(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4269343号
(P4269343)
(45)発行日　平成21年5月27日(2009.5.27)　(24)登録日　平成21年3月6日(2009.3.6)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　B

請求項の数 17　(全 39 頁)

(21)出願番号　特願2007-30119(P2007-30119)
(22)出願日　平成19年2月9日(2007.2.9)
(62)分割の表示　特願2005-180014(P2005-180014)の分割
原出願日　平成15年2月28日(2003.2.28)
(65)公開番号　特開2007-166659(P2007-166659A)
(43)公開日　平成19年6月28日(2007.6.28)
審査請求日　平成19年2月9日(2007.2.9)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100093595
弁理士　松本　正夫
(72)発明者　藤田　範人
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　石川　雄一
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　岩田　淳
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】名前解決サーバおよびパケット転送装置

(57)【特許請求の範囲】
【請求項１】
受信したパケットを他のノードに転送する機能を備えるパケット転送装置と、
受信した名前解決要求メッセージに対して名前解決を行い、名前解決応答メッセージによって前記名前解決の結果を返す名前解決サーバと
を備える名前解決システムであって、
クライアントから前記名前解決サーバへ送信された名前解決要求メッセージは、前記パケット転送装置によって一旦受信され、
前記名前解決要求メッセージを一旦受信し、前記名前解決要求メッセージの送信者に関する属性情報を取得し、前記属性情報を付加した前記名前解決要求メッセージを前記名前解決サーバへ送信するDNSプロキシ部とを有し、
前記名前解決サーバは、前記パケット転送装置によって送信された前記名前解決要求に含まれる前記属性情報に基づいて、前記名前解決の結果である名前解決応答メッセージを返す、ことを特徴とする名前解決システム。
【請求項２】
前記パケット転送装置は、
前記属性情報が格納されたユーザ情報データベースを内部要素として備え、
前記名前解決要求メッセージの送信者であるユーザに関する属性情報を、前記ユーザ情報データベースから取得することを特徴とする請求項１に記載の名前解決システム。
【請求項３】

前記パケット転送装置は、前記属性情報が格納されたユーザ情報データベースを備える外部のデータベースサーバから、前記属性情報を取得することを特徴とする請求項１に記載の名前解決システム。

【請求項４】

前記パケット転送装置は、前記外部のデータベースサーバからの前記属性情報の取得において、名前解決要求メッセージを用いることを特徴とする請求項３に記載の名前解決システム。

【請求項５】

前記外部のデータベースサーバが、外部に設置された名前解決サーバであることを特徴とする請求項３又は請求項４に記載の名前解決システム。

【請求項６】

前記パケット転送装置は、さらに

自ノードに接続するクライアントにおけるユーザを識別、認証するユーザ認証部と、

認証時に得られた前記ユーザに関する属性情報に基づいて、前記ユーザ情報データベースの内容を更新するユーザ情報更新部とを備えたことを特徴とする請求項１から請求項５のいずれか１項に記載の名前解決システム。

【請求項７】

前記パケット転送装置は、前記名前解決要求メッセージに含まれる送信元アドレスに基づいて前記名前解決要求メッセージの送信者に関する属性情報を取得することを特徴とする請求項１から請求項６のいずれか１項に記載の名前解決システム。

【請求項８】

クライアントが送信した名前解決要求メッセージに対して、名前解決サーバが名前解決を行い、名前解決応答メッセージによって前記名前解決の結果を返す名前解決方法であって、

前記クライアントから前記名前解決サーバへ送信された名前解決要求メッセージを、前記クライアントと前記名前解決サーバとの間に存在する、受信したパケットを他のノードに転送する機能を備えるパケット転送装置が一旦受信し、

前記パケット転送装置により、前記名前解決要求メッセージの送信者であるユーザに関する属性情報が、前記名前解決要求メッセージに含まれる送信元アドレスに基づいて取得され、前記属性情報を前記名前解決要求メッセージに付加された後に前記名前解決要求メッセージを前記名前解決サーバへ送信され、

前記名前解決サーバは、前記パケット転送装置によって送信された前記名前解決要求に含まれる前記属性情報に基づいて、前記名前解決の結果である名前解決応答メッセージを返す、ことを特徴とする名前解決方法。

【請求項９】

受信したパケットを他のノードに転送するパケット転送装置であって、

クライアントから名前解決サーバへ送信された名前解決要求メッセージの送信者に関する属性情報を取得するユーザ情報取得部と、

前記名前解決要求メッセージを一旦受信し、前記名前解決要求メッセージの送信者に関する属性情報を前記ユーザ情報取得部を介して取得し、前記属性情報を付加した前記名前解決要求メッセージを前記名前解決サーバへ送信するDNSプロキシ部とを有することを特徴とするパケット転送装置。

【請求項１０】

さらに、前記属性情報が格納されたユーザ情報データベースを内部要素として備え、

前記名前解決要求メッセージの送信者であるユーザに関する属性情報を、前記ユーザ情報データベースから前記ユーザ情報取得部を介して取得することを特徴とする請求項９に記載のパケット転送装置。

【請求項１１】

さらに、前記属性情報が格納されたユーザ情報データベースを備える外部のデータベースサーバから、前記ユーザ情報取得部を介して前記属性情報を取得することを特徴とする

請求項９に記載のパケット転送装置。
【請求項１２】
さらに、前記外部のデータベースサーバからの前記属性情報の取得において、名前解決要求メッセージを用いることを特徴とする請求項１１に記載のパケット転送装置。
【請求項１３】
前記外部のデータベースサーバが、外部に設置された名前解決サーバであることを特徴とする請求項１１又は請求項１２に記載のパケット転送装置。
【請求項１４】
さらに自ノードに接続するクライアントにおけるユーザを識別、認証するユーザ認証部と、
認証時に得られた前記ユーザに関する属性情報に基づいて、前記ユーザ情報データベースの内容を更新するユーザ情報更新部とを有することを特徴とする請求項９から請求項１３のいずれか１項に記載のパケット転送装置。
【請求項１５】
前記情報取得部は、前記名前解決要求メッセージに含まれる送信元アドレスに基づいて前記名前解決要求メッセージの送信者に関する属性情報を取得することを特徴とする請求項９～１４のいずれかに記載のパケット転送装置。
【請求項１６】
受信したパケットを他のノードに転送するパケット転送装置におけるパケット転送方法であって、
クライアントから名前解決サーバへ送信された名前解決要求メッセージを一旦受信し、前記名前解決要求メッセージの送信者に関する属性情報を取得し、前記属性情報を付加した前記名前解決要求メッセージを前記名前解決サーバへ送信する、ことを特徴とするパケット転送方法。
【請求項１７】
受信したパケットを他のノードに転送するパケット転送装置を、
クライアントから名前解決サーバへ送信された名前解決要求メッセージの送信者に関する属性情報を取得するユーザ情報取得部と、
前記名前解決要求メッセージを一旦受信し、前記名前解決要求メッセージの送信者に関する属性情報を前記ユーザ情報取得部を介して取得し、前記属性情報を付加した前記名前解決要求メッセージを前記名前解決サーバへ送信するDNSプロキシ部として機能させること特徴とするパケット転送プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、名前解決サーバおよびパケット転送装置に関し、特に名前解決要求メッセージの送信者の属性情報に基づいて名前解決応答をカスタマイズできる名前解決サーバおよびパケット転送装置に関する。
【背景技術】
【０００２】
従来この種の名前解決サーバとしてＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）サーバが知られている。このＤＮＳサーバは、例えばＲＦＣ１０３４に示されるように、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）網において、主にＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）からＩＰアドレスまたはＩＰアドレスからＦＱＤＮへの名前解決を行うために用いられている。名前解決を要求するクライアントは、ＤＮＳサーバに対して名前解決要求メッセージであるＤＮＳクエリメッセージを送信することで名前解決の要求を行い、ＤＮＳサーバから名前解決応答としてＤＮＳ応答メッセージを受信する。
【０００３】
一般的なＤＮＳサーバは、同一の名前（ＦＱＤＮやＩＰアドレスなど）について問い合

わされた場合は、常に同一の解決結果（ＩＰアドレスやＦＱＤＮなど）を返すことを基本としている。しかし、近年、同一の名前について問い合わされても、状況に応じて異なる名前解決結果を返すという付加機能を備えたＤＮＳサーバを用いるケースも増えている。以下、前記の付加機能の具体例を挙げる。

【０００４】

まず挙げられるのが、ＤＮＳのサーバソフトウェアとして広く普及しているＢＩＮＤ（Ｂｅｒｋｅｌｅｙ Ｉｎｔｅｒｎｅｔ Ｎａｍｅ Ｄｏｍａｉｎ）の、Ｖｉｅｗと呼ばれる機能である。Ｖｉｅｗを用いることにより、ＤＮＳサーバは同一の名前について問い合わされたとしても、ＤＮＳクエリメッセージのソースＩＰアドレスまたはＤＮＳクエリメッセージにより問い合わせたＦＱＤＮもしくはＩＰアドレスによって、クライアントに返す解決結果を変えることができる。

【０００５】

例えば、ＤＮＳクエリメッセージのソースＩＰアドレスがプライベートアドレスである場合には、ＦＱＤＮ：ｗｗｗ．ａａａ．ｃｏｍについての問い合わせに対してイントラネットに設置されたウェブサーバのＩＰアドレスを返し、逆に、ＤＮＳクエリメッセージのソースＩＰアドレスがグローバルＩＰアドレスである場合には、ＦＱＤＮ：ｗｗｗ．ａａａ．ｃｏｍについての問い合わせに対してエクストラネットに設置されたウェブサーバのＩＰアドレスを返す、といったことができる。

【０００６】

また、ＣＤＮ（Ｃｏｎｔｅｎｔ Ｄｅｌｉｖｅｒｙ Ｎｅｔｗｏｒｋ）において、コンテンツ配信サーバの負荷分散やユーザパフォーマンスの向上のために、ＤＮＳサーバの前記付加機能が利用される場合がある。ＣＤＮでは、サーバ間負荷分散及びユーザパフォーマンス向上を目的として、一つのコンテンツを複数のサーバに配置しておき、各ユーザからのリクエストを適切なサーバに振り分けることが一般的に行われている。ここで、ＤＮＳサーバはユーザのリクエストを送信するサーバを選択する際に利用される。

【０００７】

ＤＮＳサーバにおいて、一つのＦＱＤＮに対して同一のコンテンツを持つ複数のコンテンツ配信サーバのＩＰアドレスを登録しておき、クライアントがかかるＦＱＤＮに対して問い合わせを行った場合、ＤＮＳサーバは、サーバ負荷及びユーザパフォーマンスの観点から最適なコンテンツ配信サーバのＩＰアドレスをクライアントに返す。ここで、クライアントに関する情報として、一般的にクライアントまたはローカルＤＮＳサーバ（クライアントからのＤＮＳクエリメッセージを受信し、名前解決処理を引き受けるＤＮＳサーバ）が送信したＤＮＳクエリメッセージのソースＩＰアドレスが用いられる。

【０００８】

さらに、特開２００１－２７３２２５号公報（以下、特許文献１）では、ＤＮＳサーバがコンテンツ配信サーバの負荷状況及び位置情報の他、クライアントに関する情報として、ＤＮＳクエリメッセージのソースＩＰアドレスだけではなく、クライアントの位置情報（緯度・軽度など）も取得し、クライアントからのＤＮＳクエリに対して、これらの情報に基づいてクライアントとって最適なサーバを選択し、そのサーバのＩＰアドレスを返すという方法が示されている。

【０００９】

ＤＮＳサーバがクライアントの位置情報を取得できるようにするために、クライアントのリゾルバは、該クライアントの位置情報をＤＮＳクエリメッセージに埋め込み、ＤＮＳサーバに送信する。ＤＮＳサーバは位置情報が含められたＤＮＳクエリメッセージを受信することにより、該クライアントの位置情報を取得することができる。

【００１０】

【特許文献１】特開２００１－２７３２２５号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

従来技術の第１の問題点は、ＤＮＳサーバが、ＤＮＳクエリメッセージを送信したユーザの多様な属性情報に基づいて名前解決をカスタマイズできないことである。また、仮にカスタマイズできたとしても、ＤＮＳクエリメッセージ内に該クエリメッセージを送信したユーザの多様な属性情報を埋めこまなくてはならないため、クライアントまたはＤＮＳクエリを行うノード上のリゾルバの変更が必要となる。

【００１２】

ところで、名前解決を要求する個々のユーザは、位置や嗜好、利用端末やネットワークへの接続状況などの非常に多様な属性を持ち、また、これらの属性はユーザ毎に異なる。名前解決のカスタマイズとは、このようにユーザ毎に異なる属性を考慮して、応答する名前解決結果を名前解決を要求したユーザの属性に応じて変えることである。名前解決のカスタマイズの例としては、動画配信を行っているサーバのＦＱＤＮに対応するＩＰアドレスの解決を行う際に、同一のＦＱＤＮに対するＤＮＳクエリであっても、例えば接続回線種別がＡＤＳＬ回線のユーザには広帯域で配信を行っているサーバのＩＰアドレスを解決したり、逆に接続回線種別がＩＳＤＮ回線のユーザには狭帯域で配信を行っているサーバのＩＰアドレスを解決したりするといったことが挙げられる。さらに、ユーザの位置や嗜好、利用端末等、より多くのユーザ属性情報を考慮して名前解決を行うことにより、名前解決のカスタマイズを行うことができる。

【００１３】

しかし、従来のＤＮＳサーバは、ＤＮＳクエリメッセージ内に埋めこまれたデータに基づいてしか名前解決をカスタマイズできない。一般的なＤＮＳにおいて、ユーザに関する情報としてＤＮＳクエリメッセージに含まれるのは、多くともＤＮＳクエリメッセージのソースＩＰアドレスのみである。このため、一般的なＤＮＳサーバはユーザに関して、ＤＮＳクエリメッセージのソースＩＰアドレス以外の情報を取得することができない。前述したＢＩＮＤのＶｉｅｗ機能においても、ＤＮＳサーバが名前解決の際に考慮できるのは、ＤＮＳクエリメッセージのソースＩＰアドレスのみである。

【００１４】

また、従来の技術において、ＤＮＳクエリメッセージのソースＩＰアドレス以外の情報も用いて名前解決のカスタマイズを行おうとする場合、ＤＮＳクエリメッセージ内に必要な情報を全て埋めこむ必要があった。

【００１５】

特許文献１では、ＤＮＳサーバにおいてユーザの位置情報に基づいた名前解決を行うために、クライアントが送信するＤＮＳクエリメッセージ内にユーザの位置情報を埋めこむ方式が記載されている。しかしながら、この方式は２つの点において問題がある。まず第１の点は、名前解決のカスタマイズを行うために必要な情報をＤＮＳクエリメッセージ内に埋めこむためには、ユーザが利用するＯＳやアプリケーションソフトウェア等のユーザ環境を変更しなければならない。

【００１６】

昨今普及しているリゾルバには、ユーザ属性情報を把握しそれをＤＮＳクエリメッセージに埋め込むという機能が無いためリゾルバを変更する必要があるが、ＤＮＳサーバを利用する全てのユーザのリゾルバを変更することは大きなコストが必要である。

【００１７】

さらに、第２の点は、リゾルバを変更しＤＮＳクエリメッセージ内にユーザ属性情報を埋めこむとしても、埋めこまれるユーザ属性情報の種類は固定的であるため、ＤＮＳサーバが必要とするユーザ属性情報が各々のＤＮＳサーバによって異なる場合は対応できない。以上より、従来の技術によって、ＤＮＳサーバが名前解決をカスタマイズするために必要なユーザ属性情報を得ることは困難である。

【００１８】

従来技術の第２の問題点は、ＤＮＳサーバからクライアントに対して応答されるＤＮＳ応答メッセージに含まれる情報（ＦＱＤＮに対するＩＰアドレスなど）を、ＤＮＳサーバとクライアント間の経路上に設置されているパケット転送装置が利用することができない

ことである。

【００１９】

例えば、クライアントがあるＷｅｂサイトに接続することを考える。クライアントは該Ｗｅｂサイトに接続するために、まず該ＷｅｂサイトのＦＱＤＮに対するＩＰアドレスをＤＮＳによって解決し、解決の結果得られたＩＰアドレスに対して接続を行う。ＤＮＳサーバは、クライアントとＷｅｂサイトの接続に関する制御において、該ＷｅｂサイトのＩＰアドレスをクライアントに教えるという、すなわち接続先の制御しか行わない。

【００２０】

クライアントとＷｅｂサイトの接続に関する制御には、他にも、該接続上を通過するパケットをどのように転送するか（ヘッダ書換え、出方路制御、優先転送制御、など）といったパケット転送方法の制御があるが、これらのパケット転送方法の制御は、クライアントによってではなく、クライアントとＷｅｂサイト間の通過経路上に設置されているパケット転送装置上に静的にまたはルーティングプロトコル等で動的に設定されることによりなされるため、ＤＮＳサーバではこれらのパケット転送方法の制御を行うことはできない。

【００２１】

ここでパケット転送装置とは、イーサネット(登録商標)スイッチ、ＡＴＭ（Ａｓｙｎｃｈｒｏｎｏｕｓ　Ｔｒａｎｓｆｅｒ　Ｍｏｄｅ）スイッチ、ルータ、レイヤ４スイッチ、レイヤ７スイッチなど、パケットの転送処理を行う装置全般を指す。

【００２２】

もしクライアントにおける接続先の制御とパケット転送装置における転送方法の制御の両方を、ＤＮＳサーバによって同時に行うことができるようになれば、２つの制御が連携する効果があるといえる。例えば、先のクライアントとＷｅｂサイトとの間の接続において、クライアントの接続先を最も負荷の低いＷｅｂサーバとし、途中のパケット転送装置における該クライアントと該Ｗｅｂサーバとの接続上を通過するパケットに対して優先転送する制御を、ＤＮＳサーバによって同時に行えば、クライアントとＷｅｂサイト間のアクセスの高速化を効果的に実現することが可能となる。

【００２３】

しかしながら、現状において、クライアントにおける接続先の制御とパケット転送装置における転送方法の制御は分離されている。パケット転送装置の立場からは、ＤＮＳサーバがクライアントに対して送信するＤＮＳ応答メッセージに含まれる情報を利用することができず、また、ＤＮＳサーバの立場からは、クライアントに対して送信するＤＮＳ応答メッセージによってパケット転送装置における転送方法を制御することができない。

【００２４】

本発明の第１の目的は、現在のユーザ環境（ユーザが利用する端末やＯＳ、アプリケーションソフトウェアなど）に変更を強いることなく、名前解決サーバが名前解決をカスタマイズするために必要なユーザ属性情報を取得し、取得したユーザ属性情報に基づききめ細かに名前解決をカスタマイズできる名前解決サーバを提供することである。

【００２５】

本発明の第２の目的は、現在のユーザ環境（ユーザが利用する端末やＯＳ、アプリケーションソフトウェアなど）に変更を強いることなく、名前解決サーバが名前解決をカスタマイズするために必要なユーザ属性情報を動的に取得し、取得したユーザ属性情報に基づききめ細かに名前解決をカスタマイズできるだけではなく、該ユーザ属性情報を動的に取得し、管理する機能を有する名前解決サーバを提供することである。

【００２６】

本発明の第３の目的は、クライアントにおける接続先とパケット転送装置におけるパケット転送方法の両者を制御することができる名前解決サーバを提供することである。

【００２７】

本発明の第４の目的は、クライアントと名前解決サーバとの間でやり取りされる名前解決メッセージによって、パケット転送方法の制御がなされることができるパケット転送装

置を提供することである。
【課題を解決するための手段】
【００２８】
請求項１の本発明は、受信したパケットを他のノードに転送する機能を備えるパケット転送装置と、受信した名前解決要求メッセージに対して名前解決を行い、名前解決応答メッセージによって前記名前解決の結果を返す名前解決サーバとを備える名前解決システムであって、クライアントから前記名前解決サーバへ送信された名前解決要求メッセージは、前記パケット転送装置によって一旦受信され、前記パケット転送装置により、前記名前解決要求メッセージの送信者であるユーザに関する属性情報が、前記名前解決要求メッセージに含まれる送信元アドレスに基づいて取得され、前記属性情報を前記名前解決要求メッセージに付加された後に前記名前解決要求メッセージを前記名前解決サーバへ送信され、前記名前解決サーバは、前記パケット転送装置によって送信された前記名前解決要求に含まれる前記属性情報に基づいて、前記名前解決の結果である名前解決応答メッセージを返し、前記名前解決応答メッセージは、前記パケット転送装置を介して前記クライアントへ返されることを特徴とする。
【００２９】
請求項２の本発明の名前解決システムは、前記パケット転送装置は、前記属性情報が格納されたユーザ情報データベースを内部要素として備え、前記名前解決要求メッセージの送信者であるユーザに関する属性情報を、前記ユーザ情報データベースから取得することを特徴とする。
【００３０】
請求項３の本発明の名前解決システムは、前記パケット転送装置は、前記属性情報が格納されたユーザ情報データベースを備える外部のデータベースサーバから、前記属性情報を取得することを特徴とする。
【００３１】
請求項４の本発明の名前解決システムは、前記パケット転送装置は、前記外部のデータベースサーバからの前記属性情報の取得において、名前解決要求メッセージを用いることを特徴とする。
【００３２】
請求項５の本発明の名前解決システムは、前記外部のデータベースサーバが、外部に設置された名前解決サーバであることを特徴とする。
【００３３】
請求項６の本発明の名前解決システムは、前記パケット転送装置は、自ノードに接続するクライアントにおけるユーザを識別、認証するユーザ認証部と、認証時に得られた前記ユーザに関する属性情報に基づいて、前記ユーザ情報データベースの内容を更新するユーザ情報更新部とを備えたことを特徴とする。
【００３４】
請求項７の本発明は、クライアントが送信した名前解決要求メッセージに対して、名前解決サーバが名前解決を行い、名前解決応答メッセージによって前記名前解決の結果を返す名前解決方法であって、前記クライアントから前記名前解決サーバへ送信された名前解決要求メッセージは、前記クライアントと前記名前解決サーバとの間に存在する、受信したパケットを他のノードに転送する機能を備えるパケット転送装置によって一旦受信され、前記パケット転送装置により、前記名前解決要求メッセージの送信者であるユーザに関する属性情報が、前記名前解決要求メッセージに含まれる送信元アドレスに基づいて取得され、前記属性情報を前記名前解決要求メッセージに付加された後に前記名前解決要求メッセージを前記名前解決サーバへ送信され、前記名前解決サーバは、前記パケット転送装置によって送信された前記名前解決要求に含まれる前記属性情報に基づいて、前記名前解決の結果である名前解決応答メッセージを返し、前記名前解決応答メッセージは、前記パケット転送装置を介して前記クライアントへ返されることを特徴とする。
【００３５】

本発明の第１の名前解決サーバは、名前解決要求メッセージを送信したユーザの属性情報が登録されているユーザ情報データベースを参照することにより、名前解決要求メッセージを送信したユーザの属性情報を取得するユーザ情報取得部と、取得した属性情報に基づいて名前解決をきめ細かにカスタマイズする応答作成部を有する。このような構成を採用することにより、本発明の第１の名前解決サーバは、受信した名前解決要求メッセージには含まれていない該メッセージ送信者の属性情報を用いて名前解決をカスタマイズすることができるため、クライアントは名前解決サーバが名前解決をカスタマイズするために必要な属性情報を該メッセージに含める必要はない。すなわち現在のユーザ環境（ユーザが利用する端末やＯＳ、アプリケーションソフトウェアなど）を変更する必要なく、名前解決サーバにおいて多様な属性情報に基づく名前解決のカスタマイズが可能になる。したがって本発明の第１の目的を達成することができる。

【００３６】

本発明の第２の名前解決サーバは、本発明の第１の名前解決サーバの構成に加えて、ユーザ情報管理部を含む。ユーザ情報管理部は、認証サーバが収集した属性情報及びログイン状況についての情報を認証サーバから取得する認証情報取得部と、さらに取得した属性情報及びログイン状況についての情報に基づいて、ユーザ情報データベースに属性情報を動的に登録したり、またはユーザ情報データベースから属性情報を動的に削除したりするユーザ情報管理部とを有する。このような構成を採用し、名前解決の際に参照される属性情報の登録または削除をユーザ情報データベースに対して自動的に行うことにより、本発明の第２の目的を達成することができる。

【００３７】

本発明の第３の名前解決サーバは、名前に対応する接続先と該接続先へのパケット転送方法との両方が登録されている応答用データベースを参照し、名前解決要求メッセージにより問い合わされた名前に対応する接続先と該接続先へのパケット転送方法との両方を含む名前解決応答メッセージを作成する応答作成部を有する。このような構成を採用し、名前解決要求メッセージ受信した場合は、問い合わされた名前に対応する接続先と該接続先へのパケット転送方法を含む名前解決応答メッセージをクライアントに送信することにより、本発明のパケット転送装置が該名前解決応答メッセージに含まれるパケット転送方法を利用することが可能となる。したがって本発明の第３の目的を達成することができる。

【００３８】

本発明のパケット転送装置は、名前解決要求メッセージを送信したユーザの属性情報を取得するユーザ情報取得部と、ユーザ情報取得部が取得した属性情報を名前解決要求メッセージに埋め込み、さらに本発明の第２の名前解決サーバが送信した名前解決応答メッセージからパケット転送方法を抜き取り、これをルーティングテーブルに保存するＤＮＳプロキシ部とを有する。このような構成を採用し、パケットを転送する際には、本発明の第２の名前解決サーバが送信した名前解決応答メッセージから抽出したパケット転送方法を参照することにより、本発明の第４の目的を達成することができる。

【発明の効果】

【００３９】

第１の効果は、クライアントにおけるリゾルバの変更なしに、名前解決サーバにおける名前解決応答を、名前解決要求メッセージの送信者（ユーザ）の任意の属性情報に基づいて柔軟にカスタマイズできる。

【００４０】

その理由は、本発明の第１の名前解決サーバが、ユーザ属性情報が格納されたユーザ情報データベースを保持し、名前解決要求メッセージ受信時に、該データベースを参照することにより、ユーザ属性情報を考慮した名前解決処理のカスタマイズを行うことができるからである。

【００４１】

第２の効果は、名前解決サーバにおいて、名前解決応答をカスタマイズするために用いる名前解決要求メッセージの送信者に関するユーザ属性情報を含むデータベースを自動的

に作成・管理することができる。

【００４２】

その理由は、本発明の第２の名前解決サーバが認証サーバと連携し、該認証サーバから該ユーザ属性情報を動的に取得し、該データベースに対して該ユーザ属性情報の登録・削除を自動的に行うことができるからである。

【００４３】

第３の効果は、名前解決サーバがクライアントに対して送信する名前解決応答メッセージに含まれる情報を、クライアントだけではなく、クライアントとＤＮＳサーバ間に設置されているパケット転送装置も利用することが可能になる。

【００４４】

その理由は、本発明の名前解決サーバがクライアントに名前解決応答メッセージを送信する際に、通常の名前解決応答とともに該応答に対応する本発明のパケット転送装置におけるパケット転送方法も埋めこんで送信し、さらに本発明のパケット転送装置は該応答メッセージがクライアントに到達する前に該応答メッセージを一旦受信し、該応答メッセージ内に埋めこまれたパケット転送方法を抽出して自ノード内のルーティングテーブルに対応するエントリを作成するからである。

【実施例１】

【００４５】

次に、本発明の実施の形態について図面を参照して詳細に説明する。

図１を参照すると、本発明の第１の実施の形態は、クライアントＡ１と名前解決サーバであるＤＮＳサーバＢ１とによって実現される。クライアントＡ１とＤＮＳサーバＢ１はネットワークＣ１を介して接続されている。ＤＮＳサーバＢ１は、ＤＮＳにおける名前解決機能をもつサーバだけではなく、他の用途における名前解決機能をもつサーバとして一般化することもできる。他の用途における名前解決機能をもつサーバの例として、ＷＩＮＳ（Windows（登録商標） Ｉｎｔｅｒｎｅｔ Ｎａｍｅ Ｓｅｒｖｉｃｅ）サーバやＮＩＳ（Ｎｅｔｗｏｒｋ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｒｖｉｃｅ）サーバが挙げられる。ただし、以下では名前解決機能を持つサーバとしてＤＮＳサーバを例にとり説明する。

【００４６】

クライアントＡ１は、「ｗｗｗ．ｂｉｇｌｏｂｅ．ｎｅ．ｊｐ」や、「ｆｔｐ．ｎｅｃ．ｃｏｍ」など、ネットワーク上のノードのＦＱＤＮに対応するＩＰアドレスを解決するため、あるいは逆にあるＩＰアドレスに対応するＦＱＤＮを解決するためにＤＮＳサーバＢ１に対して名前解決要求メッセージとしてＤＮＳクエリメッセージを送信する。他にも、クライアントＡ１がＤＮＳサーバＢ１を利用する目的の例としては、ＲＦＣ２７８２に記載されているような、ｆｔｐやｈｔｔｐなどのサービス名に対応する該サービスを提供するホストとポート番号の解決や、ＲＦＣ２９１６に記載されているような、電話番号に対応するＵＲＩ（Ｕｎｉｖｅｒｓａｌ Ｒｅｓｏｕｒｃｅ Ｉｄｅｎｔｉｆｉｅｒ）の解決などが挙げられる。ただし、以下、ＤＮＳサーバＢ１によってＦＱＤＮからＩＰアドレスの解決またはＩＰアドレスからＦＱＤＮの解決を行なう場合を中心にして説明する。

【００４７】

クライアントＡ１は、送信したＤＮＳクエリメッセージに対して、ＤＮＳサーバＢ１から返される名前解決応答メッセージとしてＤＮＳ応答メッセージを受信する。ＤＮＳ応答メッセージには、名前解決の結果が含まれる。

【００４８】

クライアントＡ１の例としては、一般的にはＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）や携帯端末、ワークステーションなどの端末ノード（利用端末）が挙げられるが、その他、ＤＮＳサーバＢ１以外の別のＤＮＳサーバが何らかの名前解決を行うためにＤＮＳサーバＢ１に対して再帰的なＤＮＳクエリを行う場合もあり、このようなＤＮＳサーバをクライアントＡ１に含めて考えることができる。

【００４９】

ＤＮＳサーバＢ１は、クエリ受信部Ｂ１１と、ユーザ情報識別部Ｂ１２と、ユーザ情報

取得部Ｂ１３と、ユーザ情報データベースＢ１４と、応答作成部Ｂ１５と、応答用データベースＢ１６と、応答送信部Ｂ１７とを含む。

【００５０】

ＤＮＳサーバＢ１は、従来のＤＮＳサーバの構成と比べ、ユーザ情報識別部１２と、ユーザ情報取得部Ｂ１３と、ユーザ情報データベースＢ１４とを新たに有する点が大きく異なる。

【００５１】

クエリ受信部Ｂ１１は、クライアントＡ１が送信したＤＮＳクエリメッセージを受信し、それをユーザ情報識別部Ｂ１２に渡す。

【００５２】

ユーザ情報識別部Ｂ１２は、ＤＮＳクエリメッセージを受け取ると、該メッセージ内に、該メッセージの送信者であるユーザのユーザ属性情報が含まれているかを調べ、含まれている場合は該ユーザ属性情報を読み取って識別する。もし含まれていない場合は、ユーザ情報取得部Ｂ１３を介してユーザ情報データベースＢ１４からＤＮＳクエリメッセージの送信者のユーザ属性情報を取得する処理を行う。

【００５３】

また、ユーザ情報識別部Ｂ１２は、ユーザ属性情報を取得できた場合は、ユーザ属性情報とＤＮＳクエリメッセージを応答作成部Ｂ１５に渡す。ユーザ属性情報を取得できなかった場合は、ＤＮＳクエリメッセージのみを応答作成部Ｂ１５に渡す。

【００５４】

ここで、ユーザ属性情報とは、例えばユーザ（クライアントＡ１）のユーザＩＤ、位置情報、趣味若しくは行動履歴などの嗜好に関する情報、携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）、ノートパソコンといった利用端末種別、利用端末にインストールされているＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）、装備されているネットワークインタフェースやＣＰＵ速度、メモリ量といった利用端末に関する情報、利用端末のＩＰアドレスおよびＭＡＣアドレス、ＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）やＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ　Ｓｅｒｖｉｃｅｓ　Ｄｉｇｉｔａｌ　Ｎｅｔｗｏｒｋ）といった接続回線種別、接続回線速度、接続しているＮＡＳ（Ｎｅｔｗｏｒｋ　Ａｃｃｅｓｓ　Ｓｅｒｖｅｒ）のＩＰアドレスといったネットワークへの接続状況に関する情報などの、ユーザに関する情報全般を指す。

【００５５】

ユーザ情報取得部Ｂ１３は、ＤＮＳサーバＢ１が受信したＤＮＳクエリメッセージ内に該メッセージの送信者のユーザ属性情報が含まれていない場合に、ユーザ情報識別部Ｂ１２から渡された情報（該メッセージのソースＩＰアドレスまたはソースＭＡＣアドレスなど）を基にユーザ情報データベースＢ１４から該ユーザ属性情報を取得し、ユーザ情報識別部Ｂ１２へ渡す。

【００５６】

ユーザ情報データベースＢ１４には、ＤＮＳサーバＢ１に対して名前解決を行うユーザのユーザ属性情報及びユーザ属性情報を取得するための参照先が登録されている。ユーザ情報データベースＢ１４には、必要に応じて任意のユーザ属性情報を登録しておくことができる。

【００５７】

ユーザ情報データベースＢ１４の内容例を図２に示す。図２のユーザ情報データベースＢ１４では、ＩＳＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）が運営するネットワークへのログインＩＤ、利用端末のＩＰアドレス、接続回線種別、接続しているＮＡＳのＩＰアドレス、及びユーザ情報データベースＢ１４には直接登録されていないが外部のサーバから必要なユーザ属性情報が取得できる場合に、該ユーザ属性情報を取得するための参照先が登録されている。

【００５８】

図２において「－」は、該当する項目の内容がこのユーザ情報データベースＢ１４に登録されていないことを示している。例えば１番目のエントリでは参照先が「－」となっており、このエントリに属性情報が登録されているユーザに関してはこれ以上の属性情報を得るための参照先が不明または存在しないことを示している。また２番目のエントリは、接続回線種別が不明であることが示されており、登録されていないユーザ属性情報については参照先に登録されているＩＰアドレス「８．９．１．４」で指定されるノードを参照することで取得可能であることが示されている。さらに３番目のエントリでは、利用端末のＩＰアドレスが「１２３．４５．１．０／２４」の範囲にあるユーザ属性情報を、ＩＰアドレスが「９．９．９．９」で指定されるノードを参照することで取得可能であることが示されている。

【００５９】

応答作成部Ｂ１５は、応答用データベースＢ１６を参照し、ＤＮＳクエリメッセージにより要求されたＦＱＤＮ→ＩＰアドレスまたは、ＩＰアドレス→ＦＱＤＮなどの名前解決処理を行う。ここで、ユーザ情報識別部Ｂ１２からＤＮＳクエリメッセージと共に、ユーザ属性情報を渡された場合は、ユーザ属性情報を考慮した名前解決処理を行う。ユーザ属性情報を考慮することにより、例えばユーザが動画の配信を行っているサーバのＦＱＤＮ→ＩＰアドレスの名前解決を要求した際、同一のＦＱＤＮに関するＤＮＳクエリであっても、例えば接続回線種別がＡＤＳＬ回線であるユーザには広帯域で配信を行っているサーバのＩＰアドレスを解決したり、接続回線種別がＩＳＤＮ回線であるユーザには狭帯域で配信を行っているサーバのＩＰアドレスを解決したりするといったユーザ毎の名前解決処理のカスタマイズを行うことができる。

【００６０】

応答用データベースＢ１６には、ユーザの属性毎にＦＱＤＮ→ＩＰアドレス及び、ＩＰアドレス→ＦＱＤＮなどの解決方法を示すエントリが登録されている。ユーザ属性情報に依存しないデフォルトの名前解決方法も登録されている。

【００６１】

応答用データベースＢ１６の例を図３に示す。図３に示した応答用データベースＢ１６は２種類のテーブルから構成される。一つはＦＱＤＮ→ＩＰアドレスなどの具体的な名前解決方法が登録されているテーブル（ゾーンファイル）であり、ゾーンファイル２０２及び２０３が該当する。このゾーンファイル２０２、２０３に登録される主な情報には、エントリの種類を示すＴＹＰＥ、名前解決のキーとなるＦＱＤＮ、名前解決により応答するデータを示すＤＡＴＡがある。用いられるＴＹＰＥの例としては、あるＦＱＤＮに対応するＩＰアドレスの解決を示すＡレコード、あるＦＱＤＮに対応するメールサーバのアドレスの解決を示すＭＸレコード、あるＦＱＤＮの別名を示すＣＮＡＭＥレコードなどがある。ここで、ゾーンファイル２０２の１番目のエントリを参照すると、エントリの種類（ＴＹＰＥ）がＦＱＤＮからＩＰアドレスの解決を示すＡレコードであり、ＦＱＤＮ：ｗｗｗ．ａａａ．ｃｏｍに対応するＩＰアドレス（ＤＡＴＡ）が「９．８．７．６」であることが示されている。

【００６２】

もう一つは、ユーザ属性情報及びドメイン空間毎に名前解決方法の参照先が登録されているテーブル（名前解決テーブル）であり、名前解決テーブル２０１が該当する。名前解決テーブル２０１では、ユーザＩＰアドレス、ユーザＩＤ、接続回線種別及びＮＡＳのＩＰアドレスといったユーザ属性情報の組み合わせ毎に、名前解決方法の参照先が登録されている。

【００６３】

名前解決テーブル２０１において、「－」は名前解決の際に考慮しないユーザ属性情報を示している。例えば１番目のエントリでは、ユーザ属性情報のうち、ユーザＩＰアドレス及びユーザＩＤは考慮されず、接続回線種別およびＮＡＳアドレスのみが考慮されることになる。１番目のエントリは、ユーザＩＰアドレス及びユーザＩＤが任意であって、接続回線種別がＡＤＳＬ回線でありかつ、接続しているＮＡＳのＩＰアドレスが「３０．３

０．３０．３０」であるユーザが、ドメイン空間ａａａ．ｃｏｍに属するＦＱＤＮの問い合わせを行った際に、ゾーンファイルａｄｓｌ＿ａａａ＿ｃｏｍ．ｄａｔ（ゾーンファイル２０２）が参照されることを示している。同様に、３番目のエントリは、ユーザ属性情報のうち、ユーザＩＰアドレス、アクセス回線種別及びＮＡＳのＩＰアドレスが任意で、ユーザＩＤが「ｊｉｒｏ」のユーザが、ドメイン空間ｂｂｂ．ｃｏｍに属するＦＱＤＮの問い合わせを行った際に、ゾーンファイルｊｉｒｏ＿ｂｂｂ＿ｃｏｍ．ｄａｔが参照されることを示している。また、４番目のエントリは、ＩＰアドレス「１２３．４５．１．５」から、ドメイン空間ｂｂｂ．ｃｏｍに属するＦＱＤＮのＤＮＳクエリがあった場合は、ＩＰアドレス「１．２．３．４」で指定される他のＤＮＳサーバにおいて名前解決処理が行われることを示している。

【００６４】

また、最後のエントリ（ＤＥＦＡＵＬＴ）にはユーザ属性情報に依存しないデフォルトのＩＰアドレスの解決方法が登録されている。このエントリは、ユーザ属性情報が名前解決テーブル２０１に登録されているユーザ属性情報のいずれにも該当しない場合、またはユーザ情報識別部Ｂ１２においてＤＮＳクエリメッセージに対応するユーザ属性情報が取得できなかった場合に参照される。

【００６５】

応答送信部Ｂ１７は、応答作成部Ｂ１５から渡された名前解決の処理結果を元にＤＮＳ応答メッセージを生成し、クライアントＡ１へ送信する。

【００６６】

次に、図４を参照して、本実施の形態において、ＤＮＳサーバＢ１がＤＮＳクエリメッセージを受信してから応答メッセージを送信するまでの動作について詳細に説明する。

【００６７】

クエリ受信部Ｂ１１は、クライアントＡ１からＤＮＳクエリメッセージを受信すると（図４のステップＳ１０１）、該メッセージをユーザ情報識別部Ｂ１２に渡す。

【００６８】

ユーザ情報識別部Ｂ１２は、ＤＮＳクエリメッセージを受け取ると、該メッセージの送信者のユーザ属性情報の取得処理を行う（ステップＳ１０２）。

【００６９】

ここで、図５を参照して、ステップＳ１０２のユーザ属性情報の取得処理を詳細に説明する。

【００７０】

まず、ユーザ情報識別部Ｂ１２は、受信したＤＮＳクエリメッセージに、ユーザ属性情報が埋め込まれているか否かを判断する（図５のステップＳ１０２１）。ユーザ属性情報が埋め込まれている場合はこれを読み出して取得し（ステップＳ１０２２）、ユーザ属性情報の取得処理は終了する。

【００７１】

ステップＳ１０２１でユーザ属性情報が埋め込まれていない場合は、受信したＤＮＳクエリメッセージはユーザ情報識別部Ｂ１２からユーザ情報取得部Ｂ１３へ渡され、ユーザ情報取得部Ｂ１３は該メッセージを送信したユーザを特定する手がかりとなる情報を抽出する（ステップＳ１０２３）。抽出する手がかりとなる情報の例としては、ＤＮＳクエリメッセージのソースＩＰアドレスが挙げられる。クライアントＡ１がユーザ利用端末のリゾルバである場合、ＤＮＳクエリメッセージのソースＩＰアドレスはユーザの利用端末のＩＰアドレスであるためである。また、クライアントＡ１がユーザ利用端末のリゾルバであり、クライアントＡ１とＤＮＳサーバＢ１が途中にルータを介さず直接接続されている場合は、クライアントＡ１のソースＭＡＣアドレスも同様にＤＮＳクエリメッセージを送信したユーザを特定する手がかりとして利用することができる。

【００７２】

次に、ユーザ情報取得部Ｂ１３は、ユーザ情報データベースＢ１４からステップＳ１０２３で抽出した情報に該当するエントリを検索する（ステップＳ１０２４）。

【００７３】
ステップＳ１０２４において、対応するエントリが存在しない場合は、ステップＳ１０３の取得処理は終了する（ステップＳ１０２５）。
【００７４】
ステップＳ１０２４において、対応するエントリが存在した場合、ユーザ情報取得部Ｂ１３は、対応するエントリの内容をもとに、ユーザ属性情報をローカルのユーザ情報データベースＢ１４以外の情報源も参照して取得すべきか否かを判断する（ステップＳ１０２５、Ｓ１０２６）。ユーザ属性情報をローカルのユーザ情報データベースＢ１４以外の他の情報源を参照して取得する必要がないと判断した場合は、ユーザ情報取得部Ｂ１３はステップＳ１０２５で発見したエントリからユーザ属性情報を取得する（ステップＳ１０２７）。
【００７５】
他の情報源も参照してユーザ属性情報を取得すべきと判断した場合は、ユーザ情報取得部Ｂ１３はステップＳ１０２５で発見したエントリからユーザ属性情報を取得するのに加えて、更にユーザ情報データベースＢ１４以外の情報源も参照してユーザ属性情報の取得処理を行う。（ステップＳ１０２８）。
【００７６】
上記において、ローカルのユーザ情報データベースＢ１４以外の情報源も参照して取得すべきか否かは、ユーザ情報データベースＢ１４に外部のサーバ等の参照先が登録されているかどうかによって判断する。
【００７７】
例えば、ユーザ情報データベースＢ１４が図２に示す内容である場合のステップＳ１０２５～Ｓ１０２８の例を述べる。ＤＮＳクエリメッセージからユーザを特定する手がかりとなる情報としてソースＩＰアドレスを抽出し、そのＩＰアドレスが「１２３．４５．０．２」であった場合、ユーザ情報取得部Ｂ１３は、ユーザ情報データベースＢ１４からＩＰアドレスが「１２３．４５．０．２」となっているエントリを検索する（ステップＳ１０２５）。この場合発見されるエントリは１番目のエントリであり、その参照先は「－」となっているため、ユーザ情報取得部Ｂ１３は、他のノード（外部のサーバ等）を参照せず、ユーザ情報データベースＢ１４のみを参照して取得すると判断し（ステップＳ１０２６）、１番目のエントリに示されているユーザ属性情報を取得する（ステップＳ１０２７）。
【００７８】
ＤＮＳクエリメッセージのソースＩＰアドレスが「１２３．４５．０．４」であった場合は、２番目のエントリが発見される。その参照先には、参照先のノードのＩＰアドレスが登録されているため、ユーザ情報取得部Ｂ１３は、他のノードを参照すべきだと判断し（ステップＳ１０２６）、２番目のエントリに登録されているユーザ属性情報を取得するとともに、登録されているＩＰアドレスのノードが保持するユーザ属性情報のデータベースからもユーザ属性情報を取得する（ステップＳ１０２８）。
【００７９】
図４のフローチャートの説明に戻る。ユーザ情報識別部Ｂ１２は、ステップＳ１０２におけるユーザ属性情報取得処理の後、ＤＮＳサーバＢ１が受信したＤＮＳクエリメッセージと該メッセージ送信者のユーザ属性情報とを一緒に応答作成部Ｂ１５へ渡す。ステップＳ１０２において、該メッセージ送信者のユーザ属性情報が取得できなかった場合は、対応するユーザ属性情報はないものとして該メッセージを取り扱い、該ＤＮＳクエリメッセージだけを応答作成部Ｂ１５へ渡す。
【００８０】
応答作成部Ｂ１５は、ＤＮＳクエリメッセージと対応するユーザ属性情報を一緒に渡された場合、ＤＮＳクエリメッセージで問い合わされたＦＱＤＮ又はＩＰアドレス、及びユーザ属性情報に該当するエントリを、応答用データベースＢ１６を参照して検索する（ステップＳ１０３）。ＤＮＳクエリメッセージだけを受け取った場合は、受け取ったＤＮＳ

クエリメッセージで問い合わされたＦＱＤＮ又はＩＰアドレスに該当するデフォルトのエントリを、応答用データベースＢ１６を参照して検索する（ステップＳ１０３）。

【００８１】

応答作成部Ｂ１５は、検索したエントリの内容から名前解決が他のＤＮＳサーバで行われるべきか否かを判断する（ステップＳ１０４）。ここでは、図３に示す応答用データベースＢ１６の名前解決テーブル２０１の参照先として他のＤＮＳサーバのアドレスが登録されている場合に、名前解決が他のＤＮＳサーバで行われるべきと判断される。

【００８２】

ステップＳ１０４において、他のＤＮＳサーバで行われるべきであると判断した場合は、名前解決処理が他のＤＮＳサーバによって行なわれるように処理する（ステップＳ１０６）。名前解決処理が他のＤＮＳサーバで行われるように処理する方法の例として、以下の二つの方法が挙げられる。

【００８３】

第１の方法は、他のＤＮＳサーバに、ユーザ情報識別部Ｂ１２から渡されたユーザ属性情報とＤＮＳクエリメッセージの両方またはＤＮＳクエリメッセージのみを、転送する方法である。この方法を採用する場合の応答作成部Ｂ１５の構成を図６に示す。

【００８４】

図６を参照すると、応答作成部Ｂ１５は応答作成メイン部Ｂ１５１とリゾルバ部Ｂ１５２とを含む。応答作成メイン部Ｂ１５１は、上記のステップＳ１０３及びステップＳ１０４の処理を行い、ステップＳ１０４において名前解決が他のＤＮＳサーバで行われるべきであると判断した場合、リゾルバ部Ｂ１５２に対して、ユーザ情報識別部Ｂ１２から渡されたユーザ属性情報とＤＮＳクエリメッセージの両方またはＤＮＳクエリメッセージのみを渡し、さらに名前解決が行われるべき他のＤＮＳサーバを通知する。リゾルバ部Ｂ１５２は、応答作成メイン部Ｂ１５１から渡された情報を元に、ユーザ属性情報とＤＮＳクエリメッセージの両方またはＤＮＳクエリメッセージのみの転送を行う。

【００８５】

リゾルバ部Ｂ１５２がユーザ属性情報とＤＮＳクエリメッセージの両方を他のＤＮＳサーバへ転送する方法としては、例えばＤＮＳクエリメッセージをＤＮＳメッセージのフォーマットに従って構築し、その中にユーザ属性情報を埋め込んで送信する方法が考えられる。ＤＮＳメッセージのフォーマットには、付加的な情報を埋め込むために付加情報部と呼ばれるフィールドが用意されており、付加情報部には任意の情報をＤＮＳの資源レコードの形式で埋め込むことができる。

【００８６】

この方法では、受け取ったユーザ属性情報を資源レコードの形式にエンコードし、それをＤＮＳクエリメッセージの付加情報部に埋め込み、他のＤＮＳサーバに転送する（ステップＳ１０６）。そしてリゾルバ部Ｂ１５２は、該ＤＮＳクエリメッセージを転送した他のＤＮＳサーバから、対応するＤＮＳ応答メッセージを受信すると、それを応答送信部Ｂ１７に渡し、応答送信部Ｂ１７が該応答メッセージをクライアントＡ１へ転送する（ステップＳ１０７）。

【００８７】

この転送方法をとることで、ユーザ属性情報が埋め込まれたＤＮＳクエリメッセージを従来のＤＮＳサーバにおいて処理することも可能となるため、本発明によるＤＮＳサーバＢ１とそれ以外の従来からのＤＮＳサーバの共存を図ることができる。

【００８８】

第２の方法は、クライアントＡ１に、名前解決が他のＤＮＳサーバで行われるべき旨を通知するメッセージをＤＮＳ応答メッセージとして返し、通知を受け取ったクライアントＡ１が改めて他のＤＮＳサーバにＤＮＳクエリメッセージを送信する方法である。この場合、応答送信部Ｂ１７は、クライアントＡ１が改めてＤＮＳクエリメッセージを送信すべき他のＤＮＳサーバのＩＰアドレスを含むＤＮＳ応答メッセージをクライアントＡ１へ送信する（ステップＳ１０７）。

【００８９】
一方、ステップＳ１０４において、応答作成部Ｂ１５が、自サーバにおいて名前解決を行うべきであると判断した場合は、検索したエントリの内容に従って、ＦＱＤＮ→ＩＰアドレスまたはＩＰアドレス→ＦＱＤＮの名前解決を行い（ステップＳ１０５）、その結果を応答送信部Ｂ１７に渡す。
【００９０】
応答送信部Ｂ１７は、受け取った名前解決結果を元にＤＮＳ応答メッセージを生成し、それをクライアントＡ１へ送信する（ステップＳ１０７）。
【００９１】
以上の第１の実施の形態の説明においては、ＤＮＳサーバＢ１はユーザ情報データベースＢ１４をその構成要素として含むものであった。他の構成として、ユーザ情報データベースＢ１４がＤＮＳサーバＢ１内ではなく別のサーバ内に保持される形態も考えられる。この場合の構成を第１の実施の形態の他例として図７に示す。
【００９２】
この他例では、先に示した図１の構成と比べ、先に示したＤＮＳサーバＢ１の代わりに、ユーザ情報データベースＢ１４を含まないＤＮＳサーバＢ２が用いられ、さらに、ユーザ情報データベースＤ１１をその構成要素として含むデータベースサーバＤ１が用いられる。
【００９３】
図７に示す構成におけるＤＮＳサーバＢ２の動作については、上述したＤＮＳサーバＢ１の動作においてユーザ情報データベースＢ１４をユーザ情報データベースＤ１１と置きかえることにより同様に考えることができる。
【００９４】
データベースサーバＤ１の機能は、専用のノードにより実現することも、他のＤＮＳサーバＢ１またはＢ２の一機能として実現することも可能である。後者の場合、ユーザ情報データベースＤ１１は応答用データベースＢ１６として管理され、ユーザ情報取得部Ｂ１３は当該他のＤＮＳサーバＢ１またはＢ２に対してＤＮＳメッセージを用いてユーザ属性情報を取得することになる。
【００９５】
この場合の応答用データベースＢ１６の内容例を図８に示す。図８に示す名前解決テーブル３０１は、図３に示した名前解決テーブル２０１と同様の形式をとっており、ユーザ属性情報は３番目のエントリを参照することで取得される。３番目のエントリは、ユーザ属性情報がファイルｕｓｅｒ＿ｃｏｍ．ｄａｔ（ゾーンファイル３０２）に格納されていることを示している。ゾーンファイル３０２には、図２に示したユーザ情報データベースＢ１４と同じユーザ属性情報が格納されており、ユーザ属性情報はユーザの利用端末のＩＰアドレスを含むＦＱＤＮをキーとして、ＤＮＳの資源レコードの一種であるＴＸＴレコードの形で格納されている。
【００９６】
例えば、ゾーンファイル３０２の１番目のエントリからは、利用端末のＩＰアドレスが「１２３．４５．０．２」であるユーザのユーザ属性情報として、ログインＩＤがｔａｒｏ（ｌｏｇｉｎ　ｉｄ＝ｔａｒｏ）、接続回線種別がＡＤＳＬ回線（ａｃｃｅｓｓ　ｍｅｄｉａ＝ＡＤＳＬ）、接続しているＮＡＳのＩＰアドレスが「３０．３０．３０．３０」（ＮＡＳ　ａｄｄｒｅｓｓ＝３０．３０．３０．３０）であることが分かる。ユーザ情報取得部Ｂ１３は、利用端末のＩＰアドレスが「１２３．４５．０．２」であるユーザのユーザ属性情報を取得したい場合、データベースサーバＤ１に対して、ドメイン名が「１２３．４５．０．２．ｕｓｅｒ．ｃｏｍ」のＴＸＴレコードを要求するＤＮＳクエリメッセージを送信する。
【００９７】
次に第１の実施の形態の効果について説明する。
【００９８】

本実施の形態では、ＤＮＳサーバＢ１が、ユーザ属性情報が管理されているユーザ情報データベースＢ１４を参照することにより、ユーザ属性情報を考慮した名前解決処理のカスタマイズを行う。ユーザ情報データベースＢ１４に予めユーザ属性情報を登録しておけば、ＤＮＳサーバＢ１は、ユーザ情報データベースＢ１４を参照することで、任意のユーザ属性情報を考慮した名前解決処理を行うことができる。

【００９９】

前述のように、従来の技術では、ＤＮＳサーバがユーザに関する属性情報として利用できるのは、受信したＤＮＳクエリメッセージのソースＩＰアドレスだけであった。もしくは、その他の属性情報も利用しようとする場合は、クライアントが送信するＤＮＳクエリメッセージ内に必要な属性情報を全て埋めこむ必要があり、クライアントにおけるリゾルバの変更が必要であった。

【０１００】

本実施の形態では、ＤＮＳサーバＢ１はユーザ情報データベースＢ１４を参照することにより、クライアントにおけるリゾルバの変更の必要がない。また、ＤＮＳサーバごとに考慮するユーザ属性情報の種類が異なる場合でも、従来技術では対応が困難であったが、本実施の形態によりユーザ情報データベースＢ１４に登録するユーザ属性情報の種類をＤＮＳサーバごとに変えるだけで柔軟かつ容易に実現できる。

【０１０１】

次に、本発明の第２の実施の形態について図面を参照して詳細に説明する。

【０１０２】

図９を参照すると、本発明の第２の実施の形態は、図１の第１の実施の形態で示されたクライアントＡ１とネットワークＣ１に加え、本発明によるＤＮＳサーバＢ３と認証サーバＥ１とを備えて実現される。

【０１０３】

本発明の第２の実施の形態では、ユーザ情報データベースＢ１４の管理を、ＤＮＳサーバＢ３の構成要素であるユーザ情報管理部Ｂ１８が認証サーバＥ１と連携することによって自動的に行う点が、本発明の第１の実施の形態と異なる。以下、クライアントＡ１、ＤＮＳサーバＢ３、認証サーバＥ１から構成されるシステムを本システムと呼ぶ。

【０１０４】

認証サーバＥ１は、システム内のユーザ（クライアントＡ１）の認証要求に応じてユーザ認証を行い、ユーザのシステムへのログインを許可または禁止する。ここでのシステムとは、本システムに限らず、例えばＩＳＰが運営するネットワークやＡＳＰ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）が運営する会員制ＷＥＢサービスなど、利用する際にユーザ認証が行われるもの全般を指す。本システム内のユーザは、ここでのシステムのユーザの一部若しくは全てである。

【０１０５】

認証サーバＥ１は、ユーザ認証を行うとともに、認証要求を送信したユーザ（クライアントＡ１）がシステムにログインしたのかログアウトしたのかというユーザのログイン状況を把握し、さらにユーザ属性情報を収集し、これらの情報をログとして保持する。認証サーバＥ１が収集するユーザ属性情報の例としては、第１の実施の形態の説明で述べたのと同様に、ユーザ（クライアントＡ１）の位置情報、趣味若しくは行動履歴などの嗜好に関する情報、携帯電話やＰＤＡ、ノートパソコンといった利用端末種別、利用端末にインストールされているＯＳ、装備されているネットワークインタフェースやＣＰＵ速度、メモリ量といった利用端末に関する情報、利用端末のＩＰアドレス、ＡＤＳＬ回線やＩＳＤＮ回線といった接続回線種別、接続回線速度、接続しているＮＡＳのＩＰアドレスといったネットワークへの接続状況に関する情報などが挙げられる。

【０１０６】

認証サーバＥ１の例としては、ＩＳＰ等でユーザ認証および課金処理に広く利用されているＲＡＤＩＵＳサーバが挙げられる。ＲＡＤＩＵＳサーバは、ＲＡＤＩＵＳプロトコルによるユーザ認証処理において、ユーザから受信した認証要求に含まれるＩＤとパスワー

ドを元にユーザの認証を行い、ユーザのログインを許可または禁止する。ＲＡＤＩＵＳプロトコルは、ＩＳＰが運用するネットワークに限らず、多くのネットワークシステムにおいてユーザ認証に用いられている。

【０１０７】

また、ＲＡＤＩＵＳサーバには、ユーザがネットワークシステムにログインまたはログアウトする度に、ユーザのログイン状況及びユーザ属性情報が、ＮＡＳなどのＲＡＤＩＵＳクライアントから送信される。ＲＡＤＩＵＳサーバは、これらの情報を課金やバックトレースの目的で収集し、Ａｃｃｏｕｎｔ　Ｌｏｇとして保持する。ＲＡＤＩＵＳクライアントがＲＡＤＩＵＳサーバに送信するユーザ属性情報としては、例えばユーザのＩＳＰのログインＩＤ、ユーザが利用している端末のＩＰアドレス、ユーザが接続しているＮＡＳのＩＰアドレス、接続回線種別などが含まれる。

【０１０８】

ユーザ情報管理部Ｂ１８は、認証情報取得部Ｂ１８１とユーザ情報更新部Ｂ１８２とを含む。

【０１０９】

認証情報取得部Ｂ１８１は、ユーザのログイン状況の変化を検出し、認証サーバＥ１からユーザのログイン状況を示す情報及びユーザ属性情報を取得し、これらの情報をユーザ情報更新部Ｂ１８２に渡す。ユーザのログイン状況の変化の検出と、ユーザのログイン状況を示す情報及びユーザ属性情報の取得を実現する方法の例として、次の２つの方法が挙げられる。

【０１１０】

第１の方法は、認証サーバＥ１がユーザのログイン状況の変化を検出した際に、ユーザのログイン状況を示す情報とユーザ属性情報とを認証サーバＥ１から認証情報取得部Ｂ１８１に通知してもらう方法である。

【０１１１】

第２の方法は、認証情報取得部Ｂ１８１が、認証サーバＥ１にユーザのログイン状況を問い合わせることによって、ユーザのログイン状況の変化を検出し、ログイン状況の変化を検出した際に、認証サーバＥ１からユーザのログイン状況を示す情報とユーザ属性情報を取得する方法である。

【０１１２】

第１の方法では、認証情報取得部Ｂ１８１は認証サーバＥ１からの通知を待つという受動的な処理で、ユーザのログイン状況の変化を検出するのに対し、第２の方法では、ユーザのログイン状況の変化を検出するために、認証情報取得部Ｂ１８１が認証サーバＥ１にユーザのログイン状況を問い合わせるという能動的な処理を行う。

【０１１３】

以下、それぞれの方法の具体例について述べる。

【０１１４】

まず、第１の方法の具体例としては、ＲＡＤＩＵＳプロトコルのＰｒｏｘｙ機能及びＲｅｌａｙ機能を利用する方法が挙げられる。Ｐｒｏｘｙ機能は、ＲＡＤＩＵＳサーバがＲＡＤＩＵＳクライアントからユーザのログイン状況及びユーザ属性情報を受信する度に、これらの情報を他のノードへ転送する機能である。Ｐｒｏｘｙ機能は標準化された機能であり、現在利用されているＲＡＤＩＵＳサーバのほぼ全てに実装されている。

【０１１５】

Ｐｒｏｘｙ機能を用いてユーザのログイン状況及び属性情報を取得する場合のシーケンスの例を図１０に示す。図１０ではユーザがシステムにログインした際のシーケンス例を示している。なお、図１０において認証サーバＥ１はＲＡＤＩＵＳサーバである。ユーザ認証が成功し、ユーザがシステムにログインすると、ＲＡＤＩＵＳクライアントから認証サーバＥ１に対して、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージが送信される。

【０１１６】

Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージには、ユーザ属性情報が、属性＝属

性値の形で含まれている。図に示した例では、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージに、ユーザＩＤがｔａｒｏ（（１）Ｕｓｅｒ　Ｎａｍｅ　＝　ｔａｒｏ）、ＮＡＳのＩＰアドレスが「３０．３０．３０．３０」（（４）ＮＡＳ－ＩＰ－Ａｄｄｒｅｓｓ　＝　３０．３０．３０．３０）、ユーザ利用端末のＩＰアドレスが１２３．４５．０．２（（８）Ｆｒａｍｅｄ－ＩＰ－Ａｄｄｒｅｓｓ　＝　１２３．４５．０．２）、接続回線種別がＡＤＳＬ（（６１）ＮＡＳ－Ｐｏｒｔ－Ｔｙｐｅ＝ＡＤＳＬ）であることを示す情報が含まれる。また、ユーザがシステムにログインした旨を示す情報（（４０）Ａｃｃｔ－Ｓｔａｔｕｓ－Ｔｙｐｅ＝Ｓｔａｒｔ　）も含まれる。

【０１１７】

認証サーバＥ１はＡｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージを受信すると、Ｐｒｏｘｙ機能を利用して、受信したＡｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージをユーザ情報管理部Ｂ１８へ送信する。ユーザ情報管理部Ｂ１８は受信したＡｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージからユーザ属性情報を取得する。ユーザ情報管理部Ｂ１８は、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージを受信後、認証サーバＥ１に対してＡｃｃｏｕｎｔｉｎｇ　Ｒｅｓｐｏｎｓｅメッセージを送信する。

【０１１８】

次に、Ｒｅｌａｙ機能を用いたユーザ情報の取得について説明する。Ｒｅｌａｙ機能は、Ａｃｃｏｕｎｔ　Ｌｏｇに新たなログが追加されるたびに、ＲＡＤＩＵＳサーバがそれを他のノードへ送信する機能である。Ｒｅｌａｙ機能はデファクト化された機能であり、多くのＲＡＤＩＵＳサーバに実装されている。

【０１１９】

Ｒｅｌａｙ機能を用いてユーザのログイン状況及び属性情報を取得する場合のシーケンスの例を図１１に示す。図１１では、ユーザがシステムにログインした際のシーケンスを示している。なお、図１１において認証サーバＥ１はＲＡＤＩＵＳサーバである。ユーザ認証が成功し、ユーザがシステムにログインすると、認証サーバＥ１が保持するＡｃｃｏｕｎｔ　Ｌｏｇに新たなログが追加される。認証サーバＥ１は新たに追加されたログを元に、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージを生成し、これをユーザ情報管理部Ｂ１８へ送信する。

【０１２０】

図１１では、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージに、ユーザＩＤがｔａｒｏ（（１）Ｕｓｅｒ　Ｎａｍｅ　＝　ｔａｒｏ）、ＮＡＳのＩＰアドレスが「３０．３０．３０．３０」（（４）ＮＡＳ－ＩＰ－Ａｄｄｒｅｓｓ　＝　３０．３０．３０．３０）、ユーザ利用端末のＩＰアドレスが１２３．４５．０．２（（８）Ｆｒａｍｅｄ－ＩＰ－Ａｄｄｒｅｓｓ　＝　１２３．４５．０．２）、接続回線種別がＡＤＳＬ（（６１）ＮＡＳ－Ｐｏｒｔ－Ｔｙｐｅ＝ＡＤＳＬ）であることを示す情報が含まれる。また、ユーザがシステムにログインした旨を示す情報（（４０）Ａｃｃｔ－Ｓｔａｔｕｓ－Ｔｙｐｅ＝Ｓｔａｒｔ　）も含まれる。ユーザ情報管理部Ｂ１８は受信したＡｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージからユーザ属性情報を取得する。ユーザ情報管理部Ｂ１８は、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージを受信後、認証サーバＥ１に対してＡｃｃｏｕｎｔｉｎｇ　Ｒｅｓｐｏｎｓｅメッセージを送信する。

【０１２１】

次に、第２の方法の具体例を説明する。認証情報取得部Ｂ１８１は、定期的にユーザのログイン状況を問い合わせるメッセージを認証サーバＥ１に送信し、ユーザのログイン状況に変化があるか否かを確認する。ユーザのログイン状況に変化がある場合には、認証サーバＥ１に対して、ユーザのログイン状況を示す情報とユーザ属性情報の送信を要求する。

【０１２２】

第２の方法の更に具体的な例としては、ＮＦＳ（Ｎｅｔｗｏｒｋ　Ｆｉｌｅ　Ｓｙｓｔｅｍ）機能を用いる方法とＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）を用いる方法が挙げられる。ＮＦＳは、ＴＣＰ／ＩＰ環境で一

般的に使用されるネットワーク経由のファイルサービスであり、ネットワークで接続されている他のノードが保持するファイルを、自ノード上にマウントすることにより、あたかもローカルファイルのように扱えるようにする機能を持つ。ＮＦＳ機能を用いる方法では、ユーザ情報管理部Ｂ１８が、認証サーバＥ１が保持するユーザのログイン状況とユーザ属性情報を含むログファイルを、マウントする。認証情報取得部Ｂ１８１は、自ノード上にマウントされているログファイルを定期的にチェックすることにより、ユーザのログイン状況の変化を検出する。ユーザのログイン状況の変化を検出した場合は、マウントされているログファイルから、ログイン状況が変化したユーザ属性情報を取得する。

【０１２３】

一方、ＳＮＭＰはＴＣＰ／ＩＰネットワーク環境で、他のノードの管理及び監視を行うためのプロトコルである。管理する側の「ＳＮＭＰマネージャ」と管理される側の「ＳＮＭＰエージェント」の２つでＭＩＢ（Ｍａｎａｇｅｍｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｂａｓｅ）と呼ばれる管理情報を交換することで、他のノードの管理が行なわれる。ＳＮＭＰを用いる方法では、認証情報取得部Ｂ１８１がＳＮＭＰマネージャとなり、認証サーバＥ１をＳＮＭＰエージェントとして、認証サーバＥ１のＭＩＢのうち、ユーザのログイン状況を示す部分を定期的にチェックする。ユーザのログイン状況の変化を検出した場合は、認証サーバＥ１のＭＩＢから、ログイン状況が変化したユーザ属性情報に該当する部分を取得する。

【０１２４】

ユーザ情報更新部Ｂ１８２は、認証情報取得部Ｂ１８２から渡された情報を基に、ユーザ情報データベースＢ１４の管理を行う。例えば、本システムにログインしたユーザのユーザ属性情報をユーザ情報データベースＢ１４に追加したり、逆にログアウトしたユーザのユーザ属性情報をユーザ情報データベースＢ１４から削除したりする。

【０１２５】

次に、第２の実施の形態の動作を図面を参照して詳細に説明する。なお、ＤＮＳサーバＢ１がクライアントＡ１からＤＮＳクエリメッセージを受信してからＤＮＳ応答メッセージを送信するまでの動作は、図４で示した第１の実施の形態における動作と同一のため説明は省略する。以下、図１２を参照して、ユーザ情報管理部Ｂ１８における、ユーザ情報データベースＢ１４の管理について詳細に説明する。

【０１２６】

認証情報取得部Ｂ１８１は、ユーザのログイン状況の変化を検出すると（図１２のステップＳ２０１）、当該ログイン状況の変化がユーザのログインかログアウトかを判断する（ステップＳ２０２）。

【０１２７】

ユーザがシステムへログインした場合は、認証サーバＥ１からユーザのログイン状況を示す情報とユーザ属性情報を取得し、これらの情報をユーザ情報更新部Ｂ１８２に渡す（ステップＳ２０３）。ユーザ情報更新部Ｂ１８２は、ユーザのログイン状況を示す情報を調査し、ユーザ属性情報をユーザ情報データベースＢ１４に追加登録する（ステップＳ２０４）。

【０１２８】

ステップＳ２０２で、ユーザがシステムからログアウトした場合は、認証情報取得部Ｂ１８１が認証サーバＥ１からユーザのログイン状況を示す情報とユーザ属性情報を取得し、これらの情報をユーザ情報更新部Ｂ１８２に渡し（ステップＳ２０５）、ユーザ情報更新部Ｂ１８２がユーザ属性情報を元にユーザ情報データベースＢ１４からユーザに該当するエントリを検索し、そのエントリを削除する（ステップＳ２０６）。

【０１２９】

以上の第２の実施の形態の説明において、ＤＮＳサーバＢ１はユーザ情報データベースＢ１４をその構成要素として含むものであった。他の構成として、第１の実施の形態と同様に、ユーザ情報データベースＢ１４がＤＮＳサーバＢ１内ではなく別のサーバ内に保持される形態も考えられる。この場合の構成を第２の実施の形態の他例として図１３に示す

。
【０１３０】
図１３に示す構成では、先に示した図９の構成と比べ、先に示したＤＮＳサーバＢ３の代わりに、ユーザ情報データベースＢ１４を含まないＤＮＳサーバＢ４が用いられ、さらに、ユーザ情報データベースＤ１１をその構成要素として含むデータベースサーバＤ１が用いられている。
【０１３１】
なお、図１３に示す構成において、従来のＤＮＳサーバまたは本発明におけるＤＮＳサーバＢ１、Ｂ２、Ｂ３、Ｂ４（後述する第３の実施の形態におけるＤＮＳサーバＢ５も含む）をデータベースサーバＤ１の用途として用いてもよい。この場合、ＤＮＳサーバにおける応答用データベースＢ１６がユーザ情報データベースＤ１１として用いられる。
【０１３２】
また、この場合、ユーザ情報更新部Ｂ１８２がユーザ情報データベースＤ１１に対してユーザ属性情報を更新する方法として、ＤＮＳ　Ｄｙｎａｍｉｃ　Ｕｐｄａｔｅを用いる方法が考えられる。ＤＮＳ　Ｄｙｎａｍｉｃ　Ｕｐｄａｔｅとは、ＤＮＳサーバが保持するデータベースに対して、エントリの追加及び削除を他のノードから行うための方式である。ＤＮＳ　Ｄｙｎａｍｉｃ　Ｕｐｄａｔｅを行うノードは、追加または削除を行う情報をＤＮＳで規定されている資源レコードの形式にエンコードし、これを埋め込んだメッセージをＤＮＳサーバに送信する。ＤＮＳサーバはメッセージを受信すると、保持する応答用データベースに対してエントリの追加または削除を行う。
【０１３３】
ＤＮＳ　Ｄｙｎａｍｉｃ　Ｕｐｄａｔｅを用いる方法では、ユーザ情報更新部Ｂ１８２が、認証情報取得部Ｂ１８１から渡されたユーザ属性情報をＤＮＳの資源レコードにエンコードし、これを埋め込んだメッセージをＤＮＳサーバに送信する。ＤＮＳサーバは、メッセージを受信すると、応答用データベース（ユーザ情報データベースＤ１１に対応）に対して、メッセージに埋め込まれた資源レコードに該当するエントリを追加または削除する。作成される応答用データベース内のエントリの例として、図８に示したゾーンファイル３０２が挙げられる。
【０１３４】
図１３に示す構成におけるＤＮＳサーバＢ４の動作については、上述したＤＮＳサーバＢ３の動作において、ユーザ情報データベースＢ１４をユーザ情報データベースＤ１１と置き換えることにより、同様に考えることができる。
【０１３５】
次に、第２の実施の形態の効果について説明する。
【０１３６】
ＤＮＳサーバが名前解決をカスタマイズするために必要なユーザ属性情報を取得して管理するにあたって、該属性情報を人的に管理するのは非常に手間とコストがかかることになる。
【０１３７】
例えば、ＩＳＰ(Internet Service Provider)網には膨大な数のユーザが存在し、さらに個々のユーザの属性情報（位置、ＩＰアドレス、接続回線種別など）は動的に変化するため、これを人的に管理するのは極めて困難となる。
【０１３８】
本実施の形態では、ユーザ情報管理部Ｂ１８が、認証サーバＥ１と連携することにより、ユーザ情報データベースＢ１４の管理を行う。ユーザ情報データベースＢ１４に対するユーザ属性情報の登録及び削除が、ユーザ情報管理部Ｂ１８により自動的に行われる。このため、ユーザ情報データベースＢ１４の設定管理（ユーザ属性情報の登録及び削除）に要する手間やコストを第１の実施の形態と比較して低減することができる。
【０１３９】
また、本実施の形態では、認証情報取得部Ｂ１８１は認証サーバＥ１からユーザ情報を

取得するが、ユーザ情報の取得にあたり、認証サーバに特別な機能を必要とならない。ユーザ情報を取得する方法として、上記ではＲＡＤＩＵＳサーバのＰｒｏｘｙ機能またはＲｅｌａｙ機能を用いる方法、ＮＦＳを用いる方法及びＳＮＭＰを用いる方法を例として示したが、これらの機能は標準化またはデファクト化された機能であり、今日利用されている多くの認証サーバにおいて設定変更を行うのみで利用可能な機能である。したがって本システムを既存のシステムに導入する際、新たな認証サーバを設置したり、既存の認証サーバを専用の認証サーバに置き換えたりするなどの導入コストが必要ない。また、本システム導入後も、同一の認証サーバで認証処理やログの収集が行われるため、既存のシステムにおける認証処理や課金処理などの運用形態を変更するためのコストが発生しない。

【０１４０】

次に、本発明の第３の実施の形態について図面を参照して詳細に説明する。

【０１４１】

図１４を参照すると、本発明の第３の実施の形態は、図９の第２の実施の形態で示されたクライアントＡ１と認証サーバＥ１に加え、ＤＮＳサーバＢ５とパケット転送装置Ｆ１とを備えて実現される。ＤＮＳサーバＢ５と認証サーバＥ１とパケット転送装置Ｆ１は、ネットワークＣ１によって相互接続される。クライアントＡ１がネットワークＣ１側と送受信するパケットは、必ずパケット転送装置Ｅ１を経由する。ここでパケット転送装置とは、イーサネット(登録商標)スイッチ、ＡＴＭスイッチ、ルータ、レイヤ４スイッチ、レイヤ７スイッチなど、パケットの転送処理機能をもつ装置全般を指す。

【０１４２】

ＤＮＳサーバＢ５は、図１に示した第１の実施の形態におけるＤＮＳサーバＢ１の構成と比べ、ユーザ情報取得部Ｂ１３およびユーザ情報データベースＢ１４をその構成要素として必要としない点が異なる。以下、ＤＮＳサーバＢ５を含む構成について説明するが、ＤＮＳサーバＢ５の代わりに第１、第２の実施の形態で示したＤＮＳサーバＢ１、Ｂ２、Ｂ３、Ｂ４のいずれかを用いてもよい。

【０１４３】

また、応答用データベースＢ１６において登録される内容例を図１５に示す。この応答用データベースＢ１６には、名前解決テーブル４０１、ゾーンファイル４０２、４０３が含まれている。名前解決テーブル４０１およびゾーンファイル４０２（または４０３）はそれぞれ、本発明の第１の実施の形態において説明した図３における名前解決テーブル２０１およびゾーンファイル２０２（または２０３）に対応するものである。

【０１４４】

ここで、第３の実施の形態では、ユーザ属性情報として、第１、第２の実施の形態で述べたユーザ属性情報の例に加えて、パケット転送装置に関する属性情報を含めて取り扱うものとする。すなわち、名前解決テーブル４０１は、名前解決テーブル２０１と比べ、ユーザ属性情報として、ユーザＩＤや接続回線種別といった属性情報だけではなく、パケット転送装置Ｆ１に関する属性情報を含み、このパケット転送装置Ｆ１に関する属性情報毎にも名前解決方法の参照先が登録できる点が異なる。ここで、パケット転送装置Ｆ１に関する属性情報の例として、パケット転送装置Ｆ１の識別子（ＩＤ）、パケット転送装置Ｆ１がサポートする転送方法（例として、イーサネット(登録商標)のｖｌａｎをサポートするか、ＵＲＬベースのスイッチングをサポートするか、など）などの情報が挙げられる。

【０１４５】

図１５に示す名前解決テーブル４０１では、ユーザ属性として、ユーザＩＤ、接続回線種別、グループＩＤといった属性情報だけではなく、パケット転送装置ＩＤを含み、このパケット転送装置ＩＤ毎にも名前解決方法の参照先が登録できるようになっている。また、ゾーンファイル４０２（または４０３）は、ゾーンファイル２０２（または２０３）で示したフィールド（Ｔｙｐｅ，ＦＱＤＮ，Ｄａｔａ）に加え、各エントリにおける付加的な情報を格納するフィールド（Ａｄｄｉｔｉｏｎａｌ　Ｄａｔａ）をもつ点が異なる。

【０１４６】

本実施の形態では、この付加的な情報を格納するフィールドを、パケット転送装置Ｆ１

におけるパケットに対する転送方法を格納するために用いる。パケットに対する転送方法の例として、該パケットを転送する優先度（パケット転送優先度）、該パケットが転送されるべき論理ネットワーク（ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）、ｖｌａｎなど）のＩＤ（論理ネットワークＩＤ）、該パケットが転送される論理チャネル（ＡＴＭのＶＣＩ（Ｖｉｒｔｕａｌ　Ｃｈａｎｎｅｌ　Ｉｄｅｎｔｉｆｉｅｒ）、ＭＰＬＳ（ＭｕｌｔｉＰｒｏｔｏｃｏｌ　Ｌａｂｅｌ　Ｓｗｉｔｃｈｉｎｇ）のＬＳＰ（Ｌａｂｅｌ　Ｓｗｉｔｃｈｅｄ　Ｐａｔｈ）など）のＩＤ、該パケットのヘッダに対する書き換え・追加・削除の方法、などが挙げられる。

【０１４７】

ゾーンファイル４０２における１番目のエントリでは、ｗｗｗ．ｄｄｄ．ｃｏｍに対するＡレコードの応答は「２０．１．１．１」であり、さらに、クライアントＡ１が該エントリを参照した結果送信する、宛先ＩＰアドレスが「２０．１．１．１」であるパケットに対して、パケット転送装置Ｆ１において、ソースＩＰアドレス（ＳｒｃＩＰＡｄｄｒ）を「４０．１．１．１」に書換え、ＭＡＣヘッダ内のｖｌａｎ－ＩＤ（ｖｌａｎＩＤ）を「１１１」に書換え、出力ポート２１から、通常の転送優先度（ｐｒｉｏｒｉｔｙ）で転送するという転送方法を用いるということを示している。

【０１４８】

応答作成部Ｂ１５は、ＤＮＳクエリメッセージに対するＤＮＳ応答メッセージを作成するときに、参照される応答用データベースＢ１６内のエントリにおいてＡｄｄｉｔｉｏｎａｌ　Ｄａｔａフィールドが登録されている場合は、作成されるＤＮＳ応答メッセージ内に、Ａｄｄｉｔｉｏｎａｌ　Ｄａｔａに記されている内容を格納する。この格納方法として、先に述べたＤＮＳメッセージにおける付加情報部にＡｄｄｉｔｉｏｎａｌ　Ｄａｔａに記されている内容を格納するなどの方法が挙げられる。

【０１４９】

ＤＮＳ応答メッセージにおける付加情報部にＡｄｄｉｔｉｏｎａｌ　Ｄａｔａに記されている内容を格納することにより、該応答メッセージは、クライアントＡ１から問合わせされたＦＱＤＮに対するＩＰアドレス（またはその他のリソースレコードデータ）だけではなく、パケット転送装置Ｆ１におけるクライアントＡ１から該ＩＰアドレス宛てに送信されたパケットに対する転送方法も同時に含むことができる。

【０１５０】

パケット転送装置Ｆ１は、ユーザ認証部Ｆ１１と、ユーザ情報更新部Ｆ１２と、ユーザ情報データベースＦ１３と、ユーザ情報取得部Ｆ１４と、ＤＮＳプロキシ部Ｆ１５と、ルーティングテーブルＦ１６と、フォワーディング部Ｆ１７とを含む。

【０１５１】

ユーザ認証部Ｆ１１は、パケット転送装置Ｆ１に対して接続するクライアントＡ１におけるユーザを識別、認証する機能を有する。さらに、認証時に得られたユーザのさまざまなユーザ属性情報を、ユーザ情報更新部Ｆ１２を介してユーザ情報データベースＦ１３に格納する。パケット転送装置Ｆ１においてユーザ認証を行う代表的な例として、イーサネット(登録商標)スイッチにおいて標準化されているユーザ認証機構であるＩＥＥＥ　８０２．１ｘが挙げられる。

【０１５２】

パケット転送装置Ｆ１がＩＥＥＥ　８０２．１ｘをサポートする場合、クライアントＡ１上のユーザのユーザＩＤ、パスワードなどの情報を基にして、ユーザ認証部Ｆ１１が認証サーバＣ１とＲＡＤＩＵＳプロトコルを用いて通信を行って認証を行うことにより、クライアントＡ１がネットワークＣ１側と通信することを許可すべきかどうか判定する。

【０１５３】

ユーザ情報更新部Ｆ１２は、ユーザ認証部Ｆ１１から渡された情報を基に、ユーザ情報データベースＦ１３の管理を行う。例えば、パケット転送装置Ｆ１にログインして通信を行うユーザのユーザ属性情報をユーザ情報データベースＦ１３に追加し、逆にログアウトしたユーザのユーザ属性情報をユーザ情報データベースＦ１３から削除するといった処理

を行なう。

【０１５４】

ユーザ情報データベースＦ１３は、ユーザ認証部Ｆ１１が認証したユーザのユーザ属性情報を格納するデータベースである。ユーザ情報データベースＦ１３に格納されるユーザ属性情報の例は、第１の実施の形態で述べたユーザ属性情報の例と同様である。ユーザ情報データベースの例を、図１６のユーザ情報データベース５０１に示す。ユーザ情報データベース５０１では、パケット転送装置Ｆ１が受信したパケットに対応する入力ポートおよびソースＭＡＣアドレスに対して、該パケットのユーザＩＤ，接続回線種類、接続回線速度、グループＩＤが記述されている。

【０１５５】

例えば、１番目のエントリでは、入力ポートが「０２」で、ソースＭＡＣアドレスが「００：１２：３４：５６：７８：９ａ」であるパケットに対しては、該パケットの送信者のユーザＩＤが「ｔａｒｏ」であり、接続している回線の種類がイーサネット(登録商標)であり、その速度が１００Ｍｂｐｓであり、該パケット送信者が含まれるグループのＩＤが「ｓｉｌｖｅｒ」であることを示している。

【０１５６】

ユーザ情報取得部Ｆ１４は、ＤＮＳプロキシ部Ｆ１５内のクエリ書換部Ｆ１５１において受信したＤＮＳクエリメッセージの送信者に対応するユーザ属性情報を、ユーザ情報データベースＦ１３から取得し、該ユーザ属性情報をクエリ書換部Ｆ１５１へ渡す機能を有する。

【０１５７】

ＤＮＳプロキシ部Ｆ１５は、クライアントＡ１とＤＮＳサーバＢ５との間に流れるＤＮＳクエリメッセージおよびＤＮＳ応答メッセージに対してその内容を読み込んで解析し、メッセージの内容を書きかえて送信する機能を有する。ＤＮＳプロキシ部Ｆ１５は、その構成要素として、クエリ書換部Ｆ１５１と応答解析部Ｆ１５２とを含む。

【０１５８】

クエリ書換部Ｆ１５１は、クライアントＡ１がＤＮＳサーバＢ５へ向けて送信したＤＮＳクエリメッセージに対して、該ＤＮＳクエリメッセージを送信したユーザに関するユーザ属性情報を該ＤＮＳクエリメッセージに対して付加してＤＮＳサーバＢ５へ送信する機能を有する。この際に必要に応じてユーザ属性情報にパケット転送装置Ｆ１に関する属性情報を含めることができる。ここで、該ＤＮＳクエリメッセージを送信したユーザに関するユーザ属性情報は、ユーザ情報取得部Ｆ１４を介してユーザ情報データベースＦ１３から取得され、必要に応じてパケット転送装置F1に関する属性情報が付加される。

【０１５９】

応答解析部Ｆ１５２は、ＤＮＳサーバＢ５がクライアントＡ１へ向けて送信したＤＮＳ応答メッセージから、該メッセージ内に埋めこまれたパケット転送方法を抽出する機能を有する。さらに、抽出したパケット転送方法に対応するエントリをルーティングテーブルＦ１６に登録する。

【０１６０】

ルーティングテーブルＦ１６は、フォワーディング部Ｆ１７が受信したパケットの転送方法が格納されたデータベースである。ルーティングテーブルＦ１６が示すテーブルの例として、ルータにおける受信パケットの転送方法が格納されたテーブル、イーサネット(登録商標)スイッチにおけるスイッチング方法が格納されたテーブル、などが挙げられる。ルーティングテーブルＦ１６内のエントリは、従来のように、静的に設定されたりあるいはルーティングプロトコルによって動的に得られた情報を基に作成される方法の他に、応答解析部Ｆ１５２によって作成されることも可能である。

【０１６１】

ルーティングテーブルＦ１６の内容例を図１７に示す。ルーティングテーブルＦ１６における２番目のエントリでは、パケット転送装置Ｆ１が受信したパケットの入力ポート、ソースＭＡＣアドレス、宛先ＩＰアドレス、ｖｌａｎ－ＩＤがそれぞれ「１１」、「００

：ｂｃ：ｄｅ：ｆ０：１２：３４」、「６０．１．１．１」、「２００」である場合に、該パケットに対して、ソースＩＰアドレス、宛先ＩＰアドレス、ｖｌａｎ－ＩＤをそれぞれ、「４０．１．１．１」、「９０．１．１．１」、「３３３」に書換え、出力ポート「３１」から送信するということを示している。さらに、優先度が「優先」となっており、パケット転送の優先度を高くして送信することを示している。

【０１６２】

フォワーディング部Ｆ１７は、パケット転送装置Ｆ１が受信したパケットの転送方法を解決し、該転送方法に基づいて該パケットを転送する機能を有する。ここで受信したパケットの転送方法は、ルーティングテーブルＦ１６を参照することにより解決される。

【０１６３】

次に、本実施の形態において、クライアントＡ１がＤＮＳクエリメッセージをＤＮＳサーバＢ５に対して送信し、対応するＤＮＳ応答メッセージがクライアントＡ１へ返されるまでのパケット転送装置Ｆ１およびＤＮＳサーバＢ５の動作を図面を参照して詳細に説明する。

【０１６４】

まず、クライアントＡ１がＤＮＳサーバＢ５へＤＮＳクエリメッセージを送信した際のパケット転送装置Ｆ１における動作を図１８のフローチャートを参照して説明する。

【０１６５】

クライアントＡ１がＤＮＳクエリメッセージをネットワークＣ１側へ送信すると、パケット転送装置Ｆ１は該メッセージを検出し、該メッセージを受信する。パケット転送装置Ｆ１によって受信されたＤＮＳクエリメッセージは、ＤＮＳプロキシ部Ｆ１５内のクエリ書換部Ｆ１５１へと渡される（図１８のステップＳ３０１）。

【０１６６】

ここで、該メッセージには、宛先ＩＰアドレスとしてＤＮＳサーバＢ５のＩＰアドレスが指定されているため、該メッセージだけを通常のパケットと同様に転送せずにクエリ書換部Ｆ１５１へ渡す方法が必要となる。この方法として、ＤＮＳクエリメッセージであることを示す特定のポート番号をもつパケットだけをクエリ書換部Ｆ１５１へ渡す（一般的にＤＮＳクエリメッセージは宛先ポート番号５３番であるパケットであることを基に識別できる）、などの方法がある。

【０１６７】

次に、クエリ書換部Ｆ１５１において、受信したＤＮＳクエリメッセージの送信者のユーザ属性情報をユーザ情報データベースＦ１３を参照することにより検索する（ステップＳ３０２）。

【０１６８】

例えば、ユーザ情報データベースＦ１３が、図１６に示したユーザ情報データベース５０１と同じエントリを格納しているとすると、ポート１１から受信し、ソースＭＡＣアドレスが「００：ｂｃ：ｄｅ：ｆ０：１２：３４」であるＤＮＳクエリメッセージは、ユーザ情報データベースＦ１３を参照することにより、送信者のユーザＩＤが「ｈａｎａｋｏ」であり、接続回線の種類がイーサネット(登録商標)であり、接続回線の速度が１０Ｍｂｐｓ等のユーザ属性情報が検索される。グループＩＤの項目は「－」となっており、グループＩＤが不明であるか、あるいは取得する必要のない属性であることを示している。

【０１６９】

ステップＳ３０２におけるユーザ属性情報の検索の結果、受信したＤＮＳクエリメッセージの送信者に対応するユーザ属性情報が存在する場合、クエリ書換部Ｆ１５１で対応するユーザ属性情報を該ＤＮＳクエリメッセージに付加し、該メッセージをＤＮＳサーバＢ５へ送信する（ステップＳ３０３、Ｓ３０４）。

【０１７０】

ステップＳ３０４において、ユーザ情報データベースＦ１３を参照して解決したユーザ属性情報の他、ユーザ属性情報としてパケット転送装置Ｆ１に関する属性情報を該ＤＮＳクエリメッセージに対して付加する必要があれば、パケット転送装置Ｆ１に関する属性情

報も該メッセージに付加し、ＤＮＳサーバＢ５へ送信する。例えば、ユーザ情報データベースＦ１３を参照して解決したユーザ属性情報の他に、パケット転送装置Ｆ１のＩＤを該メッセージに対して付加する。

【０１７１】

ステップＳ３０２におけるユーザ属性情報の検索の結果、受信したＤＮＳクエリメッセージの送信者に対応するユーザ属性情報が存在しなかった場合、クエリ書換部Ｆ１３１は該メッセージに対しては何も情報を付加することなくそのままＤＮＳサーバＢ５へ送信する（ステップＳ３０３、Ｓ３０５）。

【０１７２】

次に、ＤＮＳサーバＢ５がパケット転送装置Ｆ１を経由してＤＮＳクエリメッセージを受信した際のＤＮＳサーバＢ５における動作について図１９を参照して説明する。

【０１７３】

まず、クエリ受信部Ｂ１１がＤＮＳクエリメッセージを受信すると（図１９のステップＳ４０１）、該メッセージをユーザ情報識別部Ｂ１２へ渡す。

【０１７４】

ユーザ情報識別部Ｂ１２は、受け取ったＤＮＳクエリメッセージ内に、送信者のユーザ属性情報が埋めこまれているかどうかを識別する（ステップＳ４０２）。

【０１７５】

ステップＳ４０２の結果、該メッセージ内に、送信者のユーザ属性情報が埋めこまれている場合は、埋めこまれている送信者のユーザ属性情報を読み出し識別し、識別したユーザ属性情報と一緒に該メッセージを応答作成部Ｂ１５へ渡す（ステップＳ４０３）。

【０１７６】

ステップＳ４０２の結果、該メッセージ内に、送信者のユーザ属性情報が埋めこまれていない場合は、該メッセージに対応する送信者のユーザ属性情報はないものとして該メッセージを応答作成部Ｂ１５へ渡す。

【０１７７】

ステップＳ４０２、Ｓ４０３の後、ステップＳ４０４～ステップＳ４０８の動作については、第１の実施の形態において説明した図４のステップＳ１０３～ステップＳ１０７と同様である。

【０１７８】

また、ステップＳ４０８では、応答作成部Ｂ１５が作成したＤＮＳ応答メッセージにおいて、パケット転送装置Ｆ１におけるパケット転送方法も同時に付加されている場合、応答送信部Ｂ１７はパケット転送装置Ｆ１におけるパケット転送方法を含むＤＮＳ応答メッセージをクライアントＡ１に対して送信する。

【０１７９】

次に、パケット転送装置Ｆ１がＤＮＳサーバＢ５からＤＮＳ応答メッセージを受信したときの動作を図２０のフローチャートを参照して説明する。

【０１８０】

ＤＮＳサーバＢ５がＤＮＳ応答メッセージをクライアントＡ１へ送信すると、パケット転送装置Ｆ１は該メッセージを検出し、該メッセージを受信する。パケット転送装置Ｆ１によって受信されたＤＮＳ応答メッセージは、ＤＮＳプロキシ部Ｆ１５内の応答解析部Ｆ１５２へと渡される（図２０のステップＳ５０１）。

【０１８１】

ここで、該メッセージには、宛先ＩＰアドレスとしてクライアントＡ１のアドレスが指定されているため、該メッセージだけを通常のパケットと同様に転送せずに応答解析部Ｆ１５２へ渡す方法が必要となるが、この方法に関しては、図１８のステップＳ３０１の動作の説明で述べた方法と同様に考えられる（ＤＮＳ応答メッセージはソースポート番号５３番であるパケットであることを基に識別できる）。

【０１８２】

次に、応答解析部Ｆ１５２は、受信したＤＮＳ応答メッセージの内容を調べ、該メッセ

ージにパケット転送装置Ｆ１におけるパケット転送方法が埋めこまれているかどうかを調べる（ステップＳ５０２）。

【０１８３】

ステップＳ５０２の結果、パケット転送方法が埋めこまれている場合、応答解析部Ｆ１５２は埋めこまれたパケット転送方法を読み出す（ステップＳ５０３）。以下、ＤＮＳサーバＢ５において、図１５に示したゾーンファイル４０２における１番目のエントリを用いてＤＮＳ応答メッセージが作成され、該メッセージがＤＮＳサーバＢ５からクライアントＡ１へ送信された場合について説明する。

【０１８４】

次に、応答解析部Ｆ１３２はルーティングテーブルＦ１６内に登録されているエントリを参照し、受信したＤＮＳ応答メッセージ内に埋めこまれたパケット転送方法から作成されるエントリと同一のエントリが存在するかどうか調べる（ステップＳ５０４、Ｓ５０５）。

【０１８５】

ステップＳ５０５の結果、同一の転送方法を示すエントリが存在しない場合、応答解析部Ｆ１５２は、ルーティングテーブルＦ１６に対して、受信したＤＮＳ応答メッセージ内に埋めこまれたパケット転送方法に対応するエントリを作成する（ステップＳ５０６）。

【０１８６】

ここで、ルーティングテーブルＦ１６に対してパケット転送方法を示すエントリを作成する例を示す。ＤＮＳサーバＢ５が、図１５に示した応答用データベースＢ１６におけるゾーンファイル４０２の１番目のエントリを用いてＤＮＳ応答メッセージを作成し、クライアントＡ１へ向けて送信された該メッセージをパケット転送装置Ｆ１が受信したとする。さらに、該メッセージの送信先であるクライアントＡ１のＭＡＣアドレスが「００：１２：３４：５６：７８：９ａ」であり、クライアントＡ１とパケット転送装置Ｆ１との間は、パケット転送装置Ｆ１のポート「０２」を経由し、ｖｌａｎ－ＩＤが「１００」のイーサネット(登録商標)ｖｌａｎを用いて転送されるとすると、図１７に示したルーティングテーブルＦ１６における１番目のエントリが作成される。

【０１８７】

ステップＳ５０５の結果、同一の転送方法を示すエントリが存在する場合は、重複するエントリを作成することを避けるために、ステップＳ５０６の動作はスキップする。

【０１８８】

次に、応答解析部Ｆ１５２は、受信したＤＮＳ応答メッセージ内に埋めこまれたパケット転送方法を該メッセージから削除し（ステップＳ５０７）、該メッセージをクライアントＡ１に対して転送する（ステップＳ５０８）。

【０１８９】

ステップＳ５０２の結果、パケット転送方法が埋めこまれていない場合は、応答解析部Ｆ１５２は、受信したＤＮＳ応答メッセージをそのままクライアントＡ１に対して転送する（ステップＳ５０８）。

【０１９０】

以上で図１４を用いて説明した本実施の形態において、パケット転送装置Ｆ１内のユーザ情報データベースＦ１３は、ユーザ認証部Ｆ１１と認証サーバＥ１との間での認証時に得られたユーザ属性情報をユーザ認証部Ｆ１１がユーザ情報更新部Ｆ１２を介して格納することによって作成された。この他にも、パケット転送装置Ｆ１の管理者などによって、外部から手動でユーザ情報データベースＦ１３内にユーザ属性情報が書きこまれる形態も考えられる。この場合、ユーザ認証部Ｆ１１およびユーザ情報更新部Ｆ１２および認証サーバＥ１は本実施の形態における構成要素としては必要ない。

【０１９１】

また、図１４を用いて説明した第３の実施の形態において、パケット転送装置Ｆ１はユーザ情報データベースＦ１３をその構成要素として含むものであった。他の構成として、ユーザ情報データベースＦ１３がパケット転送装置Ｆ１内ではなく、他のサーバ（外部デ

ータベースなど）内に保持される形態も考えられる。この場合の構成を第３の実施の形態の他例として図２１に示す。

【０１９２】

図２１に示す構成では、先に示した図１４の構成に比べ、先に示したパケット転送装置Ｆ１に代わりに、ユーザ情報データベースＦ１３を含まないパケット転送装置Ｆ２が用いられ、さらに、第１の実施の形態の説明において図７で示したデータベースサーバＤ１が用いられる。データベースサーバＤ１の機能は、第１の実施の形態で説明したのと同様に、ＤＮＳサーバＢ１、Ｂ２あるいは Ｂ５の一機能として実現することも可能である。この場合、ユーザ情報取得部Ｆ１４はＤＮＳメッセージを用いてユーザ属性情報の取得を行う。

【０１９３】

図２１に示す構成におけるパケット転送装置Ｆ２の動作については、上述したパケット転送装置Ｆ１の動作の説明において、ユーザ情報データベースＦ１３をユーザ情報データベースＤ１１と置きかえることにより同様に考えることができる。

【０１９４】

さらに、図１４を用いて説明した本実施の形態において、パケット転送装置のＤＮＳプロキシ部Ｆ１５がクエリ書換部Ｆ１５１と応答解析部Ｆ１５２との両方を有する構成について説明したが、ＤＮＳプロキシ部Ｆ１５が、クエリ書換部Ｆ１５１または応答解析部Ｆ１５２のいずれか一方のみを有する構成も考えられる。

【０１９５】

ＤＮＳプロキシ部Ｆ１５がクエリ書換部Ｆ１５１のみを有するパケット転送装置Ｆ３の構成例を図２２に示す。この構成の場合、パケット転送装置Ｆ３は、クライアントＡ１から受信したＤＮＳクエリメッセージに対して送信者のユーザ属性情報を埋めこみ、ＤＮＳサーバＢ５へ送信する一方、ＤＮＳサーバＢ５から返されたＤＮＳ応答メッセージに対しては、そのままクライアントＡ１へ送信する。

【０１９６】

また、ＤＮＳプロキシ部Ｆ１５が応答解析部Ｆ１５２のみを有するパケット転送装置Ｆ４の構成例を図２３に示す。この構成の場合、パケット転送装置Ｆ４は、クライアントＡ１から受信したＤＮＳクエリメッセージに対してはそのままＤＮＳサーバＢ５へ送信する一方、ＤＮＳサーバＢ５から返されたＤＮＳ応答メッセージに対しては、埋めこまれたパケット転送方法を抽出し、ルーティングテーブルに対してエントリの作成を行う。

【０１９７】

次に、第３の実施の形態の効果について説明する。

【０１９８】

本実施の形態では、クライアントＡ１がＤＮＳサーバＢ５に対して送信したＤＮＳクエリメッセージを、パケット転送装置Ｆ１が途中で一旦受信し、該ＤＮＳクエリメッセージを送信したユーザに関するユーザ属性情報を該ＤＮＳクエリメッセージに埋め込む。この際に必要に応じてユーザ属性情報としてパケット転送装置Ｆ１に関する属性情報をも埋め込みＤＮＳサーバＢ５へ転送する。さらに、ＤＮＳサーバＢ５は該ＤＮＳクエリメッセージを受信すると、該ＤＮＳクエリメッセージ内に埋め込まれたユーザ属性情報を基に、ＤＮＳ応答および該応答に対応するパケット転送装置Ｆ１におけるパケット転送方法をＤＮＳ応答メッセージに埋めこみクライアントＡ１へ送信する。パケット転送装置Ｆ１は、該応答メッセージを一旦受信し、該応答メッセージ内に埋めこまれたパケット転送方法を抽出してルーティングテーブルＦ１６に対応するエントリを作成する。

【０１９９】

従来、ＤＮＳサーバからクライアントに対して送信されたＤＮＳ応答メッセージは、クライアントが利用するものであったが、本実施の形態により、クライアントだけではなく、クライアントとＤＮＳサーバ間に設置されているパケット転送装置も該ＤＮＳ応答メッセージ内に格納された情報を利用することが可能になる。

【０２００】

本実施の形態では、該ＤＮＳ応答メッセージ内に、該応答メッセージを受信した結果クライアントが送信するパケットに対するパケット転送装置Ｆ１における転送方法が埋めこまれる。これにより、例えばＷｅｂのアプリケーションの場合、クライアントＡ１に負荷の低いＷｅｂサーバに接続させると同時に、パケット転送装置Ｆ１においてクライアントＡ１と該Ｗｅｂサーバ間の接続上を通過するパケットに対して優先的に転送させる、などといった制御をＤＮＳサーバが行うことが可能になる。

【０２０１】

さらに、本発明の第１の実施の形態で述べたＤＮＳ応答のカスタマイズ機能により、パケット転送装置Ｆ１における転送方法の制御も同様にユーザ属性情報およびパケット転送装置Ｆ１に関する属性情報を基にカスタマイズすることが可能である。例えば、特権ユーザの送受信するパケットは優先的に転送したり、特権ユーザ用のｖｌａｎを用いて転送するなどの制御を行うことが可能となる。

【実施例２】

【０２０２】

次に、本発明の第１の実施例を、図面を参照して説明する。かかる実施例は本発明の第１の実施の形態に対応するものである。また、本実施例は図１に示した構成をとるものとする。実施例において、クライアントＡ１は、ＤＮＳサーバＢ１に対して名前解決を要求するユーザが利用する端末である。また、ＤＮＳサーバＢ１は図２に示した内容をユーザ情報データベースＢ１４として保持し、図３に示した名前解決テーブル２０１、ゾーンファイル２０２、２０３を応答用データベースＢ１６として保持するものとする。

【０２０３】

今、ＩＰアドレスが「１２３．４５．０．２」である端末を利用するユーザ１と、ＩＰアドレスが「１２３．４５．０．４」である端末を利用するユーザ２がＦＱＤＮ：ｗｗｗ．ａａａ．ｃｏｍの名前解決をＤＮＳサーバＢ１に要求したとする。ｗｗｗ．ａａａ．ｃｏｍは、地域情報を提供するウェブサイトのＦＱＤＮであり、かかるウェブサイトでは、アクセスしてくるユーザの位置情報（接続しているＮＡＳのＩＰアドレス）とネットワークへの接続回線種別を考慮し、これらのユーザ属性情報に適したウェブページを表示するサービスが提供されているものとする。

【０２０４】

具体的に川崎市からネットワーク接続しているユーザ（以下では、ＩＰアドレスが「３０．３０．３０．３０」のＮＡＳに接続しているユーザが川崎市からネットワーク接続しているユーザであるものとする）には、川崎市の地域情報が提供され、横浜市からネットワーク接続しているユーザ（以下では、ＩＰアドレスが「２０．２０．２０．２０」のＮＡＳに接続しているユーザが横浜市からネットワーク接続しているユーザであるものとする）には、横浜市の地域情報が提供される。

【０２０５】

また、ＡＤＳＬ回線で接続しているユーザには、地域情報が、広帯域アクセスに適したマルチメディアコンテンツを主とするウェブページにより表示され、逆にＩＳＤＮ回線でネットワークに接続しているユーザに対しては、狭帯域アクセスに適したテキストベースのコンテンツを主とするウェブページにより表示される。これらのウェブページは異なるウェブサーバにホスティングされているものとし、以下では、川崎市からＡＤＳＬ回線によりネットワーク接続しているユーザ向けのウェブページはＩＰアドレス「９．８．７．６」のウェブサーバにホスティングされており、また、横浜市からＩＳＤＮ回線によりネットワーク接続しているユーザ向けのウェブページはＩＰアドレス「９．８．７．３」のウェブサーバにホスティングされているものとする。

【０２０６】

まず、ユーザ１及びユーザ２はそれぞれの利用端末を通じてＤＮＳサーバＢ１にＤＮＳクエリメッセージを送信する。ＤＮＳサーバＢ１のクエリ受信部Ｂ１１は、受信したＤＮＳクエリメッセージをユーザ情報識別部Ｂ１２に渡す。ＤＮＳクエリメッセージには、ユーザ属性情報が埋め込まれていないため、ユーザ情報識別部Ｂ１２は、ＤＮＳクエリメッ

セージをユーザ情報取得部Ｂ１３に渡す。ユーザ情報取得部Ｂ１３は、まず受け取ったＤＮＳクエリメッセージのソースＩＰアドレスを調査する。この場合、ユーザ１の送信したＤＮＳクエリメッセージのソースＩＰアドレスは「１２３．４５．０．２」であり、ユーザ２の送信したＤＮＳクエリメッセージのソースＩＰアドレスは「１２３．４５．０．４」である。

【０２０７】

次にソースＩＰアドレスを元に、ユーザ情報データベースＢ１４からユーザ１及びユーザ２に該当するエントリを検索する。この場合、ユーザ１に該当するエントリは、図２に示したユーザ情報データベースＢ１４の１番目のエントリであり、ユーザ１の属性情報として、ログインＩＤが「ｔａｒｏ」、接続回線種別がＡＤＳＬ回線、接続しているＮＡＳのＩＰアドレスが「３０．３０．３０．３０」であるという情報が得られる。

【０２０８】

また、ユーザ２に該当するエントリは、ユーザ情報データベースＢ１４の２番目のエントリであり、ユーザ２の属性情報として、ログインＩＤがｈａｎａｋｏ、ＩＰアドレスが「１２３．４５．０．４」、接続しているＮＡＳのＩＰアドレスが「２０．２０．２０．２０」であるという情報が得られる。更に、ＩＰアドレスが「８．９．１．４」であるノードを参照することで、他の属性情報が得られることが分かる。ここでは、ユーザ情報取得部Ｂ１３が、ＩＰアドレス「８．９．１．４」のノードを参照し、ユーザ２の属性情報として更に接続回線種別がＩＳＤＮ回線であるという情報を得られたとする。

【０２０９】

ユーザ情報取得部Ｂ１３は、上記のようにして得られたユーザ１及びユーザ２の属性情報を、ユーザ情報識別部Ｂ１２に渡し、さらに、ユーザ情報識別部Ｂ１２は、ユーザ１及びユーザ２の属性情報と、クエリ受信部Ｂ１１から渡されたユーザ１及びユーザ２が送信したＤＮＳクエリメッセージを応答作成部Ｂ１５に渡す。応答作成部Ｂ１５は、ユーザ属性情報及び問い合わせのあったＦＱＤＮに該当するエントリを応答用データベースＢ１６から検索する。

【０２１０】

この場合、ユーザ１からのＤＮＳクエリに該当するエントリとして、図３に示した名前解決テーブル２０１の１番目のエントリが発見され、さらに、名前解決方法として、ゾーンファイル２０２の１番目のエントリが発見される。この結果、ユーザ１のＦＱＤＮ：ｗｗｗ．ａａａ．ｃｏｍに対するＤＮＳクエリに対しては、ＩＰアドレス「９．８．７．６」が名前解決される。

【０２１１】

また、ユーザ２のＤＮＳクエリメッセージに該当するエントリとして、名前解決テーブル２０１の２番目のエントリが発見され、さらに、名前解決方法として、ゾーンファイル２０３の１番目のエントリが発見される。この結果、ユーザ２のＦＱＤＮ：ｗｗｗ．ａａａ．ｃｏｍに対するＤＮＳクエリに対しては、ＩＰアドレス「９．８．７．３」が名前解決される。

【０２１２】

応答作成部Ｂ１７は名前解決結果を応答送信部Ｂ１７に渡す。応答送信部Ｂ１７は、受け取った名前解決結果をＤＮＳ応答メッセージの中に埋め込み、ユーザ１及びユーザ２に送信する。

【０２１３】

ユーザ１は、ＤＮＳサーバＢ１からＤＮＳ応答メッセージを受信すると、ＩＰアドレスが「９．８．７．６」のウェブサーバにアクセスすることになる。前述した通り、ＩＰアドレスが「９．８．７．６」のウェブサーバには、川崎市からＡＤＳＬ回線によりネットワーク接続しているユーザに適したウェブページがホスティングされており、ユーザ１にはユーザ１の属性に適したウェブページが表示されることになる。

【０２１４】

また、ユーザ２も同様に、ＤＮＳサーバＢ１からＤＮＳ応答メッセージを受信すると、

ＩＰアドレスが「９．８．７．３」のウェブサーバにアクセスすることになる。前述した通り、ＩＰアドレスが「９．８．７．３」のウェブサーバには、横浜市からＩＳＤＮ回線によりネットワーク接続しているユーザに適したウェブページがホスティングされており、ユーザ２にはユーザ２の属性に適したウェブページが表示されることになる。

【０２１５】

次に第２の実施例を、図面を参照して説明する。かかる実施例は、第２の実施の形態に対応するものである。また、本実施例は図９に示した構成をとるものとする。本実施例において、認証サーバＥ１はＲＡＤＩＵＳサーバであり、ＩＳＰが運営しているネットワークにログインするユーザのユーザ認証および課金処理に利用されているものとする。また、クライアントＡ１は、上記ＩＳＰが運営するネットワークにログインするユーザの利用端末であり、このユーザはクライアントＡ１を利用してＤＮＳサーバＢ３に対して名前解決を要求するものとする。

【０２１６】

今、ユーザがＩＳＰの運営するネットワークにログインしたとする。図９に示すようにユーザがログインすると、認証サーバＥ１はＲＡＤＩＵＳクライアントからＡｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージを受信し、Ｐｒｏｘｙ機能を利用して受信したＡｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージをを転送する。ここで、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージには、図９に示すように、ユーザ属性情報として、ユーザのログインＩＤがｔａｒｏ、接続しているＮＡＳのＩＰアドレスが３０．３０．３０．３０、ユーザの利用端末（クライアントＡ１）のＩＰアドレスが１２３．４５．０．２、接続性回線種別がＡＤＳＬ回線であることが記載されており、またユーザがネットワークにログインした旨が記載されているものとする。

【０２１７】

ユーザ情報管理部Ｂ１８の認証情報取得部Ｂ１８１は、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージを受信すると、これをユーザ情報管理部Ｂ１８２に渡す。この場合、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージには、ユーザがネットワークにログインした旨が記載されているため、ユーザ情報管理部Ｂ１８２は、Ａｃｃｏｕｎｔｉｎｇ　Ｒｅｑｕｅｓｔメッセージに記載されたユーザ属性情報をユーザ情報データベースＢ１４に登録する。この結果、ユーザ情報データベースＢ１４には、例えば図２に示すユーザ情報データベースの１番目のエントリが追加される。なお、ユーザがネットワークにログイン後、ＤＮＳサーバＢ１に名前解決を要求した場合の動作は、前述した第１の実施例と同様である。

【０２１８】

次に、本発明の第３の実施例を、図面を参照して説明する。かかる実施例は本発明の第３の実施の形態に対応するものである。また、本実施例は図１４に示した構成をとるものとする。実施例において、クライアントＡ１は、ＤＮＳサーバＢ５に対して名前解決を要求するユーザが利用する端末である。また、ＤＮＳサーバＢ５は図１５に示した名前解決テーブル４０１、ゾーンファイル４０２、４０３を応答用データベースＢ１６として保持し、パケット転送装置Ｆ１はＮＡＴ（Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｔｒａｎｓｌａｔｉｏｎ）機能を有し、図１６に示す内容をユーザ情報データベースＦ１３として保持するものとする。また、パケット転送装置Ｆ１の識別子（ＩＤ）は「ｓｗｉｔｃｈ９９」であるとする。

【０２１９】

今、ＭＡＣアドレスが「００：１２：３４：５６：７８：９ａ」であり、パケット転送装置Ｆ１のポート「０２」にｖｌａｎＩＤが「１００」のｖｌａｎで接続されている端末を利用するユーザ１と、ＭＡＣアドレスが「００：ｂｃ：ｄｅ：ｆ０：１２：３４」であり、パケット転送装置Ｆ１のポート「１１」にｖｌａｎＩＤが「２００」のｖｌａｎで接続されている端末を利用するユーザ２の各々が、ｈｔｔｐ：／／ｗｗｗ．ｄｄｄ．ｃｏｍ／ｉｎｄｅｘ．ｈｔｍｌのＵＲＬをもつＷｅｂサイトにアクセスするものとする。

【０２２０】

まず、ユーザ１またはユーザ２が利用する端末に対応するクライアントＡ１は、ＦＱＤＮ：ｗｗｗ．ｄｄｄ．ｃｏｍに対するＩＰアドレスを解決すべくＤＮＳサーバＢ５にＤＮＳクエリメッセージを送信する。該ＤＮＳクエリメッセージがパケット転送装置Ｆ１を経由する際に、パケット転送装置Ｆ１では、ＤＮＳメッセージの宛先ポート番号（５３）にマッチするパケットをＤＮＳプロキシ部Ｆ１５内のクエリ書換部Ｆ１５１に渡す。クエリ書換部Ｆ１５１は、該クエリメッセージの送信者に対応するユーザ属性情報をユーザ取得部Ｆ１４を介してユーザ情報データベースＦ１３から取得する。

【０２２１】

ユーザ１の場合、ユーザ情報データベース５０１の１番目のエントリにマッチし、ユーザ２の場合、２番目のエントリにマッチする。クエリ書換部Ｆ１５１は、受信したＤＮＳクエリメッセージの付加情報部に取得したユーザ属性情報およびパケット転送装置Ｆ１のＩＤ（「ｓｗｉｔｃｈ９９」）を埋めこみ、ＤＮＳサーバＢ５へ転送する。

【０２２２】

ＤＮＳサーバＢ５は、ユーザ属性情報が埋めこまれたＤＮＳクエリメッセージを受信すると、ユーザ情報識別部Ｂ１２で該ＤＮＳクエリメッセージ内に埋めこまれたユーザ属性情報を識別し、応答作成部Ｂ１５で該ユーザ属性情報およびクエリの内容に対応するエントリを検索する。ユーザ１からのＤＮＳクエリメッセージの場合は、応答用データベースＢ１６内の名前解決テーブル４０１の１番目のエントリにマッチし、さらに名前解決方法としてゾーンファイル４０２の１番目のエントリにマッチする。

【０２２３】

この結果、ユーザ１のＦＱＤＮ：ｗｗｗ．ｄｄｄ．ｃｏｍに対するＤＮＳクエリメッセージに対して応答されるＤＮＳ応答メッセージには、ＩＰアドレス２０．１．１．１が応答部に入れられ、さらに対応するパケットに対するパケット転送装置Ｆ１における転送方法である、「ＳｒｃＩＰＡｄｄｒ＝４０．１．１．１，ｖｌａｎＩＤ＝１１１，ｏｕｔｐｏｒｔ＝２１，ｐｒｉｏｒｉｔｙ＝０」が付加情報部に入れられる。また、ユーザ２のＤＮＳクエリメッセージの場合は、名前解決テーブル４０１の３番目のエントリにマッチし、さらに名前解決方法としてゾーンファイル４０３の１番目のエントリにマッチする。

【０２２４】

この結果、ユーザ２のＦＱＤＮ：ｗｗｗ．ｄｄｄ．ｃｏｍに対するＤＮＳクエリメッセージに対して応答されるＤＮＳ応答メッセージには、ＩＰアドレス「６０．１．１．１」が応答部に入れられ、さらに対応するパケットに対するパケット転送装置Ｆ１における転送方法である、「ＳｒｃＩＰＡｄｄｒ＝４０．１．１．１，ＤｅｓｔＩＰＡｄｄｒ＝９０．１．１．１，ｖｌａｎＩＤ＝３３３，ｏｕｔｐｏｒｔ＝３１，ｐｒｉｏｒｉｔｙ＝１」が付加情報部に入れられる。応答作成部Ｂ１５で作成されたＤＮＳ応答メッセージは応答送信部Ｂ１７によってクライアントＡ１（ユーザ１またはユーザ２）へ送信される。

【０２２５】

ＤＮＳサーバＢ５からクライアントＡ１へ送信されたＤＮＳ応答メッセージは、途中でパケット転送装置Ｆ１を経由する。該応答メッセージがパケット転送装置Ｆ１を経由する際に、パケット転送装置Ｆ１では、ＤＮＳメッセージのソースポート番号（５３）にマッチするパケットをＤＮＳプロキシ部Ｆ１５内の応答解析部Ｆ１５２に渡す。応答解析部Ｆ１５２は、該応答メッセージに含まれている情報を解析し、該情報に基づいてルーティングテーブルＦ１６にエントリを作成する。

【０２２６】

ユーザ１へのＤＮＳ応答メッセージの場合、該応答メッセージの応答部および付加情報部に含まれている情報に基づいて、図１７に示す内容例の１番目のエントリがルーティングテーブルＦ１６に作成される。また、ユーザ２へのＤＮＳ応答メッセージの場合、該応答メッセージの応答部および付加情報部に含まれている情報に基づいて、図１７に示す内容例の２番目のエントリがルーティングテーブルＦ１６に作成される。

【０２２７】

応答解析部Ｆ１５２は、ルーティングテーブルＦ１６へのエントリ作成を行うと、受信

したＤＮＳ応答メッセージ内の付加情報部フィールドを削除し、クライアントＡ１へ転送する。

【０２２８】

クライアントＡ１は、送信したＤＮＳクエリメッセージに対応するＤＮＳ応答メッセージを受信すると、該応答メッセージによって応答されたｗｗｗ．ｄｄｄ．ｃｏｍのＩＰアドレスに対して、ＨＴＴＰコネクションを確立し、該コネクション上でリクエスト処理等を行う。ユーザ１の場合は、ＩＰアドレス「２０．１．１．１」に対してＨＴＴＰコネクションを確立し、ユーザ２の場合はＩＰアドレス「６０．１．１．１」に対してＨＴＴＰコネクションを確立する。これらのコネクション上を流れるパケットは全てパケット転送装置Ｆ１を通過する。

【０２２９】

この際、ユーザ１とＩＰアドレス「２０．１．１．１」との間のコネクション上を流れるパケットに関しては、図１７のルーティングテーブル６０１における１番目のエントリに基づく転送方法が適用され、ユーザ２とＩＰアドレス「６０．１．１．１」との間のコネクション上を流れるパケットに関しては、ルーティングテーブルＦ１６における２番目のエントリに基づく転送方法が適用される。

【０２３０】

例えば、ユーザ１が送信したパケットは、ルーティングテーブルＦ１６において、転送優先度が「通常」となっているため、通常の転送優先度で転送が行われるが、ユーザ１が送信したパケットは、転送優先度が「優先」となっているため、通常の転送優先度で転送されるパケットと比べ優先的に転送が行われる。すなわち、ユーザ２はユーザ１と比べてスムーズなＷｅｂ接続を行えると期待される。

【０２３１】

本実施例によって、ＤＮＳサーバＢ５およびパケット転送装置Ｆ１を用いることにより、従来のＤＮＳサーバが提供するＦＱＤＮからＩＰアドレスへの解決機能だけではなく、クライアントＡ１が送信したパケットが通過するパケット転送装置Ｆ１におけるパケット転送方法も同時に制御できることが分かる。

【０２３２】

本発明のＤＮＳサーバおよびパケット転送装置は、構成要素である各装置の機能をハードウェア的に実現することは勿論として、上記した各装置の機能を実行して名前解決処理を行う名前解決プログラム（アプリケーション）をＤＮＳサーバを実現するコンピュータ処理装置のメモリにロードして実行することで実現することができる。すなわち、上述したＤＮＳサーバおよびパケット転送装置の機能をソフトウェアによって実現することができる。この名前解決プログラムプログラムは、磁気ディスク、半導体メモリその他の記録媒体に格納され、その記録媒体からコンピュータ処理部にロードされ、コンピュータ処理部の動作を制御することにより、上述した各機能を実現する。

【０２３３】

以上好ましい実施の形態及び実施例をあげて本発明を説明したが、本発明は必ずしも上記実施の形態及び実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【図面の簡単な説明】

【０２３４】

【図１】本発明の第１の実施の形態の構成を示すブロック図である。

【図２】本発明の第１の実施の形態のユーザ情報データベースの例を示す図である。

【図３】本発明の第１の実施の形態の応答用データベースの例を示す図である。

【図４】本発明の第１の実施の形態のＤＮＳサーバの動作を示すフローチャートである。

【図５】本発明の第１の実施の形態におけるＤＮＳサーバのユーザ属性情報の取得の動作を示すフローチャートである。

【図６】本発明の第１の実施の形態におけるＤＮＳサーバ内の応答作成部の構成を示すブロック図である。

【図７】本発明の第１の実施の形態においてユーザ情報データベースをデータベースサーバが保持する場合の構成を示すブロック図である。
【図８】本発明の第１の実施の形態のユーザ属性情報が登録されている応答用データベースの例を示す図である。
【図９】本発明の第２の実施の形態の構成を示すブロック図である。
【図１０】本発明の第２の実施の形態において認証サーバがＲＡＤＩＵＳサーバである場合に認証情報取得部がユーザ属性情報をＲＡＤＩＵＳプロトコルのＰｒｏｘｙ機能を利用して認証サーバから取得する際のメッセージシーケンスの例を示すシーケンス図である。
【図１１】本発明の第２の実施の形態において認証サーバがＲＡＤＩＵＳサーバである場合に認証情報取得部がユーザ属性情報をＲＡＤＩＵＳサーバのＲｅｌａｙ機能を利用して認証サーバから取得する際のメッセージシーケンスの例を示すシーケンス図である。
【図１２】本発明の第２の実施の形態におけるユーザ情報管理部の動作を示すフローチャートである。
【図１３】本発明の第２の実施の形態においてユーザ情報データベースをデータベースサーバが保持する場合の構成を示すブロック図である。
【図１４】本発明の第３の実施の形態の構成を示すブロック図である。
【図１５】本発明の第３の実施の形態の応答用データベースの例を示す図である。
【図１６】本発明の第３の実施の形態のユーザ情報データベースの例を示す図である。
【図１７】本発明の第３の実施の形態のルーティングテーブルの例を示す図である。
【図１８】本発明の第３の実施の形態においてクライアントからＤＮＳクエリメッセージを受信した際のパケット転送装置の動作を示すフローチャートである。
【図１９】本発明の第３の実施の形態のＤＮＳサーバの動作を示すフローチャートである。
【図２０】本発明の第３の実施の形態においてＤＮＳサーバからＤＮＳ応答メッセージを受信した際のパケット転送装置の動作を示すフローチャートである。
【図２１】本発明の第３の実施の形態においてユーザ情報データベースをデータベースサーバが保持する場合の構成を示すブロック図である。
【図２２】本発明の第３の実施の形態における他の構成例を示すブロック図である。
【図２３】本発明の第３の実施の形態におけるさらに他の構成例を示すブロック図である。

【符号の説明】
【０２３５】
Ａ１：クライアント
Ｂ１：ＤＮＳサーバ
Ｂ１１：クエリ受信部
Ｂ１２：ユーザ情報識別部
Ｂ１３：ユーザ情報取得部
Ｂ１４：ユーザ情報データベース
Ｂ１５：応答作成部
Ｂ１５１：応答作成メイン部
Ｂ１５２：リゾルバ部
Ｂ１６：応答用データベース
Ｂ１７：応答送信部
Ｂ１８：ユーザ情報管理部
Ｂ１８１：認証情報取得部
Ｂ１８２：ユーザ情報管理部
Ｂ２：ＤＮＳサーバ
Ｂ３：ＤＮＳサーバ
Ｂ４：ＤＮＳサーバ
Ｂ５：ＤＮＳサーバ

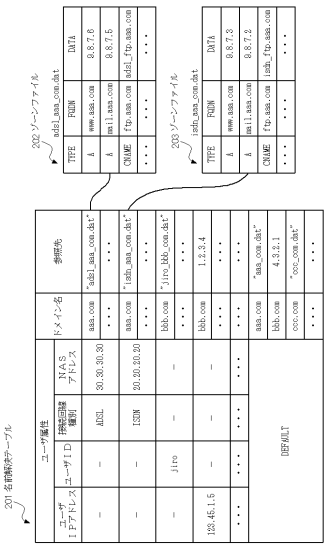
Ｃ１：ネットワーク
Ｄ１：データベースサーバ
Ｄ１１：ユーザ情報データベース
Ｅ１：認証サーバ
Ｆ１：パケット転送装置
Ｆ１１：ユーザ認証部
Ｆ１２：ユーザ情報更新部
Ｆ１３：ユーザ情報データベース
Ｆ１４：ユーザ情報取得部
Ｆ１５：ＤＮＳプロキシ部
Ｆ１５１：クエリ書換部
Ｆ１５２：応答解析部
Ｆ１６：ルーティングテーブル
Ｆ１７：フォワーディング部
Ｆ２：パケット転送装置
２０１：名前解決テーブル
２０２：ゾーンファイル
２０３：ゾーンファイル
３０１：名前解決テーブル
３０２：ゾーンファイル
４０１：名前解決テーブル
４０２：ゾーンファイル
４０３：ゾーンファイル
６０１：ルーティングテーブル

【図２】

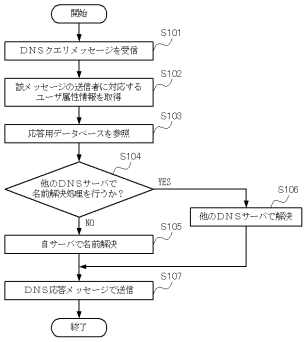
D14 ユーザ情報データベース

ユーザＩＰアドレス	ログインＩＤ	接続回線種別	ＮＡＳアドレス	参照先
123.45.0.2	taro	ADSL	30.30.30.30	－
123.45.0.4	hanako	－	20.20.20.20	8.8.1.4
123.45.1.0/24	－	－	－	9.9.9.9
・・・	・・・	・・・	・・・	・・・

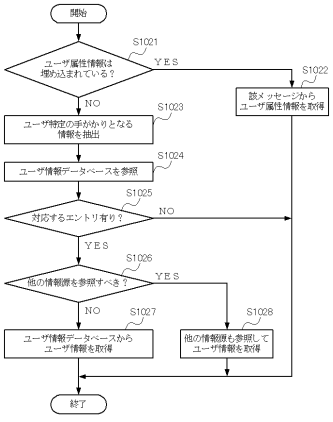
【図３】



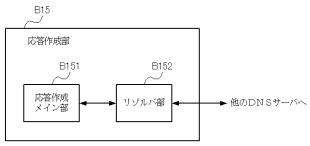
【図４】



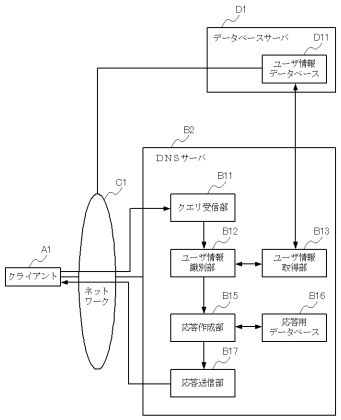
【図５】



【図６】



【図７】



【図８】

301 名前解決テーブル

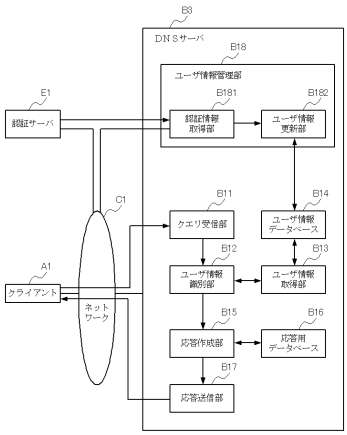
ユーザ属性				ドメイン名	参照先
ユーザＩＰアドレス	ユーザＩＤ	接続回線種別	ＮＡＳアドレス		
－	－	ADSL	30.30.30.30	aaa.com	"adsl aaa com.dat"
				・・・	・・・
－	－	ISDN	20.20.20.20	aaa.com	"isdn aaa com.dat"
				・・・	・・・
－	－	－	－	user.com	"user com.dat"
－	－	－	－	・・・	・・・
DEFAULT				aaa.com	"aaa com.dat"
				bbb.com	4.3.2.1
				ccc.com	"ccc com.dat"
				・・・	・・・

302 ゾーンファイル

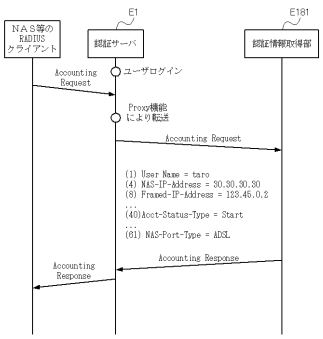
user com.dat

TYPE	FQDN	DATA
TXT	123-45-0-2.user.com	"login id=taro""access media=ADSL""NAS address=10.10.10.10
TXT	123-45-0-4.user.com	"login id=hanako""NAS address=20.20.20.20""refer=9.8.1.4"
TXT	123-45-1-0_24.user.com	"refer=9.8.8.8"
・・・	・・・	・・・

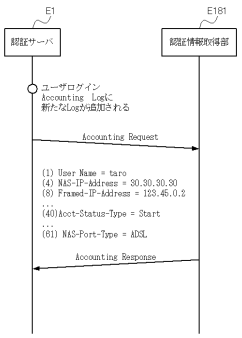
【図９】



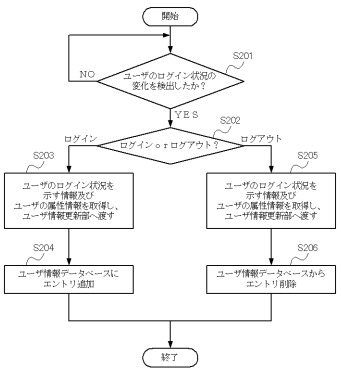
【図１０】



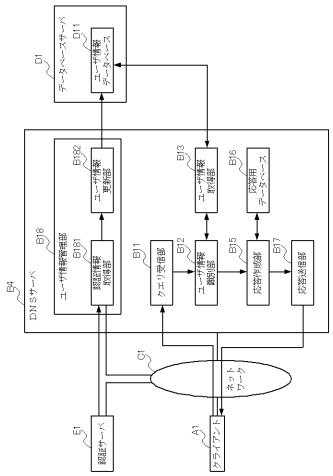
【図１１】



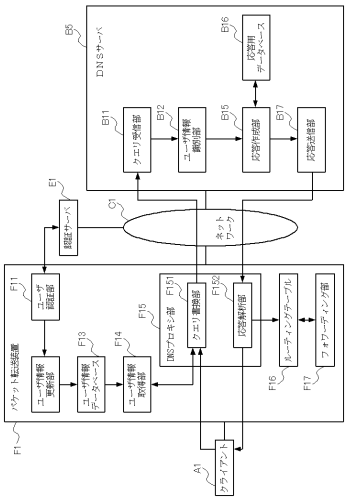
【図１２】



【図１３】



【図１４】



【図１５】

401 名前解決テーブル

ユーザ属性				ドメイン名	参照先
ユーザＩＤ	接続回線種別	グループＩＤ	パケット転送装置ＩＤ		
–	ethernet	silver	switch99	ddd.com	"sw99 ddd com.dat"
				・・・	・・・
–	wireless LAN	–	–	ddd.com	"wlan ddd com.dat"
				・・・	・・・
hanako	–	–	switch99	ddd.com	"hanako ddd com.dat"
				・・・	・・・
–	–	–	–	・・・	・・・
DEFAULT				aaa.com	"aaa com.dat"
				bbb.com	4.3.2.1
				ccc.com	"ccc com.dat"
				・・・	・・・

402ゾーンファイル
sw99 ddd com.dat

TYPE	FQDN	DATA	ADDITIONAL DATA
A	www.ddd.com	20.1.1.1	SrcPAddr=40.1.1.1,vlanID=111,outport=21,priority=0
A	ftp.ddd.com	30.1.1.1	SrcPAddr=40.1.1.1,DestIPAddr=50.1.1.1,vlanID=222, outport=21,priority=0
A	host.ddd.com	40.1.1.1	–
・・・	・・・	・・・	・・・

403ゾーンファイル
hanako ddd com.dat

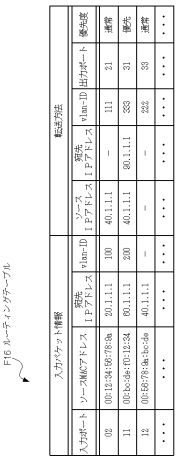
TYPE	FQDN	DATA	ADDITIONAL DATA
A	www.ddd.com	60.1.1.1	SrcPAddr=40.1.1.1,DestIPAddr=60.1.1.1,vlanID=333, outport=31,priority=1
A	ftp.ddd.com	70.1.1.1	SrcPAddr=50.1.1.1,DestIPAddr=80.1.1.1,vlanID=333, outport=32,priority=1
A	host.ddd.com	80.1.1.1	–
・・・	・・・	・・・	・・・

【図１６】

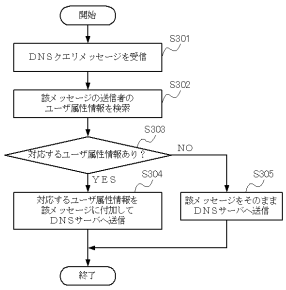
F13 ユーザ情報データベース

入力ポート	ソースMACアドレス	ユーザＩＤ	接続回線種別	接続回線速度	グループＩＤ	・・・
02	00:11:24:80:78:8a	taro	ethernet	100Mbps	silver	・・・
11	00:bc:de:f0:12:34	hanako	ethernet	10Mbps	–	・・・
12	00:6b:78:8a:bc:de	pochi	wireless LAN	10Mbps	silver	・・・
・・・	・・・	・・・	・・・	・・・	・・・	・・・

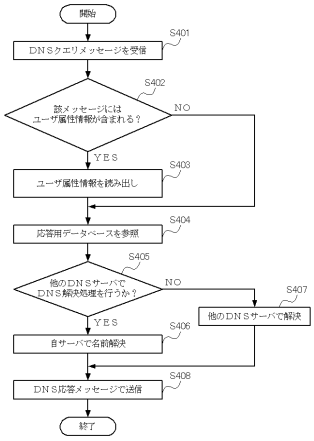
【図１７】



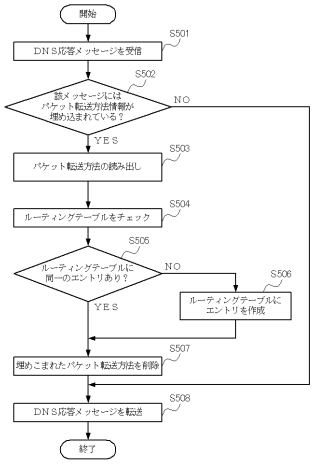
【図１８】



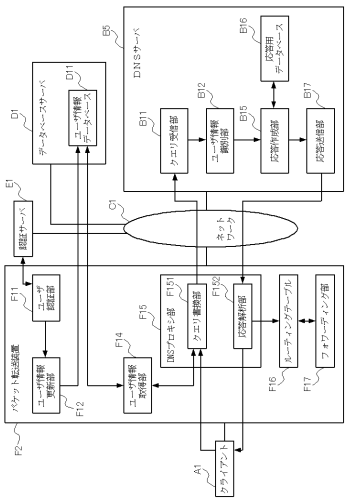
【図１９】



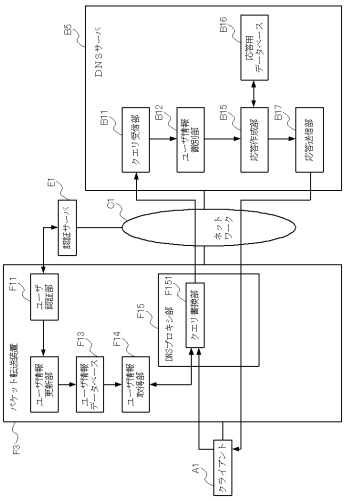
【図２０】



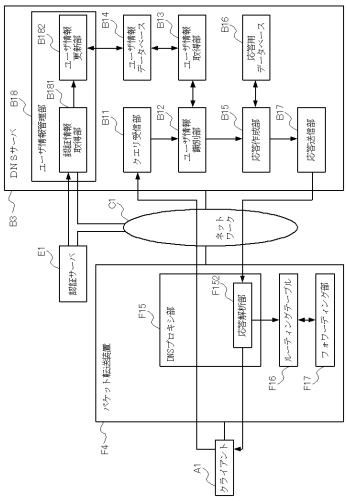
【図２１】



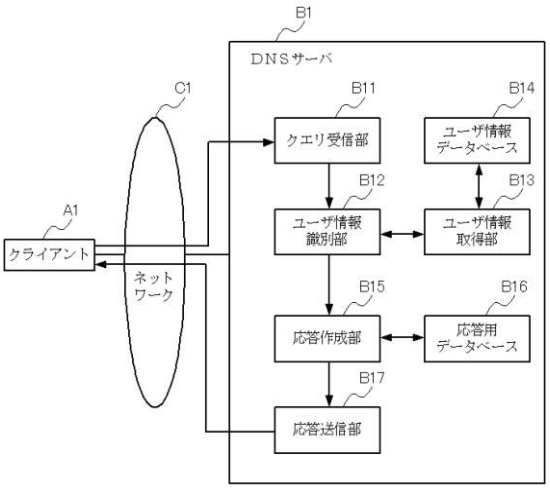
【図２２】



【図２３】



【図１】


B1
DNSサーバ
C1
B11
クエリ受信部
B14
ユーザ情報
データベース
B12
ユーザ情報
識別部
B13
ユーザ情報
取得部
A1
クライアント
ネット
ワーク
B15
応答作成部
B16
応答用
データベース
B17
応答送信部

フロントページの続き

審査官　吉田　隆之

(56)参考文献　特開２００３－３２２８１（ＪＰ，Ａ）
特開２００２－３６８７８１（ＪＰ，Ａ）
2002年信学通ソ大会 B-6-41

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２