(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-299448
(P2008-299448A)
(43)公開日　平成20年12月11日(2008.12.11)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	540P	5B017
G09C 1/00	(2006.01)	G09C	1/00	660D	5D044
H04L 9/08	(2006.01)	G06F	12/14	530P	5J104
G11B 20/10	(2006.01)	H04L	9/00	601A	
		G11B	20/10	H	

審査請求 未請求　請求項の数 16　ＯＬ　（全 19 頁）

(21)出願番号　特願2007-142649 (P2007-142649)
(22)出願日　平成19年5月29日 (2007.5.29)

(71)出願人　503116280
ヒタチグローバルストレージテクノロジーズネザーランドビーブイ
オランダ国　アムステルダム　１０７６　エイズィ　パルナスストーレン　ロカテリケード　１
(74)代理人　100113697
弁理士　新藤　善信
(74)代理人　100103894
弁理士　家入　健
(72)発明者　渡部　善寿
神奈川県小田原市国府津２８８０番地　株式会社日立グローバルストレージテクノロジーズ内

最終頁に続く

(54)【発明の名称】データ記憶装置及び暗号鍵に関する情報の更新方法

(57)【要約】
【課題】暗号処理に使用するデータを安全に更新する。
【解決手段】本発明の一実施形態において、ＨＤＤは、ユーザ・データを暗号化した状態で取り扱う。ユーザ・データの暗復号化に使用するデータ用暗号鍵は、パスワードを使用して暗号化され、磁気ディスクに格納されている。ＭＰＵは、パスワードと乱数とを使用してデータ用暗号鍵を復号化し、暗号処理部に供給する。パスワードと暗号化されたデータ用暗号鍵（鍵情報）は、二重化されて磁気ディスクに格納されている。更新状態を示すフラグと、鍵情報を無効化してから更新することで、電源遮断により更新処理が中断しても、回復することができる。
【選択図】図５

STEP	PRIMARY PASSWORD	PRIMARY KEY INFO	BACKUP PASSWORD	BACKUP KEY INFO
10	PREVIOUS	PREVIOUS (COMPLETE FLAG)	PREVIOUS	PREVIOUS
11	PREVIOUS	PREVIOUS **(UPDATING FLAG)**	PREVIOUS	PREVIOUS
12	PREVIOUS	PREVIOUS (UPDATING FLAG)	PREVIOUS	**INVALID**
13	PREVIOUS	PREVIOUS (UPDATING FLAG)	**NEW**	INVALID
14	PREVIOUS	PREVIOUS (UPDATING FLAG)	NEW	**NEW**
15	PREVIOUS	**INVALID (UPDATING FLAG)**	NEW	NEW
16	NEW	INVALID (UPDATING FLAG)	NEW	NEW
17	NEW	**NEW (COMPLETE FLAG)**	NEW	NEW

【特許請求の範囲】
【請求項１】
暗号化したユーザ・データを記憶するデータ記憶装置であって、
プライマリ第１データと、プライマリ第２データと、前記プライマリ第１データのコピーであるバックアップ第１データと、前記プライマリ第２データのコピーであるバックアップ第２データと、をそれぞれ不揮発性メモリ領域の異なるアドレスに格納する、不揮発メモリ領域と、
前記プライマリ第１データと前記プライマリ第２データとを用いてユーザ・データの暗号処理を実行する暗号処理部と、
前記プライマリ第１データと前記バックアップ第１データの一方を無効状態に設定し、前記無効状態に設定した第１データと同じ種類の第２データを更新し、前記同じ種類の第２データを更新した後に前記無効状態に設定した第１データを更新し、前記無効状態に設定した第１データを更新した後に、前記無効状態に設定した第１データと異なる種類の第１データ及び第２データを更新する、更新処理部と、
を有するデータ記憶装置。
【請求項２】
前記無効状態に設定した第１データは、前記バックアップ第１データである、
請求項１に記載のデータ記憶装置。
【請求項３】
前記更新処理部は、前記異なる種類の第１データを無効状態に設定した後に前記異なる種類の第２データを更新し、前記異なる種類の第２データを更新した後に前記異なる種類の第１データを更新する、
請求項１に記載のデータ記憶装置。
【請求項４】
前記更新処理部は、前記プライマリ第１データが無効状態である場合に前記バックアップ第１データをコピーし、前記バックアップ第１データが無効状態である場合に前記プライマリ第１データをコピーする、
請求項３に記載のデータ記憶装置。
【請求項５】
前記更新処理部は、前記プライマリ第１データと前記バックアップ第１データの一方を無効状態に設定する前に、フラグを更新中状態に設定し、前記異なる種類の第１データ及び第２データを更新した後に前記フラグを更新完了状態に設定する、
請求項１に記載のデータ記憶装置。
【請求項６】
前記フラグは、前記異なる種類の第１データ及び第２データの内の後に更新されるデータと同一のアドレスに格納されている、
請求項５に記載のデータ記憶装置。
【請求項７】
前記プライマリ第１データ、前記プライマリ第２データ、前記バックアップ第１データ、前記バックアップ第２データのそれぞれは、格納されているアドレス領域内においてランダム・データ内にある、
請求項１に記載のデータ記憶装置。
【請求項８】
前記プライマリ第１データ、前記プライマリ第２データ、前記バックアップ第１データ、前記バックアップ第２データの少なくとも一つは、複数のアドレス領域に分割して格納されている、
請求項７に記載のデータ記憶装置。
【請求項９】
対象データの暗号処理に用いる複数のデータを更新する方法であって、
プライマリ第１データと、プライマリ第２データと、前記プライマリ第１データのコピ

ーであるバックアップ第１データと、前記プライマリ第２データのコピーであるバックアップ第２データと、をそれぞれ不揮発性メモリ領域の異なるアドレスに格納し、
前記プライマリ第１データと前記プライマリ第２データとを用いて暗号処理を実行し、
前記プライマリ第１データと前記バックアップ第１データの一方を無効状態に設定し、
前記無効状態に設定した第１データと同じ種類の第２データを更新し、
前記同じ種類の第２データを更新した後に前記無効状態に設定した第１データを更新し、
前記無効状態に設定した第１データを更新した後に、前記無効状態に設定した第１データと異なる種類の第１データ及び第２データを更新する、
方法。
【請求項１０】
前記無効状態に設定した第１データは、前記バックアップ第１データである、
請求項９に記載の方法。
【請求項１１】
前記異なる種類の第１データ及び第２データの更新は、
前記異なる種類の第１データを無効状態に設定した後に前記異なる種類の第２データを更新し、
前記異なる種類の第２データを更新した後に、前記異なる種類の第１データを更新する、
請求項９に記載の方法。
【請求項１２】
前記プライマリ第１データが無効状態である場合に前記バックアップ第１データをコピーし、
前記バックアップ第１データが無効状態である場合に前記プライマリ第１データをコピーする、
請求項１１に記載の方法。
【請求項１３】
前記プライマリ第１データと前記バックアップ第１データの一方を無効状態に設定する前に、フラグを更新中状態に設定し、
前記異なる種類の第１データ及び第２データを更新した後に、前記フラグを更新完了状態に設定する、
請求項９に記載の方法。
【請求項１４】
前記フラグは、前記異なる種類の第１データ及び第２データの内の後に更新されるデータと同一のアドレスに格納されている、
請求項１３に記載の方法。
【請求項１５】
前記プライマリ第１データ、前記プライマリ第２データ、前記バックアップ第１データ、前記バックアップ第２データのそれぞれを、ランダム・データ内格納する、
請求項９に記載の方法。
【請求項１６】
前記プライマリ第１データ、前記プライマリ第２データ、前記バックアップ第１データ、前記バックアップ第２データの少なくとも一つを、複数のアドレス領域に分割して格納する、
請求項１５に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はデータ記憶装置及び暗号処理に用いる複数のデータを更新する方法に関し、特に、暗号処理に用いる複数のデータの更新時に中断した場合にも、それら複数のデータを

回復する技術に関する。
【背景技術】
【０００２】
データを記憶するメディアとして、光ディスク、光磁気ディスク、磁気ディスクあるいは半導体メモリなどの様々な方式が知られている。これらメディアを使用してデータを記憶するデータ記憶装置において、メディアに保存されるユーザ・データを不正なアクセスから保護するため、そのユーザ・データを暗号化する技術が知られている。例えば、特許文献１は、磁気ディスクをメディアとして使用するハードディスク・ドライブ（ＨＤＤ）において、磁気ディスクに記憶するデータを暗号化する技術の一例を開示している。
【０００３】
具体的には、ＨＤＤはデータの暗号化と復号化とを行う暗号処理部を有している。この暗号処理部は、磁気ディスク装置内において、磁気ディスクに記録されるデータ、そして磁気ディスクから再生されるデータを、それぞれデータ転送速度で暗号化及び復号化する。このＨＤＤは、ユーザ・データの暗復号化のためのデータ用暗号鍵を、個人識別情報（例えばパスワード）を暗号化することで生成する。
【０００４】
更に、このＨＤＤは、パスワードをデータ用暗号鍵で暗号化し、その暗号化したパスワードを認証データとしてＨＤＤ内に格納しておく。利用者の認証時において、ＨＤＤは、格納されている認証データと入力されたパスワードから生成したデータ用暗号鍵による暗号処理結果とを比較し、それらの一致を検証する。利用者認証が成功すると、ＨＤＤは、データ用暗号鍵を生成し、そのデータ用暗号鍵を磁気ディスクのユーザ・データの暗復号に使用する。
【０００５】
また、上記特許文献１は、別の方法を開示している。この別の方法は、データの暗復号化のためのデータ用暗号鍵を個別に生成する。ＨＤＤは、さらに、パスワードを暗号化した認証暗号鍵でデータ用暗号鍵を暗号化し、その内部に保持する。ＨＤＤを使用する際には、ＨＤＤは利用者の認証を実施し、正規の利用者であれば、入力されたパスワードから生成した認証暗号鍵でＨＤＤ内に保持されている暗号化されたデータ用暗号鍵を復号し、そのデータ用暗号鍵を磁気ディスクのデータの暗復号に使用する。
【特許文献１】特開２００４－２０１０３８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
保存されているデータの安全性を高めるためには、ＨＤＤは、所定の頻度でパスワードに関する情報やデータ用暗号鍵に関する情報を更新することが好ましい。これによって、不正使用者が、ＨＤＤ内のこれらのデータを取得し、不正に磁気ディスク上のユーザ・データにアクセスする可能性を小さくすることができる。
【０００７】
しかし、ＨＤＤ内のパスワードやデータ用暗号鍵に関する情報を更新する際に、予期していない電源遮断等の障害が発生することが考えられる。このような障害により更新途中で処理が中断されると、パスワードやデータ用暗号鍵に関する情報が正しく更新されず、それらの情報を消失してしまう。すると、ＨＤＤは正しく認証処理を行うことができない、あるいは、暗号化されたデータを正しく再生することができなくなる。
【０００８】
従って、ＨＤＤなどのデータ記憶装置が、暗号処理に使用する情報を、安全に更新することができる手法が必要となる。つまり、更新処理が中断した場合であっても、必要な情報を回復することができる技術が必要となる。特に、ユーザ認証用のパスワードとデータ用暗号鍵とを連携させている場合、一方に関する情報の変更と共に他方に関する情報も書き換える必要がある。このように、暗号処理に使用される複数の情報を共に更新する場合に、更新処理が中断しても必要な情報を回復することができる技術が要求される。

【課題を解決するための手段】
【０００９】
本発明の一態様にかかる暗号化したユーザ・データを記憶するデータ記憶装置は、プライマリ第１データと、プライマリ第２データと、前記プライマリ第１データのコピーであるバックアップ第１データと、前記プライマリ第２データのコピーであるバックアップ第２データと、をそれぞれ不揮発性メモリ領域の異なるアドレスに格納する不揮発メモリ領域と、前記プライマリ第１データと前記プライマリ第２データとを用いてユーザ・データの暗号処理を実行する暗号処理部と、前記プライマリ第１データと前記バックアップ第１データの一方を無効状態に設定し、前記無効状態に設定した第１データと同じ種類の第２データを更新し、前記同じ種類の第２データを更新した後に前記無効状態に設定した第１データを更新し、前記無効状態に設定した第１データを更新した後に、前記無効状態に設定した第１データと異なる種類の第１データ及び第２データを更新する、更新処理部とを有する。第１及び第２データを二重化して上記更新処理を行うことで、第１及び第２データをより安全に更新することができる。
【００１０】
前記無効状態に設定した第１データは、前記バックアップ第１データであることが好ましい。これによって、更新途中で処理が中断した場合に、バックアップ・データがプライマリ・データと異なる状態が続くことを避けることができる。
【００１１】
好ましくは、前記更新処理部は、前記異なる種類の第１データを無効状態に設定した後に前記異なる種類の第２データを更新し、前記異なる種類の第２データを更新した後に前記異なる種類の第１データを更新する。これによって、第１及び第２データをより安全に更新することができる。
【００１２】
前記更新処理部は、前記プライマリ第１データが無効状態である場合に前記バックアップ第１データをコピーし、前記バックアップ第１データが無効状態である場合に前記プライマリ第１データをコピーする。これによって、更新が中断した場合に第１及び第２データの回復を行うことができる。
【００１３】
好ましくは、前記更新処理部は、前記プライマリ第１データと前記バックアップ第１データの一方を無効状態に設定する前に、フラグを更新中状態に設定し、前記異なる種類の第１データ及び第２データを更新した後に前記フラグを更新完了状態に設定する。フラグを使用することで、更新中断の事実を迅速に知ることができる。前記フラグは、前記異なる種類の第１データ及び第２データの内の後に更新されるデータと同一のアドレスに格納されていることが好ましい。これによって、処理工程を少なくすることができる。
【００１４】
前記プライマリ第１データ、前記プライマリ第２データ、前記バックアップ第１データ、前記バックアップ第２データのそれぞれは、格納されているアドレス領域内においてランダム・データ内にあることが好ましい。さらに、前記プライマリ第１データ、前記プライマリ第２データ、前記バックアップ第１データ、前記バックアップ第２データの少なくとも一つは、複数のアドレス領域に分割して格納されていることが好ましい。これらによって、これらのデータへのアクセスをより難しいものとすることができる。
【００１５】
本発明の他の態様は、対象データの暗号処理に用いる複数のデータを更新する方法である。この方法は、プライマリ第１データと、プライマリ第２データと、前記プライマリ第１データのコピーであるバックアップ第１データと、前記プライマリ第２データのコピーであるバックアップ第２データと、をそれぞれ不揮発性メモリ領域の異なるアドレスに格納する。前記プライマリ第１データと前記プライマリ第２データとを用いて暗号処理を実行する。前記プライマリ第１データと前記バックアップ第１データの一方を無効状態に設定する。前記無効状態に設定した第１データと同じ種類の第２データを更新する。前記同

じ種類の第２データを更新した後に前記無効状態に設定した第１データを更新する。前記無効状態に設定した第１データを更新した後に、前記無効状態に設定した第１データと異なる種類の第１データ及び第２データを更新する。第１及び第２データを二重化して上記更新処理を行うことで、第１及び第２データをより安全に更新することができる。

【発明の効果】

【００１６】

本発明によれは、暗号処理に使用される複数のデータをより安全に更新することができる。

【発明を実施するための最良の形態】

【００１７】

以下に、本発明を適用可能な実施の形態を説明する。説明の明確化のため、以下の記載及び図面は、適宜、省略及び簡略化がなされている。又、各図面において、同一要素には同一の符号が付されており、説明の明確化のため、必要に応じて重複説明は省略されている。以下においては、データ記憶装置の一例であるハードディスク・ドライブ（ＨＤＤ）を例として、本発明の実施形態を説明する。本形態は、磁気ディスク上のデータの暗号処理に使用する情報の更新処理にその特徴を有している。

【００１８】

まず、図１を参照してＨＤＤの全体構成を説明する。ＨＤＤ１は、エンクロージャ１０の外側に固定された回路基板２０を有している。回路基板２０上に、リード・ライト・チャネル（ＲＷチャネル）２１、モータ・ドライバ・ユニット２２、ロジック回路であるハードディスク・コントローラ（ＨＤＣ）とＭＰＵの集積回路（ＨＤＣ／ＭＰＵ）２３及びＲＡＭ２４などの各回路が実装されている。

【００１９】

エンクロージャ１０内において、スピンドル・モータ（ＳＰＭ）１４は所定の角速度で磁気ディスク１１を回転する。磁気ディスク１１は、データを記憶する不揮発性メモリである。ＨＤＣ／ＭＰＵ２３からの制御データに従って、モータ・ドライバ・ユニット２２がＳＰＭ１４を駆動する。各ヘッド・スライダ１２は、磁気ディスク上を浮上するスライダと、スライダに固定されデータの読み書きを行うヘッド素子部とを備えている。各ヘッド・スライダ１２はアクチュエータ１６の先端部に固定されている。アクチュエータ１６はボイス・コイル・モータ（ＶＣＭ）１５に連結され、回動軸を中心に回動することによって、ヘッド・スライダ１２を回転する磁気ディスク１１上においてその半径方向に移動する。

【００２０】

モータ・ドライバ・ユニット２２は、ＨＤＣ／ＭＰＵ２３からの制御データに従ってＶＣＭ１５を駆動する。アーム電子回路（ＡＥ：Arm Electronics）１３は、ＨＤＣ／ＭＰＵ２３からの制御データに従って複数のヘッド素子部１２の中から磁気ディスク１１にアクセス（リードもしくはライト）するヘッド・スライダ１２を選択し、リード／ライト信号の増幅を行う。ＲＷチャネル２１は、リード処理において、ＡＥ１３から供給されたリード信号を一定の振幅となるように増幅し、その後、取得したリード信号からデータを抽出し、デコード処理を行う。デコード処理されたデータは、ＨＤＣ／ＭＰＵ２３に供給される。また、ＲＷチャネル２１は、ライト処理において、ＨＤＣ／ＭＰＵ２３から供給されたライト・データをコード変調し、さらに、コード変調されたデータをライト信号に変換してＡＥ１３に供給する。

【００２１】

コントローラの一例であるＨＤＣ／ＭＰＵ２３において、ＭＰＵはＲＡＭ２４にロードされたファーム・ウェアに従って動作する。ＨＤＣ／ＭＰＵ２３は、リード／ライト処理制御、コマンド実行順序の管理、サーボ信号を使用したヘッド・ポジショニング制御（サーボ制御）、ホスト５１との間のインターフェース制御、ディフェクト管理、エラー対応処理など、データ処理に関する必要な処理及びＨＤＤ１の全体制御を実行する。

【００２２】

本形態のＨＤＣ／ＭＰＵ２３は、磁気ディスク１１に記録されるユーザ・データの暗号処理を実行する。図２は、この暗号処理に関連する構成要素を模式的に示すブロック図である。ＨＤＣ／ＭＰＵ２３は、ホスト・インターフェース２３１、ＥＣＣ処理部２３２、メモリ・マネージャ２３３、暗号処理部２３４を有している。これらは、論理回路で構成されている。また、ＨＤＣ／ＭＰＵ２３は、ファーム・ウェアに従って動作するＭＰＵ２３５を有している。

【００２３】

ホスト・インターフェース２３１は、外部ホスト５１とのデータ通信におけるインターフェースである。ＥＣＣ処理部２３２は、磁気ディスク１１の記録データの誤り検出及び誤り訂正処理を行う。メモリ・マネージャ２３３は、データ・フローの制御やメモリ・バスのアクセス制御等を実施する。暗号処理部２３４は、磁気ディスク１１のユーザ・データの暗号化及び復号化を行う。ＲＡＭ２４に形成されたデータ・バッファ２４１は、ライト・データ及びリード・データを一時的に格納する。

【００２４】

ライト処理において、ホスト５１からのライト・データは、ホスト・インターフェース２３１を介して、暗号処理部２３４に転送される。暗号処理部２３４は、ライト・データを暗号化して、メモリ・マネージャ２３３送る。メモリ・マネージャ２３３は、暗号化されたライト・データをデータ・バッファ２４１に格納する。メモリ・マネージャ２３３は、その後、データ・バッファ２４１からライト・データを取得して、ＥＣＣ処理部２３２に送る。ＥＣＣ処理部２３２は、誤り訂正のために必要な処理をライト・データに行い、ＲＷチャネル２１に送る。

【００２５】

リード処理において、ＥＣＣ処理部２３２は、ＲＷチャネル２１から転送された磁気ディスク１１からのリード・データの誤り訂正処理を行う。その後、リード・データは、メモリ・マネージャ２３３を介して、データ・バッファ２４１に格納される。メモリ・マネージャ２３３は、データ・バッファ２４１からリード・データを取得して暗号処理部２３４に送る。暗号処理部２３４は、リード・データの復号化処理を行う。復号化されたリード・データは、ホスト・インターフェース２３１を介して、ホスト５１に転送される。

【００２６】

図２に示すように、データの暗復号を実施する暗号処理部２３４は、ホスト・インターフェース２３１とメモリ・マネージャ２３３との間に位置する。従って、ＨＤＤ１のホスト・インターフェース２３１を除く他の部分において、ＨＤＤ１は、ユーザ・データを暗号化した状態で取り扱うことが出来る。つまり、ＨＤＤ１の動作中において、データ・バッファ２４１内のユーザ・データも、暗号化により保護されている。暗号処理部２３４がユーザ・データの暗号化及び復号化に使用するデータ用暗号鍵は、磁気ディスク１１に格納されているデータを基に、ＭＰＵ２３５によって再現（復号化）され、暗号処理部２３４に供給される。暗号処理部２３４が使用する暗号方法は、ＡＥＳ（Advanced Encryption Standard）のような共通鍵暗号方式（秘密鍵暗号方式）とする。なお、本発明は、他の暗号方式に適用することもできる。

【００２７】

図３のブロック図を参照して、ＨＤＤ１の認証処理及びユーザ・データの暗号処理について説明する。ＨＤＤ１は、データ用暗号鍵ＤＫｅｙを暗号化して磁気ディスク１１に保存する。ＨＤＤ１は、認証用パスワードＰＷと乱数ＲＳｘを使用して鍵用暗号鍵ＥＫｅｙを生成し、それを使用してデータ用暗号鍵ＤＫｅｙを暗号化する。この暗号化されたデータ用暗号鍵を、Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝と表す。つまり、Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝は、データ用暗号鍵ＤＫｅｙを鍵用暗号鍵Ｅｋｅｙで暗号化していることを表す。磁気ディスク１１には、認証用パスワードＰＷ、乱数ＲＳｘ、そして暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝が保存されている。

【００２８】

以下において、認証処理及びユーザ・データの暗号処理の流れを説明する。認証処理及

びユーザ・データの暗号処理において、ＭＰＵ２３５は、認証処理部３５１、ハッシュ関数３５２、排他的論理和演算子３５３、そして鍵復号部３５４として機能する。ＭＰＵ２３５がホスト５１から認証用パスワードＰＷを取得すると、認証処理部３５１が磁気ディスク１１から認証用パスワードＰＷを取得し、認証処理を実行する。

【００２９】

認証処理に成功すると、ハッシュ関数３５２がホスト５１からの認証用パスワードＰＷのハッシュ値Ｈ（ｐｗ）を算出する。ＭＰＵ２３５は、磁気ディスク１１から乱数Ｒｘを取得し、排他的論理和演算子３５３が、ハッシュ値Ｈ（ｐｗ）と乱数Ｒｘの排他的論理和を算出する。この排他的論理和は、鍵用暗号鍵ＥＫｅｙである。ＭＰＵ２３５は、磁気ディスク１１から暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を取得する。鍵復号部３５４は、鍵用暗号鍵ＥＫｅｙを使用して暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を復号化し、データ用暗号鍵ＤＫｅｙを得る。暗号処理部２３４は、データ用暗号鍵ＤＫｅｙを使用してユーザ・データの暗号処理（暗号化あるいは復号化）を実行する。

【００３０】

データ用暗号鍵ＤＫｅｙは、磁気ディスク１１のデータの暗号処理に使用されるため、徒に変更することができない。しかし、この暗号鍵管理方法は、データ用暗号鍵ＤＫｅｙを暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝として安全に保持しつつ、認証用パスワードＰＷの変更が可能である。また、認証用パスワードＰＷの変更により、データ用暗号鍵ＥＫｅｙ及び暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝が変化するので、データ用暗号鍵Ｄｋｅｙの管理をよりセキュアに実施することができる。

【００３１】

同様に、必要に応じて乱数データＲＳｘを定期的に更新することにより、データ用暗号鍵ＥＫｅｙ及び暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を定期的に更新できる。このように、磁気ディスク１１上の暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝が変化するため、データ用暗号鍵Ｄｋｅｙの管理をよりセキュアに実施することができる。

【００３２】

以下において、本形態の認証用パスワードＰＷの更新処理について説明する。上述のように、本形態のＨＤＤ１は、認証用パスワードＰＷを使用して鍵用暗号鍵ＥＫｅｙを生成し、その鍵用暗号鍵ＥＫｅｙで暗号化したデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を保存する。従って、ＨＤＤ１は、認証用パスワードＰＷの更新において、磁気ディスク１１上の認証用パスワードＰＷを書き換えると共に、暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を書き換えることが必要となる。

【００３３】

以下の説明において、認証用パスワードＰＷと暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝とは、異なるデータ・セクタに記録されている。データ・セクタは、磁気ディスク１１上のユーザ・データの記録単位であり、各データ・セクタには異なるアドレスが割り当てられている。磁気ディスク１１上のパスワードＰＷ自体が認証用パスワードに関する情報であり、暗号化したデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝がデータ用暗号鍵に関する情報である。

【００３４】

本形態において、ＰＷとＥ｛ＥＫｅｙ、ＤＫｅｙ｝とは、磁気ディスク１１上において二重化されて、記録、保持されている。一方はプライマリ・データであり、他方はバックアップ・データである。以下において、各データを、プライマリ・パスワード、プライマリ鍵情報、バックアップ・パスワード、バックアップ鍵情報と呼ぶ。４つのデータ・セクタのそれぞれが、プライマリ・パスワード、プライマリ鍵情報、バックアップ・パスワード、バックアップ鍵情報を保持している。ＭＰＵ２３５は、認証処理及びユーザ・データの暗号処理において、プライマリ・データを使用する。バックアップ・データは、更新処理を安全に行うためのデータである。

【００３５】
図４及び図５は、認証用パスワードＰＷ及び暗号化したデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を書き換える処理の流れを示す図である。図５のテーブルにおけるＳＴＥＰ１１～ＳＴＥＰ１７が、図４の各工程Ｓ１１～Ｓ１７に対応している。図５のＳＴＥＰ１０は、各データ・セクタの書き換えを開始する前の状態を示している。各レコード（行）における各エントリ（ボックス）は、一つのデータ・セクタに対応する。プライマリ鍵情報を格納しているデータ・セクタは、更新フラグも格納している。この更新フラグは、更新処理の完了と中断とを示す。
【００３６】
ホスト５１から入力されたパスワードを取得すると（Ｓ１０）、ＭＰＵ２５はプライマリ鍵情報を格納しているデータ・セクタ内のフラグを更新中の状態にセットする（Ｓ１１、ＳＴＥＰ１１）。ＭＰＵ２５はプライマリ鍵情報を変更せずに、フラグだけを完了から更新中に変更する。次に、ＭＰＵ２５は、バックアップ鍵情報を無効にセットする（Ｓ１２、ＳＴＥＰ１２）。例えば、ＭＰＵ２５は、バックアップ鍵情報を格納しているデータ・セクタを予め設定されたデータで上書きする（書きつぶす）。
【００３７】
この他、ＭＰＵ２５は、鍵情報のIntegrity check用のコード（例えばＣＲＣコード）を不正なものに変更する、あるいは、バックアップ鍵情報を格納しているデータ・セクタが、バックアップ鍵情報の有効／無効を示すフラグを格納していてもよい。ＭＰＵ２５は、予め決められた方法により、鍵情報が無効であることを表すように書き直す。バックアップ鍵情報が無効であるということは、バックアップ側のデータが更新途中にあることを示している。なお、バックアップ鍵情報セクタと異なるセクタにバックアップ鍵情報の有効／無効を示すフラグを格納することもできるが、データ処理速度の点からは同一のデータ・セクタ内に格納することが好ましい。
【００３８】
続いて、ＭＰＵ２５は、バックアップ・パスワードを新しいパスワードに書き換える（Ｓ１３、ＳＴＥＰ１３）。ＭＰＵ２５は、ＨＤＣ／ＭＰＵ２３内のハードウェアやＲＷチャネル２１を制御して、バックアップ・パスワードを格納しているデータ・セクタに新しいバックアップ・パスワードを書き込む。ＭＰＵ２５は、好ましくは、書き込んだバックアップ・パスワードのベリファイ処理も行う。これによって、バックアップ・パスワードをより安全に更新することができる。
【００３９】
次に、ＭＰＵ２５は、バックアップ鍵情報を新しい鍵情報に書き換える（Ｓ１４、ＳＴＥＰ１４）。ＭＰＵ２５は、好ましくは、書き込んだバックアップ鍵情報のベリファイ処理も行う。具体的には、ＭＰＵ２５は書き込んだバックアップ鍵情報を読み出して、正しく書き込まれたかを照合する。これによって、バックアップ鍵情報をより安全に更新することができる。
【００４０】
続いて、ＭＰＵ２５は、プライマリ鍵情報を無効にセットする（Ｓ１５、ＳＴＥＰ１５）。無効にする方法は、バックアップ鍵情報と同様である。ＭＰＵ２５は、プライマリ鍵情報を無効にセットするのみで、プライマリ鍵情報内のセクタを、更新中状態に維持する。次に、ＭＰＵ２５は、プライマリ・パスワードを新しいパスワードに書き換える（Ｓ１６、ＳＴＥＰ１６）。ＭＰＵ２５は、好ましくは、書き込んだプライマリ・パスワードのベリファイ処理も行う。最後に、ＭＰＵ２５は、プライマリ鍵情報を新しい鍵情報に書き換えると共に、更新フラグを完了に書き換える。ＭＰＵ２５は、好ましくは、書き込んだプライマリ鍵情報とフラグのベリファイ処理も行う（Ｓ１７、ＳＴＥＰ１７）。これらの一連の手続きにより、パスワードの更新と共にパスワードから生成される鍵情報を安全に更新することが出来る。
【００４１】
次に、パスワード及び鍵情報の利用方法を、図６のフローチャートを参照して説明する

。認証のためのパスワードＰＷがホスト５１から入力されと（Ｓ２１）、ＭＰＵ２５は、プライマリ鍵情報（データ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝）とプライマリ・パスワードのデータ・セクタを読み出す（Ｓ２２）。ＭＰＵ２５は、プライマリ鍵情報セクタのフラグの状態を確認する（Ｓ２３）。フラグが完了の状態にある場合（Ｓ２３におけるＹ）、ＭＰＵ２５は、先に入力された認証のためのパスワードＰＷで認証処理を実施する（Ｓ２４）。

【００４２】

認証が成功すれば（Ｓ２５におけるＹ）、ＭＰＵ２５は磁気ディスク１１から乱数Ｒｘを読み出し、その乱数Ｒｘと取得したＰＷとから鍵用暗号鍵ＥＫｅｙを生成する。さらに、ＭＰＵ２５は、プライマリ鍵情報である暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を、鍵用暗号鍵ＥＫｅｙを使用して復号化し、データ用暗号鍵ＤＫｅｙを取得する。ＭＰＵ２５は、そのデータ用暗号鍵ＤＫｅｙを暗号処理部２３４に設定する（Ｓ２６）。認証が失敗すれば（Ｓ２５におけるＮ）、ＭＰＵ２５は、パスワード認証のエラー処理をする（Ｓ２７）。この場合、データ用暗号鍵ＤＫｅｙは再現されない。

【００４３】

Ｓ２３においてプライマリ鍵情報セクタのフラグが完了以外の状態にあるとき、つまり、フラグが更新中の状態にあるか、プライマリ鍵情報セクタの再生でハード・エラーが発生するような場合、ＭＰＵ２５は、プライマリ・パスワード・セクタとプライマリ鍵情報セクタの再生状況を確認する（Ｓ２８）。いずれのデータ・セクタにおいてもハード・エラーの発生がなく、プライマリ鍵情報セクタの鍵情報の内容が「つぶされていない」（記録されている鍵情報が有効である）ならば、情報は正しく再生されている（Ｓ２８におけるＹ）。

【００４４】

このように情報が正しく再生されている場合（Ｓ２８におけるＹ）、前回のパスワードの更新が図５におけるＳＴＥＰ１２～ＳＴＥＰ１４（図４におけるＳ１２～Ｓ１４）の処理中に中断したと判定することができる。従って、ＭＰＵ２５は、プライマリ鍵情報セクタ及びプライマリ・パスワード・セクタの内容を、バックアップのデータ・セクタにそれぞれ書き込む。このとき、ＭＰＵ２５は、図５のＳＴＥＰ１２～ＳＴＥＰ１４（図４のＳ１２～Ｓ１４）の手順によって書き込むことで（Ｓ２９）、全てのプライマリ・データ・セクタとバックアップ・データ・セクタとを、更新処理の中断前の状態に戻すことができる。さらに、ＭＰＵ２５は、プライマリ鍵情報セクタのフラグを完了状態に書き換えることで（Ｓ３０）、図５のＳＴＥＰ１０まで戻ることができる。このフラグの書き換えは。図５のＳＴＥＰ１７（図４におけるＳ１４）の手順を踏むことと等価である。

【００４５】

ＭＰＵ２５は、引き続き、入力されたパスワードＰＷで認証処理を実施する（Ｓ２４）。入力されたパスワードＰＷが更新後のもの、あるいは、誤ったものであれば、パスワード認証処理はエラーとなる（Ｓ２５におけるＮ）。また、更新前のパスワードが正しく入力されていれば、パスワードの認証処理が正常に実施される（Ｓ２５におけるＹ）。認証が成功すれば（Ｓ２５におけるＹ）、ＭＰＵ２５は、プライマリ鍵情報セクタからの暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝とパスワードＰＷとから、データ用暗号鍵ＤＫｅｙを再現させ、暗号処理部２３４に設定する（Ｓ２６）。

【００４６】

プライマリ鍵情報セクタのフラグの状態が完了以外であり（Ｓ２３におけるＮ）、さらに、プライマリ鍵情報セクタとプライマリ・パスワード・セクタのデータ再生の何れかでハード・エラーが生じるような場合、または、プライマリ鍵情報セクタの鍵情報の内容が「つぶされている」（書かれている鍵情報が無効の状態になっている）場合（Ｓ２８におけるＮ）、前回のパスワードの更新が図５のＳＴＥＰ１５～ＳＴＥＰ１６（図４におけるＳ１５～Ｓ１６）の処理中に中断したと判定できる。

【００４７】

Ｓ２８がＮの場合、ＭＰＵ２５は、バックアップ鍵情報セクタとバックアップ・パスワ

ード・セクタとを読み出す（Ｓ３１）。そして、読み出したバックアップ鍵情報セクタとバックアップ・パスワード・セクタの内容をそれぞれのプライマリ・データ・セクタに書き込む（Ｓ３２）。このとき、ＭＰＵ２５は、図５のＳＴＥＰ１５～１７の手順によって書き込むことで、更新処理で中断された状態を更新することが出来る。その後、ＭＰＵ２５はバックアップ鍵情報セクタとバックアップ・パスワード・セクタの情報（プライマリ・データ・セクタに書き込んだ情報）を使用して（Ｓ３３）、認証処理（Ｓ２４）以降の処理を実施する。

【００４８】

以上の処理において、パスワードの更新が正常に実施されている時には、プライマリ鍵情報セクタのフラグを確認することでプライマリ側のパスワードと鍵情報を再生すればよいので、正常時の処理時間を短縮できる。つまり、ＭＰＵ２５は、認証処理やデータ用暗号鍵の復号において、プライマリ・データ・セクタを参照する。プライマリ鍵情報セクタのフラグが有効を示している場合、ＭＰＵ２５はプライマリ側のパスワードと鍵情報を再生する。これらが正常に再生されれば、ＭＰＵ２５はバックアップを参照することなく処理を進めることができる。また、フラグがプライマリ・データ・セクタ内に格納されているので、他のデータ・セクタのアクセスする必要がなく処理を高速化することができる。

【００４９】

先のパスワード更新が中断（異常終了）していた場合も、ＭＰＵ２５は、その中断の状況により、パスワードの更新前あるいは更新後の状態に正しく復帰することができる。つまり、ＭＰＵ２５は、プライマリ鍵情報セクタのフラグを参照することで、更新中断を迅速に知ることができる。また、プライマリ・データ・セクタ及びバックアップ・データ・セクタのそれぞれにおいて、最後に更新するデータ・セクタ（上記処理において鍵情報セクタ）が無効状態にセットされているので、更新処理のいずれの段階で中断されたかを判定することができる。

【００５０】

ここで、上述の処理は、図５のＳＴＥＰ１４の後でありＳＴＥＰ１５に前に中断した場合、プライマリ側のデータをバックアップ側に書き込んでいる。上述の処理は、プライマリ側のデータの有効／無効によって、いずれのデータを使用するかを判定している。これによって、判定処理を迅速に行うことができる。しかし、更新されてデータを使用することが好ましい場合は、ＭＰＵ２５はバックアップ側のデータをプライマリ側に書き込む。この場合、ＭＰＵ２５は、プライマリ側のデータの後にバックアップ側のデータの状態を確認する。双方のデータが有効状態である場合、ＭＰＵ２５は、正常に更新されているバックアップ側のデータをプライマリ側に書き込む。

【００５１】

更新状態を示すフラグは、上述のように、最後に書き換えられるデータ・セクタ（プライマリ鍵情報セクタ）に格納しておくことが好ましい。これによって、最後のデータ・セクタの書き換え時にフラグも変更することができ、処理時間を短縮することができる。処理時間を考慮せずともよい場合、フラグを他のデータ・セクタに格納することも可能である。また、上記処理は、バックアップ・データ・セクタから更新を行うが、プライマリ・データ・セクタから更新を行ってもよい。あるいは、パスワード・セクタではなく、鍵情報セクタから更新を行ってもよい。この場合、ＭＰＵ２５はパスワード・セクタを無効にセットしてから、鍵情報セクタを更新する。

【００５２】

他の好ましい実施形態を、図７～図９を参照して説明する。上記処理と異なり、この更新処理は、プライマリ・データ・セクタ内の更新状態を示すフラグを使用しない。図７は、パスワード、鍵情報の他の好ましい更新方法を示すフローチャートである。このフローチャートは、図４におけるＳ１１が存在しないものに相当する。図８は、図７の処理を実行した際のプライマリとバックアップの各パスワード・セクタと鍵情報セクタの状態の変遷を示している。図８は、上記他の形態の図５からフラグを省略したものに相当する。

【００５３】

更新のためのパスワードＰＷがホスト５１から入力されると（Ｓ４０）、ＭＰＵ２５は、バックアップ鍵情報を無効にセットする（Ｓ４１、ＳＴＥＰ４１）。例えば、ＭＰＵ２５は、バックアップ鍵情報を格納しているデータ・セクタを予め設定されたデータで上書きする（書きつぶす）。この工程は、図４のＳ１２と同様である。

【００５４】

続いて、ＭＰＵ２５は、バックアップ・パスワードを新しいパスワードに書き換える（Ｓ４２、ＳＴＥＰ４２）。ＭＰＵ２５は、好ましくは、書き込んだバックアップ・パスワードのベリファイ処理も行う。これによって、バックアップ・パスワードをより安全に更新することができる。

【００５５】

次に、ＭＰＵ２５は、バックアップ鍵情報を新しい鍵情報に書き換える（Ｓ４３、ＳＴＥＰ４３）。ＭＰＵ２５は、好ましくは、書き込んだバックアップ鍵情報のベリファイ処理も行う。具体的には、ＭＰＵ２５は書き込んだバックアップ鍵情報を読み出して、正しく書き込まれたかを照合する。これによって、バックアップ鍵情報をより安全に更新することができる。

【００５６】

続いて、ＭＰＵ２５は、プライマリ鍵情報を無効にセットする（Ｓ４４、ＳＴＥＰ４４）。無効にする方法は、バックアップ鍵情報と同様である。ＭＰＵ２５は、プライマリ鍵情報を無効にセットするのみで、プライマリ鍵情報内のセクタを、更新中状態に維持する。次に、ＭＰＵ２５は、プライマリ・パスワードを新しいパスワードに書き換える（Ｓ４５、ＳＴＥＰ４５）。ＭＰＵ２５は、好ましくは、書き込んだプライマリ・パスワードのベリファイ処理も行う。最後に、ＭＰＵ２５は、プライマリ鍵情報を新しい鍵情報に書き換える。ＭＰＵ２５は、好ましくは、書き込んだプライマリ鍵情報とフラグのベリファイ処理も行う（Ｓ４６、ＳＴＥＰ４６）。これらの一連の手続きにより、パスワードの更新と共にパスワードから生成される鍵情報を安全に更新することが出来る。

【００５７】

次に、パスワード及び鍵情報の利用方法を、図９のフローチャートを参照して説明する。認証のためのパスワードＰＷがホスト５１から入力されと（Ｓ５１）、ＭＰＵ２５は、プライマリ鍵情報、プライマリ・パスワード、バックアップ鍵情報そしてバックアップ・パスワードのデータ・セクタを読み出す（Ｓ５２）。ＭＰＵ２５は、プライマリ鍵情報とバックアップ鍵情報とを比較し、それらが一致するか判定する（Ｓ５３）。それらが一致する場合（Ｓ５３におけるＹ）、ＭＰＵ２５は、プライマリ鍵情報とプライマリ・パスワードとを使用する（Ｓ５４）。ＭＰＵ２５は、プライマリ・パスワードで認証処理を実施する（Ｓ５５）。

【００５８】

認証が成功すれば（Ｓ５６におけるＹ）、ＭＰＵ２５は、磁気ディスク１１上の乱数Ｒｘとプライマリ・パスワードとから鍵用暗号鍵ＥＫｅｙを生成し、プライマリ鍵情報である暗号化されたデータ用暗号鍵Ｅ｛ＥＫｅｙ、ＤＫｅｙ｝を復号する。さらに、ＭＰＵ２５は、再現したデータ用暗号鍵ＤＫｅｙを暗号処理部２３４に設定する（Ｓ５７）。認証が失敗すれば（Ｓ５６におけるＮ）、ＭＰＵ２５は、パスワード認証のエラー処理をする（Ｓ５８）。データ用暗号鍵ＤＫｅｙは再現されない。

【００５９】

プライマリ鍵情報とバックアップ鍵情報とが一致しない場合（Ｓ５３におけるＮ）、前回のパスワード更新による鍵更新は途中で中断していると判定できる。そこで、ＭＰＵ２５は、プライマリ・パスワード・セクタとプライマリ鍵情報セクタの再生状況を確認する（Ｓ５９）。つまり、いずれのデータ・セクタのデータ再生でもハード・エラーの発生がなく、プライマリ鍵情報セクタの鍵情報の内容が「つぶされていない」（書かれている鍵情報が有効であることが確認できる）なら（Ｓ５９におけるＹ）、前回のパスワードの更新が図８のＳＴＥＰ４１～ＳＴＥＰ４３の処理中に中断したと判定できる。ＭＰＵ２５は、プライマリ鍵情報セクタ及びプライマリ・パスワード・セクタの内容を、バックアップ

鍵情報セクタ及びバックアップ・パスワード・セクタのそれぞれ書き込む（Ｓ６０）。このとき、図７のＳ４１～４３の手順によって書き込むことで、更新処理の中断前の状態に移行できる。

【００６０】

引き続き、ＭＰＵ２５は、入力されたパスワードＰＷで認証処理を実施する（Ｓ５５）。入力されたパスワードＰＷが更新後のもの、あるいは、誤ったものであれば、パスワード認証処理はエラーとなる（Ｓ５６におけるＮ）。また、更新前のパスワードが正しく入力されていれば、パスワードの認証処理が正常に実施される（Ｓ５６におけるＹ）。ＭＰＵ２５は、データ用暗号鍵ＤＫｅｙを再現し、それを暗号処理部２３４に設定する（Ｓ５７）。

【００６１】

プライマリ・パスワード・セクタとプライマリ鍵情報セクタのデータ再生のいずれかでハード・エラーが生じる場合、または、プライマリ鍵情報セクタの鍵情報の内容が「つぶされている」（書かれている鍵情報が無効の状態になっている）場合（Ｓ５９におけるＮ）、前回のパスワードの更新が図８のＳＴＥＰ４４～ＳＴＥＰ４５の処理中に中断したことが判定できる。

【００６２】

ＭＰＵ２５は、バックアップ・パスワード・セクタとバックアップ鍵情報セクタを読み出す。そして、読み出した、バックアップ・パスワード・セクタとバックアップ鍵情報セクタの内容を、それぞれのプライマリ・データ・セクタに書き込む（Ｓ６１）。このとき、図７のＳ４４～４６の手順によって書き込むことで、更新処理で中断された状態を更新することが出来る。ＭＰＵ２５は、その後、バックアップ・パスワード・セクタとバックアップ鍵情報セクタの情報（プライマリ・データ・セクタに書き込んだ情報）を使用して（Ｓ６２）、パスワードで認証処理（Ｓ５５）以降の工程を実行する。

【００６３】

このように、本処理はプライマリ・データ・セクタとバックアップ・データ・セクタの両方の情報を再生し、それらを比較することによって、状態フラグを使用することなくパスワード更新の中断の状況を把握することができる。これにより、先のパスワード更新が中断（異常終了）していた場合でも、その中断の状況により、パスワードの更新前あるいは更新後の正しい状態を遷移することができる。

【００６４】

好ましくは、上述のように、ＭＰＵ２５は、バックアップ・データ・セクタから更新を行う。プライマリ・データ・セクタから更新を行うと、バックアップ・データ・セクタがプライマリ・データ・セクタと異なる状態が維持されてしまうからである。つまり、ＭＰＵ２５は、通常の処理においてプライマリ・データ・セクタのみを参照する。プライマリ・データ・セクタが正しい場合、バックアップ・データ・セクタは参照されない。そのため、バックアップ・データ・セクタが更新途中の状態にあっても、ＭＰＵ２５は、それを見出すことがない。ＭＰＵ２５が、定期的にプライマリ・データ・セクタとバックアップ・データ・セクタとを比較し、一致させることもできる。しかし、パフォーマンスへの影響を少なくするため、バックアップ・データ・セクタから更新することが好ましい。

【００６５】

上記処理は、図８のＳＴＥＰ１３終了後の中断の場合、プライマリ・データ・セクタをバックアップ・データ・セクタに反映させる。しかし、更新を完了させるためには、ＭＰＵ２５は、バックアップ・データ・セクタをプライマリ・データ・セクタに反映させることが好ましい。また、ＭＰＵ２５は、鍵情報セクタから更新を行い、その次にパスワード・セクタを更新してもよい。この場合、ＭＰＵ２５はパスワード・セクタを無効にセットしてから、鍵情報セクタを更新する。これらの点は、図４～６を参照して説明した上記他の形態と同様である。

【００６６】

以下において、暗号処理に使用するデータを、より安全にデータ・セクタに格納する手

法を説明する。暗号処理に使用するデータを磁気ディスク１１上で見つけにくくすることで、耐性を向上させる（攻撃に対してより多くの労力を必要とさせる）ことができる。本形態のＨＤＤ１は、ランダム・データ内に鍵情報やパスワード情報を書き込む。以下においては、鍵情報を表す鍵データの格納方法の例を説明する。パスワードについても同様に格納することができる。

【００６７】

図１０（ａ）において、１セクタの所定位置に鍵データ１１１が格納されている。鍵データ以外の部分は、ランダムなデータで埋められている。鍵データ１１１は、およそランダムなデータのビット列で構成されるので、データ・セクタ自体がランダム・データで構成されており、セクタ・データだけからは、鍵データ１１１の位置が分からない。セクタ内の位置は、データ・セクタの所定のバイト位置になるようにプログラムすること、データ・セクタの所定位置のビット情報から決めること、あるいはＲＯＭなどの別の不揮発性メモリに格納しておくこと等が可能である。

【００６８】

図１０（ｂ）において、鍵データ格納領域として、複数データ・セクタ使用されている。複数データ・セクタの鍵データ１１１以外の部分は、ランダム・データが格納されている。鍵データ１１１は、データ・セクタ内に配置する、あるいは、データ・セクタ間にまたがって配置しても良い。図１０（ｃ）は、さらに、鍵データ１１１を所定の長さの所定の数のブロック１１１ａ～１１１ｃに分割して、配置する例である。

【００６９】

鍵データの配置位置は、所定のタイミングで変更することが好ましい。例えば、鍵データの更新時に、鍵データの格納位置を変える。あるいは、データ・セクタを埋めるランダム・データを、鍵データの更新時に更新することが好ましい。好ましい他の方法は、ＨＤＤの個体毎に、鍵データの位置を変える。例えば、製造時にＲＯＭへランダムな値を入れて、その値を鍵データの位置情報として、ＨＤＤの個体毎に異なる位置に鍵データを格納するようにする。これらによって、鍵データをより発見しづらくし、より安全に鍵データを保存しておくことができる。

【００７０】

以上、本発明を好ましい実施形態を例として説明したが、本発明が上記の実施形態に限定されるものではない。当業者であれば、上記の実施形態の各要素を、本発明の範囲において容易に変更、追加、変換することが可能である。例えば、本発明を、磁気ディスクと異なる不揮発性メモリを有するデータ記憶装置に適用することができる。あるいは、データを記録あるいは再生のみ行うデータ記憶装置に適用することができる。この場合、暗号処理部は暗号化もしくは復号化のみ行う。

【００７１】

プライマリ・データとバックアップ・データとは、ユーザ・データを格納する不揮発性メモリと異なる不揮発性メモリに格納してもよい。プライマリ・データとバックアップ・データは、それぞれ異なるその不揮発性メモリの異なるアドレスの領域に格納される。また、プライマリ・データとバックアップ・データとを、それぞれ異なる単体の不揮発性メモリに格納することも可能である。

【００７２】

鍵用暗号鍵の生成に使用するパスワードは、認証処理に使用するパスワードと異なるデータでもよい。また、設計によっては、認証処理を省略することができ、パスワード以外データを使用して鍵用暗号鍵を生成することができる。ＨＤＤ１は、パスワードのハッシュ値など、パスワードから生成したデータをパスワードに関する情報として磁気ディスク１１に保存することができる。本発明の更新処理の適用は、パスワード情報や鍵情報に限定されず、また、３以上のデータの更新にも適用することができる。

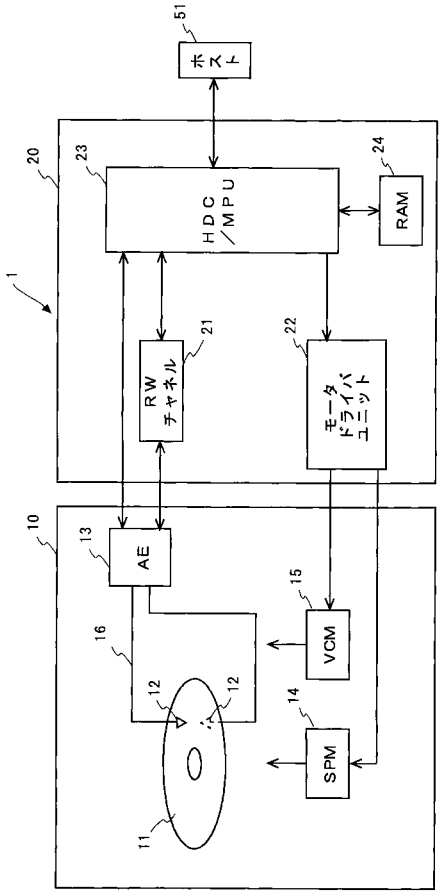
【図面の簡単な説明】

【００７３】

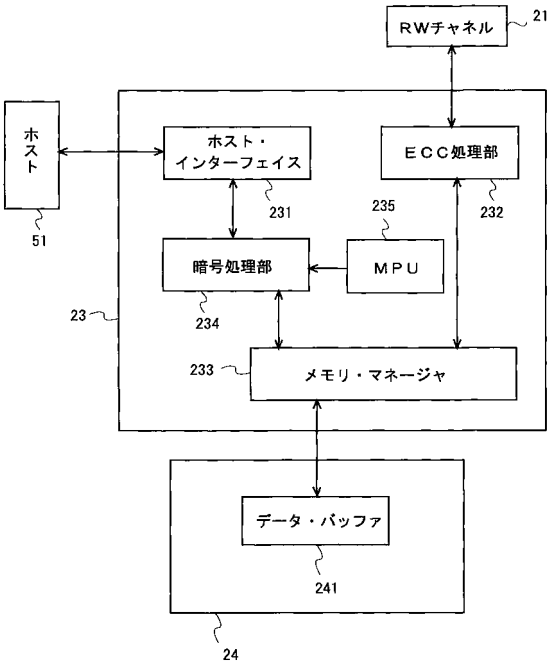
【図１】本実施形態に係るＨＤＤの全体構成を模式的に示すブロック図である。

【図２】本実施形態に暗号処理に関連する構成要素を模式的に示すブロック図である。
【図３】本実施形態ＨＤＤ内で、パスワードが設定されたＨＤＤを利用者が使用する場合の、各工程もしくは各工程を実行する構成要素を示すブロック図である。
【図４】本実施形態のパスワード及び鍵情報を更新する処理の流れを示すフローチャートである。
【図５】本実施形態のパスワード及び鍵情報を更新処理における、パスワードと鍵情報の変化の状態を示すフローチャートである。
【図６】本実施形態の更新処理が中断した場合における、パスワード及び鍵情報の回復方法を示すフローチャートである。
【図７】他の実施形態のパスワード及び鍵情報を更新する処理の流れを示すフローチャートである。
【図８】他の実施形態のパスワード及び鍵情報を更新処理における、パスワードと鍵情報の変化の状態を示すフローチャートである。
【図９】他の実施形態のパスワード及び鍵情報を更新する処理の流れを示すフローチャートである。
【図１０】本実施形態において、パスワード及び鍵情報がデータ・セクタ内に格納されている状態を模式的に示す図である。
【符号の説明】
【００７４】
１　ハード・ディスク・ドライブ、１０　エンクロージャ、１１　磁気ディスク
１２　ヘッド・スライダ、１３　アーム・エレクトロニクス（ＡＥ）、
１４　スピンドル・モータ、１５　ボイス・コイル・モータ、１６　アクチュエータ
２０　回路基板、２１　ＲＷチャネル、２２　モータ・ドライバ・ユニット
２３　ＨＤＣ／ＭＰＵ、２４　ＲＡＭ、５１　ホスト、１１１　鍵情報
２３１　ホスト・インターフェース、２３２　ＥＣＣ処理部
２３３　メモリ・マネージャ、２３４　暗号処理部、２３５　ＭＰＵ
２４１　データ・バッファ、３５１　認証処理部、３５２　ハッシュ関数
３５３　排他的論理和演算子、３５４　鍵復号化部

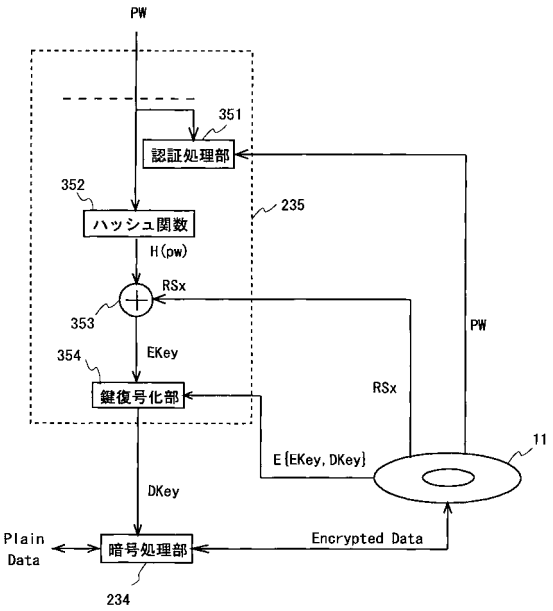
【図１】


ホスト
51
HDC/MPU
20
23
24
RAM
1
RW チャネル
21
22
モータドライバユニット
10
13
AE
15
VCM
16
12
12
14
SPM
11

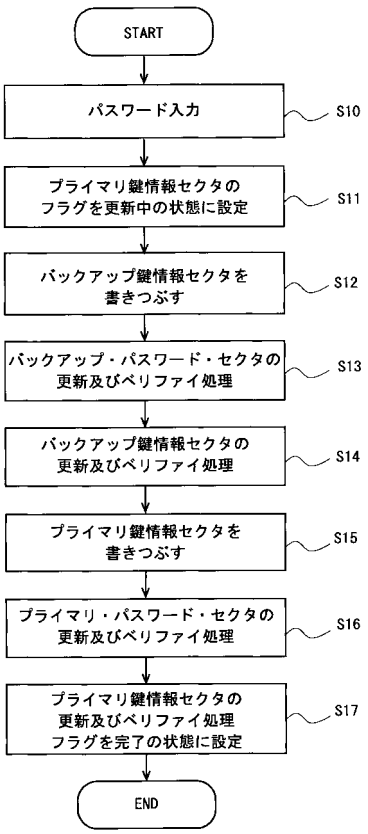
【図２】


RWチャネル
21
ホスト
51
ホスト・インターフェイス
231
ECC処理部
232
235
暗号処理部
234
MPU
23
233
メモリ・マネージャ
データ・バッファ
241
24

【図３】


PW
351
認証処理部
352
ハッシュ関数
235
H(pw)
RSx
353
PW
354
EKey
RSx
鍵復号化部
E{EKey, DKey}
11
DKey
Plain Data
暗号処理部
Encrypted Data
234

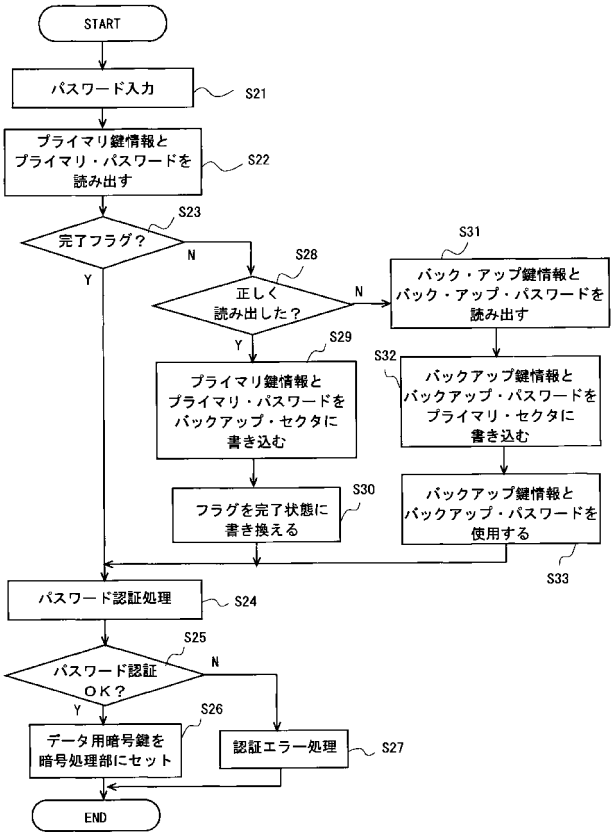
【図４】


START
パスワード入力
S10
プライマリ鍵情報セクタのフラグを更新中の状態に設定
S11
バックアップ鍵情報セクタを書きつぶす
S12
バックアップ・パスワード・セクタの更新及びベリファイ処理
S13
バックアップ鍵情報セクタの更新及びベリファイ処理
S14
プライマリ鍵情報セクタを書きつぶす
S15
プライマリ・パスワード・セクタの更新及びベリファイ処理
S16
プライマリ鍵情報セクタの更新及びベリファイ処理フラグを完了の状態に設定
S17
END

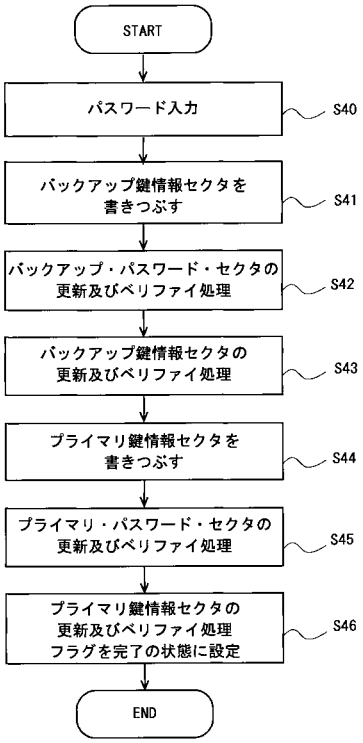
【図５】

STEP	PRIMARY PASSWORD	PRIMARY KEY INFO	BACKUP PASSWORD	BACKUP KEY INFO
10	PREVIOUS	PREVIOUS (COMPLETE FLAG)	PREVIOUS	PREVIOUS
11	PREVIOUS	PREVIOUS **(UPDATING FLAG)**	PREVIOUS	PREVIOUS
12	PREVIOUS	PREVIOUS (UPDATING FLAG)	PREVIOUS	**INVALID**
13	PREVIOUS	PREVIOUS (UPDATING FLAG)	**NEW**	INVALID
14	PREVIOUS	PREVIOUS (UPDATING FLAG)	NEW	**NEW**
15	PREVIOUS	**INVALID (UPDATING FLAG)**	NEW	NEW
16	NEW	INVALID (UPDATING FLAG)	NEW	NEW
17	NEW	**NEW (COMPLETE FLAG)**	NEW	NEW

【図６】



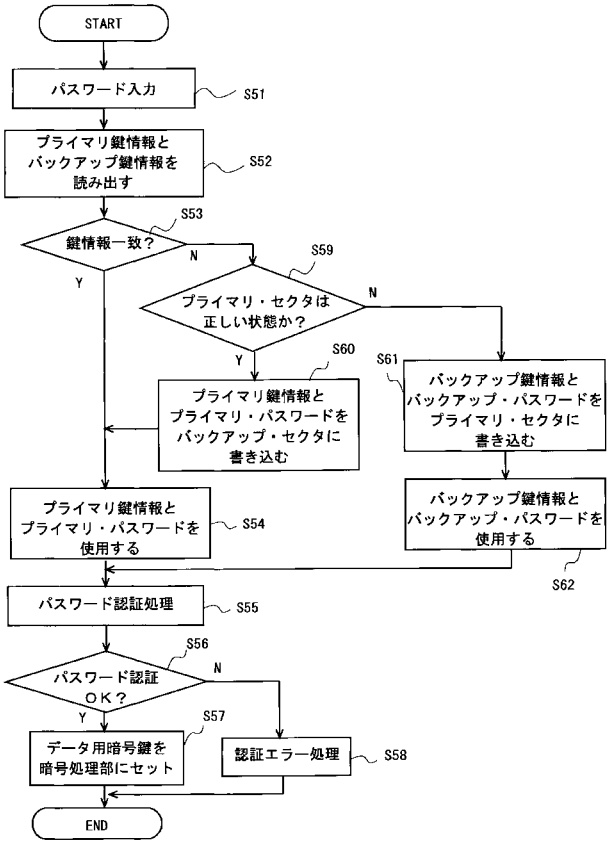
【図７】



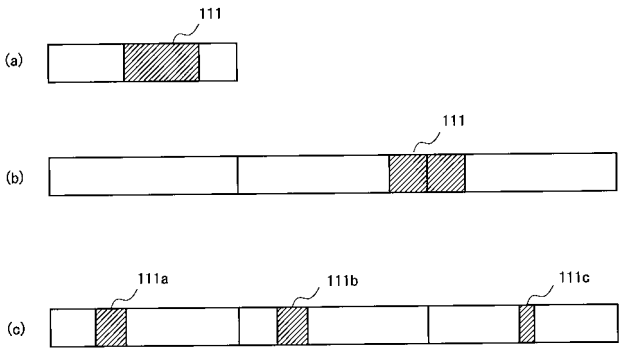
【図８】

STEP	PRIMARY PASSWORD	PRIMARY KEY INFO	BACKUP PASSWORD	BACKUP KEY INFO
40	PREVIOUS	PREVIOUS	PREVIOUS	PREVIOUS
41	PREVIOUS	PREVIOUS	PREVIOUS	**INVALID**
42	PREVIOUS	PREVIOUS	**NEW**	INVALID
43	PREVIOUS	PREVIOUS	NEW	**NEW**
44	PREVIOUS	**INVALID**	NEW	NEW
45	NEW	INVALID	NEW	NEW
46	NEW	**NEW**	NEW	NEW

【図９】


START
パスワード入力
S51
プライマリ鍵情報と
バックアップ鍵情報を
読み出す
S52
S53
鍵情報一致？
N
Y
S59
プライマリ・セクタは
正しい状態か？
N
Y
S60
プライマリ鍵情報と
プライマリ・パスワードを
バックアップ・セクタに
書き込む
S61
バックアップ鍵情報と
バックアップ・パスワードを
プライマリ・セクタに
書き込む
プライマリ鍵情報と
プライマリ・パスワードを
使用する
S54
バックアップ鍵情報と
バックアップ・パスワードを
使用する
S62
パスワード認証処理
S55
S56
パスワード認証
OK？
N
Y
S57
データ用暗号鍵を
暗号処理部にセット
認証エラー処理
S58
END

【図１０】


(a)
111
(b)
111
(c)
111a
111b
111c

フロントページの続き

(72)発明者　横江　祐司
神奈川県小田原市国府津２８８０番地　株式会社日立グローバルストレージテクノロジーズ内
(72)発明者　柿原　俊男
神奈川県小田原市国府津２８８０番地　株式会社日立グローバルストレージテクノロジーズ内

Ｆターム(参考) 5B017 AA04 BA05 BA07 BB09 CA05
5D044 BC01 CC05 DE50 GK17 HL11
5J104 AA12 PA07 PA14