世界知的所有権機関
国際事務局

PCT 特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 **G06F 12/14**	**A1**	(11) 国際公開番号 **WO99/38078** (43) 国際公開日 1999年7月29日(29.07.99)

(21) 国際出願番号 PCT/JP99/00170

(22) 国際出願日 1999年1月20日(20.01.99)

(30) 優先権データ
特願平10/9303 1998年1月21日(21.01.98) JP

(71) 出願人（米国を除くすべての指定国について）
東京エレクトロン株式会社
(TOKYO ELECTRON LIMITED)[JP/JP]
〒107-8481 東京都港区赤坂五丁目3番6号 Tokyo, (JP)
株式会社 ビー・ユー・ジー (B.U.G., INC.)[JP/JP]
〒004-0015 北海道札幌市厚別区下野幌テクノパーク一丁目1番14号 Hokkaido, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
中村泰弘(NAKAMURA, Yasuhiro)[JP/JP]
〒191-0041 東京都日野市南平5-2-1 アルカディア梨園103 Tokyo, (JP)
平賀誠二(HIRAKA, Seiji)[JP/JP]
〒023-0041 岩手県水沢市秋葉町32-3 Iwate, (JP)
浅田一憲(ASADA, Kazunori)[JP/JP]
〒062-0000 北海道札幌市豊平区清田7条1丁目18番5号 Hokkaido, (JP)
江良 聡(ERA, Satoshi)[JP/JP]
〒069-0803 北海道江別市野幌屯田町13-19 Hokkaido, (JP)
(74) 代理人
弁理士 木村 満(KIMURA, Mitsuru)
〒101-0054 東京都千代田区神田錦町二丁目7番地 協販ビル7階 Tokyo, (JP)

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

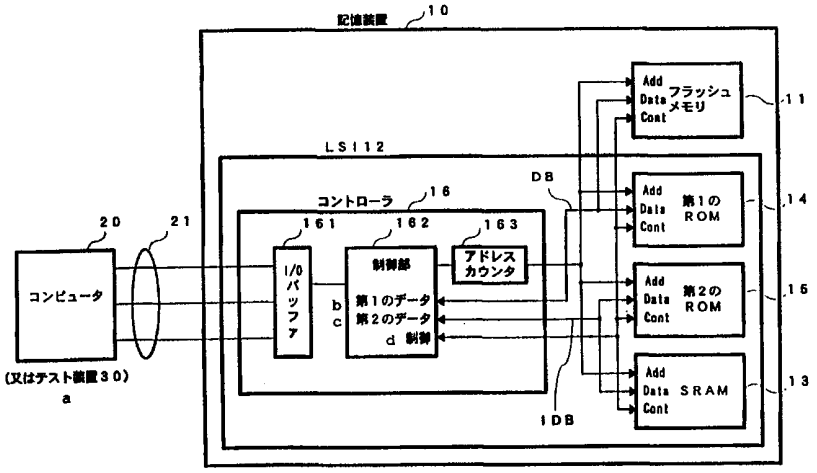
添付公開書類
国際調査報告書

(54)Title: **STORAGE DEVICE, ENCRYPTING/DECRYPTING DEVICE, AND METHOD FOR ACCESSING NONVOLATILE MEMORY**

(54)発明の名称 記憶装置、暗号化・復号化装置、及び不揮発性メモリのアクセス方法

(57) Abstract

A storage device (10) has a flash memory (11), a controller (16), and a second ROM (15). In the flash memory (11), a data key is stored, which is a key specific to each storage device (10). In the second ROM (15), a system key is stored, which is an encrypting key common to storage devices (10). The controller (16), to write data, encrypts the data with the data and system keys and writes the encrypted data in the flash memory (11); and to read data, decrypts the data with the data and system keys to output the decrypted data. The data key may be encrypted with the system key. In this case, to write data, the controller (16) may decrypt the data key with the system key, and encrypt data with the decrypted key; and to read data, the controller may decrypt the data key with the system key, and decrypt the encrypted data with the decrypted data key.



10 ... STORAGE DEVICE
11 ... FLASH MEMORY
14 ... FIRST ROM
15 ... SECOND ROM
16 ... CONTROLLER
20 ... COMPUTER
161 ... I/O BUFFER
161 ... I/O BUFFER
162 ... CONTROL SECTION
163 ... ADDRESS COUNTER
a ... OR TESTER 30
b ... FIRST DATA
c ... SECOND DATA
d ... CONTROL

(57)要約

記憶装置（１０）は、フラッシュメモリ（１１）とコントローラ（１６）と第２のＲＯＭ１５とを備える。フラッシュメモリ（１１）には、データ鍵が格納されている。第２のＲＯＭ（１５）には、システム鍵が登録されている。システム鍵は複数の記憶装置（１０）に共通の暗号鍵であり、データ鍵は各記憶装置（１０）に固有の鍵である。コントローラ（１６）はデータを書き込む際は、データ鍵とシステム鍵を用いてデータを暗号化して、フラッシュメモリ（１１）に書き込む。データを読み出す際は、データ鍵とシステム鍵を用いてデータ鍵を復号化して、外部に出力する。データ鍵は、システム鍵により暗号化されていてもよい。この場合、コントローラ（１６）は、データを書き込む際、データ鍵をシステム鍵で復号化し、復号化したデータ鍵を用いてデータを暗号化してもよい。データを読み出す際は、システム鍵を用いてデータ鍵を復号化し、暗号化されたデータを復号化されたデータ鍵を用いて復号化してもよい。

明細書

記憶装置、暗号化・復号化装置、及び不揮発性メモリのアクセス方法

この特許出願は、平成１０年１月２１日に日本国特許庁に出願された特願平１０－９３０３のパリ条約に基づく優先権を主張する出願であり、この日本国特許出願の内容は参照のため、この明細書に取り込むものとする。

技術分野

この発明は、コンピュータ等の外部記憶装置等として使用される記憶装置に関し、特に、データを暗号化した状態で保存する記憶装置に関する。

背景技術

コンピュータ技術の発展に伴い、機密情報の保護の必要性が増大している。このため、データを暗号化して記憶したり、送信したりする暗号化技術の重要性が高まっており、例えば、記憶装置に暗号鍵を格納しておき、データをこの暗号鍵を用いて暗号化してメモリに格納し、メモリから読み出されたデータをこの暗号鍵を用いて復号化すること等が行われている。

しかし、暗号鍵を全ての記憶装置に共通にすると、１つの記憶装置の暗号鍵が知られると、大量生産されている他の記憶装置の暗号鍵も知られることになり、記憶データが解読されるおそれがある。

記憶装置に個別に暗号鍵を設定することも可能であるが、製造工程が増加し、記憶装置の製造コストが上昇してしまう。

また、コンピュータで全てのデータを暗号化してメモリカードに格納し、メモリカードから読み出したデータをコンピュータで復号化する技術も知られている。しかし、この方法では、コンピュータと記憶装置間の通信をモニタすることにより、暗号鍵が知られてしまうおそれがある。

この発明は上記実状に鑑みてなされたもので、データを暗号化及び復号化する機能を備え、且つ、暗号鍵等の機密情報の漏洩の虞の少ない記憶装置を提供することを目的とする。

また、この発明は、たとえ、一部の記憶装置の暗号鍵等が漏洩しても、他の記憶装置の暗号鍵が漏洩することのない記憶装置を提供することを他の目的とする。

発明の開示

上記目的を達成するため、この発明の第１の観点にかかる記憶装置は、

データを記憶するための書換可能な不揮発性メモリ（１１）と、

前記不揮発性メモリをアクセスするための制御手段（１２）とより構成され、データを記憶するための記憶装置であって、

前記不揮発性メモリに第１の暗号鍵が格納され、前記制御手段内に第２の暗号鍵が格納され、前記第１の暗号鍵は、前記第２の暗号鍵により暗号化されており、

前記制御手段は、前記第２の暗号鍵を用いて前記第１の暗号鍵を復号化する鍵復号手段（１２）と、前記鍵復号手段により復号化された第１の暗号鍵を用いてデータを暗号化して前記不揮発性メモリに書き込む書込手段（１２）と、前記不揮発性メモリからデータを読み出して、前記鍵復号手段により復号化された前記第１の暗号鍵を用いて読み出したデータを復号化する読出手段（１２）とを備える、

ことを特徴とする。

この記憶装置によれば、第１と第２の暗号鍵を使用し、これらを分散して格納し、さらに、第１の暗号鍵を第２の暗号鍵で暗号化しているので、暗号鍵が１つの場合よりも、暗号鍵が漏洩する危険が少なく、データが盗用されにくい。

特に、第１の暗号鍵を書き換え可能な不揮発性メモリに格納しているので、第１の暗号鍵を装置毎、或いは、一定台数毎に変更することができる。従って、第２の暗号鍵が漏洩しても、全ての記録装置のデータを解読することは困難である。

また、不揮発性メモリは、データを格納するために用意されているものであり、第１の暗号鍵を格納しても、コスト等が上昇することがない。

前記第２の暗号鍵は複数の前記記憶装置に共通であり、前記第１の暗号鍵は、同一の第２の暗号鍵を記憶している前記記憶装置の一部のみに共通或いはそれぞれに固有の暗号鍵である。この構成により、装置毎に異なる暗号鍵を使用できる。

例えば、前記不揮発性メモリはフラッシュメモリ（１１）から構成され、前記制御手段は前記第２の暗号鍵を記憶したマスクＲＯＭ（読み出し専用メモリ）（１５）から構成される。マスクＲＯＭなどは大量生産に適しており、第２の暗号鍵を含む情報を安価に製造することができる。一方、フラッシュメモリは、書き換え可能であり、第１の暗号鍵を装置毎又は所定台数毎に変更して、任意のタイミングで記録することができる。

パスワードを取り込み、正しいパスワードが入力された場合のみ、前記暗号化された第１の暗号鍵を復号化するようにしてもよい。この場合、例えば、前記第１の暗号鍵は、前記第２の暗号鍵とパスワードを基に生成された第３の暗号鍵により暗号化されて前記不揮発性メモリに格納され、前記鍵復号手段は、パスワードを入力する手段と、入力されたパス

ワードから第３の暗号鍵を生成する手段と、前記第２の暗号鍵と生成された第３の暗号鍵とを用いて前記暗号化されている第１の暗号鍵を復号化する手段を備える。

前記鍵復号手段は、例えば、復号プログラムと該復号プログラムを実行する手段（１６）とより構成され、前記復号プログラムは前記不揮発性メモリに格納される。このような構成とすれば、パスワードに応じた復号プログラムを適宜不揮発性メモリに記録することができる。

前記鍵復号手段と前記書込手段と前記読出手段は、復号化された第１の暗号鍵を記憶し、外部からのアクセスに対して保護された揮発性メモリ（１３）を含む。復号化された第１の暗号鍵はＲＡＭ（ランダムアクセスメモリ）などに格納され、使用される。このＲＡＭの内容が外部から読み出せると、不揮発性メモリに格納されたデータが解読されてしまう。このため、揮発性メモリは、外部からのアクセスに対してプロテクトされていることが望ましい。

前記不揮発性メモリは、例えば、フラッシュメモリ（１１）である。

前記制御手段は、前記第１の暗号鍵を生成し、生成した第１の暗号鍵を前記第２の暗号鍵を用いて暗号化して前記不揮発性メモリに記録する鍵生成手段（１６）を備えるものであってもよい。この構成によれば、記憶装置自体が第１の暗号鍵を生成し、データの暗号化・復号化に使用することができる。

前記鍵生成手段は、入力されたパスワードに基づいて前記第１の暗号鍵を生成するように構成してもよい。このような構成とすることにより、第１の暗号鍵の特定が一層困難となる。

前記第２の暗号鍵は、例えば、複数の記憶装置に共通の暗号鍵であってもよい。このような構成とすれば、制御手段を、複数の装置に共通な暗号鍵が格納されたマスクＲＯＭ等を備えるものとするなどして、コス

トを低減できる。

また、この発明の第２の観点にかかる記憶装置は、

第１の暗号鍵とデータを記憶するための書換可能な不揮発性メモリ（１１）と、

第２の暗号鍵を記憶し、前記不揮発性メモリをアクセスするための制御手段（１２）と、

より構成され、データを記憶する記憶装置であって、

前記制御手段は、前記第１と第２の暗号鍵を用いてデータを暗号化して前記不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読みだして前記第１と第２の暗号鍵を用いて復号化して出力する読出手段（１６）とを備える、

ことを特徴とする。

このような構成によれば、不揮発性メモリに格納されているデータは複数の暗号鍵を用いて暗号化されている。従って、両方の暗号鍵を知らなければ、不揮発性メモリに記録されているデータを復号できず、単一の暗号鍵を使用する場合よりも、機密性の高いデータを安全に記憶することができる。

また、２つの暗号鍵が、記憶装置内の異なった位置に分散して格納されているので、暗号鍵の特定が困難である。

例えば、前記第２の暗号鍵は、複数の記憶装置に共通の暗号鍵であり、前記制御手段に配置された読出専用メモリ（１５）に格納される。また、前記第１の暗号鍵は、前記第２の暗号鍵を共通とする複数の記憶装置の一部のみに共通又は固有の暗号鍵である。

第１の暗号鍵を書き換え可能な不揮発性メモリに格納することにより、例えば、記憶装置毎に容易に第１の暗号鍵を変更することができる。また、複数の記憶装置に共通の第２の暗号鍵を読出専用メモリに格納する

ことにより、第２の暗号鍵を記憶するメモリを大量生産する事が可能となる。

例えば、前記不揮発性メモリは、フラッシュメモリ（１１）であり、前記読出専用メモリはマスクＲＯＭ（読み出し専用メモリ）（１５）である。

また、この発明の第３の観点にかかる記憶装置は、

暗号化された暗号鍵を記憶する暗号鍵記憶手段（１１）と、

前記暗号鍵を用いて暗号化されたデータを記憶するための書換可能な不揮発性メモリ（１１）と、

前記暗号鍵を復号する復号手段（１６）と、前記復号手段により復号された暗号鍵を記憶する揮発性メモリ（１３）と、前記揮発性メモリに記憶された暗号鍵を用いて外部より供給されるデータを暗号化して前記不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読み出し、読み出したデータを前記揮発性メモリに記憶されている暗号鍵を用いて復号化して出力する読出手段（１６）とを備える制御手段（１２）と、前記揮発性メモリへの外部からのアクセスを禁止する禁止手段（１６，２２，ＩＤＢ，２５）と、を備え、

復号化された暗号鍵への外部からのアクセスが防止されていることを特徴とする。

暗号鍵は、暗号化されているが、使用時には復号化され、揮発性メモリに格納される。従って、この揮発性メモリをアクセスして、データを読み出せば暗号鍵が知られてしまう。この発明では、禁止手段により、揮発性メモリへの外部からのアクセスを禁止しているので、このような事態を防止できる。

前記禁止手段は、例えば、前記制御手段を封止する封止手段（２５）と、前記封止手段に封止され、前記揮発性メモリと前記復号手段との間

でデータを伝送する内部バス（ＩＤＢ）と、を含む。この構成によれば、揮発性メモリが封止されているので、この揮発性メモリを外部から直接アクセスすることができない。また、復号手段と揮発性メモリ間のバスも封止されているので、バス上のデータをプローブして、暗号鍵を判別することも困難である。

前記暗号鍵記憶手段と前記復号手段との間で暗号化された暗号鍵を伝送し、及び、前記書込手段及び前記読出手段と前記不揮発性メモリとの間で暗号化されているデータを伝送するデータバス（ＤＢ）と、前記内部バスとを別体に構成し、前記復号化された暗号鍵は前記データバス上には出力されないように構成することが望ましい。この構成により、外部に引き出されているバスをプローブして、暗号鍵をモニタする事態を防止できる。

前記禁止手段は、この記憶装置が開封されたことを検出する開封検出手段（２２）と、前記開封検出手段が開封を検出した際に、前記不揮発性メモリの内容を消去する手段（１６）を含んでもよい。

この構成によれば、不揮発性メモリや揮発性メモリへの不正なアクセスを禁止できる。

また、この発明の第４の観点にかかる記憶装置は、

不揮発性メモリと、

第１の暗号鍵を生成する鍵生成手段（１６）と、

第２の暗号鍵を記憶する鍵記憶手段（１５）と、

前記鍵生成手段により生成された前記第１の暗号鍵と前記鍵記憶手段に記憶されている前記第２の暗号鍵とを用いてデータを暗号化して前記不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読出して前記第１と第２の暗号鍵を用いて復号化して出力する読出手段（１６）とを備える、

ことを特徴とする。

この構成によれば、記憶装置自体が第１の暗号鍵を生成することができる。この暗号鍵を、例えば、使用者のパスワード等に基づいて生成するようにすれば、暗号鍵が装置毎に異なることになり、暗号の解読は非常に困難となり、システムの信頼度を高めることができる。

前記鍵生成手段は、生成した第１の暗号鍵を、前記不揮発性メモリに格納し、前記書込手段及び読出手段は、前記不揮発性メモリに格納された第１の暗号鍵を暗号化・復号化に使用してもよい。この構成によれば、例えば、フォーマット時等に、第１の暗号鍵を生成して不揮発性メモリに格納しておき、以後は、この鍵を使用するので、処理を高速化することができる。

入力されたパスワードに基づいて前記第１の暗号鍵を生成するように構成してもよい。このような構成とすることにより、第１の暗号鍵の特定が一層困難となる。

前記第２の暗号鍵は、例えば、複数の記憶装置に共通の暗号鍵であり、マスクＲＯＭ等の読出専用メモリからなる鍵記憶手段に格納される。このような構成とすれば、複数の装置に共通な暗号鍵をマスクＲＯＭ等で製造でき、コストを低減できる。

また、この発明の第５の観点にかかる記憶装置は、

第１の暗号鍵を記憶する第１の暗号鍵記憶手段（１１）と、

第２の暗号鍵を記憶する第２の暗号鍵記憶手段（１５）と、

第３の暗号鍵を記憶する第３の暗号鍵記憶手段（１５）と、

前記第１乃至第３の暗号鍵記憶手段に記憶された前記第１乃至第３の暗号鍵を用いてデータを暗号化して不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読出して前記第１乃至第３の暗号鍵を用いて復号化して出力する読出手段（１６）とを備え、

前記第１乃至第３の暗号鍵は、装置内において分散して配置されていることを特徴とする。

この発明によれば、３以上の暗号鍵を使用し、かつ、これらを分散して格納することにより、暗号の解読を非常に困難にすることができる。

また、この発明の第６の観点にかかる暗号化・復号化装置は、

第１の暗号鍵が格納された書換可能な不揮発性メモリ（１１）と、

第２の暗号鍵が格納された読み出し専用メモリ（１５）と、

データを前記第１と第２の暗号鍵を用いて暗号化して出力する暗号化手段（１６）と、暗号化されたデータを前記第１と第２の暗号鍵を用いて復号化して出力する復号化手段（１６）とを備える、

ことを特徴とする。

この構成によれば、２つの暗号鍵を用いてデータを暗号化・復号化することができる。しかも、読み出し専用メモリに、複数の装置に共通の第２の暗号鍵を配置し、不揮発性メモリに個別暗号鍵を格納することができる。

また、この発明の第７の観点に係る不揮発性メモリのアクセス方法は、

複数の装置に共通の共通暗号鍵を読出専用メモリに記憶させ、ユニークな個別暗号鍵を前記共通暗号鍵で暗号化して書換可能な不揮発性メモリに記憶させておき、

前記不揮発性メモリにデータを書き込む際は、前記共通暗号鍵を用いて前記個別暗号鍵を復号化し、復号化した前記個別暗号鍵を用いてデータを暗号化して前記不揮発性メモリに書き込み、

前記不揮発性メモリからデータを読み出す際は、前記共通暗号鍵を用いて前記個別暗号鍵を復号化し、前記不揮発性メモリから読み出したデータを復号化した個別暗号鍵を用いて復号化して出力する、

ことを特徴とする。

このアクセス方法によっても、暗号鍵が１つの場合よりも、暗号鍵が漏洩する危険が少なく、データが盗用されにくい。また、コストの上昇も少ない。

所定のパスワードが入力された時にのみ、前記個別暗号鍵を復号化するようにしても良い。この場合、前記個別暗号鍵は、前記共通暗号鍵とパスワードを基に生成された第３の暗号鍵により暗号化されて前記不揮発性メモリに記憶されており、パスワードを入力し、入力されたパスワードから前記第３の暗号鍵を生成し、前記共通暗号鍵と生成された第３の暗号鍵とを用いて前記個別暗号鍵を復号化する。

また、前記共通暗号鍵及び復号化された個別暗号鍵は、例えば、外部からのアクセスに対し、プロテクトされてもよい。このような構成とすることにより、信頼性をより高めることができる。

図面の簡単な説明

図１は、この発明の第１～第３の実施の形態にかかる記憶装置、コンピュータ、及び、テスト装置の基本構成を示すブロック図である。

図２は、フラッシュメモリと第２のＲＯＭの内部構成を示す図である。

図３は、フラッシュメモリへのデータの書き込み動作を説明するためのフローチャートである。

図４は、フラッシュメモリからのデータの読み出し動作を説明するためフローチャートである。

図５は、テスト動作を説明するためのフローチャートである。

図６は、機密情報を記憶した領域へのアクセスを禁止する構成の一例を説明するためのブロック図である。

図７は、テストモードで、ＳＲＡＭの内容をリセットする構成の一例を示す図である。

図８は、この発明の第４の実施の形態にかかる記憶装置のフラッシュメモリの構成を示す図である。

図９は、第２の実施の形態におけるデータ鍵復号動作を説明するためのフローチャートである。

図１０は、この発明の第４～第７の実施の形態にかかる記憶装置の構成を示すブロック図である。

図１１は、図１０に示すＥＥＰＲＯＭの構成を示す図である。

図１２は、第６の実施の形態にかかる記憶装置の暗号鍵生成処理を説明するためのフローチャートである。

図１３は、第７の実施の形態にかかる記憶装置の暗号鍵生成・記録処理を説明するためのフローチャートである。

図１４は、この発明の第８の実施の形態にかかる記憶装置の構造を示すブロック図である。

発明を実施するための最良の形態

以下、この発明の実施の形態にかかる記憶装置を、フラッシュメモリ装置を例に説明する。

図１は、この発明の第１の実施の形態にかかる記憶装置の構成を示す。

図示するように、記憶装置１０は、フラッシュメモリ１１と、フラッシュメモリ１１をアクセスするためのＬＳＩ１２とより構成されている。

フラッシュメモリ１１は、通常知られているように、ブロック消去型の記憶素子である。すなわち、フラッシュメモリ１１は、複数のメモリセルから構成された複数のブロックを備え、予め消去されたブロックにデータの書き込みが可能なメモリである。

フラッシュメモリ１１が有する記憶領域には、図２（Ａ）に示すように、エリアＴ１が含まれる。エリアＴ１には、データを暗号化及び復号

化するための暗号鍵であるデータ鍵ｋ１が、予め記録されている。データ鍵ｋ１は、十分大きなビット数の素数等から構成され、後述するシステム鍵ｋ２により暗号化されている。

また、ファイルの位置を示すファイルアロケーションテーブル（ＦＡＴ）、ディレクトリ情報、消去済みのブロックを示す空きブロックテーブル等もフラッシュメモリ１１に格納されている。

また、データ鍵ｋ１により暗号化されたデータもフラッシュメモリ１１に格納されている。

ＬＳＩ１２は、コンピュータ２０の制御に従って、フラッシュメモリ１１をアクセスするために種々の制御動作を行う。ＬＳＩ１２は、ＳＲＡＭ１３と、第１と第２のＲＯＭ１４、１５と、コントローラ１６と、より構成される。

ＳＲＡＭ（スタティックランダムアクセスメモリ）１３は、揮発性の高速メモリであり、コントローラ１６のワークエリアとして機能する。

第１のＲＯＭ（リードオンリメモリ）１４は、マスクＲＯＭ等からなる読出専用メモリであり、コントローラ１６の動作プログラムを記憶する。

第２のＲＯＭ１５は、マスクＲＯＭ等からなる読出専用メモリである。第２のＲＯＭ１５が有する記憶領域には、図２（Ｂ）に示すように、システム鍵エリアＴ２、復号プログラム記憶エリアＴ３、期待値エリアＴ４及びハッシュ関数エリアＴ５が含まれる。

システム鍵エリアＴ２は、全ての記憶装置１０に共通に設定された暗号鍵であるシステム鍵ｋ２を記憶する。復号プログラム記憶エリアＴ３は、データ鍵ｋ１を復号化するための復号プログラムを記憶する。期待値エリアＴ４は、後述する期待値Ｄを記憶する。ハッシュ関数エリアＴ５は、ハッシュ関数を記憶する。

フラッシュメモリ１１、ＳＲＡＭ１３、及び第１及び第２のＲＯＭ１４、１５には、互いに異なった物理アドレスが割り当てられている。

また、第２のＲＯＭ１５の、システム鍵エリアＴ２の先頭アドレスはＡ１である。復号プログラムエリアＴ３の先頭アドレスはＡ２である。期待値エリアＴ４の先頭アドレスはＡ３である。ハッシュ関数エリアＴ５はの先頭アドレスはＡ４である。

コントローラ１６は、ＣＰＵ（中央処理装置）、ＤＳＰ（ディジタルシグナルプロセッサ）等とその周辺回路から構成されている。コントローラ１６は、第１のＲＯＭ１４のプログラムエリアに格納されたプログラムに従って動作する。具体的には、コントローラ１６は、（１）フラッシュメモリ１１へのデータの書き込み動作、（２）フラッシュメモリ１１からのデータの読み出し動作、（３）記憶装置１０内のメモリをテストするテスト動作を行う。

コントローラ１６は、機能的には、Ｉ／Ｏバッファ（インタフェース回路）１６１と、インタフェース回路１６１に接続された制御部１６２と、アドレスカウンタ１６３と、より構成される。

インタフェース回路１６１は、外部のコンピュータ２０及びテスト装置３０等にバス（データバス及びコントロールバス）２１を介して接続されている。

アドレスカウンタ１６３は、アドレスバスを介してフラッシュメモリ１１、ＳＲＡＭ１３、第１及び第２のＲＯＭ１４、１５のアドレス端子Addに接続されている。

また、制御部１６２の制御端子は、制御バスを介してフラッシュメモリ１１、ＳＲＡＭ１３、第１及び第２のＲＯＭ１４、１５の制御端子Contに接続されている。

制御部１６２の第１のデータ入出力端子は、データバスＤＢを介して

フラッシュメモリ１１と第１のＲＯＭ１４のデータ端子Dataに接続されている。制御部１６２の第２のデータ入出力端子は、内部データバスＩＤＢを介してＳＲＡＭ１３と第２のＲＯＭ１５のデータ端子Dataに接続されている。

ＳＲＡＭ１３、第１及び第２のＲＯＭ１４、１５、コントローラ１６、及び内部データバスＩＤＢは、樹脂等により一体にモールドされている。このため、ＳＲＡＭ１３及び第２のＲＯＭ１５の記憶データがＬＳＩ１２の外部に出力されることはない。即ち、ＳＲＡＭ１３及び第２のＲＯＭ１５の記憶データは、外部からのアクセスに対してプロテクトされている。

この記憶装置１０は、コンピュータ２０にケーブルにより接続され又はプラグイン接続される。

接続後の記憶装置１０とコンピュータ２０（又はテスト装置３０）の動作を説明する。

（０）　相互認証時

この記憶装置１０を使用する場合、先ず、コンピュータ２０と記憶装置１０の間で相互認証を行う。

この相互認証時、コンピュータ２０は、例えば、図示せぬ表示画面に「パスワードを入力してください」等のメッセージを表示する。このメッセージに応答して、使用者がパスワードを入力する。

コンピュータ２０のドライバとコントローラ１６の制御部１６２は、このパスワードに基づいて、相互に認証し合う。そして、相互認証に成功すると、記憶装置１０の使用を許可する。一方、相互認証に失敗すると、制御部１６２は、以後のアクセスを禁止する。

（１）　書き込み動作

記憶装置１０にデータを書き込む場合、コンピュータ２０は、バス２

１を介して記憶装置１０に書込コマンドを出力する。この書き込みコマンドはＩ／Ｏバッファ１６１にセットされる。制御部１６２は、このコマンドを解読し、データの書き込みコマンドであることを判別すると、図３に示す処理を開始する。

まず、制御部１６２は、Ｉ／Ｏバッファ１６１を介して、バス２１上に書き込みデータの送信を要求するコマンドを出力する（ステップＳ１）。

この要求に応答して、コンピュータ２０は、書き込みデータの総量と、先頭の論理アドレスを送信する。続いて、コンピュータ２０は書き込みデータを順次送信する。

制御部１６２は、コンピュータ２０から送信されて来たデータ総量と先頭論理アドレスをＩ／Ｏバッファ１６１を介して取り込む（ステップＳ２）。

制御部１６２は、フラッシュメモリ１１のエリアＴ１から暗号化されたデータ鍵ｋ１をＳＲＡＭ１３上に読み出す。さらに、復号プログラムエリアＴ３に格納されている復号プログラムを実行し、システム鍵ｋ２を用いて、データ鍵ｋ１をＳＲＡＭ１３上で復号化し、平文のデータ鍵ｋ１を生成する。そして、生成したデータ鍵ｋ１をＳＲＡＭ１３に記憶させる（ステップＳ３）。

次に、制御部１６２は、フラッシュメモリ１１に格納されている空きブロックテーブルを参照して、書き込み対象の空きブロックを特定する。そして、書き込み対象として特定された空きブロックの物理アドレスをアドレスカウンタに設定する（ステップＳ４）。

一方、コンピュータ２０は書き込み対象のデータをデータバス２１上に順次出力する。

制御部１６２は、コンピュータ２０から供給されるデータを取り込む

（ステップＳ５）。そして、制御部１６２は、取り込んだデータをＳＲＡＭ１３に保持されている平文のデータ鍵ｋ１を用いて暗号化する（ステップＳ６）。

制御部１６２は、書込制御信号を制御バスに出力し、さらに、暗号化したデータをデータバスＤＢに出力する。データバスＤＢに出力された、この暗号化済みのデータは、フラッシュメモリ１１のアドレスカウンタ１６３が指示する位置に書き込まれる（ステップＳ７）。

制御部１６２は、全てのデータについて処理を終了したか否かを判別する（ステップＳ８）。処理が終了していなければ、アドレスカウンタ１６３を更新して（ステップＳ９）、ステップＳ５に戻って次のデータを取り込み、暗号化して、フラッシュメモリ１１の次の記憶エリアに書き込む。

なお、現在の書込対象ブロックが一杯になった場合には、ステップＳ９で次の空きブロックを選択し、選択した空きブロックの物理アドレスをアドレスカウンタ１６３にセットし、次の空きブロックにデータを書き込む。

制御部１６２は、データを格納し終わると、フラッシュメモリ１１に格納されているＦＡＴ、ディレクトリ情報、空きブロックテーブル等を更新する。さらに、ＳＲＡＭ１３に記憶されたデータ鍵ｋ１を消去し（ステップＳ１０）、処理を終了する。

（２）　読み出し動作

記憶装置１０からデータを読み出す場合、コンピュータ２０は、バス２１を介して記憶装置１０に読み出しコマンドを出力する。

読み出しコマンドがＩ／Ｏバッファ１６１にセットされると、制御部１６２は、このコマンドを解読する。そして、このコマンドがデータの読み出しの指示であることを判別すると、図４に示す処理を開始する。

まず、制御部１６２は、Ｉ／Ｏバッファ１６１を介して、バス２１上に先頭の論理アドレスと読み出し対象データの総量の送信を要求するコマンドを出力する（ステップＳ１１）。

この要求に応答し、コンピュータ２０は、読み出し対象データの先頭アドレス（論理アドレス）とデータ総量をバス２１を介してコントローラ１６に通知する。

制御部１６２は、Ｉ／Ｏバッファ１６１を介して先頭アドレスとデータ総量を受信する（ステップＳ１２）。

次に、制御部１６２は、復号プログラムエリアＴ３に格納された復号プログラムを実行する。そして、復号プログラムに従い、暗号化されたデータ鍵ｋ１をフラッシュメモリ１１のデータ鍵エリアＴ１から読み出し、システム鍵ｋ２を用いてこれを復号化して、平文のデータ鍵ｋ１を生成して、ＳＲＡＭ１３に格納する（ステップＳ１３）。

次に、制御部１６２は、フラッシュメモリ１１に記憶されているＦＡＴ及びディレクトリ情報などに基づき、読み出し対象ファイル（データ）が格納されている物理アドレスを判別する。そして、判別された物理アドレスをアドレスカウンタ１６３にセットし、内部データバスＩＤＢ上に出力させる（ステップＳ１４）。

さらに、制御部１６２は、読み出し制御信号を出力し、アドレスカウンタ１６３が指示する物理アドレスに記憶されたデータを、データバスＤＢを介して読み出す（ステップＳ１５）。

制御部１６２は、読み出したデータを、ＳＲＡＭ１３に格納したデータ鍵ｋ１を用いて復号化する。次いで制御部１６２は、復号化したデータを、Ｉ／Ｏバッファ１６１及びバス２１を介してコンピュータ２０に送信する（ステップＳ１６）。

次に、制御部１６２は、読み出しが終了したか否かを判別する（ステ

ップＳ１７）。ステップＳ１７において、制御部１６２は、具体的には、例えば、読み出したデータの総量がコンピュータ２０から指示された総量に一致したか否かを判別する。そして、読み出しが終了していない場合、アドレスカウンタ１６３は、物理アドレスを更新する（ステップＳ１８）。

制御部１６２は、以後、同様にして、物理アドレスを順次更新しながら、データを読み出し、復号化して出力する。

指定された量のデータを読み終えたと判断されると、制御部１６２は、ＳＲＡＭ１３上のデータ鍵を消去し（ステップＳ１９）、読み出し動作を終了する。

このように、この実施の形態によれば、複数の記憶装置１０の第２のＲＯＭ１５に共通の暗号鍵（システム鍵ｋ２）が格納され、各記憶装置１０に固有の暗号鍵（データ鍵ｋ１）がフラッシュメモリ１１に格納される。データ鍵ｋ１は、システム鍵ｋ２により予め暗号化されている。従って、データ鍵ｋ１とシステム鍵ｋ２の両方を知らなければ、フラッシュメモリ１１に記録されているデータを復号化することができない。従って、フラッシュメモリ１１に機密性の高いデータを格納している場合でも、その機密の漏洩を有効に防止できる。

しかも、複数の記憶装置１０に共通なシステム鍵ｋ２を、マスクＲＯＭなどの大量生産に適した読み出し専用メモリからなる第２のＲＯＭ１５に記録し、個別のデータ鍵ｋ１をデータ記録用のフラッシュメモリ１１に記録すれば、コストの上昇を抑えることも可能である。

また、データ鍵ｋ１が記録装置１０毎に設定されていれば、何らかの理由により、ある記憶装置１０のデータ鍵ｋ１とシステム鍵ｋ２の両方が知られても、他の記憶装置１０が記憶するデータを復号化することはできない。従って、被害を最小（１台）に抑えることができる。

また、この構成によれば、ＳＲＡＭ１３と第２のＲＯＭ１５とコントローラ１６との間のデータの送受信は内部データバスＩＤＢを介して行われる。このため、ＬＳＩ１２の外部からは送受信されるデータを観察することができない。従って、復号化されたデータ鍵ｋ１及びシステム鍵ｋ２を含む機密情報の漏洩を防ぐことができる。

（３）　テスト動作

記憶装置１０は、製造時や出荷時にテストされ、フラッシュメモリ１１、ＳＲＡＭ１３、第１のＲＯＭ１４及び第２のＲＯＭ１５の全てがデータを正しく記憶できること、或いは正しくデータを記憶していることが確認される。

一方、第２のＲＯＭ１５はマスクＲＯＭ等で構成されているため、テスト時にシステム鍵ｋ２や復号プログラムが既に記録されている。システム鍵ｋ２や復号プログラムは、テストであっても外部に漏れることは望ましくない。

そこで、この実施の形態では、第２のＲＯＭ１５のテストとして、特有なテストモードを使用する。

記憶装置１０をテストする場合、記憶装置１０は外部のテスト装置３０等に接続され、テスト装置３０はコントローラ１６にテストコマンドを送出する。

制御部１６２は、このテストコマンドに応答し、図５に示す処理を開始する。

まず、制御部１６２は、フラッシュメモリ１１のテストを行う（ステップＳ２１）。

フラッシュメモリ１１のテストは、具体的には、以下に述べる手順で行う。すなわち、まず制御部１６２は、フラッシュメモリ１１を一旦初期化し、全体にデータ「０」が格納されていることをチェックする。次

に、制御部１６２は、フラッシュメモリ１１に「１」を書き込み、これを読み出して、書込データと読出データが一致することを確認する。フラッシュメモリ１１は一定の確率でエラービットを含んでおり、エラービットが検出された場合には、その位置等も判別する。

フラッシュメモリ１１のテストが完了すると、制御部１６２は、ＳＲＡＭ１３をテストする（ステップＳ２２）。

具体的には、まず、制御部１６２は、アドレスを順次更新しながら、ＳＲＡＭ１３の全てのビットに所定の値を書き込む。次いで、ＳＲＡＭ１３からデータを読み出し、書き込んだデータと読み出したデータとが一致するか否かを、テスト装置３０により判別する。

ＳＲＡＭ１３のテストが完了すると、制御部１６２は、第１のＲＯＭ１４をテストする（ステップＳ２３）。第１のＲＯＭ１４のテストは、第１のＲＯＭ１４の記憶データを読み出し、読み出されたデータが期待値と一致することをテスト装置３０で確認することにより行う。

第１のＲＯＭ１４のテストが完了すると、制御部１６２は、第２のＲＯＭ１５をテストする。第２のＲＯＭ１５のテストは、基本的には、第１のＲＯＭ１４のテストと同一である。つまり、記憶データを読み出し、正しいデータが記憶されているか否かを判別することにより行う。

但し、システム鍵ｋ２及び復号プログラムをそのまま読み出すと、システム鍵ｋ２及び復号プログラムが第三者に知られ、データ鍵ｋ１及びシステム鍵ｋ２が盗用又は悪用される虞がある。そこで、システム鍵エリアＴ２と復号プログラムエリアＴ３については、異なるテスト方法を採用する。

まず、制御部１６２は、第２のＲＯＭ１５の先頭アドレスＡ１をアドレスカウンタ１６３にセットする（ステップＳ２４）。次に、制御部１６２は、アドレスカウンタ１６３が指示するアドレスがシステム鍵エリ

アＴ２又は復号プログラムエリアＴ３のアドレス（Ａ１≦アドレスカウンタ１６３が指示するアドレス＜Ａ３）であるか否かを判別する（ステップＳ２５）。これらのエリアのアドレスであると判断された場合、何もせずにアドレスを更新して（ステップＳ２６）、ステップＳ２５にリターンする。

一方、これらのエリアのアドレスではないと判断された場合、そのデータを読み出し、テスト装置３０に供給する（ステップＳ２７）。さらに、次のアドレスが存在するか否かを判別し（ステップＳ２８）、存在すれば、アドレスを更新して（ステップＳ２６）、ステップＳ２５にリターンする。

このようにして、制御部１６２は、第２のＲＯＭ１５のアドレスＡ３以降の記憶データを順次読み出し、Ｉ／Ｏバッファ１６１を介してバス２１上に出力する。テスト装置３０は、読み出されたデータが、予め定められている記録パターンと一致するか否か等を判断し、一致しない場合には、そのアドレスを判別する。

アドレスＡ３以降のエリアのテストが終了すると、システム鍵エリアＴ２と復号プログラムエリアＴ３のテストに移る。

まず、制御部１６２は、ハッシュ関数エリアＴ５に記憶されたハッシュ関数Ｈを読み出す（ステップＳ２９）。次に、制御部１６２は、期待値エリアＴ４に格納されている期待値のセットＤｉを読み出す（ステップＳ３０）。

制御部１６２は、システム鍵エリアＴ２と復号プログラムエリアＴ３から順次読み出した所定バイトのデータの組について、この２つのデータをハッシュ関数Ｈに代入した値を求める（ステップＳ３１）。具体的には、制御部１６２は、システム鍵エリアＴ２と復号プログラムエリアＴ３から順次読み出した所定バイトのデータの組のうちｉ番目に読み出

した組をａi及びｂiとした場合、ａi及びｂiをハッシュ関数Ｈに代入した値Ｈ（ａi，ｂi）を求める。

そして、制御部１６２は、ステップＳ３１で求めた値ｙi（つまり、ｙi＝Ｈ（ａi，ｂi））が、期待値Ｄiに一致するか否かを判別する（ステップＳ３２）。

制御部１６２は、システム鍵エリアＴ２と復号プログラムエリアＴ３の全記憶データを読み出すまで、比較動作を繰り返す。例えば、システム鍵エリアＴ２のサイズと復号プログラムエリアＴ３のサイズとの合計が４ｋバイトであり、ａ、ｂのサイズがいずれも５１２バイトとすれば、４回作業を繰り返す。

制御部１６２は、全ての演算結果ｙiと全ての期待値Ｄiが一致する場合、一致検出信号をテスト装置３０に送信する（ステップＳ３３）。１回でも不一致があった場合、制御部１６２は、テスト装置３０に不一致検出信号を送信する（ステップＳ３４）。以上でテスト動作を終了する。

このようなテストモードを採用することにより、システム鍵ｋ２や復号プログラム等の機密情報をテスト実施者に公開することなく、記憶装置１０内のメモリの良・不良を検査することができる。

なお、このテスト手法は、一例に過ぎない。従って、システム鍵ｋ２や復号化されたデータ鍵ｋ１がＬＳＩ１２の外部に出力されないならば、どのようなテスト手法を採用してもよい。例えば、第２のＲＯＭ１５に格納されているすべてのデータについて、上述のハッシュ関数Ｈを用いたテストを行ってもよい。また、期待値Ｄiをテスト装置３０から記憶装置１０に提供するようにしてもよい。

また、関数Ｈは、ハッシュ関数に限定されない。しかし、関数Ｈは、一つの演算結果に対して複数の変数が対応する一方向関数が望ましい。このような構成とすれば、たとえ、期待値Ｄiが第三者に知られても、

システム鍵ｋ２と復号プログラム自体を特定することはできなくなる。

なお、以上の説明では、テストモードで、制御部１６２がデータの書き込み及び読み出しを順次行った。しかし、この記憶装置１０は、テストモードが設定されると、テストモードが解除されるまで、外部のバス２１と内部バスを直結し、テスト装置３０が、各メモリを直接アクセスできるように構成されても良い。

この場合、システム鍵エリアＴ２及び復号プログラムエリアＴ３がアドレッシングされたときは、第２のＲＯＭ１５をディスエイブル状態に設定し、外部からの直接アクセスを受付けない（禁止する）ように、アドレス信号をマスクすることが望ましい。具体的には、例えば図６に示すように、上位のアドレス信号をデコードすればよい。

上記実施の形態では、フラッシュメモリ１１にデータを書き込んだり、フラッシュメモリ１１からデータを読み出したりする間は、ＳＲＡＭ１３に平文のデータ鍵ｋ１が記憶される。一方、この状態で、動作クロックを停止し、テストモードに入り、ＳＲＡＭ１３の記憶データを読み出すと、データ鍵ｋ１が第三者に知られてしまう虞がある。

このため、図７に示すように、テストモードが指示されると、制御部１６２が、ＳＲＡＭ１３にリセット信号を送出して、これをリセットしてもよい。この場合は、例えば、リセットの後、外部からの制御に従ったテストを実行できるように、リセット信号をオフする構成とすればよい。

（第２の実施の形態）

第１の実施の形態では、システム鍵ｋ２が漏洩した場合、このシステム鍵ｋ２を用いてデータ鍵ｋ１が復号可能である。しかし、システム鍵ｋ２を知っているだけではデータ鍵が復号できないように構成することも可能である。このような構成の第２の実施の形態を以下に説明する。

この実施の形態の記憶装置の基本構成は、図１に示す構成と同一であり、データ鍵ｋ１は、フラッシュメモリ１１のデータ鍵エリアＴ１に格納されている。

但し、データ鍵エリアＴ１に格納されているデータ鍵ｋ１は、システム鍵ｋ２と所定値ＲＮとを組み合わせて得られた値を暗号鍵として用いて暗号化されている。この所定値ＲＮは、出力値が初期値に依存するタイプの乱数発生プログラムにより生成された値である。この初期値として、暗号解読のためのパスワードＰＷが用いられる。

さらに図８に示すように、フラッシュメモリ１１には、復号プログラム及び乱数プログラムが記憶されている。復号プログラムは、パスワードＰＷに基づいてデータ鍵ｋ１を復号化するためのプログラムである。乱数プログラムは、上述した所定値ＲＮを生成する際に使用するものと実質的に同一のものである。

この記憶装置１０を使用する際（データのリード／ライト時等）、コンピュータ２０上のドライバは、使用者にパスワードの入力を要求する。

ドライバは、パスワードが入力されると、データ鍵ｋ１の復号化を指示する指示信号と、この指示信号と共に入力されたパスワードとを、バス２１を介してコントローラ１６に供給する。

制御部１６２は、この指示信号に応答し、パスワードを受信して（図９、ステップＳ４１）、乱数プログラムを起動する。そして、受信したパスワードを初期値として与える（ステップＳ４２）。この乱数発生プログラムは、出力値が初期値に依存するタイプのものであり、出力される値が初期値により定まる。

制御部１６２は、乱数プログラムが生成した乱数値ＲＮとシステム鍵ｋ２とを組み合わせて暗号鍵を作成する（ステップＳ４３）。暗号鍵は、例えば、システム鍵ｋ２と乱数値ＲＮとを、互いに加算（「ｋ２＋ＲＮ」）

したり、互いに連結（「ｋ２；ＲＮ」）したり、互いに乗算（「ｋ２・ＲＮ」）したりして作成する。

暗号鍵が作成されると、制御部１６２は、作成された暗号鍵を用いてデータ鍵ｋ１を復号化する（ステップＳ４４）。

以後、制御部１６２は、復号化されたデータ鍵ｋ１を用いて、コンピュータ２０から供給されたデータを暗号化してフラッシュメモリ１１に格納する。そして、制御部１６２は、フラッシュメモリ１１から読み出したデータを復号化し、コンピュータ２０に供給する。

このような構成とすれば、システム鍵ｋ２が何らかの原因で第三者に知られても、その第三者がパスワードを知らない限り、データ鍵ｋ１を復号化することができず、フラッシュメモリ１１に記憶されているデータを復号化することができない。従って、フラッシュメモリ１１に格納されたデータの漏洩を防止することができる。

また、データ鍵ｋ１を暗号化するための暗号鍵及び復号プログラムを、記憶装置１０毎に個別に作成して、フラッシュメモリ１１に格納することもできる。これにより、記憶装置１０毎に暗号鍵を異ならせることができる。

なお、第２の実施の形態で、例えば、復号プログラムと乱数プログラムをシステム鍵ｋ２で暗号化して、フラッシュメモリ１１に格納しておいても良い。この場合、システム鍵ｋ２でこれらのプログラムを復号化した後、これらのプログラムを実行し、データ鍵を復号化する処理を実行する。

また、第２の実施の形態の復号プログラムは、パスワード等の使用者を特定する情報に基づいてデータ鍵ｋ１を復号化できるならば、任意の構成が採用可能である。

例えば、パスワードＰＷに基づいて一時的な暗号鍵ｋｔを生成し、数

式１に示すように、データ鍵ｋ１を一時的な暗号鍵ｋｔで暗号化し、暗号結果をシステム鍵ｋ２で暗号化した結果ｋ１ｄをフラッシュメモリ１１のエリアＴ１に格納してもよい。一時的な暗号鍵ｋｔは、例えば、パスワードＰＷを種として乱数を発生することにより生成すればよい。

（数式１）

ｋ１ｄ＝ｋ２（ｋｔ（ｋ１））

この場合、エリアＴ１に格納されているデータ鍵ｋ１を復号化するためには、まず、エリアＴ１に格納されているデータｋ１ｄをシステム鍵ｋ２で復号化して（ｋｔ（ｋ１））を生成する。次に、入力されたパスワードＰＷに基づいて一時的な暗号鍵ｋｔを生成する。そして、この一時的な暗号鍵ｋｔを用いてデータ鍵ｋ１を復号化するようにすればよい。

第１及び第２の実施の形態では、システム鍵ｋ２を平文のまま第２のＲＯＭ１５に格納した。しかし、システム鍵ｋ２は一時的な暗号鍵ｋｔで暗号化された状態で第２のＲＯＭ１５に格納されてもよい。この場合には、一時的な暗号鍵ｋｔを用いてシステム鍵ｋ２を復号化した後、データ鍵ｋ１を復号化する処理を行う。

また、図１では、第１のＲＯＭ１４と第２のＲＯＭ１５を別体とした。しかし、第１のＲＯＭ１４と第２のＲＯＭ１５とを、１つのＲＯＭの異なる領域としてもよい。この場合も、このＲＯＭとコントローラ１６との間の通信内容がＬＩＳ１２の外部に漏れないようにデータバスを構成する。

システム鍵ｋ２は全ての記憶装置１０に共通である必要はなく、一定台数毎にシステム鍵ｋ２を変更してもよい。また、データ鍵ｋ１は、記憶装置１０毎に異なる必要はなく、複数の記憶装置１０に共通でもよい。但し、システム鍵ｋ２を同一にする記憶装置１０の間では、データ鍵ｋ１が異なるように設定することが望ましい。

（第３の実施の形態）

第１の実施の形態で、データ鍵ｋ１は、システム鍵ｋ２を用いて暗号化された上でフラッシュメモリ１１に格納されていた。第２の実施の形態で、データ鍵ｋ１は、一時的な暗号鍵ｋｔを用いて暗号化された上でフラッシュメモリ１１に格納されていた。

しかし、データ鍵ｋ１は平文のままフラッシュメモリ１１に格納されていてもよい。この場合は、例えば、データ鍵ｋ１及びシステム鍵ｋ２の両方を用いてデータの暗号化及び復号化を行えばよい。以下では、データ鍵ｋ１及びシステム鍵ｋ２の両方を用いてデータの暗号化及び復号化を行うこの発明の第３の実施の形態を説明する。

この発明の第３の実施の形態にかかる記憶装置１０の構成は、図１に示す、第１の実施の形態における構成と実質的に同一である。暗号化された一般のデータはフラッシュメモリ１１に格納される。

ただし、フラッシュメモリ１１のエリアＴ１には、データ鍵ｋ１は平文のまま記憶されている。データ鍵ｋ１は平文のままエリアＴ１に格納されているため、第２のＲＯＭ１５は、データ鍵ｋ１を復号化するための復号プログラムを格納する必要がなく、従って復号プログラムエリアＴ３は不要である。

次に、上記構成の記憶装置１０及びコンピュータ２０（又はテスト装置３０）の動作を説明する。ただし、コンピュータ２０と記憶装置１０との間での相互認証の動作は、第１の実施の形態における上述した（０）の相互認証時の動作と実質的に同一である。

記憶装置１０にデータを書き込む場合の動作も、第１の実施の形態における上述した（１）の書き込み動作と実質的に同一である。

ただし、ステップＳ３で、制御部１６２は、フラッシュメモリ１１のエリアＴ１からデータ鍵ｋ１を単に読み出してＳＲＡＭ１３に格納する。

すなわち、データ鍵ｋ１の復号化は行わない。

また、ステップＳ６で、制御部１６２は、ステップＳ５でコンピュータ２０から取り込んだデータを、ＳＲＡＭ１３に保持されているデータ鍵ｋ１とシステム鍵ｋ２を用いて暗号化する。

例えば、制御部１６２は、データ鍵ｋ１とシステム鍵ｋ２を加算（ｋ１＋ｋ２）、連結（ｋ１；ｋ２）、乗算（ｋ１・ｋ２）等することにより、新たな暗号鍵を生成し、この鍵を用いてデータを暗号化する。或いは、データ鍵ｋ１でデータを暗号化し、さらに、暗号化されたデータをシステム鍵ｋ２で暗号化する。

そして、ステップＳ１０で、制御部１６２は、空きブロックテーブルとＦＡＴ及びディレクトリ情報などを更新し、ＳＲＡＭ１３に記憶されたデータ鍵ｋ１及びシステム鍵ｋ２を両方消去して、処理を終了する。

記憶装置１０からデータを読み出す場合の動作も、第１の実施の形態における上述の（２）の読み出し動作と実質的に同一である。

ただし、ステップＳ１３で、制御部１６２は、フラッシュメモリ１１のエリアＴ１から平文のデータ鍵ｋ１を読み出すと、ＳＲＡＭ１３に格納する。また、第２のＲＯＭ１５のシステム鍵エリアＴ２からシステム鍵ｋ２を読み出し、ＳＲＡＭ１３に格納する。

また、ステップＳ１６で、制御部１６２は、ステップＳ１５で読み出したデータを、ＳＲＡＭ１３上のデータ鍵ｋ１に加えシステム鍵ｋ２も用いて復号化することにより、平文のデータを生成する。

そして、ステップＳ１９で、コントローラ１６は、ＳＲＡＭ１３上のデータ鍵ｋ１及びシステム鍵ｋ２を両方消去してから、読み出し動作を終了する。

この実施の形態によれば、データ鍵ｋ１とシステム鍵ｋ２とを用いてデータが暗号化及び復号化される。従って、データ鍵ｋ１とシステム鍵

ｋ２の両方を知らなければ、フラッシュメモリ１１に記録されているデータを復号できない。このため、単一の暗号鍵を使用する場合よりも、機密性の高いデータを安全に記憶することができる。

また、データ鍵ｋ１及びシステム鍵ｋ２は、記憶装置１０の異なった位置に分散して格納されている。このため、暗号鍵の特定が困難となる。特に、システム鍵ｋ２は、ＬＳＩ１２内に封止されており、システム鍵ｋ２を外部から直接知ることはできない。また、データ鍵ｋ１が、記憶装置１０毎に個別に設定されていれば、ある記憶装置１０についてデータ鍵ｋ１が知られても、他の記憶装置１０についてはそのデータ鍵ｋ１では、データを復号できない。従って、被害を最小（１台）に抑えることができる。

また、テスト動作のうち、フラッシュメモリ１１、ＳＲＡＭ１３及び第１のＲＯＭ１４をテストする動作は、第１の実施の形態における上述の（３）のテスト動作と実質的に同一である。

フラッシュメモリ１１、ＳＲＡＭ１３及び第１のＲＯＭ１４のテストが完了すると、制御部１６２は、第１の実施の形態におけるステップＳ２９～Ｓ３４の処理と実質的に同一の処理を第２のＲＯＭ１５について行うことにより、第２のＲＯＭ１５をテストする。

具体的には、制御部１６２は、第２のＲＯＭ１５内の期待値エリアＴ４及びハッシュ関数エリアＴ５から、期待値のセットＤi及びハッシュ関数Ｈを読み出す。次に、読み出したハッシュ関数Ｈに、第２のＲＯＭ１５から順次読み出した所定バイトのデータの組を代入した値を求める。そして、求めた値ｙiが、期待値Ｄiに一致するか否かを判別する。

制御部１６２は、第２のＲＯＭ１５の全記憶データを読み出すまで、比較動作を繰り返す。そして、全ての演算結果と全ての期待値が一致する場合、一致検出信号をテスト装置３０に送信し、テスト動作を終了す

る。１回でも不一致の場合、不一致検出信号をテスト装置３０に送信して、テスト動作を終了する。

このようなテストモードを採用することにより、システム鍵ｋ２等の機密情報をテスト実施者に公開することなく、記憶装置１０内のメモリの良・不良を検査することができる。このため、テスト担当者等によるシステム鍵ｋ２の盗用又は悪用を避けられる。

なお、このテスト手法は、一例であり、システム鍵ｋ２がＬＳＩ１２の外部に出力されないならば、どのようなテスト手法を採用してもよい。例えば、第２のＲＯＭ１５のうち、システム鍵ｋ２が格納されている領域等の機密性の高い情報が格納されている領域についてのみ、上述のハッシュ関数Ｈを用いたテストを行い、他の領域については、第１のＲＯＭ１４と同様に、記憶データを順次読み出し、期待値と比較するようにしてもよい。また、期待値Ｄｉをテスト装置３０から記憶装置１０に提供するようにしてもよい。

（第４の実施の形態）

第３の実施の形態では、データ鍵ｋ１とシステム鍵ｋ２の２つの暗号鍵を使用してデータを暗号化及び復号化した。しかし、３以上の暗号鍵を使用して、データを暗号化及び復号化してもよい。以下、３以上の暗号鍵を使用する第４の実施の形態を説明する。

この実施の形態の記憶装置の基本構成は、第１～第３の実施の形態におけるものと実質的に同一である。ただし、コントローラ１６は、図１０に示すように、ＥＥＰＲＯＭ１６４を内蔵している。ＥＥＰＲＯＭ１６４には、第３の暗号鍵ｋ３が格納されている。

この実施の形態の記憶装置１０の基本動作は、第３の実施の形態における記憶装置１０の基本動作と同一である。ただし、コンピュータ２０から受信したデータの暗号化は、データ鍵ｋ１、システム鍵ｋ２及び第

３の暗号鍵ｋ３を用いて行う。フラッシュメモリ１１から読み出したデータの復号化も、データ鍵ｋ１、システム鍵ｋ２及び第３の暗号鍵ｋ３を用いて行う。

データの暗号化の手法は任意である。暗号鍵の作成方法は、任意である。たとえば、コンピュータ２０から受信したデータをデータ鍵ｋ１で暗号化し、さらに、これをシステム鍵ｋ２で暗号化し、さらに、第３の暗号鍵ｋ３で暗号化してもよい。この場合、復号化は、フラッシュメモリ１１から読み出したデータを第３の暗号鍵ｋ３で復号化し、復号化されたデータをシステム鍵ｋ２で復号化し、さらに、これをデータ鍵ｋ１で復号化することにより行う。

また、これら３つの暗号鍵について加算（ｋ１＋ｋ２＋ｋ３）、連結（ｋ１；ｋ２；ｋ３）等の演算を行って新たな暗号鍵を生成し、この暗号鍵を使用してデータを暗号化してもよい。

このように、暗号鍵を多数箇所に分散して格納することにより、暗号の解読がより困難となる。従って、信頼性の高い記憶装置を提供できる。

なお、第３の暗号鍵ｋ３の記憶位置は、ＥＥＰＲＯＭ１６４に限定されない。たとえば、第２のＲＯＭ１５の任意の領域でもよい。

（第５の実施の形態）

第３及び第４の実施の形態では、各暗号鍵（データ鍵ｋ１、システム鍵ｋ２、第３の暗号鍵ｋ３）が平文のまま各メモリに格納されている。しかし、これらの手法では、各暗号鍵の記憶位置が漏洩すると、各暗号鍵が読み出され、データ鍵が復号化され、解読される虞がある。

そこで、暗号鍵自体を暗号化して各メモリに格納してもよい。例えば、第３の暗号鍵ｋ３をシステム鍵ｋ２で暗号化してＥＥＰＲＯＭ１６４に記録してもよい。この場合、データの書込時及び読み出し時には、例えば、システム鍵ｋ２を用いて第３の暗号鍵ｋ３を復号化する。そして、

復号化された第３の暗号鍵ｋ３を用いて、データの暗号化や復号化を行う。

この構成では、第３の暗号鍵ｋ３は暗号化されているが、使用時には復号化され、ＳＲＡＭ１３に格納される。従って、このＳＲＡＭ１３を外部からアクセスして、データを読み出せば第３の暗号鍵ｋ３が知られてしまう。しかし、図１０の物理的構成では、封止及びバスの分割等により、ＳＲＡＭ１３への外部からのアクセスが禁止されているので、平文である第３の暗号鍵ｋ３の漏洩が防止される。

（第６の実施の形態）

第３～第５の実施の形態では、各暗号鍵（データ鍵ｋ１、システム鍵ｋ２、第３の暗号鍵ｋ３）が不揮発性メモリに予め格納されている。しかし、この記憶装置１０の使用時に、暗号鍵を一時的に生成してもよい。以下、このような構成の第６の実施の形態を説明する。

この実施の形態の記憶装置１０の基本構成は、図１０に示す構成と実質的に同一である。ただし、ＥＥＰＲＯＭ１６４には、図１１に示すように、設定された初期値に対応して定まる値を出力する乱数プログラムと暗号鍵生成プログラムが記憶されている。

この場合の記憶装置１０の動作を図１２を参照して説明する。

まず、この記憶装置１０を使用する際、コンピュータ２０は、記憶装置１０の要求に従って（又はコンピュータ２０上のドライバの要求に従って）、使用者にパスワードの入力を要求する（ステップＳ５１）。

この要求に従って、使用者によりパスワードが入力されると（ステップＳ５２）、制御部１６２は、乱数プログラムを起動し、供給されたパスワードを初期値として設定する（ステップＳ５３）。乱数プログラムは、実行されると、初期値に対応する値を１つ発生する。制御部１６２は、この値をＳＲＡＭ１３に格納し、第３の暗号鍵ｋ３として使用する

（ステップＳ５４）。

以後のデータ読出動作、書込動作は、第５の実施の形態と同様である。

第３の暗号鍵ｋ３を生成するタイミングは任意である。第３の暗号鍵ｋ３は、記憶装置１０の使用開始時や、フラッシュメモリ１１をアクセスする際などのタイミングで生成されてよい。

データを格納した際に設定したパスワードと、データを読み出す際に設定したパスワードが異なる場合、第３の暗号鍵ｋ３は異なった値となる。このため、この実施の形態によれば、正しいパスワードを入力しなければ、記憶データの暗号が解読できない。従って、システムキーが漏洩した場合でも、記憶データを安全に保持できる。

なお、乱数プログラムをデータ鍵ｋ１及び／又はシステム鍵ｋ２で暗号化して、フラッシュメモリ１１に格納してもよい。

なお、乱数プログラムを含む暗号鍵生成プログラムの記憶位置は、ＥＰＲＯＭ１６４に限定されず、任意である。例えば、第１の実施の形態において、データ鍵ｋ１又はシステム鍵ｋ２に代えて、暗号生成プログラムを記憶させ、この暗号プログラムを実行して得られた暗号鍵を第１又は第２の暗号鍵として使用してもよい。

（第７の実施の形態）

この発明の実施の形態では、使用者が生成した暗号鍵をフラッシュメモリ１１に登録し、以後この暗号鍵を使用することも可能である。以下、このような構成の第７の実施の形態を説明する。

この実施の形態の記憶装置１０の基本構成は、図１０に示す構成と実質的に同一である。ただし、この実施の形態では、この記憶装置１０を最初に使用する際（例えば、記憶装置１０のフォーマット時）、使用者は、この記憶装置１０を所定のドライバ機能を有するコンピュータ２０に接続し、コンピュータ２０から記憶装置１０に、データ鍵の設定を指

示する指示信号を送信する。

この指示信号に応答し、制御部１６２は、図１３に示す処理を開始し、コンピュータ２０にパスワードの供給を要求する（ステップＳ６１）。この要求に応答したコンピュータから、使用者の操作等に従ってパスワードが供給されると、制御部１６２は、パスワードを受信し（ステップＳ６２）、例えばフォーマットの処理を含む所定の処理を行う（ステップＳ６３）。

所定の処理終了後、制御部１６２は、供給されたパスワード（又は、パスワードが示す値）を初期値として、乱数プログラムを起動する（ステップＳ６４）。

制御部１６２は、得られた乱数値をデータ鍵ｋ１とし、エリアＴ１に格納し（ステップＳ６５）、処理を終了する。

通常状態でのフラッシュメモリ１１へのデータの書き込み・フラッシュメモリ１１からのデータの読み出し等の動作は、上述の第３の実施の形態と同様である。すなわち、この記憶装置１０は、データ鍵ｋ１とシステム鍵ｋ２（第４の実施の形態では、さらに、第３の暗号鍵ｋ３）を用いてデータを暗号化及び復号化する。

このような構成とすれば、使用者自身が入力したパスワードに基づいてデータ鍵が生成される。また、データ鍵ｋ１をフラッシュメモリ１１から読み出すだけで済むので、暗号化・復号化の処理時間が短くてすむ。

なお、乱数プログラムが発生した値をデータ鍵ｋ１として設定する際に、例えば、このデータ鍵ｋ１をシステム鍵ｋ２で暗号化してもよい。この場合、通常状態でのフラッシュメモリ１１へのデータの書き込み・フラッシュメモリ１１からのデータの読み出し等の動作は、例えば、上述の第１の実施の形態と同様である。

（第８の実施の形態）

この発明は、タンパフリー技術と組み合わせることにより、より完全なものとなる。即ち、この記憶装置１０の筐体２５が開封された時点で、記憶データを破壊するように構成することが望ましい。

このような構成を有する記憶装置１０の一例を説明する。

この実施の形態の記憶装置１０は、図１４に示すように、筐体２５内の複数箇所に配置されたマイクロスイッチ２２と、コンデンサ（又は二次電池）２３とオアゲート２４を備えている。

記憶装置１０がコンピュータ２０に接続された状態において、バス２１の電源ラインからコンデンサ（又は二次電池）２３に電力が供給され、コンデンサ２３は充電される。

マイクロスイッチ２２は、通常状態では、オフ状態にあり、筐体２５が開封された時にオンする。１つでもマイクロスイッチ２２がオンすると、このオン信号は、オアゲート２４を介して割り込み信号として、制御部１６２に供給される。

この割り込み信号に応答して、制御部１６２は、フラッシュメモリ１１及びＳＲＡＭ１３を初期化する。この際、初期化に要する電力は、コンデンサ（又は二次電池）２３から供給される。

この構成によれば、筐体２５の一部が開封された際に、制御部１６２は割り込み処理を行う。この割り込み処理を、フラッシュメモリ１１の内容及びＳＲＡＭ１３の内容を消去する処理とすれば、フラッシュメモリ１１の内容及びＳＲＡＭ１３の内容は消去される。従って、フラッシュメモリ１１に記憶されていた機密情報が第三者に漏れることが避けられる。

なお、フラッシュメモリ１１としては、メモリ全体を一括して消去できるものが望ましい。

また、ブロック単位で順次消去する場合には、制御部１６２は、フラ

ッシュメモリ１１の任意のブロックを消去する際、空きブロックテーブルを参照し、空きブロックではないブロックを先に消去し、空きブロックを最後に消去する。一般的なＤＯＳ（ディスクオペレーティングシステム）では、ファイル等を消去する際、先頭の１文字を所定コードに書き換えることにより、実際にはデータを消去しない場合がある。この種のシステムでは、データを消去する際には、消去対象のデータが位置するブロック内に他のデータがある場合に、他のデータを空きブロックに移動（コピー）してから、そのブロックを物理的に消去しておくことが望ましい。

また、周知のタンパフリー技術を使用し、ＬＳＩ１２のパッケージが開封された際に、記憶データを強制的に消失させるようにしてもよい。これにより、記憶装置１０の信頼性をより高めることができる。

また、周知のタンパフリー技術を使用し、記憶装置１０のケース又はコントローラ１６のパッケージがあけられた時等で、ＥＥＰＲＯＭ１６４の記憶内容を自動的に消去できるようにしてもよい。これによれば、第３の暗号鍵ｋ３が第三者に漏れることが避けられ、信頼性がさらに向上する。

なお、この発明は、受信した平文のデータを暗号化して出力し、受信した暗号文を復号化して出力する装置等にも適用可能である。

この場合の構成及び動作は、フラッシュメモリ１１へのデータの書込処理が外部への出力（送信）処理、フラッシュメモリ１１からのデータの読み出しが外部からの入力（受信）処理に変更される点を除けば、上述の第１～第８の実施の形態の処理と同一である。

その他、この発明は上述の第１～第８の実施の形態に限定されず、種々の変形及び応用が可能である。

以上説明したように、この発明によれば、記憶装置に記憶された機密情

報を安全に記憶でき、記憶装置の記録内容の信頼性を高めることができる。

請求の範囲

1．　データを記憶するための書換可能な不揮発性メモリ（１１）と、前記不揮発性メモリをアクセスするための制御手段（１２）とより構成され、データを記憶するための記憶装置であって、

前記不揮発性メモリに第１の暗号鍵が格納され、前記制御手段内に第２の暗号鍵が格納され、前記第１の暗号鍵は、前記第２の暗号鍵により暗号化されており、

前記制御手段は、前記第２の暗号鍵を用いて前記第１の暗号鍵を復号化する鍵復号手段（１２）と、前記鍵復号手段により復号化された第１の暗号鍵を用いてデータを暗号化して前記不揮発性メモリに書き込む書込手段（１２）と、前記不揮発性メモリからデータを読み出して、前記鍵復号手段により復号化された前記第１の暗号鍵を用いて読み出したデータを復号化する読出手段（１２）とを備える、

ことを特徴とする記憶装置。

2．　前記第２の暗号鍵は複数の前記記憶装置に共通であり、前記第１の暗号鍵は、同一の第２の暗号鍵を記憶している前記記憶装置の一部に共通の暗号鍵である、ことを特徴とする請求項１に記載の記憶装置。

3．　前記第２の暗号鍵は複数の前記記憶装置に共通であり、前記第１の暗号鍵は、同一の第２の暗号鍵を記憶している前記記憶装置のそれぞれに固有の暗号鍵である、ことを特徴とする請求項１に記載の記憶装置。

4．　前記不揮発性メモリはフラッシュメモリ（１１）から構成され、前記制御手段は前記第２の暗号鍵を記憶したマスクＲＯＭ（読み出し専

用メモリ）（１５）を含む、ことを特徴とする請求項１に記載の記憶装置。

５．　前記鍵復号手段は、パスワードを取り込み、正しいパスワードが入力された場合のみ、前記暗号化された第１の暗号鍵を復号化する、ことを特徴とする請求項１に記載の記憶装置。

６．　前記第１の暗号鍵は、前記第２の暗号鍵とパスワードを基に生成された第３の暗号鍵により暗号化されて前記不揮発性メモリに格納されており、

前記鍵復号手段は、パスワードを入力する手段と、入力されたパスワードから第３の暗号鍵を生成する手段と、前記第２の暗号鍵と生成された第３の暗号鍵とを用いて前記暗号化されている第１の暗号鍵を復号化する手段（１６）を備える、ことを特徴とする請求項１に記載の記憶装置。

７．　前記鍵復号手段は、復号プログラムと該復号プログラムを実行する手段（１６）とより構成され、

前記復号プログラムは前記不揮発性メモリに格納されている、

ことを特徴とする請求項１に記載の記憶装置。

８．　前記鍵復号手段と前記書込手段と前記読出手段は、復号化された第１の暗号鍵を記憶し、外部からのアクセスに対して保護された揮発性メモリ（１３）を含む、

ことを特徴とする請求項１に記載の記憶装置。

９．　前記不揮発性メモリはフラッシュメモリ（１１）である、ことを特徴とする請求項１に記載の記憶装置。

１０．　前記制御手段は、前記第１の暗号鍵を生成し、生成した第１の暗号鍵を前記第２の暗号鍵を用いて暗号化して前記不揮発性メモリに記録する鍵生成手段（１６）を備える、

ことを特徴とする請求項１に記載の記憶装置。

１１．　前記鍵生成手段は、入力されたパスワードに基づいて前記第１の暗号鍵を生成する、ことを特徴とする請求項１０に記載の記憶装置。

１２．　前記第２の暗号鍵は、複数の記憶装置に共通の暗号鍵である、

ことを特徴とする請求項１０に記載の記憶装置。

１３．　第１の暗号鍵とデータを記憶するための書換可能な不揮発性メモリ（１１）と、

第２の暗号鍵を記憶し、前記不揮発性メモリをアクセスするための制御手段（１２）と、

より構成され、データを記憶する記憶装置であって、

前記制御手段は、前記第１と第２の暗号鍵を用いてデータを暗号化して前記不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読みだして前記第１と第２の暗号鍵を用いて復号化して出力する読出手段（１６）とを備える、

ことを特徴とする記憶装置。

１４．　前記第２の暗号鍵は、複数の記憶装置に共通の暗号鍵であり、

前記制御手段に配置された読出専用メモリに格納され、

前記第１の暗号鍵は、前記第２の暗号鍵を共通とする複数の記憶装置の一部のみに共通又は固有の暗号鍵である、

ことを特徴とする請求項１３に記載の記憶装置。

１５．　前記不揮発性メモリはフラッシュメモリ（１１）から構成され、前記制御手段は前記第２の暗号鍵を記憶したマスクＲＯＭ（読み出し専用メモリ）（１５）を備える、

ことを特徴とする請求項１３に記載の記憶装置。

１６．　暗号化された暗号鍵を記憶する暗号鍵記憶手段（１１）と、

前記暗号鍵を用いて暗号化されたデータを記憶するための書換可能な不揮発性メモリ（１１）と、

前記暗号鍵を復号する復号手段（１６）と、前記復号手段により復号された暗号鍵を記憶する揮発性メモリ（１３）と、前記揮発性メモリに記憶された暗号鍵を用いて外部より供給されるデータを暗号化して前記不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読み出し、読み出したデータを前記揮発性メモリに記憶されている暗号鍵を用いて復号化して出力する読出手段（１６）とを備える制御手段（１２）と、前記揮発性メモリへの外部からのアクセスを禁止する禁止手段（１６，２２，ＩＤＢ，２５）と、を備え、

復号化された暗号鍵への外部からのアクセスが防止されていることを特徴とする記憶装置。

１７．　前記禁止手段は、この記憶装置が開封されたことを検出する開封検出手段（１６，２２）と、前記開封検出手段が開封を検出した際に、

前記不揮発性メモリの内容を消去する手段（１６）を含む、ことを特徴とする請求項１６に記載の記憶装置。

１８．　前記禁止手段は、前記制御手段を封止する封止手段（２５）と、前記封止手段に封止され、前記揮発性メモリと前記復号手段との間でデータを伝送する内部バス（ＩＤＢ）と、を含む、ことを特徴とする請求項１６に記載の記憶装置。

１９．　前記暗号鍵記憶手段と前記復号手段との間で暗号化された暗号鍵を伝送し、かつ、前記書込手段及び前記読出手段と前記不揮発性メモリとの間で暗号化されているデータを伝送するデータバス（ＤＢ）と、前記内部バスとは別体に構成され、

前記復号化された暗号鍵は前記データバス上には出力されないように構成されている、

ことを特徴とする請求項１８に記載の記憶装置。

２０．　不揮発性メモリ（１１）と、

第１の暗号鍵を生成する鍵生成手段（１６）と、

第２の暗号鍵を記憶する鍵記憶手段（１５）と、

前記鍵生成手段により生成された前記第１の暗号鍵と前記鍵記憶手段に記憶されている前記第２の暗号鍵とを用いてデータを暗号化して前記不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読出して前記第１と第２の暗号鍵を用いて復号化して出力する読出手段（１６）とを備える、

ことを特徴とする記憶装置。

２１．　前記鍵生成手段は、生成した第１の暗号鍵を、前記不揮発性メモリに格納する手段を備え、前記書込手段及び前記読出手段は、前記不揮発性メモリに格納された第１の暗号鍵を使用する、

ことを特徴とする請求項２０に記載の記憶装置。

２２．　前記鍵生成手段は、入力されたパスワードに基づいて前記第１の暗号鍵を生成する、ことを特徴とする請求項２０に記載の記憶装置。

２３．　前記第２の暗号鍵は、複数の記憶装置に共通の暗号鍵であり、読出専用メモリからなる前記鍵記憶手段に格納されている、

ことを特徴とする請求項２０に記載の記憶装置。

２４．　第１の暗号鍵を記憶する第１の暗号鍵記憶手段（１１）と、

第２の暗号鍵を記憶する第２の暗号鍵記憶手段（１５）と、

第３の暗号鍵を記憶する第３の暗号鍵記憶手段（１５）と、

前記第１乃至第３の暗号鍵記憶手段に記憶された前記第１乃至第３の暗号鍵を用いてデータを暗号化して不揮発性メモリに書き込む書込手段（１６）と、前記不揮発性メモリからデータを読出して前記第１乃至第３の暗号鍵を用いて復号化して出力する読出手段（１６）とを備え、

前記第１乃至第３の暗号鍵が分散して配置されていることを特徴とする記憶装置。

２５．　第１の暗号鍵が格納された書換可能な不揮発性メモリ（１１）と、

第２の暗号鍵が格納された読み出し専用メモリ（１５）と、

データを前記第１と第２の暗号鍵を用いて暗号化して出力する暗号化

手段（１６）と、暗号化されたデータを前記第１と第２の暗号鍵を用いて復号化して出力する復号化手段（１６）とを備える、

ことを特徴とする暗号化・復号化装置。

２６．　複数の装置に共通の共通暗号鍵を読出専用メモリに記憶させ、ユニークな個別暗号鍵を前記共通暗号鍵で暗号化して書換可能な不揮発性メモリに記憶させておき、

前記不揮発性メモリにデータを書き込む際は、前記共通暗号鍵を用いて前記個別暗号鍵を復号化し、復号化した前記個別暗号鍵を用いてデータを暗号化して前記不揮発性メモリに書き込み、

前記不揮発性メモリからデータを読み出す際は、前記共通暗号鍵を用いて前記個別暗号鍵を復号化し、前記不揮発性メモリから読み出したデータを復号化した個別暗号鍵を用いて復号化して出力する、

ことを特徴とする不揮発性メモリのアクセス方法。

２７．　所定のパスワードが入力された時にのみ、前記個別暗号鍵を復号化する、ことを特徴とする請求項２６に記載の不揮発性メモリのアクセス方法。

２８．　前記個別暗号鍵は、前記共通暗号鍵とパスワードを基に生成された第３の暗号鍵により暗号化されて前記不揮発性メモリに記憶されており、

パスワードを入力し、入力されたパスワードから前記第３の暗号鍵を生成し、前記共通暗号鍵と生成された第３の暗号鍵とを用いて前記個別暗号鍵を復号化する、ことを特徴とする請求項２６に記載の不揮発性メモリのアクセス方法。

２９．　前記共通暗号鍵及び復号化された個別暗号鍵は、外部からのアクセスに対し、プロテクトされている、ことを特徴とする請求項２６に記載の不揮発性メモリのアクセス方法。

図面

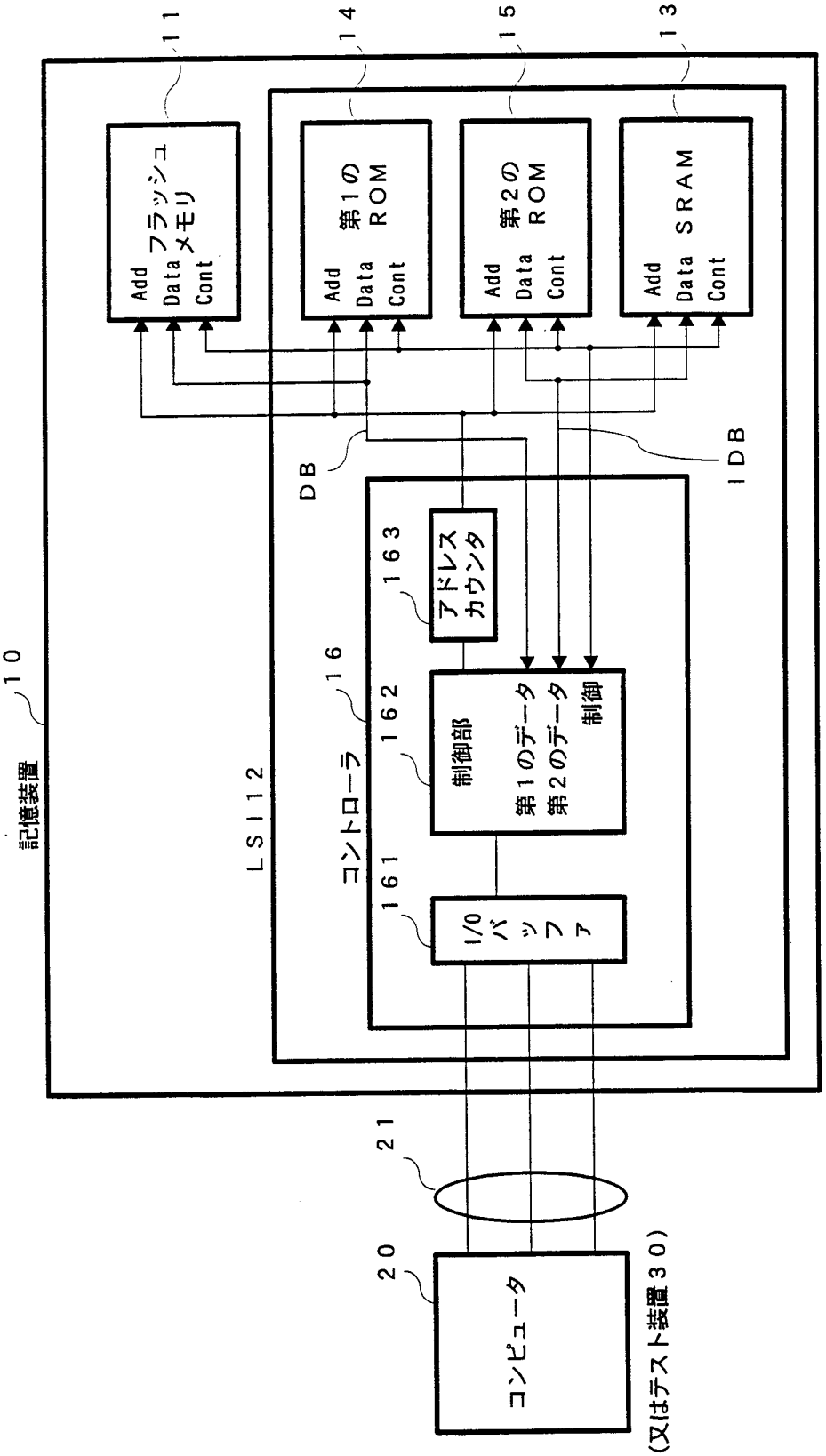
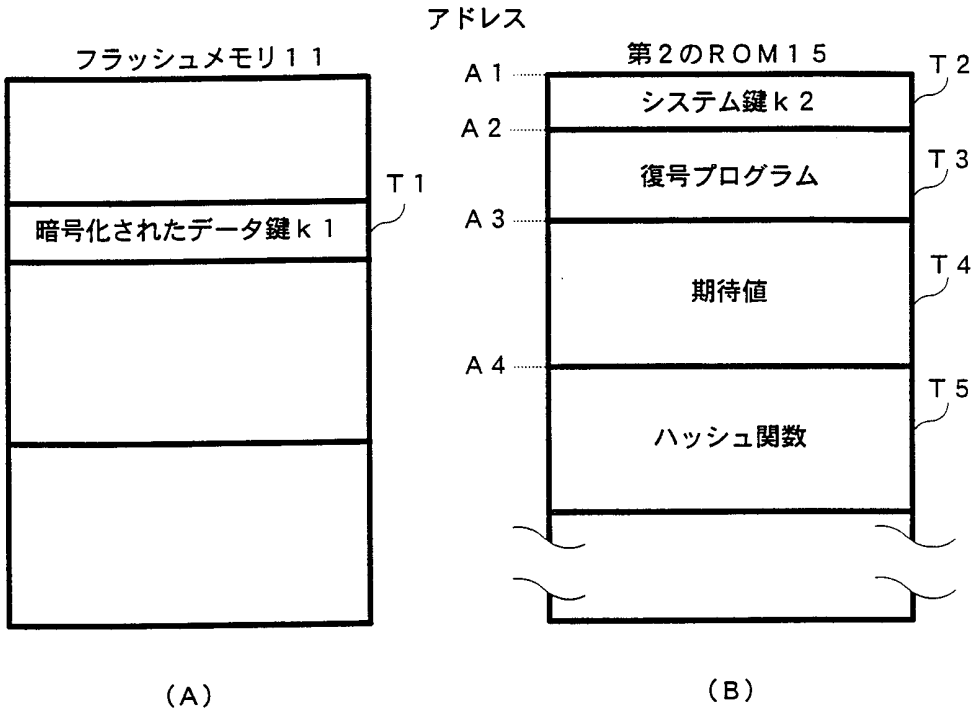

11
14
15
13
Add フラッシュ Data メモリ Cont
Add 第1の Data ROM Cont
Add 第2の Data ROM Cont
Add Data SRAM Cont
DB
IDB
10
記憶装置
LSI 12
コントローラ 16
163 アドレスカウンタ
162 制御部 第1のデータ 第2のデータ 制御
161 I/O バッファ
21
20
コンピュータ
(又はテスト装置30)

FIG. 1


アドレス
フラッシュメモリ１１
暗号化されたデータ鍵ｋ１
Ｔ１
第２のＲＯＭ１５
Ａ１
システム鍵ｋ２
Ａ２
復号プログラム
Ａ３
期待値
Ａ４
ハッシュ関数
Ｔ２
Ｔ３
Ｔ４
Ｔ５
（Ａ）
（Ｂ）

ＦＩＧ．２

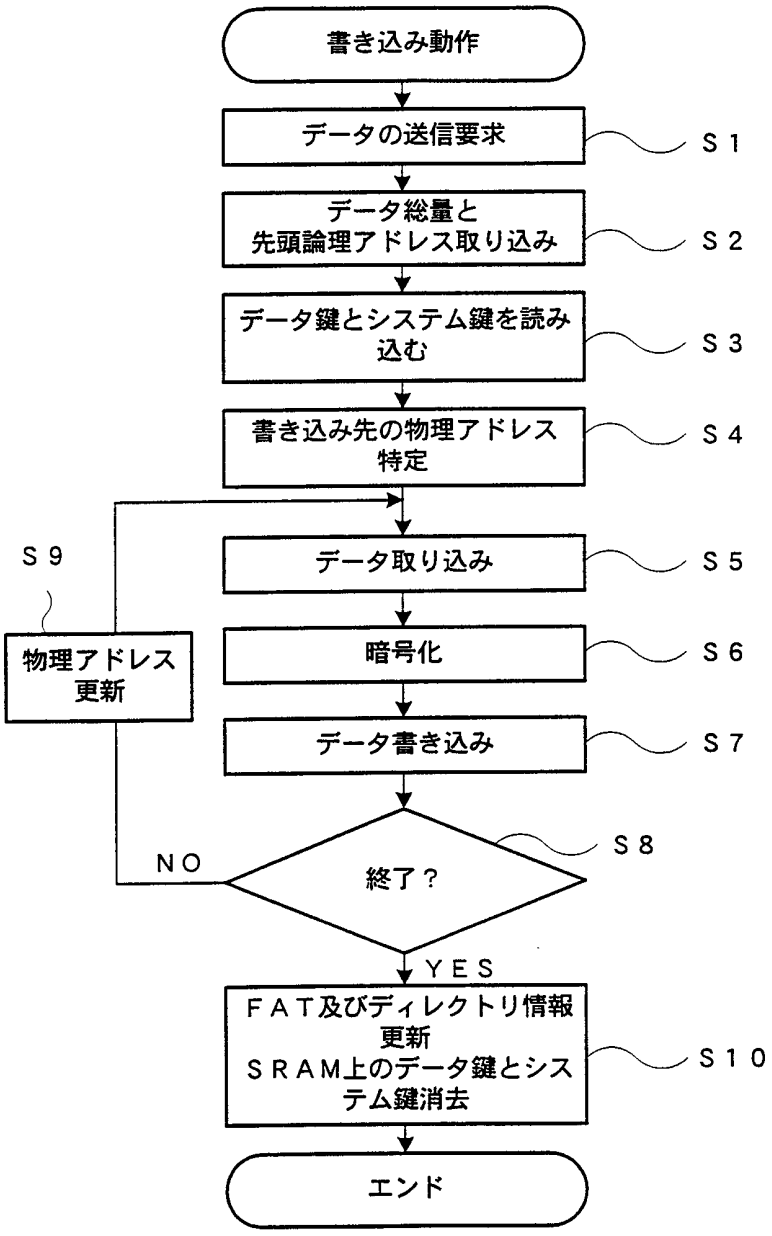

書き込み動作
データの送信要求
S1
データ総量と
先頭論理アドレス取り込み
S2
データ鍵とシステム鍵を読み
込む
S3
書き込み先の物理アドレス
特定
S4
データ取り込み
S5
暗号化
S6
データ書き込み
S7
終了？
S8
NO
YES
S9
物理アドレス
更新
FAT及びディレクトリ情報
更新
SRAM上のデータ鍵とシス
テム鍵消去
S10
エンド

FIG. 3

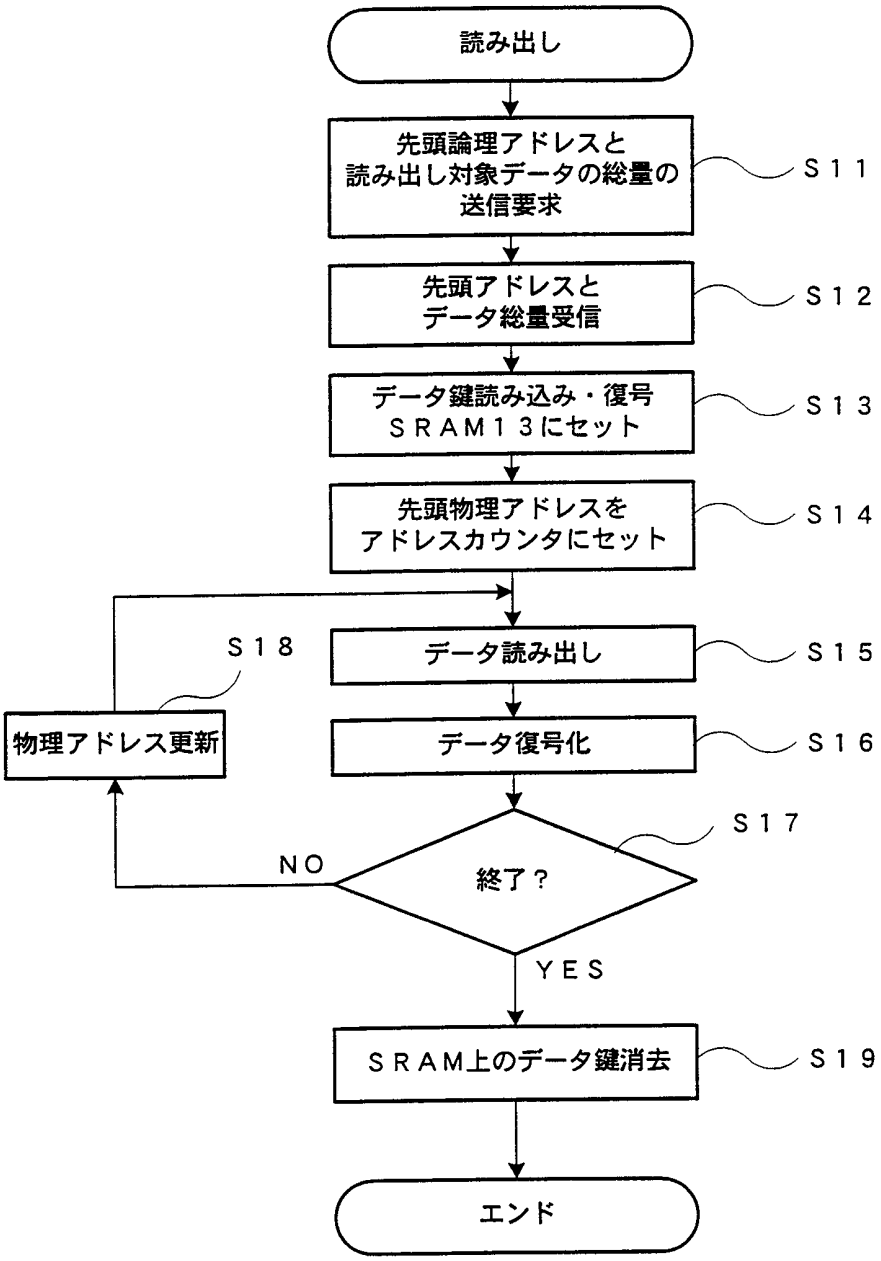

読み出し
先頭論理アドレスと
読み出し対象データの総量の
送信要求
S11
先頭アドレスと
データ総量受信
S12
データ鍵読み込み・復号
SRAM13にセット
S13
先頭物理アドレスを
アドレスカウンタにセット
S14
データ読み出し
S15
データ復号化
S16
終了？
S17
NO
YES
物理アドレス更新
S18
SRAM上のデータ鍵消去
S19
エンド

FIG. 4

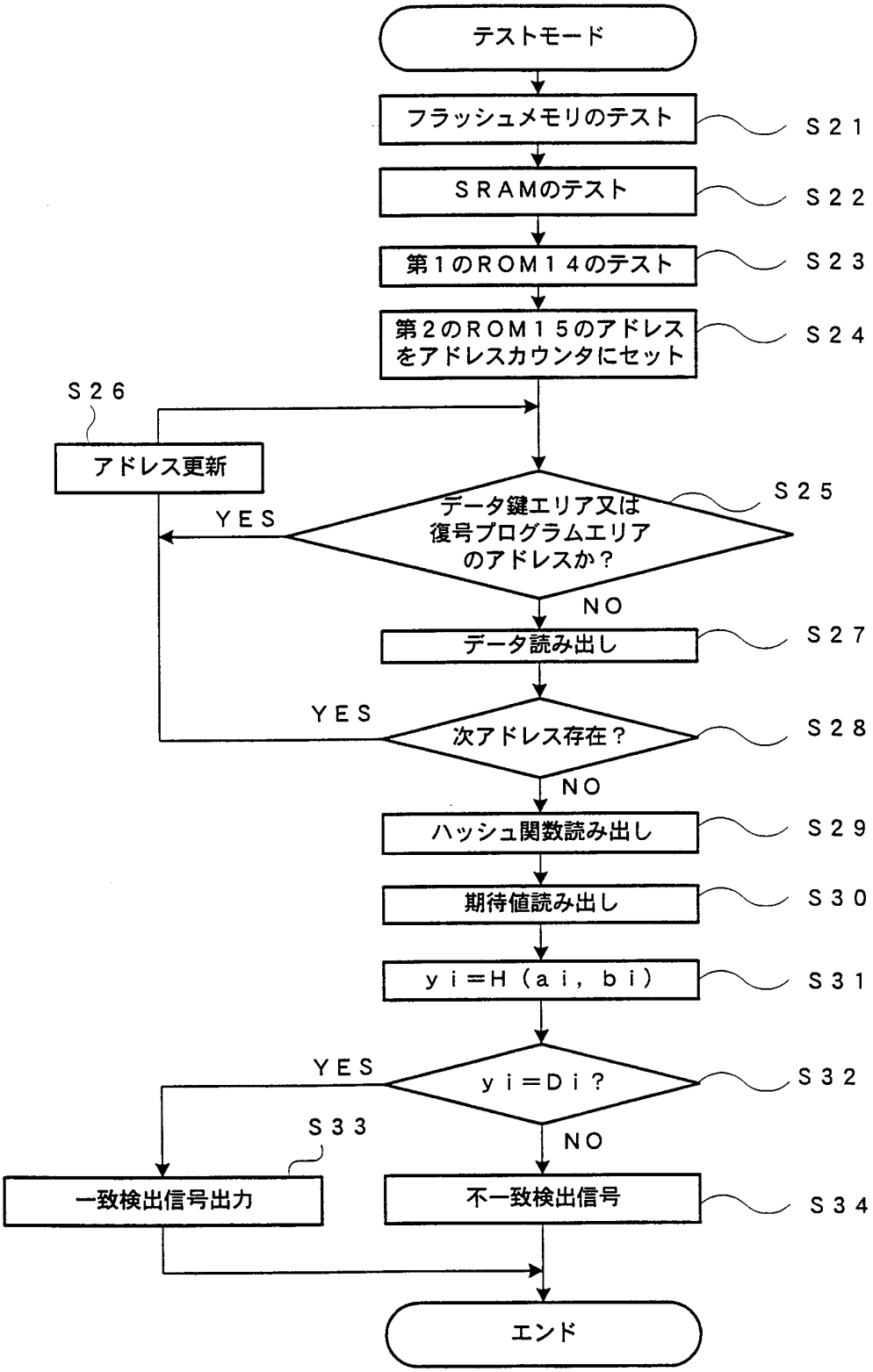

テストモード
フラッシュメモリのテスト
S21
SRAMのテスト
S22
第1のROM14のテスト
S23
第2のROM15のアドレス
をアドレスカウンタにセット
S24
S26
アドレス更新
データ鍵エリア又は
復号プログラムエリア
のアドレスか？
S25
YES
NO
データ読み出し
S27
YES
次アドレス存在？
S28
NO
ハッシュ関数読み出し
S29
期待値読み出し
S30
yi＝H（ai，bi）
S31
YES
yi＝Di？
S32
S33
NO
一致検出信号出力
不一致検出信号
S34
エンド

FIG. 5

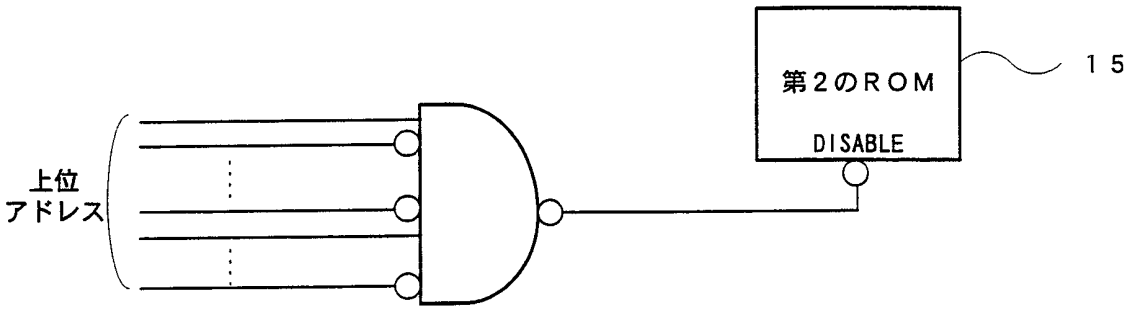


FIG. 6

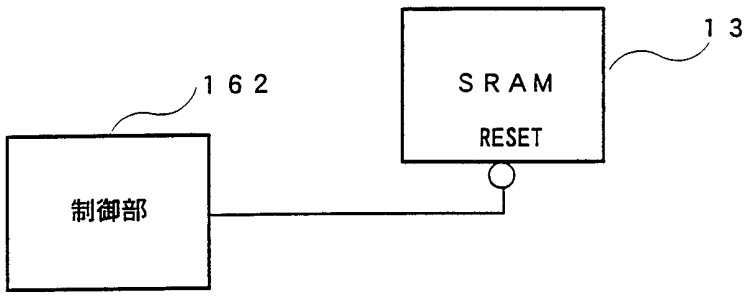

13
SRAM
RESET
162
制御部

FIG. 7

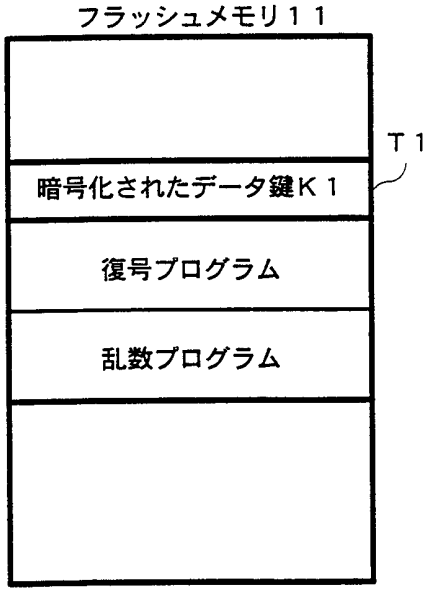

フラッシュメモリ11
T1
暗号化されたデータ鍵K1
復号プログラム
乱数プログラム

FIG. 8

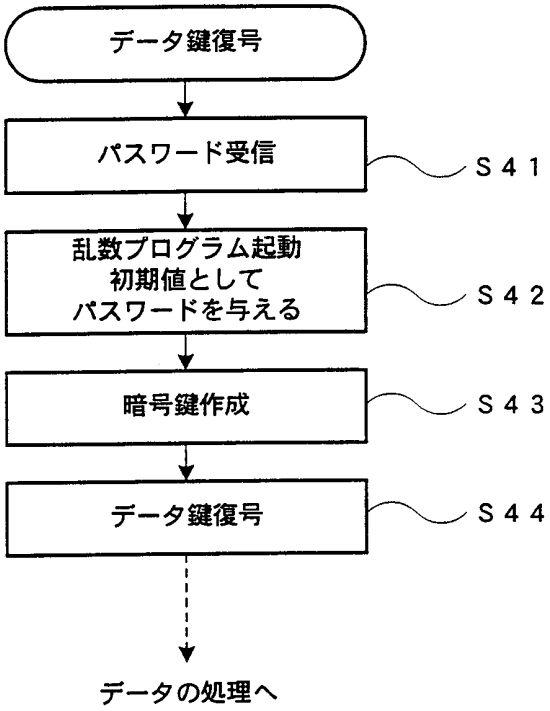

データ鍵復号
パスワード受信
S41
乱数プログラム起動
初期値として
パスワードを与える
S42
暗号鍵作成
S43
データ鍵復号
S44
データの処理へ

FIG. 9

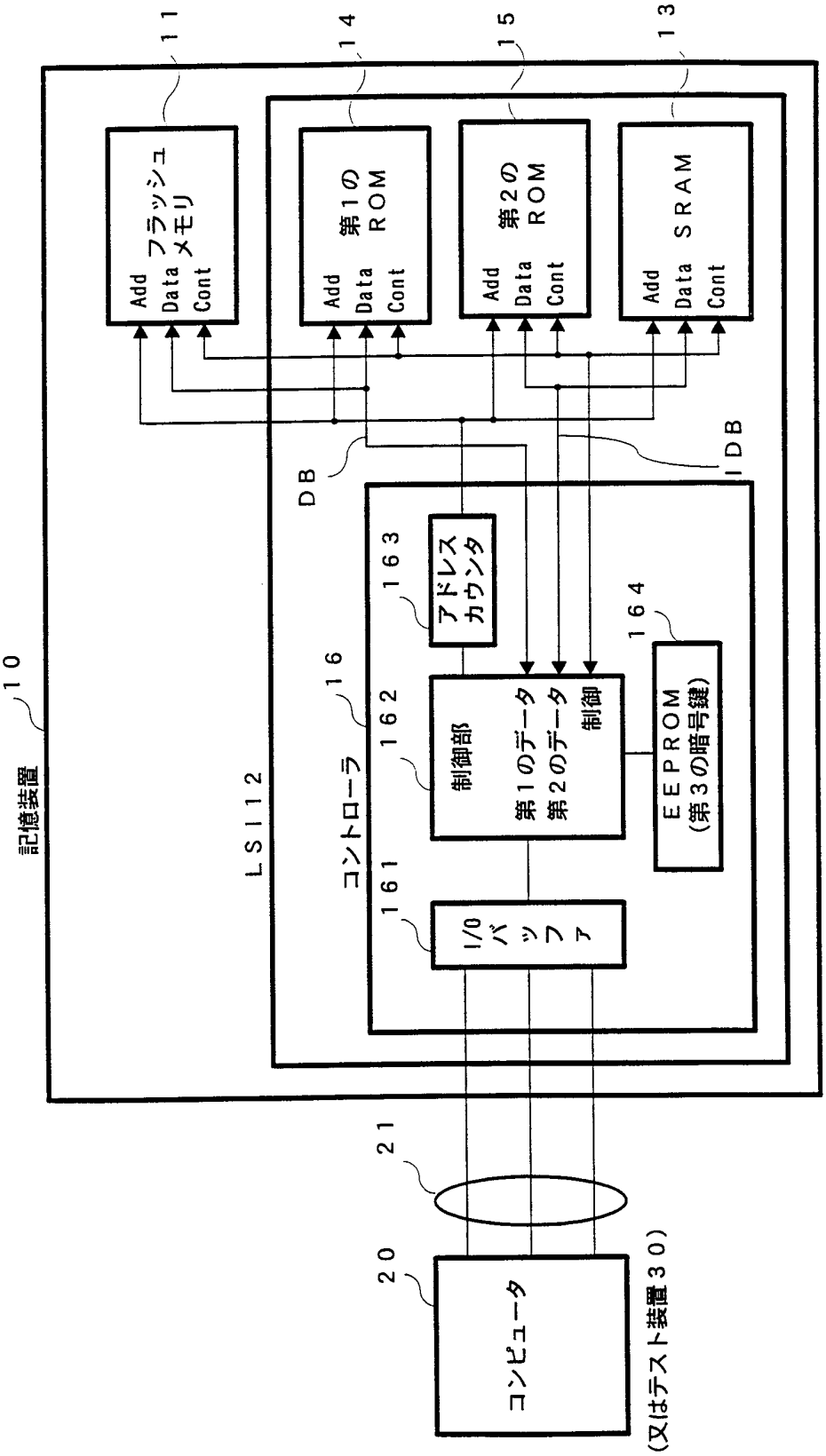

10
記憶装置
LSI12
コントローラ
16
161
I/O バッファ
162
制御部
第1のデータ
第2のデータ
制御
163
アドレスカウンタ
164
EEPROM
(第3の暗号鍵)
DB
IDB
11
Add Data Cont
フラッシュメモリ
14
第1の ROM
15
第2の ROM
13
SRAM
21
20
コンピュータ
(又はテスト装置30)

FIG. 10

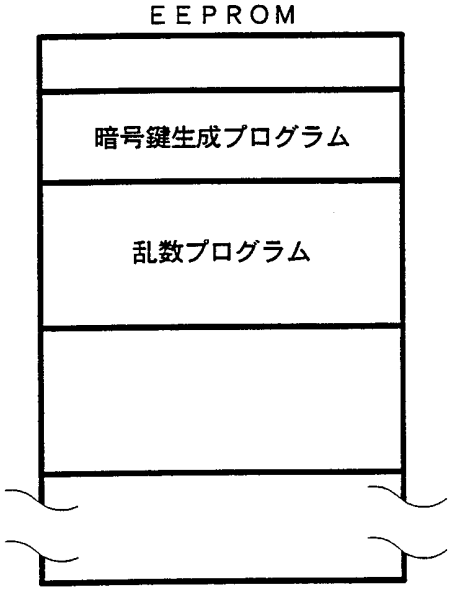


FIG. 11

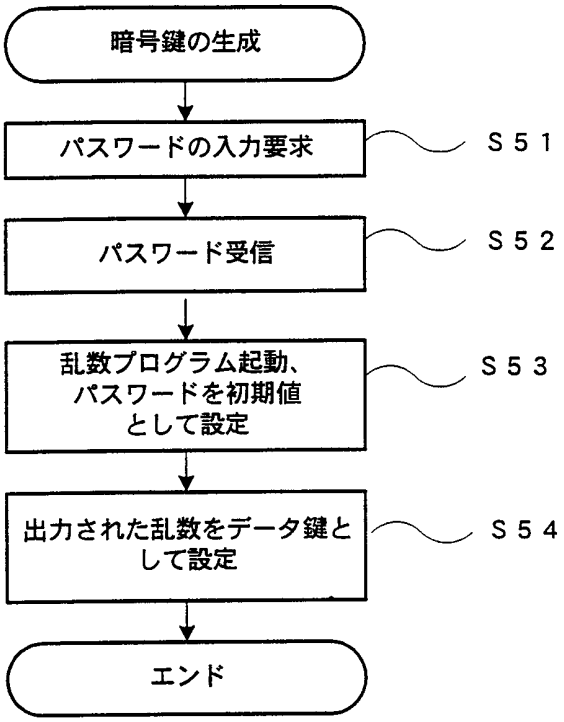

暗号鍵の生成
パスワードの入力要求
S51
パスワード受信
S52
乱数プログラム起動、
パスワードを初期値
として設定
S53
出力された乱数をデータ鍵と
して設定
S54
エンド

FIG. 12

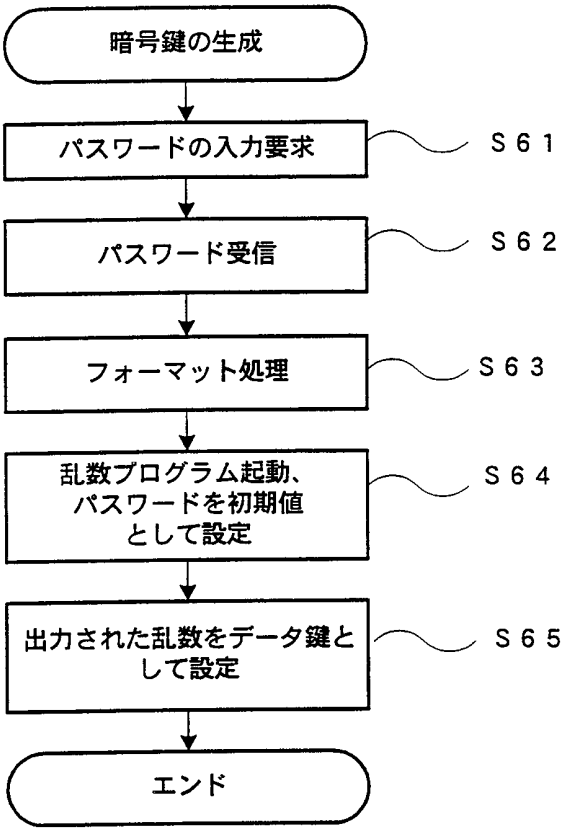

暗号鍵の生成
パスワードの入力要求
S61
パスワード受信
S62
フォーマット処理
S63
乱数プログラム起動、
パスワードを初期値
として設定
S64
出力された乱数をデータ鍵と
して設定
S65
エンド

FIG. 13

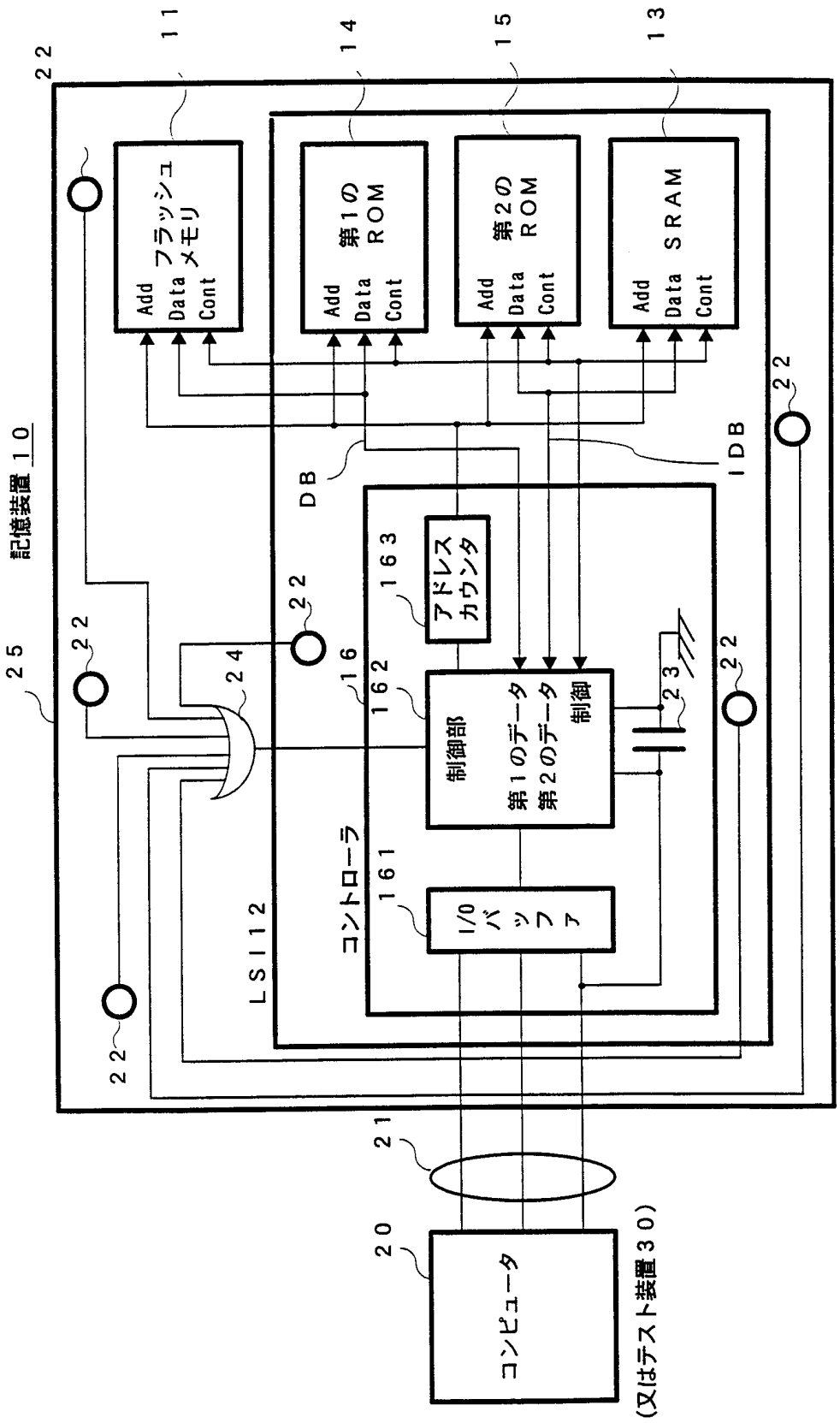

記憶装置 10
LSI 12
コントローラ
161
I/O バッファ
制御部
162
第1のデータ 第2のデータ 制御
163
アドレスカウンタ
16
24
23
DB
IDB
Add Data Cont
フラッシュメモリ
11
第1の ROM
14
第2の ROM
15
SRAM
13
22
25
21
20
コンピュータ
(又はテスト装置 30)

FIG. 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/00170

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G06F12/14

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G06F12/14, G11C16/06, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1971-1999 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1994

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-3431, A (Nippon Telegraph & Telephone Corp.), 6 January, 1998 (06. 01. 98) (Family: none)	1, 5-7, 9-11, 13, 20-22, 25-28
A		2-4, 8, 12, 14-19, 23, 29
Y	JP, 10-3430, A (Dainippon Printing Co., Ltd.), 6 January, 1998 (06. 01. 98) (Family: none)	1, 5-7, 9-11, 13, 20-22, 24-28
Y	JP, 2-235158, A (Mitsubishi Electric Corp.), 18 September, 1990 (18. 09. 90) (Family: none)	5, 27
Y	JP, 2-130044, A (Aisin Seiki Co., Ltd.), 18 May, 1990 (18. 05. 90) (Family: none)	6, 10, 11, 22, 28
Y	JP, 8-95490, A (NEC Corp.), 12 April, 1996 (12. 04. 96) & EP, 705005, A & AU, 9532885, A & CA, 2159159, A & US, 5640455, A & AU, 688569, B	24

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
20 April, 1999 (20. 04. 99)	11 May, 1999 (11. 05. 99)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/00170

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 8-161232, A (Oki Electric Industry Co., Ltd.), 21 June, 1996 (21. 06. 96) (Family: none)	17

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／００１７０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl[6]　Ｇ０６Ｆ１２／１４

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl[6]　Ｇ０６Ｆ１２／１４，Ｇ１１Ｃ１６／０６，Ｇ０９Ｃ１／００

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９７１－１９９９年
日本国公開実用新案公報　１９７１－１９９４年
日本国登録実用新案公報　１９９４－１９９９年

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

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，１０－３４３１，Ａ（日本電信電話株式会社）６．１月．１９９８（０６．０１．９８）　（ファミリーなし）	1,5-7,9-11,13,20-22,25-28
Ａ		2-4,8,12,14-19,23,29
Ｙ	ＪＰ，１０－３４３０，Ａ（大日本印刷株式会社）６．１月．１９９８（０６．０１．９８）　（ファミリーなし）	1,5-7,9-11,13,20-22,24-28
Ｙ	ＪＰ，２－２３５１５８，Ａ（三菱電機株式会社）１８．９月．１９９０（１８．０９．９０）　（ファミリーなし）	5,27

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

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

国際調査を完了した日
２０．０４．９９

国際調査報告の発送日　11.05.99

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｂ　９２９２
金田　利規

電話番号　０３－３５８１－１１０１　内線　３５４５

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ９９／００１７０

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，２－１３００４４，Ａ（アイシン精機株式会社）１８．５月．１９９０（１８．０５．９０）（ファミリーなし）	6,10,11,22,28
Ｙ	ＪＰ，８－９５４９０，Ａ（日本電気株式会社）１２．４月．１９９６（１２．０４．９６）　＆ＥＰ，７０５００５，Ａ　＆ＡＵ，９５３２８８５，Ａ　＆ＣＡ，２１５９１５９，Ａ　＆ＵＳ，５６４０４５５，Ａ　＆ＡＵ，６８８５６９，Ｂ	24
Ａ	ＪＰ，８－１６１２３２，Ａ（沖電気工業株式会社）２１．６月．１９９６（２１．０６．９６）　（ファミリーなし）	17