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

特許第4476815号
(P4476815)

(45)発行日　平成22年6月9日(2010.6.9)　(24)登録日　平成22年3月19日(2010.3.19)

(51)Int.Cl.		F I		
H04W 84/12	(2009.01)	H04L	12/28	300Z
H04L 9/32	(2006.01)	H04L	9/00	675A
H04L 9/08	(2006.01)	H04L	9/00	675D
H04W 12/00	(2009.01)	H04L	9/00	601A
H04W 74/00	(2009.01)	H04Q	7/00	180

請求項の数 9　(全 8 頁)　最終頁に続く

(21)出願番号　特願2004-571480 (P2004-571480)
(86)(22)出願日　平成15年12月29日 (2003.12.29)
(65)公表番号　特表2006-524925 (P2006-524925A)
(43)公表日　平成18年11月2日 (2006.11.2)
(86)国際出願番号　PCT/US2003/041574
(87)国際公開番号　WO2004/098166
(87)国際公開日　平成16年11月11日 (2004.11.11)
審査請求日　平成18年10月23日 (2006.10.23)
(31)優先権主張番号　10/424,442
(32)優先日　平成15年4月28日 (2003.4.28)
(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，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　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】セキュア無線ＬＡＮアクセスの技術

(57)【特許請求の範囲】
【請求項１】
モバイル通信装置が無線ローカルエリアネットワーク（ＬＡＮ）にセキュアにアクセスすることを可能にする方法であって、
前記無線ＬＡＮにおいて前記モバイル通信装置からアクセス要求を受信するステップと、
前記モバイル通信装置を認証するステップと、
前記モバイル通信装置について前記モバイル通信装置内でコントロール要素をパラメータ化する暗号鍵を確立するステップと、
前記暗号鍵を有するコマンドを前記モバイル通信装置に送信し、前記コマンドは、前記パラメータ化されたコントロール要素を前記モバイル通信装置により実行させ、前記装置内に前記暗号鍵を設定させ、実行時に、前記モバイル通信装置により生じた通信トラヒックが前記暗号鍵で暗号化されるように、前記暗号鍵で前記装置を構成するステップと
を有する方法。
【請求項２】
請求項１に記載の方法であって、
前記確立するステップは、Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ暗号鍵を確立するステップを有する方法。
【請求項３】
請求項２に記載の方法であって、

前記パラメータ化するステップは、前記パラメータ化されたコントロール要素のパラメータとして前記Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ暗号鍵を使用するステップを有する方法。

【請求項４】

請求項３に記載の方法であって、

前記パラメータ化されたコントロール要素に署名し、前記Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ暗号鍵に署名し、どのサーバが前記パラメータ化されたコントロール要素を起動して前記Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ暗号鍵を生じたかを示すステップを更に有する方法。

【請求項５】

請求項４に記載の方法であって、

前記Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ暗号鍵に署名するステップは、前記モバイル通信装置により保持されたローカル時間を有するタイムスタンプを前記鍵に埋め込むステップを有する方法。

【請求項６】

少なくとも１つのモバイル通信装置にセキュアなアクセスを提供する無線ローカルエリアネットワーク（ＬＡＮ）であって、

モバイル通信装置からアクセス要求を受信する少なくとも１つのアクセスポイントと、

（１）前記モバイル通信装置を認証し、（２）前記モバイル通信装置について前記モバイル通信装置のコントロール要素をパラメータ化する暗号鍵を確立し、（３）前記暗号鍵を有するコマンドを送信し、前記コマンドは、前記モバイル通信装置により生じた通信トラヒックが前記暗号鍵で暗号化されるように、前記パラメータ化されたコントロール要素を前記モバイル通信装置により実行させ、前記暗号鍵を設定させる認証サーバと、

前記アクセスポイントと前記認証サーバとをリンクするコアネットワークと

を有する無線ローカルエリアネットワーク。

【請求項７】

請求項６に記載の無線ＬＡＮであって、

前記暗号鍵は、Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ鍵を有する無線ＬＡＮ。

【請求項８】

請求項７に記載の無線ＬＡＮであって、

前記認証サーバは、パラメータとしてＷｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ暗号鍵を使用して前記コントロール要素をパラメータ化する無線ＬＡＮ。

【請求項９】

請求項８に記載の無線ＬＡＮであって、

前記認証サーバは、前記コントロールに署名し、前記Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ暗号鍵に署名する無線ＬＡＮ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、モバイル通信装置がセキュアに無線ローカルエリアネットワーク（ＬＡＮ）にアクセスすることを可能にする技術に関する。

【背景技術】

【０００２】

現在、データ通信サービスのプロバイダは、休憩施設やカフェや図書館のような公衆アクセス可能施設で無線ローカルエリアネットワーク（ＬＡＮ）（“ホットスポット”）を確立しており、モバイル通信装置がプライベート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有料でアクセスすることを可能にしている。このような公衆アクセス可能施設に入ると、モバイル通信装置は、一般的に無線チャネルで、アクセスポイント（ＡＰ）と通信リンクを確立し、無線ＬＡＮとその向こうの公衆又はプライ

ベートネットワークとにアクセスする。現在、ウェブブラウザに基づく認証では、モバイル通信装置の初期検証は、装置のブラウザソフトウェアにより実行されるセキュア・ハイパーテキスト転送プロトコル（ＨＴＴＰＳ）の使用を通じて生じる。しかし、モバイル通信装置の認証は、全体のセキュリティに影響を与える複数の要因のうちの１つに過ぎない。セキュリティに影響を与える他の要因は、トラヒック認証である。

【０００３】

モバイル通信装置の成功した認証の後に、受信したトラヒックが認証済のモバイル通信装置から生じており、無許可の送信者から生じていないことを、無線ＬＡＮがどのように確認するかについて問題が残る。実際に、モバイル通信装置は、装置の識別又は署名なしに、ＩＰパケット（更にＥｔｈｅｒｎｅｔ（登録商標）フレームに分解され得る）を生じる。従って、無線ＬＡＮの観点から、許可された送信者からの入力ＩＰパケットは、無許可の送信者からのものと全く同一に見える。従って、無線ＬＡＮには、許可されたモバイル通信装置からのトラヒックと、初期認証処理をなんとか回避したハッカーからのトラヒックとを区別する方法がない。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

従って、モバイル通信装置がセキュアに無線ＬＡＮにアクセスし、それにより前述の従来技術の欠点を克服することを可能にする技術の必要性が存在する。

【課題を解決するための手段】

【０００５】

簡単には、本原理によれば、モバイル通信装置がセキュアに無線ＬＡＮにアクセスすることを可能にする方法が提供される。その方法は、モバイル通信装置からのアクセス要求の無線ＬＡＮでの受信時に始まる。その後、無線ＬＡＮは、装置から受信した認証情報に従ってモバイル通信装置を認証する。モバイル通信装置を認証した後に、無線ＬＡＮは、実行可能プログラムを起動し、プライバシー鍵（一般的にはＷｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ（ＷＥＰ）暗号鍵）を可能にするように、モバイル通信装置に通知する。実際には、実行可能プログラムは、一般的に、成功した認証のときにモバイル通信装置にダウンロードされるＡｃｔｉｖｅＸプログラムを有する。ＷＥＰ暗号鍵を可能にするようにモバイル通信装置で実行可能プログラムを起動することに加えて、無線ＬＡＮはＷＥＰ自体を起動し、モバイル通信装置とのセキュアな通信を可能にする。最近、モバイル通信装置にあるブラウザソフトウェアプログラムは、ＡｃｔｉｖｅＸコントロールをサポートするため、ＷＥＰ暗号鍵を起動するためにこのような機能を使用することで、セキュアな無線ＬＡＮアクセスを確保するために、モバイル通信装置のトラヒックを認証する簡単な技術を得ることができる。ＡｃｔｉｖｅＸコントロールがモバイル装置のブラウザでサポートされていない場合、プラグインのような他の技術が使用され得る。

【発明を実施するための最良の形態】

【０００６】

図１は、少なくとも１つのモバイル通信装置、好ましくは複数のモバイル通信装置（例えばモバイル通信装置12_1、12_2及び12_3）が、プライベートデータネットワーク１４又はインターネットのような公衆データネットワーク１６にセキュアにアクセスすることを可能にするアクセス構成１１を有する通信ネットワーク１０のブロック概略図を示している。好ましい実施例では、モバイル通信装置12_1はラップトップコンピュータを有し、モバイル通信装置12_2は携帯情報端末（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）を有し、モバイル通信装置12_3は無線ハンドセットを有する。

【０００７】

図１のアクセス構成１１は、少なくとも１つ、好ましくは複数のアクセスポイント（ＡＰ）を有し（$AP18_1$－18_4で例示する）、そのアクセスポイントを介して、モバイル通信装置12_1、12_2及び12_3は、無線ローカルエリアネットワーク（ＬＡＮ）２０にそれぞれアクセスする。別々に図示されているが、$AP18_1$－18_4は、無線ＬＡ

Ｎ２０の一部を有する。ゲートウェイ２２は、無線ＬＡＮ２０とプライベート及び公衆ネットワーク（それぞれ１４及び１６）との間の通信パスを提供する。図示の実施例では、ＡＰ１８$_1$のような各ＡＰは、各モバイル通信装置内の無線トランシーバ（図示せず）と無線周波数信号を交換する無線トランシーバ（図示せず）を有する。このため、それぞれのＡＰ１８$_1$－１８$_4$は、“ＨｉｐｅｒＬａｎ２”又はＩＥＥＥ８０２．１１プロトコルのような１つ以上の周知の無線データ交換プロトコルを使用する。実際に、異なるＡＰは、異なるモバイル通信装置に適合するために、異なる無線プロトコルを使用してもよい。

【０００８】

ゲートウェイ２２は、無線ＬＡＮ２０と認証サーバ２４との間のリンクを提供する。実際に、認証サーバ２４は、潜在的なユーザについての情報を有するデータベースシステムの形式をとり、アクセスを求めるモバイル通信装置を各ＡＰ１８$_1$－１８$_4$が認証することを可能にする。別々のスタンドアローン型エントリーとして存在するのではなく、認証サーバ２４は無線ＬＡＮ２０内に存在してもよい。課金エージェント２６はゲートウェイ２２を通じて無線ＬＡＮ２０と接続を有し、無線ＬＡＮにアクセスする各モバイル通信装置の課金を容易にする。認証サーバ２４と同様に、課金エージェント２６の機能も無線ＬＡＮ２０内に存在してもよい。

【０００９】

本原理によれば、各装置１２$_1$－１２$_3$のような各モバイル通信装置が、無線ＬＡＮ２０にセキュアにアクセスし、装置自体とそれから生じたトラヒックとの双方の認証を提供することを可能にする技術が提供される。本原理の認証技術は、図２を参照してうまく理解され得る。図２は、モバイル通信装置（例えば装置１２$_1$）とＡＰ（例えばＡＰ１８$_1$）と認証サーバ２４との間で時間と共に生じた通信のシーケンスを示している。セキュアなアクセスを開始するために、図２のステップ１００の間に、モバイル通信装置１２$_1$はＡＰ１８$_1$にアクセス要求を送信する。実際には、モバイル通信装置１２$_1$は、装置により実行されたブラウザソフトウェアプログラム（図示せず）により開始されたＨＴＴＰＳアクセス要求を用いて、アクセス要求を開始する。アクセス要求に応じて、ステップ１０２の間に、ＡＰは、モバイル通信ソフトウェアのブラウザソフトウェアをＡＰのローカルウェルカムページにリダイレクトする。

【００１０】

ステップ１０２に続いて、図２のステップ１０４の間に、図１のモバイル通信装置１２$_1$は、適切な認証サーバの識別について図１のＡＰ１８$_1$にクエリ送出することにより、認証を開始する。それに応じて、図２のステップ１０６の間に、ＡＰ１８$_1$は適切な認証サーバ（例えばサーバ２４）の識別を決定し、図２のステップ１０８の間に、ＨＴＴＰコマンドを介してそのサーバにモバイル通信装置１２$_1$のブラウザソフトウェアを指示する。ステップ１０８の間に認証サーバ２４の識別を受信しているため、図２のステップ１１０の間に、モバイル通信装置１２$_1$はそのユーザ証明書をサーバに送信する。

【００１１】

モバイル通信装置１２$_1$からのユーザ証明書の受信時に、ステップ１１２の間に、認証サーバ２４はモバイル通信装置が有効なユーザを構成するか否かを決定する。そうである場合、ステップ１１４の間に、認証サーバ２４は、装置が装置のブラウザソフトウェアを通じてＡｃｔｉｖｅＸコントロールのＡｃｔｉｖｅＸコマンドを介して起動したＷｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ（ＷＥＰ）暗号鍵で、モバイル通信装置１２$_1$に応答する。簡単に言えば、基本的には、ＡｃｔｉｖｅＸコントロールはウェブページ内に埋め込まれ得る実行可能プログラムである。

Ｍｉｃｒｏｓｏｆｔ　Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒのような多数のソフトウェアブラウザプログラムは、このようなウェブページを表示し、遠隔サーバ（例えば認証サーバ２４）からダウンロードされ得る埋め込みＡｃｔｉｖｅＸコントロールを起動する機能を有する。ＡｃｔｉｖｅＸコントロールの実行は、ブラウザソフトウェアに内蔵されたセキュリティ機構により制限される。実際には、ほとんどのブラウザプログラムは、複数の異なる選択可能なセキュリティレベルを有する。最低レベルでは、ウェブページからの如

何なるＡｃｔｉｖｅＸコントロールも制限なしに起動され得る。最高レベルでは、ブラウザソフトウェアからＡｃｔｉｖｅＸコントロールは起動され得ない。

【００１２】

通常は、セキュリティレベルは中間に設定されており、その場合、デジタル署名を有するＡｃｔｉｖｅＸコントロールのみが起動され得る。このようなＡｃｔｉｖｅＸコントロールについて、ブラウザソフトウェアは、ＡｃｔｉｖｅＸコントロールを起動する前にまず署名の有効性を検査し、以下の条件が存在することを確認する。（１）ＡｃｔｉｖｅＸコントロールのソースがトレース可能であること、及び（２）ＡｃｔｉｖｅＸコントロールがそれに署名したエンティティ以外のものにより変更されていないこと。図示の実施例では、認証サーバ２４は、装置が認証された後に、モバイル通信装置１２$_1$のＷＥＰ鍵を配信及び設定するためにＡｃｔｉｖｅＸコントロールを使用する。ＡｃｔｉｖｅＸコントロールは非常に簡単であり、その唯一の機能は、埋め込みＡｃｔｉｖｅＸコントロールを備えたウェブページを装置に提供することにより、モバイル通信装置１２$_1$の鍵を設定することである。その埋め込みＡｃｔｉｖｅＸコントロールは、装置の認証に続いて認証サーバ２４により署名される。

【００１３】

ステップ１１４の間にモバイル通信装置１２$_1$にＷＥＰセッション鍵を提供した後に、ステップ１１６の間に、認証サーバ２４は対応のＷＥＰセッション鍵をＡＰ１８$_1$に提供する。次に、図２のステップ１１８の間に、モバイル通信装置１２$_1$はＷＥＰを可能にし、ステップ１２０の間に、ＡＰ１８$_1$に対してＷＥＰ暗号トラヒックの送信を開始する。その後、ＡＰはそのＷＥＰセッション鍵に従ってデータを解読する。

【００１４】

ほとんどの装置はＡｃｔｉｖｅＸコントロールをサポートするブラウザソフトウェアを使用しており、ほとんどの装置のブラウザソフトウェアのセキュリティレベルは一般的に中間に設定されているため、セキュアな無線ＬＡＮアクセスを可能にする前述の方法は、多数のモバイル通信装置にシームレスに動作する。ブラウザソフトウェアが最高レベルのセキュリティに現在設定されているモバイル通信装置では、ウェブブラウザソフトウェアのセキュリティ設定を中間に一時的に変更することをユーザに求める要求が装置に送信される。ＡｃｔｉｖｅＸコントロールをサポート可能なブラウザソフトウェアを使用しないモバイル通信装置では、ブラウザソフトウェアのプラグインが使用され得る。アクセスを求めるモバイル通信装置１２$_1$のブラウザソフトウェアがＡｃｔｉｖｅＸコントロールをサポートしないということをＡＰ１８$_1$が検出すると、モバイル通信装置１２$_1$のユーザは、小型のプラグインをダウンロードしてインストールするように促される。プラグインの機能は、ＡｃｔｉｖｅＸコントロールの鍵設定機能と基本的に同じである。プラグインがモバイル通信装置１２$_1$にインストールされると、認証サーバ２４は、プラグインを起動する特別のファイルにＷＥＰ鍵をパッケージすることにより、モバイル通信装置のＷＥＰ鍵を設定することができる。次に、プラグインは鍵のＷＥＰファイルを読み取り、モバイル通信装置１２$_1$に鍵を設定する。

【００１５】

実際には、ＡｃｔｉｖｅＸコントロールを設定するＷＥＰ鍵はパラメータ化されるべきである。換言すると、ＡｃｔｉｖｅＸコントロールはＷＥＰ鍵をパラメータとして受け取るべきである。このように、認証サーバ２４は、単一のコンパイル済ＡｃｔｉｖｅＸコントロールを維持し、要求側のモバイル通信装置に異なるパラメータを提供することにより、それを異なるセッションで使用しさえすればよい。その他の場合には、認証サーバ２４は、ＡｃｔｉｖｅＸコントロール内にＷＥＰ鍵を構築する（すなわちセッション毎に異なるＡｃｔｉｖｅＸコントロールを構築する）必要があり、非効率な処理になる。

【００１６】

ある状況では、パラメータ化の手法はセキュリティ攻撃を受けやすいことがある。ＡｃｔｉｖｅＸコントロールについて認識しているハッカーは、任意のパラメータでこのＡｃｔｉｖｅＸコントロールを起動するウェブページを潜在的に構成し得る。モバイル通信装

置がこのようなウェブページに直面した場合、装置のＷＥＰ鍵は不正確に設定され得る。大きな損害は生じないが、このような攻撃は、不正確に設定されたＷＥＰ鍵のため、モバイル通信装置のユーザを不便にする。モバイル通信装置１２$_1$がＡｃｔｉｖｅＸコントロールをサポートしておらず、適切なプラグインをダウンロードしなければならないときに、同様の問題が存在し得る。ハッカーは、モバイル通信装置１２$_1$のＷＥＰ鍵設定プラグインを起動する特別のファイル形式を備えたウェブページを構成し得る。この場合にも同様に、ＷＥＰ鍵がモバイル通信装置に不正確に設定されることを除いて、大きな損害は生じない。

【００１７】

この種類のセキュリティ攻撃は、サーバ署名の使用により阻止され得る。換言すると、認証サーバ２４は、ＡｃｔｉｖｅＸコントロールに署名するだけでなく、パラメータにも署名する。更に、ハッカーが以前に使用したパラメータを格納してユーザの装置の鍵を誤構成する繰り返し攻撃を回避するために、署名の鍵は埋め込みタイムスタンプを有する。この処理は以下のように動作する。モバイル通信装置１２$_1$により認証サーバ２４に提示された認証要求は、装置のローカルタイムスタンプを有するスクリプト（例えばＪａｖａｓｃｒｉｐｔ）を有する。モバイル通信装置１２$_1$は、一般的にはページのＨＴＭＬのフォームの隠れたフィールドとして、この情報を認証サーバ２４に送信する。それに応じて、認証サーバ２４は、暗号ＷＥＰ鍵を生成し、モバイル通信装置１２$_1$のローカルタイムとそれを連結し、サーバの秘密鍵でその結果を署名する。

【００１８】

認証サーバ２４は、ＡｃｔｉｖｅＸコントロールに対するパラメータとして署名の文字列（プラグインの場合には、プラグイン用のファイル）をモバイル通信装置１２$_1$に送信する。ＡｃｔｉｖｅＸコントロールは、サーバの公開鍵を内蔵している。モバイル通信装置１２$_1$での実行時に、ＡｃｔｉｖｅＸコントロールはパラメータを検査し、（１）パラメータが実際に認証サーバ２４からのものであること、及び（２）現在のローカルタイム及びパラメータのローカルタイムが繰り返し攻撃を回避するために適度にマッチすることを確保する。検査を通過した場合にのみ、鍵が設定される。

【００１９】

プラグインの場合には、署名の文字列は、プラグインを実行する特別の拡張子を有するファイルに配置される。複数のサーバが同じプラグインを使用し得るため、プラグインは、特定のサーバの公開鍵を内蔵しない。従って、前述の署名の文字列に加えて、そのファイルはまたサーバの証明書を有する。ファイルがモバイル通信装置１２$_1$に配信され、プラグインが起動されると、プラグインはファイルのサーバの証明書を検査し、有効なサーバの公開鍵を取得し、前述のように署名の文字列を確認する。

【００２０】

無線ＬＡＮへのセキュアなアクセスを可能にする技術について、前述した。

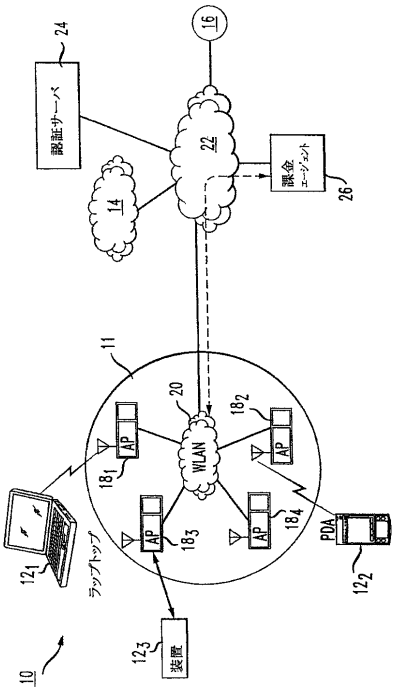
【図面の簡単な説明】

【００２１】

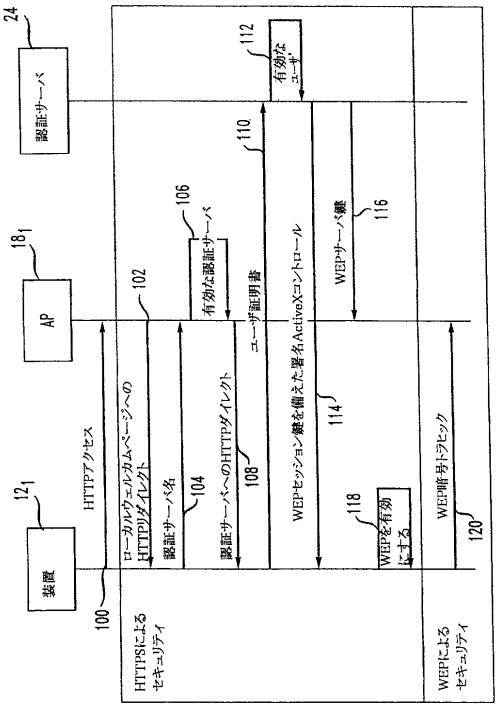
【図１】課金エージェントとビジネス関係を確立するために、本発明の方法を実装した無線ＬＡＮのブロック概略図

【図２】セキュアな無線ＬＡＮアクセスを可能にするために、時間と共に無線ＬＡＮとモバイル通信装置との間で生じた通信を示したラダー図

【図１】


認証サーバ
24
16
22
課金
エージェント
26
14
11
WLAN
20
AP
AP
AP
AP
18₁
18₂
18₃
18₄
ラップトップ
12₁
PDA
12₂
装置
12₃
10

【図２】


認証サーバ
24
AP
18₁
装置
12₁
100
HTTPアクセス
ローカルウェルカムページへの
HTTPリダイレクト
102
認証サーバ名
104
有効な認証サーバ
106
認証サーバへのHTTPダイレクト
108
ユーザ証明書
110
有効な
ユーザ
112
WEPセッション鍵を備えた署名ActiveXコントロール
114
WEPサーバ鍵
116
WEP鍵を有効
にする
118
WEP暗号トラヒック
120
HTTPSによる
セキュリティ
WEPによる
セキュリティ

フロントページの続き

(51)Int.Cl. F I
H04Q 7/00 570
H04Q 7/00 630

(74)代理人 100135105
弁理士 渡邊 直満
(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 マサール，サウラブ
アメリカ合衆国，ニュージャージー州 ０８５３６，プレインズボロ，クウェイル・リッジ・ドライヴ ４７０１
(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 福岡 裕貴

(56)参考文献 特開平１１－１６８４６０（ＪＰ，Ａ）
特開平１０－３２２３２５（ＪＰ，Ａ）
特開２００１－１１１５４４（ＪＰ，Ａ）
特開２００２－２８１０４５（ＪＰ，Ａ）
大水祐一，LifeStyle:無線LANに十分なセキュリティをもたらす「802.1x」，２００２年１０月１６日，ＵＲＬ，http://plusd.itmedia.co.jp/broadband/0210/16/musenlan.html
横田 英俊，IEEE802.1X認証との連携によるIPモビリティ提供手法に関する検討，情報処理学会研究報告:モバイルコンピューティングとワイヤレス通信，２００３年 3月 6日，Vol.2003，No.21，pp.53-58

(58)調査した分野(Int.Cl.，ＤＢ名)
H04W 4/00-99/00
H04L 12/28-12/46
H04L 9/00- 9/38