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

特許第4197959号
(P4197959)

(45)発行日　平成20年12月17日(2008.12.17)　(24)登録日　平成20年10月10日(2008.10.10)

(51)Int.Cl.		F I		
H04Q 7/38	(2006.01)	H04Q	7/00	152
H04Q 7/32	(2006.01)	H04Q	7/00	185
G06F 21/22	(2006.01)	H04Q	7/00	645
		G06F	9/06	660E

請求項の数 7　(全 11 頁)

(21)出願番号　特願2003-508(P2003-508)
(22)出願日　平成15年1月6日(2003.1.6)
(65)公開番号　特開2004-32666(P2004-32666A)
(43)公開日　平成16年1月29日(2004.1.29)
審査請求日　平成17年12月22日(2005.12.22)
(31)優先権主張番号　10/037267
(32)優先日　平成14年1月2日(2002.1.2)
(33)優先権主張国　米国(US)

(73)特許権者　398038580
ヒューレット・パッカード・カンパニー
HEWLETT-PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(74)代理人　100099623
弁理士　奥山　尚一
(74)代理人　100096769
弁理士　有原　幸一
(74)代理人　100107319
弁理士　松島　鉄男

最終頁に続く

(54)【発明の名称】無線装置の権限なき使用を防止するシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
権限なき使用を防止するプロセッサベースの装置であって、
ソフトウェア命令を実行するプロセッサと、
少なくとも１つのユーザ・アプリケーションを定義するソフトウェア命令と、
無線プロトコルを利用してデータを送受信するように動作可能な無線通信サブシステムと、
該無線通信サブシステムを介してメッセージを受け取ったときに、前記少なくとも１つのユーザ・アプリケーションを定義する前記ソフトウェア命令が前記プロセッサによって実行されるのを防止するように動作可能であるセキュリティ・プロトコル・プロセスを定義するソフトウェア命令であって、前記プロセッサベースの装置が正当なユーザによって所有されていないことを前記メッセージが示すものである、ソフトウェア命令と、
前記セキュリティ・プロトコル・プロセスが、少なくとも１つのユーザ・アプリケーションを定義する前記ソフトウェア命令の実行が許可されないことを示す情報を記憶するように動作可能である不揮発性メモリと、
前記プロセッサベースの装置を起動するために動作可能であり、起動動作を完了する前に前記セキュリティ・プロトコル・プロセスの完全性を検証するように動作可能な基本入出力システムと
を備えてなる装置。
【請求項２】

ユーザ・データをさらに含み、前記セキュリティ・プロトコル・プロセスが、前記メッセージを受け取ったときに前記ユーザ・データへのアクセスを防止するように動作可能である請求項１に記載のプロセッサベースの装置。

【請求項３】

前記メッセージを受け取ったときに前記少なくとも１のユーザ・アプリケーションが実行されている場合には、前記セキュリティ・プロトコル・プロセスが、前記少なくとも１つのユーザ・アプリケーションを終了させるように動作可能である請求項１または２に記載のプロセッサベースの装置。

【請求項４】

表示装置をさらに含み、前記セキュリティ・プロトコル・プロセスは、前記正当なユーザが前記プロセッサベースの装置を所有していないことを示す情報を前記表示装置に提示させる請求項１に記載のプロセッサベースの装置。

【請求項５】

無線通信を行うプロセッサベースの装置を権限なき使用から保護する方法であって、

前記プロセッサベースの装置が、正当なユーザによって所有されていないという通知を受け取るステップと、

前記プロセッサベースの装置にメッセージを送って、無線通信プロトコルを介したセキュリティ・プロトコルを開始するステップと、

前記プロセッサベースの装置が前記メッセージを受け取るステップと、

前記受け取ったメッセージに応じて、前記プロセッサベースの装置上で前記セキュリティ・プロトコルを開始するステップであって、前記プロセッサベースの装置による前記メッセージの受け取りに応じて、前記プロセッサベースの装置に記憶されたソフトウェア命令によって定義された少なくとも１つのユーザ・アプリケーションを前記プロセッサベースの装置が実行するのを防止するものである、開始するステップと、

前記プロセッサベースの装置の不揮発性メモリに、前記受け取ったメッセージに応じて、前記プロセッサベースの装置が前記正当なユーザによって所有されていないという情報を書き込むステップと、

起動動作を完了する前に前記セキュリティ・プロトコル・プロセスの完全性を検証するステップと

を含んでなる方法。

【請求項６】

前記受け取ったメッセージに応じて、前記プロセッサベースの装置に記憶されたユーザ・データへのアクセスを防止するステップをさらに含む請求項５に記載の方法。

【請求項７】

前記プロセッサベースの装置が、前記正当なユーザによって所有されてないというメッセージを前記プロセッサベースの装置の表示装置に表示するステップをさらに含む請求項５に記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、無線通信に関し、より詳細には、無線装置が権限なく使用されるのを防止するシステムおよび方法に関する。

【０００２】

【従来の技術】

セルラ式電話製品は、これまで相当な数の消費者に配布されている。最も一般的なセルラ式電話製品は携帯電話である。米国では、一般に、携帯電話の動作を定義する２つのセルラ式電話規格が利用されている。第１に、時分割多重化／時分割多元接続（ＴＤＭ／ＴＤＭＡ）携帯電話規格が、米国電気通信工業会／米国電子工業会（ＴＩＡ／ＥＩＡ）の規格ＩＳ－４１およびＩＳ－１３６によって定義されている。第２に、符号分割多元接続（ＣＤＭＡ）携帯電話規格が、ＴＩＡ／ＥＩＡ規格ＩＳ－９５によって定義されている。この

両方の規格は、携帯電話加入者がそれぞれの携帯電話ネットワークにアクセスできるようにする様々な物理層要件および公衆インタフェース・プロトコルを定義している。

【０００３】

携帯電話（ＴＤＭ／ＴＤＭＡ準拠とＣＤＭＡ準拠との両方の電話）には、それぞれの電子的シリアル番号（Electronic Serial Number：以下、「ＥＳＮ」とよぶ）とモバイル識別番号（Mobile Identification Number：以下、「ＭＩＮ」とよぶ）が割り当てられる。ＥＳＮは、携帯電話を識別するために使用される固有の３２ビット・シリアル番号である。ＭＩＮは、例えば、携帯電話の電話番号である。

【０００４】

セルラ・ネットワークは、加入者が実際に任意の場所からネットワークにアクセスすることを可能にするので、セルラ・ネットワークは、様々なセキュリティ・アルゴリズムを使用して無許可のセルラ・ネットワークの使用を防止している。具体的には、セルラ・ネットワークでは、サービス制御ポイント（service control point：以下、「ＳＣＰ」とよぶ）を利用してセキュリティ・アルゴリズムを働かせている。ＳＣＰは、Ｎｏ．７共通線信号方式（Signaling System 7：以下、「ＳＳ７」とよぶ）ネットワーク内のリモート・データベースである。ＳＣＰは、一般に、多くのセルラ・システムにおいて、ホーム・ロケーション・レジストリ（home location registry：以下、「ＨＬＲ」とよぶ）機能を実現するために使用されている。ＨＬＲ機能は、それぞれのセルラ装置用にセルラ・ネットワークとの対話を制御するデータベース・レコードを維持する。データベース・レコードは、セルラ装置がネットワークにアクセスすることを許可されているかどうかを示すことができる。また、データベース・レコードは、セルラ装置がネットワーク内で現在アクティブかどうかを示すことができ、ネットワーク内のセルラ装置のそれぞれの位置を識別してセルラ装置へのデータ・ルーティングを容易にすることができる。

【０００５】

携帯電話が、セルラ・ネットワークにアクセスして、例えばネットワークに登録して呼を受け取ろうとするとき、携帯電話は、ＥＳＮとＭＩＮとを加入者電話交換機に送る。加入者電話交換機は、ＭＩＮを利用して携帯電話と関連付けられたセルラ・プロバイダを決定する。そして、加入者交換機は、ＳＳ７メッセージ伝達によってそれぞれのＨＬＲを維持するセルラ・プロバイダにＥＳＮを送る。ＳＣＰは、携帯電話が正当な装置かどうかをＥＳＮから判定する。正当な装置の場合には、ＳＣＰは加入者交換機に適切なメッセージを送り、加入者交換機はセルラ・ネットワークへのアクセスを許可する。装置が正当でない場合には、ＳＣＰは加入者交換機に適切なメッセージを送り、加入者交換機はセルラ・ネットワークへのアクセスを拒否する。

【０００６】

セルラ装置が盗まれたときには、そのセルラ装置の所有者は、顧客サービス代理店またはセルラ・プロバイダの自動化されたシステムに連絡をとることができる。その所有者は、盗まれた装置のＭＩＮを提供することができる。セルラ・プロバイダは、対応するＥＳＮと関連付けられた装置が正当でないことを示すためにそのＨＬＲ内のレコードを更新する。この結果、盗まれた装置は動作可能なままではあるが、携帯電話を利用しようとしても、どのセルラ・ネットワークにもアクセスすることができない。セルラ・ネットワークのセキュリティ・プロトコルを利用することによって、携帯電話を盗む動機が著しく低減される。

【０００７】

しかしながら、この手法は他の無線装置には問題である。具体的には、携帯電話は、本質的に、セルラ・ネットワークにアクセスする以外に他の目的がない。しかしながら、多くの市販の無線およびセルラ装置は、様々な機能を実行する。例えば、ヒューレット・パッカード社のＪｏｒｎａｄａ　５６０　ＰＤＡ等の無線携帯情報端末（personal data assistant：以下、「ＰＤＡ」とよぶ）は、無線通信を実行できる他に、様々な業務と、マルチメディアと、娯楽アプリケーションとを実行することができる。従来の携帯電話のセキュリティ・プロトコルが無線ＰＤＡに適用されている場合には、無線ＰＤＡを盗んだ人は

、ＰＤＡを無線通信に使用することができない。しかしながら、その人は、ＰＤＡを使って様々な他のソフトウェア・アプリケーションを実行することができる。

【０００８】

さらに、盗まれたパーソナル・コンピュータが権限なく使用されるのを防ぐために、これまで様々なセキュリティ・アルゴリズムが利用されてきた。例えば、多くのパーソナル・コンピュータは、様々なユーザ・アプリケーションを利用するにはパスワードを必要とする。このパスワードは、起動スクリプトから要求されることがある。あるいは、パスワードは、ユーザが所定の期間データを入力しなかったときに起動される「スクリーン・セーバ」プロセスから要求されることがある。しかしながら、このようなパスワード要求は両方とも、一般に効果がない。第１に、ほとんどのユーザは、パスワード要求を面倒だと感じており、そのような機能を意図的に解除している。さらに、パスワード要求は、パスワード・スクリプトを呼び出さない（例えば、フロッピー・ディスク等の）システム・ディスクを利用するパーソナル・コンピュータを起動するか、またはパスワード機能の実施方法によりパーソナル・コンピュータを再設定することによって克服される場合がある。

【０００９】

【課題を解決するための手段】

１つの実施形態において、本発明は、ソフトウェア命令を実行するプロセッサと、少なくとも１つのユーザ・アプリケーションを定義するソフトウェア命令と、無線プロトコルを利用してデータを送受信するように動作可能な無線通信サブシステムと、無線通信サブシステムを介して、正当なユーザによって所有されていないことを示すメッセージを受け取ったときに、少なくとも１つのユーザ・アプリケーションを定義するソフトウェア命令がプロセッサによって実行されないように動作可能なセキュリティ・プロトコル・プロセスを定義するソフトウェア命令とを含む、権限なき使用を防止するプロセッサベースの装置を対象とする。

【００１０】

【発明の実施の形態】

図１は、本発明の実施形態を実現することができる例示的な無線装置１００を示す。無線装置１００は、無線通信サブシステム１０１を含むことが好ましい。無線通信サブシステム１０１は、無線装置１００が無線通信を行うことができるようにする。無線通信サブシステム１０１は、トランシーバや変復調装置やアンテナ等（図示せず）の無線通信用の様々な電子回路および構成要素を含みうる。無線通信サブシステム１０１は、ＴＤＭ／ＴＤＭＡや、ＣＤＭＡや、移動体通信標準（global system for mobile communications：以下、「ＧＳＭ」とよぶ）や、Ｍｏｂｉｔｅｘパケット交換や、ＣＤＰＤ（Cellular Digital Packet Data）、電気電子学会（ＩＥＥＥ）８０２．１１ｂ無線ＬＡＮ規格や、ブルートゥース（Bluetooth）規格等を含むが、これらに限定されない任意の数の無線通信プロトコルを実施することができる。しかしながら、本発明が、特定の無線通信プロトコルに限定されないことを理解されたい。本発明の実施形態は、一意に識別された装置へのリモート・アクセスを可能にする任意の適切な通信プロトコルを利用することによって実行することができる。

【００１１】

無線装置１００は、プロセッサ１０２を含む。プロセッサ１０２は、実行可能な命令またはコードの管理の下で動作する。プロセッサ１０２は、例えばＳＴＲＯＮＧＡＲＭプロセッサやＲＩＳＣプロセッサ等を利用することにより実現することができる。本発明が、プロセッサ１０２のアーキテクチャに限定されないことを理解されたい。プロセッサ１０２が、本明細書に示したような発明の動作に関する限り、任意の適切なプロセッサ１０２を利用することができる。

【００１２】

無線装置１００は、オペレーティング・システム１０３をさらに含みうる。オペレーティング・システム１０３は、不揮発性メモリ１０６にインストールすることができる。不揮発性メモリ１０６は、（ＰＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ等の）フラッシュ・メモリ

や、メモリ・カードや、ハード・ディスク等を利用することによって実現することができる。（動的にロード可能なカーネルが利用される場合には）オペレーティング・システム１０３またはその一部分を、起動手順の間に、ランダム・アクセス・メモリ（ＲＡＭ）１０８へとロードすることができる。オペレーティング・システム１０３は、無線装置１００上で実行する他のすべてのプログラムまたはアプリケーションを管理することができる。オペレーティング・システム１０３は、例えば、プロセス管理を実行し、内部メモリを管理し、入出力（Ｉ／Ｏ）動作を制御することができる。

【００１３】

オペレーティング・システム１０３は、セキュリティ・プロトコル１１０を含むことが好ましい。セキュリティ・プロトコル１１０は、無線装置１００が適切なセキュリティ初期化メッセージを受け取ると、リモートで呼び出すことができる。セキュリティ・プロトコル１１０の動作については、図５と関連してさらに詳しく論じる。

【００１４】

さらに、オペレーティング・システム１０３は、他のプログラムまたはアプリケーションがアクセスできるより下位レベルの機能を提供することができる。例えば、オペレーティング・システム１０３は、好ましい実施形態による保護カーネル１０４を含む。保護カーネル１０４は、カーネル・ルーチンやカーネル・ルーチン・テーブル等の修正を防止することにより、オペレーティング・システム１０３の修正を防止する。保護カーネル１０４を利用することにより、無線装置１００は、本発明の実施形態のセキュリティ・プロトコルが悪意のあるユーザによって欺かれる可能性を最小にする。アプリケーション・プログラム・インタフェース（ＡＰＩ）等を呼び出すか、またはシステム・コールを実行することによって、プログラムは保護カーネル１０４にアクセスすることができる。例えば、プログラムは、システム・コールを実行してファイルにアクセスする。同様に、プログラムは、システム・コールを実行して、無線通信サブシステム１０１を利用する伝送制御プロトコル／インターネット・プロトコル（ＴＣＰ／ＩＰ）接続を確立することができる。

【００１５】

無線装置１００は、基本入出力システム（ＢＩＯＳ）１０５を含みうる。ＢＩＯＳ１０５は、無線装置１００の最低レベルの機能を決定する組み込みソフトウェアである。ＢＩＯＳ１０５は、一般に、ＰＲＯＭやＥＰＲＯＭやＥＥＰＲＯＭ等のフラッシュ・メモリに記憶される。ＢＩＯＳ１０５は、キーボードと、表示画面と、ディスク・ドライブと、シリアル通信と、いくつかの補助機能を制御するコードとを含みうる。ＢＩＯＳ１０５は、無線装置１００の起動操作を定義するコードも含みうる。ＢＩＯＳ１０５は、オペレーティング・システム１０３またはその一部分をＲＡＭ１０８にロードするコードと、オペレーティング・システム１０３に処理制御を転送するコードとを含みうる。ＢＩＯＳ１０５は、例えばチェックサム計算を利用することによって、オペレーティング・システム１０３またはその一部分が修正されていないことを検証するコードも含みうる。詳細には、ＢＩＯＳ１０５は、セキュリティ・プロトコル１１０の完全性を検証することが好ましい場合、つまり、無線装置１００の起動条件として、セキュリティ・プロトコル１１０およびオペレーティング・システム１０３のロックアップ機能と関連したコードが修正されたかどうかを判定することが好ましい場合がある。さらに、ＢＩＯＳ１０５は、不揮発性メモリ１０６に記憶された状態情報を利用することによって、起動条件として、無線装置１００が権限なく使用されていないことを検証することができる。無線装置１００が権限なく使用されている場合には、ＢＩＯＳ１０５は、ユーザ・アプリケーション１０７とユーザ・データとに対するアクセスを防止する保護モードで無線装置１００を起動することができる。

【００１６】

無線装置１００は、ユーザ・アプリケーション１０７をさらに含みうる。ユーザ・アプリケーション１０７は、不揮発性メモリ１０６に記憶され、ユーザが初期化したときにＲＡＭ１０８にロードすることができる。ユーザ・アプリケーション１０７は、スケジューリング・プログラムや、パーソナル・コンタクト・プログラムや、ワード処理プログラムや

、表計算プログラムや、ブラウザ・プログラムや、音声コンテンツ表現プログラムや、ディジタル画像表示プログラム等のコードを含みうる。ユーザ・アプリケーション１０７は、ユーザ・インタフェース１０９を介してユーザと対話することができる。ユーザ・インタフェース１０９をタッチ式画面として実現することができる。ユーザ・アプリケーション１０７は、不揮発性メモリ１０６に適切なユーザ・データを記憶することができる。

【００１７】

図２は、本発明の実施形態に従ってセキュリティ・プロトコルがどのように開始されるかを示す例示的なフローチャート２００を表す。ステップ２０１において、無線装置１００が正当なユーザに所有されていないという通知を受け取る。正当なユーザは、例えば、無線装置１００を認可された形で利用することができる任意の人である。正当なユーザは、所有者や、賃借人や、装置を一時的に借りている人等でありうる。正当な所有者は、無線装置１００を、紛失したか、置き忘れたか、盗まれたか、返却されていない、または権限なく使用されているときに通知を受け取ることができる。例えば、無線装置１００の所有者は、無線装置１００に関連した適切なパスワードまたはコードおよび識別子を入力することができるウェブサイトを利用する。代わりに、通話料無料番号によって、自動システムまたは顧客サービス代理店からこの通知を受け取ることがある。

【００１８】

ステップ２０２において、サービス制御ポイント／ホーム・ロケーション・レジストリ（ＳＣＰ／ＨＬＲ）やその他のデータベースが、無線装置１００を紛失したか、置き忘れたか、返却されていない、盗まれたか、または権限なく使用されている可能性があることを示すために更新される。無線装置１００のユーザから通知を受け取ることができる。代わりに、通知を自発的に生成する場合がある。例えば、ユーザは、無線装置１００を利用して、アクセスが許可される前にパスワードを必要とする（無線装置１００に内部または外部にある）リソースにアクセスすることを試みる。ユーザが、誤ったパスワードを何度も送信した場合には、無線装置１００へのアクセスをユーザに許可すべきではないとみなされる場合がある。その結果、パスワード要求に関連した通知をリソースから生成する場合がある。

【００１９】

ステップ２０３において、無線装置１００が、ＳＣＰ／ＨＬＲのデータベース内でアクティブなものとして登録されている場合には、無線装置１００の使用を停止する「セキュリティ・プロトコル開始」メッセージが、無線装置１００に送られる。無線装置１００が、アクティブなものとして登録されていない場合には、通信を行うことができず、そのときＳＣＰ／ＨＬＰは通信を試みないことが好ましい。ステップ２０４において、プロセス・フローが終了する。

【００２０】

通知を受け取ったときに無線装置１００がアクティブなものとして登録されていなかった場合は、無線装置１００と無線通信することはできない。それにより、セキュリティ・プロトコルの開始は、後の時間まで遅延される。図３は、セキュリティ・プロトコルを後で開始する例示的なフローチャート３００を示す。フローチャート３００は、ユーザが、無線装置１００が盗まれているかまたは権限なく使用されていることを既に通信してあり、ＳＣＰ／ＨＬＲまたは別の適切なデータベースが適切に更新されていると仮定している。

【００２１】

フローチャート３００のステップ３０１で、無線装置１００の電源が投入される。この時点で、無線装置１００は、例えばＲＡＭ１０８の初期化、様々な構成要素の検査や、オペレーティング・システム１０３のロード等の通常の起動手順を開始する。さらに、無線装置１００は、ＭＩＮやＥＳＮ等を伝えることによりローカル・ネットワークに登録を試みる（ステップ３０２）。ローカル・ネットワークは、受け取った情報をＳＣＰ／ＨＬＲに転送する（ステップ３０３）。ＳＣＰ／ＨＬＲは、データベース探索動作を実行し、無線装置１００が盗まれているかまたは権限なく使用されていることを判定する（ステップ３０４）。ＳＣＰ／ＨＬＲは、ローカル・ネットワークを介して、「セキュリティ・プロト

コル開始」メッセージを無線装置１００に送る（ステップ３０５）。ステップ３０６において、プロセス・フローが終了する。

【００２２】

本発明の実施形態は、公衆セルラ・ネットワークと関連付けられたメッセージプロトコルを利用するセキュリティ・プロトコル１１０を開始するように動作可能であるが、本発明は、そのようなプロトコルに限定されない。例えば、無線通信は、ＳＣＰ／ＨＬＲを介して検証アルゴリズムを実施しない（例えば、ＩＥＥＥ８０２．１１ｂやブルートゥース・ネットワーク等の）専用無線通信ネットワークを介して行われる。

【００２３】

それゆえに、図４は、無線装置１００を識別するときにＥＳＮ／ＭＩＮプロトコルに依存しないセキュリティ・プロトコル１１０の初期化を示す例示的なフローチャート４００を表す。ステップ４０１において、無線装置１００は、無線ネットワーク・アクセス・ポイントを検出する。無線装置１００は、適切な無線通信プロトコルにしたがって無線ネットワークに入る（ステップ４０２）。ステップ４０３において、無線装置１００は、インターネットを介して通信するために、無線ネットワークと関連付けられた動的ホスト構成プロトコル（ＤＨＣＰ）サーバからインターネット・プロトコル（ＩＰ）アドレスを取得する。ステップ４０４において、無線装置１００は、無線装置１０９を、紛失したか、置き忘れたか、返却されていないか、盗まれたか、または権限なく使用されている可能性があるかどうかを判定する（例えば、ウェブ・サーバ等の）データベースに自動的に登録する。登録メッセージは、無線装置１００のＩＰアドレスをデータベースに伝える。さらに、登録メッセージは、無線装置１００に関連付けられた（例えば、媒体アクセス・コントロール（ＭＡＣ）識別子等の）固有の識別子を通信することがある。ステップ４０５において、無線装置１００を、紛失したか、置き忘れたか、返却されていないか、盗まれたか、または権限なく使用されている可能性があると仮定して、無線装置１００は、データベースから「セキュリティ・プロトコル開始」データベースを受け取る。ステップ４０６において、プロセス・フローが終了する。

【００２４】

図５は、本発明の実施形態によるセキュリティ・プロトコル１１０を実施するステップを示す例示的なフローチャート５００を示す。ステップ５０１では、無線装置１００が「セキュリティ・プロトコル開始」メッセージを受け取ることによりフローチャート５００が始まる（図２のステップ２０３と、図３のステップ３０５と、図４のステップ４０５とを参照のこと）。このメッセージは、無線通信サブシステム１０１を介して受け取った入力無線データにおいて識別される。ステップ５０２において、オペレーティング・システム１０３は、「セキュリティ・プロトコル開始」メッセージに応じてセキュリティ・プロトコル１１０を呼び出す。

【００２５】

ステップ５０３において、セキュリティ・プロトコル１１０は、不揮発性メモリ１０６に「盗難」状態を書き込むことが好ましい。この状態は、不揮発性メモリ１０６に書き込まれるので、無許可のユーザが、無線装置１００をリセットしてセキュリティ手段を欺くことは簡単にはできない。具体的には、無線装置１００がリセットされるときに、ＢＩＯＳ１０５が動作する。ＢＩＯＳ１０５は、不揮発性メモリ１０６にアクセスし、無線装置１００の状態を検証することができる。不揮発性メモリ１０６が、装置を紛失したか、置き忘れたか、返却されないか、盗まれたか、または権限なく使用されていることを示す場合には、ＢＩＯＳ１０５が、無許可のユーザがユーザ・データにアクセスしたり、ユーザ・アプリケーション１０７を開始したりするのを防止する保護モードでオペレーティング・システム１０３を起動する。代わりに、ＢＩＯＳ１０５は、無線装置１００を起動させることなく単に動作を停止することができる。

【００２６】

ステップ５０４において、セキュリティ・プロトコル１１０は、例えばオペレーティング・システム１０３に関連付けられた適切なプロセス管理ＡＰＩ呼び出しを実行することに

よって、ユーザ・アプリケーション１０７を終了させることが好ましい。ステップ５０５において、セキュリティ・プロトコル１１０は、例えばパスワードをユーザ・データ・ファイルと関連付けることにより、ユーザ・データへのアクセスを防ぐためにユーザ・データをロックすることが好ましい。ステップ５０６において、セキュリティ・プロトコル１１０は、ユーザ・インタフェース１０９上に適切なメッセージを表示する。例えば、セキュリティ・プロトコル１１０は、「装置がなくされたか盗まれました。１－８００－ＸＸＸ－ＸＸＸＸに電話してください」と表示する。装置を紛失しただけで良心的な人に発見された場合には、その人が、１－８００－電話番号に電話して、適切な仲介人を介して無線装置をその所有者に返せるようにすることができる。

【００２７】

セキュリティ・プロトコル１１０の実行後に無線装置１００が再起動またはリセットされた場合には、前に述べたように、オペレーティング・システム１０３は、ユーザ・アプリケーション１０７の実行またはユーザ・データへのアクセスを許可しない。しかしながら、無線装置１００が、いくつかの最小限の機能を実行できるようにすることが好ましい。例えば、オペレーティング・システム１０３は、ユーザ・インタフェース１０９に適切なメッセージを表示することが好ましい。さらに、オペレーティング・システム１０３は、正当な所有者が適切なパスワードを入力して無線装置１００の動作の復元を可能にするプロンプトの提示することができる。さらに、いくつかの操作を許可することによって、無線装置１００は、最小限の無線通信を実行することができる。無線装置１００が、適切な権限によって無線装置１００を探すことができる無線通信を自発的に実行できるようにすることが望ましい。

【００２８】

本発明の実施形態は、いくつかの利点を提供する。まず、本発明の実施形態は、無線ネットワークへの無線機能付き装置のアクセスを防止するだけではない。それよりもむしろ、本発明の実施形態は、無許可のユーザが、ユーザ・アプリケーションの実行等の無線装置の他の価値ある機能を利用するのを防止する。さらに、本発明の実施形態は、無許可のユーザが、セキュリティ手段を欺くのを防止する。具体的には、無線装置１００の状態は、不揮発性メモリ１０６に維持されることが好ましい。その結果、各起動プロセス後に、ＢＩＯＳ１０５とオペレーティング・システム１０３とがその状態情報を利用して、無線装置１００の動作を制限することができる。さらに、オペレーティング・システム１０３およびＢＩＯＳ１０５は、セキュリティ機能を回避する実行可能命令の修正を防止するように実現されることが好ましい。

【図面の簡単な説明】

【図１】本発明の実施形態を実現することができる例示的な無線装置のブロック図である。

【図２】本発明の実施形態によるセキュリティ・プロトコルを開始する例示的なステップのフローチャートである。

【図３】本発明の実施形態によるセキュリティ・プロトコルを開始するもう１つの例示的なステップのフローチャートである。

【図４】本発明の実施形態によるセキュリティ・プロトコルを開始するもう１つの例示的なステップのフローチャートである。

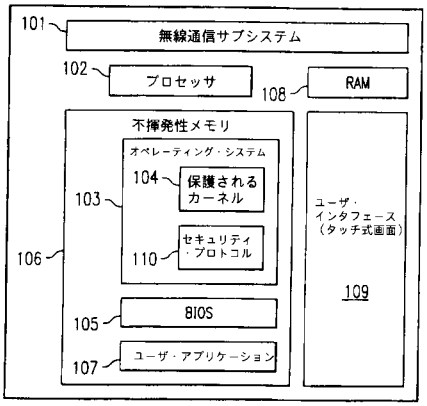
【図５】本発明の実施形態による無線装置への無許可のアクセスを防ぐセキュリティ・プロトコルを実行する例示的なステップのフローチャートである。

【符号の説明】

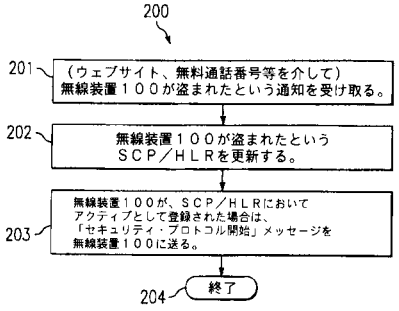
１０１　無線通信サブシステム
１０２　プロセッサ
１０５　基本入出力システム
１０６　不揮発性メモリ
１０７　ユーザ・アプリケーション
１０９　表示装置

１１０　セキュリティ・プロトコル・プロセス

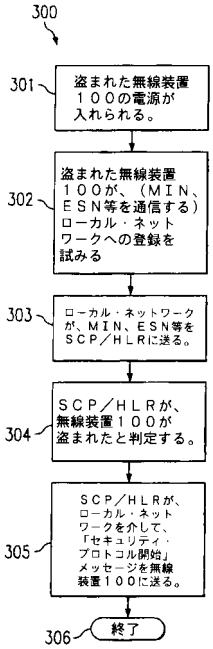
【図１】



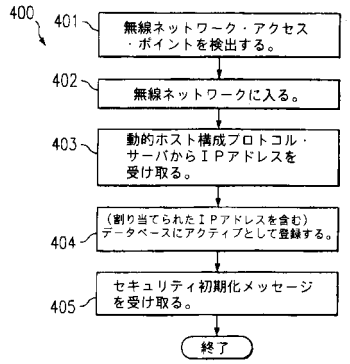
【図２】



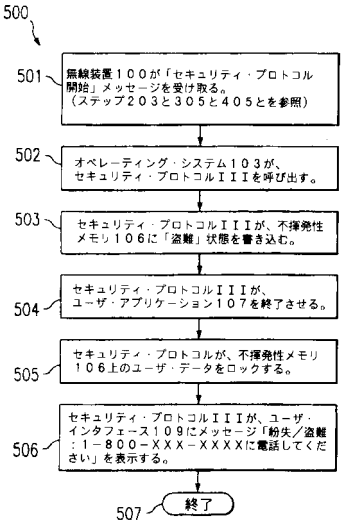
【図３】



【図４】


400
401
無線ネットワーク・アクセス・ポイントを検出する。
402
無線ネットワークに入る。
403
動的ホスト構成プロトコル・サーバからＩＰアドレスを受け取る。
404
（割り当てられたＩＰアドレスを含む）データベースにアクティブとして登録する。
405
セキュリティ初期化メッセージを受け取る。
終了

【図５】


500
501
無線装置１００が「セキュリティ・プロトコル開始」メッセージを受け取る。（ステップ２０３と３０５と４０５とを参照）
502
オペレーティング・システム１０３が、セキュリティ・プロトコルＩＩＩを呼び出す。
503
セキュリティ・プロトコルＩＩＩが、不揮発性メモリ１０６に「盗難」状態を書き込む。
504
セキュリティ・プロトコルＩＩＩが、ユーザ・アプリケーション１０７を終了させる。
505
セキュリティ・プロトコルが、不揮発性メモリ１０６上のユーザ・データをロックする。
506
セキュリティ・プロトコルＩＩＩが、ユーザ・インタフェース１０９にメッセージ「紛失／盗難：１－８００－ＸＸＸ－ＸＸＸＸに電話してください」を表示する。
507
終了

フロントページの続き

(72)発明者　トム・ハワード
アメリカ合衆国コロラド州８０５２６，フォート・コリンズ，ブランボウドライブ　２９４２
(72)発明者　ティム・ゴールドスタイン
アメリカ合衆国コロラド州８０５３８，ラブランド，パロヴェルデ・ドライブ　９２６

審査官　久松　和之

(56)参考文献　特開平０７－１９３８６５（ＪＰ，Ａ）
特開平０９－２１５０５７（ＪＰ，Ａ）
特開２００１－３４６２５７（ＪＰ，Ａ）
特開２０００－１０５７４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04Q　7/00　-　7/38
G06F　21/22