

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3823634号

(P3823634)

(45) 発行日 平成18年9月20日(2006.9.20)

(24) 登録日 平成18年7月7日(2006.7.7)

(51) Int. Cl.			F I		
G 1 1 B	20/10	(2006.01)	G 1 1 B	20/10	H
G 0 6 F	12/14	(2006.01)	G 0 6 F	12/14	3 2 0 B
G 0 9 C	1/00	(2006.01)	G 0 9 C	1/00	6 6 0 G
H 0 4 L	9/08	(2006.01)	H 0 4 L	9/00	6 0 1 C
H 0 4 L	9/32	(2006.01)	H 0 4 L	9/00	6 7 3 B

請求項の数 4 (全 10 頁)

(21) 出願番号	特願平11-267618	(73) 特許権者	000004329
(22) 出願日	平成11年9月21日(1999.9.21)		日本ビクター株式会社
(65) 公開番号	特開2000-228061(P2000-228061A)		神奈川県横浜市神奈川区守屋町3丁目12番地
(43) 公開日	平成12年8月15日(2000.8.15)	(74) 代理人	100083806
審査請求日	平成14年4月26日(2002.4.26)		弁理士 三好 秀和
(31) 優先権主張番号	特願平10-345938	(74) 代理人	100100712
(32) 優先日	平成10年12月4日(1998.12.4)		弁理士 岩▲崎▼ 幸邦
(33) 優先権主張国	日本国(JP)	(74) 代理人	100100929
			弁理士 川又 澄雄
		(74) 代理人	100108707
			弁理士 中村 友之
		(74) 代理人	100095500
			弁理士 伊藤 正和

最終頁に続く

(54) 【発明の名称】 エンコード装置、デコード装置及び通信方法

(57) 【特許請求の範囲】

【請求項1】

コンテンツデータをエンコードするためのエンコード装置であって、少なくとも信号圧縮手段と、識別信号生成手段と、フォーマット手段と、スクランブル手段と、を有し、

前記信号圧縮手段が、前記コンテンツデータを圧縮し、

前記識別信号生成手段が、前記コンテンツデータに共通する共通管理情報と、各コンテンツデータ別の個別管理情報とを生成し、

前記フォーマット手段が、前記共通管理情報を共通ヘッダエリアに、前記した各個別管理情報を各コンテンツヘッダエリアに、前記各コンテンツデータを各コンテンツデータエリアにそれぞれ記録し、

前記スクランブル手段が、前記コンテンツデータエリアに記録される各コンテンツデータを所定の共通鍵であって本エンコード装置と受信手段で共通で使用され、さらに前記受信手段から他の受信手段に前記各コンテンツデータが送信された場合に、受信手段間で共通で使用される共通鍵を使用してスクランブルし、

前記コンテンツデータを受信する受信手段から受け取った前記受信手段に固有の受信手段識別コードを前記共通ヘッダエリアに記録し、

前記共通鍵を前記コンテンツデータを受信する受信手段から受け取った前記受信手段に固有の受信手段識別コード又はメモリカード識別コードを用いて暗号化して前記共通ヘッダエリアに記録する、

ことを特徴とするエンコード装置。

【請求項 2】

請求項 1 に記載のエンコード装置でエンコードされたコンテンツデータをデコードするためのデコード装置であって、

前記エンコード装置で生成された共通ヘッダエリアに記録されている暗号化された共通鍵を前記デコード装置に関する受信手段識別コード又はメモリカード識別コードを用いて復号し、前記復号した鍵を用いて前記コンテンツデータをデスクランブルする手段を、

有するデコード装置。

【請求項 3】

請求項 1 に記載のエンコード装置でエンコードされたコンテンツデータを伝送路を介して前記受信手段に送信することを特徴とするコンテンツデータ用の通信方法。

10

【請求項 4】

請求項 1 に記載のエンコード装置でエンコードされたコンテンツデータを伝送路を介して前記受信手段が受信することを特徴とするコンテンツデータ用の通信方法。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、コンテンツデータを記録した記録媒体に関し、特に送信先によって異なる鍵によりスクランブル化されたコンテンツデータを記録した記録媒体に関する。

【0002】**【従来の技術】**

20

近年、流通の対象となる情報のデジタル化が進んでいる。流通対象となるデジタルデータをデジタルコンテンツという。デジタルコンテンツの代表例は、音楽データであるが、静止画データ、動画データ、文献データ、ゲームのプログラム、アプリケーションソフトウェア等も含まれる。

【0003】**【発明が解決しようとする課題】**

デジタルデータは正確かつ迅速なコピーが容易に行えるため、不法コピー防止の必要性が高い。また、多量かつ種々のデータが流通の対象となるに従い、迅速なデータ転送及び迅速な再生の必要性が高まってきている。

【0004】

30

【課題を解決するための手段】

上記目的を達成するために、請求項 1 の発明は、複数のコンテンツデータに共通する管理情報を記録する共通ヘッダエリアと、前記複数のコンテンツデータを記録するコンテンツエリアとを有し、前記コンテンツエリアは、各コンテンツデータ別の管理情報を記録するコンテンツヘッダエリアと、前記コンテンツデータを記録するコンテンツデータエリアから構成され、各コンテンツに固有のコンテンツ識別コードが前記コンテンツヘッダエリアに記録され、前記コンテンツデータエリアに記録される各コンテンツデータが所定の鍵を用いて暗号化されていることを特徴とするコンテンツデータを記録した記録媒体である。

【0005】

各コンテンツデータは、そのコンテンツデータを受信する受信手段に固有の暗号鍵により暗号化されている。コンテンツデータを送信する側は、受信手段から受信手段識別コード又はメモリカード識別コードを受け取り、その受信手段識別コード又はメモリカード識別コードを使用して前記暗号鍵を暗号化（スクランブル化）し、このようにスクランブル化した暗号鍵と前記コンテンツデータを送信する。

40

【0006】

つまり、受信手段が異なれば、受信する端末 ID 又は内部のメモリカード ID が異なるため、スクランブル化後の暗号鍵（暗号再生鍵）も異なる。このため、ある受信手段の識別コード又はメモリカード識別コードを用いてスクランブル化された暗号鍵は、他の受信手段ではデスクランブルできない。これにより、コンテンツデータの不法なコピーを防止することができる。

50

【0007】

また、前記コンテンツデータを圧縮し、前記コンテンツヘッダエリアに該圧縮の方式を記録することが好ましい。コンテンツデータの種別に依りて圧縮効率が最も高くなる圧縮方式を選択し、その圧縮方式の識別情報を各コンテンツヘッダエリアに記録することにより、選択した圧縮方式に対応した伸長が可能となる。

【0008】

さらに、前記共通ヘッダエリアおよび/または前記各コンテンツヘッダエリア毎に各コンテンツデータのTOCおよび/または使用エリアを記録することが好ましい。TOCを記録することにより、各コンテンツの素早い頭出しが可能となる。

【0009】

また、請求項6の発明は、コンテンツデータをエンコードするためのエンコード装置であって、少なくとも信号圧縮手段と、識別信号生成手段と、フォーマット手段と、スクランブル手段と、を有し、前記信号圧縮手段が、前記コンテンツデータを圧縮し、前記識別信号生成手段が、前記コンテンツデータに共通する共通管理情報と、各コンテンツデータ別の個別管理情報とを生成し、前記フォーマット手段が、共通管理情報を共通ヘッダエリアに、各個別管理情報を各コンテンツヘッダエリアに、前記各コンテンツデータを各コンテンツデータエリアにそれぞれ記録し、前記スクランブル手段が、所定の鍵により前記コンテンツデータをスクランブルすることを特徴とする。

【0010】

また、請求項7の発明は、請求項6に記載のエンコード装置でエンコードされたコンテンツデータをデコードするためのデコード装置であって、少なくともデスクランブル手段と、デフォーマット手段と、信号伸長手段と、を有し、前記デスクランブル手段が、前記所定の鍵を用いて前記コンテンツデータをデスクランブルし、前記デフォーマット手段が、デスクランブルされたコンテンツデータを共通管理情報から分離し、前記信号伸長手段が、分離されたコンテンツデータを伸長することを特徴とする。

【0011】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態を説明をする。図1(a)及び(b)は、本発明のデータ構造を有するデータの送受信を行うシステム全体を概念的に示すブロック図である。この実施の形態のシステムは、ユーザ携帯端末(送信側)40、販売店設置端末41、課金センター42、コンテンツセンター43、通信回線44、通信衛星45、ユーザ携帯端末(受信側)46により構成される。

【0012】

各携帯端末40、46は、それぞれ固有の識別コード(以下、プレイヤーIDとする。)を有する。また、各コンテンツもそれぞれ固有の識別コード(以下、コンテンツIDとする。)を有する。携帯端末40は、販売店設置端末41にコンテンツデータの送信を要求する。その際、携帯端末40は、コンテンツIDとプレイヤーIDを送信する。

【0013】

各販売店設置端末41も、それぞれ固有の識別コード(以下、事業者IDとする。)を有する。コンテンツデータの送信を要求された設置端末41は、携帯端末40からコンテンツデータの送信要求があった旨を課金センター42及びコンテンツセンター43へ通知する。

【0014】

課金センター42へコンテンツID、プレイヤーID及び事業者IDが通知される。課金センター42は、予め作成してある料金表を参照してコンテンツIDに対応するコンテンツデータ料の送付要求を通信回線44、設置端末41を経由して携帯端末40に送る。

【0015】

コンテンツデータ料の送付を要求された携帯端末40は、コンテンツ料として電子マネーを設置端末41、通信回線44を経由して課金センター42へ送る。電子マネーとしては、ICチップに貨幣金額を記憶しておきICカードリーダーを通じて支払いを行うICカ

10

20

30

40

50

ード型電子マネー（例えば、モンデックス、VISAキャッシュ）または電子財布（例えば、NTTフレキシブル電子チケット）等が使用できる。

【0016】

課金センター42は、所定の電子マネーを受領したらその旨をコンテンツセンター43へ通知する。コンテンツセンター43は、課金センター42から電子マネー受領通知を受け取ったら、通信衛星45、設置端末41を経由して携帯端末40へコンテンツデータを送る。

【0017】

設置端末41を経由して携帯端末40がコンテンツデータを受信した後は、携帯端末40を設置端末41から取り外して自由に持ち運び可能であり、いつでもどこでも受信したコンテンツデータ（例えば、音楽データ）を再生して楽しむことができる。

10

【0018】

同図(b)に示すように、コンテンツデータ受領後、携帯端末(送信側)40を設置端末41から取り外し、自由に持ち運ぶことができ、かつ携帯端末(送信側)40に記憶されたコンテンツデータは、携帯端末(受信側)46にコピー(転送)することができる。かかるコピーには設置端末41は関与しない。つまり、設置端末41が無い所で、携帯端末(送信側)40と携帯端末(受信側)46との間でコンテンツデータをコピーすることができる。携帯端末間でのコンテンツデータのコピーに対しても課金がなされ、携帯端末(受信側)46から携帯端末(送信側)40へコンテンツデータ料に相当する電子マネーが送られる。また、携帯端末間でコンテンツデータのコピーが行われると、携帯端末(受信側)46の携帯端末ID及びコピーされたコンテンツデータのコンテンツIDが転送履歴として、携帯端末(送信側)40に記憶される。この転送履歴は、携帯端末(送信側)40を後日、販売店設置端末41に接続したときに、前記電子マネーと共に、販売店設置端末41に吸い上げられ、課金センター42へ転送される。これにより、どのコンテンツをどの携帯端末が入手したのかという情報、及び電子マネーが課金センター42に集められる。

20

【0019】

なお、携帯端末(送信側)40と携帯端末(受信側)46は、便宜上「送信側」、「受信側」として区別するが、いずれも送受信の両機能を有し、装置としては同じ物である。そして、「送信側」とは、携帯端末間でデータを転送するときに「送信側」となることを意味し、「受信側」とは、携帯端末間でデータを転送するときに「受信側」となることを意味する。

30

【0020】

図2は、送信側のエンコード装置の構成を示すブロック図である。エンコード装置102は、コンテンツセンター43(図1)に設置され、送信データを所定フォーマットにエンコードするために使用される。このエンコード装置102は、入力端子105、A/Dコンバータ110、信号処理回路120、メモリ130、フォーマット回路140、識別信号生成回路150、スクランブル回路160、メモリ170、出力端子191~193により構成される。

【0021】

複数のチャネルの音楽信号は、入力端子105からA/Dコンバータ110に供給され、所定のサンプリング周波数と量子化数(例えば、サンプリング周波数44.1kHzと20ビットの量子化数)のデジタル信号に変換される。

40

【0022】

A/Dコンバータ110から出力されるデジタル信号は、信号処理回路120に入力される。信号処理回路120では、バッファ用兼信号処理パラメータ用メモリ130とともにミキシング(チャネル数の調整)及び圧縮等の信号処理を行う。

【0023】

信号処理パラメータとは、具体的にはコンプレッサ/リミッタの信号処理におけるアタック時間、リリース時間、コンプレス比の各パラメータであり、あるいは具体的にはパラメ

50

トリック・イコライザーの信号処理における各イコライザーの中心周波数、レベル、Qの各パラメータであり、あるいは具体的には各チャンネルのアッテネータにおけるアッテネート・レベルである。コンプレッサ/リミッタは、音楽信号のダイナミックレンジを適切な範囲に調整するものであり、オーバーフローを防止できる。パラメトリック・イコライザーは、音楽信号の周波数帯の振幅をブースト、カットして周波数特性を調整するものであり、低域などの特定の帯域を強調あるいは減衰できる。チャンネル数の調整とは、具体的には24chや48chのマルチチャンネルから2チャンネルに落とすためのミキシングをいう。

【0024】

データ圧縮方式としては、TwinVQ(商標)、AAC(Advanced Audio Coding)、MPEG(Motion Picture Experts Group) Layer 1、MPEG Layer 3、ATRAC(Adaptive Transform Acoustic Coding)等が使用できる。処理後の信号は、フォーマット回路140に供給される。

10

【0025】

フォーマット回路140では、識別信号生成回路150からの識別信号と共に所定の記録フォーマットに基づいて音声データ等が配列される。識別信号とは、コンテンツID、事業者ID、タイトル情報、転送レベルフラグ、付加情報などのコンテンツヘッダエリア260(図3(b))に収納される情報信号、およびコンテンツ数などの共通ヘッダエリア200(図3(a))に収納される情報信号である。

20

【0026】

所定の記録フォーマットとは、図3に示すデータ形式を意味する。所定のフォーマットに配列された音声データ等は、直接モニター出力端子191に供給され、モニター(不図示)へ出力され、モニタリングされる。また、所定のフォーマットに配列された音声データは、保存用メモリ170にも一旦記憶される。メモリ170に記憶されたデータは、スクランブル回路160でスクランブルされた後、出力端子192に供給され、衛星放送の送信機(不図示)に送られる。

【0027】

また、スクランブル回路160でスクランブルされたデータは、出力端子193に供給され、インターネットに送られる。インターネットを用いて配信されるデータに対するデスクランブル処理の困難性を高めるために、スクランブル回路160と出力端子193の間に第2のスクランブル回路(不図示)を設けて、二重にスクランブル処理を施しても良い。なお、スクランブル処理とは、64ビット等のブロックを処理単位として平文をかくはんするブロック暗号を一例とする秘密鍵暗号の処理、あるいは、暗号鍵によるエクスクルーシブオア(EX-OR)の処理をいう。

30

【0028】

図3(a)及び(b)は、本発明の実施形態に係るデータ構造を示す。同図(a)に示すように、同データは、共通ヘッダエリア200とコンテンツエリア250から構成される。

【0029】

共通ヘッダエリア200は、プレイヤーIDエリア、スクランブルIDエリア、コンテンツ数エリア、使用エリア情報エリア、転送用プリペイドエリア、転送履歴エリアから構成される。

40

【0030】

プレイヤーIDエリアは、暗号処理において使用されるプレイヤーIDを格納するためのエリアである。プレイヤーIDは、まずデータ転送先からデータ転送元へ送られる。つまり、携帯端末40が設置端末41からデータを受け取る場合は、携帯端末40のプレイヤーIDが携帯端末40から設置端末41へ送られる。また、携帯端末46が携帯端末40からデータを受け取る場合は、携帯端末46のプレイヤーIDが携帯端末46から携帯端末40へ送られる。

50

【0031】

スクランブルIDエリアは、暗号処理において使用される秘密鍵等を暗号化したスクランブルIDを格納するためのエリアである。スクランブルIDはプレイヤーIDで暗号化された暗号再生鍵である。暗号前の鍵はエンコーダ時にコンテンツ業者が発行する。

【0032】

コンテンツ数エリアには、コンテンツエリアに格納されているコンテンツの総数が格納される。使用エリア情報エリアには、全国を複数に分けたエリア名が格納される。日本の場合には、関東、関西、九州、北海道などであり、世界の場合には、国名を使用する。転送用プリペイドエリアには、コンテンツの販売情報（対価）が格納される。

【0033】

転送履歴エリアは、コンテンツID（以下、CIDとする。）エリア、転送回数エリア、転送日時エリアから構成される。転送回数とは、送信側となる携帯端末40から受信側となる携帯端末46へデータを転送した回数をいい、転送日時とはこの転送を行った日時を指す。あるいは、使用エリアが格納される。

【0034】

図3（b）はコンテンツエリア250の詳細なデータ構造を示す。同図に示すように、コンテンツエリア250は、コンテンツヘッダエリア260とコンテンツデータエリア280から構成される。

【0035】

コンテンツヘッダエリア260は、コンテンツIDエリア、事業者IDエリア、タイトル情報エリア、プレイヤーIDエリア、転送レベルフラグエリア、付加情報エリアから構成される。

【0036】

事業者IDエリアには、配信データを受信する各設置端末に割り当てられた識別コードである事業者IDが格納される。タイトル情報エリアには、曲名の著作権識別コード（ISRC）であるタイトル情報が格納される。転送レベルフラグエリアには、転送レートの種類である転送レベルフラグが格納される。付加情報エリアには、TOC（Total Of Contents）等の付加情報が格納される。TOCは、いわゆる曲の頭出しのためのアドレス情報と演奏時間等を記録した目次である。TOCは共通ヘッダ200に、あるいは共通ヘッダ200とコンテンツヘッダ260の両方に格納するようにしてもよい。

【0037】

コンテンツデータエリア280には、プレイヤーIDを用いてスクランブル化されたコンテンツデータが格納される。コンテンツデータエリア280は、複数のバック281から構成される。各バック281は、バックヘッダ283とパケット282から構成される。各パケット282は、パケットヘッダ284、プライベートヘッダ285およびユーザデータで構成される。ユーザデータは、サブパケット286a、圧縮同期信号287a、サブパケット286b、圧縮同期信号287b、・・・、サブパケット286mからなり、圧縮同期信号は後続のサブパケットの同期をとるために設けられる。なお、プレーヤIDの代わりにメモリIDを用いるようにしても良い。

【0038】

図4は、携帯端末内のデータ再生手段を示すブロック図である。302は携帯端末を示す。設置端末41等から受け取ったデータはメモリ310に記録され、デスクランブル回路311においてデスクランブルされる。暗号化処理回路313は、デスクランブルに必要な鍵を生成し、デスクランブル回路311に供給する。メモリ310にはメモリカードIDが記録されている。このメモリカードIDは書き換えすることができない。

【0039】

デスクランブルされたデータは、デフォーマット回路312へ供給され、デフォーマットされる。デフォーマット回路312への供給は、システムクロックレファランス（以下、SCRとする。）毎に行われる。SCR（6バイト）は、バックヘッダ283（14バイト）の5バイト目に格納されている。デフォーマットとは、各コンテンツデータが、共通

10

20

30

40

50

ヘッダから分離されること等をいう。受信したコンテンツデータのコンテンツ料に相当する電子マネーが、電子財布320から支払われる。

【0040】

図5に示すように、デフォーマットされたデータは、SCR毎にバッファ回路314へ送られる。バッファ回路314へ転送されたデータは、パケットヘッダ284に記録されるデコーディングタイムスタンプ(以下、DTSとする。)毎に読み出され、信号処理回路315へ転送される。ただし、先頭アクセスユニットのみに関してDTSは記述されているため、パックの2番目以降のアクセスユニットについては、信号処理回路315内の情報に従って、バッファ回路314から信号処理回路315へ転送される。信号処理回路315により圧縮されていたデータが伸長される。その際、プライベートヘッダ285および圧縮同期信号287に記録されている圧縮方式に関する詳しい情報が参照され、個々の圧縮方式に応じた伸長処理が実施される。伸長されたデータは、パケットヘッダ284に記録される再生時間刻印(Presentation Time Stamp、以下PTSとする。)で一定速度のサンプリング周波数となるように取り出され、D/A変換機316に入力される。D/A変換機316に入力されたデータは、アナログ信号に変換されて外部に出力される。

10

【0041】

TOCをTOCメモリ319に記録しておくことと高速なコンテンツのサーチが行える。TOCは、第1のコンテンツ、第2のコンテンツ、・・・、第Nのコンテンツをユーザが指定した場合、TOCの対応箇所を参照し、そのアドレス、サンプリング周波数、チャンネル数、再生時間を読み、アクセスを開始すると共にサンプリング周波数、チャンネル数の設定、再生時間の表示等を行うためのものである。コンテンツのヘッダをスキャンする必要がないので、いわゆる待ち時間がなく、アクセスしやすいので、高速スキャン(イントロスキャン)にも有効に使うことができる。

20

【0042】

なお、上述したエンコード装置では、コンテンツデータをプレーヤID又はメモリカードIDで暗号化するようにしているが、これに限らず、エンコード装置に共通鍵を持たせておき、予めエンコード装置で共通鍵によりコンテンツデータを暗号化し、共通鍵の方をプレーヤID又はメモリカードIDで暗号化するようにしても良い。

【0043】

また、本発明は上記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変形して実施することができる。例えば、携帯端末の使用例としては、その出力をスピーカ付きのオーディオ装置の外部入力から供給して、その装置と組み合わせて用いることもできる。

30

【0044】

【発明の効果】

以上のように本発明によれば、コンテンツデータを暗号鍵を使用してスクランブル化し、また、各受信手段別の識別コードを使用して暗号鍵をスクランブル化して伝送することにより、同一コンテンツデータを各受信手段別に異なる暗号再生鍵を付与されて配信することができる。このため、正当な受信手段以外の受信手段がこのスクランブル化データを仮に入手しても、データを再生することができない。

40

【0045】

また、コンテンツデータを複数の圧縮方式のいずれかで圧縮し、そこで採用された圧縮方式の識別情報がコンテンツヘッダエリアに記録される。データの性質に応じて圧縮方式を適宜選択することにより圧縮効率、伝送効率を向上させることができる。さらに、使用エリアを記録することにより、使用エリアを限定することができる

【0046】

さらに、TOCを共通ヘッダやコンテンツヘッダに配置することにより、複数のトラックからなるコンテンツに対して各トラックを再生時に容易に頭出しすることが可能となる。さらに、転送履歴を記録することにより、回収して著作権を管理できる。

50

【図面の簡単な説明】

【図1】本発明のデータ構造を有するデータの送受信を行うシステム全体を概念的に示すブロック図。

【図2】送信側のエンコード装置の内容を示すブロック図。

【図3】本発明の実施形態に係るデータ構造を示す図。

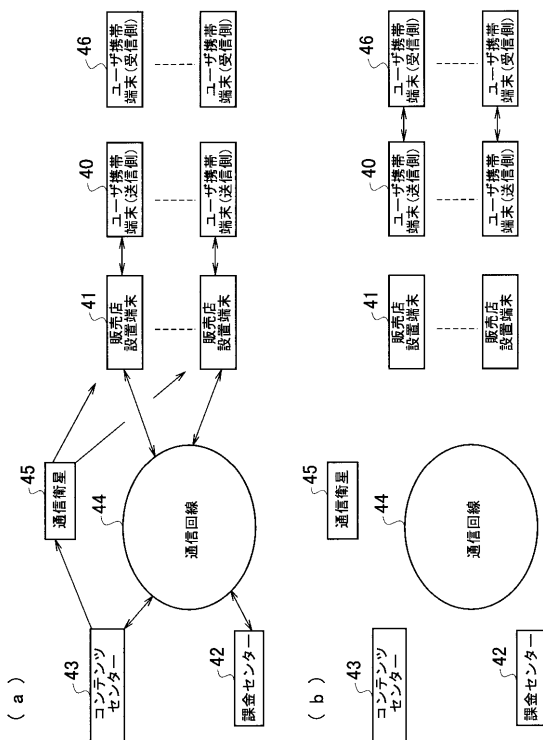
【図4】携帯端末内のデータ再生手段を示すブロック図。

【図5】図4のバッファ回路から信号処理回路へデータが転送されるタイミングを示す図。

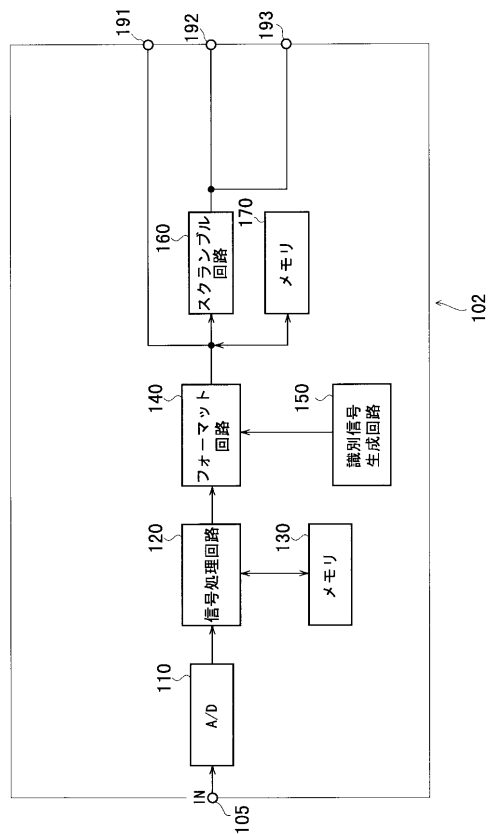
【符号の説明】

- 200 共通ヘッダエリア
- 250 コンテンツエリア
- 260 コンテンツヘッダエリア
- 280 コンテンツデータエリア

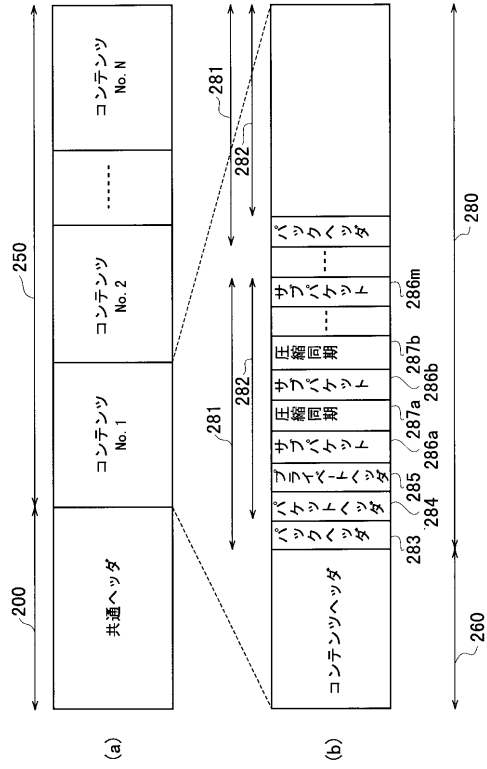
【図1】



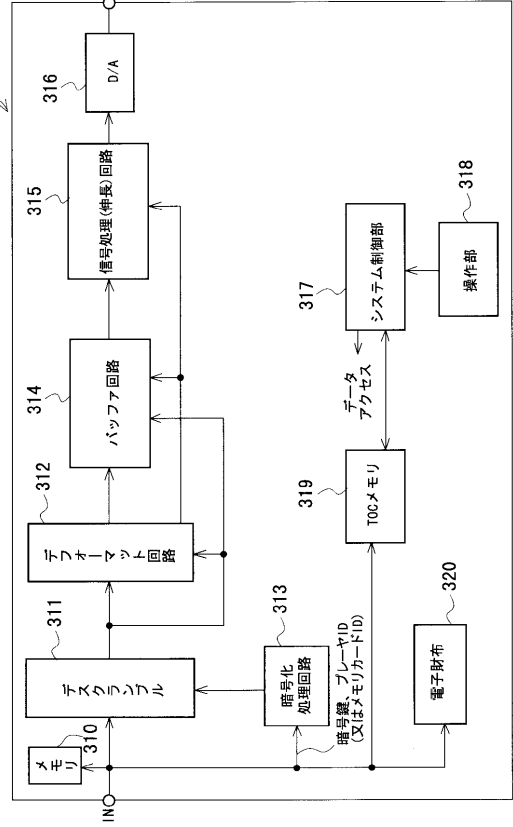
【図2】



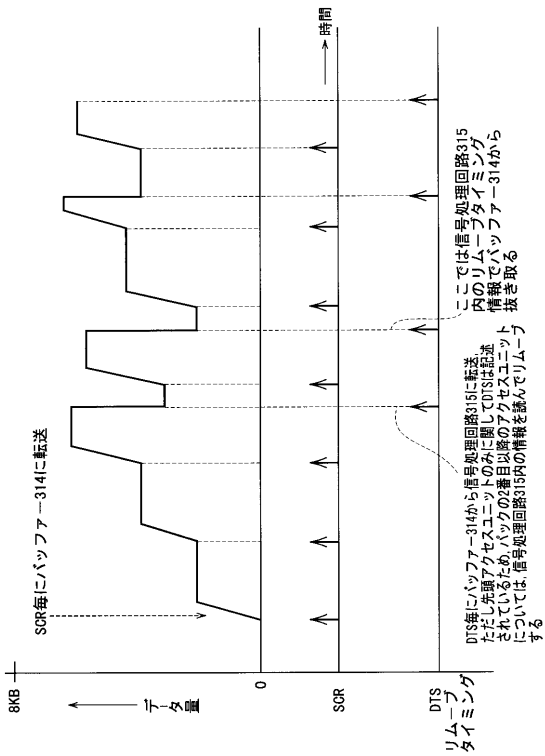
【 図 3 】



【 図 4 】



【 図 5 】



フロントページの続き

(74)代理人 100101247

弁理士 高橋 俊一

(74)代理人 100098327

弁理士 高松 俊雄

(72)発明者 田中 美昭

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(72)発明者 毛利 智博

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

審査官 高野 美帆子

(56)参考文献 特開2000-099010(JP,A)

国際公開第97/014147(WO,A1)

(58)調査した分野(Int.Cl., DB名)

G11B 20/10

G06F 12/14

G09C 1/00

H04L 9/00