

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4009108号
(P4009108)

(45) 発行日 平成19年11月14日(2007.11.14)

(24) 登録日 平成19年9月7日(2007.9.7)

(51) Int. Cl.	F I
G 1 O K 15/02 (2006.01)	G 1 O K 15/02
G O 6 F 21/20 (2006.01)	G O 6 F 15/00 3 3 O E
G O 6 Q 50/00 (2006.01)	G O 6 F 17/60 1 4 2
G O 6 F 21/24 (2006.01)	G O 6 F 12/14 5 4 O A
G O 6 K 19/07 (2006.01)	G O 6 F 12/14 5 4 O B
請求項の数 25 (全 61 頁) 最終頁に続く	

(21) 出願番号	特願2001-517375 (P2001-517375)	(73) 特許権者	000005223
(86) (22) 出願日	平成12年8月9日(2000.8.9)		富士通株式会社
(86) 国際出願番号	PCT/JP2000/005339		神奈川県川崎市中原区上小田中4丁目1番1号
(87) 国際公開番号	W02001/013358	(73) 特許権者	000004167
(87) 国際公開日	平成13年2月22日(2001.2.22)		コロムビアミュージックエンタテインメント株式会社
審査請求日	平成14年1月30日(2002.1.30)		東京都港区六本木一丁目4番33号 六本木21森ビル
(31) 優先権主張番号	特願平11-226406	(73) 特許権者	000001889
(32) 優先日	平成11年8月10日(1999.8.10)		三洋電機株式会社
(33) 優先権主張国	日本国(JP)		大阪府守口市京阪本通2丁目5番5号
(31) 優先権主張番号	特願平11-349336	(74) 代理人	100064746
(32) 優先日	平成11年12月8日(1999.12.8)		弁理士 深見 久郎
(33) 優先権主張国	日本国(JP)		最終頁に続く

(54) 【発明の名称】 メモリカード

(57) 【特許請求の範囲】

【請求項1】

暗号化コンテンツデータ ([Dc]Kc) を受けて記録するためのメモリカード (110,130,140,150,160,170) であって、

前記メモリカードに対応して予め定められた第1の公開暗号化鍵 (KPmedia) によって暗号化されたデータを復号化するための第1の秘密復号鍵 (Kmedia) を保持する第1の鍵保持部 (1402) と、

コンテンツキー (Kc) の通信ごとに更新されて配信され、前記第1の公開暗号化鍵 (KPmedia) によって暗号化された第1の共通鍵 ([Ks]Kmedia) を受けて、復号処理する (Ks) ための第1の復号処理部 (1404) と、

前記メモリカードごとに固有な第2の公開暗号化鍵 (KPcard(1)) を保持するための第2の鍵保持部 (1405) と、

前記第2の公開暗号化鍵 (KPcard(1)) を、前記第1の共通鍵 (Ks) に基づいて暗号化し ([Ks]Kcard(1))、出力するための第1の暗号化処理部 (1406) と、

前記第2の公開暗号化鍵 (KPcard(1)) で暗号化され、さらに前記第1の共通鍵 (Ks) で暗号化された前記コンテンツキー ([Kc]Kcard(1)]Ks) を受け、前記第1の共通鍵 (Ks) に基づいて復号化する ([Kc]Kcard(1)) ための第2の復号処理部 (1410) と、

前記第2の復号処理部 (1410) の出力を受けて、格納するための第1の記憶部 (1412) と、

前記第2の公開暗号化鍵 (KPcard(1)) によって暗号化されたデータを復号化するための第2の秘密復号鍵 (Kcard(1)) を保持する第3の鍵保持部 (1415) と、

10

20

前記第1の記憶部に格納されたデータ([Kc]Kcard(1))に基づいて、前記第2の秘密復号鍵(Kcard(1))により前記コンテンツキー(Kc)を復号するための第3の復号処理部(1416)とを備える、メモリカード。

【請求項2】

前記第1の記憶部(1412)は、前記コンテンツキー(Kc)に基づいて復号できる前記暗号化コンテンツデータ([Dc]Kc)を受けて格納する、請求項1記載のメモリカード。

【請求項3】

前記メモリカード(110,130,140,150,160,170)は、

外部から指示される動作モードに応じて、前記メモリカードの動作を制御するための制御部(1420)をさらに備え、

前記第1の暗号化処理部(1406)は、前記制御部に制御されて、前記コンテンツデータ(Dc)の再生動作が指示されるのに応じて、前記第3の復号処理部(1416)からの前記コンテンツキー(Kc)を受けて、前記第1の共通鍵(Ks)に基づいて暗号化して出力し([Kc]Ks)、

前記第1の記憶部(1412)は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータ([Dc]Kc)を出力する、請求項2記載のメモリカード。

【請求項4】

前記メモリカード(140,150,160,170)の前記第2の復号処理部(1410)は、前記第2の公開暗号化鍵(KPcard(1))で暗号化され、さらに前記第1の共通鍵(Ks)で暗号化されて、前記コンテンツキー(Kc)とともに配信されるライセンス情報データ([Kc,License-ID,User-ID]Kcard(1)]Ks)を受け、前記第1の共通鍵(Ks)に基づいて復号し([Kc,License-ID,User-ID]Kcard(1))、

前記第3の復号処理部(1416)は、前記第2の復号処理部(1410)から与えられる、第1の共通鍵(Ks)について復号され前記第2の公開暗号化鍵については暗号化された状態の前記ライセンス情報データ([Kc,License-ID,User-ID]Kcard(1))を復号し(Kc,License-ID,User-ID)、

前記第3の復号処理部からの復号された前記ライセンス情報データ(Kc,License-ID,User-ID)を格納するための第2の記憶部(1500)をさらに備える、請求項3記載のメモリカード。

【請求項5】

前記メモリカード(160,170)は、

前記メモリカードに対応して予め定められた第1の公開暗号化鍵(KPmedia)を保持し、外部に出力可能な第4の鍵保持部(1440)をさらに備える、請求項1記載のメモリカード。

【請求項6】

前記第1の記憶部(1412)は、前記コンテンツキー(Kc)に基づいて復号できる前記暗号化コンテンツデータ([Dc]Kc)を受けて格納する、請求項5記載のメモリカード。

【請求項7】

前記メモリカード(110,130,140,150,160,170)は、

外部から指示される動作モードに応じて、前記メモリカードの動作を制御するための制御部(1420)をさらに備え、

前記第1の暗号化処理部(1406)は、前記制御部(1420)に制御されて、前記コンテンツデータ(Dc)の再生動作が指示されるのに応じて、前記第3の復号処理部(1416)からの前記コンテンツキー(Kc)を受けて、前記第1の共通鍵(Ks)に基づいて暗号化して出力し([Kc]Ks)、

前記第1の記憶部(1412)は、前記制御部(1420)に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータ([Dc]Kc)を出力する、請求項6記載のメモリカード。

【請求項8】

前記第2の復号処理部(1410)は、前記第2の公開暗号化鍵で暗号化され、さらに前記第1の共通鍵(Ks)で暗号化されて、前記コンテンツキー(Kc)とともに配信されるライセンス

10

20

30

40

50

情報データ ([[Kc,License-ID,User-ID]Kcard(1)]Ks)を受け、前記第1の共通鍵(Ks)に基づいて復号し([[Kc,License-ID,User-ID]Kcard(1)))、

前記第3の復号処理部(1416)は、前記第2の復号処理部(1410)から与えられる、第1の共通鍵(Ks)について復号され前記第2の公開暗号化鍵については暗号化された状態の前記ライセンス情報データ ([[Kc,License-ID,User-ID]Kcard(1)))を復号し(Kc,License-ID,User-ID)、

前記第3の復号処理部(1416)からの復号された前記ライセンス情報データ (Kc,License-ID,User-ID)を格納するための第2の記憶部(1500)をさらに備える、請求項7記載のメモリカード。

【請求項9】

10

前記メモリカード(130,150,170)は、

第2の共通鍵(Ks)を生成するキーデータ生成部(1432)と、

前記第2の共通鍵(Ks)を、前記第1の公開暗号化鍵(KPmedia)によって暗号化する([[Ks]Kmedia))ための第2の暗号化処理部(1430)とをさらに備え

暗号化された前記第2の共通鍵([[Ks]Kmedia))は、前記メモリカードから前記他のメモリカードに送信される、請求項1記載のメモリカード。

【請求項10】

前記メモリカードは、

少なくとも前記第1の暗号化処理部(1406)と、前記第1の復号処理部(1404)と、前記第2の復号処理部(1410)と、前記第3の復号処理部(1416)とが設けられ、不当な開封処理に対しては、内部のデータが破壊されるタンパーレジスタンスモジュールにより構成され、ユーザが読出不可能なセキュリティ領域(TRM)と、

20

前記第1の記憶部(1412)が設けられ、ユーザが読出可能なデータ領域とを備える、請求項2または6記載のメモリカード。

【請求項11】

前記メモリカードは、

少なくとも前記第1の暗号化処理部(1406)と、前記第1の復号処理部(144)と、前記第2の復号処理部(1410)と、前記第3の復号処理部(1416)と、前記第2の記憶部(1500)とが設けられ、不当な開封処理に対しては、内部のデータが破壊されるタンパーレジスタンスモジュールにより構成されるユーザが読出不可能なセキュリティ領域(TRM)と、

30

前記第1の記憶部が設けられ、ユーザが読出可能なデータ領域とを備える、請求項4または8記載のメモリカード。

【請求項12】

前記第1の記憶部(1412)は、前記暗号化コンテンツデータに付随した非暗号化データを、前記暗号化コンテンツデータとともに受けて格納する請求項2または6記載のメモリカード。

【請求項13】

暗号化データ([[Dc]Kc)と前記暗号化データを復号するための復号情報データ(Kc,License-ID,User-ID)を受けて記録するためのメモリカードであって、

前記暗号化データを格納する第1の記憶部(1412)と、

40

前記メモリカードに対応して予め定められた第1の公開暗号化鍵(KPmedia)と自身の認証データ(Crtf1)とを公開認証鍵(KPmaster)により復号できるように暗号化して([[KPmedia,Crtf1]KPmaster))保持し、外部に対して出力可能な第1の鍵保持部(1442)と、

第1の公開暗号化鍵(KPmedia)によって暗号化されたデータを復号化するための第1の秘密復号鍵(Kmedia)を保持する第2の鍵保持部(1402)と、

前記復号情報データの通信ごとに更新されて送信され、前記第1の公開暗号化鍵(KPmedia)によって暗号化された第1の共通鍵([[Ks]Kmedia))を受けて、復号処理するための第1の復号処理部(1404)と、

前記メモリカードごとに固有な第2の公開暗号化鍵(KPcard(1))を保持するための第3の鍵保持部(1405)と、

50

前記復号情報データの通信ごとに更新される第2の共通鍵(Ks1)を生成するセッションキー発生部(1432)と、

前記第2の公開暗号化鍵(KPcard(1))と前記第2の共通鍵(Ks1)を、前記第1の共通鍵(Ks)に基づいて暗号化し([KPcard(1),Ks1]Ks)、出力するための第1の暗号化処理部(1406)と、

外部にて前記第2の公開暗号化鍵(KPcard(1))によって暗号化され、さらに第2の共通鍵(Ks1)によって暗号化された前記復号情報データ([Kc,License-ID,User-ID]Kcard(1)]Ks1)を前記第2の共通鍵(Ks1)に基づいて復号する([Kc,License-ID,User-ID]Kcard(1))ための第2の復号処理部(1410)と、

前記第2の復号処理部(1410)の出力である前記第2の公開暗号化鍵(KPcard(1))によって暗号化された前記復号情報データ([Kc,License-ID,User-ID]Kcard(1))を格納する第2の記憶部(1500)と、

前記第2の公開暗号化鍵(KPcard(1))によって暗号化されたデータ([Kc,License-ID,User-ID]Kcard(1))を復号するための第2の秘密復号鍵(Kcard(1))を保持する第4の鍵保持部(1415)と、

前記第2の記憶部(1500)に格納されたデータ([Kc,License-ID,User-ID]Kcard(1))を前記第2の秘密復号鍵(Kcard(1))に基づいて復号し(Kc,License-ID,User-ID)、前記復号情報データを抽出するための第3の復号処理部(1416)とを備える、メモリカード。

【請求項14】

前記メモリカードは、

前記公開認証鍵(KPmaster)を保持する第4の鍵保持部(1450)と、

前記公開認証鍵(KPmaster)によって復号できるように暗号化された外部から与えられる自身以外の第3の公開暗号化鍵(KPp),(KPmedia)と、自身以外の第2の認証データ(Crtf),(Crtf2)を([KPp,Crtf]KPmaster),([KPmedia,Crtf2]KPmaster)復号して抽出する(KPp,Crtf),(KPmedia,Crtf2)第4の復号処理部(1452)と、

前記第4の復号処理部(1452)により抽出された前記第2の認証データ(Crtf),(Crtf2)に基づいて認証処理を行ない、認証できない場合、前記復号情報データ(Kc,License-ID,User-ID)の出力を禁止する制御部(1420)と、

前記セッションキー生成部(1432)にて通信ごとに更新した第2の共通鍵(Ks1)を、前記第1の公開暗号化鍵(KPmedia)あるいは前記第3の公開暗号化鍵(KPp),(KPmedia)に基づいて暗号化して([Ks1]KPp),([Ks1]KPmedia)出力する第2の暗号化処理部(1430)と、

外部からの自身以外の固有の第4の公開暗号化鍵(KPcard(2))に基づいて暗号化を行なうための第3の暗号処理部(1414)をさらに備え、

外部からの復号情報データ(Kc,License-ID,User-ID)の出力要求があり、かつ、前記制御部(1420)が復号情報データの出力を禁止しない場合、

i) 前記第2の復号処理部(1410)は、第2の共通鍵(Ks1)によって暗号化された前記第1の共通鍵([Ks]Ks1)、または前記第2の共通鍵(Ks1)によって暗号化された第4の公開暗号化鍵および第3の共通鍵([KPcard(2),Ks2]Ks1)をさらに復号出力(Ks),(KPcard(2),Ks2)し、

ii) 前記第2の復号処理部(1410)にて前記第4の公開暗号化鍵(KPcard(2))が抽出された場合、前記第3の復号処理部(1416)は、前記第2の記憶部(1500)に記録されたデータから復号情報データ(Kc,License-ID,User-ID)を抽出し、前記第3の暗号化処理部(1414)は、前記第3の復号処理部(1416)で抽出した復号情報データ(Kc,License-ID,User-ID)を前記第2の復号処理部(1410)にて出力された第4の公開暗号化鍵(KPcard(2))にて暗号化して([Kc,License-ID,User-ID]Kcard(2))、さらに、第1の暗号化処理部(1406)は、第3の暗号化処理部(1414)の出力を前記第2の復号処理部(1410)にて抽出された第3の共通鍵(Ks2)に基づいて暗号化して([Kc,License-ID,User-ID]Kcard(2)]Ks2)出力し、

iii) 前記第2の復号処理部(1410)にて前記第1の共通鍵(Ks)のみが抽出された場合、前記第3の復号処理部(1416)は、前記第2の記憶部に格納されたデータから復号情報データ(Kc,License-ID,User-ID)を抽出し、前記第1の暗号化処理部(1406)は、前記第3の

10

20

30

40

50

復号処理部(1416)で抽出した復号情報データに含まれるコンテンツキー(Kc)を、前記第2の復号処理部(1410)にて抽出された第1の共通鍵(Ks)に基づいて暗号化出力する([Kc]Ks)、請求項13記載のメモリカード。

【請求項15】

前記復号情報データ(Kc,License-ID,User-ID)は、前記復号情報データのメモリカードからの出力を制御するためのアクセス制御データ(License-ID)をさらに含み、

前記第3の復号処理部(1416)にて前記第2の公開暗号化鍵(KPcard(1))によって暗号化された復号情報データ([Kc,License-ID,User-ID]Kcard(1))から抽出した(Kc,License-ID,User-ID)前記アクセス制御データを格納する第3の記憶部をさらに備え、

前記制御部は、前記第3の記憶部に格納された前記アクセス制御データに基づいて復号情報データの出力を禁止する、請求項14記載のメモリカード。 10

【請求項16】

前記メモリカードの記録空間は、

不当な開封処理に対しては、内部のデータが破壊されるタンパーレジスタンスモジュールにより構成され、ユーザが読出不能かつ書替不可能なセキュリティ領域(1490)と、

格納データはメモリカード固有の暗号化が施されており、ユーザが読出可能であるが書替不可能である準セキュリティ領域(1491)と、

ユーザが読出可能および書替可能な非セキュリティ領域(1492)とに区分され、

前記セキュリティ領域は、前記第1、第3の鍵保持部(1442,1405)および第3の記憶部を含み、 20

前記準セキュリティ領域は、前記第2の記憶部(1500)を含み、

前記非セキュリティ領域は、第1の記憶部(1412)を含む、請求項15記載のメモリカード。

【請求項17】

前記準セキュリティ領域(1491)および前記非セキュリティ領域(1492)は、同一メモリ上に配置される請求項16記載のメモリカード。

【請求項18】

暗号化データ([Dc]Kc)と前記暗号化データを復号するための復号情報データ(Kc,License-ID,User-ID)を受けて記録するためのメモリカードであって、

前記暗号化データを格納する第1の記憶部(1412)と、 30

前記メモリカードに対応して予め定められた第1の公開暗号化鍵(KPmedia)と自身の認証データ(Crtf1)とを公開認証鍵(KPmaster)により復号できるように暗号化して([KPmedia,Crtf1]KPmaster)保持し、外部に対して出力可能な第1の鍵保持部(1442)と、

第1の公開暗号化鍵(KPmedia)によって暗号化されたデータを復号化するための第1の秘密復号鍵(Kmedia)を保持する第2の鍵保持部(1402)と、

前記復号情報データの通信ごとに更新されて送信され、前記第1の公開暗号化鍵(KPmedia)によって暗号化された前記第1の共通鍵([Ks]Kmedia)を受けて、復号処理するための第1の復号処理部(1404)と、

前記メモリカードごとに固有な第2の公開暗号化鍵(KPcard(1))を保持するための第3の鍵保持部(1405)と、 40

前記復号情報データの通信ごとに更新される第2の共通鍵(Ks1)を生成するセッションキー発生部(1432)と、

前記第2の公開暗号化鍵(KPcard(1))と前記第2の共通鍵(Ks1)を、前記第1の共通鍵(Ks)に基づいて暗号化し([KPcard(1),Ks1]Ks)、出力するための第1の暗号化処理部(1406)と、

外部にて前記第2の公開暗号鍵(KPcard(1))によって暗号化され、さらに第2の共通鍵(Ks1)によって暗号化された前記復号情報データ([Kc,License-ID,User-ID]Kcard(1)]Ks1)を前記第2の共通鍵(Ks1)に基づいて復号する([Kc,License-ID,User-ID]Kcard(1))ための第2の復号処理部(1410)と、

前記第2の公開暗号化鍵(KPcard(1))によって暗号化されたデータ([Kc,License-ID,Use 50

r-ID]Kcard(1))を復号化するための第2の秘密復号鍵(Kcard(1))を保持する第4の鍵保持部(1415)と、

外部にて前記第2の公開暗号化鍵(KPcard(1))によって暗号化された復号情報データ([Kc,License-ID,User-ID]Kcard(1))を受けて、前記第2の秘密復号鍵(Kcard(1))により前記復号情報データ(Kc,License-ID,User-ID)を復号するための第3の復号処理部(1416)と、

前記復号情報データを格納する第2の記憶部(1500)とを備える、メモリカード。

【請求項19】

前記メモリカードは、

前記公開認証鍵(KPmaster)を保持する第4の鍵保持部(1450)と、

前記公開認証鍵(KPmaster)により復号できるように暗号化された外部から与えられる自身以外の第3の公開暗号化鍵(KPp),(KPmedia)と、自身以外の第2の認証データ(Crtf),(Crtf2)を([KPp,Crtf]KPmaster),([KPmedia,Crtf2]KPmaster)復号して抽出する(KPp,Crtf),(KPmedia,Crtf2)第4の復号処理部(1452)と、

前記第4の復号処理部(1452)により抽出された前記第2の認証データ(Crtf),(Crtf2)に基づいて認証処理を行ない、認証できない場合、前記復号情報データ(Kc,License-ID,User-ID)の出力を禁止する制御部(1420)と、

前記セッションキー生成部(1432)にて通信ごとに更新した第2の共通鍵(Ks1)を、前記第3の公開暗号化鍵(KPp),(KPmedia)に基づいて暗号化して([Ks1]KPp),([Ks1]KPmedia)出力する第2の暗号化処理部(1430)と、

外部からの自身以外の固有の第4の公開暗号化鍵(KPcard(2))に基づいて暗号化を行うための第3の暗号処理部(1414)をさらに備え、

外部から復号情報データ(Kc,License-ID,User-ID)の出力要求があり、かつ、前記制御部(1420)において復号情報データの出力を禁止しない場合、

i) 前記第2の復号処理部(1410)は、外部にて第2の共通鍵(Ks1)によって暗号化された前記第1の共通鍵([Ks]Ks1)を、または外部にて前記第2の共通鍵(Ks1)によって暗号化された第4の公開暗号化鍵および第3の共通鍵([KPcard(2),Ks2]Ks1)をさらに復号抽出し(Ks),(KPcard(2),Ks2)、

ii) 前記第2の復号処理部(1410)にて前記第4の公開暗号化鍵(KPcard(2))が抽出された場合、前記第3の復号処理部(1416)は、前記第2の記憶部(1500)に記録された復号情報データ(Kc,License-ID,User-ID)を前記第2の復号処理部(1410)にて抽出された第4の公開暗号化鍵(KPcard(2))にて暗号化して([Kc,License-ID,User-ID]Kcard(2))、さらに、第1の暗号化処理部(1406)は、第3の暗号化処理部(1414)の出力を前記第2の復号処理部(1410)にて抽出された第3の共通鍵(Ks2)に基づいて暗号化し([Kc,License-ID,User-ID]Kcard(2)]Ks2)出力し、

iii) 前記第2の復号処理部(1410)にて前記第1の共通鍵(Ks)のみが抽出された場合、前記第1の暗号化処理部(1406)は、前記第2の記憶部(1500)にも記録された復号情報データに含まれるコンテンツキー(Kc)を前記第3の復号処理部(1416)にて抽出された第1の共通鍵(Ks)に基づいて暗号化し([Kc]Ks)出力する、請求項18記載のメモリカード。

【請求項20】

前記復号情報データ(Kc,License-ID,User-ID)は、前記復号情報データのメモリカードからの出力を制御するためのアクセス制御データをさらに含み、

前記制御部は、前記第2の記憶部(1500)に格納された前記アクセス制御データに基づいて復号情報データの出力を禁止する、請求項19記載のメモリカード。

【請求項21】

前記メモリカードの記録空間は、

不当な開封処理に対しては、内部のデータが破壊されるタンパーレジスタンスモジュールにより構成され、ユーザが読出不能かつ書替不可能なセキュリティ領域(1490)と、

ユーザが読出かつ書替が可能な非セキュリティ領域(1492)とに区分され、

前記セキュリティ領域は、前記第1および第3の鍵保持部(1442,1405)および第2の記憶部(1500)を含み、

10

20

30

40

50

前記非セキュリティ領域は、前記第1の記憶部(1412)を含む、請求項20記載のメモリカード。

【請求項22】

暗号化データ([Dc]Kc)と前記暗号化データを復号するための復号情報データ(Kc,License-ID,User-ID)を受けて記録するためのメモリカードであって、

前記メモリカードに対応して予め定められた第1の公開暗号化鍵(KPmedia)と自身の認証データ(Crtf1)とを公開認証鍵(KPmaster)により復号できるように暗号化して([KPmedia,Crtf1]KPmaster)保持し、外部に対して出力可能な第1の鍵保持部(1442)と、

第1の公開暗号化鍵(KPmedia)によって暗号化されたデータを復号化するための第1の秘密復号鍵(Kmedia)を保持する第2の鍵保持部(1402)と、

10

前記復号情報データの通信ごとに更新されて送信され、前記第1の公開暗号化鍵(KPmedia)によって暗号化された前記第1の共通鍵([Ks]Kmedia)を受けて、復号処理するための第1の復号処理部(1404)と、

前記メモリカードごとに固有な第2の公開暗号化鍵(KPcard(1))を保持するための第3の鍵保持部(1405)と、

前記復号情報データの通信ごとに更新される第2の共通鍵(Ks1)を生成するセッションキー発生部(1432)と、

前記第2の公開暗号化鍵(KPcard(1))と前記第2の共通鍵(Ks1)を、前記第1の共通鍵(Ks)に基づいて暗号化し([Kcard(1),Ks1]Ks)、出力するための第1の暗号化処理部(1406)と、

20

外部にて前記第2の公開暗号鍵(KPcard(1))によって暗号化され、さらに第2の共通鍵(Ks1)によって暗号化された前記復号情報データ([Kc,License-ID,User-ID]Kcard(1)]Ks1)を前記第2の共通鍵(Ks1)に基づいて復号する([Kc,License-ID,User-ID]Kcard(1))ための第2の復号処理部(1410)と、

前記第2の公開暗号化鍵(KPcard(1))によって暗号化されたデータ([Kc,License-ID,User-ID]Kcard(1))を復号化するための第2の秘密復号鍵(Kcard(1))を保持する第4の鍵保持部(1415)と、

外部にて前記第2の公開暗号化鍵(KPcard(1))によって暗号化された復号情報データ([Kc,License-ID,User-ID]Kcard(1))を受けて、前記第2の秘密復号鍵(Kcard(1))により前記復号情報データ(Kc,License-ID,User-ID)を復号するための第3の復号処理部(1416)と、

30

前記復号情報データを格納する記憶部(1500)とを備える、メモリカード。

【請求項23】

前記メモリカードは、

前記公開認証鍵(KPmaster)を保持する第4の鍵保持部(1450)と、

前記公開認証鍵(KPmaster)により復号できるように暗号化された外部から与えられる自身以外の第3の公開暗号化鍵(KPp),(KPmedia)と、自身以外の第2の認証データ(Crtf),(Crtf2)を([KPp,Crtf]KPmaster),([KPmedia,Crtf2]KPmaster)復号して抽出する(KPp,Crtf),(KPmedia,Crtf2)第4の復号処理部(1452)と、

前記第4の復号処理部(1452)により抽出された前記第2の認証データ(Crtf),(Crtf2)に基づいて認証処理を行ない、認証できない場合、前記復号情報データ(Kc,License-ID,User-ID)の出力を禁止する制御部(1420)と、

40

前記セッションキー生成部(1432)にて通信ごとに更新した第2の共通鍵(Ks1)を、前記第3の公開暗号化鍵(KPp),(KPmedia)に基づいて暗号化して([Ks1]KPp),([Ks1]KPmedia)出力する第2の暗号化処理部(1430)と、

外部からの自身以外の固有の第4の公開暗号化鍵(KPcard(2))に基づいて暗号化を行うための第3の暗号処理部(1414)をさらに備え、

外部から復号情報データ(Kc,License-ID,User-ID)の出力要求があり、かつ、前記制御部(1420)において復号情報データの出力を禁止しない場合、

i) 前記第2の復号処理部(1410)は、外部にて第2の共通鍵(Ks1)によって暗号化された前記第1の共通鍵([Ks]Ks1)を、または外部にて前記第2の共通鍵(Ks1)によって暗号

50

化された第4の公開暗号化鍵および第3の共通鍵([KPCard(2),Ks2]Ks1)をさらに復号抽出し(Ks),(KPCard(2),Ks2)、

ii) 前記第2の復号処理部(1410)にて前記第4の公開暗号化鍵(KPCard(2))が抽出された場合、前記第3の復号処理部(1416)は、前記記憶部(1500)に記録された復号情報データ(Kc,License-ID,User-ID)を前記第2の復号処理部(1410)にて抽出された第4の公開暗号化鍵(KPCard(2))にて暗号化して([Kc,License-ID,User-ID]Kcard(2))、さらに、第1の暗号化処理部(1406)は、第3の暗号化処理部(1414)の出力を前記第2の復号処理部(1410)にて抽出された第3の共通鍵(Ks2)に基づいて暗号化し([Kc,License-ID,User-ID]Kcard(2)]Ks2)出力し、

iii) 前記第2の復号処理部(1410)にて前記第1の共通鍵(Ks)のみが抽出された場合、前記第1の暗号化処理部(1406)は、前記記憶部(1500)にも記録された復号情報データに含まれるコンテンツキー(Kc)を前記第3の復号処理部(1416)にて抽出された第1の共通鍵(Ks)に基づいて暗号化し([Kc]Ks)出力する、請求項2記載のメモリカード。

【請求項24】

前記復号情報データ(Kc,License-ID,User-ID)は、前記復号情報データのメモリカードからの出力を制御するためのアクセス制御データをさらに含み、

前記制御部は、前記記憶部(1500)に格納された前記アクセス制御データに基づいて復号情報データの出力を禁止する、請求項23記載のメモリカード。

【請求項25】

前記メモリカードの記録空間は、

不当な開封処理に対しては、内部のデータが破壊されるタンパーレジスタンスモジュールにより構成され、ユーザが読出不能かつ書替不可能なセキュリティ領域(1490)と、

ユーザが読出かつ書替が可能な非セキュリティ領域(1492)とに区分され、

前記セキュリティ領域は、前記第1および第3の鍵保持部(1442,1405)および記憶部(1500)を含む、請求項24記載のメモリカード。

【発明の詳細な説明】

技術分野

本発明は、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いて、コピーされた情報に対する著作権保護を可能とするメモリカード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情報が伝送される。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情報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、情報のコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、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情報通信網を介して著作物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。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したCD(コンパクトディスク)については、CDから光磁気ディスク(MD等)への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報が

10

20

30

40

50

コピー劣化のほとんどないデジタル情報であることに鑑み、1つのMDからさらに他のMDに音楽データをデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、自由に行なうことができるものの、記録可能なMDからMDへのコピーを行なうことはできない。

そのような事情からも、音楽情報や画像情報をデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権原のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権原を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

発明の開示

本発明の目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムにおけるメモリカードを提供することである。

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムにおけるメモリカード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メモリカードは、暗号化コンテンツデータを受けて記録するためのメモリカードであって、第1の鍵保持部と、第1の復号処理部と、第2の鍵保持部と、第1の暗号化処理部と、第2の復号処理部と、第1の記憶部と、第3の鍵保持部と、第3の復号処理部とを備える。

第1の鍵保持部は、メモリカードに対応して予め定められた第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。

第1の復号処理部は、暗号化コンテンツデータの通信ごとに更新されて配信され、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。

第2の鍵保持部は、メモリカードごとに異なる第2の公開暗号化鍵を保持する。第1の暗号化処理部は、第2の公開暗号化鍵を、第1の共通鍵に基づいて暗号化し、出力する。

第2の復号処理部は、第2の公開暗号化鍵で暗号化され、さらに第1の共通鍵で暗号化されたコンテンツキーを受け、第1の共通鍵に基づいて復号化する。第1の記憶部は、第2の復号処理部の出力を受けて、格納する。第3の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する。第3の復号処理部は、第1の記憶部に格納されたデータに基づいて、第2の秘密復号鍵によりコンテンツキーを復号する。

本発明の他の局面に従うと、暗号化データと暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであって、第1の記憶部と、第1の鍵保持部と、第2の鍵保持部と、第1の復号処理部と、第3の鍵保持部と、セッションキー発生部と、第1の暗号化処理部と、第2の復号処理部と、第2の記憶部と、第4の鍵保持部と、第3の復号処理部とを備える。

第1の記憶部は、暗号化データを格納する。第1の鍵保持部は、メモリカードに対応して予め定められた第1の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能である。

第2の鍵保持部は、第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。第1の復号処理部は、復号情報データの通信ごとに更新されて送信され、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。

第3の鍵保持部は、メモリカードごとに異なる第2の公開暗号化鍵を保持する。

セッションキー発生部は、復号情報データの通信ごとに更新される第2の共通鍵を生成する。第1の暗号化処理部は、第2の公開暗号化鍵と第2の共通鍵を、第1の共通鍵に基づ

10

20

30

40

50

いて暗号化し、出力する。第2の復号処理部は、外部にて第2の公開暗号鍵によって暗号化され、さらに第2の共通鍵によって暗号化された復号情報データを第2の共通鍵に基づいて復号する。

第2の記憶部は、第2の復号処理部の出力である第2の公開暗号鍵によって暗号化された復号情報データを格納する。第4の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号するための第2の秘密復号鍵を保持する。第3の復号処理部は、第2の記憶部に格納されたデータを第2の秘密復号鍵に基づいて復号し、復号情報データを抽出する。

この発明のさらに他の局面に従うと、暗号化データと暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであって、第1の記憶部と、第1の鍵保持部と、第2の鍵保持部と、第1の復号処理部と、第3の鍵保持部と、セッションキー発生部と、第1の暗号化処理部と、第2の復号処理部と、第4の鍵保持部と、第3の復号処理部と、第2の記憶部とを備える。

第1の記憶部は、暗号化データを格納する。第1の鍵保持部は、メモリカードに対応して予め定められた第1の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能である。

第2の鍵保持部は、第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。第1の復号処理部は、復号情報データの通信ごとに更新されて送信され、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。第3の鍵保持部は、メモリカードごとに異なる第2の公開暗号化鍵を保持する。セッションキー発生部は、復号情報データの通信ごとに更新される第2の共通鍵を生成する。第1の暗号化処理部は、第2の公開暗号化鍵と第2の共通鍵を、第1の共通鍵に基づいて暗号化し、出力する。

第2の復号処理部は、外部にて第2の公開暗号鍵によって暗号化され、さらに第2の共通鍵によって暗号化された復号情報データを第2の共通鍵に基づいて復号する。

第4の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する。

第3の復号処理部は、外部にて第2の公開暗号化鍵によって暗号化された復号情報データを受けて、第2の秘密復号鍵により復号情報データを復号する。第2の記憶部は、復号情報データを格納する。

したがって、本発明によれば、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、1度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能になってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

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、本発明の情報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、他の著作物データ、たとえば画像データ等の著作物データを、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情報を管理するコンテンツサーバ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）を暗号化したうえで、情報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、このような暗号化データを与える。

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）をコンテンツサーバ10に中継する。コンテンツサーバ10は配線リクエストに応じて、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア20の携帯

10

20

30

40

50

電話網を介して、各ユーザの携帯電話機に対して配信する。

図1においては、たとえば携帯電話ユーザ1の携帯電話機100には、携帯電話100により受信された暗号化された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化したうえで、携帯電話機100中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード110に格納する構成となっている。

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た音楽を聴取することが可能である。

以下では、このようなコンテンツサーバ10と配信キャリア20とを併せて、音楽サーバ30と総称することにする。

また、このような音楽サーバ30から、各携帯電話端末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、正規のメモリカードであるメモリカード110を購入していないユーザは、音楽サーバ30からの配信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を受信（ダウンロード）す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ド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、音楽サーバ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が直接音楽サーバ30から受信することとすると、そ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に示した例では、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および当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ2に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ1は、再生のために必要な情報（再生情報）ごとユーザ2にコピーさせるため、情報の移動を行なった後には、ユーザ1においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータとは所定の暗号化方式に従って暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたが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、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のライセンス情報とを意味する。

これに対して、コンテンツデータのみを暗号化されたままの状態、ユーザ2にコピーさせることを音楽情報の「複製」と呼ぶこととする。

この場合、ユーザ2の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないため、ユーザ2は、暗号化されたコンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ2が、このような音楽の再生を望む場合は、改めて音楽サーバ30からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいから、ユーザ2が直接音楽サーバ30からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

たとえば、携帯電話機100および102が、PHS（Personal Handy

10

20

30

40

50

Phooe) (登録商標)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からユーザ2への一括した情報の移転(移動)や、暗号化したコンテンツデータのみの転送(複製)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、通信における暗号化キー(鍵)を配送するための方式であり、さらに第2には、配信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、このようにして配信された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。

図2は、図1に示した情報配信システムにおいて使用される通信のためのキーデータ(鍵データ)等の特性をまとめて説明するための図である。

10

まず、図1に示した構成において、メモ리카ード100内のデータ処理を管理するための鍵としては、メモ리카ードという媒体の種類に固有で、すべてのメモ리카ードに対して共通な秘密復号鍵Kmediaと、メモ리카ードごとに異なる公開暗号化鍵KPCard(n)と、公開暗号化鍵KPCard(n)により暗号化されたデータを復号するための秘密復号鍵Kcard(n)とがある。

ここで、秘密復号鍵Kcard(n)や秘密復号鍵KPCard(n)の表記中の自然数nは、各ユーザ(メモ리카ード)を区別するための番号を表わす。

すなわち、公開暗号化鍵KPCard(n)で暗号化されたデータは、各メモ리카ードごとに存在する秘密復号鍵Kcard(n)で復号可能である。したがって、メモ리카ードにおける配信データの授受にあたっては、基本的には、後に説明するように3つの鍵Kmedia、Kcard(n)、KPCard(n)が用いられることになる。

20

さらに、メモ리카ード外とメモ리카ード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有、すなわち、メモ리카ードすべてに共通な公開暗号化鍵KPCmediaと、公開暗号化鍵KPCmediaにより暗号化されたデータを復号化するための秘密復号鍵Kmediaと、各通信ごと、たとえば、音楽サーバ30へのユーザのアクセスごとに生成される共通鍵Ksが用いられる。

ここで、共通鍵Ksは、上述のとおり、ユーザが音楽サーバ30に対して1回のアクセスを行なうごとに発生する構成として、1回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

30

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵Ksを「セッションキー」とも呼ぶことにする。

したがって、共通鍵Ksは各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

また、配信されるべきデータについては、まず、暗号化されたコンテンツデータを復号する鍵であるKc(以下、ライセンスキーと呼ぶ)があり、このライセンス鍵Kcにより暗号化されたコンテンツデータが復号化されるものとする。さらに、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスIDデータLicense-IDと、受信者を識別するためのユーザIDデータUser-ID等が存在する。ここで、ユーザIDデータUser-IDとしては、たとえばユーザの電話番号等を用いることが可能である。

40

このような構成とすることで、ライセンスIDデータLicense-IDに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザIDデータUser-IDを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

配信データにおけるコンテンツデータDcは、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキーKcで復号化可能なデータを、暗号化コンテンツデータ[Dc]Kcと呼ぶ。

50

ここで、[Y] Xという表記は、データYを、キー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している。

図3は、図1に示したコンテンツサーバ10の構成を示す概略ブロック図である。コンテンツサーバ10は、コンテンツデータ（音楽データ）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データLicense-ID等の配信情報を保持するための配信情報データベース304と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベース302と、配信情報データベース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、所定の暗号化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。

10

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312と、配信制御部312に制御されて、セッションキーKsを発生するためのセッションキー発生部314と、セッションキー発生部314より生成されたセッションキーKsを、公開暗号化鍵Kpmediaにより暗号化して、データバスBS1に与えるための暗号化処理部316と、各ユーザの携帯電話機においてセッションキーKsにより暗号化されたうえで送信されたデータを通信装置350およびデータバスBS1を介して受けて、復号処理を行なう復号処理部318と、復号処理部318により抽出された公開暗号化鍵Kpcard(n)を用いて、ライセンスキーやライセンスIDデータLicense-ID等のデータを配信制御部312に制御されて暗号化するための暗号化処理部320と、暗号化処理部320の出力を、さらにセッションキーKsにより暗号化して、データバスBS1を介して通信装置350に与える暗号化処理部322を含む。

20

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、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、通常の通話モードにおいて、データバスBS2を介して与えられる受信データに基づいて音声を再生するための音声再生部1112とを備える。

30

携帯電話機100は、さらに、コンテンツサーバ10からのコンテンツデータを復号化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ーインタフェース1200と、メモリカード110と携帯電話機の他の部分とのデータ授受にあたり、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Ksを乱数等により発生するセッションキー発生部1502と、セッションキー発生部1502により生成されたセッションキーを公開暗号化鍵Kpmediaで暗号化して、データバスBS2に与えるための暗号化処理部1504と、セッションキー発生部1502において生成されたセッションキーKsに基づいて、データバスBS2上のデータをセッションキーKsにより復号して出力する復号処理部1506と、復号処理部1506の出力を受けて、音楽信号を再生するための音楽再生部1508と、音楽再生部1508の出力と音声再生部1112の出力とを受けて、動作モードに応じて選択的に出力するための混合部1510と、混合部1510の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部1512と、デジタルアナログ変換部1512の出力を受けて、ヘッドホン120と接続するための接続端子1514とを含む。

40

なお、説明の簡素化のため本発明のコンテンツデータの配信に関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、一部割愛されている。

50

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。

メモリカード110は、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、秘密復号鍵Kmediaを保持するためのKmedia保持部1402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、秘密復号鍵Kmediaにより復号処理をすることにより、セッションキーKsを抽出する復号処理部1404と、公開暗号化キーKPcard(1)を保持するためのKPcard(1)保持部1405と、復号処理部1404により抽出されたセッションキーKsに基づいて、切換えスイッチ1408からの出力を暗号化してデータバスBS3に与えるための暗号化処理部1406と、データバスBS3上のデータを復号処理部1404により抽出されたセッションキーKsにより復号処理してデータバスBS4に与えるための復号処理部1410と、データバスBS4からメモリカードごとに異なる公開暗号化鍵KPcard(n)で暗号化されているライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のデータを格納し、データバスBS3からライセンスキーKcにより暗号化されている暗号化コンテンツデータ[Dc] Kcを受けて格納するためのメモリ1412とを備える。

切換えスイッチ1408は、接点Pa、Pb、Pcを有し、接点PaにはKPcard(1)保持部1405からの暗号化キーKPcard(1)が、接点PbにはデータバスBS5が、接点Pcには暗号化処理部1414の出力が与えられる。切換えスイッチ1408は、それぞれ、接点Pa、Pb、Pcに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部1406に与える。

メモリカード110は、さらに、秘密復号キーKcard(1)の値を保持するためのKcard(1)保持部1415と、公開暗号化鍵KPcard(1)により暗号化されており、かつ、メモリ1412から読出されたライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等([Kc, License-ID, User-ID] Kcard(1))を、復号処理してデータバスBS5に与える復号処理部1416と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵KPcard(n)を復号処理部1410から受けて、この相手方の公開暗号化鍵KPcard(n)に基づいて、データバスBS5上に出力されているライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を暗号化したうえで、切換えスイッチ1408に出力するための暗号化処理部1414と、データバスBS5との間でライセンスIDデータLicense-ID、ユーザIDデータUser-ID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とを備える。

なお、図5において実線で囲んだ領域は、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み出し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スモジュール(Tamper Resistance Module)と呼ばれる。

もちろん、メモリ1412も含めて、モジュールTRM内に組み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1412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1412中のデータのみでは、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スモジュール内にメモリ1412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。

図6は、図1および図3～図5で説明したデータ配信システムにおける配信モードを説明するためのフローチャートである。

図6においては、ユーザ1が、メモリカード110を用いることで、コンテンツサーバ1

10

20

30

40

50

0 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、ユーザのキーボタンの操作等によって、コンテンツサーバ10に対して配信リクエストがなされる（ステップS100）。

コンテンツサーバ10においては、この配信リクエストに応じて、セッションキー発生部314が、セッションキーKsを生成する（ステップS103）。

続いて、サーバ内の暗号化処理部316が、公開暗号化キーK P m e d i aにより、セッションキーKsを暗号化処理して、データベースBS1に与える（ステップS104）。

通信装置350は、暗号化処理部316からの暗号化セッションキー[Ks] K m e d i aを、通信網を通じて、携帯電話機100のメモリカード110に対して送信する（ステップS106）。

10

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、データベースBS3に与えられた受信データを、復号処理部1404が、K m e d i a保持部1402から与えられる秘密復号キーK m e d i aにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS108）。

続いて、配信モードにおいては、切換えスイッチ1408は、接点Paが閉じる状態が選択されているので、暗号化処理部1406は、接点Paを介してK P c a r d (1)保持部1405から与えられる公開暗号化鍵K P c a r d (1)（ユーザ1のメモリカードにおける公開暗号化鍵）を、セッションキーKsにより暗号化して、データベースBS3に与える（ステップS110）。

携帯電話機100は、暗号化処理部1406により暗号化されたデータ[K P c a r d (1)] Ksをコンテンツサーバ10に対して出力する（ステップS112）。

20

コンテンツサーバ10では、通信装置350により受信され、データベースBS1に与えられたデータ[K P c a r d (1)] Ksを復号処理部318が、セッションキーKsにより復号化処理して、公開暗号化キーK P c a r d (1)を復号抽出する（ステップS114）。

続いて、配信制御部312は、ライセンスキーKcを配信情報データベース304より取得し（ステップS116）、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等のライセンス情報を生成する（ステップS118）。

暗号化処理部320は、配信制御部312からのライセンスキーKc、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等のデータを受取って、復号処理部318より与えられた公開暗号化キーK P c a r d (1)により暗号化処理する（ステップS120）。

30

暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーKsにより暗号化して、データベースBS1に与える（ステップS122）。

通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, L i c e n s e - I D, U s e r - I D] K c a r d (1)] Ksをカード110に対して送信する。

メモリカード110においては、復号処理部1410がセッションキーKsにより、復号処理を行ない、データ[Kc, L i c e n s e - I D, U s e r - I D] K c a r d (1)を抽出し（ステップS126）、メモリ1412に格納する（ステップS128）。

40

一方、コンテンツサーバ10は、暗号化コンテンツデータ[Dc] Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード110に送信する（ステップS130）。

メモリカード110においては、受信したデータ[Dc] Kcをそのままメモリ1412に格納する（ステップS132）。

以上のような動作により、メモリカード110が格納するコンテンツデータは再生可能な状態となるので、以下では、メモリカードが格納するコンテンツデータが再生可能な状態となっていることを、「メモリカード110は、状態SAにある」と呼ぶことにする。

50

図7は、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、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図7を参照して、携帯電話機100のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード110に対して出力される(ステップS200)。

メモリカード110では、メモリ1420から、暗号化されているライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読み出し(ステップS203)、秘密復号キーKcard(1)によって、ライセンスキーKc、ライセンスIDデータLicense-IDやユーザIDデータUser-IDを復号処理する(ステップS204)。

10

コントローラ1420は、復号化されたライセンスIDデータLicense-ID等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し(ステップS206)、復号可能と判断した場合は、携帯電話機のコントローラ1106に対して、再生許可通知を送信する(ステップS208)。

携帯電話機100においては、セッションキー発生回路1502がセッションキーKsを生成し(ステップS210)、暗号化処理部1504が、公開暗号化キーKpmediaによりセッションキーKsを暗号化して(ステップS212)、データベースBS2に暗号化セッションキー[Ks]Kmediaが出力される(ステップS214)。

メモリカード110は、データベースBS2を介して、携帯電話機100により生成された暗号化セッションキーを受け取り、秘密復号キーKmediaにより復号し抽出する(ステップS216)。

20

続いて、メモリカード110は、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し(ステップS219)、暗号化ライセンスキー[Kc]KsをデータベースBS2に与える(ステップS220)。

携帯電話機100の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する(ステップS222)。

続いて、メモリカード110は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、データベースBS2に与える(ステップS224)。

携帯電話機100の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、抽出されたライセンスキーKcにより復号処理し(ステップS226)、コンテンツデータを再生して混合部1510に与える(ステップS228)。

30

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード110は、携帯電話機100に対して、再生不許可通知を送信する(ステップS230)。

ステップS230の状態では、コンテンツデータの再生を行なうことができないので、このような状態を以下では「メモリカード110は、状態SBにある」と表現することにする。

図8は、2つのメモリカード間において、コンテンツデータおよび再生情報の移動を行なう処理を説明するためのフローチャートである。

まず、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。

40

携帯電話機100は、まず、自身の側のメモリカード110と、受信側の携帯電話機102に挿入されたメモリカード112に対して、移動リクエストを出力する(ステップS300)。

さらに、携帯電話機100においては、セッションキー発生回路1502は、セッションキーKsを生成し(ステップS303)、公開暗号化キーKpmediaを用いて、暗号化処理部1504がセッションキーKsを暗号化し(ステップS304)、その暗号化セッションキー[Ks]KmediaをデータベースBS2を介して、メモリカード110に伝達するとともに、携帯電話機102に装着されたメモリカード112に対して、たとえば、トランシーバモードではアンテナ1102を介して、上記暗号化セッションキー[Ks]Kmediaを伝達する(ステップS306)。

50

メモリカード110においては、秘密復号キーKmediaによりセッションキーKsを復号抽出する(ステップS318)。

同様に、カード112においても、秘密復号キーKmediaにより、セッションキーKsを復号抽出し(ステップS320)、さらに、セッションキーKsによりメモリカード112の公開暗号化キーKPCard(2)を暗号化して(ステップS322)、メモリカード110に対して、暗号化されたデータ[KPCard(2)]Ksを送信する(ステップS324)。

メモリカード110においては、メモリカード112から送信された暗号化データをセッションキーKsにより復号化して、メモリカード112の公開暗号化キーKPCard(2)を復号抽出する(ステップS326)。

10

続いて、メモリカード110においては、メモリ1412からメモリカード110の公開暗号化キーKCard(1)により暗号化されているライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDが読出される(ステップS328)。

続いて、復号処理部1416が、秘密復号キーKCard(1)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを復号処理する(ステップS330)。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたカード112における公開暗号化キーKPCard(2)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを暗号化する(ステップS332)。

20

暗号化処理部1414により暗号化されたデータは、切換えスイッチ1408(接点Pcが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, License-ID, User-ID]KCard(2)をセッションキーKsにより暗号化する(ステップS334)。

続いて、メモリカード110は、携帯電話機100を介して、メモリカード112に対して、暗号化されたデータ[[Kc, License-ID, User-ID]KCard(2)]Ksを送信する(ステップS336)。

メモリカード112においては、メモリカード110から送信されたデータを復号処理部1410により、セッションキーKsに基づいて復号化処理して(ステップS338)、メモリ1412に格納する(ステップS340)。

30

一方、メモリカード110は、さらに、メモリ1412内のデータのうち、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDに対応したデータを消去する(ステップS342)。

続いて、メモリカード110は、暗号化コンテンツデータ[Dc]Kcをメモリから読出し、メモリカード112に対して送信する(ステップS344)。

メモリカード112は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する(ステップS346)。

以上のような処理を行なうと、ステップS342において、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等がメモリカード110からは消去されているので、メモリカード110は「状態SB」となる。

40

一方、メモリカード112においては、暗号化コンテンツデータ以外にも、ライセンスキー、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のすべてのデータが移動されているので、メモリカード112は「状態SA」となっている。

図9は、図1に示した情報配信システムにおいて、携帯電話機100から携帯電話機102へ、暗号化コンテンツデータの複製を行なう処理を説明するためのフローチャートである。

図9を参照して、携帯電話機100が、メモリカード110およびメモリカード112に対して複製リクエストを出力する(ステップS400)。

50

続いて、メモリカード１１０は、暗号化コンテンツデータ〔Dc〕Kcをメモリ１４１２から読出し、メモリカード１１２に対して出力する（ステップＳ４０２）。

メモリカード１１２においては、メモリカード１１０から送信された暗号化されたコンテンツデータを、そのままメモリ１４１２に記録する（ステップＳ４０４）。

以上のような動作を行なうと、メモリカード１１０には、暗号化コンテンツデータ、ライセンスキーKc、ユーザIDデータUser-ID、ライセンスIDデータLicense-ID等のすべてのデータが残されているため、メモリカード１１０は再生可能な状態、すなわち、「状態SA」にある。

一方、メモリカード１１２は、暗号化コンテンツデータのみを有しているため、そのままでは再生処理を行なうことができない。したがって、この時点ではメモリカード１１２は、「状態SB」にある。

10

メモリカード１１２が状態SAとなるためには、改めてコンテンツサーバ１０から、ライセンスキーKc、ライセンスIDデータLicense-IDやユーザIDデータUser-ID等の再生情報を取得する必要がある。

以上のような構成とすることで、メモリカードを有する正規のユーザのみがコンテンツデータ（音楽データ）を受信してメモリ中に格納することが可能となり、かつ、１度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能になってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

20

なお、以上の説明では、コンテンツサーバ１０からの暗号化データを復号するための回路は、携帯電話機に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作りこまれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込まれる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

〔実施例２〕

図１０は、本発明の実施例２のメモリカード１３０の構成を説明するための概略ブロック図であり、実施例１の図５と対比される図である。

実施例１のメモリカード１１０の構成と異なる点は、１つには、メモリカード１３０内にセッションキーKsを生成するためのセッションキー発生回路１４３２が設けられ、かつ、メモリカードという媒体に対応する公開暗号化キーKpmediaの値を保持するKpmedia保持部１４４０が設けられていることである。メモリカード１３０は、これに応じて、セッションキー発生回路１４３２で生成されたセッションキーKsを、公開暗号化キーKpmediaにより暗号化してデータバスBS３に与えるための暗号化処理部１４３０と、セッションキー発生回路１４３２からの出力と復号処理部１４０４との出力を受けて、選択的に暗号化処理部１４０６と復号処理部１４１０に与えるための切換えスイッチ１４３４を備える構成となっている。

30

切換えスイッチ１４３４は、接点Pd、Pe、Pfを有し、接点Pd、Peには、復号処理部１４０４の出力が、接点Pfにはセッションキー発生回路１４３２の出力が与えられる。切換えスイッチ１４３４は、それぞれ、接点Pd、Pe、Pfに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部１４０６と復号処理部１４１０に与える。

40

その他の構成は、図５に示した実施例１のメモリカード１１０の構成と同様であるの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。

メモリカード１３０の動作が、メモリカード１１０の動作と異なるのは、「移動」処理を行う場合である。

図１１は、メモリカード１３０の移動処理を説明するためのフローチャートであり、実施例１の図８と対比される図である。

図１１を参照して、まず、図１１においても、携帯電話機１００が送信側であり、携帯電話機１０２が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１３

50

0と同様の構成を有するメモリカード132が装着されているものとする。

携帯電話機100は、まず、自身の側のメモリカード130と、受信側の携帯電話機102に挿入されたメモリカード132に対して、移動リクエストを出力する（ステップS300）。

さらに、携帯電話機100においては、メモリカード130内のセッションキー発生回路1432は、セッションキーKsを生成し（ステップS312）、公開暗号化キーK P m e d i aを用いて、暗号化処理部1430がセッションキーKsを暗号化して（ステップS314）、たとえば、トランシーバモードではアンテナ1102を介して、暗号化されたセッションキーKsをカード132に伝達する（ステップS316）。

メモリカード132においては、復号処理部1404が、秘密復号キーK m e d i aにより、セッションキーKsを復号抽出し（ステップS320）、さらに、セッションキーKsによりメモリカード132の公開暗号化キーK P c a r d（2）を暗号化して（ステップS322）、メモリカード110に対して、暗号化されたデータ[K P c a r d（2）] Ksを送信する（ステップS324）。 10

メモリカード110においては、メモリカード112から送信された暗号化データをセッションキーKsにより復号化して、メモリカード112の公開暗号化キーK P c a r d（2）を復号抽出する（ステップS326）。

以下の処理は、基本的に、図8で説明した実施例1の移動処理と同様であるのでその説明は繰り返さない。

以上のような処理を行なうと、ステップS342において、ライセンスキーKc、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等がカード130からは消去されているので、メモリカード130は「状態SB」となる。 20

一方、メモリカード132においては、暗号化コンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I D等の再生情報が移動されているので、メモリカード132は「状態SA」となっている。

以上のような構成を用いることで、実施例1のメモリカードが奏する効果に加えて、たとえば、メモリカード130からメモリカード132へのデータの移動を、上述したようなセッションキー発生回路1502を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。 30

〔実施例3〕

図12は、本発明の実施例3のメモリカード140の構成を説明するための概略ブロック図であり、実施例1の図5と対比される図である。

実施例1のメモリカード110の構成と異なる点は、メモリカード140内にコントローラ1420とデータの授受が可能なレジスタ1500が設けられていることである。

その他の構成は、図5に示した実施例1のメモリカード5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13は、図12で説明したメモリカード140を用いた配信モードを説明するためのフローチャートである。

図13においても、ユーザ1が、メモリカード140を用いることで、コンテンツサーバ10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。 40

まず、ユーザ1の携帯電話機100から、ユーザのタッチキー1108の操作等によって、コンテンツサーバ10に対して配信リクエストがなされる（ステップS100）。

コンテンツサーバ10においては、この配信リクエストに応じて、セッションキー発生部314が、セッションキーKsを生成する（ステップS103）。

続いて、コンテンツサーバ10内の暗号化処理部316が、公開暗号化キーK P m e d i aにより、セッションキーKsを暗号化処理して、データバスBS1に与える（ステップS104）。

通信装置350は、暗号化処理部316からの暗号化コンテンツデータ[Ks] K m e d i aを、通信網を通じて、携帯電話機100のメモリカード140に対して送信する（ス 50

テップS106)。

メモリカード140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、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する(ステップS108)。

続いて、配信モードにおいては、切換えスイッチ1408は、接点Paが閉じる状態が選択されているので、暗号化処理部1406は、接点Paから与えられる公開暗号化鍵KPcard(1)(ユーザ1のメモリカードにおける公開暗号化鍵)を、セッションキーKsにより暗号化して、データバスBS3に与える。

携帯電話機100は、暗号化処理部1406により暗号化されたデータ[KPcard(1)]Ksをコンテンツサーバ10に対して出力する(ステップS112)。 10

コンテンツサーバ10では、通信装置350により受信され、データバスBS1に与えられたデータ[KPcard(1)]Ksを復号処理部318が、セッションキーKsにより復号化処理して、公開暗号化キーKPcard(1)を復号抽出する(ステップS114)。

続いて、配信制御部312は、ライセンスキーKcを配信情報データベース304より取得し(ステップS116)、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを生成する(ステップS118)。

暗号化処理部320は、配信制御部312からのライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを受取って、復号処理部318より与えられた公開暗号化キーKPcard(1)により暗号化処理する(ステップS120)。 20

暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーKsにより暗号化して、データバスBS1に与える(ステップS122)。

通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License-ID, User-ID]Kcard(1)]Ksをカード140に対して送信する。

メモリカード140においては、復号処理部1410がセッションキーKsにより、復号処理を行ない、データ[KC, License-ID, User-ID]Kcard(1)を抽出し(ステップS126)、メモリ1412に格納する(ステップS128)。 30

さらに、メモリカード140においては、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License-ID, User-ID]Kcard(1)を復号し、復号されたデータLicense-ID, User-IDをコントローラ1420が、レジスタ1500に格納する(ステップ129)。

一方、サーバ30は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード140に送信する(ステップS130)。

メモリカード140においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する(ステップS132)。 40

以上のような動作により、メモリカード140は、音楽情報を再生可能な状態となる。

図14は、携帯電話機100内において、メモリカード140に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図14を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード140に対して出力される(ステップS200)。

メモリカード140では、コントローラ1420がレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す(ステップS205)。

コントローラ1420は、ライセンスIDデータLicense-ID等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップS206）、復号可能と判断した場合は、携帯電話機のコントローラ1106に対して、再生許可通知を送信する（ステップS208）。

携帯電話機100においては、セッションキー発生回路1502がセッションキーKsを生成し（ステップS210）、暗号化処理部1504が、公開暗号化キーKpmediaによりセッションキーKsを暗号化して（ステップS212）、データバスBS2に暗号化セッションキー[Ks]Kmediaが出力される（ステップS214）。

メモリカード140は、データバスBS2を介して、携帯電話機により生成された暗号化セッションキー[Ks]Kmediaを受け取り、公開暗号化キーKmediaにより復号し、セッションキーKsを抽出する（ステップS216）。

10

続いて、メモリカード140は、メモリ1412から、暗号化されているデータ[Kc, License-ID, User-ID]Kcard(1)を読出し、復号処理部1416が復号してライセンスキーKcを抽出する（ステップS218）。

続いて、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS219）、暗号化ライセンスキー[Kc]KsをデータバスBS2に与える（ステップS220）。

携帯電話機100の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS222）。

続いて、メモリカード140は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読出し、データバスBS2に与える（ステップS224）。

20

携帯電話機の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、抽出されたライセンスキーKcにより復号処理し（ステップS226）、コンテンツデータを再生して混合部1510に与える（ステップS228）。

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード140は、携帯電話機100に対して、再生不許可通知を送信する（ステップS230）。

ステップS230の状態では、メモリカード140は、状態SBにある。

図15は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

30

まず、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。

また、携帯電話機102にも、メモリカード140と同様の構成を有するメモリカード142が装着されているものとする。

携帯電話機100は、まず、自身の側のメモリカード140と、受信側の携帯電話機102に挿入されたメモリカード142に対して、移動リクエストを出力する（ステップS300）。

さらに、携帯電話機100においては、セッションキー発生回路1502は、セッションキーKsを生成し（ステップS303）、公開暗号化キーKpmediaを用いて、暗号化処理部1504がセッションキーKsを暗号化して（ステップS304）、データバスBS2を介して、メモリカード140に伝達し、さらに、たとえば、トランシーバモードではアンテナ1102を介して、暗号化されたセッションキーKsをメモリカード142に伝達する（ステップS306）。

40

メモリカード140においては、秘密復号キーKmediaによりセッションキーKsを復号抽出する（ステップS318）。

同様に、メモリカード142においても、秘密復号キーKmediaにより、セッションキーKsを復号抽出し（ステップS320）、さらに、セッションキーKsによりカード142の公開暗号化キーKpcard(2)を暗号化して（ステップS322）、メモリカード140に対して、暗号化されたデータ[Kpcard(2)]Ksを送信する（ステップS324）。

メモリカード140においては、メモリカード142から送信された暗号化データをセッ

50

セッションキーKsにより復号化して、メモリカード142の公開暗号化キーK P c a r d (2)を復号抽出する(ステップS326)。

続いて、メモリカード140においては、メモリ1412からメモリカード140の公開暗号化キーK c a r d (1)により暗号化されているライセンスキーKc、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I Dが読出される(ステップS328)。

続いて、復号処理部1416が、秘密復号キーK c a r d (1)により、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dとを復号処理する(ステップS330)。

コントローラ1420は、このようにして復号されたライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dの値を、レジスタ1500内のデータ値と置換する(ステップS331)。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたメモリカード142における公開暗号化キーK P c a r d (2)により、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dとを暗号化する(ステップS332)。

暗号化処理部1414により暗号化されたデータは、切換えスイッチ1408(接点Pcが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, L i c e n s e - I D, U s e r - I D] K c a r d (2)をセッションキーKsにより暗号化する(ステップS334)。

続いて、メモリカード140は、携帯電話機100を介して、メモリカード142に対して、暗号化されたデータ[[Kc, L i c e n s e - I D, U s e r - I D] K c a r d (2)] Ksを送信する(ステップS336)。

メモリカード142においては、メモリカード140から送信されたデータを復号処理部1410により、セッションキーKsに基づいて復号化処理して、メモリ1412に格納する(ステップS339)。さらに、メモリカード142においては、復号処理部1416が、秘密復号キーK c a r d (2)に基づいて、データ[Kc, L i c e n s e - I D, U s e r - I D] K c a r d (2)を復号し、復号されたライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dをレジスタに格納する(ステップS341)。

一方、メモリカード140は、さらに、レジスタ1500に格納されたライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I Dを消去する(ステップS343)。

続いて、メモリカード140は、暗号化コンテンツデータ[Dc] Kcをメモリから読出し、メモリカード142に対して送信する(ステップS344)。

メモリカード142は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する(ステップS346)。

以上のような処理を行なうと、ステップS343において、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I Dがメモリカード140のレジスタ1500からは消去されているので、メモリカード140は「状態SB」となる。

一方、メモリカード142においては、暗号化コンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I D等のすべてのデータが移動されているので、メモリカード142は「状態SA」となっている。

図16は、図12に示したメモリカード140において、携帯電話機100から携帯電話機102へ、暗号化コンテンツデータの複製を行なう処理を説明するためのフローチャートである。

図16を参照して、携帯電話機100が、メモリカード140およびメモリカード142に対して複製リクエストを出力する(ステップS400)。

続いて、メモリカード140は、暗号化コンテンツデータ[Dc] Kcをメモリ1412

10

20

30

40

50

から読出し、メモリカード142に対して送信する（ステップS402）。

メモリカード142においては、メモリカード140から送信された暗号化コンテンツデータを、そのままメモリ1412に記録する（ステップS404）。

以上のような動作を行なうと、メモリカード140には、暗号化されたコンテンツデータ、ライセンスキーKc、ユーザIDデータUser-ID、ライセンスIDデータLicense-ID等のすべてのデータが残されているため、メモリカード140は再生可能な状態、すなわち、「状態SA」にある。

一方、メモリカード142は、暗号化コンテンツデータのみを有しているため、そのままでは再生処理を行なうことができない。したがって、この時点ではメモリカード142は、「状態SB」にある。

10

メモリカード142が状態SAとなるためには、改めてコンテンツサーバ10から、ライセンスキーKc、ライセンスIDデータLicense-IDやユーザIDデータUser-ID等を取得する必要がある。

以上のような構成とすることで、実施例1のメモリカード110と同様の効果を奏する上に、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいと、動作に必要な処理量を低減できる。

なお、以上の説明では、コンテンツサーバ10からの暗号化データを復号するための回路は、携帯電話機に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作りこまれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込まれる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

20

[実施例3の変形例]

実施例3のメモリカード140の再生処理では、ライセンスIDデータLicense-IDにより復号処理が可能であるかを判断する構成であった。このライセンスIDデータLicense-IDとしては、曲目の特定情報のみならず、再生回数の制限情報を含む構成とし、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。特に、メモリカード140では、ライセンスIDデータLicense-IDをレジスタ1500に保持する構成としたので、以下に説明するように再生処理を行なうたびに、ライセンスIDデータLicense-IDの内容を更新することが容易である。以下に、このようなメモリカード140の再生処理を説明する。

30

図17は、携帯電話機100内において、実施例3の変形例のメモリカード140に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図17を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード140に対して出力される（ステップS200）。

メモリカード140では、コントローラ1420がレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す（ステップS205）。

コントローラ1420は、復号化されたライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し（ステップS206）、再生可能回数を超えていないと判断した場合は、携帯電話機のコントローラ1106に対して、再生許可通知を送信する（ステップS208）。

40

携帯電話機100においては、セッションキー発生回路1502がセッションキーKsを生成し（ステップS210）、暗号化処理部1504が、秘密復号キーKpmediaによりセッションキーKsを暗号化して（ステップS212）、データバスBS2に暗号化セッションキーデータ[Ks]Kmediaが出力される（ステップS214）。

メモリカード140は、データバスBS2を介して、携帯電話機により生成された暗号化セッションキー[Ks]Kmediaを受け取り、秘密復号キーKmediaにより復号

50

し、セッションキーKsを抽出する（ステップS216）。

さらに、メモリカード140は、再生処理が行われることに応じて、レジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する（ステップ217）。

続いて、メモリカード140は、メモリ1412から、暗号化されているデータ[Kc, License-ID, User-ID] Kcard(1)を読み出し、復号処理部1416が復号してライセンスキーKcを抽出する（ステップS218）。

続いて、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS219）、暗号化ライセンスキー[Kc] KsをデータバスBS2に与える（ステップS220）。

10

携帯電話機100の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS222）。

続いて、メモリカード140は、暗号化コンテンツデータ[Dc] Kcをメモリ1412から読み出し、データバスBS2に与える（ステップS224）。

携帯電話機の音楽再生部1508は、暗号化コンテンツデータ[Dc] Kcを、抽出されたライセンスキーKcにより復号処理し（ステップS226）、コンテンツデータを再生して混合部1510に与える（ステップS228）。

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード140は、携帯電話機100に対して、再生不許可通知を送信する（ステップS230）。

20

以上のような構成とすることで、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

移動時には、再生情報内の再生回数を制限するライセンスIDデータLicense-IDについて、メモリ1412に記録されたライセンスIDデータLicense-IDを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンスIDデータLicense-IDに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

[実施例4]

30

図18は、本発明の実施例4のメモリカード150の構成を説明するための概略ブロック図であり、実施例2の図10と対比される図である。

実施例2のメモリカード130の構成と異なる点は、メモリカード150内にコントローラ1420とデータの授受が可能なレジスタ1500が設けられていることである。

その他の構成は、図10に示した実施例2のメモリカード130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19は、メモリカード150の移動モードを説明するためのフローチャートであり、実施例2の図11と対比される図である。

図19を参照して、まず、図19においても、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。また、携帯電話機102にも、メモリカード150と同様の構成を有するメモリカード152が装着されているものとする。

40

携帯電話機100は、まず、自身の側のメモリカード150と、受信側の携帯電話機102に挿入されたメモリカード152に対して、移動リクエストを出力する（ステップS300）。

さらに、携帯電話機100においては、メモリカード150内のセッションキー発生回路1432は、セッションキーKsを生成し（ステップS312）、公開暗号化キーKpm mediaを用いて、暗号化処理部1430がセッションキーKsを暗号化して（ステップS314）、たとえば、トランシーバモードではアンテナ1102を介して、暗号化されたセッションキーKsをカード152に伝達する（ステップS316）。

メモリカード152においても、復号処理部1404が、秘密復号キーKmediaによ

50

り、セッションキーKsを復号抽出し（ステップS320）、さらに、セッションキーKsによりメモリカード152の公開暗号化キーK P c a r d（2）を暗号化して（ステップS322）、メモリカード150に対して、暗号化されたデータ[K P c a r d（2）] Ksを送信する（ステップS324）。

メモリカード150においては、メモリカード152から送信された暗号化データをセッションキーKsにより復号化して、メモリカード152の公開暗号化キーK P c a r d（2）を復号抽出する（ステップS326）。

続いて、メモリカード150においては、メモリ1412からメモリカード150の公開暗号化キーK c a r d（1）により暗号化されているライセンスキーKc、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I Dが読出される（ステップS328）。 10

続いて、復号処理部1416が、秘密復号キーK c a r d（1）により、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dとを復号処理する（ステップS330）。

コントローラ1420は、このようにして復号されたライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dの値を、レジスタ1500内のデータ値と置換する（ステップS331）。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたメモリカード152における公開暗号化キーK P c a r d（2）により、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dとを暗号化する（ステップS332）。 20

暗号化処理部1414により暗号化されたデータは、切換えスイッチ1408（接点Pcが閉じている）を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, L i c e n s e - I D, U s e r - I D] K c a r d（2）をセッションキーKsにより暗号化する（ステップS334）。

続いて、メモリカード150は、携帯電話機100を介して、メモリカード152に対して、暗号化されたデータ[[Kc, L i c e n s e - I D, U s e r - I D] K c a r d（2）] Ksを送信する（ステップS336）。

メモリカード152においては、メモリカード150から送信されたデータを復号処理部1410により、セッションキーKsに基づいて復号化処理して、メモリ1412に格納する（ステップS339）。さらに、メモリカード152は、秘密復号キーK c a r d（2）に基づいて、データ[Kc, L i c e n s e - I D, U s e r - I D] K c a r d（2）を復号し、復号されたライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I Dをレジスタ1500に格納する（ステップS341）。 30

一方、メモリカード150は、さらに、レジスタ1500に格納されたライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I Dを消去する（ステップS343）。

続いて、メモリカード150は、暗号化コンテンツデータ「Dc」Kcをメモリから読出し、メモリカード152に対して送信する（ステップS344）。

メモリカード152は、秘密復号キーをそのままメモリ1412に格納する（ステップS346）。 40

以上のような処理を行なうと、ステップS342において、ライセンスキーKc、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等がメモリカード150からは消去されているので、メモリカード150は「状態SB」となる。

一方、メモリカード152においては、暗号化されたコンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I D等のすべてのデータが移動されているので、メモリカード152は「状態SA」となっている。

以上のような構成を用いることで、実施例2のメモリカード130が奏する効果に加えて、たとえば、メモリカード150からメモリカード152へのデータの移動を、上述した 50

ようなセッションキー発生回路1502を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

〔実施例5〕

図20は、本発明の実施例5のメモリカード160の構成を説明するための概略ブロック図であり、実施例3の図12と対比される図である。 10

以下では、携帯電話機100に装着されるメモリカード160の公開暗号化キーK P m e d i aと、携帯電話機102に装着されるメモリカード162の公開暗号化キーK P m e d i aとを区別して、それぞれ、メモリカード160に対するものを公開暗号化キーK P m e d i a (1)と、メモリカード162に対するものを公開暗号化キーK P m e d i a (2)と称することにする。

また、これに対応して、公開暗号化キーK P m e d i a (1)で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーK m e d i a (1)と称し、公開暗号化キーK P m e d i a (2)で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーK m e d i a (2)と称することにする。 20

このように、媒体固有の公開暗号化キーを区別することにより、以下の説明で明らかとなるように、メモリカードに複数の種類が存在する場合や、より一般的に、メモリカード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。図20を参照して、本発明の実施例5のメモリカード160の構成が、実施例3のメモリカード140の構成と異なる点は、メモリカード160内にメモリカードという媒体に対応する公開暗号化キーK P m e d i a (1)の値を保持し、データベースBS3に公開暗号化キーK P m e d i a (1)を出力するためのK P m e d i a保持部1440が設けられていることである。

その他の構成は、図12に示した実施例3のメモリカード140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。 30

図21は、図20で説明したメモリカード160を用いた配信モードを説明するためのフローチャートである。

図21においても、ユーザ1が、メモリカード160を用いることで、コンテンツサーバ10から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、ユーザのタッチキーの操作等によって、配信リクエストがなされる(ステップS100)。

メモリカード160においては、この配信リクエストに応じて、K P m e d i a保持部1440から、公開暗号化キーK P m e d i a (1)をコンテンツサーバ10に対して送信する(ステップS101)。

コンテンツサーバ10では、メモリカード160から転送された配信リクエストならびに公開暗号化キーK P m e d i a (1)を受信すると(ステップS102)、セッションキー発生部314が、セッションキーK sを生成する(ステップS103)。 40

続いて、コンテンツサーバ10内の暗号化処理部316が、公開暗号化キーK P m e d i a (1)により、セッションキーK sを暗号化処理して、データベースBS1に与える(ステップS104)。

通信装置350は、暗号化処理部316からの暗号化セッションキー[K s] K m e d i a (1)を、通信網を通じて、携帯電話機100のメモリカード160に対して送信する(ステップS106)。

メモリカード160においては、メモリインタフェース1200を介して、データベースBS3に与えられた受信データを、復号処理部1404が、秘密復号キーK m e d i a (1) 50

）により復号処理することにより、セッションキーKsを復号し抽出する（ステップS108）。

以下の処理は、図13において説明した実施例3のメモリカード140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で、メモリカード自身が、セッションキーKsを送る側（コンテンツサーバ10）に、公開暗号化キーK_{Pmedia}(1)を送信した上で、配信を受けることができ、メモリカード160は、コンテンツデータを再生可能な状態となる。

図22は、携帯電話機100内において、メモリカード160に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図22を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード160に対して出力される（ステップS200）。

メモリカード160においては、この再生リクエストに応じて、K_{Pmedia}保持部1440から、公開暗号化キーK_{Pmedia}(1)を携帯電話機100に対して送信する（ステップS201）。

携帯電話機100では、メモリカード160からの公開暗号化キーK_{Pmedia}(1)を受信して保持する（ステップS202）。

メモリカード160では、コントローラ1420がレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す（ステップS205）。

コントローラ1420は、ライセンスIDデータLicense-ID等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップS206）、復号可能と判断した場合は、携帯電話機のコントローラ1106に対して、再生許可通知を送信する（ステップS208）。

携帯電話機100においては、セッションキー発生回路1502がセッションキーKsを生成し（ステップS210）、暗号化処理部1504が、公開暗号化キーK_{Pmedia}(1)によりセッションキーKsを暗号化して（ステップS212）、データバスBS2に暗号化セッションキー[Ks]K_{media}(1)が出力される（ステップS214）。

メモリカード160は、データバスBS2を介して、携帯電話機により生成され、かつ暗号化されたセッションキーKsを受け取り、秘密復号キーK_{media}(1)により復号し、セッションキーKsを抽出する（ステップS216）。

以下の処理は、図14において説明した実施例3のメモリカード140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で、メモリカード自身が、セッションキーKsを送る側（携帯電話機100）に、公開暗号化キーK_{Pmedia}(1)を送信した上で、再生動作を行なうことが可能となる。

図23は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

まず、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。

また、携帯電話機102にも、メモリカード160と同様の構成を有するメモリカード162が装着されているものとする。

携帯電話機100は、まず、自身の側のメモリカード160と、受信側の携帯電話機102に挿入されたメモリカード162に対して、移動リクエストを出力する（ステップS300）。

メモリカード160においては、公開暗号化キーK_{Pmedia}(1)を携帯電話機100に対して送信し（ステップS301）、メモリカード162においては、公開暗号化キーK_{Pmedia}(2)を携帯電話機100に対して送信する（ステップS301'）。

携帯電話機100は、公開暗号化キーK_{Pmedia}(1)および公開暗号化キーK_{Pmedia}(2)を受信する（ステップS302）。

10

20

30

40

50

さらに、携帯電話機100においては、セッションキー発生回路1502は、セッションキーKsを生成し(ステップS303)、公開暗号化キーK P m e d i a (1)および公開暗号化キーK P m e d i a (2)を用いて、暗号化処理部1504がセッションキーKsを暗号化する(ステップS304)。携帯電話機100は、データバスBS2を介して、メモリカード160に対しては暗号化セッションキー[Ks] K P m e d i a (1)を伝達し、さらに、たとえば、トランシーバモードではアンテナ1102を介して、暗号化セッションキー[Ks] K P m e d i a (2)をメモリカード162に伝達する(ステップS306)。

メモリカード160においては、秘密復号キーK m e d i a (1)によりセッションキーKsを復号抽出する(ステップS318)。

10

同様にして、メモリカード162においても、秘密復号キーK m e d i a (2)により、セッションキーKsを復号抽出する(ステップS320)。

以下の処理は、図15において説明した実施例3のメモリカード140および142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で、メモリカード自身が、セッションキーKsを送る側(携帯電話機100)に、公開暗号化キーK P m e d i a (1)およびK P m e d i a (2)を送信した上で、移動モードを行なうことが可能となる。

なお、複製モードについては、メモリカード160および162の動作は、実施例3のメモリカード140および142の動作と同様である。

また、以上の説明では、レジスタ1500が設けられているものとして説明したが、図5に示した実施例1のメモリカード110と同様に、レジスタ1500が設けられていない構成とすることも可能である。

20

なお、以上の説明では、コンテンツサーバ10からの暗号化データを復号するための回路は、携帯電話に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作りこまれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込まれる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

さらに、図17において説明した実施例3の変形例のメモリカードの動作と同様に、ライセンスIDデータL i c e n s e - I Dとして、曲目の特定情報のみならず、再生回数の制限情報を含む構成とし、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

30

[実施例6]

図24は、本発明の実施例6のメモリカード170の構成を説明するための概略ブロック図であり、実施例4の図18と対比される図である。

実施例4のメモリカード150の構成と異なる点は、第1のK P m e d i a 保持部1440が、データバスBS3を介して他の媒体から送信された公開暗号化キー、たとえば、公開暗号化キーK P m e d i a (2)を受信して保持し、暗号化処理部1430は、この公開暗号化キーK P m e d i a (2)により、セッションキーKsを暗号化して、データバスBS3に与える構成となっていることである。

さらに、メモリカード170は、自身に対応した公開暗号化キーK P m e d i a (1)を保持して、データバスBS3に出力することが可能な第2のK P m e d i a 保持部1450を備える構成となっている。

40

その他の構成は、図18に示した実施例4のメモリカード150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25は、メモリカード170の移動処理を説明するためのフローチャートであり、実施例4の図19と対比される図である。

図25を参照して、まず、図25においても、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。また、携帯電話機102にも、メモリカード170と同様の構成を有するメモリカード172が装着されているものとする。

携帯電話機100は、まず、自身の側のメモリカード170と、受信側の携帯電話機10

50

2に挿入されたメモリカード172に対して、移動リクエストを出力する（ステップS300）。

メモリカード172は、第2のK P m e d i a保持部1450から、自身に対応する公開暗号化キーK P m e d i a（2）を携帯電話機102および100を介して、メモリカード170に送信し（ステップS301）、メモリカード170は、公開暗号化キーK P m e d i a（2）を受信して、第1のK P m e d i a保持部1440に格納する（ステップS302）。

さらに、携帯電話機100の側においては、メモリカード170内のセッションキー発生回路1432は、セッションキーK sを生成し（ステップS312）、公開暗号化キーK P m e d i a（2）を用いて、暗号化処理部1430がセッションキーK sを暗号化して（ステップS314）、たとえば、トランシーバモードではアンテナ1102を介して、暗号化セッションキー[K s] K m e d i a（2）をメモリカード172に伝達する（ステップS316）。

10

メモリカード172においては、復号処理部1404が、秘密復号キーK m e d i a（2）により、セッションキーK sを復号抽出する（ステップS320）。

以下の動作は、図19に示したメモリカード150および152の動作と同様であるのでその説明は繰り返さない。

以上のような構成を用いることで、メモリカード150の種類に応じて、公開暗号化キーK P m e d i aの値が異なるような場合等においても、実施例4のメモリカードが奏する効果と同様に、たとえば、メモリカード170からメモリカード172へのデータの移動を、上述したようなセッションキー発生回路を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

20

しかも、ライセンスIDデータL i c e n s e - I D等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、本実施例においても、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

なお、本実施例においても、図10に示した実施例2のメモリカード130と同様に、レジスタ1500を設けない構成とすることも可能である。

30

[実施例7]

実施例7のメモリカード180は、実施例4のメモリカード150の構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを1つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをK sとし、一方のメモリカード180の発生するセッションキーをK s 1とし、メモリカード180と同様の構成を有する他方のメモリカード182の発生するセッションキーをK s 2とする。

また、再生モードにおいて、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化キーをK P pとし、この公開暗号化キーK P pで暗号化されたデータを復号化できる秘密復号キーをK pとする。

40

図26は、実施例7における携帯電話機101の構成を説明するための概略ブロック図である。

図5に示した携帯電話機100の構成と異なる点は、まず、メモリカード180が装着されていること以外に、携帯電話機101は、公開暗号化キーK P pを保持して、再生モード時にキーK P pをデータバスB S 2に出力するK P p保持部1524を備える構成となっていることである。

さらに、携帯電話機101は、秘密復号キーK pを保持するK p保持部1520と、このK p保持部1520から与えられるキーK pに基づいて、データバスB S 2を介してメモリカード180から与えられるキーK P pで暗号化されたセッションキーK s 1を復号し抽出する復号処理部1522とをさらに備える構成となっている。しかも、暗号化処理部

50

1504は、この復号処理部1522から与えられるセッションキーKs1により、Ks発生部1502からの自身のセッションキーKsを暗号化してデータバスBS2に出力する。

携帯電話機101のその他の点は、図5に示した実施例1の携帯電話機100の構成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27は、実施例7のメモリカード180に対応したコンテンツサーバ11の構成を示す概略ブロック図である。図3に示したコンテンツサーバ10の構成と異なる点は、データ処理部310における暗号化処理部322は、Ks発生部314からのセッションキーKsに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーKsにより暗号化されて送信され、復号処理部318により復号抽出されたセッションキー、たとえば、セッションキーKs1に基づいて、暗号化処理部320の出力をさらに暗号化して、データバスBS1を介して通信装置350に与える点である。

10

コンテンツサーバ11のその他の点は、図3に示した実施例1のコンテンツサーバ10の構成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28は、本発明の実施例7のメモリカード180の構成を説明するための概略ブロック図であり、実施例4の図18と対比される図である。

メモリカード180の構成が、メモリカード150の構成と異なる点は、まず、セッションキーKs1発生部1432は、このカード独自のセッションキーKs1を発生することである。

メモリカード180は、さらに、カードという媒体に固有の公開暗号化キーK P m e d i aを保持するK P m e d i a保持部1440の出力と、データバスBS3を介して携帯電話機101から与えられる公開暗号化キーK P pとを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ1436を備える。切換えスイッチ1436は、接点P iおよびP hとを有し、接点P iはデータバスBS3と、接点P hはK P m e d i a保持部1440とそれぞれ結合する。暗号化処理部1430は、切換えスイッチ1436から与えられる公開暗号化キーK P m e d i aまたは公開暗号化キーK P pのいずれかにより、Ks1発生部1432からのセッションキーKs1を暗号化して、データバスBS3に与える。

20

すなわち、切換えスイッチ1436は、配信モードのとき、および移動モードにおいて移動先となっているときは、未使用状態であり、再生モードの時は、接点P iの側に閉じており、移動モードにおいて移動元となっているときは、接点P hの側に閉じている。

30

メモリカード180は、さらに、接点P e、P fおよびP gを有し、復号処理部1404から与えられるコンテンツサーバ11からのセッションキーKsと、Ks1発生部1432の出力と、データバスBS4から与えられる携帯電話機101からのセッションキーKsとを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1435を、切換えスイッチ1434の替わりに備える。接点P eには復号処理部1404からの出力が、接点P fにはKs1発生部1432の出力が、接点P gにはデータバスBS4がそれぞれ結合している。したがって、暗号化処理部1406と復号処理部1410は、この切換えスイッチ1435から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行なう。

40

すなわち、切換えスイッチ1435は、配信モードの場合にコンテンツサーバ11からのセッションキーの抽出を行なうときは、接点P eの側に閉じており、配信モードの場合に配信サーバからの暗号化されたライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I DについてキーKs1による復号を行なうときは、接点P fの側に閉じている。切換えスイッチ1435は、再生モードにおいて復号処理を行なうときは、接点P fの側に閉じており、再生モードにおいて暗号化処理を行なうときは、接点P gの側に閉じている。切換えスイッチ1435は、移動モードにおいて移動元となっている場合に復号処理を行うときは、接点P fの側に閉じており、移動モードにおいて移動元となっている場合に暗号化処理を行うときは、接点P gの側に閉じている。切換えスイッチ1435は、移動モードにおいて移動先となっている場合に移動元のセ

50

セッションキーを受け取る時は、接点P eの側に閉じており、移動モードにおいて移動先となっている場合にライセンスキーK c、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを受け取る時は、接点P fの側に閉じている。

メモリカード180は、さらに、接点P a、P b、P cおよびP eを有し、K s 1発生部1432から与えられる自身のセッションキーK s 1と、K P c a r d保持部1405の出力と、データベースBS5から与えられるライセンスキーK cと、暗号化処理部1414から与えられ、相手方の公開暗号化キーK P c a r d (n)により暗号化されたライセンスキーK c、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDとを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1409を、切換えスイッチ1408の替わりに備える。接点P aにはK s 1発生部1432からの出力が、接点P bにはK P c a r d保持部1405の出力が、接点P cにはデータベースBS5が、接点P dには暗号化処理部1414の出力が、それぞれ結合している。したがって、暗号化処理部1406は、この切換えスイッチ1409から与えられるデータに対して、それぞれ、暗号化処理を行なう。

すなわち、切換えスイッチ1409は、配信モードにおいて、配信先となっている場合にコンテンツサーバ11に自身の公開暗号化キーK P c a r d (1)や自身のセッションキーK s 1を送信するときは、順次、接点P bの側および接点P aの側に閉じる。切換えスイッチ1409は、再生モードのときは、接点P cの側に閉じており、移動モードにおいて移動元となっているときは、接点P dの側に閉じている。切換えスイッチ1409は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化キーK P c a r d (1)や自身のセッションキーK s 1を送信するときは、順次、接点P bの側および接点P aの側に閉じる。

図29は、図28で説明したメモリカード180を用いた配信モードを説明するためのフローチャートである。

図28においては、ユーザ1が、メモリカード180を用いることで、コンテンツサーバ11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101から、ユーザのタッチキー1108の操作等によって、コンテンツサーバ11に対して配信リクエストがなされる(ステップS100)。

コンテンツサーバ11においては、この配信リクエストに応じて、セッションキー発生部314が、セッションキーK sを生成する(ステップS103)。一方、メモリカード180の側では、K s 1発生部1432がセッションキーK s 1を生成する(ステップS103')。

コンテンツサーバ11では、続いて、コンテンツサーバ11内の暗号化処理部316が、公開暗号化キーK P m e d i aにより、セッションキーK sを暗号化処理して、データベースBS1に与える(ステップS104)。

通信装置350は、暗号化処理部316からの暗号化セッションキー[K s] K m e d i aを、通信網を通じて、携帯電話機101のメモリカード180に対して送信する(ステップS106)。

メモリカード180においては、メモリインタフェース1200を介して、データベースBS3に与えられた受信データを、復号処理部1404が、秘密復号キーK m e d i aにより復号処理することにより、セッションキーK sを復号し抽出する(ステップS108)。

続いて、配信モードにおいては、まず、切換えスイッチ1409が接点P bが閉じる状態が選択されているので、暗号化処理部1406は、接点P bを介してK P c a r d (1)保持部1405から与えられる公開暗号化鍵K P c a r d (1)(ユーザ1のメモリカードにおける公開暗号化鍵)を受け取り、続いて、切換えスイッチ1409が接点P aが閉じる状態となって、暗号化処理部1406は、接点P aを介してK s 1保持部1432から与えられるセッションキーK s 1を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点P eが閉じる状態が選択されているので、復号処理部1404からのセッションキーK sにより、公開暗号化鍵K P c a r d (1)およびセッションキーK s 1

10

20

30

40

50

を暗号化してデータバスBS3に与える。

携帯電話機101は、暗号化処理部1406により暗号化されたデータ[KPcard(1)、Ks1]Ksをコンテンツサーバ11に対して出力する(ステップS112)。

サーバ31では、通信装置350により受信され、データバスBS1に与えられたデータ[KPcard(1)、Ks1]Ksを復号処理部318が、セッションキーKsにより復号化処理して、公開暗号化キーKPcard(1)およびセッションキーKs1を復号抽出する(ステップS114)。

続いて、配信制御部312は、ライセンスキーKcを配信情報データベース304より取得し(ステップS116)、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを生成する(ステップS118)。

10

暗号化処理部320は、配信制御部312からのライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを受取って、復号処理部318より与えられた公開暗号化キーKPcard(1)により暗号化処理する(ステップS120)。

暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーKs1により暗号化して、データバスBS1に与える(ステップS122)。

通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License-ID, User-ID]Kcard(1)]Ks1をカード180に対して送信する。

20

カード180においては、切換えスイッチ1435が接点Pfが閉じる状態が選択される状態に切換えられているので、復号処理部1410は、Ks1発生部1432からのセッションキーKs1により、復号処理を行ない、データ[KC, License-ID, User-ID]Kcard(1)を抽出し(ステップS126)、メモリ1412に格納する(ステップS128)。

さらに、メモリカード180においては、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License-ID, User-ID]Kcard(1)を復号し、復号されたデータLicense-ID, User-IDをコントローラ1420が、レジスタ1500に格納する(ステップ129)。

30

一方、コンテンツサーバ11は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード180に送信する(ステップS130)。

メモリカード180においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する(ステップS132)。

以上のような動作により、メモリカード180は、コンテンツデータを再生可能な状態となる。

図30は、携帯電話機101内において、実施例7のメモリカード180に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明するフローチャートである。

40

図30を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード180に対して出力される(ステップS200)。

メモリカード180では、コントローラ1420がレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す(ステップS205)。

コントローラ1420は、復号化されたライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ(音楽データ)の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し(ステップS206)、再生可能回数を超えていないと判断した場合は、携帯電話機101のコントローラ1106に対して、再生許可通知を

50

送信する（ステップS208）。

携帯電話機101においては、まず、公開暗号化キーK_{pp}をメモリカード180に対して送信し、セッションキー発生回路1502がセッションキーK_sを生成する（ステップS210）。

一方、メモリカード180でもセッションキーK_s1を生成し（ステップS210'）、公開暗号化キーK_{pp}でセッションキーK_s1を暗号化して（ステップS211）、携帯電話機101に暗号化セッションキー「K_s1」K_pを送信する（ステップS212）。携帯電話機101では、復号処理部1522が秘密復号キーK_pにより、データバスBS2を介してメモリカード180から与えられた暗号化セッションキー「K_s1」K_pを復号し、セッションキーK_s1を抽出し（ステップS213）、暗号化処理部1504が、セッションキーK_s1によりセッションキーK_sを暗号化して（ステップS214）、データバスBS2に暗号化セッションキー「K_s」K_s1が出力される（ステップS215）。

10

メモリカード180は、データバスBS3を介して、携帯電話機101により生成された暗号化セッションキー「K_s」K_s1を受け取り、セッションキーK_s1により復号し、セッションキーK_sを抽出する（ステップS216）。

さらに、メモリカード180は、再生処理が行われることに応じて、レジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する（ステップ217）。

続いて、メモリカード180は、メモリ1412から、暗号化されているデータ「K_c, License-ID, User-ID」K_ccard(1)を読み出し、復号処理部1416が復号してライセンスキーK_cを抽出する（ステップS218）。

20

続いて、抽出したセッションキーK_sにより、ライセンスキーK_cを暗号化し（ステップS219）、暗号化ライセンスキー「K_c」K_sをデータバスBS2に与える（ステップS220）。

携帯電話機101の復号処理部1506は、セッションキーK_sにより復号化処理を行なうことにより、ライセンスキーK_cを取得する（ステップS222）。

続いて、メモリカード180は、暗号化コンテンツデータ「D_c」K_cをメモリ1412から読み出し、データバスBS2に与える（ステップS224）。

携帯電話機の音楽再生部1508は、暗号化コンテンツデータ「D_c」K_cを、抽出されたライセンスキーK_cにより復号処理し（ステップS226）、コンテンツデータを再生して混合部1510に与える（ステップS228）。

30

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード180は、携帯電話機101に対して、再生不許可通知を送信する（ステップS230）。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図31は、実施例7の2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

40

図31を参照して、まず、図31においては、携帯電話機101が送信側であり、これと同様の構成を有する携帯電話機103が受信側であるものとする。また、携帯電話機103にも、メモリカード180と同様の構成を有するメモリカード182が装着されているものとする。

携帯電話機101は、まず、自身の側のメモリカード180と、受信側の携帯電話機103に挿入されたメモリカード182に対して、移動リクエストを出力する（ステップS300）。

これに応じて、携帯電話機101においては、メモリカード180内のセッションキー発生回路1432は、セッションキーK_s1を生成し（ステップS312）、一方、携帯電話機103においては、メモリカード182内のセッションキー発生回路1432は、セ

50

セッションキーKs2を生成する(ステップS312')。

携帯電話機101においては、メモリカード180は、公開暗号化キーKpmediaを用いて、暗号化処理部1430がセッションキーKs1を暗号化して(ステップS314)、たとえば、トランシーバモードではアンテナ1102を介して、暗号化セッションキー[Ks]Kmediaをメモリカード182に伝達する(ステップS316)。

メモリカード182においては、復号処理部1404が、秘密復号キーKmediaにより、セッションキーKs1を復号抽出し(ステップS320)、さらに、セッションキーKs1によりメモリカード182の公開暗号化キーKpcard(2)およびセッションキーKs2を暗号化して(ステップS322)、メモリカード180に対して、暗号化されたデータ[Kpcard(2)、Ks2]Ks1を送信する(ステップS324)。

10

メモリカード180においては、メモリカード182から送信された暗号化データを復号処理部1410がセッションキーKs1により復号化して、メモリカード182の公開暗号化キーKpcard(2)およびセッションキーKs2を復号抽出する(ステップS326)。このとき、切換えスイッチ1435では接点Pfが閉じており、Ks1発生回路1432からのキーKs1が復号処理部1410に与えられている。

続いて、メモリカード180においては、メモリ1412からメモリカード150の公開暗号化キーKcard(1)により暗号化されているライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDが読出される(ステップS328)。

続いて、復号処理部1416が、秘密復号キーKcard(1)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを復号処理する(ステップS330)。

20

コントローラ1420は、このようにして復号されたライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDの値を、レジスタ1500内のデータ値と置換する(ステップS331)。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたカード182における公開暗号化キーKpcard(2)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを暗号化する(ステップS332)。

暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点Pdが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, License-ID, User-ID]Kcard(2)をメモリカード182のセッションキーKs2により暗号化する(ステップS334)。このとき、切換えスイッチ1435は、接点Pgが閉じており、復号処理回路1410からのセッションキーKs2が暗号化処理部1406に与えられている。

30

続いて、メモリカード180は、携帯電話機101を介して、メモリカード152に対して、暗号化されたデータ[[Kc, License-ID, User-ID]Kcard(2)]Ks2を送信する(ステップS336)。

メモリカード182においては、メモリカード180から送信されたデータを復号処理部1410により、セッションキーKs2に基づいて復号化処理して、メモリ1412に格納する(ステップS339)。さらに、メモリカード182は、ライセンスキーKcard(2)に基づいて、データ[Kc, License-ID, User-ID]Kcard(2)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-IDをレジスタ1500に格納する(ステップS341)。

40

一方、メモリカード180は、さらに、レジスタ1500に格納されたライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを消去する(ステップS343)。

続いて、メモリカード180は、暗号化コンテンツデータ[Dc]Kcをメモリから読出し、メモリカード182に対して送信する(ステップS344)。

メモリカード182は、受信した暗号化コンテンツデータをそのままメモリ1412に格

50

納する（ステップS346）。

以上のような処理を行なうと、ステップS342において、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等がメモリカード180からは消去されているので、メモリカード180は「状態SB」となる。

一方、メモリカード182においては、暗号化コンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のすべてのデータが移動されているので、メモリカード182は「状態SA」となっている。

以上のような構成を用いることで、たとえば、メモリカード180からメモリカード182へのデータの移動を、上述したようなセッションキー発生回路1502を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、セッションキーが、携帯電話機、メモリカードの各々で異なるため、通信のセキュリティが一層向上する。

ここで、移動時には、再生情報内の再生回数を制限するライセンスIDデータLicense-IDについては、メモリ1412に記録されたライセンスIDデータLicense-IDを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンスIDデータLicense-IDに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

〔実施例8〕

実施例8の携帯電話機105およびメモリカード190は、以下に説明するように、実施例7の携帯電話機101およびメモリカード180の構成とは、以下の点で異なることを特徴とする。

すなわち、実施例8の携帯電話機105では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機105を登録する際に、この携帯電話機105に割当てられた公開暗号化鍵Kppおよび認証データCrtfとを公開復号鍵（公開認証鍵）Kpmasterにより暗号化された形で記録保持する手段を有している。

同様に、実施例8のメモリカード190でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード190を登録する際に、このメモリカードに割当てられた公開暗号化鍵Kpmediaおよび認証データCrtfとを公開復号鍵（公開認証鍵）Kpmasterにより暗号化された形で記録保持する手段を有している。

ここで、メモリカード190および実施例8のコンテンツサーバ12には、この公開復号鍵（公開認証鍵）Kpmasterを記録保持する手段を有している。この公開復号鍵（公開認証鍵）Kpmasterは、システム中でデータ出力を行なう全ての機器がセッションキーにやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号鍵の獲得に用いるシステム共通の鍵である。

以下、さらに、実施例8の携帯電話機105、メモリカード190およびコンテンツサーバ12の構成をより詳しく説明する。

図32は、実施例8における携帯電話機105の構成を説明するための概略ブロック図である。

図26に示した携帯電話機101の構成と異なる点は、Kpp保持部1524の替わりに、公開復号鍵（公開認証鍵）Kpmasterにより暗号化された、公開暗号鍵Kppおよび認証データCrtfを保持するための〔Kpp, Crtf〕Kpmaster保持部1525を備える構成となっていることである。

10

20

30

40

50

携帯電話機 105 のその他の点は、図 26 に示した実施例 7 の携帯電話機 101 の構成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 33 は、実施例 8 のメモリカード 190 に対応したコンテンツサーバ 12 の構成を示す概略ブロック図である。図 27 に示したコンテンツサーバ 11 の構成と異なる点は、データ処理部 310 は、公開復号鍵 $KPmaster$ を保持する $KPmaster$ 保持部 324 と、 $KPmaster$ 保持部 324 から出力される公開復号キー $KPmaster$ に基づいて、通信網から通信装置 350 を介してデータバス $BS1$ に与えられるデータを復号するための復号処理部 326 とをさらに備える構成となっている点である。暗号化処理部 316 は、復号処理部 326 での復号処理により抽出された公開暗号化キー $KPmedia$ により、 Ks 発生部 314 で発生されたセッションキー Ks を暗号化し、また、配信制御部 312 は、復号処理部 326 での復号処理により抽出された認証データ $Crtf$ により、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

コンテンツサーバ 12 のその他の点は、図 27 に示した実施例 7 のコンテンツサーバ 11 の構成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 34 は、本発明の実施例 8 のメモリカード 190 の構成を説明するための概略ブロック図であり、実施例 7 の図 28 と対比される図である。

実施例 8 のメモリカード 190 の構成が、実施例 7 のメモリカード 180 の構成と異なる点は、まず、メモリカード 190 は、公開暗号鍵 $KPmedia$ および証明データ $Crtf$ とを公開復号鍵（公開認証鍵） $KPmaster$ により暗号化された形で記録保持する [$KPmedia$, $Crtf$] $KPmaster$ 保持部 1442 を備える構成となっていることである。一方で、切換えスイッチ 1436 は省略され、[$KPmedia$, $Crtf$] $KPmaster$ 保持部 1442 の出力は直接データバス $BS3$ に与えられる。

さらに、メモリカード 190 は、公開復号鍵 $KPmaster$ を記録保持するための $KPmaster$ 保持部 1450 と、 $KPmaster$ 保持部 1450 から出力される公開復号キー $KPmaster$ に基づいて、データバス $BS3$ 上のデータを復号するための復号処理部 1452 とを備える。

復号処理部 1452 での復号処理により抽出される公開暗号化鍵 $KPmedia$ および認証データ $Crtf$ のうち、公開暗号化鍵 $KPmedia$ は、暗号化処理部 1430 に与えられ、認証データ $Crtf$ は、データバス $BS5$ を介して、コントローラ 1420 に与えられる。

メモリカード 190 のその他の構成は、図 28 に示したメモリカード 180 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 35 は、図 34 に示したメモリカード 190 内の記録空間の構成を示す概略図である。メモリカードが独自に管理して、ユーザが自由にその内容を書きかえることも読み出すこともできず、かつ、不当な開封処理に対しては、内部のデータが破壊される TRM モジュールにより構成されるセキュリティ領域 1490、ユーザからデータの存在は確認できるものの、そのデータがメモリカード固有の暗号化、ここでは公開暗号化鍵 $KPcard(1)$ による暗号化が施され記録され、データの書き換えが自由に行なえない準セキュリティ領域 1491 と、ユーザがその内容を自由に読み出し、書き換えが行なえる非セキュリティ領域 1492 とを備える。

セキュリティ領域 1490 には、メモリカード 190 の出荷時から保持する鍵の保持部、すなわち、 $Kmedia$ 保持部 1402、 $KPcard(1)$ 保持部 1405、 $Kcard(1)$ 保持部 1415、[$KPmedia$, $Crtf$] $KPmaster$ 保持部 1442、 $KPmaster$ 保持部 1450 と、平文のライセンス情報が格納されるレジスタ 1500 が設けられる。

準セキュリティ領域 1491 には、メモリカード 190 固有の暗号化をされたデータである [Kc , $Lisence-ID$, $User-ID$] $Kcard(1)$ が格納され、メモリ 1412 内に設けられる。

非セキュリティ領域 1493 には、暗号化コンテンツデータ [Dc] Kc が格納され、

10

20

30

40

50

メモリ1412内に設けられる。したがって、暗号化コンテンツデータ[Dc]Kcは自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。準セキュリティ領域1491に格納されたライセンス情報を他のメモリカードに複製しても、メモリカード1900の固有の公開暗号鍵K P c a r d (1)にてかけられた暗号化は、対の秘密復号鍵K c a r d (1)を持たない他のメモリカードでは複製できないからである。

また、鍵を保持する全ての鍵保持部をセキュリティ領域に設けるよう説明したが、秘密復号鍵を保持するK m e d i a保持部1402およびK c a r d (1)保持部1415のみセキュリティ領域に配置さえすれば良く、他の鍵保持部に保持された鍵は外部より参照できるROM (Read Only Memory) に配置されていてもよい。

10

図36は、図35で説明したメモリカード190を用いた配信モードを説明するためのフローチャートである。

図36においては、ユーザ1が、メモリカード190を用いることで、コンテンツサーバ12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105から、ユーザのタッチキー1108の操作等によって、メモリカード190に対して配信リクエストがなされる(ステップS400)。

メモリカード190からは、[K P m e d i a, C r t f] K P m a s t e r保持部1442から、携帯電話機105を経由して、コンテンツサーバ12に対して、暗号化データ[K P m e d i a, C r t f] K P m a s t e rが送信される(ステップS402)。

コンテンツサーバ12においては、暗号化データ[K P m e d i a, C r t f] K P m a s t e rを受信すると、K P m a s t e r保持部324が保持する公開復号キーK P m a s t e rに基づいて、復号処理部326が復号処理することにより、公開暗号化キーK P m e d i aおよび認証データC r t fを取得する(ステップS404)。

20

さらに、コンテンツサーバ12においては、認証データC r t fによりメモリカード190の認証を行ない(ステップS406)、メモリカード190が正規のメモリカードであることが証明されれば、処理はS412に移行する。一方、コンテンツサーバ12は、メモリカード190が正規のメモリカードであることが証明されない場合は、配信不許可通知を送信し(ステップS408)、携帯電話機105が配信不許可通知を受信する(ステップS410)。

メモリカード190が正規のメモリカードであることが証明された場合、コンテンツサーバ12では、セッションキー発生部314が、セッションキーK sを生成する(ステップS412)。

30

コンテンツサーバ12では、続いて、コンテンツサーバ12内の暗号化処理部316が、公開暗号化キーK P m e d i aにより、セッションキーK sを暗号化処理して、データベースB S 1に与える(ステップS414)。

通信装置350は、暗号化処理部316からの暗号化セッションキー[K s] K m e d i aを、通信網を通じて、携帯電話機105のメモリカード190に対して送信する(ステップS416)。

メモリカード190においては、メモリインタフェース1200を介して、データベースB S 3に与えられた受信データを、復号処理部1404が、秘密復号キーK m e d i aにより復号処理することにより、セッションキーK sを復号し抽出する(ステップS418)。

40

さらに、メモリカード190では、K s 1発生部1432がセッションキーK s 1を生成する(ステップS420)。

続いて、配信モードにおいては、まず、切換えスイッチ1409が接点P bが閉じる状態が選択されているので、暗号化処理部1406は、接点P bを介してK P c a r d (1)保持部1405から与えられる公開暗号化鍵K P c a r d (1)を受け取り、続いて、切換えスイッチ1409が接点P aが閉じる状態となって、暗号化処理部1406は、接点P aを介してK s 1発生部1432から与えられるセッションキーK s 1を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点P eが閉じる状態が選択されているので、復号処理部1404からのセッションキーK sにより、公開暗号化鍵K P c a r

50

d (1) およびセッションキー K s 1 を暗号化してデータバス B S 3 に与える (ステップ S 4 2 2)。

携帯電話機 1 0 5 を介して、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1)、K s 1] K s がコンテンツサーバ 1 2 に対して送信される (ステップ S 4 2 4)。

コンテンツサーバ 1 2 では、通信装置 3 5 0 により受信され、データバス B S 1 に与えられたデータ [K P c a r d (1)、K s 1] K s を復号処理部 3 1 8 が、セッションキー K s により復号化処理して、公開暗号化キー K P c a r d (1) およびセッションキー K s 1 を復号抽出する (ステップ S 4 2 6)。

続いて、配信制御部 3 1 2 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し (ステップ S 4 2 8)、かつ、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ L i c e n s e e - I D およびユーザ I D データ U s e r - I D 等のデータを生成する (ステップ S 4 3 0)。

暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのライセンスキー K c、ライセンス I D データ L i c e n s e e - I D およびユーザ I D データ U s e r - I D 等のデータを受取って、復号処理部 3 1 8 より与えられた公開暗号化キー K P c a r d (1) により暗号化処理する (ステップ S 4 3 2)。

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータを受取って、さらにセッションキー K s 1 により暗号化して、データバス B S 1 に与える (ステップ S 4 3 4)。

通信装置 3 5 0 は、暗号化処理部 3 2 2 により暗号化されたデータ [[K c, L i c e n s e e - I D, U s e r - I D] K c a r d (1)] K s 1 をメモリカード 1 9 0 に対して送信する (ステップ S 4 3 6)。

メモリカード 1 9 0 においては、切換えスイッチ 1 4 3 5 が接点 P f が閉じる状態が選択される状態に切換えられているので、復号処理部 1 4 1 0 は、K s 1 発生部 1 4 3 2 からのセッションキー K s 1 により、復号処理を行ない、データ [K c, L i c e n s e e - I D, U s e r - I D] K c a r d (1) を抽出し (ステップ S 4 3 8)、メモリ 1 4 1 2 に格納する (ステップ S 4 4 0)。

さらに、メモリカード 1 9 0 においては、復号処理部 1 4 1 6 が、メモリ 1 4 1 2 に格納されたデータ [K c, L i c e n s e e - I D, U s e r - I D] K c a r d (1) を復号し、復号されたデータ L i c e n s e e - I D, U s e r - I D をコントローラ 1 4 2 0 が、レジスタ 1 5 0 0 に格納する (ステップ S 4 4 2)。

一方、コンテンツサーバ 1 2 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、通信装置 3 5 0 を介して、メモリカード 1 8 0 に送信する (ステップ S 4 4 4)。

メモリカード 1 9 0 においては、受信した暗号化コンテンツデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する (ステップ S 4 4 6)。

以上のような動作により、メモリカード 1 9 0 は、コンテンツデータを再生可能な状態となる。

図 3 7 は、携帯電話機 1 0 5 内において、実施例 8 のメモリカード 1 9 0 に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明するフローチャートである。

図 3 7 を参照して、携帯電話機のキーボード 1 1 0 8 等からのユーザ 1 の指示により、再生リクエストが携帯電話機 1 0 5 に与えられると (ステップ S 5 0 0)、携帯電話機 1 0 5 からメモリカード 1 9 0 に対して暗号化データ [K P p、C r t f] K P m a s t e r が送信される (ステップ S 5 0 2)。

メモリカード 1 9 0 では、復号処理部 1 4 5 2 での公開復号キー K P m a s t e r による復号処理により、公開暗号化鍵 K P p および認証データ C r t f が取得される (ステップ S 5 0 4)。コントローラ 1 4 2 0 は、認証データ C r t f により携帯電話機 1 0 5 が正規の機器であるかを認証し (ステップ S 5 0 6)、正規の機器であると証明されると、処

10

20

30

40

50

理をステップS508に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機105に対して送信する(ステップS544)。

携帯電話機105が正規の機器であると証明された場合(ステップS506)、セッションキー発生部1432がセッションキーKs1を生成する(ステップS508)。暗号化処理部1430は、復号処理部1452からの公開暗号化キーKppに基づいて、セッションキーKs1を暗号化し(ステップS510)、暗号化セッションキー[Ks1]Kpがメモリカード190から携帯電話機105に対して送信される(ステップS512)。携帯電話機105では、復号処理部1522での復号処理により、セッションキーKs1が復号され抽出される(ステップS514)。続いて、セッションキー発生部1502においてセッションキーKsが生成され(ステップS516)、暗号化処理部1504がセッションキーKs1によりキーKsを暗号化して(ステップS518)、携帯電話機105からメモリカード190に対して、暗号化セッションキー[Ks]Ks1が送信される(ステップS520)。

10

メモリカード190では、復号処理部1410がセッションキーKs1により、暗号化セッションキー[Ks]Ks1を復号処理してセッションキーKsを抽出する(ステップS522)。さらに、メモリカード190では、コントローラ1420がレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読み出す(ステップS524)。

コントローラ1420は、復号化されたライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ(音楽データ)の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し(ステップS526)、再生可能回数を超えていないと判断した場合は、メモリカード190は、再生処理が行われることに応じて、レジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する(ステップS528)。

20

続いて、メモリカード190は、メモリ1412から、暗号化されているデータ[Kc, License-ID, User-ID]Kcard(1)を読み出し、復号処理部1416が復号してライセンスキーKcを抽出する(ステップS530)。

続いて、ステップS522において抽出したセッションキーKsにより、ライセンスキーKcを暗号化し(ステップS532)、暗号化ライセンスキー[Kc]KsをデータベースBS2に与える(ステップS534)。

30

携帯電話機105の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する(ステップS536)。

続いて、メモリカード190は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、データベースBS2に与える(ステップS538)。

携帯電話機の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、抽出されたライセンスキーKcにより復号処理し(ステップS540)、コンテンツデータを再生して混合部1510に与える(ステップS542)。

一方、ステップS526において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード190は、携帯電話機105に対して、再生不許可通知を送信する(ステップS544)。

40

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図38は、実施例8の2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図38を参照して、まず、図38においては、携帯電話機105が送信側であり、これと同様の構成を有する携帯電話機107が受信側であるものとする。また、携帯電話機107にも、メモリカード190と同様の構成を有するメモリカード192が装着されているものとする。

50

携帯電話機105は、まず、受信側の携帯電話機107に挿入されたメモリカード192に対して、移動リクエストを出力する（ステップS600）。

これに応じて、携帯電話機107に装着されたメモリカード192からは、メモリカード190に対して、暗号化データ[KPmedia、Crtf]KPmasterが送信される（ステップS602）。

メモリカード190においては、暗号化データ[KPmedia、Crtf]KPmasterを受信すると、KPmaster保持部1450が保持する公開復号キーKPmasterに基づいて、復号処理部1452が復号処理することにより、公開暗号化キーKPmediaおよび認証データCrtfを取得する（ステップS604）。

さらに、メモリカード190においては、認証データCrtfによりメモリカード192の認証を行ない（ステップS606）、メモリカード192が正規のメモリカードであることが証明されれば、処理はS612に移行する。一方、メモリカード190は、メモリカード192が正規のメモリカードであることが証明されない場合は、移動不許可通知を送信し（ステップS608）、携帯電話機107が移動不許可通知を受信する（ステップS610）。 10

メモリカード192が正規のメモリカードであることが証明された場合、メモリカード190では、セッションキー発生部1432が、セッションキーKs1を生成する（ステップS612）。

メモリカード190では、続いて、暗号化処理部1430が、公開暗号化キーKPmediaにより、セッションキーKs1を暗号化処理して、データバスBS3に与える（ステップS614）。 20

メモリカード190からは、暗号化処理部1430からの暗号化セッションキー[Ks]Kmediaを、携帯電話機105を通じて、携帯電話機107のメモリカード192に対して送信する（ステップS616）。

メモリカード192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、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS618）。さらに、メモリカード192では、Ks1発生器1432と同様の構成を有するKs2発生部1432'がセッションキーKs2を生成する（ステップS620）。

続いて、メモリカード192では、まず、切換えスイッチ1409が接点Pbが閉じる状態が選択されているので、暗号化処理部1406は、接点Pbを介してKPcard(1)保持部1405から与えられる公開暗号化鍵KPcard(1)を受け取り、続いて、切換えスイッチ1409が接点Paが閉じる状態となって、暗号化処理部1406は、接点Paを介してKs2発生部1432'から与えられるセッションキーKs2を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点Peが閉じる状態が選択されているので、復号処理部1404からのセッションキーKs1により、公開暗号化鍵KPcard(1)およびセッションキーKs2を暗号化してデータバスBS3に与える（ステップS622）。 30

携帯電話機107を介して、暗号化処理部1406により暗号化されたデータ[KPcard(1)、Ks2]Ks1がメモリカード190に対して送信される（ステップS624）。 40

メモリカード190においては、メモリカード192から送信された暗号化データを復号処理部1410がセッションキーKs1により復号化して、メモリカード192の公開暗号化キーKPcard(2)およびセッションキーKs2を復号抽出する（ステップS626）。このとき、切換えスイッチ1435では接点Pfが閉じており、Ks1発生回路1432からのキーKs1が復号処理部1410に与えられている。

続いて、メモリカード190においては、メモリ1412から、メモリカード190の公開暗号化キーKcard(1)により暗号化されているライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDが読出される（ステップS628）。 50

続いて、メモリカード190では、復号処理部1416が、秘密復号キーKcard(1)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを復号処理する(ステップS630)。

メモリカード190のコントローラ1420は、このようにして復号されたライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDの値を、レジスタ1500内のデータ値と置換する(ステップS632)。

さらに、メモリカード190の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード192における公開暗号化キーKpcard(2)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを暗号化する(ステップS634)。

10

メモリカード190の暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点Pdが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, License-ID, User-ID]Kcard(2)をメモリカード192のセッションキーKs2により暗号化する(ステップS636)。このとき、切換えスイッチ1435は、接点Pgが閉じており、復号処理回路1410からのセッションキーKs2が暗号化処理部1406に与えられている。続いて、メモリカード190は、携帯電話機105を介して、メモリカード192に対して、暗号化されたデータ[[Kc, License-ID, User-ID]Kcard(2)]Ks2を送信する(ステップS638)。

メモリカード192においては、メモリカード190から送信されたデータを復号処理部1410により、セッションキーKs2に基づいて復号化処理して、メモリ1412に格納する(ステップS640)。さらに、メモリカード192は、ライセンスキーKcard(2)に基づいて、データ[Kc, License-ID, User-ID]Kcard(2)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-IDをレジスタ1500に格納する(ステップS642)。

20

一方、メモリカード190は、さらに、レジスタ1500に格納されたライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを消去する(ステップS644)。

続いて、メモリカード190は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読出し、メモリカード192に対して送信する(ステップS646)。

30

メモリカード192は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する(ステップS648)。

以上のような処理を行なうと、ステップS644において、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等がメモリカード190からは消去されているので、メモリカード190は「状態SB」となる。

一方、メモリカード192においては、暗号化コンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のすべてのデータが移動されているので、メモリカード192は「状態SA」となっている。

ここで、実施例7と同様に、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいので、動作に必要な処理量を低減できる。

40

さらに、セッションキーが、携帯電話機、メモリカードの各々で異なるため、通信のセキュリティが一層向上する。

ここで、移動時には、再生情報内の再生回数を制限するライセンスIDデータLicense-IDについては、メモリ1412に記録されたライセンスIDデータLicense-IDを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンスIDデータLicense-IDに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにする

50

ことが可能である。

〔実施例 9〕

図 39 は、実施例 9 のメモリカード 200 の構成を示す概略ブロック図である。

実施例 9 のメモリカード 200 は、以下に説明するように、実施例 8 のメモリカード 190 の構成とは、以下の点で異なることを特徴とする。

すなわち、実施例 9 のメモリカード 200 では、実施例 8 のメモリカード 190 の構成において、Kmedia 保持部 1402、KPCard (1) 保持部 1405、Kcard (1) 保持部 1415、[KPMedia、Crtf] KPMaster 保持部 1442、KPMaster 保持部 1450 およびレジスタ 1500 が、メモリ 1412 の所定の領域内に設けられる構成となっている。これに応じて、切換えスイッチ 1409 の接点 P 10
b および Pc が省略され、データバス BS4 とメモリ 1412 とは直接データのやり取りを行わず、メモリ 1412 は、データバス BS3 との間でのみデータを授受するものとする。データバス BS4 は、データバス BS3 を介してメモリ 1412 とデータの授受を行なう。

図 40 は、図 39 に示したメモリカード 200 内の記録空間の構成を示す概略図である。メモリカードが独自に管理して、ユーザが自由にその内容を書きかえることも読み出すこともできず、かつ、不当な開封処理に対しては、内部のデータが破壊される TRM モジュールにより構成されるセキュリティ領域 1490 と、ユーザがその内容を自由に読み出し、書き換えが行なえる非セキュリティ領域 1492 とを備える。

セキュリティ領域 1490 には、メモリカード 200 の出荷時から保持する鍵の保持部 20
すなわち、Kmedia 保持部 1402、KPCard (1) 保持部 1405、Kcard (1) 保持部 1415、[KPMedia、Crtf] KPMaster 保持部 1442、KPMaster 保持部 1450 と、平文のライセンス情報が格納されるレジスタ 1500 が設けられる。実施例 8 における図 35 と異なるのは準セキュリティ領域が設けられていない点であり、このため準セキュリティ領域 1491 の格納されていた [Kc、Licence-ID、User-ID] Kcard (1) を Kcard (1) で復号した平文のライセンスキー Kc、ライセンス ID Licence-ID、ユーザ ID User-ID の内、実施例 8 においてレジスタ 1500 に格納されていなかったコンテンツキー Kc もセキュリティ領域 1490 に平文で格納される。このため、実施例 8 に比べてセキュリティ領域 1490 は、より広い記録空間が必要となる。 30

非セキュリティ領域 1493 には、暗号化コンテンツデータ [Dc] Kc が格納され、メモリ 1412 がこれにあたる。したがって、暗号化コンテンツデータ [Dc] Kc は自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。

また、鍵を保持する全ての鍵保持部をセキュリティ領域に設けるよう説明したが、秘密復号鍵を保持する Kmedia 保持部 1402 および Kcard (1) 保持部 1415 のみセキュリティ領域に配置さえすれば良く、他の鍵保持部に保持された鍵は外部より参照できる ROM (Read Only Memory) に配置されていても良い。

図 41 は、図 39 で説明したメモリカード 200 を用いた配信モードを説明するためのフローチャートであり、実施例 8 の図 36 と対比される図である。 40

図 41 においては、ユーザ 1 が、メモリカード 200 を用いることで、コンテンツサーバ 12 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 105 から、ユーザのタッチキー 1108 の操作等によって、メモリカード 200 に対して配信リクエストがなされる (ステップ S400)。

メモリカード 200 からは、メモリ 1412 中の [KPMedia、Crtf] KPMaster 保持部 1442 から、携帯電話機 105 を経由して、コンテンツサーバ 12 に対して、暗号化データ [KPMedia、Crtf] KPMaster が送信される (ステップ S402)。

コンテンツサーバ 12 においては、暗号化データ [KPMedia、Crtf] KPMaster を受信すると、KPMaster 保持部 324 が保持する公開復号キー KPMa 50

s t e rに基づいて、復号処理部326が復号処理することにより、公開復号キーK P m e d i aおよび認証データC r t fを取得する（ステップS404）。

さらに、コンテンツサーバ12においては、認証データC r t fによりメモリカード200の認証を行ない（ステップS406）、メモリカード200が正規のメモリカードであることが証明されれば、処理はS412に移行する。

一方、コンテンツサーバ12は、メモリカード200が正規のメモリカードであることが証明されない場合は、配信不許可通知を送信し（ステップS408）、携帯電話機105が配信不許可通知を受信する（ステップS410）。

メモリカード200が正規のメモリカードであることが証明された場合、コンテンツサーバ12では、セッションキー発生部314が、セッションキーK sを生成する（ステップS412）。 10

コンテンツサーバ12では、続いて、コンテンツサーバ12内の暗号化処理部316が、公開暗号化キーK P m e d i aにより、セッションキーK sを暗号化処理して、データバスB S 1に与える（ステップS414）。

通信装置350は、暗号化処理部316からの暗号化セッションキー[K s] K m e d i aを、通信網を通じて、携帯電話機105のメモリカード200に対して送信する（ステップS416）。

メモリカード200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B S 3に与えられた受信データを、復号処理部1404が、データバスB S 3を介してメモリ1412から与えられる秘密復号キーK m e d i aにより復号処理することにより、セッションキーK sを復号し抽出する（ステップS418）。さらに、メモリカード200では、K s 1発生部1432がセッションキーK s 1を生成する（ステップS420）。 20

続いて、配信モードにおいては、まず、暗号化処理部1406は、データバスB S 3を介してメモリ1412中のK P c a r d（1）保持部1405から与えられる公開暗号化鍵K P c a r d（1）を受け取り、続いて、切換えスイッチ1409が接点P aが閉じる状態となっているので、暗号化処理部1406は、接点P aを介してK s 1発生部1432から与えられるセッションキーK s 1を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点P eが閉じる状態が選択されているので、復号処理部1404からのセッションキーK sにより、公開暗号化鍵K P c a r d（1）およびセッションキーK s 1を暗号化してデータバスB S 3に与える（ステップS422）。 30

携帯電話機105を介して、暗号化処理部1406により暗号化されたデータ[K P c a r d（1）、K s 1] K sがコンテンツサーバ12に対して送信される（ステップS424）。

コンテンツサーバ12では、通信装置350により受信され、データバスB S 1に与えられたデータ[K P c a r d（1）、K s 1] K sを復号処理部318が、セッションキーK sにより復号化処理して、公開暗号化キーK P c a r d（1）およびセッションキーK s 1を復号抽出する（ステップS426）。

続いて、配信制御部312は、ライセンスキーK cを配信情報データベース304より取得し（ステップS428）、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等のデータを生成する（ステップS430）。 40

暗号化処理部320は、配信制御部312からのライセンスキーK c、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等のデータを受取って、復号処理部318より与えられた公開暗号化キーK P c a r d（1）により暗号化処理する（ステップS432）。

暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーK s 1により暗号化して、データバスB S 1に与える（ステップS434）。

通信装置350は、暗号化処理部322により暗号化されたデータ[[K c, L i c e n s e - I D, U s e r - I D] K c a r d（1）] K s 1をメモリカード200に対して 50

送信する（ステップS436）。

メモリカード200においては、切換えスイッチ1435が接点Pfが閉じる状態が選択される状態に切換えられているので、復号処理部1410は、Ks1発生部1432からのセッションキーKs1により、復号処理を行ない、データ[Kc, License-ID, User-ID] Kcard(1)を抽出する（ステップS438）。

さらに、メモリカード200においては、復号処理部1416が、メモリ1412中のKcard(1)保持部1415からの出力に基づいて、復号処理部1410からのデータ[Kc, License-ID, User-ID] Kcard(1)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-ID、ライセンスキーKcをメモリ1412中のレジスタ1500に格納する（ステップ443）。
一方、コンテンツサーバ12は、暗号化コンテンツデータ[Dc] Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード180に送信する（ステップS444）。

10

メモリカード200においては、受信した暗号化コンテンツデータ[Dc] Kcをそのままメモリ1412に格納する（ステップS446）。

以上のような動作により、メモリカード200は、コンテンツデータを再生可能な状態となる。

図42は、携帯電話機105内において、実施例9のメモリカード200に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートであり、実施例8の図37と対比される図である。

20

図41を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストが携帯電話機105に与えられると（ステップS500）、携帯電話機105からメモリカード200に対して暗号化データ[KPp, Crtf] KPmasterが送信される（ステップS502）。

メモリカード200では、復号処理部1452での公開復号キーKPmasterによる復号処理により、公開暗号化鍵KPpおよび認証データCrtfが取得される（ステップS504）。コントローラ1420は、認証データCrtfにより携帯電話機105が正規の機器であるかを認証し（ステップS506）、正規の機器であると証明されると、処理をステップS508に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機105に対して送信する（ステップS544）。

30

携帯電話機105が正規の機器であると証明された場合（ステップS506）、セッションキー発生部1432がセッションキーKs1を生成する（ステップS508）。暗号化処理部1430は、復号処理部1452からの公開暗号化キーKPpに基づいて、セッションキーKs1を暗号化し（ステップS510）、暗号化セッションキー[Ks1] Kpがメモリカード200から携帯電話機105に対して送信される（ステップS512）。携帯電話機105では、復号処理部1522での復号処理により、セッションキーKs1が復号され抽出される（ステップS514）。続いて、セッションキー発生部1502においてセッションキーKsが生成され（ステップS516）、暗号化処理部1504がセッションキーKs1によりセッションキーKsを暗号化して（ステップS518）、携帯電話機105からメモリカード200に対して、暗号化セッションキー[Ks] Ks1が送信される（ステップS520）。

40

メモリカード200では、復号処理部1410がセッションキーKs1により、暗号化セッションキー[Ks] Ks1を復号処理してセッションキーKsを抽出する（ステップS522）。さらに、メモリカード200では、コントローラ1420がメモリ1412中のレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す（ステップS524）。

コントローラ1420は、ライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限值を超えてい

50

るかいないかを判断し（ステップS526）、再生可能回数を超えていないと判断した場合は、メモリカード200は、再生処理が行われることに応じて、メモリ1412中のレジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する（ステップ528）。

続いて、メモリカード200は、メモリ1412から、ライセンスキーKcを読み出し、ステップS522において抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS532）、暗号化ライセンスキー[Kc]KsをデータバスBS2に与える（ステップS534）。

携帯電話機105の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS536）。

10

続いて、メモリカード200は、暗号化コンテンツキー[Dc]Kcをメモリ1412から読み出し、データバスBS2に与える（ステップS538）。

携帯電話機の音楽再生部1508は、暗号化コンテンツキー[Dc]Kcを、抽出されたライセンスキーKcにより復号処理し（ステップS540）、コンテンツデータを再生して混合部1510に与える（ステップS542）。

一方、ステップS526において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード200は、携帯電話機105に対して、再生不許可通知を送信する（ステップS544）。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

20

図43は、実施例9の2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートであり、実施例8の図38と対比される図である。

図43を参照して、まず、図43においては、携帯電話機105が送信側であり、これと同様の構成を有する携帯電話機107が受信側であるものとする。また、携帯電話機107にも、メモリカード200と同様の構成を有するメモリカード202が装着されているものとする。

携帯電話機105は、まず、受信側の携帯電話機107に挿入されたメモリカード202に対して、移動リクエストを出力する（ステップS600）。

30

これに応じて、携帯電話機107に装着されたメモリカード202からは、メモリカード200に対して、暗号化データ[KPmedia, Crtf]KPmasterが送信される（ステップS602）。

メモリカード200においては、暗号化データ[KPmedia, Crtf]KPmasterを受信すると、KPmaster保持部1450が保持する公開復号キーKPmasterに基づいて、復号処理部1452が復号処理することにより、公開暗号化キーKPmediaおよび認証データCrtfを取得する（ステップS604）。

さらに、メモリカード200においては、認証データCrtfによりメモリカード202の認証を行ない（ステップS606）、メモリカード202が正規のメモリカードであることが証明されれば、処理はS612に移行する。一方、メモリカード200は、メモリカード202が正規のメモリカードであることが証明されない場合は、移動不許可通知を送信し（ステップS608）、携帯電話機107が移動不許可通知を受信する（ステップS610）。

40

メモリカード202が正規のメモリカードであることが証明された場合、メモリカード200では、セッションキー発生部1432が、セッションキーKs1を生成する（ステップS612）。

メモリカード200では、続いて、暗号化処理部1430が、公開暗号化キーKPmediaにより、セッションキーKs1を暗号化処理して、データバスBS3に与える（ステップS614）。

メモリカード200からは、暗号化処理部1430からの暗号化セッションキー[Ks]

50

Kmediaを、携帯電話機105を通じて、携帯電話機107のメモリカード202に対して送信する（ステップS616）。

メモリカード202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、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS618）。さらに、メモリカード202では、Ks1発生器1432と同様の構成を有するKs2発生部1432'がセッションキーKs2を生成する（ステップS620）。

続いて、メモリカード202では、まず、暗号化処理部1406は、データバスBS3を介してメモリ1412中のKPcard(1)保持部1405から与えられる公開暗号化鍵KPcard(1)を受け取り、切換えスイッチ1409が接点Paが閉じる状態とな
10
っているため、暗号化処理部1406は、接点Paを介してKs2発生部1432'から与えられるセッションキーKs2を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点Peが閉じる状態が選択されているため、復号処理部1404からのセッションキーKs1により、公開暗号化鍵KPcard(1)およびセッションキーKs2を暗号化してデータバスBS3に与える（ステップS622）。

携帯電話機107を介して、暗号化処理部1406により暗号化されたデータ[KPcard(1)、Ks2]Ks1がメモリカード200に対して送信される（ステップS624）。

メモリカード200においては、メモリカード202から送信された暗号化データを復号処理部1410がセッションキーKs1により復号化して、メモリカード202の公開暗
20
号化キーKPcard(2)およびセッションキーKs2を復号抽出する（ステップS626）。このとき、切換えスイッチ1435では接点Pfが閉じており、Ks1発生回路1432からのセッションキーKs1が復号処理部1410に与えられている。

続いて、メモリカード200では、メモリ1412中のレジスタ1500から、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとが読み出される（ステップS629）。

さらに、メモリカード200の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード202における公開暗号化キーKPcard(2)により、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを暗号化する（ステップS634）。
30

メモリカード200の暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409（接点Pdが閉じている）を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, License-ID, User-ID]Kcard(2)をメモリカード202のセッションキーKs2により暗号化する（ステップS636）。このとき、切換えスイッチ1435は、接点Pgが閉じており、復号処理回路1410からのセッションキーKs2が暗号化処理部1406に与えられている。
続いて、メモリカード200は、携帯電話機105を介して、メモリカード202に対して、暗号化されたデータ[[Kc, License-ID, User-ID]Kcard(2)]Ks2を送信する（ステップS638）。

メモリカード202においては、メモリカード200から送信されたデータを復号処理部
40
1410により、セッションキーKs2に基づいて復号化処理する（ステップS641）。さらに、メモリカード202は、秘密復号キーKcard(2)に基づいて、データ[Kc, License-ID, User-ID]Kcard(2)を復号し、復号されたライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDをメモリ1412中のレジスタ1500に格納する（ステップS643）。一方、メモリカード200は、レジスタ1500よりライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDを消去し（ステップS644）、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読出し、メモリカード202に対して送信する（ステップS646）。

メモリカード202は、受信した暗号化コンテンツデータをそのままメモリ1412に格
50

納する（ステップS648）。

すなわち、以上のような構成でも、実施例8と同様の動作を実現できる。

なお、以上説明してきた各実施例において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作権データや音楽サーバ30に対するアクセス情報等を、付加情報Diとして暗号化コンテンツデータ併せて配信することも可能である。この付加データDiは、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ1412に記録される。

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、限定となつてはならず、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。

【図面の簡単な説明】

図1は、本発明の情報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に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

図3は、図1に示したコンテンツサーバ10の構成を示す概略ブロック図である。

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。

図5は、図4に示したメモ리카ード110の構成を説明するための概略ブロック図である。

図6は、図1および図3～図5で説明したデータ配信システムにおける配信モード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の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図8は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図9は、暗号化されたコンテンツデータの複製を行なうモードを説明するためのフローチャートである。

図10は、本発明の実施例2のメモ리카ード130の構成を説明するための概略ブロック図である。

図11は、メモ리카ード130の移動モードを説明するためのフローチャートである。

図12は、本発明の実施例3のメモ리카ード140の構成を説明するための概略ブロック図である。

図13は、図12で説明したメモ리카ード140を用いた配信モードを説明するためのフローチャートである。

図14は、実施例3の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図15は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図16は、暗号化されたコンテンツデータの複製を行なうモードを説明するためのフローチャートである。

図17は、実施例3の変形例の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図18は、本発明の実施例4のメモ리카ード150の構成を説明するための概略ブロック図である。

図19は、メモ리카ード150の移動モードを説明するためのフローチャートであり、実施例2の図11と対比される図である。

図20は、本発明の実施例5のメモ리카ード160の構成を説明するための概略ブロック図である。

図21は、図20で説明したメモ리카ード160を用いた配信モードを説明するためのフ

10

20

30

40

50

ローチャートである。

図22は、実施例5の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図23は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図24は、本発明の実施例6のメモ리카ード170の構成を説明するための概略ブロック図である。

図25は、メモ리카ード170の移動モードを説明するためのフローチャートである。

図26は、実施例7の携帯電話機101の構成を説明するための概略ブロック図である。

図27は、実施例7のメモ리카ード180に対応したコンテンツサーバ11の構成を示す概略ブロック図である。 10

図28は、本発明の実施例7のメモ리카ード180の構成を説明するための概略ブロック図である。

図29は、本発明の実施例7のメモ리카ード180を用いた配信モードを説明するためのフローチャートである。。

図30は、実施例7の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図31は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図32は、実施例8における携帯電話機105の構成を説明するための概略ブロック図である。 20

図33は、実施例8のメモ리카ード190に対応したコンテンツサーバ12の構成を示す概略ブロック図である。

図34は、本発明の実施例8のメモ리카ード190の構成を説明するための概略ブロック図である。

図35は、実施例8のメモ리카ード190の記録領域の配置を示す概略図である。

図36は、図35で説明したメモ리카ード190を用いた配信モードを説明するためのフローチャートである。

図37は、メモ리카ード190に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生モードを説明するフローチャートである。 30

図38は、実施例8の2つのメモ리카ード間において、移動を行なう処理を説明するためのフローチャートである。

図39は、実施例9のメモ리카ード200の構成を示す概略ブロック図である。

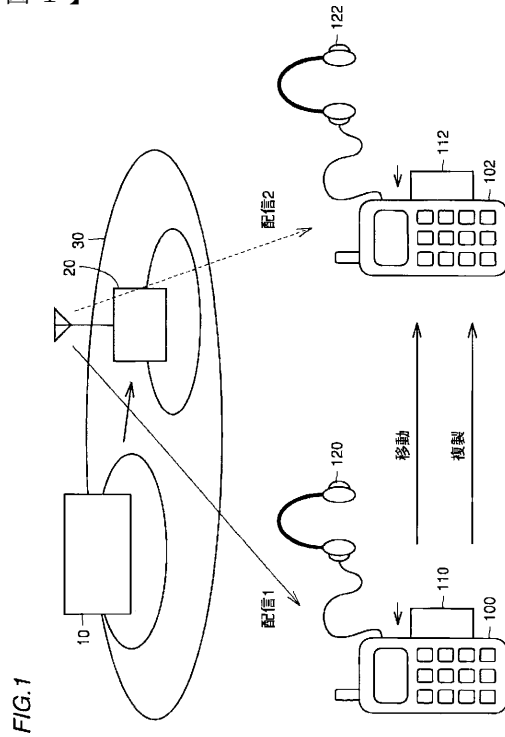
図40は、実施例9のメモ리카ード200の記録領域の配置を示す概略ブロック図である。

図41は、図38で説明したメモ리카ード200を用いた配信モードを説明するためのフローチャートである。

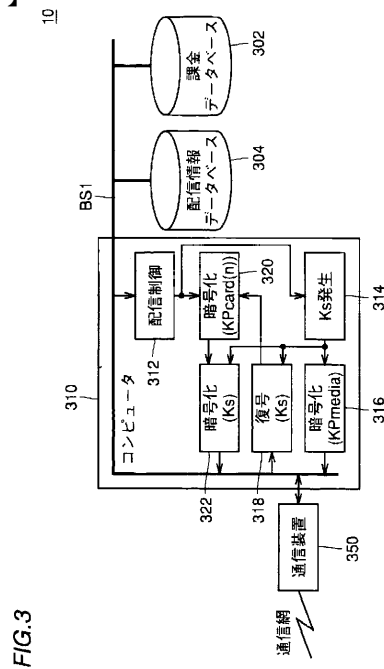
図42は、メモ리카ード200に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生モードを説明するフローチャートである。

図43は、実施例9の2つのメモ리카ード間において、移動を行なうモードを説明するためのフローチャートである。 40

【図 1】



【図 3】

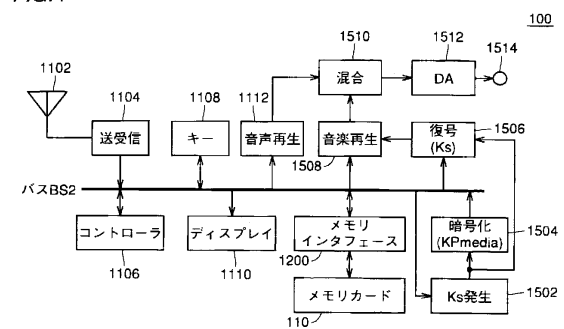


【図 2】

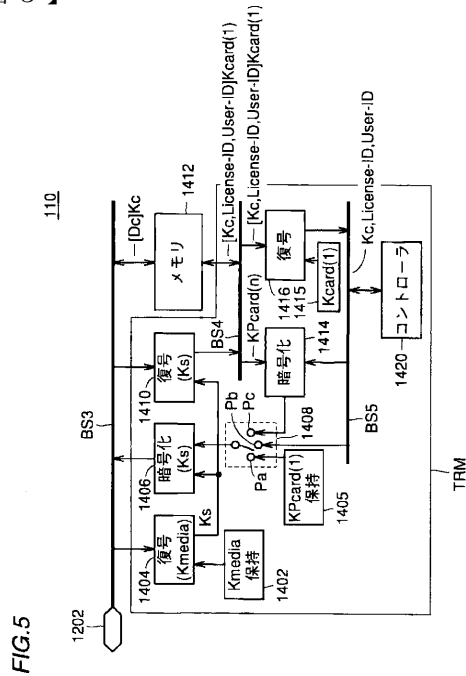
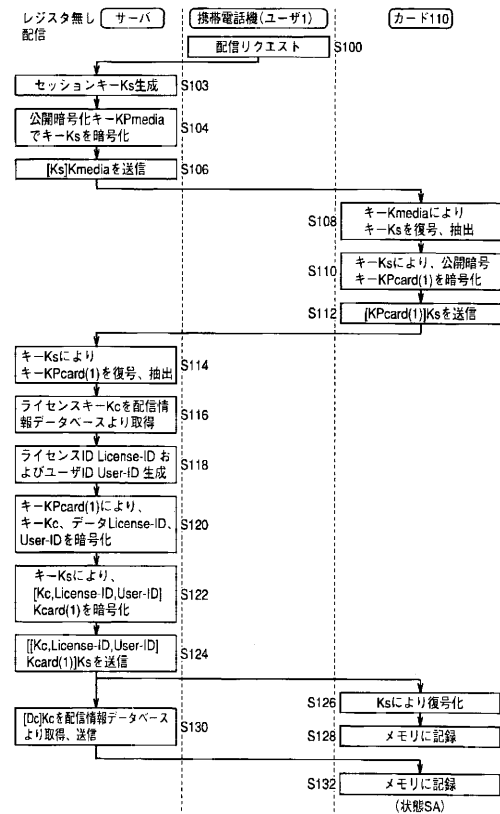
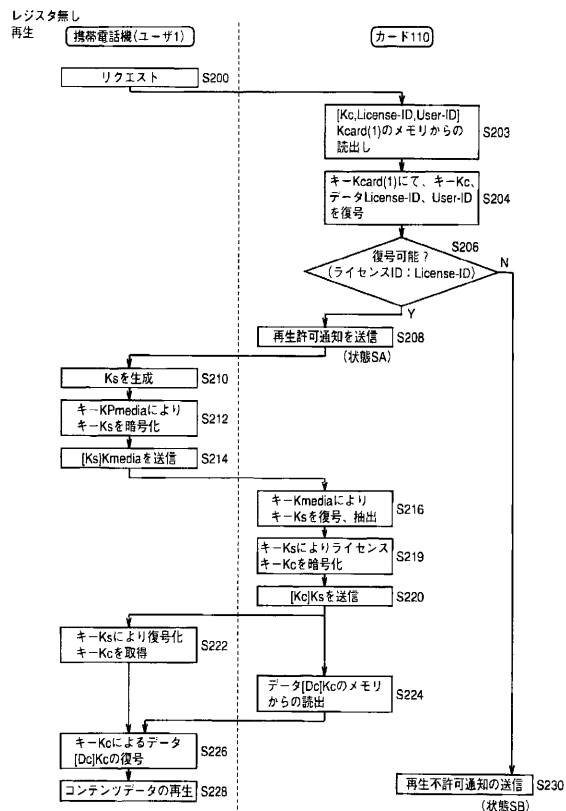
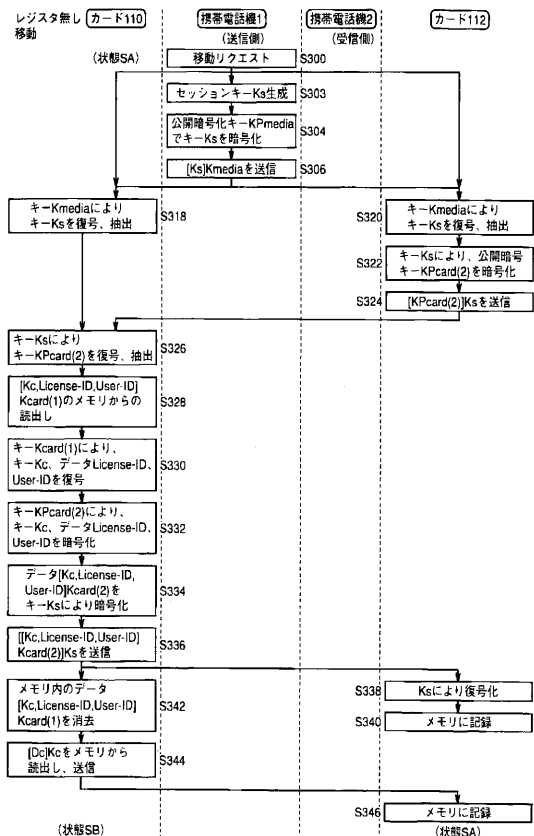
FIG.2

記号	属性	特性
Kmedia	秘密復号鍵	全てのメモリカードに共通
Kcard(n)	秘密復号鍵	メモリカード毎に異なる
KPcard(n)	公開暗号化鍵	Kcard(n)と対を成す KPcard(n)により暗号化されたデータ は、Kcard(n)で復号可能
KPmedia	公開暗号化鍵	Kmediaと対を成す KPmediaにより暗号化されたデータ は、Kmediaで復号可能
Ks	共通鍵	通信毎 (例: アクセス毎) に発生 配信サーバ、携帯電話機にて管理
Kc	共通鍵	暗号化コンテンツデータの復号鍵
License-ID	再生に関する 情報	例: 曲目の特定情報 再生回数の制限情報
User-ID	受信者を識別 する情報	例: 電話番号
Dc	コンテンツ データ	例: 音楽情報データ
[De]Kc	暗号化コン テンツデータ	共通鍵Kcにより暗号化されたコンテ ンツデータ

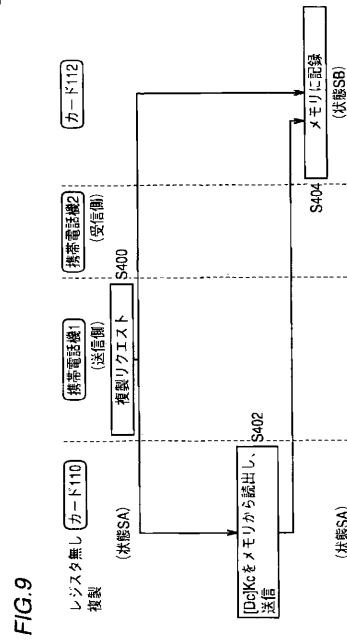
【図 4】



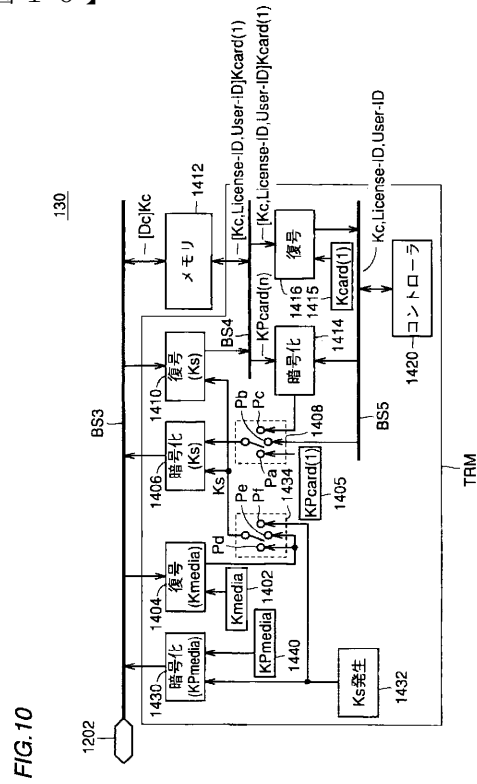
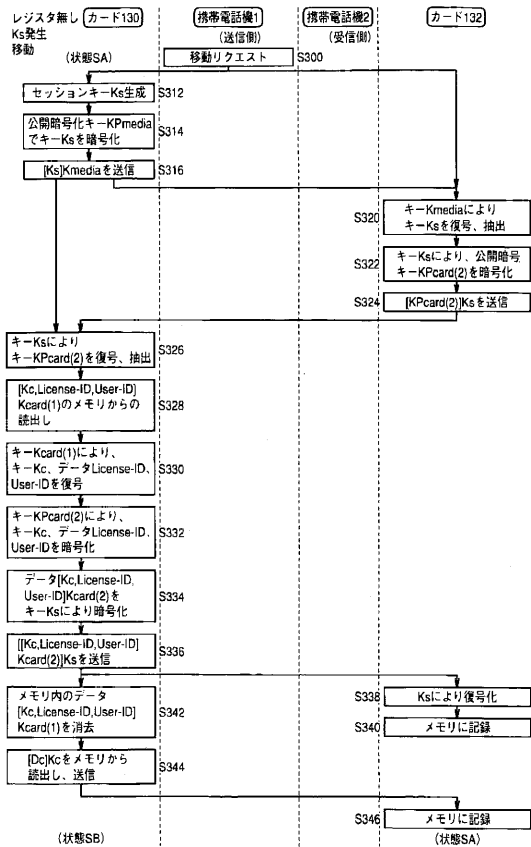
【図 5】

【図 6】
FIG. 6【図 7】
FIG. 7【図 8】
FIG. 8

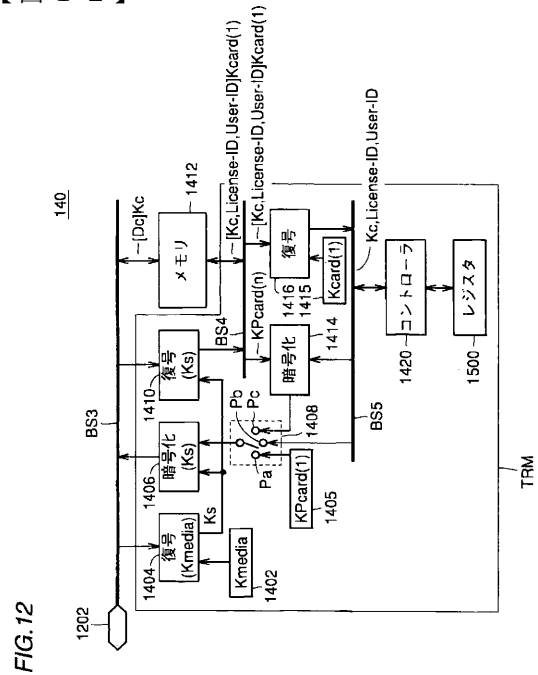
【図 9】

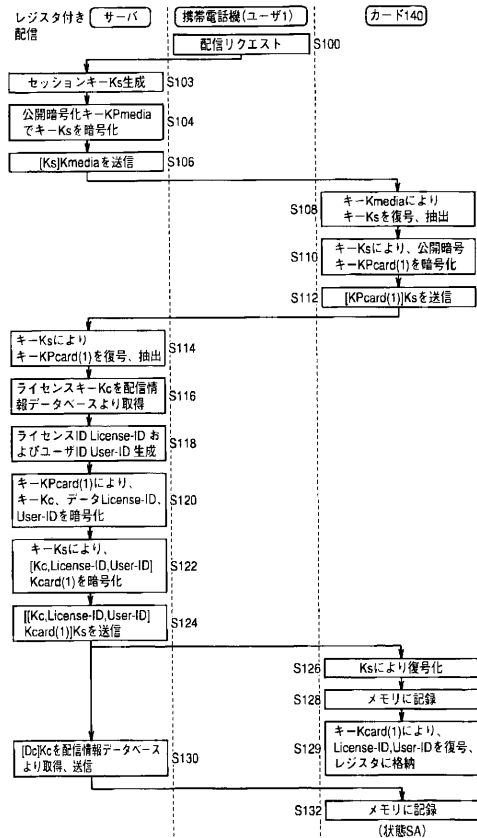
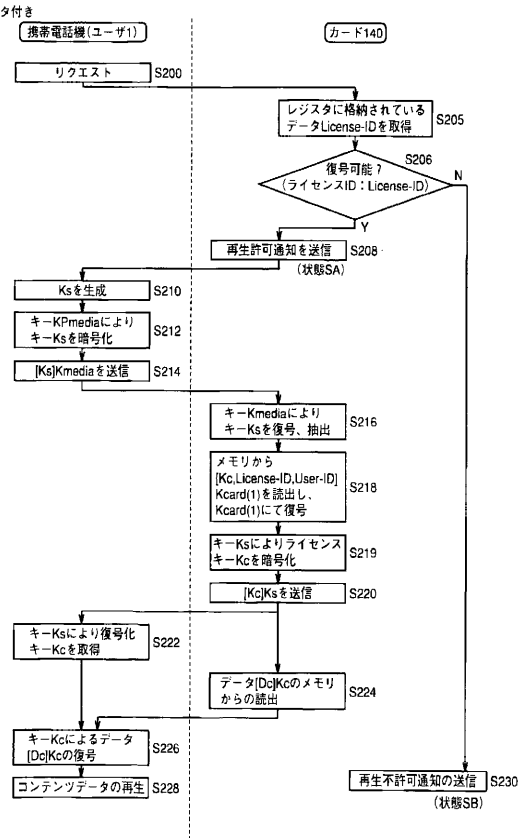
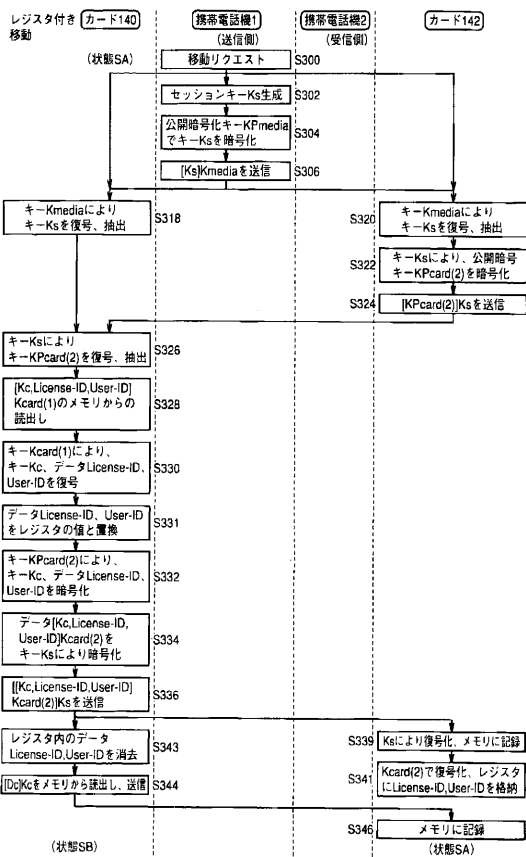


【図 10】

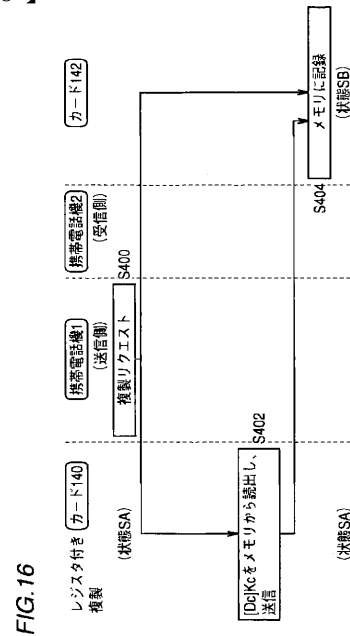
【図 11】
FIG. 11

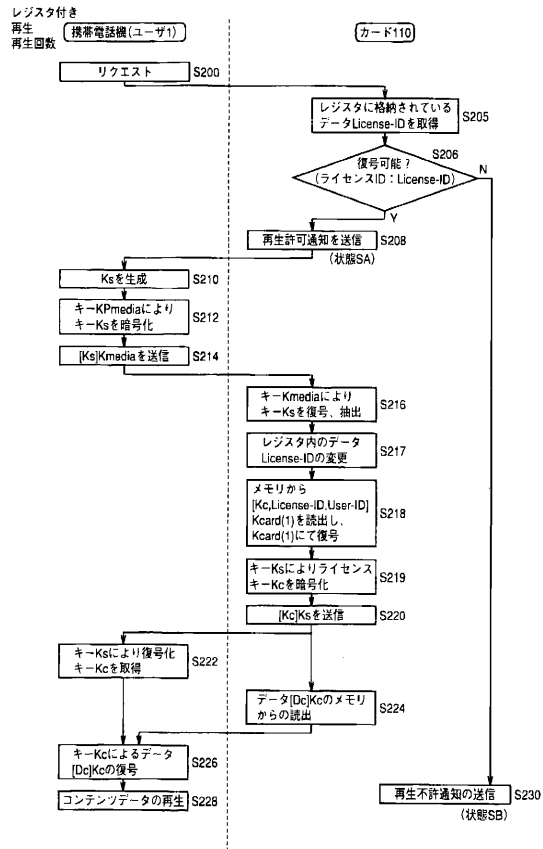
【図 12】



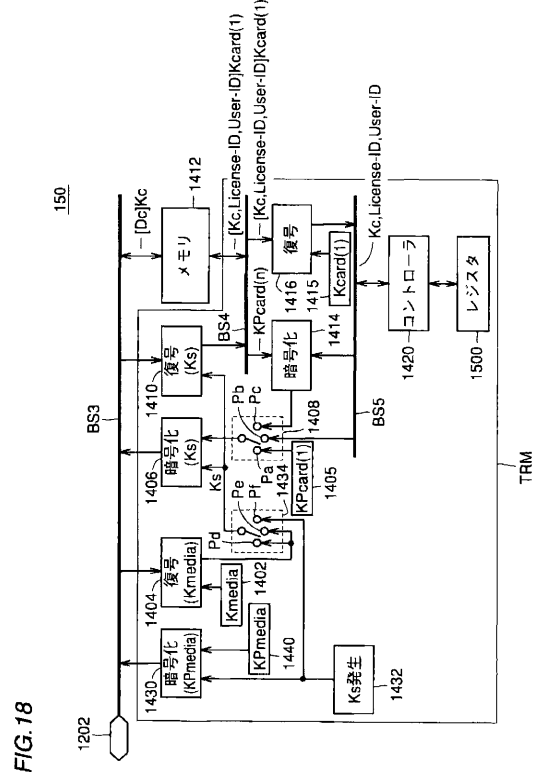
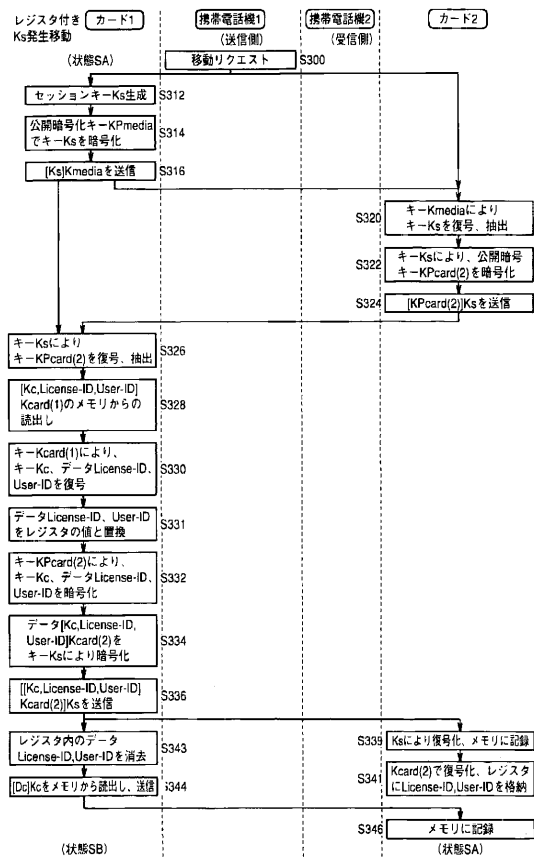
【図 13】
FIG. 13【図 14】
FIG. 14【図 15】
FIG. 15

【図 16】

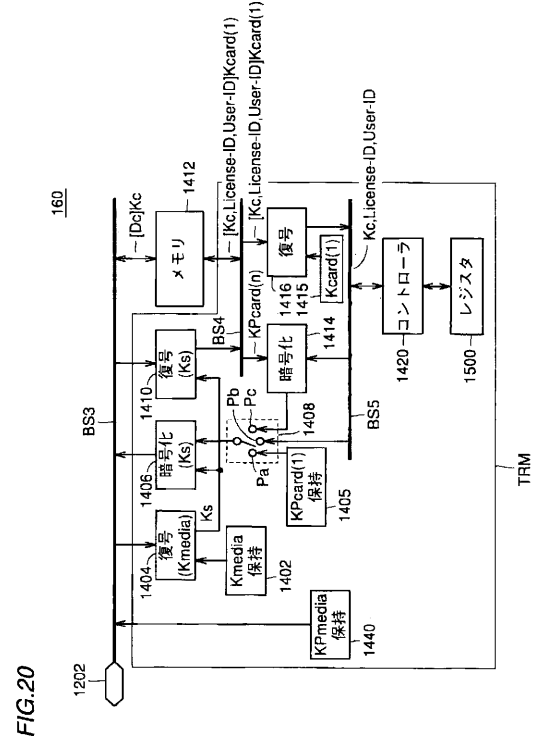


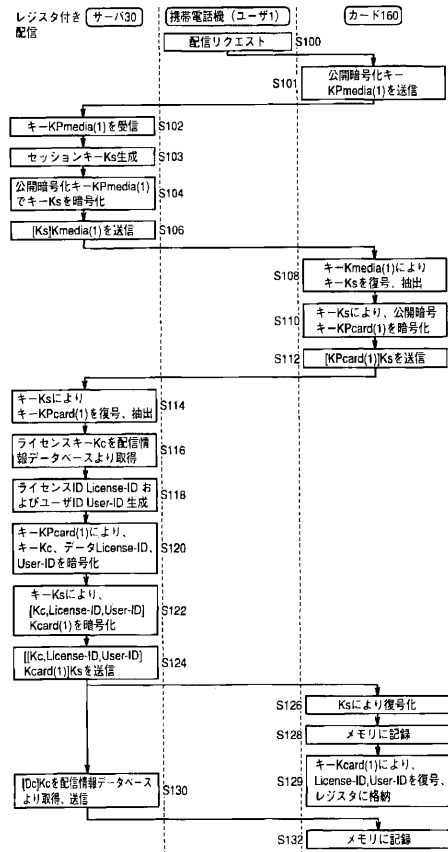
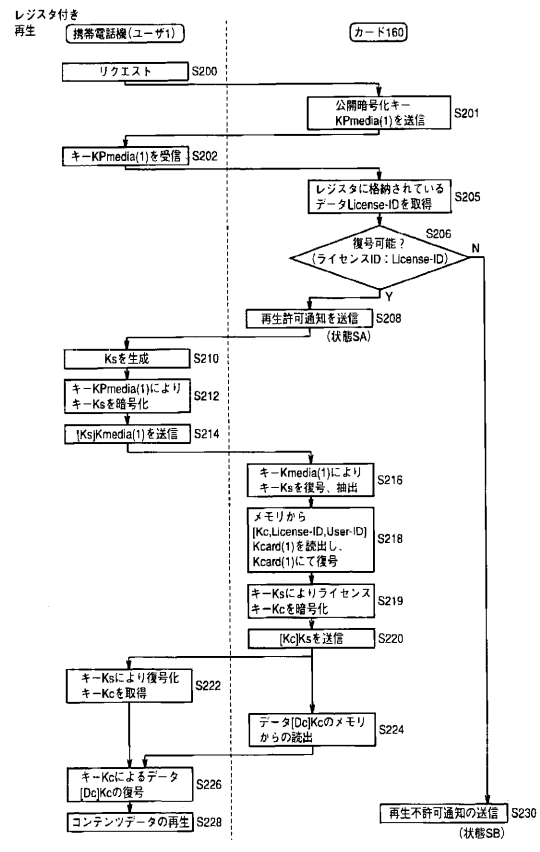
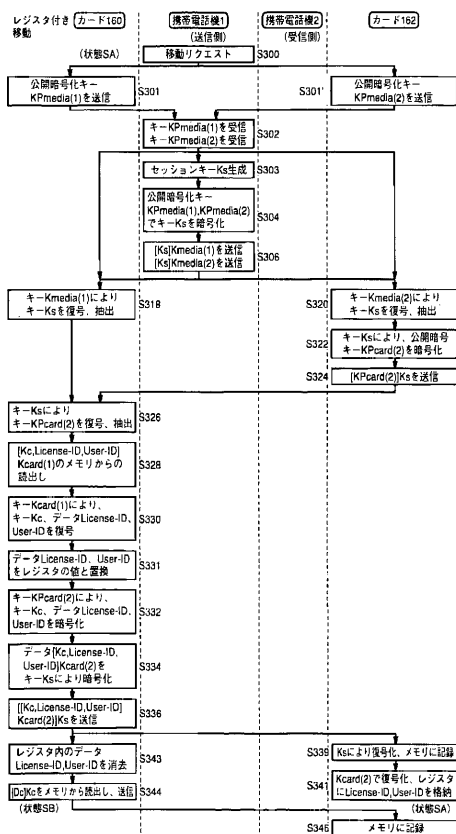
【図 17】
FIG. 17

【図 18】

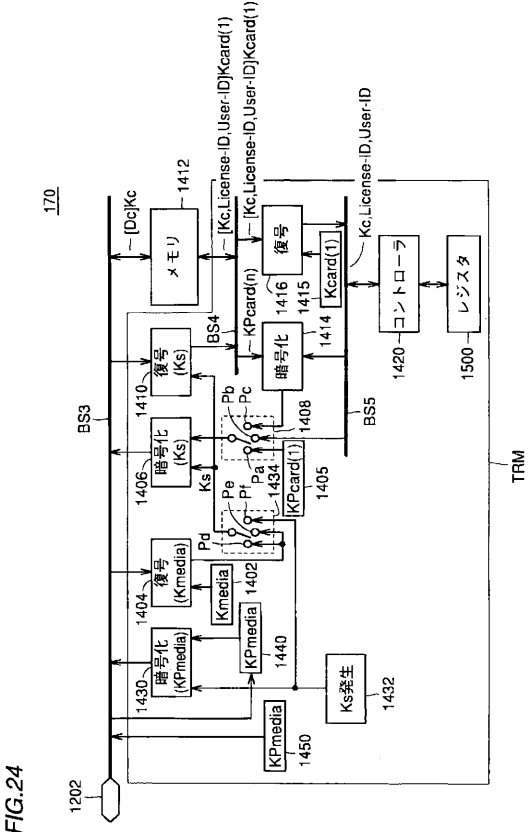
【図 19】
FIG. 19

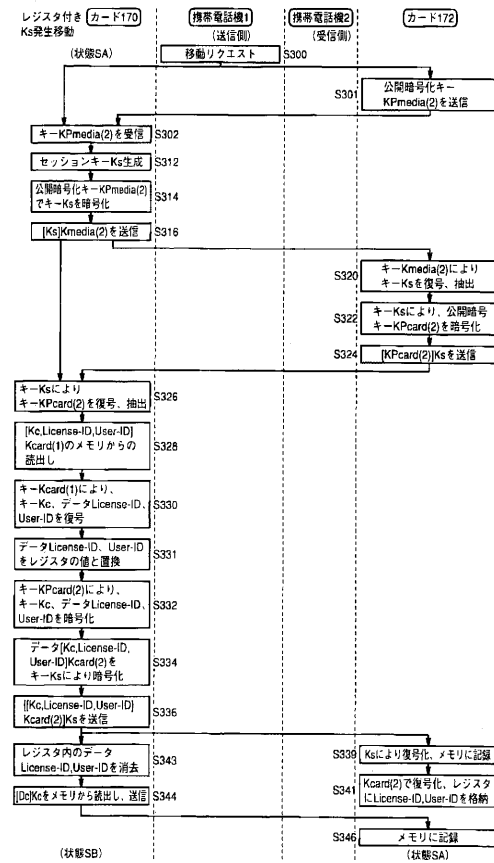
【図 20】



【図 2 1】
FIG.21【図 2 2】
FIG.22【図 2 3】
FIG.23

【図 2 4】



【図 25】
FIG.25

【図 26】

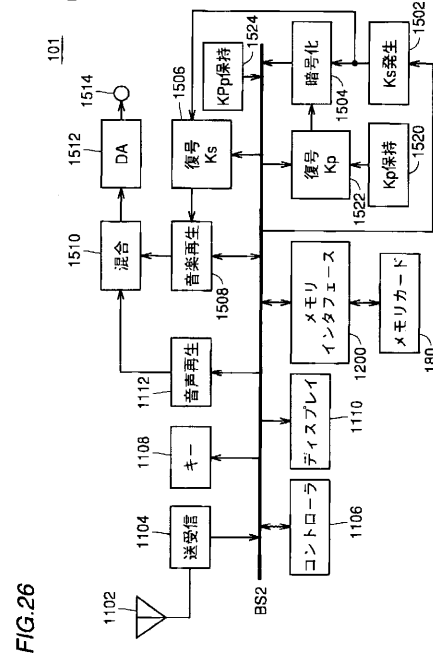


FIG.26

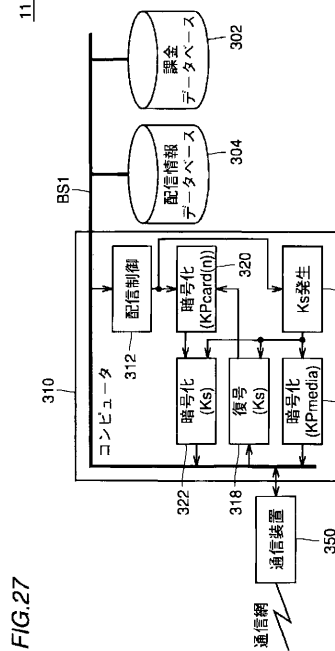
【図 27】
11

FIG.27

【図 28】

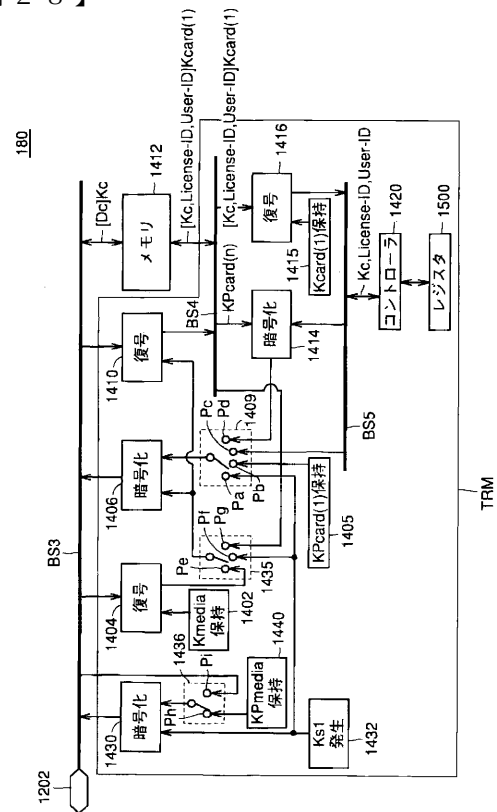
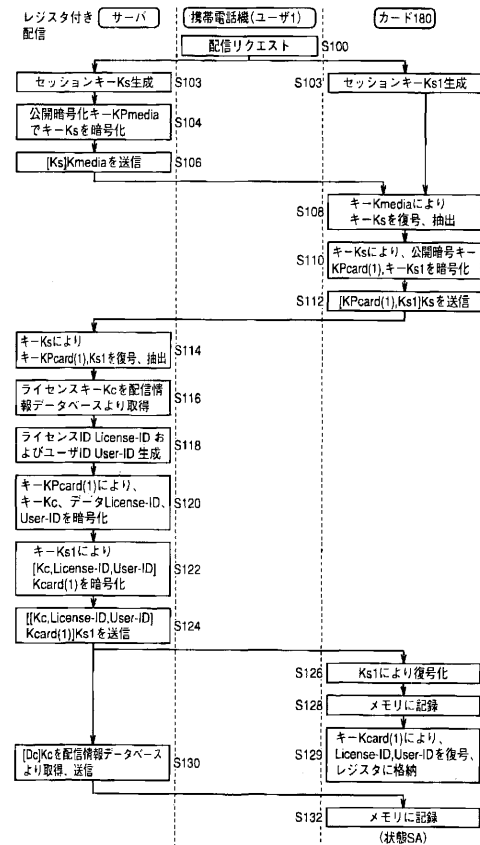
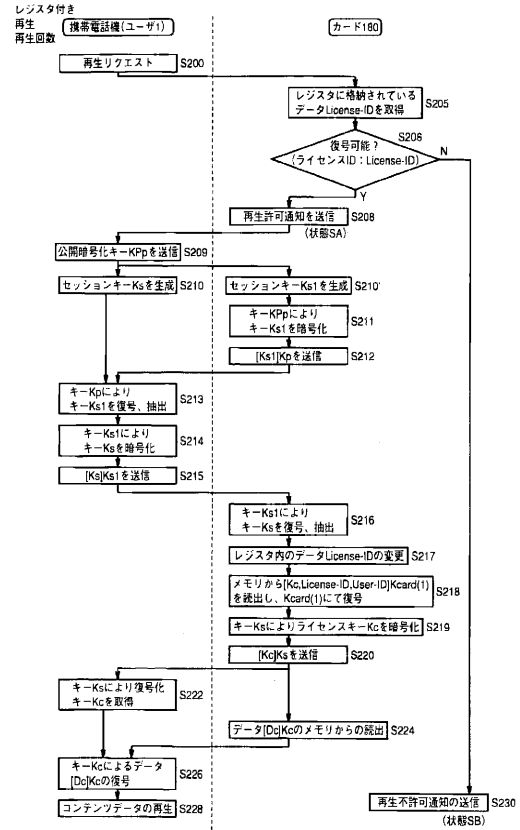
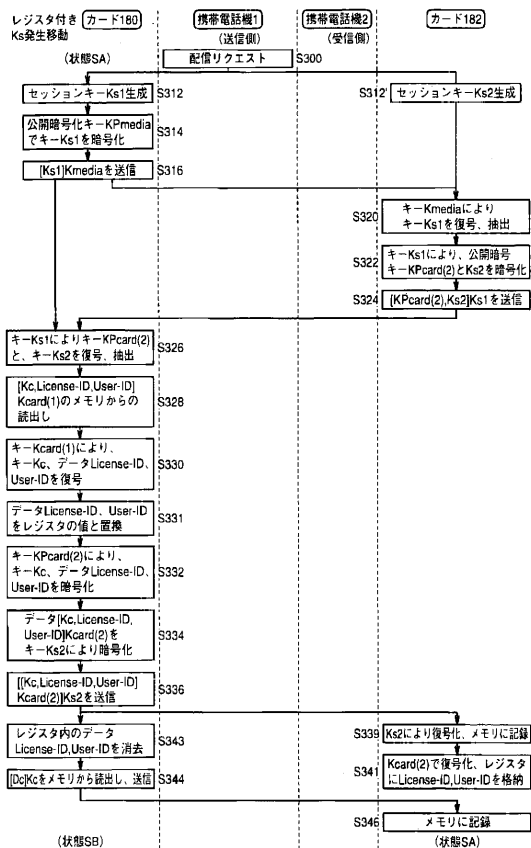
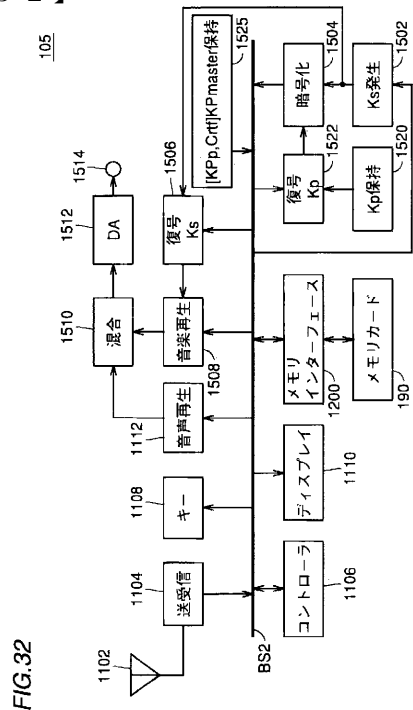


FIG.28

【図 29】
FIG.29【図 30】
FIG.30【図 31】
FIG.31

【図 32】



【図 3 3】

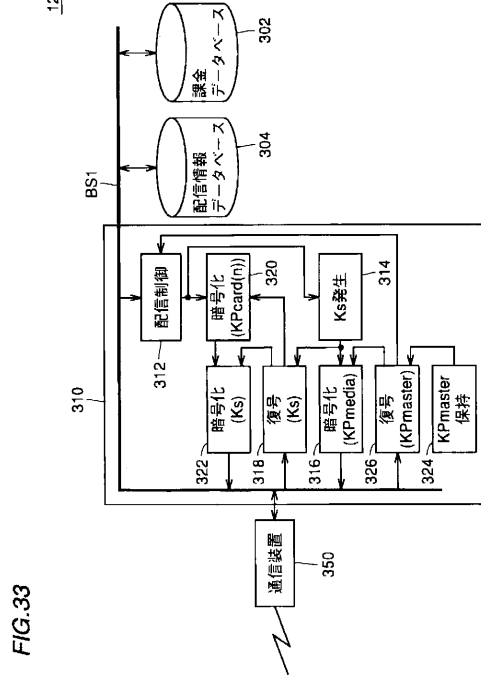


FIG.33

【図 3 4】

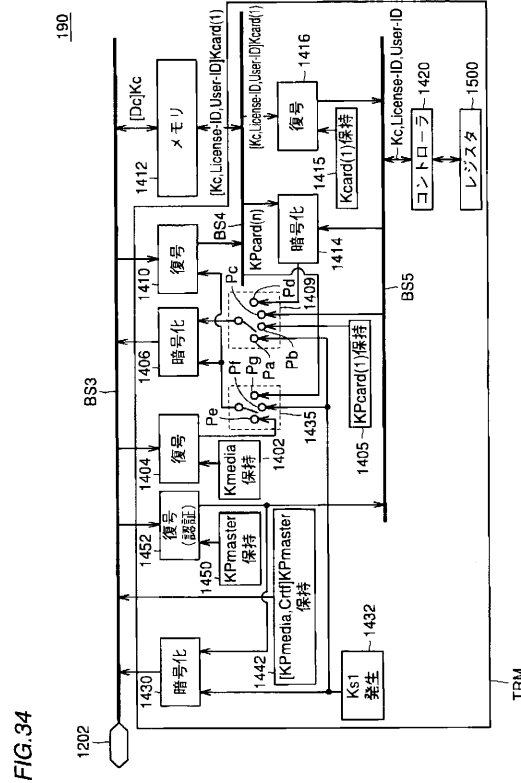


FIG.34

【図 3 5】

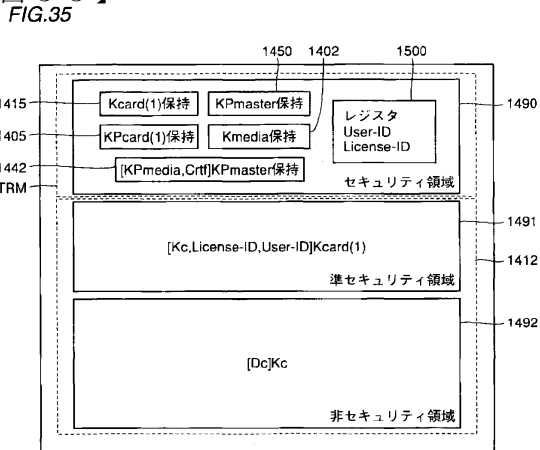


FIG.35

【図 3 6】

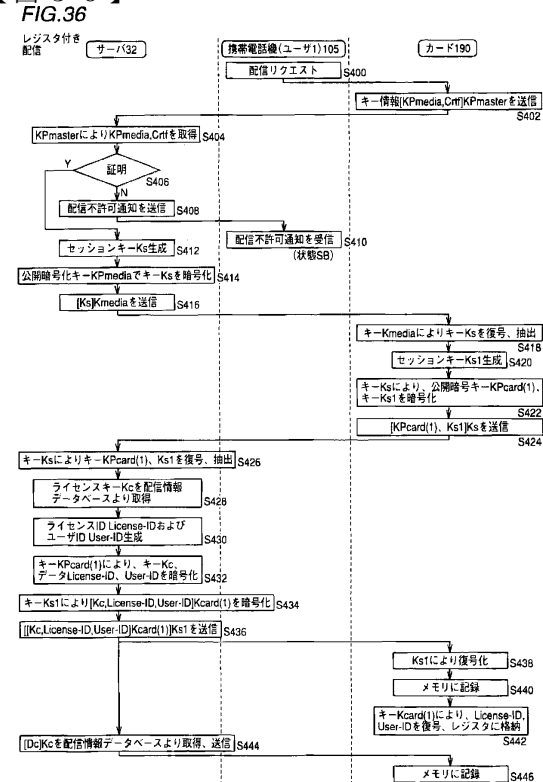
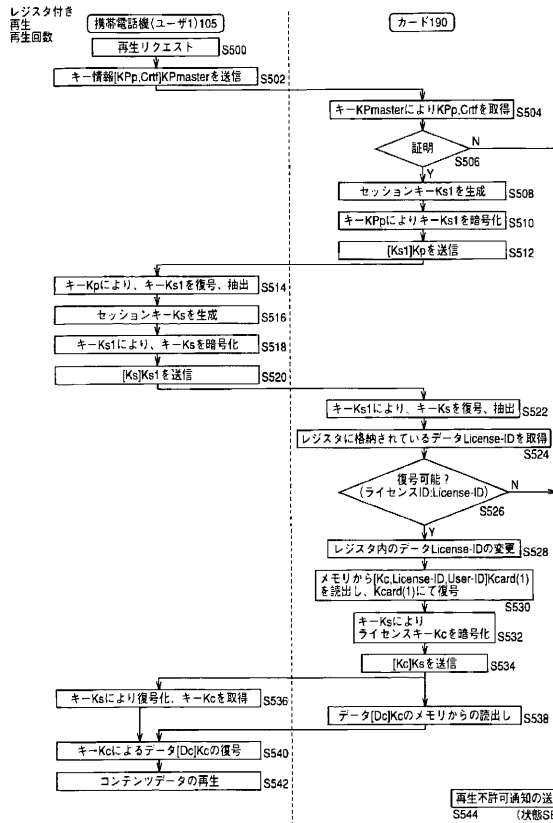
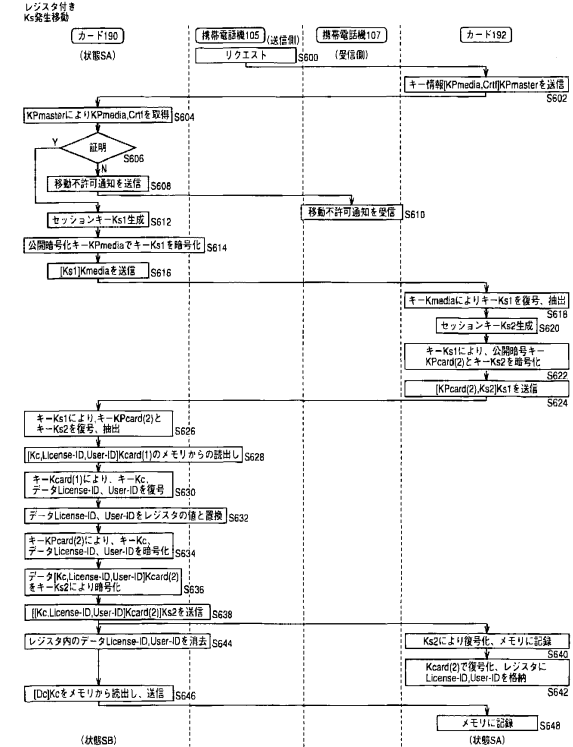
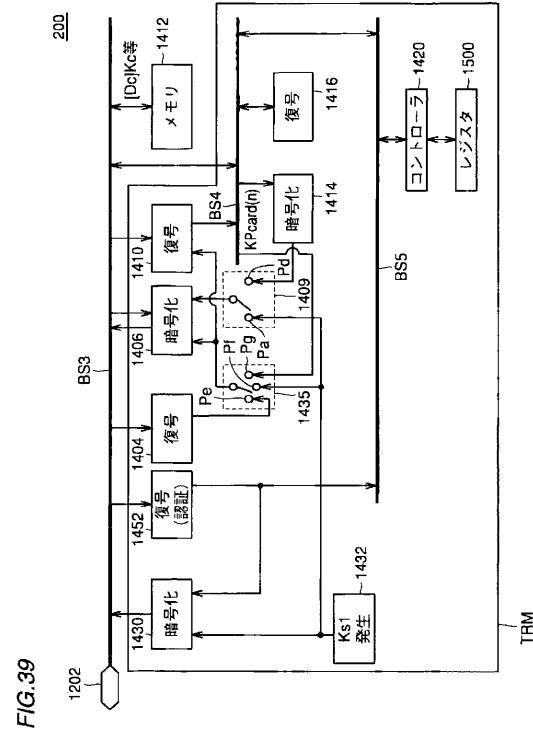
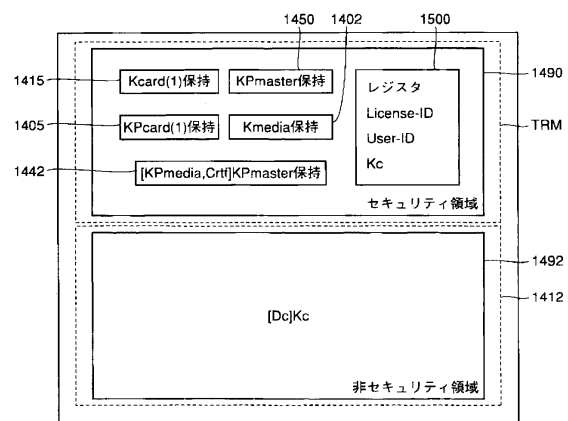
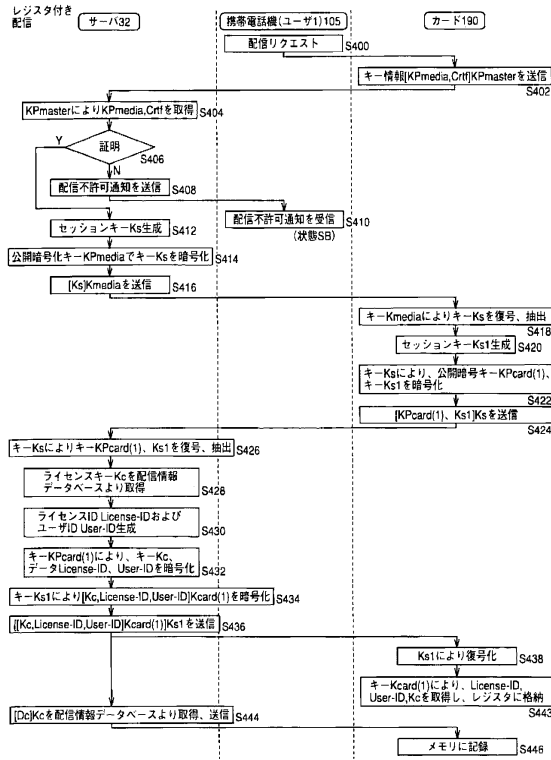
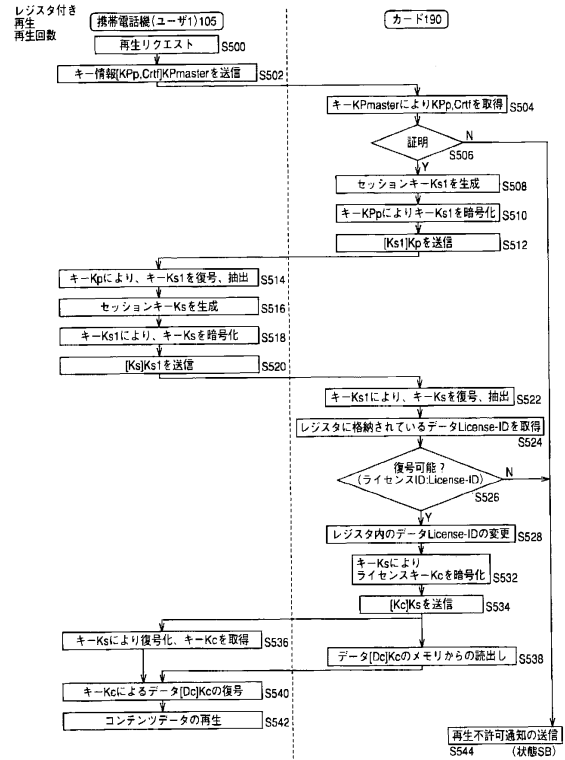
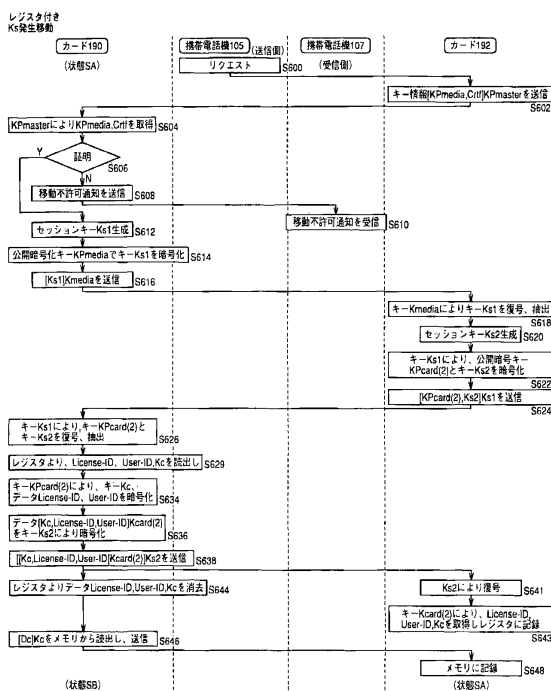


FIG.36

【図 37】
FIG.37【図 38】
FIG.38【図 39】
FIG.39【図 40】
FIG.40

【図 4 1】
FIG.41【図 4 2】
FIG.42【図 4 3】
FIG.43

フロントページの続き

(51)Int.Cl.		F I	
G 1 0 L	19/00	(2006.01)	G 0 6 F 12/14 5 4 0 P
H 0 4 H	1/00	(2006.01)	G 0 6 F 12/14 5 5 0 B
H 0 4 L	9/08	(2006.01)	G 0 6 K 19/00 N
H 0 4 L	9/32	(2006.01)	G 1 0 L 19/00 2 4 0
H 0 4 M	3/42	(2006.01)	G 1 0 L 19/00 3 1 3 B
H 0 4 M	3/493	(2006.01)	H 0 4 H 1/00 6 2 1
H 0 4 M	11/08	(2006.01)	H 0 4 L 9/00 6 0 1 A
			H 0 4 L 9/00 6 0 1 B
			H 0 4 L 9/00 6 7 3 E
			H 0 4 M 3/42 E
			H 0 4 M 3/493
			H 0 4 M 11/08

- (74)代理人 100085132
弁理士 森田 俊雄
- (74)代理人 100091409
弁理士 伊藤 英彦
- (74)代理人 100096781
弁理士 堀井 豊
- (73)特許権者 503121103
株式会社ルネサステクノロジ
東京都千代田区大手町二丁目6番2号
- (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 100096781
弁理士 堀井 豊
- (72)発明者 畑中 正行
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 蒲田 順
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 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 小谷 誠剛
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 古田 茂樹
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 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
- (72)発明者 利根川 忠明
東京都小平市上水本町5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 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 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

審査官 古市 徹

(56)参考文献 特開平05-257816 (JP, A)
特開平08-186667 (JP, A)
特開平08-069419 (JP, A)
特開平11-328033 (JP, A)
特開昭62-053042 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G10K 15/02
G06F 21/20
G06F 21/24
G06K 19/07
G06Q 50/00
G10L 19/00
H04H 1/00
H04L 9/08
H04L 9/32
H04M 3/42
H04M 3/493
H04M 11/08