(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2004-336719
(P2004-336719A)
(43)公開日　平成16年11月25日(2004.11.25)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04Q 7/38	H04B 7/26	109S	5B017
G06F 12/14	G06F 12/14	510D	5K067
	G06F 12/14	530C	
	G06F 12/14	540C	
	G06F 12/14	550A	

審査請求 有　請求項の数 18　ＯＬ　（全 18 頁）

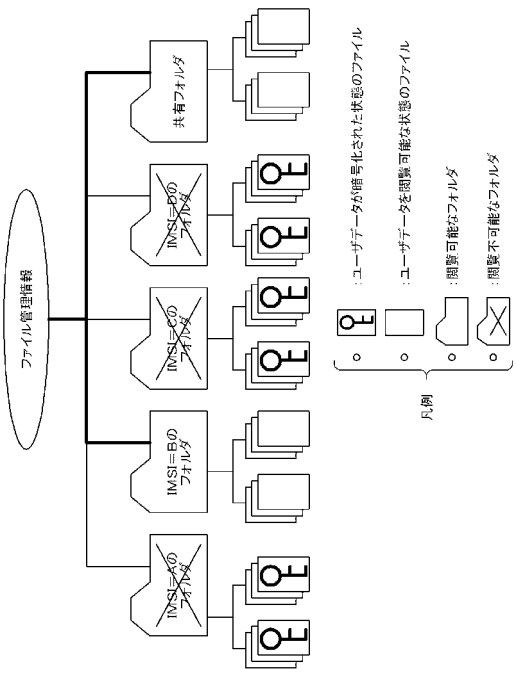
(21)出願番号　特願2004-109316(P2004-109316)
(22)出願日　平成16年4月1日(2004.4.1)
(31)優先権主張番号　特願2003-112110(P2003-112110)
(32)優先日　平成15年4月16日(2003.4.16)
(33)優先権主張国　日本国(JP)

(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　100109313
弁理士　机　昌彦
(74)代理人　100085268
弁理士　河合　信明
(74)代理人　100111637
弁理士　谷澤　靖久
(72)発明者　塚本　直史
東京都港区芝五丁目７番１号
日本電気株式会社内

Ｆターム(参考)　5B017 BA07 CA14
5K067 AA30 BB04 DD17 HH23 HH24
HH36 KK15

(54)【発明の名称】携帯端末及びその情報管理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】着脱可能な記憶媒体に記憶されている識別情報に従ってユーザを識別する携帯端末を、複数ユーザ間で共有使用する場合において、その携帯端末内に残される各ユーザの個人用コンテンツに対するプライバシーの保護を向上する。
【解決手段】ＵＩＭカード８により加入者情報（ＩＭＳＩ）と本体とを分離した状態で保有可能な携帯電話機１００において、当該携帯電話機内のユーザデータ（個人用コンテンツ）を、ＵＩＭカード８内のＩＭＳＩと関連付けた状態で、その識別情報に対応する固有のフォルダ（ＩＭＳＩ固有フォルダ）内に暗号化して記憶する。
【選択図】　図４



【特許請求の範囲】
【請求項１】
着脱可能な記憶媒体が装着された際に、その記憶媒体に記憶されている識別情報に従って、利用可能なユーザを識別する携帯端末であって、
前記識別情報に関連付けた状態で、ユーザ個別の記憶領域を生成する記憶領域生成手段と、
装着された前記記憶媒体から識別情報を読み出すと共に、前記携帯端末内の個人用コンテンツを、その識別情報を基に暗号化する暗号化手段と、
前記暗号化された個人用コンテンツを、前記識別情報に関連付けされた特定の記憶領域に保存する保存手段と、
装着された前記記憶媒体から識別情報を読み出すと共に、その識別情報に関連付けされた前記特定の記憶領域に暗号化された状態で保存されている個人用コンテンツを、該識別情報を基に復号することにより、ユーザによる閲覧が可能な状態に展開する復号手段と、
を備えることを特徴とする携帯端末。
【請求項２】
前記記憶領域生成手段は、
前記記憶媒体が装着されるのに応じて、その記憶媒体に記憶されている前記識別情報に関連付けされたところの、前記特定の記憶領域を自動的に生成する
ことを特徴とする請求項１記載の携帯端末。
【請求項３】
前記記憶領域生成手段は、
前記記憶媒体が装着される状態において、前記特定の記憶領域に関連付けされた副記憶領域を、ユーザによる設定操作に応じて設定する副記憶領域設定手段を含む
ことを特徴とする請求項２記載の携帯端末。
【請求項４】
前記携帯端末を使用可能な複数のユーザのための共有記憶領域へのコンテンツの書き込み、及び該記憶領域に保存されているコンテンツの参照のうち、少なくとも何れかが可能な情報共有手段を更に備える
ことを特徴とする請求項１記載の携帯端末。
【請求項５】
前記記憶媒体が装着され、且つ前記個人用コンテンツの閲覧が可能な状態において、その記憶媒体に記憶されている前記識別情報に関連付けされたところの、前記特定の記憶領域に保存されている個人用コンテンツに対して、前記共有記憶領域への移動及び複写のうち少なくとも何れかを、ユーザの操作に応じて実行する操作手段を更に備える
ことを特徴とする請求項４記載の携帯端末。
【請求項６】
前記記憶媒体が装着され、且つ前記個人用コンテンツの閲覧が可能な状態において、前記共有記憶領域に保存されている情報に対して、該記憶媒体に記憶されている前記識別情報に関連付けされた前記特定の記憶領域への移動及び複写のうち少なくとも何れかを、ユーザの操作に応じて実行する操作手段を更に備える
ことを特徴とする請求項４記載の携帯端末。
【請求項７】
前記暗号化手段は、
前記記憶媒体から読み出された前記識別情報に基づいて暗号鍵を生成すると共に、その暗号鍵を利用して前記個人用コンテンツを暗号化する
ことを特徴とする請求項１乃至請求項６の何れかに記載の携帯端末。
【請求項８】
前記復号手段は、
前記記憶媒体から読み出された前記識別情報に基づいて暗号鍵を生成すると共に、前記識別情報に既に関連付けされている前記特定の記憶領域内に暗号化された状態で保存されて

いる個人用コンテンツを、該暗号鍵を利用して復号する
ことを特徴とする請求項１乃至請求項７の何れかに記載の携帯端末。
【請求項９】
前記識別情報は、
前記携帯端末によるサービスを利用可能な加入者を識別する加入者情報、または前記記憶媒体毎に固有のシリアル番号である
ことを特徴とする請求項１乃至請求項８の何れかに記載の携帯端末。
【請求項１０】
前記保存手段および復号手段は、
前記暗号化された個人用コンテンツを、前記識別情報と前記特定の記憶領域との関連付けの状態を管理するファイル管理情報を利用して、可変サイズのデータファイルとして動的に管理する
ことを特徴とする請求項１乃至請求項９の何れかに記載の携帯端末。
【請求項１１】
前記記憶領域として、複数のユーザのために個別の固定領域が確保されており、
前記保存手段は、前記暗号化された個人用コンテンツを、対象となるユーザのための特定の固定領域に保存するに際して、その特定の固定領域のヘッダ部分にタグを付与し、
前記復号手段は、前記暗号化された個人用コンテンツの復号に際して、装着された前記記憶媒体から読み出された識別情報に従って前記タグを参照することにより、対象となるユーザのための特定の固定領域を判断する
ことを特徴とする請求項１乃至請求項９の何れかに記載の携帯端末。
【請求項１２】
前記記憶媒体は、共通規格のＩＣカードである
ことを特徴とする請求項１乃至請求項１１の何れかに記載の携帯端末。
【請求項１３】
本体と着脱可能な、識別情報が記憶された記憶媒体を使用する携帯端末における情報管理方法であって、
前記携帯端末に装着された前記記憶媒体から前記識別情報を読み出し、該識別情報に基づいて、前記携帯端末内の個人用コンテンツを暗号化すると共に、暗号化された個人用コンテンツを、前記識別情報に関連付けされた特定の記憶領域に保存する暗号化工程と、
前記携帯端末が前記記憶媒体に装着されたときに、その記憶媒体から識別情報を読み出すと共に、その識別情報に関連付けされた前記特定の記憶領域に前記暗号化された個人用コンテンツが保存されている場合には、その暗号化された状態の個人用コンテンツを、該識別情報を基に復号することによってユーザによる閲覧が可能な状態に展開する復号工程と、
を有することを特徴とする情報管理方法。
【請求項１４】
前記記憶媒体が装着されるのに応じて、その記憶媒体から識別情報を読み出すと共に、その識別情報に関連付けした状態の前記特定の記憶領域を、該識別情報毎に個別に、自動的に生成する記憶領域作成工程を更に有する
ことを特徴とする請求項１３記載の情報管理方法。
【請求項１５】
前記暗号化工程では、
前記記憶媒体から読み出された前記識別情報に基づいて暗号鍵を生成すると共に、その暗号鍵を利用して前記個人用コンテンツを暗号化する
ことを特徴とする請求項１３または請求項１４記載の情報管理方法。
【請求項１６】
前記復号工程では、
前記記憶媒体から読み出された前記識別情報に基づいて暗号鍵を生成すると共に、前記記憶領域内に暗号化された状態で保存されている個人用コンテンツを、該暗号鍵を利用して

復号する
ことを特徴とする請求項１３または請求項１４記載の情報管理方法。
【請求項１７】
前記識別情報は、
前記携帯端末によるサービスを利用可能な加入者を識別する加入者情報、または前記記憶媒体毎に固有のシリアル番号である
ことを特徴とする請求項１３乃至請求項１６の何れかに記載の情報管理方法。
【請求項１８】
着脱可能な記憶媒体が装着された際に、その記憶媒体に記憶されている識別情報に従って、利用可能なユーザを識別する携帯端末の動作制御のためのコンピュータ・プログラムであって、そのコンピュータ・プログラムにより、
前記識別情報に関連付けた状態で、ユーザ個別の記憶領域を生成する記憶領域生成機能と、
装着された前記記憶媒体から識別情報を読み出すと共に、前記携帯端末内の個人用コンテンツを、その識別情報を基に暗号化する暗号化機能と、
前記暗号化された個人用コンテンツを、前記識別情報に関連付けされた特定の記憶領域に保存する保存機能と、
装着された前記記憶媒体から識別情報を読み出すと共に、その識別情報に関連付けされた前記特定の記憶領域に暗号化された状態で保存されている個人用コンテンツを、該識別情報を基に復号することにより、ユーザによる閲覧が可能な状態に展開する復号機能とを、コンピュータに実行させることを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、携帯電話等の携帯端末の技術分野に関し、特に、記憶媒体に記憶されている識別情報に従って利用可能なユーザを識別する携帯端末の技術分野に関する。
【背景技術】
【０００２】
近年においては、ＩＭＴ－２０００等の次世代の標準規格に基づく携帯電話機（所謂、第三世代携帯電話機）が開発されている。このような第三世代携帯電話機においては、加入者情報等が記録された機構媒体（ＩＣカード）と、携帯電話機本体とが分離した構成である。
【０００３】
係る第三世代携帯電話機において、個々のユーザは、ＵＩＭ（User Identity Module：但しＵＳＩＭまたはＲ－ＵＩＭと称される場合もある）カードを保有している。このＵＩＭカードには、自身用の加入者情報（契約者情報）及び他の情報（クレジット決済用の個人識別情報など）が記録されたＩＣカードである。ユーザは、自分用のＵＩＭカードを本体に挿入することにより、任意の第三世代携帯電話機においてサービスを利用することが可能である。
【０００４】
従来のＧＳＭ携帯電話においては、ＳＩＭ（Subscriber Identity Module）に記憶される情報が加入者情報に限られている。これに対して、第三世代携帯電話機においては、ＵＩＭカードを利用することにより、単一の電話機を複数のユーザが使用可能である。
従って、このような使用形態が可能な第三世代携帯電話機において、個人のプライバシーを確保するためには、契約者情報だけでなく、各種の個人用コンテンツを、個人用のＵＩＭカード内に全て保持できることが理想である。ここで、個人用コンテンツとは、例えば、ユーザが入力した電話帳、電子メール、スケジュール、並びに個人設定情報などの情報である。
【０００５】
しかしながら、ＵＩＭカードのサイズや記憶容量の制限により、１枚のＵＩＭカードに

全ての個人用コンテンツ（以下、「ユーザデータ」と称する場合がある）を保持することは不可能である。このため、現実的には、ユーザ個人が設定、収集、並びに利用する各種コンテンツ（即ち、メール、電話帳、アプリケーションの設定情報など）の殆どは携帯電話機本体に記録され、当該ユーザによる利用終了後もその携帯電話機の内部に残ることになる。

【０００６】

即ち、第三世代携帯電話機においては、ある個人の携帯電話機に他人のＵＩＭカードが挿入（装着）された場合、当該他人の契約者情報に基づくサービスを提供可能である。しかしながら、この場合、当該他人は、先のユーザによって当該携帯電話機の内部に残された各種コンテンツを、自由に使用並びに変更できることになる。

【０００７】

より具体的には、

（１）前のユーザの発着信履歴が携帯電話機内に残る。

（２）同一携帯電話機を先に利用したユーザ宛てのメール等を他人が参照できる。

（３）同一携帯電話機を先に利用したユーザが利用したネットワーク利用型コンテンツ（ネットワーク接続を利用するアプリケーション等)を他人が使用可能となる。

（４）同一携帯電話機を先に利用したユーザが設定、収集等を行った個人用コンテンツの追加および削除等の操作が可能となる。

【０００８】

また、従来の第３世代携帯電話において、ＵＩＭカードを挿入せずに携帯電話機の電源を投入した場合には、携帯電話のサービスを利用することは不可能である。しかしながら、その携帯電話機の内部に残っている個人用コンテンツを他人が自由に参照、使用等できる。

【０００９】

一般に、従来の日本国内における第２世代以前の携帯電話機においては、個々の携帯電話機の不揮発記憶領域にユーザ個人の契約者情報が記録されている。このため、その契約者情報（加入者情報）の管理と、携帯電話機内の個人用コンテンツの管理とは、１対１の関係を有する。これに対して、第三世代の携帯電話機においては、上述した通り１台の携帯電話機を複数の契約者で共有する機会が格段に増すため、個人用コンテンツの保護する手段が必要となる。

【００１０】

ここで、従来の技術例としては、ユーザデータを不揮発性メモリへ格納する構成の携帯端末において、ユーザデータの書き込み時の消失や不正化を防止する「携帯端末とそのユーザデータ保護方法」がある（例えば、特許文献１参照）。

【００１１】

また、ユーザの識別情報やユーザが独自に決めた識別情報を、キーワードを用いて自動的に暗号化および復号化する「情報の暗号化／解読方法と同システム」がある（例えば、特許文献２参照）。

【００１２】

また、ＳＩＭカードを用いて利用した携帯電話機を他者に渡した場合には、内部に記録されたプライベートな個人データ（即ち、ユーザが入力した電話帳、電子メール、スケジュール、および個人設定情報など）の閲覧を防止できる「加入者カードを用いる携帯電話機」がある（例えば、特許文献３参照）。

【００１３】

【特許文献１】特開２００１－１０１０７９号公報（段落番号００１３、図１）

【特許文献２】特開２００２－２８１０２２号公報（段落番号００２６、図１）

【特許文献３】特開２００２－３００２５４号公報（段落番号００２６、００４０、図１）

【発明の開示】

【発明が解決しようとする課題】

【００１４】
しかしながら、上記特許文献１記載の発明は、ＵＩＭカード等を使用する第３世代携帯端末に対応していない構成である。
【００１５】
また、特許文献２記載の発明は、データの暗号化に用いるキーワードがユーザによって作成されるものであり、ＵＩＭカード内の識別情報を用いるものではなく、第３世代携帯端末に対応していない構成である。
【００１６】
また、特許文献３記載の発明は、第３世代携帯電話機に対応する構成であり、且つ本体内部に記憶された個人データは、ＳＩＭカードを本体からから引き抜くときに消去される。しかしながら、その個人データは、ＳＩＭカードを本体からから引き抜く際に、暗号化された状態で、そのＳＩＭカードとは異なる他の外付けメモリに記録される。即ち、特許文献３記載の発明では、ＳＩＭカード以外に、データ保護のために外付けのメモリを必要とする。
【００１７】
従って、このような背景を鑑みれば、ＵＩＭカード以外の他のメモリカード等を必要とせず、且つＵＩＭカードが装着されていない状態で本体の電源が投入された場合であっても、内部に記憶されている個人用コンテンツを閲覧することができない第３世代携帯電話機対応の携帯端末が望まれる。
【００１８】
そこで、本発明は、着脱可能な記憶媒体に記憶されている識別情報に従ってユーザを識別する携帯端末を、複数ユーザ間で共有使用する場合において、その携帯端末内に残される各ユーザの個人用コンテンツに対するプライバシーの保護向上が可能な携帯端末及びその情報管理方法、並びにコンピュータ・プログラムの提供を目的とする。
【課題を解決するための手段】
【００１９】
上記の目的を達成すべく、本発明に係る携帯端末は、以下の構成を備えることを特徴とする。
【００２０】
即ち、着脱可能な記憶媒体（ＩＣカード、ＵＩＭカード８）が装着された際に、その記憶媒体に記憶されている識別情報（ＩＭＳＩ、加入者情報、契約者情報）に従って、利用可能なユーザを識別する携帯端末（携帯電話機１００）であって、
前記識別情報に関連付けた状態で、ユーザ個別の記憶領域（ＩＭＳＩ固有フォルダ）を生成する記憶領域生成手段（３）と、
装着された前記記憶媒体から識別情報を読み出すと共に、前記携帯端末内の個人用コンテンツを、その識別情報を基に暗号化する暗号化手段（３，１３）と、
前記暗号化された個人用コンテンツを、前記識別情報に関連付けされた特定の記憶領域に保存する保存手段（３）と、
装着された前記記憶媒体から識別情報を読み出すと共に、その識別情報に関連付けされた前記特定の記憶領域に暗号化された状態で保存されている個人用コンテンツを、該識別情報を基に復号することにより、ユーザによる閲覧が可能な状態に展開する復号手段（３，１３）と、
を備えることを特徴とする。
【００２１】
また、前記記憶領域生成手段は、
前記記憶媒体が装着されるのに応じて、その記憶媒体に記憶されている前記識別情報に関連付けされたところの、前記特定の記憶領域を自動的に生成すると良い。
【００２２】
好適な実施形態において、前記携帯端末を使用可能な複数のユーザのための共有記憶領域（共有フォルダ）へのコンテンツの書き込み、及び該記憶領域に保存されているコンテ

ンツの参照のうち、少なくとも何れかが可能な情報共有手段を更に備えることを特徴とする。

【００２３】

また、前記暗号化手段（暗号処理ソフトウエア・プログラム１３）は、前記記憶媒体から読み出された前記識別情報に基づいて暗号鍵を生成すると共に、その暗号鍵を利用して前記個人用コンテンツを暗号化すると良い。

【００２４】

また、前記復号手段（暗号処理ソフトウエア・プログラム１３）は、前記記憶媒体から読み出された前記識別情報に基づいて暗号鍵を生成すると共に、前記識別情報に既に関連付けされている前記特定の記憶領域内に暗号化された状態で保存されている個人用コンテンツを、該暗号鍵を利用して復号すると良い。

【００２５】

尚、同目的は、上記の各構成を有する携帯端末に対応する情報管理方法によっても達成される。

【００２６】

また、同目的は、上記の各構成を有する携帯端末、並びに対応する方法を、コンピュータによって実現するプログラム・コード、及びそのプログラム・コードが格納されている、コンピュータ読み取り可能な記憶媒体によっても達成される。

【発明の効果】

【００２７】

上記の本発明によれば、着脱可能な記憶媒体に記憶されている識別情報に従ってユーザを識別する携帯端末を、複数ユーザ間で共有使用する場合において、その携帯端末内に残される各ユーザの個人用コンテンツに対するプライバシーの保護向上が可能な携帯端末及びその情報管理方法、並びにコンピュータ・プログラムの提供が実現する。

【発明を実施するための最良の形態】

【００２８】

以下、本発明に係る携帯端末を、代表的な携帯端末である携帯電話機に適用した実施形態として、添付図面を参照しながら詳細に説明する。

【００２９】

図２は、本発明を適用可能な携帯電話機の一般的な装置構成例を示すブロック図である。

【００３０】

同図に示す携帯電話機１００は、例えばＩＭＴ－２０００等の標準規格に基づく第３世代携帯電話機であって、ＵＩＭカード８を本体に対してユーザが着脱可能な構成を有する。

【００３１】

ＵＩＭ（User Identity Module）カード８は、所謂ＩＣカード等の記憶媒体である。ＵＩＭカード８の内部には、携帯電話機１００を使用可能なユーザを識別するための識別情報が予め記憶されている。本実施形態において、係る識別情報は、ＩＭＳＩ（International Mobile Subscriber Identifier）と呼ばれる加入者情報（契約者情報）である。ＩＭＳＩは、個々の加入者（ユーザ）を特定すべく、加入者毎に個別に付与された情報である。

【００３２】

図２において、無線ユニット１は、基地局との無線通信を実現するための所定の周波数帯域の無線電波の送受信を行う。通信処理ユニット２は、無線ユニット１による受信電波に応じた信号を、中央制御ユニット３が認識可能なデジタル信号に変換する。また、通信処理ユニット２は、中央制御ユニット３から出力されるデジタル信号を、無線ユニット１にて送信信号に変換可能な信号形態に変換する。

【００３３】

中央制御ユニット３は、携帯電話機１００の全体の動作を司るＣＰＵ(Central Process

ing Unit)及びメモリ等（何れも不図示）からなるハードウエアと、そのＣＰＵによって実行される各種ソフトウエア・プログラムとからなる。本実施形態において、携帯電話機１００には、実行されるべきソフトウエア・プログラムとして、暗号処理ソフトウエア・プログラム１３が実装されている（詳細は後述する）。

【００３４】

周辺装置制御ユニット４は、中央制御ユニット３による指示に従って、レシーバ（スピーカ）９への音声出力処理、マイク１０から入力される音声の信号処理、並びに不図示の操作スイッチやディスプレイ等の入出力処理を行う。

【００３５】

ＵＩＭカード制御ユニット７は、中央制御ユニット３による指示に従って、携帯電話機１００に装着されたＵＩＭカード８から情報を読み出すと共に、必要な場合には情報を書き込む。電源制御ユニット５は、不図示のバッテリを有しており、携帯電話機１００の各部への電源供給を行う。

【００３６】

不揮発性メモリ（あるいは常時バックアップされる揮発性メモリ）１１は、ユーザデータ（個人用コンテンツ）、中央制御ユニット３のＣＰＵが実行すべき各種ソフトウエア・プログラム等が記憶されるＥＥＰＲＯＭ等の記憶素子である。

【００３７】

本実施形態において、ユーザデータ（個人用コンテンツ）とは、電話帳、メール、発着信履歴、その他のコンテンツ、更には携帯電話機操作部のカスタマイズ情報（例えば、画面上に置かれたアイコンの配置情報）である。

【００３８】

次に、一時記憶メモリ１２は、ＵＩＭカード８から読み出された情報や書き込むべき情報の一時記憶、並びに中央制御ユニット３が実行している各種プログラムのためのワークエリアとして使用される。

【００３９】

そして、共通バス６は、上述した携帯電話機１００の各ブロックに接続されており、同携帯電話機の動作に応じて各種情報の転送を行う。

【００４０】

そして、ユーザは、携帯電話機１００の利用に際して、ＵＩＭカード８を携帯電話機１００の本体に設けられたスロット（不図示）等の所定位置に装着する。これにより、ユーザは、携帯電話網を介した他者との会話や、契約している各種サービス（Ｗｅｂサイトの閲覧等）を利用することができる。

【００４１】

尚、携帯電話機１００が備える装置構成（図２：特に、無線通信のために備える構成）自体は、あくまでも一例であって、現在では一般的な各種の技術を採用することができるので、本実施形態における詳細な説明は省略する。

【００４２】

次に、本実施形態におけるユーザデータ（個人用コンテンツ）の管理方法について、図１、図３－Ａ、並びに図３－Ｂを参照して説明する。

【００４３】

図３－Ａは、情報処理装置においてデータを静的に管理する場合を概念的に示す図である。また、図３－Ｂは、情報処理装置においてデータを動的に管理する場合を概念的に示す図である。

【００４４】

各種の情報処理装置において、処理すべきデータを管理する場合の一般的な方法としては、従来から様々な方式が提案されている。これらの方式のうち、図３－Ａに示す静的管理方式では、１つ１つのデータ（データＡ乃至Ｄ）が、予め設定した各々固定サイズのデータエリアに記憶される。また、図３－Ｂに示す動的管理方式では、１つ１つのデータが、ファイル管理情報（ファイル管理テーブル）による管理の基に、可変サイズのファイル

化されたデータファイルとして記憶される。係るファイル管理情報は、情報処理装置内の不揮発メモリの所定領域に確保され、その所定領域の物理アドレスとのマッピングが記録される。

【００４５】

これらのデータ管理方式において、個々のデータ（データファイル）は、不揮発メモリに格納される。また、格納された個々のデータは、例えば、情報処理装置の電源ＯＮ時、あるいはユーザの読み出し操作に応じて、当該不揮発性メモリから読み出された後、一時記憶メモリに一旦展開されてから利用される。そして、データの変更等が行われる際には、まず一時記憶メモリに展開されたデータの変更が行われた後、その変更内容が不揮発メモリに反映される。係る変更内容を反映すべく、不揮発メモリを書き換えるタイミングは、データ毎の性質により異なる。

【００４６】

そして本実施形態では、このようなデータの管理方式のうち、動的管理方式（図３－Ｂ）を基本として、ユーザデータを管理する際のプライバシーの保護を実現する。

【００４７】

図１は、本実施形態に係る携帯電話機１００において行われるユーザデータの管理手法を概念的に示す図である。

【００４８】

本実施形態において、携帯電話機１００内のユーザデータは、動的に管理されることを前提としている。不揮発メモリ１１内に用意されたユーザデータの保存領域には、ＩＭＳＩに関連付けられたフォルダ情報が記録される。このフォルダ情報（以下、「ＩＭＳＩ固有フォルダ」と称する）は、携帯電話機１００を利用可能なユーザに個別に付与されたＩＭＳＩ（加入者情報）に１対１で関連付けされた状態で、ユーザ毎に確保される。そして、あるユーザのユーザデータは、そのユーザのＵＩＭカード８に記憶されているＩＭＳＩに関連付けされた「ＩＭＳＩ固有フォルダ」内に保存される。

【００４９】

即ち、本実施形態において、同一の携帯電話機１００の不揮発メモリ１１内には、その携帯電話機に装着されるＵＩＭカード８の枚数（換言すれば、同一携帯電話機を共有使用するユーザの人数分）だけ、「ＩＭＳＩ固有フォルダ（図１ではＩＭＳＩ＝Ａ乃至Ｄと示されたフォルダ）」が作成される。

【００５０】

また、不揮発メモリ１１内に用意されたユーザデータの保存領域には、携帯電話機１００を利用するユーザが共通に利用できるコンテンツを保存するための「共有フォルダ」が設定されている。

【００５１】

そして、「ＩＭＳＩ固有フォルダ」と「共有フォルダ」とは、図３－Ｂを参照して説明した場合と同様に、ファイル管理情報（ファイル管理テーブル）によって管理される。但し、本実施形態におけるユーザデータの管理の特徴として、図１に概念的に示すように、ＩＭＳＩ＝Ａ乃至Ｄと示された「ＩＭＳＩ固有フォルダ」に保管されるユーザデータは、ＵＩＭカード８から読み出されたＩＭＳＩを基にする鍵情報によって暗号化された状態で、その「ＩＭＳＩ固有フォルダ」内に記憶される。また、「ＩＭＳＩ固有フォルダ」は、当該フォルダが生成されるに際して、対応するＩＭＳＩと関連付けがなされる。

【００５２】

即ち、暗号化された個人用コンテンツのファイルは、可変サイズのデータファイルである。中央制御ユニット３は、暗号化された個人用コンテンツのファイルを、識別情報であるＩＭＳＩと、特定の記憶領域である「ＩＭＳＩ固有フォルダ」との関連付けの状態を管理するファイル管理情報を利用して動的に管理する。

【００５３】

ここで、本実施形態において、鍵情報（暗号鍵）は、ＵＩＭカード８から読み出されたＩＭＳＩを基にして生成される。より具体的に、暗号化及び復号化を行う際に使用する鍵

情報は、ＩＭＳＩの一部を利用しても、或いは全部を利用しても良い。また、ＩＭＳＩの一部または全部を利用して暗号鍵を生成するには、暗号処理やハッシュ処理等を施した結果を利用すれば良い。

【００５４】

また、中央制御ユニット３による動的管理が行われるに際して、暗号処理ソフトウエア・プログラム１３は、ユーザデータ（個人用コンテンツ）の暗号化と複合化（解読）とを行う。

【００５５】

より具体的に、暗号処理ソフトウエア・プログラム１３は、ＵＩＭカード８（記憶媒体）から読み出された識別情報（ＩＭＳＩ）に基づいて暗号鍵（鍵情報）を生成すると共に、その暗号鍵を利用して個人用コンテンツを暗号化する。また、暗号処理ソフトウエア・プログラム１３は、ＵＩＭカード８から読み出されたＩＭＳＩに基づいて暗号鍵を生成すると共に、そのＩＭＳＩに既に関連付けされている「ＩＭＳＩ固有フォルダ」内に暗号化された状態で保存されている個人用コンテンツを、該暗号鍵を利用して復号する。

【００５６】

尚、暗号処理ソフトウエア・プログラム１３は、上記の如く暗号化及び復号化を行うに際して、ＵＩＭカード８より読み出されたＩＭＳＩを一時記憶する。

【００５７】

携帯電話機１００の中央制御ユニット３では、同携帯電話機の全体の動作制御を司るメインプログラム（不図示）が実行されている。このメインプログラムは、携帯電話機１００の電源ＯＮ時に、ＵＩＭカード１８が装着されているか否かに関わらず、暗号処理ソフトウエア・プログラム１３を起動する。

【００５８】

更に、このメインプログラムは、ユーザによる入力操作や外部からのダウンロード等によって、一時記憶メモリ１２に格納されている個人用コンテンツ（暗号化されていないユーザデータ）が変更（或いは更新）された場合にも、暗号処理ソフトウエア・プログラム１３を起動する。

【００５９】

そして、上記の何れの場合においても、暗号処理ソフトウエア・プログラム１３は、当該暗号鍵を用いて変更内容を暗号化した後で、暗号化したユーザデータを、一時記憶メモリ１２から、対応する「ＩＭＳＩ固有フォルダ」内に移動する。本実施形態において、中央制御ユニット３のメインプログラムは、１回の暗号化処理または復号化処理が完了するのに応じて、暗号処理ソフトウエア・プログラム１３の動作を中止する。

【００６０】

図４は、本実施形態に係る携帯電話機１００において行われるユーザデータの管理手法により、復号化されたユーザデータと、暗号化されたユーザデータとが同電話機内に存在する状態を概念的に示す図である。

【００６１】

同図において、ＩＭＳＩ＝Ａ乃至Ｄと示されたフォルダは、それぞれ「ＩＭＳＩ固有フォルダ」である。これらのフォルダと、ＩＭＳＩ（＝Ａ乃至Ｄ）との対応関係は、下記の通りである。

【００６２】

即ち、ＩＭＳＩ＝Ａと示されたフォルダは、対応するＩＭＳＩ＝”Ａ”なる識別情報を基に生成された暗号鍵によって保護（暗号化／復号化）される。

【００６３】

ＩＭＳＩ＝Ｂと示されたフォルダは、対応するＩＭＳＩ＝”Ｂ”なる識別情報を基に生成された暗号鍵によって保護される。

【００６４】

ＩＭＳＩ＝Ｃと示されたフォルダは、対応するＩＭＳＩ＝”Ｃ”なる識別情報を基に生成された暗号鍵によって保護される。

【００６５】
そして、フォルダＩＭＳＩ＝Ｄは、対応するＩＭＳＩ＝”Ｄ”なる識別情報を基に生成された暗号鍵によって保護される。
【００６６】
図４に示す例では、識別情報（加入者情報）としてＩＭＳＩ＝“Ｂ”が格納されたＵＩＭカード８を所有するユーザが、携帯電話機１００を使用している状態を表している。この場合、当該ユーザは、ＩＭＳＩ＝Ｂと示された「ＩＭＳＩ固有フォルダ」内に格納されていた個人用コンテンツを、復号化した上で操作可能である。更に、当該ユーザは、「共有フォルダ」内に格納されているコンテンツを操作可能である。一方、当該ユーザは、ＩＭＳＩ＝Ｂ以外の「ＩＭＳＩ固有フォルダ」内に暗号化された状態で格納されている個人用コンテンツにはアクセスすることができない。
【００６７】
次に、上述した携帯電話機１００の動作を実現する制御処理について、図５から図７を参照して説明する。
【００６８】
図５は、本実施形態における携帯電話機１００の電源投入時の制御処理のフローチャートである。図６は、本実施形態における携帯電話機１００のユーザデータ読み出し時の制御処理のフローチャートである。そして、図７は、本実施形態における携帯電話機１００のユーザデータ保存時の制御処理のフローチャートである。
【００６９】
図５乃至図７に示すフローチャートは、図２に示す中央制御ユニット３において不図示のＣＰＵが実行するソフトウエア・プログラムの処理手順を表す。
【００７０】
はじめに、電源投入時の動作について、図５を参照して説明する。図５に示すフローチャートの処理は、所定の電源投入操作が検出されるのに応じて、電源制御ユニット５による中央制御ユニット３への電源供給が開始されることによって起動される。
【００７１】
中央制御ユニット３は、携帯電話機１００の初期設定を行う（ステップＳ５０１）と共に、ＵＩＭカード８が装置に装着されているかを調べる（ステップＳ５０２）。
【００７２】
ステップＳ５０２の判断でＹＥＳ判定（ＵＩＭカード８有り）の場合、中央制御ユニット３は、装着されているＵＩＭカード８を活性化する（ステップＳ５０３）と共に、同カード内の各種情報を読み出す（ステップＳ５０４）。ステップＳ５０４にて読み出される情報には、ユーザの識別情報であるＩＭＳＩが含まれている。そこで、中央制御ユニット３は、読み出したＩＭＳＩを、一時記憶メモリ１２内に一時記憶し（ステップＳ５０５）、ステップＳ５０６に処理を進める。
【００７３】
ステップＳ５０６において、中央制御ユニット３は、暗号処理ソフトウエア・プログラム１３を起動する。ステップＳ５０６は、ステップＳ５０２の判断でＮＯ判定（ＵＩＭカード８無し）の場合にも実行される。
【００７４】
次に、中央制御ユニット３は、「共有フォルダ」内の情報を、一時記憶メモリ１２内に読み出す（ステップＳ５０７）。「共有フォルダ」内に存在する情報は各ユーザに対して開放されたものであるため、暗号化及び復号化は行われない。
【００７５】
中央制御ユニット３は、ステップＳ５０５にて一時記憶されたＩＭＳＩが一時記憶メモリ１２内に存在するかを判断する（ステップＳ５０８）。そして、ステップＳ５０８にてＹＥＳ判定（ＩＭＳＩ有り）の場合、中央制御ユニット３は、一時記憶されている当該ＩＭＳＩに対応するフォルダ（即ち、当該ＩＭＳＩに関連付けされた「ＩＭＳＩ固有フォルダ」）が存在するか否かを判断する（ステップＳ５０９）。

【００７６】
次に、ステップＳ５０９にてＹＥＳ判定（「ＩＭＳＩ固有フォルダ」有り）の場合、中央制御ユニット３は、その「ＩＭＳＩ固有フォルダ」内に暗号化された状態で記憶されているユーザデータを、不揮発メモリ１１から一時記憶メモリ２１に読み出す（ステップＳ５１０）。
【００７７】
そして、中央制御ユニット３は、一時記憶しているＩＭＳＩを基に暗号鍵を生成すると共に、その暗号鍵を利用して、ステップＳ５１０にて読み出したユーザデータの復号化を行う（ステップＳ５１１）。ステップＳ５１２において、中央制御ユニット３は、ステップＳ５１１にて復号化したユーザデータと、ステップＳ５０７にて読み出した「共有フォルダ」内のコンテンツ（共有データ）とを、一時記憶メモリ１２内に展開する。
【００７８】
一方、ステップＳ５０８またはステップＳ５０９にてＮＯ判定の場合とは、
（１）ＵＩＭカード８が装着されていない状態で電源がオン状態とされた場合、
（２）ＵＩＭカード８は装着されているが、同カード内のＩＭＳＩに対応する「ＩＭＳＩ固有フォルダ」が存在しない場合、
の何れかである。そこで、この何れかの場合において、中央制御ユニット３は、ステップＳ５０７にて読み出した共有データを一時記憶メモリ１２内に展開すべく、処理をステップＳ５１２に進める。
【００７９】
次に、ユーザによる装置操作に伴うユーザデータの読み出し時の動作について、図６を参照して説明する。
【００８０】
中央制御ユニット３は、ユーザによる操作を検出する（ステップＳ６０１）と、その操作が「共有フォルダ」内の共有データの読み出しを指定するものであるかを判断する（ステップＳ６０２）。
【００８１】
ステップＳ６０２にてＹＥＳ判定の場合、中央制御ユニット３は、「共有フォルダ」内の共有データを読み出し（ステップＳ６０３）、読み出した共有データを一時記憶メモリ１２内に展開する（ステップＳ６０９）。共有データは、各ユーザに開放されたものであるため、復号化処理は必要ない。
【００８２】
一方、ステップＳ６０２にてＮＯ判定の（共有データではない）場合、ステップＳ６０１にてユーザが読み出しを指定したデータは、そのユーザのためのユーザデータである。そこで、この場合、中央制御ユニット３は、電源投入に際して先に実行した制御処理（図５）のステップＳ５０５において一時記憶しているＩＭＳＩが存在するか否かを判断する（ステップＳ６０４）。
【００８３】
次に、ステップＳ６０４にてＹＥＳ判定（ＩＭＳＩ有り）の場合、中央制御ユニット３は、一時記憶されている当該ＩＭＳＩに対応するフォルダ（即ち、当該ＩＭＳＩに関連付けされた「ＩＭＳＩ固有フォルダ」）が存在するか否かを判断する（ステップＳ６０５）。
【００８４】
そして、ステップＳ６０５の判定にて「ＩＭＳＩ固有フォルダ」が存在すると判断された場合、中央制御ユニット３は、ステップＳ６０６にて暗号処理ソフトウエア・プログラム１３を起動した後、上述したステップＳ５１０及びステップＳ５１１と同様な処理をステップＳ６０７及びステップＳ６０８にて実行する。これにより、一時記憶されているＩＭＳＩに対応する復号化後のユーザデータを得る。中央制御ユニット３は、このユーザデータを、一時記憶メモリ１２内に展開する（ステップＳ６０９）。
【００８５】

一方、ステップＳ６０４またはステップＳ６０５にてＮＯ判定の場合は、ステップＳ５０８及びステップＳ５０９にて説明した上記の（１）または（２）の場合である。そこで、この何れかの場合に、中央制御ユニット３は情報を読み出すことなく処理を完了する（ステップＳ６１０）。

【００８６】

次に、ユーザによる装置操作に伴うユーザデータの保存時の動作について、図７を参照して説明する。

【００８７】

電話帳の入力操作やメールの送受信、ネットワークからのダウンロード等によって得られたコンテンツは、一時記憶メモリ１１に記録される。本実施形態において、ユーザは、このようにして得られたコンテンツの保存操作を行うことができる。

【００８８】

中央制御ユニット３は、ユーザによる操作を検出する（ステップＳ７０１）と、その操作が「共有フォルダ」内の共有データとしての保存を指示するのか、或いは暗号化した状態で自分用の「ＩＭＳＩ固有フォルダ」内に保存することを指示するものであるかを判断する（ステップＳ７０２）。

【００８９】

中央制御ユニット３は、ユーザの操作が共有データとしての保存を指示するとステップＳ７０２にて判断した場合には、対象となるデータを、暗号化することなく共有データとして「共有フォルダ」内に保存する（ステップＳ７０３）。

【００９０】

一方、ステップＳ７０２にて、ユーザが自分用の「ＩＭＳＩ固有フォルダ」内に保存することを指示したと判断した場合、中央制御ユニット３は、電源投入に際して先に実行した制御処理（図５）のステップＳ５０５において一時記憶しているＩＭＳＩが存在するか否かを判断する（ステップＳ７０４）。

【００９１】

ステップＳ７０４にてＮＯ判定の場合は、携帯電話機１００内に当該ユーザのための「ＩＭＳＩ固有フォルダ」が存在しない、またはＵＩＭカード８が装着されていないことを表す。そこで、中央制御ユニット３は、このような場合には処理を完了する（ステップＳ７１１）。

【００９２】

一方、ステップＳ７０４にてＹＥＳ判定の場合は、一時記憶しているＩＭＳＩが存在する。そこで、中央制御ユニット３は、一時記憶されている当該ＩＭＳＩに対応するフォルダ（即ち、当該ＩＭＳＩに関連付けされた「ＩＭＳＩ固有フォルダ」）が存在するか否かを判断する（ステップＳ７０５）。

【００９３】

ステップＳ７０５の判定にて「ＩＭＳＩ固有フォルダ」が存在すると判断された場合、中央制御ユニット３は、ステップＳ７０６にて暗号処理ソフトウエア・プログラム１３を起動した後、ステップＳ７０１にて保存を指定されているユーザデータを、当該ＩＭＳＩを基に暗号鍵を生成すると共に、その暗号鍵を利用して暗号化する（ステップＳ７０７）。そして、中央制御ユニット３は、ステップＳ７０７にて暗号化したユーザデータを、不揮発メモリ１１内の当該ＩＭＳＩに関連付けされている「ＩＭＳＩ固有フォルダ」に保存する（ステップＳ７０８）。

【００９４】

一方、ステップＳ７０５にて対応する「ＩＭＳＩ固有フォルダ」が存在しないと判断された場合であっても、ステップＳ７０４にてＹＥＳ判定の場合は、一時記憶しているＩＭＳＩが存在する。そこで、この場合、中央制御ユニット３は、当該ＩＭＳＩに対応する「ＩＭＳＩ固有フォルダ」を新たに作成するかを判断する（ステップＳ７０９）。

【００９５】

即ち、ステップＳ７０９において、中央制御ユニット３は、ユーザに対して、現時点で

「ＩＭＳＩ固有フォルダ」が存在しないことの報知と、当該ユーザのための新たな「ＩＭＳＩ固有フォルダ」の作成を行うか否かの選択操作の要求とを行う。

【００９６】

そして、ステップＳ７０９にてＹＥＳ判定の場合、中央制御ユニット３は、当該ＩＭＳＩ対応する「ＩＭＳＩ固有フォルダ」を新たに作成する。即ち、この処理ステップ以降、携帯電話機１００の内部には、当該新たに作成された「ＩＭＳＩ固有フォルダ」が、当該ＩＭＳＩとの関連付けを表す情報と共に、不揮発メモリ１１内に記憶される。

【００９７】

その後、中央制御ユニット３は、処理をステップＳ７０５に進め、上述したステップＳ７０６乃至ステップＳ７０８の処理が行われ、当該「ＩＭＳＩ固有フォルダ」には暗号化されたユーザデータが記憶される。

【００９８】

[実施形態の効果]

以上説明した本実施形態では、ＵＩＭカード８等の記憶媒体（ＩＣカード）により加入者情報（ＩＭＳＩ）と本体とを分離した状態で保有可能な携帯端末（携帯電話機１００）を前提とした。そして、係る携帯端末において、その携帯端末内のユーザデータ（個人用コンテンツ）を、ＵＩＭカード内の識別情報(ＩＭＳＩ)と関連付けた状態で、その識別情報に対応する固有のフォルダ（ＩＭＳＩ固有フォルダ）内に暗号化して記憶することができる。また、当該フォルダに暗号化して記憶されたユーザデータは、対応する識別情報が記憶されたＵＩＭカードが当該携帯端末に装着された場合以外は閲覧できない。

【００９９】

このような本実施形態によれば、所謂第３世代の携帯電話機のように１台の携帯端末が複数の契約者によって共有利用される場合であっても、自分以外の他人のユーザデータの閲覧、変更等を禁止することができる。

【０１００】

また、本実施形態に係る携帯端末の装置構成によれば、ＵＩＭカードなしで携帯電話機の電源を投入した場合には、内部に記憶されているユーザデータを復号化することができない。このため、内部のユーザデータを閲覧することはできない。

【０１０１】

即ち、本実施形態によれば、着脱可能な記憶媒体に記憶されている識別情報に従ってユーザを識別する１台の携帯端末を複数のユーザ間で共有する場合であても、個々人のユーザデータの管理を強固にすることができ、プライバシーの保護を図ることができる。

【０１０２】

また、上述した本実施形態による効果は、ユーザが携帯電話機１００の本体と、ＵＩＭカード８とを携帯していれば実現する。従って、本実施形態によれば、携帯電話機の本体と、契約者情報が記憶されたＩＣカードとに加えて、更に他の記憶媒体が必要な従来の技術とは異なり、ユーザの利便性が格段に向上する。

【０１０３】

ここで、上述した本実施形態の効果は、以下に説明する変形例によっても享受することができる。

【０１０４】

＜実施形態の第１変形例＞

上述した実施形態では、暗号化及び復号化処理に使用する鍵情報（暗号鍵）を生成するに際して、識別情報としてＩＭＳＩを利用した。また、ユーザ毎の固有のフォルダへの関連付けに際して、識別情報としてＩＭＳＩを利用した。これに対して、本変形例では、係る識別情報として、ＩＣカードであるＵＩＭカードに固有のシリアル番号を使用する。

【０１０５】

＜実施形態の第２変形例＞

上述した実施形態では、暗号化されたユーザデータを、可変サイズのファイル化されたデータファイルとして管理するに際して、ファイル管理情報（ファイル管理テーブル）に

よる動的な管理を行った。これに対して、本変形例では、不揮発メモリ１１に図３－Ａに示した如く固定領域を確保することにより、係る暗号化されたユーザデータに対して静的な管理を行う。但し、この場合、携帯電話機１００を複数のユーザで共有する使用形態では、ユーザ毎に固定領域を割当てることは無駄が多い。

【０１０６】

そこで、本変形例では、個々の固定領域のヘッダ部分にタグを付与しておく。そして暗号化された個人用コンテンツの復号に際しては、装着されたＵＩＭカード８から読み出された識別情報に従って当該タグを参照することにより、対象となるユーザのための特定の固定領域を判断する。

【０１０７】

＜実施形態の第３変形例＞

上述した実施形態では、あるユーザを特定するＩＭＳＩに関連付けされた「ＩＭＳＩ固有フォルダ」が不揮発メモリ１１内に存在していない場合、ステップＳ７０９において、新たに「ＩＭＳＩ固有フォルダ」を作成するか否かの選択操作をユーザに要求した。これに対して、本変形例では、ステップＳ７０９の処理を省略することにより、ステップＳ７０５の判断にて「ＩＭＳＩ固有フォルダ」が存在していないと判断された場合には、新たな「ＩＭＳＩ固有フォルダ」を自動的に作成する。

【０１０８】

＜実施形態の第４変形例＞

本変形例では、ＵＩＭカード８が装着された状態において、ＩＭＳＩに関連付けされた「ＩＭＳＩ固有フォルダ」が不揮発メモリ１１内に存在する場合に、そのフォルダに関連付けされたサブフォルダ（副記憶領域）を、ユーザによる設定操作に応じて設定可能な装置構成とする。このような装置構成によれば、ユーザの利便性を更に向上することができる。

【０１０９】

＜実施形態の第５変形例＞

本変形例では、閲覧可能な状態の個人用コンテンツ（即ち、復号化されたユーザデータ）を、ユーザの操作に応じて、「共有フォルダ」に移動及び複写することが可能な装置構成を採用する。更に好適な態様として、「共有フォルダ」に保存されているコンテンツ（共有データ）を、ユーザの操作に応じて、「ＩＭＳＩ固有フォルダ」に移動及び複写することが可能な装置構成を採用する。

【０１１０】

但し、上記の移動及び複写操作を可能とする携帯電話機１００の状態として、ＵＩＭカード８が装着され、且つＩＭＳＩに関連付けされた「ＩＭＳＩ固有フォルダ」が不揮発メモリ１１内に存在することにより、個人用コンテンツの閲覧が可能な状態にあることを前提とする。このような本変形例によれば、複数のユーザ間で装置だけでなく情報共有も行う際の利便性を向上することができる。

【０１１１】

尚、上述した実施形態においては、本発明を携帯電話機に適用して説明した。しかしながら、本発明に係る携帯端末は携帯電話機への適用に限られるものではない。より具体的な例として、本発明は、ＩＣカード等の着脱可能な記憶媒体を使用可能なＰＤＡ（Personal Digital Assistance：携帯情報端末）等にも適用可能である。

【０１１２】

また、上述した実施形態を例に説明した本発明は、上述した携帯電話１００に対して、その説明において参照したフローチャートの機能を実現可能なコンピュータ・プログラムを供給した後、その装置のＣＰＵに読み出して実行することによって達成される。また、当該装置内に供給されたコンピュータ・プログラムは、読み書き可能なメモリ（例えば不揮発メモリ１１）等の記憶デバイスに格納すれば良い。

【０１１３】

また、前記の場合において、当該各装置内へのコンピュータ・プログラムの供給方法は

、例えばＵＩＭカード８と物理的に共通規格のＩＣカード（或いはメモリカード）等の各種記録媒体を介して当該装置内にインストールする方法や、インターネット等の通信回線を介して外部よりダウンロードする方法等のように、現在では一般的な手順を採用することができ、このような場合において、本発明は、係るコンピュータ・プログラムのコード或いは記憶媒体によって構成される。

【図面の簡単な説明】

【０１１４】

【図１】本実施形態に係る携帯電話機１００において行われるユーザデータの管理手法を概念的に示す図である。

【図２】本発明を適用可能な携帯電話機の一般的な装置構成例を示すブロック図である。

【図３－Ａ】情報処理装置においてデータを静的に管理する場合を概念的に示す図である。

【図３－Ｂ】情報処理装置においてデータを動的に管理する場合を概念的に示す図である。

【図４】本実施形態に係る携帯電話機１００において行われるユーザデータの管理手法により、復号化されたユーザデータと、暗号化されたユーザデータとが同電話機内に存在する状態を概念的に示す図である。

【図５】本実施形態における携帯電話機１００の電源投入時の制御処理のフローチャートである。

【図６】本実施形態における携帯電話機１００のユーザデータ読み出し時の制御処理のフローチャートである。

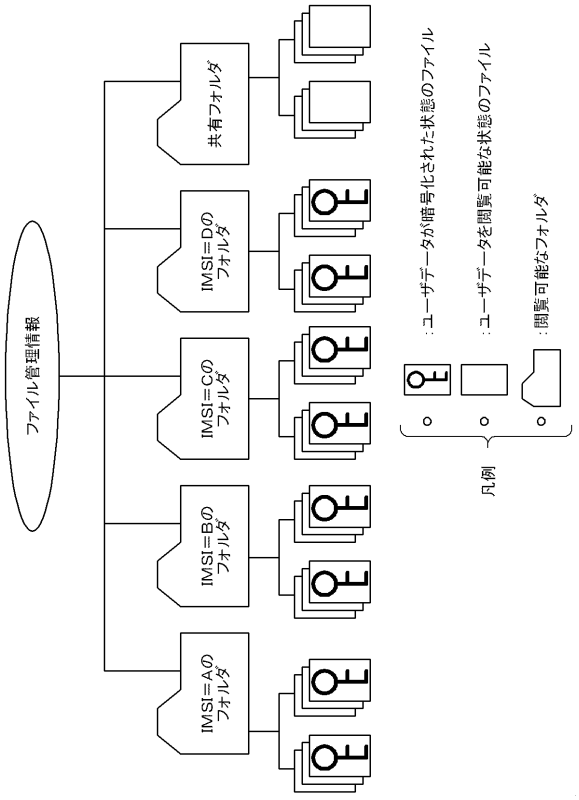
【図７】本実施形態における携帯電話機１００のユーザデータ保存時の制御処理のフローチャートである。

【符号の説明】

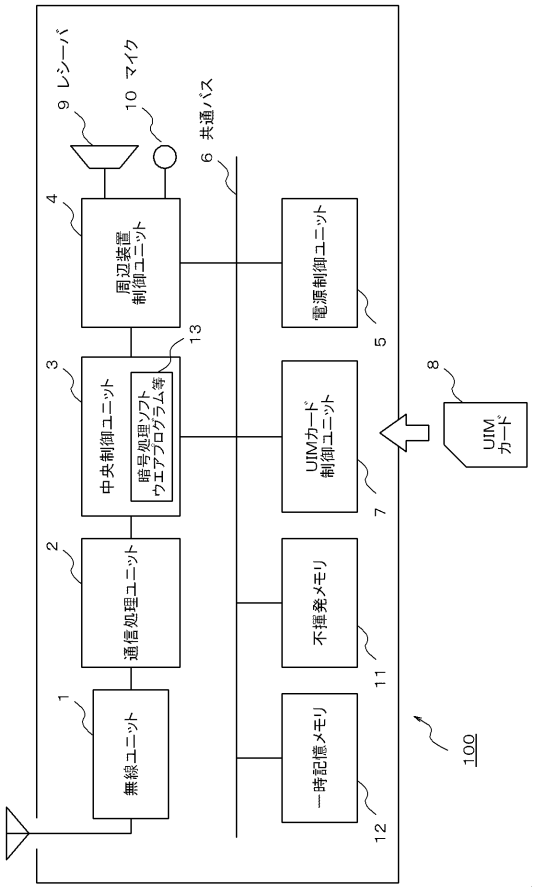
【０１１５】

１　無線ユニット
２　通信処理ユニット
３　中央制御ユニット
４　周辺装置制御ユニット
５　電源制御ユニット
６　共通バス
７　ＵＩＭカード制御ユニット
８　ＵＩＭカード
９　レシーバ（スピーカ）
１０　マイク
１１　不揮発性メモリ
１２　一時記憶メモリ
１３　暗号処理ソフトウエア・プログラム
１００　携帯電話機

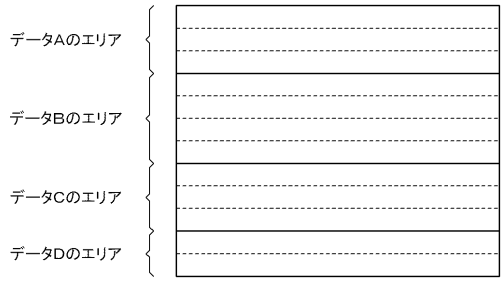
【図１】



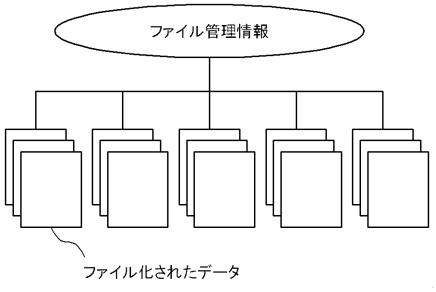
【図２】



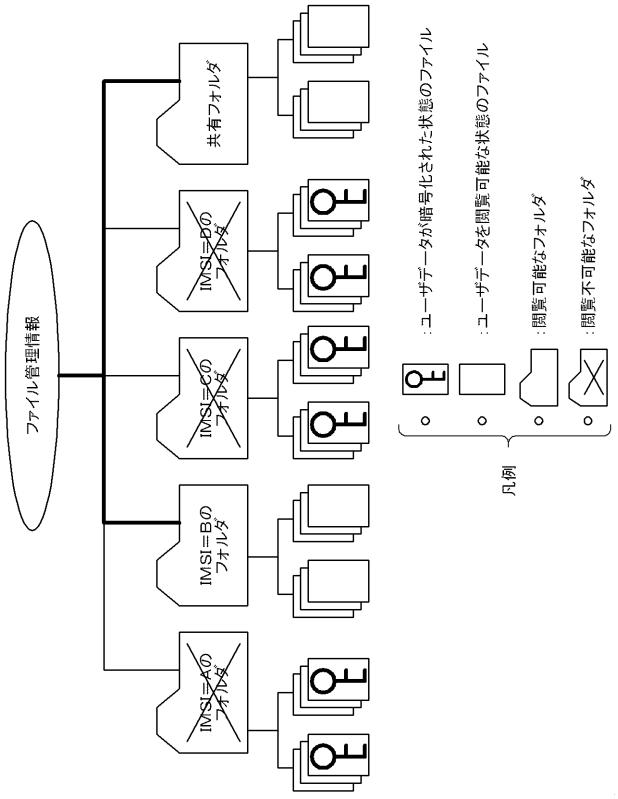
【図３－Ａ】



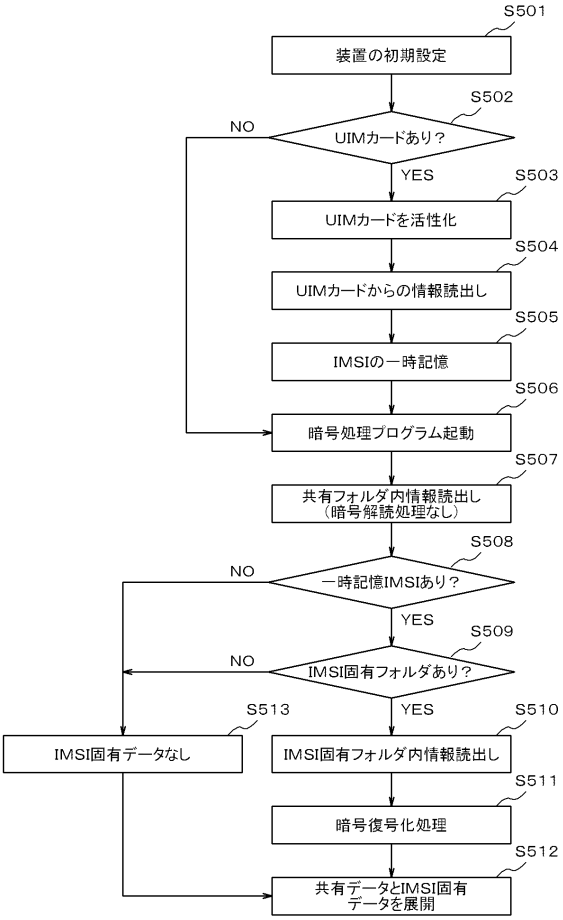
【図３－Ｂ】



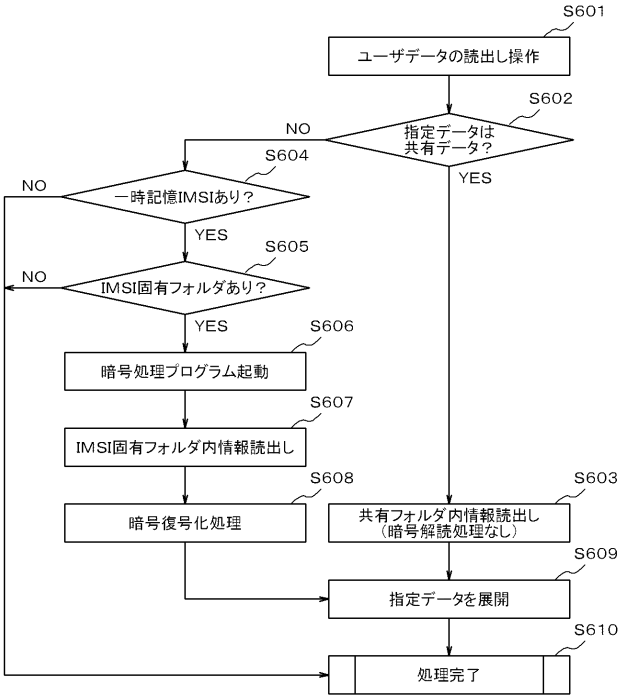
【図４】



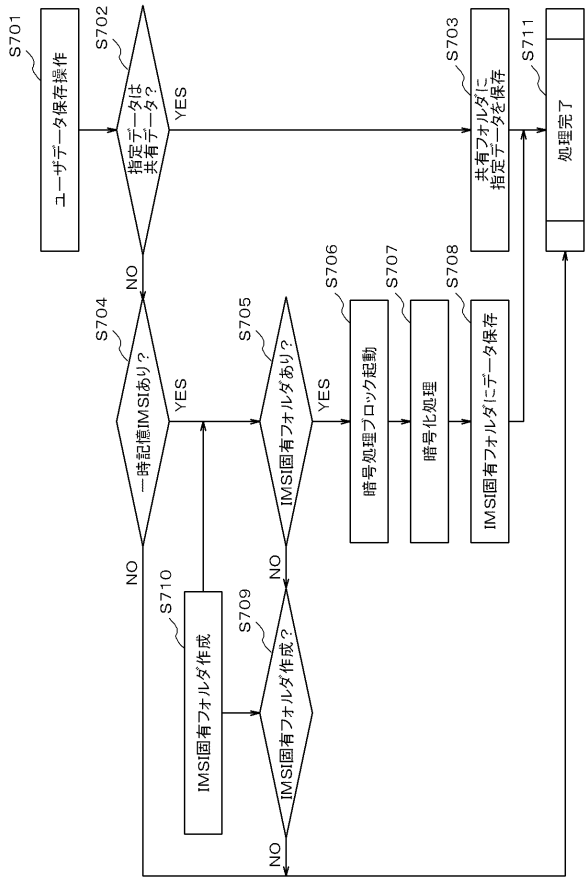
【図５】


S501
装置の初期設定
S502
UIMカードあり？
NO
YES
S503
UIMカードを活性化
S504
UIMカードからの情報読出し
S505
IMSIの一時記憶
S506
暗号処理プログラム起動
S507
共有フォルダ内情報読出し
（暗号解読処理なし）
S508
一時記憶IMSIあり？
NO
YES
S509
IMSI固有フォルダあり？
NO
YES
S513
IMSI固有データなし
S510
IMSI固有フォルダ内情報読出し
S511
暗号復号化処理
S512
共有データとIMSI固有
データを展開

【図６】


S601
ユーザデータの読出し操作
S602
指定データは
共有データ？
NO
YES
S604
一時記憶IMSIあり？
NO
YES
S605
IMSI固有フォルダあり？
NO
YES
S606
暗号処理プログラム起動
S607
IMSI固有フォルダ内情報読出し
S608
暗号復号化処理
S603
共有フォルダ内情報読出し
（暗号解読処理なし）
S609
指定データを展開
S610
処理完了

【図７】


S701
ユーザデータ保存操作
S702
指定データは
共有データ？
YES
NO
S703
共有フォルダに
指定データを保存
S711
処理完了
S704
一時記憶IMSIあり？
YES
NO
S705
IMSI固有フォルダあり？
YES
NO
S706
暗号処理ブロック起動
S707
暗号化処理
S708
IMSI固有フォルダにデータ保存
S709
IMSI固有フォルダ作成？
NO
S710
IMSI固有フォルダ作成