

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4568933号
(P4568933)

(45) 発行日 平成22年10月27日(2010.10.27)

(24) 登録日 平成22年8月20日(2010.8.20)

(51) Int.Cl.		F I		
G 0 6 F 21/24	(2006.01)	G 0 6 F	12/14	5 5 0 A
G 1 1 B 20/10	(2006.01)	G 1 1 B	20/10	H
G 1 1 B 27/00	(2006.01)	G 1 1 B	27/00	A

請求項の数 7 (全 45 頁)

(21) 出願番号	特願平11-366086	(73) 特許権者	000002185
(22) 出願日	平成11年12月24日(1999.12.24)		ソニー株式会社
(65) 公開番号	特開2000-305854(P2000-305854A)		東京都港区港南1丁目7番1号
(43) 公開日	平成12年11月2日(2000.11.2)	(74) 代理人	100082131
審査請求日	平成18年3月10日(2006.3.10)		弁理士 稲本 義雄
(31) 優先権主張番号	特願平10-369414	(72) 発明者	河上 達
(32) 優先日	平成10年12月25日(1998.12.25)		東京都品川区北品川6丁目7番35号 ソニー株式会社内
(33) 優先権主張国	日本国(JP)	(72) 発明者	石黒 隆二
(31) 優先権主張番号	特願平11-39222		東京都品川区北品川6丁目7番35号 ソニー株式会社内
(32) 優先日	平成11年2月17日(1999.2.17)	(72) 発明者	田辺 充
(33) 優先権主張国	日本国(JP)		東京都品川区北品川6丁目7番35号 ソニー株式会社内

最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、並びにプログラム格納媒体

(57) 【特許請求の範囲】

【請求項1】

第1の記録媒体に記録されているコンテンツを複製し、その結果得られるコピーコンテンツを前記第1の記録媒体とは異なる第2の記録媒体に記録する複製手段と、

前記第1の記録媒体に記録されている前記コンテンツが前記複製手段によって複製される毎、前記コンテンツを識別する識別情報に前記コンテンツが複製されたときの時刻情報を対応付けて記憶している期限データベースを更新する更新手段と、

第1の記録媒体に記録されている前記コンテンツの複製がユーザから指示された場合、複製が指示されたコンテンツの識別情報を取得する取得手段と、

取得された前記識別情報に対応するコンテンツが前回複製されたときの時刻情報を前記期限データベースから読み出し、

複製が指示された前記コンテンツが前回複製されてから所定の時間が経過している場合には、前記複製手段に対して前記コンテンツの複製を許可し、

複製が指示された前記コンテンツが前回複製されてから所定の時間が経過していない場合には、前記複製手段に対して前記コンテンツの複製を禁止する複製制御手段とを含む情報処理装置。

【請求項2】

前記識別情報は、ISRC(International Standard Recording Code)である

請求項1に記載の情報処理装置。

【請求項3】

10

20

前記識別情報は、TOC(Table of Contents)である
請求項 1 に記載の情報処理装置。

【請求項 4】

前記取得手段は、前記コンテンツの識別情報である前記ISRCを、前記コンテンツが記憶されている前記第 1 の記録媒体から読み出し、前記ISRCが前記第 1 の記録媒体に記録されていない場合は、前記コンテンツの識別情報としてTOCを用いる

請求項 1 に記載の情報処理装置。

【請求項 5】

前記期限データベースの改竄を、ハッシュ関数を用いて検出する検出手段をさらに含み、

前記複製制御手段は、前記期限データベースの改竄が検出された場合にも、前記複製手段に対して前記コンテンツの複製を禁止する

請求項 1 に記載の情報処理装置。

【請求項 6】

第 1 の記録媒体に記録されているコンテンツを複製し、その結果得られるコピーコンテンツを前記第 1 の記録媒体とは異なる第 2 の記録媒体に記録する複製手段を備える情報処理装置の情報処理方法において、

前記第 1 の記録媒体に記録されている前記コンテンツが前記複製手段によって複製される毎、前記コンテンツを識別する識別情報に前記コンテンツが複製されたときの時刻情報を対応付けて記憶している期限データベースを更新する更新ステップと、

第 1 の記録媒体に記録されている前記コンテンツの複製がユーザから指示された場合、複製が指示されたコンテンツの識別情報を取得する取得ステップと、

取得された前記識別情報に対応するコンテンツが前回複製されたときの時刻情報を前記期限データベースから読み出し、

複製が指示された前記コンテンツが前回複製されてから所定の時間が経過している場合には、前記複製手段に対して前記コンテンツの複製を許可し、

複製が指示された前記コンテンツが前回複製されてから所定の時間が経過していない場合には、前記複製手段に対して前記コンテンツの複製を禁止する複製制御ステップと

を含む情報処理方法。

【請求項 7】

第 1 の記録媒体に記録されているコンテンツを複製し、その結果得られるコピーコンテンツを前記第 1 の記録媒体とは異なる第 2 の記録媒体に記録する複製手段を備える情報処理装置の制御用のプログラムであって、

前記第 1 の記録媒体に記録されている前記コンテンツが前記複製手段によって複製される毎、前記コンテンツを識別する識別情報に前記コンテンツが複製されたときの時刻情報を対応付けて記憶している期限データベースを更新する更新ステップと、

第 1 の記録媒体に記録されている前記コンテンツの複製がユーザから指示された場合、複製が指示されたコンテンツの識別情報を取得する取得ステップと、

取得された前記識別情報に対応するコンテンツが前回複製されたときの時刻情報を前記期限データベースから読み出し、

複製が指示された前記コンテンツが前回複製されてから所定の時間が経過している場合には、前記複製手段に対して前記コンテンツの複製を許可し、

複製が指示された前記コンテンツが前回複製されてから所定の時間が経過していない場合には、前記複製手段に対して前記コンテンツの複製を禁止する複製制御ステップと

を含む処理を情報処理装置のコンピュータに実行させるプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、例えば、

10

20

30

40

50

コンテンツの複製を適切に制限することができるようにした情報処理装置および方法、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】

著作権が設定されているAVコンテンツ（例えば、音楽や画像）の複製を制限する方法として、SCMS(Serial Copy Management System)、CGMS(Copy Generation Management System)などが提案されている。

【0003】

これらのシステムにおいては、図1に示すように、著作権が設定されたコンテンツA1（第1世代）を複製し、コンテンツA2（第2世代）を得ることは（記録することは）できるが、コンテンツA2（第2世代）自体をさらに複製して、コンテンツA3（第3世代）を得ることはできない。

10

【0004】

【発明が解決しようとする課題】

しかしながら、この場合、図1に示すように、コンテンツA1の複製を繰り返すことより、複数の第2世代のコンテンツA2を得ることができ、コンテンツA1の著作権が十分に保護されない課題があった。

【0005】

そこで、コンテンツA1を1度だけ複製することができるようにした方法として、UCS(Uni Copy System)が提案されているが、この場合、ユーザは、個人の使用の範囲においても、1度だけしか複製することができず、ユーザに不利益を与える課題があった。

20

【0006】

本発明はこのような状況に鑑みてなされたものであり、ユーザの利益を大きく損なうことなく、大量の複製を実質的に禁止することができるようにするものである。

【0007】

【課題を解決するための手段】

本発明の情報処理装置は、第1の記録媒体に記録されているコンテンツを複製し、その結果得られるコピーコンテンツを前記第1の記録媒体とは異なる第2の記録媒体に記録する複製手段と、前記第1の記録媒体に記録されている前記コンテンツが前記複製手段によって複製される毎、前記コンテンツを識別する識別情報に前記コンテンツが複製されたときの時刻情報に対応付けて記憶している期限データベースを更新する更新手段と、第1の記録媒体に記録されている前記コンテンツの複製がユーザから指示された場合、複製が指示されたコンテンツの識別情報を取得する取得手段と、取得された前記識別情報に対応するコンテンツが前回複製されたときの時刻情報を前記期限データベースから読み出し、複製が指示された前記コンテンツが前回複製されてから所定の時間が経過している合には、前記複製手段に対して前記コンテンツの複製を許可し、複製が指示された前記コンテンツが前回複製されてから所定の時間が経過していない場合には、前記複製手段に対して前記コンテンツの複製を禁止する複製制御手段とを含む。

30

【0008】

本発明の情報処理方法は、第1の記録媒体に記録されているコンテンツを複製し、その結果得られるコピーコンテンツを前記第1の記録媒体とは異なる第2の記録媒体に記録する複製手段を備える情報処理装置の情報処理方法において、前記第1の記録媒体に記録されている前記コンテンツが前記複製手段によって複製される毎、前記コンテンツを識別する識別情報に前記コンテンツが複製されたときの時刻情報に対応付けて記憶している期限データベースを更新する更新ステップと、第1の記録媒体に記録されている前記コンテンツの複製がユーザから指示された場合、複製が指示されたコンテンツの識別情報を取得する取得ステップと、取得された前記識別情報に対応するコンテンツが前回複製されたときの時刻情報を前記期限データベースから読み出し、複製が指示された前記コンテンツが前回複製されてから所定の時間が経過している場合には、前記複製手段に対して前記コンテンツの複製を許可し、複製が指示された前記コンテンツが前回複製されてから所定の時間

40

50

が経過していない場合には、前記複製手段に対して前記コンテンツの複製を禁止する複製制御ステップとを含む。

【0009】

本発明のプログラム格納媒体は、第1の記録媒体に記録されているコンテンツを複製し、その結果得られるコピーコンテンツを前記第1の記録媒体とは異なる第2の記録媒体に記録する複製手段を備える情報処理装置の制御用のプログラムであって、前記第1の記録媒体に記録されている前記コンテンツが前記複製手段によって複製される毎、前記コンテンツを識別する識別情報に前記コンテンツが複製されたときの時刻情報を対応付けて記憶している期限データベースを更新する更新ステップと、第1の記録媒体に記録されている前記コンテンツの複製がユーザから指示された場合、複製が指示されたコンテンツの識別情報を取得する取得ステップと、取得された前記識別情報に対応するコンテンツが前回複製されたときの時刻情報を前記期限データベースから読み出し、複製が指示された前記コンテンツが前回複製されてから所定の時間が経過している場合には、前記複製手段に対して前記コンテンツの複製を許可し、複製が指示された前記コンテンツが前回複製されてから所定の時間が経過していない場合には、前記複製手段に対して前記コンテンツの複製を禁止する複製制御ステップとを含む処理を情報処理装置のコンピュータに実行させるプログラムが格納されている。

10

【0010】

本発明においては、第1の記録媒体に記録されているコンテンツが複製手段によって複製される毎、コンテンツを識別する識別情報にコンテンツが複製されたときの時刻情報を対応付けて記憶している期限データベースが更新され、第1の記録媒体に記録されているコンテンツの複製がユーザから指示された場合、複製が指示されたコンテンツの識別情報が取得され、取得された識別情報に対応するコンテンツが前回複製されたときの時刻情報が期限データベースから読み出され、複製が指示されたコンテンツが前回複製されてから所定の時間が経過している場合には、複製手段に対してコンテンツの複製が許可される。反対に、複製が指示されたコンテンツが前回複製されてから所定の時間が経過していない場合には、複製手段に対してコンテンツの複製が禁止される。

20

【0011】

【発明の実施の形態】

図2は、本発明に係る音声データ管理システムの一実施の形態を示す図である。パーソナルコンピュータ1は、ローカルエリアネットワークまたはインターネットなどから構成されるネットワーク2に接続されている。パーソナルコンピュータ1は、EMD (Electrical Music Distribution) サーバ4-1乃至4-3から受信した、または後述するCD (Compact Disc) から読み取った音楽のデータ(以下、コンテンツと称する)を、所定の圧縮の方式(例えば、ATRAC3(商標))に変換するとともにDES (Data Encryption Standard) などの暗号化方式で暗号化して記録する。

30

【0012】

パーソナルコンピュータ1は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に3台のポータブルデバイス (Portable Device (PDとも称する)) 6-1乃至6-3で利用できる、コピー(ポータブルデバイス6-1乃至6-3にコンテンツを記憶させても、パーソナルコンピュータ1が記録しているコンテンツは使用できる。ポータブルデバイス6-1乃至6-3にコンテンツを記憶させることができる回数は制限される場合がある。この場合、その回数は、増えることがない。)することができる、他のパーソナルコンピュータに移動する(ポータブルデバイス6-1乃至6-3にコンテンツを記憶させた後、パーソナルコンピュータ1が記録しているコンテンツは使用できなくなる。)ことができるなどを示す。利用条件のデータの詳細は、後述する。

40

【0013】

パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連

50

するデータ（例えば、曲名、または再生条件など）と共に、USB（Universal Serial Bus）ケーブル7-1を介して、接続されているポータブルデバイス6-1に記憶させるとともに、ポータブルデバイス6-1に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1減らされる。チェックアウトできる回数が0のとき、対応するコンテンツは、チェックアウトすることができない。

【0014】

パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル7-2を介して、接続されているポータブルデバイス6-2に記憶させるとともに、ポータブルデバイス6-2に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル7-3を介して、接続されているポータブルデバイス6-3に記憶させるとともに、ポータブルデバイス6-3に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

【0015】

また、パーソナルコンピュータ1は、USBケーブル7-1を介して、接続されているポータブルデバイス6-1にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-1に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。より詳細には、チェックインしたとき、パーソナルコンピュータ1が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、1増やされる。

【0016】

パーソナルコンピュータ1は、USBケーブル7-2を介して、接続されているポータブルデバイス6-2にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-2に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、USBケーブル7-3を介して、接続されているポータブルデバイス6-3にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-3に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

【0017】

パーソナルコンピュータ1は、図示せぬ他のパーソナルコンピュータがポータブルデバイス6-1にチェックアウトしたコンテンツをチェックインできない。

パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-2にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-3にチェックアウトしたコンテンツをチェックインできない。

【0018】

EMD登録サーバ3は、パーソナルコンピュータ1がEMDサーバ4-1乃至4-3からコンテンツの取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とEMDサーバ4-1乃至4-3との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、EMDサーバ4-1乃至4-3に接続するためのプログラムをパーソナルコンピュータ1に送信する。

【0019】

EMDサーバ4-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータ（例えば、曲名、または再生制限など）と共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共

10

20

30

40

50

に、パーソナルコンピュータ 1 にコンテンツを供給する。EMDサーバ 4 - 3 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ 1 にコンテンツを供給する。

【 0 0 2 0 】

EMDサーバ 4 - 1 乃至 4 - 3 のそれぞれが供給するコンテンツは、同一または異なる圧縮の方式で圧縮されている。EMDサーバ 4 - 1 乃至 4 - 3 のそれぞれが供給するコンテンツは、同一または異なる暗号化の方式で暗号化されている。

【 0 0 2 1 】

WWW (World Wide Web) サーバ 5 - 1 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツを読み取った CD (例えば、CD のアルバム名、または CD の販売会社など)、および CD から読み取ったコンテンツに対応するデータ (例えば、曲名、または作曲者名など) をパーソナルコンピュータ 1 に供給する。WWW サーバ 5 - 2 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツを読み取った CD、および CD から読み取ったコンテンツに対応するデータをパーソナルコンピュータ 1 に供給する。

10

【 0 0 2 2 】

ポータブルデバイス 6 - 1 は、パーソナルコンピュータ 1 から供給されたコンテンツ (すなわち、チェックアウトされたコンテンツ) を、コンテンツに関連するデータ (例えば、曲名、または再生制限など) と共に記憶する。ポータブルデバイス 6 - 1 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドホンなどに出力する。

20

【 0 0 2 3 】

例えば、コンテンツに関連するデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス 6 - 1 は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス 6 - 1 は、対応するコンテンツの再生を停止する。

【 0 0 2 4 】

使用者は、コンテンツを記憶したポータブルデバイス 6 - 1 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドホンなどで聴くことができる。

30

【 0 0 2 5 】

ポータブルデバイス 6 - 2 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス 6 - 2 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドホンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6 - 2 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドホンなどで聴くことができる。

【 0 0 2 6 】

ポータブルデバイス 6 - 3 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス 6 - 3 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドホンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6 - 3 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドホンなどで聴くことができる。

40

【 0 0 2 7 】

以下、ポータブルデバイス 6 - 1 乃至 6 - 3 を個々に区別する必要がないとき、単にポータブルデバイス 6 と称する。

【 0 0 2 8 】

図 3 は、パーソナルコンピュータ 1 の構成を説明する図である。CPU (Central Processin

50

g Unit) 11は、各種アプリケーションプログラム(詳細については後述する)や、OS(Operating System)を実際に行う。ROM(Read-only Memory)12は、一般的には、CPU11が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM(Random-Access Memory)13は、CPU11の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス14により相互に接続されている。

【0029】

ホストバス14は、ブリッジ15を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス16に接続されている。

【0030】

キーボード18は、CPU11に各種の指令を入力するとき、使用者により操作される。マウス19は、ディスプレイ20の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ20は、液晶表示装置またはCRT(Cathode Ray Tube)などから成り、各種情報をテキストやイメージで表示する。HDD(Hard Disk Drive)21は、ハードディスクを駆動し、それらにCPU11によって実行するプログラムや情報を記録または再生させる。

【0031】

ドライブ22は、装着されている磁気ディスク41、光ディスク42(CDを含む)、光磁気ディスク43、または半導体メモリ44に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース17、外部バス16、ブリッジ15、およびホストバス14を介して接続されているRAM13に供給する。

【0032】

USBポート23-1には、USBケーブル7-1を介して、ポータブルデバイス6-1が接続される。USBポート23-1は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ(例えば、コンテンツまたはポータブルデバイス6-1のコマンドなどを含む)をポータブルデバイス6-1に出力する。

【0033】

USBポート23-2には、USBケーブル7-2を介して、ポータブルデバイス6-2が接続される。USBポート23-2は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ(例えば、コンテンツまたはポータブルデバイス6-2のコマンドなどを含む)をポータブルデバイス6-2に出力する。

【0034】

USBポート23-3には、USBケーブル7-3を介して、ポータブルデバイス6-3が接続される。USBポート23-3は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ(例えば、コンテンツまたはポータブルデバイス6-3のコマンドなどを含む)をポータブルデバイス6-3に出力する。

【0035】

IEC(International Electrotechnical Commission)60958端子を有する音声入出力インタフェース24は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ45は、音声入出力インタフェース24から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

【0036】

これらのキーボード18乃至音声入出力インタフェース24は、インターフェース17に接続されており、インターフェース17は、外部バス16、ブリッジ15、およびホストバス14を介してCPU11に接続されている。

【0037】

通信部25は、ネットワーク2が接続され、CPU11、またはHDD21から供給されたデー

10

20

30

40

50

タ（例えば、登録の要求、またはコンテンツの送信要求など）を、所定の方式の packets に格納して、ネットワーク 2 を介して、送信するとともに、ネットワーク 2 を介して、受信した packets に格納されているデータ（例えば、認証鍵、またはコンテンツなど）を CPU 1 1、RAM 1 3、または HDD 2 1 に出力する。

【 0 0 3 8 】

半導体 IC として、一体的に形成され、パーソナルコンピュータ 1 に装着されるアダプタ 2 6 の CPU 3 2 は、外部バス 1 6、ブリッジ 1 5、およびホストバス 1 4 を介してパーソナルコンピュータ 1 の CPU 1 1 と共働し、各種の処理を実行する。RAM 3 3 は、CPU 3 2 が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ 3 4 は、パーソナルコンピュータ 1 の電源がオフされた後も保持する必要があるデータを記憶する。ROM 3 6 には、パーソナルコンピュータ 1 から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 3 5 は、計時動作を実行し、時刻情報を提供する。

10

【 0 0 3 9 】

通信部 2 5 およびアダプタ 2 6 は、外部バス 1 6、ブリッジ 1 5、およびホストバス 1 4 を介して CPU 1 1 に接続されている。

【 0 0 4 0 】

以下、USBポート 2 3 - 1 乃至 2 3 - 3 を個々に区別する必要がないとき、単に、USBポート 2 3 と称する。以下、USBケーブル 7 - 1 乃至 7 - 3 を個々に区別する必要がないとき、単に USBケーブル 7 と称する。

20

【 0 0 4 1 】

次に、ポータブルデバイス 6 の構成を図 4 を参照して説明する。電源回路 5 2 は、乾電池 5 1 から供給される電源電圧を所定の電圧の内部電力に変換して、CPU 5 3 乃至表示部 6 7 に供給することにより、ポータブルデバイス 6 全体を駆動させる。

【 0 0 4 2 】

USBコントローラ 5 7 は、USBコネクタ 5 6 を介して、パーソナルコンピュータ 1 と USBケーブル 7 を介して接続された場合、パーソナルコンピュータ 1 から転送されたコンテンツを、内部バス 5 8 を介して、CPU 5 3 に供給する。

【 0 0 4 3 】

コンテンツは、1 packet 当たり 64 バイトのデータから構成され、12 Mbit/sec の転送レートでパーソナルコンピュータ 1 から転送される。

30

【 0 0 4 4 】

ポータブルデバイス 6 に転送されるコンテンツは、ヘッダおよび音声データ（コンテンツの実体である、音声信号に対応したデータ）から構成され、ヘッダには、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデック ID、ファイル情報などが格納されていると共に、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限、および再生回数カウンタなどが格納されている。音声データは、ATRAC3 などの符号化方式で符号化され、暗号化されている、所定の曲の音声信号に対応するデータである。

【 0 0 4 5 】

ヘッダサイズは、ヘッダのデータ長（例えば、33 バイトなど）を表し、ファイルサイズは、音声データのデータ長（例えば、33,636,138 バイトなど）を表す。

40

【 0 0 4 6 】

コンテンツ鍵は、暗号化されている音声データを復号するための鍵であり、パーソナルコンピュータ 1 とポータブルデバイス 6 との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ 1 からポータブルデバイス 6 に送信される。

【 0 0 4 7 】

ポータブルデバイス 6 が USBケーブル 7 を介してパーソナルコンピュータ 1 の USBポート 2 3 に接続されたとき、ポータブルデバイス 6 とパーソナルコンピュータ 1 とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の

50

処理である。ちなみに、ポータブルデバイス6のDSP59は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読(復号)の処理を実行する。

【0048】

チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ1が生成するある値(チャレンジ)に対して、ポータブルデバイス6がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値(レスポンス)で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ1が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス6が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ1は不正を検出できる。

10

【0049】

コーデックIDは、音声データの符号化方式に対応したIDであり、例えば、コーデックID"1"は、ATRAC3に対応し、コーデックID"0"は、MP3(MPEG(Moving Picture Experts Group) Audio Layer-3)に対応する。

【0050】

ファイル名は、コンテンツに対応するパーソナルコンピュータ1が記録しているコンテンツファイル(後述する)をASCII(American National Standard Code for Information Interchange)コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、または作曲者名などをASCIIコードに変換したデータである。

20

【0051】

再生制限データは、コンテンツの再生が可能な期間(すなわち、開始日時または終了日時)または回数制限(再生の回数の制限)が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、"1"が割り当てられ、再生が可能な期間が設定されているとき、"2"が割り当てられ、回数制限および再生が可能な期間がいずれも設定されていないとき(いわゆる、買い取りで購入されたとき)、"0"が割り当てられる。

【0052】

開始日時および終了日時は、再生制限データが"2"であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が"00040F"であり、終了日時が"00070F"であるとき、対応するコンテンツは、2000年4月15日から2000年7月15日まで、再生が可能である。

30

【0053】

同様に、回数制限および再生回数カウンタは、再生制限データが"1"または"2"であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときCPU53により更新される、コンテンツが再生された回数を示す。例えば、回数制限が"02"であるとき、そのコンテンツの再生可能な回数は2回であり、再生回数カウンタが"01"であるとき、そのコンテンツが再生された回数は1回である。

40

【0054】

例えば、再生制限データが"2"であり、開始日時が"00040F"であり、終了日時が"00070F"であり、再生制限データが"2"であるとき、ポータブルデバイス6は、対応するコンテンツを、2000年4月15日から2000年7月15日までの期間において、1日2回ずつ繰り返し再生できる。

【0055】

例えば、再生制限データが"1"であり、開始日時が"000000"であり、終了日時が"000000"であり、再生制限データが"0a"であり、再生回数カウンタが"05"であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が10回であり、再生された回数が5回である。

50

【 0 0 5 6 】

ポータブルデバイス 6 が、パーソナルコンピュータ 1 からコンテンツと共にコンテンツの書き込み命令を受信した場合、ROM 5 5 から RAM 5 4 に読み出したメインプログラムを実行する CPU 5 3 は、書き込み命令を受け取り、フラッシュメモリコントローラ 6 0 を制御して、パーソナルコンピュータ 1 から受信したコンテンツをフラッシュメモリ 6 1 に書き込ませる。

【 0 0 5 7 】

フラッシュメモリ 6 1 は、約 64 MByte の記憶容量を有し、コンテンツ（音声データ）を記憶する。また、フラッシュメモリ 6 1 には、所定の圧縮方式で圧縮されている音声データを伸張するための再生用コードが予め格納されている。

10

【 0 0 5 8 】

なお、フラッシュメモリ 6 1 は、ポータブルデバイス 6 に着脱可能とすることができる。

【 0 0 5 9 】

使用者による、図示せぬ再生 / 停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ 6 2 を介して CPU 5 3 に供給されると、CPU 5 3 は、フラッシュメモリコントローラ 6 0 に、フラッシュメモリ 6 1 から、再生用コードと音声データとを読み出させ、DSP 5 9 に転送させる。

【 0 0 6 0 】

DSP 5 9 は、フラッシュメモリ 6 1 から転送された再生用コードに基づいて音声データを CRC (Cyclic Redundancy Check) 方式で誤り検出をした後、再生して、再生したデータ（図 4 中において D1 で示す）をデジタル / アナログ変換回路 6 3 に供給する。

20

【 0 0 6 1 】

DSP 5 9 は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発信子 5 9 A からのマスタークロック MCLK を基に、音声データを再生するとともに、マスタークロック MCLK、マスタークロック MCLK を基に内部の発振回路で生成した所定の周波数のピットクロック BCLK、並びにフレーム単位の L チャンネルクロック LCLK、および R チャンネルクロック RCLK からなる動作クロック LRCLK をデジタルアナログ変換回路 6 3 に供給する。

【 0 0 6 2 】

DSP 5 9 は、音声データを再生するとき、再生用コードに従って上述の動作クロックをデジタルアナログ変換回路 6 3 に供給して、音声データを再生しないとき、再生用コードに従って動作クロックの供給を停止して、デジタルアナログ変換回路 6 3 を停止させて、ポータブルデバイス 6 全体の消費電力量を低減する。

30

【 0 0 6 3 】

同様に、CPU 5 3 および USB コントローラ 5 7 も、水晶でなる発振子 5 3 A または 5 7 A がそれぞれ外付けされ、発振子 5 3 A または 5 7 A からそれぞれ供給されるマスタークロック MCLK に基づき、所定の処理を実行する。

【 0 0 6 4 】

このように構成することで、ポータブルデバイス 6 は、CPU 5 3、DSP 5 9、USB コントローラ 5 7 等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化すると共に小型化することができる。

40

【 0 0 6 5 】

デジタルアナログ変換回路 6 3 は、再生した音声データをアナログの音声信号に変換して、これを増幅回路 6 4 に供給する。増幅回路 6 4 は、音声信号を増幅して、ヘッドフォンジャック 6 5 を介して、図示せぬヘッドフォンに音声信号を供給する。

【 0 0 6 6 】

このように、ポータブルデバイス 6 は、図示せぬ再生 / 停止ボタンが押圧操作されたとき、CPU 5 3 の制御に基づいてフラッシュメモリ 6 1 に記憶されている音声データを再生するとともに、再生中に再生 / 停止ボタンが押圧操作されたとき、音声データの再生を停止する。

50

【 0 0 6 7 】

ポータブルデバイス 6 は、停止後に再度再生 / 停止ボタンが押圧操作されたとき、CPU 5 3 の制御に基づいて停止した位置から音声データの再生を再開する。再生 / 停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス 6 は、自動的に電源をオフして消費電力を低減する。

【 0 0 6 8 】

因みに、ポータブルデバイス 6 は、電源がオフになった後に再生 / 停止ボタンが押圧操作されたとき、前回の停止した位置から音声データを再生せず、1 曲目から再生する。

【 0 0 6 9 】

また、ポータブルデバイス 6 の CPU 5 3 は、LCD コントローラ 6 8 を制御して、表示部 6 7 に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量および乾電池 5 1 の残量等の情報を表示させる。

10

【 0 0 7 0 】

さらに、ポータブルデバイス 6 は、EEPROM 6 8 に、フラッシュメモリ 8 0 に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ 6 1 のブロック位置、およびその他種々のメモリ蓄積情報等のいわゆる FAT (File Allocation Table) を格納する。

【 0 0 7 1 】

因みに、本実施の形態においては、音声データは、64KByte を 1 ブロックとして扱われ、1 曲のコンテンツに対応したブロック位置が FAT に格納される。

20

【 0 0 7 2 】

フラッシュメモリ 6 1 に FAT が格納される場合、例えば、1 曲目のコンテンツが CPU 5 3 の制御によりフラッシュメモリ 6 1 に書き込まれると、1 曲目のコンテンツに対応するブロック位置が FAT としてフラッシュメモリ 6 1 に書き込まれ、次に、2 曲目のコンテンツがフラッシュメモリ 6 1 に書き込まれると、2 曲目のコンテンツに対応するブロック位置が FAT としてフラッシュメモリ 6 1 (1 曲目と同一の領域) に書き込まれる。

【 0 0 7 3 】

このように、FAT は、フラッシュメモリ 6 1 へのコンテンツの書き込みの度に書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に 2 重に書き込まれる。

30

【 0 0 7 4 】

FAT がフラッシュメモリ 6 1 に書き込まれると、1 回のコンテンツの書き込みに対応して、フラッシュメモリ 6 1 の同一の領域が 2 回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ 6 1 に規定されている書き換えの回数に達してしまい、フラッシュメモリ 6 1 の書き換えができなくなってしまう。

【 0 0 7 5 】

そこで、ポータブルデバイス 6 は、FAT を EEPROM 6 8 に記憶させて、1 回のコンテンツの書き込みに対応するフラッシュメモリ 6 1 の書き換えの頻度を少なくしている。

【 0 0 7 6 】

書き換えの回数の多い FAT を EEPROM 6 8 に記憶させることにより、FAT をフラッシュメモリ 6 1 に記憶させる場合に比較して、ポータブルデバイス 6 は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、CPU 5 3 は、EEPROM 6 8 に FAT を追記するように書き込ませるので、EEPROM 6 8 の同一の領域の書き換えの頻度を少なくして、EEPROM 6 8 が短期間で書き換え不能になることを防止する。

40

【 0 0 7 7 】

ポータブルデバイス 6 は、USB ケーブル 7 を介してパーソナルコンピュータ 1 に接続されたとき（以下、これを USB 接続と称する）、USB コントローラ 5 7 から CPU 5 3 に供給される割り込み信号に基づき、USB 接続されたことを認識する。

【 0 0 7 8 】

ポータブルデバイス 6 は、USB 接続されたことを認識すると、パーソナルコンピュータ 1

50

からUSBケーブル7を介して規定電流値の外部電力の供給を受けるとともに、電源回路52を制御して、乾電池51からの電力の供給を停止させる。

【0079】

CPU53は、USB接続されたとき、DSP59の音声データの再生の処理を停止させる。これにより、CPU53は、パーソナルコンピュータ1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

【0080】

このようにCPU53は、USB接続されると、乾電池51から供給される電力からパーソナルコンピュータ1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ1からの外部電力が使用され、電力単価の高い乾電池51の消費電力が低減され、かくして乾電池51の寿命を延ばすことができる。

10

【0081】

なお、CPU53は、パーソナルコンピュータ1からUSBケーブル7を介して外部電力の供給を受けたとき、DSP59の再生処理を停止させることにより、DSP59からの輻射を低減させ、その結果としてパーソナルコンピュータ1を含むシステム全体の輻射を一段と低減させる。

【0082】

図5は、CPU11の所定のプログラムの実行等により実現される、パーソナルコンピュータ1の機能の構成を説明するブロック図である。コンテンツ管理プログラム111は、EMD選択プログラム131、チェックイン/チェックアウト管理プログラム132、暗号方式変換プログラム133、圧縮方式変換プログラム134、暗号化プログラム135、利用条件変換プログラム136、署名管理プログラム137、認証プログラム138、復号プログラム139、PD用ドライバ140、購入用ドライバ141、および購入用ドライバ142などの複数のプログラムで構成されている。

20

【0083】

コンテンツ管理プログラム111は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム111を読み出しても、インストラクションを特定できないなど）ように構成されている。

30

【0084】

EMD選択プログラム131は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされるとき、コンテンツ管理プログラム111には含まれず、後述するEMDの登録の処理において、ネットワーク2を介して、EMD登録サーバ3から受信される。EMD選択プログラム131は、EMDサーバ4-1乃至4-3のいずれかとの接続を選択して、購入用アプリケーション115、または購入用ドライバ141若しくは142に、EMDサーバ4-1乃至4-3のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【0085】

チェックイン/チェックアウト管理プログラム132は、チェックインまたはチェックアウトの設定、およびコンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにチェックアウトするか、またはポータブルデバイス6-1乃至6-3に記憶されているコンテンツをチェックインする。

40

【0086】

チェックイン/チェックアウト管理プログラム132は、チェックインまたはチェックアウトの処理に対応して、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータを更新する。

【0087】

50

暗号方式変換プログラム 1 3 3 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの暗号化の方式、購入用ドライバ 1 4 1 が EMD サーバ 4 - 2 から受信したコンテンツの暗号化の方式、または購入用ドライバ 1 4 2 が EMD サーバ 4 - 3 から受信したコンテンツの暗号化の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式に変換する。

【 0 0 8 8 】

また、暗号方式変換プログラム 1 3 3 は、ポータブルデバイス 6 - 1 または 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6 - 1 または 6 - 3 が利用可能な暗号化方式に変換する。

10

【 0 0 8 9 】

圧縮方式変換プログラム 1 3 4 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの圧縮の方式、購入用ドライバ 1 4 1 が EMD サーバ 4 - 2 から受信したコンテンツの圧縮の方式、または購入用ドライバ 1 4 2 が EMD サーバ 4 - 3 から受信したコンテンツの圧縮の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の圧縮の方式に変換する。

【 0 0 9 0 】

圧縮方式変換プログラム 1 3 4 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の符号化の方式で符号化する。

20

【 0 0 9 1 】

また、圧縮方式変換プログラム 1 3 4 は、ポータブルデバイス 6 - 1 または 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6 - 1 または 6 - 3 が利用可能な圧縮の方式に変換する。

【 0 0 9 2 】

暗号化プログラム 1 3 5 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式で暗号化する。

30

【 0 0 9 3 】

利用条件変換プログラム 1 3 6 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの利用条件を示すデータ（いわゆる、Usage Rule）、購入用ドライバ 1 4 1 が EMD サーバ 4 - 2 から受信したコンテンツの利用条件を示すデータ、または購入用ドライバ 1 4 2 が EMD サーバ 4 - 3 から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース 1 1 4 が記録している利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件データと同一のフォーマットに変換する。

【 0 0 9 4 】

また、利用条件変換プログラム 1 3 6 は、ポータブルデバイス 6 - 1 または 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス 6 - 1 または 6 - 3 が利用可能な利用条件のデータに変換する。

40

【 0 0 9 5 】

署名管理プログラム 1 3 7 は、チェックインまたはチェックアウトの処理を実行する前に、コンテンツデータベース 1 1 4 に記録されている利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件のデータに含まれている署名（後述する）を基に、利用条件のデータの改竄を検出する。署名管理プログラム 1 3 7 は、チェックインまたはチェックアウトの処理に伴う、コンテンツデータベース 1 1 4 に記録されている利用条件ファ

50

イル162-1乃至162-Nに格納されている利用条件のデータを更新に対応して、利用条件のデータに含まれる署名を更新する。

【0096】

認証プログラム138は、コンテンツ管理プログラム111と購入用アプリケーションプログラム115との相互認証の処理、およびコンテンツ管理プログラム111と購入用ドライバ141との相互認証の処理を実行する。また、認証プログラム138は、EMDサーバ4-1と購入用アプリケーションプログラム115との相互認証の処理、EMDサーバ4-2と購入用ドライバ141との相互認証の処理、およびEMDサーバ4-3と購入用ドライバ142との相互認証の処理で利用される認証鍵を記憶している。

【0097】

認証プログラム138が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされたとき、認証プログラム138に記憶されておらず、表示操作指示プログラム112により登録の処理が正常に実行されたとき、EMD登録サーバ3から供給され、認証プログラム138に記憶される。

【0098】

復号プログラム139は、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツをパーソナルコンピュータ1が再生するとき、コンテンツを復号する。

【0099】

PD用ドライバ140は、ポータブルデバイス6-2に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス6-2から所定のコンテンツをチェックインするとき、ポータブルデバイス6-2にコンテンツまたはポータブルデバイス6-2に所定の処理を実行させるコマンドを供給する。

【0100】

PD用ドライバ140は、ポータブルデバイス6-1に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス6-1から所定のコンテンツをチェックインするとき、デバイスドライバ116-1にコンテンツ、またはデバイスドライバ116-1に所定の処理を実行させるコマンドを供給する。

【0101】

PD用ドライバ140は、ポータブルデバイス6-3に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス6-3から所定のコンテンツをチェックインするとき、デバイスドライバ116-2にコンテンツ、またはデバイスドライバ116-2に所定の処理を実行させるコマンドを供給する。

【0102】

購入用ドライバ141は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム111と共にインストールされ、EMD登録サーバ3からネットワーク2を介して供給され、または所定のCDに記録されて供給される。購入用ドライバ141は、パーソナルコンピュータ1にインストールされたとき、コンテンツ管理プログラム111の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム111とデータを送受信する。

【0103】

購入用ドライバ141は、ネットワーク2を介して、EMDサーバ4-2に所定のコンテンツの送信を要求するとともに、EMDサーバ4-2からコンテンツを受信する。また、購入用ドライバ141は、EMDサーバ4-2からコンテンツを受信するとき、課金の処理を実行する。

【0104】

購入用ドライバ142は、コンテンツ管理プログラム111と共にインストールされるプログラムであり、ネットワーク2を介して、EMDサーバ4-3に所定のコンテンツの送信を要求するとともに、EMDサーバ4-3からコンテンツを受信する。また、購入用ドライバ142は、EMDサーバ4-3からコンテンツを受信するとき、課金の処理を実行する。

10

20

30

40

50

【0105】

表示操作指示プログラム112は、フィルタリングデータファイル181、表示データファイル182、画像ファイル183-1乃至183-K、または履歴データファイル184を基に、ディスプレイ20に所定のウィンドウの画像を表示させ、キーボード18またはマウス19への操作を基に、コンテンツ管理プログラム111にチェックインまたはチェックアウトなどの処理の実行を指示する。

【0106】

フィルタリングデータファイル181は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD21に記録されている。

10

【0107】

表示データファイル182は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツに対応するデータを格納して、HDD21に記録されている。

【0108】

画像ファイル183-1乃至183-Kは、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに対応する画像、または後述するパッケージに対応する画像を格納して、HDD21に記録されている。

【0109】

以下、画像ファイル183-1乃至183-Kを個々に区別する必要がないとき、単に、画像ファイル183と称する。

20

【0110】

履歴データファイル184は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD21に記録されている。

【0111】

表示操作指示プログラム112は、登録の処理のとき、ネットワーク2を介して、EMD登録サーバ3に、予め記憶しているコンテンツ管理プログラム111のIDを送信するとともに、EMD登録サーバ3から認証用鍵およびEMD選択プログラム131を受信して、コンテンツ管理プログラム111に認証用鍵およびEMD選択プログラム131を供給する。

30

【0112】

録音プログラム113は、所定のウィンドウの画像を表示させて、キーボード18またはマウス19への操作を基に、ドライブ22に装着された光ディスク42であるCDからコンテンツの録音時間などのデータを読み出す。

【0113】

録音プログラム113は、CDに記録されているコンテンツの録音時間などを基に、ネットワーク2を介して、WWWサーバ5-1または5-2にCDに対応するデータ（例えば、アルバム名、またはアーティスト名など）またはCDに記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWWサーバ5-1または5-2からCDに対応するデータまたはCDに記録されているコンテンツに対応するデータを受信する。

40

【0114】

録音プログラム113は、受信したCDに対応するデータまたはCDに記録されているコンテンツに対応するデータを、表示操作指示プログラム112に供給する。

【0115】

また、録音の指示が入力されたとき、録音プログラム113は、ドライブ22に装着された光ディスク42であるCDからコンテンツを読み出して、コンテンツ管理プログラム111に出力する。

【0116】

50

コンテンツデータベース114は、コンテンツ管理プログラム111から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル161-1乃至161-Nのいずれかに格納する(HDD21に記録する)。コンテンツデータベース114は、コンテンツファイル161-1乃至161-Nにそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル161-1乃至161-Nにそれぞれ対応する利用条件ファイル162-1乃至162-Nのいずれかに格納する(HDD21に記録する)。

【0117】

コンテンツデータベース114は、コンテンツファイル161-1乃至161-Nまたは利用条件ファイル162-1乃至162-Nをレコードとして記録してもよい。

10

【0118】

例えば、コンテンツファイル161-1に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル162-1に格納されている。コンテンツファイル161-Nに格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル162-Nに格納されている。

【0119】

なお、利用条件ファイル162-1乃至162-Nに記録されているデータは、後述する期限データベースに記録されているデータ、または曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース114は、後述する期限データベースおよび曲データベースを包含して、構成されている。

20

【0120】

以下、コンテンツファイル161-1乃至161-Nを個々に区別する必要がないとき、単に、コンテンツファイル161と称する。以下、利用条件ファイル162-1乃至162-Nを個々に区別する必要がないとき、単に、利用条件ファイル162と称する。

【0121】

購入用アプリケーションプログラム115は、EMD登録サーバ3からネットワーク2を介して供給され、または所定のCDに記録されて供給される。購入用アプリケーションプログラム115は、ネットワーク2を介して、EMDサーバ4-1に所定のコンテンツの送信を要求するとともに、EMDサーバ4-1からコンテンツを受信して、コンテンツ管理プログラム111に供給する。また、購入用アプリケーションプログラム115は、EMDサーバ4-1からコンテンツを受信するとき、課金の処理を実行する。

30

【0122】

次に、表示データファイル82に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル161-1乃至161-Nとの対応付けについて説明する。

【0123】

コンテンツファイル161-1乃至161-Nのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、またはフィルタリングパッケージのいずれかである。

【0124】

オリジナルパッケージは、1以上のコンテンツが属し、EMDサーバ4-1乃至4-3におけるコンテンツの分類(例えば、いわゆるアルバムに対応する)、または一枚のCDに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集(情報の追加、または追加した情報の変更)することができる。

40

【0125】

マイセレクトパッケージは、使用者が任意に選択した1以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1以上のマイセレクトパッケージに同時に属することができる。

50

また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

【 0 1 2 6 】

フィルタリングパッケージには、フィルタリングデータファイル 1 8 1 に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMDサーバ 4 - 1 乃至 4 - 3 または WWWサーバ 5 - 1 若しくは 5 - 2 などからネットワーク 2 を介して供給され、または所定の CD に記録されて供給される。使用者は、フィルタリングデータファイル 1 8 1 に格納されているフィルタリングデータを編集することができる。

【 0 1 2 7 】

フィルタリングデータは、所定のコンテンツを選択する、またはコンテンツに対応する重みを算出する基準となる。例えば、今週の J - P O P (日本のポップス) ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ 1 は、今週の日本のポップス 1 位のコンテンツ乃至今週の日本のポップス 1 0 位のコンテンツを特定することができる。

10

【 0 1 2 8 】

フィルタリングデータファイル 1 8 1 は、例えば、過去 1 月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、または曲名に " 愛 " の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

【 0 1 2 9 】

このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ 2 2 1 (コンテンツ用表示データ 2 2 1 に使用者が設定したデータを含む)、または履歴データ 1 8 4 などと、フィルタリングデータとを対応させて選択される。

20

【 0 1 3 0 】

図 6 は、WWWサーバ 5 - 2 から CD の情報を受信したとき、録音プログラム 1 1 3 がディスプレイ 2 0 に表示させるウィンドウを説明する図である。WWWサーバ 5 - 2 から受信した CD の情報を基に、録音プログラム 1 1 3 は、フィールド 2 0 1 に、例えば、" アシンクロナイズド " などの CD のタイトルを表示する。WWWサーバ 5 - 2 から受信した CD の情報を基に、録音プログラム 1 1 3 は、フィールド 2 0 2 に、例えば、" クワイ " などのアーティスト名を表示する。

30

【 0 1 3 1 】

WWWサーバ 5 - 2 から受信した CD の情報を基に、録音プログラム 1 1 3 は、フィールド 2 0 3 の曲名を表示する部分に、例えば、" ヒート " , " プラネット " , " ブラック " , " ソウル " などの曲名を表示する。同様に、録音プログラム 1 1 3 は、フィールド 2 0 3 のアーティストを表示する部分に、例えば、" クワイ " などのアーティスト名を表示する。

【 0 1 3 2 】

録音プログラム 1 1 3 が所定の CD の情報を受信した後、録音プログラム 1 1 3 は、HDD 2 1 の所定のディレクトリに CD の情報を格納する。

【 0 1 3 3 】

ボタン 2 0 4 などがクリックされて、CD の情報の取得の指示を受けたとき、録音プログラム 1 1 3 は、始めに、HDD 2 1 の所定のディレクトリを検索する。録音プログラム 1 1 3 は、そのディレクトリに CD の情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されている CD の情報を利用するか否かを選択させる。

40

【 0 1 3 4 】

録音プログラム 1 1 3 が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン 2 0 6 がクリックされたとき、録音プログラム 1 1 3 は、ドライブ 2 2 に格納されている CD からコンテンツを読み出して、CD から読み出したコンテンツを CD の情報と共にコンテンツ管理プログラム 1 1 1 に供給する。コンテンツ管理プログラム 1 1 1 の圧縮方式変換プログラム 1 3 4 は、録音プログラム 1 1 3 から供給されたコンテンツを

50

所定の圧縮の方式で圧縮して、暗号化プログラム 1 3 5 は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム 1 3 6 は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

【 0 1 3 5 】

コンテンツ管理プログラム 1 1 1 は、圧縮され、暗号化されたコンテンツを利用条件のデータと共に、コンテンツデータベース 1 1 4 に供給する。

【 0 1 3 6 】

コンテンツデータベース 1 1 4 は、コンテンツ管理プログラム 1 1 1 から受信したコンテンツに対応するコンテンツファイル 1 6 1 および利用条件ファイル 1 6 2 を生成して、コンテンツファイル 1 6 1 にコンテンツを格納するとともに、利用条件ファイル 1 6 2 に利用条件のデータを格納する。

10

【 0 1 3 7 】

コンテンツ管理プログラム 1 1 1 は、コンテンツデータベース 1 1 4 にコンテンツおよびコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム 1 1 3 から受信したCDの情報および利用条件のデータを表示操作指示プログラム 1 1 2 に供給する。

【 0 1 3 8 】

表示操作指示プログラム 1 1 2 は、録音の処理でコンテンツデータベース 1 1 4 に格納されたコンテンツに対応する利用条件のデータおよびCDの情報を基に、オリジナルパッケージ用表示データ 2 0 1 およびコンテンツ用表示データ 2 2 1 を生成する。

【 0 1 3 9 】

20

録音プログラム 1 1 3 が表示させるウィンドウには、更に、CDから読み出したコンテンツをコンテンツデータベース 1 1 4 に記録したとき、自動的に、CDから読み出したコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにチェックアウトさせるか否かの設定を行うボタン 2 0 5 が配置されている。

【 0 1 4 0 】

例えば、ボタン 2 0 5 がクリックされたとき、録音プログラム 1 1 3 は、ポータブルデバイス 6 - 1 乃至 6 - 3 のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかを選択したとき、パーソナルコンピュータ 1 は、選択されたポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに、自動的に、CDから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから "チェックアウトしない" を選択した場合、パーソナルコンピュータ 1 は、CDからコンテンツを記録したとき、チェックアウトしない。

30

【 0 1 4 1 】

次に、図 7 のフローチャートを参照して、録音プログラム 1 1 3 を実行するCPU 1 1 による、ドライブ 2 2 に装着されたCDから再生した音楽データをHDD 2 1 に転送し、コピーする場合の処理について説明する。使用者がキーボード 1 8 またはマウス 1 9 を操作して、インタフェース 1 7 を介してCPU 1 1 に対してドライブ 2 2 に装着されたCD (図示せず) から再生された音楽データをHDD 2 1 に転送、コピーする指令を入力すると、CPU 1 1 は、ステップ S 1 1 において、インタフェース 1 7 を介してディスプレイ 2 0 にコピーする曲を選択するためのGUI (Graphical User Interface) を表示させる。

40

【 0 1 4 2 】

具体的には、例えば、CPU 1 1 は、ドライブ 2 2 に装着されたCDのTOC (Table Of Contents) を読み込み、そのCDに含まれる曲の情報を得て、ディスプレイ 2 0 に表示させる。または、CPU 1 1 は、CDに含まれている各曲毎のISRC (International Standard Recording Code) を読み出し、その曲の情報を得て、ディスプレイ 2 0 に表示させる。あるいはまた、CPU 1 1 は、ネットワーク 2 を介してWWWサーバ 5 - 1 または 5 - 2 にアクセスし、TOCを用いて、そのCDの曲の情報を得て、対応するGUIをディスプレイ 2 0 に表示させる。使用者は、ディスプレイ 2 0 のGUIを利用してキーボード 1 8 またはマウス 1 9 を操作し、コピーする曲を選択する。

【 0 1 4 3 】

50

次に、ステップS 1 2において、CPU 1 1は、HDD 2 1に格納されている期限データベース（図5に示すコンテンツデータベース1 1 4の利用条件ファイル1 6 2 - 1乃至1 6 2 - Nに対応する）をチェックする。この期限データベースチェック処理の詳細は、図8のフローチャートに示されている。

【0 1 4 4】

ステップS 3 1においてCPU 1 1は、アダプタ2 6のCPU 3 2と共働して、期限データベース全体のハッシュ値を計算し、ステップS 3 2において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【0 1 4 5】

なお、期限データベースにデータが何ら記録されていないとき、CPU 1 1は、ハッシュ値を計算しない。

10

【0 1 4 6】

すなわち、HDD 2 1には、期限データベースが形成されており、この期限データベースには、図9に示すように、HDD 2 1に記録されている音楽データ（コンテンツ）を管理する管理情報として、過去に記録されたことのある曲のISRCとコピー日時が対応して記憶されている。この例においては、アイテム1乃至アイテム3の3つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全ての曲のISRCとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS 3 8において、アダプタ2 6のCPU 3 2により計算され、不揮発性メモリ3 4に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、SHA（Secure Hash Algorithm）、MD（Message Digest）5などがある。CPU 1 1は、ステップS 3 1において、CPU 3 2が実行したのと同様にハッシュ値を計算する。そして、ステップS 3 2において、CPU 1 1は、CPU 3 2に、不揮発性メモリ3 4に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップS 3 1で、いま自分自身が計算したハッシュ値とを比較する。

20

【0 1 4 7】

ステップS 3 3において、CPU 1 1は、ステップS 3 1でいま計算したハッシュ値と、不揮発性メモリ3 4に記憶されている前回の期限データベースのハッシュ値とが一致するかどうかを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、CPU 1 1は、ステップS 3 4において、例えば、「期限データベースが改竄されたので、コピーができません」といったメッセージを発生し、インタフェース1 7を介してディスプレイ2 0に出力し、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されている音楽データを再生し、HDD 2 1にコピーする処理が禁止される。

30

【0 1 4 8】

ステップS 3 1で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップS 3 5に進み、CPU 1 1は、ステップS 1 1で指定されたコピーする曲として選択された曲（選択曲）のISRCをCDから取得する。CDにISRCが記録されていない場合、CPU 1 1は、そのCDのTOCのデータを読み出し、そのデータにハッシュ関数を適用するなどして、例えば、5 8ビットなどの適当な長さのデータを得て、これをISRCに代えて用いる。

40

【0 1 4 9】

ステップS 3 6において、CPU 1 1は、ステップS 3 5で取得したISRC（すなわち、選択曲）が期限データベース（図9）に登録されているか否かを判定する。ISRCが期限データベースに登録されていない場合には、その曲はまだHDD 2 1に記録されていないことになるので、ステップS 3 7に進み、CPU 1 1は、その曲のISRCと現在の日時とを期限データベースに登録する。なお、CPU 1 1は、この現在の日時として、CPU 3 2から転送を受けた、アダプタ2 6のRTC 3 5が出力する値を利用する。そして、ステップS 3 8において、CPU 1 1は、その時点における期限データベースのデータを読み出し、アダプタ2 6のCPU 3 2に転送する。CPU 3 2は、転送されてきたデータのハッシュ値を計算し、不揮発性メ

50

メモリ34に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS32において、前回保存しておいたハッシュ値として利用される。

【0150】

次に、ステップS39において、CPU11は、選択曲が期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図7のステップS13において、選択曲が期限データベースに登録されているか否かの判定を行うときに用いられる。

【0151】

ステップS36において、選択曲のISRCが期限データベースに登録されていると判定された場合、その選択曲は、少なくとも一度、HDD21に登録されたことがある曲であるということになる。そこで、この場合、ステップS40に進み、CPU11は、期限データベースに登録されているその選択曲の登録日時より、現在の日時（アダプタ26のRTC35が出力した現在の日時）が48時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に48時間以上経過している場合には、HDD21に、少なくとも一度は記録したことがあるが、既に、その時から48時間以上経過しているため、その曲を再度コピーさせたとしても、それほど実害がないので、この場合には、HDD21へのコピーが許容される。そこで、ステップS41に進み、CPU11は、期限データベースの日時を、過去の登録日時から現在の日時（RTC35の出力する日時）に変更させる。そして、ステップS38に戻り、CPU11は、再び、期限データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させるとともに、ステップS39において、その曲に対して未登録のフラグを設定する。

10

20

【0152】

一方、ステップS40において、現在時刻が登録日時より、まだ48時間以上経過していないと判定された場合、その選択曲のHDD21へのコピーが禁止される。そこで、この場合には、ステップS42に進み、CPU11は、その選択曲に対応して登録済みのフラグを設定する。

【0153】

以上のようにして、期限データベースチェック処理により、選択曲がHDD21に登録されているか否かを表すフラグが設定される。

【0154】

図7に戻り、ステップS13においてCPU11は、選択曲が期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択曲が登録済みである場合には、ステップS14に進み、CPU11は、ディスプレイ20に、例えば、「この曲は一度コピーされてからまだ48時間以上経過していないので、コピーすることができません」のようなメッセージを表示させる。これにより、使用者は、その曲をHDD21にコピーすることができない理由を知ることができる。

30

【0155】

ステップS13において、選択した曲が期限データベースに登録されていないと判定された場合、ステップS15に進み、CPU11は、ドライブ22を制御し、そこに装着されているCDから音楽データを読み出させる。この音楽データには、図10に示すように、所定の位置にウォータマークコードが挿入されている。

40

CPU11は、ステップS16において、音楽データに含まれているウォータマークコードを抽出し、そのウォータマークコードがコピー禁止を表しているか否かをステップS17において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップS18に進み、CPU11は、インタフェース17を介してディスプレイ20に、例えば、「コピーは禁止されています」のようなメッセージを表示させ、コピー処理を終了させる。

【0156】

これに対して、ステップS17において、ウォータマークがコピー禁止を表していないと判定された場合、ステップS19に進み、CPU11は、音楽データを、例えば、ATRAC（Ad

50

aptive Transform Acoustic Coding) 3 (商標) などの方式で、ソフトウェア処理により圧縮させる。ステップ S 2 0 において、CPU 1 1 は、予め設定され、メモリ 1 3 に記憶されている暗号鍵を用いて、例えば、DES (Data Encryption Standard) 方式、FEAL (Fast Encipherment Algorithm) 方式などの暗号化方法により、音楽データを暗号化する。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ 2 6 の CPU 3 2 により発生させた乱数に基づいて生成したものをを用いることもできる。このように、パーソナルコンピュータ 1 だけではなく、それに付随して装着されたハードウェアとしてのアダプタ 2 6 の CPU 3 2 と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

【 0 1 5 7 】

10

次に、ステップ S 2 1 において、CPU 1 1 は、暗号化されたデータを HDD 2 1 に転送し、1 つのファイル (コンテンツファイル 1 6 1 として) としてファイル名を付けて保存させる。あるいはまた、1 つのファイルの一部として、そのファイル名の位置情報 (例えば、先頭からのバイト数) を与えて保存するようにしてもよい。

【 0 1 5 8 】

この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

【 0 1 5 9 】

さらに、ステップ S 2 2 において、CPU 1 1 は、予め定められている RAM 1 3 に記憶されている保存用鍵 (不正な読み出しでは読み出しが困難になるように記憶されている) を使って、上述した DES 方式、FEAL 方式などの方式で、音楽データを暗号化した暗号鍵を暗号化し、HDD 2 1 の曲データベース (図 5 に示すコンテンツデータベース 1 1 4 の利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に対応する) に保存する。

20

【 0 1 6 0 】

ステップ S 2 3 において、CPU 1 1 は、保存したファイルに関する情報、暗号化された暗号鍵、その曲の情報、使用者が GUI を介して入力した曲名の情報の要素を組にして HDD 2 1 の曲データベースに登録する。そして、ステップ S 2 4 において、CPU 1 1 は、CPU 3 2 に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ 3 4 に保存させる。

【 0 1 6 1 】

このようにして、例えば、図 1 1 に示すような曲データベースが、HDD 2 1 上に登録される。この例においては、アイテム 1 乃至アイテム 3 のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件 (開始日時、終了日時、回数制限)、再生回数カウンタ、再生時課金条件、コピー条件 (回数)、コピー回数カウンタ、およびコピー条件 (SCMS) が記録されている。

30

【 0 1 6 2 】

複製されて一定期間が経過すると、再び複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとする、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ 1 が故障して、HDD 2 1 に記録されていたコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、HDD 2 1 に記録することができる。

40

【 0 1 6 3 】

また、例えば、ネットワーク 2 を介して HDD 2 1 に記録されている期限データベースの内容を共有することもできる。

【 0 1 6 4 】

以上においては、ISRC に対応して複製された日時が記憶されている場合を例として説明したが、コンテンツや CD を識別する情報であれば、他のもの (例えば、曲名、アルバム名、それらの組み合わせなど) を利用することもできる。

【 0 1 6 5 】

次に、図 1 2 乃至図 1 4 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1

50

を実行するCPU 1 1およびメインプログラムを実行するCPU 5 3による、HDD 2 1からポータブルデバイス6のフラッシュメモリ6 1（例えば、メモリースティック（商標））に、音楽データを移動する処理について説明する。ステップS 5 1において、CPU 1 1は、曲データベース全体のハッシュ値を計算し、ステップS 5 2で、前回CPU 3 2に計算させ、不揮発性メモリ3 4に保存しておいたハッシュ値と比較する。両者が一致しない場合、CPU 1 1は、ステップS 5 3に進み、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ2 0に表示させた後、処理を終了させる。この場合の処理は、図8のステップS 3 1乃至ステップS 3 4の処理と同様の処理である。この場合においては、HDD 2 1からポータブルデバイス6への音楽データの移動が実行されないことになる。

10

【0166】

次に、ステップS 5 4において、CPU 1 1は、HDD 2 1に形成されている曲データベースから、そこに登録されている曲の情報を読み出し、ディスプレイ2 0に、選択のためのGUIとして表示させる。使用者は、この選択のためのGUIに基づいて、HDD 2 1からポータブルデバイス6へ移動させる曲を、キーボード1 8またはマウス1 9を操作して選択する。次に、ステップS 5 5において、CPU 1 1は、ステップS 5 4で選択された選択曲の再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図15のフローチャートを参照して後述する。

【0167】

次に、ステップS 5 6において、パーソナルコンピュータ1のCPU 1 1とポータブルデバイス6のCPU 5 3との間において、相互認証処理が行われ、通信用鍵が共有される。

20

【0168】

例えば、ポータブルデバイス6のフラッシュメモリ6 1（または、EEPROM 6 8）には、マスター鍵KMが予め記憶されており、パーソナルコンピュータ1のRAM 1 3（または、HDD 2 1の所定のファイル）には、個別鍵KPとIDが予め記憶されているものとする。CPU 5 3は、CPU 1 1から、RAM 1 3に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵KMにハッシュ関数を適用して、RAM 1 3に記憶されているパーソナルコンピュータ1の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1とポータブルデバイス6の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

30

【0169】

あるいはまた、パーソナルコンピュータ1のRAM 1 3にIDとマスター鍵KMPを予め記憶させておくとともに、ポータブルデバイス6のフラッシュメモリ6 1にもポータブルデバイス6のIDとマスター鍵KMMを記憶させておく。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。

そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

【0170】

なお、認証の方法としては、例えば、IOS (International Organization for Standardization) 9 7 9 8 - 2を利用することができる。

40

【0171】

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップS 5 7において、CPU 1 1は、選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データ（例えば、図7のステップS 2 0の処理で暗号化されている）をHDD 2 1から読み出す。ステップS 5 8において、CPU 1 1は、ステップS 5 7で読み出したデジタル音楽データの圧縮符号化方式（ステップS 1 9の処理）、暗号化方式（ステップS 2 0の処理）、フォーマットなどをポータブルデバイス6のものに変換する処理を実行する。

この変換処理の詳細は、図17のフローチャートを参照して後述する。

【0172】

50

ステップS 5 9において、CPU 1 1は、ステップS 5 8で変換した音楽データを、ステップS 5 6の相互認証処理により共有した通信用鍵で暗号化し、ポータブルデバイス6にUSBポート2 3を介して転送する。ステップS 6 0において、ポータブルデバイス6のCPU 5 3は、USBコネクタ5 6を介してこの伝送されてきた音楽データを受信すると、その音楽データを、そのままフラッシュメモリ6 1に記憶させる。

【0 1 7 3】

ステップS 6 1において、CPU 1 1は、さらに、曲データベースに登録されているその選択曲の再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス6が管理している形式に変換する。ステップS 6 2において、CPU 1 1は、さらに選択曲の曲データベース中に登録されているコピー条件中のSCMS情報を、ポータブルデバイス6の管理する形式に変換する。そして、ステップS 6 3において、CPU 1 1は、ステップS 6 1で変換した再生条件と、ステップS 6 2で変換したSCMS情報を、ポータブルデバイス6に転送する。ポータブルデバイス6のCPU 5 3は、転送を受けた再生条件とSCMS情報を、フラッシュメモリ6 1に保存する。

10

【0 1 7 4】

ステップS 6 4において、CPU 1 1はまた、選択曲の曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU 1 1が曲データベース中で扱っている形式のまま、ポータブルデバイス6に転送し、フラッシュメモリ6 1に保存させる。

【0 1 7 5】

ステップS 6 5において、CPU 1 1は、選択曲の暗号化されている暗号鍵を曲データベースから読み出し、ステップS 6 6において、その暗号鍵をRAM 1 3に保存されている保存用鍵で復号し、通信用鍵で暗号化する。そして、通信用鍵で暗号化した暗号鍵を、CPU 1 1は、ポータブルデバイス6に転送する。

20

【0 1 7 6】

ポータブルデバイス6のCPU 5 3は、ステップS 6 7で、パーソナルコンピュータ1から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ6 1に保存する。

【0 1 7 7】

CPU 5 3は、暗号鍵の保存が完了すると、ステップS 6 8において、パーソナルコンピュータ1に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ1のCPU 1 1は、ポータブルデバイス6からこの通知を受けると、ステップS 6 9において、HDD 2 1から、その音楽データのファイルを削除するとともに、曲データベースからその曲の要素の組を削除する。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップS 7 0において、CPU 1 1は、アダプタ2 6のCPU 3 2に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ3 4に保存させる。このハッシュ値が、上述したステップS 5 2において、前回保存しておいたハッシュ値として用いられることになる。

30

【0 1 7 8】

次に、コンテンツ管理プログラム1 1 1を実行するCPU 1 1による、図1 2のステップS 5 5における選択曲の再生条件などのチェック処理について説明する。ステップS 8 1において、CPU 1 1は、曲データベースから、各種の条件を読み出す。CPU 1 1は、ステップS 8 2において、ステップS 8 1で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既に過ぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップS 8 3に進み、CPU 1 1は、例えば、「既にコピー回数がコピー制限回数に達しています」とのようなメッセージをディスプレイ2 0に表示させ、処理を終了させる。ステップS 8 2において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップS 8 4に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ2 6のRTC 3 5より出力されたものが用いられる。これにより、使用者が、パーソナルコ

40

50

ンピュータ 1 の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。CPU 1 1 は、この現在日時を CPU 3 2 から提供を受けて、ステップ S 8 4 の判断を自ら行うか、または、ステップ S 8 1 で、曲データベースから読み出した再生条件アダプタ 2 6 の CPU 3 2 に供給し、CPU 3 2 に、ステップ S 8 4 の判定処理を実行させる。

【 0 1 7 9 】

現在日時が再生終了日時を過ぎている場合、ステップ S 8 5 に進み、CPU 1 1 は、選択曲を HDD 2 1 から消去するとともに、曲データベースから、その選択曲の情報を消去する。ステップ S 8 6 において、CPU 1 1 は、CPU 3 2 に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ 3 4 に保存させる。以後、処理は終了される。従って、この場合、音楽データの移動が実行されない。

10

【 0 1 8 0 】

ステップ S 8 4 において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップ S 8 7 に進み、CPU 1 1 は、その選択曲の再生時課金条件（例えば、再生 1 回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、CPU 1 1 は、ステップ S 8 8 において、ポータブルデバイス 6 と通信し、ポータブルデバイス 6 に課金機能が存在するか否かを判定する。ポータブルデバイス 6 に課金機能が存在しない場合には、選択曲をポータブルデバイス 6 に転送する訳にはいかないので、ステップ S 8 9 において、CPU 1 1 は、例えば、「転送先が課金機能を有しておりません」のようなメッセージをディスプレイ 2 0 に表示させ、音楽データの移動処理を終了させる。

20

【 0 1 8 1 】

ステップ S 8 7 において再生時課金条件が登録されていないと判定された場合、または、ステップ S 8 8 において、ポータブルデバイス 6 に課金機能が存在すると判定された場合、ステップ S 9 0 に進み、CPU 1 1 は、選択曲に関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。

その他の再生条件が登録されている場合には、ステップ S 9 1 に進み、CPU 1 1 は、ポータブルデバイス 6 に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス 6 が、その再生条件を守る機能を有していない場合には、ステップ S 9 2 に進み、CPU 1 1 は、例えば、「転送先の装置が再生条件を守る機能を有しておりません」のようなメッセージをディスプレイ 2 0 に表示させ、処理を終了させる。

30

【 0 1 8 2 】

ステップ S 9 0 において、再生条件が登録されていないと判定された場合、またはステップ S 9 1 において、ポータブルデバイス 6 が再生条件を守る機能を有している判定された場合、再生条件等のチェック処理が終了され、図 1 2 のステップ S 5 6 に戻る。

【 0 1 8 3 】

図 1 6 は、ポータブルデバイス 6 が管理している（守ることが可能な）再生条件の例を表している。この例においては、アイテム 1 乃至アイテム 3 の各曲について、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム 2 についてのみ登録されており、アイテム 1 とアイテム 3 については登録されていない。従って、アイテム 2 の曲が選択曲とされた場合、再生回数の再生条件は守ることが可能であるが、アイテム 1 またはアイテム 3 の曲が選択曲とされた場合、再生回数の条件は守ることができないことになる。

40

【 0 1 8 4 】

次に、図 1 7 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、図 1 2 のステップ S 5 8 におけるフォーマット変換処理の詳細について説明する。ステップ S 1 0 1 において、CPU 1 1 は、HDD 2 1 に記録されている選択曲のフォーマット（再生条件、使用条件、コピー条件など）を調べる。ステップ S 1 0 2 において、CPU 1 1 は、相手先の機器（今の場合、ポータブルデバイス 6 ）に設定することが可能な条件を調べる。すなわち、CPU 1 1 は、ポータブルデバイス 6 の CPU 5 3 に設定可能な条件を問い合わせ、その回答を得る。ステップ S 1 0 3 において CPU 1 1 は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をス

50

ステップS102で調べた条件に基づいて決定する。

【0185】

ステップS104において、CPU11は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップS105に進み、音楽データをポータブルデバイス6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス6が守ることができないので、そのようなポータブルデバイス6には、音楽データを移動することが禁止されるのである。

【0186】

ステップS104において設定可能な条件が存在すると判定された場合、ステップS106に進み、CPU11は、その条件を相手先の機能フォーマットの条件に変換する。そして、ステップS107において、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス6は、設定された条件に従って（その条件を守って）、音楽データ再生することが可能となる。

【0187】

次に、図18乃至図20のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6に音楽データをコピーする場合の処理について説明する。この図18乃至図20のステップS111乃至ステップS127の処理は、図12乃至図14のHDD21からポータブルデバイス6へ音楽データを移動させる場合のステップS51乃至ステップS67の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択曲の再生条件とのチェック処理が行われる。さらに、ポータブルデバイス6と、パーソナルコンピュータ1との間の相互認証処理の後、音楽データが、パーソナルコンピュータ1のHDD21からポータブルデバイス6のフラッシュメモリ61に転送され、保存される。その後、ステップS128において、パーソナルコンピュータ1のCPU11は、曲データベースのコピー回数カウンタを1だけインクリメントする。そして、ステップS129において、CPU11は、CPU32に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ34に保存させる。

【0188】

次に、図21のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、ポータブルデバイス6からHDD21に音楽データを移動する処理について説明する。ステップS161において、パーソナルコンピュータ1のCPU11は、ポータブルデバイス6のCPU53に対してフラッシュメモリ61に記憶されている曲の情報の読み出しを要求する。CPU53は、この要求に対応して、フラッシュメモリ61に記憶されている曲の情報をパーソナルコンピュータ1に送信する。パーソナルコンピュータ1のCPU11は、この情報に基づいて、ディスプレイ20に、フラッシュメモリ61に記憶されている曲を選択するためのGUIを表示させる。使用者は、キーボード18またはマウス19を操作して、そのGUIに基づいて、ポータブルデバイス6からHDD21に移動させる曲を指定する。

【0189】

ステップS162において、CPU11は、CPU53との間において、相互認証処理を実行し、通信用鍵を共有する。この処理は、図12のステップS56における場合と同様の処理である。

【0190】

次に、ステップS163において、CPU53は、フラッシュメモリ61に記憶されている暗号化されている選択曲の音楽データを読み出し、パーソナルコンピュータ1に転送する。パーソナルコンピュータ1のCPU11は、ステップS164において、ポータブルデバイス6から転送されてきた音楽データを、1つのファイルとしてファイル名を付けて、HDD21に保存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

【0191】

ステップS 1 6 5において、CPU 5 3は、フラッシュメモリ 6 1に記憶されている選択曲の暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ 1に転送する。この暗号鍵は、例えば、図 1 4のステップS 6 7の処理でフラッシュメモリ 6 1に保存されていたものである。

【 0 1 9 2 】

ステップS 1 6 6において、パーソナルコンピュータ 1のCPU 1 1は、ポータブルデバイス 6から暗号鍵の転送を受けると、それを通信用鍵で復号し、自分自身の保存用鍵で暗号化する。ステップS 1 6 7で、CPU 1 1は、ステップS 1 6 4で保存した音楽データのファイルのファイル名、その曲の情報を使用者がGUIを介して入力した曲名、ステップS 1 6 6で暗号化した暗号鍵などを、HDD 2 1の曲データベースに登録する。そして、ステップS 1 6 8において、CPU 1 1は、その曲データベース全体のハッシュ値をCPU 3 2に計算させ、不揮発性メモリ 3 4に保存させる。

10

【 0 1 9 3 】

ステップS 1 6 9において、パーソナルコンピュータ 1のCPU 1 1は、ポータブルデバイス 6に対して暗号鍵が保存されたことを通知し、その曲の音楽データの削除を要求する。CPU 5 3は、パーソナルコンピュータ 1から、その曲の音楽データの削除が要求されてきたとき、ステップS 1 7 0において、フラッシュメモリ 6 1に記憶されているその曲の音楽データを削除する。

【 0 1 9 4 】

次に、コンテンツ管理プログラム 1 1 1を実行するCPU 1 1およびメインプログラムを実行するCPU 5 3による、ポータブルデバイス 6からHDD 2 1へ音楽データをコピーする場合の処理について、図 2 2のフローチャートを参照して説明する。この図 2 2に示すステップS 1 8 1乃至ステップS 1 8 8の処理は、図 2 1のポータブルデバイス 6からHDD 2 1へ音楽データを移動させる場合の処理におけるステップS 1 6 1乃至ステップS 1 6 8の処理と同様の処理である。すなわち、コピー処理の場合は、図 2 1のステップS 1 6 9，S 1 7 0の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

20

【 0 1 9 5 】

次に、図 2 3のフローチャートを参照して、EMDサーバ 4およびコンテンツ管理プログラム 1 1 1を実行するCPU 1 1による、EMDサーバ 4から転送を受けた音楽データをHDD 2 1にコピーする処理について説明する。ステップS 2 0 1において、CPU 1 1は、キーボード 1 8またはマウス 1 9を介して使用者からEMDサーバ 4へのアクセスが指令されたとき、通信部 2 5を制御し、ネットワーク 2を介してEMDサーバ 4にアクセスさせる。EMDサーバ 4は、このアクセスに対応して、自分自身が保持している曲の曲番号、曲名、各情報などの情報を、ネットワーク 2を介してパーソナルコンピュータ 1に転送する。パーソナルコンピュータ 1のCPU 1 1は、通信部 2 5を介して、この情報を取得したとき、それをインタフェース 1 7を介してディスプレイ 2 0に表示させる。使用者は、ディスプレイ 2 0に表示されたGUIを利用して、ステップS 2 0 2において、コピーを希望する曲を指定する。この指定情報は、ネットワーク 2を介してEMDサーバ 4に転送される。ステップS 2 0 3において、CPU 1 1は、EMDサーバ 4との間において、ネットワーク 2を介して相互認証処理を実行し、通信用鍵を共有する。

30

40

【 0 1 9 6 】

パーソナルコンピュータ 1とEMDサーバ 4との間で行われる相互認証処理は、例えば、ISO 9 7 9 8 - 3で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ 1は、自分自身の機密鍵とEMDサーバ 4の公開鍵を予め有しており、EMDサーバ 4は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ 1の公開鍵は、EMDサーバ 4から転送したり、あるいはパーソナルコンピュータ 1に予め配布されている証明書 (certificate) をパーソナルコンピュータ 1からEMDサーバ 4に転送し、その証明書をEMDサーバ 4が確認し、公開鍵を得るようにしてもよい。さらに、ステップS 2 0 4において、CPU 1 1は、EMDサーバ 4との間において課金

50

に関する処理を実行する。この課金の処理の詳細は、図24のフローチャートを参照して後述する。

【0197】

次に、ステップS205において、EMDサーバ4は、パーソナルコンピュータ1に対して、ステップS202で指定された曲の暗号化されている音楽データをネットワーク2を介してパーソナルコンピュータ1に転送する。このとき、時刻情報も適宜転送される。ステップS206において、CPU11は、転送を受けた音楽データをファイル名を付けてHDD21に1つのファイルとして保存する。ステップS207において、EMDサーバ4は、さらに、その曲の暗号鍵をステップS203でパーソナルコンピュータ1と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ1へ転送する。

10

【0198】

CPU11は、ステップS208において、EMDサーバ4より転送を受けた暗号鍵を単独で、またはアダプタ26のCPU32と共同して通信用鍵を用いて復号し、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化する。ステップS209において、CPU11は、その曲のファイル名、曲の情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD21の曲データベースに登録する。さらに、ステップS210において、CPU11は、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0199】

なお、ステップS205においてEMDサーバ4は、音楽データとともに、時刻データをパーソナルコンピュータ1に送信する。この時刻データは、パーソナルコンピュータ1からアダプタ26に転送される。アダプタ26のCPU32は、パーソナルコンピュータ1より転送されてきた時刻データを受信すると、ステップS211において、RTC35の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ26のRTC35の時刻情報を修正するようにしたので、アダプタ26を常に正しい時刻情報を保持することが可能となる。

20

【0200】

次に、図24のフローチャートを参照して、EMDサーバ4およびコンテンツ管理プログラム111を実行するCPU11による、図23のステップS204における課金に関する処理の詳細について説明する。ステップS221において、パーソナルコンピュータ1のCPU11は、ステップS201でEMDサーバ4から伝送されてきた価格情報の中から、ステップS202で指定された選択曲の価格情報を読み取り、これをHDD21上の課金ログに書き込む。図25は、このような課金ログの例を表している。この例においては、使用者は、アイテム1乃至アイテム3を、EMDサーバ4からコピーしており、アイテム1とアイテム2の領域は50円とされ、アイテム3の料金は60円とされている。その時点における課金ログのハッシュ値も、CPU32により計算され、不揮発性メモリ34に登録されている。

30

【0201】

次に、ステップS222において、パーソナルコンピュータ1のCPU11は、ステップS221で書き込んだ課金ログをHDD21から読み出し、これをネットワーク2を介してEMDサーバ4に転送する。EMDサーバ4は、ステップS223において、パーソナルコンピュータ1から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMDサーバ4は、内蔵するデータベースに、パーソナルコンピュータ1の使用者から伝送されてきた課金ログを追加更新する。そして、ステップS224において、EMDサーバ4は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップS225に進み、EMDサーバ4は、決裁に必要な商品名、金額などを決裁サーバ(図示せず)に転送する。そして、ステップS226において、決裁サーバは、パーソナルコンピュータ1の使用者に対する決裁処理を実行する。ステップS224において、決裁は直ちには行われないと判定された場合、ステップS225とS226の処理はスキップされる。すなわち、この処理は、例えば、月に1回など、定期的にその後実行される。

40

50

【0202】

次に、図26と図27のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、音声入出力インタフェース24のIEC60958端子から入力された、図示せぬCDプレーヤなどからの再生音楽データを、HDD21にコピーする場合の処理について説明する。ステップS241において、使用者は、CDプレーヤのIEC60958出力端子を、パーソナルコンピュータ1の音声入出力インタフェース24のIEC60958端子に接続する。ステップS242において、使用者は、キーボード18またはマウス19を操作し、CDプレーヤからコピーする曲の曲名（または、曲に対応する番号）を入力する。そして、ステップS243において使用者は、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ1との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ1のキーボード18またはマウス19を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

10

【0203】

CDプレーヤにおいて、CDの再生が開始されると、ステップS244において、CDプレーヤから出力された音楽データが、IEC60958端子を介してパーソナルコンピュータ1に転送されてくる。ステップS245において、CPU11は、IEC60958端子を介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。このSCMSデータには、コピー禁止、コピー1回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップS246において、CPU11は、SCMSデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップS247に進み、CPU11は、ディスプレイ20に、例えば、「コピーが禁止されています」といったメッセージを表示させ、コピー処理を終了する。すなわち、この場合には、HDD21へのコピーが禁止される。

20

【0204】

CPU11は、ステップS246において、ステップS245で読み取ったSCMS情報がコピー禁止を表していないと判定した場合、ステップS248に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップS249において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップS247に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

30

【0205】

ステップS249において、ウォータマークがコピー禁止を表していないと判定された場合、ステップS250に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択曲が既に登録されていれば、ステップS251、S252の処理で、処理が終了される。この処理は、図7のステップS13、S14の処理と同様の処理である。

【0206】

選択曲がまだHDD21に登録されていない曲であれば、ステップS253乃至S258で、その登録処理が実行される。このステップS253乃至ステップS258の処理は、ステップS257において、IEC60958端子から供給されてくるSCMS情報も曲データベースに登録される点を除き、図7のステップS19乃至ステップS24の処理と同様の処理であるので、その説明は省略する。

40

【0207】

次に、図28と図29のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、音楽データをHDD21からIEC60958端子に出力（再生）する場合の処理について説明する。ステップS271乃至ステップS273において、図18のステップS111乃至S113における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された

50

場合、ステップS 2 7 4に進み、CPU 1 1は、HDD 2 1の曲データベースにアクセスし、そこに登録されている曲の情報を読み出し、ディスプレイ 2 0に表示させる。使用者は、その表示を見て、キーボード 1 8またはマウス 1 9を適宜操作して、再生出力する曲を選択する。ステップS 2 7 5において、CPU 1 1は、選択曲の再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図 3 0のフローチャートを参照して後述する。

【 0 2 0 8 】

次に、ステップS 2 7 6において、CPU 1 1は、ステップS 2 7 4において選択された曲の暗号鍵を曲データベースから読み出し、保存用鍵で復号する。ステップS 2 7 7において、CPU 1 1は、選択曲のSCMS情報を曲データベースから読み出し、IEC60958端子から出力するSCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は1だけインクリメントされ、新たなSCMS情報とされる。ステップS 2 7 8において、CPU 1 1はさらに、選択曲のISRCを曲データベースから読み出す。

10

【 0 2 0 9 】

次に、ステップS 2 7 9において、CPU 1 1は、曲データベースから選択曲ファイル名を読み出し、そのファイル名を基に、その音楽データをHDD 2 1から読み出す。CPU 1 1はさらに、その音楽データに対応する暗号鍵を曲データベースから読み出し、保存用鍵で復号し、復号した暗号鍵を用いて、暗号化されている音楽データを復号する。CPU 1 1は、さらに、その音楽データの圧縮符号を復号する。ステップS 2 8 0において、CPU 1 1は、ステップS 2 7 9で、復号したデジタル音楽データを、ステップS 2 7 7で決定したSCMS情報、並びにステップS 2 7 8で読み出したISRC情報とともに、IEC60958の規定に従って、IEC60958端子から出力する。さらにまた、デジタル音楽データをアナログ化し、音声入出力インタフェース 2 4のアナログ出力端子から出力する。

20

【 0 2 1 0 】

ステップS 2 8 1において、CPU 1 1は、曲データベース中の再生回数カウンタの値を1だけインクリメントする。そして、ステップS 2 8 2において、選択曲に再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS 2 8 3に進み、CPU 1 1は、対応する料金を課金ログに書き込み、ステップS 2 8 4において、曲データベース全体のハッシュ値をCPU 3 2に計算させ、不揮発性メモリ 3 4に記憶させる。ステップS 2 8 2において、選択曲に再生時課金条件が付加されていないと判定された場合、ステップS 2 8 3とステップS 2 8 4の処理はスキップされる。

30

【 0 2 1 1 】

次に、図 3 0のフローチャートを参照して、コンテンツ管理プログラム 1 1 1を実行するCPU 1 1による、図 2 8のステップS 2 7 5の再生条件等のチェック処理の詳細について説明する。ステップS 3 0 1において、CPU 1 1は、曲データベースの各種条件を読み出す。ステップS 3 0 2においてCPU 1 1は、読み出した条件のうち、再生回数が制限回数を過ぎていないか否かを判定し、過ぎていない場合には、ステップS 3 0 3に進み、選択曲をHDD 2 1から削除させるとともに、曲データベースから選択曲の情報を削除させる。ステップS 3 0 4において、CPU 1 1はさらに、曲データベースの新たなハッシュ値をCPU 3 2に計算させ、そのハッシュ値を不揮発性メモリ 3 4に保存させる。この場合、再生出力は禁止される。

40

【 0 2 1 2 】

ステップS 3 0 2において、再生回数が制限回数を過ぎていないと判定された場合、ステップS 3 0 5に進み、CPU 1 1は、再生終了日時が現在日時を過ぎていないか否かを判定する。再生終了日時が現在日時を過ぎていない場合には、上述した場合と同様にステップS 3 0 3において、選択曲をHDD 2 1から削除させるとともに、曲データベースからも削除させる。そして、ステップS 3 0 4において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【 0 2 1 3 】

ステップS 3 0 5において、再生終了日時が現在日時を過ぎていないと判定された場合は

50

、ステップS 3 0 6に進み、CPU 3 2は、その選択曲に対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS 3 0 7に進み、CPU 1 1は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ 2 0に表示させる。ステップS 3 0 6において、再生時課金条件が付加されていないと判定された場合、ステップS 3 0 7の処理はスキップされる。

【 0 2 1 4 】

次に、図 3 1と図 3 2のフローチャートを参照して、コンテンツ管理プログラム 1 1 1を実行するCPU 1 1およびメインプログラムを実行するCPU 5 3による、HDD 2 1からポータブルデバイス 6経由で音楽データを出力(再生)する場合の処理について説明する。ステップS 3 2 1乃至ステップS 3 2 5において、曲データベースの改竄チェックと選択曲の指定、並びに選択曲の再生条件等のチェック処理が行われる。その処理は、図 2 8のステップS 2 7 1乃至ステップS 2 7 5の処理と同様の処理であるので、その説明は省略する。

10

【 0 2 1 5 】

ステップS 3 2 6において、ポータブルデバイス 6とパーソナルコンピュータ 1の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップS 3 2 7において、パーソナルコンピュータ 1のCPU 1 1は、ポータブルデバイス 6に対して、これから送る暗号化音声データを再生するように命令する。ステップS 3 2 8において、CPU 1 1は、ステップS 3 2 4で指定された選択曲のファイル名を曲データベースから読み出し、そのファイル名の音楽データをHDD 2 1から読み出す。CPU 1 1は、ステップS 3 2 9において、音楽データの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス 6の方式のものに変換する処理を実行する。そして、ステップS 3 3 0において、CPU 1 1は、ステップS 3 2 9において変換した音楽データを通信用鍵で暗号化し、ポータブルデバイス 6に転送する。

20

【 0 2 1 6 】

ステップS 3 3 1において、ポータブルデバイス 6のCPU 5 3は、ステップS 3 2 7において、パーソナルコンピュータ 1から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップS 3 3 2において、CPU 1 1は、曲データベースの再生回数カウントを1だけインクリメントする。さらに、ステップS 3 3 3において、CPU 1 1は、選択曲に再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップS 3 3 4において、その料金を課金ログに書き込み、ステップS 3 3 5において、CPU 3 2に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択曲に再生時課金条件が付加されていない場合には、ステップS 3 3 4, ステップS 3 3 5の処理はスキップされる。

30

【 0 2 1 7 】

本発明においては、音楽データが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU 1 1を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

【 0 2 1 8 】

さらに、上述したように、CPU 1 1の機能の一部は、ハードウェアとしてのアダプタ 2 6に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

40

【 0 2 1 9 】

例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ 2 6の不揮発性メモリ 3 4に保存される。

すなわち、図 8のステップS 3 2, S 3 3などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ 3 4に記憶されているものとされる。これにより、例えば、HDD 2 1に保存されている音楽データを、他の記録媒体にコピーまたは移動させる前に、HDD 2 1の記録内容をバックアップしておき、HDD 2 1から、そこに保存されている音楽データを他の記録媒体にコピーまたはムーブした

50

後、HDD 2 1 にバックアップしておいたデータを再びリストアするようにすることで、実質的に再現なく、コピーまたはムーブができてしまうようなことが防止される。

【 0 2 2 0 】

例えば、図 3 3 に示すように、HDD 2 1 に曲 A , B が保存されている場合、不揮発性メモリ 3 4 には、曲 A と曲 B の情報に対応するハッシュ値が保存されている。この状態において、HDD 2 1 の記録データを他の記録媒体 2 5 1 にバックアップしたとする。その後、HDD 2 1 に保存されている曲 A と曲 B のうち、曲 A を他の記録媒体 2 5 2 に移動させた場合、その時点において、HDD 2 1 に記録されている曲は、曲 B だけとなるので、不揮発性メモリ 3 4 のハッシュ値も、曲 B に対応するハッシュ値に変更される。

【 0 2 2 1 】

従って、その後、記録媒体 2 5 1 にバックアップしておいた HDD 2 1 の内容を HDD 2 1 にリストアして、HDD 2 1 に、再び曲 A と曲 B を保存させたとしても、不揮発性メモリ 3 4 には、曲 B の情報から演算されたハッシュ値が記憶されており、曲 A と曲 B の情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD 2 1 に記憶されている曲 A と曲 B に基づくハッシュ値が、不揮発性メモリ 3 4 に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD 2 1 に保存されている曲 A と曲 B の利用が制限されてしまうことになる。

【 0 2 2 2 】

さらに、上述したように、アダプタ 2 6 は、RTC 3 5 を内蔵しており、この RTC 3 5 の値は、正しい認証結果が得られた他の装置（例えば、EMD サーバ 4）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ 1 が管理するものではなく、RTC 3 5 が出力するものが利用される。従って、使用者が、パーソナルコンピュータ 1 の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

【 0 2 2 3 】

また、アダプタ 2 6 は、暗号化されて転送されてきたプログラムを ROM 3 6 に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図 3 4 のフローチャートを参照して説明する。

【 0 2 2 4 】

すなわち、パーソナルコンピュータ 1 は、アダプタ 2 6 に対して、所定の処理を実行させたいとき、ステップ S 3 5 1 において、アダプタ 2 6 に実行させるべきプログラムを RAM 1 3 に予め記憶されている暗号鍵を用いて暗号化してアダプタ 2 6 に転送する。アダプタ 2 6 の ROM 3 6 には、パーソナルコンピュータ 1 から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。CPU 3 2 は、この ROM 3 6 に記憶されているプログラムに従って、パーソナルコンピュータ 1 から転送されてきた暗号化されているプログラムをステップ S 3 5 2 において復号する。そして、ステップ S 3 1 3 において、CPU 3 2 は、復号したプログラムを RAM 3 3 に展開し、ステップ S 3 5 4 において、そのプログラムを実行する。

【 0 2 2 5 】

例えば、上述したように、パーソナルコンピュータ 1 の CPU 1 1 は、HDD 2 1 の曲データベースのハッシュ値をアダプタ 2 6 に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ 2 6 の CPU 3 2 に転送する。CPU 3 2 は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ 3 4 に記憶させる。あるいは、そのハッシュ値を、CPU 3 2 は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ 1 の CPU 1 1 に転送する。

【 0 2 2 6 】

図 3 5 は、アダプタ 2 6 の内部のより具体的な構成を表している。アダプタ 2 6 は、半導体 IC として形成される。アダプタ 2 6 は、図 3 に示したインタフェース 3 1、CPU 3 2、R

10

20

30

40

50

AM 3 3、不揮発性メモリ 3 4、RTC 3 5、ROM 3 6 以外に、RAM 3 3 に対する書き込みと読み出しを制御するRAMコントローラ 2 6 1、並びに論理回路 2 6 2 を有している。論理回路 2 6 2 は、例えば、暗号化されている音楽データを解読した後、解読したデータをアダプタ 2 6 から直接出力するような場合の処理のために用いられる。

【 0 2 2 7 】

これらのインタフェース 3 1 乃至ROM 3 6、RAMコントローラ 2 6 1、並びに論理回路 2 6 2 は、半導体IC内に一体的に組み込まれ、外部からは分解できないように構成されている。

【 0 2 2 8 】

水晶振動子 2 7 1 は、アダプタ 2 6 が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路 2 7 2 は、RTC 3 5 を動作させるための発振回路である。バッテリー 2 7 3 は、発振回路 2 7 2、不揮発性メモリ 3 4、およびRTC 3 5 に対してバックアップ用の電力を供給している。アダプタ 2 6 のその他の回路には、パーソナルコンピュータ 1 の電源供給回路 2 8 1 からの電力が供給されている。

【 0 2 2 9 】

不揮発性メモリ 3 4 は、書き込み消去可能なROMで構成することも可能であるが、バッテリー 2 7 3 からのバックアップ電源でバックアップされるRAMで構成する場合には、例えば、図 3 6 に示すように、不揮発性メモリ 3 4 の上に保護アルミニウム層 2 9 1 を形成し、さらに、その保護アルミニウム層 2 9 1 と同一平面上となるように、不揮発性メモリ 3 4 にバッテリー 2 7 3 からの電力を供給する電源パターン 2 9 2 を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ 3 4 を改竄すべく、保護アルミニウム層 2 9 1 を削除しようとする、同一平面上の電源パターン 2 9 2 も削除されてしまい、不揮発性メモリ 3 4 に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【 0 2 3 0 】

さらに、図 3 7 に示すように、不揮発性メモリ 3 4 に対するデータの書き込みまたは読み出しのための配線 3 0 1 - 1 乃至 3 0 1 - 3 は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線 3 0 1 - 3 からデータを読み出すためには、上方の配線 3 0 1 - 1、1 0 1 - 2 を除去しなければならず、複数の配線 3 0 1 - 1、3 0 1 - 2、3 0 1 - 3 から同時にデータを読み取ることができなくなる。さらにまた、この配線 3 0 1 - 1 乃至 3 0 1 - 3 を冗長に形成し、直接プローブすると、その付加容量により、その内容を解析することが困難になるようにすることができる。

【 0 2 3 1 】

以上においては、記録媒体として、ポータブルデバイス 6 を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【 0 2 3 2 】

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

【 0 2 3 3 】

以上のように、本発明によれば、次のような効果を奏することができる。

【 0 2 3 4 】

(1) HDD 2 1 に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でHDD 2 1 に記録するようにしたので、HDD 2 1 に記録されている音楽データをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【 0 2 3 5 】

(2) 所定の曲を 1 回コピーしたとき、一定時間（上記例の場合、4 8 時間）の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布す

10

20

30

40

50

ることを防止することができる。

【0236】

さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【0237】

(3) 外部の装置に音楽データを渡したら、HDD 2 1上の音楽データを消去するようにしたので、HDD 2 1内に元のデジタル音楽データが残らず、その複製を大量に配布することが防止される。

【0238】

(4) HDD 2 1内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD 2 1の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをHDD 2 1にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

10

【0239】

(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【0240】

(6) 外部機器から、パーソナルコンピュータ1に対してデータを渡す前に、パーソナルコンピュータ1のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対して音楽データを渡してしまうようなことが防止される。

20

【0241】

(7) 曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

【0242】

(8) パーソナルコンピュータ1におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ1に外付けされるアダプタ26に負担させるようにしたので、パーソナルコンピュータ1のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

30

【0243】

なお、アダプタ26が実行する処理は、セキュアなプログラムでCPU 1 1が実行するようにしてもよい。この場合において、パーソナルコンピュータ1は、アダプタ26のRTC 3 5が供給する現在時刻に代えて、ネットワーク2に接続されている特定のサーバ(例えば、EMD登録サーバ3)から現在時刻のデータをダウンロードして、その現在時刻を基に、判定の処理を実行する。また、この場合において、パーソナルコンピュータ1は、所定の時間間隔で現在時刻を記憶して、記憶している時刻より以前の時刻が設定されたとき、エラーの表示を行い、時刻の設定を受け付けないようにしてもよい。

【0244】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

40

【0245】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図3に示すように、磁気ディスク41(フロッピーディスクを含む)、光ディスク42(CD-ROM(Compact Disc-Read Only Memory)、DVD(

50

Digital Versatile Disc)を含む)、光磁気ディスク43(MD(Mini-Disc)を含む)、若しくは半導体メモリ44などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM12や、HDD21などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部25などのインタフェースを介して、ローカルエリアネットワークまたはインターネットなどのネットワーク2、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0246】

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

10

【0247】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0248】

【発明の効果】

本発明によれば、ユーザの利益を大きく損なうことなく、大量の複製を実質的に禁止することができるようになる。

【図面の簡単な説明】

【図1】 SCMSおよびCGMSを説明するための図である。

【図2】本発明に係る音声データ管理システムの一実施の形態を示す図である。

20

【図3】パーソナルコンピュータ1の構成を説明する図である。

【図4】ポータブルデバイス6の構成を説明する図である。

【図5】パーソナルコンピュータ1の機能の構成を説明するブロック図である。

【図6】録音プログラム113がディスプレイ20に表示させるウィンドウの例を説明する図である。

【図7】コンパクトディスクからHDD21にコピーする場合の処理を説明するフローチャートである。

【図8】図7のステップS12の期限データベースチェック処理を説明するフローチャートである。

【図9】期限データベースの例を示す図である。

30

【図10】ウォータマークを説明する図である。

【図11】曲データベースの例を示す図である。

【図12】HDD21からポータブルデバイス6へデータを移動する動作を説明するフローチャートである。

【図13】HDD21からポータブルデバイス6へデータを移動する動作を説明するフローチャートである。

【図14】HDD21からポータブルデバイス6へデータを移動する作を説明するフローチャートである。

【図15】図12のステップS55の選択曲の再生条件などのチェック処理を説明するフローチャートである。

40

【図16】ポータブルデバイス6が管理している再生条件を説明する図である。

【図17】図12のステップS58のフォーマット変換処理の詳細を説明するフローチャートである。

【図18】HDD21からポータブルデバイス6へデータをコピーする場合の動作を説明するフローチャートである。

【図19】HDD21からポータブルデバイス6へデータをコピーする場合の動作を説明するフローチャートである。

【図20】HDD21からポータブルデバイス6へデータをコピーする場合の動作を説明するフローチャートである。

【図21】ポータブルデバイス6からHDD21へデータを移動する場合の動作を説明する

50

フローチャートである。

【図 2 2】ポータブルデバイス 6 から HDD 2 1 ヘデータをコピーする場合の動作を説明フローチャートである。

【図 2 3】 EMDサーバ 4 から HDD 2 1 ヘデータをコピーする場合の処理を説明するフローチャートである。

【図 2 4】図 2 3 のステップ S 2 0 4 の課金に関する処理の詳細を説明するフローチャートである。

【図 2 5】課金ログを説明する図である。

【図 2 6】図 3 のパーソナルコンピュータ 1 の IEC60958 端子から HDD 2 1 ヘデータをコピーする 2 合の処理を説明するフローチャートである。

10

【図 2 7】図 3 のパーソナルコンピュータ 1 の IEC60958 端子から HDD 2 1 ヘデータをコピーする場合の処理を説明するフローチャートである。

【図 2 8】 HDD 2 1 から IEC60958 端子にデータを出力する場合の動作を説明するフローチャートである。

【図 2 9】 HDD 2 1 から IEC60958 端子にデータを出力する場合の動作を説明するフローチャートである。

【図 3 0】図 2 8 のステップ S 2 7 5 の再生条件などのチェック処理を説明するフローチャートである。

【図 3 1】 HDD 2 1 からポータブルデバイス 6 経由でデータを出力する場合の動作を説明するフローチャートである。

20

【図 3 2】 HDD 2 1 からポータブルデバイス 6 経由でデータを出力する場合の動作を説明するフローチャートである。

【図 3 3】不揮発性メモリ 3 4 の機能を説明する図である。

【図 3 4】アダプタ 2 6 の動作を説明するフローチャートである。

【図 3 5】アダプタ 2 6 の内部の構成を示す図である。

【図 3 6】不揮発性メモリ 3 4 の内部の構成例を示す図である。

【図 3 7】不揮発性メモリ 3 4 の内部の構成例を示す図である。

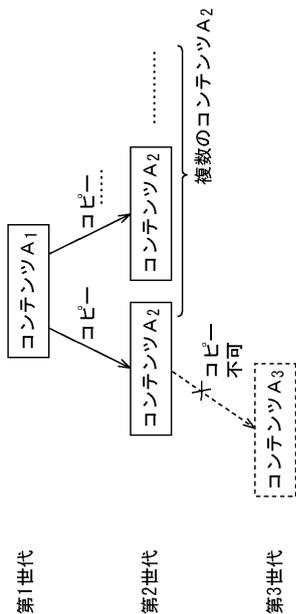
【符号の説明】

1 パーソナルコンピュータ, 2 ネットワーク, 3 EMD登録サーバ, 1 1 CPU, 1 2 ROM, 1 3 RAM, 2 1 HDD, 2 4 音声入出力インターフェース, 2 6 アダプタ, 3 2 CPU, 3 3 RAM, 3 4 不揮発性メモリ, 3 5 RTC, 3 6 ROM, 4 1 磁気ディスク, 4 2 光ディスク, 4 3 光磁気ディスク, 4 4 半導体メモリ, 5 3 CPU, 5 4 RAM, 5 5 ROM, 5 9 DSP, 6 1 フラッシュメモリ, 1 1 1 コンテンツ管理プログラム, 1 1 2 表示操作指示プログラム, 1 1 3 録音プログラム, 1 1 4 コンテンツデータベース, 1 3 1 EMD選択プログラム, 1 3 2 チェックイン/チェックアウト管理プログラム, 1 3 3 暗号方式変換プログラム, 1 3 4 圧縮方式変換プログラム, 1 3 5 暗号化プログラム, 1 3 6 利用条件変換プログラム, 1 3 7 署名管理プログラム, 1 3 8 認証プログラム, 1 3 9 復号プログラム, 1 4 0 PD用ドライバ, 1 4 1 購入用ドライバ, 1 4 2 購入用ドライバ, 1 8 1 フィルタリングデータファイル, 1 8 2 表示データファイル, 1 8 3 画像ファイル, 1 8 4 履歴データファイル

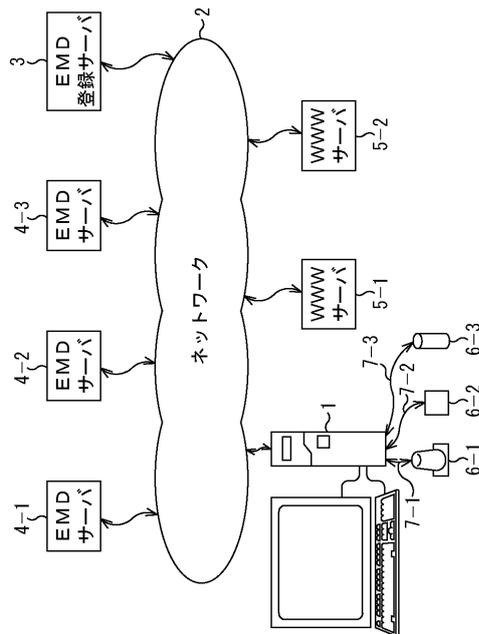
30

40

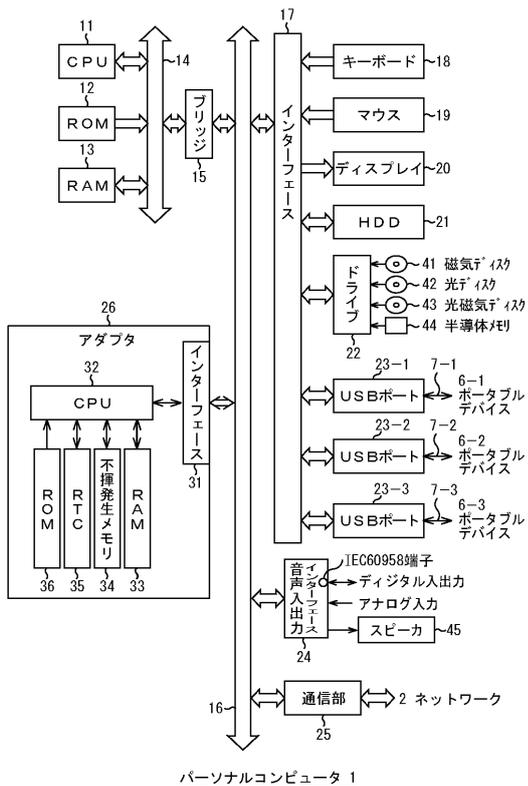
【図1】



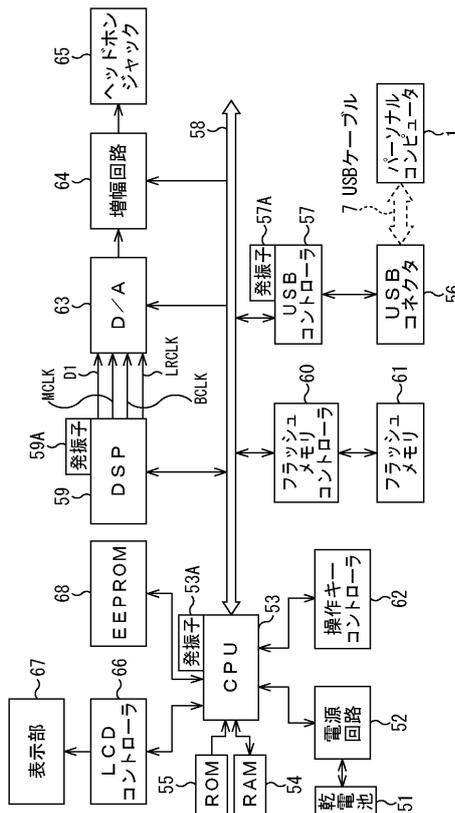
【図2】



【図3】

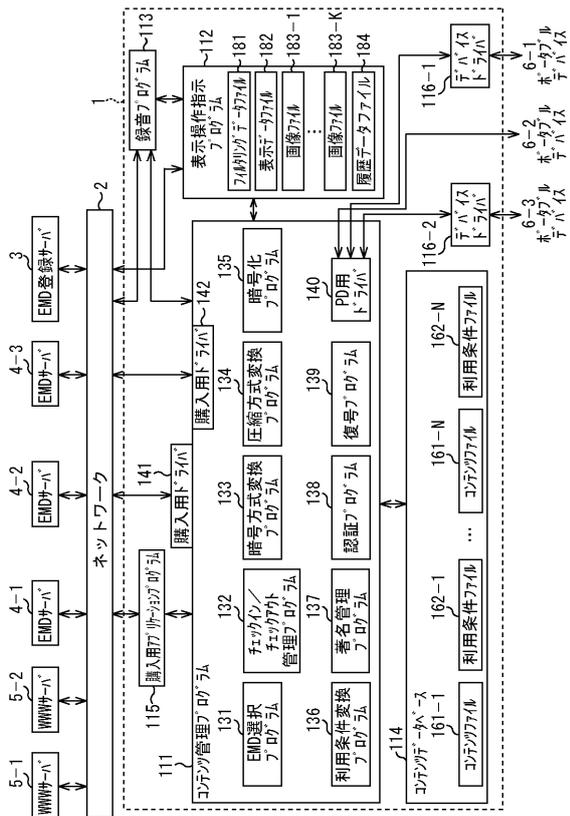


【図4】

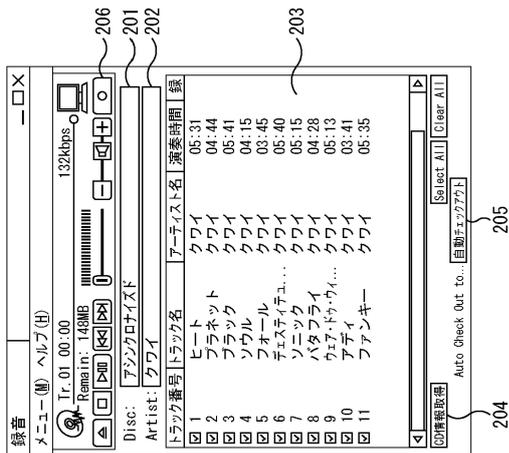


ポータブルデバイス 6

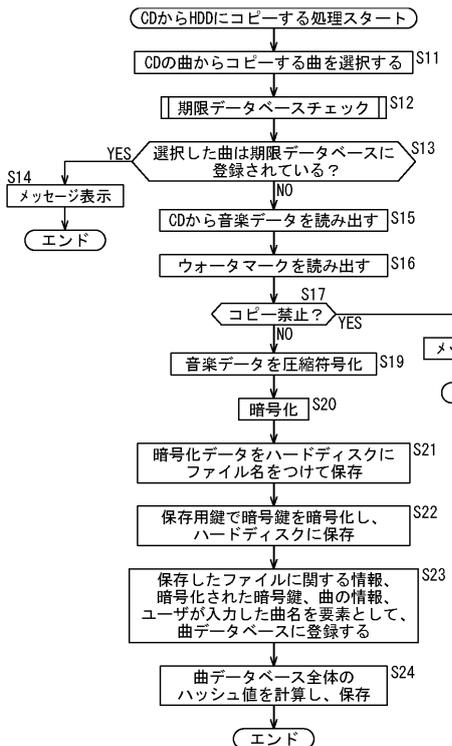
【図5】



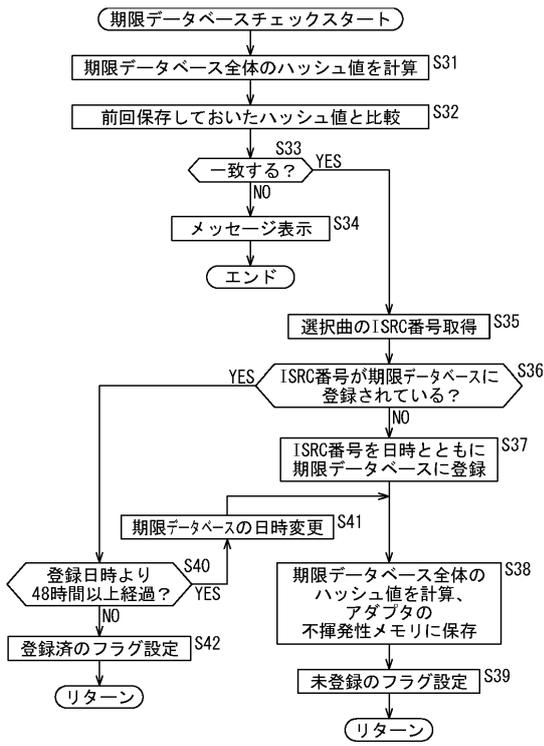
【図6】



【図7】



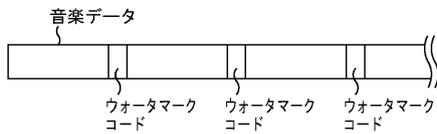
【図8】



【図9】

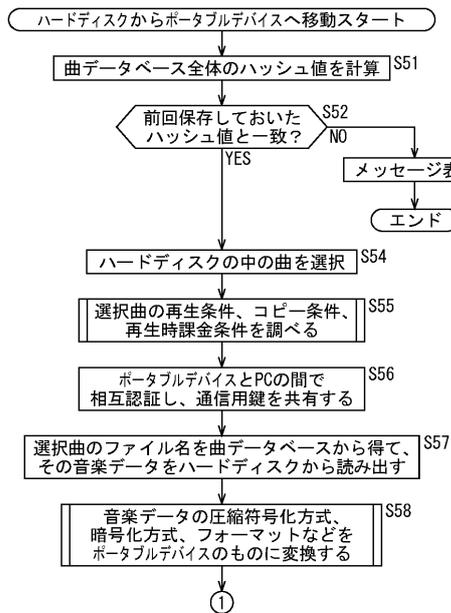
期限データベース		
アイテム1	アイテム2	アイテム3
JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347
1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15
ハッシュ値 0xf3352e125934		

【図10】



【図12】

(12-1)

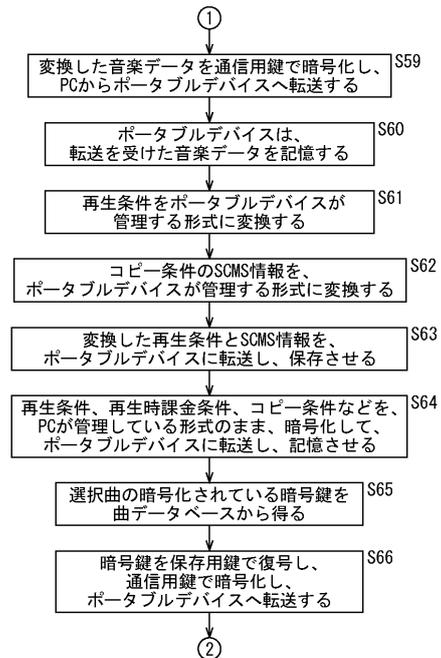


【図11】

曲データベース		
アイテム1	アイテム2	アイテム3
xd000110.at2	px92341234.at2	aa0234287034.at2
0xabababababab	0x9898989898989	0x123456789012
春の小川	運命	荒城の月
180	190	200
-	2001.01.01.00:00	-
1999.07.31.23:59	-	-
-	20	-
-	12	-
-	-	Y5
2	0	0
1	0	0
0b01	0b10	0b00
ハッシュ値 0xf9951e566321		

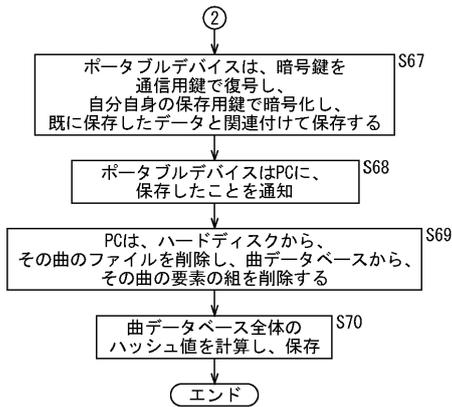
【図13】

(12-2)

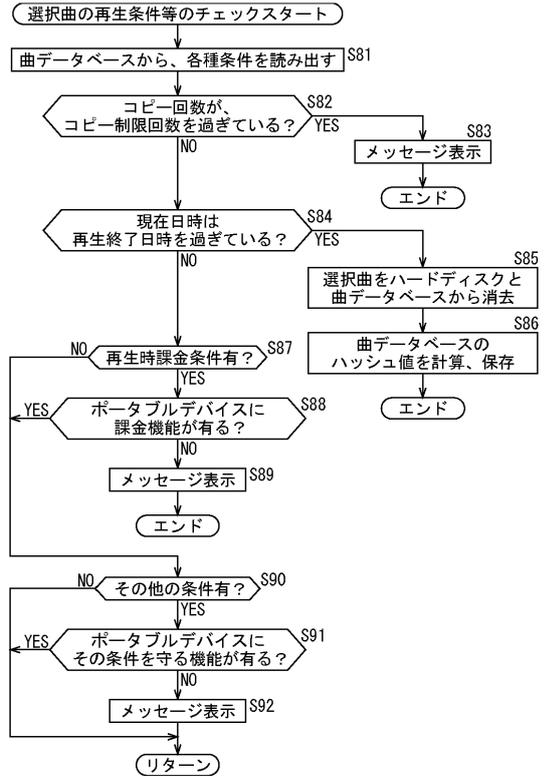


【図14】

(12-3)



【図15】

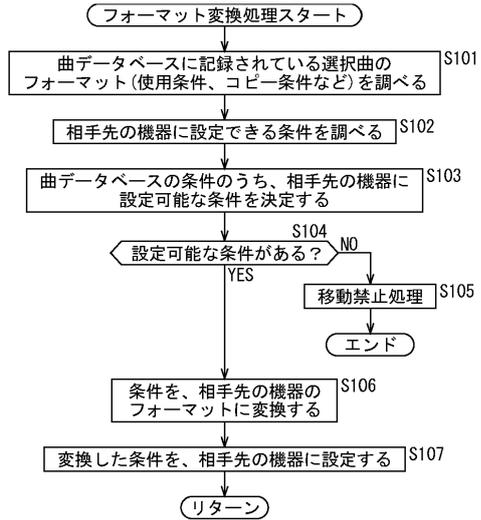


【図16】

ポータブルデバイスが管理している再生条件

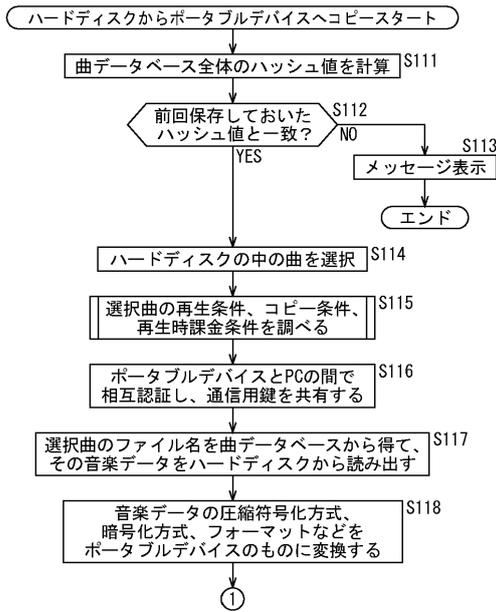
	アイテム1	アイテム2	アイテム3
曲ID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

【図17】



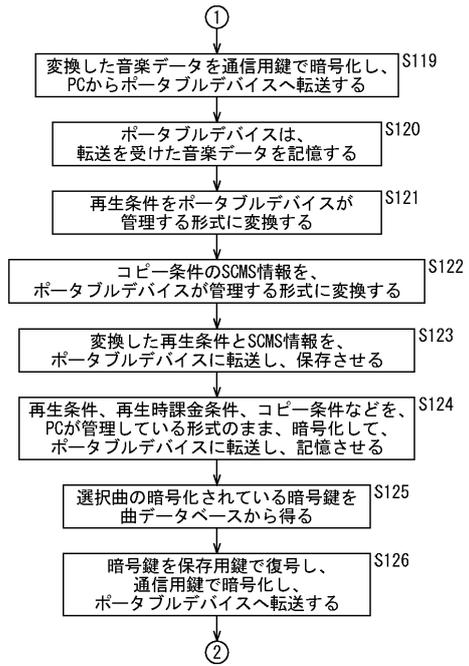
【図18】

(18-1)



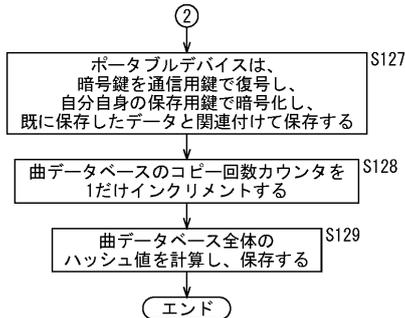
【図19】

(18-2)

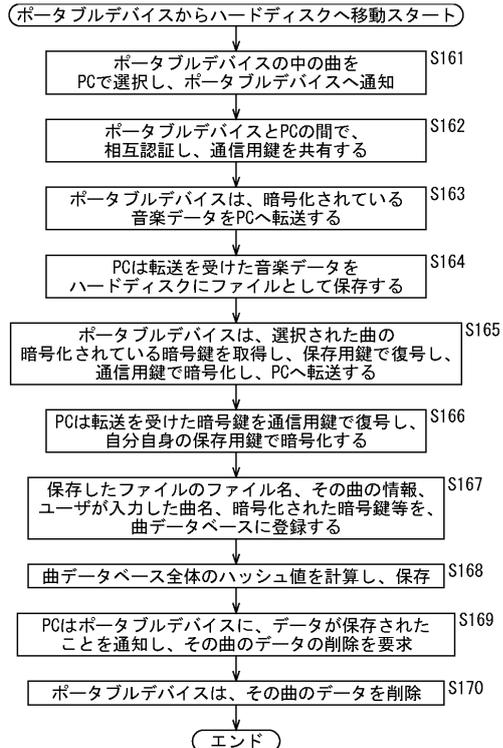


【図20】

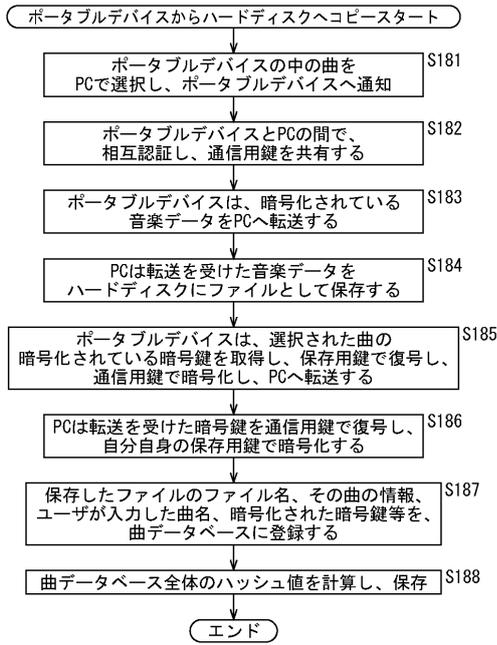
(18-3)



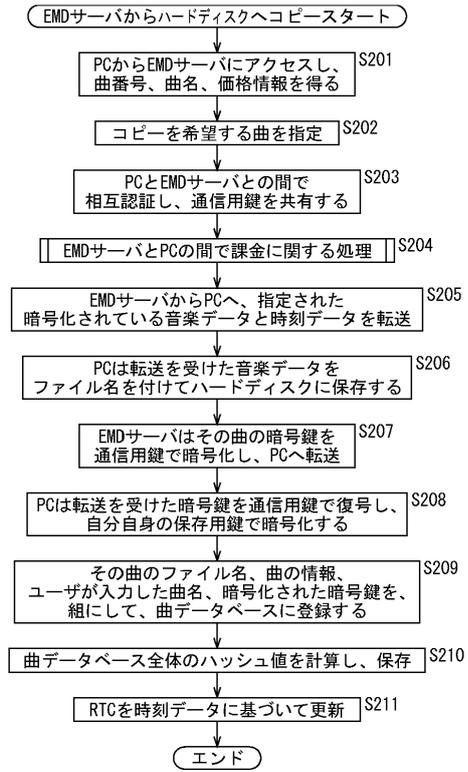
【図21】



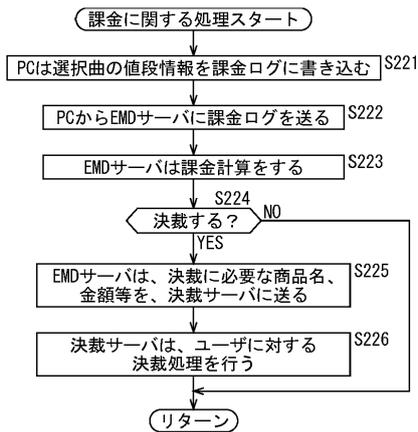
【図 2 2】



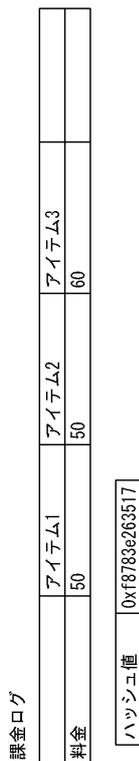
【図 2 3】



【図 2 4】

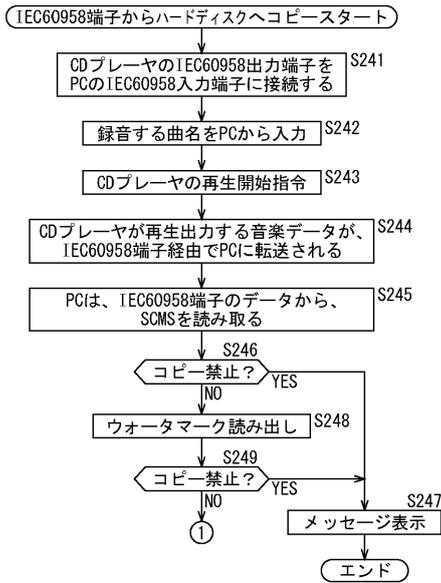


【図 2 5】



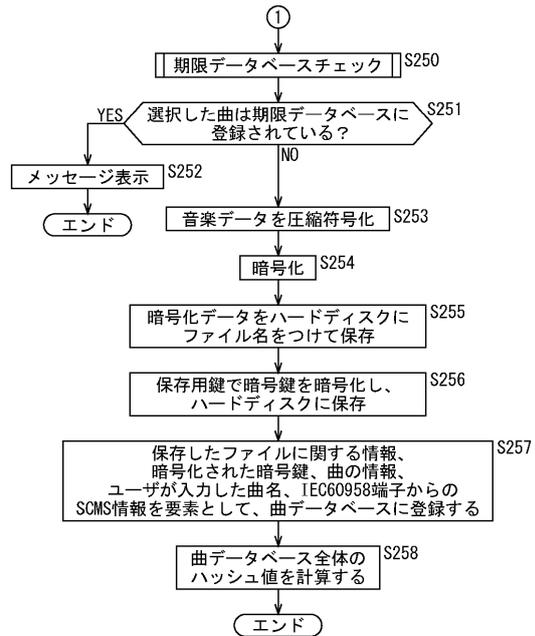
【図 26】

(26-1)



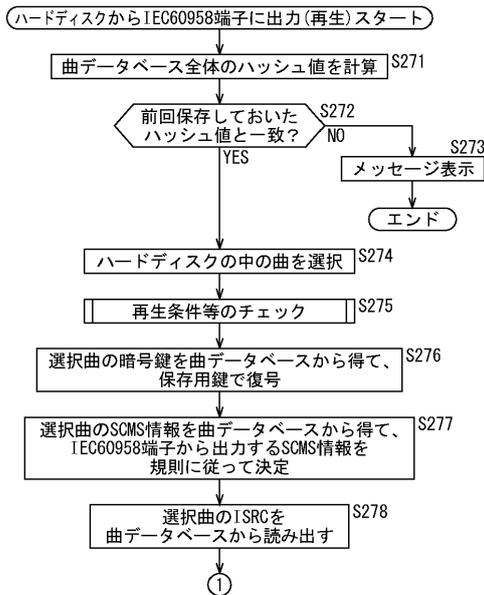
【図 27】

(26-2)



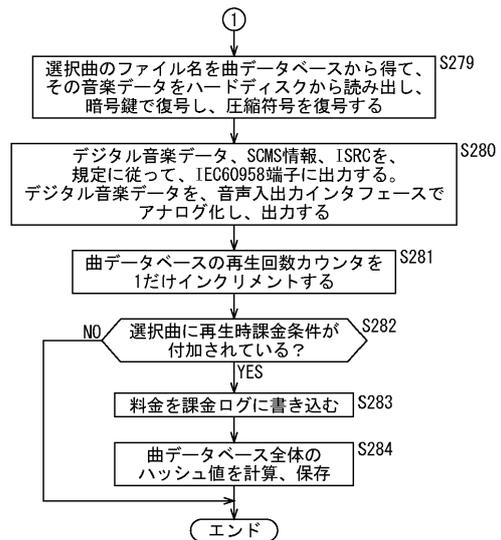
【図 28】

(28-1)

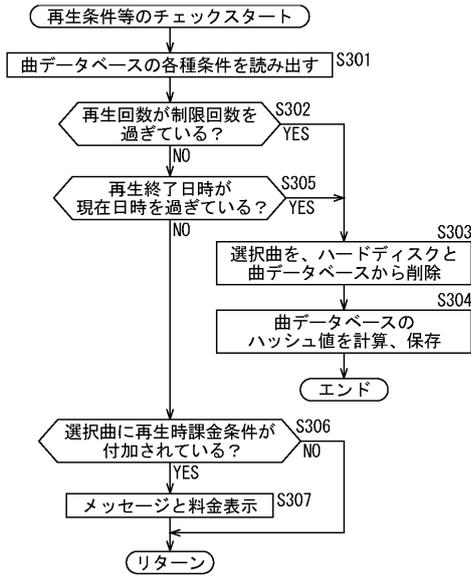


【図 29】

(28-2)

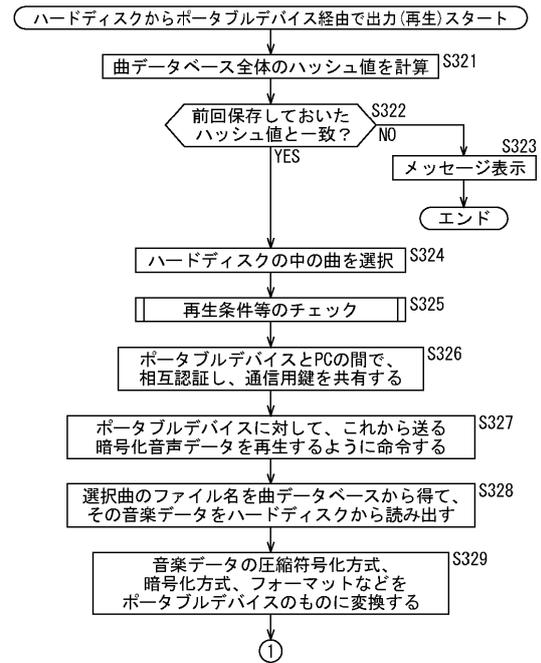


【図30】



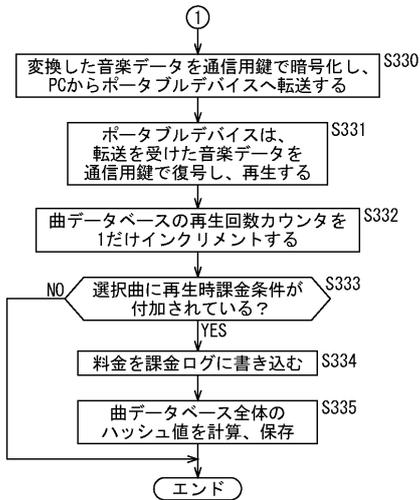
【図31】

(31-1)

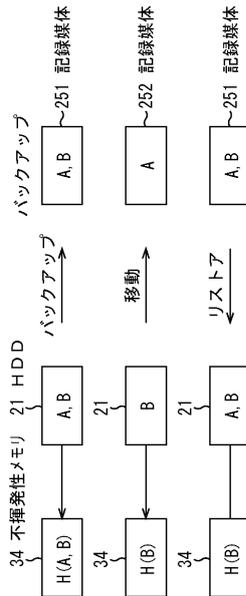


【図32】

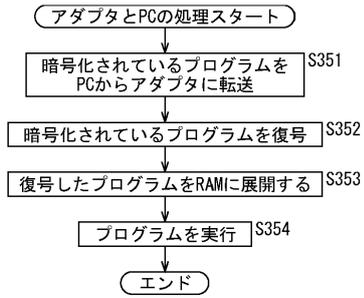
(31-2)



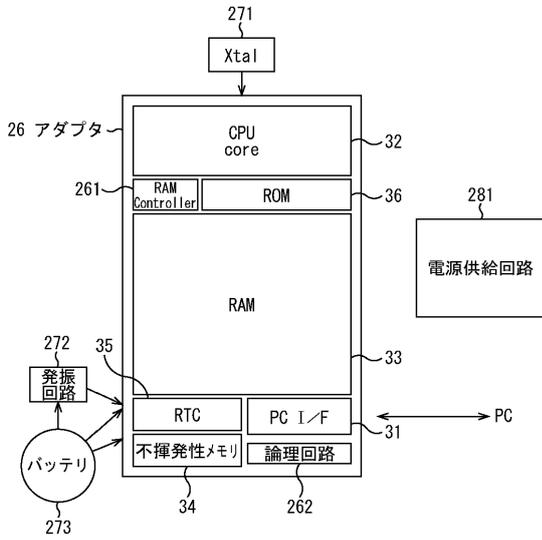
【図33】



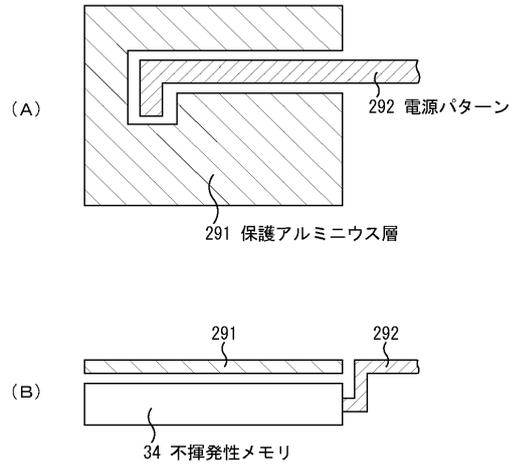
【図34】



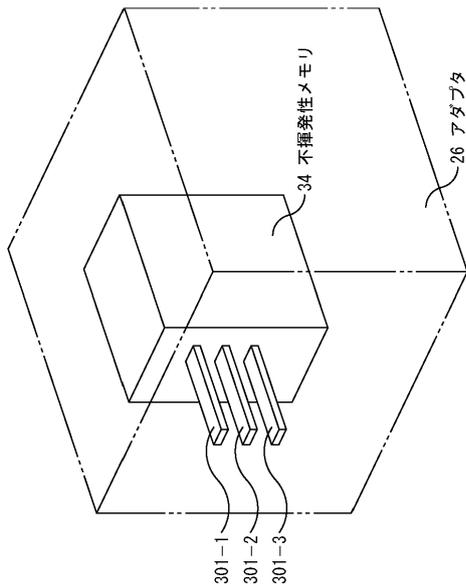
【図35】



【図36】



【図37】



フロントページの続き

(72)発明者 江面 裕一
東京都品川区北品川6丁目7番35号 ソニー株式会社内

審査官 児玉 崇晶

(56)参考文献 特開平07-244900(JP,A)
特開平07-230667(JP,A)
特開平10-003745(JP,A)
特開平10-222931(JP,A)
特開平11-53818(JP,A)
特開2000-207832(JP,A)
特開平7-226733(JP,A)

(58)調査した分野(Int.Cl., DB名)
G06F 21/24