

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4100845号
(P4100845)

(45) 発行日 平成20年6月11日(2008.6.11)

(24) 登録日 平成20年3月28日(2008.3.28)

(51) Int.Cl. F I
G06F 21/24 (2006.01)
 G06F 12/14 540C
 G06F 12/14 530C
 G06F 12/14 550A

請求項の数 4 (全 11 頁)

<p>(21) 出願番号 特願平11-348782 (22) 出願日 平成11年12月8日(1999.12.8) (65) 公開番号 特開2001-166999(P2001-166999A) (43) 公開日 平成13年6月22日(2001.6.22) 審査請求日 平成16年6月8日(2004.6.8)</p>	<p>(73) 特許権者 000005016 パイオニア株式会社 東京都目黒区目黒1丁目4番1号 (74) 代理人 100063565 弁理士 小橋 信淳 (72) 発明者 野中 慶也 埼玉県川越市大字山田字西町25番地1 パイオニア株式会社 川越工場内 (72) 発明者 柴▲さき▼ 裕昭 東京都目黒区目黒1丁目4番1号 パイオ ニア株式会社内 審査官 岩崎 志保</p>
--	--

最終頁に続く

(54) 【発明の名称】 情報記録読取方法ならびに装置

(57) 【特許請求の範囲】

【請求項1】

それぞれに固有の識別情報が付された第一の記録媒体と第二の記録媒体とに対して、情報の記録または記録された情報の読取りを行う情報記録読取方法であって、

前記第一の記録媒体に付された識別情報に基づいて情報が暗号化され第一の記録媒体に記録された第一の暗号化情報を読取り、前記読取られた第一の暗号化情報を、前記第二の記録媒体に付された識別情報に基づいて暗号化して第二の暗号化情報を生成し、前記生成された第二の暗号化情報を前記第二の記録媒体に記録し、前記第二の記録媒体から第二の暗号化情報を読取り、前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読し、前記解読された第二の暗号化情報を前記第一の暗号化情報として復元し前記第一の記録媒体に記録すること、

を特徴とする情報記録読取方法。

【請求項2】

前記第一、第二の記録媒体の認証を行い、いずれも正規の記録媒体と認証された場合に、前記第一、第二の記録媒体からそれぞれの暗号化情報の読取りを許可すること、
 を特徴とする請求項1に記載の情報記録読取方法。

【請求項3】

第一の記録媒体が持つ識別情報に基づいて情報が暗号化され第一の記録媒体に記録された第一の暗号化情報を読取り、当該第一の暗号化情報を第二の暗号化情報として第二の記録媒体に記録すると共に、前記第二の暗号化情報を読取り、当該第二の暗号化情報を第一

の記録媒体に記録する情報記録読取装置であって、

前記第一の記録媒体から第一の暗号化情報を読取る第一の読取手段と、

前記読取られた第一の暗号化情報を、前記第二の記録媒体が持つ識別情報に基づいて暗号化して第二の暗号化情報を生成する暗号化手段と、

前記生成された第二の暗号化情報を、前記第二の記録媒体に記録する第二の記録手段と

、
前記第二の記録媒体から第二の暗号化情報を読取る第二の読取手段と、

前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読する解読手段と、

前記解読された第二の暗号化情報を第一の暗号化情報として復元し前記第一の記録媒体に記録する第二の記録手段と、を有すること、

を特徴とする情報記録読取装置。

【請求項 4】

前記読取手段は、

前記第一、第二の記録媒体の認証を行う認証手段と、

前記認証手段によって、前記第一、第二の記録媒体がいずれも正規の記録媒体と認証された場合、前記第一の暗号化情報の読取りを許可する許可手段と、を更に有すること、

を特徴とする請求項 3 に記載の情報記録読取装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、音楽や映像、或いはコンピュータプログラム等の情報を記録再生する装置に用いて好適な、情報記録読取方法ならびに装置に関する。

【0002】

【従来の技術】

音楽や映像、或いはコンピュータプログラムなどの情報（著作物）を、通信によって電子的に配信する頒布方法が主流になりつつある。かかる頒布方法では、情報の正規の供給元からの頒布のみを認める取り決めが必要である。つまり、違法なコピーが氾濫して、著作権者に多大な不利益を生じることが無いように、情報を受信してこれを記録、再生する装置において、一方の装置から他方の装置へのコピーを禁止する取り決めをしておかなければならない。ここでいうコピーとは、同時に 2 種類以上の媒体上に、同一のデータが存在している状態をいう。

【0003】

【発明が解決しようとする課題】

しかしながら、上記の取り決めによると、バックアップするためのコピーであっても認められないことになり、正規にその著作物を入手したユーザに不利益を生じかねない。例えば、HDD（ハードディスク）内に格納された音楽、映像、あるいはプログラムデータが何らかの原因により破壊された場合には再度入手する必要があり、場合によっては入手できなかったり、あるいはプログラムの場合、バージョンアップ等の関係により対応できないことも考えられる。

【0004】

本発明は上記事情に鑑みてなされたものであり、複数の記録媒体を有する情報記録読取装置において、第一の記録媒体に記録された情報データを、バックアップ用の第二の記録媒体に記録する際、バックアップ用の第二の記録媒体に固有の識別情報に基づき暗号化して記録することにより第一の記録媒体とはその内容を異にし、このことにより、コピー禁止の概念を維持しつつ、バックアップするための記録を可能とする、情報記録読取方法ならびに装置を提供することを目的とする。

【0005】

【課題を解決するための手段】

請求項 1 に記載の発明は、それぞれに固有の識別情報が付された第一の記録媒体と第二

10

20

30

40

50

の記録媒体とに対して、情報の記録または記録された情報の読取りを行う情報記録読取方法であって、前記第一の記録媒体に付された識別情報に基づいて情報が暗号化され第一の記録媒体に記録された第一の暗号化情報を読取り、前記読取られた第一の暗号化情報を、前記第二の記録媒体に付された識別情報に基づいて暗号化して第二の暗号化情報を生成し、前記生成された第二の暗号化情報を前記第二の記録媒体に記録し、前記第二の記録媒体から第二の暗号化情報を読取り、前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読し、前記解読された第二の暗号化情報を前記第一の暗号化情報として復元し前記第一の記録媒体に記録すること、を特徴とする。

【0006】

請求項2に記載の発明は、請求項1に記載の情報記録読取方法において、前記第一、第二の記録媒体の認証を行い、いずれも正規の記録媒体と認証された場合に、前記第一、第二の記録媒体からそれぞれの暗号化情報の読取りを許可すること、を特徴とする。

【0007】

このことにより、第一の記録媒体に記録された情報を、バックアップ用の第二の記録媒体に記録する際、第二の記録媒体に固有の識別情報(第二の識別情報)に基づいて暗号化されて記録される。つまり、第二の記録媒体に記録される情報は、第二の識別情報に基づいて暗号化されたものであるから、第一の暗号化情報とは異なるものとなり、同一の情報を複製するというコピーの概念には当たらなくなる。従って、コピー禁止の概念を維持しつつ、バックアップするための記録が可能となる。また、バックアップにあたり相互認証を実行しながら行っているため不正なコピーの生成は発生しない。

【0008】

請求項3に記載の発明は、第一の記録媒体が持つ識別情報に基づいて情報が暗号化され第一の記録媒体に記録された第一の暗号化情報を読取り、当該第一の暗号化情報を第二の暗号化情報として第二の記録媒体に記録すると共に、前記第二の暗号化情報を読取り、当該第二の暗号化情報を第一の記録媒体に記録する情報記録読取装置であって、前記第一の記録媒体から第一の暗号化情報を読取る第一の読取手段と、前記読取られた第一の暗号化情報を、前記第二の記録媒体が持つ識別情報に基づいて暗号化して第二の暗号化情報を生成する暗号化手段と、前記生成された第二の暗号化情報を、前記第二の記録媒体に記録する第二の記録手段と、前記第二の記録媒体から第二の暗号化情報を読取る第二の読取手段と、前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読する解読手段と、前記解読された第二の暗号化情報を第一の暗号化情報として復元し前記第一の記録媒体に記録する第二の記録手段と、を有すること、を特徴とする。

【0009】

請求項4に記載の発明は、請求項3に記載の情報記録読取装置において、前記読取手段は、前記第一、第二の記録媒体の認証を行う認証手段と、前記認証手段によって、前記第一、第二の記録媒体がいずれも正規の記録媒体と認証された場合、前記第一の暗号化情報の読取りを許可する許可手段と、を更に有すること、を特徴とする。

【0012】

上記構成により、第一の記録媒体に記録された内容を第二の記録媒体にバックアップする場合暗号化手段を介して暗号化される。ここでの暗号化は、第二の記録媒体に固有の識別情報(ID)を抽出し、かかる抽出した識別情報を暗号化するための鍵データとして用いることにより行われる。従って、ここでは、第一の記録媒体が持つ固有の識別情報で暗号化された情報は、更に第二の記録媒体が持つ識別情報で暗号化されることになる。一方、第一の記録媒体に記録されたデータ(元データ)が何らの原因によって破壊された場合には第二の記録媒体から得られるデータ(バックアップデータ)を用いて復元する必要がある。このとき、第二の記録媒体から読み出されたデータは復調され、解読手段によって第二の記録媒体が持つ識別情報を元に解読が行われ、その解読された情報、つまり、第一の記録媒体が持つ固有の識別情報で暗号化された情報が第一の記録媒体に書き込まれる。このことにより、第一の記録媒体が持つ識別情報のみによって暗号化された情報が第一の記録媒体に書込まれたことになる。

10

20

30

40

50

【 0 0 1 3 】

以上によりコピー禁止の概念を維持しつつ、バックアップするための記録、あるいは復元するための読取りが可能となる。尚、上記読取り及び書込みはいずれも相互認証を行うことによつてなされるため、不正なコピーやデータが消失することはない。

【 0 0 1 4 】

【 発明の実施の形態 】

図 1 は、本発明が採用される情報再生システムの実施形態を示す図である。情報再生システムは、音源となるホームサーバ 1 を核に、マンマシンインタフェースとなるワイヤレススピーカ 3 が複数分散配置されることによつてユーザに再生情報が享受される構成になっている。そして、ユーザが携帯するワイヤレス端末 2 の移動に伴い、ホームサーバ 1 に接続されるワイヤレススピーカ 3 が選択されるようになっている。

10

【 0 0 1 5 】

図 2 は、図 1 に示すホームサーバ 1 の内部構成を示すブロック図である。図において、11 は親機となる当該ホームサーバ 1 の制御中枢となる CPU である。CPU 11 は、操作キー 12 を介してユーザから与えられる指令を解読して表示部 13 に処理結果を表示したり、後述する各ブロックの制御を行う。CPU 11 は、上記したいずれの制御も内蔵プログラム（図示せず）を読み出し逐次実行することによりなされる。14 は DRAM であり、当該ホームサーバ 1 が持つユニークな識別番号を主に格納するメモリである。

【 0 0 1 6 】

15 は送受信ユニットであり、制御部 151 を核に、送信部 152 と受信部 153 で構成される。送信部 152 は、CPU 11 ならびに制御部 151 による制御の下、CD プレーヤ 45、チューナ 46、HDD 16 等の音源からアドレスデータバス 161、162 経由で供給される音声信号を、マルチプレクサ 17、エンコーダ 18 を介して変調し、マンマシンインタフェースとなる複数のワイヤレススピーカ 3 へ送信する。受信部 153 は、CPU 11 ならびに制御部 151 による制御の下、ワイヤレス端末 2、またはワイヤレススピーカ 3 から供給される信号を受信し、デコーダ 19 で復元し、必要に応じてデマルチプレクサ 20、アドレスデータバス 161、162 経由で HDD 16 にダウンロードする。

20

【 0 0 1 7 】

44 はバックアップ用 HDD であり、HDD 16 と同じくアドレスデータバス 161、162 に接続され、CPU 11 による制御の下で音楽データが記録され、また、読出され、音源として再生系に供給するものとする。図 5 にその詳細が示されている。

30

【 0 0 1 8 】

図 3 は、図 1 に示すワイヤレス端末 2 の内部構成を示すブロック図である。図において、21 は子機となる当該ワイヤレス端末 2 の制御中枢となる CPU である。CPU 21 は、命令コード記憶部 25 に格納された再生指令や記録指令等を表す命令コード（後述するリレーコードを含む）を読み出し実行する他、操作キー 22、表示部 23 による入出力処理を行う。24 は DRAM であり、主に当該ワイヤレス端末のユニークな識別番号（ID）が格納されている。

【 0 0 1 9 】

26 は送受信ユニットであり、制御部 261 を核に、送信部 262 と受信部 263 で構成される。送信部 262 は、CPU 21 ならびに制御部 261 による制御の下、エンコーダ 42 を介して変調された信号をホームサーバ 1 及びワイヤレススピーカ 3 に供給する。受信部 263 は、CPU 21 及び制御部 261 による制御の下、受信した信号をデコーダ 41 によつて復元し、デマルチプレクサ 43 を介して CPU 21 に供給する。HDD 27 に記録された音声情報は、CPU 21 による制御の下、D/A 変換器 28 を介してアナログ信号に変換され、アンプ 29 経由でワイヤレス端末 2 が持つ携帯スピーカ 30 に供給される。

40

【 0 0 2 0 】

図 4 は、図 1 に示すワイヤレススピーカ 3 の内部構成を示すブロック図である。図において、31 は子機となる当該ワイヤレススピーカ 3 の制御中枢となる CPU である。CPU

50

31は、内蔵するプログラムに従い後述する各ブロックの制御を行う。32はIDROMであり、当該ワイヤレススピーカ3に付されたユニークな識別番号が主に格納されるメモリである。

【0021】

33は送受信ユニットであり、制御部331を核に、送信部332、受信部333、そして、電界強度測定部334で構成される。送信部332は、CPU31により生成される信号をエンコーダ36を介して変調し、親機であるホームサーバ1あるいは子機であるワイヤレス端末2へ供給する。受信部333は、制御部331による制御の下、親機であるホームサーバ1から受信した音声信号をデコーダ37により復元し、デマルチプレクサ38経由でCPU31に供給する。CPU31が受信した音声信号は、D/A変換器39を介してアナログ信号に変換され、アンプ34経由でマンマシンインタフェースとしてのスピーカ35に供給され所望の音声として出力される。

10

【0022】

尚、電界強度測定部334は、CPU31による制御の下、子機であるワイヤレス端末2から発せられるリレーコードの電界強度を測定する部分であり、ユーザが当該ワイヤレススピーカ3近傍（例えば半径50cm四方）にいるか否かの判定のために微弱電力で発信されるリレーコードが使用される。リレーコードの受信結果はCPU31に供給される。

【0023】

上述した情報再生システムにおいて、本発明の情報記録読取装置は、例えばホームサーバ1に適用される。ホームサーバ1は、それぞれ固有の識別情報(ID)が付された元データを記録する元ディスクであるHDD16と、バックアップデータを記録するバックアップ用ディスクであるHDD44とを備え、元ディスクである一方のHDD16に付された媒体ID(ID1)に基づいて、例えば、DES(Data Encryption Standard)等の良く知られた暗号化技術を用いて暗号化され、記録された暗号化情報を読み取り、ここで読取られた暗号化情報を更にバックアップ用のHDD44に付された媒体ID(ID2)に基づいて暗号化することによりバックアップ用データを生成し、この生成された暗号化情報をバックアップ用HDD44に記録する。一方、HDD16に記録されている元データが何らかの理由により破壊された場合には、その媒体ID(ID2)を使用してバックアップ用HDD44から元データを復元する。

20

【0024】

尚、記録媒体に固有の識別情報であるIDは、本発明実施形態で用いられるHDDであればディスクの固定領域(FAT:File Allocation Table)に、また、光ディスクであればプリフォーマットとして同じく固定領域に書替え不可の状態を設定されている。本発明では、これら記録媒体が物理的に破壊されない限り、IDが書き替えられることはないことを前提に以下に詳細に説明する。

30

【0025】

図5は、図1に示すホームサーバ1のHDD16、44が持つ周辺回路の詳細を示すブロック図である。図中、Aサイドに元ディスクとなるHDD16の周辺回路が、BサイドにバックアップディスクとなるHDD44の周辺回路が示されている。

【0026】

HDD16の周辺回路は、ピックアップユニット111、復調器112、変調器113、解読器114、118、ID抽出回路115、ドライブCPU116、マルチプレクサ117、暗号器119で構成される。HDD44の周辺回路は、ピックアップユニット120、変調器121、復調器122、暗号器123、ドライブCPU124、ID抽出回路125で構成される。

40

【0027】

HDD16の周辺回路にあるピックアップユニット111は、元ディスク16に対してリードライトを行うために用意される磁気ヘッドを含むリードライト回路である。ここで書き込まれる内容は、例えば、外部から通信により供給される入力データを、暗号器119により元ディスク16が持つ媒体IDに従って暗号化することにより生成される。ここで

50

の暗号化は、ID抽出回路115によって抽出されたID1がドライブCPU116経由で供給されることによりなされる。そして、マルチプレクサ117、変調器113経由でピックアップ111に供給し、元ディスク16に書込む。また、元ディスク16から読出されたデータは、復調器112を経由し、解読器114で暗号化が解かれて、ホームサーバ1が持つD/A変換回路等の再生系(図示せず)に出力される。

【0028】

一方、元ディスク16に記録された内容をHDD44にバックアップする場合は、元ディスク16からピックアップ111、復調器112経由で読出された内容は、Bサイドに示されるHDD44周辺回路にある暗号器123で暗号化される。ここでの暗号化は、ドライブCPU124の制御の下でID抽出回路125によって抽出されるバックアップ用HDD44の媒体ID(ID2)がドライブCPU124を経由して供給され、このIDに基づいて暗号化される。従って、ここでは、ID1で暗号化された情報が更にID2で暗号化されることになる。

10

【0029】

元ディスク16に記録されていたデータが何らの原因により破壊された場合には、バックアップディスク44から得られるデータを復元する。このとき、バックアップディスク44からピックアップ120経由で読み出されたデータは、復調器122によって復調され、ドライブCPU124の制御の下、HDD16の周辺回路の解読器118に供給される。解読器118では、復調器122から得られるデータに関し、ドライブCPU116を介して通知されるバックアップ用HDD44の媒体IDであるID2による暗号化を解いて、ID2を分離してマルチプレクサ117、変調器113経由でピックアップ111へ供給する。このことにより、ピックアップユニット111は、ID1のみにより暗号化された情報を元ディスク16に書き込む。

20

【0030】

尚、上述した各ブロックは、いずれもハードウェアとして説明したが、一部をドライブCPU116、124が持つファームウェアで実現してもよい。

【0031】

図6、図7は本発明実施形態の動作を示すフローチャートであり、それぞれ、バックアップ記録の際におけるドライブCPU124の動作手順、復元記録の際におけるドライブCPU116の動作手順が示されている。いずれも(a)はメインルーチン、(b)あるいは(c)はサブルーチンを示す。

30

【0032】

以下、図6、図7を参照しながら図5に示す本発明実施形態の動作について詳細に説明する。まず、ドライブCPU124は、ドライブCPU116との間で相互認証処理を行う(ステップS61)。相互認証は、図6(b)に示すように、CPU116に対してあらかじめ定義された認証コードを要求し(ステップS611)、その認証コードをチェックして(ステップS611)、それが所定のコードであれば、あらかじめ定義されたドライブCPU124の認証コードをドライブCPU116に送出し(ステップS613)、ドライブCPU116からACKが返答されたときに認証成功(ステップS614)とする。認証が失敗に終わった場合はエラーとする(ステップS615)。

40

【0033】

次に、ドライブCPU124は、バックアップディスク44の媒体ID(ID2)を抽出する(ステップS62)。そしてドライブCPU116に対してデータ転送要求を発行し(ステップS63)、元ディスク16から元データを供給することを要求し、そのデータに基づいて記録処理を行う(ステップS64)。記録処理は、図6(c)に示すように、暗号器123でドライブCPU124を介して供給されるID2に基づき、復調器112から得られる元データ(ID1により暗号化済み)を暗号化し(ステップS641)、変調器121で記録変調して、ピックアップ120経由でバックアップディスク44にその内容を書き込む(ステップS642)ことによりなされる。そして、所望の所定量のデータ転送が終了したか否かをチェック(ステップS65)し、否の場合、ステップS63以

50

降の処理を繰り返し全ての転送終了を待ってバックアップ処理を終える。

【0034】

次に、元データが何らかの原因により破壊されたときのバックアップディスク44による復元記録処理について図7のフローチャートを参照しながら説明する。まず、ドライブCPU116は、相互認証処理を行う(ステップS71)。相互認証処理は、図6(b)で示す手順と同様である。次に、ドライブCPU124に対してバックアップディスク44の媒体IDであるID2の送信要求を発行する(ステップS72)。そして、バックアップディスク44からのデータ転送を要求し(ステップS73)、元ディスク16への記録処理を実行する(ステップS74)。

【0035】

記録処理は、図7(b)に示すように、ドライブCPU116は、復調器122を介して得られるバックアップ用HDD44の媒体ID(ID2)で暗号化されているバックアップデータを解読器118により、ステップS72で供給されたID2に基づいて解読し(ステップS741)、マルチプレクサ117を介して変調器113で記録変調する(ステップS742)。変調器113で記録変調されたバックアップデータは、ピックアップユニット111経由で元ディスク16に書き込まれる。

【0036】

次に、所望の所定量のデータ転送が終了したか否かをチェック(ステップS75)し、否の場合、ステップS73以降の処理を繰り返し全ての転送終了を待って復元記録処理を終える。

【0037】

以上説明のように本発明は、第一の記録媒体16に記録された元データをバックアップするとき、第一の記憶媒体に付された識別情報(ID1)に基づいて暗号化され記録される第一の暗号化情報を読み取り、読み取られた第一の暗号化情報を、バックアップ用の第二の記録媒体44に付された識別情報(ID2)に基づいて暗号化して第二の暗号化情報を生成し、ここで生成された第二の暗号化情報を第二の記録媒体に記録する。バックアップデータを復元するとき、第二の記録媒体から第二の暗号化情報を読み取り、第二の暗号化情報を第二の記録媒体が持つ識別情報に基づいて解読し、この解読された第二の暗号化情報を第一の暗号化情報として復元して第一の記録媒体に記録するものである。このことによりバックアップ記録が可能となり、正規のユーザに不利益を与えず、著作権者の権利を保護することができる。

【0038】

【発明の効果】

以上説明のように本発明によれば、複数の記録媒体を有する情報記録読み取り装置において、第一の記録媒体に記録された情報データを、バックアップ用の第二の記録媒体に記録する際、バックアップ用の第二の記録媒体に固有の識別情報に基づき暗号化して記録することにより、第一の記録媒体とはその内容を異にし、このことにより、コピー禁止の概念を維持しつつ、バックアップするための記録を可能とするものである。また、何らかの原因により第一の記録媒体に記録された元データが破壊されたとき、第二の記録媒体が持つ識別情報に基づき解読することによって第一の記録媒体に元データの復元が可能となる。更に、上記した記録、復元は相互認証により行われるため、違法なコピーを防止できる。

【0039】

従って、著作権者に対する権利の保護がはかれると共に、更に、正規のユーザにも不利益が生じることが無いようにコピー禁止の概念を維持しつつバックアップのための記録が可能となり、今後の情報通信分野において有効な手段となる。

【図面の簡単な説明】

【図1】 本発明が採用される情報再生システムの構成例を示すブロック図である。

【図2】 図1におけるホームサーバの内部構成を示すブロック図である。

【図3】 図1におけるワイヤレス端末の内部構成を示すブロック図である。

【図4】 図1におけるワイヤレススピーカの内部構成を示すブロック図である。

10

20

30

40

50

【図5】 図1、図2に示すホームサーバのうち、本発明と関係する部分のみ抽出して示したブロック図である。

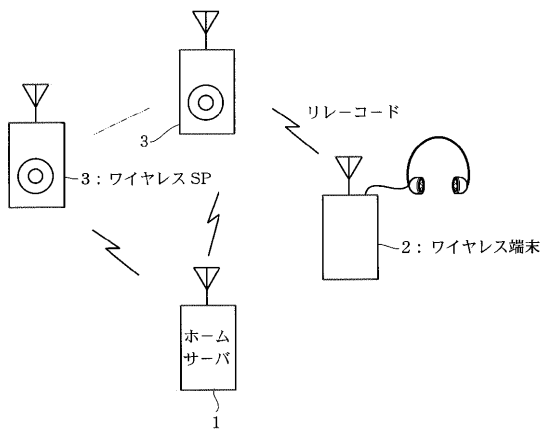
【図6】 本発明実施形態の動作手順をフローチャートで示した図である。

【図7】 本発明実施形態の動作手順をフローチャートで示した図である。

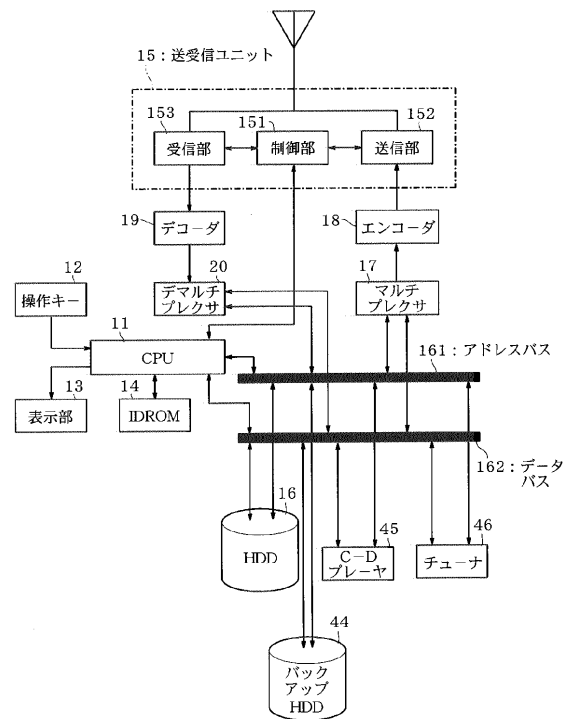
【符号の説明】

1 ... ホームサーバ、 2 ... ワイヤレス端末、 11 (21、 31) ... CPU、 12 (22) ... 操作キー、 14 (24、 32) ... IDROM、 15 (26、 33) ... 送受信ユニット、 16 (27) ... ハードディスク装置 (HDD)、 44 ... バックアップディスク装置 (HDD)、 112 (122) ... 復調器、 113 (121) ... 変調器、 114 (118) ... 解読器、 115 (125) ... ID抽出回路、 116 (124) ... ドライブCPU、 117 ... マルチプレクサ、 119 (123) ... 暗号器

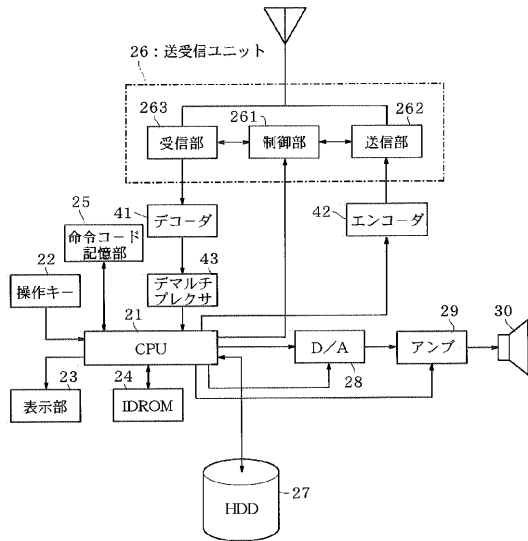
【図1】



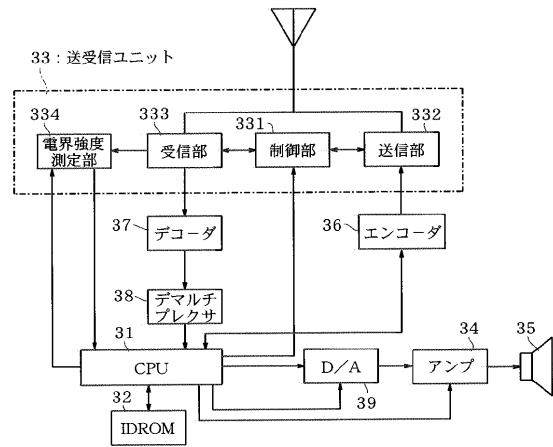
【図2】



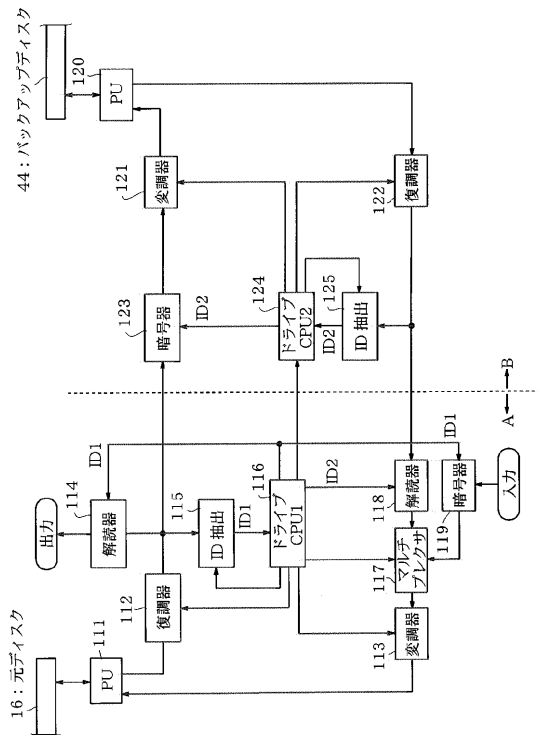
【図3】



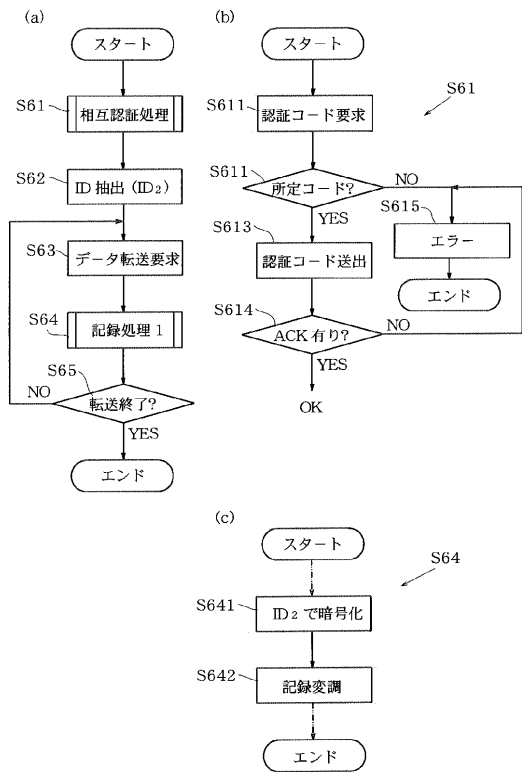
【図4】



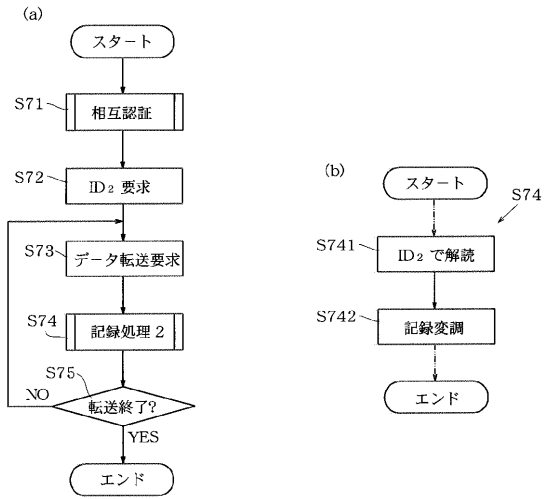
【図5】



【図6】



【図7】



フロントページの続き

- (56)参考文献 特開平02 - 110491 (JP, A)
特開平08 - 069419 (JP, A)
特開平10 - 021144 (JP, A)
特開平05 - 233459 (JP, A)
特開平04 - 184650 (JP, A)
特開平11 - 328033 (JP, A)

- (58)調査した分野(Int.Cl., DB名)

G06F 21/24