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

特許第4950730号
(P4950730)

(45)発行日　平成24年6月13日(2012.6.13)　(24)登録日　平成24年3月16日(2012.3.16)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	21/24	163D
G06F 21/02	(2006.01)	G06F	21/02	179A
G06K 19/07	(2006.01)	G06K	19/00	N

請求項の数 3　(全 11 頁)

(21)出願番号　特願2007-86139(P2007-86139)
(22)出願日　平成19年3月29日(2007.3.29)
(65)公開番号　特開2008-243099(P2008-243099A)
(43)公開日　平成20年10月9日(2008.10.9)
審査請求日　平成21年9月4日(2009.9.4)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100084618
弁理士　村松　貞男

最終頁に続く

(54)【発明の名称】携帯可能電子装置、携帯可能電子装置におけるファイルアクセス方法およびＩＣカード

(57)【特許請求の範囲】

【請求項１】

メモリを有し、このメモリには少なくとも１つのレコード構造のエレメンタリファイルが設定され、このエレメンタリファイルには複数のレコードが格納されていて、外部から入力される命令を解釈して実行することで、前記エレメンタリファイルに対しアクセスする携帯可能電子装置において、

外部から入力され、少なくともアクセス対象レコードを指定するレコード識別子および当該レコード識別子で指定されるレコードが格納されているファイルを指定するファイル識別子を示すパラメータデータから構成され、レコードに対するデータの書込み、書換え、読出し、削除、レコードの追加のうち少なくともいずれか１つを実行するための命令を受信する受信手段と、

前記受信手段により受信される命令を実行するためのアクセス条件であって、当該アクセス条件に沿ってレコードのアクセス可否を判断する命令の実行前に実行された照合命令に基づく照合キーの照合結果、認証命令に基づく認証キーによる認証結果、あるいは、レコードをアクセスする命令自身のセキュアメッセージング処理の有無を前記レコードごとに設定するアクセス条件設定手段と、

前記受信手段により前記命令を受信すると、当該命令のパラメータデータの正当性を確認する確認手段と、

前記確認手段による確認の結果、当該命令のパラメータデータの正当性が確認できた場合、当該命令のパラメータデータにより指定されたレコードのアクセス条件を当該アクセ

ス対象レコードに対して許容できるか否かを判定する判定手段と、
前記判定手段による判定の結果、当該アクセス対象レコードに対して処理が許容される場合、前記受信手段により受信される命令を実行することにより、当該アクセス対象レコードに対してアクセスするアクセス制御手段と、
を具備する携帯可能電子装置。
【請求項２】
メモリを有し、このメモリには少なくとも１つのレコード構造のエレメンタリファイルが設定され、このエレメンタリファイルには複数のレコードが格納されていて、外部から入力される命令を解釈して実行することで、前記エレメンタリファイルに対しアクセスする携帯可能電子装置におけるファイルアクセス方法であって、
外部から入力され、少なくともアクセス対象レコードを指定するレコード識別子および当該レコード識別子で指定されるレコードが格納されているファイルを指定するファイル識別子を示すパラメータデータから構成され、レコードに対するデータの書込み、書換え、読出し、削除、レコードの追加のうち少なくともいずれか１つを実行するための命令を受信する受信ステップと、
前記受信ステップにより受信される命令を実行するためのアクセス条件であって、当該アクセス条件に沿ってレコードのアクセス可否を判断する命令の実行前に実行された照合命令に基づく照合キーの照合結果、認証命令に基づく認証キーによる認証結果、あるいは、レコードをアクセスする命令自身のセキュアメッセージング処理の有無を前記レコードごとに設定するアクセス条件設定ステップと、
前記受信ステップにより前記命令を受信すると、当該命令のパラメータデータの正当性を確認する確認ステップと、
前記確認ステップによる確認の結果、当該命令のパラメータデータの正当性が確認できた場合、当該命令のパラメータデータにより指定されたレコードのアクセス条件を当該アクセス対象レコードに対して許容できるか否かを判定する判定ステップと、
前記判定ステップによる判定の結果、当該アクセス対象レコードに対して処理が許容される場合、前記受信ステップにより受信される命令を実行することにより、当該アクセス対象レコードに対してアクセスするアクセス制御ステップと、
を具備する携帯可能電子装置におけるファイルアクセス方法。
【請求項３】
メモリを有し、このメモリには少なくとも１つのレコード構造のエレメンタリファイルが設定され、このエレメンタリファイルには複数のレコードが格納されていて、外部から入力される命令を解釈して実行することで、前記エレメンタリファイルに対しアクセスするＩＣカードにおいて、
外部から入力され、少なくともアクセス対象レコードを指定するレコード識別子および当該レコード識別子で指定されるレコードが格納されているファイルを指定するファイル識別子を示すパラメータデータから構成され、レコードに対するデータの書込み、書換え、読出し、削除、レコードの追加のうち少なくともいずれか１つを実行するための命令を受信する受信手段と、前記受信手段により受信される命令を実行するためのアクセス条件であって、当該アクセス条件に沿ってレコードのアクセス可否を判断する命令の実行前に実行された照合命令に基づく照合キーの照合結果、認証命令に基づく認証キーによる認証結果、あるいは、レコードをアクセスする命令自身のセキュアメッセージング処理の有無を前記レコードごとに設定するアクセス条件設定手段と、前記受信手段により前記命令を受信すると、当該命令のパラメータデータの正当性を確認する確認手段と、前記確認手段による確認の結果、当該命令のパラメータデータの正当性が確認できた場合、当該命令のパラメータデータにより指定されたレコードのアクセス条件を当該アクセス対象レコードに対して許容できるか否かを判定する判定手段と、前記判定手段による判定の結果、当該アクセス対象レコードに対して処理が許容される場合、前記受信手段により受信される命令を実行することにより、当該アクセス対象レコードに対してアクセスするアクセス制御手段とを有したＩＣモジュールと、

このＩＣモジュールを収納したＩＣカード本体と、
を具備するＩＣカード。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、たとえば、データを保持する不揮発性メモリを有し、このメモリには少なくとも１つのファイルが設定され、このファイルには複数のレコードが格納されていて、外部から入力されるコマンド（命令）を解釈して実行することで、前記ファイルに対しアクセスするＩＣカードなどの携帯可能電子装置、および携帯可能電子装置におけるファイルアクセス方法、およびＩＣカードに関する。
【背景技術】
【０００２】
この種のＩＣカードにあっては、その内部の不揮発性メモリに保持するデータについて、デディケイトファイル（ＤＦ：Ｄｅｄｉｃａｔｅｄ　Ｆｉｌｅ）やエレメンタリファイル（ＥＦ：Ｅｌｅｍｅｎｔａｒｙ　Ｆｉｌｅ、以降、単にファイルともいう）など、ファイルを単位としたファイル管理を行なう方法が一般的である（たとえば、特許文献１参照）。
【０００３】
また、このようなＩＣカードにおいて、コマンドは、ファイル（ＥＦ）に対してアクセス条件を設定し、このアクセス条件に基づき、コマンドによるアクセス制御を行なっている（たとえば、特許文献２参照）。
【特許文献１】特許第２６９５８５７号公報
【特許文献２】特開平８－２６３３５３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかし、最近、１つのファイル（ＥＦ）に複数のレコードが格納されている場合があり、その場合、従来のアクセス制御方式では、アクセス制御はファイル単位で行なうため、レコードごとのアクセス制御を行なうことはできないという問題がある。
【０００５】
そこで、本発明は、レコードごとにアクセス条件を設定することにより、従来のファイルに対してアクセス条件を設定した場合よりも細かなアクセス制御を行なうことが可能となる携帯可能電子装置、携帯可能電子装置におけるファイルアクセス方法およびＩＣカード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】
【０００６】
本発明の携帯可能電子装置は、メモリを有し、このメモリには少なくとも１つのレコード構造のエレメンタリファイルが設定され、このエレメンタリファイルには複数のレコードが格納されていて、外部から入力される命令を解釈して実行することで、前記エレメンタリファイルに対しアクセスする携帯可能電子装置において、外部から入力され、少なくともアクセス対象レコードを指定するレコード識別子および当該レコード識別子で指定されるレコードが格納されているファイルを指定するファイル識別子を示すパラメータデータから構成され、レコードに対するデータの書込み、書換え、読出し、削除、レコードの追加のうち少なくともいずれか１つを実行するための命令を受信する受信手段と、前記受信手段により受信される命令を実行するためのアクセス条件であって、当該アクセス条件に沿ってレコードのアクセス可否を判断する命令の実行前に実行された照合命令に基づく照合キーの照合結果、認証命令に基づく認証キーによる認証結果、あるいは、レコードをアクセスする命令自身のセキュアメッセージング処理の有無を前記レコードごとに設定するアクセス条件設定手段と、前記受信手段により前記命令を受信すると、当該命令のパラメータデータの正当性を確認する確認手段と、前記確認手段による確認の結果、当該命令

のパラメータデータの正当性が確認できた場合、当該命令のパラメータデータにより指定されたレコードのアクセス条件を当該アクセス対象レコードに対して許容できるか否かを判定する判定手段と、前記判定手段による判定の結果、当該アクセス対象レコードに対して処理が許容される場合、前記受信手段により受信される命令を実行することにより、当該アクセス対象レコードに対してアクセスするアクセス制御手段とを具備する。

【０００７】

本発明の携帯可能電子装置におけるファイルアクセス方法は、メモリを有し、このメモリには少なくとも１つのレコード構造のエレメンタリファイルが設定され、このエレメンタリファイルには複数のレコードが格納されていて、外部から入力される命令を解釈して実行することで、前記エレメンタリファイルに対しアクセスする携帯可能電子装置におけるファイルアクセス方法であって、外部から入力され、少なくともアクセス対象レコードを指定するレコード識別子および当該レコード識別子で指定されるレコードが格納されているファイルを指定するファイル識別子を示すパラメータデータから構成され、レコードに対するデータの書込み、書換え、読出し、削除、レコードの追加のうち少なくともいずれか１つを実行するための命令を受信する受信ステップと、前記受信ステップにより受信される命令を実行するためのアクセス条件であって、当該アクセス条件に沿ってレコードのアクセス可否を判断する命令の実行前に実行された照合命令に基づく照合キーの照合結果、認証命令に基づく認証キーによる認証結果、あるいは、レコードをアクセスする命令自身のセキュアメッセージング処理の有無を前記レコードごとに設定するアクセス条件設定ステップと、前記受信ステップにより前記命令を受信すると、当該命令のパラメータデータの正当性を確認する確認ステップと、前記確認ステップによる確認の結果、当該命令のパラメータデータの正当性が確認できた場合、当該命令のパラメータデータにより指定されたレコードのアクセス条件を当該アクセス対象レコードに対して許容できるか否かを判定する判定ステップと、前記判定ステップによる判定の結果、当該アクセス対象レコードに対して処理が許容される場合、前記受信ステップにより受信される命令を実行することにより、当該アクセス対象レコードに対してアクセスするアクセス制御ステップとを具備する。

【０００８】

本発明のＩＣカードは、メモリを有し、このメモリには少なくとも１つのレコード構造のエレメンタリファイルが設定され、このエレメンタリファイルには複数のレコードが格納されていて、外部から入力される命令を解釈して実行することで、前記エレメンタリファイルに対しアクセスするＩＣカードにおいて、外部から入力され、少なくともアクセス対象レコードを指定するレコード識別子および当該レコード識別子で指定されるレコードが格納されているファイルを指定するファイル識別子を示すパラメータデータから構成され、レコードに対するデータの書込み、書換え、読出し、削除、レコードの追加のうち少なくともいずれか１つを実行するための命令を受信する受信手段と、前記受信手段により受信される命令を実行するためのアクセス条件であって、当該アクセス条件に沿ってレコードのアクセス可否を判断する命令の実行前に実行された照合命令に基づく照合キーの照合結果、認証命令に基づく認証キーによる認証結果、あるいは、レコードをアクセスする命令自身のセキュアメッセージング処理の有無を前記レコードごとに設定するアクセス条件設定手段と、前記受信手段により前記命令を受信すると、当該命令のパラメータデータの正当性を確認する確認手段と、前記確認手段による確認の結果、当該命令のパラメータデータの正当性が確認できた場合、当該命令のパラメータデータにより指定されたレコードのアクセス条件を当該アクセス対象レコードに対して許容できるか否かを判定する判定手段と、前記判定手段による判定の結果、当該アクセス対象レコードに対して処理が許容される場合、前記受信手段により受信される命令を実行することにより、当該アクセス対象レコードに対してアクセスするアクセス制御手段とを有したＩＣモジュールと、このＩＣモジュールを収納したＩＣカード本体とを具備する。

【発明の効果】

【０００９】

本発明によれば、レコードごとにアクセス条件を設定することにより、従来のファイルに対してアクセス条件を設定した場合よりも細かなアクセス制御を行なうことが可能となる携帯可能電子装置、携帯可能電子装置におけるファイルアクセス方法およびＩＣカードを提供できる。

【発明を実施するための最良の形態】

【００１０】

以下、本発明の実施の形態について図面を参照して説明する。

図１は、本発明に係る携帯可能電子装置としてのＩＣカードを取扱うＩＣカードシステムの構成例を示すものである。このＩＣカードシステムは、ＩＣカード１０１を外部装置としてのカードリーダ・ライタ１０２を介して端末装置１０３と接続可能にするとともに、端末装置１０３にキーボード１０４、ＣＲＴ表示部１０５、プリンタ１０６を接続して構成される。

【００１１】

ＩＣカード１０１は、カードリーダ・ライタ１０２からの電源供給により動作可能な状態となり、カードリーダ・ライタ１０２から供給されるコマンドに応じて種々の処理を実行する。カードリーダ・ライタ１０２は、ＩＣカード１０１に対し動作電源を供給するとともに種々の処理を要求するコマンドを供給する。

【００１２】

ここに、カードリーダ・ライタ１０２からＩＣカード１０１に供給されるコマンドの内容は、レコードの操作（アクセス）であり、たとえば、レコードに対するデータの書込み、書換え、読出し、削除、レコードの追加のうち少なくともいずれか１つである。

【００１３】

端末装置１０３は、たとえば、パーソナルコンピュータなどにより構成されていて、図示しないメモリに記憶されている各種制御プログラムを実行することにより、各種の処理を実行するとともに、カードリーダ・ライタ１０２を介してＩＣカード１０１との間でデータの入出力を行なう。

【００１４】

図２は、ＩＣカード１０１の構成を示すもので、制御素子としてのＣＰＵ２０１、記憶内容が書換え可能な記憶手段（メモリ）としてのデータメモリ２０２、ワーキングメモリ２０３、プログラムメモリ２０４、および、カードリーダ・ライタ１０２との通信を行なうための通信部２０５によって構成されている。そして、これらのうち、破線内の部分（ＣＰＵ２０１、データメモリ２０２、ワーキングメモリ２０３、プログラムメモリ２０４）は１つ（あるいは複数）のＩＣチップ２０６で構成され、さらに、このＩＣチップ２０６と通信部２０５とが一体的にＩＣモジュール化されて、ＩＣカード本体１０１ａ内に埋設されている。

【００１５】

ＣＰＵ２０１は、各種の判定処理や判断処理およびメモリへの書込みや読出しなどの各種のデータ処理を行なう制御部である。

【００１６】

データメモリ２０２は、たとえば、ＥＥＰＲＯＭ（エレクトリカリ・イレーザブル・アンド・プログラマブル・リード・オンリ・メモリ）などの消去（書換え）可能な不揮発性メモリで構成されていて、各種アプリケーションデータなどの各種データがファイル構造で記憶される。

【００１７】

ワーキングメモリ２０３は、ＣＰＵ２０１が処理を行なう際の処理データを一時的に保持するための作業用のメモリであり、たとえば、ＲＡＭ（ランダム・アクセス・メモリ）などの揮発性メモリで構成されている。

【００１８】

プログラムメモリ２０４は、たとえば、マスクＲＯＭ（リード・オンリ・メモリ）などの書換え不可能な固定メモリで構成されており、ＣＰＵ２０１の制御プログラムなどを記

憶している。

【００１９】

通信部２０５は、ＩＣカード１０１が非接触式（無線式）ＩＣカードの場合にはアンテナ部として構成され、カードリーダ・ライタ１０２から送信された変調波を非接触で受信したり外部へ変調波を発信したりするようになっている。また、この通信部２０５で受信した変調波から内部回路に供給するための電源やクロックを生成するようになっている。また、接触式ＩＣカードの場合にはコンタクト部として構成され、カードリーダ・ライタ１０２に設けられたＩＣカード端子部（図示しない）と接触することにより電源やクロックを得るようになっている。

【００２０】

図３は、データメモリ１０２の内部構造例を示すものである。この例では、３つのファイル（ＥＦ）が設定されている場合を示している。

データメモリ１０２内には、たとえば、レコード構造のＥＦ（以下、レコードＥＦと称す）を定義するレコードＥＦ定義情報(1)３０１、レコードＥＦ定義情報(2)３０２、レコードＥＦ定義情報(3)３０３、照合キーを格納する照合キーＥＦを定義する照合キーＥＦ定義情報３０４、認証キーを格納する認証キーＥＦを定義する認証キーＥＦ定義情報３０５、認証子生成鍵を格納する認証子生成鍵ＥＦを定義する認証子生成鍵ＥＦ定義情報３０６、データ暗号化鍵を格納するデータ暗号化鍵ＥＦを定義するデータ暗号化鍵ＥＦ定義情報３０７が格納されているとともに、レコードＥＦ定義情報(1)３０１で定義されるレコードＥＦ(1)３０８、レコードＥＦ定義情報(2)３０２で定義されるレコードＥＦ(2)３０９、レコードＥＦ定義情報(3)３０３で定義されるレコードＥＦ(3)３１０、照合キーＥＦ定義情報３０４で定義される照合キーＥＦ３１１、認証キーＥＦ定義情報３０５で定義される認証キーＥＦ３１２、認証子生成鍵ＥＦ定義情報３０６で定義される認証子生成鍵ＥＦ３１３、データ暗号化鍵ＥＦ定義情報３０７で定義されるデータ暗号化鍵ＥＦ３１４が格納されている。

【００２１】

図４は、ワーキングメモリ２０３の内部構造例を示すものである。ワーキングメモリ２０３は、照合キーの照合状態を格納する領域２０３ａおよび認証キーや認証子の認証状態を格納する領域２０３bを有している。

【００２２】

図５は、レコードＥＦ定義情報３０１，３０２，３０３の詳細を示している。この例では、１つのレコードＥＦに３つのレコードが格納されている場合を示している。

レコードＥＦ定義情報３０１，３０２，３０３は、当該レコードＥＦが定義される位置を示すアドレス４０１、当該レコードＥＦの識別情報としてのＥＦ－ＩＤ４０２、当該レコードＥＦのファイルタイプ４０３、レコードの長さを示すレコード長４０４、レコードの数（この例では「３」）を示すレコード数４０５、レコード(1)のアクセス条件を示すレコード(1)アクセス条件４０６、レコード(2)のアクセス条件を示すレコード(2)アクセス条件４０７、レコード(3)のアクセス条件を示すレコード(3)アクセス条件４０８を有して構成される。

【００２３】

ここに、レコードアクセス条件４０６，４０７，４０８としては、たとえば、データ読出処理のアクセス条件、データ書込処理のアクセス条件、データ追記処理のアクセス条件、データ書換処理のアクセス条件、セキュアメッセージング処理のアクセス条件などが考えられる。

【００２４】

データ読出処理のアクセス条件としては、読出禁止、照合キーの照合が成功したときに読出可能、認証キーの認証が成功したときに読出可能、照合キーの照合が成功あるいは認証キーの認証が成功したときに読出可能、照合キーの照合が成功し、かつ、認証キーの認証が成功したときに読出可能、読出しフリーなどが考えられる。

【００２５】

ここに、照合キーの照合とは、カードリーダ・ライタ１０２からの照合コマンドに付加された照合キーと照合キーＥＦ３１１内の照合キーとを照合し、両照合キーが一致したとき照合成功とし、両照合キーが一致しなかったとき照合不成功とすることを意味しており、その照合結果はワーキングメモリ２０３の照合状態格納領域２０３ａに格納される。この照合処理は、書込みや読出し等の実際の処理コマンドを実行する前に先立って行なわれる。

【００２６】

また、認証キーの認証とは、カードリーダ・ライタ１０２からの認証コマンドに付加された暗号化された認証用データを認証キーＥＦ３１２内の認証キーにより復号化し、正しく復号化されたとき認証成功とし、正しく復号化されなかったとき認証不成功とすることを意味しており、その認証結果はワーキングメモリ２０３の認証状態格納領域２０３ｂに格納される。この認証処理も、書込みや読出し等の実際の処理コマンドを実行する前に先立って行なわれる。

【００２７】

セキュアメッセージング処理のアクセス条件としては、セキュアメッセージング無し、認証子が必要、データ暗号化が必要、認証子およびデータ暗号化が必要などが考えられる。

ここに、認証子が必要とは、受信したコマンドの特定部（たとえば、ヘッダ部やデータ部等）のデータを認証子生成鍵ＥＦ３１３内の認証子生成鍵を用いて暗号化することで認証子を生成し、この生成した認証子と受信したコマンドに付加されている認証子とを照合し、両認証子が一致したとき認証成功とし、両認証子が一致しなかったとき認証不成功とすることを意味しており、その認証結果はワーキングメモリ２０３の認証状態格納領域２０３ｂに格納される。認証子の認証が成功したときにコマンド処理が行なわれる。

【００２８】

また、データ暗号化が必要とは、データ暗号化鍵ＥＦ３１４内のデータ暗号化鍵を用いてデータを復号化（暗号化）してからコマンド処理を行なうことを意味している。たとえば、データ書込コマンドの場合、当該コマンドに付加された書込みデータをデータ暗号化鍵ＥＦ３１４内のデータ暗号化鍵を用いて復号化してから、データメモリ１０２に対する書込み処理を行なう。また、たとえば、データ読出コマンドの場合、データメモリ１０２から当該コマンドで指定されたレコード（データ）を読出し、この読出したレコード（データ）をデータ暗号化鍵ＥＦ３１４内のデータ暗号化鍵を用いて暗号化してから、カードリーダ・ライタ１０２へ出力する。

【００２９】

また、認証子およびデータ暗号化が必要とは、認証子およびデータ暗号化が必要であり、上記したように認証子の認証が成功し、かつ、データ部を復号化（暗号化）してからコマンド処理を行なうことを意味している。

【００３０】

図６は、レコードＥＦ３０８，３０９，３１０に格納されるレコードを示している。この例では、１つのレコードＥＦに３つのレコードがある場合で、５０１はレコード(1)を示し、５０２はレコード(2)を示し、５０３はレコード(3)を示している。これらのレコード５０１，５０２，５０３は、たとえば、レコード管理情報（当該レコードのサイズ、次に続くレコードの位置情報等）と当該レコードのデータとから構成されている。

【００３１】

図７は、カードリーダ・ライタ１０２からＩＣカード１０１へ送られるコマンドのフォーマット例を示している。この例は、たとえば、データを書込む際のコマンドを示していて、コマンドを識別する機能などを持つ分類部（ＣＬＡ：ｃｌａｓｓ）８０１、命令部（ＩＮＳ：ｉｎｓｔｒｕｃｔｉｏｎ）８０２、パラメータデータ（Ｐ１、Ｐ２）８０３，８０４、書込むデータの長さを表すデータ長（Ｌｃ）８０５、および、書込みデータ（Ｄａｔａ）８０６から構成されている。

【００３２】

パラメータデータ（Ｐ１）８０３には、たとえば、データの書込み対象となるレコードを指定するデータ（レコード番号等）が格納され、パラメータデータ（Ｐ２）８０４には、たとえば、パラメータデータ（Ｐ１）８０３で指定されるレコードが格納されているファイル（レコードＥＦ）を示す識別子（ＥＦ－ＩＤ等）が格納される。

【００３３】

次に、このような構成において、カードリーダ・ライタ１０２からのコマンドに対するアクセス処理について図８に示すフローチャートを参照して説明する。

ＣＰＵ２０１は、カードリーダ・ライタ１０２から入力されるコマンドを受信すると（ステップＳ１）、当該コマンドとしての正当性を確認すべく、コマンドフォーマットのチェックを行なう（ステップＳ２）。このフォーマットチェックでは、たとえば、当該コマンドの分類部８０１および命令部８０２が正規のコマンドを示すものかどうかを確認し、パラメータデータ８０３，８０４が機能外に設定されていないかを確認し、データ長８０５が「００」などの規定外に設定されていないかを確認し、データ８０６がデータ長８０５で示されるデータ長のデータ列であるかを確認する。

【００３４】

ステップＳ２におけるフォーマットチェックの結果、フォーマットに異常が発見された場合、ＣＰＵ２０１は、フォーマットエラーを示すステータスワードを設定して、当該ステータスワードの出力処理を実行し（ステップＳ３）、当該処理を終了する。

【００３５】

ステップＳ２におけるフォーマットチェックの結果、フォーマットに異常が発見されなかった場合、ＣＰＵ２０１は、当該コマンドのパラメータデータ（Ｐ１）８０３に格納されたレコード番号は正しいか否かをチェックし（ステップＳ４）、正しくない場合、処理エラーを示すステータスワードを設定して、当該ステータスワードの出力処理を実行し（ステップＳ３）、当該処理を終了する。

【００３６】

ステップＳ４におけるチェックの結果、パラメータデータ（Ｐ１）８０３に格納されたレコード番号が正しい場合、ＣＰＵ２０１は、当該コマンドのパラメータデータ（Ｐ２）８０４に格納されたＥＦ－ＩＤは正しいか否かをチェックし（ステップＳ５）、正しくない場合、処理エラーを示すステータスワードを設定して、当該ステータスワードの出力処理を実行し（ステップＳ３）、当該処理を終了する。

【００３７】

ステップＳ５におけるチェックの結果、当該コマンドのパラメータデータ（Ｐ２）８０４に格納されたＥＦ－ＩＤが正しい場合、ＣＰＵ２０１は、当該コマンドのパラメータデータ（Ｐ２）８０４に格納されたＥＦ－ＩＤは、短縮ＥＦ識別子（Short EF Identifier）であるかカレントＥＦ識別子であるかをチェックし（ステップＳ６）、短縮ＥＦ識別子である場合、指定されたレコードＥＦをカレント状態にし（ステップＳ７）、ステップＳ８に進む。

ステップＳ６におけるチェックの結果、カレントＥＦ識別子である場合、ＣＰＵ２０１は、ステップＳ７をジャンプしてステップＳ８に進む。

【００３８】

ステップＳ８では、当該コマンドのパラメータデータ（Ｐ１）８０３により指定されたレコードのアクセス条件を、図３の対応するレコードＥＦ定義情報および図４の照合状態、認証状態を参照することによって、当該コマンド処理が対象となっているレコードに対して許容できるか否かを判定する。

【００３９】

ステップＳ８における判定の結果、対象レコードに対して処理が許容されない場合、ＣＰＵ２０１は、処理エラーを示すステータスワードを設定して、当該ステータスワードの出力処理を実行し（ステップＳ３）、当該処理を終了する。

【００４０】

ステップＳ８における判定の結果、対象レコードに対して処理が許容される場合、ＣＰ

Ｕ２０１は、当該レコードに対してコマンド処理（たとえば、データの書込みや読出し等）を実行し（ステップＳ９）、その後、当該処理が終了すると、正常終了を示すステータスワードを設定して、当該ステータスワードの出力処理を実行し（ステップＳ１０）、当該処理を終了する。

【００４１】

以上説明したように、上記実施の形態によれば、データを保持する不揮発性メモリを有し、このメモリには少なくとも１つのファイルが設定され、このファイルには複数のレコードが格納されていて、外部から入力されるコマンドを解釈して実行することで、前記ファイルに対しアクセスするＩＣカードにおいて、レコードごとにアクセス条件を設定することにより、従来のファイルに対してアクセス条件を設定した場合よりも細かなアクセス制御を行なうことが可能となる。

【００４２】

なお、前記実施の形態では、携帯可能電子装置としてＩＣカードに適用した場合について説明したが、本発明はこれに限定されるものではなく、たとえば、ＰＤＡと称される携帯端末装置や携帯電話機などであっても適用でき、また、形状もカード型に限らず、冊子型、ブロック形あるいはタグ型などであってもよい。

【図面の簡単な説明】

【００４３】

【図１】本発明に係る携帯可能電子装置としてのＩＣカードを取扱うＩＣカードシステムの構成例を示すブロック図。

【図２】ＩＣカードの構成を概略的に示すブロック図。

【図３】データメモリの内部構造例を示す模式図。

【図４】ワーキングメモリの内部構造例を示す模式図。

【図５】レコードＥＦ定義情報の詳細を示す構成図。

【図６】レコードＥＦに格納されるレコードを示す構成図。

【図７】ＩＣカードへ送られるコマンドのフォーマット例を示す模式図。

【図８】コマンドに対するアクセス処理について説明するフローチャート。

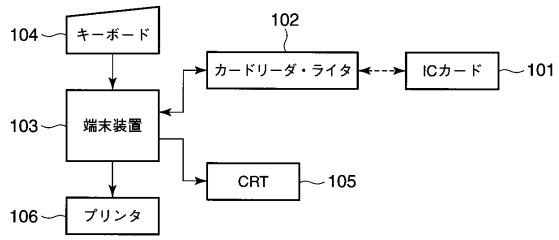
【符号の説明】

【００４４】

１０１…ＩＣカード（携帯可能電子装置）、１０１ａ…ＩＣカード本体、１０２…カードリーダ・ライタ、１０３…端末装置、１０４…キーボード、１０５…ＣＲＴ表示部、１０６…プリンタ、２０１…ＣＰＵ（制御素子）、２０２…データメモリ（記憶手段）、２０３…ワーキングメモリ、２０４…プログラムメモリ、２０５…通信部、２０６…ＩＣチップ、３０１，３０２，３０３…レコードＥＦ定義情報、３０８，３０９，３１０…レコードＥＦ（ファイル）、４０６，４０７，４０８…レコードアクセス条件。

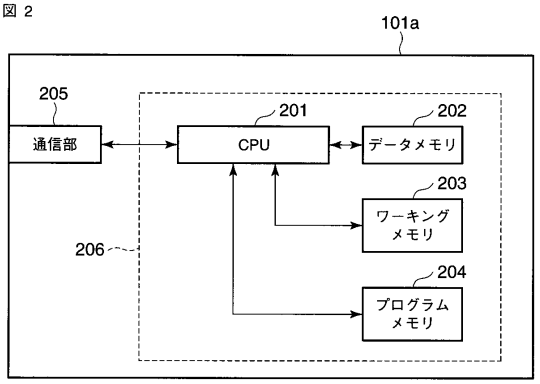
【図１】

図 1



【図２】

図 2

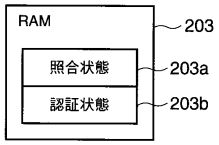


【図３】

図 3

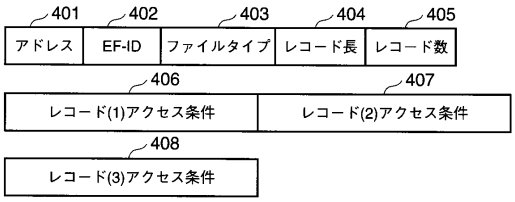
【図４】

図 4



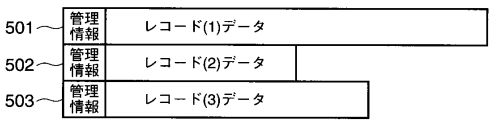
【図５】

図 5



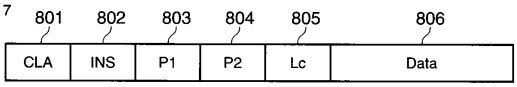
【図６】

図 6



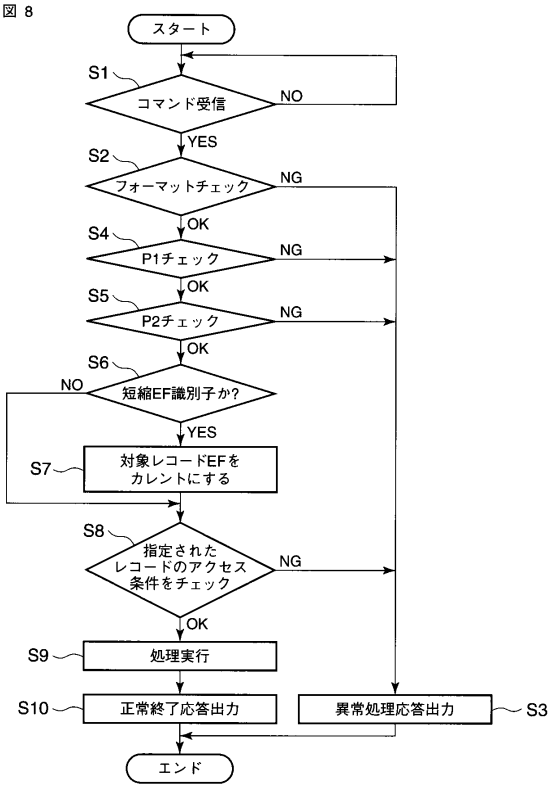
【図７】

図 7



【図８】

図 8



フロントページの続き

(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 福田 亜紀
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 後藤 彰

(56)参考文献 特開２００２－７４３０７（ＪＰ，Ａ）
特開２００１－２４３１１８（ＪＰ，Ａ）
特開平２－６４８８８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２４
Ｇ０６Ｆ ２１／０２
Ｇ０６Ｋ １９／０７