(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2010-220019
(P2010-220019A)
(43)公開日　平成22年9月30日(2010.9.30)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 19　ＯＬ　（全 14 頁）

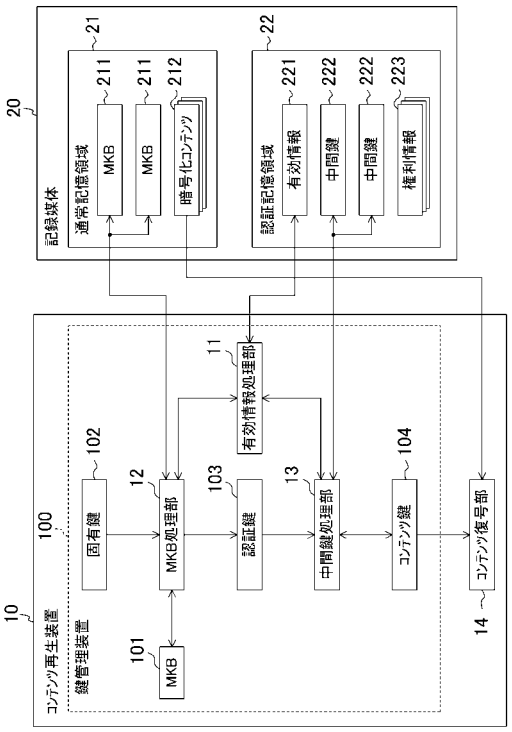
(21)出願番号　特願2009-66113(P2009-66113)
(22)出願日　平成21年3月18日(2009.3.18)

(71)出願人　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100077931
弁理士　前田　弘
(74)代理人　100110939
弁理士　竹内　宏
(74)代理人　100110940
弁理士　嶋田　高久
(74)代理人　100113262
弁理士　竹内　祐二
(74)代理人　100115059
弁理士　今江　克実
(74)代理人　100115691
弁理士　藤田　篤史

最終頁に続く

(54)【発明の名称】鍵管理方法および鍵管理装置

(57)【要約】
【課題】記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを安全・確実に更新する。
【解決手段】有効情報処理部（１１）は、記録媒体（２０）における有効情報（２２１）を参照して有効なＭＫＢ（２１１）および中間鍵（２２２）を判定するとともに、有効でないＭＫＢ（２１１）および中間鍵（２２２）が書き換えられたとき有効情報（２２１）を書き換える。ＭＫＢ処理部（１２）は、有効なＭＫＢ（２１１）を読み出してＭＫＢ（１０１）の更新処理を行うとともに、有効でないＭＫＢ（２１１）を書き換える。中間鍵処理部（１３）は、有効な中間鍵（２２２）を読み出して認証鍵（１０３）で復号および再暗号化するとともに、有効でない中間鍵（２２２）を再暗号化した中間鍵に書き換える。
【選択図】図１



【特許請求の範囲】
【請求項１】
記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理装置であって、
前記記録媒体に、ＭＫＢおよび中間鍵がそれぞれ二つずつ保存されており、かつ、そのいずれが有効であるかを示す有効情報が保存されているとき、前記有効情報を参照して前記保存されているＭＫＢおよび中間鍵のそれぞれについて有効なものを判定するステップと、
有効であると判定されなかったＭＫＢおよび中間鍵を新たなＭＫＢおよび中間鍵に書き換えるステップと、
ＭＫＢおよび中間鍵の書き換え後に、前記有効情報を、当該書き換えられたＭＫＢおよび中間鍵が有効であることを示す内容に書き換えるステップとを備えている
ことを特徴とする鍵管理方法。
【請求項２】
前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むステップと、
有効情報の書き込み後に、前記記録媒体に保存されているＭＫＢおよび中間鍵をそのまま残して新たなＭＫＢおよび中間鍵を前記記録媒体に書き込むステップと、
ＭＫＢおよび中間鍵の書き込み後に、前記有効情報を、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す内容に書き換えるステップとを備えている
ことを特徴とする請求項１の鍵管理方法。
【請求項３】
前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵をそのまま残して新たなＭＫＢおよび中間鍵を前記記録媒体に書き込むステップと、
ＭＫＢおよび中間鍵の書き込み後に、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むステップとを備えている
ことを特徴とする請求項１の鍵管理方法。
【請求項４】
ＭＫＢ、中間鍵、および有効情報の書き換えが前記記録媒体への一連のアクセスとして一気に行われる
ことを特徴とする請求項１の鍵管理方法。
【請求項５】
ＭＫＢおよび中間鍵の書き込みおよび有効情報の書き換えが前記記録媒体への一連のアクセスとして一気に行われる
ことを特徴とする請求項２の鍵管理方法。
【請求項６】
ＭＫＢ、中間鍵、および有効情報の書き込みが前記記録媒体への一連のアクセスとして一気に行われる
ことを特徴とする請求項３の鍵管理方法。
【請求項７】
ＭＫＢの書き換え後に、当該書き換えられたＭＫＢを検証するステップを備えている
ことを特徴とする請求項１の鍵管理方法。
【請求項８】
ＭＫＢの書き込み後に、当該書き込まれたＭＫＢを検証するステップを備えている
ことを特徴とする請求項２および３のいずれか一つの鍵管理方法。
【請求項９】
有効情報の書き換え後に、当該書き換えられた有効情報によって有効でないと示されているＭＫＢおよび中間鍵を前記記録媒体から削除するステップを備えている

ことを特徴とする請求項１および２のいずれか一つの鍵管理方法。
【請求項１０】
　有効情報の書き込み後に、当該書き込まれた有効情報によって有効でないと示されているＭＫＢおよび中間鍵を前記記録媒体から削除するステップを備えている
ことを特徴とする請求項３の鍵管理方法。
【請求項１１】
記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理方法であって、
　前記記録媒体に保存されているＭＫＢを前記記録媒体に複製するステップと、
　ＭＫＢの複製後に、複製元のＭＫＢを新たなＭＫＢに書き換えるステップと、
　前記記録媒体に保存されている中間鍵を前記記録媒体に複製するステップと、
　中間鍵の複製後に、複製元の中間鍵を新たな中間鍵に書き換えるステップとを備えている
ことを特徴とする鍵管理方法。
【請求項１２】
　ＭＫＢおよび中間鍵の書き換えが前記記録媒体への一連のアクセスとして一気に行われる
ことを特徴とする請求項１１の鍵管理方法。
【請求項１３】
　ＭＫＢの書き込み後に、当該書き込まれたＭＫＢを検証するステップを備えている
ことを特徴とする請求項１１の鍵管理方法。
【請求項１４】
　ＭＫＢの書き換え後に、複製されたＭＫＢを前記記録媒体から削除するステップと、
　中間鍵の書き換え後に、複製された中間鍵を前記記録媒体から削除するステップとを備えている
ことを特徴とする請求項１１の鍵管理方法。
【請求項１５】
記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理装置であって、
　前記記録媒体に、ＭＫＢおよび中間鍵がそれぞれ二つずつ保存されており、かつ、そのいずれが有効であるかを示す有効情報が保存されているとき、前記有効情報を参照して前記保存されているＭＫＢおよび中間鍵のそれぞれについて有効なものを判定するとともに、有効であると判定しなかったＭＫＢおよび中間鍵が書き換えられたとき、前記有効情報を、当該書き換えられたＭＫＢおよび中間鍵が有効であることを示す内容に書き換える有効情報処理部と、
　有効であると判定されたＭＫＢを読み出して当該鍵管理装置に保存されているＭＫＢの更新処理を行い、前記認証鍵を生成するとともに、有効であると判定されなかったＭＫＢを前記更新したＭＫＢに書き換えるＭＫＢ処理部と、
　有効であると判定された中間鍵を読み出して前記認証鍵で復号および再暗号化するとともに、有効であると判定されなかった中間鍵を前記再暗号化した中間鍵に書き換える中間鍵処理部とを備えている
ことを特徴とする鍵管理装置。
【請求項１６】
請求項１５の鍵管理装置において、
　前記有効情報処理部は、前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むとともに、前記記録媒体に別のＭＫＢおよび中間鍵が書き込まれたとき、前記有効情報を、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す内容に書き換えるものであり、
　前記ＭＫＢ処理部は、前記記録媒体に保存されているＭＫＢをそのまま残して前記更新

したＭＫＢを前記記録媒体に書き込むものであり、
　前記中間鍵処理部は、前記記録媒体に保存されている中間鍵をそのまま残して前記再暗号化した中間鍵を前記記録媒体に書き込むものである
ことを特徴とする鍵管理装置。
【請求項１７】
請求項１５の鍵管理装置において、
　前記有効情報処理部は、前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵が有効であると判定するとともに、前記記録媒体に別のＭＫＢおよび中間鍵が書き込まれたとき、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むものであり、
　前記ＭＫＢ処理部は、前記記録媒体に保存されているＭＫＢをそのまま残して前記更新したＭＫＢを前記記録媒体に書き込むものであり、
　前記中間鍵処理部は、前記記録媒体に保存されている中間鍵をそのまま残して前記再暗号化した中間鍵を前記記録媒体に書き込むものである
ことを特徴とする鍵管理装置。
【請求項１８】
記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理装置であって、
　前記記録媒体に保存されているＭＫＢを読み出して当該鍵管理装置に保存されているＭＫＢの更新処理を行い、前記認証鍵を生成するとともに、前記記録媒体に保存されているＭＫＢを前記記録媒体に複製し、複製元のＭＫＢを前記更新したＭＫＢに書き換えるＭＫＢ処理部と、
　前記記録媒体に保存されている中間鍵を読み出して前記認証鍵で復号および再暗号化するとともに、前記記録媒体に保存されている中間鍵を前記記録媒体に複製し、複製元の中間鍵を前記再暗号化した中間鍵に書き換える中間鍵処理部とを備えている
ことを特徴とする鍵管理装置。
【請求項１９】
記録媒体に保存されている暗号化コンテンツを再生するコンテンツ再生装置であって、
　請求項１５および１８のいずれか一つの鍵管理装置と、
　前記記録媒体から前記暗号化コンテンツを読み出し、前記鍵管理装置における前記中間鍵処理部によって復号された中間鍵またはさらに当該中間鍵で復号したコンテンツ鍵で前記読み出した暗号化コンテンツを復号するコンテンツ復号部とを備えている
ことを特徴とするコンテンツ再生装置。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、記録媒体における鍵情報の管理、特に、鍵情報の更新に関する。
【背景技術】
【０００２】
　近年、コンテンツの著作権保護の必要性が高まり、地上波デジタル放送やインターネットなどでは鍵や権利情報を含んだコンテンツの放送や配信が行われるようになってきた。そのようなコンテンツを記録媒体に記録するには、コンテンツを暗号化するとともに鍵や権利情報を安全に記録する必要がある。コンテンツの高画質化に伴い、コンテンツの暗号方式、鍵長、機器認証の方式などはより複雑化しつつある。また、コンテンツの不正コピーや不正利用を困難にするための仕組みが次々と導入されている。
【０００３】
　そのような仕組みとして、ＣＰＲＭ（Content Protection for Recordable Media）やＡＡＣＳ（Advanced Access Content System）などの、ＭＫＢ（Media Key Block）を用いた機器無効化がある。ＭＫＢを用いることで、鍵の暴露などにより不正使用される機器においてコンテンツの不正利用をできなくすることができる。機器無効化を有意なものに

するためにはネットワークや認証機器を通じてＭＫＢを常に最新バージョンに保つ必要がある。そのため、機器と記録媒体間で常にＭＫＢのバージョンを確認しあい、ＭＫＢの共有や更新を行うことが必要である。すなわち、ユーザが意識することなく、ＭＫＢの更新に伴う認証鍵やコンテンツ鍵などの鍵情報の更新を安全・確実に行う仕組みが必要である。

【０００４】

従来、ＭＫＢの更新に伴う鍵情報の更新処理（鍵の再設定と再暗号化）およびこの更新処理によって得られる更新情報をＢＤ（Blu-ray Disc）やＤＶＤ（Digital Versatile Disc）など光ディスクやハードディスクなどに書き込む処理を所定のタイミングで一括して行うことで、ＡＡＣＳの鍵更新処理に伴うユーザ待ちを極力避けている（例えば、特許文献１参照）。

【特許文献１】特開２００８－２２３６６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

コンテンツ記録媒体として光ディスク、ハードディスク以外にＳＤカードなどのメモリカードがある。これまではメモリカードの記憶容量は比較的小さかったため、メモリカードに保存されるコンテンツは１セグ放送などの比較的容量の小さなものであった。しかし、メモリカードの記録容量は飛躍的に増大し、いまや光ディスクに匹敵する数十ＧＢの記録容量を持つものも登場している。したがって、今後はメモリカードにもハイビジョン画質のコンテンツが保存されるようになると考えられる。現在、メモリカードにおける著作権保護としてＣＰＲＭが採用されているが、今後は光ディスクにおける著作権保護に採用されているような、より高度なＭＫＢ更新処理をメモリカードにも採用する必要がある。

【０００６】

メモリカードにおいてＭＫＢ更新処理を行うに当たって、光ディスクなどとは異なるメモリカードの使用態様の特殊性を考慮する必要がある。すなわち、光ディスクはユーザが機器のイジェクトボタンを押すなどしないと排出されないのに対して、メモリカードはたとえアクセス中であってもユーザの意思でいつでも自由に機器から抜き取ることができる。また、メモリカードは可搬性のよさや扱いの手軽さなどから携帯電話機、デジタルスチルカメラ、デジタルビデオカメラ、カーナビゲーションなどのモバイル用途で用いられることが多いが、これらモバイル機器は意図せず電源断となることがある。データ書き込み中にメモリカードが強制的に抜き取られたり機器電源断などがあるとデータが破損してリカバリも困難となるおそれがある。特に、ＭＫＢやコンテンツ鍵などの鍵情報の更新処理中にそのような事態が生じると、そのメモリカードに保存されている暗号化コンテンツがすべて利用できなくなるおそれがある。光ディスク、ハードディスクなどについても、鍵情報の書き込み中に機器電源断などがあると同様の結果となる。

【０００７】

例えば、ＡＡＣＳでは、ＭＫＢやコンテンツ鍵などの鍵情報の更新に関して、更新処理が失敗してもリカバリ可能なように鍵情報を一時的に二重化することが規格化されている。しかし、鍵情報を二重化する際に鍵情報ファイルのリネーム処理が発生し、リネーム処理中に上記事態が生じると記録媒体のＦＡＴ（File Allocation Tables）情報が破壊されて記録媒体に保存されているファイルがすべて利用できなくなるおそれがある。

【０００８】

さらに、管理すべきコンテンツ数の増大に伴い、ＭＫＢ更新処理におけるコンテンツ鍵の再暗号化の長時間化が問題となりつつある。このため、認証鍵でコンテンツ鍵を暗復号するのではなく、間にアプリケーション鍵を挟んで、認証鍵でアプリケーション鍵を暗復号し、アプリケーション鍵でコンテンツ鍵を暗復号することも検討されている。アプリケーション鍵が導入されると、ＭＫＢ更新処理でコンテンツ鍵のすべてを再暗号化しなくてよくなり、アプリケーション鍵を再暗号化すればよい。

【０００９】

上記問題に鑑み、本発明は、記録媒体における鍵情報、特に、ＭＫＢ、および認証鍵で暗号化されたアプリケーション鍵やコンテンツ鍵などの中間鍵を安全・確実に更新することを課題とする。

【課題を解決するための手段】

【００１０】

上記課題を解決するために本発明によって次の手段を講じた。すなわち、記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理方法であって、前記記録媒体に、ＭＫＢおよび中間鍵がそれぞれ二つずつ保存されており、かつ、そのいずれが有効であるかを示す有効情報が保存されているとき、前記有効情報を参照して前記保存されているＭＫＢおよび中間鍵のそれぞれについて有効なものを判定するステップと、有効であると判定されなかったＭＫＢおよび中間鍵を新たなＭＫＢおよび中間鍵に書き換えるステップと、ＭＫＢおよび中間鍵の書き換え後に、前記有効情報を、当該書き換えられたＭＫＢおよび中間鍵が有効であることを示す内容に書き換えるステップとを備えているものとする。

【００１１】

同様に、記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理装置であって、前記記録媒体に、ＭＫＢおよび中間鍵がそれぞれ二つずつ保存されており、かつ、そのいずれが有効であるかを示す有効情報が保存されているとき、前記有効情報を参照して前記保存されているＭＫＢおよび中間鍵のそれぞれについて有効なものを判定するとともに、有効であると判定しなかったＭＫＢおよび中間鍵が書き換えられたとき、前記有効情報を、当該書き換えられたＭＫＢおよび中間鍵が有効であることを示す内容に書き換える有効情報処理部と、有効であると判定されたＭＫＢを読み出して当該鍵管理装置に保存されているＭＫＢの更新処理を行い、前記認証鍵を生成するとともに、有効であると判定されなかったＭＫＢを前記更新したＭＫＢに書き換えるＭＫＢ処理部と、有効であると判定された中間鍵を読み出して前記認証鍵で復号および再暗号化するとともに、有効であると判定されなかった中間鍵を前記再暗号化した中間鍵に書き換える中間鍵処理部とを備えているものとする。

【００１２】

この鍵管理方法および鍵管理装置によると、有効情報によって有効ではないと示されているＭＫＢおよび中間鍵を新しいＭＫＢおよび中間鍵に書き換えてから、有効情報を書き換えることでＭＫＢおよび中間鍵の更新が完了する。したがって、ＭＫＢおよび中間鍵の更新処理においてファイルのリネーム処理が不要となる。さらに、ＭＫＢおよび中間鍵の更新処理に要する時間を短縮することができる。

【００１３】

好ましくは、上記鍵管理方法は、さらに、前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むステップと、有効情報の書き込み後に、前記記録媒体に保存されているＭＫＢおよび中間鍵をそのまま残して新たなＭＫＢおよび中間鍵を前記記録媒体に書き込むステップと、ＭＫＢおよび中間鍵の書き込み後に、前記有効情報を、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す内容に書き換えるステップとを備えている。

【００１４】

同様に、好ましくは、上記鍵管理装置において、前記有効情報処理部は、前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むとともに、前記記録媒体に別のＭＫＢおよび中間鍵が書き込まれたとき、前記有効情報を、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す内容に書き換えるものであり、前記ＭＫＢ処理部は、前記記録媒体に保存されているＭＫＢをそのまま残して前記更新したＭＫＢを前記記録媒体に書き込むものであり、前記中間鍵処理部は、前記記録媒体に保存されている中間鍵をそのまま残して前記再暗号化した中間鍵を前記記録媒体に書き込むものである。

【００１５】
この鍵管理方法および鍵管理装置によると、記録媒体に有効情報が保存されていなくても有効情報を新規に作成して安全・確実な鍵情報の更新処理を実現することができる。
【００１６】
あるいは、好ましくは、上記鍵管理方法は、さらに、前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むステップと、有効情報の書き込み後に、前記記録媒体に保存されているＭＫＢおよび中間鍵をそのまま残して新たなＭＫＢおよび中間鍵を前記記録媒体に書き込むステップと、ＭＫＢおよび中間鍵の書き込み後に、前記有効情報を、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す内容に書き換えるステップとを備えている。
【００１７】
同様に、好ましくは、上記鍵管理装置において、前記有効情報処理部は、前記記録媒体に前記有効情報が保存されていないとき、前記記録媒体に保存されているＭＫＢおよび中間鍵が有効であると判定するとともに、前記記録媒体に別のＭＫＢおよび中間鍵が書き込まれたとき、当該書き込まれたＭＫＢおよび中間鍵が有効であることを示す有効情報を前記記録媒体に書き込むものであり、前記ＭＫＢ処理部は、前記記録媒体に保存されているＭＫＢをそのまま残して前記更新したＭＫＢを前記記録媒体に書き込むものであり、前記中間鍵処理部は、前記記録媒体に保存されている中間鍵をそのまま残して前記再暗号化した中間鍵を前記記録媒体に書き込むものである。
【００１８】
この鍵管理方法および鍵管理装置によると、記録媒体に有効情報が保存されていなくても有効情報を新規に作成して安全・確実な鍵情報更新処理を実現することができる。さらに、新規に作成される有効情報が早い段階で記録媒体に書き込まれるため、新たなＭＫＢおよび中間鍵の書き込み後に、有効情報の新規書き込みに伴うＦＡＴ情報更新処理が発生しない。このため、より安全・確実な鍵情報の更新処理を実現することができる。
【００１９】
また、好ましくは、ＭＫＢ、中間鍵、および有効情報の書き換えまたは書き込みが前記記録媒体への一連のアクセスとして一気に行われる。これによると、ＭＫＢ、中間鍵、および有効情報の書き換えまたは書き込みに要する時間を極力短くすることができる。
【００２０】
また、好ましくは、上記鍵管理方法は、さらに、ＭＫＢの書き換えまたは書き込み後に、当該書き換えられたまたは書き込まれたＭＫＢを検証するステップを備えている。これによると、ＭＫＢが改竄されている場合などには不正なＭＫＢの更新を制限することができる。
【００２１】
また、好ましくは、上記鍵管理方法は、さらに、有効情報の書き換えまたは書き込み後に、当該書き換えられたまたは書き込まれた有効情報によって有効でないと示されているＭＫＢおよび中間鍵を前記記録媒体から削除するステップを備えている。これによると、記録媒体の限られた記憶容量を有効に活用することができる。
【００２２】
また、記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理方法であって、前記記録媒体に保存されているＭＫＢを前記記録媒体に複製するステップと、ＭＫＢの複製後に、複製元のＭＫＢを新たなＭＫＢに書き換えるステップと、前記記録媒体に保存されている中間鍵を前記記録媒体に複製するステップと、中間鍵の複製後に、複製元の中間鍵を新たな中間鍵に書き換えるステップとを備えている。
【００２３】
同様に、記録媒体におけるＭＫＢと認証鍵で暗号化された中間鍵とを管理する鍵管理装置であって、前記記録媒体に保存されているＭＫＢを読み出して当該鍵管理装置に保存されているＭＫＢの更新処理を行い、前記認証鍵を生成するとともに、前記記録媒体に保存

されているＭＫＢを前記記録媒体に複製し、複製元のＭＫＢを前記更新したＭＫＢに書き換えるＭＫＢ処理部と、前記記録媒体に保存されている中間鍵を読み出して前記認証鍵で復号および再暗号化するとともに、前記記録媒体に保存されているコンテンツ鍵を前記記録媒体に複製し、複製元の中間鍵を前記再暗号化した中間鍵に書き換える中間鍵処理部とを備えている。

【００２４】

この鍵管理方法および鍵管理装置によると、記録媒体においてＭＫＢおよび中間鍵を複製してから複製元のＭＫＢおよび中間鍵を新たなものに書き換えることでＭＫＢおよび中間鍵の更新が完了する。したがって、ＭＫＢおよび中間鍵の更新処理においてファイルのリネーム処理が不要となる。

【００２５】

好ましくは、ＭＫＢおよび中間鍵の書き換えが前記記録媒体への一連のアクセスとして一気に行われる。これによると、ＭＫＢおよび中間鍵の書き換えに要する時間を極力短くすることができる。

【００２６】

また、好ましくは、上記鍵管理方法は、ＭＫＢの書き込み後に、当該書き込まれたＭＫＢを検証するステップを備えている。これによると、ＭＫＢが改竄されている場合などには不正なＭＫＢの更新を制限することができる。

【００２７】

また、好ましくは、上記鍵管理方法は、ＭＫＢの書き換え後に、複製されたＭＫＢを前記記録媒体から削除するステップと、中間鍵の書き換え後に、複製された中間鍵を前記記録媒体から削除するステップとを備えている。これによると、記録媒体の限られた記憶容量を有効に活用することができる。

【発明の効果】

【００２８】

本発明によると、記録媒体における鍵情報、特に、ＭＫＢ、および認証鍵で暗号化されたアプリケーション鍵やコンテンツ鍵などの中間鍵を安全・確実に更新することができる。

【発明を実施するための最良の形態】

【００２９】

以下、本発明を実施するための最良の形態について、図面を参照しながら説明する。図１は、一実施形態に係るコンテンツ再生システムの構成を示す。本システムは、記録媒体２０に記録されている暗号化コンテンツをコンテンツ再生装置１０で再生するものである。なお、以下では記録媒体２０に記録されたコンテンツを再生する場合について説明するが、コンテンツを記録媒体２０に記録する場合についても同様のことが言える。

【００３０】

記録媒体２０は、例えば、ＢＤ、ＤＶＤ、メモリカードなどである。コンテンツ再生装置１０は、例えば、デジタル放送テレビ受像機、デジタル放送レコーダ、パソコン、携帯電話機、デジタルスチルカメラ、デジタルビデオカメラ、携帯型コンテンツビューアなどである。具体的には、レコーダなどの民生機器によってデジタル放送やインターネット配信の高画質コンテンツをメモリカードなどの記憶媒体に記録し、そのメモリカードを持ち出して別のさまざまな機器に挿入するまたは機器間をネットワーク接続することで、記録した高画質コンテンツをさまざまな機器で再生する、といったことが想定される。

【００３１】

記録媒体２０には、コンテンツ再生装置１０との間の相互認証を経ずにアクセス可能な通常記憶領域２１と、相互認証を経てアクセス可能となる認証記憶領域２２とがある。通常記憶領域２１には、二つのＭＫＢ２１１と、１または複数の暗号化コンテンツ２１２とが保存されている。認証記憶領域２２には、有効情報２２１と、二つの中間鍵２２２と、１または複数の権利情報２２３とが保存されている。中間鍵２２２は、具体的にはコンテンツ鍵またはアプリケーション鍵である。暗号化コンテンツ２１２はコンテンツ鍵として

の中間鍵２２２で暗号化されたもの、あるいはアプリケーション鍵としての中間鍵２２２で暗号化されたコンテンツ鍵で暗号化されたものである。権利情報２２３は、暗号化コンテンツ２１２ごとにコンテンツプロバイダによって設定されたコピー可能回数などの権利情報を含む。有効情報２２１は、二つのＭＫＢ２１１および二つの中間鍵２２２のそれぞれについていずれが有効であるかを示す情報である。

【００３２】

コンテンツ再生装置１０には、記録媒体２０におけるＭＫＢ２１１および中間鍵２２２を管理する鍵管理装置１００と、コンテンツ復号部１４とが含まれている。コンテンツ復号部１４は、記録媒体２０から読み出した暗号化コンテンツ２１２を、鍵管理装置１００によって生成されたコンテンツ鍵１０４で復号する。

【００３３】

鍵管理装置１００において、有効情報処理部１１は、有効情報２２１を参照して、記録媒体２０に保存されている二つのＭＫＢ２１１および二つの中間鍵２２２のそれぞれについて有効なものを判定する。また、有効情報処理部１１は、有効であると判定しなかったＭＫＢ２１１および中間鍵２２２が書き換えられたとき、有効情報２２１を、当該書き換えられたＭＫＢおよび中間鍵が有効であることを示す内容に書き換える。

【００３４】

ＭＫＢ処理部１２は、有効であると判定されたＭＫＢ２１１を読み出して鍵管理装置１００に保存されているＭＫＢ１０１の更新処理を行い、鍵管理装置１００の固有鍵１０２から認証記憶領域２２にアクセスするための認証鍵１０３を生成する。また、ＭＫＢ処理部１２は、有効であると判定されなかったＭＫＢ２１１を、更新したＭＫＢ１０１に書き換える。

【００３５】

中間鍵２２２がコンテンツ鍵の場合には、中間鍵処理部１３は、認証鍵１０３を用いて記録媒体２０との間で相互認証を行い、認証記憶領域２２に保存されている中間鍵２２２であって有効であると判定された中間鍵２２２を読み出して認証鍵１０３で復号してコンテンツ鍵１０４を生成する。また、中間鍵処理部１３は、認証鍵１０３でコンテンツ鍵１０４を再暗号化して、有効であると判定されなかった中間鍵２２２を当該再暗号化したコンテンツ鍵に書き換える。

【００３６】

中間鍵２２２がアプリケーション鍵の場合には、中間鍵処理部１３は、読み出した中間鍵２２２を認証鍵で復号し、さらに認証記憶領域２２に保存されている図示しない暗号化されたコンテンツ鍵を読み出して当該復号したアプリケーション鍵で復号してコンテンツ鍵１０４を生成する。また、中間鍵処理部１３は、認証鍵１０３でアプリケーション鍵を再暗号化して、有効であると判定されなかった中間鍵２２２を当該再暗号化したアプリケーション鍵に書き換える。

【００３７】

ＭＫＢを更新するか否かの判断は下記の手順に従う。なお、下記の手順はＡＡＣＳを想定したものであるが、それ以外の規格に準拠してもよい。

【００３８】

まず、鍵管理装置１００に保存されているＭＫＢ１０１の署名またはハッシュ値などの検証情報を算出し、当該算出した検証情報が、あらかじめＭＫＢ１０１内に記録されている署名またはハッシュ値などの検証情報と等しいか否かを確認する。両者が一致すればＭＫＢ１０１は不正に改竄されていないということであるため、ＭＫＢ１０１のバージョンを確認する。また、記録媒体２０に保存されている二つのＭＫＢ２１１のうち有効なものについても同様の検証作業を実施する。そして、有効なＭＫＢ２１１のバージョンを確認する。

【００３９】

次に、ＭＫＢ１０１と有効なＭＫＢ２１１とでバージョン比較をして、後者の方が新しい場合にはＭＫＢ１０１を有効なＭＫＢ２１１で上書きする。この場合、ＭＫＢ２１１の

更新は不要であるため、記録媒体２０に保存されている中間鍵２２２の更新も不要である。すなわち、ＭＫＢ１０１を単に上書きするだけでよい。一方、前者の方が新しい場合には記録媒体２０に保存されているＭＫＢ２１１を更新する必要がある。さらに、ＭＫＢ２１１が更新されるため、記録媒体２０に保存されている中間鍵２２２も更新する必要がある。すなわち、記録媒体２０におけるＭＫＢ２１１および中間鍵２２２の更新処理が発生する。この更新処理に失敗すると暗号化コンテンツ２１２がすべて再生できなくなるおそれがあるため、本実施形態に係る鍵管理装置１００は下記の手順に従って安全・確実にＭＫＢ２１１および中間鍵２２２の更新処理を行う。

【００４０】

なお、ＭＫＢ２１１および中間鍵２２２の更新処理を行うタイミングとして、記録媒体２０をコンテンツ再生装置１０に挿入した直後または記録媒体２０を排出する直前、対応アプリケーションの起動直後または終了直前、暗号化コンテンツ２１２を再生する直前または再生完了直後、記録媒体２０に暗号化コンテンツ２１２を記録する直前または記録完了直後、記録媒体２０が挿入されたコンテンツ再生装置１０の起動直後または終了直前などさまざまなものが考えられる。ただし、これら具体的なタイミングはコンテンツ再生装置１０に依存するものであり、その他のタイミングであってもよい。

【００４１】

以下、図２のフローチャートを参照しながら鍵管理装置１００による鍵情報更新処理について説明する。まず、記録媒体２０に有効情報２２１が存在するか否かを確認する（ステップＳ１）。有効情報２２１が存在する場合（ステップＳ１のＹＥＳ）、有効情報２２１を参照して二つのＭＫＢ２１１および中間鍵２２２のうちそれぞれ有効なものを判定する（ステップＳ２）。一方、有効情報２２１が存在しない場合（ステップＳ１のＮＯ）、記録媒体２０に保存されているＭＫＢ２１１および中間鍵２２２が有効であることを示す有効情報を作成する（ステップＳ３）。作成した有効情報は鍵管理装置１００に一時保存しておいて後ほど（具体的には、後述するＭＫＢおよび中間鍵の更新後に）書き込んでもよい。好ましくはこの時点で記録媒体２０に書き込む。記録媒体２０に有効情報２２１を新規に書き込む場合、記録媒体２０におけるＦＡＴを更新するため比較的長い時間がかかるが、この時点でこの時間のかかる処理を済ませておくことで、後述するＭＫＢおよび中間鍵の書き換えまたは新規書き込み後の有効情報２２１の更新処理を素早く完了させることができる。

【００４２】

記録媒体２０における有効なＭＫＢ２１１および中間鍵２２２が判定された後、有効であると判定されなかったＭＫＢ２１１を新バージョンのＭＫＢに書き換える、または、記録媒体２０に保存されているＭＫＢ２１１をそのまま残して新バージョンのＭＫＢを別のＭＫＢ２１１として新規書き込みする（ステップＳ４）。新バージョンのＭＫＢは鍵管理装置１００に保存されているＭＫＢ１０１である。その後、書き換えたまたは書き込んだＭＫＢ２１１を記録媒体２０から読み出し、その読み出したＭＫＢ２１１の検証情報とＭＫＢ１０１の検証情報とが等しいか否かを確認する（ステップＳ５）。すなわち、書き換えまたは書き込んだＭＫＢ２１１が不正に改竄されていないことを確認する。なお、ステップＳ５は省略してもかまわない。

【００４３】

ステップＳ４と同様に、有効であると判定されなかった中間鍵２２２を最新の中間鍵で書き換える、または、記録媒体２０に保存されている中間鍵２２２をそのまま残して最新の中間鍵を別の中間鍵２２２として新規書き込みする（ステップＳ６）。最新の中間鍵は鍵管理装置１００における中間鍵処理部１３によって再暗号化されたものである。

【００４４】

ＭＫＢ２１１および中間鍵２２２の書き換えまたは新規書き込みが完了したら、有効情報２２１を、書き換えられたまたは新規に書き込まれたＭＫＢ２１１および中間鍵２２２が有効であることを示す内容に書き換える、またはステップＳ３で記録媒体２０に有効情報２２１を新規書き込みしていない場合には同内容を示す有効情報２２１を新規に書き込

む（ステップＳ７）。すなわち、有効なＭＫＢ２１１および中間鍵２２２を切り替える。これにより、書き換えられたまたは新規書き込みされたＭＫＢ２１１および中間鍵２２２が、以後の記録媒体２０へのアクセスにおいて判定される。

【００４５】

記録媒体２０に鍵情報の記憶容量などに制約がある場合には、有効情報２２１の書き換えまたは新規書き込みの完了後に、有効情報２２１によって有効でないと示されているＭＫＢ２１１および中間鍵２２２を記録媒体２０から削除してもよい（ステップＳ８）。ステップＳ８は省略可能である。

【００４６】

上記の鍵情報更新処理において、ステップＳ４以前に鍵管理装置１００において新バージョンのＭＫＢおよび最新の中間鍵を作成しておき、ステップＳ４、Ｓ６、Ｓ７は記録媒体２０への一連のアクセスとして一気に行うことが好ましい。すなわち、記録媒体２０におけるＭＫＢ２１１、中間鍵２２２および有効情報２２１の更新処理は中断されてはならない処理であるところ、そのような処理を一括して一気に行うことでクリティカルな処理に要する時間を極力短くすることができる。

【００４７】

なお、有効情報２２１は通常記憶領域２１に保存されていてもよいし、省略することも可能である。有効情報２２１を省略する場合、有効情報処理部１１も省略することができる（図３参照）。以下、有効情報２２１を用いない変形例について説明する。

【００４８】

有効情報２２１および有効情報処理部１１を省略した場合、記録媒体２０において有効なＭＫＢ２１１および中間鍵２２２はただ一つに決まる。ＭＫＢ処理部１２は、記録媒体２０からＭＫＢ２１１を読み出して鍵管理装置１００に保存されているＭＫＢ１０１の更新処理を行い、鍵管理装置１００の固有鍵１０２から認証記憶領域２２にアクセスするための認証鍵１０３を生成する。ＭＫＢ処理部１２は、記録媒体２０に保存されているＭＫＢ２１１の複製であるＭＫＢ２１３を記録媒体２０に作成し、複製元のＭＫＢ２１１を、更新したＭＫＢ１０１に書き換える。その後、必要に応じて、ＭＫＢ処理部１２はＭＫＢ２１３を記録媒体２０から削除する。このように、ＭＫＢ２１１の書き換え前にＭＫＢ２１１をバックアップしておく、すなわち、ＭＫＢ２１３を作成しておくことで、ＭＫＢ２１１の書き換えが失敗してもＭＫＢ２１３からＭＫＢ２１１をリカバリすることができる。

【００４９】

中間鍵２２２がコンテンツ鍵の場合には、中間鍵処理部１３は、認証鍵１０３を用いて記録媒体２０との間で相互認証を行い、認証記憶領域２２に保存されている中間鍵２２２を読み出して認証鍵１０３で復号してコンテンツ鍵１０４を生成する。また、中間鍵処理部１３は、認証鍵１０３でコンテンツ鍵１０４を再暗号化するとともに、記録媒体２０に保存されている中間鍵２２２の複製である中間鍵２２４を記録媒体２０に作成し、複製元の中間鍵２２２を当該再暗号化したコンテンツ鍵に書き換える。

【００５０】

中間鍵２２２がアプリケーション鍵の場合には、中間鍵処理部１３は、読み出した中間鍵２２２を認証鍵で復号し、さらに認証記憶領域２２に保存されている図示しない暗号化されたコンテンツ鍵を読み出して当該復号したアプリケーション鍵で復号してコンテンツ鍵１０４を生成する。また、中間鍵処理部１３は、認証鍵１０３でアプリケーション鍵を再暗号化するとともに、記録媒体２０に保存されている中間鍵２２２の複製である中間鍵２２４を記録媒体２０に作成し、複製元の中間鍵２２２を当該再暗号化したアプリケーション鍵に書き換える。

【００５１】

その後、必要に応じて、中間鍵処理部１３は中間鍵２２４を記録媒体２０から削除する。このように、中間鍵２２２の書き換え前に中間鍵２２２をバックアップしておく、すなわち、中間鍵２２４を作成しておくことで、中間鍵２２２の書き換えが失敗しても中間鍵

２２４から中間鍵２２２をリカバリすることができる。

【００５２】

以下、図４のフローチャートを参照しながら、有効情報２２１を用いない鍵情報更新処理について説明する。まず、記録媒体２０に保存されているＭＫＢ２１１を記録媒体２０に複製し（ステップＳ１１）、複製後に複製元のＭＫＢ２１１を新バージョンのＭＫＢに書き換える（ステップＳ１２）。そして、書き換えたＭＫＢ２１１の検証を行う（ステップＳ１３）。ステップＳ１３は省略してもよい。同様に、記録媒体２０に保存されている中間鍵２２２を記録媒体２０に複製し（ステップＳ１４）、複製後に、複製元の中間鍵２２２を最新の中間鍵に書き換える（ステップＳ１５）。ＭＫＢ２１１および中間鍵２２２のいずれも書き換えが完了すると、複製されたＭＫＢ２１３および中間鍵２２４を削除する（ステップＳ１６）。ステップＳ１６は省略してもよい。

【００５３】

以上、本実施形態によると、記録媒体２０においてファイルのリネーム処理を行うことなくＭＫＢ２１１および中間鍵２２２の更新処理を行うことができる。これにより、ＭＫＢ２１１および中間鍵２２２の更新処理に要する時間を短縮することができる。したがって、記録媒体２０における鍵情報の更新処理中に記録媒体２０の強制排出やコンテンツ再生装置１００の電源断などの不測の事態が生じる可能性が減り、安全・確実な鍵情報の更新処理を実現することができる。

【産業上の利用可能性】

【００５４】

本発明に係る鍵管理方法および鍵管理装置は、記録媒体におけるＭＫＢ、コンテンツ鍵、アプリケーション鍵を安全・確実に更新することができるため、メモリカードなどにおける鍵情報の管理に有用である。

【図面の簡単な説明】

【００５５】

【図１】一実施形態に係るコンテンツ再生システムの構成図である。

【図２】鍵情報更新処理のフローチャートである。

【図３】変形例に係るコンテンツ再生システムの構成図である。

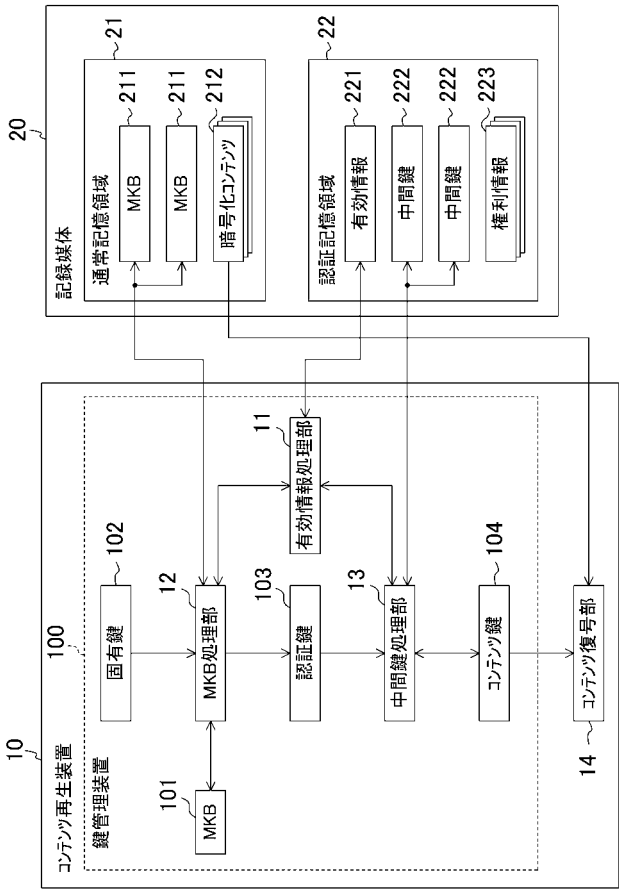
【図４】変形例に係る鍵情報更新処理のフローチャートである。

【符号の説明】

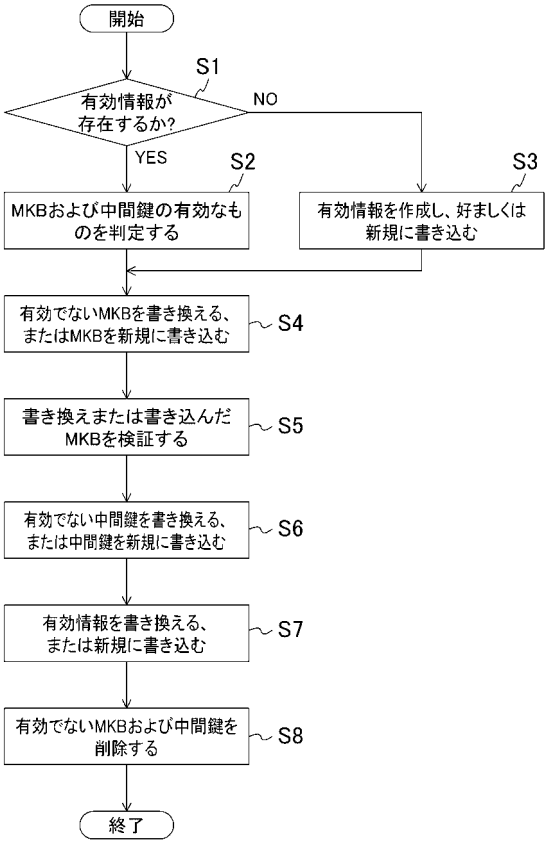
【００５６】

１０　コンテンツ再生装置
１１　有効情報処理部
１２　ＭＫＢ処理部
１３　中間鍵処理部
１４　コンテンツ復号部
２０　記録媒体
２２　認証記憶領域
１００　鍵管理装置
１０１　ＭＫＢ
１０２　固有鍵
１０３　認証鍵
１０４　コンテンツ鍵
２１１　ＭＫＢ
２１２　暗号化コンテンツ
２１３　ＭＫＢ
２２１　有効情報
２２２　中間鍵
２２４　中間鍵

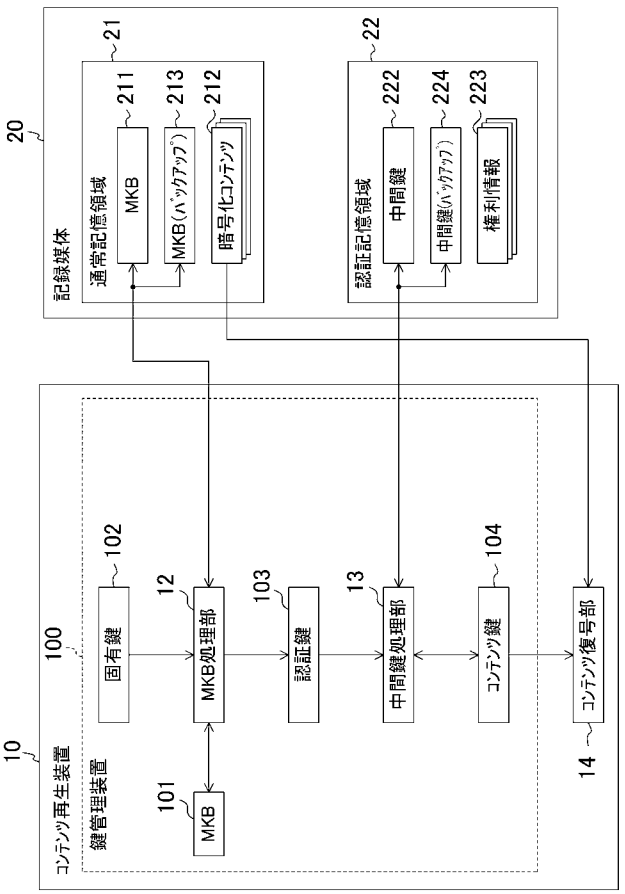
【図１】


20
記録媒体
21
通常記憶領域
211
MKB
211
MKB
212
暗号化コンテンツ
22
認証記憶領域
221
有効情報
222
中間鍵
222
中間鍵
223
権利情報
10
コンテンツ再生装置
100
鍵管理装置
11
有効情報処理部
102
固有鍵
12
MKB処理部
103
認証鍵
13
中間鍵処理部
104
コンテンツ鍵
14
コンテンツ復号部
101
MKB

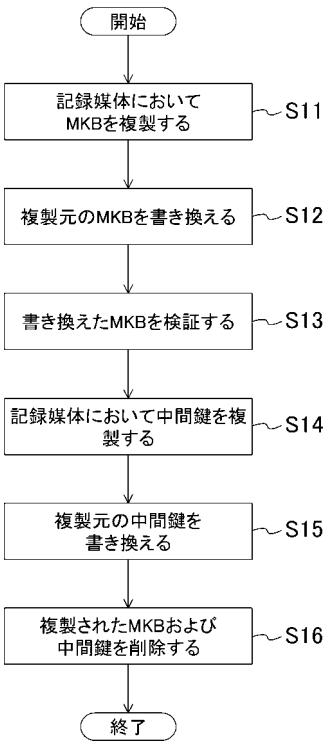
【図２】


開始
S1
有効情報が存在するか?
NO
YES
S2
MKBおよび中間鍵の有効なものを判定する
S3
有効情報を作成し、好ましくは新規に書き込む
有効でないMKBを書き換える、またはMKBを新規に書き込む
S4
書き換えまたは書き込んだMKBを検証する
S5
有効でない中間鍵を書き換える、または中間鍵を新規に書き込む
S6
有効情報を書き換える、または新規に書き込む
S7
有効でないMKBおよび中間鍵を削除する
S8
終了

【図３】


20
記録媒体
21
通常記憶領域
211
MKB
213
MKB(バックアップ)
212
暗号化コンテンツ
22
認証記憶領域
222
中間鍵
224
中間鍵(バックアップ)
223
権利情報
10
コンテンツ再生装置
100
鍵管理装置
102
固有鍵
12
MKB処理部
103
認証鍵
13
中間鍵処理部
104
コンテンツ鍵
14
コンテンツ復号部
101
MKB

【図４】


開始
記録媒体においてMKBを複製する
S11
複製元のMKBを書き換える
S12
書き換えたMKBを検証する
S13
記録媒体において中間鍵を複製する
S14
複製元の中間鍵を書き換える
S15
複製されたMKBおよび中間鍵を削除する
S16
終了

フロントページの続き

(74)代理人 100117581
弁理士 二宮 克也
(74)代理人 100117710
弁理士 原田 智雄
(74)代理人 100121728
弁理士 井関 勝守
(74)代理人 100124671
弁理士 関 啓
(74)代理人 100131060
弁理士 杉浦 靖也
(72)発明者 和田 紘幸
大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者 大井田 篤
大阪府門真市大字門真１００６番地 パナソニック株式会社内

Ｆターム(参考) 5J104 AA16 EA01 EA04 EA15 EA16 EA17 EA18 JA03 MA05 NA02
NA27 NA37 PA14