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

特許第5217541号
(P5217541)

(45)発行日　平成25年6月19日(2013.6.19)　(24)登録日　平成25年3月15日(2013.3.15)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/24	165F
G06F 21/10	(2013.01)	G06F	21/24	166A
H04N 5/85	(2006.01)	G06F	21/22	110L
H04N 5/91	(2006.01)	H04N	5/85	Z
G11B 20/10	(2006.01)	H04N	5/91	P

請求項の数 8　(全 15 頁)　最終頁に続く

(21)出願番号　特願2008-69508(P2008-69508)
(22)出願日　平成20年3月18日(2008.3.18)
(65)公開番号　特開2009-223766(P2009-223766A)
(43)公開日　平成21年10月1日(2009.10.1)
審査請求日　平成22年10月18日(2010.10.18)

前置審査

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100119987
弁理士　伊坪　公一
(74)代理人　100081330
弁理士　樋口　外治
(74)代理人　100114177
弁理士　小林　龍
(72)発明者　佐野　圧一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】コピープロテクト方法、コンテンツ再生装置およびＩＣチップ

(57)【特許請求の範囲】
【請求項１】
コンテンツ記録媒体に付加され、書き換え不能に一意に設定されたチップＩＤが元々記録され、かつ、前記コンテンツ記録媒体に対するコピープロテクトに供するＩＣチップであって、
前記コンテンツを特定するコンテンツＩＤを暗号化した暗号化コンテンツＩＤと、前記チップＩＤを暗号化した暗号化チップＩＤとを格納する書込み読出し可能なＩＤメモリを内蔵し、前記チップＩＤは、当該コンテンツ記録媒体のコンテンツを再生するコンテンツ再生装置において、前記ＩＣチップが付加される前記コンテンツ記録媒体を一意に特定し、前記暗号化チップＩＤおよび暗号化コンテンツＩＤはそれぞれ所定の鍵により復号化されて前記コンテンツ再生装置でのコピープロテクトに供する、ＩＣチップ。
【請求項２】
前記コンテンツＩＤは、前記コンテンツをなすＮバイトのデジタルデータを、所定の関数により演算して得た、ｎ（ｎ＜＜Ｎ）バイトの演算値である請求項１に記載のＩＣチップ。
【請求項３】
前記コンテンツＩＤと前記チップＩＤとを共に第1の鍵により暗号化してそれぞれ、前記暗号化コンテンツＩＤと前記暗号化チップＩＤとを生成する請求項１に記載のＩＣチップ。
【請求項４】

前記第１の鍵は、前記コンテンツ記録媒体に記録されたコンテンツを再生する際に、前記暗号化コンテンツＩＤおよび暗号化チップＩＤを復号化するために用いる第２の鍵と、相互に対をなす請求項３に記載のＩＣチップ。

【請求項５】

請求項１に記載のコピープロテクトＩＣチップを付加したコンテンツ記録媒体。

【請求項６】

ＩＣチップを用いてコンテンツのコピープロテクトを行うコンテンツ再生装置であって、該ＩＣチップは、コンテンツ記録媒体に付加され、書き換え不能に一意に設定されたチップＩＤが元々記録され、かつ、前記コンテンツ記録媒体に対するコピープロテクトに供するＩＣチップであって、前記コンテンツを特定するコンテンツＩＤを暗号化した暗号化コンテンツＩＤと、前記チップＩＤを暗号化した暗号化チップＩＤとを格納する書込み読出し可能なＩＤメモリを内蔵し、前記チップＩＤは、当該コンテンツ記録媒体のコンテンツを再生する該コンテンツ再生装置において、前記ＩＣチップが付加される前記コンテンツ記録媒体を一意に特定し、前記暗号化チップＩＤおよび暗号化コンテンツＩＤはそれぞれ所定の鍵により復号化されて前記コピープロテクトに供する、前記コンテンツ再生装置において、

前記コンテンツを一意に特定するために該コンテンツをもとに所定の処理により得た前記コンテンツＩＤと、一意に設定されて書き換え不能に前記ＩＣチップに元々記録されている前記チップＩＤとをそれぞれ、第１の前記鍵により暗号化した前記暗号化コンテンツＩＤとその第１の鍵により暗号化した前記暗号化チップＩＤとを前記ＩＤメモリに格納して前記コンテンツ記録媒体に付加される前記ＩＣチップから、前記暗号化コンテンツＩＤおよび暗号化チップＩＤを読み出す第1読出し機能部および前記ＩＣチップ自体に内蔵される前記チップＩＤを読み出す第２読出し機能部と、

読み出した前記暗号化コンテンツＩＤおよび暗号化チップＩＤを、前記第１の鍵と相互に対をなす第２の鍵により復号化し、元の前記コンテンツＩＤおよびチップＩＤを再生する復号化機能部と、

前記コンテンツ記録媒体に記録された前記コンテンツを、前記所定の処理と同一の処理により得た前記コンテンツＩＤを生成するコンテンツＩＤ生成機能部と、を有し、

前記復号化機能部からの復号データと、前記第２読出し機能部およびコンテンツＩＤ生成機能部からの各出力データとが一致したときのみ、前記コンテンツの再生を許可する再生許可機能部と、

を備えるコンテンツ再生装置。

【請求項７】

ＩＣチップを用いてコンテンツのコピープロテクトを行うコピープロテクト方法であって、該ＩＣチップは、コンテンツ記録媒体に付加され、書き換え不能に一意に設定されたチップＩＤが元々記録され、かつ、前記コンテンツ記録媒体に対するコピープロテクトに供するＩＣチップであって、前記コンテンツを特定するコンテンツＩＤを暗号化した暗号化コンテンツＩＤと、前記チップＩＤを暗号化した暗号化チップＩＤとを格納する書込み読出し可能なＩＤメモリを内蔵し、前記チップＩＤは、当該コンテンツ記録媒体のコンテンツを再生するコンテンツ再生装置において、前記ＩＣチップが付加される前記コンテンツ記録媒体を一意に特定し、前記暗号化チップＩＤおよび暗号化コンテンツＩＤはそれぞれ所定の鍵により復号化されて前記コンテンツ再生装置において前記コピープロテクトを行うコピープロテクト方法において、

前記ＩＣチップに元々記録されて該ＩＣチップを一意に特定する前記チップＩＤを読み出すステップと、

前記コンテンツ記録媒体に記録された前記コンテンツを一意に特定する前記コンテンツＩＤを生成するステップと、

前記所定の鍵により前記チップＩＤを暗号化した前記暗号化チップＩＤと、その所定の鍵により暗号化した前記暗号化コンテンツＩＤとを生成するステップと、

暗号化された前記暗号化チップＩＤおよび暗号化コンテンツＩＤを、前記ＩＣチップ内

に記録するステップと、
前記暗号化チップＩＤおよび暗号化コンテンツＩＤを格納した前記ＩＣチップを、前記コンテンツ記録媒体に付加するステップと、
を有するコピープロテクト方法。
【請求項８】
ＩＣチップを用いてコンテンツのコピープロテクトを行うコピープロテクト方法であって、該ＩＣチップは、コンテンツ記録媒体に付加され、書き換え不能に一意に設定されたチップＩＤが元々記録され、かつ、前記コンテンツ記録媒体に対するコピープロテクトに供するＩＣチップであって、前記コンテンツを特定するコンテンツＩＤを暗号化した暗号化コンテンツＩＤと、前記チップＩＤを暗号化した暗号化チップＩＤとを格納する書込み読出し可能なＩＤメモリを内蔵し、前記チップＩＤは、当該コンテンツ記録媒体のコンテンツを再生するコンテンツ再生装置において、前記ＩＣチップが付加される前記コンテンツ記録媒体を一意に特定し、前記暗号化チップＩＤおよび暗号化コンテンツＩＤはそれぞれ所定の鍵により復号化されて前記コンテンツ再生装置において前記コピープロテクトを行うコピープロテクト方法において、
一意に設定されて書き換え不能に前記ＩＣチップに元々記録されている前記チップＩＤを第1の前記鍵で暗号化した前記暗号化チップＩＤと、前記コンテンツ記録媒体に記録されたコンテンツを一意に特定するべく所定の処理により生成された前記コンテンツＩＤを前記第1の鍵で暗号化した前記暗号化コンテンツＩＤと、を格納する当該ＩＣチップが付加された前記コンテンツ記録媒体を、前記コンテンツ再生装置にセットするステップと、
前記ＩＣチップ内の、前記チップＩＤと前記暗号化チップＩＤと前記暗号化コンテンツＩＤと、を読み出すステップと、
読み出した前記暗号化チップＩＤおよび暗号化コンテンツＩＤを、前記第１の鍵と相互に対をなす第２の鍵でそれぞれ復号化するステップと、
復号化して再生された前記チップＩＤおよびコンテンツＩＤと、前記の読み出されたチップＩＤおよび前記所定の処理と同一の処理により生成された前記コンテンツＩＤと、の一致／不一致をそれぞれ検出するステップと、
前記の検出により一致とされたときにのみ前記コンテンツ再生装置での前記コンテンツの再生を許可するステップと、
を有するコピープロテクト方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツ記録媒体が不正にコピーされることを防止するためのコピープロテクト方法に関し、さらに該コピープロテクト方法に適合するコンテンツ再生装置、さらにまた該プロテクト方法の実施に供されるＩＣチップに関する。
【背景技術】
【０００２】
映画、音楽あるいはソフトウェア等の種々コンテンツを記録するためのコンテンツ記録媒体は、種々の形態をもって市場に多数提供されている。例えば代表的にはＤＶＤやＣＤ等、あるいはメモリカード等である。
【０００３】
これらのコンテンツ記録媒体が不正に使用されたりあるいは不正にコピーされたりすることを防止するためのいわゆるコピープロテクト手法は、これまでに種々提案されてきており、また広く実用にも供されている。その一例としては、下記の〔特許文献１〕や〔特許文献２〕がある。
【０００４】
〔特許文献１〕の発明によれば、パソコンでアプリケーションを実行する際に、パソコン外部のＵＳＢメモリの書き換え不可能な領域に記録されたＩＤ等をアプリケーションが読み取り、ＩＤ等が正しければアプリケーションを実行するようにしている。

【０００５】
また〔特許文献２〕の発明によれば、録画操作のとき、（１）配布装置において、媒体からＩＤと公開鍵Ｋｐを読み取り、ＩＤと共通鍵Ｋｗを公開鍵Ｋｐで暗号化し媒体に記録し、（２）配布するコンテンツは共通鍵Ｋｗで暗号化して媒体へ格納する。一方、再生操作のときは、（１）端末装置（再生装置）は媒体から、暗号化されていないＩＤと暗号化されたＩＤと共通鍵Ｋｗを読み取り、（２）端末装置は、端末装置に保持している秘密鍵Ｋｓで、暗号化されたＩＤと共通鍵Ｋｗを復号し、（３）端末装置は、復号したＩＤと、媒体から読み取った暗号化されていないＩＤを比較し、一致することを確認し、（４）暗号化されたコンテンツを、復号して得たＫｗにより復号する。
【０００６】
【特許文献１】特開２００３－２８８１２８号公報
【特許文献２】特開平１１－２５０５７１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
従来の典型的なコピープロテクト方法においては、「秘密鍵」が、市場に大量に流通する再生装置の中に含まれている。このため、その秘密鍵がその再生装置から盗み出された場合には、コンテンツ記録媒体に含まれる共通鍵が解読可能となり、また、公開鍵もその媒体に含まれることから、容易にコンテンツの海賊版が作成できてしまう。すなわちコピープロテクト機能が弱い。
【０００８】
したがって本発明は、従来に比してより一層プロテクション機能を増強させたコピープロテクション方法を提供することを目的とするものである。
【０００９】
さらにまた、そのコピープロテクション方法に適合するコンテンツ再生装置およびＩＣチップを提供することを目的とするものである。
【課題を解決するための手段】
【００１０】
本明細書で開示するコピープロテクト方法は、「コンテンツ記録媒体の製造時」における第１の方法ステップと、「コンテンツの再生時」における第２の方法ステップとに分けられる。
【００１１】
上記第１の方法ステップは、（ａ）ＩＣチップを一意に特定するチップＩＤを読み出すステップと、（ｂ）コンテンツ記録媒体に記録されたコンテンツを一意に特定するコンテンツＩＤを生成するステップと、（ｃ）これらのＩＤを暗号化するステップと、（ｄ）該ステップ（ｃ）による暗号化チップＩＤおよび暗号化コンテンツＩＤを、上記のＩＣチップ内に記録するステップと、（ｅ）これらの暗号化ＩＤを格納した上記のＩＣチップを、コンテンツ記録媒体に付加するステップと、からなる。
【００１２】
一方上記第２の方法ステップは、（ｆ）チップＩＤを第１の鍵で暗号化した暗号化チップＩＤと、コンテンツを一意に特定するコンテンツＩＤを上記の第１の鍵で暗号化した暗号化コンテンツＩＤと、を格納するＩＣチップが付加されたコンテンツ記録媒体を、コンテンツ再生装置にセットするステップと、（ｇ）上記のチップＩＤと暗号化チップＩＤと暗号化コンテンツＩＤと、を読み出すステップと、（ｈ）読み出したこれらの暗号化ＩＤを、第２の鍵でそれぞれ復号化するステップと、（ｉ）復号化して再生されたチップＩＤおよびコンテンツＩＤと、上記のステップ（ｇ）で読み出されたチップＩＤおよび上記コンテンツから改めて生成されたコンテンツＩＤと、の一致／不一致をそれぞれ検出するステップと、（ｊ）その検出により一致とされたときにのみコンテンツ再生装置でのコンテンツの再生を許可するステップと、からなる。
【発明の効果】

【００１３】
本明細書で開示するコピープロテクト方法によれば、ハードウェアチップであるＩＣチップを媒介として、コンテンツ記録媒体の不正コピーを防止する。このＩＣチップ内には、他に同一のものが２つと存在しないチップＩＤが元々記録されているので、これをコピープロテクトとして利用する。しかも特定の製造者のみが知る秘密鍵によってこれを暗号化した暗号化チップＩＤを用いる。さらに加えて、このＩＣチップ内には、このＩＣチップが付加されるコンテンツ記録媒体に記録されたコンテンツを一意に表すコンテンツＩＤも格納される。これもまた上記の秘密鍵によって暗号化される。
【００１４】
かくして、コンテンツ再生装置において暗号化チップＩＤおよび暗号化コンテンツＩＤとをそれぞれ復号化したＩＤおよび、元々のチップＩＤが、このコンテンツ再生装置においてそれぞれ「正しく元通り再現」できたときに限り、当該コンテンツの再生が許可されるようにする。
【００１５】
したがって、悪意の第三者により、コンテンツ（暗号化されているかいないかに拘らず）のコピーがされたとしても、その不正コピーのコンテンツは、最終的に、上記した「正しい再現」ができない限り、再生不可能である。このことから、悪意の第三者がコンテンツそのもののコピーに成功しても、結局はそのコンテンツの再生ができないので、不正なコピーを未然に防ぐことができる。ここで用いるＩＣチップ少なくともメモリが内蔵されていれば十分であって、ＣＰＵ等の高機能部分は必要としないから、安価であり、かつ小型でもある。
【発明を実施するための最良の形態】
【００１６】
図１は本明細書により開示する第１の方法ステップを図解的に表す図であり、
図２は本明細書により開示する第２の方法ステップを図解的に表す図である。なお、上述のとおり、上記第１の方法ステップは「コンテンツ記録媒体の製造時」に相当し、一方、上記第２の方法ステップは「コンテンツの再生時」に相当する。
【００１７】
まず図１の製造側１００を参照すると、右端のブロック１０が、コピープロテクトの対象となるコンテンツ記録媒体（以下、単に記録媒体とも称す）を表す。この記録媒体１０には、本図の左端に示す「コンテンツ」１１が焼き付けられる（矢印Ａ）。このコンテンツ１１は、例えば映画であり音楽であり、あるいはソフトウェアであってもよい。なお、このコンテンツ１１は暗号化してもしてなくてもどちらでも良く、どちらであっても本発明のコピープロテクト機能には影響しない。
【００１８】
本発明において注目すべき部分は、本図の右端に示すブロック１２であり、これが前述したＩＣチップである。このＩＣチップ１２には元々、同じものが２つとないチップＩＤ（個別識別番号）１３が記録されている。またこのＩＣチップ１３内には、ＩＤメモリ１４が設けられる。
【００１９】
本発明によるコピープロテクト方法の第１段階は、チップＩＤとコンテンツＩＤの各情報を揃えることである。これを概念的にＩＤ情報１６として示す。ＩＤ情報１６内のチップＩＤは、図の矢印Ｂで示すように、ＩＣチップ１２から読み出したチップＩＤ１３である。一方、該ＩＤ情報１６内のコンテンツＩＤは、次のようにして用意される。
【００２０】
まず前述のコンテンツ１１に対し所定の演算処理を行って（矢印Ｃ参照）、コンテンツＩＤ１５を得る。この所定の演算処理の一例としてはハッシュ関数による演算があり、この演算により「ハッシュ値」を得る。このハッシュ関数によると、例えば５ＧＢのコンテンツ１１を一意に特定する、例えば１２８Ｂのハッシュ値（コンテンツＩＤ）が得られる。かくして得られたコンテンツＩＤ１５を、上記ＩＤ情報１６の１つとしてエントリーす

る。
【００２１】
続く第２段階では、ＩＤ情報１６を暗号化する（矢印Ｅ参照）。この暗号化は秘密鍵１７により行われ、暗号化ＩＤ情報１６′を得る。この場合、この秘密鍵１７は特定の製造者（例えばＩＣチップ製造者）といった一部の者しか知ることができず、きわめて機密性が高い。
【００２２】
ここに、暗号化チップＩＤ１３′と暗号化コンテンツＩＤ１５′とからなる暗号化ＩＤ情報１６′が得られる。そしてさらにＩＣチップ１２内の上記ＩＤメモリ１４にそのＩＤ情報１６′が格納される。
【００２３】
このようにして加工されたＩＣチップ１２は、対応する唯一のコンテンツ記録媒体１０に付加され、さらにユーザによる購買のために市場に流通することになる。
【００２４】
市場においてユーザに購入された、ＩＣチップ付きのコンテンツ記録媒体は、例えばユーザ宅内のコンテンツ再生装置（プレーヤ）にセットされる。もしこのＩＣチップ付きの記録媒体が不正に製造されたものであれば（海賊版）、その再生は不可となる。これは上記の第２の方法ステップにより可能となる。
【００２５】
ここで図２を参照して第２の方法ステップを図解的に説明する。本図において上記のコンテンツ再生装置（以下、単に再生装置とも称す）は、参照番号２００で示される。まず第１段階では、再生装置２００にセットされたコンテンツ記録媒体２０から、コンテンツ２１を読み出す（矢印Ｇ）。またこの記録媒体２０に付加されているＩＣチップ２２からチップＩＤ２３と、このＩＣチップ２２内のＩＤメモリ２４に格納された暗号化チップＩＤ２３′と、暗号化コンテンツＩＤ２５′とを読み出し、暗号化ＩＤ情報２６′を再生する（矢印Ｈ）。
【００２６】
次に第２段階では、前述した矢印Ｇにより再生した上記のコンテンツ２１に対し、上述した所定の演算処理（図１の矢印Ｃ）と全く同一の演算処理を施して、コンテンツＩＤ２５を生成する（図２の矢印Ｃ）。
【００２７】
さらに第３段階では、暗号化ＩＤ情報２６′をなす暗号化チップＩＤ２３′と暗号化コンテンツＩＤ２５′とを、公開鍵２７により復号化する（図２の矢印Ｉ）。ここに、復号化されたＩＤ情報２６″を得、復号化チップＩＤ２３″と復号化コンテンツＩＤ２５″、すなわち元のチップＩＤと元のコンテンツＩＤを再現する。
【００２８】
最後の第４段階では、上記のとおり再現された各ＩＤの一致／不一致を、第１比較部３１と第２比較部３２とにより、検出する。第１比較部３１では、再現した「チップＩＤ２３″」と、ＩＣチップ２２から読み出した「チップＩＤ２３」とを比較し、両者の一致（ＯＫ）または不一致（ＮＧ）を判定する。
【００２９】
これと並行して、第２比較部３２では、再現した「コンテンツＩＤ２５″」と、上述のハッシュ関数により演算された「コンテンツＩＤ２５」とを比較し、両者の一致（ＯＫ）または不一致（ＮＧ）を判定する。
【００３０】
ここに、当該コンテンツ記録媒体２０が不正コピーによるものか否かが判明する。上記の比較（３１，３２）の結果が、双方共一致（ＯＫ）であればそれの媒体２０は真正品（すなわち媒体１０）であり、再生装置２００においては、当該コンテンツの再生が可能となる。逆に、上記の比較（３１，３２）の結果において、少なくとも一方が不一致（ＮＧ）ならばそれは不正コピー品であり、再生装置２００においては、当該コンテンツを再生

することができない。結局、悪意の第三者は、不正コピー品を作製してもそれは、究極、再生不能であって商品とはならないから、始めからそのような不正コピーをすることを計画しないであろう。

【００３１】

このような不正コピーの防止例としては次の（ａ）および（ｂ）が考えられる。すなわち、

（ａ）図１の右端に示す、ＩＣチップ１２を付加したコンテンツ記録媒体１０が市場に提供される。このＩＣチップ１２を第三者が媒体１０から取り外し、他の記録媒体に不正に付加したとする。

【００３２】

このような記録媒体を再生装置２００にセットしたとする。そうすると、ＩＣチップ１２はそのまま使用されているから、両ＩＤは当然一致し、第１比較部３１はパスする。ところが、両コンテンツは異なるから、ハッシュ値（コンテンツＩＤ）が合わず、第２比較部３２での判定をパス（ＯＫ）することができず、結局、再生不能となる。

【００３３】

（ｂ）同一のコンテンツを有する不正にコピーされた他の記録媒体（海賊版）に、第三者が類似のＩＣチップを付加した不正コピー品を作製したとする。そうすると、その類似のＩＣチップのチップＩＤと、ＩＤメモリ２４から再現したチップＩＤとは、必ず不一致（同一のチップＩＤは２つとない）となり、第１比較部３１でＮＧとなり再生不能である。ＩＣチップ１２のチップＩＤを知り得たとしても、秘密鍵１７は知り得ないので、本来の暗号化チップＩＤ１３′を作ることはできないし、また真正品と同一のコンテンツＩＤも作ることができない。

【００３４】

ここで上述したＩＣチップ１２について要約すると、このＩＣチップは、コンテンツ記録媒体１０に付加可能で、かつ、書き換え不能に一意に設定されたチップＩＤ１３が元々記録されているＩＣチップであって、コンテンツ１１を特定するコンテンツＩＤ１５を暗号化した暗号化コンテンツＩＤ１５′と、チップＩＤ１３を暗号化した暗号化チップＩＤ１３′とを格納する書込み読出し可能なＩＤメモリ１４を内蔵するものである。

【００３５】

そしてそのコンテンツＩＤ１５は、コンテンツ１１をなすＮバイトのデジタルデータを、所定の関数により演算して得た、ｎ（ｎ＜＜Ｎ）バイトの演算値から生成される。この所定の関数は、例えばハッシュ関数であり、その演算値は該ハッシュ関数によるハッシュ値である。

【００３６】

さらに、コンテンツＩＤ１５とチップＩＤ１３とを共に第１の鍵（１７）により暗号化してそれぞれ、暗号化コンテンツＩＤ１５′と暗号化チップＩＤ１３′とを生成するようにする。ここにその第１の鍵は、コンテンツ記録媒体１０に記録されたコンテンツ１１を再生する際に、暗号化コンテンツＩＤ１５′および暗号化チップＩＤ１３′を復号化するために用いる第２の鍵（２７）と、相互に対をなすものである。この場合、第１の鍵（１７）は、当該ＩＣチップ１２の製造者のみが秘密裏に保有する秘密鍵１７であり、また第２の鍵（２７）は、コンテンツ記録媒体１０に記録されたコンテンツ１１を再生するコンテンツ再生装置２００の各々に公開して付与される公開鍵２７である。

【００３７】

かかるＩＣチップ１２は、コンテンツ記録媒体１０の製造者とは異なる製造者により製造されることが望ましい。ＩＣチップ１２の秘密性をより一層強固にするためである。このようなＩＣチップ１２を付加したコンテンツ記録媒体１０は、新規なものである。なお、このＩＣチップ１２は、例えば接着又は埋め込み等によりコンテンツ記録媒体１２に付加することができる。

【００３８】

次に図２において概念を示したコンテンツ再生装置２００の具体例について説明する。

【００３９】
図３はコンテンツ再生装置２００の具体例を示す図である。本図において、コンテンツ再生装置２００は、まず第１読出し機能部４１と第２読出し機能部４２とを有する。これら機能部は、
（ｉ）コンテンツ１１を一意に特定するために該コンテンツ１１をもとに所定の処理により得たコンテンツＩＤ１５と、一意に設定されて書き換え不能にＩＣチップ１２に元々記録されているチップＩＤ１３とをそれぞれ、第１の鍵（１７）により暗号化した暗号化コンテンツＩＤ１５′と暗号化チップＩＤ１３′とをＩＤメモリ２４に格納してコンテンツ記録媒体２０に付加されるＩＣチップ２２から、暗号化コンテンツＩＤ２５′および暗号化チップＩＤ２３′を読み出す第１読出し機能部４１、および
（ii）該ＩＣチップ２２自体に内蔵されるチップＩＤ２３を読み出す第２読出し機能部４２、
である。なお、上記（ｉ）において、コンテンツＩＤ１５とチップＩＤ１３とをそれぞれ第１の鍵により暗号化する、すなわちこれらＩＤを別々に暗号化する、としているが、これに限らず、該コンテンツＩＤ１５とチップＩＤ１３とを合わせて１つのＩＤデータとしてから一度に暗号化するようにしてもよい。
【００４０】
さらには復号化機能部４３を有する。この機能部は、読み出した暗号化コンテンツＩＤ２５′および暗号化チップＩＤ２３′を、第１の鍵（１７）と相互に対をなす第２の鍵（２７）により復号化し、元のコンテンツＩＤ２５″およびチップＩＤ２３″を再生する復号化機能部４３である。
【００４１】
一方、コンテンツ記録媒体２０に記録されたコンテンツ２１を、前述した所定の処理と同一の処理により得たコンテンツＩＤ２５を生成するコンテンツＩＤ生成機能部４４も有している。
【００４２】
そして最終段には、復号化機能部４３からの復号データ（ＣＨ，ＣＯ）と、第２読出し機能部４２およびコンテンツＩＤ生成機能部４４からの各出力データ（ＣＨ，ＣＯ）とが一致したときのみ、コンテンツ２１の再生を許可する再生許可機能部４５が備えられる。この再生許可機能部４５は、復号化機能部４３からの復号化チップＩＤ（ＣＨ）と、第２読出し機能部４２からのチップＩＤ（ＣＨ）との一致／不一致を検出するチップＩＤ比較部５１と、復号化機能部４３からの復号化コンテンツＩＤ（ＣＯ）と、コンテンツＩＤ生成機能部４４からのコンテンツＩＤ（ＣＯ）との一致／不一致を検出するコンテンツＩＤ比較部５２と、からなる。
【００４３】
これら両比較部５１，５２からの比較結果が共に一致していれば（ＯＫ）、第１のゲート（ＡＮＤ相当）５３を介し、第２のゲート（スイッチ相当）５４をＯＮにし、真正な記録媒体２０のコンテンツ２１（すなわち元の記録媒体１０のコンテンツ１１）を、映画／音楽等の再生ユニット（図示せず）に転送する。
【００４４】
なお前述したように、コンテンツＩＤ１５は、コンテンツ１１をなすＮバイトのデジタルデータを、所定の関数により演算して得た、ｎ（ｎ＜＜Ｎ）バイトの演算値であり、またその所定の関数は、ハッシュ関数であって、その演算値は該ハッシュ関数によるハッシュ値である。
【００４５】
既述の図１および図２には、前述した第１の方法ステップ（製造側時）と第２の方法ステップ（再生時）とを概念的に表したので、これらの方法ステップを具体的なフローチャートにより表すと次のようになる。
【００４６】
図４は製造側１００での方法ステップを表すフローチャートであり、また

図５は再生装置２００側での方法ステップを表すフローチャートである。まず図４を参照する。

【００４７】

本図において、

ステップＳ１１：ＩＣチップ１２内に元々記録されて該ＩＣチップを一意に特定するチップＩＤ１３を読み出す。

ステップＳ１２：コンテンツ記録媒体１０に記録されたコンテンツ１１を一意に特定するコンテンツＩＤ１５を生成する。

ステップＳ１３：チップＩＤ１３およびコンテンツＩＤ１５を暗号化する。

ステップＳ１４：暗号化された暗号化チップＩＤ１３′および暗号化コンテンツＩＤ１５′を、ＩＣチップ１２内に記録する。

ステップＳ１５：暗号化チップＩＤ１３′および暗号化コンテンツＩＤ１５′を格納したＩＣチップ１２を、コンテンツ記録媒体１０に付加する。

かくして製造された、ＩＣチップ付きコンテンツ記録媒体１０が市場に供給される。

【００４８】

次に図５を参照すると、

ステップＳ２１：一意に設定されて書き換え不能にＩＣチップに元々記録されているチップＩＤ１３を第１の鍵（１７）で暗号化した暗号化チップＩＤ１３′と、コンテンツ記録媒体１０に記録されたコンテンツ１１を一意に特定するべく所定の処理により生成されたコンテンツＩＤ１５を第１の鍵（１７）で暗号化した暗号化コンテンツＩＤ１５′と、を格納する当該ＩＣチップ２２が付加されたコンテンツ記録媒体２０を、コンテンツ再生装置２００にセットする。

ステップＳ２２：ＩＣチップ２２内の、チップＩＤ２３と暗号化チップＩＤ２３′と暗号化コンテンツＩＤ２５′と、を読み出す。

ステップＳ２３：読み出した暗号化チップＩＤ２３′および暗号化コンテンツＩＤ２５′を、第１の鍵（１７）と相互に対をなす第２の鍵（２７）でそれぞれ復号化する。

ステップＳ２４：復号化して再生されたチップＩＤ２３″およびコンテンツＩＤ２５″と、読み出されたチップＩＤ２３および前記の所定の処理と同一の処理により生成されたコンテンツＩＤ２５と、の一致／不一致をそれぞれ検出する。

ステップＳ２５：前記の検出により一致とされたときにのみコンテンツ再生装置２００でのコンテンツ２１の再生を許可する。このコンテンツ２１は、真正の記録媒体１０内のコンテンツ１１と全く同一のものである。

【００４９】

以上述べたコピープロテクト方法の新規な点をまとめると、次の（１）～（４）に示すとおりである。

【００５０】

（１）コンテンツ記録媒体に、コンテンツに対応したコンテンツＩＤをハードウェア（チップ）で実装し、複製を困難にする点。

【００５１】

（２）コンテンツに依存するコンテンツＩＤを使用し、ＩＣチップが他のコンテンツには使用（流用）できなくする点。

【００５２】

（３）許可された製造者（秘密鍵を持っている製造者）だけが媒体を製造できる環境のもとで、コンテンツＩＤやチップＩＤを暗号化して、ＩＣチップに書き込む点。

【００５３】

（４）製造されたコンテンツ記録媒体のセキュリティ管理を向上させるために、コンテンツ情報を含むＩＣチップと、コンテンツ本体を含む記録媒体とを別々に生産できる点。

【００５４】

またその効果を列記すると、次の（ａ）～（ｄ）に示すとおりである。

【００５５】

（ａ）記録媒体にソフトウェアを入れて販売する際に本発明のコピープロテクト方法を用いることで、不正な媒体の複製を防ぎ、そのソフトウェアが真正であることを証明できる。つまり、真正の媒体から、真正のＩＣチップを取り外し、別の媒体に付加し、改ざんしたソフトウェアを媒体に入れたとしても、ＩＣチップ内のコンテンツＩＤを参照することで、ソフトウェアが改ざんしたものであることが容易に判明する。

【００５６】

（ｂ）コンテンツＩＤを書き込んだＩＣチップをある製造者が製造し、複数の媒体製造業者へ配布することで、コンテンツの製造数や、ある記録媒体がどこの媒体製造業者で作られたか、などのコンテンツ管理における利便性が向上する。つまり、ＩＣチップ製造業者と記録媒体製造業者とを別々に分けることで、コンテンツ管理がより厳密になる。もし、単一の業者にＩＣチップへのコンテンツＩＤ書き込みと記録媒体の製造とを任せたとすると、焼かれたチップの製造数が外部から分かりにくくなり、不正をよりし易くさせることになるためである。

【００５７】

（ｃ）ハードウェアチップであるチップＩＤはコピーできない。また、暗号化されたコンテンツＩＤは改ざんできない。このため、コンテンツだけを他の記録媒体へコピーしても、そのコンテンツを再生することはできず、違法コピーを防ぐことができる。

【００５８】

（ｄ）コンテンツが暗号化されていると否とに拘らず、そのコンテンツだけを他の媒体へコピーして配布したとしても、チップＩＤを確認しないようにした海賊版プレーヤも一緒に提供しない限り、海賊版の媒体を受け取ったユーザは、当該不正コンテンツの再生ができない。同じ海賊版の媒体を作るためには、製造者しか知らない秘密鍵を盗み出し、かつ、何も書き込まれていないＩＣチップを入手することが必要である。しかし、これは事実上困難である。

【００５９】

上述した実施形態に関し、以下の付記を開示する。

【００６０】

（付記１）

コンテンツ記録媒体に付加可能で、かつ、書き換え不能に一意に設定されたチップＩＤが元々記録されているＩＣチップであって、

前記コンテンツを特定するコンテンツＩＤを暗号化した暗号化コンテンツＩＤと、前記チップＩＤを暗号化した暗号化チップＩＤとを格納する書込み読出し可能なＩＤメモリを内蔵するＩＣチップ。

【００６１】

（付記２）

前記コンテンツＩＤは、前記コンテンツをなすＮバイトのデジタルデータを、所定の関数により演算して得た、ｎ（ｎ＜＜Ｎ）バイトの演算値である付記１に記載のＩＣチップ。

【００６２】

（付記３）

前記所定の関数は、ハッシュ関数であり、前記演算値は該ハッシュ関数によるハッシュ値である付記２に記載のＩＣチップ。

【００６３】

（付記４）

前記コンテンツＩＤと前記チップＩＤとを共に第１の鍵により暗号化してそれぞれ、前記暗号化コンテンツＩＤと前記暗号化チップＩＤとを生成する付記１に記載のＩＣチップ。

【００６４】

（付記５）

前記第１の鍵は、前記コンテンツ記録媒体に記録されたコンテンツを再生する際に、前

記暗号化コンテンツＩＤおよび暗号化チップＩＤを復号化するために用いる第２の鍵と、相互に対をなす付記４に記載のＩＣチップ。

【００６５】

（付記６）

前記第１の鍵は、当該ＩＣチップの製造者のみが秘密裏に保有する秘密鍵であり、

前記第２の鍵は、前記コンテンツ記録媒体に記録されたコンテンツを再生するコンテンツ再生装置の各々に公開して付与される公開鍵である付記５に記載のＩＣチップ。

【００６６】

（付記７）

前記ＩＣチップは、前記コンテンツ記録媒体の製造者とは異なる製造者により製造される付記６に記載のＩＣチップ。

【００６７】

（付記８）

付記１に記載のＩＣチップを付加したコンテンツ記録媒体。

【００６８】

（付記９）

付記８において、前記ＩＣチップを、接着又は埋め込みにより前記コンテンツ記録媒体に付加すること。

【００６９】

（付記１０）

コンテンツを一意に特定するために該コンテンツをもとに所定の処理により得たコンテンツＩＤと、一意に設定されて書き換え不能にＩＣチップに元々記録されているチップＩＤとをそれぞれ、第１の鍵により暗号化した暗号化コンテンツＩＤと暗号化チップＩＤとをＩＤメモリに格納してコンテンツ記録媒体に付加される前記ＩＣチップから、前記暗号化コンテンツＩＤおよび暗号化チップＩＤを読み出す第１読出し機能部および前記ＩＣチップ自体に内蔵される前記チップＩＤを読み出す第２読出し機能部と、

読み出した前記暗号化コンテンツＩＤおよび暗号化チップＩＤを、前記第１の鍵と相互に対をなす第２の鍵により復号化し、元の前記コンテンツＩＤおよびチップＩＤを再生する復号化機能部と、

前記コンテンツ記録媒体に記録されたコンテンツを、前記所定の処理と同一の処理により得たコンテンツＩＤを生成するコンテンツＩＤ生成機能部と、を有し、

前記復号化機能部からの復号データと、前記第２読出し機能部およびコンテンツＩＤ生成機能部からの各出力データとが一致したときのみ、前記コンテンツの再生を許可する再生許可機能部と、

を備えるコンテンツ再生装置。

【００７０】

（付記１１）

前記コンテンツＩＤは、前記コンテンツをなすＮバイトのデジタルデータを、所定の関数により演算して得た、ｎ（ｎ＜＜Ｎ）バイトの演算値である付記１０に記載のコンテンツ再生装置。

【００７１】

（付記１２）

前記所定の関数は、ハッシュ関数であり、前記演算値は該ハッシュ関数によるハッシュ値である付記１１に記載のコンテンツ再生装置。

【００７２】

（付記１３）

前記再生許可機能部は、

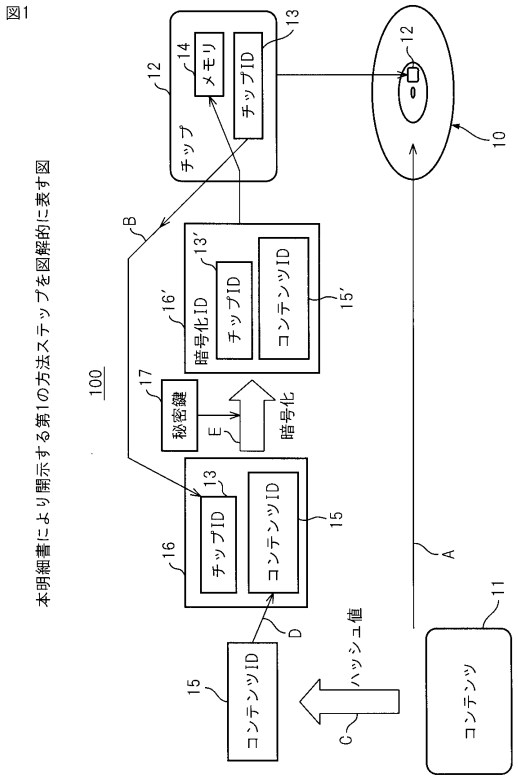
前記復号化機能部からの復号化チップＩＤと、前記第２読出し機能部からのチップＩＤとの一致／不一致を検出するチップＩＤ比較部と、

前記復号化機能部からの復号化コンテンツＩＤと、前記コンテンツＩＤ生成機能部から

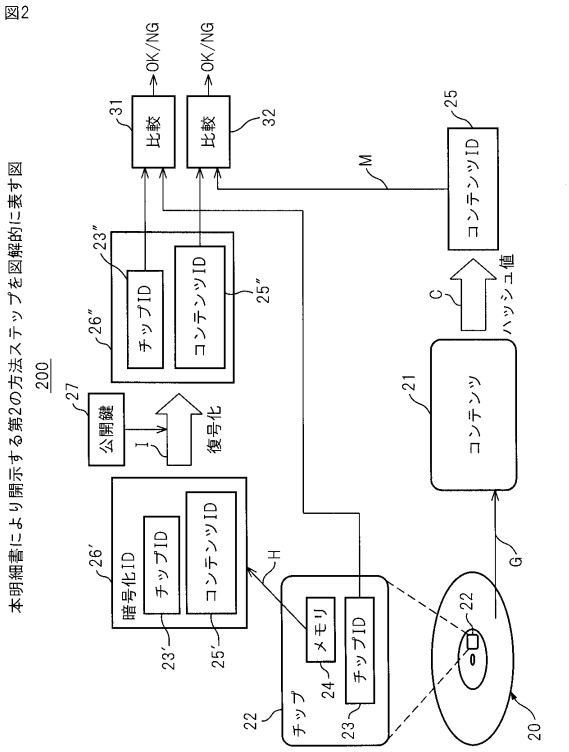
のコンテンツＩＤとの一致／不一致を検出するコンテンツＩＤ比較部と、
からなる付記１１に記載のコンテンツ再生装置。
【００７３】
（付記１４）
ＩＣチップ内に元々記録されて該ＩＣチップを一意に特定するチップＩＤを読み出すステップと、
コンテンツ記録媒体に記録されたコンテンツを一意に特定するコンテンツＩＤを生成するステップと、
前記チップＩＤおよび前記コンテンツＩＤを暗号化するステップと、
暗号化された暗号化チップＩＤおよび暗号化コンテンツＩＤを、前記ＩＣチップ内に記録するステップと、
前記暗号化チップＩＤおよび暗号化コンテンツＩＤを格納した前記ＩＣチップを、前記コンテンツ記録媒体に付加するステップと、
を有するコピープロテクト方法。
【００７４】
（付記１５）
一意に設定されて書き換え不能にＩＣチップに元々記録されているチップＩＤを第１の鍵で暗号化した暗号化チップＩＤと、コンテンツ記録媒体に記録されたコンテンツを一意に特定するべく所定の処理により生成されたコンテンツＩＤを前記第１の鍵で暗号化した暗号化コンテンツＩＤと、を格納する当該ＩＣチップが付加されたコンテンツ記録媒体を、コンテンツ再生装置にセットするステップと、
前記ＩＣチップ内の、前記チップＩＤと前記暗号化チップＩＤと前記暗号化コンテンツＩＤと、を読み出すステップと、
読み出した前記暗号化チップＩＤおよび暗号化コンテンツＩＤを、前記第１の鍵と相互に対をなす第２の鍵でそれぞれ復号化するステップと、
復号化して再生された前記チップＩＤおよびコンテンツＩＤと、前記の読み出されたチップＩＤおよび前記所定の処理と同一の処理により生成された前記コンテンツＩＤと、の一致／不一致をそれぞれ検出するステップと、
前記の検出により一致とされたときにのみ前記コンテンツ再生装置での前記コンテンツの再生を許可するステップと、
を有するコピープロテクト方法。
【図面の簡単な説明】
【００７５】
【図１】本明細書により開示する第１の方法ステップを図解的に表す図である。
【図２】本明細書により開示する第２の方法ステップを図解的に表す図である。
【図３】コンテンツ再生装置２００の具体例を示す図である。
【図４】製造側１００での方法ステップを表すフローチャートである。
【図５】コンテンツ再生装置２００側での方法ステップを表すフローチャートである。
【符号の説明】
【００７６】
１０，２０　コンテンツ記録媒体
１１，２１　コンテンツ
１２，２２　ＩＣチップ
１３，２３　チップＩＤ
１３′，２３′　暗号化チップＩＤ
１４，２４　ＩＤメモリ
１５，２５　コンテンツＩＤ
１５′，２５　暗号化コンテンツＩＤ
１６，２６　ＩＤ情報
１６′，２６′　暗号化ＩＤ情報

１７　秘密鍵
２３〃　復号化チップＩＤ
２５〃　復号化コンテンツＩＤ
２６〃　復号化ＩＤ情報
２７　公開鍵
３１　第１比較部
３２　第２比較部
４１　第１読出し機能部
４２　第２読出し機能部
４３　復号化機能部
４４　コンテンツＩＤ生成機能部
４５　再生許可機能部
１００　製造側
２００　コンテンツ再生装置

【図１】

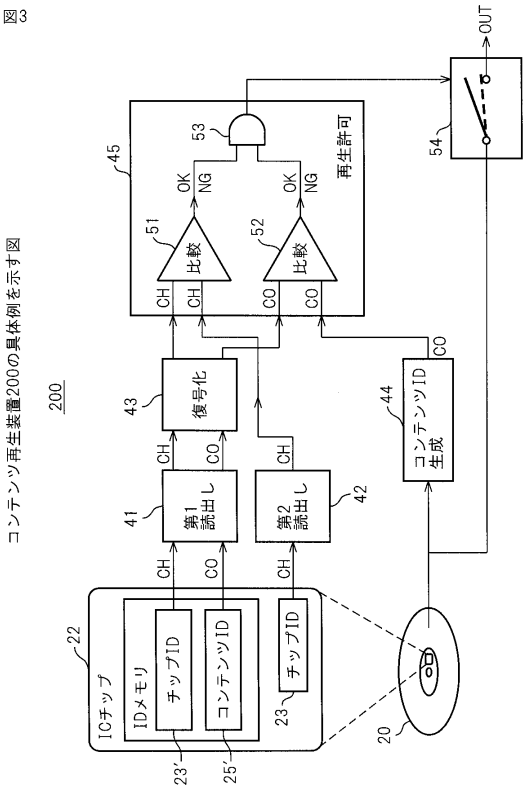


【図２】



【図３】

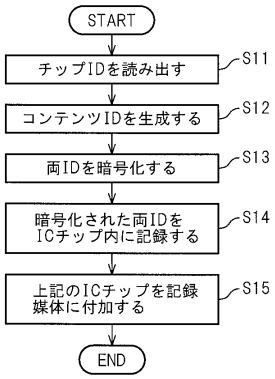
図3



【図４】

図4

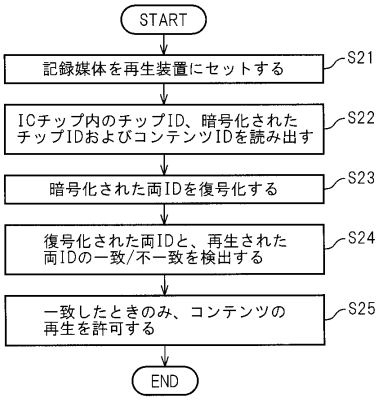
製造側100での方法ステップを表すフローチャート



【図５】

図5

コンテンツ再生装置200側での方法ステップを表すフローチャート



フロントページの続き

(51)Int.Cl.			FI		
G11B	***7/005***	***(2006.01)***	G11B	20/10	H
G11B	***7/007***	***(2006.01)***	G11B	7/005	Z
			G11B	7/007	

審査官　平井　誠

(56)参考文献　特開２００３－０５８８４０（ＪＰ，Ａ）
特開２００４－０４６４５２（ＪＰ，Ａ）
再公表特許第９６／０１６４０１（ＪＰ，Ａ１）
特開２００３－１２３４０１（ＪＰ，Ａ）
特開２００４－１９９１７８（ＪＰ，Ａ）
特開２００６－０９９２６２（ＪＰ，Ａ）
特開２００６－２６８５１３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ１１Ｂ　７／００５
Ｇ１１Ｂ　７／００７
Ｇ１１Ｂ　２０／１０
Ｈ０４Ｎ　５／８５
Ｈ０４Ｎ　５／９１