(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2006-344112
(P2006-344112A)
(43)公開日　平成18年12月21日(2006.12.21)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	530D	5B017
		G06F	12/14	520F	
		G06F	12/14	560D	

審査請求 未請求　請求項の数 6　ＯＬ　（全 14 頁）

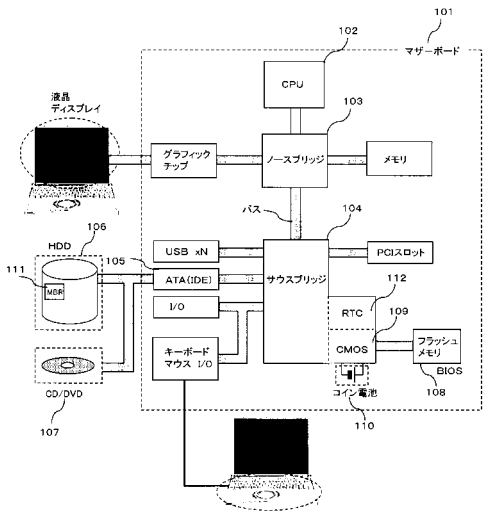
(21)出願番号　特願2005-170633 (P2005-170633)
(22)出願日　平成17年6月10日 (2005.6.10)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100097445
弁理士　岩橋　文雄
(74)代理人　100109667
弁理士　内藤　浩樹
(74)代理人　100109151
弁理士　永野　大介
(72)発明者　松下　尚史
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　山田　仁司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置のセキュリティ装置およびセキュリティ方法

(57)【要約】
【課題】ＰＣの不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにする。
【解決手段】正しいパスワードを所定回数内に入力されない場合はセキュリティ機能を発動して、ＨＤＤ内に自己消去プログラムを設定し、ＨＤＤ内のデータは自己消去するだけでなく、一旦、ＨＤＤ内の自己消去プログラムは発動がなされれば、たとえ消去中に電源ＯＦＦしても、次回必ずＨＤＤより自己消去プログラムを起動しＨＤＤ消去を続ける。その際はＦＤＤなど他のデバイスからの起動、ユーザーインターフェース使用も抑止する。ユーザーインターフェースも抑止（使用不能）するのでＢＩＯＳセットアップに入って起動順を操作することも不可能にする。これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることが可能となる。
【選択図】図１



【特許請求の範囲】
【請求項１】
情報処理装置内に設置されて、プログラム、データを記録可能な第１の記録媒体と、
前記情報処理装置内に設置されて、前記情報処理装置起動時にパスワードを入力、照合するプログラムを記録した第２の記録媒体と、
を備え、
前記パスワードを所定回数誤入力すると、前記第１の記録媒体に自己消去プログラムを設定し、当該自己消去プログラムによって前記第１の記録媒体に記録されたプログラム、データを自己消去することを特徴とする情報処理装置のセキュリティ装置。
【請求項２】
情報処理装置内に設置されて、プログラム、データを記録可能な第１の記録媒体と、
前記情報処理装置内に設置された時計と、
前記情報処理装置内に設置されて、前記情報処理装置の終了時刻を記録する第３の記録媒体と、
を備え、
前記情報処理装置の起動時刻と前回終了時刻の時間差が所定時間を越えたと判断した場合には前記第１の記録媒体に自己消去プログラムを設定し、当該自己消去プログラムによって前記第１の記録媒体に記録されたプログラム、データを自己消去することを特徴とする情報処理装置のセキュリティ装置。
【請求項３】
前記第１の記録媒体に一旦自己消去プログラムを設定すると、プログラム、データ消去動作を強制的に中断しても次回の前記情報処理装置の起動時には前記第１の記録媒体より設定した前記自己消去プログラムを再実行し、前記第１の記録媒体に記録されたプログラム、データを自己消去することを特徴とする請求項１または請求項２に記載の情報処理装置のセキュリティ装置。
【請求項４】
プログラム、データを記録可能な記録媒体を備えた情報処理装置のセキュリティ方法であって、
前記情報処理装置を起動し、ユーザーが入力したパスワードが正しいかどうかを判断するステップと、
正しくないパスワードを入力した場合はセキュリティ発動条件になったかを判断するステップと、
誤ったパスワードを所定回数続けて入力した場合には前記記録媒体に自己消去プログラムを設定し、前記自己消去プログラムにより前記記録媒体に記録したプログラム、データを消去するステップと、
を含む情報処理装置のセキュリティ方法。
【請求項５】
プログラム、データを記録可能な記録媒体を備えた情報処理装置のセキュリティ方法であって、
前記情報処理装置を起動した時刻を取得するステップと、
前記情報処理装置を前回終了した時刻を取得するステップと、
前記情報処理装置を前回終了時刻から起動した時刻までの時間差が所定時間を越えたかを判断するステップと、
前記所定時間を越えた場合には前記記録媒体に自己消去プログラムを設定し、前記自己消去プログラムにより前記記録媒体に記録したプログラム、データを消去するステップと、
を含む情報処理装置のセキュリティ方法。
【請求項６】
前記プログラム、データを消去するステップは、プログラム、データ消去動作を強制的に中断しても次回の前記情報処理装置の起動時には前記記録媒体より、設定した前記自己消去プログラムを再実行し、前記記録媒体に記録したプログラム、データを消去する請求項

４または請求項５に記載の情報処理装置のセキュリティ方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、パーソナルコンピュータ（以下「ＰＣ」）を代表とする情報処理装置のセキュリティ装置およびセキュリティ方法に関する。
【背景技術】
【０００２】
近年、ノート型ＰＣのような携帯型の情報処理装置が一般に広く普及し、容易に屋外にそれらを持ち出せるようになった反面、それらの盗難、そして内部に記録された情報が漏洩する事件が多発し社会問題化している。このような課題に対して、一般に最近のＰＣにはセキュリティ機能を付加していることは衆知の事実である。
【０００３】
例えばＰＣの不正使用を防止するために、その起動時にはパスワードを入力、照合しないとＯＳ（オペレーティングシステム）が起動せずＰＣ自体の起動を拒否する。
【０００４】
また、個別情報へのアクセス時にはパスワードの正誤判定を一般的に行っている。しかし、パスワードは一定桁の英数字または記号からなるために、英数字を変化させながら繰り返しパスワードを入力して行けば、いずれは正しいパスワードと一致することとなる。従って、単にパスワード判定ステップを設けても解読される可能性は依然として高く、個別情報への不正アクセスを有効に防止することができない。
【０００５】
図６は従来技術である特許文献１に係るコンピュータの不正アクセス防止システムの動作を示すフローチャートである。
【０００６】
まず、ステップＡでは、使用者が、ＰＣの電源のＯＮを行う。ステップＢでは、ＰＣのパスワード確認処理部が、オペレーティングシステムを起動する前に、パスワード入力画面をディスプレイ装置に表示せしめ、使用者にパスワードの入力を促す。ここで、使用者は、パスワードを入出力装置であるキーボードから入力する。上記入力要求により、使用者がキーボードからパスワードを入力したならば、ステップＣにて、パスワード確認処理部は、上記入力されたパスワードを、予め設定されたパスワードと比較し、上記パスワードが不正な場合は、ステップＤにて、パスワード確認処理部がディスプレイ装置上に警告メッセージを表示した後、警告メッセージの表示回数のカウンタをカウントアップし、ステップＦにて、警告メッセージの表示回数が２回までならステップＢに戻して、再度、パスワードの入力を促す。あるいはステップＦにて、上記入力されたパスワードがキーボードから入力された３回目の不正なパスワードである場合、パスワード確認処理部はＰＣの電源をＯＦＦにする。
【０００７】
以上説明したように、ＯＳでは防止できなかったコンピュータへの不正なアクセスを、ＰＣの電源投入段階で防止することが可能となり、ＯＳを不正使用者によるファイルのコピーや削除の心配を無くして、安心して使用することが可能となる。
【０００８】
また、特許文献２のように情報処理装置の立ち上げ時、パスワードを比較し間違ったパスワード入力等不正なアクセスの試みと判断した場合、ＢＩＯＳのフラッショＲＯＭのプログラムを書き換え情報処理装置としての価値を減じせしめ、またＨＤＤ（ハードディスクドライブ）等の二次記憶装置の内容を破壊することにより情報の漏洩を防ぐ方法もある。
【０００９】
あるいは、特許文献３のように、無線選択呼出受信機に内蔵されたメモリの個別情報領

域への不正書き込み防止方法として、メモリには個別情報領域へのアクセスを可能にするためのパスワードが格納されており、入力されたパスワードと格納されたパスワードとの一致／不一致が判定され、不一致回数がカウンタによってカウントされる。不一致回数が所定値を超えると、メモリの所定部分の情報を消去し、以後、個別情報領域への情報書き込みを不可能にするといったものである。

【特許文献１】特開２００１－２７９１１号公報
【特許文献２】特開平１１－２５９３６９号公報
【特許文献３】特開２０００－７８１２７号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

しかしながら、上記従来の構成では、データセキュリティとしては十分とは言えない。上記のような特許文献１の従来の技術では、ＰＣなどの装置にデータを記録した媒体、例えばＨＤＤをＰＣに装着した状態において、一旦このＰＣ上でパスワード設定をすればＰＣ起動時にこのパスワードを正しく入力しない限り複数回の試行で電源が切れるため、結果的に媒体の内容を読み出すことは確かに不可能である。特許文献２，特許文献３では正しいパスワードを所定回数内に入力しない場合、読み出したいプログラム、データはＰＣなど本体装置によって消去されるため、より強力である。

【００１１】

しかし、上記特許文献１の従来技術ではパスワード入力の複数回の試行で電源が切れるとは言え、有限回数の試行によりパスワード解読は不可能ではなく、パスワードの解読によってＰＣ起動時に他のデバイスからＯＳ起動するなどの方法によりＨＤＤ内に記録したデータを不正に読み出すことは依然として可能である。また上記特許文献２にあるようにＨＤＤの消去を開始しても強制的にＰＣの電源をＯＦＦし、続いて同様の方法でパスワードを解読するか、ＨＤＤを取り出して他のＰＣに接続するなどの方法によってＨＤＤ内に記録したデータを不正に読み出すことも不可能ではない。

【００１２】

本発明は上記従来の課題を解決するもので、上記のような従来のＰＣの不正アクセス防止システムにおける問題点に鑑みてなされたものであり、ＰＣの電源投入段階でＰＣ内部への不正なアクセスを防止することができ、さらに正しいパスワードを所定回数内に入力しない場合は、ＨＤＤ内のプログラム、データは自己消去するだけでなく、一旦、ＨＤＤ内の自己消去プログラムの発動がなされれば、たとえ消去中に電源ＯＦＦしても、次回、必ずＨＤＤより自己消去プログラムを起動しＨＤＤ消去を続ける。その際はＦＤＤなど他のデバイスからの起動、ユーザーインターフェース使用も抑止する。ユーザーインターフェースも抑止（使用不能）するのでＢＩＯＳセットアップに入って起動順を操作することも不可能にする。これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることが可能となる。

【課題を解決するための手段】

【００１３】

本発明の請求項１に記載の発明は、
情報処理装置内に設置されて、プログラム、データを記録可能な第１の記録媒体（例えば図１のＨＤＤ１０６）と、
前記情報処理装置内に設置されて、前記情報処理装置起動時にパスワードを入力設定するプログラムを記録した第２の記録媒体（例えば図１のＢＩＯＳを記録したフラッシュメモリ１０８）と、
を備え、
前記パスワードを所定回数誤入力すると、前記第１の記録媒体に自己消去プログラムを設定し、当該自己消去プログラムによって前記第１の記録媒体に記録されたプログラム、データを自己消去することを特徴とする情報処理装置のセキュリティ装置
としたものであり、ＨＤＤ内のプログラム、データを完全消去することによりセキュリテ

ィは強化され、これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることが実現できる。

【００１４】

本発明の請求項２に記載の発明は、

情報処理装置内に設置されて、プログラム、データを記録可能な第１の記録媒体（例えば図１のＨＤＤ１０６）と、

前記情報処理装置内に設置された時計（例えば図１のＲＴＣ（リアルタイムクロック）１１２）と、

前記情報処理装置内に設置されて、前記情報処理装置の終了時刻を記録する第３の記録媒体（例えば図１のＣＭＯＳ１０９）と、

を備え、

前記情報処理装置の起動時刻と前回終了時刻の時間差が所定時間を越えたと判断した場合には前記第１の記録媒体に自己消去プログラムを設定し、当該自己消去プログラムによって前記第１の記録媒体に記録されたプログラム、データを自己消去することを特徴とする情報処理装置のセキュリティ装置

としたものである。

【００１５】

本発明の請求項４に記載の発明は、

プログラム、データを記録可能な記録媒体を備えた情報処理装置のセキュリティ方法であって、

前記情報処理装置を起動し、ユーザーが入力したパスワードが正しいかどうかを判断するステップ（例えば図３のＳ０５）と、

正しくないパスワードを入力した場合はセキュリティ発動条件になったかを判断するステップ（例えば図３のＳ０６）と、

誤ったパスワードを所定回数続けて入力した場合には前記記録媒体に自己消去プログラムを設定し、前記自己消去プログラムにより前記記録媒体に記録したプログラム、データを消去するステップ（例えば図３のＳ０７）と、

を含む情報処理装置のセキュリティ方法

としたものであり、ＨＤＤ内のプログラム、データを完全消去することによりセキュリティは強化され、これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることが実現できる。

【００１６】

本発明の請求項５に記載の発明は、

プログラム、データを記録可能な記録媒体を備えた情報処理装置のセキュリティ方法であって、

前記情報処理装置を起動した時刻を取得するステップ（例えば図４のＳ３２）と、

前記情報処理装置を前回終了した時刻を取得するステップ（例えば図４のＳ３３）と、

前記情報処理装置を前回終了時刻から起動した時刻までの時間差が所定時間を越えたかを判断するステップ（例えば図４のＳ３４）と、

前記所定時間を越えた場合には前記記録媒体に自己消去プログラムを設定し、前記自己消去プログラムにより前記記録媒体に記録したプログラム、データを消去するステップ（例えば図４のＳ３５）と、

を含む情報処理装置のセキュリティ方法

としたものである。

【発明の効果】

【００１７】

以上のように、本発明によれば、不正アクセスによりＨＤＤ自己消去発動がなされるとＨＤＤ内に記録したプログラム、データを自己消去するだけでなく、ＨＤＤ内の自己消去プログラムは一旦、自己消去発動がなされれば、たとえ消去中に電源ＯＦＦしても、次回、必ずＨＤＤより自己消去プログラムを起動しＨＤＤ消去を続ける。その際はＦＤＤなど

他のデバイスからの起動、ユーザーインターフェース使用も抑止する。ユーザーインターフェースも抑止（使用不能）するのでＢＩＯＳセットアップに入って起動順を操作することも不可能にする。ＨＤＤ内のプログラム、データを完全消去することによりセキュリティは強化され、これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることができる。

【発明を実施するための最良の形態】

【００１８】

以下、本発明を実施するための最良の形態について図１を用いて説明する。

【００１９】

（実施の形態１）

図１は実施の形態１に係る一般的なＰＣのハードウエア構成図である。

【００２０】

図１において１０１はマザーボードであり、ＰＣを構成する主要なパーツを固定したり装着するためのパーツである。１０２はＣＰＵ（中央演算処理装置）、１０３，１０４はチップセットと呼ばれノースブリッジ１０３はＣＰＵ１０２とメモリ、グラフィックチップの間を流れるデータを制御する。サウスブリッジ１０４は、ＨＤＤ１０６，ＣＤ／ＤＶＤドライブ１０７をつなぐＡＴＡ（ＩＤＥ）インターフェース１０５、キーボードやマウスのインターフェース、拡張カード（ＬＡＮカードやサウンドカードなどのＰＣＩスロット）、その他のインターフェイス間を流れるデータの制御を行う。１０８は不揮発性のフラッシュメモリであり、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）と呼ばれるＰＣに接続されているＨＤＤ１０６やＣＤ／ＤＶＤ１０７、ＦＤＤ（フロッピディスクドライブ、記載せず）などのディスクやキーボード、グラフィックチップなどのデバイスをコントロールするプログラム群が組み込まれている。ＢＩＯＳはユーザーのよりＰＣの起動直後に所定のキーを押すことによりセットアップメニューを呼び出し、設定内容を変更することができる。設定した内容はサウスブリッジ１０４内のＣＭＯＳ領域にあるＣＭＯＳ１０９に記憶し、コイン電池１１０でバックアップするので電源を切っても保持され、消えることはない。

【００２１】

以上のように構成されたＰＣのデータセキュリティ装置関して図１を用いてその動作を説明する。

【００２２】

セキュリティのためにＰＣ起動時にパスワードを設定する。図２（ａ）はパスワードの入力画面である。正しいパスワードを入力、照合すると、ハードディスクの先頭に置かれ、ハードディスク内に収められたどのＯＳをどのように起動するかなどの情報が記録されているマスターブートレコード（ＭＢＲ）が読み込まれ、ブートローダと呼ばれるプログラムが動作する。ブートローダはハードディスク内の領域の位置や大きさなどを記録したパーティションテーブルを読み込み、起動するパーティションのブートセクタと呼ばれる領域を読み込む。ブートセクタに置かれたプログラムは、そのパーティションに置かれたＯＳを起動する。

【００２３】

（１）正しいパスワードが設定されない場合は図２（ｂ）ような「パスワードが正しくありません」のメッセージが画面に出力され上記のような動作は行われない。さらに正しいパスワードが所定回数設定されない場合はＰＣの不正アクセスとして認識され、セキュリティ機能が発動され以下の動作を行う。なお、図２の例では３回までは（ａ）－（ｂ）を繰り返す。

（２）図２（ｃ－１）の例では４回目のパスワード誤入力には「パスワードが正しくありません。システム管理者に連絡して下さい。」のメッセージが画面に出力され、上記のような（ａ）－（ｂ）の繰り返し動作は行われない。

（３）しばらくすると続けて図２（ｃ－１）の表示から図２（ｃ－２）のように「不正なアクセスが行われました。シャットダウンします。」の表示とともに電源が自動的にシャ

ットダウンモードになる。
（４）さらにシャットダウンしたＰＣを再度（５回目）に起動しパスワード誤入力すれば対象ＨＤＤ１０６内のＭＢＲ１１１を書き換え、ＯＳ起動を抑止する。ＭＢＲ１１１に自己消去プログラムを設定し、ＨＤＤ自己消去機能の発動を示す図２（ｄ）のような「不正なアクセスが行われました。ＨＤＤの消去を開始します。」などのメッセージを表示して自動的に再起動（ハードウエアリセット）し、ＨＤＤ全体のプログラム、データの消去を開始する。ＨＤＤ１０６上には、ＨＤＤを工場出荷時と同じ状態に戻すリカバリー領域も存在するが、これも含め完全に消去した状態になる。
【００２４】
たとえ消去中に電源ＯＦＦしても、ＢＩＯＳは自己消去プログラムを発動させたことを記憶しており、ＦＤＤなど他のデバイスからの起動、パスワード入力を含む全てのユーザーインターフェース使用を抑止し、ＨＤＤからのみ起動するよう制御するため必ず書き換えたＭＢＲ１１１を経由して自己消去プログラムを実行しＨＤＤ消去を続ける。発動後はユーザーインターフェースが抑止され、使用不能となるのでＢＩＯＳセットアップに入って起動順を操作することも不可能である。
【００２５】
なお、上記所定回数設定を図２の例では（ａ）－（ｂ）の繰り返す回数は３回とし、４回目で警告、５回目でＨＤＤ自己消去発動としたが、これらの回数はＢＩＯＳによるユーザー設定より変更可能である。
【００２６】
ＨＤＤ自己消去発動は以下の場合である。
「１」起動時のパスワードを所定回数間違えたとき。
但し、ＰＣ管理者は上記所定回数およびＨＤＤ自己消去機能自体の有効／無効の設定を変更できる。
「２」休止状態から復帰後もＢＩＯＳのパスワードを聞くようにしてＨＤＤ自己消去発動条件の対象とする。
「３」ＢＩＯＳセットアップに入るパスワードもＨＤＤ自己消去発動条件の対象とする。
「４」パスワードが入力されない場合は所定時間経過後シャットダウンするが、この場合は上記所定回数としてカウントされない。
【００２７】
以上のように本実施の形態によれば、不正アクセスによりＨＤＤ自己消去発動がなされるとＨＤＤ内に記録されたプログラム、データを自己消去するだけでなく、ＨＤＤ内の自己消去プログラムは一旦、自己消去発動がなされれば、たとえ消去中に電源ＯＦＦしても、次回、必ずＨＤＤより自己消去プログラムを起動しＨＤＤ消去を続ける。その際はＦＤＤなど他のデバイスからの起動、ユーザーインターフェース使用も抑止する。ユーザーインターフェースも抑止（使用不能）するのでＢＩＯＳセットアップに入って起動順を操作することも不可能である。ＨＤＤ内のプログラム、データを完全消去することによりセキュリティは強化され、これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることができる。
【００２８】
なお、ＨＤＤの自己消去発動をした時間をＭＢＲに証拠として記録してもよい。
【００２９】
また、消去中に「ＨＤＤを消去中です。」、消去終了後に「ＨＤＤを完全消去しました。」などのメッセージをＭＢＲの自己消去プログラムを設定してもよい。消去終了後は、メッセージは表示したままで、この状態で電源をオフして、再度電源をＯＮしてもＨＤＤ以外の装置は起動せず、続けてＭＢＲの自己消去プログラムを実行し、消去中、消去終了後のメッセージを表示する。メッセージは表示だけでなく、音声によるメッセージであってもよい。
【００３０】
また、ＢＩＯＳはＨＤＤ自己消去発動したことを記憶しているので、ＨＤＤをはずした

状態でＰＣを起動してもＨＤＤがないことを検出してシャットダウンしてもよい。この状態で他の異なるＨＤＤに差し替えてもＢＩＯＳによりＨＤＤに自己消去プログラムを再設定し、ＨＤＤ自己消去を行うようにすればＨＤＤのデータ漏洩以外にもＰＣ自体の再使用も制限できる。

【００３１】

また、ユーザーインターフェースも禁止するので、ＢＩＯＳセットアップに入って起動順を操作することも不可能にすることは既に述べた。

【００３２】

また、図２の例では（ａ）－（ｂ）の繰り返す回数は３回とし、４回目で警告、５回目でＨＤＤ自己消去発動としたが、これらの誤入力の容認回数はＢＩＯＳによるユーザー設定が可能であることは既に述べた。この時パスワードの誤入力時には警告音を発し、音色はその回数により音の周波数、トーン、音量をかえてもよい。

【００３３】

また、パスワードは設定時に所定文字数以上であること、できるだけ多くの文字種を複雑に組み合わせ、類推しにくくすることが望ましい。

【００３４】

また、ＨＤＤ自己消去機能自体の有効／無効の設定を変更できるとしてもよい。

【００３５】

また、本実施の形態では情報処理装置としてＰＣとＰＣ内蔵のＨＤＤを中心につて述べたがこれに限るものではなく、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）、ゲーム機、ＨＤＤ内蔵ＤＶＤレコーダであってもよい。また、ＨＤＤに限らず半導体メモリ、記録型ＤＶＤのような書き換え可能な記録媒体であってもよいことは言うまでもない。

【００３６】

（実施の形態２）

図３は実施の形態２に係る本発明の情報処理装置のセキュリティ方法に関するフローチャートである。

【００３７】

以下、図３に従って本発明の情報処理装置のセキュリティ方法について説明する。

【００３８】

ＰＣがシャットダウン／休止状態（Ｓ０１）から起動して、パスワードが設定されているかを判断し（Ｓ０２）、パスワードが設定されていればパスワードの入力をユーザーに促す（Ｓ０３）。パスワードが正しいかどうかを判断して（Ｓ０４）、正しくないパスワードが入力された場合はセキュリティ発動条件になったかを判断する（Ｓ０５）。誤ったパスワードが所定回数続けて入力された場合にはセキュリティ発動条件であるとの判断からＨＤＤのＭＢＲを書き換え、ＭＢＲに自己消去プログラムを設定し、ＨＤＤ自己消去機能の発動し、ＨＤＤ内のプログラム、データ全体の消去を開始する（Ｓ０６）。Ｓ０６で一旦このステップに入ると、たとえ消去中に電源ＯＦＦしても、次回必ずＨＤＤより自己消去プログラムを起動しＨＤＤ消去を続ける。その際はＦＤＤなど他のデバイスからの起動、ユーザーインターフェース使用も抑止する。ユーザーインターフェースも抑止（使用不能）するのでＢＩＯＳセットアップに入って起動順を操作することも不可能にする。

【００３９】

Ｓ０５で誤ったパスワード入力が所定回数に達しない場合は図２（ｂ）のように再度正しいパスワードを入力するように促す。

【００４０】

また、正しいパスワードが所定回数内に入力された場合は誤り回数のカウント内容をクリアし（Ｓ０７）、通常起動を行いＯＳ起動する（Ｓ０８）。

【００４１】

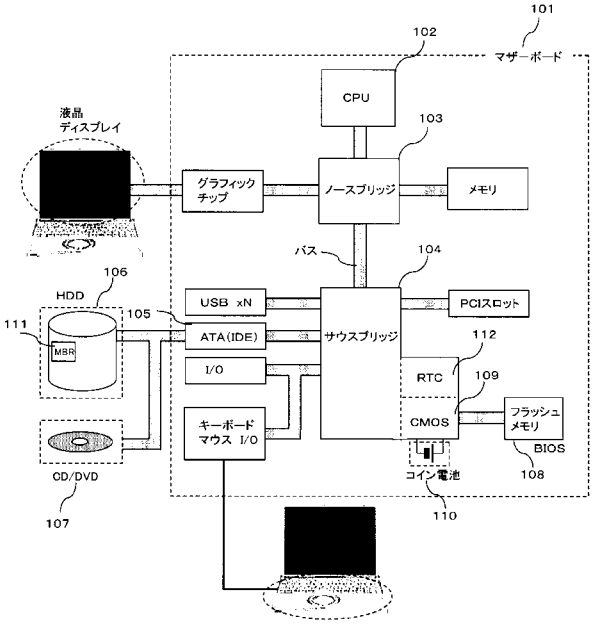
パスワードが設定されていないと判断すると（Ｓ０２）、セキュリティのためユーザーにパスワードを設定するよう促し（Ｓ０９）、通常起動に移行する（Ｓ１０）。

【００４２】
以上、実施の形態２に係る本発明の情報処理装置のセキュリティ方法（波線内）である。
【００４３】
このようにすることで、パスワードの誤入力からＰＣの不正アクセスと判断されるとＨＤＤ自己消去発動がなされ、ＨＤＤ内のプログラム、データを完全消去することによりセキュリティは強化され、ＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることができる。
【００４４】
（実施の形態３）
図１は実施の形態１同様、実施の形態３に係る一般的なＰＣのハードウエア構成図である。
【００４５】
図１において１１２はサウスブリッジ１０４に内蔵されたＲＴＣ（リアルタイムクロック）であり、ＣＭＯＳ１０９と同様にコイン電池１１０で動作するので電源を切っても時間（年日時分秒）を刻み続けることができる。またはＣＭＯＳにＰＣが終了した時間を保持させることも可能である。その他については実施の形態１と同様の構成である。
【００４６】
以上のように構成されたＰＣのデータセキュリティ装置関して図１を用いてその動作を説明する。
【００４７】
以下、実施の形態３について説明する。
【００４８】
盗難にあったＰＣにパスワードが設定されていれば一般には使用は困難であり、窃盗犯の心理として次の行為として譲渡、転売、放置といったものが考えられる。いずれにしてもパスワードを知り得ない限りＯＳまで起動することはできない。そこでＰＣのＯＳ終了処理時にその終了時刻（年日時分秒）を記録しておく。ＰＣを数日、数週、さらに数ヶ月、数年単位で使用されない状態が継続し再び起動された場合にその使用されなかった時間が所定時間をこえていれば窃盗にあったＰＣと判断し実施の形態１同様、セキュリティ発動条件であるとの判断からＨＤＤのＭＢＲを書き換え、ＭＢＲに自己消去プログラムを設定し、ＨＤＤ自己消去機能の発動し、ＨＤＤ内のプログラム、データ全体の消去を開始する。仮に窃盗にあったＰＣではなくても長期間使われなかったＰＣであり，ＨＤＤ内のプログラム、データは有用でないものとして消去しても問題は少ない。
【００４９】
なお、ＰＣ管理者は上記所定時間、不使用時間によるＨＤＤ自己消去機能自体の有効／無効の設定を変更することができる。
【００５０】
図４は実施の形態３に係る本発明の情報処理装置のセキュリティ方法に関するフローチャートである。
【００５１】
以下、図４に従って本発明の情報処理装置のセキュリティ方法について説明する。
【００５２】
ＰＣがシャットダウン／休止状態（Ｓ３１）から起動して、ＲＴＣ１１２からＰＣの起動時刻を取得する（Ｓ３２）。次に前回ＰＣを終了した時刻をＣＭＯＳ１０９から読み出して取得し（Ｓ３３）、前回終了時から所定年日数以上経過しているかを判断する（Ｓ３４）。所定時間以上経過していればセキュリティ発動条件であるとの判断しＨＤＤ内のプログラム、データ全体の消去を開始する。
【００５３】
所定時間以上経過していなければ、通常起動（Ｓ３６）動作をする。実施の形態２の機能を併用する場合はでは図３のＳ０３から実行する。

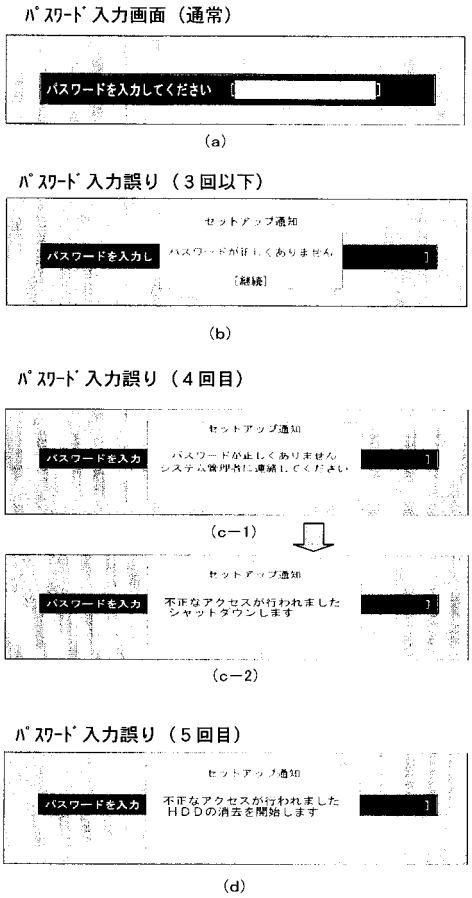
【００５４】
正しくＰＣ起動し、終了処理時には（Ｓ３７）、終了日時を記録し（Ｓ３８）、終了する（Ｓ３９）。
【００５５】
このようにすることで、一定期間使用されなかったＰＣは盗難にあったＰＣとの判断からＨＤＤ自己消去発動がなされ、ＨＤＤ内のプログラム、データを完全消去することによりセキュリティは強化され、ＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることができる。
【００５６】
（実施の形態４）
さらに、ＰＣからＨＤＤを取り外し、セットしていたものとは異なるＰＣや他の装置に取り付けて、ＨＤＤ内に記録されたデータを不正に読み出すことは依然として可能である。
【００５７】
図５はＨＤＤの接続端子面の一例でありＡＴＡ（ＩＤＥ）端子、設定用ジャンパ端子、電源コネクタを接続する端子が示されている。（ＡＴＡ（ＩＤＥ）端子に関して、近年はシリアルＡＴＡのような新たな規格が普及しつつありこのような態様をなしていないものも多い。）
電源コネクタよりＨＤＤに電源供給し、ＨＤＤが記録しているプログラム、データをＡＴＡ端子より不正に読み出しを行うのであるが、一旦ＨＤＤが自己消去モードになればセットしていたものとは異なるＰＣや他の装置を使って電源コネクタよりＨＤＤに電源供給しても、この時点でＨＤＤ単独で自己消去プログラムを実行し、記録しているプログラム、データを自己消去することも可能である。この機能を実現するために以下のシステム構築をする。
【００５８】
(i)ＨＤＤ内の制御回路部の一部を構成するマイクロコンピュータ（マイコン）のプログラム(ファームウェア)に自己消去プログラムを実装する。
(ii)不正アクセスによって、ＢＩＯＳより自己消去モードに移行する指令をＨＤＤのマイコンが受信し、ファームウェアを記憶するフラッシュＲＯＭの一部、またはＨＤＤの磁気ディスク上の未使用領域にこれを記憶しておく。ＨＤＤの未使用領域を使う場合は、一般のＯＳやデータ、プログラムによって書き換えられたりできないような領域である必要がある。
(iii)自己消去モードであれば、ＨＤＤの電源供給と同時にファームウェア上の自己消去プログラムを強制的に実行し、ＨＤＤに記録しているプログラム、データを自己消去する。
【００５９】
上記のようなシステムを構築することで、ＰＣからＨＤＤを取り外し、セットしていたものとは異なるＰＣや他の装置に取り付けて中に記録されたデータを不正に読み出そうとしても、一旦ＨＤＤが自己消去モードになればＨＤＤ単独で自己消去プログラムを実行する。これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることが可能となる。
【産業上の利用可能性】
【００６０】
本発明にかかる情報処理装置のセキュリティ装置およびセキュリティ方法は、ＨＤＤ内のプログラム、データを完全消去することによりセキュリティは強化され、これにより不正アクセスによるＨＤＤなどの記録媒体のデータ漏洩防止をさらに強固なものにすることができ、パーソナルコンピュータを代表とする情報処理装置のセキュリティ装置およびセキュリティ方法に好適である。
【図面の簡単な説明】
【００６１】

【図１】本発明の実施の形態１に係る一般的なＰＣのハードウエア構成図
【図２】（ａ）パスワードの入力画面を示す図、（ｂ）再度正しいパスワードを入力するように促すパスワード入力画面を示す図、（ｃ－１）（ｃ－２）所定回数以上のパスワード誤入力したときの画面を示す図（ｄ）ＨＤＤ自己消去機能の発動を示す画面の図
【図３】本発明の実施の形態２に係る本発明の情報処理装置のセキュリティ方法に関するフローチャート
【図４】本発明の実施の形態３に係る本発明の情報処理装置のセキュリティ方法に関するフローチャート
【図５】ＨＤＤの接続端子面の一例の図
【図６】従来技術である特許文献１に係るコンピュータの不正アクセス防止システムの動作を示すフローチャート
【符号の説明】
【００６２】
１０１　マザーボード
１０２　ＣＰＵ
１０３　ノースブリッジ
１０４　サウスブリッジ
１０５　ＡＴＡ（ＩＤＥ）インターフェース
１０６　ＨＤＤ（ハードディスクドライブ）
１０７　ＣＤ／ＤＶＤドライブ
１０８　フラッシュメモリ
１０９　ＣＭＯＳ
１１０　コイン電池
１１１　ＭＢＲ（マスターブートレコード）
１１２　ＲＴＣ（リアルタイムクロック）

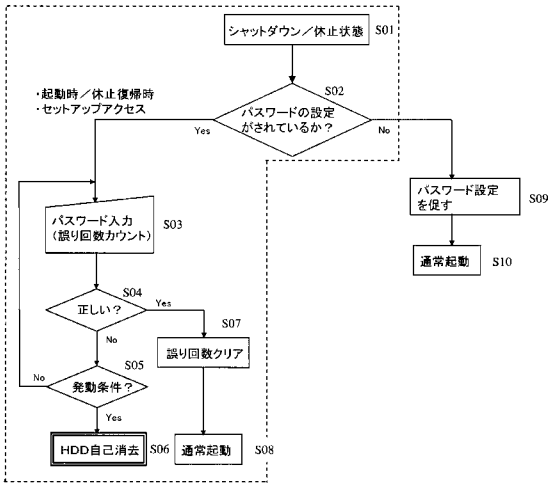
【図１】


101
マザーボード
102
CPU
液晶
ディスプレイ
103
グラフィック
チップ
ノースブリッジ
メモリ
バス
104
106
HDD
105
USB xN
PCIスロット
111
MBR
ATA(IDE)
サウスブリッジ
112
I/O
RTC
109
キーボード
マウス I/O
CMOS
フラッシュ
メモリ
BIOS
CD/DVD
コイン電池
108
107
110

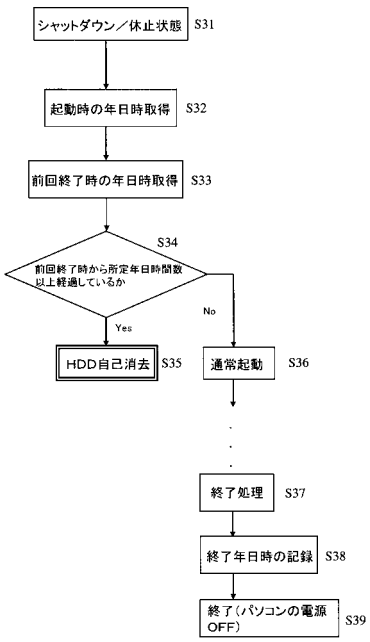
【図２】


ﾊﾟｽﾜｰﾄﾞ入力画面（通常）
パスワードを入力してください
(a)
ﾊﾟｽﾜｰﾄﾞ入力誤り（３回以下）
セットアップ通知
パスワードを入力し
パスワードが正しくありません
[継続]
(b)
ﾊﾟｽﾜｰﾄﾞ入力誤り（４回目）
セットアップ通知
パスワードを入力
パスワードが正しくありません
システム管理者に連絡してください
(c－1)
セットアップ通知
パスワードを入力
不正なアクセスが行われました
シャットダウンします
(c－2)
ﾊﾟｽﾜｰﾄﾞ入力誤り（５回目）
セットアップ通知
パスワードを入力
不正なアクセスが行われました
ＨＤＤの消去を開始します
(d)

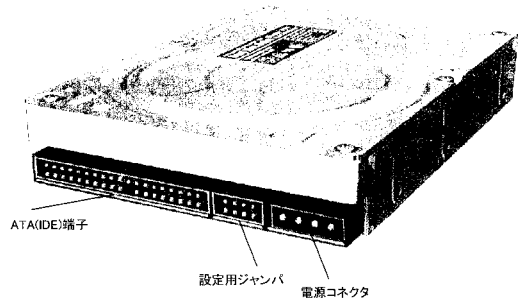
【図３】


シャットダウン／休止状態
S01
・起動時／休止復帰時
・セットアップアクセス
S02
パスワードの設定
がされているか？
Yes
No
パスワード設定
を促す
S09
パスワード入力
（誤り回数カウント）
S03
通常起動
S10
S04
正しい？
Yes
S07
No
誤り回数クリア
S05
No
発動条件？
Yes
HDD自己消去
S06
通常起動
S08

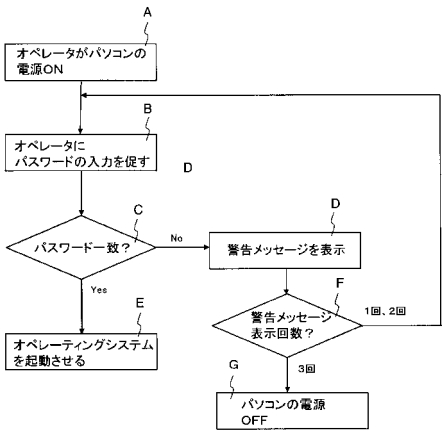
【図４】


シャットダウン／休止状態
S31
起動時の年日時取得
S32
前回終了時の年日時取得
S33
S34
前回終了時から所定年日時間数
以上経過しているか
No
Yes
HDD自己消去
S35
通常起動
S36
終了処理
S37
終了年日時の記録
S38
終了（パソコンの電源
OFF）
S39

【図５】


ATA(IDE)端子
設定用ジャンパ
電源コネクタ

【図６】


A
オペレータがパソコンの電源ON
B
オペレータにパスワードの入力を促す
D
C
パスワード一致？
No
D
警告メッセージを表示
Yes
F
警告メッセージ表示回数？
1回、2回
E
オペレーティングシステムを起動させる
3回
G
パソコンの電源OFF

フロントページの続き

(72)発明者　奥田　秀人
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　野口　直人
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考) 5B017 AA03　BA05　BA08　BB10　CA15　CA16