

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4546256号
(P4546256)

(45) 発行日 平成22年9月15日 (2010. 9. 15)

(24) 登録日 平成22年7月9日 (2010. 7. 9)

(51) Int. Cl.	F I
GO 6 K 19/073 (2006. 01)	GO 6 K 19/00 P
GO 6 K 17/00 (2006. 01)	GO 6 K 17/00 E

請求項の数 8 (全 8 頁)

(21) 出願番号	特願2004-559826 (P2004-559826)	(73) 特許権者	501287850
(86) (22) 出願日	平成15年12月12日 (2003. 12. 12)		アエスカ エス. ア.
(65) 公表番号	特表2006-510099 (P2006-510099A)		ASK S. A.
(43) 公表日	平成18年3月23日 (2006. 3. 23)		フランス、エフー06560 バルボン、
(86) 国際出願番号	PCT/FR2003/003696		ソフィア アンティポリス、トラバース
(87) 国際公開番号	W02004/055741		デ ブリュクス、15、レブイード
(87) 国際公開日	平成16年7月1日 (2004. 7. 1)		Les Bouillides, 15, t
審査請求日	平成18年12月5日 (2006. 12. 5)		raverse des Brucs, S
(31) 優先権主張番号	0215740		ophia Antipolis, F-
(32) 優先日	平成14年12月12日 (2002. 12. 12)		06560 Valbonne, Fra
(33) 優先権主張国	フランス (FR)		nce
		(74) 代理人	100066865
			弁理士 小川 信一
		(74) 代理人	100066854
			弁理士 野口 賢照

最終頁に続く

(54) 【発明の名称】 メモリカードに記録されているデータの安全な変更方法

(57) 【特許請求の範囲】

【請求項 1】

スマートカードと、該スマートカードがリーダに対し所定の位置関係にあるとき前記スマートカードを読み取り可能なリーダと、を含むカード処理システムにおいて、前記スマートカードは、該スマートカードにより実行される処理に関するデータ値を記録するための少なくとも1つのメモリ位置を含む不揮発性、消去および書換可能なメモリを含み、各処理は前記データ値の増加を生じる、カード処理システムにおけるデータの変更方法であって、

各処理毎に、前記データ値の書込み動作は、前記メモリ内でデータ値としての値ゼロが記録された第1メモリ位置(B)と第2メモリ位置(A)とを持つカウンタの第1メモリ位置(B)に新しいデータ値(Y)の書込みを実行し、

前記書込み動作はまた前記第2メモリ位置(A)に記録されている古いデータ値(X)の消去を実行するようになっており、

その結果、前記書込み動作の最後に、その書込み動作が正しく実行された場合は、前記第1メモリ位置に新しいデータ値が記録され、前記第2メモリ位置には値ゼロが記録され、

処理の過程で前記スマートカードの突然の取出しがあった結果、前記書込み動作が正しく実行されない場合には、前記カウンタの前記第1、第2メモリ位置のどちらにも値ゼロが記録されない、ことを特徴とするカード処理システムにおけるデータの変更方法。

【請求項 2】

10

20

前記新しい値の書込み動作中に突然の取出しが行われた場合に、前記リーダによる前記スマートカードの再度の読み取り時において、前記新しい値（Ｙ）の前記第１メモリ位置（Ｂ）への書換と、前記古い値（Ｘ）の前記第２メモリ位置（Ａ）からの消去と、を含む書換動作による、前記カウンタの修復を更に含むことを特徴とする請求項１に記載の方法。

【請求項３】

前記第１メモリ位置（Ｂ）が前記古いデータ値（Ｘ）と前記新しいデータ値（Ｙ）の間の不正な値（Ｙ'）を含むとき、前記第１メモリ位置への前記不正な値（Ｙ'）への書換と、前記古い値の前記第２メモリ位置からの消去とを含む書換動作と、それに続く、前記新しい値の前記第２メモリ位置（Ａ）への書込みと、前記不正な値の前記第１メモリ位置からの消去とを含む新たな書込み動作とによる、前記カウンタの修復をさらに含むことを特徴とする請求項１に記載の方法。

10

【請求項４】

前記第１メモリ位置（Ｂ）が前記古い値（Ｘ）より小さい不正なデータ値（Ｙ'）を含むとき、前記第２メモリ位置（Ａ）への前記古いデータ値（Ｘ）への書換と、前記不正な値の前記第１メモリ位置（Ｂ）からの消去とを含む書換動作と、それに続く、前記新しいデータ値（Ｙ）の前記第１メモリ位置への書込みと、前記古いデータ値の前記第２メモリ位置からの消去とを含む新たな書込み動作とによる、前記カウンタの修復を更に含むことを特徴とする請求項１に記載の方法。

20

【請求項５】

突然の取出しが前記新しいデータ値の書込み動作と前記古いデータ値の消去動作との間で起こるとき、前記リーダによる前記スマートカードの再度の読み取り時において、前記第１メモリ位置（Ｂ）への前記新しいデータ値（Ｙ）への書換と、前記古いデータ値（Ｘ）の前記第２メモリ位置（Ａ）からの消去を含む書換動作による、前記カウンタの修復を更に含むことを特徴とする請求項１に記載の方法。

【請求項６】

突然の取出しが前記古いデータ値（Ｘ）の消去動作中に起こり、不正なデータ値（Ｘ'）が前記第２メモリ位置（Ａ）に記録されているとき、前記リーダによる前記スマートカードの再度の読み取り時において、前記第１メモリ位置（Ｂ）への前記新しいデータ値（Ｙ）への書換と、前記不正な値の前記第２メモリ位置からの消去とを含む書換動作による、前記カウンタの修復を更に含むことを特徴とする請求項１に記載の方法。

30

【請求項７】

スマートカードと、該スマートカードがリーダに対し所定の位置関係にあるとき前記スマートカードを読み取り可能なリーダと、を含み、前記スマートカードは、該スマートカードにより実行される処理に関するデータ値を記録するための少なくとも１つのメモリ位置を含む不揮発性、消去および書換可能なメモリを含み、各処理は前記データ値の増加を生じるカード処理システムであって；

前記システムは、前記メモリが、カウンタを形成する所定の第１メモリ位置（Ｂ）と所定の第２メモリ位置（Ａ）とを含み、

前記カウンタの前記データ値としての値ゼロが記録された第１メモリ位置（Ｂ）への新しいデータ値（Ｙ）の書込みと、前記カウンタの他方の第２メモリ位置（Ａ）からの古いデータ値（Ｘ）の消去とを実行する各処理の書込み命令の結果、

40

書込み動作の最後に、その書込み動作が正しく実行された場合は、前記第１メモリ位置（Ｂ）に新しいデータ値が記録され、前記第２メモリ位置（Ａ）には値ゼロが記録され、

あるいは取引の過程で前記スマートカードの突然の取出しがあった結果、前記書込み動作が正しく実行されない場合には、前記カウンタの前記第１、第２メモリ位置のどちらにも値ゼロが記録されない、ことを特徴とするカード処理システム。

【請求項８】

前記スマートカードが非接触カードであることを特徴とする請求項７に記載のシステム。

50

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、カードリーダを用いた処理が実行されるとき、スマートカードに記録されているデータ記録の一部を変更するためのシステムに関し、さらに詳細には、スマートカードに記録されているデータを、リーダを用いた処理の間に変更するための安全な方法に関する。

【背景技術】

【0002】

チップカードとも呼ばれるスマートカードは、カード所有者のデータキャリアとして益々その使用は増加している。これらのカードには、カードに搭載されたアンテナと、関連するリーダとの間の情報交換を非接触電磁結合により行う非接触カードが含まれる。これは、アクセス制限領域へのアクセスカード又は電子財布として開発されてきた。

【0003】

一般的に、スマートカードは不揮発性、消去および書換可能なEEPROM又はフラッシュEPROM型メモリを使用するので、メモリのスイッチが切れているときでもデータはメモリに書込まれたままである。これらはさらに、1つ又はいくつかのメモリ位置を消去して新しいデータを書込むことによりデータ記録を更新することが出来る。

【0004】

処理の間に、一般的にはカードの「突然の取出し」、即ち処理動作が完了する前の取出し、による偶発的停電によりメモリが壊れ、それにより新しいデータが記録されずにデータを喪失することがある。このリスクが特に大きいのは、カードが正しく作動できる空間的限度を認知することの出来ない非接触カードを用いるときである。

【0005】

不揮発性EEPROM型メモリの場合には、別のリスクがある。この場合、書込み動作が正常に終了する前に中断されてもデータは書込まれ、書込み動作の直後には正しく読取ることが出来るが、後の時点でこの読取りを繰返しても、これが正しく実行される保証はない。途中で中断された書込み動作の結果、メモリセル内の情報の保持が不十分だからである。

【0006】

したがって、データの完全性を確保するには、データが変更済み状態か、又は変更前の状態の何れかにあり、決して「突然の取出し」による未確定の中間状態にはならないことを確保することにより、このようなリスクに対してカードを保護することが望ましい。

【0007】

処理の安全性の理由から、万一処理中に停電を生じ、処理を最初からやり直すことが出来ない場合は、重要データ（電子財布の預金残高など）の修復不能な喪失の危険を覚悟の上で、処理全体を再実行する必要がある。

【0008】

上述の問題に対応して、データ変更を実行する前にデータ記録をバッファメモリに記憶することが考案されてきた。変更すべき記録に対する変更が全て完了すると、古い記録はバッファメモリから消去される。

【0009】

残念なことに、この方法は、各記録毎に、バッファ領域への退避動作、変更すべき記録の消去動作、書換動作及びバッファ領域内の古い記録の消去動作と、全部で4つの動作を必要とする。したがってこの作業には、時間がかかる欠点があり、非接触カードにとっては重大な欠点である。

【0010】

さらに、前のデータを消去する前にメモリ内の別の位置に退避させるには、変更作業が正しく実行されたか否かをフラグ値に従って示すための「フラグ」の存在を必要とする。このフラグは、変更が正しく行われたか否かに従ってゼロ又は1の値を取る単一ビットに

10

20

30

40

50

することが出来る。データと同一位置にチェックビットを記録する明白な理由が考えられない限り、唯一の解決策は、このフラグ（単一又は複数のチェックビット）を、この目的に予約されたメモリ位置に記録することであり、したがって単一ビット又は数ビットで十分であれば、このためのメモリは全体で16ビット又は32ビットのブロックである。

【0011】

メモリ内の位置を浪費しないことが必須となる低容量のメモリのみが必要とされ、また処理毎に変更されるデータ値が時間の単調関数である特定の用途にスマートカードを使用する場合、上述の欠点はさらに重大である。このような用途において、メモリデータ記録は、写真複写機などのように時間と共に増加する増加カウンタか又は、記録の値が乗車毎に1単位ずつ減少する公共交通機関用カード若しくは記録の値が減少するだけの電子財布の場合の減少カウンタである。

10

【発明の開示】

【発明が解決しようとする課題】

【0012】

したがって本発明の目的は、スマートカードの中のデータをカードの処理中に変更するための方法であって、処理中にカードが制限を受けるアクセス時間に対応する最少時間で実行できる方法を実現することにある。

【0013】

本発明の別の目的は、非接触型のスマートカードの中のデータを変更するための方法であって、メモリ位置にチェックビット（フラグ）を予約する必要のない方法を実現することにある。

20

【課題を解決するための手段】

【0014】

本発明の対象はしたがって、スマートカードなどや、カードがリーダに対し所定の位置関係にあるときカードを読取り可能なリーダと、を含むカード処理システムであって、そのカードは、カードによる処理に関するデータ値を記録するための少なくとも1つの位置を含む不揮発性、消去および書換可能なメモリを含み、各処理はデータ値の変更を生じ、データ値は時間に関し単調関数であるカード処理システムにおけるデータ変更方法である。データ値の書込み動作が、各処理毎に、メモリ内でカウンタを形成する所定の2つの位置のうちの第1位置に新しいデータ値の書込みを実行し、その書込み動作は、第2位置に記録される古いデータ値の消去を実行するので、正しく書込み動作が実行されると、第1位置に新しいデータ値を含み、第2位置に値ゼロを含む。

30

【発明を実施するための最良の形態】

【0015】

本発明の対象及び特徴は、図面を参照して以下の記述を読むことにより、一層明確になる。

【0016】

少量のメモリを必要とする用途に使用される布線論理メモリを有する型のチップカードでは、メモリ位置が限られている。このように、図1に示すようなチップカードのメモリはEPROM型メモリであって、16ビットの32ワードの容量を有する。以下に記述する本発明により、メモリ内でワード全部の予約を必要とするチェック領域を省くことが出来る。そのためには、2層カウンタを形成する2つのメモリ位置（A層、B層）が、リーダとスマートカードとの間で実行される各処理における新しいデータ値の記録に対して予約される。

40

【0017】

本発明の原理は、それぞれの処理において変更されるデータ値が時間の単調関数である全ての用途において有効に利用される。アクセス制限領域へのアクセス、又は電子財布など別の用途において、データ値は減少するが、場合によっては（コピーをするのに使用されるカードなど）記録される値は増加する。しかし、カウンタは、減少させるよりも増加させる方が好ましい。実際問題として、突然の取出しが行われると、メモリに書込まれた

50

ビットが正しく保持されないリスクが発生する。この場合、各ビット1をゼロに切換られる可能性があるので、記録された値が減少することがありうる。減少させる方法を用いた場合、不正な書込み値が減少しているので、メモリの中の値が正常な減少の結果であるか、又はメモリ内容の異常減少の結果であるかを知ることが出来ない限り、その減少はカード所有者側のリスクになる。逆に、増加させる方法を用いた場合、突然の取出しの結果不正に記録される値の減少があるとき、当該値が増加する前の値である限り、メモリの減少は所有者側のリスクにならない。

【0018】

減少させる方法の場合、データ値の2の補数バイナリを毎回考慮するのは容易である。したがって、以下においては、問題の用途に関係なくデータ値はそれぞれの処理において増加される。

10

【0019】

本発明による方法は、値ゼロを含んだカウンタの層の変更の対象となった新しいデータ値の記録と、カウンタのもう一方の層の消去と値ゼロへの設定とを含む。逆にすることの出来ないこれら2つの位相は、処理時のリーダからの新しい値の書込み命令により始動する。

【0020】

図2は、通常の動作経過を示す。最初に、カウンタの読取りによりA層に値X、B層に値ゼロがあらわれる。このとき書込み命令は、新しい値YのB層への書込み、続いてA層からの値Xの消去を実行する。こうして、カウンタは1つの命令で増加される。

20

【0021】

残念なことに、特にチップカードが非接触カードの場合は、処理中にカードの突然の取出しが起こりうる。この場合、書込み動作が正しく進行せず、新しい値の書込みが正しく実行されていないか、又は古い値が消去されていないかの何れかになる。この場合、処理は不成立、あるいは有効とはならない。この結果、アクセス制限領域へのアクセスを許可するゲートの開放が認められないことや、電子財布の場合に小売端末機による購入が許可されないことが起こりうる。

【0022】

したがってカード所有者は、自分のカードをリーダの中又は前を通過させることを含む動作を再始動する。先ずカウンタの読取りが実行され、この時カウンタの2つの層が何れもゼロでないことを示す。そこから突然の取出しがあったことが直ちに推定されるので、以下に記述するようにカウンタの修復が実行される。

30

【0023】

図3～7は、突然の取出しがあった場合のカウンタ修復動作を、この突然の取出しを書込み位相、書込み位相と消去位相との間、又は消去位相のいずれで発生したかに従って示す。

【0024】

図3に示す第1状態においては、カードの突然の取出しは書込み位相で行われ、値Yは書込まれているが値Xは消去されていない。この場合、値Yは正しいが、この値のB層への保持は保証されない。したがって、値XをA層から消去してゼロに設定する前に、値Yは書換られる。メモリ位置への書込みは、そこにある値と新しい値との間のOR関数であるので、新しい値は古い値がゼロに等しいか新しい値と同一のとき（この場合に相当）にのみ書込みが可能であることに注意すべきである。

40

【0025】

図4に示す第2状態においては、突然の取出しは書込み位相で行われており、B層にXとYとの間の値Y'が書込まれているが、値XはA層から消去されていない。この場合、第1書込み動作はB層へのY'の書換と、A層からのXの消去を実行する。次いで、書込み動作はA層へのYの書込みと、B層からのY'の消去を実行するので、カウンタは1つの層が新しい値を含み、別の層がゼロを含む正常な状態に戻る。

【0026】

50

図 5 に示す第 3 状態においては、突然の取出しは書込み位相で行われており、B 層に X より小さい値 Y' が書込まれているが、値 X は消去されていない。この場合、第 1 書込み動作は A 層への X の書換と B 層からの Y' の消去を実行する。これは、カウンタの修復は常に最大値、この例では X、を用いて実行されることをその根拠としている。次いで、書込み動作は、B 層への値 Y の書込みと A 層からの X の消去を実行する。

【 0 0 2 7 】

図 6 に示す第 4 状態においては、突然の取出しは書込み位相と消去位相との間で行われ、B 層には値 Y が記録されているが値 X は A 層から消去されていない。この場合、値 Y の保持は保証されないので、書換動作により B 層への値 Y の書換と A 層からの X の消去が実行される。

10

【 0 0 2 8 】

図 7 に示す第 5 状態においては、突然の取出しが消去位相で行われ、B 層に値 Y は書込まれているが、値 X が正しく消去されず A 層には値 X' が見られる。したがって、B 層への値 Y の書換動作の実行が必要であり、その結果 A 層からの値 X' の消去が可能になる。

【 0 0 2 9 】

上述の状態すべてにおいて、2 つの層のいずれにもゼロを含まない場合にカウンタの修復は行われ、修復後は、2 つの層のうち一方は新しいデータ値を含み、他方はゼロを含む。どの状態においても、カウンタの A 層又は B 層に見られる最大値が古い値 (X) より小さい状態にはならないことに注意すべきである。

【図面の簡単な説明】

20

【 0 0 3 0 】

【図 1】本発明による方法を実行するスマートカードのメモリの概略図である。

【図 2】書込み動作の各位相に関するメモリの 2 層カウンタの内容の概略図である。

【図 3】「突然の取出し」後の第 1 状態における書換動作の各位相に関するスマートカードの 2 層カウンタの概略図である。

【図 4】「突然の取出し」後の第 2 状態における書換動作の各位相に関するスマートカードの 2 層カウンタの概略図である。

【図 5】「突然の取出し」後の第 3 状態における書換動作の各位相に関するスマートカードの 2 層カウンタの概略図である。

【図 6】「突然の取出し」後の第 4 状態における書換動作の各位相に関するスマートカードの 2 層カウンタの概略図である。

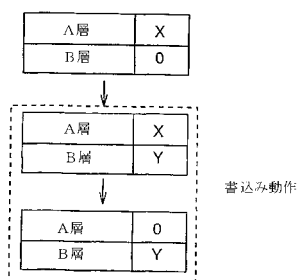
30

【図 7】「突然の取出し」後の第 5 状態における書換動作の各位相に関するスマートカードの 2 層カウンタの概略図である。

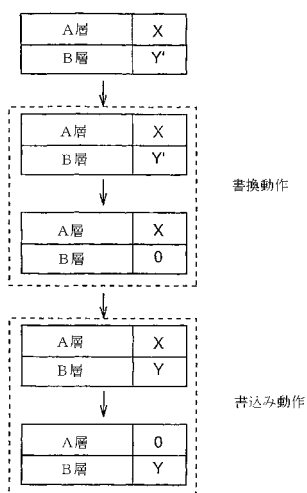
【図 1】

アドレス	16ビット/ワード
0	シリアル番号
1	
2	
3	
4	領域 1
5	
6	
7	
8	領域 2
9	
10	
11	
12	カウンタA域
13	
14	
15	
16	カウンタB域
17	
18	
19	
20	領域 3
21	
22	
23	
24	領域 4
25	
26	
27	
28	
29	
30	
31	

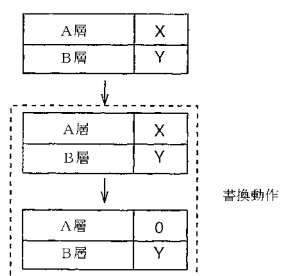
【図 2】



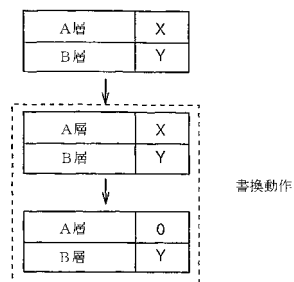
【図 5】



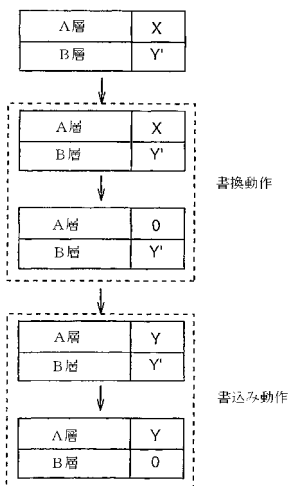
【図 6】



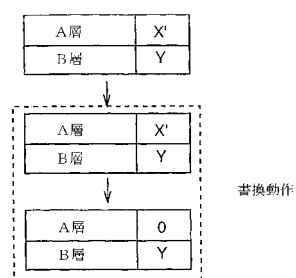
【図 3】



【図 4】



【図 7】



フロントページの続き

(74)代理人 100068685

弁理士 斎下 和彦

(72)発明者 パンゴード, ニコラ

フランス、エフ - 0 6 5 6 0 ヴァルボンヌ、ルート ド ニース、4 8 1、レ ヴェルジュ デ
ベル テール

審査官 村田 充裕

(56)参考文献 特開平 0 5 - 1 4 3 4 6 8 (J P , A)

特開平 0 4 - 3 4 4 9 9 3 (J P , A)

特開平 0 8 - 0 4 4 8 3 2 (J P , A)

特開 2 0 0 0 - 0 9 9 6 5 2 (J P , A)

特開 2 0 0 0 - 3 5 7 2 1 6 (J P , A)

特開平 0 7 - 2 4 8 9 7 8 (J P , A)

特開 2 0 0 1 - 5 2 7 2 6 3 (J P , A)

特開 2 0 0 1 - 0 4 3 1 0 1 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)

G06K 19/00-19/08

G06K 17/00

B42D 15/10