(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4771553号
(P4771553)
(45)発行日　平成23年9月14日(2011.9.14)　(24)登録日　平成23年7月1日(2011.7.1)

(51)Int.Cl.　F I
H04L 12/46 (2006.01)　H04L 12/46　V

請求項の数 8　(全 13 頁)

(21)出願番号	特願2007-541930 (P2007-541930)
(86)(22)出願日	平成17年11月11日 (2005.11.11)
(65)公表番号	特表2008-521305 (P2008-521305A)
(43)公表日	平成20年6月19日 (2008.6.19)
(86)国際出願番号	PCT/EP2005/055909
(87)国際公開番号	WO2006/053856
(87)国際公開日	平成18年5月26日 (2006.5.26)
審査請求日	平成20年7月31日 (2008.7.31)
(31)優先権主張番号	10/992,380
(32)優先日	平成16年11月18日 (2004.11.18)
(33)優先権主張国	米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】ＩＰｖ６パケットをトンネリングする方法、システム、及びコンピュータ・プログラム

(57)【特許請求の範囲】
【請求項１】
ＩＰｖ６パケットをトンネリングする方法であって、
発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを発信元ＩＰｖ６ホストから受信するステップと、
発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付けるデータ構造から検索された宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを、発信元ＩＰｖ６ホストから受信するステップと、
前記発信元ＩＰｖ６境界ルータが前記ＩＰｖ６パケットに対して受信した前記ＩＰｖ４アドレスを前記ＩＰｖ６パケットの拡張ヘッダにカプセル化するステップと、
前記カプセル化パケットを前記ＩＰｖ４アドレス上の宛先ＩＰｖ６境界ルータに送信するステップと、
を有する方法。
【請求項２】
前記宛先ＩＰｖ６境界ルータが前記カプセル化パケットを非カプセル化するステップと、前記宛先ＩＰｖ６境界ルータが前記非カプセル化パケットを前記ＩＰｖ６宛先アドレスを有する宛先ホストに転送するステップと、を更に有する請求項１に記載の方法。
【請求項３】
前記宛先ＩＰｖ６境界ルータが前記カプセル化パケットを非カプセル化する前記ステップは、前記発信元境界ルータによって追加されたＩＰｖ４ヘッダを前記カプセル化パケッ

トから取り除くステップを更に有する、請求項２に記載の方法。
【請求項４】
前記ＩＰｖ６ホストが前記パケットのＩＰｖ６宛先アドレスを識別するステップと、
宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを、ＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付けるデータ構造から検索するステップと、
前記ＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを前記発信元ＩＰｖ６境界ルータに送信するステップと、
前記ＩＰｖ６パケットに関連する宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを発信元ＩＰｖ６境界ルータに提供するステップと、
を更に有する請求項１に記載の方法。
【請求項５】
ＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付ける前記データ構造は、ＤＮＳリソース・レコードを更に有する、請求項４に記載の方法。
【請求項６】
前記発信元ＩＰｖ６境界ルータが前記ＩＰｖ６パケットをＩＰｖ４パケットにカプセル化する前記ステップは、ＩＰｖ４ヘッダを前記ＩＰｖ６パケットに追加するステップを更に有する、請求項１に記載の方法。
【請求項７】
ＩＰｖ６パケットをトンネリングするシステムであって、
発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを発信元ＩＰｖ６ホストから受信する手段と、
発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付けるデータ構造から検索された宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを、発信元ＩＰｖ６ホストから受信する手段と、
前記発信元ＩＰｖ６境界ルータが前記ＩＰｖ６パケットに対して受信した前記ＩＰｖ４アドレスを前記ＩＰｖ６パケットの拡張ヘッダにカプセル化する手段と、
前記カプセル化パケットを前記ＩＰｖ４アドレス上の宛先ＩＰｖ６境界ルータに送信する手段と、
を有するシステム。
【請求項８】
ＩＰｖ６パケットをトンネリングするコンピュータ・プログラムであって、
発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを発信元ＩＰｖ６ホストから受信する手段、
発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付けるデータ構造から検索された宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを、発信元ＩＰｖ６ホストから受信する手段、
前記発信元ＩＰｖ６境界ルータが前記ＩＰｖ６パケットに対して受信した前記ＩＰｖ４アドレスを前記ＩＰｖ６パケットの拡張ヘッダにカプセル化する手段、
前記カプセル化パケットを前記ＩＰｖ４アドレス上の宛先ＩＰｖ６境界ルータに送信する手段、
としてコンピュータを機能させる、コンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はデータ処理の分野に関するものであり、より詳細にはＩＰｖ６パケットをトンネリングする方法、システム、及び製品に関するものである。
【背景技術】
【０００２】
インターネット・プロトコル・バージョン６（「ＩＰｖ６」）は、広く使用されているインターネット・プロトコル・バージョン４（「ＩＰｖ４」）の進化版として設計された

インターネット・プロトコル（ＩＰ）である。ＩＰｖ６では、アドレス空間が拡大され、ヘッダ・フォーマットが簡略化され、認証／プライバシー、アドレス割当ての自動構成、及び新しいＱｏＳ機能がサポートされている。

【０００３】

ＩＰｖ６の使用が益々増加しているにも関わらず、インターネットの主要なプロトコルは依然としてＩＰｖ４であることから、前記ＩＰｖ４のルーティング・インフラストラクチャを使用してＩＰｖ６パケットを送信するための移行の仕組みが提供されてきている。「トンネリング」を用いると、ＩＰｖ６と互換性のあるホスト又はルータがＩＰｖ６パケットを既存のＩＰｖ４ネットワークを介して送信することが可能となる。ＩＰｖ６パケットをＩＰｖ４ネットワークを介してトンネリングすることは、典型的には前記ＩＰｖ６パケットをＩＰｖ４パケットにカプセル化し、前記パケットをＩＰｖ４と互換性のあるルータに送信することによって実施される。ＩＰｖ６パケットをＩＰｖ４パケットにカプセル化することは、前記パケットをＩＰｖ４ネットワークを介して送信できるようにするＩＰｖ４ヘッダを前記パケットに追加することによって実施される。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

ＩＰｖ６パケットをＩＰｖ４ネットワークを介してトンネリングする従来の技法では、典型的にはＩＰｖ６と互換性のある特定の発信元ルータを、カプセル化パケットを受信するＩＰｖ６と互換性のある別のルータのＩＰｖ４宛先アドレスを用いて手動で構成する必要がある。ルータをそのようなＩＰｖ４宛先アドレスを用いて手動で構成することはシステム管理者にとって時間の掛かる煩雑な作業である。また、そのような手動構成ではＩＰｖ６と互換性のあるルータ上で限られた数の宛先アドレスしか構成されないので、カプセル化パケットのルーティングの柔軟性が低下する。したがって、ＩＰｖ６パケットをトンネリングする改善された方法、システム、及び製品が依然として必要とされている。

【課題を解決するための手段】

【０００５】

ＩＰｖ６パケットをトンネリングする方法、システム、及び製品を提供する。諸実施形態は、発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを発信元ＩＰｖ６ホストから受信するステップと、発信元ＩＰｖ６境界ルータがＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付けるデータ構造から検索された宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを、発信元ＩＰｖ６ホストから受信するステップと、前記発信元ＩＰｖ６境界ルータが前記ＩＰｖ６パケットをＩＰｖ４パケットにカプセル化するステップと、前記カプセル化パケットを前記ＩＰｖ４アドレス上の宛先ＩＰｖ６境界ルータに送信するステップと、を含む。多くの実施形態において、前記発信元ＩＰｖ６境界ルータが前記ＩＰｖ６パケットをＩＰｖ４パケットにカプセル化する前記ステップは、ＩＰｖ４ヘッダを前記ＩＰｖ６パケットに追加することによって実施される。

【０００６】

典型的な諸実施形態はまた、前記宛先ＩＰｖ６境界ルータが前記カプセル化パケットを非カプセル化するステップと、前記宛先ＩＰｖ６境界ルータが前記非カプセル化パケットを前記ＩＰｖ６宛先アドレスを有する宛先ホストに転送するステップと、を含む。多くの実施形態において、前記宛先ＩＰｖ６境界ルータが前記カプセル化パケットを非カプセル化する前記ステップは、前記発信元境界ルータによって追加されたＩＰｖ４ヘッダを前記カプセル化パケットから取り除くことによって実施される。

【０００７】

典型的な諸実施形態はまた、前記ＩＰｖ６ホストが前記パケットのＩＰｖ６宛先アドレスを識別するステップと、宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを、ＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付けるデータ構造から検索するステップと、前記ＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを前記発信元ＩＰ

ｖ６境界ルータに送信するステップと、前記ＩＰｖ６パケットに関連する宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを発信元ＩＰｖ６境界ルータに提供するステップと、を含む。多くの実施形態において、ＩＰｖ６宛先アドレスを宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスと関連付ける前記データ構造は、ＤＮＳリソース・レコードを含む。

【０００８】

ここで添付図面を参照しながら本発明の好ましい諸実施形態を単なる例示として説明する。

【発明を実施するための最良の形態】

【０００９】

本発明は、本明細書の大部分においてＩＰｖ６パケットをトンネリングする方法に関して説明される。しかしながら、当業者なら、本明細書に開示される方法に従って動作する適切なプログラミング手段を含むどのようなコンピュータ・システムであっても本発明の範囲に含まれることを理解するだろう。適切なプログラミング手段としては、例えばコンピュータ・メモリに連結された処理ユニット及び算術論理回路から構成され、処理ユニットによって実行されるようにプログラムされた本発明の各方法ステップを、データ及びプログラム命令を記憶するように構成された電子回路を含むコンピュータ・メモリに記憶することが可能なシステムを含めたコンピュータ・システムに、本発明の各方法ステップを実行するよう指示する任意の手段が挙げられる。

【００１０】

本発明は、任意の適切なデータ処理システムと共に使用されるディスケットや他の記録媒体のようなコンピュータ・プログラムの形で実施することもできる。コンピュータ・プログラムの諸実施形態は、磁気媒体、光媒体、又は他の適切な媒体を含めて、機械に読み込み可能な情報を記録する任意の記録媒体を使用することによって実行することができる。当業者なら、適切なプログラミング手段を有するどのようなコンピュータ・システムであってもプログラムの形で実施される本発明の各方法ステップを実行することができることを容易に理解するであろう。当業者なら、本明細書に記載される例示的な諸実施形態の大部分はコンピュータ・ハードウェア上にインストールされ実行されるソフトウェアを対象としているが、ファームウェアとして又はハードウェアとして実装される諸代替実施形態もまた本発明の諸実施形態の範囲に十分含まれることを容易に理解するだろう。

【００１１】

図１から始まる添付図面を参照して、ＩＰｖ６パケットをトンネリングする方法、システム、及び製品について説明する。図１は、本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングすることができる例示的なデータ処理システムを図示している。図１のシステムは、３つのネットワーク（１０１、１０２、及び１０３）内のデータ通信のために接続されるいくつかのコンピュータを含んでいる。

【００１２】

図１の実施例では、ＰＤＡ（１１２）、コンピュータ・ワークステーション（１０４）、携帯電話（１１０）、及びパーソナル・コンピュータ（１０８）を含めたいくつかの例示的なデバイスが、ＩＰｖ６ネットワーク（１０１）に接続されている。図１の実施例において、ネットワーク使用可能な携帯電話（１１０）は、無線接続（１１６）を介してＩＰｖ６ネットワーク（１０１）に接続されている。ワークステーション（１０４）は、有線接続（１２２）を介してＩＰｖ６ネットワーク（１０１）に接続されている。ＰＤＡ（１１２）は、無線接続（１１４）を介してＩＰｖ６ネットワーク（１０１）に接続されている。また、パーソナル・コンピュータ（１０８）は、有線接続（１２０）を介してＩＰｖ６ネットワーク（１０１）に接続されている。

【００１３】

図１の実施例は、別のＩＰｖ６ネットワーク（１０３）も含んでいる。ラップトップ（１２６）、ネットワーク使用可能な携帯電話（１３２）、及びパーソナル・コンピュータ（１０５）を含めたいくつかの例示的なデバイスは、ＩＰｖ６ネットワーク（１０３）に接続されている。図１の実施例において、ラップトップは、無線接続（１１８）を介して

ＩＰｖ６ネットワーク（１０３）に接続されている。携帯電話（１３２）は、無線接続（１３０）を介してＩＰｖ６ネットワーク（１０３）に接続されている。また、パーソナル・コンピュータ（１０５）は、有線接続（１２４）を介してＩＰｖ６ネットワーク（１０３）に接続されている。

【００１４】

図１の実施例において、各ＩＰｖ６ネットワーク（１０１及び１０３）は、本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングすることができる境界ルータ（１４２及び１３４）を有する。境界ルータ（１４２）は、有線接続（１４０）を介して１つのＩＰｖ６ネットワーク（１０１）に接続され、境界ルータ（１３４）は、有線接続（１１７）を介してもう１つのＩＰｖ６ネットワーク（１０３）に接続されている。例示的な各境界ルータは、ＩＰｖ６パケットを各々のＩＰｖ６ネットワーク内のデバイスから各々のＩＰｖ６ネットワーク外の他のデバイスにルーティングすることができる故にそう呼ばれている。したがって、これらのルータは各々のＩＰｖ６ネットワークの境界線上に所在する。

【００１５】

ＩＰｖ６パケットを１つのＩＰｖ６ネットワークから別のＩＰｖ６ネットワークにルーティングするために、図１の例示的な各境界ルータは、データ通信のためにＩＰｖ４ネットワーク（１０２）を介して相互に連結される。図１の実施例において、ＩＰｖ６パケットを１つのＩＰｖ６ネットワーク（１０１）から別のＩＰｖ６ネットワーク（１０３）に送信するために、ＩＰｖ６パケットは、１つの境界ルータ（１４２）からＩＰｖ４ネットワークを経由して別の境界ルータ（１３４）にトンネリング（１３８）される。

【００１６】

図１の実施例において、発信元ホスト（１０８、１１２、１０４、１１０）は、ＩＰｖ６パケットを発信元のＩＰｖ６ネットワーク（１０１）内の発信元ＩＰｖ６ホスト（１０８、１１２、１０４、１１０）から宛先ＩＰｖ６ネットワーク（１０３）内のＩＰｖ６宛先ホスト（１２６、１３２、１０５）に送信するために、パケットを受信するホストのＩＰｖ６宛先アドレスを識別する。図１のシステムにおいて、パケットに関するＩＰｖ６宛先アドレスの識別は、宛先ホストのドメイン・ネームを解決することによって実施される。宛先ホストのドメイン・ネームの解決は、ＤＮＳリソース・レコード及びＩＰアドレスをＤＮＳサーバ（１４３）から検索することによって実施される。

【００１７】

ドメイン・ネーム・システム（「ＤＮＳ」）は、典型的にはインターネットに関連するネーム・サービスである。ＤＮＳはドメイン・ネームをネットワーク・アドレスに翻訳する。ドメイン・ネームは、ネットワーク・サービスを提供するウェブ・サーバや電子メール・サーバ等のコンピュータ・ホストの名前である。図１の実施例において、ネットワーク・アドレスはＩＰｖ６アドレスである。ドメイン・ネームは典型的には、数字で表されるネットワーク・アドレスよりも人間にとって扱いやすいアルファベットで表されたテキストで表現される。一方、ネットワークは数字で表されたネットワーク・アドレスを取り扱う。したがって、ユーザがドメイン・ネームを使用してリソースを要求する度に、どこかにあるＤＮＳサービスがドメイン・ネームを対応するネットワーク・アドレスに翻訳する。例えば「ｉｂｍ．ｃｏｍ」というドメイン・ネームは、１２９．４２．１９．９９というＩＰネットワーク・アドレスに翻訳することができる。ドメイン・ネームの目的は、様々なホスト、ネットワーク、プロトコル・ファミリー、相互ネットワーク、及び管理組織で使用可能となるような名前をリソースに付ける仕組みを提供することである。ドメイン・ネームはユーザの視点から見ると、ドメイン・ネームに関連する情報を検索するリゾルバと呼ばれる関数に対する引数として役立つ。それによってユーザは特定のドメイン・ネームに関連するホスト・アドレス又はメール情報を要求することができる。ユーザが特定のタイプの情報を要求することが可能となるように、適切な照会タイプがドメイン・ネームを有するリゾルバに渡される。ドメイン・ツリーはユーザにとっての単一の情報空間であり、例えばリゾルバは、ネーム・サーバ間のデータ配信をユーザから隠蔽する責任を

負っている。

【００１８】

リゾルバは、クライアント要求に応じて情報をＤＮＳネーム・サーバから抽出するプログラムである。リゾルバは、少なくとも１つのネーム・サーバにアクセスし、当該ネーム・サーバの情報を使用して照会に直接回答すること、又は照会を他のネーム・サーバへの参照を使用して追跡することができなければならない。リゾルバは、典型的にはユーザ・プログラムから直接アクセス可能なシステム・ルーチンであり、そのため、リゾルバとユーザ・プログラムの間では通常プロトコルは必要とされない。ネーム・サーバとリゾルバはどちらも１つ又は複数のコンピュータ上で実行されるソフトウェア・プロセスである。リゾルバは本質的に、ドメイン・ネームに関する照会の処理依頼をネーム・サーバに対して行う。ネーム・サーバは、ドメイン・ネームと機械アドレスとのマッピングを「解決」し、機械アドレスを紹介に対する「回答」としてリゾルバに返送する。

【００１９】

多くのネットワーク・ホストにおいて、リゾルバはオペレーティング・システムの一部である。より具体的には、ＴＣＰ／ＩＰの場合には、リゾルバは、ソケットＡＰＩのようなアプリケーション・プログラミング・インターフェイス（「ＡＰＩ」）を介して、アプリケーション・レベルからＣ又はＣ＋＋コールを使用してアクセス可能なＴＣＰ／ＩＰクライアントの一部であることが多い。例えば、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）（Ｒ）Ｓｏｃｋｅｔｓ　ＡＰＩは、ホストのドメイン・ネームが入力として与えられた場合にそれぞれ同期的及び非同期的にネットワーク・ホストのネットワーク・アドレスを取得する働きをする、ｇｅｔｈｏｓｔｂｙｎａｍｅ（）及びＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＮａｍｅ（）と呼ばれる関数を提供する。同様に、Ｊａｖａ（登録商標）（Ｒ）メソッドであるＩｎｅｔＡｄｄｒｅｓｓ．ｇｅｔＢｙＮａｍｅ（ｓｔｒｉｎｇ　ｈｏｓｔ）は、ネットワーク・ホストのインターネット・プロトコル・アドレスを表すＩｎｅｔＡｄｄｒｅｓｓクラスのオブジェクトをインスタンス化する静的なＪａｖａ（登録商標）（Ｒ）メソッドである。

【００２０】

ＤＮＳは、標準的なメッセージ・タイプの要求／応答データ通信プロトコルを含んでいる。ｇｅｔｈｏｓｔｂｙｎａｍｅ（）及びＩｎｅｔＡｄｄｒｅｓｓ．ｇｅｔＢｙＮａｍｅ（）は、Ｕｎｉｘ（登録商標）（Ｒ）やＷｉｎｄｏｗｓ（登録商標）（Ｒ）のようなオペレーティング・システムにおけるＴＣＰ／ＩＰクライアントに対するＡＰＩコールの実施例である。そのようなＴＣＰ／ＩＰクライアントは、１つ又は複数の予め指定されたＤＮＳサーバ・アドレスと、あるコンピュータに関する１次ＤＮＳサーバの指定と、場合によっては１つ又は複数の２次ＤＮＳサーバの指定と、を保持している。ＴＣＰ／ＩＰクライアントは、ｇｅｔｈｏｓｔｂｙｎａｍｅ（）やＩｎｅｔＡｄｄｒｅｓｓ．ｇｅｔＢｙＮａｍｅ（）のようなリゾルバ関数のコールに応じて、標準的な形式のドメイン・ネームを含むＤＮＳ要求メッセージを予め指定された１次ＤＮＳサーバに送信し、それによって対応するネットワーク・アドレスを要求し、応答メッセージを受信したときはそれに応じてネットワーク・アドレスをコール中のプログラムに提供する。コール中のアプリケーションは、ネットワーク・アドレスをオペレーティング・システムから受け取ったときは、ネットワーク・アドレスを使用してネットワーク・アドレスに関連するドメイン・ネームで識別されたネットワーク・ホスト上のリソースにアクセスすることができる。ＤＮＳリソース・レコードは有利なことに、本発明の諸実施形態に従って、要求されたＩＰｖ６宛先アドレスだけでなく、パケットをＩＰｖ６宛先アドレスに配信することができる宛先境界ルータに関連するＩＰｖ４アドレスも含むように修正を施すことができる。すなわち、ＤＮＳリソース・レコードは、関連するＩＰｖ６宛先アドレス宛てのカプセル化ＩＰｖ６パケットを受信することができるＩＰｖ４アドレスも含むことになる。したがって、図１のシステムにおいて、ホスト（１０８、１１２、１０４、１１０）は、ＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを発信元ＩＰｖ６境界ルータに送信し、ＤＮＳリソース・レコード内で識別された関連する宛先境界ルータのＩＰｖ４アドレスも境界ルータに提供する

。いくつかの実施形態において、発信元ホストは、宛先境界ルータのＩＰｖ４アドレスをＩＰｖ６パケットの拡張ヘッダに埋め込む。図１のシステムにおいて、境界ルータ（１４２）は、ＩＰｖ６パケットをホストから受信し、宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを受信し、ＩＰｖ６パケットをＩＰｖ４パケットにカプセル化し、カプセル化パケットをＩＰｖ４アドレス上の宛先ＩＰｖ６境界ルータ（１３４）に送信することができる。図１の境界ルータ（１３４）は、カプセル化パケットを非カプセル化し、非カプセル化パケットをＩＰｖ６宛先アドレスを有する宛先ホスト（１２６、１３２、１０５）に転送することができる。

【００２１】

図１のアーキテクチャにおけるネットワーク接続の態様は単なる説明的なものであり、限定的なものではない。実際、本発明の諸実施形態によれば、コンピュータ・リソースを好ましいブラウザを介して表示するシステムを、ＬＡＮ、ＷＡＮ、イントラネット、相互ネットワーク、インターネット、ウェブ、ワールド・ワイド・ウェブ自体、又は当業者が想到する他の接続と接続することができる。そのようなネットワークは、全体的なデータ処理システムの範囲内で相互に接続されている様々なデバイスとコンピュータとの間のデータ通信接続を提供するのに使用することができる媒体である。

【００２２】

図１に示される例示的なシステムを構成するホスト、境界ルータ、及びデバイスの配置は例示的なものであり、限定的なものではない。本発明の様々な実施形態に従って利用されるデータ処理システムは、図１には示されていないが当業者が想到する追加的なサーバ、ルータ、他のデバイス、及びピア・ツー・ピア・アーキテクチャを含むことができる。そのようなデータ処理システムのネットワークは、例えばＴＣＰ／ＩＰ、ＨＴＴＰ、ＷＡＰ、ＨＤＴＰ、及び当業者が想到する他のプロトコルを含めた多くのデータ通信プロトコルをサポートすることができる。本発明の様々な実施形態は、図１に示されるものに加えて様々なハードウェア・プラットフォーム上で実行することができる。

【００２３】

上述したように、本発明の諸実施形態に係るＩＰｖ６パケットのトンネリングは一般に、コンピュータを用いてすなわち自動計算機を用いて実施される。更なる説明を行うために、図２には本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングする際に利用される境界ルータ（１３４）を有する自動計算機のブロック図が記載されている。図２の境界ルータ（１３４）は、少なくとも１つのコンピュータ・プロセッサ（１５６）すなわち「ＣＰＵ」並びにランダム・アクセス・メモリ（１６８）（「ＲＡＭ」）を含んでいる。ＲＡＭ（１６８）にはオペレーティング・システム（１５４）が記憶されている。本発明の諸実施形態に係る境界ルータ内で利用されるオペレーティング・システムとしては、Ｕｎｉｘ（登録商標）（Ｒ）、ＡＩＸ（Ｒ）、Ｌｉｎｕｘ（Ｒ）、ＭｉｃｒｏｓｏｆｔＮＴ（Ｒ）、及び当業者が想到する他の多くのオペレーティング・システムが挙げられる。図２の実施例のオペレーティング・システム（１５４）はＲＡＭ（１６８）内のものとして示されているが、オペレーティング・システムの多くのコンポーネントは典型的には不揮発性メモリ（１６６）にも記憶されている。

【００２４】

ＲＡＭ（１６８）には、本発明の諸実施形態に従ってパケットをトンネリングすることができるトンネル・ブローカ（１８８）も記憶されている。トンネル・ブローカ（１８８）は、ＩＰｖ６宛先アドレスを有するＩＰｖ６パケットを発信元ＩＰｖ６ホストから受信し、宛先ＩＰｖ６境界ルータのＩＰｖ４アドレスを発信元ＩＰｖ６ホストから受信し、ＩＰｖ６パケットをＩＰｖ４パケットにカプセル化し、カプセル化パケットをＩＰｖ４アドレス上の宛先ＩＰｖ６境界ルータに送信することができるソフトウェアである。図２に図示されるようなトンネル・ブローカは、典型的には境界ルータ上にインストールされ、有利なことには本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングする。

【００２５】

図２の境界ルータ（１３４）は、システム・バス（１６０）を介してプロセッサ（１５

６）及び境界ルータの他のコンポーネントと連結された不揮発性コンピュータ・メモリ（１６６）を含んでいる。不揮発性コンピュータ・メモリ（１６６）は、ハード・ディスク・ドライブ（１７０）、光ディスク・ドライブ（１７２）、電気的消去再書込可能読取り専用メモリ空間（いわゆる「ＥＥＰＲＯＭ」又は「フラッシュ」メモリ）（１７４）、ＲＡＭドライブ（図示せず）、又は当業者が想到する他の任意の種類のコンピュータ・メモリとして実装することができる。

【００２６】

図２の例示的な境界ルータ（１３４）は、サーバ、クライアント、及び当業者が想到する他のコンピュータを含む他のコンピュータ（１８２）とのネットワーク間接続を含めたデータ通信（１８４）接続を実施する、通信アダプタ（１６７）を含んでいる。通信アダプタは、ローカル・デバイス及びリモート・デバイス又はサーバが当該接続及びネットワークを介して互いにデータ通信の送信を行うハードウェア・レベルのデータ通信接続を実施する。本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングする際に利用される通信アダプタの例としては、有線ダイヤルアップ接続用のモデム、有線ＬＡＮ接続用のイーサネット（登録商標）（ＩＥＥＥ８０２．３）アダプタ、及び無線ＬＡＮ接続用の８０２．１１ｂアダプタが挙げられる。

【００２７】

図２の例示的な境界ルータは、１つ又は複数の入出力インターフェイス・アダプタ（１７８）を含んでいる。コンピュータ内の入出力インターフェイス・アダプタは、例えばコンピュータ表示画面のような表示デバイス（１８０）に対する出力と共にキーボードやマウスのようなユーザ入力デバイス（１８１）からのユーザ入力も制御するソフトウェア・ドライバ及びコンピュータ・ハードウェア等を介してユーザ指向の入出力を実施する。

【００２８】

更なる説明のために、図３にはＩＰｖ６パケットをトンネリングする例示的な方法を示すフローチャートが記載されている。図３の方法は、ＩＰｖ６ホスト（３０４）がパケットのＩＰｖ６宛先アドレス（３１０）を識別するステップ（３０６）を含む。図３の方法において、ＩＰｖ６ホスト（３０４）がパケットのＩＰｖ６宛先アドレス（３１０）を識別するステップ（３０６）は、典型的にはＤＮＳサービスを使用することによって宛先ホストのドメイン・ネームを解決するステップを含む。上述したように、ドメイン・ネーム・システム（「ＤＮＳ」）は、典型的にはドメイン・ネームをネットワーク・アドレスに翻訳する、インターネットに関連するネーム・サービスである。

【００２９】

図３の方法は、宛先ＩＰｖ６境界ルータ（３３２）のＩＰｖ４アドレス（３１２）をＤＮＳリソース・レコード（３０２）から検索するステップ（３０８）を含む。図３のＤＮＳリソース・レコード（３０２）は、ドメイン・ネームに関するＩＰｖ６宛先アドレスを含むだけでなく、ＩＰｖ６宛先アドレス宛てのカプセル化ＩＰｖ６パケットを受信することができ、パケットを非カプセル化し、非カプセル化パケットを宛先アドレスに転送することもできる境界ルータのＩＰｖ４アドレスも含んでいる。本発明の諸実施形態に従って修正されるＤＮＳリソース・レコードは有利なことに、ＩＰｖ６ネットワーク・アドレスと、ＩＰｖ６ネットワーク・アドレス上のホスト宛てのＩＰｖ６パケットを受信する好ましい境界ルータとの関連付けを行うビークル（ｖｅｈｉｃｌｅ）を提供する。

【００３０】

更なる説明のために、図４には本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングする際に利用される例示的なデータ構造が記載されている。図４の実施例は、本発明の諸実施形態に従って修正されるＤＮＳリソース・レコード（４５２）を含んでいる。図４のＤＮＳリソース・レコード（４５２）は、宛先ホストのドメイン・ネームを含むドメイン・ネーム・フィールド（４５４）を含んでいる。図４のＤＮＳリソース・レコード（４５２）は、宛先ホストのＩＰｖ６ネットワーク・アドレス（４５６）も含んでいる。図４のＤＮＳリソース・レコード（４５２）は、カプセル化ＩＰｖ６メッセージを非カプセル化し、非カプセル化メッセージを所期の宛先ＩＰｖ６ネットワーク・アドレスに転送

することができる境界ルータを識別する、ＩＰｖ４境界ルータ・アドレス（４５８）を更に含んでいる。例示的なＤＮＳリソース・レコード（４５２）はＩＰｖ４境界ルータ・アドレス（４５８）をレコード内のフィールドとして含んでいるが、諸代替実施形態では、ＩＰｖ４境界ルータ・アドレスを、ＩＰｖ４境界ルータ・アドレスを含むように設計された＞ＢＲ’タイプの別個のレコードに提供することもできる。図４の例示的なＤＮＳリソース・レコードは例示的なものであり、限定的なものではない。実際、ＩＰｖ６宛先アドレスと境界ルータのアドレスとは、当業者が想到する任意のデータ構造の形で関連付けることができる。さらに、図４のＤＮＳリソース・レコード（４５２）は、説明が明確になるように簡略化してある。本発明の諸実施形態に従って修正される典型的なＤＮＳリソース・レコードは、図４に提示されるフィールド以外にも、例えばレコードのタイプやレコードの存続時間データ等、当業者が想到する他の多くのフィールドを含むことになる。

【００３１】

再び図３を参照すると、図３の方法はまた、ＩＰｖ６宛先アドレス（３１０）を有するＩＰｖ６パケット（３１８）を発信元ＩＰｖ６境界ルータ（３２０）に送信するステップ（３１６）と、ＩＰｖ６パケットに関連する宛先ＩＰｖ６境界ルータ（３３２）のＩＰｖ４アドレス（３１２）を発信元ＩＰｖ６境界ルータ（３２０）に提供するステップ（３１４）と、を含む。ＩＰｖ６パケットに関連する宛先ＩＰｖ６境界ルータ（３３２）のＩＰｖ４アドレス（３１２）を発信元ＩＰｖ６境界ルータ（３２０）に提供するステップ（３１４）の１つの手法は、宛先境界ルータのＩＰｖ４アドレスをＩＰｖ６パケットの拡張ヘッダに埋め込むことによって実施される。ＩＰｖ６は、拡張ヘッダを提供することによって、追加的なルーティング・オプションを実装する実用的手段を提供する。拡張ヘッダは、トランスポート層ヘッダとＩＰｖ６ヘッダの間に置かれる。ＩＰｖ６ではいくつかのタイプの拡張ヘッダが定義されており、「ｎｅｘｔ　ｈｅａｄｅｒ」フィールドの値は、後続の別の拡張ヘッダを識別する。拡張ヘッダは、ルータがヘッダ・フィールドの読み出し中に当該ルータと関連をもつ可能性がある最後の値又は拡張ヘッダに到達したときは、その次のヘッダ・フィールドを読み出すのを止めることができるように配置される。拡張オプションは、パケットがそれ自体の宛先に届くまでに通過する各ルータによって、必ずしもすべて処理される必要はない。実際、多くのＩＰｖ６拡張ヘッダは、それぞれの宛先に到着するまで処理されない。ＩＰｖ６拡張ヘッダで使用される多くのオプションが既に定義されている。既に定義されている拡張ヘッダの実施例としては以下の４つが挙げられる。

【００３２】

（ルーティング拡張ヘッダ）ルーティング拡張ヘッダは、パケットのルーティングを制御するものである。ルーティング拡張ヘッダは、発信元から宛先までのルートを明示的に規定することができる。ルーティング拡張ヘッダには経路沿いの各ノードのＩＰｖ６アドレスが含められ、宛先は後に逆の経路も通信のために使用する。

【００３３】

（フラグメンテーション・ヘッダ）フラグメンテーション・ヘッダは、断片化したパケットがＩＰｖ６ネットワークをどのように通過するかを定義するものである。

【００３４】

（認証ヘッダ）認証ヘッダは、認証アルゴリズムを使用してＩＰｖ６パケットがそれ自体の経路上で改変されていないことを保証するものである。ヘッダは、ＩＰｖ６パケットがＩＰヘッダのリスト内にある発信元から到着したものであることも保証する。

【００３５】

（ホップ・バイ・ホップ・ヘッダ）ＩＰｖ６は、特別な処理が必要なパケットであることをルータに警告する効率的な方法を実施する。ＩＰｖ６のホップ・バイ・ホップ拡張ヘッダを含んでいないパケットは、各ルータが完全に処理するのではなくそれぞれの宛先に迅速に届くようにすることができる。ホップ・バイ・ホップ拡張ヘッダを用いると、ルータは特別なルート処理が必要なパケットを迅速に識別し、それを完全に処理することが可能となる。本ヘッダを認識したルータは、それに応じてパケットを検査し、本オプション

を認識しないルータは、パケットを無視する。

【００３６】

宛先境界ルータのＩＰｖ４アドレスをＩＰｖ６パケットの拡張ヘッダに埋め込むことによって関連する宛先ＩＰｖ６境界ルータ（３３２）のＩＰｖ４アドレス（３１２）を発信元ＩＰｖ６境界ルータ（３２０）に提供するステップ（３１４）は、ＩＰｖ６パケットに関する宛先境界ルータのＩＰｖ４アドレスを含む、本発明の諸実施形態に係る新しい拡張ヘッダを使用することによって実施することができる。有利なことに、宛先境界ルータのＩＰｖ４アドレスをパケット自体に提供することによって、発信元境界ルータを他の境界ルータのアドレスを用いて手動で構成する必要がなくなる。その代わりに、発信元境界ルータには、ＩＰｖ６パケットを宛先境界ルータにパケット単位（ｐａｃｋｅｔ－ｂｙ－ｐａｃｋｅｔ　ｂａｓｉｓ）でトンネリングするのに必要なルーティング情報が提供される。

【００３７】

図３の方法はまた、発信元ＩＰｖ６境界ルータ（３２０）がＩＰｖ６宛先アドレス（３１０）を有するＩＰｖ６パケット（３１８）を発信元ＩＰｖ６ホスト（３０４）から受信するステップ（３２２）と、発信元ＩＰｖ６境界ルータ（３２０）が宛先ＩＰｖ６境界ルータ（３３２）のＩＰｖ４アドレス（３１２）を発信元ＩＰｖ６ホスト（３０４）から受信するステップ（３２４）と、を含む。図３の方法において、宛先ＩＰｖ６境界ルータ（３３２）のＩＰｖ４アドレス（３１２）は、ＩＰｖ６パケット自体の拡張ヘッダに埋め込まれた形で受信される。

【００３８】

図３の方法は、発信元ＩＰｖ６境界ルータ（３２０）がＩＰｖ６パケット（３１８）をＩＰｖ４パケット（３２８）にカプセル化するステップ（３２６）も含む。図３の方法において、発信元ＩＰｖ６境界ルータ（３２０）がＩＰｖ６パケット（３１８）をＩＰｖ４パケット（３２８）にカプセル化するステップ（３２６）は、ＩＰｖ４ヘッダをＩＰｖ６パケットに追加することによって実施される。ＩＰｖ４ヘッダをＩＰｖ６パケットに追加することにより、発信元境界ルータは、埋め込みパケット（ｅｍｂｅｄｄｅｄ　ｐａｃｋｅｔ）をＩＰｖ４ネットワークを介して送信することが可能となる。更なる説明のために、図５には本発明の諸実施形態に係る埋め込みパケットを示すブロック図が記載されている。図５の実施例において、ＩＰｖ６ヘッダ（４０４）と、その後に続く、カプセル化パケットを送信すべきＩＰｖ４アドレスを発信元境界ルータに対して識別する拡張ヘッダ（４０６）と、宛先ホストに送信すべきデータ（４０８）と、を含むＩＰｖ６パケット（４０２）は、ＩＰｖ４パケット（４１０）にカプセル化される。図５の実施例において、カプセル化ＩＰｖ４パケット（４１０）は、ＩＰｖ６ヘッダ（４０４）に追加されるＩＰｖ４ヘッダ（４１１）と、拡張ヘッダ（４０６）と、データ（４０８）と、を有する。追加的なＩＰｖ４ヘッダを有するカプセル化ＩＰｖ４パケット（４１０）は、ＩＰｖ４ネットワークを介して送信することができる。

【００３９】

再び図３を参照すると、図３の方法は、カプセル化パケット（３２８）をＩＰｖ４アドレス（３１２）上の宛先ＩＰｖ６境界ルータ（３３２）に送信するステップ（３３０）も含む。図３の実施例では、カプセル化パケットは、発信元ホストによって識別されたＩＰｖ４アドレスに送信され、ＩＰｖ４パケットにカプセル化されたＩＰｖ６パケット内の拡張ヘッダに埋め込まれる。

【００４０】

図３の方法はまた、宛先ＩＰｖ６境界ルータ（３３２）がカプセル化パケット（３２８）を非カプセル化するステップ（３３４）と、宛先ＩＰｖ６境界ルータ（３３２）が非カプセル化パケット（３３６）をＩＰｖ６宛先アドレスを有する宛先ホスト（３４０）に転送するステップ（３３８）と、を含む。図３の方法において、宛先ＩＰｖ６境界ルータ（３３２）がカプセル化パケット（３２８）を非カプセル化するステップ（３３４）は、発信元境界ルータ（３２０）によって追加されたＩＰｖ４ヘッダをカプセル化パケットから

取り除くことによって実施される。

【図面の簡単な説明】

【００４１】

【図１】本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングすることができる例示的なデータ処理システムを示す図である。

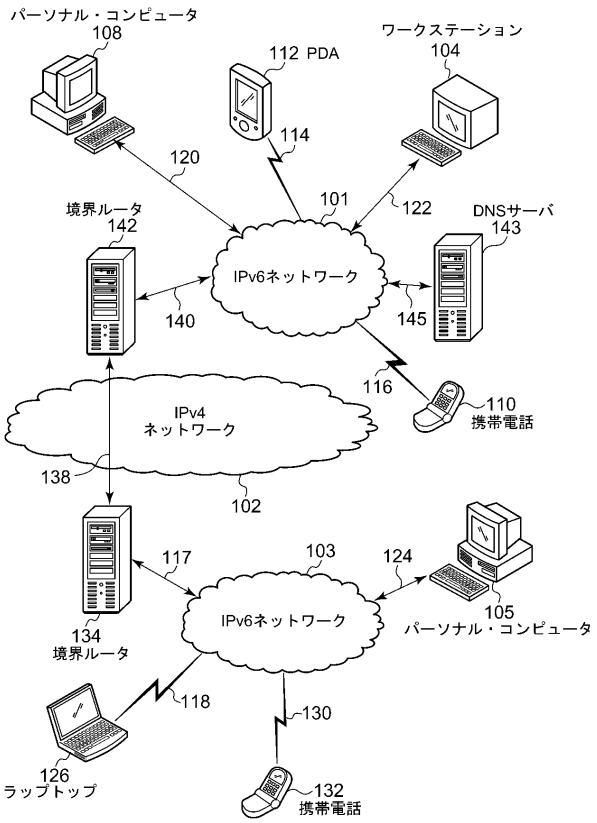
【図２】本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングする際に利用される境界ルータのブロック図である。

【図３】ＩＰｖ６パケットをトンネリングする例示的な方法を示すフローチャートである。

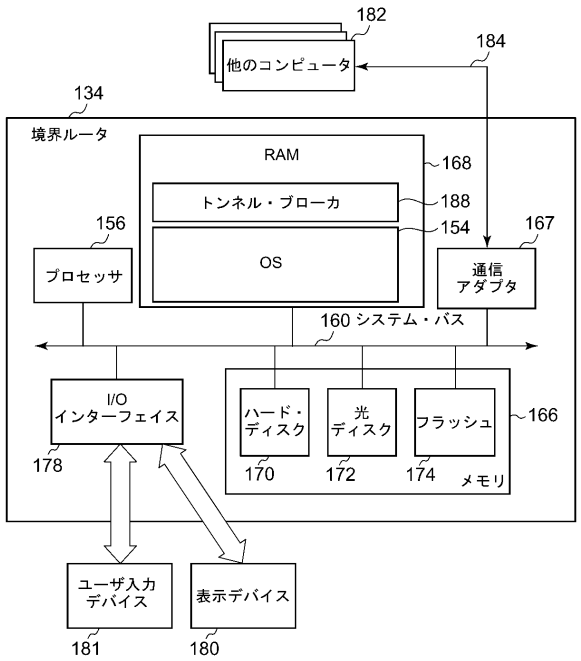
【図４】本発明の諸実施形態に従ってＩＰｖ６パケットをトンネリングする際に利用されるデータ構造のブロック図である。

【図５】本発明の諸実施形態に係る埋め込みパケットを詳細に示すブロック図である。

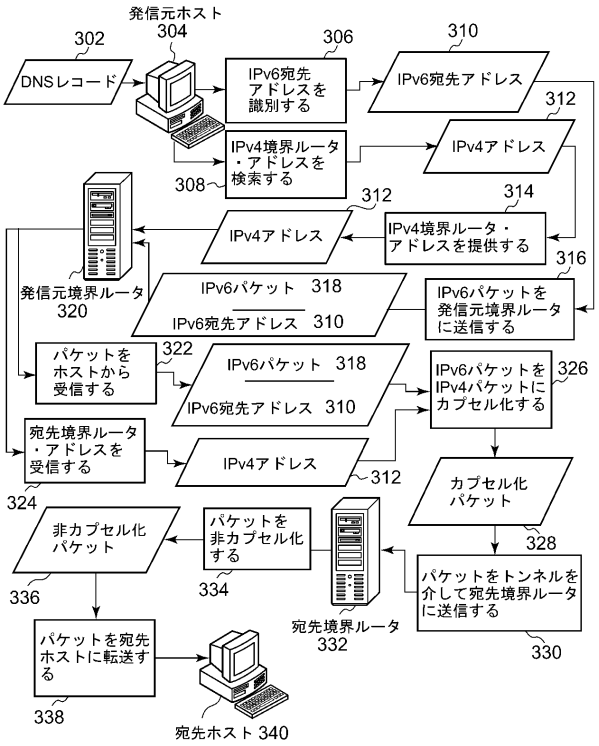
【図１】



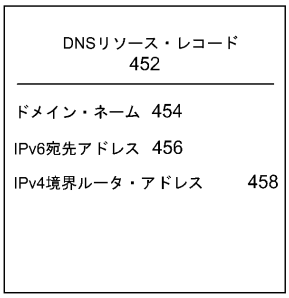
【図２】



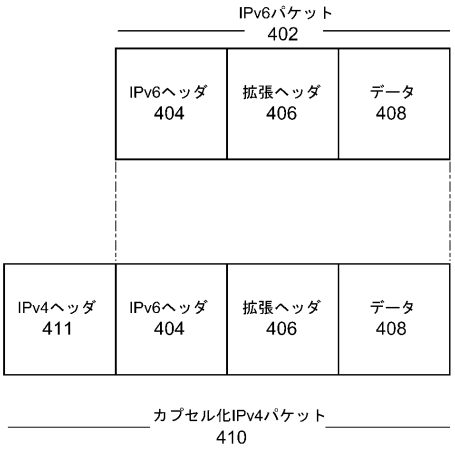
【図３】


発信元ホスト
304
302
DNSレコード
306
IPv6宛先アドレスを識別する
310
IPv6宛先アドレス
312
IPv4アドレス
IPv4境界ルータ・アドレスを検索する
308
314
IPv4境界ルータ・アドレスを提供する
312
IPv4アドレス
発信元境界ルータ
320
316
IPv6パケット 318
IPv6宛先アドレス 310
IPv6パケットを発信元境界ルータに送信する
322
パケットをホストから受信する
IPv6パケット 318
IPv6宛先アドレス 310
326
IPv6パケットをIPv4パケットにカプセル化する
宛先境界ルータ・アドレスを受信する
IPv4アドレス
312
カプセル化パケット
324
328
非カプセル化パケット
パケットを非カプセル化する
パケットをトンネルを介して宛先境界ルータに送信する
336
334
宛先境界ルータ
332
330
パケットを宛先ホストに転送する
338
宛先ホスト 340

【図４】


DNSリソース・レコード
452
ドメイン・ネーム 454
IPv6宛先アドレス 456
IPv4境界ルータ・アドレス 458

【図５】


IPv6パケット
402
IPv6ヘッダ
404
拡張ヘッダ
406
データ
408
IPv4ヘッダ
411
IPv6ヘッダ
404
拡張ヘッダ
406
データ
408
カプセル化IPv4パケット
410

フロントページの続き

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 フェルナンデス、リリアン、シルヴィア
アメリカ合衆国７８７２８ テキサス州オースティン ウェルズ・ブランチ・パークウェイ３１０１ ＃１２２８
(72)発明者 ジャイン、ヴィニット
アメリカ合衆国７８７１７ テキサス州オースティン ラスティック・レーン１６００７
(72)発明者 バラバンネーニ、ヴァス
アメリカ合衆国７８７５０ テキサス州オースティン トップリッジ・ドライヴ９１０３
(72)発明者 ヴォー、パトリック、タム
アメリカ合衆国７７０９９ テキサス州ヒューストン プラム・ポイント・ロード１２０７５

審査官 大石 博見

(56)参考文献 国際公開第０１／０２２６８３（WO，Ａ１）
米国特許出願公開第２００４／０１７９５３６（ＵＳ，Ａ１）
特開２００４－２６６８２２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/46