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

特許第4222509号
(P4222509)

(45)発行日　平成21年2月12日(2009.2.12)　(24)登録日　平成20年11月28日(2008.11.28)

(51)Int.Cl.　F I
G06K 19/073 (2006.01)　G06K 19/00　P
G06K 19/10 (2006.01)　G06K 19/00　R

請求項の数 16　(全 32 頁)

(21)出願番号　特願2003-502779(P2003-502779)
(86)(22)出願日　平成14年5月29日(2002.5.29)
(86)国際出願番号　PCT/JP2002/005236
(87)国際公開番号　WO2002/099742
(87)国際公開日　平成14年12月12日(2002.12.12)
審査請求日　平成17年5月12日(2005.5.12)
(31)優先権主張番号　特願2001-167617(P2001-167617)
(32)優先日　平成13年6月4日(2001.6.4)
(33)優先権主張国　日本国(JP)

(73)特許権者　503121103
株式会社ルネサステクノロジ
東京都千代田区大手町二丁目６番２号
(74)代理人　100080001
弁理士　筒井　大和
(72)発明者　水島　永雅
日本国神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　常広　隆司
日本国神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】記憶装置

(57)【特許請求の範囲】

【請求項１】

データを記憶可能なメモリと、前記データを記憶可能でかつ前記データのセキュリティ処理を実行可能な処理装置と、外部のホスト機器からのコマンドに基づいて、前記メモリと前記処理装置とを制御するコントローラとを備えた記憶装置であって、

前記コントローラは、前記ホスト機器からの前記コマンドに前記データのセキュリティ処理に関する情報が含まれていた場合に、前記処理装置を選択し、前記コントローラが生成した前記処理装置を駆動するための駆動クロックを供給して制御し、

前記コントローラは、生成する前記駆動クロックの周波数および前記処理装置への供給タイミングを動的に変更することができる記憶装置。

【請求項２】

請求の範囲第１項に記載の記憶装置において、

前記メモリは、

前記ホスト機器からアクセス可能な第１の記憶領域と、

前記ホスト機器からのアクセスが制限され、かつ、前記コントローラと前記処理装置の少なくとも１つからの要求に応じて、前記処理装置によって利用されるデータを記憶するための第２の領域とを備え、

前記第２の領域に記憶される、前記処理装置によって利用されるデータは、前記処理装置を制御するためのパラメータと、前記処理装置の環境設定のための情報と、前記処理装置を駆動するための前記駆動クロックを設定するための情報と、前記処理装置がセキュリ

ティ処理を実行するためのステータスとの、少なくとも１つを含む記憶装置。
【請求項３】
請求の範囲第１項に記載の記憶装置において、
前記コントローラは、前記ホスト機器からの処理要求が低速である場合の前記駆動クロックの周波数よりも、前記ホスト機器からの処理要求が高速である場合の前記駆動クロックの周波数を大きくする記憶装置。
【請求項４】
請求の範囲第１項に記載の記憶装置において、
前記データのセキュリティ処理は、前記データの暗号化又は復号化のための処理を含む記憶装置。
【請求項５】
請求の範囲第１項に記載の記憶装置において、
前記コントローラは、前記メモリが解釈可能な第１のコマンドを前記ホスト機器から受信し、予め定められたルールに従って、前記第１のコマンドを、前記処理装置が解釈可能な第２のコマンドへ変換し、前記第２のコマンドを前記処理装置へ送信する記憶装置。
【請求項６】
請求の範囲第１項に記載の記憶装置において、
前記メモリは、前記コントローラが前記処理装置への前記データの書き込み要求を前記ホスト機器から受信した場合に、前記データが前記処理装置へ書き込まれるためのバッファとして利用される記憶装置。
【請求項７】
請求の範囲第６項に記載の記憶装置において、
前記コントローラは、前記ホスト機器から書き込み要求された前記データのサイズに応じて、前記メモリをバイパスして前記処理装置に前記データを送信するか又は前記メモリに一旦記憶させた後に前記処理装置へ前記データを送信するかを決定する記憶装置。
【請求項８】
請求の範囲第７項に記載の記憶装置において、
前記コントローラは、前記ホスト機器から書き込み要求された前記データのサイズが、前記処理装置が受信可能な許容データサイズ以上の場合に、前記メモリに一旦記憶させた後に前記処理装置へ前記データを送信する記憶装置。
【請求項９】
請求の範囲第７項に記載の記憶装置において、
前記コントローラは、前記ホスト機器から書き込み要求された前記データのサイズが、前記処理装置が受信可能な許容データサイズ以下の場合に、前記メモリをバイパスして前記処理装置に前記データを送信する記憶装置。
【請求項１０】
請求の範囲第１項に記載の記憶装置において、
前記コントローラは、前記処理装置を駆動するための電力を生成して前記処理装置へ供給する記憶装置。
【請求項１１】
請求の範囲第１０項に記載の記憶装置において、
前記コントローラは、前記処理装置を停止する場合に、前記処理装置への前記電力の供給を維持したまま、前記処理装置への前記駆動クロックの供給を停止する記憶装置。
【請求項１２】
請求の範囲第１０項に記載の記憶装置において、
前記コントローラは、
前記処理装置への前記電力の供給が停止している場合に、前記処理装置への前記電力の供給を開始し、その後、前記処理装置への前記駆動クロックの供給を開始し、その後、前記処理装置のデータ入出力端子をプルアップ状態とし、その後、前記処理装置へ供給するリセット信号をハイレベル状態とすることで、前記処理装置のコールドリセットを行い、

前記処理装置へ前記電力が供給されている場合に、前記処理装置への前記駆動クロックの供給を開始し、前記リセット信号をローレベル状態とし、前記データ入出力端子をプルアップ状態とし、前記リセット信号をハイレベルとすることで、前記処理装置のウォームリセットを行う記憶装置。

【請求項１３】

請求の範囲第１項に記載の記憶装置からなるメモリカードであって、

前記メモリはフラッシュメモリチップであり、

前記処理装置は、認証機関によって予め認証されたＩＣチップであるメモリカード。

【請求項１４】

請求の範囲第１３項に記載のメモリカードにおいて、

該記憶装置は、前記コントローラと前記ホスト機器とを接続するための外部端子とを備え、

前記ＩＣチップのグランド端子は、前記外部端子に接続され、

前記ＩＣチップの電源入力端子とリセット入力端子とクロック入力端子とデータ入出力端子は、前記コントローラに接続されるメモリカード。

【請求項１５】

請求の範囲第１４項に記載のメモリカードにおいて、

前記フラッシュメモリチップの電源端子とグランド端子は、前記外部端子に接続され、

前記フラッシュメモリチップのデータ入出力端子とレディ／ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロック端子とリセット端子とは、前記コントローラに接続されるメモリカード。

【請求項１６】

請求の範囲第１４項に記載のメモリカードにおいて、

前記ホスト機器からの特定のコマンドにより、前記ＩＣチップの前記電源入力端子と前記リセット入力端子と前記クロック入力端子と前記データ入出力端子を、前記外部端子に接続するメモリカード。

【発明の詳細な説明】

技術分野

本発明は、セキュリティ機能を搭載した記憶装置及びその記憶装置が挿入可能なホスト機器及びその記憶装置が挿入されたホスト機器に係り、特に、電気的に消去可能な不揮発性メモリ（例えば、フラッシュメモリ）を有するメモリカード及びそのメモリカードが挿入可能なホスト機器及びそのメモリカードが挿入されたホスト機器に関する。

背景技術

ＩＣカードは、プラスチックカード基板中にＩＣ（集積回路）チップを埋め込んだものであり、その表面にＩＣチップの外部端子を持つ。ＩＣチップの外部端子には電源端子、クロック端子、データ入出力端子などがある。ＩＣチップは、接続装置が外部端子から電源や駆動クロックを直接供給することによって動作する。ＩＣカードは外部端子を通して端末機などの接続装置との間で電気信号を送受信することにより、接続装置と情報交換をおこなう。情報交換の結果として、ＩＣカードは計算結果や記憶情報の送出、記憶情報の変更をおこなう。ＩＣカードは、これらの動作仕様に基づいて、機密データ保護や個人認証などのセキュリティ処理を実行する機能を持つことができる。ＩＣカードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

セキュリティシステムにおいて利用されるＩＣカードは、秘密情報を用いて演算を行う際に、その秘密情報あるいはその秘密情報を推定できるような情報を外にもらさないように設計される必要がある。すなわち、耐タンパ性を持つことが必要とされる。このような外にもらしてはならない秘密情報を解析する攻撃方法としては、タイミング解析、電力差分解析、故障利用解析などが知られている。

タイミング解析は、暗号処理時間が秘密情報の内容に依存して異なる場合、その時間差を統計的に解析して秘密情報を推定する攻撃法である。暗号アルゴリズムを実装する際、処

理時間の短縮やプログラムサイズの縮小を目的として、秘密情報の内容に依存して不要処理をスキップしたり分岐処理を行ったりするような最適化を適用することがある。このような最適化を適用すると、暗号処理時間が秘密情報の内容に依存して異なる。そのため処理時間を見ることで秘密情報の内容を推定できる可能性がある。
電力差分解析は、暗号処理の実行中にＩＣカードの電源端子から供給される電力を測定し、そこから消費電力の差分を解析することにより秘密情報を推定する攻撃法である。
故障利用解析は、ＩＣカードの計算誤りを利用した攻撃法である。ＩＣカードに一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、ＩＣカードに攻撃者の望む異常な処理を行わせる。ＩＣカードに高電圧を加えたり、瞬間的にクロック周波数や駆動電圧を変動させることにより故意にエラーを発生させた場合、その結果得られる誤った計算結果と正しい計算結果から秘密情報が得られる可能性がある。
ＩＣカードは、実用上、これらの攻撃法に対する対策手段を持たなければならない。
発明の開示
本発明の第１の目的は、セキュリティを向上した記憶装置を提供することである。
本発明の第２の目的は、製造が簡略化された記憶装置を提供することである。
第１の目的を達成するために、本発明は、データを記憶可能なメモリと、データを記憶可能でかつデータのセキュリティ処理を実行可能な処理装置と、外部のホスト機器からのコマンドに基づいて、メモリと処理装置とを制御するコントローラとを備える。
第１の目的を達成するために、本発明は、フラッシュメモリチップと、コントローラと、外部端子と、ＩＣチップとを備え、ＩＣチップのグランド端子は外部端子に接続され、ＩＣチップの電源入力端子とリセット入力端子とクロック入力端子とデータ入出力端子は、コントローラに接続される。
第２の目的を達成するために、データを記憶可能なフラッシュメモリチップと、フラッシュメモリチップへのデータの読み書きを制御するコントローラと、ＩＣチップとを備え、ＩＣチップは、認証機関によって予め認証された後に搭載される。
本発明の他の目的、特徴及び利点は添付図面に関する以下の本発明の実施例の記載から明らかになるであろう。
発明を実施するための最良の形態
以下、本発明の一実施形態について説明する。
図２２は、本発明を適用したＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ（Ｍｕｌｔｉ Ｍｅｄｉａ ＣａｒｄはＩｎｆｉｎｅｏｎ ＴｅｃｈｎｏｌｏｇｉｅｓＡＧの登録商標である。以下、「ＭＭＣ」と略記する。）の内部構成図を簡単に表したものである。ＭＭＣ１１０は、Ｍｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠するのが好ましい。ＭＭＣ１１０は、外部に接続したホスト機器２２０がＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠したメモリカードコマンドを発行することによって、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ホスト機器２２０は、例えば、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、決済端末等が該当する。ＭＭＣ１１０は、ＭＭＣ外部端子１４０、コントローラチップ１２０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＭＭＣ外部端子１４０は７つの端子から構成され、外部のホスト機器２２０と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ１２０は、ＭＭＣ１１０内部の他の構成要素（ＭＭＣ外部端子１４０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０）と接続されており、これらを制御するマイコンチップである。ＩＣカードチップ１５０は、ＩＣカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはＩＳＯ／ＩＥＣ７８１６規格に準拠している。ＩＣカードチップ１５０の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子、グランド端子がある。コントローラチップ１２０は

、ＩＣカードチップ１５０の外部端子からＩＣカードチップ１５０にＩＣカードコマンドを発行することによって、外部のホスト機器２２０から要求されたセキュリティ処理に必要な演算をおこなう。

図２６は、本発明のＩＣカードチップの内部構成を示す図である。ＩＣカードチップ１５０は、演算処理を行うためのＣＰＵ（マイコン）１５８と、データ（プログラムを含む。）を記憶するためのＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１５９とＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１６０とＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）１６２と、暗号／復号に関する処理を行うための暗号コプロセッサ１６３と、外部とデータを送受信するためのシリアルインターフェース１６１とを備え、それらは、バス１６４によって接続される。そして、その暗号コプロセッサ１６３によって、ホスト機器２２０からのコマンドに応じて、ＩＣカードチップ１５０自らが、セキュリティ処理を実行することが可能である。尚、暗号コプロセッサ１６３（ハードウェア）の替わりに、プログラム（ソフトウェア）に従ってＣＰＵ１５８がセキュリティ処理を実行してもよい。

一方、フラッシュメモリチップ１３０には、記憶素子を備えるが、マイコンは存在しない。セキュリティ処理は、例えば、ＩＣカードチップ１５０内の記憶領域にデータが書き込まれるとき、又は、ＩＣカードチップ１５０内の記憶領城からデータが読み出されるときに実行される。ＩＣカードチップ１５０のＥＥＰＲＯＭの記憶容量は、フラッシュメモリチップ１３０の記憶容量より小さい。但し、ＩＣカードチップ１５０のＥＥＰＲＯＭの記憶容量は、フラッシュメモリチップ１３０の記憶容量と同じでもよいし、大きくてもよい。

ＩＣカードチップ１５０には、セキュリティ評価基準の国際標準であるＩＳＯ／ＩＥＣ１５４０８の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つＩＣカードを実際の電子決済サービスなどで利用する場合、そのＩＣカードはＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣにセキュリティ処理をおこなう機能を追加することによってＭＭＣ１１０を実現し、それを実際の電子決済サービスなどで利用する場合、ＭＭＣ１１０も同様にＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。本発明によれば、ＭＭＣ１１０は、評価・認証機関によって認証済みのＩＣカードチップ１５０を内蔵し、そのＩＣカードチップ１５０を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、ＭＭＣ１１０はＩＳＯ／ＩＥＣ１５４０８に基づくセキュリティ評価基準を容易に満足することができ、ＭＭＣにセキュリティ処理機能を追加するための開発期間を短縮することができる。

ＭＭＣ１１０は、Ｍｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した外部インタフェースを持つのが好ましい。ＭＭＣ１１０は、一種類の外部インタフェースを通じて、標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）に加えて、セキュリティ処理を実行するコマンドを受け付ける必要がある。コントローラチップ１２０は、ＭＭＣ１１０が受信したコマンドが標準メモリカードコマンドであるか、セキュリティ処理を実行するコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。本発明によれば、標準メモリカードコマンドを受信したならば、フラッシュメモリチップ１３０を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュリティ処理を実行するコマンドを受信したならば、ＩＣカードチップ１５０を選択し、これにＩＣカードコマンドを発行してセキュリティ処理を実行することができる。

ＩＣカードチップ１５０の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子がコントローラチップ１２０に接続されている。

コントローラチップ１２０は、電源供給端子、クロック入力端子を通して、ＩＣカードチップ１５０への電源供給、クロック供給を制御する。本発明によれば、ホスト機器２２０からセキュリティ処理を要求されないときには、ＩＣカードチップ１５０への電源供給や

クロック供給を停止させることができ、ＭＭＣ１１０の電力消費を削減することができる。
電源供給されていないＩＣカードチップ１５０を、ＩＣカードコマンドを受信できる状態にするには、まず、ＩＣカードチップ１５０に電源供給を開始し、リセット処理（クロック供給の開始を含む）を施すことが必要である。例えば、コントローラチップ１２０は、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、電源供給端子を通してＩＣカードチップ１５０への電源供給を開始してもよい。あるいは、コントローラチップ１２０は、セキュリティ処理を実行しないときもＩＣカードチップ１５０への電源供給を維持しておき、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、リセット入力端子を通してＩＣカードチップ１５０のリセット処理をおこなってもよい。本発明によれば、コントローラチップ１２０は、セキュリティ処理を実行するコマンドを受信するまでＩＣカードチップ１５０への電源とクロック両方の供給、あるいはクロック供給のみを停止させておくことができる。したがって、ＭＭＣ１１０の電力消費を削減することができる。ＩＣカードチップ１５０がスリープモードの動作をサポートしている場合は、セキュリティ処理を実行していない時にクロック供給のみを停止するだけでも電力消費を大幅に削減できる。これはＩＳＯ／ＩＥＣ７８１６－３規格により、電源電圧３ＶでのＩＣカードの電気特性は、通常動作状態で最大５０ｍＡ、クロック停止状態で最大０．５ｍＡと規定されているためである。なお、スリープモードとは、クロック供給を止めても電源さえ供給していれば、ＩＣカードチップ１５０の内部状態（コアＣＰＵのレジスタやＲＡＭに保持されたデータ）が保存される動作モードである。
コントローラチップ１２０は、ＩＣカードチップ１５０のクロック入力端子を通してＩＣカードチップ１５０に供給するクロック信号をＭＭＣ１１０内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。本発明によれば、ＭＭＣ外部端子１４０のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器２２０によるタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。
図２１は、フラッシュメモリチップ１３０の詳細な内部構成を表している。フラッシュメモリチップ１３０は、ホストデータ領域２１１５と管理領域２１１０とを含む。ホストデータ領域２１１５は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器２２０が論理アドレスを指定してデータを読み書きできる領域である。ホストデータ領域２１１５は、ユーザファイル領域２１３０とセキュリティ処理アプリケーション領域２１２０とを含む。ユーザファイル領域２１３０は、ユーザが自由にファイルデータを読み書きできる領域である。セキュリティ処理アプリケーション領域２１２０は、ホスト機器２２０がセキュリティ処理アプリケーションに必要なデータを格納する領域であり、ユーザが不正にアクセスしないように、ホスト機器２２０のセキュリティ処理アプリケーションが論理的にユーザアクセス制限をかける。ここに格納するデータとしては、ホスト機器２２０のアプリケーションプログラム、そのアプリケーション専用のデータ、セキュリティ処理に使用される証明書など（例えば、電子決済アプリケーションプログラム、電子決済ログ情報、電子決済サービス証明書など）が可能である。本発明によれば、ＭＭＣ１１０が、ホスト機器２２０がセキュリティ処理をおこなう上で使用するデータをホスト機器２２０の代わりに格納するため、ホスト機器２２０にとって利便性が向上する。一方、管理領域２１１０は、コントローラチップ１２０がＩＣカードチップ１５０を管理するための情報を格納する領域である。管理領域２１１０は、ＩＣカード制御パラメータ領域２１１１、ＩＣカード環境設定情報領域２１１２、ＣＬＫ２設定情報領域２１１３、セキュリティ処理バッファ領城２１１４、セキュリティ処理ステータス領域２１１６とを含む。２１１１～２１１６の領域の詳細な使用法については後述する。
コントローラチップ１２０は、フラッシュメモリチップ１３０の管理領域２１１０のセキュリティ処理バッファ領域２１１４を、ＩＣカードチップ１５０でセキュリティ処理を実行する際のメインメモリまたはバッファメモリとして利用する。ホスト機器２２０がセキ

ュリティ処理を実行するコマンドによりＭＭＣ１１０にアクセスした際に、ＭＭＣ１１０がホスト機器２２０からＩＣカードチップ１５０に一度に送信できないほどの大きなサイズのセキュリティ関連データを受信したならば、コントローラチップ１２０はフラッシュメモリチップ１３０へのアクセスを選択し、そのデータを十分な容量を持つセキュリティ処理バッファ領域２１１４に一時的に格納する。ＩＣカードチップ１５０に一度に送信できないほどのサイズは、ＩＣカードコマンドの許容データサイズ（例えば、２５５バイト又は２５６バイト）を超えるサイズである。そして、コントローラチップ１２０はそれをＩＣカードチップ１５０に送信できるサイズのデータに分割し、分割データをフラッシュメモリチップ１３０から読み出し、段階的にＩＣカードチップ１５０に送信する。つまり、分割されたデータの読み出し、書き込みを繰り返す。本発明によれば、ホスト機器２２０にとって、大きなサイズのセキュリティ関連データを扱うことができるので、セキュリティ処理の利便性が向上する。

上記のセキュリティ処理バッファ領域２１１４を含む管理領域２１１０は、ホスト機器２２０が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ１２０により物理的にホストアクセス制限がかけられている。つまり、管理領域２１１０はホスト機器２２０が直接データを読み書きできない。本発明によれば、ホスト機器２２０がセキュリティ処理バッファ領域２１１４の内容を自由に読み出したり改ざんすることができないため、セキュリティ処理の信頼性や安全性が向上する。

図２３は、ＭＭＣ１１０を利用したセキュリティ処理の一例として、コンテンツ配信のセキュリティ処理を表したものである。コンテンツプロバイダ２３１０は、ＭＭＣ１１０を所有するユーザにコンテンツ２３１４を販売する業者である。ホスト機器２２０は、この例では、コンテンツプロバイダ２３１０とネットワークなどを介して接続することができる端末機である。ユーザはＭＭＣ１１０をホスト機器２２０に接続してコンテンツ２３１４を購入する。以下、その手順を説明する。

まず、ホスト機器２２０はＭＭＣ１１０に、フラッシュメモリチップ１３０に格納されたユーザ証明書２３２１を読み出すコマンドを発行する。ＭＭＣ１１０のコントローラチップ１２０は、フラッシュメモリチップ１３０のセキュリティ処理アプリケーション領域２１２０に格納されたユーザ証明書２３２１を読み出し、それをホスト機器２２０に送信する。そして、ホスト機器２２０はそれをコンテンツプロバイダ２３１０に送信する。コンテンツプロバイダ２３１０はユーザ証明書２３２１につけられたデジタル署名を検証する（２３１１）。検証が成功したならば、乱数発生器によりセッション鍵を生成し（２３１２）、それをユーザ証明書２３２１から抽出したユーザ公開鍵によって暗号化する（２３１３）。さらに、コンテンツ２３１４をそのセッション鍵によって暗号化する（２３１５）。コンテンツプロバイダ２３１０はステップ２３１３の結果をホスト機器２２０に送信する。ホスト機器２２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するＩＣカードコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、ユーザ秘密鍵２３２２によってステップ２３１３の結果を復号して、セッション鍵を取得する（２３２３）。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。次に、コンテンツプロバイダ２３１０は、ステップ２３１５の結果を、ホスト機器２２０に送信する。ホスト機器２２０は、ステップ２３１３の結果をセッション鍵（ステップ２３２３によって取得した鍵）によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１５の結果をセッション鍵によって復号するＩＣカードコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、セッション鍵によってステップ２３１５の結果を復号して、コンテンツ２３１４を復元する（２３２４）。コントローラ

チップ１２０は、このコンテンツ２３１４をＩＣカードチップ１５０から受信し、フラッシュメモリチップ１３０に書きこむ。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。ホスト機器２２０が、コンテンツを無事に受信したことをコンテンツプロバイダ２３１０に伝えると、コンテンツプロバイダ２３１０はユーザ証明書に記載されたユーザにコンテンツ料金を課金する。ユーザは、ホスト機器２２０でＭＭＣ１１０内のフラッシュメモリチップ１３０に格納されたコンテンツ２３１４を読み出して利用することができる。また、フラッシュメモリチップ１３０の記憶媒体に大容量のフラッシュメモリを使用すれば、多くのコンテンツを購入できる。

本発明によれば、コンテンツ配信におけるセキュリティ処理とコンテンツ蓄積の両方をＭＭＣ１１０によって容易に実現できる。コンテンツ料金の決済を、ＩＣカードチップ１５０を利用して行ってもよい。

図２４と図２５は、それぞれ、本発明をＳＤカード（幅２４ミリメートル、長さ３２ミリメートル、厚さ２．１ミリメートルで、９つの外部端子をもち、フラッシュメモリを搭載した小型メモリカードである。）とメモリースティック（メモリースティックはソニー株式会社の登録商標である。）に適用したときの簡単な内部構成図を表したものである。本発明を適用したＳＤカード２４１０は、ＳＤカードコントローラチップ２４２０、フラッシュメモリチップ２４３０、ＳＤカード外部端子２４４０、ＩＣカードチップ１５０とを含む。本発明を適用したメモリースティック２５１０は、メモリースティックコントローラチップ２５２０、フラッシュメモリチップ２５３０、メモリースティック外部端子２５４０、ＩＣカードチップ１５０とを含む。フラッシュメモリチップ２４３０と２５３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＳＤカードコントローラチップ２４２０とメモリースティックコントローラチップ２５２０はそれぞれＳＤカードとメモリースティック内の他の構成要素を制御するマイコンチップである。

ＳＤカード外部端子２４４０は９つの端子からなり、それらの位置は、端からＤａｔａ２端子２４４１、Ｄａｔａ３端子２４４２、Ｃｏｍ端子２４４３、Ｖｓｓ端子２４４４、Ｖｄｄ端子２４４５、Ｃｌｏｃｋ端子２４４６、Ｖｓｓ端子２４４７、Ｄａｔａ０端子２４４８、Ｄａｔａ１端子２４４９の順で並んでいる。Ｖｄｄ端子２４４５は電源供給端子、Ｖｓｓ端子２４４４と２４４７はグランド端子、Ｄａｔａ０端子２４４８とＤａｔａ１端子２４４９とＤａｔａ２端子２４４１とＤａｔａ３端子２４４２はデータ入出力端子、Ｃｏｍ端子２４４３はコマンド入出力端子、Ｃｌｏｃｋ端子２４４６はクロック入力端子である。ＳＤカード２４１０は、外部に接続するＳＤカードホスト機器２４６０とのインタフェース仕様にＭＭＣ１１０と違いがあるものの、ＭＭＣ外部端子１４０と非常に類似した外部端子を持ち、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

一方、メモリースティック外部端子２５４０は１０個の端子からなり、それらの位置は、端からＧｎｄ端子２５４１、ＢＳ端子２５４２、Ｖｃｃ端子２５４３、予約端子Ｒｓｖを１つ飛ばしてＤＩＯ端子２５４４、ＩＮＳ端子２５４５、予約端子Ｒｓｖを１つ飛ばしてＳＣＫ端子２５４６、Ｖｃｃ端子２５４７、Ｇｎｄ端子２５４８の順で並んでいる。Ｖｃｃ端子２５４３と２５４７は電源供給端子、Ｇｎｄ端子２５４１と２５４８はグランド端子、ＤＩＯ端子２５４４はコマンドおよびデータ入出力端子、ＳＣＫ端子２５４６はクロック入力端子である。メモリースティック２５１０は、外部に接続するメモリースティックホスト機器２５６０とのインタフェース仕様にＭＭＣ１１０と違いがあるものの、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

図１は、本発明を適用したＭＭＣの詳細な内部構成図を表したものである。また、図２は、図１のＭＭＣ１１０と接続したホスト機器２２０の構成とその接続状態を表したもので

ある。ホスト機器２２０は、ＶＣＣ１電源２２１、ＣＬＫ１発振器２２２、ホストインタフェース２２３を持つ。
ＭＭＣ１１０は、外部のホスト機器２２０と情報交換するためのＭＭＣ外部端子１４０を持つ。ＭＭＣ外部端子１４０は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＧＮＤ１端子１４３および１４６、ＶＣＣ１端子１４４、ＣＬＫ１端子１４５、ＤＡＴ端子１４７の７つの端子とを含む。Ｍｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ仕様は、ＭＭＣの動作モードとしてＭＭＣモードとＳＰＩモードという２種類を規定しており、動作モードによってＭＭＣ外部端子１４０の使用法は異なる。本実施例ではＭＭＣモードでの動作の場合について詳細に説明する。ＶＣＣ１端子１４４は、ＶＣＣ１電源２２１と接続されており、ホスト機器２２０がＭＭＣ１１０に電力を供給するための電源端子である。ＧＮＤ１端子１４３および１４６は、ＶＣＣ１電源２２１と接続されており、ＭＭＣ１１０の電気的なグランド端子である。ＧＮＤ１端子１４３とＧＮＤ１端子１４６は、ＭＭＣ１１０内部で電気的に短絡されている。ＣＳ端子１４１は、ホストインタフェース２２３に接続されており、ＳＰＩモードの動作において使用される入力端子である。ホスト機器２２０が、ＭＭＣ１１０にＳＰＩモードでアクセスするときには、ＣＳ端子１４１にＬレベルを入力する。ＭＭＣモードの動作では、ＣＳ端子１４１を使用する必要はない。ＣＭＤ端子１４２は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠したメモリカードコマンドをＭＭＣ１１０に送信したり、同仕様に準拠したメモリカードレスポンスをＭＭＣ１１０から受信するために使用する入出力端子である。ＤＡＴ端子１４７は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠した形式の入力データをＭＭＣ１１０に送信したり、同仕様に準拠した形式の出力データをＭＭＣ１１０から受信するために使用する入出力端子である。ＣＬＫ１端子１４５は、ＣＬＫ１発振器２２２に接続されており、ＣＬＫ１発振器２２２が生成するクロック信号が入力される端子である。ホスト機器２２０が、ＣＭＤ端子１４２を通してメモリカードコマンド、メモリカードレスポンスを送受信したり、ＤＡＴ端子１４７を通してホストデータを送受信するときに、ＣＬＫ１端子１４５にクロック信号が入力される。ホストインタフェース２２３には、ＣＬＫ１発振器２２２からクロック信号が供給されており、メモリカードコマンド、メモリカードレスポンス、ホストデータは、ＣＬＫ１発振器２２２が生成するクロック信号にビット単位で同期して、ホスト機器２２０とＭＭＣ１１０との間を転送される。
ＭＭＣ１１０は、コントローラチップ１２０を持つ。コントローラチップ１２０は、ＣＰＵ１２１、フラッシュメモリＩ／Ｆ制御回路１２２、ＭＭＣＩ／Ｆ制御回路１２３、ＣＬＫ０発振器１２４、ＶＣＣ２生成器１２５、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８とを含む。これらの構成要素１２１～１２８は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。ＭＭＣＩ／Ｆ制御回路１２３は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７と接続されており、ＭＭＣ１１０がそれらの端子を通してホスト機器２２０と情報交換するためのインタフェースを制御する論理回路である。ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３と接続されており、ＭＭＣＩ／Ｆ制御回路１２３を制御する。ＭＭＣＩ／Ｆ制御回路１２３がＣＭＤ端子１４２を通してホスト機器２２０からメモリカードコマンドを受信すると、ＭＭＣＩ／Ｆ制御回路１２３はそのコマンドの受信が成功したかどうかの結果をホスト機器２２０に伝えるためＣＭＤ端子１４２を通してホスト機器２２０にレスポンスを送信する。ＣＰＵ１２１は、受信したメモリカードコマンドを解釈し、コマンド内容に応じた処理を実行する。また、そのコマンド内容に応じてホスト機器２２０とＤＡＴ端子１４７を通してデータの送受信をおこなう必要がある場合、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３へのデータの送出、ＭＭＣＩ／Ｆ制御回路１２３からのデータの取得をおこなう。さらに、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３とホスト機器２２０との間のデータ転送手続きも制御する。例えば、ホスト機器２２０から受信したデータの処理中に、ホスト機器２２０がＭＭＣ１１０への電源供給を停止することがないように、ＣＰＵ１２１はＤＡＴ端子１４７に

Ｌレベルを出力させ、ＭＭＣ１１０がビジー状態であることをホスト機器２２０に伝える。ＣＬＫ０発振器１２４は、ＣＰＵ１２１と接続され、ＣＰＵ１２１を動作させる駆動クロックを供給する。尚、ＩＣカードチップ１５０は、駆動クロックを要するが、フラッシュメモリチップ１３０は、駆動クロックが不要である。しかし、ＩＣカードチップ１５０及びフラッシュメモリチップ１３０は共に、データを転送するためのデータ転送クロックを要する。

ＭＭＣ１１０は、フラッシュメモリチップ１３０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップである。フラッシュメモリチップ１３０は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。フラッシュメモリチップ１３０は、外部からのフラッシュメモリコマンドに従って、入力されたデータを不揮発性の半導体メモリに格納するライト機能、また同メモリに格納されたデータを外部に出力するリード機能を持つ。フラッシュメモリＩ／Ｆ制御回路１２２は、フラッシュメモリチップ１３０にフラッシュメモリコマンドを発行したり、そのコマンドで入出力するデータを転送するための論理回路である。ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２を制御し、フラッシュメモリチップ１３０にデータのライト機能やリード機能を実行させる。ホスト機器２２０から受信したデータをフラッシュメモリチップ１３０にライトしたり、フラッシュメモリチップ１３０に格納されたデータをホスト機器２２０に送信する必要があるとき、ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２とＭＭＣＩ／Ｆ制御回路１２３の間のデータ転送を制御する。

ＭＭＣ１１０は、ＩＣカードチップ１５０を持つ。ＩＣカードチップ１５０は、ＩＣカードの基板中に埋め込むことを目的として設計されたＩＣチップであり、ＩＣカードの外部端子規格に準拠した８つの外部端子を持つ。このうち６つの端子は、ＩＣカードの外部端子規格により使用法が割り付けられており、残りの２つは将来のための予備端子である。その６つの端子は、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、ＧＮＤ２端子１５５、ＶＰＰ端子１５６、Ｉ／Ｏ端子１５７である。

ＩＣカードチップ１５０のグランド端子は、ＭＭＣ外部端子１４０のＧＲＮ１（グランド端子）１４６に接続される。ＩＣカードチップ１５０のＶＣＣ２端子（電源入力端子）１５１は、コントローラチップ１２０のＶＣＣ２制御回路１２６に接続される。ＩＣカードチップ１５０のＲＳＴ端子（リセット入力端子）１５２とＩ／Ｏ端子（データ入出力端子）１５７は、コントローラチップ１２０のＩＣカードＩ／Ｆ制御回路１２８に接続される。ＩＣカードチップ１５０のＣＬＫ２端子（クロック入力端子）１５３は、コントローラチップ１２０のＣＬＫ２制御回路１２７に接続される。

フラッシュメモリチップ１３０のＶＣＣ端子（電源入力端子）は、ＭＭＣ外部端子１４０のＶＣＣ１１４４に接続される。フラッシュメモリチップ１３０のＶＳＳ端子（グランド端子）は、ＭＭＣ外部端子１４０のＧＲＤ１１４６に接続される。フラッシュメモリチップ１３０のＩ／Ｏ端子（データ入出力端子）とレディ／ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロック端子とリセット端子とは、コントローラチップ１２０のフラッシュメモリＩＦ制御回路１２２に接続される。

ＶＣＣ２端子１５１は、ＩＣカードチップ１５０に電力を供給するための電源端子である。ＶＣＣ２制御回路１２６は、ＭＯＳ－ＦＥＴ素子を用いたスイッチ回路によりＶＣＣ２端子１５１への電力の供給開始と供給停止を制御する回路である。ＶＣＣ２生成器１２５はＶＣＣ２端子１５１に供給する電圧を発生し、それをＶＣＣ２制御回路１２６に供給する。ＩＣカードの電気信号規格はＩＣカードの動作クラスとしてクラスＡとクラスＢを規定している。ＶＣＣ２端子１５１に供給する標準電圧は、クラスＡでは５Ｖ、クラスＢでは３Ｖである。本発明はＩＣカードチップ１５０の動作クラスによらず適用できるが、本実施例ではＩＣカードチップ１５０がクラスＢで動作する場合について詳細に説明する。

ＶＰＰ端子１５６は、ＩＣカードチップ１５０がクラスＡで動作する時に、内部の不揮発性メモリにデータを書き込んだり消去したりするために使用される可変電圧を供給する端子であり、クラスＢで動作する時には使用しない。ＧＮＤ２端子１５５は、ＩＣカードチ

ップ１５０の電気的なグランド端子であり、ＧＮＤ１端子１４３、１４６と短絡されている。ＶＣＣ２制御回路１２６はＣＰＵ１２１と接続され、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給の開始と停止を制御することができる。ＩＣカードチップ１５０を使用しないときは、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給を停止することができる。ＭＭＣ１１０は、ＩＣカードチップ１５０への電力供給を停止することにより、それが消費する電力を節約することができる。ただし、電力供給を停止すると、ＩＣカードチップ１５０の内部状態は、ＩＣカードチップ１５０内部の不揮発性メモリに記憶されたデータを除いて維持されない。

ＣＬＫ２端子１５３は、ＩＣカードチップ１５０にクロック信号を入力する端子である。ＣＬＫ２制御回路１２７は、ＣＬＫ２端子１５３にクロックを供給する回路である。ＣＬＫ２制御回路１２７は、ＣＬＫ０発振器１２４から供給されたクロック信号をもとにしてＣＬＫ２端子１５３に供給するクロック信号を生成する。ＣＬＫ２制御回路１２７はＣＰＵ１２１と接続されており、ＣＬＫ２端子１５３へのクロックの供給開始と供給停止をＣＰＵ１２１から制御することができる。ＩＣカードチップ１５０は、自身内部に駆動クロック発振器をもたない。そのため、ＣＬＫ２端子１５３から駆動クロックを供給することによって動作する。ＣＬＫ２制御回路１２７が、ＣＬＫ２端子１５３へのクロック供給を停止すると、ＩＣカードチップ１５０の動作は停止するため、ＩＣカードチップ１５０の消費電力を低下させることができる。この時、ＶＣＣ２端子１５１への電力供給が保たれていれば、ＩＣカードチップ１５０の内部状態は維持される。ここで、ＣＬＫ２端子１５３に供給するクロック信号の周波数をＦ２、ＣＬＫ０発振器１２４から供給されたクロック信号の周波数をＦ０、ＰとＱを正の整数とすると、ＣＬＫ２制御回路１２７は、Ｆ２＝（Ｐ／Ｑ）＊Ｆ０の関係になるようなクロック信号を作成して、これをＣＬＫ２端子１５３に供給する。ＰとＱの値はＣＰＵ１２１により設定できるようになっている。Ｐを大きく設定してＦ２を大きくすると、ＩＣカードチップ１５０の内部処理をより高速に駆動できる。Ｑを大きく設定してＦ２を小さくすると、ＩＣカードチップ１５０の内部処理はより低速に駆動され、ＩＣカードチップ１５０の消費電力を低下させることができる。ＩＣカードチップ１５０の駆動クロック周波数は、ＩＣカードチップ１５０が正しく動作できるような許容周波数範囲内に設定される必要がある。そのため、ＣＬＫ２制御回路１２７は、Ｆ２の値がその許容周波数範囲を外れるようなＰとＱの値を設定させない特徴を持つ。

Ｉ／Ｏ端子１５７は、ＩＣカードチップ１５０にＩＣカードコマンドを入力したり、ＩＣカードチップ１５０がＩＣカードレスポンスを出力するときに使用する入出力端子である。ＩＣカードＩ／Ｆ制御回路１２８は、Ｉ／Ｏ端子１５７と接続されており、Ｉ／Ｏ端子１５７を通してＩＣカードコマンドの信号送信やＩＣカードレスポンスの信号受信をおこなう回路である。ＩＣカードＩ／Ｆ制御回路１２８はＣＰＵ１２１に接続されており、ＣＰＵ１２１は、ＩＣカードＩ／Ｆ制御回路１２８によるＩＣカードコマンドやＩＣカードレスポンスの送受信の手続きを制御したり、送信すべきＩＣカードコマンドデータをＩＣカードＩ／Ｆ制御回路１２８に設定したり、受信したＩＣカードレスポンスをＩＣカードＩ／Ｆ制御回路１２８から取得する。ＩＣカードＩ／Ｆ制御回路１２８にはＣＬＫ２制御回路１２７からクロックが供給されており、ＩＣカードコマンドやＩＣカードレスポンスは、ＣＬＫ２端子１５３に供給するクロック信号にビット単位で同期して、Ｉ／Ｏ端子１５７を通して送受信される。また、ＲＳＴ端子１５２は、ＩＣカードチップ１５０をリセットするときにリセット信号を入力する端子である。ＩＣカードＩ／Ｆ制御回路１２８は、ＲＳＴ端子１５２と接続されており、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にリセット信号を送ることができる。

ＩＣカードチップ１５０は、ＩＣカードの電気信号規格やコマンド規格に基づいて情報交換をおこなう。ＩＣカードチップ１５０へのアクセスパターンは４種類であり、図３～図６を用いて各パターンを説明する。図３は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が非活性状態（電源が遮断されている状態）から起動して内部状態を初期化するプロセス（以下、コールドリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子

の信号波形をシンプルに表したものである。図４は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が活性状態（電源が供給されている状態）で内部状態を初期化するプロセス（以下、ウォームリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図５は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信するプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図６は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０を非活性状態にするプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図３～図６において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、破線はそれぞれの信号の基準（Ｌレベル）を表す。

図３を参照して、ＩＣカードチップ１５０のコールドリセット操作を説明する。まず、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（３０１）。次に、ＶＣＣ２制御回路１２６はＶＣＣ２端子への電源供給を開始する（３０２）。次に、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（３０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚ（プルアップされた状態）にする（３０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（３０５）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（３０６）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（３０７）。これで、コールドリセットの操作が完了する。なお、ステップ３０７は消費電力を低下させるための工夫であり、省略してもよい。

図４を参照して、ＩＣカードチップ１５０のウォームリセット操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（４０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（４０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（４０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（４０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（４０５）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（４０６）。これで、ウォームリセットの操作が完了する。なお、ステップ４０６は消費電力を低下させるための工夫であり、省略してもよい。

図５を参照して、ＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（５０１）。なお、クロックがすでに供給されている場合、ステップ５０１は不要である。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７にコマンドデータの送信を開始する（５０２）。コマンドデータの送信が終了したら、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（５０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるレスポンスデータの受信を開始する（５０４）。レスポンスデータの受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（５０５）。これで、ＩＣカードコマンド送信とＩＣカードレスポンス受信の操作が完了する。なお、ステップ５０５は、消費電力を低下させるための工夫であり、省略してもよい。

図６を参照して、ＩＣカードチップ１５０を非活性化する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３をＬレベルにする（６０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（６０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７をＬレベルにする（６０３）。最後に、ＶＣＣ２制御回路１２６はＶＣＣ２端子への電源供給を停止する（６０４）。これで、非活性

化の操作が完了する。
尚、ＩＣカードチップ１５０の停止時（例えば、セキュリティ処理を実行していない状態等）は、コントローラチップ１２０からＩＣカードチップ１５０へ電源の供給を維持したまま、クロックの供給のみを停止してもよい。
ＩＣカードチップ１５０は、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ＩＣカードチップ１５０は、ＣＰＵ１２１との間でＩＣカードコマンドやＩＣカードレスポンスの送受信することにより情報交換をおこない、その結果として、計算の結果や記憶されている情報の送出、記憶されている情報の変更などをおこなう。ＣＰＵ１２１は、ＩＣカードチップ１５０を利用してセキュリティ処理を実行することができる。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、ＶＣＣ２制御回路１２６を通してＩＣカードチップ１５０への電源供給を制御したり、またはＣＬＫ２制御回路１２７を通してＩＣカードチップ１５０へのクロック供給を制御したり、またはＩＣカードＩ／Ｆ制御回路１２８を通してＩＣカードチップ１５０にＩＣカードコマンドを送信する。これにより、ＣＰＵ１２１は、ＩＣカードチップ１５０を利用して、ホスト機器２２０が要求するセキュリティ処理を実行する。ＣＰＵ１２１は、特定のメモリカードコマンドの受信を契機に、ＩＣカードチップ１５０に対する電源供給制御、クロック供給制御、ＩＣカードコマンド送信、ＩＣカードレスポンス受信を複数組み合わせて操作することによって、セキュリティ処理を実行してもよい。また、ＣＰＵ１２１は、ホスト機器２２０がＭＭＣ１１０へ電源供給を開始したのを契機として、セキュリティ処理を実行してもよい。セキュリティ処理の結果は、ＩＣカードチップ１５０が出力するＩＣカードレスポンスをベースにして構成され、ＭＭＣ１１０内に保持される。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、セキュリティ処理の結果をホスト機器２２０に送信する。
図７は、ホスト機器２２０がＭＭＣ１１０にアクセスするときのフローチャートを表したものである。まず、ホスト機器２２０はＭＭＣ１１０を活性化するためにＶＣＣ１端子１４４に電源供給を開始する（７０１）。これを契機として、ＭＭＣ１１０は、第１次ＩＣカード初期化処理を実行する（７０２）。第１次ＩＣカード初期化処理の詳細は後述する。次に、ホスト機器２２０はＭＭＣ１１０を初期化するためにＣＭＤ端子１４２を通してＭＭＣ１１０の初期化コマンドを送信する（７０３）。この初期化コマンドはＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠したものであり、複数種類ある。ホスト機器２２０は、ＭＭＣ１１０を初期化するために、複数の初期化コマンドを送信する場合がある。ＭＭＣ１１０が初期化コマンドを受信すると、ＭＭＣ１１０はそれを処理する（７０４）。これを契機として、ＭＭＣ１１０は、第２次ＩＣカード初期化処理を実行する（７０５）。第２次ＩＣカード初期化処理の詳細は後述する。ホスト機器２２０は、ＭＭＣ１１０の初期化コマンドに対するメモリカードレスポンスを、ＣＭＤ端子１４２を通して受信し、そのメモリカードレスポンスの内容からＭＭＣ１１０の初期化が完了したかを判定する。未完了ならば、再び初期化コマンドの送信をおこなう（７０３）。ＭＭＣ１１０の初期化が完了したならば、ホスト機器２２０は、Ｍｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）や、上に述べたセキュリティ処理に関連した特定のメモリカードコマンド（ＩＣカードチップ１５０へアクセスするためのコマンド）の送信を待機する状態に移る（７０７）。この待機状態では、ホスト機器２２０は標準メモリカードコマンドを送信することができる（７０８）。ＭＭＣ１１０が標準メモリカードコマンドを受信したら、ＭＭＣ１１０はそれを処理する（７０９）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。この待機状態では、ホスト機器２２０はセキュリティ処理要求ライトコマンドを送信することもできる（７１０）。セキュリティ処理要求ライトコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０にセキュリティ処理を実行させるために処理要求を送信するメモリカードコマンドである。ＭＭＣ１１０がセキュリティ処理要求ライトコマンドを受信したら、ＣＰ

Ｕ１２１は、要求されたセキュリティ処理の内容を解釈し、セキュリティ処理をＩＣカードコマンドの形式で記述する（７１１）。即ち、ＣＰＵ１２１は、予め定められたルールに従って、ホスト機器２３０からの標準メモリカードコマンドを、ＩＣカードチップ１５０が解釈可能な特定のメモリカードコマンドへ変換する。そして、その結果として得られたＩＣカードコマンドをＩＣカードチップ１５０に発行するなどして、要求されたセキュリティ処理を実行する（７１２）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。この待機状態では、ホスト機器２２０はセキュリティ処理結果リードコマンドを送信することもできる（７１３）。セキュリティ処理結果リードコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０によるセキュリティ処理の実行結果を知るために処理結果を受信するメモリカードコマンドである。ＭＭＣ１１０がセキュリティ処理結果リードコマンドを受信したら、ＣＰＵ１２１は、ＩＣカードチップ１５０から受信したＩＣカードレスポンスをベースに、ホスト機器２２０に送信すべきセキュリティ処理結果を構築する（７１４）。そして、ホスト機器２２０は、ＭＭＣ１１０からセキュリティ処理結果を受信する。受信が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。なお、ステップ７１４は、ステップ７１２の中でおこなってもよい。

図７において、ステップ７０２およびステップ７０５で実行する第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＭＭＣ１１０内でセキュリティ処理を実行するのに備えて、ＣＰＵ１２１がＩＣカードチップ１５０に対してアクセスする処理である。具体的には、ＩＣカードチップ１５０の活性化や非活性化、ＩＣカードチップ１５０のリセット、ＩＣカードチップ１５０の環境設定を行う。環境設定とは、セキュリティ処理を実行するために必要な情報（例えば、使用可能な暗号アルゴリズムの情報、暗号計算に使用する秘密鍵や公開鍵に関する情報、個人認証に使用する認証データに関する情報など）をＩＣカードチップ１５０から読み出したり、あるいはＩＣカードチップ１５０に書き込んだりすることを意味する。ＩＣカードチップ１５０の環境設定は、ＩＣカードチップ１５０にＩＣカードコマンドをＮ個（Ｎは正の整数）発行することによっておこなう。例えば、セッション鍵が３個必要ならば、ＩＣカードコマンドを３回発行し、セッション鍵が２個必要ならば、ＩＣカードコマンドを２回発行する。Ｎ個のＩＣカードコマンドは、互いに相違するものであってもよいし、同一のものであってもよい。Ｎの値は固定されたものではなく、状況によってさまざまな値となる。以下、環境設定で発行するＩＣカードコマンドを、設定コマンドと呼ぶ。また、この環境設定に基づいてセキュリティ処理を実行するＩＣカードコマンドを、以下、セキュリティコマンドと呼ぶ。セキュリティコマンドの例としては、デジタル署名の計算、デジタル署名の検証、メッセージの暗号化、暗号化メッセージの復号、パスワードによる認証などをおこなうコマンドがある。

ＣＰＵ１２１は、ＩＣカードチップ１５０の環境設定の内容を自由に変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれを変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれを変更してもよい。また、ＣＰＵ１２１は、環境設定の内容を示した情報をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からその情報をリードして使用することもできる。この情報は、図２１においてＩＣカード環境設定情報２１１２として示されている。これにより、ＭＭＣ１１０が非活性化されてもその情報を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＩＣカード制御パラメータＡ、Ｂ、Ｃに設定された値に基づいておこなわれる。また、ＣＰＵ１２１は、ステップ７１２で実行するセキュリティ処理において、ＩＣカード制御パラメータＤに設定された値に基づいてＩＣカードチップ１５０の活性化や非活性化を制御する。図８は、ＩＣカード制御パラメータの種類と設定値、それに対応した処理の内容を表している。まず、パラメータＡは、ＭＭＣ１１０に電源が供給されたときに実行される第１次ＩＣカード初期化処理に関するパラメータである。Ａ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ａ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコ

ールドリセットする。Ａ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ａ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカードチップ１５０を非活性化する。Ａ＝０またはＡ＝３のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０が非活性状態となる。Ａ＝１またはＡ＝２のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０は活性状態となる。次に、パラメータＢとＣは、ＭＭＣ１１０がＭＭＣ初期化コマンドを処理したときに実行される第２次ＩＣカード初期化処理に関するパラメータである。Ｂ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ｂ＝１かつＣ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセット（コールドリセットまたはウォームリセット）する。Ｂ＝１かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝１かつＣ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカードチップ１５０を非活性化する。Ｂ＝２かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝２かつＣ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなった後にＩＣカードチップ１５０を非活性化する。Ｂ＝３のときは、ＩＣカードチップ１５０が活性状態ならば、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。最後に、パラメータＤは、ホスト機器２２０から要求されたセキュリティ処理を実行したあとに、ＩＣカードチップ１５０を非活性化するか否かを示すパラメータである。Ｄ＝０のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化せず、活性状態に保つ。Ｄ＝１のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。

ＣＰＵ１２１は、ＩＣカード制御パラメータＡ、Ｂ、Ｃ、Ｄの設定値を変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれらの設定値を変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれらの設定値を変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＩＣカード制御パラメータ２１１１として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

図９は、第１次ＩＣカード初期化処理のフローチャートを表している。初期化処理を開始する（９０１）と、まず、ＩＣカード制御パラメータＡが０かチェックする（９０２）。Ａ＝０ならばそのまま初期化処理は終了する（９０８）。Ａ＝０でないならばＩＣカードチップ１５０をコールドリセットする（９０３）。次に、ＩＣカード制御パラメータＡが１かチェックする（９０４）。Ａ＝１ならば初期化処理は終了する（９０８）。Ａ＝１でないならばＩＣカードチップ１５０の環境設定をおこなう（９０５）。次に、ＩＣカード制御パラメータＡが２かチェックする（９０６）。Ａ＝２ならば初期化処理は終了する（９０８）。Ａ＝２でないならばＩＣカードチップ１５０を非活性化する（９０７）。そして、初期化処理は終了する（９０８）。

図１０は、第２次ＩＣカード初期化処理のフローチャートを表している。初期化処理を開始する（１００１）と、まず、ＩＣカード制御パラメータＢが０かチェックする（１００２）。Ｂ＝０ならばそのまま初期化処理は終了する（１０１３）。Ｂ＝０でないならばＢ＝１かチェックする（１００３）。Ｂ＝１ならばＩＣカード制御パラメータＡが０または３かチェックする（１００４）。Ａが０または３ならば、ＩＣカードチップ１５０をコールドリセットし（１００５）、ステップ１００７に移る。Ａが１または２ならば、ＩＣカードチップ１５０をウォームリセットし（１００６）、ステップ１００７に移る。ステップ１００７では、ＩＣカード制御パラメータＣが１かチェックする。Ｃ＝１ならば初期化処理は終了する（１０１３）。Ｃ＝１でないならばステップ１００９に移る。ステップ１

００３においてＢ＝１でないならば、Ｂが２かチェックする（１００８）。Ｂ＝２ならばステップ１００９に移る。Ｂ＝２でないならば、ＩＣカード制御パラメータＡが０または３かチェックする（１０１１）。Ａが０または３ならば初期化処理を終了する（１０１３）。Ａが１または２ならば、ステップ１０１２に移る。ステップ１００９ではＩＣカードチップ１５０の環境設定をおこなう。そして、ＩＣカード制御パラメータＣが２かチェックする（１０１０）。Ｃ＝２ならば初期化処理を終了する（１０１３）。Ｃ＝２でないならばステップ１０１２に移る。ステップ１０１２ではＩＣカードチップ１５０を非活性化する。そして、初期化処理を終了する（１０１３）。

図１１は、ＩＣカードチップ１５０が非活性状態であるときに第１次ＩＣカード初期化処理あるいは第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１２は、ＩＣカードチップ１５０が活性状態であるときに第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１１と図１２において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。図１１において１１０２は図３に示したコールドリセットの信号波形を表す。図１２において１２０２は図４に示したウォームリセットの信号波形を表す。図１１と図１２において、第１設定コマンド処理１１０４ａと１２０４ａ、第２設定コマンド処理１１０４ｂと１２０４ｂ、第Ｎ設定コマンド処理１１０４ｃと１２０４ｃは、それぞれ図５に示したＩＣカードコマンド処理の信号波形を表す。ＩＣカードチップ１５０の環境設定の信号波形１１０４と１２０４は、Ｎ個の設定コマンド処理の信号波形が連なって構成される。図１１と図１２において、１１０６と１２０６は、それぞれ図６に示した非活性化の信号波形を表す。図１１と図１２において、縦方向の破線１１０１、１１０３、１１０５、１１０７、１２０１、１２０３、１２０５、１２０７はそれぞれ特定の時刻を表す。１１０１はコールドリセット前の時刻、１２０１はウォームリセット前の時刻、１１０３はコールドリセット後から環境設定前の間にある時刻、１２０３はウォームリセット後から環境設定前の間にある時刻、１１０５と１２０５は環境設定後から非活性化前の間にある時刻、１１０７と１２０７は非活性化後の時刻である。

図１１を参照して、第１次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＡが０のときは、信号波形に変化はない。Ａ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ａ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ａ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

図１１を参照して、ＩＣカード制御パラメータＡが０または３のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

図１２を参照して、ＩＣカード制御パラメータＡが１または２のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１２０１から時刻１２０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１２０１から時刻１２０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１２０１から時刻１２０７までの範囲の信号波形となる。Ｂ＝２かつＣ＝２のときは、時刻１２０３から時刻１２０５までの範囲の信号波形となる。Ｂ＝２かつＣ＝３のときは、時刻１２０３から時刻１２０７までの範囲の信号波形となる。Ｂ＝３のときは、時刻１２０５から時刻１２０７までの範囲の信号波形となる。

図１３は、図７のステップ７１２において、ＣＰＵ１２１が、ホスト機器２２０が要求し

たセキュリティ処理をＩＣカードチップ１５０によって実行するときのフローチャートを表している。セキュリティ処理を開始する（１３０１）と、まずＩＣカードチップ１５０が非活性状態かをチェックする（１３０２）。非活性状態ならば、ＩＣカードチップ１５０をコールドリセットし（１３０３）、ステップ１３０６に移る。活性状態ならば、ステップ１３０４に移る。ステップ１３０４では、ＩＣカードチップ１５０にＩＣカードコマンドを発行する前にＩＣカードチップ１５０を再リセットする必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０をウォームリセットし（１３０５）、ステップ１３０６に移る。必要がないならば、ステップ１３０６に移る。ステップ１３０６では、ＩＣカードチップ１５０の環境設定をおこなう必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０の環境設定をおこない（１３０７）、ステップ１３０８に移る。必要がないならば、ステップ１３０８に移る。ステップ１３０８では、ＩＣカードチップ１５０のＣＬＫ２端子に供給するクロック信号の周波数Ｆ２を設定する。そして、ＣＰＵ１２１はＩＣカードチップ１５０にセキュリティコマンドを発行し、ＩＣカードチップ１５０はそれを処理する（１３０９）。セキュリティコマンドの処理時間は、クロック周波数Ｆ２に依存する。次に、ＩＣカードチップ１５０が出力するＩＣカードレスポンスにより、その処理が成功したかどうかを判定する（１３１０）。成功ならば、ステップ１３１１に移る。失敗ならば、ステップ１３１２に移る。ステップ１３１１では、ＩＣカードチップ１５０に発行すべきセキュリティコマンドが全て完了したかをチェックする。発行すべきセキュリティコマンドがまだあるならば、ステップ１３０４に移る。発行すべきセキュリティコマンドが全て完了したならば、ステップ１３１４に移る。ステップ１３１２では、失敗したセキュリティコマンドをリトライすることが可能かを判定する。リトライできるなら、リトライ設定をおこない（１３１３）、ステップ１３０４に移る。リトライ設定とは、リトライすべきセキュリティコマンドやその関連データをＣＰＵ１２１が再度準備することである。リトライできないならステップ１３１４に移る。これは、ホスト機器２２０が要求したセキュリティ処理が失敗したことを意味する。ステップ１３１４では、ＩＣカード制御パラメータＤをチェックする。Ｄ＝１ならば、ＩＣカードチップ１５０を非活性化して（１３１５）、セキュリティ処理を終了する（１３１６）。Ｄ＝１でないならば、ＩＣカードチップ１５０を活性状態に保ったままセキュリティ処理を終了する（１３１６）。図１３のフローチャートにおいては、クロック周波数Ｆ２を、ステップ１３０９で発行するセキュリティコマンドの種類によって変えることができるように、ステップ１３０８をステップ１３０９の直前に位置させたが、ステップ１３０８はそれ以外の位置にあってもよい。

従来のＩＣカードへの攻撃法を有効にしている要因のひとつとして、ＩＣカードの駆動クロックが外部の接続装置から直接供給されることがあげられる。駆動クロックが接続装置の制御下にあるため、タイミング解析や電力差分解析においては、電気信号の測定においてＩＣカード内部処理のタイミングの獲得が容易になる。一方、故障利用解析においては、異常な駆動クロックの供給による演算エラーの発生が容易になる。これに対し、本発明によれば、ＭＭＣ１１０内部でＩＣカードチップ１５０によりセキュリティ処理を実行するとき、ホスト機器２２０はＩＣカードチップ１５０の駆動クロックを直接供給できない。ＣＰＵ１２１は、ＩＣカードチップ１５０へ供給するクロックの周波数Ｆ２を自由に設定することができる。これにより、ホスト機器２２０の要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。ホスト機器２２０が高速なセキュリティ処理を要求するならば周波数Ｆ２を高く設定し、低い消費電力を要求するならば周波数Ｆ２を低く設定したり、クロックを適度に停止させればよい。また、ＣＰＵ１２１は、周波数Ｆ２だけでなくクロックの供給開始タイミング、供給停止タイミングを自由に設定できる。これらをランダムに変化させることにより、ＩＣカードチップ１５０に対するタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法を困難にすることができる。タイミング解析は、攻撃者が暗号処理１回の処理時間を正確に計測可能であることを仮定しているため、その対策としては、攻撃者が処理時間計測を正確に行えないようにすることが有効である。本発明によりタイミング解析が困難になる理由は、ＩＣカードチップ１５０がＩＣカー

ドコマンドを処理している時間の長さをホスト機器２２０が正確に計測できないためである。電力差分解析の対策としては、処理の実行タイミングや順序に関する情報を外部から検出不可能にすることが有効である。本発明により電力差分解析が困難になる理由は、ＩＣカードコマンドが発行された時刻、発行されたＩＣカードコマンドの内容、発行されたＩＣカードコマンドの順序（ＩＣカードコマンドを複数組み合わせてセキュリティ処理を実行する場合）の検出がホスト機器２２０にとって困難になるためである。故障利用解析の対策としては、ＩＣカードにクロックや電圧や温度等の動作環境検知回路を搭載し、異常を検出したならば処理を停止あるいは使用不能にするという方法が有効である。本発明により故障利用解析が困難になる理由は、ＣＬＫ２制御回路１２７がＩＣカードチップ１５０に異常な駆動クロックを供給しないことが、ホスト機器２２０がＩＣカードチップ１５０に演算エラーを発生させるのを防止するからである。

ＣＰＵ１２１は、ＩＣカードチップ１５０に供給するクロックの周波数Ｆ２、供給開始タイミング、供給停止タイミングの設定値を、セキュリティ処理の内容や結果に応じて変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機として変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＣＬＫ２設定情報２１１３として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

図１４は、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程（図７のステップ７１０～７１２）において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスをシンプルに表したものである。図１４において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。図１４を参照して、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程を説明する。まず、ホスト機器２２０はＣＭＤ端子１４２にセキュリティ処理要求ライトコマンドを送信する（１４０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理要求ライトコマンドのレスポンスを受信する（１４０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理の実行結果ではない。次に、ホスト機器２２０はＤＡＴ端子１４７にセキュリティ処理要求を送信する（１４０３）。セキュリティ処理要求とは、セキュリティ処理の内容や処理すべきデータを含むホストデータである。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１４０４）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、ホスト機器２２０から受信したセキュリティ処理要求をフラッシュメモリチップ１３０にライトするコマンドを発行する（１４０５）。セキュリティ処理要求をフラッシュメモリチップ１３０にライトすることにより、ＣＰＵ１２１がセキュリティ処理要求をＩＣカードコマンド形式で記述する処理（図７のステップ７１１）において、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求のデータサイズが大きいときに有効である。なお、フラッシュメモリチップ１３０にライトされたセキュリティ処理要求は、図２１においてセキュリティ処理バッファ領域２１１４に格納される。また、ライトコマンド発行１４０５は必須な操作ではない。ライト処理期間１４０６は、フラッシュメモリチップ１３０がセキュリティ処理要求のライト処理を実行している期間を表す。セキュリティ処理１４０７はＩＣカードチップ１５０によるセキュリティ処理の信号波形を表す。

この信号波形は図１３のフローチャートの遷移過程に依存する。セキュリティ処理１４０７は、ライト処理期間１４０６とオーバラップさせることができる。一般にフラッシュメモリチップ１３０のライト処理期間１４０６はミリ秒のオーダーであるため、セキュリティ処理１４０７とオーバラップさせることは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。リード／ライト１４０８は、セキュリティ処理１４０７の実行中に、フラッシュメモリチップ１３０からセキュリティ処理要求をリードしたり、ＩＣカードチップ１５０が出力した計算結果をフラッシュメモリチップ１３０にライトするアクセスを示している。このアクセスにより、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求やセキュリティ処理結果のデータサイズが大きいときに有効である。リード／ライト１４０８は必須ではない。セキュリティ処理１４０７が完了したら、ＭＭＣ１１０はＤＡＴ端子１４７をＨレベルにセットする（１４０９）。ＭＭＣ１１０は、これによりセキュリティ処理が完了したことをホスト機器２２０に示す。

図１５は、図１４におけるセキュリティ処理１４０７の信号波形の一例を表したものである。図１５において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１５０１は図３に示したコールドリセットの信号波形を表し、１５０４は図４に示したウォームリセットの信号波形を表し、１５０２および１５０５は図１１（あるいは図１２）に示した環境設定の信号波形を表し、１５０３および１５０６および１５０７は図５に示したＩＣカードコマンド処理の信号波形を表し、１５０８は図６に示した非活性化の信号波形を表す。ＩＣカードチップ１５０の外部端子において図１５に示した信号波形が観測されるのは、図１３のフローチャートが１３０１、１３０２、１３０３、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０５、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０６、１３０８、１３０９、１３１０、１３１１、１３１４、１３１５、１３１６の順で遷移するときである。図１５を参照して、図１４のセキュリティ処理１４０７の実行中におけるＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセス（リード／ライト１４０８）を説明する。このアクセスには、図２１におけるセキュリティ処理バッファ領域２１１４を使用する。リード１５０９、１５１１、１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、１５０７においてＩＣカードチップ１５０に送信するＩＣカードコマンドを構築するために必要なデータを、フラッシュメモリチップ１３０からリードするアクセスである。ライト１５１０は、セキュリティコマンド処理１５０３においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にライトするアクセスである。ライト１５１３は、セキュリティコマンド処理１５０６および１５０７においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にまとめてライトするアクセスである。リード１５０９、１５１１、１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、１５０７以前のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。ライト１５１０、１５１３は、それぞれ、セキュリティコマンド処理１５０３、１５０７以後のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。これらのオーバラップは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。さらに、フラッシュメモリチップ１３０のライト単位が大きい場合は、ライト１５１３のように複数の計算結果をまとめてライトすることができる。これは、フラッシュメモリチップ１３０へのライト回数を削減し、フラッシュメモリチップ１３０の劣化を遅らせる効果がある。なお、ライト１５１０、１５１３でフラッシュメモリチップ１３０にライトする内容は、ＩＣカードチップ１５０が出力した計算結果そのものに限定されず、図７のステップ７１５でホスト機器２２０に返すセキュリティ処理結果またはその一部であってもよい。この場合、図７のステップ７１４またはその一部は、ステップ７１２の中で実行されることになる。

図１６は、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程（図７のステップ７１３～７１５）において、ＭＭＣ１１０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスをシンプルに表したものである。図１６において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。図１６を参照して、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程を説明する。まず、ホスト機器２２０はＣＭＤ端子１４２にセキュリティ処理結果リードコマンドを送信する（１６０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理結果リードコマンドのレスポンスを受信する（１６０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理結果ではない。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１６０３）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）から、ＩＣカードチップ１５０が出力した計算結果をリードする（１６０４）。ＣＰＵ１２１は、これをもとにセキュリティ処理結果を構築し、ＭＭＣ１１０がＤＡＴ端子１４７にセキュリティ処理結果を出力する（１６０５）。なお、図７のステップ７１４またはその一部が、ステップ７１２の中で実行されている場合、ステップ１６０４ではフラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）からセキュリティ処理結果またはその一部をリードする。なお、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）を利用しないでセキュリティ処理結果を構築する場合、ステップ１６０４は必要ない。

図２７は、図７のステップ７１０においてＭＭＣ１１０に送信するセキュリティ処理要求データ、およびステップ７１５でホスト機器２２０が受信するセキュリティ処理結果データそれぞれのフォーマットの一例を示したものである。このフォーマットは、要求されたセキュリティ処理の内容が１つのＩＣカードコマンドで表現でき、セキュリティ処理の結果が１つのＩＣカードレスポンスで表現できる場合に適用することが好ましい。ＩＣカードチップ１５０に送信するＩＣカードコマンド、ＩＣカードチップ１５０から受信するＩＣカードレスポンスはともにＩＳＯ／ＩＥＣ７８１６－４規格に従う。本規格によれば、ＩＣカードコマンドの構成は、４バイトのヘッダ（クラスバイトＣＬＡ、命令バイトＩＮＳ、パラメータバイトＰ１とＰ２）が必須であり、必要に応じて、入力データ長指示バイトＬｃ、入力データＤａｔａ　Ｉｎ、出力データ長指示バイトＬｅが後に続く。また、ＩＣカードレスポンスの構成は、２バイトのステータスＳＷ１とＳＷ２が必須であり、必要に応じて、出力データＤａｔａ　Ｏｕｔがその前に置かれる。本フォーマットにおけるセキュリティ処理要求のデータ２７０１は、ＩＣカードコマンド２７０２の前にフォーマット識別子ＦＩＤ２７０３とＩＣカードコマンド長Ｌｃａ２７０４を付け、さらにＩＣカードコマンド２７０２の後にダミーデータ２７０５をパディングしたものである。ＦＩＤ２７０３はフォーマットの識別番号またはフォーマットの属性データを含む。Ｌｃａ２７０４の値はＩＣカードコマンド２７０２の各構成要素の長さを合計した値である。一方、セキュリティ処理結果のデータ２７１１は、ＩＣカードレスポンス２７１２の前にフォーマット識別子ＦＩＤ２７１３とＩＣカードレスポンス長Ｌｒａ２７１４を付け、さらにＩＣカードレスポンス２７１２の後にダミーデータ２７１５をパディングしたものである。ＦＩＤ２７１３はフォーマットの識別番号またはフォーマットの属性データを含む。Ｌｒａ２７１４の値はＩＣカードレスポンス２７１２の各構成要素の長さを合計した値である。なお、この図では、ＩＣカードコマンドにＬｃ、Ｄａｔａ　Ｉｎ、Ｌｅが含まれ、ＩＣカードレスポンスにＤａｔａ　Ｏｕｔが含まれる場合のフォーマット例を表している。Ｍｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ仕様では、リード／ライトアクセスするデータを固定長の

ブロック単位で処理することが標準となっている。よって、セキュリティ処理要求のデータ２７０１やセキュリティ処理結果のデータ２７１１のサイズもＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠したブロックサイズに一致させることが好ましい。ダミーデータ２７０５、２７１５は、セキュリティ処理要求のデータ２７０１やセキュリティ処理結果のデータ２７１１のサイズをブロックサイズに一致させるために適用される。ブロックサイズとして採用する値は、一般の小型メモリカードが論理ファイルシステムに採用しているＦＡＴ方式におけるセクタサイズ（５１２バイト）が望ましい。パディングするダミーデータ２７０５、２７１５は全てゼロでもよいし、乱数でもよいし、ＣＰＵ１２１やホスト機器２２０がデータエラーを検出したり訂正するためのチェックサムでもよい。Ｌｃａ２７０４の値はＣＰＵ１２１がセキュリティ処理要求のデータ２７０１からダミーデータ２７０５を除去するために使用し、Ｌｒａ２７１４の値はホスト機器２２０がセキュリティ処理結果のデータ２７１１からダミーデータ２７１５を除去するために使用する。

ＭＭＣ１１０の製造者や管理者は、セキュリティシステムのユーザにＭＭＣ１１０を提供する前やそのユーザが所有するＭＭＣ１１０に問題が発生した時に、ＭＭＣ１１０に内蔵されたＩＣカードチップ１５０に様々な初期データを書きこんだり、ＩＣカードチップ１５０のテストをおこなったりする必要がある。ＭＭＣ１１０の製造者や管理者によるこれらの操作の利便性を高めるために、ＭＭＣ１１０は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるインタフェース機能を持つ。これにより、図３～図６で示したようなＩＣカードチップ１５０へのアクセス信号を、ＭＭＣ外部端子１４０から直接送受信できる。このようなＭＭＣ１１０の動作モードを、Ｍｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した動作モードと区別して、以下、インタフェース直通モードと呼ぶ。

インタフェース直通モードについて詳細に説明する。図１７は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるときの対応関係の一例を表している。この例では、ＲＳＴ端子１５２をＣＳ端子１４１に割り付け、ＧＮＤ２端子１５５をＧＮＤ１端子１４３、１４６に割り付け、ＶＣＣ２端子１５１をＶＣＣ１端子１４４に割り付け、ＣＬＫ２端子１５３をＣＬＫ１端子１４５に割り付け、Ｉ／Ｏ端子１５７をＤＡＴ端子１４７に割り付ける。このとき、ＣＳ端子１４１とＣＬＫ１端子１４５は入力端子、ＤＡＴ端子１４７は入出力端子として機能する。

ＭＭＣ１１０は、特定のメモリカードコマンドを受信すると、動作モードをインタフェース直通モードへ移したり、インタフェース直通モードからＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した動作モードに戻すことができる。以下、動作モードをインタフェース直通モードへ移すメモリカードコマンドを直通化コマンド、動作モードをインタフェース直通モードから通常の状態に戻すメモリカードコマンドを復帰コマンドと呼ぶ。図１を参照して、ＭＭＣＩ／Ｆ制御回路１２３は、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８と接続されており、ＭＭＣ１１０がホスト機器２２０から直通化コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けをおこなう。ＭＭＣ１１０がホスト機器２２０から復帰コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した動作モードに戻る。

インタフェース直通モードでは、ホスト機器２２０がＩＣカードチップ１５０に直接アクセスできるため、セキュリティの観点からインタフェース直通モードを利用できるのは限られた者だけにする必要がある。そこで、直通化コマンドの発行には、一般のユーザに知られないパスワードの送信を必要とする。正しいパスワードが入力されないとインタフェース直通モードは利用できない。

図１８は、ホスト機器２２０が、ＭＭＣ１１０の動作モードをＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した動作モードからインタフェース直通モードに移し、ＩＣカードチップ１５０に直接アクセスし、その後、ＭＭＣ１１０の動作モードを再びＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した動作モードに戻すまでの処理のフローチャートを表している。ホスト機器２２０は処理を開始し（１８０１）、まずＭＭＣ１１０に直通化コマ

ンドを発行する（１８０２）。ＭＭＣ１１０は、直通化コマンドで送信されたパスワードが正しいかチェックする（１８０３）。正しければステップ１８０４に移り、間違っていれば処理は終了する（１８１０）。ステップ１８０４では、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする。そして、図１７で示した端子割り付けをおこないインタフェースを直通化する（１８０５）。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする（１８０６）。ホスト機器２２０がＩＣカードチップ１５０への直接アクセスを終了し、ＭＭＣ１１０の動作モードを再びＭｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ仕様に準拠した動作モードに戻すときは、ＭＭＣ１１０に復帰コマンドを発行する（１８０７）。すると、ＣＰＵ１２１は図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ仕様に準拠した動作モードに戻る（１８０８）。そして、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（１８０９）。以上で、処理は終了する（１８１０）。

図１９は、図１８のステップ１８０１～１８０６の過程において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１９において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１９０５は、図３のコールドリセットの信号波形を示す。モード移行時刻１９０６は、動作モードがインタフェース直通モードに移る時刻を表す。

図１９を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをＭｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ仕様に準拠した動作モードからインタフェース直通モードに移しＩＣカードチップ１５０に直接アクセスする過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に直通化コマンドを入力すると（１９０１）、ＣＭＤ端子１４２から直通化コマンドのレスポンスが出力される（１９０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。次に、ホスト機器２２０はＤＡＴ端子１４７にパスワードを入力する（１９０３）。パスワード入力後、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力し（１９０４）、ビジー状態であることをホスト機器２２０に示す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする（１９０５）。そして、モード移行時刻１９０６において、動作モードをインタフェース直通モードに移す。このときに、ＤＡＴ端子１４７はＬレベルからハイインピーダンス状態になる。これにより、ホスト機器２２０はビジー状態の解除を知ることができる。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする。例えば、ＣＬＫ１端子１４５にクロックを供給すると（１９０７）、ＣＬＫ２端子１５３にそのクロックが供給される（１９０８）。また、ＤＡＴ端子１４７にＩＣカードコマンドを送信すると（１９０９）、Ｉ／Ｏ端子１５７にそのＩＣカードコマンドが送信される（１９１０）。

図２０は、図１８のステップ１８０７～１８１０の過程において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図２０において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。モード復帰時刻２００３は、動作モードがインタフェース直通モードからＭｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ仕様に準拠した動作モードに戻る時刻を表す。２００４は、図６の非活性化の信号波形を示す。

図２０を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをインタフェース直通モードからＭｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ仕様に準拠した動作モードに戻す過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に復帰コマンドを入力す

ると（２００１）、ＣＭＤ端子１４２から復帰コマンドのレスポンスが出力される（２００２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。そして、モード復帰時刻２００３において、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力してビジー状態であることをホスト機器２２０に示し、それと同時に動作モードをＭｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ仕様に準拠した動作モードに戻す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（２００４）。そして、ＭＭＣ１１０は、ＤＡＴ端子１４７をハイインピーダンス状態にし（２００５）、復帰コマンドの処理が完了したことをホスト機器２２０に示す。これ以後、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスできない。ホスト機器２２０が、ＣＬＫ１端子１４５にクロックを供給しながらＣＭＤ端子１４２に何らかのメモリカードコマンドを送信した場合、ＩＣカードチップ１５０にそのクロック信号（２００６）は伝わらない。２００１や２００２においてホスト機器２２０がＣＬＫ１端子１４５に供給するクロック信号は、ＩＣカードチップ１５０のＣＬＫ２端子１５３にも伝わるが、ＤＡＴ端子１４７がハイインピーダンス状態であるため、ＩＣカードチップ１５０がＩＣカードコマンドを誤って認識することはない。

図２１において、セキュリティ処理ステータス領域２１１６には、ＩＣカードチップ１５０によるセキュリティ処理の進捗状況を示す情報を格納する。ＣＰＵ１２１は、この情報をセキュリティ処理の実行中に更新することができる。例えば、セキュリティ処理の途中でＭＭＣ１１０への電源供給が停止した場合、電源供給再開時にＣＰＵ１２１がこの情報をリードして参照すれば、セキュリティ処理を中断した段階から再開することができる。

本発明の実施形態によれば、メモリカード外部からＩＣチップの駆動クロックを直接供給しないため、ＩＣチップの処理時間を正確に計測できず、また、処理の実行タイミングや順序の検出が困難になる。さらに、異常な駆動クロックを供給することができず、演算エラーを発生させるのが困難になる。したがって、タイミング解析、電力差分解析、故障利用解析攻撃法に対するセキュリティが向上する。

本発明の実施形態によれば、メモリカード外部からＩＣチップの制御方式を自由に設定できる。例えば、高速処理が要求されるならば、ＩＣチップの駆動クロックの周波数を高くした制御方式を設定し、低消費電力が要求されるならば、ＩＣチップの駆動クロックの周波数を低くしたり、ＩＣチップの駆動クロックを適度に停止させる制御方式を設定することができる。したがって、セキュリティシステムの要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。

本発明によれば、ＩＣチップによるセキュリティ処理に必要なデータや、ＩＣチップを管理するための情報を、フラッシュメモリに保持することができる。したがって、セキュリティ処理の利便性を向上させることができる。

本発明の実施形態によれば、ＭＭＣの製造者や管理者が、ＭＭＣ内部のＩＣチップに直接アクセスすることができる。したがって、ＭＭＣ内部のＩＣチップの初期化やメンテナンスを、従来のＩＣカードと同様な方法で実現できる。

本発明の実施形態によれば、フラッシュメモリチップを備えたＭＭＣに、セキュリティ機能を追加する場合、セキュリティ評価機関の認証を予め受けたＩＣカードチップ追加搭載することによって、セキュリティ評価機関によるＭＭＣの認証が不要となるため、ＭＭＣの開発期間又は製造期間が短縮する。

産業上の利用可能性

本発明によれば、記憶装置のセキュリティを向上するという効果を奏する。

本発明によれば、記憶装置の製造が簡略化されるという効果を奏する。

上記記載は実施例についてなされたが、本発明はその精神と添付クレームの範囲内で種々の変更および修正をすることができることは当業者に明らかである。

【図面の簡単な説明】

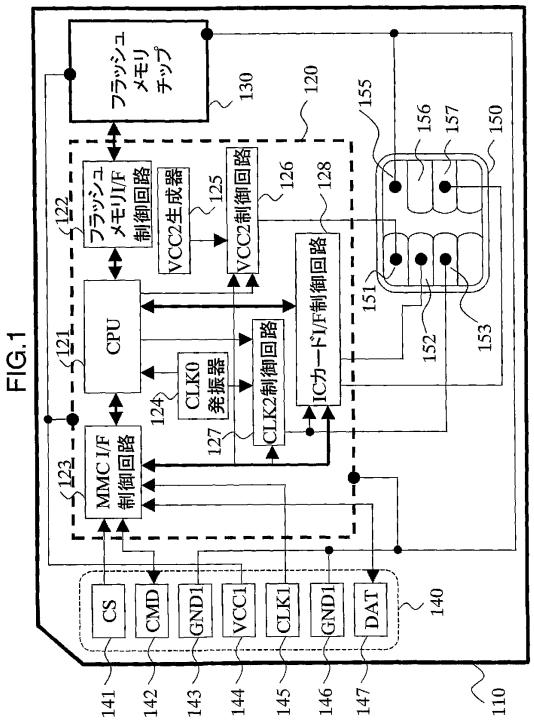
第１図は、本発明を適用したＭＭＣの内部構成を示す図である。

第２図は、本発明を適用したＭＭＣのホスト機器の内部構成、およびホスト機器とＭＭＣとの接続状態を示す図である。

第３図は、ＩＣカードチップのコールドリセット時の信号波形を示す図である。
第４図は、ＩＣカードチップのウォームリセット時の信号波形を示す図である。
第５図は、ＩＣカードチップのＩＣカードコマンド処理時の信号波形を示す図である。
第６図は、ＩＣカードチップの非活性化時の信号波形を示す図である。
第７図は、ホスト機器によるＭＭＣへのアクセスを示したフローチャートである。
第８図は、ＩＣカード制御パラメータとそれに対応するＩＣカードへの処理内容を示す図表である。
第９図は、ＩＣカードチップに対する第１次ＩＣカード初期化の詳細なフローチャートである。
第１０図は、ＩＣカードチップに対する第２次ＩＣカード初期化の詳細なフローチャートである。
第１１図は、非活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。
第１２図は、活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。
第１３図は、ＩＣカードチップによるセキュリティ処理の詳細なフローチャートである。
第１４図は、セキュリティ処理要求ライトコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。
第１５図は、ＩＣカードチップによるセキュリティ処理実行時の信号波形とフラッシュメモリチップアクセスの一例を示す図である。
第１６図は、セキュリティ処理結果リードコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。
第１７図は、インタフェース直通モードにおけるＭＭＣ外部端子とＩＣカードチップ外部端子の対応関係を示す図である。
第１８図は、インタフェース直通モードへ移行する処理とインタフェース直通モードから復帰する処理のフローチャートである。
第１９図は、インタフェース直通モードへ移行する処理時の信号波形を示す図である。
第２０図は、インタフェース直通モードから復帰する処理時の信号波形を示す図である。
第２１図は、フラッシュメモリチップの内部構成を示す図である。
第２２図は、本発明を適用したＭＭＣの内部構成を簡単に示す図である。
第２３図は、本発明を適用したＭＭＣをコンテンツ配信に応用した例を示す図である。
第２４図は、本発明を適用したＳＤカードの内部構成を簡単に示す図である。
第２５図は、本発明を適用したメモリースティックの内部構成を簡単に示す図である。
第２６図は、本発明のＩＣカードチップの内部構成を示す図である。
第２７図は、セキュリティ処理要求とセキュリティ処理結果の各データフォーマットの一例を示す図である。

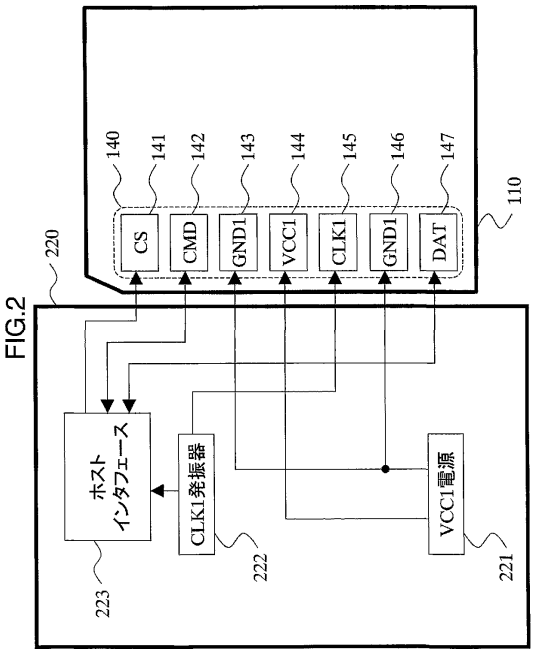
【図１】

FIG.1



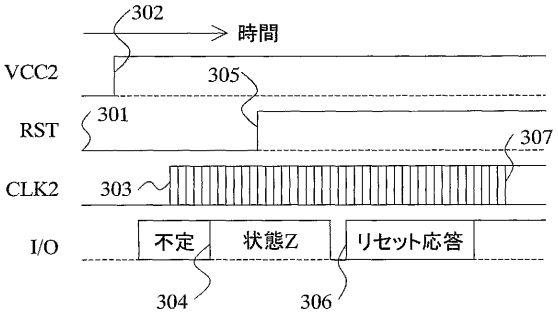
【図２】

FIG.2



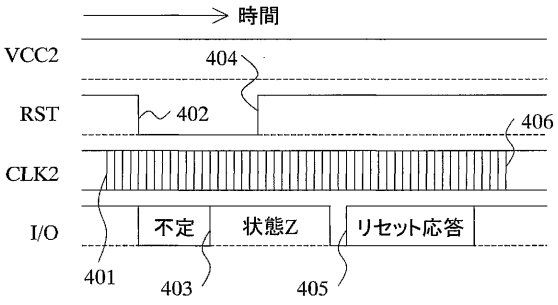
【図３】

FIG.3



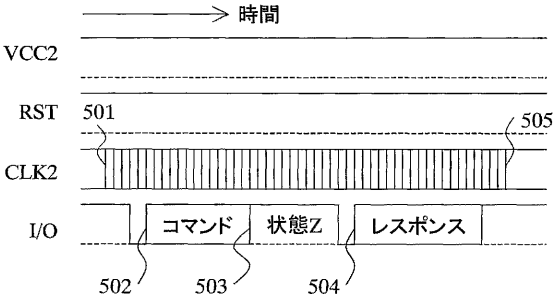
【図４】

FIG.4



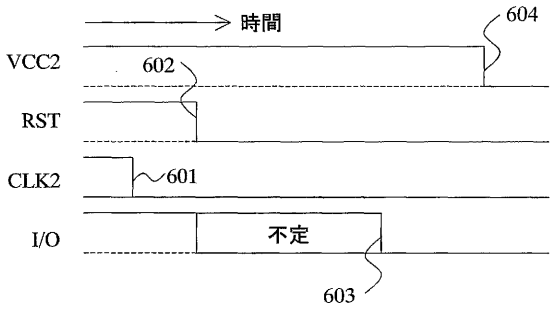
【図５】

FIG.5



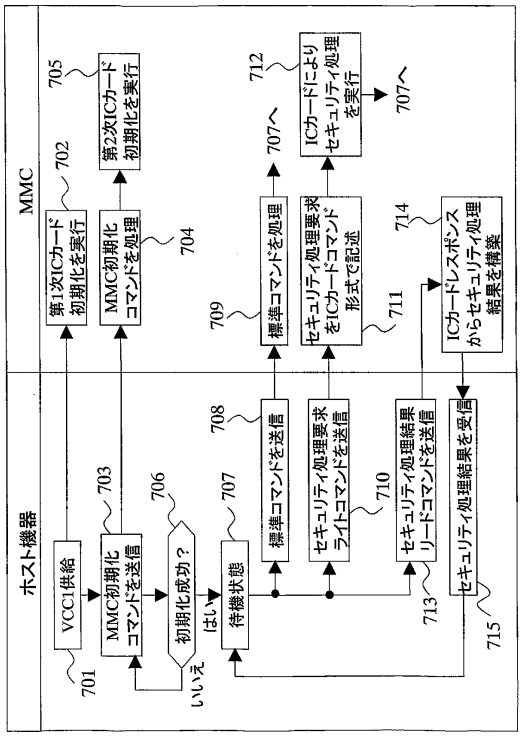
【図６】

FIG.6



【図７】

FIG.7



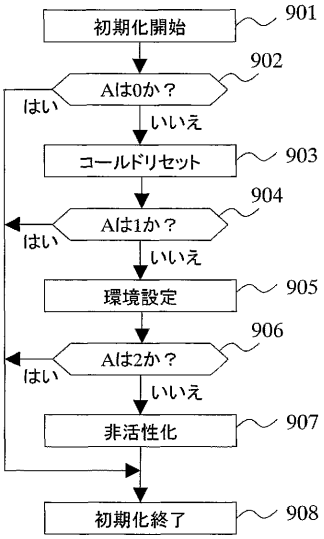
【図８】

FIG.8

ICカード制御パラメータ		ICカードに対する処理
A=0		MMCのパワーオン時に，何もしない
A=1		MMCのパワーオン時に，リセット
A=2		MMCのパワーオン時に，リセットと環境設定
A=3		MMCのパワーオン時に，リセットと環境設定し，非活性化
B=0		MMCの初期化時に，何もしない
B=1	C=1	MMCの初期化時に，リセット
	C=2	MMCの初期化時に，リセットと環境設定
	C=3	MMCの初期化時に，リセットと環境設定し，非活性化
B=2	C=2	MMCの初期化時に，環境設定
	C=3	MMCの初期化時に，環境設定し，非活性化
B=3		MMCの初期化時に，活性状態ならば，非活性化
D=0		セキュリティ処理後に，非活性化しない
D=1		セキュリティ処理後に，非活性化する

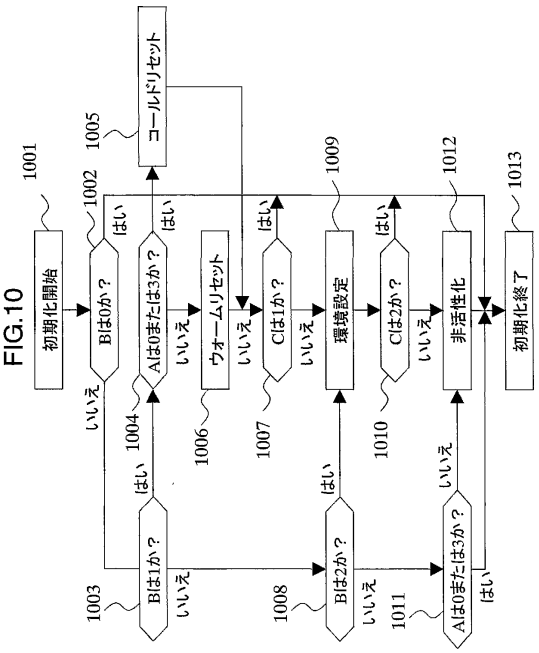
【図９】

FIG.9



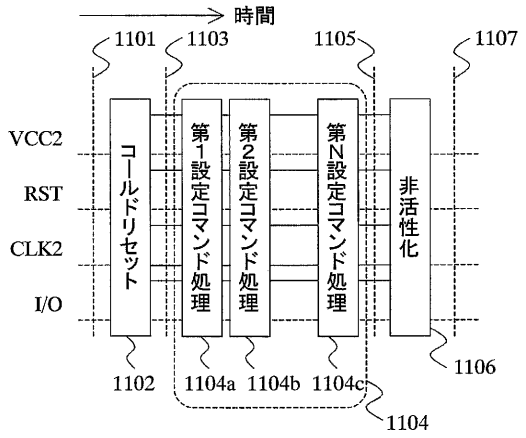
【図１０】

FIG.10



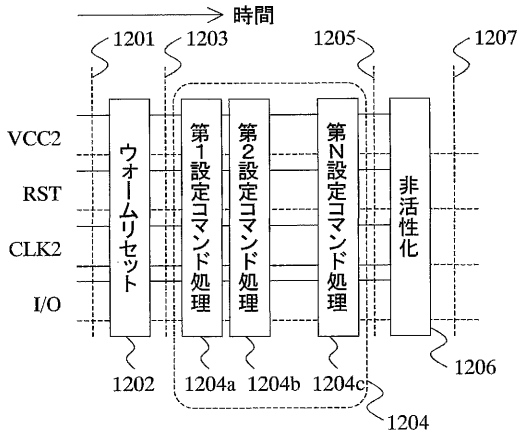
【図１１】

FIG.11



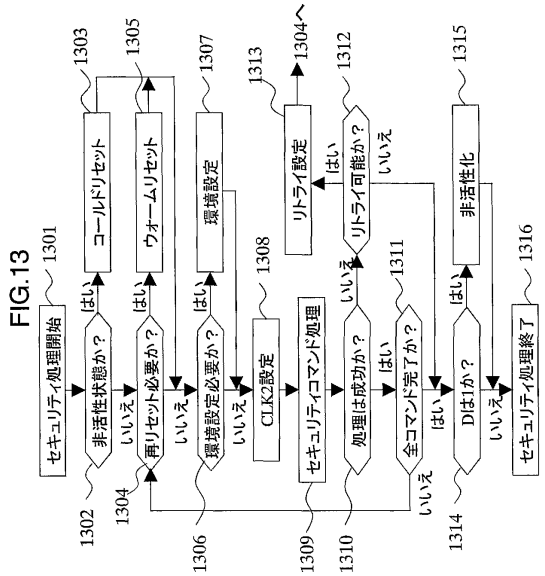
【図１２】

FIG.12



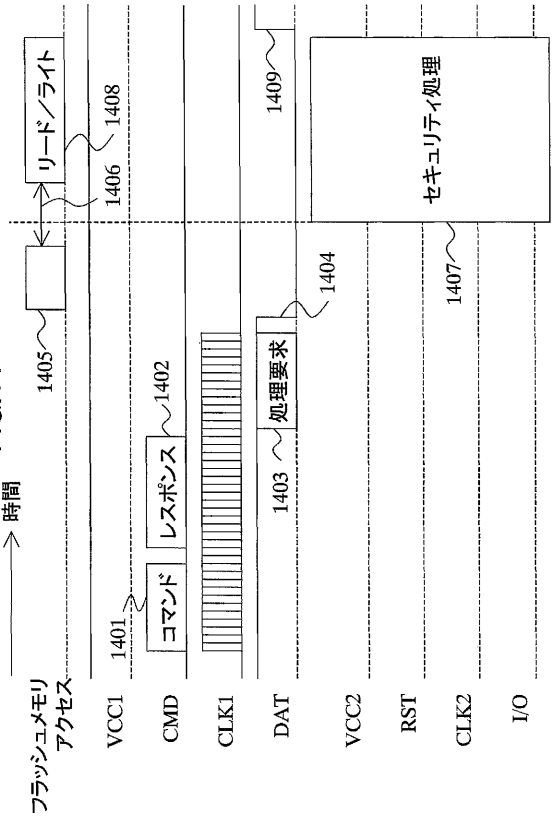
【図１３】

FIG.13



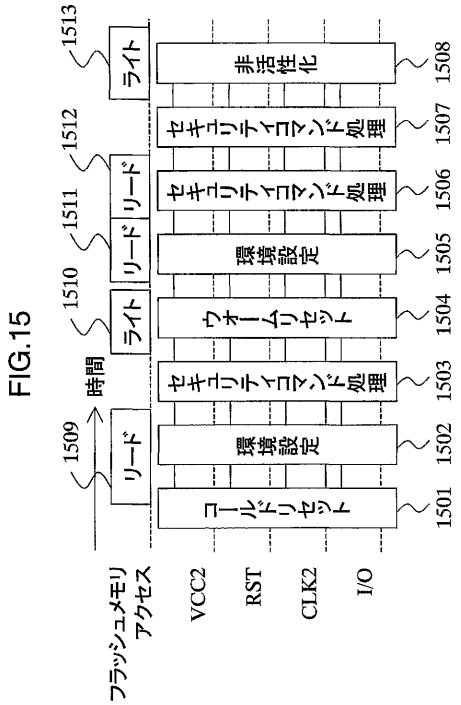
【図１４】

FIG.14



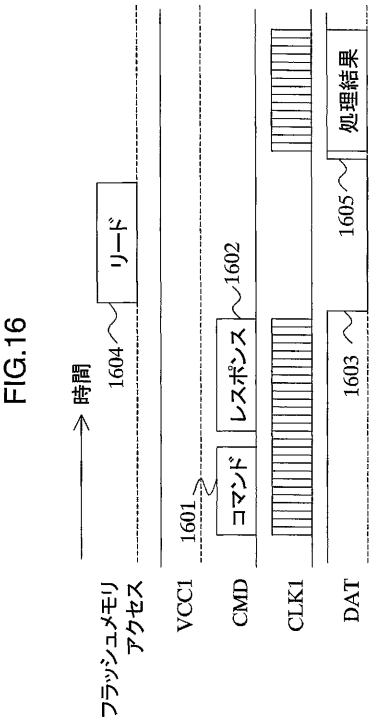
【図１５】

FIG.15



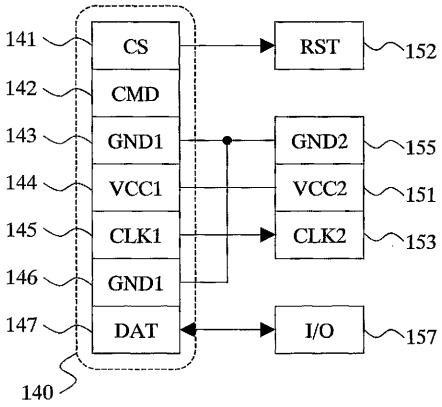
【図１６】

FIG.16



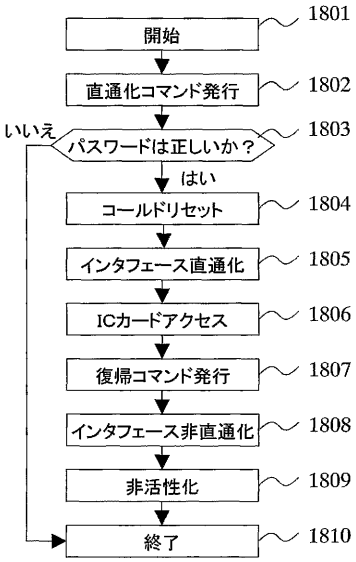
【図１７】

FIG.17



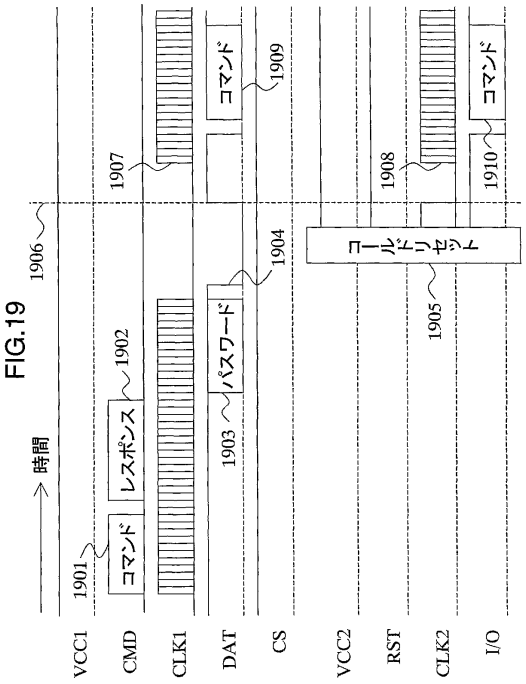
【図１８】

FIG.18



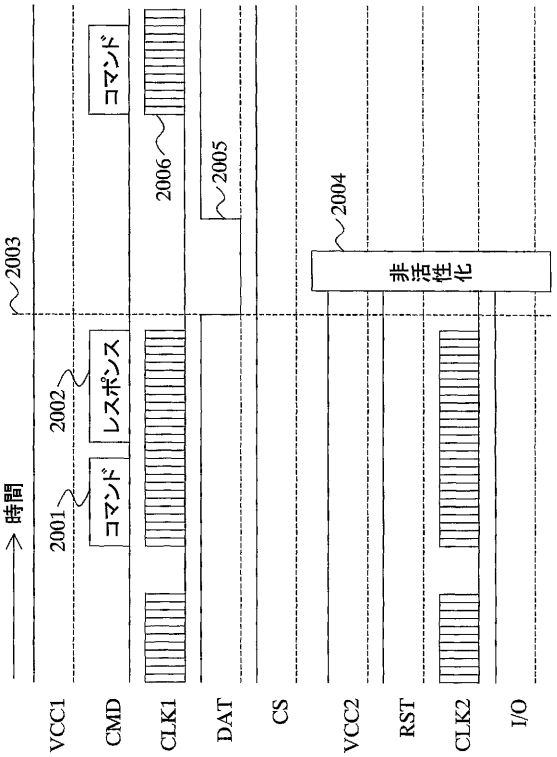
【図１９】

FIG.19



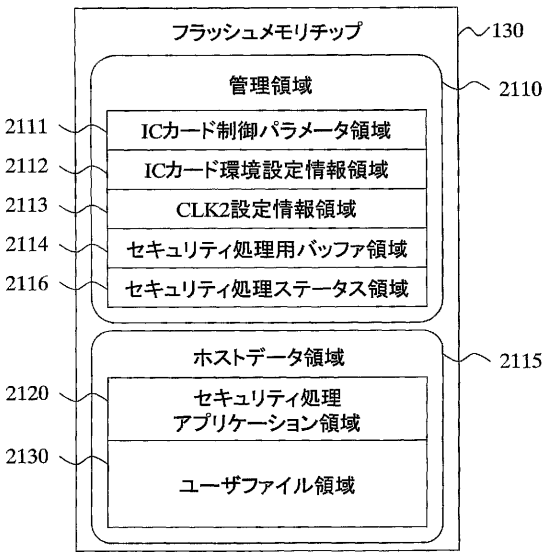
【図２０】

FIG.20



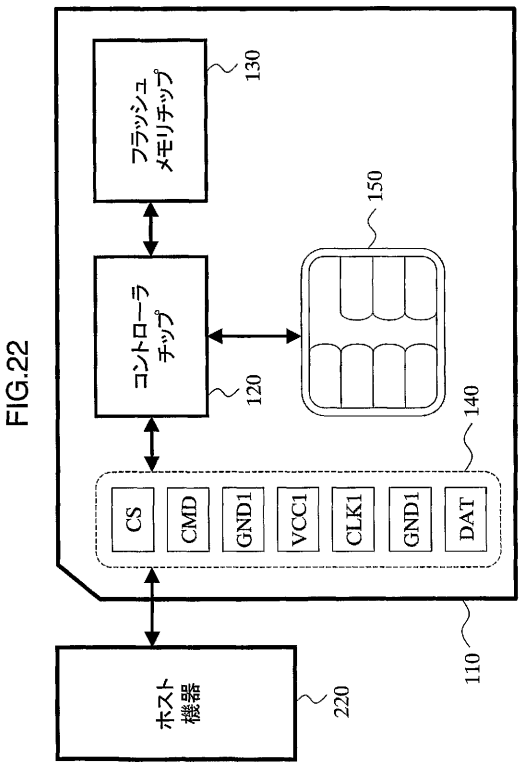
【図２１】

FIG.21

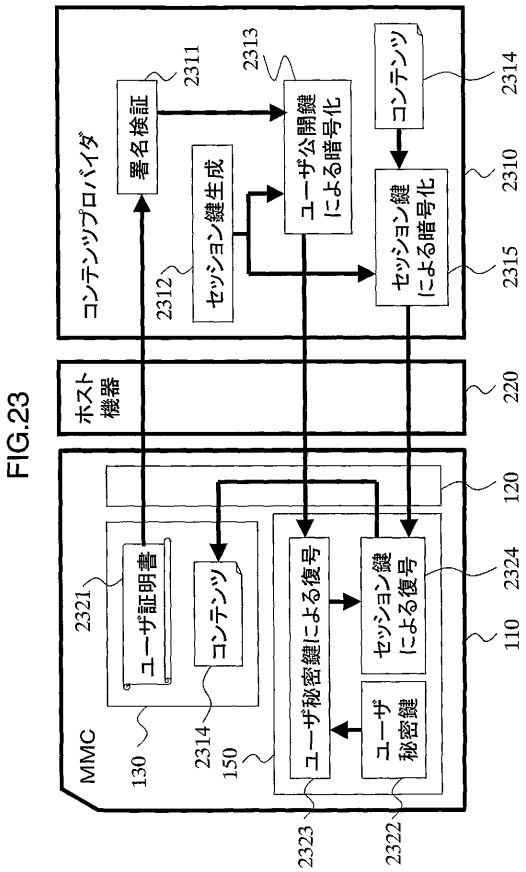


【図２２】

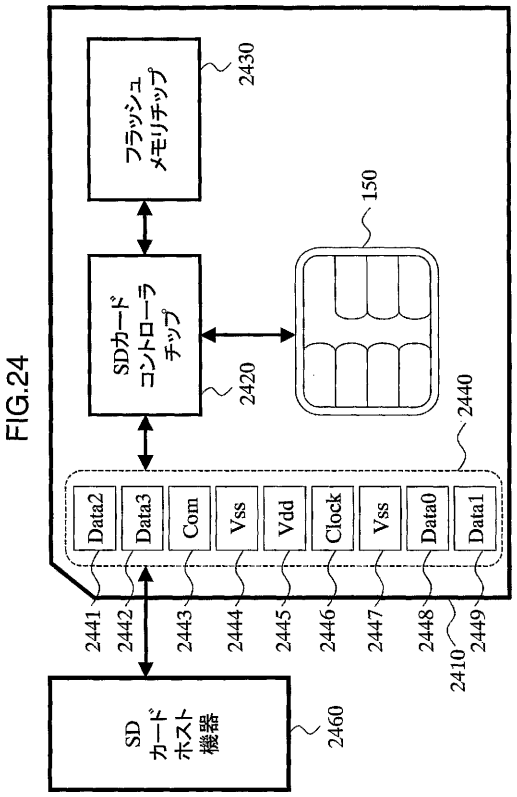
FIG.22



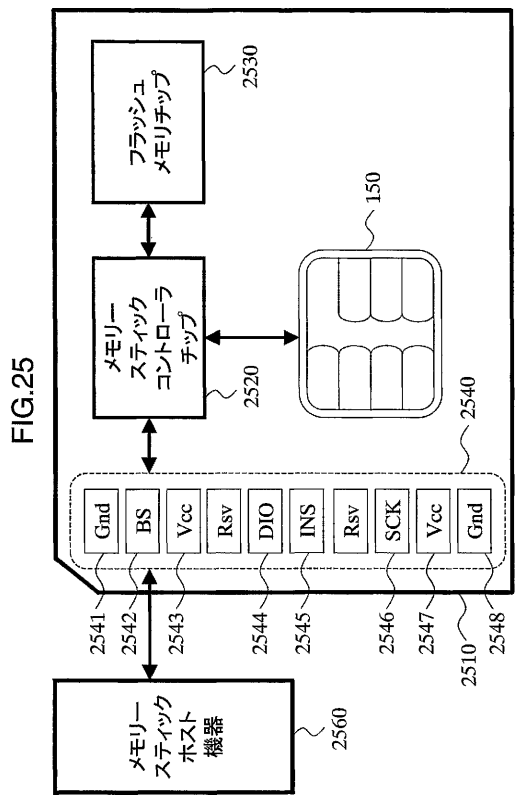
【図２３】



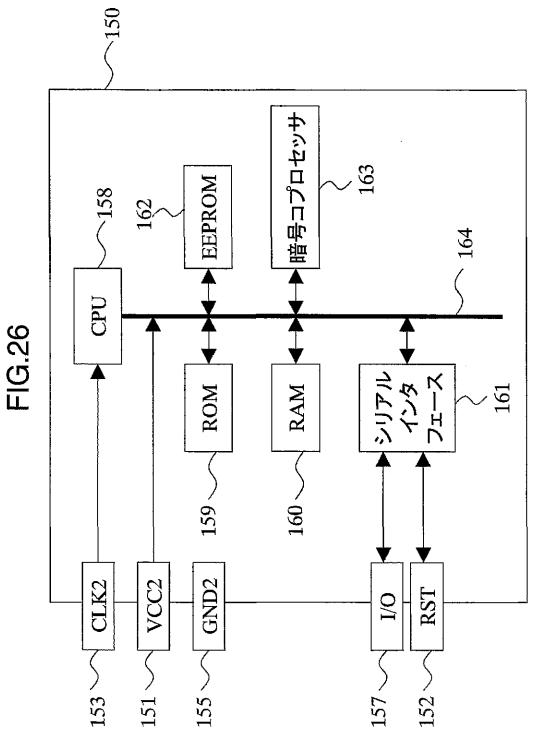
【図２４】



【図２５】

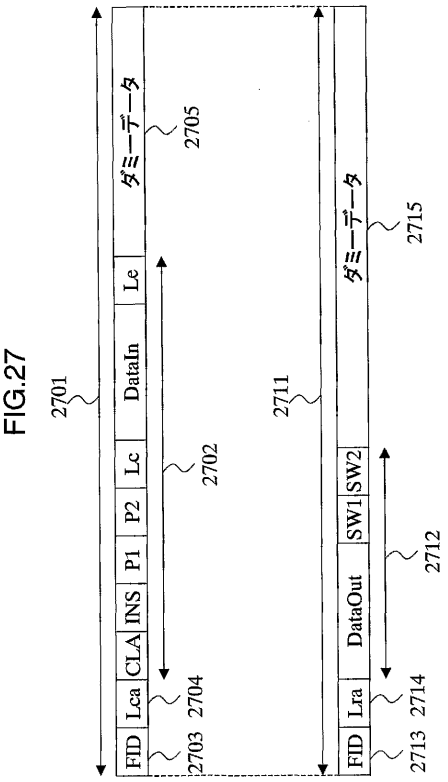


【図２６】



【図２７】

FIG.27


2701
FID
Lca
CLA
INS
P1
P2
Lc
DataIn
Le
ダミーデータ
2703
2704
2702
2705
2711
FID
Lra
DataOut
SW1
SW2
ダミーデータ
2713
2714
2712
2715

フロントページの続き

(72)発明者　角田　元泰
日本国神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　田中　紀夫
日本国神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所金融システム事業部内
(72)発明者　片山　国弘
日本国東京都小平市上水本町五丁目２０番１号　株式会社日立製作所半導体グループ内
(72)発明者　木村　光一
日本国神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　幡野　富久
日本国神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

審査官　日下　善之

(56)参考文献　特開平０９－０５４７１０（ＪＰ，Ａ）
特開平０７－２８２１６３（ＪＰ，Ａ）
特開平０６－１３１５１７（ＪＰ，Ａ）
特開平１１－０３１０６６（ＪＰ，Ａ）
特開２００１－０７７８０５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06K　19/073
G06K　19/10