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

特許第3759455号

(P3759455)

(45)発行日　平成18年3月22日(2006.3.22)　(24)登録日　平成18年1月13日(2006.1.13)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G10K 15/02	(2006.01)	G10K	15/02	
H04L 9/32	(2006.01)	H04L	9/00	675B
H04N 7/167	(2006.01)	H04N	7/167	Z
G10L 19/00	(2006.01)	G10L	9/00	N

請求項の数 9　(全 36 頁)　最終頁に続く

(21)出願番号　特願2001-542926(P2001-542926)
(86)(22)出願日　平成12年12月6日(2000.12.6)
(86)国際出願番号　PCT/JP2000/008615
(87)国際公開番号　WO2001/043339
(87)国際公開日　平成13年6月14日(2001.6.14)
審査請求日　平成14年4月4日(2002.4.4)
(31)優先権主張番号　特願平11-347904
(32)優先日　平成11年12月7日(1999.12.7)
(33)優先権主張国　日本国(JP)

前置審査

(73)特許権者　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(73)特許権者　503121103
株式会社ルネサステクノロジ
東京都千代田区丸の内二丁目４番１号
(73)特許権者　000004167
コロムビアミュージックエンタテインメント株式会社
東京都港区六本木一丁目４番３３号　六本木２１森ビル

最終頁に続く

(54)【発明の名称】データ再生装置

(57)【特許請求の範囲】

【請求項１】

暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置（１００）であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのライセンスキーを保持して、前記ライセンスキーを暗号化した状態で出力し、かつ前記データ再生装置に着脱可能なデータ格納部（１１０）と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部と、

前記データ格納部と前記データ再生部間のデータの授受を制御する第１の制御部（１１０６）とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記ライセンスキーと前記暗号化コンテンツデータを受けて、前記ライセンスキーにより前記暗号化コンテンツデータを復号してコンテンツデータを抽出するための第１の復号処理部（１５１６）と、

前記データ再生部に予め付与された公開鍵（KPp(1)）を公開認証鍵（KPma）により復号可能なように暗号化を施した認証データ（{KPp(1)}KPma）を保持し、前記データ格納部に対して出力可能な認証データ保持部（１５００）と、

予め付与された前記公開鍵にて暗号化されたデータを復号するための秘密鍵を保持する秘密鍵保持部（１５０２）と、

前記データ格納部から前記公開鍵にて暗号化されて供給される第１のセッションキー（Ks3）を受けて、前記秘密鍵によって復号して前記第１のセッションキーを抽出し、抽出した前記第１のセッションキーを保持する第２の復号処理部（１５０４）と、
前記データ格納部に対して前記ライセンスキーの取得のためにアクセスするごとに更新される第２のセッションキー（Ks4）を生成する第１のセッションキー発生部（１５０８）と、
前記第２の復号処理部に保持された前記第１のセッションキーにて前記第２のセッションキーを暗号化して、前記データ格納部に対して出力可能な第１の暗号化処理部（１５０６）と、
前記データ格納部から前記第２のセッションキーにて暗号化され供給される前記ライセンスキー（Kc）を受けて、前記第２のセッションキーによって復号して前記ライセンスキーを抽出し、抽出した前記ライセンスキーを前記第１の復号処理部に供給する第３の復号処理部（１５１０）とを含み、
前記データ格納部は、
前記暗号化コンテンツデータおよび前記ライセンスキーを記録する記録部（１４１５）と、
前記認証データを受けて前記公開認証鍵により前記認証データを復号処理して、前記公開鍵を抽出するための第４の復号処理部（１４０８）と、
前記第４の復号処理部における復号処理結果に基づいて、前記データ再生部に対して前記ライセンスキーを出力するか否かを判断する認証処理を行なう第２の制御部（１４２０）と、
前記第２の制御部において前記データ再生部に対して前記ライセンスキーを出力すると判断されるごとに更新される前記第1のセッションキー（Ks3）を生成して保持する第２のセッションキー発生部（１４１８）と、
前記データ再生部に前記第1のセッションキーを与えるために、前記第1のセッションキーを前記公開鍵によって暗号化する第２の暗号化処理部（１４１０）と、
前記データ再生部から入力され、かつ、前記第１のセッションキーによって暗号化された前記第２のセッションキーを、前記第１のセッションキーによって復号し前記第2のセッションキーを抽出する第５の復号処理部（１４１２）と、
前記データ再生部に前記ライセンスキーを与えるために、前記ライセンスキーを前記第２のセッションキーによって暗号化する第３の暗号化処理部（１４０６）とを含み、
前記第１の制御部は、
複数の前記暗号化コンテンツデータの連続した再生動作に対応する前記データ格納部から前記コンテンツ再生部への複数の前記ライセンスキーの供給処理に対して共通な前記第１のセッションキーを利用し、かつ、複数の前記ライセンスキーの供給処理ごとに異なる前記第２のセッションキーを利用するように制御し、
複数の前記ライセンスキーの供給処理に共通な所定の期間中に前記第２の復号処理部に対して前記第１のセッションキーを保持させるように制御する、データ再生装置。

【請求項２】
前記データ格納部は、前記データ再生装置に着脱可能なメモリカードである、請求項１記載のデータ再生装置。

【請求項３】
前記所定の期間は、前記データ再生装置が活性な期間中において、前記データ格納部が前記データ再生部に装着された後の期間である、請求項１記載のデータ再生装置。

【請求項４】
前記所定の期間は、前記データ再生装置に前記データ格納部が装着された状態で前記再生装置が活性化された後の期間である、請求項１記載のデータ再生装置。

【請求項５】
前記ライセンスキーは、前記データ再生部に対して予め定められた復号鍵（Kcom）により復号可能なように暗号化され上で、前記記録部に記録され、

前記第３の復号処理部は、前記復号鍵にて暗号化され、さらに、前記第２のセッションキーにて暗号化された前記ライセンスキーを前記第２のセッションキーによって復号する第１の復号ブロック（１５１０）と、
前記第１の復号ブロックの出力を受けて、前記復号鍵によって復号し、前記ライセンスキーを抽出する第２の復号ブロック（１５１２，１５１４）とを有する、請求項１記載のデータ再生装置。
【請求項６】
暗号化コンテンツデータおよび前記暗号化データを復号するためのライセンスキーを格納し、かつ、前記ライセンスキーの出力に当たって暗号化通信路を形成して、前記暗号化通信路を介して前記ライセンスキーを出力するデータ記録装置から、前記暗号化コンテンツデータおよびライセンスキーを受け取って、前記暗号化コンテンツデータの再生を行なうためのデータ再生装置（１００）であって、
前記データ記録装置と前記データ再生装置開のデータの授受を制御する制御部（１１０６）と、
前記データ記録装置から読み出された前記ライセンスキーと前記暗号化コンテンツデータとを受けて、前記ライセンスキーにより前記暗号化コンテンツデータを復号してコンテンツデータを抽出するための第1の復号処理部（１５16）と、
前記データ再生装置に予め付与された公開鍵（KPp(1)）を公開認証鍵（KPma）により復号可能なように暗号化を施した認証データ（{KPp(1)}KPma）を保持し、前記データ記録装置に対して出力可能な認証データ保持部（１５００）と、
予め付与された前記公開鍵にて暗号化されたデータを復号するための秘密鍵（Kp）を保持する秘密鍵保持部（１５０２）と、
前記データ記録装置から前記認証データの入力ごとに更新されて、前記公開鍵にて暗号化されて供給される第１のセッションキー（Ks3）を受けて、前記秘密鍵によって復号して前記第１のセッションキーを抽出し、抽出した前記第１のセッションキーを保持する第２の復号処理部（１５０４）と、
前記データ記録装置に対して前記ライセンスキーの取得のためにアクセスするごとに更新される第２のセッションキー（Ks4）を生成する第１のセッションキー発生部（１５０８）と、
前記第２の復号処理部に保持された前記第１のセッションキーにて前記第２のセッションキーを暗号化して、前記データ記録装置に対して出力可能な第１の暗号化処理部（１５０６）と、
前記データ記録装置から前記第２のセッションキーにて暗号化され供給される前記ライセンスキー（Kc）を受けて、前記第２のセッションキーによって復号して前記ライセンスキーを抽出し、抽出した前記ライセンスキーを前記第１の復号処理部に供給する第３の復号処理部（１５１０）とを備え、
前記制御部は、
複数の前記暗号化コンテンツデータの連続した再生動作に対応する前記データ記録装置から前記コンテンツ再生部への複数の前記ライセンスキーの供給処理に対して共通な前記第１のセッションキーを利用し、かつ、複数の前記ライセンスキーの供給処理ごとに異なる前記第２のセッションキーを利用するように制御し、
複数の前記ライセンスキーの供給処理に共通な所定の期間中に前記第２の復号処理部に対して前記第1のセッションキーを保持させるように制御する、データ再生装置。
【請求項７】
前記ライセンスキーは、前記データ再生装置に対して予め定められた復号鍵（Kcom）にて復号可能なように暗号化された上で前記データ記録装置に格納され、
前記第３の復号処理部は、前記復号鍵にて暗号化され、さらに、前記第２のセッションキーにて暗号化されたライセンスキーを前記第２のセッションキーによって復号する第１の復号ブロック（１５１０）と、
前記第１のブロックの出力を受けて、前記復号鍵によって復号し、前記ライセンスキーを

抽出する第２の復号ブロック（１５１２，１５１４）とを有する、請求項６記載のデータ再生装置。

【請求項８】

前記所定の期間は、前記データ再生装置が活性な期間中において、前記データ記録装置が前記データ再生装置に装着された後の期間である、請求項６記載のデータ再生装置。

【請求項９】

前記所定の期間は、前記データ再生装置に前記データ記録装置が装着された状態で前記データ再生装置が活性化された後の期間である、請求項６記載のデータ再生装置。

【発明の詳細な説明】

技術分野

本発明は、コピーされた情報に対する著作権保護を可能とする携帯電話等の端末に対して情報を配送するための情報配信システムにおけるデータ再生装置に関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においては、デジタル信号によりデータが伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

つまり、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタルデータ通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ところで、上述したようなデジタル情報通信網を介した著作権の存在する音楽データなどのコンテンツデータの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

このような記録装置としては、たとえば、メモリカードのように電気的にデータの書込および消去が可能な媒体が用いられることになる。

さらに、コンテンツデータを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータを自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティー対策を施す必要がある。

このようなシステムのセキュリティーを向上させるためには、システムを構成する機器間で、または当該機器の内部でも外部からアクセス可能な領域で行なわれるデータの授受には、認証処理や暗号化処理等を十分に考慮する必要がある。

一方で、このような認証処理や暗号化処理が厳重になるほど、正規の機器でさえ、コンテンツデータの再生を行なって視聴する際に、再生が開始できるまでの時間が必要以上にかかってしまうなどの問題がある。

発明の開示

本発明の目的は、配信されて記録装置に保持されたコンテンツデータを再生する再生装置において、ユーザ以外の者が無断で当該コンテンツデータに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

この発明の他の目的は、データ配信システムのセキュリティーを向上させ、かつ、コンテンツデータの再生処理を迅速に開始することが可能なデータ再生装置を提供することである。

係る目的を達成するために本願発明に係るデータ再生装置は、暗号化コンテンツデータを

復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ格納部と、データ再生部と、第１の制御部とを備える。
データ格納部は、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスキーを保持して、ライセンスキーを暗号化した状態で出力し、かつデータ再生装置に着脱可能である。データ再生部は、データ格納部からの出力を受けて、暗号化コンテンツデータを再生する。第１の制御部は、データ格納部とデータ再生部間のデータの授受を制御する。
データ再生部は、第１の復号処理部と、認証データ保持部と、秘密鍵保持部と、第２の復号処理部と、第１のセッションキー発生部と、第１の暗号化処理部と、第３の復号処理部とを含む。第１の復号処理部は、データ格納部から読出されたライセンスキーと暗号化コンテンツデータを受けて、ライセンスキーにより暗号化コンテンツデータを復号してコンテンツデータを抽出する。認証データ保持部は、前記データ再生部に予め付与された公開鍵を公開認証鍵により復号可能なように暗号化を施した認証データを保持し、前記データ格納部に対して出力可能である。秘密鍵保持部は、予め付与された前記公開鍵にて暗号化されたデータを復号するための秘密鍵を保持する。第２の復号処理部は、前記データ格納部から前記公開鍵にて暗号化されて供給される第１のセッションキーを受けて、前記秘密鍵によって復号して前記第１のセッションキーを抽出し、抽出した前記第１のセッションキーを保持する。第１のセッションキー発生部は、前記データ格納部に対して前記ライセンスキーの取得のためたアクセスするごとに更新される第２のセッションキーを生成する。第１の暗号化処理部は、前記第２の復号処理部に保持された前記第１のセッションキーにて前記第２のセッションキーを暗号化して、前記データ格納部に対して出力可能である。第３の復号処理部は、前記データ格納部から前記第２のセッションキーにて暗号化され供給される前記ライセンスキーを受けて、前記第２のセッションキーによって復号して前記ライセンスキーを抽出し、抽出した前記ライセンスキーを前記第１の復号処理部に供給する。
データ格納部は、記録部と、第４の復号処理部と、第２の制御部と、第２のセッションキー発生部と、第２の暗号化処理部と、第５の復号処理部と、第３の暗号化処理部を含む。記録部は、前記暗号化コンテンツデータおよび前記ライセンスキーを記録する。第４の復号処理部は、前記認証データを受けて前記公開認証鍵により前記認証データを復号処理して、前記公開鍵を抽出する。第２の制御部は、前記第４の復号処理部における復号処理結果に基づいて、前記データ再生部に対して前記ライセンスキーを出力するか否かを判断する認証処理を行う。第２のセッションキー発生部は、前記第２の制御部において前記データ再生部に対して前記ライセンスキーを出力すると判断されるごとに更新される前記第２のセッションキーを生成して保持する。第２の暗号化処理部は、前記データ再生部に前記第２のセッションキーを与えるために、前記第２のセッションキーを前記公開鍵によって暗号化する。第５の復号処理部は、前記データ再生部から入力され、かつ、前記第１のセッションキーによって暗号化された前記第２のセッションキーを、前記第１のセッションキーによって復号し前記第１のセッションキーを抽出する。第３の暗号化処理部は、前記データ再生部に前記ライセンスキーを与えるために、前記ライセンスキーを前記第２のセッションキーによって暗号化する。
前記第１の制御部は、複数の前記暗号化コンテンツデータの連続した再生動作に対応する前記データ格納部から前記コンテンツ再生部への複数の前記ライセンスキーの供給処理に対して共通な前記第１のセッションキーを利用し、かつ、複数の前記ライセンスキーの供給処理ごとに異なる前記第２のセッションキーを利用するように制御し、複数の前記ライセンスキーの供給処理に共通な所定の期間中に前記第２の復号処理部に対して前記第１のセッションキーを保持させるように制御する。
好ましくは、所定の期間は、データ再生装置が活性な期間中において、データ格納部がデータ再生部に装着された後の期間である、
あるいは、好ましくは、所定の期間は、データ再生装置にデータ格納部が装着された状態で再生装置が活性化された後の期間である。

この発明の他の局面に従うと、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスキーを格納し、かつ、前記ライセンスキーの出力に当たって暗号化通信路を形成して、前記暗号化通信路を介して前記ライセンスキーを出力するデータ記録装置から、前記暗号化コンテンツデータおよびライセンスキーを受け取って、前記暗号化コンテンツデータの再生を行なうためのデータ再生装置であって、制御部と、第１の復号処理部と、認証データ保持部と、秘密鍵保持部と、第２の復号処理部と、第１のセッションキー発生部と、第１の暗号化処理部と、第３の復号処理部とを備える。

制御部は、前記データ記録装置と前記データ再生装置開のデータの授受を制御する。第１の復号処理部は、前記データ記録装置から読出された前記ライセンスキーと前記暗号化コンテンツデータとを受けて、前記ライセンスキーにより前記暗号化コンテンツデータを復号してコンテンツデータを抽出する。認証データ保持部は、前記データ再生装置に予め付与された公開鍵（KPp(1)）を公開認証鍵（KPma）により復号可能なように暗号化を施した認証データ（｛KPp(1)｝KPma）を保持し、前記データ記録装置に対して出力可能である。

秘密鍵保持部は、予め付与された前記公開鍵にて暗号化されたデータを復号するための秘密鍵を保持する。第２の復号処理部は、前記データ記録装置から前記認証データの入力ごとに更新されて、前記公開鍵にて暗号化されて供給される第１のセッションキーを受けて、前記秘密鍵によって復号して前記第１のセッションキーを抽出し、抽出した前記第１のセッションキーを保持する。第１のセッションキー発生部は、前記データ記録装置に対して前記ライセンスキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成する。第１の暗号化処理部は、前記第２の復号処理部に保持された前記第１のセッションキーにて前記第２のセッションキーを暗号化して、前記データ記録装置に対して出力可能である。第３の復号処理部は、前記データ記録装置から前記第２のセッションキーにて暗号化され供給される前記ライセンスキー（Kc）を受けて、前記第２のセッションキーによって復号して前記ライセンスキーを抽出し、抽出した前記ライセンスキーを前記第１の復号処理部に供給する。

前記制御部は、複数の前記暗号化コンテンツデータの連続した再生動作に対応する前記データ格納部から前記コンテンツ再生部への複数の前記ライセンスキーの供給処理に対して共通な前記第１のセッションキーを利用し、かつ、複数の前記ライセンスキーの供給処理ごとに異なる前記第２のセッションキーを利用するように制御し、複数の前記ライセンスキーの供給処理に共通な所定の期間中に前記第２の復号処理部に対して前記第１のセッションキーを保持させるように制御する。

したがって、本願に係るデータ再生装置を用いた配信システムでは、データ再生装置とメモリカードとの相互認証処理の一部を、複数の再生処理において共有化することで、個々の再生動作を迅速に行なうことが可能となる。

【図面の簡単な説明】

図１は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

図３は、ライセンスサーバ１０の構成を示す概略ブロック図である。

図４は、携帯電話機１００の構成を示す概略ブロック図である。

図５は、メモリカード１１０の構成示す概略ブロック図である。

図６は、実施例１に従う携帯電話機１００における再生初期化セッションを説明するためのフローチャートである。

図７は、実施例１に従う携帯電話器１００における音楽を再生する再生動作を説明するためのフローチャートである。

図８は、実施例１に従うデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

図９は、実施例１に従うデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

図１０は、実施例１に従うデータ配信システムにおける配信動作を説明するための第３のフローチャートである。
図１１は、実施例１に従う２つのメモリカード間の移動動作を説明するための第１のフローチャートである。
図１２は、実施例１に従う２つのメモリカード間の移動動作を説明するための第２のフローチャートである。
図１３は、実施例１に従う２つのメモリカード間の移動動作を説明するための第３のフローチャートである。
図１４は、実施例２のデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。
図１５は、実施例２のメモリカード１１４の構成を示すブロック図である。
図１６は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第１のフローチャートである。
図１７は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第２のフローチャートである。
図１８は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第３のフローチャートである。
図１９は、実施例２のメモリカードを用いた場合の再生セッション時における各部の動作を説明するためのフローチャートである。
図２０は、実施例２に従う２つのメモリカード間の移動動作を説明するための第１のフローチャートである。
図２１は、実施例２に従う２つのメモリカード間の移動動作を説明するための第２のフローチャートである。
図２２は、実施例２に従う２つのメモリカード間の移動動作を説明するための第３のフローチャートである。
図２３は、実施例３のデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。
図２４は、実施例３に従うライセンスサーバ１１の構成を示す図である。
図２５は、携帯電話器１０３の構成を示す概略ブロック図である。
図２６は、実施例３に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第１のフローチャートである。
図２７は、実施例３に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第２のフローチャートである。
図２８は、実施例３に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第３のフローチャートである。
図２９は、実施例３のメモリカードを用いた場合の再生セッション時における各部の動作を説明するためのフローチャートである。
図３０は、実施例３に従う２つのメモリカード間の移動動作を説明するための第１のフローチャートである。
図３１は、実施例３に従う２つのメモリカード間の移動動作を説明するための第２のフローチャートである。
図３２は、実施例３に従う２つのメモリカード間の移動動作を説明するための第３のフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

［実施例１］

図１は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような

場合に限定されることなく、他のコンテンツデータ、たとえば画像データ、映像データ、教材データ、テキストデータ、朗読（音声）データ、ゲームプログラム等のコンテンツデータを、他の情報通信網を介して配信する場合にも適用することが可能なものである。
図１を参照して、著作権の存在する音楽データを管理するライセンスサーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータを与える。一方、認証サーバ１２は、コンテンツデータの配信を求めてアクセスしてきたユーザの携帯電話機およびメモリカードが正規の機器であるか否かの認証を行なう。
配信キャリア２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）をライセンスサーバ１０に中継する。ライセンスサーバ１０は、配信リクエストがあると、認証サーバ１２によりユーザの携帯電話機およびメモリカードが正規の機器であることを認証し、要求された音楽情報をさらに暗号化した上で配信キャリア２０の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。
図１においては、たとえばユーザ１の携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。
さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを「再生」して、音楽を聴取することが可能である。
以下では、このようなライセンスサーバ１０と認証サーバ１２と配信キャリア（携帯電話会社）２０と併せて、配信サーバ３０と総称することにする。
また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。
このような構成とすることで、まず、正規の携帯電話機および正規のメモリカードを購入していないユーザは、配信サーバ３０からのコンテンツデータを受取って再生することが困難な構成となる。
しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータの配信を受けるたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。
しかも、このようなコンテンツデータの配信は、携帯電話網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。
このとき、たとえばメモリカード１１２を有するユーザ２が自己の携帯電話機１０２により、配信サーバ３０から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ２が直接配信サーバ３０から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ１から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。
しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。
図１に示すように、ユーザ１が受信したコンテンツデータを、コンテンツデータそのものをコピーさせ、ユーザ１がもつ当該コンテンツデータを再生可能とするために必要な再生情報（再生するために必要な権利）を、ユーザ２に対して移動させる場合を音楽データの「移動」と呼ぶ。この場合に、携帯電話機１００および１０２を介して、メモリカード１１０と１１２との間で暗号化されたコンテンツデータおよび再生のために必要な情報（再生情報）が移動される。ここで、「再生情報」とは、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、著作権保護

にかかわる情報であるライセンスＩＤやアクセス再生に関する制限情報等のライセンス情報とを有する。
「移動」に対して、コンテンツデータそのもののみのコピーを行なうことを「複製」と呼ぶ。複製においては再生情報を伴なわないため、ユーザ２は、当該コンテンツデータを再生することができない。ここでは説明しないが、ライセンスキーを含む再生情報のみを配信する新たな配信によって前記ユーザ２は当該コンテンツデータを再生できるようになる。
このような構成とすることによって、一旦配信サーバ３０より配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。
また、携帯電話機１００および１０２がＰＨＳ（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１とユーザ２との間における情報の移動を行なうことが可能である。
図１に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、コンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのデータ保護を実現する構成である。
本発明の実施例においては、特に、配信および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させるとともに、コンテンツ再生回路（たとえば、携帯電話機）におけるコンテンツデータ再生時間を短縮する構成を説明する。
［システムの鍵およびデータの構成］
図２は、図１に示したデータ配信システムにおいて、使用される通信のための暗号に関する鍵および配信するデータ等の特性を説明する図である。
まず、配信サーバより配信されるデータDataは、音楽データ等のコンテンツデータである。コンテンツデータDataは、後に説明するように、少なくともライセンスキーKcによって復号可能な暗号化が施された暗号化コンテンツデータ{Data}Kcという形式で、配信サーバ３０よりユーザに配布される。
なお、以下においては、{Y}Xという表記は、データYを、鍵Xにより復号可能な暗号に変換した情報であることを示すものとする。
さらに、配信サーバ３０からは、コンテンツデータとともに、コンテンツデータに関する、あるいはサーバへのアクセスに関する平文データとしての付加情報Data-infが配布される。すなわち、付加情報Data-infには、コンテンツデータの曲目などのコンテンツデータを特定するための情報や、配信サーバ３０が、いずれのサーバであるかを特定するための情報等が含まれる。
次に、コンテンツデータの暗号化や復号・再生処理や、コンテンツ再生回路である携帯電話機や記録装置であるメモリカードの認証に関わる鍵として、以下のものがある。
すなわち、上述したとおり、コンテンツデータを暗号化および復号するためのライセンスキーＫｃと、コンテンツ再生回路（携帯電話機１００）認証を行なうための公開暗号鍵KPp（n）と、メモリカードの認証を行なうための公開暗号鍵KPmc（n）とがそれぞれ設けられる。
公開暗号鍵KPp（n）およびKPmc（n）により暗号化されたデータは、コンテンツ再生回路（携帯電話機１００）の固有の秘密復号鍵Kp（n）およびメモリカード固有の秘密復号鍵Kmc（n）によってそれぞれ復号可能である。これら固有の秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる内容を有する。ここで、携帯電話機やメモリカードの種類とは、それらを製造するメーカの種類や、製造時期（製造ロット）の違い等に基づき規定され、自然数nは、各メモリカードおよびコンテンツ再生回路（携帯電話機）の種類を区別するための番号を表わす。なお、公開暗号鍵ＫＰｍｃ（ｎ）およびＫＰｐ（ｎ）を共有する単位をクラスと称す。
さらに、コンテンツ再生回路に共通の秘密鍵として、主としてライセンスキーKcや後に説

明するコンテンツ再生回路に対する制限情報などの取得に利用される秘密鍵Kcomと、配信システム全体で共通に運用される認証鍵KPmaとが存在する。秘密鍵Kcomは、共通鍵方式における復号鍵であるため、配信サーバにおいては、この秘密鍵Kcomが暗号鍵として保持される。
また、秘密鍵Kcomは、共通鍵方式における復号鍵に限定されず、公開鍵方式における秘密鍵Kcomとしても同様に構成することができる。この場合、配信サーバにおける暗号鍵は復号鍵とは非対称な公開暗号鍵Kpcomを保持するように構成すればよい。
なお、上述したメモリカードおよびコンテンツ再生部ごとに設定される公開暗号鍵KPmc（n）およびKPp（n）は、認証データ｛KPmc（n）｝KPmaおよび｛KPp（n）｝KPmaの形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。なお、認証データは認証鍵である認証鍵KPmaを用いて復号すると、その復号結果から認証データの正当性が確認できる鍵であり、言い換えれば、公開暗号鍵を認証するのに用いられる鍵である。なお、認証データを作成するための暗号は、認証鍵と対をなす非対称な秘密鍵にて行われる。
さらに、システムを構成する機器、すなわち、コンテンツ再生回路である携帯電話機１００やメモリカード１１０の動作を制御するための情報として、利用者がライセンスキー等を購入する際に、携帯電話機１００から配信サーバ３０に対してその購入条件を指定するために送信される購入条件情報ＡＣと、購入条件情報ＡＣに応じて、配信サーバ３０からメモリカード１１０に対して配信され、メモリカード１１０へのアクセス回数に対する制限等を示すアクセス制限情報ＡＣ１と、配信サーバ３０から携帯電話機１００に対して配信され、コンテンツ再生回路の再生条件の制限を示すコンテンツ再生回路制限情報ＡＣ２とが存在する。コンテンツ再生回路の再生条件とは、たとえば、新曲のプロモーションとして廉価にまたは無償でサンプルを配信する場合などに、各コンテンツデータの冒頭の所定時間のみ再生を許す等の条件を意味する。
また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵KPm（i）（i：自然数）と、秘密暗号鍵KPm（i）で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Km（i）とが存在する。ここで、自然数ｉは、各メモリカードを区別するための番号を表わす。
さらに、図１に示したデータ配信システムにおいて、データの通信時に使用される鍵（キー）等として以下のものがある。
すなわち、メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、再生情報の配信、再生および移動が行なわれるごとに配信サーバ３０、携帯電話機１００または１０２、メモリカード１１０または１１２において生成される共通鍵Ks１～Ks４が用いられる。
ここで、共通鍵Ks１～Ks４は、サーバ、携帯電話もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks１～Ks４を「セッションキー」とも呼ぶこととする。
これらのセッションキーKs１～Ks４は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。
具体的には、セッションキーKs１は、配信サーバ内のライセンスサーバによって配信セッションごとに発生される。セッションキーKs２は、メモリカードによって配信セッションおよび移動（受信側）セッションごとに発生し、セッションキーKs３は、同様にメモリカードにおいて再生セッションおよび移動（送信側）セッションごとに発生する。セッションキーKs４は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。
さらに、配信サーバと携帯電話機との間で授受されるデータとしては、コンテンツデータをシステムが識別するためのコンテンツＩＤや、ライセンスの発行がいつ、誰に対して行なわれたかを特定するための管理コードであるライセンスＩＤや、配信セッションごとに生成され、各配信セッションを特定するためのコードであるトランザクションＩＤなどが

ある。
［ライセンスサーバ１０の構成］
図３は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。
ライセンスサーバ１０は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンスID等の配信するデータを保持するための情報データベース３０４と、各ユーザごとに音楽データへのアクセス開始に従った課金データを保持するための課金データベース３０２と、情報データベース３０４および課金データベース３０２からのデータをデータバスBS１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。
データ処理部３１０は、データバスBS１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーKs１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた、復号することでその正当性がわかるよう暗号化された認証データ｛KPmc（n）｝KPmaおよび｛KPp（n）｝KPmaを通信装置３５０およびデータバスBS１を介して受けて、認証鍵KPmaに対する復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーKs１を復号処理部３１２によって得られた公開暗号鍵KPmc（n）を用いて暗号化して、データバスBS１に出力するための暗号化処理部３１８と、各ユーザにおいてセッションキーKs１によって暗号化された上で送信されたデータをデータバスBS１をより受けて、復号処理を行なう復号処理部３２０とを含む。
データ処理部３１０は、さらに、再生回路共通の秘密鍵Kcomを暗号鍵として保持するKcom保持部３２２と、配信制御部３１５から与えられるライセンスキーKcおよび再生回路制御情報AC２を再生回路共通の暗号鍵KPcomで暗号化する暗号化処理部３２４と、暗号化処理部３２４から出力されたデータを復号処理部３２０によって得られたメモリカード固有の公開暗号鍵KPm（i）によって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーKs２によってさらに暗号化してデータバスBS１に出力するための暗号化処理部３２８とを含む。
なお、ライセンスサーバ１０において、共通鍵方式における秘密鍵Kcomを暗号鍵として利用する構成を説明したが、公開鍵方式においては、携帯電話機側が秘密復号鍵Kcomを備える場合、秘密復号鍵Kcomと非対称かつ秘密復号鍵Kcomにて復号可能な公開暗号鍵KPcomをKcom保持部３２２に保持する。
［携帯電話機１００の構成］
図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。
携帯電話機１００においては、クラスを表わす自然数ｎは、ｎ＝１とする。
携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機１００からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスBS２と、データバスBS２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。
携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのタッチキー部１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データベースBS２を介して与えられる受信データに基いて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバスBS２に与え得る信号に変換し、または、データバスBS２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インタフェース部１１２２とを含む。
携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を

記憶し、かつ復号処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスBS２との間のデータの授受を制御するためのメモリインタフェース１２００と、携帯電話機のクラスごとに設定される公開暗号鍵KPp（1）を、認証鍵KPmaで復号可能な状態に暗号化したデータを保持する認証データ保持部１５００を含む。
携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の秘密復号鍵であるKp（n）（ｎ＝１）を保持するKp保持部１５０２と、データバスBS２から受けたデータを秘密復号鍵Kp（１）によって復号し、メモリカードによって発生されたセッションキーKs３を得る復号処理部１５０４と、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいて、メモリカード１１０との間でデータバスBS２上においてやり取りされるデータを暗号化するためのセッションキーKs４を乱数等により発生するセッションキー発生部１５０８と、生成されたセッションキーKs４を復号処理部１５０４によって得られたセッションキーKs３によって暗号化しデータバスBS２に出力する暗号化処理部１５０６と、データバスBS２上のデータをセッションキーKs４によって復号して、データ｛Kc//AC２｝Kcomを出力する復号処理部１５１０とをさらに含む。
携帯電話機１００は、さらに、コンテンツ再生回路に共通に設定される秘密鍵Kcomを保持するKcom保持部１５１２と、復号処理部１５１０が出力するデータ｛Kc//AC２｝Kcomを秘密鍵Kcomで復号し、ライセンスキーKcおよび再生回路制御情報AC２を出力する復号処理部１５１４と、データバスBS２より暗号化コンテンツデータ｛Data｝Kcを受けて、復号処理部１５１４より取得してライセンスキーKcによって復号しコンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８と音声再生部１１１２の出力を受けて、動作モードに応じて選択的に出力するための切換部１５２５と、切換部１５２５の出力を受けて、ヘッドホン１３０と接続するための接続端子１５３０とを含む。
ここで、復号処理部１５１４から出力される再生回路制御情報AC２は、データバスＢＳ２を介して、コントローラ１１０６に与えられる。
なお、図４においては、説明の簡素化のため、携帯電話機を構成するブロックのうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては一部割愛している。
［メモリカード１１０の構成］
図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。
既に説明したように、公開暗号鍵KPm（i）およびこれに対応する秘密復号鍵Km（i）は、メモリカードごとに固有の値であるが、メモリカード１１０においては、この自然数i＝１であるものとする。また、メモリカードの種類(クラス)に固有の公開暗号鍵および秘密復号鍵として、KPmc（n）およびKmc（n）が設けられるが、メモリカード１１０においては、自然数nは、n＝１で表わされるものとする。
メモリカード１１０は、認証データとして｛KPmc（１）｝KPmaを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるKmc（１）を保持するKmc保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Km（１）を保持するKm（１）保持部１４２１と、秘密復号鍵Km（１）によって暗号化されたデータを復号可能な公開暗号鍵KPm（１）を保持するKPm（１）保持部１４１６とを含む。ここで、認証データ保持部１４００は、メモリカードの種類(クラス)ごとに設定される公開暗号鍵KPmc（1）を認証鍵KPmaで復号可能な状態に暗号化して保持する。
メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスBS３と、データバスBS３にメモリインタフェース１２００から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Kmc（１）をKmc（１）保持部１４０２から受けて配信サーバ３０が配信セッションにおいて生成したセッションキーKs１または他のメモリカードが移動セッションにおいて生成したセッションキーKs３を接点Paに出力する復号処理部１４０４と、KPma保持部１４１４からの認証鍵KPmaを受けて、データバスBS３に与えられるデータから認証鍵KPmaによる復号処理を実行し

て復号結果をデータバスＢＳ４を介してコントローラ１４２０と暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してデータバスBS３に出力する暗号化処理部１４０６とを含む。

メモリカード１１０は、さらに、配信、再生および移動の各セッションにおいてセッションキーＫｓ２あるいはＫｓ３を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ３を復号処理部１４０８によって得られる公開暗号鍵KPp（n）あるいはKPmc(ｎ)によって暗号化してデータバスBS３に出力する暗号化処理部１４１０と、BS３よりセッションキーKs2あるいはKs3によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーKs2あるいはKs３によって復号し、復号結果をデータバスBS４に送出する復号処理部１４１２とを含む。

メモリカード１１０は、さらに、移動（移動元）セッションにおいてデータバスBS４上のデータを他のメモリカード公開暗号鍵KPm(ｉ)(ｉ≠１）で暗号化する暗号化処理部１４２４と、データバスBS４上のデータを公開暗号鍵KPm（１）と対をなすメモリカード１１０固有の秘密復号鍵Km（１）によって復号するための復号処理部１４２２と、公開暗号鍵KPm（１）で暗号化されている、再生情報（ライセンスキーKc、コンテンツID、ライセンスID、アクセス制限情報AC１、再生回路制御情報AC２）をデータバスBS４より受けて格納するとともに、暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data-infをデータバスBS３より受けて格納するためのメモリ１４１５とを含む。

メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスID、コンテンツIDおよびアクセス制限情報AC１を保持するためのライセンス情報保持部１４４０と、データバスBS３を介して外部との間でデータ授受を行ない、データバスBS４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

なお、図５において、実線で囲んだ領域TRMは、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタントモジュール（Tamper Resistant Module）である。

もちろん、メモリ１４１５も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図５に示したような構成とすることで、メモリ１４１５中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、コンテンツデータから音楽を再生することは不可能であり、かつ高価なタンパーレジスタントモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

［再生動作］

（再生初期化セッション）

次に、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから、音楽を再生し、外部に出力するための再生動作（以下、再生セッションともいう）を説明する。

図６は、初期化処理(再生初期化セッションともいう)として携帯電話機１００とメモリカード１１０との相互認証処理の一部を行なうための再生初期化セッション各部の動作を説明するためのフローチャートである。

以下に説明するように、ｉ）携帯電話機１００にメモリカード１１０が装着されている状態で、携帯電話機１００の電源が投入された時や、ｉｉ）携帯電話機１００に電源が投入されている状態で、メモリカード１１０が携帯電話機１００に挿入された時や、ｉｉｉ）配信セッション等や移動セッション等において新たなセッションキーが生成された場合において、一括して再生初期化セッションの処理を行なうこととし、携帯電話機１００とメモリカード１１０との相互認証処理の一部を、複数の再生処理において共有化することで、個々の再生動作を迅速に行なうことが可能となる。

図６を参照して、上述したようなタイミングで、携帯電話機１００のコントローラ１１０６の制御により、再生初期化セッションが開始されると（ステップＳ２００）、携帯電話機１００は、認証データ保持部１５００より、認証鍵KPmaで復号可能な認証データ｛KPp（１）｝KPmaをデータバスBS２に出力する（ステップＳ２０２）。
認証データ｛KPp（１）｝KPmaは、データバスBS２およびメモリインタフェース１２００を介してメモリカード１１０に伝達される。
メモリカード１１０においては、端子１２０２を介してデータバスBS３に伝達される認証データ｛KPp（１）｝Kpmaが、復号処理部１４０８に取込まれる。復号処理部１４０８は、KPma保持部１４１４から認証鍵KPmaを受けて、データバスBS３のデータを復号処理を実行する。この、Kpmaにて暗号化された公開暗号鍵KPp（１）が正規に登録され、正規の暗号化を施されている場合、すなわち、認証鍵Kpmaにて復号化でき、復号時に発生する従属するデータが認識できる場合、復号したKPp（１）を受理する。一方、復号できない場合、または、復号処理において発生する従属データが認識できない場合、得られたデータを受理しない(ステップＳ２４３)。
コントローラ１４２０は、復号処理部１４０８にて携帯電話機１００のコンテンツ再生回路に固有の公開暗号鍵KPp（１）が受理された場合、送信されてきた公開暗号鍵KPp（１）が、このデータ配信システムに対して承認されたコンテンツ再生回路に付与された公開暗号鍵であると判断し、次のステップＳ２１０に進める(ステップＳ２０６）。一方、受理されなかった場合、非承認の機器からの不正なアクセスであると判断し、処理を終了する(ステップＳ２４０)。
公開暗号鍵KPp（１）が受理された場合には、コントローラ１４２０は、セッションキー発生部１４１８に、再生セッションにおけるセッションキーKs３の生成をデータバスBS４を介して指示する。セッションキー発生部１４１８によって生成されたセッションキーKs３は、暗号化処理部１４１０に送られる。暗号化処理部１４１０は、復号処理部１４０８によって得られた携帯電話機１００の公開暗号鍵KPp（１）によってセッションキーKs３を暗号化し、暗号化データ｛Ks３｝Kp（１）をデータバスBS３に出力する（ステップＳ２１０）。
携帯電話機１００は、端子１０２およびメモリインタフェース１２００を介して、データバスBSに暗号化データ｛Ks３｝Kp（１）を受ける。暗号化データ｛Ks３｝Kp（１）は、復号処理部１５０４によって復号され、メモリカード１１０で生成されたセッションキーKs３が受理され（ステップＳ２１２）、再生初期化セッションが終了する（ステップＳ２１３）。
このように、メモリカード１１０は再生に際してデータを出力する出力先であるコンテンツ再生回路(携帯電話機１００)が持つ、認証データを受け、携帯電話機１００が正規の再生機器であることを確認した後、確認した相手との接続状態を確保するために、セッション固有のセッションキーKs３を送付する。セッションキーKs３を受けた携帯電話機１００および送付したメモリカード１１０はともに、このセッションキーKs３を保持して、共有化を図ったうえで再生に備える。
（再生処理）
図７は、図６の再生初期化セッションに続く再生処理を説明するためのフローチャートである。
携帯電話機１００のタッチキー部１１０８等からのユーザ１の指示により、再生リクエストが生成されと（ステップＳ２０１）、携帯電話機１００のコントローラ１１０６は、再生リクエストの生成に応じて、セッションキー発生部１５０８に対して、再生セッションにおいて携帯電話機１００で生成されるセッションキーKs４の発生をデータバスBS２を介して指示する。生成されたセッションキーKs４は暗号化処理部１５０６に送られ、復号処理部１５０４によって得られたセッションキーKs３によって暗号化された｛Ks４｝Ks３がデータバスBS２に出力される（ステップＳ２１４）。
暗号化されたセッションキー｛Ks４｝Ks３は、メモリインタフェース１２００を介してメモリカード１１０に伝達される。メモリカード１１０においては、データバスBS３に伝達

される暗号化されたセッションキー｛Ks４｝Ks３を復号処理部１４１２によって復号し、携帯電話機１００で生成されたセッションキーKs４を受理する（ステップＳ２１６）。
セッションキーKs４の受理に応じて、コントローラ１４２０は、ライセンス保持部１４４０内の対応するコンテンツＩＤを持つアクセス制限情報AC１を確認する（ステップＳ２１８）。
ステップＳ２１８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC１を確認することにより、既に再生不可の状態である場合には再生セッションを終了し（ステップＳ２４０）、再生可能であるが再生回数に制限がある場合にはアクセス制限情報AC１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ２２０）。一方、アクセス制限情報AC１によって再生回数が制限されていない場合においては、ステップＳ２２０はスキップされ、アクセス制御情報AC１は更新されることなく処理が次のステップＳ２２２に移行する。
また、ライセンス保持部１４４０内に、リクエスト曲の当該コンテンツＩＤが存在しない場合においても再生不可の状態にあると判断して、再生セッションを終了する（ステップＳ２４０）。
ステップＳ２１８において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキーKcや再生回路制御情報AC２を取得するための復号処理が実行される。具体的には、コントローラ１４２０の指示に応じて、メモリ１４１５からデータバスBS４に読出された暗号化データ｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（１）を復号処理部１４５４がメモリカード１１０固有の秘密復号鍵Km（１）によって復号する。これにより、秘密復号鍵Kcomによって復号可能な暗号化データ｛Kc//AC２｝Kcomが取得される（ステップＳ２２２）。
得られた暗号化データ｛Kc//AC２｝Kcomは、切換スイッチ１４４４の接点Pdを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Pbを介して復号処理部１４１２より受けたセッションキーKs４によって、データバスBS４から受けた暗号化データ｛Kc//AC２｝Kcomをさらに暗号化し、｛｛Kc//AC２｝Kcom｝Ks４をデータバスBS３に出力する（ステップＳ２２４）。
データバスBS３に出力された暗号化データは、メモリインタフェース１２００を介して携帯電話機１００に送出される。
携帯電話機１００においては、メモリインタフェース１２００を介してデータバスBS２に伝達される暗号化データ｛｛Kc//Ac２｝Kcom｝Ks４を復号処理部１５１０によって復号処理を行ない、暗号化されたライセンスキーKcおよび再生回路制御情報AC２である｛Kc//AC２｝Kcomを受理する（ステップＳ２２６）。復号処理部１５１４は、暗号化データ｛Kc//AC２｝Kcomを、Kcom保持部１５１２から受けたコンテンツ再生回路に共通の秘密復号鍵Kcomによって復号し、ライセンスキーKcおよび再生回路制御情報AC２を受理する（ステップＳ２２８）。復号処理部１５１４は、ライセンスキーKcを復号処理部１５１６に伝達し、再生回路制御情報AC２をデータバスBS２に出力する。
コントローラ１１０６は、データバスBS２を介して、再生回路制御情報AC２を受理して再生の可否の確認を行なう（ステップＳ２３０）。
ステップＳ２３０においては、再生回路制御情報AC２によって再生不可と判断される場合には、再生セッションは終了される（ステップＳ２４０）。
一方、再生可能である場合には、メモリカード１１０よりメモリに記録されたリクエスト曲の暗号化コンテンツデータ｛Data｝Kcがデータバス BS３に出力され、メモリインタフェース１２００を介して携帯電話機１００に伝達される（ステップＳ２３２）。
携帯電話機１００においては、メモリカード２１０から出力されデータバスBS２に伝達された暗号化コンテンツデータ｛Data｝Kcを復号処理部１５１６においてライセンスキーKcによって復号し、平文化されたコンテンツデータDataを得ることができる（ステップＳ２３４）。復号された平文のコンテンツデータDataは音楽再生部１５１８によって音楽に再生され、混合部１５２５および端子１５３０を介して外部に再生された音楽を出力することによって処理が終了する（ステップＳ２４０）。

このように再生セッションにおける処理から再生初期化セッションを分離し、再生初期化セッションを複数の曲で共有することで、ユーザの再生リクエストに対して迅速に音楽の再生を開始することができる。
さらには、セッションキーKs４を再生毎に発生し、これを用いてメモリカード１１０からコンテンツ再生回路（携帯電話機１００）へのライセンスキーKcの送信に対して暗号化を施すために、同一の曲を続けて再生したとしても同一のデータがメモリインタフェース１２００を通過することがない構成になっている。ゆえに、再生初期化セッションを分離せず、再生処理の都度、再生初期化セッションから開始して再生した場合に比べて、セキュリティ強度が低下することがない。
再生セッションでは、再生初期化セッションからの一連の動作において、携帯電話機およびメモリカードでそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信する。この結果、配信セッションにおける暗号化データのそれぞれの送受信においても、相互認証を行なうことができ、データ配信システムのセキュリティを確保させることができる。
［配信動作］
次に、本発明の実施例に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。
図８、図９および図１０は、実施例１に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１、第２および第３のフローチャートである。
図８～図１０においては、ユーザ１が、メモリカード１１０を用いることで、携帯電話機１００を介して配信サーバ３０からコンテンツデータの配信を受ける場合の動作を説明している。
まず、ユーザ１の携帯電話機１００からユーザ１によりタッチキー部１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。
メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛KPmc（１）｝KPmaが出力される（ステップＳ１０２）。
携帯電話機１００は、メモリカード１１０から受理した認証データ｛KPmc（１）｝KPmaに加えて、携帯電話機１００自身の認証データ｛KPp（１）｝KPmaと、配信を受けるコンテンツデータを指示するためのコンテンツID、ライセンス購入条件のデータACとを配信サーバ３０に対して送信する（ステップＳ１０４）。
配信サーバ３０では、携帯電話機１００からコンテンツID、認証データ｛KPmc（１）｝KPma、認証データ｛KPp（１）｝KPma、ライセンス購入条件ACを受信し（ステップＳ１０６）、復号処理部３１２において認証鍵KPmaで復号処理を実行する。この、認証鍵Kpmaにて暗号化された公開暗号鍵Kpp（１）、KPmc（１）が正規に登録され、正規の暗号化を施されている場合、メモリカード１１０の公開暗号鍵KPmc（１）と、携帯電話機１００の公開暗号鍵KPp（１）とを受理する。一方、正規に登録されていない場合、登録されていない公開暗号鍵KPp（１）、KPmc（１）は受理されない（ステップＳ１０８）。
配信制御部３１５は、受理した秘密暗号鍵KPmc（１）およびKPp（１）に基づいて、認証サーバ１２に対して照会を行ない（ステップＳ１１０）、これらの公開暗号鍵がすてっぷＳ１０８にて受理され、正規に登録された鍵の場合には、有効と判断し、次の処理（ステップＳ１１２）に移行し、これらの公開暗号鍵が受理されない、あるいは受理されても登録されていない鍵である場合には、無効と判断し、処理を終了する（ステップＳ１７０）。
ここで、認証鍵KPmaによる復号処理において、公開暗号鍵KPp(1)あるいはKPmc(1)の正当性の認証が行なわれるにあたり、公開暗号鍵KPp(1)あるいはKPmc(1)のそれぞれに付随して、認証書が認証鍵Kpmaにより復号できるよう暗号化されて配信サーバ３０に送信される構成としてもよい。
また、認証サーバ１２に対して照会せず、認証データ｛KPmc（１）｝KPmaおよび｛KPp（１）｝KPmaは、それぞれが認証鍵KPmaによって復号することでその正当性が判断可能な暗

号化が施されているため、ライセンスサーバ１０の配信制御部３１５が認証鍵Kpmaによる復号結果から独自に認証を行う構成としてもよい。
照会の結果、有効であることが認識されると、配信制御部３１５は、次に、配信セッションを特定するためのトランザクションＩＤを生成する（ステップＳ１１２）。
続いて、セッションキー発生部３１６は、配信のためのセッションキーKs1を生成する。セッションキーKs1は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵KPmc（１）によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。
トランザクションＩＤと暗号化されたセッションキー｛Ks1｝Kmc（１）とは、データバスBS1および通信装置３５０を介して外部に出力される（ステップＳ１１６）。
携帯電話機１００が、トランザクションＩＤおよび暗号化されたセッションキー｛Ks1｝Kmc（１）を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスBS3に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵Kmc（１）により復号処理することにより、セッションキーKs1を復号し抽出する（ステップＳ１２０）。
コントローラ１４２０は、配信サーバ３０で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部１４１８に対して、メモリカード１１０において配信セッションに生成されるセッションキーKs2の生成を指示する。配信セッションでは、メモリカード１１０のセッションキー発生部１４１８にて新しいセッションキーを発生したため、再生初期化セッションにおいて保持したセッションキーKs3がセッションキーKs2に書換えられる。
暗号化処理部１４０６は、切換スイッチ１４４２の接点Paを介して復号処理部１４０４より与えられるセッションキーKs1によって、切換スイッチ１４４４の接点Pcを介して切換スイッチ１４４６の接点を切換えることによって与えられるセッションキーKs2および公開暗号鍵KPm（１）を暗号化して、｛Ks2//KPm（１）｝Ks1をデータバスBS3に出力する（ステップＳ１２２）。
データバスBS3に出力されたデータ｛Ks2//KPm（１）｝Ks1は、データバスBS3から端子１２０２およびメモリインタフェース１２００を介して携帯電話機１００に送信され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。
配信サーバ３０は、暗号化データ｛Ks2//KPm（１）｝Ks1を受信して、復号処理部３２０においてセッションキーKs1による復号処理を実行し、メモリカード１１０で生成されたセッションキーKs2およびメモリカード１１０固有の公開暗号鍵Kpm（１）を受理する（ステップＳ１２６）。
さらに、配信制御部３１５は、ステップＳ１０６で取得したコンテンツIDおよびライセンス購入条件データACに従って、ライセンスID、アクセス制限情報AC1および再生回路制御情報AC2を生成する（ステップＳ１３０）。さらに、暗号化コンテンツデータを復号するためのライセンスキーKcを情報データベース３０４より取得する（ステップＳ１３２）。
図９を参照して、配信制御部３１５は、取得したライセンスキーKcおよび再生回路制御情報AC2を暗号化処理部３２４に与える。暗号化処理部３２４は、Kcom保持部３２２より得られる、コンテンツ再生回路共通の秘密復号鍵Kcomを暗号鍵として、ライセンスキーKcおよび再生回路制御情報AC2を暗号化する（ステップＳ１３４）。
暗号化処理部３２４が出力する暗号化データ｛Kc//AC2｝Kcomと、配信制御部３１５が出力するライセンスID、コンテンツIDおよびアクセス制限情報AC1とは、暗号化処理部３２６によって、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵KPm（１）によって暗号化される（ステップＳ１３６）。
暗号化処理部３２８は、暗号化処理部３２６の出力を受けて、メモリカード１１０において生成されたセッションキーKs2によって暗号化する。暗号化処理部３２８より出力された暗号化データ{{{Kc//AC2｝Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1}Km(1)}Ks2は、データバスBS1および通信装置３５０を介して携帯電話機１００に送信される（ステッ

プＳ１３８）。
このように、送信サーバ３０およびメモリカード１１０でそれぞれ生成されるセッションキーをやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。
携帯電話機１００は、送信された暗号化データ{{{Kc//AC２} Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1}Km(1)}Ks2を受信し（ステップＳ１４０）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスBS３に与えられた受信データを復号化処理部１４１２によって復号する。すなわち、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーKs２を用いてデータバスBS３の受信データを復号しデータバスBS４に出力する。
この段階で、データバスBS４には、Km（１）保持部１４２１に保持される秘密復号鍵Km（１）で復号可能なデータ{{Kc//AC２} Kcom//ライセンスＩＤ//コンテンツＩＤ//CA1}Km(1)が出力される。このデータ{{Kc//AC２} Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1}Km(1)がメモリ１４１５に記録される（ステップＳ１４４）。
さらに、復号処理部１４２２において、メモリカード１１２に固有の秘密復号鍵Km（１）による復号処理を実施することにより、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報AC1は、データバスBS４を介してライセンス情報保持部１４４０に記録される(ステップＳ１４８）。
さらに、ライセンスID、コンテンツIDおよびアクセス制御情報AC１については、ライセンス情報保持手段１４４０に記録される（ステップＳ１５０）。
ステップＳ１５０までの処理が正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ１５２）。
配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ {Data} Kcおよび付加データDATA-infを取得して、これらのデータをデータバスBS１および通信装置３５０を介して出力する（ステップＳ１５４）。
携帯電話機１００は、 {Data} Kc//Data-infを受信して、暗号化コンテンツデータ {Data} Kcおよび付加データData-infを受理する（ステップＳ１５６）。暗号化コンテンツデータ {Data} Kcおよび付加データData-infはメモリインタフェース１２００および端子１２０２を介してメモリカード１１０のデータバスBS３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ {Data} Kcおよび付加データData-infがそのままメモリ１４１５に記録される（ステップＳ１５８）。
さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ１６０）、配信サーバ３０で配信受理を受信すると（ステップＳ１６２）、課金データベース３０２への課金データの格納等を伴って、配信終了の処理が実行され（ステップＳ１６４）、配信サーバの処理が終了する（ステップＳ１７０）。
一方、携帯電話機１００は再生処理における再生初期化セッションを開始する。以後の処理は、後に図６に示す再生初期化セッションと同一の処理を行なう。ステップＳ１７２、Ｓ１７４、Ｓ１７６、Ｓ１７８、Ｓ１８０がそれぞれ、図６におけるステップＳ２０２、Ｓ２０４、Ｓ２０６、Ｓ２０８、Ｓ２１０にあたる。
このように、配信セッションにおける携帯電話機１００は、配信によるコンテンツデータの記録が終了するとすぐに再生に備えて再生初期化セッションを実行することによって、ユーザは再生をタッチキー部１１０８を介して入力する以前に再生初期化セッションを終了し、ユーザの再生の要求に対して、セキュリティー強度を保った上で、迅速にコンテンツデータを再生して音楽の再生を開始できるようになる。
さらには、配信リクエストに対して携帯電話機１００のコンテンツ再生部およびメモリカード１１０の送信してきた公開暗号鍵Kp（１）、Kmc（１）が有効であることを確認した上でのみ、コンテンツデータを配信することができるため、不正な機器への配信を禁止することができ、さらに、受信側に依存する鍵を用いた暗号化を行なってデータの送受信を

するため、配信におけるセキュリティ強度が確保されている。
［移動動作］
次に、２つのメモリカード間においてコンテンツデータの移動を行なう処理を説明する。図１１、図１２および図１３は、２つのメモリカード１１０および１１２の間で携帯電話機１００および１０２を介してコンテンツデータおよび鍵等の移動を行なう処理を説明するための第１、第２および第３のフローチャートである。
図１０～図１２においては、携帯電話機１００およびメモリカード１１０についての種類を識別するための自然数をｎをともに１とし、携帯電話機１０２およびメモリカード１１２についての種類を認識するため自然数をｎをともに２とする。また、メモリカード１１０および１１２を識別するための自然数ｉは、それぞれｉ＝１およびｉ＝２であるものとする。
図１０～図１２においては、携帯電話機１００およびメモリカード１１０が送信側であり、携帯電話機１０２およびメモリカード１１２が受信側であるものとする。また、携帯電話機１０２も、メモリカード１１０と同様の構成を有するメモリカード１１２が装着されているものとする。以下、メモリカード１１２の各構成部分については、メモリカード１１０の対応する部分と同一の符号を用いて説明する。
図１０を参照して、まず、送信側であるユーザ１の携帯電話機１００から、ユーザによりタッチキー部１１０８のキーボタンの操作等によって、コンテンツ移動リクエストがなされる。（ステップＳ３００）。
生成された移動リクエストは、受信側であるユーザ２の携帯電話機１２０を介してメモリカード１１２に伝達される。メモリカード１１２においては、認証データ保持部１５００より、メモリカード１１２に対応する公開暗号鍵KPmc（２）が認証データ｛KPmc（２）｝KPmaが出力される（ステップＳ３０２）。
メモリカード１１２の認証用データ｛KPmc（２）｝KPmaは、ユーザ２の携帯電話機１２０から送信され、ユーザ１の携帯電話機１１０を経由してメモリカード１１０に受信される（ステップＳ３０４）。
メモリカード１１０においては、復号処理部１４０８にて復号処理を実行する。この、KPmaにて暗号化された公開暗号鍵KPmc（２）が正規に登録され、正規の暗号化を施されている場合、すなわち、認証鍵KPmaにて復号でき、復号時に発生する従属するデータが認識できる場合、復号したKPmc（２）をメモリカード１１２の公開暗号鍵として受理する。一方、復号できない場合、または、信号処理において発生する従属データが認識できない場合、得られたデータを受理しない（ステップＳ３０６）。
コントローラ１４２０は、復号処理部１４０８にてメモリカード１１２のコンテンツに固有の公開暗号鍵KPmc（２）が受理された場合、送信されてきた公開暗号鍵KPmc（２）が、このデータ配信システムに対して承認されたメモリカードに付与された公開暗号鍵であると判断し、次のステップＳ３１２に進める（ステップＳ３０８）。一方、受理されなかった場合、非承認の機器からの不正なアクセスであると判断し、処理を終了する（ステップＳ３６０）。
認証結果が有効である場合には、コントローラ１４２０は、セッションキー発生部１４１８に対して、移動セッション時に送信側で発生されるセッションキーKs３の出力を指示する。移動セッションにおける受信側では、メモリカード１１０のセッションキー発生部１４１８にて新しいセッションキーを発生したため、再生初期化セッションにおいて保持したセッションキーKs３がセッションキーKs２に書換えられる。セッションキー発生部１４１８によって生成されたセッションキーKs３は、暗号化処理部１４１０に伝達される。暗号化処理部１４１０は、さらに、ステップＳ３０６において復号処理部１４０８によって復号されたメモリカード１１２の秘密暗号鍵KPmc（２）を受けて、KPmc（２）によってセッションキーKs３を暗号化する。これにより、暗号化されたセッションキー｛Ks３｝Kmc（２）がデータバスBS３に出力される（ステップＳ３１４）。
データバスBS３に出力された｛Ks３｝Kmc（２）は、メモリインタフェース１２００、携帯電話機１００および携帯電話機１２０を介してメモリカード１１２に伝達される。

メモリカード１１２は、メモリカード１１０から出力された｛Ks３｝Kmc（２）を受けて、復号処理部１４０４によってメモリカード１１２に対応する秘密復号鍵Kmc（２）による復号処理を実行し、送信側のメモリカード１１０によって生成されたセッションキーKs３を受理する（ステップＳ３１６）。
メモリカード１１２のコントローラ１４２０は、セッションキーKs３の受理に応じて、セッションキー発生部１４１８に対して、移動セッションにおいて受信側で発生されるべきセッションキーKs２の生成を指示する。移動セッションにおける受信側では、メモリカード１１０中のセッションキー発生部１４１８にて新しいセッションキーを発生したため、再生初期化セッションにおいて保持したセッションキーKs３がセッションキーKs２に書き換えられる。生成されたセッションキーKs２は、切換スイッチ１４４６中の接点Pfおよび切換スイッチ１４４４中の接点Pcを経由して暗号化処理部１４０６に伝達される。
暗号化処理部１４０６は、復号処理部１４０４からステップＳ３１６で得られたセッションキーKs３を受けて、切換スイッチ１４４４の接点Pcと切換スイッチ１４４６の接点PfとPeの切換によって得られるセッションキーKs２と公開暗号鍵KPm（２）をセッションキーKs１によって暗号化し、｛Ks２//KPm（２）｝Ks３をデータバスBS３に出力する（ステップＳ３１８）。
データバスBS３に出力された暗号化データ｛Ks２//KPm（２）｝Ks３は、携帯電話機１０２および１００を介してメモリカード１１０のデータバスBS３に伝達される。
メモリカード１１０においては、データバスBS３に伝達された暗号化データを復号処理部１４１２によってセッションキーKs３を用いて復号し、メモリカード１１２に関するセッションキーKs２および公開暗号鍵KPm（２）を受理する（ステップＳ３２０）。
メモリカード１１０のコントローラ１４２０は、セッションキーKs２および公開暗号鍵Kpm（２）の受理に応じて、ライセンス情報保持部１４４０内のアクセス制限情報AC１の確認を実行する（ステップＳ３２２）。アクセス制御情報AC１を確認した結果、ライセンスの移動が不可である場合には、この段階で移動セッションを終了する（ステップＳ３６０）。
一方、アクセス制限情報AC１を確認した結果、移動が許可されている場合には、次のステップＳ３２２に処理が移行し、コントローラ１４２０は、ライセンス情報保持部１４４０より対応するコンテンツIDおよびライセンスIDを取得し、ライセンス保持部１４４０内のアクセス制限情報を更新し、以降の再生および移動の禁止を記録する（ステップＳ３２４）。これに対応して、再生セッションおよび移動セッションにおいて当該アクセス制限情報AC１を確認して処理が行なわれ、以降のそれぞれのセッションが禁止される。
さらに、コントローラ１４２０は、移動するコンテンツに対応したセッションキーKcおよび再生情報に関する暗号化データ｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（１）の出力をメモリ１４１５に対して指示する。メモリ１４１５から出力された暗号化データ｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（１）は、復号処理部１４２２によって復号化され、｛Kc//AC２｝KcomがデータバスBS４上に得られる（ステップＳ３２６）。
ステップＳ３２４でライセンス情報保持部から取得されたライセンスID、コンテンツIDおよびアクセス制限情報AC１と、ステップＳ３２６で得られた｛Kc//AC２｝Kcomは、データバスBS４から暗号化処理部１４２４に取込まれて暗号化される。暗号化処理部１４２４は、ステップＳ３２０において復号処理部１４１２で得られたメモリカード１１２固有の公開暗号鍵KPm（２）によって、これらのデータを暗号化し、｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（２）を生成する（ステップＳ３２８）。
データバスBS４に出力された暗号化データ｛｛KC//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（２）は、切換スイッチ１４４４中の接点Pdを介して暗号化処理部１４０６に伝達される。暗号化処理部１４０６は、復号処理部１４１２によって得られたメモリカード１１２の生成したセッションキーKs２を切換スイッチ１４４２の接点Pdを介して受けて、接点Pdより受けたデータをセッションキーKs２によって暗号化する。
暗号化処理部１４０６は、｛｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝

Km（２）｝Ks２をデータバスBS３に出力する（ステップＳ３３０）。ステップＳ３３０においてデータバスBS３に出力された暗号化データは、携帯電話機１００および１０２を介して、移動セッションの受信側であるメモリカード１１２に伝達される。
メモリカード１１２においては、復号処理部１４１２においてセッションキー発生部１４１８によって生成されたセッションキーKs２による復号が実行され、｛｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（２）が受理される（ステップＳ３３２）。受理された｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（２）は、公開暗号鍵KPm（２）で暗号化されたまま記録される（ステップＳ３３４）。
さらに、復号処理部１４２２において、メモリカード１１２に固有の秘密復号鍵Km（２）による復号処理を実行することにより、ライセンスID、コンテンツIDおよびアクセス制限情報AC１が受理される（ステップＳ３３６）。
受理されたライセンスID、およびコンテンツIDおよびアクセス制限情報AC１は、データバスBS４を介してライセンス情報保持部１４４０に記録される（ステップＳ３３８）。
このようにして、ステップＳ３３８までの処理が正常に終了することによって、ライセンスキーKcの暗号化データおよび配信情報が移動されたことに応答して、携帯電話機１０２を介してコンテンツデータの複製要求がさらに行なわれる（ステップＳ３４０）。
コンテンツデータの複製要求は携帯電話機１００を経由してメモリカード１１０に伝達され、これに応答して、メモリカード１１０中のメモリ１４１５より対応する暗号化コンテンツデータ｛Data｝Kcと付加情報Data-infとがデータバスBS３に出力される（ステップＳ３４２）。データバスBS３に出力されたこれらのデータは、メモリインタフェース１２００、携帯電話機１００および携帯電話機１０２を介してメモリカード１１２に伝達され、メモリカード１１２中のメモリ１４１５に記録される（ステップＳ３４４）。
暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data-infの記録が終了すると、携帯電話機１０２を介して移動受理が送信される（ステップＳ３４６）。
これにより、メモリカード１１２および対応する携帯電話機１０２において正常に再生セッションが実行されれば、携帯電話機１０２によって、メモリカード１１２に記録されたコンテンツデータに基づいて音楽を聴取することが可能となる。
送信側の携帯電話機１００においては、携帯電話機１０２から送信された移動受理を受信して（ステップＳ３４８）、コンテンツデータの消去もしくは保持のいずれかの指示をキー入力部１１０８よりユーザから受ける（ステップＳ３５０）。
したがって、キー入力部１１０８よりコンテンツデータの消去が指示されることにより、メモリカード１１０内のメモリ１４１５において、対応する｛Data｝Kcおよび付加情報Data-infが消去される（ステップＳ３５４）。一方、コンテンツデータの保持が指示された場合においては、ステップＳ３５４はスキップされ、移動処理はこの段階で終了する（ステップＳ３５６）。
正常に移動セッションが行なわれた場合の移動処理終了ステップＳ３５６の後、もしくは認証等によって移動セッションが中止された場合にはステップＳ３０８およびＳ３２２からスキップされて、次のステップＳ３５８に処理が移行する。
なお、ライセンス保持部１４４０内に記録された対応するコンテンツＩＤ等の再生情報は、ステップＳ３２４にてアクセス制限情報AC１が更新され、再生セッションおよび移動セッションを禁止しているため、消去と同じ状態となっている。この状態にある再生情報が記録されたバンクに対して、新たなコンテンツデータに対する再生情報の配信あるいは移動を受けた際に、上書きが許可されている。ステップＳ３２４において、当該バンク内のデータを全て消去しても同様な効果が得られる。
さらに、暗号化コンテンツデータをメモリ１４１５に記録された状態では、新たに配信サーバ３０をアクセスし、再生情報の配信のみ受ければ、また、暗号化コンテンツデータを再生して、音楽を聴取することができるようになる。再生情報のみの配信処理はフローチャートには図示されていないが、配信セッションにおける図９および図１０において暗号化コンテンツデータの授受に関するステップＳ１５２、Ｓ１５４、Ｓ１５６、Ｓ１５８を行わない処理であるため、説明を繰り返さない。

携帯電話機１００は、ステップＳ３５６において移動処理が終了すると、メモリカード１１０に対して認証のためのデータ[KPp(1)]Kpmaを出力する（ステップＳ３５８）。
メモリカード１１０は、携帯電話機１００からのデータ[KPp(1)]Kpmaを受けて、復号処理部１４０８がキーKpmaにて復号することで、キーKPp(1)を受理する（ステップＳ３６０）。
メモリカード１１０では、コントローラ１４２０が受理されたキーKPp(1)に基づいて、携帯電話機１００の認証を行なう（ステップＳ３６２）。
携帯電話機１００は、ステップＳ３５６において移動終了処理が終了すると、メモリカード１１０との間で、再生初期化セッションを開始する。以降、ステップＳ３５８、Ｓ３６０、Ｓ３６２、Ｓ３６４、Ｓ３６６は、図６におけるステップＳ２０２、Ｓ２０４、Ｓ２０６、Ｓ２０８、Ｓ２１０にあたるため、繰り返し説明は行わない。携帯電話機１００は再生初期化セッションが終了すると携帯電話機１００の処理を終了する（ステップＳ３９０）。
一方、携帯電話機１０２は、ステップＳ３４６において移動受理を送信すると、メモリカード１１０との間で、再生初期化セッションを開始する。以降、ステップＳ３４８、Ｓ３５０、Ｓ３５２、Ｓ３５４、Ｓ３５６は、図６におけるステップＳ２０２、Ｓ２０４、Ｓ２０６、Ｓ２０８、Ｓ２１０にあたるため、繰り返し説明は行わない。携帯電話機１０２は再生初期化セッションが終了すると携帯電話機１０２の処理を終了する（ステップＳ３９０）。
このように、移動セッションにおける送信側の携帯電話機１００および受信側携帯電話機１０２は、移動によるコンテンツデータの授受が終了するとすぐに再生に備えて再生初期化セッションを実行することによって、それぞれのユーザがそれぞれの携帯電話機のタッチキー部１１０８を介し再生を指示する以前に再生初期化セッションを終了し、ユーザの再生の要求に対して、セキュリティ強度を保った上で、迅速にコンテンツデータを再生して音楽の再生を開始できるようになる。
さらには、移動リクエストに対して、送信側メモリカード１１０は、受信側のメモリカード１１２の送信してきた公開暗号化Kmc（２）が有効であることを確認した上でのみライセンスキー等の再生情報を移動させるため、不正なメモリカードへの移動を禁止することができ、さらに、受信側に依存した鍵を用いて暗号化を行った上でデータの送受信をするため、移動セッションに対するセキュリティ強度が確保されている。

［実施例２］

実施例２のデータ配信システムにおいては、実施例１のデータ配信システムの構成と異なって、以下に説明するように、暗号鍵と復号鍵が非対称な公開暗号化方式における公開鍵暗号鍵Km(1)で暗号化された上で配信された暗号化ライセンスキー等のデータ {{Kc//AC２} Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1}Km(1)をキーKm(1)で復号した後、対称型の鍵であってメモリカード固有の秘密共通鍵K(i)により暗号化しなおした上で、メモリ１４１５に格納する点を特徴とする。
すなわち、実施例２のデータ配信システムは、図５において説明した、実施例１のデータ配信システムが具備するメモリカード１１０に代えてメモリカード１１４を備える点で異なる。
図１４は、実施例２のデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図であり、実施例１の図２と対比される図である。ただし、図１４においては、図２の場合と比べて、上述のとおり、対称型の鍵であってメモリカード固有の秘密共通鍵K(i)が設けられる構成となっている点が異なるのみであるので、その説明は繰り返さない。
図１５は実施例２のメモリカード１１４の構成を示すブロック図であり、実施例１の図５と対比される図である。
図１５を参照して、メモリカード１１４は、図５に示す実施例１のメモリカード１１０と比較して、メモリカード固有の秘密共通鍵K（１）を保持するK（１）保持部１４５０と、データバスＢＳ４上のデータを秘密共通鍵K（１）により暗号化する暗号化処理部１４５

２と、データバスＢＳ４上のデータを秘密共通鍵K（１）により復号する復号処理部１４５４とをさらに備える構成となっている点で異なる。
その他の点は、実施例１のメモリカード１１０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。
図１６、図１７および図１８は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第１、第２および第３のフローチャートであり、実施例１の図８、図９および図１０と対比される図である。
図１６～図１８においては、ユーザ１が、メモリカード１１４を用いることで、携帯電話機１００を介して配信サーバ３０からコンテンツデータの配信を受ける場合の動作を説明している。
ここで、実施例１のメモリカード１１０の場合の配信処理と異なる点は、ステップＳ１４４の処理により、メモリカード１１４がデータ{{Kc//AC２} Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1}Km(1)を受理した後に、コントローラ１４２０の指示によって、データ{{Kc//AC２} Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1}Km(1)は、復号処理部１４２２において、秘密復号鍵Km（１）によって復号され、データ{Kc//AC２} Kcom、ライセンスID、コンテンツIDおよびアクセス制限情報AC１が受理され（ステップＳ１４６′）ることである。さらに、このようにして受理された {Kc//AC2} Kcom、ライセンスID、コンテンツIDおよびAC1は、メモリカード１１４に固有の秘密共通鍵K（１）によって暗号化処理部１４５２で暗号化され、｛{Kc//AC2} Kcom//ライセンスID//コンテンツID//AC1} K（１）がTRM領域外のメモリ１４１５に記録される（ステップＳ１４８′）。
以上の配信処理において、ステップＳ１４６において、{Kc//AC2} Kcom、ライセンスID、コンテンツIDおよびAC1を秘密復号鍵Km（１）によって復号した後、ステップＳ１４８′において、再び秘密共通鍵K（１）によって暗号化した上でメモリ１４１５に格納するのは、以下の理由による。
非対称鍵による公開鍵方式である公開暗号鍵KPm（１）と秘密復号鍵Km（１）の組合せでは、復号処理に要する時間が大きくなる可能性がある。
そこで、高速に復号可能な共通鍵方式によるメモリカード固有の秘密共通鍵K（１）によって、これらのデータを暗号化しなおすことで、暗号化コンテンツデータに対応するコンテンツデータの再生処理において、再生処理に必要な情報であるライセンスキーKcおよび再生制限情報AC1に対する復号処理を高速化することが可能となる。
さらには、このようにデータ送信時の鍵と、メモリカード内に格納する際の鍵を変更することで、セキュリティー強度も向上する。
ここで、上述したような公開鍵方式としては、ＲＡＳ暗号方式（Rivest-Shamir-Adleman cryptosystem）や楕円曲線暗号化方式があり、共通鍵暗号方式としては、ＤＥＳ（Data Encryption Standard）暗号方式などがある。
なお、以上の説明では、暗号鍵と復号鍵が非対称な公開暗号化方式における鍵KPm（１）／Km（１）に基づく暗号化データを、全て暗号鍵と復号鍵が対称な共通鍵方式における秘密共通鍵K（１）で暗号化しなおす構成について説明したが、たとえば、メモリカード１１０のＴＲＭ領域内に設けられたライセンス情報保持部１４４０に保持されるライセンスID、コンテンツIDおよびアクセス制御情報AC１については、暗号化のやり直しを行なわず、かつメモリ１４１５に格納することをやめ、データ {Kc//AC2} Kcomについては、秘密共通鍵K（１）で暗号化しなおした上でメモリ１４１５に格納する構成とすることも可能である。
その他の点は、実施例１の配信動作と同様であるので、同一処理には同一符号を付してその説明は繰り返さない。
図１９は、実施例２のメモリカード１１４を用いた場合の再生セッション時における各部の動作を説明するためのフローチャートである。
ここで、実施例２のメモリカード１１４においても、実施例１のメモリカード１１０と同様にして、再生初期化セッションの処理が行なわれているものとする。
図１０に示した実施例１のメモリカード１１０の場合の配信処理と異なる点は、メモリカ

ード１１４においては、図１９のステップＳ２２２′の処理では、コントローラ１４２０の指示に応じて、メモリ１４１５からデータバスBS４に読出された暗号化データ｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝K（１）を、復号処理部１４５４がK（１）保持部１４５１の保持された秘密鍵K（１）によって復号する構成となっていることである。
その他の点は、実施例１の再生動作と同様であるので、同一処理には同一符号を付してその説明は繰り返さない。
［移動動作］
図２０、図２１、および図２２は、実施例２における移動の動作を説明するための第１、第２および第３のフローチャートである。
また、実施例２のメモリカードの移動動作も基本的には、実施例１の移動動作と同様である。
実施例１のメモリカード１１０と１１２との間の移動動作に対して、実施例２のメモリカード１１４と１１６との間の移動動作の異なるステップはステップＳ３２６′、Ｓ３３４′およびＳ３３６′である。ステップＳ３２６′においては、コントローラ１４２０は、移動するコンテンツに対応したセッションキーKcおよび再生情報に関する暗号化データ｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝K（１）の出力をメモリ１４１５に対して指示し、メモリ１４１５から出力された暗号化データ｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝K（１）は、復号処理部１４５４によって秘密共通鍵K（１）について復号化され、｛Kc//AC２｝Kcomがデータバス BS４上に得られる。
ステップＳ３３４′においては、ステップＳ３３２にて受理された｛｛Kc//AC２｝Kcom//ライセンスID//コンテンツID//AC１｝Km（２）をメモリカード１１６固有の秘密復号鍵Km（２）にて復号処理部１４２２にて復号し、｛Kc//AC２｝Kcom、ライセンスID、コンテンツID、アクセス制限情報AC１をデータバスBS４に出力する。
ステップＳ３３６′においては、ステップＳ３３４′にてデータバスBS４に出力された、｛Kc//AC２｝Kcom、ライセンスID、コンテンツID、アクセス制限情報AC１を、秘密共通鍵K（２）にて暗号処理部１４５２にて再び暗号化した後、データバスBS４を介してメモリ１４１５に記録される。
その他の点は、実施例１の移動動作と同様であるので、同一処理には同一符号を付してその説明は繰り返さない
以上のような構成とすることで、一層、迅速に再生が開始できるようになるとともに、コンテンツデータに対するセキュリティーが強化されることになる。
なお、実施例１および２における処理はメモリカード内の処理が異なるだけで、メモリカード外部におけるデータの暗号化に違いはない。移動動作についても送り側と受信側の組合せとしてこれまでに説明したきた実施例１と２のいずれの組合せにおいても移動が行える。
ゆえに、メモリカード１１０および１１４は互換性のあるメモリカードである。
［実施例３］
実施例３のデータ配信システムにおいては、実施例１のデータ配信システムの構成と異なって、配信サーバおよび携帯電話機のコンテンツ再生回路においてコンテンツ再生回路共通の秘密鍵Kcomによる暗号化および復号処理を用いない点を特徴とする。
すなわち、実施例３のデータ配信システムは、図３において説明した、実施例１のデータ配信システムが具備する配信サーバ３０内のライセンスサーバ１０に代えてライセンスサーバ１１を備える点で異なる。また、実施例３のデータ配信システムにおける携帯電話機の構成は、図４で説明した携帯電話機１００の構成に代えて、携帯電話機１０３の構成が採用される。
図２３は、実施例３のデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図であり、実施例１の図２と対比される図である。ただし、図２３においては、図２の場合と比べて、秘密復号鍵Kcomが省略された構成となっている点が異なるのみであるのでその説明は繰り返さない。

図２４は、実施例３に従うデータ配信システムのライセンスサーバ１１の構成を示す概略ブロック図である。
ライセンスサーバ１１は、ライセンスサーバ１０と比較して、再生回路共通の秘密復号鍵Kcom保持部３２２と、秘密鍵Kcomを暗号鍵として暗号化を行う暗号化処理部３２４を具備しない点で異なる。すなわち、配信サーバ３１においては、配信制御部３１５が出力するライセンスキーKcおよび再生回路制御情報AC２は、直接暗号化処理部３２６に伝達される。その他の回路構成および動作については図３に示すライセンスサーバ１０と同様であるので説明は繰返さない。
以降、ライセンスサーバ１１、認証サーバ１２および配信キャリア２０を併せて配信サーバ３１と総称することとする。
図２５は、実施例３に従うデータ配信システムにおいて使用される携帯電話機１０３の構成を示す概略ブロック図である。
図２５を参照して、携帯電話機１０３は、実施例１の図４で説明した携帯電話機１００の構成と比較して、再生回路共通の秘密鍵Kcomを保持するKcom保持部１５１２と秘密鍵Kcomによる復号処理部１５１４を具備しない点で異なる。
すなわち、携帯電話機１０３においては、配信サーバ３１において秘密鍵Kcomによる暗号化処理が施されていないことに対応して、セッションキーKs４による復号処理を実行する復号処理部１５１０によって直接ライセンスキーKcが得られるため、これを復号処理部１５１０に直接与える構成となる。その他の回路構成および動作については携帯電話機１００の場合と同様であるので説明は繰返さない。
また、実施例３に従うデータ配信システムにおいて使用されるメモリカードについては、図５に示すメモリカード１１０と同一の構成であるので説明は繰返さない。
次に、再生回路共通の秘密鍵Kcomによる暗号化を省略することによる、配信および再生の各セッションにおける動作の差異についてフローチャートで説明する。
図２６、図２７および図２８は、実施例３に従うデータ配信システムにおける配信動作を説明するための第１、第２および第３のフローチャートである。図２６～図２８においては、図８～図１０で示した実施例１に従うデータ配信システムにおける配信動作のフローチャートと異なる点について説明する。
図２６～図２８を参照して、ステップＳ１３２までの処理は、図９で説明したフローチャートと同一である。
図２４で説明したように、ステップＳ１３２で得られるライセンスキーKcおよび再生回路制御情報AC２は、秘密鍵Kcomによる暗号化を施されることなくメモリカード１１０固有の公開暗号鍵KPm（１）によって暗号化されるので、ステップＳ１３４は省略される。
以下、ステップＳ１３２に続いて、ステップＳ１３６～Ｓ１４８に代えて、ステップＳ１３６ａ～Ｓ１４８ａが実行される。ステップＳ１３６ａ～Ｓ１４８ａのそれぞれにおいては、ステップＳ１３６～Ｓ１４８において取り扱われる｛Kc//AC２｝Kcomに代えて、ライセンスキーKcおよび再生回路制御情報AC２がKc//AC２の形でそのまま取扱われる点が異なる。その他の暗号化および復号処理については既に図９で説明したのと同様であるので説明は繰返さない。
図２９は、実施例３に従うデータ配信システムにおける再生動作を説明するためのフローチャートである。実施例３においても、再生初期セッションは、実施例１と同様の処理が行なわれているものとする。
図２９を参照して、実施例３に従うデータ配信システムにおける再生動作においては、図６に示した実施例１に従うデータ配信システムにおける再生動作と比較して、ステップＳ２２２～Ｓ２２６に代えて、ステップＳ２２２ａ～Ｓ２２６ａが実行される点で異なる。ステップＳ２２２ａ～Ｓ２２６ａのそれぞれにおいては、ステップＳ２２２～Ｓ２２６において取り扱われる｛Kc//AC２｝Kcomに代えて、ライセンスキーKcおよび再生回路制御情報AC２がKc//AC２の形でそのまま取扱われる点が異なる。その他の暗号化および復号処理については既に図１０で説明したのと同様であるので説明は繰返さない。さらに、また、ライセンスキーKcおよび再生回路制御情報AC２は、秘密復号鍵Kcomによる暗号化を施され

ることなくメモリカード１１０固有の公開暗号鍵Km（１）によって暗号化されているので、ステップＳ２２８は省略される。その他のステップについては図１０と同様であるので説明は繰返さない。

図３０、図３１および図３２は、実施例３の移動動作を説明するための第１、第２および第３のフローチャートである。

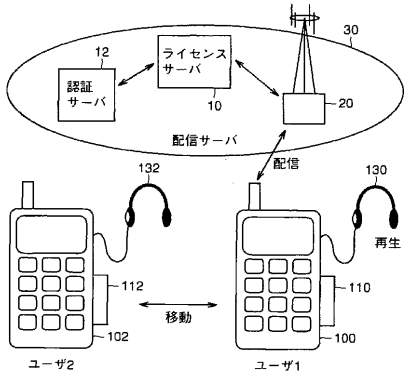
携帯電話機が１０３およびそれと同等の構成を有する携帯電話機１０５との間における移動動作においては、ライセンスキーKcおよび再生回路制御情報AC２は、秘密鍵Kcomによる暗号化を施されていないことを除いて、実施例１の動作と同様である。つまり、ステップＳ３２６～Ｓ３３６がステップＳ３２６ａ～Ｓ３３６ａとなる点を除いては、実施例１の動作と同様であるので、その説明は繰り返さない。

このような構成とすることによって、コンテンツ再生回路（携帯電話機）に共通の秘密復号化鍵Kcomによるライセンスサーバ１１での暗号化処理および携帯電話機での復号処理を行わない構成としても、実施例１に従うデータ配信システムと同様の効果を享受するデータ配信システムを構築することが可能である。

さらに、同様にして、実施例２のデータ配信システムにおいても、配信サーバおよび携帯電話機において再生回路共通の秘密鍵Kcomによる暗号化および復号処理を用いない構成とすることが可能である。また、再生装置としては、携帯電話機でなくてもよく、配信を受けられる必要性もない。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

【図１】
FIG.1



【図２】
FIG.2

名称	機能・特徴	保持・発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて配布	配信サーバ
Data-inf	付加情報、コンテンツデータに関する著作関連あるいはサーバアクセス関連等の平文情報	配信サーバ
Kc	ライセンスキー 暗号化コンテンツデータを復号するための復号鍵	配信サーバ
Kp(n)/Kmc(n)	コンテンツ再生回路／メモリカードのクラスに固有な秘密復号鍵 nはクラスを識別するための識別子	携帯電話機 メモリカード
KPp(n)/KPmc(n)	Kp(n)/Kmc(n)にて復号可能な非対称な公開暗号化鍵 {KPp(n)}KPma/{KPmc(n)}KPmaの形で出荷時に記録され、 復号時において、復号された公開暗号鍵KPp(n)/KPmc(n)の正当性を示す付随情報が生成される。 nはクラスを識別するための識別子	携帯電話機 メモリカード
Kcom	再生回路共通の秘密復号鍵、暗号化されたKc,AC2の復号に利用 （非対称　配信サーバKPcom／再生回路Kcom　も良い）	配信サーバ 携帯電話機
KPma	認証鍵	配信サーバ
AC	利用者側からのライセンスに対する購入条件(機能限定、ライセンス数etc)	携帯電話機
AC1	メモリのアクセスに対する制限情報	配信サーバ
AC2	再生回路における制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵(iはカードを識別する識別子)	メモリカード
KPm(i)	Km(i)にて復号可能な非対称暗号化鍵	メモリカード
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信／移動(受)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生／移動(送信側)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	配信サーバ
ライセンスID	ライセンスの発行を特定できる管理コード(コンテンツIDをも含めて識別することも考えられる)	配信サーバ
トランザクションID	配信セッション毎に生成される配信セッションを特定できるコード（ライセンスIDとの兼用も可）	配信サーバ

【図３】

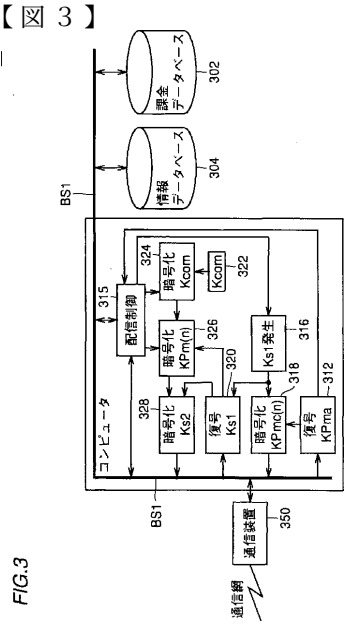


FIG.3

【図４】

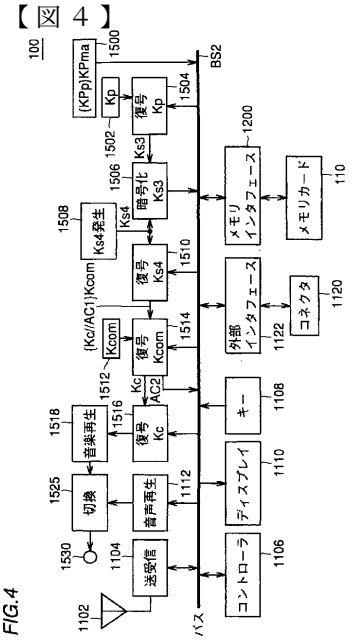


FIG.4

【図５】

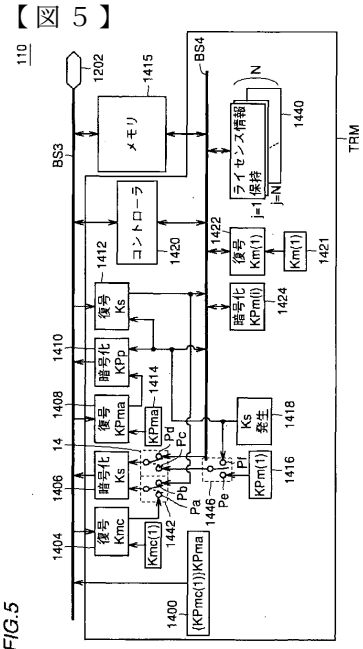
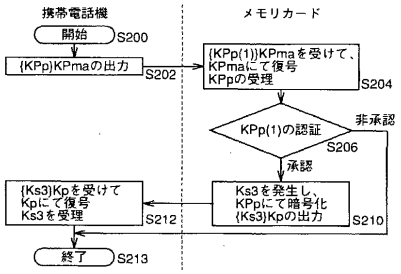


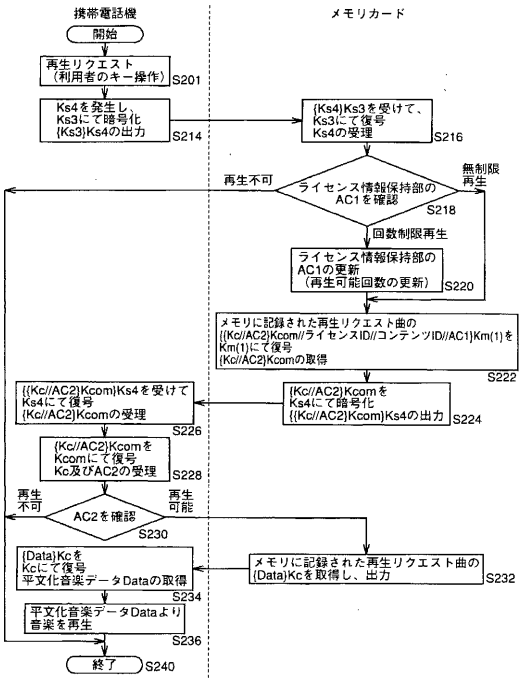
FIG.5

【図６】

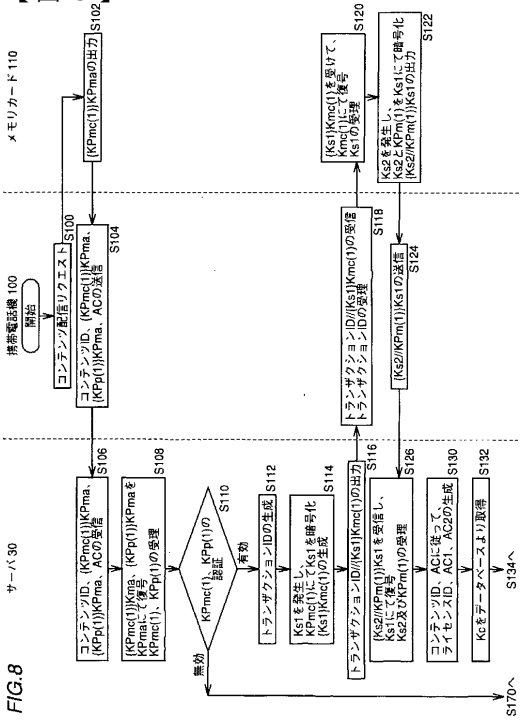
FIG.6



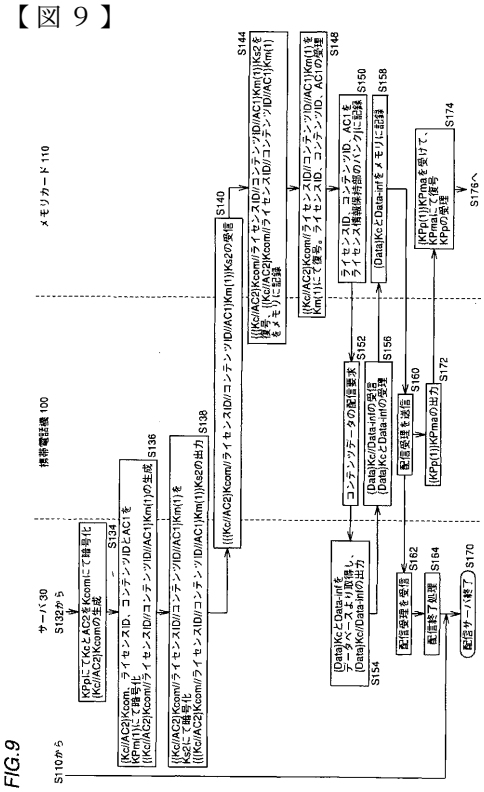
【図７】
FIG.7



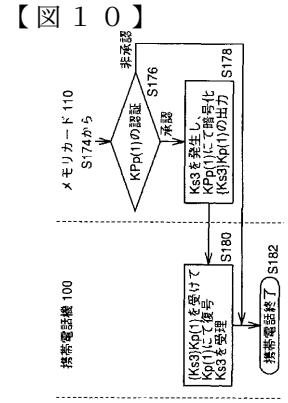
【図８】
FIG.8



【図９】
FIG.9



【図１０】
FIG.10



【図１１】

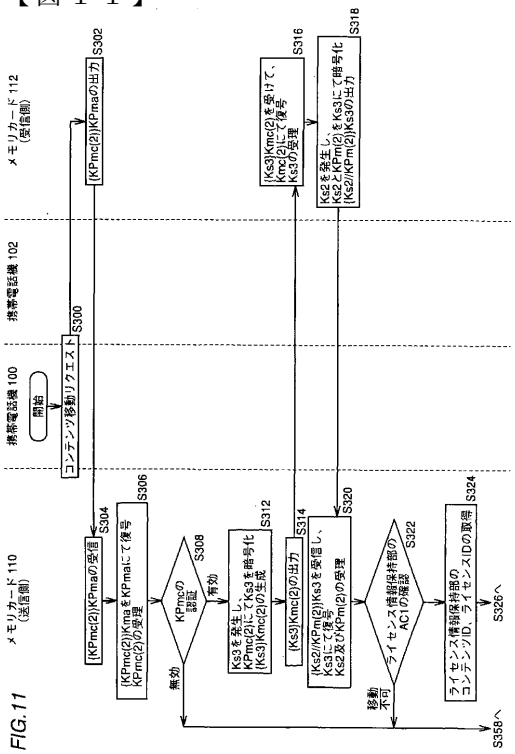


FIG.11

【図１２】

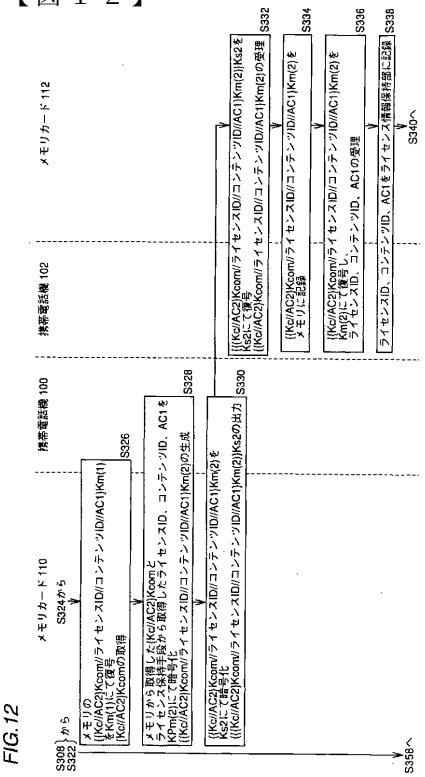


FIG.12

【図１３】

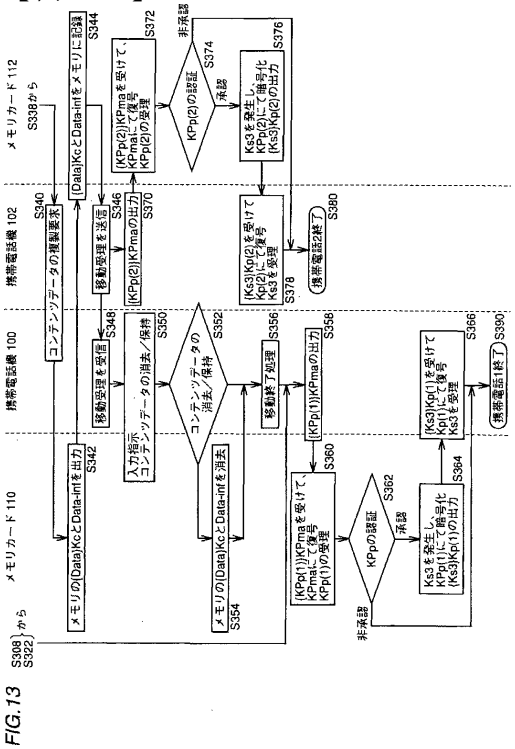


FIG.13

【図１４】

FIG.14

名称	機能・特徴	保持・発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて配布	配信サーバ
Data-inf	付加情報、コンテンツデータに関する著作関連あるいはサーバアクセス関連等の平文情報	配信サーバ
Kc	ライセンスキー 暗号化コンテンツデータを復号するための復号鍵	配信サーバ
Kp(n)/Kmc(n)	コンテンツ再生回路／メモリカードのクラスに固有な秘密復号鍵 nはクラスを識別するための識別子	携帯電話機 メモリカード
KPp(n)/KPmc(n)	Kp(n)/Kmc(n)にて復号可能な非対称な公開暗号化鍵 {KPp(n)}KPma/{KPmc(n)}KPmaの形で出荷時に記録され、 復号時において、復号された公開暗号鍵KPp(n)/KPmc(n)の正当性を示す付随情報が生成される。 nはクラスを識別するための識別子	携帯電話機 メモリカード
Kcom	再生回路共通の秘密復号鍵、暗号化されたKc,AC2の復号に利用 （非対称　配信サーバKPcom／再生回路Kcom　も良い）	配信サーバ 携帯電話機
KPma	認証鍵	配信サーバ
AC	利用者側からのライセンスに対する購入条件(機能限定、ライセンス数etc)	携帯電話機
AC1	メモリのアクセスに対する制限情報	配信サーバ
AC2	再生回路における制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵(iはカードを識別する識別子)	メモリカード
KPm(i)	Km(i)にて復号可能な非対称暗号化鍵	メモリカード
K(i)	対称型のメモリ固有の秘密鍵(iはカードを識別する識別子)	メモリカード
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信／移動(受)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生／移動(送信側)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	配信サーバ
ライセンスID	ライセンスの発行を特定できる管理コード(コンテンツIDをも含めて識別することも考えられる)	配信サーバ
トランザクションID	配信セッション毎に生成される配信セッションを特定できるコード（ライセンスIDとの兼用も可）	配信サーバ

【図１５】

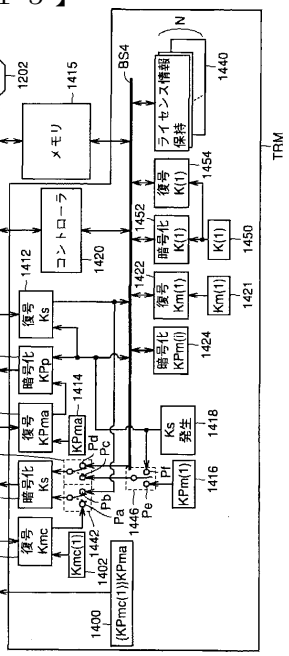


FIG.15

【図１６】

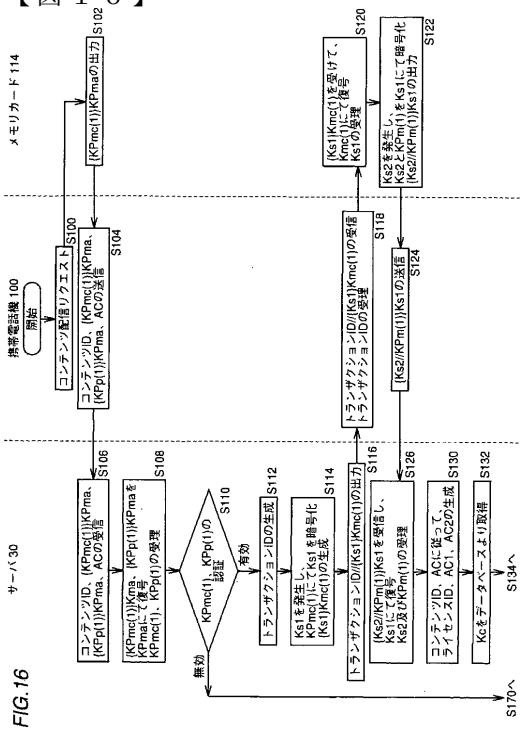


FIG.16

【図１７】

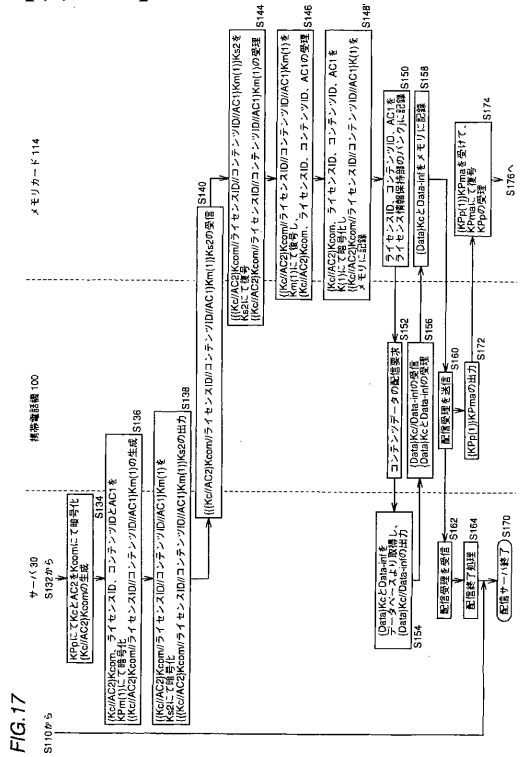


FIG.17

【図１８】

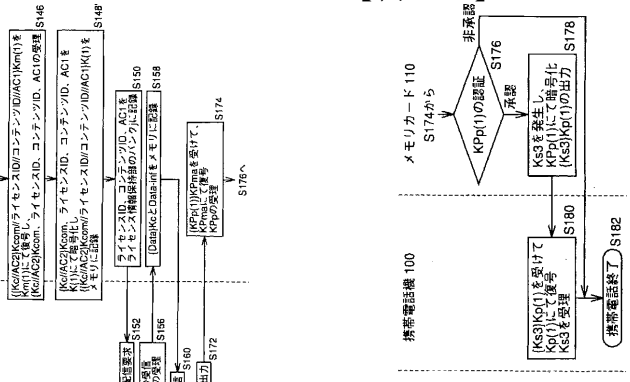
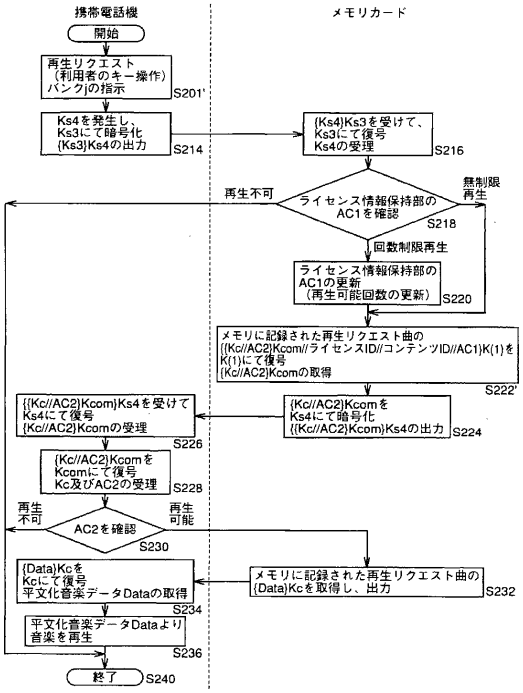
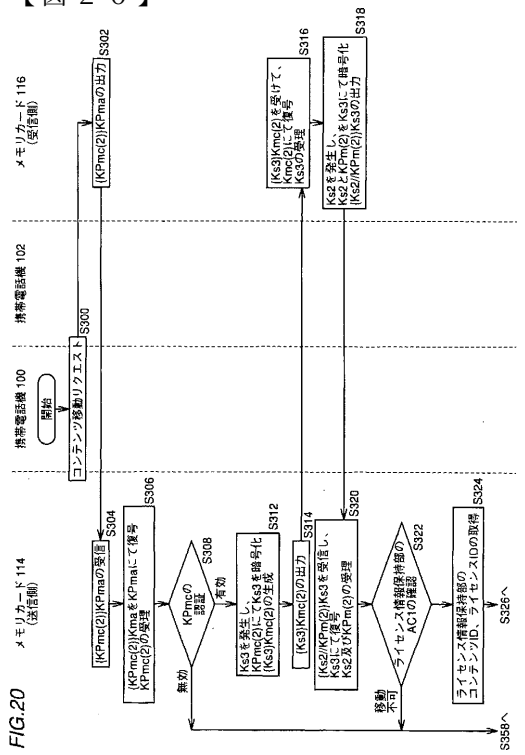


FIG.18

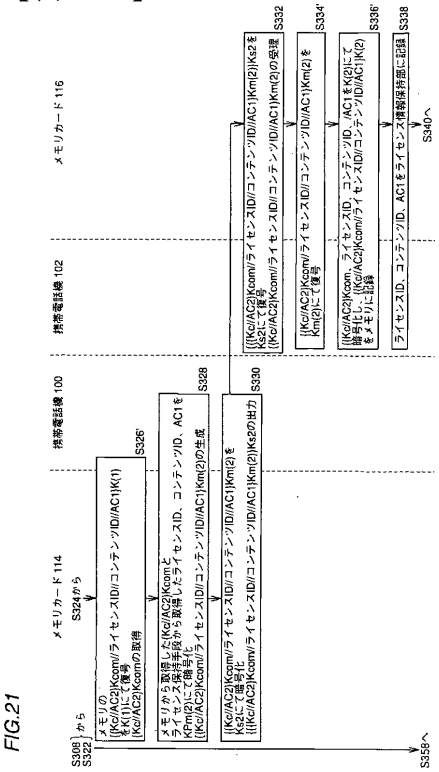
【図１９】
FIG.19



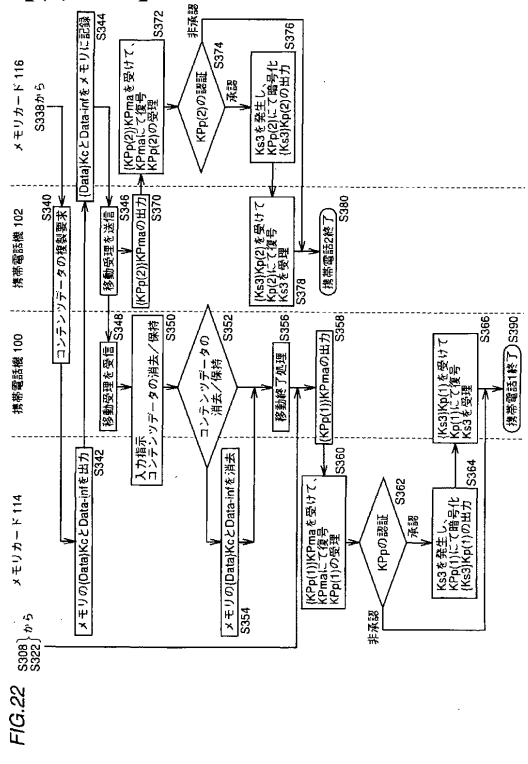
【図２０】
FIG.20



【図２１】
FIG.21



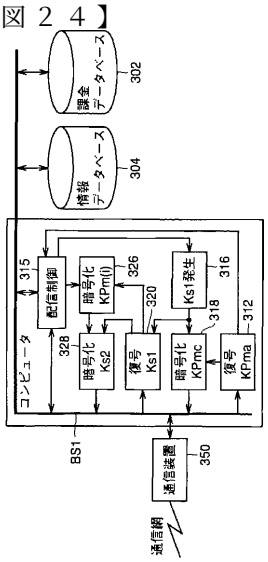
【図２２】
FIG.22



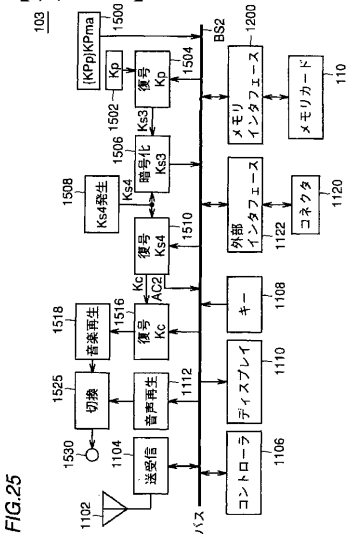
【図２３】
FIG.23

名称	機能・特徴	保持・発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて配布	配信サーバ
Data-inf	付加情報、コンテンツデータに関する著作関連あるいはサーバアクセス関連等の平文情報	配信サーバ
Kc	ライセンスキー 暗号化コンテンツデータを復号するための復号鍵	配信サーバ
Kp(n)/Kmc(n)	コンテンツ再生回路／メモリカードのクラスに固有な秘密復号鍵 nはクラスを識別するための識別子	携帯電話機 メモリカード
KPp(n)/KPmc(n)	Kp(n)/Kmc(n)にて復号可能な非対称な公開暗号化鍵 {KPp(n)}KPma/{KPmc(n)}KPmaの形で出荷時に記録され、 復号時において、復号された公開暗号鍵KPp(n)/KPmc(n)の正当性を示す付随情報が生成される。 nはクラスを識別するための識別子	携帯電話機 メモリカード
KPma	認証鍵	配信サーバ
AC	利用者側からのライセンスに対する購入条件(機能限定、ライセンス数etc)	携帯電話機
AC1	メモリのアクセスに対する制限情報	配信サーバ
AC2	再生回路における制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵(iはカードを識別する識別子)	メモリカード
KPm(i)	Km(i)にて復号可能な非対称暗号化鍵	メモリカード
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信／移動(受)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生／移動(送信側)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	配信サーバ
ライセンスID	ライセンスの発行を特定できる管理コード(コンテンツIDをも含めて識別することも考えられる)	配信サーバ
トランザクションID	配信セッション毎に生成される配信セッションを特定できるコード（ライセンスIDとの兼用も可）	配信サーバ

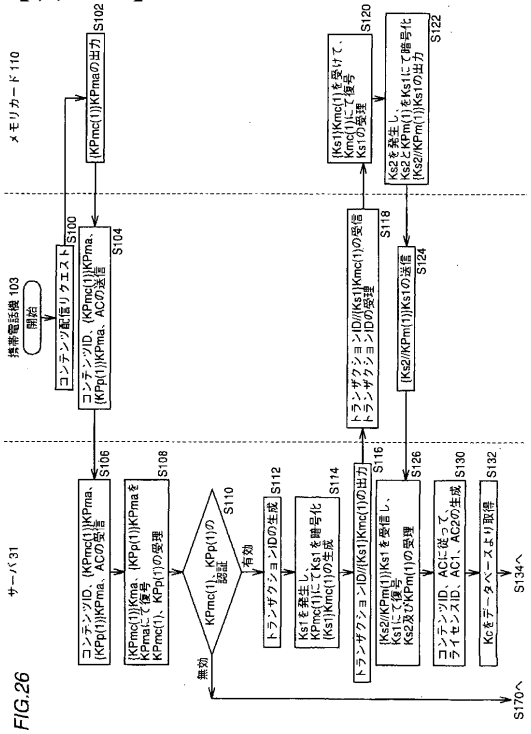
【図２４】
FIG.24



【図２５】
FIG.25



【図２６】
FIG.26



【図２７】

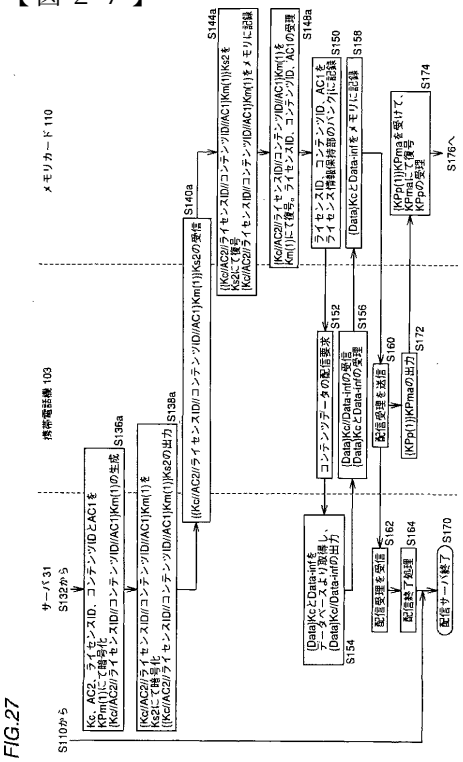


FIG.27

【図２８】

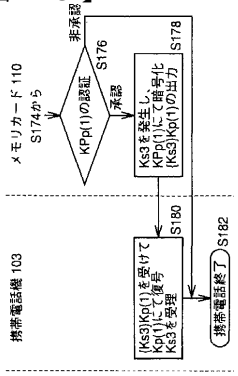
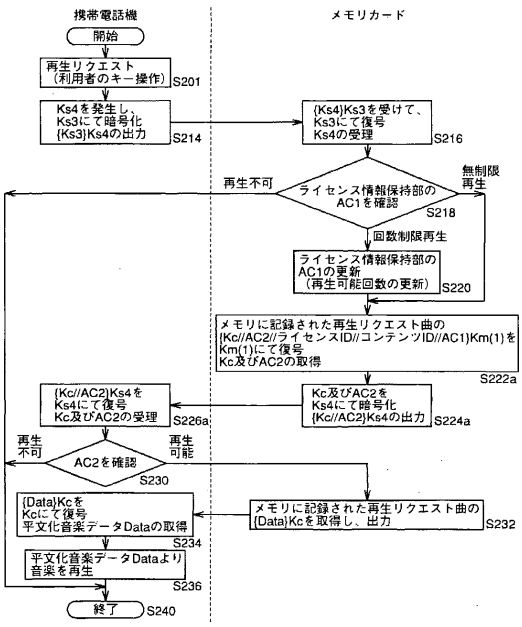


FIG.28

【図２９】

FIG.29



【図３０】

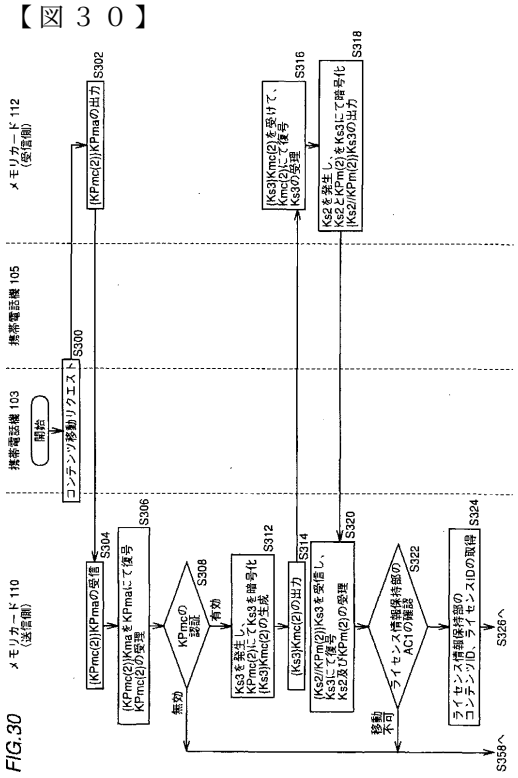


FIG.30

【図３１】

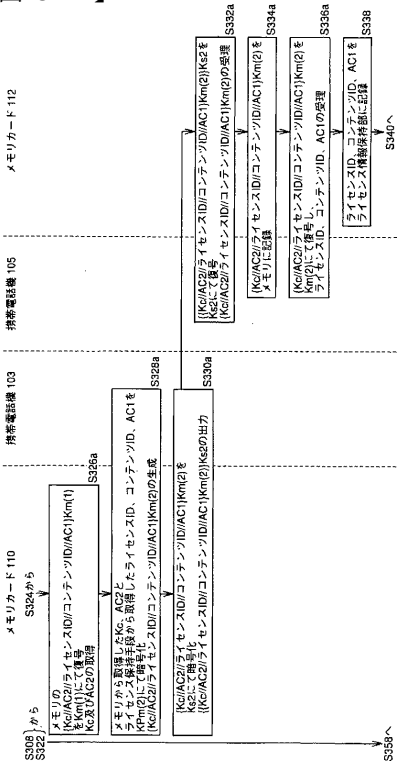


FIG.31

【図３２】

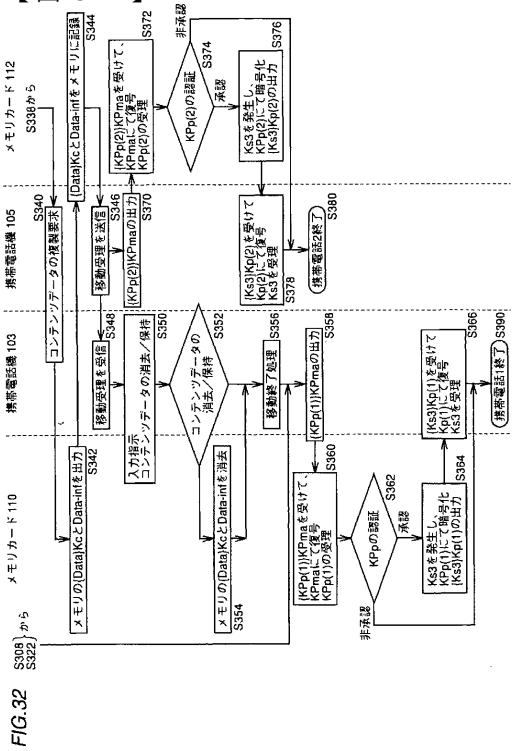


FIG.32

フロントページの続き

(51)Int.Cl.		FI		
H04L 9/10	***(2006.01)***	H04L	9/00	601A
		H04L	9/00	621A
		G10L	9/18	J

(74)代理人 100064746
弁理士 深見 久郎
(74)代理人 100085132
弁理士 森田 俊雄
(74)代理人 100083703
弁理士 仲村 義平
(74)代理人 100096781
弁理士 堀井 豊
(74)代理人 100098316
弁理士 野田 久登
(74)代理人 100109162
弁理士 酒井 將行
(72)発明者 堀 吉宏
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 日置 敏昭
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 金森 美和
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 吉川 隆敏
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 武村 浩司
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 長谷部 高行
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内
(72)発明者 畠山 卓久
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内
(72)発明者 利根川 忠明
東京都小平市上水本町五丁目２０番１号 株式会社日立製作所 半導体グループ内
(72)発明者 穴澤 健明
東京都港区赤坂四丁目１４番１４号 日本コロムビア株式会社内

審査官 青木 重徳

(56)参考文献 特開平１０－０４０１７２（ＪＰ，Ａ）
特開平０５－０７５５９８（ＪＰ，Ａ）
山中喜義，高嶋洋一，小柳津育郎，“マルチメディアオンデマンドサービスにおける情報保護システム”，ＮＴＴ Ｒ&Ｄ，日本，社団法人 電気通信協会，１９９５年 7月 9日，Ｖｏｌ．４４，Ｎｏ．１０，ｐ．８１３（１０１）－８１８（１０６）
“小型メモリ・カードで音楽著作権を守る”，日経エレクトロニクス，日本，日経ＢＰ社，１９９９年 3月２２日，３－２２，第７３９号，ｐ．４９－５３
岡本栄司，“暗号理論入門”，日本，共立出版株式会社，１９９３年 2月２５日，初版1刷，ｐ．１１０

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/08
G10K 15/02
G10L 19/00
H04L 9/10
H04L 9/32
H04N 7/167