

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年11月29日 (29.11.2001)

PCT

(10) 国際公開番号
WO 01/91365 A1

- (51) 国際特許分類: H04L 9/08, 9/32, G09C 1/00, G06F 15/00, H04Q 7/38
- (21) 国際出願番号: PCT/JP01/04240
- (22) 国際出願日: 2001年5月21日 (21.05.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2000-149989 2000年5月22日 (22.05.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP];

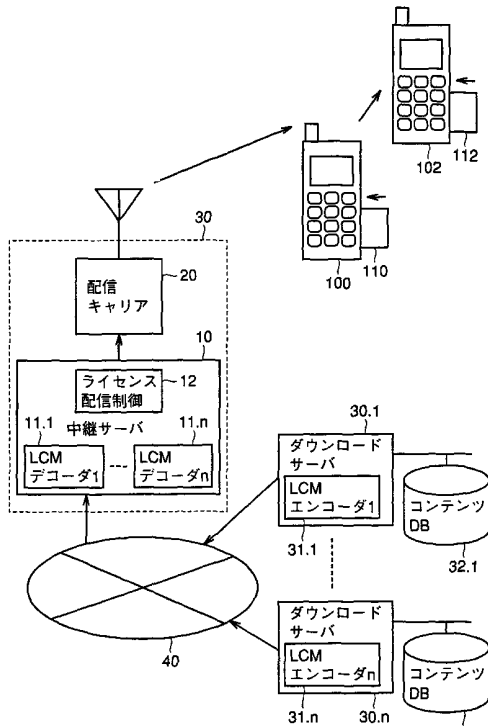
〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社ピーエフユー (PFU LIMITED) [JP/JP]; 〒929-1192 石川県河北郡宇ノ気町字宇野気又98番地の2 Ishikawa (JP). 株式会社日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).

- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 堀 吉宏 (HORI, Yoshihiro) [JP/JP];

[続葉有]

(54) Title: DATA DISTRIBUTION SYSTEM

(54) 発明の名称: データ配信システム



(57) Abstract: Through the internet (40), download servers (31. 1 to 30. n) transmit content data encrypted by LCM encoders (31.1 to 31.n) according to encryption methods corresponding to the download servers (30.1 to 30.n). In response to a content distribution request of a mobile telephone (100), a distribution server (30) receives the data through the Internet (40), decodes the received data by LCM decoders (11.1 to 11.n), encrypts the content data requested by the mobile telephone (100) by a predetermined encryption method, and distributes it by radio.

- 10...RELAY SERVER
- 11.1...LCM DECODER 1
- 11.n...LCM DECODER n
- 12...LICENSE DISTRIBUTION CONTROL
- 30.1...DOWNLOAD SERVER
- 31.1...LCM ENCODER 1
- 30.n...DOWNLOAD SERVER
- 31.n...LCM ENCODER n
- 32.1...CONTENT DB
- 32.n...CONTENT DB
- 20...DISTRIBUTION CARRIER



WO 01/91365 A1

[続葉有]



- 〒570-8677 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 Osaka (JP). 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 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 Kanagawa (JP). 高橋政孝 (TAKAHASHI, Masataka) [JP/JP]; 〒929-1192 石川県河北郡宇ノ気町宇野気又98番地の2 株式会社 ピーエフユー内 Ishikawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 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 Tokyo (JP).
- (74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 三井住友銀行南森町ビル Osaka (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM,

DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

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

(57) 要約:

インターネット (40) は、複数のダウンロードサーバ (30. 1~30. n) から、それぞれ対応する暗号化方式に従ってLCMエンコーダ (31. 1~31. n) より暗号化されたコンテンツデータを伝送する。配信サーバ (30) は、携帯電話機 (100) からのコンテンツ配信要求に応じて、インターネット (40) からのデータを受けて、LCMデコーダ (11. 1~11. n) でデコードし、携帯電話機 (100) から要求のあったコンテンツデータを所定の暗号化方式により暗号化して無線配信する。

明細書

データ配信システム

5 技術分野

本発明は、携帯電話やパーソナルコンピュータ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の構成に関するものである。

背景技術

10 インターネットや情報通信網等の進歩により、パーソナルコンピュータや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、例えば、上述のような情報通信網において音楽や映像情報を各ユーザが、
15 音質や画質の劣化を生じさせることなく伝送を行なうことが可能である。

したがって、急拡大する情報通信網を介して著作権物情報の配信を行ない、適切な料金を徴収することが可能であれば、著作権者にとって有益なシステムである。

しかし、このような情報通信網上において、音楽データや画像データ等の著作権の存在する創造物が伝達される場合、適切な著作権保護のための方策が採られないと、著作権の存在するデータの複製が情報通信網内に氾濫し、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。
20

ここで、インターネット経由での配信について見てみると、音楽など著作権が存在するようなコンテンツデータの配信サービスが開始されつつある一方で、携帯電話網を介したコンテンツデータの配信も実用化されようとしている。
25

したがって、インターネット経由で個人のパーソナルコンピュータに向けた配信を行なうダウンロードサーバの系統と、携帯電話網を介したコンテンツデータの配信を行なう配信サーバの系統が、互いにコンテンツデータのやり取りができず、相互に独立したシステムとなるように構成してしまうと、システム側からみれば、

二重の投資が必要となり効率が悪い。また、ユーザの側から見れば、いずれか一方の系統からのみでは、自分の希望するコンテンツの配信が受けられないといった問題も発生しうる。

5 発明の開示

本発明の目的は、インターネットなどの情報通信網を介しても、また、携帯電話網等の情報通信網を介しても、著作権を保護しつつ、ユーザに対して音楽データ等のコンテンツデータの供給を行なうことが可能なデータ配信システムを提供することである。

10 係る目的を達成するために本願発明に係るデータ配信システムは、データ情報通信網と、配信中継サーバとを備える。

データ情報通信網は、複数のコンテンツデータ供給元から、それぞれ対応する複数の第1の所定の暗号化方式により暗号化されたコンテンツデータを伝送する。配信中継サーバは、第1のユーザ端末からのコンテンツ配信要求に応じて、第1
15 のユーザ端末から要求のあったコンテンツデータをデータ情報通信網から受けて、第2の所定の暗号化方式により暗号化して配信する。

配信中継サーバは、複数の第1のコンテンツデータ復号部と、コンテンツデータ暗号化部と、送信部とを含む。複数の第1のコンテンツデータ復号部は、複数のコンテンツデータ供給元からの、複数の第1の所定の暗号化方式により暗号化
20 されたコンテンツデータを復号する。コンテンツデータ暗号化部は、第1のコンテンツデータ復号部の出力を受けて、第2の所定の暗号化方式で暗号化し、暗号化コンテンツデータを生成する。送信部は、暗号化コンテンツデータを配信する。

したがって、本願に係るデータ配信システムでは、インターネットなどの情報通信網を介しても、また、携帯電話網等の情報通信網を介して、著作権を保護し
25 つつ、ユーザに対して手音楽データ等のコンテンツデータの供給を行なうことが可能である。

図面の簡単な説明

図1は、本発明のデータ配信システムの全体構成を概略的に説明するための概

念図である。

図 2 は、データ配信システムにおいて、パーソナルコンピュータ 60 にコンテンツデータの配信を受ける場合を示す概念図である。

5 図 3 は、図 1 に示したデータ配信システムにおいて、使用される通信のための暗号に関する鍵および配信するデータ等の特性を説明する図である。

図 4 は、図 1 に示した中継サーバ 10 の構成を示す概略ブロック図である。

図 5 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。

10 図 6 は、図 5 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。

図 7 は、実施例 1 に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第 1 のフローチャートである。

図 8 は、実施例 1 に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第 2 のフローチャートである。

15 図 9 は、実施例 1 に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第 3 のフローチャートである。

図 10 は、再生セッション時における各部の動作を説明するためのフローチャートである。

20 図 11 は、実施例 1 の変形例におけるコンテンツの購入時に発生する配信動作を説明するための第 1 のフローチャートである。

図 12 は、実施例 1 の変形例におけるコンテンツの購入時に発生する配信動作を説明するための第 2 のフローチャートである。

図 13 は、実施例 1 の変形例におけるコンテンツの購入時に発生する配信動作を説明するための第 3 のフローチャートである。

25

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

[実施例 1]

図 1 は、本発明のデータ配信システムの全体構成を概略的に説明するための概

念図である。

5 なお、以下では、携帯電話網およびインターネット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、ゲームソフト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。

10 図1を参照して、著作権の存在する音楽データを管理し、インターネット40を介して配信するためのダウンロードサーバ30. 1~30. nは、それぞれコンテンツデータ保護のために暗号化処理を行なうライセンスコンプライアントモジュール (Licensed Compliant Module : 以下、LCMと略称する) エンコーダ31. 1~31. nを備える。ダウンロードサーバ30. 1~30. nは、それぞれ対応するコンテンツデータベース32. 1~32. nから読み出したコンテンツデータを、LCMエンコーダ31. 1~31. nにより所定の暗号方式により暗号化した上で、インターネット網40に出力する。LCMエンコーダ31. 15 1~31. nにおけるコンテンツ保護のための暗号化方式はダウンロードサーバ30. 1~31. nにおいて、それぞれが独自に予め定めた暗号化方式を採用しているため、LCMエンコーダ31. 1~31. nにおける処理は、同一の処理であるとは限らない。仮に、同じ暗号化方式を採用していたとしても暗号化および復号処理に用いられる鍵が同一であるとは限らない。

20 したがって、配信中継サーバ (以下、単に「中継サーバ」と呼ぶ) 10は、LCMエンコーダ31. 1~31. nにより暗号化されインターネット網40により伝達されたデータをそれぞれ復号するためのLCMデコーダ11. 1~11. nを備える。中継サーバ10中のライセンス配信制御部12は、LCMデコーダ11. 1~11. nからのデータを受けて、携帯電話網で配信するための暗号化を施した上で、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) を中継サーバ10に中継する。

中継サーバ10は、配信リクエストがあると、ユーザのメモリカードが正規の

機器であることを確認し、要求された音楽データに対応する暗号化データをダウンロードサーバ30. 1～30. nから受取ってLCMデコーダ11. 1～11. nで復号化し、さらに暗号化した上で配信キャリア20の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

5 図1においては、たとえばユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、携帯電話機100中の音楽再生部（図示せず）が正規の機器であることを確認し、上記送信にあたって行なわれた暗号化については復号して上記音楽再生部に与える。

10 さらに、たとえばユーザ1は、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、音楽を聴取することが可能である。

以下では、このような中継サーバ10と配信キャリア（携帯電話会社）20と併せて、配信サーバ30と総称することにする。

15 また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、正規の携帯電話機および正規のメモリカードを購入していないユーザは、配信サーバ30からの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。

20 しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータの配信を受けるたびに発生する著作権料を、配信キャリア20が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

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
25 102により、配信サーバ30から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ2が直接配信サーバ30から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ1から、そのコンテンツデータをコピーできること

を可能としておけば、ユーザにとっての利便性が向上する。

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

図1に示すように、ユーザ1が受信したデータについて、コンテンツデータそのものをコピーさせ、かつ、ユーザ1が持つ当該コンテンツデータを再生可能とするために必要なライセンス情報（再生するための権利に対応する情報）をユーザ2に対して移動させる場合をライセンス情報の「移動」と呼ぶ。この場合に、携帯電話機100および102を介して、メモ리카ード110と112との間で暗号化されたコンテンツデータおよびライセンス情報が移動される。すなわち、移動先のメモ리카ード112に対して移動元のメモ리카ード110からライセンス情報を出力するとき、メモ리카ード110からライセンス情報が削除され、ユーザ1は当該コンテンツデータの再生ができない。ここで、「ライセンス情報」は、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なコンテンツ復号キーと、著作権保護にかかわる情報であるライセンスIDやアクセス再生に関する制限情報等の著作権情報とを有する。

「移動」に対して、著作権者が許可するライセンス情報についてのみ、ライセンス情報のコピーを行なうことができる。この場合をライセンス情報の「複製」と呼ぶ。複製先のメモリーカード112に対して複製元のメモ리카ード110からライセンス情報を出力した後も、メモ리카ード110からライセンス情報が削除されない。すなわち、ユーザ1も、ユーザ2も当該コンテンツデータを再生することが可能である。

さらには、ライセンス情報の「移動」あるいは「複製」を伴わないまま、コンテンツデータのみをコピーすることもできる、この場合、ライセンス情報を伴わないため、ユーザ2は、当該コンテンツデータを再生することができない。ここでは説明しないが、コンテンツ復号キーを含むライセンス情報のみを配信する新たな配信によって、ユーザ2は当該コンテンツデータを再生できるようになる。

このような構成とすることによって、一旦配信サーバ30より配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機100および102がPHS（Personal Handy Phone）であ

る場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ1とユーザ2との間における情報の移動を行なうことが可能である。

5 図2は、図1に示したデータ配信システムにおいて、インターネットのプロバイダ50を介して、パーソナルコンピュータ60にコンテンツデータの配信を受ける場合を示す概念図である。

パーソナルコンピュータ60のユーザは、ダウンロードサーバ30. 1~30. nのうちのダウンロードサーバ30. iと契約しているものとする。

10 パーソナルコンピュータ60には、ハードウェアまたはソフトウェアとして、ダウンロードサーバ30. iに対応するLCMデコーダ62が搭載される。

パーソナルコンピュータ60では、プロバイダ50から配信されたコンテンツデータが、LCMデコーダ62により復号化された後、さらにローカルLCMエンコーダ64で再度暗号化された後に記録装置66中に格納される。ユーザが音楽を聴取する際には、記録装置66に格納された暗号化コンテンツデータを、記録装置66から読み出し、ローカルLCMエンコーダ66にて行なった暗号化をローカルLCMデコーダ67で復号し、平文化してから音楽再生部68にて音楽が再生される。

20 このような構成とすることで、ダウンロードサーバ30. 1~30. nは契約を行なったユーザのパーソナルコンピュータ60に対してインターネット40およびプロバイダ50経由で配信することが可能であると同時に、中継サーバ10から配信を受けられる携帯電話機100およびメモリカード110のユーザに対して、キャリア20を介して携帯電話網により配信を行なうことも可能となる。

なお、図2のパーソナルコンピュータ70については後に説明を行なう。

[システムの鍵およびデータの構成]

25 図3は、図1に示した配信サーバ30からユーザの携帯電話機100への配信において、使用される通信のための暗号に関する鍵および配信するデータ等の特性を説明する図である。

まず、配信サーバ30より配信されるDataは、音楽データ等のコンテンツデータである。コンテンツデータDataは、後に説明するように、少なくともコン

コンテンツ復号キー K_c によって復号可能な暗号化が施された暗号化コンテンツデータ $\{Data\}K_c$ という形式で、配信サーバ 30 よりユーザに配布される。

なお、以下においては、 $\{Y\}X$ という表記は、データ Y を、鍵 X により復号可能な暗号に変換した情報であることを示すものとする。

5 さらに、配信サーバ 30 からは、コンテンツデータとともに、コンテンツデータに関する著作あるいはサーバアクセス関連等の平文データとしての付加データ $Data-inf$ が配布される。すなわち、付加データ $Data-inf$ には、コンテンツデータの曲目などコンテンツデータを特定するための情報や、配信サーバ 30 が、いずれのサーバであるかを特定するための情報等が含まれる。

10 次に、コンテンツデータの暗号化や復号・再生処理や、コンテンツ再生回路である携帯電話機や記録装置であるメモリカードの正当性に対する認証に関わる鍵として、以下のものがある。

すなわち、上述したとおり、暗号化されて供給されたコンテンツデータを復号するためのコンテンツ復号キー K_c と、コンテンツ再生回路（携帯電話機 100）の公開暗号化鍵 $KP_p(x)$ と、メモリカードの公開暗号化鍵 $KP_{mc}(x)$ とがそれぞれ設けられる。

公開暗号化鍵 $KP_p(x)$ および $KP_{mc}(x)$ により暗号化されたデータは、コンテンツ再生回路（携帯電話機 100）の固有の秘密復号鍵 $K_p(x)$ およびメモリカード固有の秘密復号鍵 $K_{mc}(x)$ によってそれぞれ復号可能である。公開暗号化鍵 $KP_p(x)$ および $KP_{mc}(x)$ は、それぞれ秘密復号鍵 $K_p(x)$ および $K_{mc}(x)$ によってそれぞれ復号可能な非対称暗号化鍵である。これら固有の秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる内容を有する。ここで、携帯電話機やメモリカードの種類とは、それらを製造するメーカーの種類や、製造時期（製造ロット）の違い等に基づき規定され、自然数 x は、各メモリカードおよびコンテンツ再生回路（携帯電話機）の種類を区別するための番号を表わす。

25 さらに、配信システム全体で共通に運用される公開認証鍵 KP_{ma} が存在する。なお、上述したメモリカードおよびコンテンツ再生部ごとに設定される公開暗号化鍵 $KP_{mc}(x)$ および $KP_p(x)$ は、上述の認証鍵 KP_{ma} によって認証可能な証明付データとして $\{KP_{mc}(x)\}KP_{ma}$ および $\{KP_p(x)\}KP_{ma}$ の形式で、出荷時にメモリカード

および携帯電話機にそれぞれ記録される。なお、以降では、公開暗号化鍵を含む証明付データを認識データと称する。

さらに、システムを構成する機器、すなわち、コンテンツ再生回路である携帯電話機100やメモリカード110の動作を制御するための情報として、利用者がコンテンツ復号キー等を購入する際に、携帯電話機100から配信サーバ30に対してその購入条件を指定するために送信される購入条件情報ACと、購入条件情報ACに応じて、配信サーバ30からメモリカード110に対して配信され、メモリカード110へのアクセス回数に対する制限等を示すアクセス制御情報AC1と、配信サーバ30から携帯電話機100に対して配信され、コンテンツ再生回路の再生条件の制限を示す再生回路制御情報AC2とが存在する。コンテンツ再生回路の再生条件とは、たとえば、新曲のプロモーションとして廉価にまたは無償でサンプルを配信する場合などに、各コンテンツデータの冒頭の所定時間のみ再生を許す等の条件を意味する。

また、メモリカード110内のデータ処理を管理するための鍵として、メモリカードという記録装置ごとに設定される公開暗号化鍵 $KP_m(i)$ (i : 自然数) と、公開暗号化鍵 $KP_m(i)$ で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 $K_m(i)$ とが存在する。ここで、自然数 i は、各メモリカードを区別するための番号を表わす。

さらに、データの通信時に使用される鍵（キー）等として以下のものがある。すなわち、メモリカード外とメモリカード間でのデータ授受における秘密保持のための鍵として、コンテンツデータの配信、再生および移動が行なわれるごとにサーバ30、携帯電話機100または102、メモリカード110または112において生成される共通鍵 $K_{s1} \sim K_{s4}$ が用いられる。

ここで、共通鍵 $K_{s1} \sim K_{s4}$ は、配信サーバ、携帯電話もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 $K_{s1} \sim K_{s4}$ を「セッションキー」とも呼ぶこととする。

これらのセッションキー $K_{s1} \sim K_{s4}$ は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理され

る。

具体的には、セッションキーKs1は、配信サーバ内のライセンスサーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカードによって配信セッションおよび移動（受信側）セッションごとに発生し、セッションキーKs3は、同様にメモリカードにおいて再生セッションおよび移動（送信側）セッションごとに発生する。セッションキーKs4は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでコンテンツ復号キー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

さらに、配信サーバと携帯電話機との間で授受されるデータとしては、コンテンツデータをシステムが識別するためのコンテンツIDや、ライセンスの発行がいつ、誰に対して行なわれたかを特定するための管理コードであるライセンスIDや、配信セッションごとに生成され、各配信セッションを特定するためのコードであるトランザクションIDなどがある。なお、ライセンスIDとしてトランザクションIDを兼用しても良い。

[中継サーバ10の構成]

図4は、図1に示した中継サーバ10の構成を示す概略ブロック図である。

中継サーバ10は、インターネット網40との間でデータを授受するための通信装置301と、通信装置301を介して、ダウンロードサーバ30.1~30.nの各LCMエンコーダ31.1から31.nとの間でデータの授受を行ない、ダウンロードサーバ30.1~30.nからダウンロードする音楽データ（コンテンツデータ）を保護するために、それぞれに備えられたLCMエンコーダ31.1~31.nとの間でデータ伝送に関する処理や、LCMエンコーダ31.1~31.nにおいて暗号化された音楽データ（暗号化コンテンツデータ）をそれぞれ受けて復号するためのLCMデコーダ11.1~11.nと、コンテンツデータを暗号化するための鍵（コンテンツ復号キー）Kcを発生するKc発生部306と、LCMデコーダ11.1~11.nからのコンテンツデータを鍵（コンテンツ復号キー）Kcで暗号化するための暗号化処理部308と、付加情報、コンテ

ンツIDおよびライセンスID等のデータを保持するためのライセンスデータベース302と、各ユーザごとに音楽データのライセンス情報の配信に従った課金データを保持するための課金データベース304と、ライセンスデータベース302および課金データベース304からのデータをデータバスBS0を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

データ処理部310は、データバスBS0上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカードから携帯電話機を介して送られてきた認証データ{KPmc(y)}KPmaを通信装置350およびデータバスBS1を介して受けて、認証鍵KPmaに対する復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られた公開暗号化鍵KPmc(y)を用いて暗号化して、データバスBS1に出力するための暗号化処理部318と、各ユーザにおいてセッションキーKs1によって暗号化された上で送信されたデータをデータバスBS1をより受けて、復号処理を行なう復号処理部320とを含む。

データ処理部310は、さらに、配信制御部315から出力されたライセンス情報を復号処理部320によって得られたメモリカード固有の公開暗号化鍵KPm(x)によって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してデータバスBS1に出力するための暗号化処理部328とを含む。

[携帯電話機100の構成]

図5は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

携帯電話機100においては、種類（クラス）を表わす自然数xは、 $x = 1$ とする。

携帯電話機100は、携帯電話網により無線伝送される信号を受信するための

アンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機100からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのデータバスBS2と、データバスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106とを含む。

携帯電話機100は、さらに、外部からの指示を携帯電話機100に与えるためのタッチキー部1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるためのディスプレイ1110と、通常の話動作において、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再生するための音声再生部1112と、外部との間でデータの授受を行なうためのコネクタ1120と、コネクタ1120からのデータをデータバスBS2に与え得る信号に変換し、または、データバスBS2からのデータをコネクタ1120に与え得る信号に変換するための外部インタフェース部1122とを含む。

携帯電話機100は、さらに、暗号化音楽データ（暗号化コンテンツデータ）を記憶し、かつ復号処理するための情報を随時格納するために着脱可能なメモリカード110と、メモリカード110とデータバスBS2との間のデータの授受を制御するためのメモリインタフェース1200と、携帯電話機のクラスごとに設定される公開暗号化鍵 $K_{p(1)}$ を、認証鍵 K_{pma} で認証可能な状態に暗号化した認証データを保持する認証データ保持部1500とを含む。

携帯電話機100は、さらに、携帯電話機（コンテンツ再生回路）固有の秘密復号鍵である $K_p(1)$ を保持する K_p 保持部1502と、データバスBS2から受けたデータを秘密復号鍵 $K_p(1)$ によって復号し、メモリカードによって発生されたセッションキー K_s3 を得る復号処理部1504と、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいて、メモリカード110との間でデータバスBS2上においてやり取りされるデータを暗号化するためのセッションキー K_s4 を乱数等により発生するセッションキー発生部1508と、生成されたセッションキー K_s4 を復号処理部1504によって得られたセッションキー K_s3 によって暗号化しデータバスBS2に出力する暗号化処理部1506と、データバスBS2上のデータをセッションキー K_s4 によって復号して、

コンテンツ復号キーKc および再生回路制御情報 AC2 を出力する復号処理部1510とをさらに含む。

5 携帯電話機100は、さらに、データバスBS2より暗号化コンテンツデータ{Data}Kcを受けて、復号処理部1510より取得したコンテンツ復号キーKcによって復号し、コンテンツデータを出力する復号処理部1516と、復号処理部1516の出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518と音声再生部1112の出力を受けて、動作モードに応じて選択的に出力するための混合部1525と、混合部1525の出力を受けて、ヘッドホン130と接続するための接続端子1530とを含む。

10 ここで、復号処理部1510から出力される再生回路制御情報 AC2は、データバスBS2を介して、コントローラ1106に与えられる。

15 なお、図5においては、説明の簡素化のため、携帯電話機を構成するブロックのうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては一部割愛している。

[メモ리카ード110の構成]

図6は、図5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。

20 既に説明したように、公開暗号化鍵 $KP_m(i)$ およびこれに対応する秘密復号鍵 $K_m(i)$ は、メモ리카ードごとに固有の値であるが、メモ리카ード110においては、この自然数 $i=1$ であるものとする。また、メモ리카ードの種類(クラス)に固有の公開暗号化鍵および秘密復号鍵として、 $KP_{mc}(x)$ および $K_{mc}(x)$ が設けられるが、メモ리카ード110においては、自然数 x は、 $x=1$ で表わされるものとする。

25 メモ리카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、認証データとして{ $KP_{mc}(1)$ } KP_{ma} を保持する認証データ保持部1400と、メモ리카ードの種類ごとに設定される固有の復号鍵である $K_{mc}(1)$ を保持する K_{mc} 保持部1402と、メモ리카ードごとに固有に設定される公開暗号化鍵 $KP_m(1)$ を保持する $KP_m(1)$ 保持部1416と、

公開暗号化鍵 $KP_m(1)$ によって暗号化されたデータを復号可能な秘密復号鍵 $K_m(1)$ を保持する $K_m(1)$ 保持部 1 4 2 1 とを含む。

ここで、認証データ保持部 1 4 0 0 は、メモリカードのクラスごとに設定される公開暗号化鍵 $KP_{mc}(1)$ を認証鍵 KP_{ma} で復号可能な状態に暗号化して保持する。

- 5 メモリカード 1 1 0 は、さらに、データバス BS_3 にメモリインタフェース 1 2 0 0 から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵 $K_{mc}(1)$ を $K_{mc}(1)$ 保持部 1 4 0 2 から受けて配信サーバ 3 0 が配信セッションにおいて生成したセッションキー $K_s 1$ または他のメモリカードが移動セッションにおいて生成したセッションキー $K_s 3$ を接点 Pa に出力する復号処理部 1 4 0 4 と、
- 10 認証鍵 KP_{ma} を保持するための認証鍵保持部 1 4 1 4 と、認証鍵保持部 1 4 1 4 の出力を受けて、データバス BS_3 に与えられるデータから認証鍵 KP_{ma} による復号処理を実行して復号結果をデータバス BS_4 を介してコントローラ 1 4 2 0 と暗号化処理部 1 4 1 0 に出力する復号処理部 1 4 0 8 と、切換スイッチ 1 4 4 2 によって選択的に与えられる鍵によって、切換スイッチ 1 4 4 4 によって選択的に与えられるデータを暗号化してデータバス BS_3 に出力する暗号化処理部 1 4 0 6 とを含む。

- メモリカード 1 1 0 は、さらに、配信、再生および移動の各セッションにおいてセッションキー $K_s 2$ あるいは $K_s 3$ を発生するセッションキー発生部 1 4 1 8 と、セッションキー発生部 1 4 1 8 の出力したセッションキー $K_s 3$ を復号処理部
- 20 1 4 0 8 によって得られる公開暗号化鍵 $KP_p(x)$ あるいは $KP_{mc}(x)$ によって暗号化してデータバス BS_3 に出力する暗号化処理部 1 4 1 0 と、データバス BS_3 よりセッションキー $K_s 2$ あるいは $K_s 3$ によって暗号化されたデータを受けてセッションキー発生部 1 4 1 8 より得たセッションキー $K_s 2$ あるいは $K_s 3$ によって復号し、復号結果をデータバス BS_4 に送出する復号処理部 1 4 1 2 とを含む。

- 25 メモリカード 1 1 0 は、さらに、データバス BS_4 上のデータを他のメモリカード固有の公開暗号化鍵 $KP_m(i)$ ($i \neq 1$) で暗号化する暗号化処理部 1 4 2 4 と、データバス BS_4 上のデータを公開暗号化鍵 $KP_m(1)$ と対をなすメモリカード 1 1 0 固有の秘密復号鍵 $K_m(1)$ によって復号するための復号処理部 1 4 2 2 と、復号処理部 1 4 2 2 にて復号されたコンテンツ復号キー K_c を含むライセンス情

報（コンテンツ復号キーKc、コンテンツID、ライセンスID、アクセス制御情報AC1、再生回路制御情報AC2）をデータベースBS4より受けて格納するライセンス保持部1440と、暗号化コンテンツデータ{Data}Kc および付加データData-inf をデータベースBS3より受けて格納するためのメモリ1415とを含む。ライセンス保持部1440およびメモリ1415は、特に限定されないが、たとえば、フラッシュメモリなどの半導体メモリで構成される。

メモリカード110は、さらに、データベースBS3を介して外部との間でデータ授受を行ない、データベースBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420とを含む。

10 ライセンス保持部1440は、データベースBS4との間でライセンス情報の授受が可能である。ライセンス保持部1440は、N個（N：自然数）のバンクを有し、各ライセンスに対応する再生情報の一部をバンクごとに保持する。

15 なお、図6において、点線で囲んだ領域は、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出を不能化するためのモジュールTRM1 およびTRM2 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）である。

20 もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図6に示したような構成とすることで、メモリ1415中に保持されているコンテンツデータは、いずれも暗号化されているコンテンツデータであるため、第三者はこのメモリ1415中のデータのみでは、音楽データ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1415を設ける必要がないので、製造コストが低減されるという
25 利点がある。

また、図6において、領域TRM1に含まれる部分は、メモリカード110の外部からの直接アクセスが禁止されている領域であり、領域TRM2に含まれる部分は、メモリカード110の外部から変更が禁止されている領域である。図6においては、便宜上、領域TRM1と領域TRM2とを分離して示しているが、これらは、

1つのタンパーレジスタンスモジュール内に設けられるものとしてよい。

[配信動作]

次に、本発明の実施例1に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

- 5 図7、図8および図9は、実施例1に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第1、第2および第3のフローチャートである。

10 図7、図8および図9においては、ユーザ1が、メモリカード110を用いることで、携帯電話機100を介して配信サーバ30からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機100からユーザ1によりタッチキー部1108のキーボタンの操作等によって選曲がなされ、配信リクエストがなされる。さらに、タッチキー部1108のキーボタンの操作等によって、ライセンスの購入条件ACが入力される（ステップS102）。

- 15 携帯電話機100からのコンテンツ配信リクエストに応じて、配信サーバ中の中継サーバ10では、リクエストされたコンテンツを得るため対象となるダウンロードサーバ30、iを特定し、コンテンツの平文コンテンツデータDataとコンテンツIDおよび添付データを、ダウンロードサーバ30、iのLCMエンコーダ31、iと対応するLCMデコーダ11、iを介して取得する（ステップS104）。

20 ここで、「添付データ」とは、ダウンロードサーバから中継サーバ10に与えられるコンテンツのタイトルデータ、歌詞データ、歌手名データを含み、さらに、コンテンツの収められるジャケットのイメージ画像データを含むことも可能である。

- 25 続いて、配信サーバ30中の中継サーバ10では、ライセンス情報ACおよびコンテンツの添付データ等に基づいて、中継サーバ10におけるコンテンツID、ライセンスID、コンテンツ復号キーKc、アクセス制御情報AC1、再生回路制御情報AC2を生成する（ステップS116）。

なお、中継サーバ10におけるコンテンツIDは、ダウンロードサーバ30、

1 ~ 30. nからコンテンツデータ Data とともに取得した個々のダウンロードサーバにおけるコンテンツIDをそのまま使用するようにすることも可能であり、また、ダウンロードサーバにおけるコンテンツIDを含む形で生成することも可能である。また、以後、中継サーバ10におけるコンテンツIDを単にコンテンツIDということとする。

さらに、中継サーバ10中の配信制御部315は、取得した添付データを含む付加データ Data-inf を生成する（ステップS118）。

続いて、中継サーバ10中の暗号化処理部308は、平文コンテンツデータ Data をコンテンツ復号キーKcにより暗号化して、暗号化コンテンツデータ {Data}Kc を生成する（ステップS120）。

図8を参照して、配信サーバ30からは、メモリカード110に対して、{KPmc(x)}KPma の送信要求を送信する（ステップS130）。

メモリカード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ {KPmc(1)}KPma が出力される（ステップS132）。

携帯電話機100は、メモリカード110から受理した認証データ {KPmc(1)}KPma を配信サーバ30に対して送信する（ステップS134）。

配信サーバ30では、携帯電話機100から認証データ {KPmc(1)}KPma を受信し（ステップS136）、復号処理部312において認証鍵 KPma で復号処理を実行する（ステップS138）。

この認証鍵 KPma にて暗号化された公開暗号化鍵 KPmc(1)が正規に登録され、正規の暗号化を施されているか否かの判断を行なう（ステップS140）、すなわち、認証鍵 KPma にて復号でき、復号処理において従属するデータが認識できる場合、メモリカード110の公開暗号化鍵 KPmc(1)を受理し、ステップS142に移行する。一方、復号できない場合、または、復号処理において従属するデータが認識できない場合、認証鍵 Kpma について非認証であるものとして、公開暗号化鍵 KPmc(1)は受理せず、処理を終了する（ステップS194）。

公開暗号化鍵 KPmc(1)を受理すると、配信制御部315は、次に、配信セッションを特定するためのトランザクションIDを生成する（ステップS142）。

続いて、セッションキー発生部316は、配信のためのセッションキーKs1を

生成する。セッションキー $Ks1$ は、復号処理部312によって得られたメモリカード110に対応する公開暗号化鍵 $KPm(1)$ によって、暗号化処理部318によって暗号化される（ステップS144）。

5 トランザクションIDと暗号化されたセッションキー $\{Ks1\}Kmc(1)$ とは、データバスBS1および通信装置350を介して外部に出力される（ステップS146）。

10 携帯電話機100が、トランザクションIDおよび暗号化されたセッションキー $\{Ks1\}Kmc(1)$ を受信すると（ステップS148）、メモリカード110においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、保持部1402に保持されるメモリカード110固有の秘密復号鍵 $Kmc(1)$ により復号処理することにより、セッションキー $Ks1$ を復号し抽出する（ステップS150）。

15 コントローラ1420は、配信サーバ30で生成されたセッションキー $Ks1$ の受理を確認すると、セッションキー発生部1418に対して、メモリカード110において配信セッション時に生成されるセッションキー $Ks2$ の生成を指示する。

20 暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキー $Ks1$ によって、切換スイッチ1444の接点Pcを介して、切換スイッチ1446の接点Peと接点Pfを順に切換えることによって与えられるセッションキー $Ks2$ および公開暗号化鍵 $KPm(1)$ を暗号化して、 $\{Ks2//KPm(1)\}Ks1$ をデータバスBS3に出力する（ステップS152）。

なお、 $\{X//Y\}Z$ との表記は、データXとデータYとをそれぞれ鍵Zで復号できるように暗号化したデータであることを示す。

25 データバスBS3に出力されたデータ $\{Ks2//KPm(1)\}Ks1$ は、データバスBS3から端子1202およびメモリインタフェース1200を介して携帯電話機100に送信され（ステップS152）、携帯電話機100にてトランザクションIDを付した後、携帯電話機100から配信サーバ30に送信される（ステップS154）。

配信サーバ30は、暗号化データトランザクションID// $\{Ks2//KPm(1)\}Ks$

1を受信して、復号処理部320においてセッションキー $Ks1$ による $\{Ks2//KpM(1)\}Ks1$ の復号処理を実行し、メモリカードで生成されたセッションキー $Ks2$ およびメモリカード110固有の公開暗号化鍵 $KpM(1)$ を受信する（ステップS156）。

- 5 暗号化処理部326は、ライセンス情報であるコンテンツ復号キー Kc および再生回路制御情報 $AC2$ 、ライセンスID、コンテンツIDおよびアクセス制御情報 $AC1$ とを、復号処理部320によって得られたメモリカード110固有の公開暗号化鍵 $KpM(1)$ によって暗号化する（ステップS164）。

10 暗号化処理部328は、暗号化処理部326の出力を受けて、メモリカード110において生成されたセッションキー $Ks2$ によって暗号化する（ステップS166）。

図9を参照して、暗号化処理部328より出力された暗号化データ $\{\{Kc//AC2//ライセンスID//コンテンツID//AC1\}Km(1)\}Ks2$ は、トランザクションIDを付した後、データバス $BS1$ および通信装置350を介して携帯電話機100

15 に送信される（ステップS168）。

このように、配信サーバ30およびメモリカード110でそれぞれ生成されるセッションキーをやりとりし、お互いが受領した暗号化鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システム

20 のセキュリティを向上させることができる。

携帯電話機100は、送信されたトランザクションIDと暗号化データ $\{\{Kc//AC2//ライセンスID//コンテンツID//AC1\}Km(1)\}Ks2$ を受信し、暗号化データのみをメモリカード110に入力する（ステップS170）。メモリカード110においては、メモリインタフェース1200を介して、データバス $BS3$ に与えられた暗号化データを復号化処理部1412によって復号する。すな

25 わち、復号処理部1412は、セッションキー発生部1418から与えられたセッションキー $Ks2$ を用いてデータバス $BS3$ の暗号化データを復号しデータバス $BS4$ に出力する（ステップS174）。

$Km(1)$ 保持部1421に保持される秘密復号鍵 $Km(1)$ で復号可能であって、デ

ータバス B S 4 に出力されているデータ {Kc//AC 2//ライセンス I D//コンテンツ I D//AC1} Km(1) は、コントローラ 1 4 2 0 の指示によって、復号処理部 1 4 2 2 において、秘密復号鍵 Km(1) によって復号され、コンテンツ復号キー Kc、再生回路制御情報 AC 2、ライセンス I D、コンテンツ I D およびアクセス制御情報 AC1 が受理される (ステップ S 1 7 6)。

さらに、コンテンツ復号キー Kc、再生回路制御情報 AC2、ライセンス I D、コンテンツ I D およびアクセス制御情報 AC1 については、ライセンス情報保持部 1 4 4 0 の空である j 番目のバンクのバンク j に記録される (ステップ S 1 7 8)。ここで、自然数 j はコンテンツデータに対応する番号であり、 $1 \leq j \leq N$ (N :
10 バンクの総数) である。

ステップ S 1 7 8 までの処理が正常に終了した段階で、携帯電話機 1 0 0 から配信サーバ 3 0 にトランザクション I D およびコンテンツデータの配信要求が送信される (ステップ S 1 8 0)。

配信サーバ 3 0 は、コンテンツデータの配信要求を受けて、ダウンロードサーバ 3 0 . i からのコンテンツデータ Data をコンテンツ復号キー Kc にて復号できるように暗号化した暗号化コンテンツデータ {Data}Kc および生成した付加データ DATA-inf をデータバス B S 1 および通信装置 3 5 0 を介して出力する (ステップ S 1 8 2)。

携帯電話機 1 0 0 は、{Data}Kc//Data-inf を受信して、暗号化コンテンツデータ {Data}Kc および付加データ Data-inf を受理する (ステップ S 1 8 4)。暗号化コンテンツデータ {Data}Kc および付加データ Data-inf はメモリインタフェース 1 2 0 0 および端子 1 2 0 2 を介してメモリカード 1 1 0 のデータバス B S 3 に伝達される。メモリカード 1 1 0 においては、受信した暗号化コンテンツデータ {Data}Kc および付加データ Data-inf がそのままメモリ 1 4 1 5 に記録される (ステップ S 1 8 6)。

さらに、携帯電話機 1 0 0 から配信サーバ 3 0 へは、トランザクション I D および配信受理の通知が送信され (ステップ S 1 8 8)、配信サーバ 3 0 で配信受理を受信すると (ステップ S 1 9 0)、課金データベース 3 0 2 への課金データの格納等を伴って、配信終了の処理が実行され (ステップ S 1 9 2)、全体の処

理が終了する（ステップS194）。

5 なお、トランザクションIDは、一連の配信における送受信に対して付与され、同一の配信処理における通信であることを識別するために用いられる。特に、図示されていないが、トランザクションIDの対応が送信側と受信側でとれなくなると、そこで配信処理は終了する。

10 このような処理により、配信リクエストに対して携帯電話機100のコンテンツ再生部およびメモリカード110の送信してきた公開暗号化鍵 K_{Pm}(1)が有効であることを確認した上でのみ、コンテンツデータを配信することができるため、不正な機器への配信を禁止することができるため、配信におけるセキュリティーの向上が確保されている。

 課金データベースに記録された課金データに従って、徴収されたコンテンツの代金は、中継サーバ10とダウンロードサーバ30.1～30.nに分配する。なお、各ダウンロードサーバ30.1～30.nには、それぞれ提供したコンテンツに基づいて分配される。

15 このように、中継サーバ10によるコンテンツ料金の徴収体制にすれば、ユーザは中継サーバと契約すれば、他のダウンロードサーバ30.1～30.nと個々に契約することなく、更には、同一の環境下で、多種のコンテンツを入手することが可能となる。また、コンテンツ提供者にとっては、方式の異なる複数のダウンロードサーバ30.1～30.nに対してコンテンツの提供を行なう必要

20 がなくなるという利便性を図ることができる。

 [再生動作]

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

25 図10は、再生セッション時における各部の動作を説明するためのフローチャートである。

 図10を参照して、携帯電話機100のタッチキー部1108等からのユーザ1の指示により、再生リクエストが生成される（ステップS200）。

 携帯電話機100は、再生リクエストの生成に応じて、認証データ保持部15

00より、認証鍵 KPma で復号可能な認証データ {Kp(1)}KPma をデータベース BS 2に出力する（ステップS 202）。

認証のための暗号化データ {Kp(1)}KPma は、データベース BS 2およびメモリインタフェース 1200を介してメモリカード 110に伝達される。

- 5 メモリカード 110においては、端子 1202を介してデータベース BS 3に伝達される認証のための暗号化データ {Kp(1)}KPma が、復号処理部 1408に取込まれる。復号処理部 1408は、認証鍵保持部 1414から認証鍵 KPma を受けて、データベース BS 3のデータを復号処理を実行する（ステップS 204）。

- 10 この認証鍵 KPma にて暗号化された公開暗号化鍵 Kp(1)が正規に登録され、正規の暗号化を施されている、すなわち、認証鍵 KPma にて復号でき、復号時に発生する従属するデータが認識できる場合（ステップS 206）、認証鍵 KPma による認証結果が承認されたものとして、公開暗号鍵 Kp(1)が受理されて、処理はステップS 210に移行する。

- 15 一方、復号できない場合、または、復号処理において発生する従属データが認識できない場合（ステップS 206）、認証鍵 KPma による認証結果が非承認であるものとして処理は終了する（ステップS 240）。

- 20 コントローラ 1420は、復号処理部 1408にて携帯電話機 100のコンテンツ再生回路に固有の公開暗号化鍵 Kp(1)が受理され、認証の結果、コンテンツ再生装置として携帯電話機 100が承認された場合、送信されてきた公開暗号化鍵 Kp(1)が、このデータ配信システムに対して承認されたコンテンツ再生回路に付与された公開暗号化鍵であると判断し、セッションキー発生部 1418に、再生セッションにおけるセッションキーKs 3の生成をデータベース BS 4を介して指示する。セッションキー発生部 1418によって生成されたセッションキーKs 3は、暗号化処理部 1410に送られる。暗号化処理部 1410は、復号処理部 25 1408によって得られた携帯電話機 100の公開暗号化鍵 Kp(1)によってセッションキーKs 3を暗号化し、暗号化データ {Ks 3}Kp(1)をデータベース BS 3に出力する（ステップS 210）。

携帯電話機 100は、端子 1202およびメモリインタフェース 1200を介して、データベース BS に暗号化データ {Ks 3}Kp(1)を受ける。暗号化データ

{Ks3}Kp(1)は、復号処理部1504によって復号され、メモ리카ード110で生成されたセッションキーKs3が受理される（ステップS212）。

5 コントローラ1106は、セッションキーKs3の受理に応じて、セッションキー発生部1508に対して、再生セッションにおいて携帯電話機100で生成されるセッションキーKs4の発生をデータバスBS2を介して指示する。生成されたセッションキーKs4は暗号化処理部1506に送られ、復号処理部1504によって得られたセッションキーKs3によって暗号化された{Ks4}Ks3がデータバスBS2に出力される（ステップS214）。

10 暗号化されたセッションキー{Ks4}Ks3は、メモリインタフェース1200を介してメモ리카ード110に伝達される。メモ리카ード110においては、データバスBS3に伝達される暗号化されたセッションキー{Ks4}Ks3を復号処理部1412によって復号し、携帯電話機100で生成されたセッションキーKs4を受理する（ステップS216）。

15 セッションキーKs4の受理に応じて、コントローラ1420は、ライセンス保持部1440内の対応するコンテンツIDを格納するバンクjに格納されているアクセス制御情報AC1を確認する（ステップS218）。

20 ステップS218においては、メモリのアクセスに対する制限に関する情報であるアクセス制御情報AC1を確認することにより、既に再生不可の状態である場合、すなわちアクセス制御情報AC1の下位が”00”、あるいは対応するコンテンツIDがライセンス保持部1440に記録されていない場合には再生セッションを終了し（ステップS240）、再生可能であるが再生回数に制限がある場合、すなわちアクセス制御情報AC1の下位が”FE”～”01”の場合にはアクセス制御情報AC1のデータを更新（1減）し再生可能回数を更新した後に次のステップS222に進む（ステップS220）。一方、再生可能であって、再生回数が制限されていない場合においては、ステップS220はスキップされ、アクセス制御情報AC1は更新されることなく処理が次のステップS222に移行する。

25 ステップS218において、当該再生セッションにおいて再生が可能であると判断された場合には、ライセンス保持部1440のバンクjに格納されている再生リクエスト曲のコンテンツ復号キーKcや再生回路制御情報AC2を取得する処

理が実行される（ステップS 2 2 2）。

得られたコンテンツ復号キーKc および再生回路制御情報 AC 2 は、切換スイッチ 1 4 4 4 の接点 Pd を介して暗号化処理部 1 4 0 6 に送られる。暗号化処理部 1 4 0 6 は、切換スイッチ 1 4 4 2 の接点 Pb を介して復号処理部 1 4 1 2 より
5 受けたセッションキーKs 4 によって、データバス BS 4 から受けたライセンス復号キーKc および再生回路制御情報 AC 2 を暗号化し、暗号化データ {Kc//AC2}Ks4 をデータバス BS 3 に出力する（ステップS 2 2 4）。

データバス BS 3 に出力された暗号化データは、端子 1 2 0 2 およびメモリアンタフェース 1 2 0 0 を介して携帯電話機 1 0 0 に送出される。

10 携帯電話機 1 0 0 においては、メモリアンタフェース 1 2 0 0 を介してデータバス BS 2 に伝達される暗号化データ {Kc//AC2}Ks4 を復号処理部 1 5 1 0 によって復号処理を行ない、コンテンツ復号キーKc および再生回路制御情報 AC 2 を受理する（ステップS 2 2 6）。復号処理部 1 5 1 0 は、コンテンツ復号キーKc を復号処理部 1 5 1 6 に伝達し、再生回路制御情報 AC 2 をデータバス BS 2 に
15 出力する。

コントローラ 1 1 0 6 は、データバス BS 2 を介して、再生回路制御情報 AC 2 を受理して再生の可否の確認を行なう（ステップS 2 2 8）。

ステップS 2 3 2 においては、再生回路制御情報 AC 2 によって再生不可と判断される場合には、再生セッションは終了される（ステップS 2 4 0）。

20 一方、再生可能である場合には、メモリカード 1 1 0 よりメモリに記録されたリクエスト曲の暗号化コンテンツデータ {Data}Kc がデータバス BS 3 に出力され、端子 1 2 0 2 およびメモリアンタフェース 1 2 0 0 を介して携帯電話機 1 0 0 に伝達される（ステップS 2 3 0）。

携帯電話機 1 0 0 においては、メモリカード 1 1 0 から出力されデータバス BS 2 に伝達された暗号化コンテンツデータ {Data}Kc を復号処理部 1 5 1 6 においてコンテンツ復号キーKc によって復号し、平文化されたコンテンツデータ Data を得ることができる（ステップS 2 3 2）。復号された平文のコンテンツデータ Data は音楽再生部 1 5 1 8 によって音楽に再生され、混合部 1 5 2 5 および端子 1 5 3 0 を介して外部に再生された音楽を出力し（ステップS 2 3 4）、
25

処理が終了する（ステップS240）。

再生セッションにおいても、携帯電話機100およびメモ리카ード110でそれぞれ生成される暗号化鍵をやりとりし、お互いが受領した暗号化鍵を用いた暗号化を実行して、その暗号化データを相手方に送信する。この結果、配信セッション同様、再生セッションにおいてもデータのそれぞれの送受信において、相互認証を行なうことができ、データ配信システムのセキュリティーを向上させることができる。

また、本発明では携帯電話網を介して、ユーザにコンテンツを供給する場合について説明したが、インターネット等を介してユーザにコンテンツを供給する場合についても同様の効果が得られる。図2における中継サーバ10は、各ダウンロードサーバ30.1～30.nより、それぞれに対応するLCMデコーダ11.1～11.nを介して取得したコンテンツデータを、ライセンス配信制御部12、インターネット網40、プロバイダ50を介して、ユーザの端末となるパーソナルコンピュータ70に接続されたメモ리카ードライター72に装着された、メモ리카ード110と同一の構成のメモ리카ード112に暗号化コンテンツデータとライセンス情報を図6、図7、図8に従って供給すればよい。このとき、図6、図7、図8における携帯電話機100をパーソナルコンピュータ70に置き換えればよい。

したがって、本発明に係るデータ配信システムでは、ユーザに対してコンテンツデータを供給する場合に、インターネット等の情報通信網を介しても、携帯電話網等の情報通信網を介しても、著作権を保護しつつ、著作権保護方式の異なる複数のダウンロードサーバによって供給されるコンテンツ音楽データ等のコンテンツデータをユーザに対して供給することが可能である。

[実施例1の変形例]

本発明の実施例1の変形例に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

図11、図12および図13は、実施例1の変形例に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第1、第2および第3のフローチャートである。

図11、図12および図13においても、ユーザ1が、メモ리카ード110を用いることで、携帯電話機100を介して配信サーバ30からコンテンツデータの配信を受ける場合の動作を説明している。

5 まず、ユーザ1の携帯電話機100からユーザ1によりタッチキー部1108のキーボタンの操作等によって選曲がなされ、配信リクエストがなされる。さらに、タッチキー部1108のキーボタンの操作等によって、ライセンスの購入条件ACが入力される（ステップS102）。

10 携帯電話機100からのコンテンツ配信リクエストに応じて、配信サーバ中の中継サーバ10では、リクエストされたコンテンツの平文コンテンツデータDataとダウンロードサーバにおけるコンテンツIDおよび添付データを、ダウンロードサーバ30.1～30.nのうち対象となるダウンロードサーバ30.iから受けて、対応するLCMデコーダ11.iを介して取得する（ステップS104）。

15 ここで、配信制御部315は、コンテンツデータの送り元がいずれのダウンロードサーバであるかということと、ダウンロードサーバから取得したコンテンツIDに従って、ライセンスデータベース302において、対応するコンテンツ復号キーKcが存在するかの検索を行なう（ステップS106）。

20 当該コンテンツに対応するコンテンツ復号キーKcが存在する場合（ステップS108）、処理はステップS114に移行する。一方、当該コンテンツに対応するコンテンツ復号キーKcが存在しない場合（ステップS108）、処理は次のステップS110に移行する。

当該コンテンツに対応するコンテンツ復号キーKcが存在しない場合、配信サーバ30の中継サーバ10では、コンテンツの添付データ等に基づいて、コンテンツID、コンテンツ復号キーKcを生成する（ステップS110）。

25 さらに、ダウンロードサーバと、ダウンロードサーバから取得したコンテンツIDおよび生成したコンテンツID、コンテンツ復号キーKcをライセンスデータベース302に登録して（ステップS112）、処理はステップS116に移行する。

一方、当該コンテンツに対応するコンテンツ復号キーKcが存在する場合は、

当該コンテンツに対応する、中継サーバ10におけるコンテンツIDおよびコンテンツ復号キーKcをライセンスデータベース302から取得して（ステップS114）、処理はステップS116'に移行する。

5 ステップS116'では、配信サーバ30中の中継サーバ10では、ライセンス情報ACおよびコンテンツの添付データ等に基づいて、ライセンスID、アクセス制御情報AC1、再生回路制御情報AC2を生成する（ステップS116'）。

さらに、中継サーバ10中の配信制御部315は、取得した添付データを含む付加情報Data-infを生成する（ステップS118）。

10 続いて、中継サーバ10中の暗号化処理部308は、平文コンテンツデータDataをコンテンツ復号キーKcにより暗号化して、暗号化コンテンツデータ{Data}Kcを生成する（ステップS120）。

以下、図12および図13の処理は、図8および図9の処理と同様であるので、その説明は繰り返さない。

15 このような処理を行なうこととすれば、配信サーバ30から配信される同一のコンテンツデータに対するコンテンツIDおよびコンテンツ復号キーKcは、同一となるので、上述したコンテンツデータの「複製」処理を行なった後などに、複製の受け手のユーザが、改めて、コンテンツ復号キーKcの配信のみを受けたときにも、再生処理を行なうことが可能になる。

20 なお、以上の説明では、メモリ1415は、TRMの外の領域に設けられるものとして説明したが、メモリ1415が、TRM内に設けられたとしても何ら問題はない。

この発明を詳細に説明し示してきたが、これは例示のためのものであって、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。

請求の範囲

1. 複数のコンテンツデータ供給元から、それぞれ対応する複数の第1の所定の暗号化方式により暗号化されたコンテンツデータを伝送するためのデータ情報通信網（40）と、
- 5 第1のユーザ端末からのコンテンツ配信要求に応じて、前記第1のユーザ端末から要求のあったコンテンツデータを前記データ情報通信網から受けて、第2の所定の暗号化方式により暗号化して配信するための配信中継サーバ（30）とを備え、
- 10 前記配信中継サーバは、
- 前記複数のコンテンツデータ供給元からの、前記複数の第1の所定の暗号化方式により暗号化された前記コンテンツデータを復号するための複数の第1のコンテンツデータ復号手段（11. 1-11. n）と、
- 前記第1のコンテンツデータ復号手段の出力を受けて、前記第2の所定の暗号化方式で暗号化し、暗号化コンテンツデータを生成するコンテンツデータ暗号化手段（310）と、
- 15 前記暗号化コンテンツデータを配信するための送信手段（350）とを含む、データ配信システム。
2. 前記配信中継サーバは、携帯電話網に接続された前記第1のユーザ端末からのコンテンツ配信要求に応じて、前記第2の所定の暗号化方式により暗号化された前記コンテンツデータを配信し、
- 20 前記送信手段は、前記暗号化コンテンツデータを前記携帯電話網を介して配信する、請求項1記載のデータ配信システム。
3. 前記配信中継サーバは、
- 25 前記暗号化コンテンツデータを復号するためのコンテンツ復号キーを少なくとも含むライセンス情報に対して、前記第1のユーザ端末に保持される秘密復号鍵により前記第1のユーザ端末において復号可能な暗号化を施す第1の暗号化手段をさらに備え、
- 前記送信手段は、暗号化された前記ライセンス情報をさらに配信する、請求項

- 1に記載のデータ配信システム。
4. 前記第1のユーザ端末は、
前記暗号化コンテンツデータおよび前記ライセンス情報を格納して、前記ライセンス情報を暗号化した状態で入出力し、かつ、データ再生装置に着脱可能なデータ格納部を備え、
- 5
前記データ格納部は、
前記暗号化されたコンテンツデータを格納し、前記データ格納部の外部からの要求に従って、前記データ格納部の外部に出力するための第1の記憶手段と、
前記配信中継サーバにより配信され、前記暗号化コンテンツデータに対応した
10
前記ライセンス情報を格納することが可能な第2の記憶手段と、
前記データ格納部の外部からの要求に従って、前記第2の記憶手段に格納された前記ライセンス情報のうちの少なくとも一部を前記データ格納部の外部に出力するため制御手段とを有する、請求項3記載のデータ配信システム。
5. 前記データ格納部は、
- 15
予め定められた認証鍵によって正当性が判断できるように暗号化された前記データ格納部の安全性を証明するための証明書を保持し、前記証明書を外部に出力可能な認証データ保持部をさらに含み、
前記配信中継サーバは、
前記データ格納部から出力された証明書の正当性を判定する承認手段を備える、
20
請求項4記載のデータ配信システム。
6. 前記データ格納部は、
前記第2の記憶手段に格納されたライセンス情報のうちの少なくとも一部を暗号化する手段をさらに備え、
前記データ格納部の外部からの要求に従って、前記ライセンス情報のうちの少
25
なくとも一部を暗号化した上で、前記データ格納部の外部に出力する、請求項4記載のデータ配信システム。
7. 前記第1のユーザ端末は、
前記データ格納部に格納された前記暗号化コンテンツデータと前記ライセンス情報を受けて、前記暗号化コンテンツデータを復号してコンテンツデータの再生

- を行なうためのデータ再生部を備え、
- 前記データ再生部は、
- 前記データ格納部に対して、前記ライセンス情報の少なくとも一部の出力および前記暗号化コンテンツデータの出力を要求するデータ制御手段と、
- 5 前記コンテンツ復号キーに従って前期暗号化コンテンツデータを復号して、前記コンテンツデータを出力するコンテンツデータ復号部と、
- 前記コンテンツデータを再生するコンテンツデータ再生手段とを含む、請求項4記載のデータ配信システム。
8. 前記第1の暗号化手段は、前記第1のユーザ端末から予め暗号化されて送信された第1の暗号鍵によって前記コンテンツ復号キーを暗号化する、請求項3
- 10 記載のデータ配信システム。
9. 前記データ情報通信網により伝送される、前記複数のコンテンツデータ供給元のうちのいずれか1つのコンテンツ供給元からの対応する前記第1の所定の暗号化方式により暗号化された前記コンテンツデータを受ける第2のユーザ端末
- 15 をさらに備え、
- 前記第2のユーザ端末は、
- 前記第1の所定の暗号化方式により暗号化された前記コンテンツデータを復号するための第2のコンテンツデータ復号手段を含む、請求項1記載のデータ配信システム。
- 20 10. ユーザ端末からのコンテンツ配信要求に応じて、複数のコンテンツデータ供給元から1つを選択してコンテンツデータを取得し、取得したコンテンツデータを前記ユーザ端末に送信する配信中継サーバであって、
- 複数のコンテンツデータ供給元から、それぞれ対応する複数の第1の所定の暗号化方式により暗号化されたコンテンツデータを受信するために第1のデータ情報通信網(40)との間でデータの送受信を行なう第1の送受信手段(301)
- 25 と、
- 前記複数のコンテンツデータ供給元からの、前記複数の第1の所定の暗号化方式により暗号化された前記コンテンツデータを復号するための複数の第1のコンテンツデータ復号手段(11. 1-11. n)と、

前記複数の第1のコンテンツデータ復号手段のいずれか一つの出力を受けて、前記第2の所定の暗号化方式で暗号化し、暗号化コンテンツデータを生成するコンテンツデータ暗号化手段(310)と、

5 前記ユーザ端末からコンテンツ配信要求を受信し、かつ前記暗号化コンテンツデータを送信するために第2のデータ通信網を介して前記ユーザ端末とデータの送受信を行なう第2の送受信手段(350, 20)とを備え、

10 前記ユーザ端末からの前記コンテンツ配信要求によって指示された前記コンテンツデータを提供可能なコンテンツデータ供給元を前記複数のコンテンツデータ供給元から選択し、前記選択したコンテンツデータ供給元から前記選択したコンテンツデータ供給元に対応する第1の所定の暗号化方式により暗号化された前記コンテンツデータを受信し、前記複数の第1のコンテンツデータ復号手段のうち前記選択したコンテンツデータ供給元に対応する第1の所定の暗号化方式に対応したコンテンツデータ復号手段にて復号し、復号したコンテンツデータを前記第2のコンテンツ暗号化手段によって暗号化した前記暗号化コンテンツデータを、
15 前記ユーザ端末に送信する配信中継サーバ。

1 1. 前記第2のデータ通信網は、携帯電話網である、請求項10記載の配信
中継サーバ。

1 2. 前記配信
中継サーバは、

20 前記ユーザ端末からのコンテンツ配信要求にしたがって、前記暗号化コンテンツデータを復号するためのコンテンツ復号キーを少なくとも含むライセンス情報を送信し、

前記第2の送信手段は、暗号化された前記ライセンス情報をさらに送信する、請求項10に記載の配信
中継サーバ。

1 3. 前記配信
中継サーバは、

25 前記ユーザ端末に保持される秘密復号鍵により前記ユーザ端末において復号可能な暗号化を施す第1の暗号化手段(326)をさらに備え、

前記第2の送受信手段は、暗号化された前記ライセンス情報をさらに配信する、請求項10に記載の配信
中継サーバ。

1 4. 前記コンテンツ配信要求は、予め定められた認証鍵によって送信先の正当

- 性が判断できる証明書を含み、
前記配信中継サーバは、
前記証明書の正当性を判定する認証手段を備え、
前記認証手段において正当性が確認された場合、前記暗号化コンテンツデータ
5 および前記ライセンス情報のいずれかを送信する、請求項1-3に記載の配信中継
サーバ。

FIG. 1

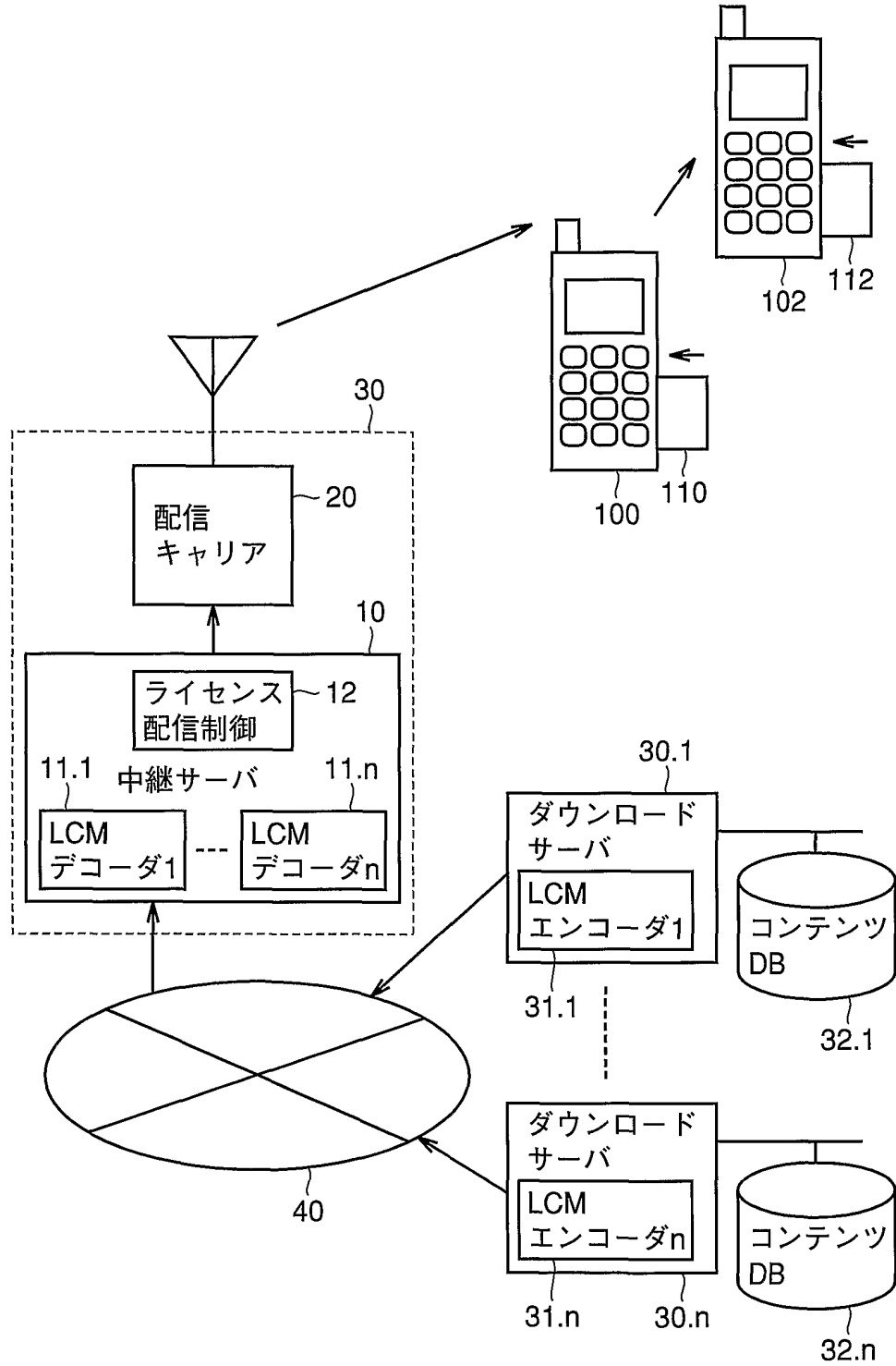


FIG.2

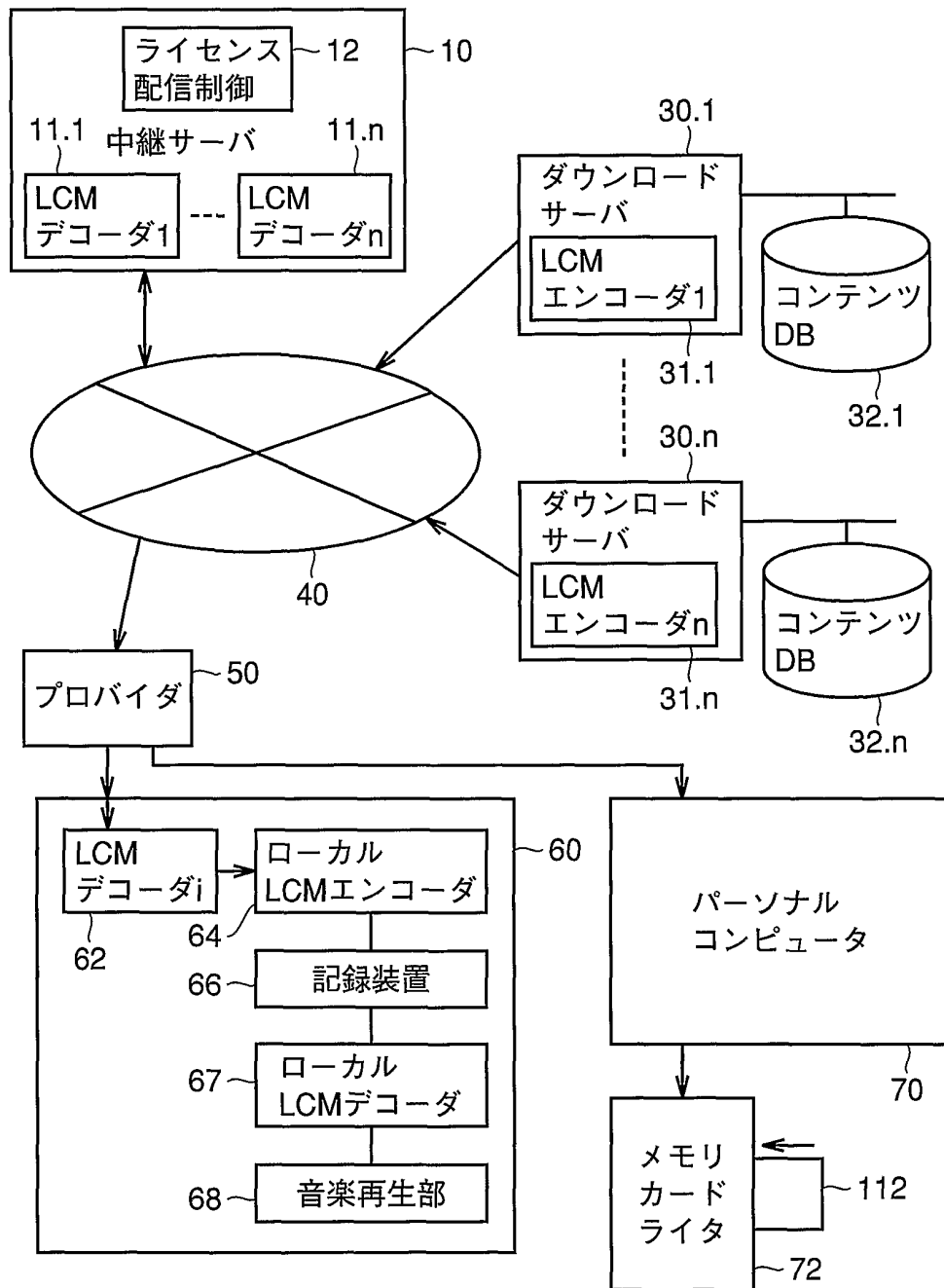


FIG.3

名称	機能・特徴	保持・発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて配布	配信サーバ
Data-inf	付加データ、コンテンツデータに関する著作関連あるいはサーバアクセス関連等の平文情報	配信サーバ
Kc	コンテンツ復号キー	配信サーバ
Kp(x)/Kmc(x)	コンテンツ再生/メディアのクラス(種類等)に依存する復号鍵 xはクラスを識別する識別子	携帯電話機 メモリカード
KPp(x)/KPmc(x)	Kp(x)/Kmc(x)にて復号可能な非対称暗号化鍵、 {KPp(x)}KPma/{KPp(x)}KPmaの形式で証明付き暗号化を施され記録	携帯電話機 メモリカード
KPma	システム共通の公開鍵(認証鍵)	配信サーバ
AC	利用者側からのライセンスに対する購入条件(機能限定、ライセンス数 etc)	配信サーバ
AC1	メモリのアクセスに対する制御情報	配信サーバ
AC2	再生回路における制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵 iはカードを識別する識別子	メモリカード
KPm(i)	Km(i)にて復号可能な非対称暗号化鍵	メモリカード
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信/移動(受)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	配信サーバ
トランザクションID	配信セッション毎に生成される配信セッションを特定できるコード	配信サーバ
ライセンスID	ライセンスの発行を特定できる管理コード(トランザクションIDとの兼用も可)	配信サーバ

FIG.4

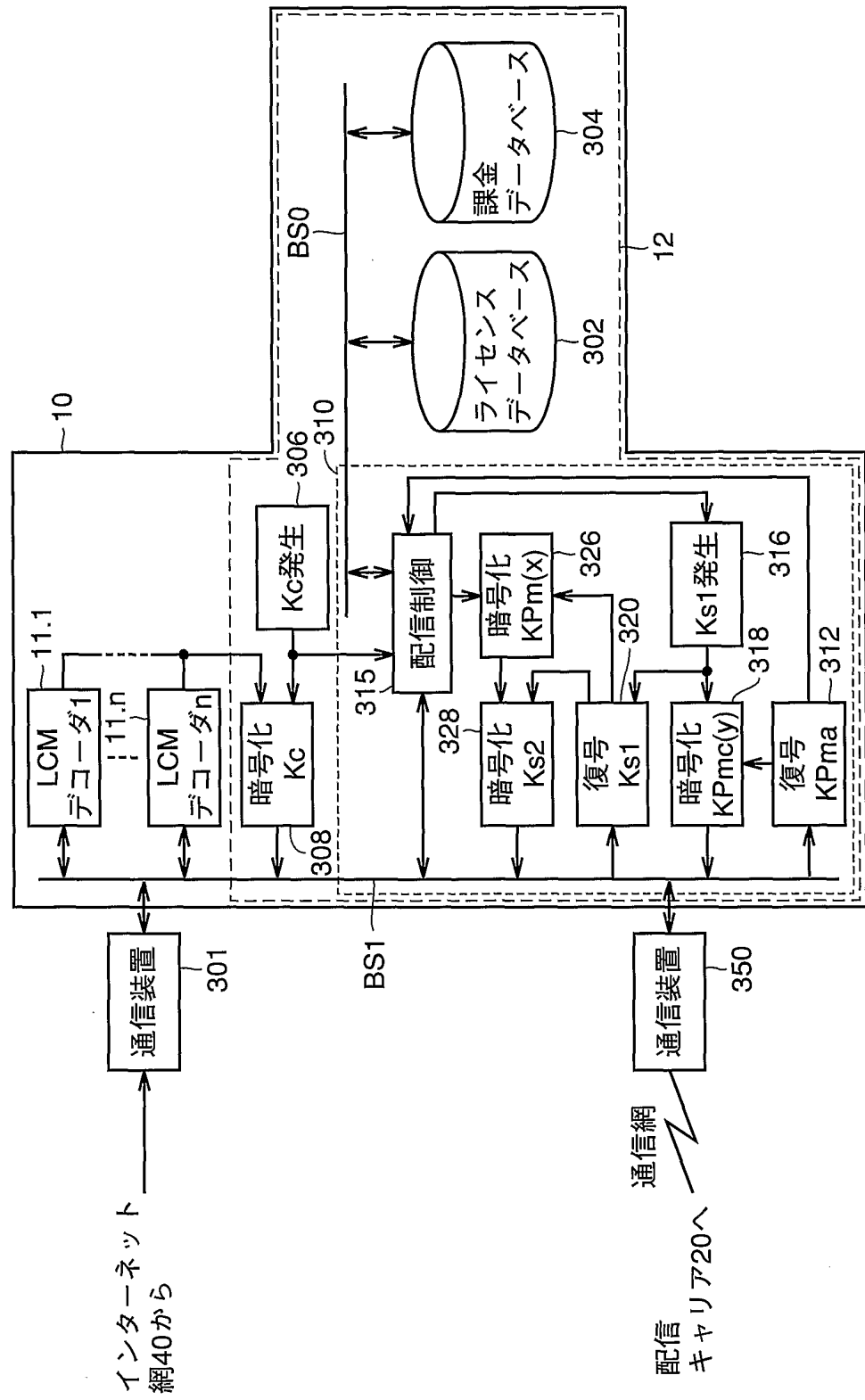


FIG.5

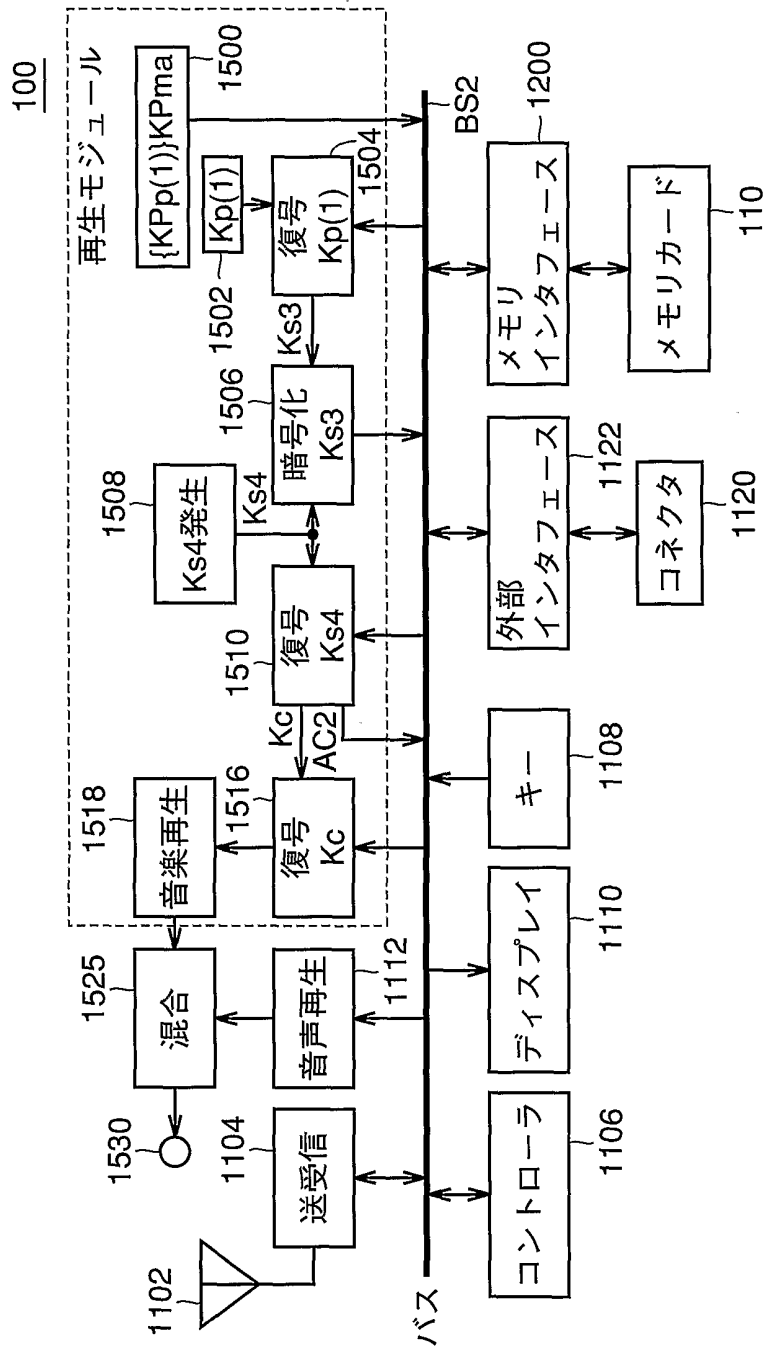


FIG.6

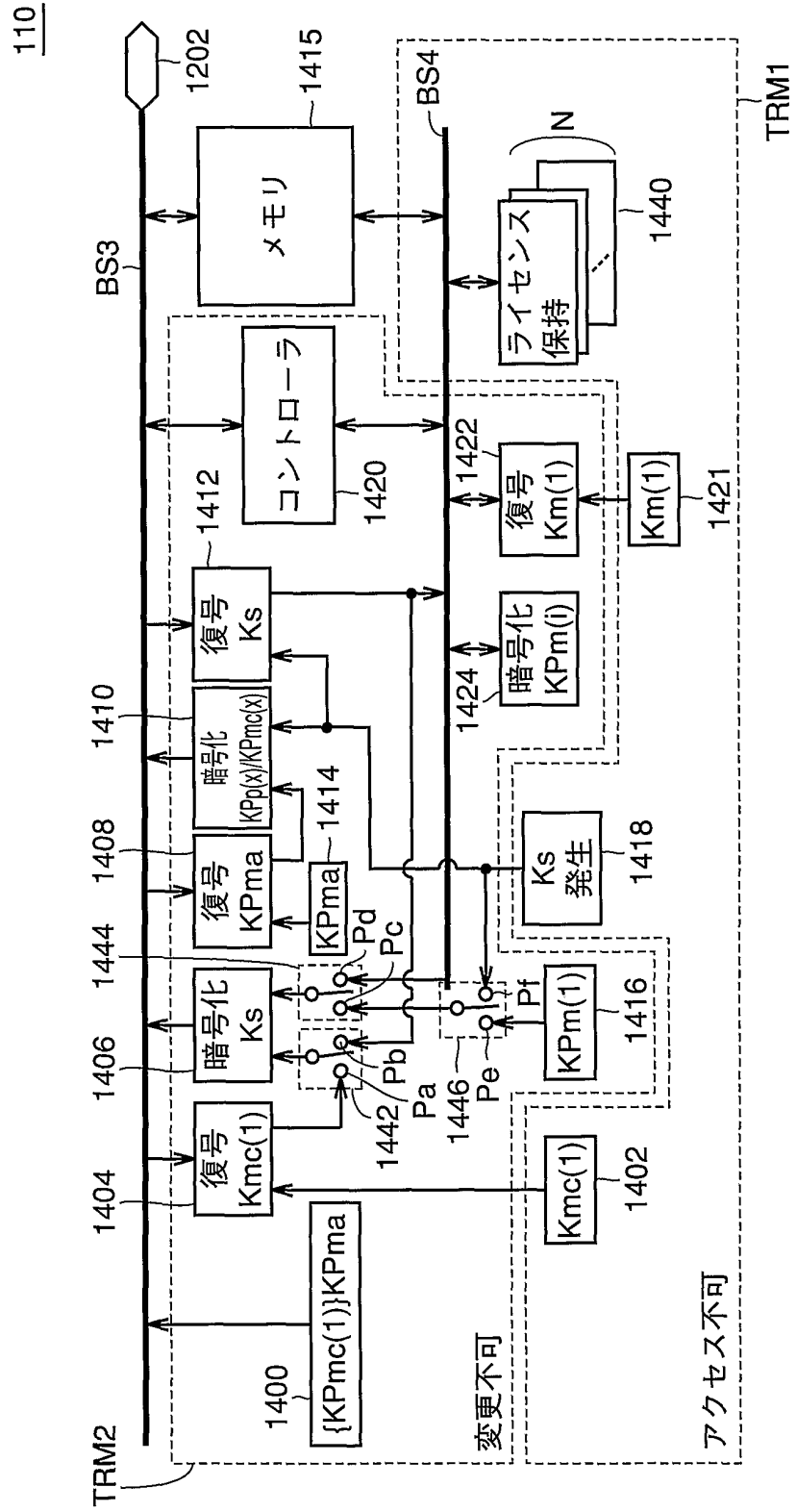
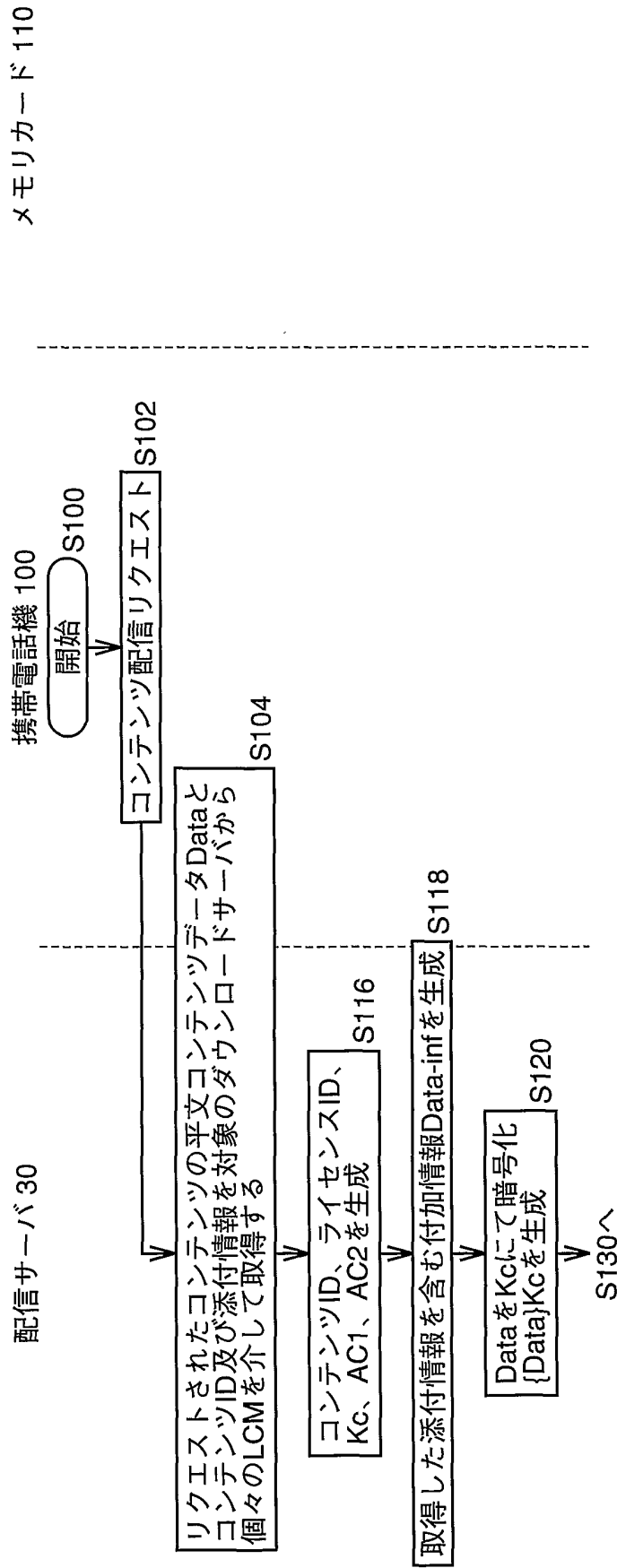


FIG.7



メモリカード 110

携帯電話機 100

配信サーバ 30

FIG.8

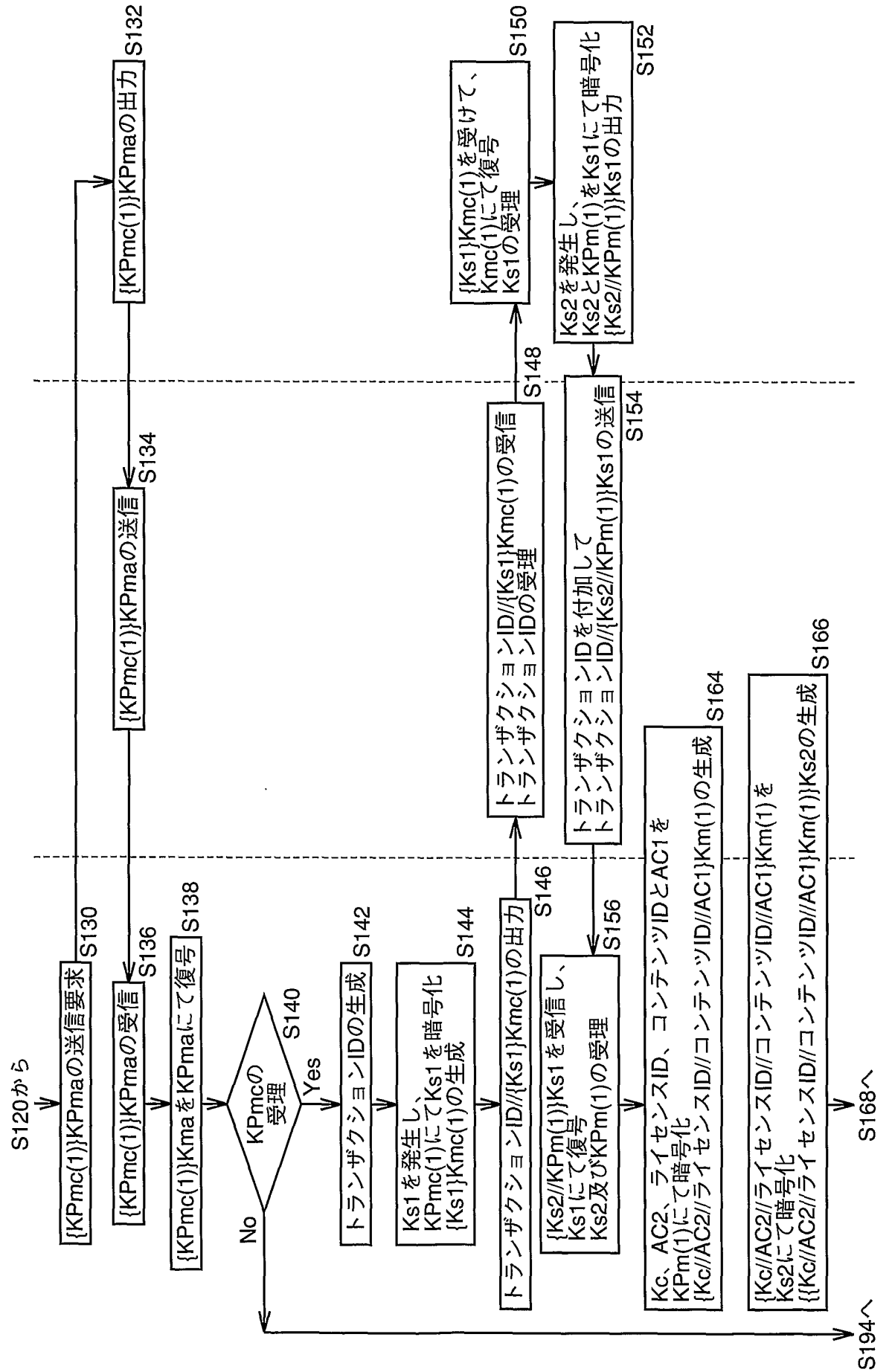


FIG. 9

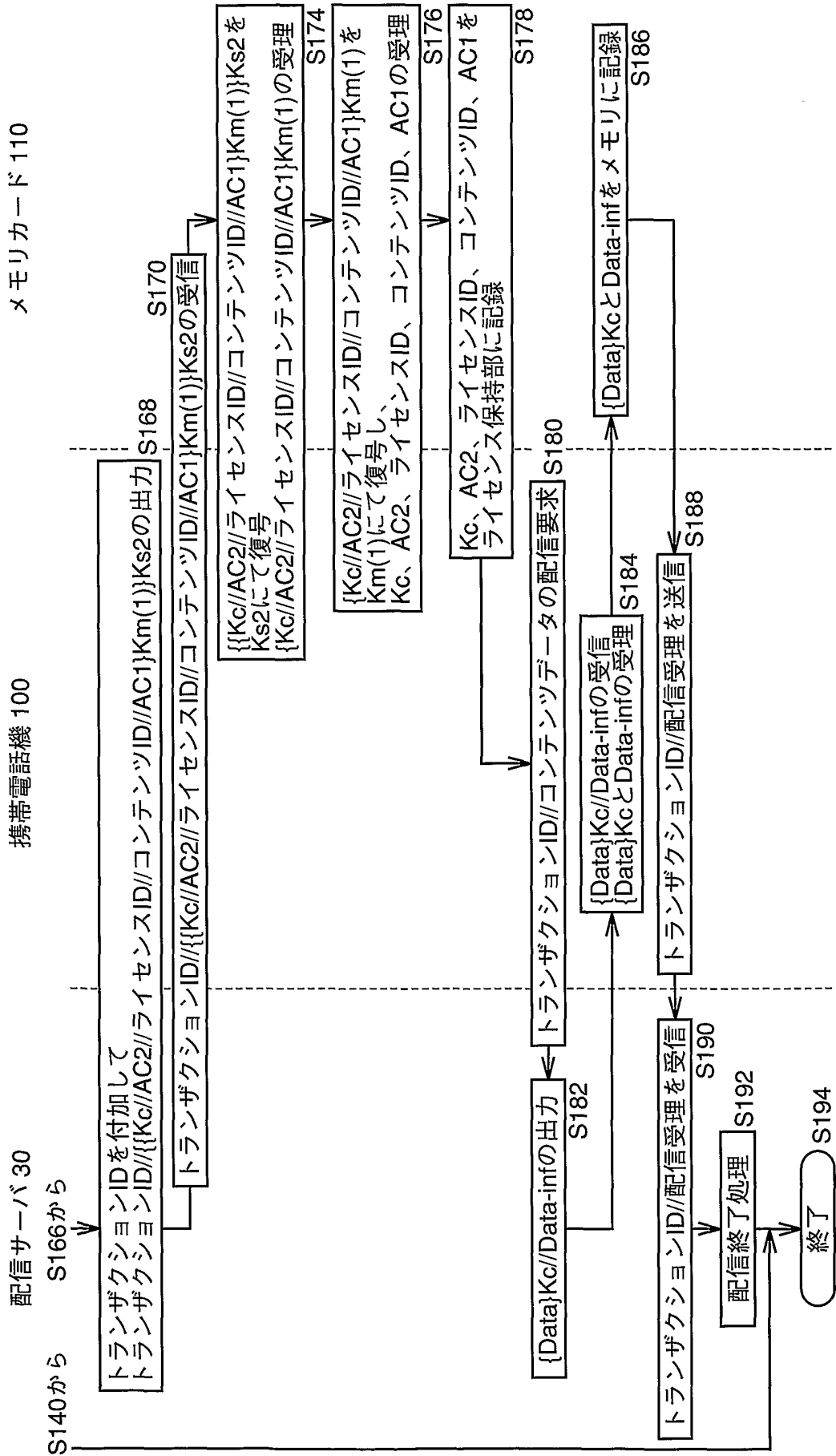
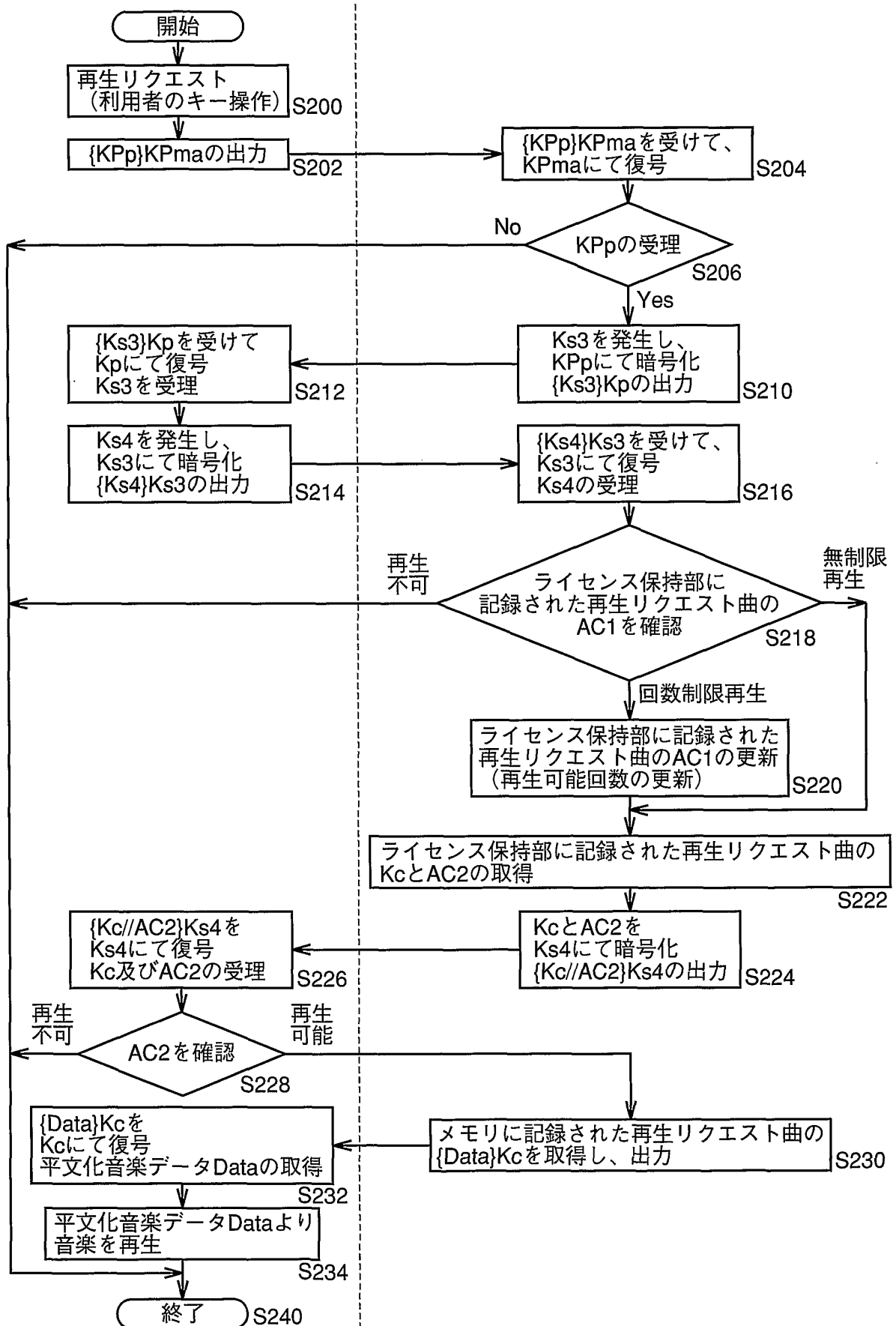


FIG.10 携帯電話機 100

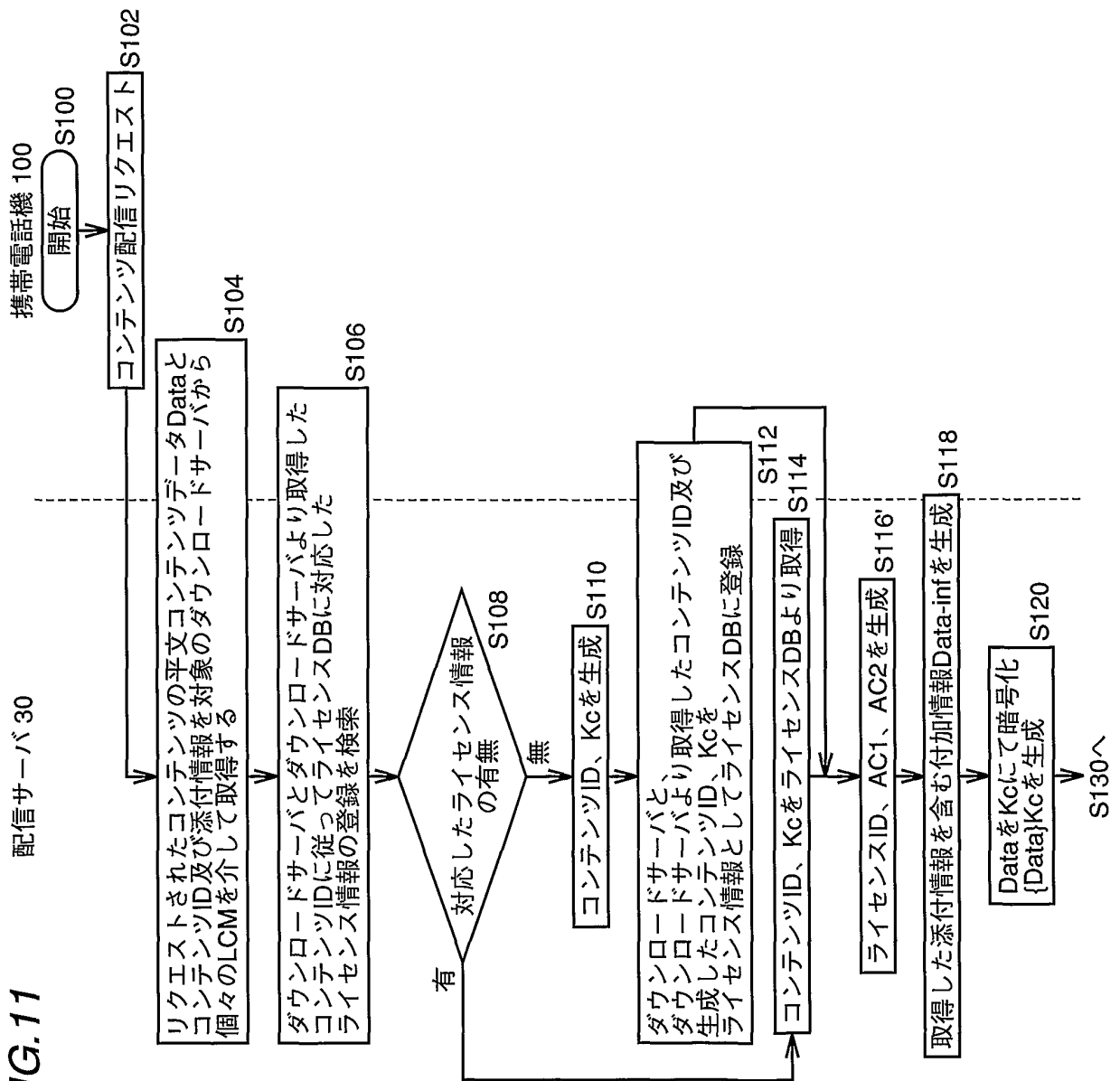
メモ리카ード 110



メモリカード 110

配信サーバ 30

FIG.11



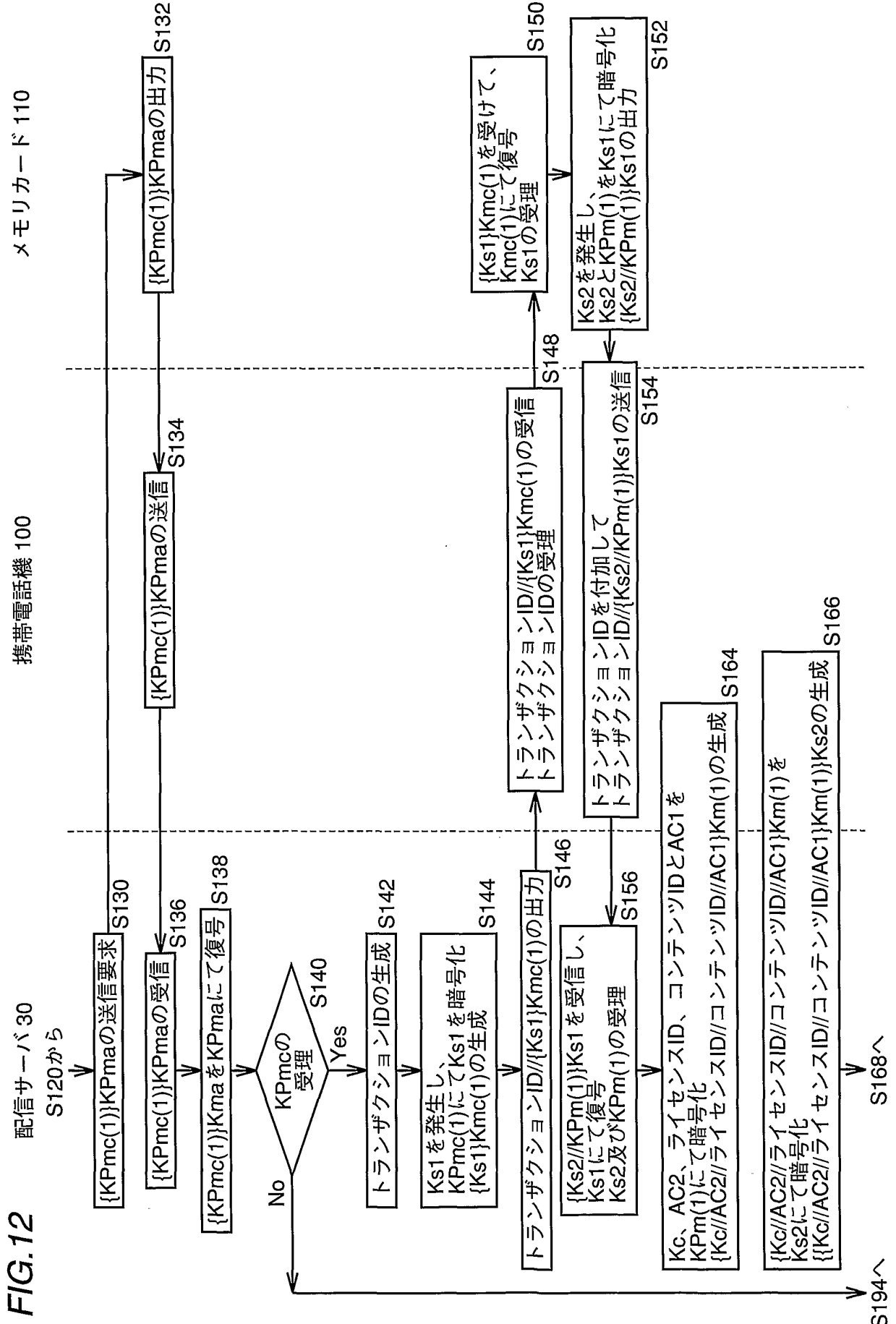
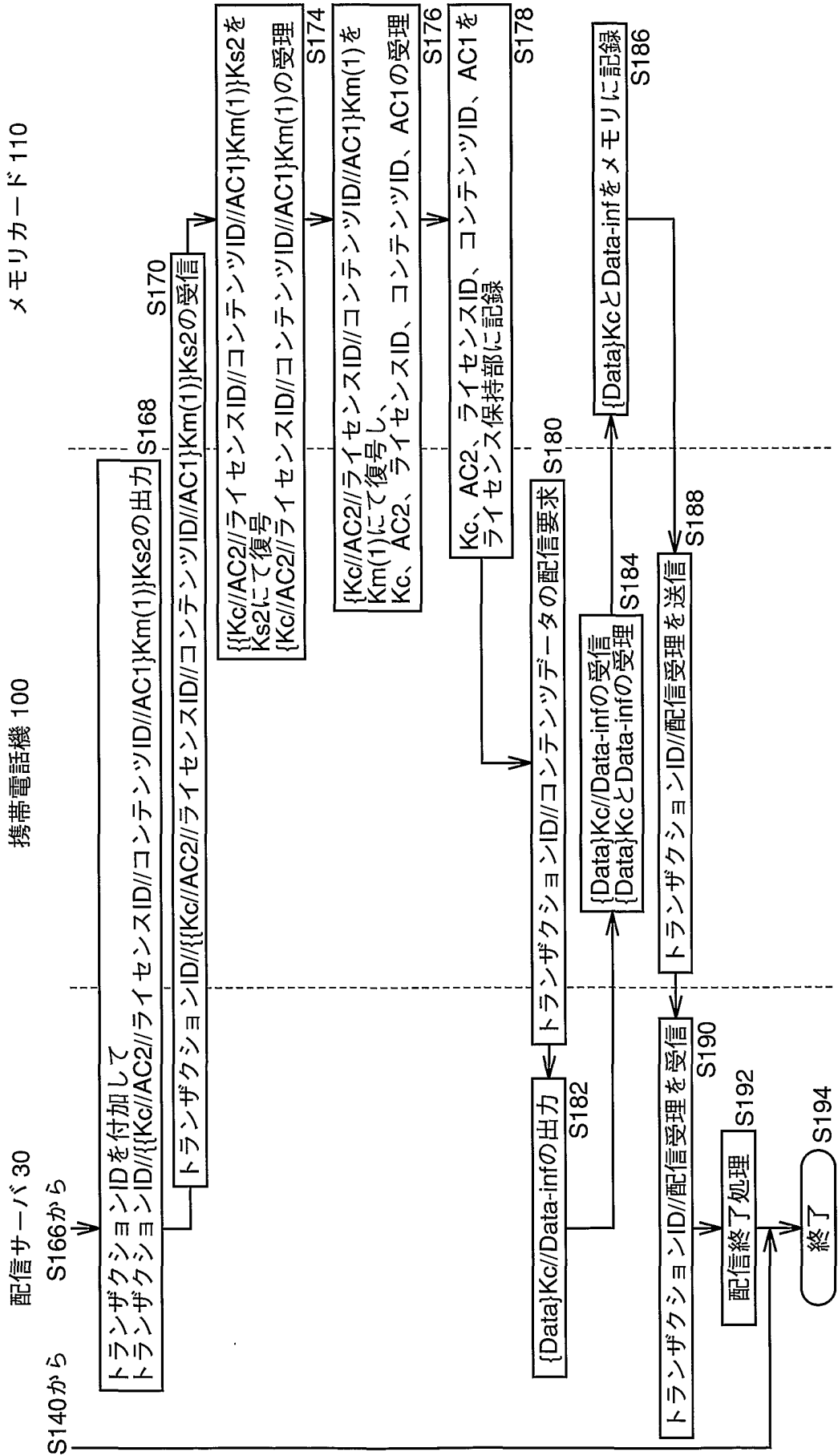


FIG. 12

FIG. 13



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/04240

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl. ⁷ H04L9/08, H04L9/32, G09C1/00, G06F15/00, H04Q7/38		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) Int.Cl. ⁷ H04L9/08, H04L9/32, G09C1/00, G06F15/00, H04Q7/38		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DAVIES, D. W. and PRICE, W. L., Translation: Tadahiro KAMIZONO, "Network Security", (1 st edition, 1 st printing), McGraw-Hill, 05 December, 1985 (05.12.85), pages 102 to 108	1, 3, 8, 10, 12, 13
Y	pages 102 to 108	2, 4-7, 9, 11, 14
Y	JP 11-355268 A (Sony Corporation), 24 December, 1999 (24.12.99), Par. Nos. [0055] to [0058]; Fig. 1 (Family: none)	2, 11
Y	"Kogata Memory Card de Ongaku Chosakuken wo mamoru", Nikkei Electronics, No.739, 22 March, 1999 (22.03.99), pages 49 to 53	4-7, 9, 14
A	JP 9-503322 A (Syprus, Inc.), 31 March, 1997 (31.03.97), Full text; Figs. 1 to 16 & AU 7687494 A & AU 6259596 A & IL 110891 A & WO 95/08231 A	1-14
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* "A"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E"	earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed	
Date of the actual completion of the international search 30 July, 2001 (30.07.01)	Date of mailing of the international search report 07 August, 2001 (07.08.01)	
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer	
Facsimile No.	Telephone No.	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/04240

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	& US 5457746 A & EP 719485 A & WO 96/41445 A & CA 5703951 A & CN 1191643 A & JP 11-507774 A	
A	JP 9-307543 A (Matsushita Electric Ind. Co., Ltd.), 28 November, 1997 (28.11.97), Full text; Figs. 1 to 8 (Family: none)	1-14
A	JP 8-287014 A (Mitsubishi Corporation), 01 November, 1996 (01.11.96), Full text; Figs. 1 to 15 & EP 715241 A & US 5867579 A & US 6128605 A	1-14

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L9/32, G09C1/00, G06F15/00, H04Q7/38

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L9/32, G09C1/00, G06F15/00, H04Q7/38

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	DAVIES, D. W. and PRICE, W. L. 著, 上園忠弘 訳; “ネットワーク・セキュリティ” (1版1刷) 日経マグローヒル社 発行, 5. 12月. 1985 (05. 12. 85) p. 102-108	1, 3, 8, 10, 12, 13
Y	p. 102-108	2, 4-7, 9, 11, 14
Y	J.P. 11-355268 A (ソニー株式会社)	2, 11

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的な技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日 30. 07. 01

国際調査報告の発送日 07.08.01

国際調査機関の名称及びあて先
 日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
 青木 重徳
 5M 4229
 電話番号 03-3581-1101 内線 3597



C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	24. 12月. 1999 (24. 12. 99) 第【0055】 - 【0058】段落, 図1 (ファミリーなし)	
Y	“小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス, No. 739 22. 3月. 1999 (22. 03. 99) p. 49-53	4-7, 9, 14
A	JP 9-503322 A (スピラス インコーポレイテッド) 31. 3月. 1997 (31. 03. 97) 全文, 図1-16 & AU 7687494 A & AU 6259596 A & IL 110891 A & WO 95/08231 A & US 5457746 A & EP 719485 A & WO 96/41445 A & CA 5703951 A & CN 1191643 A & JP 11-507774 A	1-14
A	JP 9-307543 A (松下電器産業株式会社) 28. 11月. 1997 (28. 11. 97) 全文, 図1-8 (ファミリーなし)	1-14
A	JP 8-287014 A (三菱商事株式会社) 1. 11月. 1996 (01. 11. 96) 全文, 図1-15 & EP 715241 A & US 5867579 A & US 6128605 A	1-14