(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2004-22085
(P2004-22085A)
(43)公開日　平成16年1月22日(2004.1.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11B 20/10	G11B 20/10	H	5B017
G06F 12/00	G11B 20/10	F	5B082
G06F 12/14	G11B 20/10	301Z	5C053
H04L 9/10	G06F 12/00	537H	5D044
H04N 5/91	G06F 12/14	320B	5J104

審査請求 未請求　請求項の数 3　OL　（全 15 頁）　最終頁に続く

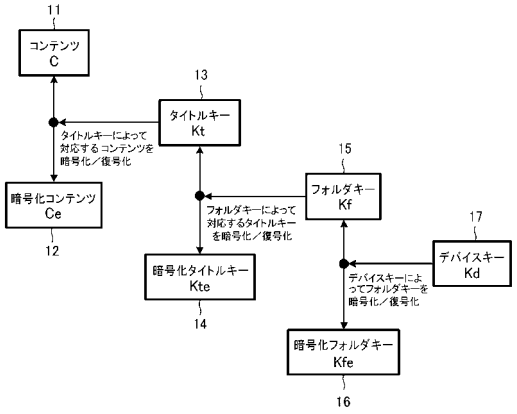
(21)出願番号　特願2002-176578(P2002-176578)
(22)出願日　平成14年6月18日(2002.6.18)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100083161
弁理士　外川　英明
(72)発明者　原澤　昭典
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(72)発明者　山田　雅弘
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(72)発明者　坂本　典哉
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

Fターム(参考)　5B017 AA03　BA07　CA09　CA16
最終頁に続く

(54)【発明の名称】記録再生装置

(57)【要約】
【課題】内容的にまとまりのあるタイトルをその単位で取り扱いやすくするフォルダ（ディレクトリ）の導入によって、タイトルの移動／消去をより効率的に行う。
【解決手段】フォルダおよびフォルダキーを導入し、タイトル移動あるいは消去を行う場合に、移動あるいは消去したいタイトルが属するフォルダに関してはそのフォルダキーとそのフォルダ内にある全タイトルキーを再暗号化するが、移動／消去したいタイトルが属さない残りのフォルダに関してはそのフォルダキーのみを再暗号化するだけの処理とする。これにより、暗号化に係る時間の短縮化を図ることができる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを他の記録媒体に移動する記録再生装置において、
前記移動するコンテンツが属さない全フォルダの暗号化フォルダキーを、不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって移動するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、前記移動するコンテンツが属するフォルダの暗号化フォルダキーを、前記不揮発性メモリに保持されているデバイスキーによって復号化し、移動するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって移動するコンテンツが属するフォルダ内のタイトルキーを再暗号化する手段と、
前記新デバイスキーによって移動するコンテンツが属するフォルダのフォルダキーを再暗号化する手段とを具備したことを特徴とする記録再生装置。
【請求項２】
記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを消去する記録再生装置において、
前記消去するコンテンツが属さない全フォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって消去するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、
前記消去するコンテンツが属するフォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、消去するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって消去するコンテンツが属するフォルダ内のタイトルキーを再暗号化する手段と、
前記新デバイスキーによって消去するコンテンツが属するフォルダのフォルダキーを再暗号化する手段とを具備したことを特徴とする記録再生装置。
【請求項３】
前記デバイスキーは記録再生装置内の不揮発性メモリに保持され、各記録再生装置ごとに異なる値を持つことを特徴とする請求項１または２記載の記録再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、記録媒体に映像や音声など暗号化されたコンテンツを移動あるいは消去を行う記録再生装置に関する。
【０００２】
【従来の技術】
従来の記録再生装置に用いられる暗号化／復号化は、特開２０００－２３２４４１公報に開示されるデバイスキーＫｄとタイトルキー（この公報ではマスタキー）Ｋｔにより行われている。
【０００３】
図９はこの２つの鍵の役割について説明するための概念図である。タイトルキー９３はコンテンツ９１を暗号化／復号化するための鍵で、デバイスキー９５はタイトルキー９３を暗号化／復号化するための鍵である。また、タイトルキー９３は各コンテンツごとに異なり、デバイスキー９５は全タイトルキー共通の鍵である。以下、暗号化されたコンテンツを暗号化コンテンツ９２（Ｃｅ）と、暗号化されたタイトルキーを暗号化タイトルキー９

４（Ｋｔｅ）とする。

【０００４】

記録再生装置の主記録媒体に記録されているコンテンツを他の記録媒体に移動する場合、コンテンツ移動前に主記録媒体のバックアップをとっておき、コンテンツ移動後の主記録媒体にそのバックアップを戻すことでコピー操作が実現できるという問題がある。これを解決するため、従来の記録再生装置では、コンテンツ移動後の主記録媒体にバックアップを戻しても、その戻したコンテンツを復号化（再生）できないよう鍵を更新している。

【０００５】

図１０はこの鍵の更新について説明するためのもので、再生記録装置の主記録媒体に３つのコンテンツがそれぞれタイトルＡ、タイトルＢ、タイトルＣのタイトルで記録されている場合を考える。

【０００６】

タイトルＡ１０２の移動と同時にデバイスキー１０１を更新し、この新しいデバイスキー１０５により、タイトルＢのタイトルキー１０３とタイトルＣのタイトルキー１０４を再暗号化する。この結果、バックアップタイトルＡ１０６を主記録媒体に戻しても、デバイスキーが更新されているためバックアップタイトルＡ１０６は復号化できず、不正コピーを防ぐことができる。

【０００７】

同様に、記録再生装置の主記録媒体に記録されているコンテンツを消去する場合も、コンテンツの消去後にバックアップが利用できないようコンテンツ移動時と同様な鍵の更新が行われている。

【０００８】

しかしながら、上記した従来の技術でタイトルの移動／消去を行う場合、タイトルの移動／消去と同時に、記録媒体が記録しているタイトルキーを全て再暗号化しなければならないため、記録媒体内の記録タイトル数が膨大な数に及ぶ場合は、ＣＰＵへの負荷が大きくなり、処理速度が遅くなるなどの問題があった。

【０００９】

【発明が解決しようとする課題】

上記した従来の技術でタイトルの移動／消去を行う場合は、タイトルの移動／消去と同時に、記録媒体が記録しているタイトルキーを全て再暗号化しなければならないことから処理速度が遅くなるなどの問題があった。

【００１０】

この発明の目的は、内容的にまとまりのあるタイトルをその単位で取り扱いやすくするフォルダ（ディレクトリ）の導入によって、より効率的なタイトルの移動や消去を実現することにある。

【００１１】

【課題を解決するための手段】

上記した課題を解決するために、この発明の記録再生装置では、記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを他の記録媒体に移動するものにあって、前記移動するコンテンツが属さない全フォルダの暗号化フォルダキーを、不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって移動するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、前記移動するコンテンツが属するフォルダの暗号化フォルダキーを、前記不揮発性メモリに保持されているデバイスキーによって復号化し、移動するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって移動するコンテンツが属するフォルダ内のタイトルキーを再暗号化する手段と、前記新デバイスキーによって移動するコンテンツが属するフォルダのフォルダキーを再暗号化する手段とを具備することを特徴とする。

【００１２】
また、この発明の記録再生装置では、記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを消去するものにあって、前記消去するコンテンツが属さない全フォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって消去するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、前記消去するコンテンツが属するフォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、消去するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって消去するコンテンツが属するフォルダ内のタイトルキーを再暗号化する手段と、前記新デバイスキーによって消去するコンテンツが属するフォルダのフォルダキーを再暗号化する手段とを具備することを特徴とする。
【００１３】
【発明の実施の形態】
以下、この発明の実施の形態について、図面を参照しながら詳細に説明する。まず、この発明の実施の形態を説明する前に、フォルダ（ディレクトリ）とフォルダキーについて説明する。フォルダとは内容的にまとまり（関連）のあるタイトルをその単位で取り扱いやすくするために作成する管理領域である。フォルダキーとはフォルダ内に記録されている全てのタイトルのタイトルキーを暗号化／復号化するもので、各フォルダごとに異なる値を持っている。また、フォルダキーはデバイスキーによって暗号化／復号化される。
【００１４】
図１は、この発明における鍵の種類とその役割について説明するための説明図である。
タイトルキー（Ｋｔ）１３はコンテンツ（Ｃ）１１を暗号化／復号化するための鍵で、フォルダキー（Ｋｆ）１５はタイトルキー１３を暗号化／復号化するための鍵である。また、タイトルキー１３はコンテンツごとに異なり、フォルダキー１５はフォルダ内の全タイトルキー共通の鍵である。デバイスキー（Ｋｄ）１７はフォルダキー１５を暗号化して暗号化フォルダキー（Ｋｆｅ）１６を、フォルダキー１５はタイトルキー１３を暗号化して暗号化タイトルキー（Ｋｔｅ）１４を、タイトルキー１３はコンテンツ１１を暗号化して暗号化コンテンツ（Ｃｅ）１２をそれぞれ得る。
【００１５】
図２はフォルダを考慮した場合のコンテンツ記録例について説明するための説明図である。この例では、デバイスキーＫｄにより暗号化／復号化されたフォルダＡ～Ｃを有し、フォルダＡのフォルダキーＫｆ（Ａ）によりタイトル１～３のタイトルキーＫｔ（１）～（３）の暗号化／復号化を行い、タイトル１～３はタイトルキーＫｔ（１）～（３）によりそれぞれ暗号化／復号化が行われている。
【００１６】
フォルダＢ，Ｃについても同じように、それぞれのタイトルに対するタイトルキーによりそれぞれ暗号化／復号化が行われている。
図３は、この発明の一実施の形態について説明するための回路構成図である。図３において、入力インターフェース３１は記録再生装置３００の外部から供給される映像や音声などのコンテンツを受信し、信号の通路であるバス３３上に出力する。出力インターフェース３２はバス３３からコンテンツを受信し、記録再生装置３００の外部に送信する。
【００１７】
ＣＰＵ３４は演算処理や各ブロックの制御等を行う。暗号化／復号化処理部３５はデバイスキー発生部３５１、フォルダキー発生部３５２およびタイトルキー発生部３５３をそれぞれ有し、バス３３を介して供給されるコンテンツ、タイトルキーおよびフォルダキーの暗号化／復号化を行う。メモリ３６はＣＰＵ３４が動作上必要なデータの一時記憶等を行う。記録媒体３７はＤＶＤ等の光ディスク、磁気ディスク、光磁気ディスク、磁気テープ

、あるいは半導体メモリ等のディジタルデータ記録媒体を指す。

【００１８】

不揮発性メモリ３８は暗号化／復号化処理部３５が暗号化／復号化する際に必要となるデバイスキーＫｄの記憶等を行っている。外部記録媒体インターフェース３９は他の外部記録媒体とこの記録再生装置３００をつなぐインターフェースである。

【００１９】

以下、図３を用いながら記録再生装置で行われるフォルダ導入時におけるコンテンツの記録／再生／移動／消去の信号の流れについて図４～図８を用いて説明する。

（コンテンツ記録）

まず、フォルダ導入時におけるコンテンツの記録について、図４のフローチャートとともに説明する。

記録再生装置３００の外部から供給されるコンテンツＣを入力インターフェース３１が受信し、バス３３に出力する。そのコンテンツＣはバス３３を介してメモリ３６に一時記録され、その後、バス３３経由で暗号化／復号化処理部３５へ送られる。暗号化／復号化処理部３５内のタイトルキー発生部３５３によって乱数的に発生されたタイトルキーＫｔが送られてきたコンテンツＣを暗号化する（Ｓ４０１，Ｓ４０２）。記録先のフォルダを新規か既存か決定し（Ｓ４０３）、暗号化された暗号化コンテンツＣｅをバス３３経由でメモリ３６に一時記録した後、バス３３経由で記録媒体３７に記録する。以後、記録先のフォルダが新規か既存かにより処理方法が分かれる。

【００２０】

ステップＳ４０３において記録先が新規のフォルダと決定した場合は、ステップＳ４０２で暗号化された暗号化コンテンツを新規フォルダに記録する（Ｓ４０４）。暗号化／復号化処理部３５内のフォルダキー発生部３５２がフォルダキーＫｆを乱数的に発生させる（Ｓ４０５）。暗号化／復号化処理部３５はこのフォルダキーＫｆによって前記タイトルキーＫｔを暗号化する（Ｓ４０６）。暗号化された暗号化タイトルキーＫｔｅは、バス３３経由でメモリ３６に一時記録された後、バス３３経由で記録媒体３７に記録される（Ｓ４０７）。

【００２１】

さらに、不揮発性メモリ３８からデバイスキーＫｄをバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ４０８）。暗号化／復号化処理部３５はこのデバイスキーＫｄによって前記フォルダキーＫｆを暗号化する（Ｓ４０９）。暗号化された暗号化フォルダキーＫｆｅはバス３３経由でメモリ３６に一時記録された後、バス３３経由で記録媒体３７に記録される（Ｓ４１０）。以上で記録処理を終了する。

【００２２】

ステップＳ４０３において記録先が既存のフォルダと決定した場合は、ステップＳ４０２で暗号化された暗号化コンテンツを既存フォルダに記録する（Ｓ４１１）。記録媒体３７から記録先フォルダの暗号化フォルダキーＫｆｅをバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ４１２）。

【００２３】

また、不揮発性メモリ３８からデバイスキーＫｄをバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ４１３）。暗号化／復号化処理部３５はデバイスキーＫｄによって暗号化フォルダキーＫｆｅを復号化する（Ｓ４１４）。復号化されたフォルダキーＫｆは前記タイトルキーＫｔを暗号化し（Ｓ４１５）、暗号化された暗号化タイトルキーＫｔｅはバス３３経由でメモリ３６に一時記録された後、バス３３経由で記録媒体３７に記録される（Ｓ４１６）。

【００２４】

さらに、デバイスキーＫｄがフォルダキーＫｆを暗号化し（Ｓ４１７）、ステップＳ４１４で暗号化された暗号化フォルダキーＫｆｅはバス３３経由でメモリ３６に一時記録された後、バス３３経由で記録媒体３７に記録される（Ｓ４１８）。以上で記録処理を終了す

る。
【００２５】
（コンテンツ再生）
次にフォルダ導入時におけるコンテンツの再生処理について、図５のフローチャートとともに説明する。
不揮発性メモリ３８からデバイスキーＫｄをバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ５０１）。また、記録媒体３７から再生したいコンテンツが記録されているフォルダの暗号化フォルダキーＫｆｅをバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ５０２）。暗号化／復号化処理部３５はデバイスキーＫｄによって暗号化フォルダキーＫｆｅを復号化する（Ｓ５０３）。
【００２６】
次に、記録媒体３７から再生したいコンテンツの暗号化タイトルキーＫｔｅをバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ５０４）。暗号化／復号化処理部３５は、前述で復号化されたフォルダキーＫｆによって暗号化タイトルキーＫｔｅを復号化する（Ｓ５０５）。
【００２７】
最後に、記録媒体３７から再生したいコンテンツの暗号化コンテンツＣｅをバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ５０６）。暗号化／復号化処理部３５は、前述で復号化されたタイトルキーＫｔによって暗号化コンテンツＣｅを復号化する（Ｓ５０７）。復号化されたコンテンツＣはバス３３経由でメモリ３６に一時記録された後、バス３３から出力インターフェース３２を経由して外部へ送信される（Ｓ５０９）。以上で再生処理を終了する。
【００２８】
フォルダ導入時におけるコンテンツの移動について説明する。図６は記録再生装置の記録媒体がフォルダ１～ｎを記録しており、その内の任意のフォルダｙ６０１が内容的にまとまりのある複数のコンテンツをタイトル１～ｍのタイトルで記録している状態図である。このとき、フォルダｙ６０１内の任意のタイトルｘ６０２を他の記録媒体に移動する例を考える。
【００２９】
（タイトル移動）
このタイトル移動のプロセスについて、図７のフローチャートとともに説明する。
まず、移動したいタイトルｘを、記録媒体３７からバス３３経由でメモリ３６に一時記録した後、バス３３から外部記録媒体インターフェース３９を介し、暗号化した状態で移動先メディアにコピーする（Ｓ７０１）。この段階では、復号キーをコピーしないので、移動先のタイトルｘは利用できない。
【００３０】
デバイスキーＫｄを不揮発性メモリ３８からバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ７０２）。また、フォルダｙ以外の全ての暗号化フォルダキーＫｆｅ（１～ｎ）、フォルダｙの暗号化フォルダキーＫｆｅ（ｙ）、およびタイトルｘが属するフォルダｙ内の全ての暗号化タイトルキーＫｔｅ（１～ｍ）を記録媒体３７からバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ７０３）。
【００３１】
暗号化／復号化処理部３５はデバイスキーＫｄを使って、フォルダｙを除く暗号化フォルダキーＫｆｅ（１～ｎ）からフォルダキーＫｆ（１～ｎ）を復号する。同様に、デバイスキーＫｄを使って、フォルダｙの暗号化フォルダキーＫｆｅ（ｙ）からフォルダキーＫｆ（ｙ）を復号する（Ｓ７０４）。
【００３２】
暗号化／復号化処理部３５は３で得られたフォルダｙのフォルダキーＫｆ（ｙ）を使って

、フォルダｙ内の暗号化タイトルキーＫｔｅ（１～ｍ）からタイトルキーＫｔ（１～ｍ）を復号する（Ｓ７０５）。

【００３３】

暗号化／復号化処理部３５はフォルダキー発生部３５２によってフォルダｙの新しいフォルダキーＫｆ（ｙ）（ｎｅｗ）を乱数的に発生させる（Ｓ７０６）。暗号化／復号化処理部３５は5で得られた新フォルダキーＫｆ（ｙ）（ｎｅｗ）を使って、タイトルｘを除くフォルダｙ内のタイトルキーＫｔ（１～ｍ）を暗号化する（Ｓ７０７）。

【００３４】

暗号化／復号化処理部３５はデバイスキー発生部３５１によって新しいデバイスキーＫｄ（ｎｅｗ）を乱数的に発生させる（Ｓ７０８）。

暗号化／復号化処理部３５は7で得られた新デバイスキーＫｄ（ｎｅｗ）を使って、フォルダｙを除くフォルダキーＫｆ（１～ｎ）を暗号化する。同様に、新デバイスキーＫｄ（ｎｅｗ）を使って、フォルダｙの新フォルダキーＫｆ（ｙ）（ｎｅｗ）を暗号化する（Ｓ７０９）。

【００３５】

ステップＳ７０７で再暗号化したタイトルｘを除く新暗号化タイトルキーＫｔｅ（１～ｍ）（ｎｅｗ）と、ステップ７０９で再暗号化したフォルダｙを除く新暗号化フォルダキーＫｆｅ（１～ｎ）（ｎｅｗ）、さらに、ステップＳ７０６のプロセスで新たに発生し、ステップＳ７０７で暗号化したフォルダｙの新暗号化フォルダキーＫｆｅ（ｙ）（ｎｅｗ）をバス３３経由でメモリ３６に一時記録した後、バス３３経由で記録媒体３７に記録する（Ｓ７１０）。

【００３６】

ステップＳ７０８で発生した新デバイスキーＫｄ（ｎｅｗ）をバス３３経由でメモリ３６に一時記録した後、バス３３経由で不揮発性メモリ３８に記録する（Ｓ７１１）。

【００３７】

ステップＳ７０５で復号化したタイトルｘのタイトルキーＫｔ（ｘ）をバス３３経由でメモリ３６に一時記録した後、バス３３から外部記録媒体インターフェース３９を介し、移動先メディアに伝送する。この伝送方式は移動先メディアとの取り決めに従う（Ｓ７１２）。

【００３８】

新しいキーの発生により不要になったデバイスキーＫｄ、フォルダｙのフォルダキーＫｆｅ（ｙ）、およびタイトルｘのタイトルキーＫｔ（ｘ）とタイトルｘを消去する１～１０の途中で処理が中止された場合には、移動は行われずに終わる。１１～１２の途中で処理が中止された場合には、移動タイトルが消失する（Ｓ７１３）。これにより、タイトルｘの移動が実現する。

【００３９】

このプロセスにより、バックアップされていたタイトルｘを移動後の主記録媒体のフォルダｙに戻しても、フォルダｙのフォルダキーが更新されているためバックアップのタイトルｘは復号化できない。さらに、タイトルｘを復号するためのフォルダキーが同時にバックアップされていても、デバイスキーが更新されているためそのフォルダキーを復号することができず、結局タイトルｘは復号化できない。

【００４０】

次に、フォルダ導入時におけるコンテンツの消去について説明する。図６で示した任意のフォルダｙ６０１内の任意のタイトルｘ６０２を消去する例を考える。

（タイトル消去）

このタイトル消去のプロセスについて、図８のフローチャートとともに説明する。

デバイスキーＫｄを不揮発性メモリ３８からバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ８０１）。また、フォルダｙ以外の全ての暗号化フォルダキーＫｆｅ（１～ｎ）、フォルダｙの暗号化フォルダキーＫｆｅ（ｙ）、およびタイトルｘが属するフォルダｙ内の全ての暗号化タイトルキーＫｔｅ

（１～ｍ）を、記録媒体３７からバス３３経由でメモリ３６に一時記録した後、バス３３経由で暗号化／復号化処理部３５へ読み出す（Ｓ８０２）。

【００４１】

暗号化／復号化処理部３５はデバイスキーＫｄを使って、フォルダｙを除く暗号化フォルダキーＫｆｅ（１～ｎ）からフォルダキーＫｆ（１～ｎ）を復号する。同様に、デバイスキーＫｄを使って、フォルダｙの暗号化フォルダキーＫｆｅ（ｙ）からフォルダキーＫｆ（ｙ）を復号する（Ｓ８０３）。

【００４２】

暗号化／復号化処理部３５はステップＳ８０２で得られたフォルダｙのフォルダキーＫｆ（ｙ）を使って、フォルダｙ内の暗号化タイトルキーＫｔｅ（１～ｍ）からタイトルキーＫｔ（１～ｍ）を復号する（Ｓ８０４）。

【００４３】

暗号化／復号化処理部３５はフォルダキー発生部３５２によってフォルダｙの新しいフォルダキーＫｆ（ｙ）（ｎｅｗ）を乱数的に発生する（Ｓ８０５）。

暗号化／復号化処理部３５はステップ８０５で得られた新フォルダキーＫｆ（ｙ）（ｎｅｗ）を使って、タイトルｘを除くフォルダｙ内のタイトルキーＫｔ（１～ｍ）を暗号化する（Ｓ８０６）。

【００４４】

暗号化／復号化処理部３５はデバイスキー発生部３５１によって新しいデバイスキーＫｄ（ｎｅｗ）を乱数的に発生する（Ｓ８０７）。

暗号化／復号化処理部３５はステップ８０７で得られた新デバイスキーＫｄ（ｎｅｗ）を使って、フォルダｙを除くフォルダキーＫｆ（１～ｎ）を暗号化する。同様に、新デバイスキーＫｄ（ｎｅｗ）を使って、フォルダｙの新フォルダキーＫｆ（ｙ）（ｎｅｗ）を暗号化する（Ｓ８０８）。

【００４５】

ステップＳ８０６において再暗号化されたタイトルｘを除く新暗号化タイトルキーＫｔｅ（１～ｍ）（ｎｅｗ）、ステップ８０７のプロセスで再暗号化されたフォルダｙを除く新暗号化フォルダキーＫｆｅ（１～ｎ）（ｎｅｗ）、さらにステップＳ８０５において新たに発生し、ステップＳ８０８で暗号化されたフォルダｙの新暗号化フォルダキーＫｆｅ（ｙ）（ｎｅｗ）をそれぞれバス３３経由でメモリ３６に一時記録した後、バス３３経由で記録媒体３７に記録する（Ｓ８０９）。

【００４６】

ステップＳ８０７において発生した新デバイスキーＫｄ（ｎｅｗ）をバス３３経由でメモリ３６に一時記録した後、バス３３経由で不揮発性メモリ３８に記録する（Ｓ８１０）。

【００４７】

新しいキーの発生により不要になったデバイスキーＫｄ、フォルダｙのフォルダキーＫｆｅ（ｙ）を消去する（Ｓ８１１）。

タイトルｘのタイトルキーＫｔ（ｘ）、およびタイトルｘを消去する。以上のプロセスでタイトルｘの消去が実現する（Ｓ８１２）。

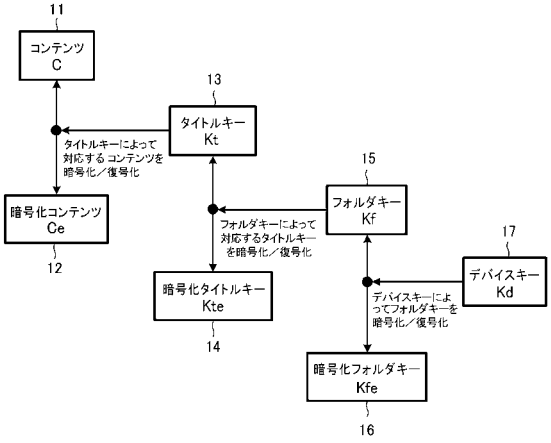
このプロセスにより、バックアップされていたタイトルｘを移動後の主記録媒体のフォルダｙに戻しても、フォルダｙのフォルダキーが更新されているためバックアップのタイトルｘは復号化できない。さらに、タイトルｘを復号するためのフォルダキーが同時にバックアップされていても、デバイスキーが更新されているためそのフォルダキーを復号することができず、結局タイトルｘは復号化できない。

【００４８】

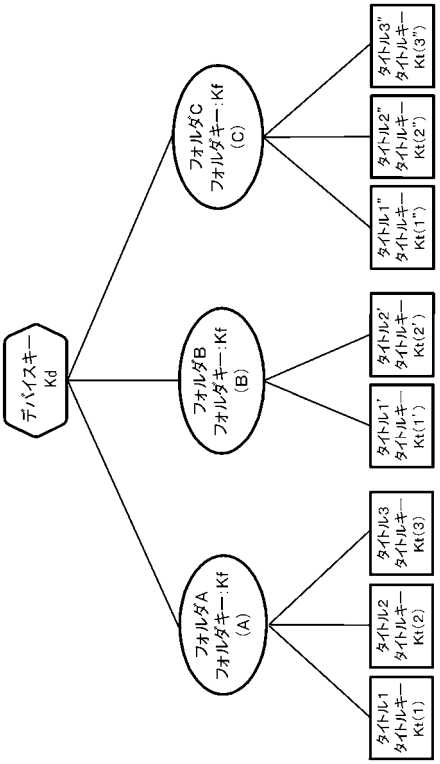
以上説明したように、フォルダおよびフォルダキーを導入したタイトル移動あるいは消去では、移動あるいは消去したいタイトルが属するフォルダに関してはそのフォルダキーとそのフォルダ内にある全タイトルキーを再暗号化するが、移動／消去したいタイトルが属さない残りのフォルダに関してはそのフォルダキーのみを再暗号化するだけの処理となる。

【００４９】
これより、記録媒体内の記録タイトル数が膨大な数に及ぶ場合でも、全てのタイトルキーを再暗号化する必要がなくなるため、処理時間の大幅な改善が見込まれる。また、著作権を侵害することなく記録されたコンテンツを移動／消去することができる。
【００５０】
この発明は、上記した実施の形態に限定されるものではなく、たとえば記録媒体３７を記録再生装置３００は、この記録再生装置３００に着脱可能な構成のものであってもよい。
【００５１】
【発明の効果】
以上説明したように、この発明の記録再生装置によれば、内容的にまとまりのあるタイトルを、その単位で取り扱いやすくするフォルダの導入によって、タイトルの移動／消去をより効率的に行うことが可能となる。
【図面の簡単な説明】
【図１】この発明における鍵の種類とその役割について説明するための説明図。
【図２】この発明のフォルダを考慮した場合のコンテンツ記録例について説明するための説明図。
【図３】この発明の一実施の形態について説明するための回路構成図。
【図４】この発明のフォルダ導入時におけるコンテンツの記録について説明するためのフローチャート。
【図５】この発明のフォルダ導入時におけるコンテンツの再生処理について説明するためのフローチャート。
【図６】この発明のフォルダ導入時におけるコンテンツの移動について説明するための説明図。
【図７】この発明のタイトルの移動プロセスについて説明するためのフローチャート。
【図８】この発明のタイトルの消去プロセスについて説明するためのフローチャート。
【図９】従来の記録再生装置における鍵の種類とその役割について説明するための説明図。
【図１０】従来の課題について説明するための説明図。
【符号の説明】
１１・・・コンテンツ（Ｃ）
１２・・・暗号化コンテンツ（Ｃｅ）
１３・・・タイトルキー（Ｋｔ）
１４・・・暗号化タイトルキー（Ｋｔｅ）
１５・・・フォルダキー（Ｋｆ）
１６・・・暗号化フォルダキー（Ｋｆｅ）
１７・・・デバイスキー（Ｋｄ）

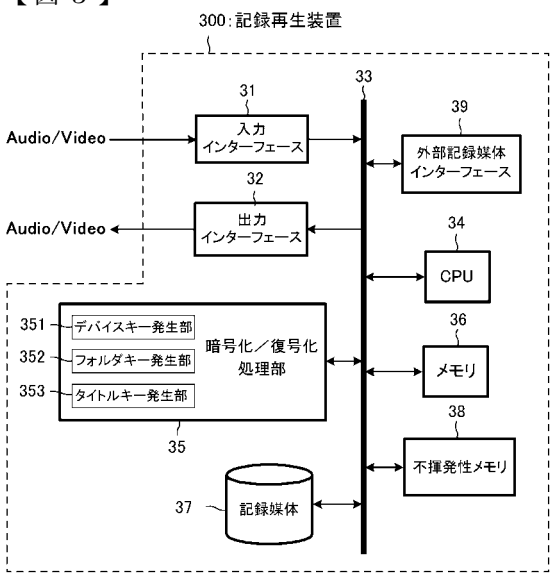
【図１】


11
コンテンツ C
13
タイトルキー Kt
タイトルキーによって対応するコンテンツを暗号化／復号化
15
フォルダキー Kf
暗号化コンテンツ Ce
12
フォルダキーによって対応するタイトルキーを暗号化／復号化
17
デバイスキー Kd
暗号化タイトルキー Kte
14
デバイスキーによってフォルダキーを暗号化／復号化
暗号化フォルダキー Kfe
16

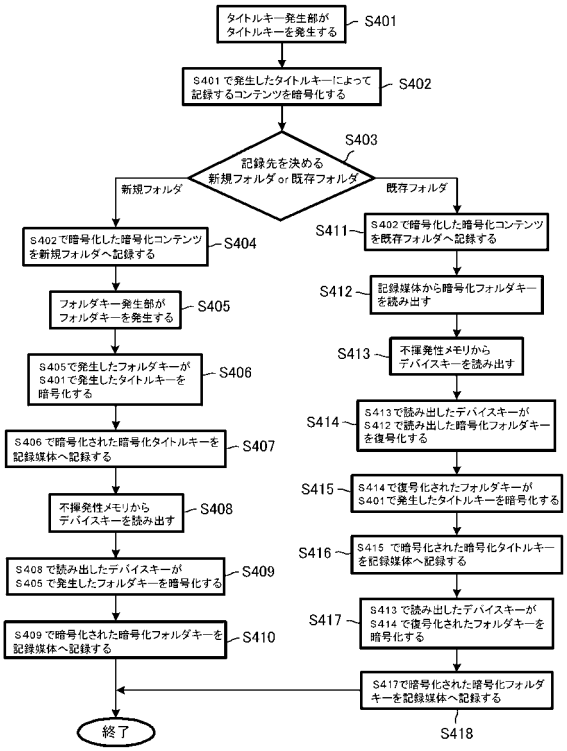
【図２】


デバイスキー Kd
フォルダA フォルダキー：Kf (A)
フォルダB フォルダキー：Kf (B)
フォルダC フォルダキー：Kf (C)
タイトル1 タイトルキー Kt(1)
タイトル2 タイトルキー Kt(2)
タイトル3 タイトルキー Kt(3)
タイトル1' タイトルキー Kt(1')
タイトル2' タイトルキー Kt(2')
タイトル3' タイトルキー Kt(3')
タイトル1" タイトルキー Kt(1")
タイトル2" タイトルキー Kt(2")
タイトル3" タイトルキー Kt(3")

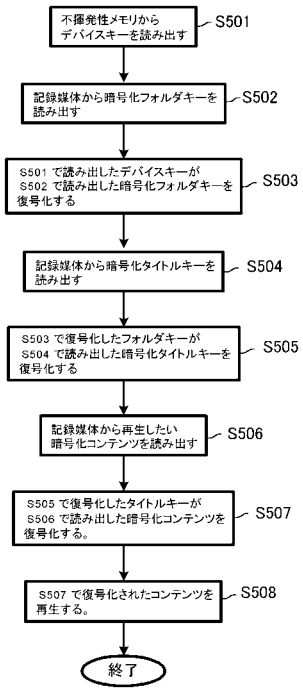
【図３】


300：記録再生装置
31
入力インターフェース
Audio/Video
32
出力インターフェース
Audio/Video
33
39
外部記録媒体インターフェース
34
CPU
36
メモリ
38
不揮発性メモリ
351 デバイスキー発生部
352 フォルダキー発生部
353 タイトルキー発生部
暗号化／復号化処理部
35
37
記録媒体

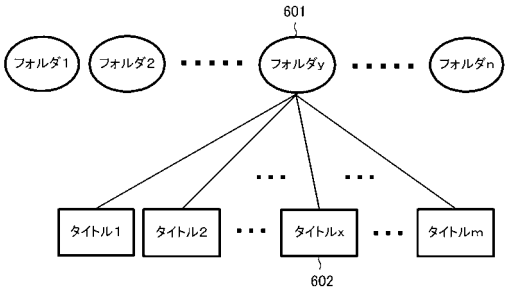
【図４】


タイトルキー発生部がタイトルキーを発生する
S401
S401で発生したタイトルキーによって記録するコンテンツを暗号化する
S402
記録先を決める 新規フォルダ or 既存フォルダ
S403
新規フォルダ
既存フォルダ
S402で暗号化した暗号化コンテンツを新規フォルダへ記録する
S404
フォルダキー発生部がフォルダキーを発生する
S405
S405で発生したフォルダキーがS401で発生したタイトルキーを暗号化する
S406
S406で暗号化された暗号化タイトルキーを記録媒体へ記録する
S407
不揮発性メモリからデバイスキーを読み出す
S408
S408で読み出したデバイスキーがS405で発生したフォルダキーを暗号化する
S409
S409で暗号化された暗号化フォルダキーを記録媒体へ記録する
S410
終了
S411
S402で暗号化した暗号化コンテンツを既存フォルダへ記録する
S412
記録媒体から暗号化フォルダキーを読み出す
S413
不揮発性メモリからデバイスキーを読み出す
S414
S413で読み出したデバイスキーがS412で読み出した暗号化フォルダキーを復号化する
S415
S414で復号化されたフォルダキーがS401で発生したタイトルキーを暗号化する
S416
S415で暗号化された暗号化タイトルキーを記録媒体へ記録する
S417
S413で読み出したデバイスキーがS414で復号化されたフォルダキーを暗号化する
S417で暗号化された暗号化フォルダキーを記録媒体へ記録する
S418

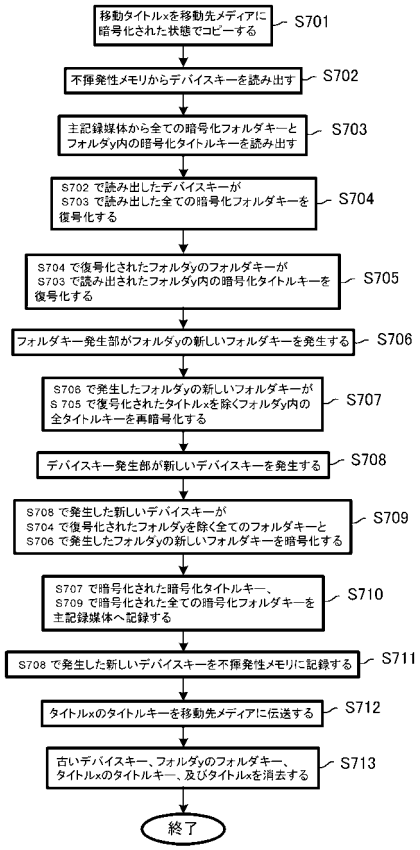
【図５】


不揮発性メモリから
デバイスキーを読み出す
S501
記録媒体から暗号化フォルダキーを
読み出す
S502
S501 で読み出したデバイスキーが
S502 で読み出した暗号化フォルダキーを
復号化する
S503
記録媒体から暗号化タイトルキーを
読み出す
S504
S503 で復号化したフォルダキーが
S504 で読み出した暗号化タイトルキーを
復号化する
S505
記録媒体から再生したい
暗号化コンテンツを読み出す
S506
S505 で復号化したタイトルキーが
S506 で読み出した暗号化コンテンツを
復号化する。
S507
S507 で復号化されたコンテンツを
再生する。
S508
終了

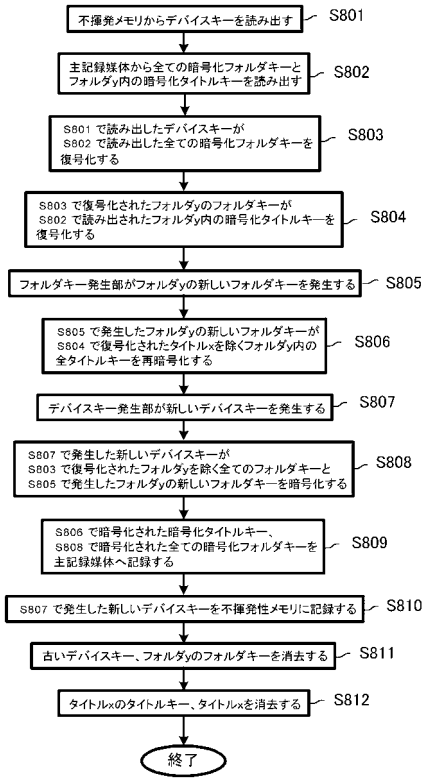
【図６】


601
フォルダ1
フォルダ2
フォルダy
フォルダn
タイトル1
タイトル2
タイトルx
タイトルm
602

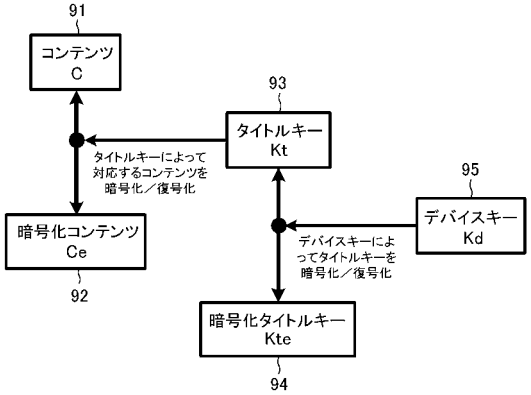
【図７】


移動タイトルxを移動先メディアに
暗号化された状態でコピーする
S701
不揮発性メモリからデバイスキーを読み出す
S702
主記録媒体から全ての暗号化フォルダキーと
フォルダy内の暗号化タイトルキーを読み出す
S703
S702 で読み出したデバイスキーが
S703 で読み出した全ての暗号化フォルダキーを
復号化する
S704
S704 で復号化されたフォルダyのフォルダキーが
S703 で読み出されたフォルダy内の暗号化タイトルキーを
復号化する
S705
フォルダキー発生部がフォルダyの新しいフォルダキーを発生する
S706
S706 で発生したフォルダyの新しいフォルダキーが
S 705 で復号化されたタイトルxを除くフォルダy内の
全タイトルキーを再暗号化する
S707
デバイスキー発生部が新しいデバイスキーを発生する
S708
S708 で発生した新しいデバイスキーが
S704 で復号化されたフォルダyを除く全てのフォルダキーと
S706 で発生したフォルダyの新しいフォルダキーを暗号化する
S709
S707 で暗号化された暗号化タイトルキー、
S709 で暗号化された全ての暗号化フォルダキーを
主記録媒体へ記録する
S710
S708 で発生した新しいデバイスキーを不揮発性メモリに記録する
S711
タイトルxのタイトルキーを移動先メディアに伝送する
S712
古いデバイスキー、フォルダyのフォルダキー、
タイトルxのタイトルキー、及びタイトルxを消去する
S713
終了

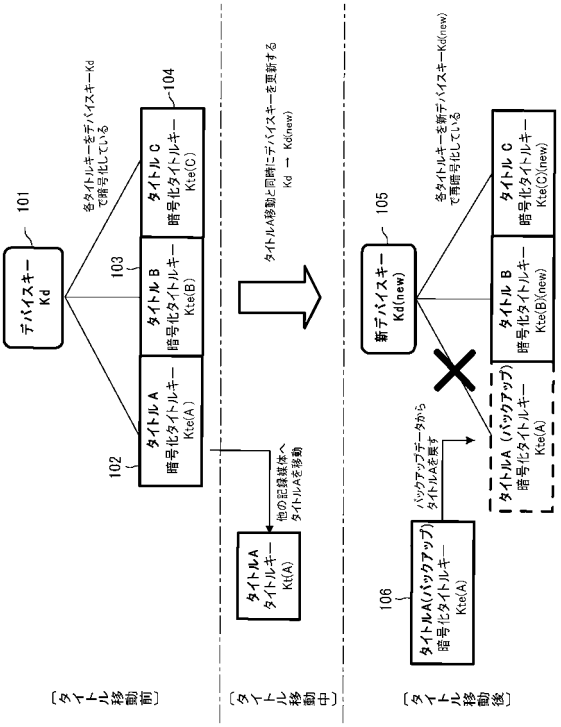
【図８】


不揮発メモリからデバイスキーを読み出す
S801
主記録媒体から全ての暗号化フォルダキーと
フォルダy内の暗号化タイトルキーを読み出す
S802
S801 で読み出したデバイスキーが
S802 で読み出した全ての暗号化フォルダキーを
復号化する
S803
S803 で復号化されたフォルダyのフォルダキーが
S802 で読み出されたフォルダy内の暗号化タイトルキーを
復号化する
S804
フォルダキー発生部がフォルダyの新しいフォルダキーを発生する
S805
S805 で発生したフォルダyの新しいフォルダキーが
S804 で復号化されたタイトルxを除くフォルダy内の
全タイトルキーを再暗号化する
S806
デバイスキー発生部が新しいデバイスキーを発生する
S807
S807 で発生した新しいデバイスキーが
S803 で復号化されたフォルダyを除く全てのフォルダキーと
S805 で発生したフォルダyの新しいフォルダキーを暗号化する
S808
S806 で暗号化された暗号化タイトルキー、
S808 で暗号化された全ての暗号化フォルダキーを
主記録媒体へ記録する
S809
S807 で発生した新しいデバイスキーを不揮発性メモリに記録する
S810
古いデバイスキー、フォルダyのフォルダキーを消去する
S811
タイトルxのタイトルキー、タイトルxを消去する
S812
終了

【図９】



【図１０】



【手続補正書】
【提出日】平成14年9月30日(2002.9.30)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを他の記録媒体に移動する記録再生装置において、
予め移動するコンテンツを、移動先のメディアに暗号化したまま移動する手段と、
前記移動するコンテンツが属するフォルダを含む全フォルダの暗号化フォルダキーを、不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって移動するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、
前記移動するコンテンツが属するフォルダの暗号化フォルダキーを、前記不揮発性メモリに保持されているデバイスキーによって復号化し、移動するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって移動するコンテンツが属するフォルダ内のタイトルキーを再暗号化し、前記新デバイスキーによって移動するコンテンツが属するフォルダの該新フォルダキーを暗号化する手段と、
前記移動先のメディアに移動されたコンテンツを解く前記タイトルキーを、前記メディアに移動する手段とを具備したことを特徴とする記録再生装置。

【請求項２】
記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを消去する記録再生装置において、
前記消去するコンテンツが属さない全フォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって消去するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、
前記消去するコンテンツが属するフォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、消去するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって消去するコンテンツが属するフォルダ内のタイトルキーを再暗号化し、前記新デバイスキーによって消去するコンテンツが属する前記新フォルダのフォルダキーを再暗号化する手段とを具備したことを特徴とする記録再生装置。
【請求項３】
前記デバイスキーは記録再生装置内の不揮発性メモリに保持され、各記録再生装置ごとに異なる値を持つことを特徴とする請求項１または２記載の記録再生装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
【課題を解決するための手段】
上記した課題を解決するために、この発明の記録再生装置では、記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを他の記録媒体に移動するものにあって、予め移動するコンテンツを、移動先のメディアに暗号化したまま移動する手段と、前記移動するコンテンツが属するフォルダを含む全フォルダの暗号化フォルダキーを、不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって移動するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、前記移動するコンテンツが属するフォルダの暗号化フォルダキーを、前記不揮発性メモリに保持されているデバイスキーによって復号化し、移動するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって移動するコンテンツが属するフォルダ内のタイトルキーを再暗号化し、前記新デバイスキーによって移動するコンテンツが属するフォルダの該新フォルダキーを暗号化する手段と、前記移動先のメディアに移動されたコンテンツを解く前記タイトルキーを、前記メディアに移動する手段とを具備したことを特徴とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
また、この発明の記録再生装置では、記録媒体に映像や音声などのコンテンツを暗号化して記録し、暗号化されたコンテンツを復号化する機能を有し、前記記録媒体に記録されている任意のフォルダ内の任意のコンテンツを消去するものにあって、前記消去するコンテ

ンツが属さない全フォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、新たなデバイスキーをデバイスキー発生部により乱数的に発生させ、該新デバイスキーによって消去するコンテンツが属さない全フォルダのフォルダキーを再暗号化する手段と、前記消去するコンテンツが属するフォルダの暗号化フォルダキーを不揮発性メモリに保持されているデバイスキーによって復号化し、消去するコンテンツが属するフォルダ内の暗号化タイトルキーをフォルダキーによって復号化し、新たなフォルダキーをフォルダキー発生部により乱数的に発生させ、該新フォルダキーによって消去するコンテンツが属するフォルダ内のタイトルキーを再暗号化し、前記新デバイスキーによって消去するコンテンツが属する前記新フォルダのフォルダキーを再暗号化する手段とを具備したことを特徴とする。

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	Ｈ０４Ｎ	5/91 Ｐ	
	Ｈ０４Ｌ	9/00 ６２１Ａ	

Ｆターム(参考) 5B082 EA11 GA11
5C053 FA13 FA15 JA21
5D044 AB05 AB07 BC01 BC04 BC06 CC03 CC04 DE50 GK17 HL08
5J104 AA12 AA13 PA14