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

特許第4923143号
(P4923143)

(45)発行日　平成24年4月25日(2012.4.25)　(24)登録日　平成24年2月10日(2012.2.10)

(51)Int.Cl.		F I		
H04M 11/00	(2006.01)	H04M	11/00	302
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 92/08	(2009.01)	H04Q	7/00	684
H04M 1/00	(2006.01)	H04M	1/00	R

請求項の数 20　(全 15 頁)

(21)出願番号	特願2010-522893 (P2010-522893)
(86)(22)出願日	平成20年7月25日 (2008.7.25)
(65)公表番号	特表2010-539741 (P2010-539741A)
(43)公表日	平成22年12月16日 (2010.12.16)
(86)国際出願番号	PCT/US2008/009009
(87)国際公開番号	WO2009/029156
(87)国際公開日	平成21年3月5日 (2009.3.5)
審査請求日	平成22年4月30日 (2010.4.30)
(31)優先権主張番号	11/849,286
(32)優先日	平成19年9月1日 (2007.9.1)
(33)優先権主張国	米国(US)

(73)特許権者　503260918
アップル　インコーポレイテッド
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　インフィニット　ループ　１
(74)代理人　100092093
弁理士　辻居　幸一
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100109070
弁理士　須田　洋之

最終頁に続く

(54)【発明の名称】サービスプロバイダ起動

(57)【特許請求の範囲】

【請求項１】

装置上で実行されるモバイル機器を起動する方法であって、前記方法は、

挿入中のＳＩＭカードを有するモバイル機器から起動リクエストを発行し、前記起動リクエストは、前記モバイル機器を一意的に識別するデータと前記挿入中のＳＩＭカードを一意的に識別するデータとを含むものであり、

前記モバイル機器のデータと前記ＳＩＭカードのデータとを含む署名された起動レコードを前記モバイル機器内に記憶し、前記起動レコードは、前記起動リクエストを受けて、起動サーバによって生成されかつ署名されたものであり、

前記挿入中のＳＩＭカードについて前記起動レコードを検証し、

前記起動レコードの検証が成功した後、前記モバイル機器を通信ネットワークに登録することを特徴とする方法。

【請求項２】

前記モバイル機器を一意的に識別する前記データは、前記モバイル機器のシリアル番号を含む請求項１記載の方法。

【請求項３】

前記モバイル機器のシリアル番号は、前記モバイル機器に符号化された国際モバイル機器識別番号（ＩＭＥＩ）である請求項２記載の方法。

【請求項４】

前記モバイル機器を一意的に識別するデータは、前記モバイル機器のハードウェア指紋

を含む請求項１記載の方法。
【請求項５】
前記モバイル機器のハードウェア指紋は、乱数と組み合わされて、前記モバイル機器のベースバンド構成部品のシリアル番号、前記モバイル機器のメモリ構成部品のシリアル番号、前記モバイル機器のシリアル番号のうち少なくとも１つから得られる請求項４記載の方法。
【請求項６】
前記ＳＩＭカードを一意的に識別するデータは、前記ＳＩＭカードのシリアル番号を含む請求項１記載の方法。
【請求項７】
前記ＳＩＭカードを一意的に識別するデータは、前記ＳＩＭカードと関係する加入者識別番号を含む請求項１記載の方法。
【請求項８】
前記ＳＩＭカードと関係する加入者識別番号は、前記ＳＩＭカードを使用する権限を有する加入者を示す国際モバイル加入者識別番号（ＩＭＳＩ）である請求項７記載の方法。
【請求項９】
前記モバイル機器内に記憶される前記起動レコードは、さらに、起動パブリックキーを含み、前記起動レコードは、前記起動パブリックキーに対応する起動プライベートキーを使用して、前記起動サーバによって署名される請求項１記載の方法。
【請求項１０】
前記モバイル機器内に記憶される前記起動レコードの検証は、さらに、前記モバイル機器のハードウェア指紋から得られる機器難読化キーと、共通難読化キーとを使用して、前記起動レコードの内容を解読することを含む請求項１記載の方法。
【請求項１１】
前記モバイル機器内に記憶される前記起動レコードの検証は、さらに、前記起動レコードに含まれる起動パブリックキーを有効にすることを含む請求項１記載の方法。
【請求項１２】
前記モバイル機器内に記憶される前記起動レコードの検証は、さらに、有効にされた前記起動パブリックキーを使用して、前記モバイル機器内に記憶される前記起動レコードの署名を有効にすることを含む請求項１１記載の方法。
【請求項１３】
前記モバイル機器内に記憶される前記起動レコードの検証は、さらに、最大再試行カウンタが最大回数に達していないことを検証することを含む請求項１記載の方法。
【請求項１４】
さらに、前記起動レコードの検証が成功しなかったとき、最大再試行カウンタをインクリメントすることを含む請求項１記載の方法。
【請求項１５】
プログラム命令が記録された装置読み取り可能な記録媒体であって、
前記プログラム命令が実行されるとき、データプロセッシングシステムが、請求項１～１４のいずれか１項に記載の方法を実行することを特徴とする記録媒体。
【請求項１６】
挿入中のＳＩＭカードを有するモバイル機器から起動リクエストを発行する手段であって、前記起動リクエストは、前記モバイル機器を一意的に識別するデータと前記挿入中のＳＩＭカードを一意的に識別するデータとを含む、前記手段と、
前記モバイル機器のデータと前記ＳＩＭカードのデータとを含む署名された起動レコードを前記モバイル機器内に記憶する手段であって、前記起動レコードは、前記起動リクエストを受けて、起動サーバによって生成されかつ署名される、前記手段と、
前記挿入中のＳＩＭカードについて前記起動レコードを検証する手段と、
前記起動レコードの検証が成功した後、前記モバイル機器を通信ネットワークに登録する手段と、を有することを特徴とするデータプロセッシングシステム。

【請求項１７】
前記モバイル機器内に記憶される前記起動レコードは、さらに、起動パブリックキーを含み、前記起動レコードは、前記起動パブリックキーに対応する起動プライベートキーを使用して、前記起動サーバによって署名される請求項１６記載のシステム。
【請求項１８】
前記モバイル機器内に記憶される前記起動レコードを検証する手段は、さらに、前記モバイル機器のハードウェア指紋から得られる機器難読化キーと、共通難読化キーとを使用して、前記起動レコードの内容を解読する手段を有する請求項１６記載のシステム。
【請求項１９】
前記モバイル機器内に記憶される前記起動レコードを検証する手段は、さらに、前記起動レコードに含まれる起動パブリックキーを有効にする手段を有する請求項１６記載のシステム。
【請求項２０】
前記モバイル機器内に記憶される前記起動レコードを検証する手段は、さらに、最大再試行カウンタが最大回数に達していないことを検証する手段を有する請求項１６記載のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
グローバル・システム・フォー・モバイル・コミュニケーションズ（ＧＳＭ）デジタル携帯電話技術とともに使用されるために製造されるモバイル機器は、任意のモバイル通信ネットワーク・サービスプロバイダとともに動作するように設計される。その機器は、ＳＩＭカードと称される加入者識別モジュール（ＳＩＭ）の使用を必要とするが、これは、加入者のサービスプロバイダ・ネットワークにサインオン（Sign on）するために、ＧＳＭ機器に挿入されなければならない。ＳＩＭカードは、とりわけ、ＳＩＭカードの使用が許されるサービスプロバイダを識別する識別番号を含む小さい回路基板である。一般的に、ＡＴ＆Ｔ、Ｖｅｒｉｚｏｎのような各サービスプロバイダは、それらのネットワークで使用するためのＳＩＭカード識別番号の個別の範囲が割り当てられる。
【０００２】
多くのＧＳＭは、特定のサービスプロバイダ用のＳＩＭカードへ機器を制限するサービスプロバイダ・ロック（lock）を備えて製造される。例えば、ＡＴ＆Ｔサービスプロバイダによって市場化されているノキアによって製造されるモバイル機器は、ＡＴ＆Ｔネットワークで使用するために割り当てられたＳＩＭカード識別番号の範囲内にある識別番号で符号化されたＳＩＭカードへ、その機器を制限するロックを備えている。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
サービスプロバイダ・ロックを実行する方法は、製造業者によって様々である。サービスプロバイダ・ロックを備えて機器が製造されたとき、そのロックは、通常、その機器内に記憶された、またはアルゴリズムを使用して導き出されたコードに基づいている。しかし、機器が、ロックを外され、他のサービスプロバイダ用に割り当てられた識別番号を有するＳＩＭカードで使用されるように、コードおよび／またはアルゴリズムが漏洩するかもしれない。機器が、たぶん、それらのネットワークでもはや使用されなくなるので、その結果、元のサービスプロバイダの収益の損失となる。
【０００４】
ＧＳＭ機器の製造業者の観点からみると、サービスプロバイダ・ロックを備えた機器の製造上の障害がある。例えば、ロックするコードおよび／またはアルゴリズムは、サービスプロバイダによって変わるので、特定のサービスプロバイダ・ロックを備えた機器の製造は、異なるサービスプロバイダ用に製造されたモバイル機器用の異なる部品番号（part number）を維持する製造業者を必要とする。このことは、著しい在庫管理コストの増加

とともに、機器の製造の論理上の複雑さを増加させることになるであろう。

【０００５】

消費者の立場からすると、多くの人は、１つの特定のサービスプロバイダに制限されることなく、モバイル機器を自由に購入できることを望むであろう。例えば、海外旅行や国内の様々な場所を旅行するときに、異なるサービスプロバイダへ切り替えることが望ましいであろう。

【課題を解決するための手段】

【０００６】

モバイル機器におけるサービスプロバイダ起動の方法及びシステムが説明される。

【０００７】

本発明の一態様によると、モバイル機器は、特定のサービスプロバイダ用に起動されるまで、限られたサービスモードで動作する。モバイル機器は、サービスプロバイダ・サインプロセス(signing process)の使用を通じて、起動の準備がされ、続いて、サービスプロバイダ起動プロセス（activation process）の使用を通じて、特定のサービスプロバイダ用に起動される。サービスプロバイダ・サインプロセスおよび起動プロセスは、本発明の実施形態によって実施される。

【０００８】

本発明の一態様によると、サービスプロバイダ・サインプロセスは、機器と、サインプロセス中に機器内に挿入されるＳＩＭカードの両方からの情報を安全に組み込む、機器上に記憶されるべき起動チケット（activation ticket）を発生することによって、機器の起動の準備をする。

【０００９】

本発明の別の態様によると、サービスプロバイダ起動プロセスは、そのサービスプロバイダのネットワーク上で使用するために機器を起動するのに先立って、機器上に以前に記憶された起動チケットが真正なものであるか、機器と、機器内に挿入中のＳＩＭカードの両方に関連するものであるかを検証する。

【００１０】

本発明の一態様によると、機器内に新しいＳＩＭカードが挿入されたとき、または、機器がリブート（re-boot）されたとき、挿入中のＳＩＭカードで識別されたサービスプロバイダで使用できるように機器を起動するために、サービスプロバイダ・サインプロセスおよび起動プロセスが必要に応じて繰り返される。例えば、挿入中のＳＩＭカードが、機器内への以前の挿入中にサインプロセスがすでに行われているとき、機器の起動のために起動プロセスのみが必要である。ＳＩＭカードが、機器にとって新しいとき（すなわち、サインプロセスも起動プロセスも、この機器上でまだ実行されていない）、サービスプロバイダで使用できるように機器を起動するために、サインプロセスと起動プロセスが繰り返される。

【００１１】

本発明の一態様によると、サービスプロバイダ・サインプロセスは、２つ以上の起動チケットを機器上に記憶するような、異なるＳＩＭカード用に繰り返される。機器上に記憶された起動チケットのそれぞれは、サインプロセス中に機器内に挿入されたＳＩＭカードのうちの１つに対応している。このようにして、モバイル機器は、サインプロセス中に使用された異なるＳＩＭカードに対応する異なるサービスプロバイダで、起動の準備がされる（それらのサービスプロバイダの加入者アカウントが、起動時にまだ有効である限り）。

【００１２】

本発明の一態様によると、サービスプロバイダ・サインプロセスは、機器と、機器内に挿入中のＳＩＭカードの両方から情報がまとめられる起動リクエストの生成を含む。まとめられる情報は、特に、機器内に挿入中のＳＩＭカードの集積回路カードＩＤ（ＩＣＣＩＤ）および国際モバイル加入者識別番号（ＩＭＳＩ）、機器上で符号化された国際モバイル機器識別番号（ＩＭＥＩ）、機器のハードウェア指紋を含む。

【００１３】
本発明の一態様によると、サービスプロバイダ・サインプロセスは、さらに、起動サーバ内で起動リクエストを受信することを含むが、ここで、起動リクエストは、通常、機器と通信中の起動クライアントを介して起動サーバへ中継される。起動サーバは、起動リクエスト内にまとめられた情報に基づいて起動チケットを生成する。サービスプロバイダ用のバックエンドサーバと通信している起動サーバは、ＩＭＳＩ内で特定された加入者が有効アカウントと関連しているかどうかを最初に検証する。いくつかの実施形態では、機器のＩＭＥＩに基づいて、ＩＭＳＩで特定されるモバイル国コード（ＭＣＣ）およびモバイルネットワークコード（ＭＮＣ）が機器の期待される流通経路に適合するかどうかの確認のようなことも含めて、起動チケットを生成するかどうかを管理する他の方針決定を起動サーバが実行する。

【００１４】
本発明の一態様によると、サインプロセスの間、起動サーバ上に記憶された、または起動サーバからアクセス可能な起動プライベートキーを使用して、起動サーバが、サインされた（signed）起動チケットを生成する。生成された起動チケットは、起動リクエスト内へまとめられた情報ばかりでなく、チケットの署名を有効にするのに機器上で後に使用される起動パブリックキーも含んでフォーマット化される。さらに安全な方法として、機器へ起動チケットを送信する前の暗号化によって起動チケットの内容が秘密にされる。暗号化は、機器と起動サーバの両方に記憶された、または機器と起動サーバの両方からアクセス可能な機器ごとのシメトリックキー（symmetric key）を使用して実行される。このキーは、共通難読化キー（shared obfuscation key）と称される。

【００１５】
本発明の一態様によると、サインプロセスの最後に、通常、機器と通信している起動クライアントを介して、起動サーバからの生成された起動チケットが機器内で受信される。機器は、後のサービスプロバイダ起動プロセス中に使用する起動チケットを記憶する。

【００１６】
本発明の一態様によると、サービスプロバイダ起動プロセスは、スタートアップで挿入中のＳＩＭカードのＩＣＣＩＤを照会し、この値を、起動チケットがこのＳＩＭカード用に前もって記憶されているかどうかを確認するのに使用する。もしそうであれば、サービスプロバイダ起動プロセスは、共通難読化キーを使用して起動チケットを復号化することや、起動サーバによってチケット内の供給されたパブリック起動キーを有効化することや、起動チケットの署名を有効にするために有効化されたキーを使用することを含めて（これに限定されるものではないが）、起動チケットを検証するために、機器内にコマンドを発行する。

【００１７】
本発明の一態様によると、サービスプロバイダ起動プロセスは、ＩＭＥＩおよびハードウェア指紋が機器内のそれらと適合しているかどうか、ＩＣＣＩＤおよびＩＭＳＩが挿入中のＳＩＭカード内のそれらと適合しているかどうかを検証することを含めて、機器と、機器に挿入中のＳＩＭカードに対して、起動チケットの内容を検証する。もし、機器およびＳＩＭカードが適合するものとして、起動チケットの内容が検証されない場合、起動チケットは無効であるものとして処理され、機器は、サービスプロバイダのネットワーク用に起動されない。もし、起動チケットの内容が検証された場合、機器は、サービスプロバイダのネットワーク用に起動される。

【００１８】
本発明は、実施例によって説明され、類似の参照符号が類似の要素を示している添付図面の形態に限定されない。

【図面の簡単な説明】

【００１９】
【図１】本発明の一実施形態によるサービスプロバイダ起動システムの概略構成を示すブロック図である。

【図２】本発明の一実施形態によるモバイル機器の選択された構成部品の概略を示すブロック図である。
【図３】本発明の一実施形態によるサービスプロバイダ起動システムの概略を示すブロック図である。
【図４】本発明の一実施形態によるサービスプロバイダ・サインプロセスの方法の実施の一態様を示すフロー図である。
【図５Ａ】本発明の一実施形態によるサービスプロバイダ起動プロセスの方法の実施の一態様を示すフロー図である。
【図５Ｂ】本発明の一実施形態によるサービスプロバイダ起動プロセスの方法の実施の一態様を示すフロー図である。
【図６】これに制限されるものではないが、起動クライアント、起動サーバ、およびモバイル通信ネットワークのサービスプロバイダの他のバックエンドサーバのような構成部品を含む、本発明の一実施形態に従いサービスプロバイダ起動システムの一構成部品が実装される、多目的コンピュータの一実施形態の概略を示すブロック図である。
【発明を実施するための形態】
【００２０】
本発明の実施形態は、以下の多くの記載を参照して説明され、図面は詳細な実施形態を示す。そのようなものとして、以下の記載および図面は、本発明の例示的実施形態であり、本発明を限定するものとして解釈されるものではない。多くの詳細情報は、本発明の十分な理解を提供するために記載されている。しかし、場合によっては、本発明が不必要に不明瞭とならないように、周知または従来の詳細は記述されない。
【００２１】
記述は、グラフィカル・ユーザインターフェイス・イメージの描写のようなコピーライトによって保護されるものを含むかもしれない。本発明の譲受人を含むコピーライトの所有者は、これらの資料内のコピーライトを含んで彼らの権利を留保する。コピーライトの所有者は、特許庁におけるファイリングまたは登録にみられるような特許ドキュメントまたは特許開示のいずれかによるファクシミリの再生産に対して異議を唱えないが、他の点では、どんなものであれ、すべてのコピーライトを保持する。コピーライト・アップルコンピュータ・インコーポレイテッド、２００７。
【００２２】
図４、図５Ａ、図５Ｂに示される方法の実施など、ここで記載される機能および動作を実施するために、様々な異なるシステム構成が使用される。以下の説明は、このような構成の一例を提供するが、当然のことながら、同等の結果を実現するために他の構成も取り得る。図１に示されるサービスプロバイダ・ロッキング・システム１００は、アップルコンピュータ・インコーポレイテッドによって販売されているアイフォーン（iPhone）機器と、アイフォーン機器と、アイフォーン機器が使用されるモバイル通信ネットワークとに関連するバックエンド・クライアントおよびサーバと、に基づく一例である。しかし、当然のことながら、アーキテクチャ１００は、変わり得るし、アイフォーン機器と関連しないモバイル通信ネットワークと他の機器がさらに使用され得る。アーキテクチャ１００は、アイフォーン機器のようなモバイル機器１０２、モバイル機器１０２に挿入される１つまたはそれ以上のＳＩＭカード１０４を含んでいる。ＳＩＭカード１０４は、機器が、ＳＩＭカード１０４および／または機器１０２の１つと関係があるサービスプロバイダによって操作されるモバイル通信ネットワーク１１８に登録し、それを使用することを可能にする。
【００２３】
モバイル機器１０２は、さらに、機器１０２が接続されているパーソナルコンピュータ(ＰＣ)１０６または他の種類のコンピューティング機器上で動作する起動クライアント１０８と通信を行う。起動クライアント１０８は、一般的にネットワーク１１６を介して１つまたはそれ以上の起動サーバ１１０と通信を行っている。ネットワーク１１６は、起動クライアント１０８・起動サーバ１１０間の通信が伝送される任意のプライベートまたは

パブリックなインターネットワークまたは他の種類の通信経路である。起動サーバ１１０は、同様に、モバイル通信ネットワーク１１８に登録してそれを使用することが許されている機器と加入者に関する情報を含んでいるサービスプロバイダ・データベース１１４と、サービスプロバイダのバックエンドサーバ１１２と通信を行っている。

【００２４】

図２は、本発明の一実施形態によるモバイル機器１００の選択された構成部品２００の概略を示すブロック図である。モバイル機器１００は、本発明の一実施形態によるサービスプロバイダ起動システムのいくつかの機能を実行するのに使用されるアプリケーションプロセッサ（ＡＰ）２０２を含んでいる。ＡＰ２０２は、一般的に、ベースバンド（ＢＢ）２０４集積回路と連携して動作するファームウェアとして実現される。特に、ＢＢ２０４は、モバイル機器の機能が実行されるオペレーティングシステム・プラットフォームを提供する。典型的な実施形態では、ＢＢ２０４は、モバイル機器を一意的に識別する記憶されたＩＭＥＩ２０６と、共通難読化キー（shared obfuscation key）２０８とを含んでいる。これの使用方法については、後述の起動チケットプロセスを参照して詳細に説明する。さらに、機器１００は、詳細については後述するが、特に、サービスプロバイダ起動システムで使用される起動チケットの記憶に使用される揮発性メモリおよび不揮発性メモリの両方を含むメモリ構成部品２１０を含んでいる。

【００２５】

さらに、モバイル機器１００は、ＳＩＭカード２１２が挿入されるＳＩＭカードスロットを備えている。ＳＩＭカード２１２は、ＳＩＭカード２１２を一意的に識別するＩＣＣＩＤ２１４と、加入者を示すＩＭＳＩ２１６とを含んでもよい。そして、これは、機器が使用されるべきモバイル通信ネットワーク１１８の準備（provision）に使用される。

【００２６】

図３は、本発明の一実施形態によるサービスプロバイダ起動システムの概略を示すブロック図である。図に示すように、ＢＢ２９４およびＡＰ２０８を有するモバイル機器に、ＳＩＭカードＡ３０２Ａ、ＳＩＭカードＢ３０２Ｂ、ＳＩＭカードＣ３０２Ｃの３つのＳＩＭカード３０２の１つが挿入される。当然のことながら、機器１００は、多くのＳＩＭカードのうちいずれかとともに使用され、３つのＳＩＭカードは一例として示したものにすぎない。

【００２７】

一実施形態において、モバイル機器１００は、サービスプロバイダ・ロックなしで製造されることを意味する「ジェネリック(generic)」機器である。サービスプロバイダ・ロックなしの機器は、ＳＩＭカードＡ，Ｂ，Ｃ（３０２Ａ，Ｂ，Ｃ）のうちいずれかとともに使用可能である。他の実施形態において、モバイル機器１００は、最初にアンロックしなければＳＩＭカードＡ，Ｂ，Ｃとともに使用できないように、前もってロックされる。一度、機器１００がアンロックされると、緊急呼び出し（emergency calls）でのみ使用可能であり、サービスプロバイダ・ネットワーク上で未だ起動されていないことを意味する、限られたサービスモードでのみ、一般的に動作が可能である。

【００２８】

一実施形態において、ＳＩＭカードＡ，Ｂ，Ｃ（３０２）のうちの１つの挿入が検出されたとき、または、ＢＢ２０４がブートしたとき、ＡＰ２０８が、挿入されたＳＩＭカードＡ，Ｂ，Ｃに関する、すでに記憶された起動チケット３０８があるかどうかを確認する。もし、なければ、ＡＰ２０８は、起動サーバ１１０へ起動リクエスト３０４を発行することにより、サインプロセスを開始する。起動リクエスト３０４は、機器１００、挿入中のＳＩＭカード３０２からの情報を有しており、例えば、ＩＭＥＩ２０６、ＩＭＳＩ２１６、ＩＣＣＩＤ２１４の値を含み、起動リクエスト３０４の中にまとめられている。

【００２９】

一実施形態において、起動リクエスト３０４を受け取ると、起動サーバ１１０は、起動リクエスト３０４の中にまとめられた情報に基づいて、起動チケット３０６を生成すべきかどうかを確認する。図４を参照して詳細に後述するが、起動チケット３０６は、チケッ

ト・ジェネレータ・ロジック３１０および起動パブリック／プライベート・キーペア３１２を使用して、機器１００および挿入中のＳＩＭカードＡ，Ｂ，Ｃの両方からの識別情報を取り込む。

【００３０】

典型的な実施形態において、起動チケット３０６を生成すべきかどうかの確認は、少なくとも部分的には、起動リクエスト３０４の中にまとめられたＩＭＳＩ２１６がサービスプロバイダの通信ネットワーク１１８上で起動可能であることを、サービスプロバイダ・サーバ１１２および／またはサービスプロバイダ・データベース１１４が、示すかどうかに依存する。いくつかの実施形態において、起動チケットを生成すべきかどうかの決定は、所定のＩＭＥＩ／ＩＣＣＩＤペア用の起動チケット３０６を生成すべきかどうかなど他の方針検討に依存するであろう（起動リクエスト３０４の中にまとめられたＩＭＥＩ／ＩＣＣＩＤを使用して）。もし、起動サーバ１１０が、起動チケット３０６を生成することができないことを確認した場合、起動リクエスト３０４は失敗となるであろう。

【００３１】

一実施形態において、一度、起動チケット３０６が生成されると、起動サーバ１１０は、起動チケットの内容を保護するため、機器１００へ起動チケットを返信する前に、起動チケット３０６の内容を難読化する。一実施形態において、起動チケット３０６は、機器ごとのシメトリックキーで暗号化することによって、難読化される。機器ごとのシメトリックキーは、機器１００の個別のデータと、機器と起動サーバ１１０との間で共通のキーから得られる。共通キーは、図示した例では、機器１００上の共通難読化キー２０８と称されており、また、起動サーバ１１０上で定義されるキー３１２の１つとして記憶される。一例として、機器ごとのシメトリックキーは、機器難読化キーと称され、以下のアルゴリズムを使用して、キー３１２内の、機器１００のハードウェア指紋と、サーバ上に記憶された共通難読化キーを使用して得られる。

機器難読化キー＝ＳＨＡ－１（ハードウェア指紋｜｜共通難読化キー）

【００３２】

起動チケット３０６が生成されて暗号化された後、起動チケット３０６は、機器１００へ送り返される状態になり、その機器１００では、前に記憶された他の起動チケット３０８とともに起動チケット３０６が記憶される。図５Ａ～図５Ｂを参照して詳細を説明するが、記憶された起動チケット３０８Ａ，Ｂ，Ｃは、起動プロセスを開始するため、ＡＰ２０８によって後で使用される。

【００３３】

一実施形態において、表１に、起動チケット３０６／３０８のフォーマットを示す。表２に、起動チケットに含まれる起動パブリックキーのフォーマットを示す。

【表１】

名称	サイズ(8ビットバイト)	符号化
バージョン	1	BCD
起動パブリックキー	N	パブリックキー
ICCID	10	BCD
IMSI	8	BCD
IMEI	8	BCD
ハードウェア指紋	20	2進数
チケット署名	キー長/8	2進数

表１－起動チケットのフォーマット

【表２】

名称	サイズ(8ビットバイト)	符号化
レコード長	4	2進数
シリアル番号	4	2進数
キー長	4	2進数
指数	4	2進数
モジュラス	キー長/8	2進数
モンゴメリ・ファクタ	キー長/8	2進数
キー署名	Mキー長/8	2進数

表2－起動パブリックキーのフォーマット

【００３４】

一実施形態において、起動チケット３０６／３０８のバージョン・フィールドは、上位互換性のある起動チケットの処理を可能にする。一実施形態において、符号化された整数バージョンは、古い起動チケットを認識するため、またはそれらをサポートするため、機器１００における将来のファームウェアのリリースを可能にする。また、バージョンは、改変されないことを検証するため、起動チケットの要約内に含まれる。一実施形態において、ＢＢ２０４は、起動チケットのフォーマットが漏洩したときのロールバックアタック（rollback attack）を防止することができる、その中に編集された最小レコードバージョンを有するであろう。

【００３５】

一実施形態において、起動チケット３０６／３０８の起動パブリックキー・フィールドは、表２に示すようにフォーマットされる。しかし、注目すべきは、他のパブリックキー・フォーマットは、その後の特許請求の範囲から逸脱することなく採用され得るということである。

【００３６】

ＩＣＣＩＤ（集積回路カードＩＤ）は、２桁の主産業識別番号（ＳＩＭでは８９）、１～３桁の国コード（ＩＴＵ－ＴＥ．１６４）、発行ネットワークのＭＮＣを通常含む１～４桁（国コード長に依存する）の発行者識別コード、個人アカウント識別番号、および１桁のチェックサム（checksum）から成るＩＳＯ／ＩＥＣ７８１２－１で規定された２０桁の数字である。

【００３７】

ＩＭＳＩ（国際モバイル加入者識別番号）は、３桁のモバイル国コード（ＭＭＣ）、２または３桁のモバイルネットワークコード（ＭＮＣ）、および９または１０桁のモバイル加入者識別番号（ＭＳＩＮ）から成る３ＧＰＰ　ＴＳ　２３．００３で規定された１５桁の数字である。

【００３８】

一実施形態において、ハードウェア指紋は、所定の乱数系列（random sequence）がプラスされた、機器のハードウェア構成部品のシリアル番号、およびＩＭＥＩなど、通常、機器特有のデータから得られる値である。例えば、一実施形態において、指紋は、以下のように計算される。

ハードウェア指紋＝ＳＨＡ－１（ＳＧｏｌｄ－シリアル番号｜｜Ｆｌａｓｈシリアル番号｜｜ＩＭＥＩ｜｜Ｓａｌｔ）

ここで、Ｓａｌｔは、乱数系列である。

【００３９】

一実施形態において、チケット署名は、以下のように生成される。

メッセージ＝バージョン｜｜ＩＣＣＩＤ｜｜ＩＭＳＩ｜｜ＩＭＥＩ｜｜ハードウェア指紋
ハッシュ＝ＳＨＡ－１（メッセージ）
符号化メッセージ＝０ｘ００｜｜０ｘ０４｜｜ＰａｄｄｉｎｇＳｔｒｉｎｇ｜｜０ｘ００｜｜ハッシュ
チケット署名＝ＲＳＡ暗号化（起動プライベートキー，符号化メッセージ）

【００４０】

注目すべきは、表１に示した起動チケット３０６／３０８の記載されたフォーマットは、使用されるフォーマットの一例に過ぎず、それ以後の特許請求の範囲から逸脱することなく、他のフォーマットおよびデータフィールドが起動チケットを構成し得るということである。

【００４１】

図４、図５Ａおよび図５Ｂは、本発明の一実施形態によるサービスプロバイダ起動の一態様を示すフロー図である。図４において、サービスプロバイダ・サインプロセス４００の方法が示されている。実施される方法４００は、ベースバンド・ブートまたは新しいＳＩＭカードの挿入を機器１００が検出するブロック４０２から始まる。ブロック４０４で、方法４００は、ＩＭＳＩ、ＩＣＣＩＤ、ＩＭＥＩおよびハードウェア指紋を起動リクエストの中にまとめ、機器から起動サーバへ起動リクエストを送信する。ブロック４０６で、起動サーバが起動リクエストを受信し、所定の方針検討に基づいて起動リクエストに応答して起動チケットを生成すべきかどうかを確認する（例えば、サービスプロバイダと関係のあるバックエンドサーバが、サービスプロバイダの通信ネットワークでＩＭＳＩ情報が有効であることを確認する）。

【００４２】

一実施形態において、処理ブロック４０８で、方法４００は、起動リクエストの中にまとめられたＩＣＣＩＤ、ＩＭＳＩ、ＩＭＥＩ、およびハードウェア指紋情報を使用して起動チケットを生成する。一実施形態において、方法４００は、起動チケット内への起動パブリックキーを含み、ブロック４１０で、起動サーバ上に安全に記憶された、対応する起動プライベートキーを使用して起動チケットを署名する。ブロック４１２で、方法４００は、起動リクエスト内のハードウェア指紋のような機器特有の情報から得られた機器の難読化キー、および起動サーバおよび機器の両方で利用可能な共通難読化キーで、内容を暗号化することにより、起動チケットの内容を難読化する。処理ブロック４１４で、方法４００は、記憶用に機器へ起動チケットを送り返すことで終わる。例えば、起動チケットは、機器のベースバンドへアクセス可能な、機器上のメモリ内に記憶される。

【００４３】

図５Ａ、図５Ｂを参照すると、サービスプロバイダ起動プロセス５００の方法が示されている。実施される方法５００は、スタートアップで、挿入中のＳＩＭカードのＩＣＣＩＤを機器１００が問い合わせるブロック５０２から開始される。ブロック５０４で、方法５００は、現在のＩＣＣＩＤに対応する起動チケットを配置するため、ＩＣＣＩＤを使用する。ブロック５０６で、機器は、起動チケットの検証を開始するコマンドを発行する。起動チケットの検証により、機器のベースバンドが制限されたサービスモードから移行し、通信ネットワークに登録される。もし、起動チケットが成功裏に検証できなかった場合、コマンドはエラーコードを返す。

【００４４】

典型的な実施形態において、方法５００は、機器に挿入中のＳＩＭカードがレディ状態（すなわちＳＩＭがアンロックされていないか）にあるかどうかの確認の後、起動チケットの検証を実行する。もし、レディ状態でない場合、方法５００は、ＳＩＭカードが成功裏にアンロックされた後に起動チケットの検証を実施する。

【００４５】

方法５００は、多様な起動チケット検証を実行するため、続いて、処理ブロック５０８Ａ～５０８Ｈを行う。ブロック５０８Ａで、方法５００は、はじめに、再試行回数が超過

していないことを検証する。再試行回数（カウンタ）は、起動チケット検証コマンドを使用して機器上でアンロックしてサービスを起動する試行に失敗したときごとにインクリメントされる。機器を起動する多数の試行が存在するブルートフォースアタック（brute-force attack（強力な攻撃））を防止するため、検証における予め定められた回数のみの試行が許される。

【００４６】

一実施形態において、方法５００は、続いて、ブロック５０８Ｂ／５０８Ｃで、暗号化情報から、起動チケット内のバージョン情報を解析し、検証対象の起動チケット内のバージョンが、機器のベースバンドの現在のバージョンでサポートされているかどうかを確認する。

【００４７】

ブロック５０８Ｄで、方法５００は、機器に記憶された共通難読化キーと、機器のハードウェア指紋のような機器特有の情報から得られる機器難読化キーを使用して起動チケットの内容を解読（復号化）する。ブロック５０８Ｅで、方法５００は、起動チケット内に供給された起動パブリックキーを有効にし、ブロック５０８Ｆで、起動チケットの署名を有効にするのにパブリックキーを使用する。ブロック５０８Ｇ／Ｈで、方法５００は、起動チケットの解読したハッシュ値が、計算されたハッシュ値と一致するかどうかを検証することにより、起動チケット検証プロセスを終了する。一致する場合は、方法は、続いて、処理ブロック５１０を実行する。一致しない場合は、起動チケット検証は、失敗し、方法はブロック５１６へ分岐する。

【００４８】

ブロック５１０で、ある機器からの起動チケットが別の機器上で使用されるのを防止するため、起動チケット内のＩＭＥＩが、機器内に記憶されたＩＭＥＩと比較される。一実施形態において、各ＩＭＥＩの１５桁すべてが一致しなければならない。一致しない場合は、ＢＢ起動チケット。

【００４９】

処理ブロック５１２で、方法５００は、続いて、起動チケットに含まれるハードウェア指紋の値を確認し、それを機器のハードウェア指紋と比較することにより、起動チケットの検証を実行する。それらが一致しない場合、起動チケットは無効として扱われる。

【００５０】

ブロック５１４で、方法５００は、続いて、起動チケットに含まれるＩＣＣＩＤの値を、機器内に挿入中のＳＩＭカードのＩＣＣＩＤと比較することにより、起動チケットの検証を実行する。ＩＣＣＩＤが１０　０ｘＦＦ８ビットで符号化されているときなど、特別な場合、ＩＣＣＩＤ検証は省略される。同様に、ブロック５１６で、方法５００は、続いて、起動チケットに含まれるＩＭＳＩの値を、機器内に挿入中のＳＩＭカードのＩＭＳＩと比較することにより、起動チケットの検証を実行する。再び、ＩＭＳＩが１０　０ｘＦＦ８ビットで符号化されているときなど、特別な場合、ＩＭＳＩ検証は省略される。

【００５１】

ブロック５１６で、方法は、起動チケット検証プロセスのいずれかが失敗というコマンドに応答して、再試行カウンタをインクリメントし、エラーを返す。処理ブロック５１８で、検証プロセスが成功した場合、サービスプロバイダのモバイル通信ネットワーク上への機器の登録を開始することにより、機器は、機器上のサービスを起動することができる。

【００５２】

図６は、モバイル機器のサービス起動を提供するのに使用されるバックエンド・クライアントおよびサーバのような、本発明のいくつかの態様が実施される、一般的なコンピュータシステムの一例を示している。図６は、コンピュータシステムの種々の構成部品を示しているが、ここで留意すべきは、詳細が本発明と関係のないものとして、いずれかの特定の構成または構成部品を相互接続する手段を表すことを意図するものではないということである。また、当然のことながら、より少ない構成部品またはより多くの構成部品を有

するネットワークコンピュータおよび他のデータプロセッシングシステムもまた、本発明で使用される。例えば、図６のコンピュータシステムは、アップルコンピュータ・インコーポレイテッドのマッキントッシュ（登録商標）コンピュータかもしれない。

【００５３】

図６に示すように、データプロセッシングシステムの形態をとるコンピュータシステム６０１は、マイクロプロセッサ６０３およびＲＯＭ（読み出し専用メモリ）６０７および揮発性ＲＡＭ６０５および不揮発性メモリ６０６に接続されたバス６０２を備えている。一実施形態において、マイクロプロセッサ６０３は、モトローラ社のＧ３またはＧ４マイクロプロセッサまたは１つまたはそれ以上のＩＭＢのＧ５マイクロプロセッサかもしれない。バス６０２は、これらの種々の構成部品を相互接続し、またこれらの構成部品６０３，６０７，６０５，６０６を、ディスプレイコントローラおよびディスプレイデバイス６０４、およびネットワークインターフェイス、プリンタおよび本技術分野において周知の他のデバイス等の入力／出力（Ｉ／Ｏ）デバイスのような周辺デバイスに相互接続する。一般に、入力／出力デバイス６０９は、入力／出力コントローラ６０８を介してシステムに接続されている。揮発性ＲＡＭ（ランダムアクセスメモリ）６０５は、一般に、リフレッシュするため、またはメモリ内のデータを維持するために継続的な電力を必要とするダイナミックＲＡＭ（ＤＲＡＭ）として実現される。大容量記憶装置６０６は、一般に、磁気ハードドライブまたは磁気オプティカルドライブまたはオプティカルドライブまたはＤＶＤＲＡＭ、またはシステムから電力を取り除いた後もデータ（例えば、大容量のデータ）を保持する他の種類のメモリシステムである。一般に、大容量記憶装置６０６もまた、必須ではないが、ランダムアクセスメモリである。図６は、データプロセッシングシステムにおいて、大容量記憶装置６０６が、残りの構成部品に直接接続されるローカルデバイスであることを示しているが、当然のことながら、本発明は、モデムまたはイーサネット（登録商標）インターフェイスのようなネットワークインターフェイスを介してデータプロセッシングシステムに接続されたネットワーク記憶装置のような、本システムから離れた不揮発性メモリを用いてもよい。バス６０２は、本技術分野において周知の、種々のブリッジ、コントローラおよび／またはアダプタを介してお互いに接続された１つまたはそれ以上のバスを具備してもよい。一実施形態において、Ｉ／Ｏコントローラ６０８は、ＵＳＢ周辺部品を制御するＵＳＢ（ユニバーサルシリアルバス）アダプタ、およびＩＥＥＥ１３９４規格周辺部品用のＩＥＥＥ１３９４コントローラを具備している。

【００５４】

本発明の態様が少なくとも部分的にソフトウェアで具体化される得ることが、本詳細な説明から明らかであろう。すなわち、ＲＯＭ６０７、ＲＡＭ６０５、大容量記憶装置６０６またはリモート記憶装置などのメモリに含まれる命令シーケンスを実行するマイクロプロセッサのようなコンピュータシステムまたは他のデータプロセッシングシステムで、そのプロセッサに応答して、その技術が実行される。種々の実施形態において、本発明を実現するため、ハードワイヤード（hardwired）回路が、ソフトウェア命令と組み合わされて使用される。したがって、その技術は、ハードウェア回路およびソフトウェアのいずれかの特定の組み合わせに制限されないし、データプロセッシングシステムによって実行される命令のいずれかの特定のソースにも制限されない。さらに、本詳細な説明を通じて、説明を簡潔化するため、種々の機能および動作は、ソフトウェアコードによって（またはそれに起因して）実行されるものとして説明されている。しかし、当業者は、マイクロプロセッサ６０３のようなプロセッサによるコードの実行から生じる機能であるそのような表現が何を意味しているかを認識するであろう。

【図１】

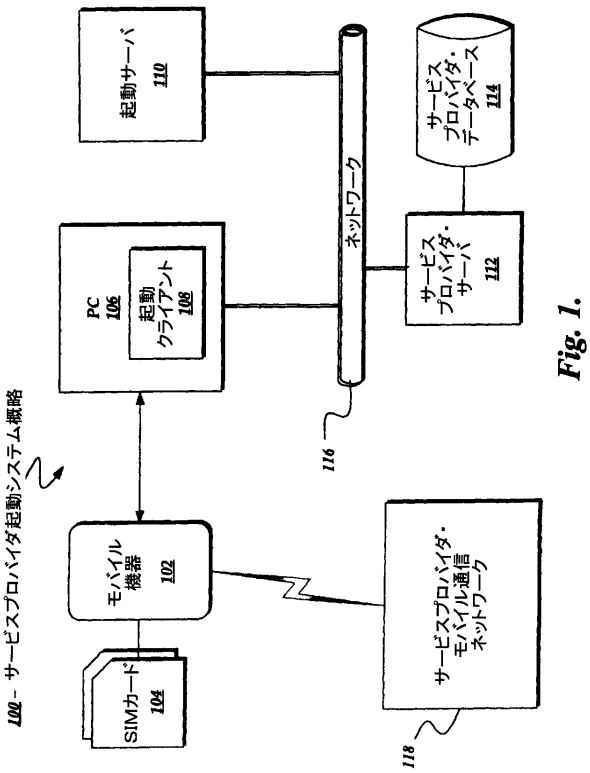

Fig. 1.

【図２】

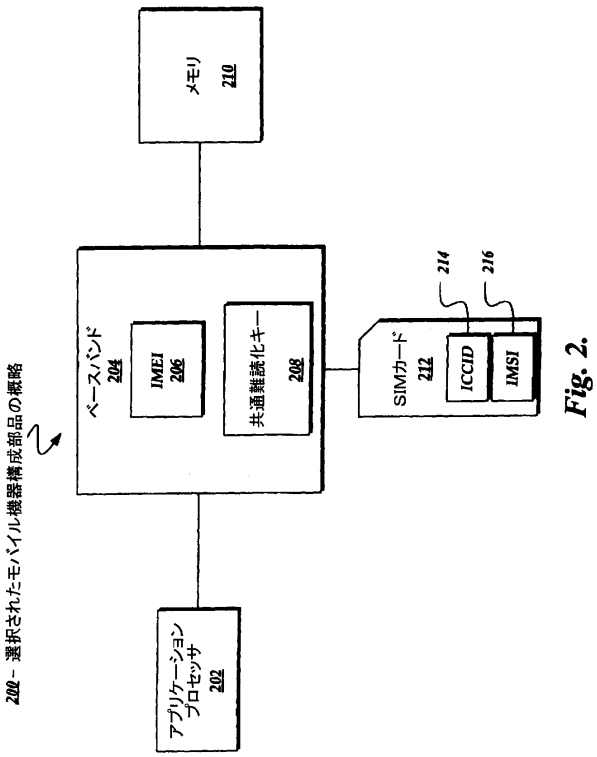

Fig. 2.

【図３】

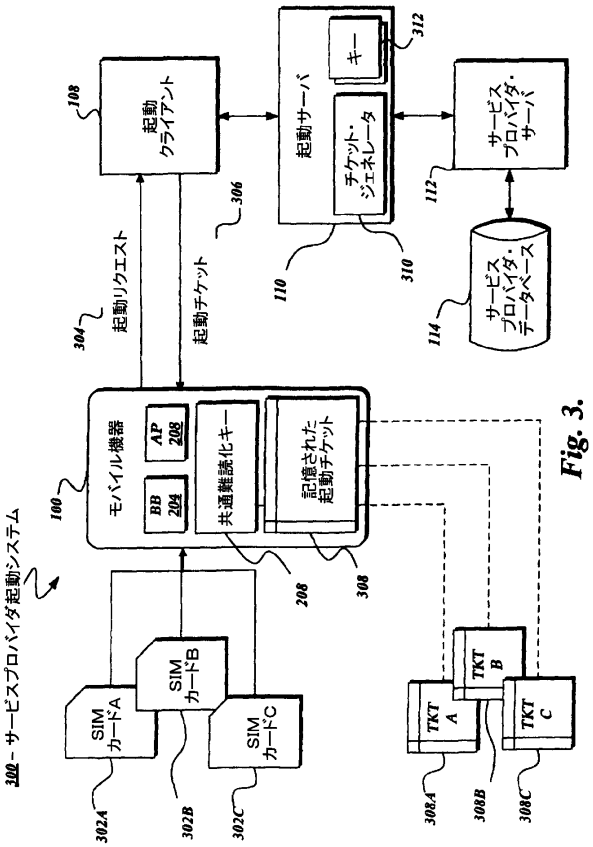

Fig. 3.

【図４】

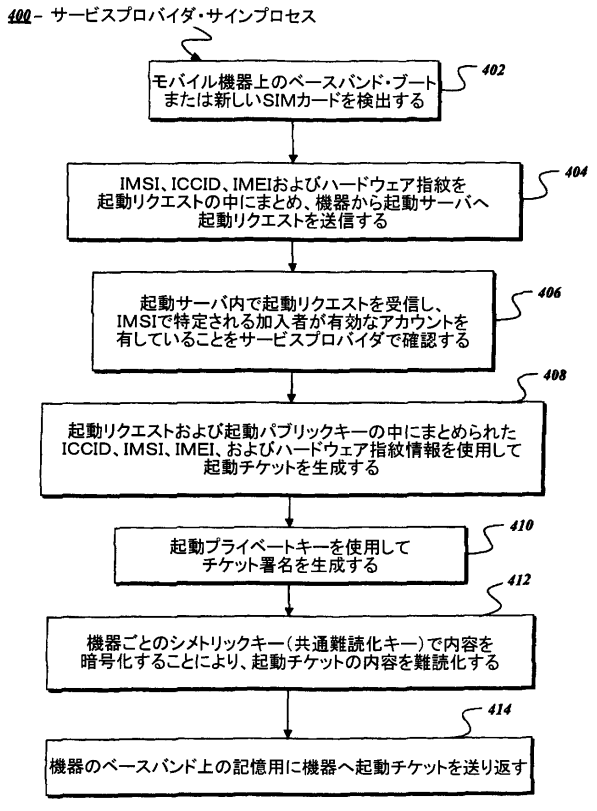

Fig. 4.

【図５Ａ】

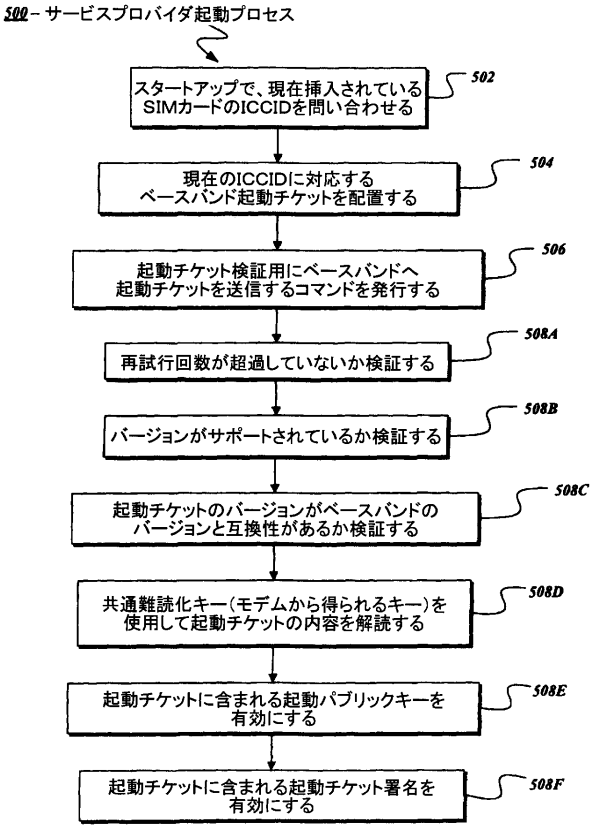

Fig. 5A.

【図５Ｂ】

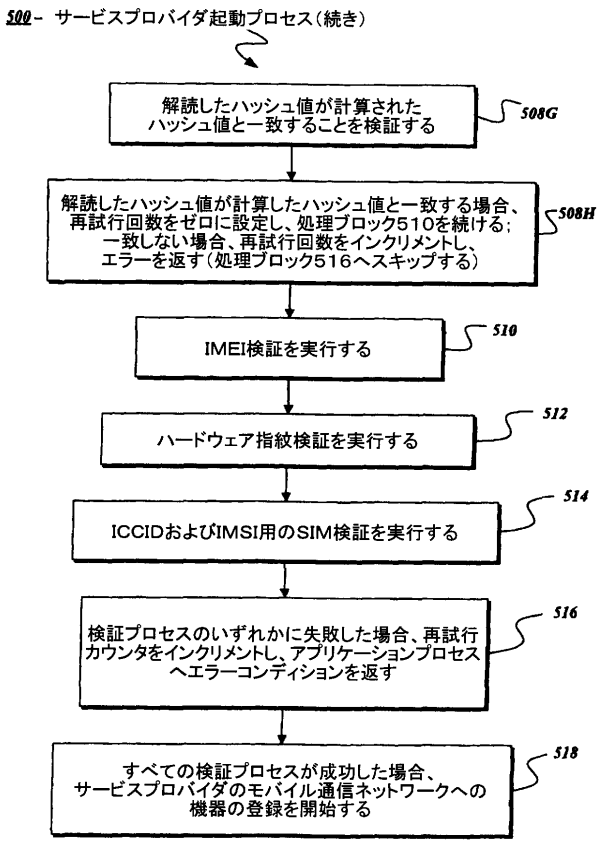

Fig. 5B.

【図６】

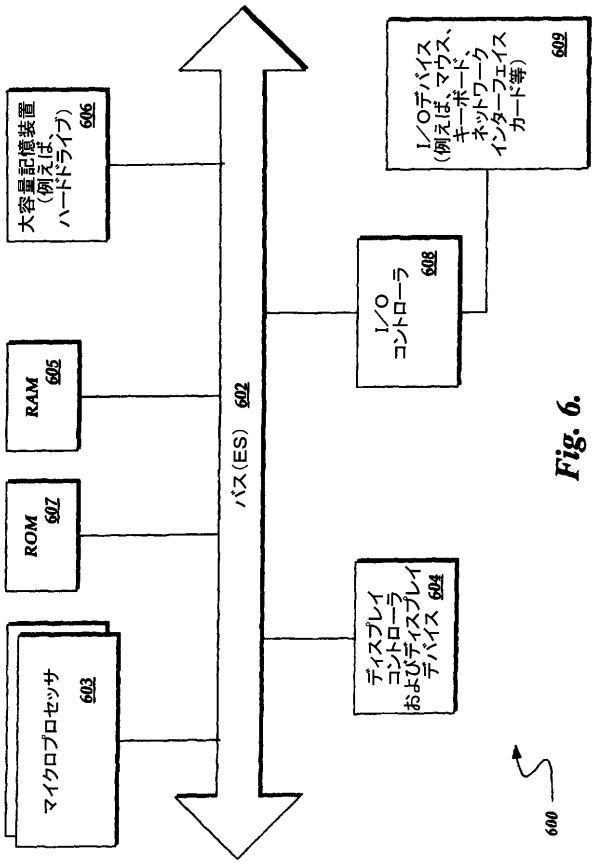

Fig. 6.

フロントページの続き

(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100121979
弁理士 岩崎 吉信
(72)発明者 デ アトレイ ダラス
アメリカ合衆国 カリフォルニア州 ９４１１４ サンフランシスコ セヴンティーンス ストリート ４５０８ ＃２
(72)発明者 ブッシュ ジェフリー
アメリカ合衆国 カリフォルニア州 ９５１１７ サン ホセ リンデンオークス ドライヴ ３２８３
(72)発明者 ホーク ジェリー
アメリカ合衆国 フロリダ州 ３４７８６ ウィンダミア ワイランド コート ９７４０
(72)発明者 フアン ロナルド ケリュアン
アメリカ合衆国 カリフォルニア州 ９５０３５ ミルピタス サンドハースト ドライヴ ４３３
(72)発明者 サティアナサン ブライナード
アメリカ合衆国 カリフォルニア州 ９５１３５ サン ホセ キング エステイツ コート ５３７９

審査官 松元 伸次

(56)参考文献 国際公開第２００６／０３３０８７（WO，Ａ２）
特表２００７－５１２６０２（ＪＰ，Ａ）
特表２００４－５１８３５６（ＪＰ，Ａ）
特表２００６－５２２５１４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B 7/24- 7/26、
H04M 1/00、 1/24- 3/00、 3/16- 3/20、
3/38- 3/58、 7/00- 7/16、
11/00-11/10、99/00、
H04W 4/00-99/00