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

特許第4340626号
(P4340626)

(45)発行日　平成21年10月7日(2009.10.7)　(24)登録日　平成21年7月10日(2009.7.10)

(51)Int.Cl.　　F I
H04W 24/00 (2009.01)　H04L 12/28　300M
H04W 84/12 (2009.01)　H04L 12/28　310
H04W 88/08 (2009.01)　G09C 1/00　640E
G09C 1/00 (2006.01)

請求項の数 14　(全 8 頁)

(21)出願番号　特願2004-504401 (P2004-504401)
(86)(22)出願日　平成15年5月13日 (2003.5.13)
(65)公表番号　特表2005-525740 (P2005-525740A)
(43)公表日　平成17年8月25日 (2005.8.25)
(86)国際出願番号　PCT/US2003/015026
(87)国際公開番号　WO2003/096554
(87)国際公開日　平成15年11月20日 (2003.11.20)
審査請求日　平成18年4月13日 (2006.4.13)
(31)優先権主張番号　60/378,029
(32)優先日　平成14年5月13日 (2002.5.13)
(33)優先権主張国　米国(US)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　エフ－９２１００　ブローニュ　ビヤンクール，　ケ　アルフォンス　ル　ガロ，　４６番地
４６　Ｑｕａｉ　Ａ．　Ｌｅ　Ｇａｌｌｏ，　Ｆ－９２１００　Ｂｏｕｌｏｇｎｅ－Ｂｉｌｌａｎｃｏｕｒｔ，　Ｆｒａｎｃｅ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】シームレスな公衆無線ローカル・エリア・ネットワーク・ユーザ認証

(57)【特許請求の範囲】
【請求項１】
公衆無線ローカル・エリア・ネットワーク（ＬＡＮ）において移動無線通信装置を認証する方法であって：
非認証情報に対する要求を受信する工程；
制御ポートを部分的に開いた状態にする工程であって、
該制御ポートを通じて該情報要求が第１サーバに誘導され、該第１サーバが回答を該移動無線通信装置に対して供給することによって応答する工程；
アクセス要求を受信する工程；
該移動無線通信装置を、非制御ポートを通じて認証する工程；及び
該制御ポートを完全に開いた状態にして該移動無線通信装置との該制御ポートを通じたトラフィックの交換を可能にする工程；
を含むことを特徴とする方法。
【請求項２】
請求項１記載の方法であって、該非認証情報に対する要求が該第１サーバに、該要求において規定された宛て先にかかわらず、誘導されることを特徴とする方法。
【請求項３】
請求項１記載の方法であって、該認証する工程が：
該移動無線通信装置からの、該移動無線通信装置に対する該回答に応じた、受け入れを受信する工程；

ユーザ識別要求を該移動無線通信装置に送信する工程；
該移動無線通信装置からのユーザ識別応答を該ユーザ識別要求に対する回答として受信する工程；及び
該ユーザ識別応答を認証サーバに転送する工程；
を含むことを特徴とする方法。
【請求項４】
請求項３記載の方法であって、該ユーザ識別要求を送信する工程が：
拡張可能認証プロトコル（ＥＡＰ）要求を送信する工程；
を含むことを特徴とする方法。
【請求項５】
請求項４記載の方法であって、該ユーザ識別応答を受信する工程が：
ＥＡＰ識別応答を受信する工程；
を含むことを特徴とする方法。
【請求項６】
請求項１記載の方法であって、更に：
認証に後続して認証鍵を設定する工程；
を含むことを特徴とする方法。
【請求項７】
請求項６記載の方法であって、該認証鍵を設定する工程が：
ワイヤード・イクイバレント・プライバシ（ＷＥＰ）暗号化鍵を設定する工程；
を含むことを特徴とする方法。
【請求項８】
移動無線通信装置を認証する通信ネットワーク・システムであって：
非認証情報を記憶する第１サーバ；
移動無線通信装置を認証する第２サーバ；及び
少なくとも１つのアクセス・ポイント（ＡＰ）；
を有し；
該少なくとも１つのＡＰが：
制御ポート；及び
非制御ポート；
を有し；
該制御ポートを通じて該少なくとも１つのＡＰは、移動無線通信装置からの非認証情報に対する要求の受信に応じて、部分的に開いた状態になり、該制御ポートは該情報要求を、該移動無線通信装置によって受信される回答を送出する該第１サーバに対して、誘導するものであり；
該非制御ポートを通じて該少なくとも１つのＡＰは該移動無線通信装置から受信された認証トラフィックを、該移動無線通信装置と認証トラフィックを交換する該第２サーバに対して、誘導するものであり；
更に、該少なくとも１つのＡＰと、該第１サーバ並びに該第２サーバ、とに結合された公衆無線ローカル・エリア・ネットワーク（ＬＡＮ）；
を含むことを特徴とするシステム。
【請求項９】
請求項８記載のシステムであって、該ＡＰがＩＥＥＥ８０２．１ｘ準拠の通信プロトコルを利用することを特徴とするシステム。
【請求項１０】
請求項８記載のシステムであって、該第１サーバに記憶された前記非認証情報がアクセス・コストを含むことを特徴とするシステム。
【請求項１１】
請求項８記載のシステムであって、該第２サーバが該移動無線通信装置を拡張可能認証プロトコル（ＥＡＰ）によって認証することを特徴とするシステム。

【請求項１２】
請求項８記載のシステムであって、該少なくとも１つのＡＰで受信された該認証トラフィックが認証サーバの識別を含むことを特徴とするシステム。
【請求項１３】
アクセス・ポイント（ＡＰ）・システムであって：
制御ポート；及び
非制御ポート；
を備え；
該制御ポートを通じて該ＡＰシステムは移動無線通信装置からの非認証情報に対する要求の受信に応じて、部分的に開いた状態になり、該制御ポートは該情報要求を、該移動無線通信装置によって受信される回答を送出する第１サーバに対して、誘導するものであり；
該非制御ポートを通じて該ＡＰシステムは該移動無線通信装置から受信された認証トラフィックを、該移動無線通信装置と認証トラフィックを交換する第２サーバに対して、誘導するものであることを特徴とするシステム。
【請求項１４】
請求項１３記載のシステムであって、ＩＥＥＥ８０２．１ｘ準拠の通信プロトコルを利用することを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、公衆無線ローカル・エリア・ネットワーク（ＬＡＮ）において移動無線通信装置を認証する手法に関する。
【背景技術】
【０００２】
無線ＬＡＮ技術の分野における発展は、サービス・エリア、喫茶店、図書館及び同様な公共施設で公にアクセス可能な無線ＬＡＮ（例えば、「ホット・スポット」）の出現をもたらしている。現在、公衆無線ＬＡＮは移動無線通信装置のユーザに、企業イントラネットのような私設データ・ネットワーク又はインターネットのような公衆データ・ネットワークに対するアクセスを提供している。公衆無線ＬＡＮを実施して運用するうえでのコストが比較的低いこと、更には、（通常１０メガビット／秒超の）高帯域が利用可能であることが、公衆無線ＬＡＮを、理想的なアクセス手順で、該手順を通じてユーザが外部エンティティとパケットを交換し得るもの、にしている。
【０００３】
ユーザが公衆無線ＬＡＮカバレッジ区域内に移動する場合、公衆無線ＬＡＮは最初に、ネットワーク・アクセスを付与する前にユーザを認証し、許可する。認証後、公衆無線ＬＡＮのアクセス・ポイント（ＡＰ）は移動無線通信装置に対するセキュアなデータ・チャネルを開いて該装置と交換されるデータのプライバシを保護する。現在、無線ＬＡＮ機器のメーカの多くはＩＥＥＥ８０２．１ｘプロトコルを配備機器に採用している。したがって、無線ＬＡＮに対して最も有力な認証手順はこの標準を利用する。残念ながら、ＩＥＥＥ８０２．１ｘプロトコルは安全な認証手順であったが、そのような手順はＷＥＰ（ワイヤード・イクイバレント・プライバシ：無線通信暗号化技術（ウェップ））の暗号化鍵をウェブ・ブラウザに設定することを可能にするものでない。したがって、認証後に無線ＬＡＮ経由で伝送されたデータは非保護状態のままである。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
したがって、公衆無線ＬＡＮ環境において用いる認証処理で、ＩＥＥＥ８０２．１ｘプロトコルによる認証を可能にし、それによって交換データのプライバシを、カスタム化された相互作用手順を与える一方で、保護するもの、に対する必要性が存在する。

【課題を解決するための手段】
【０００５】
簡潔に、本発明の好適実施例によって、公衆無線ＬＡＮにおける移動無線通信装置のユーザを認証する方法を備える。該方法は、移動無線通信装置から受信された非認証情報に対する要求を受け取ることによって開始し、該非認証情報はアクセス・コストのようなアクセス情報を含み得る。そのような情報要求に応じて、公衆無線ＬＡＮにおける制御ポートが部分的に開かれて、非認証（例えば、アクセス）情報要求のＬＡＮを通じた第１サーバで、要求情報によって応答するもの、に対する伝送を可能にする。移動無線通信装置のユーザが、第１サーバからの応答において規定されたアクセス条件が受け入れ可能であることを見出すものであると仮定すれば、ユーザはアクセス要求を、認証資格証明付認証サーバに送出する。該アクセス要求に応じて、該認証サーバはユーザを認証して、公衆無線ＬＡＮに無線ＬＡＮサービスの利用を可能にすることを通知する。認証が正常であることによって、公衆無線ＬＡＮは制御ポートを完全に開いて、移動無線通信装置とのデータの交換を、制御ポートを通じて、可能にする。
【発明を実施するための最良の形態】
【０００６】
〔実施例〕
図１は、通信ネットワーク１０で、少なくとも１つの移動通信装置、更には、好ましくは、複数の移動通信装置（例えば、移動通信装置１２１及び１２２）、を動作可能にして、外部データ源１４のセキュアなアクセスを行うアクセス装置１１を含むもの、のブロック概略図を表し、該外部データ源は、公衆データ・ネットワーク（例えば、インターネット）のような、ネットワーク１５内のサーバ、又は私設データ・ネットワーク（例えば、企業イントラネット）の形態を取り得る。好適実施例では、移動通信装置１２１は、無線モデム又は無線ネットワーク・アクセス・カードを含むラップトップ型コンピュータを備える一方、移動通信装置１２２は、携帯情報端末（ＰＤＡ）を備える。アクセス装置１１は更に、別の種類の移動無線通信装置（図示せず）の役目を担い得る。
【０００７】
図１のアクセス装置１１は、少なくとも１つの、更には、好ましくは複数の、アクセス・ポイント（ＡＰ）で、ＡＰ１８１乃至１８４によって最もよく例示されるもの、を含み、該ＡＰを介して移動無線通信装置１２１及び１２２は公衆無線ローカル・エリア・ネットワーク（ＬＡＮ）２０をアクセスし得る。別個に表すが、ＡＰ１８１乃至１８４は公衆無線ＬＡＮ２０の一部を構成する。図示した実施例では、ＡＰ１８１のような、各ＡＰは各移動無線通信装置内のラジオ・トランシーバ（図示せず）と無線周波数信号を交換するワイヤレス・トランシーバ（図示せず）を含む。この目的で、ＡＰ１８１乃至１８４の各々は少なくとも１つの周知の無線データ交換プロトコルで、ＩＥＥＥ８０２．１ｘプロトコルのようなもの、を利用する。
【０００８】
アクセス装置１１は更に、サーバ２１を、非認証情報を記憶するローカル・ウェブ・サーバの形態で、含む。そのような非認証情報はアクセス情報で、ユーザに対するコストを含む、アクセス条件のようなもの、を含み得る。ローカル・ウェブ・サーバ２１は装置ユーザがそのような非認証情報を、公衆無線ＬＡＮ２０との実際の通信セッションを設定し、したがって認証を経る必要なく、得ることを可能にする。別個に表すが、ローカル・サーバ２１は公衆無線ＬＡＮ２０内に存在し得る。
【０００９】
ゲートウェイ２２は公衆無線ＬＡＮ２０と、ネットワーク１５に対するリンクを備えるパケット・データ・ネットワーク（ＰＤＮ）２４との間の通信経路を備える。ＰＤＮ２４はしたがって、各移動無線通信装置とデータ源１４との間の通信を可能にする。ＰＤＮ２４は更に、ゲートウェイ２２を認証サーバ２６にリンクする。実際には、認証サーバ２６は、データベースで、潜在ユーザに関する情報を含んで無線ＬＡＮ２０にアクセスしようとするものの認証を可能にするもの、の形態をとる。別個のスタンド・アロンのエンティテ

ィとして存在するのではなく、認証サーバ２６は公衆無線ＬＡＮ２０内に存在し得る。更に、ＰＤＮ２４は公衆無線ＬＡＮ２０とビリング・エージェント（図示せず）との間のリンクを備えてビリング装置のユーザが公衆無線ＬＡＮをアクセスすることを促進する。認証サーバ２４と同様に、ビリング・エージェントの機能は公衆無線ＬＡＮ２０内に存在し得る。

【００１０】

公衆無線ＬＡＮ２０との実際の認証通信セッションを実際に設定することに先立って、装置ユーザは特定の非認証情報で、アクセスの条件、更にはコストのようなもの、を得ようとし得る。今まで、装置ユーザはそのような非認証情報を、公衆無線ＬＡＮで、そのアクセス・ポイント（ＡＰ）がＩＥＥＥ８０２．１ｘプロトコルを利用するもの、から得ることは、認証通信セッションを設定することなしでは、可能でなかった。本発明のアクセス装置１１はこの欠点を、公衆無線ＬＡＮ２０との限定的な接続を可能にして非認証情報で、アクセス情報を含むもの、を、認証通信セッションを実際に設定する前に、得ることによって、克服する。

【００１１】

図２は相互作用のシーケンスで、経時的に、移動無線通信装置、例えば、装置１２１、公衆無線ＬＡＮ２０、ローカル・ウェブ・サーバ２１、及び認証サーバ２６、間で行われて、所望のセキュアなアクセスを、特定情報の受け取りを認証なしで可能にする一方で、実現するもの、を表す。図２を参照すれば、実際に認証通信セッションを設定する前に、移動無線通信装置１２１のユーザは非認証情報を、最初に工程１０２でＨＴＴＰ情報要求を起動することによって、得ることが可能である。該情報要求は当初、図１のＡＰ１８１のような、ＡＰの１つで受信される。ＩＥＥＥ８０２．１ｘによって構成された場合、図１のＡＰ１８１は、制御ポート及び非制御ポートで、それらを通じてＡＰが移動無線通信装置１２１と情報を交換するもの、を維持する。ＡＰ１８１によって維持される制御ポートは非認証情報が公衆無線ＬＡＮ２０と移動無線通信装置１２１との間のＡＰを通過する入り口用通路としての役目を担う。通常、ＡＰ１８１はその制御ポートを、ＩＥＥＥ８０２．１ｘプロトコルによって、移動無線通信装置の認証まで、閉じた状態のままにする。ＡＰ１８１は常に、非制御ポートを開いた状態に維持して移動無線通信装置１２１が認証データを認証サーバ、例えば、サーバ２６、と交換することを可能にする。

【００１２】

移動無線通信装置１２１が非認証情報、更には、特に、アクセス情報、を、本発明による認証なしで、得ることを可能にするよう、公衆無線ＬＡＮ２０は、図１のＡＰ１８１のような、ＡＰ各々に、その制御アクセス・ポートを、非認証情報に対する要求を受信した後に、部分的に開いた状態にさせる。ＡＰ１８１における制御ポートを部分的に開いた状態にすることによって、工程１０４で、公衆無線ＬＡＮ２０におけるそのような非認証情報要求を制御ポートを通じて受領することを可能にする。該情報要求を受領することによって、公衆無線ＬＡＮ２０は該要求を、工程１０６で、ローカル・ウェブ・サーバ２１に転送する。工程１０２で当初行われた情報要求において規定された宛て先にかかわらず、公衆無線ＬＡＮ２０は常に、該要求を図１のウェブ・サーバ２１に、工程１０６で、誘導する。ウェブ・サーバ２１は該情報要求に工程１０８で、該要求情報（例えば、アクセス条件、更には、認証サーバ２６のドメイン名）を要求移動無線通信装置１２１に供給することによって、応答する。該装置のユーザが、該条件が受け入れ可能であることを見出す（か、ユーザが受け入れ可能な条件を協議した）と仮定すれば、移動無線通信装置１２１はＡＰ１８１に工程１１０で受け入れメッセージを送信する。受け入れメッセージは認証サーバ２６をその名称又はＵＲＬによって識別する。移動無線装置１２１は自動的にそのような受け入れメッセージを、ウェブ・サーバ２１によって通信されたアクセス条件が該装置に記憶された所定のアクセス基準に照合する場合に、送信する。そのような照合がない場合には、ユーザは受け入れメッセージの送信を引き起こすことを要し得る。

【００１３】

該受け入れメッセージを受信することによって、ＡＰ１８１は移動無線通信装置１２１に

工程１１２の間に、自らを識別するよう要求する。移動無線装置１２１が公知の拡張可能認証プロトコル（ＥＡＰ）を利用することを仮定すれば、ＡＰ１８１は該装置をＥＡＰ識別要求によって識別しようとする。ＥＡＰ識別要求に応じて、移動無線通信装置１２１は工程１１４でＥＡＰ識別応答をＡＰ１８１に送出して、工程１１６で公衆無線ＬＡＮ２０を介して転送され、認証サーバ２６で受信される。

【００１４】

該装置を識別する当該処理の一部として、公衆無線ＬＡＮ２０は通常、装置ユーザが無線ＬＡＮ２０に対応するビリング・エージェントとの関係を有するか否かを確かめる。ユーザが関係を有する場合、ビリング・エージェントがアクセス・チャージの明細を明らかにするため、ユーザは更に何もすることを要しない。ビリング・エージェントとの関係がない場合には、ユーザはそのような関係を設定することを要する。ユーザの受諾によって、無線ＬＡＮ２０は動的にそのような関係を設定しようとすることが可能である。

【００１５】

ＥＡＰ識別応答を受信することによって、ＡＰ１８１は工程１１８で、ＥＡＰ識別応答を認証サーバ２６に非制御ポートを通じて送出する。認証サーバ２６は工程１２０の間にＥＡＰ識別応答に、ＥＡＰ認証要求をＡＰ１８１に誘導することによって、応答して、後に工程１２２で、ＡＰ１８１を介して移動無線通信装置１２１に送信する。移動無線通信装置１２１は工程１２４の間にＥＡＰ認証応答で、ＡＰ１８１における非制御ポートを通じて受信されるもの、によって応答する。同様に、ＡＰ１８１は工程１２６の間にＥＡＰ認証応答を認証サーバ２６に転送する。

【００１６】

移動無線通信装置１２１の認証が正常であることによって、認証サーバ２６は工程１２８でＥＡＰ認証正常メッセージを生成してＡＰ１８１において受信される。同様に、ＡＰ１８１は認証鍵、通常、ワイヤード・イクイバレント・プライバシ（ＷＥＰ）暗号化鍵、を設定して、工程１３０の間に移動無線通信装置１２１に送信する。最後に、ＡＰ１８１はその制御ポートを完全に開いた状態にして移動無線通信装置１２１との制御ポートを通じたトラフィックの交換を可能にする。

【００１７】

上記は公衆無線ＬＡＮにおける移動無線通信装置を認証する手法で、該装置のユーザに非認証情報を受信する機会を該公衆無線ＬＡＮとの通信セッションを実際に設定することに先立って与えるもの、を記載したものである。

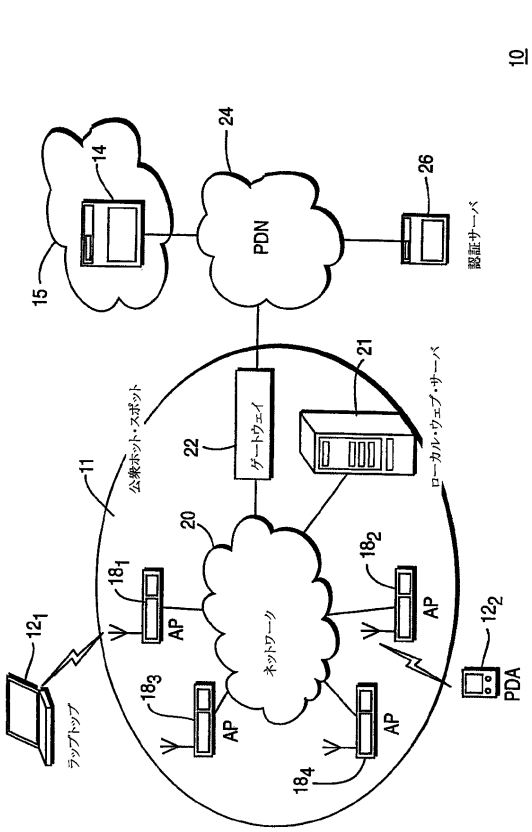
【図面の簡単な説明】

【００１８】

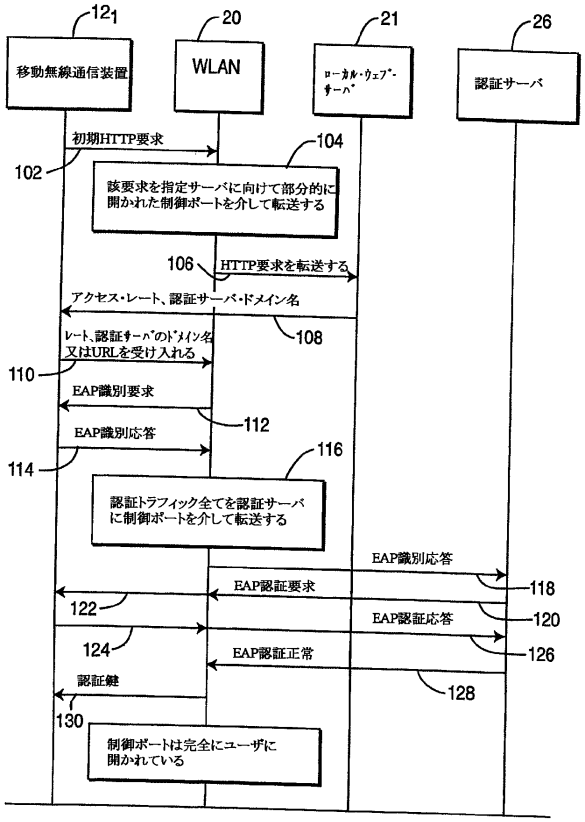
【図１】移動無線通信装置のユーザを認証する本発明の方法を実施する通信システムのブロック概略図である。

【図２】図１の通信システムにおける移動無線通信装置のユーザの認証に関連したイベントのシーケンスを表すタイミング図である。

【図１】


10
24
14
26
PDN
認証サーバ
15
21
ローカル・ウェブ・サーバ
22
ゲートウェイ
公衆ホット・スポット
11
20
ネットワーク
18₁
18₂
AP
AP
12₁
12₂
18₃
18₄
AP
AP
ラップトップ
PDA

【図２】


12₁
移動無線通信装置
20
WLAN
21
ローカル・ウェブ・サーバ
26
認証サーバ
初期HTTP要求
102
104
該要求を指定サーバに向けて部分的に開かれた制御ポートを介して転送する
106
HTTP要求を転送する
アクセス・レート、認証サーバ・ドメイン名
108
レート、認証サーバのドメイン名又はURLを受け入れる
110
EAP識別要求
112
EAP識別応答
114
116
認証トラフィック全てを認証サーバに制御ポートを介して転送する
EAP識別応答
118
EAP認証要求
122
EAP認証応答
120
124
EAP認証正常
126
認証鍵
128
130
制御ポートは完全にユーザに開かれている

フロントページの続き

(72)発明者　ワン，チャールズ，チョアンミン
アメリカ合衆国，ペンシルヴェニア州　１８９２９，ジェイミソン，スペアミント・サークル　１５０４
(72)発明者　モディー，サチン，サティッシュ
アメリカ合衆国，ニュージャージー州　０８６４８，ローレンスヴィル，ホワイト・パイン・サークル　７０８
(72)発明者　ジャン，ジュンビアオ
アメリカ合衆国，ニュージャージー州　０８８０７，ブリッジウォーター，ジェンナ・ドライヴ　２０
(72)発明者　ラマスワミー，クマール
アメリカ合衆国，ニュージャージー州　０８５４０，プリンストン，セイアー・ドライヴ　７１

審査官　岩田　玲彦

(56)参考文献　特開２００２－１１８５６２（ＪＰ，Ａ）
高田学也，２００２年の注目技術　無線ＬＡＮのすべて，日経ＮＥＴＷＯＲＫ，日本，日経ＢＰ社，２００１年１２月２２日，第２１号，pp.59-79，2002年1月号

(58)調査した分野(Int.Cl.，ＤＢ名)
H04W　24/00
G09C　 1/00
H04W　84/12
H04W　88/08