(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5170802号
(P5170802)

(45)発行日　平成25年3月27日(2013.3.27)　(24)登録日　平成25年1月11日(2013.1.11)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/24	165A
G06F 21/80	(2013.01)	G06F	21/02	180A
H04L 9/08	(2006.01)	G06F	21/24	165E
G06F 3/06	(2006.01)	G06F	21/24	166A
G11B 20/10	(2006.01)	H04L	9/00	601A

請求項の数 20　(全 9 頁)　最終頁に続く

(21)出願番号　特願2011-254187(P2011-254187)
(22)出願日　平成23年11月21日(2011.11.21)
(62)分割の表示　特願2008-73333(P2008-73333)の分割
原出願日　平成20年3月21日(2008.3.21)
(65)公開番号　特開2012-59282(P2012-59282A)
(43)公開日　平成24年3月22日(2012.3.22)
審査請求日　平成23年12月14日(2011.12.14)
(31)優先権主張番号　11/728,320
(32)優先日　平成19年3月23日(2007.3.23)
(33)優先権主張国　米国(US)

(73)特許権者　500373758
シーゲイト　テクノロジー　エルエルシー
アメリカ合衆国、９５０１４　カリフォルニア州、クパチーノ、サウス・デ・アンザ・ブールバード、１０２００
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100111246
弁理士　荒川　伸夫

最終頁に続く

(54)【発明の名称】データ記憶装置の制限イレーズおよびアンロック

(57)【特許請求の範囲】
【請求項１】
データ記憶装置であって、
データを格納するように構成されたメモリと、
コントローラとを備え、前記コントローラは、
前記メモリに格納された暗号化データを復号し、
第１のセキュリティコードを受信し、
前記第１のセキュリティコードを第１のセキュリティキーと比較し、
前記第１のセキュリティコードが前記第１のセキュリティキーと一致したときに、前記暗号化データへの第１レベルのアクセスを許可するために、前記データ記憶装置をアンロックするように構成されており、前記第１レベルのアクセスは、第１の動作を実行させ、かつ、前記暗号化データをホストに検索させず、
前記コントローラは、
第２のセキュリティコードを受信し、
前記第２のセキュリティコードを第２のセキュリティキーと比較し、
前記第２のセキュリティコードが前記第２のセキュリティキーと一致したときに、前記暗号化データへの第２レベルのアクセスを許可するために、前記データ記憶装置をアンロックするように構成されており、前記第２レベルのアクセスは、前記暗号化データを前記ホストに検索させる第２の動作を実行させる、データ記憶装置。
【請求項２】

前記第１のセキュリティキーは、前記データ記憶装置に対する製作プロセスデータから発生される、請求項１に記載のデータ記憶装置。
【請求項３】
前記製作プロセスデータは、前記データ記憶装置に示されている、請求項２に記載のデータ記憶装置。
【請求項４】
前記メモリは、ディスクデータ記憶媒体を含む、請求項１に記載のデータ記憶装置。
【請求項５】
前記第１の動作は故障解析動作を含み、前記第２の動作は前記暗号化データに対するデータアクセス動作を含む、請求項１に記載のデータ記憶装置。
【請求項６】
前記第１の動作はイレーズ・コマンドを含み、前記第２の動作は前記暗号化データに対するデータアクセス動作を含む、請求項１に記載のデータ記憶装置。
【請求項７】
前記イレーズ・コマンドは、前記暗号化データの復号を可能にする少なくとも一つの復号キーを削除することを含む、請求項６に記載のデータ記憶装置。
【請求項８】
前記コントローラは、さらに、
前記メモリに格納されるデータを受信し、
前記受信されたデータを暗号化して前記暗号化データを生成し、
前記暗号化データを前記メモリに格納するように構成されている、請求項１に記載のデータ記憶装置。
【請求項９】
前記コントローラは、さらに、
前記第１のセキュリティキーを用いた認証を避けて、前記第２のセキュリティコードが前記第２のセキュリティキーと一致する場合に、前記第２レベルのアクセスをアンロックし、
前記第２レベルのアクセスがアンロックされたときに、前記暗号化データを復号し、
前記第１レベルのアクセスだけがアンロックされたときに、前記暗号化データが復号されないように構成されている、請求項１に記載のデータ記憶装置。
【請求項１０】
前記第１のセキュリティキーおよび前記第２のセキュリティキーは、異なる方法によって生成される、請求項１～９のいずれかに記載のデータ記憶装置。
【請求項１１】
コントローラとメモリとを備えるデータ記憶装置を制御するための方法であって、
前記データ記憶装置に接続されるホストから受信した第１のセキュリティコードが、前記メモリに格納されている第１のセキュリティキーと一致したときに、前記コントローラが、暗号化データへの第１レベルのアクセスを許可するために、前記データ記憶装置をアンロックするステップを備え、前記第１レベルのアクセスは、第１の動作を実行させ、かつ、前記暗号化データを前記ホストに検索させず、
前記ホストから受信した第２のセキュリティコードが前記メモリに格納されている第２のセキュリティキーと一致したときに、前記コントローラが、前記暗号化データへの第２レベルのアクセスを許可するために、前記データ記憶装置をアンロックするステップを備え、前記第２レベルのアクセスは、前記暗号化データを前記ホストに検索させる第２の動作を実行させる、方法。
【請求項１２】
前記コントローラが、データを暗号化して前記暗号化データを生成するステップと、
前記コントローラが、前記暗号化データを前記データ記憶装置に格納するステップとをさらに備える、請求項１１に記載の方法。
【請求項１３】

前記第２のセキュリティコードが前記第２のセキュリティキーと一致する場合に、前記コントローラが、前記第１のセキュリティキーを用いた認証を避けて、前記第２レベルのアクセスをアンロックするステップと、
前記第２レベルのアクセスがアンロックされたときに、前記コントローラが前記暗号化データを復号するステップと、
前記第１レベルのアクセスだけがアンロックされたときに、前記コントローラが、前記暗号化データが復号されないようにするステップとをさらに備える、請求項１２に記載の方法。
【請求項１４】
前記動作は、前記暗号化データの復号を可能にする少なくとも１つの復号キーを消去することをさらに含む、請求項１３に記載の方法。
【請求項１５】
コントローラを備え、
前記コントローラは、
第１のセキュリティコードが第１のセキュリティキーと一致したときに、暗号化データへの第１レベルのアクセスを許可するために、データ記憶装置をアンロックするように構成されており、前記第１レベルのアクセスは、第１の動作が実行されるように許可し、かつ、前記暗号化データをホストに検索させず、
前記コントローラは、
第２のセキュリティコードが第２のセキュリティキーと一致したときに、前記暗号化データへの第２レベルのアクセスを許可するために、前記データ記憶装置をアンロックするように構成されており、前記第２レベルのアクセスは、前記暗号化データを前記ホストに検索させる第２の動作を実行させる、装置。
【請求項１６】
前記コントローラは、さらに、
メモリに格納されるデータを受信し、
前記受信されたデータを暗号化して前記暗号化データを生成し、
前記暗号化データを前記メモリに格納するように構成されている、請求項１５に記載の装置。
【請求項１７】
前記コントローラは、さらに、
前記第２のセキュリティコードが前記第２のセキュリティキーと一致する場合に、前記第１のセキュリティキーを用いた認証を避けて前記第２レベルのアクセスをアンロックし、
前記第２のセキュリティコードが前記第２のセキュリティキーと一致する場合に、前記暗号化されたされたデータを復号するように構成されている、請求項１５に記載の装置。
【請求項１８】
前記第１の動作は故障解析動作を含み、前記第２の動作は前記暗号化データに対するデータアクセス動作を含む、請求項１７に記載の装置。
【請求項１９】
前記第１の動作はイレーズ・コマンドを含み、前記第２の動作は前記暗号化データに対するデータアクセス動作を含む、請求項１７に記載の装置。
【請求項２０】
前記第１の動作および前記第２の動作は、アンロック動作ではない、請求項１７に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
（分野）

本発明は一般的にデータ記憶装置に関する。特に、本発明はデータ記憶装置におけるセキュリティ機能に関連している。

【背景技術】

【０００２】

（背景）

大容量記憶装置は最新のコンピュータの１コンポーネントである。大容量記憶装置の一種がディスク装置である。このようなディスク装置はオペレーティングシステム、アプリケーション、およびユーザデータに関する膨大な量の情報を格納するのに使用される。この情報のいくらかはその中でディスク装置が作動するホストシステムの作用にとって極めて重要である。アプリケーション・ソフトウェアまたは他の重要な情報が故意にまたは意図せずにオーバライトされると、著しい損失を生じることがある。そのため、これらのアプリケーションは精巧なライト保護セキュリティ機能を必要とする。さらに、機密ユーザデータの無許可アクセスを防止する方式も必要である。

【０００３】

多くの場合、ライト保護方式、およびユーザデータの無許可アクセス防止方式は主としてホストコンピュータ内に実現され、ディスク装置はこれらの方式の操作を殆んどまたは全く制御しない。ディスク装置内にこのような方式の制御が欠けていることは機密データの保護の場合特に問題となり、それはディスク装置が盗まれたり元のホストコンピュータから取外されると機密ユーザデータはもはや保護されないためである。さらに、たとえば、ユーザがこのようなディスク装置を故障時にメーカへ返すと、ディスク装置の故障解析を行うことはセキュリティ観点、複雑性およびコストの面で問題となることがある。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

本開示の態様はこれらおよび／または他の問題に対するソリューションを提供し、従来技術に優る他の利点を提供する。

【課題を解決するための手段】

【０００５】

（概要）

ユーザデータへのアクセスが制限されるデータ記憶装置が提供される。データ記憶装置はユーザデータを格納するメモリ場所を有するデータメモリを含んでいる。データ記憶装置はプログラムメモリも有する。プログラムメモリはユーザが第１の装置・セキュリティＩＤを生成して、格納されたデータへのアクセスを制限できるようにする第１のプログラムコードを含んでいる。プログラムメモリ内に含まれる第２のプログラムコードはセキュリティ・コマンドを受信し、受信したセキュリティ・コマンドに関連する第２の装置セキュリティＩＤを格納されたセキュリティ・キーと比較することができる。第２の装置セキュリティＩＤおよび格納されたセキュリティ・キーが対応する場合、第１の装置セキュリティＩＤによる認証はバイパスされて、格納されたデータへのアクセスが提供される。あるデータ記憶装置では、格納されたデータは暗号化形式である。このような態様において、第２の装置セキュリティＩＤおよび格納されたセキュリティ・キーが対応する場合、第２のプログラムコードは非復号化形式でしか格納されたデータへのアクセスを提供しない。これは、暗号化され格納されたユーザデータ内の情報が明らかにされずに、データ記憶装置の故障解析等の操作を実施することができる。

【図面の簡単な説明】

【０００６】

【図１】データ記憶装置を例示する単純化されたブロック図である。

【図２】ディスク装置の等角図である。

【図３】単純化されたフロー図である。

【発明を実施するための形態】

【０００７】

本開示の態様を特徴づけるこれらおよび他の特徴および利点は添付図を参照して以下の説明を読めば明らかである。図１に、ユーザデータへのアクセスが制限されるデータ記憶装置１００の単純化されたブロック図を示す。装置１００は、主要コンポーネントとして、データメモリ１０２、プログラムメモリ１０４および、データメモリ１０２とプログラムメモリ１０４に接続されるコントローラ１０６を含んでいる。コントローラ１０６はホストシステム１０８とデータ記憶装置１００間のホスト記憶装置インターフェイス１１０を介した通信を促進する１つ以上のプロセッサおよび回路を含むことができる。また、コントローラ１０６はホストシステム１０８からコマンドを受信しそれに応答してプログラムメモリ１０４からのプログラムコードを実行することができる。ホストシステム１０８は一連の論理演算を実施することができるパーソナルコンピュータまたは他のシステム（ローカルまたはリモート）等のマイクロプロセッサ・ベースデータ処理システムを含むことができる。

【０００８】

データメモリ１０２は暗号化および／または非暗号化ユーザデータ１１４、暗号化ユーザデータ用暗号化および復号キー１１６、および任意他のタイプの暗号化／非暗号化データ１１８を格納することができる複数のメモリ場所を含んでいる。プログラムメモリ１０４は、そのメモリ場所１２２内に、第１のプログラムコード１２４、第２のプログラムコード１２６、セキュリティ・キー１２８、および任意他のプログラム・モジュール１３１を含んでいる。いくつかの態様において、セキュリティ・キー１２８は、データ記憶装置１００の通し番号および製造日等の製作プロセスデータから装置１００の製作時に発生されてプログラムメモリ１０４内に格納されることができる。それからセキュリティ・キー１２８を発生することができる製作プロセスデータは製作されたセキュリティＩＤをも含むことができ、それも製作時に発生することができるが、セキュリティ・キー１２８とは異なることがある。一まとめにして参照番号１４４で示される装置通し番号、装置の製造日および製作されたセキュリティＩＤは、データ記憶装置１００のハウジング上に含まれる。特定の態様において、情報１４４をデータ記憶装置１００のハウジングに付されるラベルに含むことができる。

【０００９】

本態様において、第１のプログラムコード１２４によりユーザは第１の装置セキュリティＩＤを生成して、格納されたデータ１１４へのアクセスを制限することができる。第１の装置セキュリティＩＤは装置から読み出されることをしないように装置１００内で通常は暗号化される。第２のプログラムコード１２６はセキュリティ・コマンド１２７を受信し、それに応答して、受信したセキュリティ・コマンドに関連する第２の装置セキュリティＩＤ１２９を格納されたセキュリティ・キー１２８と比較する。第２の装置セキュリティＩＤ１２９および格納されたセキュリティ・キー１２８が対応する場合、第２のプログラムコード１２６は第１の装置セキュリティＩＤによる認証をバイパスして、格納されたデータ１１４へのアクセスを提供する。

【００１０】

あるデータ記憶装置では、格納されたデータは暗号化形式とすることができる。このような態様において、第２の装置セキュリティＩＤ１２９および格納されたセキュリティ・キー１２８が対応する場合、第２のプログラムコード１２６は非復号化形式でしか格納されたデータ１１４へのアクセスを提供しない。格納されたデータ１１４へのアクセスが非復号化形式でしか提供されない場合、通常はそこから情報を引き出すことができない２進データである暗号化データしか読み出すことができない。故障時に、第１の装置セキュリティＩＤをディセーブルせずに、ユーザが装置１００をメーカへ戻す時にこの特徴は特に有用である。特に、これは暗号化され格納されたユーザデータ内の情報を明らかにすることなくデータ記憶装置の故障解析等の操作を実施することができる。ユーザデータをさらに保護するために、ある態様において、セキュリティ・コマンド１２７はセキュリティ・イレーズ・コマンド（ｓｅｃｕｒｉｔｙ　ｅｒａｓｅ　ｃｏｍｍａｎｄ）を含んでいる。このような態様において、第２の装置セキュリティＩＤ１２９および格納されたセキュリ

ティ・キー１２８が対応する場合、第２のプログラムコード１２６は格納された暗号化データ１１４に関連する少なくとも１つの復号キー１１６を削除してセキュリティ・イレーズ・コマンドを実行するように構成される。格納された暗号化データ１１４に関連する復号キー１１６が削除されると、データを回復することができない。

【００１１】

装置１００の故障解析は記憶装置故障解析システムにより実施することができ、それは図１のホストシステム１０８等の適切に構成されたコンピュータとすることができる。図１に示すように、システム１０８は入力１３０、出力１３２、プログラムメモリ１３４、コントローラ１３６およびホスト記憶装置インターフェイス１１０を介してデータ記憶装置通信ポート１２０に連結する通信ポート１３８を含んでいる。入力１３０はそれを介してデータを入力することができかつさまざまなコマンドを入力して有効にすることができるようなキーボード等の、任意適切な入力装置とすることができる。出力１３２は、たとえば、故障解析結果の視覚レンダリングを提供することができるディスプレイユニットまたはミラー等の任意の適切な出力装置とすることができる。１つ以上のプロセッサを含むことができるコントローラ１３６が入力１３０、出力１３２、プログラムメモリ１３４および通信ポート１３８に連結されてシステム１０８の動作を制御する。

【００１２】

プログラムメモリ１３４はデータ記憶装置１００に関連する製作プロセスデータ（１４４等）に基づいて第２の装置セキュリティＩＤ１２９を発生し、発生されたセキュリティＩＤ１２９を有するセキュリティ・コマンド（すなわち、装置アンロック・コマンド）１２７を通信ポート１３８を介してデータ記憶装置１００に送るように構成される第１のプログラムコード１４０を含んでいる。プログラムメモリ１３４内に含まれる第２のプログラムコード１４２は、装置アンロックコマンド１２７が正常に実行されると、データ記憶装置１００上で故障解析を実施して故障解析結果を提供するように構成される。

【００１３】

前述したように、セキュリティ・キー１２８および第２の装置セキュリティＩＤ１２９を発生するのに使用された製作プロセスデータは同じであるか少なくとも類似している。したがって、同じまたは類似プログラムコードを使用してセキュリティ・キー１２８および第２の装置セキュリティＩＤ１２９を発生することができる。前述したように、製作プロセスデータ１４４内に含まれる製作されたセキュリティＩＤはデータ記憶装置１００とは別個のいかなる場所にも記憶されることはなく、装置ハウジングまたは外部カバー以外の任意の場所、または装置１００に付したラベルから通常読み出されることができない。したがって、第２の装置セキュリティＩＤ１２９を発生するために、製作されたセキュリティＩＤを必要とする態様では、装置１００のアンロッキングは装置１００を物理的に所有し製作されたセキュリティＩＤを装置から読み出すことができる人しか実施することができない。一態様において、データ記憶装置１００はユーザデータへのアクセスが図１に関して前記したように制限され、図２に関して前述した、ディスク装置である。

【００１４】

図２は本態様が有用であるディスク装置２００の等角図である。ディスク装置２００はベース２０２およびトップカバー（図示せず）を有するハウジングを含んでいる。ディスク装置２００は、さらに、単一ディスクまたはディスクパック２０６を含み、それはディスククランプ２０８によりスピンドルモータ（図示せず）上に搭載される。ディスクパック２０６は複数の個別ディスクを含み、それらは中心軸２０９周りを一緒に回転するように搭載される。各ディスク表面には関連するディスクヘッド・スライダ２１０があり、それはディスク表面と通信するためにディスク装置２００に搭載される。図２に示す例では、スライダ２１０はサスペンション２１２により支持されており、それは次にアクチュエータ２１６のトラック・アクセスアーム２１４に取り付けられる。図２に示すアクチュエータはロータリ・ムービングコイル・アクチュエータとして知られるタイプのアクチュエータであり、一般的に２１８に示す、ボイスコイルモータ（ＶＣＭ）を含んでいる。ボイスコイルモータ２１８はアクチュエータ２１６をその取り付けられたヘッド２１０と共に

ピボット軸２２０周りに回転させ、ヘッド２１０をディスク内径２２４およびディスク外径２２６間の円弧状経路２２２に沿った所望のデータトラック上に位置決めする。ボイスコイルモータ２１８はヘッド２１０およびホストコンピュータ（図示せず）により発生される信号に基づいてサーボエレクトロニクス２３０により駆動される。異なるディスクまたはディスクの異なる部分を、それぞれ、プログラムコード（図１に関して記述した１２４および１２８等）および暗号化ユーザデータ（図１の１１４等）を格納するプログラムメモリおよびデータメモリ部として使用することができる。あるいは、ディスク装置２００において、プログラムコードおよびセキュリティ・キー（図１の１２８等）を１つまたは複数のディスク２０６とは別個のディスク装置不揮発性メモリ内に格納することができ、ユーザデータだけを１または複数のディスク２０６上に格納することができる。いずれにせよ、第１の装置セキュリティＩＤの確立と関連する第２の装置セキュリティＩＤを有するセキュリティ・コマンドを使用するディスク装置のアンロックとは、図１に関して記述したのと実質的に同じ方法で実施される。

【００１５】

次に、図３に、データ記憶装置内に格納されたユーザデータへのアクセスを制限する方法のフロー図を示す。この方法の第１のステップは格納されたデータへのアクセスを制限する第１の装置セキュリティＩＤをユーザが生成できるようにすることを含んでいる。これはステップ３０２に例示されている。ステップ３０４において、セキュリティ・キーが確立される。次に、セキュリティ・キーはデータ記憶装置内に格納される。これはステップ３０６に例示されている。ステップ３０８において、記憶装置はセキュリティ・コマンドを受信し、それに応答して、受信したセキュリティ・コマンドに関連する第２の装置セキュリティＩＤを格納されたセキュリティ・キーと比較し、第２の装置セキュリティＩＤおよび格納されたセキュリティ・キーが対応するならば、第１の装置セキュリティＩＤによる認証をバイパスして格納されたデータへのアクセスを提供できるようにプログラム可能とされる。ある態様において、格納されたデータは暗号化形式とすることができる。このような態様では、第２の装置セキュリティＩＤおよび格納されたセキュリティ・キーが対応するならば、非復号化形式の格納されたデータへのアクセスが提供される。

【００１６】

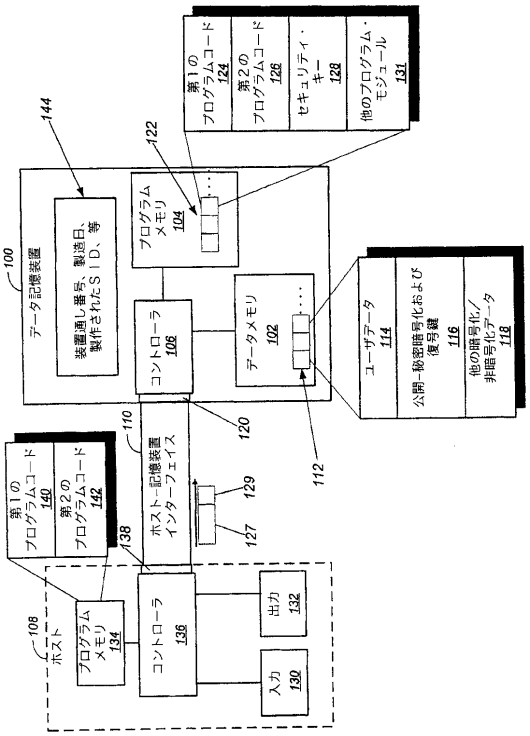
本開示のさまざまな態様の構造および機能の詳細と共に、本開示のさまざまな態様の非常に多くの特性および利点を前記説明において述べてきたが、本開示は実例にすぎず、添付特許請求の範囲が表現される用語の広範な一般的意味合いにより示される全範囲までの本開示の原理内で詳細、特に部品の構造および配置に関して、変更を行うことができる。たとえば、本開示の範囲および精神から逸脱することなく実質的に同じ機能性を維持しながら、データ記憶装置の特定の応用に応じて特定の要素を変えることができる。さらに、ここで記述された好ましい態様はディスク装置に対する制限されたイレーズおよびアンロックに向けられているが、当業者ならば本開示の教示は本開示の範囲および精神から逸脱することなく任意のデータ記憶装置に応用できることが理解される。

【符号の説明】

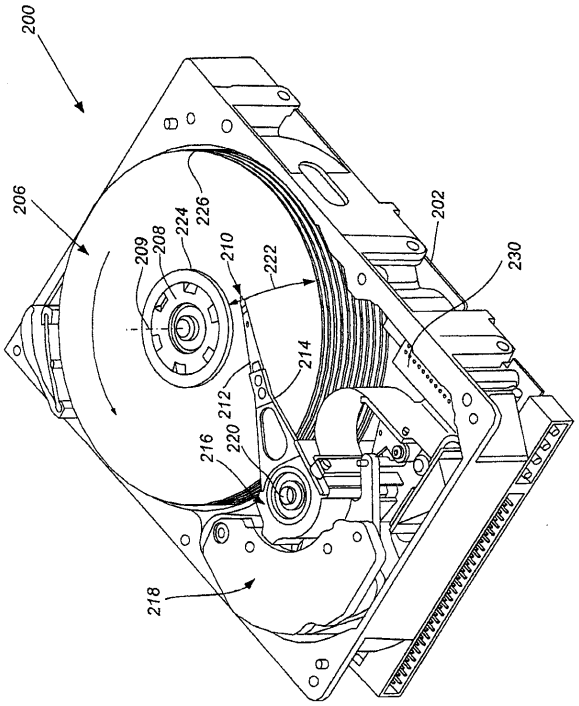
【００１７】

１００　データ記憶装置、１０２　データメモリ、１０４，１３４　プログラムメモリ、１０６，１３６　コントローラ、１０８　ホストシステム、１１０　ホスト記憶装置インターフェイス、１１２，１２２　メモリ場所、１１４　格納されたデータ、１１６　復号キー、１１８　暗号化／非暗号化データ、１２０　データ記憶装置通信ポート、１２４，１２６，１４０，１４２　プログラムコード、１２７　装置アンロック・コマンド、１２８　セキュリティ・キー、１２９　装置セキュリティＩＤ、１３０　入力、１３１　プログラム・モジュール、１３２　出力、１３８　通信ポート、１４４　情報、２００　ディスク装置、２０２　ベース、２０６　ディスク、２０８　ディスククランプ、２０９　中心軸、２１０　スライダ、２１２　サスペンション、２１４　アーム、２１６　アクチュエータ、２１８　ボイスコイルモータ、２２０　ピボット軸、２２２　円弧経路、２２４　ディスク内径、２２６　ディスク外径、２３０　サーボエレクトロニクス。

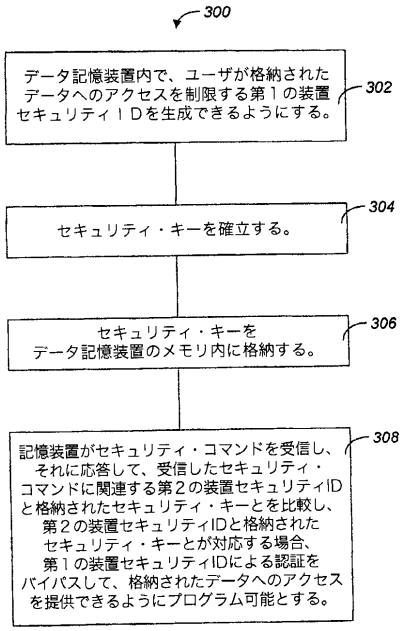
【図１】


第1のプログラムコード 124
第2のプログラムコード 126
セキュリティ・キー 128
他のプログラム・モジュール 131
144
122
プログラムメモリ 104
100
データ記憶装置
装置通し番号、製造日、製作されたSID、等
コントローラ 106
データメモリ 102
ユーザデータ 114
公開−秘密暗号化および復号鍵 116
他の暗号化／非暗号化データ 118
120
112
110
ホスト−記憶装置インターフェイス
第1のプログラムコード 140
第2のプログラムコード 142
129
127
138
108
ホスト
プログラムメモリ 134
コントローラ 136
出力 132
入力 130

【図２】


200
206
202
209
208
224
226
210
222
230
214
212
216
220
218

【図３】


300
データ記憶装置内で、ユーザが格納されたデータへのアクセスを制限する第１の装置セキュリティＩＤを生成できるようにする。
302
セキュリティ・キーを確立する。
304
セキュリティ・キーをデータ記憶装置のメモリ内に格納する。
306
記憶装置がセキュリティ・コマンドを受信し、それに応答して、受信したセキュリティ・コマンドに関連する第２の装置セキュリティIDと格納されたセキュリティ・キーとを比較し、第２の装置セキュリティIDと格納されたセキュリティ・キーとが対応する場合、第１の装置セキュリティIDによる認証をバイパスして、格納されたデータへのアクセスを提供できるようにプログラム可能とする。
308

フロントページの続き

(51)Int.Cl. FI
G06F 3/06 301F
G11B 20/10 H
G11B 20/10 D

(74)代理人 100124523
弁理士 佐々木 眞人
(72)発明者 ロバート イー. ヴァインスタイン
アメリカ合衆国、コロラド、バーサド、フェザント ラン 1311
(72)発明者 モンティ エー. フォアハンド
アメリカ合衆国、コロラド、ラブランド、ルーシール コート 4832

審査官 岸野 徹

(56)参考文献 特開2004-201038（JP, A）
特表2003-523016（JP, A）
特開2007-272476（JP, A）
特開2003-280752（JP, A）
葛原 高志, 磁気ディスク装置, 東芝技術公開集 VOL. 17-12, 株式会社東芝, 1999年 2月15日, 第17-12巻, p.1

(58)調査した分野(Int.Cl., DB名)
G06F 21/24
G06F 21/02
H04L 9/08