(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-524017
(P2006-524017A)
(43)公表日　平成18年10月19日(2006.10.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	300Z	5B285
H04Q 7/38	(2006.01)	H04B	7/26	109S	5J104
H04L 9/32	(2006.01)	H04L	9/00	673A	5K033
G09C 1/00	(2006.01)	G09C	1/00	640E	5K067
G06F 21/20	(2006.01)	G06F	15/00	330C	

審査請求 未請求　予備審査請求 有　（全 19 頁）

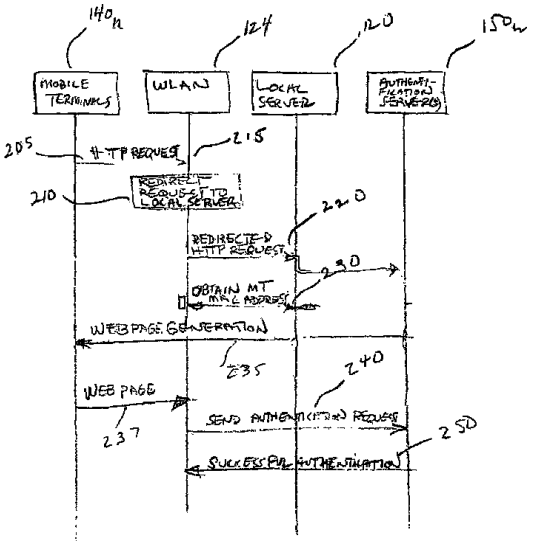
(21)出願番号　特願2006-509073 (P2006-509073)
(86)(22)出願日　平成16年3月4日 (2004.3.4)
(85)翻訳文提出日　平成17年10月21日 (2005.10.21)
(86)国際出願番号　PCT/US2004/006566
(87)国際公開番号　WO2004/081718
(87)国際公開日　平成16年9月23日 (2004.9.23)
(31)優先権主張番号　60/453,329
(32)優先日　平成15年3月10日 (2003.3.10)
(33)優先権主張国　米国 (US)

(71)出願人　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　100087321
弁理士　渡辺　勝徳
(74)代理人　100115864
弁理士　木越　力
(74)代理人　100118496
弁理士　青山　耕三

最終頁に続く

(54)【発明の名称】公的認証サーバで無線ＬＡＮアクセスを制御するＩＤマッピング機構

(57)【要約】
ブラウザのリクエストを向け直し、セッションの識別（セッションＩＤ）をＨＴＴＰのリクエスト内に埋め込み、認証サーバ内でこのセッションＩＤを使用して２つのＨＴＴＰセッションをマッチさせることによって、無線ＬＡＮ環境内でモバイル端末のセキュリティを改善する方法。アクセス・ポイントは、セッションＩＤがＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）に埋め込まれるように、モバイル端末からのｗｅｂリクエストを処理する。それに加え、このセッションとモバイル端末のＩＰアドレスまたは媒体アクセス制御アドレス間のマッピングが無線ＬＡＮ内で維持される。認証サーバが認証の結果をアクセス・ポイントに通知すると、モバイル端末を独自に識別するためにそのセッションＩＤが使用される。これらのオペレーションはすべて、モバイル端末に対しトランスペアレント（ｔｒａｎｓｐａｒｅｎｔ：気付かれない）である。



【特許請求の範囲】
【請求項１】
無線ローカル・エリア・ネットワークへのアクセスを制御するための方法であって、
無線ＬＡＮの視聴圏内に配置されるモバイル端末から無線ＬＡＮにアクセスするためのリクエストを受信するステップと、
セッション（ｓｅｓｓｉｏｎ）ＩＤを、モバイル端末に関連する識別子と関連づけ、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶するステップと、
セッションＩＤを含む、認証リクエストを該当する認証サーバに送信するステップと、
モバイル端末に関する認証メッセージ（セッションＩＤを含む）を該当する認証サーバから受信するステップと、
記憶されたマッピング・データに応答し、受信された認証メッセージをモバイル端末に相関させるステップと、
受信された認証メッセージに応答し、モバイル端末から無線ＬＡＮへのアクセスを制御するステップと、から成る、前記方法。
【請求項２】
前記関連づけるステップで、セッションＩＤをモバイル端末の媒体アクセス制御アドレスと関連づけ、セッションＩＤをモバイル端末の媒体アクセス制御アドレスにマップするデータを記憶する、請求項１記載の方法。
【請求項３】
前記関連づけるステップで、セッションＩＤを、モバイル端末に関連するＩＰアドレスと関連づけ、セッションＩＤをモバイル端末に関連するＩＰアドレスにマップするデータを記憶する、請求項１記載の方法。
【請求項４】
セッションＩＤをモバイル端末に送信するステップと、
モバイル端末から認証のリクエスト（その中に埋め込まれたセッションＩＤを含む）を受信するステップと、
受信された認証リクエストを該当する認証サーバに送信するステップと、を更に含む、請求項１記載の方法。
【請求項５】
第１の送信するステップで、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、ｗｅｂページをモバイル端末に送信する、請求項４記載の方法。
【請求項６】
ＨＴＴＰＳセッションを開始するためにサブミット（ｓｕｂｍｉｔ）ボタンに関連するＵＲＬ（ｕｎｉｖｅｒｓａｌ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ）内にセッションＩＤが埋め込まれる、請求項５記載の方法。
【請求項７】
ＨＴＴＰＳセッションがモバイル端末と認証サーバとの間で開始されると、無線ＬＡＮと認証サーバとの間に通信環境を確立し、よって、認証サーバが認証メッセージを無線ＬＡＮに送信するステップを更に含む、請求項６記載の方法。
【請求項８】
無線ＬＡＮへのアクセスを制御するための方法であって、
無線ＬＡＮに関連するアクセス・ポイントにおいて、無線ＬＡＮの視聴圏内に配置されるモバイル端末から無線ＬＡＮにアクセスするためのリクエストを受信するステップと、
リクエストを無線ＬＡＮに関連するローカル・サーバの方に向け直し、ローカル・サーバはセッションＩＤを、モバイル端末に関連する識別子と関連づけ、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶するステップと、
セッションＩＤを含む、認証リクエストを該当する認証サーバに送信するステップと、
ローカル・サーバにおいて、モバイル端末に関する認証メッセージ（セッションＩＤを

含む）を該当する認証サーバから受信するステップと、
ローカル・サーバにおいて、記憶されたマッピング・データに応答し、受信された認証メッセージをモバイル端末に相関させるステップと、
受信された認証メッセージに応答し、モバイル端末から無線ＬＡＮへのアクセスを制御するステップと、から成る、前記方法。
【請求項９】
ローカル・サーバが、モバイル端末の媒体アクセス制御アドレスとセッションＩＤを関連づけ、前記セッションＩＤをモバイル端末の媒体アクセス制御アドレスにマップするデータを記憶する、請求項８記載の方法。
【請求項１０】
ローカル・サーバがセッションＩＤを、モバイル端末に関連するＩＰアドレスと関連づけ、前記セッションＩＤをモバイル端末に関連する前記ＩＰアドレスにマップするデータを記憶する、請求項８記載の方法。
【請求項１１】
セッションＩＤをモバイル端末に送信するステップと、
モバイル端末から認証リクエスト（その中に埋め込まれたセッションＩＤを含む）を受信するステップと、
受信された認証リクエストを該当する認証サーバに送信するステップと、を更に含む、請求項８記載の方法。
【請求項１２】
ローカル・サーバは、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、モバイル端末に送信されるｗｅｂページ内にセッションＩＤを埋め込む、請求項１１記載の方法。
【請求項１３】
無線通信チャンネルを通して複数のモバイル端末のうち１つと通信するためのアクセス・ポイントと、
アクセス・ポイントに結合されるローカル・サーバと、
前記アクセス・ポイントとローカル・サーバに結合されて、無線ＬＡＮを、複数の認証サーバの１つに結合される外部の通信ネットワークに結合させる手段と、からなる、無線ローカル・エリア・ネットワークにおいて、
無線ＬＡＮの視聴圏内に配置されるモバイル端末によるアクセスのリクエストに応答し、
前記ローカル・サーバは、セッションＩＤを、リクエストしているモバイル端末に関連する識別子と関連づけ、セッションＩＤを、リクエストしているモバイル端末に関連する識別子にマップするマッピング・データを記憶し、
セッションＩＤを含む、認証のリクエストを該当する認証サーバに送信し、
該当する認証サーバから受信された認証メッセージを、リクエストしているモバイル端末に相関させ、
受信された認証メッセージに応答し、モバイル端末による無線ＬＡＮへのアクセスを制御する、前記無線ローカル・エリア・ネットワーク。
【請求項１４】
リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末の媒体アクセス制御アドレスに対応する、請求項１３記載の無線ＬＡＮ。
【請求項１５】
リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末に関連するＩＰアドレスに対応する、請求項１３記載の無線ＬＡＮ。
【請求項１６】
アクセス・ポイントで、セッションＩＤをモバイル端末に送信し、認証サーバに送信される認証のリクエスト（その中に埋め込まれたセッションＩＤを含む）をモバイル端末から受信する、請求項１３記載の無線ＬＡＮ。

【請求項１７】
ローカル・サーバは、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、アクセス・ポイントから前記ｗｅｂページをモバイル端末に送信する、請求項１６記載の無線ＬＡＮ。
【請求項１８】
ローカル・サーバが、ＨＴＴＰＳセッションを開始させるために、サブミット・ボタン（ｓｕｂｍｉｔ　ｂｕｔｔｏｎ）に関連するＵＲＬ内にセッションＩＤを埋め込む、請求項１７記載の無線ＬＡＮ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セッションＩＤ（ｉｄｅｎｆｉｃａｔｉｏｎ：識別）を認証リクエスト内に埋め込み、認証サーバ内のセキュリティ処理にＩＤを使用して２つのセッションをマッチさせることにより、無線（ワイヤレス）ローカル・エリア・ネットワーク（無線ＬＡＮ）上でセキュリティとアクセス制御を改善する装置と方法を提供する。
【背景技術】
【０００２】
本発明は、モバイル装置のためにそして他のネットワーク（ハード・ワイヤドＬＡＮ）およびグローバル・ネットワーク（インターネット）へのアクセスを提供するアクセス・ポイント（Ａｃｃｅｓｓ　Ｐｏｉｎｔ：ＡＰ）を有するＩＥＥＥ８０２．１ｘアーキテクチャを使用する無線ＬＡＮのファミリである。無線ＬＡＮ技術の進歩は、休憩停車地、カフェ、図書館などの公共施設で公的にアクセスできるホット・スポットを生じている。現在、公的無線ＬＡＮにより、モバイル通信装置の利用者は、私的データ・ネットワーク（企業のイントラネット）、あるいは公的データ・ネットワーク（インターネット）、ピア・ツー・ピア通信および生の無線ＴＶ放送へのアクセスが得られる。公的無線ＬＡＮは、割合低コストで実現／運営され、高帯域幅（通常、１０メガビット／秒を超える）が利用できるので、理想的なアクセス機構となり、モバイル無線通信装置の利用者（ユーザ）は外部のエンティティとパケットを交換できる。しかしながら、以下に述べるように、このようにオープンの配備では、識別（ＩＤ）と認証のための十分な手段が存在しなければ、セキュリティが危うくなるかもしれない。
【０００３】
利用者が公的無線ＬＡＮの視聴圏（ｃｏｖｅｒａｇｅ　ａｒｅａ：カバレッジ・エリア、サービス・エリア）内でサービスにアクセスしようとすると、無線ＬＡＮは最初にユーザを認証／認可してから、ネットワークへのアクセスを許可する。認証後、公的無線ＬＡＮはモバイル通信装置に安全確実なデータ・チャンネルを開いて無線ＬＡＮと装置間を通るデータのプライバシーを保護する。無線ＬＡＮ装置の製造者の多くは現在、配備された無線ＬＡＮ装置に関するＩＥＥＥ８０２．１ｘ標準を採用している。従って、この標準は、無線ＬＡＮで利用される支配的な認証機構である。あいにく、ＩＥＥＥ８０２．１ｘ標準は、私的ＬＡＮアクセスをその使用モデルとして設計されており、従って、ＩＥＥＥ８０２．１ｘ標準では、公的無線ＬＡＮの環境内でのセキュリティを改善すると思われる確かな特徴が得られない。
【０００４】
図１は、公的無線ＬＡＮ環境内で認証に関る３つのエンティティ：モバイル端末（Ｍｏｂｉｌｅ　Ｔｅｒｍｉｎａｌ：ＭＴ）、無線ＬＡＮのアクセス・ポイント（Ａｃｃｅｓｓ　Ｐｏｉｎｔ：ＡＰ）、および特定のサービス・プロバイダに関連する認証サーバ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｅｒｖｅｒ：ＡＳ）、またはバーチャル・オペレータ、の間の関係を例示する。信頼関係は以下のようになる：モバイル端末は認証サーバとアカウント（ａｃｃｏｕｎｔ：取引）があり、互いに信頼関係を共有する。無線ＬＡＮオペレータ、および認証サーバを所有するオペレータ（以下、「バーチャル・オペレータ」と称す）はビジネス（営業）関係を有し、従ってアクセス・ポイントと認証サーバは信頼関係を

有する。認証手続きの目的は、現存する２つの信頼関係を利用して、モバイル端末とアクセス・ポイント間の信頼関係を確立することである。

【０００５】

ｗｅｂブラウザをベースとする認証方法において、ＨＴＴＰＳ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ Ｓｅｃｕｒｅｄ Ｓｏｃｋｅｔｓ）プロトコルによるｗｅｂブラウザを使用し、モバイル端末は直接認証サーバと認証して、アクセス・ポイント（およびモバイル端末と認証サーバ間の経路上にいる誰か）が秘密のユーザ情報に侵入したり、盗めないようにする。チャンネルが危険性のない安全な状態にある限り、認証サーバからはっきり通知されなければ、アクセス・ポイントは認証の結果を確かめることはできない。認証サーバがモバイル端末に話した唯一の情報は、ＨＴＴＰＳセッションの他端における、そのインターネット・プロトコルまたはＩＰアドレスである。ファイアウォール（防護壁）、ネットワーク・アドレス変換サーバ、あるいはｗｅｂプロキシィ（代理人）が電子的にモバイル端末と認証サーバ間に位置するとき（これは通常、バーチャル・オペレータ構成についての場合であるが）、このような情報は、モバイル端末を識別するのに使用することはできない。

【０００６】

現存する大多数の無線ＬＡＮホットスポット・ワイヤレス・プロバイダは、ユーザの認証とアクセス制御のために、ｗｅｂブラウザを基（ベース）とする方法を使用する。これはユーザにとって便利であることが判明しており、ユーザの装置でソフトウェアのダウンロードを必要としない。このような方法で、ユーザはＨＴＴＰＳを通しサーバにより安全に認証され、サーバは無線アクセス・ポイントに通知しユーザにアクセスを許可する。このような認証サーバ（ＡＳ）の所有者は、無線ＬＡＮオペレータ、あるいはＩＳＰ（Ｉｎｄｅｐｅｎｄｅｎｔ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ：独立サービス・プロバイダ）のような、第三者のプロバイダ、プリペイド・カードのプロバイダ、あるいはセル・オペレータ（もっと広く、バーチャル・オペレータと称される）である。

【０００７】

従来技術では、セキュア・トンネルを通る、ユーザと認証サーバ間の通信により認証が達成される。従ってアクセス・ポイントは、ユーザと認証サーバ間の通信を翻訳しない。そのため、アクセス・ポイントと認証サーバ間に別個の通信（認可情報と称される）を確立して、アクセス・ポイントがその認可情報を受信できるようにする必要がある。

【０００８】

アクセス・ポイントにおけるアクセス制御は、媒体アクセス制御アドレスまたはＩＰアドレスに基づいており、従って、認証サーバ（ＡＳ）は、認証の結果をアクセス・ポイントに返送する際、モバイル端末のＩＰアドレス（ＨＴＴＰＳトンネルのソース・アドレス）を識別子として使用することができる。この方法は、もしアクセス・ポイントと認証サーバとの間に、ファイアウォール（ｆｉｒｅｗａｌｌ：ＦＷ）およびローカル・サーバ（Ｌｏｃａｌ Ｓｅｒｖｅｒ：ＬＳ）のような、ファイアウォールもＮＡＴ（Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ）も存在しなければ、成功する。一般に、そしてバーチャル・オペレータが存在する場合、認証サーバは、無線アクセス・ネットワークの領域外に位置し、従って、ファイアウォール（ＦＷ）の外部に位置しており、しばしば、認証に使用されるＨＴＴＰＳ接続は実際にｗｅｂプロキシィを通る。認証サーバ（ＡＳ）が受け取るソース・アドレスはｗｅｂプロキィシのアドレスであり、これは、モバイル端末（ＭＴ）のユーザ装置の識別に使用することはできず、従って、安全な接続を確保する際、アクセス・ポイントにより使用することはできない。

【０００９】

現在のｗｅｂブラウザと基とする認証方法においては、無線ＬＡＮとＡＳ（認証サーバ）は同一のエンティティの一部であり、従って前述の問題は問題とならないかもしれない。しかしながら、ホット・スポット無線ＬＡＮへのアクセスのためにバーチャル・オペレータのコンセプトが一層広範囲に展開されるにつれ、コンピュータに侵入するハッキングの可能性が増大するので、ソースＩＰアドレスだけに頼らずに認証セッションを識別（確

認）することは、より一層緊急の問題となる。
【発明の開示】
【００１０】
（発明の概要）
本発明は、上述した問題を解決するために、無線ＬＡＮ環境内でセキュリティとアクセスの制御を改善するための方法を提供する。本発明による方法では、セッションの識別（セッションＩＤ）をＨＴＴＰのリクエストの内に埋め込み、認証サーバ内でセッションＩＤを使用して２つのＨＴＴＰセッションをマッチさせることにより、認証メッセージに関連するモバイル端末を独自に識別（確認）する。アクセスのリクエストは、無線ＬＡＮ内のサーバの方に向け直され、無線ＬＡＮはそのセッションＩＤを提供し、セッションＩＤをモバイル端末にマップするマッピング・データを記憶して、セッションＩＤが埋め込まれているｗｅｂページを発生し、そのｗｅｂページはモバイル端末に送信される。
【００１１】
アクセス・ポイントは、モバイル端末からのｗｅｂリクエストを処理して、セッションＩＤがＵＲＬ（ｕｎｉｖｅｒａｌ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ）内に埋め込まれるようにする。更に、アクセス・ポイントは、セッションＩＤとモバイル端末の媒体アクセス制御アドレスとの間のマッピングを維持する。認証サーバが、認証の結果を受信したことをアクセス・ポイントに通知すると、セッションＩＤはその後、そのモバイル端末を独自に識別（確認）するために使用される。
【００１２】
本発明の１つの実施例で、無線ローカル・エリア・ネットワーク（無線ＬＡＮ）へのアクセスを制御するための方法は：無線ＬＡＮの視聴圏（カバレッジ・エリア）内に配置されるモバイル端末から無線ＬＡＮにアクセスするためのリクエストを受信するステップと、セッションＩＤを、モバイル端末に関連する識別子に関連づけるステップと、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶するステップと、認証リクエスト（これには、セッションＩＤが含まれる）を該当する認証サーバに送信するステップと、モバイル端末に関する認証メッセージ（セッションＩＤを含む）を該当する認証サーバから受信するステップと、記憶されたマッピング・データに応答し、受信された認証メッセージをモバイル端末に相関させるステップと、受信された認証メッセージに応答し、モバイル端末から無線ＬＡＮへのアクセスを制御するステップと、から成る。
【００１３】
識別子は、モバイル端末を独自に識別するために使用できるモバイル端末のパラメータまたは特性である。モバイル端末の識別子は、モバイル端末に関連する媒体アクセス制御アドレス、またはモバイル端末に関連するＩＰアドレスからなる。セッションＩＤは、無線ＬＡＮで発生されるｗｅｂページ内に、例えば、認証サーバとＨＴＴＰＳセッションへのサブミット・ボタン（ｓｕｂｍｉｔ　ｂｕｔｔｏｎ）に関連するＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）内に、埋め込まれる。
【００１４】
本発明は、添付されている図面に関連して読まれる以下の詳細な説明から最も良く理解される。図面に示す種々の特徴は完全に特定されておらず、明確にするため、任意に拡張されまたは短縮される。
【発明を実施するための最良の形態】
【００１５】
図面において、回路および関連するブロックおよび矢印は、電気信号を搬送する電気回路および関連する配線またはデータ・バスとして実施される本発明による方法の機能を表す。１つまたは複数の関連する矢印は、本発明の方法または装置がディジタル・プロセスとして実施される場合、ソフトウェア・ルーチン間の通信（例えば、データの流れ）を表す。
【００１６】
図１で、１つまたは複数のモバイル端末（１４０$_1$～１４０$_n$）は、アクセス・ポイン

ト（１３０$_1$～１３０$_n$）および関連するコンピュータ１２０を介して認証サーバ１５０と通信し、安全を確保されたデータ・ベース、またはハッカーのような無認可のエンティティからの高度のセキュリティを要する他のソース、にアクセスすることを目的とする。

【００１７】

図１で、ＩＥＥＥ８０２．１ｘアーキテクチャは、相互に作用し比較的高いネットワーク・スタックの層に透明なステーション・モビリティ（可動性）を与える幾つかのコンポーネントおよびサービスを包含する。ＩＥＥＥ８０２．１ｘネットワークは、アクセス・ポイント１３０$_{1-n}$およびモバイル端末１４０$_{1-n}$のようなアクセス・ポイント・ステーションを、無線メディアと接続しＩＥＥＥ８０２．１ｘプロトコルの機能を含むコンポーネントとして、規定する、これはＭＡＣ（Ｍｅｄｉｕｍ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ：媒体アクセス制御）１３４$_{1-n}$および対応するＰＨＹ（Ｐｈｙｓｉｃａｌ Ｌａｙｅｒ：物理層）（図示せず）、および無線メディアへの接続１２７である。ＩＥＥＥ８０２．１ｘの機能は、無線モデムまたはネットワーク・アクセスまたはインタフェース・カードのハードウェアとソフトウェアで実施される。本発明は、ダウンロード・リンクのトラフィック（認証サーバからラップトップのようなモバイル端末にいたる）のためにＩＥＥＥ８０２．１ｘ無線ＬＡＮの媒体アクセス制御層と互換性のアクセス・ポイント１３０$_{1-n}$が、１つまたは複数の無線モバイル装置１４０$_{1-n}$、ローカル・サーバ１２０およびバーチャル・オペレータ（認証サーバ１５０を含む）の認証に参加できるように、通信ストリーム内で識別手段を実施するための方法を提案する。

【００１８】

本発明では、モバイル端末自体およびＩＥＥＥ８０２．１ｘプロトコルに従うその通信ストリームを認証することによって、アクセス１６０は、各モバイル端末１４０$_{1-n}$が無線ＬＡＮ１２４（複数のアクセス・ポイントおよびローカル・サーバ１２０を含む）に安全にアクセスできるようにする。アクセス１６０がこのように安全なアクセスを可能にする様子は、モバイル無線通信装置（例えば、モバイル端末１４０$_n$）、公的無線ＬＡＮ１２４、ローカルｗｅｂサーバ１２０、および認証サーバ１５０$_n$の間で起こる相互作用の順序を示す図２を参照することにより最も良く理解できる。ＩＥＥＥ８０２．１ｘプロトコルで構築されると、アクセス・ポイント１３０$_n$（図１）は、被制御ポートと未制御ポート（アクセス・ポイントがモバイル端末１４０$_n$と情報を交換する経路となる）を維持する。アクセス・ポイント１３０$_n$で維持される被制御ポートは、無線ＬＡＮ１２４とモバイル端末１４０$_n$間のアクセス・ポイントを通過するデータ・トラフィックのような非認証情報のエントリウエイ（ｅｎｔｒｙｗａｙ：入り道）として機能する。通常、アクセス・ポイント１３０$_n$は、モバイル無線通信装置の認証まで、ＩＥＥＥ８０２．１ｘに従いそれぞれの被制御ポートを閉じられた状態に保つ。アクセス・ポイント１３０$_n$は常に、それぞれの未制御（制御されない）ポートを開いた状態に維持して、モバイル端末１４０$_n$が認証サーバ１５０$_n$とデータを交換できるようにする。

【００１９】

図２に関し、無線ＬＡＮ１２４内のモバイル端末１４０$_n$のセキュリティを改善する本発明の方法は、ＨＴＴＰブラウザのリクエスト（２０５）を向け直し（２１０）、ＨＴＴＰリクエスト２０５内にセッションＩＤ２１５を埋め込み、そして認証サーバ１５０$_n$内のセッションＩＤ（２１５）を使用して２つのＨＴＴＰセッションをマッチさせることにより、達成される。

【００２０】

本発明の方法は、ＵＲＬ内にセッションＩＤ２１５を埋め込むことによって、無線ＬＡＮ１２４、アクセス・ポイント１３０$_n$、を通してモバイル端末１４０$_n$からのアクセスのリクエスト（モバイル端末１４０$_n$からのｗｅｂのリクエスト２０５）を処理する。

【００２１】

図２に関して、無線ＬＡＮ環境１２４内でモバイル端末１４０$_n$のセキュリティを改善するための本発明による方法は、ブラウザのリクエストをローカルｗｅｂサーバ１２０に向け直す（２２０）。ローカル・サーバ１２０は、モバイル端末１４０$_n$に関連する媒体

アクセス制御アドレス１３８$_n$を獲得し、セッションＩＤ２１５を発生し、媒体アクセス制御アドレス１３８$_n$とセッションＩＤ２１５を関連づけるマッピングを記憶する。無線ＬＡＮ１２４は、モバイル端末１４０$_n$の媒体アクセス制御アドレス１３８$_n$とセッションＩＤ２１５との間のマッピングを維持する。ローカル・サーバ１２０はｗｅｂページを発生し、バーチャル・オペレータを選択することをモバイル端末１４０のユーザにリクエストし、該当する認証サーバ１５０を選択し、送信するためのセッションＩＤ２１５をｗｅｂページ２３７内に埋め込む。また、ローカル・サーバ１２０は、ＵＲＬアドレス内に埋め込まれた関連するセッションＩＤ２１５を有する媒体アクセス制御アドレス１３８$_n$を送り返す（２３０）。

【００２２】

モバイル端末は反応し、サブミット・ボタンに関連するＵＲＬを埋め込み、認証サーバ１５０でＨＴＴＰＳセッションを開始させる。それによって、無線ＬＡＮ１２４は、セッションＩＤ２１５が埋め込まれている認証リクエスト２４０をＨＴＴＰＳを通して認証サーバ１５０$_n$に送信する。その後、認証サーバ１５０$_n$はセッションＩＤ２１５を処理し、認証の成功を確認（２５０）するセッションＩＤ２１５を、無線ＬＡＮ１２４を介しアクセス・ポイント１３０$_n$に伝達する。このプロセスには、セッションＩＤ２１５に関連する媒体アクセス制御アドレスをアクセス・ポイントで受信するステップも含まれ、それにより、媒体アクセス制御アドレスを有するすべての通信がモバイル端末１４０$_n$で受信できるようにする。前述したプロセスによって、アクセス・ポイント１３０$_n$とモバイル端末１４０$_n$間の通信が暗号化され、より一層安全なアクセス制御が保証される。

【００２３】

アクセス・ポイント１３０$_n$と認証サーバ１５０$_n$がファイアウォール１２２あるいはネットワーク・アドレス変換サーバで分離されると、認証サーバ１５０$_n$はアクセス・ポイント１３０$_{1-n}$と直接通信できない。この問題は、最初にアクセス・ポイント１３０$_n$を認証サーバ１５０$_n$と接触させて、通信環境を確立することによって解決できる。モバイル端末１４０$_{1-n}$のうちの１つが認証サーバ１５０$_n$とＨＴＴＰＳ通信を開始することをアクセス・ポイント１３０$_n$が検出すると、関連するアクセス・ポイント１４０$_n$は、関連するセッションＩＤ２１５と共に、認証サーバ１５０$_n$にメッセージを送信し、認証サーバ１５０$_n$がそのセッションに関する認証の結果を返送することを知らせる。

【００２４】

アクセス・ポイント１４０$_n$は、認証サーバ１５０$_n$との接触を確立する際に利用できる幾つかのオプションを有する。例えば、アクセス・ポイント１４０$_n$は、アクセス・ポイント１４０$_n$の付加利益を有するＨＴＴＰＳおよび現存するプロトコルを利用する認証サーバ１５０$_n$を利用して、互いに認証し合い、相互間の通信を確保する。この方法における１つの不利な点は、ＨＴＴＰＳが、ＴＣＰ（Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）に繰越しされる（ｃａｒｒｉｅｄ ｏｖｅｒ）ことであり、従って、モバイル端末１４０$_n$が認証されるまで、ＴＣＰ接続が開いた状態のままであることが要求される。このため、リソースがアクセス・ポイント１４０$_n$上でキュー（ｑｕｅｕｅ）の中に入れられるかもしれない。

【００２５】

これに代る別の例では、アクセス・ポイント１３０$_n$と認証サーバ１５０との間の通信のために、ＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）に基づくＲＡＤＩＵＳ（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ-Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ）プロトコルを利用する。この方法の利点は、モバイル端末１４０$_n$が認証されている間、アクセス・ポイント１３０$_n$と認証サーバ１５０との間に接続を維持する必要がないことである。この方法は、特定のファイアウォールだけがＨＴＴＰ、ＨＴＴＰＳ、ＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、ＴＥＬＮＥＴ（テルネット）を通過させられるので、すべてのファイアウォール（１２２）構成においてうまく機能するとはかぎらない。

【００２６】

図示した本発明の形態は単に好ましい実施例であり、部品の機能と構成に種々の変更がなされ得る、例示され記述されたものに替えて同等の手段も使用される、特許請求の範囲に記載の本発明の精神と範囲から離脱することなく或る特徴が他の特徴と独立して使用される。

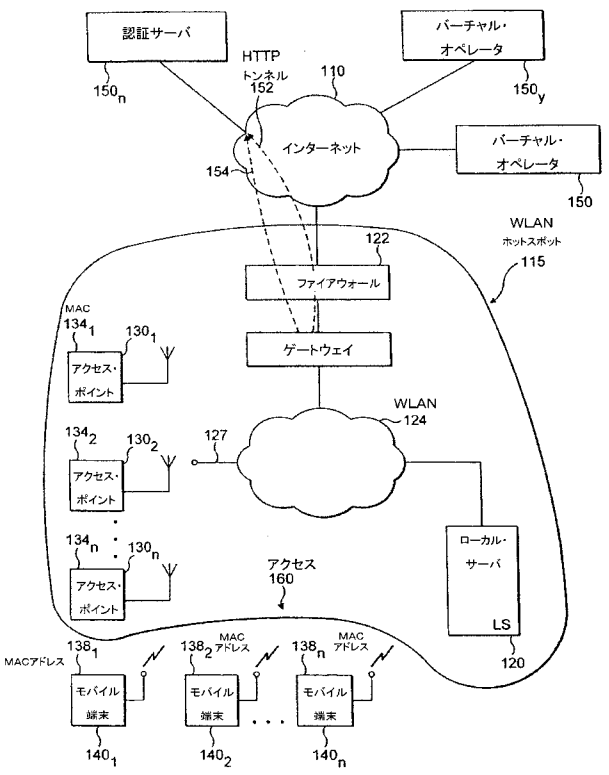
【図面の簡単な説明】

【００２７】

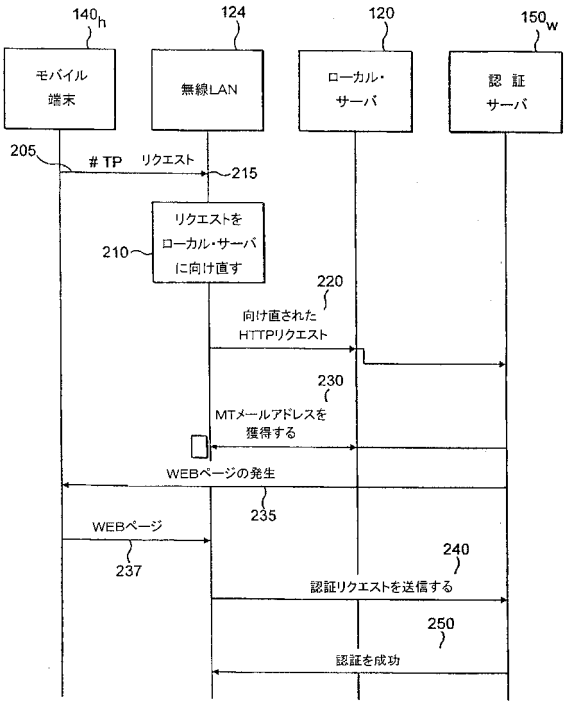
【図１】モバイル無線通信装置を認証する本発明の原理による方法を実施するための通信システムのブロック図である。

【図２】本発明の方法の流れ図である。

【図１】



【図２】



【手続補正書】
【提出日】平成17年3月29日(2005.3.29)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コミュニケーション・ネットワークへのアクセスを制御するための方法であって、
コミュニケーション・ネットワークの視聴圏内に配置されるモバイル端末からコミュニケーション・ネットワークにアクセスするためのリクエストを受信するステップと、
セッションＩＤを、モバイル端末に関連する識別子と関連づけ、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶するステップと、
セッションＩＤを含む、認証リクエストをコミュニケーション・ネットワークからコミュニケーション・ネットワークの外側の該当する認証サーバに送信するステップと、
モバイル端末に関する認証メッセージ（セッションＩＤを含む）を該当する認証サーバから前記コミュニケーション・ネットワーク内に受信するステップと、
記憶されたマッピング・データに応答し、受信された認証メッセージをモバイル端末に相関させるステップと、
受信された認証メッセージに応答し、モバイル端末からコミュニケーション・ネットワークへのアクセスを制御するステップと、から成る、前記方法。
【請求項２】
前記関連づけるステップで、セッションＩＤをモバイル端末の媒体アクセス制御アドレスと関連づけ、セッションＩＤをモバイル端末の媒体アクセス制御アドレスにマップするデータを記憶する、請求項１記載の方法。
【請求項３】
前記関連づけるステップで、セッションＩＤを、モバイル端末に関連するＩＰアドレスと関連づけ、セッションＩＤをモバイル端末に関連するＩＰアドレスにマップするデータを記憶する、請求項１記載の方法。
【請求項４】
セッションＩＤを含むリクエストをモバイル端末に送信するステップと、
モバイル端末から前記リクエストへの応答（その中に埋め込まれたセッションＩＤを含む）を受信し、認証モバイル端末用に認証サーバに該当するインジケータを受信するステップと、を更に含む、請求項１記載の方法。
【請求項５】
前記モバイル端末にリクエストを送信するステップで、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、ｗｅｂページをモバイル端末に送信する、請求項４記載の方法。
【請求項６】
ＨＴＴＰＳセッションを開始するためにサブミット・ボタンに関連するＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）内にセッションＩＤが埋め込まれる、請求項５記載の方法。
【請求項７】
ＨＴＴＰＳセッションがモバイル端末と認証サーバとの間で開始されると、コミュニケーション・ネットワークと認証サーバとの間に通信環境を確立し、よって、認証サーバが認証メッセージをコミュニケーション・ネットワークに送信するステップを更に含む、請求項６記載の方法。
【請求項８】
前記コミュニケーション・ネットワークのアクセス・ポイントからリクエストをコミュ

ニケーション・ネットワークに関連するローカル・サーバの方に向け直し、ローカル・サーバは前記セッションＩＤを、モバイル端末に関連する前記識別子と関連づけ、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶する、請求項１に記載の方法。

【請求項９】

無線通信チャンネルを通して複数のモバイル端末のうち１つと通信するためのアクセス・ポイントと、

アクセス・ポイントに結合されるローカル・サーバと、

前記アクセス・ポイントとローカル・サーバに結合されて、コミュニケーション・ネットワークを、複数の認証サーバの１つに結合される第２のコミュニケーション・ネットワークに結合させる手段と、からなる、コミュニケーション・ネットワークにおいて、

第１のコミュニケーション・ネットワークの視聴圏内に配置されるモバイル端末によるアクセスのリクエストに応答し、

前記ローカル・サーバは、セッションＩＤを、リクエストしているモバイル端末に関連する識別子と関連づけ、セッションＩＤを、リクエストしているモバイル端末に関連する識別子にマップするマッピング・データを記憶し、

セッションＩＤを含む、認証のリクエストを前記第２のコミュニケーション・ネットワークに結合される前記複数の認証サーバの１つの該当する認証サーバに送信し、

該当する認証サーバから受信された認証メッセージを、リクエストしているモバイル端末に相関させ、

受信された認証メッセージに応答し、モバイル端末による前記第１のコミュニケーション・ネットワークへのアクセスを制御する、前記第１のコミュニケーション・ネットワーク。

【請求項１０】

リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末の媒体アクセス制御アドレスに対応する、請求項１３記載の第１のコミュニケーション・ネットワーク。

【請求項１１】

リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末に関連するＩＰアドレスに対応する、請求項１３記載の第１のコミュニケーション・ネットワーク。

【請求項１２】

アクセス・ポイントで、セッションＩＤをモバイル端末に送信し、認証サーバに送信される認証のリクエスト（その中に埋め込まれたセッションＩＤを含む）をモバイル端末から受信する、請求項１３記載の第１のコミュニケーション・ネットワーク。

【請求項１３】

ローカル・サーバは、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、アクセス・ポイントから前記ｗｅｂページをモバイル端末に送信する、請求項１６記載の第１のコミュニケーション・ネットワーク。

【請求項１４】

ローカル・サーバが、ＨＴＴＰＳセッションを開始させるために、サブミット・ボタンに関連するＵＲＬ内にセッションＩＤを埋め込む、請求項１７記載の第１のコミュニケーション・ネットワーク。

【手続補正書】

【提出日】平成18年6月2日(2006.6.2)

【手続補正１】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】
【特許請求の範囲】
【請求項１】
コミュニケーション・ネットワークへのアクセスを制御するための方法であって、
コミュニケーション・ネットワークの視聴圏内に配置されるモバイル端末からコミュニケーション・ネットワークにアクセスするためのリクエストを受信するステップと、
セッションＩＤを、モバイル端末に関連する識別子と関連づけ、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶するステップと、
セッションＩＤを含む、認証リクエストをコミュニケーション・ネットワークからコミュニケーション・ネットワークの外側の該当する認証サーバに送信するステップと、
モバイル端末に関する認証メッセージ（セッションＩＤを含む）を該当する認証サーバから前記コミュニケーション・ネットワーク内に受信するステップと、
記憶されたマッピング・データに応答し、受信された認証メッセージをモバイル端末に相関させるステップと、
受信された認証メッセージに応答し、モバイル端末からコミュニケーション・ネットワークへのアクセスを制御するステップと、から成る、前記方法。
【請求項２】
前記関連づけるステップで、セッションＩＤをモバイル端末の媒体アクセス制御アドレスと関連づけ、セッションＩＤをモバイル端末の媒体アクセス制御アドレスにマップするデータを記憶する、請求項１記載の方法。
【請求項３】
前記関連づけるステップで、セッションＩＤを、モバイル端末に関連するＩＰアドレスと関連づけ、セッションＩＤをモバイル端末に関連するＩＰアドレスにマップするデータを記憶する、請求項１記載の方法。
【請求項４】
セッションＩＤを含むリクエストをモバイル端末に送信するステップと、
モバイル端末から前記リクエストへの応答（その中に埋め込まれたセッションＩＤを含む）を受信し、認証モバイル端末用に認証サーバに該当するインジケータを受信するステップと、を更に含む、請求項１記載の方法。
【請求項５】
前記モバイル端末にリクエストを送信するステップで、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、ｗｅｂページをモバイル端末に送信する、請求項４記載の方法。
【請求項６】
ＨＴＴＰＳセッションを開始するためにサブミット・ボタンに関連するＵＲＬ内にセッションＩＤが埋め込まれる、請求項５記載の方法。
【請求項７】
ＨＴＴＰＳセッションがモバイル端末と認証サーバとの間で開始されると、コミュニケーション・ネットワークと認証サーバとの間に通信環境を確立し、よって、認証サーバが認証メッセージをコミュニケーション・ネットワークに送信するステップを更に含む、請求項６記載の方法。
【請求項８】
前記コミュニケーション・ネットワークのアクセス・ポイントからリクエストをコミュニケーション・ネットワークに関連するローカル・サーバの方に向け直し、ローカル・サーバは前記セッションＩＤを、モバイル端末に関連する前記識別子と関連づけ、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶する、請求項１に記載の方法。
【請求項９】
無線通信チャンネルを通して複数のモバイル端末のうち１つと通信するためのアクセス・ポイントと、

アクセス・ポイントに結合されるローカル・サーバと、
前記アクセス・ポイントとローカル・サーバに結合されて、第１のコミュニケーション・ネットワークを、複数の認証サーバの１つに結合される第２のコミュニケーション・ネットワークに結合させる手段と、からなる、第１のコミュニケーション・ネットワークにおいて、
第１のコミュニケーション・ネットワークの視聴圏内に配置されるモバイル端末によるアクセスのリクエストに応答し、
前記ローカル・サーバは、セッションＩＤを、リクエストしているモバイル端末に関連する識別子と関連づけ、セッションＩＤを、リクエストしているモバイル端末に関連する識別子にマップするマッピング・データを記憶し、
セッションＩＤを含む、認証のリクエストを前記第２のコミュニケーション・ネットワークに結合される前記複数の認証サーバの１つの該当する認証サーバに送信し、
該当する認証サーバから受信された認証メッセージを、リクエストしているモバイル端末に相関させ、
受信された認証メッセージに応答し、モバイル端末による前記第１のコミュニケーション・ネットワークへのアクセスを制御する、前記第１のコミュニケーション・ネットワーク。
【請求項１０】
リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末の媒体アクセス制御アドレスに対応する、請求項９記載の第１のコミュニケーション・ネットワーク。
【請求項１１】
リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末に関連するＩＰアドレスに対応する、請求項９記載の第１のコミュニケーション・ネットワーク。
【請求項１２】
アクセス・ポイントで、セッションＩＤをモバイル端末に送信し、認証サーバに送信される認証のリクエスト（その中に埋め込まれたセッションＩＤを含む）をモバイル端末から受信する、請求項９記載の第１のコミュニケーション・ネットワーク。
【請求項１３】
ローカル・サーバは、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、アクセス・ポイントから前記ｗｅｂページをモバイル端末に送信する、請求項１２記載の第１のコミュニケーション・ネットワーク。
【請求項１４】
ローカル・サーバが、ＨＴＴＰＳセッションを開始させるために、サブミット・ボタンに関連するＵＲＬ内にセッションＩＤを埋め込む、請求項１３記載の第１のコミュニケーション・ネットワーク。
【請求項１５】
コミュニケーション・ネットワークへのアクセスを制御するための方法であって、
コミュニケーション・ネットワークの視聴圏内に配置されるモバイル端末からコミュニケーション・ネットワークにアクセスするためのリクエストを受信するステップと、
セッションＩＤを、モバイル端末に関連する識別子と関連づけ、セッションＩＤをモバイル端末に関連する識別子にマップするデータを記憶するステップと、
セッションＩＤを含む、認証リクエストをコミュニケーション・ネットワークからコミュニケーション・ネットワークの外側の該当する認証サーバに送信するステップと、
モバイル端末に関する認証メッセージ（セッションＩＤを含む）を該当する認証サーバから前記コミュニケーション・ネットワーク内に受信するステップと、
記憶されたマッピング・データに応答し、受信された認証メッセージをモバイル端末に相関させるステップと、

受信された認証メッセージに応答し、モバイル端末からコミュニケーション・ネットワークへのアクセスを制御するステップと、から成る、前記方法。

【請求項１６】

前記関連づけるステップで、セッションＩＤをモバイル端末の媒体アクセス制御アドレスと関連づけ、セッションＩＤをモバイル端末の媒体アクセス制御アドレスにマップするデータを記憶する、請求項１５記載の方法。

【請求項１７】

前記関連づけるステップで、セッションＩＤを、モバイル端末に関連するＩＰアドレスと関連づけ、セッションＩＤをモバイル端末に関連するＩＰアドレスにマップするデータを記憶する、請求項１５記載の方法。

【請求項１８】

セッションＩＤを含むリクエストをモバイル端末に送信するステップと、

モバイル端末から前記リクエストへの応答（その中に埋め込まれたセッションＩＤを含む）を受信し、認証モバイル端末用に認証サーバに該当するインジケータを受信するステップと、を更に含む、請求項１５記載の方法。

【請求項１９】

前記モバイル端末にリクエストを送信するステップで、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、ｗｅｂページをモバイル端末に送信する、請求項１８記載の方法。

【請求項２０】

ＨＴＴＰＳセッションを開始するためにサブミット・ボタンに関連するＵＲＬ内にセッションＩＤが埋め込まれる、請求項１９記載の方法。

【請求項２１】

ＨＴＴＰＳセッションがモバイル端末と認証サーバとの間で開始されると、コミュニケーション・ネットワークと認証サーバとの間に通信環境を確立し、よって、認証サーバが認証メッセージをコミュニケーション・ネットワークに送信するステップを更に含む、請求項２０記載の方法。

【請求項２２】

無線通信チャンネルを通して複数のモバイル端末のうち１つと通信するためのアクセス・ポイントと、

アクセス・ポイントに結合されるローカル・サーバと、

前記アクセス・ポイントとローカル・サーバに結合されて、コミュニケーション・ネットワークを、複数の認証サーバの１つに結合される第２のコミュニケーション・ネットワークに結合させる手段と、からなる、コミュニケーション・ネットワークにおいて、

第１のコミュニケーション・ネットワークの視聴圏内に配置されるモバイル端末によるアクセスのリクエストに応答し、

前記ローカル・サーバは、セッションＩＤを、リクエストしているモバイル端末に関連する識別子と関連づけ、セッションＩＤを、リクエストしているモバイル端末に関連する識別子にマップするマッピング・データを記憶し、

セッションＩＤを含む、認証のリクエストを前記第２のコミュニケーション・ネットワークに結合される前記複数の認証サーバの１つの該当する認証サーバに送信し、

該当する認証サーバから受信された認証メッセージを、リクエストしているモバイル端末に相関させ、

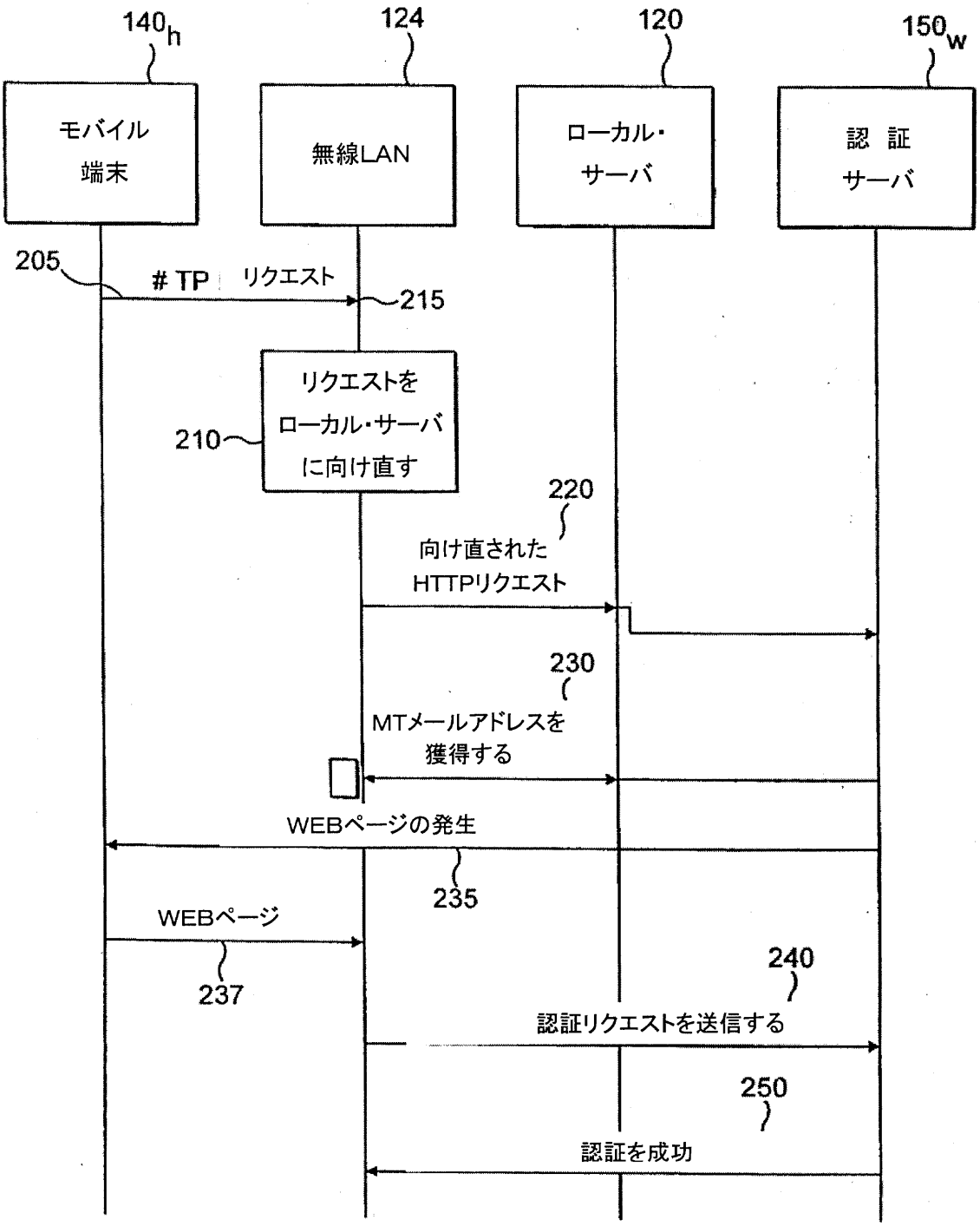
受信された認証メッセージに応答し、モバイル端末による前記第１のコミュニケーション・ネットワークへのアクセスを制御する、前記第１のコミュニケーション・ネットワーク。

【請求項２３】

リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末の媒体アクセス制御アドレスに対応する、請求項２２記載の第１のコミュニケーション・ネットワーク。

【請求項２４】
リクエストしているモバイル端末に関連する識別子が、リクエストしているモバイル端末に関連するＩＰアドレスに対応する、請求項２２記載の第１のコミュニケーション・ネットワーク。
【請求項２５】
アクセス・ポイントで、セッションＩＤをモバイル端末に送信し、認証サーバに送信される認証のリクエスト（その中に埋め込まれたセッションＩＤを含む）をモバイル端末から受信する、請求項２２記載の第１のコミュニケーション・ネットワーク。
【請求項２６】
ローカル・サーバは、モバイル端末が該当する認証サーバを選択することをリクエストするｗｅｂページを発生し、セッションＩＤをｗｅｂページ内に埋め込み、アクセス・ポイントから前記ｗｅｂページをモバイル端末に送信する、請求項２５記載の第１のコミュニケーション・ネットワーク。
【請求項２７】
ローカル・サーバが、ＨＴＴＰＳセッションを開始させるために、サブミット・ボタンに関連するＵＲＬ内にセッションＩＤを埋め込む、請求項２６記載の第１のコミュニケーション・ネットワーク。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図２
【補正方法】変更
【補正の内容】

【図２】


140h
124
120
150w
モバイル
端末
無線LAN
ローカル・
サーバ
認 証
サーバ
205
TP リクエスト
215
リクエストを
ローカル・サーバ
に向け直す
210
220
向け直された
HTTPリクエスト
230
MTメールアドレスを
獲得する
WEBページの発生
235
WEBページ
237
240
認証リクエストを送信する
250
認証を成功

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/06566

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 713/155,168
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/155,168,200,201; 455/410,411

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,233,608 B1 (LAURSEN et al) 15 May 2001 (15.05.2001),column 6,lines 33-62; column 11,lines 4-41.	1-18
A	US 6,151,628 A (XU et al) 21 November 2000 (21.11.2000),column 4,lines 45-64; column 10,lines 28-52.	1-18
A	US 6,223,289 B1 (WALL et al) 24 April 2001(24.04.2001), column 7,lines 3-30;column 9,lines 42-61.	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
10 December 2004 (10.12.2004)

Date of mailing of the international search report
05 JAN 2005

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Hosuk Song
for James R. Matthews
Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

PCT/US04/06566

INTERNATIONAL SEARCH REPORT

Continuation of B. FIELDS SEARCHED Item 3:
EAST
search terms: WLAN, wireless,cellular,authentication,MAC,session,key,mobile,access,point,ipsec,packets,https,ISP,proxy

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 ザング，ジヤンビアオ
アメリカ合衆国 ニユージヤージ州 ブリツジウオーター ジエンナ・ドライブ ２０

Ｆターム(参考) 5B285 AA01 BA01 CA04 CB42 CB73 CB84 DA05
5J104 AA07 KA02 KA04 MA01 NA05 NA38 PA01 PA07
5K033 AA08 CB01 DA19
5K067 AA32 BB04 DD17 DD51 DD57 EE02 EE10 EE16 EE23 HH23