(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-281861
(P2007-281861A)
(43)公開日　平成19年10月25日(2007.10.25)

(51)Int.Cl.			F I			テーマコード（参考）
H04Q	7/38	(2006.01)	H04B	7/26	109S	5K067
H04M	3/42	(2006.01)	H04M	3/42	E	5K201

審査請求 未請求　請求項の数 6　ＯＬ　（全 11 頁）

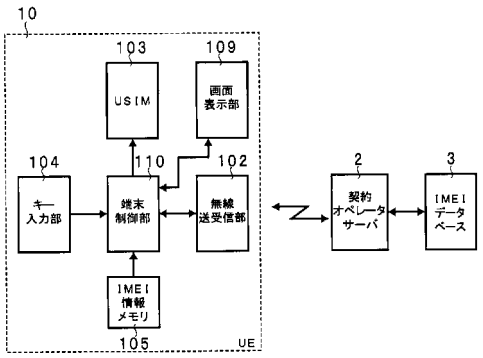
(21)出願番号　特願2006-105115 (P2006-105115)
(22)出願日　平成18年4月6日 (2006.4.6)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100085235
弁理士　松浦　兼行
(72)発明者　山本　晃二
東京都港区芝５丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5K067 AA32 BB04 DD17 EE02 EE16 FF07 HH22 HH23 HH36
5K201 AA09 BC25 BD01 BD10 CB01 CB10 EA07 EC06 ED05 EE05

(54)【発明の名称】端末認証方法及び携帯端末装置

(57)【要約】
【課題】従来の携帯端末装置では、装置内部で端末認証を行っているため、端末内部を解析され認証を改竄されると、契約オペレータ以外でも携帯端末装置が使用可能となってしまう。
【解決手段】携帯電話機１０の契約オペレータサーバ２への接続後、端末制御部１１０は契約オペレータサーバ２に、その端末固有の端末識別番号（ＩＭＥＩ）を送信する。契約オペレータサーバ２は、このＩＭＥＩデータベース３からのＩＭＥＩ情報と、受信した携帯電話機１０からのＩＭＥＩデータとを比較照合し、端末認証結果が一致したときは使用許可信号をネットワーク経由で携帯電話機１０に送信し、端末認証結果が不一致のときは、使用不許可信号をネットワーク経由で携帯電話機１０に送信する。携帯電話機１０は、使用不許可信号を受信すると、端末機能を停止する。
【選択図】図１



【特許請求の範囲】
【請求項１】
携帯端末装置の端末識別番号と、前記携帯端末装置を使用する加入者の加入者情報とを用いて、前記携帯端末装置の使用の可否を決定する端末認証方法であって、
前記携帯端末装置から前記加入者情報を、ネットワークを介して契約オペレータサーバへ送信する第１のステップと、
前記契約オペレータサーバが、受信した前記加入者情報を使用した認証を行い、認証が成功した時のみ前記携帯端末装置との接続を行う第２のステップと、
接続した前記契約オペレータサーバに対して、前記携帯端末装置が予め保持している前記端末識別番号を、前記ネットワークを介して送信する第３のステップと、
前記契約オペレータサーバにより、受信した前記端末識別番号が、予めデータベースに格納されている特定の通信事業者が保有する多数の端末識別番号の中に存在するかどうか判定する認証を行う第４のステップと、
前記第４のステップにより、一致する認証結果が得られたときは、使用許可信号を生成して前記ネットワークを介して前記携帯端末装置へ送信し、不一致の認証結果が得られたときは、使用不許可信号を生成して前記ネットワークを介して前記携帯端末装置へ送信してその携帯端末装置の機能を停止させる第５のステップと
を含むことを特徴とする端末認証方法。
【請求項２】
携帯端末装置の端末識別番号以外の端末製造番号やＲＦ　ＩＤの識別コードなどの所定の端末固有情報と、前記携帯端末装置を使用する加入者の加入者情報とを用いて、前記携帯端末装置の使用の可否を決定する端末認証方法であって、
前記携帯端末装置から前記加入者情報を、ネットワークを介して契約オペレータサーバへ送信する第１のステップと、
前記契約オペレータサーバが、受信した前記加入者情報を使用した認証を行い、認証が成功した時のみ前記携帯端末装置との接続を行う第２のステップと、
接続した前記契約オペレータサーバに対して、前記携帯端末装置が予め保持している一又は二以上の前記所定の端末固有情報を、前記ネットワークを介して送信する第３のステップと、
前記契約オペレータサーバにより、受信した一又は二以上の前記所定の端末固有情報が、予めデータベースに格納されている特定の通信事業者が保有する多数の前記所定の端末固有情報の中にすべて存在するかどうか判定する認証を行う第４のステップと、
前記第４のステップにより、すべて存在する認証結果が得られたときは、使用許可信号を生成して前記ネットワークを介して前記携帯端末装置へ送信し、不一致の認証結果が得られたときは、使用不許可信号を生成して前記ネットワークを介して前記携帯端末装置へ送信してその携帯端末装置の機能を停止させる第５のステップと
を含むことを特徴とする端末認証方法。
【請求項３】
前記加入者情報は、ＵＳＩＭカードから読み出したＵＳＩＭデータ中のＩＭＳＩ情報であることを特徴とする請求項１又は２記載の端末認証方法。
【請求項４】
端末識別番号と加入者情報とを保存しており、ネットワークを介して使用許可又は使用不許可が設定される携帯端末装置であって、
ネットワークへ信号を送信し、前記ネットワークから信号を受信する送受信手段と、
前記端末識別番号を保存する記憶手段と、
前記加入者情報を取得する加入者情報取得手段と、
取得した前記加入者情報を、前記送受信手段により前記ネットワークを介して契約オペレータサーバへ送信し、前記契約オペレータサーバが、受信した前記加入者情報を使用した認証を行い、認証が成功した時に接続される前記契約オペレータサーバに対して、前記記憶手段から前記端末識別番号を読み出して、前記送受信手段により前記ネットワークを

介して送信する送信制御手段と、
前記契約オペレータサーバにより、受信した前記端末識別番号が、予めデータベースに格納されている特定の通信事業者が保有する多数の端末識別番号の中に存在する一致の認証結果が得られたときに生成されて送信される使用許可信号、又は不一致の認証結果が得られたときに生成されて送信される使用不許可信号を、前記契約オペレータサーバから前記ネットワークを介して前記送受信手段により受信し、前記使用許可信号を受信したときは、端末の機能を使用可能に設定し、前記使用不許可信号を受信したときは、端末の機能を使用不可に設定する機能設定手段と
を有することを特徴とする携帯端末装置。
【請求項５】
携帯端末装置の端末識別番号以外の端末製造番号やＲＦ　ＩＤの識別コードなどの所定の端末固有情報と加入者情報とを保存しており、ネットワークを介して使用許可又は使用不許可が設定される携帯端末装置であって、
ネットワークへ信号を送信し、前記ネットワークから信号を受信する送受信手段と、
前記所定の端末固有情報を保存する記憶手段と、
前記加入者情報を取得する加入者情報取得手段と、
取得した前記加入者情報を、前記送受信手段により前記ネットワークを介して契約オペレータサーバへ送信し、前記契約オペレータサーバが、受信した前記加入者情報を使用した認証を行い、認証が成功した時に接続される前記契約オペレータサーバに対して、前記記憶手段から一又は二以上の前記端末固有情報を読み出して、前記送受信手段により前記ネットワークを介して送信する送信制御手段と、
前記契約オペレータサーバにより、受信した一又は二以上の前記端末固有情報が、予めデータベースに格納されている特定の通信事業者が保有する多数の端末固有情報の中にすべて存在する一致の認証結果が得られたときに生成されて送信される使用許可信号、又は不一致の認証結果が得られたときに生成されて送信される使用不許可信号を、前記契約オペレータサーバから前記ネットワークを介して前記送受信手段により受信し、前記使用許可信号を受信したときは、端末の機能を使用可能に設定し、前記使用不許可信号を受信したときは、端末の機能を使用不可に設定する機能設定手段と
を有することを特徴とする携帯端末装置。
【請求項６】
前記加入者情報取得手段は、ＵＳＩＭカードからＵＳＩＭデータを読み出し、読み出した前記ＵＳＩＭデータ中のＩＭＳＩ情報を前記加入者情報として取得するカード読み出し手段であることを特徴とする請求項４又は５記載の携帯端末装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は端末認証方法及び携帯端末装置に係り、特に携帯電話機、ＰＨＳ(Personal Handyphone System)、ＰＤＡ(Personal Data Assistance,Personal Digital Assistants：個人向け携帯型情報通信機器）等の携帯端末装置の端末認証方法及び携帯端末装置に関する。
【背景技術】
【０００２】
図４は従来の携帯端末装置の一例のブロック図を示す。この携帯端末装置１は、端末の制御を行う端末制御部１０１と、無線通信を行う無線送受信部１０２と、ＩＣカードであるＵＳＩＭ(Universal Subscriber Identity Module)カードの情報を読み書きするＵＳＩＭ１０３と、端末にキー入力を行うキー入力部１０４、ＩＭＳＩ(International Mobile Subscriber Identity)情報を保持したＩＭＳＩ情報メモリ１０７と、ＵＳＩＭデータの一部を記憶したＳＩＭ ＬＯＣＫ情報メモリ１０８と、画面表示部１０９とを有する。
【０００３】
端末制御部１０１は、携帯端末装置１のネットワークとの通信制御・認証や端末上のソ

フト等の実行・制御、端末画面表示制御、キー入力制御、ＩＭＳＩ情報制御を司るものであり、無線送受信部１０２、ＵＳＩＭ１０３、キー入力部１０４、ＩＭＳＩ情報メモリ１０７、画面表示部１０９と接続する。無線送受信部１０２は、端末とネットワークの無線通信を行う機能を有し、端末制御部１０１からの信号を変調して無線信号としてネットワークに送出し、ネットワークを介して受信した無線信号を復調しディジタル信号として端末制御部１０１に送出する。

【０００４】

ＵＳＭ１０３はＵＳＩＭカードを実装し、ＵＳＩＭカード内を読み書きする機能を有し、ＵＳＩＭカードから読み出したデータを端末制御部１０１に送出し、端末制御部１０１からのデータをＵＳＩＭカードに書き込みをする。キー入力部１０４は、各種キーからのキー入力を信号に変換し、端末制御部１０１に送出する。ＩＭＳＩ情報メモリ１０７は、加入者の電話番号であるＩＭＳＩ情報を記憶する機能を有し、ＩＭＳＩ情報を端末制御部１０１に送出する。

【０００５】

次に、この従来の携帯端末装置の動作について図５のフローチャートを併せ参照して説明する。携帯端末装置１は電源投入されると、その端末制御部１０１がＵＳＩＭ１０３を用いてＵＳＩＭカードのデータを読み出し、ＳＩＭ ＬＯＣＫ情報メモリ１０８からＵＳＩＭデータの一部を読み出し端末制御部１０１内のメモリに保持する（ステップＳ１１）。

【０００６】

その後、端末制御部１０１は、読み出したＵＳＩＭデータとメモリに保持しておいたＵＳＩＭデータの一部の照合を行い（ステップＳ１２）、端末認証結果が一致するかどうか判定し（ステップＳ１３）、端末認証結果が不一致となる場合には画面表示部１０９に使用不可の画面を表示し（ステップＳ１４）、端末機能を停止し、端末認証結果が一致する場合には、画面表示部１０９に待ち受け画面を表示し端末の使用を許可する（ステップＳ１５）。

【０００７】

このように、従来の携帯端末装置１では、その携帯端末装置１を契約オペレータ以外で使われないように端末の内部にＵＳＩＭ情報の一部を記憶させておき、端末の電源投入時にＳＩＭ ＬＯＣＫ情報メモリ１０８から読み込んだ値との照合を行い、照合結果が一致した場合にのみ携帯端末装置１を使用可能とする端末認証を行い、契約オペレータ以外のＵＳＩＭを使用した場合は、端末使用を不可能としている。

【０００８】

その理由は、携帯端末装置は、携帯端末通信事業者であるオペレータにおいて原価よりも安く販売され、携帯端末装置に付加したサービスを使用してもらうことで費用を回収したり、他のオペレータに無い付加機能を付けることで他オペレータとの差別化を行っているので、他のオペレータでも携帯端末装置が使用されると、付加サービスでの携帯端末装置の費用回収ができず、付加機能での差別化ができなくなり、上記のビジネスモデルが成り立たなくなるからである。しかし、携帯端末装置内部を解析し、上記認証をマスクする改造を行うことで、契約オペレータ以外のＵＳＩＭ以外で使用するケースが現れた。

【０００９】

一方、ディジタルセルラ移動通信システム（ＧＳＭシステム）では、自己が提供する電話サービスの加入者であるか否かを認識するのに、加入者識別カード（ＳＩＭ）を使用することで、ＧＳＭシステムの通信事業者からＳＩＭの発給を受けるだけで、電話サービスを受ける事ができるが、ＳＩＭは１枚しか発給されないため、例えば同一の加入者電話番号を共有する特定のグループ（例えば、家族）では、ＧＳＭシステムの電話サービスを共有できないという課題を解決するため、加入者識別情報と端末識別情報との組み合わせ情報を保持し、ＧＳＭシステムのサービスの提供要求の発生時、この要求に関する組み合わせ情報が保持されているかどうかを判定し、保持されている場合のみ、このサービスを提供する構成とすることにより、同じ加入者識別情報を持つ複数の加入者識別媒体を同時に

使用することを可能にした通信システムが従来提案されている（例えば、特許文献１参照）。

【００１０】

【特許文献１】特開平８－１４０１３６号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

しかし、図４に示した従来の携帯端末装置１では、装置内部で端末認証を行っているため、端末内部を解析され認証を改竄されると、契約オペレータ以外でも携帯端末装置が使用可能となってしまう。

【００１２】

一方、特許文献１の通信システムは、移動電話機は加入者認識カードに格納されている加入者電話番号ＩＭＳＩなどを含む認証登録要求信号を、移動電話交換局に送信し、移動電話機交換局は機器認識番号メモリを検索し、認証登録要求信号に含まれるＩＭＥＩが、自己が認める正規の番号かを判定し、正規の番号であれば移動電話機に登録を許可する旨を通知する構成であるが、このものは一つの加入者情報（ＩＭＳＩ）を複数の移動電話機で同時に使用することを目的としたものであり、契約オペレータ以外の使用を防止することを目的とするものではなく、また、同一の加入者情報（ＩＭＳＩ）と端末識別番号（ＩＭＥＩ）とを用いてホームキャリアを識別することに利用しているが、移動電話機の内部の値を解析して認証を改竄された場合はやはり契約オペレータ以外でも携帯電話機が使用可能となってしまう。

【００１３】

本発明は以上の点に鑑みなされたもので、契約オペレータ以外では端末使用不可能となる端末認証方法及び携帯端末装置を提供することを目的とする。

【課題を解決するための手段】

【００１４】

上記の目的を達成するため、本発明の端末認証方法は、携帯端末装置の端末識別番号と、携帯端末装置を使用する加入者の加入者情報とを用いて、携帯端末装置の使用の可否を決定する端末認証方法であって、携帯端末装置から加入者情報を、ネットワークを介して契約オペレータサーバへ送信する第１のステップと、契約オペレータサーバが、受信した加入者情報を使用した認証を行い、認証が成功した時のみ携帯端末装置との接続を行う第２のステップと、接続した契約オペレータサーバに対して、携帯端末装置が予め保持している端末識別番号を、ネットワークを介して送信する第３のステップと、契約オペレータサーバにより、受信した端末識別番号が、予めデータベースに格納されている特定の通信事業者が保有する多数の端末識別番号の中に存在するかどうか判定する認証を行う第４のステップと、第４のステップにより、一致する認証結果が得られたときは、使用許可信号を生成してネットワークを介して携帯端末装置へ送信し、不一致の認証結果が得られたときは、使用不許可信号を生成してネットワークを介して携帯端末装置へ送信してその携帯端末装置の機能を停止させる第５のステップとを含むことを特徴とする。

【００１５】

この発明では、特定の通信事業者が加入者情報と端末識別番号とを管理している特定の通信事業者が販売した携帯端末装置である場合にのみ、使用許可信号が契約オペレータサーバから携帯端末装置に送信され、それ以外の場合は使用不許可信号が契約オペレータサーバから携帯端末装置に送信されて携帯端末装置の使用を不許可とするため、契約オペレータ（特定の通信事業者）以外での携帯端末装置の使用を不可能とすることができる。

【００１６】

また、上記の目的を達成するため、本発明の端末認証方法は、携帯端末装置の端末識別番号以外の端末製造番号やＲＦ　ＩＤの識別コードなどの所定の端末固有情報と、携帯端末装置を使用する加入者の加入者情報とを用いて、携帯端末装置の使用の可否を決定する端末認証方法であって、携帯端末装置から加入者情報を、ネットワークを介して契約オペ

レータサーバへ送信する第１のステップと、契約オペレータサーバが、受信した加入者情報を使用した認証を行い、認証が成功した時のみ携帯端末装置との接続を行う第２のステップと、接続した契約オペレータサーバに対して、携帯端末装置が予め保持している一又は二以上の所定の端末固有情報を、ネットワークを介して送信する第３のステップと、契約オペレータサーバにより、受信した一又は二以上の所定の端末固有情報が、予めデータベースに格納されている特定の通信事業者が保有する多数の所定の端末固有情報の中にすべて存在するかどうか判定する認証を行う第４のステップと、第４のステップにより、すべて存在する認証結果が得られたときは、使用許可信号を生成してネットワークを介して携帯端末装置へ送信し、不一致の認証結果が得られたときは、使用不許可信号を生成してネットワークを介して携帯端末装置へ送信してその携帯端末装置の機能を停止させる第５のステップとを含むことを特徴とする。

【００１７】

この発明では、特定の通信事業者が加入者情報と所定の端末固有情報とを管理している特定の通信事業者が販売した携帯端末装置である場合にのみ、使用許可信号が契約オペレータサーバから携帯端末装置に送信され、それ以外の場合は使用不許可信号が契約オペレータサーバから携帯端末装置に送信されて携帯端末装置の使用を不許可とするため、契約オペレータ（特定の通信事業者）以外での携帯端末装置の使用を不可能とすることができる。

【００１８】

また、上記の目的を達成するため、本発明の携帯端末装置は、端末識別番号と加入者情報とを保存しており、ネットワークを介して使用許可又は使用不許可が設定される携帯端末装置であって、ネットワークへ信号を送信し、ネットワークから信号を受信する送受信手段と、端末識別番号を保存する記憶手段と、加入者情報を取得する加入者情報取得手段と、取得した加入者情報を、送受信手段によりネットワークを介して契約オペレータサーバへ送信し、契約オペレータサーバが、受信した加入者情報を使用した認証を行い、認証が成功した時に接続される契約オペレータサーバに対して、記憶手段から端末識別番号を読み出して、送受信手段によりネットワークを介して送信する送信制御手段と、契約オペレータサーバにより、受信した端末識別番号が、予めデータベースに格納されている特定の通信事業者が保有する多数の端末識別番号の中に存在する一致の認証結果が得られたときに生成されて送信される使用許可信号、又は不一致の認証結果が得られたときに生成されて送信される使用不許可信号を、契約オペレータサーバからネットワークを介して送受信手段により受信し、使用許可信号を受信したときは、端末の機能を使用可能に設定し、使用不許可信号を受信したときは、端末の機能を使用不可に設定する機能設定手段とを有することを特徴とする。

【００１９】

この発明では、特定の通信事業者が加入者情報と端末識別番号とを管理している特定の通信事業者が販売した携帯端末装置である場合にのみ、一致の認証結果が得られて使用許可信号を生成し、それ以外の場合は使用不許可信号を生成する端末認証を契約オペレータサーバが行うようにしたため、携帯端末装置は認証機能を有しないようにできる。

【００２０】

また、上記の目的を達成するため、本発明の携帯端末装置は、携帯端末装置の端末識別番号以外の端末製造番号やＲＦ　ＩＤの識別コードなどの所定の端末固有情報と加入者情報とを保存しており、ネットワークを介して使用許可又は使用不許可が設定される携帯端末装置であって、ネットワークへ信号を送信し、ネットワークから信号を受信する送受信手段と、所定の端末固有情報を保存する記憶手段と、加入者情報を取得する加入者情報取得手段と、取得した加入者情報を、送受信手段によりネットワークを介して契約オペレータサーバへ送信し、契約オペレータサーバが、受信した加入者情報を使用した認証を行い、認証が成功した時に接続される契約オペレータサーバに対して、記憶手段から一又は二以上の端末固有情報を読み出して、送受信手段によりネットワークを介して送信する送信制御手段と、契約オペレータサーバにより、受信した一又は二以上の端末固有情報が、予

めデータベースに格納されている特定の通信事業者が保有する多数の端末固有情報の中にすべて存在する一致の認証結果が得られたときに生成されて送信される使用許可信号、又は不一致の認証結果が得られたときに生成されて送信される使用不許可信号を、契約オペレータサーバからネットワークを介して送受信手段により受信し、使用許可信号を受信したときは、端末の機能を使用可能に設定し、使用不許可信号を受信したときは、端末の機能を使用不可に設定する機能設定手段とを有することを特徴とする。

【００２１】

この発明では、特定の通信事業者が加入者情報と所定の端末固有情報とを管理している特定の通信事業者が販売した携帯端末装置である場合にのみ、一致の認証結果が得られて使用許可信号を生成し、それ以外の場合は使用不許可信号を生成する端末認証を契約オペレータサーバが行うようにしたため、携帯端末装置は認証機能を有しないようにできる。

【発明の効果】

【００２２】

本発明によれば、特定の通信事業者が加入者情報と端末識別番号とを管理している特定の通信事業者が販売した携帯端末装置である場合にのみ、使用許可信号が契約オペレータサーバから携帯端末装置に送信され、それ以外の場合は使用不許可信号が契約オペレータサーバから携帯端末装置に送信されて携帯端末装置の使用を不許可とすることにより、契約オペレータ（特定の通信事業者）以外での携帯端末装置の使用を不可能とするようにしたため、特定の通信事業者と他の通信事業者との間の差別化ができ、通信費の費用回収などが可能にできる。

【００２３】

また、本発明によれば、端末認証をネットワーク経由にて契約オペレータサーバで行い、携帯端末装置は認証機能を有しないようにすることで、携帯端末装置で解析を行っても端末認証方法を特定することができないようにしたため、携帯端末装置の改造による不正な端末認証を行うことができず、特定の通信事業者以外の携帯端末装置の使用を不可能にできる。

【発明を実施するための最良の形態】

【００２４】

次に、本発明の実施の形態について図面と共に説明する。図１は本発明になる携帯端末装置の第１の実施の形態のブロック図を示す。同図において、携帯端末装置の一例としての携帯電話機１０は、契約オペレータサーバ２に端末識別番号（ＩＭＥＩ）を送信する。契約オペレータサーバ２は、携帯電話機１０から送信された端末ＩＭＥＩと、ＩＭＥＩデータベース３からのＩＭＥＩデータとから携帯電話機１０の契約者のＩＭＥＩを照合する端末認証と、加入者情報の認証とをそれぞれ行い、得られた認証結果を携帯電話機１０に送信する。携帯電話機１０は、受信した認証結果が認証成功を示す場合にのみ起動し、認証失敗では使用付加とする機能を有する。

【００２５】

図１において、図４と同一構成部分には同一符号を付してあり、携帯電話機１０は、当該電話機（以下端末ともいう）の制御を統括的に行う端末制御部１１０と、図示しない最寄りの基地局との間で無線通信を行う無線送受信部１０２と、ＵＳＩＭカードの情報を読み書きするリーダ／ライタであるＵＳＩＭ１０３と、端末制御部１１０に各種の情報をキーを用いて入力するキー入力部１０４と、端末識別番号であるＩＭＥＩ情報を予め保持しているＩＭＥＩ情報メモリ１０５と、画面表示部１０９とを有する。

【００２６】

端末制御部１１０は、携帯電話機１０のネットワークとの通信制御・認証や端末上のソフトウェア等の実行・制御、端末画面表示制御、キー入力制御、ＩＭＳＩ、ＩＭＥＩ情報制御を司るものであり、無線送受信部１０２、ＵＳＩＭ１０３、キー入力部１０４、ＩＭＥＩ情報メモリ１０５、画面表示部１０９と接続している。

【００２７】

無線送受信部１０２は、最寄りの基地局を介して携帯電話機１０とネットワークの無線

通信を行う機能を有し、端末制御部１１０からの信号を変調して無線信号としてネットワーク上の基地局に送出し、ネットワーク上の基地局からの無線信号を受信して復調しディジタル信号として端末制御部１１０に送出する。

【００２８】

ＵＳＭ１０３はＵＳＩＭカードを実装し、ＵＳＩＭカード内を読み書きする機能を有し、ＵＳＩＭカードから読み出したＵＳＩＭデータを端末制御部１１０に送出し、端末制御部１１０からのデータをＵＳＩＭカードに書き込みをする。キー入力部１０４は、各種キーからのキー入力を信号に変換し、端末制御部１１０に送出する。ＩＭＥＩ情報メモリ１０５は、製造時に付与された固有の端末識別番号（ＩＭＥＩ）を予め記憶する機能を有し、記憶している端末識別番号（ＩＭＥＩ）を端末制御部１１０に送出する。

【００２９】

契約オペレータサーバ２は、加入者情報であるＩＭＳＩ(International Mobile Subscriber Identity)による契約者認証と、携帯電話機１０から送信されたＩＭＥＩ情報とＩＭＥＩデータベース３からのＩＭＥＩデータとを照合する認証とを行い、それらの認証結果を携帯電話機１０に送出する機能を有する。ＩＭＥＩデータベース３は、オペレータに契約している全携帯端末装置（ここでは携帯電話機）のＩＭＥＩデータを予め保持している。

【００３０】

次に、本実施の形態の端末認証動作について、図２のフローチャートを併せ参照して説明する。図１の携帯電話機１０の電源が投入されると、端末制御部１１０はＵＳＩＭ１０３に挿入されているＵＳＩＭカードからＵＳＩＭデータを読み出し、読み出したＵＳＩＭデータ中の加入者情報（ＩＭＳＩ）を端末制御部１１０内のメモリに一旦保持する（ステップＳ１）。

【００３１】

その後、端末制御部１１０は、無線送受信部１０２を用いてバンドサーチを行い、サーチしたセルに、内部のメモリに保持した上記のＩＭＳＩを用いて、無線送受信部１０２を介して契約オペレータサーバ（ＯＰサーバ）２に接続する（ステップＳ２）。このとき、契約オペレータサーバ２は受信した上記のＩＭＳＩが、その契約オペレータサーバ２の電話事業者（キャリア）の加入者情報であるかどうかの第１の認証を行い、その認証が成功した時のみ、携帯電話機１０の契約オペレータサーバ２への接続を許可する。

【００３２】

携帯電話機１０の契約オペレータサーバ２への接続後、端末制御部１１０は契約オペレータサーバ２に、ＩＭＥＩ情報メモリ１０５から読み出した、その端末固有の端末識別番号（ＩＭＥＩ）を、無線送受信部１０２を通して送信する。

【００３３】

ＩＭＥＩデータベース３には、契約オペレータサーバ２の電話事業者（キャリア）が販売した全携帯電話機の端末識別番号（ＩＭＥＩ）が予め格納されており、キャリアにて管理されている。契約オペレータサーバ２は、このＩＭＥＩデータベース３に格納されているＩＭＥＩ情報と、受信した携帯電話機（ＵＥ）１０からのＩＭＥＩデータとを比較照合する第２の認証である端末認証を行う（ステップＳ３、Ｓ４）。

【００３４】

受信したＩＭＥＩデータがＩＭＥＩデータベース３のＩＭＥＩ情報中に存在する場合は、契約オペレータサーバ２は、端末認証結果が一致（成功）と判定して、使用許可信号をネットワーク経由で携帯電話機１０に送信する（ステップＳ５）。携帯電話機１０は、無線送受信部１０２により上記の使用許可信号を受信すると、端末制御部１１０が画面表示部１０９に待ち受け画面を表示させ、端末の使用を許可する（ステップＳ６）。

【００３５】

一方、受信したＩＭＥＩデータがＩＭＥＩデータベース３のＩＭＥＩ情報中に存在しない場合は、契約オペレータサーバ２は、端末認証結果が不一致（失敗）と判定して、使用不許可信号をネットワーク経由で携帯電話機１０に送信する（ステップＳ７）。携帯電話

機１０は、無線送受信部１０２により上記の使用不許可信号を受信すると、端末制御部１１０が画面表示部１０９に使用不可の画面を表示させると共に、端末機能を停止する（ステップＳ８）。ここでの端末使用不可により停止される機能は、携帯電話機１０の単独の機能（例えば、電話帳、カメラなど携帯電話機単体でも使用できる機能）である。

【００３６】

このように、本実施の形態によれば、電話事業者（キャリア）が管理する既知の加入者情報（ＩＭＳＩ）と、端末識別番号（ＩＭＥＩ）とを利用してそれぞれ認証を行い、両者の認証が共に一致（成功）したときには、携帯電話機１０はキャリアが販売した携帯電話機であり、かつ、キャリアの加入者であると、契約オペレータサーバ２が判断して使用許可を与え、それ以外の場合は契約オペレータサーバ２が携帯電話機１０の機能を停止するため、たとえ、携帯電話機の内部を解析し、どのキャリアでも使用可能とする改造を行ったとしても、契約オペレータサーバ２のキャリアのＵＳＩＭ以外では使用できず、上記の改造携帯電話機の使用を停止させることができる。

【００３７】

次に、本発明の第２の実施の形態について説明する。図３は本発明になる携帯端末装置の第２の実施の形態のブロック図を示す。同図中、図１と同一構成部分には同一符号を付し、その説明を省略する。図３に示す実施の形態は、携帯端末装置の一例としての携帯電話機１１が、端末固有情報メモリ１０６を有し、端末制御部１１１が第１の実施の形態のＩＭＥＩ情報に替えて端末固有情報を、契約オペレータサーバ２へ送信する点に特徴がある。ここで、上記の端末固有情報としては、携帯電話機の製造番号やＲＦ　ＩＤの識別コードなどである。

【００３８】

一方、端末固有データベース４には、契約オペレータサーバ２の電話事業者（キャリア）が管理する全携帯電話機の端末固有情報が予め保持されている。これにより、本実施の形態では、契約オペレータサーバ２は、携帯電話機１１と接続後、携帯電話機１１から送信された端末固有情報メモリ１０６からの端末固有情報と、端末固有データベース４に格納されている端末固有情報とを比較照合する端末認証を行い、認証結果一致の場合のみ携帯電話機１１へ使用許可信号を送信し、それ以外では使用不許可信号を送信する。なお、この場合の端末認証は、端末固有情報としてＩＭＥＩ以外の一つ又は二つ以上の固有情報を用いて行う。

【図面の簡単な説明】

【００３９】

【図１】本発明の携帯端末装置の第１の実施の形態のブロック図である。

【図２】図１の端末認証動作説明用フローチャートである。

【図３】本発明の携帯端末装置の第２の実施の形態のブロック図である。

【図４】従来の携帯端末装置の一例のブロック図である。

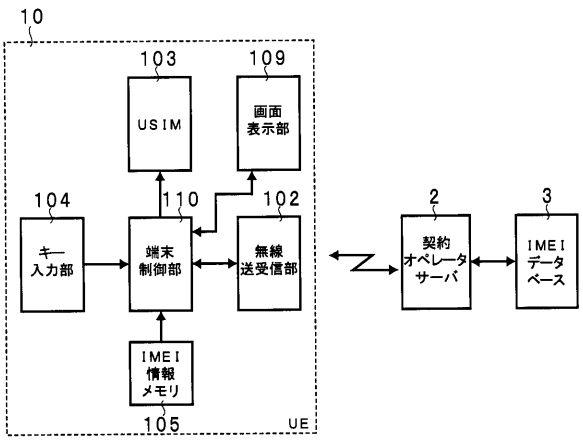
【図５】図４の端末認証動作説明用フローチャートである。

【符号の説明】

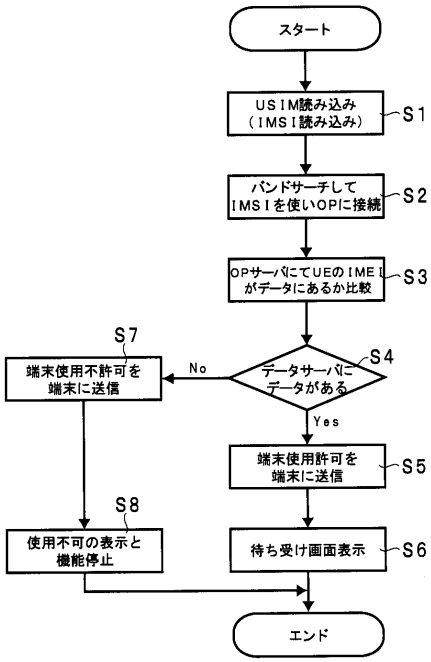
【００４０】

２　契約オペレータサーバ
３　ＩＭＥＩデータベース
４　端末固有データベース
１０、１１　携帯電話機
１０２　無線送受信部
１０３　ＵＳＩＭ
１０４　キー入力部
１０５　ＩＭＥＩ情報メモリ
１０６　端末固有情報メモリ
１０９　画面表示部
１１０、１１１　端末制御部

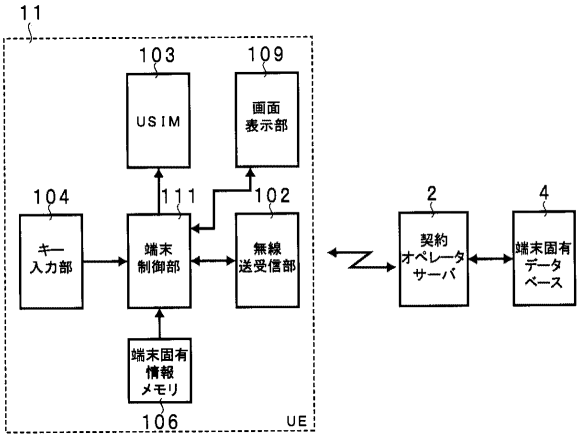
【図１】


10
103
USIM
109
画面
表示部
104
キー
入力部
110
端末
制御部
102
無線
送受信部
2
契約
オペレータ
サーバ
3
IMEI
データ
ベース
IMEI
情報
メモリ
105
UE

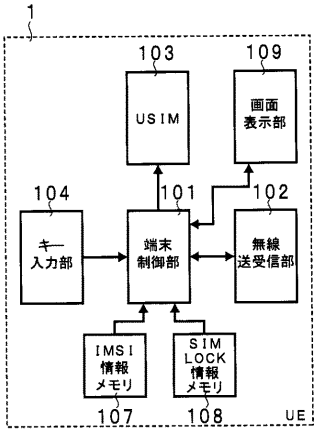
【図２】


スタート
USIM読み込み
（IMSI読み込み）
S1
バンドサーチして
IMSIを使いOPに接続
S2
OPサーバにてUEのIMEI
がデータにあるか比較
S3
S4
データサーバに
データがある
No
Yes
S7
端末使用不許可を
端末に送信
端末使用許可を
端末に送信
S5
S8
使用不可の表示と
機能停止
待ち受け画面表示
S6
エンド

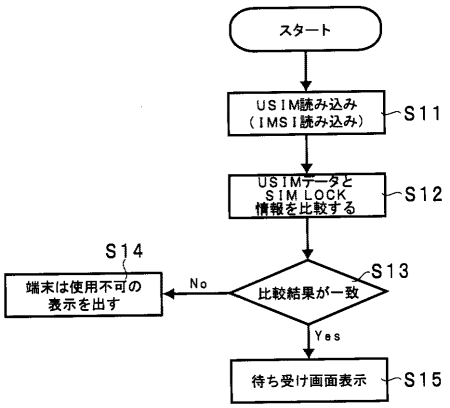
【図３】


11
103
USIM
109
画面
表示部
104
キー
入力部
111
端末
制御部
102
無線
送受信部
2
契約
オペレータ
サーバ
4
端末固有
データ
ベース
端末固有
情報
メモリ
106
UE

【図４】


1
103
USIM
109
画面
表示部
104
キー
入力部
101
端末
制御部
102
無線
送受信部
IMSI
情報
メモリ
107
SIM
LOCK
情報
メモリ
108
UE

【図５】


スタート
USIM読み込み
（IMSI読み込み）
S11
USIMデータと
SIM LOCK
情報を比較する
S12
S14
端末は使用不可の
表示を出す
No
比較結果が一致
S13
Yes
待ち受け画面表示
S15