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

特許第5385941号
(P5385941)

(45)発行日　平成26年1月8日(2014.1.8)　(24)登録日　平成25年10月11日(2013.10.11)

(51)Int.Cl.　F I
G06F 21/44 (2013.01)　G06F 21/20　144C
H04W 12/06 (2009.01)　H04W 12/06

請求項の数 18　外国語出願　(全 16 頁)

(21)出願番号　特願2011-96013(P2011-96013)
(22)出願日　平成23年4月22日(2011.4.22)
(65)公開番号　特開2011-244439(P2011-244439A)
(43)公開日　平成23年12月1日(2011.12.1)
審査請求日　平成23年4月25日(2011.4.25)
(31)優先権主張番号　12/800,173
(32)優先日　平成22年5月10日(2010.5.10)
(33)優先権主張国　米国(US)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　メイレマンズ、マルク
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

最終頁に続く

(54)【発明の名称】無線ネットワークへのエンロールのためのオーディブルな認証

(57)【特許請求の範囲】
【請求項１】
無線ネットワークへの登録のための認証方法であって、
前記無線ネットワークへの登録を試みる未承認の無線デバイスを識別する秘密コードを音で出力する段階と、
前記無線デバイスを前記無線ネットワークに登録する段階と
を備え、
前記秘密コードを音で出力する段階は、前記無線デバイスが音声生成機能を内蔵されていない場合には、ＷＬＡＮを介して前記無線デバイスにリンクされたオーディオデバイスを用いて、前記秘密コードを音で出力する段階を含む認証方法。
【請求項２】
音で出力された前記秘密コードを受信した、という受領確認を、前記無線ネットワークを介して受信する段階をさらに備える請求項１に記載の認証方法。
【請求項３】
前記無線デバイスは、前記秘密コードをユーザに表示する視覚ディスプレイを有さない請求項１または２に記載の認証方法。
【請求項４】
前記無線デバイスのメモリに格納されている前記秘密コードのコンピュータ符号化されたバージョンを取得する段階をさらに備える請求項１から３の何れか一項に記載の認証方法。

【請求項５】
前記秘密コードのコンピュータ符号化されたバージョンを動的に生成する段階をさらに備える請求項１から４の何れか一項に記載の認証方法。
【請求項６】
前記秘密コードのコンピュータ符号化されたバージョンを取得する段階と、
前記秘密コードの前記コンピュータ符号化されたバージョンを、前記秘密コードの音で出力できるバージョンに変換する段階と
をさらに備える請求項１から５の何れか一項に記載の認証方法。
【請求項７】
前記秘密コードのコンピュータ符号化されたバージョンを取得する段階と、
言語を選択する段階と、
前記秘密コードの前記コンピュータ符号化されたバージョンを、選択された前記言語に対応する人間の言語における前記秘密コードの音で出力できるバージョンに変換する段階と
をさらに備える請求項１から６の何れか一項に記載の認証方法。
【請求項８】
前記秘密コードは、前記無線デバイスを一意に識別する請求項１から７の何れか一項に記載の認証方法。
【請求項９】
前記無線ネットワークへの登録についてのネットワーク証書を受信する段階をさらに備える請求項１から８の何れか一項に記載の認証方法。
【請求項１０】
前記秘密コードは、前記無線デバイスをグローバルに識別する請求項１から７の何れか一項に記載の認証方法。
【請求項１１】
前記秘密コードを音で出力する段階は、前記秘密コードを、人間の可聴範囲外の音で出力する請求項１から１０の何れか一項に記載の認証方法。
【請求項１２】
前記秘密コードを音で出力する段階は、前記秘密コードを、音楽で出力する請求項１から１０の何れか一項に記載の認証方法。
【請求項１３】
無線デバイスが無線ネットワークへの登録を試みるときに、前記無線デバイスを識別する個人識別番号（ＰＩＮ）のコンピュータ符号化されたバージョンを格納するメモリと、
音声を出力する１以上のスピーカと、
前記メモリに格納されている前記ＰＩＮの前記コンピュータ符号化されたバージョンを処理するＰＩＮマネージャと、
前記ＰＩＮの前記コンピュータ符号化されたバージョンを、前記ＰＩＮの音で出力できるバージョンに変換して、前記ＰＩＮの前記音で出力できるバージョンを、前記１以上のスピーカを介して音で出力させるオーディオマネージャと、
前記無線デバイスの前記無線ネットワークへの登録を処理するエンロールマネージャとを備え、
前記オーディオマネージャは、前記無線デバイスが音声生成機能を内蔵されていない場合には、ＷＬＡＮを介して前記無線デバイスにリンクされたオーディオデバイスを用いて、前記ＰＩＮを音で出力させる無線デバイス。
【請求項１４】
前記ＰＩＮマネージャは、さらに、前記ＰＩＮの前記コンピュータ符号化されたバージョンを生成する請求項１３に記載の無線デバイス。
【請求項１５】
前記無線デバイスは、前記ＰＩＮをユーザに表示する視覚ディスプレイを有さない請求項１３または１４に記載の無線デバイス。

【請求項１６】
前記ＰＩＮは前記無線デバイスを一意に識別する請求項１３から１５の何れか一項に記載の無線デバイス。
【請求項１７】
前記オーディオマネージャは、前記ＰＩＮを、人間の可聴範囲外の音で出力させる請求項１３から１６の何れか一項に記載の無線デバイス。
【請求項１８】
前記オーディオマネージャは、前記ＰＩＮを、音楽で出力させる請求項１３から１６の何れか一項に記載の無線デバイス。
【発明の詳細な説明】
【背景技術】
【０００１】
無線ローカルエリアネットワーク（ＷＬＡＮ）はユビキタスとなり、単なるパソコン以外のものによっても利用されるようになってきている。現在の消費者機器は、無線でＷＬＡＮに接続可能なものが増えてきている。より多くのデバイスおよびユーザが無線接続でき、利用可能となっている昨今では、無認可の侵入者がセキュリティを脅かす可能性も同様に高まってきている。しかしながら、セキュリティ上の方策を高めると、不慣れな無線ユーザが混乱することも多い。
【０００２】
幸い、ユーザフレンドリーなＷＬＡＮ相互運用可能なセキュリティ方策が既に幾つか利用可能である。例えば、Ｗｉ－Ｆｉアライアンスの証書規格（ＷＩ－ＦＩ　ＣＥＲＴＩＦＩＥＤ（登録商標））により証明されたデバイスが互いを相互利用することができる（つまりデバイスの製造業者に関らず）。さらに、Ｗｉ－Ｆｉアライアンスは、セキュアなＷＬＡＮのセットアップ法、および、証明された新たな無線デバイスをこれらＷＬＡＮにセキュアに且つユーザフレンドリーに追加する方法について説明しているＷｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ｓｅｔｕｐ（登録商標）（ＷＰＳ）プロトコルを導入している。これに関する詳細な情報に関しては、Ｗｉ－Ｆｉアライアンスのウェブサイトwww.wi-fi.orgの、「Ｗｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ｓｅｔｕｐ（登録商標）」を参照されたい。
【０００３】
従来の簡単でユーザフレンドリーなデバイスのセットアッププロシージャ（例えばＷＰＳ）を利用する場合、ユーザは、デバイス供給された個人情報番号（ＰＩＮ）を手動でユーザインタフェース（ＵＩ）から入力してネットワーク認証を行うことで、セキュアなＷＬＡＮに新たなデバイスを追加することができる。デバイス供給されたＰＩＮは、新たなデバイスと、既存のセキュアなＷＬＡＮとの間で共有された秘密として機能する。
【０００４】
しかし、デバイスの中には、ＰＩＮがデバイス自身に（例えばラベル上に）印刷されているものがある。このようなＰＩＮは、他の種類のデバイスが動的に生成するＰＩＮよりも安全性が低い。不変である鍵同様に、印刷されたＰＩＮのセキュリティは低い。さらに、従来のセキュアなネットワークエンロールプロシージャ（ＷＰＳ等）の目的の１つは、ユーザの簡便性を高めることである。しかし、この従来のプロシージャは、ユーザが重要なステップを手動で行うことを要求している。例えばＷＰＳを利用する場合、ユーザは、先ず新たなデバイスのＰＩＮ（通常８桁の長さを有する）を見つけて読み出し、さらにこの８桁のＰＩＮを、既存のセキュアなネットワークの公認ＵＩに手動で入力する必要がある。
【０００５】
詳細な記載は添付図面を参照して行われる。図面においては、参照番号が最初に現れる図面を、参照番号の左端の桁（１または複数）で表している。同じ番号の付された部材は図面全体にわたり同様の特徴およびコンポーネントである。
【図面の簡単な説明】
【０００６】

【図１】ここで記載する技術を実装可能なセキュアな無線ネットワークを有する例示的なネットワーク環境を示す。
【図２】ここで記載するネットワークへのエンロールのためのオーディブルな認証技術の例示的なプロセスを示すフロー図である。
【図３】ここで記載するネットワークへのエンロールのためのオーディブルな認証技術の例示的なプロセスを示すフロー図である。
【発明を実施するための形態】
【０００７】
ここには、セキュアな無線ネットワークへのエンロールのために無線デバイスのオーディブルな認証を利用する１以上の技術が記載されている。１以上の記載されている技術を利用することで、未承認の無線デバイスが、一意に識別する秘密コード（例えば個人識別番号またはＰＩＮ）をオーディブルに発信する。一部の実装例では、オーディブルコードは、ユーザにより可聴であり、ネットワークエンロールユーザインタフェースを介して手動で入力することができる。他の実装例では、ネットワーク承認デバイス（例えば無線アクセスポイント）が、自動的にこのオーディブルコードを得て、このコードを検証する。無線デバイスは、コードが検証された場合にセキュアな無線ネットワークにエンロールされる。
【０００８】
記載されている技術は、無線ローカルエリアネットワーク（ＷＬＡＮ）の、現在および将来のユーザフレンドリー且つ相互運用可能な、セキュアなネットワークエンロール法の一部として作動され、その利用可能性を高める。ここで記載されている１以上の実装例とともに利用されるのに適した既存の方法の一例に、Ｗｉ－Ｆｉアライアンスの Ｗｉ－Ｆｉ Ｐｒｏｔｅｃｔｅｄ Ｓｅｔｕｐ（登録商標）（ＷＰＳ）がある。
【０００９】
従来の方法（ＷＰＳ等）によると、ユーザは、新たな無線デバイスの既存のセキュアなＷＬＡＮへのエンロールを、デバイス供給されたＰＩＮを手動で入力することで確かめる。新たなデバイス（例えばデジタルビデオカメラ）が視覚ディスプレイを有する場合には、デバイスは、ユーザ向けに該ディスプレイ上に、動的に生成されたＰＩＮを示す。このようなディスプレイのないデバイスでは、従来の方法では、デバイスに貼付されたラベル上にＰＩＮが印刷されていた。印刷されているＰＩＮというものは、通常、デバイスの製造業者が予め生成して予め印刷しておくものである。動的に生成されるＰＩＮは、静的に生成されるＰＩＮよりセキュアであるが、従来の方法では、ディスプレイがないデバイスのユーザには、ＷＰＳが提供しているような、セキュアなネットワークエンロールプロセス中に動的に生成されるＰＩＮを示す手立てがない。さらには、従来の方法は、視覚の不自由なユーザがアクセスして利用することができない。
【００１０】
従来の方法では、ユーザは、デバイスの視覚ディスプレイ上の、またはラベル上のＰＩＮを見つけて読み出した後に、承認デバイス（例えば無線アクセスポイント）のユーザインタフェース（ＵＩ）または承認デバイスの代わりとして動作することを既にエンロール済みのデバイス（例えばパソコン）のＵＩを介してＰＩＮを入力する。ＷＬＡＮにエンロールすると、新たなデバイスはセキュアにＷＬＡＮと通信をすることができるようになる。デバイス供給されたＰＩＮは、新たなデバイスとセキュアなＷＬＡＮとの間で共有された秘密として機能して、ＰＩＮの手動入力がこの秘密を共有する動作である。
【００１１】
従来の方法と違って、ここで記載する技術の１以上の実装例では、ユーザフレンドリーで、相互運用可能で、セキュアなネットワークエンロール法を視覚の不自由なユーザに対して利用可能としたり、および／または、この方法の利用可能性を高めたりするために、動的に生成されたＰＩＮを表示するディスプレイがないデバイスであっても利用可能な方法を提供する。ここで記載する技術のうちの１以上を利用することで、ディスプレイがないデバイスであっても、動的に生成されたＰＩＮを、ネットワークエンロールプロセスの

一環としてオーディブルに発信することができる。例えば、デバイスはスピーカでＰＩＮを再生してよい。加えて、承認デバイス（例えばネットワークアクセスポイント）が、デバイスがオーディブルに発信したＰＩＮを捉えて解釈するマイクロフォンを備えていてもよい。解釈すると、承認デバイスは、オーディブルなＰＩＮを発信したデバイスの新たなエンロールプロセスを続けることができる。このようにすることで、ユーザは、デバイスのＰＩＮを見つけて読み出してから手動でそのピンをセキュアなＷＬＡＮへのエンロールを試みるデバイスに入力するという、容易に誤りがちな手入力作業を回避することができるようになる。

【００１２】

＜例示的な無線ネットワーク環境＞

図１は、例示的な無線ネットワーク環境１００を示す。この例示的なネットワーク環境１００は、インターネットその他のＷＬＡＮ等の他のネットワーク（有線、無線、セルラー式、衛星によるもの等を含む）に通信可能にリンクさせることのできる無線ローカルエリアネットワーク（ＷＬＡＮ）１０２を含む。ネットワーク環境１００はさらに、少なくとも１つの無線アクセスポイント（ＡＰ）および多くの他の無線ステーション（ＳＴＡ）１０６－１２２を含む。

【００１３】

ＡＰ１０４は、ＷＬＡＮ１０２の認証機器として機能して、ＡＰは、（不図示の）他の通信可能にリンクされたネットワークへのブリッジとして機能してよい。ＡＰ１０４は、専用ネットワークデバイスであってよいが、多目的デバイスあるいは汎用コンピューティングデバイスであってもよい。例えば、ＡＰ１０４はブリッジ、ルータ、リピータ、サーバ、クライアント、または、ＷＬＡＮ１０２用の無線承認デバイスとして機能しうる任意の他のネットワークデバイスであってよい。一部の実装例では、ＷＬＡＮ１０２のネットワーク認証機能は、ＡＰ１０４とその他のネットワークデバイスとの間で共有されてよい。また、ＡＰ１０４は、このネットワーク認証機能を他のネットワークデバイスに委任してもよい。

【００１４】

図示されているように、ステーションまたはＳＴＡ（例えば無線デバイス）は、ラップトップコンピュータ１０６、タブレット式コンピュータ１０８、ネットワークプリンタ１１０、ネットワークされたテレビ１１２、ＶｏＩＰ（ボイスオーバインターネットプロトコル）電話１１４、無線スピーカセット１１６、デジタルビデオカメラ１１８、携帯電話１２０、およびパソコン１２２（ユーザとともに示されている）を含む。もちろん、ＳＴＡ１０６ー１２２は、例示的な無線ネットワーク環境１００のコンテキストで利用可能な種類の無線デバイスを単に例示したものである。他の適切な無線デバイスには（例示であり限定ではない）、パーソナルデジタルアシスタント（ＰＤＡ）、デジタル音楽プレーヤ、デジタルスチルカメラ、オフィスプロジェクタ、デジタルフォトフレーム、スマートフォン、オーディオ機器、ナビゲーションシステム、計算機、ビデオ機器、電話、家庭用機器、ヒータおよび／またはクーラシステム、家庭用電化製品、医療機器、セキュリティシステム、放送チューニング機器、オンデマンドアクセス機器等が含まれてよい。

【００１５】

この例示的な無線ネットワーク環境１００においては、無線スピーカセット１１６は、現在、セキュアなＷＬＡＮ１０２の一部としてエンロールされていない。無線スピーカセット１１６は、ＷＬＡＮ１０２へのエンロールまたは参加を望んでいる。ネットワークへのエンロールを望む、無線スピーカセット１１６等のデバイスを、ここでは「エンロール側機器」と称することにする。

【００１６】

他の適切な無線デバイスおよびＡＰ１０４同様に、ＳＴＡ１０６ー１２２各々は、ＷＬＡＮ１０２等のＷＬＡＮの既存のまたは将来の、ユーザフレンドリーで、相互運用可能で、セキュアなネットワークエンロール方法で利用可能なように設計されている。例えばＳＴＡ１０６ー１２２は、Ｗｉ－Ｆｉアライアンスの Ｗｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ｓ

ｅｔｕｐ（登録商標）（ＷＰＳ）を利用して、デバイスをセキュアなＷＬＡＮにエンロールさせるよう設計されている。同様に、ＡＰ１０４は、ＷＰＳを利用して新たなＳＴＡをＷＬＡＮ１０２にエンロールさせるよう設計されている。図１には明示されていないが、ＳＴＡ１０６ー１２２の各々は、ここに記載されている技術の少なくとも一部を実行するよう構成された、ハードウェア、ファームウェア、ソフトウェア、またはこれらの組み合わせを含んでよい。

【００１７】

例示的なＷＬＡＮ１０２は、インフラストラクチャの無線ネットワークであってよいが、ＷＬＡＮの他の実装（例えば、いわゆる「アドホック」ネットワークまたはパーソナルエリアネットワーク（ＰＡＮ）等）も利用可能である。ＷＬＡＮ１０２は、既存または将来の無線ローカルエリアネットワーク規格のいずれかに準拠している。ＩＥＥＥ８０２．１１規格（ＩＥＥＥ８０２．１１ａ、８０２．１１ｂ、８０２．１１ｇ、および８０２．１１ｎ等）が、ここに記載されている技術の適切な無線ローカルエリアネットワーク規格の例である。一般的に、適切な無線ネットワークは、セキュアな無線ネットワークについての既存のまたは将来のユーザフレンドリー、相互運用可能、且つセキュアなネットワークエンロール方法とともに利用可能なように設計された、ネットワークされたデバイスを有する。

【００１８】

図１に示すように、ＡＰ１０４は、ここで記載する技術の少なくとも一部を実装するコンポーネントを有する。ＡＰ１０４は、１以上のプロセッサ１２４、メモリ１２６、およびマイクロフォン１２８を含む。メモリ１２６には、ユーザインタフェース（ＵＩ）マネージャ１３０、オーディオ入力マネージャ１３２、および承認機器１３４を含む１以上のコンポーネントが常駐している。

【００１９】

通常、マイクロフォン１２８は、ＡＰ１０４に統合され、その一部を形成している。または、マイクロフォン１２８が、ＡＰ１０４の外部にあっても、有線接続されていてもよい。またあるいは、マイクロフォン１２８は、ＡＰ１０４に無線接続されてもよく、ＷＬＡＮ１０２に既にエンロールされたデバイスであっても、その一部であってもよい。マイクロフォン１２８は、発信が予期されるデバイスの可聴範囲の周波数を検知することができるよう設計される。この周波数は、典型的な人間の可聴範囲内、それより上の範囲、および／またはそれより下の範囲を含んでもよい。

【００２０】

ＵＩマネージャ１３０は、新たなデバイスのエンロールプロセスを行うユーザに提示されるネットワークエンロール・ユーザインタフェース（ＵＩ）を管理する。ＡＰ１０４がユーザ入力を受け取ってＵＩを生成する機能を有する場合には、ＵＩをＡＰ１０４自身上に提示してよい。通常ＵＩは、別個の、既にエンロールされたネットワークデバイス（例えばパソコン１２２）を介して提示される。ＵＩマネージャ１２８は、ＵＩのユーザからの入力をパソコン１２２上で処理して、このコンピュータの出力の生成を助ける。

【００２１】

オーディオ入力マネージャ１３２は、マイクロフォン１２８からのアナログオーディオ入力を処理する。具体的にはオーディオ入力マネージャ１３２は、ネットワークエンロールを望むデバイスからオーディブルに発信されたＰＩＮに整合するオーディオ入力を受信して認識する。オーディオ入力マネージャ１３２は、アナログオーディオ入力ＰＩＮを、承認機器１３４が利用可能なコンピュータ符号化された形態に変換する。ここで、コンピュータ符号化されたＰＩＮは、ＰＩＮの値および意味を、コンピュータのコンポーネントがアクセス且つ利用できるような方法で格納および処理される。例えば、ＰＩＮ「１３４４２ＧＲ３ＵＴ９」のコンピュータ符号化された形態は、文字列であってよく、または、浮動小数点値として格納されてよい。

【００２２】

承認機器１３４は、オーディオ入力マネージャ１３２からコンピュータ符号化されたＰ

ＩＮを受信する。ＰＩＮは、エンロール側機器とＡＰ１０４（および／またはセキュアなＷＬＡＮ上の他の既存のデバイスの一部）との間で共有された秘密として機能する。承認機器１３４（例えばネットワークレジストラ）は、ＰＩＮの信憑性を確かめる。承認機器１３４は、暗号計算、テーブル検索、信頼のおける第三者に対する（例えばインターネット接続による）照会、またはその他の公知の検証プロセスを利用して検証を行うことができる。エンロール側機器は、ＰＩＮの検証に失敗すると、エンロールを拒否する。ＰＩＮの検証に成功すると、承認機器１３４は、オーディブルＰＩＮを発信したエンロール側機器のネットワークエンロールプロシージャを開始する。このネットワークエンロールプロシージャには、例えば、セキュアな無線ネットワークに対するＷＰＳその他のユーザフレンドリー、相互運用可能、且つ、セキュアなネットワークエンロール法に準拠したものが含まれてよい。

【００２３】

エンロール側機器の例としては、ディスプレイを有さないデバイスである、無線スピーカセット１１６が挙げられる。もちろん無線スピーカセット１１６は、あくまで、（特に情報が電気信号で供給された場合に）ユーザに対して視覚的に情報を提示する電子出力メカニズムを有さないデバイスの種類の一例にすぎない。ここでは、このようなデバイスを「ディスプレイのない機器」と称することにする。ディスプレイのない機器が含まない視覚ディスプレイの例には、（例示であって限定ではないが）、エレクトロルミネセントディスプレイ（ＥＬＤ）、発光ダイオード（ＬＥＤ）ディスプレイ、陰極線管（ＣＲＴ）ディスプレイ、液晶ディスプレイ（ＬＣＤ）、プラズマディスプレイパネル（ＰＤＰ）、有機発光ダイオード（ＯＬＥＤ）ディスプレイ、デジタル光処理（ＤＬＰ）ディスプレイ、電子ペーパ、非ビデオディスプレイ（例えば電気機械ディスプレイ等）が含まれる。

【００２４】

図１に示すように、無線スピーカセット１１６は、ここに記載する技術の少なくとも一部を実装するコンポーネントを有する。無線スピーカセット１１６は、１以上のプロセッサ１３６およびメモリ１３８を含む。メモリ１３８には、ＰＩＮマネージャ１４０、オーディオマネージャ１４２、エンロールマネージャ１４４を含む１以上のコンポーネントが常駐している。図示されているように、無線スピーカセット１１６は、ワードバブルに示されている個人識別番号（ＰＩＮ）１４６をオーディブルに発信する。

【００２５】

無線スピーカセット１１６のコンポーネントおよびＡＰ１０４のコンポーネントは、コンピュータ実行可能命令のモジュールであってよく、この命令は、コンピュータ、コンピューティングデバイス、またはこれらデバイスのプロセッサ上で実行可能な命令であってよい。ここではモジュールとして示されているが、コンポーネントは、ハードウェア、ファームウェア、ソフトウェア、または任意のこれらの組み合わせとして具現化されてよい。ここに記載する技術の全体または一部は、ハードウェア、ソフトウェア、ファームウェアまたは任意のこれらの組み合わせで実行されてよい。

【００２６】

ＰＩＮマネージャ１４０は、ネットワーク承認機器に理解および承認され、エンロール側機器を識別して、セキュアなＷＬＡＮ１０２へエンロールする、固有のネットワークエンロールＰＩＮ（例えばネットワークエンロール秘密コード）を処理する。ＰＩＮマネージャ１４０はさらに、ＰＩＮをオーディオマネージャ１４２に提供して、無線スピーカセット１１６がＰＩＮをオーディブルにアナウンスすることができるようにする。ＰＩＮマネージャ１４０は、製造業者が供給する公式に基づいてＰＩＮを動的に生成することができる。あるいは、ＰＩＮマネージャ１４０は、単に、メモリ１３８から静的なＰＩＮにアクセスしてもよい。

【００２７】

固有のネットワークエンロールＰＩＮは、エンロール側機器（例えば無線スピーカセット１１６）に対して、ＷＬＡＮ１０２が利用する相互運用可能でセキュアなネットワークエンロール法（例えばＷＰＳ）の一環として関連付けられる。ネットワークエンロールＰ

ＩＮは、エンロール側機器が参加を試みる特定のネットワーク（例えばＷＬＡＮ１０２）に固有なものであってよい。加えて、ネットワークエンロールＰＩＮは、グローバルに固有なコードであってよい（つまり、他のいずれの無線デバイスもこのコードを有さない、ということ）。ネットワークエンロールＰＩＮは通常、複数桁の番号（例えば４－８桁）である。または、ネットワークエンロールＰＩＮがアルファベットの文字列であってもよい。または、ネットワークエンロールＰＩＮは、特定の音、トーン、または音楽と関連付けられたシンボルその他のコードを含んでもよい。

【００２８】

オーディオマネージャ１４２は、ＰＩＮマネージャ１４０からコンピュータ符号化されたＰＩＮを受信する。オーディオマネージャ１４２は、ＰＩＮをコンピュータ符号化されたフォーマットから、無線スピーカセット１１６のスピーカを駆動する電気信号へと変換する。この結果、無線スピーカセット１１６は、ワードバブルに示す「ＰＩＮ」１４６が示す音声をオーディブルに発信する。

【００２９】

オーディブルＰＩＮ１４６は、任意の再生可能な音声、トーン、音楽等であってよい。オーディブルＰＩＮ１４６の例としては（例示であって限定ではないが）、話された言葉、文字、および／または数字（ユーザが選択する言語においてであってよい）、トーン、クリック、ビープ音、音符、および音楽が含まれる。オーディブルＰＩＮ１４６は、オーディオマネージャ１４２がコンピュータで生成してもよい。あるいは、オーディブルＰＩＮは、メモリ１３８または格納システムから取得された、後に再生されてよい１以上の格納ファイル（デジタルオーディオファイル等）であってもよい。オーディブルＰＩＮ１４６は、典型的な人間の可聴範囲内および／または可聴範囲外であってよい。オーディブルＰＩＮ１４６のオーディブルな性質は、ＡＰ１０４がオーディブルＰＩＮ１４６を、マイクロフォン１２８を利用して捉らえる機能、および、ＡＰのオーディオ入力マネージャ１３２が、無線スピーカセット１１６のＰＩＮマネージャ１４０が提供する元の固有のネットワークエンロールＰＩＮに対応するものを発見する機能に制限を受ける。

【００３０】

図１に示すエンロール側機器の例（例えば無線スピーカセット１１６）は、生来、ＰＩＮをオーディブルに発信するスピーカを有する。しかし他の種類のエンロール側機器も他の実装例では利用可能である。他の実装例においては、エンロール側機器は、製造業者によりオーディオ機能が内蔵されていてよい。例えば、無線デバイス製造業者は、一体型スピーカを別個に埋め込んでもよく、ヘッドフォンジャックを含んでもよく、短距離ネットワークスキーム（ＢＬＵＥＴＯＯＴＨ（登録商標）等）を提供して別のオーディオデバイス（例えば携帯電話またはイヤホン）へリンクさせてもよく、または、エンロール側機器を、ＷＬＡＮ１０２を介してネットワークされたスピーカを有するデバイスへリンクさせる選択肢を提供してもよい。

【００３１】

エンロールマネージャ１４４は、承認機器１３４が、オーディブルＰＩＮ１４６から導出したネットワークエンロールＰＩＮの信憑性を確かめると、ＡＰ１０４のネットワークエンロールプロシージャを処理する。エンロールマネージャ１４４は、ネットワーク証書のプロビジョンを管理して、無線スピーカセット１１６をセキュアなＷＬＡＮ１０２の一部とする。概して、エンロールマネージャ１４４は、セキュアな無線ネットワークについての、ＷＰＳまたは他のユーザフレンドリー、相互運用可能、且つ、セキュアなネットワークエンロール法に従って、ネットワークエンロールプロシージャを実行する。

【００３２】

＜例示的なプロシージャ＞

図２および図３は、ここで記載する無線ネットワークへのエンロールのためのオーディブルな認証技術の例示的なプロセス２００および３００を示すフロー図である。これらプロセス各々は、ハードウェア、ソフトウェア、またはこれらの組み合わせで実装可能な一連の処理として表される論理フローグラフのブロック図の集合として示されている。これ

らのブロックは、ソフトウェアのコンテキストにおいては、このようなコンピュータの１以上のプロセッサにより実行されると記載される処理を実行するコンピュータ命令を表している。プロセスを記載する順序は、限定として解釈されるべきではなく、任意の数の記載処理ブロックを任意の順序で組み合わせて、このプロセスまたは他のプロセスを実装することができる。加えて、個々のブロックは、ここに記載する主題の精神および範囲から逸脱することなく、プロセスから削除することもできる。

【００３３】

図２は、ネットワークのエンロール側機器（例えば図１の無線スピーカセット１１６）が、ネットワーク認証機器（例えばＡＰ１０４）との間で秘密コードを共有して、セキュアな無線ネットワーク（例えばＷＬＡＮ１０２）にエンロールするプロセス２００を示す。例示的なプロセス２００は、エンロール側機器が情報を受信して、セキュアな無線ネットワークにネットワークエンロールする共通の相互運用規格／方法に参加するネットワーク認証機器に対してエンロール側機器を識別する固有の秘密コードを生成する処理２０２を開始する。秘密コードは、セキュアな無線ネットワークにおいて固有であるので、ネットワークの認証機器に対してエンロール側機器を一意に識別することができる。さらに、秘密コードはグローバルに一意であり、識別可能であってもよい。これは、他のいずれのエンロール側機器もが、同じ秘密コードを所有しない、ということを意味している。固有の秘密コードは、個人識別情報（ＰＩＮ）とも称される。

【００３４】

ユーザがエンロール側機器を起動すると、エンロール側機器は、無線ネットワークを検索する。エンロール側機器が、エンロールを希望するネットワークを発見すると、エンロール側機器はこのネットワークへの参加を試みてよい。エンロールされていないネットワークは、エンロール側機器に対してＰＩＮの提供を要求してよい。または、ユーザがエンロール側機器においてボタンを押す等の処理行い、エンロール側機器にＰＩＮを提供させてもよい。

【００３５】

処理２０４においては、エンロール側機器は、セキュアなネットワーク上で、またはグローバルに、エンロール側機器を一意に識別するＰＩＮのコンピュータ符号化されたバージョンを取得する。ここでは、エンロール側機器は、製造業者が供給する公式または一意に識別する秘密鍵を作成する他の公知の方法に基づいてＰＩＮを動的に生成することができる。または、エンロール側機器が、単にメモリ（メモリ１３８）または格納サブシステム（例えばディスクまたはフラッシュドライブ）から静的ＰＩＮにアクセスしてもよい。

【００３６】

処理２０６で、エンロール側機器は、取得したコンピュータ符号化されたＰＩＮを、ＰＩＮのオーディブルなバージョンを生成することのできる電気信号に変換する。例えば電気信号は、無線スピーカセット１１６のスピーカを駆動してよい。変換は、取得したＰＩＮの桁を特定の音声にマッピングすることであってもよい。変換により生じる音声は、コンピュータ格納されている数または文字を、特定の言語で対応する音声に単にマッピングすることで得られてもよい。これを実行する際に、エンロール側機器は、各桁に対して適切な音声を動的に生成してもよい。またはエンロール側機器が、桁と格納されている音声との間の所定の関連付けに基づいて、メモリまたはストレージに格納されている音声にアクセスしてもよい。例えば「１２３」のＰＩＮを例にとると、エンロール側機器は、各桁「１」「２」および「３」に対応する３つの音声ファイルにアクセスすることができる。またはＰＩＮが、人間が理解できる単語を含んでよく、場合によっては文を含んでもよい。

【００３７】

さらに、エンロール側機器は、各セットが特定の言語の音声を有するような複数の音声セットを有してよい。ユーザは、エンロール側デバイスから一定の選択肢を選択することにより（例えばボタンの押下および／またはスイッチを押すことにより）、特定の言語（例えばフランス語）を選択することができる。製造業者は、エンロール側機器が販売され

る場所に応じてデフォルトの言語を設定しておくこともできる。変換から生じうる音声は、人が理解可能な数、文字、または単語でもなく、典型的な人間の言語の一部を構成しなくてもよい。例えば、ＰＩＮの桁は、トーン、クリック、ビープ音、音符、音楽、ブラスト、動物の鳴き声、サウンドエフェクト、またはその他の典型的な人間の言語の一部ではないサウンドにマッピングすることもできる。

【００３８】

または、ＰＩＮのコンピュータ符号化可能なバージョン（例えば「134RG34FF2W99」）をＰＩＮのオーディブルなバージョンに変換する代わりに、エンロール側機器は、メモリから、ＰＩＮまたはその部分の予め生成されたオーディオバージョンを取得することもできる。例えばエンロール側機器は、メモリに、再生されると、女性が「赤色、緑色、青色、８、９、３１、アルファ、タンゴ、９１、オレンジ」と言う音声を発生するデジタルオーディオファイルを格納していてもよい。このレコーディングの音声は、この音声を聴いてネットワークエンロールＵＩを利用してユーザからこの入力を受信するネットワーク認証機器への適切なネットワークエンロールＰＩＮに対応していてよい。

【００３９】

処理２０８で、エンロール側機器は、ＰＩＮを、無線スピーカセット１１６のもの同様のスピーカを介してオーディブルに発信する。これは、図１のワードバブルに示す「ＰＩＮ」１４６に示されている。エンロール側機器が、音声生成機能を内蔵されていない場合には、エンロール側機器は、スピーカを有するデバイスへ、オーディブルＰＩＮをパッケージして送信するステップを直後に行うこともできる。これは、別のオーディオデバイス（例えば携帯電話またはイヤホン）へのリンクを可能とする短距離ネットワークスキームを介して行うこともでき、あるいは、エンロール側機器を、スピーカを有するネットワークされた機器に、一部のセキュアではないネットワークを介してリンクさせることにより行うこともできる。

【００４０】

処理２１０で、エンロール側機器は、ネットワーク認証機器（例えばＡＰ１０４）がオーディブルＰＩＮを受信および／または検証したことの確認を待つ。ネットワーク認証機器は、オーディオＰＩＮを捉らえるマイクロフォンを介してＰＩＮを取得することができる。または、認証機器は、オーディブルＰＩＮを聴いたユーザが、聴いたＰＩＮを手動で入力することにより、ＰＩＮを取得することもできる。一部の実装例では、受信および／または検証したことの確認は、明示的に行われない場合がある。この場合には、ネットワークエンロールプロセスが開始された、ということが、ＰＩＮが受信され検証されたことの間接的な確認として機能する。

【００４１】

処理２１２で、エンロール側機器は、セキュアな無線ネットワークに参加する。この処理には、エンロール側機器が、ネットワーク認証機器からネットワーク証書を受け取ることが含まれてよい。エンロールプロセスが完了すると、エンロール側機器は、セキュアな無線ネットワークに構築された無線デバイスとなる。

【００４２】

図３は、ネットワークエンロール側機器（例えば図１の無線スピーカセット１１６）から秘密コードを取得して、エンロール側機器をセキュアな無線ネットワーク（例えばＷＬＡＮ１０２）に登録させる、ネットワーク認証機器（例えばＡＰ１０４）の例示的なプロセス３００を示す。例示的なプロセス３００は、認証機器が、セキュアな無線ネットワークへのネットワークエンロールのために通常の相互運用可能な規格／方法で参加するエンロール側機器を認証機器に対して識別する固有の秘密コードを受信する処理３０２から始まる。固有の秘密コードは、個人識別番号（ＰＩＮ）とも称される。

【００４３】

ユーザが認証機器を立ち上げ、または、検索の選択肢を選択すると、認証機器はエンロール側機器を探してよい。認証機器がエンロール側機器を見つけると、認証機器は、セキュアなネットワークへの参加を試みるかどうかをエンロール側機器に対して尋ねる。実際

に具体的には、認証機器はエンロール側機器に、「ＰＩＮを提供せよ」と要求してよい。または認証機器が、エンロール側機器の、「ネットワークに参加したい」という要求または「エンロール側機器がＰＩＮをこれから送信する」という示唆に対して応答してもよい。あるいは、認証機器は、ネットワークを介した信号、または、ＰＩＮが来るということを示す何らかのオーディブルコードを受信してもよい。さらに一部の実装例では、認証機器は常にオーディブルＰＩＮを捉らえる準備が整っていてもよい。

【００４４】

処理３０４で、認証機器は、エンロール側機器が発信したオーディブルＰＩＮのアナログ電気信号をマイクロフォン（例えばマイクロフォン１２８）を介して取得する。これは、マイクロフォン１２８に近接している無線スピーカセット１１６から来る図１のワードバブルに示すＰＩＮ１４６に示されている。近接の度合いは、多くの音声要素（例えばオーディブルＰＩＮのボリューム、マイクロフォン１２８の感度、他の音源から生じうる干渉（ノイズ等））に基づいて定まる。通常は、認証機器（例えばＡＰ１０４）およびエンロール側機器（例えば無線スピーカセット１１６）は共に、ＰＩＮがオーディブルに発信されるときに同じ部屋に配置されていてよい。

【００４５】

処理３０６で、認証機器は、認証機器がエンロール側機器からオーディブルＰＩＮを受信した旨を示す受領確認をエンロール側機器に送信する。一部の実装例では、認証機器は、明示的に受領確認を送信しない場合がある。この場合には、ネットワークエンロールプロセスが開始された、ということが、ＰＩＮが受信され検証されたことの間接的な受領確認として機能する。

【００４６】

処理３０８で、認証機器は、アナログ電気信号を、ＰＩＮのコンピュータ符号化されたバージョンに変換する。認証機器による変換は、例えばプロセス２００の処理２０６に関して上述した、エンロール側機器がオーディブルＰＩＮを生成するために利用するものと逆のマッピングにより行うこともできる。オーディブルＰＩＮの音声は、ＰＩＮのコンピュータ符号化されたバージョンにマッピングされる。

【００４７】

または、オーディブルＰＩＮを受信および変換する代わりに、認証機器は、ＰＩＮのコンピュータ符号化されたバージョンを、人間を介在させて受け取ることもできる。この場合には、ユーザが、エンロール側機器が発信したオーディブルＰＩＮを聴いて、ＰＩＮを手動で認証機器のＵＩに入力する。ＵＩは、認証機器自身の一部であっても、ネットワーク上の別のデバイスにより提供されるものであってもよい。

【００４８】

処理３１０で、認証機器は、デジタルネットワークエンロールＰＩＮの信憑性を確かめる。認証機器はこれを、暗号計算、テーブル検索、信頼のおける第三者に対する（例えばインターネット接続による）照会、またはその他の公知の検証プロセスを利用して行うことができる。処理３０８の受領確認の代わりに、またはこれに加えて、認証機器は、認証機器がエンロール側機器から受け取ったオーディブルＰＩＮの信憑性を検証した、ということの確認をエンロール側機器に送信してもよい。一部の実装例では、認証機器は、明示的に受領確認を送信しない場合がある。この場合には、ネットワークエンロールプロセスが開始された、ということが、ＰＩＮが受信され検証されたことの間接的な受領確認として機能する。

【００４９】

ＰＩＮの検証に成功すると、認証機器は、処理３１２で、オーディブルＰＩＮを発信したエンロール側機器とのネットワークエンロールプロシージャを開始する。この処理には、認証機器がネットワークを介してエンロール側機器にネットワーク証書を送信することが含まれてよい。エンロールプロセスが完了すると、エンロール側機器は、セキュアな無線ネットワークに構築された無線デバイスとなる。ＰＩＮの検証が失敗すると、認証機器は、エンロール側機器のセキュアな無線ネットワークへの参加を拒否する。認証機器は、

拒否するという旨の示唆をネットワークを介してエンロール側機器に送信してもよい。

【００５０】

＜まとめ＞

本願で利用される用語「コンポーネント」「モジュール」「システム」「インタフェース」等は、概してコンピュータ関連の実体（ハードウェア、ソフトウェアとハードウェアの組み合わせ、ソフトウェア、実行中のソフトウェア等）を示すことを意図している。例えば、コンポーネントは、プロセッサ上で実行されているプロセス、プロセッサ、オブジェクト、実行ファイル、実行スレッド、プログラム、および／または、コンピュータを含んでよいが、これらに限定はされない。あくまで例示であるが、コントローラ上で実行されているアプリケーションおよびコントローラの両方が、コンポーネントであってよい。１以上のコンポーネントは、プロセスおよび／または実行スレッド内に常駐していてよく、コンポーネントは、１つのコンピュータにローカライズされていても、および／または、２以上のコンピュータ間に分配されてもよい。

【００５１】

さらに、請求されている主題は、開示される主題を実装するべくコンピュータを制御するために、ソフトウェア、ファームウェア、ハードウェア、またはこれらの任意の組み合わせを生成する標準的なプログラミングおよび／または工学上の技術を利用する方法、装置、または製品として実装可能である。ここで利用する「製品」という用語は、任意のコンピュータ可読デバイス、搬送波、または媒体からアクセス可能なコンピュータプログラムを含むことを意図する。例えばコンピュータ可読媒体には、これらに限定はされないが、磁気格納デバイス（例えばハードディスク、フロッピー（登録商標）ディスク、磁気ストリップ等）、光ディスク（例えばコンパクトディスク（ＣＤ）、ＤＶＤ等）、スマートカード、およびフラッシュメモリデバイス（例えばカード、スティック、キードライブ等）が含まれてよい。もちろん当業者であれば、この構成に対して請求されている主題の範囲または精神を逸脱することなく数多くの変形例を想到するであろう。

【００５２】

本願で利用されている用語「または／あるいは」は、排他的な選言ではなくて両立的な選言の意味を意図している。つまり、そうではないと明示されている場合を除き、また、コンテキストからそうではないことが明らかである場合を除き、「ＸはＡまたはＢを利用する」といった表現は、自然な両立的な置き換えを意味する。つまり、「ＸがＡまたはＢを利用する」は、ＸがＡを利用する、ＸがＢを利用する、またはＸがＡおよびＢの両方を利用する、という意味である。加えて、本願および添付請求項における不定冠詞の利用は、単一であることが明示されている場合を除き、また、コンテキストから単一であることが明らかである場合を除き、概して「１以上」と解釈されるべきである。

【００５３】

主題を、構造的な特徴および／または方法上のアクションに特定の言語により記載してきたが、添付請求項に定義されている主題は、必ずしも記載された特定の特徴またはアクションに限定はされないことを理解されたい。特定の特徴およびアクションは、請求項を実装するときの例示的な形態として開示されている。

［項目１］

無線ネットワークへのエンロールのためのオーディブルな認証方法であって、

前記無線ネットワークへのエンロールを試みる未承認の無線デバイスを識別する秘密コードをオーディブルに発信する段階と、

前記無線デバイスを前記無線ネットワークにエンロールする段階とを備える認証方法。

［項目２］

オーディブルに発信された前記秘密コードを受信した、という受領確認を、前記無線ネットワークを介して受信する段階をさらに備える項目１に記載の認証方法。

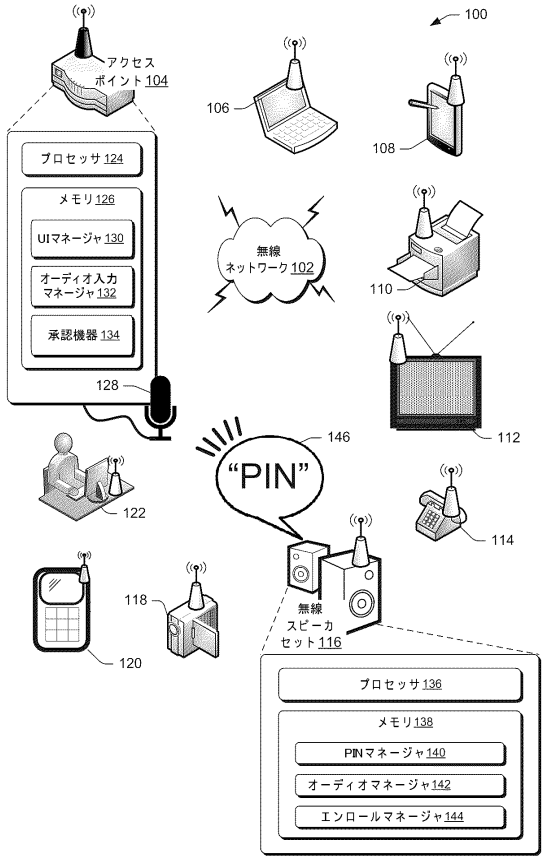
［項目３］

前記未承認の無線デバイスは、前記秘密コードをユーザに表示する視覚ディスプレイを有さない項目１に記載の認証方法。

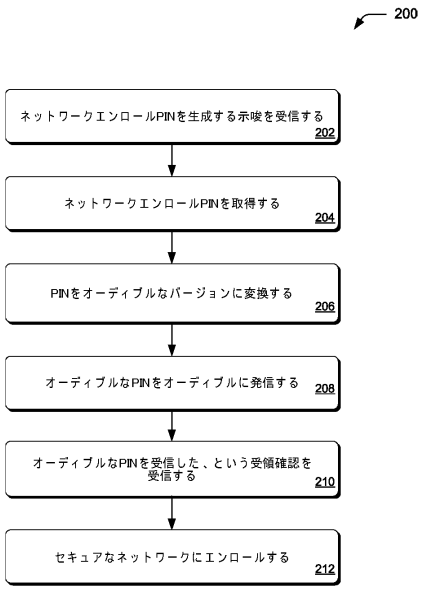
［項目４］
前記未承認の無線デバイスのメモリに格納されている前記秘密コードのコンピュータ符号化されたバージョンを取得する段階をさらに備える項目１に記載の認証方法。
［項目５］
前記秘密コードのコンピュータ符号化されたバージョンを動的に生成する段階をさらに備える項目１に記載の認証方法。
［項目６］
前記秘密コードのコンピュータ符号化されたバージョンを取得する段階と、
前記秘密コードの前記コンピュータ符号化されたバージョンを、前記秘密コードのオーディブルなバージョンに変換する段階とをさらに備える項目１に記載の認証方法。
［項目７］
前記秘密コードのコンピュータ符号化されたバージョンを取得する段階と、
言語を選択する段階と、
前記秘密コードの前記コンピュータ符号化されたバージョンを、選択された前記言語に対応する人間の言語における前記秘密コードのオーディブルなバージョンに変換する段階とをさらに備える項目１に記載の認証方法。
［項目８］
前記無線ネットワークへのエンロールを要求する段階と、
前記要求に呼応して、エンロールの拒否を受信する段階と、
前記エンロールの拒否の前記受信に呼応して、前記秘密コードを取得する段階、および、前記発信する段階と前記エンロールする段階とを実行する段階とをさらに備える項目１に記載の認証方法。
［項目９］
前記秘密コードは、前記未承認の無線デバイスを一意に識別する項目１に記載の認証方法。
［項目１０］
前記無線ネットワークへのエンロールについてのネットワーク証書を受信する段階をさらに備える項目１に記載の認証方法。
［項目１１］
前記秘密コードは、前記無線デバイスをグローバルに識別する項目１に記載の認証方法。
［項目１２］
無線ネットワークへのエンロールのためのオーディブルな認証方法であって、
前記無線ネットワークへのエンロールを試みる未承認の無線デバイスを識別する個人識別番号（ＰＩＮ）のオーディブルなバージョンを取得する段階と、
前記ＰＩＮの前記オーディブルなバージョンを、前記ＰＩＮのコンピュータ符号化されたバージョンに変換する段階と、
前記ＰＩＮの信憑性を検証する段階と、
前記ＰＩＮの信憑性が検証されると、前記無線デバイスを前記無線ネットワークにエンロールする段階とを備える認証方法。
［項目１３］
前記取得する段階の前に、前記ＰＩＮの前記オーディブルなバージョンが来ることを示す示唆を受信する段階をさらに備える項目１２に記載の認証方法。
［項目１４］
前記取得する段階の後に、前記ＰＩＮの前記オーディブルなバージョンを受信した、という受領確認を送信する段階をさらに備える項目１２に記載の認証方法。
［項目１５］
前記検証する段階の後に、前記ＰＩＮの前記オーディブルなバージョンを検証した、という確認を送信する段階をさらに備える項目１２に記載の認証方法。
［項目１６］

前記取得する段階は、
前記未承認の無線デバイスがオーディブルに発信した音声を捉らえて、前記音声を、前記ＰＩＮの前記オーディブルなバージョンとして格納する段階を有する項目１２に記載の認証方法。
［項目１７］
無線デバイスが無線ネットワークへのエンロールを試みるときに、前記無線デバイスを識別する個人識別番号（ＰＩＮ）のコンピュータ符号化されたバージョンを格納するメモリと、
音声をオーディブルに発信する１以上のスピーカと、
前記メモリに格納されている前記ＰＩＮの前記コンピュータ符号化されたバージョンを処理するＰＩＮマネージャと、
前記ＰＩＮの前記コンピュータ符号化されたバージョンを、前記ＰＩＮのオーディブルなバージョンに変換して、前記ＰＩＮの前記オーディブルなバージョンを、前記１以上のスピーカを介してオーディブルに発信させるオーディオマネージャと、
前記無線デバイスの前記無線ネットワークへのエンロールを処理するエンロールマネージャとを備える無線デバイス。
［項目１８］
前記ＰＩＮマネージャは、さらに、前記ＰＩＮの前記コンピュータ符号化されたバージョンを生成する項目１７に記載の無線デバイス。
［項目１９］
前記無線デバイスは、前記ＰＩＮをユーザに表示する視覚ディスプレイを有さない項目１７に記載の無線デバイス。
［項目２０］
前記ＰＩＮは前記無線デバイスを一意に識別する項目１７に記載の無線デバイス。

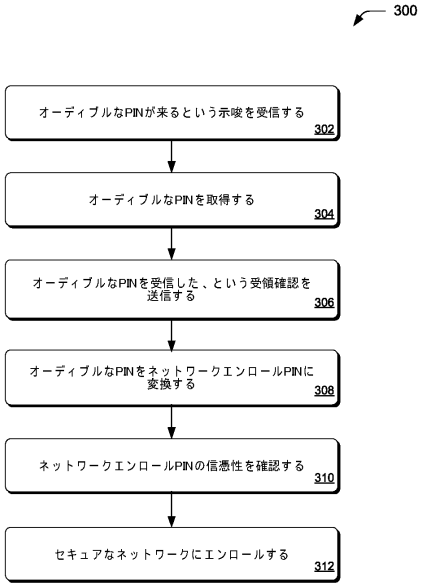
【図１】



【図２】



【図３】


300
オーディブルなPINが来るという示唆を受信する
302
オーディブルなPINを取得する
304
オーディブルなPINを受信した、という受領確認を送信する
306
オーディブルなPINをネットワークエンロールPINに変換する
308
ネットワークエンロールPINの信憑性を確認する
310
セキュアなネットワークにエンロールする
312

フロントページの続き

(72)発明者　マルツ、ジュニア、ゲアリー　エー.
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

審査官　中里　裕正

(56)参考文献　特表２０１０－５００８１７（ＪＰ，Ａ）
特開２００５－１７４３２７（ＪＰ，Ａ）
米国特許出願公開第２００８／０１１３６１９（ＵＳ，Ａ１）
米国特許出願公開第２０１０／０１１０８３７（ＵＳ，Ａ１）
特開２００９－１８７３８６（ＪＰ，Ａ）
特開２００４－３０４２４０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４
Ｈ０４Ｗ　１２／０６