(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3984749号
(P3984749)
(45)発行日　平成19年10月3日(2007.10.3)　(24)登録日　平成19年7月13日(2007.7.13)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G11B 20/10 | (2006.01) | G11B | 20/10 | H |
| H04L 9/14 | (2006.01) | H04L | 9/00 | 641 |
| H04N 5/91 | (2006.01) | H04N | 5/91 | P |
| H04N 5/92 | (2006.01) | H04N | 5/92 | H |
| H04N 7/167 | (2006.01) | H04N | 7/167 | Z |

請求項の数 6　(全 13 頁)

(21)出願番号　特願平11-102153
(22)出願日　平成11年4月9日(1999.4.9)
(65)公開番号　特開2000-3559(P2000-3559A)
(43)公開日　平成12年1月7日(2000.1.7)
審査請求日　平成13年1月17日(2001.1.17)
審判番号　不服2005-4625(P2005-4625/J1)
審判請求日　平成17年3月17日(2005.3.17)
(31)優先権主張番号　特願平10-102386
(32)優先日　平成10年4月14日(1998.4.14)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　川前　治
神奈川県横浜市戸塚区吉田町２９２番地株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　竹内　敏文
神奈川県横浜市戸塚区吉田町２９２番地株式会社日立製作所マルチメディアシステム開発本部内

最終頁に続く

(54)【発明の名称】認証方法、データ処理装置

(57)【特許請求の範囲】

【請求項１】

符号化されたデータを出力する符号化データ出力装置とディスク状の記録媒体にデータを記録する記録装置間でコピー制御されたデータの受け渡しを行うときに装置間の認証を行う認証方法において、

前記符号化データ出力装置と記録装置との間で認証を行う関係にあり、

受け渡すデータは、複数の暗号方法からデータのコピー制御の情報に対応した暗号方法が選択され、選択された暗号方法により暗号化されており、

前記符号化データ出力装置と記録装置は前記選択された暗号方法に対応した認証方法を複数の認証方法から選択し、前記選択された認証方法により前記符号化データ出力装置と記録装置間の認証を行うことを特徴とする認証方法。

【請求項２】

請求項１に記載の認証方法において、

前記複数の暗号方法は、前記記録媒体の種類を示す情報と記録するデータのコピーを制御する情報との組み合わせに対応した暗号化処理を行う暗号化処理ステップを備え、

認証の結果によりデータの受け渡しの制御を行うようにしたことを特徴とする認証方法。

【請求項３】

請求項２に記載の認証方法において、

前記記録媒体の種類を示す情報は、再生専用の媒体か記録可能な媒体かを示す情報を備え、前記記録するデータのコピーを制御する情報は、コピー制限がないか、コピー禁止か

、一世代だけコピー可能かを示す情報を備えていることを特徴とする認証方法。
【請求項４】
請求項２に記載の認証方法において、
前記組み合わせは少なくとも、記録可能な媒体であってかつコピー禁止か一世代だけコピー可能かを示す情報と、記録可能な媒体であってコピー制限がないとの情報という２種類の組み合わせを有することを特徴とする認証方法。
【請求項５】
データを再生し出力する再生装置と画像復号装置間でコピー制御されたデータの受け渡しを行うときに装置間の認証を行う認証方法において、
前記再生装置と画像復号装置との間で認証を行う関係にあり、
受け渡すデータは、複数の暗号方法からデータのコピー制御の情報に対応した暗号方法が選択され、選択された暗号方法により暗号化されており、
前記再生装置と画像復号装置は前記選択された暗号方法に対応した認証方法を複数の認証方法から選択し、前記選択された認証方法により前記再生装置と画像復号装置間の認証を行うことを特徴とする認証方法。
【請求項６】
データバスを介して、データの受け渡しを行う複数のデータ処理手段を備えたデータ処理装置において、
前記複数のデータ処理手段は、それぞれ複数の認証手段を備え、データ処理手段とデータ処理手段との間で認証を行う関係にあり、
データのコピーを制御するために、前記データ処理手段の間で受け渡しを行うデータのコピー制御の情報に対応した暗号手段がそれぞれのデータ処理手段で複数の暗号手段から選択され、選択された暗号手段に対応した認証手段を前記複数の認証手段から選択して、前記データ処理手段間の認証を行うことを特徴とするデータ処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は画像や音声データを再生する再生装置に関わり、特に記録媒体をコピー管理情報によって再生及び／又は記録を制御するデータ再生装置及びデータ記録装置に関する。
【０００２】
【従来の技術】
ＤＶＤ－ＲＯＭはＣＤ－ＲＯＭの約７倍の容量を持つ媒体である。これにはＰＣ用のプログラムコードだけでなく、映像や音声データを圧縮することで映画ソフトを記録することもできる。ＤＶＤにデータを記録する記録媒体としてはＤＶＤ－ＲＡＭや、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷがある。これらにも大容量のデータを記録することが出来るため、映画などのソフトウェアがそのままディジタルコピーされることを防止しなければならない。このため、不正コピー防止技術が重要になる。この技術は、日経ＢＰ社「日経エレクトロニクス」(1997.8.18 P110～P119)に記載されている。
【０００３】
ＤＶＤ－Ｖｉｄｅｏディスクに記録されている映画などは通常ＣＳＳ（content scrambling system）方式で暗号化されており、ディスクのデータをコピーしてもこれをデスクランブルしない限り再生できない。
【０００４】
【発明が解決しようとする課題】
しかし、これにはＤＶＤ－Ｖｉｄｅｏディスクのように、もとからデータが記録されているメディアの再生については記載されているが、ユーザーが記録可能な記録媒体の再生については記載されていない。
【０００５】
記録可能な記録媒体で異なるスクランブルがかかったデータを再生する場合には、その再生信号がどの記録媒体からの信号かを判別してスクランブルを解除する必要があり、また

、データの種類がコピー可能なデータかコピー禁止のデータかを判別して、それぞれの制御を行なう必要がある。

【０００６】

【課題を解決するための手段】

上記目的を達成するため、本発明は、データの種類に対応した認証をするために複数の認証手段を有し、データの種類に対応して認証手段を切替えることにより装置間の認証をおこなうことを特徴とするデータ再生方法、データ再生装置、データ符号化方法、データ記録方法、データ記録装置、データ記録再生装置、認証方法及び半導体チップを提供するものである。

【０００７】

【発明の実施の形態】

以下、本発明の実施例を図面を用いて説明する。

【０００８】

図１は本発明によるコピー制御情報を含むデータを再生する再生装置の一実施例を示したものである。本実施例は例えばＤＶＤのような記録再生可能な媒体について示すが、勿論これは光ディスクに限定するものではなく、データを蓄える媒体全般にあてはまる。

【０００９】

同図において、１はデータ再生装置１、２は再生手段１、３は切り替えＳＷ１、４は認証手段１ａ、５は認証手段２ａ、６は認証手段３ａ、７はデータ再生装置２、８は認証手段１ｂ、９は認証手段２ｂ、１０は認証手段３ｂ、１１は暗号解読手段１、１２は暗号解読手段２、１３は切り替えＳＷ２、１４はWM検出手段、１５はMPEG再生手段、１６はデータ入力、１７はデータ出力、１８はデータバス１、１９は認証バス１、２０はデータバス２、２１は認証バス２、２２はデータバス３、２３は認証バス３、２４はＣＳＳ認証手段ａ、２５はＣＳＳデータバス、２６はＣＳＳ認証バス、２７はＣＳＳ認証手段ｂ、２８はＣＳＳ暗号解読手段、２９は認証ブロック１、３０は認証ブロック２、である。

【００１０】

本システムの動作を図１及び図２を用いて説明する。

【００１１】

ディスクから例えばＤＶＤドライブのようなデータ再生装置１によって読み出されたデータ入力１６は、再生手段１により記録されたフォーマットにしたがって復号される。この時、データの種類、例えばデータ中に含まれている記録媒体の種類を示すコード（例えば、再生専用か、記録可能かを示すコード）や、そのデータの構造がスクランブルがかかった構造かを示すコードや、ビデオデータかオーディオデータやコピー制限を示すコード（例えば、コピー許可か、一世代コピー可能か、コピー禁止かを示すコード）を読取る。また、光ディスクの場合にはディスクのトラッキング信号から記録媒体の種類を判別する場合もある。ここで、読取ったこれらの情報から切り替えＳＷ１(３)を切り替えて、どの認証手段を用いるかを選択する。認証はデータの受け渡しを行う相手を確認するために行い、暗号を解くための鍵情報のやり取りをする。この鍵により受け渡されるデータに暗号をかけられており、その鍵を用いて暗号を解読するようにして、データを保護する。

【００１２】

認証手段１ａが例えば再生専用の記録媒体の認証を行なう手段であり、認証手段２ａが記録可能な記録媒体で、コピー制限情報によりコピーが制限されているものの認証を行なう手段であり、認証手段３ａが記録可能な記録媒体で、コピー制限情報によりコピーが制限されていないものの認証を行なう手段であるとする。ＣＳＳ認証手段ａ(２４)は現行のＣＳＳ（content scrambling system）に対応したＤＶＤドライブ用の認証手段であり、ここで、本実施例では、ＣＳＳ認証手段ａ(２４)を独立に記載したが、これは認証ブロック１(２９)のように新たな認証手段１ａ、２ａ、３ａとともにまとめることも出来る。

【００１３】

データ再生装置２は例えばＭＰＥＧデータをデコードするＭＰＥＧボードであるとする。認証手段１ｂは認証手段１ａに対応した関係にあり、認証バス１(１９)を用いて認証の確

認を行ない、対応したものでなければそれぞれのスクランブルを解除するための方法が受け渡されないだけでなく、データバス１(１８)からのデータの出力を行なわないようにする。認証手段２ｂ、３ｂについても同様に認証手段２ａ、３ａに対応した関係にあり、対応したものでなければ認証が行われず、データの出力も止められる。ここでは、説明をわかりやすくするために３組の認証手段の認証を行なうための認証バスと、それぞれからデータを伝送するデータバスを独立としたが、１系列で切り替えながら用いることも可能である。ＣＳＳ認証手段ｂ(２７)は現行のＣＳＳに対応したＭＰＥＧボード用の認証手段であり、ここで、本実施例では、ＣＳＳ認証手段ｂ(２７)を独立に記載したが、これは認証ブロックｂ(３０)のように新たな認証手段１ｂ、２ｂ、３ｂとともにまとめることも出来る。

【００１４】

再生装置１から再生装置２へデータバス１で伝送されるデータは、伝送の途中でのコピーを防止するためにスクランブルがかけられた状態でデータを伝送する。スクランブルの種類は、再生専用の記録媒体のデータと、記録可能な記録媒体で、コピー制限情報によりコピーが制限されているもののデータと、異なる種類でスクランブルがかけられており、記録可能な記録媒体で、コピー制限情報によりコピーが制限されていないもののデータについてはコピー防止をする必要がないので、スクランブルはかけらていない。そのため、再生装置１からは、認証手段によって記録媒体の種類とデータのスクランブル状態が伝送されることになる。ここで、コピー制限無しのディスクについては、コピー防止のためのスクランブルをかける必要がないが、その場合だけ認証を行なわないようにすると、コピー制限無しと同じコピー制御状態で違法に複製されたディスクを検出することが困難になるため、コピー制限無しのディスクについても認証を行なうようにする。

【００１５】

認証が確認されるとそれぞれのスクランブルをかけられた状態でデータが伝送される。認証手段によって伝送された記録媒体の種類とデータのスクランブル構造に応じてデータが伝送されるデータバスが選択され、それに応じた暗号解読手段１(１１)または暗号解読手段２(１２)が動作して、デスクランブルされ切り替えＳＷ２(１３)によってＭＰＥＧ再生手段(１５)に送られる。ウォーターマーク検出手段(１４)は、ＭＰＥＧ再生手段(１５)でデコードされたデータに埋め込まれた付加情報を検出する検出手段の例であり、本実施例では付加情報としてウォーターマークを検出し、コピー制御情報が検出された場合にはそれにしたがって、データの出力を制御する。本実施例ではＭＰＥＧ再生手段(１５)を制御してデータの出力を制御する一例を示したが、制御方法は、出力データを止めたり、データをバス上で破壊するなど、これに限られるものではない。

【００１６】

ここで、再生手段１と切り替えＳＷ１(３)、認証手段１ａ(４)、認証手段２ａ(５)、認証手段３ａ(６)は同一のＬＳＩ内に組み込むことにより、データを途中から取り出すことを困難にし、認証手段１ｂ(８)、認証手段２ｂ(９)、認証手段３ｂ(１０)、暗号解読手段１(１１)、暗号解読手段２(１２)、切り替えＳＷ２(１３)、とWM検出手段(１４)、MPEG再生手段(１５)を同一のＬＳＩ内に組み込むことにより、データを途中から取り出すことを困難にする。

【００１７】

図２は本発明によるデータ再生装置をＤＶＤドライブ装置に当てはめた場合を示したものである。本実施例は例えばＤＶＤのような記録再生可能な記録媒体について示すが、勿論これは光ディスクに限定するものではなく、記録再生可能な媒体全般にあてはまる。

【００１８】

同図において、２４はＤＶＤディスク、２５はＤＶＤドライブ、２６はピックアップ、２７はプリアンプ、２８はシステム制御手段１、２９はＭＰＥＧ再生ボード、３０はシステム制御手段２、３１はコンバータ、３２はモニタ、である。

【００１９】

ＤＶＤディスク(２４)からピックアップ(２６)で読み出された信号はプリアンプ(２７)を

介してデータ再生装置１(１)に入力される。データ再生装置１(１)はシステム制御手段１(２８)により制御され、動作の状態を決定する。ここまでがＤＶＤドライブ(２５)の主な動作である。データ再生装置１(１)で再生された信号は、データ再生装置２(７)に伝送される。データ再生装置２(７)はシステム制御手段２(３０)により制御され、動作の状態を決定する。データ再生装置２(７)で再生されたデータはコンバータ(３１)で変換されて、モニタ(３２)に出力し映像が映し出される。ここまでがＭＰＥＧ再生ボード(２９)の主な動作である。

【００２０】

図３は本発明の記録媒体の種類とデータのスクランブル構造が記録されたコードを含むデータの一例として、ＤＶＤのセクタデータの構成を示したものである。ＤＶＤではメインデータ２０４８バイトの前にＩＤと呼ばれる識別データや、ＣＰＲ＿ＭＡＩと呼ばれる著作権管理情報が書かれている。

【００２１】

著作権管理情報（ＣＰＲ＿ＭＡＩ）には、著作権管理情報及び地域管理情報の両者に対応している。リードインエリアにおいては、著作権保護システムの特定データ構造（スクランブル構造に相当する）を持つか持たないか、指定された地域で再生してよいかいけないかを記述している。データ領域では、そのセクタが著作権を有する素材を含むか含まないか、著作権保護システムの特定データ構造を持つか持たないか、コピー制限があるか（コピー許可、一世代コピー可能、コピー禁止）を記述している。

【００２２】

図４はＤＶＤの識別（ＩＤ）データの構成を示したものである。ＩＤはセクタ情報を構成する最初の４バイトの中にデータタイプと呼ばれる再生専用データか、追記用データと書換用データのための予備を示すコードがある。

【００２３】

セクタフォーマットタイプには再生専用ディスク及び追記用ディスクに規定されたＣＬＶフォーマットタイプか、書換用ディスク用に規定されたゾーンフォーマットタイプかが記録されている。領域タイプには、データ領域、リードイン領域、リードアウト領域、再生専用ディスクのミドル領域かが記録されている。データタイプには、再生専用データか追記用データ（リンクデータ）と書換用データのための予備とされている。

【００２４】

図５は本発明によるコピー制御情報を含むデータを記録する記録装置の一実施例を示したものである。本実施例は例えばＤＶＤのような記録再生可能な記録媒体について示すが、勿論これは光ディスクに限定するものではなく、記録再生可能な媒体全般にあてはまる。

【００２５】

同図において、５１はデータ記録装置２、５２は記録手段１、５３は切り替えＳＷ４、５５は認証手段２ｄ、５６は認証手段３ｄ、５７はデータ記録装置１、５９は認証手段２ｃ、６０は認証手段３ｃ、６２は暗号化手段２、６３は切り替えＳＷ３、６４はWM検出手段、６５はMPEG符号化手段、６６はデータ出力、６７はデータ入力、７０はデータバス２、７１は認証バス２、７２はデータバス３、７３は認証バス３である。

【００２６】

ディスクからＤＶＤドライブのようなデータ再生装置１によって読み出され、モニタに出力された映像データ等を入力とするデータ入力(６７)は、記録手段１(５２)によりディジタルデータに変換され記録するためのフォーマットにしたがって符号化される。この時、データの種類、例えば、記録媒体の種類を示すコード（例えば、再生専用か、記録可能かを示すコード）をフォーマットにしたがって書き込む。また、他のデータの種類として、例えば、コピー制御により暗号化（スクランブル）をかけるデータ構造かを示すコードや、コピー制限を示すコード（例えば、コピー許可か、一世代コピー可能か、コピー禁止かを示すコード）を書き込む。次に、そのデータがコピー制御を行なう必要があるデータであるならば、その記録媒体と、コピー制御の状態に応じたスクランブルを施す。ここで、コピー制御情報から切り替えＳＷ３を切り替えて、どの認証手段を用いるかを選択する。

【００２７】
ウォーターマーク検出手段６４では、ＭＰＥＧ符号化手段６５に入力されたデータに付加された付加情報であるコピー制御情報を検出して、その情報に従って制御を行なう。例えば、検出された情報がコピー禁止の情報であれば、記録データを出力することを止め、コピー制限無しのデータであるならば、スクランブルを行なわずに符号化処理を行なうようにする。本実施例ではＭＰＥＧ符号化手段６５を制御してデータの出力を制御する一例を示したが、制御方法は、出力データを止めたり、データをバス上で破壊するなど、これに限られるものではない。
【００２８】
認証手段２ｃが、記録可能な記録媒体であってコピー制限情報によりコピーが制限されているものの認証を行なう手段であり、認証手段３ｃが、記録可能な記録媒体であってコピー制限情報によりコピーが制限されていないものの認証を行なう手段であるとする。
【００２９】
また、本実施例には省略したが、再生装置と同様に現行のＣＳＳに対応した認証手段が含まれる場合もあり、これとあわせて認証ブロックとすることも可能である。
【００３０】
データ記録装置１は例えばＭＰＥＧデータをエンコードするＭＰＥＧボードである。認証手段２ｄは認証手段２ｃに対応した関係にあり、７１認証バス２を用いて認証の確認を行ない、対応したものでなければそれぞれのスクランブルを解除するための方法が受け渡されないだけでなく、７０データバス２からのデータの出力を行なわないようにする。認証手段３ｄについても同様に認証手段３ｃに対応した関係にあり、対応したものでなければ認証が行われず、データの出力も止められる。ここでは、説明をわかりやすくするために２組の認証手段の認証を行なうための認証バスと、それぞれからデータを伝送するデータバスを独立としたが、１系列で切り替えながら用いることも可能である。
【００３１】
データ記録装置１からデータ記録装置２へデータバス２で伝送されるデータは、伝送の途中でのコピーを防止するためにスクランブルがかけられた状態でデータを伝送する。コピー制限情報によりコピーが制限されていないもののデータについてはコピー防止をする必要がないので、スクランブルはかけられていない。
【００３２】
そのため、データ記録装置１からは、認証手段によってデータのスクランブル状態が伝送されることになる。切り替えＳＷ３(６３)はそのデータに応じた暗号化手段２または暗号化手段を通らないパスのどれかを選択し、データに応じたスクランブルがかけられるようにする。
【００３３】
認証が確認されるとそれぞれのスクランブルをかけられた状態でデータが伝送される。認証手段によって伝送された記録媒体の種類とデータのスクランブル構造に応じてデータが伝送されるデータバスが選択され、切り替えＳＷ４(５３)によって記録手段１(５２)に送られる。
【００３４】
ここで、認証手段２ｃ(５９)、認証手段３ｃ(６０)、暗号化手段２(６２)、切り替えＳＷ３(６３)とＷＭ検出手段(６４)、MPEG符号化手段(６５)を同一のＬＳＩ内に組み込むことにより、データを途中から取り出すことを困難にし、記録手段１(５２)と切り替えＳＷ４(５３)、認証手段２ｄ(５５)、認証手段３ｄ(５６)は同一のＬＳＩ内に組み込むことにより、データを途中から取り出すことを困難にする。
【００３５】
図６は本発明によるコピー制御情報を含むデータを再生する再生装置の別の一実施例を示したものである。本実施例は図１で示した実施例で、データバスと認証バスを独立に示したものを、兼用化した場合についての実施例である。図１と同じ番号のものは同じ物を示す。

【００３６】
図６において、７０は１本化されたデータバス、７１は１本化された認証バス、７２は認証ブロック１の認証手段を切替えるSW、７３は認証ブロック２の認証手段を切替えるSWである。このような構成とすることで、データバス、認証バスを兼用化し、デバイス間の接続線の数を削減することが出来る。
【００３７】
図７は本発明によるデータ再生装置をＤＶＤドライブ装置に当てはめ、その出力信号を別のデバイス、例えばハードディスクのような記録可能なデバイスへ接続する場合を示したものである。本実施例は例えばハードディスクのような記録再生可能な記録媒体について示すが、勿論これはハードディスクのような記録再生可能な媒体全般に限定するものではなく、データバスを介してデータの受け渡しを行う装置全体にあてはまる。同図において、８０はハードディスク装置、８１はデータ記録装置１、８２はシステム制御手段３、８３はハードディスクである。
【００３８】
ＤＶＤディスク２４からピックアップ２６で読み出された信号はプリアンプ２７を介してデータ再生装置１に入力される。データ再生装置１はシステム制御手段１により制御され、動作の状態を決定する。ここまでがＤＶＤドライブ２５の主な動作である。データ再生装置１で再生された信号は、データ記録装置１に伝送される。データ記録装置１はシステム制御手段３により制御され、記録動作の状態を決定する。データ記録装置１で再生されたデータは、ハードディスク８３にデータが記録される。ここまでがハードディスク装置８０の主な動作である。
【００３９】
ここで、データを記録することが出来る機器に関しては、コピー制御情報に従って記録制御を行う必要がある。そのため、正しく記録を制御する機能を備えた機器であるかどうかを確認するために、データ再生装置１からデータ記録装置１に対して認証を行う必要がある。データ再生装置１からデータ記録装置２へ受け渡すデータは、データを保護する場合にはスクランブルをかけて送るようにする。そのため、データ再生装置１及びデータ記録装置２には、スクランブルをかける手段、スクランブルを解く手段、スクランブルのための鍵の受け渡しを行う手段を備えている。仮に、認証に失敗した場合には、データ再生装置１からデータ記録装置２へデータを出力しないようにし、もし、データを出力しても、スクランブルがかかっていて、鍵の受け渡しができていないため、データを正しく再生することが不可能となる。よって、スクランブルがかかったデータをそのまま記録装置で記録しても、正しく再生できなくなる。
【００４０】
また、ここでは、記録装置とのデータの受け渡しを行う場合についてのべたが、再生もしくは出力装置に場合にも同様に、正しくコピー制御を行う装置かどうかを認証して、データの保護を行うようにする。
【００４１】
このような手段を備えて、データの受け渡しを行うようにすることで、著作権などの権利のあるデータのコピー制御を正しく行い、不正なコピーや再生を防止することが可能となる。
【００４２】
図８は本発明によるデータ出力装置をモニタに当てはめた場合を示したものである。本実施例は例えばモニタのような出力について示すが、勿論これはモニタに限定するものではなく、データバスを介してデータの受け渡しを行う装置全体にあてはまる。同図において、９０はモニタ、９１はデータ処理装置３、９２はコンバータ、９３は表示装置である。
【００４３】
MPEGボード２９からモニタ９０に出力される。モニタ９０で入力されたデータはコンバータ３１で変換されて、モニタ３２に出力し映像が映し出される。ここまでがモニタの主な動作である。

【００４４】
ここで、データが データバス１００を介してモニタ９０に入力される場合、不正に記録されないように保護するために、データにスクランブルがかかっている場合があり、その場合には、データ処理装置３でスクランブルを解いてコンバータ９２へ出力するようにする。よって、この場合には、データ処理装置３の中に、ＭＰＥＧボード２９に対応した認証処断を備えることが必要となる。また、MPEGボード２９からの出力がモニタ９０のような表示装置のみに出力し、記録装置に出力しないことを確認するための認証を行うこともあり、記録装置の接続が無い場合には、データを不正にコピーされることがないため、モニタ９０に出力する時に、データにスクランブルをかける必要はない。
【００４５】
このような手段を備えて、データの受け渡しを行うようにすることで、著作権などの権利のあるデータのコピー制御を正しく行い、不正なコピーや再生を防止することが可能となる。
【００４６】
図９は、上述したデータ再生装置やデータ記録装置等のデータ処理手段（以下「デバイス」という）を複数備えたシステムとしての再生または記録再生装置、例えばパーソナルコンピュータの場合を示したものである。パーソナルコンピュータでは、各デバイスの組み込みを容易に変更できるので、本実施例に示した組み合わせに限定されるものではなく、データの受け渡しを行う全てのデバイスの組み合わせが含まれる。
【００４７】
同図の１０１はMPEGボード、１０２はMOドライブ、１０３はディジタルカメラである。
【００４８】
パーソナルコンピュータでは、データバス１００を介して、各デバイスとの間でデータの受け渡しが行われる。その時に、データバス上で不正にコピーされることを防止するため、データバスに接続しているデバイスとの間で認証を行う。
【００４９】
ここで、認証が成立しなかった場合には、そのデバイスが正しくコピー制御を行う機能を備えていない機器であると判断して、データを出力することを止める。また、この時、再生だけが認められているデータである場合には、データバスに記録デバイスが接続されておらず、再生機能を持つ機器だけの場合には出力することも可能である。
【００５０】
また、認証が成立なかった場合には、受け渡すデータがコピー制限が無いものに限ってデータバス上を介してデータを受け渡すことができるようにしてもよい。
【００５１】
これらの認証は、各デバイスに備えられている回路により行うことも可能であるが、パーソナルコンピュータ等のような場合には、各デバイスを制御するためのソフトウェアにより、認証を行うことも可能である。また、各デバイスを統括的にコントロールするOS上で認証を行い、その認証結果に応じて、各デバイスを制御するようにすることも可能である。
【００５２】
このようにデータバスに接続する各デバイス間で、データの種類に応じて認証を行い、その結果に従って、データの受け渡しを制御するようにすることで、正しくコピー制御を行うことを可能とした。
【００５３】
図１０は本発明によるコピー制御情報を含むデータを再生する再生装置の別の一実施例を示したものである。図１０は、図１に示したものが、例えば、民生用DVDプレーヤーのように、一つの機器の中で構成されているときの例を示したものである。このような機器の場合、DVDドライブとMPEGボードを組み替えることは困難なため、認証を行う必要はない。また、これらDVD信号処理とMPEGデコードが同一のLSI内部の処理として行われる場合にも、他に接続されたり、信号をデータバスの取り出したりされることはないため、認証は

必要なくなる。これらの場合には、認証手段を複数持つことはなく、暗号の解読手段を複数切り替えて再生するようにする。

【００５４】

【発明の効果】

本発明によれば、記録媒体の種類とコピー制御の情報によって、異なるスクランブルがかけられたデータの再生を行なう場合に、それぞれに対応した認証手段を切り替えて用いることにより、スクランブルに応じたデスクランブル処理を行なうことが可能となる。また、認証が出来なかったデータは出力しないため、不正にコピーしたデータを記録再生することを防止できる。

【００５５】

また、これらの機能を同一のＬＳＩ内に組み込むことにより、データを途中から取り出すことを困難にできる。

【図面の簡単な説明】

【図１】本発明によるコピー制御情報を含むデータを再生する再生装置の一実施例を示す図である。

【図２】本発明によるデータ再生装置をＤＶＤドライブ装置に当てはめた場合の一実施例を示す図である。

【図３】本発明の記録媒体の種類とデータのスクランブル構造が記録されたコードを含むデータの一例として、ＤＶＤのセクタデータの構成を示した図である。

【図４】ＤＶＤの識別（ＩＤ）データの構成を示した図である。

【図５】本発明によるコピー制御情報を含むデータを記録する記録装置の一実施例を示す図である。

【図６】本発明によるコピー制御情報を含むデータを再生する再生装置の別の一実施例を示したものである。

【図７】本発明によるデータ再生装置をＤＶＤドライブ装置に当てはめ、その出力信号をハードディスクのような記録可能なデバイスへ接続する場合を示したものである。

【図８】本発明によるデータ出力装置をモニタに当てはめた場合を示したものである。

【図９】本発明による各デバイスを備えたシステム、例えばパーソナルコンピュータの場合を示したものである。

【図１０】本発明によるコピー制御情報を含むデータを再生する再生装置の別の一実施例を示したものである。

【符号の説明】

１…データ再生装置１、２…再生手段１、３…切り替えＳＷ１、４…認証手段１ａ、５…認証手段２ａ、６…認証手段３ａ、７…データ再生装置２、８…認証手段１ｂ、９…認証手段２ｂ、１０…認証手段３ｂ、１１…暗号解読手段１、１２…暗号解読手段２、１３…切り替えＳＷ２、１４…WM検出手段、１５…MPEG再生手段、１６…データ入力、１７…データ出力、１８…データバス１、１９…認証バス１、２０…データバス２、２１…認証バス２、２２…データバス３、２３…認証バス３。

【図１】

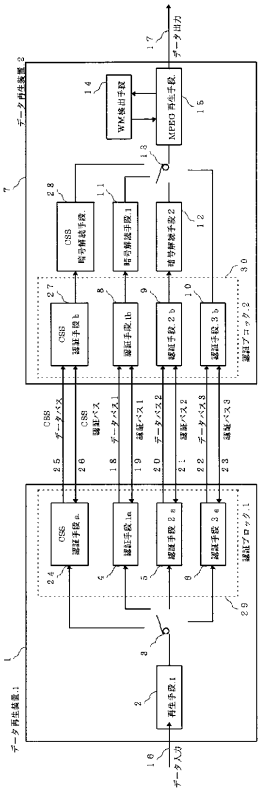


図１

【図２】

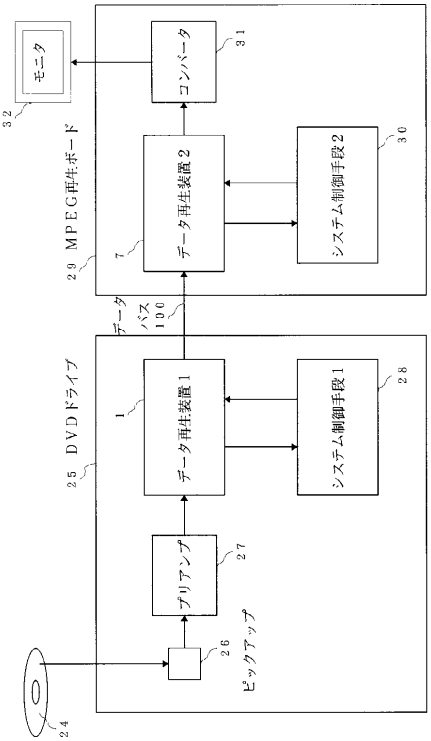
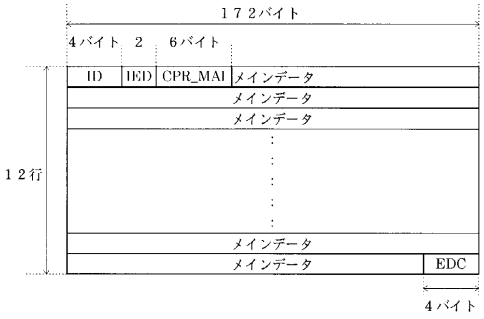


図２

【図３】

図３




【図４】

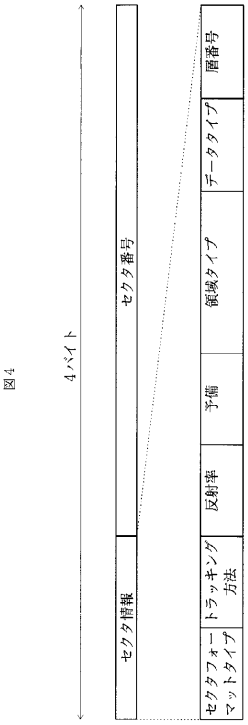
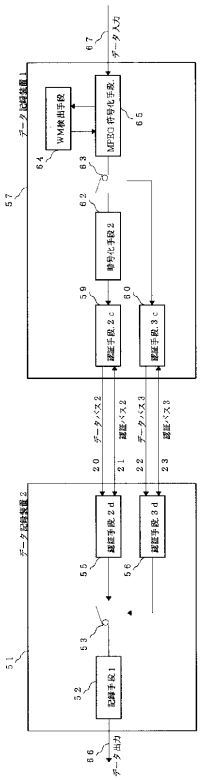
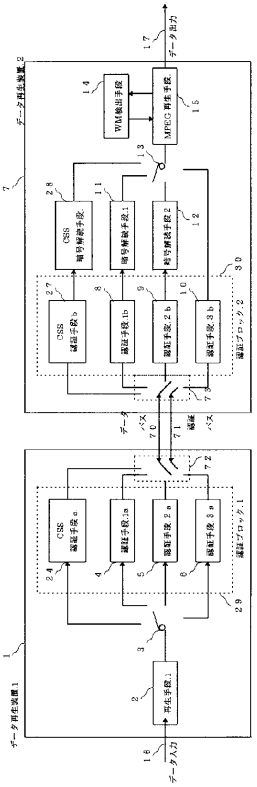



図４

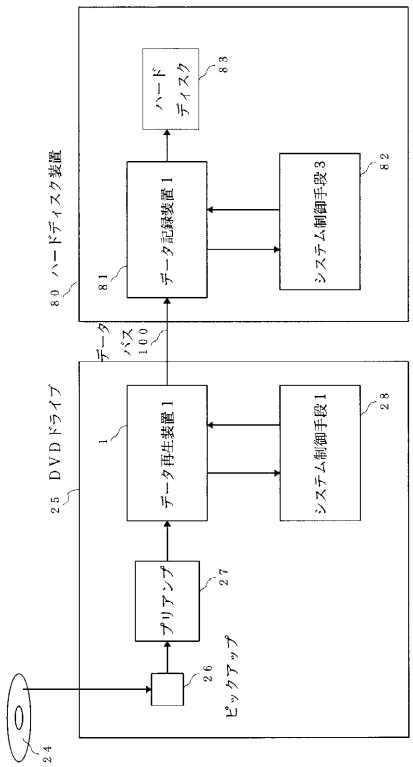
【図５】



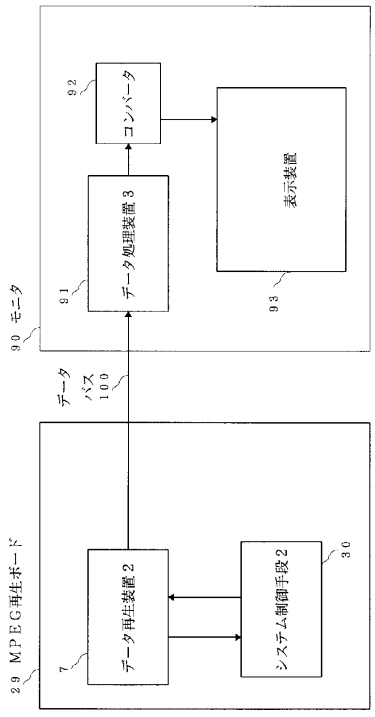
【図６】



【図７】

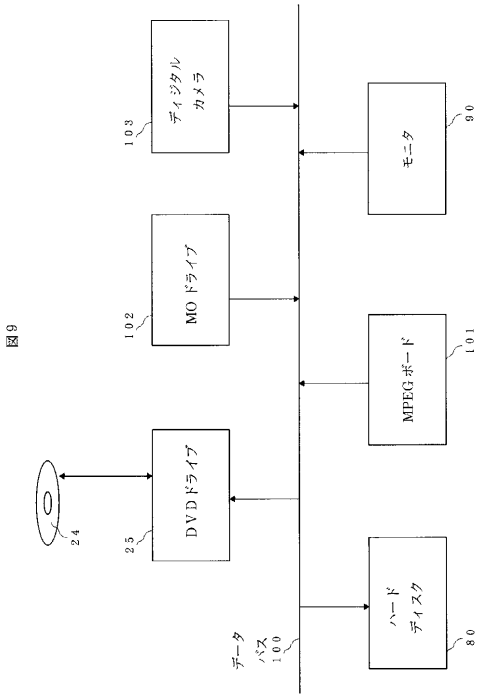

25 DVDドライブ
ピックアップ
26
プリアンプ
27
データ再生装置 1
1
システム制御手段 1
28
データ
バス
100
80 ハードディスク装置
データ記録装置 1
81
システム制御手段 3
82
ハード
ディスク
83
24

【図８】


29 MPEG再生ボード
データ再生装置 2
7
システム制御手段 2
30
データ
バス
100
90 モニタ
データ処理装置 3
91
コンバータ
92
表示装置
93

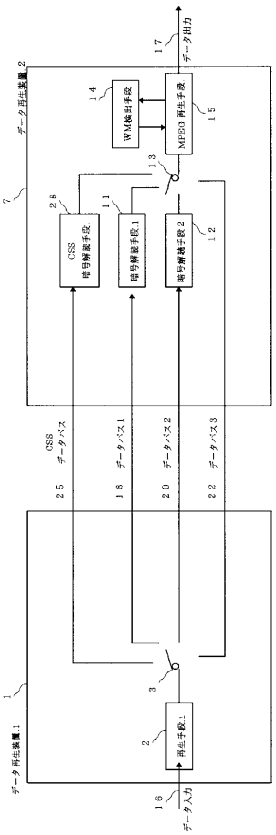
【図９】

図9


ディジタル
カメラ
103
MO ドライブ
102
DVDドライブ
25
24
モニタ
90
MPEG ボード
101
ハード
ディスク
80
データ
バス
100

【図１０】

図10


データ再生装置1
データ入力
16
再生手段1
2
3
1
CSS
データバス
25
データバス1
18
データバス2
20
データバス3
22
CSS
信号解読手段
26
信号解読手段1
11
暗号解読手段2
12
13
7
データ再生装置2
WM検出手段
14
MPEG 再生手段
15
データ出力
17

フロントページの続き

(72)発明者 荒井 孝雄
神奈川県横浜市戸塚区吉田町２９２番地株式会社日立製作所情報メディア事業本部内
(72)発明者 木村 寛之
神奈川県横浜市戸塚区吉田町２９２番地株式会社日立製作所情報メディア事業本部内
(72)発明者 吉浦 裕
神奈川県川崎市麻生区王禅寺１０９９番地株式会社日立製作所システム開発研究所内

合議体
審判長 江畠 博
審判官 樫本 剛
審判官 早川 卓哉

(56)参考文献 特開平１０－３７４４（ＪＰ，Ａ）
国際公開第９７／１４１４７（WO，Ａ１）
特開平１０－７９１７４（ＪＰ，Ａ）
特開平８－２９７６３８（ＪＰ，Ａ）
特開平９－１８４６９（ＪＰ，Ａ）
特開平６－２６１０３３（ＪＰ，Ａ）
特開２０００－５９３２３（ＪＰ，Ａ）
特開平１０－６５６６２（ＪＰ，Ａ）
特開平９－９７２１６（ＪＰ，Ａ）
特開平５－１３００９８（ＪＰ，Ａ）
特開平９－２１８８２７（ＪＰ，Ａ）
特開平１０－９８４６２（ＪＰ，Ａ）
特開平９－９７２１６（ＪＰ，Ａ）
特開平９－２７０７８５（ＪＰ，Ａ）
特開平８－４６９４８（ＪＰ，Ａ）
特開平１０－３０４３３３（ＪＰ，Ａ）
特開平１１－２８３３２６（ＪＰ，Ａ）
特開平７－２８８７６２（ＪＰ，Ａ）
特開２００１－２３６７２９（ＪＰ，Ａ）
松崎他、ＤＶＤ著作権保護システム、Ｎａｔｉｏｎａｌ Ｔｅｃｈｎｉｃａｌ Ｒｅｐｏｒｔ、１９９７年6月、第４３巻、第3号、ｐ．１１８－１２２
白橋、第２章 セキュリティのためのプロトコル技術、Ｉｎｔｅｒｆａｃｅ、１９９７年9月、ｐ．１０９－１１５

(58)調査した分野(Int.Cl.，ＤＢ名)
IPC G11B20/10
H04L 9/00
H04N 5/91
H04N 5/92
H04N 7/167