(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6891285号
(P6891285)
(45)発行日　令和3年6月18日(2021.6.18)　(24)登録日　令和3年5月28日(2021.5.28)

(51)Int.Cl.　F I
H04L 12/721 (2013.01)　H04L 12/721　Z
H04L 12/70 (2013.01)　H04L 12/70　D

請求項の数 18　(全 23 頁)

(21)出願番号　特願2019-540377(P2019-540377)
(86)(22)出願日　平成30年1月25日(2018.1.25)
(65)公表番号　特表2020-505856(P2020-505856A)
(43)公表日　令和2年2月20日(2020.2.20)
(86)国際出願番号　PCT/US2018/015228
(87)国際公開番号　WO2018/144314
(87)国際公開日　平成30年8月9日(2018.8.9)
審査請求日　令和1年9月3日(2019.9.3)
(31)優先権主張番号　15/422,076
(32)優先日　平成29年2月1日(2017.2.1)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　506329306
アマゾン　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　100106541
弁理士　伊藤　信和
(72)発明者　ハシミ　オマール
アメリカ合衆国　９８１０９－５２１０
ワシントン州　シアトル　テリー　アヴェニュー　ノース　４１０

審査官　大石　博見

最終頁に続く

(54)【発明の名称】仮想プライベートゲートウェイでのサービスエンドポイント相互接続

(57)【特許請求の範囲】
【請求項１】
プロセッサに結合されたメモリを含む仮想プライベートゲートウェイ（ＶＧＷ）プロビジョニングサービスであって、前記メモリが、実行時に前記ＶＧＷプロビジョニングサービスに、
サービスプロバイダの顧客からＶＧＷを確立する要求を受信することであって、前記要求が、前記ＶＧＷを通じてアクセス可能で且つ前記サービスプロバイダから前記顧客に提供されるサービスと顧客設定可能ポリシーとを指定し、前記顧客設定可能ポリシーが、前記指定されたサービスへのアクセスを、前記指定されたサービスに前記ＶＧＷを介して送信された要求に制限する、前記ＶＧＷを確立する要求を受信すること、
前記要求に応じて、演算デバイス上でＶＧＷ仮想マシンをインスタンス化することであって、前記ＶＧＷ仮想マシンが、パブリックネットワークを経由してリモートノードへのセキュアトンネルを確立し、前記セキュアトンネルを経由して前記リモートノードから暗号化されたトラフィックを受信するように構成されたＶＧＷアプリケーションを含む、前記ＶＧＷ仮想マシンをインスタンス化すること、
前記ＶＧＷ仮想マシンに前記指定されたサービスの経路データが提供されるようにすることであって、前記ＶＧＷアプリケーションが、実行時に、前記指定されたサービスの前記経路データを、前記セキュアトンネル経由で前記ＶＧＷアプリケーションにアドバタイズさせる命令を含む、前記経路データが提供されるようにすること、及び
前記サービスが順守するように、前記指定されたサービスに前記顧客設定可能ポリシ

ーを提供すること、
を行わせる命令を含む、前記ＶＧＷプロビジョニングサービスを備えたシステム。
【請求項２】
前記ＶＧＷプロビジョニングサービスが、経路交換サービスへの経路要求の送信を通じて、前記指定されたサービスの前記経路データが前記ＶＧＷ仮想マシンに提供されるように構成され、
前記経路要求が、前記指定されたサービスを識別し、
前記経路交換サービスが、アプリケーションプログラミングインタフェース（ＡＰＩ）呼出しを前記顧客のＶＧＷに送信するように構成され、前記ＡＰＩ呼出しが前記経路データを含む、請求項１に記載のシステム。
【請求項３】
所与のサービスが、前記所与のサービスの経路データを更新することに応じて、前記サービスが、サービス経路リフレクタサービスにアクセス可能なデータベース内で前記所与のサービスに対応する経路レコードを更新し、
前記サービス経路リフレクタサービスが、前記更新された経路データをＶＧＷ経路リフレクタサービスに送信し、
前記サービス経路リフレクタサービスが、前記所与のサービスの経路データを含むメッセージを各ＶＧＷに送信し、前記メッセージが、前記更新された経路データを含む、請求項１に記載のシステム。
【請求項４】
前記ＶＧＷアプリケーションはさらに、実行時に、前記ＶＧＷアプリケーションが前記セキュアトンネルを介してリモートノードから暗号化されたパケットを受信することであって、前記暗号化されたパケットは、前記指定されたサービスのサービス要求を含む、前記受信することに応じて、前記ＶＧＷアプリケーションに、
前記暗号化されたパケットを復号化して前記サービス要求を取得すること、
前記サービス要求のヘッダー内の情報を使用して、経路表にアクセスし、前記サービス要求の対象となる前記サービスへの経路を判定すること、及び
前記判定された経路を介して、前記要求の対象となる前記サービスに前記サービス要求を転送すること、
を行わせる命令を含み、
前記サービスが、前記サービス要求を実行するように構成されている、請求項１に記載のシステム。
【請求項５】
プロセッサに結合されたメモリを含む仮想プライベートゲートウェイ（ＶＧＷ）プロビジョニングサービスであって、前記メモリが、実行時に前記ＶＧＷプロビジョニングサービスに、
ＶＧＷを確立するため、前記ＶＧＷを通じてアクセス可能で且つサービスプロバイダから顧客に提供されるサービスを指定する要求を受信すること、
前記要求に応じて、演算デバイス上でＶＧＷ仮想マシンをインスタンス化することであって、前記ＶＧＷ仮想マシンが、パブリックネットワークを経由してリモートノードへのセキュアトンネルを確立し、前記セキュアトンネルを経由して前記リモートノードから暗号化されたトラフィックを受信するように構成されたＶＧＷアプリケーションを含む、前記ＶＧＷ仮想マシンをインスタンス化すること、及び
前記指定されたサービスの経路データが、前記ＶＧＷ仮想マシンに提供されるようにすること
を行わせる命令を含む、前記ＶＧＷプロビジョニングサービスを備えたシステム。
【請求項６】
前記サービスの前記経路データが、前記指定されたサービスのパブリックインターネットプロトコル（ＩＰ）アドレスを含み、
前記ＶＧＷアプリケーションが、パブリックネットワークを経由して、前記パブリック

ＩＰアドレスをリモートノードにアドバタイズするように構成され、
前記サービスの更新されたパブリックインターネットプロトコル（ＩＰ）アドレスの生成が、
前記サービスに、前記更新されたパブリックＩＰアドレスを含む更新された経路データで経路交換サービスの経路エントリを更新させ、
前記経路交換サービスに、前記サービスの前記更新された経路データを前記ＶＧＷ仮想マシンへ送信させ、
前記ＶＧＷアプリケーションに、前記サービスの前記更新された経路データを前記リモートノードへアドバタイズさせる、請求項５に記載のシステム。
【請求項７】
前記ＶＧＷアプリケーションが、実行時に、前記セキュアトンネルを介したリモートノードからの暗号化パケットの受信と、前記暗号化パケットが、前記指定されたサービスのサービス要求を含むこととに応じて、前記ＶＧＷアプリケーションに、
前記暗号化されたパケットを復号化して前記サービス要求を取得すること、
前記サービス要求のヘッダー内の情報を使用して、経路表にアクセスし、前記サービス要求の対象となる前記サービスへの経路を判定すること、及び
前記判定された経路を介して、前記要求の対象となる前記サービスに前記サービス要求を転送すること
を行わせる命令をさらに含む、請求項５に記載のシステム。
【請求項８】
複数のサービスの経路データを含むように構成された経路表を含む経路交換サービスをさらに含み、
前記ＶＧＷプロビジョニングサービスが、前記経路交換サービスに要求を送信して、前記指定されたサービスの前記経路データを提供するように構成されている、請求項５に記載のシステム。
【請求項９】
前記要求が、前記指定されたサービスへのアクセスを制限するように構成された顧客設定可能ポリシーを含み、
前記ＶＧＷアプリケーションが、前記顧客設定可能ポリシーを受信し、前記顧客設定可能ポリシーを確実に順守するように構成されている、請求項５に記載のシステム。
【請求項１０】
プロセッサに結合されたメモリを含む仮想プライベートゲートウェイ（ＶＧＷ）プロビジョニングサービスの実行方法であって、前記メモリが、実行時に前記ＶＧＷプロビジョニングサービスに、
サービスプロバイダの顧客からＶＧＷを確立する要求を受信する工程であって、前記要求が、前記ＶＧＷを通じてアクセス可能で且つ前記サービスプロバイダから前記顧客に提供されるサービスと顧客設定可能ポリシーとを指定し、前記顧客設定可能ポリシーが、前記指定されたサービスへのアクセスを、前記指定されたサービスに前記ＶＧＷを介して送信された要求に制限する、前記ＶＧＷを確立する要求を受信する工程、
前記要求に応じて、演算デバイス上でＶＧＷ仮想マシンをインスタンス化する工程であって、前記ＶＧＷ仮想マシンが、パブリックネットワークを経由してリモートノードへのセキュアトンネルを確立し、前記セキュアトンネルを経由して前記リモートノードから暗号化されたトラフィックを受信するように構成されたＶＧＷアプリケーションを含む、前記ＶＧＷ仮想マシンをインスタンス化する工程、
前記ＶＧＷ仮想マシンに前記指定されたサービスの経路データが提供されるようにする工程であって、前記ＶＧＷアプリケーションが、実行時に、前記指定されたサービスの前記経路データを、前記セキュアトンネル経由で前記ＶＧＷアプリケーションにアドバタイズさせる命令を含む、前記経路データが提供されるようにする工程、及び
前記サービスが順守するように、前記指定されたサービスに前記顧客設定可能ポリシーを提供する工程、

を行わせる命令を含む、前記ＶＧＷプロビジョニングサービスの実行方法。
【請求項１１】
前記ＶＧＷプロビジョニングサービスが、経路交換サービスへの経路要求の送信を通じて、前記指定されたサービスの前記経路データが前記ＶＧＷ仮想マシンに提供されるように構成され、
前記経路要求が、前記指定されたサービスを識別し、
前記経路交換サービスが、アプリケーションプログラミングインタフェース（ＡＰＩ）呼出しを前記顧客のＶＧＷに送信するように構成され、前記ＡＰＩ呼出しが前記経路データを含む、請求項１０に記載の実行方法。
【請求項１２】
所与のサービスが、前記所与のサービスの経路データを更新することに応じて、前記サービスが、サービス経路リフレクタサービスにアクセス可能なデータベース内で前記所与のサービスに対応する経路レコードを更新し、
前記サービス経路リフレクタサービスが、前記更新された経路データをＶＧＷ経路リフレクタサービスに送信し、
前記サービス経路リフレクタサービスが、前記所与のサービスの経路データを含むメッセージを各ＶＧＷに送信し、前記メッセージが、前記更新された経路データを含む、請求項１０に記載の実行方法。
【請求項１３】
前記ＶＧＷアプリケーションはさらに、実行時に、前記ＶＧＷアプリケーションが前記セキュアトンネルを介してリモートノードから暗号化されたパケットを受信することであって、前記暗号化されたパケットは、前記指定されたサービスのサービス要求を含む、前記受信することに応じて、前記ＶＧＷアプリケーションに、
前記暗号化されたパケットを復号化して前記サービス要求を取得する工程、
前記サービス要求のヘッダー内の情報を使用して、経路表にアクセスし、前記サービス要求の対象となる前記サービスへの経路を判定する工程、及び
前記判定された経路を介して、前記要求の対象となる前記サービスに前記サービス要求を転送する工程、
を行わせる命令を含み、
前記サービスが、前記サービス要求を実行するように構成されている、請求項１０に記載の実行方法。
【請求項１４】
プロセッサに結合されたメモリを含む仮想プライベートゲートウェイ（ＶＧＷ）プロビジョニングサービスの実行方法であって、前記メモリが、実行時に前記ＶＧＷプロビジョニングサービスに、
ＶＧＷを確立するため、前記ＶＧＷを通じてアクセス可能で且つサービスプロバイダから顧客に提供されるサービスを指定する要求を受信する工程、
前記要求に応じて、演算デバイス上でＶＧＷ仮想マシンをインスタンス化することであって、前記ＶＧＷ仮想マシンが、パブリックネットワークを経由してリモートノードへのセキュアトンネルを確立し、前記セキュアトンネルを経由して前記リモートノードから暗号化されたトラフィックを受信するように構成されたＶＧＷアプリケーションを含む、前記ＶＧＷ仮想マシンをインスタンス化する工程、及び
前記指定されたサービスの経路データが、前記ＶＧＷ仮想マシンに提供されるようにする工程
を行わせる命令を含む、前記ＶＧＷプロビジョニングサービスの実行方法。
【請求項１５】
前記サービスの前記経路データが、前記指定されたサービスのパブリックインターネットプロトコル（ＩＰ）アドレスを含み、
前記ＶＧＷアプリケーションが、パブリックネットワークを経由して、前記パブリックＩＰアドレスをリモートノードにアドバタイズするように構成され、

前記サービスの更新されたパブリックインターネットプロトコル（ＩＰ）アドレスの生成が、

前記サービスに、前記更新されたパブリックＩＰアドレスを含む更新された経路データで経路交換サービスの経路エントリを更新させ、

前記経路交換サービスに、前記サービスの前記更新された経路データを前記ＶＧＷ仮想マシンへ送信させ、

前記ＶＧＷアプリケーションに、前記サービスの前記更新された経路データを前記リモートノードへアドバタイズさせる、請求項１４に記載の実行方法。

【請求項１６】

前記ＶＧＷアプリケーションが、実行時に、前記セキュアトンネルを介したリモートノードからの暗号化パケットの受信と、前記暗号化パケットが、前記指定されたサービスのサービス要求を含むこととに応じて、前記ＶＧＷアプリケーションに、

前記暗号化されたパケットを復号化して前記サービス要求を取得する工程、

前記サービス要求のヘッダー内の情報を使用して、経路表にアクセスし、前記サービス要求の対象となる前記サービスへの経路を判定する工程、及び

前記判定された経路を介して、前記要求の対象となる前記サービスに前記サービス要求を転送する工程

を行わせる命令をさらに含む、請求項１４に記載の実行方法。

【請求項１７】

複数のサービスの経路データを含むように構成された経路表を含む経路交換サービスをさらに含み、

前記ＶＧＷプロビジョニングサービスが、前記経路交換サービスに要求を送信して、前記指定されたサービスの前記経路データを提供するように構成されている、請求項１４に記載の実行方法。

【請求項１８】

前記要求が、前記指定されたサービスへのアクセスを制限するように構成された顧客設定可能ポリシーを含み、

前記ＶＧＷアプリケーションが、前記顧客設定可能ポリシーを受信し、前記顧客設定可能ポリシーを確実に順守するように構成されている、請求項１４に記載の実行方法。

【発明の詳細な説明】

【背景技術】

【０００１】

パブリックサービスプロバイダは、顧客が使用可能なハードウェアデバイス（例えば、サーバ、ストレージドライブなど）及びサービスを提供し、それによって顧客がそのような設備を所有して運用する必要をなくす。一部のサービスプロバイダは、顧客にサービスを各種取り合わせて提供しており、顧客は、パブリックネットワーク越しに顧客自身のデバイスからこれらのサービスにアクセスする。顧客デバイスとプロバイダネットワークとの間の通信は、インターネットなどのパブリックネットワークを通じて行われ、暗号化されない場合がある。

【０００２】

様々な例を詳細に説明するために、ここで添付の図面を参照する。

【図面の簡単な説明】

【０００３】

【図１】様々な例によるシステムを示す図である。

【図２】様々な例によるサービスの経路データを更新するための実施形態を示す図である。

【図３】様々な例による仮想プライベートゲートウェイを作成する方法を示す図である。

【図４】様々な例による仮想プライベートゲートウェイによって実行される方法を示す図である。

【図５】経路データを更新し、更新した経路データを仮想プライベートゲートウェイ及び

ピア接続されたリモートノードに配布する方法を示す図である。
【図６】様々な例による計算デバイスのブロック図である。
【発明を実施するための形態】
【０００４】
本明細書に記載されている実施形態は、プロバイダネットワークを具体的に説明するものである。このプロバイダネットワークは、顧客のそれぞれが仮想プライベートゲートウェイ（ＶＧＷ）を作成し使用して、顧客のリモートノード（すなわち、プロバイダネットワークからリモートのノード）とＶＧＷとの間にセキュアな（例えば、暗号化された）トンネルを確立することを可能にする。顧客は、暗号化トンネルを使用して、プロバイダネットワーク内で実行されるサービス（例えば、ストレージサービス）を求めて要求を送信できる。顧客は、リモートノードから、プロバイダネットワークホスト型サービス向けの要求を暗号化するか、または暗号化させることができる。暗号化されたパケットは、セキュアトンネルを経由してＶＧＷに伝送される。ＶＧＷは、例えば、仮想マシン内で実行されるアプリケーションとして実装してもよく、仮想マシン自体は、プロバイダネットワーク内のサーバなどの演算デバイス上で実行される。このアプリケーションは、本明細書に記載されているＶＧＷによる機能を実行できる。ＶＧＷは、サービスエンドポイントとして動作し、パケットを復号化してサービス要求を復元する。ＶＧＷは、サービス要求を対象サービスが実行されるサーバに配信するために、経路表内の対象サービスの経路データを使用して、サービスプロバイダの内部ネットワークを通じてサービス要求を転送する。その後、サービスがサービス要求を実行し得る。リモートノードに送り返すべき、サービスによって生成された全ての応答パケットは、ＶＧＷに返送され、次いでＶＧＷはパケットを暗号化し、暗号化したパケットをトンネル経由でリモートノードに伝送する。したがって、顧客は、サービスと関連したパブリックインターネットプロトコル（ＩＰ）アドレスにサービス要求を送信することによってではなく、ＶＧＷへの専用暗号化トンネルを通じてサービスにアクセスすることができる。
【０００５】
いくつかの実施形態では、プロバイダネットワークは、顧客がＶＧＷの作成の要求を送信することができるＶＧＷプロビジョニングサービスを含み得る。プロビジョニングサービスは、所与の顧客のＶＧＷを作成する要求を受信すると、ＶＧＷ仮想マシンをロードして実行するサーバを選択する。ＶＧＷ仮想マシンは、ＶＧＷの機能を実装する上記のアプリケーションを含むマシンイメージを備えてもよい。ＶＧＷを作成する要求には、顧客が暗号化トンネルを通じたアクセスを希望する１つ以上のサービスの識別子が含まれる場合もある。
【０００６】
いくつかの実施形態では、ＶＧＷは、ＶＧＷによって受信された着信パケットをどこに送信すべきかをＶＧＷが判定するのを容易にする経路データを収めた経路表を含み得る。顧客のＶＧＷを経由してアクセスできるように顧客が指定したサービス（複数可）は、プレフィックスリスト識別子及び対応するサービスの正規名を含むプレフィックスリストなどの経路データを生成することができる。プレフィックスリスト識別子は、サービス用のパブリックＩＰアドレスの範囲を論理的に表し得るものである。プレフィックスリストに加えて他の形式の経路データも可能である。プロバイダネットワークは、経路交換サービスを実装し得る。この経路交換サービスは、サービスが、ＶＧＷに再配布すべきそれらの経路データを提供し更新できるようにする。ＶＧＷは、そのような各サービスにアクセスするように構成されている。ＶＧＷの作成後、ＶＧＷプロビジョニングサービスは、経路交換サービスに要求を送信することができる。要求は、ＶＧＷがどのサービス（複数可）にアクセスするように構成されるべきかを指定し、経路交換サービスは、指定されたサービスの経路データをＶＧＷに提供し得、次いでＶＧＷが、その経路表にそのような経路データを追加する。
【０００７】
各顧客がプロビジョニングサービスにアクセスして、顧客が顧客自身のＶＧＷを介して

アクセス可能であるように指定した所与のサービスに対するポリシーを作成することもできる。一例では、ポリシーは、ＶＧＷを通る（したがって、ＶＧＷへの暗号化トンネルを通る）サービス要求のみがサービスによって受け入れられるということを指定できる。他の種類のポリシーも可能である。ポリシーは、対応するサービスに提供され、それらのサービスによって実装され得る。

【０００８】

図１は、複数のサーバ（例えば、サーバ１１０及び１６０）、複数のサービス１３０、ＶＧＷプロビジョニングサービス１４０、及び経路交換サービス１５０を含むプロバイダネットワーク１００の例を示す。仮想マシン（ＶＭ）１６５が、プロバイダネットワークの顧客の代理としてサーバ１６０にインストールされ実行され得る。顧客は、１つ以上の仮想マシン１６５を有する場合があり、顧客のニーズ（例えば、企業の業務アプリケーション）をサポートするために、これらの各仮想マシン内で実行される顧客固有のソフトウェアを有し得る。プロバイダネットワーク内の演算エンティティとリモートノード（例えば、リモートノード８０など）との間に、パブリックネットワークを介して通信が確立され得る。図１の例では、ネットワーク９０を介したリモートノード８０への通信接続性が示されている。ネットワーク９０は、パブリックネットワーク（例えば、インターネット）を含み、ワイドエリアネットワーク、ローカルエリアネットワーク、有線ネットワーク、無線ネットワークなどのいずれか１つ以上を含んでもよい。

【０００９】

リモートノード８０は、単一のコンピュータまたは互いにネットワークで結ばれたコンピュータの一群を含んでもよい。いくつかの実施形態では、リモートノード８０は、顧客のデータセンター内のゲートウェイを含んだものであってもよく、またはデータセンター自体であってもよい。リモートノード８０を使用して、ＶＧＷプロビジョニングサービス１４０にアクセスし、それによって顧客向けにＶＧＷが作成されるように要求することができる。所与の顧客向けのＶＧＷ１０５の実装の例を、ＶＧＷアプリケーション１２０がインストールされ実行されているサーバ１１０として図１に示す。リモートノード８０を使用して、またはリモートノード８０によってＶＧＷ１０５が作成されると、顧客は、以下に説明するように、ＶＧＷへのセキュアトンネル９０を確立することができる。

【００１０】

ＶＧＷアプリケーション１２０は仮想マシン１１５内で実行され、仮想マシン１１５自体はサーバ１１０上で実行され得る。同様に、顧客固有のアプリケーション１７０が実行され得る仮想マシン１６５を実行するために、サーバ１６０を使用することができる。さらに、サービス１３０（例えば、サービスＡ、サービスＢ、・・・、サービスｎ）のいずれか１つ以上、及びＶＧＷプロビジョニングサービス１４０は、物理サーバ上で実行される仮想マシン内で実行されるアプリケーションを備え得る。したがって、プロバイダネットワーク１００は、様々な用途のためにサーバ上で仮想マシンを起動して実行するように構成されている。

【００１１】

仮想マシンは、物理コンピュータシステムのソフトウェア実装である。仮想マシンは、単一のホストコンピュータで同時に実行するように、複数のオペレーティングシステム環境及び／または異なるオペレーティングシステム環境を提供し得る。一例では、Ｌｉｎｕｘ（登録商標）オペレーティングシステム環境の複数の仮想マシンが、単一の物理コンピュータ上でＭｉｃｒｏｓｏｆｔ（登録商標）Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステム環境の複数のインスタンスと同時に実行され得る。仮想マシンは、複数のゲストオペレーティングシステムが単一のハードウェアホストを共有できるようにする、物理コンピュータ上で実行されるプログラムであるハイパーバイザまたは仮想マシンモニタ（または他の種類の仮想化システム）と対話することができる。各仮想マシンのオペレーティングシステムは、ホストのプロセッサ、メモリ、及びその他のリソースに排他的にアクセスできるように見える。また一方、ハイパーバイザはホストプロセッサ及びリソースを制御して、各仮想マシンのオペレーティングシステムに必要なリソースを順に割り当てる

とともに、仮想マシンのゲストオペレーティングシステムが相互に妨害しないようにする。各仮想マシンを、それぞれの顧客が制御することができる。顧客が作成した仮想マシン（例えば、仮想マシン１６５）は、顧客がそのように選択した顧客固有の任意のアプリケーションと共に、顧客がロードすることができる。例えば、顧客のアプリケーションは、ウェブサーバアプリケーション、データ処理アプリケーション、または顧客が望むその他のあらゆる種類の機能を含み得る。仮想マシン内で実行されるアプリケーションは、そのような仮想マシンの起動に使用されるマシンイメージに予め格納されていてもよく、プロビジョニングサービスによる起動後に仮想マシンにロードされてもよい。

【００１２】

引き続き図１を参照すると、サービス１３０は、サービスプロバイダによってその顧客に提供される無数のサービスを含み得る。ある例では、サービス１３０がストレージサービスを含む場合があり、このストレージサービスは、顧客が大容量記憶の割り当てを要求し、顧客のリモートノードから顧客の記憶域割り当てにデータを格納させるようにすることができる。それ以降、データの一部または全部をストレージから取り出し、リモートノードに提供することができる。別の例では、サービスがデータベースサービスを提供する場合がある。一実施形態では、このデータベースサービスは、プロバイダネットワークの顧客による使用のために、柔軟な非リレーショナルデータベースを提供する場合がある。データベースは、ドキュメントストレージモデル及びキーバリューストレージモデルをサポートし得る。別の例では、サービスにより、顧客が実行可能コードをアップロードし、顧客が指定したトリガイベントの発生時にそのコードをプロバイダネットワークによって自動的に実行させることができる。トリガイベントが発生すると（例えば、写真がシステムにアップロードされたり、センサの制限を超えることなど）、顧客固有のコードが実行されるが、そのようなコードを実行する仮想マシンをプロビジョニングして管理する必要はない。サービス１３０のいずれか、または全ては、仮想マシンを使用せずに、対応するアプリケーションを実行するサーバとして実装してもよいが、他の実施形態では、サービスのいずれかは、上記の仮想マシン内で実行することができるソフトウェアを含んでもよい。

【００１３】

いくつかの実施形態では、各サービス１３０は、パブリックＩＰアドレス公開サービス１３３によってアドバタイズされるパブリックＩＰアドレス（またはＩＰアドレスの範囲）を有し得る。各サービス１３０を、パブリックＩＰアドレス公開サービス１３３の別個の対応するインスタンシエーションに関連付けてもよく、または複数のサービス１３０が共通のパブリックＩＰアドレス公開サービス１３３を使用してもよい。所与のサービス１３０のパブリックＩＰアドレスは、パブリックネットワーク９０を経由してアドバタイズされ、それによってリモートデバイスがパブリックＩＰアドレスを含むサービス要求を送信できるようになり得る。場合によっては、ドメインネームサービス（ＤＮＳ）がサービスのパブリックＩＰアドレスを受信して格納し、リモートノードからのＤＮＳ要求に応じて、サービス名（例えば、ユニフォームリソースロケータ）をサービスのパブリックＩＰアドレスに解決してもよい。

【００１４】

また一方、プロバイダネットワークの顧客は、対象サービスのパブリックＩＰアドレスに要求を送信するのではなく、サービス（複数可）を使用するためにプロバイダネットワークに要求を送信する目的で、セキュアトンネルを介して１つ以上のサービス１３０を使用し、プロバイダネットワーク１００への通信リンクを確立することを望む場合がある。図１の例では、リモートノード８０と顧客のために作成されたＶＧＷ１０５との間に確立されたセキュアトンネル９２が示されている。上記のように、ＶＧＷは、仮想マシン１１５を実行するサーバ１１０として実装してもよく、この仮想マシン１１５はＶＧＷアプリケーション１２０を実行する。ＶＧＷアプリケーション１２０は、顧客のＶＧＷに起因するものとして本明細書に記載されている機能を実装する。いくつかの実施形態では、セキュアトンネル９２は、トンネルに沿って往復して伝送されるデータパケットが暗号化され

ることを意味する暗号化されたトンネルである。すなわち、トンネルの送信元端によって暗号化され、宛先端によって復号化されることを意味する。トンネル９２は双方向トンネルであり得るので、ＶＧＷ１０５は、リモートノード８０からの着信暗号化パケットを復号化し、トンネル９２を介してリモートノードへ送信するために発信パケットを暗号化することができる。同様に、リモートノード８０は、ＶＧＷ１０５からの着信暗号化パケットを復号化し、トンネルを介してＶＧＷへ送信するために発信パケットを暗号化することができる。

【００１５】

上記のようにサービスの経路データを受信した顧客のＶＧＷ１０５は、サービスのパブリックアドレスをＶＧＷの識別子と共に顧客のリモートノード８０にアドバタイズする。その時点で、リモートノード８０は、リモートノード８０がサービス１３０に対するアクセス要求を生成する場合に、その経路情報は、サービスのパブリックＩＰアドレスを使用して生成すべきパケットが、代わりにＶＧＷのＩＰアドレスを宛先アドレスとして使用して作成されることを要するように構成されている。したがって、サービス要求パケットは、サービス自体のパブリックＩＰアドレスにではなく、ＶＧＷにセキュアトンネル９２を介して送信される。そのため、サービス１３０は、少なくとも２通りでアクセス可能であり得る。ＶＧＷのＩＰアドレスを宛先アドレスとして含み、セキュアトンネル９２を介して送信され、ＶＧＷ１０５によってサービスにルーティングされるパケットによって、またはサービスのパブリックＩＰアドレスを宛先アドレスとして含むパケットによってである。

【００１６】

いくつかの実装では、トンネル９２はインターネットプロトコルセキュリティ（ＩＰＳｅｃ）規格を用いて実装されてもよく、トンネルの両端（すなわち、ＶＧＷ１０５及びリモートノード８０）は、ノード間のセキュリティアソシエーションの確立を促進するために、インターネットキー交換（ＩＫＥ）プロトコルを実行してもよい。ＩＫＥプロトコルには、フェーズＩとフェーズＩＩの２つのフェーズが含まれる。フェーズＩでは、プロトコルは、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎキー交換アルゴリズムを使用してセキュアな認証済み通信チャネルを確立し、さらにＩＫＥ通信を暗号化するための共有秘密キーを生成する。認証は、事前共有秘密キー、デジタル署名、または公開キー暗号化を使用して実行できる。フェーズＩＩの間中、２つのＩＫＥピアは、フェーズＩで確立されたセキュアチャネルを使用して、インターネットプロトコルセキュリティ（ＩＰＳｅｃ）などの他のサービスに代わってセキュリティアソシエーションをネゴシエートする。このネゴシエーションにより、２つの単方向セキュリティアソシエーションが作成される。１つのインバウンド、及び１つのアウトバウンドである。各セキュリティアソシエーションには、パケットの暗号化／復号化に使用される暗号化キーが含まれる。Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ暗号化キー及びＩＰＳｅｃ暗号化キーは、ＩＫＥプロトコルのフェーズＩ動作及びフェーズＩＩ動作のいずれかまたは両方を実行することによって、セキュリティを強化するために、定期的にローテーションされる。リモートノード８０によって生成され暗号化されたパケットは、サービス１３０のいずれかの使用を求める要求を含み得る。したがって、開示される実施形態は、顧客が暗号化トンネルを介してＶＧＷ１０５にサービス要求を送信することを可能にする。ＶＧＷは着信パケットを復号化し、サービス要求を対象サービスに転送する。

【００１７】

上記のように、顧客は、ＶＧＷプロビジョニングサービス１４０にアクセスして、顧客による排他的使用のためにＶＧＷ１０５が作成され割り当てられるように要求することができる。要求は、例えば、アプリケーションプログラミングインターフェース（ＡＰＩ）呼出しの形式でＶＧＷプロビジョニングサービス１４０に送信されてもよい。ＡＰＩ呼出しは、顧客が実行を希望するアクションを指定する正規名であり得る。例えば、ＡＰＩ呼出しは、「ＶＧＷＣｒｅａｔｅ（）」を含み得、ここで括弧の間に挿入すべき値は、所望のＶＧＷ１０５の様々な特性を指定する。例えば、顧客は、顧客がＶＧＷを介してアクセ

スすることを望む各サービス１３０の識別子、顧客または顧客アカウントの識別子、要求を認証するために使用されるクレデンシャル情報、ＶＧＷがトンネルを確立しようとするリモートノード８０のパブリックＩＰアドレスなどを含み得る。

【００１８】

要求に応じて、ＶＧＷプロビジョニングサービス１４０は、ＶＧＷに使用するために、複数の利用可能なサーバの中から、物理サーバ１１０を選択することができる。選択したサーバは、現在、別のアプリケーションまたはＶＧＷを実行している場合があり、または実行していない場合がある。ＶＧＷプロビジョニングサービス１４０は、選択されたサーバ１１０にマシンイメージをダウンロードさせる。一実施形態では、特定のマシンイメージを、マシンイメージストレージ（図示せず）から取得し、選択したホストコンピュータに送信することができる。マシンイメージは、パケットの暗号化及び復号化、トンネル９２のための暗号化キーのローテーション、リモートノード８０から対象サービス１３０へのパケットのルーティングなどのＶＧＷ機能の一部または全部を実装するように構成されたオペレーティングシステム、ドライバ、及びＶＧＷアプリケーション１２０を含み得る。適切なマシンイメージがホストサーバのストレージドライブに伝送され、ロードされる。マシンイメージは、プロバイダネットワーク内の集中型データベースまたはデータストアに格納され得る。ＶＧＷベースのマシンイメージ、及び顧客が他種の仮想マシンを起動するのに使用できる他種のマシンイメージを含む各マシンイメージは、予め割り当てられた識別子（ＩＤ）を有し得る。このＩＤは、ＶＧＷプロビジョニングサービスが物理サーバ上で仮想マシンをＶＧＷ１０５として起動するために使用することができる。ＶＧＷプロビジョニングサービス１４０は、ＶＧＷ機能を実装するのに必要なマシンイメージに関連付けられたＩＤを使用して、ＶＧＷ仮想マシンを起動する選択されたサーバにコピーするためのマシンイメージを選択する。ＶＧＷプロビジョニングサービス１４０、または別個のプロビジョニングサービスはまた、同様の動作を実行して、顧客がアプリケーションを実行するために使用する仮想マシン１６５、及びサービス１３０など、プロバイダネットワーク内の他の仮想マシンを起動することができる。

【００１９】

ＶＧＷ機能を提供するために作成される仮想マシン１１５はまた、経路表１２５を含むことができる。経路表１２５は、着信パケットをどのようにルーティングするかを決定するのに使用可能なデータを含む１つ以上のエントリを含み得る。例えば、顧客がリモートノード８０からＶＧＷを通じてアクセスされることを識別した各サービス１３０に対応する経路表１２５に、別個のエントリを追加してもよい。所与の経路表エントリに含まれる経路データには、例えば、宛先値、対象値、及び「ネクストホップ」ＩＰアドレスが含まれ得る。宛先値はサービスのパブリックＩＰアドレスの範囲を含んでもよく、対象値はＶＧＷ１０５の識別子を含んでもよい。ネクストホップＩＰアドレスには、サービスのためのパケットが送信されるプロバイダネットワーク内のネットワーキングエンティティのＩＰアドレスが含まれる。ネクストホップアドレスによって識別されるネットワーキングエンティティは、プロバイダネットワーク内のサービスのローカルネットワーク用のエッジルータを含んでもよい。エッジルータがパケットを受信すると、サービスのエッジルータは、パケットに含まれるサービス要求を実行するために、そのパケットをサービスのローカルネットワーク内の適切なサーバに転送することができる。各経路表エントリに、異種及び／または別種の経路データが含まれていてもよい。

【００２０】

経路交換サービス１５０は、各サービス１３０の経路データを格納することができ、そのような経路データを、そのようなサービスにアクセスするように顧客によって指定されたＶＧＷに提供することができる。そのような経路データは、ＶＧＷが着信パケットをパケットの対象とされたサービスにどのように転送すべきかを指定する。そのような経路データの一例が上に記載されている。所与のサービスの経路データは、そのサービスによって変更される場合がある。例えば、所与のサービスの使用率が、そのサービスのアプリケーションを実行するために、サーバ及び／または仮想マシンを追加することによって、プ

ロバイダネットワークがサービスをスケールアップし得る程度にまで、増加する可能性がある。さらに、サービスを実装するサーバの保守は、サービスへの経路データの変更を必要とする可能性がある。所与のサービスの経路データを変更する理由にかかわらず、サービスのアプリケーションを実行しているサーバ及び仮想マシンにアクセスするパケットの経路データを、変更し、拡張し、及び／または削減する必要がある場合がある。

【００２１】

図２は、経路交換サービス１５０の一実施形態を示す。この実施形態では、経路交換サービス１５０は、サービス経路リフレクタサービス１５１及びＶＧＷ経路リフレクタサービス１５３を含み得る。経路リフレクタ１５１、１５３は、サーバ上で実行されるマシンコードとして実装されてもよい。各経路リフレクタ１５１、１５３は、他の経路リフレクタから利用可能な経路を学習するように構成されている。各サービス１３０が、別個のサービス経路リフレクタサービス１５１と通信してもよく、または複数のサービス１３０が単一のサービス経路リフレクタサービス１５１を使用してもよい。単一のＶＧＷ経路リフレクタサービス１５３が、複数もしくは全てのＶＧＷ１０５に関連付けられてもよく、または個々のＶＧＷが、ＶＧＷ経路リフレクタサービス１５３の別個のインスタンスに関連付けられてもよい。

【００２２】

所与のサービス１３０がその経路データを更新すると、そのサービスは、更新した経路データをサービス経路リフレクタサービス１５３に提供することができる。サービス経路リフレクタサービス１５１は、更新された経路データをＶＧＷ経路リフレクタサービス１５３に提供することによって応じてもよい。いくつかの実施形態では、経路交換サービス１５０は、ボーダゲートウェイプロトコル（ＢＧＰ）を実装してもよい。ＢＧＰは、ネットワーク上のノード間でルーティング情報及び到達可能性情報の交換を可能にする。ＢＧＰを使用して、経路リフレクタサービス１５１及び１５３は、サービス１３０の更新された経路データの交換に従事する。他の実施形態では、サービス経路リフレクタサービス１５１はＢＧＰを実装せず、代わりにＡＰＩ呼出しをＶＧＷ経路リフレクタサービス１５３に送る。ＡＰＩの引数は、更新された経路データを含むか、またはそのようなデータがＶＧＷ経路リフレクタサービス１５３によってどこで取得され得るかの参照を含み得る。ＡＰＩ呼出しには、経路データを追加するためのＡＰＩ呼出し、経路データを削除するためのＡＰＩ呼出しなどが含まれる。ＶＧＷ経路リフレクタサービス１５３が更新された経路データを受信すると、ＶＧＷ経路リフレクタサービス１５３は、経路データが更新されているサービス１３０にアクセスするように構成されている各ＶＧＷ１０５にＡＰＩ呼出しを送信することができる。無論、他の実施形態では、第２のシステムまたはサービスにＡＰＩ呼出しを送信するものとして記載されるシステムまたはサービスが、代わりに、その第２のシステムまたはサービスからＡＰＩ呼出しを受信するように構成され得るように、本システムを構成することができる。その後、更新された経路データは、そのような各ＶＧＷ１０５の経路表１２５に追加される。

【００２３】

再び図１を参照すると、顧客によってＶＧＷが作成されると、ＶＧＷプロビジョニングサービス１４０は、顧客がＶＧＷによってアクセス可能である１つ以上の特定のサービス１３０を指定した場合に、経路交換サービス１５０に要求（例えば、ＡＰＩ呼出し）を送信してもよい。要求は、ＶＧＷを識別することができ、識別されたＶＧＷが経路データを必要とするサービス（複数可）を指定することができる。その場合に、経路交換サービス１５０は、ＶＧＷの経路表１２５に追加すべき識別されたＶＧＷ１０５に、必要な経路データを提供することができる。別の実施形態では、ＶＧＷプロビジョニングサービス１４０は、ＶＧＷが構成されるサービス（複数可）を指定する引数と共に、ＡＰＩ呼出しをＶＧＷに送信してもよい。それに応じて、ＶＧＷは、経路交換サービス１５０にクエリを送信して、指定されたサービス（複数可）の経路データを取得することができる。さらに別の構成では、ＶＧＷ１０５がオンラインになったときに、ＶＧＷ１０５がＡＰＩ要求を経路交換サービス１５０に送信するように事前構成してもよい。さらに、ＶＧＷ経路リフレ

クタサービス１５３は、どのＶＧＷ１０５が特定のサービスへの経路を有するかを記録することができる。そのため、サービスが経路データを変更する場合には、更新メッセージが、ＶＧＷ経路リフレクタサービス１５３によって、そのサービスへの経路データを含む全てのＶＧＷに送信され得る。

【００２４】

ＶＧＷプロビジョニングサービス１４０（または図示されていない権限付与サービス）はまた、リモートノード８０を介して、顧客がサービスポリシー１４５を作成することを可能にすることができる。例えば、権限付与サービスは、ＶＧＷプロビジョニングサービスとは別個に、顧客がサービスポリシー１４５を作成するためにインタラクトすることができる管理インタフェースを実装してもよい。そのようなインタフェースを介して、顧客は、サービスを指定しまたは選択し、そのポリシーに固有のポリシーを選択しまたは指定し、そのポリシーの実装を要求することができる。権限付与サービスは、例えばＡＰＩ呼出しを介して、指定されたサービスに、そこに実装する目的でポリシーを伝送することができる。サービスポリシー１４５は、例えば、所与のサービス１３０へのアクセスを制限する場合がある。例えば、顧客が、ストレージサービスのストレージにアクセスできる場合がある。顧客は、ストレージサービス内の特定のデータへのアクセスを、暗号化トンネル９２から顧客のＶＧＷ１０５を通過するアクセス要求のみに制限するサービスポリシー１４５を作成することができる。ＶＧＷは、パケットがＶＧＷを通過したことをサービス１３０が判定できるように、サービス要求にタグを追加してもよい。タグは、サービス要求パケットに（例えば、ヘッダーフィールドに）挿入されるか、またはＶＧＷに関連付けられたサービスによって事前に知られているサービス要求パケットをラップしたカプセル化パケットに挿入されるメタデータ値（識別子やデジタル署名など）を含み得る。サービスポリシーは、顧客が作成することができ、基となるサービス１３０に特化し得る。

【００２５】

いくつかの実施形態では、リモートノード８０を介した顧客と認証サービスまたはＶＧＷプロビジョニングサービス１４０との間のインタラクションを通じて、セキュリティポリシー１４５が作成され得る。インタラクションは、ＶＧＷプロビジョニングサービス１４０によって実装され、例えば、リモートノードまたはリモートノード８０に通信可能に結合されたコンピュータで実行されるウェブブラウザによって表示される、グラフィカルコンソールを介して行われてもよい。他の実施形態では、顧客は、ＶＧＷプロビジョニングサービス１４０にセキュリティポリシーを作成するためにＡＰＩ呼出しを送信してもよい。ある場合には、セキュリティポリシー１４５は、コンプライアンス評価及びコンプライアンスのために対応するＶＧＷに伝送されてもよく、他の場合には、セキュリティポリシーは、コンプライアンスのために対応するサービス１３０に伝送されてもよい。ポリシー１４５がＶＧＷ１０５に提供されるかサービス１３０に提供されるかは、サービス及びポリシーの性質による。ポリシーが、顧客のＶＧＷからのみアクセスされる顧客のストレージへのアクセス要求を受け入れ、顧客のＶＧＷを通過しないアクセス要求は無視する、ストレージサービスのためのポリシーである上記の例では、セキュリティポリシーがストレージサービスに提供されることになる。

【００２６】

図１は、ＶＧＷ１０５が、１つ以上のサービス１３０と、顧客によって作成され使用される仮想マシン１６５が実行される１つ以上のサーバ１６０とに通信可能に結合される例を示す。顧客の仮想マシン１６５は、仮想ネットワーク（ＶＮ）内で実行することができる。ＶＮは、顧客によって定義されたネットワーク内で実行される仮想マシンの論理グループを備える。顧客は、ＩＰアドレス範囲の選択、サブネットの作成、ならびに経路表及びネットワークゲートウェイの構成など、環境を定義することについて完全に制御することができる。顧客のＶＮは、顧客の仮想マシンが実行されるホストコンピュータを相互接続する１つ以上の中間物理ネットワーク上に実装され得る。つまり、仮想ネットワークは物理ネットワーク上に実装され得る。各顧客は、仮想ネットワーク内で動作するインスタンスを有することができる。仮想ネットワークは、物理ネットワーク内で動作する仮想Ｉ

Ｐアドレス及びシステムを使用して、仮想ネットワーク内の他の仮想マシンをホストとして処理するマシンに関連付けられた物理ＩＰアドレスに対応するパケットをルーティングする。仮想ネットワークの実装には、パケットに追加のヘッダーを変更し、または追加して、仮想ネットワークと整合性のある仮想アドレスを、基となる物理ネットワークに関連付けられた物理アドレスにマッピングし、ホストコンピュータ間の物理ネットワークを介してパケットをルーティングできるようにすることが含まれ得る。顧客用にＶＮを実装した各ホストコンピュータには、プロバイダネットワーク内で使用される物理ＩＰアドレスに基づいて、顧客の仮想ネットワーク内の別の仮想マシンの仮想ＩＰアドレス宛ての発信パケットを変更することができる通信マネージャが含まれ得る。例えば、通信パケットがサービスプロバイダのネットワーク内のコンピューティングノード間で送信される場合、この送信元パケットは、特定のプロトコル（例えば、ＩＰｖ４）によるＩＰアドレスを含むことができ、送信ホストコンピュータに関連する仮想マシン通信マネージャは、仮想ネットワークパケットを、物理的な送信元及び宛先のＩＰアドレスを含む基盤ネットワークパケットに埋め込む。次に、仮想マシン通信マネージャは、プロバイダネットワークの内部ネットワーク（例えば、スイッチ、ルータなど）を介してパケットを送信する。受信ホストコンピュータに関連する仮想マシン通信マネージャは、基盤パケットを受信し、仮想ネットワークパケットを抽出し、仮想ネットワークパケットを対象の仮想マシンに転送する。

【００２７】

仮想ネットワーク内の仮想マシン間で送信すべきパケットを変更する際に使用する仮想から物理へのアドレスマッピングを格納し、更新し、提供するために、マッピングサービスが提供されてもよい。仮想ネットワークは、オーバーレイネットワークパケットサイズとしてＩＰｖ４（「インターネットプロトコルバージョン４」）またはＩＰｖ６（「インターネットプロトコルバージョン６」）パケットを使用するなど、様々な実施形態で様々なように実装することができる。例えば、仮想ネットワークの仮想ネットワークアドレス情報は、１つ以上の中間物理ネットワークのネットワーキングプロトコルに使用される、より大きな物理パケットネットワークアドレス空間に埋め込むことができる。説明のための一例として、仮想ネットワークは、３２ビットのＩＰｖ４ネットワークアドレスを使用して実装することができ、それらの３２ビット仮想ネットワークアドレスは、通信パケットもしくは他のデータ送信のヘッダーを付け直すこと、または別の方法でそのようなデータ送信を変更して、それらが構成されている第１のネットワーキングプロトコルから別の第２のネットワーキングプロトコルに変換することなどによって、１つ以上の中間物理ネットワークによって使用される１２８ビットのＩＰｖ６ネットワークアドレスの一部として埋め込むことができる。他の実施形態では、ＩＰｖ４パケットが物理ネットワーク及び仮想ネットワークによって使用され得る。例えば、仮想マシンによって生成されるＩＰｖ４パケットのサイズを、ＩＰｖ４パケットに挿入できるサイズに制限し、サービスプロバイダがパケットにヘッダーを追加できるように十分なビットを残すことができる。

【００２８】

図１の実施形態では、リモートノード８０によって送信されるパケットは、上記のようにサービス１３０に、または顧客の仮想ネットワーク内の仮想マシン１６５にルーティングされ得る。したがって、ＶＧＷ１０５は、サービス１３０への接続性、及び／または顧客の仮想ネットワークへの接続性を提供することができる。さらに、図１は、サービス１３０がプロバイダネットワーク１００内に実装された例を示している。また一方、他の例では、サービスの１つ以上をプロバイダネットワークの外部に実装することがあるが、これらは、それにもかかわらず、プロバイダネットワークでホストとして処理される顧客のＶＧＷ１０５を介してアクセス可能である。経路交換サービスによって経路表に提供される経路データには、サービスがローカル（すなわち、プロバイダネットワーク１００内）でホストされているか、それともリモート（すなわち、プロバイダネットワーク外）でホストされているかにかかわらず、サービスにアクセスするために使用できるルーティング情報が含まれる。

【００２９】
図３は、顧客用のＶＧＷを作成する方法を示す。動作は、示されている順序で実行されることも、別の順序で実行されることもあり得る。その上、動作は順次に実行されてもよく、または動作のうちの２つ以上が同時に実行されてもよい。２００で本方法は、例えば、リモートノード８０を介して顧客によって送信された、ＶＧＷを作成する要求を、ＶＧＷを介して顧客がアクセスすべき１つ以上のサービスを指定することと共に受信することを含み得る。サービスポリシーもまた、要求の一部として含めることができる。いくつかの実施形態では、ＶＧＷを介してアクセスすべきサービス（複数可）の仕様は、ＶＧＷを作成する要求の一部であってもよいし、または別個のＡＰＩ呼出しでＶＧＷを作成した後に送信されてもよい。同様に、サービスポリシーは、ＶＧＷを作成する要求の一部であってもよいし、またはＶＧＷの作成後に送信されてもよい。いくつかの実施形態では、ＶＧＷを作成する要求はＡＰＩ呼出しを含むことができ、一方他の実施形態では、要求は、グラフィカルユーザインタフェース（例えば、Ｗｅｂブラウザに実装される）、または顧客が選択を行うことができるコマンドラインインタフェースを介して行うことができる。作成要求は、顧客のアカウント、ＶＧＷが暗号化トンネル９２を確立しようとするリモートノード８０のパブリックＩＰアドレス、認証キー、及びトンネル９２の確立に使用可能な他の任意の値を指定することができる。顧客が作成要求を送信するために使用するノードは、ＶＧＷ１０５への暗号化トンネル９２に参加するノードとは異なるコンピューティングデバイスであってもよい。したがって、作成要求と共に送信されるパブリックＩＰアドレスは、ＶＧＷプロビジョニングサービス１４０に要求を送信するコンピューティングデバイスのパブリックＩＰアドレスであってもよいし、そうでなくてもよい。ＶＧＷプロビジョニングサービス１４０は、ＶＧＷを作成するための要求を受信してもよい。

【００３０】
２０２で本方法は、要求されたＶＧＷ１０５を実装するために、物理サーバ上に仮想マシンをプロビジョニングすることを含む。仮想マシンのプロビジョニングには、ＶＧＷアプリケーション１２０を含むマシンイメージをサーバにコピーし、次いで仮想マシンを起動することが含まれ得る。この動作には、トンネル９２で使用するためにＶＧＷにセキュリティアソシエーションを確立することも含まれ得る。セキュリティアソシエーションには、暗号化アルゴリズム、認証値、リモートノードのパブリックＩＰアドレスなどが含まれ得る。ＶＧＷは、ＩＫＥプロトコルを実行して、暗号化キーを確立することができる。２０４において、顧客の要求で識別されるサービス（複数可）の経路データを、例えば経路交換サービス１５０によって取得することができる。経路データは、上記のように暗号化トンネル９２を介してＶＧＷによって受信されたサービス要求を転送するために、ＶＧＷによって使用可能なルーティング情報を含む。次いで２０６で、経路データをＶＧＷ１０５内に確立された経路表にロードすることができる。

【００３１】
２０８でＶＧＷ１０５は、ＶＧＷにピア接続されたリモートノード８０に経路データをアドバタイズする。アドバタイズには、ＶＧＷを介してアクセス可能なサービス（複数可）のパブリックＩＰアドレス（またはアドレス範囲）とＶＧＷの識別子とを含めることができる。この情報により、仮想プライベートネットワーク（ＶＰＮ）デバイスなどのネットワークデバイスを介して暗号化トンネル９２に接続されたコンピュータシステムが、パブリックインターネットを介したサービス自体にではなく、暗号化トンネル９２を介したＶＧＷに対して、提供すべきサービスの要求を含むパケットを作成できるようになる。

【００３２】
２１０で、本方法は、顧客が作成したポリシー（もしあれば）を、対応するサービス、すなわちポリシーが適用されるサービスに提供することをさらに含む。無論、いくつかの実施形態では、ポリシーは、サービスにではなく、ＶＧＷに提供されてもよい。

【００３３】
図４は、ＶＧＷの動作の一例を示す方法である。動作は、示されている順序で実行されることも、別の順序で実行されることもあり得る。その上、動作は順次に実行されてもよ

く、または動作のうちの２つ以上が同時に実行されてもよい。２２０で本方法は、ＶＧＷが、トンネル９２を介してリモートノード８０から暗号化パケットを受信することを含む。パケットは、サービス１３０に対する要求を含むことができる。２２２でＶＧＷは、パケットを復号化して、暗号化されていないサービス要求を復元する。２２４で、復号化されたパケット内のヘッダー情報（例えば、宛先ＩＰアドレス）を用いて、ＶＧＷがその経路表にアクセスして、サービス要求に対する適切な経路を判定する。

【００３４】

２２６でＶＧＷは、経路表を用いて判定された経路上に、サービス要求を転送する。対象サービス１３０は、２２８でサービス要求を受信し、サービス要求を実行する。サービス要求は、サービスがその動作を実行するために使用する引数を含み得る。データ（例えば、応答データ、受信確認など）がサービスの要求元（すなわち、リモートノード８０）に戻されるべきである場合、そのようなデータはパケットに含まれ、概して逆の経路に沿って、ＶＧＷ１０５経由でトンネル９２を介して、リモートノードにルーティングされ得る。ＶＧＷは、パケットを暗号化してから、リモートノード８０へ送信してもよい。

【００３５】

図５は、所与のサービスの経路データを更新する方法を示す。動作は、示されている順序で実行されることも、別の順序で実行されることもあり得る。その上、動作は順次に実行されてもよく、または動作のうちの２つ以上が同時に実行されてもよい。２５０で本方法は、サービスが、更新された経路データを、そのリフレクタサービス（例えば、サービス経路リフレクタサービス１５１）に提供することを含む。２５２で、サービス経路リフレクタサービス１５１は、更新された経路データをＶＧＷ経路リフレクタサービス１５３に提供することによって応答することができる。上記のように、ＢＧＰプロトコルを使用して、更新された経路データをＶＧＷ経路リフレクタサービスに提供することができるが、追加、削除など、ＡＰＩ呼出しを使用して、経路データの更新を提供することもできる。

【００３６】

２５４で本方法は、経路データが更新されているサービスにアクセスするように構成された各ＶＧＷに、更新された経路データを提供することを含む。ＶＧＷ経路リフレクタサービス１５３は、個々のサービスの経路データを有する各ＶＧＷの識別情報を記録することができ、したがって、サービスへの経路を有するものとして記録されたそれらのＶＧＷに、更新された経路データを転送することができる。次いでそのような各ＶＧＷは、２５６で、ＶＧＷ経路リフレクタサービス１５３から受信した更新されたルートデータを、その経路表１２５に格納することができる。２５８で各ＶＧＷはまた、その更新された経路表をそのリモートノード８０にアドバタイズすることができる。アドバタイズは、既知のプロトコルに従ってもよいし、または任意の適切な種類のメッセージ交換を含んでもよい。アドバタイズに含まれる情報の種類の例は、上に記載されている。

【００３７】

一部の実施態様では、顧客は、サービスを追加しまたは削除するために、ＶＧＷ１０５の構成を変更できる。例えば、顧客は、上記で説明した１つ以上のサービス用に構成された既存のＶＧＷを有し、その後ＶＧＷを介してアクセス可能なそれらのサービスに追加のサービスを追加することを望む場合がある。あるいは、現在そのようなアクセスを提供しているＶＧＷから、特定のサービスへのアクセスを除去することを望む場合がある。そのような変更は、顧客のコンピューティングデバイスを介して、パブリックネットワーク９０にわたって、顧客がＶＧＷプロビジョニングサービス１４０を通じて開始することができる。いずれの場合も、顧客のＶＧＷの経路表１２５は、変更を反映するように更新される。顧客が特定のサービスへのアクセスを追加したい場合、顧客は追加すべきサービスを指定し、ＶＧＷプロビジョニングサービス１４０は、顧客がそのサービスにアクセスするために選択したいずれかのＶＧＷに、指定されたサービスの経路データを追加する要求を経路交換サービス１５０に送信する。次に、ＶＧＷプロビジョニングサービス１４０は、上記のメッセージを顧客のＶＧＷ（複数可）１０５に送信する。メッセージには、指定さ

れたサービスの経路データが含まれる場合がある。次に、経路データが経路表１２５に追加される。

【００３８】

同様に、顧客が所与のＶＧＷのサービスへのアクセスを削除したい場合、顧客はＶＧＷプロビジョニングサービス１４０に要求を送信し、ＶＧＷ及び削除すべき特定のサービスを識別する。ＶＧＷプロビジョニングサービスは、顧客指定のＶＧＷにメッセージを送信することによって、削除要求に応答する。メッセージには、削除される経路データの識別子が含まれる。次に、ＶＧＷは、要求された経路データを経路表１２５から削除する。

【００３９】

図６は、様々な実施形態による、本明細書に記載される仮想マシン（例えば、仮想マシン１１５、１６５）、サービス１３０、ＶＧＷプロビジョニングサービス１４０、サービスデータベース１５０のいずれかの実装に適したコンピューティングシステム５００の概略図を示す。このシステムは、１つ以上のコンピューティングデバイス５０２を含む。コンピューティングシステム５００は、ネットワーク５１８を介して互いに通信可能に結合されたコンピューティングデバイス５０２及び二次ストレージ５１６を含む。コンピューティングデバイス５０２及び関連する二次ストレージ５１６のうちの１つ以上を使用して、本明細書に記載される様々なサービスの機能を提供することができる。

【００４０】

各コンピューティングデバイス５０２は、ストレージデバイス５０６、ネットワークインタフェース５１２、及びＩ／Ｏデバイス５１４に結合された１つ以上のプロセッサ５０４を含む。いくつかの実施形態では、コンピューティングデバイス５０２は、システム１００の複数の構成要素の機能を実装してもよい。様々な実施形態では、コンピューティングデバイス５０２は、１つのプロセッサ５０４を含むユニプロセッサシステム、またはいくつか（例えば、２、４、８、または他の適切な数）のプロセッサ５０４を含むマルチプロセッサシステムであり得る。プロセッサ５０４は、命令を実行することが可能な任意の適切なプロセッサであり得る。例えば、様々な実施形態では、プロセッサ５０４は、ｘ８６、ＰｏｗｅｒＰＣ、ＳＰＡＲＣ、もしくはＭＩＰＳ　ＩＳＡ、または任意の他の好適なＩＳＡなどの様々な命令セットアーキテクチャ（「ＩＳＡ」）のうちのいずれかを実装する、汎用または組込み型マイクロプロセッサであってもよい。マルチプロセッサシステムでは、プロセッサ５０４のそれぞれは、必ずしも必要ではないが、一般に同じＩＳＡを実装することができる。同様に、プロバイダネットワーク１００を集合的に実装するような分散コンピューティングシステムでは、コンピューティングデバイス５０２のそれぞれが同じＩＳＡを実装してもよく、または個々のコンピューティングノード及び／またはノードのレプリカグループが異なるＩＳＡを実装してもよい。

【００４１】

ストレージ５０６は、プロセッサ（複数可）５０４によってアクセス可能なプログラム命令５０８及び／またはデータ５１０を格納するように構成された非一時的なコンピュータ可読記憶装置を含み得る。ストレージ５０６はまた、上で説明されたようにマシンイメージを格納するために使用されてもよい。ストレージデバイス５０６は、任意の適切な揮発性メモリ（例えば、ランダムアクセスメモリ）、不揮発性ストレージ（ハードディスクドライブなどの磁気ストレージ、光学ストレージ、ソリッドストレージなど）を使用して実装され得る。本明細書で開示される機能を実装するプログラム命令５０８及びデータ５１０は、ストレージデバイス５０６内に格納される。例えば、命令５０８は、プロセッサ（複数可）５０４によって実行されると、本明細書で開示されているサービスプロバイダのネットワークの様々なサービス及び／または他のコンポーネントを実行する命令を含み得る。

【００４２】

二次ストレージ５１６は、本明細書で説明するサービスプロバイダのネットワークの様々な態様を実施するために、本明細書に記載のプログラム命令及び／またはデータなどの情報を格納する追加の揮発性または不揮発性のストレージ及びストレージデバイスを含む

ことができる。二次ストレージ５１６は、ネットワーク５１８を介してコンピューティングデバイス５０２によってアクセス可能な様々なタイプのコンピュータ可読媒体を含み得る。コンピュータ可読媒体は、半導体記憶装置、磁気媒体、または光学媒体、例えば、ディスクもしくはＣＤ／ＤＶＤ－ＲＯＭ、あるいは他の記憶技術などの記憶媒体またはメモリ媒体を含み得る。二次ストレージ５１６に格納されたプログラム命令及びデータは、プロセッサ５０４による実行のために、有線または無線のネットワークまたはそれらの組合せであり得るネットワーク５１８を介した伝送媒体または伝送信号によって、コンピューティングデバイス５０２に送信され得る。本明細書に記載される仮想マシン（例えば、仮想マシン１１５、１６５）、サービス１３０、ＶＧＷプロビジョニングサービス１４０、サービスデータベース１５０、及び他の構成要素のそれぞれは、ソフトウェアを実行する別個のコンピューティングデバイス５０２として実装されて、本明細書に記載される機能をコンピューティングノードに提供することができる。いくつかの実施形態では、様々なサービスの一部または全部が同じコンピューティングデバイスによって実装されてもよい。

【００４３】

ネットワークインタフェース５１２は、コンピューティングデバイス５０２及び／またはネットワーク５１８に結合された他のデバイス（他のコンピュータシステム、通信デバイス、入力／出力デバイス、または外部ストレージデバイスなど）間でデータを交換できるように構成され得る。ネットワークインタフェース５１２は、例えば、任意の適切なタイプのイーサネットネットワークなどの有線または無線のデータネットワーク、例えば、アナログ音声ネットワークまたはデジタルファイバ通信ネットワークなどの電気通信／テレフォニネットワーク、ファイバチャネルＳＡＮなどのストレージエリアネットワーク、または任意の他の適切なタイプのネットワーク及び／またはプロトコルを介した通信をサポートし得る。

【００４４】

入力／出力デバイス５１４は、１つ以上のディスプレイ端末、キーボード、キーパッド、タッチパッド、マウス、スキャンデバイス、音声または光学認識デバイス、または１つ以上のコンピューティングデバイス５０２によるデータの入力または取得に適した他のいずれかのデバイスを含んでもよい。複数の入力／出力デバイス５１４は、コンピューティングデバイス５０２内に存在してもよく、またはシステム５００の様々なコンピューティングデバイス５０２上に分散されてもよい。いくつかの実施形態では、同様の入力／出力デバイスは、コンピューティングデバイス５０２とは別個であってもよく、ネットワークインタフェース５１２などの有線または無線接続を介してシステム５００の１つ以上のコンピューティングデバイス５０２と対話し得る。

【００４５】

本開示は、様々な条項に関して理解され得る様々な態様を教示する。条項１では、仮想プライベートゲートウェイ（ＶＧＷ）プロビジョニングサービスが提供され、プロセッサに結合されたメモリを含み、メモリが、実行時にＶＧＷプロビジョニングサービスに、顧客からＶＧＷを確立する要求を受信することであって、要求が、ＶＧＷを通じてアクセス可能なサービスと、顧客設定可能ポリシーとを指定し、顧客設定可能ポリシーが、指定されたサービスへのアクセスを、指定されたサービスにＶＧＷを介して送信された要求に制限する、ＶＧＷを確立する要求を受信すること、を行わせる命令を含む。要求に応じて、本サービスは、演算デバイス上でＶＧＷ仮想マシンをインスタンス化することであって、ＶＧＷ仮想マシンが、パブリックネットワークを経由してリモートノードへのセキュアトンネルを確立し、セキュアトンネルを経由してリモートノードから暗号化されたトラフィックを受信するように構成されたＶＧＷアプリケーションを含む、ＶＧＷ仮想マシンをインスタンス化することができる。本サービスは、ＶＧＷ仮想マシンに指定されたサービスの経路データが提供されるようにすることであって、ＶＧＷアプリケーションが、実行時に、指定されたサービスの経路データを、セキュアトンネル経由でＶＧＷアプリケーションにアドバタイズさせる命令を含む、経路データが提供されるようにすることができる。

そして、本サービスは、サービスが順守するように、識別されたサービスに顧客設定可能ポリシーを提供することができる。

【００４６】

条項２では、経路データには、指定したサービスに関連付けられたパブリックインターネットプロトコル（ＩＰ）アドレス、及び顧客のＶＧＷの識別子が含まれる。

【００４７】

条項３では、ＶＧＷプロビジョニングサービスが、経路交換サービスへの経路要求の送信を通じて、指定されたサービスの経路データがＶＧＷ仮想マシンに提供されるように構成され、経路要求が指定されたサービスを識別し、経路交換サービスが、アプリケーションプログラミングインタフェース（ＡＰＩ）呼出しを顧客のＶＧＷに送信するように構成され、ＡＰＩ呼出しが経路データを含む。

【００４８】

条項４では、本システムは、所与のサービスが、所与のサービスの経路データを更新することに応じて、サービスが、サービス経路リフレクタサービスにアクセス可能なデータベース内の経路レコードを更新し、レコードが、所与のサービスに対応し、サービス経路リフレクタサービスが、更新された経路データをＶＧＷ経路リフレクタサービスに送信し、サービス経路リフレクタサービスが、所与のサービスの経路データを含むメッセージを各ＶＧＷに送信し、メッセージが、更新された経路データを含む。

【００４９】

条項５では、ＶＧＷアプリケーションが、実行時にＶＧＷアプリケーションに以下を実行させる命令をさらに含み、ＶＧＷアプリケーションが、セキュアトンネルを介してリモートノードから暗号化されたパケットを受信することに応じて、暗号化されたパケットは、指定されたサービスのサービス要求を含み、命令が、暗号化されたパケットを復号化してサービス要求を取得すること、サービス要求のヘッダー内の情報を使用して、経路表にアクセスし、サービス要求の対象となるサービスへの経路を判定すること、及び判定された経路を介して、要求の対象となるサービスにサービス要求を転送することを含み、サービスが、サービス要求を実行するように構成されている。

【００５０】

条項６では、システムは、プロセッサに結合されたメモリを含む仮想プライベートゲートウェイ（ＶＧＷ）プロビジョニングサービスであって、メモリが、実行時にＶＧＷプロビジョニングサービスに、ＶＧＷを確立するための要求を受信することであって、要求が、ＶＧＷを通じてアクセス可能なサービスを指定する、要求を受信すること、要求に応じて、演算デバイス上でＶＧＷ仮想マシンをインスタンス化することであって、ＶＧＷ仮想マシンが、パブリックネットワークを経由してリモートノードへのセキュアトンネルを確立し、セキュアトンネルを経由してリモートノードから暗号化されたトラフィックを受信するように構成されたＶＧＷアプリケーションを含む、ＶＧＷ仮想マシンをインスタンス化すること、指定されたサービスの経路データが、ＶＧＷ仮想マシンに提供されるようにすることを実行させる命令を含むＶＧＷプロビジョニングサービスを備える。

【００５１】

条項７では、サービスの経路データが、指定されたサービスのパブリックインターネットプロトコル（ＩＰ）アドレスを含み、ＶＧＷアプリケーションが、パブリックネットワークを経由して、パブリックＩＰアドレスをリモートノードにアドバタイズするように構成されている。

【００５２】

条項８では、サービスの経路データが、指定されたサービスのパブリックインターネットプロトコル（ＩＰ）アドレスを含み、ＶＧＷアプリケーションが、パブリックネットワークを経由して、パブリックＩＰアドレスをリモートノードにアドバタイズするように構成されており、サービスの更新されたパブリックインターネットプロトコル（ＩＰ）アドレスの生成が、サービスに、更新されたパブリックＩＰアドレスを含む更新された経路データで経路交換サービスの経路エントリを更新させ、経路交換サービスに、サービスの更

新された経路データをＶＧＷ仮想マシンへ送信させ、ＶＧＷアプリケーションに、サービスの更新された経路データをリモートノードへアドバタイズさせる。

【００５３】

条項９では、ＶＧＷアプリケーションが、実行時に、セキュアトンネルを介したリモートノードからの暗号化パケットの受信と、暗号化パケットが、識別されたサービスのサービス要求を含むこととに応じて、ＶＧＷアプリケーションに、暗号化されたパケットを復号化してサービス要求を取得すること、サービス要求のヘッダー内の情報を使用して、経路表にアクセスし、サービス要求の対象となるサービスへの経路を判定すること、及び判定された経路を介して、要求の対象となるサービスにサービス要求を転送することを行わせる命令をさらに含む。

【００５４】

条項１０では、ＶＧＷアプリケーションは、セキュアトンネルにインターネットプロトコルセキュリティ（ＩＰＳｅｃ）を実装するように構成されている。

【００５５】

条項１１では、経路交換サービスが提供され、複数のサービスの経路データを含むように構成された経路表を含み、ＶＧＷプロビジョニングサービスが、経路交換サービスに要求を送信して、指定されたサービスの経路データを提供するように構成されている。

【００５６】

条項１２では、要求が、指定されたサービスへのアクセスを制限するように構成された顧客設定可能ポリシーを含む。

【００５７】

条項１３では、指定されたサービスは、顧客設定可能ポリシーを受信し、顧客設定可能ポリシーを要求の少なくとも一部に適用するように構成されている。

【００５８】

条項１４では、ＶＧＷアプリケーションが、顧客設定可能ポリシーを受信し、顧客設定可能ポリシーを確実に順守するように構成されている。

【００５９】

条項１５では、仮想プライベートゲートウェイ（ＶＧＷ）によって、サービスプロバイダネットワークに実装され、パブリックネットワークを経由してノードからＶＧＷによって受信されたサービスに対する要求を含む暗号化パケットを復号化すること、ＶＧＷ内の経路表にアクセスして、サービスプロバイダネットワーク内のサービスへの経路を判定すること、ＶＧＷによって、経路サービスへの経路を経由して要求を転送すること、ＶＧＷによって、サービスの更新された経路データを受信することであって、更新された経路データが、サービスの更新されたパブリックインターネットプロトコル（ＩＰ）アドレスを含む、更新された経路データを受信すること、及びＶＧＷによって、更新されたパブリックＩＰアドレスをアドバタイズすることを含む方法が開示されている。

【００６０】

条項１６では、本方法はさらに、仮想マシンの作成要求に応じて、サーバ上にＶＧＷ仮想マシンをプロビジョニングすることであって、作成要求がサービスを指定する、プロビジョニングすること、指定されたサービスに関連した経路データの経路要求に応じて、経路データをＶＧＷに提供すること、及びプロビジョニングされた仮想マシンの経路表に経路データをロードすることを含む。

【００６１】

条項１７では、本方法は、サービスへのアクセスを制限する顧客設定可能ポリシーを生成し、ポリシーコンプライアンスを実行するために、顧客設定可能ポリシーをサービスに送信することをさらに含む。

【００６２】

条項１８では、サービスの更新された経路データを受信することが、更新された経路データをサービスリフレクタサービスに提供すること、サービスリフレクタサービスからＶＧＷリフレクタサービスへ更新された経路データを提供するために、ボーダゲートウェイ

プロトコル（ＢＧＰ）を実装すること、及びＶＧＷリフレクタサービスからＶＧＷへ更新された経路データを提供することを含む。

【００６３】

条項１９では、本方法は、経路を経由して要求を転送する前に、ＶＧＷを示す識別子で要求にタグ付けすることをさらに含む。

【００６４】

条項２０では、本方法は、サービスによって要求を実行することをさらに含み、サービスを実行することが、要求を送信した顧客による排他的な使用に割り当てられたストレージまたはデータベースにアクセスすること、及び顧客提供のコードを実行することのうちの少なくとも１つを含む。

【００６５】

「～に基づいて」への言及は、「少なくとも～に基づいて」と解釈されるべきである。例えば、値または条件の判定がＹの値「に基づいて」いる場合、その判定は少なくともＹの値に基づいている。つまり、判定は他の値にも基づいて行われる。

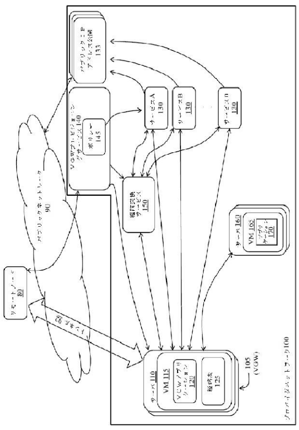
【００６６】

当業者はまた、いくつかの実施形態において、本明細書に開示される機能は、より多くのソフトウェアモジュールまたはルーチンに分割されるか、より少ないモジュールまたはルーチンに統合されるかなどの代替の形式で提供され得ることを理解するであろう。同様に、一部の実施形態では、図示された方法は、例えば、他の図示された方法がそのような機能をそれぞれ欠いているかまたは含んでいる場合、または提供される機能の量が変更された場合など、説明されているよりも多くの機能または少ない機能を提供することができる。更に、種々の作用が、特定の方法（例えば、直列または並列で）で及び／または特定の順序で実行されるように説明されることがあるが、当業者は、他の実施形態では、作用が他の順序及び他の様式で実行してもよいことが認められる。図面に示され、本明細書で記載される様々な方法は、方法の例示的な実施形態を表す。方法は、様々な実施形態において、ソフトウェア、ハードウェア、またはそれらの組合せで実装されてもよい。同様に、任意の方法の順序を変更することができ、様々な実施形態では、様々な要素を追加し、並べ替え、組み合わせ、省略し、修正したりすることができる。

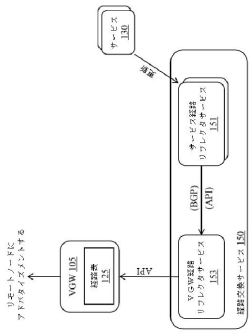
【００６７】

上記の議論は、本開示の原理及び様々な実施形態を例示することを意図している。上記の開示が十分に理解されれば、多くの変形及び変更が当業者に明らかになるであろう。添付の特許請求の範囲は、そのような変形及び修正を全て包含するように解釈されることが意図される。

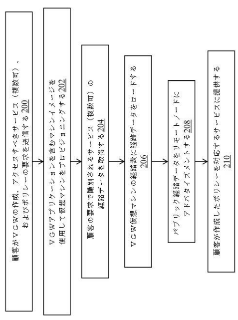
【図１】



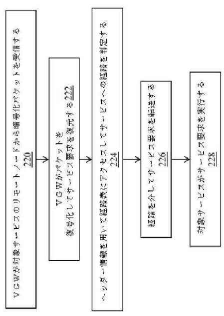
【図２】


サービス 130
通知
サービス経路リフレクタサービス 151
(BGP)
(API)
VGW経路リフレクタサービス 153
経路交換サービス 150
VGW 105
経路表 125
リモートノードにアドバタイズメントする

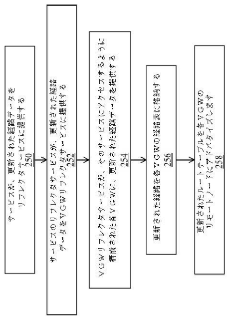
【図３】


顧客がVGWの作成、アクセスすべきサービス（複数可）、およびポリシーの要求を送信する 200
VGWアプリケーションを含むマシンイメージを使用して仮想マシンをプロビジョニングする 202
顧客の要求で識別されるサービス（複数可）の経路データを取得する 204
VGW仮想マシンの経路表に経路データをロードする 206
パブリック経路データをリモートノードにアドバタイズメントする 208
顧客が作成したポリシーを対応するサービスに提供する 210

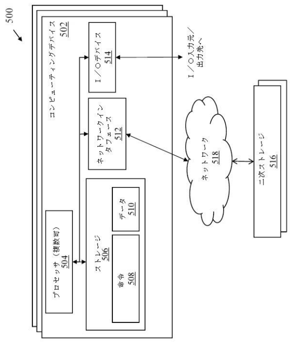
【図４】


VGWが対象サービスのリモートノードから暗号化パケットを受信する 220
VGWがパケットを復号化してサービス要求を露出する 222
ヘッダー情報を用いて経路表にアクセスしてサービスへの経路を判定する 224
経路を介してサービス要求を転送する 226
対象サービスがサービス要求を実行する 228

【図５】


サービスが、更新された経路データを
リフレクタサービスに提供する
250
サービスのリフレクタサービスが、更新された経路
データをＶＧＷリフレクタサービスに提供する
252
ＶＧＷリフレクタサービスが、そのサービスにアクセスするように
構成された各ＶＧＷに、更新された経路データを提供する
254
更新された経路を各ＶＧＷの経路表に格納する
256
更新されたルートテーブルを各ＶＧＷの
リモートノードにアドバタイズします
258

【図６】


500
コンピューティングデバイス
502
プロセッサ（複数可）
504
ストレージ
506
命令
508
データ
510
ネットワークイン
タフェース
512
Ｉ／Ｏデバイス
514
Ｉ／Ｏ入力元／
出力先へ
ネットワーク
518
二次ストレージ
516

フロントページの続き

(56)参考文献　特開２０１６－１４９６３４（ＪＰ，Ａ）
米国特許出願公開第２０１６／０２８５８３１（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／７２１
Ｈ０４Ｌ　１２／７０