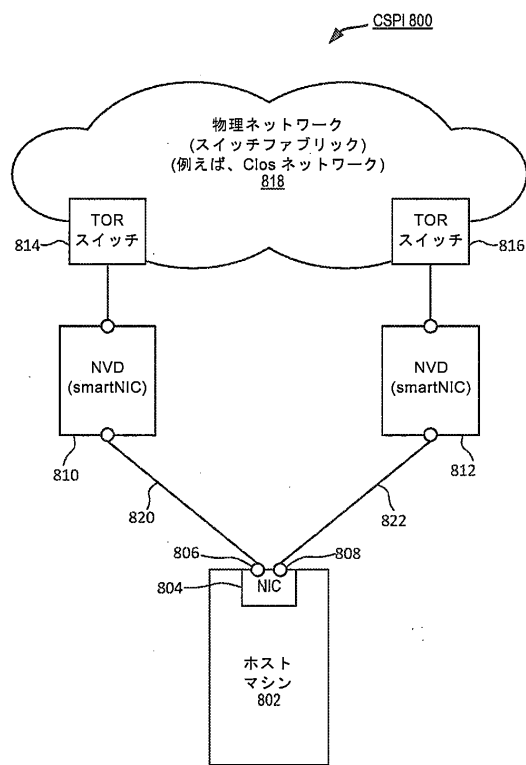


FIG. 8

【図 9】

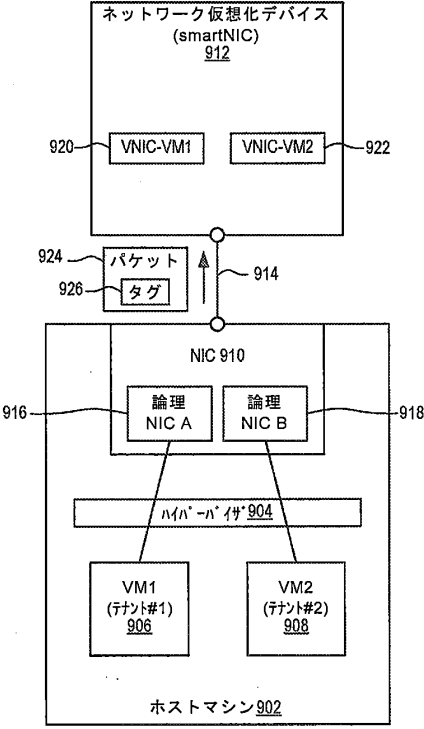


FIG. 9

【図 10】

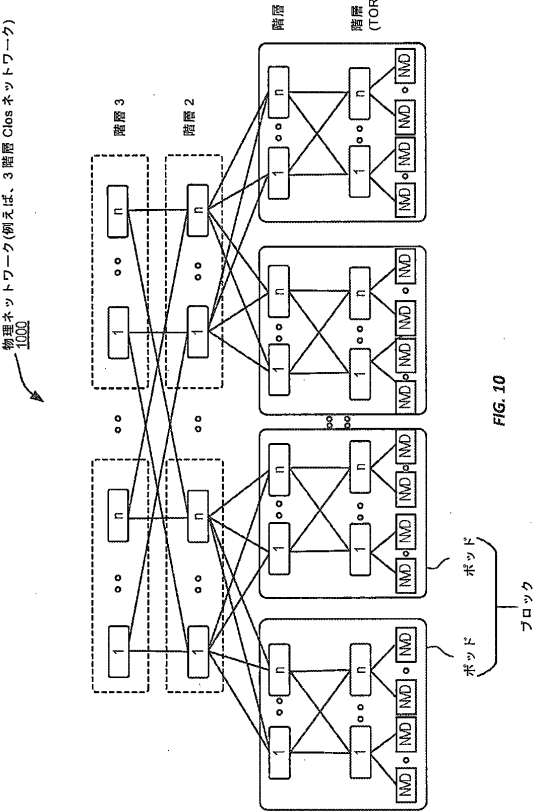


FIG. 10

【図 11】

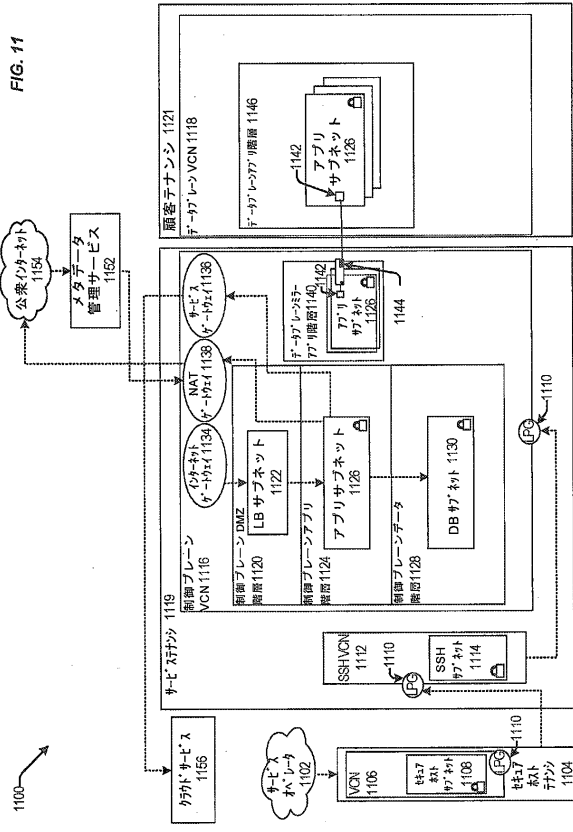


FIG. 11

【図 12】

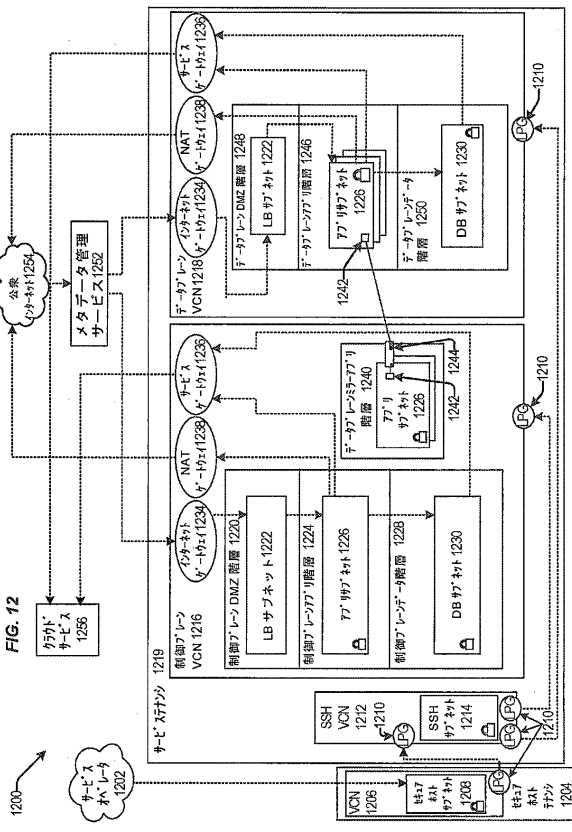


FIG. 12

10

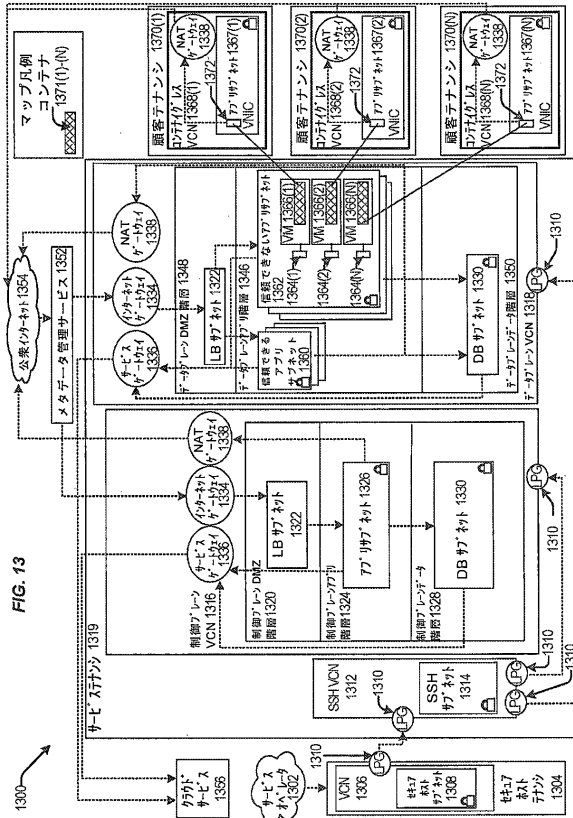
20

30

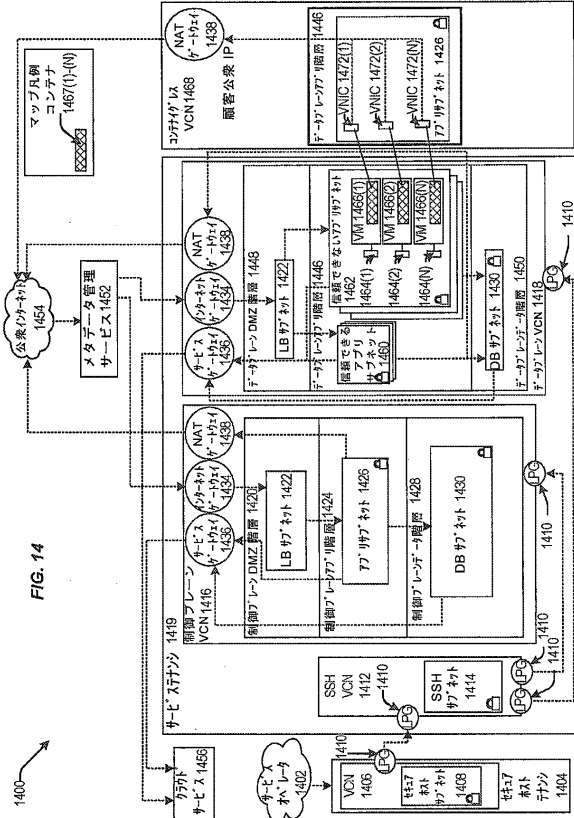
40

50

【図 13】



【圖 14】



【図 15】

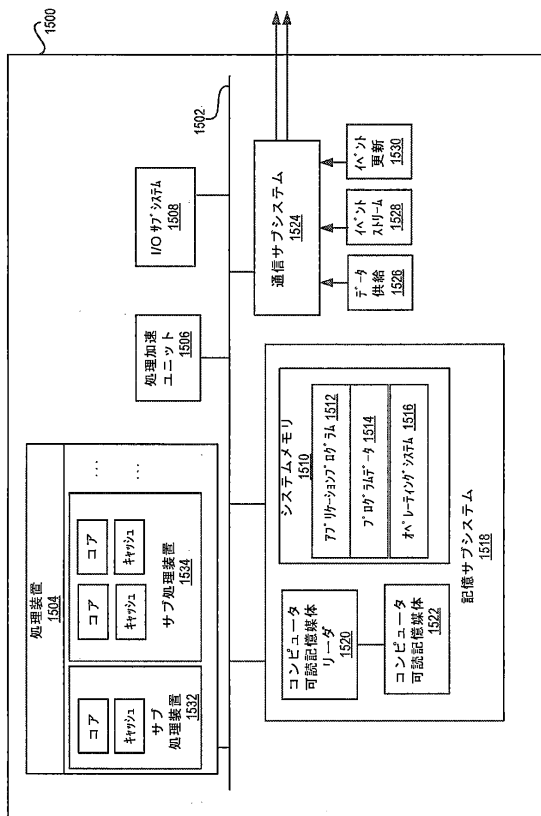


FIG. 15

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/034753

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/40 H04L45/00 G06F9/455 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/382471 A1 (JANAKIRAMAN RAJAGOPALAN [US] ET AL) 3 December 2020 (2020-12-03) paragraph [0001] - paragraph [0075] -----	1-21
X	US 2018/062920 A1 (SRINIVASAN ARAVIND [US] ET AL) 1 March 2018 (2018-03-01) paragraph [0002] - paragraph [0046] -----	1-21
X	US 2019/222559 A1 (WANG NAN [CN] ET AL) 18 July 2019 (2019-07-18) paragraph [0001] - paragraph [0031] -----	1, 12, 17, 21
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 15 September 2022		Date of mailing of the international search report 23/09/2022
Name and mailing address of the ISA/ European Patent Office, P.B. 5618 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Veshi, Erzim

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/034753

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

10

20

30

40

50

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,N
E,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,
CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,J
O,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,M
Z,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. i O S

ヨン

(72)発明者 カルケラ, アビマン・ヤシュパラ

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

(72)発明者 シャー, ドウワニッシュ・プラムテシュ

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

(72)発明者 ペイ, グアンホン

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

(72)発明者 マグウィルク, クレイトン・マシュー

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

(72)発明者 ケインカー, ポール・ジェイムズ

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