(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-201038
(P2004-201038A)
(43)公開日　平成16年7月15日(2004.7.15)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601A	5B017
G06F	12/14	G06F	12/14	320B	5J104
G09C	1/00	G09C	1/00	660D	
H04L	9/32	H04L	9/00	673Z	

審査請求 有　請求項の数 23　ＯＬ　（全 24 頁）

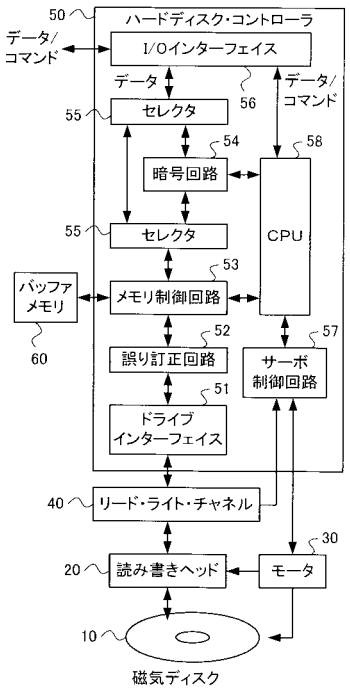
(21)出願番号　特願2002-367334(P2002-367334)
(22)出願日　平成14年12月18日(2002.12.18)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】データ記憶装置、これを搭載した情報処理装置及びそのデータ処理方法並びにプログラム

(57)【要約】
【課題】記憶装置に対してユーザ認証と格納データの暗号化とを併せて適用する場合に好適な格納データの暗号処理及び暗号鍵の管理を実現する。
【解決手段】パスワードなど所定の個人識別情報から生成された暗号鍵を用いて所望のデータ及び個人識別情報自体を暗号化する暗号回路５４と、この暗号回路５４にて暗号化されたデータ及び個人識別情報を記録した磁気ディスク１０と、この磁気ディスク１０に格納されている暗号化された個人識別情報を用いてユーザ認証を行うＣＰＵ５８とを備える。そして、この認証データに基づいてユーザ認証を行い、先の暗号鍵を用いてホストシステムから送信された書き込みデータを暗号化して磁気ディスク１０に記録し、またはこの暗号鍵を用いて磁気ディスク１０から読み出したデータを復号してホストシステムへ送信する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
情報処理装置のデータ記憶装置において、
所定の個人識別情報から生成された暗号鍵を用いて所望のデータ及び当該個人識別情報自体を暗号化する暗号回路と、
前記暗号回路にて暗号化された前記データ及び前記個人識別情報を記録した記録媒体と、
前記記録媒体に格納されている暗号化された前記個人識別情報を用いてユーザ認証を行う制御部と
を備えることを特徴とするデータ記憶装置。
【請求項２】
前記暗号回路は、前記暗号鍵を、他の暗号鍵を用いて暗号化し、
前記記録媒体は、前記他の暗号鍵を用いて暗号化された前記暗号鍵を記録したことを特徴とする請求項１に記載のデータ記憶装置。
【請求項３】
前記記録媒体は、通常の使用ではアクセスできない特別の記憶領域を備え、当該特別の記憶領域に前記暗号鍵を記録したことを特徴とする請求項１に記載のデータ記憶装置。
【請求項４】
前記暗号回路は、複数の個人識別情報から複数の暗号鍵を生成し、当該複数の暗号鍵ごとに、ユーザ認証及びデータの暗号化を制御し、
前記記録媒体は、記憶領域を前記複数の暗号鍵に応じて管理し、当該記憶領域ごとに、対応する前記暗号鍵を用いて暗号化されたデータを記録することを特徴とする請求項１に記載のデータ記憶装置。
【請求項５】
情報処理装置のデータ記憶装置において、
第１の暗号鍵を用いて所望のデータを暗号化し、所定の個人識別情報から生成された第２の暗号鍵を用いて当該第１の暗号鍵及び当該個人識別情報自体を暗号化する暗号回路と、
前記第１の暗号鍵を用いて暗号化された前記データ及び前記第２の暗号鍵を用いて暗号化された前記第１の暗号鍵及び前記第２の暗号鍵を用いて暗号化された前記個人識別情報を記録した記録媒体と、
前記記録媒体に格納されている暗号化された前記個人識別情報を用いてユーザ認証を行う制御部と
を備えることを特徴とするデータ記憶装置。
【請求項６】
前記暗号回路は、前記記録媒体から読み出された暗号化された前記第１の暗号鍵を、前記第２の暗号鍵を用いて復号化し、復号化された当該第１の暗号鍵を用いて所望のデータの暗号化または復号化を行うことを特徴とする請求項５に記載のデータ記憶装置。
【請求項７】
記録媒体である磁気ディスクと、
前記磁気ディスクに対してデータの読み書きを行う読み書き機構と、
前記磁気ディスクに書き込むデータを暗号化し、かつ前記磁気ディスクから読み出された暗号化されたデータを復号化する暗号機能を有し、前記読み書き機構によるデータの読み書きを制御する制御機構とを備え、
前記制御機構は、前記磁気ディスクに対するデータの書き込み処理に際し、前記暗号機能のオン・オフに応じて、前記磁気ディスクの記録領域におけるデータの読み書きの単位ごとに、当該磁気ディスクに書き込むデータの暗号化を行うことを特徴とするハードディスク装置。
【請求項８】
前記制御機構は、前記記録媒体からデータを読み出す際に、当該データが暗号化されているか否かを判断し、暗号化されているならば復号化することを特徴とする請求項７に記載のハードディスク装置。

【請求項９】
前記制御機構は、前記記録媒体から読み出したデータが暗号化されている場合は、読み出した当該データを復号化し、前記暗号機能がオンの状態で前記記録媒体にデータを書き込む場合は、当該データを暗号化して書き込むことを特徴とする請求項７に記載のハードディスク装置。
【請求項１０】
前記制御機構は、所定の個人識別情報から生成された暗号鍵を用いて所望のデータ及び当該個人識別情報自体を暗号化する暗号機能を有し、かつ暗号化された当該個人識別情報を用いてユーザ認証を行うことを特徴とする請求項７に記載のハードディスク装置。
【請求項１１】
前記制御機構の暗号機能は、複数の個人識別情報から複数の暗号鍵を生成し、当該複数の暗号鍵ごとに、ユーザ認証及びデータの暗号化を制御し、
前記磁気ディスクは、記憶領域を前記複数の暗号鍵に応じて管理し、当該記憶領域ごとに、対応する前記暗号鍵を用いて暗号化されたデータを記録することを特徴とする請求項１０に記載のハードディスク装置。
【請求項１２】
前記制御機構は、第１の暗号鍵を用いて所望のデータを暗号化し、所定の個人識別情報から生成された第２の暗号鍵を用いて当該第１の暗号鍵及び当該個人識別情報自体を暗号化する暗号機能を有し、かつ暗号化された当該個人識別情報を用いてユーザ認証を行うことを特徴とする請求項７に記載のハードディスク装置。
【請求項１３】
種々の演算処理を行う演算制御部と、
前記演算制御部にて処理されるデータを格納するデータ記憶装置とを備え、
前記データ記憶装置は、データ用暗号鍵を用いて所望のデータを暗号化し、所定の個人識別情報から生成された認証用暗号鍵を用いて当該個人識別情報自体を暗号化する暗号機能を有し、かつ暗号化された当該個人識別情報を用いてユーザ認証を行うことを特徴とする情報処理装置。
【請求項１４】
前記データ用暗号鍵と前記認証用暗号鍵とは同一の暗号鍵であることを特徴とする請求項１３に記載の情報処理装置。
【請求項１５】
前記データ記憶装置は、他の暗号鍵を用いて前記データ用暗号鍵を暗号化し、保存することを特徴とする請求項１３に記載の情報処理装置。
【請求項１６】
前記データ記憶装置は、他の暗号鍵として前記認証用暗号鍵を用いて前記データ用暗号鍵を暗号化することを特徴とする請求項１５に記載の情報処理装置。
【請求項１７】
データ記憶装置の記録媒体に対してデータの読み書きを行うデータ記憶装置のデータ処理方法であって、
所定の個人識別情報から暗号鍵を生成するステップと、
前記暗号鍵を用いて前記個人識別情報を暗号化し認証データとして記録媒体に記録するステップと、
前記記録媒体に記録されている前記認証データに基づいてユーザ認証を行うステップと、
前記暗号鍵を用いてホストシステムから送信された書き込みデータを暗号化して前記記録媒体に記録し、または前記暗号鍵を用いて前記記録媒体から読み出したデータを復号化しホストシステムへ送信するステップと
を含むことを特徴とするデータ記憶装置のデータ処理方法。
【請求項１８】
前記暗号鍵を、他の暗号鍵を用いて暗号化し、暗号化された当該暗号鍵を前記記録媒体に記録するステップと、

暗号化された前記暗号鍵を、前記他の暗号鍵を用いて復号化し、復号化された当該暗号鍵を用いて、前記記録媒体から読み出されたデータを復号化するステップと
をさらに含むことを特徴とする請求項１７に記載のデータ記憶装置のデータ処理方法。
【請求項１９】
データ記憶装置の記録媒体に対してデータの読み書きを行うデータ記憶装置のデータ処理方法であって、
所定の個人識別情報から認証用暗号鍵を生成するステップと、
前記認証用暗号鍵を用いて前記個人識別情報を暗号化し認証データとして記録媒体に記録し、当該認証用暗号鍵を用いてデータ用暗号鍵を暗号化し当該記録媒体に記録するステップと、
前記記録媒体に記録されている前記認証データに基づいてユーザ認証を行うステップと、
前記認証用暗号鍵を用いて前記記録媒体に記録されている前記データ用暗号鍵を復号化するステップと、
復号化された前記データ用暗号鍵を用いてホストシステムから送信された書き込みデータを暗号化して前記記録媒体に記録し、または当該データ用暗号鍵を用いて前記記録媒体から読み出したデータを復号化しホストシステムへ送信するステップと
を含むことを特徴とするデータ記憶装置のデータ処理方法。
【請求項２０】
個人識別情報の変更に伴って、前記記録媒体に記録されている暗号化された前記データ用暗号鍵を、変更前の個人識別情報から生成される前記認証用暗号鍵を用いて復号化し、変更後の個人識別情報から生成される前記認証用暗号鍵を用いて当該データ用暗号鍵を暗号化し直し当該記録媒体に格納するステップをさらに含むことを特徴とする請求項１９に記載のデータ記憶装置のデータ処理方法。
【請求項２１】
前記記録媒体に記録されているデータの暗号化を解除する場合に、前記記録媒体に記録されている暗号化された前記データ用暗号鍵を、変更前の個人識別情報から生成される前記認証用暗号鍵を用いて復号化し、復号化された当該データ用暗号鍵を当該記録媒体に格納するステップをさらに含むことを特徴とする請求項１９に記載のデータ記憶装置のデータ処理方法。
【請求項２２】
コンピュータを制御して、磁気ディスクに対するデータの読み書きを制御するプログラムであって、
所定の個人識別情報から暗号鍵を生成する処理と、
前記暗号鍵を用いて前記個人識別情報を暗号化し認証データとして前記磁気ディスクに記録する処理と、
前記磁気ディスクに記録されている前記認証データに基づいてユーザ認証を行う処理と、
前記暗号鍵を用いてホストシステムから送信された書き込みデータを暗号化して前記磁気ディスクに記録し、または前記暗号鍵を用いて前記磁気ディスクから読み出したデータを復号化しホストシステムへ送信する処理と
を前記コンピュータに実行させることを特徴とするプログラム。
【請求項２３】
コンピュータを制御して、磁気ディスクに対するデータの読み書きを制御するプログラムであって、
所定の個人識別情報から認証用暗号鍵を生成する処理と、
前記認証用暗号鍵を用いて前記個人識別情報を暗号化し認証データとして前記磁気ディスクに記録し、当該認証用暗号鍵を用いてデータ用暗号鍵を暗号化し当該磁気ディスクに記録する処理と、
前記磁気ディスクに記録されている前記認証データに基づいてユーザ認証を行う処理と、
前記認証用暗号鍵を用いて前記磁気ディスクに記録されている前記データ用暗号鍵を復号化する処理と、

復号化された前記データ用暗号鍵を用いてホストシステムから送信された書き込みデータを暗号化して前記磁気ディスクに記録し、または当該データ用暗号鍵を用いて前記磁気ディスクから読み出したデータを復号化しホストシステムへ送信する処理と
を前記コンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ハードディスク装置に代表される外部記憶装置（データ記憶装置）におけるデータの暗号処理（書き込みデータの暗号化及び読み出しデータの復号化）に関する。
【０００２】
【従来の技術】
コンピュータシステムの外部記憶装置には、磁気ディスク装置（ハードディスク装置等）、光ディスク装置、半導体メモリを用いたメモリカードなど、種々のものが存在する。これらの記憶装置に格納されるデータは、セキュリティの観点から種々の保護手段が導入されているが、ユーザが個人的な情報を格納することが多いハードディスク装置では、ユーザ認証機能としてパスワード・ロック機能が標準的にサポートされている。パスワード・ロック機能とは、ユーザが設定したパスワードをハードディスクの特別の領域に書き込んでおき、起動時に入力されたパスワードが予め書き込まれているパスワードと一致すればハードディスク装置を稼働させてアクセス要求を受け付け、不一致ならばハードディスク装置へのアクセスを拒絶（ロック）するものである。
【０００３】
また、記憶装置に格納されたデータ（以下、格納データ）を第３者によるアクセスから保護する手段としては、格納データを暗号化することが有効である。従来、記憶装置に格納されるデータを暗号化する場合、コンピュータ装置側に備えた暗号化用のソフトウェアやハードウェアを用いて、記憶装置にデータを格納する前に行っていた（例えば、特許文献１、２参照。）。
【０００４】
【特許文献１】
特開２００２－３１９２３０号公報
【特許文献２】
特開平１１－３５２８８１号公報
【０００５】
【発明が解決しようとする課題】
上述したパスワード・ロックのようなユーザ認証と格納データの暗号化とを併せて行うことにより、仮に第３者によってユーザ認証におけるロックが解除されたとしても格納データの内容が当該第３者に盗まれる心配はなくなる。しかし、ここで暗号化の鍵（以下、暗号鍵）をどのように与えるかという問題が生じる。暗号鍵の鍵長は、通常１２８ビット以上であるので、ユーザが格納データの暗号化あるいは復号化の際に直接与えるには長すぎる。一方、この暗号鍵を記録媒体に記録して保持したのでは、暗号の機能が損なわれる。そこで、ユーザ認証と格納データの暗号化とを併用する場合、認証に用いる個人識別情報（パスワードを含む）に基づいて暗号鍵を作成する手法が考えられる。しかし、この手法では、セキュリティの観点から定期または不定期に個人識別情報を変更すると、そのたびに暗号鍵も変わってしまうので、新しい暗号鍵で格納データの暗号化を再施行しなければならない。今日、ハードディスク装置の記憶容量は大容量化が進み、１００ＧＢ（ギガバイト）を越えるものもある。そのため、個人識別情報を変更する度に格納データの暗号化を再施行するとすれば、多大な時間を要してしまい、好ましくない。
【０００６】
また最近では、ハードディスク装置をコンピュータ装置に対して着脱自在（リムーバブル）に実装し、ハードディスク装置を切り替えたり、反対にハードディスク装置を他のコンピュータ装置に装着してデータを利用したりするといった形での使用が増えている。この

ような使用環境でハードディスク装置にデータの暗号機能を実装する際、暗号機能を持たないハードディスク装置との互換性を十分考慮する必要がある。暗号化を行う場合の初期設定などに特別なコマンドを用意することは問題ないが、データの暗号化時にリード／ライトの処理にも特別なコマンドを必要とする実装では、このコマンドをサポートするためにＢＩＯＳ（Basic Input/Output System）やＯＳ（Operating System）の大幅な変更が必要となってしまうため、好ましくない。

【０００７】

ハードディスク装置の格納データの暗号化を行うか行わないかを、磁気ディスクの全体に対してジャンパーピンの設定やフォーマットオプションで決めてしまうことも可能である。しかし今日、多くのハードディスク装置がコンピュータ装置に内蔵され、ＯＳやソフトウェアのプレインストール後に出荷されており、この初期状態でデータを暗号化することはできない。なぜなら、暗号化の秘密鍵は、ディスクごとに違っていなければ意味がなく、ユーザが決めるべきものだからである。

この場合、上記のようなソフトウェアのプレインストール時には暗号化機能をオフしておき、暗号化機能を必要とするユーザが自分で磁気ディスクの全体を暗号化することも１つの方法である。しかし、磁気ディスクの記憶容量が大きいと、磁気ディスクの全体を暗号化する処理には多大な時間を要し、ユーザの負担が増大してしまう。

【０００８】

さらに、磁気ディスクの記憶領域を暗号化領域と非暗号化領域に分け、プレインストールするデータは非暗号化領域に書き込んでおくことも可能である。しかし、その後のデータの読み書きにおいて、データが暗号化領域と非暗号化領域とを移動してしまわないように、常に監視するためには、ＯＳ等のシステムの変更が必要となってしまう。

【０００９】

そこで本発明は、記憶装置に対してユーザ認証と格納データの暗号化とを併せて適用する場合に好適な格納データの暗号処理及び暗号鍵の管理を実現することを目的とする。

また本発明は、着脱自在に実装された記憶装置に好適な格納データの暗号処理方法及びこれを実現する記憶装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】

上記の目的を達成する本発明は、次のように構成されたデータ記憶装置として実現される。すなわち、このデータ記憶装置は、パスワードなど所定の個人識別情報から生成された暗号鍵を用いて所望のデータ及び個人識別情報自体を暗号化する暗号回路と、この暗号回路にて暗号化されたデータ及び個人識別情報を記録した記録媒体と、この記録媒体に格納されている暗号化された個人識別情報を用いてユーザ認証を行う制御部とを備えることを特徴とする。

【００１１】

この暗号鍵は、さらに他の暗号鍵（マスター鍵）を用いて暗号化し、記録媒体に記録しておいても良い。あるいは、暗号化せずに、記録媒体に設けられた通常の使用ではアクセスできない特別の記憶領域に記録しておくこともできる。このようにすることで、個人識別情報を喪失した場合（パスワードを忘れた場合等）にも、記録媒体に保存されている暗号鍵を用いて、暗号化されたデータを復号化して読み出すことが可能となる。

また、複数の個人識別情報から複数の暗号鍵を生成し、当該複数の暗号鍵ごとに、ユーザ認証及びデータの暗号化を制御することも可能である。この場合、記憶領域を前記複数の暗号鍵に応じて管理し、当該記憶領域ごとに、対応する前記暗号鍵を用いて暗号化されたデータを記録する。これにより、複数のユーザによってデータ記憶装置を共用する場合などに、個々のユーザに対して個別に認証を行い、かつ個別の暗号鍵による暗号処理を行うことが可能となる。

【００１２】

また、本発明の他のデータ記憶装置は、暗号回路にて、第１の暗号鍵を用いて所望のデータを暗号化し、所定の個人識別情報から生成された第２の暗号鍵を用いて第１の暗号鍵及

び個人識別情報自体を暗号化する。そして、第１の暗号鍵を用いて暗号化されたデータ及び第２の暗号鍵を用いて暗号化された第１の暗号鍵及び第２の暗号鍵を用いて暗号化された個人識別情報を記録媒体に記録する。また、制御部にて、記録媒体に格納されている暗号化された個人識別情報を用いてユーザ認証を行う。なお、第１の暗号鍵は、第２の暗号鍵と同様に個人識別情報から生成しても良いし、乱数列等の任意の情報を設定して暗号鍵として用いても良い。かかる構成では、暗号回路は、記録媒体から読み出された暗号化された第１の暗号鍵を、第２の暗号鍵を用いて復号化し、復号化された第１の暗号鍵を用いて所望のデータの暗号化または復号化を行う。

このように、暗号鍵を多重化し、上位の暗号鍵を個人識別情報から生成することにより、セキュリティの向上のために個人識別情報を変更した場合などには、上位の暗号鍵は変更されるが、掛かる上位の暗号鍵を用いて暗号化される下位の暗号鍵自体は変更しなくても良い。すなわち、下位の暗号鍵を変更された上位の暗号鍵で暗号化し直すだけで個人識別情報の変更に対応でき、下位の暗号鍵にて暗号化されるデータを暗号化し直す必要はない。

【００１３】

さらに、上記の目的を達成する他の本発明は、次のように構成されたデータ記憶装置としても実現される。すなわち、このデータ記憶装置は、磁気ディスクと、データの読み書きを行う読み書き機構と、磁気ディスクに書き込むデータを暗号化し、かつ磁気ディスクから読み出された暗号化されたデータを復号化する暗号機能を有し、読み書き機構によるデータの読み書きを制御する制御機構とを備える。そして、制御機構により、磁気ディスクに対するデータの書き込み処理に際し、暗号機能のオン・オフに応じて、磁気ディスクの記録領域におけるデータの読み書きの単位ごとに、磁気ディスクに書き込むデータの暗号化を行うことを特徴とする。ここで、磁気ディスクの記録領域におけるデータの読み書きの単位は、セクタや論理ブロック等とすることができる。また、制御機構は、記録媒体からデータを読み出す際に、データが暗号化されているか否かを判断し、暗号化されているならば復号化するといった制御をさらに行う。

【００１４】

また、上記の目的を達成する他の本発明は、データ記憶装置の記録媒体に対してデータの読み書きを行う、次のようなデータ処理方法としても実現される。すなわち、このデータ処理方法は、所定の個人識別情報を暗号化関数や一方向性関数にて変換することにより暗号鍵を生成するステップと、生成された暗号鍵を用いて個人識別情報を暗号化し認証データとして記録媒体に記録するステップと、この認証データに基づいてユーザ認証を行うステップと、先に生成された暗号鍵を用いてホストシステムから送信された書き込みデータを暗号化して記録媒体に記録し、または、この暗号鍵を用いて記録媒体から読み出したデータを復号化しホストシステムへ送信するステップとを含む。

【００１５】

さらに本発明による他のデータ処理方法は、所定の個人識別情報から認証用暗号鍵を生成するステップと、この認証用暗号鍵を用いて個人識別情報を暗号化し認証データとして記録媒体に記録し、認証用暗号鍵を用いてデータ用暗号鍵を暗号化し記録媒体に記録するステップと、この認証データに基づいてユーザ認証を行うステップと、認証用暗号鍵を用いてデータ用暗号鍵を復号化するステップと、復号化されたデータ用暗号鍵を用いてホストシステムから送信された書き込みデータを暗号化して記録媒体に記録し、またはこのデータ用暗号鍵を用いて記録媒体から読み出したデータを復号化しホストシステムへ送信するステップとを含むことを特徴とする。

【００１６】

また、本発明は、コンピュータを制御して、上記のデータ処理方法における各ステップに対応する処理を実行させるプログラムとしても実現される。

さらに、これらのデータ記憶装置を搭載し外部記憶装置として使用する情報処理装置としても実現することができる。

【００１７】

【発明の実施の形態】
以下、添付図面に示す実施の形態に基づいて、この発明を詳細に説明する。
本発明は、磁気ディスク装置（ハードディスク装置等）、光ディスク装置、メモリカード等、各種の外部記憶装置において適用可能な暗号化技術であるが、本実施の形態では、ハードディスク装置に適用した場合を例として説明する。
ハードディスク装置は、例えば、パーソナルコンピュータやワークステーション、その他のコンピュータ装置（情報処理装置）の外部記憶装置として使用される。
図１８は、ハードディスク装置を外部記憶装置として備えたコンピュータ装置の概略構成を示す図である。
図１８に示すように、コンピュータ装置２００は、ＣＰＵ及びＲＡＭ等の内部メモリで実現される演算制御部２１０と、外部記憶装置であるハードディスク装置１００にアクセスするためのインターフェイス２２０（ＡＴＡ（AT Attachment）、ＳＣＳＩ（Small Computer System Interface）等）とを備え、外部記憶装置としてハードディスク装置１００を搭載している。ハードディスク装置１００は、ホストシステムであるコンピュータ装置２００の演算制御部２１０の制御により、データを格納（書き込み）し、転送（読み出し）する。なお、特に図示しないが、実際には、コンピュータ装置２００は、データやコマンドを入力するためのキーボード、マウス等の入力手段、処理結果を出力するためのディスプレイ装置等の出力手段等を備えて構成されることは言うまでもない。
【００１８】
図１は、本実施の形態におけるハードディスク装置１００の構成例を示す図である。
図１を参照すると、ハードディスク装置１００は、記録媒体である磁気ディスク１０を備えると共に、磁気ディスク１０に対してデータの読み書きを行う読み書き機構として、読み書きヘッド２０と、磁気ディスク１０を回転駆動するスピンドルモータ及び読み書きヘッド２０をシークするボイス・コイル・モータ（図ではまとめてモータ３０と表記）と、読み書きヘッド２０を介して磁気ディスク１０に対して読み書きするデータ（信号）の変調及び復調を行いデータの読み書き処理を実行するリード・ライト・チャネル４０とを備え、制御機構としてハードディスク装置１００の動作を統轄制御するハードディスク・コントローラ５０と、バッファメモリ６０とを備える。
【００１９】
ハードディスク・コントローラ５０は、リード・ライト・チャネル４０との間でデータをやり取りするためのドライブインターフェイス５１と、磁気ディスク１０から読み出されたデータの当該読み出しにおける誤りを訂正する誤り訂正回路５２と、バッファメモリ６０にアクセスするためのメモリ制御回路５３と、磁気ディスク１０に対して読み書きするデータの暗号化及び復号化を行う暗号回路５４及びセレクタ５５と、ホストシステムであるコンピュータ装置２００との間でデータやコマンドをやり取りするためのＩ／Ｏインターフェイス５６と、読み書きヘッド２０にて磁気ディスク１０から読み出されたサーボ信号に基づいてサーボ制御を行うためのサーボ制御回路５７と、これら各回路の動作制御を行う制御部としてのＣＰＵ５８とを備える。
【００２０】
上記構成において、磁気ディスク１０にデータを書き込む場合、まずコンピュータ装置２００から送られた書き込み要求コマンドがＩ／Ｏインターフェイス５６を介してＣＰＵ５８に受信され、ＣＰＵ５８の制御により、以下の動作が行われる。すなわち、書き込み要求コマンドの後にコンピュータ装置２００から送られた書き込みデータがＩ／Ｏインターフェイス５６を介して入力され、セレクタ５５及び暗号回路５４にて必要に応じて暗号化され、メモリ制御回路５３及びバッファメモリ６０によるバッファリングを経て、ドライブインターフェイス５１からリード・ライト・チャネル４０へ送られる。そして、読み書きヘッド２０により、磁気ディスク１０に磁気的にデータの書き込みが行われる。なお、読み書きヘッド２０のシーク、磁気ディスク１０の回転駆動といった物理的動作は、ＣＰＵ５８により、サーボ制御回路５７及びモータ３０を介して制御される。セレクタ５５及び暗号回路５４による暗号化処理の制御の詳細は後述する。

【００２１】
一方、磁気ディスク１０からデータを読み出す場合、まずコンピュータ装置２００から送られた読み出し要求コマンドがＩ／Ｏインターフェイス５６を介してＣＰＵ５８に受信され、ＣＰＵ５８の制御により、以下の動作が行われる。すなわち、サーボ制御回路５７及びモータ３０を介して読み書きヘッド２０及び磁気ディスク１０の動作が制御されて磁気ディスク１０の所望の領域に記録されているデータが読み出される。読み出されたデータは、リード・ライト・チャネル４０を経てハードディスク・コントローラ５０へ送られ、ドライブインターフェイス５１を介して誤り訂正回路５２へ送られる。誤り訂正回路５２でビット化け等のエラーが訂正された後、セレクタ５５及び暗号回路５４にて必要に応じて復号化され、Ｉ／Ｏインターフェイス５６を介してコンピュータ装置２００へ送られる。セレクタ５５及び暗号回路５４による復号化処理の制御の詳細は後述する。
【００２２】
本実施の形態では、ＣＰＵ５８の制御下、暗号回路５４及びセレクタ５５を用いて、磁気ディスク１０に書き込まれるデータの暗号化及び磁気ディスク１０から読み出されたデータの復号化を制御する。
暗号回路５４は、暗号アルゴリズムを用いて、データの暗号化を行うと共に、暗号化されたデータの復号化を行う。セレクタ５５は、書き込みデータ及び読み出しデータを暗号回路５４にて処理するかどうかを選択する。
本実施の形態による暗号機能による処理は、大きく分けて、ユーザ認証と格納データの暗号化を併用する場合の暗号鍵の管理に関する処理（Ａ）と、磁気ディスク１０に書き込まれる格納データの暗号化及び復号化の制御に関する処理（Ｂ）とがある。以下、それぞれについて説明する。
【００２３】
Ａ．暗号鍵の管理に関する処理。
この処理では、ユーザ認証と格納データの暗号処理に、同じ暗号アルゴリズムを用いる。すなわち、格納データを暗号化し復号化するための暗号鍵は、ユーザ認証に用いる個人識別情報を暗号化関数や一方向性関数にて変換することにより作成される。そして、暗号回路５４がこの暗号鍵を用いて個人識別情報自体をも暗号化し、暗号化された個人識別情報（以下、認証データ）が磁気ディスク１０に書き込まれて保存される。ユーザ認証時には、ＣＰＵ５８が、まず個人識別情報の入力を求め、暗号回路５４に入力された個人識別情報を同一の暗号アルゴリズムで変換させ、変換されたデータが磁気ディスク１０に書き込まれている認証データと一致するか否かを判断し、判断結果に基づいて正当なユーザを識別する。たとえ、磁気ディスク１０に書き込まれている認証データが不当に読み出されたとしても、暗号処理の一方向性（暗号鍵がなければ元のデータを復元できない）のために、元の個人識別情報が復元されてしまうことはない。
なお、個人識別情報には、ハードディスク装置１００に標準搭載されるパスワード・ロック機能におけるパスワードの他、任意の長さの文字列、ＩＣカードなどに記録されたＩＤ情報、指紋等を用いたバイオメトリクスによる生体情報等、種々の情報を用いることができる。
【００２４】
以下、本手法における各種の動作を個別に説明する。
１．初期設定（暗号鍵の作成及び認証データの保存）。
図２は、ユーザ認証の初期設定の方法を説明する図である。
図２に示すように、まず、暗号回路５４により個人識別情報を暗号化することにより、暗号鍵が生成される（１－ａ）。個人識別情報のデータ長が短すぎる場合は、不足分を適当なデータでパディングすることができる。反対に個人識別情報のデータ長が長すぎる場合は、共通鍵暗号をフィードバックモードであるＭＡＣモード（Message Authentication Code）で使用して、所望の鍵長にまで圧縮することができる。また、このときの暗号化に用いられる暗号鍵には、個人識別情報の一部を用いても良いし、適当な鍵情報（データ）を設定して用いても良い。

次に、処理（１－ａ）で生成された暗号鍵を用いて、暗号回路５４により、個人識別情報が再度暗号化されて認識データとされ、磁気ディスク１０に書き込まれる（１－ｂ）。データ長の十分に長い個人識別情報の入力が保証されるのであれば、当該個人識別情報を２つに分けて、暗号鍵の生成用と認証データの生成用に与えても良い。
これ以後、暗号回路５４による磁気ディスク１０に対して読み書きされるデータの暗号化及び復号化には、処理（１－ａ）で生成された認証データの生成に用いられた暗号鍵が使用されることとなる（１－ｃ）。

【００２５】

２．ユーザ認証と格納データの暗号処理。

図３は、ユーザ認証の方法と格納データの暗号処理を説明する図である。

図３に示すように、まず個人識別情報が入力され、暗号回路５４にて暗号化されて暗号鍵が生成される（２－ａ）。そして、この暗号鍵を用いて暗号回路５４により個人識別情報が再度暗号化され、認証データが生成される（２－ｂ）。入力された個人識別情報が正当なものであれば（すなわち図２を参照して説明した初期設定で暗号鍵及び認証データの生成に用いられた個人識別情報と同一である場合）、生成された認証データは磁気ディスク１０に記録されている認証データと一致するので、ＣＰＵ５８による認証処理において認証成功し、ハードディスク装置１００がアクティベイトされる。そして、処理（２－ａ）で生成された暗号鍵によって、暗号回路５４により、コンピュータ装置２００から送信され磁気ディスク１０に書き込むデータの暗号化、または磁気ディスク１０から読み出してコンピュータ装置２００へ送信するデータの復号化が行われる（２－ｃ）。
これに対し、入力された個人識別情報が正当でなければ（すなわち図２を参照して説明した初期設定で暗号鍵及び認証データの生成に用いられた個人識別情報と同一でない場合）、生成された認証データは磁気ディスク１０に記録されている認証データと一致しないので、認証を失敗し、ハードディスク装置１００はロック（アクセスできない状態）される（２－ａ’）（２－ｂ’）。したがって、磁気ディスク１０へのデータの読み書きは行うことができない。何らかの方法で磁気ディスク１０の暗号化された格納データが読み出されたとしても、正しい暗号鍵が生成されていないので、データを復号化することはできない（２－ｃ’）。さらに、暗号処理の一方向性故に磁気ディスク１０に格納されている暗号化された認証データから暗号鍵や個人識別情報を復元することもできない。

【００２６】

３．格納データの復元。

図４は、磁気ディスク１０に不具合が発生した場合の格納データの復元方法を説明する図である。
磁気ディスク１０に不具合が発生した場合、図４に示すように、格納データを部分的にでも読み出すことができれば（３－ａ）、暗号回路５４による暗号処理と同様のアルゴリズムによる暗号ソフトウェア等を用いて、個人識別情報から暗号鍵を生成し（３－ｂ）、読み出された部分のデータを復元することが可能である（３－ｃ）。
本実施の形態では、認証・暗号化のアルゴリズムが公開されても暗号化されている格納データの安全性が損なわれることはない。なぜなら、暗号化されたデータは、個々のユーザの個人識別情報から生成される暗号鍵によって守られているためである。すなわち、上述した手順（動作１、２参照）で個人識別情報から生成された暗号鍵を用いない限り暗号化されたデータを復号化することはできず、認証データや暗号化されたデータから個人識別情報や元のデータを復元することはできない。したがって、ハードディスク装置１００が故障した場合などに、ユーザ認証におけるロックの解除及びデータの読み出しを第三者に依頼したとしても、その第三者が格納データの内容を取得してしまう心配はない。
なお、磁気ディスク１０以外の機構部分、例えば基板上の回路に何らかの故障が発生した場合は、上記のようにデータを読み出して復元するまでもなく、当該磁気ディスク１０を他のハードディスク装置１００に載せ代えるだけで復旧することができる。

【００２７】

４．マスター鍵を用いた格納データの復元。

図５は、マスター鍵を用いた格納データの復元方法を説明する図である。
図５に示すように、暗号回路５４により、まず個人識別情報が暗号化されて暗号鍵が生成される（４－ａ）。そして、別途生成されたマスター鍵を用いてこの暗号鍵が暗号化され（４－ｂ）、磁気ディスク１０に書き込まれ保存される（４－ｃ）。格納データは、暗号回路５４により、動作（４－ａ）で生成された暗号鍵を用いて暗号化され、または復号化される（４－ｄ）。
このようにして暗号化された暗号鍵を磁気ディスク１０に保存しておけば、たとえユーザが個人識別情報を喪失（パスワードを忘れた場合など）しても、マスター鍵を用いて暗号鍵を復元できるので（４－ｅ）、暗号化された格納データの読み出し、復号化が可能となる（４－ｆ）。
このマスター鍵は、例えばハードディスク装置１００のメーカー等で生成し、管理しておき、製品の保守のために用いることが考えられる。ただしこの場合、マスター鍵の所有者が、ユーザによって暗号化された格納データにアクセスできることになるので、格納データのセキュリティはそれだけ低下することとなる。また、個人識別情報によってハードディスク装置１００が完全にロックされていると、ハードディスク装置１００の故障時等には、暗号化されたデータを読み出すことさえできなくなる。そこで、格納データを暗号化する場合はユーザ認証によるロックを行わない、あるいは、ユーザ認証によるロックだけはマスター鍵ではずせるようにする、というようにセキュリティレベルの様々なオプションを、ユーザの要求に応じて柔軟に設定できるようにしておくことも重要である。
【００２８】
５．認証データの複数設定。
ハードディスク装置１００の故障時には、格納データを復元するとしないとに関わらず、故障解析のためにハードディスク装置１００のロック機能を解除する必要がある。このため、ハードディスク装置１００のロックや格納データの暗号化に使用する認証データ（個人識別情報から生成された認証データ）とは別に、ハードディスク装置１００のロックを解除するための認証データを用意すると便利である。
図６は、個人識別情報による認証データとは別に、ハードディスク装置１００のロックを解除するための認証データを設定する方法を説明する図である。
図６に示すように、動作１で個人識別情報から暗号鍵が生成され（５－ａ）、認証データが生成されるプロセス（５－ｂ）とは別に、個人識別情報とは異なる認証用情報が暗号回路５４にて暗号化されて、別の認証データとして磁気ディスク１０に書き込まれ保存される（５－ｃ）。この認証データを用いたユーザ認証は、動作２の場合と同様であり、ＣＰＵ５８にて実行される。
この認証データは、暗号鍵とは無関係であるので、動作４で説明したマスター鍵のように格納データを復元することはできない。したがって、認証用情報を第三者が保有していても格納データの内容が漏洩する恐れはない。この他、複数のユーザがハードディスク装置１００を共用したり、ハードディスク装置１００のメーカーがシステム専用のデータ領域を磁気ディスク１０上に確保したりするために、複数の認証データや暗号鍵を用意することも有用である。この場合、認証データや暗号鍵ごとに磁気ディスク１０の記憶領域を管理し、あるいは物理的に分割し（パーティションに分割する等）、ユーザ認証及び暗号処理を個別に制御する。すなわち、認証データや暗号鍵ごとに管理される個々の記憶領域に、対応する暗号鍵で暗合されたデータの書き込みを行う。
【００２９】
６．個人識別情報の変更への対応。
図７及び図８は、個人識別情報を変更する場合における暗号処理の対応方法を説明する図である。
ユーザ認証では、セキュリティの向上のため、認証のための個人識別情報を定期または不定期に変更することが推奨される。しかし、個人識別情報から生成された暗号鍵を用いて単純に格納データの暗号化を行った場合、個人識別情報を変更すると暗号鍵が変わってしまうため、格納データを、変更前の個人識別情報から生成された暗号鍵で一旦復号化し、

新たな個人情報から生成された暗号鍵で暗号化し直すという処理が必要となる。今日、ハードディスク装置１００の記憶容量は増大しており、１００ＧＢを越えるデータが格納される場合もあるため、そのような大量のデータに対して復号化及び再暗号化を行うとすれば膨大な時間を要することとなる。そこで、格納データを暗号処理するためのデータ用暗号鍵を、個人識別情報を暗号化して生成された認証用暗号鍵で暗号化して保存することにより、個人識別情報の変更に対して、セキュリティを低下させることなく容易に対応することができる。なお、上述した動作１、２等における暗号鍵は、ここで述べるデータ用暗号鍵と認識用暗号鍵とが同一の暗号鍵である場合と考えることができる（ただし、動作１の初期設定では暗号鍵を磁気ディスク１０に保存していない）。

【００３０】

図７を参照して、初期設定の動作を説明する。

図７に示すように、暗号回路５４により、まず、個人識別情報が暗号回路５４にて暗号化されて認証用暗号鍵が生成される（６－ａ）。そして、この認証用暗号鍵を用いて個人識別情報が再度暗号化され、認証データとして磁気ディスク１０に書き込まれて保存される（６－ｂ）。同様に、この認証用暗号鍵を用いてデータ用暗号鍵が暗号化され、磁気ディスク１０に書き込まれて保存される（６－ｃ）。この動作６では、読み出しデータの暗号化及び書き込みデータの復号化には、処理（６－ａ）で個人識別情報から生成される認証用暗号鍵ではなく、データの暗号処理専用のデータ用暗号鍵が用いられる（６－ｄ）。このデータ用暗号鍵は、認証用暗号鍵や上述した動作１、２等の場合と同様に、所定の暗号鍵生成用の情報を暗号回路５４で暗号化することにより生成しても良いし、任意の鍵情報（乱数列等）を設定して暗号鍵として用いても良い。さらに、認証用暗号鍵と同一の個人識別情報を、認証用暗号鍵を生成する場合とは異なる暗号化関数あるいは一方向性関数で暗号化することによりデータ用暗号鍵を生成することも可能である。なお、個人識別情報から別個の操作（関数）により相異なる認証用暗号鍵とデータ用暗号鍵とを生成する場合、個人識別情報が正しければ正しいデータ用暗号鍵を生成することができるので、必ずしも認証用暗号鍵で暗号化して磁気ディスク１０に保存しておかなくても良い。

【００３１】

次に図８を参照して、ユーザ認証及び格納データの暗号処理を説明する。

図８に示すように、まず個人識別情報が暗号回路５４にて暗号化されて認証用暗号鍵が生成される（６－ｅ）。そして、この認証用暗号鍵を用いて個人識別情報が再度暗号化され、認証データが生成される（６－ｆ）。生成された認証データと磁気ディスク１０に記録されている認証データとが一致すれば、ＣＰＵ５８による認証処理において認証成功し、ハードディスク装置１００がアクティベイトされる（６－ｇ）。また、磁気ディスク１０から暗号化されたデータ用暗号鍵が読み出され、暗号回路５４により、認証用暗号鍵を用いて復号化される（６－ｈ）。そして、暗号回路５４により、データ用暗号鍵を用いて、コンピュータ装置２００から送信され磁気ディスク１０に書き込むデータの暗号化、または磁気ディスク１０から読み出してコンピュータ装置２００へ送信するデータの復号化が行われる（６－ｉ）。

【００３２】

図７及び図８のようにして格納データの暗号処理を行った場合、個人識別情報を変更したとしても、当該新たな個人識別情報から認証データを再生成し、当該新たな個人識別情報から生成される認証用暗号鍵で暗号化されるデータ用暗号鍵を改めて暗号化し直すだけで良く、格納データ全体を復号化して再暗号化する必要はない。したがって、磁気ディスク１０に大量の格納データが記録されている場合であっても現実的な処理で対応することができる。

図９は、個人識別情報を変更する際の動作を説明する図である。

図９に示すように、まず暗号回路５４により、変更前の個人識別情報から認証用暗号鍵が生成され（６－ｊ）、この認証用暗号鍵を用いて個人識別情報から認証データが生成される。そして、ＣＰＵ５８により、磁気ディスク１０に記録されている認証データと照会される（６－ｋ）。認証がすんだ後、磁気ディスク１０に記録されている暗号化されたデー

タ用暗号鍵が読み出され、暗号回路５４により、当該認証用暗号鍵を用いて復号化される（６－ｌ）。
一方、暗号回路５４により、新たな個人識別情報から新たな認証用暗号鍵が生成され（６－ｍ）、この新たな認証用暗号鍵を用いて個人識別情報が再度暗号化され、新たな認証データとして磁気ディスク１０に書き込まれて保存される（６－ｎ）。そして、この新たな認証用暗号鍵を用いて、暗号回路５４により、先に復号化されたデータ用暗号鍵が再度暗号化され、磁気ディスク１０に書き込まれて保存される（６－ｏ）。
【００３３】
また、図７及び図８のようにして格納データの暗号処理を行った場合、ハードディスク装置１００が故障した場合でも、暗号化された格納データを磁気ディスク１０から読み出すことができれば、格納データの暗号化の際と同様にデータ用暗号鍵を取得するか、または個人識別情報から認証用暗号鍵を生成してデータ用暗号鍵を復元することによって、当該データ用暗号鍵により格納データを復号化し、所望のデータを得ることができる。
図１０は、データリカバリーの方法を説明する図である。
データ用暗号鍵が所定の暗号鍵生成用の情報を暗号回路５４にて暗号化して生成されている場合、図１０（Ａ）に示すように、同一の情報を暗号回路５４と同一の暗号ロジックにて暗号化することによりデータ用暗号鍵を再度生成することができる（６－ｐ）。そして、磁気ディスク１０から読み出された格納データがこのデータ用暗号鍵を用いて復号化される（６－ｑ）。
また、個人識別情報を暗号回路５４と同一の暗号ロジックにて暗号化することにより認証用暗号鍵が生成される（６－ｒ）。したがって、磁気ディスク１０から暗号化されたデータ用暗号鍵を読み出すことができれば、図１０（Ｂ）に示すように、この認証用暗号鍵を用いてデータ用暗号鍵が復号化される（６－ｓ）。そして、磁気ディスク１０から読み出された格納データがこのデータ用暗号鍵を用いて復号化される（６－ｔ）。
【００３４】
７．ユーザ認証の解除。
パスワード・ロック機能を備えるハードディスク装置１００には、パスワードを解除するコマンドが標準で設定されている。このコマンドの実行後は、誰でもディスクの内容を読み書きできるようにしなければならない。しかし、磁気ディスク１０の格納データが暗号化されている場合、ユーザ認証の解除に伴って、暗号化されている格納データを全て復号化して磁気ディスク１０に書き戻すことは、多大な時間を要し実用的ではない。そこで、ユーザ認証が解除された場合は、格納データの暗号処理に用いられる暗号鍵を磁気ディスク１０に書き込んでおき、格納データの読み出しの際に誰でも自由に（認証無しに）当該暗号鍵を使用できるようにする。
【００３５】
図７及び図８のようにして格納データの暗号処理を行った場合、磁気ディスク１０には暗号化されたデータ用暗号鍵が保存されている。したがって、このデータ用暗号鍵を復号化して磁気ディスク１０に書き込むことにより、誰でも自由に当該データ用暗号鍵を使用できることとなる。
図１１は、ユーザ認証の解除に伴ってデータ用暗号鍵を誰でも使用できる状態に設定する方法を説明する図である。
図１１に示すように、まず暗号回路５４により、変更前の個人識別情報から認証用暗号鍵が生成され（７－ａ）、この認証用暗号鍵を用いて個人識別情報から認証データが生成される。そして、ＣＰＵ５８により、磁気ディスク１０に記録されている認証データと照会される（７－ｂ）。認証がすんだ後、磁気ディスク１０に記録されている暗号化されたデータ用暗号鍵が読み出され、暗号回路５４により、当該認証用暗号鍵を用いて復号化された後（７－ｃ）、磁気ディスク１０に再度書き込まれる（７－ｄ）。これ以後、磁気ディスク１０に書き込まれたデータ用暗号鍵を用いて、データの読み書きにおける暗号処理が可能となる（７－ｅ）。
【００３６】

以上のようにして暗号鍵（データ用暗号鍵）を誰でも自由に使用できるようにした後、ＣＰＵ５８の制御により、磁気ディスク１０にデータを書き込む際の暗号化及び磁気ディスク１０からデータを読み出した際の復号化を自動的に行うこととすれば、ユーザは、格納データが暗号化されていることを意識せずに、磁気ディスク１０に対してデータの読み書きを行うことが可能となる。また、ユーザ認証が解除された後に磁気ディスク１０に書き込まれるデータは、暗号化しないといった制御を行うことも可能である。この場合、格納データの読み書きの際に、当該格納データが暗号化されているか否かに応じて暗号回路５４による処理を行うかどうかを判断するため、例えばフラグビットを付加するなどの手段によって、暗号化されている格納データと暗号化されていない格納データとを区別することが必要である。

【００３７】

なお、上記のようなユーザ認証の解除を行う場合、

ユーザ認証をセット→ユーザ認証を解除→ユーザ認証をセット

という一連の処理によって、暗号化されていない暗号鍵（データ用暗号鍵）が一時的に磁気ディスク１０に記録されることになる。したがって、このときに第三者に暗号鍵を読み出されてしまうと、当該第三者が、当該暗号鍵によって磁気ディスク１０の格納データを復号化できることとなる。しかしながら、一般のハードディスク装置１００では磁気ディスク１０上に、ユーザによる通常の使用ではアクセスできない特別の記憶領域が設けられているので、暗号化されていない暗号鍵を記録する場合にはこの特別の記憶領域を使用することにより、第三者が暗号鍵を容易に読み出すことができなくなる。

だがこの場合であっても、特殊な測定装置を用いることによって当該記憶領域に書き込まれているデータを読み出すことができるので、ハードディスク装置１００自体が第三者の手に渡った場合には、当該第三者によって格納データを復号化されてしまう危険が残されている。

【００３８】

具体的な事例として、次のような場合が考えられる。

悪意のある第三者が

ユーザ認証をセット→ユーザ認証を解除→ユーザ認証をセット

という手順で、暗号化されていない暗号鍵（データ用暗号鍵）を事前に入手したハードディスク装置１００を、データを盗もうとする対象ユーザに渡したものとする。この場合、対象ユーザが当該ハードディスク装置１００に格納したデータは、暗号化されていても、先の悪意のある第三者が持つ暗号鍵によって復号化できてしまう。

しかし、ハードディスク装置１００の出荷後に、当該ハードディスク装置１００に対してユーザ認証の解除やセットが行われたかどうかをチェックすることは容易なので、かかるチェックによりこのような状況が危惧される場合は、多少時間を要するが、磁気ディスク１０をフォーマットし直す、あるいは暗号化されているデータを、新たな暗号鍵で再暗号化する等の手段で対処することができる。

【００３９】

８．マスター鍵を用いた格納データの復元。

動作６のように、認証用鍵を用いてデータ用暗号鍵を暗号化するのではなく、マスター鍵を用いてデータ用暗号鍵を暗号化し、磁気ディスク１０に保存することもできる。

図１２は、マスター鍵を用いた格納データの復元方法を説明する図である。

図１２に示すように、暗号回路５４により、まず個人識別情報が暗号化されて認証用暗号鍵が生成される（８－ａ）。そして、この認証用暗号鍵を用いて暗号回路５４により個人識別情報が再度暗号化されて認証データが生成され、磁気ディスク１０に保存される（８－ｂ）。また、データ用暗号鍵が、別途生成されたマスター鍵を用いて暗号化され、磁気ディスク１０に書き込まれ保存される（８－ｃ）。格納データの暗号化及び復号化には、データ用暗号鍵が用いられる（８－ｄ）。データ用暗号鍵に関して、所定の暗号鍵生成用の情報から暗号回路５４で暗号化して生成したり、乱数列等の任意の情報を設定して暗号鍵としたり、個人識別情報を認証用暗号鍵とは異なる関数で変換して生成したりできるこ

とは、動作６の場合と同様である。
このようにして暗号化されたデータ用暗号鍵を磁気ディスク１０に保存しておけば、マスター鍵を用いてデータ用暗号鍵を復元できるので（８－ｅ）、動作７のようにデータ用暗号鍵を復号化して磁気ディスク１０に保存しておかなくても、マスター鍵の所持者は自由に、暗号化された格納データの読み出し、復号化が可能となる（８－ｆ）。
【００４０】
Ｂ．格納データの暗号化及び復号化の制御に関する処理。
この処理では、ハードディスク装置１００の暗号機能のオン・オフに応じて、記録媒体に対する読み込み及び書き込みの単位ごとに、データに対する暗号処理を制御する。データの読み込み及び書き込みの単位は、例えば、磁気ディスク１０の記憶領域に設定されるセクタや論理ブロックとすることができる。以下では、セクタごとに暗号化を行うか否かを制御する場合を例として説明する。なお、ハードディスク装置１００における暗号機能のオン・オフの切り替えは、例えばホストシステムであるコンピュータ装置からハードディスク・ドライバ等を介して切り替えコマンドを発行する等の手段によって行うことができる。また、ハードウェア筐体の物理的なスイッチ（ジャンパースイッチ等）で暗号機能のオン・オフの切り替えを行うことも可能である。
データの暗号化に広く用いられる共通鍵暗号法の処理単位は、通常、６４ビットまたは１２８ビットであり、この場合５１２バイト（４０９６ビット）のディスク・セクタは、６４個あるいは３２個のブロックに分割されて暗号処理が施されることになる。暗号化の代表的な利用モードには、ＥＣＢ（Electronic Code Book）モードとＣＢＣ（Cipher Block Chaining）モードとがある。
【００４１】
図１３は、ＥＣＢモード及びＣＢＣモードにおける暗号化及び復号化処理の概念を示す図である。
図１３に示すように、セクタを分割して生成された平文（暗号化されていないデータ）ブロックP_i（ｉ＝０、１、２、・・・）をＥＣＢモードで暗号化した場合、対応する暗号文ブロックC_iから元の平文ブロックP_i求めることは計算上不可能であるが、同じ値の６４あるいは１２８ビットの暗号文ブロックは同じ値の平文ブロックに対応するので、どのデータとどのデータとが同じものなのかといった情報が露見してしまう。
【００４２】
そこで通常、ある程度のデータ長を持つデータを暗号化する場合にはＣＢＣモードが用いられる。これは、対象データと前のデータとのＸＯＲ（Exclusive OR：排他的論理和）を次々に取りながら暗号化していく方式である。図１３に示すＣＢＣモードの暗号化において、平文ブロックP_iは、前の暗号文ブロックC_{i-1}とＸＯＲされた後に暗号化される。これにより、同じ平文であっても違う暗号文に変換されることとなる。
ＣＢＣモードでは、最初の平文ブロックP_0は、ＸＯＲすべき暗号文がないため、通常はイニシャル・ベクタ（ＩＶ）とよばれる適当なデータを暗号化し、擬似乱数C_{IV}を生成した後に平文ブロックP_0とＸＯＲする。本実施の形態ではこのイニシャル・ベクタに、各セクタを識別するためのセクタ番号を用いることとする。なお、セクタ以外の単位でデータを暗号処理する場合は、各単位を特定する情報をイニシャル・ベクタとして用いれば良い（例えば、論理ブロックを暗号処理の単位とする場合、ＬＢＡ（Logical Block Address：論理ブロックアドレス）を用いることができる）。
【００４３】
図１４は、本実施の形態による暗号処理に対応したセクタのデータ構成を模式的に示す図である。
図１４を参照すると、各セクタには、個々のセクタを識別するためのセクタ番号１４０１と、格納データであるセクタデータ１４０２と、セクタデータ１４０２が暗号化されているか否かを示す制御フラグであるフラグビット１４０３とが記録される。
セクタデータ１４０２が暗号化されていないセクタのフラグビット１４０３は「０」にセットされ、セクタデータ１４０２が暗号化されているセクタのフラグビット１４０３は「

１」にセットされるものとする。したがって、ハードディスク装置１００の出荷時のように初期状態では暗号機能がオフにされているので、磁気ディスク１０における各セクタのフラグビット１４０３は「０」にリセットされることになる。

【００４４】

本実施の形態では、格納データの暗号処理に関して、次の２種類の制御を行う。すなわち、データの書き込み処理において、ハードディスク装置１００における暗号機能のオン・オフに応じて、磁気ディスク１０に書き込むデータの暗号化を行うか否かを制御する。また、データの読み出し処理において、格納データが暗号化されたデータである場合（すなわちフラグビット１４０３の値が「１」である場合）に、読み出したデータを復号化する。

図１に示したハードディスク装置１００では、セクタごとの読み書きデータに対して、セレクタ５５が、暗号機能のオン・オフ及びフラグビット１４０３の値を調べて、暗号回路５４にて書き込みデータの暗号化、または読み出しデータの復号化を行うか否かを判断することができる。

【００４５】

図１５は、ハードディスク装置１００の暗号機能をオフにした状態でデータの読み書きを行った場合のセクタデータ１４０２及びフラグビット１４０３の様子を示す図である。

ハードディスク装置１００の暗号機能をオフにした状態のままでデータの読み書きを行った場合、セクタデータ１４０２は暗号化されない生のデータであり、フラグビット１４０３の値は「０」のままである。

図１５に示す例では、セクタ番号「０」、「２」のセクタデータ１４０２が読み出され、新たに書き込まれているが、データは暗号化されず、フラグビット１４０３の値は「０」である。

【００４６】

図１６は、ハードディスク装置１００の暗号機能をオンにした状態でデータの読み書きを行った他の場合のセクタデータ１４０２及びフラグビット１４０３の様子を示す図である。

ハードディスク装置１００の暗号機能をオンにした場合、その後のデータの書き込みでは暗号化が行われ、フラグビット１４０３の値は「１」となる。すなわち、暗号機能をオンにした後には、データの書き込み処理が行われる度に、徐々に磁気ディスク１０の格納データが暗号化されていく。このため、ユーザは、暗号機能をオンにした時点で磁気ディスク１０の格納データが全て暗号化されるのを待つことなく、直ちにデータアクセスが可能である。

格納データの読み出しにおいては、フラグビット１４０３の値が「０」であれば（すなわち暗号化されていない格納データの読み出しであれば）、データをそのまま読み出す。一方、フラグビット１４０３の値が「１」であれば、（すなわち暗号化された格納データの読み出しであれば）読み出したデータを復号化する。

図１６（Ａ）に示す例では、セクタ番号「０」、「２」のセクタデータ１４０２が読み出され、セクタ番号「０」に新たなデータが書き込まれているが、このデータ書き込みの際、書き込まれるセクタデータ１４０２は暗号化され、フラグビット１４０３の値は「１」となる。また図１６（Ｂ）に示す例では、セクタ番号「０」、「２」のセクタデータ１４０２が読み出され、新たに書き込まれている。セクタ番号「０」のセクタデータ１４０２は、図１６（Ａ）に示した書き込みで暗号化されているので、読み出しの際に復号化される。またセクタ番号「０」、「２」とも、新たに書き込まれるセクタデータ１４０２は暗号化され、フラグビット１４０３の値は「１」となる。

【００４７】

図１７は、一旦ハードディスク装置１００の暗号機能をオンにした後に再度オフにした状態でデータの読み書きを行った場合のセクタデータ１４０２及びフラグビット１４０３の様子を示す図である。

この場合、暗号機能がオンの状態であったときに書き込まれたセクタデータ１４０２は暗

号化されているので、読み出しの際に復号化される。一方、暗号化されていないセクタデータ１４０２はそのまま読み出される。暗号機能をオフの状態にした後に新たに書き込まれるセクタデータ１４０２は暗号化されず、フラグビット１４０３の値は「０」となる。図１７に示す例では、セクタ番号「０」、「２」のセクタデータ１４０２が読み出され、新たに書き込まれているが、暗号化されているセクタ番号「０」のセクタデータ１４０２の読み出しではデータの復号化が行われる。また、書き込みの際にはいずれも暗号化は行われない。

【００４８】

以上のようにして、ハードディスク装置１００の暗号機能のオン・オフに応じてセクタごとのデータの読み書きのたびに暗号化及び復号化処理が行われる。ここで、「Ａ．暗号鍵の管理に関する処理。」で説明したように、パスワード等の個人識別情報を用いたユーザ認証を行う場合、暗号機能をオンの状態にしたときには暗号鍵を使用するために認証を行い、暗号機能をオフの状態にしたときには認証を行わずに暗号鍵を使用できるようにする（例えば動作７のように、暗号鍵を暗号化せずに磁気ディスク１０に保存しておく）。これによって、暗号機能がオフであれば、セクタデータ１４０２の読み出し時にフラグビット１４０３の値が「１」でも自動的に復号化を行うようにし、ユーザは読み出したデータが暗号化されていたものか否かを意識しないで読み書きができることとなる。

なお、複数のフラグビット１４０３が用意できるならば、複数ユーザで１台のハードディスク装置１００を共用する場合に、セクタごとの暗号処理をユーザ別に管理することも可能である。

【００４９】

上述した格納データの暗号化及び復号化の制御では、暗号化の利用モードとしてＣＢＣモードを用い、セクタ番号をイニシャル・ベクタとし、これを暗号化した擬似乱数C_{IV}を初期的に用いて格納データの暗号化を行うこととした。しかしながら、イニシャル・ベクタやこれを暗号化した疑似乱数C_{IV}には機密性が必要なく、任意の値を用いることができる。また、セクタ番号は各セクタにユニークに振られた値であるので、これを乱数化せずに直接用いて同じデータを暗号化しても、セクタごとに異なる暗号文が得られる。したがって、初期的にセクタ番号を直接平文ブロックP_0とＸＯＲして暗号化を行っても良い。

【００５０】

以上説明したように、本実施の形態では、ハードディスク装置１００のハードディスク・コントローラ５０に暗号回路５４を組み込んだことにより、ホストシステムであるコンピュータ装置（ＯＳ）側で特別の処理を行わずに、すなわちユーザが意識することなくハードディスク装置１００の格納データを暗号処理することが可能である。

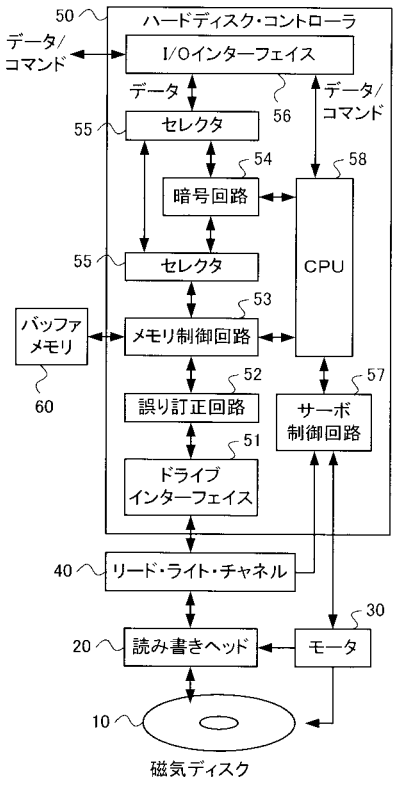
また、格納データの暗号処理に用いるデータ用の暗号鍵を、個人識別情報から生成した別の暗号鍵で暗号化し、磁気ディスク１０に格納しておくことにより、個人識別情報を変更する場合にも、データ用の暗号鍵を暗号化し直すだけで対応できる。このため、格納データ全体を一旦復号化して暗号化し直すといった繁雑な作業が不要となる。

さらに、セクタ等の格納データの読み書き単位ごとに、ハードディスク装置１００における暗号機能のオン・オフに応じて、データの暗号処理を行うか否かを制御することにより、データアクセスの際にユーザに意識させることなく、格納データの暗号化もしくは暗号解除を進めることができる。このため、磁気ディスク１０中に暗号化された格納データと暗号化されていない格納データとを無理なく混在させることができる。したがって、暗号機能をオン・オフする度に、格納データ全体を暗号化したり復号化したりするといった繁雑な作業が不要となる。また、ハードディスク装置１００（もしくはコンピュータ装置）の出荷時に所定のソフトウェアがプレインストールされる場合にも、かかるソフトウェアは機密性がないので出荷時の初期状態では暗号化せずにおき、ユーザが暗号化機能をオンした後の書き込みデータは機密性を有すると考えられるので、暗号化していくといった使用方法が容易に実現される。また、暗号化機能をオンした後に、磁気ディスク１０に格納されているデータの全てを暗号化する必要がある場合、全データあるいは全セクタを順次読み出し、暗号化して再書き込みすることによって、処理に時間を要するものの、全デー

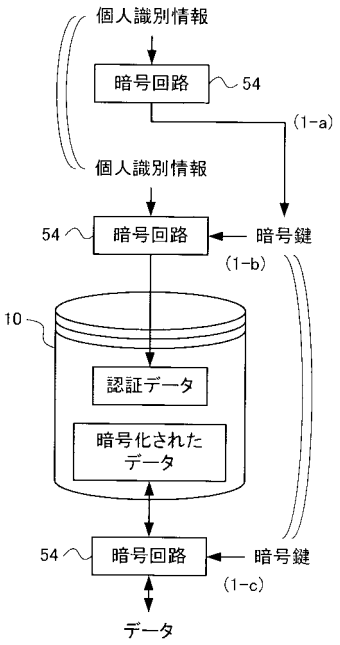
タを暗号化することが可能である。
【００５１】
なお、上述した実施の形態では、記録媒体として磁気ディスクを用いたハードディスク装置１００を対象として説明したが、ＤＶＤ（Digital Versatile Disc）やＣＤ（Compact Disc）といった光ディスク、メモリカード等を記録媒体に用いた各種の外部記憶装置において、記録媒体に対してデータの読み書きを行う際の暗号処理に適用することができる。
また、上記の実施の形態では、書き込みデータを暗号化し読み出しデータを復号化する使用の利便性を考慮し、暗号方式として共通鍵暗号を用いる場合を説明したが、格納データや個人識別情報を暗号化する暗号方式としては必ずしも共通鍵暗号に限るものではない。例えば、ユーザ認証を行う際にも認証データから元のデータを復号化する必要のない個人識別情報の暗号化などは、公開鍵暗号などを用いることも可能である。
さらに、上記の実施の形態による暗号処理は、ホストシステムによらずに外部記憶装置自身で格納データの暗号処理を制御すると共に、かかる暗号処理とユーザ認証とを併せて行う場合に特に適するものであるが、この暗号処理及びユーザ認証をホストシステムからの制御によって行う実施態様もあり得ることは言うまでもない。その場合、ホストシステムであるコンピュータ装置のプログラム制御されたＣＰＵ、あるいは当該ＣＰＵと所定の暗号回路とを暗号処理手段として用い、これによって、これらの暗号処理及びユーザ認証が実行されることとなる。
【００５２】
【発明の効果】
以上説明したように、本発明によれば、記憶装置に対してユーザ認証と格納データの暗号化とを併せて適用する場合に好適な格納データの暗号処理及び暗号鍵の管理を実現することができる。
また本発明によれば、着脱自在に実装された記憶装置に好適な格納データの暗号処理方法及びこれを実現する記憶装置を提供することができる。
【図面の簡単な説明】
【図１】本実施の形態におけるハードディスク装置の構成例を示す図である。
【図２】本実施の形態によるユーザ認証の初期設定の方法を説明する図である。
【図３】本実施の形態によるユーザ認証の方法と格納データの暗号処理を説明する図である。
【図４】本実施の形態による磁気ディスクに不具合が発生した場合の格納データの復元方法を説明する図である。
【図５】本実施の形態によるマスター鍵を用いた格納データの復元方法を説明する図である。
【図６】個人識別情報による認証データとは別にハードディスク装置のロックを解除するための認証データを設定する方法を説明する図である。
【図７】本実施の形態による個人識別情報を変更する場合における暗号処理の対応方法を説明する図であり、初期設定の動作を説明する図である。
【図８】本実施の形態による個人識別情報を変更する場合における暗号処理の対応方法を説明する図であり、ユーザ認証及び格納データの暗号処理を説明する図である。
【図９】本実施の形態による個人識別情報を変更する際の動作を説明する図である。
【図１０】本実施の形態によるデータリカバリーの方法を説明する図である。
【図１１】本実施の形態によるユーザ認証の解除に伴ってデータ用暗号鍵を誰でも使用できる状態に設定する方法を説明する図である。
【図１２】本実施の形態において、認証用暗号鍵とデータ用暗号鍵とを別に設けた場合に、マスター鍵を用いて格納データを復元する方法を説明する図である。
【図１３】ＥＣＢモード及びＣＢＣモードにおける暗号化及び復号化処理の概念を示す図である。
【図１４】本実施の形態による暗号処理に対応したセクタのデータ構成を模式的に示す図である。

【図１５】本実施の形態における、ハードディスク装置の暗号機能をオフにした状態でデータの読み書きを行った場合のセクタデータ及びフラグビットの様子を示す図である。
【図１６】本実施の形態における、ハードディスク装置の暗号機能をオンにした状態でデータの読み書きを行った他の場合のセクタデータ及びフラグビットの様子を示す図である。
【図１７】本実施の形態における、一旦ハードディスク装置の暗号機能をオンにした後に再度オフにした状態でデータの読み書きを行った場合のセクタデータ及びフラグビットの様子を示す図である。
【図１８】本実施の形態の暗号機能を備えたハードディスク装置を搭載した情報処理装置の概略構成を示す図である。
【符号の説明】
１０…磁気ディスク、２０…読み書きヘッド、３０…モータ、４０…リード・ライト・チャネル、５０…ハードディスク・コントローラ、５１…ドライブインターフェイス、５２…誤り訂正回路、５３…メモリ制御回路、５４…暗号回路、５５…セレクタ、５６…Ｉ／Ｏインターフェイス、５７…サーボ制御回路、５８…ＣＰＵ、６０…バッファメモリ、１４０１…セクタ番号、１４０２…セクタデータ、１４０３…フラグビット

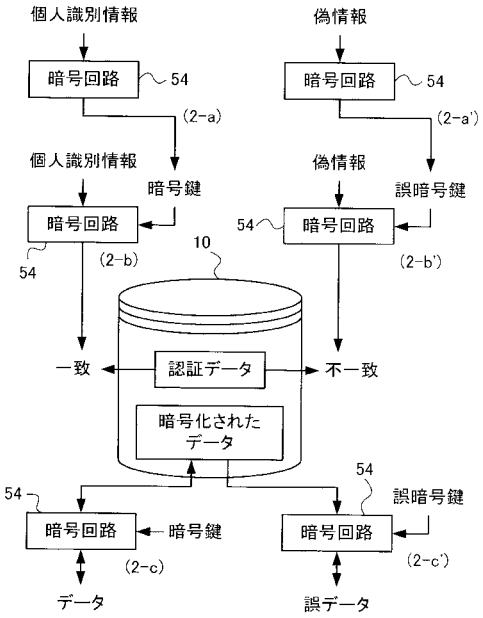
【図１】



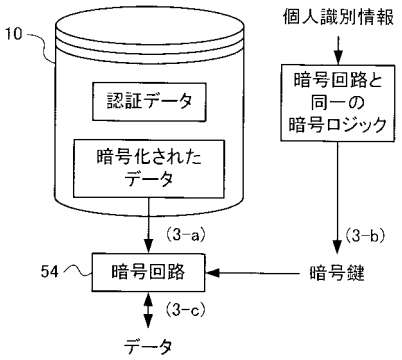
【図２】



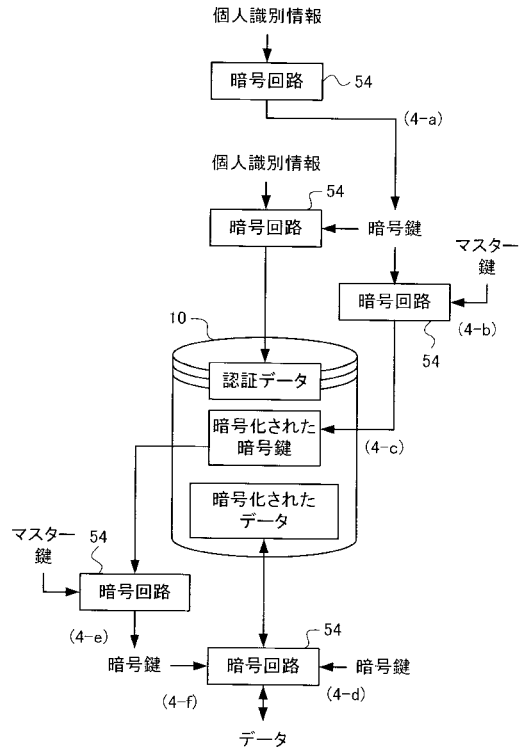
【図３】


個人識別情報
偽情報
暗号回路
54
(2-a)
(2-a')
暗号鍵
誤暗号鍵
(2-b)
(2-b')
10
一致
認証データ
不一致
暗号化された
データ
誤暗号鍵
(2-c)
(2-c')
データ
誤データ

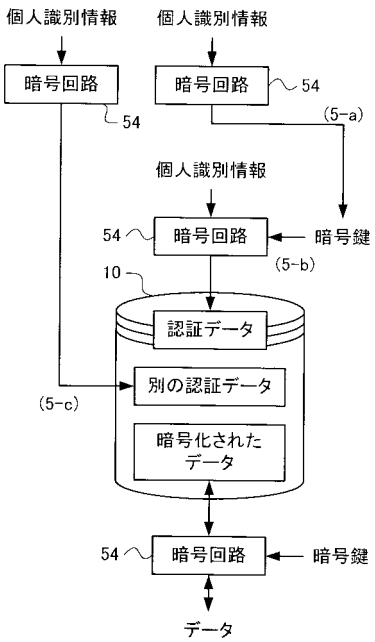
【図４】


10
認証データ
暗号化された
データ
個人識別情報
暗号回路と
同一の
暗号ロジック
(3-a)
(3-b)
暗号回路
暗号鍵
(3-c)
データ

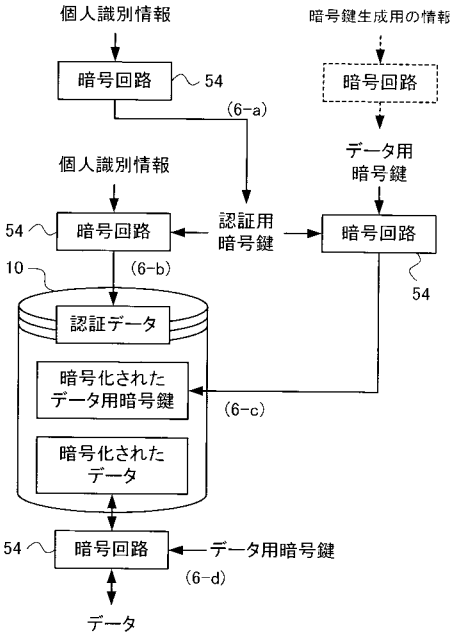
【図５】


個人識別情報
暗号回路
54
(4-a)
暗号鍵
マスター
鍵
(4-b)
10
認証データ
暗号化された
暗号鍵
(4-c)
暗号化された
データ
(4-e)
(4-f)
(4-d)
データ

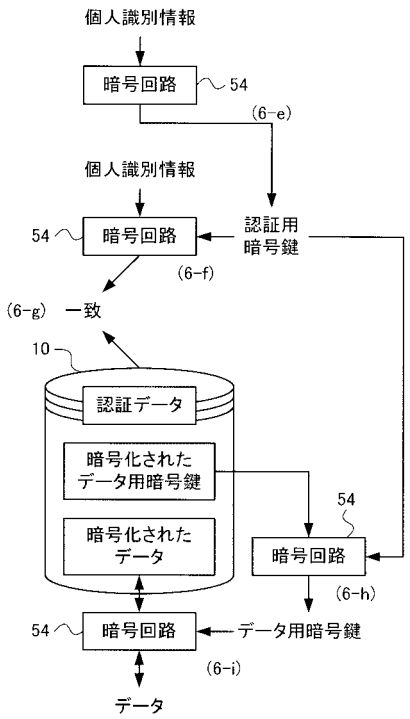
【図６】


個人識別情報
暗号回路
54
(5-a)
暗号鍵
(5-b)
10
認証データ
別の認証データ
(5-c)
暗号化された
データ
データ

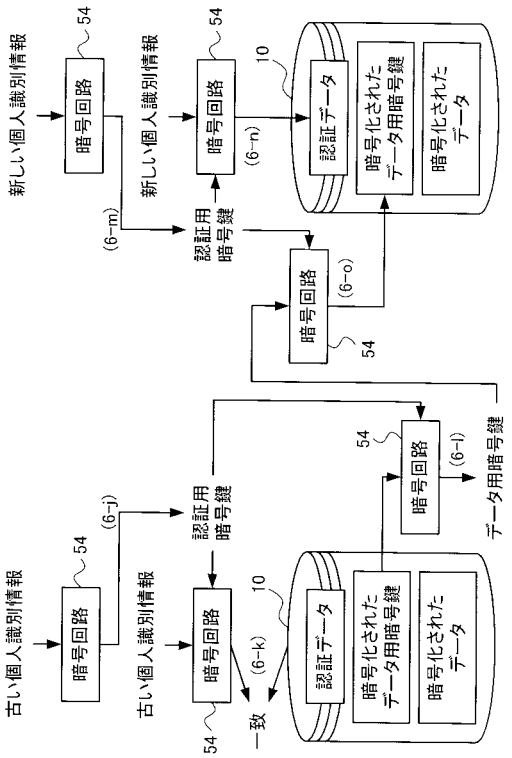
【図７】


個人識別情報
暗号回路
54
(6-a)
暗号鍵生成用の情報
暗号回路
データ用
暗号鍵
個人識別情報
54
暗号回路
認証用
暗号鍵
暗号回路
54
10
(6-b)
認証データ
暗号化された
データ用暗号鍵
(6-c)
暗号化された
データ
54
暗号回路
データ用暗号鍵
(6-d)
データ

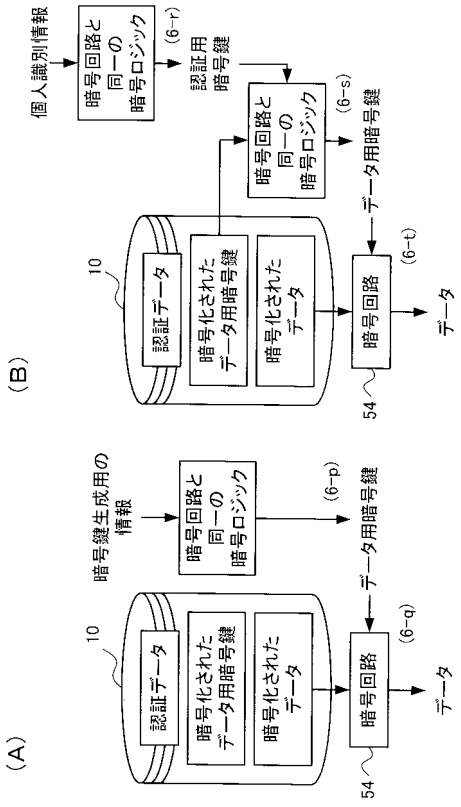
【図８】


個人識別情報
暗号回路
54
(6-e)
個人識別情報
54
暗号回路
認証用
暗号鍵
(6-f)
(6-g) 一致
10
認証データ
暗号化された
データ用暗号鍵
暗号化された
データ
54
暗号回路
(6-h)
54
暗号回路
データ用暗号鍵
(6-i)
データ

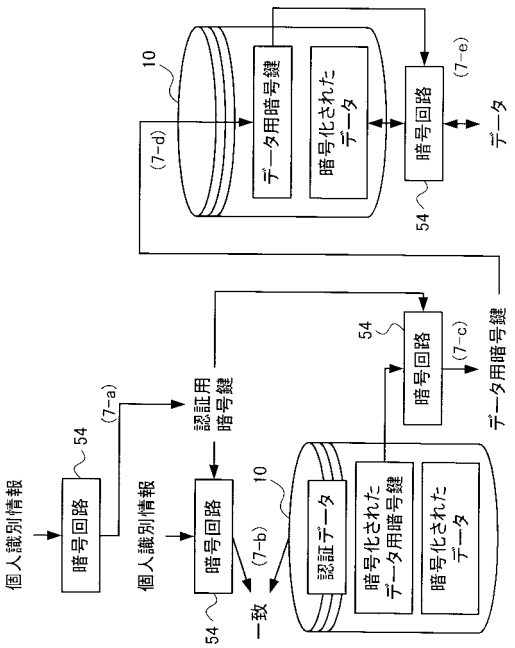
【図９】


新しい個人識別情報
54
暗号回路
(6-m)
新しい個人識別情報
54
暗号回路
(6-n)
10
認証データ
暗号化された
データ用暗号鍵
暗号化された
データ
認証用
暗号鍵
暗号回路
(6-o)
54
古い個人識別情報
54
暗号回路
(6-j)
古い個人識別情報
認証用
暗号鍵
暗号回路
(6-k)
10
認証データ
暗号化された
データ用暗号鍵
暗号化された
データ
54
一致
54
暗号回路
(6-l)
データ用暗号鍵

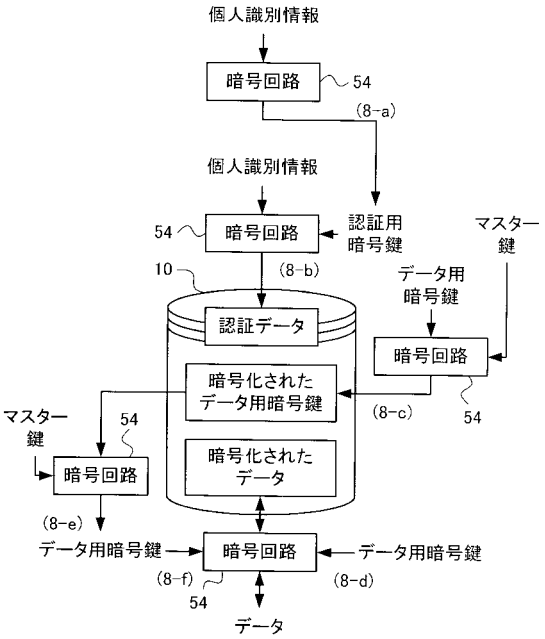
【図１０】


(B)
個人識別情報
暗号回路と
同一の
暗号ロジック
(6-r)
認証用
暗号鍵
暗号回路と
同一の
暗号ロジック
(6-s)
データ用暗号鍵
10
認証データ
暗号化された
データ用暗号鍵
暗号化された
データ
暗号回路
(6-t)
54
データ
(A)
暗号鍵生成用の
情報
暗号回路と
同一の
暗号ロジック
(6-p)
データ用暗号鍵
10
認証データ
暗号化された
データ用暗号鍵
暗号化された
データ
暗号回路
(6-q)
54
データ

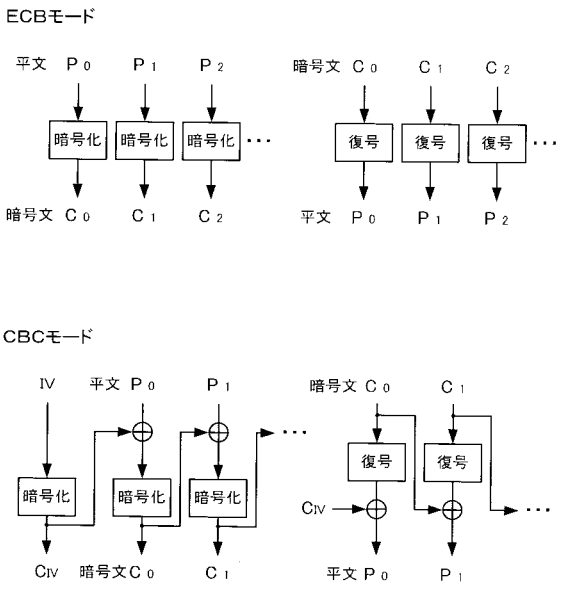
【図１１】



【図１２】



【図１３】



【図１４】

【図１５】

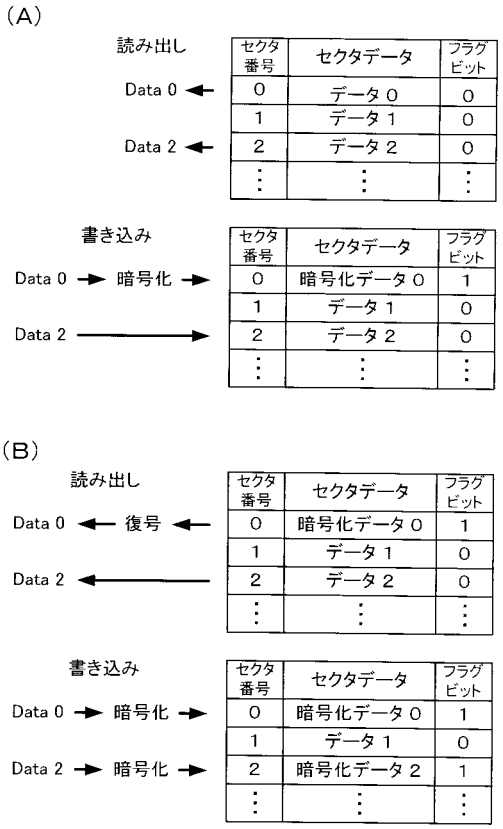
読み出し

	セクタ番号	セクタデータ	フラグビット
Data 0 ←	0	データ０	0
	1	データ１	0
Data 2 ←	2	データ２	0
	⋮	⋮	⋮

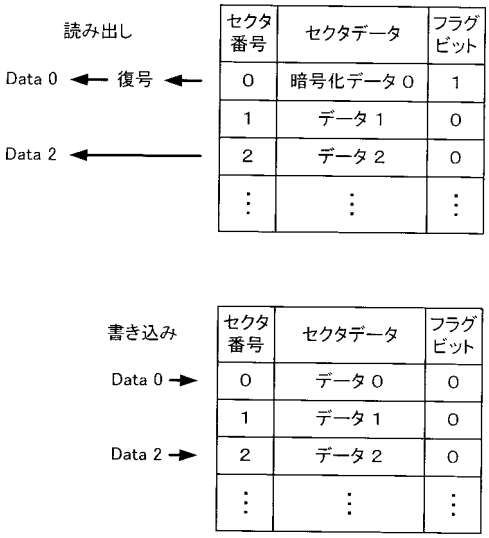
書き込み

	セクタ番号	セクタデータ	フラグビット
Data 0 →	0	データ０	0
	1	データ１	0
Data 2 →	2	データ２	0
	⋮	⋮	⋮

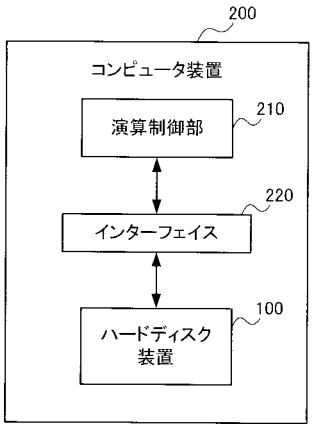
【図１６】


(A)
読み出し
Data 0
Data 2
セクタ番号
セクタデータ
フラグビット
0
データ０
0
1
データ１
0
2
データ２
0
書き込み
Data 0
暗号化
Data 2
0
暗号化データ０
1
1
データ１
0
2
データ２
0
(B)
読み出し
Data 0
復号
Data 2
0
暗号化データ０
1
1
データ１
0
2
データ２
0
書き込み
Data 0
暗号化
Data 2
暗号化
0
暗号化データ０
1
1
データ１
0
2
暗号化データ２
1

【図１７】


読み出し
Data 0
復号
Data 2
セクタ番号
セクタデータ
フラグビット
0
暗号化データ０
1
1
データ１
0
2
データ２
0
書き込み
Data 0
Data 2
0
データ０
0
1
データ１
0
2
データ２
0

【図１８】


200
コンピュータ装置
演算制御部
210
220
インターフェイス
100
ハードディスク装置

フロントページの続き

(74)復代理人 100104880
弁理士 古部 次郎
(74)復代理人 100118201
弁理士 千田 武
(72)発明者 佐藤 証
神奈川県大和市下鶴間１６２３番地１４ 日本アイ・ビー・エム株式会社 東京基礎研究所内
(72)発明者 森岡 澄夫
神奈川県大和市下鶴間１６２３番地１４ 日本アイ・ビー・エム株式会社 東京基礎研究所内
(72)発明者 高野 光司
神奈川県大和市下鶴間１６２３番地１４ 日本アイ・ビー・エム株式会社 東京基礎研究所内

Ｆターム(参考) 5B017 AA03 BA07 CA07 CA16
5J104 AA07 AA12 AA16 EA04 EA15 JA03 KA01 KA04 NA02 PA14