(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号

特許第5112555号
(P5112555)

(45)発行日　平成25年1月9日(2013.1.9)　(24)登録日　平成24年10月19日(2012.10.19)

(51)Int.Cl.		F I		
G06F 12/14	(2006.01)	G06F	12/14	510A
G06F 21/10	(2013.01)	G06F	21/22	110L
G06F 21/62	(2013.01)	G06F	21/24	166C
H04L 9/08	(2006.01)	H04L	9/00	601C
H04L 9/32	(2006.01)	H04L	9/00	675A

請求項の数 14　(全 62 頁)　最終頁に続く

(21)出願番号　特願2011-265306 (P2011-265306)
(22)出願日　平成23年12月2日 (2011.12.2)
審査請求日　平成24年8月23日 (2012.8.23)

早期審査対象出願

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100159651
弁理士　高倉　成男
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】メモリカード、ストレージメディア、及びコントローラ

(57)【特許請求の範囲】
【請求項１】
エラー訂正機能を有したコントローラと、
前記コントローラによりコントロールされるメモリ装置と、
を備え、
前記メモリ装置は、認証処理に用いられるデータが格納されて外部からリードが制限される第１領域と、キーインデックスデータと暗号化された前記メモリ装置ユニークなシークレットデータ（E-SecretID）とが格納されてリードオンリーとされる第２領域と、ファミリーキーブロックデータ（FKB）が格納されてリーダブル及びライタブルとされる第３領域と、を有し、
前記コントローラは、
ホスト装置からの前記ファミリーキーブロックデータのリードコマンドを受けた場合、前記第３領域から前記ファミリーキーブロックデータをリードするとともに該ファミリーキーブロックデータを前記ホスト装置に送り、
前記ホスト装置からの前記暗号化されたメモリ装置ユニークなシークレットデータのリードコマンドを受けた場合、前記第２領域から前記暗号化されたメモリ装置ユニークなシークレットデータをリードするとともに該暗号化されたメモリ装置ユニークなシークレットデータを前記ホスト装置に送り、
前記ホスト装置からの前記キーインデックスデータのリードコマンドを受けた場合、前記第２領域から前記キーインデックスデータをリードするとともに該キーインデックスデ

ータを前記ホスト装置に送り、
前記ホスト装置からの認証情報データを得るためのコマンドを受けた場合、前記ホスト装置から受けた乱数データ（RN）を含む数値データを前記メモリ装置に送り、
前記メモリ装置は、前記乱数データを含む数値データを参照して認証情報データ（Ｏｎｅｗａｙ－ＩＤ）を計算し、
前記コントローラは、前記メモリ装置での前記認証情報データの計算後、前記メモリ装置から前記認証情報データをリードし、前記ホスト装置に送る
ことを特徴とするメモリカード。
【請求項２】
請求項１の記載において、
前記第１領域には、複数の前記認証処理に用いられるデータが格納され、該複数のデータは１つのスロットとして組み合わされおり、前記キーインデックスデータには、前記スロットと対応したインデックスデータが含まれるメモリカード。
【請求項３】
請求項２の記載において、
前記乱数データを含む数値データには、前記スロットと対応するスロット番号が含まれるメモリカード。
【請求項４】
請求項３の記載において、
前記コントローラは、前記ホスト装置からの前記ファミリーキーブロックデータのリードコマンドを受けた場合、前記ホスト装置から受けた前記スロット番号を参照し、前記第３領域から前記ファミリーキーブロックデータをリードするメモリカード。
【請求項５】
請求項１又は請求項４の何れかの記載において、
前記乱数データを含む前記数値データには、定数データ（HC）が含まれ、該定数データは、前記認証処理に用いられるデータとともに前記メモリ装置での認証情報データの生成に用いられるメモリカード。
【請求項６】
請求項１又は請求項５の何れかの記載において、
前記ファミリーキーブロックデータと、前記キーインデックスデータ及び前記暗号化された前記メモリ装置ユニークなシークレットデータとは、前記メモリカード出荷前に、其々異なる業者により記録されるメモリカード。
【請求項７】
請求項１又は請求項６の記載において、
前記ファミリーキーブロックデータは、前記メモリカード出荷前に、該メモリカードの製造者により記録されるメモリカード。
【請求項８】
請求項１又は請求項７の記載において、
前記キーインデックスデータと、前記暗号化された前記メモリ装置ユニークなシークレットデータとは、前記メモリ装置出荷前に、該メモリ装置の製造者により記録されるメモリカード。
【請求項９】
請求項１又は請求項７の記載において、
前記第１領域は、出荷後に外部からの前記コントローラを介したリードが禁止されるメモリカード。
【請求項１０】
コントローラと、
前記コントローラによりコントロールされるとともに、外部からリード不可能なシークレットデータと、外部からリード可能な暗号化シークレットデータとが格納されたメモリ装置と、

を備え、
前記コントローラは、
前記ホスト装置からの前記暗号化シークレットデータのリードコマンドを受けた場合、前記メモリ装置から前記暗号化シークレットデータをリードするとともに該前記暗号化シークレットデータを前記ホスト装置に送り、
前記ホスト装置からの認証情報データを得るためのコマンドを受けた場合、前記ホスト装置から受けた数値データを前記メモリ装置に送り、前記メモリ装置での前記認証情報データが計算された後、前記メモリ装置から前記認証情報データをリードするとともに該認証情報データをホスト装置に送るストレージメディア。
【請求項１１】
請求項１０の記載において、
前記外部からリード不可能なシークレットデータには、第１キーデータ（NKey）と固有のシークレットデータ（SecretID）とが含まれ、
前記メモリ装置は、
前記第１キーデータを第１領域からリードし、
前記第１キーデータに基づき暗号化処理を行うことにより、セッションキーデータ（SKey）を生成し、
前記セッションキーデータと、前記第１領域からリードされた前記シークレットデータとを用いて一方向性変換処理を行うことにより、認証情報データ（Oneway-ID）を計算するストレージメディア。
【請求項１２】
請求項１１の記載において、
前記メモリ装置は、
前記第１キーデータと、前記ホスト装置から受けた定数データ（HC）とを用いてAES（Advanced Encryption Standard）暗号化処理を行うことにより、第２キーデータ（HKey）を生成し、
前記第２キーデータと、前記ホスト装置から受けた第２数値データ（RN）とを用いてAES暗号化処理を行うことにより、セッションキーデータ（SKey）を生成するストレージメディア。
【請求項１３】
請求項１２の記載において、
第３領域には、前記シークレットデータを暗号化する際に用いられるファミリーキーデータ（FKey）を暗号化して生成された暗号化ファミリーキーデータが、前記ファミリーキーブロックデータ（FKB）に含まれた状態で格納された
ストレージメディア。
【請求項１４】
エラー訂正機能を有したコントローラであって、
外部のホスト装置からファミリーキーブロックデータのリードコマンドを受けた場合、コントロール可能な外部のメモリ装置におけるリーダブル及びライタブルな領域から前記ファミリーキーブロックデータをリードするとともに該ファミリーキーブロックデータを前記ホスト装置に送り、
前記ホスト装置から暗号化された前記メモリ装置にユニークなシークレットデータのリードコマンドを受けた場合、前記メモリ装置におけるリードオンリーの領域から前記暗号化された前記メモリ装置にユニークなシークレットデータをリードするとともに該暗号化された前記メモリ装置にユニークなシークレットデータを前記ホスト装置に送り、
前記ホスト装置からキーインデックスデータのリードコマンドを受けた場合、前記リードオンリーとされる領域から前記キーインデックスデータをリードするとともに該キーインデックスデータを前記ホスト装置に送り、
前記ホスト装置からの認証情報データを得るためのコマンドを受けた場合、前記ホスト装置から受けた乱数データを含む数値データを前記メモリ装置に送り、

前記乱数データを含む数値データを用いて前記メモリ装置で生成された前記認証情報データを、前記メモリ装置からリードし、前記ホスト装置に送る
ことを特徴とするコントローラ。

【発明の詳細な説明】
【技術分野】
【０００１】
半導体記憶装置に関するものである。
【背景技術】
【０００２】
一般に、情報セキュリティを要する分野において、自己の正当性を証明する手段として互いに共有した秘密情報と暗号器とを用いた手法が採られている。
【０００３】
例えば、電子決済に用いるICカード（Smart Card）等では、カード内のICには当該ICカードを個別化するためのID及び秘密情報が保持されている。更にICカードは、ID及び秘密情報に基づく認証を行うための暗号処理機能を有している。
【０００４】
別の例では、コンテンツの著作権保護技術において、SD（登録商標）カードの正当性を証明するために、Content Protection for Recordable Media（CPRM）と呼ばれる認証方式が規定されている。
【先行技術文献】
【特許文献】
【０００５】
【非特許文献１】Content Protection for Recordable Media (CPRM), http://www.4centity.com/
【非特許文献２】Media Identifier Management Technology (MIMT), http://www.4ecntity.com/
【非特許文献３】D. Naor, M. Naor and J. Lotspiech, “Revocation and Tracing Schemes for Stateless Receivers,” Proc. CRYPTO 2001, LNCS 2139, Springer-Verlag, pp. 41-62, 2001
【発明の概要】
【発明が解決しようとする課題】
【０００６】
秘密情報の不正利用を防止することが可能なメモリカード、ストレージメディア、及びコントローラを提供する。
【課題を解決するための手段】
【０００７】
実施形態のメモリカードによれば、エラー訂正機能を有したコントローラと、前記コントローラによりコントロールされるメモリ装置と、を備え、前記メモリ装置は、認証処理に用いられるデータが格納されて外部からリードが制限される第１領域と、キーインデックスデータと暗号化された前記メモリ装置ユニークなシークレットデータ（E-SecretID）とが格納されてリードオンリーとされる第２領域と、ファミリーキーブロックデータ（FKB）が格納されてリーダブル及びライタブルとされる第３領域と、を有し、前記コントローラは、ホスト装置からの前記ファミリーキーブロックデータのリードコマンドを受けた場合、前記第３領域から前記ファミリーキーブロックデータをリードするとともに該ファミリーキーブロックデータを前記ホスト装置に送り、前記ホスト装置からの前記暗号化されたメモリ装置ユニークなシークレットデータのリードコマンドを受けた場合、前記第２領域から前記暗号化されたメモリ装置ユニークなシークレットデータをリードするとともに該暗号化されたメモリ装置ユニークなシークレットデータを前記ホスト装置に送り、前記ホスト装置からの前記キーインデックスデータのリードコマンドを受けた場合、前記第２領域から前記キーインデックスデータをリードするとともに該キーインデックスデータ

を前記ホスト装置に送り、前記ホスト装置からの認証情報データを得るためのコマンドを受けた場合、前記ホスト装置から受けた乱数データ（RN）を含む数値データを前記メモリ装置に送り、前記メモリ装置は、前記乱数データを含む数値データを参照して認証情報データ（Ｏｎｅｗａｙ－ＩＤ）を計算し、前記コントローラは、前記メモリ装置での前記認証情報データの計算後、前記メモリ装置から前記認証情報データをリードし、前記ホスト装置に送る。

【図面の簡単な説明】

【０００８】

【図１】第１の実施形態に係るメモリシステムの構成例を示すブロック図。

【図２】第１の実施形態に係るメモリシステムの認証フローを示すフロー図。

【図３】第１の実施形態に係る暗号化FKey束（FKB）の構成例を示す図。

【図４】第１の実施形態に係るメモリシステムの構成例を示すブロック図。

【図５】第１の実施形態に係るＮＡＮＤ製造者による秘密情報の書き込み処理を例示する図。

【図６】図５の処理を示すフロー図。

【図７】第１の実施形態に係るカード製造者によるFKBの書き込み処理を例示する図。

【図８】図７の処理を示すフロー図。

【図９】変形例１に係る被認証装置を示す図。

【図１０】変形例１に係るFKBをダウンロードするシステムを示すブロック図。

【図１１】変形例１に係るFKBをダウンロードするフローを示すフロー図。

【図１２】第２の実施形態に係るメモリシステムの構成例を示すブロック図。

【図１３】第３の実施形態に係るメモリシステムの構成例を示すブロック図。

【図１４】第３の実施形態に係るメモリシステムの認証フローを示すフロー図。

【図１５】第４の実施形態に係るメモリシステムの構成例を示すブロック図。

【図１６】第４の実施形態に係るメモリシステムの認証フローを示すフロー図。

【図１７】第３、第４の実施形態に係る機能制御の構成例を示すブロック図。

【図１８】第５の実施形態に係るＮＡＮＤチップの全体構成例を示すブロック図。

【図１９】図１８中のＮＡＮＤ型チップの一ブロックの構成例を示す等価回路図。

【図２０】第５の実施形態に係るセルアレイの構成例を示すブロック図。

【図２１】第５の実施形態に係るロムブロックの読み出し専用データを示す図。

【図２２】ＥＣＣの構成例１を示すブロック図。

【図２３】ＥＣＣの構成例２を示すブロック図。

【図２４】ＥＣＣの構成例３を示すブロック図。

【図２５】ＥＣＣの構成例４を示すブロック図。

【図２６】第５の実施形態に係る秘匿ブロック内の秘匿データを示す図。

【図２７】第５の実施形態に係るアクセス制御パターンの例を示す図。

【図２８】第５の実施形態に係るアクセス制御パターンの利用例を示すブロック図。

【図２９】第５の実施形態に係るテストフローを示す図。

【図３０】第５の実施形態に係るデータ消去フローを示す図。

【図３１】第６の実施形態に係るＮＡＮＤチップの構成例を示すブロック図。

【図３２】第６の実施形態に係るＮＡＮＤチップの演算フロー１を示す図。

【図３３】第６の実施形態に係るＮＡＮＤチップの演算フロー２を示す図。

【図３４】第６の実施形態に係るテストフローを示す図。

【図３５】第６の実施形態に係る秘匿情報の検査フローを示す図。

【図３６】第７の実施形態に係るコマンドマッピング例を示すタイミングチャート図。

【図３７】第７の実施形態に係るコマンドマッピング例（Set/Get featureコマンド）を示すタイミングチャート図。

【図３８】第８の実施形態に係るメモリカードの構成例を示す図。

【図３９】第８の実施形態に係るコンテンツ保護への応用例１を示す図。

【図４０】第８の実施形態に係るＨＤＤへの応用例１を示す図。

【図４１】第８の実施形態に係るＨＤＤへの応用例２を示す図。
【図４２】第８の実施形態に係るコンテンツ保護への応用例２を示す図。
【図４３】第８の実施形態に係るコンテンツ保護への応用例３を示す図。
【図４４】第８の実施形態に係るコンテンツ保護への応用例４を示す図。
【図４５】変形例２に係るセンスアンプおよびその周辺回路の構成例を示すブロック図。
【図４６】図４５中のセンスアンプおよびデータキャッシュの等価回路図。
【発明を実施するための形態】
【０００９】
認証処理を採用したセキュリティシステムを構築する場合には、当該認証処理を行う装置が攻撃を受けて、秘匿されている情報が抜き出されるといった事態も想定しておく必要がある。従って、抜き出された秘匿情報を無効化（Revoke）する方法が重要となる。
【００１０】
前述のCPRMや、Blu-ray Discに記録されたコンテンツを保護するために規定されている著作権保護技術であるAdvanced Access Content System（AACS）等では、秘匿情報であるデバイス鍵を無効化するために、Media Key Block（MKB）と呼ばれる技術を利用している。また、公開鍵暗号に基づくプロトコルを採用している方式では、漏洩した秘密鍵情報と対になった公開鍵証明書のリスト（Revocation List）を利用している。
【００１１】
SDカードに記録されたビデオコンテンツをPCにインストールされたソフトウェアで再生するシステムを例に挙げる。SDカード内のCPRM処理はハードウェアで実装されているため、秘匿された情報を不正に取り出すことは非常に困難である。それに比べて、ビデオ再生ソフトウェアから秘匿情報を抜き出す方が、攻撃としては容易である場合が多い。現実にも、保護されたDVDやBlu-ray Diskに記録されたコンテンツを不正に復号するソフトウェアが多く出回っている。当該不正ソフトウェアにおいては、正規のソフトウェアプレーヤから抜き出した秘匿情報が利用される。
【００１２】
加えて、正規のソフトウェアから抜き出した秘匿情報を利用してSDカードに成り済まし、正規のソフトウェアプレーヤを騙すといったカード模倣ソフトウェアや模倣カードを防ぐための対策が必要な場合もある。例えば、模倣SDカードからはコンテンツ暗号化に使われた暗号化鍵を容易に読み出せるようにしておくことで、正規の録画機器を使って模倣SDカードに録画したビデオコンテンツを、後から容易に復号できるようになる。
【００１３】
ここで、認証装置は、民生機器のような専用ハードウェア装置だけでなく、例えば、PC（パーソナルコンピュータ）等で実行可能なプログラム（ソフトウェア）として提供され、当該ソフトウェアが実質的な認証装置となる場合もある。一方、被認証装置は、例えば、記録メディア等であり、記録メディアを構成するハードウェアの動作にファームウェアと呼ばれるプログラムが介在する場合であっても、重要な処理や情報はセルアレイ中のハードウェア内に秘匿された状態で記憶される。そのため、PC上で実行されるソフトウェアが認証装置の場合では、記録メディア等の被認証装置に比べて耐タンパー性能（攻撃に対する耐性）が低くなってしまうことが懸念される。
【００１４】
そのため、耐タンパー性能の低い認証装置を攻撃することで、耐タンパー性の高い被認証装置に秘匿された秘密情報をも暴露され、耐タンパー性の高い装置に成りすまされることが懸念されている。このような状況に対応するため、秘密情報の不正利用を効率的に防止する方法が要求されている。
【００１５】
また、近年では、比較的大きな回路規模を要求される公開鍵暗号処理やMKB処理のハードウェア実装が困難である等の回路規模上の制約が同時に課せられる環境下においても、上記要求が強くなる傾向がある。従って、回路規模の増大を最小限に抑制しつつ、秘密情報の不正利用を効率的に防止する方法が要求されている。

【００１６】
以下、複数の実施形態について図面を参照して説明する。この説明においては、認証装置、被認証装置、及びその認証方法として、メモリシステムを一例に挙げるが、これに限られることはない。なお、この説明においては、全図にわたり共通の部分には共通の参照符号を付す。
【００１７】
［第１の実施形態］
第１の実施形態に係る認証装置、被認証装置、及びその認証方法について説明する。
【００１８】
＜１．構成例（メモリシステム）＞
図１を用いて、第１の実施形態に係るメモリシステムの構成例について説明する。
【００１９】
図示するように、第１の実施形態に係るメモリシステムは、被認証装置であるＮＡＮＤ型フラッシュメモリ１０、認証装置であるホスト装置２０、及び両者を仲介するコントローラ１９を備える。ホスト装置２０は、コントローラ１９を介して、ＮＡＮＤ型フラッシュメモリ１０にアクセスする。
【００２０】
ここで、ＮＡＮＤ型フラッシュメモリ１０等の半導体製品の製造工程について、簡単に説明する。半導体製品の製造工程は、主に基板ウェハ上に回路を形成する前工程と、このウェハを個片に切り分けた後、配線や樹脂パッケージ封入等を行う後工程と、に分けることができる。
【００２１】
コントローラ１９は、前工程においてＮＡＮＤ型フラッシュメモリ１０内に包含されるよう構成される場合、前工程においては包含されないが後工程において同一パッケージに包含されるように構成される場合、ＮＡＮＤ型フラッシュメモリ１０とは異なるチップとして提供される場合、等様々な場合がある。図１を含め、以下では、コントローラ１９がＮＡＮＤ型フラッシュメモリ１０とは異なるチップとして提供される場合を例にとって説明している。
【００２２】
以下、特に断りのない限り、ホスト装置２０とＮＡＮＤ型フラッシュメモリ１０との間のデータや命令のやり取りは、多くの場合コントローラ１９が仲介する。この場合でも、コントローラ１９は、前述のデータや命令の本質的内容を変えることはないため、詳細については省略して説明する場合がある。なお、ＮＡＮＤ型フラッシュメモリ１０及びコントローラ１９の構成例の詳細については後述する。
【００２３】
また、ホスト装置２０の構成としては、民生機器のように専用ハードウェアで構成される場合、専用ハードウェアとそれを動作させるファームウェアの組み合わせで構成される場合だけでなく、装置の全機能がPC上で動作するソフトウェアで実現される場合も想定される。本実施形態は、ホスト装置２０がどのような構成を採用していても、基本的には適用し得るものである。
【００２４】
図１に示す各コンポーネント、データ処理について、以下で説明する。本実施形態では、被認証装置に記録されている秘密識別情報SecretIDを第三者から秘匿した状態で読み出すと共に、正規の被認証装置から読み出されたデータであることを確認する方法、及び同方法を、ＮＡＮＤ型フラッシュメモリ１０を利用したメモリシステムに適用する場合の構成例を示すものである。
【００２５】
１－１．ＮＡＮＤ型フラッシュメモリ
本実施形態において、ＮＡＮＤ型フラッシュメモリ１０は、被認証装置である。
【００２６】

図示するように、本実施形態に係るＮＡＮＤ型フラッシュメモリ１０は、セルアレイ（Cell array）１１、及びセルアレイ１１の周辺領域に配置されるデータキャッシュ（Data Cache）１２、データ生成回路（Generate）１３，１４、一方向性変換器（Oneway）１５を備える。データ生成回路（Generate）１３，１４及び一方向性変換器（Oneway）１５は認証回路１７を構成する。

【００２７】

セルアレイ１１は、外部からの読み出し及び書き込みの両方が可能な読み書き可能領域（Read/Write area）１１－１、外部からの読み出し及び書き込みの両方が禁止された秘匿領域（Hidden area）１１－２、外部からの書き込みが禁止されたロム領域（ROM area）１１－３等を備える。

【００２８】

読み書き可能領域（一般領域）１１－１は、ＮＡＮＤ型フラッシュメモリ１０の外部からのデータ書き込み及びデータ読み出し両方が可能な領域である。読み書き可能領域１１－１には、$FKey_v$を秘匿するために用意された暗号化FKey束である鍵管理情報FKBv（Family Key Block）が記録される。FKBvはＮＡＮＤ型フラッシュメモリ１０に記録される他のデータとは異なり、ＮＡＮＤ型フラッシュメモリ１０の製造時だけでなく、例えばSDカードのようにＮＡＮＤ型フラッシュメモリ１０にコントローラを結合させて一般ユーザ向けのストレージメディアを製造する段階や、或いは前記ストレージメディアの販売後に、ユーザの要求に従ってサーバからダウンロードして記録するように構成することも可能である。詳細については、後述する。

【００２９】

ここで、鍵管理情報FKBvとは、ホスト装置２０が保持する秘密情報$IDKey_k$と、当該秘密情報$IDKey_k$のインデックス情報kとに基づいて秘匿情報$FKey_v$を復号するために用いられる情報、または、ホスト装置２０が保持する秘密情報$IDKey_k$と、当該ホスト装置２０の識別情報とに基づいて秘匿情報$FKey_v$を復号するために用いられる情報である。

【００３０】

また、鍵管理情報FKBvは、ＮＡＮＤ型フラッシュメモリ１０毎にユニークに用意するだけでなく、製造工程に合わせて例えばＮＡＮＤ型フラッシュメモリ１０の製造ロット（lot）単位やウェハ（Wafer）単位等、複数のＮＡＮＤ型フラッシュメモリ１０に共通に付すことが可能な情報（対応付けられることが可能な情報）である。また、鍵管理情報FKBvのインデックス情報vは、鍵管理情報FKBvの識別情報またはバージョン番号情報であってもよい。

【００３１】

秘匿領域１１－２は、ＮＡＮＤ型フラッシュメモリ１０の外部からのデータ書き込み及びデータ読み出し両方が禁止される領域（Read/Write inhibit）である。秘匿領域１１－２には、認証処理においてＮＡＮＤ型フラッシュメモリ１０が用いる秘密情報$NKey_i$及びＮＡＮＤ型フラッシュメモリ１０の秘密識別情報SecretIDが記録される。

【００３２】

ロム領域１１－３は、ＮＡＮＤ型フラッシュメモリ１０外部からのデータ書き込みが禁止され、一方データ読み出しが許可される領域である。ロム領域１１－３には、鍵管理情報FKBvによって秘匿されている秘匿情報$FKey_v$を示すためのインデックス情報v（index of FKey）、秘匿情報$FKey_v$によって暗号化された秘密識別情報SecretID（E-SecretID）、秘密情報$NKey_i$を示すためのインデックス情報i（index of NKey）が記録される。

【００３３】

本実施形態では、インデックス情報iやインデックス情報vを記録する際にデータに誤りが生じてしまった場合でも、正しい識別情報が読み出せるようにするために、一般的には誤り訂正符号を付加した状態で記録される。しかしながら、説明を簡略化するため、ここでは誤り訂正符号化及び復号化処理については特に図示しないものとする。

【００３４】

なお、ロム領域１１－３は、例えば１回の書き込みのみ許容されるＯＴＰ（One Time P

rogram）領域であってもよいし、ＮＡＮＤ型フラッシュメモリ１０の製造工程においては読み出し及び書き込みが可能な一般領域であって、出荷後の管理フラグの書き換えによって読み出し専用となる領域であってもよい。または、当該領域に対する書き込みコマンドを一般領域とは異なる特殊コマンドとし、ＮＡＮＤ型フラッシュメモリ１０の受領者にはこの特殊コマンドを提供しない等の方法を利用してもよい。他には、ＮＡＮＤ型フラッシュメモリ１０上では一般領域の扱いであるが、コントローラ１９がホスト装置２０に提供する機能を読み出しのみに限定する、などの構成をとってもよい。

【００３５】

なお、ロム領域１１－３に記録される情報は後述の通り、秘匿領域１１－２に記録される情報と関連付けられているため、ロム領域１１－３に記録される情報を改ざんした場合、ＮＡＮＤ型フラッシュメモリ１０の認証機能を有効に働かせることができなくなる。従って改ざんされることによるセキュリティ上の懸念はないため、必ずしもロム領域である必要はなく、読み出し及び書き込みが可能な一般領域で代用してもよい。この場合、図面中のロム領域１１－３を読み書き可能領域（一般領域）１１－１と読み替えればよい。関連して、ロム領域１１－３中に記載されているデータの一部を読み書き可能領域（一般領域）１１－１に記録してもよい。例えば、インデックス情報v（index of FKey）を読み書き可能領域（一般領域）に記録し、暗号化された秘密識別情報（E-SecretID）とインデックス情報v（index of FKey）をロム領域１１－３に記録するという構成も可能である。上記ロム領域１１－３の構成例については、本明細書にて他の実施形態や変形例として後述されるロム領域１１－３にも適用可能である。

【００３６】

暗号化された秘密識別情報E-SecretIDとは、ＮＡＮＤ型フラッシュメモリチップ１０毎に固有に（ユニークに）付される秘密識別情報SecretIDを秘匿情報$FKey_v$によって暗号化したデータである。或いは、ＮＡＮＤ型フラッシュメモリに予めコンテンツを記録して販売するようなプリレコーディング（事前記録）コンテンツ配布用途において同じコンテンツデータを記録する際には、敢えて同じ暗号化秘密識別情報E-SecretIDを記録する等、用途に合わせて同じ暗号化秘密識別情報を複数のＮＡＮＤ型フラッシュメモリに記録することもできる。

【００３７】

データキャッシュ１２は、セルアレイ１１から読み出したデータを一時的に記憶する。

【００３８】

データ生成部１３，１４は、複数の入力データから予め定められた演算によって出力データを生成する回路である。

【００３９】

データ生成部１３は、ホスト装置２０から受信した定数HC_jを前述の秘密情報$NKey_i$を用いて変換することで、秘密情報$HKey_{i,j}$を生成する。データ生成部１４は、ホスト装置２０から受信した乱数RN_hを秘密情報$HKey_{i,j}$を用いて変換することで、セッション鍵$SKey_{i,j}$を生成する。データ生成部１３，１４は、ハードウェア（回路）若しくはソフトウェア、またはハードウェアとソフトウェア両方の組み合わせでも実装され得る。

【００４０】

データ生成部１３，１４は、回路として実装される場合は、全体の回路規模を小さくするために後述の一方向性変換器１５と同じ或いは一方向性変換器を流用した回路や、AES（Advanced Encryption Standard）暗号化器等を用いることも可能である。同様に、データ処理手順を分かり易くするために異なる構成要素として図示されている二つのデータ生成部は、同じ回路を繰り返し利用することが可能である。この例の場合、$HKey_{i、j}$=AES_E($NKey_i$，HC_j)、$SKey_{i、j}$= AES_E($HKey_{i、j}$，RN_h)などの構成をとることが可能である。

【００４１】

一方向性変換器１５は、入力されたデータと別途入力された鍵データに一方向性の変換を施し、一方向性変換された入力データを出力する。一方向性変換器１５はハードウェア（回路）若しくはソフトウェア、またはハードウェアとソフトウェア両方の組み合わせで

も実装され得る。

【００４２】

一方向性変換器１５は、秘匿領域１１－２から読み出した秘密識別情報SecretIDを、データ生成回路１４によって生成されたセッション鍵$SKey_{i,j}$を用いて一方向性関数により変換し、一方向性変換識別情報Oneway-ID (= Oneway($SKey_{i,j}$, SecretID))を生成する。また、一方向性変換器１５は、回路として実装される場合は、前述の通り、全体の回路規模を小さくするために、データ生成部１４等を流用して使用することも可能である。この例の場合、Oneway-ID=AES_E($SKey_{i,j}$, SecretID) (+) SecretIDなどの構成をとることが可能である。

【００４３】

また、図示しないが、コントローラ１９を介してホスト装置２０にデータを出力する出力部等も実際には構成要素として配置されている。

【００４４】

１－２．ホスト装置

本実施形態において、ホスト装置２０は、認証装置である。

【００４５】

図示するように、本実施形態に係るホスト装置（Host）２０は、復号部（Decrypt）２１、FKB処理部（Process FKB）２２、メモリ（Memory）２３、乱数生成部（RNG: Random Number Generator）２４、選択部（Select 2）２５、データ生成部（Generate）２６、一方向性変換器（Oneway）２７、及びデータ検証部（Verify）２８等を備える。この他、例えば、図示しない誤り訂正処理部等も必要に応じて構成要素として備えることが可能である。

【００４６】

復号部２１は、入力されたデータを別途入力された鍵データで複合し、復号された入力データを出力する。本実施形態では、復号部２１は、コントローラ１９を介して、暗号化秘密識別情報E-SecretIDをＮＡＮＤ型フラッシュメモリ１０から読み出す。そして、暗号化秘密識別情報E-SecretIDを、後述のFKB処理部２２（データ選択部２２－２）から入力された秘匿情報FKeyを用いて復号し、秘密識別情報SecretIDを出力する。

【００４７】

FKB処理部２２は、ＮＡＮＤ型フラッシュメモリ１０から読み出される鍵管理情報FKBvを、メモリ２３に秘匿されている秘密情報$IDKey_k$及び秘密情報$IDKey_k$のインデックス情報kを用いて復号し、生成した秘匿情報FKeyを復号部２１に出力する。本実施形態では、FKB処理部２２は、データ選択部（Select 1）２１－１及び復号部（Decrypt）２２－２を備えている。

【００４８】

第１段目のデータ選択部２１－１は、ＮＡＮＤ型フラッシュメモリ１０から読み出した暗号化FKey束（鍵管理情報FKBv）の中から、メモリ２３に記録されているインデックス情報kを用いて、メモリ２３に秘匿されている秘密情報$IDKey_k$によって復号可能なデータを選択して、復号部２２－２に出力する。

【００４９】

復号部２２－２は、メモリ２３に秘匿されている秘密情報$IDKey_k$を用いて、データ選択部２２－１において選択されたデータを復号し、生成された秘匿情報FKeyを復号部２１に出力する。

【００５０】

メモリ２３は、インデックス情報k、秘密情報$IDKey_k$、秘密情報セット$HKey_{i,j}$ (i=1,…,m。なお、jは当該$HKey_{i,j}$においては固定の値である)、及び定数HC_jを記録し、少なくとも秘密情報$IDKey_k$及び秘密情報セット$HKey_{i,j}$ (i=1,…,m)をホスト装置２０の外部に対して秘匿する。ここで、定数HC_jとは、認証要求（Request authentication）時にＮＡＮＤ型フラッシュメモリ１０に送出するために予め保持しているホスト装置２０の定数である。詳細については後述する。

【００５１】
乱数生成部２４は、認証処理に用いる乱数RN_hを生成し、出力する。
【００５２】
第２段目のデータ選択部２５は、ＮＡＮＤ型フラッシュメモリ１０のロム領域１１－３からデータキャッシュ１２を介して読み出したインデックス情報iを用いて、当該ホスト装置２０が秘匿している秘密情報セット$HKey_{i,j}$の中から、認証処理に必要な秘密情報$HKey_{i,j}$を選択する。
【００５３】
データ生成部２６は、複数の入力データから予め定められた演算によって出力データを生成する演算部である。本実施形態では、データ生成部２６は、ホスト装置２０自身が生成した乱数RN_hを、ホスト装置２０が秘匿している秘密情報$HKey_{i,j}$を用いて変換することで、セッション鍵$SKey_{i,j}$を生成する。データ生成部２６として、例えば上述したAES暗号化器等を用いることも可能である。
【００５４】
一方向性変換器２７は、復号部２１から出力される秘密識別情報SecretIDを、データ生成部２６から出力されるセッション鍵$SKey_{i,j}$を用いて一方向性関数により変換し、一方向性変換識別情報Oneway-IDを生成する。
【００５５】
データ検証部２８は、ＮＡＮＤ型フラッシュメモリ１０から受信した一方向性変換識別情報Oneway-IDと、ホスト装置２０内の一方向性変換器２７から得られた一方向性変換識別情報Oneway-IDとが一致するか否かを比較する。上記一方向性変換識別情報Oneway-IDの両方の値が一致した場合（OK）には、復号部２１で得られた秘密識別情報SecretIDが正規のIDであると判定して、得られた秘密識別情報SecretIDを以降の処理に引き渡す。一方、不一致の場合（NG）には、秘密識別情報SecretIDが不正なIDであると判定して、その旨を出力する。
【００５６】
他に、ホスト装置２０が有する秘密情報、例えば$IDKey_k$、$HKey_{i、j}$が流出し、流出情報を有する不正ホスト装置が不正製造者によって製造された場合などにおいて、当該不正ホスト装置を無効化する手段として、鍵管理情報（FKBv）から不正ホスト装置が有する$IDKey_k$にてFKeyを導出可能な情報を除くなどの対応をとることも可能である。この対応については、図３における説明にて後述する。この対応をするに当たっては、秘密情報$IDKey_k$及びインデックス情報k、秘密情報$HKey_{i、j}$及びホスト定数HC_jの間に関連を持たせることが有用である。これは、関連があれば、不正ホスト装置が認証において通知するHC_jを観測することによって当該不正ホスト装置が有する秘密情報$IDKey_k$及び$HKey_{i、j}$の両方が特定可能となる。関連付けの方法としては、HC_jの全部もしくは一部の情報を$IDKey_k$と共有することや、HC_jの全部もしくは一部の情報を$IDKey_k$を暗号処理した結果により構成することや、$IDKey_k$の全部もしくは一部の情報をHC_jを暗号処理した結果により構成することなどの方法がとれる。更に、鍵管理情報（FKBv）の生成に当たり、FKeyおよび$IDKey_k$に加えて、$HKey_{i、j}$を用いるのが望ましい。これについてはFKBの構成例を説明している箇所にて後述する。
【００５７】
ここで、上記秘密情報$IDKey_k$、秘密情報$HKey_{i,j}$は、例えば、ホスト装置２０が民生機器のような専用ハードウェア装置であれば内部の専用メモリにメーカ独自の方法で暗号化した上で記録されていたり、PC等で実行されるプログラムであればタンパーレジスタントソフトウェア（TRS）技術によって不正な解析から保護できる状態で保持していたり、或いはセキュリティモジュールを内蔵している場合には当該セキュリティモジュールの機能を利用して秘匿する等の対策を採った状態で記録される。
【００５８】
なお、コントローラ（Controller）１９は、ＮＡＮＤ型フラッシュメモリ１０を制御して、ホスト装置２０との間のデータ転送等を行う。例えばコントローラ１９は、ホスト装

置２０から受信した命令を解釈し、ＮＡＮＤ型フラッシュメモリ１０のインターフェース仕様に適合した命令に変換した上で、当該命令をＮＡＮＤ型フラッシュメモリ１０に送出する。コントローラ１９は、例えばSD Memory規格、SDIO規格、eMMC規格等、必要に応じて様々なインターフェース規格を採用することができる。

【００５９】

また、コントローラ１９は、一般領域１１－１の一部を確保し、自身の動作に必要な制御データを保存する。また、コントローラ１９は、ホスト装置２０から受信した論理アドレスをＮＡＮＤ型フラッシュメモリの物理アドレスに変換する機能を有していてもよい。また、セルアレイ１１の疲弊を平準化するため、所謂ウェアレベリングを実行する機能を有していてもよい。ただし、少なくとも秘匿領域１１－２についてはウェアレベリングの対象外とされる。

【００６０】

また、メモリシステムの構成例は、上記説明したものに限られない。例えば、図示しない誤り訂正処理部等のその他の構成要素も必要に応じて備えることが可能である。更に、ＮＡＮＤ型フラッシュメモリ１０が有する秘密情報$NKey_i$が複数あってもよい。すなわち、秘密情報$NKey_i$とこれに対応するインデックス情報iの組み合わせを1つのスロットとし、複数スロットがＮＡＮＤ型フラッシュメモリ１０に記録されている。ここで、上記スロットには各々スロット番号が付与されており、ホスト装置２０は各スロット番号のインデックス情報ｉを読み出し、いずれか一つを選択して認証を行う。この場合、ホスト装置２０はＮＡＮＤ型フラッシュメモリ１０に対して選択したスロット番号に相当する情報を通知し、ＮＡＮＤ型フラッシュメモリ１０は通知されたスロット番号に相当する情報を用いて認証処理を行う。更には、ＮＡＮＤ型フラッシュメモリ１０が有する全ての情報を1つのスロットとし、当該情報スロットを複数有してもよい。すなわち、秘密情報$NKey_i$、インデックス情報i、鍵管理情報（FKBv）、インデックス情報v（index of FKey）、秘密識別情報SecretID、暗号化された秘密識別情報（E-SecretID）を1つのスロットとし、複数スロットがＮＡＮＤ型フラッシュメモリ１０に記録されている。ここで、上記スロットには各々スロット番号が付与されており、ホスト装置２０は各スロット番号のインデックス情報ｉを読み出し、いずれか一つを選択して認証を行う。この場合、ホスト装置２０はＮＡＮＤ型フラッシュメモリ１０に対して選択したスロット番号に相当する情報を通知し、ＮＡＮＤ型フラッシュメモリ１０は通知されたスロット番号に相当する情報を用いて認証処理を行う。

【００６１】

上記において、ＮＡＮＤ型フラッシュメモリ１０が複数のスロットを有する方法を示したが、これらに限らず、一部の情報を複数のスロットで共有するいかなる構成をとることも可能である。例えば、秘密識別情報SecretID、暗号化された秘密識別情報（E-SecretID）、鍵管理情報（FKBv）、インデックス情報v（index of FKey）は複数のスロットで共有し、他の情報はスロット毎に個別に有するなども可能である。

【００６２】

また、ＮＡＮＤ型フラッシュメモリ１０が複数のスロットとスロット番号を有し、いずれのスロットを認証に用いるかをホスト装置２０が通知する方法は本明細書にて後述する他の実施例全てに適用可能である。

【００６３】

＜２．認証フロー＞

次に、図２に沿って、第１の実施形態に係るメモリシステムの認証フローについて説明する。

【００６４】

（Step Ｓ１１）

認証を開始（Start）すると、ホスト装置２０は、ＮＡＮＤ型フラッシュメモリ１０から鍵管理情報である暗号化FKey束（FKB: Family Key Block）及び暗号化秘密識別情報SecretID（E-SecretID）を読み出す。

【００６５】
（Step Ｓ１２）
続いて、ホスト装置２０は、読み出した鍵管理情報FKBからデータ選択部（Select1）２２－１によりデータ選択処理を行い、ホスト装置２０が復号可能な暗号化された秘匿情報FKeyを読み出すと共に、秘匿している秘密情報$IDKey_k$を用いて上記復号部２２－２により復号することにより、秘匿情報FKeyを得る。更に、ホスト装置２０は、得られた秘匿情報FKeyを用いて、ＮＡＮＤ型フラッシュメモリ１０から読み出した暗号化秘密識別情報E-SecretIDを復号することにより、秘密識別情報SecretIDを得る。
【００６６】
（Step Ｓ１３）
続いて、ホスト装置２０は、ＮＡＮＤ型フラッシュメモリ１０に対して、インデックス情報iの読み出し要求を行う。
【００６７】
（Step Ｓ１４）
続いて、ＮＡＮＤ型フラッシュメモリ１０は、ホスト装置２０の要求を受けて、インデックス情報iをセルアレイ１１からロードし、ホスト装置２０に出力する。
【００６８】
（Step Ｓ１５）
続いて、ホスト装置２０は、認証要求時に必要となる乱数RN_hを生成する。認証処理に乱数RN_hを用いることにより、以下の処理でＮＡＮＤ型フラッシュメモリ１０との間で毎回異なる共有鍵を利用することができる。
【００６９】
（Step Ｓ１６）
続いて、ホスト装置２０は、認証要求（Request authentication）と共に、予め保持している定数HC_j及び乱数RN_hをＮＡＮＤ型フラッシュメモリ１０に送出する。
【００７０】
（Step Ｓ１７）
続いて、ＮＡＮＤ型フラッシュメモリ１０は、秘密情報$NKey_i$ (i=1,…,m)及び秘密識別情報SecretIDを秘匿領域１１－２からロードし、データキャッシュ１２に保存する。
【００７１】
（Step Ｓ１８）
続いて、ＮＡＮＤ型フラッシュメモリ１０は、秘匿している秘密情報$NKey_i$とホスト装置２０から受信した定数HC_jとを用いて、データ生成回路１３におけるデータ生成処理により秘密情報$HKey_{i,j}$を生成する。
【００７２】
（Step Ｓ１９）
続いて、ＮＡＮＤ型フラッシュメモリ１０は、受信した乱数RN_hを用いて、データ生成回路１４におけるデータ生成処理により、セッション鍵$SKey_{i,j}$ (= Generate($HKey_{i,j}$, RN_h))を生成する。
【００７３】
（Step Ｓ２０）
続いて、ＮＡＮＤ型フラッシュメモリ１０は、生成したセッション鍵$SKey_{i,j}$を用いて、秘密識別情報SecretIDに一方向性変換器１５における一方向性変換処理を行い、一方向性変換識別情報Oneway-ID (=Oneway($SKey_{i,j}$, SecretID))を生成する。生成された一方向性変換識別情報Oneway-IDは、ホスト装置２０に送出される。
【００７４】
（StepＳ２１）
上記StepＳ１８と並行して、ホスト装置２０は、受信したインデックス情報iを用いて、予め秘匿していた秘密情報セット$HKey_{i,j}$ (i=1,…,m)から当該ＮＡＮＤ型フラッシュメモリ１０との認証処理に必要な秘密情報$HKey_{i,j}$を選択する。

【００７５】
（Step Ｓ２２）
続いて、ホスト装置２０は、選択した秘密情報$HKey_{i,j}$と生成した乱数RN_hとを用いて、データ生成部２６におけるデータ生成処理により、セッション鍵$SKey_{i,j}$ (= Generate($HKey_{i,j}$, RN_h))を生成する。
【００７６】
（Step Ｓ２３）
続いて、ホスト装置２０は、生成したセッション鍵$SKey_{i,j}$を用いて、秘密識別情報SecretIDに一方向性変換器２７における一方向性変換処理を行い、一方向性変換データOneway-IDを生成する。
【００７７】
（Step Ｓ２４）
続いて、ホスト装置２０は、ＮＡＮＤ型フラッシュメモリ１０より受信した一方向性変換識別情報Oneway-IDと、自身が生成した一方向性変換識別情報Oneway-IDとが一致するか否かを判定する。上記一方向性変換識別情報Oneway-IDの両方の値が一致した場合（OK）には、復号部２１で得られた秘密識別情報SecretIDが正規のIDであると判定して、以降の処理に秘密識別情報SecretIDを引き渡す。一方、不一致の場合（NG）には、秘密識別情報SecretIDが不正なIDであると判定し、その旨を以降の処理に出力する。
【００７８】
以上の動作により、第１の実施形態に係る認証フローを終了する（End）。
【００７９】
なお、ここで、メモリシステムの構成例において示した通り、ＮＡＮＤ型フラッシュメモリ１０が複数のスロットを有する場合、ホスト装置２０は認証に用いるスロット番号をＮＡＮＤ型フラッシュメモリ１０に通知する必要がある。この場合、上記Step Ｓ１６にてスロット番号を付随して通知してもよいし、もしくはStep Ｓ１６より以前のStepにおいて通知してもよい。
【００８０】
＜３．FKB(Family Key Block)について＞
次に、図３を用い、第１の実施形態に係る鍵管理情報FKB(Family Key Block)についてより詳しく説明する。
【００８１】
秘密識別情報SecretIDが記録されているＮＡＮＤ型フラッシュメモリ１０に適合した鍵管理情報FKBを生成するためには、予め用意された秘密鍵情報である$IDKey_i$ (i=1,…,n)（Set of $IDKey_i$ ’s）の１つ１つの$IDKey_i$を用いて、$FKey_v$を１つ１つ暗号化（Encrypt）する。つまり、鍵管理情報FKBとは、暗号化$FKey_v$(E- $FKey_v$,i) = Encrypt($IDKey_i$, $FKey_v$)の集合であり、この暗号化$FKey_v$の集合を暗号化FKey束と称する。
【００８２】
なお、鍵管理情報FKBの構成については、本実施形態に限られない。例えば、特定の$IDKey_i$が露呈してしまった場合、当該$IDKey_i$を保持しているホスト装置２０では暗号化FKey束からFKeyを復号することができないようにするために、当該秘密情報$IDKey_i$で復号可能な暗号化$FKey_v$（上述の例ではE- FKeyv,i）をFKBから削除することにより、新たに構成されたFKBを記録したＮＡＮＤ型フラッシュメモリ１０を使用した場合には、当該ホスト装置２０では正しい$FKey_v$及び秘密識別情報SecretIDを得る（復号する）ことができないようにすることも可能である。このようにすることで、当該秘密情報$IDKey_i$を保持したホスト装置２０を無効化する機能を提供することも可能である。
【００８３】
また、前述の通り、秘密情報$IDKey_k$及びインデックス情報k、秘密情報$HKey_{i、j}$及びホスト定数HC_jの間に関連を持たせるにあたり、鍵管理情報（FKBv）の生成においてFKeyおよび$IDKey_k$に加えて、$HKey_{i、j}$を流用することもできる。例えば、(E- $FKey_v$,i) = Encrypt (Encrypt($IDKey_i$, $FKey_v$), $HKey_{i、j}$)、(E- $FKey_v$,i) = Encrypt (Encrypt($HKey_{i、j}$,

$FKey_v$), $IDKey_i$)、(E- $FKey_v$,i) = Encrypt($HKey_{i,j}$, $IDKey_i$(+)$FKey_v$)などの構成をとってもよい。これは、複数のホスト装置２０から鍵が流出した場合に、異なる装置の秘密鍵$IDKey_i$、$HKey_{i,j}$を組み合わせることを防止する効果がある。つまり、正しく組み合わされた$IDKey_i$、$HKey_{i,j}$でない限り、FKeyの復号を不可能とすることにより、HC_jを観測することでこれに紐付いた$HKey_{i,j}$が判明し、更に$IDKey_i$も特定することができ、ひいては露呈した$IDKey_i$を無効化することが可能となる。

【００８４】

鍵管理情報FKBの生成方法についても、本実施形態に限られない。例えば、CPRM（非特許文献１参照）において用いられているMKB（Media Key Block）技術や、非特許文献３に開示されたMKB技術を用いて鍵管理情報FKBを生成しても、ホスト装置２０を無効化する機能を提供することが可能である。

【００８５】

ここで、MKB技術とは、複数の機器がそれぞれ異なる秘密情報を持つ状況で、機器の無効化を実現しつつ、（無効化対象でない機器の間で）共通の秘密情報（Media Key）を効率よく共有するための技術であり、Broadcast Encryptionとも称されるものである。

【００８６】

例えば、上記MKB技術を適用した場合、メモリシステムの構成例は、図４のように示される。図示するメモリシステムは、FKB処理部（Process FKB）２２が上位概念化されて図示される点で、図１と相違する。この場合においても、Kや$IDKey_i$に対応する情報であるホスト装置２０のノード番号やノード番号に割り当てられたホスト鍵群によって復号されるFKBの当該データを$HKey_{i,j}$やHC_jと関連付けることにより、露呈した鍵の特定と無効化が可能となる。

【００８７】

＜４．秘密情報やFKBの書き込みについて＞

次に、ＮＡＮＤ型フラッシュメモリ１０への秘密情報や鍵管理情報FKBの書き込みについて説明する。

【００８８】

４－１．ＮＡＮＤ型フラッシュメモリの製造時等に書き込む場合

まず、図５、図６を用い、例えば、ＮＡＮＤ型フラッシュメモリ１０の製造時等に秘密情報や鍵管理情報FKBを書き込む場合について説明する。ここでは、図６のフローに即して説明する。

【００８９】

ライセンス管理者（Licensing Administrator）４０は、以下のデータを生成する：鍵管理情報FKBv (v=1,…,n)、秘匿情報$FKey_v$(v=1,…,n)、インデックス情報v(v=1,…,n)、秘密情報$NKey_i$、及びインデックス情報i。なお、前述した通り、FKBvは、$FKey_v$を暗号化したものである。また、vは複数の値であっても良い。例えば、vとして1,2,3の３つの値をライセンス管理者４０が生成する場合、ライセンス管理者４０は、生成したvに対応させる形で、(FKB1, $FKey_1$), (FKB2, $FKey_2$), (FKB3, $FKey_3$)を生成する。

【００９０】

ライセンス管理者４０は、生成したデータの内、$FKey_v$(v=1,…,n)、v(v=1,…,n)、$NKey_i$、iをメモリ製造者３０に渡す。これらのデータを渡す際には、例えば、ライセンス管理者４０は、予めメモリ製造者３０の公開鍵を入手しておき、当該公開鍵を用いてデータを暗号化した上でメモリ製造者３０に送信する、等といった安全な手段を用いる。

【００９１】

メモリ製造者（Memory Vender）３０は、上記ＮＡＮＤ型フラッシュメモリ１０に加え、ライセンス管理者４０から渡されたFKBv (v=1,…,n)等のデータ３１を保持し、選択部３２、３３、生成部３４、暗号部３５を備える。

【００９２】

（Step Ｓ３１）

上記構成により、まず、メモリ製造者３０は、生成部（SecretID Generator）３４にお

いて、秘密識別情報SecretIDを生成する。

【００９３】

（Step Ｓ３２）

続いて、データ３１を受け取ったメモリ製造者３０は、vの中から一つの値を選択部３２により選択する。更に、選択部３２は、前記選択したvに対応する$FKey_v$を選択する。メモリ製造者３０は、選択した$FKey_v$を用いて、生成したSecretIDを暗号化し、暗号化された秘密識別情報E-SecretIDを生成する。

【００９４】

（Step Ｓ３３）

続いて、メモリ製造者３０は、当該vの値をＮＡＮＤ型フラッシュメモリ１０のロム領域１１－３へインデックス情報v（index of FKey）として書き込む。

【００９５】

また、メモリ製造者３０は、インデックス情報i（index of NKey）の値をＮＡＮＤ型フラッシュメモリ１０のロム領域１１－３へ、$NKey_i$の値を秘匿領域１１－２へそれぞれ書き込む。

【００９６】

更に、メモリ製造者３０は、秘密識別情報SecretIDの値をＮＡＮＤ型フラッシュメモリ１０の秘匿領域１１－２へ、暗号化された秘密識別情報E-SecretIDの値をロム領域１１－３へそれぞれ書き込む。

【００９７】

以上の動作により、ＮＡＮＤ型フラッシュメモリ１０の製造時等に所定の秘密情報や鍵管理情報FKBを書き込むことができる（End）。なお、上記各値を書き込む順番は、暗号化された秘密識別情報E-SecretIDは、暗号化処理しないと得られない値であるため、暗号部３５による上記暗号化処理後となる。しかし、それ以外の書き込み動作の順序について制約はなく、上述の例以外の順番で書き込んでも良い。

【００９８】

更に、メモリ製造者３０は、書き込み処理を終えたＮＡＮＤ型フラッシュメモリ１０をカード製造者（Card Vendor）に渡す。

【００９９】

このように、本実施形態では、インデックス情報v（index of FKey）等が、ＮＡＮＤ型フラッシュメモリ１０にあらかじめ書き込まれた状態とすることができる。

【０１００】

４－２．FKBをカード製造者（Card Vendor）が書き込む場合

次に、図７、図８を用い、FKBをカード製造者５０が書き込む場合について説明する。ここでも、図８のフローに即して説明する。

【０１０１】

カード製造者（Card Vendor）５０は、上記メモリ製造者３０から上記所定の情報v等が書き込まれたＮＡＮＤ型フラッシュメモリ１０を受け取る。

【０１０２】

そして、例えばSDカード等のように、そのＮＡＮＤ型フラッシュメモリ１０を制御するコントローラ１９を結合させ、一般ユーザ等向けのストレージメディア（ここでは、Card）５５を製造する。

【０１０３】

カード製造者５０は、上記ストレージメディア（Card）５５に加え、ライセンス管理者４０から受け取るデータ（FKBv）５１、選択部５２を備える。

【０１０４】

カード製造者５０が鍵管理情報FKBvを書き込む処理については、次の通りである。

【０１０５】

（Step Ｓ３５）

まず、カード製造者５０は、鍵管理情報FKBvをライセンス管理者４０からデータ５１と

して受け取る。この際、データ５１の受け渡しには、上述した安全な手段を用いる。

【０１０６】

そして、カード製造者５０は、（コントローラ１９を介して）ＮＡＮＤ型フラッシュメモリ１０のロム領域１１－３に記録されるインデックス情報vの値をデータキャッシュ１２等に読み出す。

【０１０７】

（Step Ｓ３６）

続いて、カード製造者５０は、読み出したインデックス情報vの値に対応する鍵管理情報FKBvを選択部５２により選択する。

【０１０８】

（Step Ｓ３７）

続いて、カード製造者５０は、コントローラ１９を介して、ＮＡＮＤ型フラッシュメモリ１０の読み書き可能領域１１－１に選択した鍵管理情報FKBvを書き込む。

【０１０９】

＜作用効果＞

上記のように、第１の実施形態に係る認証装置、被認証装置、及びその認証方法によれば、少なくとも下記（１）乃至（３）の効果が得られる。

【０１１０】

（１）ホスト装置２０から秘密情報が漏洩した場合であっても、漏洩した情報を用いたＮＡＮＤ型フラッシュメモリ１０の秘密情報の不正利用を防止することができる。

ここで、上述した通り、認証装置であるホスト装置２０は、民生機器のような専用ハードウェア装置だけでなく、例えば、PC等で実行可能なプログラムとして提供され、当該ソフトウェアが実質的なホスト装置となる場合がある。一方、被認証装置であるＮＡＮＤ型フラッシュメモリ１０は、記録メディアであり、ファームウェアと呼ばれるプログラムが介在する場合であっても、重要な処理や情報はセルアレイ１１中のハードウェア内に秘匿された状態で記憶される。

【０１１１】

そのため、現実的には、例えば、PC上で実行されるソフトウェアは、記録メディアに比べて耐タンパー性能（攻撃に対する耐性）が低くなってしまうことが懸念される。そのため、耐タンパー性能の低いホスト装置（認証装置）２０を攻撃することで、耐タンパー性の高いＮＡＮＤ型フラッシュメモリ１０（被認証装置）に秘匿された秘密情報をも暴露され、耐タンパー性の高い装置に成りすまされることが懸念される。

【０１１２】

そこで、第１の実施形態に係る構成及びその認証方式では、上記のように、比較的耐タンパー性の高いＮＡＮＤ型フラッシュメモリ１０は、第１鍵情報（$NKey_i$）から第２鍵情報（$HKey_{i,j}$）を生成することができる第１鍵情報（$NKey_i$）をセルアレイ１１に秘匿する。一方、ホスト装置２０は、第２鍵情報（$HKey_{i,j}$）からは第１鍵情報（$NKey_i$）を生成することができない第２鍵情報（$HKey_{i,j}$）のみをメモリ２３に秘匿する。

【０１１３】

そのため、ＮＡＮＤ型フラッシュメモリ１０は、ホスト装置２０から受領した定数HC_jと自身が秘匿する第１鍵情報（$NKey_i$）とを用いて、認証装置２０が秘匿する第２鍵情報（$HKey_{i,j}$）を生成する。ＮＡＮＤ型フラッシュメモリ１０は、第２鍵情報（$HKey_{i,j}$）と乱数RN_hとを用いて、セッション鍵$SKey_{i,j}$を生成する。

【０１１４】

ホスト装置２０は、インデックス情報iにより選択される第２鍵情報（$HKey_{i,j}$）と乱数RN_hとを用いて、セッション鍵$SKey_{i,j}$を生成する。その結果、ＮＡＮＤ型フラッシュメモリ１０とホスト装置２０とは、同じセッション鍵$SKey_{i,j}$を共有する。

【０１１５】

このように、本実施形態では、ＮＡＮＤ型フラッシュメモリ（被認証装置）１０が秘匿する情報の秘密レベルと、ホスト装置（認証装置）２０が秘匿する情報の秘密レベルとを

非対称とすることができる。例えば、本実施形態では、比較的耐タンパー性の高いＮＡＮＤ型フラッシュメモリ１０が秘匿する情報の秘密レベルを、比較的耐タンパー性の低いホスト装置２０が秘匿する情報の秘密レベルよりも、より高く設定することができる。

【０１１６】

そのため、仮にホスト装置２０が秘匿する情報が漏洩した場合であっても、比較的耐タンパー性の高いＮＡＮＤ型フラッシュメモリ１０が秘匿する情報の秘密レベルが更に高いため、漏洩した情報を用いてＮＡＮＤ型フラッシュメモリ１０に”成りすますこと”ができない。従って、漏洩した情報を用いたＮＡＮＤ型フラッシュメモリ１０の秘密情報の不正利用を防止することができる点で有利である。その結果、例えば、ホスト装置２０から読み出されたID情報が、目的の被認証装置１０から読み出した情報であることを確実に判定し、その相手方の不正利用の無効化等が可能となる。

【０１１７】

（２）実装化において有利である。

上述した通り、本実施形態のような構成では、比較的大きな回路規模を要求される公開鍵暗号処理やMKB処理のハードウェア実装が困難である等の回路規模上の制約が同時に課せられる環境下である。

【０１１８】

しかしながら、本実施形態によれば、鍵情報が非対称であるものの比較的大きな回路規模を必要とする公開鍵暗号処理を用いる必要がない。更に、上記のように、ホスト装置（認証装置）２０とＮＡＮＤ型フラッシュメモリ（被認証装置）１０とが秘匿する情報の秘密レベルを非対称とすることにより、片方の装置から漏れた情報だけではもう一方の装置に成りすますことができない認証手段を行い、認証装置２０と被認証装置１０との間で秘密情報であるセッション鍵$SKey_{i,j}$を共有する。

【０１１９】

そのため、上記制約が課される厳しい環境下であっても、実装化において有利であると言える。更に、上記のように、メモリシステムを構成するデータ生成回路や暗号化器を同じ処理として共有することにより、回路規模を更に小さくすることも可能である。

【０１２０】

（３）製造工程の簡略化、製造コストの低減化に対して有利である。

本実施形態に係るＮＡＮＤ型フラッシュメモリ１０は、読み書き可能領域１１－１に、その用途に応じてＮＡＮＤ型フラッシュメモリ１０毎に固有（ユニーク）、或いは製造ロット（lot）単位等複数のＮＡＮＤ型フラッシュメモリ１０に共通に付される鍵管理情報（FKBv）を備える。更に、ロム領域１１－３に、ＮＡＮＤ型フラッシュメモリ１０毎に固有に（ユニークに）付される暗号化された秘密識別情報（E-SecretID）を備える。

【０１２１】

鍵管理情報（FKBv）を製造ロット単位で共通化させた場合には、ＮＡＮＤ型フラッシュメモリ１０毎に記録しなければならない固有（ユニーク）な情報を、暗号化された秘密識別情報（E-SecretID）のようにデータサイズの小さいデータだけに減らすことができる。換言すれば、共通に付される鍵管理情報（FKBv）と固有の暗号化秘密識別情報（E-SecretID）とに分け、２段階に暗号化することにより、ＮＡＮＤ型フラッシュメモリ１０に書き込むべき固有の暗号化秘密識別情報（E-SecretID）のデータサイズを抑えることができるものである。

【０１２２】

例えば、上記図５、図６で示したように、ＮＡＮＤ型フラッシュメモリの製造時等において、メモリ製造者３０は、ライセンス管理者４０から受け取ったＮＡＮＤ型フラッシュメモリ１０毎に固有な情報（E-SecretID）を書き込む。

【０１２３】

そして、ＮＡＮＤ型フラッシュメモリ１０に共通に付される暗号化された鍵管理情報（FKBv）については、カード製造者５０等がＮＡＮＤ型フラッシュメモリ１０に共通に書き込むことができる。例えば、上記図７、図８で示したように、カード製造者５０が、上記

ライセンス管理者４０から受け取ったＮＡＮＤ型フラッシュメモリ１０毎に共通な鍵管理情報FKBvを書き込む。そのため、メモリ製造者３０が書き込まなければならないＮＡＮＤ型フラッシュメモリ１０毎に固有（ユニーク）なデータのサイズを低減することが可能となる。

【０１２４】

ここで、ＮＡＮＤ型フラッシュメモリ１０の製造時等に、ＮＡＮＤ型フラッシュメモリ１０に固有かつデータサイズの大きい情報を書き込む場合、製造工程が煩雑となり、製造時間が長期化し、製造コストが増大してしまう。しかしながら、本実施形態に係る構成及び方法によれば、共通に付される鍵管理情報FKBvと固有の暗号化秘密識別情報（E-Secret ID）とに分けて２段階に暗号化することにより、このような煩雑な製造工程は不要となるため、製造工程を簡略化でき、製造コストを低減できる点で有利である。また、製造時間を短縮化できるため、消費電力を低減できる点でもメリットがある。

【０１２５】

また、ホスト装置２０の側においても、秘匿情報FKeyを用いてＮＡＮＤ型フラッシュメモリに固有な値であるSecretIDを暗号化してE-SecretIDを生成し、更に、$IDKey_k$を用いてFKeyを暗号化して鍵管理情報FKBを生成するという構成を取ることにより、ＮＡＮＤ型フラッシュメモリ１０と同様のメリットを享受することが可能となる。

【０１２６】

［変形例１（FKBを後からダウンロードして書き込む場合）］

次に、変形例１に係る認証装置、被認証装置、及びその認証方法について説明する。この説明において、上記第１の実施形態と重複する部分の説明については、省略する。

【０１２７】

＜FKBの書き込みについて＞

暗号化FKey束（FKB）の書き込みについて、説明する。

本変形例１における処理は、暗号化FKey束（FKB）が、ＮＡＮＤ型フラッシュメモリ１０の製造時に書き込まれる場合等には、特に必要のない処理である。しかし、ＮＡＮＤ型フラッシュメモリ１０とコントローラ１９等が結合されて、例えば、SDカード等のストレージメディア製品として一般ユーザ入手し、カード利用時に市場において後から書き込まれる場合等には、必要となるFKBの書き込み処理に関するものである。

【０１２８】

図９では、上記のように鍵管理情報FKBが未記録のストレージメディア（Card）５５に記録されたデータの場合の状態を示している。

図示するように、ＮＡＮＤ型フラッシュメモリ１０は、秘密情報$NKey_i$と秘密識別情報SecretIDとが秘匿領域１１－２に記録される。前記秘密情報$NKey_i$を特定するために必要なインデックス情報i、鍵管理情報FKBを特定するために必要となるインデックス情報v、及びインデックス情報vで指定された$FKey_v$によって暗号化されたSecretID（E-SecretID）がロム領域１１－３に記録される。

【０１２９】

読み書き可能領域１１－１には、暗号化FKey束である鍵管理情報FKBが書き込まれていない点で、上記第１の実施形態と相違する。

【０１３０】

次に、図１０を用い、上記のように鍵管理情報FKBが未記録状態のストレージメディア５５に、サーバからFKBをダウンロードして記録する場合について説明する。

【０１３１】

図示するように、この場合には、ＮＡＮＤ型フラッシュメモリ１０に、必要に応じてデータキャッシュ１２が配置される。

【０１３２】

本実施形態に係るサーバ７０は、FKBデータベース（Set of FKB_i 's (i=1,…,x)）７１及びインデックス情報vから鍵管理情報FKBvを選択するための選択部７２を備える。

【０１３３】

また、サーバ７０とメモリシステム（ＮＡＮＤ型フラッシュメモリ１０、コントローラ１９、ホスト装置２０）とは、インターネット６０を介して電気的に通信接続される。

【０１３４】

なお、ホスト装置２０は、FKBの新規書き込みが必要かどうかを判定し、必要に応じてFKBをサーバに要求する機能を備える。

【０１３５】

＜FKB書き込みフロー＞

次に、図１１に沿って、暗号化FKeyID束（FKB）をサーバ６０からダウンロードしてＮＡＮＤ型フラッシュメモリ１０に書き込むフローについて説明する。

【０１３６】

（Step Ｓ４１）

図示するように、まず、ホスト装置２０が、FKBダウンロードが必要と判定したことにより、FKB書き込みが開始（Start）され、ホスト装置２０はサーバ６０に対してFKB要求を出す。

【０１３７】

（Step Ｓ４２）

続いて、サーバ７０は、ＮＡＮＤ型フラッシュメモリ１０に対して、$FKey_v$を特定するために必要となるインデックス情報vを要求する。

【０１３８】

（Step Ｓ４３）

続いて、ＮＡＮＤ型フラッシュメモリ１０は、ロム領域１１－３からvを読み出し、vをサーバに送出される。

【０１３９】

（Step Ｓ４４）

続いて、サーバ７０は、受信したvに対応するFKBvをFKBデータベース７１の中から選択する。

【０１４０】

（Step Ｓ４５）

続いて、サーバ７０は、選択したFKBvをＮＡＮＤ型フラッシュメモリ１０に送出する。

【０１４１】

（Step Ｓ４６）

続いて、ＮＡＮＤ型フラッシュメモリ１０は、受信したFKBvを読み書き可能領域１１－１に書き込み、記録する。

【０１４２】

以上の動作により、第１の実施形態に係る暗号化FKey束（FKB）ダウンロードフローを終了する（End）。

【０１４３】

その他の構成、動作等に関しては、上記第１の実施形態と実質的に同様である。

【０１４４】

＜作用効果＞

変形例１に係る認証装置、被認証装置及び認証方法によれば、少なくとも第１の実施形態と同様の作用効果（１）乃至（３）を得ることができる。

【０１４５】

更に、変形例１によれば、後からFKBを書き込む場合においても、必要に応じて本実施形態を適用することが可能である。

【０１４６】

［第２の実施形態］

次に、第２の実施形態について説明する。この説明において、上記第１の実施形態と重複する部分の説明については、省略する。

【０１４７】

ここで、第１の実施形態では、ホスト装置２０によるＮＡＮＤ型フラッシュメモリ１０の認証が成功した後、両者は秘密識別情報SecretIDを共有している。認証後の処理として、例えば、ホスト装置２０がコンテンツを暗号化し、ＮＡＮＤ型フラッシュメモリ１０へ当該暗号化コンテンツを書き込むこと等が挙げられるが、この際に、共有した秘密識別情報SecretIDを用いることが考えられる。

【０１４８】

本実施形態は、そのような処理においても秘密識別情報SecretIDを保護することを目的とするものである。そのため、この説明においては、上記第１の実施形態と重複する部分の説明については省略する。

【０１４９】

＜メモリシステム＞

第２の実施形態に係るメモリシステムは、図１２のように示される。

【０１５０】

図１２に示すように、本実施形態に係るメモリシステムは、一方向性変換器（Oneway）２７Ｂ、スイッチ部２９、及び対象となるコンテンツを取り扱う全てのホスト装置２０が共通に保持している情報（ASSV）を更に備える点で、上記第１の実施形態と相違する。

【０１５１】

スイッチ部２９は、データ検証部（Verify）２８において一方向性変換識別情報Oneway-IDの両方の値が一致した場合（OK）の判定結果が制御信号として入力されると、信号経路をオンとさせ、秘密識別情報SecretIDを一方向変換部２７Ｂに出力する。

【０１５２】

一方向変換部（Oneway）２７Ｂは、スイッチ部２９から入力される秘密識別情報SecretIDを、対象となるコンテンツを取り扱う全てのホスト装置が共通に保持している情報（ASSV）を用いて一方向性関数により変換し、一方向性変換識別情報EMID（EMID=Oneway(SecretID, ASSV)）を生成する。

【０１５３】

このように第２の実施形態では、ホスト装置２０で秘密識別情報SecretIDが検証された後に、ホスト装置２０が、対象となる全てのホスト装置が共通に保持している情報（ASSV）を用いて秘密識別情報SecretIDを変換し、一方向性変換識別情報EMIDを計算する。そのため、ホスト装置２０は、秘密識別情報SecretIDの代わりに、一方向性変換識別情報EMIDを用いて、コンテンツ暗号化等の処理を行うことができる。

【０１５４】

その他の構成、動作等は、上記第１の実施形態と実質的に同様であるため、詳細な説明については省略する。

【０１５５】

＜作用効果＞

第２の実施形態に係る認証装置、被認証装置及び認証方法によれば、少なくとも第１の実施形態と同様の作用効果（１）乃至（３）を得ることができる。

【０１５６】

更に、第２の実施形態では、ホスト装置２０は、一方向性変換器（Oneway）２７Ｂ、スイッチ部２９、及び対象となるコンテンツを取り扱う全てのホスト装置が共通に保持している情報（ASSV）を更に備える点で、上記第１の実施形態と相違する。

【０１５７】

上記構成によれば、ホスト装置２０で秘密認識情報SecretIDが検証された後に、ホスト装置２０が、対象となる全てのホスト装置が共通に保持している情報（ASSV）を用いて秘密識別情報SecretIDを変換し、一方向性変換識別情報EMIDを計算する。そのため、ホスト装置２０は、秘密識別情報SecretIDの代わりに、一方向性変換識別情報EMIDを用いて、コンテンツ暗号化等の処理を行うことができる。

【０１５８】

その結果、ここでは図示を省略するが、後工程におけるコンテンツ暗号化等おいて一方

向性変換識別情報EMIDを用いることができ、当該後工程において秘密識別情報SecretIDが漏洩することを防止することが可能となり、秘密識別情報SecretIDの秘匿性を強化することができる点で、更に有利である。詳細については、後述する。

【０１５９】

［第３の実施形態］

次に、第３の実施形態について説明する。第３の実施形態は、ＮＡＮＤ型フラッシュメモリ１０が、ホスト装置２０を認証する一例に関するものである。本実施形態では、ＮＡＮＤ型フラッシュメモリ１０に記録されている秘密識別情報SecretIDを第三者から秘匿した状態で読み出すと共に、ＮＡＮＤ型フラッシュメモリ１０から読み出されたデータであることを確実に判定する方法、また読みだされたデータに基づいてＮＡＮＤ型フラッシュメモリ１０がホスト装置２０を検査する方法を示すものである。

【０１６０】

この説明において、上記実施形態と重複する部分の説明については、省略する。

【０１６１】

＜メモリシステム＞

図１３を用い、第３の実施形態に係るメモリシステムについて説明する。

図示するように、本実施形態では、ＮＡＮＤ型フラッシュメモリ１０が、機能コントロール部１８、乱数生成器２４ｎ、及びデータ検証部２８ｎを更に備える。また、ホスト装置２０が、機能呼び出し部３０を更に備える点で、上記第１の実施形態と相違する。

【０１６２】

乱数生成部（RNG: Random Number Generator）２４ｎは、認証に用いる乱数RN_nを生成する。

【０１６３】

データ検証部（Verify）２８ｎは、ホスト装置２０から受信した一方向性変換識別情報Oneway-IDとＮＡＮＤ型フラッシュメモリ１０装置内の一方向性変換器１５から得られた一方向性変換識別情報を比較して判定する。両方の値が一致した場合にはホスト装置２０が正しいOneway-IDを得ている（OK）、不一致の場合には正しいOneway-IDを得ていない（NG）と判定する。

【０１６４】

機能コントロール部（Function Control Unit）１８は、ホスト装置２０が正しいOneway-IDを得た場合（OK）にのみ、ＮＡＮＤ型フラッシュメモリ１０の所定機能をホスト装置２０に対して利用可能とするように、所定機能のイネーブルをメモリセルアレイ１１に行う。また、ホスト装置２０から受領した定数HC_jを機能コントロール部１８に入力させ、定数HC_jに応じて所定機能の制御を実施してもよい。ここで、所定機能については別途後述する。

【０１６５】

機能呼び出し部３０は、ホスト装置２０が生成した一方向性変換識別情報Oneway-IDの正当性をＮＡＮＤフラッシュメモリ１０が確認したことを示すアクセス許可情報（Access Permission）をホスト装置２０が受領すると、ＮＡＮＤ型フラッシュメモリ１０の所定機能を呼びだすための処理を行う。

【０１６６】

＜認証フロー＞

次に、図１４に沿って、第３の実施形態に係るメモリシステムの認証フローについて説明する。

【０１６７】

（Step Ｓ１１）－（Step Ｓ１４）

図示するように、まず認証開始（Start）から上記ステップＳ１１－Ｓ１４は、第１の実施形態と同様の処理を行う。

【０１６８】

（Step Ｓ５１）

続いて、ホスト装置２０は、インデック情報iを受け取ると、乱数発生要求（Request RN_n）をＮＡＮＤ型フラッシュメモリ１０に対して送出する。

【０１６９】

（Step Ｓ５２）

続いて、ＮＡＮＤ型フラッシュメモリ１０は、上記要求を受け、乱数生成部２４ｎにより乱数RN_nを生成する。生成された乱数RN_nは、ホスト装置２０に送出される。

【０１７０】

（Step Ｓ２１）－（Step Ｓ２３）

続いて、ホスト装置２０は、第１の実施形態と同様のステップＳ２１－Ｓ２３を行う。

【０１７１】

（Step Ｓ５３）

続いて、ホスト装置２０は、ＮＡＮＤ型フラッシュメモリ１０に対して、認証要求（Request authentication）を行い、定数HC_j、及び一方向性変換識別情報Oneway-IDを送出する。

【０１７２】

（Step Ｓ１７）－（Step Ｓ２０）

上記同様のステップＳ１７－Ｓ１９に続いて、Ｓ２０の際に、ＮＡＮＤ型フラッシュメモリ１０は、生成したセッション鍵$SKey_{i,j}$を用いて、秘密識別情報SecretIDに上記一方向性変換器１５における一方向性変換処理を行い、一方向性変換識別情報Oneway-ID (=Oneway($SKey_{i,j}$, SecretID))を生成する。

【０１７３】

（Step Ｓ５４）

続いて、ＮＡＮＤ型フラッシュメモリ１０は、受信した一方向性変換識別情報Oneway-IDと、自身が生成した一方向性変換識別情報が一致することを確認する。一致した場合（OK）には前記SecretIDが正規のIDであると判定し、不一致の場合（NG）には前記SecretIDが不正なIDであると判定し、判定結果をホスト装置２０に返送するとともに、所定機能の呼び出し受付を許可（Permission）する。

【０１７４】

（Step Ｓ５５）

続いて、ＮＡＮＤ型フラッシュメモリ１０は、上記Ｓ５４の際の判定結果が一致した場合（OK）に、機能コントロール部１８において、ＮＡＮＤ型フラッシュメモリ１０の所定機能をホスト装置２０に対して利用可能とするように、所定機能のイネーブル（有効化）を行う。

【０１７５】

（Step Ｓ５６）

続いて、ホスト装置２０は、機能呼び出し部３０において、ホスト装置２０が生成した一方向性変換識別情報Oneway-IDの正当性をＮＡＮＤフラッシュメモリ１０が確認したことを示すアクセス許可情報（Access Permission）をホスト装置２０が受領すると、ＮＡＮＤ型フラッシュメモリ１０の所定機能を呼びだすための命令を返信する。

【０１７６】

（Step Ｓ５７）

続いて、ＮＡＮＤ型フラッシュメモリ１０は、機能の呼び出しを受け、機能コントロール部１８において、ホスト装置２０から受領した機能呼び出し命令に従った処理を行い、処理結果のステータス（Status）を返送する。

【０１７７】

なお、この際、ホスト装置２０から受領した定数HC_jを機能コントロール部１８に入力させ、定数HC_jに応じて所定機能の制御を実施してもよい。所定機能については別途後述する。

【０１７８】

＜作用効果＞

第３の実施形態に係る認証装置、被認証装置及び認証方法によれば、少なくとも第１の実施形態と同様の作用効果（１）乃至（３）を得ることができる。更に、少なくとも下記の作用効果（４）及び（５）を得ることが可能である。

【０１７９】

（４）ＮＡＮＤ型フラッシュメモリ１０が、ホスト装置２０を認証できる。

【０１８０】

第３の実施形態では、ＮＡＮＤ型フラッシュメモリ１０が、機能制御部１８、乱数生成器２４ｎ、及びデータ検証部２８ｎを更に備える。また、ホスト装置２０が、機能呼び出し部３０を更に備える点で、上記第１の実施形態と相違する。

【０１８１】

そのため、上記構成によれば、ＮＡＮＤ型フラッシュメモリ１０に対し、ホスト装置２０がアクセスする際に、当該ホスト装置２０が信頼に足る場合にのみ、ＮＡＮＤ型フラッシュメモリ１０は所定の機能を提供する等の認証機能の制御が可能となる。

【０１８２】

このように、本実施形態によれば、必要に応じて、通常、被認証装置となる場合が多いＮＡＮＤ型フラッシュメモリ等の記録メディアが、逆にホスト装置２０を認証できる点で有利である。

【０１８３】

（５）認証したホスト装置２０の固有情報（定数HC_j等）に応じて、所定の機能を提供するか否かを更に制御するような機構を設けることが可能となる点で有利である。所定の機能の詳細については、後述する。

【０１８４】

［第４の実施形態（相互認証）］

次に、第４の実施形態について説明する。第４の実施形態は、ＮＡＮＤ型フラッシュメモリ１０と、ホスト装置２０とがそれぞれ相互に認証し合う一例に関するものである。

【０１８５】

この説明において、上記実施形態と重複する部分の説明については、省略する。

【０１８６】

＜メモリシステム＞

図１５を用い、第４の実施形態に係るメモリシステムについて説明する。

図示するように、本実施形態では、上記第１の実施形態に係るメモリシステムと第３の実施形態に係るメモリシステムとを実質的に組み合わせた構成を備える。

【０１８７】

より具体的には、ＮＡＮＤ型フラッシュメモリ１０、ホスト装置２０が、乱数発生部２４ｎ、２４ｈ、生成部１４－２、２６－２、一方向性変換器１５－２、２６－２、データ検証部２８ｎ、２８ｈを備える。更に、ホスト装置２０が、スイッチ部２９Ｂを更に備える点で、上記第３の実施形態と相違する。

【０１８８】

上記各構成の動作については、上記実施形態と同様である。

【０１８９】

＜認証フロー＞

次に、図１６に沿って、第４の実施形態に係るメモリシステムの認証フローについて説明する。本実施形態に係る認証フローは、原則的には、上記第１の実施形態に係る認証動作（ホスト装置がＮＡＮＤ型フラッシュメモリを認証する）を行った後、上記第３の実施形態に係る認証動作（ＮＡＮＤ型フラッシュメモリがホスト装置を認証する）を行うものである。

【０１９０】

（Step Ｓ１１）－（Step Ｓ２４）

図示するように、まず認証開始（Start）すると、上記第１の実施形態と同様のステップＳ１１－Ｓ２４を行い、ホスト装置２０がＮＡＮＤ型フラッシュメモリ１０の認証を行

う。
【０１９１】
この際、乱数生成部２４ｈから生成される乱数RN_hを用いて、同様の認証を行う。
【０１９２】
（Step Ｓ５１）－（Step Ｓ７０）
続いて、上記ステップＳ２４の際の検証結果が一致した場合（OK）、ＮＡＮＤ型フラッシュメモリ１０の認証が完了したと判断する。
【０１９３】
続いて、上記第３の実施形態と同様のステップＳ５１－Ｓ７０を行い、ＮＡＮＤ型フラッシュメモリ１０がホスト装置２０の認証を行う。
【０１９４】
この際、乱数生成部２４ｎから生成される乱数RN_nを用いて、同様の認証を行う。
【０１９５】
以上のステップにより、第４の実施形態に係る認証動作を終了する（End）。
【０１９６】
＜機能制御の構成例＞
次に、図１７を用い、機能制御の構成例について説明する。
【０１９７】
ここで、機能制御とは、ＮＡＮＤ型フラッシュメモリ１０が認証装置であり、ホスト装置２０が被認証装置である場合、すなわちＮＡＮＤ型フラッシュメモリ１０がホスト装置２０を認証し、認証結果に基づいてホスト装置２０に対して所定機能を提供する上記第３、第４の実施形態に係る所定機能の制御方法をいう。
【０１９８】
図示する機能制御の構成は、後述するようにＮＡＮＤ型フラッシュメモリ１０がそれぞれ備えるものである。機能制御は、認証回路１７に備える機能コントロール部１８、パラメータレジスタ８９、及びシーケンス制御回路８８を備える。
【０１９９】
認証回路１７内に含まれる上記機能コントロール部（Function Control Unit）１８は、認証結果、また必要に応じたホスト装置２０の固有情報（定数HC_j等）に基づき、ホスト装置２０に対して所定機能を提供するための機能制御をおこなう。機能コントロール部（Function Control Unit）１８は、パラメータレジスタ８９に含まれる制御パラメータ８９０を、ホスト装置２０の認証結果や固有情報に基づき、更新を行う。
【０２００】
パラメータレジスタ８９が有する制御パラメータ８９０には、一つ以上のアクセス許可情報（＃０、＃１、、、＃３）が含まれる。例えば、アクセス許可情報＃０には、ブロックアドレス、ページアドレス、読み出し属性、書き込み属性、消去属性、固有情報等が含まれる。ここで、ブロックアドレスは、当該ブロックアドレスのメモリセルアレイ１１に対する制御を示す。ページアドレスは、当該ページアドレスのメモリセルアレイ１１に対する制御を示す。読み出し属性は、ブロックアドレス、若しくはブロックアドレス及びページアドレスに対する読み出し許可情報を示す。書き込み属性は、ブロックアドレス、若しくはブロックアドレス及びページアドレスに対する書き込み許可情報を示す。消去属性は、ブロックアドレス、若しくはブロックアドレス及びページアドレスに対する消去許可情報を示す。固有情報は、当該アクセス許可情報が同固有情報を有するホスト装置２０に対する制御パラメータであることを示す。
【０２０１】
なお、アクセス許可情報（＃０、＃１、、、＃３）のそれぞれは、上記情報のすべてを含んでいる必要はなく、必要とされる制御レベルに応じた情報を含んでいればよい。例えば、ホスト装置２０の固有情報（定数HC_j等）に基づいた制御が必要なければ固有情報はなくてもよい。また、ページ単位での制御が不要であればページアドレスはなくてもよい。更に、任意のブロックアドレスでの制御が不要であり、例えばあらかじめ定められたブ

ロックのみに対する制御や、ＮＡＮＤ型フラッシュメモリ１０全体としての制御であれば、ブロックアドレスもなくてもよい。同ように、読み出し属性、書き込み属性、消去属性についても、制御が必要とされる機能についてのみ含んでいればよい。

【０２０２】

シーケンス制御回路８８は、制御パラメータ８９０に従って、ホスト装置２０から与えられるコマンド（CMD）に応じた動作シーケンスを制御する。例えば、データ読み出しコマンドの場合、シーケンス制御回路８８は、制御パラメータ８９０中のアクセス許可情報の読み出し属性に従って、与えられる読み出しコマンドに応じたデータ読み出す（Read）もしくは読み出しを拒否するなどの動作を制御する。読み出し属性において読出しが許可されていれば、セルアレイ１１からデータを読み出すことが可能となる。その他、データ書き込み動作、データ消去動作等についても同様である。

【０２０３】

＜作用効果＞

第４の実施形態に係る認証装置、被認証装置及び認証方法によれば、少なくとも上記と同様の作用効果（１）乃至（５）を得ることができる。

【０２０４】

本実施形態によれば、必要に応じて、ＮＡＮＤ型フラッシュメモリ１０とホスト装置２０とがそれぞれ相互に認証することが可能である。

【０２０５】

更に、本実施形態に係るＮＡＮＤ型フラッシュメモリ１０は、図１７に示した構成による機能制御を実現する。シーケンス制御回路８８は、制御パラメータ８９０に従って、与えられるコマンドに応じた動作シーケンスを制御することができる。そのため、ＮＡＮＤ型フラッシュメモリ１０が認証したホスト装置２０において、そのホスト装置２０の固有情報（定数HC_j等）等に基づいて、制御パラメータ８９０を更新した各種の機能動作を行うことをホスト装置２０に許可すること（Process function）ができる点で有利である。

【０２０６】

さらに、本例に係るＮＡＮＤ型フラッシュメモリ１０は、図１７に示した構成の機能制御を第３の実施形態及び第４の実施形態とともに備えることが可能である。

【０２０７】

［第５の実施形態（ＮＡＮＤ型フラッシュメモリの構成例）］

次に、第５の実施形態について説明する。第５の実施形態は、上記第１至第４の実施形態に係る認証機能を適用したＮＡＮＤ型フラッシュメモリ１０の構成例に関するものである。

【０２０８】

この説明において、上記実施形態と重複する部分の説明については、省略する。

【０２０９】

＜ＮＡＮＤ型フラッシュメモリの全体構成例＞

図１８を用い、第５の実施形態に係るＮＡＮＤ型フラッシュメモリ１０の全体構成例について説明する。

図示するように、ＮＡＮＤ型フラッシュメモリ１０は、メモリセルアレイ１１及びその周辺回路を備える。

【０２１０】

メモリセルアレイ１１は、複数のブロックBLOCK1- BLOCKnを含む。各ブロックの構成は、図１９において後述するが、複数のメモリセルトランジスタＭＣ、ワード線ＷＬ、ビット線ＢＬ等を含むものである。各ブロック中のメモリセルトランジスタＭＣ中のデータは、一括して消去される。メモリセルトランジスタ単位及びページ単位でのデータ消去はできない。すなわち、個々のブロックが最小の消去単位となる。

【０２１１】

周辺回路は、センスアンプ７７、入出力制御回路８４、ロジックコントロール回路８５等を備える。

【０２１２】
センスアンプ７７は、ビット線ＢＬを介してメモリセルアレイ１１内のメモリセル（メモリセルトランジスタＭＣ）のデータを読み出し、ビット線ＢＬを介してメモリセルアレイ２内のメモリセルの状態を検出する。
【０２１３】
データキャッシュ１２は、センスアンプ７７から読み出されたデータまたはセンスアンプ７７に供給されるデータを一時的に保持する。
【０２１４】
カラムデコーダ７５は、ＮＡＮＤ型フラッシュメモリ１０の外部からＩＯ端子を介して供給されたアドレス信号に基づいて、特定のビット線ＢＬ、センスアンプ等を選択する。
【０２１５】
カラムアドレスバッファ７４は、アドレス信号を一時的に保持し、カラムデコーダ７５に供給する。
【０２１６】
ロウデコーダ７８は、データ読み出し、書き込み、あるいは消去に必要な種々の電圧を電圧生成回路８６から受け取り、そのような電圧をアドレス信号に基づいて特定のワード線ＷＬに印加する。
【０２１７】
ロウアドレスバッファデコーダ７９は、アドレス信号を一時的に保持し、ロウデコーダ７８に供給する。
【０２１８】
電圧生成回路８６は、基準電源電圧ＶＳＳ、ＶＣＣ、電圧ＶＳＳＱ、ＶＣＣＱ等を受け取り、これらからデータ書き込み、読み出し、消去等に必要な電圧を生成する。
【０２１９】
入出力制御回路８４は、ＩＯ端子を介して、ＮＡＮＤ型フラッシュメモリ１０の動作を制御する種々のコマンド、アドレス信号、書き込みデータを受け取り、また読み出しデータを出力する。入出力制御回路８４から出力されたアドレス信号は、アドレスレジスタ８２によってラッチされる。ラッチされたアドレス信号は、カラムアドレスバッファ７４及びロウアドレスバッファ７９に供給される。入出力制御回路８４から出力されたコマンドは、コマンドレジスタ８３によってラッチされる。ステータスレジスタ８１は、入出力制御回路１２のための種々のステータスについての値を保持する。
【０２２０】
ＮＡＮＤ型フラッシュメモリ１０は、外部インターフェイス（ＮＡＮＤ　Ｉ／Ｆ）として、コマンド、アドレス、データ入出力用のＩＯ端子、動作を制御するための種々の制御信号を外部から受け取る。制御信号には、例えばチップイネーブル／ＣＥ、コマンドラッチイネーブルＣＬＥ、アドレスラッチイネーブルＡＬＥ、リードイネーブルＲＥ及び／ＲＥ、ライトイネーブルＷＥ及び／ＷＥ、ライトプロテクトＷＰ、クロックＤＱＳ、／ＤＱＳが含まれる。
【０２２１】
これらの制御信号は、対応する端子において受け取られ、ロジック制御回路２１に供給される。ロジックコントロール回路８５は、制御信号に基づいて、入出力制御回路８４を制御して、端子ＩＯ上の信号をコマンド、アドレス、またはデータとして入出力制御回路８４を介してアドレスレジスタ８２、コマンドレジスタ８３、ページバッファ１２等に到達することを許可したり禁止したりする。また、ロジックコントロール回路８５は、コマンドレジスタ８３から、ラッチされたコマンドを受け取る。
【０２２２】
制御信号のうち、ＷＥ端子はデータ入力用クロックを供給し、ＲＥ端子はデータ出力用クロックを供給し、ＤＱＳ端子はデータ入出力用クロックを伝送し、ＣＬＥ端子はデータ入力をコマンドとして入力するイネーブル用であり、ＡＬＥ端子はデータ入力をアドレスとして入力するイネーブル用であり、ＣＥ端子はデータ入出力等全般の機能を有効化する

ためである。
【０２２３】
また、Ｒ／Ｂ端子はＮＡＮＤ型フラッシュメモリ１０の内部動作状態を示し、ＷＰ端子は誤書き込み防止用の書き込み防止信号を伝送し、Ｖｃｃ／Ｖｓｓ／Ｖｃｃｑ／Ｖｓｓｑ端子等は電力供給用である。また、本実施形態では、高速インターフェースにてデータ伝送を実現する際に利用される端子（Toggle）として、ＲＥ端子、ＷＥ端子、ＤＱＳ端子には、各々相補信号を伝送する／ＲＥ端子、／ＷＥ端子、／ＤＱＳ端子が存在する。
【０２２４】
ロジックコントロール回路８５は、シーケンス制御回路８８、パラメータレジスタ８９、認証回路１７を備える。ロジック制御回路８５は、また、レディ／ビジー信号（Ｒ／Ｂ）の出力を司る。具体的には、ロジック制御回路８５は、ＮＡＮＤ型フラッシュメモリ１０がビジー状態の間、ビジー信号を出力する。
【０２２５】
シーケンス制御回路８８は、コマンドレジスタ８３からコマンドを受け取る。シーケンス制御回路８８は、受け取ったコマンドに基づいて、コマンドにより指示される処理（データ読み出し、書き込み、消去等）を実行するように、センスアンプ７７、電圧生成回路８６等を制御する。
【０２２６】
パラメータレジスタ８９は、ロジック制御回路８５の動作を規定する種々の上記制御パラメータ８９０等を保持する。制御パラメータ８９０は、シーケンス制御回路８８から参照、または更新され、ロジックコントロール回路８５や入出力制御回路８８におけるシーケンスの制御に利用される。
【０２２７】
認証回路１７は、上記の認証に関する処理を行う。例えば、認証回路１７は、上記のように、パラメータレジスタに含まれる制御パラメータ８９０の書き換え等の更新も行う。また、認証回路１７は、認証を要求するコマンドを受け取り、メモリセルアレイ１１中の特定のデータを用いて認証のための特定の演算を行い、結果をメモリ１０の外部へ出力する。この一連の動作の実行の過程で、認証回路１７は、必要なデータの読み出し、書き込み等を制御パラメータ８９０の更新を通じて、シーケンス制御回路８８に許可する。
【０２２８】
レディ／ビジー回路（RY/BY）８７は、ロジックコントロール回路８５の制御を受けて、スイッチトランジスタを介して、Ｒ／Ｂ信号をＮＡＮＤ型フラッシュメモリ１０の外部に通知する。
【０２２９】
＜ブロック（ＢＬＯＣＫ）の構成例＞
次に、図１９を用い、メモリセルアレイ１１を構成するブロック（ＢＬＯＣＫ）の構成例について説明する。ここでは、図１８中のＢＬＯＣＫ１を一例に挙げて説明する。ここで、上記のように、ブロックＢＬＯＣＫ１中のメモリセルは、一括してデータ消去されるため、ブロックはデータ消去単位である。
【０２３０】
ブロックＢＬＯＣＫ１は、ワード線方向（ＷＬ方向）に配置される複数のメモリセルユニットＭＵから構成される。メモリセルユニットＭＵは、ＷＬ方向と交差するビット線方向（ＢＬ方向）に配置され、電流経路が直列接続される８個のメモリセルＭＣ０～ＭＣ７からなるＮＡＮＤス通りング（メモリセルストリング）と、ＮＡＮＤストリングの電流経路の一端に接続されるソース側の選択トランジスタＳ１と、ＮＡＮＤストリングの電流経路の他端に接続されるドレイン側の選択トランジスタＳ２とから構成される。
【０２３１】
なお、本実施形態では、メモリセルユニットＭＵは、８個のメモリセルＭＣ０～ＭＣ７から構成されるが、２つ以上のメモリセル、例えば、５６個、３２個等から構成されていればよく、８個に限定されるというものではない。

【０２３２】
ソース側の選択トランジスタＳ１の電流経路の他端はソース線ＳＬに接続される。ドレイン側の選択トランジスタＳ２の電流経路の他端は、各メモリセルユニットＭＵに対応してメモリセルユニットＭＵの上方に設けられ、ＢＬ方向に延出するビット線ＢＬに接続される。
【０２３３】
ワード線ＷＬ０～ＷＬ７は、ＷＬ方向に延び、ＷＬ方向の複数のメモリセルの制御ゲート電極ＣＧに共通に接続される。選択ゲート線ＳＧＳは、ＷＬ方向に延び、ＷＬ方向の複数の選択トランジスタＳ１に共通に接続される。選択ゲート線ＳＧＤも、ＷＬ方向に延び、ＷＬ方向の複数の選択トランジスタＳ２に共通に接続される。
【０２３４】
また、ワード線ＷＬ０～ＷＬ７毎にページ（ＰＡＧＥ）が存在する。例えば、図中の破線で囲って示すように、ワード線ＷＬ７には、ページ７（ＰＡＧＥ７）が存在する。このページ（ＰＡＧＥ）毎に、データ読み出し動作、データ書き込み動作が行われるため、ページ（ＰＡＧＥ）はデータ読み出し単位であり、データ書き込み単位である。
【０２３５】
＜セルアレイの構成例＞
次に、図２０を用い、メモリセルアレイ１１の構造を示す。
（ａ）に示すように、メモリセルアレイ１１内部は、ノーマルブロック１１－１、秘匿ブロック１１－２、ロムブロック１１－３、ロムヒューズブロック１１－４、保護ブロック１１－５等の上記複数のブロック（BLOCK）から構成される。各ブロックは、上記のように、複数のページから構成される。通常、データの読み出しや書き込みはページ単位で行い、消去はブロック単位で行われる。
【０２３６】
ノーマルブロック１１－１は、上記のように、データの書き込み、読み出し等いずれも許可され、通常のデータ保持用に用いられる。ノーマルブロックは、上述した読み書き可能領域１１－１に対応する。ブロック数は特に限定されない。
【０２３７】
秘匿ブロック１１－２及びロムブロック１１－３は、上記のような認証動作に適用される。秘匿ブロック１１－２は、上述した秘匿領域１１－２に対応する。ロムブロック１１－３は、上述したロム領域１１－３に対応する。何れもブロック数は特に限定されない。
【０２３８】
（ｂ）に示すように、本実施形態では、ロムブロック１１－３のメモリ空間には、読み出し専用データが更に記録される。
【０２３９】
（ｃ）に示すように、本実施形態では、秘匿ブロック１１－２のメモリ空間には、秘匿データが更に記録される。
【０２４０】
（ｄ）に示すように、本実施形態では、保護ブロック１１－５のメモリ空間には、後述する認証機能により利用される保護データが更に記録される。
【０２４１】
ロムヒューズブロック１１－４は、例えば、ＮＡＮＤ型フラッシュメモリ１０の動作制御用のパラメータ保持等に用いられる。
【０２４２】
＜ロムブロック内の読み出し専用データ＞
次に、図２１を用い、ロムブロック１１－３内の読み出し専用データについて説明する。
（ａ）に示すように、ロムブロック１１－３のメモリ空間のあるページには、読み出し専用データが記録されている。ここで、読み出し専用データＡからＺの系列とした場合、本図ではデータのエラー訂正を目的にした（ｂ－１）－（ｂ－３）の３つの例を示す。

【０２４３】
（ｂ－１）に示すように、第１のデータパターン１は、同一のデータ（Ａ、Ａ、、、Ｂ、Ｂ、、、）を繰り返し記録する例である。この場合、繰り返し読み出し専用データをホスト装置２０が読み出し、ホスト装置２０等が有するエラー訂正部において、多数決判定を行うことで、エラー訂正が可能である。または、繰り返し読み出し専用データをコントローラ１９が読み出し、コントローラ１９等が有するエラー訂正部において、多数決判定を行うことで、エラー訂正が可能である。または、繰り返し読み出し専用データをＮＡＮＤ型フラッシュメモリ１０が有するエラー訂正部において、多数決判定を行うことで、エラー訂正が可能である。例えば、繰り返し回数は１６回程度以上あることが望ましい。
【０２４４】
（ｂ－２）に示すように、第２のデータパターン２は、各データ（Ａ、Ｂ、、、）とその反転データ（Ａの反転、Ｂの反転、、、）からなる相補データペアを繰り返し記録する例である。この場合、繰り返し読み出し専用データをホスト装置２０が読み出し、ホスト装置２０等が有するエラー訂正部において相補データペアに配慮した多数決判定を行うことで、エラー訂正が可能である。または、繰り返し読み出し専用データをコントローラ１９が読み出し、コントローラ１９等が有するエラー訂正部において相補データペアに配慮した多数決判定を行うことで、エラー訂正が可能である。または、繰り返し読み出し専用データをＮＡＮＤ型フラッシュメモリ１０が有するエラー訂正部において相補データペアに配慮した多数決判定を行うことで、エラー訂正が可能である。
【０２４５】
ここで、相補データペアとして繰り返し記録する理由は、ＮＡＮＤ型フラッシュメモリ１０のエラーモードによる。ＮＡＮＤ型フラッシュメモリ１０はメモリセルＭＣに対して所定電圧を印加することによってフローティングゲートＦＧに電子を注入し、データの書き込みを行う。データの読み出しは当該メモリセルＭＣのフローティングゲートＦＧに電子が存在しているか否かによって変化する閾値電圧を用いて行う。データの消去は書き込みと逆方向に電圧を印加し、フローティングゲートＦＧから基板へ電子を引き抜くことで実行する。データ読み出し、書き込み、消去の動作に伴う電圧印加量や電圧印加ゲートは各々異なるが、いずれにおいてもメモリセルＭＣにおいて電圧を印加する。この原理に起因して、ＮＡＮＤ型フラッシュメモリ１０の代表的なエラーモードとして、リード・プログラムディスターブ、データリテンションがある。リード・プログラムディスターブは、自身若しくは隣接のページを繰り返し読み出す、若しくは隣接ページに書き込むことによって、フローティングゲートＦＧにおける電子量が変化することデータが変化するエラーモードである。このため弱書き込みに近い状態となり、一般に閾値電圧が増加する。データリテンションとは、一度書き込んだページを長時間放置することによって、フローティングゲートに保持されていた電子が抜け落ちることにより、データが変化するエラーモードである。このため、弱消去に近い状態となり、一般に閾値電圧が低下する。すなわち、これら不良モードにおいては全般的に増加するか、低下するかの傾向があることから、データは同一方向にエラーする可能性が高い。
【０２４６】
そこで、（ｂ－２）に示すように、相補データとして記録することにより、仮にデータが１（未記録状態）であった場合その反転データは０（記録状態）であることから、リード・プログラムディスターブにおいては両データとも０方向に移行し、データリテンションにおいては逆に１方向に移行する。このため、少なくともエラーが発生しているか否かは相補データである方が判別しやすい。この場合、例えば、相補データペアとして少なくとも８回程度の繰り返しがあることが望ましい。
【０２４７】
（ｂ－３）に示すように、第３のデータパターン３は、読み出し専用データ（Ａ、Ｂ、、、Ｚ）に更に誤り訂正符号を用いる例である。ここで、誤り訂正符号としては、ＮＡＮＤ型フラッシュメモリ１０のエラー発生形式がビット単位でのランダムエラーであることから、ランダムビットエラーが訂正可能な例えば、ＢＣＨ符号やＬＤＰＣ符号等が望まし

い。
【０２４８】
ここで、第１乃至第３のデータパターンのいずれの例においても、各データはランダマイズされていてもよい。ランダマイズとは、データの偏りをなくすために、発生させたランダム系列と記録するデータとの排他的論理和をとる等の方法で、記録するデータをランダム化することである。ランダム系列の発生方法としては、M系列等を用いてもよい。
【０２４９】
加えて、第１乃至第３のデータパターンのいずれの例においても、各データは２値状態として記録されていてもよい。２値状態とは、一つのメモリセルにおける閾値電圧を所定の１レベルを基準にして高いレベルに属するか低いレベルに属するかを定めてデータを記録する方法であり、1メモリセル当たり1ビットの情報を保持することができる。このような記録方法は一般にＳＬＣ（Single Level Cell）記録と呼ぶ。一方で、一つのメモリセルにおける閾値電圧を所定の複数レベルを基準にして、どのレベルに属するかを定めてデータを記録する方法であり、1メモリセル当たり複数ビットの情報を保持することができる。前記属するレベルを例えば、4つ設けてデータを記録する場合、1メモリセル当たり2ビットの情報を保持することができる。このような記録方法は一般にＭＬＣ（Multi Level Cell）記録と呼ばれる。ＭＬＣ記録は1セルあたりの記録容量が多いため、より高い記録密度を実現できるが、一方で閾値電圧のずれに対して記録データ変化が比較的おこりやすい。このことから、前記ロムブロック１１－３に記憶される読み出し専用データは、通常データよりも1セルあたりのビット数を少なく記録する方が望ましい。例えば、1セルあたりのビット数が2ビットで構成される4 Ｌｅｖｅｌ記録のＭＬＣである場合、ＲＯＭデータはＳＬＣ記録の方が望ましい。また、1セルあたりのビット数が4ビットで構成される8 Ｌｅｖｅｌ記録のＭＬＣである場合、ＲＯＭデータは1セルあたりのビット数が2ビットで構成される4 Ｌｅｖｅｌ記録のＭＬＣ若しくはＳＬＣ記録の方が望ましい。
【０２５０】
＜ＥＣＣの構成例＞
次に、誤り訂正符号化（ＥＣＣ：Error Correcting Code）の構成例について説明する。
【０２５１】
ここで、上記図２１で示した、第１乃至第３のデータ構造は、厳密には異なるものの、元となるデータに対して冗長語を付与しているという意味合いでは、広義には訂正符号化ＥＣＣととれる。そのため、ここでは、いずれのデータ構造においてもデータと、それに付与された訂正符号と称する。ホスト装置２０、コントローラ１９、若しくはＮＡＮＤ型フラッシュメモリ１０の少なくともいずれかが対応する訂正機能を有する必要がある。
【０２５２】
図２２で示す第１の例は、ホスト装置２０が訂正機能（ECC decode）９０を有する例である。この場合、コントローラ１９及びＮＡＮＤ型フラッシュメモリ１０は、訂正処理を行わず、符号付きのデータ（Data）をホスト装置２０に渡し、ホスト装置２０は訂正機能（ECC decode）９０により訂正処理を行い、所定のデータ（Data）を生成する。
【０２５３】
図２３で示す第２の例は、コントローラ１９が、訂正機能（ECC decode）９０を有する例である。この場合、ＮＡＮＤ型フラッシュメモリ１０は、訂正処理を行わず、コントローラ１９は訂正処理を行い、訂正済みのデータ（Data）をホスト装置２０に渡す。
【０２５４】
図２４で示す第３の例は、ＮＡＮＤ型フラッシュメモリ１０が、訂正機能（ECC decode）９０を有する例である。この場合、ＮＡＮＤ型フラッシュメモリ１０は訂正処理を行い、訂正済みのデータ（Data）をコントローラ１９を経由してホスト装置２０に渡す。
【０２５５】
図２５で示す第４の例は、コントローラ１９及びホスト装置２０の両方が訂正機能９０－１、９０－２を有する例である。この場合は、まず付与されている訂正符号が２重構造

をとっており、内符号（Inner code）及び外符号（Outer code）のいずれかを各々コントローラ１９とホスト装置２０とが訂正処理を行う。

【０２５６】

なお、上記の場合に限らず、ＮＡＮＤ型フラッシュメモリ１０、コントローラ１９、ホスト装置２０は、各々自身の訂正機能に応じて協調しつつ訂正を行うことが可能である。

【０２５７】

＜秘匿ブロック１１－２内の秘匿データ＞

次に、図２６を用い、秘匿ブロック１１－２内の秘匿データの保持状態の例を説明する。

【０２５８】

（ａ）に示すように、秘匿ブロック１１－２内のメモリ空間には、ページに秘匿データが記録されている。ここで、秘匿データをＡからＺの系列とした場合、本図では3つの例を示す。

【０２５９】

（ｂ－１）に示すデータパターン１では、複数の秘匿データ（Ａ、Ａ、、、Ｂ、Ｂ、、、）及びアクセス制御パターンＢ１を記憶する。

【０２６０】

（ｂ－２）に示すデータパターン２では、複数の秘匿データ（Ａ、Ａ、、、Ｂ、Ｂ、、、）とその反転データ、及びアクセス制御パターンＢ２を記憶する。

【０２６１】

（ｂ－３）に示すデータパターン３では、複数の秘匿データ（Ａ、Ｂ、、、、Ｚ）、エラー訂正符号、及びアクセス制御パターンＢ３を記憶する。

【０２６２】

各例における目的の一つは、同ようにエラー訂正である。他の目的は秘匿ブロック１１－２若しくは当該ブロック１１－２内のページに対する読み出し、書き込み、消去に関わる制御をおこなうことである。当該領域は秘匿データを記録していること、また前述の認証回路１７においてＮＡＮＤ型フラッシュメモリ１０の内部でのみ利用する情報を保持することから、外部からの読み出し、書き込み、消去に関わる動作は全て禁止しておく必要がある。一方で、ＮＡＮＤ型フラッシュメモリ１０の製造初期段階においては、同領域は未記録であることから、製造のいずれかの段階において秘匿データを記録しなければいけない。更に、ＮＡＮＤ型フラッシュメモリ１０のメモリセルの特性として、メモリセルの初期状態ではデータ保持性能が不十分である場合があるため、当該メモリセルがデータを仕様通りに保持できるか否かを検査するために、読み出し、書き込み、消去の動作をさせる必要がある。

【０２６３】

そこで、同領域１１－２に関し、製造段階においては読み出し、書き込み、消去が可能であるが、製造完了後の出荷時においては、同領域は読み出し、書き込み、消去の全てを禁止しておく必要がある。この状態変更を行うための情報として、当該領域１１－２にアクセス制御パターンＢ１、Ｂ２、Ｂ３を記録する。

【０２６４】

アクセス制御パターンＢ１、Ｂ２、Ｂ３は、ページ毎に記録されていてもよいし、ブロック内の先頭ページのみに記録されていてもよい。また、ページ内でのアクセス制御パターンＢ１、Ｂ２、Ｂ３の記録位置は、一般データ領域であってもよいし、冗長領域であってもよい。ここで、冗長領域とはコントローラ等が訂正符号の付与に利用する領域や、若しくはNANDフラッシュメモリ１０が内部的なページ毎のステータス等を示すための情報を記録するのに利用する領域等である。

【０２６５】

秘匿データやアクセス制御パターンＢ１、Ｂ２、Ｂ３においても、ＲＯＭデータと同ように２値（ＳＬＣ）モードで記録される方が望ましい。

【０２６６】

次に、図２７を用い、アクセス制御パターンの構成例を示す。
まず、アクセス制御パターンは、エラーによる損失を防ぐため、少なくとも複数のビットから構成されている必要がある。
【０２６７】
一つ目の例のアクセス制御パターンＢ１は、複数の制御フラグビットＡからＺを設け、これら制御フラグビットを所定パターンとしておく。ＮＡＮＤ型フラッシュメモリ１０は、当該領域に対する読み出し、書き込み、消去等のアクセス要求をホスト装置２０より受けた場合、当該領域１１－２のアクセス制御パターンＢ１と所定パターンとの照合を行い、両者の一致率が所定率以上となった場合にアクセスを禁止する、という構成をとる。
【０２６８】
二つ目の例のアクセス制御パターンＢ２は、制御フラグを繰り返し記録しておく方法である。これは、所定パターンがエラーする確率を低下させる上で有効である。
【０２６９】
三つ目の例のアクセス制御パターンＢ３は、各制御フラグと各制御フラグの反転データを記録しておく方法である。前述の通り、本方法もエラーする確率を低下させる上で有効である。
【０２７０】
＜アクセス制御パターンの利用例＞
次に、アクセス制御パターンの検知方法及び検知結果の利用方法を説明する。
【０２７１】
図２８に示すように、メモリセルアレイ１１中の秘匿領域１１－２から読み出される上記アクセスパターンは、ロジックコントロール回路８５内のパターン検知回路９１に入力される。
【０２７２】
パターン検知回路９１は、入力されるアクセス制御パターンに対し、パターン認識処理を行い、一致率が所定確率以上であるか否かを判定し、アクセス制御をおこなう。一致率は、ＮＡＮＤ型フラッシュメモリ１０のメモリセルアレイにおけるエラー確率と、アクセス制御パターンのデータ量から計算され、例えば、誤検出確率が少なくとも10^{-3}以下となるように設定することが望ましい。パターン検知回路９１は、検知結果に基づき、データ読み出し、データ書き込み、データ消去を制御するためのイネーブル信号をシーケンス制御回路８８に入力する。
【０２７３】
シーケンス制御回路８８は、上記検知結果のイネーブル信号に従い、データ読み出し、データ書き込み、データ消去を制御する。
【０２７４】
＜テストフロー＞
次に、図２９に沿って、上記アクセス制御パターン（例えば、Ｂ１－Ｂ３）を用いたＮＡＮＤ型フラッシュメモリ１０の製造工程の検査フローを説明する。
【０２７５】
（Step Ｓ７１、Ｓ７２）
製造工程において、まず、アクセス制御パターンに該当しないデータを、秘匿領域１１－２に記録し、テストを行う。この段階では、秘匿領域１１－２のアクセスは許可されている。
【０２７６】
ただし、データ読み出し、データ書き込み、データ消去のすべてのアクセスを許可するのか、データ書き込み及びデータ消去を許可するか等、によりセキュリティーレベルが異なる。高いセキュリティーレベルが必要な場合、仮にアクセス制御パターンにより全てのアクセスを禁止したとしても、アクセス制御パターンのデータが劣化することにより、誤ったアクセス許可をする可能性がある。この場合、秘匿データが読みだされる恐れがあるため、このステップＳ７１の際のテスト工程においても、データ読み出しを禁止する、す

なわちＮＡＮＤ型フラッシュメモリ１０のハードワイヤードレベルにおいて読み出しを当該領域にはそもそも許可しない、という選択も可能である。

【０２７７】

または、アクセス制御パターンのデータ劣化耐性が十分である場合、例えば、アクセス制御パターンが多数回繰り返し記録されている、強固な誤り訂正符号が付与されている場合等においては、テストの利便性を確保するために、データ読み出しを含めた制御をアクセス制御パターンによっておこなってもよい。この場合、先に示した誤検出確率は更に低く、例えば、10^{-5}以下であることが望ましい。

【０２７８】

（Step Ｓ７３）

続いて、Ｓ７２の際の所定のテストが完了した後、秘匿領域１１－２に秘匿データ及びアクセス制御パターン（Ｂ１－Ｂ３等）が各々書き込まれる。

【０２７９】

（Step Ｓ７４）

続いて、上記のデータが書き込まれた状態で、ＮＡＮＤ型フラッシュメモリ１０が出荷される。

【０２８０】

＜データ消去フロー＞

次に、図３０に沿って、ＮＡＮＤ型フラッシュメモリ１０の内部のデータ消去動作を説明する。

【０２８１】

（Step Ｓ７６）

まず、ホスト装置２０より消去動作の動作命令が発効されると、ＮＡＮＤ型フラッシュメモリ１０は、当該命令における選択ブロックアドレスが特定ブロックであるか否かを判定する。

【０２８２】

（Step Ｓ７７）

続いて、選択ブロックアドレスが特定ブロックでない場合（No）、通常通りの消去シーケンスを行う。

【０２８３】

（Step Ｓ７８）

一方、選択ブロックアドレスが特定ブロックの場合（Yes）、秘匿領域１１－２からアクセス制御情報（Ｂ１－Ｂ３等）の読み出しを行う。

【０２８４】

（Step Ｓ７９）

続いて、アクセス制御情報（Ｂ１－Ｂ３等）のパターン検知を行い、パターン一致率が所定値以上であるか否かを判定する。

【０２８５】

（Step Ｓ８０）

続いて、パターン一致率が所定値以下であった場合（Yes）、通常通りの消去シーケンスを行う。

【０２８６】

（Step Ｓ８１）

続いて、パターン一致率が所定値以上であった場合（No）、消去シーケンスを抜け、データ消去フローを終了する（End）。

【０２８７】

なお、本実施形態では、データ消去を一例に挙げたが、同ようにデータ読み出し、データ書き込みにおいても適用可能である。

【０２８８】

＜作用効果＞

第５の実施形態に係る認証装置、被認証装置及び認証方法によれば、少なくとも上記と同様の作用効果（１）乃至（５）を得ることができる。

【０２８９】

更に、必要に応じて、本実施形態の構成及び方法を適用することで、信頼性を向上できる点で有効である。

【０２９０】

［第６の実施形態（データキャッシュの認証処理への利用の一例）］

第６の実施形態は、データキャッシュの認証処理への利用の一例に関するものである。この説明において、上記実施形態と重複する部分の説明については、省略する。

【０２９１】

＜データキャッシュ、センスアンプ等の構成例＞

図３１を用い、第６の実施形態に係るデータキャッシュ、センスアンプ等の構成例について説明する。

図示するように、上記実施形態に係る認証処理のデータキャッシュ１２が１コンポーネントとして示される。ＮＡＮＤ型フラッシュメモリ１０は、メモリセルアレイ１１から読み出したページデータを一時的に記憶する、また外部から記録用データとして受領した書き込みページデータを一時的に記憶する、等を目的とした揮発性データキャッシュ１２を有する。本実施形態のデータキャッシュ１２は、ページバッファ、データバッファ等とも呼ばれ、通常ページサイズ以上の領域を有する。更に、ページデータの読出しや書込み処理の高速化、ランダムページアクセスをするために、データキャッシュはページサイズの複数倍の領域を持つことが多い。

【０２９２】

データキャッシュ１２は、複数のデータキャッシュＡ、データキャッシュＢ、データキャッシュＣを備える。各データキャッシュは、メモリセルアレイ１１の読出しに用いるセンスアンプ（ＳＡ）とデータ線とに各々接続される。

【０２９３】

センスアンプＳＡは、図示しないビット線を介し、メモリセルアレイ１１に電気的に接続される。

【０２９４】

データキャッシュのうちのＤＣ＿Ａは、直接データ線とのデータのやり取りが可能であるデータキャッシュである。ＤＣ＿Ａを通じてデータキャッシュ１２のデータを、データ線を介してＩＯへ接続されることにより、ＮＡＮＤチップ１０の外部に出力し、ＮＡＮＤチップ１０の外部のデータをデータキャッシュにロードすることが可能である。

【０２９５】

更に、データキャッシュ１２に接続され、データキャッシュ１２間の演算を行うための演算器を備える。演算器は、上記実施形態における認証処理に用いるデータ生成器１３、１４や一方向性回路１５等を備える認証回路１７に相当する。

【０２９６】

また、一時的にデータを格納しておくための内部レジスタ９２を備える。

【０２９７】

ここで、ＮＡＮＤ型フラッシュメモリ１０には、データ読出しにおいて、メモリセルアレイ１１への読出しコマンドに加え、データキャッシュ１２にメモリセルアレイ１１から読み出されたデータを読み出すためのコマンドとしてレジスタリードと呼ばれるコマンドがある。

【０２９８】

この際、上記認証方法においては、ＮＡＮＤ型フラッシュメモリ１０内の秘匿ブロック１１－２は、秘匿ブロック１１－２に記録されている秘匿情報（NKey、SecretID等）をＮＡＮＤチップ１０の外部からのアクセスによって読みだされることがあってはならない。一方で、ＮＡＮＤ型フラッシュメモリ１０が認証処理を行う場合は、秘匿ブロック１１－２に記録されている秘匿情報（NKey、SecretID等）を内部的に読出し、認証処理に用いる

必要がある。すなわち、メモリセルアレイ１１からデータキャッシュ１２への秘匿情報（NKey、SecretID等）の読出しは可能としておく必要がある一方で、データキャッシュ１２からＮＡＮＤ型フラッシュメモリ１０の外部へのデータ出力を禁止する必要がある。これは、前記のレジスタリードを無効化することに相当する。

【０２９９】

そこで、秘匿ブロック１１－２が、ＮＡＮＤ型フラッシュメモリ１０の外部からアクセスされたときのデータ読み出し動作については、通常の読み出し動作と異なる動作をさせる。より具体的には、秘匿ブロック１１－２がアクセスされた場合、メモリセルアレイ１１からセンスしたデータを、データキャッシュＤＣ＿Ａ以外のデータキャッシュＤＣ＿Ｂ、ＤＣ＿Ｃに留め外部への出力ができないようにして、レジスタリードコマンドが効かないように無効化する。一方、アクセスされたブロックが、秘匿ブロック１１－２でない場合、通常通り、データキャッシュＤＣ＿Ａを用いて、データ読み出しを行う。

【０３００】

このように、上記構成によれば、複数種類のデータキャッシュＤＣ＿Ａ～ＤＣ＿Ｃを設け、外部からユーザがアクセスできないデータキャッシュＤＣ＿Ｂ、ＤＣ＿Ｃのみで上記認証処理を実行する。そのため、上記認証処理に秘匿情報（NKey、SecretID等）を利用する際に、鍵情報（NKey）等の秘匿情報が外部から不正に読み取られない点で有利である。

【０３０１】

＜認証処理におけるＮＡＮＤ内部演算フロー１＞

次に、図３２に沿って、認証処理の過程において、ホスト装置２０に対して秘匿ブロック１１－２の情報を直接的・間接的にも出力しないためのフローを示す。

【０３０２】

（Step Ｓ８２）

まず、認証処理において、ホスト装置２０等のＮＡＮＤ型フラッシュメモリ１０の外部からデータが入力されるとする。この入力データは、例えば、上記乱数ＲＮやホスト定数ＨＣj等であり、同データは、データキャッシュＤＣ＿Ａにロードされる。

【０３０３】

（Step Ｓ８３）

続いて、ホスト装置２０から秘匿ブロック１１－２等の特別ブロックへアクセスする間接的読み出し要求が行われる。これは、すなわち認証における認証情報の計算要求に該当する。

【０３０４】

この要求を受けて、メモリセルアレイ１１からリードされた機密ページのデータが読み出される。

【０３０５】

（Step Ｓ８４）

続いて、リードされた機密ページのデータは、データキャッシュＤＣ＿Ｂに格納される。

【０３０６】

（Step Ｓ８５）

続いて、データキャッシュＤＣ＿ＡとデータキャッシュＤＣ＿Ｂのそれぞれに記憶されているデータ間で、上記実施形態で説明した認証処理における演算を演算器（認証回路１７）を用いて行う。

【０３０７】

（Step Ｓ８６）

続いて、演算の結果は、データキャッシュＤＣ＿Ｃに格納される。

【０３０８】

（Step Ｓ８７）

ここで、一連のシーケンスを抜けてチップレディとなったときに機密データがデータキャッシュに残っていると、これを外部から読み出されるおそれがある。これを防ぐために

シーケンスを抜ける前に、全てのデータキャッシュＤＣ＿Ａ～ＤＣ＿Ｃの情報をリセットしておかなければならない。一方、ホスト装置２０は、上記演算の結果をデータキャッシュＤＣ＿Ａ～ＤＣ＿Ｃがリセットされた後に得なければならない。

【０３０９】

そこで、まず、データキャッシュＤＣ＿Ｃに保持されている演算の結果を、内部レジスタ９２にコピーする。

【０３１０】

（Step Ｓ８８）

続いて、全てのデータキャッシュＤＣ＿Ａ～ＤＣ＿Ｃのデータをリセットする。

【０３１１】

（Step Ｓ８９）

続いて、内部レジスタ９２に退避しておいたデータを、データキャッシュＤＣ＿Ａに戻す。ここまでの動作が終了すると、ＮＡＮＤ型フラッシュメモリ１０はこのシーケンスを抜け、レディ状態となる。この際、データキャッシュＤＣ＿Ａには演算の結果が格納されている。

【０３１２】

（Step Ｓ９０）

続いて、ホスト装置２０は、レジスタリードコマンドにより、データキャッシュＤＣ＿Ａに格納されたデータを得ることが出来る。

【０３１３】

＜認証処理におけるＮＡＮＤ内部演算フロー２＞

次に、図３３に沿って、ＮＡＮＤ型フラッシュメモリ１０内部に乱数生成器（２４ｎ）を備えた実施形態のＮＡＮＤ内部演算フローについて説明する。上記図３２の場合と異なるのは、ＮＡＮＤ型フラッシュメモリ１０内部の乱数発生器（２４ｎ）で発生した乱数（RN_n）を使用する点である。

【０３１４】

（Step Ｓ９１）

まず、認証処理において、ホスト装置２０からＮＡＮＤ型フラッシュメモリ１０に対して乱数読出し要求が行われると、ＮＡＮＤ型フラッシュメモリ１０は乱数を生成させ、生成された乱数はデータキャッシュＤＣ＿Ａにロードされる。

【０３１５】

（Step Ｓ９２）

続いて、ホスト装置２０は、レジスタリードコマンドによって、データキャッシュＤＣ＿Ａの乱数を読み出す。

【０３１６】

（Step Ｓ９３）

続いて、認証処理において、ホスト装置２０から例えばホスト定数（ＨＣｊ）等のデータが、ＮＡＮＤ型フラッシュメモリ１０に対して入力される。上記データは、データキャッシュＤＣ＿Ａにロードされる。

【０３１７】

更に、ホスト装置２０からＮＡＮＤ型フラッシュメモリ１０に対してホスト装置２０で演算した認証情報が入力される。このデータは、例えばＯｎｅｗａｙ－ＩＤ等であり、同データはデータキャッシュＤＣ＿Ａにロードされる。

【０３１８】

（Step Ｓ９４）

続いて、ホスト装置２０から秘匿ブロック１１－２にアクセスして、間接的読み出し要求が行われる。これはすなわち認証における認証情報の計算要求に該当する。

【０３１９】

すると、メモリセルアレイ１１から機密ページのリードがされる。

【０３２０】

（Step Ｓ９５）
続いて、リード結果は、データキャッシュＤＣ＿Ｂに格納される。
【０３２１】
（Step Ｓ９６）
続いて、データキャッシュＤＣ＿Ａとデータキャッシュ ＤＣ＿Ｂとのそれぞれに記憶されているデータ間で、上記実施形態で説明した認証処理における演算を演算器（認証回路１７）を用いて行う。
【０３２２】
（Step Ｓ９７）
続いて、上記演算の結果は、データキャッシュＤＣ＿Ｂに格納される。
【０３２３】
（Step Ｓ９８）
続いて、データキャッシュＤＣ＿Ａに保持されているホストの演算結果とデータキャッシュＤＣ＿Ｂに保持されているＮＡＮＤの演算結果とを照合する。
【０３２４】
（Step Ｓ９９）
続いて、上記ステップＳ９８の際の照合において、照合結果の一致が確認された場合、制御パラメータ（８９０）を更新する。
【０３２５】
（Step Ｓ１００）
続いて、ＮＡＮＤ型フラッシュメモリ１０は、全てのデータキャッシュＤＣ＿Ａ～ＤＣ＿Ｃの情報をリセットする。ここまでの動作が終了すると、ＮＡＮＤ型フラッシュメモリ１０は、このシーケンスを抜け、レディ状態となる。
【０３２６】
（Step Ｓ１０１）
続いて、ホスト装置２０は、照合結果を確認するコマンドにより、ＮＡＮＤチップ１０の外部にリードアウトされた照合結果を得る。
【０３２７】
＜秘匿情報の検査方法について＞
次に、秘匿情報の検査方法について説明する。
【０３２８】
検査フロー
図３４に沿って、工場でシリコンが出来上がってから、ＮＡＮＤ型フラッシュメモリ１０を出荷するまでの過程で、本認証方法に関係する工程を示す。
【０３２９】
図示するように、製造工程、テスト、秘匿データ書き込み、出荷の順に工程が進む。
【０３３０】
（Step Ｓ７１、Ｓ７２）
まず、製造工程が終了すると、所定の検査テストを行って、良品チップ１０をウェハから選別する。
【０３３１】
（Step Ｓ７３）
続いて、上記ステップＳ７２の際の通常のテスト工程が終了した後、秘匿データを書き込む工程が行われ、正しく秘匿データが書かれたか否かをテストしなければならない。
【０３３２】
一方で、この際、秘匿ブロック１１－２から秘匿データを直接読み出すことはできない。なぜなら、当該読出し機能はセキュリティーホールとなる恐れがあるためである。
【０３３３】
（Step Ｓ７４）
続いて、正しく秘匿データが書かれたＮＡＮＤ型フラッシュメモリ１０について、出荷

を行う。
【０３３４】
　秘匿情報の間接的読み出し検査フロー
　上記ステップＳ７３の際、秘匿ブロック１１－２から秘匿データを直接読み出すことは、セキュリティーホールとなる恐れがある観点から、行うことができない。
【０３３５】
　そこで、図３５に沿って、直接データ読出し機能を提供せずに、記録されたデータの確認をするフローを説明する。
【０３３６】
（Step Ｓ１１１）
　まず、メモリセルアレイ１１の秘匿ブロック１１－２から、秘匿情報（Nkey等）の情報を読み出す。
【０３３７】
（Step Ｓ１１２）
　続いて、読み出した秘匿情報（Nkey等）のリード結果を、データキャッシュＤＣ＿Ｂに格納する。
【０３３８】
（Step Ｓ１１３）
　続いて、ＮＡＮＤ型フラッシュメモリ１０の外部から、同一の秘匿情報（Nkey等）を、データキャッシュＤＣ＿Ａに記憶させる。
【０３３９】
（Step Ｓ１１４）
　続いて、演算器（認証回路１７）を用いて、データキャッシュＤＣ＿ＡのデータとデータキャッシュＤＣ＿Ｂのデータとの排他的論理和をとる。
【０３４０】
（Step Ｓ１１５）
　続いて、排他的論理和の結果を、データキャッシュＤＣ＿Ｃに格納する。
【０３４１】
（Step Ｓ１１６）
　続いて、データキャッシュＤＣ＿Ｃのデータを検知する。
【０３４２】
（Step Ｓ１１７）
　この際、データキャッシュＤＣ＿Ａのデータと、データキャッシュＤＣ＿Ｂのデータとが一致している場合（Yes）にはテストはパス(OK)である。一方、一致していない場合（No）テストはフェイルである。
【０３４３】
　具体的には、データキャッシュＤＣ＿Ｃには排他的論理和の結果が入っているから、データキャッシュＤＣ＿Ｃのデータが全て“０”の場合（Yes）、テストはパス（OK）である。一方、“１”である場合（No）、フェイルとなる。
【０３４４】
　まず、データキャッシュＤＣ＿Ｃのデータがすべて“０”であるかどうかの検知を行う。ここで、すべてのビットが“０”となっていれば（Yes）、テストはパスとなる。そうでなかった場合（No）、次のステップＳ１１８に続く。
【０３４５】
（Step Ｓ１１８）
　続いて、すべてのビットが“０”でない場合（No）、“１”の数を数える。この際、“１”の数が規定の数以下である場合（Yes）、多数決誤り訂正や訂正符号による誤り訂正が可能であると判断されるのでテストはパスとなる（OK）。一方、“１”の数が規定数以上であった場合（Mo）、テストはフェイルとなる（NG）。
【０３４６】

ここで、上記実施形態に記載した、特定ブロックへのアクセス制御に認証を用いる方法を用いて、秘匿ブロック１１－２に記録された秘匿情報の代わりに、ＮＡＮＤ型フラッシュメモリ１０にハードワイヤードで構成した第２の秘匿情報を別途持っておき、同第２の秘匿情報によって秘匿ブロック１１－２へのアクセス制御を行うという方法も可能である。この場合、データ読み出しだけではなく、データ書き込みやデータ消去等も第２の秘匿情報に基づく認証によって制御してもよい。

【０３４７】

＜作用効果＞

第６の実施形態に係る認証装置、被認証装置及び認証方法によれば、少なくとも上記と同様の作用効果（１）乃至（５）を得ることができる。

【０３４８】

更に、本実施形態では、秘匿ブロック１１－２がアクセスされた場合、メモリセルアレイ１１からセンスしたデータを、データキャッシュＤＣ＿Ａ以外のデータキャッシュＤＣ＿Ｂ、ＤＣ＿Ｃに留め外部への出力ができないようにして、レジスタリードコマンドが効かないように無効化する。一方、アクセスされたブロックが、秘匿ブロック１１－２でない場合、通常通り、データキャッシュＤＣ＿Ａを用いて、データ読み出しを行う。

【０３４９】

このように、上記構成によれば、複数種類のデータキャッシュＤＣ＿Ａ～ＤＣ＿Ｃを設け、外部からユーザがアクセスできないデータキャッシュＤＣ＿Ｂ、ＤＣ＿Ｃのみで上記認証処理を実行する。そのため、上記認証処理に秘匿情報（NKey、SecretID等）を利用する際に、鍵情報（NKey）等の秘匿情報が外部から不正に読み取られない点で有利である。

【０３５０】

加えて、上記ステップＳ８８、Ｓ１００に示すように、Busy状態からReady状態に戻る前に、データキャッシュＤＣ＿ＡＤ～Ｃ＿Ｃ中の鍵情報等の秘匿情報を全て消去する。そのため、安全性を確保することが可能である。

【０３５１】

［第７の実施形態（コマンドマッピングの一例）］

第７の実施形態は、コマンドマッピングの一例に関するものである。この説明において、上記実施形態と重複する部分の説明については、省略する。

【０３５２】

＜Read,Writeコマンドと親和性の良いコマンドマッピング例＞

ここで、ＮＡＮＤ型フラッシュメモリ１０は、読出し用のコマンドとして、例えば、００ｈ－Ａｄｄｒｅｓｓ－３０ｈにより読出し対象のブロック及びページアドレスを指定する。Ａｄｄｒｅｓｓ部分はブロックアドレス、ページアドレス、更にページ内のバイト位置を示すカラムアドレスから構成されることが多い。カラムアドレス部分の入力データは無視されることもあれば、ページ読出し後のバイトポインタの設定に用いられて当該バイト位置からの読出しに用いられることもある。コマンド３０ｈの入力後にＮＡＮＤ型フラッシュメモリ１０は読出しのためのBusy状態となり、読出し完了後にReady状態へと遷移する。Ready状態へ遷移後、データ出力（Dout）が可能となり、ＲＥやＤＱＳ等を供給することでデータを読み出すことが可能となる。また、読み出したページ内で読み出すバイト位置を変更する場合は、０５ｈ－Ａｄｄｒｅｓｓ－Ｅ０ｈにて読み出したいバイト位置に相当するカラムアドレスを設定する。

【０３５３】

データ書き込み（記録）用のコマンドとしては、８０ｈ－Ａｄｄｒｅｓｓ－Ｄａｔａｉｎｐｕｔ－１０ｈにより、書き込み対象のブロック及びページアドレスを指定する。ここで、Ａｄｄｒｅｓｓ部分はブロックアドレス、ページアドレス、更にページ内のバイト位置を示すカラムアドレスから構成されることが多い。カラムアドレス部分の入力データは無視されることもあれば、ページ書き込み用データ入力におけるバイトポインタの設定に用いられて当該バイト位置からの書き込みデータ入力に用いられることもある。コマンド１０ｈ入力後、ＮＡＮＤ型フラッシュメモリ１０は、書き込みのためのBusy状態となり

、書き込み完了後Readyへと遷移する。

【０３５４】

上記が、ＮＡＮＤ型フラッシュメモリ１０で広く用いられているコマンド体系である。上記実施形態に係る認証機能を実装する場合に、コマンドシーケンスをできるだけ共通化させることが回路の実装面積を極小化する上で好ましい。しかしながら、認証機能はセキュリティを要する分野で利用されることから、機能利用者を限定した方が望ましいという視点もある。

【０３５５】

そこで、図３６は、上記観点を考慮して、ＮＡＮＤ型フラッシュメモリ１０の上記Read,Writeコマンドと親和性の良いコマンドマッピング例を示している。

【０３５６】

上記一般的なコマンドシーケンスと異なる点は、Security Prefixの入力コマンドを当該コマンドの前に付与している点である。ここで、Security Prefixは、単バイトで構成する場合、複数バイトで構成する場合が考えられる。コマンドSecurity Prefixは、当該認証機能を必要とする利用者にのみ開示される。利用者管理の観点では、コマンドSecurity Prefixは、複数バイトで構成されるほうが望ましい。

【０３５７】

（ａ）で示すように、データ読出しコマンドシーケンスと同ように、ＩＯ端子に、順次、コマンド（Security Prefix）－コマンド（００ｈ）－アドレス（ＡＤＤ）－コマンド（３０ｈ）により読出し対象のブロック及びページアドレスが指定される。ここで、Ａｄｄｒｅｓｓに設定された値を更に利用者管理用に特別な値とすることも可能であり、若しくは内部にて無視される値とすることも可能である。

続いて、コマンド（３０ｈ）の入力後にＮＡＮＤ型フラッシュメモリ１０は、読出しのためのBusy状態となり、読出し完了後にReady状態へと遷移する。Ready状態へ遷移後、データ出力（Dout）が可能となり、ＲＥやＤＱＳ等を供給することで、インデックス情報ｉ，ｖ、固有の暗号化秘密識別情報（E-SecretID）、共通に付される鍵管理情報（FKB）等のデータを読み出すことが可能となる。

（ｂ）で示すように、データ書き込みコマンドシーケンスと同ように、ＩＯ端子に、順次、コマンド（Security Prefix）－コマンド（８０ｈ）－アドレス（ＡＤＤ）－データ（Din 32B）－コマンド（１０ｈ）を入力することにより、対象データの入力を行う。ここで、Ａｄｄｒｅｓｓに設定された値を更に利用者管理用に特別な値とすることも可能であり、若しくは内部にて無視される値とすることも可能である。ここで、本シーケンスは書き込みシーケンスと共通箇所が多いものの、実際にはセルアレイへのデータ書き込みは必要としなく、ＮＡＮＤ型フラッシュメモリ１０が認証処理の計算に必要とするデータ入力のために使用される。認証処理の計算に必要とするデータの例としては、ホスト装置２０の固有情報ＨＣｉや乱数等がある。

続いて、認証処理の計算が終了するまでの期間Busy状態となり、計算が終了し、かつ上記のように、データキャッシュＤＣ＿Ａ～ＤＣ＿Ｃ中のセキュリティーデータが全てクリアされた後に、Ready状態へと遷移する。

【０３５８】

（ｂ）で示すように、Ready状態へと遷移した後、ホスト装置２０は、ＩＯ端子に、順次、コマンド（０５ｈ）－アドレス（ＡＤＤ）－コマンド（Ｅ０ｈ）を入力し、認証処理の計算結果が保持されているカラムアドレスを指定することで結果の取得が可能となる。認証処理の計算結果の例としてはＯｎｅｗａｙ－ＩＤ等がある。

【０３５９】

＜Set / Get featureコマンドと親和性の良いコマンドマッピング例＞

次に、図３７に沿って、本認証機能を適用したＮＡＮＤ型フラッシュメモリ１０のコマンド構成の別の例を示す。

ＮＡＮＤ型フラッシュメモリ１０には、当該メモリ１０の機能を有効化するためのSet Featureと呼ばれるコマンド、及び、当該メモリ１０の機能の有効化・無効化状況を読み

出すためのGet Featureと呼ばれるコマンドがある。これらのコマンドは、例えば、高速データ転送用の相補信号である/ＲＥ、/ＷＥ、/ＤＱＳ等の入力を有効化するため等に用いられる。

【０３６０】

Set Featureは、ＥＥｈ－Ａｄｄｒｅｓｓ－Data inputにて機能の設定を行う。ここで、Ａｄｄｒｅｓｓには機能番号が設定され、Data inputには当該機能番号にて示される機能のパラメータが入力される。その後、機能有効化のためのBusy期間があり、有効化の後、Readyへと遷移する。

【０３６１】

Get Featureは、ＥＦｈ－Ａｄｄｒｅｓｓ－Data outputにて、機能の有効化・無効化状況の読出しを行う。ここで、Ａｄｄｒｅｓｓには機能番号が設定され、Data outputには当該機能番号にて示される機能のパラメータが出力される。ＡｄｄｒｅｓｓとData outputとの間には、内部での設定パラメータ読出しのためのBusy期間が存在する。

【０３６２】

本実施形態は、これらSet Feature、Get Featureを流用したコマンドシーケンスの例である。

【０３６３】

（ａ）に示すように、コマンドシーケンスは、上記と同様であるが、指定するＡｄｄｒｅｓｓが異なる。ここで、Ａｄｄｒｅｓｓは単バイトで構成する場合、複数バイトで構成する場合が考えられる。Ａｄｄｒｅｓｓは当該認証機能を必要とする利用者にのみ開示される。利用者管理の観点では、Ａｄｄｒｅｓｓは複数バイトで構成されるほうが望ましい。Data output及びData inputの例としては、上記図３７にて示したものと同様のインデックス情報i、ｖである。

【０３６４】

（ｂ）に示すように、Data input用のコマンド（ＥＥｈ）－アドレス（ＡＤＤ）－データ（Din）のコマンドシーケンスは、同時に認証処理の実行を誘発し、Busy期間中にＮＡＮＤ型フラッシュメモリ１０は認証処理の計算を行う。

【０３６５】

続いて、計算が終了し、かつセキュリティーデータがデータキャッシュよりクリアされた後に、Ready状態へと遷移する。Ready状態へと遷移した後、ホスト装置２０は、Ｏｎｅｗａｙ－ＩＤを読み出すことが可能である。

【０３６６】

＜作用効果＞

第７の実施形態に係る認証装置、被認証装置及び認証方法によれば、少なくとも上記と同様の作用効果（１）乃至（５）を得ることができる。

【０３６７】

更に、本実施形態では、図３６に示したように、ＮＡＮＤ型フラッシュメモリ１０のコマンドシーケンスとできるだけ共通化させることできる。そのため、セキュリティを考慮しつつ、回路の実装面積を極小化できるため、上記実施形態に係る認証機能を実装する場合により有効である。

【０３６８】

また、図３７に示したように、当該メモリ１０の機能を有効化するためのSet Featureと呼ばれるコマンド、及び、当該メモリ１０の機能の有効化・無効化状況を読み出すためのGet Featureと呼ばれるコマンドに対しても、必要に応じて共通化させて適用が可能である。

【０３６９】

ここで、Busy状態からReady状態へ戻る前のタイミングで、データキャッシュＤＣ＿Ａ～ＤＣ＿Ｃのデータを全てクリアする点は、上記と同様である。

【０３７０】

［第８の実施形態（メモリカード、コンテンツ保護、ＨＤＤへの一応用例）］

第８の実施形態は、メモリカード、コンテンツ保護、ＨＤＤへの一応用例の関するものである。この説明において、上記実施形態と重複する部分の説明については、省略する。

【０３７１】

メモリカードへの応用例

図３８を用い、本認証機能を適用したＮＡＮＤ型フラッシュメモリ１０を搭載したメモリカードの構成例を示す。

【０３７２】

図示するように、メモリカード５５は、ＮＡＮＤフラッシュメモリ１０の動作を制御する機能、ホスト装置２０側とのインターフェースを制御する機能等を有するコントローラ１９を搭載する。

【０３７３】

ＮＡＮＤパッケージ内に積層された複数のＮＡＮＤ型フラッシュメモリチップ１０（ＭＣＰ１）、（ＭＣＰ２）を少なくとも1つ以上有する。ここで、ＮＡＮＤパッケージ内の少なくとも１つ以上のＮＡＮＤフラッシュメモリチップ１０が、上記実施形態に係る認証機能・被認証機能を有すれば良い。換言すると、ＮＡＮＤパッケージ内のＮＡＮＤフラッシュメモリチップ１０の全てが、上記実施形態における認証機能・被認証機能を有していなくてもよい。更に、メモリカード５５内に搭載されたＮＡＮＤパッケージの全てが実施形態における認証機能・被認証機能を有していなくともよい。明確化のために、本実施形態のＮＡＮＤ型フラッシュメモリ１０は、ＮＡＮＤパッケージを指すこともあれば、ＮＡＮＤフラッシュメモリチップを指すこともある。

【０３７４】

メモリカード５５内のコントローラ１９は、ＮＡＮＤパッケージ内のＮＡＮＤ　Ｉ／Ｆを経由して、上記実施形態に係る認証機能・被認証機能を制御する機能を有する。ここで、複数のＮＡＮＤパッケージのいずれか一つのみの認証機能・被認証機能を制御する機能であってもよいし、複数のＮＡＮＤパッケージの各々の認証機能・被認証機能を制御する機能であってもよい。更に、ＮＡＮＤパッケージ内のいずれか一つのＮＡＮＤフラッシュメモリチップ１０の認証機能・被認証機能を制御する機能であってもよいし、ＮＡＮＤパッケージ内の各々のＮＡＮＤフラッシュメモリチップ１０の認証機能・被認証機能を制御する機能であってもよい。

【０３７５】

コンテンツ保護への応用例１

図３９を用い、上記認証機能を適用したＮＡＮＤ型フラッシュメモリ１０を搭載したメモリカード５５のコンテンツ保護への応用例１を示す。簡略化のため、本発明明細書内で既に説明した内容については説明を割愛する。

【０３７６】

メモリカード５５内には、コントローラ１９、ＮＡＮＤパッケージ（ＭＣＰ１）、（ＭＣＰ２）が搭載されている。ここで、ＮＡＮＤパッケージ（ＭＣＰ１）、（ＭＣＰ２）は、上記実施形態に係る認証機能・被認証機能を有する。

【０３７７】

ホスト装置２０は、上記実施形態にて示した認証処理により、ＮＡＮＤ型フラッシュメモリ１０のＮＡＮＤパッケージ（ＭＣＰ１）、（ＭＣＰ２）は、秘密識別情報Secret IDの正当性を確認する。

【０３７８】

正当性確認後、ホスト装置２０は、秘密識別情報Secret IDに基づいて、第２の実施形態において説明した方法を用い、ＥＭＩＤの計算処理を行う。

【０３７９】

ここで、ＮＡＮＤパッケージ（ＭＣＰ２）は、コンテンツ（Content）書き込み時に、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataを生成する。Binding Dataには、コンテンツを暗号化・復号化するための鍵に関わるデータを含んでおくことが望ましい。Binding Dataは、カード５５内に搭載されたＮＡＮＤパッケージ（ＭＣＰ１）、（ＭＣＰ

２）のいずれかに記録される。ここで、Binding Dataが記録されるＮＡＮＤパッケージは、認証処理に用いた秘密識別情報Secret IDを有するＮＡＮＤパッケージ（ＭＣＰ１）であってもよいし、他のＮＡＮＤパッケージ（ＭＣＰ２）であってもよい。図３９では後者の例を示しているがこれに限られない。また、コンテンツの記録位置も同ように、いずれのＮＡＮＤパッケージであってもよい。

【０３８０】

コンテンツ（Content）再生時には、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataと秘密識別情報Secret IDとを認証処理して得られたＥＭＩＤと、コンテンツの関連性を計算・確認して、関連性が確認された場合にのみコンテンツを再生する。

【０３８１】

上記構成により、コンテンツ（Content）は、秘密識別情報Secret IDと関連付けられる。そのため、同一の秘密識別情報Secret IDを有さない他のメモリカードにコンテンツやBinding Dataを不正に複製しても、コンテンツの再生ができなくなる効果が得られる点で、有利である。

【０３８２】

ＨＤＤへの応用例１

図４０を用い、本認証機能を適用したＮＡＮＤ型フラッシュメモリ１０を利用したハードディスクドライブ（ＨＤＤ）の構成例１を示す。

【０３８３】

図示するように、ＨＤＤパッケージ２００には、少なくとも一つ以上のＮＡＮＤパッケージ（ＭＣＰ１）を搭載し、内少なくとも一つのＮＡＮＤパッケージは上記実施形態に係る認証機能・被認証機能を有する。

【０３８４】

また、ＨＤＤパッケージ２００には、少なくとも一つのＨＤＤ２１０を搭載する。

【０３８５】

更に、ＮＡＮＤパッケージ（ＭＣＰ１）の制御、ＨＤＤ２１０の制御、ホスト装置とのインターフェースの制御等を実行するブリッジコントローラ１９０を搭載する。ブリッジコントローラ１９０は、単独の集積回路から構成されていてもよいし、複数の集積回路から構成されていてもよい。また、集積回路とファームウェアの組み合わせにより機能を実現してもよい。

【０３８６】

ＮＡＮＤパッケージ（ＭＣＰ１）内の認証機能・被認証機能は、ブリッジコントローラ１９０を経由してホスト装置であるＨＤＤ２１０へと提供される。

【０３８７】

ＨＤＤへの応用例２

図４１を用い、本認証機能を適用したＮＡＮＤ型フラッシュメモリ１０を利用したハードディスクドライブ（ＨＤＤ）の別の構成例を示す。

【０３８８】

図示するように、ＨＤＤパッケージ２００には、上記図３８にて説明したメモリカード５５を接続するためのメモリカードソケット５５０を有する。

【０３８９】

また、ＨＤＤパッケージ２００には、少なくとも一つの以上のＨＤＤ２１０を搭載する。更に、メモリカード５５の制御、ＨＤＤ２１０の制御、ホスト装置とのインターフェースの制御等を実行するブリッジコントローラ１９０を搭載する。ブリッジコントローラ１９０は、単独の集積回路から構成されていてもよいし、複数の集積回路から構成されていてもよい。また、集積回路とファームウェアの組み合わせにより機能を実現してもよい。

【０３９０】

メモリカード５５内の認証機能・被認証機能は、ブリッジコントローラ１９０を経由してホスト装置であるＨＤＤ２１０へと提供される。

【０３９１】

コンテンツ保護への応用例２

図４２にて、本認証機能を適用したＮＡＮＤ型フラッシュメモリ１０を利用したハードディスクドライブ（ＨＤＤ）のコンテンツ保護への応用例を示す。本実施形態は、図４１にて示したＨＤＤ構成を例に取っているが、図４０にて示したＨＤＤ構成にも適用可能である。

【０３９２】

図示するように、ＨＤＤパッケージ２００Ａ、２００Ｂ内には、ブリッジコントローラ１９０Ａ、１９０Ｂ、メモリカードソケット５５０Ａ、５５０Ｂ、ＨＤＤ２１０Ａ、２１０Ｂがそれぞれ搭載されている。

【０３９３】

ここで、メモリカード５５は、上記実施形態のいずれかの認証機能・被認証機能を有する。ホスト装置２０は、上記実施形態にて示した認証処理によりＮＡＮＤ型フラッシュメモリ１０の秘密識別情報Secret IDの正当性を確認する。正当性確認後、ホスト装置２０は、秘密識別情報Secret IDに基づいて第２の実施形態にて示した方法にて、ＥＭＩＤの計算処理を行う。

【０３９４】

コンテンツ（Cntent）書き込み時には、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataを生成する。Binding Dataにはコンテンツを暗号化・復号化するための鍵に関わるデータを含んでおくことが望ましい。Binding Dataは、メモリカード５５、若しくは、ＨＤＤ２１０Ａ、２１０Ｂのいずれかに記録される。ここでは、ＨＤＤ２１０Ａ、２１０Ｂに記録される例を示しているがこれに限られない。また、コンテンツの記録位置も同ように、カード５５若しくはＨＤＤ２１０Ａ、２１０Ｂのいずれであってもよい。

【０３９５】

コンテンツ（Content）再生時には、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataと、秘密識別情報Secret IDを認証処理して得られたＥＭＩＤと、コンテンツの関連性を計算・確認し関連性が確認された場合にのみコンテンツを再生する。

【０３９６】

本実施形態は、カードソケット５５０Ａを経由してメモリカード５５内のＮＡＮＤフラッシュメモリ１０が有する認証機能・被認証機能を利用する例であるが、図４０に示したＨＤＤが直接ＮＡＮＤパッケージを搭載し、制御する構成においても適用可能である。この場合、メモリカードをＮＡＮＤパッケージに置き換えればよい。

【０３９７】

更に、カードソケット５５０Ａ、５５０Ｂを有するＨＤＤについて適用可能な応用例として、同様のＨＤＤパッケージが複数あった場合、両ＨＤＤパッケージにコンテンツやBinding Dataを複製することで、カードを移動するのみでいずれのＨＤＤに記録されたコンテンツを再生することも可能となる。ここで、Binding Dataは、ＨＤＤでなく、カードに記録されていてもよいし、または両方に記録されていてもよい。

【０３９８】

本構成により、コンテンツ（Content）は、メモリカード５５若しくはＮＡＮＤパッケージ内の秘密識別情報Secret IDと関連付けられるため、同一の秘密識別情報Secret IDを有さないメモリカード５５にコンテンツやBinding Dataを不正複製しても、コンテンツの再生ができなくなる効果が得られる。

【０３９９】

更に、図４１にて示したＨＤＤパッケージがメモリソケットを有する例においては、メモリカードのみを移動することで複数のＨＤＤに記録されたコンテンツを再生することが可能となる。これは一般にメモリカードに比較し、ＨＤＤは筐体が大きく、据え置き用途等で用いられることもあることから、可搬性上有利である。

【０４００】

コンテンツ保護への応用例３

図４３を用い、本認証機能を適用したＮＡＮＤ型フラッシュメモリ１０を利用したハー

ドディスクドライブ（ＨＤＤ）のコンテンツ保護への応用例３を説明する。本実施形態は、ホスト装置２０が、メモリカードソケット５５０を有し、外付けＨＤＤ２１０を利用する例である。

【０４０１】

図示するように、ＨＤＤパッケージ２００内には、ブリッジコントローラ１９０、ＨＤＤ２１０が搭載されている。

【０４０２】

ホスト装置２０には、メモリカードソケット５５０に挿入されるメモリカード５５内に備える認証機能、カード制御機能が搭載されている。メモリカード５５には、上記実施形態いずれかに係る認証機能・被認証機能を有するＮＡＮＤパッケージが搭載されている。

【０４０３】

上記構成において、ホスト装置２０は、上記実施形態にて示した認証処理によりＮＡＮＤ型フラッシュメモリ１０の秘密識別情報Secret IDの正当性を確認する。

【０４０４】

正当性確認後、ホスト装置２０は、秘密識別情報Secret IDに基づいて、上記第２の実施形態に係る方法を用い、ＥＭＩＤの計算処理を行う。

【０４０５】

コンテンツ（Content）書き込み時には、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataを生成する。Binding Dataには、コンテンツを暗号化・復号化するための鍵に関わるデータを含んでおくことが望ましい。Binding Dataは、メモリカード５５、若しくは、ＨＤＤ２１０のいずれかに記録される。ここでは、後者の例を示しているがこれにと限られない。また、コンテンツの記録位置も同ように、カード５５若しくはＨＤＤ２１０のいずれであってもよい。

【０４０６】

コンテンツ（Content）再生時には、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataと、秘密識別情報Secret IDを認証処理して得られたＥＭＩＤと、コンテンツの関連性を計算・確認し関連性が確認された場合にのみコンテンツを再生する。

【０４０７】

本実施形態は、カードソケット５５０を経由してメモリカード５５内のＮＡＮＤフラッシュメモリ１０が有する認証機能・被認証機能を利用する例であるが、ホスト装置２０は、直接ＮＡＮＤパッケージを搭載し、制御する構成においても適用可能である。この場合、前記のメモリカード５５をＮＡＮＤパッケージに置き換えればよい。

【０４０８】

更に、カードソケット５５０を有するホスト装置２０について適用可能な応用例として、同様のホスト装置２０が複数あった場合、メモリカード５５とＨＤＤパッケージ２００を別のホスト装置２０と接続することで、いずれのホスト装置２０でもコンテンツを再生することも可能となる。ここで、コンテンツやBinding Dataは、ＨＤＤ２１０でなく、カード５５に記録されていてもよいし、または両方に記録されていてもよい。

【０４０９】

本構成により、コンテンツはメモリカード５５若しくはＮＡＮＤパッケージ内の秘密識別情報Secret IDと関連付けられるため、同一の秘密識別情報Secret IDを有さないメモリカードにコンテンツやBinding Dataを不正複製しても、コンテンツの再生ができなくなる効果が得られる。更に、メモリカード５５とＨＤＤ２１０を移動することで複数のホスト装置でコンテンツを再生することが可能となる。

【０４１０】

コンテンツ保護への応用例４

図４４を用い、本認証機能を適用したＮＡＮＤ型フラッシュメモリ１０を利用したハードディスクドライブ（ＨＤＤ）のコンテンツ保護への応用例４を説明する。本実施形態は、ホスト装置２０がメモリカードソケット５５０を有し、更に内蔵ＨＤＤ２１０を利用した例である。

【０４１１】
図示するように、ＨＤＤパッケージ２００内には、ブリッジコントローラ１９０、ＨＤＤ２１０が搭載されている。
【０４１２】
ホスト装置２０には、メモリカードソケット５５０に挿入されるメモリカード５５内に備える認証機能、カード制御機能が搭載されている。メモリカード５５には、上記実施形態いずれかに係る認証機能・被認証機能を有するＮＡＮＤパッケージが搭載されている。
【０４１３】
上記構成において、ホスト装置２０は、上記実施形態にて示した認証処理によりＮＡＮＤ型フラッシュメモリ１０の秘密識別情報Secret IDの正当性を確認する。
【０４１４】
正当性確認後、ホスト装置２０は、秘密識別情報Secret IDに基づいて、上記第２の実施形態に係る方法を用い、ＥＭＩＤの計算処理を行う。
【０４１５】
コンテンツ（Content）書き込み時には、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataを生成する。Binding Dataには、コンテンツを暗号化・復号化するための鍵に関わるデータを含んでおくことが望ましい。Binding Dataは、メモリカード５５、若しくは、ＨＤＤ２１０のいずれかに記録される。ここでは、後者の例を示しているがこれにと限られない。また、コンテンツの記録位置も同ように、カード５５若しくはＨＤＤ２１０のいずれであってもよい。
【０４１６】
コンテンツ（Content）再生時には、ＥＭＩＤとコンテンツを関連付けるためのBinding Dataと、秘密識別情報Secret IDを認証処理して得られたＥＭＩＤと、コンテンツの関連性を計算・確認し関連性が確認された場合にのみコンテンツを再生する。
【０４１７】
本実施形態は、カードソケット５５０を経由してメモリカード５５内のＮＡＮＤフラッシュメモリ１０が有する認証機能・被認証機能を利用する例であるが、ホスト装置２０は、直接ＮＡＮＤパッケージを搭載し、制御する構成においても適用可能である。この場合、前記のメモリカード５５をＮＡＮＤパッケージに置き換えればよい。
【０４１８】
更に、カードソケット５５０を有するホスト装置２０について適用可能な応用例として、同様のホスト装置２０が複数あった場合、メモリカード５５とＨＤＤパッケージ２００を別のホスト装置２０と接続することで、いずれのホスト装置２０でもコンテンツを再生することも可能となる。ここで、コンテンツやBinding Dataは、ＨＤＤ２１０でなく、カード５５に記録されていてもよいし、または両方に記録されていてもよい。
【０４１９】
本構成により、コンテンツはメモリカード５５若しくはＮＡＮＤパッケージ内の秘密識別情報Secret IDと関連付けられるため、同一の秘密識別情報Secret IDを有さないメモリカードにコンテンツやBinding Dataを不正複製しても、コンテンツの再生ができなくなる効果が得られる。更に、メモリカード５５とＨＤＤ２１０を移動することで複数のホスト装置でコンテンツを再生することが可能となる。
【０４２０】
［変形例２（データキャッシュ利用のその他の一例）］
変形例２は、上記第６の実施形態で説明したデータキャッシュの認証処理への利用のその他の構成例に関するものである。この説明において、上記実施形態と重複する部分の説明については、省略する。
【０４２１】
＜センスアンプおよびその周辺回路の構成例＞
上記センスアンプおよび周辺回路の構成例については、図４５のように示される。
図示するように、変形例２では、ＤＣ＿Ａ、ＤＣ＿Ｂ，ＤＣ＿Ｃ、ＤＣ＿Ｓがデータキ

ャッシュ１２であり、ＤＣ＿Ａのみが、カラム制御回路を介してデータ線と接続されており、チップ外部とのデータの授受に使用される。またＤＣ＿Ｓは、データに応じてセンスアンプの動作を制御する用途で使われるラッチである。ＤＣ＿Ｂ、ＤＣ＿Ｃ、ＤＣ＿ＳはＤＣ＿Ａとセンスアンプの間のバス（ＬＢＵＳ）に並列に接続されてデータキャッシュとして使用され、外部とデータの授受を行う場合にはＤＣ＿Ａを介する必要がある。カラム制御回路は、カラムアドレスに応じたアドレスのＤＣ＿Ａをデータ線と接続する。ＮＡＮＤフラッシュメモリが通常の動作で使用される場合には、アドレス制御回路から供給されたカラムアドレスを用いるが、本提案の認証シーケンスを行う場合には演算器が指定するアドレスを用いる。通常のアドレスを使用するか、演算器のアドレスを使用するかはモード切替信号によって切り替えられるようになっている。

【０４２２】

＜センスアンプ、データキャッシュの等価回路例＞

図４６は、図４５中のセンスアンプ７７、およびデータキャッシュ１２の等価回路例について示すものである。

【０４２３】

以上、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

【符号の説明】

【０４２４】

１０…ＮＡＮＤ型フラッシュメモリ、１９…コントローラ、２０…ホスト装置、１１…セルアレイ、２３…メモリ、E-SecretID…固有の暗号化秘密識別情報、SecretID…固有の秘密識別情報、FKB…共通に付される鍵管理情報、NKey…第１鍵情報、HKey…第２鍵情報、SKey…セッション鍵情報。

【要約】

【課題】秘密情報の不正利用の防止に有利な半導体記憶装置を提供する。

【解決手段】実施形態によれば、半導体記憶装置は、外部からアクセスが可能な通常領域と、外部からのアクセスが制限され認証に利用される秘匿情報が記録される秘匿領域と、を少なくとも有するセルアレイ１１と、外部との認証を行う認証回路１７と、外部からのアクセスが可能な第１データキャッシュ回路と、外部からのアクセスが制限される第２データキャッシュ回路とを備えるデータキャッシュ１２とを具備し、外部から認証パラメータを含む認証要求を受信した場合、前記認証パラメータを前記第１データキャッシュ回路に格納し、前記秘匿領域から前記秘匿情報を読み出して前記第２データキャッシュ回路に格納して、外部への出力を禁止し、前記秘匿情報により前記認証パラメータを暗号処理して認証情報を取得し、前記認証情報を前記第１データキャッシュ回路に格納する。

【選択図】図３１

【図１】

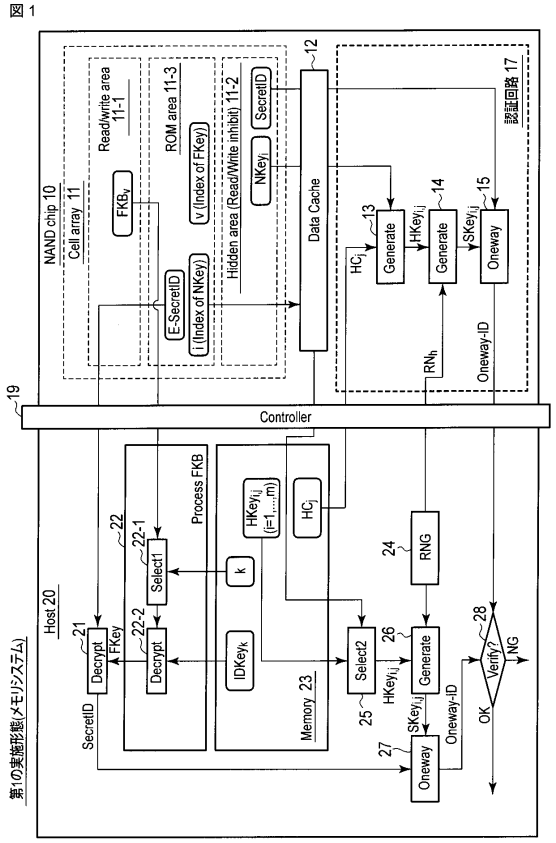


図 1
NAND chip 10
Cell array 11
Read/write area 11-1
FKB$_v$
ROM area 11-3
v (Index of FKey)
Hidden area (Read/Write inhibit) 11-2
SecretID
NKey$_j$
E-SecretID
i (Index of NKey)
Data Cache
12
認証回路 17
HC$_j$
13 Generate
HKey$_{i,j}$
14 Generate
SKey$_{i,j}$
15 Oneway
RN$_h$
Oneway-ID
19
Controller
Host 20
Process FKB
22
22-1 Select1
22-2 Decrypt
21 Decrypt
FKey
k
IDKey$_k$
HKey$_{i,j}$ (i=1,...,m)
HC$_j$
Memory 23
24 RNG
25 Select2
26 Generate
27 Oneway
28 Verify?
OK
NG
SecretID
第1の実施形態(メモリシステム)

【図２】

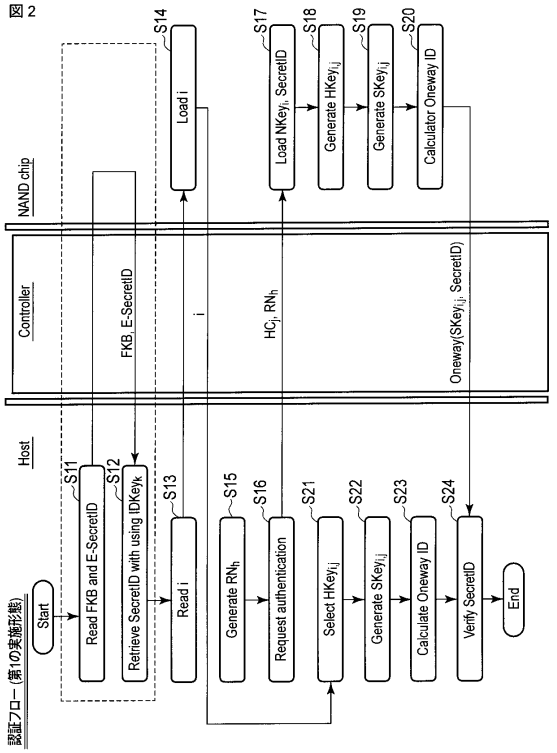


図 2
NAND chip
Controller
Host
S11 Read FKB and E-SecretID
S12 Retrieve SecretID with using IDKey$_k$
S13 Read i
S14 Load i
S15 Generate RN$_h$
S16 Request authentication
S17 Load NKey$_j$, SecretID
S18 Generate HKey$_{i,j}$
S19 Generate SKey$_{i,j}$
S20 Calculator Oneway ID
S21 Select HKey$_{i,j}$
S22 Generate SKey$_{i,j}$
S23 Calculate Oneway ID
S24 Verify SecretID
Start
End
FKB, E-SecretID
i
HC$_j$, RN$_h$
Oneway(SKey$_{i,j}$, SecretID)
認証フロー(第1の実施形態)

【図３】

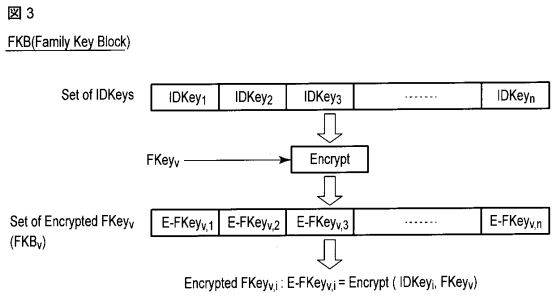


図 3
FKB(Family Key Block)
Set of IDKeys
IDKey$_1$ IDKey$_2$ IDKey$_3$ ····· IDKey$_n$
FKey$_v$
Encrypt
Set of Encrypted FKey$_v$ (FKB$_v$)
E-FKey$_{v,1}$ E-FKey$_{v,2}$ E-FKey$_{v,3}$ ····· E-FKey$_{v,n}$
Encrypted FKey$_{v,i}$: E-FKey$_{v,i}$ = Encrypt (IDKey$_i$, FKey$_v$)

【図４】

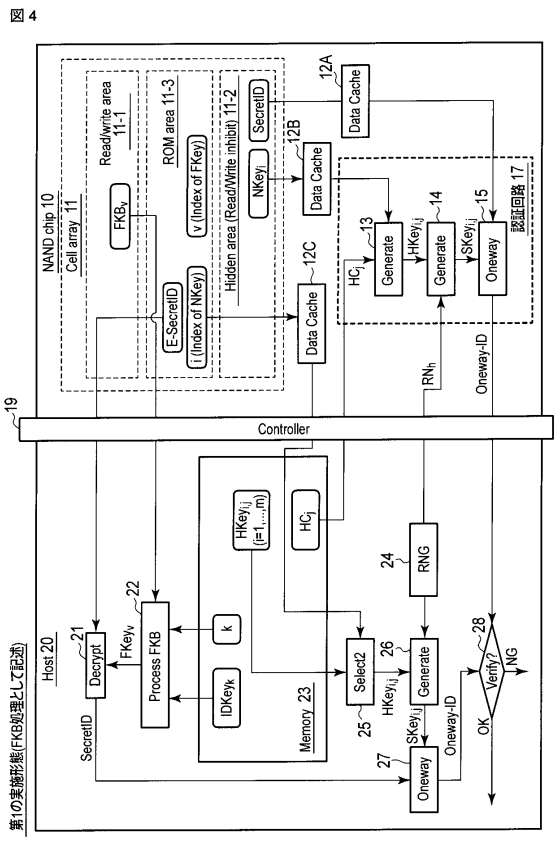
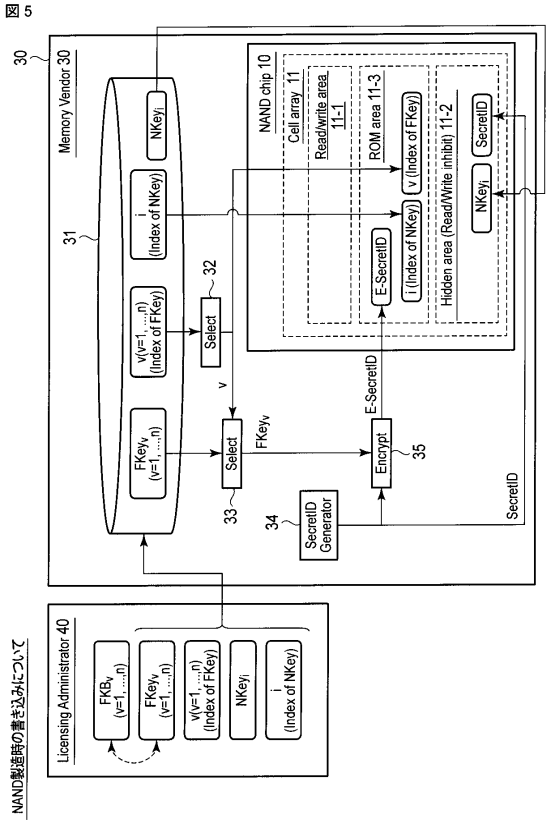


図 4
NAND chip 10
Cell array 11
Read/write area 11-1
FKB$_v$
ROM area 11-3
v (Index of FKey)
Hidden area (Read/Write inhibit) 11-2
SecretID
NKey$_j$
E-SecretID
i (Index of NKey)
12A Data Cache
12B Data Cache
12C Data Cache
HC$_j$
13 Generate
HKey$_{i,j}$
14 Generate
SKey$_{i,j}$
15 Oneway
認証回路 17
RN$_h$
Oneway-ID
19
Controller
Host 20
Process FKB
22
21 Decrypt
FKey$_v$
k
IDKey$_k$
HKey$_{i,j}$ (i=1,...,m)
HC$_j$
Memory 23
24 RNG
25 Select2
26 Generate
27 Oneway
28 Verify?
OK
NG
SecretID
第1の実施形態(FKB処理として記述)

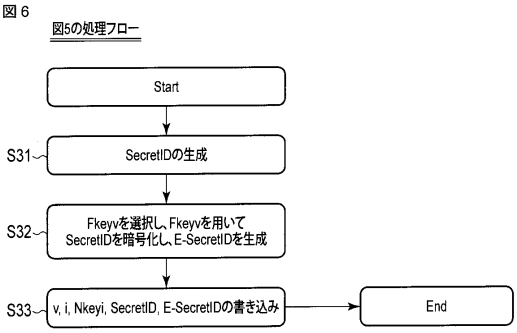
【図５】

図５



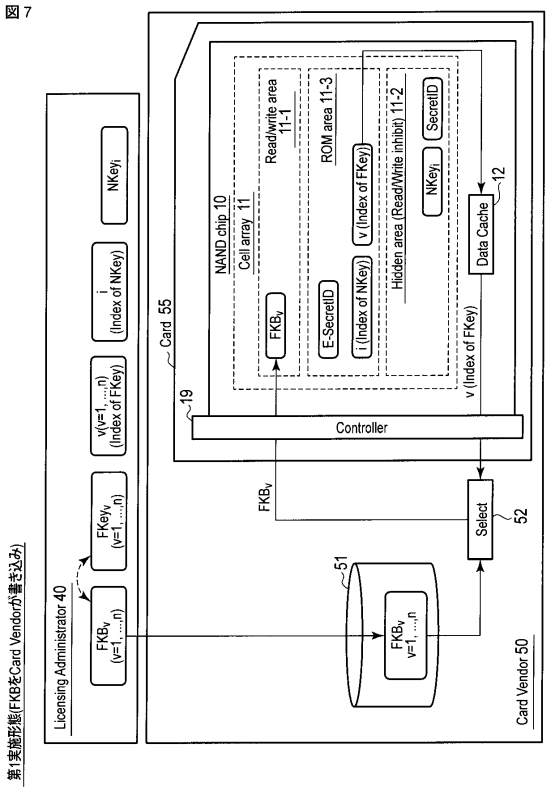
【図６】

図６



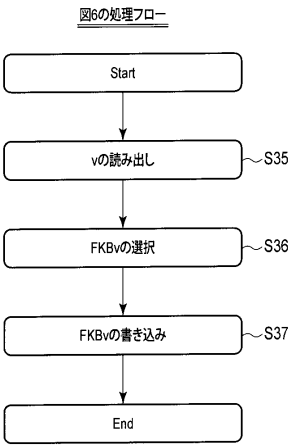
【図７】

図７



【図８】

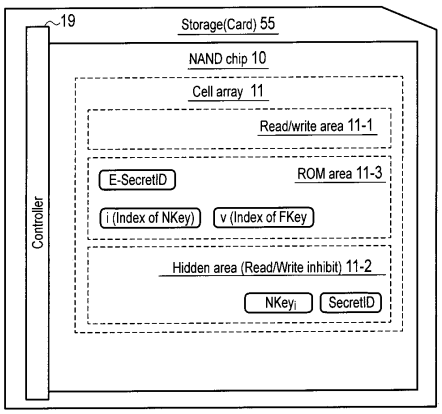
図８



【図９】

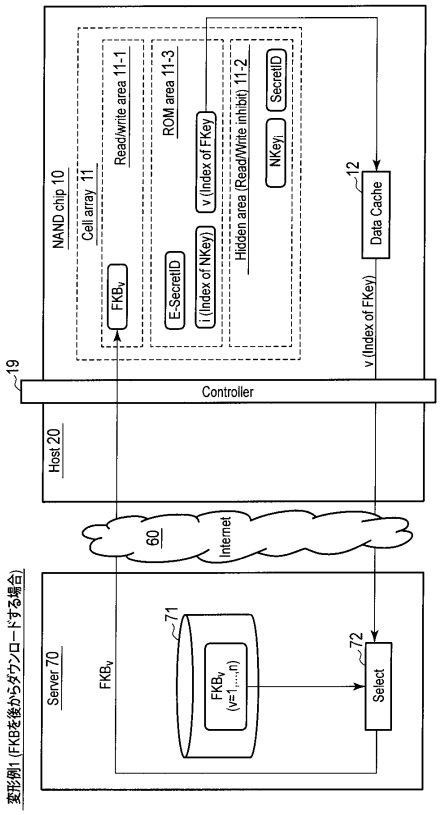
図 9

変形例1(Storage(Card)販売時にFKBが未記録の場合)



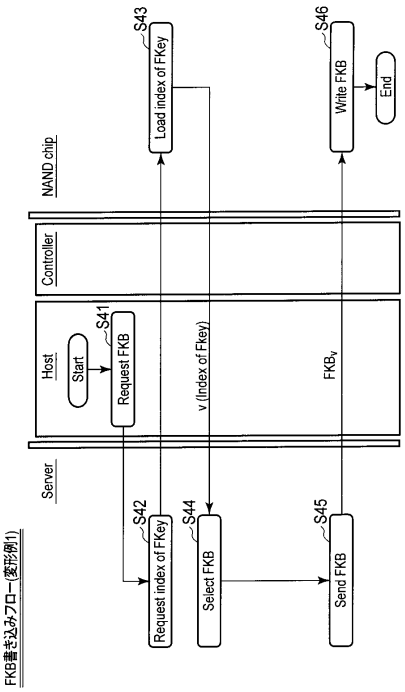
【図１０】

図 10



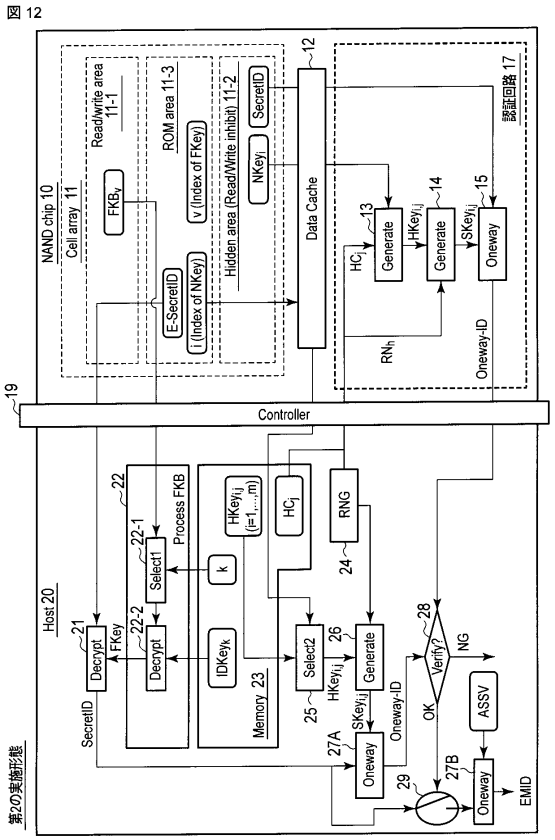
【図１１】

図 11

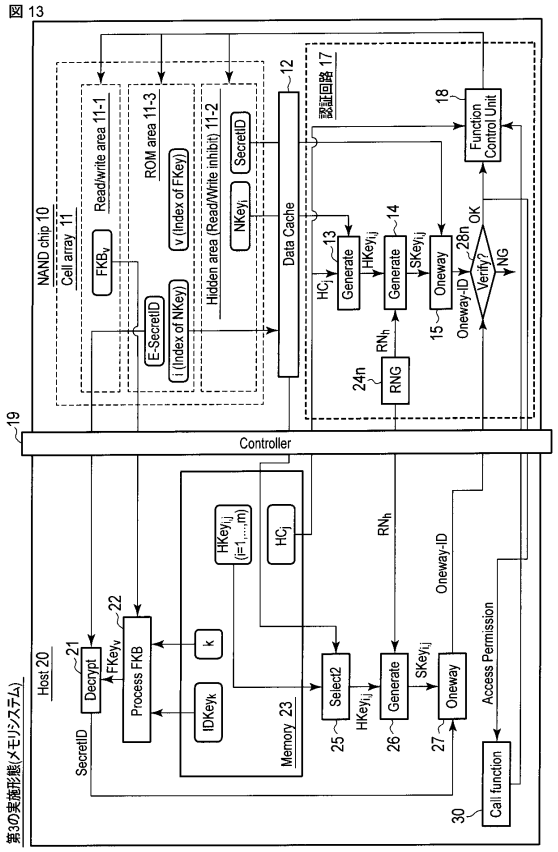


【図１２】

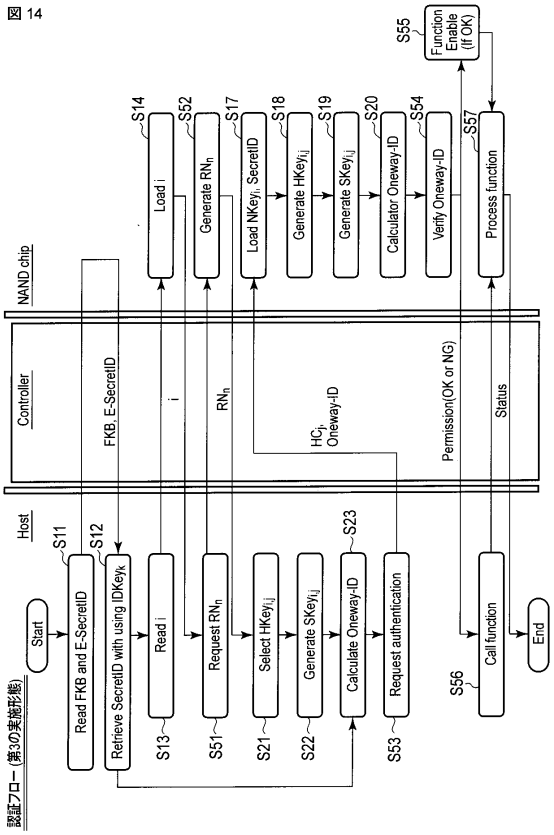
図 12



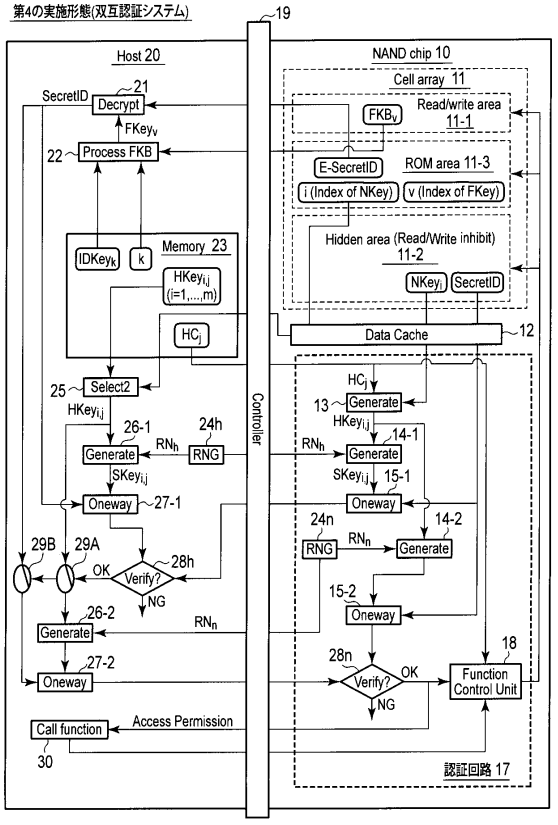
【図１３】



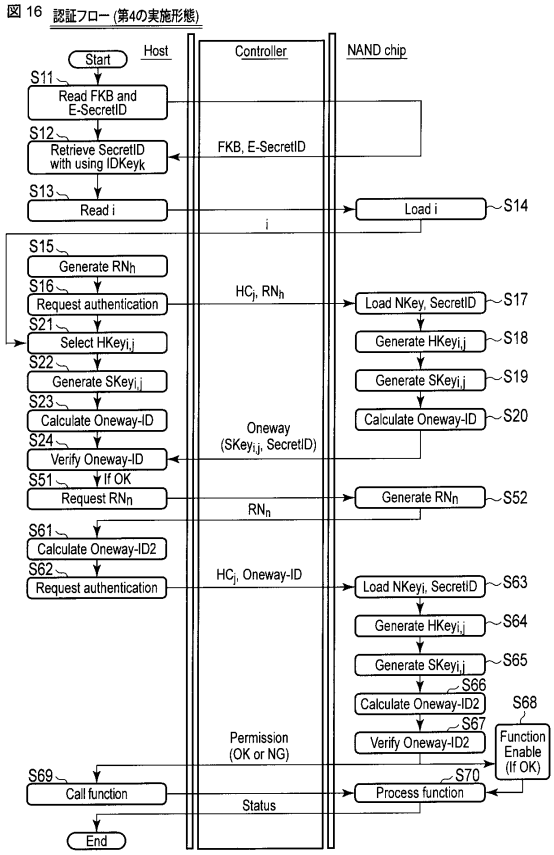
【図１４】



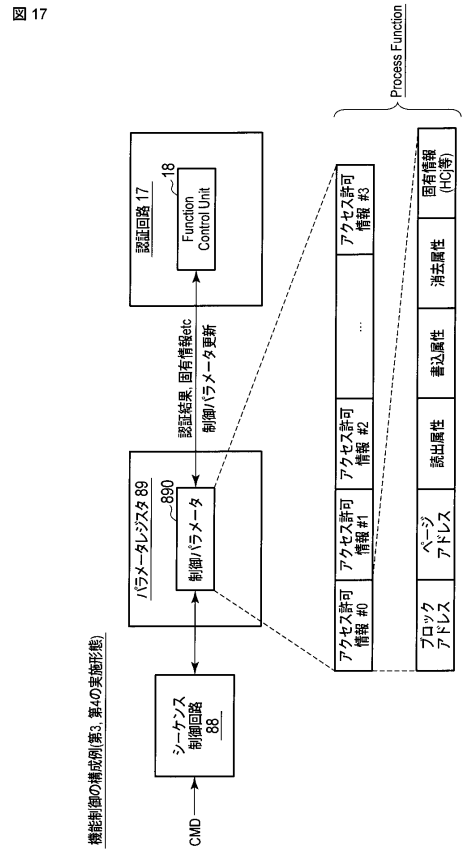
【図１５】



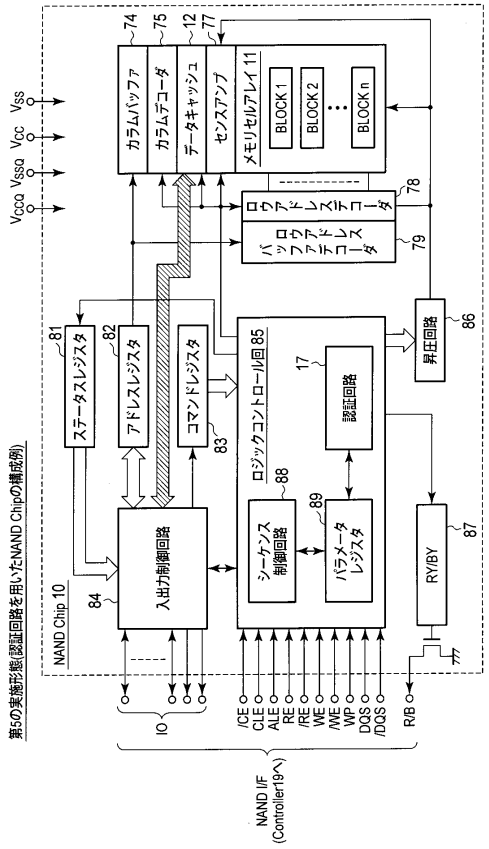
【図１６】



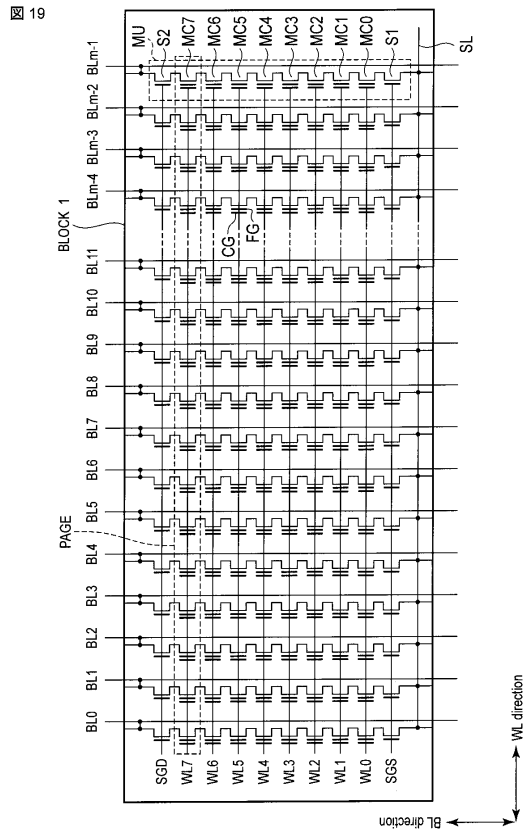
【図１７】



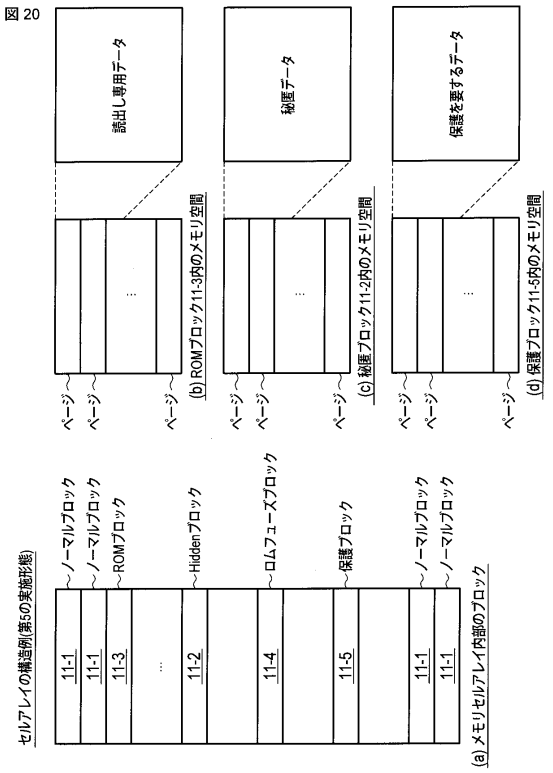
【図１８】



【図１９】

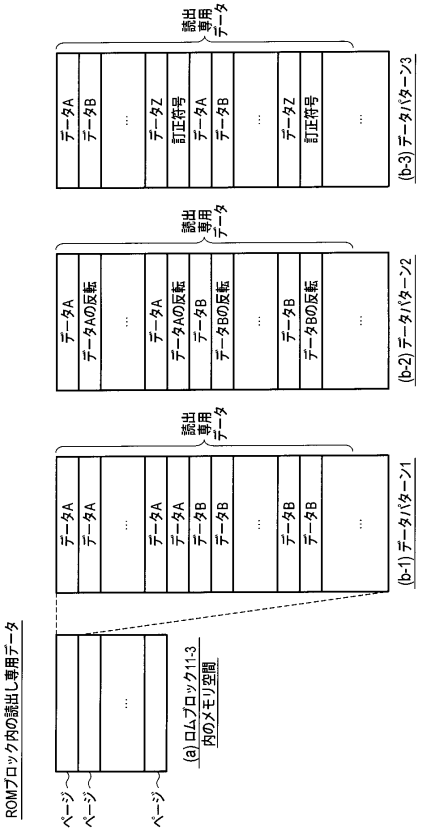


【図２０】



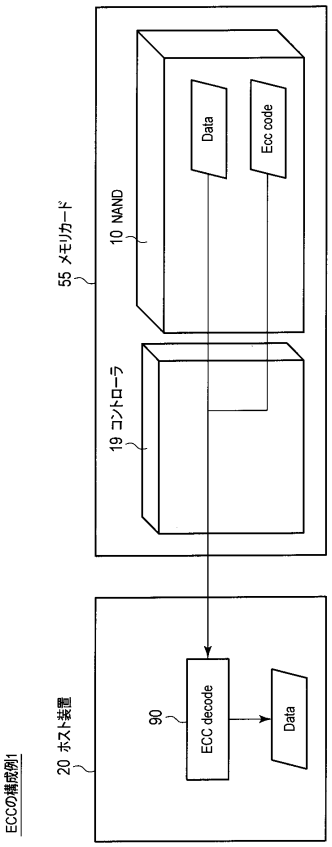
【図２１】

図21



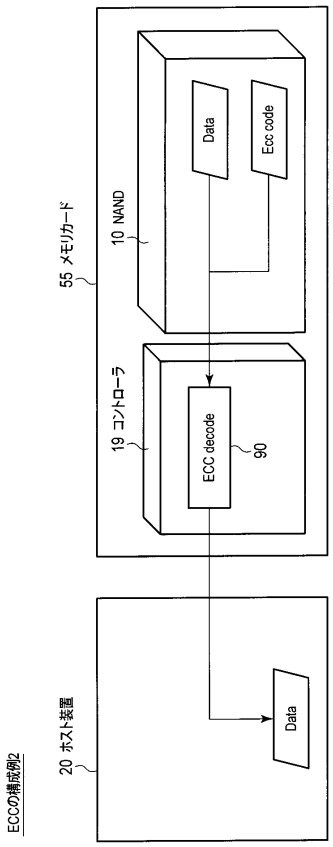
【図２２】

図22



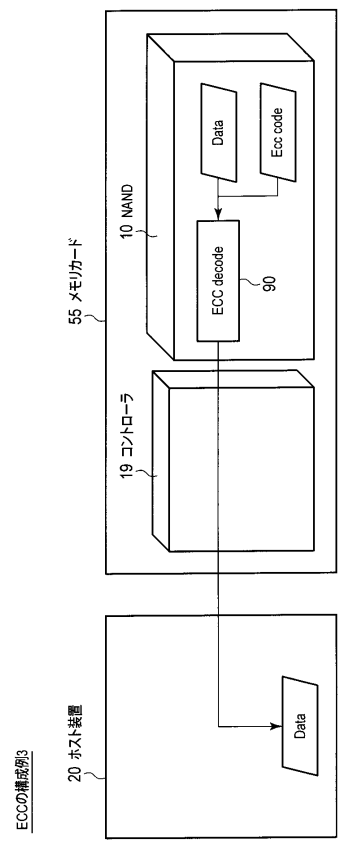
【図２３】

図23



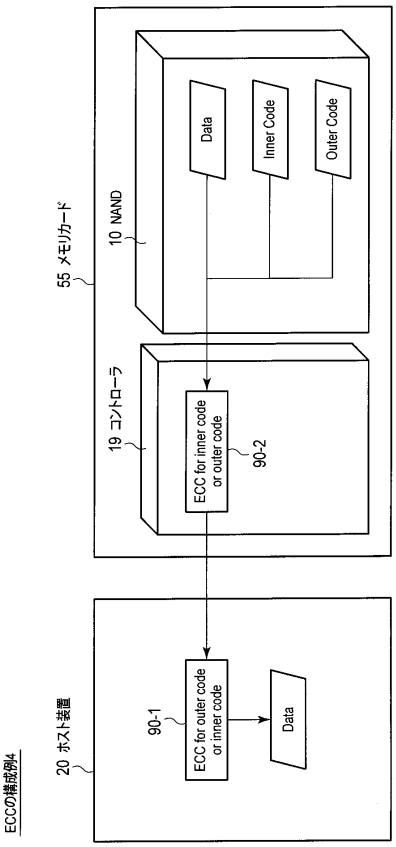
【図２４】

図24



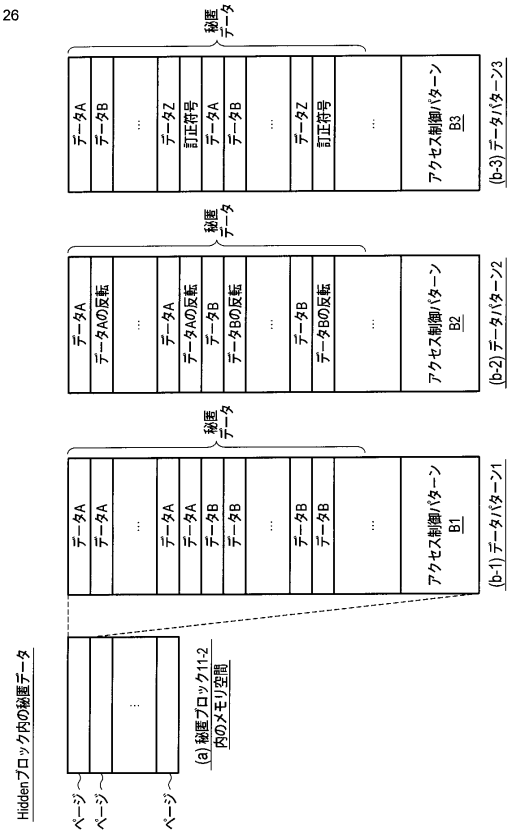
【図２５】

図 25



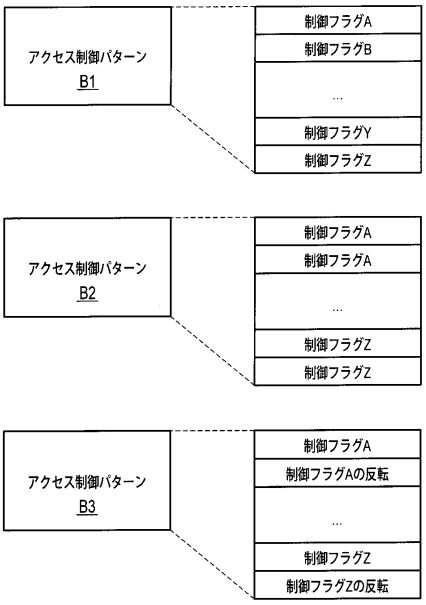
【図２６】

図 26



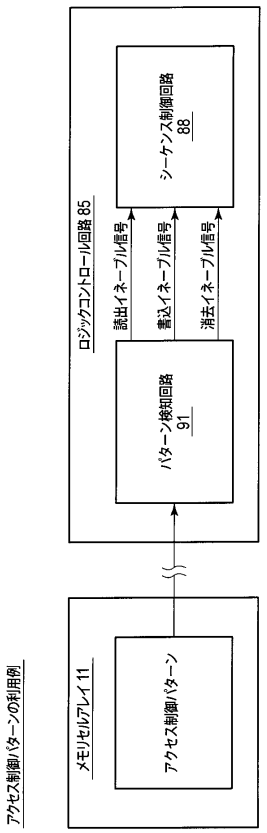
【図２７】

図 27 アクセス制御パターンの例



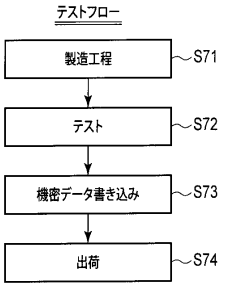
【図２８】

図 28



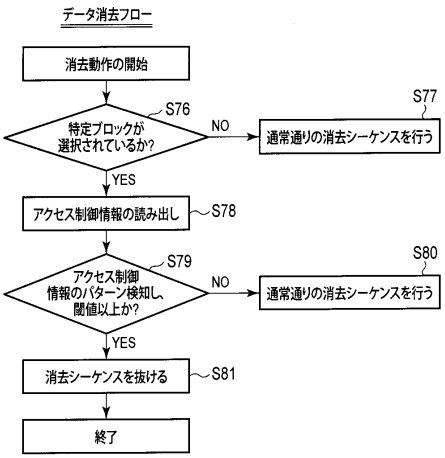
【図２９】

図 29



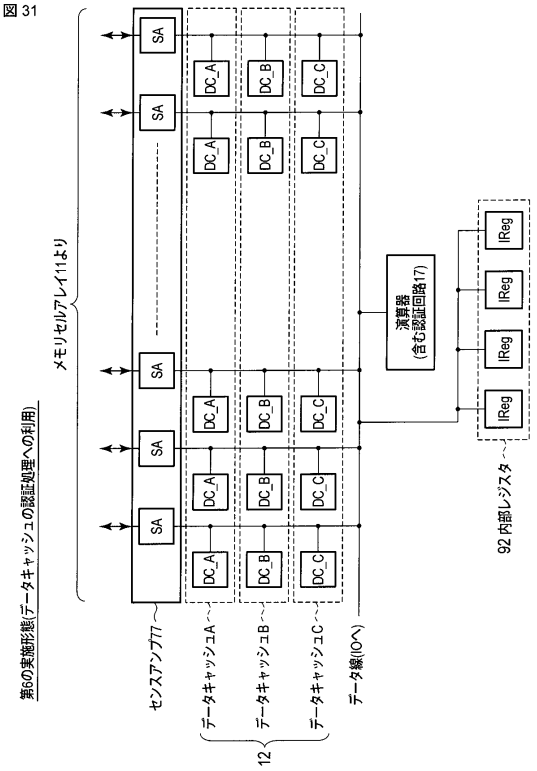
【図３０】

図 30



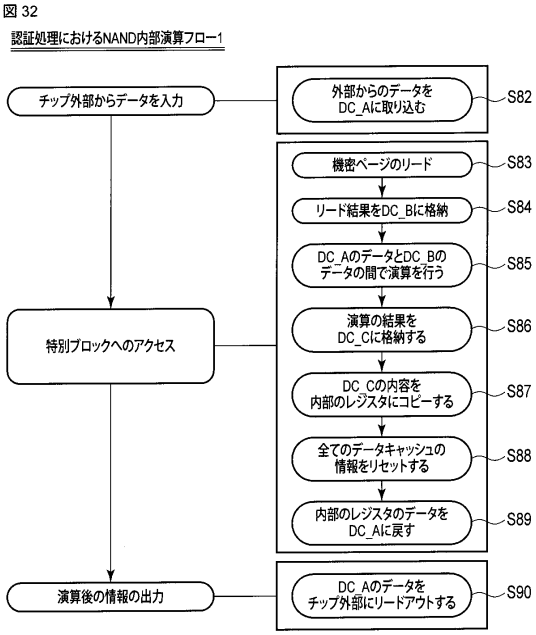
【図３１】

図 31



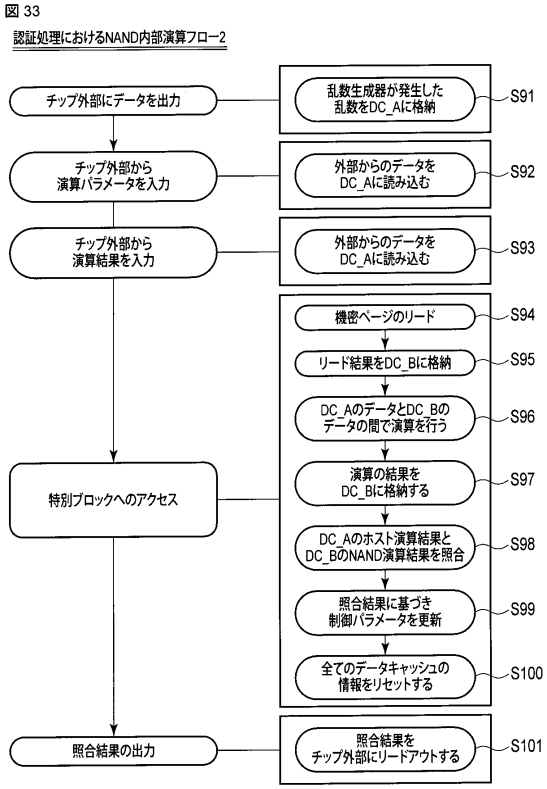
【図３２】

図 32



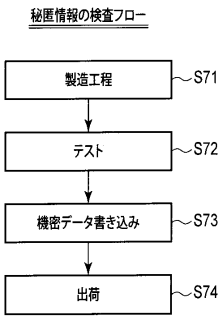
【図３３】

図 33



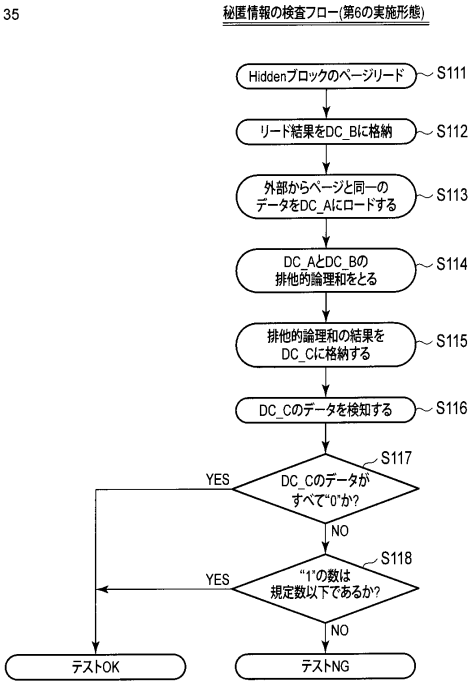
【図３４】

図 34



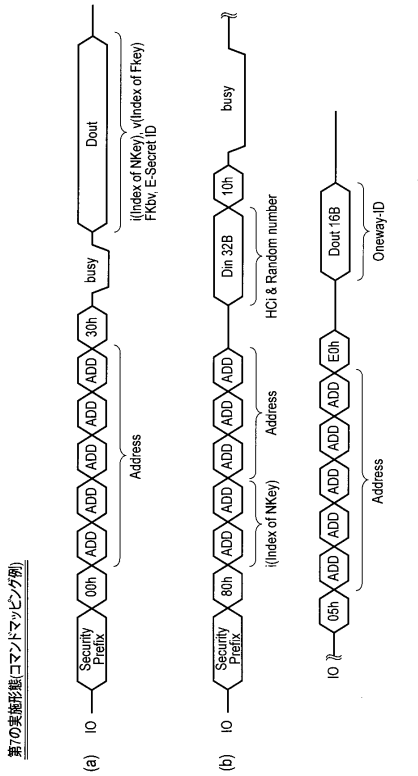
【図３５】

図 35



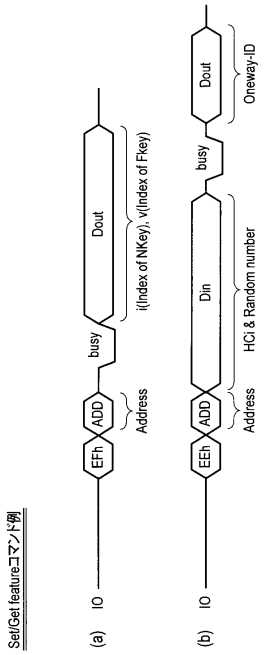
【図３６】

図 36

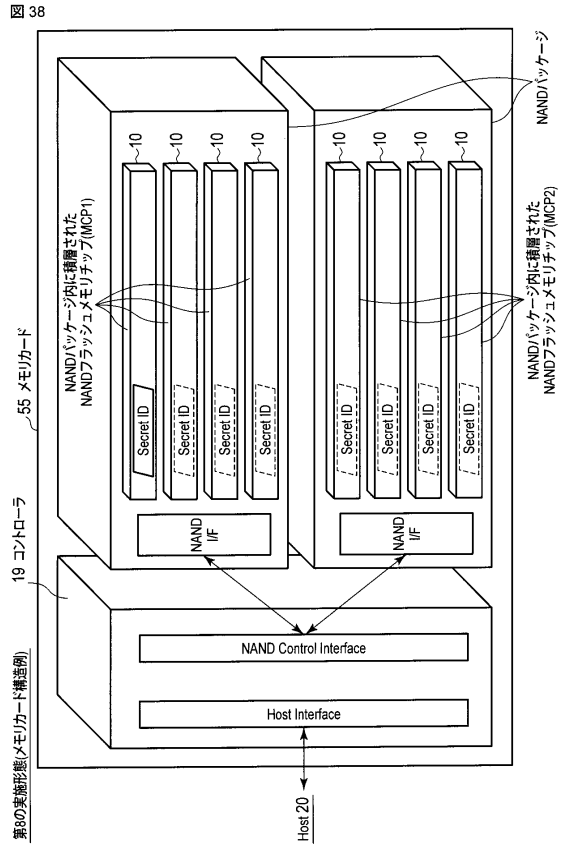


【図３７】

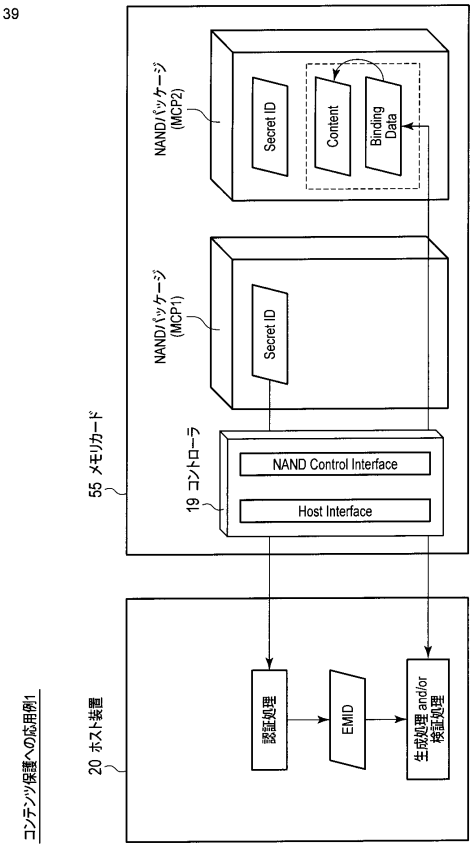
図 37



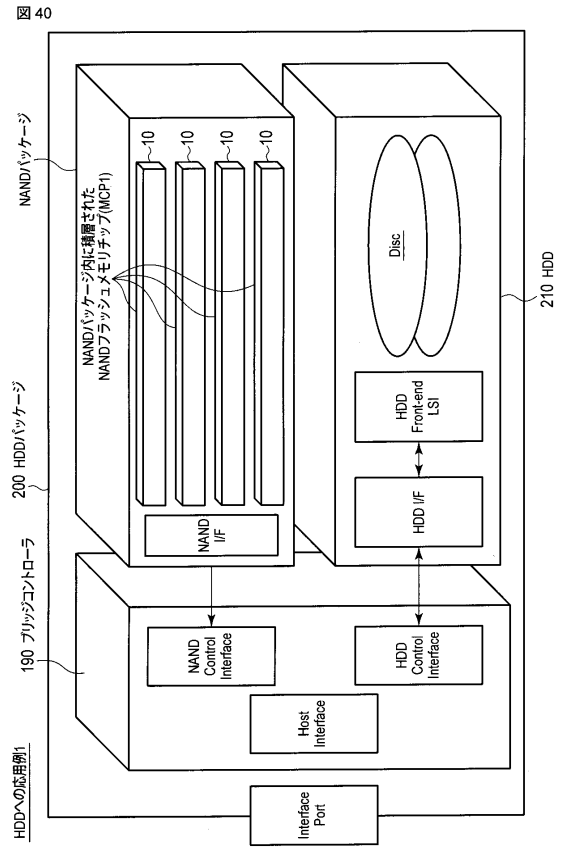
【図３８】



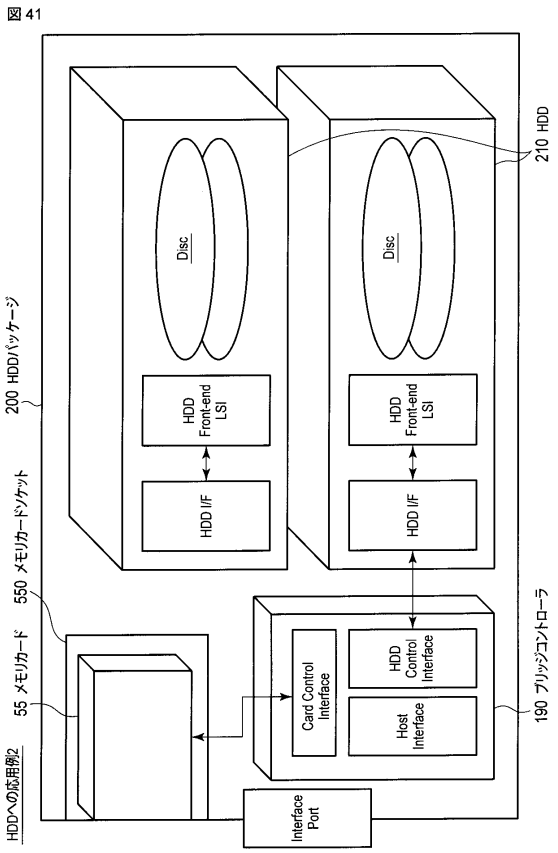
【図３９】



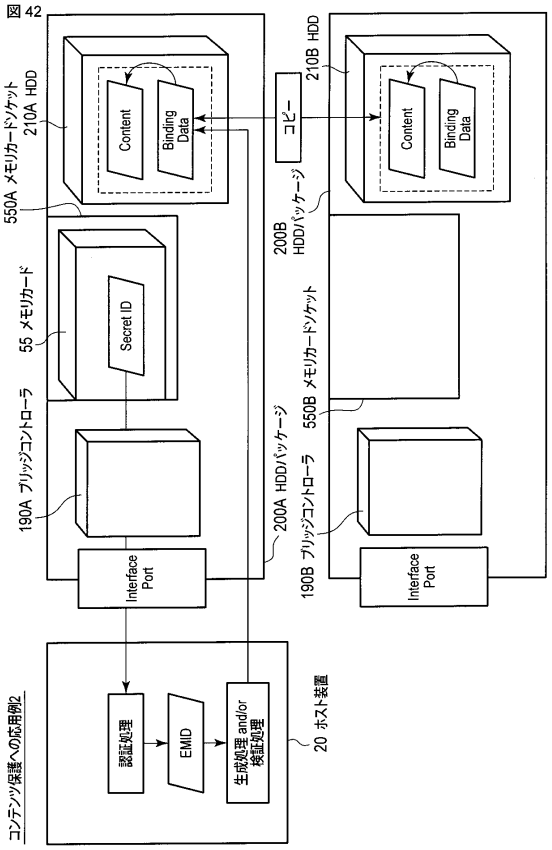
【図４０】



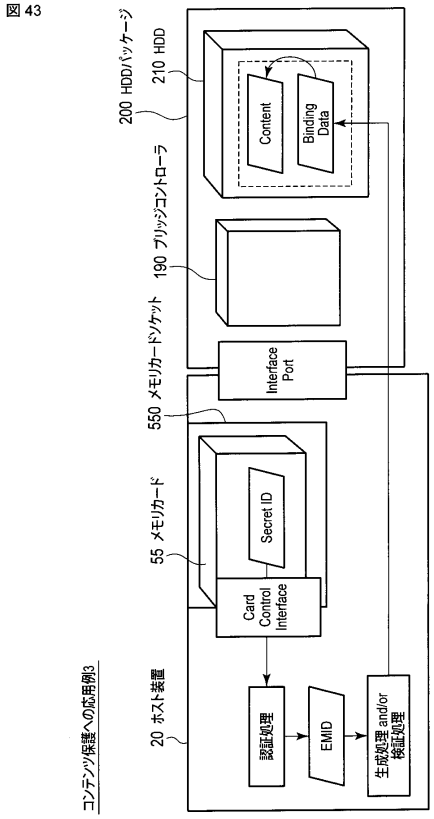
【図４１】



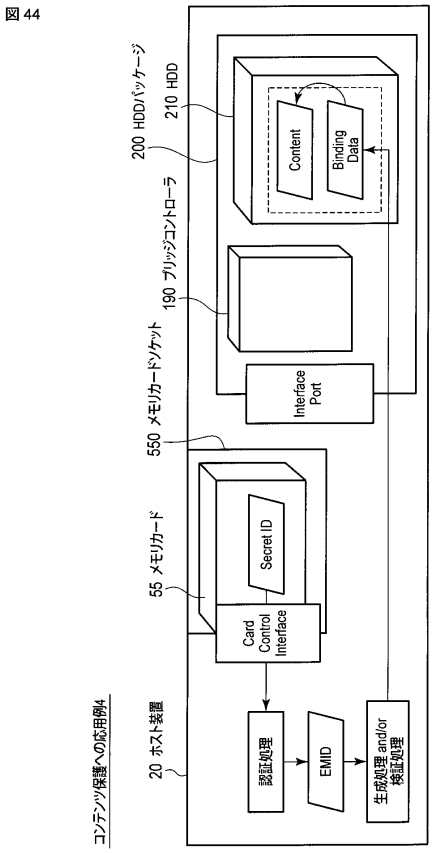
【図４２】



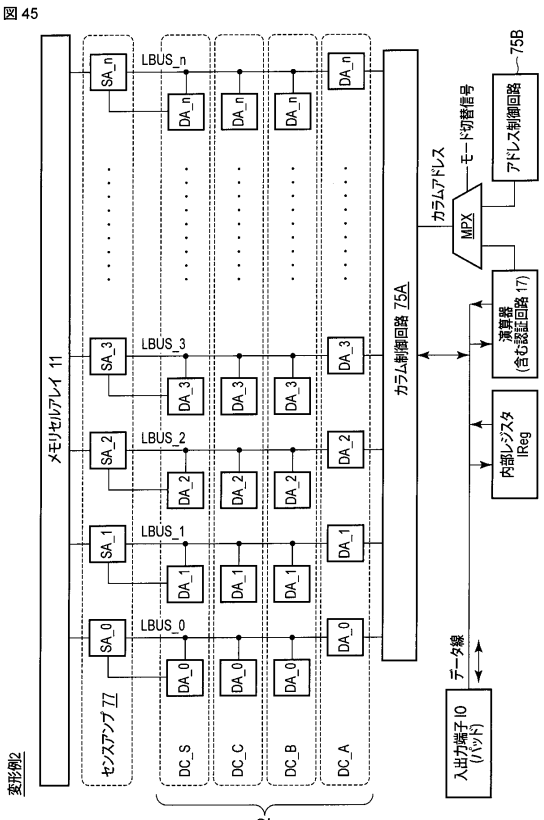
【図４３】



【図４４】

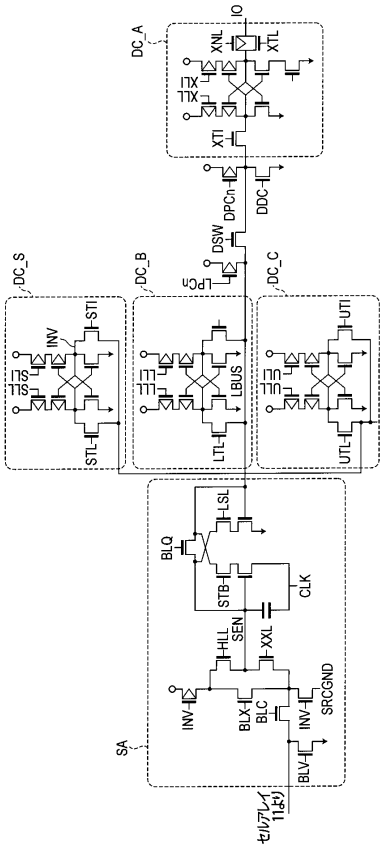


【図４５】



【図４６】

図46


IO
DC_A
XNL
XTL
XLL
XLI
XTI
DPCn
DDC
DSW
LPCn
DC_S
DC_B
DC_C
STI
INV
SLL
SLI
STL
LTL
LBUS
LLL
LLI
UTI
ULL
ULI
UTL
LSL
BLQ
STB
CLK
HLL
SEN
XXL
INV
BLX
BLC
INV
SRCGND
BLV
SA
セルアレイ(1ビット)

フロントページの続き

(51)Int.Cl. FI
G11C 16/02 (2006.01) G11C 17/00 601T

(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100158805
弁理士 井関 守三
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(72)発明者 長井 裕士
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 鈴木 俊宏
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 柴田 昇
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 加藤 拓
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 松下 達之
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 岸野 徹

(56)参考文献 特許第４９９１９７１（ＪＰ，Ｂ１）
特開２００９－０２７５５７（ＪＰ，Ａ）
特開２０１０－２６８４１７（ＪＰ，Ａ）
特開２００４－２５２７０７（ＪＰ，Ａ）
特開２００８－２６９０８８（ＪＰ，Ａ）
特開２０１２－０１４４１６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １２／１４
Ｇ０６Ｆ ２１／２２

G06F 21/24
H04L 9/08
H04L 9/32