(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3584913号
(P3584913)
(45)発行日　平成16年11月4日(2004.11.4)　(24)登録日　平成16年8月13日(2004.8.13)

(51)Int.Cl.[7]	F I
G11B 20/12	G11B 20/12
G11B 20/10	G11B 20/10 H
H04N 5/92	G11B 20/10 311
	G11B 20/10 321Z
	H04N 5/92 H

請求項の数 49　(全 19 頁)

(21)出願番号　特願2001-289982(P2001-289982)
(22)出願日　平成13年9月21日(2001.9.21)
(65)公開番号　特開2003-100019(P2003-100019A)
(43)公開日　平成15年4月4日(2003.4.4)
審査請求日　平成15年3月4日(2003.3.4)

(73)特許権者　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　100082762
弁理士　杉浦　正知
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　齋藤　哲

最終頁に続く

(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)【特許請求の範囲】
【請求項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。
【請求項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項１に記載のデータ出力方法。
【請求項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項１に記載のデータ出力方法。
【請求項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項３に記載のデータ出力方法。

【請求項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項３に記載のデータ出力方法。

【請求項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項３に記載のデータ出力方法。

【請求項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項１に記載のデータ出力方法。

【請求項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。

【請求項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項８に記載の記録方法。

【請求項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項８に記載の記録方法。

【請求項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項１０に記載の記録方法。

【請求項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項１０に記載の記録方法。

【請求項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項１０に記載の記録方法。

【請求項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項８に記載の記録方法。

【請求項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。

【請求項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項１５に記載の記録装置。

【請求項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項１５に記載の記録装置。

【請求項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項１７に記載の記録装置。

【請求項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項１７に記載の記録装置。

【請求項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項１７に記載の記録装置。

【請求項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項１５に記載の記録装置。

【請求項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。

【請求項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項２２に記載の再生方法。

【請求項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項２３に記載の再生方法。
【請求項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項２２に記載の再生方法。
【請求項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項２５に記載の再生方法。
【請求項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項２５に記載の再生方法。
【請求項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項２２に記載の再生方法。
【請求項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。
【請求項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項２９に記載の再生装置。
【請求項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項３０に記載の再生装置。
【請求項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項２９に記載の再生装置。
【請求項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項３２に記載の再生装置。
【請求項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項３２に記載の再生装置。
【請求項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項２９に記載

の再生装置。
【請求項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。
【請求項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項３６に記載のデータ送信方法。
【請求項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項３６に記載のデータ送信方法。
【請求項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項３８に記載のデータ送信方法。
【請求項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項３８に記載のデータ送信方法。
【請求項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項３８に記載のデータ送信方法。
【請求項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項３６に記載のデータ送信方法。
【請求項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。
【請求項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項４３に記載のデータ受信方法。
【請求項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項４４に記載のデータ受信方法。
【請求項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項４３に記載のデータ受信方法。
【請求項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項４６に記載のデータ受信方法。
【請求項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項４６に記載のデータ受信方法。
【請求項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項４３に記載のデータ受信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
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。
【０００２】
【従来の技術】
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することがなされる。セクタ単位で暗号化する、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。また、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。
【０００３】
マルチメディアコンテンツ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。図１Ａ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。
【０００４】
図１Ａ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）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。
【０００５】

図１Ｂ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）からなる。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）が続いている。

【０００６】

図２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。図２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）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。このような図２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。

【０００７】

パックヘッダは、図１Ａ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）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。

【０００８】

ＰＥＳヘッダは、図１Ｂ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。

【０００９】

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 Ｔｒａｎｓｆｅｒ 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。

【００１０】

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。

【００１１】

また、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。

【００１２】

図３Ａ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。

【００１３】

【発明が解決しようとする課題】

上述したＭＰＥＧ２システムのデータフォーマットと、図３Ａ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。また、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。

【００１４】

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。また、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。

【００１５】

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。図３Ｂ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、図２Ａ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。

【００１６】

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、図３Ｃ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バイトのヘッダを付加するようになされる。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。

【００１７】
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。

【００１８】
【課題を解決するための手段】
上述した課題を解決するために、請求項１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。

【００１９】
請求項８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。

【００２０】
請求項１５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。

【００２１】
請求項２２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。

【００２２】
請求項２９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。

【００２３】
請求項３６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。

【００２４】

請求項４３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。

【００３０】

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。

【００３１】

【発明の実施の形態】

以下、この発明の一実施形態について説明する。最初に、図４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。図４Ａ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に使用する。この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。

【００３２】

図４Ｂ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、図２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、図２の場合と同様に、２０１６バイトである。

【００３３】

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。

【００３４】

図４Ｃ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、図３Ａに示すデータ構成と同様に、２０４０バイトとなる。

【００３５】

図５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。図５Ａ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。

【００３６】

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、”ａ１ａ２”　＝”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。

【００３７】

図５Ｂ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、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。

【００３８】

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を復号するのに使用され、鍵Ｋｂが試聴用のコンテンツを復号するのに使用される。鍵Ｋａから鍵Ｋｂは、ハッシュ演算で作成できるが、鍵Ｋｂからは、ハッシュ関数が一方向性のために、鍵Ｋａを作成できない。

【００３９】

さらに、図５Ｂ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、復号を行うと、”ａ１　ａ２”を”００”に書き換え、ＭＰＥＧ２システムでは、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。

【００４０】

図６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。図６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。

【００４１】

入力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、使用するシステムが決定される。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。

【００４２】

ＭＰＥＧ１システムを使用する場合では、ＭＰＥＧ１システム化部４に多重化データが供給される。ＭＰＥＧ２システムを使用する場合では、ＭＰＥＧ２システム化部５に多重化データが供給される。一般アプリケーションを使用する場合では、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、図４Ｃ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する。

【００４３】

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、図２および図４Ｂを参照して上述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、図４Ｂ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。

【００４４】

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、暗号化を行うか否かを制御する。暗号化方法が複数用意されている場合は、暗号化の種類を制御する。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制御する。

【００４５】

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。このデータがエンクリプタ９に供給され、暗号化される。ビット６４以降のデータが暗号化される。この暗号化は、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。図５Ａに示すように、ａ１＝”１” 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。暗号化を行なわない場合は、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。

【００４６】

エンクリプタ９の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、エラー訂正符号の符号化がなされる。エラー訂正符号化回路１１の出力が変調回路１２に供給される。

【００４７】

記録装置の場合では、変調回路１２からの変調出力が記録アンプ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、例えばＣＤ－ＲＷまたはＣＤ－Ｒ等の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、光ピックアップ１４のトラッキングおよびフォーカシング、並びにスピンドルモータ１６の回転制御のためにサーボ回路（図示しない）が設けられている。

【００４８】

この一実施形態の光ディスク１５は、記録に必要とされる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再生可能な相変化型ディスクである。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

ら見て手前側がランドであり、遠い側がグルーブ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、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追記形ディスクに対しても適用できる。

【００４９】

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。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、グルーブのウォブル情報としてアドレス情報としての絶対時間情報を連続的に記録している。ＣＤ－Ｒディスク、ＣＤ－ＲＷディスクでは、グルーブのウォブル情報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上の所望の書き込み位置を検索し、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、データをディスクに書き込むようにしている。

【００５０】

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、アドレス情報、クロック情報等を有するウォブリング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、ディスク原盤から電鋳処理によってスタンパが作成され、スタンパを用いて射出成形を行うことによって、上述したウォブル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が作成される。

【００５１】

なお、図６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、図４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記録され、または送信される。

【００５２】

送信装置の場合では、変調回路１２の出力が送信アンプ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から衛星に対して放送信号が送出される。また、放送ではなく、無線通信を行う場合、インターネットを介して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。

【００５３】

図７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ドライブ（ＣＤ－ＲＯＭドライブ、ＣＤ－Ｒドライブ、ＣＤ－ＲＷドライブ等）と、アプリケーションソフトウェアとによって構成される。全てハードウエアの構成とすることも可能である。

【００５４】

図７において、参照符号２１で示す光ディスクは、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２１からデータが読み出される。光ディスク２１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。検出された信号が再生ＲＦ処理部２４に供給される。

【００５５】

再生ＲＦ処理部２４では、マトリックスアンプがフォトディテクタの検出信号を演算することによって、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。ウォブリンググルーブの情報としてクロックおよびアドレスが記録されている場合では、ウォブル信号が再生ＲＦ処理部２４から出力される。ＲＦ信号が復調部２５に供給され、例えばＥＦＭ復調がなされる。

【００５６】

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、エラー訂正処理がなされる。ドライブの場合では、エラー訂正回路２８までのハードウエア構成を有し、その後の処理がソフトウェアによってなされる。

【００５７】

図示しないサーボ回路に対して、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、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が制御される。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、スレッドサーボを行う。

【００５８】

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。ａ１＝”１” であれば、再生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。図４に示したように、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。

【００５９】

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にて暗号化が復号される。デクリプタ３１の復号出力がビット設定回路３２に供給される。ビット設定回路３２では、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。ビットａ１が”０” に設定された再生データが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” の場合では、暗号化されていない再生データがＭＰＥＧ判断部３３に供給される。

【００６０】

ＭＰＥＧ判断部３３は、再生データが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。再生データが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。。再生データが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得られる。

【００６１】

ＭＰＥＧ判断部３３において、一般アプリケーションのものと判断された再生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に対して、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。

【００６２】

図８は、ＣＢＣモードによるエンクリプタ９（図６参照）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、ＤＥＳＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、ＡＥＳ、トリプルＤＥＳ等のエンクリプタである。

【００６３】

ブロックエンクリプタ４２に対して鍵（１２８ビット）が供給され、加算器４１の出力が鍵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。

【００６４】

図９は、エンクリプタ９に対応するデクリプタ３１（図７参照）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。

【００６５】

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、図６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。

【００６６】

【発明の効果】

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。

【００６７】

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。

【図面の簡単な説明】

【図１】この発明を適用できるＭＰＥＧ２システムのデータ構成を説明する略線図である。

【図２】ＭＰＥＧ２システムのデータ構成の一例を示す略線図である。

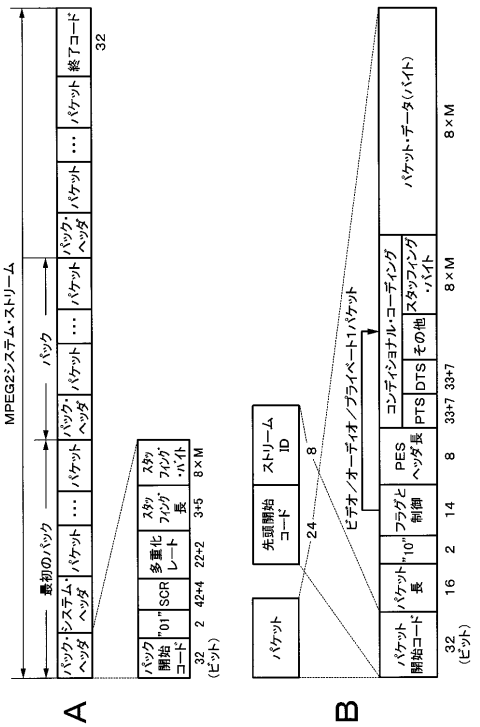
【図３】一般的アプリケーションにおけるデータフォーマットとＭＰＥＧ２システムのデータフォーマットとの融合方法の例を説明するための略線図である。

【図４】この発明の一実施形態におけるデータ構成を説明するための略線図である。

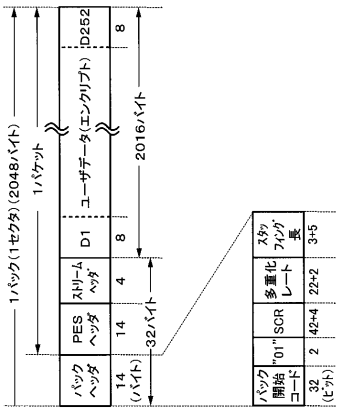
【図５】この発明の一実施形態における暗号化制御ビットの定義の一例および他の例を示す略線図である。

【図６】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る。
【図７】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る。
【図８】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る。
【図９】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。
【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、１５，２１・・・光ディスク、別部、１１，１３・・・エンクリプタ、３０・・・ＩＶ読取部、３１・・・デクリプタ

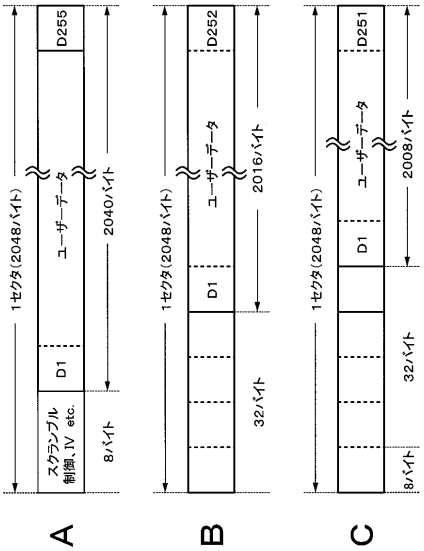
【図１】



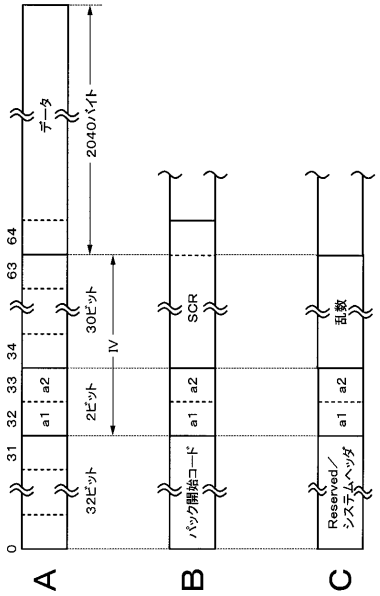
【図２】



【図３】



【図４】



【図５】

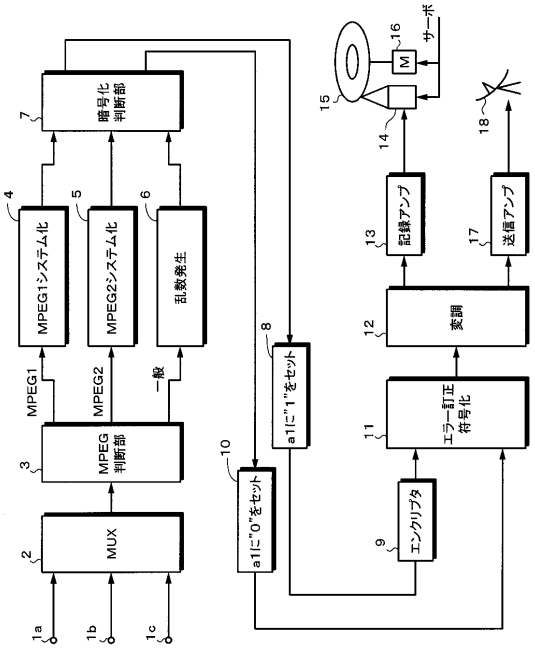
A

	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

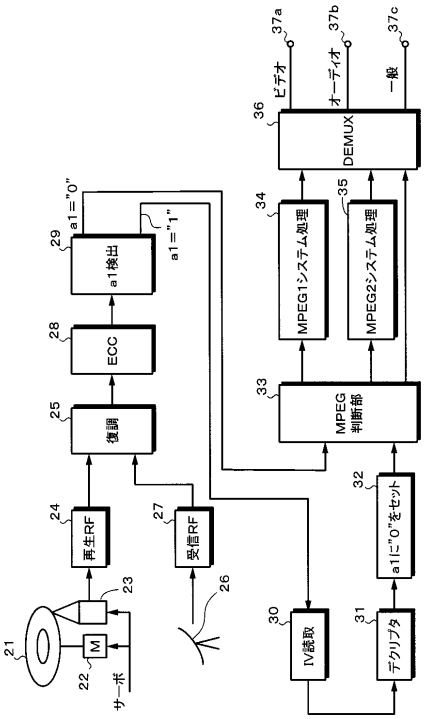
B

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

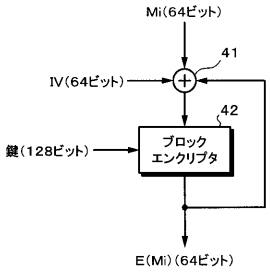
【図６】



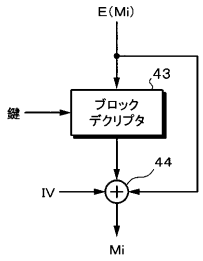
【図７】


37a
37b
37c
ビデオ
オーディオ
一般
36
DEMUX
34
35
MPEG1システム処理
MPEG2システム処理
33
MPEG
判断部
29
a1検出
a1="0"
a1="1"
28
ECC
25
復調
24
再生RF
27
受信RF
32
a1に"0"をセット
30
IV読取
31
デクリプタ
21
22
M
サーボ
23
26

【図８】


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

【図９】


E(Mi)
43
鍵
ブロック
デクリプタ
44
IV
Mi

フロントページの続き

(56)参考文献 特開２００２－０４２４２４（ＪＰ，Ａ）
特開２００３－１９９０６４（ＪＰ，Ａ）
特開２０００－２９３９３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G11B 20/10
H04N 5/92