(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2006-31818
(P2006-31818A)
(43)公開日　平成18年2月2日(2006.2.2)

(51)Int.Cl.		F I			テーマコード（参考）
G11B 20/10	(2006.01)	G11B	20/10	H	5B017
G06F 21/24	(2006.01)	G11B	20/10	D	5C053
G09C 1/00	(2006.01)	G11B	20/10	301Z	5D044
G11B 20/12	(2006.01)	G06F	12/14	530C	5D110
G11B 27/00	(2006.01)	G06F	12/14	530P	5J104

審査請求 未請求　請求項の数 15　ＯＬ　（全 34 頁）　最終頁に続く

(21)出願番号　特願2004-209116 (P2004-209116)
(22)出願日　平成16年7月15日 (2004.7.15)

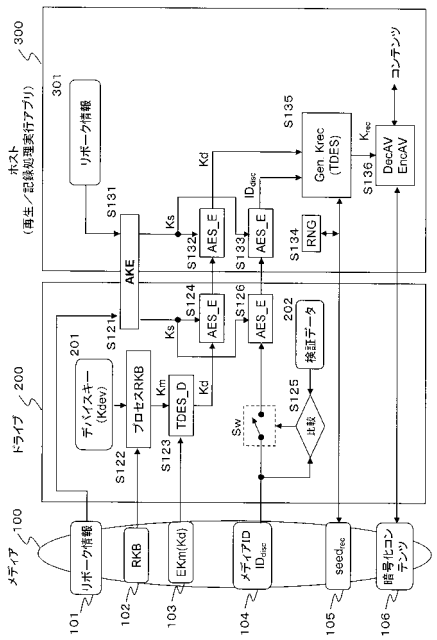
（特許庁注：以下のものは登録商標）
１．レーザーディスク

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　木谷　聡
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　村松　克美
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、および情報処理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】　異なるデバイス間のデータ転送を伴うコンテンツ利用における情報漏洩、コンテンツ不正処理を防止する構成を提供する。
【解決手段】　ドライブとホストなど異なるデバイス間のデータ転送を伴うコンテンツの再生あるいは記録処理において、コンテンツの暗号化または復号処理に適用するメディアＩＤ（ディスクＩＤ）を、メディアから読み取り、これが正しい正当なメディアに設定されたヘッダコードに対応して記録されているかをドライブ側で検証し、検証によって、正当メディアであると確認された場合、ドライブ側でメディアＩＤを暗号化してホストに出力する。本構成により、メディアＩＤの外部漏洩の防止、不正メディアを利用したコンテンツの再生または記録処理の防止が実現される。
【選択図】　図６



【特許請求の範囲】
【請求項１】
情報処理装置であり、
情報記録媒体に対する書き込みデータ、または情報記録媒体からの読み取りデータの入出力を実行する記録媒体インタフェースと、
外部機器との転送データの入出力を実行するデータ転送用インタフェースと、
情報記録媒体の正当性を確認するための検証データを格納した記憶部と、
前記情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取り、該コードと前記検証データとの照合処理により情報記録媒体の正当性確認処理を実行し、正当性が確認されたことを条件として前記メディア識別子を暗号化して外部出力する処理を実行するデータ処理部と、
を有することを特徴とする情報処理装置。
【請求項２】
前記データ処理部は、
前記データ転送用インタフェースを介したデータ入出力を実行する外部機器との認証処理を実行し、該認証処理の成立を条件として、前記メディア識別子の前記外部機器への出力処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記データ処理部は、
前記認証処理において生成したセッションキーを適用して、前記メディア識別子の暗号化処理を実行し、セッションキーに基づく暗号化データとして前記メディア識別子を外部機器に出力する構成であることを特徴とする請求項２に記載の情報処理装置。
【請求項４】
前記記憶部は、
ライセンスに基づいて正当に製造された情報記録媒体の識別子に対応して設定されるコード情報を格納し、
前記データ処理部は、
前記情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取り、該コードと前記検証データとして格納されたコードとの照合処理により情報記録媒体の正当性確認処理を実行し、正当性が確認されたことを条件として前記メディア識別子を暗号化して外部出力する処理を実行することを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記データ処理部は、
情報記録媒体のＢＣＡ（バースト・カッティング・エリア）に記録されたメディア識別子の対応情報としてのコードを読み取り、該コードと前記検証データとの照合処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記データ処理部は、
前記データ転送用インタフェースを介して、外部機器から前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを入力し、
該入力データの情報記録媒体に対する書き込み処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項７】
前記データ処理部は、
前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを前記情報記録媒体から読み取り、
該読み取りデータを前記データ転送用インタフェースを介して外部機器に出力する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項８】

情報処理方法であり、
情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取るコード読み取りステップと、
前記コードと、記憶部に格納された検証データとの照合処理により情報記録媒体の正当性確認処理を実行する正当性確認ステップと、
前記正当性確認ステップにおいて、情報記録媒体の正当性が確認されたことを条件として前記メディア識別子を暗号化して外部出力するメディア識別子出力ステップと、
を有することを特徴とする情報処理方法。
【請求項９】
前記情報処理方法は、さらに、
前記データ転送用インタフェースを介したデータ入出力を実行する外部機器との認証処理を実行する認証処理実行ステップを有し、該認証処理の成立を条件として、前記メディア識別子の前記外部機器への出力処理を実行することを特徴とする請求項８に記載の情報処理方法。
【請求項１０】
前記メディア識別子出力ステップは、
前記認証処理において生成したセッションキーを適用して、前記メディア識別子の暗号化処理を実行し、セッションキーに基づく暗号化データとして前記メディア識別子を外部機器に出力するステップであることを特徴とする請求項９に記載の情報処理方法。
【請求項１１】
前記正当性確認ステップは、
前記情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取り、該コードと、記憶部に格納されたライセンスに基づいて正当に製造された情報記録媒体の識別子に対応して設定されるコードとの照合処理により情報記録媒体の正当性確認処理を実行するステップであることを特徴とする請求項８に記載の情報処理方法。
【請求項１２】
前記コード読み取りステップは、
情報記録媒体のＢＣＡ（バースト・カッティング・エリア）に記録されたメディア識別子の対応情報としてのコードを読み取るステップであることを特徴とする請求項８に記載の情報処理方法。
【請求項１３】
前記情報処理方法は、さらに、
前記データ転送用インタフェースを介して、外部機器から前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを入力するステップと、
該入力データの情報記録媒体に対する書き込み処理を実行するステップと、
を有することを特徴とする請求項８に記載の情報処理方法。
【請求項１４】
前記情報処理方法は、さらに、
前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを前記情報記録媒体から読み取るステップと、
該読み取りデータを前記データ転送用インタフェースを介して外部機器に出力する処理を実行するステップと、
を有することを特徴とする請求項８に記載の情報処理方法。
【請求項１５】
情報記録媒体に対するアクセス制御を実行するコンピュータ・プログラムであり、
情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取るコード読み取りステップと、
前記コードと、記憶部に格納された検証データとの照合処理により情報記録媒体の正当性確認処理を実行する正当性確認ステップと、
前記正当性確認ステップにおいて、情報記録媒体の正当性が確認されたことを条件とし

て前記メディア識別子を暗号化して外部出力するメディア識別子出力ステップと、
を有することを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、コンテンツの不正利用を防止する構成を持つ情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。
【背景技術】
【０００２】
近年、ＤＶＤや、青色レーザーディスク（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）など、大容量データの格納可能な情報記録媒体が普及し、例えば高精細画像データや、高品質音声データなどのデジタルコンテンツをディスクなどの記録媒体に記録再生する利用形態が一般化してきている。
【０００３】
デジタル記録装置および記録媒体によれば、画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーされたコンテンツのインターネットを介した配信や、ＣＤ－Ｒ、ＤＶＤ等の記録媒体にコンテンツをコピーした海賊版ディスクの流通は大きな問題となってきている。
【０００４】
情報記録媒体からのコンテンツ再生、コンテンツ記録処理を行なう態様としては、情報記録媒体（ディスク）を駆動するドライブと、再生／記録処理機能を一体化した装置を利用する態様と、ドライブと、再生処理あるいは記録処理プログラムを実行するホストとしての情報処理装置、例えばＰＣなどをバスなどによって接続し、ドライブとホスト間でのデータ転送を伴う処理態様とがある。
【０００５】
例えば、ドライブとホスト間でのデータ転送を行なう場合の問題点として、コンテンツ、鍵情報、その他の秘密情報の漏洩が発生しやすく、その結果、不正なコンテンツの利用、流出の可能性が高くなるという問題がある。音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。
【０００６】
ＤＶＤや青色レーザディスク等の大容量型記録媒体には、映像情報、音楽情報をデジタルデータとして格納することが可能である。このようなデジタルデータ記録媒体を市場に流通させる場合には、不正コピーを防止し著作権者の保護を図る構成が必須となる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。
【０００７】
例えば、コンテンツ・スクランブルシステム（ＣＳＳ：Ｃｏｎｔｅｎｔ　Ｓｃｒａｍｂｌｅ　Ｓｙｓｔｅｍ）、ＣＰＲＭ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ）などが知られている。ＣＰＲＭは、暗号鍵が漏洩した場合にも、鍵の選択的な無効処理を可能とした構成であり、強固な著作権保護機能を持つ。
【０００８】
ＣＰＲＭでは、情報記録媒体からの暗号化コンテンツの再生、または情報記録媒体に対する暗号化コンテンツの記録処理を行なう装置は、記録媒体に記録されている暗号化キーブロック（例えばＭＫＢ：Ｍｅｄｉａ　Ｋｅｙ　Ｂｌｏｃｋ、ＲＫＢ：Ｒｅｎｅｗａｌ　Ｋｅｙ　Ｂｌｏｃｋ）を取得し、装置に格納されているデバイスキーによって、暗号化キ

ーブロックの復号を実行してメディアキーを取得し、取得したメディアキーと、記録媒体から読み出し可能な記録媒体固有のメディアＩＤとに基づく暗号処理、さらに、ＣＰＲＭで規定するシーケンスに従った暗号処理を含む複数のデータ処理を実行してコンテンツの復号または暗号化に適用する鍵を取得し、取得した鍵によってコンテンツの復号再生、またはコンテンツの暗号化記録処理を行なう。

【０００９】

なお、一般にメディアＩＤは、特定のライセンスされたメディア製造者のみが記録可能なデータとして設定され、ＣＰＲＭの処理に従ったデータ記録、再生プログラムによってのみ読み取り可能なデータとしてメディアに記録される。具体的には、メディアＩＤは、情報記録媒体の内周領域に設定されたバースト・カッティング・エリア（ＢＣＡ）に通常のデータ記録とは異なる方式によって記録される。

【００１０】

暗号化キーブロックとしてのＭＫＢやＲＫＢは、鍵管理センタなどの特定の管理センタによって管理された暗号鍵ブロックデータであり、特定のライセンスされたメディア製造者などに提供され、また適宜更新される。ＭＫＢ、ＲＫＢの更新の際には、不正と判断されたデバイス（再生機器、ＰＣ）に配布されている個々のデバイスキーを選択的にして無効化し、無効化されたデバイスキーを用いたメディアキーの取得を不可能にしたキーブロックとする更新を行なう。この構成により、不正なデバイスにおけるコンテンツ利用を排除することができる。

【００１１】

ＣＰＲＭに基づくコンテンツの再生または記録を行なう場合、情報処理装置は、上述したようにＣＰＲＭによって規定された一定の処理シーケンスで処理を実行する。なお、ＣＰＲＭでは、コピー制御情報（ＣＣＩ：Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）に従って、コンテンツのコピーの許容態様が決定され、コンテンツの再生、記録を実行する情報処理装置は、ＣＣＩに従った処理を行なうように規制される。ＣＣＩには、コピーを許容しないコピーノーモア（Copy No more）、一度のみのコピーを許容するコピーワンス（Copy Once）、コピーを許容するコピーフリー（Copy Free）等の設定があり、ＣＰＲＭに従ったコンテンツ、再生、コピー、記録を行なう装置は、ＣＰＲＭ準拠のコンテンツ再生または記録プログラムを実行し、そのプログラムに含まれる処理として、ＣＣＩの読み取り、更新などの処理を実行する。

【００１２】

しかし、このようなＣＰＲＭ方式を適用した場合にも、不正なコンテンツの利用可能性を完全に排除出来ない場合がある。例えば、以下のシナリオで正規ライセンスを受けないデバイスにおいて、ＣＰＲＭに準拠したコンテンツ記録メディアを自作される可能性がある。

【００１３】

ａ）正規のＣＰＲＭ記録ソフトウェア、すなわちＣＰＲＭに準拠する暗号化コンテンツをメディアに記録する際に使用されるプログラムを解析し、ＣＰＲＭの処理シーケンスを把握する。コンテンツ暗号化に関するすべての秘密はＣＰＲＭ記録ソフトウェアが処理をするため、解析されるとすべての仕組みが公開されてしまう。

ｂ）解析したＣＰＲＭ記録ソフトウェアを利用して、多くのＣＰＲＭ記録ディスクのＭＫＢ（Media Key Block)に秘匿して記録されているメディアキーを抽出する。さらに、ＢＣＡに記録されたメディアＩＤを読みだし、メディアＩＤと、ＭＫＢから取得したメディアキーの対応関係をデータベース化する。この解析は、解析したＣＰＲＭ記録ソフトウェアを保有しているデバイスのデバイスキーが無効化（リボーク）されるまで実行可能である。

ｃ）解析した正規のＣＰＲＭ記録ソフトウェアを利用して、ＣＰＲＭ記録ソフトウェアをライセンスを受けずに自作する。自作ソフトウェアにより、ＣＰＲＭ記録ディスク（ＣＰＲＭ準拠のデータ書き込み可能ディスク）のＢＣＡに記録されたメディアＩＤを読みだし、読み出したメディアＩＤを、［メディアＩＤ－メディアキー］の対応関係をデータベ

ースとして保持する管理サーバへ送信し、メディアＩＤに対応するメディアキーをサーバから送信してもらう。

ｄ）自作ＣＰＲＭ記録ソフトウェアを適用し、かつ、サーバから取得したメディアキーを利用して、ＣＰＲＭ対応メディアに対して、不正取得したメディアキーを利用して、ＣＰＲＭに従ったデータ暗号化、記録シーケンスに従って暗号化コンテンツを生成し、メディアに記録する。

【００１４】

この処理により、正式なＣＰＲＭシーケンスに従った処理、すなわち、デバイスキーによるＭＫＢの処理を実行することなしに、サーバから取得したメディアキーを利用することで、ＣＰＲＭ対応のＤＶＤなどのメディアに対して、暗号化コンテンツを記録することが可能であり、暗号化記録したコンテンツは正規ライセンスを受けて製造された製品との互換性も維持可能となる。

【００１５】

この結果として、正規ライセンスを受けない自作のＣＰＲＭ記録ソフトウェアが流通することによって、守るべきルールが守られない、たとえば、コピー制御情報（ＣＣＩ）の不正な書き換えにより、一度のみのコピー許容コンテンツ（コピーワンス：Copy Once）の設定されたコンテンツがコピーフリー（Copy Free）に改ざんされて、不正なコンテンツ記録メディアとともにメディアに記録されることが起こりうる。また、正規に記録された暗号化コンテンツが自作ソフトにより読み出されて平文化されて複製されるという問題も発生し得る。

【発明の開示】

【発明が解決しようとする課題】

【００１６】

本発明は、上述の問題点に鑑みてなされたものであり、著作権保護コンテンツの不正な利用の排除を実現する情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。具体的には、ＤＶＤなどのメディア（情報記録媒体）に対応して記録されているメディアＩＤの外部流出を防止した構成を提供するものであり、例えば不正なＣＰＲＭソフトウェアプログラムによるメディアＩＤの不正得を防止した構成を持つ情報処理装置、および情報処理方法、並びにコンピュータ・プログラム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】

【００１７】

本発明の第１の側面は、

情報処理装置であり、

情報記録媒体に対する書き込みデータ、または情報記録媒体からの読み取りデータの入出力を実行する記録媒体インタフェースと、

外部機器との転送データの入出力を実行するデータ転送用インタフェースと、

情報記録媒体の正当性を確認するための検証データを格納した記憶部と、

前記情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取り、該コードと前記検証データとの照合処理により情報記録媒体の正当性確認処理を実行し、正当性が確認されたことを条件として前記メディア識別子を暗号化して外部出力する処理を実行するデータ処理部と、

を有することを特徴とする情報処理装置にある。

【００１８】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記データ転送用インタフェースを介したデータ入出力を実行する外部機器との認証処理を実行し、該認証処理の成立を条件として、前記メディア識別子の前記外部機器への出力処理を実行する構成であることを特徴とする。

【００１９】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記認証

処理において生成したセッションキーを適用して、前記メディア識別子の暗号化処理を実行し、セッションキーに基づく暗号化データとして前記メディア識別子を外部機器に出力する構成であることを特徴とする。

【００２０】

さらに、本発明の情報処理装置の一実施態様において、前記記憶部は、ライセンスに基づいて正当に製造された情報記録媒体の識別子に対応して設定されるコード情報を格納し、前記データ処理部は、前記情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取り、該コードと前記検証データとして格納されたコードとの照合処理により情報記録媒体の正当性確認処理を実行し、正当性が確認されたことを条件として前記メディア識別子を暗号化して外部出力する処理を実行することを特徴とする。

【００２１】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、情報記録媒体のＢＣＡ（バースト・カッティング・エリア）に記録されたメディア識別子の対応情報としてのコードを読み取り、該コードと前記検証データとの照合処理を実行する構成であることを特徴とする。

【００２２】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記データ転送用インタフェースを介して、外部機器から前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを入力し、該入力データの情報記録媒体に対する書き込み処理を実行する構成であることを特徴とする。

【００２３】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを前記情報記録媒体から読み取り、該読み取りデータを前記データ転送用インタフェースを介して外部機器に出力する処理を実行する構成であることを特徴とする。

【００２４】

さらに、本発明の第２の側面は、

情報処理方法であり、

情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取るコード読み取りステップと、

前記コードと、記憶部に格納された検証データとの照合処理により情報記録媒体の正当性確認処理を実行する正当性確認ステップと、

前記正当性確認ステップにおいて、情報記録媒体の正当性が確認されたことを条件として前記メディア識別子を暗号化して外部出力するメディア識別子出力ステップと、

を有することを特徴とする情報処理方法にある。

【００２５】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記データ転送用インタフェースを介したデータ入出力を実行する外部機器との認証処理を実行する認証処理実行ステップを有し、該認証処理の成立を条件として、前記メディア識別子の前記外部機器への出力処理を実行することを特徴とする。

【００２６】

さらに、本発明の情報処理方法の一実施態様において、前記メディア識別子出力ステップは、前記認証処理において生成したセッションキーを適用して、前記メディア識別子の暗号化処理を実行し、セッションキーに基づく暗号化データとして前記メディア識別子を外部機器に出力するステップであることを特徴とする。

【００２７】

さらに、本発明の情報処理方法の一実施態様において、前記正当性確認ステップは、前記情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取り、該コードと、記憶部に格納されたライセンスに基づいて正当に製造された情報記

録媒体の識別子に対応して設定されるコードとの照合処理により情報記録媒体の正当性確認処理を実行するステップであることを特徴とする。

【００２８】

さらに、本発明の情報処理方法の一実施態様において、前記コード読み取りステップは、情報記録媒体のＢＣＡ（バースト・カッティング・エリア）に記録されたメディア識別子の対応情報としてのコードを読み取るステップであることを特徴とする。

【００２９】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記データ転送用インタフェースを介して、外部機器から前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを入力するステップと、該入力データの情報記録媒体に対する書き込み処理を実行するステップと、を有することを特徴とする。

【００３０】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記メディア識別子を適用して生成した暗号鍵に基づく暗号化データを前記情報記録媒体から読み取るステップと、該読み取りデータを前記データ転送用インタフェースを介して外部機器に出力する処理を実行するステップと、を有することを特徴とする。

【００３１】

さらに、本発明の第３の側面は、

情報記録媒体に対するアクセス制御を実行するコンピュータ・プログラムであり、

情報記録媒体のメディア識別子の対応情報として情報記録媒体に記録されたコードを読み取るコード読み取りステップと、

前記コードと、記憶部に格納された検証データとの照合処理により情報記録媒体の正当性確認処理を実行する正当性確認ステップと、

前記正当性確認ステップにおいて、情報記録媒体の正当性が確認されたことを条件として前記メディア識別子を暗号化して外部出力するメディア識別子出力ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００３２】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記録媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００３３】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００３４】

本発明の構成によれば、ドライブとホストなど２つの異なるデバイス間のデータ転送を伴うコンテンツの再生あるいは記録処理において、コンテンツの記録、再生を行なう場合に実行するコンテンツの暗号化または復号処理に適用するメディアＩＤ（ディスクＩＤ）の外部漏洩を防止することができる。

【００３５】

本発明の構成によれば、ドライブがメディアＩＤ（ディスクＩＤ）をメディアから読み取り、これが正しい正当なメディアに設定されたヘッダコードに対応して記録されているかをドライブ側で検証し、さらに、検証によって、正当なメディアであることが確認された場合に、ドライブ側でメディアＩＤを暗号化してホストに出力する構成としたので、メディアＩＤの外部漏洩の可能性を低減させることが可能となり、また、正当なメディアで

あることの確認を条件として、コンテンツの再生または記録処理を許容する構成としたので、不正なメディアを利用したコンテンツの再生または記録処理の防止が実現される。

【発明を実施するための最良の形態】

【００３６】

以下、図面を参照しながら本発明の情報処理装置、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の記載項目に従って行う。

１．ＣＰＲＭ規定に従った処理の概要

２．本発明に従ったドライブ－ホスト間のコンテンツ転送を伴う処理構成

３．情報処理装置の構成

【００３７】

［１．ＣＰＲＭ規定に従った処理の概要］

まず、本発明の理解の容易のために、図１を参照して、例えばＤＶＤ等のメディア（情報記録媒体）に対応する著作権保護技術として知られるＣＰＲＭ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ）のアーキテクチャについて説明する。

【００３８】

メディア（情報記録媒体）からのコンテンツ再生、コンテンツ記録処理を行なう態様としては、情報記録媒体（ディスク）を駆動するドライブと、再生／記録処理機能を一体化した記録再生装置を利用する第１の処理態様と、ドライブと、再生処理あるいは記録処理プログラムを実行するホストとしての情報処理装置、例えばＰＣなどをバスなどによって接続し、ドライブとホスト間でのデータ転送を伴う第２の処理態様とがある。図１を参照して、第１の処理態様におけるデータ記録再生処理、図２を参照して第２の処理態様におけるデータ記録再生処理について説明する。

【００３９】

図１において、中央が例えばＣＰＲＭ規格に準拠したＤＶＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＡＭ等の記録型メディア（情報記録媒体）１０であり、左サイドに、例えばＣＰＲＭ規格に準拠したレコーダ２０、右サイドに、例えばＣＰＲＭ規格に準拠したプレーヤ３０を示す。レコーダ２０およびプレーヤ３０は、機器またはアプリケーションソフトウェアである。

【００４０】

未記録ディスクの状態において、メディア１０の最内周側のリードインエリアのバースト・カッティング・エリア（ＢＣＡ：Burst Cutting Area)またはＮＢＣＡ(Narrow Burst Cutting Area)と称されるエリアには、メディアＩＤ１１が記録され、リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、ＭＫＢと適宜略す）１２が予め記録されている。メディアＩＤ１１は、個々のメディア単位例えばディスク１枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアＩＤ１１は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックＭＫＢは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための暗号鍵ブロックデータである。メディアＩＤは、各メディア（記録媒体）に固有の情報である。

【００４１】

メディア１０において、データの書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ１３が記録される。暗号化方式としては、例えばＣ２(Cryptomeria Cipher)が使用される。

【００４２】

メディア１０には、暗号化タイトルキー１４およびＣＣＩ(Copy Control Information)１５が記録される。暗号化タイトルキー１４は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。ＣＣＩは、コピーノーモア、コピーワンス、コピーフリー等のコピー制御情報である。

【００４３】
レコーダ２０は、デバイスキー２１、プロセスＭＫＢ２２、Ｃ２＿Ｇ２３、乱数発生器２４、Ｃ２＿Ｅ２５、Ｃ２＿Ｇ２６およびＣ２＿ＥＣＢＣ２７の構成要素を有する。プレーヤ３０は、デバイスキー３１、プロセスＭＫＢ３２、Ｃ２＿Ｇ３３、Ｃ２＿Ｄ３５、Ｃ２＿Ｇ３６およびＣ２＿ＤＣＢＣ３７の構成要素を有する。
【００４４】
デバイスキー２１、３１は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に異なる秘密鍵であり、鍵管理センタから発行される。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。メディア１０から再生されたＭＫＢ１２とデバイスキー２１とがプロセスＭＫＢ２２において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ２０におけるのと同様に、プレーヤ３０においても、ＭＫＢ１２とデバイスキー３１とがプロセスＭＫＢ３２において演算され、リボケーションされたかどうかの判別がなされる。
【００４５】
さらに、プロセスＭＫＢ２２、３２のそれぞれにおいて、ＭＫＢ１２とデバイスキー２１、３１からメディアキーが算出される。ＭＫＢ１２は、有効なデバイスキー、すなわち無効化（リボーク）されていない場合に、その有効なデバイスキーで復号することで、メディアキーを取得できる。
【００４６】
従って、レコーダ２０のデバイスキー２１が無効化（リボーク）されている場合は、プロセスＭＫＢ２２において、ＭＫＢ１２とデバイスキー２１からメディアキーが算出できない。同様に、プレーヤ３０のデバイスキー３１が無効化（リボーク）されている場合は、プロセスＭＫＢ３２において、ＭＫＢ１２とデバイスキー３１からメディアキーが算出できない。レコーダ２０，プレーヤ３０は、有効なデバイスキーを有する場合にのみＭＫＢ１２からメディアキーを取得することができる。
【００４７】
Ｃ２＿Ｇ２３、３３は、それぞれ、メディアキーとメディアＩＤとを演算し、メディアユニークキーを導出する処理である。
【００４８】
乱数発生器（ＲＮＧ：Random Number Generator)２４は、タイトルキーの生成に利用される。乱数発生器２４からのタイトルキーがＣ２＿Ｅ２５に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー１４がメディア１０に記録される。
【００４９】
プレーヤ３０では、メディア１０から再生された暗号化タイトルキー１４とメディアユニークキーとがＣ２＿Ｄ３５に供給され、暗号化タイトルキーがメディアユニークキーで復号され、タイトルキーが得られる。
【００５０】
レコーダ２０においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ２６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ２７に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１３がメディア１０に記録される。
【００５１】
プレーヤ３０においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ３６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ３７に供給され、メディア１０から再生された暗号化コンテンツ１３がコンテンツキーを鍵として復号される。
【００５２】
図１の構成において、レコーダ２０によるコンテンツ記録の手順について説明する。レコーダ２０は、メディア１０からＭＫＢ１２を読み出し、プロセスＭＫＢ２２によってデ

バイスキー２１とＭＫＢ１２とを演算し、メディアキーを計算する。メディアキーの取得に失敗した場合（演算結果が予め定められた値を示す）は、デバイスキー２１（レコーダ２０の機器またはアプリケーション）がＭＫＢによってリボークされたと判定され、レコーダ２０は、以後の処理を中断し、メディア１０への記録を禁止する。メディアキーが取得された場合（予め定められた値以外）には、処理を継続する。

【００５３】

次に、レコーダ２０は、メディア１０からメディアＩＤ１１を読み、メディアキーと共にメディアＩＤをＣ２＿Ｇ２３に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器２４で発生させたタイトルキーがＣ２＿Ｅ２５で暗号化され、暗号化タイトルキー１４としてメディア１０に記録される。また、タイトルキーとコンテンツのＣＣＩ情報がＣ２＿Ｇ２６で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをＣ２＿ＥＣＢＣ２７で暗号化し、メディア１０上に暗号化コンテンツ１３としてＣＣＩ１５と共に記録する。

【００５４】

次に、プレーヤ３０による再生の手順について説明する。最初にＭＫＢ１２をメディア１０から読み出し、デバイスキー３１とＭＫＢ１２を演算し、リボケーションの確認がなされる。デバイスキー３１、すなわち、プレーヤ３０の機器またはアプリケーションがリボークされない場合には、メディアＩＤを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー１４とメディアユニークキーからタイトルキーが演算される。タイトルキーとＣＣＩ１５とがＣ２＿Ｇ３６に入力され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＤＣＢＣ３７に入力され、コンテンツキーを鍵として、メディア１０から再生された暗号化コンテンツ１３に対してＣ２＿ＤＣＢＣ３７の演算が施される。その結果、暗号化コンテンツ１３が復号される。

【００５５】

このように、コンテンツの復号に必要なコンテンツキーを得るためには、メディアの１枚毎に異なるメディアＩＤが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアＩＤがオリジナルのメディアＩＤと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

【００５６】

上述した図１の構成は、記録再生機器として構成された場合のメディア（情報記録媒体）からのコンテンツ再生、コンテンツ記録処理態様である。次に、ドライブと、再生処理あるいは記録処理プログラムを実行するホストとしての情報処理装置、例えばＰＣなどをバスなどによって接続し、ドライブとホスト間でのデータ転送を伴う第２の処理態様におけるデータ記録再生処理について説明する。

【００５７】

図２において、データ処理装置としてのホスト５０は、例えばＰＣを示す。ホスト５０は、メディア１０に記録可能で、メディア１０から再生可能なコンテンツを扱うことができ、且つドライブ４０と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばＰＣに対してアプリケーションソフトウェアがインストールされることによってホスト５０が構成される。

【００５８】

ドライブ４０とホスト５０との間は、インタフェース６０で接続されている。インタフェース６０は、例えば、ＡＴＡＰＩ(AT Attachment Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers)１３９４等である。

【００５９】

メディア１０には、メディアＩＤ１１、メディアキーブロック１２およびＡＣＣ(Authentication Control Code)が予め記録されている。ＡＣＣは、ドライブ４０とホスト５０との間の認証がメディア１０によって異なるようにするために予めメディア１０に記録さ

れたデータである。

【００６０】

ドライブ４０は、ＡＣＣ１６をメディア１０から読み出す。メディア１０から読み出されたＡＣＣ１６がドライブ４０のＡＫＥ(Authentication and Key Exchange)４１に入力されると共に、ホスト５０へ転送される。ホスト５０は、受け取ったＡＣＣをＡＫＥ５１に入力する。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣの値とから認証動作の度に異なる値となる共通のセッションキー（バスキーと称する）を生成する。

【００６１】

バスキーがＭＡＣ(Message Authentication Code)演算ブロック４２および５２にそれぞれ供給される。ＭＡＣ演算ブロック４２および５２は、ＡＫＥ４１および５１でそれぞれ得られたバスキーをパラメータとして、メディアＩＤおよびメディアキーブロック１２のＭＡＣを計算するプロセスである。ＭＫＢとメディアＩＤの完全性(integrity)をホスト５０が確認するために利用される。

【００６２】

ＭＡＣ４２および５２によってそれぞれ計算されたＭＡＣがホスト５０の比較部５３において比較され、両者の値が一致するかどうかが判定される。これらのＭＡＣの値が一致すれば、ＭＫＢとメディアＩＤの完全性が確認されたことになる。比較出力でスイッチＳＷ１が制御される。

【００６３】

図３のフローチャートを参照してＭＡＣ検証に基づくスイッチ制御処理について説明する。ステップＳ１１は、ホスト５０の比較部５３の処理であり、ドライブ４２のＭＡＣ演算ブロック４２でバスキーをパラメータとして求められたＭＡＣ計算値と、ホスト５０のＭＡＣ演算ブロック５３でバスキーをパラメータとして求められたＭＡＣ計算値とを比較するステップである。両者が一致すれば、ＭＫＢとメディアＩＤの完全性が確認されたと判定し、ステップＳ１２に進み、スイッチＳＷ１がＯＮとされ、両者が一致しない場合は、ＭＫＢとメディアＩＤの完全性が確認されないと判定し、ステップＳ１３に進み、スイッチＳＷ１がＯＦＦとされ、処理が停止する。

【００６４】

スイッチＳＷ１は、ドライブ４０のメディア１０の記録または再生経路と、ホスト５０の暗号化／（または）復号モジュール５４との間の信号路をＯＮ／ＯＦＦするものとして示されている。なお、スイッチＳＷ１は、信号路のＯＮ／ＯＦＦを行うものとして示されているが、より実際には、ＯＮの場合にホスト５０の処理が継続し、ＯＦＦの場合にホスト５０の処理が停止することを表している。暗号化／復号モジュール５４は、メディアユニークキーと暗号化タイトルキーとＣＣＩとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ１３へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ１３を復号する演算ブロックである。

【００６５】

メディアユニークキー演算ブロック５５は、ＭＫＢ１２とメディアＩＤとデバイスキー５６とからメディアユニークキーを演算する演算ブロックである。すなわち、図１に示すレコーダまたはプレーヤと同様に、デバイスキーとＭＫＢ１２とからメディアキーが演算され、さらに、メディアキーとメディアＩＤ１１とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック５５は、リボケーションを行うリボーク処理部としての機能も有する。

【００６６】

記録時に、比較部５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされ、暗号化／復号モジュール５４からスイッチＳＷ１を通じてドライブ４０に対して、暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５が供給され、メディア１

０に対してそれぞれ記録される。再生時に、比較部５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされ、メディア１０からそれぞれ再生された暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５がスイッチＳＷ１を通じてホスト５０の暗号化／復号モジュール５４に対して供給され、暗号化コンテンツが復号される。

【００６７】

上述の処理において、メディア１０に記録されたメディアＩＤ１１は、ドライブ４０を介して、平文のままホスト５０に提供される。このような構成では、先に説明したように、メディアＩＤを取得したホストは、メディアＩＤとメディアキーとの対応関係を推定することが可能となる。

【００６８】

メディアＩＤは、メディア１枚毎に異なる識別データであり、通常のプロセスでの書き込みのできないメディアの最内周側のリードインエリアのＢＣＡ(Burst Cutting Area)またはＮＢＣＡ(Narrow Burst Cutting Area)と称されるエリアに記録されている。

メディアキーはＭＫＢから取得可能なキーであるが、ＭＫＢは、複数のメディアに対して共通なデータとして設定される。例えばあるディスクメーカーの作成するディスク（メディア）には、ある製造ロット単位や、ある一定期間は同じＭＫＢが格納され、同じメディアキーが取得可能なＭＫＢが適用される。

【００６９】

ホストがリボークされていない有効なデバイスである間は、様々なメディアから複数のメディアＩＤの取得することが可能となり、さらに、正規のＣＰＲＭ記録ソフトウェア、すなわちＣＰＲＭに準拠する暗号化コンテンツをメディアに記録する際に使用されるプログラムを解析し、ＣＰＲＭの処理シーケンスが解析されると、解析したＣＰＲＭ記録ソフトウェアを利用して、多くのＣＰＲＭ記録ディスクのＭＫＢ（Media Key Block)に秘匿して記録されているメディアキーが抽出される可能性がある。

【００７０】

この結果、メディアＩＤとメディアキーの対応関係データとして、例えば下記のようなデータ、

メディアＩＤ：ａａａａ～ｂｂｂｂ＝メディアキーＸ

メディアＩＤ：ｃｃｃｃ～ｄｄｄｄ＝メディアキーＹ

メディアＩＤ：ｅｅｅｅ～ｆｆｆｆ＝メディアキーＺ

このようなメディアＩＤの範囲と、メディアキーとの対応関係が推定されてしまう可能性がある。

【００７１】

さらに、解析した正規のＣＰＲＭ記録ソフトウェアを利用してＣＰＲＭ記録ソフトウェアを、ライセンスを受けずに不正に自作し、この不正作成ソフトウェアにより、ＣＰＲＭ記録ディスク（ＣＰＲＭ準拠のデータ書き込み可能ディスク）のＢＣＡに記録されたメディアＩＤを読みだし、読み出したメディアＩＤを、［メディアＩＤ－メディアキー］の対応関係をデータベースとして保持する管理サーバへ送信し、メディアＩＤに対応するメディアキーをサーバから送信してもらい、この取得メディアキーを利用して、ＭＫＢの記録されたＣＰＲＭ対応メディアに対して、不正取得したメディアキーを利用して、ＣＰＲＭに従ったデータ暗号化、記録シーケンスに従って暗号化コンテンツを生成し、メディアに記録することが可能となる。この処理により、正式なＣＰＲＭシーケンスに従った処理、すなわち、デバイスキーによるＭＫＢの処理を実行することなしに、サーバから取得したメディアキーを利用することで、ＣＰＲＭ対応のＤＶＤなどのメディアに対して、暗号化コンテンツを記録することが可能となってしまい、正規なライセンスを持たないデバイスによるＣＰＲＭ準拠メディアが製造されてしまう。

【００７２】

［２．本発明に従ったドライブ－ホスト間のコンテンツ転送を伴う処理構成］

以下に述べる本発明は、上記の問題点を解決する構成を持つ。まず、本発明の構成の概要について説明する。

【００７３】
本発明の構成では、メディアの最内周側のリードインエリアのバースト・カッティング・エリア（ＢＣＡ：Burst Cutting Area)に記録されたメディアＩＤを平文のままドライブからホストへ転送せず、認証されたホストに対してのみ、暗号化して出力する構成とする。この構成により、不正なホストによるメディアＩＤの取得を防止し、メデイアＩＤとメディアキーの対応関係を推定不可能とする。
【００７４】
具体的には、ＢＣＡへ記録されたメディアＩＤをドライブからをホストへ転送する場合には、ホストとドライブ間の相互認証および鍵交換（ＡＫＥ：Authentication and Key-Exchange）が完了し、完了後に生成されるセッションキー（Session Key(Ks)）でメディアＩＤを暗号化してセキュアにドライブからホストへ転送する。これにより、ドライブ－ホスト間の接続インタフェースである例えばＡＴＡＰＩなどのＩ／Ｆバスからのメディアの盗難を防止する。この構成により、メディアＩＤとメディアキーの対応関係を推定不可能とするものである。
【００７５】
なお、ＢＣＡにはメディアＩＤ以外のデータも記録されることがある。例えば、ＢＤ－ＲＯＭ（読みだし専用）、ＢＤ－ＲＥ（書き換え型）、ＢＤ－Ｒ（ライトワンス）といった、メディアの記録タイプなどの情報が記録される。メディアＩＤ等の秘密情報以外のデータは、ホストとドライブ間の相互認証および鍵交換（ＡＫＥ）の完了に依存せずにドライブからホストへ転送することができる。ただし、メディアＩＤのヘッダコード以外のＢＣＡデータ領域は、非公開であり、これらのデータ形式はコピープロテクション技術のライセンスを受けた例えばディスク製造エンティテイなどにおいてのみしか知り得ない。ＢＣＡのデータ形式を物理規格だけのライセンスを受けるすべて使用者に開放してしまうと、コピープロテクション技術のライセンスを受けない人が、知らずに偶然、メディアＩＤと同じヘッダ情報を使用してしまい、正規コピープロテクション技術を適用したメディアＩＤと運用上の干渉が起こることが想定される。
【００７６】
従って、物理規格だけのライセンスを受領する場合、メディアＩＤ対応のヘッダコードとは異なるヘッダコード情報を強制的に利用してもらい、物理規格ライセンスの許容範囲での自由な運用がコピープロテクション規格ライセンスで規定するメディアＩＤと使用上の衝突を受けないようにしておくことが必要とされる。つまり、物理規格で規定するＢＣＡデータは、コピープロテクション規格で定めるメディアＩＤのヘッダとは異なるヘッダの下で運用するものとする。
【００７７】
図４、図５を参照して、メディア（ディスク）のＢＣＡに記録されるメディアＩＤのフォーマットについて説明する。
【００７８】
図４は、ＢＣＡのデータ記録構成を示す図である。図４（ａ）に示すようにＢＣＡは、１６バイトデータを記録可能なスロットを４スロット持つ。計６４バイトデータが記録可能である。前述したように、一般のデータ記録処理とは異なる特殊なデータ記録方式によるものであり、ライセンスを受けたディスク製造エンティテイのみが記録処理を実行することができる。
【００７９】
図４（ｂ）に示すように、各スロットのデータ構成は、ヘッダ部およびＢＣＡデータ部とによって構成される。ヘッダ部は、ＢＣＡデータ部の格納データの種類を識別するデータとして利用される。
【００８０】
例えばヘッダ部には、１バイトの様々なコードが格納され、その一部は、著作権保護技術で利用するＢＣＡデータを明示するための公開されたコード（０３ｈなど）として設定され、ヘッダ部に続くＢＣＡデータ領域には、ヘッダコードに対応するデータが格納され

る。

【００８１】

図５に、メディアＩＤを格納したＢＣＡのデータ記録構成を示す。図５（ａ）は、図４（ａ）と同様、ＢＣＡ領域の全体構成を示している。図５（ｂ）は、メディアＩＤ格納スロットのデータ構成を示している。なお、メディアＩＤは、ディスクＩＤと呼ばれる場合もある。

【００８２】

図５（ｂ）に示すメディアＩＤ（ディスクＩＤ）格納スロットのヘッダ格納部には、スロット格納データがメディアＩＤ（ディスクＩＤ）などの著作権保護技術で利用されるデータであることを示すヘッダコード＝０３ｈが格納される。このヘッダコード、すなわち、ＢＣＡスロット格納データがメディアＩＤなどの著作権保護技術で利用されるデータであることを示す場合、ヘッダコード以外のＢＣＡデータ領域は、非公開であり、ライセンスを受けたディスク製造エンティテイ等、特定のライセンス保持エンティテイのみが知り得るＢＣＡデータ部として設定される。カテゴリーコード（Category Code）によってＢｙｔｅ２からＢｙｔｅ１５までのデータ構成が分類される。カテゴリーコードがある決められた値（たとえば０１ｈなど）のときはＢＣＡスロットデータはメディアＩＤに分類される。ＢＣＡスロットデータがメディアＩＤの場合のＢＣＡデータ部には、メディアＩＤの構成データとして、カテゴリコード（Category Code）、マニュファクチァーコード（Manufacturer Code）、シリアルナンバー（Serial Number）が格納される。各データの意味は、以下の通りである。

カテゴリコード（Category Code）：著作権保護技術で利用されるデータの分類コード

マニュファクチァーコード（Manufacturer Code）：ディスク製造者ごとに配布される識別コード

シリアルナンバー（Serial Number）：ディスク製造者が製造するディスクのシリアル番号

【００８３】

本発明の処理においては、以下の構成を持つことを特徴としている。

（１）ヘッダデータ０３ｈをもつＢＣＡデータのヘッダデータ以外のＢＣＡデータ領域は秘密である。

（２）ヘッダデータ＝０３ｈをもつＢＣＡデータは、ＡＫＥが完了し、セッションキーＫｓが生成されていないときは、ドライブはホストへ転送しない。

（３）ヘッダデータ０３ｈをもつＢＣＡデータは、ＡＫＥが完了し、セッションキーＫｓが生成されているならば、ＫｓでＢＣＡデータを暗号化した上で、ドライブはホストへ転送する。

（４）０３ｈ以外のヘッダデータをもつＢＣＡデータは、ＡＫＥの完了する、しない、に関係なく、ドライブはホストへ暗号化をせずにそのままのデータを転送することができる。つまり、そのＢＣＡデータは秘密ではない。

【００８４】

次に、図６以下を参照して、本発明に従ったドライブ－ホスト間のコンテンツ転送を伴う処理の詳細について、説明する。図６は、ドライブとホストとをバス接続し、コンテンツの転送をドライフとホスト間で実行して、メデイアからのコンテンツ再生またはメディアに対してコンテンツを記録する処理を説明する図である。

【００８５】

図６は、メディア（情報記録媒体）１００と、メディア１００をセットし、メディア１００からのデータ読み取り、メディア１００へのデータ書き込みを実行するドライブ２００と、ドライブ２００と接続バスを介して接続され、アプリケーション・プログラムに従ったコンテンツ再生または記録処理を実行するホスト３００の処理を示している。なお、ドライブ２００とホスト３００とを接続するバスは、例えばＡＴＡＰＩ(AT Attachment Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers)１３９４等

である。
【００８６】
メディア１００には、以下の情報が格納される。
有効なデバイスまたは、無効化（リボーク）されたデバイスを識別するためのリボーク情報１０１、
メディアキー（Ｋｍ）を格納した暗号鍵ブロックとしてのＲＫＢ１０２、
ディスクキー（Ｋｄ）をメディアキー（Ｋｍ）で暗号化した暗号化ディスクキーＥＫｍ（Ｋｄ）１０３
ＢＣＡ領域に記録されたメディアＩＤ（ＩＤｄｉｓｃ）１０４、
コンテンツの暗号化および復号処理に適用する暗号鍵としての記録キー（Ｋｒｅｃ）の生成に適用するシード情報（Ｓｅｅｄｒｅｃ）１０５、
暗号化コンテンツ１０６
である。
【００８７】
なお、メディア１００が暗号化コンテンツの記録済みメディアである場合は、シード情報（Ｓｅｅｄｒｅｃ）１０５、暗号化コンテンツ１０６は、メディア１００に記録されているが、メディア１００が、コンテンツの書き込みがなされていないデータ書き込み可能メディアの場合には、これらのデータは書き込まれていない状態であり、ホスト３００によって生成した暗号化コンテンツをメディアに記録する際に、ホストによって生成する乱数がシード情報（Ｓｅｅｄｒｅｃ）１０５としてメディア１００に記録され、記録キー（Ｋｒｅｃ）を適用して暗号化された暗号化コンテンツがメディア１００に記録されることになる。
【００８８】
リボーク情報１０１は、各デバイスの登録または無効化情報を記録したデータであり、管理センタの電子署名が付加され、改竄の検証が可能な構成を持つ。
【００８９】
ＲＫＢ（Renewal Key Block）１０２は、前述のメディアキーブロック（ＭＫＢ）と同様の暗号鍵ブロックデータであり、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。ＭＫＢと同様、メディア（情報記録媒体）を利用したコンテンツ再生／記録を実行する正当なライセンスを保有するユーザ機器としての情報処理装置に配布されたデバイスキーを適用した復号処理によってメディアキー：Ｋｍが取得可能である。暗号鍵ブロック：ＲＫＢの構成データを変更することにより、メディアキー：Ｋｍを取得可能なユーザ機器を選別することが可能である。すなわち、リボークされたデバイスのデバイスキーを適用した場合には、メディアキー：Ｋｍを取得できないように、随時、更新される。
【００９０】
管理センタが、コンテンツ再生／記録を実行するデバイス（ユーザ機器や再生アプリケーション）を不正であると判定した場合は、ＲＫＢの構成を変更して、不正機器によるメディアキー：Ｋｍの取得を不可能とすることが可能となる。なお、不正と判定されたデバイスはリボーク（無効）デバイスとして管理センタに登録される。管理センタは、デバイスの登録情報、リボーク情報を保持し、適宜更新する。
【００９１】
メディアＩＤ１０４は、ＢＣＡ領域に記録されたメディア固有の識別情報である。メディアＩＤは、前出したようにディスクＩＤとも呼ばれ、ライセンスを受けたメディア（ディスク）製造エンティティのみが記録可能なデータである。
【００９２】
ドライブ２００には、デバイスキー２０１、検証データ２０２が格納されている。これらは不揮発性メモリにセキュアに格納されており、外部からのアクセス、外部からの改竄が許容されないデータとして格納される。デバイスキー２０１は、前述のＲＫＢの復号処理に適用される鍵であり、有効性が担保されている場合、すなわちドライブがリボークさ

れていない場合にのみＲＫＢからメディアキー（Ｋｍ）を取得することができる。

【００９３】

検証データ２０２は、メディア１００のＢＣＡから読み出したメディアＩＤ（ＩＤｄｉｓｃ）の検証処理のためにドライブに格納されるデータである。検証データ２０２は、先に図５（ｂ）を参照して説明したＢＣＡデータがメディアＩＤである場合のヘッダコードに相当するコードを含むデータとして構成される。すなわち、本例において、ＢＣＡデータがメディアＩＤである場合のヘッダコードはヘッダコード＝０３ｈであり、０３ｈが検証データ２０２としてドライブ２００のメモリに格納される。

【００９４】

前述したように、ＢＣＡデータがメディアＩＤである場合には、ヘッダコードの値［０３ｈ］以外のＢＣＡスロットデータは公開値ではなく、デバイスキー２０１とともに例えば管理センタとの契約に基づいたディスク製造エンティティの管理下でのディスク製造が義務付けられる。また、管理センタのライセンスを受けたドライブ製造エンティティは各ドライブのメモリ（不揮発性メモリ）にヘッダコードの値を格納し、ディスクから読み出すＢＣＡデータの適切な転送制御が義務付けられる。

【００９５】

ホスト（再生／記録処理実行アプリケーション）３００は、リボーク情報３０１を格納している。これは各デバイスの登録または無効化情報を記録したデータであり、管理センタの電子署名が付加され、改竄検証が可能な構成を持ち、改竄検証がなされて正当性が確認されたことを条件として参照情報として適用される。

【００９６】

なお、図には示していないが、ドライブ２００、ホスト３００は、それぞれ公開鍵暗号方式に従った自己の公開鍵、秘密鍵のペアを格納している。さらに、外部から取得した公開鍵証明書の署名検証、リボーク情報の署名検証等に適用する管理センタの公開鍵を格納している。

【００９７】

図６を参照して、メディア１００からのコンテンツ再生、メディア１００に対するコンテンツ記録処理の処理シーケンスについて説明する。

【００９８】

まず、ステップＳ１２１、Ｓ１３１において、ドライブ２００とホスト３００間で相互認証および鍵交換（ＡＫＥ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ）処理が実行される。

【００９９】

相互認証および鍵交換（ＡＫＥ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ）処理の詳細シーケンスについて、図７を参照して説明する。この処理は、例えば、ＩＳＯ／ＩＥＣ９７９８－３に規定された公開鍵アルゴリズムを利用した相互認証、ＩＳＯ／ＩＥＣ１１７７０－３に規定された公開鍵アルゴリズムを利用した鍵生成処理方式を適用して実行可能である。なお、公開鍵を利用した相互認証方式として実用化された方式としては、例えば、ＤＴＣＰ(Digital Transmission Content Protection) Specification Volume 1 (Informational Version)に記載される方法がある。

【０１００】

図７に示す処理シーケンスについて説明する。ステップＳ２０１において、ホストは、ドライブに対して乱数生成処理によって生成したチャレンジデータ［Ｃ＿ｈｏｓｔ］と、公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］を送信する。

【０１０１】

図８を参照して公開鍵証明書（ＰＫＣ）のデータ構成について説明する。図８（ａ）は、公開鍵証明書（ＰＫＣ）の証明書データの例を示している。図８（ｂ）は、楕円暗号（鍵長１６０ビット）を適用した公開鍵証明書（ＰＫＣ）のデータ構成例を示している。

【０１０２】

図８（ａ）に示すように、公開鍵証明書（ＰＫＣ）の証明書データには、証明書ＩＤ、

公開鍵、その他の情報が含まれる。例えばドライブは、ドライブに対応する公開鍵を格納した公開鍵証明書（ＰＫＣ－Ｄ）を管理センタから受領し、ドライブが例えばフラッシュメモリなどの不揮発性メモリに格納保持する。また公開鍵に対応する秘密鍵（ＫＳ－Ｄ）も提供される。ホストに対しても公開鍵証明書（ＰＫＣ）と秘密鍵のペアが提供され、ホスト内のハードディスクやフラッシュメモリなどの不揮発性メモリに保持される。

【０１０３】

公開鍵証明書（ＰＫＣ）は、公開の許容されたデータであり、例えば他の機器の要求に応じて出力される。他の機器の公開鍵証明書を受領した機器は、受領した公開鍵証明書に付加された管理センタの署名に基づく公開鍵証明書の改竄検証を実行し、受領した公開鍵証明書の正当性を確認した後、公開鍵証明書から公開鍵を取得する。なお、管理センタの署名に基づく公開鍵証明書の改竄検証は、管理センタの公開鍵を適用して実行される。管理センタの公開鍵も公開されたデータであり、例えばドライブ、ホストの不揮発性メモリ等へ予め格納してあるものを利用する、または、ネットワークあるいは記録媒体を介して受領できる。

【０１０４】

ドライブ、ホストには、公開鍵証明書に併せて秘密鍵が提供される。すなわち、ドライブ、ホストには、それぞれ公開鍵証明書（ＰＫＣ）と秘密鍵のペアが提供され、それぞれのメモリに保持される。公開鍵を格納した公開鍵証明書は公開の許容されたデータであるが、秘密鍵は外部に漏洩することのないように各デバイスにおいてセキュアに保持される。

【０１０５】

図８（ｂ）は、楕円暗号（鍵長１６０ビット）を適用した公開鍵証明書（ＰＫＣ）のデータ構成例を示している。証明書タイプ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｔｙｐｅ＝１）、証明書ＩＤ（Ｃｅｒｔｉｆｉｃａｔｅ　ＩＤ）、公開鍵（Ｐｕｂｌｉｃ　Ｋｅｙ）が格納され、これらの格納データに対応して管理センタの秘密鍵を適用して生成された電子署名（Ｓｉｇｎａｔｕｒｅ）が設定される。

【０１０６】

図７に戻り、相互認証シーケンスについての説明を続ける。ステップＳ２０１において、ホストからチャレンジデータ［Ｃ＿ｈｏｓｔ］と、公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］を受け取ったドライブは、公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］の署名検証処理により、公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］の正当性を検証する。署名検証処理は、ドライブの保持する管理センタの公開鍵を適用して実行される。

【０１０７】

公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］の正当性が検証されると、ドライブは、公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］から公開鍵証明書ＩＤを取得して、メディア１００から読み取ったリボーク情報１０１にホストの公開鍵証明書ＩＤが記録されていないかを確認する。すなわち、ホストの公開鍵証明書ＩＤが無効化（リボーク）されていない有効なＩＤであるか否かを確認する。

【０１０８】

公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］の正当性が確認されなかったり、あるいは、リボーク情報１０１に基づいて、ホストが無効化（リボーク）されていることが判明した場合にはエラーメッセージの通知などを実行し、処理を終了する。以後の処理、コンテンツ再生または記録処理は中止される。

【０１０９】

公開鍵証明書［Ｃｅｒｔ＿ｈｏｓｔ］の正当性が確認され、ホストが無効化（リボーク）されていない正当な公開鍵証明書を有するホストであることが確認されると、ステップＳ２０２において、ドライブは、ホストに対して乱数生成処理によって生成したチャレンジデータ［Ｃ＿ｄｒｉｖｅ］と、ドライブ側の公開鍵証明書［Ｃｅｒｔ＿ｄｒｉｖｅ］を送信する。

【０１１０】

ホストは、ドライブ側の公開鍵証明書［Ｃｅｒｔ＿ｄｒｉｖｅ］の署名検証を実行する。署名検証処理は、ホスト側で保持する管理センタの公開鍵［Ｋｐ＿ｋｉｃ］を適用して実行される。

【０１１１】

公開鍵証明書［Ｃｅｒｔ＿ｄｒｉｖｅ］の正当性が確認されると、公開鍵証明書［Ｃｅｒｔ＿ｄｒｉｖｅ］から公開鍵証明書ＩＤを取得して、リボーク情報３０１との照合を実行し、ドライブの公開鍵証明書ＩＤが無効化（リボーク）されていない有効なＩＤであるか否かを確認する。

【０１１２】

公開鍵証明書［Ｃｅｒｔ＿ｄｒｉｖｅ］の正当性が確認されなかったり、あるいは、リボーク情報３０１に基づいて、ドライブが無効化（リボーク）されていることが判明した場合にはエラーメッセージの通知などを実行し、処理を終了する。以後のコンテンツ再生または記録処理は中止される。

【０１１３】

公開鍵証明書［Ｃｅｒｔ＿ｄｒｉｖｅ］の正当性が確認された場合には、ホストは、ドライブから受信したチャレンジデータ［Ｃ＿ｄｒｉｖｅ］に基づく演算を実行しパラメータ［Ａ＿ｈｏｓｔ］を算出し、新たに生成した乱数［Ｒ＿ｈｏｓｔ］とともに、ドライブに送信（ステップＳ２０３）する。

【０１１４】

一方、ドライブは、ホストから受信したチャレンジデータ［Ｃ＿ｈｏｓｔ］に基づく演算を実行しパラメータ［Ａ＿ｄｒｉｖｅ］を算出し、新たに生成した乱数［Ｒ＿ｄｒｉｖｅ］とともに、ホストに送信（ステップＳ２０４）する。

【０１１５】

この処理により、ドライブ、ホストの双方は、乱数[Ｒ_ｈｏｓｔ]、［Ｒ＿ｄｒｉｖｅ］、パラメータ［Ａ＿ｈｏｓｔ］、［Ａ＿ｄｒｉｖｅ］を共有することになり、ドライブと、ホストアプリケーションの双方は、これらの共有データに基づいて共通のセッションキーＫｓを生成（ステップＳ２０５）する。

【０１１６】

図６に戻り、ドライブ２００とホスト３００間のコンテンツ転送を伴うコンテンツ再生または記録処理シーケンスについて説明を続ける。

【０１１７】

ドライブ２００は、ホスト３００との相互認証および鍵交換（ＡＫＥ）が終了すると、ドライブ内に保持するデバイスキー：Ｋｄｅｖ２０１を適用し、ステップＳ１２２において、メディア１００から読み出した暗号鍵ブロックとしてのＲＫＢ１０２の復号処理を実行して、ＲＫＢ１０２からメディアキー：Ｋｍを取得する。なお、ＲＫＢ１０２からメディアキー：Ｋｍを取得できるのは、コンテンツの利用を認められた機器のみであり、前述したように不正機器としてリボークされた機器の持つデバイスキーではＲＫＢに暗号化されて格納されたメディアキーの復号が出来ず、メディアキー：Ｋｍを取得することができない。

【０１１８】

ステップＳ１２２においてメディアキー：Ｋｍの取得に成功すると、次に、ステップＳ１２３において、取得したメディアキー：Ｋｍを適用して、メディア１００から取得した暗号化ディスクキー：ＥＫｍ（Ｋｄ）２０３の復号処理を実行し、ディスクキー：Ｋｄを取得する。この復号処理としてはたとえばトリプルＤＥＳ（ＴＤＥＳ）アルゴリズムが適用される。なお、図中、ＴＤＥＳはトリプルＤＥＳ暗号アルゴリズム、ＡＥＳはＡＥＳ暗合ルゴリズムを示し、ＴＤＥＳ，ＡＥＳの後続文字として示す［Ｅ］は暗号化処理（Ｅｎｃｒｙｐｔｉｏｎ）、［Ｄ］は復号処理（Ｄｅｃｒｙｐｔｉｏｎ）を示している。

【０１１９】

ドライブ２００は、次にステップＳ１２４において、相互認証および鍵交換（ＡＫＥ）処理で、生成したセッションキー（Ｋｓ）を適用してディスクキー：Ｋｄを暗号化してホ

スト３００に送信する。この暗号処理は、例えばＡＥＳ暗号アルゴリズムを適用して実行される。

【０１２０】

ドライブ２００は、次に、ステップＳ１２５において、メディア１０４から読み出したメディアＩＤ（ＩＤｄｉｓｃ）と、ドライブ２００内のメモリに格納した検証データ２０２との比較処理を実行する。

【０１２１】

ドライブ２００は、メディア１０４のＢＣＡから読み出した複数のＢＣＡデータ格納スロットからメディアＩＤ格納スロット（図５参照）の格納データを読み出し、そのヘッダコードと、ドライブ２００内のメモリに格納した検証データ２０２と比較する処理を実行する。前述したように、メディアＩＤ格納スロット（図５参照）のヘッダコードは予め定められた値［０３ｈ］である。この値をヘッダコードとするＢＣＡデータは、ライセンスを受けたメディア製造エンティテイが知り得るが、不正なディスク製造者は知りえない値である。ドライブ２００は、ステップＳ１２５において、検証データ２０２として格納されたメディアＩＤ格納ＢＣＡスロットのヘッダコードの値［０３ｈ］と比較する。

【０１２２】

メディア１００から読み出したヘッタデータの値が、ドライブに格納された検証データ［０３ｈ］と一致すれば、メディア１００は、正当なメディアであると判定し、スイッチ（ＳＷ）をクローズとし、メディアＩＤ（ＩＤｄｉｓｃ）をセッションキー（Ｋｓ）で暗号化して、ホスト３００に出力（ステップＳ１２６）する。

【０１２３】

一方、メディア１００から読み出したヘッタデータの値が、ドライブに格納された検証データ［０３ｈ］と一致しない場合は、メディア１００は、著作権保護技術を利用したコンテンツ記録再生を適用することができないメディアであると判定し、スイッチ（ＳＷ）をオープンとし、メディアＩＤ（ＩＤｄｉｓｃ）のホスト３００に対する出力を中止し、その後の処理を全て中止する。すなわち、コンテンツの再生または記録処理は実行しない。

【０１２４】

ホスト３００側の処理について説明する。ホスト３００はステップＳ１３１でのドライブ２００との相互認証および鍵交換（ＡＫＥ）において相互認証が成立した場合、セッション鍵（Ｋｓ）をドライブ２００と共に共有する。ステップＳ１３２において、ドライブ２００から受信した暗号化ディスクキー、すなわちセッションキー（Ｋｓ）で暗号化されたディスクキー［ＥＫｓ（Ｋｄ）］をセッションキーで復号しディスクキー（Ｋｄ）を取得する。

【０１２５】

さらに、ステップＳ１３３において、ドライブから受領した暗号化メディアＩＤ、すなわち、セッションキー（Ｋｓ）で暗号化されたメディアＩＤ［ＥＫｓ（ＩＤｄｉｓｃ）］をセッションキーで復号しメディアＩＤ（ＩＤｄｉｓｃ）を取得する。

【０１２６】

さらに、ステップＳ１３５において、暗号化コンテンツの復号またはコンテンツの暗号化に適用する記録キー（Ｋｒｅｃ）を生成する。この処理以降は、コンテンツ再生時と、コンテンツ記録時とで異なる処理となる。

【０１２７】

まず、コンテンツ再生時の処理について説明する。コンテンツ再生の際には、ステップＳ１３５において、メディア１０５に格納されたシード情報（Ｓｅｅｄｒｅｃ）と、ディスクキー（Ｋｄ）と、メディアＩＤ（ＩＤｄｉｓｃ）とに基づく暗号処理（トリプルＤＥＳ（ＴＤＥＳ））によって、記録キー（Ｋｒｅｃ）を生成する。なお、この記録キー（Ｋｒｅｃ）生成に際しては、ドライブ２００を介して、メディア１０５に格納されたシード情報（Ｓｅｅｄｒｅｃ）１０５を受領する。シード情報は所定のコンテンツを格納するファイル単位に読み込まれ、コンテンツを格納するファイル毎にシード情報を適用して記録

キー（Ｋｒｅｃ）が生成されて、生成した記録キーによってコンテンツを格納するファイル単位の復号処理が実行され、コンテンツ復号、再生が実行される。

【０１２８】

次に、ステップＳ１３６において、ドライブ２００を介して、メディア１０５に格納された暗号化コンテンツ１０６を受領し、生成した記録キー（Ｋｒｅｃ）を適用した復号処理を実行して、コンテンツを取得してコンテンツ再生を実行する。

【０１２９】

次にコンテンツ記録時の処理について説明する。コンテンツ記録の際には、その後、ステップＳ１３５において、メディア１０５に格納されるシード情報（Ｓｅｅｄｒｅｃ）と、ディスクキー（Ｋｄ）と、メディアＩＤ（ＩＤｄｉｓｃ）とに基づく暗号処理（トリプルＤＥＳ（ＴＤＥＳ））によって、記録キー（Ｋｒｅｃ）を生成する。なお、ステップＳ１３４において、乱数生成処理が実行され、その乱数に基づいてシード情報が生成される。記録対象コンテンツを、コンテンツを格納するファイル単位で暗号化する際の記録キー（Ｋｒｅｃ）が生成され、ステップＳ１３６において、外部入力コンテンツなどのデータが記録キーを適用してコンテンツを格納するファイル単位で暗号化される。

【０１３０】

生成した暗号化コンテンツは、ドライブ２００に出力され、ドライブ２００におけるデータ書き込み処理によってメディア１００に書き込まれる。なお、ステップＳ１３４で生成した乱数は、シード情報１０５として書き込み暗号化コンテンツ１０６に対応付けて書き込まれる。

【０１３１】

次に、メディア１００に格納されたメディアＩＤ（ＩＤｄｉｓｃ）１０４のドライブにおける検証およびホストへの出力処理のシーケンスについて、図９を参照して詳細に説明する。

【０１３２】

図９（ａ）は、メディアに格納されたメディアＩＤ（ＩＤｄｉｓｃ）のドライブにおける検証およびホストへの出力処理の全体シーケンスを示し、図９（ｂ）は、図９（ａ）のステップＳ２５４のＢＣＡレコードの検証処理の詳細を説明するフロー図である。

【０１３３】

図９（ａ）のステップＳ２５１において、ドライブがディスク挿入を検知すると、ステップＳ２５２においてホストとの相互認証および鍵交換（ＡＫＥ）処理が実行され、認証が成立しセッションキー（Ｋｓ）の共有が実行されると、ステップＳ２５３に進む。認証不成立の場合は、ステップＳ２５８に進み、エラーメッセージをホストに通知し、処理を終了する。

【０１３４】

認証が成立した場合は、ステップＳ２５３に進み、ドライブは、メディア（Ｄｉｓｃ）のＢＣＡからＢＣＡスロットデータを読み出し、ステップＳ２５４において、ＢＣＡスロットデータの検証処理を実行する。この検証処理の詳細について、図９（ｂ）のフローを参照して説明する。

【０１３５】

まずステップＳ２６１において、ドライブ内のメモリに格納された検証データを読み出す。図６に示す検証データ２０２である。先に説明したように、この検証データは、ＢＣＡレコード中のメディアＩＤ対応のヘッダの値（本例では０３ｈ）である。

【０１３６】

ステップＳ２６２において、変数（ｉ）の初期設定としてｉ＝０とする設定をする。この変数ｉは、メディアの複数スロットを順次読み出すために設定される変数である。先に図４、図５を参照して説明したようにメディアのＢＣＡは所定データ単位のスロットが複数設定されており、ドライブは各スロット（ｉ＝１～４）を順次読み出す。

【０１３７】

ステップＳ２６３で、変数ｉの更新処理を実行するまずｉ＝１に設定される。次にステ

ップＳ２６４において、メディアのＢＣＡスロット＃ｉからヘッダコードを取得する。ステップＳ２６５においてヘッダコードがドライブの保持している検証データ（図６の検証データ２０２）に一致するか否か、すなわちメディアからの読み出しスロットのヘッダコードが０３ｈに等しいか否かの判定が実行される。

【０１３８】

ステップＳ２６５においてメディアからの読み出しスロットのヘッダコードが０３ｈに等しいと判定された場合は、ステップＳ２６８に進み、メディアがメディアＩＤに対応する正しいヘッダコードを保持した正当なメディアであると判定する。

【０１３９】

ステップＳ２６５においてメディアからの読み出しスロットのヘッダコードが０３ｈに等しくないと判定された場合は、ステップＳ２６６に進み、変数ｉの値がＢＣＡスロット数＝４であるか否かを判定し、ｉ＝４でない場合は、ステップＳ２６３に戻り、変数ｉの更新を実行し、順次、異なるＢＣＡスロットのヘッダコードの読み取り、照合を実行する。ｉ＝４に至るまで、０３ｈに等しいヘッダコードが検出されない場合は、ステップＳ２６７に進み、装着メディアがメディアＩＤに対応する正しいヘッダコードを保持していない、すなわち著作権保護技術を適用したコンテンツの記録再生には利用できないメディアであると判定する。

【０１４０】

この処理の後、図９（ａ）のステップＳ２５５に進む。ステップＳ２５５において、図９（ｂ）に示す検証処理において、装着メディアがメディアＩＤに対応する正しいヘッダコードを保持している正当メディアと判定されたことが確認された場合は、ステップＳ２５６に進み、メディアのＢＣＡスロットから取得したメディアＩＤをセッションキー（Ｋｓ）で暗号化し、ステップＳ２５７において暗号化メディアＩＤをホストからの転送要求に応じてホストに転送する。

【０１４１】

ステップＳ２５５において、図９（ｂ）に示す検証処理において、装着メディアがメディアＩＤに対応する正しいヘッダコードを保持していない著作権保護技術を利用したコンテンツ記録再生の適用できないメディアと判定されたことが確認された場合は、ステップＳ２５８に進み、ホストからの転送要求に対してエラーメッセージをホストに転送し、処理を終了する。

【０１４２】

このように、ドライブは、ホストに対してメディアＩＤを出力する場合、ドライブとホストとの間の相互認証が成立し、さらに、セッションキーの共有に成功したことを条件として、メディアからのＢＣＡレコードのヘッダコードの検証を実行し、ヘッダコードがドライブの保持する検証用データに一致する場合に限り、そのヘッダコードに対応するＢＣＡレコードであるメディアＩＤを読み出して、さらに読み出したメディアＩＤをセッションキーで暗号化してホストに対して出力する。ドライブから出力されるメディアＩＤはセッションキーで暗号化されたデータであり、メディアＩＤが外部に漏洩する可能性は低減される。

【０１４３】

前述したように、メディアＩＤに対応するヘッダコードを持つＢＣＡデータは、非公開データであるので、不正なディスク製造業者が、たとえＢＣＡ領域にデータ書き込み可能な装置を持つ場合であっても、メディアＩＤに対応する正当なヘッダコードを知ることはできず、このような不正な業者の製造したディスクは、正当なメディアＩＤ対応のヘッダコード（例えば０３ｈ）を持たない。従って、このような不正なメディア（ディスク）を利用したコンテンツの再生、あるいはこのような不正なメディア（ディスク）に対するコンテンツの記録は排除されることになる。

【０１４４】

なお、ＢＣＡレコードは、ディスクＩＤのみならず、その他のデータも書き込まれる場合があり、ＢＣＡレコードの中には公開可能なデータも含まれる。このような著作権保護

技術と関係しない秘匿性の低いデータについては、ホストへの出力について特に制限されることはない。図１０には、このような秘匿性の低いＢＣＡデータをドライブからホストへ出力する場合の処理を説明するフローを示している。

【０１４５】

図１０（ａ）は、メディアに格納されたメディアＩＤ（ＩＤｄｉｓｃ）以外の秘匿性の低いＢＣＡデータのホストへの出力処理の全体シーケンスを示し、図１０（ｂ）は、図１０（ａ）のステップＳ２７３のＢＣＡレコードの検証処理の詳細を説明するフロー図である。なお、ここでは、ヘッダコード≠０３ｈが秘匿性の低いＢＣＡデータに対応するヘッダコードであるとする。

【０１４６】

図１０（ａ）のステップＳ２７１において、ドライブがディスク挿入を検知すると、ステップＳ２７２に進み、ドライブは、メディア（Ｄｉｓｃ）のＢＣＡからＢＣＡスロットデータを読み出し、ステップＳ２７３において、ＢＣＡスロットレコードの検証処理を実行する。この検証処理の詳細について、図１０（ｂ）のフローを参照して説明する。

【０１４７】

まずステップＳ２８１において、変数（ｉ）の初期設定としてｉ＝０とする設定をする。この変数ｉは、メディアの複数スロットを順次読み出すために設定される変数である。ステップＳ２８２で、変数ｉの更新処理を実行するまずｉ＝１に設定される。次にステップＳ２８３において、メディアのＢＣＡスロット＃ｉからヘッダコードを取得する。ステップＳ２８４においてヘッダコードが秘匿性の低いＢＣＡデータ対応のヘッダコード（０３ｈ）に一致するか否か、すなわちメディアからの読み出しスロットのヘッダコードが０３ｈに等しいか否かの判定が実行される。

【０１４８】

ステップＳ２８４においてメディアからの読み出しスロットのヘッダコードが０３ｈに等しくないと判定された場合は、ステップＳ２８７に進み、メディアが出力可能なＢＣＡデータを保持していると判定する。

【０１４９】

ステップＳ２８４においてメディアからの読み出しスロットのヘッダコードが０３ｈに等しいと判定された場合は、ステップＳ２８５に進み、変数ｉの値がＢＣＡスロット数＝４であるか否かを判定し、ｉ＝４でない場合は、ステップＳ２８２に戻り、変数ｉの更新を実行し、順次、異なるＢＣＡスロットのヘッダコードの読み取り、照合を実行する。ｉ＝４に至るまで、０３ｈに等しくないヘッダコードが検出されない場合は、ステップＳ２８６に進み、装着メディアには、出力可能なＢＣＡデータを保持していないと判定する。

【０１５０】

この処理の後、図１０（ａ）のステップＳ２７４に進む。ステップＳ２７４において、図１０（ｂ）に示す検証処理において、装着メディアが出力可能なＢＣＡデータを保持していると判定されたことが確認された場合は、ステップＳ２７５に進み、メディアのＢＣＡスロットから取得したＢＣＡデータをホストからの転送要求に応じてホストに転送する。

【０１５１】

ステップＳ２７４において、図１０（ｂ）に示す検証処理において、装着メディアが出力可能なＢＣＡデータを保持していないと判定されたことが確認された場合は、ステップＳ２７６に進み、ホストからの転送要求に対してエラーメッセージをホストに転送し、処理を終了する。

【０１５２】

次に、メディアを利用したコンテンツの再生または記録処理においてドライブの実行する処理と、ホストの実行する処理について、それぞれ個別のフローを参照して説明する。

【０１５３】

まず、図１１、図１２を参照してドライブ側の処理について説明する。ドライブは、図１１のステップＳ３０１において、メディア（ディスク）の装着を検知すると、ステップ

Ｓ３０２において、メディア（ディスク）から暗号化キーブロックとしてメディアキー（Ｋｍ）を暗号化データとして格納したＲＫＢを読み出す。

【０１５４】

ステップＳ３０３において、ＲＫＢの読み取りに失敗したと判定された場合は、図１２に示す［Ｅ］に進み、ステップＳ３３１において、挿入されたメディアを利用した著作権保護の必要なＡＶデータ（コンテンツ）の記録を禁止し、著作権保護対象とされない暗号処理の不要なデータの記録再生のみを許容する。

【０１５５】

ステップＳ３０３において、ＲＫＢの読み取りに成功したと判定された場合は、ステップＳ３０４において、ドライブに格納されたデバイスキー（Ｋｄｅｖ）を適用したＲＫＢの処理を実行する。ＲＫＢの処理に失敗し、メディアキー（Ｋｍ）を取得できなかった場合は、ドライブはリボークされていると判定（ステップＳ３０５：Ｙｅｓ）し、図１２［Ｅ］のステップＳ３３１に進み、著作権保護対象データでないコンテンツのみの記録再生処理のみを許容する。

【０１５６】

ＲＫＢの処理に成功した場合は、ドライブはリボークされていないと判定（ステップＳ３０５：Ｎｏ）し、ステップＳ３０６で、ＲＫＢからのメディアキー（Ｋｍ）の取得を行う。次に、ステップＳ３０７において、メディアのＢＣＡからのＢＣＡレコードの読み取りを行い、ステップＳ３０８において、ＢＣＡスロットデータの検証処理を実行する。

【０１５７】

メディアＩＤの読み取りに失敗（Ｓ３０９：Ｎｏ）した場合は、図１２［Ｅ］のステップＳ３３１に進み、著作権保護対象データでないコンテンツのみの記録再生処理のみを許容する。

【０１５８】

メディアＩＤの読み取りに成功（Ｓ３０９：Ｙｅｓ）した場合は、ステップＳ３１０に進み、ホストからの相互認証処理要求を待機し、ホストからの相互認証処理要求があると、ステップＳ３１１において、ホスト－ドライブ間の相互認証および鍵交換（ＡＫＥ）処理（図７参照）を実行して、ホストとドライブ相互において、セッションキー（Ｋｓ）を共有する。ステップＳ３１２において、相互認証および鍵交換（ＡＫＥ）処理の完了を確認し、ステップＳ３１３において、ホストからの鍵情報の転送要求を待機し、ホストからの鍵情報の転送要求があると、ステップＳ３１４において、セッションキー（Ｋｓ）を適用して暗号化したメディアＩＤ、すなわち［ＥＫｓ（ＩＤｄｉｓｃ）］と、セッションキー（Ｋｓ）を適用して暗号化したディスクキー、すなわち［ＥＫｓ（Ｋｄ）］を生成して、ホストへ転送する。

【０１５９】

ステップＳ３１５において鍵情報の転送の完了を確認すると、図１２のステップ３２１に進む。ステップＳ３２１では新たな相互認証要求を待機し、新たな相互認証要求が発生した場合は、［Ｄ］、すなわちステップＳ３１１に戻り、相互認証以下の処理を実行する。この処理は、ホスト側でアプリケーションの切り替えが行なわれた場合に発生する処理である。

【０１６０】

ステップＳ３２２ではディスクの排出の有無を判定し、ディスクが排出された場合は、初期状態［Ａ］、すなわちステップＳ３０１に戻る。ステップＳ３２３では、ホストからのコンテンツ（ＡＶデータ）の読み出し要求の有無を判定し、ホストからのコンテンツ（ＡＶデータ）の読み出し要求があった場合は、ステップＳ３２６で、メディアからのコンテンツの読み出しを実行し、ホストへ転送する。なお、この処理の際には、コンテンツ復号処理に直接適用するブロックキーの生成に適用するシード情報も適時実施されるホストからの読みだし要求に応じてメディアから読み出してホストへ転送する。

【０１６１】

さらに、ステップＳ３２４において、ホストからのコンテンツ（ＡＶデータ）の書き込

み要求の有無を判定し、ホストからのコンテンツ（ＡＶデータ）の書き込み要求があった場合は、ステップＳ３２５で、ホストからコンテンツ（ＡＶデータ）を入力し、入力コンテンツをメディアへ書き込む処理を実行する。なお、この処理の際には、コンテンツ暗号化処理に適用するブロックキーの生成に適用した乱数も適時ホストから入力し、これをシード情報としてメディアに書き込む処理を実行する。

【０１６２】

次に、図１３、図１４を参照して、ホスト側の処理について説明する。ステップＳ４０１において、コンテンツ再生アプリケーション、あるいはコンテンツ記録アプリケーション・プログラムを起動し、ステップＳ４０２においてディスクがドライブに挿入されたことの通知を受領すると、ステップＳ４０３でドライブとの相互認証、セッションキーの共有処理を実行する。

【０１６３】

ステップＳ４０４において、相互認証および鍵交換（ＡＫＥ）処理の完了が確認されると、ステップＳ４０５に進み、ホストは、ドライブに対して、セッションキー（Ｋｓ）で暗号化されたディスクキー（Ｋｄ）の転送を要求する。

【０１６４】

ステップＳ４０６において、暗号化ディスクキー［ＥＫｓ（Ｋｄ）］のドライブからの受信を確認すると、ステップＳ４０７において、セッションキーＫｓを適用して暗号化ディスクキー［ＥＫｓ（Ｋｄ）］の復号を実行し、ディスクキー（Ｋｄ）を取得する。

【０１６５】

さらに、ホストはステップＳ４０８において、ドライブに対して、セッションキー（Ｋｓ）で暗号化されたメディアＩＤ（ＩＤｄｉｓｃ）の転送を要求する。ステップＳ４０９において、暗号化メディアＩＤ［ＥＫｓ（ＩＤｄｉｓｃ）］のドライブからの受信を確認すると、ステップＳ４１０において、セッションキーＫｓを適用して暗号化メディアＩＤ［ＥＫｓ（ＩＤｄｉｓｃ）］の復号を実行し、メディアＩＤ（ＩＤｄｉｓｃ）を取得する。

【０１６６】

ホストは、ステップＳ４１１において、コンテンツの記録・再生の準備が整うこととなり、画面表示などのユーザーインターフェイスを通じてコンテンツ記録再生レディであることをユーザへ知らせることができる。

【０１６７】

次に、記録または再生ソフトウェアの完了（Ｓ４２１）がなされておらず、ディスク排出がない（Ｓ４２２）ことの確認の後、ユーザの指示などによりコンテンツの読み出しを行うと判定した場合（Ｓ４２３：Ｙｅｓ）は、ステップＳ４３１においてドライブに対して暗号化コンテンツ（ＡＶデータ）の転送要求を出力する。

【０１６８】

ステップＳ４３２において、ドライブからのコンテンツ受信の完了を確認（Ｓ４３２：Ｙｅｓ）すると、ステップＳ４３３でドライブから適時取得したディスクへ記録されているシード情報（Ｓｅｅｄｒｅｃ）、ディスクキー（Ｋｄ）と、メディアＩＤ（ＩＤｄｉｓｃ）から記録キー（Ｋｒｅｃ）を計算し、計算された記録キー（Ｋｒｅｃ）を適用して、ドライブから受信した暗号化コンテンツの復号処理を実行してコンテンツの再生を可能とする。なお、前述したように、記録キー（Ｋｒｅｃ）を計算する際には、シード情報が所定のコンテンツ単位に適用され所定単位のコンテンツ毎に異なるシード情報が生成されて、コンテンツの記録時にディスクへ同時に記録されている。

【０１６９】

一方、ステップＳ４２４において、ユーザの指示などによりコンテンツの書き込みを行うと判定した場合（Ｓ４２４：Ｙｅｓ）は、ステップＳ４２５に進み、ホストは、適時乱数生成して得られたシード情報（Ｓｅｅｄｒｅｃ）、ドライブから受信したディスクキー（Ｋｄ）と、メディアＩＤ（ＩＤｄｉｓｃ）とを適用して生成した記録キー（Ｋｒｅｃ）を適用してコンテンツの暗号化処理を実行する。なお、前述したように、コンテンツ暗号

化処理においては、乱数を生成し、生成した乱数を用いてブロック単位の暗号化キーとしてのブロックキーを生成し、生成したブロックキーによってブロックデータ単位の暗号化処理が実行される。

【０１７０】

ホストは、ステップＳ４２６においてドライブに対して生成した暗号化データの転送（出力）処理を実行し、ステップＳ４２７において転送完了を確認して処理を終了する。

【０１７１】

［３．情報処理装置の構成］

次に、図１５、図１６を参照して、ホストおよびドライブの情報処理装置構成例について説明する。

【０１７２】

まず、図１５を参照して、ホストとしての情報処理装置の構成について説明する。情報処理装置８００は、ＯＳやコンテンツ再生または記録アプリケーション・プログラム、相互認証処理プログラムなどの各種プログラムに従ったデータ処理を実行するＣＰＵ８０９、プログラム、パラメータ等の記憶領域としてのＲＯＭ８０８、メモリ８１０、デジタル信号を入出力する入出力Ｉ／Ｆ８０２、アナログ信号を入出力し、Ａ／Ｄ，Ｄ／Ａコンバータ８０５を持つ入出力Ｉ／Ｆ８０４、ＭＰＥＧデータのエンコード、デコード処理を実行するＭＰＥＧコーデック８０３、ＴＳ（Transport Stream）・ＰＳ(Program Stream)処理を実行するＴＳ・ＰＳ処理手段８０６、相互認証、暗号化コンテンツの復号処理など各種の暗号処理を実行する暗号処理手段８０７、ハードディスクなどの記録媒体８１２、記録媒体８１２の駆動、データ記録再生信号の入出力を行なうドライブ８１１を有し、バス８０１に各ブロックが接続されている。

【０１７３】

情報処理装置（ホスト）８００は、例えばＡＴＡＰＩ－ＢＵＳ等の接続バスによってドライブと接続され、上述したセッションキーによって暗号化されたメディアＩＤやディスクキーなどの秘密情報、あるいは転送コンテンツなどは、デジタル信号用入出力Ｉ／Ｆ８０２を介して入出力される。暗号化処理、復号処理は、暗号化処理手段８０７によって、例えば、トリプルＤＥＳ、ＡＥＳアルゴリズムなどを適用して実行される。

【０１７４】

なお、コンテンツ再生あるいは記録処理を実行するプログラムは例えばＲＯＭ８０８内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ８１０を使用する。

【０１７５】

ＲＯＭ８０８または記録媒体８１２には、管理センタの公開鍵、ホスト対応秘密鍵、ホスト対応の公開鍵証明書、さらに、リボケーションリストが格納されている。

【０１７６】

次に、図１６を参照して、情報記録媒体の格納コンテンツの読み取りおよび記録、ホストとのデータ転送を実行するドライブとしての情報処理装置の構成について説明する。ドライブ８５０は、コンテンツ読み取り、コンテンツ記録、転送処理プログラム、相互認証処理プログラムなどの各種プログラムに従ったデータ処理を実行するＣＰＵ８５２、プログラム、パラメータ等の記憶領域としてのＲＯＭ８５５、メモリ８５６、デジタル信号を入出力する入出力Ｉ／Ｆ８５３、相互認証、出力データの暗号化処理など各種の暗号処理を実行する暗号処理手段８５４、ＤＶＤ，Ｂｌｕ－ｒａｙディスクなどの情報記録媒体８５８の駆動、データ記録再生信号の入出力を行なう記録媒体Ｉ／Ｆ８５７を有し、バス８５１に各ブロックが接続されている。

【０１７７】

ドライブ８５０は、例えばＡＴＡＰＩ－ＢＵＳ等の接続バスによってホストと接続される。例えばメディアＩＤやディスクキーなどの秘密情報、さらに、情報記録媒体８５８に格納された暗号化コンテンツ、情報記録媒体８５８に記録する暗号化コンテンツなどは、外部機器とのデータ転送用インタフェースとして設定された入出力Ｉ／Ｆ８５３を介して

入出力される。暗号化処理、復号処理は、暗号化処理手段８５４によって、例えば、トリプルＤＥＳ、ＡＥＳアルゴリズムなどを適用して実行される。

【０１７８】

なお、ＲＯＭ８５５、またはメモリ８５６には、管理センタの公開鍵、ドライブに対応する秘密鍵、ドライブに対応する公開鍵証明書、および暗号鍵ブロックＲＫＢの処理に適用するためのデバイスキー：Ｋｄｅｖ、さらに、前述のメディアＩＤ対応のヘッダコードとしての検証情報（図６に示す検証データ２０２）が格納されている。また、コンテンツの読み取り、取得、および相互認証処理を実行するプログラム等が格納されている。

【０１７９】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

【０１８０】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１８１】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１８２】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０１８３】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０１８４】

以上、説明したように、本発明の構成によれば、ドライブとホストなど２つの異なるデバイス間のデータ転送を伴うコンテンツの再生あるいは記録処理において、コンテンツの記録、再生を行なう場合に実行するコンテンツの暗号化または復号処理に適用するメディアＩＤ（ディスクＩＤ）の外部漏洩を防止することができる。

【０１８５】

本発明の構成によれば、ドライブがメディアＩＤ（ディスクＩＤ）をメディアから読み取り、これが正しい正当なメディアに設定されたヘッダコードに対応して記録されているかをドライブ側で検証し、さらに、検証によって、正当なメディアであることが確認された場合に、ドライブ側でメディアＩＤを暗号化してホストに出力する構成としたので、メ

ディアＩＤの外部漏洩の可能性を低減させることが可能となり、また、正当なメディアであることの確認を条件として、コンテンツの再生または記録処理を許容する構成としたので、不正なメディアを利用したコンテンツの再生または記録処理の防止が実現される。

【図面の簡単な説明】

【０１８６】

【図１】ＣＰＲＭに従ったコンテンツ記録再生処理シーケンスについて説明する図である。

【図２】ＣＰＲＭに従ったコンテンツ記録再生処理シーケンスについて説明する図である。

【図３】ＣＰＲＭに従ったコンテンツ記録再生処理におけるＭＡＣ検証に基づく処理制御シーケンスを説明するフロー図である。

【図４】ＢＣＡ領域のデータ構成について説明する図である。

【図５】ＢＣＡ領域に記録されるメディアＩＤ（ディスクＩＤ）のデータフォーマットについて説明する図である。

【図６】本発明に従ったホスト－ドライブ間のコンテンツ転送を伴うコンテンツ記録再生処理について説明する図である。

【図７】ホスト－ドライブ間の相互認証および鍵交換処理シーケンスについて説明する図である。

【図８】公開鍵証明書のデータ構成について説明する図である。

【図９】ＢＣＡ領域に記録されるメディアＩＤ（ディスクＩＤ）の転送および検証処理シーケンスについて説明するフロー図である。

【図１０】ＢＣＡ領域に記録されるメディアＩＤ（ディスクＩＤ）以外の出力可能データの転送および検証処理シーケンスについて説明するフロー図である。

【図１１】本発明に従ったホスト－ドライブ間のコンテンツ転送を伴うコンテンツ記録再生処理におけるドライブ側の処理シーケンスを説明するフロー図である。

【図１２】本発明に従ったホスト－ドライブ間のコンテンツ転送を伴うコンテンツ記録再生処理におけるドライブ側の処理シーケンスを説明するフロー図である。

【図１３】本発明に従ったホスト－ドライブ間のコンテンツ転送を伴うコンテンツ記録再生処理におけるホスト側の処理シーケンスを説明するフロー図である。

【図１４】本発明に従ったホスト－ドライブ間のコンテンツ転送を伴うコンテンツ記録再生処理におけるホスト側の処理シーケンスを説明するフロー図である。

【図１５】本発明のホストとしての情報処理装置の構成例を示す図である。

【図１６】本発明のドライブとしての情報処理装置の構成例を示す図である。

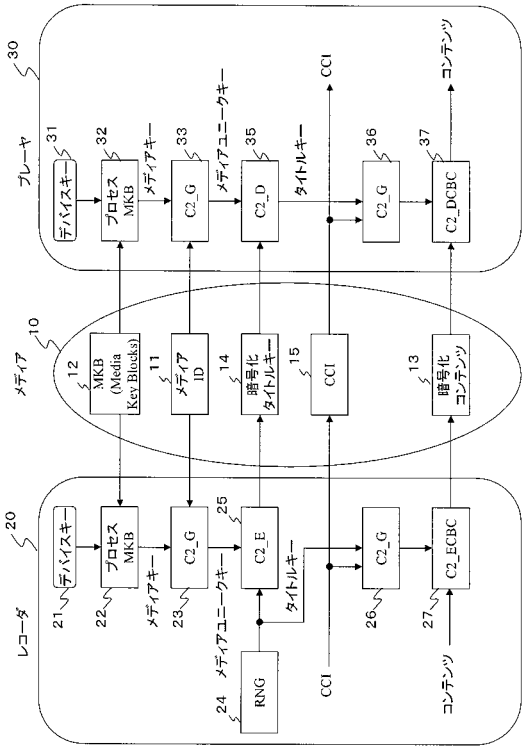
【符号の説明】

【０１８７】

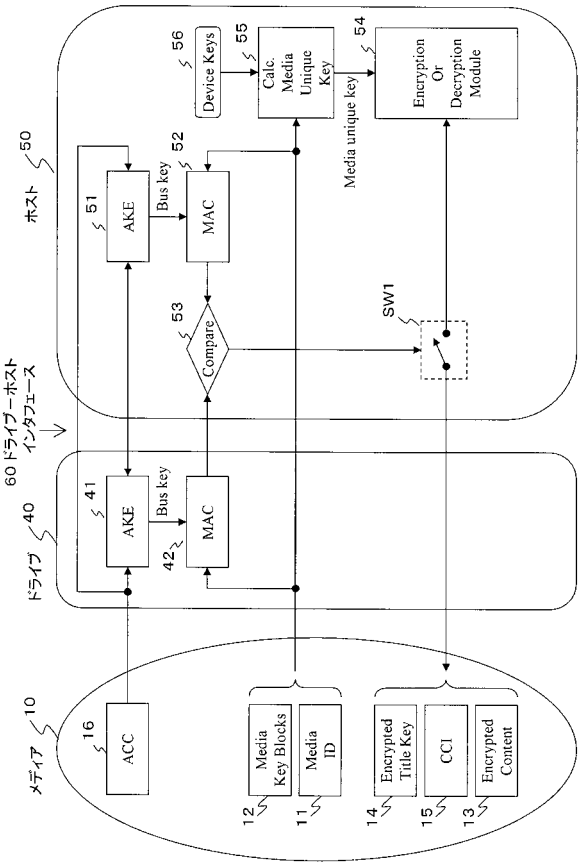
１０　メディア
１１　メディアＩＤ
１２　ＭＫＢ
１３　暗号化コンテンツ
１４　暗号化タイトルキー
１５　コピー制御情報（ＣＣＩ）
２０　レコーダ
２１　デバイスキー
２２　プロセスＭＫＢ
３０　プレーヤ
３１　デバイスキー
３２　プロセスＭＫＢ
４０　ドライブ
５０　ホスト
１００　メディア

１０１　リボーク情報
１０２　ＲＫＢ
１０３　暗号化ディスクキー
１０４　メディアＩＤ
１０５　シード情報
１０６　暗号化コンテンツ
２００　ドライブ
２０１　デバイスキー
２０２　検証データ
３００　ホスト
３０１　リボーク情報
８００　情報処理装置
８０１　バス
８０２　入出力Ｉ／Ｆ
８０３　ＭＰＥＧコーデック
８０４　入出力Ｉ／Ｆ
８０５　Ａ／Ｄ，Ｄ／Ａコンバータ
８０６　ＴＳ・ＰＳ処理手段
８０７　暗号処理手段
８０８　ＲＯＭ
８０９　ＣＰＵ
８１０　メモリ
８１１　ドライブ
８１２　記録媒体
８５０　ドライブ装置
８５１　バス
８５２　ＣＰＵ
８５３　入出力Ｉ／Ｆ
８５４　暗号処理手段
８５５　ＲＯＭ
８５６　メモリ
８５７　記録媒体Ｉ／Ｆ
８５８　情報記録媒体

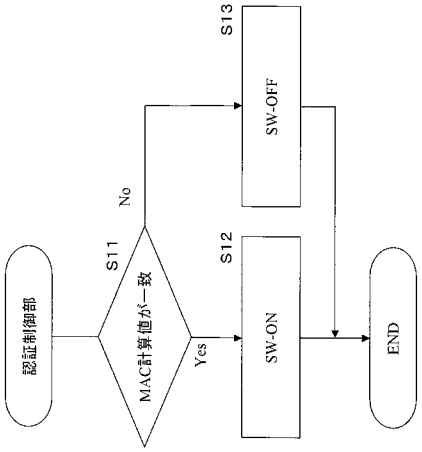
【図１】


レコーダ
20
21 デバイスキー
22 プロセスMKB
23 C2_G
24 RNG
25 C2_E
26 C2_G
27 C2_ECBC
メディアキー
メディアユニークキー
タイトルキー
CCI
コンテンツ
メディア
10
12 MKB (Media Key Blocks)
11 メディアID
14 暗号化タイトルキー
15 CCI
13 暗号化コンテンツ
プレーヤ
30
31 デバイスキー
32 プロセスMKB
33 C2_G
35 C2_D
36 C2_G
37 C2_DCBC

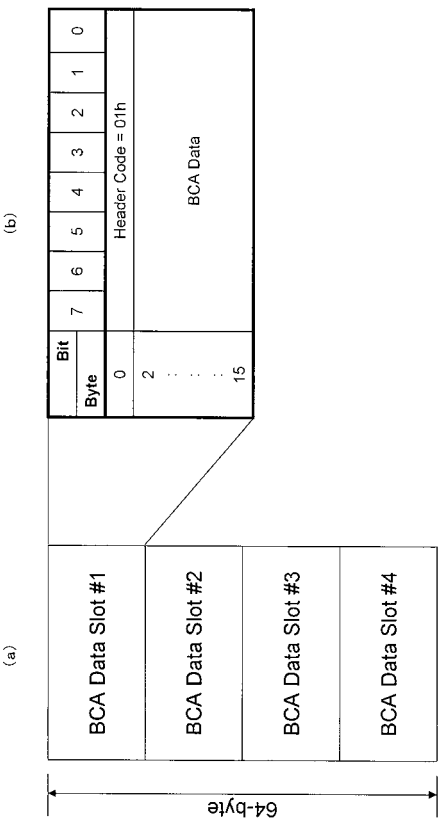
【図２】


ホスト
50
51 AKE
52 MAC
53 Compare
SW1
56 Device Keys
55 Calc. Media Unique Key
54 Encryption Or Decryption Module
Bus key
Media unique key
60 ドライブ-ホスト インタフェース
ドライブ
40
41 AKE
42 MAC
Bus key
メディア
10
16 ACC
12 Media Key Blocks
11 Media ID
14 Encrypted Title Key
15 CCI
13 Encrypted Content

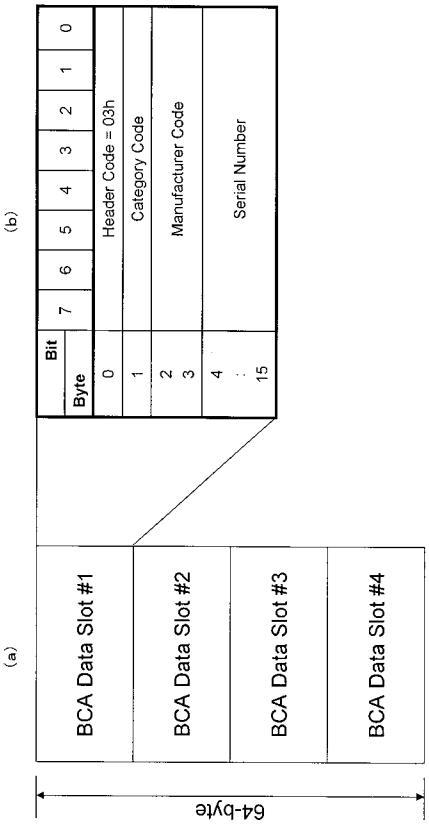
【図３】


認証制御部
S11
MAC計算値が一致
No
Yes
S12
SW-ON
S13
SW-OFF
END

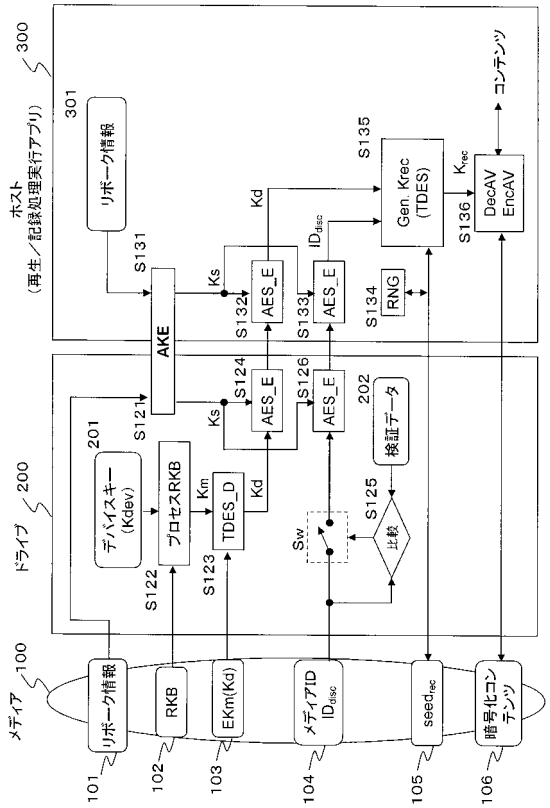
【図４】


(a)
BCA Data Slot #1
BCA Data Slot #2
BCA Data Slot #3
BCA Data Slot #4
64-byte
(b)
Byte
Bit
7 6 5 4 3 2 1 0
0
2
15
Header Code = 01h
BCA Data

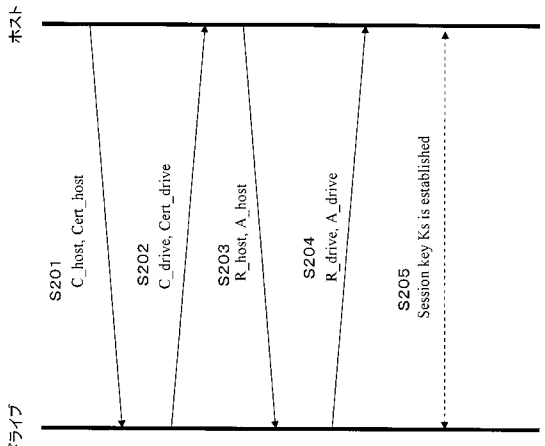
【図５】


(a)
BCA Data Slot #1
BCA Data Slot #2
BCA Data Slot #3
BCA Data Slot #4
64-byte
(b)
Bit 7 6 5 4 3 2 1 0
Byte
0 Header Code = 03h
1 Category Code
2 3 Manufacturer Code
4 : 15 Serial Number

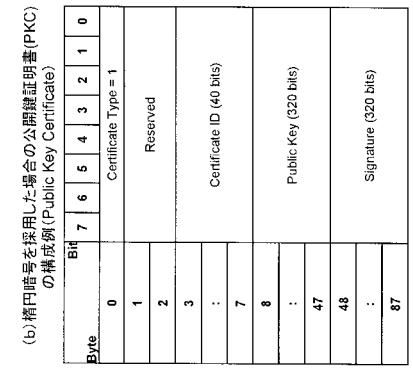
【図６】


ホスト
(再生／記録処理実行アプリ)
300
301
リボーク情報
S131
AKE
Ks
S132
AES_E
Kd
S133
AES_E
IDdisc
S134
RNG
S135
Gen. Krec (TDES)
S136
Krec
DecAV EncAV
コンテンツ
ドライブ
200
201
デバイスキー (Kdev)
S121
プロセスRKB
Km
S122
TDES_D
S123
Kd
S124
AES_E
S125
比較
Sw
S126
AES_E
202
検証データ
メディア
100
リボーク情報
RKB
EKm(Kd)
メディアID IDdisc
seeddisc
暗号化コンテンツ
101
102
103
104
105
106

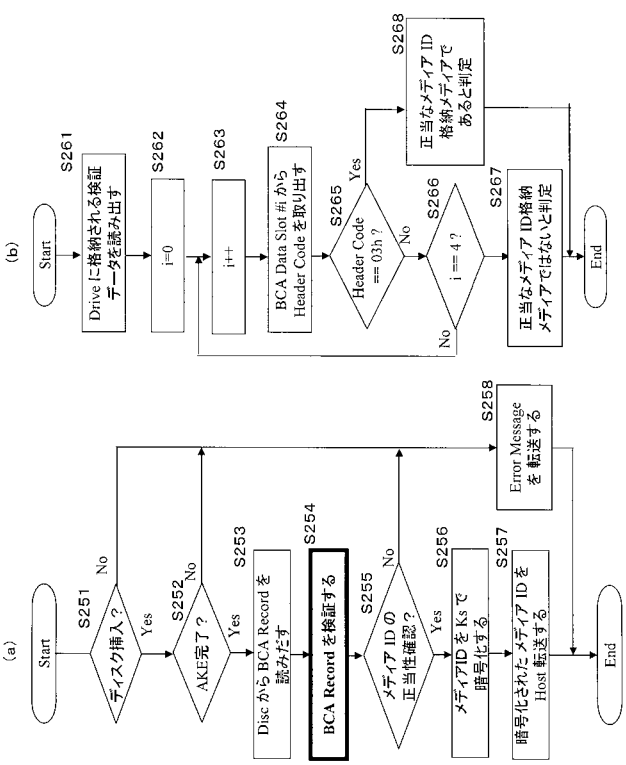
【図７】


ホスト
ドライブ
S201
C_host, Cert_host
S202
C_drive, Cert_drive
S203
R_host, A_host
S204
R_drive, A_drive
S205
Session key Ks is established

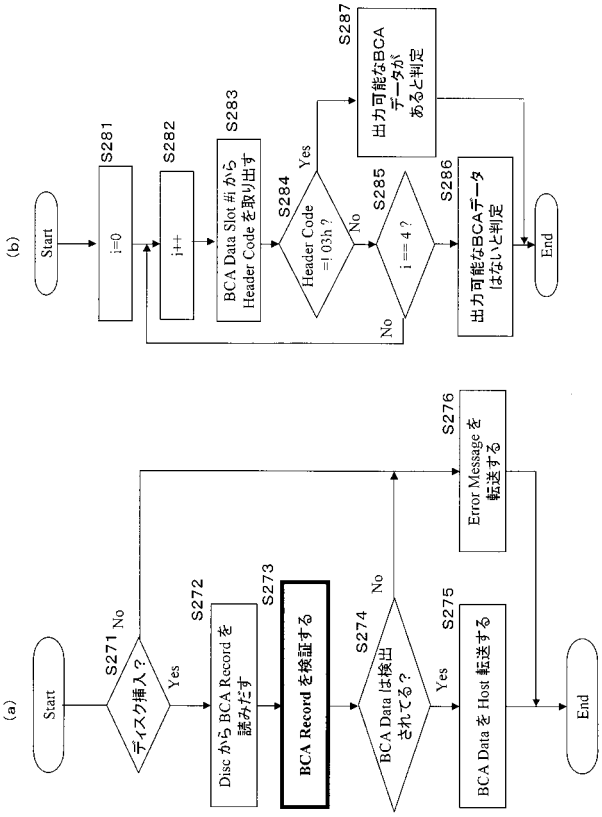
【図８】


(b) 楕円暗号を採用した場合の公開鍵証明書(PKC)の構成例 (Public Key Certificate)
Bit 7 6 5 4 3 2 1 0
Byte
0 Certificate Type = 1
1 2 Reserved
3 : 7 Certificate ID (40 bits)
8 : 47 Public Key (320 bits)
48 : 87 Signature (320 bits)
(a) 公開鍵証明書(PKC)データ
証明書ID (Certificate ID)
公開鍵 (Public Key)
その他情報 Other information (e.g. version, issuer)

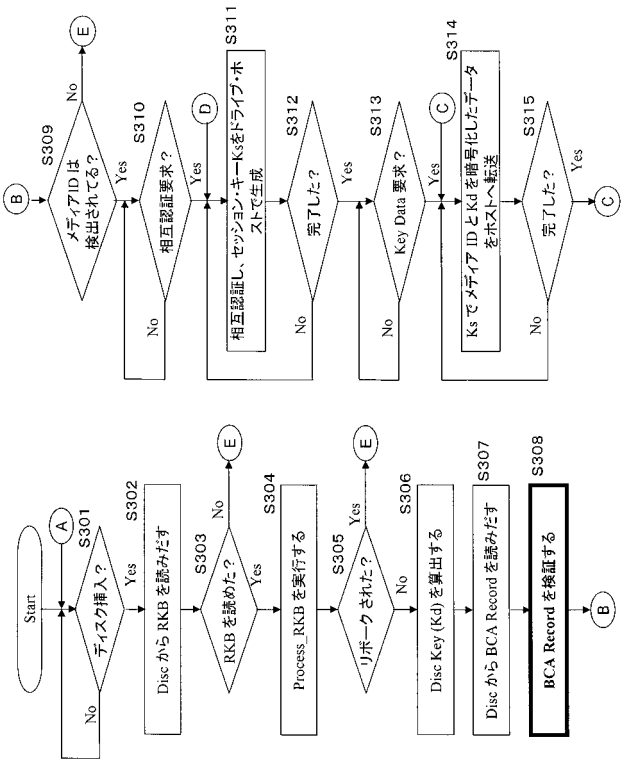
【図９】



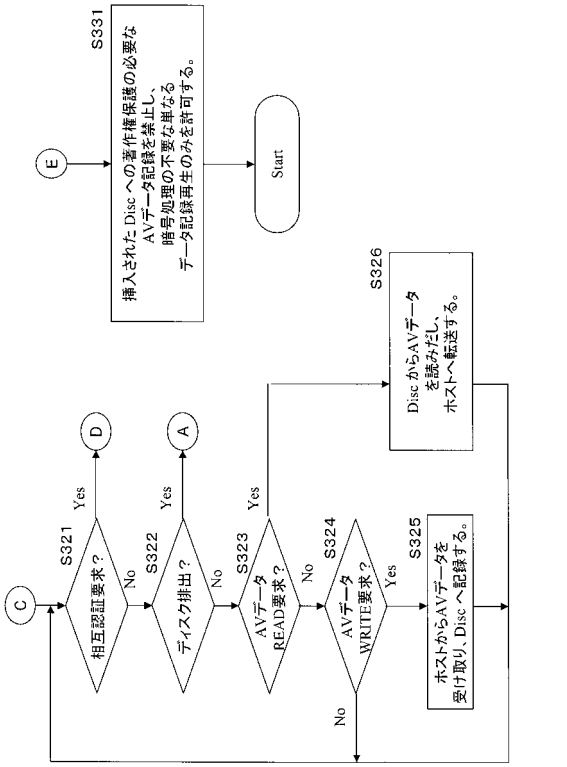
【図１０】



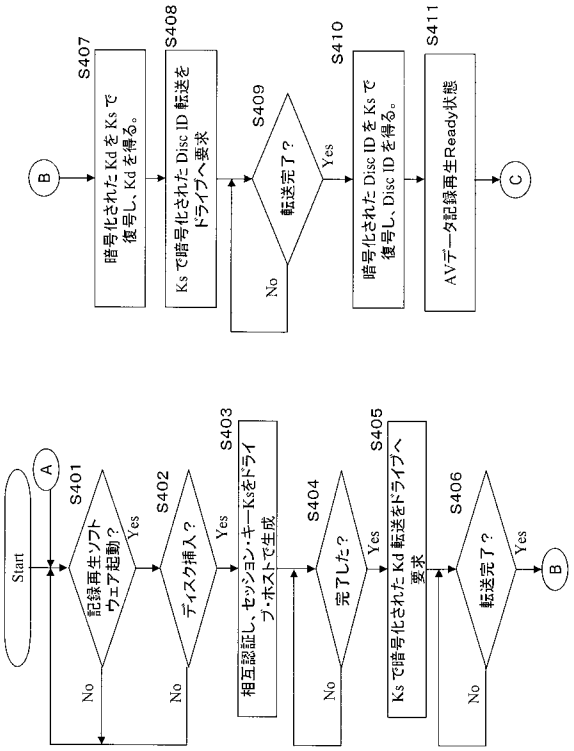
【図１１】



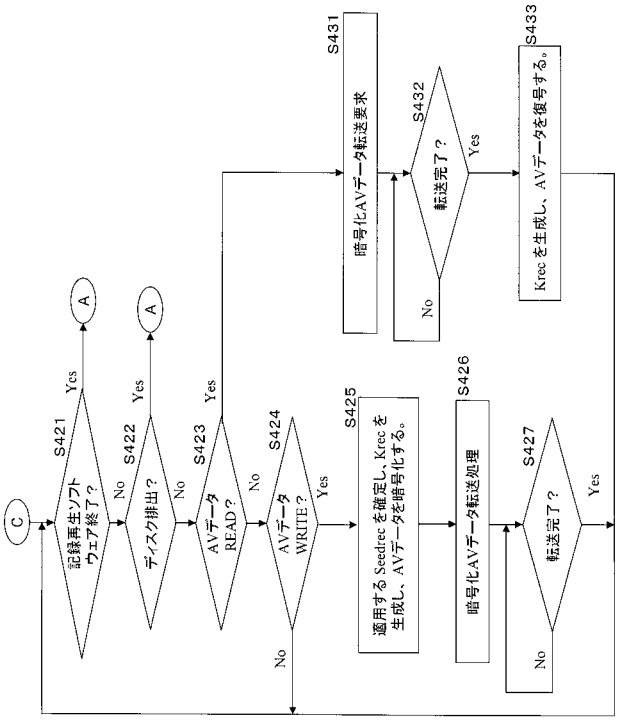
【図１２】



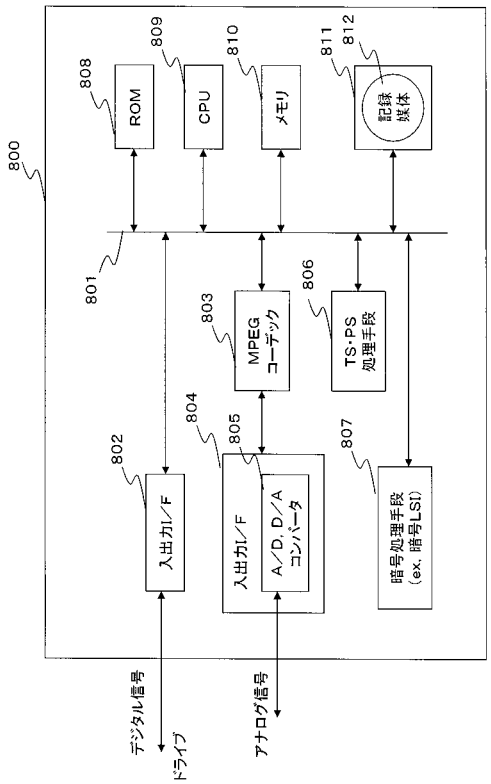
【図１３】



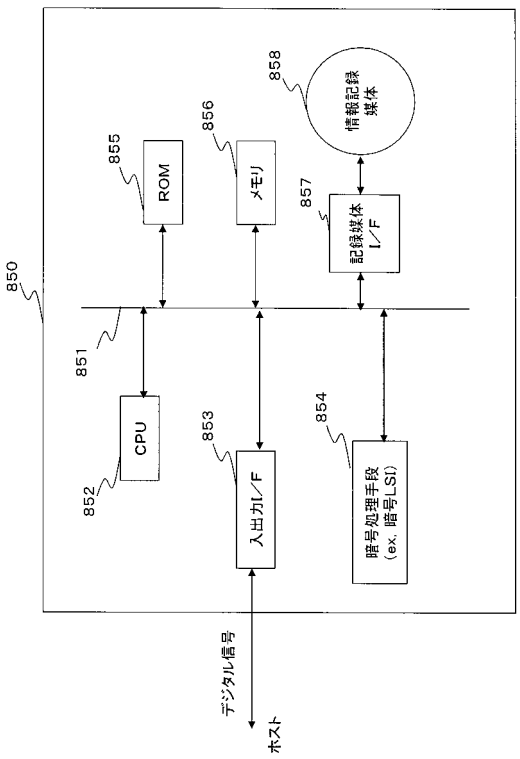
【図１４】



【図１５】



【図１６】



フロントページの続き

(51)Int.Cl.			F I			テーマコード（参考）
H04L	***9/32***	***(2006.01)***	G09C	1/00	640E	
H04N	***5/91***	***(2006.01)***	G11B	20/12		
			G11B	27/00	D	
			H04L	9/00	673C	
			H04N	5/91	P	

Fターム(参考) 5B017 BA05 BA07 BB10
5C053 FA13 FA23 KA24
5D044 BC04 CC06 DE49 DE50 DE54 GK12 GK17 HL08
5D110 AA16 AA17 BB01 DA08 DA11 DB02 DE01
5J104 AA07 AA16 EA26 KA02 PA07 PA14