(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-9933
(P2008-9933A)
(43)公開日　平成20年1月17日(2008.1.17)

(51)Int.Cl.		FI			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	540A	5B017
G06K 19/07	(2006.01)	G06K	19/00	N	5B035

審査請求 未請求　請求項の数 5　ＯＬ　（全 9 頁）

(21)出願番号　特願2006-182436 (P2006-182436)
(22)出願日　平成18年6月30日 (2006.6.30)

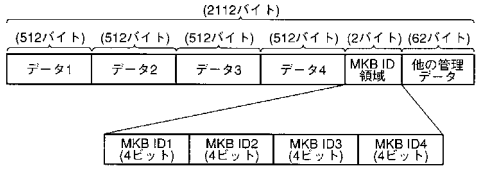
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(71)出願人　598010562
東芝エルエスアイシステムサポート株式会社
神奈川県川崎市幸区堀川町５８０番地
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊

最終頁に続く

(54)【発明の名称】記憶装置とその制御方法

(57)【要約】
【課題】セキュア領域に記憶するデータに対応する識別データを１ページ内の特定の領域において集中管理することにより、記憶領域を削減することが可能な記憶装置とその制御方法を提供する。
【解決手段】記憶装置は、セキュア領域の１ページに、複数のデータ１－４を記憶するとともに、１ページの特定の位置に、複数のデータ１－４にそれぞれ対応し、各データを暗号化するためのキーデータを識別するための複数の識別データＭＫＢ　ＩＤ１－４を記憶する記憶部を有している。
【選択図】　図１

図１



【特許請求の範囲】
【請求項１】
セキュア領域の１ページに、複数のデータを記憶するとともに、前記１ページの特定の位置に、前記複数のデータにそれぞれ対応し、各データを暗号化するためのキーデータを識別するための複数の識別データを記憶する記憶部を有することを特徴とする記憶装置。
【請求項２】
複数のデータを記憶するセキュア領域を有し、前記セキュア領域は複数のページにより構成された記憶部と、
前記セキュア領域の１ページに、複数のデータを記憶させるとともに、前記１ページの特定の位置に、前記複数のデータにそれぞれ対応し、各データを暗号化するためのキーデータを識別するための複数の識別データを記憶させるコントローラと
を具備することを特徴とする記憶装置。
【請求項３】
前記コントローラは、前記１ページにデータを追記するとともに、前記識別データを追記することを特徴とする請求項２記載の記憶装置。
【請求項４】
複数のデータをセキュア領域の１ページに記憶させ、
前記１ページの特定の位置に、前記複数のデータにそれぞれ対応し、各データを暗号化するためのキーデータを識別する複数の識別データを記憶させる
ことを特徴とする記憶装置の制御方法。
【請求項５】
前記キーデータはＭＫＢ（Media Key Block）であり、前記識別データは、ＭＫＢを識別するための識別データであることを特徴とする請求項１乃至３記載の記憶装置又は請求項４記載の記憶装置の制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えばＮＡＮＤ型フラッシュメモリを有するメモリカードのような記憶装置に係わり、特に、暗号化されたデータを扱う記憶装置とその制御方法に関する。
【背景技術】
【０００２】
例えばＮＡＮＤ型フラッシュメモリを用いたメモリカードにおいて、ホストデバイス（以下、単にホストと称す）とメモリカードとの間で暗号化されたデータを扱い、高度な秘匿性を保持する技術が開発されている。この場合、メモリカード内にＭＫＢ（Media Key Block）と称するデータが記憶されている。ホストがこのメモリカードをアクセスする場合、このＭＫＢにより、アクセスが制御される。また、１つのメモリカードには、複数のＭＫＢが記憶されており、これらＭＫＢを識別する識別データ（以下、ＭＫＢ ＩＤと称す）が使用される。
【０００３】
ホストがメモリカードにデータを書き込む場合、一般に、５１２バイト毎にデータがメモリカードに転送される。メモリカードのセキュア領域にデータを書き込む場合も同様であり、暗号化された５１２バイト毎のデータがメモリカードに転送される。セキュア領域に対するアクセスは、ＭＫＢにより制御されるため、５１２バイトのデータを書き込む毎に前記ＭＫＢ ＩＤが割り当てられ、このＭＫＢ ＩＤに対応するＭＫＢがメモリカードからホストに転送される。このＭＫＢに基づき所定の処理が行なわれてキーが生成され、このキーを用いてデータが暗号化されてメモリカードに転送される。メモリカードに転送されたデータとそのデータに対するＭＫＢ ＩＤは、ＮＡＮＤ型フラッシュメモリのセキュア領域内で管理される。
【０００４】
従来、ＭＫＢ ＩＤをＮＡＮＤ型フラッシュメモリに書き込む場合、５１２バイトのデ

ータ毎に１バイトの領域を付加し、この１バイトの領域にＭＫＤ　ＩＤを書き込んでいる。すなわち、ＮＡＮＤ型フラッシュメモリの１ページ内に５１２バイトのデータと１バイトのＭＫＢ　ＩＤの対が４つ書き込まれることとなる。つまり、データとＭＫＢ　ＩＤが交互に記憶されている。

【０００５】

また、ＭＫＢ　ＩＤは、０～１５のうちの１つのデータであるため、４ビットにより構成される。このため、ＭＫＢ　ＩＤを記憶するためには、４ビットで十分であり、１バイトの領域のうち４ビットを無駄に使用していた。

【０００６】

尚、低コストの記録媒体を用いて、記録媒体とこの記録媒体に複製コンテンツを記録する記録装置との間において、高い秘匿性を実現することが可能な技術が開発されている（例えば特許文献１参照）。

【特許文献１】特開２０００－３５７２１３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

本発明は、セキュア領域に記憶するデータに対応する識別データを１ページ内の特定の領域において集中管理することにより、記憶領域を削減することが可能な記憶装置とその制御方法を提供しようとするものである。

【課題を解決するための手段】

【０００８】

本発明の記憶装置の第１の態様は、セキュア領域の１ページに、複数のデータを記憶するとともに、前記１ページの特定の位置に、前記複数のデータにそれぞれ対応し、各データを暗号化するためのキーデータを識別するための複数の識別データを記憶する記憶部を有することを特徴とする。

【０００９】

本発明の記憶装置の第２の態様は、複数のデータを記憶するセキュア領域を有し、前記セキュア領域は複数のページにより構成された記憶部と、前記セキュア領域の１ページに、複数のデータを記憶させるとともに、前記１ページの特定の位置に、前記複数のデータにそれぞれ対応し、各データを暗号化するためのキーデータを識別するための複数の識別データを記憶させるコントローラとを具備することを特徴とする。

【００１０】

本発明の記憶装置の制御方法の態様は、複数のデータをセキュア領域の１ページに記憶させ、前記１ページの特定の位置に、前記複数のデータにそれぞれ対応し、各データを暗号化するためのキーデータを識別する複数の識別データを記憶させることを特徴とする。

【発明の効果】

【００１１】

本発明によれば、セキュア領域に記憶するデータに対応する識別データを１ページ内の特定の領域において集中管理することにより、記憶領域を削減することが可能な記憶装置とその制御方法を提供できる。

【発明を実施するための最良の形態】

【００１２】

以下、本発明の実施の形態について、図面を参照して説明する。

【００１３】

図２は、本実施形態が適用される記憶装置、例えばメモリカードの一例を示している。図２において、ホスト機器（以下、ホストと称す）１０は、接続されるメモリカードをアクセスするためのハードウェア及びソフトウェア（システム）を備えている。このホスト１０は、メモリカード１に対して、データの読み出し、データの書き込み、データの消去等のアクセスを行なう。

【００１４】

メモリカード１は、ホスト１０に接続されたとき、電源が供給されて動作し、ホスト１０からのアクセスに応じた処理を行う。例えば、データの読み出し、データの書き込み、データの消去等のアクセスにおいて、メモリカード１は、物理アドレスと論理アドレスのマッピング、ＥＣＣエラー訂正、ＮＡＮＤ型フラッシュメモリへのアクセス、ＮＡＮＤ型フラッシュメモリのセキュア領域のデータに対する暗号化又は複合化処理などを行なう。

【００１５】

コントローラ３は、メモリインタフェース部（メモリＩ／Ｆ）４、ホストインタフェース部（ホストＩ／Ｆ）５、バッファ６、ＣＰＵ７、ＲＯＭ（Read Only Memory）８、及びＲＡＭ（Random Access Memory）９を有している。

【００１６】

メモリインタフェース部４は、コントローラ３とＮＡＮＤ型フラッシュメモリ２との間のインタフェース処理を行う。ホストインタフェース部５は、コントローラ３とホスト１０との間のインタフェース処理を行う。

【００１７】

バッファ６は、ホスト１０から送られてくるデータをＮＡＮＤ型フラッシュメモリ２へ書き込む際に、一定量（例えば１ページ分）のデータを一時的に記憶したり、ＮＡＮＤ型フラッシュメモリ２から読み出されるデータをホスト１０へ送り出す際に、一定量のデータを一時的に記憶したりする。

【００１８】

ＲＯＭ８は、ＣＰＵ７により使用される制御プログラムなどを格納するメモリである。ＲＡＭ９は、ＣＰＵ７の作業エリアとして使用され、各種のテーブル等を記憶する揮発性メモリである。

【００１９】

ＣＰＵ７は、メモリカード１全体の動作を司るものである。このＣＰＵ７は、例えばメモリカード１に電源が供給された場合、ＲＯＭ８に格納されているファームウェア(制御プログラム)に従って処理を開始する。すなわち、ＣＰＵ７は、処理に必要な各種テーブル（管理データ）をＲＡＭ９上に作成したり、ホスト１０からの書き込みコマンド、読み出しコマンド、消去コマンドを受けてＮＡＮＤ型フラッシュメモリ２上の該当領域をアクセスしたり、ＮＡＮＤ型フラッシュメモリ２をアクセスするにあたってホストからの論理アドレスと物理アドレスとを変換したり、バッファ６を介してデータ転送処理を制御したりする。

【００２０】

図３は、ＮＡＮＤ型フラッシュメモリ２を概略的に示している。ＮＡＮＤ型フラッシュメモリ２は、消去時のブロックサイズ（消去ブロックサイズ）が例えば２５６ｋバイトに定められ、１ページが例えば２１１２バイト（例えば５１２バイト分のデータ×４＋１０バイト分の冗長部×４＋２４バイト分の管理情報）で構成されている。したがって、１ブロックは例えば１２８ページにより構成されている。データの書き込み、読み出しはページ単位で行なわれる。

【００２１】

ＮＡＮＤ型フラッシュメモリ２は通常のデータ領域、システム領域とセキュア領域とを有している。システム領域には、例えばメディア固有のＩＤ（ＭＩＤ）や１６個のＭＫＢなどが記憶されている。セキュア領域には秘匿すべきデータ及びＭＫＢ ＩＤなどが記憶される。通常のデータ領域、システム領域及びセキュア領域とも、ブロックが満杯となった場合、空きブロックが割り当てられ、この空きブロックにデータが転送される。旧ブロックは、所定のタイミングで消去され、空きブロックとされる。

【００２２】

図１は、本実施形態に係るＮＡＮＤ型フラッシュメモリ２に記憶されたセキュア領域の１ページの構成を示している。本実施形態において、セキュア領域の１ページには、４つのデータ１～４が、例えば連続して記憶されている。各データ１～４はそれぞれ５１２バイトにより構成されている。識別データとしてのＭＫＢ ＩＤ１～４は、１ページ内の特

定のアドレスに集中して記憶される。すなわち、ＭＫＢ　ＩＤ１～４は、２バイト、１６ビットにより構成されたＭＫＢ　ＩＤ領域に記憶される。このＭＫＢ　ＩＤ領域において、各４ビットのＭＫＢ　ＩＤ１～４がデータ１～４に対応して記憶される。また、１ページ内の残りの領域には、他の管理データが記憶される。

【００２３】

図４は、メモリカード１のセキュア領域をアクセスする場合におけるホスト１０とメモリカード１の動作を示すものであり、例えば書き込み動作について示している。

【００２４】

前述したように、ホスト１０がメモリカード１のセキュア領域をアクセスする場合、ＭＫＢのデータを必要とする。このため、ホスト１０は、先ず、ＭＫＢの取得コマンドをメモリカードに転送する（Ｓ１１）。ＭＫＢの取得コマンドは、例えば４８ビットにより構成される。コマンドフォーマットは、次のようである。スタート・ビット（１ビット）＋トランスミッション・ビット（コマンドかレスポンスかを示す）（１ビット）＋コマンド・インデックス（コマンド番号を示す）（６ビット）＋アーギュメント（引き数を示す）（３２ビット）＋ＣＲＣ７（巡回冗長検査コードを示す）（７ビット）＋エンド・ビット（１ビット）。ＭＫＢ　ＩＤは、例えばアーギュメント（３２ビット）のうちの８ビットを用いて指定される。ＭＫＢ　ＩＤは前述したように、例えば“０”～“１５”のデータであり、４ビットにより構成されている。ＭＫＢの取得コマンドには、１６個のＭＫＢ　ＩＤのうちの１つが指定される。

【００２５】

メモリカード１において、転送されてきたＭＫＢ　ＩＤは、コントローラ３の例えばＲＡＭ９に記憶される。コントローラ３は、送られてきたＭＫＢ　ＩＤに対応するＭＫＢデータ（例えば最大６４ｋバイトのデータ）をＮＡＮＤ型フラッシュメモリ２のシステム領域から読み出し、ホスト１０に転送する（Ｓ１２）。

【００２６】

ホスト１０は、このＭＫＢとホスト１０が有するデバイスキーとを用いてメディアキーを生成する（Ｓ１３）。次に、ホスト１０より、メディア固有のＩＤ（ＭＩＤ）を取得するためのコマンドがメモリカード１に転送される（Ｓ１４）。

【００２７】

メモリカード１はこのコマンドに応じて、例えば８バイトのＭＩＤデータをホスト１０に転送する（Ｓ１５）。ホスト１０は、このＭＩＤと前記メディアキーとからメディアユニークキーＫｍｕを生成する（Ｓ１６）。

【００２８】

この後、ホスト１０とメモリカード１との間において、メディアユニークキーＫｍｕを使用して、チャレンジ・アンド・レスポンス・プロトコルに基づき認証処理が実行される（Ｓ１７）。

【００２９】

この認証処理が正常に終了した場合、ホスト１０は、メディアユニークキーＫｍｕと認証処理においてメモリカード１から得たデータに基づきタイトルキーを生成する（Ｓ１８）。このとき、メモリカード１においても、同様にして、ホスト１０と共通のタイトルキーが生成される。ホスト１０は、このタイトルキーに基づき転送すべきデータを暗号化する（Ｓ１９）。この暗号化されたデータは、ホスト１０からメモリカード１に転送される（Ｓ２０）。

【００３０】

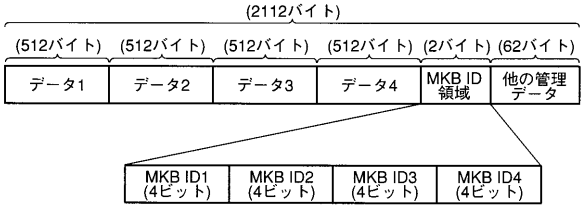
メモリカード１のコントローラ３は、転送されてきたデータをメモリカード１内で生成されたタイトルキーに基づき複合化し、この複合化されたデータと、予め送られてきたこのデータに対応する前記ＭＫＢ　ＩＤとをＮＡＮＤ型フラッシュメモリ２に書き込む（Ｓ２１）。すなわち、コントローラ３は、複合化されたデータをセキュア領域の１ページ内の空き領域に書き込むとともに、ＭＫＢ　ＩＤを同じ１ページ内のＭＫＢ　ＩＤ領域に書き込む。

【００３１】
図５は、ＮＡＮＤ型フラッシュメモリ２の書き込み動作を示している。コントローラ３は、複合化されたデータをＮＡＮＤ型フラッシュメモリ２の例えばセキュア領域ＳＲ１内の１ページの空き領域に書き込む。これとともに、ＭＫＢ ＩＤの取得コマンドにより送られてきた４ビットのＭＫＢ ＩＤをＭＫＢ ＩＤ領域の対応する領域に書き込む。すなわち、例えばデータ１を書き込む際のＭＫＢ ＩＤが“１”である場合、１ページ内の空き領域にデータ１が書き込まれ、ＭＫＢ ＩＤ＝“１”が、ＭＫＢ ＩＤ領域の対応箇所に書き込まれる。
【００３２】
次に、例えばホスト１０のセキュア領域に記憶されたデータ２とＭＫＤ ＩＤ＝“２”を書き込む場合、図４に示す動作が実行され、メモリカード１のコントローラ３は、転送されてきたデータ２をＮＡＮＤ型フラッシュメモリ２のセキュア領域ＳＲ１の１ページ内の空き領域に書き込む。これとともに、ＭＫＢ ＩＤ領域の対応箇所にＭＫＤ ＩＤ＝“２”を書き込む。この書き込み動作は、通常の追記書き込みと同様である。すなわち、例えば先ず、書き込まれたデータ１、ＭＫＢ ＩＤ＝“１”を読み出し、このデータ１、ＭＫＢ ＩＤ＝“１”と追記されるデータ２、ＭＫＢ ＩＤ＝“２”をセキュア領域ＳＲ１内の別の空きページに書き込む。このような動作が書き込みデータに従って順次行なわれる。
【００３３】
また、上記のようにして書き込まれたデータを読み出す場合、図４に示すステップＳ１１～Ｓ１８のような動作により、メモリカード１とホスト１０において共通のタイトルキーが生成される。この後、例えばデータ１を読み出す場合、読み出し時にステップＳ１１のようにして、ホスト１０からメモリカード１に供給されたＭＫＢ ＩＤ＝“１”に対応するデータ１が読み出される。この読み出されたデータは、タイトルキーにより暗号化され、ホストに転送される。
【００３４】
また、メモリカード１に記憶されたデータ１を読み出す際、ホスト１０からＭＫＤ ＩＤ＝“２”がメモリカード１に供給された場合、メモリカード１のデータ１に対応してＭＫＢ ＩＤ領域に記憶されたＭＫＢ ＩＤ＝“１”と不一致となる。この場合、メモリカード１からオール“１”のデータがホスト１０に転送され、不正アクセスからデータが保護される。
【００３５】
上記実施形態によれば、ＮＡＮＤ型フラッシュメモリ２のセキュア領域の１ページに記憶される複数のデータに対して、これらデータに対応する複数のＭＫＢ ＩＤを１つのＭＫＢ ＩＤ領域に集中して記憶している。しかも、このＭＫＢ ＩＤ領域に記憶される各ＭＫＢ ＩＤは、１６個のＭＫＢ ＩＤを記憶するに必要な４ビットにより構成されている。このため、ＭＫＢ ＩＤ領域を従来に比べて削減することができる。
【００３６】
尚、上記実施形態は、本発明を記憶装置としてのメモリカードに適用した場合を示した。しかし、メモリカードに限定されるものではなく、この種の暗号化されたデータを扱う装置に適用可能なことは言うまでもない。
【００３７】
また、図１において、複数のデータ１－４は、１ページ内において連続して記憶しているが、これに限定されるものではなく、データとデータの間に他の管理データを記憶することも可能である。
【００３８】
その他、本発明は、上記実施形態に限定されるものではなく、発明の要旨を変えない範囲において種々変形実施可能なことは勿論である。
【図面の簡単な説明】
【００３９】
【図１】本実施形態に係る１ページ内におけるデータとＭＫＢ ＩＤの配置の関係を示す

図。
【図２】本実施形態に適用されるメモリカードとホストを概略的に示す図。
【図３】本実施形態に適用されるメモリカードの構成を概略的に示す図。
【図４】本実施形態に係るデータの書き込み動作を概略的に示すフローチャート。
【図５】本実施形態に係るデータの書き込み動作を示すものであり、１ページ内に記憶されるデータとＭＫＢ　ＩＤの関係を概略的に示す図。
【符号の説明】
【００４０】
１…メモリカード、２…ＮＡＮＤ型フラッシュメモリ、３…コントローラ、１０…ホスト、データ１～４…暗号化されたデータ、ＭＫＢ　ＩＤ１～４…識別データ。

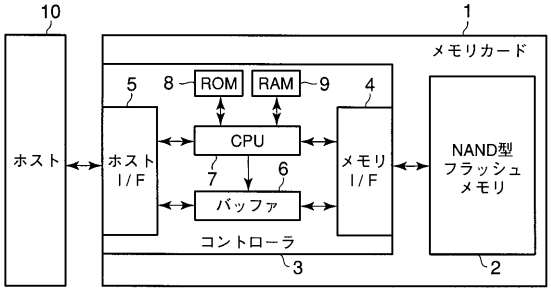
【図１】

図１



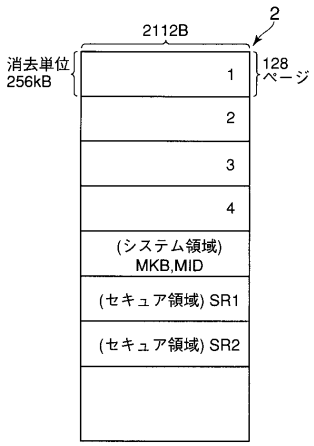
【図２】

図２



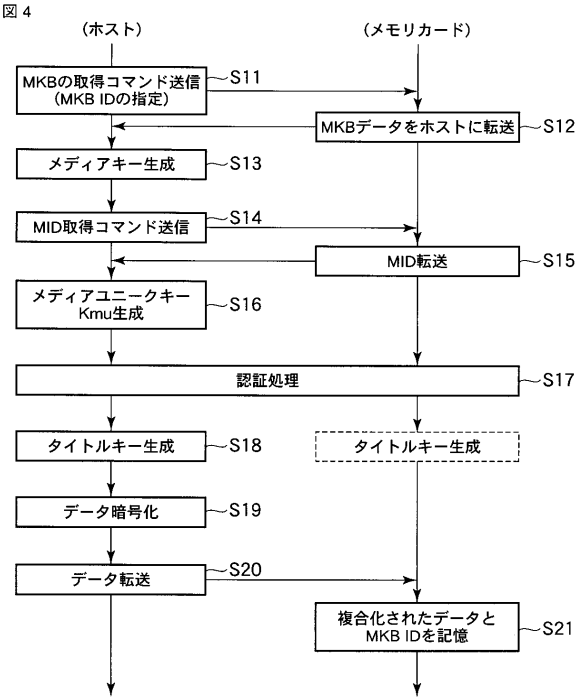
【図３】

図３



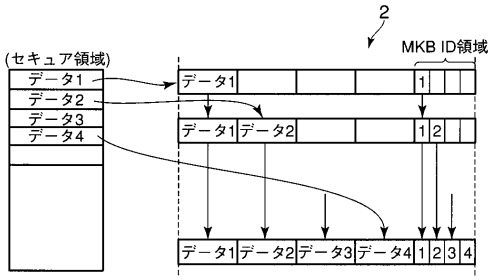
【図４】

図４


（ホスト）
（メモリカード）
MKBの取得コマンド送信
（MKB IDの指定）
S11
MKBデータをホストに転送
S12
メディアキー生成
S13
MID取得コマンド送信
S14
MID転送
S15
メディアユニークキー
Kmu生成
S16
認証処理
S17
タイトルキー生成
S18
タイトルキー生成
データ暗号化
S19
データ転送
S20
複合化されたデータと
MKB IDを記憶
S21

【図５】

図５


2
MKB ID領域
（セキュア領域）
データ1
データ2
データ3
データ4
データ1
データ1
データ2
データ1
データ2
データ3
データ4
1
1
2
1
2
3
4

フロントページの続き

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 中里 康明
神奈川県川崎市幸区堀川町５８０番地 東芝エルエスアイシステムサポート株式会社内

Ｆターム(参考) 5B017 AA03 BA07 CA14
5B035 AA00 BB09 BB11 CA11 CA29