(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2010 年 9 月 23 日(23.09.2010)

PCT

(10) 国際公開番号
WO 2010/106746 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2010/001443

(22) 国際出願日: 2010 年 3 月 3 日(03.03.2010)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2009-066113 2009 年 3 月 18 日(18.03.2009) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社 (PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 和田紘幸 (WADA, Hiroyuki). 大井田篤(OIDA, Atsushi).

(74) 代理人: 前田弘, 外 (MAEDA, Hiroshi et al.); 〒5410053 大阪府大阪市中央区本町２丁目５番７号 大阪丸紅ビル Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

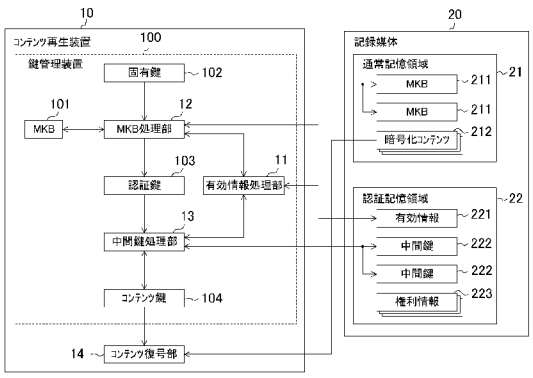
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: KEY MANAGEMENT METHOD AND KEY MANAGEMENT DEVICE

(54) 発明の名称 : 鍵管理方法および鍵管理装置

[図1]



10 content playback apparatus
100 key management device
102 unique key
12 MKB processing unit
103 authentication key
11 validity information processing unit
13 intermediate key processing unit
104 content key
14 content decrypting unit
20 recording medium
21 normal storage region
212 encrypted content
22 authentication storage region
221 validity information
222 intermediate key
223 rights information

(57) **Abstract**: A key management method and key management device which safely and reliably update the MKBs and the intermediate keys, which are encrypted with an authentication key, of a recording medium. A validity information processing unit (11) refers to validity information (221) in a recording medium (20) and assesses a valid MKB (211) and intermediate key (222), as well as rewrites the validity information (221) when an invalid MKB (211) and intermediate key (222) are rewritten. The MKB processing unit (12) reads the valid MKB (211) and updates an MKB (101), as well as rewrites the invalid MKB (211). The intermediate key processing unit (13) reads the valid intermediate key (222) and decrypts and re-encrypts the valid intermediate key (222) with the authentication key (103), as well as rewrites that invalid intermediate key (222) into the re-encrypted intermediate key.

(57) 要約: 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。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。

WO 2010/106746 A1

明　細　書

発明の名称 ： 鍵管理方法および鍵管理装置

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）。

先行技術文献

特許文献

[0005] 特許文献1：特開２００８－２２３６６号公報

発明の概要

発明が解決しようとする課題

[0006] 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。

[0007] 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。

[0008] 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。

[0009] 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。

[0010] 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

[0011] 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。

[0012] 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。

[0013] 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。

[0014] 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。

[0015] 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。

[0016] 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。

[0017] 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。

[0018] 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。

[0019] 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。

[0020] 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。

[0021] 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。

[0022] 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。

[0023] 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。

[0024] 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。

[0025] 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。

[0026] 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。

[0027] 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。

[0028] 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

[0029] 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。

図面の簡単な説明

[0030] [図1]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図である。

[図2]図２は、鍵情報更新処理のフローチャートである。

[図3]図３は、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]図４は、変形例に係る鍵情報更新処理のフローチャートである。

発明を実施するための形態

[0031] 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。

[0032] 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。

[0033] 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。

[0034] 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。

[0035] 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。

[0036] 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。

[0037] 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。

[0038] 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１０３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。

[0039] 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。

[0040] 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。

[0041] 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。

[0042] 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。

[0043] 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。

[0044] 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。

[0045] 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。

[0046] 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。

[0047] 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。

[0048] 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。

[0049] 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。

[0050] 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。

[0051] 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。

[0052] 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１０３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。

[0053] 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。

[0054] 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。

[0055] 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

[0056] 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。

符号の説明

[0057] 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

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

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。

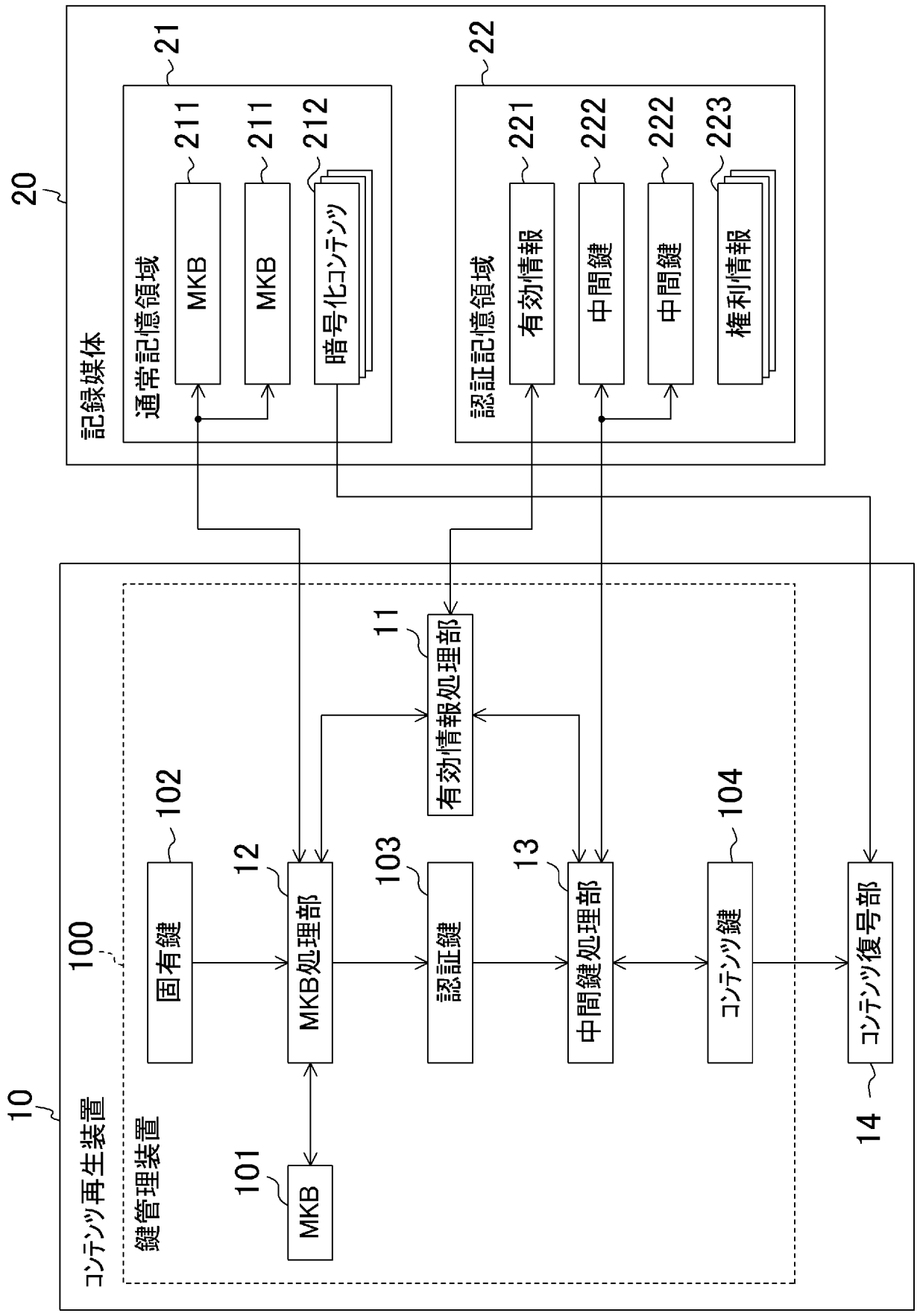
[請求項19] 記録媒体に保存されている暗号化コンテンツを再生するコンテンツ再生装置であって、

請求項１５および１８のいずれか一つの鍵管理装置と、

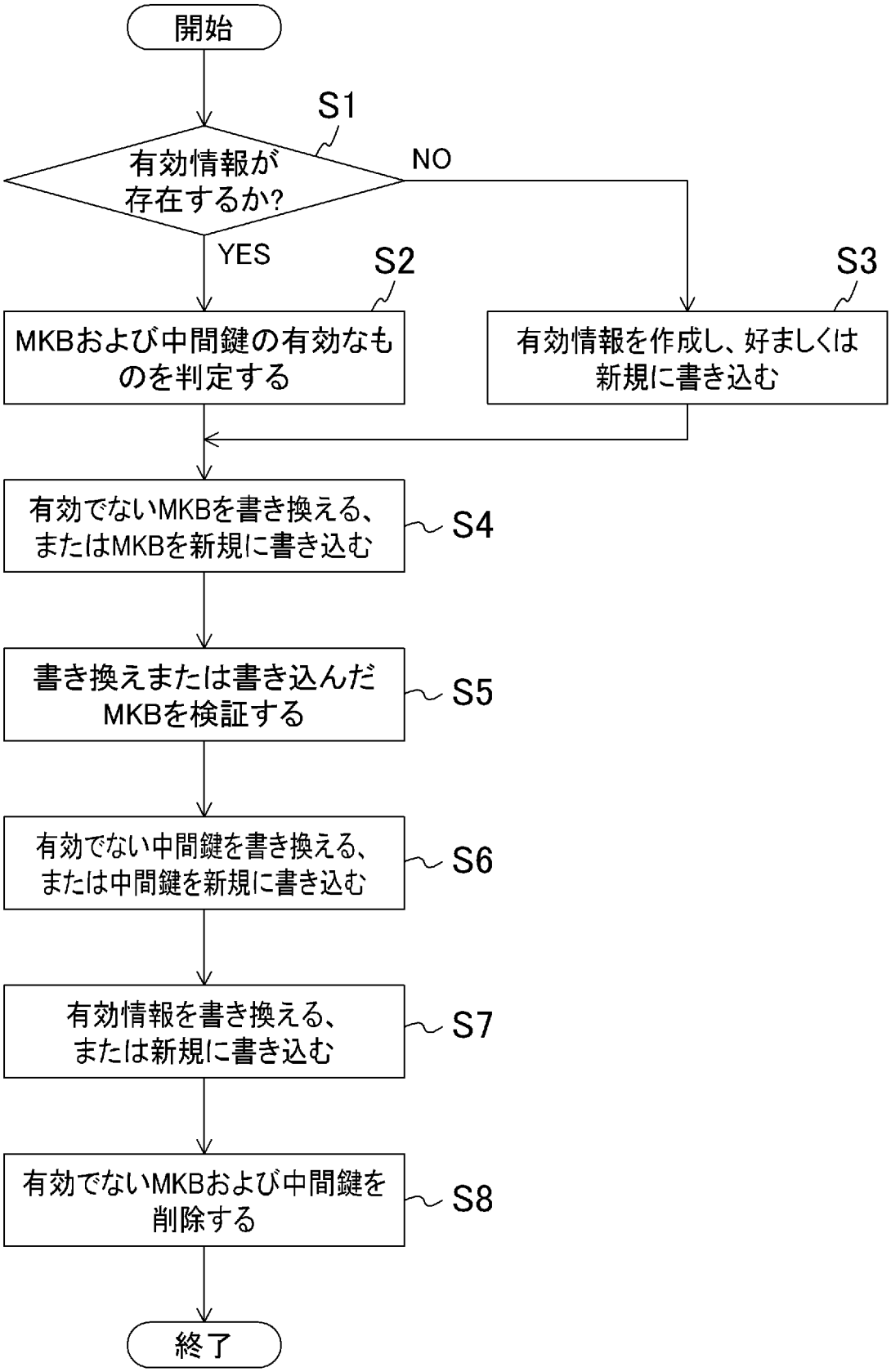
前記記録媒体から前記暗号化コンテンツを読み出し、前記鍵管理装置における前記中間鍵処理部によって復号された中間鍵またはさらに当該中間鍵で復号したコンテンツ鍵で前記読み出した暗号化コンテンツを復号するコンテンツ復号部とを備えている

ことを特徴とするコンテンツ再生装置。

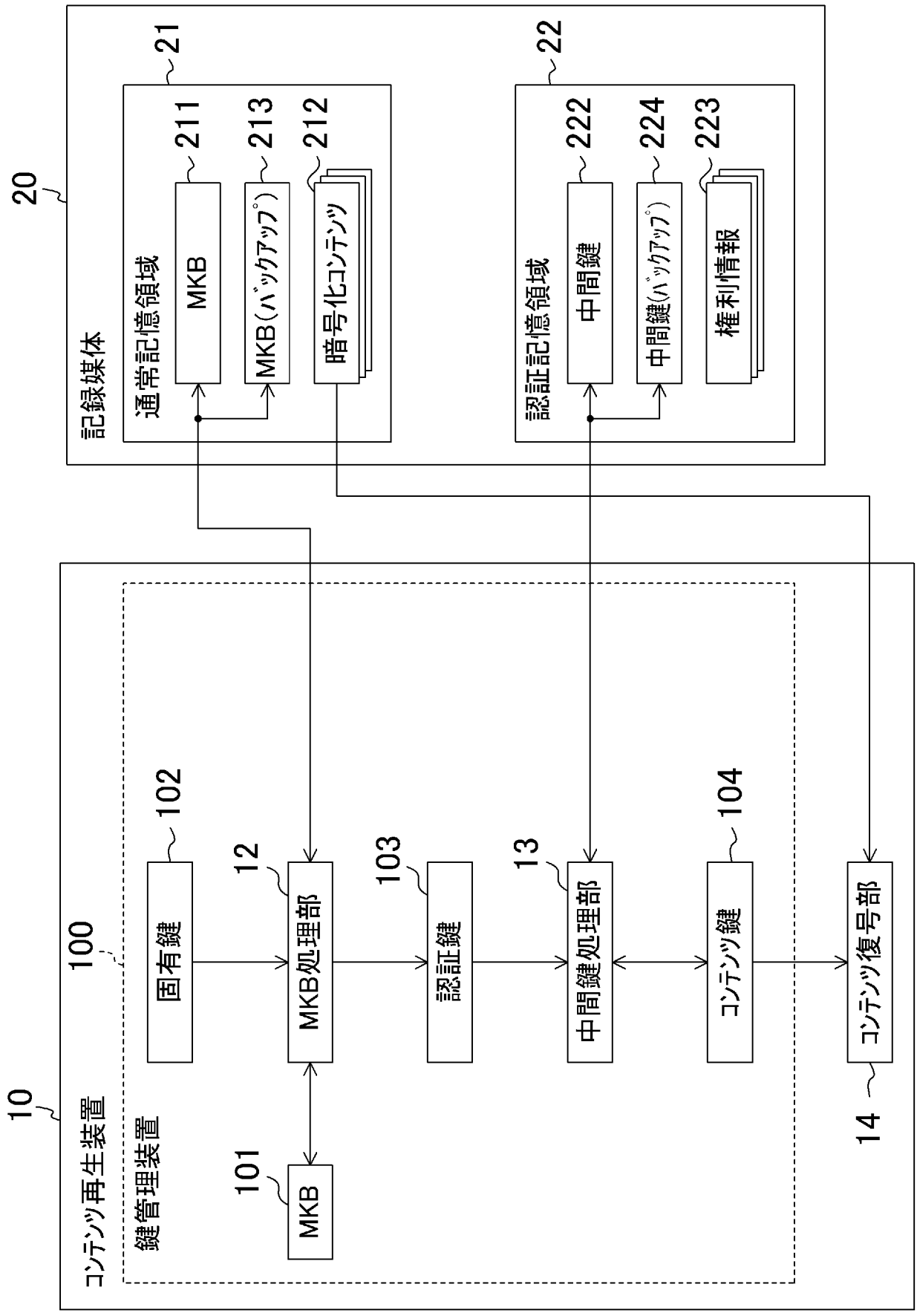
[図1]


10
コンテンツ再生装置
100
鍵管理装置
101
MKB
102
固有鍵
12
MKB処理部
103
認証鍵
11
有効情報処理部
13
中間鍵処理部
104
コンテンツ鍵
14
コンテンツ復号部
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

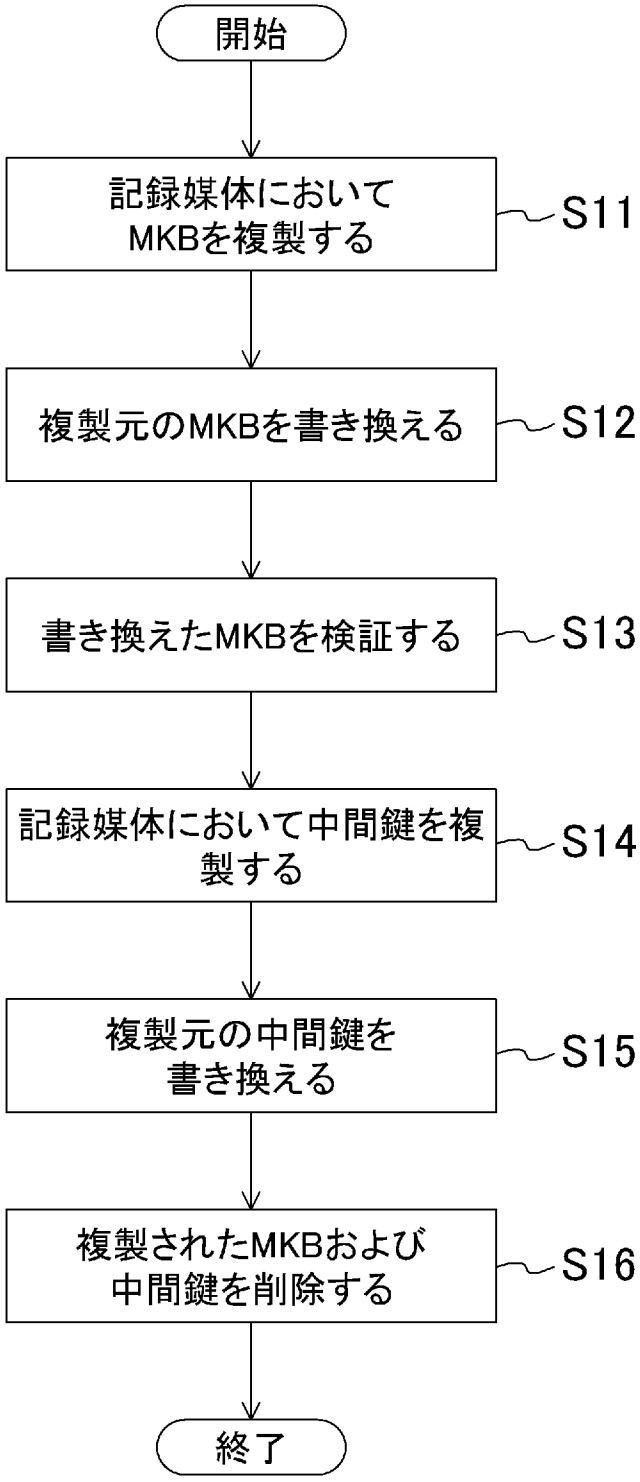
[図2]


開始
S1
有効情報が
存在するか?
NO
YES
S2
S3
MKBおよび中間鍵の有効なもの
を判定する
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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/001443

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-22367 A (Toshiba Corp.), 31 January 2008 (31.01.2008), paragraphs [0011] to [0076] & US 2008/0013732 A1	1-19
A	WO 2006/006326 A1 (Toshiba Corp.), 19 January 2006 (19.01.2006), paragraphs [0016] to [0025] & US 2007/0248231 A1	1-19
A	Advanced Access Content System(AACS) HD DVD and DVD Pre-recorded Book, [online], Revision 0.95, 2009.02.19, p.37-76, [retrieved on 2010.05.10], Retrieved from the Internet:<URL:http://www.aacsla.com/specifications/AACS_Spec_HD_DVD_and_DVD_Prerecorded_Final_9.95.pdf>	1-19

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 May, 2010 (11.05.10)	25 May, 2010 (25.05.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１０／００１４４３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2008-22367 A (株式会社東芝) 2008.01.31, 段落【００１１】～【００７６】 & US 2008/0013732 A1	1-19
A	WO 2006/006326 A1 (株式会社東芝) 2006.01.19, 段落【００１６】～【００２５】 & US 2007/0248231 A1	1-19

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １１．０５．２０１０	国際調査報告の発送日 ２５．０５．２０１０
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３８５７ 新田　亮 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	Advanced Access Content System(AACS)　HD DVD and DVD Pre-recorded Book, [online], Revision 0.95, 2009.02.19, p.37-76, [retrieved on 2010.05.10], Retrieved from the Internet:<URL: http://www.aacsla.com/specifications/AACS_Spec_HD_DVD_and_DVD_Prerecorded_Final_9.95.pdf>	1-19