世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 **G06K 19/073, 17/00, G06F 12/14**	**A1**	(11) 国際公開番号	**WO98/34193**
		(43) 国際公開日	1998年8月6日(06.08.98)

(21) 国際出願番号 PCT/JP98/00061

(22) 国際出願日 1998年1月9日(09.01.98)

(30) 優先権データ
特願平9/16353 1997年1月30日(30.01.97) JP

(71) 出願人（米国を除くすべての指定国について）
ローム株式会社(ROHM CO., LTD.)[JP/JP]
〒615 京都府京都市右京区西院溝崎町21番地 Kyoto, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
疋田純一(HIKITA, Junichi)[JP/JP]
生藤義弘(IKEFUJI, Yoshihiro)[JP/JP]
小室豊一(KOMURO, Toyokazu)[JP/JP]
〒615 京都府京都市右京区西院溝崎町21番地
ローム株式会社内 Kyoto, (JP)
(74) 代理人
弁理士 深見久郎, 外(FUKAMI, Hisao et al.)
〒530 大阪府大阪市北区南森町2丁目1番29号
住友銀行南森町ビル Osaka, (JP)

(81) 指定国 AU, CA, CN, KR, US, 欧州特許 (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

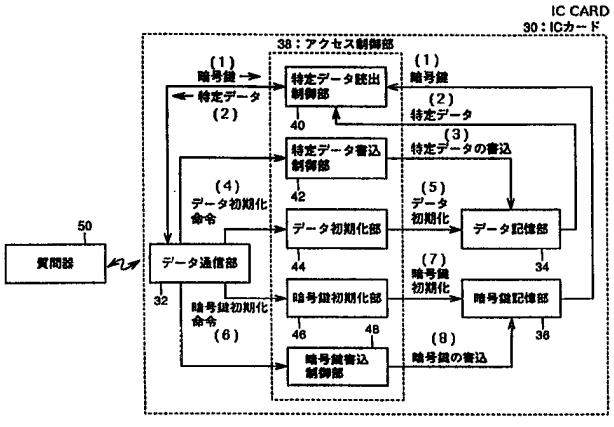
添付公開書類
国際調査報告書

(54)Title: **IC CARD AND METHOD OF USING IC CARD**

(54)発明の名称 ICカードおよびICカードの使用方法

(57) Abstract

After the initialization, a cipher key writing control unit (48) permits a cipher key memory unit (36) to write a cipher key only once. Similarly, after the initialization, a specific data writing control unit (42) permits a data memory unit (34) to write specific data only once. Thus, the cipher key and the specific data can be written by a person other than the IC card manufacturer after the IC card is manufactured, so that the flexibility in the use of the IC card can be ensured. Further, since it is prohibited to rewrite the written data, false usage of the card can be avoided. Moreover, the IC card manufacturer can initialize the data memory unit (34) and the cipher key memory unit (36) by a data initialization unit (44) and a cipher key initialization unit (46). Therefore, the IC card can be re-used, and the cost of the IC card can be lowered.



32 ... data communication unit
34 ... data storage unit
36 ... cipher key storage unit
38 ... access control unit
40 ... specific data reading control unit
42 ... specific data writing control unit
44 ... data initialization unit
46 ... cipher key initialization unit
48 ... cipher key writing control unit
50 ... interrogator
(1) ... cipher key
(2) ... specific data
(3) ... specific data writing
(4) ... data initialization command
(5) ... data initialization
(6) ... cipher key initialization command
(7) ... cipher key initialization
(8) ... cipher key writing

（５７）要約

暗号鍵書込制御部（４８）は、初期化の後、暗号鍵記憶部（３６）に対して、１回に限り暗号鍵の書込を許可する。同様に、特定データ書込制御部（４２）は、初期化の後、データ記憶部（３４）に対して、１回に限り特定データの書込を許可する。このように、ＩＣカード製造後に、ＩＣカード製造業者以外の者が暗号鍵や特定データを書込めるようになっているので、ＩＣカード運用上の柔軟性を確保することができる。また、書込まれたデータの書換は禁止されるので、不正なカードの利用を防止することができる。さらに、ＩＣカード製造業者は、データ初期化部（４４）、および暗号鍵初期化部（４６）により、データ記憶部（３４）、および暗号鍵記憶部（３６）を初期化することができる。したがって、ＩＣカードの再利用を行なうことが可能となって、ＩＣカードのコストの低下を図ることができる。

ＰＣＴに基づいて公開される国際出願のパンフレット第一頁に掲載されたＰＣＴ加盟国を同定するために使用されるコード（参考情報）

AL	アルバニア	FI	フィンランド	LT	リトアニア	SN	セネガル
AM	アルメニア	FR	フランス	LU	ルクセンブルグ	SZ	スワジランド
AT	オーストリア	GA	ガボン	LV	ラトヴィア	TD	チャード
AU	オーストラリア	GB	英国	MC	モナコ	TG	トーゴー
AZ	アゼルバイジャン	GE	グルジア	MD	モルドヴァ	TJ	タジキスタン
BA	ボスニア・ヘルツェゴビナ	GH	ガーナ	MG	マダガスカル	TM	トルクメニスタン
BB	バルバドス	GM	ガンビア	MK	マケドニア旧ユーゴスラヴィア共和国	TR	トルコ
BE	ベルギー	GN	ギニア	ML	マリ	TT	トリニダッド・トバゴ
BF	ブルキナ・ファソ	GW	ギニア・ビサオ	MN	モンゴル	UA	ウクライナ
BG	ブルガリア	GR	ギリシャ	MR	モーリタニア	UG	ウガンダ
BJ	ベナン	HU	ハンガリー	MW	マラウイ	US	米国
BR	ブラジル	ID	インドネシア	MX	メキシコ	UZ	ウズベキスタン
BY	ベラルーシ	IE	アイルランド	NE	ニジェール	VN	ヴィェトナム
CA	カナダ	IL	イスラエル	NL	オランダ	YU	ユーゴースラヴィア
CF	中央アフリカ	IS	アイスランド	NO	ノールウェー	ZW	ジンバブエ
CG	コンゴー共和国	IT	イタリア	NZ	ニューージーランド		
CH	スイス	JP	日本	PL	ポーランド		
CI	コートジボアール	KE	ケニア	PT	ポルトガル		
CM	カメルーン	KG	キルギス	RO	ルーマニア		
CN	中国	KP	北朝鮮	RU	ロシア		
CU	キューバ	KR	韓国	SD	スーダン		
CY	キプロス	KZ	カザフスタン	SE	スウェーデン		
CZ	チェッコ	LC	セント・ルシア	SG	シンガポール		
DE	ドイツ	LI	リヒテンシュタイン	SI	スロヴェニア		
DK	デンマーク	LK	スリランカ	SK	スロヴァキア		
EE	エストニア	LR	リベリア	SL	シエラ・レオーネ		
ES	スペイン	LS	レソト				

明細書

ＩＣカードおよびＩＣカードの使用方法

技術分野

この発明はＩＣカードおよびＩＣカードの使用方法に関し、特に安全性（セキュリティ）を向上させたＩＣカードおよびＩＣカードの使用方法に関する。

背景技術

スキー場のリフトや鉄道の自動改札、荷物の自動仕分けなどに、非接触型のＩＣカードを用いた通信システムが用いられる。従来の非接触型のＩＣカードの一例を第１６図に示す。第１６図に示すＩＣカード２は、１コイル型のＩＣカードであり、アンテナとして用いられるコイル４、コンデンサＣ１，Ｃ２、およびＩＣチップ８を備えている。

コンデンサＣ１，Ｃ２、およびＩＣチップ８は、フィルム状の合成樹脂基板に実装されている。コンデンサＣ１，Ｃ２、およびＩＣチップ８を実装した基板を、タブ（tab: tape automated bonding ）１０という。

第１７Ａ図に、第１６図のＩＣカード２のＳ１－Ｓ１断面図を示す。合成樹脂のコア部材１２が１対の表装材１４，１６に挟まれている。コア部材１２に設けられた空洞部１８内において露出した表層材１４に、コンデンサＣ１，Ｃ２、およびＩＣチップ８を実装したタブ１０が固定されている。タブ１０とＩＣチップ８との接合部は、エポキシ樹脂などの封止材９で被覆されている。

コイル４は、表層材１４とコア部材１２との間に配置されている。コイル４とタブ１０とは、ワイヤ２０により接続されている。

第１７Ｂ図に、ＩＣカード２の回路図を示す。ＩＣカード２は、リーダ／ライタ（質問器であり、図示しない）から送られる電磁波を、コイル４およびコンデンサＣ１により構成される共振回路２２で受け、これを電力源とする。なお、コンデンサＣ２は、電力平滑用のコンデンサである。

また、該電磁波に重畳して送られる情報をＩＣチップ８に設けられた制御部

(図示せず) が解読し、ＩＣチップ８に設けられた不揮発性メモリ (図示せず) の内容を書換えたり、リーダ／ライタに返答を行なったりする。返答は、共振回路２２のインピーダンスを変化させることにより行なう。リーダ／ライタは、ＩＣカード２側の共振回路２２のインピーダンス変化に基づく自己の共振回路 (図示せず) のインピーダンスの変化 (インピーダンス反射) を検出することにより返答内容を知る。

このように、ＩＣカード２を用いれば、カード内に電源を必要とせずかつ非接触でデータの授受を行なうことができる。

しかしながら、上述のような従来のＩＣカードを用いた通信システムは、次のような問題点があった。従来のＩＣカードを用いた通信システムにおいては、リーダ／ライタとＩＣカードとの間の通信データを暗号化することで、安全性 (セキュリティ) を担保しようとしていた。しかしながら、暗号を解読すればデータの解読、書換が可能となるため、暗号化のみではシステムの安全性を確保することが困難となる。

一方、使用済のＩＣカードのデータの書換を一切不能とすることにより、使用済のＩＣカードの不正な再生を防止する方法もある。しかし、これでは、ＩＣカードのリサイクルができなくなり、ＩＣカードのコストが上昇する。

この発明は、このような問題点を解決し、安全性が高くコストの低いＩＣカードおよびＩＣカードの使用方法を提供することをその目的としている。

発明の開示

上記目的を達成するためこの発明のある局面に従うと、ＩＣカードは、質問器との間でデータの通信を行なうデータ通信部と、データを記憶するデータ記憶部と、データ通信部から得られたデータに基づいて、データ記憶部へのアクセスを制御するアクセス制御部とを有するＩＣカードであって、アクセス制御部は、データ通信部から得られた所定のデータ初期化命令に基づいて、データ記憶部を初期化するデータ初期化部と、データ初期化部により初期化された、データ記憶部に対し、カード運用上の所定の特定データを１回に限り書込むことができるよう制御する特定データ書込制御部とを備える。

この発明によるとＩＣカードは、所定のデータ初期化命令に基づいてデータ記憶部を初期化し、初期化されたデータ記憶部に対しカード運用上の所定の特定データを１回に限り書込むことができることを特徴とする。

したがって、データ記憶部に一旦書込まれた特定データは、データ記憶部を初期化しない限り書換えることはできない。さらに、データ記憶部を初期化することができるのは、所定のデータ初期化命令を知っている者のみである。このため、特定データを書込むことができる者と、データ記憶部を初期化することができる者とを分離すれば、特定データの不正な書換をほぼ阻止することができる。すなわち、カードの安全性を向上させることができる。

また、不正な書換を阻止しつつカードを初期化することができるので、カードのリサイクルが可能となる。このため、カードのコストを低減させることができる。

さらに好ましくはそのＩＣカードは、データ記憶部に記憶された特定データにアクセスするための暗号鍵を記憶する暗号鍵記憶部をさらに備え、アクセス制御部は、暗号鍵が入力された場合にのみ、特定データを読出すことができるよう制御する特定データ読出制御部をさらに備える。

この発明によるとＩＣカードは、データ記憶部に記憶された特定データにアクセスするための暗号鍵を記憶する暗号鍵記憶部をさらに設け、暗号鍵が入力された場合にのみ、当該特定データを読出すことができることを特徴とする。

したがって、特定データを読出すことができるのは、その特定データについての暗号鍵を知っている者のみである。このため、この暗号鍵を秘密にすることにより、特定データの漏洩を防止することができる。すなわち、カードの安全性がさらに向上する。

さらに好ましくは、特定データ書込制御部は、暗号鍵が入力された場合にのみ、データ初期化部により初期化された、データ記憶部に対し、特定データを１回に限り書込むことができるよう制御することを特徴とする。

この発明によるとＩＣカードは、暗号鍵が入力された場合にのみ、初期化されたデータ記憶部に対し特定データを１回に限り書込むことができることを特徴とする。

したがって、特定データを書込むことができるのは、その特定データについての暗号鍵を知っている者のみである。このため、この暗号鍵を秘密にすることにより、所定の者以外による特定データの書込を防止することができる。

さらに好ましくは、アクセス制御部は、データ通信部から得られた所定の暗号鍵初期化命令に基づいて、暗号鍵記憶部を初期化する暗号鍵初期化部と、暗号鍵初期化部により初期化された、暗号鍵記憶部に対し暗号鍵を１回に限り書込むことができるよう制御する暗号鍵書込制御部とをさらに備える。

この発明によるとＩＣカードは、所定の暗号鍵初期化命令に基づいて、暗号鍵記憶部を初期化し、初期化された暗号鍵記憶部に対し暗号鍵を１回に限り書込むことができることを特徴とする。

したがって、暗号鍵記憶部に一旦書込まれた暗号鍵は、暗号鍵記憶部を初期化しない限り書換えることはできない。さらに、暗号鍵記憶部を初期化することができるのは、所定の暗号鍵初期化命令を知っている者のみである。このため、暗号鍵を書込むことができる者と、暗号鍵記憶部を初期化することができる者とを分離すれば、暗号鍵の不正な書換をほぼ防止することができる。すなわち、カードの安全性が一層向上する。

また、不正な書換を阻止しつつカードを初期化することができるので、カードのリサイクルが可能となる。このため、カードのコストを低減することができる。

さらに好ましくは、ＩＣカードは暗号鍵記憶部に対し暗号鍵を１回に限り書込むことができるよう構成される。

この発明によると、一旦書込まれた暗号鍵は、消去することができない。このため、暗号鍵を書換えることによるカードの不正使用を防止することができる。

さらに好ましくは、データ記憶部は特定データに対応したフラグを記憶することができ、データ初期化部は、データ初期化命令に従って前記フラグを書込可能状態に初期化し、特定データ書込制御部は、フラグが書込可能状態である場合にのみ特定データをデータ記憶部に書込むことができるよう制御し、データ記憶部に対し特定データが書込まれたときに、フラグを書込不能状態にすることを特徴とする。

この発明によるとＩＣカードは、特定データに対応したフラグを設け、初期化

命令に従って少なくとも各フラグを書込可能状態に初期化し、当該フラグが書込可能状態である場合にのみ特定データをデータ記憶部に書込むことができるようにし、データ記憶部に対し特定データが書込まれたときに、当該フラグを書込不能状態にすることを特徴とする。

したがって、特定データに対応したフラグを操作するだけで、データ記憶部を初期化したり、特定データの書換を禁止したりすることができる。このため、容易にカードの安全性を向上させることができ、カードのコストを低減することができる。

さらに好ましくは、データ記憶部は、読出および書換回数に制限のない開放データをも記憶することができることを特徴とする。

この発明によると、機密性をあまり要求されないデータをも記憶することができる。

さらに好ましくは暗号鍵記憶部は、データ記憶部に記憶された開放データにアクセスするための暗号鍵を記憶し、アクセス制御部は、開放データにアクセスするための暗号鍵が入力された場合にのみ、開放データを書換えることができるよう制御することを特徴とする。

この発明によるとＩＣカードは、データ記憶部に記憶された開放データにアクセスするための暗号鍵を記憶し、当該暗号鍵が入力された場合にのみ、開放データを書換えることができる。

したがって、開放データを書換えることができるのは、その開放データについての暗号鍵を知っている者のみである。このため、この暗号鍵を秘密にすることにより、所定の者以外による開放データの書換を防止することができる。

さらに好ましくは、データ初期化命令は、所定の方法で暗号化されたデータであり、データ初期化部は、暗号化されたデータをデータ初期化命令と認識した場合にのみデータ記憶部を初期化することを特徴とする。

この発明によるとＩＣカードのデータ初期化命令は、所定の方法で暗号化されたデータであり、暗号化されたデータをデータ初期化命令と認識した場合にのみデータ記憶部は初期化される。

したがって、所定の方法で暗号化されたデータを知っている者のみが、データ

記憶部を初期化することができる。すなわち、暗号化という比較的簡単な方法を用いて、カードの安全性を向上させることができ、カードのコストを削減することができる。

さらに好ましくはデータ通信部は、質問器との間で電磁波を介して電気的に非接触にデータの通信を行なうことを特徴とする。

この発明によると、いわゆる非接触型のＩＣカードにおいて、カードの安全性を向上させることができ、カードのコストを低減することができる。

さらに好ましくはデータ初期化命令は所定の周波数を有するデータであり、データ初期化部は、所定の周波数を有するデータをデータ初期化命令と認識した場合にのみデータ記憶部を初期化することを特徴とする。

この発明によると、所定の周波数を有するデータを与えることができる者のみが、データ記憶部を初期化することができる。すなわち、所定の者以外の者によるデータ記憶部の初期化が一層困難になる。

さらに好ましくは、データ通信部は、質問器との間で、電気的に接触してデータの通信を行なうことを特徴とする。

この発明によると、いわゆる接触型のＩＣカードにおいてカードの安全性を向上させることができ、カードのコストを低減することができる。

この発明の他の局面に従うとＩＣカードの使用方法は、質問器との間でデータの通信を行なうとともにデータを記憶するＩＣカードの使用方法であって、所定の初期化条件が整った場合にのみ、ＩＣカードの初期化を行ない得るようにするとともに、初期化されたＩＣカードに対し、所定の特定データを１回に限り書込み得るようにし、初期化を行なう者と特定データを書込む者とを分離するようにしたことを特徴とする。

この発明によると、ＩＣカードに一旦書込まれた特定データは、ＩＣカードを初期化しない限り書換えることはできない。さらに、ＩＣカードを初期化することができるのは、所定の初期化条件を知っている者のみである。また、初期化を行なう者と特定データを書込む者とを分離している。このため、特定データの不正な書換をほぼ阻止することができる。すなわち、カードを運用する際の安全性が向上する。

また、不正な書換を阻止しつつカードを初期化することができるので、カードのリサイクルが可能となる。このため、カードを運用する際のコストを低減することができる。

さらに好ましくは、初期化を行なう者はＩＣカードの製造者であり、特定データを書込む者は、質問器の製造者およびＩＣカードの運用者であり、質問器の製造者およびＩＣカードの運用者は、初期化されたＩＣカードに対し、それぞれ所定の特定データを１回に限り書込むことができ、ＩＣカードの製造者、質問器の製造者およびＩＣカードの運用者をそれぞれ分離するようにしたことを特徴とする。

この発明によると、初期化を行なうＩＣカードの製造者、特定データを書込む質問器の製造者、およびＩＣカードの運用者の三者を分離することで、カードを運用する際の機密保持に対する安全性をより向上させることができる。

さらに好ましくは、ＩＣカードに特定データにアクセスするための暗号鍵を記憶させ、暗号鍵が質問器から与えられた場合にのみ、特定データを読出すことができるようにしたことを特徴とする。

この発明によると、特定データを読出すことができるのは、その特定データについての暗号鍵を知っている者のみである。このため、その暗号鍵を秘密にすることにより、特定データの漏洩を防止することができる。すなわち、カードを運用する際の安全性がさらに向上する。

図面の簡単な説明

第１図は、この発明の第１の実施の形態におけるＩＣカードの全体構成を示す図である。

第２図は、第１図の各機能をＣＰＵを用いて実現した場合のハードウェア構成を示す図である。

第３図は、ＩＣカード３０の運用時における不揮発性メモリ７８の内容を示す図である。

第４図は、データ転送の処理を示すフローチャートである。

第５図は、データ書換の処理を示すフローチャートである。

第６図は、初期化処理を示すフローチャートである。

第７図は、初期化されたＩＣカードの不揮発性メモリ７８の内容を示す図である。

第８図は、暗号鍵の書込処理を示すフローチャートである。

第９図は、暗号鍵を書込んだ後の不揮発性メモリ７８の内容を示す図である。

第１０図は、特定データの書込処理を示すフローチャートである。

第１１図は、特定データを書込んだ後の不揮発性メモリ７８の内容を示す図である。

第１２図は、この発明によるＩＣカードの利用および再利用状況を示す図である。

第１３Ａおよび第１３Ｂ図は、本発明の第２の実施の形態において、暗号鍵をＥＰＲＯＭ１００に記憶した場合を示す図である。

第１４図は、本発明の第２の実施の形態において、暗号鍵（Ｉ）のための比較器１１４を設けた場合を示す図である。

第１５図は、本発明の第３の実施の形態において、初期化のための検出回路１２２を設けた場合を示す図である。

第１６図は、従来の非接触型のＩＣカードの一例を示す図である。

第１７Ａおよび第１７Ｂ図は、第１６図におけるＳ１－Ｓ１断面を示す図、およびＩＣカード２の回路図である。

発明を実施するための最良の形態

本発明をより詳細に説明するために、添付の図面に従ってこれを説明する。

［第１の実施の形態］

第１図は、この発明の第１の実施の形態におけるＩＣカード３０の全体構成を示すブロック図である。ＩＣカード３０は、１コイル型のＩＣカードであり、スキー場のリフトや鉄道の自動改札、荷物の自動仕分けなどに用いることができる。

ＩＣカード３０は、データ通信部３２と、データ記憶部３４と、暗号鍵記憶部３６と、アクセス制御部３８とを備えている。データ通信部３２は、質問器５０との間でデータの通信を行なう。データ記憶部３４は、データを記憶する。暗号

鍵記憶部３６は、データ記憶部３４に記憶された特定データにアクセスするための暗号鍵を記憶する。

アクセス制御部３８は、データ通信部３２から得られたデータに基づいて、データ記憶部３４、および暗号鍵記憶部３６へのアクセスを制御する。アクセス制御部３８は、特定データ読出制御部４０と、特定データ書込制御部４２と、データ初期化部４４と、暗号鍵初期化部４６と、暗号鍵書込制御部４８とを備えている。

質問器５０からデータ初期化命令および暗号鍵初期化命令が与えられると、データ通信部３２はこれを受信する。データ初期化部４４は、データ初期化命令を受けて、データ記憶部３４の記憶内容を初期化する。また、暗号鍵初期化部４６は、暗号鍵初期化命令を受けて、暗号鍵記憶部３６に記憶された暗号鍵を初期化する。このように初期化された状態でこのＩＣカード３０は、カードを使用・運用する事業者に渡される。

カードを運用する事業者は、質問器５０からＩＣカード３０に対して暗号鍵を書込むようにする。この暗号鍵は、データ通信部３２を介して、暗号鍵書込制御部４８に与えられる。暗号鍵書込制御部４８は、暗号鍵記憶部３６に対して、この暗号鍵の書込を行なうように制御する。なお、暗号鍵書込制御部４８は、上記のような暗号鍵の書込を１回に限り許可するように制御する。したがって、カードを運用する事業者以外の者が、この暗号鍵を書換えることはできないようになっている。

カードを運用する事業者は、さらに質問器５０からＩＣカード３０に対して特定データを書込むようにする。この特定データは、データ通信部３２を介して、特定データ書込制御部４２に与えられる。特定データ書込制御部４２は、データ記憶部３４に対して、この特定データの書込を行なうように制御する。なお、特定データ書込制御部４２は、上記のような特定データの書込を１回に限り許可するように制御する。したがって、カードを運用する事業者以外の者が、この特定データを書換えることはできないようになっている。

カードを使用する場合に、質問器５０の側が、データ記憶部３４に記憶された特定データが必要である場合には、暗号鍵を送信する。この暗号鍵は、データ通

信部３２を介して、特定データ読出制御部４０に与えられる。特定データ読出制御部４０は、暗号鍵記憶部３６から暗号鍵を読出すとともに、送信された暗号鍵がこれに一致しているか否かを判断する。一致していなければ、データ記憶部３４からの特定のデータの読出を許否する。これにより、暗号鍵を知らない者に対して、特定データの秘密性を保護することができる。一致していれば、データ記憶部３４から特定データを読出して、データ通信部３２を介して質問器５０に送り返す。

なお、ＩＣカード３０に対して、データ初期化命令、暗号鍵初期化命令を与えることにより、当該ＩＣカード３０を再利用することができる。また、ＩＣカードの製造事業者以外の者がこのデータ初期化命令や暗号鍵初期化命令を知り得ないようにしておくことにより、カードの不正使用を防止することができる。

第２図は、第１図のＩＣカード３０の各機能を、ＣＰＵを用いて実現した場合のハードウェア構成を示す図である。質問器５０は、制御部５４の制御により、発振回路（ＯＳＣ）６０からの高周波搬送波をアンテナ５６から送り出している。質問器５０に対してＩＣカード３０が接近すると、この高周波搬送波は、ＩＣカード３０のアンテナ８２に受信される。電源生成回路７２は、受信した高周波を直流電力に変換して、他の回路部分に供給する。このようにして、質問器５０に近づくとＩＣカード３０が動作可能となる。

質問器５０からＩＣカード３０に対する情報送信は、制御部５４の制御により、高周波搬送波を変復調回路５２において変調することにより行なう。ＩＣカード３０は、変調された高周波搬送波を変復調回路７４において復調する。ＣＰＵ７６は、復調された情報を得て、不揮発性メモリ７８の内容の書換や情報返信などの必要な処理を行なう。

上記と逆に、ＩＣカード３０から質問器５０に対しての情報送信も行なわれる。ここで、ＩＣカード３０側には、発振回路が設けられていない。したがって、質問器５０の側から無変調の高周波搬送波を送り出しておき、ＩＣカード３０側にて、変復調回路７４により、共振回路８０のインピーダンスを変化させるようにしている。質問器５０は、このインピーダンス変化を、自己側の共振回路５６のインピーダンス変化として、変復調回路５２により検出して復調を行なう。制御

部５４は、復調された情報を得て、必要な処理を行なう。

ＩＣカード３０が質問器５０から遠ざかると、電力供給がなくなるので、ＩＣカード３０の動作は停止する。しかし、不揮発性メモリ７８を用いているので、電力供給がなくなっても、記憶された情報は保持される。なお、この実施の形態では不揮発性メモリ７８として、ＥＥＰＲＯＭを用いている。

第３図に、ＩＣカード３０の使用時における、不揮発性メモリ７８の記憶内容を示す。なお、ここではＩＣカード３０を、非接触型の現金自動取引機（ＡＴＭ）におけるキャッシュカードとして用いた場合を例にとって説明する。この場合、質問器５０は、ＡＴＭの一部としてその内部に収納されている。

オープンデータ（開放データ）領域８４には、書換えることが可能な比較的機密性の低いオープンデータ（ａ）（ｂ）……が記憶されている。たとえば、取引履歴などのデータがオープンデータとして記憶される。特定データ領域８６には、特定データ（１）（２）……が記憶されている。たとえば、非接触カード型のＡＴＭ装置の形式やカードの利用者のＩＤ番号などが特定データとして記憶される。この特定データは、ＡＴＭの製造業者や、運用者である銀行によって書込まれたものである。暗号鍵領域８８には、暗号鍵（１）（２）……（Ｄ）（Ｉ）が記憶されている。暗号鍵（１）（２）……（Ｄ）は、ＡＴＭの製造業者や、運用者である銀行によって書込まれたものである。また、暗号鍵（Ｉ）は、ＩＣカードの製造業者によって書込まれたものである。

次に、ＩＣカード３０の使用時における動作を第２図～第４図を参照して説明する。預金者がＩＣカード３０（キャッシュカード）を持って、ＡＴＭに近づくと、ＩＣカード３０とＡＴＭとの間で通信が可能となる。ＡＴＭの質問器５０が、ＩＣカード３０の不揮発性メモリ７８に記憶されたオープンデータ（取引履歴など）や特定データ（装置形式、ＩＤ番号）を取得する場合には、以下のようにして行なう。

質問器５０は、ＩＣカード３０に対して、データの転送命令および予め定めた暗号鍵を与える。すなわち、質問器５０の制御部５４は、変復調回路５２を制御して、搬送波をデータ転送命令および暗号鍵によって変調して送り出す。ＩＣカード３０の変復調回路７４は、このデータ転送命令および暗号鍵を復調し、ＣＰ

Ｕ７６に与える。ＣＰＵ７６は、データ転送命令が送られてきたことを認識して、データ転送のプログラムを実行する。このプログラムは、不揮発性メモリ７８に記憶されている。

第４図に、データ転送プログラムをフローチャートによって示す。ＣＰＵ７６は、まず不揮発性メモリ７８の暗号鍵領域８８から、データ転送に対応して予め定められた暗号鍵（ここでは暗号鍵（１）とする）を読出す。次に、送られてきた暗号鍵が、読出した暗号鍵（１）と一致するか否かを判断する（ステップＳ３０）。一致していなければ、データの転送を行なわず終了する。つまり、正しい暗号鍵を知らない不正者による読出処理であると判断して、データ転送を許否する。一方、暗号鍵が一致すれば、特定データまたはオープンデータを、不揮発性メモリ７８から読出す。さらに、読出したデータを、変復調回路７４によって変調して、質問器５０に送信する（ステップＳ３２）。ＡＴＭは、質問器５０の取得したデータに基づいて、センターの中央コンピュータと交信して、入出金などの処理を行なう。以上のようにして、正しい暗号鍵を有する応答器５０からのデータ転送命令にのみ応じて、データの出力を行なう。

上記のようにして入出金などの取引が終了すると、質問器５０は、ＩＣカード３０の不揮発性メモリ７８に記憶された取引履歴を更新する命令（データ書換命令）を送信する。この際にも、質問器５０は、予め定められた暗号鍵を送信する。ＩＣカード３０のＣＰＵ７６は、このデータ書換命令を受けると、データ書換のプログラムを実行する。

第５図に、データ書換のプログラムをフローチャートによって示す。ＣＰＵ７６は、まず不揮発性メモリ７８の暗号鍵領域８８から、データ書換に対応して予め定められた暗号鍵（ここでは暗号鍵（１）とする）を読出す。次に、送られてきた暗号鍵が、読出された暗号鍵（１）と一致するか否かを判断する（ステップＳ４０）。一致していなければ、取引データの書込（データの書換）を行なわず終了する。つまり、正しい暗号鍵を知らない不正者による書換処理であると判断して、取引データの書換を許否する。一方、暗号鍵が一致すれば、次にデータ書換要求のあった対象領域が、オープンデータ領域８４であるか否かを判断する（ステップＳ４２）。オープンデータ領域８４に対する書換命令であれば、送ら

れてきた取引データに基づいて、取引履歴の書換を行なう（ステップＳ４４）。つまり、オープンデータ領域８４に記憶したデータは、正しい暗号鍵を入力することにより書換を行なうことができる。

なお、このデータ書換命令に対しては、オープンデータ領域のみが書換可能であり、それ以外の領域（特定データ領域や暗号鍵領域）は、この書換命令では書換できないようになっている。特定データ領域や暗号鍵領域に対する書込や読出については、後述する。

以上のようなＩＣカード３０の運用を行なうためには、ＩＣカード製造業者から供給されたＩＣカード３０に対して、ＡＴＭ製造業者および運用業者（銀行）が、それぞれの暗号鍵および特定データを書込可能でなければならない。ＩＣカード製造業者が、ＡＴＭ製造業者、および運用業者（銀行）のために、暗号鍵、特定データを書込んで出荷することも可能である。しかし、これでは柔軟な運用ができず、ＡＴＭ製造業者、運用業者（銀行）にとっては、使いづらいシステムとなってしまう。そこでこの実施の形態では、ＡＴＭ製造業者および運用業者（銀行）が、それぞれの暗号鍵および特定データを書込できるようにしている。

以下、これらＡＴＭ製造業者および運用業者（銀行）が、それぞれの暗号鍵および特定データを書込む場合の処理を説明する。ＩＣカード製造業者から渡されたＩＣカード３０の不揮発性メモリ７８の初期状態は、第７図に示すようになっている。図からも明らかなように、ＩＣカードの製造業者のみが知る暗号鍵（Ｉ）を除いて、すべてのデータが初期化（ここでは「０」）されている。

暗号鍵および特定データの書込は、運用時のＡＴＭが有するのと同等の質問器５０を有するリーダ／ライタによって行なう。すなわち、リーダ／ライタの質問器５０から暗号鍵の書込命令を送信する（第２図参照）。これを受けて、ＩＣカード３０のＣＰＵ７６は、第８図に示す暗号鍵の書換処理を行なう。まず、暗号鍵領域８８中の暗号鍵を書込みたい部分のＫフラグが「０」であるか否かを判断する（ステップＳ１０）。「０」であれば、送られてきた暗号鍵を、暗号鍵領域８８の当該部分に書込む（ステップＳ１２）。その後、当該部分のＫフラグを「１」とする（ステップＳ１４）。このようにして、暗号鍵の書込を行なうことができる。

なお、既に書込が行なわれＫフラグが「１」である部分に対して書込を行なおうとした場合には、ステップＳ１０から直ちに分岐して、書換を許否する。また、暗号鍵領域８８には、複数の暗号鍵を記憶可能なようにしているので、１つの事業者が処理内容に応じた暗号鍵を複数設定したり、また２以上の事業者（ＡＴＭ製造業者、カード運用業者など）が、それぞれのために暗号鍵を設定することが可能である。暗号鍵が書込まれた後の不揮発性メモリ７８の内容を、第９図に例示する。

特定データの書込処理を第１０図に示す。特定データの書込においても、暗号鍵と同じように、Ｓフラグが「０」であることを条件に、書込を可能としている。また、一旦書込んだ後は、Ｓフラグを「１」として書換を不可能にしている。特定データが書込まれた後の不揮発性メモリ７８の内容を、第１１図に例示する。なお、当該カードに対応している質問器５０の装置形式や、銀行が各預金者に対して発行したＩＤ番号などを特定データとして記憶することが好ましい。これらのデータは、機密性が高く、また、これらの書換が不正な使用に結びつく可能性が高いからである。

上記のように一旦暗号鍵、または特定データが書込まれると当該部分のフラグＫ、Ｓが「１」となり、書換不可能となるようにしている。つまり、１回のみの書込みを可能としている。したがって、暗号鍵、特定データを、ＡＴＭ製造業者、銀行が書込みできるようにして、運用上の柔軟性を高めるとともに、これらの書換による不正を防止して、セキュリティを高めている。

さらに、この実施の形態においては、使用済のＩＣカード３０を回収し、ＩＣカード製造業者が処理することによってＩＣカードを再利用可能としている。この処理は、ＩＣカード製造業者が、質問器５０を有する初期化装置を用いて行なう。すなわち、初期化装置の質問器５０から、不揮発性メモリ７８の初期化命令を、初期化のための暗号鍵とともに送信する（第２図参照）。これを受けて、ＩＣカード３０のＣＰＵ７６は、第６図に示す初期化処理を行なう。まず、不揮発性メモリ７８から、初期化のための暗号鍵（Ｉ）を読出す。次に、送られてきた暗号鍵が、この読出した暗号鍵（Ｉ）と一致しているか否かを判断する（ステップＳ２）。一致していれば、暗号鍵（Ｉ）を除いた、他の部分を初期化する（こ

こでは「0」にする）（ステップＳ４）。これにより、不揮発性メモリ７８の内容は、第７図に示すように、初期の状態に戻され、再利用が可能となる。

なお、暗号鍵が一致しない場合には、不正な初期化命令であるとして初期化を行なわない。また、初期化のための暗号鍵がN回以上連続して誤って入力された場合、初期化命令を受付けないようにしてもよい。これにより、組合せ可能なすべてのコードを暗号鍵として順次入力し、暗号鍵を不正に取得することを防止することができる。

以上のようにして、セキュリティを確保しつつ、ＩＣカード３０の再利用を可能としている。

このＩＣカード３０の再利用のサイクルを第１２図に概念的に示す。ＩＣカードの製造業者９０は、不揮発性メモリ７８を初期化してＩＣカードを出荷する。なお、各データ領域へのアクセス制御を行なうプログラム（前述のフローチャート参照）をＩＣカードに書込んだ状態にして出荷する。

ＡＴＭの製造業者９２は、このＩＣカードを受け取って、暗号鍵（１）および特定データ（１）を書込む。また、運用のためのプログラムも書込む。なお、このプログラムは、当該暗号鍵（１）によってのみ読出、書換が可能である。暗号鍵（１）は、ＡＴＭ製造者９２のみが知っており、ＩＣカードの製造業者９０、およびＩＣカードの運用業者９４も知らないので、セキュリティの面で好ましい結果を得ることができる。また、前述のように、暗号鍵、特定データの読出はもちろん、書換もできないようになっているので、不正使用が防止できる。

ＩＣカードの運用業者（銀行）９４は、運用プログラムの記録されたＩＣカード３０を受け取って、暗号鍵（２）および特定データ（２）（各預金者に与えたＩＤ番号など）を書込む。ここでも、暗号鍵（２）および特定データ（２）は、ＩＣカード運用業者９４および当該預金者のみが知っており、ＩＣカードの製造業者９０、およびＡＴＭ製造者９２も知らないので、セキュリティの上から好ましい。また、前述のように、暗号鍵、特定データの読出はもちろん書換もできないようになっているので、不正使用が防止できる。

使用が終了したＩＣカード３０（たとえば、有効期限の終了したもの）は、ＩＣカード製造業者９０に戻され、初期化して再利用される。

なお、ＡＴＭの製造者９２による暗号鍵（１）もしくは特定データ（１）の誤った書込が行なわれた場合、ＡＴＭの製造者９２自身は、これらの書換をすることができない。そこで、誤った書込がされてしまったＩＣカードをＩＣカードの製造者９０に渡し、ＩＣカードの製造者９０がこのカードの初期化をした後、再びＡＴＭの製造者９２に渡すことになる。ＩＣカードの運用業者９４による暗号鍵（２）もしくは特定データ（２）の誤った書込が生じた場合も、これと同様である。

以上のように、このＩＣカード３０を用いれば、各業者における柔軟なＩＣカードの運用の確保とセキュリティを両立させつつ、さらに再利用を図ることによるＩＣカードの低コスト化を同時に実現できる。

また、初期化のために特別に容易された質問器を、ＩＣカードの製造者９０が１台のみ保有することにしておけば、一層セキュリティを高めることができるため、さらに好ましい。

[第２の実施の形態]

なお、上記第１の実施の形態では、不揮発性メモリ７８としてＥＥＰＲＯＭを用いたが、第１３Ａ図および第１３Ｂ図に示すように、暗号鍵領域８８のみをＥＰＲＯＭによって構成してもよい。つまり、電気的な再書込を不可能とすることによって、より安全性を高めることができる。

さらに、ＥＰＲＯＭに対して、紫外線を照射できないようにして、実質的に書換ができないようにしてもよい。この場合には、各暗号鍵をＡＴＭ製造業者、カード運用業者から事前に知らせてもらっておき、ＩＣカード製造業者がＩＣカード製造時に各暗号鍵を書込むようにする。これによれば、暗号鍵を書換えることはできないが、特定データを書換えて再利用することができる。

またさらに、ＩＣカード製造業者のための暗号鍵（Ｉ）は、変更しなくてもよいので、この領域のみをマスクＲＯＭによって構成してもよい。暗号鍵（Ｉ）を用いた初期化の処理は、第６図に示されるように、プログラムによって行なってもよいが、第１４図に示されるように、比較器１４を設けることにより行なってもよい。すなわちＲＯＭ１１２には、暗号鍵（Ｉ）を記憶しておく。比較器１１４は、ＣＰＵ７６の指示により、復調された暗号鍵を、ＲＯＭ１１２に記憶され

ている暗号鍵（Ｉ）と比較する。比較器１１４は、両者が一致していると、ＣＰＵ７６に対して一致信号を出力する。一致していない場合には、不一致信号を出力する。ＣＰＵ７６は、このようにして得られる比較器１１４からの一致信号・不一致信号に基づいて、送られてきた暗号鍵が適正であるか否かを判断する。

［第３の実施の形態］

次に、ＩＣカードの初期化に関する本発明の第３の実施の形態について説明する。第１５図は、本発明の第３の実施の形態におけるＩＣカードのハードウェア構成を示すブロック図である。この実施の形態においては、通常の受信周波数とは異なる周波数の信号を与えることで、カード初期化命令としている。

たとえば、質問器５０から、共振回路８０の共振周波数の高調波にあたらない所定の周波数にて所定の断続信号を出力する。ＩＣカード１２０の検出回路１２２は、当該所定の周波数のみを検出するバンドパスフィルタを有している。さらに、検出回路１２２は、当該周波数を検出したときにのみ、検出出力信号を出す。つまり、断続的に当該周波数の信号が送られてきている場合には、その断続に応じて検出出力信号が出力される。ＣＰＵ７６は、この検出出力信号を受けて、予め定められた断続パターンに合致しているか否かを判断する。この断続パターンの一致が見られた場合にのみ、ＣＰＵ７６は、第６図のステップＳ４の処理を実行する。つまり、メモリの初期化を行なう。

当該周波数の信号が送られてこない場合や、送られてきていても断続パターンが予め定められたものに合致しない場合には、初期化は行なわれない。したがって、初期化のために特別に用意された質問器５０を有していなければ、初期化を行なうことができない。このようにすることにより、よりセキュリティを高めることができる。

なお、上記各実施の形態においては、質問器とＩＣカードとの間のデータは、暗号化せずに伝送することとしたが、所定の暗号化を行なって伝送するようにしてもよい。さらに、上記各実施の形態においては、パスワードのように用いられていた暗号鍵を、上記暗号化のための暗号キーとして用いて、データを暗号化して記憶し、暗号化して伝送するようにしてもよい。

また、上記各実施の形態においては、暗号鍵が不正な場合には、プログラムの

処理として、読出および書込を禁止するようにしている。しかし、ＣＰＵ７６が暗号鍵を不正であると判断した場合には、不揮発性メモリ７８のチップイネーブル端子などに動作禁止の信号を与え、ハードウェア的に読出および書込を禁止するようにしてもよい。

さらに、上記各実施の形態では、ＡＴＭに対応したＩＣカードを運用する場合について説明したが、スキー場のリフト改札用のＩＣカード、鉄道の定期券、高速道路の通行定期などに本発明を適用することもできる。つまり、カードに対応する機器を製造する業者や運用業者が特定データを個々に記憶したいような場合に、本発明を適用することができる。

さらに、上記各実施の形態において、第１図の各機能をＣＰＵを用いてプログラムによって実現した部分を、ハードウェアロジックによって実現してもよい。また、ハードウェアロジックによって実現した部分を、プログラムによって実現してもよい。

また、上記実施の形態においては電磁波を介して電気的に非接触にデータの通信を行なうカードについて説明したが、電気的に接触してデータの通信を行なうカードに対しても、本発明を適用することができる。

なお、「特定データ読出制御手段」とは、暗号鍵に基づいて特定データの読出の可否を制御する手段であり、たとえば実施の形態においては、第４図のステップＳ３０、およびＳ３２がこれに相当する。

「特定データ書込制御手段」とは、データ記憶部に対して１回に限り特定データを書込めるように制御する手段をいうものであり、たとえば実施の形態では第１０図のステップＳ２０、Ｓ２２、およびＳ２４がこれに相当する。

「データ初期化手段」とは、データ記憶部の少なくとも特定データ領域の一部または全部を初期化する手段をいうものであり、たとえば実施の形態においては、第６図のステップＳ２、Ｓ４、または第１４図の比較器１１４、または第１５図の検出回路１２２などがこれに相当する。なお、ここにいうデータの初期化とは、特定データが再書込可能となるようにすることをいう。したがって、実施の形態において示された、特定データを消去してＳフラグを再書込可能とする場合だけではなく、特定データを残したままＳフラグを再書込可能状態にする場合を含む

概念である。

「暗号鍵初期化手段」とは、暗号鍵の一部または全部を初期化する手段をいうものであり、たとえば実施の形態では、第６図のステップＳ２、Ｓ４、第１４図の比較器１１４、または第１５図の検出回路１２２などがこれに相当する。

なお、ここにいう暗号鍵の初期化とは、暗号鍵が再書込可能となるようにすることをいう。したがって、実施の形態において示した、暗号鍵を消去してＫフラグを再書込可能とする場合だけでなく、暗号鍵を残したままＫフラグを再書込可能状態にする場合を含む概念である。

「暗号鍵書込制御手段」とは、暗号鍵記憶部に対して１回に限り暗号鍵を書込めるように制御する手段をいうものであり、実施の形態においてはたとえば、第８図のステップＳ１０、Ｓ１２、およびＳ１４がこれに相当する。

産業上の利用可能性

以上のようにこの発明によれば、リサイクルすることができ安全性の高いＩＣカードを提供することができるので、この発明はＩＣカードを製造、販売または使用する分野において有利に適用することができる。

請求の範囲

1．質問器との間でデータの通信を行なうデータ通信手段と、

データを記憶するデータ記憶部と、

前記データ通信手段から得られたデータに基づいて、前記データ記憶部へのアクセスを制御するアクセス制御手段とを有するＩＣカードであって、

前記アクセス制御手段は、

前記データ通信手段から得られた所定のデータ初期化命令に基づいて、前記データ記憶部を初期化するデータ初期化手段と、

前記データ初期化手段により初期化された、前記データ記憶部に対し、カード運用上の所定の特定データを１回に限り書込むことができるよう制御する特定データ書込制御手段とを備えた、ＩＣカード。

2．前記データ記憶部に記憶された特定データにアクセスするための暗号鍵を記憶する暗号鍵記憶部をさらに備え、

前記アクセス制御手段は、当該暗号鍵が入力された場合にのみ、当該特定データを読出すことができるよう制御する特定データ読出制御手段をさらに備えた、請求の範囲第１項記載のＩＣカード。

3．前記特定データ書込制御手段は、前記暗号鍵が入力された場合にのみ、前記データ初期化手段により初期化された、前記データ記憶部に対し、前記特定データを１回に限り書込むことができるよう制御することを特徴とした、請求の範囲第２項記載のＩＣカード。

4．前記アクセス制御手段は、

前記データ通信手段から得られた所定の暗号鍵初期化命令に基づいて、前記暗号鍵記憶部を初期化する暗号鍵初期化手段と、

前記暗号鍵初期化手段により初期化された、前記暗号鍵記憶部に対し暗号鍵を１回に限り書込むことができるよう制御する暗号鍵書込制御手段とをさらに備えた、請求の範囲第２項記載のＩＣカード。

5．前記暗号鍵記憶部に対し、暗号鍵を１回に限り書込むことができるよう構成したことを特徴とする、請求の範囲第２項記載のＩＣカード。

6．前記データ記憶部は、前記特定データに対応したフラグを記憶することがで

き、

前記データ初期化手段は、前記データ初期化命令に従って前記フラグを書込可能状態に初期化し、

前記特定データ書込制御手段は、前記フラグが書込可能状態である場合にのみ前記特定データを前記データ記憶部に書込むことができるよう制御し、前記データ記憶部に対し前記特定データが書込まれたときに、前記フラグを書込不能状態にすることを特徴とする、請求の範囲第１項記載のＩＣカード。

７．前記データ記憶部は、読出および書換回数に制限のない開放データをも記憶することができることを特徴とする、請求の範囲第１項記載のＩＣカード。

８．前記データ記憶部は、読出および書換回数に制限のない開放データをも記憶することができることを特徴とする、請求の範囲第２項記載のＩＣカード。

９．前記暗号鍵記憶部は、前記データ記憶部に記憶された開放データにアクセスするための暗号鍵を記憶し、前記アクセス制御手段は、前記開放データにアクセスするための暗号鍵が入力された場合にのみ、前記開放データを書換えることができるよう制御することを特徴とする、請求の範囲第８項記載のＩＣカード。

１０．前記データ初期化命令は、所定の方法で暗号化されたデータであり、

前記データ初期化手段は、前記暗号化されたデータをデータ初期化命令と認識した場合にのみ前記データ記憶部を初期化することを特徴とする、請求の範囲第１項記載のＩＣカード。

１１．前記データ通信手段は、前記質問器との間で、電磁波を介して電気的に非接触にデータの通信を行なうことを特徴とする、請求の範囲第１項記載のＩＣカード。

１２．前記データ初期化命令は、所定の周波数を有するデータであり、

前記データ初期化手段は、前記所定の周波数を有するデータをデータ初期化命令と認識した場合にのみ前記データ記憶部を初期化することを特徴とする、請求の範囲第１１項記載のＩＣカード。

１３．前記データ通信手段は、前記質問器との間で、電気的に接触してデータの通信を行なうことを特徴とする、請求の範囲第１項記載のＩＣカード。

１４．質問器との間でデータの通信を行なうとともにデータを記憶するＩＣカー

ドの使用方法であって、

所定の初期化条件が整った場合にのみ、前記ＩＣカードの初期化を行ない得るようにするとともに、

初期化された前記ＩＣカードに対し、所定の特定データを１回に限り書込み得るようにし、

前記初期化を行なう者と前記特定データを書込む者とを分離するようにしたことを特徴とする、ＩＣカードの使用方法。

１５．前記初期化を行なう者は、前記ＩＣカードの製造者であり、

前記特定データを書込む者は、前記質問器の製造者および前記ＩＣカードの運用者であり、

前記質問器の製造者および前記ＩＣカードの運用者は、初期化された前記ＩＣカードに対し、それぞれ所定の特定データを１回に限り書込むことができ、

前記ＩＣカードの製造者、前記質問器の製造者および前記ＩＣカードの運用者をそれぞれ分離するようにしたことを特徴とする、請求の範囲第１４項記載のＩＣカードの使用方法。

１６．前記ＩＣカードに、前記特定データにアクセスするための暗号鍵を記憶させ、

前記暗号鍵が前記質問器から与えられた場合にのみ、前記特定データを読出すことができるようにしたことを特徴とする、請求の範囲第１４項記載のＩＣカードの使用方法。

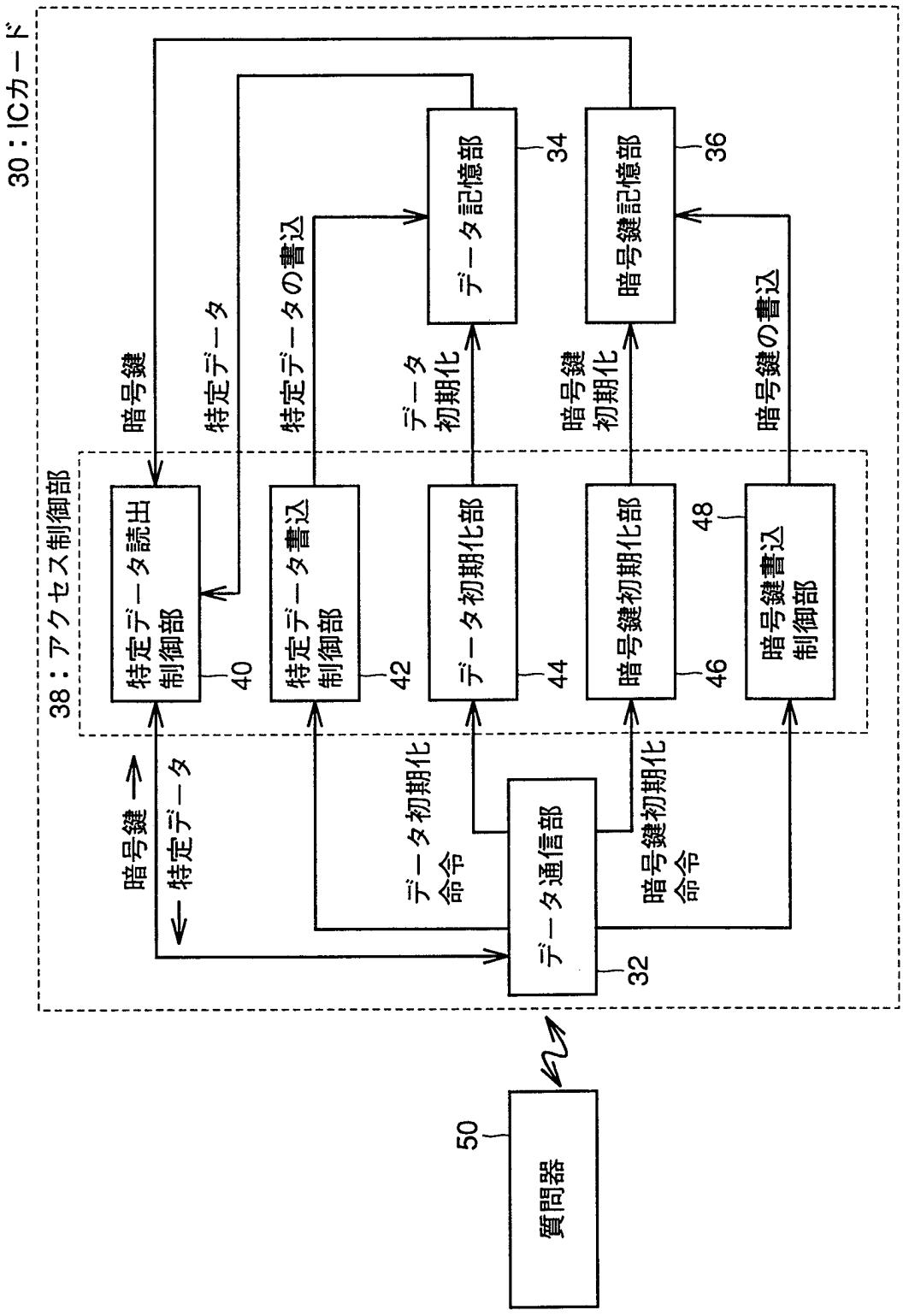

30：ICカード
38：アクセス制御部
特定データ読出制御部
40
特定データ書込制御部
42
データ初期化部
44
暗号鍵初期化部
46
暗号鍵書込制御部
48
データ通信部
32
データ記憶部
34
暗号鍵記憶部
36
暗号鍵
特定データ
特定データの書込
データ初期化命令
暗号鍵初期化命令
暗号鍵の書込
暗号鍵
特定データ
データ初期化
暗号鍵初期化
質問器
50

FIG.1

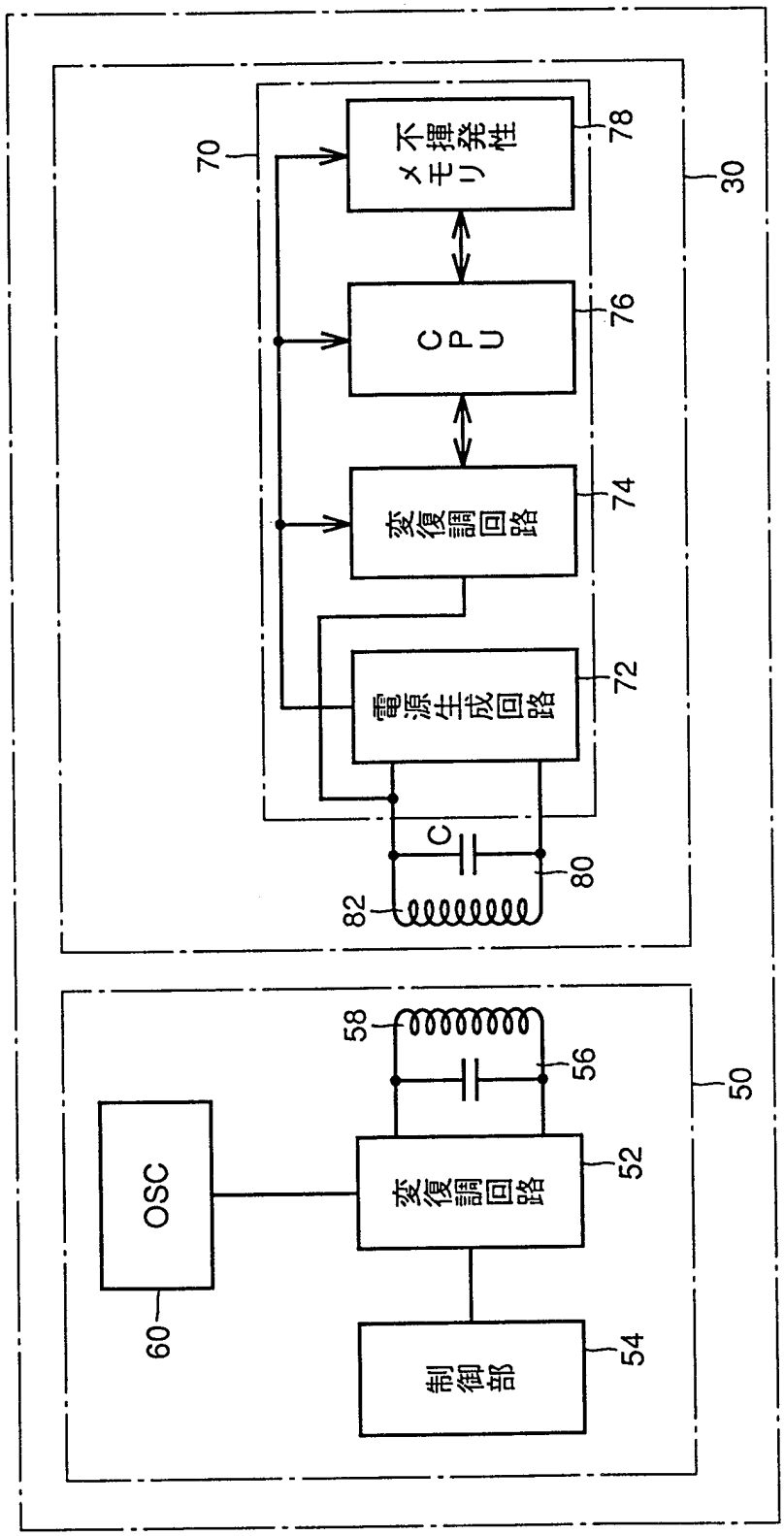

70
不揮発性メモリ
78
30
CPU
76
変復調回路
74
電源生成回路
72
C
80
82
58
56
50
OSC
変復調回路
52
60
制御部
54

FIG.2

FIG.3

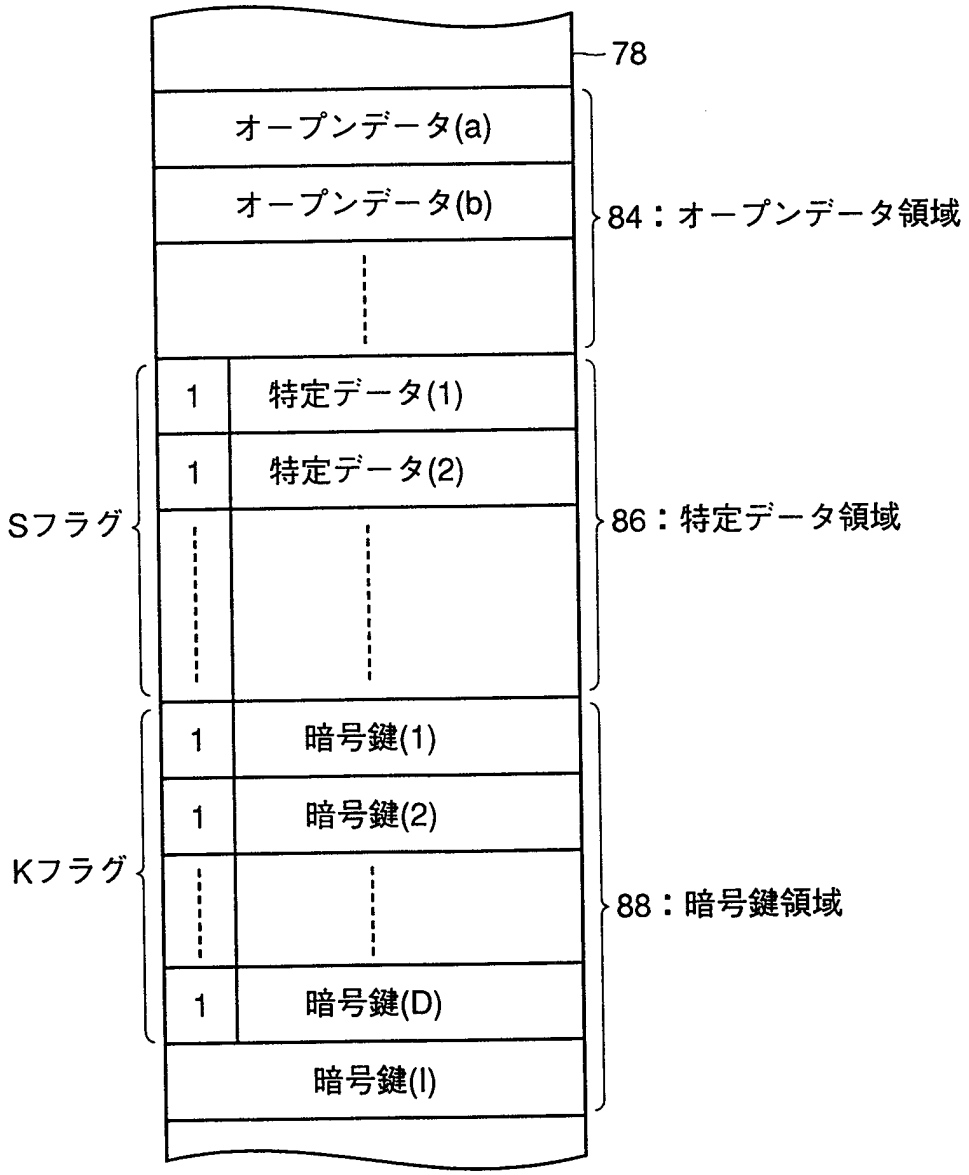

78
オープンデータ(a)
オープンデータ(b)
84：オープンデータ領域
Sフラグ
1
特定データ(1)
1
特定データ(2)
86：特定データ領域
Kフラグ
1
暗号鍵(1)
1
暗号鍵(2)
88：暗号鍵領域
1
暗号鍵(D)
暗号鍵(I)

FIG.4

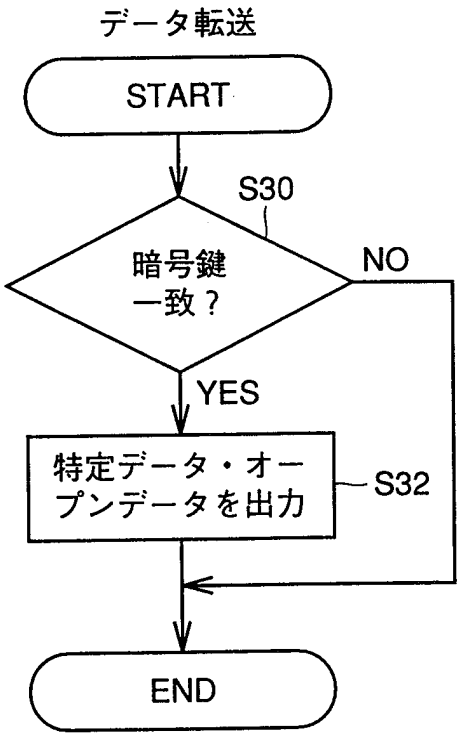


FIG.5

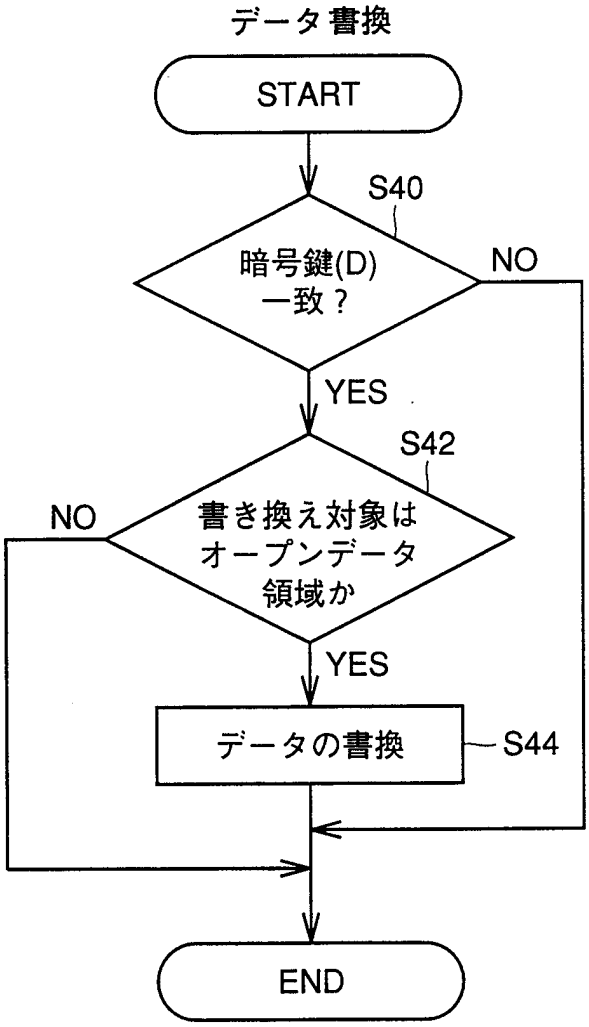

データ書換
START
S40
暗号鍵(D)
一致？
NO
YES
S42
NO
書き換え対象は
オープンデータ
領域か
YES
データの書換
S44
END

FIG.6

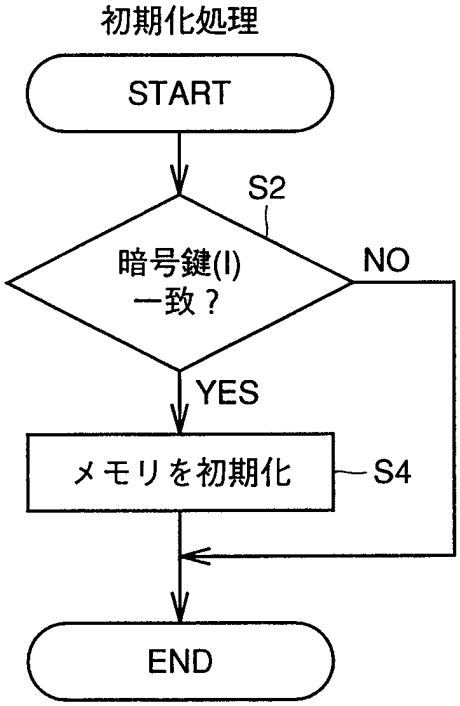


FIG.7

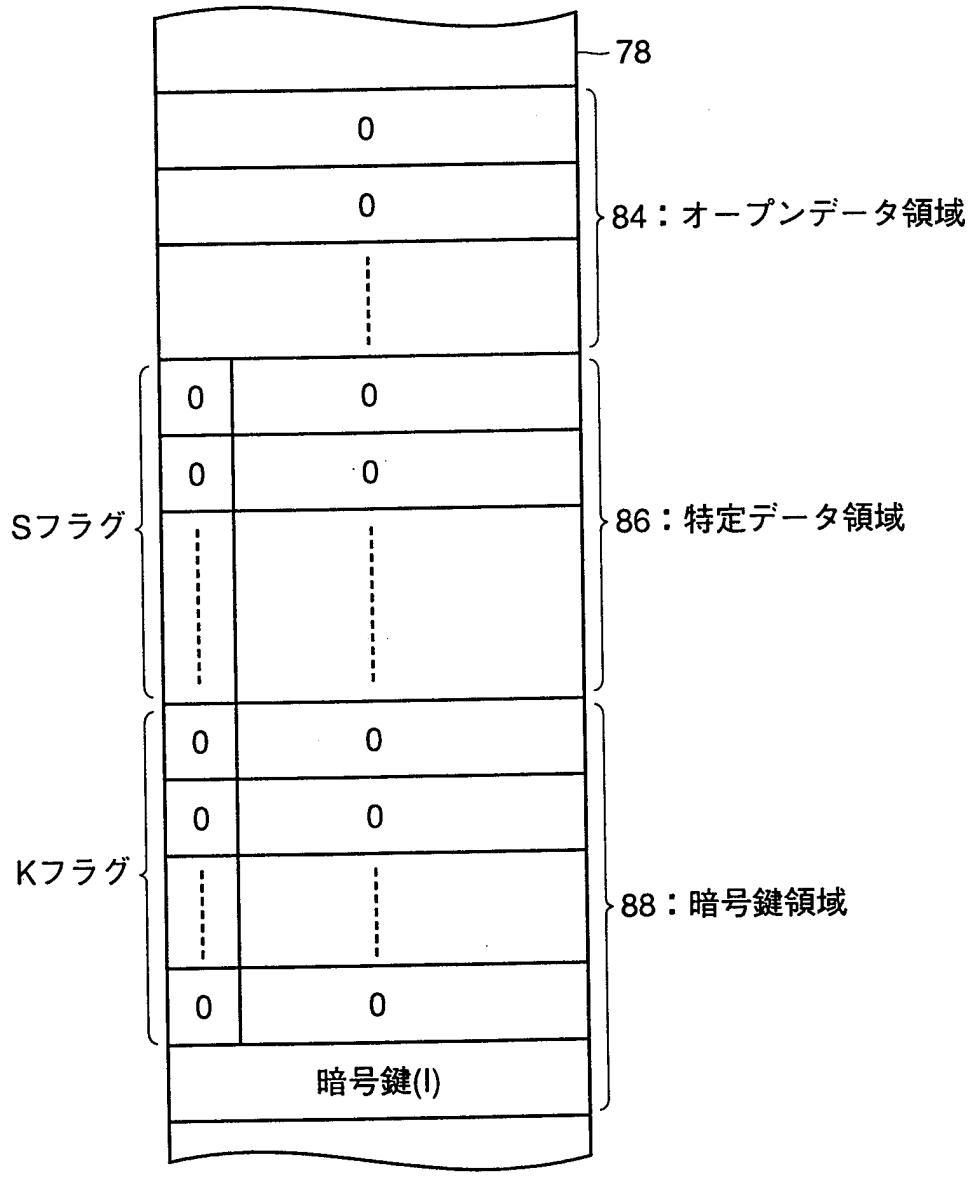

78
0
0
84：オープンデータ領域
0
0
0
0
Sフラグ
86：特定データ領域
0
0
0
0
Kフラグ
88：暗号鍵領域
0
0
暗号鍵(I)

FIG.8

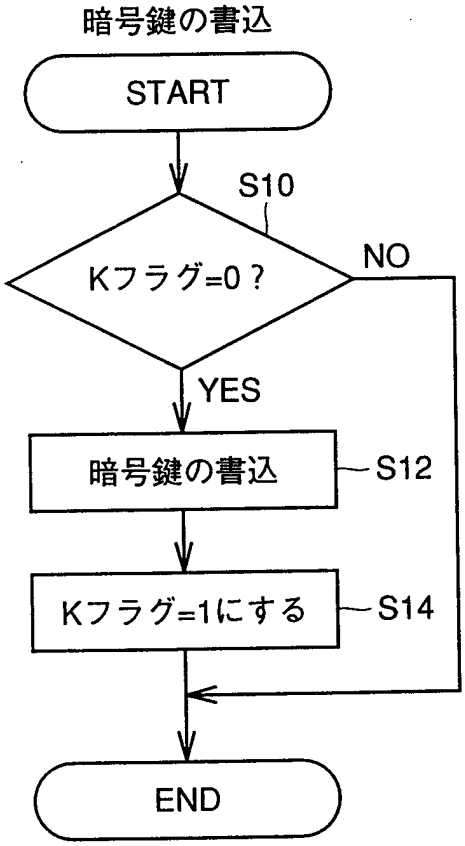


FIG.9

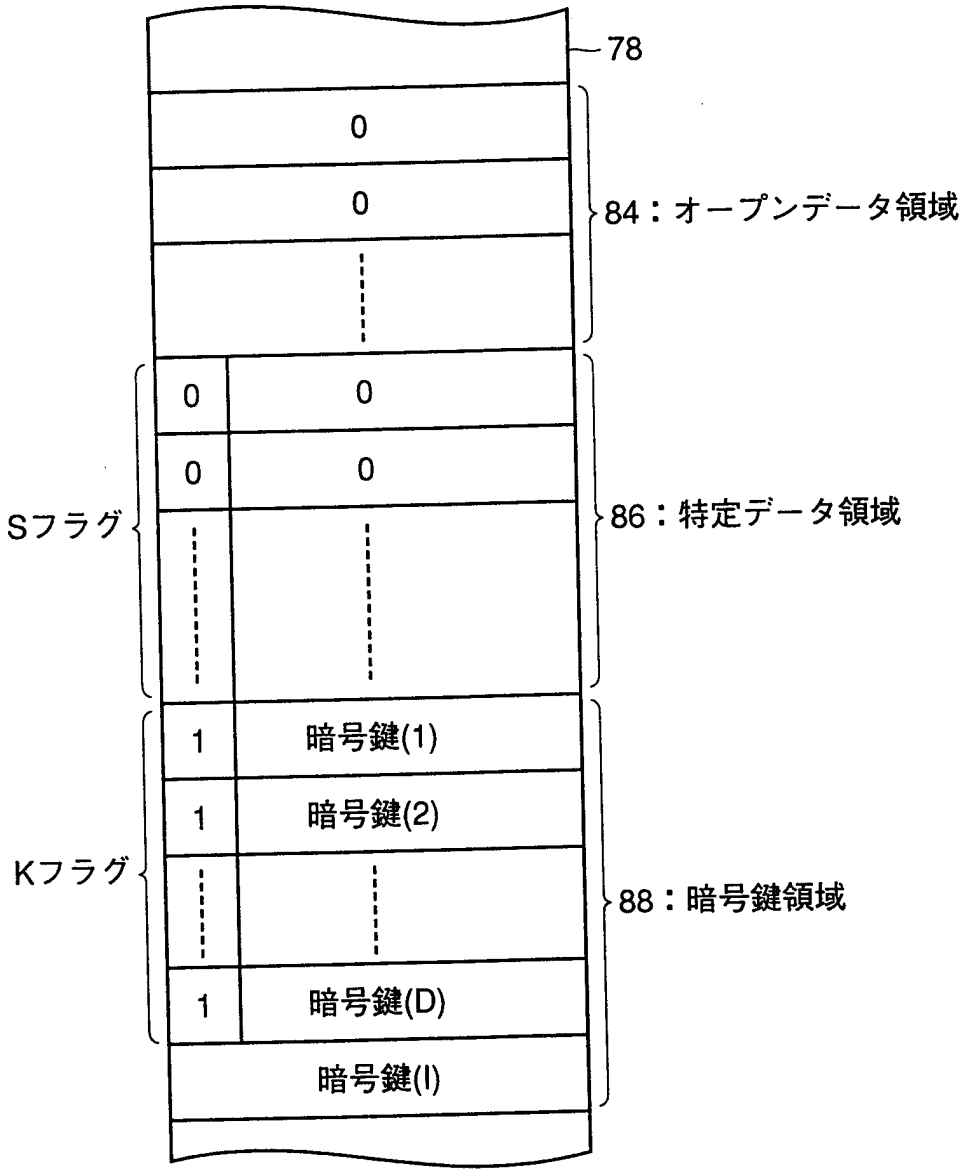

78
0
0
84：オープンデータ領域
0
0
0
0
Sフラグ
86：特定データ領域
1
暗号鍵(1)
1
暗号鍵(2)
Kフラグ
88：暗号鍵領域
1
暗号鍵(D)
暗号鍵(I)

FIG.10

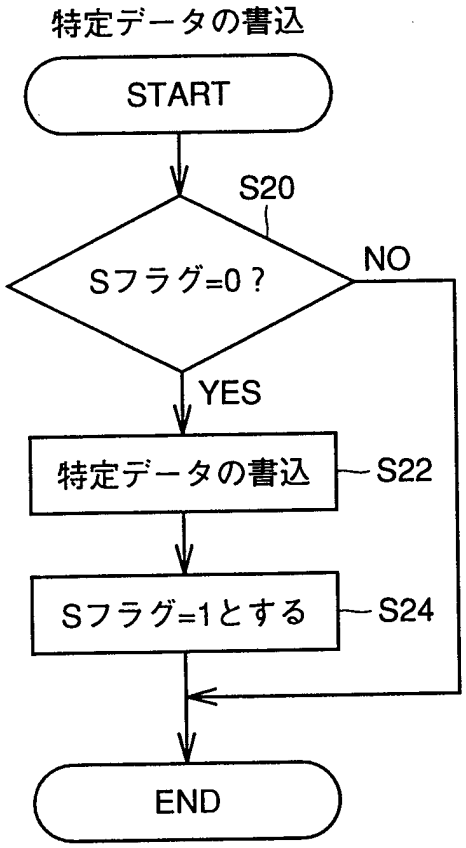

特定データの書込
START
S20
Sフラグ=0？
NO
YES
特定データの書込
S22
Sフラグ=1とする
S24
END

FIG.11

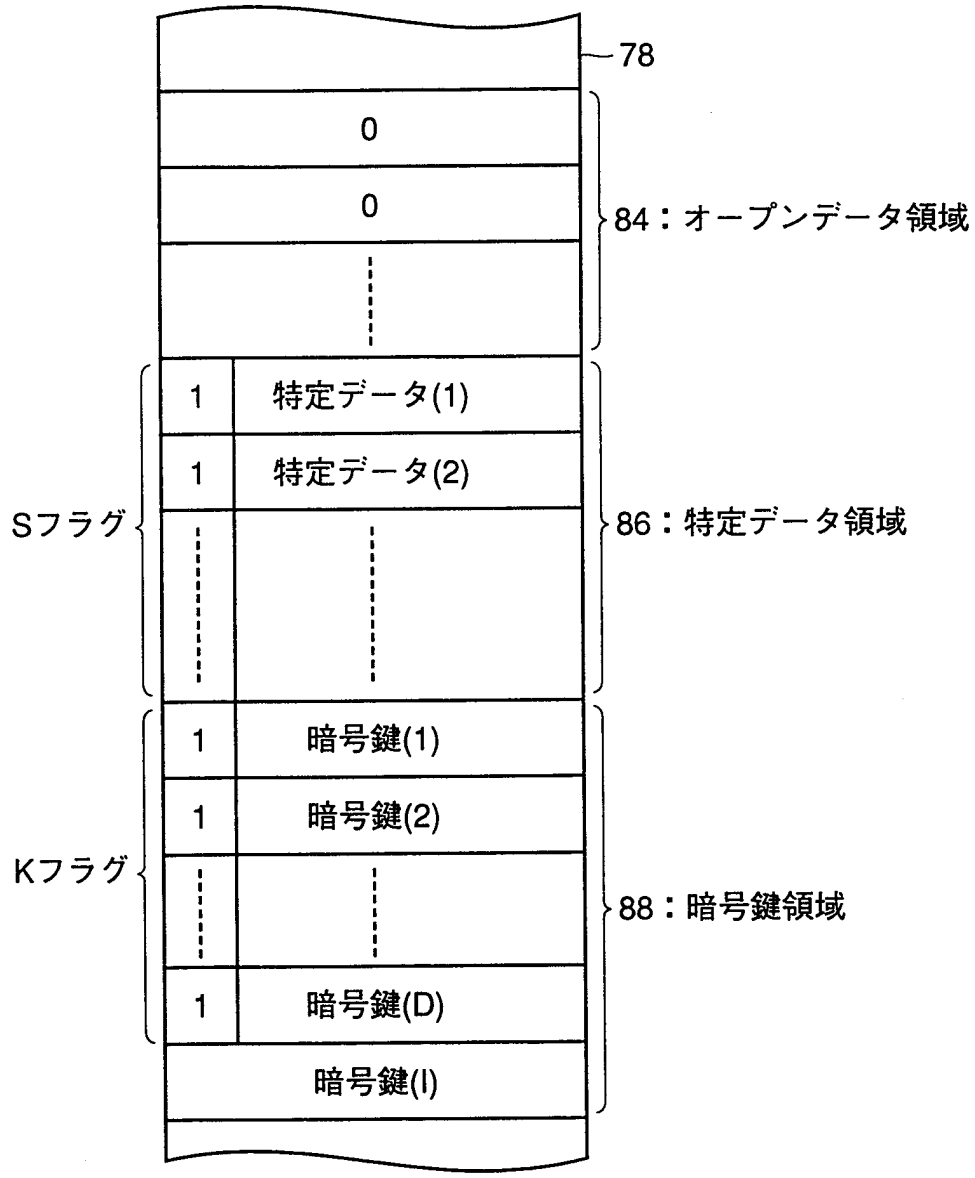

78
0
0
84：オープンデータ領域
1
特定データ(1)
1
特定データ(2)
Sフラグ
86：特定データ領域
1
暗号鍵(1)
1
暗号鍵(2)
Kフラグ
88：暗号鍵領域
1
暗号鍵(D)
暗号鍵(I)

FIG.12

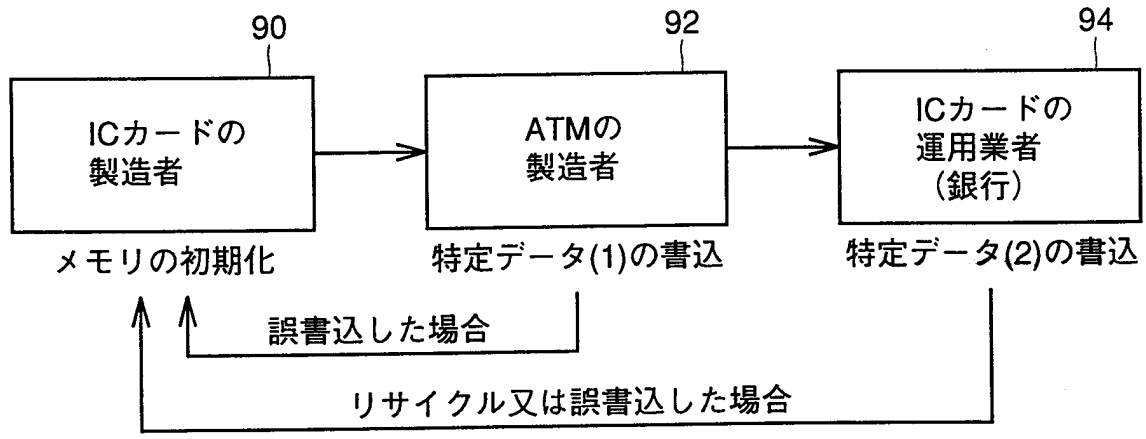

90
92
94
ICカードの
製造者
ATMの
製造者
ICカードの
運用業者
(銀行)
メモリの初期化
特定データ(1)の書込
特定データ(2)の書込
誤書込した場合
リサイクル又は誤書込した場合

FIG.13A

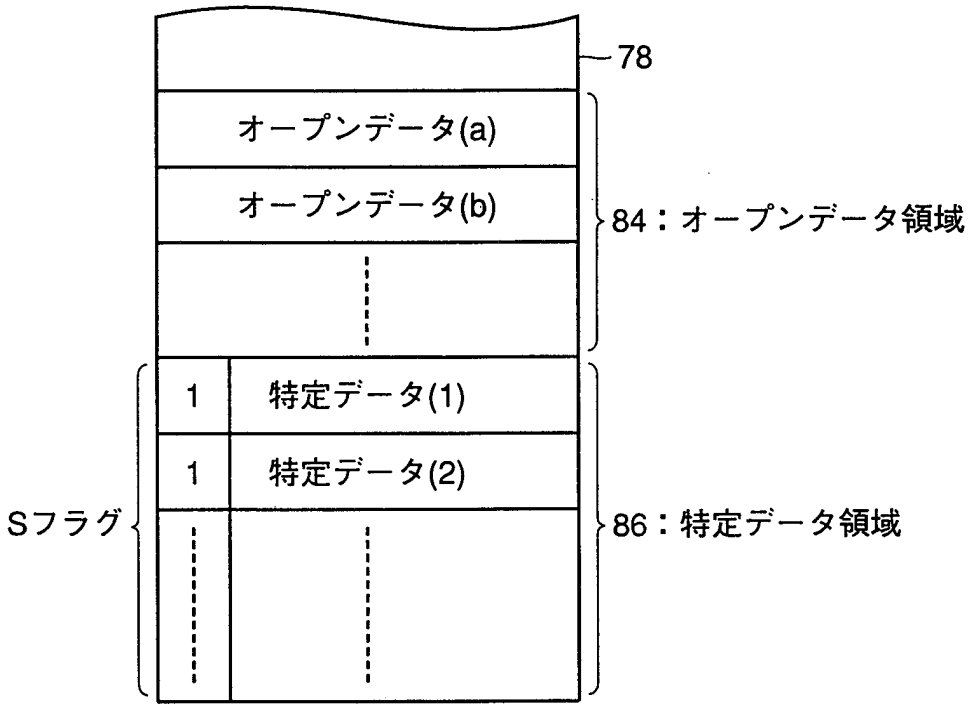


FIG.13B

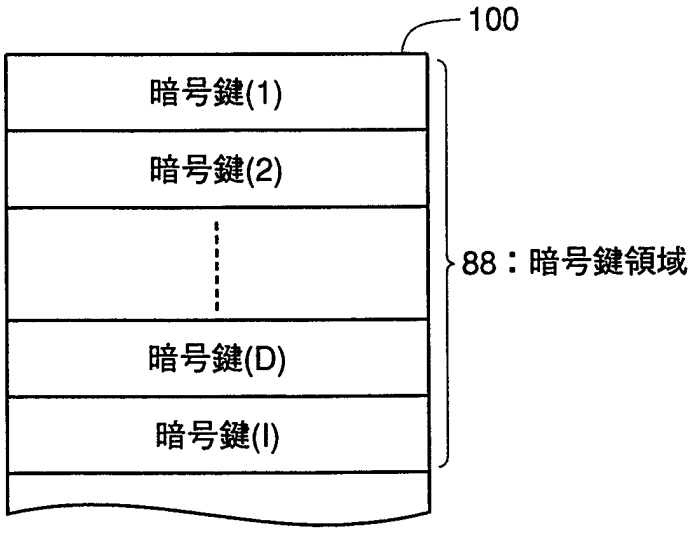


FIG.14

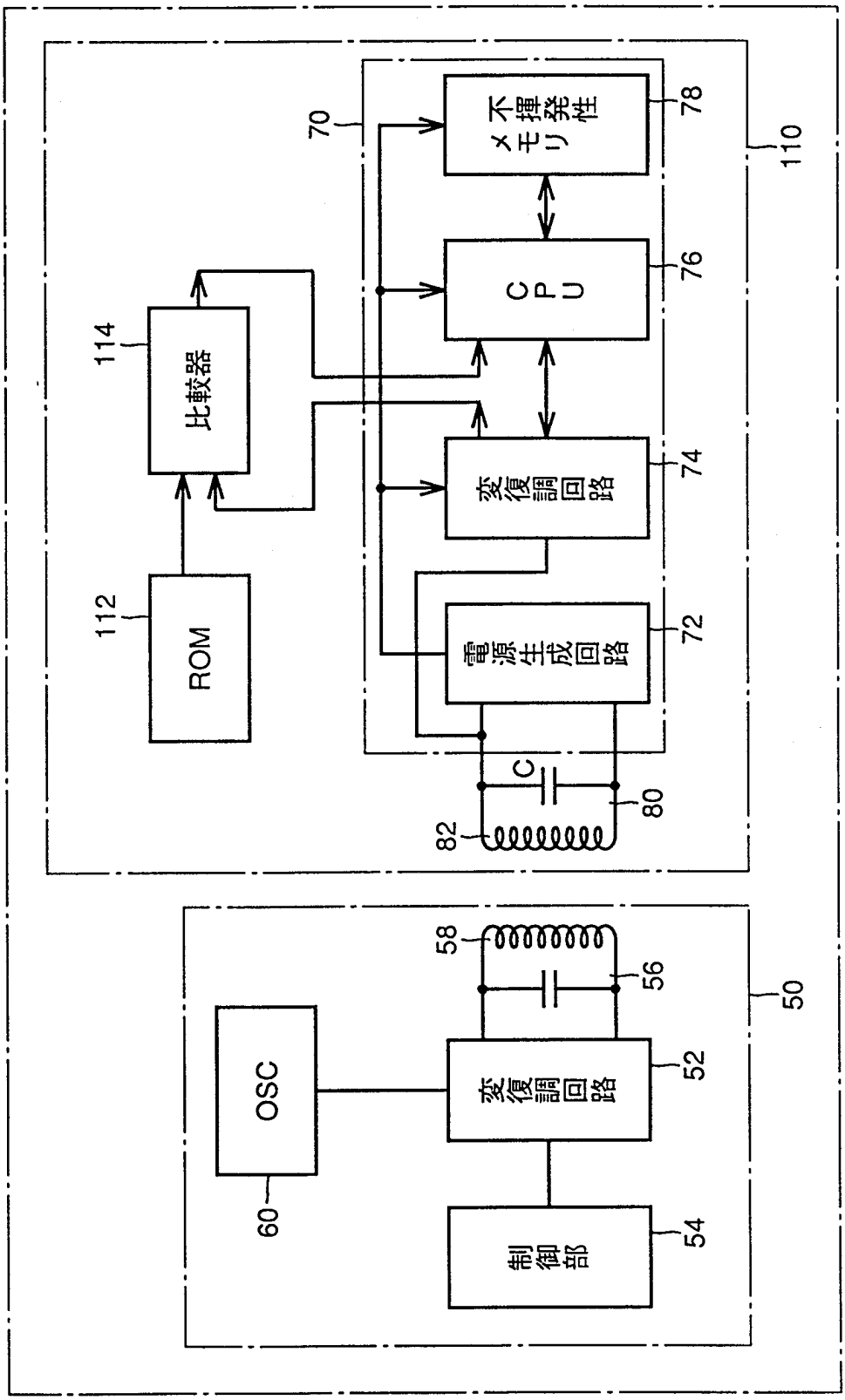
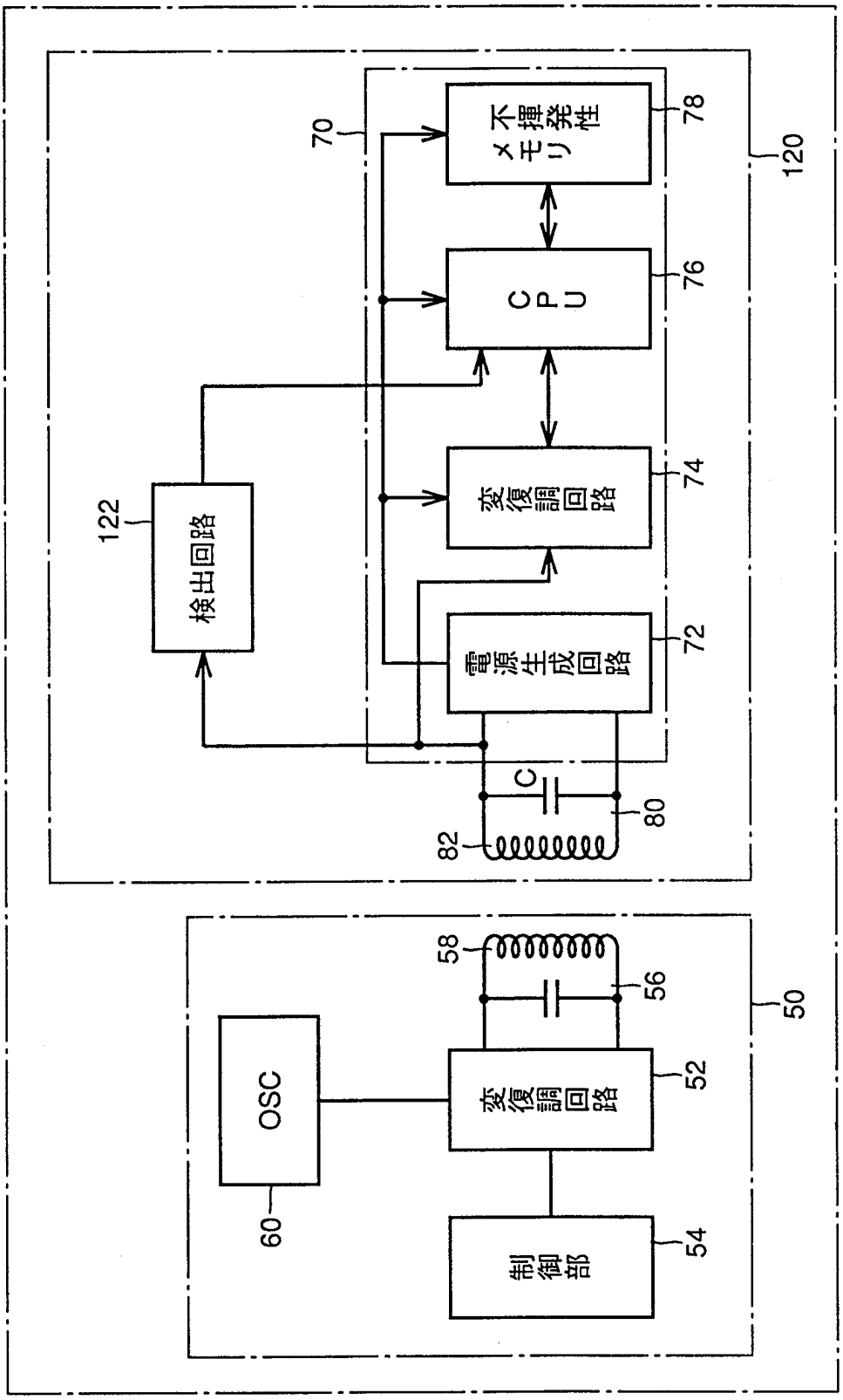

110
70
78
不揮発性メモリ
76
CPU
74
変復調回路
72
電源生成回路
C
80
82
114
比較器
112
ROM
50
58
56
52
変復調回路
OSC
60
54
制御部

FIG.15


120
70
78
不揮発性メモリ
76
CPU
74
変復調回路
72
電源生成回路
122
検出回路
C
80
82
50
58
56
52
変復調回路
OSC
60
54
制御部

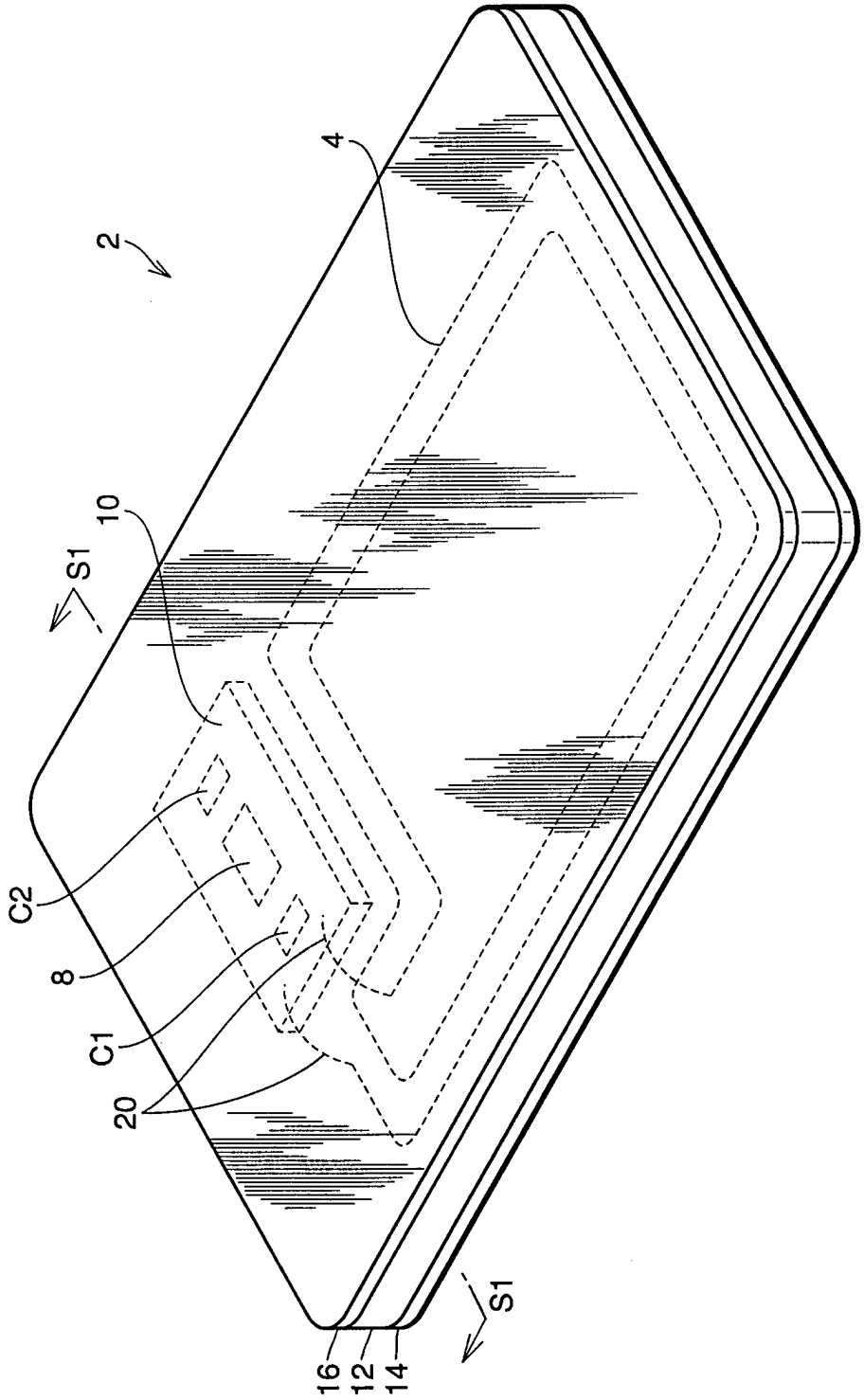


FIG.16

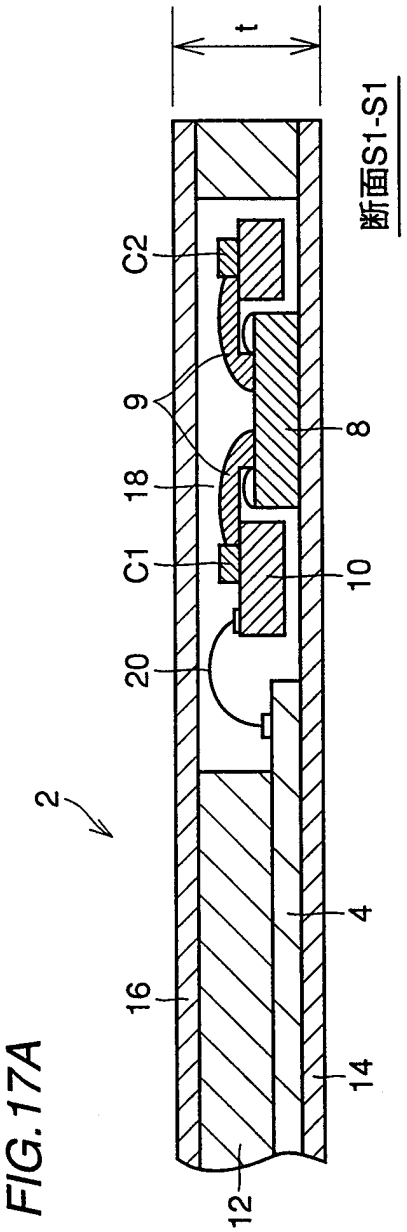


FIG.17A

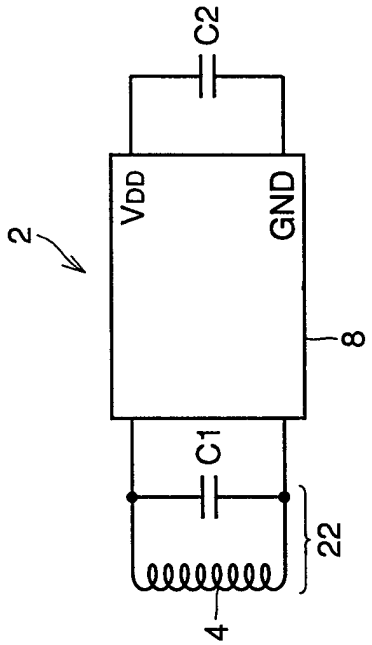


FIG.17B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/00061

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G06K19/073, G06K17/00, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G06K19/073, G06K17/00, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1998 Toroku Jitsuyo Shinan Koho 1994-1998
Kokai Jitsuyo Shinan Koho 1971-1994

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 3-208192, A (Hitachi Maxell, Ltd.), September 11, 1991 (11. 09. 91) (Family: none)	1-16
Y	JP, 56-38650, A (Compagnie Internationale pour I'Informatique CII-Honeywell Bull), April 13, 1981 (13. 04. 81) & US, 4442345, A	10, 12
Y	JP, 2-120951, A (Toshiba Corp.), May 8, 1990 (08. 05. 90) (Family: none)	1-16
Y	JP, 7-73110, A (Tokimec Inc.), March 17, 1995 (17. 03. 95) (Family: none)	1-16
Y	JP, 5-173888, A (Tokyo Electric Co., Ltd.), July 13, 1993 (13. 07. 93) (Family: none)	6
Y	JP, 60-183692, A (Mitsubishi Electric Corp.), September 19, 1985 (19. 09. 85) (Family: none)	12

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
April 7, 1998 (07. 04. 98)	April 21, 1998 (21. 04. 98)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/00061

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 2-5160, A (SJS-Thomson Microelectronics S.A.), January 10, 1990 (10. 01. 90) & US, 5014312, A	1-16
A	JP, 62-226351, A (Citizen Watch Co., Ltd.), October 5, 1987 (05. 10. 87) (Family: none)	1-16
A	JP, 60-37069, A (Citizen Watch Co., Ltd.), February 26, 1985 (26. 02. 85) (Family: none)	1-16

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／００６１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ[6]　　Ｇ０６Ｋ１９／０７３，　Ｇ０６Ｋ１７／００
Ｇ０６Ｆ１２／１４

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ[6]　　Ｇ０６Ｋ１９／０７３，　Ｇ０６Ｋ１７／００
Ｇ０６Ｆ１２／１４

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　１９２６－１９９８年，　日本国登録実用新案公報　１９９４－１９９８年
日本国公開実用新案公報　１９７１－１９９４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，３－２０８１９２，Ａ（日立マクセル株式会社） １１．９月．１９９１（１１．０９．９１）（ファミリーなし）	１－１６
Ｙ	ＪＰ，５６－３８６５０，Ａ（ｺﾝﾊﾟﾆｰ･ｱﾝﾃﾙﾅｼｮﾅﾙ･ﾌﾟｰﾙ･ﾗﾝﾌｫﾙ･ﾏﾃｲｸ･ｾｰｲｲ･ﾊﾆｰｳｪﾙ･ﾌﾞﾙ）１３．４月．１９８１（１３．０４．８１） ＆　ＵＳ，４４４２３４５，Ａ	１０，１２
Ｙ	ＪＰ，２－１２０９５１，Ａ（株式会社東芝） ８．５月．１９９０（０８．０５．９０）（ファミリーなし）	１－１６
Ｙ	ＪＰ，７－７３１１０，Ａ（株式会社トキメック） １７．３月．１９９５（１７．０３．９５）（ファミリーなし）	１－１６

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」先行文献ではあるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０７．０４．９８	21.04.98

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	野仲　松男	５Ｂ	９２９３
	電話番号　０３－３５８１－１１０１　内線　３５４５		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９２年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０００６１

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，５－１７３８８８，Ａ（東京電気株式会社） １３．７月．１９９３（１３．０７．９３）（ファミリーなし）	６
Ｙ	ＪＰ，６０－１８３６９２，Ａ（三菱電機株式会社） １９．９月．１９８５（１９．０９．８５）（ファミリーなし）	１２
Ａ	ＪＰ，２－５１６０，Ａ（ｴｽｼﾞｪｰｴｽ-ﾄﾑｿﾝ ﾐｸﾛｴﾚｸﾄﾛﾆｸｽ ｴｽ ｱｰ） １０．１月．１９９０（１０．０１．９０） ＆　ＵＳ，５０１４３１２，Ａ	１－１６
Ａ	ＪＰ，６２－２２６３５１，Ａ（シチズン時計株式会社） ５．１０月．１９８７（０５．１０．８７）（ファミリーなし）	１－１６
Ａ	ＪＰ，６０－３７０６９，Ａ（シチズン時計株式会社） ２６．２月．１９８５（２６．０２．８５）（ファミリーなし）	１－１６