(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4861975号
(P4861975)
(45)発行日　平成24年1月25日(2012.1.25)　(24)登録日　平成23年11月11日(2011.11.11)

(51)Int.Cl.　　F I
G11B 20/10 (2006.01)　　G11B 20/10　H
G06F 21/24 (2006.01)　　G06F 12/14　550B

請求項の数 10　(全 16 頁)

(21)出願番号　特願2007-501662(P2007-501662)
(86)(22)出願日　平成18年2月6日(2006.2.6)
(86)国際出願番号　PCT/JP2006/301979
(87)国際公開番号　WO2006/082961
(87)国際公開日　平成18年8月10日(2006.8.10)
審査請求日　平成20年11月5日(2008.11.5)
(31)優先権主張番号　60/650,132
(32)優先日　平成17年2月7日(2005.2.7)
(33)優先権主張国　米国(US)

(73)特許権者　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　100090446
弁理士　中島　司朗
(74)代理人　100072442
弁理士　松村　修治
(74)代理人　100125597
弁理士　小林　国人
(72)発明者　中野　稔久
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　石原　秀志
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】記録装置

(57)【特許請求の範囲】
【請求項１】
暗号化データの復号処理に用いられる復号用情報が予め第１領域に記録されている記録媒体に記録を行う記録装置であって、
前記第１領域から前記復号用情報を読み出す読出手段と、
読み出した復号用情報を、前記第１領域のデータを物理的に読み出せない装置が読み出し可能な前記記録媒体の第２領域に記録する記録手段と、
前記第２領域に情報が記録されていることを検出する検出手段と、
前記第２領域に情報が記録されている場合に、当該情報が前記第１領域に記録されている復号用情報であるか否かを判定する判定手段と、
前記判定手段により前記復号用情報でないと判定されたときに、前記復号用情報を前記第２領域に記録する上書き記録手段とを備える
ことを特徴とする記録装置。
【請求項２】
前記復号用情報とは、鍵束である
ことを特徴とする請求項１記載の記録装置。
【請求項３】
前記復号用情報とは、前記記録媒体を識別するメディアIDである
ことを特徴とする請求項１記載の記録装置。
【請求項４】

前記第２領域とは、前記記録媒体のリードイン領域に含まれるバッファ領域である
ことを特徴とする請求項１記載の記録装置。
【請求項５】
前記第１領域とは、前記記録媒体のInitial Zoneである
ことを特徴とする請求項１記載の記録装置。
【請求項６】
記録媒体から暗号化データを読み出して復号する復号処理の実行を制御する再生装置であって、
前記記録媒体は、第１領域および第２領域を備えており、
前記第１領域には、前記暗号化データの復号処理に用いられる復号用情報が、記録装置による前記暗号化データの記録前に予め記録されており、
前記暗号化データは、前記第１領域に予め記録されている復号用情報を用いて、記録対象のデータを暗号化して生成されたデータであり、
前記第２領域には、情報が記録されており、
前記再生装置は、
前記第１領域に記録されている復号用情報と一致する情報が前記第２領域に記録されているか否かを判定する判定手段と、
前記判定手段により一致していないと判定されたとき、前記復号用情報を前記第１領域から読み出して前記復号処理を実行する制御手段とを備える
ことを特徴とする再生装置。
【請求項７】
暗号化データの復号処理に用いられる復号用情報が予め第１領域に記録されている記録媒体に記録を行う記録装置において用いられる集積回路であって、
前記第１領域から前記復号用情報を読み出す処理を行う読出処理部と、
読み出した復号用情報を、前記第１領域のデータを物理的に読み出せない装置が読み出し可能な前記記録媒体の第２領域に記録する処理を行う記録処理部と、
前記第２領域に情報が記録されていることを検出する検出手段と、
前記第２領域に情報が記録されている場合に、当該情報が前記第１領域に記録されている復号用情報であるか否かを判定する判定手段と、
前記判定手段により前記復号用情報でないと判定されたときに、前記復号用情報を前記第２領域に記録する上書き記録手段とを含む
ことを特徴とする集積回路。
【請求項８】
暗号化データの復号処理に用いられる復号用情報が予め第１領域に記録されている記録媒体に記録を行う記録装置に処理を実行させるための制御プログラムであって、
前記第１領域から前記復号用情報を読み出す読出ステップと、
読み出した復号用情報を、前記第１領域のデータを物理的に読み出せない装置が読み出し可能な前記記録媒体の第２領域に記録する記録ステップと、
前記第２領域に情報が記録されていることを検出する検出ステップと、
前記第２領域に情報が記録されている場合に、当該情報が前記第１領域に記録されている復号用情報であるか否かを判定する判定ステップと、
前記判定ステップにより前記復号用情報でないと判定されたときに、前記復号用情報を前記第２領域に記録する上書き記録ステップとを含む
ことを特徴とする制御プログラム。
【請求項９】
記録媒体から暗号化データを読み出して復号する復号処理の実行を制御する再生装置において用いられる集積回路であって、
前記記録媒体は、第１領域および第２領域を備えており、
前記第１領域には、前記暗号化データの復号処理に用いられる復号用情報が、記録装置による前記暗号化データの記録前に予め記録されており、

前記暗号化データは、前記第１領域に予め記録されている復号用情報を用いて、記録対象のデータを暗号化して生成されたデータであり、
前記第２領域には、情報が記録されており、
前記集積回路は、
前記第１領域に記録されている復号用情報と一致する情報が前記第２領域に記録されているか否かを判定する処理を行う判定処理部と、
前記判定処理部により一致していないと判定されたとき、前記復号用情報を前記第１領域から読み出して前記復号処理を実行する制御処理部とを含む
ことを特徴とする集積回路。
【請求項１０】
記録媒体から暗号化データを読み出して復号する復号処理の実行を制御する処理を再生装置に行わせるための制御プログラムであって、
前記記録媒体は、第１領域および第２領域を備えており、
前記第１領域には、前記暗号化データの復号処理に用いられる復号用情報が、記録装置による前記暗号化データの記録前に予め記録されており、
前記暗号化データは、前記第１領域に予め記録されている復号用情報を用いて、記録対象のデータを暗号化して生成されたデータであり、
前記第２領域には、情報が記録されており、
前記制御プログラムは、
前記第１領域に記録されている復号用情報と一致する情報が前記第２領域に記録されているか否かを判定する判定ステップと、
前記判定ステップにより一致していないと判定されたとき、前記復号用情報を前記第１領域から読み出して前記復号処理を実行する制御ステップとを含む
ことを特徴とする制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、記録媒体に記録を行う記録装置に関し、特に、記録媒体の再生互換性を向上させる技術に関する。
【背景技術】
【０００２】
映画などのコンテンツを高品質で記録することができるDVDは、コンテンツを流通させるパッケージ媒体として広く普及している。コンテンツは、デジタルデータとしてDVDに記録される。デジタルデータは、アナログデータと比べると、複製に伴う劣化が極めて小さく、複製によってコンテンツの価値が損なわれることが少ない。そのため、不正なコピーがなされた記録媒体が安価で市場に流通すると、正規のパッケージ媒体を購入しようという消費者の減少をもたらすこととなり、コンテンツの著作権を有する著作権者等の権利者が多大な損害を被るおそれが発生する。
【０００３】
そこで、権利者の権利を保護するために、CPRM(Content Protection forRecordable Media)などの著作権保護技術が用いられている。CPRMとは、書き込み可能な記録媒体にコンテンツなどのデータを記録するときに用いられる著作権保護技術である。記録媒体にデータの記録を行う記録装置は、データの不正な複製を防ぐために、データを暗号化して記録する。このとき、記録媒体の所定の領域に予め記録されている情報を用いてデータの暗号化を行う。例えば、DVD-RAM規格の例で説明すると、記録装置は、記録媒体のInitial Zoneに記録されているMKB(Media Key Block)や、BCA(Burst CuttingArea)に記録されているメディアIDなどを用いてデータの暗号化を行う。
【０００４】
なお、DVDの各規格におけるディスクレイアウトは、DVD+RW規格については下記の非特許文献１に、DVD-RAM規格については、下記の非特許文献２にそれぞれ記載されている。

【非特許文献１】
ECMA-337 3rd Edition - December 2005
【非特許文献２】
ECMA-272 2nd Edition - June 1999
【発明の開示】
【発明が解決しようとする課題】
【０００５】
ところで、上述の非特許文献に記載されているように、DVDの各規格は、規格ごとにディスクレイアウトが異なることがある。ディスクレイアウトが異なると、データの記録位置が異なる場合があるため、再生装置は、対応していない規格に従って記録されている記録媒体を利用できないことがある。そのため、再生装置のユーザに不利益がないよう、再生装置を製造する製造者は、通常、策定されている各規格に、可能な限り対応できるように再生装置を設計して製造する。
【０００６】
しかし、再生装置が製造された後に規格が策定されると、当該再生装置は、装置の仕様上の制約により、新たに策定された規格に従った記録媒体に記録されている暗号化データを復号できないことがある。
例えば、メディアIDなどの、暗号化データの復号処理に用いられる復号用情報が、ディスク状の記録媒体の内周部分に記録されており、記録媒体のデータの読み取りを行う再生装置の読み取り部が物理的に当該内周部分を読み取れない場合、再生装置は復号用情報を読み出せないので暗号化データを復号することができない。この場合、暗号化データの復号に必要な情報が物理的に読み取り不可能なため、再生装置の再生処理を行うプログラムをアップデートする等の対策も効果がない。このように、記録媒体のデータを利用できないことは、再生装置のユーザの不利益になるだけでなく、コンテンツを流通させるコンテンツホルダーにとっても、コンテンツの利用者になりうるユーザへの流通方法の選択肢が狭まることになり、好ましくない。
【０００７】
そこで、装置の仕様上の制約により記録媒体の規格に対応できない再生装置においても当該規格に従って記録されている記録媒体のデータを利用することができるよう、記録媒体へのデータの記録を行う記録装置を提供することを目的とする。
【課題を解決するための手段】
【０００８】
上記課題を解決するため、本発明は、暗号化データの復号処理に用いられる復号用情報が予め第１領域に記録されている記録媒体に記録を行う記録装置であって、前記第１領域から前記復号用情報を読み出す読出手段と、読み出した復号用情報を、前記第１領域のデータを物理的に読み出せない装置が読み出し可能な前記記録媒体の第２領域に記録する記録手段とを備える。
【発明の効果】
【０００９】
上述の構成を備える記録装置は、第１領域から復号用情報を読み出して、読み出した復号用情報を第２領域へ記録する。
したがって、記録媒体の第１領域のデータを物理的に読み出せない装置であっても、第２領域から復号用情報を読み出せるので、記録媒体に記録されている暗号化データを復号することができる。
【００１０】
ところで、第２領域に何らかの情報が記録されている場合に、当該情報が不正な復号用情報であると、再生装置は、その不正な復号用情報を用いて暗号化データを復号することができるので、権利者の権利が十分に保護されないおそれがある。また、第２領域に記録されている復号用情報が、記録失敗などの何らかの事情のために壊れていると、再生装置は暗号化データを復号することができない。

【００１１】
そこで、前記記録装置は、さらに、前記第２領域に情報が記録されていることを検出する検出手段と、前記第２領域に情報が記録されている場合に、当該情報が前記第１領域に記録されている復号用情報であるか否かを判定する判定手段と、前記判定手段により前記復号用情報でないと判定されたときに、前記復号用情報を前記第２領域に記録する上書き記録手段とを備えることとしてもよい。
【００１２】
これにより、正当な復号用情報を、第２領域に確実に記録することができる。
また、前記復号用情報とは、鍵束であることとしてもよい。
また、前記復号用情報とは、前記記録媒体を識別するメディアIDであることとしてもよい。
また、前記第２領域とは、前記記録媒体のリードイン領域に含まれるバッファ領域であることとしてもよい。
【００１３】
また、前記第１領域とは、前記記録媒体のInitial Zoneであることとしてもよい。
また、暗号化データの復号処理に用いられる復号用情報が予め第１領域に記録されている記録媒体に記録を行う記録装置において用いられる集積回路であって、前記第１領域から前記復号用情報を読み出す処理を行う読出処理部と、読み出した復号用情報を、前記第１領域のデータを物理的に読み出せない装置が読み出し可能な前記記録媒体の第２領域に記録する処理を行う記録処理部とを含むこととしてもよい。
【００１４】
また、暗号化データの復号処理に用いられる復号用情報が予め第１領域に記録されている記録媒体に記録を行う記録装置に処理を実行させるための制御プログラムであって、前記第１領域から前記復号用情報を読み出す読出ステップと、読み出した復号用情報を、前記第１領域のデータを物理的に読み出せない装置が読み出し可能な前記記録媒体の第２領域に記録する記録ステップとを含むこととしてもよい。
【００１５】
ところで、再生装置の中には、規格に対応して、記録媒体の第１領域および第２領域を共に読み出せる装置がある。この再生装置は、復号用情報が第２領域に記録されていると、第１領域、第２領域いずれの領域からも復号用情報を読み出すことができる。
しかし、第２領域に記録されている情報が、不正な記録装置によって記録された不正な情報であるときがある。この場合、再生装置が、記録媒体の第２領域に記録された不正な情報を用いて暗号化データを復号すると、データの著作権を有する権利者等に不利益を及ぼすこととなる。
【００１６】
そこで、記録媒体から暗号化データを読み出して復号する復号処理の実行を制御する再生装置であって、前記記録媒体は、第１領域および第２領域を備えており、前記第１領域には、前記暗号化データの復号処理に用いられる復号用情報が、記録装置による前記暗号化データの記録前に予め記録されており、前記暗号化データは、前記第１領域に予め記録されている復号用情報を用いて、記録対象のデータを暗号化して生成されたデータであり、前記第２領域には、情報が記録されており、前記再生装置は、前記第１領域に記録されている復号用情報と一致する情報が前記第２領域に記録されているか否かを判定する判定手段と、前記判定手段による判定結果に応じて、前記復号処理の実行を制御する制御手段とを備えることとしてもよい。
【００１７】
上述の構成を備える再生装置は、第１領域および第２領域に記録されている情報が一致しているか否かを判定する。判定結果に応じて、暗号化データの復号処理の実行を制御する。
したがって、不正な情報が第２領域に記録されていたとしても、権利者等の不利益にならないよう、暗号化データの復号処理の実行を制御することができる。

【００１８】
ここで、前記制御手段は、前記判定手段により一致していると判定されたときに限り、前記復号処理を実行することとしてもよい。
これにより、規格に対応して第１および第２領域をともに読み出せる再生装置においては、第１領域に記録されている復号用情報と一致する情報が第２領域に記録されている場合に限って暗号化データの復号処理を行うので、第２領域に不正な情報が記録されたとしても、権利者等の不利益を防ぐことができる。
【００１９】
また、前記制御手段は、前記判定手段により一致していないと判定されたとき、前記復号処理を中止することとしてもよい。
これにより、第２領域に不正な情報が記録されている場合は、復号処理そのものを中止するので、不正者にとっては、第２領域に不正な情報を記録する利益が無くなる。したがって、不正者が第２領域に不正な情報を記録する行為を抑制しうる。
【００２０】
とはいえ、第１領域に記録されている復号用情報と一致する情報が第２領域に記録されていないからといって、必ずしも第２領域の情報が不正者によって記録されたものであるとは限らない。例えば、正当な権利者によって第２領域に復号用情報が記録された後に、記録媒体の劣化や損傷により、第２領域に記録された情報が破損する場合などが考えられる。
【００２１】
このような場合、すなわち記録媒体の破損等のために第１領域に記録されている復号用情報と一致する情報が第２領域に記録されていない場合に、再生装置が第１領域から復号用情報を読み出せるにもかかわらず、暗号化データの復号を再生装置が行えないとなると、権利者等の権利が侵害されていないにもかかわらず記録媒体のデータの利用を制限することとなり、再生装置のユーザにとって不当に不利益となる。
【００２２】
そこで、前記制御手段は、前記判定手段により一致していないと判定されたとき、前記復号用情報を前記第１領域から読み出して前記復号処理を実行することとしてもよい。
これにより、上述の場合において、再生装置のユーザが不当に不利益になるのを防ぐことができる。
また、記録媒体から暗号化データを読み出して復号する復号処理の実行を制御する再生装置において用いられる集積回路であって、前記記録媒体は、第１領域および第２領域を備えており、前記第１領域には、前記暗号化データの復号処理に用いられる復号用情報が、記録装置による前記暗号化データの記録前に予め記録されており、前記暗号化データは、前記第１領域に予め記録されている復号用情報を用いて、記録対象のデータを暗号化して生成されたデータであり、前記第２領域には、情報が記録されており、前記集積回路は、前記第１領域に記録されている復号用情報と一致する情報が前記第２領域に記録されているか否かを判定する処理を行う判定処理部と、前記判定部による判定結果に応じて、前記復号処理の実行を制御する処理を行う制御処理部とを含むこととしてもよい。
【００２３】
また、記録媒体から暗号化データを読み出して復号する復号処理の実行を制御する処理を再生装置に行わせるための制御プログラムであって、前記記録媒体は、第１領域および第２領域を備えており、前記第１領域には、前記暗号化データの復号処理に用いられる復号用情報が、記録装置による前記暗号化データの記録前に予め記録されており、前記暗号化データは、前記第１領域に予め記録されている復号用情報を用いて、記録対象のデータを暗号化して生成されたデータであり、前記第２領域には、情報が記録されており、前記制御プログラムは、前記第１領域に記録されている復号用情報と一致する情報が前記第２領域に記録されているか否かを判定する判定ステップと、前記判定ステップによる判定結果に応じて、前記復号処理の実行を制御する制御ステップとを含むこととしてもよい。
【発明を実施するための最良の形態】

＜実施の形態＞
以下、本発明にかかる記録装置の実施の一形態について、図面を用いて説明する。
【００２４】
＜概要＞
本発明の記録装置は、CPRM(Content Protection for RecordableMedia)に対応している記録媒体にAVデータを記録する。AVデータを記録する際に、記録媒体に予め記録されている情報を用いてAVデータを暗号化して記録する。暗号化の方法は、CPRMを用いるものとする。記録媒体に予め記録されている情報とは、鍵の束であるMKB(Media Key Block)やMKB Validation DataやMediaIDである。
【００２５】
MKBは、記録媒体のInitial Zoneという領域に予め記録されている。MKB Validation DataおよびMediaIDは、Initial Zone内のBCA(Burst Cutting Area)に予め記録されている。
記録装置は、これらMKBやMediaIDなどを用いてAVデータの暗号を行う。また、記録装置は、仕様上の制約により記録媒体からMKBやMediaIDなどを物理的に読み出せない再生装置でもMKBなどを用いてAVデータの復号ができるよう、当該再生装置が読み出し可能な記録媒体の所定領域に、MKBなどを記録する。これにより、当該再生装置は、記録媒体からMKBなどを読み出すことができ、AVデータの復号ができるようになる。以下の実施形態では、一例として記録装置が記録媒体のBufferZone 2にMKBなどを記録する場合を説明している。
【００２６】
さらに、記録装置は、Buffer Zone 2に既に情報が記録されている場合、その情報が、記録媒体のInitial Zoneに予め記録されているMKBやMediaIDであるかを検証し、検証結果に応じて、Buffer Zone 2にMKBやMediaIDを上書きする。
また、再生装置は、記録媒体のInitial Zoneに記録されている情報は読み出せないが、記録媒体のBuffer Zone 2に記録されている情報は読み出せるものとする。
【００２７】
以下、具体的に説明する。
＜構成＞
図１は、本発明の記録装置１０００の機能ブロック図である。なお、同図には記録媒体２０００も示している。
同図に示すように、記録装置１０００は、デバイス鍵記憶部１０１と、MKB処理部１０２と、チェック部１０３と、鍵変換部１０４と、暗号化部１０５と、AVパック記憶部１０６とからなる。暗号化部１０５は、タイトル鍵生成部１１１と、タイトル鍵結合部１１２と、タイトル鍵暗号化部１１３と、DCL_CCI生成部１１４と、中間鍵生成部１１５と、コンテンツ鍵生成部１１６と、AVパック暗号化部１１７とを含む。
【００２８】
デバイス鍵記憶部１０１は、記録装置１０００に割り当てられているデバイス鍵を記憶している。
MKB処理部１０２は、記録媒体２０００のInitialZoneからMKBを読み出して、デバイス鍵記憶部１０１が記憶している記録装置１０００のデバイス鍵を用いてMKBを復号してメディア鍵（Km）を生成する。また、生成したメディア鍵を記録媒体２０００のBuffer Zone 2に記録する。
【００２９】
チェック部１０３は、Initial Zoneに記録されているMKBのハッシュ値を計算し、BCAに記録されているMKB Validation Dataと比較してMKBの正当性を検証する。また、Buffer Zone 2に情報が記録されていることを検出する機能を有しており、Buffer Zone 2にMKBが記録されていることを検出したときは、Buffer Zone 2に記録されているMKBのハッシュ値を計算し、MKB Validation Dataと比較してBuffer Zone 2に記録されているMKBの正当性を検証する。また、Buffer Zone 2にMediaIDが記録されていることを検出したときは、BCAに記録されているMediaIDと、Buffer Zone 2に記録されているMediaIDとを比較すること

により、Buffer Zone 2に記録されているMediaIDの正当性を検証する。例えば、上述の比較の結果、各々のMediaIDが同一である場合に、BZ2に記録されているMediaIDが正当であると判定する。

【００３０】

鍵変換部１０４は、BCAに記録されているMediaIDを読み出し、読み出したMediaIDを用いて、MKB処理部１０２が読み出したMKBを変換して、メディア固有鍵（Kmu）を生成する。また、BCAから読み出したMediaIDを、BufferZone 2に記録する。

暗号化部１０５は、2048バイトのAV Pack形式でAVパック記憶部１０６から入力されるAVデータを暗号化し、暗号化したデータを記録媒体２０００のData Areaに記録する。暗号化部１０５によって暗号化されたAVデータは、2048バイトのEncrypted AV Pack形式でData Areaに記録される。Encrypted AV Packは、2048バイト中、先頭128バイトは平文のUnencrypted Portionであり、残りの1920バイトは暗号化されたEncrypted Portionである。AVパック記憶部１０６から入力される2048バイトのAV Packのうち、先頭の128バイトは、AVデータを暗号化するためのコンテンツ鍵（Kc）の生成に用いられるとともに、平文のUnencrypted PortionとしてData Areaに記録される。また、暗号化部１０５は、2048バイトのAV Packのうち、先頭128バイトを除いた残りの1920バイトを、コンテンツ鍵を用いて暗号化し、Encrypted PortionとしてData Areaに記録する。

【００３１】

ここで、暗号化部１０５を構成する各機能ブロックについて、詳しく説明する。

タイトル鍵生成部１１１は、タイトル鍵を生成する。生成したタイトル鍵を、タイトル鍵結合部１１２および中間鍵生成部１１５へ出力する。

タイトル鍵結合部１１２は、任意の値Vと、タイトル鍵生成部１１１が生成したタイトル鍵とを結合する。

【００３２】

タイトル鍵暗号化部１１３は、タイトル鍵結合部１１２による結合がなされたタイトル鍵を、鍵変換部１０４が生成したメディア固有鍵を用いて暗号化して暗号化タイトル鍵を生成する。生成した暗号化タイトル鍵を、Data Areaに記録する。

DCL_CCI生成部１１４は、AVデータのコピー制御情報などを、DCL_CCIとして生成し、生成したDCL_CCIをData Areaに記録する。また、アナログプロテクション情報（APSTB:Analog Protection SingleTrigger Bit）を中間鍵生成部１１５へ出力する。

【００３３】

中間鍵生成部１１５は、DCL_CCI生成部１１４からAPSTBを受け付けて、受け付けたAPSTBを、タイトル鍵生成部１１１から受け付けたタイトル鍵と結合して中間鍵（Ki）を生成する。生成した中間鍵を、コンテンツ鍵生成部１１６へ出力する。

コンテンツ鍵生成部１１６は、2048 バイトのAV Packのうち、先頭 128 バイト（Dtkc）の入力を受け付けて、受け付けたAV Packの先頭128バイトを用いて、中間鍵生成部１１５から受け付けた中間鍵を変換してコンテンツ鍵を生成する。なお、AV Packの先頭128バイトは、上述したように、平文のUnencrypted AV PackとしてData Areaに記録される。

【００３４】

AVパック暗号化部１１７は、2048バイトのAV Packのうち、後半1920バイトを、コンテンツ鍵生成部１１６が生成したコンテンツ鍵を用いて暗号化し、Encrypted PortionとしてData Areaに記録する。

AVパック記憶部１０６は、AVデータを記憶している。

次に、再生装置の構成について説明する。

【００３５】

図２は、記録媒体２０００からデータを読み出して復号処理を行う再生装置３０００の機能ブロック図である。

同図に示すように、再生装置３０００は、デバイス鍵記憶部３０１と、MKB処理部３０２と、鍵変換部３０３と、復号部３０４と、AVパック再生処理部３０５とからなる。復号部３０４は、タイトル鍵復号部３１１と、DCL_CCI記憶部３１２と、中間鍵生成部３１３

と、コンテンツ鍵生成部３１４と、AVパック復号部３１５とを含む。

【００３６】

デバイス鍵記憶部３０１は、再生装置３０００のデバイス鍵を記憶している。

MKB処理部３０２は、記録媒体２０００のBufferZone 2に記録されているMKBを読み出して、デバイス鍵記憶部３０１が記憶している再生装置３０００のデバイス鍵を用いてMKBを復号してメディア鍵を生成する。

鍵変換部３０３は、Buffer Zone 2に記録されているMediaIDを読み出し、読み出したMediaIDを用いて、MKB処理部３０２が生成したメディア鍵を変換して、メディア固有鍵を生成する。

【００３７】

復号部３０４は、記録媒体２０００のData AreaからEncryptedAV Packを読み出し、読み出したEncrypted AV Packを復号してAVデータを得る。得たAVデータをAVパック再生処理部３０５へ出力する。また、Data AreaからDCL_CCIを読み出して記憶する。

ここで、復号部３０４を構成する各機能ブロックについて、詳しく説明する。

タイトル鍵復号部３１１は、記録媒体２０００のData Areaから暗号化タイトル鍵を読み出し、読み出した暗号化タイトル鍵を、鍵変換部３０３が生成したメディア固有鍵を用いて復号してタイトル鍵を生成する。

【００３８】

DCL_CCI記憶部３１２は、Data Areaから読み出されたDCL_CCIを記憶する。

中間鍵生成部３１３は、Data Areaに記録されているDCL_CCIに含まれるアナログプロテクション情報（APSTB）を受け付けて、タイトル鍵復号部３１１が生成したタイトル鍵と結合して中間鍵を生成する。生成した中間鍵を、コンテンツ鍵生成部３１４へ出力する。

コンテンツ鍵生成部３１４は、Data Areaから読み出したEncryptedAV Packの先頭128バイトを用いて、中間鍵生成部３１３から受け付けた中間鍵を変換してコンテンツ鍵を生成する。

【００３９】

AVパック復号部３１５は、Encrypted AV Packの後半1920バイトを、コンテンツ鍵生成部３１４が生成したコンテンツ鍵を用いて復号する。

AVパック再生処理部３０５は、復号部３０４が復号したAVデータの映像出力や再生処理を行う。

なお、記録装置１０００や再生装置３０００は、図示していないが記録媒体２０００からデータを読み取る読み取り部を備えている。また、上述の各構成要素は、具体的にはCPU(Central Processing Unit)、ROM(Read OnlyMemory)、RAM(Random Access Memory)等からなるコンピュータシステムを構成しており、プログラムにしたがって動作する。暗号化処理など一部の処理は、専用のプロセッサが行うこととしてもよい。

【００４０】

＜データ＞

次に、記録媒体２０００のディスクレイアウトについて説明する。

図３は、記録媒体２０００のディスクレイアウトを示した図である。なお、本実施形態では、DVD+RW規格を例にして説明している。

同図に示すように、記録媒体２０００のInner Drive Areaには、Initial Zoneが含まれる。Initial ZoneのBCAには、予めMediaIDおよびMKB Validation Dataが記録されている。BCAに記録されている情報は、改ざんすることができない。また、Initial Zoneには、MKBが予め記録されている。また、Lead-inには、Buffer Zone 2が含まれる。

【００４１】

本実施形態では、記録装置１０００は、記録媒体２０００のInitial Zoneから読み出したMKBおよびMediaIDを、記録媒体２０００のBuffer Zone 2に記録することとする。また、上述したように、再生装置３０００は、Initial Zoneに記録されている情報を読み出せないものとし、記録装置１０００によってBuffer Zone 2に記録されたMKBおよびMediaIDを読み出して復号処理を行うものとする。

【００４２】
＜動作＞
次に、本発明の記録装置１０００の動作について説明する。
図４は、記録装置１０００の動作処理を示すフローチャートである。
同図に示すように、記録装置１０００は、記録媒体２０００のBuffer Zone 2を読み込んで、Buffer Zone 2にMKBおよびMediaIDが記録されているか否かを判断する（ステップＳ４１）。
【００４３】
Buffer Zone 2にMKBおよびMediaIDが記録されていないと判断した場合（ステップＳ４１：NO）、MKBおよびMediaIDをBuffer Zone 2に書き込む空き容量があるか否かを判断し（ステップＳ４２）、空き容量がなければ処理を終了する（ステップＳ４２：NO）。Buffer Zone 2に空き容量があれば（ステップＳ４２：YES）、Initial ZoneにMKBおよびMediaIDが記録されているかを判断し、記録されていなければ処理を終了する（ステップＳ４３：NO）。Initial ZoneにMKBおよびMediaIDが記録されていれば（ステップＳ４３：YES）、Initial ZoneからMKBおよびMediaIDを取得する（ステップＳ４４）。取得したMKBおよびMediaIDを、Buffer Zone 2に記録する（ステップＳ４５）。
【００４４】
ステップＳ４５の処理を終えると、MKB、MediaID、タイトル鍵などを用いてAVパック記憶部１０６に記憶されているAVデータを暗号化してData Areaに記録する（ステップＳ４６）。
また、ステップＳ４１において、Buffer Zone 2にMKBおよびMediaIDが記録されていると判断した場合（ステップＳ４１：YES）、Buffer Zone 2に記録されているMKBを読み出すとともに、Initial ZoneからMKB Validation Dataを読み出して、チェック部１０３においてBufferZone 2に記録されているMKBが正当であるかを検証する（ステップＳ４７）。
【００４５】
ステップＳ４７において、MKBが正当でない場合（ステップＳ４７：NO）は処理を終了する。ステップＳ４７において、MKBが正当であれば（ステップＳ４７：YES）、同様にチェック部１０３においてBuffer Zone 2に記録されているMediaIDが正当であるかを検証する（ステップＳ４８）。
ステップＳ４８において、MediaIDが正当でない場合（ステップＳ４８：NO）は、Initial Zoneに記録されているMediaIDを、BufferZone 2に記録されているMediaIDに上書きする（ステップＳ４９）。また、ステップＳ４８において、MediaIDが正当である場合（ステップＳ４８：YES）は、ステップＳ４９の上書き処理を行わない。その後、MKB、MediaID、タイトル鍵などを用いてAVパック記憶部１０６に記憶されているAVデータを暗号化してData Areaに記録する（ステップＳ４６）。なお、ステップＳ４６における暗号化処理は、上述の暗号化部１０５の説明において詳しく述べたように、CPRMにおける暗号化処理と同様のものを用いて行うこととする。また、ステップＳ４７において、MKBが正当でない場合は処理を終了すると説明したが（ステップＳ４７：NO）、これに限らず、Initial Zoneに記録されているMKBを、Buffer Zone 2に記録されているMKBに上書きすることとしてもよい。また、ステップＳ４８において、MediaIDが正当でない場合（ステップＳ４８：NO）は、Initial Zoneに記録されているMediaIDをBufferZone 2に記録されているMediaIDに上書きする（ステップＳ４９）と説明したが、これに限らず、処理を終了するとしてもよい。
【００４６】
次に、再生装置３０００の動作について説明する。
図５は、再生装置３０００の動作処理を示すフローチャートである。
同図に示すように、再生装置３０００は、Buffer Zone 2にMKBおよびMediaIDが記録されているか判断する（ステップＳ５１）。記録されていると判断した場合は（ステップＳ５１：YES）、Buffer Zone 2からMKBおよびMediaIDを取得する（ステップＳ５２）。

【００４７】
MKBおよびMediaIDを取得すると（ステップＳ５２）、取得したMKBおよびMediaIDを用いてAVデータを復号する（ステップＳ５３）。
また、ステップＳ５１において、Buffer Zone 2に記録されていないと判断した場合は（ステップＳ５１：NO）、処理を終了する。
＜補足＞
以上のように本発明にかかる記録装置について実施の形態に基づいて説明したが、以下のように変形することもでき、本発明は上述の実施の形態で示した記録装置に限られないことは勿論である。
（１）上述の実施形態では、再生装置は、Initial Zoneの情報を読み出せないこととして説明してきたが、これに限らず、Initial Zoneの情報を読み出せる装置であってもよい。
【００４８】
この場合、さらに、再生装置は、図６に示す再生装置３１００のように、Initial ZoneおよびBuffer Zone 2からMKB等を読み出して正当性を検証するチェック部３０６を備えることとしてもよい。チェック部３０６は、Buffer Zone 2に記録されているMKBのハッシュ値を計算し、BCAに記録されているMKB Validation Dataと比較して、Buffer Zone 2に記録されているMKBの正当性を検証する。また、Buffer Zone 2に記録されているMediaIDと、BCAに記録されているMediaIDとを比較して、Buffer Zone 2に記録されているMediaIDの正当性を検証する。
【００４９】
これにより、再生装置３１００は、記録媒体２０００のBuffer Zone 2に記録されているMKBやMediaIDの正当性を検証することができる。
さらに、検証の結果、正当でない場合は、復号化等の処理を終了させることとしてもよい。このような再生装置３１００の動作処理のフローチャートを、図７に示す。
同図に示すように、再生装置３１００は、Buffer Zone 2にMKBおよびMediaIDが記録されているか判断する（ステップＳ７１）。Buffer Zone 2に記録されていないと判断したときは（ステップＳ７１：NO）、Initial ZoneからMKBおよびMediaIDを取得し（ステップＳ７４）、取得したMKBおよびMediaIDを用いてAVデータを復号する（ステップＳ７５）。
【００５０】
ステップＳ７１において、Buffer Zone 2に記録されていると判断したときは（ステップＳ７１：YES）、チェック部３０６がBuffer Zone 2に記録されているMKBの正当性を検証する（ステップＳ７２）。Buffer Zone 2に記録されているMKBが正当であるとき、すなわちBuffer Zone 2に記録されているMKBがInitial Zoneに記録されているMKBと同一であるときは（ステップＳ７２：YES）、同様にBuffer Zone 2に記録されているMediaIDの正当性を検証し（ステップＳ７３）、Buffer Zone 2に記録されているMediaIDが正当であれば（ステップＳ７３：YES）、Buffer Zone 2またはInitial ZoneからMKBおよびMediaIDを取得し（ステップＳ７４）、取得したMKBおよびMediaIDを用いてAVデータを復号する（ステップＳ７５）。
【００５１】
また、ステップＳ７２やステップＳ７３において、Buffer Zone 2に記録されているMKBやMediaIDが正当でない場合は（ステップＳ７２：NO、ステップＳ７３：NO）、AVデータの復号を行わずに処理を終了する。
なお、ステップＳ７２およびステップＳ７３において、検証の結果、Buffer Zone 2に記録されているMKBやMediaIDが正当でない場合（ステップＳ７２：NO、ステップＳ７３：NO）、InitialZoneに記録されているMKB等を用いて復号化等の処理を行うこととしてもよい。
（２）上述の実施形態では、記録装置１０００は、Initial Zoneに記録されている情報を読み出して、読み出した情報をBuffer Zone 2に記録することとして説明してきたが、Buffer Zone 2限らず、Data Areaなど他の領域に記録することとしてもよい。
【００５２】

また、Buffer Zone 2に記録する情報は、ADIP（Address In Pre-groove）としてもよい。

また、Initial Zoneに記録されている情報に限らず、他の領域に記録されている情報を、Buffer Zone 2などに記録することとしてもよい。

（３）上述の実施形態では、MediaIDを読み出したり記録したりするものとして説明してきたが、MediaIDに限らず、MediaIDシードであってもよい。MediaIDシードを乱数生成関数で処理することによりMediaIDが生成される。

（４）上述の実施形態では、記録媒体として、CPRMに対応したDVD+RWメディアを用いる場合を例にして説明したが、これに限らず、光ディスクその他の記録媒体に記録する場合も本発明に含まれる。

（５）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレィユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。ここで、コンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

（６）上記の各装置を構成する構成要素の一部又は全部は、１個のシステムＬＳＩ（Large Scale Integration：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムＬＳＩは、その機能を達成する。

（７）上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なＩＣカード又は単体のモジュールから構成されているとしてもよい。前記ＩＣカード又は前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、などから構成されるコンピュータシステムである。前記ＩＣカード又は前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ＩＣカード又は前記モジュールは、その機能を達成する。このＩＣカード又はこのモジュールは、耐タンパ性を有するとしてもよい。

（８）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【００５３】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【００５４】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

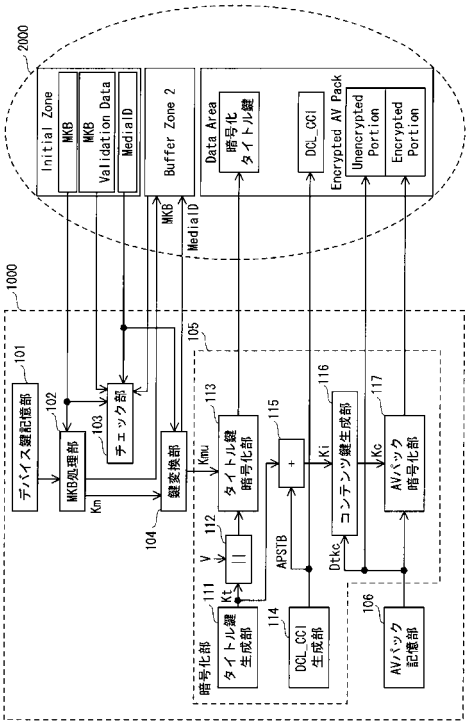
また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【００５５】

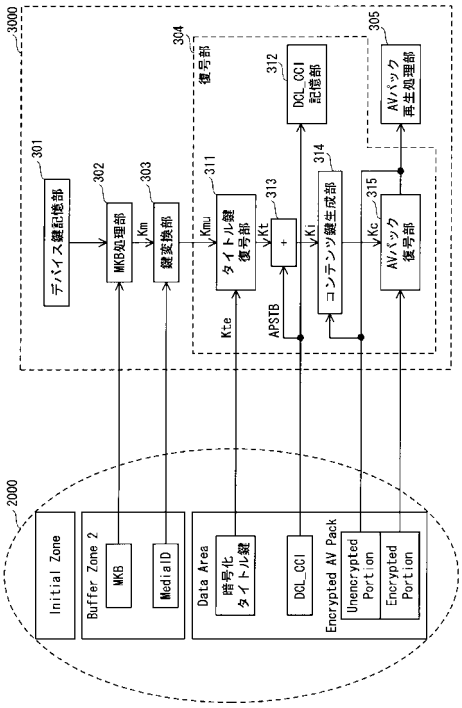
また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送す

ることにより、独立した他のコンピュータシステムにより実施するとしてもよい。
（９）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい
【産業上の利用可能性】
【００５６】
本発明は、複数の規格が策定されているDVDなどの記録媒体に、コンテンツなどのデータの記録を行う記録装置において、用いることができる。
【図面の簡単な説明】
【００５７】
【図１】本発明の記録装置１０００の機能ブロック図である。
【図２】記録媒体２０００からデータを読み出して復号する再生装置３０００の機能ブロック図である。
【図３】記録媒体２０００のディスクレイアウトを示す図である。
【図４】記録装置１０００の動作処理を示すフローチャートである。
【図５】再生装置３０００の動作処理を示すフローチャートである。
【図６】再生装置３１００の機能ブロック図である。
【図７】再生装置３１００の動作処理を示すフローチャートである。
【符号の説明】
【００５８】
１０１　デバイス鍵記憶部
１０２　MKB処理部
１０３　チェック部
１０４　鍵変換部
１０５　暗号化部
１０６　AVパック記憶部
１１１　タイトル鍵生成部
１１２　タイトル鍵結合部
１１３　タイトル鍵暗号化部
１１４　DCL_CCI生成部
１１５　中間鍵生成部
１１６　コンテンツ鍵生成部
１１７　AVパック暗号化部
３０１　デバイス鍵記憶部
３０２　MKB処理部
３０３　鍵変換部
３０４　復号部
３０５　AVパック再生処理部
３０６　チェック部
３１１　タイトル鍵復号部
３１２　DCL_CCI記憶部
３１３　中間鍵生成部
３１４　コンテンツ鍵生成部
３１５　AVパック復号部

【図１】



【図２】



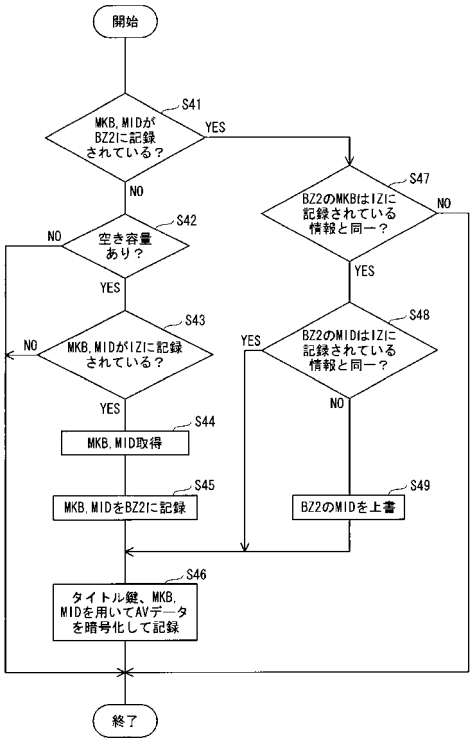
【図３】

	Description	Nominal radius in mm
Inner Drive Area	Initial Zone	start 22.000mm
	Inner Disk Test Zone	start 22.616mm
	Count Zone Run-in	start 23.052mm
	Inner Disk Count Zone	start 23.079mm
	Inner Disk Administration Zone	start 23.186mm
	Table of Contents Zone	start 23.293mm
Lead-in	Guard Zone 1	start 23.400mm
	Reserved Zone 1	
	Reserved Zone 2	
	Inner Disk Identification Zone	
	Reserved Zone 3	
	Reference Code Zone	start 23.896mm
	Buffer Zone 1	
	Control Data Zone	
	Buffer Zone 2	
Data	Data Zone	start 24.000mm
Lead-out	Buffer Zone 3	start 58.000mm (at full capacity)
	Outer Disk Identification Zone	
	Guard Zone 2	
Outer Drive Area	Outer Disk Administration Zone	start 58.053mm
	Outer Disk Count Zone	start 58.096mm
	Outer Disk Test Zone	start 58.139mm
	Guard Zone 3	start 58.310mm end ≧58.500mm

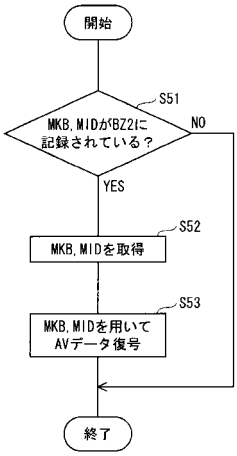
pre-record (BCA): MediaID, MKB Validation Data, MKB

record: MediaID, MKB

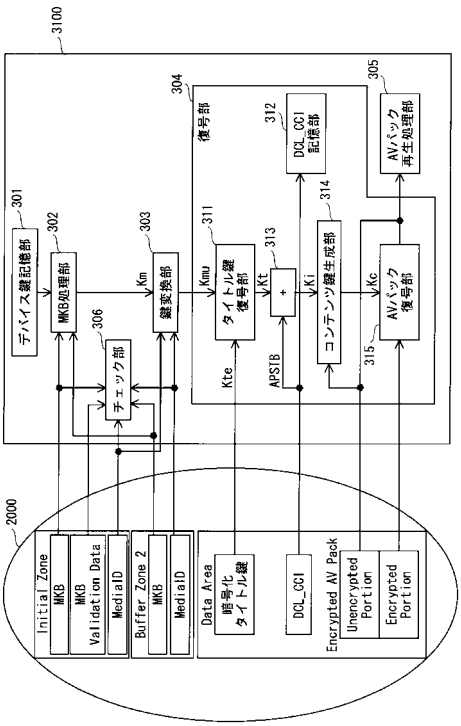
【図４】



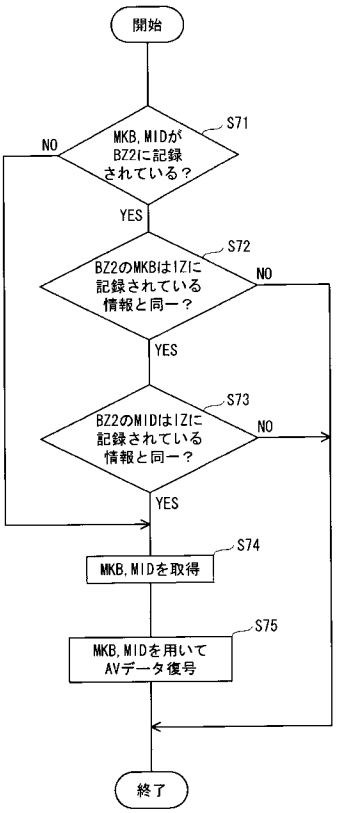
【図５】


開始
S51
MKB,MIDがBZ2に記録されている？
NO
YES
S52
MKB,MIDを取得
S53
MKB,MIDを用いてAVデータ復号
終了

【図６】


3100
301
デバイス鍵記憶部
302
MKB処理部
303
鍵変換部
304
復号部
305
AVトラック再生処理部
306
チェック部
311
タイトル鍵復号部
312
DCL_CCI記憶部
313
314
コンテンツ鍵生成部
315
AVトラック復号部
Km
Kmu
Kte
Ki
Kc
APSTB
2000
Initial Zone
MKB
MKB Validation Data
MediaID
Buffer Zone 2
MKB
MediaID
Data Area
暗号化タイトル鍵
DCL_CCI
Encrypted AV Pack
Unencrypted Portion
Encrypted Portion

【図７】


開始
S71
MKB,MIDがBZ2に記録されている？
NO
YES
S72
BZ2のMKBはIZに記録されている情報と同一？
NO
YES
S73
BZ2のMIDはIZに記録されている情報と同一？
NO
YES
S74
MKB,MIDを取得
S75
MKB,MIDを用いてAVデータ復号
終了

フロントページの続き

(72)発明者　村木　健司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　小塚　雅之
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

審査官　松尾　淳一

(56)参考文献　特開２０００－０７６１４１（ＪＰ，Ａ）
特開２０００－１６３８８３（ＪＰ，Ａ）
特開２００１－１８９０１５（ＪＰ，Ａ）
特開２００２－０７３３９６（ＪＰ，Ａ）
特表２００３－５３６１９３（ＪＰ，Ａ）
特開２００４－１８６８２５（ＪＰ，Ａ）
特開２００４－２２０３１７（ＪＰ，Ａ）
特表２００４－５２２２４５（ＪＰ，Ａ）
特開２００５－５０２９７５（ＪＰ，Ａ）
特表２００８－５２７８１６（ＪＰ，Ａ）
特許第３１６９３６６（ＪＰ，Ｂ２）
国際公開第２００６／０７４９８７（WO，Ａ１）
欧州特許出願公開第００８０２５２７（ＥＰ，Ａ１）
欧州特許出願公開第００９９７８９９（ＥＰ，Ａ１）
欧州特許出願公開第０１０５８２５４（ＥＰ，Ａ１）
米国特許第０６７８２１９０（ＵＳ，Ｂ１）
米国特許出願公開第２００２／０１４１５７６（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 12/14
G06F 21/02-21/06
G06F 21/24
G11B 20/10-20/16