

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4060032号
(P4060032)

(45) 発行日 平成20年3月12日(2008.3.12)

(24) 登録日 平成19年12月28日(2007.12.28)

(51) Int.Cl. F I
G 1 1 B 20/10 (2006.01) G 1 1 B 20/10 H
H O 4 L 9/10 (2006.01) G 1 1 B 20/10 F
 H O 4 L 9/00 6 2 1 A

請求項の数 10 (全 12 頁)

| | |
|--|---|
| <p>(21) 出願番号 特願2000-391019 (P2000-391019) (22) 出願日 平成12年12月22日 (2000.12.22) (65) 公開番号 特開2002-197787 (P2002-197787A) (43) 公開日 平成14年7月12日 (2002.7.12) 審査請求日 平成16年11月9日 (2004.11.9)</p> | <p>(73) 特許権者 000006747 株式会社リコー 東京都大田区中馬込 1 丁目 3 番 6 号 (74) 代理人 100080931 弁理士 大澤 敬 (72) 発明者 須賀 智 東京都大田区中馬込 1 丁目 3 番 6 号 株式 会社リコー内 審査官 高野 美帆子</p> |
|--|---|

最終頁に続く

(54) 【発明の名称】 情報記録装置と情報記録方法

(57) 【特許請求の範囲】

【請求項 1】

所定の暗号化処理によって暗号化された暗号化情報と該暗号化情報を解読するための暗号化キーとを記録用の情報に変換する記録用情報変換手段と、該手段によって変換された記録用の情報を記録媒体に記録する情報記録手段とを備えた情報記録装置において、

読み出し専用メモリとCPUとを設け、

前記CPUが前記読み出し専用メモリからロードされた制御手順プログラムの実行によって、前記記録用情報変換手段によって暗号化情報と暗号化キーを記録用の情報に変換するとき、前記暗号化キーを無効情報に変換する無効情報変換手段を実現するようにしたことを特徴とする情報記録装置。

【請求項 2】

所定の暗号化処理によって暗号化された暗号化情報と該暗号化情報を解読するための暗号化キーとを記録用の情報に変換する記録用情報変換手段と、該手段によって変換された記録用の情報を記録媒体に記録する情報記録手段とを備えた情報記録装置において、

読み出し専用メモリとCPUとを設け、

前記CPUが前記読み出し専用メモリからロードされた制御手順プログラムの実行によって、前記記録用情報変換手段によって暗号化情報と暗号化キーを記録用の情報に変換するとき、前記暗号化キーを含む複数領域の情報を無効情報に変換する無効情報変換手段を実現するようにしたことを特徴とする情報記録装置。

【請求項 3】

請求項 2 記載の情報記録装置において、

前記記録媒体に前記無効データに変換された暗号化キーを含む複数領域の情報を記録した後、該情報内の暗号化キー以外の部分の情報を無効情報に変換しないで再記録するように制御する再記録制御手段を設けたことを特徴とする情報記録装置。

【請求項 4】

請求項 3 記載の情報記録装置において、

該情報記録装置の全体制御を司る手段と共に前記再記録制御手段を改変不可能に設けたことを特徴とする情報記録装置。

【請求項 5】

請求項 3 記載の情報記録装置において、

該情報記録装置の全体制御を司る手段を更新可能に、前記再記録制御手段を改変不可能にそれぞれ設けたことを特徴とする情報記録装置。

10

【請求項 6】

請求項 4 又は 5 記載の情報記録装置において、

固有の識別情報を付与して前記再記録制御手段を改変不可能に設け、前記識別情報に基づいて認証された前記再記録制御手段の制御のみを実行させる手段を設けたことを特徴とする情報記録装置。

【請求項 7】

請求項 5 又は 6 記載の情報記録装置において、

該情報記録装置の中央処理手段内に前記再記録制御手段を改変不可能に設けたことを特徴とする情報記録装置。

20

【請求項 8】

所定の暗号化処理によって暗号化された暗号化情報と該暗号化情報を解読するための暗号化キーとを記録用の情報に変換し、該変換された記録用の情報を記録媒体に記録する情報記録方法において、

読み出し専用メモリからロードされた制御手順プログラムの実行によって、前記暗号化情報と暗号化キーを記録用の情報に変換するとき、前記暗号化キーを無効情報に変換することを特徴とする情報記録方法。

【請求項 9】

所定の暗号化処理によって暗号化された暗号化情報と該暗号化情報を解読するための暗号化キーとを記録用の情報に変換し、該変換された記録用の情報を記録媒体に記録する情報記録方法において、

30

読み出し専用メモリからロードされた制御手順プログラムの実行によって、前記暗号化情報と暗号化キーを記録用の情報に変換するとき、前記暗号化キーを含む複数領域の情報を無効情報に変換することを特徴とする情報記録方法。

【請求項 10】

請求項 9 記載の情報記録方法において、

前記記録媒体に前記無効データに変換された暗号化キーを含む複数領域の情報を記録した後、該情報内の暗号化キー以外の部分の情報を無効情報に変換しないで再記録することを特徴とする情報記録方法。

40

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、記録媒体に情報を記録する情報記録装置とその情報記録方法とに関する。

【0002】

【従来の技術】

記録媒体上の情報に対する不正な複製（コピー）を防止するために様々な技術があった。

例えば、記録媒体に複製が困難な複製防止パターンを付加し、その記録媒体から不正に情報を複製した記録媒体の再生時には複製防止パターンを検出できないことによって再生

50

を禁止する情報再生装置（例えば、特開平 8 - 1 0 2 1 3 3 号公報参照）や、オリジナルの記録媒体には電子透かし処理を施した情報を記録し、他の記録媒体にはオリジナルの記録媒体の電子透かし処理を施した情報を記録できないようにすることによって再生時に電子透かし処理を行った情報が検出されないと再生しないようにした情報再生装置（例えば、特開平 1 1 - 1 7 6 0 9 0 号公報参照）や、記録媒体への情報記録時に情報内に不正記録を禁止するフラグを設けて、そのフラグを検出しなかったときには再生を禁止する情報再生装置（例えば、特開平 8 - 1 4 7 7 0 4 号公報参照）などがあつた。

【 0 0 0 3 】

しかしながら、上記複製が困難な複製防止パターンを付加した記録媒体は、上述のような専用の情報再生装置以外の再生装置では情報を再生することが可能になってしまう。

また、情報に電子透かし処理を施しても不正記録の際に再生に必要な情報は他の記録媒体に記録可能なので、上述のような電子透かし処理を行った情報の確認を行わないような情報再生装置では再生が可能になってしまう。

さらに、情報内に不正記録を禁止するフラグを設けても、情報記録装置を情報と共にフラグも記録してしまうように不正に改変してしまえば不正記録ができてしまって再生が可能になってしまう。

さらにまた、上述のような電子透かし及びフラグを必要とするために記録媒体上の情報記録容量も有効に利用することができなくなってしまう。

【 0 0 0 4 】

このように、上述のような記録媒体上の情報を不正に複製して使用することを防止する技術では、比較的容易に回避されてしまったり、データ記憶容量的にも効率的ではなかったりするという問題があつた。

そこで従来、情報にコンテンツ・スクランブル・システム（Contents Scramble System：CSS）等のような所定の暗号化処理を施し、その暗号化された情報と共に暗号を解読するための暗号化キーを記録媒体に記録するようにした情報記録装置が提案されている。

このような情報記録装置によってデータが記録された記録媒体は、暗号化されたデータを暗号化キーに基づいて暗号化前の状態に復元して再生することができる。

【 0 0 0 5 】

【 発明が解決しようとする課題 】

しかしながら、上述のような情報記録装置で作成された記録媒体は、暗号化されたデータと共に暗号化キーも他の記録媒体にコピーしてしまえば容易に解読して再生できるので、不正な複製を防止できなくなるという問題があつた。

この発明は上記の課題を解決するためになされたものであり、記録媒体上の暗号化キーによって保護されているデータを再生可能な状態で複製できないようにすることを目的とする。

【 0 0 0 6 】

【 課題を解決するための手段 】

この発明は上記の目的を達成するため、所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとを記録用の情報に変換する記録用情報変換手段と、その記録用情報変換手段によって変換された記録用の情報を記録媒体に記録する情報記録手段を備えた情報記録装置において、読み出し専用メモリとCPUとを設け、上記CPUが上記読み出し専用メモリからロードされた制御手順プログラムの実行によって、上記記録用情報変換手段によって暗号化情報と暗号化キーを記録用の情報に変換するとき、上記暗号化キーを無効情報に変換する無効情報変換手段を実現するようにしたものである。

また、所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとを記録用の情報に変換する記録用情報変換手段と、その記録用情報変換手段によって変換された記録用の情報を記録媒体に記録する情報記録手段を備えた情報記録装置において、読み出し専用メモリとCPUとを設け、上記CPUが上記読み出し専

10

20

30

40

50

用メモリからロードされた制御手順プログラムの実行によって、上記記録用情報変換手段によって暗号化情報と暗号化キーを記録用の情報に変換するとき、上記暗号化キーを含む複数領域の情報を無効情報に変換する無効情報変換手段を実現するとよい。

【0007】

さらに、上記のような情報記録装置において、上記記録媒体に上記無効データに変換された暗号化キーを含む複数領域の情報を記録した後、その情報内の暗号化キー以外の部分の情報を無効情報に変換しないで再記録するように制御する再記録制御手段を設けるとよい。

また、上記のような情報記録装置において、その情報記録装置の全体制御を司る手段と共に上記再記録制御手段を改変不可能に設けるとよい。

さらに、上記のような情報記録装置において、その情報記録装置の全体制御を司る手段を更新可能に、上記再記録制御手段を改変不可能にそれぞれ設けるとよい。

また、上記のような情報記録装置において、固有の識別情報を付与して上記再記録制御手段を改変不可能に設け、上記識別情報に基づいて認証された上記再記録制御手段の制御のみを実行させる手段を設けるとよい。

さらに、上記のような情報記録装置において、その情報記録装置の中央処理手段内に上記再記録制御手段を改変不可能に設けるとよい。

【0008】

また、所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとを記録用の情報に変換し、その変換された記録用の情報を記録媒体に記録する情報記録方法において、読み出し専用メモリからロードされた制御手順プログラムの実行によって、上記暗号化情報と暗号化キーを記録用の情報に変換するとき、上記暗号化キーを無効情報に変換する情報記録方法も提供する。

さらに、所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとを記録用の情報に変換し、その変換された記録用の情報を記録媒体に記録する情報記録方法において、読み出し専用メモリからロードされた制御手順プログラムの実行によって、上記暗号化情報と暗号化キーを記録用の情報に変換するとき、上記暗号化キーを含む複数領域の情報を無効情報に変換するとよい。

さらにまた、上記のような情報記録方法において、上記記録媒体に上記無効データに変換された暗号化キーを含む複数領域の情報を記録した後、その情報内の暗号化キー以外の部分の情報を無効情報に変換しないで再記録するとなおよい。

【0009】

【発明の実施の形態】

以下、この発明の実施形態を図面に基づいて具体的に説明する。

(1) この発明の第1実施形態

図1は、この発明の第1実施形態である光ディスク記録制御装置の構成を示すブロック図である。

この光ディスク記録制御装置(光ディスクドライブ)は、マイクロコンピュータによって実現され、主に外部のホストコンピュータから送られる所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとからなる情報(ユーザデータ)の入力と、そのユーザデータをブロック単位の記録用の情報(記録データ)に変換(エンコード)するデータ処理部1と、記録媒体であるCD-R/RW等の光ディスク4を回転し、光学的手段の半導体レーザ光源から出射した光ビームが光ディスク4上に形成されたトラックに追従するように制御しながら出射光の光量(発光パワー)を変動させて上記変換された記録データをピットとして記録する信号制御処理部2と、上記データ処理部1と信号制御処理部2の各ブロック動作を統括するコントローラ処理部3とからなる。

【0010】

次に、上記信号制御処理部2内の各ブロックを説明する。

スピンドル駆動部21は、サーボ22からの制御にしたがって光ディスク4を回転させ

10

20

30

40

50

、光ピックアップ部（PU）23内の図示を省略した半導体レーザ光源のレーザダイオード（LD）からレーザ光による光ビームを出射し、また同じく図示を省略した光受光器のフォトダイオード（PD）によって光ディスク4からの反射光を受光してRF信号として出力する。

アナログ信号処理部24は、PU23からのRF信号をサーボ22にわたし、サーボ22はそのRF信号に基づいてPU23、スピンドル駆動部21、光ピックアップ（PU）駆動部25の駆動をそれぞれ制御する。

光PU駆動部25は、PU23から出射された光ビームが光ディスク4上に形成されたトラックに追従するようにPU23を移動する。

LDドライバ26は、情報（データ）の記録時にデータ処理部1から送られる記録データのビットデータパターンにしたがってPU23内のLDを駆動して記録する。

【0011】

次に、上記データ処理部1内の各ブロックを説明する。

データ処理部1は、データの記録時にデジタル信号制御処理部11の制御により、ホストインタフェース（I/F）部12を介して外部のホストコンピュータから所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとからなるユーザデータを入力し、そのユーザデータをデータバッファ13に格納する。

さらに、データバッファ13内に一旦格納したユーザデータを記録用の情報である記録データのビットパターンデータにエンコードし、その記録データを信号制御処理部2のLDドライバ26へ送る。

【0012】

次に、上記コントローラ処理部3内の各ブロックを説明する。

CPU31は、エンジンインタフェース（I/F）部32を介してデータ処理部1と信号制御処理部2内の各ブロックを制御し、この光ディスク記録制御装置の全体を統括制御している。

また、CPU31が動作するための制御手順プログラムは書き換えて改変不可能な読み出し専用メモリ（ROM）33に格納されており、CPU31が動作するための動的な記憶領域として読み書き可能なメモリ（RAM）34があり、それらの各ブロックはバス35でデータ通信可能に接続されている。

【0013】

すなわち、上記データ処理部1が所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとを記録用の情報に変換する記録用情報変換手段の機能を、上記信号制御処理部2が上記記録用情報変換手段によって変換された記録用の情報を記録媒体に記録する情報記録手段の機能を果たす。

また、上記CPU31が上記ROM33からロードされた制御手順プログラムの実行によって、上記記録用情報変換手段によって暗号化情報と暗号化キーを記録用の情報に変換するとき、上記暗号化キーを無効情報に変換する無効情報変換手段の機能を実現する。

【0014】

次に、図1に示した光ディスク記録制御装置における情報記録処理である不正コピー防止記録処理について説明する。

この不正コピー防止記録処理は、所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとを記録用の情報に変換し、その変換された記録用の情報を記録媒体に記録する際、上記暗号化情報と暗号化キーを記録用の情報に変換するとき、上記暗号化キーを無効情報に変換することにより、暗号化データと暗号化キーとからなるユーザデータを他の光ディスクに不正にディスクコピーを行っても、暗号化キーのデータをそのまま記録できないようにすることができ、ユーザデータの不正利用を防止して保護することができる。

【0015】

図2は、図1に示した光ディスク記録制御装置におけるこの発明の請求項1及び請求項8に係わる不正コピー防止記録処理について示すフローチャート図であり、図1に示した

10

20

30

40

50

データ処理部 1 内のデジタル信号制御処理部 1 1 の詳細な制御動作手順とそれに対応したデータの流れの関係を示している。

デジタル信号制御処理部 1 1 は、同図の (a) と (b) に示すように、ステップ (図中「 S 」で示す) 1 でホスト I / F 部 1 2 を介して外部のホストコンピュータから所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとからなるユーザデータを入力して取り込み、そのユーザデータをデータバッファ 1 3 に随時格納する。

ステップ 2 でデータバッファ 1 3 に格納されたデータを光ディスク 4 に記録する記録データのビットパターンデータにエンコードするエンコード処理を実行し、エンコードされた記録データをデータバッファ 1 3 に随時格納する。このエンコードのとき、ユーザデータと共にエンコードされるブロックアドレスを記憶する。ステップ 3 で上記記憶したブロックアドレスに基づいて C S S キー (暗号化キー) を含むブロックアドレスか否かを判断する。

【 0 0 1 6 】

ステップ 3 の判断で暗号化キーが格納されるブロックアドレスでなければステップ 5 へ進んでエンコードされた記録データ (ビットパターンデータ) をそのまま L D ドライバ 2 6 へ出力して光ディスクに記録する。

一方、ステップ 3 の判断で暗号化キーを含むブロックアドレスであれば、ステップ 4 へ進んで C S S キーの部分が無効なビットパターンデータ (例えばすべて “ 0 ” であるユーザデータ) にエンコードして L D ドライバ 2 6 へ出力して光ディスクに記録する。

なお、上記ステップ 2 のエンコード処理前にステップ 3 の C S S キーを含むブロックアドレスか否かのチェック処理を行い、そのチェック処理で C S S キーが格納されるブロックアドレスと判断したときにはステップ 2 のエンコード処理を行わないようにしてもよい。

また、上記制御処理においてステップ 1 のユーザデータの取り込みと、ステップ 2 のエンコード処理の実行と、ステップ 3 ~ 4 あるいは 5 の処理はデータの流れるとともに動作するが、各ブロックが連続したデータを並列で処理する形態にしてもよい。

【 0 0 1 7 】

こうして、ある規定のブロックアドレスに暗号化キーが存在するような暗号化手法によって記録された光ディスク上のデータをそのまま他の光ディスクに記録しようとしても暗号化キーはコピーできないので、この光ディスク記録制御装置で記録された光ディスクを再生しても暗号解除が不可能になり、オリジナルの光ディスクの不正複製によるデータの不正利用を防止することができる。

このようにして、この発明の第 1 実施形態の光ディスク記録制御装置は、オリジナルの記録媒体に記録された暗号化データとそれを解読するための暗号化キーを他の記録媒体に不正に記録しようとしても、暗号化キーについては無効なデータにして記録してしまうので、記録後の暗号化データの解読が不可能になり、記録可能な光ディスクへの記録を行う際に、暗号化キーによって保護されているデータを再生可能な状態で記録してしまうことを回避 (コピープロテクション) することができる。

また、その制御プログラムを R O M に格納したので容易に改変して記録されることも防止できる。

【 0 0 1 8 】

(2) この発明の第 2 実施形態

第 1 実施形態の光ディスク記録制御装置の不正コピー防止記録処理は、暗号化キーがある決まった規定のブロックアドレスに存在する場合にのみ有効である。

そこで、第 2 実施形態の光ディスク記録制御装置の不正コピー防止記録処理では、データ処理部 1 が、図 2 に示したステップ 3 の判断でブロックアドレスが暗号化キーを格納されているとしているある規定のアドレスだけでなく、それを含んだ複数ブロックの領域 (複数領域) をチェックし、その複数領域のユーザデータを無効情報に変換する。

この場合、図 1 に示した光ディスク記録制御装置のデータ処理部 1 における処理が上述

10

20

30

40

50

の場合とは異なる。

すなわち、上記CPU31が上記ROM33からロードされた制御手順プログラムの実行によって、上記記録用情報変換手段によって暗号化情報と暗号化キーを記録用の情報に変換するとき、上記暗号化キーを含む複数領域の情報を無効情報に変換する無効情報変換手段の機能を実現する。

【0019】

次に、この第2実施形態の光ディスク記録制御装置におけるこの発明の請求項2及び請求項9に係わる不正コピー防止記録処理について説明する。

デジタル信号制御処理部11は、ホストI/F部12を介して外部のホストコンピュータから所定の暗号化処理によって暗号化された暗号化情報とその暗号化情報を解読するための暗号化キーとからなるユーザデータを入力して取り込み、そのユーザデータをデータバッファ13に随時格納する。

その後、データバッファ13に格納されたデータを光ディスク4に記録する記録データのビットパターンデータにエンコードするエンコード処理を実行し、エンコードされた記録データをデータバッファ13に随時格納する。このエンコードのとき、ユーザデータと共にエンコードされるブロックアドレスを記憶する。

そして、上記記憶したブロックアドレスに基づいて複数ブロックの領域のブロックアドレスにわたってCSSキー（暗号化キー）を含むか否かを判断する。

【0020】

上記判断で暗号化キーを含んでいなければ、エンコードされた記録データ（ビットパターンデータ）をそのままLDドライバ26へ出力して光ディスクに記録する。

一方、上記判断で暗号化キーを含んでいれば、CSSキーを含む複数のブロック領域のユーザデータを全て無効なビットパターンデータ（例えばすべて“0”であるユーザデータ）にエンコードしてLDドライバ26へ出力して光ディスクに記録する。

このようにして、この発明の第2実施形態の光ディスク記録制御装置は、暗号化キーのアドレス規定が異なる暗号化であったり光ディスク記録制御装置の製造後に規定が変更されたりしても、予め定めたブロック領域内であればデータ処理部1による処理を変更することがなく暗号化キーのコピーを防止することができる。

【0021】

(3) この発明の第3実施形態

第2実施形態の光ディスク記録制御装置の不正コピー防止記録処理では、暗号化キーのブロックアドレス周辺をすべて無効データで記録してしまうので、暗号化キー周辺にデータがあったとしてもそのデータは記録されなくなってしまうことになる。

そこで、第3実施形態の光ディスク記録制御装置の不正コピー防止記録処理では、暗号化キー以外の部分については無効化することなく再記録する。

この場合、図1に示した光ディスク記録制御装置のコントローラ処理部3の制御によってデータ処理部1が再記録の処理を行うところが上述の場合と異なる。

すなわち、上記コントローラ処理部3が、上記記録媒体に前記無効データに変換された暗号化キーを含む複数領域の情報を記録した後、その情報内の暗号化キー以外の部分の情報を無効情報に変換しないで再記録するように制御する再記録制御手段の機能を果たす。

【0022】

次に、この第3実施形態の光ディスク記録制御装置におけるこの発明の請求項3及び請求項10に係わる不正コピー防止記録処理について説明する。

上述のデータ処理部1による無効化データの記録後、コントローラ処理部3がデータ処理部1に対して特別な制御手順の処理を行うことにより、データ処理部1のデジタル信号制御処理部11は、データ処理部1による一連の制御手順では記録できない領域に対して記録を許可し、無効データに変換された暗号化キーを含む複数ブロック領域のデータ中で暗号化キー以外の部分のデータを無効化データに変換しないで再記録する。その際、コントローラ処理部3の処理において記録するユーザデータのアドレスチェックを行ってプログラムレベルで暗号化キーの記録を禁止する。

10

20

30

40

50

【 0 0 2 3 】

このコントローラ処理部 3 による特別な制御手順の処理は、上述のデータ処理部 1 の制御手順とは異なる手順であればどのような手順処理であってもよい。

このようにして、この発明の第 3 実施形態の光ディスク記録制御装置は、暗号化キーを含んだ領域をデータ処理部 1 による一連の制御手順処理によって無効データを記録後、コントローラ処理部 3 の CPU 3 1 の制御によって暗号化キー部以外をあらためて再記録するので、データ処理部 1 の製造後に暗号化キーのデータのアドレス規定が変更されても、プログラムの変更のみによって容易に暗号化キーのコピーを防止することができる。

【 0 0 2 4 】

(4) この発明の第 4 実施形態

第 3 実施形態の光ディスク記録制御装置では、プログラムの変更によって任意のブロックアドレスでの記録を可能にしてしまうので、悪意を持ったユーザが CPU 3 1 で暗号化キーを記録するように改変されたプログラムに変更した場合には暗号化キーの記録を回避できなくなる恐れがある。

そこで、コントローラ処理部 1 において、光ディスク記録制御装置の外部からの書き換えが不可能な ROM に記録したプログラムをロードした CPU によって上記特別な制御手順処理を実現するようにするとよい。

すなわち、上記 CPU 3 1 及び ROM 3 3 が、上記情報記録装置の全体制御を司る手段と共に上記再記録制御手段を改変不可能に設けたものである。

【 0 0 2 5 】

この光ディスク記録制御装置は、コントローラ処理部 3 での CPU 3 1 で動作するデータ処理部 1 に対する特別な制御手順処理を書き換え不能な ROM 3 3 にプログラムとして格納している。

このようにして、この発明の第 4 実施形態の光ディスク記録制御装置は、暗号化キー部をそのまま記録することを許可してしまうプログラムを特別な制御手順処理に混入させることができなくなり、プログラム製造後の悪意のプログラムの改変を防ぐことができる。

【 0 0 2 6 】

(5) この発明の第 5 実施形態

通常、製品として出荷後に光ディスク記録制御装置を制御する CPU のプログラムを性能向上やバグの修正などのために正規にアップデートすることがある。

しかし、上述のように書き換え不可能な ROM に光ディスク記録制御装置を制御するプログラムを格納するとアップデートが容易に行えなくなる。

そこで、暗号化キーのデータ部分を含むブロック領域に特別な制御手順処理以外のプログラムの部分を光ディスク記録装置の外部からの書き換えが可能な ROM (例えば、フラッシュ ROM) に格納する。

【 0 0 2 7 】

図 3 はこの発明の第 5 実施形態である光ディスク記録制御装置の構成を示すブロック図であり、図 1 と共通する部分には同一符号を付してその説明を省略する。この光ディスク記録制御装置では、暗号化キーのデータ部分を含むブロック領域に特別な制御手順処理以外のプログラムを格納するための新たに書換可能な ROM 3 6 を設けている。

すなわち、上記 CPU 3 1 及びフラッシュ ROM 3 6 が、上記情報記録装置の全体制御を司る手段を更新可能に設け、上記 CPU 3 1 及び ROM 3 3 が、上記再記録制御手段を改変不可能にそれぞれ設けたものである。

【 0 0 2 8 】

この光ディスク記録制御装置は、図 3 に示すように、少なくとも CPU 3 1 で動作する暗号化キーのデータ部分を含むブロック領域に特別な制御手順処理を施すためのプログラムを上述と同様に書き換え不能な ROM 3 3 に格納し、さらにその特別な制御手順処理以外の CPU 制御プログラム部をフラッシュ ROM (Flash ROM) などの書換可能な ROM 3 6 に格納している。

このようにして、この第 5 実施形態の光ディスク記録制御装置は、製造後のプログラム

10

20

30

40

50

の改変による暗号化キーの記録を防ぐと共に、それ以外の無関係なプログラム部のアップデートを容易に図ることができる。

【0029】

(6) この発明の第6実施形態

この第6実施形態の光ディスク記録制御装置は、外部からの書き換えが不可能なROM 33に不揮発で一意的な識別情報(ID)を付与し、CPU 31による特別な制御手順処理を行う際にそのIDをデータ処理部1に登録することにより、データ処理部1は登録されたROM 33での操作以外の記録情報への変換要求を受け付けないようにする。

すなわち、上記CPU 31とROM 33が固有の識別情報を付与して前記再記録制御手段を改変不可能に設けたものであり、上記CPU 31が上記識別情報に基づいて認証された前記再記録制御手段(上記データ処理部1)の制御のみを実行させる手段の機能を果たす。

【0030】

この光ディスク記録制御装置は、図3に示した装置構成と同じであるが、ROM 33に予め固有なIDを付与していることと、CPU 31及びデータ処理部1の処理が若干異なる。

まず、ROM 33には、コントローラ処理部3のCPU 31で動作するデータ処理部1に対する特別な制御手順処理のプログラムを格納するが、不揮発で一意的なIDも併せて格納しており、CPU 31はデータ処理部1に対する特別な制御手順処理では必ずそのIDを使ってデータ処理部1と認証する。

例えば、データ処理部1は、CPU 31からの最初のアクセス時にROM 33のIDを記憶し、その後、ROMのIDが上記記憶したものと異なるアクセスは拒否する。

このようにして、この第6実施形態の光ディスク記録制御装置は、CPU 31で動作するデータ処理部1に対する特別な制御手順処理をプログラムとして格納しているROM 33が悪意によって取り替えられても暗号化キーの領域の記録を不可能にすることができる。

【0031】

(7) この発明の第7実施形態

この第6実施形態の光ディスク記録制御装置は、外部からの書き換えが不可能なROMをCPUに内蔵する。

図4はこの発明の第7実施形態である光ディスク記録制御装置の構成を示すブロック図であり、図3と共通する部分には同一符号を付してその説明を省略する。この光ディスク記録制御装置では、暗号化キーのデータ部分を含むブロック領域に特別な制御手順処理以外のプログラムを格納するためのROM 33をCPU 31の内部に設けている。

すなわち、上記情報記録装置の中央処理手段(CPU 31)内に上記再記録制御手段(ROM 33)を改変不可能に設けたものである。

【0032】

この光ディスク記録制御装置は、図4に示すように、上記データ処理部1に対する特別な制御手順処理をプログラムとして格納している書き換え不可能なROM 33をCPU 31に内蔵し、不正な交換を防止するようにしている。

このROM 33の不揮発で一意的なIDをCPU 31に対して付するようによい。

このようにして、この第7実施形態の光ディスク記録制御装置は、CPU 31に内蔵されているROM 33に特別な制御手順処理のプログラムを記録しておくことにより、ROMの分割による部品点数の増加、部品スペースを少なくした上で、悪意によってCPU 31を取り替えられても暗号化キーの領域には記録不可能にすることができる。

【0033】

【発明の効果】

以上説明してきたように、この発明の情報記録装置と情報記録方法によれば、記録媒体上の暗号化キーによって保護されているデータを再生可能な状態で複製できないようにすることができる。

10

20

30

40

50

【図面の簡単な説明】

【図 1】 この発明の第 1 実施形態である光ディスク記録制御装置の構成を示すブロック図である。

【図 2】 図 1 に示した光ディスク記録制御装置におけるこの発明の請求項 1 及び請求項 8 に係わる不正コピー防止記録処理について示すフローチャート図である。

【図 3】 この発明の第 5 実施形態である光ディスク記録制御装置の構成を示すブロック図である。

【図 4】 この発明の第 7 実施形態である光ディスク記録制御装置の構成を示すブロック図である。

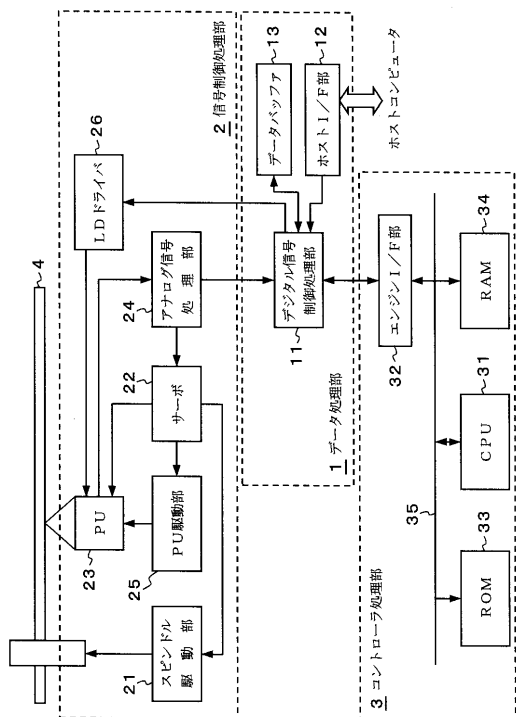
【符号の説明】

- 1 : データ処理部
- 2 : 信号制御処理部
- 3 : コントローラ処理部
- 4 : 光ディスク
- 11 : デジタル信号制御処理部
- 12 : ホスト I / F
- 13 : データバッファ
- 21 : スピンドル駆動部
- 22 : サーボ
- 23 : 光ピックアップ部
- 24 : アナログ信号処理部
- 25 : 光ピックアップ駆動部
- 26 : LD ドライバ
- 31 : CPU
- 32 : エンジン I / F 部
- 33 : ROM
- 34 : RAM
- 35 : バス
- 36 : 書換可能な ROM

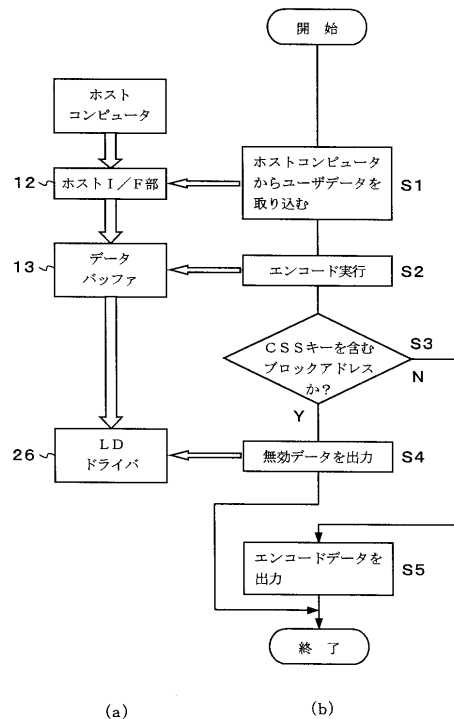
10

20

【図 1】



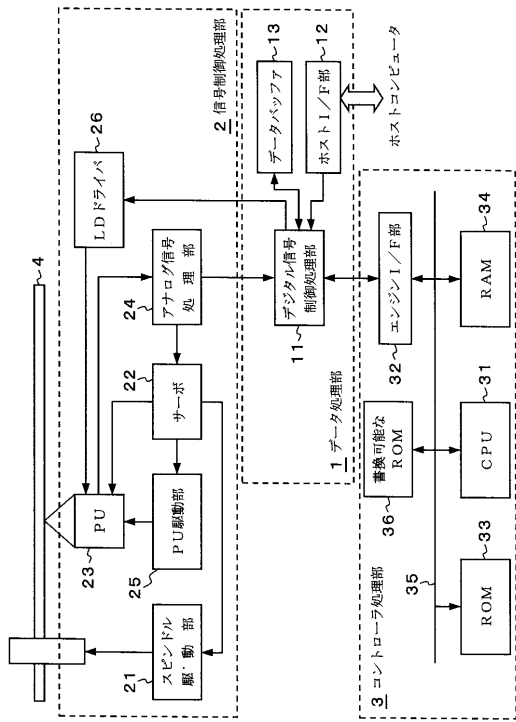
【図 2】



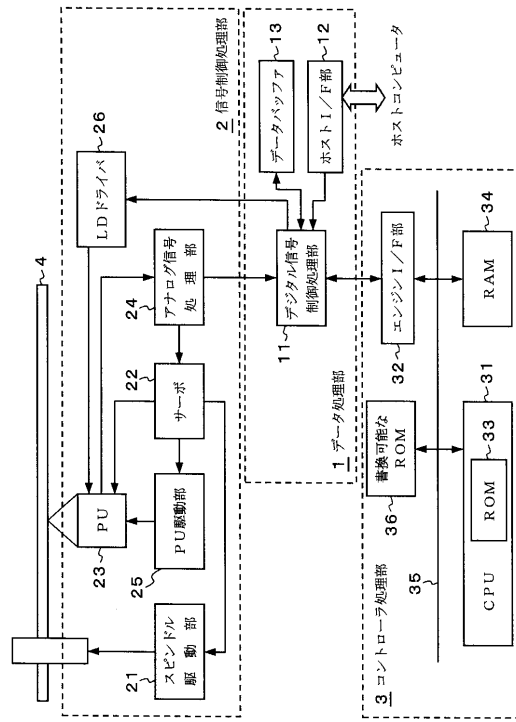
(a)

(b)

【 図 3 】



【 図 4 】



フロントページの続き

- (56)参考文献 特開平07-307060(JP,A)
特開平11-096675(JP,A)
特開平11-213566(JP,A)
特開平08-129631(JP,A)
特開平06-336319(JP,A)
特開2000-149435(JP,A)
特開2000-090213(JP,A)

(58)調査した分野(Int.Cl., DB名)

G11B 20/10
H04L 9/10
G06F 12/14