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

特許第4062842号
(P4062842)

(45)発行日　平成20年3月19日(2008.3.19)　(24)登録日　平成20年1月11日(2008.1.11)

(51)Int.Cl.		F I		
G11B 20/10	(2006.01)	G11B	20/10	H
G06F 12/14	(2006.01)	G06F	12/14	
G09C 1/00	(2006.01)	G09C	1/00	660D

請求項の数 11　(全 21 頁)

(21)出願番号　特願平11-354991
(22)出願日　平成11年12月14日(1999.12.14)
(65)公開番号　特開2001-176189(P2001-176189A)
(43)公開日　平成13年6月29日(2001.6.29)
審査請求日　平成18年3月16日(2006.3.16)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100067736
弁理士　小池　晃
(74)代理人　100086335
弁理士　田村　榮一
(74)代理人　100096677
弁理士　伊賀　誠司
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】記録装置及び方法、再生装置及び方法並びに記録媒体

(57)【特許請求の範囲】

【請求項１】

着脱可能な記録媒体に情報を記録する記録装置において、

記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し手段と、

上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し手段と、

上記第１の識別情報及び上記第２の識別情報に基づき、上記情報を暗号化する暗号化手段と、

数列を発生する数列発生手段と、

上記数列発生手段で発生された数列を上記記録媒体に第２の識別情報として書き込む書き込み手段とを有し、

上記記録媒体に第２の識別情報が記録されておらず上記第２の読み出し手段による読み出しにより第２の識別情報が得られないとき、上記書き込み手段により第２の識別情報を書き込むこと

を特徴とする記録装置。

【請求項２】

着脱可能な記録媒体に情報を記録する記録装置において、

記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し手段と、

上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し手段と、
第１の秘密情報を格納する格納手段と、
上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出手段と、
上記第２の秘密情報に基づいて上記情報を暗号化し、上記記録媒体に記録する第１の暗号化書き込み手段と
を有することを特徴とする記録装置。
【請求項３】
第３の秘密情報及び第４の秘密情報を発生する秘密情報発生手段と、
上記第３の秘密情報を用いて上記第４の秘密情報を暗号化し、上記記録媒体に記録する第２の暗号化書き込み手段と、
上記第２の秘密情報を用いて上記第３の秘密情報を暗号化し、上記記録媒体に記録する第３の暗号化書き込み手段を有することを特徴とする請求項２記載の記録装置。
【請求項４】
着脱可能な記録媒体に情報を記録する記録方法において、
記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、
上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、
数列を発生する数列発生工程と、
上記数列発生工程で発生された数列を上記記録媒体に第２の識別情報として書き込む書き込み工程と、
上記第１の識別情報及び上記第２の識別情報に基づき、上記情報を暗号化する暗号化工程とを有し、
上記記録媒体に第２の識別情報が記録されておらず上記第２の読み出し工程による読み出しにより第２の識別情報が得られないとき、上記書き込み工程により第２の識別情報を書き込むこと
を特徴とする記録方法。
【請求項５】
着脱可能な記録媒体に情報を記録する記録方法において、
記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、
上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、
上記第１の識別情報、上記第２の識別情報及び格納された第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、
上記第２の秘密情報に基づいて上記情報を暗号化し、上記記録媒体に記録する第１の暗号化書き込み工程と
を有することを特徴とする記録方法。
【請求項６】
着脱可能な記録媒体から情報を再生する再生装置において、
記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し手段と、
上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し手段と、
第１の秘密情報を格納する格納手段と、
上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出手段と、
上記記録媒体から暗号化された上記情報を読み出し、この情報を上記第２の秘密情報に

基づいて復号する第１の読み出し復号手段と
を有することを特徴とする再生装置。
【請求項７】
上記記録媒体から暗号化された第３の秘密情報を読み出す第３の読み出し手段と、上記第２の秘密情報を用いて暗号化された第３の秘密情報を復号する第３の秘密情報復号手段と、上記記録媒体から暗号化された第４の情報を読み出し、この第４の情報を上記第３の秘密情報を用いて復号する第２の読み出し復号手段とを有することを特徴とする請求項６記載の再生装置。
【請求項８】
着脱可能な記録媒体から情報を再生する再生方法において、
記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、
上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、
上記第１の識別情報、上記第２の識別情報及び格納された第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、
上記記録媒体から暗号化された上記情報を読み出し、この情報を上記第２の秘密情報に基づいて復号する第１の読み出し復号工程と
を有することを特徴とする再生方法。
【請求項９】
情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、
記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、
上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、
数列を発生する数列発生工程と、
上記数列発生工程で発生された数列を上記記録媒体に第２の識別情報として書き込む書き込み工程と、
上記第１の識別情報及び上記第２の識別情報に基づき、上記情報を暗号化する暗号化工程とを有し、
上記記録媒体に第２の識別情報が記録されておらず上記第２の読み出し工程による読み出しにより第２の識別情報が得られないとき、上記書き込み工程により第２の識別情報を書き込むこと
を特徴とする記録媒体。
【請求項１０】
情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、
記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、
上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、
第１の秘密情報を格納する格納工程と、
上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、
上記第２の秘密情報に基づいて上記情報を暗号化し、上記記録媒体に記録する第１の暗号化書き込み工程と
を有することを特徴とする記録媒体。
【請求項１１】
情報を記録媒体から再生するプログラムが記録された記録媒体において、上記プログラ

ムは、
記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、
上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、
第１の秘密情報を格納する格納工程と、
上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、
上記記録媒体から暗号化された上記情報を読み出し、この情報を上記第２の秘密情報に基づいて復号する第１の読み出し復号工程と
を有することを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、記録媒体に情報信号を記録する記録装置及び方法、記録媒体から情報信号を再生する再生装置及び方法並びに情報信号を記録される記録媒体に関する。
【０００２】
【従来の技術】
近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。
【０００３】
例えば、ミニディスク（MD）（商標）システムにおいては、 シリアルコピー管理システム(Serial Copy Management System; SCMS)と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、コピー自由（copy free ）、コピー一度許容（copy once allowed ）、またはコピー禁止（copy prohibited ）のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。
【０００４】
このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。
【０００５】
また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。
【０００６】
【発明が解決しようとする課題】

上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録することが規定されている。しかし、このような動作規定に従わない記録機器が、不正に製造されてしまう。

【０００７】

また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【０００８】

本発明は、上述の実情に鑑みてなされたものであり、記録媒体に不正コピーを抑制するように記録する記録装置及び方法、記録媒体からの不正コピーを抑制するように再生する再生装置及び方法並びに不正コピーを抑制するような記録媒体に関する。

【０００９】

【課題を解決するための手段】

上述の課題を解決するために、本発明に係る記録装置は、着脱可能な記録媒体に情報を記録する記録装置において、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し手段と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し手段と、上記第１の識別情報及び上記第２の識別情報に基づき、上記情報を暗号化する暗号化手段と、数列を発生する数列発生手段と、上記数列発生手段で発生された数列を上記記録媒体に第２の識別情報として書き込む書き込み手段とを有し、上記記録媒体に第２の識別情報が記録されておらず上記第２の読み出し手段による読み出しにより第２の識別情報が得られないとき、上記書き込み手段により第２の識別情報を書き込むものである。

【００１０】

また、本発明に係る記録装置は、着脱可能な記録媒体に情報を記録する記録装置において、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し手段と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し手段と、第１の秘密情報を格納する格納手段と、上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出手段と、上記第２の秘密情報に基づいて上記情報を暗号化し、上記記録媒体に記録する第１の暗号化書き込み手段とを有するものである。

【００１１】

本発明に係る記録方法は、着脱可能な記録媒体に情報を記録する記録方法において、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、数列を発生する数列発生工程と、上記数列発生工程で発生された数列を上記記録媒体に第２の識別情報として書き込む書き込み工程と、上記第１の識別情報及び上記第２の識別情報に基づき、上記情報を暗号化する暗号化工程とを有し、上記記録媒体に第２の識別情報が記録されておらず上記第２の読み出し工程による読み出しにより第２の識別情報が得られないとき、上記書き込み工程により第２の識別情報を書き込むものである。

【００１２】

また、本発明に係る記録方法は、着脱可能な記録媒体に情報を記録する記録方法において、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、上記第１の識別情報、上記第２の識別情報及び格納された第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、上記第２の秘密情報に基づいて上記情報を暗号化し、上記記録媒体に記録する第１の暗号化書き込み工程とを有するものである。

【００１３】
本発明に係る再生装置は、着脱可能な記録媒体から情報を再生する再生装置において、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し手段と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し手段と、第１の秘密情報を格納する格納手段と、上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出手段と、上記記録媒体から暗号化された上記情報を読み出し、この情報を上記第２の秘密情報に基づいて復号する第１の読み出し復号手段とを有するものである。

【００１４】
本発明に係る再生方法は、着脱可能な記録媒体から情報を再生する再生方法において、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、上記第１の識別情報、上記第２の識別情報及び格納された第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、上記記録媒体から暗号化された上記情報を読み出し、この情報を上記第２の秘密情報に基づいて復号する第１の読み出し復号工程とを有するものである。

【００１６】
また、本発明に係る記録媒体は、情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、数列を発生する数列発生工程と、上記数列発生工程で発生された数列を上記記録媒体に第２の識別情報として書き込む書き込み工程と、上記第１の識別情報及び上記第２の識別情報に基づき、上記情報を暗号化する暗号化工程とを有し、上記記録媒体に第２の識別情報が記録されておらず上記第２の読み出し工程による読み出しにより第２の識別情報が得られないとき、上記書き込み工程により第２の識別情報を書き込むものである。

【００１７】
さらに、本発明に係る記録媒体は、情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、第１の秘密情報を格納する格納工程と、上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、上記第２の秘密情報に基づいて上記情報を暗号化し、上記記録媒体に記録する第１の暗号化書き込み工程とを有するものである。

【００１８】
そして、本発明に係る記録媒体は、情報を記録媒体から再生するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から、当該記録媒体の製造者によって付与された第１の識別情報を読み出す第１の読み出し工程と、上記記録媒体から、上記第１の識別情報とは異なる第２の識別情報を読み出す第２の読み出し工程と、第１の秘密情報を格納する格納工程と、上記第１の識別情報、上記第２の識別情報及び上記第１の秘密情報に基づいて第２の秘密情報を算出する第２の秘密情報算出工程と、上記記録媒体から暗号化された上記情報を読み出し、この情報を上記第２の秘密情報に基づいて復号する第１の読み出し復号工程とを有するものである。

【００１９】
本発明は、第３の秘密情報及び第４の秘密情報を発生し、上記第３の秘密情報を用いて上記第４の情報を暗号化して上記記録媒体に書き込み、上記第２の秘密情報を上記第３の秘密情報を暗号化して上記記録媒体に書き込むものである。この第３の秘密情報とは、上記第１の秘密情報及び第２の秘密情報の下位にある秘密情報を意味するものである。

【００２０】
【発明の実施の形態】
以下では、本発明の実施の形態について、図面を参照して説明する。まず、本発明の実施の形態として、光ディスク記録再生装置について説明する。
【００２１】
図１は、光ディスク記録再生装置の構成例を表している。入力部１は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。
【００２２】
制御回路２は、プログラムに従って処理を実行するＣＰＵ２ａ、不揮発性の記憶素子であるＲＯＭ２ｂ、揮発性の記憶素子であるＲＡＭ２ｃなどにより構成されている。この制御回路２は、ＲＯＭ２ｂやＲＡＭ２ｃに記憶された所定のプログラムに従って、装置全体を制御する。
【００２３】
制御回路２は、ＲＯＭ２ｂに格納されたプログラムで動作する。制御回路２には、外部のネットワークや、ＨＤＤ１１からプログラムが読み込まれる可能性がある。例えば、制御回路２にパーソナルコンピュータを用い、読み込んだコンピュータプログラムに用いて処理を実行させることができる。
【００２４】
記録再生回路３は、暗号化部４と復号部５を有し、復号部５は、ピックアップ６により、光ディスク７から再生されたデータを復号し、外部に再生信号として出力する。暗号化部４は、外部から記録信号の供給を受け取ると、これを暗号化し、ピックアップ６に供給して、光ディスク７に記録させる。
【００２５】
ピックアップ６は、レーザビームを光ディスク７に照射することで、データの記録再生を行う。スピンドルモータ９は、サーボ回路８によって制御され、光ディスク７を回転させる。
【００２６】
サーボ回路８は、スピンドルモータ９を駆動することにより、光ディスク７を所定の速度、例えば線速度一定で回転させる。サーボ回路８はまた、ピックアップ６のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。
【００２７】
乱数発生回路１０は、制御回路２の制御により、所定の乱数を発生する。ＨＤＤ１１は、プログラムやデータを記録される大容量の記録装置である。
【００２８】
ここで、本実施の形態の前提となる、特願平10‐025310号明細書に記載されている記録方法について説明する。この記録方法によると、光ディスク７には、図２に示すような構造を有するデータが記録される。
【００２９】
光ディスク７のリードインエリアには、製造者により光ディスク７に付与された第１の識別情報であるディスク製造識別情報DiscIDmを予め暗号化した暗号化ディスク製造識別情報EDiscIDm、デイスクキーKdを暗号化した暗号化ディスクキーEKdが記録されている。なお、上記ではDiscIdmを暗号化するとしているが、この暗号化とは、実際はそのアクセス方法を知らない者には読み出し、書き込みが困難なように記録することで、便宜上これを暗号化と呼んでいる。
【００３０】
この記録方法によると、個々の光ディスク７を識別するためのディスク製造識別情報DiscIDmを光ディスク７に持たせ、この情報をライセンスを受けた装置にしかアクセスできないようにする。
【００３１】

また、光ディスク７のデータエリアには、ヘッダである暗号化セクタキーEKｓ１とメインデータ部である暗号化コンテンツデータとからなるセクタS1が記録されている。暗号化セクタキーEKｓ１はディスクキーKdにより、暗号化コンテンツデータはセクタキーKs1により、それぞれ暗号化されている。なお、図中の括弧は暗号化に用いる秘密情報を示している。

【００３２】

同様に、光ディスク７のデータエリアには、ヘッダである暗号化セクタキーEKｓ２とメインデータ部である暗号化コンテンツデータとからなるセクタS２が記録されている。暗号化セクタキーEKｓ２はディスクキーKdにより、暗号化コンテンツデータはセクタキーKs2により、それぞれ暗号化されている。

【００３３】

光ディスク７上のデータはディスク製造識別情報DiscIDmと、ライセンスを受けることによって得られる秘密情報、例えば秘密鍵によって暗号化し、ライセンスを受けていない装置はデータを読み出しても意味のないものとする。装置にライセンスを与える際にはその動作を規定し、不正コピーを行わないようにする。

【００３４】

ライセンスを得ていない装置はディスク製造識別情報DiscIDmにアクセスできず、またディスク製造識別情報DiscIDmは個々の光ディスク７ごとに個別の値になっているため、ライセンスを受けていない機器がアクセス可能なすべての情報を新たな光ディスク７にコピーしたとしても、そのようにして作られた光ディスク７は、ライセンスを受けていない装置でもライセンスを受けた装置でも正しく情報が読み出せないようにしている。このようにして不正コピーを防いでいる。

【００３５】

この記録方法では、ディスク製造識別情報DiscIDmを光ディスク７の製造時に製造者が記録する、という運用方法と、ある媒体に初めてデータを記録する記録装置がこの際に媒体識別情報を媒体に記録するという運用方法がある。

【００３６】

ところで、前者の方法では下記のような問題がある。

【００３７】

ディスク製造識別情報DiscIDmは光ディスク７ごとに固有の値でなければならないが、そうすることは製造者によってコストの増加を招くため、すべての光ディスク７に同一の値を記録するような製造者が出る可能性がある。

【００３８】

また、すべての光ディスク７に同一のディスク製造識別情報DiscIDmが記録されてしまうと、ライセンスを受けていない装置はその情報がアクセスできないとしても、装置間で同一なので、アクセスできる情報だけコピーすれば、まったく同じ光ディスク７ができてしまい、不正コピーが可能になってしまう。

【００３９】

また、後者の方法では下記のような問題がある。ディスク製造識別情報DiscIDmは、ライセンスを受けていない装置はアクセスできないようにしなければならないため、そのアクセス方法はライセンスを受けた装置だけが持つ秘密情報となる。

【００４０】

さらに、前者の方法においては、ディスク製造識別情報DiscIDmの記録方法は光ディスク７の製造者のみが知っていればよいが、この方法においては、すべての記録装置がディスク製造識別情報DiscIDmの記録方法を持つことが必要である。

【００４１】

このことは、不正なコピーを試みる攻撃者にとって、前者の方法よりも、ディスク製造識別情報DiscIDmの記録方法を盗み出す機会が容易に手に入るということになる。このため、この方法においては、不正者がディスク製造識別情報DiscIDmにアクセスする可能性が高く、セキュリティが低くなるという問題がある。

【００４２】
本実施の形態では、このような問題を解決するために、識別情報の記録方法として、製造者が記録する第１の識別情報と、記録装置が記録する第２の識別情報の両方を用いる。
【００４３】
上記の２つの識別情報を用いることにより、たとえ製造者が同一の第１の識別情報を記録した光ディスク７を複数製造しても、記録装置がそれぞれ別個の第２の識別情報を記録するので、識別情報全体として別個のものとなり、識別情報にアクセスされない限り不正コピーを防ぐことが可能となる。
【００４４】
また、たとえ記録機器が持つ第２の識別情報の記録方法を不正者が盗んだとしても、それだけでは製造者が記録した第１の識別情報にアクセスすることはできず、この場合も不正コピーを防ぐことが可能となる。
【００４５】
本実施の形態においては、光ディスク７には、図３に示すような構造を有するデータが記録されている。光ディスク７のリードインエリアには、ディスク製造識別情報DiscIDmを予め定められたＭ系列符号で暗号化した暗号化ディスク製造識別情報EDiscIDm、デイスクキーKdをイフェクティブマスタキーKemで暗号化した暗号化ディスクキーEKdが記録されている。
【００４６】
また、光ディスク７には、光ディスク記録再生装置により、第２の識別情報であるディスク記録識別情報DiscIDrが付与される。このディスク記録識別情報DiscIDrは、Ｍ系列符号にて暗号化された暗号化ディスク記録識別情報EDiscIDrとして光ディスク７に記録される。光ディスク７には、暗号化ディスク記録識別情報EDiscIDrを記録するための領域が予め設けられている。
【００４７】
このように、ディスク製造識別情報DiscIDm及びディスク記録識別情報DiscIDrを暗号化していることにより、これらの識別情報に対する不正なアクセスを阻止することができる。すなわち、識別情報の暗号化は、ライセンスを受けていない者やライセンスを受けていない機器が、上記識別情報を読んだり、書きかえたり、新規に書いたりことを防止する。なお、この暗号化は、必ずしも数学的な意味での暗号化でなくても、その方法を知らない者が読み出し、書き込み等のアクセスを行うのが困難という程度のものでもよい。
【００４８】
暗号化ディスク製造識別情報EDiscIDm及び暗号化ディスク記録識別情報EDiscIDrは、光ディスクの読み出し専用のＲＯＭ部分や、書き換え可能なＲＡＭ部分や、ＲＯＭ部分やＲＡＭ部分に組み合わせて書くことができる。本実施の形態における記録方式については、後述する。
【００４９】
上記Ｍ系列符号は、所定の周期で、“０”と“１”の２値がランダムに出現する疑似ランダム２値信号、すなわち一種の疑似乱数である。ディスク製造識別情報DiscIDmは、例えば、ファイル名やデイレクトリ情報などのTOC(Table Of Contents)データ内に、予め設定された所定のＭ系列符号に基づいて埋め込むことで暗号化されている。すなわち、ディスク製造識別情報DiscIDmは、TOCデータのエッジの時間ずれとして記録される。このような暗号化を行うと、TOCデータは暗号化されないでＭ系列符号がなくとも読み取ることができるが、ディスク製造識別情報DiscIDmは、暗号化に用いたのと同一のＭ系列符号がないと読み取ること、すなわち復号することができなくなる。このようなＭ系列符号に基づく暗号化に関する技術は、特願平09-288960号として本出願人が先に提案している。なお、この所定のＭ系列符号は、著作権者から適正なライセンスを受ける際、後述する第１の秘密情報であるマスタキーKmとともに、ライセンスを受けた者に与えられる。
【００５０】
上記イフェクティブマスタキーKemは、式（１）に従い、マスタキーKm、ディスク製造識

別情報DiscIDm、ディスク記録識別情報DiscIDrに基づいて、ハッシュ（hash）関数を適用することにより計算される。

【００５１】

Kem＝SHA-1（Km||DiscIDm||DiscIDr）　　（１）

ここで、“Km||DiscIDm||DiscIDr”は、マスタキーKm、DiscIDm、DiscIDrのビット連結を表している。例えば、ＡとＢとＣの連結とは、それぞれがn_A，n_B，n_Cビットであるとき、Ａの後方にＢを、Ｂの後方にＣを結合して$n_A+n_B+n_C$ビットのデータとすることを意味し、これを“A||B||C”で表すものとする。

【００５２】

また、SHA-1は、“Federal Information Processing Standards Publication (FIPS) 180-1”に定義されている一方向ハッシュ関数である。SHA-1の出力は、160ビットであるが、実際にはイフェクティブマスタキーKemは最上位から必要なビット数だけ取り出すなどして使用する。

【００５３】

マスタキーKmは、著作権者等から適正にライセンスを受けた光ディスク記録再生装置にだけ与えられる秘密情報である。

【００５４】

光ディスク７のデータエリアの各セクタSi(i=1,2,...)は、ヘッダおよびメインデータ部で構成され、ヘッダには、セクタキーKsiをディスクキーKdで暗号化した暗号化セクタキーEKsi(i=1,2,...)が格納されている。ここでKsiのiは、セクタの番号を示し、セクタキーはセクタ毎に異なるのでKsiと記述するが、特に区別する必要がない場合は、Ksとも記述する。メインデータ部には、コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータが格納されている。

【００５５】

図４は、暗号化部４の構成例を表している。

【００５６】

DiscID暗号化復号回路２１は、DiscIDm復号回路２１ａ、DiscIDr暗号化復号回路２１ｂから構成されている。

【００５７】

DiscIDm復号回路２１ａは、光ディスク７から読み出された暗号化ディスク製造識別情報EDiscIDmを、Ｍ系列符号発生回路２２から供給された、暗号化に用いたのと同一のＭ系列符号に基づいて復号し、ディスク製造識別情報DiscIDmを再現する。

【００５８】

ディスク記録識別情報DiscIDr暗号化復号回路２１ｂは、光ディスク７から読み出された暗号化ディスク記録識別情報EDiscIDrを、Ｍ系列符号発生回路２２から供給される、暗号化に用いたのと同一のＭ系列符号に基づいて復号し、ディスク記録識別情報DiscIDrを再現する。識別情報DiscID暗号化復号回路２１はまた、乱数発生回路１０から発生された乱数をディスク記録識別情報DiscIDrとして受け取り、Ｍ系列符号発生回路２２から供給されるＭ系列符号に基づいて暗号化して、ディスク記録識別情報EDiscIDrを生成し、光ディスク７に記録する。

【００５９】

Ｍ系列符号発生回路２２は、例えば、直列接続された複数のフリップフロップとイクスクルーシブオア回路からなり、所定のＭ系列符号を発生するようになされている。あるいは、ROM、EEPROMなどで構成することもできる。

【００６０】

連結回路２９は、DiscIDm復号回路２１ａにて復号されたディスク製造識別情報DiscIDm、DiscIDr暗号化復号回路２１ｂにて復号されたディスク記録識別情報DiscIDrを連結し、識別情報DiscIDを生成する。

【００６１】

Kem発生モジュール２３のKmメモリ２４は、マスタキーKmを記憶する。Kem発生モジュール

２３のhash関数回路２５は、マスタキーKmと識別情報DiscIDの結合を生成し、これにハッシュ（hash）関数を適用してイフェクティブマスタキーKemを算出する。

【００６２】

Kd暗号化復号回路２６は、光ディスク７から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを再現する。Kd暗号化復号回路２６はまた、乱数発生回路１０から発生された乱数をディスクキーKdとして受け取り、イフェクティブマスタキーKemで暗号化して暗号化ディスクキーEKdを生成し、光ディスク７に記録する。

【００６３】

例えば、この暗号化方式としては、“Federal Information Processiong Standards (FIPS) 46-2”に示されているデータ暗号化標準（Data Encryption Standard; DES)などが挙げられる。なお、Ks暗号化回路２７及びコンテンツデータ暗号化回路２８においても同様である。

【００６４】

Ks暗号化回路２７は、乱数発生回路１０から発生された乱数をセクタキーKsとして受け取り、ディスクキーKdで暗号化して暗号化セクタキーEKsを生成し、光ディスク７に記録する。コンテンツデータ暗号化回路２８は、セクタキーKsで、コンテンツデータを暗号化し、光ディスク７に記録する。全データの記録が終了するまでコンテンツデータの暗号化、記録を繰り返す。

【００６５】

ここで、コンテンツデータの暗号化鍵にイフェクティブマスタキーKemそのものを使う方法もあるが、一回の記録を表すファイルや、光ディスク７への読み書きの最小単位であるセクタ毎に、コンテンツデータを直接暗号化するセクタキーKsのようなコンテンツキーを設け、それをイフェクティブマスタキーKemで暗号化して、コンテンツデータと同様に光ディスク７に記録するなど、鍵を階層化して使用する方法も一般的である。なお、コンテンツキーは、セクタキーKsに限られず、例えばファイルキーであってもよい。

【００６６】

次に、図５に、復号部５の構成例を示す。EDiscID復号回路５１は、EDiscIDm復号回路５１ａ、EDiscIDr復号回路５１ｂから構成されている。

【００６７】

EDiscIDm復号回路５１ａは、光デイスク７から読み出された暗号化ディスク製造識別情報EDiscIDmを、Ｍ系列符号発生回路５２から供給される、暗号化に用いたのと同一のＭ系列符号に基づいて復号して、ディスク製造識別情報DiscIDmを再現する。

【００６８】

EDiscIDr復号回路５１ｂは、光デイスク７から読み出された暗号化ディスク記録識別情報EDiscIDrを、Ｍ系列符号発生回路５２から供給される、暗号化に用いたのと同一のＭ系列符号に基づいて復号して、ディスク記録識別情報DiscIDrを再現する。

【００６９】

Ｍ系列符号発生回路５２は、Ｍ系列符号発生回路２２と同様の構成を有し、同一のＭ系列符号を発生するようになされている。

【００７０】

連結回路５９は、DiscIDm復号回路５１ａにて復号されたディスク製造識別情報DiscIDm、ディスク記録識別情報DiscIDr暗号化復号回路５１ｂにて復号されたディスク記録識別情報DiscIDrを連結し、識別情報DiscIDを生成する。この連結回路５９は、連結回路２９と同様の構成を有し、同様の連結処理を行うようになされている。

【００７１】

Kem発生モジュール５３のKmメモリ５４は、マスタキーKmを記憶する。Kem発生モジュール５３のhash関数回路５５は、マスタキーKmと識別情報DiscIDの結合を生成し、これにハッシュ（hash）関数を適用してイフェクティブマスタキーKemを計算する。このKem発生モジュール５３は、Kem発生モジュール２３と同一の構成とされ、両者を兼用するようにして

もよい。

【００７２】

EKd復号回路５６は、光ディスク７から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを算出する。EKs復号回路５７は、光ディスク７から各セクタSiのヘッダに記録されている暗号化セクタキーEKsを読み出し、ディスクキーKdで復号して、セクタキーKsを算出する。コンテンツデータ復号回路５８は、光ディスク７から読み出された暗号化されたコンテンツデータを、セクタキーKsで復号する。

【００７３】

光ディスク記録再生装置において用いられる光ディスク７は、製造時にディスク製造識別情報DiscIDmが書き込まれている。この光ディスク７は、ディスク製造識別情報DiscIDmが書き込まれた状態で、ユーザで光ディスク７の製造者から提供される。

【００７４】

図６は、光ディスク７にディスク製造識別情報DiscIDmを書き込むDiscIDm書き込み装置６０の構成例を示す。

【００７５】

この書き込み処理は、通常は光ディスク７の製造者により行われる。この光ディスク７には、ディスク記録識別情報DiscIDrを記録するための領域を設けておく。

【００７６】

乱数回路６１は、６４ビットの乱数を生成する。Ｍ系列符号発生回路６２は、Ｍ系列符号回路２２と同様の構成を有し、Ｍ系列符号発生回路６２と同一のＭ系列符号を発生するようになされている。

【００７７】

DiscIDm暗号化回路６３は、乱数発生回路６１で生成された乱数をディスク製造識別情報DiscIDmとして受け取り、Ｍ系列符号発生回路６２から供給されるＭ系列符号に基づいて、上述したように、入力されるTOC情報に埋め込むように暗号化して、暗号化ディスク製造識別情報EDiscIDmを生成し、光ディスク７に記録する。

【００７８】

次に、光ディスク７の製造時に、ディスク製造識別情報DiscIDm書き込み装置により光ディスク７にディスク製造識別情報DiscIDmを書き込む処理手順を、図７のフローチャートを参照して説明する。

【００７９】

最初に、ステップＳ３１において、乱数発生回路６１は、６４ビットの乱数を発生し、ディスク製造識別情報DiscIDmとして、DiscIDm暗号化回路６３に出力する。

【００８０】

ディスク製造識別情報DiscIDmは、個々の光ディスク７について個別の値を使用する。たとえば、個別に割り振られた製造者の識別番号と、その製造者が製造したこの光ディスク７の累積度数すなわちシリアル番号を連結したものをディスク製造識別情報DiscIDmとする。

【００８１】

なお、ディスク製造識別情報DiscIDmは完全にユニークである必要はない。これは、ディスク製造識別情報DiscIDmが同一である複数の光ディスク７が不正者の手に入らなければよいので、ディスク製造識別情報DiscIDmが同一である複数の光ディスク７を探し出すのが困難であるようになっていればよいからである。このため、本実施の形態では、ディスク製造識別情報DiscIDmの生成にその場で発生させた擬似乱数を用いている。なお、時刻情報などを用いることも可能である。

【００８２】

光ディスク７への記録は、ライセンスを受けた機器のみがディスク製造識別情報DiscIDmを読み出せるように、ライセンスによる秘密情報に基づいた方法により行われる。すなわち、ステップＳ３２において、DiscIDm暗号化回路６３は、乱数発生回路６１から供給さ

れたディスク製造識別情報DiscIDmを、M系列符号発生回路６２から供給されたM系列符号に基づいて、上述したように、TOC情報中に埋め込むようにして暗号化して、暗号化ディスク製造識別情報EDiscIDmを生成する。M系列符号は、ライセンスにより与えられるものである。

【００８３】

そして、ステップＳ３３において、暗号化ディスク製造識別情報EDiscIDmを光ディスク７のリードインエリアに記録する。また、後にディスク製造識別情報DiscIDmを書きかえられないように、光ディスク７に設けた一度しか記録できないライトワンス領域にディスク製造識別情報DiscIDmを記録することも有効である。

【００８４】

次に、光ディスク７に対して、ユーザデータを記録する場合の暗号化部４における処理手順を、図８のフローチャートを参照して説明する。

【００８５】

最初に、ステップＳ５０Ａにおいて、DiscIDm復号回路２１ａは、光ディスク７のリードインエリアから読み出された暗号化ディスク製造識別情報EDiscIDmを受け取る。

【００８６】

ステップＳ５０Ｂにおいて、DiscIDm暗号化復号回路２１ａは、この光ディスク７から読み出された暗号化ディスク製造識別情報EDiscIDmを、M系列符号回路２２から供給された、暗号化に用いたのと同一のM系列符号で復号して、ディスク製造識別情報DiscIDmとする。このように、ライセンスされた秘密情報を用いて、光ディスク７からディスク製造識別情報DiscIDmが得られた。

【００８７】

ステップＳ５０Ｃにおいて、DiscIDr暗号化復号回路２１は、光ディスク７のリードインエリアから読み出された暗号化ディスク記録識別情報EDiscIDrを受け取り、またKd暗号化復号回路２６は、光ディスク７のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。

【００８８】

次に、ステップＳ５１において、DiscIDr暗号化復号回路２１は、光ディスク７のリードインエリアに、暗号化ディスク記録識別情報EDiscIDrが書き込まれているか否か、すなわち暗号化ディスク記録識別情報EDiscIDrを受けることができたか否かの判定を行い、Kd暗号化復号回路２６は、光ディスク７のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か、すなわち暗号化ディスクキーEKdを受け取ることができたか否かの判定を行う。暗号化ディスク記録識別情報EDiscIDrと暗号化ディスクキーEKdが共に書き込まれていないと判定された場合、ステップＳ５２に進み、乱数発生回路１０は、６４ビットの乱数を発生し、ディスク記録識別情報DiscIDrとして、DiscIDr暗号化復号回路２１に出力する。

【００８９】

この乱数は、ディスク記録識別情報DiscIDrとして個々の光ディスク７について個別の値を使用するために用いられる。なお、乱数に限らず、たとえば、個別に割り振られた記録再生装置の識別番号と、その記録再生が生成したディスク記録識別情報DiscIDrの個数を連結したものをディスク記録識別情報DiscIDrとしてもよい。

【００９０】

ディスク記録識別情報DiscIDrは完全にユニークである必要はない。これは、ディスク記録識別情報DiscIDrが同一である複数の光ディスク７が不正者の手に入らなければよいので、ディスク記録識別情報DiscIDrが同一である複数の光ディスク７を探し出すのが困難であるようになっていればよい。

【００９１】

このため、ディスク記録識別情報DiscIDrの生成にその場で発生させた擬似乱数を用いている。なお、時刻情報などを用いることも可能である。

【００９２】

ステップＳ５３において、連結部２９は、DiscIDm復号回路２１ａにて復号されたディスク製造識別情報DiscIDmと、乱数発生回路１０からDiscIDr暗号化復号回路２１ｂに送られたディスク記録識別情報DiscIDrとを連結し、識別情報DiscIDを生成する。

【００９３】

次に、ステップＳ５４において、DiscIDr暗号化復号回路２１ｂは、乱数発生回路１０から供給されたディスク記録識別情報DiscIDrを、Ｍ系列符号発生回路２２から供給されたＭ系列符号に基づいて暗号化して、暗号化ディスク記録識別情報EDiscIDrを生成し、光ディスク７に記録する。

【００９４】

また、後にディスク記録識別情報DiscIDrを書きかえられないように、光ディスク７に設けた一度しか情報を記録できないライトワンス領域にディスク記録識別情報DiscIDrを記録することも有効である。

【００９５】

このステップでは、光ディスク７にディスク記録識別情報DiscIDrが記録されていないので、光ディスク記録再生装置はその光ディスク７用のディスク記録識別情報DiscIDrを生成し、ライセンスされた秘密情報を用いてこれを光ディスク７に記録する。

【００９６】

この、光ディスク７への記録は、ライセンスを受けた機器のみがディスク記録識別情報DiscIDrを読み出せるように、ライセンス秘密情報に基づいた方法により行われる。

【００９７】

次に、ステップＳ５５において、Kem発生モジュール２３のhash関数回路２５は、Kem発生モジュール２３のKmメモリ２４から、ライセンスされた秘密情報として与えられ、秘密に保管しているマスタキーKmを読み出す。Kem発生モジュール２３のhash関数回路２５は、ステップＳ５６で、上述の式（１）に従い、光ディスク７の識別情報DiscID、およびKmメモリ２４から読み出したマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路２６に供給する。

【００９８】

次に、ステップＳ５７において、乱数発生回路１０は、４０ビットの乱数を発生し、ディスクキーKdとして、Kd暗号化復号回路２６に出力する。Kd暗号化復号回路２６は、ステップＳ５８において、乱数発生回路１０から供給されたディスクキーKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク７のリードインエリアに記録する。

【００９９】

ステップＳ５２で、暗号化ディスク記録識別情報EDiscIDrと暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップＳ５９Ａに進み、DiscIDr暗号化復号回路２１ｂは、この光ディスク７から読み出された暗号化ディスク記録識別情報EDiscIDrを、Ｍ系列符号回路２２から供給された、暗号化に用いたのと同一のＭ系列符号で復号して、ディスク記録識別情報DiscIDrとする。このように、ライセンスされた秘密情報を用いて、ディスク記録識別情報DiscIDrが得られた。

【０１００】

ステップＳ５９Ｂにおいて、連結部２９は、DiscIDm復号回路２１ａにて復号されたディスク製造識別情報DiscIDmと、DiscIDr暗号化復号回路２１ｂにて復号されたディスク記録識別情報DiscIDrとを連結し、識別情報DiscIDを生成する。

【０１０１】

ステップＳ６０において、Kem発生モジュール２３のhash関数回路２５は、Kem発生モジュール２３のKmメモリ２４から、マスタキーKmを読み出す。Kem発生モジュール２３のhash関数回路２５は、ステップＳ６１で、上述の式（１）に従い、光ディスク７の識別情報DiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路２６に供給する。

【０１０２】

次に、ステップＳ６２において、Kd暗号化復号回路２６は、この光ディスク７から読み出された暗号化ディスクキーEKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路２６は、ディスクキーKdを、Ks暗号化回路２７に出力する。

【０１０３】

ステップＳ５８またはＳ６２の処理の後、乱数発生回路１０は、ステップＳ６３で、４０ビットの乱数を発生し、セクタキーKsとして、Ks暗号化回路２７、およびコンテンツデータ暗号化回路２８に出力する。Ks暗号化回路２７は、ステップＳ６４で、暗号化ディスクキーEKdが光ディスク７に記録されている場合にはKd暗号化復号回路２６、または暗号化ディスクキーEKdが光ディスク７に記録されていない場合には乱数発生回路１０から受け取ったディスクキーKdで、乱数発生回路１０から受け取ったセクタキーKsを暗号化して、暗号化セクタキーEKsを生成する。Ks暗号化回路２７はまた、その暗号化セクタキーEKsを、光ディスク７のデータエリアにあるセクタヘッダに記録する。

【０１０４】

次に、ステップＳ６５において、コンテンツデータ暗号化回路２８は、ステップＳ６３で乱数発生回路１０から受け取ったセクタキーKsにより、コンテンツデータを暗号化し、光ディスク７のデータエリアのメインデータ部に記録する。

【０１０５】

ステップＳ６６において、暗号化部４の各回路は、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータがまだ記録されていないと判定された場合、ステップＳ６７に進み、暗号化部４の各回路は、光ディスク７の、まだデータを記録していないセクタにアクセスし、ステップＳ６３に戻り、以下同様の処理を繰り返す。ステップＳ６６で、全てのコンテンツデータが記録されたと判定された場合、暗号化部４の各回路は、全ての記録処理を終了する。

【０１０６】

以上のようにして、ディスク記録識別情報DiscIDrが生成され、記録媒体に記録され、そして生成されたディスク記録識別情報DiscIDrとマスタキーKmに対応して暗号化されたコンテンツデータが記録媒体に記録される。このことより、例えば、ディスク製造識別情報DiscIDmは記録されているがディスク記録識別情報DiscIDrは記録されていない既存の記録媒体に複製されたコンテンツデータを、著作権者から適正にライセンスを受けていない者は、意味のある情報として再生することができない。

【０１０７】

次に、図９のフローチャートを参照して、復号部５により行われる、ユーザデータの再生処理を説明する。

【０１０８】

最初に、ステップＳ８１Ａにおいて、EDiscIDm復号回路５１aは、光ディスク７のリードインエリアから読み出された、暗号化されたディスク製造識別情報DiscIDmである暗号化識別情報EDiscIDmを受け取る。ステップＳ８１Ｂにおいて、EDiscIDr復号回路５１ｂは、光ディスク７のリードインエリアから読み出された、暗号化されたディスク記録識別情報DiscIDrである暗号化ディスク記録識別情報EDiscIDrを受け取る。

【０１０９】

EDiscIDm復号回路５１ａはさらに、ステップＳ８２Ａにおいて、Ｍ系列符号発生回路５２から供給されたＭ系列符号に基づいて、暗号化ディスク製造識別情報EDiscIDmを復号してディスク製造識別情報DiscIDmを再現し、連結回路５９に出力する。

【０１１０】

EDiscIDr復号回路５１ｂはさらに、ステップＳ８２Ｂにおいて、Ｍ系列符号発生回路５２から供給されたＭ系列符号に基づいて、暗号化ディスク記録識別情報EDiscIDrを復号してディスク記録識別情報DiscIDrを再現し、連結回路５９に出力する。

【０１１１】

このように、ライセンスによる秘密情報として与えられた方法を用いて、光ディスク７か

らディスク製造識別情報DiscIDmとディスク記録識別情報DiscIDrが得られた。

【０１１２】

ステップＳ８２Ｃにおいて、連結回路５９は、EDiscID復号回路５１ａで復号されたディスク製造識別情報DiscIDmと、EDiscIDr復号回路５１ｂで復号されたディスク記録識別情報DiscIDrとを連結し、識別情報DiscIDとする。

【０１１３】

次に、ステップＳ８３において、Kem発生モジュール５３のhash関数回路５５は、連結回路５９から出力された識別情報DiscIDを受け取るとともに、Kmメモリ５４からライセンスによう秘密情報として与えられ、秘密に保管しているマスタキーKmを読み出し、上述の式（１）に従い、光ディスク７の識別情報DiscIDとマスタキーKmの結合にhash関数を適用してイフェクティブマスタキーKemを算出し、EKd復号回路５６に供給する。

【０１１４】

ステップＳ８４において、EKd復号回路５６は、光ディスク７のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路５６は、ステップＳ８５で、この読み出された暗号化ディスクキーEKdを、hash関数回路５５から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを算出し、EKs復号回路５７に出力する。

【０１１５】

次に、ステップＳ８６において、EKs復号回路５７は、光ディスク７のデータエリアから読み出された各セクタの暗号化セクタキーEKsi（i=1,2,...）を受け取る。EKs復号回路５７は、ステップＳ８７で、この読み出された暗号化セクタキーEKsiを、EKd復号回路５６から受け取ったディスクキーKdで復号して、セクタキーKsiを算出し、コンテンツデータ復号回路５８に出力する。

【０１１６】

ステップＳ８８において、コンテンツデータ復号回路５８は、光ディスク７から読み出された暗号化されているコンテンツデータを受け取る。コンテンツデータ復号回路５８は、ステップＳ８９で、この読み出された暗号化されているコンテンツデータを、EKs復号回路５７から受け取ったセクタキーKsiで復号し、再生信号として出力する。

【０１１７】

次に、ステップＳ９０において、復号部５の各回路は、光ディスク７のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップＳ９１に進み、復号部５の各回路は、光ディスク７の、まだ読み出されていない次のセクタのデータの供給を受け、ステップＳ８６以降の処理を繰り返す。全てのコンテンツデータが読み出されたと判定された場合、復号部５の各回路は、全ての再生処理を終了する。

【０１１８】

このように、記録媒体のIDを生成し、所定のＭ系列符号で暗号化して、記録媒体に記録することで、著作権者から適正にライセンスを受けた者だけが、その記録媒体にアクセスできるようにする。

【０１１９】

なお、本実施の形態中において、上記処理を実行するコンピュータプログムをユーザに提供する提供媒体には、磁気ディスク、CD-ROMなどの情報記録媒体の他、インターネット、デジタル衛星などのネットワークによる伝送媒体も含まれる。

【０１２０】

また、本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【０１２１】

さらに、本実施の形態においては、ディスク製造識別情報DiscIDm及びディスク記録識別情報DiscIDmは、Ｍ系列符号を用いて暗号化したが、本発明はこれに限定されない。例えば、通常使用しない変調方式を使ったり、通常使用しないエリアに書いたり、すかし（wa

termark）のように希薄化した情報を光ディスク全体など広い範囲に分散させて書くことによっても、上記識別情報に対するアクセスを阻止することができる。

【０１２２】

【発明の効果】

上述のように、本発明においては、製造者により予め記録媒体に記録された第１の識別情報と、記録装置により記録媒体に記録された第２の識別情報との両方に基づいて、情報の暗号化／復号を行っている。従って、本発明によると、記録媒体に記録された情報について従来よりも確実に不正コピーを抑制することができる。

【０１２３】

すなわち、たとえ製造業者が同一の第１の識別情報を記録した記録媒体を複数製造しても、記録装置がそれぞれ別個の第２の識別情報を記録するので、識別情報全体として別個のものとなり、この識別情報にアクセスされない限り不正コピーを防ぐことが可能となる。

【０１２４】

また、たとえ記録装置が持つ第２の識別情報の記録方法を不正者が盗んだとしても、それだけでは製造業者が記録した第１の識別情報にアクセスすることはできず、この場合も不正コピーを防ぐことが可能となる。

【図面の簡単な説明】

【図１】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

【図２】特願平10－025310号明細書に記載されている記録方法により光ディスクに記録されるデータを説明する図である。

【図３】光ディスクに記録されるデータを説明する図である。

【図４】暗号化部の内部の構成を示す図である。

【図５】復号部の内部の構成を示す図である。

【図６】　DiscIDm書き込み装置の内部の構成を示す図である。

【図７】　DiscIDm書き込み装置の動作を説明するフローチャートである。

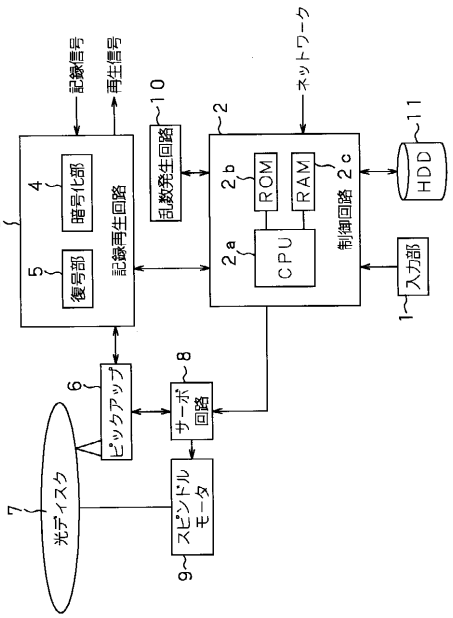
【図８】の暗号化部の動作を説明するフローチャートである。

【図９】の復号部の動作を説明するフローチャートである。

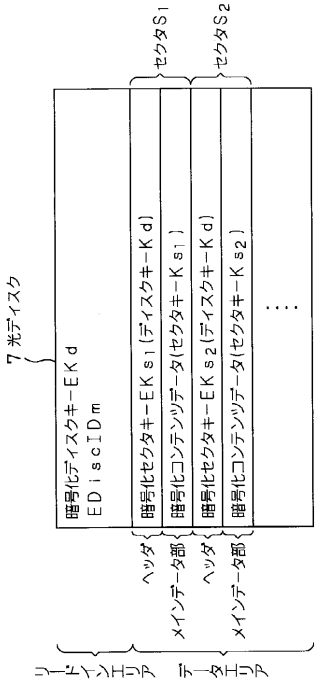
【符号の説明】

１　入力部，２　制御回路，３　記録再生回路，４　暗号化部，５　復号部，６　ピックアップ，７　光ディスク，８　サーボ回路，９　スピンドルモータ，１０　乱数発生回路，２１　DiscID暗号化復号回路，２２　M系列符号発生回路，２３　Kem発生モジュール，２４　Kmメモリ，２５　hash関数回路，２６　Kd暗号化復号回路，２７　Ks暗号化回路，２８　コンテンツデータ暗号化回路，５１　EDiscID復号回路，５２　M系列符号発生回路，５３　Kem発生モジュール，５４　Kmメモリ，５５　hash関数回路，５６　EKd復号回路，５７　EKs復号回路，５８　コンテンツデータ復号回路

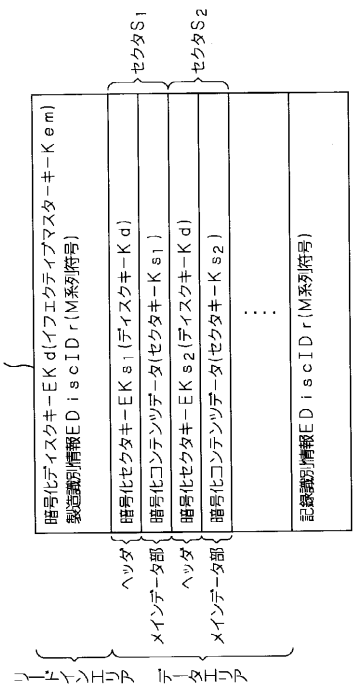
【図１】


記録信号
再生信号
ネットワーク
3
4
暗号化部
5
復号部
記録再生回路
乱数発生回路
10
2
2b
ROM
RAM
2a
CPU
制御回路
2c
HDD
11
入力部
1
6
ピックアップ
8
サーボ回路
9
スピンドルモータ
7
光ディスク

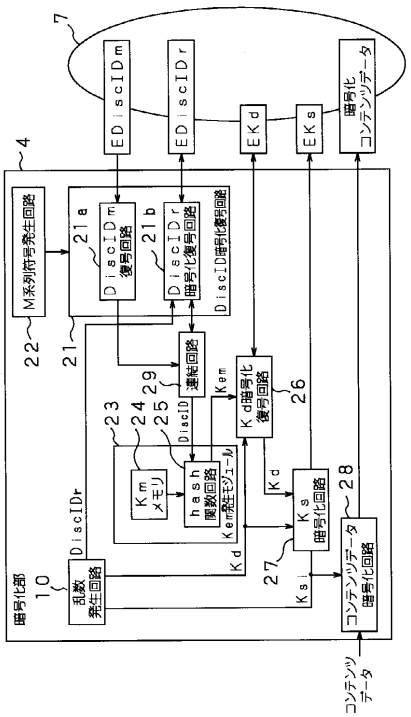
【図２】


セクタS1
セクタS2
7 光ディスク
暗号化ディスクキーEKd
EDiscIDm
暗号化セクタキーEKs1(ディスクキーKd)
暗号化コンテンツデータ(セクタキーKs1)
暗号化セクタキーEKs2(ディスクキーKd)
暗号化コンテンツデータ(セクタキーKs2)
ヘッダ
メインデータ部
ヘッダ
メインデータ部
リードインエリア
データエリア

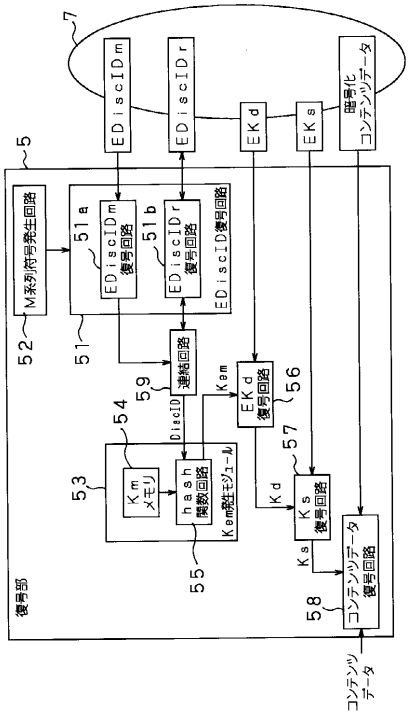
【図３】


7 光ディスク
暗号化ディスクキーEKd(イフエクティブマスターキーKem)
製造識別情報EDiscIDr(M系列符号)
暗号化セクタキーEKs1(ディスクキーKd)
暗号化コンテンツデータ(セクタキーKs1)
暗号化セクタキーEKs2(ディスクキーKd)
暗号化コンテンツデータ(セクタキーKs2)
記録識別情報EDiscIDr(M系列符号)
セクタS1
セクタS2
ヘッダ
メインデータ部
ヘッダ
メインデータ部
リードインエリア
データエリア

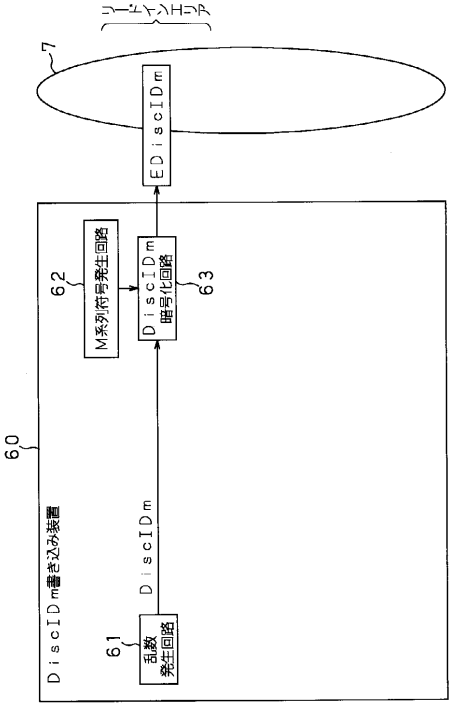
【図４】


7
EDiscIDm
EDiscIDr
EKd
EKs
暗号化コンテンツデータ
4
M系列符号発生回路
22
21
21a
DiscIDm復号回路
21b
DiscIDr暗号化復号回路
DiscID暗号化復号回路
23
24
25
29
Kmメモリ
hash関数回路
Km発生モジュール
DiscID
連結回路
Km
Kd暗号化復号回路
26
暗号化部
10
乱数発生回路
DiscIDr
Kd
Ksi
27
Ks暗号化回路
Kd
28
コンテンツデータ暗号化回路
コンテンツデータ

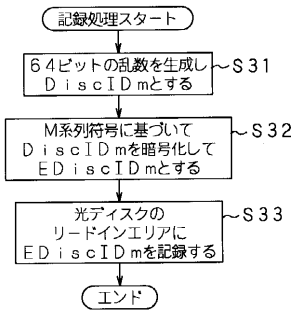
【図５】


7
EDiscIDm
EDiscIDr
EKd
EKs
暗号化コンテンツデータ
5
M系列符号発生回路
51a
EDiscIDm復号回路
51b
EDiscIDr復号回路
EDiscID復号回路
52
51
59
連結回路
DiscID
Kam
EKd復号回路
56
54
57
53
Km メモリ
hash関数回路
Kam発生モジュール
Kd
Ks復号回路
55
Ks
58
コンテンツデータ復号回路
復号部
コンテンツデータ

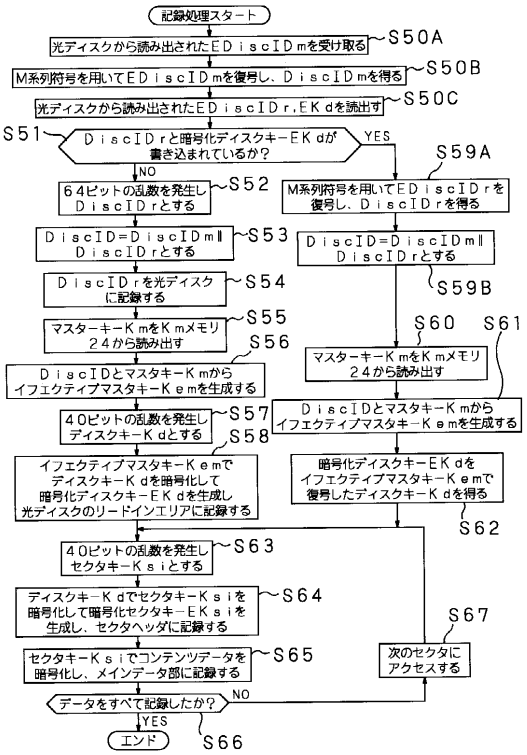
【図６】


コンピュータハードディスク
7
EDiscIDm
62
M系列符号発生回路
DiscIDm暗号化回路
63
60
DiscIDm書き込み装置
DiscIDm
61
乱数発生回路

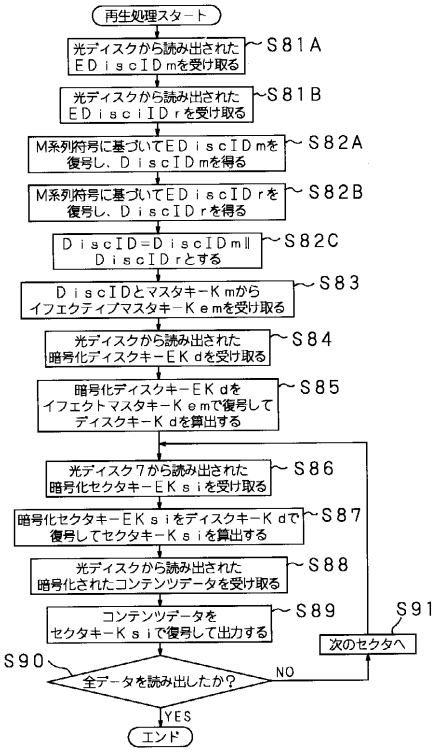
【図７】


記録処理スタート
64ビットの乱数を生成しDiscIDmとする
S31
M系列符号に基づいてDiscIDmを暗号化してEDiscIDmとする
S32
光ディスクのリードインエリアにEDiscIDmを記録する
S33
エンド

【図８】


記録処理スタート
光ディスクから読み出されたEDiscIDmを受け取る
S50A
M系列符号を用いてEDiscIDmを復号し、DiscIDmを得る
S50B
光ディスクから読み出されたEDiscIDr,EKdを読出す
S50C
S51
DiscIDrと暗号化ディスクキーEKdが書き込まれているか?
YES
NO
S59A
64ビットの乱数を発生しDiscIDrとする
S52
M系列符号を用いてEDiscIDrを復号し、DiscIDrを得る
DiscID=DiscIDm‖DiscIDrとする
S53
DiscID=DiscIDm‖DiscIDrとする
S59B
DiscIDrを光ディスクに記録する
S54
マスターキーKmをKmメモリ24から読み出す
S55
S60
S61
マスターキーKmをKmメモリ24から読み出す
S56
DiscIDとマスタキーKmからイフェクティブマスタキーKemを生成する
40ビットの乱数を発生しディスクキーKdとする
S57
DiscIDとマスタキーKmからイフェクティブマスタキーKemを生成する
S58
イフェクティブマスタキーKemでディスクキーKdを暗号化して暗号化ディスクキーEKdを生成し光ディスクのリードインエリアに記録する
暗号化ディスクキーEKdをイフェクティブマスタキーKemで復号したディスクキーKdを得る
S62
40ビットの乱数を発生しセクタキーKsiとする
S63
ディスクキーKdでセクタキーKsiを暗号化して暗号化セクタキーEKsiを生成し、セクタヘッダに記録する
S64
S67
セクタキーKsiでコンテンツデータを暗号化し、メインデータ部に記録する
S65
次のセクタにアクセスする
データをすべて記録したか?
NO
YES
エンド
S66

【図９】


再生処理スタート
光ディスクから読み出された EDiscIDmを受け取る
S81A
光ディスクから読み出された EDiscIDrを受け取る
S81B
M系列符号に基づいてEDiscIDmを復号し、DiscIDmを得る
S82A
M系列符号に基づいてEDiscIDrを復号し、DiscIDrを得る
S82B
DiscID=DiscIDm‖DiscIDrとする
S82C
DiscIDとマスタキーKmからイフェクティブマスタキーKemを受け取る
S83
光ディスクから読み出された暗号化ディスクキーEKdを受け取る
S84
暗号化ディスクキーEKdをイフェクトマスタキーKemで復号してディスクキーKdを算出する
S85
光ディスク7から読み出された暗号化セクタキーEKsiを受け取る
S86
暗号化セクタキーEKsiをディスクキーKdで復号してセクタキーKsiを算出する
S87
光ディスクから読み出された暗号化されたコンテンツデータを受け取る
S88
コンテンツデータをセクタキーKsiで復号して出力する
S89
次のセクタへ
S91
全データを読み出したか？
S90
NO
YES
エンド

フロントページの続き

審査官　高野　美帆子

(56)参考文献　特開平０９－１３９０２３（ＪＰ，Ａ）
特開平０９－１９８７７８（ＪＰ，Ａ）
特開平１１－２２４４６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G11B 20/10
G06F 12/14
G09C 1/00