

(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2010-146410

(P2010-146410A)

(43) 公開日 平成22年7月1日(2010.7.1)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 F 12/00 (2006.01)	G 0 6 F 12/00 5 4 2 J	5 B 0 3 5
G 0 6 K 19/07 (2006.01)	G 0 6 K 19/00 N	5 B 0 8 2
	G 0 6 F 12/00 5 3 7 A	

審査請求 未請求 請求項の数 6 O L (全 14 頁)

(21) 出願番号	特願2008-324631 (P2008-324631)	(71) 出願人	000003078
(22) 出願日	平成20年12月19日 (2008.12.19)		株式会社東芝
			東京都港区芝浦一丁目1番1号
		(74) 代理人	100058479
			弁理士 鈴江 武彦
		(74) 代理人	100108855
			弁理士 蔵田 昌俊
		(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	100109830
			弁理士 福原 淑弘
		(74) 代理人	100075672
			弁理士 峰 隆司

最終頁に続く

(54) 【発明の名称】 携帯可能電子装置

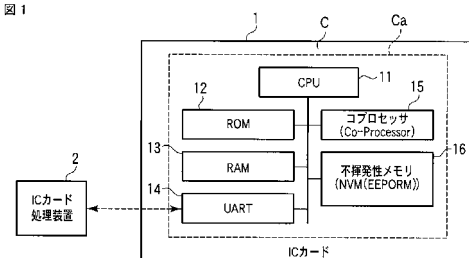
(57) 【要約】

【課題】複数チャネルでの確実なアクセス制御を実現でき、別のロジカルチャネルとカレント設定が競合する場合のコマンドに対する処理内容をアプリケーションごとに運用形態などに応じて設計できるICカード1を提供できる。

【解決手段】ICカード1において、オペレーティングシステム41がチャネル管理テーブル42aにより各ファイルに対する各チャネルのアクセス順番を管理し、アプリケーションがチャネル管理テーブル42aにより管理されるアクセス順番に基づいて各ファイルへのアクセスを制御する。上記チャネル管理テーブル42aでは、各ロジカルチャネルが各ファイルをカレントに設定した順番をアクセス順番として記憶する。特定のロジカルチャネルによるカレント設定が解除された場合、テーブル更新機能42bは、上記チャネル管理テーブル42aに記憶されている当該ロジカルチャネルを削除し、当該ロジカルチャネル以降のアクセス順番であった各ロジカルチャネルのアクセス順番を繰り上げる。

【選択図】 図1

図1



【特許請求の範囲】**【請求項 1】**

オペレーティングシステムプログラムを記憶する第 1 の記憶手段と、アプリケーションプログラムを記憶する第 2 の記憶手段と、ファイルを記憶する第 3 の記憶手段と、前記オペレーティングシステムプログラムおよび前記アプリケーションプログラムを実行する制御手段とを有する携帯可能電子装置であって、

前記オペレーティングシステムプログラムは、

前記第 3 の記憶手段に記憶しているファイルへアクセスするための複数のチャンネルを管理するチャンネル管理機能と、

前記チャンネル管理機能により管理される各チャンネルが前記第 3 の記憶手段に記憶しているファイルをカレント状態とした順番をアクセス順番として管理するアクセス順番管理機能と、

前記チャンネル管理機能により管理される第 1 のチャンネルが前記第 3 の記憶手段に記憶しているファイルに対するカレント状態を解除した場合、前記第 1 のチャンネルを当該ファイルに対するアクセス順番の管理対象から外し、前記第 1 のチャンネルよりもアクセス順番が後であった全チャンネルのアクセス順番を繰り上げるアクセス順番更新機能と、

前記第 3 の記憶手段に記憶しているファイルに対するチャンネルのアクセス順番を示す情報を前記第 2 の記憶手段に記憶しているアプリケーションプログラムへ提供する提供機能と、を有し、

前記アプリケーションプログラムは、

前記オペレーティングシステムプログラムから提供される前記ファイルに対するチャンネルのアクセス順番に基づいて、当該アプリケーションプログラムに割り当てられているチャンネルでの前記ファイルに対するアクセスを制御するアクセス制御機能を有する、

ことを特徴とする携帯可能電子装置。

【請求項 2】

前記アプリケーションプログラムのアクセス制御機能は、当該アプリケーションプログラムに割り当てられているチャンネルの前記ファイルに対するアクセス順番に応じて、前記ファイルに対するアクセスを制限する、

ことを特徴とする前記請求項 1 に記載の携帯可能電子装置。

【請求項 3】

前記アプリケーションプログラムのアクセス制御機能は、当該アプリケーションプログラムに割り当てられているチャンネルの前記ファイルに対するアクセス順番が最上位である場合に、前記ファイルに対して制限無しでアクセスする、

ことを特徴とする前記請求項 2 に記載の携帯可能電子装置。

【請求項 4】

前記アプリケーションプログラムのアクセス制御機能は、当該アプリケーションプログラムに割り当てられているチャンネルの前記ファイルに対するアクセス順番が最上位である場合には前記ファイルに対して制限無しでアクセスし、それ以外の場合には前記ファイルに対して一律の制限を加える、

ことを特徴とする前記請求項 1 に記載の携帯可能電子装置。

【請求項 5】

前記アプリケーションプログラムのアクセス制御機能は、前記ファイルに対してファイルの状態を変更する処理を実行する場合、当該アプリケーションプログラムに割り当てられているチャンネルの前記ファイルに対するアクセス順番が最上位でなければ、前記ファイルへのアクセスを禁止とする、

ことを特徴とする前記請求項 1 乃至 4 の何れか 1 項に記載の携帯可能電子装置。

【請求項 6】

前記アプリケーションプログラムのアクセス制御機能は、前記ファイルに対してファイルの状態を変更させない処理を実行する場合、前記ファイルに対するアクセス順番にかかわらず、前記ファイルへのアクセスを許可する、

ことを特徴とする前記請求項 1 乃至 5 の何れか 1 項に記載の携帯可能電子装置。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、たとえば、データの書込み、書換え可能な不揮発性メモリおよびCPUなどの制御素子を有したモジュールを内蔵し、外部から入力されるコマンドに対応した処理を実行するICカードなどの携帯可能電子装置に関する。

【背景技術】

【0002】

従来、携帯可能電子装置としては、たとえば、メモリやCPUなどの機能を有したICモジュールがプラスチック板などで構成される筐体内に埋設されているICカードがある。このようなICカードでは、外部装置からのコマンドに応じて書き換え可能な不揮発性メモリにデータを書き込んだり、不揮発性メモリからデータを読み出したりするようになっている。このようなICカードは、セキュリティの重要性から、入退出管理、クレジットカード、携帯電話機、電子商取引など様々な分野で利用されている。さらに、近年では、1つのICカードを様々な用途で利用するために、複数のアプリケーションを動作させる運用形態も多くなっている。

【0003】

一般に、ICカードと上位装置（端末）のデータの送受信は、ロジカルチャネルと呼ばれる「通信のためのチャネル」を経由して実施される。従来、一般的な運用形態では、ICカードと端末とが1対1で通信を行うことが多いため、1つのチャネルのみで処理が完結することが多い。ただし、近年では、1つのICカードと複数の端末とで通信を行うケースが増えてきている。これは、ICカードの基本性能が向上したこと、あるいは、外部との複数のインターフェース（接触型、非接触型、あるいは、高速タイプの接触型など）を有するICカードが多くなっていることなどが要因である。複数の端末と通信を行う場合、ICカードは、複数のチャネルを開設し、それぞれのチャネルがそれぞれの対象ファイル（あるいはアプリケーション）にアクセスする制御を行う。

【0004】

しかしながら、ICカードにおける各ファイルへのアクセスは、複数のチャネルごとに管理されていないのが現状である。つまり、従来のICカードでは、複数のチャネルから各ファイルに無条件にアクセスすることが可能となっている。このように複数のチャネルから無条件で各ファイルにアクセス可能であると、ICカード内で、様々が問題が発生することがある。たとえば、第1のチャネルでアクセス中のファイルが第2のチャネルで書換えられてしまうようなことが起こりうる。このような現象が起こると、第1のチャネルで期待された処理が実現できなくなってしまうという問題がある。

【特許文献1】特開2005-11147号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

この発明は、複数のチャネルでのアクセス制御を確実にかつ効率的に行うことができる携帯可能電子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】

【0006】

この発明の一形態としての携帯可能電子装置は、オペレーティングシステムプログラムを記憶する第1の記憶手段と、アプリケーションプログラムを記憶する第2の記憶手段と、ファイルを記憶する第3の記憶手段と、前記オペレーティングシステムプログラムおよび前記アプリケーションプログラムを実行する制御手段とを有するものであって、前記オペレーティングシステムプログラムは、前記第3の記憶手段に記憶しているファイルへアクセスするための複数のチャネルを管理するチャネル管理機能と、前記チャネル管理機能により管理される各チャネルが前記第3の記憶手段に記憶しているファイルをカレント状

10

20

30

40

50

態とした順番をアクセス順番として管理するアクセス順番管理機能と、前記チャンネル管理機能により管理される第1のチャンネルが前記第3の記憶手段に記憶しているファイルに対するカレント状態を解除した場合、前記第1のチャンネルを当該ファイルに対するアクセス順番の管理対象から外し、前記第1のチャンネルよりもアクセス順番が後であった全チャンネルのアクセス順番を繰り上げるアクセス順番更新機能と、前記第3の記憶手段に記憶しているファイルに対するチャンネルのアクセス順番を示す情報を前記第2の記憶手段に記憶しているアプリケーションプログラムへ提供する提供機能と、を有し、前記アプリケーションプログラムは、前記オペレーティングシステムプログラムから提供される前記ファイルに対するチャンネルのアクセス順番に基づいて、当該アプリケーションプログラムに割り当てられているチャンネルでの前記ファイルに対するアクセスを制御するアクセス制御機能を有する。

10

【発明の効果】

【0007】

この発明によれば、複数のチャンネルでのアクセス制御を確実かつ効率的に行うことができる携帯可能電子装置を提供することができる。

【発明を実施するための最良の形態】

【0008】

以下、この発明を実施するための最良の形態について図面を参照して説明する。

図1は、この実施の形態に係る携帯可能電子装置としてのICカード1のハードウェア構成を概略的に示すものである。

20

図1に示すように、ICカード1は、CPU（セントラル・プロセッシング・ユニット）11、ROM（リード・オンリ・メモリ）12、RAM（ランダム・アクセス・メモリ）13、通信ユニット（UART）14、不揮発性メモリ（NV（EEPROM））15、および、コプロセッサ（Co-Processor）16などを有している。

【0009】

上記CPU11、ROM12、RAM13、通信ユニット14、コプロセッサ15および不揮発性メモリ16は、ICチップなどにより一体的に形成されたモジュールCaにより構成される。このモジュールCaは、当該ICカード1を形成する筐体Cの内部に埋設される。すなわち、上記ICカード1は、モジュールCaが埋設された筐体Cにより構成されている。

30

また、上記ICカード1は、上位装置としての上記ICカード処理装置2から電力などの供給を受けた際、活性化し（動作可能な状態となり）、上記ICカード処理装置2からのコマンドに応じて動作するようになっている。

【0010】

上記CPU11は、全体的な管理や制御を司るものである。上記CPU11は、処理手段や判断手段として機能する。上記CPU11は、制御プログラム等に基づいて動作することにより種々の処理を行う。上記ROM12は、制御用プログラムや制御データなどが予め格納されている不揮発性メモリである。上記RAM13は、ワーキングメモリとして機能する揮発性のメモリである。

【0011】

40

上記通信ユニット14は、通信手段として機能し、上位装置としてのICカード処理装置2とのデータ通信を制御するものである。また、上記通信ユニット14は、上記ICカード1が動作するための電源を受給する手段としても機能する。上記コプロセッサ15は、暗号化あるいは復号化などの演算の補助を行うものである。上記不揮発性メモリ16は、各種データやアプリケーション（アプリケーションプログラム）などを記憶する書き換え可能な不揮発性メモリである。なお、上記不揮発性メモリ16に記憶されるデータの構造については、後で詳細に説明する。

【0012】

また、上記通信ユニット14は、ICカード1の通信方式に応じた構成を有している。たとえば、上記ICカード1の通信方式が接触式の通信方式である場合、上記通信ユニッ

50

ト 1 4 は、上位装置としての I C カード処理装置 2 のコンタクト部と物理的に接触するためのコンタクト部などにより構成される。この場合、I C カード 1 は、I C カード処理装置 2 と物理的に接触している上記通信ユニット 1 4 により I C カード処理装置 2 からの電源を受給する。つまり、上記 I C カード 1 が接触式 I C カードである場合、上記 I C カード 1 は、通信ユニット 1 4 としてのコンタクト部を介して I C カード処理装置 2 からの動作電源および動作クロックの供給を受けて活性化される。

【0013】

また、上記 I C カード 1 の通信方式が非接触式（無線式）の通信方式である場合、上記通信ユニット 1 4 は、電波の送受信を行うアンテナおよび通信を制御する通信制御部等により構成される。この場合、上記 I C カード 1 は、通信ユニット 1 4 により受信した電波から図示しない電源部により動作電源および動作クロックを生成するようになっている。つまり、上記 I C カード 2 が非接触式 I C カードである場合、上記 I C カード 2 は、通信ユニット 1 4 としてのアンテナおよび通信制御部等を介して I C カード処理装置 2 からの電波を受信し、その電波から図示しない電源部により動作電源および動作クロックを生成して活性化するようになっている。

【0014】

次に、上記不揮発性メモリ 1 6 に記憶されるデータの構成について説明する。

上記不揮発性メモリ 1 6 には、たとえば、I S O / I E C 7 8 1 6 において定義されたファイル構造で各種のデータが記憶される。たとえば、上記不揮発性メモリ 1 6 には、複数階層構造（ツリー構造）で管理されるデータファイルとしてのファイル（E F : E l e m e n t a r y F i l e）、および、データフォルダとしてのファイル（D F : D e d i c a t e d F i l e）が記憶されている。

【0015】

図 2 は、上記不揮発性メモリ 1 6 に記憶されているファイル構造の例を示す図である。

図 2 に示す例では、最上位がマスタファイルとしてのファイル（M F : M a s t e r F i l e）2 1 である。上記 M F 2 1 の配下には、フォルダとしての D F （アプリケーション A）2 2 A、および、フォルダとしての D F （2 アプリケーション B）2 2 B が設けられている。さらに、上記 D F （アプリケーション A）2 2 A の配下には、データの格納などに使用される E F （ファイル A 1）2 3 A 1 および E F （ファイル A 2）2 3 A 2 が設けられている構成になっている。さらに、上記 D F （アプリケーション B）2 2 B の配下には、データの格納などに使用される E F （ファイル B 1）2 3 B 1 が設けられている構成になっている。このようなファイル構造では、各種のデータは、データファイルとしての E F に記憶される。

【0016】

次に、上記 I C カード 1 におけるソフトウェア構成について説明する。

上記 I C カード 1 では、上述したように、C P U 1 1 が R O M 1 2 あるいは不揮発性メモリ 1 6 に記憶されているプログラムを実行することにより、種々の処理を実現している。すなわち、上記 I C カード 1 では、C P U 1 1 が実行するソフトウェアによって R O M 1 2、R A M 1 3、不揮発性メモリ 1 6、U A R T 1 4 あるいはコプロセッサ 1 5 などを制御することにより種々の処理を実現している。

【0017】

図 3 は、上記 I C カード 1 におけるソフトウェア構成を模式的に示す図である。

上記 I C カード 1 におけるソフトウェアは、ハードウェア（H / W）層 3 1、O S （オペレーティングシステム）層 3 2、および、アプリケーション層 3 3 から構成される。図 3 に示すように、上記 I C カード 1 では、上記アプリケーション層 3 3 が最上位に位置し、上記 O S 層 3 2 が上記 H / W 層 3 1 の上位に位置するような構造となっている。

【0018】

上記 H / W 層 3 1 は、上記 C P U 1 1、R O M 1 2、R A M 1 3、U A R T 1 4、コプロセッサ 1 5、不揮発性メモリ 1 6 などのハードウェアから構成される。上記 H / W 層 3

10

20

30

40

50

1の各ハードウェアは、上記OS層32からの処理要求に応じて処理を実行したり、実行した処理の結果を上記OS層32に送ったりするものである。

【0019】

上記OS層32は、当該ICカード1における基本的な制御を実行するためのプログラムとしてのカードOS（オペレーティングシステム）41を有する。なお、上記OS層32は、環境設定モジュール、アプリケーションインタフェース群などのモジュールなどを有するようにしても良い。上記カードOS41としてのソフトウェアは、当該ICカードの基本的な動作を司るプログラムであり、上記H/W層31の各ハードウェアを制御したり、各ハードウェアからの処理結果などの情報を受けて動作したりするプログラムである。上記カードOS41としてのソフトウェアは、ICカード内における不揮発性のメモリに予め記憶されているものであり、たとえば、上記ROM23などに記憶される。

10

【0020】

また、上記カードOS41は、当該ICカード1の基本動作を実現するためのH/W層の各ハードウェアを制御する基本機能に加えて、ロジカルチャネル管理機能42を有している。ロジカルチャネルとは、上記不揮発性メモリ16内の各ファイルあるいは各アプリケーションに対してアクセスするための論理的なチャネルを管理するものである。たとえば、複数の通信方式で通信を行っている場合、各通信方式ごとにロジカルチャネルが割り当てられる。このようなロジカルチャネルによる制御を行うことにより、ICカード1では、各チャネルごとに複数系列のコマンド群を処理することができる。たとえば、アプリケーションAでは、第1のチャネルでコマンド処理を実行し、アプリケーションBでは、第2のチャネルでコマンド処理を実行するという処理が可能となっている。

20

【0021】

上記ロジカルチャネル管理機能42は、上記のようなロジカルチャネルを管理する機能である。すなわち、上記ロジカルチャネル管理機能42は、ロジカルチャネルのオープン及びクローズを制御したり、アプリケーションプログラムに対してロジカルチャネルを割り当てたり、チャネル管理テーブル42aを用いてファイルあるいはアプリケーションに対する各ロジカルチャネルのアクセス順番を管理したりするものである。また、上記チャネル管理テーブル42aに記憶される情報は、各ロジカルチャネルでカレントとして設定するファイルあるいはアプリケーションプログラムなどの変更に応じて、テーブル更新機能42bにより更新される。

30

【0022】

上記アプリケーション層33は、各種の処理を実現するためのプログラムとしての各種のアプリケーション（アプリケーションA、アプリケーションB、…）から構成される。上記各アプリケーションとしてのソフトウェアは、当該ICカード1の運用形態に応じた各種の処理を実現するためのプログラムおよびデータなどにより構成される。上記アプリケーションとしてのソフトウェアは、予めICカード1内の不揮発性のメモリ16に記憶されたり、適宜外部装置からダウンロードしてICカード1内の不揮発性メモリ16に記憶されたりするものである。

すなわち、上記H/W層31の各ハードウェアは、上記OS層32のカードOS41により制御される。上記OS層32のカードOS41は、上記アプリケーション層33の各アプリケーションから要求に応じて各ハードウェアの動作を制御する。また、上記H/W層31の各ハードウェアによる処理結果等は、上記OS層32のカードOS41を介してアプリケーションへ供給される。たとえば、外部装置からのコマンドは、上記H/W層31のハードウェアにより受信され、上記OS層32のカードOS41へ供給される。上記カードOS41では、上記H/W層31で受信したコマンドを選択的にアプリケーション層33における特定のアプリケーションへ供給する。

40

【0023】

たとえば、上記H/W層31で外部装置からアプリケーション選択コマンドを受信した場合、上記カードOS41は、上記アプリケーション層33から当該アプリケーション選択コマンドで指定されたアプリケーションをカレント状態とする。この状態において上記

50

H/W層 3 1で外部装置からコマンドを受信した場合、上記カードOS 4 1は、当該コマンドをカレント状態のアプリケーションへ供給する。これにより、アプリケーション層 3 3の各アプリケーションは、上記OS層 3 2のカードOS 4 1から供給されるコマンドに応じた処理を実行する。すなわち、上記カードOS 4 1は、カレント状態のアプリケーション（以下、カレントアプリケーションとも称する）を指定し、カレントアプリケーションに対してコマンドを供給するようになっている。

【0024】

次に、上記ロジカルチャネル管理機能 4 2について説明する。

図 4、図 5 及び図 6 は、上記チャネル管理テーブル 4 2 a の構成例を示す図である。

すなわち、図 4、図 5 及び図 6 に示すように、上記チャネル管理テーブル 4 2 a は、各アプリケーションおよび各ファイルごとに各ロジカルチャネルのアクセス順番が格納されている。つまり、上記チャネル管理テーブル 4 2 a に格納されるアクセス順番は、各ロジカルチャネルが各ファイルあるいは各アプリケーションをカレントに設定した順番（アクセスした順番）を示す情報である。

【0025】

上記チャネル管理テーブル 4 2 a に格納される情報は、上記テーブル更新機能 4 2 b により適宜更新される。たとえば、新たなロジカルチャネルをオープンした場合、上記テーブル更新機能 4 2 b は、当該ロジカルチャネルでカレントに設定するファイルあるいはアプリケーションに追加する。この場合、カレントに設定するファイルあるいはアプリケーションに対する当該ロジカルチャネルのアクセス順番は、アクセス中のロジカルチャネルの後（つまり、アクセス順番が最後尾）とする。また、既存のロジカルチャネルをクローズした場合、上記テーブル更新機能 4 2 b は、当該ロジカルチャネルをチャネル管理テーブル 4 2 a から削除する。この場合、上記テーブル更新機能 4 2 b は、当該ロジカルチャネルをチャネル管理テーブル 4 2 a から削除するとともに、当該ロジカルチャネルより後のアクセス順番となっている全ロジカルチャネルのアクセス順番を繰り上げる。

【0026】

まず、上記テーブル更新機能 4 2 b がチャネル管理テーブル 4 2 a に格納されるアクセス順番にロジカルチャネルを追加する処理について説明する。

【0027】

図 4 に示すチャネル管理テーブル 4 2 a では、アプリケーション A は、ロジカルチャネル「ch. 1」、「ch. 3」、「ch. 0」の順にカレント設定され、ファイル A 1 は、ロジカルチャネル「ch. 1」、「ch. 3」の順にカレント設定されていることを示している。すなわち、図 4 に示すチャネル管理テーブル 4 2 a では、ロジカルチャネル「ch. 1」は、アプリケーション A とファイル A 1 とをそれぞれカレント設定していることを示している。また、図 4 に示すチャネル管理テーブル 4 2 a において、アプリケーション B は、ロジカルチャネル「ch. 2」でカレント設定されている。

【0028】

チャネル管理テーブル 4 2 a が図 4 に示すような状態において、ロジカルチャネル「ch. 2」でアプリケーション A のファイル A 1 を選択する処理（ロジカルチャネル「ch. 2」でアプリケーション A 及びファイル A 1 をカレント設定する処理）を実施したものとすると、この場合、上記テーブル更新機能 4 2 b は、チャネル管理テーブル 4 2 a の状態を図 5 に示すような状態に遷移させる。

【0029】

すなわち、ロジカルチャネル「ch. 2」のカレントファイルをアプリケーション A のファイル A 1 にする場合、上記テーブル更新機能 4 2 b は、上記チャネル管理テーブル 4 2 a におけるアプリケーション B に対するアクセス順番からロジカルチャネル「ch. 2」を削除すると共に、チャネル管理テーブル 4 2 a におけるアプリケーション A 及びファイル A 1 に対するアクセス順番の最後尾にそれぞれロジカルチャネル「ch. 2」を追加する。これにより、チャネル管理テーブル 4 2 a は、図 5 に示すように、アプリケーション A 及びファイル A 1 を最後にカレントに設定したロジカルチャネルが「ch. 2」であ

ることを示す状態となる。図 5 に示すようなチャンネル管理テーブル 4 2 a によれば、ロジカルチャンネル「c h. 2」のファイル A 1 へのアクセス順番は、ロジカルチャンネル「c h. 1」及び「c h. 3」の次であることが判別できる。

【0030】

次に、上記テーブル更新機能 4 2 b がチャンネル管理テーブル 4 2 a に格納されるアクセス順番からロジカルチャンネルを削除する処理について説明する。

ここでは、上記チャンネル管理テーブル 4 2 a が図 5 に示すような状態において、ロジカルチャンネル「c h. 1」をクローズする処理が実施される場合を想定するものとする。この場合、上記テーブル更新機能 4 2 b は、クローズされるロジカルチャンネル「C h. 1」を上記チャンネル管理テーブル 4 2 a から削除する（ロジカルチャンネル「C h. 1」を管理対象から外す）ことにより、チャンネル管理テーブル 4 2 a の状態を図 6 に示すような状態に遷移させる。

10

【0031】

すなわち、ロジカルチャンネル「c h. 1」をクローズする場合、上記テーブル更新機能 4 2 b は、チャンネル管理テーブル 4 2 a におけるロジカルチャンネル「c h. 1」を削除すると共に、ロジカルチャンネル「c h. 1」以外に続く各ロジカルチャンネルのアクセス順番をそれぞれ繰り上げる。たとえば、図 5 に示すチャンネル管理テーブル 4 2 a では、アプリケーション A 及びファイル A 1 に対するアクセス順番が最上位のロジカルチャンネル「c h. 1」が削除される。このため、上記チャンネル管理テーブル 4 2 a は、図 6 に示すように、アプリケーション A に対するアクセス順番がロジカルチャンネル「C h. 3」、「C h. 0」、「C h. 2」となり、ファイル A 1 に対するアクセス順番がロジカルチャンネル「C h. 3」、「C h. 2」となる。

20

【0032】

上記のように、チャンネル管理テーブル 4 2 a において、各アプリケーション及び各ファイルに対する各ロジカルチャンネルのアクセス順番は、各ロジカルチャンネルがカレントに設定した順番を示すものである。ロジカルチャンネルがクローズされた場合、あるいは、ロジカルチャンネルのカレント設定が変更された場合、各ロジカルチャンネルに与えられていたアクセス順番は変更される。言い換えると、本 I C カード 1 では、特定のロジカルチャンネルに対してクローズ及びオープン、あるいは、各ロジカルチャンネルのカレント設定の変更を行うことにより、チャンネル管理テーブル 4 2 a における各ロジカルチャンネルのアクセス順番を変更することが可能である。

30

【0033】

すなわち、特定のロジカルチャンネルがクローズされた場合、上記チャンネル管理テーブル 4 2 a では、クローズされたロジカルチャンネルが管理対象から除外され、それ以外の各ロジカルチャンネルのアクセス順番が繰り上がる。これにより、ロジカルチャンネルがクローズされた場合であっても、他のロジカルチャンネルでのアプリケーションあるいはファイルに対するアクセスに矛盾が生じることのない管理を実現できる。言い換えると、特定のロジカルチャンネルに対してクローズとオープンとを行うことにより、当該ロジカルチャンネルのアクセス順番を最後尾にすることが可能となっている。

【0034】

40

次に、I C カード処理装置 2 からのコマンドに対する I C カード 1 における処理について説明する。

上記のようなチャンネル管理テーブル 4 2 a によって、上記カード O S 4 1 のロジカルチャンネル管理機能 4 2 では、各アプリケーションに処理を実施しているチャンネル番号を通知したり、各ファイルあるいは各アプリケーションに対する各ロジカルチャンネルの優先権（アクセス順序）を通知したりする。これにより、コマンドを受けた各アプリケーションでは、カード O S 4 1 から提供される優先権を示す情報に基づいて、当該コマンドに対する処理内容を決定することが可能となる。

【0035】

各アプリケーションでは、カード O S 4 1 を介して I C カード処理装置 2 からのコマン

50

ドが与えられる。この場合、アプリケーションは、自身のロジカルチャネルの優先順位に基づいて受信したコマンドに対する処理を実行するか否かを判断する。さらに、各アプリケーションでは、自身のロジカルチャネルの優先順位と受信したコマンドの種類とに基づいて、当該コマンドに対する処理を実行するか否かを判断するようにしても良い。言い換えると、受信したコマンドを実行するか否かを判断するか否かは、各アプリケーションがカードOS 41から提供されるロジカルチャネルのアクセス順序（優先権）を示す情報により決定するようになっている。

【0036】

たとえば、コマンドを受信したアプリケーションでは、自身のロジカルチャネルの優先順位が最上位である場合、全てのコマンドに対する処理を実行可と判断するようにする。また、コマンドを受信したアプリケーションでは、自身のロジカルチャネルの優先順位が最上位でない場合、受信したコマンドがファイルの状態を変更するコマンド（たとえば、書換えあるいは削除などのコマンド）に対する処理を実行不可と判断し、受信したコマンドがファイルの状態を変更しないコマンド（たとえば、読出しなどのコマンド）に対する処理を実行可と判断するようにする。

【0037】

上記のように、受信したコマンドに対する処理内容（実行の可否）は、アプリケーションが決定ようにすることができる。従って、各アプリケーションにより実現される処理は、上述した例にかかわらずに、以下のような種々の形態が可能である。

たとえば、特定のアプリケーション（最優先とするアプリケーション）は、ロジカルチャネルの優先順位によらずに、常に全てのコマンドに対する処理を実行するようにしても良い。また、受信したコマンドの種類によらずに、最上位のロジカルチャネルでなければ、全てのコマンドに対する処理を実行しないようにしても良い。さらには、たとえば、履歴情報をレコード単位で順次格納する特定のファイルについては、ロジカルチャネルの優先順位によらずに、書込み処理を許可するようにしても良い。

上記のように、本ICカード1では、アプリケーションごとに、別のロジカルチャネルとカレント設定が競合する場合のコマンドに対する処理内容に自由に設計でき、運用形態などに応じた自由度の高いシステムを実現できる。

【0038】

図7は、ICカード処理装置2からのコマンドに対する処理例を説明するためのフローチャートである。なお、カードOS 41および各アプリケーションの動作は、CPU 11により実現されるものであるが、以下の処理例では、カードOS 41の動作と各アプリケーション22（22A、22B、…）の動作とに分けて説明するものとする。

まず、ICカード処理装置2からのコマンドをUART 14により受信すると（ステップS10）、CPU 11により実行されるカードOS 41は、受信したコマンドをアプリケーション（ここではアプリケーション22Aとする）に通知する（ステップS11）。

【0039】

上記カードOS 41からコマンドを取得すると（ステップS12）、上記アプリケーション22Aは、自身のロジカルチャネルをカードOS 41に対して問合せ（ステップS13）。

この問合せに対して、カードOS 41は、ロジカルチャネル管理機能42によりチャネル管理テーブル42aを参照し、当該アプリケーション22Aのロジカルチャネルを判別する（ステップS14）。上記アプリケーション22Aのロジカルチャネルを判別すると、カードOS 41は、上記アプリケーション22Aに対してロジカルチャネルを示す情報を通知する（ステップS15）。

これにより、上記アプリケーション22Aは、自身のロジカルチャネルを確認する。なお、コマンドを受信したアプリケーションが自身に割り当てられたロジカルチャネルを確認する方法としては、上記ステップS13～S16の処理に限らず、受信したコマンドのCLASS バイトから直接確認する方法、あるいは、カード仕様によって予め用意されている専用のAPIにより取得する方法なども適用可能である。

【0040】

上記カードOS 41から自身のロジカルチャネルを示す情報を取得すると、上記アプリケーション22Aは、当該コマンドにおいてアクセス対象となるファイルを判別し、アクセス対象となるファイルの各ロジカルチャネルによるアクセス状況をカードOS 41に問い合わせる（ステップS 21）。

この問合せに対して、カードOS 41は、上記ロジカルチャネル管理機能42によりチャネル管理テーブル42aを参照して、アクセス対象とするファイルに対する各ロジカルチャネルのアクセス順番（優先順位）を判定する（ステップS 22）。上記アクセス対象のファイルに対する各ロジカルチャネルのアクセス順番を判別すると、カードOS 41は、上記アプリケーション22Aに対して当該ファイルに対する各ロジカルチャネルのアクセス順番を示す情報を通知する（ステップS 23）。 10

【0041】

上記アクセス対象とするファイルに対する各ロジカルチャネルのアクセス順番を示す情報を取得すると（ステップS 24）、アプリケーション22Aは、当該コマンドに対する処理を実行するか否かを判定する処理を行う（ステップS 25～S 26）。すなわち、アプリケーション22Aは、当該コマンドがアクセス対象とするファイルにアクセスしている（当該ファイルをカレントに設定している）別のロジカルチャネルが存在するか否かを判断する（ステップS 25）。

【0042】

別のロジカルチャネルで当該ファイルへのアクセスが無いと判断した場合（ステップS 25、NO）、上記アプリケーション22Aは、当該コマンドに対する処理を実行し（ステップS 28）、その処理結果をカードOS 41へ通知する（ステップS 29）。なお、上記ステップS 28のコマンドに対する処理では、アプリケーション22Aは、カードOS 41と共同して当該ファイルが格納されているメモリへのアクセスなどを実現するようになっている。 20

【0043】

また、別のロジカルチャネルで当該ファイルへのアクセスが有ると判断した場合（ステップS 25、NO）、上記アプリケーション22Aは、カードOS 41から取得した各ロジカルチャネルのアクセス順番を示す情報に基づいて、自身のロジカルチャネルに当該ファイルに対する優先権があるか否かを判断する（ステップS 26）。たとえば、上記アプリケーション22Aは、カードOS 41から取得した各ロジカルチャネルのアクセス順番において、自身のロジカルチャネルが最上位であるか否かにより、当該ファイルに対する優先権があるか否かを判断する。 30

【0044】

上記判断により自身のロジカルチャネルに優先権があると判断した場合（ステップS 26、YES）、上記アプリケーション22Aは、当該コマンドに対する処理を実行し（ステップS 28）、その処理結果をカードOS 41へ通知する（ステップS 29）。

【0045】

また、上記判断により自身のロジカルチャネルに優先権がないと判断した場合（ステップS 26、NO）、上記アプリケーション22Aは、当該コマンドの種類が実行可能なコマンドであるか否かを判断する（ステップS 27）。上記ステップS 27の処理は、各アプリケーションごとの設定に応じて判断されるものである。たとえば、ライト系のコマンドを実行不可とし、リード系のコマンドを実行可能となるような形態が可能である。また、全コマンドを実行不可としたり、全コマンドを実行可としたりする形態も可能である。さらには、アクセス対象となるファイルのタイプによって、実行の可否を判定するような形態も可能である。 40

【0046】

たとえば、アプリケーション22Aでは、書換えなどのファイルの状態を書き換えてしまうようなコマンドを実行不可とし、それ以外のコマンドを実行可と設定されているものとする。このような場合、上記アプリケーション22Aは、受信したコマンドが書換えコ 50

マンドであれば、当該コマンドの処理を実行不可を判断する。また、受信したコマンドが読出しコマンドであれば、上記アプリケーション 22A は、当該コマンドの処理を実行可と判断する。

【0047】

上記判断により受信したコマンドの処理を実行可と判断した場合（ステップ S27、YES）、上記アプリケーション 22A は、当該コマンドに対する処理を実行し（ステップ S28）、その処理結果をカード OS 41 へ通知する（ステップ S29）。また、上記判断により受信したコマンドの処理を実行不可と判断した場合（ステップ S27、NO）、上記アプリケーション 22A は、当該コマンドに対する処理を実行不可（中断）し、当該コマンドに対する処理を中断した旨を処理結果としてカード OS 41 へ通知する（ステップ S29）。 10

【0048】

上記アプリケーション 22A から受信したコマンドに対する処理を取得すると（ステップ S30）、カード OS 41 は、上記アプリケーション 22A から通知された処理結果を受信したコマンドに対するレスポンスデータとして IC カード処理装置 2 へ送信する（ステップ S31）

上記のように、本 IC カード 1 のカード OS 41 では、各ファイルに対してカレント設定しているチャンネルとそれらのチャンネルのアクセス順番とを管理しておき、アプリケーションが、受信したコマンドに応じてアクセスしようとするファイルについて、「既に他のチャンネルが対象のファイルをカレント設定しているか」、「アクセスする優先権（アクセスした順番）はどのチャンネルにあるか」をカード OS 41 から提供される情報により確認することにより、複数のチャンネルでのカレント設定に応じたアクセス制御を行う。 20

上記のような処理により、あるアプリケーションのコマンド処理において、アクセスするファイルが他のチャンネルで既にカレント設定されていなかをカード OS 41 が確認することができ、複数のロジカルチャンネルでカレント設定されているファイルに対する処理を確実に管理することができる。

【0049】

つまり、本実施の形態の IC カードでは、オペレーティングシステムが、不揮発性メモリに記憶されている各ファイルに対してアクセス中のチャンネルを示す情報をチャンネル管理テーブルにより管理し、前記チャンネル管理テーブルで管理されている情報を参照することにより受信したコマンドがアクセス対象とするファイルにアクセス中のロジカルチャンネルを示す情報を当該コマンドを処理するアプリケーションに提供し、前記アプリケーションが前記オペレーティングシステムから提供された情報に基づいて前記コマンドに対する処理の実行の可否を判定する。これにより、複数のロジカルチャンネルでのアクセス制御において、別のロジカルチャンネルとカレント設定（アクセス中のファイル）が競合する場合のコマンドに対する処理内容をアプリケーションごとに運用形態などに応じて設計できる。 30

【図面の簡単な説明】

【0050】

【図 1】この発明の実施の形態に係る携帯可能電子装置としての IC カードのハードウェア構成を概略的に示すブロック図。 40

【図 2】不揮発性メモリに記憶されるデータのファイル構成例を示す図。

【図 3】IC カードにおけるソフトウェア構成を説明するための模式図。

【図 4】チャンネルのアクセス順序を管理するためのチャンネル管理テーブルの構成例を示す図。

【図 5】チャンネルのアクセス順序を管理するためのチャンネル管理テーブルの構成例を示す図。

【図 6】チャンネルのアクセス順序を管理するためのチャンネル管理テーブルの構成例を示す図。

【図 7】IC カードにおけるコマンドに対する処理例を説明するためのフローチャート。

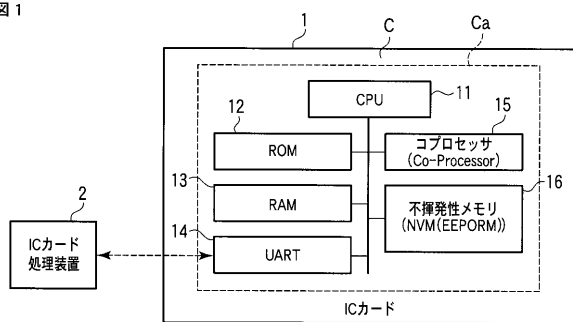
【符号の説明】

【 0 0 5 1 】

1 … ICカード、2 … ICカード処理装置、11 … CPU、12 … ROM、13 … RAM、14 … 通信ユニット (UART)、15 … コプロセッサ、16 … 不揮発性メモリ、Ca … モジュール、C … 本体、31 … ハードウェア層、32 … OS層、33 … アプリケーション層、41 … カードOS、42 … ロジカルチャネル管理機能、42a … チャネル管理テーブル、42b … テーブル更新機能。

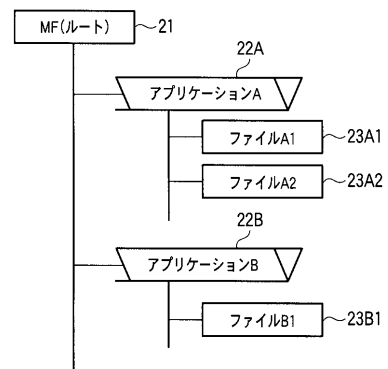
【 図 1 】

図 1



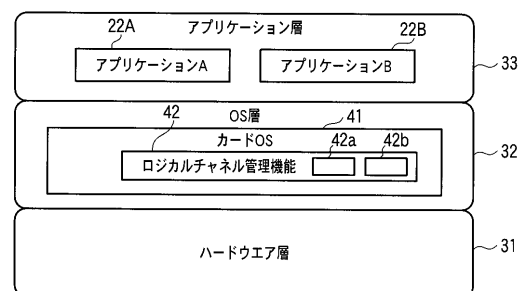
【 図 2 】

図 2



【 図 3 】

図 3



【図 4】

図 4

アプリケーション/ファイル	アクセス順番
アプリケーションA	Ch.1, Ch.3, Ch.0
ファイルA1	Ch.1, Ch.3
vファイルA2	
アプリケーションB	Ch.2
ファイルB1	

【図 6】

図 6

アプリケーション/ファイル	アクセス順番
アプリケーションA	Ch.3, Ch.0, Ch.2
ファイルA1	Ch.3, Ch.2
vファイルA2	
アプリケーションB	
ファイルB1	

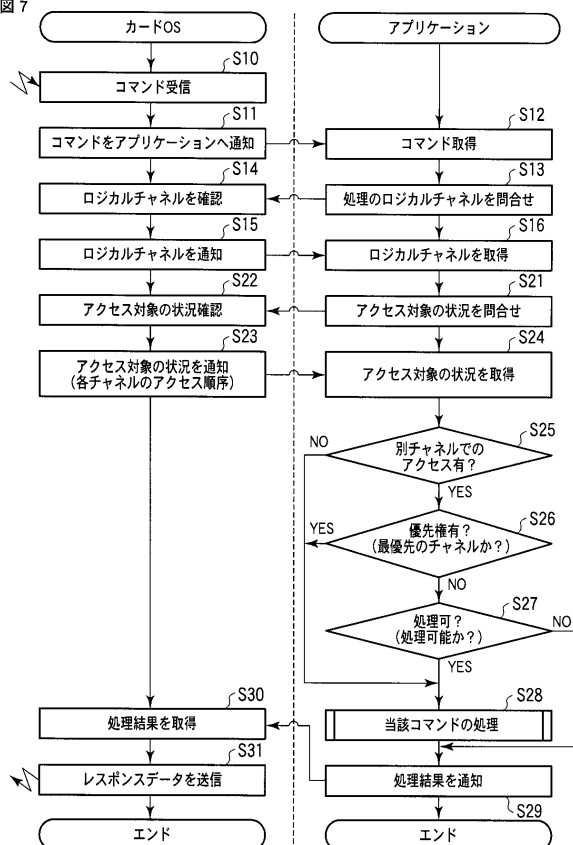
【図 5】

図 5

アプリケーション/ファイル	アクセス順番
アプリケーションA	Ch.1, Ch.3, Ch.0, Ch.2
ファイルA1	Ch.1, Ch.3, Ch.2
ファイルA2	
アプリケーションB	
ファイルB1	

【図 7】

図 7



フロントページの続き

- (74)代理人 100095441
弁理士 白根 俊郎
- (74)代理人 100084618
弁理士 村松 貞男
- (74)代理人 100103034
弁理士 野河 信久
- (74)代理人 100119976
弁理士 幸長 保次郎
- (74)代理人 100153051
弁理士 河野 直樹
- (74)代理人 100140176
弁理士 砂川 克
- (74)代理人 100100952
弁理士 風間 鉄也
- (74)代理人 100101812
弁理士 勝村 紘
- (74)代理人 100070437
弁理士 河井 将次
- (74)代理人 100124394
弁理士 佐藤 立志
- (74)代理人 100112807
弁理士 岡田 貴志
- (74)代理人 100111073
弁理士 堀内 美保子
- (74)代理人 100134290
弁理士 竹内 将訓
- (74)代理人 100127144
弁理士 市原 卓三
- (74)代理人 100141933
弁理士 山下 元
- (72)発明者 石橋 則夫
東京都港区芝浦一丁目1番1号 株式会社東芝内
- Fターム(参考) 5B035 AA06 BB09 CA23 CA29 CA39
5B082 GA14 JA08