(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-204189
(P2005-204189A)
(43)公開日　平成17年7月28日(2005.7.28)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/56	H04L 12/56	400Z	5K030
H04L 12/66	H04L 12/66	A	

審査請求 未請求　請求項の数 11　OL　（全 13 頁）

(21)出願番号　特願2004-10011(P2004-10011)
(22)出願日　平成16年1月19日(2004.1.19)

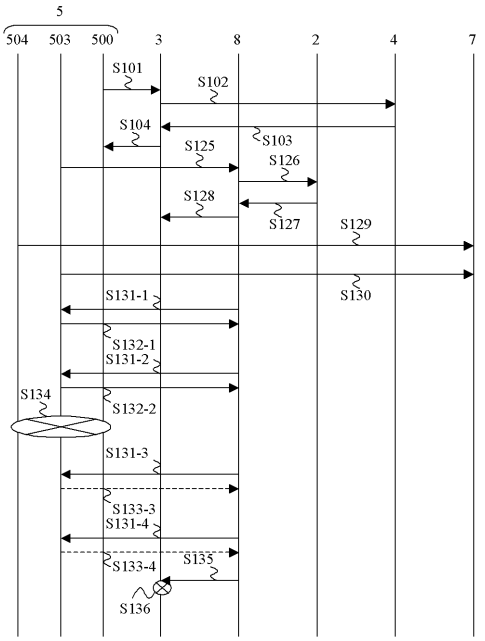
(71)出願人　000153465
株式会社日立コミュニケーションテクノロジー
東京都品川区南大井六丁目２６番３号
(74)代理人　100075096
弁理士　作田　康夫
(74)代理人　100100310
弁理士　井上　学
(72)発明者　吉本　哲郎
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
(72)発明者　滝広　眞利
東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

最終頁に続く

(54)【発明の名称】アクセスユーザ管理システム、アクセスユーザ管理装置

(57)【要約】
【課題】ユーザの再認証の不便が解消された新規なweb認証方式を提供する。
【解決手段】認証用webサーバに換えて、ユーザを認証する機能と、ユーザに対し定期的に再認証要求するもしくは接続確認パケットを送りその返信を受け取ることでユーザの接続状態を確認する機能と、アクセスサーバに対しポリシールーティングを設定する機能を持つサーバをおき、端末において、webブラウザの代わりに上記サーバと通信し、起動時に認証を行い、再認証要求もしくは接続確認パケットに応答するクライアントを動作させることにより接続状態の保持を行う。または、認証用webサーバの位置に、ユーザを認証する機能を持つ機能を持つサーバをおき、端末においてwebブラウザの代わりに上記サーバと通信し、起動時に認証を行い、その後も定期的に認証を行うクライアントを動作させることにより接続状態の保持を行う。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
ユーザ端末からのアクセス要求を受信して前記ユーザ端末をネットワークへ接続するアクセスサーバと、前記ユーザのネットワークへの接続状態を監視する監視サーバと、前記アクセスサーバへアクセス要求を送信したユーザ端末の認証を行なう認証サーバとを用いて、前記ユーザ端末をネットワークに接続する際のユーザアクセス管理方法において、
前記アクセスサーバにより前記ユーザ端末からのアクセス要求を受信し、
該アクセス要求が認証されていないユーザ端末からのアクセス要求である場合には、前記ユーザ端末からの送信パケットが前記認証サーバへ転送されるよう当該アクセスサーバの経路制御条件を設定し、
前記アクセス要求が既に認証されているユーザ端末からのアクセス要求である場合には、前記ユーザ端末からの送信パケットがネットワークへ接続されるように前記アクセスサーバの経路制御条件を設定し、
前記認証されたユーザ端末のネットワークへのアクセス状態を前記監視サーバにより監視し、
該監視の結果、ネットワークへアクセスしていないと判断したユーザ端末からの送信パケットに対しては、前記認証サーバへ転送されるよう前記アクセスサーバの経路制御条件を設定することを特徴とするアクセスユーザ管理方法。
【請求項２】
請求項１に記載のアクセスユーザ管理方法において、
前記監視サーバと前記認証サーバとが同一のサーバであることを特徴とするアクセスユーザ管理方法。
【請求項３】
請求項１に記載のアクセスユーザ管理方法において、
前記監視サーバにより、生存確認パケットまたはユーザ認証要求パケットを前記ユーザ端末に送信し、
該ユーザ端末からの応答が一定時間以上無い場合には、前記ユーザ端末がネットワークへアクセスしていないと判断することを特徴とするアクセスユーザ管理方法。
【請求項４】
請求項３に記載のアクセスユーザ管理方法において、
前記ユーザ端末は、前記生存確認要求パケットまたはユーザ認証要求パケットへの応答をバックグラウンドで実行することを特徴とするアクセスユーザ管理方法。
【請求項５】
ユーザ端末からのアクセス要求を受信して前記ユーザ端末をネットワークへ接続するアクセスサーバと、前記ユーザのネットワークへの接続状態を監視する監視サーバと、前記アクセスサーバへアクセス要求を送信したユーザ端末の認証を行なう認証サーバとを備え、
前記アクセスサーバは、
パケットを送受信する手段と、
ユーザ端末から送信されたパケットに対して所定の経路制御を施す手段と、
受信した変更要求に基づき該経路制御の条件を変更する手段とを有し、
前記監視サーバは、
パケットを送受信する手段と、
受信パケットの送信元が認証されていないユーザ端末か認証されたユーザ端末かを弁別する手段と、
既に認証されたユーザ端末に対して送信する生存確認パケットないし再認証要求パケットを生成する手段と、
前記アクセスサーバに対して送信する経路制御条件の変更要求パケットを生成する手段とを有し、
前記生存確認要求パケットないし再認証要求パケットへの応答が一定時間以上無い場合に

は、前記アクセスサーバに対し前記経路制御条件の変更要求パケットを送信し、
当該一定時間以上応答のないユーザ端末からの送信パケットを前記認証サーバへ転送するように前記アクセスサーバの経路制御条件を設定することを特徴とするアクセスユーザ管理装置。
【請求項６】
請求項５に記載のアクセスユーザ管理装置において、
前記監視サーバには、プレゼンスアウェアネスソフトウェアが実装されることを特徴とするアクセスユーザ管理装置。
【請求項７】
請求項６に記載のアクセスユーザ管理装置において、
前記プレゼンスアウェアネスソフトウェアが、ＩＭ（Instant Messaging）であることを特徴とするアクセスユーザ管理装置。
【請求項８】
請求項５に記載のアクセスユーザ管理装置において、
前記監視サーバには、メールサーバソフトウェアが実装されることを特徴とするアクセスユーザ管理装置。
【請求項９】
受信パケットをインターネットへ転送するアクセスサーバに接続されるアプリケーションサーバであって、
パケットを送受信する手段と、
受信パケットの送信元が認証されていないユーザ端末か認証されたユーザ端末かを弁別する手段と、
前記認証されたユーザ端末に対して送信する生存確認パケットないし再認証要求パケットを生成する手段と、
当該ユーザ端末に対して送信した生存確認パケットないし再認証要求パケットの送信時から経過した時間をカウントするカウンタと、
前記アクセスサーバに対して送信する経路制御条件の変更要求パケットを生成する手段とを有し、
前記生存確認パケットないし再認証要求パケットに対する応答が所定時間無い場合には、前記経路制御条件の変更要求パケットを前記アクセスサーバに対して送信することを特徴とするアプリケーションサーバ。
【請求項１０】
請求項９に記載のアプリケーションサーバにおいて、
メールサーバソフトウェアが実装されたことを特徴とするアクセスユーザ管理装置。
【請求項１１】
請求項９に記載のアプリケーションサーバにおいて、
ＩＭ（Instant Messaging）機能が実装されたことを特徴とするアクセスユーザ管理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ブロードバンドインターネット接続におけるアクセスユーザの管理に関する。
【背景技術】
【０００２】
ネットワーク通信のセキュリティを確保する上で、ユーザ認証技術は非常に重要な技術である。ブロードバンドインターネット接続におけるアクセスユーザの認証および状態管理においては、現在、PPPoE（Point-to-Point Protocol Over Ethernet）（Ethernetは登録商標）が広く使われている。PPPoEは、ダイアルアップ接続で使われていたPPPをEthernet上で使えるようにしたものであり、認証プロトコルによってレイヤ2レベルでユーザ認

証をすることが可能であり、また定期的にユーザ再認証を要求する、もしくはLCP Echoパケットを用いることによりユーザの接続状態を監視することが可能である。

【０００３】

また、IEEE802.1xという通信規格を用いる認証方法もある。これは、レイヤ2でのポート単位の認証を行う方法であり、現在はローカルな無線接続の認証に使われることが多い。認証プロトコルによってレイヤ2レベルでユーザ認証をすることが可能であり、また定期的にユーザ再認証を要求することによりユーザの接続状態を監視することが可能である。

【０００４】

上記2つの認証方法はレイヤ2でのユーザ管理が可能であるが、最近のルータに一般的に入っている機能であるポリシールーティング機能と、World-Wide-Web（web）によるアプリケーションレイヤレベルでの認証を組み合わせてアクセスユーザを認証することも可能である。これは、ポリシールーティング機能を用いてユーザの接続当初は特定のwebサーバにしかアクセスできないようにアクセスユーザとレイヤ3レベルで直接接続する装置であるアクセスサーバ（ルータ）を設定しておき、ユーザが接続した後にwebブラウザから認証をさせ、認証されたユーザのIPアドレスのみが普通にルーティングされるようにwebサーバからアクセスサーバを設定しなおしに行くというユーザ認証方法である。

【０００５】

図10は一般的なアクセスサーバのハードウェア構成図である。31はCPUであり、ユーザ管理や、場合によってはルーティングなどの複雑な処理をソフトウェアで処理するために存在する。32はCPU31が使用するメモリであり、この上にアクセスサーバとして必要なソフトウェアやデータが格納されている。32上には端末の接続情報を保持する接続情報管理部321、外部からの接続情報更新要求を受け取り321および323に状態変更指示を出す外部管理サーバ連携部322、321と322の指示に従いパケット転送部の情報を更新するパケット転送部設定部323などが最低存在する。33はパケット転送部である。パケット転送は31のソフトウェア処理でも実行できるが、多くの場合は独立したパケット転送部を持ち、CPU31を用いるよりも高速に実行できる。パケット転送部は、完全にハードウェアロジックで構築されたプロセッサの場合もあるし、ネットワークプロセッサと呼ばれるパケット転送に特化した特殊なMPUを使う場合もある。331のパケット転送部は、通常のパケット転送を高速に行う。332のポリシールーティング部は、特定のパターンを持つパケットに関して、331の転送結果をオーバーライドし、ポリシーにしたがってパケット転送の宛先を変更する機能を持つ。331および332は33の構成により、ハードで実現される場合もあれば、ソフトで実現される場合もある。NIF34は実際にネットワークと物理的に接続する箇所である。ここまで述べた各モジュールはバス35によって接続されている。35はバスでなくスイッチでもよい。

【０００６】

図２及び図３を用いてポリシールーティングとweb認証を組み合わせる方法について説明する。図２は、システム模式図である。端末5がインターネット7にアクセスサーバ3を介して接続している。アクセスサーバ3はDHCPサーバ4とwebサーバ1と接続している。webサーバ1は認証サーバ2と接続している。端末5の下部には、端末5上で動作するソフトウェア構成を示す。端末5上ではOS500が動作しており、その上でwebブラウザ501とその他のネットワークアプリケーション502が動作している。

【０００７】

図３は、ポリシールーティングとweb認証を組み合わせる認証方法のシーケンス図である。端末が起動すると、端末上のOSはDHCPによりIPアドレスを得ようとする（S101）。DHCPリクエストを受けたアクセスサーバは、DHCPリレーによりDHCPサーバにリクエストを転送する（S102）。DHCPサーバは端末にIPアドレスを割り振り、アクセスサーバに結果を返信する（S103）。アクセスサーバはIPアドレスを端末に転送し（S104）、端末5はIP通信可能な状態となる。

【０００８】

端末5に割り振られたIPアドレスは、この時点ではポリシールーティングがアクセスサーバ3によって設定されており、インターネットへ自由にアクセスすることはできない。アプリケーション502からのインターネットアクセスS105もwebブラウザからのインターネットアクセスS106も失敗する。図３に示された×印は、各ステップS105もS106も両方共が実現できないことを意味する。この時点で端末5がアクセス可能なのはwebサーバ1のみである。端末はwebサーバ1にアクセスし、ユーザ名とパスワードを入力することで認証を要求する（S107）。認証要求を受けたwebサーバは認証サーバ2に認証要求を転送する（S108）。認証サーバからの承認（S109）を受けたwebサーバはアクセスサーバ3に端末5のIPアドレスに関してポリシールーティングの設定をはずすように設定する（S110）。これにより、端末5はインターネットアクセスが可能となり、webブラウザからのインターネットアクセスS111もその他のアプリケーションからのインターネットアクセスS112も成功するようになる。

【０００９】

図２および図３を用いた説明では、簡単のため、アクセスサーバ3とwebサーバ1、認証サーバ2、DHCPサーバ4を別のサーバとして表したが、機能的に等価であれば各サーバは任意の組み合わせで縮退していてもよい。またIPアドレス割り振りの例としてDHCPをあげたが、IPアドレスの割当方法は任意の方法を用いることが可能である。たとえば、IPプロトコルがIPv6であればRA（Router Advertisement）を使ってもいい。また、S106とS107において、webブラウザが明示的にwebサーバ1にアクセスすることとしたが、webサーバのリダイレクト機能を使うことによりS106からS107は連続したシーケンスにすることも可能である。

【００１０】

【特許文献１】特開2003-224577

【００１１】

【非特許文献１】RFC2516:A Method for Transmitting PPP Over Ethernet （PPPoE）IEEE 802.1X-2001：IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control

【発明の開示】

【発明が解決しようとする課題】

【００１２】

PPPoEはPPPヘッダおよびPPPoEヘッダがパケットに付与されることによる通信効率の悪さや、Ethernetが本来持っているマルチキャスト機能が使用できなくなるなどの制限を持つ。また、PPPoEはレイヤ2レベルの通信プロトコルであるため、アクセスユーザとレイヤ3レベルで直接接続するアクセスサーバにPPPoE機能を持たせる必要があり、それによりアクセスサーバのコストが高くなるという問題がある。

IEEE802.1xは通信効率やマルチキャスト機能の制限はないが、PPPoEと同様にレイヤ2レベルの通信規格であるため、アクセスサーバにIEEE802.1xへの対応機能を実装する必要があり、それによりアクセスサーバのコストが高くなるという問題がある。

【００１３】

ポリシールーティングとwebによる認証を組み合わせるユーザ認証方法では、ユーザの接続状態を監視する手段がない。ユーザがインターネットにアクセスしているということは、ISP（Internet Service Provider）側からみれば、ユーザに対して特定のネットワークリソース（例えば、DHCP経由でユーザに割り当てられるIPアドレス等）を割り当てていることを意味する。従って、現行のweb認証方法では、ネットワークリソースを割り当てたユーザが、今現在インターネットに接続しているかいないか判らない。しかしながら、IPv4アドレスをはじめとしてネットワークリソースは有限であるので、接続していないユーザにリソースを割り当てたままにすることはできない。そのため現在は、アクセスサーバ1でデータパケットの導通を監視し、タイムアウトした場合はユーザが不通になったものとみなしてユーザのIPアドレスを再びwebサーバにしか接続できないように再設定し、ユーザが再びwebブラウザを動作させた際に再認証を要求するという手段をとっている。

【００１４】
図３を用いて、タイムアウト時のアクセスサーバの再認証要求動作を説明する。図３において、S113はタイムアウト期間をあらわしている。S113であらわされた期間、端末5からのIPアクセスがなかった場合、アクセスサーバ3はS114において端末5のIPアドレスに対し、再びポリシールーティングを設定する。この後は端末5のアプリケーションからのインターネットアクセスS115は失敗するようになる。よって、ユーザはwebブラウザで再びwebサーバ1にアクセスして、S107～S110までと同様の認証動作をS116からS119で再び繰り返す。ユーザの再認証により、ユーザ側では再び端末5からのインターネットアクセスS120が可能となる。これはユーザから見ると不要な負担を増やすこととなる。特に、ユーザがwebブラウザ以外のアプリケーションしか使っていない場合には、認証のためだけにいちいちwebブラウザを再動作させる必要があり、ブロードバンドで一般的な常時接続の利便性を著しく阻害する。
【００１５】
そこで本発明は、従来のweb認証方式における、ユーザの接続状態を把握できないという課題と、ユーザにとって再認証手続を繰り返す手間が煩雑という２つの課題を解決できる新規なweb認証方法及び当該認証方法を提供可能なweb認証装置を提供することを目的とする。
【課題を解決するための手段】
【００１６】
従来のポリシールーティングとweb認証を組み合わせる認証方法の問題点は、端末側の認証の枠組みとして、自立的に動作することのできないwebブラウザを用いている点にある。
よって、本発明においては、従来の認証用webサーバに換えて、ユーザの接続状態を確認する機能と、確認したユーザの接続状態に基づきアクセスサーバに対しポリシールーティングのポリシー変更要求ないし現ポリシーの解除要求を送信する機能を持つサーバを配置し、一方、当該サーバと通信可能なクライアント機能を端末側に実装し、ユーザの接続が切れたことを確認したら、アクセスサーバがユーザの自由なインターネットへのアクセスを許さなくすることを特徴とする。
【００１７】
端末のインターネットアクセス開始時には、webブラウザの代わりに前記クライアント機能を用いて最初の認証を行う。端末に実装されるクライアント機能は、前記サーバからの接続確認要求に対して、バックグランドで応答可能であることが必要である。これにより、ユーザが再認証動作を繰り返すことなく、端末が接続状態を保持することが可能となる。
上述したサーバとクライアントは、ユーザ管理専用のものでもよいし、すでに存在する同様の機能を持つアプリケーションのサーバにアクセスサーバ設定機能を付加するのでもよい。すでに存在するアプリケーションの例としては、Instant Messenger（IM）に代表される、ユーザの端末使用状態をネットワーク上の特定あるいは不特定ユーザに対して開示するプレゼンスアウェアネスソフトウェア、あるいは、メールサーバ（MTA）とメールクライアント（MUA）などである。
【００１８】
サーバとしては、一台のサーバに、従来の認証用サーバの持つ認証機能とポリシールーティングのポリシー変更要求の送信機能を実装しても良い。あるいは、プレゼンスアウェアネスサーバと従来の認証用サーバを組み合わせて用いても良い。
サーバは、前記の接続確認要求に替えて、端末に対して再認証要求を送ることにしてもよい。但し、この場合、端末に実装されたクライアントが、サーバからの再認証要求に対してバックグラウンドで応答可能な機能を備えていることが必要となる。端末は、実装されたクライアント機能を介して、定期的にサーバに接続し、再認証動作を実行する。
【発明の効果】
【００１９】

本発明により、PPPoEやIEEE802.1xを扱える特殊なアクセスサーバを置くことなく、ユーザの接続状態を適切に管理し、IPアドレスなどのリソースを適切にユーザに配分することが可能となる。

【実施例１】

【００２０】

本実施例ではユーザ端末のネットワーク接続状態に関する情報を取得可能なアプリケーションとして、IMを用いた場合について説明する。以下、図１、図５及び図７を用いて、詳細を説明する。図４は本発明のシステム模式図である。図２と比較して、認証用webサーバ1の代わりにアクセスサーバ設定機能つきIMサーバ8が置かれ、端末5上ではwebブラウザの代わりにIMクライアント503が動作し、webブラウザを含むその他のインターネットアプリケーション504が動作している。

【００２１】

図１は本発明のシーケンス図である。まず端末が起動すると図３とまったく同様にOS500がIPアドレスを取得する（S101～S104）。ついで、IMクライアント503からIMサーバ8へユーザ名とパスワードを用いた認証要求を送信する（S125）。通常IMクライアントはOSが起動した時点で自動的に起動され、OSがIPアドレスを取得した時点で認証要求をサーバに向けて自動的に発する。認証要求を受けたIMサーバ8は、認証サーバ2に認証確認用の認証パケットを送信する（S126）。認証サーバ2は、データベースに登録されたユーザ名とパスワードが一致すれば、IMサーバ8に対して認証可の承認パケットを送信する（S127）。ユーザ名とパスワードが一致しない場合には、認証サーバ2は、IMサーバ8に対して、認証否の否認パケットを送信する。

【００２２】

IMサーバ8は、認証サーバ2からの承認パケットを受信すると、アクセスサーバ3に対して、ポリシールーティングの解除要求パケットまたはポリシールーティングで用いる経路制御ポリシーの変更要求パケットを送信する（S128）。これにより、送信元のアドレスが端末5のアドレスであるパケットに対してアクセスサーバ3が設定していた経路制御の設定条件が解除ないし変更され、アプリケーション504を介して端末5から送信されたパケットは、インターネット７上の任意の相手に対して送信可能となる（S129）。また、IMクライアント503もインターネット7上の他のIMサーバにアクセスできるようになる（S130）。

【００２３】

認証成功後、IMサーバ8は定期的に認証確認または生存確認をIMクライアント503に送信する（S131）。これに対し、IMクライアントは認証要求か生存通知を返信する（S132）。これによりIMサーバ8は端末5が通信継続中であることを確認する。これにより、ユーザは端末が動作している間にわたって再認証のための動作を行うことなくインターネットアクセスが可能となる。

ここで、S134の時点で端末5が停止した場合を考える。IMサーバは定期的に認証確認または生存確認を送り続けるが、端末が停止しているので応答は帰らない（S133）。これが一定回数続いた場合は、IMサーバは端末が不通になったと判断し、アクセスサーバ3に対して、端末5のIPアドレスに対するポリシールーティングの設定を行う（S135）。アクセスサーバでの設定が終了した時点S136で端末5へのインターネットリソースは解放され、再び他の端末向けに使うことが可能となる。

【００２４】

図５は本発明におけるIMサーバ8の機能ブロック図である。端末インターフェイス部801は、端末5からの認証要求、他ユーザへのメッセージなどの各種通信を受けて、各々を適切な機能ブロックに分配し、また、8内の各々の機能ブロックから端末5への通信を媒介する。認証部802は端末5からの認証を受け、認証サーバ2に認証確認を行い、その結果ユーザのアクセス可否を判断する。また、本発明においては、アクセスサーバ設定部805に対しても判断結果を通知する。端末管理部803は定期的に認証確認要求または生存確認要求を端末5に対して送信し、その応答を受け取ることか、端末5からの再認証要求または生存確認を定期的に受け付けることにより端末5の状態を管理する。また、本発明においては

、アクセスサーバ設定部805に対しても管理状態を通知する。その他IM機能部804は端末5と他ユーザとのメッセージ通信などの、本発明と関連しない機能を実現する。アクセスサーバ設定部805は、本発明に特徴的な機能ブロックであり、アクセスサーバに対して端末5のIPアドレスに対するポリシールーティングなどの設定を行う。

【００２５】

今回は説明のためアクセスサーバ3とIMサーバ8、認証サーバ2、DHCPサーバ4を別のサーバとして表したが、従来例と同様に、機能的に等価であれば各サーバは任意の組み合わせで縮退していてもよい。特に、アクセスサーバ3とIMサーバ8の組み合わせは、ポート単位の設定を行いたい場合に有効である。また、IMサーバと端末の間で通信を代理するProxyサーバ機能をアクセスサーバの中におくのも、ポート単位の設定を行いたい場合に有効である。またIPアドレス割り振りの例としてDHCPをあげたが、IPアドレスの割当方式はなんでもいい。

【実施例２】

【００２６】

図を用いて、web認証を用いた場合の第二の発明の実施例について説明する。本実施例では、認証サーバと接続するアプリケーションサーバとして、従来例と同様のwebサーバ1を使用できる点が実施例1との違いである。図６は本発明のシステム模式図である。図２と比較して、端末5上ではwebブラウザの代わりに505が動作し、webブラウザを含むその他のインターネットアプリケーション506が動作している。

【００２７】

図７は本発明のシーケンス図である。まず端末が起動すると図３とまったく同様にOS500がIPアドレスを取得する（S101～S104）。ついで、定期認証クライアント503から認証用webサーバ1へユーザ名とパスワードを用いた認証要求を送信する（S141）。この動作は、OSが起動した時点で定期認証クライアントを自動的に起動し、定期認証クライアントはOSがIPアドレスを取得した時点で認証要求をサーバに向けて自動的に発するように設定しておくことにより実現する。認証要求を受けた認証用webサーバ1は、認証サーバ2に認証確認を行い（S142）、認証サーバからの承認S143を受けて、アクセスサーバにポリシールーティングの期限付きの解除設定を行う（S144）。これにより、端末上のアプリケーション506はインターネット７上の任意の相手とアクセスできるようになる（S145）。認証成功後、定期認証クライアントは定期的に認証用webサーバ1に認証情報を送信する（S147）。これを受けた認証用webサーバ1はアクセスサーバに対しポリシールーティング解除の期限延長を設定する（S148）。これにより、ユーザは端末が動作している間にわたって再認証のための動作を行うことなくインターネットアクセスが可能となる。

【００２８】

ここで、S149の時点で端末5が停止した場合を考える。端末が停止しているので認証情報が送信されなくなる（S151）。これがタイムアウト期間S150のあいだ続いた場合は、アクセスサーバは端末が不通になったと判断し、端末5のIPアドレスに対するポリシールーティングの設定を行う（S152）。アクセスサーバでの設定が終了した時点S152で端末5へのインターネットリソースは解放され、再び他の端末向けに使うことが可能となる。ここではタイムアウトはアクセスサーバ3側で設定したが、タイムアウト管理を認証用webサーバ1側で行い、タイムアウトした時点で認証用webサーバ1からアクセスサーバ3にポリシールーティングを設定しに行く方式でもよい。

【００２９】

図８は定期認証クライアントの機能ブロック図である。ユーザ情報管理部5051は、ユーザ名やパスワードといった認証に必要な情報を管理する。webサーバアクセス部5052は、ユーザ情報管理部5051で管理されている情報をhttp形式に変換して、起動時とタイマ5053からの通知時に認証用webサーバに送信する。タイマ部5053はwebサーバアクセス部5052に対して、認証用webサーバにアクセスする時間を通知する。今回は説明のためアクセスサーバ3と認証用webサーバ1、認証サーバ2、DHCPサーバ4を別のサーバとして表したが、従来例と同様に、機能的に等価であれば各サーバは任意の組み合わせで縮退していてもよい

。特に、アクセスサーバ3と認証用webサーバ1の組み合わせは、ポート単位の設定を行いたい場合に有効である。また、認証用webサーバと端末の間で通信を代理するProxyサーバ機能をアクセスサーバの中におくのも、ポート単位の設定を行いたい場合に有効である。またIPアドレス割り振りの例としてDHCPをあげたが、IPアドレスの割当方式はなんでもいい。

【００３０】

図９は定期認証クライアントが動作する端末の模式図である。メモリ50上に端末で使用される各種プログラム（webブラウザやメールソフトなど506）が格納されている。定期認証クライアント505も個々に格納されている。CPU51は実際にメモリ50上のソフトウェアを実行する。NIF52はネットワークに物理的に接続するモジュールである。その他の入出力装置53はキーボードやディスプレイであり、端末5のユーザはこれらを用いてソフトウェアを利用する。

【図面の簡単な説明】

【００３１】

【図１】第一の発明のシーケンス図。

【図２】ポリシールーティングとweb認証を組み合わせた方式のシステム模式図。

【図３】ポリシールーティングとweb認証を組み合わせた方式のシーケンス図。

【図４】第一の発明のシステム模式図。

【図５】第一の発明で使われるIMサーバの機能ブロック図。

【図６】第二の発明のシステム模式図。

【図７】第二の発明のシーケンス図。

【図８】第二の発明で使われる定期認証クライアントの機能ブロック図。

【図９】認証クライアントが動作する端末の模式図。

【図１０】ルータのブロック図。

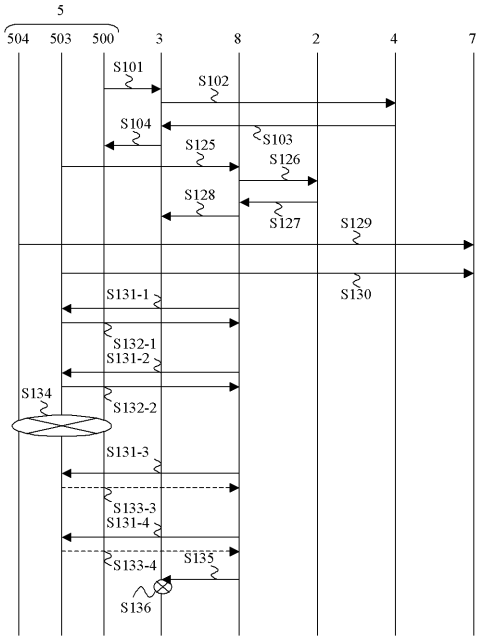
【符号の説明】

【００３２】

１　認証用webサーバ
２　認証サーバ
３　アクセスサーバ
４　DHCPサーバ
５　端末
６　接続回線
７　インターネット
８　IMサーバ
５００　端末のOS
５０１　webブラウザ
５０２　webブラウザを除くインターネットアプリケーション
５０３　IMクライアント
５０４　IMクライアントを除くインターネットアプリケーション
５０５　定期認証クライアント
５０６　定期認証クライアントを除くインターネットアプリケーション
８０１　端末インターフェイス部
８０２　認証部
８０３　端末管理部
８０４　その他IM機能部
８０５　アクセスサーバ設定機能部
５０５１　ユーザ情報管理部
５０５２　webサーバアクセス部
５０５３　タイマ。

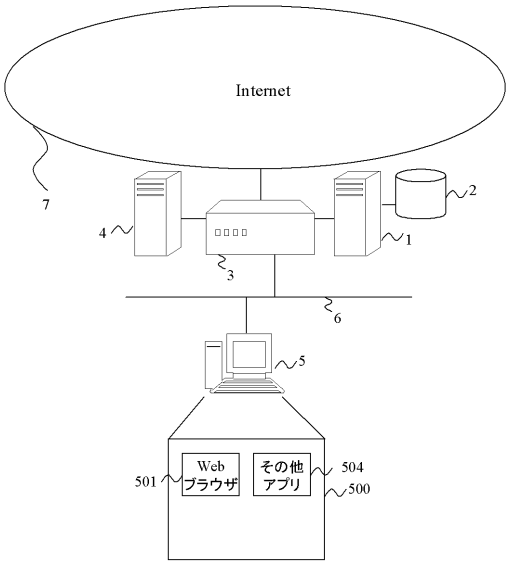
【図１】

図1



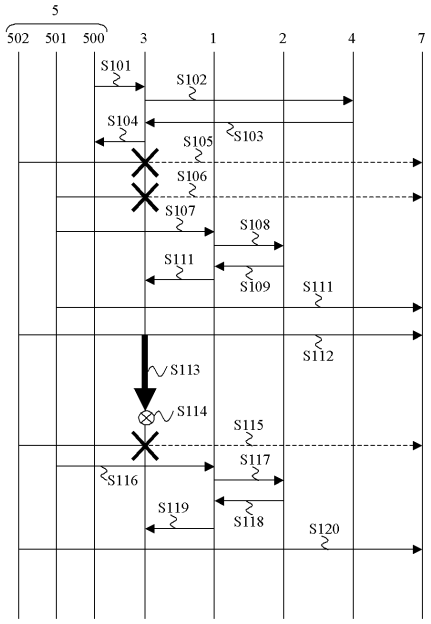
【図２】

図2



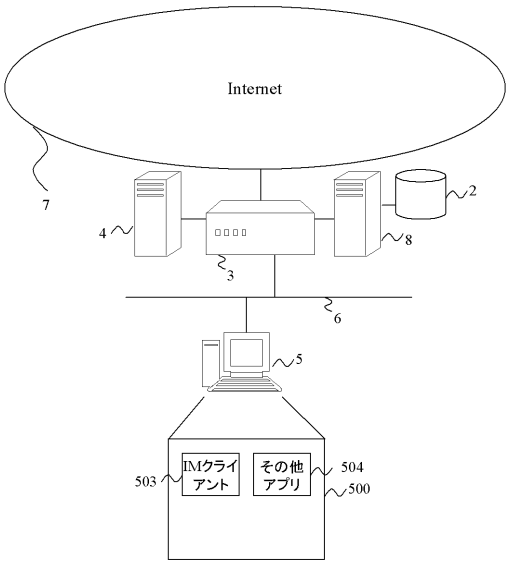
【図３】

図3



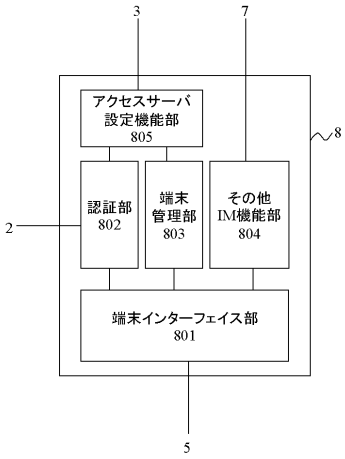
【図４】

図4



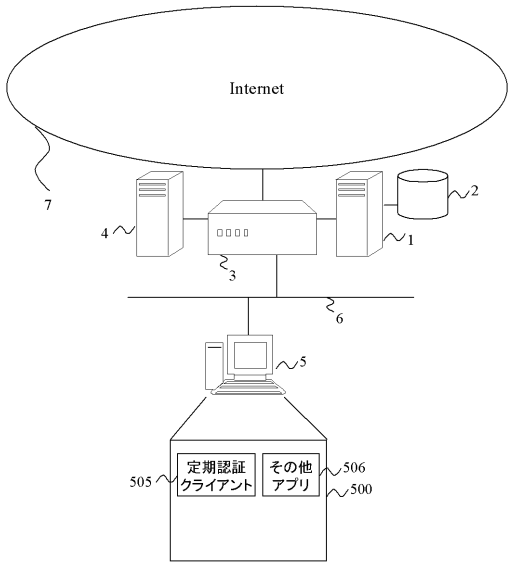
【図５】

図5



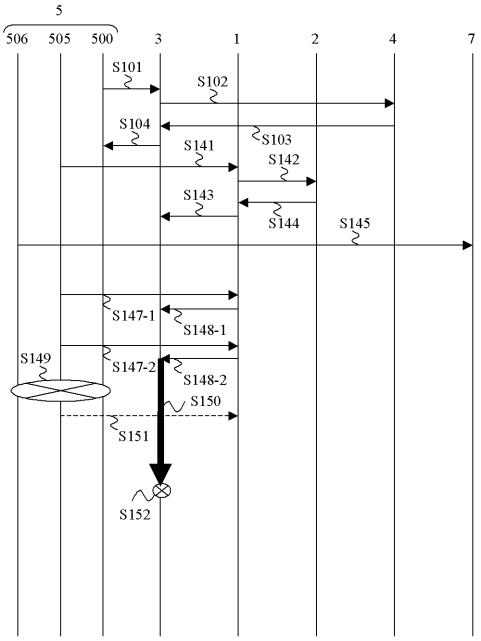
【図６】

図6



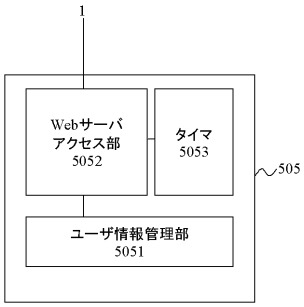
【図７】

図7



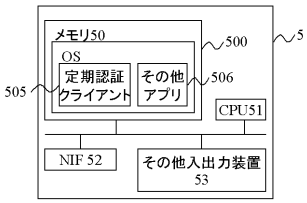
【図８】

図8



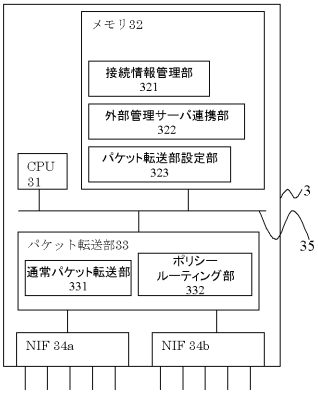
【図９】

図9



【図１０】

図10


メモリ32
接続情報管理部
321
外部管理サーバ連携部
322
パケット転送部設定部
323
CPU
31
3
35
パケット転送部33
通常パケット転送部
331
ポリシー
ルーティング部
332
NIF 34a
NIF 34b

フロントページの続き

(72)発明者　横山　卓
東京都品川区南大井六丁目２６番３号　株式会社日立コミュニケーションテクノロジー内

Ｆターム(参考) 5K030 GA15 HA08 HD03 HD06 LB09 MB09 MB12