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

特許第4332000号
(P4332000)

(45)発行日　平成21年9月16日(2009.9.16)　(24)登録日　平成21年6月26日(2009.6.26)

(51)Int.Cl.　　F I
H04W 84/12 (2009.01)　　H04L 12/28　300Z
H04L 12/46 (2006.01)　　H04L 12/46　E
　　H04L 12/46　V

請求項の数 4　(全 17 頁)

(21)出願番号　特願2003-322622 (P2003-322622)
(22)出願日　平成15年9月16日 (2003.9.16)
(65)公開番号　特開2005-94184 (P2005-94184A)
(43)公開日　平成17年4月7日 (2005.4.7)
審査請求日　平成18年9月15日 (2006.9.15)

(73)特許権者　509111836
小川　均
京都府長岡京市高台４－３－１３
(73)特許権者　509111847
西村　俊和
滋賀県草津市西大路町２－３３－６０１
ロン・ラヴィーヌ
(73)特許権者　509110600
前田　忠彦
滋賀県草津市野路１－１４－３８－８０１
(74)代理人　100094248
弁理士　楠本　高義

最終頁に続く

(54)【発明の名称】統合無線認証システム

(57)【特許請求の範囲】
【請求項１】
イーサネットフレームを受信する無線通信部と、
前記無線通信部が受信したイーサネットフレームを認証するＬＡＮ認証器を備えたＬＡＮ認証部と、
前記ＬＡＮ認証部において、認証されたイーサネットフレームの通信量を計測するトラフィックス計測器と、
前記ＬＡＮ認証部において、認証に失敗したイーサネットフレームの通信量を計測するトラフィックス計測器と、
前記認証に失敗したイーサネットフレームの帯域を制御する帯域制御装置と、
認証されたイーサネットフレームの通信量と認証に失敗したイーサネットフレームの通信量の割付け比率から、前記帯域制御装置を制御する割付け比率制御装置と、
前記ＬＡＮ認証部が認証に失敗したイーサネットフレームを該ＬＡＮ認証部から受信し、該イーサネットフレームをＩＰカプセル化されたデータグラムとし、該データグラムのＩＰヘッダをＶＰＮサーバ宛のＩＰヘッダに書き換えるリダイレクト手法により送信するＶＰＮクライアントと、
を備えた無線インターネット接続装置を含み、
前記ＩＰカプセル化されたデータグラムをインターネットを介して受信するＶＰＮサーバと、
前記ＶＰＮサーバから前記ＩＰカプセル化されたデータグラムを送信可能な、インターネ

ットと隔離されたＶＰＮと、
前記ＶＰＮを介して前記ＩＰカプセル化されたデータグラムを受信し、これを前記イーサネットフレームへ変換し、該イーサネットフレームを公衆無線で利用可能の認証を実行する公衆無線認証部と、
前記公衆無線認証部において認証に成功した前記イーサネットフレームを受信し、インターネットに接続する公衆無線ルータと、
を備えたインターネット中継装置を複数含み、ＬＡＮ認証部および各公衆無線認証部で異なる認証をおこない、
前記帯域制御装置と割付け比率制御装置は、認証に失敗したイーサネットフレームの通過に対して、認証されたイーサネットフレームの通過を優先することを特徴とし、
前記無線通信部はアンテナ、高周波部、無線信号処理部、およびテーブルを備え、
前記テーブルには、サービスエリア内の無線ＬＡＮクライアントの電波の特徴および情報が蓄積され、
前記テーブルを利用して高周波部と無線信号処理部がアンテナの指向性を制御し、
前記ＬＡＮ認証部で認証をおこなうパケットが通過し、認証過程での重要度の識別をおこない、
前記アンテナの指向性の制御は、前記認証をおこなうパケットが発射する場合に、認証をおこなう無線ＬＡＮクライアントの方向に主ビームを向け、かつ、前記割付け比率に応じて認証に失敗したイーサネットフレームの通信量を制限するようにおこない、
統合無線認証システム。

【請求項２】
前記ＩＰヘッダの書き換えられるデータグラムを適切なＶＰＮへ送信するために、前記公衆無線認証部が実行する公衆無線で利用可能の認証の情報によって適切なＶＰＮサーバアドレスが得られることを特徴とする請求項１に記載の統合無線認証システム。

【請求項３】
前記公衆無線認証部の実行する認証によって無線利用者を特定することを特徴とする請求項２に記載の統合無線認証システム。

【請求項４】
前記ＶＰＮクライアントにおいて、得られた請求項２に記載の適切なＶＰＮサーバアドレスを期限付きに記録することを特徴とする請求項２または３に記載の統合無線認証システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電磁波を利用したインターネット接続において、耐妨害・侵入性を実現するための無線共用システムに関する。

【背景技術】
【０００２】
近年、光ファイバ網が発達し、商業ビルを始め、居住マンションや一般住宅へ光ファイバが引かれている。従来は、光ファイバからルータまたはファイアウォールを介して、インターネットがイントラネットに繋がっている。最近は、光ファイバにかわって配線が不要な無線ルータが普及してきている。特に、無線ＬＡＮは一般の住宅における利用が多く見られる。

【０００３】
無線ＬＡＮの利点は、単にケーブルを引き回す手間が省けることだけでなく、無線が届く場所であれば原則的に何処でも利用できることにある。そのため、駅構内や喫茶店等の不特定多数の人が集まるところでは、無線ＬＡＮとノートパソコンの組合せはインターネット利用の方法として適切な環境を提供しているといえる。

【０００４】
しかしながら、このような無線ＬＡＮを利用するには、その無線ＬＡＮの管理者が発行

する、または、予め認めているＩＤ取得者のみが利用可能である（例えば特許文献１参照）。したがって、異なる管理の無線ＬＡＮを利用するためには異なるＩＤが必要となり、位置透過性が特徴であるＬＡＮの有効性を生かすことが出来ない状態となっている。さらに、無線ＬＡＮを一般的に提供している業者の設備がない一般住宅地では、各戸では無線ＬＡＮが利用されている場合でも、一般的には他の人が使えない状況となっている。

【０００５】

たとえば、各無線ルータを誰でも利用できるように設定することは可能であるが、そうした場合、各無線ルータの所有者の機器構成等の情報が公開となり、接続機器の無断使用・ファイル等の覗きなどプライベートが守られない状況となる。このことがアクセスポイントの乱立をまねき、相互に干渉を発生させ不要な電波の発射をおこすため、周波数の有効利用を大きく妨げてきている。また、無線ＬＡＮ使用者がインターネット内で迷惑行為を行った場合、外部からは無線ルータ所有者が行った行為と区別が付かず、迷惑行為の責任を追及するのは困難となる。

【０００６】

一方、無線通信は本質的には傍受される特質をもっていることは否めない。このために指向性を制御して不要な方向への電波の放射を抑圧する方法が考えられるが、本提案で考えている公衆無線ＬＡＮシステムに適応するには、以下のような問題点を有する。

【０００７】

すなわち、無線において特定の方向に電波を放射するためにはアンテナや高周波ブロックのリソースを多く必要とし、全てのトラフィックに対して指向性制御を適応することは、無線ルータが大型化し経済的にも問題である。したがって、必要なセキュリティーレベルを判断し、アンテナや高周波ブロックのリソースを適応的にスケジューリングする必要がある。

【０００８】

ところが、このセキュリティーレベルの判断はアプリケーションと密接に関連するため、物理レベルに近いレイヤだけの情報では適切な判断を下すことができないという問題点がある。従って従来の技術では、問題となるセキュリティーレベルを判断した上で合理的にアンテナや高周波ブロックのリソースを配分することができず、公衆無線ＬＡＮシステムの普及の大きな障害となっていた。

【０００９】

一方で、従来の無線周波数の管理はシステムごとに周波数を割り付ける、という方針のもとになされてきた。このため、アクセスポイントを設置したものが独占的にその周波数を使用することが起きている。このため、干渉局と共存できず、また認証などの重要な通信事項に対して有効な秘匿手段を提供できなかったという歴史的背景がある。そのため、独占的な電波の使用を排除し空間的にしかも適応的に周波数資源を管理し有効活用しようとする考えに基づく「アンテナ制御を含めた認証によるアクセスポイントの共用」という発想が必要である。しかし、これまでそのような技術が発表されたことはなかった。

【００１０】

この問題を解決するための一つの切り口としてアンテナシステムと認証システムを連携させる方法が考えられる。アンテナは、電波を空間に対して放射制御できる唯一の装置であり、電波の空間的分布を物理的に変更できる素子である。即ち、アンテナシステム以外のいかなる部分も空間に放射する電波の分布を制御することは出来ない。しかし、従来の技術ではアンテナシステムの制御は認証制御という上位のアプリケーションからの要求により適応的な制御がなされてはいなかった。

【００１１】

よって、従来の方法では、アプリケーションの要求からくるセキュリティーレベルを維持しつつ統合的な周波数資源の空間的高効率利用の実現が困難であり、将来のワイヤレス高速通信の大きな障害になっていた。即ち従来は、無線ルータ所有者の機器等のセキュリティと利便性を完全に確保しつつ、不特定多数に対する無線ＬＡＮの利便性を追求する無線ＬＡＮルータにより無線設備を共用し、周波数資源を共有することによりアクセスポイ

ントの有効利用をはかることができないという問題点があった。
【００１２】
【特許文献１】特開平２００２－１５２２７６号公報（図１）
【発明の開示】
【発明が解決しようとする課題】
【００１３】
上記課題を解決するため、本発明の提供する統合無線認証システムは、各無線ルータの所有者の機器構成等のプライバシーを保護しつつ、各無線ルータの所有者以外の無線ＬＡＮ使用者が当該各無線ＬＡＮを利用してインターネットにアクセス可能とすることを目的とする。
【００１４】
また、本発明の統合無線認証システムは、無線ＬＡＮ使用者が使用する使用電波の空間的、時間的、及び優先順序を管理するテーブル及び無線通信における当該通信相手の識別符号あるいは名称と電波の強さ、変調方式、方位角、仰角をテーブルとしてもつ統合無線認証システムを提供する。
【００１５】
更に本発明の統合無線認証システムは、無線通信システムに対して送受信もしくは送信または受信のどちらか一方を行うためのアンテナと無線周波数受信装置、あるいは無線周波数送信装置を、前記無線通信システムの送信と受信毎に使用電波の周波数、およびそれらの空間的な分布を制御する周波数ビーム空間割付制御機能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】
上記課題を解決するため、本発明の統合無線認証システムは、イーサネットフレームを受信する無線通信部と、前記無線通信部が受信したイーサネットフレームを認証するＬＡＮ認証部と、前記ＬＡＮ認証部が認証に失敗したイーサネットフレームを該ＬＡＮ認証部から受信し、該イーサネットフレームをＩＰカプセル化されたデータグラムとするＶＰＮ(Virtual Private Network)クライアントと、を備えた無線インターネット接続装置を含む。以下本明細書において、認証に失敗したイーサネットフレームをＩＰカプセル化したものを、ＩＰカプセル化されたデータグラムという。
【００１７】
本発明の統合無線認証システムは、前記ＩＰカプセル化されたデータグラムをインターネットを介して受信するＶＰＮサーバと、前記ＶＰＮサーバから前記ＩＰカプセル化されたデータグラムを送信可能な、インターネットと隔離されたＶＰＮと、前記ＶＰＮを介して前記ＩＰカプセル化されたデータグラムを受信し、これを前記イーサネットフレームへ変換し、該イーサネットフレームを公衆無線で利用可能の認証を実行する公衆無線認証部と、前記公衆無線認証部において認証に成功した前記イーサネットフレームを受信し、インターネットに接続する公衆無線ルータと、を備えたインターネット中継装置を含み得る。
【００１８】
本発明の統合無線認証システムは、前記無線通信部は高周波部又は無線信号処理部を備え、該高周波部又は無線信号処理部を外部装置から制御するためのインターネットプロトコルによる通信路は、前記公衆無線認証部が使用する通信路とは別に設けられることを特徴とする。
【００１９】
本発明の統合無線認証システムは、前記無線通信部はアンテナを有し、前記無線通信部の高周波部又は無線信号処理部を、前記インターネットプロトコルによる通信路を介して、前記外部装置により、前記アンテナの放射特性を遠隔的に制御することを特徴とする。
【００２０】
本発明の統合無線認証システムは、前記ＩＰカプセル化されたデータグラムを適切なＶ

ＰＮへ送信するために、公衆無線で利用可能の前記公衆無線認証部の実行する認証の情報によって適切なＶＰＮサーバアドレスが得られることを特徴とする。

【００２１】

本発明の統合無線認証システムは、前記公衆無線認証部の実行する認証によって無線利用者を特定することを特徴とする。

【００２２】

本発明の統合無線認証システムは、前記公衆無線認証部の実行する認証により、インターネットでの迷惑行為等利用者の責任と利用資源に応じた課金を可能とすることを特徴とする。

【００２３】

従って本発明の統合無線認証システムは、有線ネットワークを利用することが許可されていない無線ＬＡＮクライアントのイーサネットフレームをインターネットに送信することが可能な統合無線認証システムであり、無線ＬＡＮクライアントからインターネットに送信されたイーサネットフレームが必ずＬＡＮ認証装置あるいは公衆無線認証装置いずれかによって正当な利用者であることが認証によって保証され、公衆無線認証装置によって認証された利用者が行ったインターネット内での迷惑行為を無線ルータ所有者が行った行為と容易に区別でき、従って迷惑行為の責任の追及が可能となる。

【００２４】

本発明の統合無線認証システムは、前記ＩＰカプセル化されたデータグラムの通過に対して、請求項１に記載のＬＡＮ認証部において認証に成功した内部フレームの通過を優先することを特徴とする。

【００２５】

即ち、本発明では、無線通信アクセスポイントが接続されている有線ネットワークを利用することが許可された無線ＬＡＮクライアントのイーサネットフレーム送信をＩＰカプセル化されたデータグラムに対して優先し、利便性を保証する。

【００２６】

本発明の統合無線認証システムは、前記ＶＰＮクライアントにおいて、得られた適切なＶＰＮサーバアドレスを期限付きに記録することを特徴とする。

【００２７】

本発明の統合無線認証システムは、前記ＬＡＮ認証部が認証に成功したイーサネットフレームの通過を表示する内部フレーム表示部と、前記ＬＡＮ認証部が認証に失敗したイーサネットフレームの通過を表示する外部フレーム表示部と、を具備するフレーム通過表示部を備えたフレーム通過表示装置を含み得る。

【００２８】

本発明の統合無線認証システムは、前記フレーム通過表示装置が更に、前記公衆無線認証部により認証されたイーサネットフレームにより通信中の局数を表示する局数表示部と、前記認証に成功したイーサネットフレームと認証に失敗したイーサネットフレームの割付け比率を変更することのできる比率変更手段と、を具備し得る。

【００２９】

従って本発明では、上記課題を解決するため、正当な有線ＬＡＮ使用者でない者を認証した公衆無線認証装置と連結するＶＰＮサーバをＶＰＮクライアント装置に記録し、新たな認証作業への利用とその効率化とあいまって、ＶＰＮサーバの記録を時限的とすることにより公衆無線認証装置に認証された利用者による装置の専有化を防ぐと共に、当該利用者のプライバシーは守られる。

【００３０】

本発明の統合無線認証システムは、前記フレーム通過表示装置が更に、前記無線通信部に接続されたアンテナの向きを変更できる機構を具備し得る。

【００３１】

本発明の統合無線認証システムは、前記フレーム通過表示装置が更に、前記無線通信部に接続されたアンテナに平行に金属物を配置し、前記金属物と前記アンテナの相互の位置

関係を変更するか、又は、前期位置関係を保ったまま前記アンテナと前記金属物の全体を回転あるいは角度の変更ができる機構を具備したことを特徴とする。前記金属物は金属板あるいは金属線であり得る。

【００３２】

本発明の統合無線認証システムは、前記フレーム通過表示装置が更に、前記内部フレーム及び外部フレームの割付け比率の設定値又は目標値となるよう前記無線通信部のアンテナの指向性制御を行うことを特徴とする。

【００３３】

即ち本発明の統合無線認証システムは、無線通信システムに対して送受信もしくは送信または受信の何れか一方を行うためのアンテナと無線周波数受信装置を備え、無線周波数送信装置を、上記無線通信システムの送信と受信毎に使用電波の周波数及び使用電波の空間的な分布を制御する周波数ビーム空間割付制御機能を備える。そして本発明の統合無線認証システムは、使用電波の空間的、時間的、および優先順序を管理するテーブルを備え、無線通信における当該通信相手の識別符号又は名称と電波の強さ、変調方式、方位角、仰角をテーブルとして有する。

【００３４】

従って本発明の統合無線認証システムは、送受信される無線周波数資源の分配管理を認証過程での要求条件を参照し、そのビーム制御および周波数資源の空間割り当てを行なうことができる。本発明の統合無線認証システムは、アプリケーションの要求に応じた認証過程における秘匿性を保ちつつ、有効な周波数資源の利用を図ることができる。

【発明の効果】

【００３５】

貸借有線ＬＡＮの正規利用者の通信は無線通信部からＬＡＮ認証部へ送られ、そのままＬＡＮ内機器やインターネットに接続可能である。そうでない利用者通信はＬＡＮ認証部からＶＰＮクライアント、ついで同サーバへ送られるのでＬＡＮ内機器に影響せず、ＬＡＮ内機器等正規利用者のプライバシーは安全である。公衆無線認証装置で認証されれば、同通信はインターネットを利用可能である。さらに、認証過程の重要部分をアンテナ制御によって所望の局へ集中および対象外局へのビームの低減をおこない物理レベルでのセキュリティーを高めることができる。

【００３６】

以下に、本発明の統合無線認証システムの実施形態を図面を参照して説明する。

【発明を実施するための最良の形態】

【００３７】

図１は本発明の第一の実施形態を示す統合無線認証システムのブロック図である。インターネット１１２にインターネット上のサーバ１２３が接続されていて、あるインターネット利用者が自身所有の有線ＬＡＮ１１１をインターネットサービスを提供するブロードバンドルータ１２１を介してインターネット１１２に接続しているとする。またＬＡＮ内機器１２２は本来この利用者のみが専有して利用すべき機器であるとする。

【００３８】

本発明の統合無線認証システムを実施する機器は無線インターネット接続装置１０１と、インターネット中継装置１０２と、ＶＰＮサーバ表１０３と、からなる。それぞれ無線インターネット接続装置１０１は有線ＬＡＮ１１１、インターネット中継装置１０２とＶＰＮサーバ表１０３はインターネット１１２に接続されている。

【００３９】

有線ＬＡＮ１１１の所有者あるいは所有者の許可を得た無線インターネット接続装置１０１の利用者(以下正当な有線ＬＡＮ利用者と表記。)は、無線インターネット接続装置１０１を構成する無線通信部１０１ａと、電磁波を用いて通信可能な無線ＬＡＮクライアント１００を用いてＬＡＮ内機器１２２あるいはインターネット上のサーバ１２３と通信を行い、そのサービスを享受することになる。正当な有線ＬＡＮ利用者の用いる無線ＬＡＮクライアント装置１００はＭＡＣアドレス登録等の手法により認証可能であるとする。

【００４０】
正当な有線ＬＡＮ利用者の無線ＬＡＮクライアント装置１００がＩＰ（インターネットプロトコル）通信を行うことを考える。無線ＬＡＮクライアント装置１００のデータグラムは、通常通りイーサネット（Ｒ）のフレーム(以下イーサネットフレームと表記。)に乗せられて、無線通信部１０１ａへ届く。無線通信部１０１ａで受信されたイーサネットフレームは、無線インターネット接続装置１０１内部のＬＡＮ認証部１０１ｂに送られる。
【００４１】
ＬＡＮ認証部１０１ｂでは、上記の方法でイーサネットフレームの認証を行い、認証に成功したものは直接有線ＬＡＮ１１１へ送るものとする。これによって、正当な有線ＬＡＮ利用者の無線ＬＡＮクライアント装置１００は通常通り有線ＬＡＮ１１１と通信でき、従って、ＬＡＮ内機器１２２のサービスを享受することができる。また、有線ＬＡＮ１１１に接続されたブロードバンドルータ１２１を用いてインターネット１１２に接続でき、よってインターネット上のサーバ１２３のサービスを享受することもできる。尚、本発明においてルータはＩＰルータであれば、ブロードバンドルータ１２１に特に限定されるものではない。
【００４２】
正当な有線ＬＡＮ利用者でない者(以下本明細書において、正当な有線ＬＡＮ利用者以外の者を言う)の無線ＬＡＮクライアント装置１００のイーサネットフレームは、上記認証を成功させることはできない。ここでは認証に失敗したイーサネットフレームを破棄せずに、ＬＡＮ認証部１０１ｂからＶＰＮクライアント１０１ｃへ送り、ここで当イーサネットフレームＧＲＥ(Generic Routing Encapsulation)等の手法でＩＰカプセル化し、特定のＶＰＮサーバ１０２ａ宛のＩＰヘッダをつけるものとする。ＩＰカプセル化によって当イーサネットフレームはデータグラムのデータ部となるため、これを有線ＬＡＮ１１１へ送信しても他のＬＡＮ内機器１２２やインターネット上のサーバ１２３には到達できず、そのままブロードバンドルータ１２１を通じてＶＰＮサーバ１０２ａへ送信されることになる。
【００４３】
以下、本明細書において、ＶＰＮクライアント１０１ｃとＶＰＮサーバ１０２ａの上記働きをトンネリングと称する。よって、正当な有線ＬＡＮ利用者でない者の無線ＬＡＮクライアント装置１００がインターネット１１２に作用したり、ブロードバンドルータ１２１を介して直接インターネット上のサーバ１２３のサービスを利用することはありえない。
【００４４】
ＩＰカプセル化されたデータグラムはＶＰＮサーバ１０２ａにより、インターネット１１２と隔離されたＶＰＮ(Virtual Private Network)１１３へ送信され、イーサフレームへ変換される。このイーサフレームをさらに公衆無線で利用可能かどうか公衆無線認証部１０２ｂで認証するものとする。以下、公衆無線認証部１０２ｂでの認証を公衆無線認証と称する。
【００４５】
認証機構や方式の原理は前述のＬＡＮ認証部１０１ｂと同様である。公衆無線認証できないイーサネットフレームは破棄し、認証済みイーサネットフレームのみを対象とし、そのデータグラムを公衆無線ルータ１０２ｃを通じてインターネット１１２へ送信する。これにより、インターネット１１２上のサーバ１２３へ到達可能なデータグラムは、ＬＡＮ認証部１０１ｂあるいは公衆無線認証部１０２ｂのいずれかで必ず認証されていることが保証される。よって認証結果に応じて、インターネットでの迷惑行為等利用者の責任の追及と利用資源に応じた課金が可能となる。
【００４６】
ＶＰＮクライアント１０１ｃは同時に複数のＶＰＮサーバ１０２ａとトンネリングすることが可能であるので、複数のインターネット中継装置１０２を設置して、それぞれ異なった公衆無線認証を行うことができる。例えば組織ごとに組織構成員を認証するインター

ネット中継装置１０２を設置すれば、ＶＰＮクライアント１０１ｃは異なった組織の無線ＬＡＮクライアント装置１００の利用者それぞれに対して適切にトンネリングでき、従って組織ごとに認証された利用者が同時にインターネット接続を享受できる。

【００４７】

ＶＰＮサーバ表１０３は、複数の利用者それぞれについて公衆無線認証を行うべき対応表を保持するサーバであり、適切なＶＰＮサーバ１０２ａの識別子とＶＰＮサーバ１０２ａへのトンネリング方法を各ＶＰＮクライアント１０１ｃの要求に応じて提供するものである。ここで各ＶＰＮクライアント１０１ｃの要求とは、無線ＬＡＮクライアント装置１００のユーザを認証可能なＶＰＮサーバ１０２ａを探したいという要求である。

【００４８】

本発明においては、利用者や無線ＬＡＮクライアント装置１００は利用にあたって、ＬＡＮ認証部１０１ｂに必ず認証情報を送信しなければならない。無線ＬＡＮクライアント装置１００の利用者が正当な有線ＬＡＮ利用者でない場合、ＬＡＮ認証部１０１ｂにどのような認証情報を送信しても認証を成功させることはあり得ないと考えられる。従って本発明ではＬＡＮ認証部１０１ｂに送信する認証情報として、公衆無線認証部１０２ｂで実行する認証の情報およびＶＰＮサーバ表１０３を用いて認証可能なＶＰＮサーバ１０２ａの識別子とトンネリングの方法を得るための情報を結合した情報を送るものとする。これによって、ＬＡＮ認証部１０１ｂでの認証が失敗した場合、ＬＡＮ認証部１０１ｂに送信された結合情報を用いてＶＰＮクライアント１０１ｃがＶＰＮサーバ表１０３の表引きを行えば直ちに認証可能なＶＰＮサーバ１０２ａの識別子とトンネリングの方法が得られる。すなわち、ＩＰカプセル化されたデータグラムを適切なＶＰＮ１１３へ送信するために公衆無線認証部１０２ｂの実行する認証の情報によって適切なＶＰＮサーバアドレスを得るためには、ＶＰＮサーバ表１０３を用いて認証可能なＶＰＮサーバ１０２ａの識別子とトンネリングの方法を得るための情報を、公衆無線認証部１０２ｂで実行する認証の情報に含ませておけばよい。上述のような結合された認証情報の具体例を以下に説明する。

【実施例１】

【００４９】

複数のＶＰＮサーバ１０２ａにて互いに同じ認証情報を用いないようにすれば、ＶＰＮサーバ表１０３の表引きによって認証可能なＶＰＮサーバ１０２ａの識別子とトンネリングの方法が得られる。まず、同じ認証情報を用いる例を以下に示す。

（例）

Ａ大学ＶＰＮサーバ: 認証情報 nisimura

Ｂ大学ＶＰＮサーバ: 認証情報 nisimura

この例では、認証情報nisimura に対して複数のＶＰＮサーバが対応しているため、認証情報だけでは一意にＶＰＮサーバを定めることは出来ない。

【００５０】

同じ認証情報を用いないようにするためにはさまざまな方法があるが、ここでは例えば１の手順で認証情報ｘを、２の手順で認証情報ｙを認証情報ｘに結合して認証情報ｙ／ｘを作成する。

1．ＶＰＮサーバに一意な名前をつける。これは上記ｘの情報である。このとき名前ｘとＶＰＮサーバ１０２ａの対応はＶＰＮサーバ表１０３に記録しておく。

（例）

Ａ大学ＶＰＮサーバ: Ａ’ｓ

Ｂ大学ＶＰＮサーバ:Ｂ-u

2．認証情報ｘにｙを結合する。

（例）

Ａ大学のnisimuraさんの認証情報: nisimura/Ａ’ｓ

Ｂ大学のnisimuraさんの認証情報: nisimura/Ｂ-u

以上二手順より、認証情報から一意にＶＰＮサーバが特定できるような認証情報が構成できる。

【００５１】
なお、以下のような変更、追加等を行っても、本発明の効果は同様である。
【００５２】
ＩＰカプセル化の手法は例としてＧＲＥを挙げたが、EtherＩＰやＩＰv６-over-ＩＰv４ configured tunnel等、ＶＰＮクライアント１０１ｃとＶＰＮサーバ１０２ａ間でＩＰを用いてトンネリング可能な別手法を用いてもよい。
【００５３】
無線ＬＡＮクライアント装置１００と無線インターネット接続装置１０１間の通信、さらにトンネリングを介して無線ＬＡＮクライアント装置１００とＶＰＮ１１３の通信にはイーサネットフレームを利用したが、利用可能なパケット型データ通信方式であればパケットあるいはフレーム、あるいはデータグラムいずれを用いても同じ効果が得られる。特にデータグラムを用いる場合には、ＩＰヘッダを書き換えて特定アドレスにデータグラムを送信するリダイレクト手法をトンネリングの代わりに利用してもよい。
【００５４】
ＶＰＮ１１３はＶＰＮサーバ１０２ａと公衆無線認証部１０２ｂ間でイーサネットフレームによるデータ通信ができれば十分で、データ通信を行う物理線かあるいはそれを模擬する別装置を用いても同じ効果が得られる。また、ＬＡＮ認証部１０１ｂとＶＰＮクライアント１０１ｃとはいずれも有線ＬＡＮ１１１と接続されていればよく、その接続線は互いに分離していても共用しても構わない。
【００５５】
更に、ＶＰＮサーバ表１０３を利用するのはＶＰＮクライアント１０１ｃのみであるので、ＶＰＮサーバ表１０３はＶＰＮクライアント１０１ｃからアクセスできれば十分である。例えば各無線インターネット接続装置１０１専用のＶＰＮサーバ表１０３が有線ＬＡＮ１１１に接続されていてもよいし、無線インターネット接続装置１０１に内蔵されていてもよいし、無線ＬＡＮクライアント装置１００に内蔵されていてもよい。
【００５６】
ＬＡＮ認証部１０１ｂや公衆無線認証部１０２ｂでの認証は、上記説明では各無線ＬＡＮクライアント装置１００のＭＡＣアドレスが世界唯一であることを利用して、事前登録したＭＡＣアドレスを持つイーサネットフレームのみを認証が成功したものとみなすことにしているが、他の方法でも本発明の効果は変わらない。例えばPoint-to-Point Protocol over Ｅｔｈｅｒｎｅｔ（Ｒ）のように、事前登録したＩＤとパスワードを接続時にユーザに入力させて認証を行う方式でも構わないし、IEEE８０２.1Xのような認証スキームを利用してもよい。
【００５７】
図２は本発明の上記実施形態とは別の実施形態を示す統合無線認証方式のブロック図であり、図１におけるＶＰＮサーバ表１０３が無線インターネット接続装置１０１に内蔵されている場合の実施形態を表す。図２においては、インターネット２１２にインターネット上のサーバ２２３が接続されていて、あるインターネット利用者が自身所有の有線ＬＡＮ２１１を、インターネットサービスを提供するブロードバンドルータ２２１を介してインターネット２１２に接続しているとする。またＬＡＮ内機器２２２は本来この利用者のみが専有して利用すべき機器であるとする。この時本発明を実施する機器は無線インターネット接続装置２０１とインターネット中継装置２０２からなり、それぞれ無線インターネット接続装置２０１は有線ＬＡＮ２１１、インターネット中継装置２０２はインターネット２１２に接続されている。
【００５８】
正当な有線ＬＡＮ利用者が無線インターネット接続装置２０１を構成する無線通信部２０１ａと電磁波を用いて通信可能な無線ＬＡＮクライアント装置２００を用いてＬＡＮ内機器２２２あるいはインターネット上のサーバ２２３と通信を行い、そのサービスを享受する内容とその効果は本発明の上記実施形態と同じである。正当な有線ＬＡＮ利用者の無線インターネット接続装置２００のデータグラムはイーサネットフレームに乗せられて、

無線通信部２０１ａへ届き、無線インターネット接続装置２０１内部のＬＡＮ認証部２０１ｂで認証され、認証に成功したものは直接有線ＬＡＮ２１１へ送られる。

【００５９】

正当な有線ＬＡＮ利用者でない者の無線インターネット接続装置２００のイーサネットフレームは上記認証に失敗するため、これをＬＡＮ認証部２０１ｂからＶＰＮクライアント２０１ｃへ送ってＩＰカプセル化し、特定のＶＰＮサーバ２０２ａ宛のＩＰヘッダをつける内容とその効果は本発明の上記実施形態と同じである。

【００６０】

ＩＰカプセル化されたデータグラムを無線通信部２０１ａにより、インターネット２１２と隔離されたＶＰＮ２１３へ送信し、変換したイーサネットフレームを公衆無線認証部２０２ｂで公衆無線認証し、認証済みイーサネットフレームのデータグラムのみを公衆無線ルータ２０２ｃを通じてインターネット２１２へ送信する内容とその効果は本発明の上記実施形態と同じである。

【００６１】

本発明の上記実施形態と同様、ＶＰＮクライアント２０１ｃは同時に複数のＶＰＮサーバ２０２ａとトンネリングすることが可能であるので、複数のインターネット中継装置２０２を設置して、それぞれ異なった公衆無線認証を行うことができる。また、ＶＰＮサーバ表２０１ｄは、複数の利用者それぞれについて公衆無線認証を行うべき対応表を保持し、適切なＶＰＮサーバ２０２ａの識別子とそのトンネリング方法をＶＰＮクライアント２０１ｃの要求に応じて提供するものである。

【００６２】

以下、本発明の上記実施形態において、ＬＡＮ認証部１０１ｂ、２０１ｂ、及び無線通信部１０１ａ、２０１ａの具体的な実施例を図３～図９を用いて説明する。

【実施例２】

【００６３】

図３は本発明においてＬＡＮ認証部で認証されたイーサネットフレームをそうでないイーサネットフレームに優先して送受信する機構を説明する図である。図３は図１のＬＡＮ認証部１０１ｂ又は図２のＬＡＮ認証部２０１ｂの内部を拡大したものである。すなわちＬＡＮ認証部３００は三つの装置と二つの計測器からなり、図１の無線通信部１０１ａあるいは図２の無線通信部２０１ａと同じ働きを行う無線通信部３２１に接続されている。

【００６４】

また、ここで認証に失敗したイーサネットフレームを送信するＶＰＮクライアントは図１のＶＰＮクライアント１０１ｃあるいは図２のＶＰＮクライアント２０１ｃと同じ働きを行うＶＰＮクライアント３２２である。ＬＡＮ認証部１０１ｂ、２０１ｂの働きを実質的に行う装置をＬＡＮ認証器３０１と呼ぶ。すなわち３０１の働きは実施例１または２におけるＬＡＮ認証部１０１ｂ、２０１ｂの働きと同じである。

【００６５】

ＬＡＮ認証器３０１で認証されたイーサネットフレームは図１の有線ＬＡＮ１１１、図２の有線ＬＡＮ２１１と同様に有線ＬＡＮ３３１へ送られる。ＬＡＮ認証器３０１と有線ＬＡＮ３３１との間のイーサネットフレーム量はトラフィックス計測器３１２で測定され、その測定結果は割付け比率制御装置３０２へ送られる。

【００６６】

同様にＬＡＮ認証器３０１は帯域制御装置３０３を介してＶＰＮクライアント３２２と接続されており、ＬＡＮ認証器３０１で認証に失敗したイーサネットフレームはＶＰＮクライアント３２２へ送られる。ＬＡＮ認証器３０１と帯域制御装置３０３との間のイーサネットフレーム量はトラフィックス計測器３１１で測定され、その測定結果は割付け比率制御装置３０２へ送られる。

【００６７】

本発明の第一の実施形態および第二の実施形態によればトラフィックス計測器３１２の測定結果が正当な利用者の通信量であり、トラフィックス計測器３１１の測定結果が正当

な利用者でない者の通信量である。従って、両者の割合を勘案して後者が減少するように制御を行えば、ＬＡＮ認証部で認証されたイーサネットフレームを認証されない（即ち、認証に失敗した）イーサネットフレームに優先して送受信することが可能となる。割付け比率制御装置３０２はその割合勘案を行うための制御装置であり、正当な利用者でない者の通信量は帯域制御装置３０３によって減少させることが可能である。従って正当な利用者の通信を優先させるためには、割付け比率制御装置３０２で帯域制御装置３０３を制御すればよい。帯域を制御する方法はClass Based Queuing、TCPレートコントロール、遅延やフレーム損失の挿入等を用いればよい。すなわち、無線インターネット接続装置において認証されたイーサネットフレームを優先することが可能となる。

【００６８】

なお、原理上通信路上に帯域制御装置３０３を挟めば帯域を制御することが可能であるので、帯域制御装置３０３の機能がＶＰＮクライアント３２２あるいは図１のＶＰＮサーバ１０２ａあるいは図２のＶＰＮサーバ２０２ａに含まれていても、本発明の効果は変わらない。

【実施例３】

【００６９】

図４は本発明の認証過程におけるアンテナ制御を説明する図である。図４における無線通信部４０１は図１における無線通信部１０１ａ及び図２における無線通信部２０１ａに対応し、単数あるいは複数のアンテナ４０２、単数あるいは複数の高周波部４０３、無線信号処理部４０４とテーブル４０５によって構成される。指向性の制御を行うためには複数のアンテナを用いることが有利であることは自明である。高周波部４０３又は無線信号処理部４０１を外部装置から制御するためのインターネットプロトコルによる通信路は、図１及び図２に示す公衆無線認証部１０２ｂ、２０２ｂが使用する通信路とは別に設けられる。無線通信部４０１はアンテナを有し、当該無線通信部４０１の高周波部４０３又は無線信号処理部４０４を、上記インターネットプロトコルによる通信路を介して、上記外部装置により、無線通信部４０１の有するアンテナの放射特性を遠隔的に制御する。

【００７０】

また、指向性の制御を無線通信において行うことも従来の技術で自明であるが、発明が解決しようとする課題で説明したように、従来の技術では無線ＬＡＮルータ所有者の機器のセキュリティーと利便性を確保しつつ無線ＬＡＮルータにより無線設備を共用し、周波数資源を共有することによりアクセスポイントの有効利用を図ることはできなかった。その理由はアンテナ制御とセキュリティーに関わる認証の過程が連動していなかった点である。

【００７１】

本発明ではアンテナで受信される無線信号の強度や頻度、パケット平均長および方位などの特徴をテーブル４０５に記憶しておく。ＬＡＮ認証部は認証過程に関わるパケットが通過し、認証過程での重要度の識別が可能である。高周波部４０３では無線信号処理部４０４と協調して指向性の制御をおこなう。以下その手順を説明する。

【００７２】

アンテナ４０２では正当な有線ＬＡＮ利用者とＬＡＮを貸借して使用する正当な有線ＬＡＮ利用者でない者の両者の電波が受信されるが、本発明の無線ＬＡＮシステムでは正当な有線ＬＡＮ利用者でない者が発射する電波の頻度を直接的に制御することなくアンテナ４０２によって抑圧し、正当な有線ＬＡＮ利用者のアクセスを有利となるよう制御をおこなう。このとき指向性の制御のための計算は時間の掛かるものがあるが、これは事前の電波の聴取と監視によりあらかじめサービスエリア内に存在する無線ＬＡＮクライアントの電波の強度などの特徴をテーブル４０５に蓄積しておき、指向性制御のためのアダプティブ処理における初期値を決定するために利用する。

【００７３】

特に、重要な認証パケットを発射する場合には、当該無線ＬＡＮクライアントの方向に主ビームを向ける指向性により通信する。また、あらかじめ取得してあるテーブルの蓄積

結果にはＬＡＮ認証部で認証されず、正当な有線ＬＡＮ利用者でない者の発射局に関わる電波の情報も記録される。また正当な有線ＬＡＮ利用者でない者であって公衆無線認証部で認証されなかった利用者の発射局に関わる電波の情報も記録される。この記録により不適切局方向に認証過程での重要情報を与えないような指向性制御をおこなうことが可能となる。

【００７４】

一方で電波の干渉の状況は場所と周囲の無線局の電波の発射状況によって大きく異なっており、当該受信局の位置だけではなく、周囲の無線局のビーム形成の状態も、当該受信局が特定の電波を受信出来るか否かに大きな影響を与える。この点を鑑みると、信頼できる周囲の無線局とは電磁波の発射の一部の情報を共有することが、当該無線ゾーンでの周波数利用効率を高められる。ただし、この情報交換はあくまでも認証過程とは何らかの手段によって隔離された通信路であることがセキュリティー上のぞましい。このような通信路が確保できるときは、周囲にある複数の統合無線認証システムを利用した無線通信部が協調してビーム制御を行うことが可能である。

【００７５】

なお、このような指向性制御を常時行うことも可能であるが、これには次の２点によりその常時指向性制御をおこなうか否かが決められる。まず、常時指向性制御には無線信号処理部と高周波部のリソースを多く使用することになるという問題があり、その無線信号部と高周波部のハードウエアの規模とトラフィックに依存する。また前記不適切局の方向に適正な局が存在する場合に常時当該方向に抑圧指向性を形成するのは適切とは言いがたい。

【００７６】

本発明においては無線でのトラフィックの状況を把握できるだけでなく、無線通信部４０１はＬＡＮ認証部、ＶＰＮクライアント、ＶＰＮサーバ、公衆無線認証部と連携して認証過程の重要レベルを知りうる環境にある。従って、その重要レベルに応じたアンテナの指向性制御をセキュリティーを確保しながら行うことが可能である。これは本発明の大きな特徴であり、従来の技術では実現することが出来なかったものである。

【実施例４】

【００７７】

第５図において、統合無線認証装置５０１は本発明の方式を用いた装置のパネルの実施例を示している。以下本明細書において、ＬＡＮ認証部で認証されたイーサーネットフレームを内部フレームと、ＬＡＮ認証部で認証に失敗したイーサーネットフレームを外部フレームという。

【００７８】

統合無線認証装置５０１のパネルには内部フレームの通過を表示する内部フレーム表示ランプ５０２（内部フレーム表示部）と、外部フレームの通過を表示する外部フレーム表示ランプ５０３（外部フレーム表示部）が具備されている。この表示装置により内部フレームと外部フレームの通過比率を直視的に把握することができる。

【実施例５】

【００７９】

第６図に示す統合無線認証パネル６００は、内部フレームのトラフィックと外部フレームのトラフィックの分配割付比率を設定する、内部トラフィックス割付け比率変化スイッチ６０３と外部トラフィックス割付け比率変化スイッチ６０４が設けられていることが特徴である。また公衆無線認証部により認証された通信を行っている無線ＬＡＮクライアントの局数を表示する返信局数表示部６０２を具備することにより、本発明の統合無線認証システムを用いている無線設備の外部フレーム使用の割合を直視的に把握することができる。

【実施例６】

【００８０】

第７図は統合無線認証パネル７０１を表し、アンテナ７０２の方向制御と内部フレーム

通過表示装置７０３および外部フレーム通過表示装置７０４を組み合わせた例である。このような構成をもちいることでハードウエアの規模をおさえる条件のもとで、外部フレームのアクセスの条件を電波的に制限したい場合に、表示装置７０３及び７０４をみながら直視的に外部利用のアクセスの条件を設定できる。

【実施例７】

【００８１】

第８図に示す統合無線認証装置８０１において、反射板８０４はアンテナ基部８０３上に立設された放射器８０２の回りに回転できるように保持されている。統合無線認証装置８０１は、図７に表す統合無線認証パネル７０１の内部フレーム通過表示装置７０３及び外部フレーム通過表示装置７０４を見ながら反射板８０４の放射器８０２に対する相対位置を変化させることにより、外部と内部のトラフィックの割合を変化させることができる。これにより実施例５で前述のような、外部フレームのアクセスの条件を電波的に制限することができる。尚、反射板８０４は線状であっても本発明の主旨を損ねることはない。

【実施例８】

【００８２】

第９図は、第８図の統合無線認証装置８０１と同様、外部フレームのアクセスの条件を電波的に制限することができる、別のアンテナの具体的構造を有する統合無線認証装置９０１である。統合無線認証装置９０１はアンテナ９０２と、アンテナカバー９０３と、反射器又は導波器である９０４とから構成される。統合無線認証装置９０１は八木宇田アンテナの原理により、統合無線認証装置８０１と同様に手動によって適切および不適切無線ＬＡＮクライアントを選択する設定を直視的に行なうことができる。

【００８３】

その他、本発明は、その主旨を逸脱しない範囲で当業者の知識に基づき種々の改良、修正、変更を加えた態様で実施できるものである。

【産業上の利用可能性】

【００８４】

本発明は、電磁波を利用したインターネット接続において、耐妨害・侵入性を実現するための無線共用システムに利用し得る。

【図面の簡単な説明】

【００８５】

【図１】本発明の第一の実施例における統合無線共用方式の構成を示すブロック図

【図２】本発明の第二の実施例における統合無線共用方式の構成を示すブロック図

【図３】ＬＡＮ認証部によるイーサネットフレーム優先方法実現ブロック図

【図４】アンテナおよび無線局通信部の構造

【図５】統合無線認証装置パネル

【図６】統合無線認証装置パネル

【図７】表示装置と回転アンテナ

【図８】アンテナ指向性制御板（線）をもった背面パネル

【図９】アンテナ指向性制御板（線）

【符号の説明】

【００８６】

１００：無線ＬＡＮクライアント装置

１０１：無線インターネット接続装置

１０１ａ：無線通信部

１０１ｂ：ＬＡＮ認証部

１０１ｃ：ＶＰＮクライアント

１０２：インターネット中継装置

１０２ａ：ＶＰＮサーバ

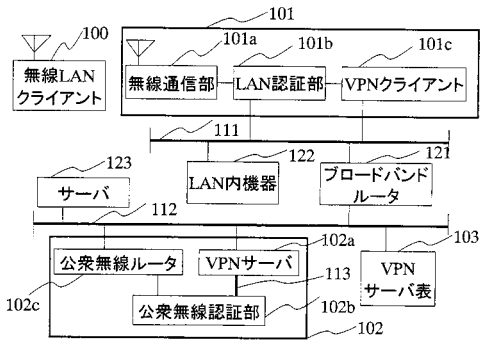
１０２ｂ：公衆無線認証部

１０２ｃ：公衆無線ルータ

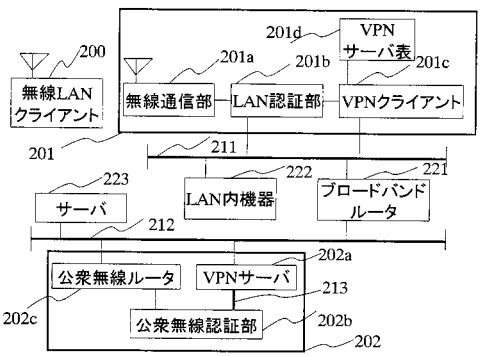
１０３：ＶＰＮサーバ表
１１１：有線ＬＡＮ
１１２：インターネット
１１３：ＶＰＮ
１２１：ブロードバンドルータ
１２２：ＬＡＮ内機器
１２３：インターネット上のサーバ
２００：無線ＬＡＮクライアント装置
２０１：無線インターネット接続装置
２０１ａ：無線通信部
２０１ｂ：ＬＡＮ認証部
２０１ｃ：ＶＰＮクライアント
２０１ｄ：ＶＰＮサーバ表
２０２：インターネット中継装置
２０２ａ：ＶＰＮサーバ
２０２ｂ：公衆無線認証部
２０２ｃ：公衆無線ルータ
２１１：有線ＬＡＮ
２１２：インターネット
２１３：ＶＰＮ
２２１：ブロードバンドルータ
２２２：ＬＡＮ内機器
２２３：インターネット上のサーバ
３００：ＬＡＮ認証部
３０１：ＬＡＮ認証器
３０２：割付け比率制御装置
３０３：帯域制御装置
３１１：トラフィックス計測器
３１２：トラフィックス計測器
３２１：無線通信部
３２２：ＶＰＮクライアント
３３１：有線ＬＡＮ
４０１：無線通信部
４０２：アンテナ
４０３：高周波部
４０４：無線信号処理部
４０５：テーブル
５０１：統合無線認証装置
５０２：内部フレーム表示ランプ（内部フレーム表示部）
５０３：外部フレーム表示ランプ（外部フレーム表示部）
６００：統合無線認証パネル
６０１：パケット表示ランプ
６０２：返信局数表示部
６０３：内部トラフィックス割付け比率変化スイッチ
６０４：外部トラフィックス割付け比率変化スイッチ
７０１：統合無線認証パネル
７０２：アンテナ
７０３：内部フレーム通過表示装置
７０４：外部フレーム通過表示装置
８０１：統合無線認証装置

８０２：放射器
８０３：アンテナ基部
８０４：反射板（線）
９０１：統合無線認証装置
９０２：アンテナ
９０３：アンテナカバー
９０４：反射器（線）又は導波器（線）

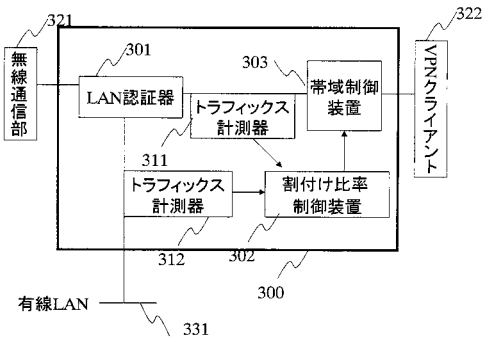
【図１】



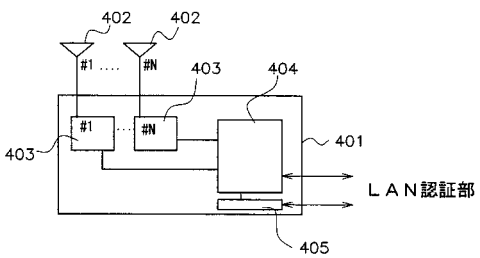
【図２】



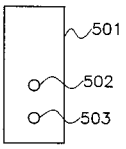
【図３】



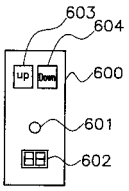
【図４】



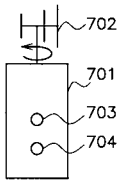
【図５】



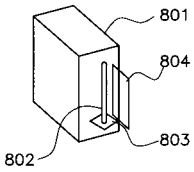
【図６】


603
604
up
Down
600
601
602

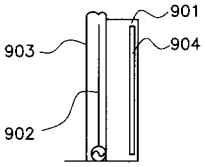
【図７】


702
701
703
704

【図８】


801
804
803
802

【図９】


901
903
904
902

フロントページの続き

(72)発明者　小川　均
滋賀県草津市野路東１－１－１　立命館大学びわこ・くさつキャンパス内
(72)発明者　西村　俊和
滋賀県草津市野路東１－１－１　立命館大学びわこ・くさつキャンパス内
(72)発明者　前田　忠彦
滋賀県草津市野路東１－１－１　立命館大学びわこ・くさつキャンパス内

審査官　岩田　玲彦

(56)参考文献　特開２００３－１６９０８５（ＪＰ，Ａ）
特開平１０－２１５２８４（ＪＰ，Ａ）
特開２００１－０５４１６５（ＪＰ，Ａ）
特開２００３－２３３５０４（ＪＰ，Ａ）
毛利公一・前田忠彦・大久保英嗣，次世代ワイヤレス通信を指向するオペレーティングシステムの提案，情報処理学会研究報告，日本，社団法人情報処理学会，２００３年　2月２８日，Vol. 2003 No.19，pp.107-114，2003-OS-92

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　８４／１２
Ｈ０４Ｌ　１２／４６