(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年4 月3 日 (03.04.2003)

PCT

(10) 国際公開番号
WO 03/028027 A1

(51) 国際特許分類[7]: G11B 20/10, 27/00, H04N 5/76

(21) 国際出願番号: PCT/JP02/09609

(22) 国際出願日: 2002 年9 月19 日 (19.09.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-289982 2001 年9 月21 日 (21.09.2001) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 佐古 曜一郎 (SAKO,Yoichiro) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 杉浦 正知, 外(SUGIURA,Masatomo et al.); 〒171-0022 東京都 豊島区 南池袋 2丁目49番 7号 池袋パークビル７階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

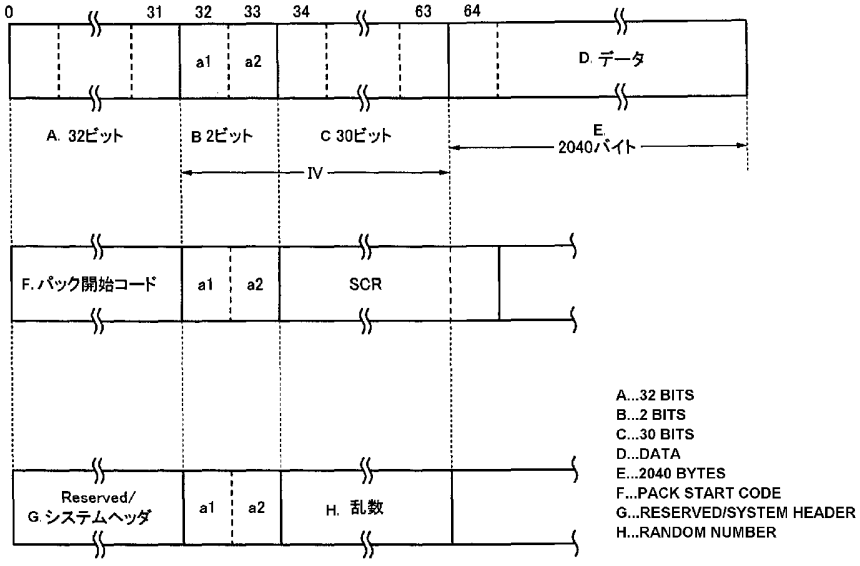
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: DATA OUTPUT METHOD, RECORDING METHOD AND APPARATUS, REPRODUCTION METHOD AND APPARATUS, DATA TRANSMISSION METHOD AND RECEPTION METHOD

(54) 発明の名称: データ出力方法、記録方法および装置、再生方法および装置、データ送信方法および受信方法



(57) Abstract: A data output method. An input data is converted into a 1-sector data set having a header in which at least one bit of a start code and subsequent two bits is a bit indicating encryption control. When encrypting the converted data, at least one bit of the two bits following the start code is set to indicate that the data is encrypted. The converted data is encrypted and the encrypted data is encoded and output.

[続葉有]

WO 03/028027 A1

(57) 要約:

入力されたデータを開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換し、変換されたデータを暗号化する場合には、開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定し、変換されたデータを暗号化し、暗号化されたデータをエンコードして出力するデータ出力方法。

明　細　書

データ出力方法、記録方法および装置、再生方法および装置、データ送信方法および受信方法

技術分野

この発明は、異なるデータフォーマットを融合するようにしたデータ出力方法、記録方法および装置、再生方法および装置、データ送信方法および受信方法に関する。

背景技術

パーソナルコンピュータの外部記憶装置としてのハードディスクドライブ、フロッピー（登録商標）ディスクドライブ、ＣＤ－ＲＯＭ／ＣＤ－Ｒ／ＣＤ－ＲＷディスクドライブ等では、セクタ単位でデータが処理される。例えばセクタサイズは、２Ｋバイト（２０４８バイト）である。コンテンツの著作権を保護するために、コンテンツデータを暗号化して記録される。セクタ単位でコンテンツデータの暗号化する、暗号化しないを制御しようとすると、セクタ毎に暗号化制御ビットが必要とされる。ＣＢＣ(Chaining Block Ciphering)モードのために、ＩＶ(Initial Vector：暗号化の初期値)が必要となる。

マルチメディアコンテンツのデータの伝送または記録フォーマットとしてＭＰＥＧ(Moving Picture Experts Group)が知られている。第１図Ａは、ＭＰＥＧ２システムのプログラムストリームのデータ構成を示す。１つのプログラムは、先頭のパックヘッダから終了コードまでである。一般的に、パックは、複数のパケットから構成されている。先頭のパックには、システムヘッダが付加される。２番目以降のパケットに対して、

システムヘッダを付加することは、オプションとされている。各パックに対して先頭にパックヘッダが付加されている。

第１図Ａに示すように、パックヘッダは、パック開始コード（３２ビット）、識別コード（２ビット）、ＳＣＲ(System Clock Reference:システム時刻基準参照値)（４２＋４ビット）、このストリームのビットレートを示す多重化レート（２２＋２ビット）、スタッフィング長（３＋８ビット）、スタッフィングバイト（８×Ｍビット）の各データによって構成される。スタッフィングバイトは、例えばパケットデータ長を一定とするために、使用されるダミーデータであり、意味のある情報を有していない。

第１図Ｂは、パケットの構成を示す。先頭に位置するパケット開始コード（３２ビット）は、先頭開始コード（２４ビット）とストリームＩＤ（８ビット）の各データから構成される。次に、パケットのデータ長を示すパケット長（１６ビット）が位置する。２ビットの制御コードは、ＭＰＥＧ２システムでは、”０１”とされる。フラグと制御（１４ビット）の先頭の２ビットがＰＥＳ(Packetized Elementary Stream)スクランブル制御に使用される。ＰＥＳヘッダ長（８ビット）によって、ヘッダ長が示される。フラグと制御に対応してコンディショナル・コーディングされた項目には、ＰＴＳ(Presentation Time Stamp)（３３＋７ビット）、ＤＴＳ(Decoding Time Stamp)（３３＋７ビット）、その他のコードに関するデータが含まれている。さらに、スタッフィングバイト（８×Ｍビット）が付加され、その後に、パケットデータ（８×Ｎビット）に関するデータが続いている。

第２図は、２Ｋバイト（２０４８バイト）をセクタ長とする、一般的なアプリケーションにおけるデータフォーマット（以下、一般データフォーマットと適宜称する）との融合を図るために、ＭＰＥＧ２システム

におけるデータ構成を２Ｋバイトに区切ったものを示す。第２図に示すように、１パックが１パケットから構成される。１パックのサイズが２Ｋバイトとされる。したがって、１パックが一般フォーマットの１セクタに相当する。１パックの先頭に、パックヘッダ（１４バイト）が位置し、以下、ＰＥＳヘッダ（１４バイト）、ストリームヘッダ（４バイト）、ユーザデータ（２０１６バイト）に関するデータが順に配置される。ユーザデータを８バイト単位で区切ると、ユーザ（またはパケット）データは、Ｄ１からＤ252までのデータからなる。ユーザデータは、例えば圧縮符号化および暗号化がされたオーディオデータである。このような第２図に示すデータ構成は、ＭＰＥＧ２システムの符号化規則を満たしている。

パックヘッダは、第１図Ａに示したものと同様のものであるが、スタッフィングバイトを付加せず、１４バイトの長さとしている。すなわち、パックヘッダは、パック開始コード（３２ビット）、制御コード（２ビット）、ＳＣＲ（４２＋４ビット）、このストリームのビットレートを示す多重化レート（２２＋２ビット）、スタッフィング長（３＋８ビット）の合計１１２ビット（＝１４バイト）のデータによって構成される。スタッフィングバイトを付加しない理由は、スタッフィングバイトによって、スクランブル制御ビットの位置が変動することを避けるためである。

ＰＥＳヘッダは、第１図Ｂに示したものと同様のものであるが、パケット開始コード（３２ビット）から、パケット長（１６ビット）、２ビットの制御コード、フラグと制御（１４ビット）、ＰＥＳヘッダ長（８ビット）、ＰＴＳ（３３＋７ビット）までの合計１１２ビット（＝１４バイト）を使用する。

ストリームヘッダ（４バイト）には、オーディオの符号化方法（リニ

アＰＣＭ、ＭＰ３(MPEG1 Audio Layer III)、ＡＡＣ(Advanced Audio Coding)、ＡＴＲＡＣ３(Adaptive Transform Acoustic Coding 3)等）を示す情報、ビットレート(６４Kbps等)の情報、チャンネル数（モノラル、ステレオ、５．１チャンネル等）の情報などが記録される。

パックヘッダ、ＰＥＳヘッダおよびストリームヘッダの３２バイト（＝２５６バイト）に対して、ビットの位置を規定するために、ビット番号を付加する。先頭のビットをビット０とすると、パックヘッダがビット０からビット111で構成され、ＰＥＳヘッダがビット112からビット223となり、ストリームヘッダがビット223からビット255となる。ＰＥＳヘッダでは、フラグと制御に含まれるスクランブル制御ビットの位置がビット162および163となる。スクランブル制御ビットは、"００"がスクランブルなし、"０１"がスクランブルあり、"１０"および"１１"がリザーブド（未定義）である。

パックヘッダ内のビット３２およびビット３３の２ビットの制御コードは、ＭＰＥＧ１システムでは、"００"であり、ＭＰＥＧ２システムでは、"０１"である。なお、ＭＰＥＧ１システムの場合、スクランブル制御ビットはない。暗号化に必要なＩＶは、パックヘッダ内のＳＣＲ、ＰＥＳヘッダ内のＰＴＳ等が使用される。

第３図Ａは、一般データフォーマット（ＭＰＥＧシステム以外の一般的なアプリケーションにおけるデータフォーマットを意味する）の１セクタのデータ構成を示す。ＣＢＣ(Chaining Block Ciphering)モードでＩＶ付きの暗号化（通常、８バイト単位の処理が多い）を仮定すると、先頭の８バイトにスクランブル制御、ＩＶ等のデータが含まれる。例えば４バイトがＩＶとして使用される。セクタヘッダを除いた２０４０バイトがユーザデータである。したがって、ユーザデータは、２０４０バイトとなり、８バイト単位に区切ると、Ｄ１からＤ255までのデータが

含まれる。

上述したＭＰＥＧ２システムのデータフォーマットと、第３図Ａに示す一般データフォーマットの両者を例えばパーソナルコンピュータ、光ディスクドライブ、アプリケーションソフトウェア（以下、ドライブ等と称する）で扱うことができることが望ましい。例えば一般アプリケーションのデータは、一般データフォーマットで扱い、オーディオ、ビデオデータをＭＰＥＧ２システムのデータで扱うようになされる。オーディオ、ビデオデータをＭＰＥＧ２システムのデータフォーマットとすることによって、オーディオデータおよびビデオデータを多重化でき、例えば音声と共に歌詞の画像を記録することができる。タイムスタンプである、ＰＴＳを利用することによって、可変長圧縮符号化を行なっている場合でも、高速アクセスが可能となる。

二つの異なるデータフォーマットを使用する場合、ドライブ等が両者を識別して切り替える方法が考えられる。この方法は、ドライブ等が二つのフォーマットを識別するのが難しい。セクタ単位で暗号化されているか否かを識別するのに、ＭＰＥＧ２システムと一般データフォーマットでは、異なる位置のビットを見なくてはならず、セクタ単位の暗号化の有無の判別が困難である。

他の方法は、二つの異なるデータフォーマットを融合するものである。この場合では、切替に伴う問題が生じない。第３図Ｂは、一般データフォーマットをＭＰＥＧ２システムに合わせた場合のデータ構成を示す。先頭の３２バイトは、ＭＰＥＧ２システムの場合では、第２図Ａに示すようなパックヘッダ、ＰＥＳヘッダ、ストリームヘッダである。一般データフォーマットのセクタヘッダ（８バイト）の持つ情報（スクランブル制御のビットおよびＩＶ）は、３２バイトが持つことができる。しかしながら、一般データフォーマットでは、８バイトのヘッダで良かった

のが、３２バイトを必要とするために、（３２－８＝２４バイト）が無駄になる問題がある。言い換えると、１セクタのユーザデータが２０４０バイトから２０１６バイトに減少する問題が生じる。さらに、ＭＰＥＧ２システムにおけるスクランブル制御ビットの位置を固定化するために、スタッフィングバイトを使用できない問題があった。

一方、ＭＰＥＧ２システムを一般データフォーマットに合わせると、第３図Ｃに示すように、ＭＰＥＧ２システムのデータフォーマットの１セクタの先頭に８バイトのヘッダが付加される。その結果、ＭＰＥＧ２システム以外のアプリケーションでは問題がないが、ＭＰＥＧ２システムのアプリケーションでは、先頭の８バイトが無駄になる問題がある。

したがって、この発明の目的は、無駄なデータが生じ、ユーザデータが減少する問題を回避して、異なるシステムのデータ構成を融合することができるデータ出力方法、記録方法および装置、再生方法および装置、データ送信方法および受信方法を提供することになる。

発明の開示

上述した目的を達成するために、請求の範囲第１項の発明は、入力されたデータを開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換し、変換されたデータを暗号化する場合には、開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定し、変換されたデータを暗号化し、暗号化されたデータをエンコードして出力するデータ出力方法である。

請求の範囲第８項の発明は、入力されたデータを開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビ

ットであるヘッダが先頭に付加された１セクタ単位のデータに変換し、変換されたデータを暗号化する場合には、開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定し、変換されたデータを暗号化し、暗号化されたデータに記録のためのエンコード処理を施して記録媒体に記録する記録方法である。

請求の範囲第１５項の発明は、入力されたデータを開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換する変換部と、変換部によって変換されたデータを暗号化する場合には、開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定する設定部と、設定部からの出力データに暗号化処理を施す暗号化処理部と、暗号化処理部からの出力データに記録のためのエンコード処理を施すエンコード処理部と、エンコード処理部からの出力データを記録媒体に記録する記録部とを備えている記録装置である。

請求の範囲第２２項の発明は、ユーザデータと開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータが記録された記録媒体から読み出されたデータをデコードし、デコードされたデータの開始コードに続く２ビットのうちの少なくとも１ビットを検出し、検出した結果、デコードされたデータが暗号化されているときには暗号を解読し、解読されたデータを１セクタ単位のデータから所定のデータ単位のデータに変換し出力する再生方法である。

請求の範囲第２９項の発明は、ユーザデータと開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータが記録された

記録媒体から読み出されたデータをデコードするデコーダと、デコーダからの出力データの開始コードに続く２ビットのうちの少なくとも１ビットを検出する検出部と、検出部による検出の結果、デコードされたデータが暗号化されているときにはデコーダからの出力データの暗号を解読する解読部と、解読部からの出力データを１セクタ単位のデータから所定のデータ単位のデータに変換して出力する変換部とを備えている再生装置である。

請求の範囲第３６項の発明は、入力されたデータを開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換し、変換されたデータを暗号化する場合には、開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定し、変換されたデータを暗号化し、暗号化されたデータに送信のためのエンコード処理を施して送信するデータ送信方法である。

請求の範囲第４３項の発明は、ユーザデータと開始コードと開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータを受信し、受信したデータをデコードし、デコードされたデータの開始コードに続く２ビットのうちの少なくとも１ビットを検出し、検出した結果、デコードされたデータが暗号化されているときには暗号を解読し、解読されたデータを１セクタ単位のデータから所定のデータ単位のデータに変換し出力するデータ受信方法である。

所定位置の２ビットを暗号化制御に使用することによって、無駄なデータを生じさせず、且つ矛盾なく、二つの異なるシステム、例えばＭＰＥＧ２システムと一般アプリケーションとを融合できる。然も、セクタ単位の暗号化制御が可能である。また、スクランブル制御ビットが規定

されていない、ＭＰＥＧ１システムであっても、暗号化制御が可能となり、ＭＰＥＧ１のコンテンツのセキュリティを保護できる。暗号化の初期値が各データフォーマットで同一の位置に配置されているので、同じ暗号化システムによる暗号化が可能となる。暗号化が復号された後では、ＭＰＥＧ１およびＭＰＥＧ２のシステムとして使用できる。ＭＰＥＧシステムでスタッフィングバイトの前の固定位置に暗号化制御のビットを配置するので、スタッフィングバイトを使用することができる。

図面の簡単な説明

第１図Ａは、この発明を適用できるＭＰＥＧ２システムのプログラムストリームのデータ構成を示す図であり、第１図Ｂは、この発明を適用できるＭＰＥＧ２システムのパケットの構成を示す図であり、第２図は、ＭＰＥＧ２システムのデータ構成の一例を示す図であり、第３図Ａは、一般的アプリケーションにおけるデータフォーマットの１セクタのデータ構成を示す図であり、第３図Ｂは、一般的アプリケーションにおけるデータフォーマットをＭＰＥＧ２システムに合わせた場合のデータ構成を示す図であり、第３図Ｃは、ＭＰＥＧ２システムを一般的アプリケーションにおけるデータフォーマットに合わせた場合のデータ構成を示す図であり、第４図Ａは、この発明の一実施形態におけるデータ構成（１セクタを２Ｋバイトとした例）を示す図であり、第４図Ｂは、ＭＰＥＧ２システムに対してこの発明を適用した場合のデータ構成の一部を示す図であり、第４図Ｃは、ＭＰＥＧ２システム以外の一般データフォーマットに対してこの発明を適用した場合のデータ構成の一部を示す図であり、第５図Ａは、この発明の一実施形態における暗号化制御ビットの定義の一例を示す図であり、第５図Ｂは、この発明の一実施形態における暗号化制御ビットの定義の他の例を示す図であり、第６図は、この発明

が適用された記録装置、送信装置の一実施形態のブロック図であり、第７図は、この発明が適用された再生装置、受信装置の一実施形態のブロック図であり、第８図は、この発明に使用できるエンクリプタの一例のブロック図であり、第９図は、この発明に使用できるデクリプタの一例のブロック図である。

発明を実施するための最良の形態

以下、この発明の一実施形態について説明する。最初に、第４図Ａ～第４図Ｃを参照してこの一実施形態におけるデータフォーマットを説明する。第４図Ａは、１セクタを２Ｋバイト（２０４８バイト）とした例である。但し、２Ｋバイトは、一例であって、１セクタを２Ｋバイト以外としても良い。１セクタの先頭の８バイト（ビット０からビット６３）の内で、ビット３２のビット（ａ１とする）とビット３３のビット（ａ２とする）の２ビットを暗号化制御用の制御コードに使用する。この制御コードａ１、ａ２の２ビットと残りの３０ビットの合計３２ビットをＩＶとして利用する。ビット６４以降のデータがＩＶを使用してＣＢＣモードで暗号化される。但し、ビット６４に限定されずに、ビット６４以降の任意のビット以降のデータ例えばビット１２８以降のデータを暗号化しても良い。

第４図Ｂは、ＭＰＥＧ２システムに対してこの発明を適用した場合のデータ構成の一部を示す。すなわち、第２図を参照して説明したように、先頭の３２ビットがパック開始コードに相当し、次に、制御コード（ａ１およびａ２）が配置され、その後に（４２＋２）ビットのＳＣＲで配置される。したがって、制御コードがスクランブル制御にも使用され、ＩＶがＳＣＲの３０ビットによって構成される。ビット６４以降のデータがＩＶを使用して暗号化される。ユーザデータのサイズは、第２図の

場合と同様に、２０１６バイトである。

ＭＰＥＧ２システムでは、ビット162および163にスクランブル制御ビットが配置され、スクランブル制御ビットは、"００"がスクランブルなし、"０１"がスクランブルあり、"１０"および"１１"がリザーブド（未定義）とされている。一実施形態のように、制御コード（ａ１およびａ２）を暗号化制御に使用する場合、制御コードの情報とスクランブル制御ビットの情報とが矛盾しないものとされる。または、制御コードの情報の方を優先する。すなわち、制御コードがスクランブル有りなら、スクランブル制御ビットが何であってもスクランブル有りとする。

第４図Ｃは、ＭＰＥＧ以外の一般データフォーマットに対してこの発明を適用した例である。先頭の３２ビットがリザーブドまたはシステムヘッダとして使用される。その次に２ビットの制御コードａ１およびａ２が配置され、残りの３０ビットがハードウエアまたはソフトウェアによって生成された乱数とされる。制御コードａ１、ａ２と乱数がＩＶに相当する。但し、ＩＶとして６４ビットの長さが必要な場合では、ビット３２からビット６３までの３２ビットを２度繰り返したデータ、またはビット０からビット６３までのデータを使用するようにしても良い。ビット６４以降がユーザデータとなり、ユーザデータのサイズは、第３図Ａに示すデータ構成と同様に、２０４０バイトとなる。

第５図は、２ビットの制御コード（ａ１およびａ２）の定義の一例および他の例を示す。第５図Ａに示す例では、ＭＰＥＧ１とＭＰＥＧ２の識別のために２ビットが使用される。"a1 a2" ＝"００"がＭＰＥＧ１システムで暗号化なしと定義され、"a1 a2" ＝"０１"がＭＰＥＧ２システムで暗号化なしと定義されている。これは、ＭＰＥＧの定義と一致している。"a1 a2" ＝"１０"がＭＰＥＧ１システムで暗号化ありと定義され、"a1 a2" ＝"１１"がＭＰＥＧ２システムで暗号化ありと定義される。な

お、ＭＰＥＧ１システムが使用されない時には、"a1 a2" ＝"００"および"a1 a2" ＝"１０"を未定義としても良い。

ビット３２（ａ１）のみを暗号化の制御に使用しても良い。この場合では、"a1 a2" ＝"００"がＭＰＥＧ１システムで暗号化なしと定義され、"a1 a2" ＝"０１"がＭＰＥＧ２システムで暗号化なしと定義され、"１ｘ"（ｘは、"0"または"1"の何れでも良いことを表している。）が暗号化ありと定義される。

第５図Ｂに示す他の例では、暗号化の制御に２ビットが使用される。"a1 a2" ＝"００"が未定義とされ、"a1 a2" ＝"０１"が暗号化なしと定義され、"a1 a2" ＝"１０"が第２の暗号化方法による暗号化と定義され、"a1 a2" ＝"１１"が第２の暗号化方法と異なる第１の暗号化方法による暗号化と定義される。第１および第２の暗号化方法では、暗号化の鍵または暗号化方法が異なったものとされる。暗号化の鍵を異ならせる方法としては、第１の暗号化方法の鍵Ｋａをハッシュ演算して第２の暗号化方法の鍵Ｋｂを求める方法、全く関係のない鍵を使用する方法等が可能である。

暗号化方法を異ならせるのは、コンテンツの種類によって暗号化方法を異ならせるためである。例えば試聴用コンテンツと試聴用でない本来の例えば課金されるコンテンツとで暗号化が異なったものとされる。上述した例における鍵Ｋａが課金対象コンテンツに関するデータを復号するのに使用され、鍵Ｋｂが試聴用のコンテンツに関するデータを復号するのに使用される。鍵Ｋａから鍵Ｋｂに関するデータは、ハッシュ演算で作成できるが、鍵Ｋｂに関するデータからは、ハッシュ関数が一方向性のために、鍵Ｋａに関するデータを作成できない。

さらに、第５図Ｂの例では、２ビット"a1 a2"が暗号化ありを意味している場合では、暗号化を復号すると、この２ビットが暗号化なしを意

味する値に変更される。ＭＰＥＧ１システムでは、コンテンツに関するデータの復号を行うと、"a1 a2"を"００"に書き換え、ＭＰＥＧ２システムでは、コンテンツに関するデータの復号を行うと、"a1 a2"を"０１"に書き換える。なお、未定義の２ビットを第３の暗号化方法を示すものとしても良い。

第６図を参照してこの発明が適用された記録装置および送信装置の一実施形態について説明する。第６図では、記録装置および送信装置が同一の図として描かれているが、通常、両者は、異なるシステムとして別々に構成される。参照符号１ａ、１ｂ、１ｃは、ビデオデータ、オーディオデータおよびテキストデータがそれぞれ入力される入力端子である。これらのデータは、必要に応じて圧縮されたデータであり、各パケットに入るデータ長に区切られている。

入力端子１ａ～１ｃから入力されたデータがマルチプレクサ２において時分割多重され、多重化データがＭＰＥＧ判断部３に供給される。ＭＰＥＧ判断部３は、使用するシステムを決定する。例えば、ＭＰＥＧ判断部３は、ユーザの選択、アプリケーションソフトウェアの判断、入力されたデータに付随する制御情報等に基づいて、使用するシステムが決定される。

ＭＰＥＧ判断部３によってＭＰＥＧ１システムを使用すると決定された場合では、ＭＰＥＧ１システム化部４に多重化データが供給される。ＭＰＥＧ判断部３によってＭＰＥＧ２システムを使用すると決定された場合では、ＭＰＥＧ２システム化部５に多重化データが供給される。ＭＰＥＧ判断部３によって一般アプリケーションを使用すると決定された場合では、乱数発生部６に多重化データが供給される。乱数発生部６からは、第４図Ｃに示すように、リザーブドまたはシステムヘッダと２ビットと乱数とが各セクタに付加されたデータ構成の出力データが発生さ

れる。

ＭＰＥＧ１システム化部４は、ＭＰＥＧ１システムのデータ構成に多重化データを変換する。ＭＰＥＧ２システム化部５は、第２図および第４図Ｂに示したようなパックヘッダ（パック開始コード、２ビット、ＳＣＲ、多重化レート、スタッフィング長）、ＰＥＳヘッダおよびストリームヘッダが各パック（セクタ）に付加されたＭＰＥＧ２システムのデータ構成に多重化データを変換する。ＭＰＥＧ１システムのデータ構成は、第４図Ｂと略同様であるが、スクランブル制御ビットが含まれない等の相違点を有している。

ＭＰＥＧ１システム化部４、ＭＰＥＧ２システム化部５および乱数発生部６の出力データが暗号化判断部７に供給される。暗号化判断部７は、ＭＰＥＧシステム化部４、ＭＰＥＧシステム化部５又は乱数発生部６のうちのいずれかから供給される出力データに暗号化を行うか否かを判断、制御する。暗号化判断部７は、暗号化方法が複数用意されている場合は、暗号化の種類を選択する。暗号化判断部７は、ユーザ例えばコンテンツ制作者の選択、アプリケーションソフトウェアの判断、オーサリングシステムの指示、入力データに付随する制御情報等に基づいて暗号化を行うか否かを判断し、制御する。

暗号化を行う場合では、暗号化判断部７から出力されたデータがビット設定回路８に供給され、その出力にａ１＝”1”にセットされたデータが得られる。ａ１＝１にセットされたデータがエンクリプタ９に供給され、暗号化される。第４図Ｂ、第４図Ｃに示したデータ構成のうちビット６４以降のデータが暗号化される。エンクリプタ９による暗号化は、ＩＶ（初期値）を使用したＣＢＣモードでなされる。ＭＰＥＧ１およびＭＰＥＧ２のシステムでは、ＩＶがＳＣＲの一部のデータであり、一般データフォーマットでは、ＩＶが乱数発生部６で生成された乱数である。

第５図Ａに示すように、ビット設定回路８によってａ１＝"1"にセットされたデータは、そのセクタのデータが暗号化されていることを意味する。暗号化判断部７によって暗号化を行なわないと判断された場合は、暗号化判断部７の出力データがビット設定回路１０に供給され、ビットａ１が"0"に設定される。

エンクリプタ９によって暗号化されたデータ、またはビット設定回路１０の出力データがエラー訂正符号化回路１１に供給され、エラー訂正符号化が施される。エラー訂正符号化回路１１の出力データが変調回路１２に供給される。

記録装置の場合では、変調回路１２からの出力データが記録アンプ１３を介して光ピックアップ１４に供給され、光ピックアップ１４によって光ディスク１５上に記録される。光ピックアップ１４が送りモータ（図示しない）によって光ディスク１５の径方向に送られる。光ディスク１５は、記録可能な光ディスクである。光ディスク１５は、スピンドルモータ１６によって、線速度一定または角速度一定で回転駆動される。さらに、記録装置には、光ピックアップ１４のトラッキングサーボおよびフォーカシングサーボ、並びにスピンドルモータ１６の回転制御を行うサーボ回路（図示しない）が設けられている。

この一実施形態の光ディスク１５は、光ディスク１５に記録を行うのに十分な出力レベルのレーザ光を照射することによってデータの記録が可能で、光ディスク１５によって反射されたレーザ光の光量の変化を検出することによって光ディスク１５に記録されたデータの再生可能な相変化型ディスクである。光ディスク１５を構成する相変化記録材料からなる記録膜が被着される基板の材質は、例えばポリカーボネートであり、ポリカーボネートを射出成形することによって、基板上にグルーブと呼ばれるトラック案内溝が予め形成されている。このディスク基板上に形

成されるグルーブは、予め形成する意味でプリグルーブとも呼ばれ、グルーブの間は、ランドと呼ばれる。通常、読取レーザ光の入射側から見て手前側がグルーブであり、遠い側がランドであると定義される。グルーブは、内周から外周へスパイラル状に連続して形成されている。なお、この発明は、記録可能であれば、ＣＤ－ＲＷディスク等の相変化型光ディスクに限らず、光磁気ディスク、有機色素を記録材料として使用するＣＤ－Ｒディスク等の追記形ディスクに対しても適用できる。

グルーブは、光ディスク１５の回転制御用と記録時の基準信号とするために光ディスクの径方向に蛇行（ウォブルと称する）している。光ディスク１５に記録されるデータは、グルーブ内、またはグルーブおよびランドに記録される。さらに、光ディスク１５にはグルーブをディスクの径方向に蛇行、即ち、ウォブリングさせることによってアドレス情報としての絶対時間情報やクロックが連続的に予め記録されている。ＣＤ－Ｒディスク、ＣＤ－ＲＷディスクでは、ディスクの径方向に蛇行されたグルーブを光学的に検出することによって得られるアドレス情報としての絶対時間情報を参照して光ディスク１５上の所望のデータ書き込み位置に、光ピックアップ１４を移動させ、光ピックアップ１４から光ディスク１５に対してレーザ光を照射することによって、データを光ディスク１５の所望の位置に書き込む。

このようなウォブリングしたグルーブを有する光ディスクは、以下のようにして製造される。マスタリング装置は、ディスク状のガラス原盤に塗布されたフォトレジスト膜にレーザ光を照射すると共に、レーザ光を径方向に偏向または径方向に振ることによって、ウォブリングされたグルーブを形成する。レーザ光の照射によって露光されたフォトレジスト膜を現像することによってディスク原盤が作成され、ディスク原盤に電鋳処理を施すことによってスタンパが作成される作製されたスタンパ

を用いて射出成形を行うことによって、上述したウォブリングされたグルーブを有するディスク基板が成形される。このディスク基板のグルーブが形成された面に相変化型の記録材料をスパッタリング等の手法を用いて被着することによって光ディスク１５が作成される。

なお、第６図に示す記録装置は、専用のハードウエアに限らず、ドライブ（ハードウエア）とパーソナルコンピュータ（ソフトウェア）によって実現することが可能である。エラー訂正符号化回路１１から後の構成がハードウエア（現行のＣＤ－Ｒドライブ、ＣＤ－Ｒ／Ｗドライブ等のドライブ）の構成とされ、残りの部分がコントローラとしてのマイクロコンピュータ等によって実行されるソフトウェアによって実現される。記録装置では、一例として物理フォーマットとしてＣＤ－ＲＯＭモード２フォーム１が使用され、ファイル管理システムとしてＵＤＦ(Universal Disc Format)が使用され、アプリケーションとしてＭＰＥＧ１システム、ＭＰＥＧ２システムまたは一般アプリケーションが使用される。アプリケーションが異なる場合でも、第４図Ａ～第４図Ｃを参照して説明したように、融合したデータフォーマットでもってデータが光ディスクに記録され、または送信される。

送信装置の場合では、変調回路１２の出力データが送信アンプ１７を介して送信アンテナ１８に供給される。送信アンテナ１８から例えば通信衛星に対して信号が送出される。通信衛星を用いる方法以外の送信方法として、インターネットを介して変調回路１２からの出力データを送信する場合等にもこの発明は、適用可能である。

第７図は、この発明が適用された再生装置および受信装置の一実施形態を示す。記録装置と同様に、再生装置は、ハードウエアの構成のディスクドライブ（ＣＤ－ＲＯＭドライブ、ＣＤ－Ｒドライブ、ＣＤ－ＲＷドライブ等）と、コントローラによって実行されるアプリケーションソ

フトウェアとによって構成される。第７図に示した再生装置は、全てハードウエアの構成とすることも可能である。

第７図において、光ディスク１５は、スピンドルモータ２２によって回転され、光ピックアップ２３によって光ディスク１５からデータが読み出される。光ディスク１５に光ピックアップ２３から再生に必要とされるレーザ光を照射し、光ピックアップ２３に設けられた４分割フォトディテクタによって光ディスク２１によって反射されたレーザ光を検出する。フォトディテクタからの出力信号としての検出された信号が再生ＲＦ処理部２４に供給される。

再生ＲＦ処理部２４では、処理部２４に設けられたマトリックスアンプによってフォトディテクタの検出信号が演算され、再生（ＲＦ）信号、トラッキングエラー信号、フォーカスエラー信号を生成する。グルーブをウォブリングさせることによってクロック、アドレスが記録されている場合では、ウォブリングされたグルーブを検出した信号が再生ＲＦ処理部２４から出力される。再生ＲＦ処理部２４によって生成されたＲＦ信号が復調部２５に供給され、例えば供給されたＲＦ信号に基づきＥＦＭ復調処理が行われる。

受信装置の場合では、受信アンテナ２６によって受信された信号が受信ＲＦ処理部２７に供給される。受信ＲＦ処理部２７では、周波数変換等の処理がなされる。受信ＲＦ処理部２７の出力信号が復調部２５に供給され、復調処理がなされる。復調部２５の出力データがエラー訂正回路２８に供給され、エラー検出及びエラー訂正処理が行われる。

図示しないサーボ回路に、再生ＲＦ処理部２４によって生成されたトラッキングエラー信号、フォーカスエラー信号が供給され、サーボ回路は、スピンドルモータ２２の回転および光ピックアップ２３のトラッキングおよびフォーカスの各制御を行う。サーボ回路は、光ピックアップ

２３に対するトラッキングサーボおよびフォーカスサーボと、スピンドルモータ２２に対するスピンドルサーボと、光ピックアップ２３を光ディスク１５の径方向に移動させるスレッドサーボを行う。

エラー訂正回路２８によってエラー訂正されたデータがビット検出回路２９に供給される。ビット検出回路２９は、ビットａ１が"0"か"1"かを判別するものである。検出回路２９による検出の結果、ａ１＝"1"であれば、再生データ、即ちエラー訂正回路２８からの出力データが暗号化されていることを意味するので、再生データがＩＶ読取部３０に供給される。第４図Ａ～第４図Ｃに示したように、再生データにおけるＩＶの位置は、固定されているので、ＩＶ読取部３０が容易にＩＶを読み取ることができる。

ＩＶ読取部３０から出力される読み取られたＩＶと暗号化データとがデクリプタ３１に供給され、デクリプタ３１にて暗号化を解くための処理、即ち復号処理が行われる。デクリプタ３１の復号出力データがビット設定回路３２に供給される。ビット設定回路３２では、デクリプタ３１から出力されるデータのビットａ１が暗号化なしを意味する"0"に設定される。ビットａ１を"0"に設定した結果の２ビットは、ＭＰＥＧ２システムの規則に一致したものとなる。設定回路３２によってビットａ１が"0"に設定されたデータがＭＰＥＧ判断部３３に供給される。ビット検出回路２９において、ビットａ１が"0"であると検出された場合では、エラー訂正回路２８からの出力データは、暗号化されていないので、そのままＭＰＥＧ判断部３３に供給される。

ＭＰＥＧ判断部３３は、入力されたデータがＭＰＥＧ１システムのものか、ＭＰＥＧ２システムのものか、一般アプリケーションのものかが判別される。例えば、ＭＰＥＧ１のシステムのものかＭＰＥＧ２のシステムのものかの判別は、データにスクランブル制御ビットが含まれてい

るか否かによって判別され、ＳＣＲの部分が乱数であるか否かによって一般アプリケーションデータなのかを判別する。入力されたデータがＭＰＥＧ１システムのものであれば、ＭＰＥＧ１システム処理部３４にて再生データが処理される。入力されたデータがＭＰＥＧ２システムのものであれば、ＭＰＥＧ２システム処理部３４にて再生データが処理される。ＭＰＥＧ１システム処理部３４およびＭＰＥＧ２システム処理部３５によって各システムのデータがそれぞれデコード処理され、パックの区切りを有するビデオデータ、オーディオデータが各々出力される。

ＭＰＥＧ判断部３３において、入力されたデータが一般アプリケーションのものと判断されたときには、そのままデータがデマルチプレクサ３６に供給される。デマルチプレクサ３６には、システム部３４又は３５によって処理後のビデオデータ、オーディオデータが供給される。デマルチプレクサ３６は、これらのデータを同じ種類毎にまとめて出力端子３７ａ、３７ｂおよび３７ｃにそれぞれ出力する。

第８図は、ＣＢＣモードによるエンクリプタ９（第６図参照）の一例を示す。例えば６４ビット（８バイト）毎に区切られたデータＭｉがmod2の加算器４１（例えばエクスクルーシブＯＲゲート）に供給される。１セクタの最初のデータＭ１の場合では、加算器４１に対してＩＶ（初期値）が供給される。加算器４１の出力がブロックエンクリプタ４２に供給される。ブロックエンクリプタ４１は、ＤＥＳ(Data Encryption Standard)、ＡＥＳ、トリプルＤＥＳ等によって暗号化処理を行うエンクリプタである。

ブロックエンクリプタ４２に対して鍵データ（１２８ビット）が供給され、加算器４１の出力が鍵データを使用して暗号化される。エンクリプタ４２から暗号化データＥ（Ｍｉ）（６４ビット）が得られる。暗号化データＥ（Ｍｉ）が出力されると共に、加算器４１にフィードバック

され、次の入力データＭ２に対して加算される。以下、同様の動作が１セクタのデータの処理が終了するまで繰り返される。

第９図は、エンクリプタ９に対応するデクリプタ３１（第７図参照）の構成例を示す。上述したように、暗号化されたデータＥ（Ｍｉ）がブロックデクリプタ４３に供給される。ブロックデクリプタ４３に対して鍵データが供給され、データＥ（Ｍｉ）が復号される。復号データがmod2の加算器４４に供給される。セクタの最初のデータに関しては、加算器４４でそのセクタのＩＶと加算される。２番目以降のデータに関しては、加算器４４にてブロックデクリプタ４３の出力データと入力データとが加算される。加算器４４の出力に復号データＭｉが得られる。

この発明は、上述した一実施形態等に限定されるものでは無く、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば再生装置、受信装置において、復号した後にビットａ１を"0"にセットしている。しかしながら、この処理を行なわないで、復号後では、ビットａ１を無視するようにしても良い。また、この発明による記録方法を読み出し専用形光ディスクに対して適用する場合では、第６図に示す記録装置は、マスタリング装置に対して適用される。さらに、この発明は、光ディスク限らず、他のデータ記録媒体例えばメモリカードに対しても適用することができる。

この発明では、ＭＰＥＧシステムと一般アプリケーションのように異なるシステムのデータを融合したデータフォーマットでセクタ単位の暗号化制御を行うことができる。したがって、二つのシステムのそれぞれのデータを識別して処理を切り替える場合の問題を生じない。また、データ構成を融合した結果、１セクタに配することができるデータ量が減少せず、効率が良い利点がある。さらに、融合した結果、各システムで矛盾を生じることがない。

この発明では、各システムにおいて、暗号化の初期値をセクタ内の同一の位置に配置することができ、異なるシステムのデータであっても、共通の暗号化および復号化を行うことができる。しかも、スクランブル制御が規定されていないＭＰＥＧ１システムにおいても、各セクタが暗号化制御の情報を持つことができ、コンテンツのセキュリティ（著作権）を保護することができる。暗号化を復号した後に、ビットの書き換えを行うことによって、復号データがＭＰＥＧ１システムおよびＭＰＥＧ２システムで利用できる。さらに、スタッフィングバイトを付加する場合でも、暗号化制御のためのビットの位置が固定であり、可変長に対応することが可能となる。

請　求　の　範　囲

１．入力されたデータを開始コードと上記開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換し、

上記変換されたデータを暗号化する場合には、上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定し、

上記変換されたデータを暗号化し、

上記暗号化されたデータをエンコードして出力するデータ出力方法。

２．上記１セクタのデータは２０４８バイトであり、上記方法は上記変換されたデータの暗号化を行う場合にはビット６４以降のデータを暗号化する請求の範囲第１項記載のデータ出力方法。

３．上記方法は、ＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換するか否かを判別し、上記ＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換すると判別されたときには上記入力されたデータをＭＰＥＧのエンコード規則にしたがって変換する請求の範囲第１項記載のデータ出力方法。

４．上記方法は、上記入力されたデータをＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換しないと判別されたときには上記開始コードに続く２ビットに後続して乱数データを付加された１セクタ単位のデータに変換する請求の範囲第３項記載のデータ出力方法。

５．上記方法は、ＭＰＥＧ－１のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第３項記載のデータ出力方法。

６．上記方法は、ＭＰＥＧ－２のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第３項記載のデータ出力方法。

７．上記方法は、上記変換されたデータの暗号化を行わない場合には上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化が行われていないことを示すように設定し、上記変換されたデータをエンコードして出力する請求の範囲第１項記載のデータ出力方法。

８．入力されたデータを開始コードと上記開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換し、

上記変換されたデータを暗号化する場合には、上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定し、

上記変換されたデータを暗号化し、

上記暗号化されたデータに記録のためのエンコード処理を施して記録媒体に記録する記録方法。

９．上記１セクタのデータは２０４８バイトであり、上記方法は上記変換されたデータの暗号化を行う場合にはビット６４以降のデータを暗号化する請求の範囲第８項記載の記録方法。

１０．上記方法は、ＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換するか否かを判別し、上記ＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換すると判別されたときには上記入力されたデータをＭＰＥＧのエンコード規則にしたがって変換する請求の範囲第８項記載の記録方法。

１１．上記方法は、上記入力されたデータをＭＰＥＧのエンコード規則

にしたがって上記入力されたデータを上記１セクタ単位のデータに変換しないと判別されたときには上記開始コードに続く２ビットに後続して乱数データを付加された１セクタ単位のデータに変換する請求の範囲第１０項記載の記録方法。

１２．上記方法は、ＭＰＥＧ－１のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第１０項記載の記録方法。

１３．上記方法は、ＭＰＥＧ－２のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第１０項記載の記録方法。

１４．上記方法は、上記変換されたデータの暗号化を行わない場合には上記開始コードに続く２ビットうちの少なくとも１ビットをデータが暗号化が行われていないことを示すように設定し、上記変換されたデータをエンコードして出力する請求の範囲第８項記載の記録方法。

１５．入力されたデータを開始コードと上記開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換する変換部と、

上記変換部によって変換されたデータを暗号化する場合には、上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定する設定部と、

上記設定部からの出力データに暗号化処理を施す暗号化処理部と、

上記暗号化処理部からの出力データに記録のためのエンコード処理を施すエンコード処理部と、

上記エンコード処理部からの出力データを記録媒体に記録する記録部とを備えている記録装置。

１６．上記変換部によって上記入力されたデータは、１セクタのデータ

が２０４８バイトのデータに変換され、上記暗号化処理部は上記変換部によって変換されたデータの暗号化を行う場合にはビット６４以降のデータを暗号化する請求の範囲第１５項記載の記録装置。

１７．上記装置は、更にＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換するか否かを判別する判別部を備え、上記判別部によって上記ＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換すると判別されたときには上記変換部は上記入力されたデータをＭＰＥＧのエンコード規則にしたがって変換する請求の範囲第１５項記載の記録装置。

１８．上記変換部は、上記判別部によって上記入力されたデータをＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換しないと判別されたときには上記開始コードに続く２ビットに後続して乱数データを付加された１セクタ単位のデータに変換する請求の範囲第１７項記載の記録装置。

１９．上記変換部は、ＭＰＥＧ－１のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第１７項記載の記録装置。

２０．上記変換部は、ＭＰＥＧ－２のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第１７項記載の記録装置。

２１．上記設定部は、上記変換されたデータの暗号化を行わない場合には上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化が行われていないことを示すように設定し、上記設定部からの出力データが上記エンコード処理部に供給される請求の範囲第１５項記載の記録装置。

２２．ユーザデータと開始コードと上記開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータが記録された記録媒体から読み出されたデータをデコードし、

上記デコードされたデータの上記開始コードに続く２ビットのうちの少なくとも１ビットを検出し、

上記検出した結果、上記デコードされたデータが暗号化されているときには暗号を解読し、

上記解読されたデータを１セクタ単位のデータから所定のデータ単位のデータに変換し出力する再生方法。

２３．上記方法は、上記解読されたデータの上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化が行われていないことを示すように設定した後に上記所定のデータ単位のデータに変換する請求の範囲第２２項記載の再生方法。

２４．上記方法は、上記デコードされたデータを上記開始コードと上記ユーザデータとの間のデータに基づいて上記ユーザデータの暗号を解く請求の範囲第２３項記載の再生方法。

２５．上記方法は、上記暗号が解読されたデータがいずれの変換規則によって変換されているかを判別し、上記暗号が解読されたデータがＭＰＥＧのエンコード規則に従って変換されていると判別されたときには上記暗号が解読されたデータをＭＰＥＧのエンコード規則にしたがった上記所定のデータ単位のデータに変換する請求の範囲第２２項記載の再生方法。

２６．上記方法は、ＭＰＥＧ－１のエンコード規則にしたがって上記入力されたデータを上記所定のデータ単位のデータに変換する請求の範囲第２５項記載の再生方法。

２７．上記方法は、ＭＰＥＧ－２のエンコード規則にしたがって上記入力されたデータを上記所定のデータ単位のデータに変換する請求の範囲第２５項記載の再生方法。

２８．上記方法は、上記検出した結果上記デコードされたデータが暗号化されていないときには上記デコードされたデータを上記所定のデータ単位のデータに変換する請求の範囲第２２項記載の再生方法。

２９．ユーザデータと開始コードと上記開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータが記録された記録媒体から読み出されたデータをデコードするデコーダと、

上記デコーダからの出力データの上記開始コードに続く２ビットのうちの少なくとも１ビットを検出する検出部と、

上記検出部による検出の結果、上記デコードされたデータが暗号化されているときには上記デコーダからの出力データの暗号を解読する解読部と、

上記解読部からの出力データを１セクタ単位のデータから所定のデータ単位のデータに変換して出力する変換部とを備えている再生装置。

３０．上記装置は、更に上記解読されたデータの上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化が行われていないことを示すように設定する設定部を備え、上記設定部からの出力データを上記変換部に供給する請求の範囲第２９項記載の再生装置。

３１．上記解読部は、上記デコードされたデータを上記開始コードと上記ユーザデータとの間のデータに基づいて上記ユーザデータの暗号を解く請求の範囲第３０項記載の再生装置。

３２．上記装置は、更に上記暗号が解読されたデータがいずれの変換規則によって変換されているかを判別する判別部を備え、上記判別部によ

って上記暗号が解読されたデータがＭＰＥＧのエンコード規則に従って変換されていると判別されたときには上記変換部によって上記暗号が解読されたデータをＭＰＥＧのエンコード規則にしたがった上記所定のデータ単位のデータに変換する請求の範囲第２９項記載の再生装置。

３３．上記変換部は、ＭＰＥＧ－１のエンコード規則にしたがって上記暗号が解読されたデータを上記所定のデータ単位のデータに変換する請求の範囲第３２項記載の再生装置。

３４．上記変換部は、ＭＰＥＧ－２のエンコード規則にしたがって上記暗号が解読されたデータを上記所定のデータ単位のデータに変換する請求の範囲第３２項記載の再生装置。

３５．上記装置は、上記検出部によって検出した結果上記デコードされたデータが暗号化されていないときには上記デコーダからの出力データを上記変換部に供給する請求の範囲第２９項記載の再生装置。

３６．入力されたデータを開始コードと上記開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータに変換し、

上記変換されたデータを暗号化する場合には、上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化されていることを示すように設定し、

上記変換されたデータを暗号化し、

上記暗号化されたデータに送信のためのエンコード処理を施して送信するデータ送信方法。

３７．上記１セクタのデータは２０４８バイトであり、上記方法は上記変換されたデータの暗号化を行う場合にはビット６４以降のデータを暗号化する請求の範囲第３６項記載のデータ送信方法。

３８．上記方法は、ＭＰＥＧのエンコード規則にしたがって上記入力さ

れたデータを上記１セクタ単位のデータに変換するか否かを判別し、上記ＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換すると判別されたときには上記入力されたデータをＭＰＥＧのエンコード規則にしたがって変換する請求の範囲第３６項記載のデータ送信方法。

３９．上記方法は、上記入力されたデータをＭＰＥＧのエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換しないと判別されたときには上記開始コードに続く２ビットに後続して乱数データを付加された１セクタ単位のデータに変換する請求の範囲第３８項記載のデータ送信方法。

４０．上記方法は、ＭＰＥＧ－１のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第３８項記載のデータ送信方法。

４１．上記方法は、ＭＰＥＧ－２のエンコード規則にしたがって上記入力されたデータを上記１セクタ単位のデータに変換する請求の範囲第３８項記載のデータ送信方法。

４２．上記方法は、上記変換されたデータの暗号化を行わない場合には上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化が行われていないことを示すように設定し、上記変換されたデータをエンコードして出力する請求の範囲第３６項記載のデータ送信方法。

４３．ユーザデータと開始コードと上記開始コードに続く２ビットのうちの少なくとも１ビットが暗号化制御を示すビットであるヘッダが先頭に付加された１セクタ単位のデータを受信し、

受信したデータをデコードし、

上記デコードされたデータの上記開始コードに続く２ビットのうちの少なくとも１ビットを検出し、

上記検出した結果、上記デコードされたデータが暗号化されているときには暗号を解読し、

上記解読されたデータを１セクタ単位のデータから所定のデータ単位のデータに変換し出力するデータ受信方法。

４４．上記方法は、上記解読されたデータの上記開始コードに続く２ビットのうちの少なくとも１ビットをデータが暗号化が行われていないことを示すように設定した後に上記所定のデータ単位のデータに変換する請求の範囲第４３項記載のデータ受信方法。

４５．上記方法は、上記デコードされたデータを上記開始コードと上記ユーザデータとの間のデータに基づいて上記ユーザデータの暗号を解く請求の範囲第４４項記載のデータ受信方法。

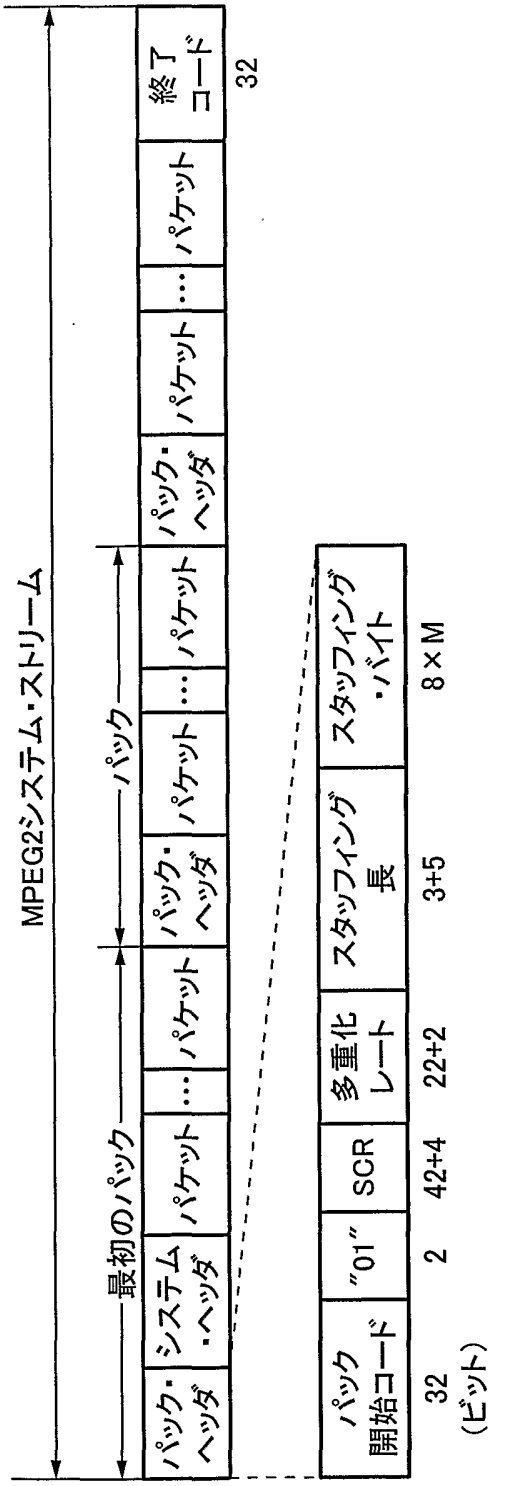
４６．上記方法は、上記暗号が解読されたデータがいずれの変換規則によって変換されているかを判別し、上記暗号が解読されたデータがＭＰＥＧのエンコード規則に従って変換されていると判別されたときには上記暗号が解読されたデータをＭＰＥＧのエンコード規則にしたがった上記所定のデータ単位のデータに変換する請求の範囲第４３項記載のデータ受信方法。

４７．上記方法は、ＭＰＥＧ－１のエンコード規則にしたがって上記暗号が解読されたデータを上記所定のデータ単位のデータに変換する請求の範囲第４６項記載のデータ受信方法。

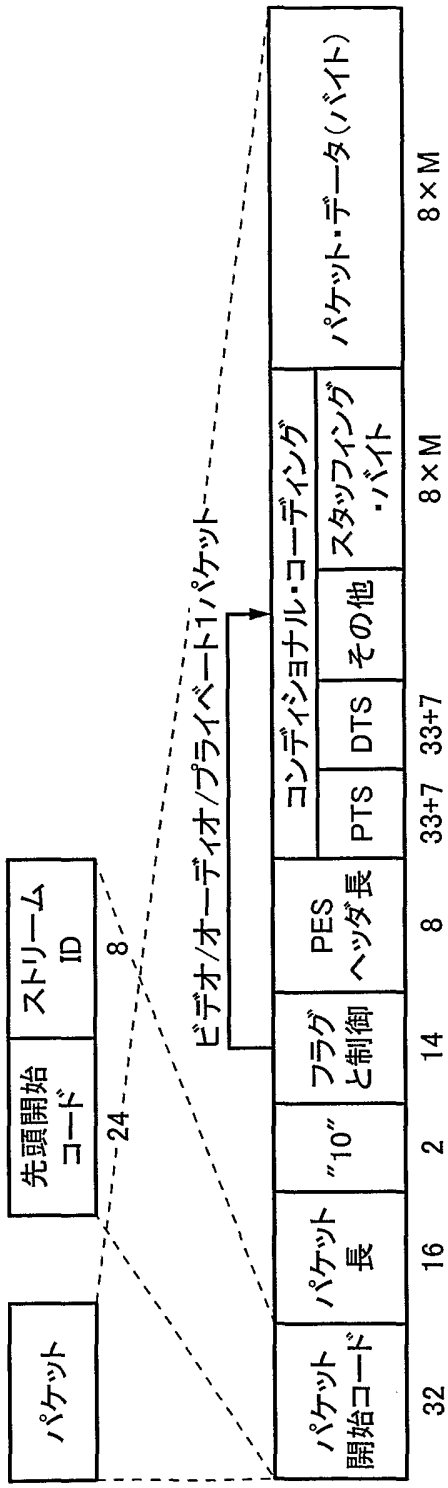
４８．上記方法は、ＭＰＥＧ－２のエンコード規則にしたがって上記暗号が解読されたデータを上記所定のデータ単位のデータに変換する請求の範囲第４６項記載のデータ受信方法。

４９．上記方法は、上記検出した結果上記デコードされたデータが暗号化されていないときには上記デコードされたデータを上記所定のデータ単位のデータに変換する請求の範囲第４３項記載のデータ受信方法。

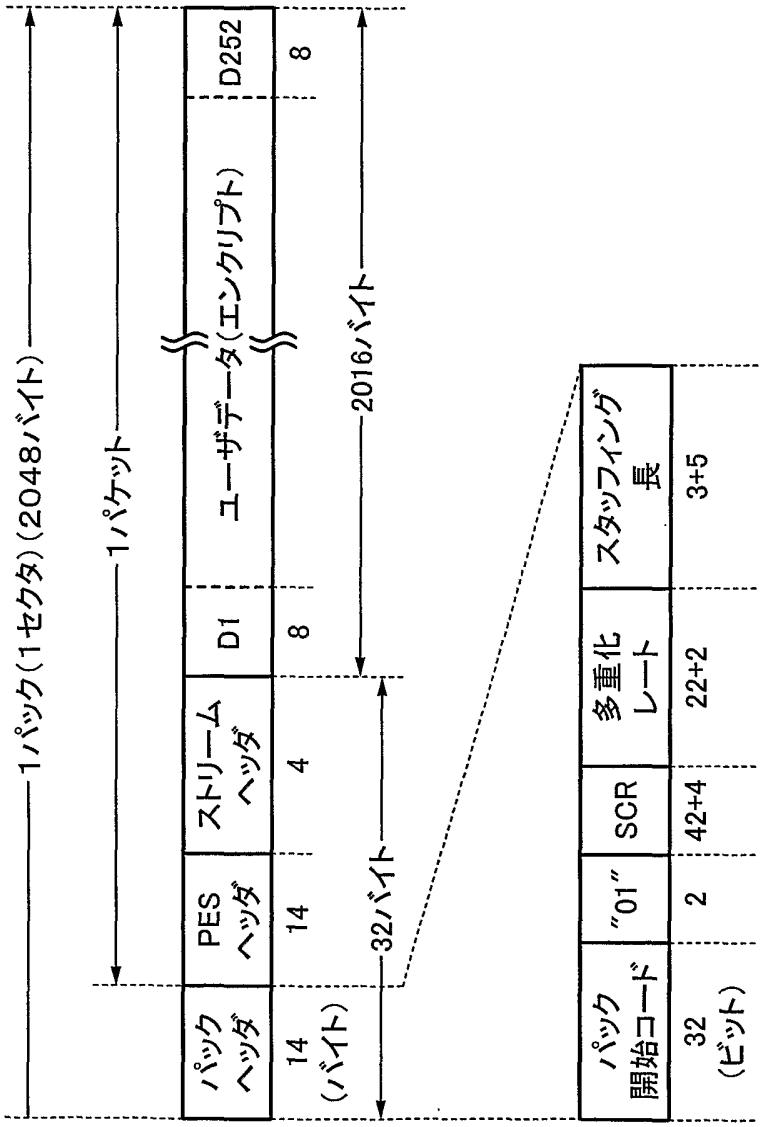
第1図A

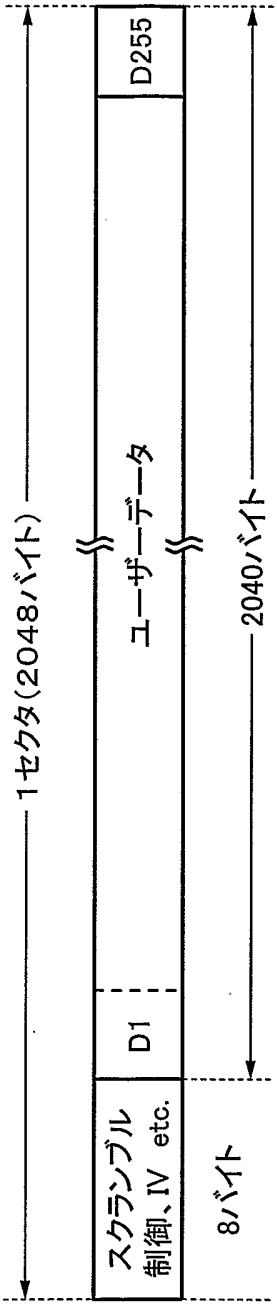

MPEG2システム・ストリーム
最初のパック
パック
パック・ヘッダ
システム・ヘッダ
パケット
…
パック・ヘッダ
パケット
…
パケット
終了コード
32
パック開始コード
"01"
SCR
多重化レート
スタッフィング長
スタッフィング・バイト
32
2
42+4
22+2
3+5
8×M
(ビット)

第1図B

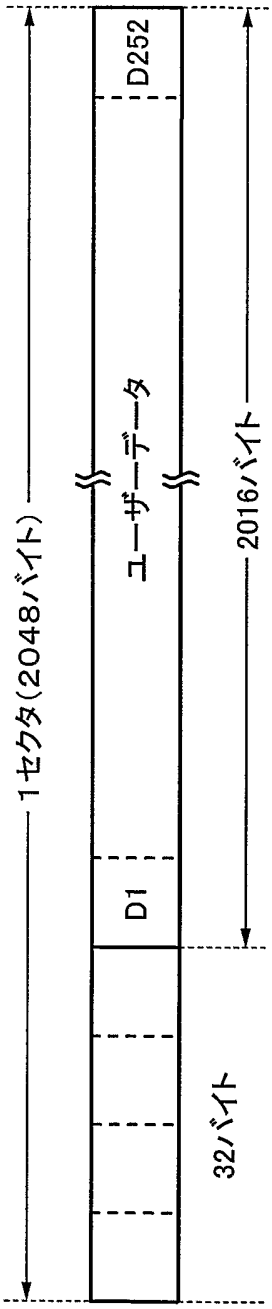

パケット
先頭開始コード
ストリーム ID
24
8
ビデオ/オーディオ/プライベート1パケット
パケット開始コード
パケット長
"10"
フラグと制御
PES ヘッダ長
コンディショナル・コーディング
PTS
DTS
その他
スタッフィング・バイト
パケット・データ(バイト)
32
16
2
14
8
33+7
33+7
8×M
8×M
(ビット)

第２図

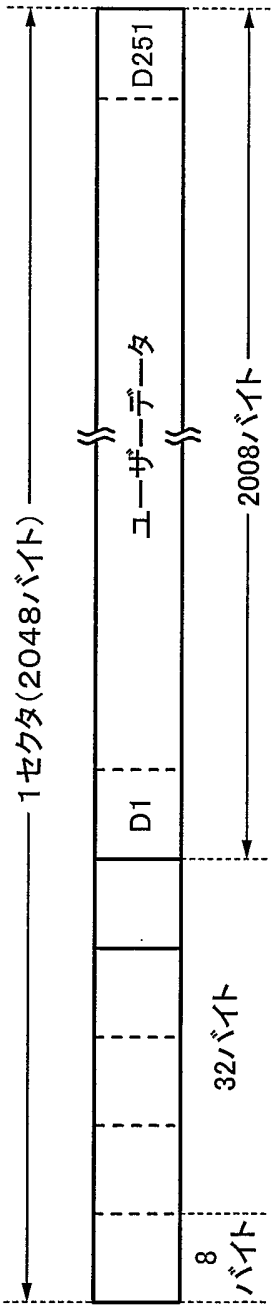

1パック(1セクタ)(2048バイト)
1パケット
パック ヘッダ
PES ヘッダ
ストリーム ヘッダ
D1
ユーザデータ(エンクリプト)
D252
14 (バイト)
14
4
8
8
32バイト
2016バイト
パック 開始コード
"01"
SCR
多重化 レート
スタッフィング 長
32 (ビット)
2
42+4
22+2
3+5



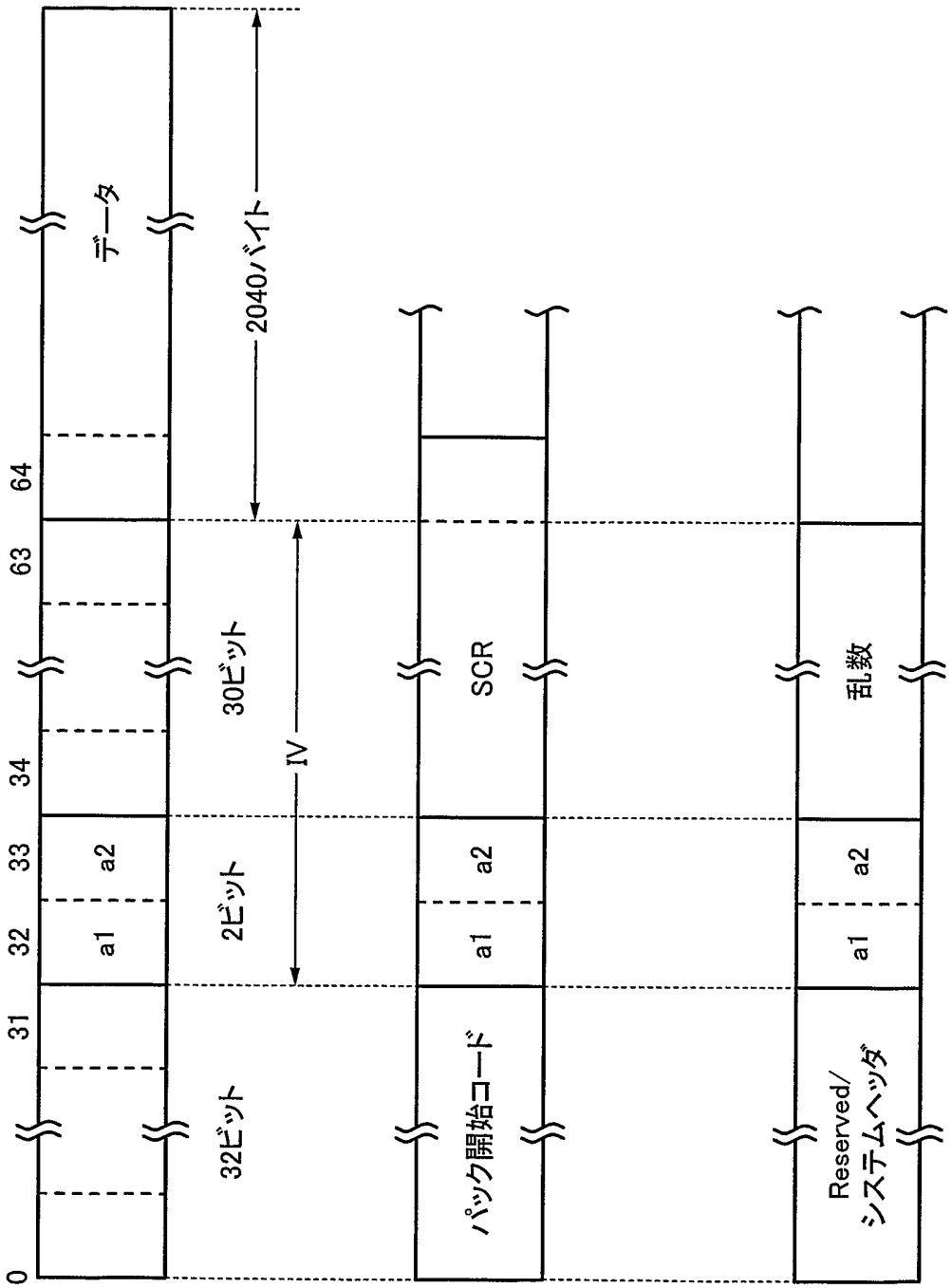
第3図A



第3図B



第3図C



第４図Ａ

第４図Ｂ

第４図Ｃ

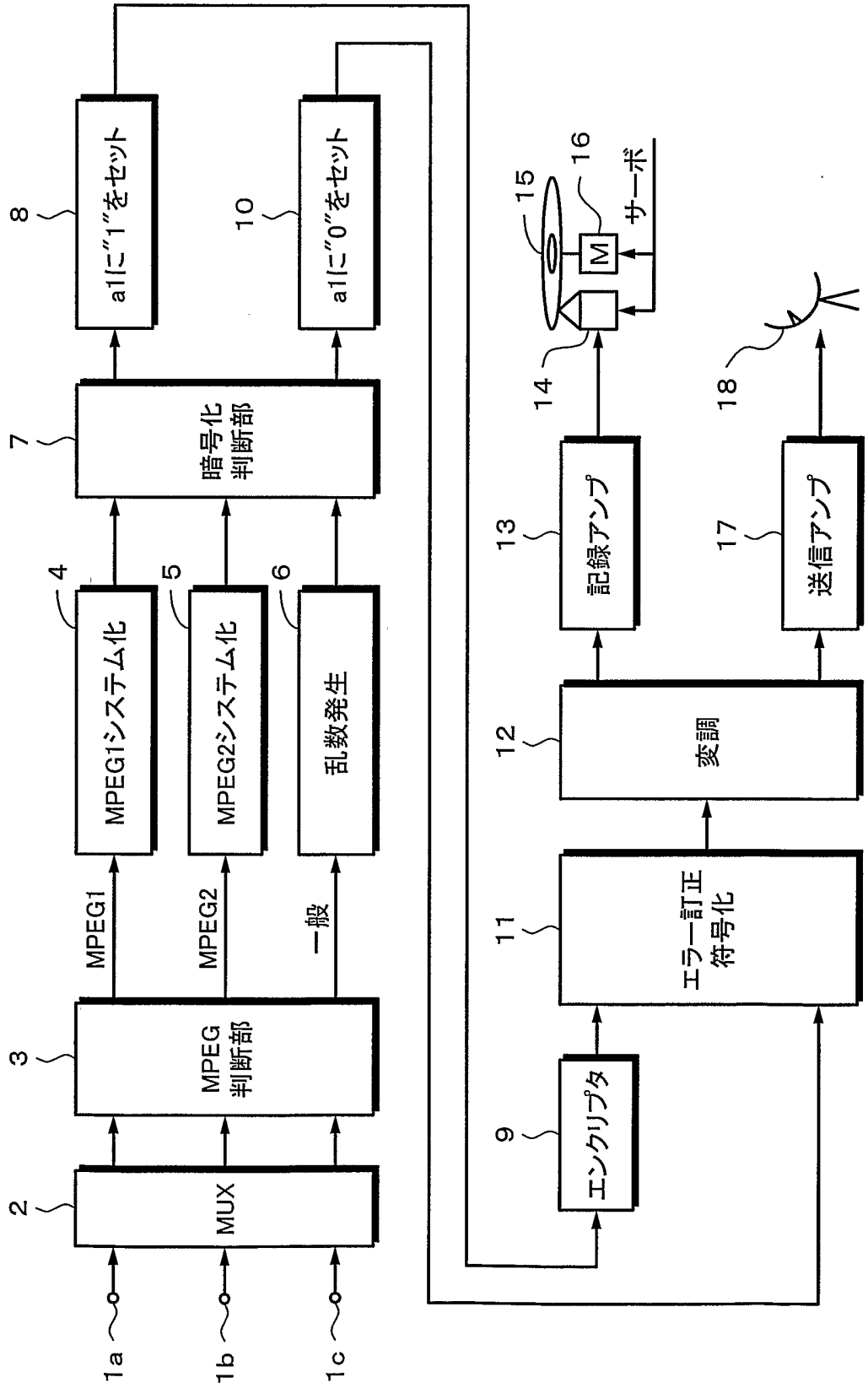
第５図Ａ

	a1	a2	定義
MPEG1	0	0	エンクリプションなし
	1	0	エンクリプションあり
MPEG2	0	1	エンクリプションなし
	1	1	エンクリプションあり

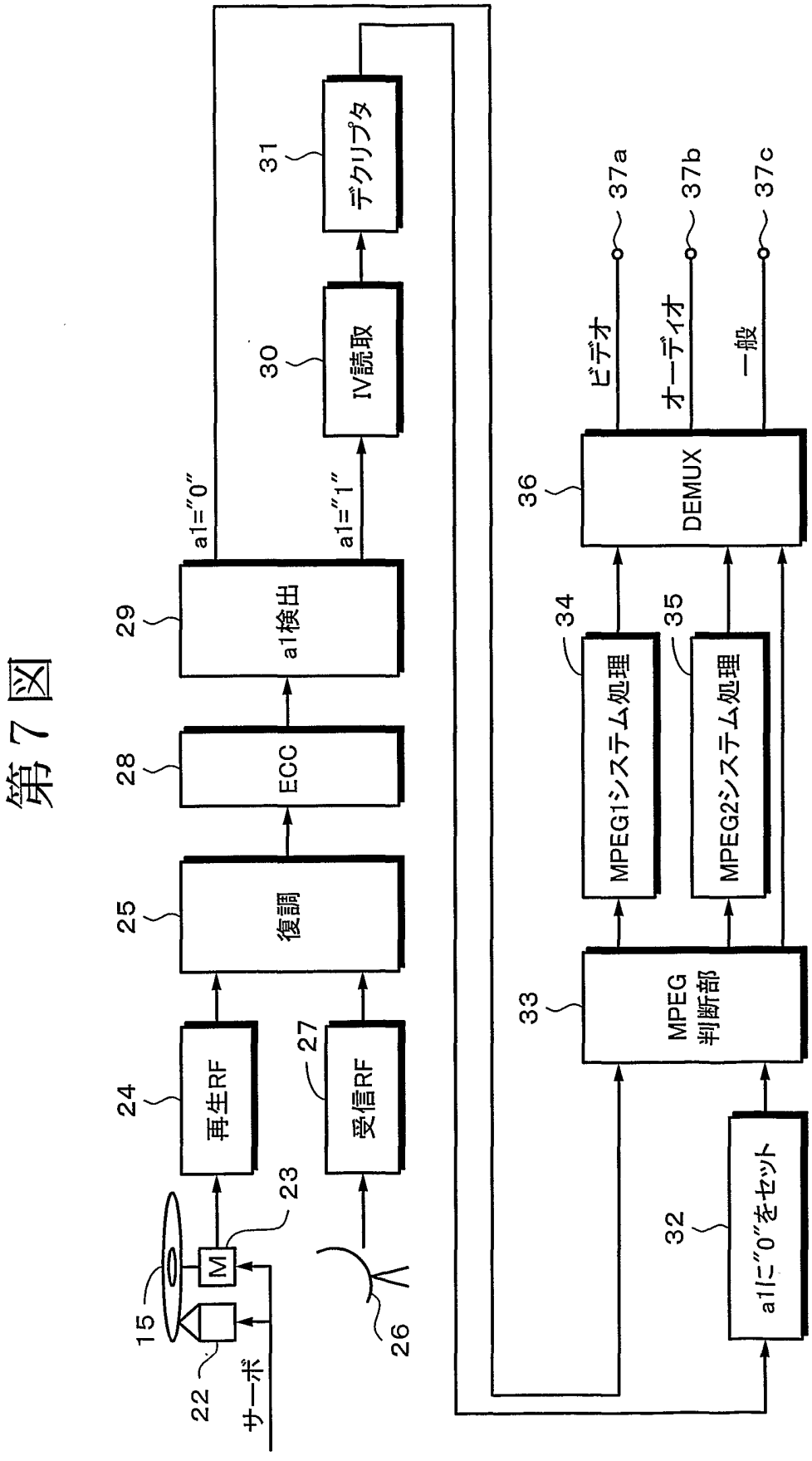
第５図Ｂ

a1	a2	定義
0	0	Reserved
0	1	エンクリプションなし
1	0	エンクリプション2
1	1	エンクリプション1

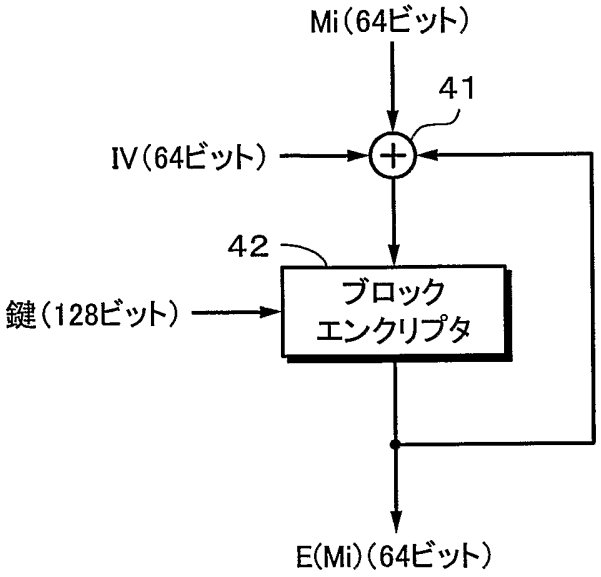
第６図


1a
1b
1c
2
MUX
3
MPEG
判断部
MPEG1
MPEG2
一般
4
MPEG1システム化
5
MPEG2システム化
6
乱数発生
7
暗号化
判断部
8
a1に"1"をセット
10
a1に"0"をセット
9
エンクリプタ
11
エラー訂正
符号化
12
変調
13
記録アンプ
14
15
16
M
サーボ
17
送信アンプ
18

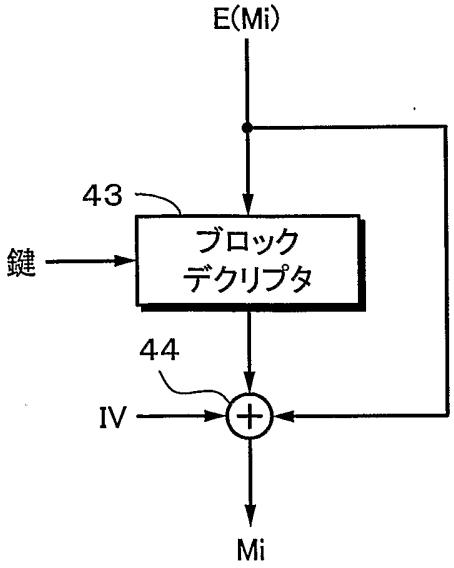
第７図


15
22
サーボ
M
23
24
再生RF
25
復調
26
27
受信RF
28
ECC
29
a1検出
a1="0"
a1="1"
30
IV読取
31
デクリプタ
32
a1に"0"をセット
33
MPEG
判断部
34
MPEG1システム処理
35
MPEG2システム処理
36
DEMUX
ビデオ
37a
オーディオ
37b
一般
37c

第８図


Mi(64ビット)
41
IV(64ビット)
42
ブロック
エンクリプタ
鍵(128ビット)
E(Mi)(64ビット)

第９図


E(Mi)
43
ブロック
デクリプタ
鍵
44
IV
Mi

符号の説明

ａ１，ａ２	暗号化制御のためのビット
7	暗号化判断部
８，１０，３２	ビット設定回路
9	エンクリプタ
１４，２３	光ピックアップ
１５	光ディスク
１１，１３	エンクリプタ
３０	ＩＶ読取部
３１	デクリプタ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/09609

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B20/10, G11B27/00, H04N5/76

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B20/10, G11B27/00, H04N5/76

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	JP 2002-042424 A (Toyo Communication Equipment Co., Ltd.), 08 February, 2002 (08.02.02), All pages; all drawings (Family: none)	1,3,5-8,10, 12-15,17, 19-22,28,29, 35,36,38, 40-43,49
P,A		2,4,9,11,16, 18,23-27, 30-34,37,39, 44-48
A	JP 2000-231758 A (Toshiba Corp.), 22 August, 2000 (22.08.00), Columns 74 to 81; Figs. 8 to 9 (Family: none)	1-49

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 29 November, 2002 (29.11.02)	Date of mailing of the international search report 17 December, 2002 (17.12.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/09609

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-293936 A (Hitachi, Ltd.), 20 October, 2000 (20.10.00), Columns 19 to 20; Figs. 3 to 4 (Family: none)	1-49

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０９６０９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷　Ｇ１１Ｂ２０／１０，
Ｇ１１Ｂ２７／００，
Ｈ０４Ｎ　５／７６

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷　Ｇ１１Ｂ２０／１０，
Ｇ１１Ｂ２７／００，
Ｈ０４Ｎ　５／７６

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　１９２２－１９９６年
日本国公開実用新案公報　１９７１－２００２年
日本国登録実用新案公報　１９９４－２００２年
日本国実用新案登録公報　１９９６－２００２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
ＰＸ	ＪＰ　２００２－０４２４２４　Ａ（東洋通信機株式会社） ２００２．０２．０８　全頁，全図（ファミリーなし）	1, 3, 5-8, 10, 12-15, 17, 19-22, 28, 29, 35, 36, 38, 40-43, 49
ＰＡ		2, 4, 9, 11, 16, 18, 23-27, 30-34, 37, 39, 44-48

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２９．１１．０２	17.12.02

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｑ	４２３２
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	齋藤　哲　印		
	電話番号　０３－３５８１－１１０１　内線　３５９０		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２０００－２３１７５８　Ａ（株式会社東芝） ２０００．０８．２２　第７４－８１欄，第８－９図 （ファミリーなし）	1-49
Ａ	ＪＰ　２０００－２９３９３６　Ａ（株式会社日立製作所） ２０００．１０．２０　第１９－２０欄，第３－４図 （ファミリーなし）	1-49