

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2009 年 1 月 8 日 (08.01.2009)

PCT

(10) 国際公開番号
WO 2009/004707 A1

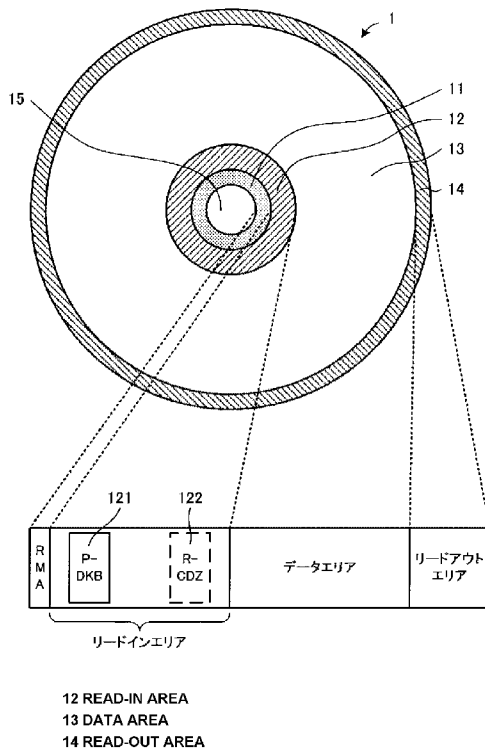
- (51) 国際特許分類:
G11B 20/10 (2006.01) H04L 9/08 (2006.01)
G11B 7/007 (2006.01)
- (21) 国際出願番号: PCT/JP2007/063234
- (22) 国際出願日: 2007 年 7 月 2 日 (02.07.2007)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): パイオニア株式会社 (PIONEER CORPORATION) [JP/JP]; 〒1538654 東京都目黒区目黒 1 丁目 4 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 片多 啓二 (KATATA, Keiji) [JP/JP]; 〒3502288 埼玉県鶴ヶ島市富士見 6 丁目 1 番 2 号 パイオニア株式会社 総合研究所内 Saitama (JP).
- (74) 代理人: 江上 達夫, 外 (EGAMI, Tatsuo et al.); 〒1040031 東京都中央区京橋一丁目 1 6 番 1 0 号 オークビル京橋 3 階 東京セントラル特許事務所内 Tokyo (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, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, JP, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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,

[続葉有]

(54) Title: INFORMATION RECORDING MEDIUM, RECORDING APPARATUS AND REGENERATION APPARATUS

(54) 発明の名称: 情報記録媒体、記録装置及び再生装置

[図1]



(57) Abstract: Information recording medium (1) comprises recording area (13) capable of recording contents and information area (12), this information area provided with control information section (122) capable of recording control information for controlling of regeneration of the contents recorded in the recording area and key information section (121) in which at least encrypted first key information resulting from encryption of first key information for regeneration of the recorded contents and second key information being part of decryption information for decryption of the encrypted first key information are recorded in advance. The state of recording of contents recorded in the information recording medium can be ensured by at the final stage of the recording, decrypting the encrypted first key information and recording the same in the control information section.

(57) 要約: 情報記録媒体 (1) は、コンテンツを記録可能な記録領域 (13) と、該記録領域に記録されるコンテンツの再生を制御する制御情報を記録可能な制御情報区画 (122)、並びに、少なくとも前記記録されるコンテンツを再生するための第 1 鍵情報が暗号化されてなる暗号化第 1 鍵情報、及び該暗号化第 1 鍵情報を復号化するための復号化情報の一部である第 2 鍵情報が予め記録されている鍵情報区画 (121) を有する情報領域 (12) とを備える。その記録時の最後に、暗号化第 1 鍵情報を復号化して、制御情報区画に記録すれば、情報記録媒体に記録されるコンテンツの記録状態を保証することができる。



CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,
IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

明 細 書

情報記録媒体、記録装置及び再生装置

技術分野

- [0001] 本発明は、例えば、デジタル方式により放送されるコンテンツ又はインターネット等のネットワークを介して配信されるコンテンツを、デジタル情報として記録可能である、或いは、デジタル情報として記録されたコンテンツを再生可能である情報記録媒体、記録装置及び再生装置の技術分野に関する。

背景技術

- [0002] この種の記録媒体には、例えば、暗号化されたコンテンツをデータエリアに記録可能な記録媒体であって、コントロールデータエリアにMKB(Media Key Block)が再生のみ可能なように予め記録されており、コントロールデータエリア内において、MKBの近傍に記録エリアが設定され、該記録エリアが未記録である記録媒体が提案されている。
- [0003] この記録媒体に、CPRM(Content Protection for Recordable Media)方式によりコンテンツが記録される際には、前記記録エリアにMKBがコピーされた後に、データエリアにタイトルキーを用いて暗号化されたコンテンツが記録される。或いは、CSS(Content Scramble System)方式によりコンテンツが記録される際には、前記記録エリアに所定のセキュアドディスクキーが記録された後に、データエリアにタイトルキーを用いて暗号化されたコンテンツが記録される(特許文献1参照)。
- [0004] 特許文献1:特開2005-109839号公報

発明の開示

発明が解決しようとする課題

- [0005] しかしながら、上述の背景技術によれば、コンテンツが記録媒体に正しく記録されたか否かを判定することはできない。すると、正しく記録されたにもかかわらず、記録が失敗したとして、別の記録媒体に記録することができたり、記録が失敗したにもかかわらず、正しく記録されたとして、別の記録媒体に記録することができなかつたりするという技術的問題点がある。

[0006] 本発明は、例えば上記問題点に鑑みてなされたものであり、記録状態を保証することができる情報記録媒体、記録装置及び再生装置を提供することを課題とする。

課題を解決するための手段

[0007] 本発明の情報記録媒体は、上記課題を解決するために、コンテンツを記録可能な記録領域と、該記録領域に記録されるコンテンツの再生を制御する制御情報を記録可能な制御情報区画、並びに、少なくとも前記記録されるコンテンツを再生するための第1鍵情報が暗号化されてなる暗号化第1鍵情報、及び該暗号化第1鍵情報を復号化するための復号化情報の一部である第2鍵情報が予め記録されている鍵情報区画を有する情報領域とを備える。

[0008] 本発明の情報記録媒体によれば、例えばDVD-R等の光ディスクである当該情報記録媒体は、例えばデータエリアである記録領域と、例えばリードインエリアである情報領域とを備える。

[0009] 記録領域は、例えば、デジタル方式により放送されるコンテンツ、又はインターネット等のネットワークを介して配信されるコンテンツを、デジタル情報として記録可能である。ここに、本発明に係る「コンテンツ」とは、典型的には、例えば映画、ドラマ、アニメ等の視覚的な、即ち、画像情報或いは映像情報を伴うコンテンツを意味するが、例えば楽曲等の聴覚的な、即ち、音声情報のみを伴うコンテンツを含んでいてもよい。尚、コンテンツは、典型的には、所定の方式(例えばCSS)により暗号化されて、記録領域に記録される。

[0010] 情報領域は、記録領域に記録されるコンテンツの再生を制御する制御情報を記録可能な制御情報区画と、少なくとも記録されるコンテンツを再生するための、例えばディスクキーブロックである第1鍵情報が、例えば所定の暗号鍵によって暗号化されてなる暗号化ディスクキーブロックである暗号化第1鍵情報、及び該暗号化第1鍵情報を復号化するための復号化情報の一部である、例えばメディアキーブロックである第2鍵情報が、予め記録されている鍵情報区画とを有する。

[0011] ここに、本発明に係る「制御情報」とは、例えば、パレンタルコントロール、リージョンコード等の、記録領域に記録されるコンテンツの再生を制御する情報、或いはコンテンツを再生するために必要な情報を意味する。尚、「再生を制御する」とは、例えば、

子供には望ましくないコンテンツの再生を不可能にする、再生可能地域を制限する、又は不正な再生装置での再生を不可能にする等、コンテンツ製作者又は当該情報記録媒体製作者等が意図しない再生が不可能な状態を、当該情報記録媒体が維持するようにすることを意味する。

[0012] 鍵情報区画には、暗号化第1鍵情報、第2鍵情報、制御情報区画に記録される制御情報の正当性を検証するための、例えばハッシュ値である検証情報等が、予め記録されている。尚、「少なくとも前記記録されるコンテンツを再生するための暗号化第1鍵情報、及び該暗号化第1鍵情報を復号化するための復号化情報の一部である、例えばメディアキープブロックである第2鍵情報が予め記録されている」とは、暗号化第1鍵情報、第2鍵情報、検証情報等の複数の情報のうち暗号化第1鍵情報及び第2鍵情報が、少なくとも予め記録されていることを意味する。

[0013] 例えばDVDレコーダ等の、ドライブモジュール及びホストコンピュータを備える記録装置において、当該情報記録媒体にコンテンツが記録される場合、先ず、記録装置のホストコンピュータは、鍵情報区画に記録されている第2鍵情報、及びホストコンピュータに予め格納されている復号化情報の他の一部である、例えばデバイスキーである第4鍵情報を用いて、復号化情報である第5鍵情報を生成する。

[0014] 続いて、ホストコンピュータは、第5鍵情報によって復号化された第1鍵情報、及びホストコンピュータに予め格納されている、例えばマスターキーである第6鍵情報を用いて、例えばディスクキーである第7鍵情報を生成する。

[0015] 当該情報記録媒体における鍵情報区画には、更に、当該記録媒体に記録されるコンテンツを暗号化又は復号化する、例えばタイトルキーである第8鍵情報を生成するための第9鍵情報が記録されている。ホストコンピュータは、第9鍵情報及び第4鍵情報を用いて、第8鍵情報を生成する。続いて、ホストコンピュータは、該生成された第8鍵情報を用いて、所定の方式により、記録されるコンテンツを暗号化する(即ち、スクランブルする)と共に、第7鍵情報を用いて第8鍵情報を暗号化する。

[0016] 記録装置のドライブモジュールは、暗号化されたコンテンツ及び暗号化された第8情報鍵を、記憶領域に記録する。更に、ドライブモジュールは、制御情報区画を除く情報領域等に所定の情報を記録した後に、正しくコンテンツ等が記録されたか否か

を判定又は検査する(即ち、ベリファイする)。

- [0017] ホストコンピュータは、正しく記録されたと判定等された場合にのみ、ドライブモジュールに対し、第5鍵情報を送信する。言い換えれば、正しく記録されなかったと判定された場合(即ち、書き損じをしたと判定された場合)、ホストコンピュータは、ドライブモジュールに対し、第5鍵情報を送信しない。
- [0018] ドライブモジュールは、送信された第5鍵情報を用い、暗号化第1鍵情報を復号化して、第1鍵情報及び他の制御情報を制御情報区画に記録する。
- [0019] 他方、例えばDVDプレーヤ等の、ドライブモジュール及びホストコンピュータを備える再生装置において、当該情報記録媒体に記録されたコンテンツが再生される場合、先ず、再生装置のホストコンピュータは、制御情報区画に記録されている第1鍵情報、及びホストコンピュータに格納されている第6鍵情報を用いて、第7鍵情報を生成する。続いて、ホストコンピュータは、第7鍵情報を用いて、記録領域に記録されている暗号化された第8鍵情報を復号化する。そして、ホストコンピュータは、復号化された第7鍵情報を用いて、記録されたコンテンツを復号化して再生する。
- [0020] 尚、再生装置のホストコンピュータは、典型的には、ユーザにより再生を指示された際に、或いは、情報記録媒体がセットされた際に、制御情報区画に記録されている第1鍵情報を示す、例えばハッシュ値である固有値を演算し、該演算された固有値が、鍵情報区画に記録されている検証情報と同一であるか否かを判定する、即ち、情報記録媒体が正規に記録又は作成された情報記録媒体であるか否かを判定する。そして、再生装置は、同一であると判定された場合にのみ、上述の処理を行い、記録されているコンテンツを再生する。
- [0021] 本願発明者の研究によれば、一般に、デジタル方式により放送されるコンテンツには、例えば「1回だけ録画可能」ということを示す制御信号が付与されている。すると、例えば、記録装置が、情報記録媒体にコンテンツを記録し始めた際に、記録回数を計数するように構成されているとすると、記録が失敗した(即ち、書き損じをした)場合に、他の情報記録媒体にコンテンツを記録すること(即ち、やりなおし)ができない可能性がある。他方、ライトワンス型の光ディスクであれば、書き損じた場合に、やりなおしはできないことは言うまでもない。

- [0022] 或いは、記録装置が、情報記録媒体にコンテンツ、並びにリードオンエリア及びリードアウトエリアに記録される所定の情報を記録し終わった際に（即ち、コンテンツ等の記録が全て終了した際に）、記録回数を計数するように構成されているとすると、計数される直前に、例えば電源を切る等の不正な行為によって、記録回数が計数されずに、定められた回数以上、情報記録媒体にコンテンツを記録することができる可能性がある。他方、記録完了を確認してから、課金を行うシステムでは、その確認作業の前に電源を切られると、やはり不正にコンテンツを課金なしで記録することが可能となってしまうことが判明している。
- [0023] しかるに本発明では、典型的には、コンテンツ等の制御情報を以外の情報が正しく記録されたことを条件に、制御情報区画に制御情報が記録される。従って、制御情報が記録される直前に、即ち、コンテンツ等の制御情報を以外の情報が正しく記録されたことを条件に、記録回数を計数するように記録装置を構成すれば、記録が失敗したにもかかわらず、別の記録媒体に記録することができなかつたり、正しく記録されたにもかかわらず、別の記録媒体に記録することができたりすることを回避することが可能である。
- [0024] これは、制御情報区画のサイズ（即ち、容量）が、例えば192ECCブロックであるのに対して、情報記録媒体全体のサイズが、例えば約14万ECCブロックであることによる。即ち、約14万ECCブロックが正しく記録できた情報記録媒体と、約14万ECCブロックを正しく記録できた記録装置とによって、192ECCブロックである制御情報区画に制御情報を記録することが失敗する確率は極めて小さいと考えられるためである。尚、制御情報区画を、情報記録媒体の中心近傍に配置することによって、情報記録媒体の歪みによる書き損じを回避することができ、制御情報の記録が失敗する確率をより小さくすることができる。この小さな制御情報区画を書く前にトレースをして物理的な損傷を検証し、より正確さを増しても良い。
- [0025] 他方、不正な行為によって、記録回数が計数されないようにしても、或いは課金の対象となる記録完了の確認を免れたとしても、第1鍵情報を含む制御情報が記録されていないので、記録されたコンテンツを再生不可能にすることができるからである。仮に、不正な制御情報を後から記録したとしても、再生する際には、例えば、制御情

報に含まれる第1鍵情報を示す固有値が演算され、該演算された固有値が鍵情報区画に記録されている検証情報と同一でなければ再生することができない。

[0026] このように、コンテンツ等の制御情報以外の情報が正しく記録されたと判定等された情報記録媒体は、制御情報を記録する際に書き損じをする確率が極めて小さいので、記録が成功したとみなすことができる、即ち、コンテンツを再生可能であることを保証することができる。他方、書き損じをしたと判定等された情報記録媒体には、制御情報が記録されることはないので、記録されたコンテンツが再生されることはない、即ち、書き損じをしたことを保証することができる。

[0027] 以上の結果、本発明の情報記録媒体によれば、当該記録媒体に記録されたコンテンツ等の記録状態を保証することができる。

[0028] 加えて、第2鍵情報が予め当該情報記録媒体に記録されているので、ネットワーク機能を有していない記録装置において、当該情報記録媒体にコンテンツを記録する際に、暗号化第1鍵情報を復号化することができる。言い換えれば、コンテンツを記録する際に、例えば鍵情報管理サーバ等にアクセスして、第2鍵情報を取得する必要がない。

[0029] 本発明の情報記録媒体の一態様では、前記制御情報区画は、前記記録されるコンテンツが前記記録領域に記録された後に、記録可能なように設定される。

[0030] この態様によれば、制御情報区画は、コンテンツが記録領域に記録された後に、典型的には、記憶領域、及び制御情報区画以外の情報領域に、コンテンツ及び所定の情報が記録され、正しく記録されたと判定されたことを条件に、制御情報を記録可能なように設定されている。言い換えれば、制御情報区画は、制御情報以外の情報等が正しく記録されたと判定されるまでは、制御情報を記録することができない。

[0031] 具体的には例えば、制御情報区画に記録される制御情報が、所定の暗号鍵によって暗号化されており、コンテンツが記録領域に記録された後でなければ、所定の暗号鍵を取得できないように設定されている。或いは、コンテンツが記録領域に記録された後でなければ、制御情報区画に記録ができないような物理的な制限が設けられている。

[0032] 尚、所定の暗号鍵は、記録装置と、例えばインターネット等のネットワークを介して

接続されている他の装置(例えば、サーバ装置等)に、コンテンツ等が正しく記録できたことを示す信号を送信することによって、取得されるようにすればよい。或いは、情報記録媒体に、該所定の暗号鍵を生成するための鍵情報が予め記録されており、記録装置におけるホストコンピュータに固有の情報によって、所定の暗号鍵が生成され、コンテンツ及び所定の情報が正しく記録されたことを条件に、ドライブモジュールに送信されるようにすればよい。

[0033] 本発明の情報記録媒体の他の態様では、前記鍵情報区画に、前記制御情報区画に記録される制御情報の正当性を検証するための検証情報が更に記録されている。

[0034] この態様によれば、不正な行為によりコンテンツが記録された情報記録媒体の再生を不可能にすることができ実用上非常に有利である。

[0035] 当該情報記録媒体にコンテンツが記録される際には、典型的には、鍵情報区画に予め記録されている暗号化第1鍵情報が、復号化されて、制御情報の一つとして制御情報区画に記録される。そして、暗号化第1鍵情報を復号化するための鍵情報は、不正な記録装置では取得できないように構成されている。このため、鍵情報区画に予め記録されている第1鍵情報を示す何らかの固有の情報を検証情報とすれば、正規にコンテンツが記録された情報記録媒体であるか否かを判定することが可能となる。

[0036] 具体的には例えば、検証情報が、ハッシュ値である場合、当該検証情報は、典型的には、鍵情報区画に予め記録されている第1鍵情報を示すハッシュ値である。再生装置において情報記録媒体が再生される際に、制御情報区画に記録されている第1鍵情報を示すハッシュ値を演算して、検証情報と比較すれば、正規にコンテンツが記録された情報記録媒体であるか否かを判定することができる。これは、不正な行為によりコンテンツが記録された情報記録媒体では、鍵情報区画に暗号化されて記録されている第1鍵情報(即ち、暗号化第1鍵情報)と、制御情報区画に記録されている第1鍵情報とは異なるので、両者のハッシュ値が異なるためである。

[0037] 或いは、検証情報が、EDC(Error Detection Code)である場合、再生装置において、情報記録媒体が再生される際に、鍵情報区画に記録されているEDCと、制御情報区画に記録されているEDCとを比較することによって、正規にコンテンツ等が

記録された情報記録媒体であるか否かを判定することができる。

[0038] 本発明の情報記録媒体の他の態様では、前記鍵情報区画に、秘匿性のある情報の送受信を行うための第3鍵情報が更に記録されている。

[0039] この態様によれば、例えば、デジタル方式により放送されるコンテンツ(例えば、デジタルテレビジョン放送の番組プログラム)が当該情報記録媒体に記録又は録画される際に、鍵情報区画に記録されている、例えば認証キーである第3鍵情報によって、記録装置におけるドライブモジュール及びホストコンピュータ間にセキュアバスが形成される。これにより、ドライブモジュール及びホストコンピュータ間の送受信の際に、例えば鍵情報等を保護することができ、実用上非常に有利である。

[0040] 或いは、例えば、ネットワークを介して配信されるコンテンツ(例えば、ダウンロード販売(Electric Sell Through:EST)により取得されるコンテンツ)が当該情報記録媒体に記録される際に、第3鍵情報によって、記録装置におけるドライブモジュールと、ネットワーク上に存在するコンテンツ配信装置、又はコンテンツを記録するために必要な鍵情報等を管理する鍵情報管理装置との間にセキュアバスが形成される。これにより、例えば盗聴やなりすましによる攻撃から鍵情報等を保護することができ、実用上非常に有利である。

[0041] 尚、ネットワークを介して配信されるコンテンツが記録される当該情報記録媒体には、暗号化第1鍵情報を復号化するための復号化情報の一部である第2鍵情報は記録されていない。或いは、コンテンツが記録される際に、当該情報記録媒体に記録されている第2鍵情報が読み込めないように設定されている。

[0042] 暗号化第1鍵情報を復号化する鍵情報は、典型的には、配信されるコンテンツが記録領域に記録された後に、正しく記録されたことを示す信号を受信したコンテンツ配信装置又は鍵情報管理装置から、ドライブモジュールに対し、セキュアバスを介して送信される。ドライブモジュールは、送信された鍵情報を用い、暗号化第1鍵情報を復号化して、該復号化された第1鍵情報を含む制御情報を制御情報区画に記録する。

[0043] 本発明の記録装置は、上記課題を解決するために、コンテンツを記録可能な記録領域と、該記録領域に記録されるコンテンツの再生を制御する制御情報を記録可能

な制御情報区画、並びに、少なくとも前記記録されるコンテンツを再生するための第1鍵情報が暗号化されてなる暗号化第1鍵情報、及び該暗号化第1鍵情報を復号化するための復号化情報の一部である第2鍵情報が予め記録されている鍵情報区画を有する情報領域とを備える情報記録媒体に前記記録されるコンテンツを記録する記録装置であって、前記情報記録媒体から前記暗号化第1鍵情報及び前記第2鍵情報を読み込む読込手段と、前記復号化情報の他の一部である第4鍵情報を予め格納している記憶手段と、前記読み込まれた暗号化第1鍵情報を、前記読み込まれた第2鍵情報及び前記格納された第4鍵情報を利用して復号化する復号化手段と、前記記録されるコンテンツを前記記録領域に記録すると共に、少なくとも前記第1鍵情報を前記制御情報の一つとして前記制御情報区画に記録する記録手段とを備える。

[0044] 本発明の記録装置によれば、当該記録装置は、鍵情報区画に、少なくとも、例えばディスクキーブロックである第1鍵情報が、例えば所定の暗号鍵によって暗号化されてなる暗号化されたディスクキーブロックである暗号化第1鍵情報、及び該暗号化第1鍵情報を復号化するための復号化情報の一部である、例えばメディアキーブロックである第2鍵情報が記録されている情報記録媒体に、コンテンツを所定の方式(例えばCSS)により暗号化して記録することが可能である。

[0045] 記録装置は、典型的には、ドライブモジュール及びホストコンピュータを備えて構成されている。ドライブモジュールにおける読込手段は、コンテンツが情報記録媒体に記録される際に、情報記録媒体の鍵情報区画から少なくとも暗号化第1鍵情報及び第2鍵情報を読み込み、ホストコンピュータに送信する。

[0046] ホストコンピュータは、送信された第2鍵情報、及びホストコンピュータの記憶手段に予め格納されている、復号化情報の他の一部である、例えばデバイスキーである第4鍵情報を用いて、暗号化第1鍵情報を復号化する復号化情報である第5鍵情報を生成して、該生成された第5鍵情報をドライブモジュールに送信する。

[0047] ドライブモジュールにおける復号化手段は、送信された第5鍵情報を用いて、暗号化第1鍵情報を復号化する。ドライブモジュールにおける記録手段は、コンテンツを情報記録媒体の記録領域に記録すると共に、少なくとも復号化された第1鍵情報を制御情報の一つとして制御情報区画に記録する。

- [0048] コンテンツを記録する際に、ホストコンピュータは、典型的には、鍵情報区画に予め記録されている、例えばタイトルキーである第8鍵情報を生成するための第9鍵情報、及び第4鍵情報を用いて、第8鍵情報を生成する。そして、ホストコンピュータは生成された第8鍵情報を用いて、コンテンツを所定の方式で暗号化して、ドライブモジュールに送信する。記録手段は、送信されたコンテンツを情報記録媒体の記録領域に記録する。
- [0049] 記録手段は、コンテンツが記録された後に、該コンテンツが正しく記録されたことを条件に、制御情報区画に第1鍵情報を記録する。尚、ホストコンピュータは、典型的には、コンテンツが正しく記録されていることを条件に、ドライブモジュールに対し、第5鍵情報を送信する。このため、復号化手段は、コンテンツが正しく記録されていない、即ち、書き損じをした場合には、暗号化第1鍵情報を復号化することができない。すると、記録手段は、制御情報区画に第1鍵情報を記録することができない。
- [0050] このように、コンテンツが正しく記録されたことを条件に、制御情報が記録されるため、制御情報が記録された情報記録媒体は、コンテンツの再生が可能であることを保証することができる。一方、書き損じをした情報記録媒体には、制御情報が記録されることはないので、書き損じをしたことを保証することができる。
- [0051] 以上の結果、本発明の再生装置によれば、記録媒体に記録されたコンテンツ等の記録状態を保証することができる。
- [0052] 本発明の記録装置の一態様では、前記記録手段は、前記記録されるコンテンツが前記記録領域に正しく記録されたか否かを判定する記録状態判定手段を含み、正しく記録されたと判定された場合に、少なくとも前記第1鍵情報を前記制御情報の一つとして前記制御情報区画に記録する。
- [0053] この態様によれば、比較的容易にして、コンテンツが記録領域に正しく記録されたか否かを判定することができ、実用上非常に有利である。
- [0054] 記録手段は、正しく記録されたと判定された場合に、少なくとも第1鍵情報を制御情報の一つとして制御情報区画に記録する。一方、記録手段は、正しく記録されていないと判定された場合(即ち、書き損じをしたと判定された場合)、典型的には、制御情報区画に何も記録しない。

- [0055] 本発明の再生装置は、上記課題を解決するために、コンテンツが記録されている記録領域と、該コンテンツの再生を制御する制御情報が記録されている制御情報区画、及び少なくとも前記制御情報の正当性を検証するための検証情報が記録されている鍵情報区画を有する情報領域とを備え、前記制御情報は、前記記録されているコンテンツを再生するための第1鍵情報を含む情報記録媒体を再生する再生装置であって、前記情報記録媒体から前記制御情報及び前記検証情報を読み込む読込手段と、前記読み込まれた制御情報に基づいて、該読み込まれた制御情報を示す固有値を演算する演算手段と、前記演算された固有値が、前記読み込まれた検証情報と同一であることを条件に、少なくとも前記読み込まれた制御情報に含まれる前記第1鍵情報を用いて、前記コンテンツを再生する再生手段とを備える。
- [0056] 本発明の再生装置によれば、当該再生装置は、コンテンツと共に、例えばディスクキーブロックである第1鍵情報を含む制御情報、及び少なくとも検証情報が記録されている情報記録媒体を再生することが可能である。尚、典型的には、コンテンツは所定の方式により暗号化されて情報記録媒体に記録されている。また、コンテンツを復号化する、例えばタイトルキーである第8鍵情報は暗号化されて情報記録媒体に記録されている。
- [0057] 再生装置は、典型的には、ドライブモジュール及びホストコンピュータを備えて構成されている。ドライブモジュールにおける読込手段は、典型的には、ユーザにより再生を指示された際に、或いは、当該再生装置に情報記録媒体がセットされた際に、情報記録媒体の制御情報区画から制御情報を読み込むと共に、鍵情報区画から検証情報を読み込む。ホストコンピュータにおける演算手段は、読み込まれた制御情報を示す、例えばハッシュ値である固有値を演算する。典型的には、制御情報に含まれる第1鍵情報を示す固有値を演算する。
- [0058] ドライブモジュールにおける再生手段は、演算された固有値が、読み込まれた検証情報と同一であることを条件に、第1鍵情報、及び当該再生装置のホストコンピュータに予め格納されている、例えばマスターキーである第6鍵情報によって、例えばディスクキーである第7鍵情報を生成して、情報記録媒体に記録されている暗号化された第8鍵情報を復号化する。そして、復号化された第8鍵情報によってコンテンツを復

号化して再生する。

[0059] 一方、同一でないことを条件に、再生手段は、典型的にはコンテンツを再生しない。これにより、不正な行為によって、記録又は作成された情報記録媒体が再生されることを防止することができる。言い換えれば、再生することができる情報記録媒体は、正規に記録又は作成された情報記録媒体であることを保証することができる。

[0060] 以上の結果、本発明の再生装置によれば、記録媒体に記録されたコンテンツ等の記録状態を保証することができる。

[0061] 本発明の作用及び他の利得は次に説明する実施するための最良の形態から明らかにされよう。

図面の簡単な説明

[0062] [図1]本発明の実施形態に係る光ディスクの基本構造を示し、上側部分は複数エリアを有する光ディスクの概略平面図であり、下側部分は、その径方向におけるエリア構造の図式的概念図である。

[図2]本発明の実施形態に係るP-DKB内に記録されている情報の一例を示す説明図である。

[図3]本発明の実施形態に係る記録再生装置の構成を示すブロック図である。

[図4]本発明の実施形態に係る記録再生装置におけるホストコンピュータのメモリ内に格納されている情報の一例を示す説明図である。

[図5]本発明の実施形態に係る記録再生装置における記録処理を示すタイミングチャートである。

[図6]本発明の実施形態に係る記録再生装置における再生処理を示すタイミングチャートである。

[図7]本発明の実施形態の変形例に係るP-DKB内に記録されている情報の一例を示す説明図である。

符号の説明

- [0063] 1 光ディスク
2 記録再生装置
11 RMA

- 12 リードインエリア
- 13 データエリア
- 14 リードアウトエリア
- 15 センターホール
- 21 ドライブモジュール
- 22 ホストコンピュータ
- 121 P-DKB
- 122 R-CDZ

発明を実施するための最良の形態

[0064] 以下、本発明の記録装置及び再生装置の一例としての記録再生装置に係る実施形態を、図1乃至図6を参照して説明する。

[0065] <光ディスク>

先ず、図1及び図2を参照して、本実施形態に係る記録再生装置によって記録又は再生される、本発明に係る情報記録媒体の一例としての光ディスクについて説明する。図1は、本実施形態に係る光ディスクの基本構造を示し、上側部分は複数エリアを有する光ディスクの概略平面図であり、下側部分は、その径方向におけるエリア構造の図式的概念図である。

[0066] 図1に示すように、光ディスク1は、該光ディスク1本体上の記録面に、センターホール15を中心として内周から外周に向けて、光ディスクに係る様々な情報を記録可能なRMA(Recording Management Area)11、リードインエリア12、コンテンツを記録可能なデータエリア13及びリードアウトエリア14が設けられている。ここに、本実施形態に係る「リードインエリア12」は、本発明に係る「情報領域」の一例であり、「データエリア13」は、本発明に係る「記録領域」の一例である。

[0067] リードインエリア12には、P-DKB(Pre-recorded CSS Disc Key Block)121、及びR-CDZ(Recordable Control Data Zone)122が設けられている。P-DKB121には、データエリア13に記録されるコンテンツの再生を制御する制御情報を取得するための情報、或いは該制御情報が暗号化されてなる暗号化情報が、予め記録されている。R-CDZ122には、データエリア13に記録されるコンテンツの再

生を制御する制御情報が記録可能である。ここに、本実施形態に係る「P-DKB121」及び「R-CDZ122」は、夫々、本発明に係る「鍵情報区画」及び「制御情報区画」の一例である。尚、R-CDZ122のサイズ(即ち、容量)は、例えば192ECCブロックであり、光ディスク1全体のサイズに対する割合は極めて小さい。

[0068] R-CDZ122に制御情報が記録された後には、伝統的なCDZ及びデータエリアを有する光ディスクとの互換性がとれるようにもでき、或いは、伝統的なCDZ及びデータエリアを有する光ディスクの再生と類似の再生方法が可能となる。

[0069] ここで、図2を参照して、P-DKB121について説明を加える。図2は、本実施形態に係るP-DKB121内に記録されている情報の一例を示す説明図である。

[0070] 図2に示すように、P-DKB121には、少なくとも、鍵 x によって暗号化されたDKB(Disc Key Block)である x DKB1211、ECE-MKB(Embedded Consumer Electronics-Media Key Block)1212、AKB(Authentication Key Block)1213、CKB(Disc Close Key Block)1214、DKBh(CSS DKB hash)1215及びEDCs(Sector Error Detection Code)1216が予め記録されている。

[0071] ここに、本実施形態に係る「 x DKB1211」、「ECE-MKB1212」、「AKB1213」、「CKB1214」、「鍵 x 」及び「DKB」は、夫々、本発明に係る「暗号化第1鍵情報」、「第2鍵情報」、「第3鍵情報」、「第9鍵情報」、「第5鍵情報」及び「第1鍵情報」の一例である。また、本実施形態に係る「DKBh1215」及び「EDCs1216」は、本発明に係る「検証情報」の一例である。

[0072] <記録再生装置>

(記録再生装置の構成)

次に、図3を参照して、本実施形態に係る記録再生装置の構成について説明する。図3は、本実施形態に係る記録再生装置の構成を示すブロック図である。

[0073] 図3において、記録再生装置2は、ドライブモジュール21及びホストコンピュータ22を備えて構成されている。

[0074] ドライブモジュール21は、CPU(Central Processing Unit)211、メモリ212、データ入出力制御部213、スピンドルモータ214、光ピックアップ215及び記録再生部216を備えて構成されている。ここに、本実施形態に係る「CPU211」は、本発明

に係る「復号化手段」及び「記録状態判定手段」の一例である。また、本実施形態に係る「記録再生部213」は、本発明に係る「記録手段」及び「再生手段」の一例であり、本実施形態に係る「光ピックアップ215」は、本発明に係る「読込手段」の一例である。

[0075] ホストコンピュータ22は、CPU221、メモリ222、データ入出力制御部223、記憶部224、操作・表示制御部225、操作ボタン226及び表示パネル227を備えて構成されている。ここに、本実施形態に係る「CPU221」及び「メモリ222」は、夫々、本発明に係る「演算手段」及び「記憶手段」の一例である。

[0076] ここで、図4を参照して、メモリ222について説明を加える。図4は、本実施形態に係る記録再生装置2におけるホストコンピュータのメモリ222内に格納されている情報の一例を示す説明図である。

[0077] 図4に示すように、メモリ222内には、少なくとも、MKB-DK(Media Key Block-Device Key)2221及びマスターキー2222が格納されている。ここに、本実施形態に係る「MKB-DK2221」及び「マスターキー2222」は、夫々、本発明に係る「第4鍵情報」及び「第6鍵情報」の一例である。

[0078] (記録処理)

次に、以上のように構成された記録再生装置2を用いて、デジタル方式により放送され、データ入出力制御部223を介して、例えばハードディスクドライブである記憶部224に格納されたコンテンツを、デジタル情報として、光ディスク1に記録する場合における、記録再生装置2の動作について図5のタイミングチャートを参照して説明する。

[0079] 図5において、まず、ユーザによって、ホストコンピュータ22における操作ボタン226に含まれている記録又は録画を示すボタンが押された際に、或いは、リモコン等によって送信された記録又は録画を示す信号を受信した際に、CPU221は、ドライブモジュール21に対し、光ディスク1を検出することを示す信号を、データ入出力制御部223を介して送信する。

[0080] ドライブモジュール21におけるCPU211は、送信された信号に従って、光ディスク1を検出するように光ピックアップ215を制御する(ステップS101)。光ディスク1が検

出されなかった場合、CPU211は、ホストコンピュータ22に対し、光ディスク1が検出されなかったことを示す信号を、データ入出力制御部213を介して送信する。該送信された信号を受信したホストコンピュータ22におけるCPU221は、典型的には、光ディスク1が検出されなかった旨を示すメッセージ等を表示パネル227に表示するように操作・表示制御部225を制御して、処理を終了する。

- [0081] 光ディスク1が検出された場合、ドライブモジュール21におけるCPU211は、ホストコンピュータ22に対し、光ピックアップ215を介して記録再生部216によって読み込まれた、P-DKB121に記録されているAKB1213を、データ入出力制御部213を介して送信する(ステップS102)。
- [0082] ホストコンピュータ22におけるCPU221は、送信されたAKB1213、及びメモリ222に格納されているMKB-DK2221を用いて、AK (Authentication Key) を生成する(ステップS103)。CPU221は、生成されたAKを用いて、ドライブモジュール21及びホストコンピュータ22間にセキュアバスを形成する(ステップS104)。
- [0083] 次に、CPU221は、ドライブモジュール21に対し、P-DKB121に記録されているECE-MKB1212を読み込むことを示す信号を、データ入出力制御部223を介して送信する(ステップS105)。ドライブモジュール21におけるCPU211は、送信された信号に従って、ECE-MKB1212を読み込むように記録再生部216を制御して、該読み込まれたECE-MKB1212を、ホストコンピュータ22に対し、データ入出力制御部213を介して送信する(ステップS106)。
- [0084] ホストコンピュータ22におけるCPU221は、送信されたECE-MKB1212、及びメモリ222に格納されているMKB-DK2221を用いて、鍵xを生成する(ステップS107)。
- [0085] 続いて、CPU221は、ドライブモジュール21に対し、P-DKB121に記録されているxDKB1211を読み込むことを示す信号を、データ入出力制御部223を介して送信する(ステップS108)。ドライブモジュール21におけるCPU211は、送信された信号に従って、xDKB1211を読み込むように記録再生部216を制御して、該読み込まれたxDKB1211を、ホストコンピュータ22に対し、データ入出力制御部213を介して送信する(ステップS109)と共に、メモリ212に格納する。

- [0086] ホストコンピュータ22におけるCPU221は、生成された鍵xを用いて、送信されたx DKB1211を復号化して、DKBを取得する(ステップS110)。続いて、CPU221は、取得したDKB、及びメモリ222に格納されているマスターキー2222を用いて、本発明に係る「第7鍵情報」の一例であるDK(Disc Key)を生成する(ステップS111)。
- [0087] 次に、CPU221は、ドライブモジュール21に対し、P-DKB121に記録されているCKB1214を読み込むことを示す信号を、データ入出力制御部223を介して送信する(ステップS112)。ドライブモジュール21におけるCPU211は、送信された信号に従って、CKB1214を読み込むように記録再生部216を制御して、該読み込まれたCKB1214を、ホストコンピュータ22に対し、データ入出力制御部213を介して送信する(ステップS113)。
- [0088] ホストコンピュータ22におけるCPU221は、送信されたCKB1214、及びメモリ222に格納されているMKB-DK2221を用いて、本発明に係る「第8鍵情報」の一例であるTK(Title Key)を生成する(ステップS114)。続いて、CPU221は、生成されたTKを、生成されたDKによって暗号化した、本発明に係る「暗号化された第8鍵情報」の一例であるdTKを生成して、該生成されたdTKをドライブモジュール21に対し、データ入出力制御部223を介して送信する(ステップS115)。
- [0089] 更に、CPU221は、生成されたTKを用いて、記録部224に格納されたコンテンツを暗号化して、ファイルシステム及びTKmap(Title Key map)を生成し、該生成されたTKmapをドライブモジュール21に対し、データ入出力制御部223を介して送信する(ステップS116)。ドライブモジュール21におけるCPU211は、送信されたdTKを光ディスク1におけるRMA11に記録するように記録再生部216を制御する(ステップS117)。尚、TKmapとは、暗号化された(即ち、スクランブルされた)データエリア13のセクターアドレスを示す情報である。
- [0090] 次に、ホストコンピュータ22におけるCPU221は、生成したTKを用いコンテンツを、CSS方式によってスクランブルして、該スクランブルされたコンテンツをドライブモジュール21に対し、データ入出力制御部223を介して送信する(ステップS118)。ドライブモジュール21におけるCPU211は、送信されたコンテンツ及び送信されたdTKを、送信されたTKmapに基づいて、光ディスク1のデータエリア13に記録するように

記録再生部216を制御する。更に、CPU211は、R-CDZ122を除くリードインエリア12及びリードアウトエリア14に所定の情報を記録するように記録再生部216を制御する(ステップS119)。

[0091] 次に、CPU211は、光ディスク1に記録されたコンテンツ等を読み込むように記録再生部216を制御して、記録されたコンテンツ等が正しいか否かを判定する、即ち、ベリファイする。更に、CPU211は、R-CDZ122をトレースするように光ピックアップ215を制御して、R-CDZ122に制御情報の記録が可能であるか否かをも判定する(ステップS120)。

[0092] 記録されたコンテンツ等が正しくない(即ち、書き損じをした)と判定された、又は制御情報の記録が不可能であると判定された場合、CPU211は、ホストコンピュータ22に対し、書き損じをしたことを示す信号を送信する。該送信された信号を受信したホストコンピュータ22におけるCPU221は、典型的には、書き損じをした旨を示すメッセージ等を表示パネル227に表示するように操作・表示制御部225を制御すると共に、記録回数を計数せずに処理を終了する。

[0093] 記録されたコンテンツ等が正しいと判定され、且つ制御情報の記録が可能であると判定された場合、即ちコンテンツの記録がベリファイされた場合、ドライブモジュール21におけるCPU211は、ホストコンピュータ22に対し、R-CDZ122以外の記録が正常に終了したことを示す信号を、データ入出力制御部213を介して送信する(ステップS121)。該信号を受信したホストコンピュータ22におけるCPU221は、記録回数を計数し、必要があれば、記憶部224に格納されているコンテンツを削除する。続いて、CPU221は、ドライブモジュール21に対し、鍵xをデータ入出力制御部223を介して送信する(ステップS122)。

[0094] ドライブモジュール21におけるCPU211は、受信した鍵xを用いて、メモリ212に格納されているxDKB1211を復号化してDKBを生成する。続いて、CPU211は、生成されたDKB及び他の制御情報をR-CDZ122に記録するように記録再生部213を制御する(ステップS123)。

[0095] R-CDZ122に、DKBを含む制御情報の記録が終了した後に、CPU211は、ホストコンピュータ22に対し、記録が終了したことを示す信号を、データ入出力制御部

213を介して送信する(ステップS124)。該送信された信号を受信したホストコンピュータ22におけるCPU221は、典型的には、記録が正常に終了した旨を示すメッセージ等を表示パネル227に表示するように操作・表示制御部225を制御して処理を終了する。

[0096] R-CDZ122以外の記録が正常に終了したと判定された光ディスク1は、例えば192ECCブロックであるR-CDZ122を記録するのみであるので、R-CDZ122に制御情報が記録される際に、書き損じをする確率は極めて小さい。このため、コンテンツの再生が可能であることを保証することができる。

[0097] 一方、書き損じをしたと判定された光ディスク1には、制御情報が記録されないので、記録されたコンテンツがされることはない、即ち、書き損じをしたことを保証することができる。この場合には、典型的には、記録回数が計数されないので、他の光ディスクにコンテンツを記録することが可能である。

[0098] (再生処理)

次に、記録再生装置2を用いて、デジタル情報として光ディスク1に記録されたコンテンツを再生する場合における、記録再生装置2の動作について図6のタイミングチャートを参照して説明する。

[0099] 尚、コンテンツが記録されている光ディスク1(以下、記録済光ディスク1ともいう)におけるRMA11には、少なくともdTKが記録されている。リードインエリア12におけるP-DKB121には、図2に示すような情報が記録されており、R-CDZ122には、DKB、物理フォーマット情報等の制御情報が記録されている。リードインエリア12には、他に、所定の情報が記録されている。

[0100] データエリア13には、CSS方式によってスクランブルされたコンテンツ及びdTKが記録されている。リードアウトエリア14には、典型的には、何も記録されていないが、何らかの情報が記録されていてもよい。

[0101] 図6において、まず、ユーザによって、ホストコンピュータ22における操作ボタン226に含まれている再生を示すボタンが押された際に、或いは、リモコン等によって送信された再生を示す信号を受信した際に、CPU221は、ドライブモジュール21に対し、記録済光ディスク1を検出することを示す信号を、データ入出力制御部223を介して

送信する。

- [0102] ドライブモジュール21におけるCPU211は、送信された信号に従って、記録済光ディスク1を検出するように光ピックアップ215を制御する(ステップS201)。記録済光ディスク1が検出されなかった場合、CPU211は、ホストコンピュータ22に対し、記録済光ディスク1が検出されなかったことを示す信号を、データ入出力制御部213を介して送信する。該送信された信号を受信したホストコンピュータ22におけるCPU221は、典型的には、記録済光ディスク1が検出されなかった旨を示すメッセージ等を表示パネル227に表示するように操作・表示制御部225を制御して、処理を終了する。
- [0103] 記録済光ディスク1が検出された場合、ドライブモジュール21におけるCPU211は、ホストコンピュータ22に対し、光ピックアップ215介して記録再生部216によって読み込まれた、P-DKB121に記録されているDKBh1215、及びR-CDZ122に記録されているDKBを、データ入出力制御部213を介して送信する(ステップS202)。
- [0104] ホストコンピュータ22におけるCPU221は、送信されたDKBに基づき、所定のハッシュ関数を用いて、送信されたDKBを示す、本発明に係る「固有値」の一例であるハッシュ値を演算する。続いて、CPU211は、演算されたハッシュ値が、送信されたDKBh1215と同一であるか否かを判定する(ステップS203)。
- [0105] 尚、CPU221がハッシュ値を演算する機能を有していない場合、典型的には、ドライブモジュール21におけるCPU211は、P-DKB121に記録されているEDCs1216を読み込むように記録再生部216を制御して、該読み込まれたEDCs1216をホストコンピュータ22に対し、データ入出力制御部213を介して送信する。ホストコンピュータ22におけるCPU221は、送信されたDKBのEDC (Error Detection Code) が、送信されたEDCs1216と同一であるか否かを判定する。
- [0106] 同一でないと判定された場合、CPU221は、典型的には、再生が不可能である旨を示すメッセージ等を表示パネル227に表示するように操作・表示制御部225を制御して、処理を終了する。
- [0107] 同一であると判定された場合、CPU221は、送信されたDKB、及びメモリ222に格納されているマスターキー2222を用いてDKを生成する(ステップS204)。続いて、CPU221は、ドライブモジュール21に対し、記録済光ディスク1のRMA11に記録さ

れているdTKを読み込むことを示す信号を、データ入出力制御部223を介して送信する(ステップS205)。

[0108] ドライブモジュール21におけるCPU211は、送信された信号に従って、dTKを読み込むように記録再生部216を制御して、該読み込まれたdTKを、ホストコンピュータ22に対し、データ入出力制御部213を介して送信する(ステップS206)。

[0109] ホストコンピュータ22におけるCPU221は、生成されたDKを用いて、送信されたdTKを復号化して、TKを取得する(ステップS207)。次に、CPU221は、ドライブモジュール21に対し、コンテンツを読み込むことを示す信号を、データ入出力制御部223を介して送信する(ステップS208)。

[0110] ドライブモジュール21におけるCPU211は、コンテンツを読み込むように記録再生部216を制御して、該読み込まれたコンテンツを、ホストコンピュータ22に対し、データ入出力制御部213を介して送信する(ステップS209)。ホストコンピュータ22におけるCPU221は、取得したTKを用いて、送信されたコンテンツを復号化して、該復号化されたコンテンツを、図示しない、例えばテレビ等の表示装置に対し、データ入出力制御部223を介して送信する(ステップS210)。

[0111] このように、再生する際に、先ず、P-DKB121に記録されているDKBh1215、及びR-CDZ122に記録されているDKBを示すハッシュ値を比較することにより、或いは、P-DKB121に記録されているEDCs1216、及びR-CDZ122に記録されているDKBのEDCを比較することにより、不正な行為によって記録された光ディスクの再生を防止することができる。

[0112] <変形例>

次に、図7を参照して、光ディスク1におけるP-DKB121の変形例について説明する。図7は、図2と同趣旨の、本実施形態の変形例に係るP-DKB121内に記録されている情報の一例を示す説明図である。

[0113] 図7に示すように、P-DKB121には、少なくとも、xDKB1211、ECE-MKB1212、AKB1213、CKB1214、DKBh1215、EDCs1216、当該光ディスク1の識別情報を示すDisc ID1217、及び本発明に係る「第3鍵情報」の他の例としてのDAK (Disc Authentication Key) 1218が予め記録されている。

- [0114] 例えば、デジタルテレビジョン放送の番組プログラム等の無料のコンテンツが、デジタル情報として、当該光ディスク1に記録される場合、P-DKB121は、少なくとも、図7における破線aで囲われていないDisc ID1217及びDAK1218が読み取られないように設定されている。この場合、記録再生装置2は、上述した記録処理と同様の処理を行い、コンテンツを光ディスク1に記録する。
- [0115] 他方、例えば、ESTにより取得される有料のコンテンツが、デジタル情報として、当該光ディスク1に記録される場合、P-DKB121は、少なくとも、図7における一点鎖線bで囲われていないECE-MKB1212、AKB1213及びCKB1214が読み取られないように設定されている。
- [0116] この場合、記録再生装置2におけるドライブモジュール21は、先ず、P-DKB121に記録されているDisc ID1217及びDAK1218を読み取る。次に、ドライブモジュール21は、例えばインターネット等のネットワーク上に存在し、コンテンツを記録するために必要な鍵情報を管理する鍵管理装置に対し、読み取られたDisc ID1217を送信する。更に、ドライブモジュール21は、読み取られたDAK1218を用いて、ドライブモジュール21及び鍵管理装置間にセキュアバスを形成する。
- [0117] 記録再生装置2におけるホストコンピュータ22は、鍵管理装置からTKを取得し、コンテンツをスクランブルして、ドライブモジュール21に対して送信する。ドライブモジュール21は、送信されたコンテンツ、及びセキュアバスを介して鍵管理装置から取得したdTKを光ディスク1に記録すると共に、R-CDZ122を除くリードインエリア12及びリードアウトエリア14に所定の情報を記録する。
- [0118] ドライブモジュール21は、コンテンツ等が正しく記録されていることを条件に、セキュアバスを介して鍵管理装置から鍵xを取得する。続いて、ドライブモジュール21は、取得された鍵xを用い、xDKB1211を復号化してDKBを生成して、該生成されたDKB及び他の制御情報をR-CDZ122に記録する。
- [0119] このように、無料コンテンツを記録する場合と有料コンテンツを記録する場合とで、暗号復号機構が異なっている、又は分離しているので、仮に一方に何らかの問題が発生したとしても、他方に影響を与えることは無い。
- [0120] また、例えば、無料コンテンツ用の光ディスク、有料コンテンツ用の光ディスク等の

用途別の光ディスクを製造しなくてよいので、例えば設備投資等のコストを削減することができ、実用上非常に有利である。

[0121] 尚、例えば、パーソナルコンピュータに内蔵又は外付けされている、DVDドライブ等を用いて、光ディスク1にコンテンツを記録する場合は、典型的には、ESTにより取得されるコンテンツの記録のみ可能である。これは、パーソナルコンピュータにおけるホストコンピュータには、図4に示すような、MKB-DK2222が配布されないためである。このようにすることによって、例えば、不正なアプリケーションソフトが作成されることを未然に防止することができる。

[0122] 尚、本発明は、上述した実施形態に限られるものではなく、請求の範囲及び明細書全体から読み取れる発明の要旨、或いは思想に反しない範囲で適宜変更可能であり、そのような変更を伴う情報記録媒体、記録装置及び再生装置もまた、本発明の技術的範囲に含まれるものである。

請求の範囲

- [1] コンテンツを記録可能な記録領域と、
該記録領域に記録されるコンテンツの再生を制御する制御情報を記録可能な制御情報区画、並びに、少なくとも前記記録されるコンテンツを再生するための第1鍵情報が暗号化されてなる暗号化第1鍵情報、及び該暗号化第1鍵情報を復号化するための復号化情報の一部である第2鍵情報が予め記録されている鍵情報区画を有する情報領域と
を備えることを特徴とする情報記録媒体。
- [2] 前記制御情報区画は、前記記録されるコンテンツが前記記録領域に記録された後に、記録可能なように設定されることを特徴とする請求の範囲第1項に記載の情報記録媒体。
- [3] 前記鍵情報区画に、前記制御情報区画に記録される制御情報の正当性を検証するための検証情報が更に記録されていることを特徴とする請求の範囲第1項に記載の情報記録媒体。
- [4] 前記鍵情報区画に、秘匿性のある送受信を行うための第3鍵情報が更に記録されていることを特徴とする請求の範囲第1項に記載の情報記録媒体。
- [5] コンテンツを記録可能な記録領域と、該記録領域に記録されるコンテンツの再生を制御する制御情報を記録可能な制御情報区画、並びに、少なくとも前記記録されるコンテンツを再生するための第1鍵情報が暗号化されてなる暗号化第1鍵情報、及び該暗号化第1鍵情報を復号化するための復号化情報の一部である第2鍵情報が予め記録されている鍵情報区画を有する情報領域とを備える情報記録媒体に前記記録されるコンテンツを記録する記録装置であって、
前記情報記録媒体から前記暗号化第1鍵情報及び前記第2鍵情報を読み込む読込手段と、
前記復号化情報の他の一部である第4鍵情報を予め格納している記憶手段と、
前記読み込まれた暗号化第1鍵情報を、前記読み込まれた第2鍵情報及び前記格納された第4鍵情報を利用して復号化する復号化手段と、
前記記録されるコンテンツを前記記録領域に記録すると共に、少なくとも前記第1

鍵情報を前記制御情報の一つとして前記制御情報区画に記録する記録手段と
を備えることを特徴とする記録装置。

[6] 前記記録手段は、

前記記録されるコンテンツが前記記録領域に正しく記録されたか否かを判定する記録状態判定手段を含み、

正しく記録されたと判定された場合に、少なくとも前記第1鍵情報を前記制御情報の一つとして前記制御情報区画に記録する

ことを特徴とする請求の範囲第5項に記載の記録装置。

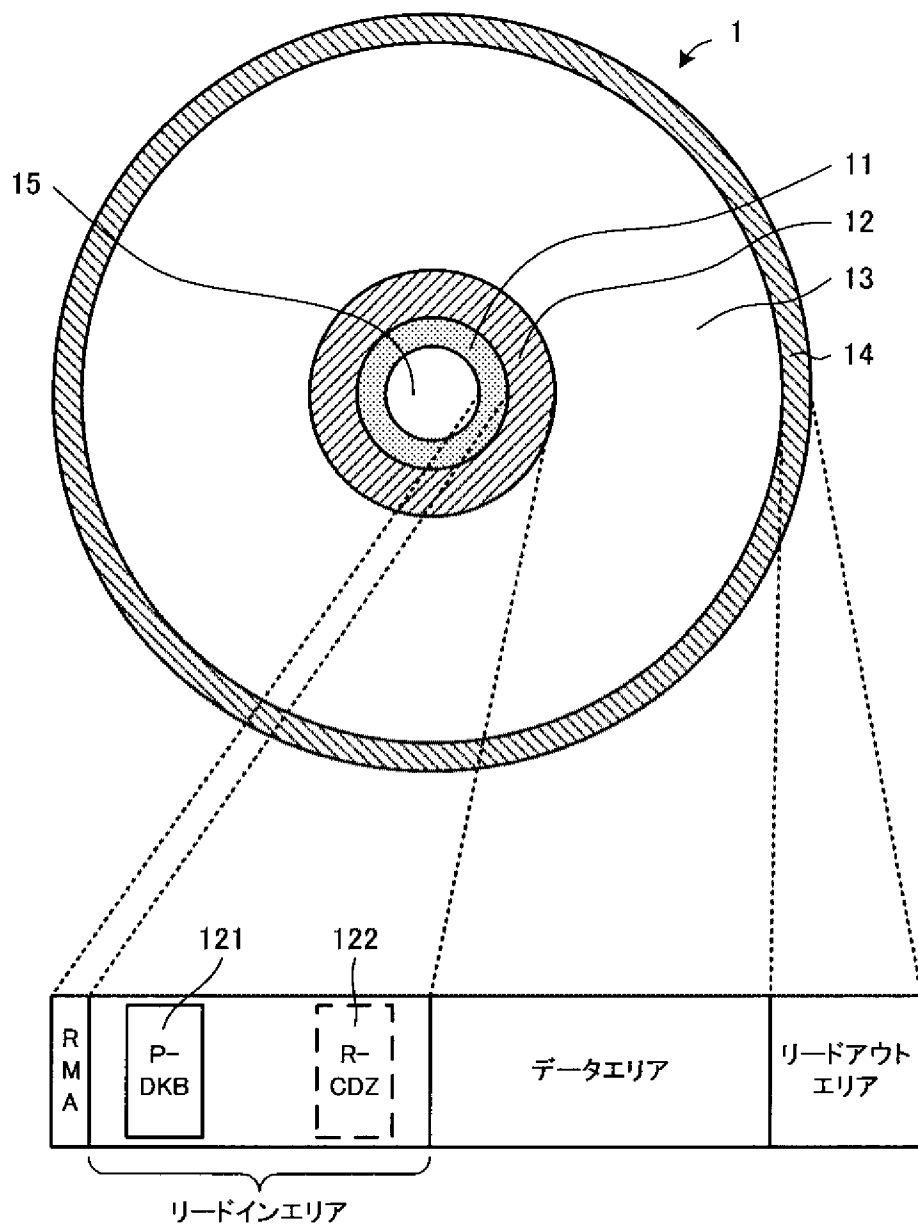
[7] コンテンツが記録されている記録領域と、該コンテンツの再生を制御する制御情報が記録されている制御情報区画、及び少なくとも前記制御情報の正当性を検証するための検証情報が記録されている鍵情報区画を有する情報領域とを備え、前記制御情報は、前記記録されているコンテンツを再生するための第1鍵情報を含む情報記録媒体を再生する再生装置であって、

前記情報記録媒体から前記制御情報及び前記検証情報を読み込む読込手段と、
前記読み込まれた制御情報に基づいて、該読み込まれた制御情報を示す固有値を演算する演算手段と、

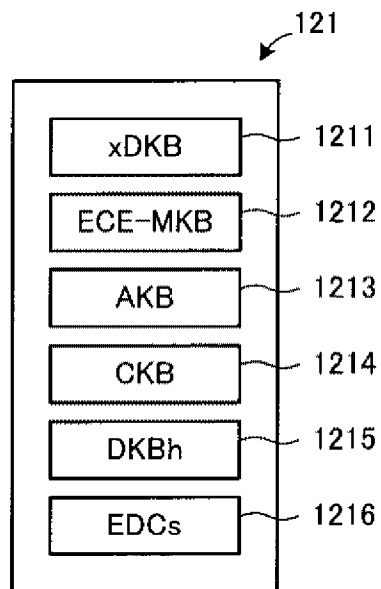
前記演算された固有値が、前記読み込まれた検証情報と同一であることを条件に、
少なくとも前記読み込まれた制御情報に含まれる前記第1鍵情報を用いて、前記コンテンツを再生する再生手段と

を備えることを特徴とする再生装置。

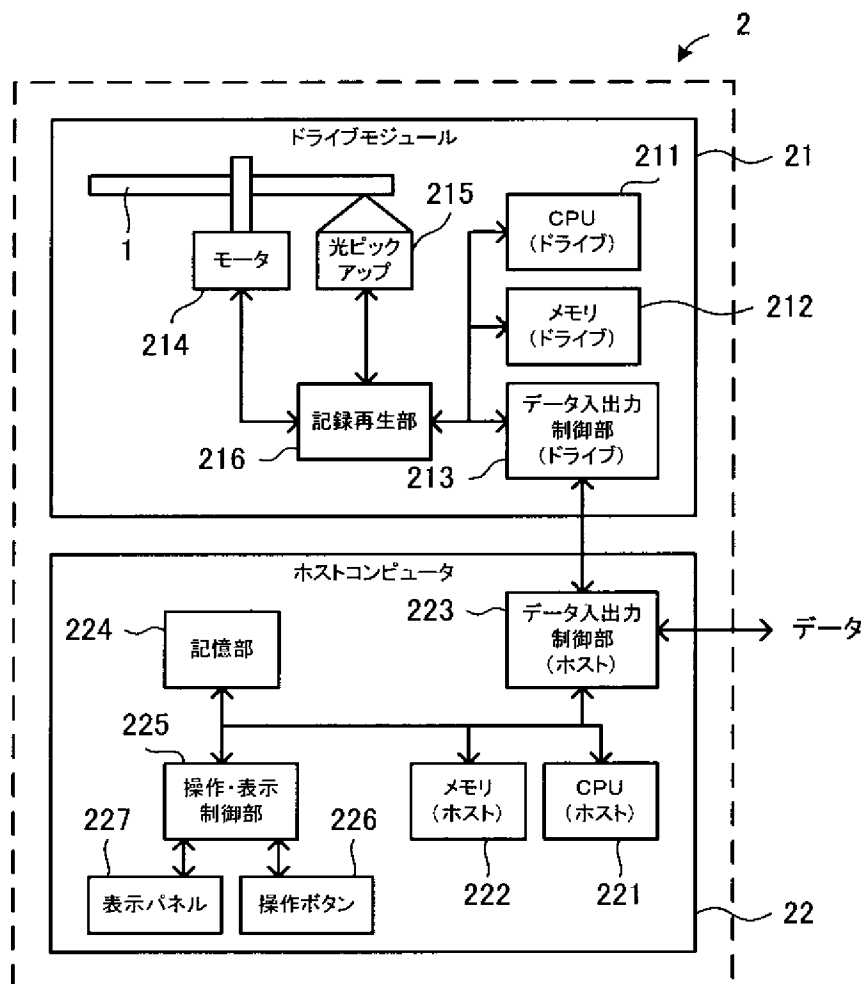
[図1]



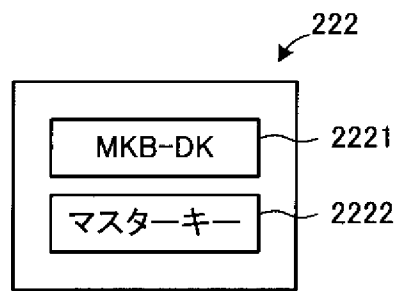
[図2]



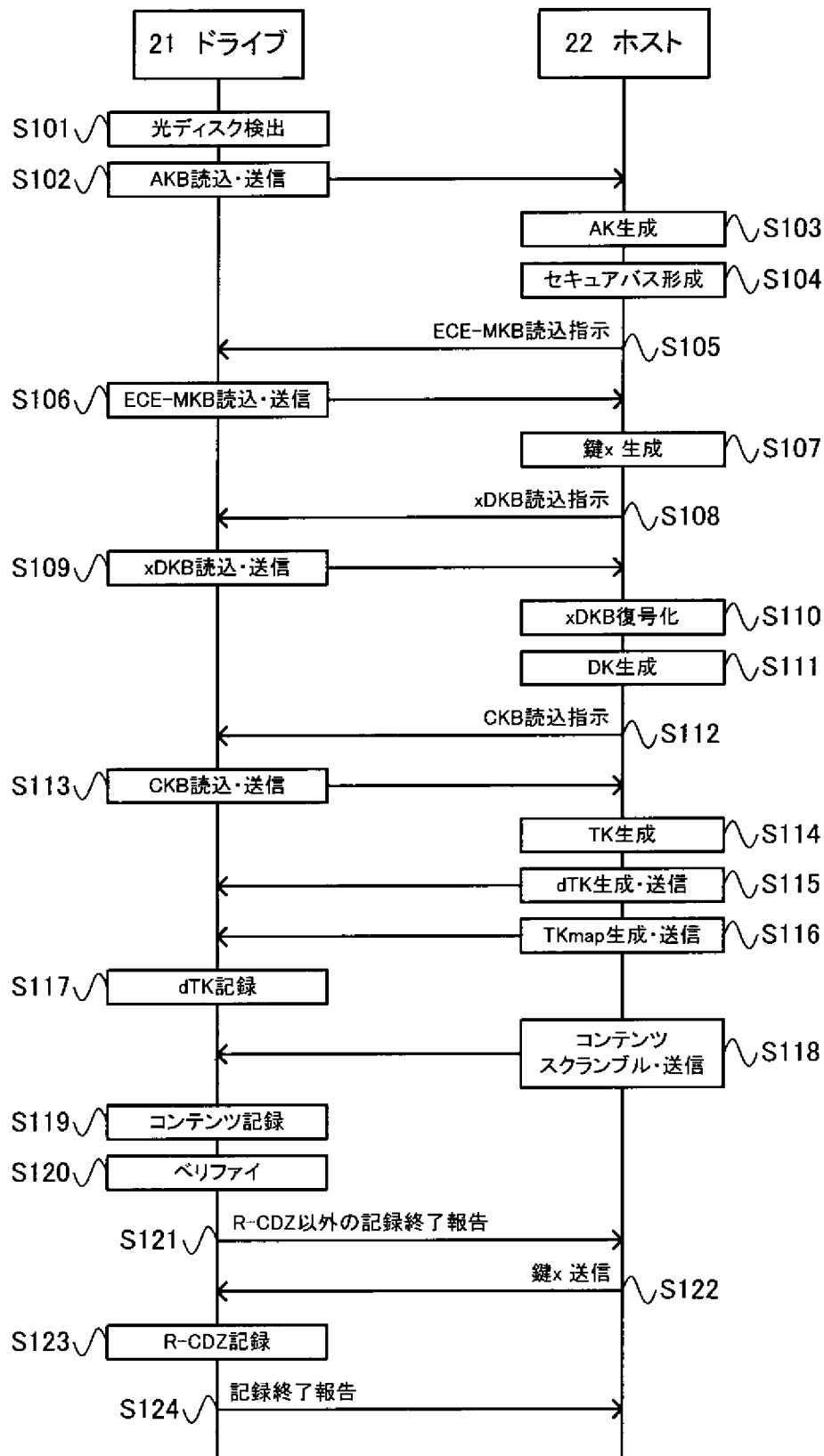
[図3]



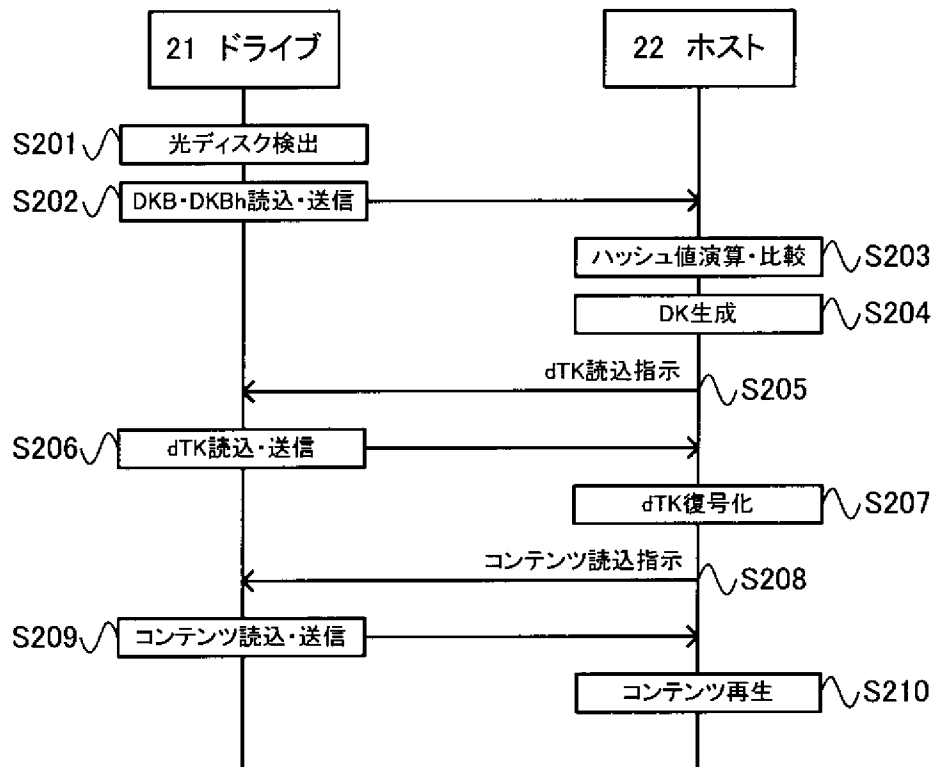
[図4]



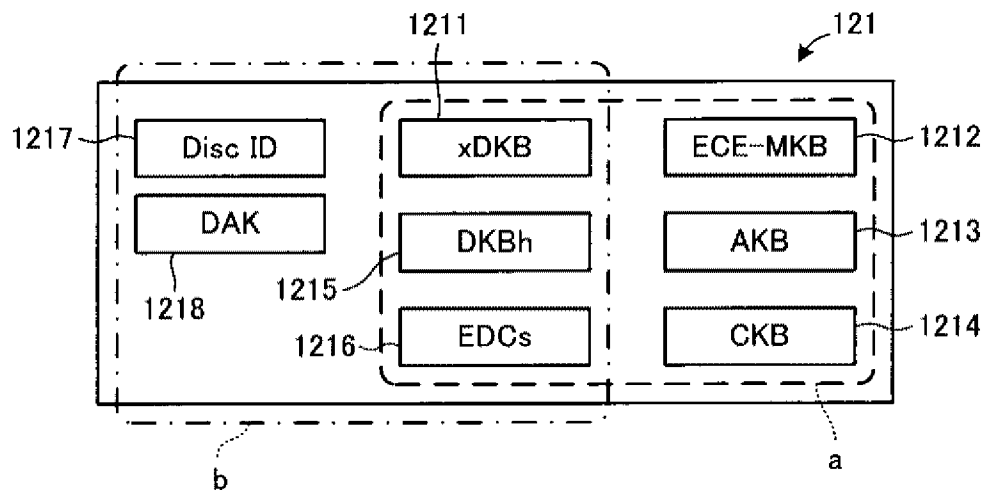
[図5]



[図6]



[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/063234

A. CLASSIFICATION OF SUBJECT MATTER

G11B20/10(2006.01) i, G11B7/007(2006.01) i, 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)

G09C1/00-5/00, G11B7/00-7/013, 7/28-7/30, 20/10-20/16, H04K1/00-3/00, H04L9/00-9/38

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	1996-2007
Kokai Jitsuyo Shinan Koho	1971-2007	Toroku Jitsuyo Shinan Koho	1994-2007

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.
Y	WO 2006/82961 A1 (Matsushita Electric Industrial Co., Ltd.), 10 August, 2006 (10.08.06), Full text; all drawings (Family: none)	1-7
Y	WO 03/36858 A2 (Matsushita Electric Industrial Co., Ltd.), 01 May, 2003 (01.05.03), Full text; all drawings & JP 2003-204320 A & US 2003/81792 A1	1-7
A	EP 1318517 A2 (Pioneer Corp.), 11 June, 2003 (11.06.03), Full text; all drawings & JP 2003-196922 A & US 2003/142560 A1	1-7

☒ 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
28 August, 2007 (28.08.07)Date of mailing of the international search report
11 September, 2007 (11.09.07)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/063234

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-109839 A (Sony Corp.), 21 April, 2005 (21.04.05), Full text; all drawings (Family: none)	1-7
A	WO 2006/11527 A1 (Matsushita Electric Industrial Co., Ltd.), 02 February, 2006 (02.02.06), Full text; all drawings (Family: none)	1-7
A	WO 2006/8972 A1 (Matsushita Electric Industrial Co., Ltd.), 26 January, 2006 (26.01.06), Full text; all drawings & JP 2006-31818 A	1-7
A	WO 2005/121977 A1 (Matsushita Electric Industrial Co., Ltd.), 22 December, 2005 (22.12.05), Full text; all drawings & JP 2005-352642 A	1-7
A	WO 00/67257 A2 (Matsushita Electric Industrial Co., Ltd.), 09 November, 2000 (09.11.00), Full text; all drawings & EP 1058254 B1 & JP 2001-189015 A & US 6938162 B1	1-7
A	WO 97/14144 A1 (Matsushita Electric Industrial Co., Ltd.), 17 April, 1997 (17.04.97), Full text; all drawings & EP 802527 B1 & US 6081785 A	1-7

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. G11B20/10(2006.01)i, G11B7/007(2006.01)i, 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 (I P C))

Int.Cl. G09C1/00-5/00, G11B7/00-7/013, 7/28-7/30, 20/10-20/16, H04K1/00-3/00, H04L9/00-9/38

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 7 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 7 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 7 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 請求の範囲の番号
Y	WO 2006/82961 A1 (松下電器産業株式会社) 2006.08.10, 全文, 全図 (ファミリーなし)	1-7
Y	WO 03/36858 A2 (Matsushita Electric Industrial Co., Ltd.) 2003.05.01, 全文, 全図 & JP 2003-204320 A & US 2003/81792 A1	1-7
A	EP 1318517 A2 (Pioneer Corporation) 2003.06.11, 全文, 全図 & JP 2003-196922 A & US 2003/142560 A1	1-7

☒ 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

2 8 . 0 8 . 2 0 0 7

国際調査報告の発送日

1 1 . 0 9 . 2 0 0 7

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)
郵便番号 1 0 0 - 8 9 1 5
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)

松尾 淳一

5 D

8 8 4 2

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 5 1

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 請求の範囲の番号
A	JP 2005-109839 A (ソニー株式会社) 2005. 04. 21, 全文, 全図 (ファミリーなし)	1-7
A	WO 2006/11527 A1 (松下電器産業株式会社) 2006. 02. 02, 全文, 全図 (ファミリーなし)	1-7
A	WO 2006/8972 A1 (松下電器産業株式会社) 2006. 01. 26, 全文, 全図 & JP 2006-31818 A	1-7
A	WO 2005/121977 A1 (松下電器産業株式会社) 2005. 12. 22, 全文, 全図 & JP 2005-352642 A	1-7
A	WO 00/67257 A2 (Matsushita Electric Industrial Co., Ltd.) 2000. 11. 09, 全文, 全図 & EP 1058254 B1 & JP 2001-189015 A & US 6938162 B1	1-7
A	WO 97/14144 A1 (松下電器産業株式会社) 1997. 04. 17, 全文, 全図 & EP 802527 B1 & US 6081785 A	1-7