(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5948647号
(P5948647)
(45)発行日　平成28年7月6日(2016.7.6)　(24)登録日　平成28年6月17日(2016.6.17)

(51)Int.Cl.　　F I
H04L 12/749 (2013.01)　　H04L 12/749
H04L 12/70 (2013.01)　　H04L 12/70　B

請求項の数 8　(全 12 頁)

(21)出願番号　特願2014-504260 (P2014-504260)
(86)(22)出願日　平成24年4月5日(2012.4.5)
(65)公表番号　特表2014-512142 (P2014-512142A)
(43)公表日　平成26年5月19日(2014.5.19)
(86)国際出願番号　PCT/EP2012/056304
(87)国際公開番号　WO2012/139971
(87)国際公開日　平成24年10月18日(2012.10.18)
審査請求日　平成27年4月2日(2015.4.2)
(31)優先権主張番号　13/084,525
(32)優先日　平成23年4月11日(2011.4.11)
(33)優先権主張国　米国(US)

(73)特許権者　506016691
スカイプ
アイルランド　ダブリン　２　サー・ジョン・　ロジャーソンズ・キー　７０
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(72)発明者　カウフマン，マシュー
アメリカ合衆国　カリフォルニア州　９５０６０，　イオニー　ドーン，ブレイモア・ドライブ　１５５

最終頁に続く

(54)【発明の名称】ネットワーク・アドレスを変換するシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
ピアツーピアネットワーク上の第１のピアホストにおいてインターネット・プロトコル・バージョン４（ＩＰｖ４）アドレス・リテラルからインターネット・プロトコル・バージョン６（ＩＰｖ６）アドレスを生成する、コンピュータ実装される方法であって、
第２のピアホストから前記ＩＰｖ４アドレス・リテラルを受信する段階と、
受信したＩＰｖ４アドレス・リテラルをドメイン名変換サーバーのドメイン名付加することによって第一のピアホストにおいてホスト名を構築する段階であって、前記ドメイン名変換サーバーは、前記ＩＰｖ４アドレス・リテラルを含むホスト名を解釈してＩＰｖ４アドレス・リテラルを含むＡレコードを生成するよう構成されている、段階と、
構築したホスト名を前記ドメイン名変換サーバーに送信する段階と、
前記送信する段階に応じて、前記Ａレコードから生成された合成ＩＰｖ６アドレスを受信する段階であって、前記合成ＩＰｖ６アドレスはネットワーク・アドレス変換（ＮＡＴ６４）サーバーを同定する第一の部分および前記ＩＰｖ４アドレス・リテラルに関連付けられたＩＰｖ４ホストを同定する第二の部分を含む段階と、
受信した合成ＩＰｖ６アドレスを用いて、前記ＮＡＴ６４サーバーを通じて、前記Ａレコードで同定された前記ＩＰｖ４ホストに接続する段階とを有する
方法。
【請求項２】
構築されたホスト名をドメイン名変換サーバーに送信する段階により、ドメイン名サー

バーが合成ＩＰｖ６アドレスを生成可能であり、前記ドメイン名サーバーは、
前記構築されたドメイン名によって同定されるドメイン名変換サーバーに問い合わせして前記Ａレコードを取得する段階と；
前記Ａレコードを既知のＮＡＴ６４サーバーのアドレスと組み合わせて前記合成ＩＰｖ６アドレスを形成する、前記ＮＡＴ６４サーバーはＩＰｖ４ホストとＩＰｖ６ホストとの間で変換するための使用可能である、段階とを実行する、
請求項１記載の方法。
【請求項３】
前記第一のピアホストにおいて複数の合成的に生成されたＩＰｖ６アドレスを解析して、前記ＩＰｖ４リテラルを合成ＩＰｖ６アドレスにエンコードするために使われている符号化スキームを判別する段階をさらに含む、請求項２記載の方法。
【請求項４】
前記解析が、前記合成ＩＰｖ６アドレスと、該ＩＰｖ６アドレスのそれぞれを生成するために使われたＩＰｖ４リテラル・アドレスとの間の相関付けを実行して、前記ＩＰｖ４アドレスがどのように前記合成ＩＰｖ６アドレス内にエンコードされているかを識別することを含む、請求項３記載の方法。
【請求項５】
ひとたび前記符号化スキームが判別されたら、その後、前記第一のピアホストにおいて合成ＩＰｖ６アドレスを生成する段階をさらに含む、請求項３記載の方法。
【請求項６】
ピアツーピアネットワーク上の第１のピアホストにおいて、インターネット・プロトコル・バージョン４（ＩＰｖ４）アドレス・リテラルからインターネット・プロトコル・バージョン６（ＩＰｖ６）アドレスを生成するコンピュータ実装されるシステムであって、当該システムはプログラム・コードを記憶するメモリおよびプロセッサを有し、前記プロセッサは前記プログラム・コードを処理して：
第２のピアホストからＩＰｖ４アドレス・リテラルを受信する段階と、
受信したＩＰｖ４アドレス・リテラルをドメイン名変換サーバーのドメイン名に付加することによって第一のピアホストにおいてホスト名を構築する段階であって、前記ドメイン名変換サーバーは、前記ＩＰｖ４アドレス・リテラルを含む前記ホスト名を解釈してＩＰｖ４アドレス・リテラルを含むＡレコードを生成するよう構成されている、段階と、
構築されたホスト名をドメイン名変換サーバに送信する段階と、
前記送信する段階に応じて、Ａコードから生成された合成ＩＰｖ６アドレスを受信する段階であって、前記合成ＩＰｖ６アドレスはネットワーク・アドレス変換（ＮＡＴ６４）サーバーを同定する第一の部分および前記ＩＰｖ４アドレス・リテラルに関連付けられたＩＰｖ４ホストを同定する第二の部分を含む段階と、
受信された前記合成ＩＰｖ６アドレスを用いて、前記ＮＡＴ６４サーバーを通じて、前記Ａレコードにより同定されたＩＰｖ４ホストに接続する段階とを含む動作を実行する、システム。
【請求項７】
構築されたホスト名をドメイン名変換サーバに送信する段階は、ドメインサーバーが合成ＩＰｖ６アドレスを生成できるようにし、前記ドメインサーバーは、
前記構築されたドメイン名によって同定されるドメイン名変換サーバーに問い合わせして前記Ａレコードを取得する段階と；
前記Ａレコードを既知のＮＡＴ６４サーバーのアドレスと組み合わせて前記合成ＩＰｖ６アドレスを形成する、前記ＮＡＴ６４サーバーはＩＰｖ４ホストとＩＰｖ６ホストとの間で変換するための使用可能である、段階とを実行する、
請求項６記載のシステム。
【請求項８】
コンピュータによって実行されたときに前記コンピュータに請求項１ないし５のうちいずれか一項記載の方法を実行させるコンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概括的にはデータ処理システムの分野に関する。より詳細には、本発明は、ネットワーク・アドレスを変換する改善されたシステムおよび方法に関する。
【背景技術】
【０００２】
現在、インターネット・プロトコル・バージョン４（IPv4）およびインターネット・プロトコル・バージョン６（IPv6）と称される、TCP/IPネットワーキング・プロトコルの二つの形がある。IPv6は、現在インターネットを横断して幅広く使われているインターネット・プロトコル・バージョン４（IPv4）の後継となるべく設計されている。IPv6はまた、異なるアドレッシング空間および接続プロトコルを使っており、IPv4とはほぼ非互換である。その結果、図１に示されるように、IPv6インターフェースをもつがIPv4インターフェースをもたないよう構成されたクライアント１０１またはサーバー１０２は、IPv6ネットワーク１１０を通じて直接通信することはできるが、IPv4ネットワーク１１１を通じてはできない。同様に、IPv4インターフェースをもつがIPv6インターフェースをもたないよう構成されたクライアント１２１またはサーバー１２２は、IPv4ネットワーク１１１を通じて直接通信することはできるが、IPv6ネットワーク１１０を通じてはできない。図のように、IPv4およびIPv6インターフェースの両方を備えるある種のクライアント１００およびサーバー（図示せず）は、IPv4およびIPv6両方のネットワークを通じて通信できる。
【０００３】
IPv4インフラストラクチャーからIPv6の次世代アドレッシング・システムへのインターネットの移行を容易にするためにさまざまなIPv6遷移機構が規定されてきた。そのような遷移機構の二つは、NAT64（Network Address Translation 64［ネットワーク・アドレス変換６４］）およびDNS64（Domain Name Service 64［ドメイン名サービス６４］）である。NAT64は、IPv6のみのホストがIPv4のみのホストと通信できるようにするためにネットワーク・アドレス変換機能を実行する。図１に示されるように、NAT64サーバー１１５は、少なくとも一つのIPv4アドレスおよび32ビットのIPv6ネットワーク・セグメントのための端点としてはたらく。IPv6ホストは、これらのビットを使って通信したいIPv4アドレスを埋め込み、その諸パケットを結果として得られるアドレスに送る。するとNAT64サーバーが、IPv6アドレスとIPv4アドレスとの間のNATマッピングを生成する。DNS64サーバー１１６は、典型的にIPv4アドレスをホスト名と関連付けるたいていのDNSサーバーによって返される「A」レコードを、合成のIPv4アドレス・マッピングされたIPv6アドレスを含む「AAAA」レコードに変換する。この合成アドレスは、NAT64変換器のIPv6インターフェースをポイントし、このアドレスの一部は実際のIPv4アドレスをエンコードする（IPv4宛先と接続するためにNAT64変換器が使うため）。
【０００４】
たとえば、図１において、IPv6クライアント１０１は、IPv4サーバー１２２に関連付けられたネットワーク名（たとえばwww.skype.com）を使ってDNS64サービス１１６にDNS問い合わせをすることによってIPv4サーバー１２２と通信しうる。応答して、DNS64サービスは、NAT64サーバー１１５を同定するIPv4マッピングされたIPv6アドレスをIPv6クライアント１２２に返す。次いでIPv6クライアント１０１がNAT64サーバー１１５を介してIPv4サーバー１２２と接続する。
【０００５】
しかしながら、IPv6のみのクライアントが「IPv4アドレス・リテラル」――すなわち、DNS探索以外の機構を介して受け取ったIPv4アドレス――をもつ場合には、上記の機構は失敗する。たとえば、Bittorrent（商標）クライアントおよびSkype（商標）クライアントのようなある種のピアツーピア（P2P）クライアントは、問い合わせに応答して他のクライアントからIPv4アドレス・リテラルを受け取ることがある。これらの場合、クライアントは、IPv4インターフェースをもっていなければ、IPv4アドレス・リテラルを使うこと

ができない。

【０００６】

これらの問題に対処するためにいくつかの手法が提案されているが、みな何らかの点で欠点があり、NAT64/DNS64に対する変更（最低限）および／またはクライアント・オペレーティング・システム・ネットワーク・スタックへの変更を要求することがある。たとえば、いくつかの提案が非特許文献１において記載されている。この文献の4.3節に記載される一つの提案は、本特許出願に特に関連がある。この節は、IPv4リテラルをもつIPv6ホストがいかにしてよく知られたIPv4のみの完全修飾ドメイン名（FQDN: Fully Qualified Domain Name）のAAAAレコードについてDNS問い合わせを送ることができるかを記述している。ホストが否定的な返答を受け取る場合、ネットワーク上にはDNS64またはNAT64サービスはない。ホストが返答を受け取る場合、ネットワークはIPv6アドレス合成を利用しているはずである。合成されたAAAAリソース・レコードを受信したのち、ホストは受信されたIPv6アドレスを調べて、（たとえば合成されたIPv6アドレスから既知のIPv4アドレスを「差し引く」ことによって）NAT64およびDNS64によって使われているネットワーク固有プレフィックス（NSP: network specific prefix）を解読しようと試みる。ひとたびNSPがわかれば、ホストはそのIPv4アドレスを使って、自らのIPv6アドレスを合成することができる。

【先行技術文献】

【非特許文献】

【０００７】

【非特許文献１】Analysis of Solution Proposals for Hosts to Learn NAT64 Prefix, Behavior Engineering for Hindrance Avoidance (BEHAVE)、2010年10月17日

【発明の概要】

【発明が解決しようとする課題】

【０００８】

しかしながら、IPv4アドレスをIPv6アドレス内に埋め込むにはさまざまな異なるエンコード技法が使用されうるので、NSPを決定するためにIPv4アドレスから「差し引く」ことは常に可能でないことがある。その結果、ある種のクライアントおよび／またはサーバーについてIPv4リテラルをIPv6アドレスに変換するためには追加的な技法が必要とされる。

【課題を解決するための手段】

【０００９】

コンピュータ・ネットワーク上でIPv6アドレスとIPv4アドレスの間の変換をするための装置および方法が記述される。たとえば、インターネット・プロトコル・バージョン４（IPv4）IPv4アドレス・リテラルからインターネット・プロトコル・バージョン６（IPv6）IPv6アドレスを生成するための方法のある実施形態は：IPv4アドレス・リテラルを第一のドメイン名サーバーのドメイン名と組み合わせることによって第一のホストにおいてドメイン名問い合わせのためのホスト名を構築する段階であって、前記第一のドメイン名サーバーは、IPv4アドレスを含むAレコードを生成するためにIPv4アドレス・リテラルを含むホスト名を解釈するよう構成されている段階を含み；前記Aレコードは、合成IPv6アドレスを生成するために使用可能であり、前記合成IPv6アドレスはネットワーク・アドレス変換（NAT）64サーバーを同定する第一の部分およびIPv4アドレス・リテラルに関連付けられたIPv4ホストを同定する第二の部分を含み；当該方法はさらに、前記第一のホストにおいて前記合成IPv6アドレスを受信する段階を含み、前記合成IPv6アドレスは前記NAT64サーバーを通じて前記IPv4ホストに接続するために前記第一のホストによって使用可能である。

【図面の簡単な説明】

【００１０】

本発明のよりよい理解は、次の図面との関連で下記の詳細な説明から得ることができる。

【図１】NAT64サービスおよびDNS64サービスを含む従来技術のネットワーク・アーキテクチャを示す図である。
【図２】本発明のある実施形態に基づくシステム・アーキテクチャを示す図である。
【図３】合成IPv6アドレス符号化方式を決定し、該符号化方式を使って剛性IPv6アドレスを生成するためのソフトウェア・アーキテクチャを示す図である。
【図４】ホストがNDS64/NAT64環境にあるかどうかを検出するための方法のある実施形態を示す図である。
【図５】IPv4リテラル・アドレスを使って合成IPv6アドレスを生成する方法のある実施形態を示す図である。
【図６】NAT64アドレスを決定するために複数のDNS応答を解析するための方法のある実施形態を示す図である。
【図７】本発明のある実施形態に基づく例示的なホストのシステム・アーキテクチャを示す図である。
【発明を実施するための形態】
【００１１】
以下の記述では、説明の目的のために以下に記述する本発明の実施形態の十全な理解を提供するよう数多くの個別的詳細が記述される。しかしながら、本発明の実施形態がこれらの個別的詳細のいくつかなしでも実施されうることは当業者には明白であろう。他方、よく知られた構造および装置は、本発明の実施形態の根底にある原理を埋没させるのを避けるために、ブロック図の形で示されている。
【００１２】
本発明のある実施形態は上記で論じた限界に対処するため、特別に作られたDNS問い合わせをアプリケーション・プロバイダー（または他のサードパーティー）によって運用される特化したDNS変換サーバーを使って、NAT64/DNS64が、他のアプリケーション機能の結果として手元にあることがありうる何らかのIPv4リテラル・アドレスについての合成されたマッピングを提供できるようにする。たとえば、ピアツーピア（P2P）実装において、これらのリテラル・アドレスは、P2Pネットワーク上で他のクライアントまたはサーバーからの問い合わせに応答して返されてもよい。しかしながら、本発明の根底にある原理はP2P実装に限定されるものではない。
【００１３】
図２に示されるある実施形態では、IPv4アドレス・リテラルが手元にあるとき、クライアント２００上で実行されるIPv4リテラル・アドレス処理モジュール２０４は、<IPv4アドレス>.<サーバー名>.<アプリケーション・プロバイダー>に関連付けられたAAAA（IPv6アドレス）レコードを要求するDNS問い合わせを構築する。ここで、<IPv4アドレス>はIPv4リテラルであり、<サーバー名>.<アプリケーション・プロバイダー>はDNS変換サーバー２０１を同定する。例として、IPv4アドレス・リテラルが172.16.254.1であり、DNS変換サーバー２０１がnat64-discovery.example.comである場合、DNS問い合わせは172.16.254.1.nat64-discovery.example.comへとなる。この実施形態において、"nat64-discovery.example.com"を受け持つDNS変換サーバー２０１は、任意の問い合わせ"w.x.y.z.nat64-discovery.example.com"についてA（IPv4アドレス）レコード"w.x.y.z"を返す特化したサーバーである。結果として、上記の例では、"172.16.254.1"を返す。
【００１４】
動作では、最初、問い合わせ172.16.254.1.nat64-discovery.example.comが、特化したDNS変換サーバー２０１に問い合わせするDNS64サーバー２０２によって受信される。DNS変換サーバー２０１は、Aレコード172.16.254.1をもって応答し、それをDNS64サーバーが合成IPv6アドレス（AAAAレコード）を構築するために使う。次いでDNS64サーバーはこの合成IPv6アドレスをクライアント２００上のIPv4リテラル・アドレス処理論理２０４に返す。次いで、クライアント２００はNAT64装置１１５を通じてIPv4アドレス172.16.254.1によって同定される（すなわち、合成されたIPv6アドレスによって同定される）リモート・クライアント２２０－２２１またはサーバー２２２への接続を開いてもよい。

【００１５】
IPv4リテラル・アドレス処理モジュール２０４は、本発明の根底にある原理に従いながら、多様な仕方で実装されうる。たとえば、ある実施形態では、IPv4リテラル・アドレス処理モジュール２０４は、より大きなピアツーピア（P2P）アプリケーション・プログラム（たとえばBittorrentクライアントまたはSkypeクライアントなど）または他の型のアプリケーションのコンポーネントを有する。代替的または追加的に、IPv4リテラル・アドレス処理モジュールは、クライアント２００上で実行されるオペレーティング・システムのコンポーネントとして（たとえばオペレーティング・システムとともに提供されるネットワーキング・スタックの一部として）提供されてもよい。しかしながら、本発明の根底にある原理は、IPv4リテラル・アドレス処理モジュール２０４のいかなる特定の実装にも限定されない。

【００１６】
IPv4リテラル・アドレス処理モジュール２０４によって生成される問い合わせは、NAT64/DNS64が存在しない場合には失敗の結果を与えうることを注意しておく。その結果、失敗が検出される場合（または指定された回数の失敗が検出される場合）、さらなる試みはなされなくてもよい。NAT64/DNS64が存在せず、IPv4リテラル・アドレスが現在使用できないことを示すフラグがセットされてもよい（利用可能なIPv4インターフェースはないものとしている）。

【００１７】
本願の背景のセクションで論じたように、単一の応答に基づいて厳密なマッピング・スキームを決定することはできないので、単一の問い合わせから帰結する合成されたIPv6プレフィックスを抽出しようと試みることは十分ではない。たとえば、マッピング・スキームは線形でなくてもよく（その場合、単純なビットごとの置換は機能しない）、および／または複数のNAT64装置が負荷均衡化を行うDNS64とともに使われていてもよく、および／または所与のIPv4宛先についてどのNAT64が選択されるかを最適化するために他の技法が使われていてもよい。

【００１８】
しかしながら、IPv4リテラル・アドレス問い合わせに対する複数の応答を発見法的に〔ヒューリスティックに〕解析することによってマッピング・スキームを解読することが可能であることがある。結果として、図３に示される本発明のある実施形態では、IPv4リテラル・アドレス処理モジュール２０４は、手元にあるすべてのIPv4リテラル・アドレス（またはその部分集合）について上記の問い合わせを実行し、対応する合成的に生成されたIPv6アドレスを受信する。次いで、ある実施形態では、ネットワーク固有プレフィックス（NSP）解析モジュール２０５が、DNS64/NAT64システムによって使用されているIPv6符号化スキームを決定しようと試みるために、前記問い合わせの結果を解析する。たとえば、IPv4アドレスが単にIPv6アドレスの特定の32ビット・フィールド（たとえば上位32ビット／下位32ビット）内に埋め込まれる場合には、NSP解析モジュール２０５は、IPv4リテラルと結果として得られる合成IPv6アドレスとの間の相関付け（correlation）を実行することによって符号化スキームを同定してもよい。ひとたび符号化スキームが決定されたら、クライアント２００上で実行された合成IPv6アドレス生成器２０６は、任意のIPv4リテラルを使ってIPv6アドレスを合成的に生成しうる（少なくともクライアントが同じDNS64/NAT64環境内である限りは）。より進んだ処理技法が、IPv6アドレスから既知のIPv4アドレスを「差し引い」て合成IPv6符号化スキームに到達するために用いられてもよい（たとえば非特許文献１に記載されるような）。

【００１９】
ホストがNDS64/NAT64環境内であるかどうかを判定する方法の一つの実施形態が、図４に示されている。４０１では、ホストはIPv6ネットワークに接続され、４０２では、ホストは、IPv4アドレスをもつがIPv6アドレスはもたないことがわかっているネットワーク名を使って試験問い合わせを生成する。たとえば、ある実施形態では、試験問い合わせは、<IPv4アドレス>.<サーバー名>.<アプリケーション・プロバイダー>の形を取ってもよい。

もちろん、本発明の根底にある原理に従いながら、他の多様な既知のIPv4ホスト名が使用されうる。試験問い合わせへの応答が４０３で受信され、判定される場合、４０４で、ホストがDNS64/NAT64環境内であるという判定がなされる。次いでホストは上記のようにNSPマッピング・スキームを決定しようと試みてもよい。応答が受信されない場合には、４０５で、ホストがDNS64/NAT64環境内でないという判定がされる。

【００２０】

図５は、IPv4リテラル・アドレスを使ってIPv6ネットワークを通じてIPv4のみのホストに接続するための方法のある実施形態を記述している。この方法のある種の側面は、図２に示したシステム・アーキテクチャに関して上述した。しかしながら、本発明のこの実施形態の根底にある原理はいかなる特定のシステム・アーキテクチャに限定されるものでもない。

【００２１】

５０１では、一つまたは複数のIPv4リテラル・アドレスに帰結する問い合わせが生成される。例として、P2Pクライアント（たとえばBittorrentまたはSkypeクライアント）は問い合わせに応答して一つまたは複数のIPv4リテラルを受信してもよい。５０２では、IPv4リテラル・アドレスは、あらかじめ規定された符号化スキームを使ってネットワーク名に変換される。先の例に戻ると、ネットワーク名は<IPv4アドレス>.<サーバー名>.<アプリケーション・プロバイダー>の形を取ってもよい。ここで、<IPv4アドレス>はIPv4リテラル・アドレスであり、<サーバー名>.<アプリケーション・プロバイダー>は特化したDNS変換サーバーを同定する。５０３では、ネットワーク名を使ってAAAA問い合わせが発され、５０４では、DNS64が問い合わせをDNS変換サーバー（たとえば、ある実施形態では、<サーバー名>.<アプリケーション・プロバイダー>によって同定される）に転送する。５０５では、DNS変換サーバーは前記問い合わせに応答してAレコードを生成し（たとえば、ある実施形態では<IPv4アドレス>）、５０６では、DNS64はIPv6アドレスを合成するためにAレコードを使う。５０７では、IPv6アドレスは要求元のホストに送信され、５０８では、該ホストが合成されたIPv6アドレスを使ってNAT64を通じたIPv4ホストへの接続を開く。

【００２２】

図６は、IPv4リテラルを使って合成IPv6アドレスのために使われるIPv6符号化スキームを検出するための方法のある実施形態を示している。この方法のある種の側面は、図３に示したシステム・アーキテクチャに関して上述した。しかしながら、本発明のこの実施形態の根底にある原理はいかなる特定のシステム・アーキテクチャにも限定されない。

【００２３】

６０１では、IPv4アドレスをもつがIPv6アドレスはもたないことがわかっているホストのネットワーク名を使ってDNS問い合わせが生成される。ある実施形態では、アプリケーション・プロバイダー（すなわち、クライアント・ソフトウェアを提供するエンティティ）は、この要件を満たす複数の既知のネットワーク名（たとえば、test1.nat64-discovery.example.com、test2.nat64-discovery.example.comなど）を提供する。あるいはまた、さまざまなよく知られた公開のホスト名が使用されてもよい。６０２では、前記問い合わせへの応答が、特定のNAT64またはNAT64装置のグループを同定する合成的に生成されたIPv6アドレスの形で受信される。６０３では、それらの応答が解析され、合成IPv6アドレスを生成するために使われた符号化スキームが判別される。例として、各IPv6アドレスは単に、IPv4アドレスをIPv6アドレスの指定された32ビット・フィールド内にエンコードしていてもよく、IPv6アドレスの残りはNAT64サーバーを同定するために使われてもよい。あるいはまた、各ホスト名は、NAT64マッピングにおいてランダムなまたはシーケンシャルなアドレッシング・スロットを割り当てられてもよい。そのような場合、IPv6符号化スキームを決定することは難しい（または不可能である）ことがある。（たとえばIPv6アドレスから既知のIPv4アドレスを「差し引く」ことによって）何らかの形の発見法的解析が符号化スキームを決定するために使われることができるとして、ひとたび決定されれば、６０４において、ホストは、（たとえばP2Pアプリケーションまたは他のアプリケーション型の一部として）任意のIPv4リテラルを使って、IPv6アドレスを合成的に生成することが

できる。

【００２４】

ある実施形態では、上記のようにDNS64サーバー２０２からIPv4 DNS変換器２０１に問い合わせを送信するのではなく、DNS64サーバー２０２は自分自身、前記試験問い合わせからIPv4アドレスを抽出するために必要な論理を含んでいてもよい。先の例に戻ると、試験問い合わせが<IPv4アドレス>.<サーバー名>.<アプリケーション・プロバイダー>の形を取り、ここで、<IPv4アドレス>はIPv4リテラルであり、<サーバー名>.<アプリケーション・プロバイダー>はDNS変換サーバー２０１を同定する場合、DNS64サーバーは、このマッピング方式の知識をもって構成されてもよく、実際に前記問い合わせを行うことなく変換サーバー２０１であるふりをしてもよい。それにより、DNS64サーバー２０２およびDNS変換器サーバー２０１に対する全体的な負荷が軽減される。さまざまな追加的な修正が本発明の根底にある原理の範囲内であると考えられる。

【００２５】

本稿で記述される方法の任意の一つは、汎用コンピュータ・システム、特殊目的コンピュータ・システムおよびモバイル・コンピューティング装置を含む多様な異なるデータ処理装置上で実装されることができる。たとえば、本稿に記載される方法を実行しうるデータ処理システムは、デスクトップ・コンピュータ、ラップトップ・コンピュータ、タブレット・コンピュータ、スマートフォン、携帯電話、携帯情報端末（PDA）、組み込み電子装置または任意の形の消費者電子装置を含みうる。図７は、本発明とともに使用されうる典型的なデータ処理システムの一例を示している。図７はコンピュータ・システムのようなデータ処理システムのさまざまなコンポーネントを示しているが、コンポーネントを相互接続するいかなる特定のアーキテクチャまたは仕方をも表すことは意図されていない。そのような詳細は、本発明と密接な関係はない。また、図示したよりも少数のコンポーネントをもつまたは図７に示したよりも多くのコンポーネントをもつ他の型のデータ処理システムが本発明とともに使われてもよいことも理解されるであろう。図７のデータ処理システムは、マッキントッシュ・コンピュータまたはPCコンピュータであってもよい。図７に示されるように、データ処理システム７０１は、システムのさまざまなコンポーネントを相互接続するはたらきをする一つまたは複数のバス７０９を含む。一つまたは複数のプロセッサ７０３が、当技術分野で知られているように、一つまたは複数のバス７０９に結合されている。メモリ７０５はDRAMまたは不揮発性RAMであってもよく、あるいはフラッシュメモリまたは他の型のメモリであってもよい。このメモリは、当技術分野で既知の技法を使って前記一つまたは複数のバス７０９に結合される。データ処理システム７０１はまた、不揮発性メモリ７０７をも含むことができる。不揮発性メモリ７０７はハードディスク・ドライブまたはフラッシュメモリまたは光磁気ドライブまたは磁気メモリまたは光学式ドライブまたはシステムから電力が除かれたとしてもデータを維持する他の型のメモリ・システムであってもよい。不揮発性メモリ７０７およびメモリ７０５はいずれも前記一つまたは複数のバスに、既知のインターフェースおよび接続技法をつかって結合される。本稿に記載されるユーザー・インターフェース特徴または実施形態の任意の物を表示できるディスプレイ装置７１３上に表示されるべき表示データを受領するために、ディスプレイ・コントローラ７１１が前記一つまたは複数のバス７０９に結合される。ディスプレイ装置７１３は、タッチスクリーンを提供するために統合されたタッチ入力を含むことができる。データ処理システム７０１は、一つまたは複数のマウス、タッチスクリーン、タッチパッド、ジョイスティックおよび当技術分野において知られている物を含む他の入力装置ならびに出力装置（たとえばスピーカー）といった一つまたは複数のI/O装置のためのインターフェースを提供する一つまたは複数の入出力（I/O）コントローラ７１５をも含むことができる。入出力装置７１７は、当技術分野で知られているように一つまたは複数のI/Oコントローラ７１５を通じて結合される。図７は不揮発性メモリ７０７およびメモリ７０５が前記一つまたは複数のバスに、ネットワーク・インターフェースを通じてではなく直接的に結合されることを示しているが、データ処理システムは、システムからリモートな不揮発性メモリを利用してもよいことは理解されるであろう。リモートな不揮発

性メモリとは、モデムまたはイーサネット（登録商標）インターフェースといったネットワーク・インターフェースまたは無線WiFiトランシーバもしくは無線セルラー電話トランシーバもしくはそのようなトランシーバの組み合わせといった無線インターフェースを通じてデータ処理システムに結合されるネットワーク記憶装置などである。当技術分野で知られているように、前記一つまたは複数のバス７０９は、さまざまなバスの間を相互接続するための一つまたは複数のブリッジまたはコントローラまたはアダプターを含んでいてもよい。ある実施形態では、I/0コントローラ７１５はUSB周辺機器を制御するためのUSBアダプターを含み、イーサネット・ポートまたは無線トランシーバまたは諸無線トランシーバの組み合わせを制御することができる。本発明の諸側面が少なくとも部分的にソフトウェアにおいて具現されうることは明白であろう。すなわち、本稿に記載される技法および方法は、有体の非一時的なメモリに含まれる命令のシーケンスを実行するそのプロセッサに応答して、データ処理システムにおいて実行されてもよい。有体な非一時的なメモリは、メモリ７０５または不揮発性メモリ７０７またはそのようなメモリの組み合わせといったものであり、こうしたメモリのそれぞれは機械可読な、有体の記憶媒体の一つの形である。さまざまな実施形態において、本発明を実装するためにソフトウェア命令と組み合わせて固定構成の回路が使用されてもよい。このように、上記技法はハードウェア回路およびソフトウェアのいかなる特定の組み合わせにも、またデータ処理システムによって実行される命令のいかなる特定の源にも限定されない。

【００２６】

以上の明細書では、本発明についてその個別的な例示的な実施形態を参照して記述してきた。付属の請求項に記載される本発明のより広義の精神および範囲から外れることなくそれにさまざまな繻子映画ないすることは明白であろう。よって、明細書および図面は、制約する意味ではなく、例解する意味で見なされるべきものである。

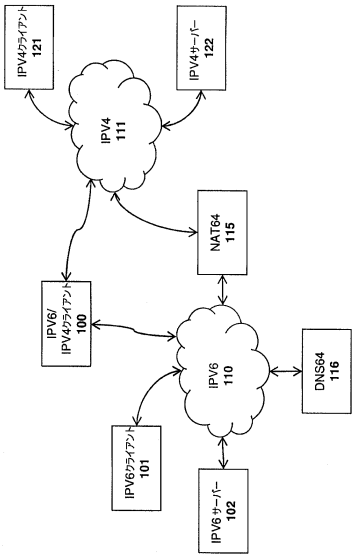
【００２７】

本発明の諸実施形態は、上記に述べたようなさまざまなステップを含みうる。それらのステップは、汎用または特殊目的プロセッサにある種のステップを実行させる機械実行可能な命令において具現されてもよい。あるいはまた、これらのステップは、該ステップを実行するための固定構成の論理を含む特定のハードウェア・コンポーネントによって、あるいはプログラムされたコンピュータ・コンポーネントおよびカスタムのハードウェア・コンポーネントの任意の組み合わせによって実行されてもよい。本発明の諸要素は、機械実行可能なプログラム・コードを記憶するための機械可読媒体として提供されてもよい。機械可読媒体は、これに限られないが、フロッピー（登録商標）ディスケット、光ディスク、CD-ROMおよび光磁気ディスク、ROM、RAM、EPROM、EEPROM、磁気もしくは光学式カードまたは電子的なプログラム・コードを記憶するのに好適な他の型のメディア／機械可読媒体を含みうる。

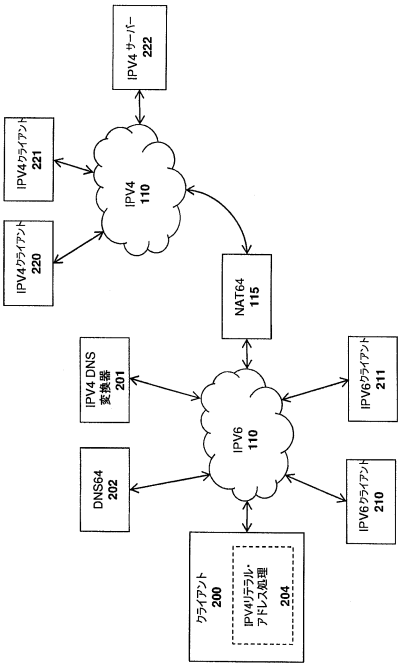
【００２８】

上記の記述を通じて、説明の目的のために、本発明の十全な理解を与えるよう、数多くの個別的詳細が記述された。しかしながら、当業者には、本発明がこれらの個別的詳細のいくつかなしでも実施されうることは明白であろう。たとえば、当業者には、本稿に記載される機能モジュールおよび方法がソフトウェア、ハードウェアまたはそれらの任意の組み合わせとして実装されうることは明白であろう。さらに、本発明のいくつかの実施形態が本稿ではクライアントP2Pアプリケーションのコンテキスト内で記載されているが、本発明の根底にある原理はサーバー・アプリケーションの形でまたはクライアント・アプリケーションの他の任意の形で実装されてもよい。よって、本発明の範囲および精神は、請求項の記載において判断されるべきである。

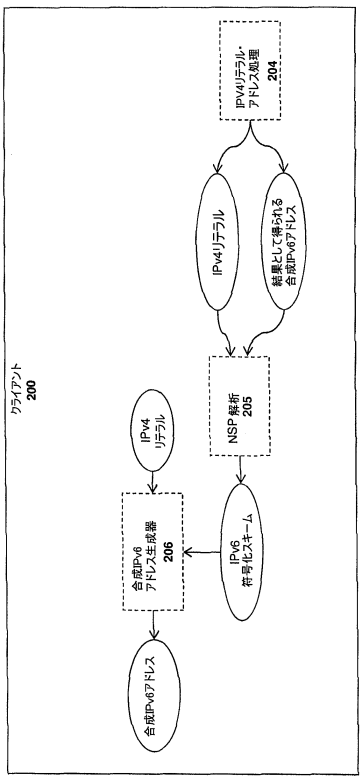
【図１】


IPV4クライアント
121
IPV4サーバー
122
IPV4
111
NAT64
115
IPV6/
IPV4クライアント
100
IPV6
110
DNS64
116
IPV6クライアント
101
IPV6サーバー
102

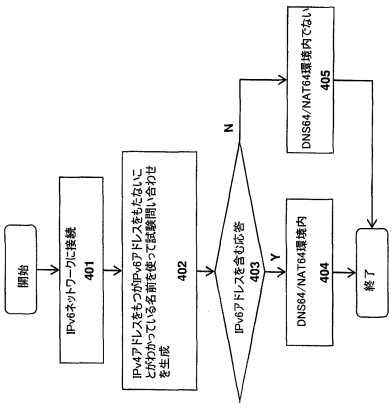
【図２】


IPV4サーバー
222
IPV4クライアント
221
IPV4
110
IPV4クライアント
220
NAT64
115
IPV4 DNS
変換器
201
IPV6
110
IPV6クライアント
211
DNS64
202
IPV6クライアント
210
クライアント
200
IPV4リテラル・
アドレス処理
204

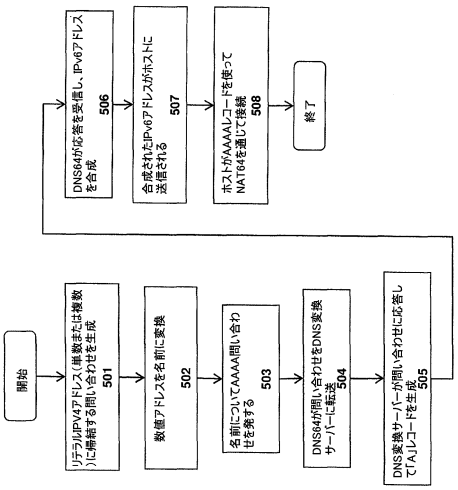
【図３】


クライアント
200
IPV4リテラル・
アドレス処理
204
IPV4リテラル
結果として得られる
合成IPv6アドレス
NSP解析
205
IPV4
リテラル
IPv6
符号化スキーム
合成IPv6
アドレス生成器
206
合成IPv6アドレス

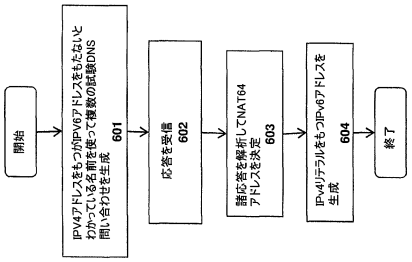
【図４】


開始
IPv6ネットワークに接続
401
IPv4アドレスをもつがIPv6アドレスをもたないに
とがかっている名前を使って試験問い合わせ
を生成
402
IPv6アドレスを含む応答
403
N
Y
DNS64/NAT64環境内でない
405
DNS64/NAT64環境内
404
終了

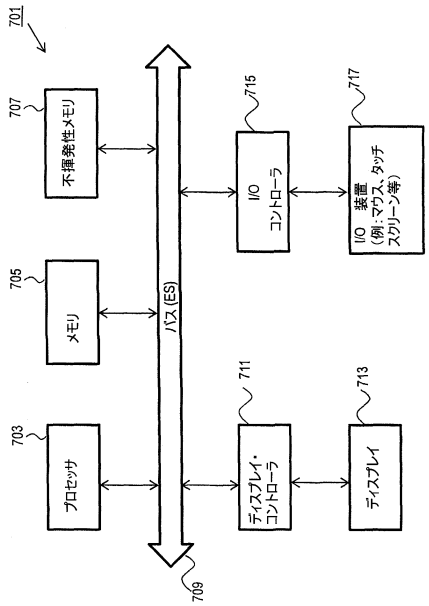
【図５】


開始
リテラルIPv4アドレス(単数または複数)に関連する問い合わせを生成
501
数値アドレスを名前に変換
502
名前についてAAAA問い合わせを発する
503
DNS64が問い合わせをDNS変換サーバーに転送
504
DNS変換サーバーが問い合わせに応答してAレコードを生成
505
DNS64が応答を受信し、IPv6アドレスを合成
506
合成されたIPv6アドレスがホストに送信される
507
ホストがAAAAレコードを使ってNAT64を通じて接続
508
終了

【図６】


開始
IPv4アドレスをもつがIPv6アドレスをもたないとわかっている名前を使って複数の試験的DNS問い合わせを生成
601
応答を受信
602
試験応答を解析してNAT64アドレスを決定
603
IPv4リテラルをもつIPv6アドレスを生成
604
終了

【図７】


701
707
不揮発性メモリ
705
メモリ
703
プロセッサ
709
バス(ES)
711
ディスプレイ・コントローラ
713
ディスプレイ
715
I/O コントローラ
717
I/O 装置(例:マウス、タッチスクリーン等)

フロントページの続き

審査官　安藤　一道

(56)参考文献　特開平１０－１３６０５２（ＪＰ，Ａ）
米国特許出願公開第２００４／０１６５６０２（ＵＳ，Ａ１）
特表２０１３－５２７６３２（ＪＰ，Ａ）

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