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

特許第5114420号
(P5114420)

(45)発行日　平成25年1月9日(2013.1.9)　(24)登録日　平成24年10月19日(2012.10.19)

(51)Int.Cl.		F I		
H04W 12/04	(2009.01)	H04Q	7/00	182
H04W 8/22	(2009.01)	H04Q	7/00	152
H04W 12/06	(2009.01)	H04Q	7/00	183

請求項の数 17　(全 13 頁)

(21)出願番号	特願2008-538129 (P2008-538129)
(86)(22)出願日	平成18年12月19日 (2006.12.19)
(65)公表番号	特表2009-513089 (P2009-513089A)
(43)公表日	平成21年3月26日 (2009.3.26)
(86)国際出願番号	PCT/US2006/048418
(87)国際公開番号	WO2007/078940
(87)国際公開日	平成19年7月12日 (2007.7.12)
審査請求日	平成20年4月23日 (2008.4.23)
(31)優先権主張番号	11/323,315
(32)優先日	平成17年12月30日 (2005.12.30)
(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　100104156
弁理士　龍華　明裕
(72)発明者　ミラー、グレゴリー、エル.
アメリカ合衆国、９７２２９　オレゴン州、ポートランド、エヌダブリュー　ヨンカラ　コート　２０５０５

審査官　山中　実

最終頁に続く

(54)【発明の名称】ネットワーク環境との通信を確立する方法、記憶媒体、及び、システム

(57)【特許請求の範囲】

【請求項１】

無線端末装置である第１の機械が、設定鍵を予め有し、または、前記設定鍵を生成することと、

前記第１の機械が、前記設定鍵を表示することと、

前記第１の機械が、前記設定鍵に基づいて第１の暗号鍵を生成することと、

アクセスポイントである第２の機械が、前記設定鍵を入力するためのインターフェースを有し、前記インターフェースを介して入力された前記設定鍵に基づいて、第1の暗号鍵を生成することと、

前記第１の機械及び第２の機械が、前記第１の暗号鍵に基づいて、前記第１の機械と前記第２の機械とを接続する一時的チャネルを確立することと、

前記第２の機械が、前記第１の暗号鍵より安全性の高い第２の暗号鍵を生成して保存することと、

前記第２の機械が、前記第２の暗号鍵を前記一時的チャネルを通じて前記第１の機械に送信し、前記第１の機械が前記第２の暗号鍵を保存することと、

前記第１の機械及び前記第２の機械が、前記第２の暗号鍵に基づいて前記第１の機械と前記第２の機械とを接続する、前記一時的チャネルよりも安全性が高い永久チャネルを確立することと、

を備える方法。

【請求項２】

前記第１の暗号鍵は、第１の部分と、前記第１の部分のチェックサムである第２の部分とを含む、請求項１に記載の方法。
【請求項３】
前記第２の機械が、前記設定鍵からアクセスポイント識別子を生成することと、
前記第２の機械が、前記第２の暗号鍵と共に、前記アクセスポイント識別子を前記第１の機械に送信することと
を更に含む、請求項１または２に記載の方法。
【請求項４】
前記第１の機械の電源投入、及び、前記第１の機械のリセットのうちの選択された１つに応じて、前記第１の機械は前記設定鍵を有し、または前記設定鍵を生成する、請求項１から３のいずれか一項に記載の方法。
【請求項５】
前記第１の機械は、前記設定鍵をランダムに生成する
請求項１から４のいずれか一項に記載の方法。
【請求項６】
コンピュータを、無線端末装置である第１の機械とアクセスポイントである第２の機械とを接続する永久チャネルを確立する前記第１の機械として機能させるためのプログラムを記憶した記憶媒体であって、
前記第２の機械は、設定鍵を入力するためのインターフェースを有し、前記インターフェースを介して入力された前記設定鍵に基づいて第１の暗号鍵を生成し、前記第１の機械と前記第２の機械が、前記第１の暗号鍵に基づいて、前記第１の機械と前記第２の機械とを接続する一時的チャネルを確立し、前記第２の機械が前記第１の暗号鍵より安全性の高い第２の暗号鍵を生成して保存し、前記第２の機械が前記第２の暗号鍵を前記一時的チャネルを通じて前記第１の機械に送信するように構成され、
前記コンピュータを、
前記設定鍵を有し、または前記設定鍵を生成する手段と、
前記設定鍵を表示する手段と、
前記設定鍵に基づいて、第1の暗号鍵を生成する手段と、
前記第２の機械とともに前記第１の機械と前記第２の機械とを接続する前記一時的チャネルを確立する手段と、
前記第２の暗号鍵を前記一時的チャネルを通じて前記第２の機械から受信し、前記第２の暗号鍵を保存する手段と
して機能させるための前記プログラムを記憶した記憶媒体。
【請求項７】
前記プログラムは、前記コンピュータを、
不揮発性設定メモリ、及び、揮発性設定メモリのうちの選択された１つにおいて、前記第２の暗号鍵を格納する手段としてさらに機能させるためのプログラムである、請求項６に記載の記憶媒体。
【請求項８】
前記プログラムは、前記コンピュータに、
前記設定鍵をランダムに生成させる
請求項６または７に記載の記憶媒体。
【請求項９】
コンピュータを、無線端末装置である第１の機械とアクセスポイントである第２の機械とを接続する永久チャネルを確立する前記第２の機械として機能させるためのプログラムを記憶した記憶媒体であって、
前記第１の機械は、
設定鍵を有し、または前記設定鍵を生成する手段と、
前記設定鍵を表示する手段と、
前記設定鍵に基づいて、第1の暗号鍵を生成する手段と、

前記第２の機械とともに前記第１の機械と前記第２の機械とを接続する一時的チャネルを確立する手段と、
第２の暗号鍵を前記一時的チャネルを通じて前記第２の機械から受信し、前記第２の暗号鍵を保存する手段と
を有し、
前記コンピュータを、
前記第１の機械に表示された前記設定鍵をインターフェースを介して入力する手段と、
入力された前記設定鍵に基づいて第１の暗号鍵を生成する手段と、
前記第１の暗号鍵に基づいて、前記第１の機械とともに前記第１の機械と前記第２の機械とを接続する前記一時的チャネルを確立する手段と、
前記第１の暗号鍵より安全性の高い第２の暗号鍵を生成して保存する手段と、
前記一時的チャネルを通じて、前記第１の機械に前記第２の暗号鍵を送信する手段と、
前記第１の機械とともに、前記第１の機械と前記第２の機械とを接続する、前記一時的チャネルよりも安全性の高い永久チャネルを確立する手段と
して機能させるプログラムを記憶した記憶媒体。
【請求項１０】
前記第１の暗号鍵は、第１の部分と、前記第１の部分のチェックサムである第２の部分とを含む、請求項９に記載の記憶媒体。
【請求項１１】
前記プログラムは、前記コンピュータを、
前記設定鍵からアクセスポイント識別子を生成して格納する手段と、
前記一時的チャネルを確立するときに、前記アクセスポイント識別子を使用させる手段として更に機能させるためのプログラムである、請求項９または１０に記載の記憶媒体。
【請求項１２】
前記第１の機械は、前記設定鍵をランダムに生成する
請求項９から１１のいずれか一項に記載の記憶媒体。
【請求項１３】
無線端末装置である第１の機械およびアクセスポイントである第２の機械を備えるシステムであって、
前記第１の機械は、
設定鍵を有し、または前記設定鍵を生成する手段と、
前記設定鍵を表示する手段と、
前記設定鍵に基づいて第１の暗号鍵を生成する手段と、
前記第２の機械とともに前記第１の機械と前記第２の機械とを接続する一時的チャネルを確立する手段と、
前記一時的チャネルを通じて前記第２の機械から前記第１の暗号鍵より安全性の高い第２の暗号鍵を受信し、前記第２の暗号鍵を保存する手段と
を有し、
前記第２の機械は、
前記設定鍵を入力するインターフェースと、
前記インターフェースを通じて入力された前記設定鍵に基づいて第１の暗号鍵を生成する手段と、
前記第１の暗号鍵に基づいて、前記第１の機械とともに前記第１の機械と前記第２の機械とを接続する一時的チャネルを確立する手段と、
前記第１の暗号鍵よりも安全性の高い第２の暗号鍵を生成し保存する手段と、
前記一時的チャネルを通じて、前記第１の機械に前記第２の暗号鍵を送信する手段と、
前記第１の機械とともに、前記一時的チャネルよりも安全性が高く、前記第１の機械と前記第２の機械とを接続する永久チャネルを確立する手段と
を有するシステム。
【請求項１４】

前記第１の暗号鍵は、第１の部分と、前記第１の部分のチェックサムである第２の部分とを含む、請求項１３に記載のシステム。
【請求項１５】
前記第２の機械が、
前記設定鍵からアクセスポイント識別子を生成する手段と、
前記第２の暗号鍵と共に、前記アクセスポイント識別子を前記第１の機械に送信する手段と
をさらに含む、請求項１３または１４に記載のシステム。
【請求項１６】
前記第１の機械は、前記第１の機械の電源投入、及び、前記第１の機械のリセットのうちの選択された１つに応じて、前記設定鍵を有し、または生成する手段をさらに含む、請求項１３から１５のいずれか一項に記載のシステム。
【請求項１７】
前記第１の機械は、前記設定鍵をランダムに生成する
請求項１３から１６のいずれか一項に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的に、ネットワーク環境への導入時に装置を設定すること、より具体的には、ネットワーク環境への導入時にワイヤレス装置を自動的に設定することに関する。
【背景技術】
【０００２】
今日、ワイヤレスネットワークにワイヤレス装置といったようにネットワーク環境に装置を追加することを希望し、且つ、自分のネットワークを侵害者に公開したくない場合、ＷＥＰ（ワイヤード・エクイバレント・プライバシ、又は、時に、ワイヤード・エイクバレンシ・プロトコル）、ＷＰＡ（Ｗｉ－Ｆｉ保護アクセス）、ＥＡＰ（拡張認証プロトコル）、ＩＥＥＥ（電気電子学会）の８０２．１１ｉ等に基づいたセキュリティシステムといったセキュリティシステムの仕組みについて徹底的に調べることが必要となってくる。
【０００３】
しかし、ワイヤレス装置とその関連付けられるアクセスポイントの両方において適切なクレデンシャル（credential）を確立することは難しく、エラーが発生しやすい。また、一般的に、装置のネットワーク環境への導入時の所有権の証明及び／又は装置の制御は、手動で行われなければならない。つまり、例えば、（一部の消費者製品で行われているように）装置を最初に公開状態で動作するようにするといった場合、装置は、安全な状態にされる前に侵害に対して脆弱になり、装置を設置するユーザは、装置を正しくないネットワーク環境に誤って関連付けてしまう場合がある。
【図面の簡単な説明】
【０００４】
本発明の特徴及び利点は、本発明の以下の詳細な説明から明らかとなろう。
【０００５】
【図１】本願に開示する実施形態の原理に従って動作しうる複数の装置からなる例示的なシステムを示す図である。
【０００６】
【図２】図１のシステムに導入される装置を設定するための一実施形態による方法を示す図である。
【０００７】
【図３】アクセスポイントを含むネットワーク環境に導入されるワイヤレス装置を設定するための一実施形態による方法を示す図である。
【０００８】
【図４】ネットワーク環境に導入される図３のワイヤレス装置を設定するようアクセスポ

イント及び他の装置のための一実施形態による方法を示す図である。
【０００９】
【図５】本発明の特定の特徴が実施されうる好適なコンピュータ環境を示す図である。
【発明を実施するための最良の形態】
【００１０】
図示する本発明の実施形態は、ネットワーク環境への装置の導入時に、その装置を安全に設定することを可能にする。さらに、様々な実施形態において、本願に説明する設置及び設定技術は、装置をネットワーク環境内に自動的に組み込み設置する前に、装置へのアクセス、装置の制御、及び／又は装置の所有権を確認することを提供する。このようなアクセス、制御、及び／又は所有権の確認によって、新しい装置が正しくないネットワーク環境に誤って設置されることを阻止することができる。正しくないネットワーク環境に誤って設置されてしまうという問題は、互いに近い多数の「デジタルオフィス」又は「デジタルホーム」環境がある場合に発生しうる。
【００１１】
例えば、１つのアパートメントビル内の多数のテナントが本願に記載するように動作するよう設定される装置を購入したと仮定すると、１ユーザの装置が自動的に設定されて、別のユーザのネットワーク環境と動作するようにされてしまうと不都合である。このようなことは、ネットワーク環境において潜在的にオーバーラップがある場合に発生しうる。例えば、ワイヤレスネットワーク環境及び／又はホームプラグ・パワーライン・アライアンス（インターネット・ユニフォーム・リソース・ロケータ（ＵＲＬ）ｗｗｗ－ｈｏｍｅｐｌｕｇ－ｏｒｇを参照されたい（なお、ハイパーリンク設定を回避する目的で、上述のＵＲＬのピリオドはハイフンに置き換えている））といった有線環境において発生しうる。これらの両方のネットワーク環境において、組み込み設置されるべき装置は、予想するよりも多くの様々な人々及び／又は装置によってアクセス可能となってしまいうる。
【００１２】
このような問題を回避するには、上述したように、自動設置は、ネットワーク環境内に設定される装置へのアクセス、装置の制御、及び／又は装置の所有権を示すなんらかの作業に最初に従事するよう適応されている。様々な実施形態は、様々な技術を使用して、そのような証明となるものを供給しうる。これには、例えば、装置上に特殊識別子（ＩＤ）、個人識別番号（ＰＩＮ）、又は他のデータを表示することや、装置に添付されるラベル上に、バーコード内に、又は、ＲＦＩＤ（無線周波数識別）マーカ又は他の専用狭域通信（ＤＳＲＣ）装置内にＩＤ、ＰＩＮ等を供給することや、ブルートゥース送信器といった短距離送受信器又はＵＳＢに基づいた携帯メモリ装置に組み込まれるようなドングル又は携帯フラッシュメモリ記憶装置によってＩＤ、ＰＩＮ等を転送することが含まれる。
【００１３】
なお、これらは、装置へのアクセス、装置の制御、及び／又は装置の所有権を証明し、同時に、ネットワーク環境内での使用のために装置を少なくとも最初に設定するために少なくとも部分的に使用されうるデータを供給する幾つかの例示的な技術に過ぎないことは理解されよう。詳細な説明及び請求項の記載において、用語「設定鍵」は、上述したような証明が装置の設定を容易にするデータと共に供給されうるこれらの及び他の方法を集合的に参照するために使用する。
【００１４】
説明する実施形態では、設定鍵は、装置、又は、装置が接続されるアクセスポイント、ルータ、ハブ、及び他の装置等に対して任意の特別なハードウェアを必要とすることなく有線及び無線のネットワーク環境において使用されうる。つまり、本発明の実施形態は、完全にソフトウェアにおいて、又は、汎用ハードウェアにロードされた命令を介して実施されうる。
【００１５】
図１は、本願に開示する実施形態の原理に従って動作しうる複数の装置からなる例示的なシステム１００を示す。ネットワーク１０２を示すが、これは、任意のタイプの有線及

び／又は無線のネットワークでありうる。有線ネットワークを標準的であると考える場合、ワイヤレスアクセスポイント１０４（即ち「基地局」）を示す。これは、例えば、有線ネットワークと無線ネットワークを互いに通信可能に結合する装置である。周知の無線システムには、ＩＥＥＥ（電気電子学会）によってＬＡＮ（ローカル・エリア・ネットワーク）技術について推奨されるＩＥＥＥ８０２．１１ｘファミリーの仕様に基づいた無線システムが含まれる。ＩＥＥＥ８０２．１１は、ワイヤレス装置１０６とアクセスポイントとの間の無線（over-the-air）インターフェイス（「インフラストラクチャ」通信モード）と、２つ以上のワイヤレスクライアント間の通信（「アドホック」通信モード）の仕様を定める。

【００１６】

ワイヤレス装置１０６は、ネットワーク１０２を介してストリーミングされる音楽を受信するよう設計された音楽プレイヤであり、このプレイヤは、既存のオーディオビジュアル処理機器１０８（例えば、ステレオ、ビデオプロセッサ、テレビ受像機、プロジェクタ、アンプ、媒体プロセッサ／モディファイア／スイッチ等）とインタラクトし、既存のワイヤレススピーカ１１０を介して音楽出力を供給することを期待して、システム１００内に導入されると仮定する。ネットワークはさらに、コンピュータ１１２システム、ＤＶＲ（デジタル・ビデオ・レコーダ）１１４、及び他の図示しない装置といった他の装置も含んでもよい。無線ネットワーク、ホームプラグ・ネットワーク、及び従来の有線ネットワークは、その上で動作し、また、システム１００内で相互に接続されて様々な所望のタスクを実行する多くの可能な装置を有しうることは理解されよう。

【００１７】

上述したように、ワイヤレス音楽装置１０６がシステム１００内に導入される場合、装置１０６へのアクセス、装置１０６の制御、及び／又は装置１０６の所有権を証明すると同時に、間違ったネットワークへの偶発的な関連付け又は装置への意図的な攻撃を阻止する目的で、装置は、電源が入れられて自動設定モードとなると仮定する。この自動設定モードでは、上述したように、装置のユーザに対して装置の設定に使用するデータが提示される。アクセス／制御／所有権は、自動設定時に提示されるデータにアクセスを有することで証明されたとみなされる。なお、本願では、自動設定の成功／失敗は詳細には説明しない。自動設定が失敗及び／又は中止される場合、従来の技術を当然使用して、新しい装置をシステム１００内に導入するよう設定してもよい。装置の設定は、以下の図面についてより詳細に説明する。

【００１８】

図２は、図１のネットワークシステム１００内に導入される、例えば、装置１０６を設定するための一実施形態による方法を示す。

【００１９】

図示する実施形態では、装置に電源が入れられ（２０２）、自動設定モードに入る（２０４）ことがデフォルトに設定される。自動設定モードでは、装置は、装置の設定に使用することのできる設定鍵を供給する（２０６）。一実施形態では、設定鍵は、設定鍵をスクリーン（例えば、ＬＣＤ（液晶ディスプレイ）、ＴＦＴ（薄膜トランジスタ）、ＬＥＤ（発光ダイオード）アレイ、又は他の出力）上に表示することで供給される。一実施形態では、設定鍵は、ランダムに生成される。従って、基本的に同一である装置が製造され世界中に出荷されることを可能にする。一実施形態では、設定は、装置が自動又は手動で設定されるまで、又は、自動設定が無効にされるまで装置の電源投入に呼応して自動的に生成される。別の実施形態では、上述したように、設定鍵は、一部の永久識別子、又は、シリアル番号、ＭＡＣ（媒体アクセス制御）アドレス等の装置の他の特徴である又はそれらに基づいてよく、様々な異なる方法で供給されうる。

【００２０】

設定鍵が供給される（２０６）と、その鍵は、装置の設定に関与する第２の装置において入力されうる（２０８）。装置が導入されるネットワーク環境は、予期せぬ侵害者が、無線ネットワーク又はホームプラグに基づく有線ネットワークといったネットワーク上で

送信されるパケットにアクセスを有しうるという意味から安全ではない場合があるという前提を思い出されたい。従って、装置が導入される場合、ネットワーク環境の既存の装置は、新しい装置の設定に関与すると期待される。これは、ネットワーク上の任意の現在の装置でありうる。無線ネットワークでは、設定に関与する装置は、一般的に、例えば、ワイヤレスアクセスポイントであってよく、装置はこれを介してネットワークに接続される。なお、ネットワーク環境は、セキュア（暗号化）モード、又は、非セキュア（非暗号化）モードで動作しうる。また、ネットワークの第２の装置は、ネットワークのセキュアな状態に関係なく新しい装置と通信すると仮定する。

【００２１】

第２の装置において鍵を入力した（２０８）後、一時的なセキュア通信チャネルが確立される（２１０）。なお、このセキュリティは、弱いと考えられる。これは、設定鍵はあまり多くのデータを提示せず、このデータから一時的なセキュリティを得るということによる。つまり、設定鍵をユーザによって容易に管理可能とする目的で（例えば、第２の装置への入力（２０８）のためにユーザが見て覚えられるもの）、幾つかの文字からなる比較的短い鍵が供給される（２０６）が、このようなユーザへの利便性の暗号的な視点から見た場合のマイナス面は、短い鍵は、あまり安全ではない暗号鍵となるということである。しかし、目標としては、一時的に安全にされたチャネルのセキュリティを破ることが不可能ではないにしても現実的ではないほどに安全であるセキュア通信チャネルを形成することである。例えば、３文字の設定鍵を使用して、鍵の１つ以上の文字を繰り返すことで４０ビットの暗号化鍵を決定しうる。一実施形態では、第２の装置でのＰＩＮ入力（２０８）の正確さを確認することを可能にする目的で、余剰桁の鍵を設定鍵のチェックサムとして作成することができる。文字によって本質的に表されるビット数に依存して、及び／又は、入力として鍵の文字の繰り返し又は関数を介して鍵の文字から任意の鍵の長さを得ることができるは理解されよう。

【００２２】

一時的に安全にされた通信チャネルがこのように確立される（２１０）と、そのチャネルは、装置内にプログラムされることが可能である（２１２）永久セキュリティ・クレデンシャルを安全に伝えるために使用される。永久クレデンシャルは、従来の暗号化形式において、その永久クレデンシャルを使用して暗号化された比較的安全な任意のチャネルを与えるよう十分に長い。従って、新しい装置は、その一部又は全体が安全であるとみなされていないネットワーク環境への導入時に装置が自動的に設定可能であり、同時にユーザがその装置に対して適切なアクセス、制御、及び／又は所有権を有することを確実にする（供給された（２０６）設定鍵へのアクセスを要求することによって）ことでネットワーク環境内に導入可能である。

【００２３】

図３は、アクセスポイントを含むネットワーク環境に導入される、例えば、ワイヤレス装置を設定するための一実施形態による方法を示す。

【００２４】

説明する実施形態では、例えば、電源を入れること、設定ボタンを押すこと等によってワイヤレス装置を起動（３０２）後、装置は、自動設定モードに入る（３０４）。自動設定モードでは、装置は、装置の設定に使用可能な設定鍵を表示する（３０６）。上述したように、様々な技術を使用して、設定鍵を表示、そうでなければ提示しうる。鍵が表示される（３０６）と、既知の機能を使用してＳＳＩＤ（サービスセット識別子）又は設定鍵に基づいた同様の識別子を生成し、このＳＳＩＤを、例えば、装置がこの一意のＳＳＩＤを使用するよう設定する等、装置のワイヤレスハードウェアによる使用に設定する（３０８）。この機能は、少なくとも、ワイヤレス装置と、新しい装置を永久セキュリティ・クレデンシャルでプログラムするアクセスポイントといった第２の装置に既知であることが期待される。

【００２５】

ＳＳＩＤを設定（３０８）後、別の既知の機能を使用して暗号鍵を生成し（例えば、W

ＥＰ、ＷＰＡ等）、暗号が、装置による使用のために設定される（３１０）。演算３０８、３１０についての「既知の機能」との参照は、設定鍵からＳＳＩＤ及びＷＥＰ／ＷＰＡ鍵を生成するために任意の変換を使用しうることを意味する。新しい装置と、その新しい装置の設定に関与する第２の装置が共に同じ変換機能を使用する限り、特定の変換である必要はない。例えば、ＳＳＩＤは、「ｉｎｉｔ」といった所定の基本句が設定鍵の１つ以上の文字と連結されることで生成可能であり、ＷＥＰ／ＷＰＡは、設定鍵の文字の一部又は全部を対応ＷＥＰ／ＷＰＡ１６進シーケンスに変換することによって決定される。

【００２６】

装置は、そのＳＳＩＤ及びＷＥＰ／ＷＰＡを設定（３０８、３１０）後、例えば、インフラストラクチャモード又はアドホックモードを介して、アクセスポイント又は永久セキュリティ・クレデンシャルで装置をプログラムする（３１４）ことに関与する他の装置との一時的に安全にされたチャンネルを確立する（３１２）ことができる。

【００２７】

図４は、ネットワーク環境に導入される図３のワイヤレス装置を設定するようアクセスポイント又は他の装置のための一実施形態による方法を示す図である。

【００２８】

図３の工程３０２乃至３１０が発生した又は実行されると仮定すると、図１の構成要素１０４といったアクセスポイントは、新しい装置を管理するよう準備をし、その新しい装置を適切なセキュリティ・クレデンシャルでプログラムすることができる。なお、セキュリティ・クレデンシャルには、暗号データだけではなく、新しい装置が導入されるネットワーク環境に適用可能であるとして新しい装置に伝えられうる、ローカルポリシー、規則、サービスの条件、請求料率等も含みうる。説明する実施形態では、必要な場合、アクセスポイントの現在のワイヤレス設定（例えば、そのＳＳＩＤ及びＷＥＰ又はＷＰＡ鍵）が保存される（４０２）。なお、設定の保存は、プロファイルマネジャ又は等価物が利用可能であり、現在の設定を交換するのではなく、より高い優先順位を有する新しい一時的なプロファイルが新しい装置の設定鍵に基づいて作成される特定の環境において不必要であり得ることは理解されよう。

【００２９】

必要に応じて現在の設定を保存（４０２）後、ユーザは、新しい装置上に表示された（３０６）設定鍵を入力するようプロンプトされる（４０４）。上述したように、この鍵へのアクセスは、新しい装置へのアクセス、制御、及び／又は所有権を証明するので、この新しい装置はまさにネットワーク環境に入ることを許可されるべきであることを保証する。図３の演算３０８、３１０に対して相補的に、アクセスポイントは、そのＳＳＩＤ及びＷＥＰ／ＷＰＡ暗号鍵を、装置の設定鍵に応じて設定する（４０６、４０８）。設定後、アクセスポイントは、図３の演算３１２に対して相補的な一時的に安全にされたチャネルを確立する（４１０）。なお、様々な技術を用いて、新しい装置と通信するようアクセスポイントを再設定しうる。一実施形態では、アクセスポイントは、設定鍵を入力するための内蔵された簡単なユーザーインターフェイスを有してもよい。別の実施形態では、ソフトウェアが、アクセスポイントと通信可能に結合されるコンピュータ又は他の機械上で実行されてもよく、このコンピュータ又は機械は、演算４０６、４０８のためにアクセスポイントを再プログラムする。

【００３０】

一時的な安全な接続の確立（３１２、４１０）後、新しい装置は、永久セキュリティ・クレデンシャルでプログラムされうる。アクセスポイントの設定と同様に、様々な技術を使用して新しい装置をプログラムしうる。例えば、一実施形態では、アクセスポイントは、その永久ワイヤレス・クレデンシャルを一時的に安全にされたチャネルを介して新しい装置に自動的に押出しするよう内蔵された機能を有してもよい。又は、別の実施形態では、ソフトウェアが、アクセスポイントと通信可能に結合されるコンピュータ又は他の機械上で実行されてもよく、このコンピュータ又は機械は、演算４１２を実行するよう永久セキュリティ・クレデンシャルで新しい装置をプログラムする。

【００３１】
新しい装置が、永久クレデンシャルでプログラムされると、一時的な通信チャネルは必要でなくなり、アクセスポイントは、そのいつもの（例えば、保存された（４０２））ワイヤレス設定に戻ってよい（４１４）。プロファイルマネジャ又は等価物を使用する上述した一実施形態では、「戻る」ことは、単純に、新しい装置との通信のために作成された一時的なプロファイルを削除することである。別の実施形態では、「戻る」ことは、アクセスポイントのＳＳＩＤ及びＷＥＰ／ＷＰＡ鍵を再設定することが必要としうる。上述したように、アクセスポイントは、アクセスポイント自身でその状態を回復するようプログラムされてもよく、又は、外部のコンピュータ又は他の機械がその状態を操作してもよい。

【００３２】
従って、新しい装置は、その新しい装置のワイヤレスネットワーク環境導入時に自動設定可能であり、同時に（表示された（３０６）設定鍵へのアクセスを要求することによって）ユーザが新しい装置へのアクセス、制御、及び／又は所有権を有することも保証することで、ワイヤレスネットワーク環境内に導入可能である。

【００３３】
図５及び以下の説明は、説明する発明の特定の特徴を実施しうる好適な環境の簡単且つ一般的な説明を与えることを目的とする。以下、本願にて使用するように、用語「機械」は、単一の機械、又は、共に動作する複数の機械又は装置に通信可能に結合されるシステムを広義に包含することを意図する。例示的な機械は、パーソナルコンピュータ、ワークステーション、サーバ、ポータブルコンピュータ、例えば、携帯情報端末（ＰＤＡ）といったハンドヘルド装置、電話機、タブレット等といったコンピューティング装置、及び、例えば、自動車、電車、タクシーといった私用又は公共の交通手段といった輸送装置を含む。

【００３４】
一般的に、環境は、プロセッサ５０４、メモリ５０６（例えば、ランダムアクセスメモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、又は他の状態保存媒体といったメモリ５０６、記憶装置５０８、ビデオインターフェイス５１０、及び入出力インターフェイスポート５１２が接続するシステムバス５０２を含む機械５００を含む。機械は、キーボード、マウス等の従来の入力装置からの入力によって、また、別の機械から受信される指示、バーチャルリアリティ（ＶＲ）環境とのインタラクション、バイオメトリックフィードバック、又は他の入力源又は信号によって、少なくとも部分的に制御されうる。

【００３５】
機械は、プログラム可能又は非プログラム可能な論理装置又はアレイ、特定用途向け集積回路、組み込みコンピュータ、スマートカード等といった組み込みコントローラを含みうる。機械は、例えば、ネットワークインターフェイス５１８、モデム５２０、又は他の通信結合を介する１つ以上の遠隔機械５１４、５１６への１つ以上の接続を使用してもよい。機械は、図１のネットワーク１０２、イントラネット、インターネット、ローカル・エリア・ネットワーク、及びワイド・エリア・ネットワークといった物理的及び／又は論理的ネットワーク５２２を介して相互接続されうる。当業者は、ネットワーク５２２との通信は、無線（ＲＦ）、衛星、マイクロ波、ＩＥＥＥ（電気電子学会）８０２．１１、ブルートゥース、光学、赤外線、ケーブル、レーザ等を含む様々な有線及び／又は無線短距離又は長距離の搬送波及びプロトコルを使用しうることは理解されよう。

【００３６】
本発明は、機械によってアクセスされると機械がタスクを実行する又は抽象的データタイプ又は下位ハードウェアコンテキストを定義する、機能、手順、データ構造、アプリケーションプログラム等といった関連データを参照して、又は、関連データとともに説明されうる。関連データは、例えば、揮発性及び／又は不揮発性メモリ５０６、又は、記憶装置５０８、及び／又は、従来のハードドライブ、フロッピー（登録商標）ディスク、光学記憶装置、テープ、フラッシュメモリ、メモリスティック、デジタルビデオディスク等、

並びに機械アクセス可能な生物状態保存記憶装置といった非標準型媒体を含む関連付けられる記憶媒体内に格納されうる。関連データは、ネットワーク５２２を含む伝送環境を介して、パケット、シリアルデータ、パラレルデータ、伝播信号等の形で供給されえ、また、圧縮又は暗号化形式で使用されうる。関連データは、分散環境において使用されてもよく、また、シングル又はマルチプロセッサ機械によるアクセスのためにローカル及び／又はリモートに格納されうる。関連データは、組み込みコントローラによって又は組み込みコントローラとともに使用されうる。従って、請求項において、用語「論理」とは、関連データ及び／又は組み込みコントローラの可能な組み合わせを一般的に指すことを意図する。

【００３７】

従って、例えば、説明した実施形態について、機械５００は、図１の新しい装置１０６を具現化し、遠隔機械５１４、５１６はそれぞれ図１のアクセスポイント１０４及びコンピュータ１１２であり得ると仮定する。なお、遠隔機械５１４、５１６は、機械５００と同様に設定されるので、機械について説明した構成要素の多く又は全てを含むことは理解されよう。

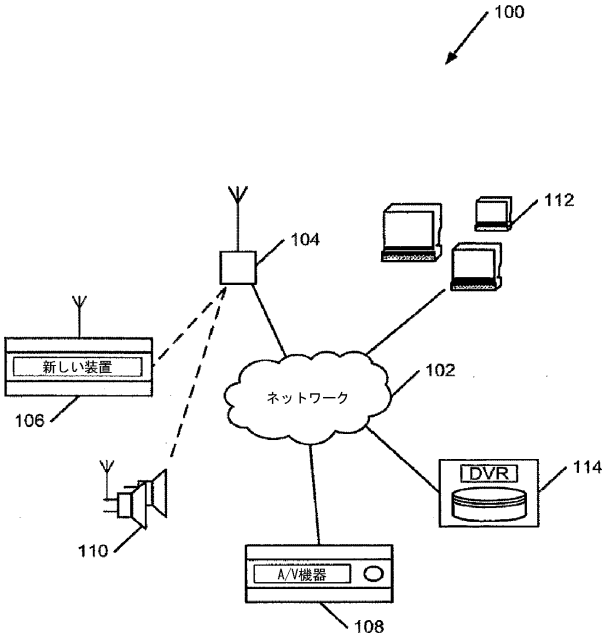
【００３８】

図示する実施形態を参照して本発明の原理を説明及び図示したが、説明した実施形態は、このような原理から逸脱することなく、配置構成及び詳細において変更可能であることは認識されよう。また、上述の説明は、特定の実施形態に注目して行ったが、他の構成も考えられる。特に、「一実施形態では」、「別の実施形態では」等の表現を本願に使用するが、これらの表現は、実施形態の可能性を一般的に参照するものであって、発明を特定の実施形態構成に限定することを意図しない。本願に使用するように、これらの用語は、他の実施形態と組み合わせ可能な同一の又は異なる実施形態を参照しうる。

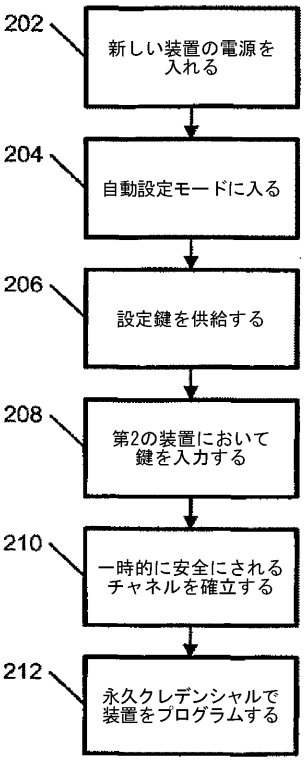
【００３９】

従って、本願に記載する実施形態に様々な置き換えが可能であることを鑑みて、この詳細な説明は、例示的に過ぎず、発明の範囲を限定するとして解釈すべきではない。従って、特許を請求する発明とは、請求項及びその等価物の範囲及び精神内に包含されるのでそのような変形も全て含む。

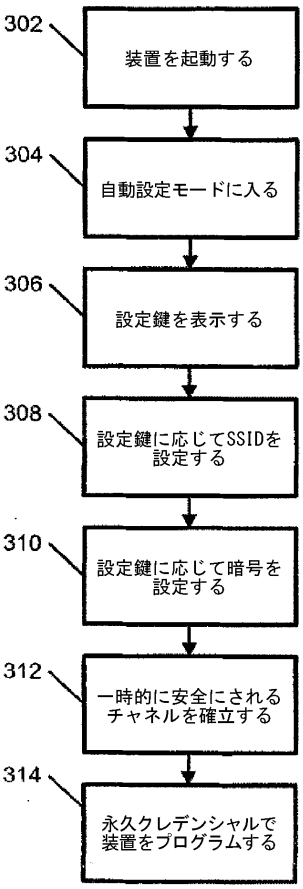
【図１】


100
104
112
新しい装置
106
ネットワーク
102
DVR
114
110
A/V機器
108

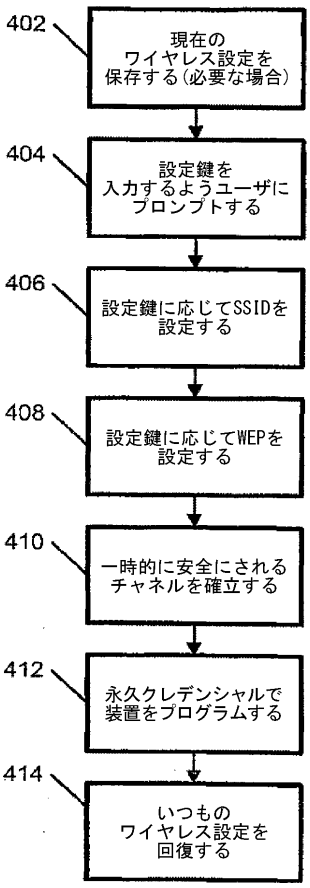
【図２】


202
新しい装置の電源を入れる
204
自動設定モードに入る
206
設定鍵を供給する
208
第2の装置において鍵を入力する
210
一時的に安全にされるチャネルを確立する
212
永久クレデンシャルで装置をプログラムする

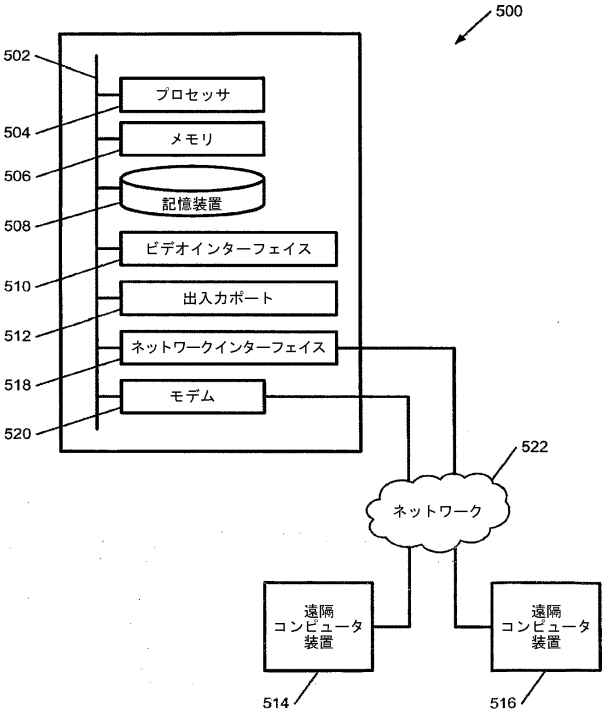
【図３】


302
装置を起動する
304
自動設定モードに入る
306
設定鍵を表示する
308
設定鍵に応じてSSIDを設定する
310
設定鍵に応じて暗号を設定する
312
一時的に安全にされるチャネルを確立する
314
永久クレデンシャルで装置をプログラムする

【図４】


402
現在のワイヤレス設定を保存する(必要な場合)
404
設定鍵を入力するようユーザにプロンプトする
406
設定鍵に応じてSSIDを設定する
408
設定鍵に応じてWEPを設定する
410
一時的に安全にされるチャネルを確立する
412
永久クレデンシャルで装置をプログラムする
414
いつものワイヤレス設定を回復する

【図５】


500
502
プロセッサ
504
メモリ
506
記憶装置
508
ビデオインターフェイス
510
出入力ポート
512
ネットワークインターフェイス
518
モデム
520
522
ネットワーク
遠隔
コンピュータ
装置
514
遠隔
コンピュータ
装置
516

フロントページの続き

(56)参考文献　特開２００５－１４２９０７（ＪＰ，Ａ）
米国特許出願公開第２００５／０１２５６６９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B 7/24- 7/26
H04W 4/00-99/00
H04M 11/00
H04L 9/08