(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4299976号
(P4299976)

(45)発行日　平成21年7月22日(2009.7.22)　(24)登録日　平成21年4月24日(2009.4.24)

(51)Int.Cl.　F I

H04N	7/173	(2006.01)	H04N	7/173	620A
H04N	5/91	(2006.01)	H04N	5/91	P
H04N	7/167	(2006.01)	H04N	7/167	Z

請求項の数 4　(全 16 頁)

(21)出願番号　特願2001-57628(P2001-57628)
(22)出願日　平成13年3月2日(2001.3.2)
(65)公開番号　特開2002-262227(P2002-262227A)
(43)公開日　平成14年9月13日(2002.9.13)
審査請求日　平成16年7月30日(2004.7.30)
審判番号　不服2008-14619(P2008-14619/J1)
審判請求日　平成20年6月11日(2008.6.11)

早期審理対象出願

(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　岡本　宏夫
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デジタルメディア開発本部内
(72)発明者　尾鷲　仁朗
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デジタルメディア開発本部内

最終頁に続く

(54)【発明の名称】ディジタル情報記録装置

(57)【特許請求の範囲】
【請求項１】
入力した映像情報または音声情報を含むディジタル情報を記録媒体に記録するためのディジタル情報記録装置において、
前記ディジタル情報には、前記ディジタル情報を記録媒体に記録することを許すか否かを示すコピー制御情報と、前記ディジタル情報のコピーの制御は行わない場合に暗号化するかどうかを示す第２の制御情報とを含み、
前記ディジタル情報に所定の処理を行ない記録媒体に記録する記録回路と、
前記ディジタル情報から、前記コピー制御情報と前記第２の制御情報とを検出する制御検出回路と、
前記制御検出回路での検出結果に基づき前記記録回路の記録動作を制御する記録制御回路と、
ディジタル情報を暗号化する暗号化回路とを備え、
前記記録制御回路は、前記制御検出回路で検出したコピー制御情報に従い前記記録回路の記録動作を制御し、
前記コピー制御情報と前記第２の制御情報の組合せにより、前記コピー制御情報が記録を許すことを示すもの（Copy Free）であり、かつ検出した第２の制御情報が暗号化することを示す場合は、前記暗号化回路により前記ディジタル情報を暗号化して記録し、前記コピー制御情報が記録を許すことを示すもの（Copy Free）であり、かつ検出した第２の制御情報が暗号化することを示していない場合は、前記ディジタル情報を暗号化することな

く記録することを特徴とするディジタル情報記録装置。
【請求項２】
請求項１に記載のディジタル情報記録装置において、
前記記録回路は、前記検出した第２の制御情報を含めて、前記記録媒体に記録することを特徴とするディジタル情報記録装置。
【請求項３】
請求項１に記載のディジタル情報記録装置において、
前記記録回路は、記録するディジタル情報に対し暗号化を行ったか否かを示す情報を含めて、前記記録媒体に記録することを特徴とするディジタル情報記録装置。
【請求項４】
受信または入力された映像情報または音声情報を含むディジタル情報を処理するディジタル情報処理装置において、
前記ディジタル情報には、前記ディジタル情報を記録媒体に記録することを許すか否かを示すコピー制御情報と、前記ディジタル情報のコピーの制御は行わない場合に暗号化するかどうかを示す第２の制御情報とを含み、
前記ディジタル情報から、前記コピー制御情報と前記第２の制御情報とを検出する制御検出回路と、
前記ディジタル情報を暗号化する暗号化回路とを備え、
前記コピー制御情報と前記第２の制御情報の組合せにより、前記コピー制御情報が記録を許すことを示すもの（Copy Free）であり、かつ検出した第２の制御情報が暗号化することを示す場合は、前記暗号化回路により前記ディジタル情報を暗号化することを特徴とするディジタル情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は映像、音声などのディジタル情報を記録する記録装置に関わり、特に著作権者などの権限により、その記録する情報を、第三者への再度の配布や送信を制限するものとする記録装置に関する。さらに本発明は、このような記録装置に対しディジタル情報を好適に送信する送信装置に関する。また、情報を受信し好適に送信する送受信装置に関する。
【０００２】
【従来の技術】
テレビジョン放送およびこれを記録し再生する装置、さらには映画ソフトなどのパッケージメディアの分野では、ディジタル放送が開始され、これに対応した民生用のディジタル記録再生装置が発売された。この装置で用いるパッケージソフトも近い将来現れるであろう。
ディジタル放送、ディジタル記録装置は、情報の伝送過程や記録再生過程での品質劣化がない、もしくはごく少ないことが長所である。
【０００３】
また、近年インタネットの普及に伴い、ディジタル化された情報を、多数のユーザに配布し、転送することが容易になった。
しかし、情報の良質なコピーが、著作権者の預かり知らぬところで多数作成されて出回り、インタネットを経由して配布され、また転送を繰返した場合、その著作権者に利益が還元されない問題がある。
【０００４】
米国特許Ｎｏ．５，８９６，４５４では、情報に２ビットのコピー制御情報を付す方法が開示されている。これは著作権者、情報作成者の意志により、コピー禁止、コピー認可、一世代のみコピー認可の三つのうち、いずれかを選択することで、記録装置の動作を制御するものである。記録装置は、コピー禁止ならば記録動作をせず、コピー認可なら記録動作を行う。一世代のみコピーが認可されるなら、記録装置はこの制御情報を、これ以上のコピーを認めない情報に書替えたうえで、記録動作を行う。

【０００５】
従来はさらに、コピー認可の場合、記録装置は情報を暗号化せずに記録し、一世代のみコピー認可の場合、暗号化して記録する。これにより、タイムシフトや再視聴のために、一回のみコピーを認めた情報が、目的外に利用されることを防止していた。
【０００６】
【発明が解決しようとする課題】
上記従来技術で開示される事項は、著作権の有効な保護方法を与えるものである。しかし、著作権者にとって、最も不利益を蒙るのは、媒体へ記録した情報を、インタネットなどにより、無断で再度送信、配布されることである。多数のユーザに向けて送信でき、またさらに第三者へ簡単に転送できるため、入手できる利益が本来のものより、桁違いに少なくなり、また情報が加工されて、本来の意図とは関係のない事項に利用される問題がある。このため、著作権者などが、コピーを制限した情報はもちろんのこと、自由なコピーを認めた場合でも、インタネットなどでの再送信は認めないようにできることが要求されるであろう。上記従来技術では、この事項については記述されていない。
【０００７】
本発明の目的は、上記した問題に鑑み、これに対する有効な解決手段を提供することにある。すなわち、媒体へ記録した情報が、その著作権者の預かり知らないうちに、たとえばインタネットなどの通信手段を利用して、多数のユーザへ再度送信して配布され、また転送されることを防止すること、また、その行為が行われたとしても、受信した情報がユーザによって利用でき難いようにすることを、目的としている。
【０００８】
【課題を解決するための手段】
上記目的を達成するために、本発明のディジタル情報記録装置においては、入力するディジタル情報には、ディジタル情報を記録媒体に記録することを許すか否かを示すコピー制御情報と、ディジタル情報を有線ないし無線の通信回線を使用して他の装置へ再度送信することを許すか否かを示す再送制御情報とを含み、上記ディジタル情報に所定の処理を行ない記録媒体に記録する記録回路と、上記ディジタル情報から、コピー制御情報と再送制御情報とを検出する制御検出回路と、制御検出回路での検出結果に基づき上記記録回路の記録動作を制御する記録制御回路と、記録するディジタル情報を暗号化する暗号化回路とを備える。
【０００９】
上記記録制御回路は、上記制御検出回路で検出したコピー制御情報に従い上記記録回路の記録動作を制御し、コピー制御情報が記録を許すことを示すもの（Copy Free）であり、かつ再送制御情報が再度送信を許すことを示す場合は、上記暗号化回路を動作させず、コピー制御情報が記録を許すことを示すもの（Copy Free）であり、かつ再送制御情報が再度送信を許さないことを示す場合は、上記暗号化回路により記録するディジタル情報を暗号化させる。また、コピー制御情報が一世代のみ記録することを許すことを示すもの（Copy One Generation）である場合は、再送制御情報に依らず、上記暗号化回路により記録するディジタル情報を暗号化させる。
【００１０】
ここで前記暗号化回路は、乱数的に発生されるコンテンツキーに基づいて、ディジタル情報を暗号化する第一の暗号化回路と、記録装置ごとに付されるデバイスキーに基づいて、上記コンテンツキーを暗号化する第二の暗号化回路とを有し、第一の暗号化回路と第二の暗号化回路の出力を記録媒体上に記録する。
【００１１】
本発明のディジタル情報送信装置においては、ディジタル情報を記録媒体に記録することを許すか否かを示すコピー制御情報と、受信装置が受信したディジタル情報を有線ないし無線の通信回線を使用して他の装置へ再度送信することを許すか否かを示す再送制御情報とをディジタル情報に含めて送信する送信回路を有する。
【００１２】

本発明のディジタル情報送受信装置においては、受信または入力したディジタル情報を、有線ないし無線の通信回線を使用して外部装置へ再度送信するものであって、上記ディジタル情報には、ディジタル情報を記録媒体に記録することを許すか否かを示すコピー制御情報と、ディジタル情報を有線ないし無線の通信回線を使用して他の装置へ再度送信することを許すか否かを示す再送制御情報とを含み、上記ディジタル情報に所定の処理を行ない外部装置へ再度送信する送信回路と、上記ディジタル情報から、コピー制御情報と再送制御情報とを検出する制御検出回路と、再度送信するディジタル情報を暗号化する暗号化回路とを備える。検出した再送制御情報が再度送信を許すことを示す場合は、上記暗号化回路により再度送信するディジタル情報を暗号化し上記送信回路にて再度送信し、検出した再送制御情報が再度送信を許さないことを示す場合は、上記送信回路による再度送信を行わない。

【００１３】

【発明の実施の形態】

以下、本発明の実施形態を必要に応じて、図面を用いながら説明する。

本発明の実施形態では、必要に応じて新たな制御ビットを設けているが、その説明の前に本発明を適用するシステム全体から述べる。

【００１４】

図１は本発明で用いるシステム全体の実施形態を示すブロック図であって、放送で情報を送受信し、また記録再生する場合を例にとって示したものである。これには、通信手段による情報の配布、転送、もしくはその利用を阻止するための、本発明の方法を適用した装置が含まれている。１は放送局などの情報提供局、２は中継局、３は受信装置、４は記録再生装置、５はディスプレイである。なお、ここで放送などを記録する際は、記録再生装置４に記録する。また、受信装置３の内部に、たとえばハードディスクを記録媒体とする装置などを内蔵することがある。将来は、記録媒体としてビデオディスク、ビデオテープが内蔵されることも予想できる。これは、記録再生装置４が受信装置３の内部に置かれた場合として以下の説明をする。勿論、受信装置３の外部に、別途記録再生装置が接続されていても良い。

【００１５】

放送局など情報提供局１は、たとえば放送用衛星などの中継局２を介して、情報によって変調された信号電波を伝送する。勿論、それ以外のたとえばケーブルによる伝送、電話線による伝送、地上波放送による伝送などを用いても良い。受信側の受信装置３で受信されたこの信号電波は、後に述べるように、復調されて情報信号となった後、記録再生装置４へ記録するに適した信号となって記録される。また、ディスプレイ５へ送られる。ここでユーザは、情報内容を直接視聴することができる。また、上記した記録再生装置４で再生された情報は、受信装置３を介してディスプレイ６へ与えられ、元の映像音声などの情報が視聴される。情報が予め記録された取外し可能な記録媒体が提供される時は、これを取付けた記録再生装置４での再生動作以降が行われる。なお、装置間の情報の授受はディジタル信号で行われることが多いが、たとえば受信装置３とディスプレイ５の間は、アナログ信号で接続することもある。

【００１６】

図２は、上記システムのうち、放送局などの情報提供局１の構成の一例を示すブロック図である。１１はソース発生部、１２はＭＰＥＧ方式等で圧縮を行うエンコード回路、１３はスクランブル回路、１４は変調回路、１５は送信アンテナ、１６は管理情報付与回路、１７は入力端子である。

【００１７】

カメラ、記録再生装置などから成るソース発生部１１で発生した映像音声などの情報は、より少ない占有帯域で伝送できるよう、エンコード回路１２でデータ量の圧縮が施される。必要に応じてスクランブル回路１３で、特定の視聴者のみが視聴可能となるように伝送暗号化される。変調回路１４で伝送するに適した信号となるよう変調された後、送信アンテナ１５から、たとえば放送用衛星などの中継局２に向けて電波として発射される。この

際管理情報付与回路１６では、前記したコピー制御情報を始め現在時刻等の情報を付加する。また入力端子１７からは、先の図１では省略したが、たとえばリクエスト情報が電話回線などを介して入力される。これはビデオオンデマンドなど、視聴者のリクエストに応えて送出する情報を決定するシステムで活用される。

【００１８】

なお、実際には一つの電波には複数の情報が、時分割、スペクトル拡散などの方法で多重されることが多い。簡単のため図２には記していないが、この場合、ソース発生部１１とエンコード回路１２の系統が複数個あり、エンコード回路１２とスクランブル回路１３との間に、複数の情報を多重するマルチプレクス回路が置かれる。

【００１９】

図３は、図１のシステムにおける受信装置３の構成の一例を示すブロック図である。３０１はＲＦ／ＩＦ変換回路、３０２は復調回路、３０３は誤り訂正回路、３０４は信号に施された伝送暗号を解除するデスクランブル回路、３０５は第一のデマルチプレクス回路、３０６は入出力端子、３０７は第二のデマルチプレクス回路、３０８はデコード回路、３０９，３１０は出力端子、３１１は受信装置３全体の制御回路、３１２は情報管理回路、３１３は課金情報管理回路、３１４はモデム（ＭＯＤＥＭ）回路、３１５は出力端子、３１６は入力端子、３１７はコマンド入力回路である。３１３，３１４，３１５の構成要素は、後述するような課金情報の送出を行わない場合は取り除いても良い。図中、実線は映像音声など主となる情報の流れを、点線は各構成要素間の制御信号情報の流れを示す。

【００２０】

ここでまず、３０１から３１０の構成要素に関し、実線で示した映像音声などの情報の流れを説明する。

ＲＦ／ＩＦ変換回路３０１には、たとえば放送用衛星などの中継局からの電波が入力される。ここでＲＦ帯域の電波はＩＦ帯域（Intermediate Frequency）に周波数変換され、また受信チャネルに依存しない一定の帯域の信号となり、復調回路３０２で伝送のために施された変調操作が復調される。さらに誤り訂正回路３０３で、伝送途中で発生した符合の誤りが検出さらには訂正された後、デスクランブル回路３０４で伝送暗号の解除を行う。その後、第一および第二のデマルチプレクス回路３０５および３０７へ送られる。上記したとおり、特にディジタル放送の場合、一つのチャネルには複数の情報が、時分割、スペクトラム拡散などの方法で多重されることが多い。デマルチプレクス回路は、これから所望の情報だけを分離するものである。第一、第二とこれを二つ設ける理由は、いわゆる裏番組記録を可能にするのみならず、第一のデマルチプレクス回路３０５で、記録に値しない情報を除去するためである。すなわち、情報の中には天気予報、番組の放送予定などの付加情報が付されていることが多く、これは放送時点で見るなら良いが、記録して後日見るには値しないため、ここで除去することも可能にしている。

【００２１】

第一のデマルチプレクス回路３０５の出力は入出力端子３０６へ与えられ、ここに接続される記録再生装置４と信号の授受を行う。入出力端子３０６は双方向の端子であって、記録再生装置４との間で、記録再生する情報などをたとえばディジタルデータで授受する。もちろん必ずしも一本の情報ラインが双方向となっていなくとも良く、複数の単方向ないし双方向の情報ラインで構成されていても良い。一般にはＩＥＥＥ１３９４規格による接続が多く用いられる。さきの第二のデマルチプレクス回路３０７には、デスクランブル回路３０４から送られた情報、あるいは、入出力端子３０６からの記録再生装置４で再生された情報が接続されており、そのいずれか視聴したい情報が選択されて、所望の情報を分離する。次のデコード回路３０８では、伝送前に施された動画像のデータ圧縮がデコードされ、出力端子３０９を介して外部のディスプレイ５へ送られる。出力端子は３０９，３１０の二つを備え、一方をディジタル出力、他方をアナログ出力としても良い。

【００２２】

次に点線で示した制御信号に関して述べる。制御回路３１１は、上記した３０１より３０５、３０７、３０８の各構成要素との間で制御信号の授受を行い、受信装置３の全体が所

望の動作を行うように制御する。
情報管理回路３１２は、制御回路３１１が制御を行う時の管理データを要求に応じて供給する。たとえば、ここには受信契約の情報が管理されている。ユーザが視聴したいチャネルを指定した時、この指定は入力端子３１６から入力され、コマンド入力回路３１７を介して制御回路３１１に送られる。制御回路３１１は情報管理回路３１２に、受信契約情報を要求する。ユーザが指定したチャネルと契約があると判断した場合、上記した各構成要素に制御信号を送り、該当チャネルの受信動作を指示する。また、情報管理回路３１２には、ユーザによるタイマ予約情報が管理されている。視聴を予約した時間になると、制御回路３１１は上記した各構成要素に制御信号を送り、受信動作を開始させる。
【００２３】
また、制御回路３１１は、課金情報管理回路３１３との間でも制御信号の授受を行う。課金情報管理回路３１３には、有料放送の課金情報が蓄えられており、ユーザへの課金が発生した場合には、この情報がモデム回路３１４へ与えられる。ここでさらに、電話回線など通信伝送路へ送出するに適した情報となって、出力端子３１５へ出力される。その後、通信伝送路を経て著作権者、金融機関あるいは図１の情報提供局１などへ送られ、規定の金額をユーザから得られるようにする。勿論、通信伝送路は無線であっても良い。
【００２４】
次に図４は、本実施形態において、図１の記録再生装置４で記録媒体へ記録する制御情報信号の一構成例を示すブロック図である。これは、図２の情報提供局１の管理情報付与回路１６で発生されて伝送された制御情報に、記録再生装置などで情報を追加、あるいは書替えして形成されるものである。たとえばテープ媒体の場合、一つの記録トラックに一個記録されれば充分であるが、当然ながら映像音声などの情報データとは決まった関係で記録され、再生時容易に分離できるようになされる。
【００２５】
プログラム番号１００は、その媒体で何番目のプログラムであるかを示す。
セクタ情報１０１は、プログラムを所定の単位で分割したセクタの番号である。分割は、固定の単位、たとえば２ｋバイト単位に分割してもよいし、情報の一定単位、たとえば、エンコードする時の分割の単位でもよい。また、番号はプログラム内で付けてもよいし、記録媒体全体での通し番号でもよい。後述する記録時刻１０７等の情報は、このセクタ単位で付加される。
時間情報１０２は、その記録部分がそのプログラム開始後、どれだけ経ているかを示す。
種類１０３は、そのプログラムが販売されたものか、レンタルか、自作か、放送からかなどの属性情報を示す。
【００２６】
コピー制御１０４は、本発明において重要なものであって、その情報を媒体に記録して良いか否かを示す。一般的には、Copy Never（コピー禁止），Copy One Generation（一世代のみコピーを認める），Copy No More（Copy One Generationで一回コピーされたもので、これ以上はコピーできない），Copy Free（コピーして良い）といった指定がある。
【００２７】
Copy Never、Copy One Generation、Copy Freeの指定は、情報の作成者など著作権者が、三つのうちいずれかを選択して決めるものであり、放送では、さきの管理情報付与回路１６で与えられることが多い。情報ソフトが記録媒体で与えられる場合は、その権利者が作成時に記録する。
Copy No Moreは、元は Copy One Generation であったものをコピーした際に、このように装置で書替えたものである。
計４つの状態があるので、２ビットの情報で伝送できる。Copy Never は（１，１）、Copy One Generation は（１，０）、Copy No More は（０，１）、Copy free は（０，０）などとする。
【００２８】
Copy Never は記録できず、Copy One Generation は Copy No More と書替えて記録する

ので、記録媒体上では、基本的には Copy No More と Copy Free の二つの状態があり得る。なお、一時記録と称して、コピー禁止の情報を条件付で記録することも本出願人により提案されているが、ここでは説明を省略する。

【００２９】

ＡＰＳ１０５は、アナログ記録機器へのコピー制御情報（ＡＰＳ； Analogue Protection System）であり、アナログ映像信号への擬似シンクパルスの追加等によりコピーの可否を制御する。

【００３０】

再送制御１０６は、本発明おいて重要なものである。これは、前記したようなインタネットなどで、情報を再度送信、転送することを認めるか否かを示す。あるいは、この目的を達するため、情報を媒体に記録する場合、情報の暗号化を要するか否かを示す場合もある。これも放送では、さきの管理情報付与回路１６で与えられることが多い。情報ソフトが記録媒体で与えられる場合は、その権利者が作成時に記録する。

【００３１】

上記コピー制御１０４と再送制御１０６の組み合わせにより、媒体への記録をどのように制御するかを説明する。コピー制御１０４が Copy Never の時は、いわゆる一時記録以外の記録が禁止されるので、この場合再送制御１０６は特に意味を持たない。Copy One Generation では、記録時には暗号化するものとし、再送制御１０６に従い情報の再送信を行う。Copy Free では、一般には厳しい管理は要求されないものと解釈され、従来は暗号化せずに記録された。本発明では、再送制御１０６に応じて暗号を施すようにする。後記するように、単に再送信を禁止するという表示に留まらず暗号を施しておけば、仮に再送信されたとしても、内容を視聴することが困難となり、積極的な阻止効果を期待できる。

【００３２】

記録時刻１０７は、たとえば、図２の管理情報付与回路１６で与えられた時刻を記録する。記録時刻１０７の記録は、たとえばセクタ単位で行われる。

放送方式１０８は、ＨＤ情報（ＨＤ；High Definition；高精細）、ＳＤ情報（ＳＤ；Standard Definition；標準精細）など、その情報が用いている放送方式を示す。

暗号化１０９は、記録した情報に暗号化を施したか否かを示す。

ユーザ識別１１０は、その媒体に記録した情報を、記録時と同じ装置あるいは同じユーザでしか再生できなくするなどのために、ユーザ固有のコードを用いる際に記録される。

【００３３】

暗号化情報１１１は、暗号化して記録された情報を再生し、暗号を復号する際に使われる。情報そのもののデータ量が多い時は、コード番号を記録しておき、再生装置で予め記憶された対応する情報を引き出して使うようにしてもよい。

【００３４】

以上は必要に応じ映像のフレーム毎、或いは決まった量のデータ毎など比較的細かい時間間隔で記録される。上記した構成要素のうち、特に１０３から１０８で示したものは、放送の場合、送信する側で予め付加することが多い。図４で示した制御情報信号の構成は一例であり、構成、媒体上での記録位置、頻度など様々なものが適用可能である。また本発明において、その内容は全てが必須ではなく、いくつかが省略されていても良い。順番がこれに限定されないことは勿論である。

【００３５】

図５を用いて、これら制御信号の媒体上での記録位置について説明する。図５は記録媒体上での制御情報信号と、映像音声などの情報データとの記録位置を、模式的に描いたものである。同図で(a)はテープ媒体に適したものである。この場合、制御信号のブロックはたとえば記録トラック毎にあることが望まれる。したがって、各トラック毎に映像音声などの情報にたとえば先行して、そのヘッダー部などに制御情報のブロックが配置される。(b)はディジタルビデオディスクなどに適したものである。この場合、ある情報量のセクタ毎にあることが望まれる。従って、各セクタ毎そのヘッダー部などに配置される。(c)はハードディスクなどに適したものである。この場合、映像音声などの情報と制御情報と

はディスク上で離れた位置に記録し、起動時は短時間の内に全体の制御情報を読み取れるようにすると良い。

【００３６】

次に図６、図７を用いて、記録再生装置４の記録再生動作を述べ、本発明による暗号化の動作を説明する。

まず記録再生装置４は、ディジタル伝送あるいは放送された圧縮ビットストリームをそのまま記録する、主には最近の、あるいは今後現れるディジタル記録方式によるものが相応しい。この場合、受信装置３との情報の授受は、前記したとおりＩＥＥＥ１３９４規格などによりディジタルで行うのが良い。また、その記録媒体はテープのみならず、ディジタルビデオディスクなどの取外し可能なディスク、ハードディスクなどの装置に内蔵されたディスクなど、様々なものが可能である。

【００３７】

図６は、記録再生装置４の回路ブロック図である。特に記録媒体として、ディスクを用いるものに適している。４１は記録回路、４１０１は記録する信号の入力端子、４１０２は半導体メモリなどの記憶手段、４１０３は暗号化回路、４１０４は暗号化キーの入力端子、４１０５は記録符号化回路、４１０６は記録媒体へ記録する信号の出力端子、４１０７は媒体検知回路、４１０８は制御検出回路、４１０９は記録制御回路、４１１０は制御信号の入出力端子、４１１１は制御信号の出力端子である。また、４２は再生回路、４２０１は再生信号の入力端子、４２０２は再生復号回路、４２０３はブロック再生回路、４２０４は半導体メモリなどの記憶手段、４２０５は誤り訂正回路、４２０６は暗号復号回路、４２０７は暗号を復号するキーの入力端子、４２０８は信号出力回路、４２０９は受信機などへ再生信号を送る出力端子、４２１０は制御信号の検出回路、４２１１は時計、４２１２は再生制御回路、４２１３は制御信号の入出力端子、４２１４は制御信号の出力端子である。

【００３８】

図７は、記録再生装置の記録媒体の周辺を示すブロック図である。４３は記録再生部、４３０１は入力端子、４３０２は記録増幅器、４３０３はハードディスク、ディジタルビデオディスク、ビデオテープなどの記録媒体を搭載した記録媒体ドライブ、４３０４は再生増幅器、４３０５は出力端子、４３０６は機構制御回路、４３０７は入力端子である。

【００３９】

まず、図６を用いて動作の説明を行う。記録回路４１から述べる。

入力端子４１０１からは、記録する情報が入力される。これは、さきの図３の入出力端子３０６から供給されるものである。デスクランブル回路３０４で伝送暗号を復号した後の情報であるが、もちろん、これを復号せずに供給される場合も本発明の範疇にある。なお、後に述べる再生回路４２の再生した情報の出力端子４２０９の出力も、図３の入出力端子３０６へ与えられる。従って、４１０１と４２０９とを一つにし、入出力端子としても良い。もちろん、これは必ずしも中の信号線が一本ということではなく、複数の単方向ないし双方向の信号線であって良い。ＩＥＥＥ１３９４規格で規定するものでも良い。

【００４０】

入力された情報は、一旦、記憶手段４１０２にブロック毎に蓄積される。これには、映像音声などのディジタル情報のほか、たとえば図４で示したような様々の制御情報が付されている。放送の場合、たとえば図２の管理情報付与回路１６で付与されたものである。これは制御検出回路４１０８に与えられ、前記したコピー制御１０４、再送制御１０６をはじめ、たとえば図４で示したような制御情報などが検出される。これを基に記録制御回路４１０９では、この信号を記録して良いか否か、記録する際に暗号化するか否かなどを判断し、その結果を暗号化回路４１０３と、記録符号化回路４１０５へ送る。

【００４１】

一方、記憶手段４１０２の映像音声などの情報は、暗号化回路４１０３において、記録制御回路４１０９からの制御信号に従い、必要に応じて暗号化が行われる。暗号化は、たとえば入力端子４１０４からの情報に基づいて行われる。これは、装置の識別番号などのデ

バイスキー、ユーザの所持するＩＣカードを装置に装着して読み取られた個人ＩＤなどのユーザキー、あるいは記録する情報（コンテンツ）ごとに乱数的に発生させたコンテンツキーなどが用いられる。

【００４２】

図９は、暗号化回路４１０３の一つの構成例を示す回路ブロック図である。４１０３１は入力端子、４１０３２は第一の暗号化回路、４１０３３は第二の暗号化回路、４１０３４は多重回路、４１０３５は入力端子、４１０３６は出力端子である。入力端子４１０４は図６で示したものと同じである。ここから入力された上記のコンテンツキーは、第一の暗号化回路４１０３２と、第二の暗号化回路４１０３３に与えられる。入力端子４１０３１への情報は、図６の記憶手段４１０２から与えられ、第一の暗号化回路４１０３２で上記コンテンツキーに基づいて暗号化される。一方、入力端子４１０３５から上記デバイスキーが与えられ、第二の暗号化回路４１０３３へ送られる。コンテンツキーは、第二の暗号化回路４１０３３で上記デバイスキーに基づいて暗号化される。これを多重回路４１０３４で先の情報に多重し、即ち図４の暗号化情報１１１に格納する。このため、記録する情報は、キー情報を伴って出力端子４１０３６より図６の記録符号化回路４１０５へ供給される。このようにすれば、決まった装置だけでコンテンツキーを復号し、さらに情報を復号して視聴できるようになり、不特定多数者の利用を阻止できる。

【００４３】

また、たとえば記録した情報を再生し、視聴する期間に制限を設ける時など、期限切れとなった後に消去することを要求されることがあるが、本発明では、記録媒体上の暗号化されたコンテンツキーを消去するだけでも目的を達成でき、動作の簡単化を図ることができる。

暗号化は、プログラム（コンテンツ）単位で行ってもよいが、同じコンテンツの中で、時間とともにキーを変え、たとえばセクタ単位でキーを変えて行っても良い。

【００４４】

上記実施形態によれば、ディスクなどへ記録した情報がその装置で再生され、あるいは取り外し可能なディスクなどへ記録した情報がパーソナルコンピュータのディスクドライブで再生され、インタネットなどで再度送信されることがあった時、これが著作権者の意志に反する場合、他の装置ないしユーザは視聴が困難となる。

【００４５】

暗号化された情報は、記録符号化回路４１０５に与えられる。記録符号化回路４１０５では、記録制御回路４１０９からの制御情報に基づき、記録が禁止された場合はここで情報を遮断し、許された場合は使用する媒体に適した変調を施し、出力端子４１０６へ出力する。コピー制御情報が Copy Neverないし Copy No More であれば、情報はここで遮断される。Copy Free であれば、そのまま変調を施し、出力端子４１０６へ送られる。また、Copy One Generation であれば、このコピー制御情報を記録符号化回路４１０５で、Copy No More と書替えてから変調を施し、出力端子４１０６へ送られる。

【００４６】

記録制御回路４１０９から記録符号化回路４１０５へは、コピー制御情報のほかに、時計４２１１から出力される記録時の現在時刻も与えられており、記録が可能な場合には、必要に応じて、これも同時に記録する。記録した情報を再生し、視聴する期間に時間制限を設ける時などに活用される。なお、現在時刻は、受信した情報に含まれている場合はそれを用いてもよいし、また、受信した情報で時計４２１１を校正するようにしてもよい。

【００４７】

また、記録符号化回路４１０５は図４の暗号化情報１０９を、たとえば暗号化を行った場合は「１」、行わない場合は「０」とする。このようにすれば、再生を行う時暗号の復号を要するか否かを容易に判断できる。

【００４８】

さらに、出力端子４１０６の情報信号は、図７に示した記録再生部４３の入力端子４３０１へ与えられる。これはレーザ発生素子や磁気ヘッドを駆動できるよう、記録増幅器４３

０２で増幅された後、記録媒体ドライブ４３０３で上記したような記録媒体へ記録される。４３０６は、記録媒体ドライブ４３０３を駆動するモータなどの機構制御回路であって、入力端子４３０７からの制御信号で記録媒体を制御する。

【００４９】

なお、さきに示した図６の記録制御回路４１０９の出力は、出力端子４１１１に与えられている。必要に応じ、これを図７の入力端子４３０７へ与え、たとえば記録が禁止された情報が入力された時に、機構制御回路４３０６へ記録動作を停止するよう指示しても良い。また、図６の入出力端子４１１０では、外部の装置との制御信号の入出力を行う。たとえば、以上述べたような制御情報を、制御検出回路４１０８で検出せずに、映像音声などのデータとは別に外部から与える方法もあり、この際に活用される。ＩＥＥＥ１３９４規格に従って、入力端子４１０１、４２０９と共用することもできる。

【００５０】

次に、記録した情報を再生する時の動作を説明する。図７の記録媒体ドライブ４３０３から再生された情報信号は、再生増幅器４３０４で後段での信号処理が可能なレベルまで増幅された後、出力端子４３０５へ出力される。入力端子４３０７には、図６の出力端子４２１４からの制御信号が入力され、機構制御回路４３０６を制御する。これは再生制御回路４２１２で生成したものである。さきの記録制御回路４１０９と、この再生制御回路４２１２は、実際には同一の半導体デバイス上にあるのが普通であり、この場合、４１１１と４２１４の出力端子は共通にできる。

【００５１】

図７の出力端子４３０５の情報信号は、図６の再生回路４２の入力端子４２０１へ与えられる。これは再生復号回路４２０２に供給される。ここでは媒体に記録再生するために記録側で施した変調が復調され、波形を等化しクロックでデータを確定する。次にブロック再生回路４２０３で同期信号、ＩＤ信号などの検出を行い、これをもとに再生データは記憶手段４２０４の所定の位置に一旦格納される。誤り訂正回路４２０５は格納されたデータより演算操作で、記録再生過程で発生した符合の誤りを検出し、正しい値に訂正する。誤り訂正後のデータは、暗号復号回路４２０６へ与えられる。これは、記録時にさきの暗号化回路４１０３で行われた、記録暗号化を復号するためのものである。ここで、入力端子４２０７からの装置のデバイスキー、個人ＩＤなどユーザキー、あるいはコンテンツキーなどによって、復号が行われる。これが所定のものでなければ、正常な暗号の復号は行われず視聴することはできない。従って、記録した装置ないしユーザが視聴することは可能であるが、記録した媒体をパーソナルコンピュータのディスクドライブなどへ取付け、インタネットなどで再送信して、第三者に配布した後は、他の装置ないしユーザが再生することとなり、視聴することは極めて困難となる。これで、本発明の一つの目的が達成できる。なお、入力端子４２０７からの復号キーは、記録媒体上にある図４の暗号化情報１１１から得たもの、あるいは、ここから暗号を復号して得たものであっても良い。

【００５２】

一方、さきの誤り訂正を施されたデータより、制御信号の検出回路４２１０で、たとえばコピー制御情報、記録時の時刻などが検出される。次に再生制御回路４２１２では、検出されたこれらの情報のほか、時計４２１１からの現在時刻などをもとに、再生出力の可否を判断し、信号出力回路４２０８の出力を制御する。あるいは、暗号復号回路４２０６を動作ないし停止させる。たとえば、再生し視聴する期間に時間制限があり、これが過ぎている場合、また、コピー制御情報が Copy One Generation を示すなどして、違法な方法で記録されたと判断できる場合などは、信号出力回路４２０８から、少なくも正常に視聴できる情報は出力しないようにする。必要に応じて、出力端子４２１４から図７の入力端子４３０７へ制御情報を送り、記録媒体ドライブ４３０３自体の再生動作を停止しても良い。

【００５３】

再生した情報を出力することを認められた時は、この情報は出力端子４２０９へ与えられ、図１の受信装置３を介して、ディスプレイ５へ供給される。図２のエンコード回路１２

で施された、ＭＰＥＧなどによるデータ量の圧縮操作は、受信装置３のデコード回路３０８で、元に戻される。このため、ユーザは情報内容を視聴することができる。デコード回路３０８は、ディスプレイ５に内蔵されることもある。

【００５４】

なお、コピー制御情報などが、ここまで述べたものと異なり、電子透かしとして映像情報中に埋め込まれているときには、再生時に、この電子透かしから検出した情報を使って同様の制御を行っても良い。

【００５５】

時計４２１１は、当然ながらある程度の正確さが要求される。ユーザの悪意で容易に変えられるものでは目的を果たさない。放送局などからの時間情報で制御のかかるものであることが望ましい。故意に時刻を変えた場合、以後は装置が動作しないようにしても良い。

【００５６】

入出力端子４２１３は、外部の装置と制御情報の授受を行うものである。たとえば再生した情報を、さらに外部の記録装置へ記録する場合などに活用される。入出力端子４１１０と４２１３とは共通化できる。また、たとえばＩＥＥＥ１３９４規格に従い、入力端子４１０１、出力端子４２０９の情報も含め、一系統で授受し、あるいは赤外線などを用いて無線で授受することができる。

【００５７】

再生制御回路４２１２から記録符号化回路４１０５へ与えられる制御信号は、たとえば再生時の情報の消去を指示するものである。これは本発明には直接関係しないが、再生回数を一回に制限し、再生後に消去することを要求されることがある。この時、この制御信号に従い、記録符号化回路４１０５は情報として意味のない信号を発生し、媒体上に記録することで、情報を消去する。この場合、記録媒体は消去可能なものでなければならない。媒体検知回路４１０７は、このために設けられており、ＣＤ－Ｒなど記録した情報の消去が不可能な媒体に、上記した情報を記録し、ないしここから再生することを阻止するようにしている。

【００５８】

以上が、図６と図７の基本的な動作説明である。ここで本発明における、特に記録暗号化回路４１０３の動作に関して、さらに詳しく述べる。

制御検出回路４１０８で検出されたコピー制御情報が、（１，１）即ち Copy Never であるならば、記録制御回路４１０９は記録符号化回路４１０５へ制御信号を送り、記録媒体への情報の記録を阻止する。当然ながら、この場合、暗号化回路４１０３は暗号化動作をする必要はない。これ以外の場合は、いくつかの動作が考えられる。

【００５９】

まず、第一のケースを述べる。これは、再送制御１０６が、Copy Free の時に機能するよう定めたケースである。（０，０）即ち Copy Free であり、制御検出回路４１０８で検出された、図４の再送制御１０６がインタネットでの再送信を認めている場合、暗号化回路４１０３は暗号化動作を行わずに、情報を記録符号化回路４１０５へ受け渡す。一方、図４の再送制御１０６がインタネットでの再送信を認めない場合、暗号化回路４１０３は記録暗号化を行ってから、情報を記録符号化回路４１０５へ受け渡す。この場合、記録暗号化を行って媒体へ記録したものは、この媒体が取り外され、パーソナルコンピュータのドライブで再生されインタネットなどへ送信されることがあっても、受信した側で暗号を復号し、視聴することは極めて困難となる。

【００６０】

次に第二のケースを述べる。これは、再送制御１０６が、Copy One Generation の時に機能するよう定めたケースである。（１，０）即ち Copy One Generation であるならば、再送制御１０６の内容いかんにかかわらず、暗号化回路４１０３で暗号化を行い、記録符号化回路４１０５でコピー制御情報を（０，１）即ち Copy No More と書替えて記録を行う。再送制御１０６は、実際に再送信する段階でその制御に用いる。

【００６１】

第三のケースは、再送制御１０６が、Copy Free の時もCopy One Generation の時にも機能するよう定めた場合である。Copy Free（０，０）の情報は第一のケースと同様に、Copy One Generation（１，０）の情報は第二のケースと同様に扱うこととする。
いずれのケースでも、図４の暗号化１０９の情報は、暗号化を行って記録する場合は、たとえば「１」、行わずに記録する場合は「０」とする。

【００６２】

なお、ここまで記録媒体上において、２ビットのコピー制御情報と、１ビットの再生制御情報を別に記録するように記した。前記したように、記録媒体上ではコピー制御情報は Copy Free を示す（０，０）と、No More Copy を示す（０，１）しかない。そこで残る（１，０）と（１，１）を活用して、ビット数を減らしても良い。たとえば（０，０）は Copy Free で再送信を認め、（１，０）は Copy Free で再送信を認めず、（０，１）は No More Copy で再送信を認め、（１，１）は No More Copy で再送信を認めないなどとする。No More Copy では一切再送信を認めないならば、これを（０，１）とし、Copy Free に対してのみ、上記した二つの場合を設けると良い。いずれにしても、ビット数を減らすことができる。

【００６３】

次に図８を用いて、本発明を用いた受信装置３の他の実施形態を説明する。同図は図３の形態と比べ、暗号化回路３１８と復号化回路３１９が加わり、モデム回路３１４、出力端子３１５（ここでは入力端子でもある）を介して、たとえば入出力端子３０６から入力された記録再生装置４の再生情報を、電話回線などを通してインタネットなどへ送信できるよう構成されている。従ってこの場合、図８の受信装置３は送受信装置としての機能を有するものである。通信回線は無線であっても良い。ここで図４に示したような制御情報の検出と、これに基づく制御は制御回路３１１で行う。

【００６４】

入出力端子３０６から入力された記録再生装置４の再生情報には、前記したようなコピー制御１０４、再送制御１０６などの制御情報が付されている。記録時に施された暗号化は既に復号されている。再生情報であるから、コピー制御１０４はCopy Free（０，０）かCopy No More（０，１）である。

【００６５】

コピー制御１０４と再送制御１０６の関係が、上記した第一のケースである場合をまず述べる。Copy Free（０，０）であり、再送制御１０６がインタネットでの再送信を認めている場合、暗号化回路３１８はモデム回路３１４、出力端子３１５を介して情報を送出する。この際、暗号化動作を行わなくても良い。一方、再送制御１０６がインタネットでの再送信を認めない場合、暗号化回路３１８は動作を停止し、ここで情報信号を遮断する。

【００６６】

次に、コピー制御１０４と再送制御１０６の関係が、上記した第二のケースである場合を述べる。コピー制御１０４がCopy No More（０，１）であり、再送制御１０６がインタネットでの再送信を認めている場合、暗号化回路３１８はモデム回路３１４、出力端子３１５を介して情報を送出する。この際、暗号化動作を行うものとする。一方、再送制御１０６がインタネットでの再送信を認めていない場合、暗号化回路３１８は動作を停止し、ここで情報信号を遮断する。

【００６７】

上記した第三のケースでは、（０，０）の情報は第一のケースと同様に、（０，１）の情報は第二のケースと同様に扱うものとする。

【００６８】

図８の復号化回路３１９は、受信装置３がインタネットなどを介した情報を受信する際に用いられる。情報が暗号化されている場合は、制御回路３１１からの指令に従い、これを復号してデコード回路３０８へ送り、外部のディスプレイ５で視聴できる。この場合、当然ながら暗号を復号するためのキーが必要となる。

【００６９】

上記説明は、記録再生装置４の再生情報が入出力端子３０６から入力され、これを再送信する場合についてであるが、これに限らず、ＲＦ／ＩＦ変換回路３０１やモデム回路の入出力端子３１５から受信した情報を再送信する場合にも、同様に適用できる。

【００７０】

【発明の効果】

以上述べたように本発明においては、映像音声などの情報に伴って送られる制御情報に、コピー制御情報１０４のほか、再送制御１０６の情報を用いて、記録時の暗号化とインタネット再送可否の制御を行う。これにより、著作権者の意図を反映したコピーの制御と、インタネットなどの通信回線への再送信の制御が可能となる。このため、権利者の預かり知らない所で、良質なコピーが大量に配布される問題を解消できるという効果がある。

【図面の簡単な説明】

【図１】本発明を適用するディジタル情報送受信記録システム全体の一実施形態を示すブロック図。

【図２】図１における情報提供局１（送信装置）の構成の一例を示すブロック図。

【図３】図１における受信装置３の構成の一例を示すブロック図。

【図４】本発明における制御情報信号の構成の一例を示すブロック図。

【図５】記録媒体上での制御情報信号と情報データの記録位置を示す図。（ａ）はテープ、（ｂ）はビデオディスク、（ｃ）はハードディスクの例である。

【図６】図１における記録再生装置４の構成の一例を示すブロック図。

【図７】図６の記録再生装置の記録媒体の周辺を示すブロック図。

【図８】図１における受信装置３の構成の一例を示すブロック図。

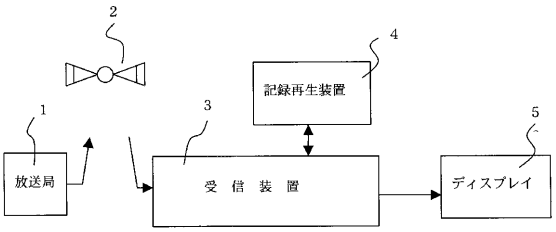
【図９】図６、図８における暗号化回路４１０３の構成の一例を示すブロック図。

【符号の説明】

１・・・・・・情報提供局（送信装置）
１６・・・・・管理情報付与回路
１０４・・・・コピー制御
１０６・・・・再送制御
１０９・・・・暗号化
１１０・・・・ユーザ識別
１１１・・・・暗号化情報
２・・・・・・中継局
３・・・・・・受信装置
３１４・・・・モデム（ＭＯＤＥＭ）回路
３１８・・・・暗号化回路
３１９・・・・復号化回路
４・・・・・・記録再生装置
４１・・・・・記録回路
４１０３・・・暗号化回路
４１０３２・・第一の暗号化回路
４１０３３・・第二の暗号化回路
４１０５・・・記録符号化回路
４１０８・・・制御検出回路
４１０９・・・記録制御回路
４２・・・・・再生回路
４２０６・・・暗号復号回路
４３・・・・・記録再生部
５・・・・・・ディスプレイ

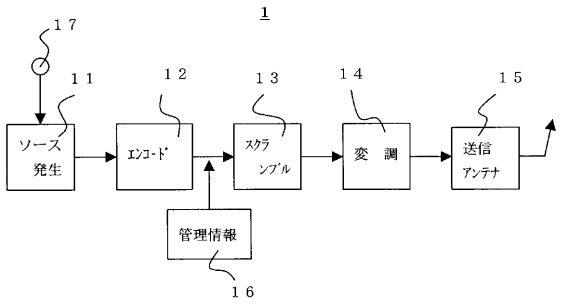
【図１】

【図１】



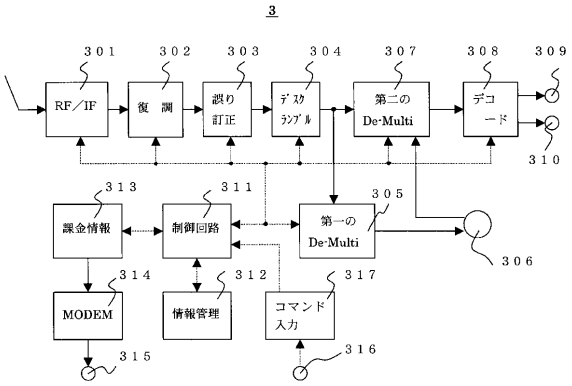
【図２】

【図２】



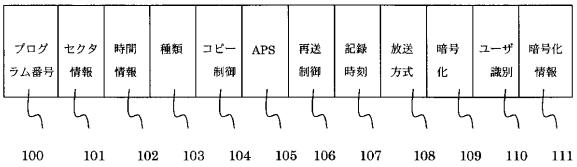
【図３】

【図３】



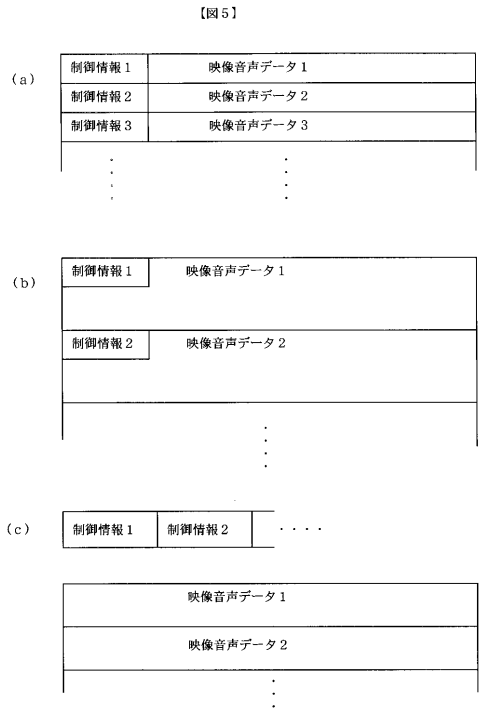
【図４】

【図４】



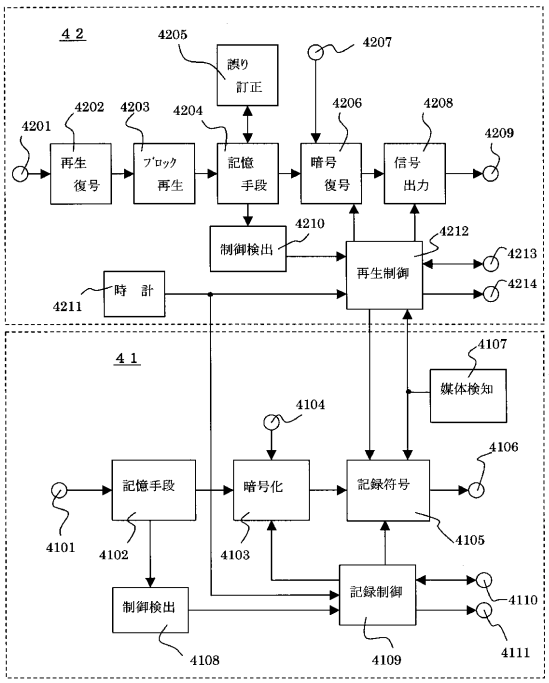
【図５】

【図５】



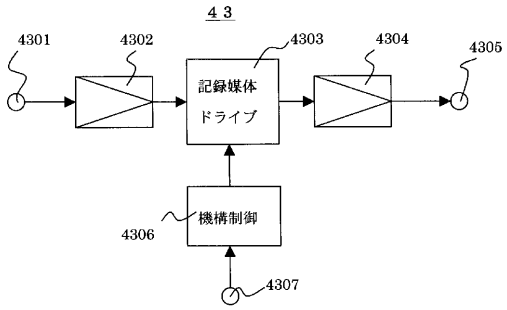
【図６】

【図６】



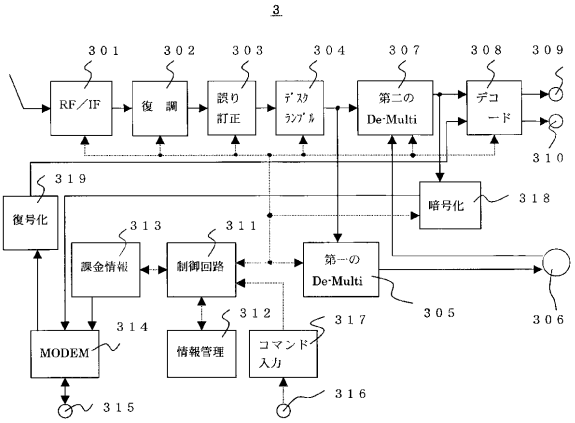
【図７】

【図７】



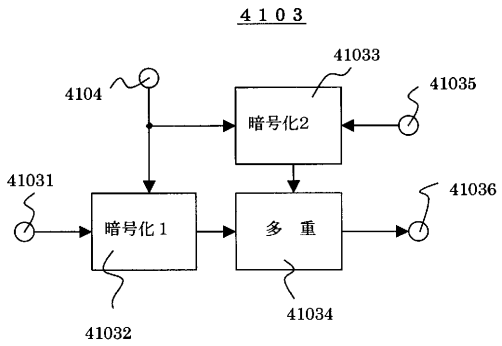
【図８】

【図８】



【図９】

【図９】



フロントページの続き

(72)発明者　吉岡　厚
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デジタルメディア開発本部内

合議体
審判長　奥村　元宏
審判官　乾　雅浩
審判官　岩井　健二

(56)参考文献　特開平１１－１０２５７２（ＪＰ，Ａ）
特開平９－１６０８９９（ＪＰ，Ａ）