(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2004-14112
(P2004-14112A)
(43)公開日　平成16年1月15日(2004.1.15)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11B 20/10	G11B 20/10	H	5D044
G11B 20/12	G11B 20/12		5D110
G11B 27/00	G11B 27/00	D	5J104
H04L 9/32	H04L 9/00	675A	

審査請求 未請求　請求項の数 4　OL　（全 26 頁）

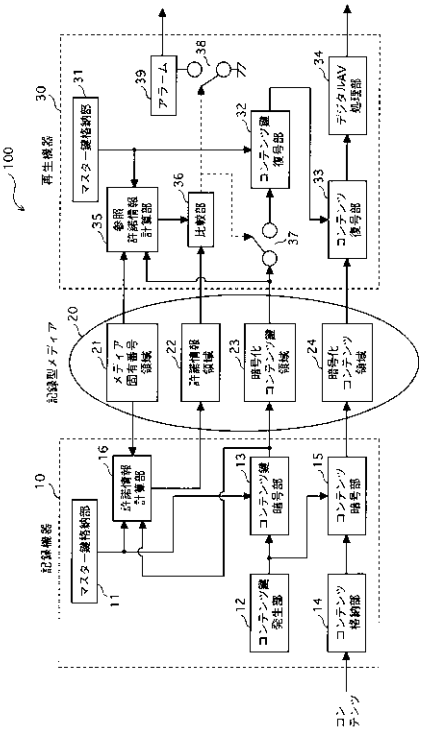
(21)出願番号　特願2003-288652(P2003-288652)
(22)出願日　平成15年8月7日(2003.8.7)
(62)分割の表示　特願2002-229221(P2002-229221)の分割
原出願日　平成14年8月6日(2002.8.6)
(31)優先権主張番号　特願2001-240778(P2001-240778)
(32)優先日　平成13年8月8日(2001.8.8)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2001-260932(P2001-260932)
(32)優先日　平成13年8月30日(2001.8.30)
(33)優先権主張国　日本国(JP)

(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　100090446
弁理士　中島　司朗
(72)発明者　中野　稔久
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　原田　俊治
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　松崎　なつめ
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】著作権保護システム、記録機器及び復号機器

(57)【要約】
【課題】　記録型メディアがオリジナルのものかコピーのものかをチェックし、オリジナルのもののみ再生することのできる著作権保護システムを提供する。
【解決手段】　記録型メディア２０には、メディア固有のメディア固有番号が書き替え不可能な状態で記録されており、記録機器１０は暗号化コンテンツと、暗号化コンテンツの復号に利用されるための暗号化コンテンツ鍵と、暗号化コンテンツ鍵及びメディア固有番号の両方を反映して生成された許諾情報とを記録型メディア２０に書込み、再生機器３０は、記録型メディア２０に記録されたメディア固有番号と暗号化コンテンツ鍵と許諾情報とを取得して、当該許諾情報が当該メディア固有番号と当該暗号化コンテンツ鍵との両方を反映しているか否かを判定し、両方を反映している場合にのみ記録型メディア２０に記録された暗号化コンテンツ鍵を復号し、復号されたコンテンツ鍵を用いて暗号化コンテンツを復号する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
記録媒体毎に異なる媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器と、暗号化コンテンツが記録された当該記録媒体から暗号化コンテンツを読み出して復号する復号機器とからなる著作権保護システムであって、
前記記録機器は、
前記暗号化コンテンツの暗号化に利用する乱数を生成して、前記記録媒体に記録された媒体固有番号と前記生成した乱数との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該乱数との両方を反映した許諾情報を生成する生成手段と、
前記許諾情報と前記乱数と前記暗号化コンテンツとを前記記録媒体に記録する記録手段と
を備え、
前記復号機器は、
記録媒体に記録された媒体固有番号と乱数と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該乱数との両方を用いて前記特定の演算により導出されるものであるか否かを判定する判定手段と、
前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記乱数を利用して復号する復号手段と、
前記判定手段により、否定判定された場合に、警告を発生する警告発生手段と
を備えることを特徴とする著作権保護システム。
【請求項２】
記録媒体固有の媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器であって、
前記暗号化コンテンツの暗号化に利用する乱数を生成して、前記記録媒体に記録された媒体固有番号と前記生成した乱数との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該乱数との両方を反映した許諾情報を生成する生成手段と、
前記許諾情報と前記乱数と前記暗号化コンテンツとを前記記録媒体に記録する記録手段と
を備えることを特徴とする記録機器。
【請求項３】
記録媒体固有の媒体固有番号が記録された書き替え不能領域を有し、暗号化コンテンツと当該暗号化コンテンツの復号に利用されるための乱数と当該暗号化コンテンツの復号を許諾するか否かの判定に利用されるための許諾情報とが記録された記録媒体から暗号化コンテンツを読み出して復号する復号機器であって、
記録媒体に記録された媒体固有番号と乱数と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該乱数との両方を用いて前記特定の演算により導出されるものであるか否かを判定する判定手段と、
前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記乱数を利用して復号する復号手段と、
前記判定手段により、否定判定された場合に、警告を発生する警告発生部と
を備えることを特徴とする復号機器。
【請求項４】
書き替え不可能な領域と書き替え可能な領域とを有し、
前記書き替え不可能な領域には、記録媒体毎に固有の媒体固有番号が記録されており、
前記書き替え可能な領域には、
暗号化されたコンテンツである暗号化コンテンツと
前記暗号化コンテンツの復号に必要な乱数と
前記媒体固有番号と前記乱数との両方を用いた特定の演算により導出される許諾情報で

あって、前記媒体固有番号と前記乱数との両方が反映された許諾情報とが記録されている
ことを特徴とする記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、媒体固有番号が記録された書込み可能な記録型メディアを利用して、記録型メディアに記録されたコンテンツの著作権を保護する技術に関する。

【背景技術】

【０００２】

近年、デジタル放送により放送される映画等のコンテンツを受信して光ディスク等の記録媒体に記録し、再生する機器を用いたコンテンツ利用形態が普及している。その一方で、このような機器によって記録媒体に記録されたコンテンツを、パーソナルコンピュータ等を利用して別の記録媒体に違法にコピーするケースが増加している。

この違法コピーされたコンテンツを再生不能にする技術として、従来、図１０に示す著作権保護システムが知られている。

【０００３】

同図において著作権保護システムは、コンテンツを暗号化して記録型メディア２０００に記録する記録機器１０００と、記録型メディア２０００に記録された暗号化コンテンツを復号、再生する再生機器３０００とから構成される。

記録型メディア２０００は、光ディスク等の記録媒体であり、メディア固有番号が記録されたメディア固有番号領域２００１を有する。メディア固有番号は、各記録型メディア毎に固有の識別子で、記録型メディアの製造時に記録される。メディア固有番号領域２００１は、製造時の記録以後に当該メディア固有番号を書き替えることができないよう保護されている。

【０００４】

記録機器１０００は、外部からコンテンツを取得してコンテンツ格納部１００４に格納する。

記録機器１０００に記録型メディア２０００が接続されると、コンテンツ暗号部１００５は、コンテンツ格納部１００４に格納されたコンテンツを読み出してコンテンツ鍵により暗号化し、記録型メディア２０００の暗号化コンテンツ領域２００３に記録する。コンテンツ鍵は、コンテンツ鍵発生部１００２で発生される乱数である。コンテンツ鍵暗号部１００３は、コンテンツ鍵をコンテンツ鍵暗号鍵で暗号化して記録型メディア２０００の暗号化コンテンツ鍵領域２００２に記録する。コンテンツ鍵暗号鍵は、鍵暗号鍵計算部１００１により算出される鍵である。鍵暗号鍵計算部１００１は、メディア固有番号領域２００１に記録されたメディア固有番号とマスター鍵とを用いてハッシュ関数によりコンテンツ鍵暗号鍵を算出する。ここでマスター鍵は、記録機器１０００と再生機器３０００とが第三者には秘密にして予め所有している鍵である。

【０００５】

図１１は、鍵暗号鍵計算部１００１の内部の演算機構を示す。

メディア固有番号はＡ点から入力され、ＤＥＳ暗号部４０００においてマスター鍵格納部４００１に保持されるマスター鍵を用いてＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）により暗号化される。暗号化されたメディア固有番号は、排他論理和回路４００２においてメディア固有番号との排他論理和が算出され、その結果がＢより出力される。このＢの出力がコンテンツ鍵暗号鍵である。

【０００６】

再生機器３０００に記録型メディア２０００が接続されると、鍵復号鍵計算部３００１は、記録型メディア２０００のメディア固有番号領域２００１からメディア固有番号を取得し、記録機器１０００の鍵暗号鍵計算部１００１と同様の演算により、コンテンツ鍵復号鍵を算出する。鍵暗号鍵計算部１００１と鍵復号鍵計算部３００１とのそれぞれが、同じ値のマスター鍵とメディア固有番号とを用いていれば、コンテンツ鍵暗号鍵とコンテン

ツ鍵復号鍵とは同じ値になる。
【０００７】
コンテンツ鍵復号部３００２は、暗号化コンテンツ鍵領域２００２から暗号化コンテンツ鍵を読み出し、それをコンテンツ鍵復号鍵で復号し、コンテンツ鍵を得る。このコンテンツ鍵は、コンテンツ鍵一時格納部３００３に一時的に格納される。
コンテンツ復号部３００４は、暗号化コンテンツ領域２００３から暗号化コンテンツを読み出し、それをコンテンツ鍵で復号し、コンテンツを得る。
【０００８】
デジタルＡＶ処理部３００５は、復号されたコンテンツをアナログ音声画像データに変換し、外部のスピーカやディスプレイ等に出力する。
以上の構成により、再生機器３０００は、暗号化の際に利用されたメディア固有番号と同じメディア固有番号を利用した場合にのみ、コンテンツ鍵を正しく復号することができる。
【０００９】
言い換えれば、暗号化の際に利用されたメディア固有番号とは異なるメディア固有番号を利用しても、コンテンツ鍵を正しく復号することはできない。
より具体的には、記録型メディア２０００に記録された暗号化コンテンツ鍵及び暗号化コンテンツを他の記録型メディアにコピーし、当該他の記録型メディアを再生機器３０００が再生しようとした場合、記録型メディア２０００と当該他の記録型メディアとではメディア固有番号が異なっているために、再生機器３０００は他の記録型メディアに記録された暗号化コンテンツ鍵から正しいコンテンツ鍵を復号することができない。
【００１０】
このようにして従来の著作権保護システムは、記録機器１０００により記録されたオリジナルのコンテンツのみ、再生機器３０００がコンテンツ鍵を正しく復号することができるようにし、コピーのコンテンツについては再生機器３０００が正しく復号できないようにすることで、違法コピーを無効にしている。
なお、これに関連する技術は特許文献１に記載されている。
【特許文献１】特許第３０７３５９０号明細書
【発明の開示】
【発明が解決しようとする課題】
【００１１】
しかしながら再生機器３０００は、コンテンツがオリジナルのものであるかコピーのものであるかを区別することができず、コピーのコンテンツも復号する。コピーのコンテンツを再生した場合には、正しく復号できていないために、本来のコンテンツの内容とは異なる全くでたらめな映像や音声を出力する。
このことにより、コピーされたコンテンツであることを知らずにそのコンテンツを利用しようとした利用者は、異常な再生の原因がコピーによるものであることがわからずに、機器の故障と勘違いしてしまう場合がある。また異常な再生により機器が破損する場合もある。
【００１２】
上記に鑑みて本発明は、記録型メディアのコンテンツがオリジナルのものかコピーのものかをチェックする機構を設け、そのチェック結果をもちいてオリジナルのもののみ再生し、コピーのものを再生しない著作権保護システムを提供することを目的とする。
【課題を解決するための手段】
【００１３】
上記問題を解決するため、本発明の著作権保護システムは、記録媒体毎に異なる媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器と、暗号化コンテンツが記録された当該記録媒体から暗号化コンテンツを読み出して復号する復号機器とからなる著作権保護システムであって、前記記録機器は、前記暗号化コンテンツの暗号化に利用する乱

数を生成して、前記記録媒体に記録された媒体固有番号と前記生成した乱数との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該乱数との両方を反映した許諾情報を生成する生成手段と、前記許諾情報と前記乱数と前記暗号化コンテンツとを前記記録媒体に記録する記録手段とを備え、前記復号機器は、記録媒体に記録された媒体固有番号と乱数と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該乱数との両方を用いて前記特定の演算により導出されるものであるか否かを判定する判定手段と、前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記乱数を利用して復号する復号手段と、前記判定手段により、否定判定された場合に、警告を発生する警告発生手段とを備える。

【００１４】

本発明の記録機器は、記録媒体固有の媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器であって、前記暗号化コンテンツの暗号化に利用する乱数を生成して、前記記録媒体に記録された媒体固有番号と前記生成した乱数との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該乱数との両方を反映した許諾情報を生成する生成手段と、前記許諾情報と前記乱数と前記暗号化コンテンツとを前記記録媒体に記録する記録手段とを備える。

【００１５】

本発明の復号機器は、記録媒体固有の媒体固有番号が記録された書き替え不能領域を有し、暗号化コンテンツと当該暗号化コンテンツの復号に利用されるための乱数と当該暗号化コンテンツの復号を許諾するか否かの判定に利用されるための許諾情報とが記録された記録媒体から暗号化コンテンツを読み出して復号する復号機器であって、記録媒体に記録された媒体固有番号と乱数と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該乱数との両方を用いて前記特定の演算により導出されるものであるか否かを判定する判定手段と、前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記乱数を利用して復号する復号手段と、前記判定手段により、否定判定された場合に、警告を発生する警告発生部とを備える。

【００１６】

本発明の記録媒体は、書き替え不可能な領域と書き替え可能な領域とを有し、前記書き替え不可能な領域には、記録媒体毎に固有の媒体固有番号が記録されており、前記書き替え可能な領域には、暗号化されたコンテンツである暗号化コンテンツと前記暗号化コンテンツの復号に必要な乱数と前記媒体固有番号と前記乱数との両方を用いた特定の演算により導出される許諾情報であって、前記媒体固有番号と前記乱数との両方が反映された許諾情報とが記録されていることを特徴とする。

【００１７】

また、本発明の著作権保護システムは、記録媒体毎に異なる媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器と、暗号化コンテンツが記録された当該記録媒体から暗号化コンテンツを読み出して復号する復号機器とからなる著作権保護システムであって、前記記録機器は、記録媒体に記録された媒体固有番号と前記暗号化コンテンツの復号に必要な復号情報との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該復号情報との両方を反映した許諾情報を生成する生成手段と、前記許諾情報と前記復号情報と前記暗号化コンテンツとを前記記録媒体に記録する記録手段とを備え、前記復号機器は、記録媒体に記録された媒体固有番号と復号情報と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該復号情報との両方を用いて前記特定の演算により導出されるものであるか否かを判定する判定手段と、前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記復号情報を利用して復号する復号手段とを備えてもよい。

【００１８】

また、前記復号情報は、前記復号情報を用いて所定の演算を行うことにより、前記暗号

化コンテンツを復号するための復号鍵を得ることができるものであり、前記復号手段は、前記復号情報に対して前記所定の演算を行って復号鍵を得る復号鍵演算手段を備え、暗号化コンテンツの復号においては、前記復号鍵を用いて前記暗号化コンテンツからコンテンツを復号するよう構成してもよい。

【００１９】

前記記録機器は、さらに、秘密鍵を外部から取得することによりあるいは予め記憶していることにより所有する記録機器側所有手段と、前記復号鍵を前記秘密鍵を用いて秘密鍵暗号化方式により暗号化して、前記復号情報を生成する復号鍵暗号化手段と、を備え、前記復号機器は、さらに、前記記録機器が所有する秘密鍵と同じ秘密鍵を外部から取得することによりあるいは予め記憶していることにより所有する復号機器側所有手段と、を備え、前記復号鍵演算手段は、前記復号情報を前記秘密鍵を用いて秘密鍵暗号化方式により復号して、復号鍵を得るよう構成してもよい。

【００２０】

前記記録機器の前記生成手段は、さらに、前記特定の演算において、前記媒体固有番号と前記復号情報との他、前記秘密鍵を用い、前記復号機器の前記判定手段は、さらに、前記媒体固有番号と前記復号情報との他、前記復号機器側所有手段に所有される秘密鍵を用いて、前記許諾情報が前記特定の演算により導出されるものであるか否かを判定するよう構成してもよい。

【００２１】

また、前記記録型メディアは、さらに、前記書き替え不能領域に、特定のデバイス鍵を用いた場合にのみ前記秘密鍵を正しく復号することのできる秘密鍵情報が記録されており、前記記録機器側所有手段及び前記復号機器側所有手段は、機器固有のデバイス鍵を予め記憶するデバイス鍵記憶手段と、前記デバイス鍵記憶手段に記憶されるデバイス鍵を用いて前記記録型メディアの秘密鍵情報を復号する秘密鍵復号手段と前記秘密鍵復号手段により前記秘密鍵が正しく復号できた場合にのみ前記秘密鍵を記憶することにより秘密鍵を所有する秘密鍵記憶手段とを備え、前記記録機器及び復号機器は、さらに、前記秘密鍵復号手段により前記秘密鍵が正しく復号できなかった場合には、以降の各手段の処理を中止する中止手段を備えてもよい。

【００２２】

また、前記復号機器において、前記判定手段は、記録媒体に記録された媒体固有番号と復号情報とを用いて、前記生成手段における前記特定の演算と同じ演算を行うことにより、演算結果である参照許諾情報を生成する生成部と、前記参照許諾情報と前記媒体固有番号とを比較し、両者が一致する場合に肯定判定し、両者が一致しない場合に否定判定する比較判定部とを備えてもよい。

【００２３】

また、前記記録機器において、前記生成手段は、前記記録型メディアに記録される暗号化コンテンツ毎に、メディア固有番号と当該暗号化コンテンツについての復号情報とを用いて許諾情報を生成し、前記記録手段は、暗号化コンテンツと復号情報と許諾情報とからなる各組を対応付けて前記記録型メディアに記録し、前記復号機器において、前記判定手段及び前記復号手段は、前記記録型メディアに記録される前記各組毎にそれぞれの処理を行うよう構成してもよい。

【００２４】

また、前記記録機器において、前記生成手段は、前記記録型メディアに記録される各暗号化コンテンツに対応する復号情報の全てとメディア固有番号とを用いて１つの許諾情報を生成するよう構成してもよい。

また、本発明の記録機器は、記録媒体固有の媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器であって、記録媒体に記録された媒体固有番号と前記暗号化コンテンツの復号に必要な復号情報との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該復号情報との両方を反映した許諾情報を生成する生成手段と、前記許諾情

報と前記復号情報と前記暗号化コンテンツとを前記記録媒体に記録する記録手段とを備えてもよい。

【００２５】

また、本発明の復号機器は、記録媒体固有の媒体固有番号が記録された書き替え不能領域を有し、暗号化コンテンツと当該暗号化コンテンツの復号に利用されるための復号情報と当該暗号化コンテンツの復号を許諾するか否かの判定に利用されるための許諾情報とが記録された記録媒体から暗号化コンテンツを読み出して復号する復号機器であって、記録媒体に記録された媒体固有番号と復号情報と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該復号情報との両方を用いて特定の演算により導出されるものであるか否かを判定する判定手段と、前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記復号情報を利用して復号する復号手段とを備えてもよい。

【発明の効果】

【００２６】

本発明の著作権保護システムは、記録媒体毎に異なる媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器と、暗号化コンテンツが記録された当該記録媒体から暗号化コンテンツを読み出して復号する復号機器とからなる著作権保護システムであって、前記記録機器は、前記暗号化コンテンツの暗号化に利用する乱数を生成して、前記記録媒体に記録された媒体固有番号と前記生成した乱数との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該乱数との両方を反映した許諾情報を生成する生成手段と、前記許諾情報と前記乱数と前記暗号化コンテンツとを前記記録媒体に記録する記録手段とを備え、前記復号機器は、記録媒体に記録された媒体固有番号と乱数と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該乱数との両方を用いて前記特定の演算により導出されるものであるか否かを判定する判定手段と、前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記乱数を利用して復号する復号手段と、前記判定手段により、否定判定された場合に、警告を発生する警告発生手段とを備える。

【００２７】

この構成によれば、生成手段は、当該記録媒体に記録された媒体固有番号と暗号化に利用する乱数とを用いて、それら両方を反映した値の許諾情報を生成する。より具体的には、許諾情報は、媒体固有番号と乱数とを結合した値を入力データとして用いて、ハッシュ関数により生成されるハッシュ値である。ハッシュ関数は、不可逆な一方向関数を含むため、許諾情報から媒体固有番号と復号情報とを求めることはできない。また同じ許諾情報が生成される、異なる入力データを作成することは困難である。このハッシュ関数の性質により、許諾情報は、当該許諾情報の生成に用いられた媒体固有番号と乱数とを用いた場合にしか生成することができない。よって、記録媒体の内容がオリジナルのものであって、コピーされたものでなければ、当該記録媒体に記録された許諾情報は、当該記録媒体に記録された媒体固有番号と乱数とを反映しているはずである。このことから、判定手段は、反映しているか否かを判定することで記録媒体の記録内容がオリジナルのものであるかコピーされたものであるかを判定する。より具体的には、判定手段は、媒体固有番号と乱数とを用いて、許諾情報書き込み手段による生成方法と同じ方法により参照許諾情報を生成し、参照許諾情報と記録媒体に記録された参照許諾情報とを比較し、双方の値が一致するか否かにより判定を行う。そして復号手段は、オリジナルの記録媒体のみコンテンツを復号し、コピーの記録媒体のコンテンツを復号しない。これにより不正にコンテンツが他の記録媒体にコピーされて利用されることを阻止する。

【００２８】

また、本発明の著作権保護システムは、記録媒体毎に異なる媒体固有番号が記録された書き替え不能領域を有する書込み可能な記録媒体に対して、暗号化されたコンテンツである暗号化コンテンツを記録する記録機器と、暗号化コンテンツが記録された当該記録媒体

から暗号化コンテンツを読み出して復号する復号機器とからなる著作権保護システムであって、前記記録機器は、記録媒体に記録された媒体固有番号と前記暗号化コンテンツの復号に必要な復号情報との両方を用いた特定の演算を行うことにより、当該媒体固有番号と当該復号情報との両方を反映した許諾情報を生成する生成手段と、前記許諾情報と前記復号情報と前記暗号化コンテンツとを前記記録媒体に記録する記録手段とを備え、前記復号機器は、記録媒体に記録された媒体固有番号と復号情報と許諾情報との全てを用いることにより、当該許諾情報が当該媒体固有番号と当該復号情報との両方を用いて前記特定の演算により導出されるものであるか否かを判定する判定手段と、前記判定手段により肯定判定された場合に限り、前記記録媒体に記録された暗号化コンテンツを前記復号情報を利用して復号する復号手段とを備える。

【００２９】

この構成によれば、生成手段は、当該記録媒体に記録された媒体固有番号と暗号化コンテンツを復号するための復号情報とを用いて、それら両方を反映した値の許諾情報を生成する。より具体的には、許諾情報は、媒体固有番号と復号情報とを結合した値を入力データとして用いて、ハッシュ関数により生成されるハッシュ値である。ハッシュ関数は、不可逆な一方向関数を含むため、許諾情報から媒体固有番号と復号情報とを求めることはできない。また同じ許諾情報が生成される、異なる入力データを作成することは困難である。このハッシュ関数の性質により、許諾情報は、当該許諾情報の生成に用いられた媒体固有番号と復号情報とを用いた場合にしか生成することができない。よって、記録媒体の内容がオリジナルのものであって、コピーされたものでなければ、当該記録媒体に記録された許諾情報は、当該記録媒体に記録された媒体固有番号と復号情報とを反映しているはずである。このことから、判定手段は、反映しているか否かを判定することで記録媒体の記録内容がオリジナルのものであるかコピーされたものであるかを判定する。より具体的には、判定手段は、媒体固有番号と復号情報とを用いて、許諾情報書き込み手段による生成方法と同じ方法により参照許諾情報を生成し、参照許諾情報と記録媒体に記録された参照許諾情報とを比較し、双方の値が一致するか否かにより判定を行う。そして復号手段は、オリジナルの記録媒体のみコンテンツを復号し、コピーの記録媒体のコンテンツを復号しない。これにより不正にコンテンツが他の記録媒体にコピーされて利用されることを阻止する。

【発明を実施するための最良の形態】

【００３０】

＜第１実施形態＞

以下、本発明の第１実施形態について図面を用いて説明する。

＜構成＞

図１は、第１実施形態の著作権保護システム１００の構成を示すブロック図である。

同図において著作権保護システム１００は、記録型メディア２０に暗号化コンテンツを記録する記録機器１０と記録型メディア２０に記録された暗号化コンテンツを復号して再生する再生機器３０とから構成される。以下では、まず記録型メディア２０について説明し、続いて記録機器１０の構成及び再生機器３０の構成について説明する。

＜記録型メディア２０＞

記録型メディア２０は、光ディスクであり、メディア固有番号が記録された書き替え不可能なメディア固有番号領域２１と、記録可能な記録領域とを有する。

【００３１】

メディア固有番号は、各記録型メディア毎に固有の、６４ビットの識別子で、記録型メディアの製造時においてメディア固有番号領域２１に書込まれる。メディア固有番号領域２１は、製造時の書込み以後に当該メディア固有番号を書き替えることができないよう保護されている。

記録領域は、記録機器１０により許諾情報領域２２、暗号化コンテンツ鍵領域２３及び暗号化コンテンツ領域２４が確保され、記録機器１０によって各種データが記録される。

【００３２】

暗号化コンテンツ領域２４には、記録機器１０により暗号化コンテンツが記録される。

暗号化コンテンツ鍵領域２３には、記録機器１０により暗号化コンテンツ鍵が記録される。

暗号化コンテンツ鍵は、再生機器３０が暗号化コンテンツを復号する際に必要とする情報であり、コンテンツ鍵を暗号化したものである。コンテンツ鍵は、コンテンツの暗号化及び復号で共通に用いられる秘密鍵暗号方式の秘密鍵である。

【００３３】

許諾情報領域２２には、記録機器１０により許諾情報が記録される。

許諾情報は、記録型メディア２０に記録されたデータが記録機器１０による記録当初のものであることを証明するための情報である。記録当初のものであるとは、記録型メディアがオリジナルのものであって、他の記録媒体等からコピーされたものではないことを意味する。再生機器３０は、この許諾情報を確認することにより、記録型メディアがオリジナルのものかコピーのものかを判別することができる。許諾情報については後に詳しく説明する。

＜記録機器１０の構成＞

次に記録機器１０の構成を説明する。

【００３４】

記録機器１０は、マスター鍵格納部１１、コンテンツ鍵発生部１２、コンテンツ鍵暗号部１３、コンテンツ格納部１４、コンテンツ暗号部１５及び許諾情報計算部１６を備える。

マスター鍵格納部１１は、５６ビットのマスター鍵が予め格納されたメモリである。マスター鍵は、記録機器１０と再生機器３０とが共通に、外部には秘匿にして所有している鍵である。

【００３５】

コンテンツ鍵発生部１２は、乱数をコンテンツ鍵として発生させる乱数発生器である。コンテンツ鍵発生部１２は、記録機器１０の制御回路（図示せず）が出力する起動信号を受信すると、５６ビットのランダムデータを１つ生成し、これをコンテンツ鍵として出力する。

コンテンツ鍵暗号部１３は、コンテンツ鍵をマスター鍵で暗号化して記録型メディア２０に記録するものである。暗号化アルゴリズムとしては、例えばＤＥＳを用いている。コンテンツ鍵暗号部１３は、コンテンツ鍵発生部１２により発生されたコンテンツ鍵とマスター鍵格納部１１に格納されているマスター鍵とを取得して、コンテンツ鍵をマスター鍵で暗号化し、６４ビットの暗号化コンテンツ鍵を得る。そして記録型メディア２０の記録領域に暗号化コンテンツ鍵領域２３を確保し、その領域に暗号化コンテンツ鍵を記録する。

【００３６】

コンテンツ格納部１４は、ハードディスクの類の記憶装置であり、外部から入力されるコンテンツを記録、保持する。外部から入力される状況として、例えば、衛星放送受信装置が、デジタル衛星放送により放送されたデジタル映画コンテンツを受信して、そのコンテンツをコンテンツ格納部１４に蓄積させるという状況である。

コンテンツ暗号部１５は、コンテンツをコンテンツ鍵で暗号化して記録型メディア２０に記録するものである。暗号化アルゴリズムとしては、例えばＤＥＳを用いている。コンテンツ暗号部１５は、コンテンツ鍵発生部１２により発生されたコンテンツ鍵とコンテンツ格納部１４に記録されているコンテンツとを取得し、コンテンツを６４ビットずつのブロックに区切り、各ブロック毎にコンテンツ鍵で暗号化する。そして記録型メディア２０の記録領域に暗号化コンテンツ領域２４を確保し、その領域に、暗号化されたブロックの集合である暗号化コンテンツを記録する。

【００３７】

許諾情報計算部１６は、許諾情報を生成する演算機構である。許諾情報計算部１６は、まず、メディア固有番号領域２１に記録されたメディア固有番号と、コンテンツ鍵暗号部

１３による暗号化結果である暗号化コンテンツ鍵と、マスター鍵格納部１１に格納されているマスター鍵とを取得する。次にメディア固有番号、マスター鍵及び暗号化コンテンツ鍵を連結して１つのビット列にし、そのビット列を入力としてＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）等のハッシュ関数による演算を行う。その結果、１６０ビットのハッシュ値を得て、このハッシュ値を許諾情報とする。最後に、記録型メディア２０の記録領域に許諾情報領域２２を確保し、その領域に許諾情報を記録する。

【００３８】

ここでハッシュ関数ＳＨＡ－１について説明する。

ハッシュ関数ＳＨＡ－１は、認証やデジタル署名等に使われるハッシュ関数の一つである。この関数は、２の６４乗以下のデータから１６０ビットのハッシュ値を生成する。ハッシュ関数ＳＨＡ－１は、不可逆な一方向関数を含むため、ハッシュ値から元のデータを再現することはできない。また同じハッシュ値を生成する別のデータを生成することは極めて困難である。この性質を利用して、送信側はデータとデータから生成されたハッシュ値とを受信側に送り、受信側は受信したデータからハッシュ値を生成して、生成したハッシュ値を受信したハッシュ値と比較することで、通信途中でデータが改ざんされていないかを検出することができる。

【００３９】

ハッシュ関数ＳＨＡ－１の性質により、許諾情報は、許諾情報の生成に使われたメディア固有番号、暗号化コンテンツ鍵及びマスター鍵以外の他の値から生成することが困難であるといえる。つまり許諾情報は、許諾情報の生成に使われたメディア固有番号、暗号化コンテンツ鍵及びマスター鍵のすべてを反映していることとなる。

よって許諾情報は、許諾情報に反映されたメディア固有番号、暗号化コンテンツ鍵及びマスター鍵が、メディア固有番号領域２１に記録されたメディア固有番号、暗号化コンテンツ鍵領域２３に記録された暗号化コンテンツ鍵、記録機器１０が所有するマスター鍵のそれぞれと同じものであることにより、メディア固有番号、暗号化コンテンツ鍵及びマスター鍵の正当性を証明する。

＜再生機器３０の構成＞

次に再生機器３０の構成を説明する。

【００４０】

再生機器３０は、マスター鍵格納部３１、コンテンツ鍵復号部３２、コンテンツ復号部３３、デジタルＡＶ処理部３４、参照許諾情報計算部３５、比較部３６、第１スイッチ３７、第２スイッチ３８及びアラーム３９を備える。

マスター鍵格納部３１は、５６ビットのマスター鍵が予め格納されたメモリである。このマスター鍵は記録機器１０のマスター鍵格納部１１に格納されているものと同じ値である。

【００４１】

コンテンツ鍵復号部３２は、記録型メディア２０に記録された暗号化コンテンツ鍵をマスター鍵で復号するものである。コンテンツ鍵復号部３２は、暗号化コンテンツ鍵領域２３に記録されている暗号化コンテンツ鍵とマスター鍵格納部３１に格納されているマスター鍵とを取得し、暗号化コンテンツ鍵をマスター鍵で復号し、コンテンツ鍵を得る。

コンテンツ復号部３３は、記録型メディア２０に記録された暗号化コンテンツをコンテンツ鍵で復号してデジタルＡＶ処理部３４に出力するものである。コンテンツ復号部３３は、コンテンツ鍵復号部３２により復号されたコンテンツ鍵と暗号化コンテンツ領域２４に記録されている暗号化コンテンツとを取得し、暗号化コンテンツを６４ビットずつのブロックに区切り、各ブロック毎にコンテンツ鍵で復号する。そして復号されたブロックの集合であるコンテンツをデジタルＡＶ処理部３４に出力する。

【００４２】

デジタルＡＶ処理部３４は、コンテンツ復号部３３からコンテンツを取得して、コンテンツをアナログ音声画像データに変換し、外部のスピーカやディスプレイ等に出力する。

第１スイッチ３７は、比較部３６からの制御に応じて開閉し、第１スイッチ３７が閉じ

ているとき暗号化コンテンツ鍵領域２３からコンテンツ鍵復号部３２へ暗号化コンテンツ鍵が読み出され、第１スイッチ３７が開いているとき暗号化コンテンツ鍵の読み出しが制止される。

【００４３】

第２スイッチ３８は、比較部３６からの制御に応じて開閉し、第２スイッチ３８が閉じているときアラーム３９に電源が供給され、開いているとき供給されない。

アラーム３９は、電源が供給されているとき動作して、警告音を発生させる回路である。

参照許諾情報計算部３５は、許諾情報計算部１６と同じ演算を行って参照許諾情報を生成する演算機構である。参照許諾情報計算部３５は、メディア固有番号領域２１に記録されたメディア固有番号と、暗号化コンテンツ鍵領域２３に記録された暗号化コンテンツ鍵と、マスター鍵格納部３１に格納されているマスター鍵とを取得する。次に、参照許諾情報計算部３５は、メディア固有番号、マスター鍵及び暗号化コンテンツ鍵を連結して１つのビット列にする。ここで各データを連結する順番は、許諾情報計算部１６における連結の順番と同じである。そして参照許諾情報計算部３５は、そのビット列を入力としてＳＨＡ－１等のハッシュ関数による演算を行う。その結果、１６０ビットのハッシュ値を得て、このハッシュ値を参照許諾情報とする。

【００４４】

比較部３６は、許諾情報領域２２に記録された許諾情報と参照許諾情報計算部３５により生成された参照許諾情報とを取得してそれら２つの値を比較し、一致するときのみ暗号化コンテンツを復号させるよう制御し、不一致のとき暗号化コンテンツの復号を制止してアラーム３９に警告音を発生させるよう制御する。

より詳しくは比較の結果、許諾情報と参照許諾情報とが一致する場合、第１スイッチ３７を閉じて暗号化コンテンツ鍵領域２３の暗号化コンテンツ鍵がコンテンツ鍵復号部３２に読み出されるようにする。これによりコンテンツ鍵が復号され、コンテンツが復号及び再生される。

【００４５】

比較の結果、許諾情報と参照許諾情報とが一致しない場合には、第１スイッチ３７を開き、第２スイッチ３８を閉じる。第１スイッチ３７を開くことにより、暗号化コンテンツ鍵領域２３の暗号化コンテンツ鍵はコンテンツ鍵復号部３２に読み出されないために、コンテンツ鍵が復号されず、コンテンツも復号及び再生されない。第２スイッチ３８を閉じることにより、アラーム３９に電源が供給され、アラーム３９が動作する。

【００４６】

参照許諾情報計算部３５及び比較部３６は、メディア固有番号領域２１に記録されたメディア固有番号と、暗号化コンテンツ鍵領域２３に記録された暗号化コンテンツ鍵と、マスター鍵格納部３１に格納されているマスター鍵とのすべてが許諾情報領域２２に記録されている許諾情報に反映されているか否かを見極め、反映している場合に限り暗号化コンテンツが復号されるように各部を制御し、反映していない場合には暗号化コンテンツの復号を制止し、警告音が発生されるよう制御する。

【００４７】

参照許諾情報の生成に使われるメディア固有番号、暗号化コンテンツ鍵、マスター鍵のそれぞれと、許諾情報の生成に使われるメディア固有番号、暗号化コンテンツ鍵、マスター鍵のそれぞれとが、いずれも同じ値である場合に限り、許諾情報と参照許諾情報とは同じ値になる。逆に言えば、参照許諾情報の生成に使われるメディア固有番号、暗号化コンテンツ鍵、マスター鍵のそれぞれと、許諾情報の生成に使われるメディア固有番号、暗号化コンテンツ鍵、マスター鍵のそれぞれとで、いずれか１つでも異なっていれば、許諾情報と参照許諾情報とは異なる値になる。

＜動作＞

以上のように構成された記録機器１０及び再生機器３０について、それぞれの動作を説明する。

【００４８】
図２は、記録機器１０の処理手順を示すフローチャートである。
まず、コンテンツ鍵発生部１２は、コンテンツ鍵を生成する（ステップＳ２０１）。
次に、コンテンツ鍵暗号部１３は、マスター鍵格納部１１からマスター鍵を読み出す（ステップＳ２０２）。
続いて、コンテンツ鍵暗号部１３は、生成されたコンテンツ鍵をマスター鍵で暗号化して、その結果、暗号化コンテンツ鍵を得る（ステップＳ２０３）。
【００４９】
コンテンツ鍵暗号部１３は、記録型メディア２０の記録領域に暗号化コンテンツ鍵領域２３を確保し、その領域に暗号化コンテンツ鍵を記録する（ステップＳ２０４）。
コンテンツ暗号部１５は、コンテンツ格納部１４に格納されたコンテンツを読み出し、コンテンツを６４ビットのブロックに区切りつつ、ブロック毎にコンテンツ鍵で暗号化し、暗号化コンテンツを生成する（ステップＳ２０５）。
【００５０】
続いて、コンテンツ暗号部１５は、記録型メディア２０に暗号化コンテンツ領域２４を確保し、その領域に生成された暗号化コンテンツを記録する（ステップＳ２０６）。
許諾情報計算部１６は、記録型メディア２０のメディア固有番号領域２１からメディア固有番号を読み出す（ステップＳ２０７）。
続いて、許諾情報計算部１６は、読み出したメディア固有番号と、マスター鍵格納部１１のマスター鍵と、コンテンツ鍵暗号部１３の出力である暗号化コンテンツ鍵とを用いて、ハッシュ関数により許諾情報を生成する（ステップＳ２０８）。
【００５１】
最後に、許諾情報計算部１６は、記録型メディア２０の記録領域に許諾情報領域２２を確保し、その領域に生成した許諾情報を記録する（ステップＳ２０９）。
図３は、再生機器３０の処理手順を示すフローチャートである。
参照許諾情報計算部３５は、記録型メディア２０のメディア固有番号領域２１からメディア固有番号を読み出し、暗号化コンテンツ鍵領域２３から暗号化コンテンツ鍵を読み出す。また比較部３６は、許諾情報領域２２から許諾情報を読み出す（ステップＳ３０１）。
【００５２】
次に、参照許諾情報計算部３５は、マスター鍵格納部３１からマスター鍵を読み出す（ステップＳ３０２）。
続いて、参照許諾情報計算部３５は、メディア固有番号と暗号化コンテンツ鍵とマスター鍵とを用いて、ハッシュ関数により参照許諾情報を生成する。この生成の演算手順は、ステップＳ２０８と同じである（ステップＳ３０３）。
【００５３】
比較部３６は、記録型メディア２０から読み出した許諾情報と参照許諾情報計算部３５により生成された参照許諾情報とを比較する（ステップＳ３０４）。
比較部３６は、比較の結果、許諾情報と参照許諾情報とが一致する場合にはステップＳ３０６、Ｓ３０７及びＳ３０８の処理を行い、許諾情報と参照許諾情報とが一致しない場合にはステップＳ３０９の処理を行う。
【００５４】
ステップＳ３０５の比較の結果、許諾情報と参照許諾情報とが一致する場合、比較部３６は、第１スイッチ３７を閉じる。これによりコンテンツ鍵復号部３２は、暗号化コンテンツ鍵領域２３から暗号化コンテンツ鍵を読み出し、暗号化コンテンツ鍵をマスター鍵格納部３１に格納されたマスター鍵で復号して、コンテンツ鍵を得る（ステップＳ３０６）。
【００５５】
続いて、コンテンツ復号部３３は、暗号化コンテンツ領域２４から暗号化コンテンツを読み出し、暗号化コンテンツをコンテンツ鍵復号部３２で復号されたコンテンツ鍵で復号

して、コンテンツを得る（ステップＳ３０７）。
デジタルＡＶ処理部３４は、復号されたコンテンツを音声、映像信号として再生し、スピーカー、ディスプレイ等に出力する（ステップＳ３０８）。
【００５６】
ステップＳ３０５の比較の結果、許諾情報と参照許諾情報とが不一致の場合、比較部３６は、第１スイッチ３７を開き、第２スイッチ３８を閉じる。これによりコンテンツ鍵復号部３２は、暗号化コンテンツ鍵の復号を行わない。このため暗号化コンテンツは復号及び再生されない。一方、アラーム３９に電源が供給され、アラーム３９は、警告音を鳴らしてスピーカー等に出力する（ステップＳ３０９）。
＜効果＞
以上のように著作権保護システム１００を構成することにより、再生機器３０は、次のような場合に記録型メディアの再生を行わない。
（１）記録型メディアに記録された許諾情報の生成に使用されたメディア固有番号と、参照許諾情報の生成に使用されるメディア固有番号とが異なっている場合。
【００５７】
これは例えば、記録機器１０により記録された記録型メディア２０の許諾情報、暗号化コンテンツ鍵及び暗号化コンテンツが、他の記録型メディアにコピーされ、当該他の記録型メディアを再生機器３０が再生しようとした場合に起こる。他の記録型メディアのメディア固有番号は、記録型メディア２０のメディア固有番号と異なっているからである。
（２）記録型メディアに記録された許諾情報の生成に使用された暗号化コンテンツ鍵と、参照許諾情報の生成に使用された暗号化コンテンツ鍵とが異なっている場合。
【００５８】
これは例えば、他の記録型メディアの暗号化コンテンツ鍵及び暗号化コンテンツが、記録型メディア２０の暗号化コンテンツ鍵領域２３及び暗号化コンテンツ領域２４それぞれに上書きコピーされ、その記録型メディア２０を再生機器３０が再生しようとした場合に起こる。他の記録型メディアに記録された暗号化コンテンツ鍵が、記録型メディア２０に最初に記録されていた暗号化コンテンツ鍵と同じ値になることは極めて稀で、異なっていることが殆どだからである。
（３）記録型メディアに記録された許諾情報の生成に使用されたマスター鍵と、参照許諾情報の生成に使用されたマスター鍵とが異なっている場合。
【００５９】
これは例えば、記録機器１０及び再生機器３０が所有しているマスター鍵を所有していない別の記録機器により記録された記録型メディアを、再生機器３０が再生しようとした場合におこる。マスター鍵は、著作権保護システム１００の機器以外には秘密にされているので、マスター鍵が盗まれない限り、著作権保護システム１００の機器以外の他の機器が、再生機器３０に再生させるための記録型メディアを作成することはできない。
【００６０】
以上のように再生機器３０は、違法コピー等で記録された記録型メディアの再生を行わず、記録機器１０により記録されたオリジナルの記録型メディアのみ再生するので、著作権保護システム１００は、違法コピー等によるコンテンツの流通を阻止することができる。
＜第２実施形態＞
次に、本発明の第２実施形態について説明する。
【００６１】
上記第１実施形態では、記録機器１０及び再生機器３０が、コンテンツの暗号化及び復号に必要とされるマスター鍵を機器内部に予め保持している構成であった。記録機器１０及び再生機器３０が複数ある場合には、各機器全てが同じマスター鍵を保持する構成である。しかしこの構成は、１つの機器が物理的な攻撃を受け、すなわち１つの機器の内部が解析されて、マスター鍵が暴露されれば、そのマスター鍵は利用することができなくなり、その機器だけでなく、同じマスター鍵を持つ全ての機器が無効になる。

【００６２】
そこで第２実施形態の著作権保護システムは、第１実施形態の著作権保護システム１００に改良を加え、１つの記録機器又は再生機器が物理的な攻撃を受けた場合であっても、そのことによって他の機器が無効にならないようにした。
主な改良点は以下である。すなわち、
（１）記録機器及び再生機器の１台ずつに異なる値のデバイス鍵を割当て、それぞれの機器内部に保持させる。
（２）記録型メディアには、その製造時において、メディア鍵と呼ばれる鍵が加工されて記録されている。メディア鍵はコンテンツ鍵及びコンテンツの暗号化及び復号に必要とされる鍵である。加工とは、後で詳しく説明するが、特定のデバイス鍵を用いた場合にのみ、加工されたメディア鍵からメディア鍵を取り出すことができ、それ以外のデバイス鍵を用いた場合には、加工されたメディア鍵からメディア鍵を取り出すことができないような加工である。特定のデバイス鍵とは、記録型メディアの製造時において物理的な攻撃を受けたことが報告されていない機器に保持されるデバイス鍵のことであり、それ以外のデバイス鍵とは、物理的な攻撃を受けたことが報告された機器に保持されるデバイス鍵のことである。
（３）記録機器は、保持しているデバイス鍵を用いて、記録型メディアに記録されたメディア鍵の取得を試みる。記録機器は、メディア鍵が取得できた場合にのみ当該メディア鍵を用いてコンテンツ鍵及びコンテンツの暗号化を行い、取得できなかった場合には暗号化を行わない。
（４）記録機器と同様に、再生機器は、保持しているデバイス鍵を用いて、記録型メディアに記録されたメディア鍵の取得を試みる。再生機器は、メディア鍵が取得できた場合にのみ当該メディア鍵を用いて記録型メディアに記録された暗号化コンテンツ鍵及び暗号化コンテンツを復号し、取得できなかった場合には復号を行わない。
【００６３】
以下、このように改良された著作権保護システムの構成及び動作を説明する。
＜構成＞
図４は、第２実施形態の著作権保護システム２００の構成を示すブロック図である。
同図において著作権保護システム２００は、記録型メディア７０に暗号化コンテンツを記録する記録機器６０と記録型メディア７０に記録された暗号化コンテンツを復号して再生する再生機器８０とから構成される。
【００６４】
同図において、図１と同じ符号の構成要素は同じものである。以下では、図１とは異なる部分を中心に説明する。
＜記録型メディア７０＞
記録型メディア７０は、記録型メディア２０と同様の光ディスクであり、記録型メディア２０と同様の構成に加えてメディア鍵データ領域２５を有する。
【００６５】
メディア鍵データ領域２５は、読み出しのみ可能で書込みが不可能な領域になっており、記録型メディア７０の製造時にメディア鍵データが記録される。
メディア鍵データは、上記改良点（２）で説明した、メディア鍵を加工したもののことである。
図５は、メディア鍵データ領域２５に記録されたメディア鍵データの一例を示す。 同図の例において、メディア鍵データは、各大きさが８バイトの、１２８個のレコードからなる。各レコードの内容は、Ｅ（Ｋｄｉ，Ｋｍ）又はＥ（Ｋｄｉ，０）〔ｉは１から１２８までの整数〕の記号で表される暗号データである。
【００６６】
Ｋｍは、メディア鍵を示す。メディア鍵は、複数の記録型メディア７０を１又は複数にグループ化して、各グループ毎に１つずつ固有に割当てられた５６ビットのランダム値である。Ｅ（Ｋｄｉ，０）における０との区別のために、メディア鍵は０以外の値をとる。

Ｋｄｉ〔ｉは１から１２８までの整数〕は、５６ビットのデバイス鍵を示す。デバイス鍵は、Ｋｄ１、Ｋｄ２、・・・、Ｋｄ１２８の１２８種類存在し、それぞれデバイス番号１、２、・・・１２８の記録機器６０又は再生機器８０に保持されているものである。デバイス番号は、１２８台の記録機器６０及び再生機器８０のそれぞれに予め割当てられた１から１２８までの番号である。第１レコード～第１２８のレコードのそれぞれは、デバイス鍵Ｋｄ１～Ｋｄ１２８に対応し、デバイス番号１～１２８の記録機器６０及び再生機器８０に対応する。

【００６７】

Ｅ（）は、暗号アルゴリズムを意味し、例えばＤＥＳである。つまりＥ（Ｋｄｉ，Ｋｍ）は、ＤＥＳを用いて、メディア鍵Ｋｍを平文とし、５６ビットのデバイス鍵Ｋｄｉを暗号鍵として、メディア鍵Ｋｍをデバイス鍵Ｋｄｉで暗号化した結果を表している。例えば第２レコードのＥ（Ｋｄ２，Ｋｍ）は、メディア鍵Ｋｍをデバイス鍵Ｋｄ２で暗号化した結果を表す。一方、Ｅ（Ｋｄｉ，０）は、０の値をデバイス鍵Ｋｄｉで暗号化した結果を表している。例えば第３レコードのＥ（Ｋｄ３，０）は、０をデバイス鍵Ｋｄ３で暗号化した結果を表す。

【００６８】

逆に、Ｅ（Ｋｄｉ，Ｋｍ）は、デバイス鍵Ｋｄｉで復号されれば、復号結果はメディア鍵Ｋｍとなる。例えば第２レコードのＥ（Ｋｄ２，Ｋｍ）は、デバイス鍵Ｋｄ２で復号されれば、復号結果はメディア鍵Ｋｍとなる。一方、Ｅ（Ｋｄｉ，０）は、デバイス鍵Ｋｄｉで復号されれば復号結果は０となる。例えば第３レコードのＥ（Ｋｄ３，０）は、デバイス鍵Ｋｄ３で復号されれば、復号結果は０となる。

【００６９】

このように１２８種類のデバイス鍵に対応する各レコードの内容を、Ｅ（Ｋｄｉ，Ｋｍ）とするかＥ（Ｋｄｉ，０）とするかによって、デバイス鍵のタイプを、メディア鍵を取得することのできるデバイス鍵と、メディア鍵を取得することのできないデバイス鍵とに分別することができる。

記録型メディア７０の製造者は、その製造時に、物理的な攻撃を受けた機器の情報を取得し、その情報に従って各デバイス鍵のタイプを、メディア鍵を取得することのできるデバイス鍵と、メディア鍵を取得することのできないデバイス鍵とに分別し、メディア鍵を取得することのできるデバイス鍵に対応するレコードの内容をＥ（Ｋｄｉ，Ｋｍ）とし、メディア鍵を取得することのできないデバイス鍵に対応するレコードの内容をＥ（Ｋｄｉ，０）としたメディア鍵データを生成し、それをメディア鍵データ領域２５に記録する。これによって、特定のメディア鍵を用いた場合にのみ、メディア鍵が取り出され、それ以外のデバイス鍵を用いた場合には、メディア鍵が取り出されないようにすることができる。

＜記録機器６０の構成＞

記録機器６０は、記録機器１０の構成に対して、マスター鍵格納部１１の代わりにデバイス鍵格納部１７、メディア鍵計算部１８及びメディア鍵一時格納部１９を備える点が異なっている。

【００７０】

デバイス鍵格納部１７は、記録機器６０に割当てられたデバイス鍵が予め格納されたメモリである。記録機器６０は、デバイス鍵を外部には秘匿にして所有している。

メディア鍵計算部１８は、デバイス鍵格納部１７からデバイス鍵を読み出し、またメディア鍵データ領域２５の当該記録機器６０のデバイス番号に対応するレコードから暗号データを読み出す。そしてメディア鍵計算部１８は、暗号データをデバイス鍵で復号する。暗号データは、Ｅ（Ｋｄｉ，Ｋｍ）又はＥ（Ｋｄｉ，０）であるから、デバイス鍵Ｋｄｉで復号すると、メディア鍵Ｋｍ又は０が得られる。メディア鍵計算部１８は、得られた値が０であるか否かを判定し、０である場合には記録機器６０のその後の処理を中止する。すなわちコンテンツ鍵及びコンテンツの暗号化等の処理を中止する。

【００７１】

一方、メディア鍵計算部１８は、得られた値がメディア鍵Ｋｍである場合には、メディア鍵Ｋｍをメディア鍵一時格納部１９に一時的に格納する。一時的に格納するとは、メディア鍵Ｋｍが格納された時から、メディア鍵Ｋｍがコンテンツ鍵の暗号等に利用された後に不要となる時までの間、メディア鍵Ｋｍをメディア鍵一時格納部１９に保持し、その期間を過ぎたらメディア鍵一時格納部１９を初期化して、メディア鍵Ｋｍの値を消去することを意味する。これは必要時以外は消去しておくことによって、記録機器６０への物理攻撃による被害を最小限にしている。

【００７２】

メディア鍵一時格納部１９は、メディア鍵計算部１８により復号されたメディア鍵Ｋｍを一時的に保持するメモリである。

許諾情報計算部１６及びコンテンツ鍵暗号部１３のそれぞれは、第１実施形態のものと同じ機構であるが、マスター鍵の代わりに、メディア鍵一時格納部１９に保持されるメディア鍵Ｋｍを用いている点が第１実施形態のものとは異なっている。

＜再生機器８０の構成＞

再生機器８０は、再生機器３０の構成に対して、マスター鍵格納部３１の代わりにデバイス鍵格納部４０、メディア鍵計算部４１及びメディア鍵一時格納部４２を備える点が異なっている。

【００７３】

デバイス鍵格納部４０は、再生機器８０に割当てられたデバイス鍵が予め格納されたメモリである。再生機器８０は、デバイス鍵を外部には秘匿にして所有している。

メディア鍵計算部４１は、デバイス鍵格納部４０からデバイス鍵を読み出し、またメディア鍵データ領域２５の当該再生機器８０のデバイス番号に対応するレコードから暗号データを読み出す。そしてメディア鍵計算部４１は、暗号データをデバイス鍵で復号する。暗号データは、Ｅ（Ｋｄｉ，Ｋｍ）又はＥ（Ｋｄｉ，０）であるから、デバイス鍵Ｋｄｉで復号すると、メディア鍵Ｋｍ又は０が得られる。メディア鍵計算部４１は、得られた値が０であるか否かを判定し、０である場合には再生機器８０のその後の処理を中止する。すなわちコンテンツ鍵及びコンテンツの復号等の処理を中止する。

【００７４】

一方、メディア鍵計算部４１は、得られた値がメディア鍵Ｋｍである場合には、メディア鍵Ｋｍをメディア鍵一時格納部４２に一時的に格納する。一時的に格納するとは、メディア鍵Ｋｍが格納された時から、メディア鍵Ｋｍが暗号化コンテンツ鍵の復号に利用された後に不要となるまでの間、メディア鍵Ｋｍをメディア鍵一時格納部４２に保持し、その期間を過ぎたらメディア鍵一時格納部４２を初期化して、メディア鍵Ｋｍの値を消去することを意味する。これは必要時以外は消去しておくことによって、再生機器８０への物理攻撃による被害を最小限にしている。

【００７５】

メディア鍵一時格納部４２は、メディア鍵計算部４１により復号されたメディア鍵Ｋｍを一時的に保持するメモリである。

参照許諾情報計算部３５及びコンテンツ鍵復号部３２のそれぞれは、第１実施形態のものと同じ機構であるが、マスター鍵の代わりに、メディア鍵一時格納部４２に保持されるメディア鍵Ｋｍを用いている点が第１実施形態のものとは異なっている。

＜動作＞

以上のように構成された記録機器６０及び再生機器８０について、それぞれ動作を説明する。

【００７６】

まず記録機器６０の動作を説明する。

（１）記録機器６０においてメディア鍵計算部１８は、デバイス鍵格納部１７からデバイス鍵を取得し、メディア鍵データ領域２５から記録機器６０に対応するレコードの暗号化データを取得する。

（２）次に、メディア鍵計算部１８は、暗号化データをデバイス鍵で復号し、その結果

が０であるか否かを判定する。
【００７７】
（３）復号結果が０である場合には、記録機器６０はその後の暗号化処理を中止する。
（４）復号結果が０でない場合には、メディア鍵計算部１８は、メディア鍵一時格納部１９に復号結果であるメディア鍵を格納する。
（５）続いて記録機器６０は図２のフローチャートと同様の処理を行う。ただし、図２及びその説明においてマスター鍵格納部１１をメディア鍵一時格納部１９に替え、マスター鍵をメディア鍵に替える。
【００７８】
（６）最後に記録機器６０は、メディア鍵一時格納部１９を初期化してメディア鍵の値を消去する。
次に再生機器８０の動作を説明する。
（１）再生機器８０においてメディア鍵計算部４１は、デバイス鍵格納部４０からデバイス鍵を取得し、メディア鍵データ領域２５から再生機器８０に対応するレコードの暗号化データを取得する。
【００７９】
（２）次に、メディア鍵計算部４１は、暗号化データをデバイス鍵で復号し、その結果が０であるか否かを判定する。
（３）復号結果が０である場合には、再生機器８０はその後の復号処理を中止する。
（４）復号結果が０でない場合には、メディア鍵計算部４１は、メディア鍵一時格納部４２に復号結果であるメディア鍵を格納する。
【００８０】
（５）続いて再生機器８０は図３のフローチャートと同様の処理を行う。ただし、図３及びその説明においてマスター鍵格納部３１をメディア鍵一時格納部４２に替え、マスター鍵をメディア鍵に替える。
（６）最後に再生機器８０は、メディア鍵一時格納部４２を初期化してメディア鍵の値を消去する。
＜効果＞
以上の構成により、著作権保護システム２００においては、メディア鍵データの各レコードの暗号化データをＥ（Ｋｄｉ，Ｋｍ）とするかＥ（Ｋｄｉ，０）とするかによって、特定のデバイス鍵を用いてのみメディア鍵が復号でき、それ以外のデバイス鍵を用いてはメディア鍵を復号できないようにすることができる。
【００８１】
これにより例えば、１つの機器が第三者により物理的に攻撃されてデバイス鍵が暴露された場合、記録型メディア７０の製造者は、当該機器に対応するレコードの暗号化データをＥ（Ｋｄｉ，０）としたメディア鍵データを作成して、それを記録型メディア７０に記録すればよい。そうすれば、第三者は、暴露されたデバイス鍵を用いてメディア鍵を不正に取得しようとしても、取得することができなくなる。そして第三者は、メディア鍵が取得できないので、そのメディア鍵により暗号化された暗号化コンテンツ鍵及び暗号化コンテンツを復号することができなくなり、第三者が不正にコンテンツを利用することを防止することができる。
【００８２】
また著作権保護システム２００は、メディア鍵データの各レコードの暗号化データをＥ（Ｋｄｉ，Ｋｍ）とするかＥ（Ｋｄｉ，０）とするかによって、各機器の暗号化又は復号を機能させるか否かを制御する。
これにより例えば、１つの機器のデバイス鍵が暴露された場合、その機器に対応するレコードの暗号化データをＥ（Ｋｄｉ，０）とすることによって、その機器を利用できないようにすることができる。
【００８３】
さらに著作権保護システム２００においては、暗号化データがＥ（Ｋｄｉ，０）となっ

ていない限り、異なるデバイス鍵を持つ記録機器、再生機器間で共通の記録型メディアを利用することができるので、記録型メディアの可搬性が損なわれないという効果がある。

なお、記録機器６０及び再生機器８０は、暗号化データをデバイス鍵で復号した復号結果が０である場合に、コンテンツの暗号化又は復号の処理を中止する構成であるが、中止せずに０を鍵として用いて暗号化又は復号を行うよう構成してもよい。０を鍵として用いて暗号化された暗号化コンテンツ鍵及び暗号化コンテンツは、メディア鍵Ｋｍを用いて復号することができない。また逆にメディア鍵Ｋｍで暗号化された暗号化コンテンツ鍵及び暗号化コンテンツは、０を鍵として用いて復号することができない。これにより物理攻撃を受けた機器を用いたコンテンツの不正利用を防止することができる。

【００８４】

デバイス鍵は、各機器毎に固有としているが、複数の機器から成るグループ毎に固有としてもよい。その場合１つの機器が物理攻撃を受けた場合、その機器に対応する暗号化データがＥ（Ｋｄｉ，０）となることによって、その機器の属するグループの機器はすべて利用できなくなるが、それ以外のグループの機器は、利用することができる。

＜第３実施形態＞

次に、本発明の第３実施形態について説明する。

【００８５】

上記第１及び第２実施形態においては、記録機器はコンテンツ鍵暗号部を有し、再生機器はコンテンツ鍵復号部を有するというように、記録機器と再生機器とで異なる構成要素を備える。これに対し、第３実施形態では、記録機器と再生機器とが同じコンテンツ鍵生成部を備えるようにして、コスト削減を図っている。

図６は、第３実施形態の著作権保護システム３００の構成を示すブロック図である。

【００８６】

同図において著作権保護システムは、記録型メディア１２０に暗号化コンテンツを記録する記録機器１１０と記録型メディア１２０に記録された暗号化コンテンツを復号して再生する再生機器１３０とから構成される。

同図において図１と同じ符号の構成要素は同じものである。以下では異なる部分を中心に説明する。

【００８７】

記録型メディア１２０は、暗号化コンテンツ鍵領域２３の代わりに、乱数領域１２１を有する点が、記録型メディア２０とは異なり、その他は、記録型メディア２０と同じである。

乱数領域１２１は、記録機器１１０によって記録型メディア１２０の記録領域に確保されて乱数が記録される。この乱数は、コンテンツ鍵の元となるものである。

【００８８】

記録機器１１０は、記録機器１０と比較して、コンテンツ鍵発生部１２及びコンテンツ鍵暗号部１３を備える代わりに、乱数発生部１１１及びコンテンツ鍵生成部１１２を備える点が異なっている。その他の構成要素は、記録機器１０と同じものである。

乱数発生部１１１は、乱数を発生して、許諾情報計算部１６とコンテンツ鍵生成部１１２に出力し、また記録型メディア１２０の記録領域に乱数領域１２１を確保してその乱数を記録する。

【００８９】

コンテンツ鍵生成部１１２は、乱数発生部１１１より与えられる乱数とマスター鍵格納部１１に格納されたマスター鍵とを用いて、例えばハッシュ関数ＳＨＡ－１等の演算を行い、コンテンツ鍵を生成する。

コンテンツ暗号部１５は、コンテンツ鍵生成部１１２が生成したコンテンツ鍵を用いてコンテンツを暗号化し、暗号化コンテンツ領域２４に記録する。

【００９０】

許諾情報計算部１６は、メディア固有番号とマスター鍵と乱数発生部１１１の乱数とを取得し、それらを連結して１つのビット列にし、そのビット列を入力としてハッシュ関数

ＳＨＡ－１等の演算を行う。そして演算結果のハッシュ値を許諾情報として許諾情報領域２２に記録する。

再生機器１３０は、再生機器３０と比較して、コンテンツ鍵復号部３２の代わりにコンテンツ鍵生成部１３１を備える点が異なっている。その他の構成要素は、再生機器３０と同じものである。

【００９１】

コンテンツ鍵生成部１３１は、コンテンツ鍵生成部１１２と同じものであり、乱数領域１２１に記録された乱数とマスター鍵格納部３１に格納されたマスター鍵とを用いて、コンテンツ鍵生成部１１２と同じ演算を行ってコンテンツ鍵を生成する。

コンテンツ復号部３３は、コンテンツ鍵生成部１３１が生成したコンテンツ鍵を用いてコンテンツを復号する。

【００９２】

参照許諾情報計算部３５は、メディア固有番号とマスター鍵と乱数領域１２１の乱数とを取得し、記録機器１１０の許諾情報計算部１６と同じ演算を行って参照許諾情報を生成する。

以上のように構成することにより、著作権保護システム１００の製造においては、コンテンツ鍵暗号部とコンテンツ鍵復号部とが製造されるのに対し、著作権保護システム３００の製造においては、それらの代わりに２つのコンテンツ鍵生成部が製造され、著作権保護システム３００は、著作権保護システム１００より製造コストを抑えることができる。

＜第４実施形態＞

次に、本発明の第４実施形態について説明する。

【００９３】

本実施形態の著作権保護システムは、著作権保護システム３００と著作権保護システム２００とのそれぞれの特徴部分を組み合わせた構成である。

図７は、第４実施形態の著作権保護システム４００の構成を示すブロック図である。

同図において著作権保護システム４００は、記録型メディア１７０に暗号化コンテンツを記録する記録機器１６０と記録型メディア１７０に記録された暗号化コンテンツを復号して再生する再生機器１８０とから構成される。

【００９４】

同図において、図４及び図６と同じ符号の構成要素は同じものである。

記録型メディア１７０は、記録型メディア１２０に、記録型メディア７０のメディア鍵データ領域２５を加えた構成である。

記録機器１６０は、記録機器１１０のマスター鍵格納部１１を、記録機器６０のデバイス鍵格納部１７、メディア鍵計算部１８及びメディア鍵一時格納部１９に代えた構成である。

【００９５】

再生機器１８０は、再生機器１３０のマスター鍵格納部３１を、再生機器８０のデバイス鍵格納部４０、メディア鍵計算部４１及びメディア鍵一時格納部４２に代えた構成である。

以上の構成により、著作権保護システム４００は、著作権保護システム２００と著作権保護システム３００の両方の利点を備える。

＜その他の実施形態＞

以上、実施形態１～４について説明したが、本発明はこれらの実施形態に限られないことは勿論である。即ち、

（１）実施形態１においては、記録機器１０は、記録型メディア２０に、許諾情報、暗号化コンテンツ鍵及び暗号化コンテンツをそれぞれ１つずつ記録する構成であった。しかし１つずつ記録することに限る必要はない。例えば、記録機器は、図８に示す記録型メディア８００のように、複数の許諾情報、暗号化コンテンツ鍵及び暗号化コンテンツを記録するよう構成してもよい。

【００９６】

より詳しくは、記録機器は、複数のコンテンツＡ、Ｂ、Ｃのそれぞれをコンテンツ鍵Ａ、Ｂ、Ｃで暗号化して、暗号化コンテンツＡ、Ｂ、Ｃを暗号化コンテンツ領域８４０に記録する。またコンテンツ鍵Ａ、Ｂ、Ｃのそれぞれをマスター鍵で暗号化して、暗号化コンテンツ鍵Ａ、Ｂ、Ｃを暗号化コンテンツ鍵領域８３０に記録する。またメディア固有番号、マスター鍵及び暗号化コンテンツ鍵Ａを全て用いて許諾情報Ａを生成し、許諾情報領域８２０に記録する。許諾情報Ｂ、Ｃについても、許諾情報Ａの場合と同様の手順で生成し、許諾情報領域８２０に記録する。

【００９７】

再生機器は、メディア固有番号、マスター鍵及び暗号化コンテンツ鍵領域８３０の暗号化コンテンツ鍵Ａを用いて参照許諾情報Ａを生成し、それを許諾情報領域８２０の許諾情報Ａと比較し、一致している場合のみ、暗号化コンテンツ鍵領域８３０の暗号化コンテンツ鍵Ａをマスター鍵で復号し、復号されたコンテンツ鍵Ａを用いて暗号化コンテンツ領域８４０の暗号化コンテンツＡを復号し、復号されたコンテンツＡを再生する。暗号化コンテンツＢ、Ｃについても暗号化コンテンツＡの場合と同様の手順で復号、再生する。

（２）また記録機器は、図９に示す記録型メディア９００のように記録してもよい。

【００９８】

より詳しくは、記録機器は、上記（１）と同様の方法で暗号化コンテンツＡ、Ｂ、Ｃ及び暗号化コンテンツ鍵Ａ、Ｂ、Ｃを生成し、それらを暗号化コンテンツ領域９４０と暗号化コンテンツ鍵領域９３０とに記録する。そしてメディア固有番号、マスター鍵、暗号化コンテンツ鍵Ａ、Ｂ、Ｃの全てを用いて許諾情報を生成し、許諾情報領域９２０に記録する。

【００９９】

再生機器は、メディア固有番号、マスター鍵、暗号化コンテンツ鍵Ａ、Ｂ、Ｃの全てを用いて参照許諾情報を生成し、それを許諾情報領域９２０の許諾情報と比較して、一致している場合にのみ、暗号化コンテンツ鍵Ａ、Ｂ、Ｃをマスター鍵で復号し、暗号化コンテンツＡ、Ｂ、Ｃをコンテンツ鍵Ａ、Ｂ、Ｃで復号、再生する。

（３）記録型メディア２０は、光ディスクに限らず、磁気ディスク、光磁気ディスク、メモリカード等の他の記録媒体にメディア固有番号を書き替え不可能な状態で付加したものでもよい。

（４）メディア固有番号は、書き替えができない状態で、かつ読み出し機構により読み出すことができる状態であれば、書き替え不可能領域以外の他の箇所に記録されていてもよい。

（５）各実施形態では、各種演算に等にハッシュ関数ＳＨＡ－１、DES等を用いているが、これらに限る必要はない。他の種類のハッシュ関数や、他の種類の演算でもよい。また各値のビット数を５６ビットや６４ビットに限る必要もない。

（６）許諾情報及び参照許諾情報は、マスター鍵なしに、メディア固有番号と復号に関する情報との２つを反映して生成されたものでもよい。

（７）比較部３６は、第１スイッチ３７及び第２スイッチ３８の開閉により各構成要素を制御するよう構成されているが、この構成に限る必要はない。要するに、許諾情報と参照許諾情報とが一致する場合のみデジタルＡＶ処理部３４が暗号化コンテンツを再生し、一致しない場合には再生しないように構成されていればよい。

（９）アラーム３９は、警告音を発生させるかわりに、警告メッセージを示すデータをディスプレイに出力するよう構成してもよい。

（１０）上記実施形態１～４及び図８、９の記録型メディアに対応する各著作権保護システムの動作手順を方法としてもよい。

（１１）上記実施形態１～４の各著作権保護システムの各構成要素の動作手順をプログラムにし、当該プログラムをコンピュータに実行させてもよい。また当該プログラムを記録媒体に記録し又は各種通信路等を用いて、流通させてもよい。このような記録媒体には、ＩＣカード、光ディスク、フレキシブルディスク、ＲＯＭ等がある。

（１２）再生機器は、ある記録型メディアの暗号化コンテンツの再生について、アラーム

が所定回数以上作動したことを検出する機構と、検出の場合に記録型メディアの該当する暗号化コンテンツにその旨の印を記録する機構と、印の有無を検査して印がある場合にはその暗号化コンテンツを復号しない機構とを備えてもよい。また再生機器は、記録型メディアの許諾情報と参照許諾情報とが一致しないと判定した場合、当該記録型メディアの記録内容を、利用することが不可能な状態に加工する構成を設けても良い。この加工の方法としては、例えば、（ｉ）再生機器が当該記録型メディアの記録内容を消去する、（ｉｉ）当該記録型メディアのメディア固有番号をメモリに記憶しておき、再生機器に接続された記録型メディアのメディア固有番号がメモリのものと一致する場合には記録内容の読み出しを行わない、等がある。

（１３）上記実施形態１～４及び上記（１）～（１２）を組み合わせて実施してもよい。

【産業上の利用可能性】

【０１００】

デジタル放送により放送される映画等のコンテンツを受信して光ディスク等の記録媒体に記録し、再生する機器を用いたコンテンツ利用形態に有用である。

【図面の簡単な説明】

【０１０１】

【図１】第１実施形態の著作権保護システム１００の構成を示すブロック図である。

【図２】記録機器１０の処理手順を示すフローチャートである。

【図３】再生機器３０の処理手順を示すフローチャートである。

【図４】第２実施形態の著作権保護システム２００の構成を示すブロック図である。

【図５】メディア鍵データ領域２５に記録されたメディア鍵データの一例を示す。

【図６】第３実施形態の著作権保護システム３００の構成を示すブロック図である。

【図７】第４実施形態の著作権保護システム４００の構成を示すブロック図である。

【図８】記録型メディアの構成例を示す。

【図９】記録型メディアの構成例を示す。

【図１０】従来の著作権保護システムの構成を示すブロック図である。

【図１１】鍵暗号鍵計算部１００１の内部の演算機構を示す。

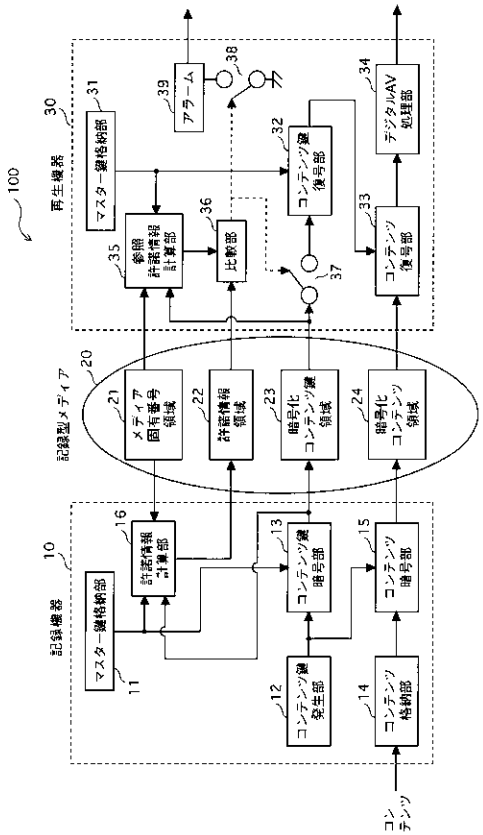
【符号の説明】

【０１０２】

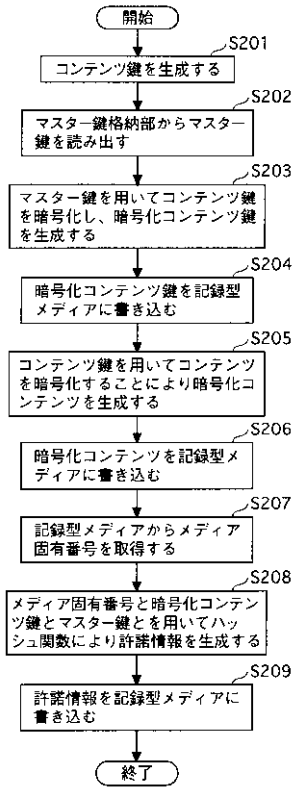
１０　記録機器
１１　マスター鍵格納部
１２　コンテンツ鍵発生部
１３　コンテンツ鍵暗号部
１４　コンテンツ格納部
１５　コンテンツ暗号部
１６　許諾情報計算部
２０　記録型メディア
２１　メディア固有番号領域
２２　許諾情報領域
２３　暗号化コンテンツ鍵領域
２４　暗号化コンテンツ領域
３０　再生機器
３１　マスター鍵格納部
３２　コンテンツ鍵復号部
３３　コンテンツ復号部
３４　デジタルＡＶ処理部
３５　参照許諾情報計算部
３６　比較部
３７　スイッチ
３８　スイッチ

３９　　アラーム
１００　　著作権保護システム

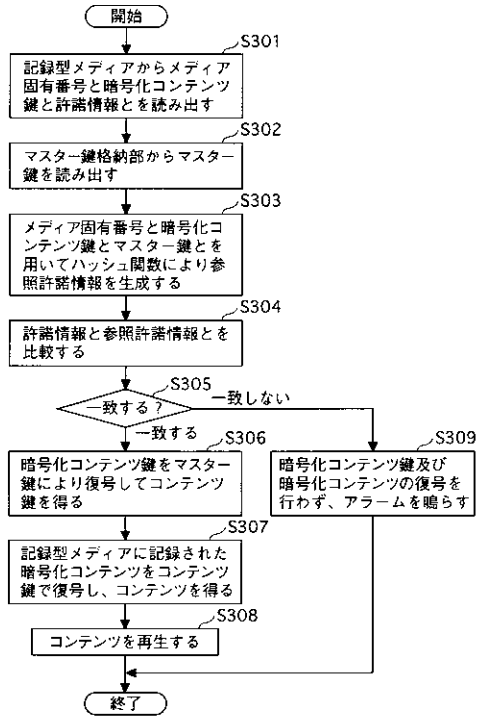
【図１】



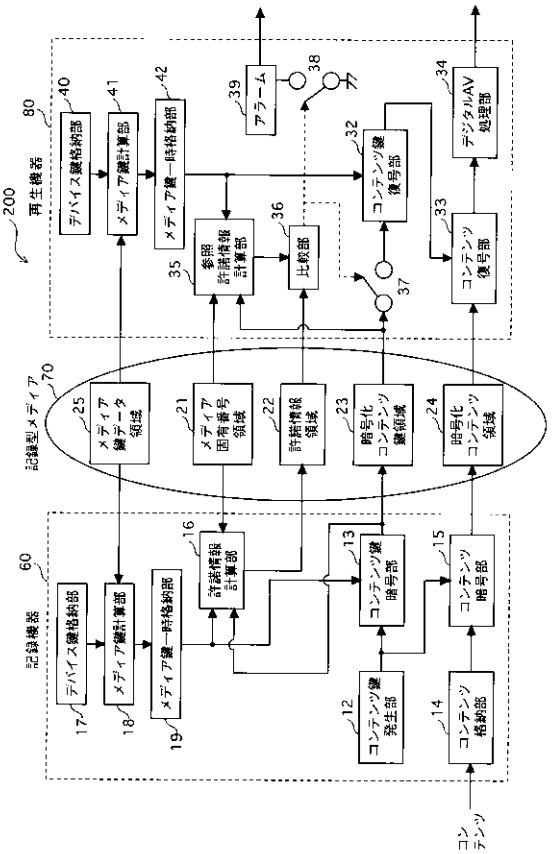
【図２】



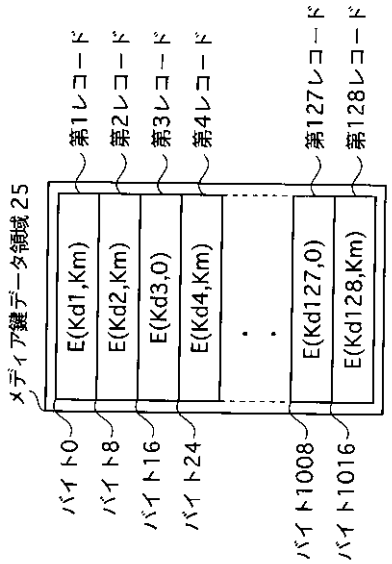
【図３】


開始
S301
記録型メディアからメディア固有番号と暗号化コンテンツ鍵と許諾情報とを読み出す
S302
マスター鍵格納部からマスター鍵を読み出す
S303
メディア固有番号と暗号化コンテンツ鍵とマスター鍵とを用いてハッシュ関数により参照許諾情報を生成する
S304
許諾情報と参照許諾情報とを比較する
S305
一致する？
一致しない
一致する
S306
暗号化コンテンツ鍵をマスター鍵により復号してコンテンツ鍵を得る
S309
暗号化コンテンツ鍵及び暗号化コンテンツの復号を行わず、アラームを鳴らす
S307
記録型メディアに記録された暗号化コンテンツをコンテンツ鍵で復号し、コンテンツを得る
S308
コンテンツを再生する
終了

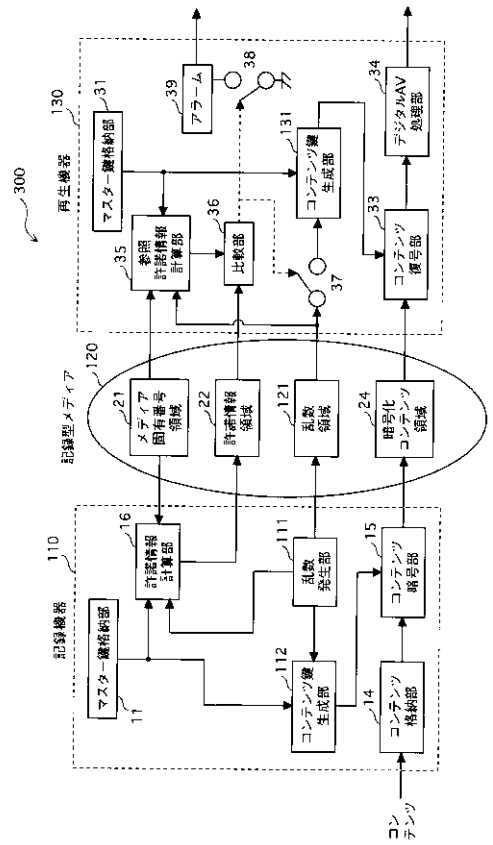
【図４】


200
再生機器
80
デバイス鍵格納部
40
メディア鍵計算部
41
メディア鍵一時格納部
42
アラーム
39
38
デジタルAV処理部
34
コンテンツ鍵復号部
32
コンテンツ復号部
33
参照許諾情報計算部
35
比較部
36
37
記録型メディア
70
メディアデータ領域
25
メディア固有番号領域
21
許諾情報領域
22
暗号化コンテンツ鍵領域
23
暗号化コンテンツ領域
24
記録機器
60
デバイス鍵格納部
17
メディア鍵計算部
18
メディア鍵一時格納部
19
許諾情報計算部
16
コンテンツ鍵暗号部
13
コンテンツ暗号部
15
コンテンツ鍵発生部
12
コンテンツ格納部
14
コンテンツ

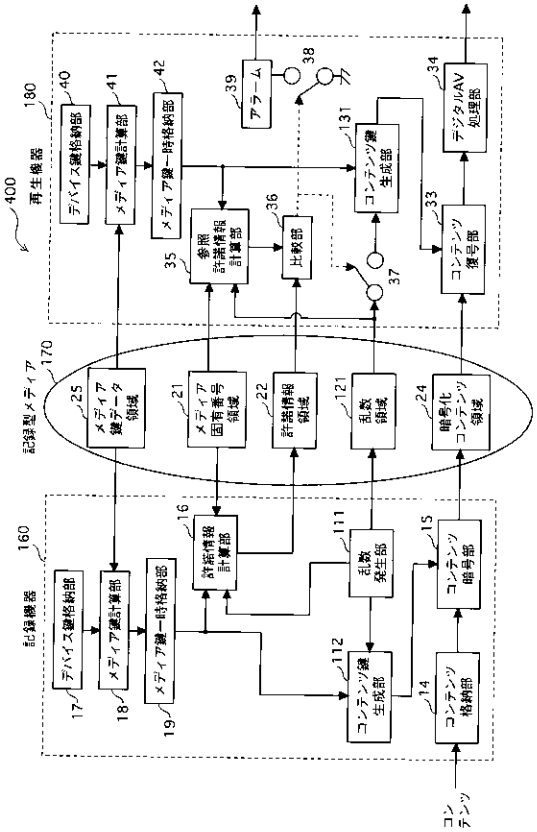
【図５】


メディア鍵データ領域 25
第1レコード
第2レコード
第3レコード
第4レコード
第127レコード
第128レコード
E(Kd1,Km)
E(Kd2,Km)
E(Kd3,0)
E(Kd4,Km)
E(Kd127,0)
E(Kd128,Km)
バイト0
バイト8
バイト16
バイト24
バイト1008
バイト1016

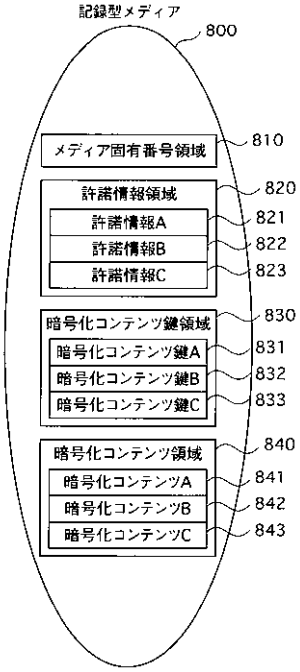
【図６】


300
再生機器
130
マスター鍵格納部
31
アラーム
39
38
デジタルAV処理部
34
コンテンツ鍵生成部
131
コンテンツ復号部
33
参照許諾情報計算部
35
比較部
36
37
記録型メディア
120
メディア固有番号領域
21
許諾情報領域
22
乱数領域
121
暗号化コンテンツ領域
24
記録機器
110
マスター鍵格納部
11
許諾情報計算部
16
乱数発生部
111
コンテンツ暗号部
15
コンテンツ鍵生成部
112
コンテンツ格納部
14
コンテンツ

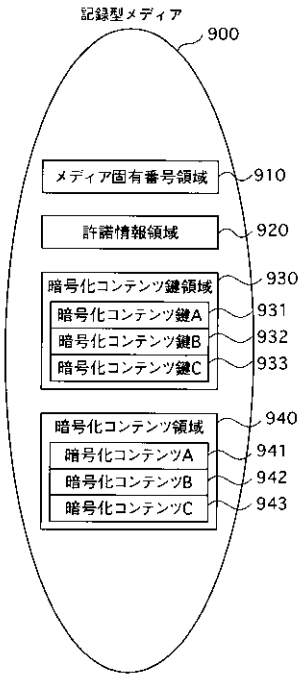
【図７】


再生機器
400
180
デバイス鍵格納部
40
メディア鍵計算部
41
メディア鍵一時格納部
42
アラーム
39
38
デジタルAV処理部
34
コンテンツ鍵生成部
131
コンテンツ復号部
33
参照許諾情報計算部
35
比較部
36
37
記録型メディア
170
メディア鍵データ領域
25
メディア固有番号領域
21
許諾情報領域
22
乱数領域
121
暗号化コンテンツ領域
24
記録機器
160
デバイス鍵格納部
17
メディア鍵計算部
18
メディア鍵一時格納部
19
許諾情報計算部
16
乱数発生部
111
コンテンツ暗号部
15
コンテンツ鍵生成部
112
コンテンツ格納部
14
コンテンツ

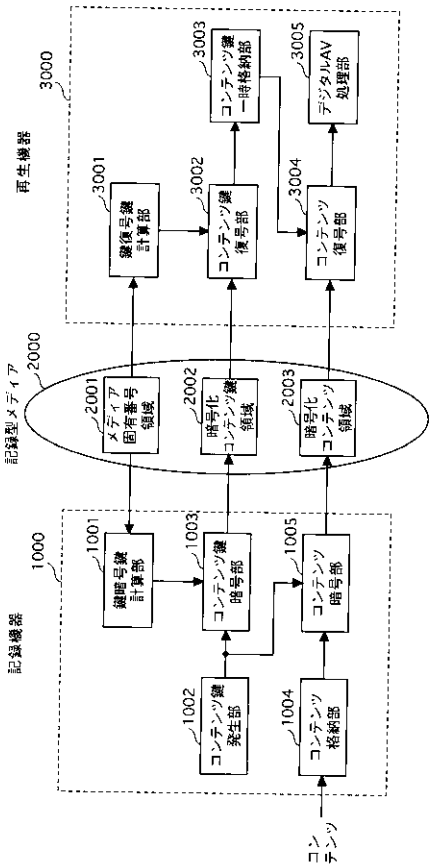
【図８】


記録型メディア
800
メディア固有番号領域
810
許諾情報領域
820
許諾情報A
821
許諾情報B
822
許諾情報C
823
暗号化コンテンツ鍵領域
830
暗号化コンテンツ鍵A
831
暗号化コンテンツ鍵B
832
暗号化コンテンツ鍵C
833
暗号化コンテンツ領域
840
暗号化コンテンツA
841
暗号化コンテンツB
842
暗号化コンテンツC
843

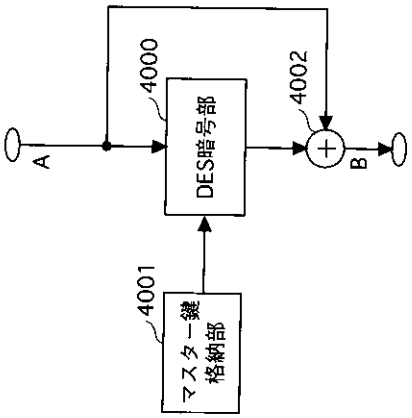
【図９】


記録型メディア
900
メディア固有番号領域
910
許諾情報領域
920
暗号化コンテンツ鍵領域
930
暗号化コンテンツ鍵A
931
暗号化コンテンツ鍵B
932
暗号化コンテンツ鍵C
933
暗号化コンテンツ領域
940
暗号化コンテンツA
941
暗号化コンテンツB
942
暗号化コンテンツC
943

【図１０】


再生機器
3000
コンテンツ鍵一時格納部
3003
デジタルAV処理部
3005
鍵復号鍵計算部
3001
コンテンツ鍵復号部
3002
コンテンツ復号部
3004
記録型メディア
2000
メディア固有番号領域
2001
暗号化コンテンツ鍵領域
2002
暗号化コンテンツ領域
2003
記録機器
1000
鍵暗号鍵計算部
1001
コンテンツ鍵暗号部
1003
コンテンツ暗号部
1005
コンテンツ鍵発生部
1002
コンテンツ格納部
1004
コンテンツ

【図１１】



フロントページの続き

(72)発明者　館林　誠
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) 5D044 AB07 BC04 CC06 DE17 DE50 DE54 EF05 FG18 GK12 GK17
HH15
5D110 AA17 AA29 BB01 DA04 DA12 DB03 DC05 DC16 DC27 DD13
DE01
5J104 AA07 AA16 EA04 EA15 EA18 GA05 JA03 KA02 KA04 KA15
NA02 NA12 NA27 NA37 NA38 PA14