

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-175190

(P2012-175190A)

(43) 公開日 平成24年9月10日 (2012.9.10)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 12/56 (2006.01)	H04L 12/56 H	5B014
G06F 13/14 (2006.01)	G06F 13/14 310F	5K030
G06F 9/46 (2006.01)	G06F 13/14 310K	
	G06F 13/14 320A	
	G06F 9/46 350	

審査請求 未請求 請求項の数 9 O L (全 27 頁)

(21) 出願番号 特願2011-32552 (P2011-32552)
 (22) 出願日 平成23年2月17日 (2011.2.17)

(71) 出願人 00004226
 日本電信電話株式会社
 東京都千代田区大手町二丁目3番1号
 (74) 代理人 100089118
 弁理士 酒井 宏明
 (74) 代理人 100112656
 弁理士 宮田 英毅
 (72) 発明者 深見 公彦
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内
 (72) 発明者 小山 高明
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

最終頁に続く

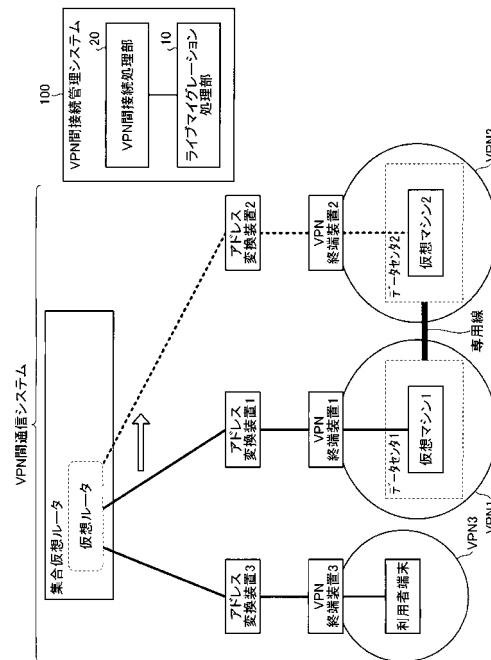
(54) 【発明の名称】 制御装置、制御システム、制御方法、及び制御プログラム

(57) 【要約】

【課題】ライブマイグレーションに伴って発生する処理時間を短縮すること。

【解決手段】実施の形態に係る制御装置は、利用者端末が第1のVPN (Virtual Private Network) に設置された仮想マシンにアクセスするための経路が現用の経路として構築されている場合に、第2のVPNに設置される仮想マシンをマイグレーション先とするライブマイグレーションの実行開始を検知する。また、制御装置は、ライブマイグレーションの実行開始が検知されると、ライブマイグレーションの実行と併行して、利用者端末が第2のVPNに設置される仮想マシンにアクセスするための経路を構築する設定を、所定のネットワーク装置に対して行う。そして、制御装置は、ライブマイグレーションの実行完了を検知し、かつ、ネットワーク装置への設定が完了すると、現用の経路を、新たに構築された経路に切り替える。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

V P N (Virtual Private Network) に設置された利用者端末が他の V P N に設置された仮想マシンにアクセスするための経路をネットワーク装置に対する設定により構築し、V P N 間の接続を制御する制御装置であって、

前記利用者端末が第 1 の V P N に設置された仮想マシンにアクセスするための経路が現用の経路として構築されている場合に、該第 1 の V P N に設置された仮想マシンをマイグレーション元として、第 2 の V P N に設置される仮想マシンをマイグレーション先とするライブマイグレーションの実行開始を検知する検知部と、

前記検知部によって前記ライブマイグレーションの実行開始が検知されると、該ライブマイグレーションの実行と併行して、前記利用者端末が前記第 2 の V P N に設置される仮想マシンにアクセスするための経路を構築する設定を、所定のネットワーク装置に対して行う設定部と、

前記ライブマイグレーションの実行完了を検知し、かつ、前記ネットワーク装置への設定が完了すると、現用の経路を、前記設定部によって構築された経路に切り替える切替部と

を備えたことを特徴とする制御装置。

【請求項 2】

前記ネットワーク装置は、

V P N 間接続の対象となる複数の V P N を収容し、V P N 間のパケット転送を制御するパケット転送制御装置と、該パケット転送制御装置と各 V P N との間に設置され、パケットに含まれるアドレスを変換するアドレス変換装置とを含み、

前記アドレス変換装置は、

パケットに含まれる送信元のアドレス及び宛先のアドレスの双方を、アドレス変換情報に従って変換し、

前記設定部は、前記検知部によって前記ライブマイグレーションの実行開始が検知されると、前記パケット転送制御装置と前記第 2 の V P N との間に設置されたアドレス変換装置に対する前記アドレス変換情報の設定を行うことを特徴とする請求項 1 に記載の制御装置。

【請求項 3】

前記設定部は、前記パケット転送制御装置と前記第 1 の V P N との間に設置されたアドレス変換装置に設定されたアドレス変換情報と同一内容のアドレス変換情報を、前記パケット転送制御装置と前記第 2 の V P N との間に設置されたアドレス変換装置に対して設定することを特徴とする請求項 2 に記載の制御装置。

【請求項 4】

前記設定部は、前記第 2 の V P N 内で前記利用者端末を一意に識別するための新たなアドレスを払い出し、払い出した新たなアドレスを用いたアドレス変換情報を、該アドレス変換装置に対して設定することを特徴とする請求項 2 に記載の制御装置。

【請求項 5】

前記設定部は、前記パケット転送制御装置と前記第 1 の V P N との間に設置されたアドレス変換装置に設定されたアドレス変換情報に含まれる、前記第 2 の V P N 内で前記利用者端末を一意に識別するためのアドレスが、前記パケット転送制御装置と前記第 2 の V P N との間に設置されたアドレス変換装置に対して設定可能であるか否かを判定し、設定可能でないと判定した場合に、前記第 2 の V P N 内で前記利用者端末を一意に識別するための新たなアドレスを払い出し、払い出した新たなアドレスを用いたアドレス変換情報を、該アドレス変換装置に対して設定することを特徴とする請求項 4 に記載の制御装置。

【請求項 6】

前記設定部は、前記第 2 の V P N 内で前記利用者端末を一意に識別するための前記新たなアドレスを、前記利用者端末と前記第 2 の V P N に設置される仮想マシンとの間に経路が構築される時間帯において、該第 2 の V P N 内で通信相手となり得る端末の中で一意に

10

20

30

40

50

識別されるように払い出すことを特徴とする請求項 4 又は 5 に記載の制御装置。

【請求項 7】

V P N に設置された利用者端末が他の V P N に設置された仮想マシンにアクセスするための経路を制御する制御システムであって、

複数の V P N を収容し、V P N 間のパケット転送を制御するパケット転送制御装置と、前記パケット転送制御装置と各 V P N との間に設置され、パケットに含まれるアドレスを変換するアドレス変換装置と、

V P N 間を接続するための経路を構築する制御装置とを備え、前記制御装置は、

前記利用者端末が第 1 の V P N に設置された仮想マシンにアクセスするための経路が現用の経路として構築されている場合に、該第 1 の V P N に設置された仮想マシンをマイグレーション元として、第 2 の V P N に設置される仮想マシンをマイグレーション先とするライブマイグレーションの実行開始を検知する検知部と、

前記検知部によって前記ライブマイグレーションの実行開始が検知されると、該ライブマイグレーションの実行と併行して、前記利用者端末が前記第 2 の V P N に設置される仮想マシンにアクセスするための経路を構築する設定を、前記パケット転送制御装置と前記第 2 の V P N との間に設置されたアドレス変換装置に対して行う設定部と、

前記ライブマイグレーションの実行完了を検知し、かつ、前記ネットワーク装置への設定が完了すると、現用の経路を、前記設定部によって構築された経路に切り替える切替部と

を備えたことを特徴とする制御システム。

【請求項 8】

V P N に設置された利用者端末が他の V P N に設置された仮想マシンにアクセスするための経路をネットワーク装置に対する設定により構築して V P N 間の接続を制御する制御装置で実行される制御方法であって、

前記利用者端末が第 1 の V P N に設置された仮想マシンにアクセスするための経路が現用の経路として構築されている場合に、該第 1 の V P N に設置された仮想マシンをマイグレーション元として、第 2 の V P N に設置される仮想マシンをマイグレーション先とするライブマイグレーションの実行開始を検知する検知工程と、

前記検知工程によって前記ライブマイグレーションの実行開始が検知されると、該ライブマイグレーションの実行と併行して、前記利用者端末が前記第 2 の V P N に設置される仮想マシンにアクセスするための経路を構築する設定を、所定のネットワーク装置に対して行う設定工程と、

前記ライブマイグレーションの実行完了を検知し、かつ、前記ネットワーク装置への設定が完了すると、現用の経路を、前記設定工程によって構築された経路に切り替える切替工程と

を含んだことを特徴とする制御方法。

【請求項 9】

コンピュータを請求項 1 ~ 6 に記載の制御装置として機能させるための制御プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明の実施形態は、制御装置、制御システム、制御方法、及び制御プログラムに関する。

【背景技術】

【0002】

近年、複数の V P N (Virtual Private Network) 間を相互に接続するサービス(以下「V P N 間接続サービス」)が提案されている。例えば、データセンタ(Data Center)の V P N と自社の V P N とを相互に接続し、データセンタに設置された社内サーバに自

10

20

30

40

50

社の利用者端末からアクセスする、といった利用形態である。

【0003】

このようなデータセンタにおいて、仮想マシン技術が用いられることがある。仮想マシン技術とは、物理的なハードウェアを論理的に分割し、分割したハードウェア毎にOS (Operating System) を動作させることで、1台のマシンをあたかも複数台のマシンであるかの如く動作させる技術である。例えば、データセンタに設置された1台のサーバにこの技術を適用することで、あたかも複数のサーバであるかの如く動作させ、複数の会社に個別にサービスを提供することができる。

【0004】

ここで、仮想マシン技術に伴う技術のひとつに、ライブマイグレーション (live migration) がある。ライブマイグレーションとは、動作中の仮想マシンで動作するOSやソフトウェアを、停止することなく他の仮想マシンに移行する技術である。ライブマイグレーションによれば、例えば、動作中の仮想マシンの負荷が高い場合に、サービスを停止することなく他のサーバで仮想マシンを動作させることができる。

10

【先行技術文献】

【非特許文献】

【0005】

【非特許文献1】小山高明、唐澤秀一、岸和宏、水野伸太郎、岩村相哲、「VPN間接続管理システムの提案」、信学技報IN2009-48(2009-09)、P.53-58

20

【非特許文献2】平初、森若和雄、鶴野龍一郎、まえだこうへい、「KVM徹底入門」、株式会社翔泳社

【発明の概要】

【発明が解決しようとする課題】

【0006】

しかしながら、ライブマイグレーションがVPNをまたがって行われる場合、マイグレーション先の仮想マシンにアクセスするための経路を新たに構築しなければならない場合がある。ライブマイグレーションの実行完了時にマイグレーション先の仮想マシンが管理サーバに通知を行う技術があるが、仮にこれを応用したとしても、ライブマイグレーションに伴ってサービス提供側に発生する処理時間は、ライブマイグレーションの実行時間と経路の構築時間とを足し合わせた時間となり、長くなってしまう。このようなことから、ライブマイグレーションに伴って発生する処理時間を短縮する技術が望まれている。

30

【課題を解決するための手段】

【0007】

実施の形態に係る制御装置は、VPNに設置された利用者端末が他のVPNに設置された仮想マシンにアクセスするための経路をネットワーク装置に対する設定により構築し、VPN間の接続を制御する制御装置である。制御装置は、検知部、設定部、及び切替部を備える。検知部は、前記利用者端末が第1のVPNに設置された仮想マシンにアクセスするための経路が現用の経路として構築されている場合に、該第1のVPNに設置された仮想マシンをマイグレーション元として、第2のVPNに設置される仮想マシンをマイグレーション先とするライブマイグレーションの実行開始を検知する。設定部は、前記検知部によって前記ライブマイグレーションの実行開始が検知されると、該ライブマイグレーションの実行と併行して、前記利用者端末が前記第2のVPNに設置される仮想マシンにアクセスするための経路を構築する設定を、所定のネットワーク装置に対して行う。切替部は、前記ライブマイグレーションの実行完了を検知し、かつ、前記ネットワーク装置への設定が完了すると、現用の経路を、前記設定部によって構築された経路に切り替える。

40

【発明の効果】

【0008】

ライブマイグレーションに伴って発生する処理時間を短縮することが可能になるという効果を奏する。

50

【図面の簡単な説明】

【0009】

【図1】図1は、第1の実施形態に係るVPN間接続サービスの概要を説明するための図である。

【図2】図2は、第1の実施形態に係るライブマイグレーションの処理手順を示すシーケンス図である。

【図3】図3は、第1の実施形態に係るVPN間接続管理システムの構成を示すブロック図である。

【図4】図4は、第1の実施形態に係る顧客ネットワーク設定記憶部を説明するための図である。

【図5】図5は、第1の実施形態におけるIPアドレスの割り当てを説明するための図である。

【図6】図6は、第1の実施形態に係るネットワーク装置設定記憶部を説明するための図である。

【図7】図7は、第1の実施形態の変形例を説明するための図である。

【図8】図8は、第2の実施形態におけるTwice-NATを説明するための図である。

【図9】図9は、Single-NATによるアドレス変換を説明するための図である。

【図10】図10は、Twice-NATによるアドレス変換を説明するための図である。

【図11】図11は、第2の実施形態におけるIPアドレスの管理を説明するための図である。

【図12】図12は、VPNサービスによって接続された複数のローカルエリアネットワーク群としてのVPNを説明するための図である。

【図13】図13は、VPNサービスによって接続された複数のローカルエリアネットワーク群としてのVPNを説明するための図である。

【図14】図14は、VPNサービスによって接続された複数のローカルエリアネットワーク群としてのVPNを説明するための図である。

【図15】図15は、実施形態に係る制御プログラムによる情報処理がコンピュータを用いて具体的に実現されることを示す図である。

【発明を実施するための形態】

【0010】

以下、実施形態に係る制御装置、制御システム、制御方法、及び制御プログラムを説明する。

【0011】

(第1の実施形態)

[VPN間接続サービスの概要]

VPN間接続サービスは、複数のVPN間を相互に接続するサービスである。例えば、データセンタのVPNと顧客の会社のVPNとを相互に接続し、データセンタに設置されたサーバに顧客の利用者端末からアクセスさせる、といったサービスを提供する。以下では、このようなVPN間接続サービスが提供されるシステムを「VPN間通信システム」と呼び、VPN間接続サービスを管理し、経路を構築するシステムを「VPN間接続管理システム」と呼ぶ。

【0012】

図1は、第1の実施形態に係るVPN間接続サービスの概要を説明するための図である。まず、VPN間通信システムを説明する。VPN間通信システムにおいては、図1に示すように、集合仮想ルータが複数のVPNをスター型に収容し、集合仮想ルータと各VPNとの間にアドレス変換装置が設置される。集合仮想ルータは、VPN間のパケット転送を制御する。また、仮想ルータは、物理的なハードウェアとしての集合仮想ルータを論理的に分割し、分割したハードウェア毎にルータとして動作させることにより実現される。

10

20

30

40

50

VPN間接続サービスは、通常、この仮想ルータ単位で提供される。また、アドレス変換装置は、パケットに含まれるアドレスを変換（NAT（Network Address Translation））する。すなわち、アドレス変換装置は、各VPN内で利用されるプライベートアドレスと、集合仮想ルータ側で利用されるアドレスとを変換する。なお、VPN終端装置は、各VPNを集合仮想ルータに収容するためにVPNを終端する。

【0013】

ここで、第1の実施形態においては、VPN3に設置された利用者端末がVPN1（データセンタ1）に設置された仮想マシン1にアクセスするための経路が、現用の経路として既に構築されていることを想定する。すなわち、利用者端末と仮想マシン1との間でパケットを転送するための情報として、アドレス変換装置1及びアドレス変換装置3にはアドレス変換情報が設定され、集合仮想ルータにはルーティング情報が設定されている。言い換えると、ライブマイグレーション実行前、アドレス変換装置1及びアドレス変換装置3は、現用のアドレス変換装置として「アクティブ」の状態にあり、アドレス変換装置2は、予備のアドレス変換装置として「スタンバイ」の状態にある。なお、第1の実施形態において、予備の経路に対応する、集合仮想ルータとアドレス変換装置2とVPN2との間は、予め物理的に接続されている。

10

【0014】

そして、第1の実施形態においては、VPN1（データセンタ1）に設置された仮想マシン1をマイグレーション元として、VPN2（データセンタ2）に設置される仮想マシン2をマイグレーション先とするライブマイグレーションを実行することを想定する。すなわち、利用者端末と仮想マシン2との間でパケットを転送するための情報を、アドレス変換装置2及び集合仮想ルータに新たに設定することを想定する。言い換えると、ライブマイグレーション実行後、現用の経路が切り替えられ、アドレス変換装置1が「スタンバイ」の状態になり、アドレス変換装置2及びアドレス変換装置3が「アクティブ」の状態になる。なお、第1の実施形態において、データセンタ1とデータセンタ2とは、予め専用線で接続されている。

20

【0015】

続いて、VPN間接続管理システムを説明する。第1の実施形態に係るVPN間接続管理システム100は、例えばVPN間接続サービスを提供する電気通信事業者などによって運用される。VPN間接続管理システム100は、制御用のネットワーク（図1において図示を省略）によって各種ネットワーク装置と接続され、制御用のネットワークを介して各種ネットワーク装置に対する設定を行う。例えば、VPN間接続管理システム100は、集合仮想ルータ、アドレス変換装置1～3、並びに、データセンタ1及びデータセンタ2と制御用のネットワークによって接続され、ライブマイグレーション処理や設定処理などを行う。

30

【0016】

なお、第1の実施形態において、VPN間接続管理システム100は、ライブマイグレーション処理部10と、VPN間接続処理部20とを備える。ライブマイグレーション処理部10が、ライブマイグレーション処理を行い、VPN間接続処理部20が、ネットワーク装置に対する設定処理を行う。

40

【0017】

[ライブマイグレーションの処理手順]

図2は、第1の実施形態に係るライブマイグレーションの処理手順を示すシーケンス図である。VPN1（データセンタ1）に設置された仮想マシン1が動作中であり、利用者端末は、VPN1（データセンタ1）に設置された仮想マシン1にアクセスしている（ステップS1）。

【0018】

このとき、例えば仮想マシン1の負荷が高い場合に、ライブマイグレーション処理部10が、VPN2（データセンタ2）に設置される仮想マシン2をマイグレーション先とするライブマイグレーションの実行指示を仮想マシン1に対して送信する（ステップS2）

50

。

【 0 0 1 9 】

すると、仮想マシン 1 は、ライブマイグレーションの実行確認通知をライブマイグレーション処理部 1 0 に対して送信し（ステップ S 3 ）、仮想マシン 2 をマイグレーション先とするライブマイグレーションを実行する（ステップ S 4 ）。

【 0 0 2 0 】

一方、ステップ S 3 において実行確認通知の受信によりライブマイグレーションの実行開始を検知したライブマイグレーション処理部 1 0 は、利用者端末が仮想マシン 2 にアクセスするための経路を構築するように、まず、アドレス変換装置 2 に対する設定指示を V P N 間接続処理部 2 0 に対して送信する（ステップ S 5 ）。

10

【 0 0 2 1 】

すると、V P N 間接続処理部 2 0 は、アドレス変換装置 2 に対してアドレス変換情報を設定し（ステップ S 6 ）、その後、アドレス変換装置 2 に対する設定が完了すると、設定完了通知をライブマイグレーション処理部 1 0 に対して送信する（ステップ S 7 ）。

【 0 0 2 2 】

一方、ステップ S 4 においてライブマイグレーションの実行を開始していた仮想マシン 1 は、ライブマイグレーションの実行が完了すると、実行完了通知をライブマイグレーション処理部 1 0 に対して送信する（ステップ S 8 ）。

【 0 0 2 3 】

こうして、ライブマイグレーション処理部 1 0 は、仮想マシン 1 からライブマイグレーションの実行完了通知を受信し、また、V P N 間接続処理部 2 0 からアドレス変換装置 2 に対する設定完了通知を受信する。

20

【 0 0 2 4 】

すると、ライブマイグレーション処理部 1 0 は、ルーティング切替指示を V P N 間接続処理部 2 0 に対して送信する（ステップ S 9 ）。V P N 間接続処理部 2 0 は、集合仮想ルータに対してルーティング情報を設定し、利用者端末から仮想マシン 1 にアクセスするための経路から、利用者端末から仮想マシン 2 にアクセスするための経路に、現用の経路（ルーティング）を切り替える（ステップ S 1 0 ）。

【 0 0 2 5 】

この結果、図 2 に示すように、ステップ S 1 において、利用者端末は仮想マシン 1 にアクセスしていたが、そのアクセスは、自動的に、仮想マシン 2 に移行することになる（ステップ S 1 1 ）。すなわち、例えば、利用者端末と仮想マシン 1 や仮想マシン 2 との間で行われる通信が T C P (Transmission Control Protocol) である場合、利用者端末は、アクセス中の仮想マシン 1 から応答が無いと、再送を行う。この再送を繰り返しているうちに、利用者端末は、自動的に、仮想マシン 2 にアクセスすることが可能になる。

30

【 0 0 2 6 】

ここで、ライブマイグレーションに伴って V P N 間接続管理システム 1 0 0 側に発生する処理時間は、ステップ S 4 においてライブマイグレーションの実行が開始されてから、ステップ S 1 0 においてルーティングが切り替えられるまでの時間であるといえる。この点、第 1 の実施形態に係る V P N 間接続管理システム 1 0 0 は、ライブマイグレーションの実行開始を検知し、これを契機として、アドレス変換装置 2 に対する設定を開始する。すなわち、ライブマイグレーションの実行と経路の構築とが、併行して進められることになる。この結果、ライブマイグレーションに伴って発生する処理時間は、ライブマイグレーションの実行時間と経路の構築時間とを足し合わせた時間ではなく、原理的には、ライブマイグレーションの実行時間又は経路の構築時間のいずれか長い方の時間でほぼ済むことになる。

40

【 0 0 2 7 】

なお、ライブマイグレーションの処理手順は図 2 に示す処理手順に限られるものではない。例えば、ライブマイグレーション処理部 1 0 は、ライブマイグレーションの実行指示（ステップ S 2 ）においてライブマイグレーションの実行開始を検知し、実行確認通知の

50

受信（ステップ S 3）より前にステップ S 5 の処理を開始してもよい。また、アドレス変換装置 2 の設定完了通知（ステップ S 7）、及びライブマイグレーションの実行完了通知（ステップ S 8）の順序が逆になる場合もある。また、ライブマイグレーションの実行完了通知（ステップ S 8）は、マイグレーション元の仮想マシン 1 からではなく、マイグレーション先の仮想マシン 2 から受信してもよい。

【 0 0 2 8 】

[第 1 の実施形態に係る V P N 間接続管理システムの構成]

図 3 は、第 1 の実施形態に係る V P N 間接続管理システム 1 0 0 の構成を示すブロック図である。図 3 に示すように、V P N 間接続管理システム 1 0 0 は、ライブマイグレーション処理部 1 0 と、V P N 間接続処理部 2 0 とを備える。

10

【 0 0 2 9 】

ライブマイグレーション処理部 1 0 は、顧客ネットワーク設定記憶部 1 1 と、通信部 1 2 と、入力部 1 3 と、設定指示送信部 1 4 と、ライブマイグレーション実行部 1 5 と、アドレス変換設定指示部 1 6 と、ルーティング設定指示部 1 7 とを備える。

【 0 0 3 0 】

顧客ネットワーク設定記憶部 1 1 は、V P N 間接続サービスの提供先である顧客のネットワーク設定情報を記憶する。図 4 は、第 1 の実施形態に係る顧客ネットワーク設定記憶部を説明するための図である。図 4 に示すように、顧客ネットワーク設定記憶部 1 1 は、顧客毎に、仮想マシン、アドレス変換装置 1 ~ 3、及び集合仮想ルータに関するネットワーク設定情報を記憶する。以下、図 4 とともに図 5 を参照しながら、ネットワーク設定情報を説明する。図 5 は、第 1 の実施形態における I P アドレスの割り当てを説明するための図である。

20

【 0 0 3 1 】

図 4 に示すように、顧客ネットワーク設定記憶部 1 1 は、仮想マシンに関するネットワーク設定情報として、マイグレーション元の仮想マシン 1 の I P (Internet Protocol) アドレス「192.168.1.10」及びその制御用の I P アドレス「172.16.100.1」、並びに、マイグレーション先の仮想マシン 2 の制御用の I P アドレス「172.16.100.2」を記憶する。なお、第 1 の実施形態において、これらの I P アドレスは、サブネットマスクが 2 4 ビットである。

【 0 0 3 2 】

図 5 を参照すると、V P N 1 (データセンタ 1) に設置された仮想マシン 1 の I P アドレスは、「192.168.1.10」である。この I P アドレスは、V P N 1 内で仮想マシン 1 を一意に識別するためのアドレスである。また、図 5 に示すように、データセンタ 1 は、制御用のインタフェースを有し、そのインタフェースの I P アドレスが、「172.16.100.1」である。また、データセンタ 2 も、制御用のインタフェースを有し、そのインタフェースの I P アドレスが、「172.16.100.2」である。V P N 間接続管理システム 1 0 0 は、図示しない制御用のネットワークによってこのインタフェースと接続され、制御用の I P アドレス「172.16.100.1」及び「172.16.100.2」を用いて、ライブマイグレーションの実行指示などを行う。

30

【 0 0 3 3 】

図 4 に戻り、顧客ネットワーク設定記憶部 1 1 は、アドレス変換装置 1 ~ 3 に関するネットワーク設定情報として、制御用の I P アドレスやアドレス変換情報を記憶する。図 5 を参照すると、第 1 の実施形態においては、V P N 3 に設置された利用者端末が V P N 1 に設置された仮想マシン 1 にアクセスするための経路が、現用の経路として既に構築されていることを想定する。すなわち、アドレス変換装置 3 及びアドレス変換装置 1 には、既にアドレス変換情報が設定されているという想定である。そこで、顧客ネットワーク設定記憶部 1 1 は、アドレス変換装置 3 及びアドレス変換装置 1 に関しては、制御用の I P アドレスの他に、アドレス変換情報も記憶する。

40

【 0 0 3 4 】

アドレス変換装置 3 に設定されているアドレス変換情報は、「192.168.1.10」と「10.0

50

.1.10」とを相互に変換すること、及び、「172.16.2.10」と「10.0.2.10」とを相互に変換することを示す。一方、アドレス変換装置1に設定されているアドレス変換情報は、「192.168.1.10」と「10.0.2.10」とを相互に変換すること、及び、「172.16.1.10」と「10.0.1.10」とを相互に変換することを示す。

【0035】

また、顧客ネットワーク設定記憶部11は、集合仮想ルータに関するネットワーク設定情報として、制御用のIPアドレスやルーティング情報を記憶する。例えば、ルーティング情報(現用)「宛先10.0.2.10:ゲートウェイ10.0.20.97」は、図5に示す仮想ルータにおいて、宛先が「10.0.2.10」の packets を受信した場合には、「10.0.20.97」のインタフェースにルーティングすることを示す。

10

【0036】

アドレス変換及びルーティングについて一例を挙げて説明する。例えば利用者端末から仮想マシン1宛に送信された packets は、アドレス変換されながら、仮想マシン1によって受信される。

【0037】

まず、利用者端末は、仮想マシン1のIPアドレスを「172.16.2.10」として把握している。一方、仮想マシン1は、利用者端末のIPアドレスを「172.16.1.10」として把握している。また、集合仮想ルータの仮想ルータは、利用者端末のIPアドレスを「10.0.1.10」として把握し、仮想マシン1のIPアドレスを「10.0.2.10」として把握している。

20

【0038】

利用者端末が仮想マシン1にアクセスする場合、利用者端末は、宛先を「172.16.2.10」、送信元を「192.168.1.10」とする packets を送信する。すると、アドレス変換装置3は、アドレス変換情報に従って、「172.16.2.10」を「10.0.2.10」に変換し、「192.168.1.10」を「10.0.1.10」に変換する。この結果、利用者端末が送信した packets は、宛先が「10.0.2.10」であり、送信元が「10.0.1.10」である packets となる。

【0039】

仮想ルータは、ルーティング情報に従ってルーティングを行う。この場合、宛先が「10.0.2.10」の packets であるので、仮想ルータは、「10.0.20.97」のインタフェースにこの packets をルーティングする。続いて、アドレス変換装置1は、アドレス変換情報に従って、「10.0.2.10」を「192.168.1.10」に変換し、「10.0.1.10」を「172.16.1.10」に変換する。この結果、利用者端末が送信した packets は、宛先が「192.168.1.10」であり、送信元が「172.16.1.10」である packets となる。図5を参照すると、仮想マシン1のIPアドレスは、「192.168.1.10」である。このため、この packets は、仮想マシン1によって受信される。このように、利用者端末から仮想マシン1宛に送信された packets は、アドレス変換されながら、仮想マシン1によって受信される。なお、図4や図5において図示を省略したが、仮想マシン1から利用者端末宛に送信された packets も同様に、アドレス変換されながら、利用者端末によって受信される。

30

【0040】

図3に戻り、通信部12は、IP通信の一般的なインタフェースであり、例えば、データセンタ1やデータセンタ2との間で制御用のネットワークを介して通信を行う。入力部13は、キーボードやマウスなどである。設定指示送信部14は、VPN間接続管理システム100内部のインタフェースであり、VPN間接続処理部20との間で情報の送受信を行う。

40

【0041】

第1の実施形態においては、VPN間接続管理システム100のオペレータが、VPN間接続サービスを遠隔監視し、例えば仮想マシン1の負荷が高いといった状況を判断した場合に、入力部13を用いて、顧客ID「000001」とともにライブマイグレーションの実行指示を入力する。

【0042】

50

ライブマイグレーション実行部 15 は、入力部 13 から顧客 ID とともにライブマイグレーションの実行指示を受け付けると、ライブマイグレーションの実行指示を、仮想マシン 1 に対して送信する。具体的には、ライブマイグレーション実行部 15 は、顧客 ID を用いて顧客ネットワーク設定記憶部 11 を参照し、マイグレーション元の仮想マシン 1 の IP アドレス「192.168.1.10」及びその制御用の IP アドレス「172.16.100.1」、並びに、マイグレーション先の仮想マシン 2 の制御用の IP アドレス「172.16.100.2」を取得する。そして、ライブマイグレーション実行部 15 は、データセンタ 1 との間で通信を行い、マイグレーション元を仮想マシン 1 とし、マイグレーション先を仮想マシン 2 とするライブマイグレーションの実行指示を、ライブマイグレーションに必要な IP アドレスなどとともに送信する。

10

【 0 0 4 3 】

また、ライブマイグレーション実行部 15 は、ライブマイグレーションの実行確認通知を仮想マシン 1 から受信すると、ライブマイグレーションの実行開始を検知したことを、顧客 ID とともにアドレス変換設定指示部 16 に対して通知する。

【 0 0 4 4 】

アドレス変換設定指示部 16 は、ライブマイグレーションの実行開始を検知したことの通知を顧客 ID とともにライブマイグレーション実行部 15 から受け付けると、顧客 ID を用いて顧客ネットワーク設定記憶部 11 を参照し、アドレス変換装置 1 の制御用の IP アドレス「172.16.10.1」及びアドレス変換情報、並びに、アドレス変換装置 2 の制御用の IP アドレス「172.16.10.2」を取得する。そして、アドレス変換設定指示部 16 は、V P N 間接続処理部 20 に対して、アドレス変換装置 2 に対する設定指示を、設定に必要なアドレス変換情報などとともに送信する。なお、アドレス変換設定指示部 16 は、設定指示情報のヘッダに、例えば「T - N A T」などの引数を付与する。

20

【 0 0 4 5 】

また、アドレス変換設定指示部 16 は、アドレス変換装置 2 に対する設定完了通知を V P N 間接続処理部 20 から受信すると、アドレス変換装置 2 に対する設定が完了したことを、顧客 ID とともにルーティング設定指示部 17 に対して通知する。

【 0 0 4 6 】

ルーティング設定指示部 17 は、ライブマイグレーションの実行完了通知を仮想マシン 1 から受信し、かつ、アドレス変換装置 2 に対する設定が完了したことの通知をアドレス変換設定指示部 16 から受け付けると、顧客 ID を用いて顧客ネットワーク設定記憶部 11 を参照し、集合仮想ルータの制御用の IP アドレス及びルーティング情報（予備）を取得する。そして、ルーティング設定指示部 17 は、V P N 間接続処理部 20 に対して、集合仮想ルータに対する設定指示を、設定に必要なルーティング情報などとともに送信する。なお、ルーティング設定指示部 17 は、設定指示情報のヘッダに、例えば「V R」などの引数を付与する。

30

【 0 0 4 7 】

一方、V P N 間接続処理部 20 は、ネットワーク装置設定記憶部 21 と、通信部 22 と、設定指示受信部 23 と、アドレス変換設定部 24 と、ルーティング設定部 25 とを備える。

40

【 0 0 4 8 】

ネットワーク装置設定記憶部 21 は、ネットワーク装置に対して設定を行うための情報を記憶する。図 6 は、第 1 の実施形態に係るネットワーク装置設定記憶部を説明するための図である。図 6 に示すように、ネットワーク装置設定記憶部 21 は、アドレス変換装置 1 ~ 3、及び集合仮想ルータについて、制御用の IP アドレス及びパスワードを記憶する。なお、図 6 は、ネットワーク装置設定記憶部 21 が記憶する情報の一部を例示するものである。

【 0 0 4 9 】

図 3 に戻り、通信部 22 は、I P 通信用の一般的なインタフェースであり、例えば、アドレス変換装置 1 ~ 3 や集合仮想ルータとの間で制御用のネットワークを介して通信を行

50

う。設定指示受信部 23 は、VPN 間接続管理システム 100 内部のインタフェースであり、ライブマイグレーション処理部 10 との間で情報の送受信を行う。なお、設定指示受信部 23 は、引数「T-NAT」がヘッダに含まれる設定指示情報については、アドレス変換設定部 24 に提供し、引数「VR」がヘッダに含まれる設定指示情報については、ルーティング設定部 25 に提供する。

【0050】

アドレス変換設定部 24 は、アドレス変換装置 2 に対する設定指示を、設定に必要なアドレス変換情報などとともにアドレス変換設定指示部 16 から受信すると、ネットワーク装置設定記憶部 21 を参照し、アドレス変換装置 2 の制御用の IP アドレス「172.16.10.2」及びパスワード「hoge hoge02」を取得する。そして、アドレス変換設定部 24 は、制御用の IP アドレス「172.16.10.2」及びパスワード「hoge hoge02」を用いてアドレス変換装置 2 にアクセスし、アドレス変換設定指示部 16 から受信したアドレス変換情報を設定する。すなわち、アドレス変換装置 2 には、アドレス変換装置 1 に設定されていたアドレス変換情報と同一内容のアドレス変換情報が設定される。

10

【0051】

なお、アドレス変換設定部 24 は、アドレス変換装置 2 にアクセスする際に、例えば、アタッチメントを利用すればよい。アタッチメントは、アドレス変換情報をアドレス変換装置 2 に対して反映するためのプログラム、及び、ルーティング情報を集合仮想ルータに対して反映するためのプログラムを含む。

20

【0052】

具体的には、アタッチメントには、VPN 間接続管理システム 100 とアドレス変換装置 2 との間で用いられる通信プロトコルや、VPN 間接続管理システム 100 と集合仮想ルータの間で用いられる通信プロトコルが規定される。また、アタッチメントには、アドレス変換装置 2 や集合仮想ルータにログインするための ID / パスワードや、アドレス変換情報やルーティング情報を格納すべきパスを指定し、指定したパスにアドレス変換情報やルーティング情報を格納するためのコマンド、アドレス変換装置 2 や集合仮想ルータを再起動させるコマンドなどが記載される。なお、アドレス変換情報やルーティング情報の反映には、格納して再起動することで反映する場合と、格納によって反映する場合とがある。なお、一般に、通信プロトコルには、アドレス変換装置 2 のベンダや集合仮想ルータのベンダによって規定される独自仕様の通信プロトコルが用いられる。VPN 間接続処理部 20 は、例えば VPN 間接続管理システム 100 のオペレータに入力されることで、アタッチメントを事前に記憶する。

30

【0053】

また、アドレス変換設定部 24 は、アドレス変換装置 2 に対する設定が完了すると、アドレス変換装置 2 に対する設定が完了したことを、アドレス変換設定指示部 16 に対して通知する。

【0054】

ルーティング設定部 25 は、集合仮想ルータに対する設定指示を、設定に必要なルーティング情報などとともにルーティング設定指示部 17 から受信すると、ネットワーク装置設定記憶部 21 を参照し、集合仮想ルータの制御用の IP アドレス「172.16.10.4」及びパスワード「hoge hoge」を取得する。そして、ルーティング設定部 25 は、制御用の IP アドレス「172.16.10.4」及びパスワード「hoge hoge」を用いて集合仮想ルータにアクセスし、ルーティング設定指示部 17 から受信したルーティング情報を設定する。

40

【0055】

すなわち、利用者端末から仮想マシン 1 にアクセスするための経路から、利用者端末から仮想マシン 2 にアクセスするための経路に、現用の経路（ルーティング）を切り替える。図 5 を用いて説明すると、仮想ルータのインタフェース「10.0.10.97」からインタフェース「10.0.20.97」にルーティングされていたパケットは、ルーティング切替後、インタフェース「10.0.10.97」からインタフェース「10.0.30.97」にルーティングされる。なお、ルーティング設定部 25 は、集合仮想ルータにアクセスする際に、例えば、上述したア

50

タッチメントを利用すればよい。

【 0 0 5 6 】

[第 1 の実施形態の効果]

上述したように、第 1 の実施形態に係る V P N 間接続管理システム 1 0 0 は、ライブマイグレーションの実行開始を検知し、これを契機として、ネットワーク装置に対する設定を開始する。すなわち、ライブマイグレーションの実行と経路の構築とが、併行して進められることになる。この結果、ライブマイグレーションに伴って V P N 間接続管理システム 1 0 0 側に発生する処理時間は、ライブマイグレーションの実行時間と経路の構築時間とを足し合わせた時間ではなく、原理的には、ライブマイグレーションの実行時間又は経路の構築時間のいずれか長い方の時間でほぼ済むことになる。よって、ライブマイグレーションに伴って発生する処理時間が短縮される。

10

【 0 0 5 7 】

また、第 1 の実施形態に係る V P N 間接続管理システム 1 0 0 は、マイグレーション元のアドレス変換装置に設定されていたアドレス変換情報と同一内容のアドレス変換情報を、マイグレーション先のアドレス変換装置に対して設定する。例えば、マイグレーション先のデータセンタ 2 が、マイグレーション元のデータセンタ 1 の予備系として運用されている場合などに可能である。すなわち、マイグレーション先のデータセンタ 2 において、マイグレーション元のデータセンタ 1 で用いられる I P アドレスが、空きの I P アドレスとして予め確保されていれば、マイグレーション元のアドレス変換装置に設定されていたアドレス変換情報をマイグレーション先のアドレス変換装置に対して複製するだけで済むことになる。なお、例えば、偶然空きの I P アドレスである場合にも、マイグレーション元のアドレス変換装置に設定されていたアドレス変換情報と同一内容のアドレス変換情報を、マイグレーション先のアドレス変換装置に対して設定すればよい。

20

【 0 0 5 8 】

[第 1 の実施形態の変形例]

続いて、第 1 の実施形態の変形例を説明する。

【 0 0 5 9 】

(変形例 1)

第 1 の実施形態においては、データセンタ 1 とデータセンタ 2 とが専用線で接続され、ライブマイグレーションの通信路として専用線を用いる例を説明したが、これに限られるものではない。図 7 は、第 1 の実施形態の変形例を説明するための図である。図 7 に示すように、ライブマイグレーションの通信路として V P N 間接続サービスを用いることも可能である。なお、一般的に、ライブマイグレーションの通信路として構築された経路には、ライブマイグレーションの実行に伴う設定変更は発生しない。

30

【 0 0 6 0 】

(変形例 2)

第 1 の実施形態においては、オペレータが、V P N 間接続サービスを遠隔監視し、例えば仮想マシン 1 の負荷が高いといった状況を判断した場合に、ライブマイグレーションの実行指示を入力する例を説明したが、これに限られるものではない。例えば、V P N 間接続管理システム 1 0 0 が、遠隔監視を行うプログラムを実行することで、仮想マシン 1 の C P U (Central Processing Unit) の負荷状況やネットワークの使用帯域を監視し、例えば所定の閾値を超過したことを条件として、ライブマイグレーションの実行を決定してもよい。すなわち、オペレータによる手動ではなく、自動化してもよい。

40

【 0 0 6 1 】

反対に、第 1 の実施形態においては、その後の処理を全て自動化する例を説明したが、これに限られるものではない。例えば、ライブマイグレーションの実行開始を検知したことを通知する情報を、V P N 間接続管理システム 1 0 0 が備える出力部に出力し、オペレータが、これを契機として、ネットワーク装置に対する設定開始指示を入力してもよい。また、例えば、ライブマイグレーションの実行が完了し、かつ、アドレス変換装置に対する設定が完了したことを通知する情報を、V P N 間接続管理システム 1 0 0 が備える出力

50

部に出力し、オペレータが、これを確認してから、ルーティングを切り替える指示を入力してもよい。なお、その他の処理も、運用の形態などに応じて、オペレータによる手動に置き換えることが可能である。

【0062】

(変形例3)

第1の実施形態においては、VPN間接続管理システム100の構成として図3を例示したが、これに限られるものではない。まず、上述したように、VPN間接続管理システム100は、VPN間接続サービスを管理し、経路を構築するシステムであり、例えばオンデマンド(On Demand)な要求にも対応するものである。このため、VPN間接続管理システム100は、このようなVPN間接続サービスを提供するために必要な情報をさら

10

【0063】

また、顧客ネットワーク設定記憶部11やネットワーク装置設定記憶部21も、第1の実施形態において説明したものに限られない。ライブマイグレーション処理部11側で記憶する情報として説明した情報を、VPN間接続処理部20側で記憶してもよいし、またその逆でもよい。また、情報の記憶方法(テーブル構造)も、任意に変更することができる。また、説明を省略したが、例えば仮想ルータを識別する必要がある場合、仮想ルータの識別情報とともに記憶し、この識別情報を用いて制御を行ってもよい。

【0064】

また、必ずしもライブマイグレーション処理部11とVPN間接続処理部20とに分か

20

【0065】

(第2の実施形態)

続いて、第2の実施形態を説明する。第1の実施形態においては、マイグレーション元のアドレス変換装置に設定されていたアドレス変換情報と同一内容のアドレス変換情報を、マイグレーション先のアドレス変換装置に対して設定することを想定した。例えば、設定しようとするIPアドレスが、マイグレーション先において、予め確保されたIPアドレスであるか、あるいは偶然空きのIPアドレスである場合などに有効である。

【0066】

第2の実施形態においては、新たなIPアドレスを払い出し、新たなアドレス変換情報を生成して設定することを想定する。例えば、マイグレーション元で使用されていたIPアドレスが、マイグレーション先において、使用中のIPアドレスであるか、あるいは予約済みのIPアドレスである場合に有効である。また、単に、ライブマイグレーション実行時には新たなIPアドレスを払い出す、といった運用の場合にも有効である。なお、第2の実施形態に係るVPN間接続管理システム100の構成は、第1の実施形態と同様である。

30

【0067】

なお、マイグレーション元の仮想マシンのIPアドレスと、マイグレーション先の仮想マシンのIPアドレスとが異なるIPアドレスである場合に、ライブマイグレーションを実現する技術は、公知の技術であるグローバルライブマイグレーションを用いればよい(例えば、渡邊英伸ら、「IPモビリティと複数インタフェースを用いたグローバルライブマイグレーション」、電子情報通信学会論文誌VOL.J93-B NO.7 JULY2010、P.893-901)。例えば同文献には、IPモビリティの技術を応用して実現することが記載されている。IPモビリティは、端末に割り振られたIPアドレスが端末の移動に伴い変更された場合でも、移動前に行っていた通信を継続する技術である。

40

【0068】

なお、「マイグレーション先の仮想マシンのIPアドレス」がライブマイグレーションの実行前に決定されていることを前提とする手法を用いる場合には、VPN間接続管理システム100は、例えば図2のステップS2よりも前に、「マイグレーション先の仮想マシンのIPアドレス」を決定すればよい。このような手法を用いない場合には、「マイグ

50

レーション先の仮想マシンのIPアドレス」は、ライブマイグレーションにおいて必要となる任意の段階で決定されればよい。

【0069】

[Twice - NATの適用]

IPアドレスの払い出しについて説明する前に、まず、VPN間通信システムに適用されるアドレス変換の技術「Twice - NAT」を説明する。Twice - NATは、IETF (Internet Engineering Task Force) によって公開されたRFC (Request for Comments) 2663の技術である。

【0070】

Twice - NATとは、送信元のIPアドレス及び宛先のIPアドレスの双方を変換する技術である。以下、あるVPN間接続サービスを利用する利用者端末や仮想マシンを、この利用者端末や仮想マシンが設置された自VPN内で一意に識別するためのIPアドレスを、「自VPN内アドレス」と呼ぶ。また、通信相手となる他のVPNに設置された利用者端末や仮想マシンを、自VPN内で一意に識別するためのIPアドレスを、「第一アドレス」と呼ぶ。また、あるVPN間接続サービスを利用する利用者端末や仮想ルータを仮想ルータにて一意に識別するためのIPアドレスを、「第二アドレス」と呼ぶ。

【0071】

図8は、第2の実施形態におけるTwice - NATを説明するための図である。図8において、「 a_i 」は、 VPN_i 内で利用者端末を一意に識別するための自VPN内アドレスであり、「 a_j 」は、 VPN_j 内で仮想マシン1を一意に識別するための自VPN内アドレスである。また、図8において図示を省略しているが、 VPN_i 、 VPN_j 以外の他のVPNである VPN_k も、VPN間接続サービスの提供を受ける。「 a_k 」は、 VPN_k 内で端末を一意に識別するための自VPN内アドレスである。なお、 i 、 j 及び k は、互いに独立な正の整数値であり、ここでは特に $i \neq j$ 、 $j \neq k$ 、 $k \neq i$ である。また、(1)は、 VPN_i から仮想ルータ(VRF_m(Virtual Routing and Forwarding))向けのアドレス変換を表す変換作用素である。また、(2)は、仮想ルータ(VRF_m)から VPN_j 向けのアドレス変換を表す変換作用素である。ここで、 m 及び n は、仮想ルータを識別する互いに独立な正の整数値であり、ここでは特に $m \neq n$ である。

【数1】

$$\hat{\eta}_m^i \dots (1)$$

【数2】

$$\hat{\xi}_j^m \dots (2)$$

【0072】

したがって、図8において、仮想ルータ(VRF_m)によって提供されるVPN間接続サービスを利用する VPN_i 配下の利用者端末及び VPN_j 配下の仮想マシン1を、仮想ルータ(VRF_m)にて一意に識別するための第二アドレスは、自VPN内アドレス「 a_i 」及び自VPN内アドレス「 a_j 」がそれぞれアドレス変換装置によって1回変換されたIPアドレスとなり、(3)と表現される。

【数3】

$$\{\hat{\eta}_m^i a_i, \hat{\eta}_m^j a_j\} \dots (3)$$

【0073】

また、図8において、 VPN_j 配下の仮想マシン1を VPN_i 内で一意に識別するための第一アドレスは、(4)となる。同様に、 VPN_i 配下の利用者端末を VPN_j 内で一意に識別するための第一アドレスは、(5)となる。

【数 4】

$$\xi_i^m \hat{\eta}_m^j a_j \quad \dots(4)$$

【数 5】

$$\xi_j^m \hat{\eta}_m^i a_i \quad \dots(5)$$

【0074】

VPN間接続管理システム100は、オンデマンドにVPN間接続サービスを提供する場合、この提供にあたり、第一アドレス及び第二アドレスを払い出し、アドレス変換情報を生成し、アドレス変換装置に対する設定を行う。具体的には、VPN間接続管理システム100は、(6)式を満たすように、第一アドレスを決定する。(6)式の右辺は、VPN_i内の端末にとって通信相手となり得るVPN_k配下の端末(VPN_i内の端末とVPN_k内の端末とは仮想ルータ(VRF_n)によってVPN間接続)をVPN_i内で一意に識別するための第一アドレスである。すなわち、VPN_j配下の仮想マシン1をVPN_i内で一意に識別するための第一アドレスと、VPN_k配下の端末をVPN_i内で一意に識別するための第一アドレスとは、異なるものでなければならない。したがって、(6)式は、「第一アドレスは、VPN_iに設置された利用者端末と仮想マシン1との間にVPN間接続サービスが提供される時間帯において、VPN_i内で利用される第一アドレスの中で一意に識別されるように払い出されなければならない」ことを示し、結局、第一アドレスには、VPN_i内でその時間帯に利用されていない(あるいはその時間帯に利用される予定のない)IPアドレスが用いられる。なお、(7)式及び(8)式も満たさなければならない。

10

20

【数 6】

$$\xi_i^m \hat{\eta}_m^j a_j \neq \xi_i^n \hat{\eta}_n^k a_k \quad (m \neq n, i \neq j, j \neq k, k \neq i) \quad \dots(6)$$

【数 7】

$$\xi_i^m \hat{\eta}_m^j a_j \neq a_i \quad (i \neq j) \quad \dots(7)$$

30

【数 8】

$$\xi_i^n \hat{\eta}_n^k a_k \neq a_i \quad (i \neq k) \quad \dots(8)$$

【0075】

また、VPN間接続管理システム100は、(9)式を満たすように、第一アドレスを決定する。(9)式の右辺は、VPN_j内の端末にとって通信相手となり得るVPN_k配下の端末(VPN_j内の端末とVPN_k内の端末とは仮想ルータ(VRF_n)によってVPN間接続)をVPN_j内で一意に識別するための第一アドレスである。すなわち、VPN_j配下の利用者端末をVPN_j内で一意に識別するための第一アドレスと、VPN_k配下の端末をVPN_j内で一意に識別するための第一アドレスとは、異なるものでなければならない。したがって、(9)式は、「第一アドレスは、VPN_jに設置された利用者端末と仮想マシン1との間にVPN間接続サービスが提供される時間帯において、VPN_j内で利用される第一アドレスの中で一意に識別されるように払い出されなければならない」ことを示し、結局、第一アドレスには、VPN_j内でその時間帯に利用されていない(あるいはその時間帯に利用される予定のない)IPアドレスが用いられる。なお、(10)式及び(11)式も満たさなければならない。

40

【数 9】

$$\hat{\xi}_j^m \hat{\eta}_m^i a_i \neq \hat{\xi}_j^n \hat{\eta}_n^k a_k \quad (m \neq n, i \neq j, j \neq k, k \neq i) \quad \dots(9)$$

【数 10】

$$\hat{\xi}_j^m \hat{\eta}_m^i a_i \neq a_j \quad (j \neq i) \quad \dots(10)$$

【数 11】

$$\hat{\xi}_j^n \hat{\eta}_n^k a_k \neq a_k \quad (j \neq k) \quad \dots(11)$$

10

【0076】

また、VPN間接続管理システム100は、例えば(12)式を満たすように、第二アドレスを決定する。(12)式は、「第二アドレスは、VPN_iに設置された利用者端末と仮想マシン1との間にVPN間接続サービスが提供される時間帯において、同じ仮想ルータ内で一意に識別されるように払い出されなければならない」ことを示す。

【数 12】

$$\hat{\eta}_m^i a_i \neq \hat{\eta}_m^j a_j \quad (i \neq j) \quad \dots(12)$$

20

【0077】

このように、VPN間接続管理システム100は、「Twice-NAT」及び「仮想ルータ」の技術を用いてIPアドレス空間を独立化することで、IPアドレスの競合を解決しつつ、IPアドレスの割り当てを簡易化している。具体的には、まず、「Twice-NAT」により、VPNと仮想ルータとの間で、IPアドレス空間を垂直方向に分離する(図8の白抜き矢印を参照)。また、「仮想ルータ」により、集合仮想ルータに設定された仮想ルータ間で、IPアドレス空間を水平方向に分離する(図8の白抜き矢印を参照)。そして、VPN間接続管理システム100は、この両者を組み合わせることにより、IPアドレス空間を、各VPN内、各仮想ルータ内にそれぞれ独立化させ、IPアドレスの競合を解決しつつ、IPアドレスの割り当てを簡易化している。

30

【0078】

このように、Twice-NATによるアドレス変換は、Single-NATによるアドレス変換と比較して、利便性が高い。この点について、具体的なIPアドレスを例に挙げて説明する。

【0079】

図9は、Single-NATによるアドレス変換を説明するための図である。まず、VPN3に設置された利用者端末をVPN3内で一意に識別するIPアドレスは、「192.168.1.10」である。このIPアドレス「192.168.1.10」は、外部には通知されない。すなわち、アドレス変換装置3が、IPアドレス「192.168.1.10」をIPアドレス「172.16.1.10」に変換することで、利用者端末の外部向けのIPアドレスは、「172.16.1.10」となる。このため、仮想ルータや、仮想マシン1が設置されたVPN1において、利用者端末を一意に識別するIPアドレスは、「172.16.1.10」である。

40

【0080】

一方、VPN1に設置された仮想マシン1をVPN1内で一意に識別するIPアドレスは、「192.168.1.10」である。このIPアドレス「192.168.1.10」は、外部には通知されない。すなわち、アドレス変換装置1が、IPアドレス「192.168.1.10」をIPアドレス「172.16.2.10」に変換することで、仮想マシン1の外部向けのIPアドレスは、「172.16.2.10」となる。このため、仮想ルータや、利用者端末が設置されたVPN3において、仮想マシン1を一意に識別するIPアドレスは、「172.16.2.10」である。

50

【 0 0 8 1 】

ここで、ライブマイグレーションの実行前、利用者端末は、宛先を「172.16.2.10」、送信元を「192.168.1.10」とするパケットを送信するので、アドレス変換装置3は、アドレス変換情報に従って、「192.168.1.10」を「172.16.1.10」に変換する。この結果、利用者端末が送信したパケットは、宛先が「172.16.2.10」であり、送信元が「172.16.1.10」であるパケットとなる。

【 0 0 8 2 】

仮想ルータは、ルーティング情報に従ってルーティングを行う。この場合、宛先が「172.16.2.10」のパケットであるので、仮想ルータは、アドレス変換装置1に向けて、このパケットをルーティングする。続いて、アドレス変換装置1は、アドレス変換情報に従って、「172.16.2.10」を「192.168.1.10」に変換する。この結果、利用者端末が送信したパケットは、宛先が「192.168.1.10」であり、送信元が「172.16.1.10」であるパケットとなる。ここで、仮想マシン1のIPアドレスは、「192.168.1.10」であるので、このパケットは、仮想マシン1に到達する。

10

【 0 0 8 3 】

一方、ライブマイグレーションの実行完了後、仮想ルータは、宛先が「172.16.2.10」であり、送信元が「172.16.1.10」であるパケットを、今度はアドレス変換装置2に向けてルーティングする。ここで、アドレス変換装置2は、宛先のIPアドレスのアドレス変換を行うが、送信元のIPアドレスのアドレス変換は行わない。すなわち、送信元のIPアドレス「172.16.1.10」は、そのままVPN2内に到達する。このため、マイグレーション先のVPN2においては、利用者端末を一意に識別するためのIPアドレスとして「172.16.1.10」を利用することが『必須』となる。仮に、VPN2内で、既に「172.16.1.10」を使用中や予約済みである場合、仮想ルータやアドレス変換装置3においても、IPアドレスを見直さなければならない。

20

【 0 0 8 4 】

図10は、Twice-NATによるアドレス変換を説明するための図である。まず、VPN3に設置された利用者端末をVPN3内で一意に識別するIPアドレスは、「192.168.1.10」である。このIPアドレス「192.168.1.10」は、外部には通知されない。すなわち、アドレス変換装置3が、IPアドレス「192.168.1.10」をIPアドレス「10.0.1.10」に変換する。このため、仮想ルータにおいて、利用者端末を一意に識別するIPアドレスは、「10.0.1.10」となる。また、アドレス変換装置1が、IPアドレス「10.0.1.10」をIPアドレス「172.16.1.10」に変換する。このため、仮想マシン1が設置されたVPN1において、利用者端末を一意に識別するIPアドレスは、「172.16.1.10」となる。

30

【 0 0 8 5 】

一方、VPN1に設置された仮想マシン1をVPN1内で一意に識別するIPアドレスは、「192.168.1.10」である。このIPアドレス「192.168.1.10」は、外部には通知されない。すなわち、アドレス変換装置1が、IPアドレス「192.168.1.10」をIPアドレス「10.0.2.10」に変換する。このため、仮想ルータにおいて、仮想マシン1を一意に識別するIPアドレスは、「10.0.2.10」となる。また、アドレス変換装置3が、IPアドレス「10.0.2.10」をIPアドレス「172.16.2.10」に変換する。このため、利用者端末が設置されたVPN3において、仮想マシン1を一意に識別するIPアドレスは、「172.16.2.10」となる。

40

【 0 0 8 6 】

ここで、ライブマイグレーションの実行前、利用者端末は、宛先を「172.16.2.10」、送信元を「192.168.1.10」とするパケットを送信するので、アドレス変換装置3は、アドレス変換情報に従って、宛先のIPアドレス「172.16.2.10」を「10.0.2.10」に変換し、送信元のIPアドレス「192.168.1.10」を「10.0.1.10」に変換する。この結果、利用者端末が送信したパケットは、宛先が「10.0.2.10」であり、送信元が「10.0.1.10」であるパケットとなる。

50

【 0 0 8 7 】

仮想ルータは、ルーティング情報に従ってルーティングを行う。この場合、宛先が「10.0.2.10」の packets であるので、仮想ルータは、アドレス変換装置 1 に向けて、この packets をルーティングする。続いて、アドレス変換装置 1 は、アドレス変換情報に従って、宛先の IP アドレス「10.0.2.10」を「192.168.1.10」に変換し、送信元の IP アドレス「10.0.1.10」を「172.16.1.10」に変換する。この結果、利用者端末が送信した packets は、宛先が「192.168.1.10」であり、送信元が「172.16.1.10」である packets となる。仮想マシン 1 の IP アドレスは、「192.168.1.10」であるので、この packets は、仮想マシン 1 に到達する。

【 0 0 8 8 】

一方、ライブマイグレーションの実行完了後、仮想ルータは、宛先が「10.0.2.10」であり、送信元が「10.0.1.10」である packets を、今度はアドレス変換装置 2 に向けてルーティングする。ここで、アドレス変換装置 2 は、宛先の IP アドレス及び送信元の IP アドレスの双方を変換する。すなわち、Single-NAT の場合のように、送信元の IP アドレスがそのまま VPN 2 内に到達することはない。このため、マイグレーション先の VPN 2 においては、利用者端末を一意に識別するための IP アドレスとして「172.16.1.10」を利用することが必須ではなく、少なくとも利用者端末と仮想マシン 2 との間に VPN 間接続サービスが提供される時間帯において、VPN 2 内で利用される IP アドレスの中で一意に選択されればよい。図 10 において、「VPN 2 内で利用者端末を一意に識別」する IP アドレスが『選択可』であると記載する理由は、「VPN 2 内で利用者端末を一意に識別」する IP アドレスとして「172.16.1.10」を利用することが必須ではないという意味である。また、図 10 において、「VPN 2 内で仮想マシン 2 を一意に識別する」IP アドレスが『既存』であると記載する理由は、「VPN 2 内で仮想マシン 2 を一意に識別する」IP アドレスが必ずしも仮想マシン 1 を一意に識別する IP アドレスと同一であることが必須ではなく、既存の IP アドレスを利用してもよいという意味である。

【 0 0 8 9 】

このように、VPN 間接続管理システム 100 は、IP アドレス空間を独立化することで、IP アドレスの競合を解決しつつ、IP アドレスの割り当てを簡易化している。

【 0 0 9 0 】

[IP アドレスの払い出し]

さて、第 2 の実施形態においては、アドレス変換設定指示部 16 又はアドレス変換設定部 24 が、新たな IP アドレスの払い出しと、新たなアドレス変換情報の生成とを行う。以下、一例として、アドレス変換設定指示部 16 が新たな IP アドレスの払い出しと、新たなアドレス変換情報の生成とを行う場合を説明する。

【 0 0 9 1 】

ここで、アドレス変換設定指示部 16 が払い出しの対象とする IP アドレスは、図 10 を用いて説明したように、「VPN 2 内で利用者端末を一意に識別するための IP アドレス」（第一アドレス）である。仮想ルータにて利用者端末や仮想マシン 2 を一意に識別するための IP アドレス（第二アドレス）は、利用者端末と仮想マシン 1 又は仮想マシン 2 との間に VPN 間接続サービスが提供される時間帯において、同じ仮想ルータ内で一意に識別されるように払い出されればよい。このため、ライブマイグレーションにより仮想マシン 1 から仮想マシン 2 に移行される場合、第二アドレスが仮想ルータ内で重複することは原則として無く、第二アドレスを変更する必要はない。利用者端末と仮想マシン 1 との間の経路と、利用者端末と仮想マシン 2 との間の経路とが、同時に現用の経路（アクティブ）となることはないからである。

【 0 0 9 2 】

図 11 は、第 2 の実施形態における IP アドレスの管理を説明するための図である。第 2 の実施形態において、アドレス変換設定指示部 16 は、図 11 に示すように、IP アドレス空間を、時間軸を用いて管理している。ここで、図 11 は、例えば、VPN 2 に関し

10

20

30

40

50

て管理された IP アドレス空間を示す。

【 0 0 9 3 】

図 1 1 において、「VPN 2 内で自 VPN 内の装置を一意に識別するために利用している IP アドレス」は、全ての時間帯において、第一アドレスの払い出しに利用することができない。既に VPN 2 内の装置に割り当てられているか、あるいは、VPN 2 内の装置に割り当てる IP アドレスとして確保されているためである。

【 0 0 9 4 】

また、太線の実線は、VPN 間接続サービスの第一アドレスとして既に使用中の IP アドレスであり、太線の点線は、VPN 間接続サービスの第一アドレスとして予約済みの IP アドレスである。アドレス変換設定指示部 1 6 は、これらの情報を時間情報とともにテーブルなどに記憶する。そして、アドレス変換設定指示部 1 6 は、アドレス変換装置 2 に対する設定指示を送信するにあたり、第一アドレスを払い出す。具体的には、アドレス変換設定指示部 1 6 は、テーブルを参照し、少なくとも利用者端末と仮想マシン 2 との間に VPN 間接続サービスが提供される時間帯において、利用されていない、かつ、利用される予定の無い IP アドレスを第一アドレスとして選択する。

【 0 0 9 5 】

そして、アドレス変換設定指示部 1 6 は、図 1 0 に示したように、仮想マシン 2 に割り当てられている既存の IP アドレスと「10.0.2.10」とを変換するアドレス変換情報、及び、新たに払い出した第一アドレスと「10.0.1.10」とを変換するアドレス変換情報を、新たに生成する。

【 0 0 9 6 】

その後、アドレス変換設定指示部 1 6 は、第 1 の実施形態と同様、VPN 間接続処理部 2 0 に対して、アドレス変換装置 2 に対する設定指示を、新たに生成したアドレス変換情報などとともに送信する。

【 0 0 9 7 】

[第 2 の実施形態の効果]

上述したように、第 2 の実施形態に係る VPN 間接続管理システム 1 0 0 は、VPN 2 内で利用者端末を一意に識別するための新たな IP アドレス（第一アドレス）を払い出し、払い出した新たな IP アドレスを用いたアドレス変換情報をアドレス変換装置 2 に対して設定する。この場合、VPN 間接続管理システム 1 0 0 は、少なくとも、利用者端末と仮想マシン 2 との間に経路が構築される時間帯において、VPN 2 内で通信相手となり得る端末の中で一意に識別されるように、新たな IP アドレスを払い出す。この結果、マイグレーション元のアドレス変換装置に設定されていたアドレス変換情報が、例えば、使用中の IP アドレスであるか、あるいは予約済みの IP アドレスを含む場合にも、柔軟に対応することが可能になる。

【 0 0 9 8 】

なお、アドレス変換設定指示部 1 6 は、マイグレーション元のアドレス変換装置に設定されていたアドレス変換情報が、アドレス変換装置 2 に対して設定可能であるか否かを判定し、設定可能でないと判定した場合に、新たな IP アドレスを払い出し、払い出した新たな IP アドレスを用いたアドレス変換情報をアドレス変換装置 2 に対して設定してもよい。

【 0 0 9 9 】

なお、第 2 の実施形態においては、第二アドレスが仮想ルータ内で重複することは原則として無く、第二アドレスを変更する必要はないと考えて、第一アドレスの払い出しのみ言及したが、これに限られるものではない。すなわち、VPN 間接続管理システム 1 0 0 は、利用者端末と仮想マシン 2 との間に新たに経路を構築する場合に、第二アドレスを払い出し、新たに払い出した第二アドレスを利用してもよい。この場合、VPN 間接続管理システム 1 0 0 は、第二アドレスを、VPN_iに設置された利用者端末と仮想マシン 2 との間に VPN 間接続サービスが提供される時間帯において、同じ仮想ルータ内で一意に識別されるように払い出す。また、第二アドレスが変更された場合には、VPN 間接続管

10

20

30

40

50

理システム 100 は、新たな第二アドレスを用いたルーティング情報を集合仮想ルータに設定するのみならず、アドレス変換装置 3 に対しても、新たな第二アドレスを用いたアドレス変換情報の設定を行う。

【0100】

(第3の実施形態)

実施形態に係る制御装置、制御システム、制御方法、及び制御プログラムは、第1の実施形態及び第2の実施形態に限られるものではない。以下、順に説明する。

【0101】

第1の実施形態及び第2の実施形態においては、ライブマイグレーションを想定したが、これに限られるものではなく、開示の技術は、「マイグレーション」にも同様に適用することができる。この場合、VPN間接続管理システム100は、利用者端末が第1のVPNに設置された仮想マシンにアクセスするための経路が現用の経路として構築されている場合に、この第1のVPNに設置された仮想マシンをマイグレーション元として、第2のVPNに設置される仮想マシンをマイグレーション先とするマイグレーションの実行開始を検知する。次に、VPN間接続管理システム100は、マイグレーションの実行開始が検知されると、このマイグレーションの実行と併行して、利用者端末が第2のVPNに設置される仮想マシンにアクセスするための経路を構築する設定を、所定のネットワーク装置に対して行う。そして、VPN間接続管理システム100は、マイグレーションの実行完了を検知し、かつ、ネットワーク装置への設定が完了すると、現用の経路を、新たに構築された経路に切り替える。

10

20

【0102】

[拠点の態様]

上述の実施形態では、VPNが、電気通信事業者などによって提供されたVPNサービスに接続するローカルエリアネットワーク(LAN(Local Area Network))である場合を想定したが、これに限られるものではない。VPNは、いわゆるネットワークではなく一端末であってもよい。例えば、VPNに設置されるルータが、物理的なルータではなく端末内のソフトウェアで実現される場合などである。また、VPNは、電気通信事業者などによって提供されたVPNサービスによって接続された複数のローカルエリアネットワーク群による社内網のようなものであってもよい。

【0103】

図12~14は、VPNサービスによって接続された複数のローカルエリアネットワーク群としてのVPNを説明するための図である。なお、図12~14においては、2種類の点線を用いて示す。一方は、通常の点線であり、他方は、破線(短い線と長い線との組合せ)である。破線は、同じVPNサービスに属する複数の拠点であって、かつ、例えば同じ社内(例えばC社内)の拠点間でVPNを形成していることを示す。一方、点線は、VPN間を接続することを示す。例えば、異なるVPNサービスに属する複数のVPN間を接続することや、同じVPNサービスに属する複数のVPN間であっても、異なる会社のVPN間を接続することを示す。

30

【0104】

図12に例示するように、例えば、C社は、VPNサービス1に属する拠点群を有し、また、VPNサービス3に属する拠点を有する。一方、D社は、VPNサービス2に属する拠点を有し、また、VPNサービス4に属する拠点を有する。VPN間接続管理システム100は、このような、異なるVPNサービスに属するC社の拠点群(VPN)とD社の拠点群(VPN)との間でVPN間接続サービスを実現する。

40

【0105】

また、図13に例示するように、例えば、C社は、VPNサービス3でグループ化された拠点群(VPN)を有する。一方、D社は、VPNサービス4でグループ化された拠点群(VPN)を有する。VPN間接続管理システム100は、このような、異なるVPNサービスに属するC社の拠点群(VPN)とD社の拠点群(VPN)との間でVPN間接続サービスを実現する。

50

【 0 1 0 6 】

また、図 1 4 に例示するように、例えば、C 社及び D 社は、いずれも、VPN サービス 2 でグループ化された拠点群 (VPN) を有する。VPN 間接続管理システム 1 0 0 は、このような、同じ VPN サービスに属する C 社の拠点群 (VPN) と D 社の拠点群 (VPN) との間で VPN 間接続サービスを実現する。

【 0 1 0 7 】

[コンピュータ]

図 1 5 は、実施形態に係る制御プログラムによる情報処理がコンピュータを用いて具体的に実現されることを示す図である。図 1 5 に示すように、コンピュータは、例えば、メモリと、CPU と、ハードディスクドライブインタフェースと、ディスクドライブインタフェースと、シリアルポートインタフェースと、ビデオアダプタと、ネットワークインタフェースとを有し、これらの各部はバスによって接続される。

10

【 0 1 0 8 】

メモリは、図 1 5 に示すように、ROM (Read Only Memory) 及び RAM (Random Access Memory) を含む。ROM は、例えば、BIOS (Basic Input Output System) 等のブートプログラムを記憶する。ハードディスクドライブインタフェースは、図 1 5 に示すように、ハードディスクドライブに接続される。ディスクドライブインタフェースは、図 1 5 に示すように、ディスクドライブに接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブに挿入される。シリアルポートインタフェースは、図 1 5 に示すように、例えばマウス、キーボードに接続される。ビデオアダプタは、図 1 5 に示すように、例えばディスプレイに接続される。

20

【 0 1 0 9 】

ここで、図 1 5 に示すように、ハードディスクドライブは、例えば、OS、アプリケーションプログラム、プログラムモジュール、プログラムデータを記憶する。すなわち、実施形態に係る制御プログラムは、コンピュータによって実行される指令が記述されたプログラムモジュールとして、例えばハードディスクドライブに記憶される。具体的には、第 1 の実施形態で説明したライブマイグレーション実行部 1 5 と同様の情報処理を実行する手順と、アドレス変換設定指示部 1 6 と同様の情報処理を実行する手順と、アドレス変換設定部 2 4 と同様の情報処理を実行する手順と、ルーティング設定指示部 1 7 と同様の情報処理を実行する手順と、ルーティング設定部 2 5 と同様の情報処理を実行する手順とが記述されたプログラムモジュールが、ハードディスクドライブに記憶される。

30

【 0 1 1 0 】

また、第 1 の実施形態で説明した顧客ネットワーク設定記憶部 1 1 やネットワーク装置設定記憶部 2 1 に記憶されるデータのように、制御プログラムによる情報処理に用いられるデータは、プログラムデータとして、例えばハードディスクドライブに記憶される。そして、CPU が、ハードディスクドライブに記憶されたプログラムモジュールやプログラムデータを必要に応じて RAM に読み出し、上述の手順を実行する。

【 0 1 1 1 】

なお、制御プログラムに係るプログラムモジュールやプログラムデータは、ハードディスクドライブに記憶される場合に限られず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ等を介して CPU によって読み出されてもよい。あるいは、制御プログラムに係るプログラムモジュールやプログラムデータは、LAN、WAN (Wide Area Network) 等を介して接続された他のコンピュータに記憶され、ネットワークインタフェースを介して CPU によって読み出されてもよい。

40

【 符号の説明 】

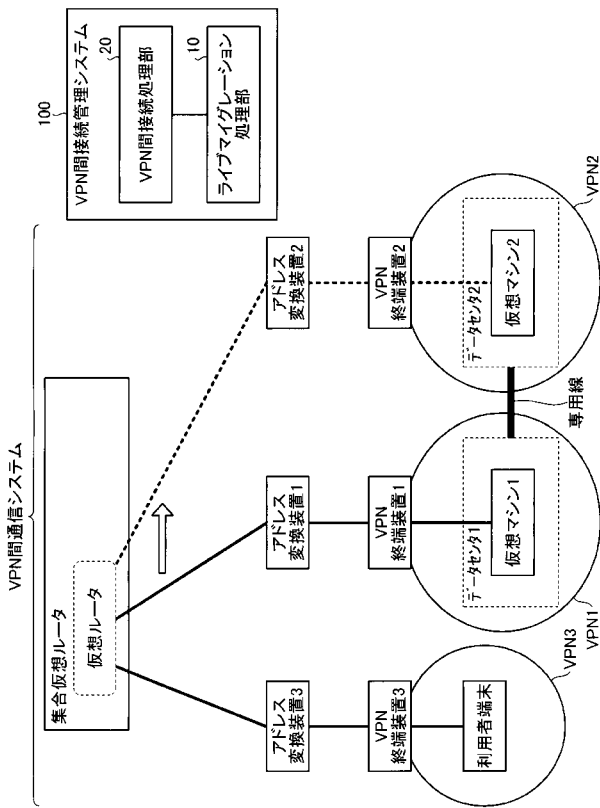
【 0 1 1 2 】

- 1 0 0 VPN 間接続管理システム
- 1 0 ライブマイグレーション処理部
- 1 1 顧客ネットワーク設定記憶部
- 1 2 通信部

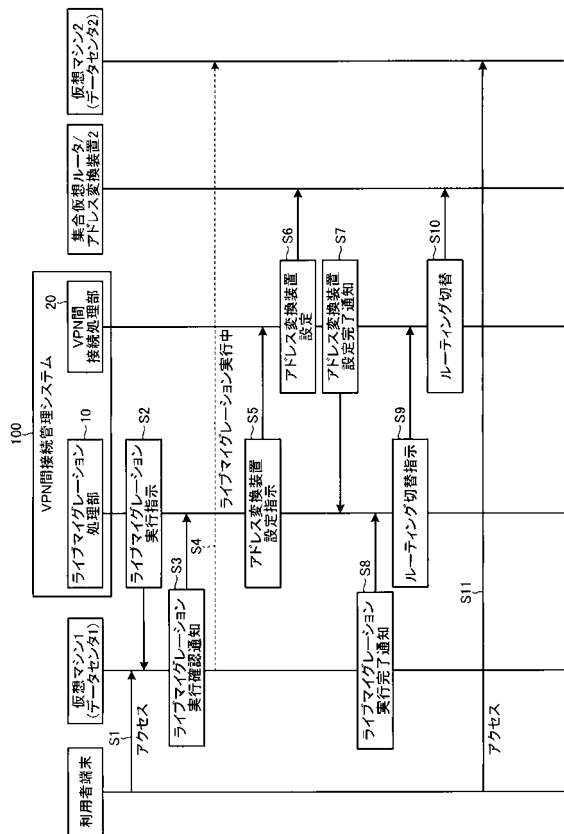
50

- 1 3 入力部
- 1 4 設定指示送信部
- 1 5 ライブマイグレーション実行部
- 1 6 アドレス変換設定指示部
- 1 7 ルーティング設定指示部
- 2 0 VPN間接続処理部
- 2 1 ネットワーク装置設定記憶部
- 2 2 通信部
- 2 3 設定指示受信部
- 2 4 アドレス変換設定部
- 2 5 ルーティング設定部

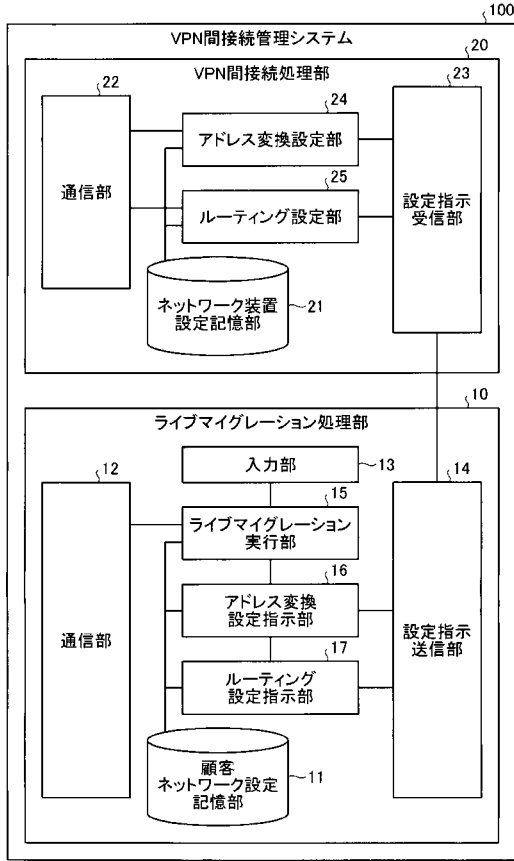
【 図 1 】



【 図 2 】



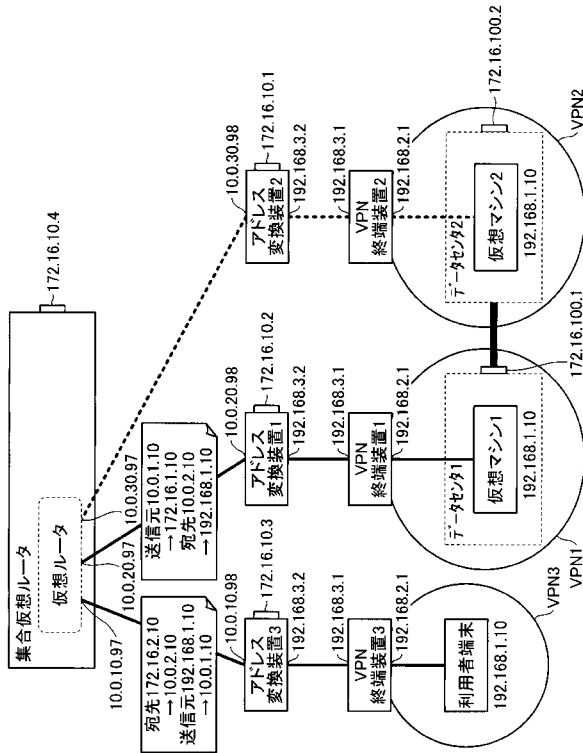
【 図 3 】



【 図 4 】

顧客ID		000001
仮想マシン	マイグレーション元	192.168.1.10
	マイグレーション元(制御用)	172.16.100.1
	マイグレーション先(制御用)	172.16.100.2
アドレス変換装置3	IPアドレス(制御用)	172.16.10.3
	アドレス変換情報	192.168.1.10⇔10.0.1.10 172.16.2.10⇔10.0.2.10
アドレス変換装置1(現用)	IPアドレス(制御用)	172.16.10.1
	アドレス変換情報	192.168.1.10⇔10.0.2.10 172.16.1.10⇔10.0.1.10
アドレス変換装置2(予備)	IPアドレス(制御用)	172.16.10.2
	IPアドレス(制御用)	172.16.10.4
集合仮想ルータ	ルーティング情報(現用)	宛先10.0.2.10:ゲートウェイ10.0.20.97
	ルーティング情報(予備)	宛先10.0.2.10:ゲートウェイ10.0.30.97

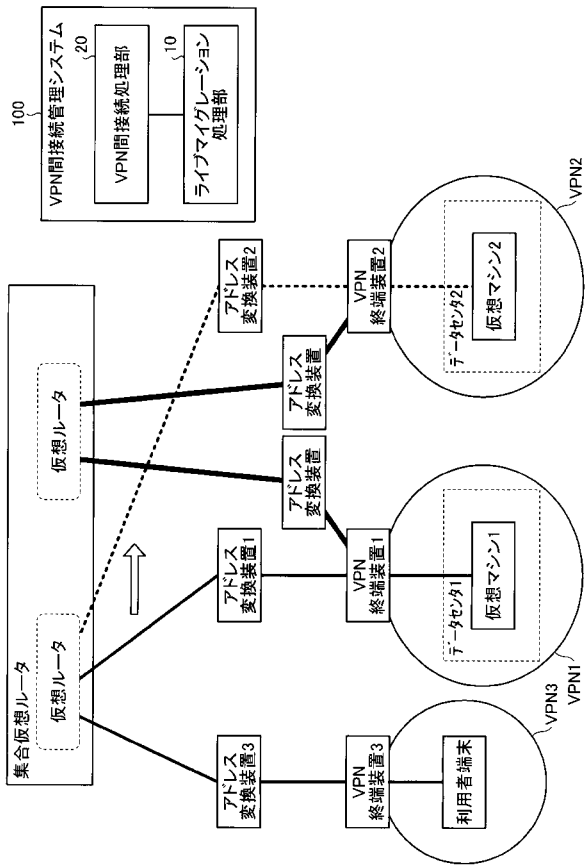
【 図 5 】



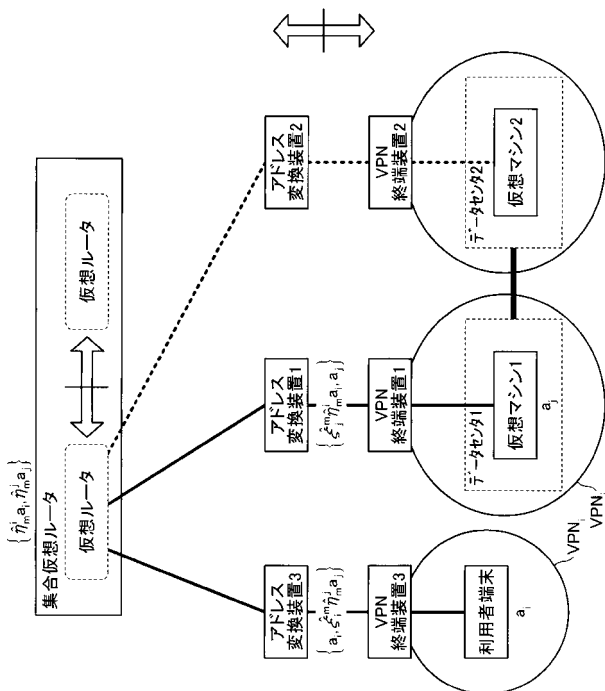
【 図 6 】

アドレス変換装置1(現用)	IPアドレス(制御用)	172.16.10.1
	パスワード	hogehoge01
アドレス変換装置2(予備)	IPアドレス(制御用)	172.16.10.2
	パスワード	hogehoge02
アドレス変換装置3	IPアドレス(制御用)	172.16.10.3
	パスワード	hogehoge03
集合仮想ルータ	IPアドレス(制御用)	172.16.10.4
	パスワード	hogehoge

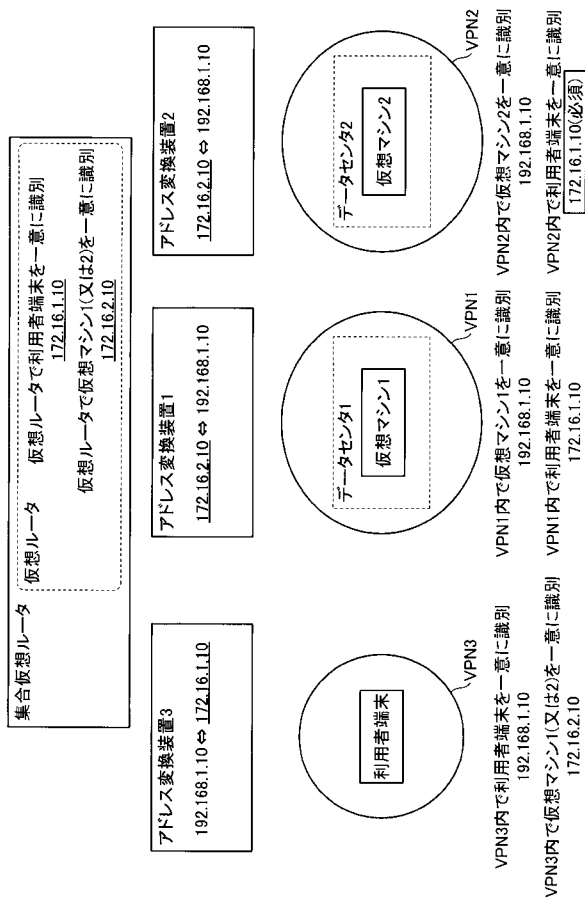
【 図 7 】



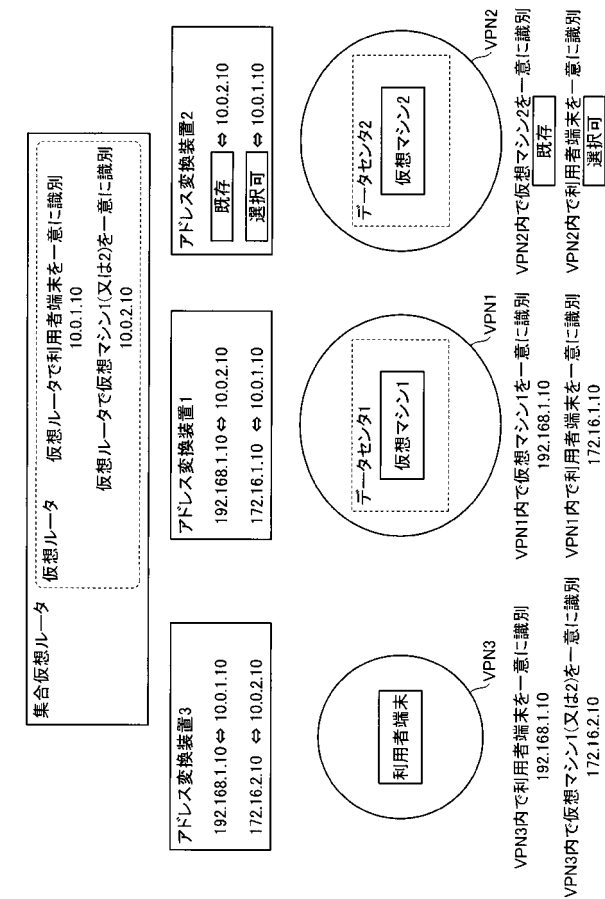
【 図 8 】



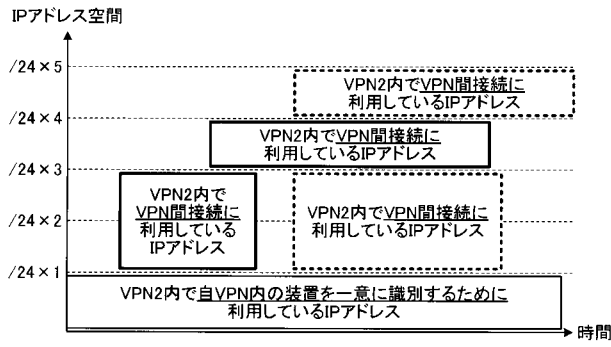
【 図 9 】



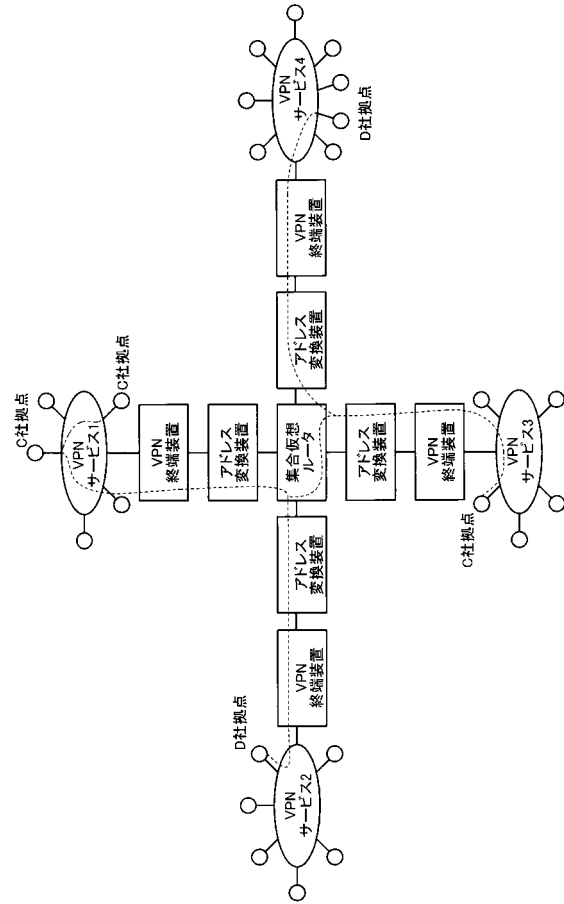
【 図 10 】



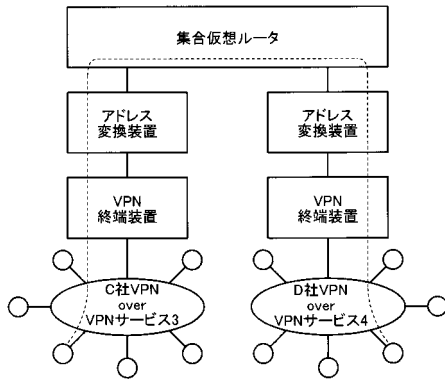
【 図 1 1 】



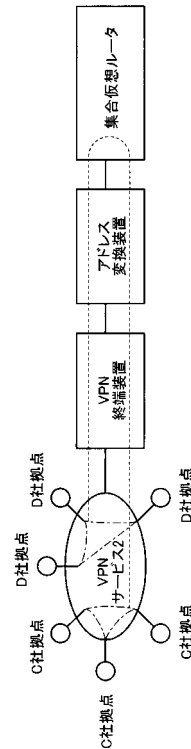
【 図 1 2 】



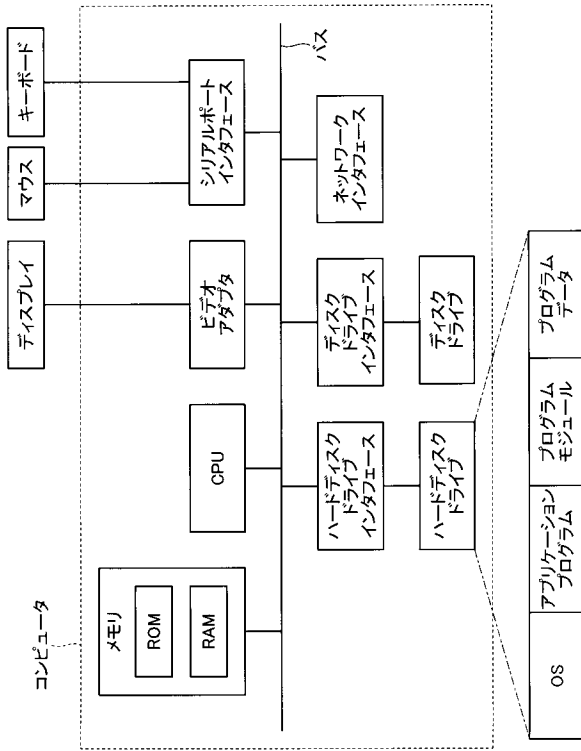
【 図 1 3 】



【 図 1 4 】



【図 15】



フロントページの続き

(72)発明者 北爪 秀雄

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

Fターム(参考) 5B014 FB05 GA27 HA07 HB01

5K030 GA19 HA08 HD07 KA05