(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6516331号
(P6516331)

(45)発行日　令和1年5月22日(2019.5.22)　(24)登録日　平成31年4月26日(2019.4.26)

(51)Int.Cl.		F I		
H04L 12/70	(2013.01)	H04L	12/70	D
H04L 12/749	(2013.01)	H04L	12/749	
H04L 12/46	(2006.01)	H04L	12/46	V
G06F 13/00	(2006.01)	G06F	13/00	520C

請求項の数 1　(全 13 頁)

(21)出願番号　特願2015-551749 (P2015-551749)
(86)(22)出願日　平成26年1月2日 (2014.1.2)
(65)公表番号　特表2016-507968 (P2016-507968A)
(43)公表日　平成28年3月10日 (2016.3.10)
(86)国際出願番号　PCT/US2014/010023
(87)国際公開番号　WO2014/107482
(87)国際公開日　平成26年7月10日 (2014.7.10)
審査請求日　平成28年12月22日 (2016.12.22)
(31)優先権主張番号　61/748,248
(32)優先日　平成25年1月2日 (2013.1.2)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　519099184
スカイキャスターズ，リミティド　ライアビリティ　カンパニー
アメリカ合衆国，オハイオ　４４３０６，アクロン，サウス　アーリントン　ストリート　１５２０
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100123582
弁理士　三橋　真二
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100114018
弁理士　南山　知広

最終頁に続く

(54)【発明の名称】ＲｅＮＡＴ通信環境を提供するシステム及び方法

(57)【特許請求の範囲】

【請求項１】

ＲｅＮＡＴ通信を行うシステムであって、ネットワーク運営センター（ＮＯＣ）を備え、前記ＮＯＣは、

プライベートネットワークとの仮想プライベートネットワーク（ＶＰＮ）通信を開始する第１の従来のＶＰＮと、

前記第１の従来のＶＰＮに結合されたＲｅＮＡＴ双方向ＮＡＴであって、前記ＲｅＮＡＴ双方向ＮＡＴは、顧客に割り当てられたプライベートＩＰアドレスと固有のプライベートＩＰ（ＵＰＩＰ）アドレスとの間の変換を行うＲｅＮＡＴ双方向ＮＡＴと、

前記ＲｅＮＡＴ双方向ＮＡＴに結合されたＲｅＮＡＴ　ＶＰＮコンポーネントであって、前記ＲｅＮＡＴ　ＶＰＮコンポーネントは、前記ＲｅＮＡＴ双方向ＮＡＴにソースＩＰアドレスを提供するＲｅＮＡＴ　ＶＰＮコンポーネントと、

プロセッサによって実行されるときに、前記システムに、従来のＶＰＮクライアント及びＲｅＮＡＴ双方向ＮＡＴクライアントを有するユーザワークステーションとの通信を促進させ、前記プライベートネットワークを用いてデータを送信する際に、前記ＮＯＣは、従来のＶＰＮポータルを介してデータを受信し、アドレス変換が、前記ＲｅＮＡＴ双方向ＮＡＴクライアントによって実行される論理と、を備え、

前記ＲｅＮＡＴ双方向ＮＡＴは、前記データのアドレスを、顧客規定プライベートアドレスにマッピングし、前記ＲｅＮＡＴ　ＶＰＮは、前記データを暗号化し、前記データを前記プライベートネットワークに転送するシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
ここで提供される実施の形態は、一般的には、ＲｅＮＡＴ通信環境の提供に関し、特に、ネットワークを通じてＲｅＮＡＴ機能を提供するシステム及び方法に関する。
【背景技術】
【０００２】
インターネットは、一群の標準プロトコルを用いるコンピュータ間の世界中の通信をサポートする。これらのプロトコルのうちの一つであるインターネットプロトコル（ＩＰ）は、ＩＰアドレスとして知られている固有のアドレスを各コンピュータに割り当てる。ＩＰは、二つのバージョン：３２ビットアドレスを有するＩＰｖ４及び１２８ビットアドレスを有するＩＰｖ６で現在利用できる。
【０００３】
インターネットの成長は、ＩＰｖ４の全ての利用できる３２ビットアドレスの利用をもたらした。限られた数のアドレスの一つの結果は、大抵の組織が現在ＩＰｖ４によって規定された三つのプライベートアドレス空間の一つを使用することである。これらのプライベートＩＰアドレスを公衆インターネット上で使用することができない。ゲートウェイルータは、専用イントラネットと公衆インターネットとの間のインタフェースを管理する。ゲートウェイルータは、プライベートネットワーク外の通信が要求されるときにプライベート内部ＩＰを秘密にする又は隠すために種々の機能を提供する。
【０００４】
商業環境においてゲートウェイルータによって用いられる共通する一つの方法は、外部ユーザを内部プライベートネットワークに接続するために仮想プライベートネットワーク（ＶＰＮ）を作成することである。ＶＰＮは、パケットを公衆インターネットを通じてユーザに送る間に内部ＩＰアドレス及びデータを隠すためのエンベロープ(envelope)又はラッパープロトコル(wrapper protocol)を提供する。
【０００５】
ＲｅＮＡＴアーキテクチャは、インターネット上でパブリックソフトウェアリソースを共有するためのプライベートアドレス体系を有するＶＰＮを用いる複数の組織に対するメカニズムを提供する。各組織は、公衆インターネット上で遠隔ユーザと通信を行うためにＶＰＮを用いる。このようにして、ＶＰＮは、組織のプライベートＩＰネットワークと、サーバーと、遠隔ユーザとの間の仮想トンネルを形成する。各ＶＰＮは、安全な通信を可能にするための二つの機能を提供する。第１の機能は、仮想トンネルの情報を不正アクセスから保護するために当該情報を暗号化できるようにすることである。第２の機能は、組織のプライベートＩＰネットワークをユーザワークステーションまで拡張することである。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
プライベートＩＰアドレス及びＶＰＮの使用によってユーザがプライベートネットワークに安全にアクセスできるが、これらの二つの事実は、ＶＰＮを用いる組織が公衆インターネット上でソフトウェア機能を使用できないことを意味する。他の問題が更に存在し、それを以下で更に詳細に説明する。
【課題を解決するための手段】
【０００７】
図面に記載された実施の形態は、本来は説明のためのものであるとともに例示的であり、特許請求の範囲によって規定される対象を限定することを意図するものではない。実施の形態の以下の詳細な説明を、以下の図面に関連して読んだときに理解することができ、同様な構造に同様な参照番号を付す。
【図面の簡単な説明】

【０００８】
【図１】図１は、ここで説明する実施の形態による遠隔コンピューティング装置とデータの通信を行うネットワーク環境を描写する。
【図２】図２は、ここで説明する実施の形態による双方向(twin)ＮＡＴ形態を利用する更に別のコンピューティング環境を描写する。
【図３】図３は、ここで説明する実施の形態による遠隔コンピューティング装置と通信を行うコンピューティング環境を描写する。
【図４】図４は、ここで説明する実施の形態によるＶＰＮを利用することなく遠隔コンピューティング装置と通信を行うコンピューティング環境を描写する。
【図５】図５は、ここで説明する実施の形態によるクライアントワークステーションが遠隔コンピューティング装置との通信を実行することができる動作を含むフローチャートを描写する。
【図６】図６は、ここで説明する実施の形態によるセッションが確立された時点でワークステーションが遠隔コンピューティング装置との通信を促進する際に実行することができる動作を含むフローチャートを描写する。
【図７】図７は、ここで説明する実施の形態によるＮＯＣがユーザワークステーションと遠隔コンピューティング装置との間の通信を促進する際に実行することができる動作を含む他のフローチャートを描写する。
【図８】図８は、ここで説明する実施の形態によるＮＯＣがユーザワークステーションと遠隔コンピューティング装置との間の通信を促進する際に実行することができる動作を含む更に別のフローチャートを描写する。
【図９】図９は、ここで説明する実施の形態によるユーザワークステーションがＮＯＣを介して遠隔コンピューティング装置からデータを受信する際に実行することができる動作を含むフローチャートを描写する。
【図１０】図１０は、ここで説明する実施の形態によるＮＯＣに存在してもよい種々のハードウェアコンポーネントを描写する。
【発明を実施するための形態】
【０００９】
ここで説明する実施の形態は、広域ネットワーク（又は他のネットワーク）上でプライベートアドレス体系のユーザコンピューティング装置と遠隔コンピューティング装置との間の通信を促進するＲｅＮＡＴシステム及び方法を有する。特に、ユーザコンピューティング装置は、衛星ネットワーク又は所望の接続速度より遅い速度を有してもよい他のネットワークを介して遠隔コンピューティング装置と通信を行ってもよい。ユーザは、仮想プライベートネットワークを利用してもよいが、情報を、ＲｅＮＡＴ双方向ＮＡＴ（ネットワークアドレス変換）クライアント及び商用オフザシェル（ＣＯＴＳ）ＶＰＮクライアントを有するユーザワークステーションからネットワーク運営センター（ＮＯＣ）に送ってもよい。ＮＯＣは、ＣＯＴＳ　ＶＰＮ、ＣＯＴＳクリアテキストソフトウェア、ＲｅＮＡＴ双方向ＮＡＴ及びＲｅＮＡＴ　ＶＰＮを有する。
【００１０】
したがって、ここで説明する実施の形態は、プライベートアドレス体系を有するＶＰＮ通信を用いるネットワークアクセスを有する一群の組織がアクセラレーション技術(acceleration technology)のようなソフトウェア機能を共有できるようにするプロセスを提供する。ＣＯＴＳアクセラレーション技術は、現在利用でき、組織のプライベートＩＰネットワーク内のクリアテキスト上で実行してもよい。実行中、ここで説明する実施の形態は、公衆インターネットＩＰアドレス及び組織のプライベートＩＰアドレスの両方から離間したプライベートＩＰアドレス体系又はアドレス空間を作成する。したがって、ここで説明する実施の形態は、全ての組織システムがＲｅＮＡＴプライベートＩＰアドレス体系内に固有のＩＰアドレスを有するようにするために、ＣＯＴＳプロセスを通じて通信を行う組織システムのそれぞれに対して固有のプライベートＩＰアドレス（ＵＰＩＰ）を割り当てる。複数の組織が同一のプライベートＩＰアドレスを有するときでさえも、クリアテキ

ストプロセスソフトウェアとして構成してもよいＣＯＴＳクリアテキストコンポーネントが、全てのユーザ組織システムに対して固有のＩＰアドレスを有するようにするために、ＲｅＮＡＴ双方向ＮＡＴクライアントは、顧客に割り当てられたプライベートＩＰアドレスと割り当てられたＵＰＩＰとの間の変換を行う。

【００１１】

ＲｅＮＡＴ環境の外側では、（ユーザワークステーションの）ユーザアプリケーション及び企業のオフィスの遠隔コンピューティング装置は、顧客の内部のプライベートＩＰアドレスしか確かめない。ＲｅＮＡＴ双方向ＮＡＴクライアント及びＲｅＮＡＴ双方向ＮＡＴは、ユーザアプリケーション及び企業のオフィスサーバが組織の内部のプライベートＩＰアドレスしか確かめないようにするために、顧客に割り当てられたプライベートＩＰアドレスとＲｅＮＡＴに割り当てられたＵＰＩＰとの間の変換を行うように調整される。

【００１２】

さらに、ここで説明する一部の実施の形態は、クライアントワークステーションと広域ネットワークとの間の通信のためのネットワークアドレスの変換を促進するように構成される。一部の実施の形態において、変換は、上述したように仮想プライベートネットワーク（ＶＰＮ）を横断する。したがって、これらの実施の形態を、双方向通信として構成してもよく、この場合、デュアル(Dual)ＮＡＴソフトウェアは、（ＩＰｖ４，ＩＰｖ６又は他の同様なプロトコルの）ＩＰアドレスのファミリーを、企業ネットワークのようなプライベートアドレス体系に割り当てる。同様に、（プライベートアドレス体系と広域ネットワークとの間にある）ネットワーク運営センター（ＮＯＣ）側において、複数のＩＰアドレスが、各プライベートアドレス体系に対して一つ割り当てられる。一例として、第１のプライベートアドレス体系を、割り当てられたＩＰアドレス１０．０．０．ｘとしてもよく、この場合、ｘ＝１，．．．，ｎである。ＮＯＣは、これらのアドレスを１０．２５４．２５４．２５４のようなＩＰアドレスと関連させてもよく、他のプライベートアドレス体系を、各々がネットワーク内アドレスとして１０．０．０．ｘを有する１０．２５４．２５４．２５３等のようなＩＰアドレスと関連させてもよい。さらに、ＮＡＴ関係を、クライアントワークステーション及び広域ネットワークが任意のＩＰアドレス変換に気付かない間に、企業のオフィスのサーバーを有するプライベートネットワークのユーザコンピューティング装置からの変換を促進する二つのデュアルＮＡＴに記憶させてもよい。

【００１３】

さらに、一部の実施の形態は、ソースゲートウェイ又は第２のＶＰＮを識別するための外部パケットのソースＩＰアドレスを提供する。デュアルＮＡＴからのパケットは、宛先ゲートウェイ又は第２のＶＰＮを識別するための宛先パブリックＩＰアドレスを有してもよい。

【００１４】

ここで説明する別の一部の実施の形態は、広域ネットワークとプライベートアドレス体系のクライアントワークステーションとの間のデータの通信を促進するためのネットワーク運営センター（ＮＯＣ）内の仮想プライベートネットワークを提供する。上述したように、ＮＯＣを、例えば、アクセラレーション技術を用いることによって衛星通信を通じてプライベートアドレス体系と広域ネットワークとの間のデータの通信を促進するように構成してもよい。したがって、ＮＯＣで作成されるＶＰＮを、商用オフザシェル（ＣＯＴＳ）の動作が装置内でのみ実行されるが装置間では通信されないようセキュリティバリア(security barrier)を提供するために利用してもよい。ここで説明する実施の形態は、デュアルＮＡＴの利用を介してＩＰｖ４及び／又はＩＰｖ６のＩＰアドレスの割当てを促進してもよい。

【００１５】

ここで図面を参照すると、図１は、ここで説明する実施の形態による遠隔コンピューティング装置１２６とデータの通信を行うネットワーク環境を描写する。図示したように、ネットワーク環境は、パーソナルコンピュータ、タブレット、モバイルコンピューティング装置等を含んでもよいユーザワークステーション１０２を有する。ユーザワークステー

ション１０２を、プライベートＩＰアドレス体系１０４を介して遠隔コンピューティング装置１２６と通信するように構成してもよい。ユーザワークステーション１０２は、ユーザアプリケーション１０８と、公衆インターネットＩＰアドレスと組織のプライベートＩＰアドレスの使用の両方から離間したプライベートＩＰアドレス体系又はアドレス空間（ＲｅＮＡＴプライベートＩＰアドレス体系）を作成するためのＲｅＮＡＴ双方向ＮＡＴクライアント１１０及びＣＯＴＳ　ＶＰＮクライアント１１２と、を有してもよい。特に、ＲｅＮＡＴ双方向ＮＡＴクライアント１１０は、（ユーザワークステーション１０２のような）全てのコンピューティング装置がプライベートＩＰアドレス体系１０４内に固有のＩＰアドレスを有するために、ＣＯＴＳ　ＶＰＮクライアントを通じて通信を行う（ユーザワークステーション１０２のような）プライベートＩＰアドレス体系１０４にアクセスするコンピューティング装置のそれぞれに対して固有のプライベートＩＰアドレス（ＵＰＩＰ）を割り当てる。ＲｅＮＡＴ双方向ＮＡＴクライアント１１０は、遠隔コンピューティング装置１２６のプライベートＩＰアドレス体系を管理するためのペアの調整された双方向ＮＡＴ機能を提供する。

【００１６】

ＣＯＴＳ　ＶＰＮ１１４、ＣＯＴＳクリアテキスト機能１１６、ＲｅＮＡＴ双方向ＮＡＴ１１８及びＲｅＮＡＴ　ＶＰＮ１２０は、プライベートＩＰアドレス体系１０４に含まれる。ＲｅＮＡＴ双方向ＮＡＴクライアント１１０及びＲｅＮＡＴ双方向ＮＡＴ１１８は、複数の組織が同一のプライベートＩＰアドレスを有するときでもＣＯＴＳクリアテキスト機能１１６が全てのユーザ組織システムに対して固有のＩＰアドレスを有するようにするために、顧客に割り当てられたプライベートＩＰアドレスと割り当てられたＵＰＩＰとの間でデータの変換を行う。

【００１７】

プライベートＩＰアドレス体系１０４の外側では、ユーザアプリケーション１０８と、企業のオフィス１０６の遠隔コンピューティング装置１２６とは、顧客の内部のプライベートＩＰアドレスしか確かめない。ＲｅＮＡＴ双方向ＮＡＴクライアント１１０及びＲｅＮＡＴ双方向ＮＡＴ１１８は、ユーザアプリケーション１０８及び遠隔コンピューティング装置１２６がユーザワークステーション１０２の内部のプライベートＩＰアドレスしか確かめないようにするために、顧客に割り当てられたプライベートＩＰアドレスとＲｅＮＡＴに割り当てられたＵＰＩＰとの間の変換を行うように調整される。したがって、ユーザワークステーション１０２から送信されたデータは、プライベートネットワーク１２４のゲートウェイ装置１２２において企業のオフィス１０６で受信される。遠隔コンピューティング装置１２６は、それに応じてデータを処理してもよい。

【００１８】

既存のソフトウェア機能１２８及びＲｅＮＡＴ機能マネージャ１３０も図１に示す。これらのコンポーネントは、図１で参照された他のコンポーネントによって利用及び／又はアクセスされてもよい既存の論理を表す。

【００１９】

図２は、ここで説明する実施の形態による双方向ＮＡＴ形態を利用する更に別のコンピューティング環境を描写する。図示したように、ユーザワークステーション２０２は、プライベートＩＰアドレスをＵＰＩＰアドレスに変換することによってデータをＮＯＣ２０４に送信してもよい。データを、企業のオフィス２０６に送信する前にプライベートアドレスに戻してもよい。ユーザワークステーション２０２は、ユーザアプリケーション２０８と、クライアントソフトウェア２０９と、を有する。クライアントソフトウェア２０９は、ＲｅＮＡＴ双方向ＮＡＴクライアント２１０と、ＣＯＴＳクリアテキスト処理（ＣＯＴＳ　ＣＴＰ）クライアント２１２と、ＣＯＴＳ　ＶＰＮクライアント２１４と、クライアントログインマネージャ２１６と、クライアントセッションマネージャ２１８と、を有する。特に、ユーザアプリケーション２０８は、データを企業のオフィス２０６の遠隔コンピューティング装置２３４に送信するようユーザワークステーション２０２に指示してもよい。したがって、クライアントログインマネージャ２１６は、ＮＯＣ２０４のログイ

ン認証情報の通信を促進することができる。ユーザのＮＯＣへのロギングの際に、クライアントセッションマネージャ２１８は、所望のコンピューティング装置（この場合、遠隔コンピューティング装置２３４）の識別及び／又はアクセスのためにユーザインタフェース及び／又は他のデータを提供してもよい。それに応じて、ＲｅＮＡＴ双方向ＮＡＴクライアント２１０は、ユーザアプリケーション２０８から受信したデータにＵＰＩＰを割り当てる。ＲｅＮＡＴ双方向ＮＡＴクライアント２１０を、クリアテキストパケットのソースＩＰアドレスから割り当てられたＵＰＩＰへの変換及び割り当てられたＵＰＩＰからクリアテキストパケットの宛先ＩＰアドレスへの変換の両方を行うように構成してもよい。ＣＯＴＳ　ＣＴＰクライアント２１２は、クリアテキスト処理（又は他のプロトコル）を用いてデータを受信及び処理する。ＣＯＴＳ　ＶＰＮクライアント２１４は、データを受信し、データをＮＯＣ２０４に安全に送信するためのＶＰＮトンネルを形成する。

【００２０】

ＮＯＣ２０４は、ＶＰＮ暗号化を解除するＣＯＴＳ　ＶＰＮ２２０でデータを受信し、ＣＯＴＳクリアテキスト処理マネージャ２２２による処理のためにデータを提供する。ＣＯＴクリアテキスト処理マネージャ２２２は、クリアテキスト又は他の同様なプロトコルに従ってデータを処理する。データをＲｅＮＡＴ双方向ＮＡＴ２２４によって処理してもよい。ＲｅＮＡＴ双方向ＮＡＴ２２４は、ＵＰＩＰを取り出し、ＵＰＩＰを、プライベートネットワーク２３３からの顧客規定ＩＰに置換し、顧客ゲートウェイ装置２３２の公衆ＩＰアドレスを提供する。ＲｅＮＡＴ双方向ＮＡＴ２２４を、クリアテキストパケットのソースＩＰアドレスから割り当てられたＵＰＩＰへの変換及び割り当てられたＵＰＩＰからクリアテキストパケットの宛先ＩＰアドレスへの変換の両方を行うように構成してもよい。入ってくるパケットに対して、ＲｅＮＡＴ双方向ＮＡＴ２２４は、ユーザを識別するためにＲｅＮＡＴ　ＶＰＮ２２６によって提供されたソースＩＰを用いる。ＲｅＮＡＴ双方向ＮＡＴ２２４からＲｅＮＡＴ　ＶＰＮ２２６に出てゆくパケットは、遠隔コンピューティング装置２３４を識別するための宛先パブリックＩＰを有する。出てゆくパケットに対して、ＲｅＮＡＴ双方向ＮＡＴ２２４は、宛先ゲートウェイ／ＶＰＮ２３２に対する宛先パブリックＩＰアドレスを識別するためにソース及び宛先ＵＰＩＰアドレスを用いる。さらに、ＶＰＮ機能は、ソースゲートウェイ／ＶＰＮを識別するよう企業のオフィスから外部パケットのソースＩＰを提供するために変更される。ＲｅＮＡＴ双方向ＮＡＴ２２４からのパケットは、宛先ゲートウェイ／ＶＰＮを識別するために宛先パブリックＩＰを有する。

【００２１】

ログインマネージャ２２８及びセッションマネージャ２３０もＮＯＣ２０４内に含み、これらは、ユーザワークステーション２０２のログインを管理するとともにユーザワークステーションのセッションを管理する。ＲｅＮＡＴ双方向ＮＡＴ２２４とＲｅＮＡＴ　ＶＰＮ２２６との間のリンク上で、パケットは、パブリックソース及び宛先ＩＰを有するプライベートＲｅＮＡＴで規定したＩＰプロトコルにおいてラッピングされる。さらに、ＲｅＮＡＴ双方向ＮＡＴ２２４は、顧客に割り当てられたプライベートＩＰアドレスとオーバーラップするＵＰＩＰを割り当ててもよい。しかしながら、これは、ルーティングの問題を生じない。その理由は、割り当てられたアドレスがＮＯＣ内で固有であるとともにセッションマネージャ２３０によってパブリックＩＰにマッピングされるからである。上述したように、セッションマネージャ２３０は、サービスにログインされるユーザワークステーション２０２の各々に対するセッション情報を維持する。セッションマネージャ２３０は、ＵＰＩＰ調整情報をＲｅＮＡＴ双方向ＮＡＴ２２４に提供し、この顧客に対して割り当てられたＵＰＩＰによってクライアントセッションマネージャ２１８を更新する。セッションマネージャ２３０は、ＵＰＩＰと顧客のゲートウェイ／ＶＰＮのパブリックＩＰとの間の関係も維持する。会社のオフィス２０６は、顧客ゲートウェイ装置２３２と、プライベートネットワーク２３３と、遠隔コンピューティング装置２３４と、を有する。

【００２２】

図３は、ここで説明する実施の形態による遠隔コンピューティング装置３０８と通信を

行うコンピューティング環境を描写する。図示したように、顧客は、顧客の企業のオフィスに対するＶＰＮを有しなくてもよいが、ＯＮＣとワークステーションとの間のＶＰＮを利用することを所望してもよい。それでも、図３のユーザワークステーション３０２は、ユーザアプリケーション３１０と、ＣＯＴＳ　ＣＴＰクライアント３１２と、ＣＯＴＳ　ＶＰＮクライアント３１４と、クライアントログインマネージャ３１６と、クライアントセッションマネージャ３１８と、を有する。上述したように、ユーザアプリケーション３１０は、ネットワーク３０４を介した遠隔コンピューティング装置３０８への最終的な送信のためのデータをＣＯＴＳ　ＣＴＰクライアント３１２に送信してもよい。ネットワーク３０４は、インターネットのような任意の広域及び／又はローカルエリアネットワークを有してもよい。

【００２３】

それに応じて、クライアントログインマネージャ３１６及びクライアントセッションマネージャ３１８は、ＮＯＣ３０６によるログイン及びセッションの管理を促進するためにログインマネージャ３２４及びセッションマネージャ３２６と通信を行ってもよい。セッションが確立されると、ＣＯＴＳ　ＣＴＰクライアント３１２は、データを処理してもよい。さらに、ＣＯＴＳ　ＶＰＮクライアント３１４は、ユーザワークステーション３０２とＮＯＣ３０６のＣＯＴＳ　ＶＰＮ３２０との間のＶＰＮトンネルを形成してもよい。ユーザワークステーション３０２は、データを受信するとともにデータをＮＯＣ３０６に送信してもよい。ＮＯＣ３０６は、ＶＰＮからのデータを解読するためにＣＯＴＳ　ＶＰＮ３２０を用いることができ、ＣＯＴＳクリアテキスト処理３２２は、遠隔コンピューティング装置３０８に送信するためにデータを更に処理することができる。

【００２４】

図４は、ここで説明する実施の形態によるＶＰＮを利用することなく遠隔コンピューティング装置４０８と通信を行うコンピューティング環境を描写する。特に、図４は、顧客が所望のレベルのサービスを選択できるようにする複数のＣＯＴＳ処理を描写する。例えば、あるＣＯＴＳ処理は、全てのトラフィックの全アクセラレーション(full acceleration)を提供してもよく、第２のＣＯＴＳ処理は、（全てのハイパーテキスト転送プロトコルのような）トラフィックの一部のみをアクセラレートする。それに応じて、図４のユーザワークステーション４０２は、遠隔コンピューティング装置４０８と情報のやり取りを行うためにユーザアプリケーション４１０を有してもよい。それに応じて、クライアントログインマネージャ４１４及びクライアントセッションマネージャ４１６は、ユーザワークステーション４０２とＮＯＣ４０６との間の接続を確立するためにログインマネージャ４２０及びセッションマネージャ４２２と通信を行ってもよい。ユーザアプリケーション４１０は、ＣＯＴＳ　ＣＴＰクライアント４１２が処理するデータを更に生成してもよい。この場合、データは、ネットワーク４０４を用いて送信され、ネットワーク４０４は、データをＮＯＣ４０６に送信する。上述したように、ネットワーク４０４を、任意の広域又はローカルエリアネットワークとしてもよい。ユーザ設定、ユーザ選択、ＮＯＣ設定等に応じて、ＭＯＣ４０６は、受信したデータの一部又は全てを処理するために一つ以上の異なるＣＯＴＳクリアテキスト処理４１８を実現してもよい。ＮＯＣ４０６は、処理のためにデータを遠隔コンピューティング装置４０８に送信してもよい。

【００２５】

図５は、ここで説明する実施の形態によるクライアントワークステーションが遠隔コンピューティング装置との通信を実行することができる動作を含むフローチャートを描写する。ブロック５５０に示すように、ライセンスＩＤを、例えば、ログインマネージャを介して認証してもよい。ブロック５５２において、サービスを要求する顧客を識別してもよい。ブロック５５４において、ユーザを追跡するためにセッションを作成してもよい。ブロック５５６において、ＶＰＮトンネルを、ユーザワークステーションのために形成してもよく、ＵＰＩＰアドレスを、ライセンスＩＤに対してユーザワークステーションに割り当ててもよい。ブロック５５８において、ＶＰＮトンネルを、遠隔コンピューティング装置に対して形成してもよい。ブロック５６０において、遠隔コンピューティング装置への

ユーザログインのエミュレーションを実行してもよい。ブロック５６２において、顧客ＶＰＮログインデータを、ログイン認証情報を入力するためにワークステーションに戻してもよい。ブロック５６４において、セッションマネージャをログイン結果によって更新してもよい。ブロック５６６において、ＲｅＮＡＴ双方向ＮＡＴを、遠隔コンピューティング装置に対するＵＰＩＰアドレスによって更新してもよい。ブロック５６８において、システムが準備できていることを表すメッセージを提供してもよい。

【００２６】

図５を参照して説明したように、ユーザワークステーションは、遠隔コンピューティング装置との通信を行うためにセッションを初期化してもよい。図６は、ここで説明する実施の形態によるセッションが確立された時点でワークステーションが遠隔コンピューティング装置との通信を促す際に実行することができる動作を含むフローチャートを描写する。ブロック６５０に示すように、ＮＯＣは、ユーザ入力に基づいて要求データグラム(request datagram)を作成してもよい。特に、この動作を、ユーザアプリケーションを介したユーザワークステーションによって作成してもよい。とにかく、ブロック６５２において、ユーザワークステーションは、データグラムの顧客規定プライベートＩＰアドレスをＵＰＩＰアドレスにマッピングしてもよい。ブロック６５４において、ユーザワークステーションは、データグラムを処理してもよい。ブロック６５６において、データグラムをＮＯＣに転送してもよい。

【００２７】

図３及び図４において、ネットワーク３０４，４０４を公衆インターネット又は他のコンピューティングネットワークの利用を説明するためにシステムコンポーネント間に描写していることを理解すべきである。理解できるように、これらは単なる例であり、図１～６に表現したコンポーネントのいずれかを、実施の形態に応じてネットワークインフラに接続してもよい。

【００２８】

図７は、ここで説明する実施の形態によるＮＯＣがユーザワークステーションと遠隔コンピューティング装置との間の通信を促進する際に実行することができる動作を含む他のフローチャートを描写する。ブロック７５０に示すように、データグラムを、ＮＯＣによって処理してもよく、異なるデータグラムを、遠隔コンピューティング装置に送信するために生成してもよい。ブロック７５２において、ＵＰＩＰアドレスを、データグラムにおいて顧客規定プライベートＩＰアドレスにマッピングしてもよい。ブロック７５４において、データグラムを暗号化するとともに遠隔コンピューティング装置に転送してもよい。

【００２９】

図８は、ここで説明する実施の形態によるＮＯＣがユーザワークステーションと遠隔コンピューティング装置との間の通信を促進する際に実行することができる動作を含む更に別のフローチャートを描写する。特に、図７は、ユーザワークステーションがデータを遠隔コンピューティング装置に送信するときに実行してもよい動作を描写するが、図８は、遠隔コンピューティング装置がデータをユーザワークステーションに送信するときに実行してもよい動作を描写する。したがって、ブロック８５０において、ユーザワークステーションのための顧客プライベートＩＰに対する宛先ＩＰアドレスを有する暗号化された応答データゴラムを受信してもよい。ブロック８５２において、データグラムを解読してもよい。ブロック８５４において、顧客規定プライベートＩＰアドレスをデータグラムにおいてＵＰＩＰアドレスにマッピングする。ブロック８５６において、新たな顧客プライベートＩＰを、解読したデータグラムのソースＩＰから記録してもよく、新たなＵＰＩＰを割り当ててもよい。ブロック８５８において、クライアントセッションマネージャは、新たなＵＰＩＰについての情報を顧客プライベートＩＰマッピングに対して通知してもよい。ブロック８６０において、データグラムを処理してもよく、新たなデータグラムをユーザアプリケーションのために生成してもよい。ブロック８６２において、新たなデータグラムをユーザワークステーションに送信してもよい。

【００３０】

特定の実施の形態に応じて、一つ以上のデータグラムを、ユーザワークステーションに対する新たなデータグラムを生成する前に遠隔コンピューティング装置に送信してもよいことを理解すべきである。一例として、コンピューティング環境がＣＯＴＳ処理としてアクセラレーションを利用する場合、遠隔コンピューティング装置による複数のデータグラムの通信を実行してもよい。

【００３１】

図９は、ここで説明する実施の形態によるユーザワークステーションがＮＯＣを介して遠隔コンピューティング装置からデータを受信する際に実行することができる動作を含むフローチャートを描写する。ブロック９５０に示すように、受信したデータグラムを処理してもよい。ブロック９５２において、ＵＰＩＰアドレスを、ダイヤグラムにおいて顧客規定プライベートＩＰアドレスにマッピングしてもよい。ブロック９５４において、データグラムの結果を表示のために提供してもよい。

【００３２】

図１０は、ここで説明する実施の形態によるＮＯＣに存在してもよい種々のハードウェアコンポーネントを描写する。図示した実施の形態において、ＮＯＣ２０４は、一つ以上のプロセッサ１０３０と、入力／出力ハードウェア１０３２と、ネットワークインタフェースハードウェア１０３４と、（ログインデータ１０３８ａ及びセッションデータ１０３８ｂを記憶する）データ記憶部１０３６と、メモリ構成要素１０４０と、を有する。メモリ構成要素１０４０は、揮発性及び／又は不揮発性メモリとして構成されてもよく、したがって、（ＳＲＡＭ、ＤＲＡＭ及び／又は他のタイプのＲＡＭを含む）ランダムアクセスメモリ、フラッシュメモリ、レジスタ、コンパクトディスク（ＣＤ）、デジタル多用途ディスク（ＤＶＤ）及び／又は他のタイプの非一時的なコンピュータ可読媒体を有してもよい。特定の実施の形態に応じて、非一時的なコンピュータ可読媒体は、ＮＯＣ２０４の内部及び／又はＮＯＣ２０４の外部に存在してもよい。

【００３３】

さらに、メモリ構成要素１０４０は、一例としてコンピュータプログラム、ファームウェア及び／又はハードウェアとして実施してもよいオペレーティング論理１０４２、データ通信論理１０４４ａ及びマネージャ論理１０４４ｂを記憶するように構成されてもよい。ローカル通信インタフェース１０４６も図１０に含まれるが、ローカル通信インタフェース１０４６を、バスとして又はＮＯＣ２０４のコンポーネント間の通信を促進する他のインタフェースとして実現してもよい。

【００３４】

プロセッサ１０３０は、（データ記憶部１０３６及び／又はメモリ構成要素１０４０からのような）命令を受信及び実行する任意の処理構成要素を有してもよい。入力／出力ハードウェア１０３２は、モニタ、キーボード、マウス、プリンタ、カメラ、マイクロホン、スピーカ及び／又はデータを受信、送信及び／又は提示する他の装置を有してもよい及び／又はこれらとインタフェースで接続するように構成されてもよい。ネットワークインタフェースハードウェア１０３４は、任意の有線又は無線ネットワークハードウェア、衛星、アンテナ、モデム、ＬＡＮポート、ワイヤレスフェディリティー（Ｗｉ－Ｆｉ（登録商標））、ＷｉＭａｘ（登録商標）カード、モバイル通信ハードウェア、ファイバー及び／又は他のネットワーク及び／又はデバイスと通信を行うための他のハードウェアを有してもよい及び／又はこれらと通信を行うように構成されてもよい。この接続から、通信をＮＯＣ２０４と他のコンピューティング装置との間で促進してもよい。

【００３５】

同様に、データ記憶部１０３６が、ＮＯＣ２０４に近接して及び／又はＮＯＣ２０４から離間して存在してもよく、かつ、ＮＯＣ２０４及び／又は他のコンポーネントによってアクセスされる一つ以上のデータを記憶するように構成されてもよいことを理解すべきである。一部の実施の形態において、データ記憶部１０３６を、ＮＯＣ２０４から離間して配置してもよく、したがって、ネットワーク接続を介してアクセス可能にしてもよい。しかしながら、一部の実施の形態において、データ記憶部１０３６を、単なる周辺装置とし

てもよいが、ＮＯＣ２０４の外部にする。

【００３６】

オペレーティング論理１０４２、データ通信論理１０４４ａ及びマネージャ論理１０４４ｂはメモリ構成要素１０４０に含まれる。オペレーティング論理１０４２は、オペレーティングシステム及び／又はＮＯＣ２０４のコンポーネントを管理する他のソフトウェアを有してもよい。同様に、データ通信論理１０４４ａは、ＣＯＴＳ　ＶＰＮ２２０、ＣＯＴＳクリアテキスト処理マネージャ２２２、ＲｅＮＡＴ双方向ＮＡＴ２２４、ＲｅＮＡＴＶＰＮ２２６及び／又はデータを操作するとともにユーザワークステーション２０２と遠隔コンピューティング装置２３４との間の通信を行うための他の論理を有してもよい。マネージャ論理１０４４ｂは、ログインマネージャ２２８、セッションマネージャ２３０及び／又はユーザワークステーション２０２とのセッションを確立するためのＮＯＣ２０４をもたらす他のコンポーネントを有してもよい。

【００３７】

図１０に示すコンポーネントは単なる例示であり、この開示の範囲を限定することを意図しないことを理解すべきである。図１０のコンポーネントがＮＯＣ２０４内に存在するものとして図示したが、これは単なる一例である。一部の実施の形態において、コンポーネントの一つ以上はＮＯＣ２０４の外部に存在してもよい。ＮＯＣ２０４を図１０に表現したが、図２又は他の図面に記載した他のコンピューティング装置が上述した機能を提供する同様なハードウェア及びソフトウェアを有してもよい。

【００３８】

特定の実施の形態をここで説明及び記載したが、種々の他の変形及び変更を特許請求の範囲に記載された対象の精神及び範囲から逸脱することなく行うことができる。さらに、特許請求の範囲に記載された対象の種々の態様をここで説明したが、そのような態様を一緒に利用する必要はない。したがって、添付した特許請求の範囲が特許請求の範囲に記載された対象の範囲内にある全てのそのような変形及び変更をカバーすることを意図する。

【図１】

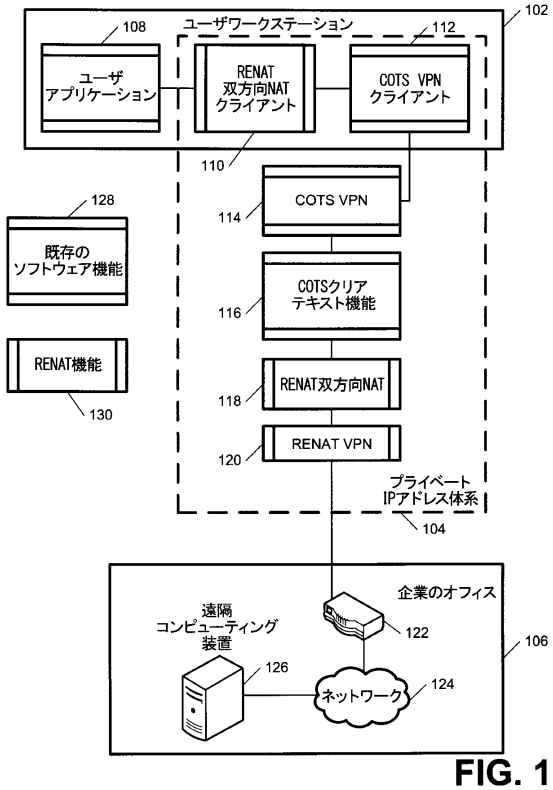

FIG. 1

【図２】

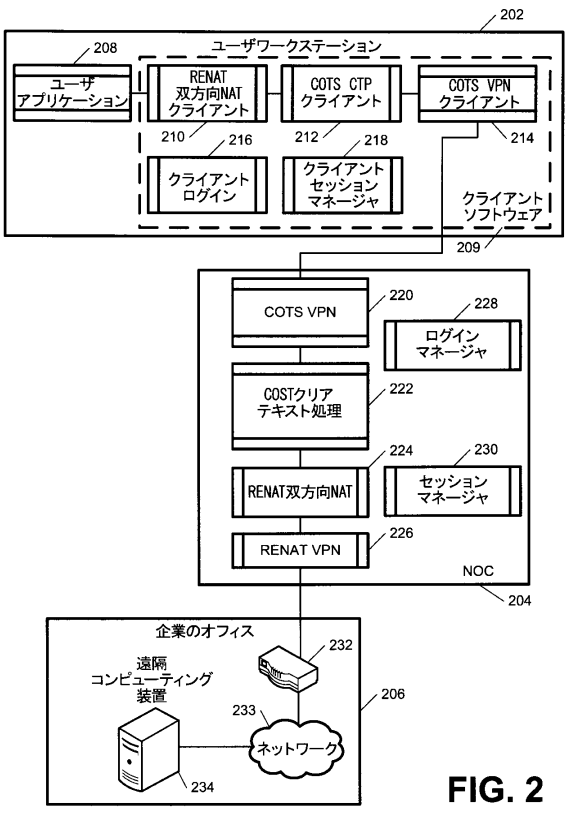

FIG. 2

【図３】

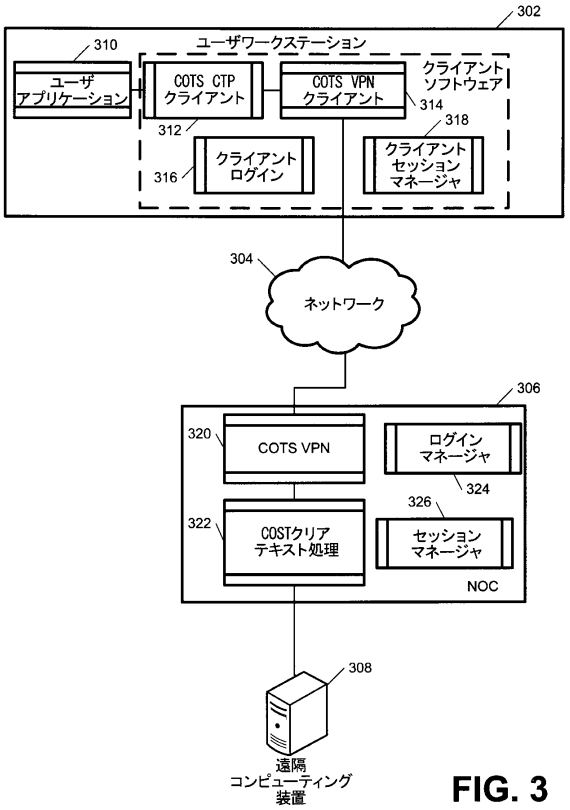

FIG. 3

【図４】

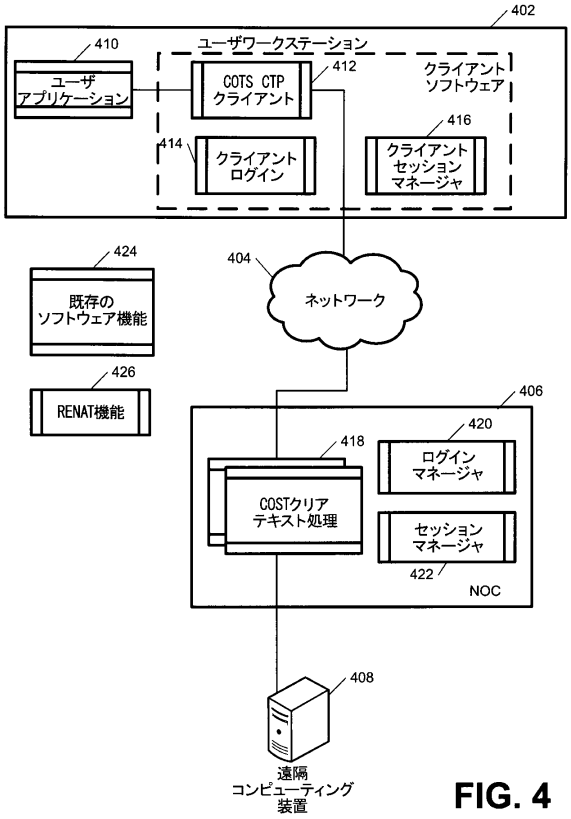

FIG. 4

【図５】

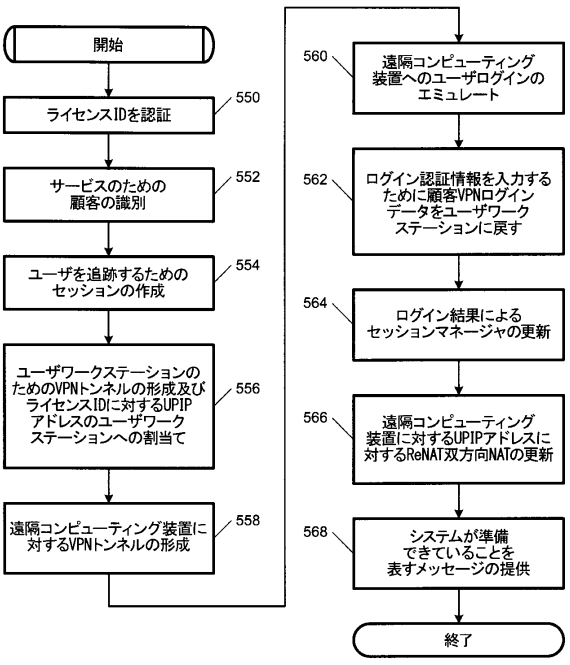

FIG. 5

【図６】

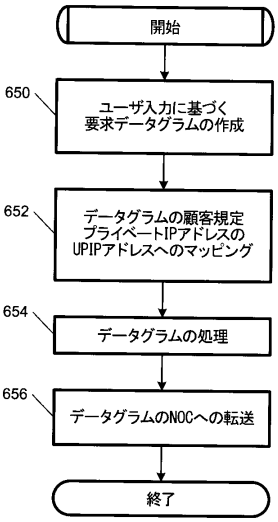

FIG. 6

【図７】

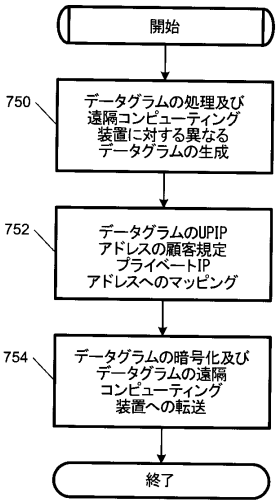

FIG. 7

【図８】

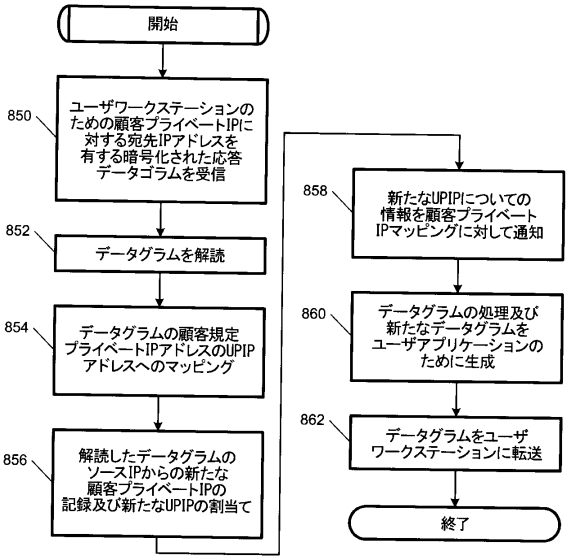

FIG. 8

【図９】

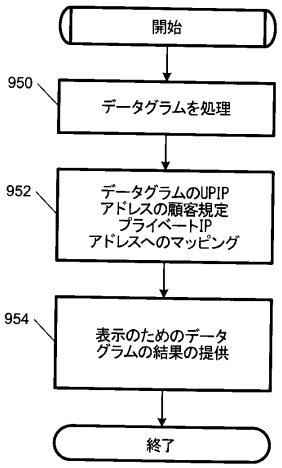

FIG. 9

【図１０】

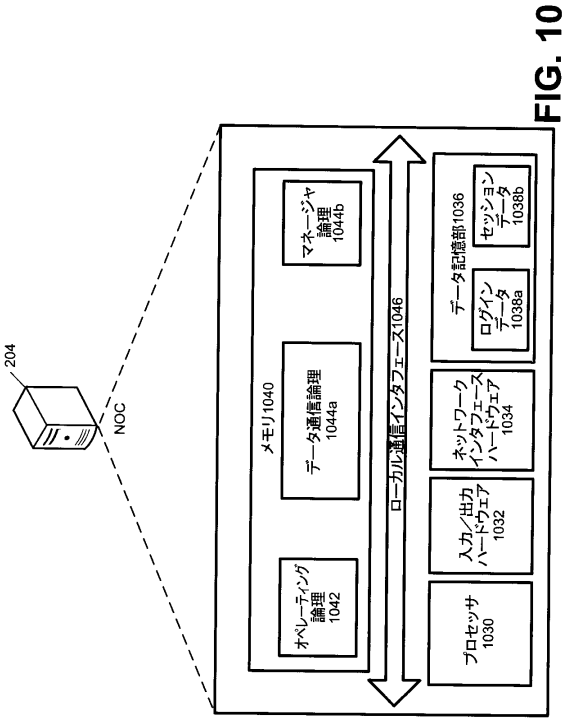

FIG. 10

フロントページの続き

(74)代理人 100117019
弁理士 渡辺 陽一
(74)代理人 100173107
弁理士 胡田 尚則
(72)発明者 ジャック デニス マッキニー
アメリカ合衆国, ケンタッキー ４０５１０, レキシントン, ジェニー ケイト レーン ５００１
(72)発明者 リチャード リー マッキニー
アメリカ合衆国, ワシントン ディーシー ２００２４, ノース ストリート サウスウエスト ５３０, アパートメント エス３０５

審査官 大石 博見

(56)参考文献 特開２０１１－１８８４４８（ＪＰ, Ａ）
米国特許出願公開第２００７／０１８０１４２（ＵＳ, Ａ1）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ １２／７０
Ｇ０６Ｆ １３／００
Ｈ０４Ｌ １２／４６
Ｈ０４Ｌ １２／７４９