

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4674591号
(P4674591)

(45) 発行日 平成23年4月20日(2011.4.20)

(24) 登録日 平成23年2月4日(2011.2.4)

(51) Int. Cl.	F 1		
G 0 6 F 21/24	(2006.01)	G 0 6 F 12/14	5 6 0 D
G 0 6 F 3/06	(2006.01)	G 0 6 F 3/06	3 0 4 H
G 1 1 B 20/10	(2006.01)	G 1 1 B 20/10	H
		G 1 1 B 20/10	F

請求項の数 6 (全 12 頁)

(21) 出願番号	特願2007-42121 (P2007-42121)	(73) 特許権者	000004237
(22) 出願日	平成19年2月22日(2007.2.22)		日本電気株式会社
(65) 公開番号	特開2008-204336 (P2008-204336A)		東京都港区芝五丁目7番1号
(43) 公開日	平成20年9月4日(2008.9.4)	(74) 代理人	100085235
審査請求日	平成20年3月10日(2008.3.10)		弁理士 松浦 兼行
		(72) 発明者	秋山 忍
			東京都港区芝5丁目7番1号 日本電気株式会社内
		審査官	高橋 克

最終頁に続く

(54) 【発明の名称】 補助記憶装置及びそのセキュリティ確保方法とプログラム

(57) 【特許請求の範囲】

【請求項1】

コンピュータに接続されて使用される補助記憶装置において、
工場出荷時の初期状態であるか、内部のデータ用記録媒体へのデータ記録が可能なことを示す使用中状態であるかの情報を記憶する情報記憶手段と、

第1の方向に移動して前記コンピュータに接続すると該コンピュータの接続部により押されて待機位置から前記第1の方向とは反対方向である第2の方向に移動し、前記コンピュータから取り外されると前記第1の方向に移動して前記待機位置に自動復帰する導体制のピンと、

前記初期状態において前記ピンの先端部に当接しており、その初期状態における前記コンピュータへの最初の接続により前記ピンの先端部に当接しつつ所定位置まで前記第2の方向に移動し、前記最初の接続後の前記コンピュータからの取り外しにより前記ピンが前記第1の方向へ移動して前記待機位置に自動復帰したときは、移動することなくそのまま前記所定位置に保持される導体制と、

前記初期状態において前記導体の外周部に当接し、かつ、前記導体と共に移動しないよう前記導体と独立して設けられた非導体制と、

前記非導体制に対して前記ピンの中心軸方向に力を付勢しており、前記導体の前記所定位置への移動により前記導体との当接状態が解除された前記非導体制を前記ピンの先端部に当接させる力付勢手段と、

前記コンピュータの二回目の接続時には、前記待機位置にある前記ピンの先端部に前記

10

20

非導体を当接しつつ前記第 2 の方向に移動し、前記所定位置にて保持されている前記導体を前記非導体を介して押して前記所定位置の外部へ移動させると共に、前記所定位置に前記非導体を保持させ、前記二回目の接続後の前記コンピュータからの取り外しにより前記ピンが前記第 1 の方向へ移動して前記待機位置に自動復帰したときは、前記非導体を移動することなくそのまま前記所定位置に保持させ、前記コンピュータの三回目以降の接続時にも前記ピンの移動に関係なく前記非導体を前記所定位置に保持させ続ける非導体移動制御手段と、

前記所定位置に前記導体が前記ピンの先端部に当接した状態で保持されているときには前記ピンと前記導体とが外部導体と導通路を形成して導通状態となり、前記ピンが待機位置にあるとき及び前記所定位置に前記非導体が保持されているときには前記導通路の解除により非導通状態となる導通検出手段と、

10

前記情報記憶手段の記憶情報が初期状態を示しており、かつ、前記導通検出手段が導通状態を検出したかを判定する第 1 の判定手段と、

前記情報記憶手段の記憶情報が使用中状態を示しており、かつ、前記導通検出手段が非導通状態を検出したかを判定する第 2 の判定手段と、

前記第 1 の判定手段による判定結果が得られたとき、又は前記第 2 の判定手段による判定結果が得られたときに前記内部のデータ用記録媒体の記憶データを消去する消去手段と

前記第 1 の判定状態による判定結果に基づき前記消去手段による消去動作が行われたときに、前記情報記憶手段に前記使用中状態を記憶する設定手段と、

20

を有することを特徴とする補助記憶装置。

【請求項 2】

前記消去手段は、前記内部のデータ用記録媒体をフォーマットした後、特定のデータを上書きする手段であることを特徴とする請求項 1 記載の補助記憶装置。

【請求項 3】

コンピュータに接続されて使用される補助記憶装置のセキュリティ確保方法において、

前記補助記憶装置は、

工場出荷時の初期状態であるか、内部のデータ用記録媒体へのデータ記録が可能なことを示す使用中状態であるかの情報を記憶する情報記憶手段と、

30

第 1 の方向に移動して前記コンピュータに接続すると該コンピュータの接続部により押されて待機位置から前記第 1 の方向とは反対方向である第 2 の方向に移動し、前記コンピュータから取り外されると前記第 1 の方向に移動して前記待機位置に自動復帰する導体製のピンと、

前記初期状態において前記ピンの先端部に当接しており、その初期状態における前記コンピュータへの最初の接続により前記ピンの先端部に当接しつつ所定位置まで前記第 2 の方向に移動し、前記最初の接続後の前記コンピュータからの取り外しにより前記ピンが前記第 1 の方向へ移動して前記待機位置に自動復帰したときは、移動することなくそのまま前記所定位置に保持される導体と、

前記初期状態において前記導体の外周部に当接し、かつ、前記導体と共に移動しないよう前記導体と独立して設けられた非導体と、

40

前記非導体に対して前記ピンの中心軸方向に力を付勢しており、前記導体の前記所定位置への移動により前記導体との当接状態が解除された前記非導体を前記ピンの先端部に当接させる力付勢手段と、

前記コンピュータの二回目の接続時には、前記待機位置にある前記ピンの先端部に前記非導体を当接しつつ前記第 2 の方向に移動し、前記所定位置にて保持されている前記導体を前記非導体を介して押して前記所定位置の外部へ移動させると共に、前記所定位置に前記非導体を保持させ、前記二回目の接続後の前記コンピュータからの取り外しにより前記ピンが前記第 1 の方向へ移動して前記待機位置に自動復帰したときは、前記非導体を移動することなくそのまま前記所定位置に保持させ、前記コンピュータの三回目以降の接続時

50

にも前記ピンの移動に関係なく前記非導体を前記所定位置に保持させ続ける非導体移動制御手段と、

前記所定位置に前記導体が前記ピンの先端部に当接した状態で保持されているときには前記ピンと前記導体とが外部導体と導通路を形成して導通状態となり、前記ピンが待機位置にあるとき及び前記所定位置に前記非導体が保持されているときには前記導通路の解除により非導通状態となる導通検出手段と、

を備えており、

前記補助記憶装置が、前記情報記憶手段の記憶情報が初期状態を示しており、かつ、前記導通検出手段が導通状態を検出したかを判定する第1の判定ステップと、

前記補助記憶装置が、前記情報記憶手段の記憶情報が使用中状態を示しており、かつ、前記導通検出手段が非導通状態を検出したかを判定する第2の判定ステップと、

前記補助記憶装置が、前記第1の判定ステップによる判定結果が得られたとき、又は前記第2の判定ステップによる判定結果が得られたときに前記内部のデータ用記録媒体の記憶データを消去する消去ステップと、

前記補助記憶装置が、前記第1の判定ステップによる判定結果に基づき前記消去ステップによる消去動作が行われたときに、前記情報記憶手段に前記使用中状態を記憶する設定ステップと

を含むことを特徴とする補助記憶装置のセキュリティ確保方法。

【請求項4】

前記消去ステップは、前記内部のデータ用記録媒体をフォーマットした後、特定のデータを上書きすることを特徴とする請求項3記載の補助記憶装置のセキュリティ確保方法。

【請求項5】

第1のコンピュータに接続されて使用される補助記憶装置のセキュリティ確保を、前記補助記憶装置内の第2のコンピュータにより実行させるプログラムであって、

前記補助記憶装置は、

工場出荷時の初期状態であるか、内部のデータ用記録媒体へのデータ記録が可能なことを示す使用中状態であるかの情報を記憶する情報記憶手段と、

第1の方向に移動して前記コンピュータに接続すると該コンピュータの接続部により押されて待機位置から前記第1の方向とは反対方向である第2の方向に移動し、前記コンピュータから取り外されると前記第1の方向に移動して前記待機位置に自動復帰する導体製のピンと、

前記初期状態において前記ピンの先端部に当接しており、その初期状態における前記コンピュータへの最初の接続により前記ピンの先端部に当接しつつ所定位置まで前記第2の方向に移動し、前記最初の接続後の前記コンピュータからの取り外しにより前記ピンが前記第1の方向へ移動して前記待機位置に自動復帰したときは、移動することなくそのまま前記所定位置に保持される導体と、

前記初期状態において前記導体の外周部に当接し、かつ、前記導体と共に移動しないよう前記導体と独立して設けられた非導体と、

前記非導体に対して前記ピンの中心軸方向に力を付勢しており、前記導体の前記所定位置への移動により前記導体との当接状態が解除された前記非導体を前記ピンの先端部に当接させる力付勢手段と、

前記コンピュータの二回目の接続時には、前記待機位置にある前記ピンの先端部に前記非導体を当接しつつ前記第2の方向に移動し、前記所定位置にて保持されている前記導体を前記非導体を介して押して前記所定位置の外部へ移動させると共に、前記所定位置に前記非導体を保持させ、前記二回目の接続後の前記コンピュータからの取り外しにより前記ピンが前記第1の方向へ移動して前記待機位置に自動復帰したときは、前記非導体を移動することなくそのまま前記所定位置に保持させ、前記コンピュータの三回目以降の接続時にも前記ピンの移動に関係なく前記非導体を前記所定位置に保持させ続ける非導体移動制御手段と、

前記所定位置に前記導体が前記ピンの先端部に当接した状態で保持されているときには

10

20

30

40

50

前記ピンと前記導体とが外部導体と導通路を形成して導通状態となり、前記ピンが待機位置にあるとき及び前記所定位置に前記非導体が保持されているときには前記導通路の解除により非導通状態となる導通検出手段と、

を備えており、

前記第2のコンピュータに、

前記情報記憶手段の記憶情報が初期状態を示しており、かつ、前記導通検出手段が導通状態を検出したかを判定する第1の判定ステップと、

前記情報記憶手段の記憶情報が使用中状態を示しており、かつ、前記導通検出手段が非導通状態を検出したかを判定する第2の判定ステップと、

前記第1の判定ステップによる判定結果が得られたとき、又は前記第2の判定ステップによる判定結果が得られたときに前記内部のデータ用記録媒体の記憶データを消去する消去ステップと、

前記第1の判定ステップによる判定結果に基づき前記消去ステップによる消去動作が行われたときに、前記情報記憶手段に前記使用中状態を記憶する設定ステップと

を実行させることを特徴とする補助記憶装置のセキュリティ確保プログラム。

【請求項6】

前記第消去ステップは、前記内部のデータ用記録媒体をフォーマットした後、特定のデータを上書きすることを特徴とする請求項5記載の補助記憶装置のセキュリティ確保プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は補助記憶装置及びそのセキュリティ確保方法とプログラムに係り、特にコンピュータに接続され、データを保持する電子媒体を持つ補助記憶装置及びそのセキュリティ確保方法とプログラムに関する。

【背景技術】

【0002】

コンピュータに搭載又は接続され、データを保持する電子媒体を持つ、ハードディスク、リムーバブルハードディスクドライブ、USBメモリ等に代表される補助記憶装置は、コンピュータから取り外し可能であるため、第三者によって取得され、その補助記憶装置に記憶されているデータが第三者により不正使用される可能性がある。なお、本明細書において、「コンピュータに搭載又は接続」とは、コンピュータの所定の端子に接続されるということの意味する。

【0003】

しかし、従来、補助記憶装置自身のハードウェアにはセキュリティを確保するための構造はなく、データの不正使用を防止するにはソフトウェア的なデータ暗号化や、パスワードによるアクセス制限を設けることが行われている（例えば、特許文献1参照）。この特許文献1には、着脱可能な記憶媒体の接続を検出すると、接続された記憶媒体にユーザIDが設定されているか否かを判定し、記憶媒体にユーザIDが設定されていないと判定した場合には、記憶媒体に対するフォーマット処理を実行し、フォーマット処理された記憶媒体に対してユーザIDとパスワードを設定し、設定されたユーザIDとパスワードを用いてユーザID毎の暗号鍵を生成し、記憶媒体にデータを書き込む際に、生成された暗号鍵を用いて暗号化する発明が開示されている。これにより、画像処理装置から取り外された記憶媒体の機密性を確保しようとするものである。

【0004】

一方、補助記憶装置の記憶内容の意図しない書き換え動作を防止する機能も従来知られている（例えば、特許文献2、特許文献3参照）。特許文献2には、ハードディスク制御装置にライトプロテクトスイッチを設けた場合に、ユーザによってスイッチが切り替えられてライトプロテクトの状態が動作中に変わる可能性をなくすため、ホストに接続されてプロトコル変換を行うアダプタとリムーバブルハードディスクとを接続するアダプタのコ

10

20

30

40

50

ネクタ側にライトプロテクト検出手段を設けると共に、リムーバブルハードディスクのネクタ側にはライトプロテクト通知手段を設けることにより、アダプタとリムーバブルハードディスクとの接続中は、ライトプロテクト通知手段の切り替えができず、動作中のライトプロテクトの状態の変更ができないようにする発明が開示されている。

【0005】

また、特許文献3には、ホストに着脱自在に装着されるハードディスクドライブの磁気ディスクに対する記録動作の禁止/許可状態を機械的に保持する記録禁止スイッチを設け、記録禁止スイッチが記録禁止状態の操作状態とされているときには、プロセッサがその操作状態を検出してホストからの記録コマンドを拒否して、磁気ヘッドによるデータ記録動作を禁止する発明が開示されている。

10

【0006】

【特許文献1】特開2006-309298号公報

【特許文献2】特開2006-155029号公報

【特許文献3】特開2001-006262号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、特許文献1記載の発明では、暗号化によってセキュリティを確保しようとしているが、暗号鍵又はパスワード等の管理方法に不備があり、悪意を持った第三者に暗号鍵やパスワードが知られてしまった場合には、全くセキュリティの効果を失うという課題がある。

20

【0008】

また、特許文献2及び3記載の発明では、補助記憶装置であるリムーバブルハードディスクやハードディスクドライブの記憶内容をホストからによる誤動作から保護することは可能であるが、第三者によって補助記憶装置が取得され、その補助記憶装置に記憶されているデータが第三者により不正使用される可能性は排除できない。

【0009】

本発明は以上の点に鑑みなされたもので、第三者によって補助記憶装置が取得された場合でも、その補助記憶装置に記憶されているデータが第三者により不正使用されたり、漏洩したり、改竄されることを防止し得る補助記憶装置及びそのセキュリティ確保方法とプログラムを提供することを目的とする。

30

【課題を解決するための手段】

【0010】

上記の目的を達成するため、第1の発明は、コンピュータに接続されて使用される補助記憶装置において、工場出荷時の初期状態であるか、内部のデータ用記録媒体へのデータ記録が可能であることを示す使用中状態であるかの情報を記憶する情報記憶手段と、第1の方向に移動してコンピュータに接続するとコンピュータの接続部により押されて待機位置から第1の方向とは反対方向である第2の方向に移動し、コンピュータから取り外されると第1の方向に移動して待機位置に自動復帰する導体制のピンと、初期状態においてピンの先端部に当接しており、その初期状態におけるコンピュータへの最初の接続によりピンの先端部に当接しつつ所定位置まで第2の方向に移動し、最初の接続後のコンピュータからの取り外しによりピンが第1の方向へ移動して待機位置に自動復帰したときは、移動することなくそのまま所定位置に保持される導体と、初期状態において導体の外周部に当接し、かつ、導体と共に移動しないよう導体と独立して設けられた非導体と、非導体に対してピンの中心軸方向に力を付勢しており、導体の所定位置への移動により導体との当接状態が解除された非導体をピンの先端部に当接させる力付勢手段と、コンピュータの二回目の接続時には、待機位置にあるピンの先端部に非導体を当接しつつ第2の方向に移動し、所定位置にて保持されている導体を非導体を介して押して所定位置の外部へ移動させると共に、所定位置に非導体を保持させ、二回目の接続後のコンピュータからの取り外しによりピンが第1の方向へ移動して待機位置に自動復帰したときは、非導体を移動することなく

40

50

そのまま所定位置に保持させ、コンピュータの三回目以降の接続時にもピンの移動に関係なく非導体を所定位置に保持させ続ける非導体移動制御手段と、所定位置に導体がピンの先端部に当接した状態で保持されているときにはピンと導体とが外部導体と導通路を形成して導通状態となり、ピンが待機位置にあるとき及び所定位置に非導体が保持されているときには導通路の解除により非導通状態となる導通検出手段と、情報記憶手段の記憶情報が初期状態を示しており、かつ、導通検出手段が導通状態を検出したかを判定する第1の判定手段と、情報記憶手段の記憶情報が使用中状態を示しており、かつ、導通検出手段が非導通状態を検出したかを判定する第2の判定手段と、第1の判定手段による判定結果が得られたとき、又は第2の判定手段による判定結果が得られたときに内部のデータ用記録媒体の記憶データを消去する消去手段と、第1の判定状態による判定結果に基づき消去手段による消去動作が行われたときに、情報記憶手段に使用中状態を記憶する設定手段と、を有することを特徴とする。

10

【0011】

この発明では、補助記憶装置がコンピュータに搭載又は接続された後、再度コンピュータに搭載又は接続されると、記憶データが消去されるので、コンピュータに搭載又は接続されている補助記憶装置を取り外して、別のコンピュータに搭載又は接続した場合は、その補助記憶装置の記憶データを消去できる。

【0012】

また、上記の目的を達成するため、第2の発明は、コンピュータに接続されて使用される補助記憶装置のセキュリティ確保方法において、補助記憶装置は、

20

工場出荷時の初期状態であるか、内部のデータ用記録媒体へのデータ記録が可能なことを示す使用中状態であるかの情報を記憶する情報記憶手段と、第1の方向に移動してコンピュータに接続するとコンピュータの接続部により押されて待機位置から第1の方向とは反対方向である第2の方向に移動し、コンピュータから取り外されると第1の方向に移動して待機位置に自動復帰する導体制のピンと、初期状態においてピンの先端部に当接しており、その初期状態におけるコンピュータへの最初の接続によりピンの先端部に当接しつつ所定位置まで第2の方向に移動し、最初の接続後のコンピュータからの取り外しによりピンが第1の方向へ移動して待機位置に自動復帰したときは、移動することなくそのまま所定位置に保持される導体と、初期状態において導体の外周部に当接し、かつ、導体と共に移動しないよう導体と独立して設けられた非導体と、非導体に対してピンの中心軸方向に力を付勢しており、導体の所定位置への移動により導体との当接状態が解除された非導体をピンの先端部に当接させる力付勢手段と、コンピュータの二回目の接続時には、待機位置にあるピンの先端部に非導体を当接しつつ第2の方向に移動し、所定位置にて保持されている導体を非導体を介して押して所定位置の外部へ移動させると共に、所定位置に非導体を保持させ、二回目の接続後のコンピュータからの取り外しによりピンが第1の方向へ移動して待機位置に自動復帰したときは、非導体を移動することなくそのまま所定位置に保持させ、コンピュータの三回目以降の接続時にもピンの移動に関係なく非導体を所定位置に保持させ続ける非導体移動制御手段と、所定位置に導体がピンの先端部に当接した状態で保持されているときにはピンと導体とが外部導体と導通路を形成して導通状態となり、ピンが待機位置にあるとき及び所定位置に非導体が保持されているときには導通路の解除により非導通状態となる導通検出手段と、を備えており、

30

40

補助記憶装置が、情報記憶手段の記憶情報が初期状態を示しており、かつ、導通検出手段が導通状態を検出したかを判定する第1の判定ステップと、補助記憶装置が、情報記憶手段の記憶情報が使用中状態を示しており、かつ、導通検出手段が非導通状態を検出したかを判定する第2の判定ステップと、補助記憶装置が、第1の判定ステップによる判定結果が得られたとき、又は第2の判定ステップによる判定結果が得られたときに内部のデータ用記録媒体の記憶データを消去する消去ステップと、補助記憶装置が、第1の判定ステップによる判定結果に基づき消去ステップによる消去動作が行われたときに、情報記憶手段に使用中状態を記憶する設定ステップとを含むことを特徴とする。

【0013】

50

また、上記の目的を達成するため、第3の発明は、第1のコンピュータに接続されて使用される補助記憶装置のセキュリティ確保を、補助記憶装置内の第2のコンピュータにより実行させるプログラムであって、補助記憶装置は、

工場出荷時の初期状態であるか、内部のデータ用記録媒体へのデータ記録が可能なことを示す使用中状態であるかの情報を記憶する情報記憶手段と、第1の方向に移動してコンピュータに接続するとコンピュータの接続部により押されて待機位置から第1の方向とは反対方向である第2の方向に移動し、コンピュータから取り外されると第1の方向に移動して待機位置に自動復帰する導体制のピンと、初期状態においてピンの先端部に当接しており、その初期状態におけるコンピュータへの最初の接続によりピンの先端部に当接しつつ所定位置まで第2の方向に移動し、最初の接続後のコンピュータからの取り外しによりピンが第1の方向へ移動して待機位置に自動復帰したときは、移動することなくそのまま所定位置に保持される導体と、初期状態において導体の外周部に当接し、かつ、導体と共に移動しないよう導体と独立して設けられた非導体と、非導体に対してピンの中心軸方向に力を付勢しており、導体の所定位置への移動により導体との当接状態が解除された非導体をピンの先端部に当接させる力付勢手段と、コンピュータの二回目の接続時には、待機位置にあるピンの先端部に非導体を当接しつつ第2の方向に移動し、所定位置にて保持されている導体を非導体を介して押して所定位置の外部へ移動させると共に、所定位置に非導体を保持させ、二回目の接続後のコンピュータからの取り外しによりピンが第1の方向へ移動して待機位置に自動復帰したときは、非導体を移動することなくそのまま所定位置に保持させ、コンピュータの三回目以降の接続時にもピンの移動に関係なく非導体を所定位置に保持させ続ける非導体移動制御手段と、所定位置に導体がピンの先端部に当接した状態で保持されているときにはピンと導体とが外部導体と導通路を形成して導通状態となり、ピンが待機位置にあるとき及び所定位置に非導体が保持されているときには導通路の解除により非導通状態となる導通検出手段と、を備えており、

上記第2のコンピュータに、

情報記憶手段の記憶情報が初期状態を示しており、かつ、導通検出手段が導通状態を検出したかを判定する第1の判定ステップと、情報記憶手段の記憶情報が使用中状態を示しており、かつ、導通検出手段が非導通状態を検出したかを判定する第2の判定ステップと、第1の判定ステップによる判定結果が得られたとき、又は第2の判定ステップによる判定結果が得られたときに内部のデータ用記録媒体の記憶データを消去する消去ステップと、第1の判定ステップによる判定結果に基づき消去ステップによる消去動作が行われたときに、情報記憶手段に使用中状態を記憶する設定ステップとを実行させることを特徴とする。

【発明の効果】

【0019】

本発明によれば、コンピュータに搭載又は接続されている補助記憶装置を取り外して、別のコンピュータに搭載又は接続した場合は、その補助記憶装置の記憶データを消去できるため、補助記憶装置がコンピュータから取り外されて持ち去られた場合でも、補助記憶装置の記憶データの漏洩を防止することができ、また、改竄も防止でき、データの暗号化やパスワードの設定に比べて、より一層セキュリティ効果を高めることができる。

【発明を実施するための最良の形態】

【0020】

次に、本発明を実施するための最良の形態について図面と共に詳細に説明する。図1は本発明になる補助記憶装置の一実施の形態のブロック図を示す。同図において、本実施の形態の補助記憶装置であるハードディスク11は、通常のハードディスクとしての動作を行うため、磁気によりデータが記録される磁気ディスクである記録媒体12と、外部のコンピュータとの間で双方向通信する基本制御部13と、追加制御部14と、挿抜検出部15とから構成されている。

【0021】

基本制御部13は、通常のハードディスクとしての動作を行うため、外部のコンピュー

10

20

30

40

50

タからの要求に従って、記録媒体 1 2 からのデータの読み出し、記録媒体 1 2 へのデータの書き込みを制御する。なお、図 1 では図示を省略したが、基本制御部 1 3 からの制御に基づいて、記録媒体 1 2 からデータを書き込み、または記録データを読み出す磁気ヘッドなどの記録再生機構が存在することは勿論である。

【 0 0 2 2 】

挿抜検出部 1 5 は、ハードディスク 1 1 がコンピュータ等の機器に搭載または取り外されることによって内部回路が導通したり非導通になる機構を備え、その機構に基づいて機器に搭載又は取り外された状態を検出し、その検出した状態を追加制御部 1 4 へ通知する。追加制御部 1 4 は、挿抜検出部 1 5 からの「導通か非導通か」の挿抜検出情報と、基本制御部 1 3 からの記録媒体 1 2 が「初期状態か使用中状態か」の情報とにより、記録媒体 1 2 のフォーマットを実行するかしないかを判断して、その判断結果を基本制御部 1 3 へ通知する。

10

【 0 0 2 3 】

図 2 は図 1 の挿抜検出部 1 5 の一実施の形態の機構的構成図を示す。初期状態では図 2 (A) に示すように、挿抜検出部 1 5 は、例えば、第 1 の導体 1、第 2 の導体 2、非導体 3、導体制のピン 4 とからなり、ピン 4 の一端がドライブ 5 側に移動自在に保持されており、ハードディスク 1 1 がコンピュータの本体 6 側に搭載されるとピン 4 の一端が押されて図中、右方向へ移動され、コンピュータの本体 6 側から取り外されると、図 2 (A) の初期状態の位置に自動復帰する構成とされている。

【 0 0 2 4 】

また、導体である丸棒状のピン 4 のドライブ 5 側とは反対側の先端部分は、ピン 4 のこの部分と中心軸は一致し、かつ、小径の構成とされており、その小径の先端部分には例えば平板状の導体 1 の中心部分が挿抜可能な状態で保持されている。導体 1 は図中、右方向に移動自在に構成されている。また、導体 1 の外周側面が例えば中空平板状の非導体 3 の中空部の内壁と接触している。非導体 3 は、図示しないスプリング等の力付勢手段により力を図中、ピン 4 の中心軸方向に付勢されており、また、図中、右方向に移動自在に構成されている。更に、導体 2 は、非導体 3 と同径の中空部を有する例えば中空平板状であり、非導体 3 の一方の面に当接した状態で、ピン 4 の動きには連動せずに固定されている。

20

【 0 0 2 5 】

次に、本実施の形態の要部である挿抜検出部 1 5 の動作について図 2 と共に説明する。まず、図 2 (A) の初期状態にあるハードディスク 1 1 がコンピュータに搭載されると、コンピュータの本体 6 側によりドライブ 5 側に移動自在に保持されているピン 4 の一端が押され、それにより、図 2 (B) に示すように、ピン 4 が矢印 a 方向に移動し、ピン 4 の先端部分に保持されている導体 1 がピン 4 と連動して導体 2 の中空部の内壁に当接する位置まで移動する。

30

【 0 0 2 6 】

これにより、図 2 (B) に矢印 d で示すように、導体 2、導体 1、ピン 4、導体 1、導体 2 の順で導通路が形成され、挿抜検出部 1 5 は導通状態になる。なお、このとき導体 1 の移動により、非導体 3 は図 2 (B) に 3 ' で示すように、図示しない力付勢手段によりピン 4 の中心軸方向に付勢されている力により、ピン 4 の外周面にまで移動してその中空の内壁が当接する。

40

【 0 0 2 7 】

続いて、ハードディスク 1 1 を搭載されているコンピュータから取り外すと、図 2 (C) に示すように、ピン 4 は矢印 b 方向に移動して自動復帰するが、ピン 4 の先端部に保持されていた導体 1 はそのまま導体 2 の中空部の内壁に当接した状態の位置に残される。これにより、ピン 4 と導体 1 との接続が解除されるので、上記の導通路が解除され、挿抜検出部 1 5 は非導通状態となる。なお、このときピン 4 の矢印 b 方向の移動により、非導体 3 は図 2 (C) に 3 " で示すように、図示しない力付勢手段によりピン 4 の中心軸方向に付勢されている力により、ピン 4 の先端部の外周面にまで移動してその中空の内壁が当接する。

50

【 0 0 2 8 】

続いて、一旦コンピュータから取り外したハードディスク 1 1 を再度コンピュータに搭載すると、コンピュータの本体 6 側によりドライブ 5 側に移動自在に保持されているピン 4 の一端が押され、それにより、図 2 (D) に示すように、ピン 4 が再び矢印 a 方向に移動し、ピン 4 の先端部分に保持されている非導体 3 がピン 4 と連動して導体 2 の中空部の内壁に当接する位置まで押し込まれると共に、それまで導体 2 の中空部の内壁に当接していた導体 1 が非導体 3 に押されて、1' で示すように導体 2 から外れた位置まで移動する。これにより、挿抜検出部 1 5 は引き続き非導通状態となる。

【 0 0 2 9 】

次に、図 1 の実施の形態の動作について、図 3 の本発明のセキュリティ確保方法のフローチャートを併せ参照して説明する。図 1 の追加制御部 1 4 は、ハードディスク 1 1 が「初期状態か使用中状態か」の情報を有する。工場出荷時のハードディスク 1 1 がフォーマットされる前の状態は初期状態であり、フォーマットされた後の状態は使用中状態である。

10

【 0 0 3 0 】

追加制御部 1 4 は内部で保持している上記のハードディスクが「初期状態か使用中状態か」の情報を判定し(図 3 のステップ S 1)、初期状態であると判定したときは、挿抜検出部 1 5 からの挿抜検出情報を判定する(図 3 のステップ S 2)。工場出荷後のハードディスク 1 1 が最初にコンピュータ等に搭載又は接続される前の状態では、挿抜検出部 1 5 は図 2 (A) に示した非導通の状態にあるので、挿抜検出情報は非導通であると判定され、何もしない。

20

【 0 0 3 1 】

工場出荷後のハードディスク 1 1 が最初にコンピュータ等に搭載又は接続されると、初期状態であり、かつ、挿抜検出部 1 5 は図 2 (B) に示した導通の状態になるので、挿抜検出情報は導通を示し、追加制御部 1 4 はこの判定結果に基づき、基本制御部 1 3 を通じて記録媒体 1 2 をフォーマットする(図 3 のステップ S 3)。このフォーマットはハードディスク 1 1 の一回目のフォーマットであり、セキュリティとは無関係である。

【 0 0 3 2 】

続いて、追加制御部 1 4 はフォーマットを完了すると、内部に保持している「初期状態か使用中状態か」の情報を「使用中状態」に設定する(図 3 のステップ S 4)。この状態ではフォーマットはしない。この状態で、ハードディスク 1 1 は通常のハードディスクとして使用される。

30

【 0 0 3 3 】

その後、ハードディスク 1 1 を第三者がコンピュータから取り外して持ち出し、別のコンピュータに搭載又は接続した場合、追加制御部 1 4 は内部に保持している「初期状態か使用中状態か」の情報が「使用中状態」であると判定し(ステップ S 1)、続いて挿抜検出部 1 5 からの挿抜検出情報を判定する(図 3 のステップ S 5)。このとき、挿抜検出部 1 5 は、前述したように、コンピュータから取り外されたときに図 2 (C) に示した非導通の状態となり、また、再度コンピュータに搭載又は接続されることで図 2 (D) に示した非導通状態にされているので、追加制御部 1 4 はステップ S 5 で挿抜検出情報は非導通と判定し、この判定結果に基づき、基本制御部 1 3 を通じて記録媒体 1 2 をフォーマットする(図 3 のステップ S 6)。

40

【 0 0 3 4 】

このステップ S 6 の二回目のフォーマットにより、ハードディスク 1 1 の記録媒体 1 2 に記録されていたデータはすべて消去される。従って、ハードディスク 1 1 を第三者がコンピュータから取り外して持ち出し、別のコンピュータに搭載又は接続した段階でハードディスク 1 1 の記録媒体 1 2 にそれまで記録されていたデータが消去されるので、記録データ(内部データ)の漏洩を防止でき、セキュリティを確保することができる。

【 0 0 3 5 】

また、ステップ S 6 の二回目のフォーマットが完了しても、ハードディスク 1 1 は使用

50

中状態で、かつ、挿抜検出部 1 5 が非導通状態であることは変化しないので、再度フォーマットを繰り返すことにより、このハードディスク 1 1 は使用不可となる。

【 0 0 3 6 】

このように、本実施の形態では、ハードディスク 1 1 のコンピュータへの二回目の搭載又は接続であることを、挿抜検出部 1 5 のハードウェア的な非可逆的な機構で検知しているので、改竄防止の効果が大きい。更に、本実施の形態では、ハードディスク 1 1 が初期状態か使用中状態かは内部の追加制御部 1 4 で保持しており、初期状態から使用中状態への移行を非可逆的にすることで、改竄防止効果を高めることができる。

【 0 0 3 7 】

なお、本発明は上記の実施の形態に限定されるものではなく、例えば、基本的構成は上記の実施の形態と同じであるが、データの消去方法について更に工夫し、フォーマットに続いて 0 等の特定データを記録媒体 1 2 に上書きすることで、より完全にデータを消去することができる。ただし、上書きには時間がかかるので、まずフォーマットすることで応急処置的にデータを読めなくする必要がある。

【 0 0 3 8 】

また、上記の実施の形態では、ハードディスク 1 1 を例にして説明したが、本発明はコンピュータに搭載又は接続され、データを保持する電子媒体を備えた補助記憶装置であれば、ハードディスク以外でも適用可能である（例えば、USBメモリなどにも適用可能である。）。更に、本発明は上記の図 3 の方法のフローチャートを追加制御部 1 4 によりソフトウェア的に実行させるコンピュータプログラムも包含するものである。

【 図面の簡単な説明 】

【 0 0 3 9 】

【 図 1 】 本発明装置の一実施の形態のブロック図である。

【 図 2 】 図 1 中の挿抜検出部の一実施の形態の動作説明用機構図である。

【 図 3 】 本発明方法の一実施の形態のフローチャートである。

【 符号の説明 】

【 0 0 4 0 】

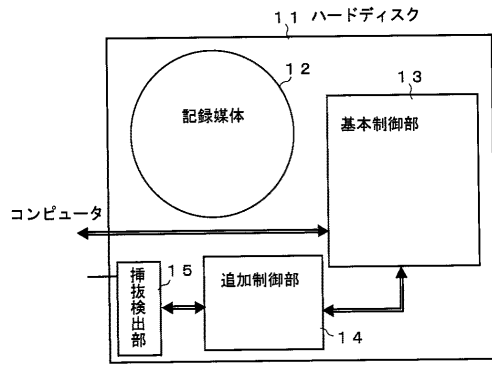
- 1、1'、2 導体
- 3、3'、3" 非導体
- 4 ピン
- 1 1 ハードディスク
- 1 2 記録媒体
- 1 3 基本制御部
- 1 4 追加制御部
- 1 5 挿抜検出部

10

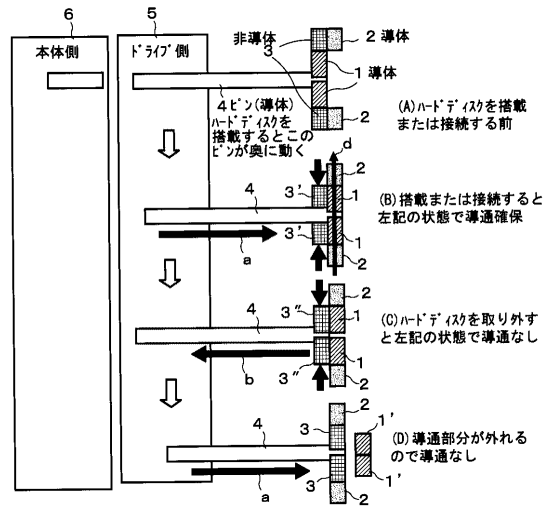
20

30

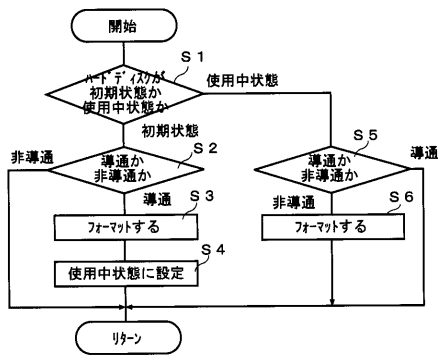
【図1】



【図2】



【図3】



フロントページの続き

- (56)参考文献 特開平05 - 250103 (JP, A)
特開平08 - 095866 (JP, A)
特開平11 - 175406 (JP, A)
特開平06 - 125525 (JP, A)
特開平09 - 106329 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G 0 6 F	2 1 / 2 4
G 0 6 F	3 / 0 6
G 0 6 K	1 7
G 0 6 K	1 9
G 1 1 B	2 0 / 1 0