(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4581219号
(P4581219)
(45)発行日　平成22年11月17日(2010.11.17)　(24)登録日　平成22年9月10日(2010.9.10)

(51)Int.Cl.　F I
G06Q 30/00 (2006.01)　G06F 17/60　302E

請求項の数 4　(全 46 頁)

(21)出願番号	特願2000-326125 (P2000-326125)
(22)出願日	平成12年10月25日 (2000.10.25)
(65)公開番号	特開2001-195509 (P2001-195509A)
(43)公開日	平成13年7月19日 (2001.7.19)
審査請求日	平成19年3月28日 (2007.3.28)
(31)優先権主張番号	特願平11-303138
(32)優先日	平成11年10月25日 (1999.10.25)
(33)優先権主張国	日本国(JP)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100067736
弁理士　小池　晃
(74)代理人　100086335
弁理士　田村　榮一
(74)代理人　100096677
弁理士　伊賀　誠司
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　河上　達
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】コンテンツ提供システム、コンテンツ配信方法、記憶媒体及びデータ処理装置

(57)【特許請求の範囲】

【請求項１】

ネットワークを介してコンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、該再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータとコンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するデータ処理装置記憶部と、

上記データ処理装置記憶部に記憶された再生用コンテンツデータを、上記ストレージ鍵と上記コンテンツ鍵とを用いて再生する再生部と、

上記データ処理装置記憶部に記憶された使用ログ情報を上記コンテンツサーバに送信するとともに、上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータを再生できなくなったときには、該データ処理装置のＩＤを上記コンテンツサーバに送信するデータ処理装置通信部とを有するデータ処理装置と、

上記使用ログ情報と、上記データ処理装置のＩＤとを対応付けて記憶するコンテンツサーバ記憶部と、

上記データ処理装置通信部が送信したデータ処理装置のＩＤに対応付いた上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置記憶部に記憶されたストレージ鍵とから、一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値を生成する生成部と、

上記生成部で生成した整合検証値を上記データ処理装置に送信するコンテンツサーバ通信部とを有するコンテンツサーバとを備え、
上記データ処理装置は、
上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータのバックアップデータから復元した再生用コンテンツデータを再生するときには、上記コンテンツサーバ通信部から送信された整合検証値により、該復元した再生用コンテンツデータのＩＤをチェックし、上記再生機器に上記再生用コンテンツデータと上記コンテンツ鍵とが移動されていたときには、該復元した再生用コンテンツデータを再生できないように制御する制御部をさらに有するコンテンツ提供システム。
【請求項２】
データ処理装置の記憶部が、ネットワークを介してコンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、該再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータとコンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するコンテンツデータ記憶ステップと、
上記コンテンツデータ記憶ステップで記憶した使用ログ情報を、データ処理装置の通信部が、上記コンテンツサーバに送信する使用ログ情報送信ステップと、
コンテンツサーバの記憶部が、上記使用ログ情報送信ステップで送信された使用ログ情報と、上記データ処理装置のＩＤとを対応付けて記憶する使用ログ情報記憶ステップと、
データ処理装置の再生部が、上記コンテンツデータ記憶ステップで記憶した再生用コンテンツデータを再生できなくなったときには、上記データ処理装置の通信部が、該データ処理装置のＩＤを上記コンテンツサーバに送信するＩＤ送信ステップと、
コンテンツサーバの生成部が、上記ＩＤ送信ステップで送信されたデータ処理装置のＩＤに対応付いた上記使用ログ情報送信ステップで記憶した上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置の記憶部に記憶されたストレージ鍵とから、一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値を生成する生成ステップと、
コンテンツサーバの通信部が、上記生成ステップで生成した整合検証値を上記データ処理装置に送信する整合検証値送信ステップと、
上記データ処理装置の再生部が、上記再生用コンテンツデータのバックアップデータから復元した再生用コンテンツデータを再生するときに、データ処理装置の制御部が、上記整合検証値送信ステップで送信された整合検証値により、該復元した再生用コンテンツデータのコンテンツＩＤをチェックするチェックステップと、
上記チェックステップにおけるチェックの結果、上記再生機器に上記再生用コンテンツデータと上記コンテンツ鍵とが移動されていたときには、上記データ処理装置の制御部が、上記復元した再生用コンテンツデータを再生できないように制御する制御ステップと
を有するコンテンツ配信方法。
【請求項３】
データ処理装置の記憶部が、ネットワークを介してコンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、該再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータとコンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するコンテンツデータ記憶ステップと、
上記コンテンツデータ記憶ステップで記憶した使用ログ情報を、データ処理装置の通信部が、上記コンテンツサーバに送信する使用ログ情報送信ステップと、
コンテンツサーバの記憶部が、上記使用ログ情報送信ステップで送信された使用ログ情報と、上記データ処理装置のＩＤとを対応付けて記憶する使用ログ情報記憶ステップと、
データ処理装置の再生部が、上記コンテンツデータ記憶ステップで記憶した再生用コン

テンツデータを再生できなくなったときには、上記データ処理装置の通信部が、該データ処理装置のＩＤを上記コンテンツサーバに送信するＩＤ送信ステップと、
コンテンツサーバの生成部が、上記ＩＤ送信ステップで送信されたデータ処理装置のＩＤに対応付いた上記使用ログ情報送信ステップで記憶した上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置の記憶部に記憶されたストレージ鍵とから生成された一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値を生成する生成ステップと、
コンテンツサーバの通信部が、上記生成ステップで生成した整合検証値を上記データ処理装置に送信する整合検証値送信ステップと、
上記データ処理装置の再生部が、上記再生用コンテンツデータのバックアップデータから復元した再生用コンテンツデータを再生するときに、データ処理装置の制御部が、上記整合検証値送信ステップで送信された整合検証値により、該復元した再生用コンテンツデータのコンテンツＩＤをチェックするチェックステップと、
上記チェックステップにおけるチェックの結果、上記再生機器に上記再生用コンテンツデータと上記コンテンツ鍵とが移動されていたときには、上記データ処理装置の制御部が、上記復元した再生用コンテンツデータを再生できないように制御する制御ステップと
を有するコンテンツ配信方法を上記データ処理装置に実行させるためのプログラムが格納された記憶媒体。
【請求項４】
コンテンツサーバとネットワークを介して接続されたデータ処理装置であって、
上記コンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、上記再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータと該コンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するデータ処理装置記憶部と、
上記データ処理装置記憶部に記憶された再生用コンテンツデータを、上記ストレージ鍵と上記コンテンツ鍵とを用いて再生する再生部と、
上記データ処理装置記憶部に記憶された使用ログ情報を上記コンテンツサーバに送信するとともに、上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータを再生できなくなったときには、該データ処理装置のＩＤを上記コンテンツサーバに送信するデータ処理装置通信部と、
上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータから復元した再生用コンテンツデータのバックアップデータを再生するときには、上記コンテンツサーバから送信された上記データ処理装置のＩＤに対応付いた上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置記憶部に記憶されたストレージ鍵とから生成された一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値により、該復元した再生用コンテンツデータのＩＤをチェックし、上記再生機器に上記再生用コンテンツデータ及び上記コンテンツ鍵が移動されていたときには、該復元した再生用コンテンツデータを再生できないように制御する制御部と
を有するデータ処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ネットワークを介して音楽データ等のコンテンツデータを提供するコンテンツ提供システム、コンテンツ配信方法、記憶媒体及びデータ処理装置に関するものである。
【０００２】
【従来の技術】
近年、インターネットやケーブルテレビ等のネットワークを用いた音楽コンテンツのオン

ライン配信が実用化され始めた。
【０００３】
このような音楽コンテンツの配信システムにおいては、コンテンツ配信業者は、音楽コンテンツをネットワークを介して配信する場合、例えば、Ｗｅｂ上に音楽コンテンツを提供する。また、この音楽配信システムを利用するユーザは、自己のパーソナルコンピュータを用いて、コンテンツ配信業者が提供するＷｅｂ等にアクセスをして、所望の音楽コンテンツをダウンロードする。
【０００４】
【発明が解決しようとする課題】
ところで、このような音楽配信システムにおいては、一般に、ダウンロードした音楽コンテンツに対して例えばネットワークを介して課金がされる。
【０００５】
しかしながら、例えば、ユーザが保有するパーソナルコンピュータ内のデータが破壊してしまうと、一旦購入した音楽コンテンツも消滅してしまう。そのため、その音楽コンテンツを復元させるには、再度、コンテンツを購入しなければならなかった。
【０００６】
本発明は、このような実情を鑑みてなされたものであり、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができるコンテンツ提供システム、コンテンツ配信方法、記憶媒体及びデータ処理装置を提供することを目的とする。
【０００７】
【課題を解決するための手段】
本発明にかかるコンテンツ提供システムは、ネットワークを介してコンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、該再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータとコンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するデータ処理装置記憶部と、上記データ処理装置記憶部に記憶された再生用コンテンツデータを、上記ストレージ鍵と上記コンテンツ鍵とを用いて再生する再生部と、上記データ処理装置記憶部に記憶された使用ログ情報を上記コンテンツサーバに送信するとともに、上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータを再生できなくなったときには、該データ処理装置のＩＤを上記コンテンツサーバに送信するデータ処理装置通信部とを有するデータ処理装置と、上記使用ログ情報と、上記データ処理装置のＩＤとを対応付けて記憶するコンテンツサーバ記憶部と、上記データ処理装置通信部が送信したデータ処理装置のＩＤに対応付いた上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置記憶部に記憶されたストレージ鍵とから、一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値を生成する生成部と、上記生成部で生成した整合検証値を上記データ処理装置に送信するコンテンツサーバ通信部とを有するコンテンツサーバとを備え、上記データ処理装置は、上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータのバックアップデータから復元した再生用コンテンツデータを再生するときには、上記コンテンツサーバ通信部から送信された整合検証値により、該復元した再生用コンテンツデータのＩＤをチェックし、上記再生機器に上記再生用コンテンツデータと上記コンテンツ鍵とが移動されていたときには、該復元した再生用コンテンツデータを再生できないように制御する制御部をさらに有する。
【０００８】
コンテンツ提供システムでは、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は制御を行う。
【００１１】
本発明にかかるコンテンツ配信方法は、データ処理装置の記憶部が、ネットワークを介

してコンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、該再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータとコンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するコンテンツデータ記憶ステップと、上記コンテンツデータ記憶ステップで記憶した使用ログ情報を、データ処理装置の通信部が、上記コンテンツサーバに送信する使用ログ情報送信ステップと、コンテンツサーバの記憶部が、上記使用ログ情報送信ステップで送信された使用ログ情報と、上記データ処理装置のＩＤとを対応付けて記憶する使用ログ情報記憶ステップと、データ処理装置の再生部が、上記コンテンツデータ記憶ステップで記憶した再生用コンテンツデータを再生できなくなったときには、上記データ処理装置の通信部が、該データ処理装置のＩＤを上記コンテンツサーバに送信するＩＤ送信ステップと、コンテンツサーバの生成部が、上記ＩＤ送信ステップで送信されたデータ処理装置のＩＤに対応付いた上記使用ログ情報送信ステップで記憶した上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置の記憶部に記憶されたストレージ鍵とから、一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値を生成する生成ステップと、コンテンツサーバの通信部が、上記生成ステップで生成した整合検証値を上記データ処理装置に送信する整合検証値送信ステップと、上記データ処理装置の再生部が、上記再生用コンテンツデータのバックアップデータから復元した再生用コンテンツデータを再生するときに、データ処理装置の制御部が、上記整合検証値送信ステップで送信された整合検証値により、該復元した再生用コンテンツデータのコンテンツＩＤをチェックするチェックステップと、上記チェックステップにおけるチェックの結果、上記再生機器に上記再生用コンテンツデータと上記コンテンツ鍵とが移動されていたときには、上記データ処理装置の制御部が、上記復元した再生用コンテンツデータを再生できないように制御する制御ステップとを有する。

【００１２】

このコンテンツ配信方法では、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は制御を行う。

【００１５】

本発明にかかる記憶媒体は、データ処理装置の記憶部が、ネットワークを介してコンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、該再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータとコンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するコンテンツデータ記憶ステップと、上記コンテンツデータ記憶ステップで記憶した使用ログ情報を、データ処理装置の通信部が、上記コンテンツサーバに送信する使用ログ情報送信ステップと、コンテンツサーバの記憶部が、上記使用ログ情報送信ステップで送信された使用ログ情報と、上記データ処理装置のＩＤとを対応付けて記憶する使用ログ情報記憶ステップと、データ処理装置の再生部が、上記コンテンツデータ記憶ステップで記憶した再生用コンテンツデータを再生できなくなったときには、上記データ処理装置の通信部が、該データ処理装置のＩＤを上記コンテンツサーバに送信するＩＤ送信ステップと、コンテンツサーバの生成部が、上記ＩＤ送信ステップで送信されたデータ処理装置のＩＤに対応付いた上記使用ログ情報送信ステップで記憶した上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置の記憶部に記憶されたストレージ鍵とから生成された一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値を生成する生成ステップと、コンテンツサーバの通信部が、上記生成ステップで生成した整合検証値を上記データ処理装置に送信する整合検証値送信ステップと、上記データ処理装置の再生部が、上記再生用コンテンツデータのバックアップデータから復元した再生用コンテンツデータを再生するときに、データ処理装置の制御部が、上記整合検証値送信ステップで送信された整合検証値により、

該復元した再生用コンテンツデータのコンテンツＩＤをチェックするチェックステップと、上記チェックステップにおけるチェックの結果、上記再生機器に上記再生用コンテンツデータと上記コンテンツ鍵とが移動されていたときには、上記データ処理装置の制御部が、上記復元した再生用コンテンツデータを再生できないように制御する制御ステップとを有するコンテンツ配信方法を上記データ処理装置に実行させるためのプログラムが格納されている。

【００１６】

この記憶媒体では、再生制御プログラムがインストールされたデータ処理装置に対して、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は制御を行わせる。

【００１８】

本発明にかかるデータ処理装置は、コンテンツサーバとネットワークを介して接続されたデータ処理装置であって、上記コンテンツサーバから送信されたコンテンツデータが、ストレージ鍵により暗号化されているコンテンツ鍵で暗号化された再生用コンテンツデータと、該コンテンツ鍵と、該ストレージ鍵と、該再生用コンテンツデータ及び該コンテンツ鍵のバックアップデータと、上記再生用コンテンツデータのＩＤのリストを含み、該再生用コンテンツデータと該コンテンツ鍵とが再生機器に移動されたときに更新される使用ログ情報とを記憶するデータ処理装置記憶部と、上記データ処理装置記憶部に記憶された再生用コンテンツデータを、上記ストレージ鍵と上記コンテンツ鍵とを用いて再生する再生部と、上記データ処理装置記憶部に記憶された使用ログ情報を上記コンテンツサーバに送信するとともに、上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータを再生できなくなったときには、該データ処理装置のＩＤを上記コンテンツサーバに送信するデータ処理装置通信部と、上記再生部が、上記データ処理装置記憶部に記憶された再生用コンテンツデータから復元した再生用コンテンツデータのバックアップデータを再生するときには、上記コンテンツサーバから送信された上記データ処理装置のＩＤに対応付いた上記使用ログ情報のコンテンツＩＤのリストと、上記データ処理装置記憶部に記憶されたストレージ鍵とから生成された一方向ハッシュ関数であって該ストレージ鍵により値が変化する整合検証値により、該復元した再生用コンテンツデータのＩＤをチェックし、上記再生機器に上記再生用コンテンツデータ及び上記コンテンツ鍵が移動されていたときには、該復元した再生用コンテンツデータを再生できないように制御する制御部とを有する。

【００１９】

【発明の実施の形態】

以下、本発明の最良の実施の形態として、本発明を適用した音楽コンテンツ配信システムについて図面を参照しながら詳細に説明する。この音楽コンテンツ配信システムは、ネットワークを介してサーバからパーソナルコンピュータやポータブルデバイスにダウンロードし、さらに、ダウンロードした音楽コンテンツやＣＤから読みとった音楽コンテンツの管理等を行うシステムである。

【００２０】

（１）音楽コンテンツ配信システムの全体構成

図１は、本発明を適用した音楽コンテンツ配信システムの全体構成を示す図である。

【００２１】

この音楽コンテンツ配信システムは、パーソナルコンピュータ１と、インターネットやローカルエリアネットワーク等のネットワーク２と、登録サーバ３と、音楽データ（以下、コンテンツと呼ぶ。）を配信する複数のＥＭＤ（ Electrical Music Distribution ）サーバ４（４－１，４－２，４－３）と、ＷＷＷサーバ５（５－１，５－２）とを備えて構成される。また、パーソナルコンピュータ１には、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、内部にメモリーカード等の記憶媒体が格納され、コンテンツの再生を行う携帯型の音楽再生器機であるポータブルデバイス６（６－１，６－２，６－３）が接続される。

【００２２】
パーソナルコンピュータ１は、ネットワーク２を介して、ＥＭＤ登録サーバ３、ＥＭＤサーバ４（４－１，４－２，４－３）、ＷＷＷ（ World Wide Web ）サーバ５（５－１，５－２）と接続される。
【００２３】
パーソナルコンピュータ１は、ＥＭＤサーバ４（４－１，４－２，４－３）から、所定の圧縮方式で圧縮されたコンテンツを受信し、所定の暗号化方式で暗号化して記録する。また、パーソナルコンピュータ１は、ＣＤ（ Compact Disc ）等から読みとったコンテンツを、所定の圧縮方式で圧縮して、所定の暗号化方式で暗号化して記録する。圧縮方式としては、例えばＡＴＲＡＣ（ Adaptive Transform Acoustic Coding ）３（商標）やＭＰ３（ MPEG Audio Layer -3）等の方式が用いられる。また、暗号化方式としては、ＤＥＳ（ Data Encryption Standard）などが用いられる。
【００２４】
また、パーソナルコンピュータ１は、コンテンツの配信を受ける場合には、そのコンテンツの利用条件を示す利用条件情報の配信も受け、それを記録する。また、パーソナルコンピュータ１は、ＣＤ等から読みとったコンテンツを記録する場合には、そのコンテンツの再生条件に応じて、利用条件情報を生成して、それを記録する。
【００２５】
また、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、利用条件情報及び曲名や演奏者等の関連情報とともに、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、ポータブルデバイス６（６－１，６－２，６－３）に記録し、記憶させたことに対応して利用条件情報を更新する。この処理のことをチェックアウトという。利用条件情報は、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、そのコンテンツのチェックアウト可能回数を１減少させる。チェックアウト可能回数が０のときには、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。
【００２６】
また、パーソナルコンピュータ１は、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、ポータブルデバイス６（６－１，６－２，６－３）に記憶されているコンテンツを、消去し（または、使用できなくさせ）、消去したことに対応させて利用条件情報を更新する。この消去処理のことをチェックインと呼ぶ。
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、そのコンテンツのチェックアウト可能回数を１増加させる。
【００２７】
なお、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にチェックアウトしたコンテンツに対してはチェックインはできない。すなわち、パーソナルコンピュータ１自身がチェックアウトしたコンテンツしか、チェックインをすることができない。
【００２８】
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（４－１，４－２，４－３）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（４－１，４－２，４－３）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（４－１，４－２，４－３）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。
【００２９】
ＥＭＤサーバ４（４－１，４－２，４－３）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、利用条件情報及びコンテンツの関連データ（例えば、曲名、又は演奏者など）とともに、パーソナルコンピュータ１にコンテンツを供給する。
【００３０】
各ＥＭＤサーバ４（４－１，４－２，４－３）が配信するコンテンツは、所定の圧縮の方

式で圧縮されている。その圧縮方式は、サーバ毎に異なっていてもよい。また、各ＥＭＤサーバ４（４－１，４－２，４－３）が供給するコンテンツは、所定の暗号化方式で暗号化されて配信される。その暗号化方式は、サーバ毎に異なっていてもよい。

【００３１】

ＷＷＷサーバ５（５－１，５－２）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（例えば、ＣＤのアルバム名、又はＣＤの販売会社など）及び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、又は作曲者名など）をパーソナルコンピュータ１に供給する。

【００３２】

ポータブルデバイス６（６－１，６－２，６－３）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（すなわち、チェックアウトされたコンテンツ）を再生し、図示せぬヘッドフォンなどに出力する装置である。

【００３３】

各ポータブルデバイス６（６－１，６－２，６－３）は、コンテンツを記憶するための記憶媒体を有している。記憶媒体としては、例えば、装置の内部基板に装着された取り外しが不可能なＩＣメモリや、着脱が可能なメモリカード等が用いられる。ポータブルデバイス６（６－１，６－２，６－３）は、ＵＳＢ等の物理的なインターフェース７（７－１，７－２，７－３）を介してパーソナルコンピュータ１と接続され、コンテンツが転送される。このとき、コンテンツは、暗号化及び圧縮された状態で転送され、利用条件情報も付加されている。

【００３４】

各ポータブルデバイス６（６－１，６－２，６－３）は、通常、パーソナルコンピュータ１との接続が切り離された状態で用いられ、この状態でユーザにより再生命令が与えられると、暗号化したコンテンツを記憶媒体から読み出し、再生をする。また、各ポータブルデバイス６（６－１，６－２，６－３）は、各コンテンツに付加されている利用条件情報に基づき、また、必要に応じて再生の制限を行ったり、コンテンツの削除等の制御を行ったり、利用条件情報の更新等を行う。

【００３５】

以下、ポータブルデバイス６－１，６－２，６－３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。

【００３６】

つぎに、図２を参照して、パーソナルコンピュータ１の構成について説明をする。

【００３７】

ＣＰＵ（ Central Processing 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 ）を実際に実行する。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。

【００３８】

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。

【００３９】

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、液晶表示装置又は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又は再生させる。

【００４０】
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、又は半導体メモリ４４に記録されているデータ又はプログラムを読み出して、そのデータ又はプログラムを、インターフェース１７、外部バス１６、ブリッジ１５及びホストバス１４を介して接続されているＲＡＭ１３に供給する。
【００４１】
ＵＳＢポート２３（２３－１，２３－２，２３－３）には、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、ポータブルデバイス６（６－１，６－２，６－３）が接続される。ＵＳＢポート２３は、インターフェース１７、外部バス１６、ブリッジ１５、又はホストバス１４を介して、ＨＤＤ２１、ＣＰＵ１１、又はＲＡＭ１３から供給されたデータ（例えば、コンテンツ又はポータブルデバイス６のコマンドなどを含む）をポータブルデバイス６（６－１，６－２，６－３）に出力する。
【００４２】
ＩＥＣ（Internationl Electrotechnical Commission）６０９５８端子２４ａ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。
【００４３】
これらのキーボード１８、マウス１９、ディスプレイ２０、ＨＤＤ２１、ドライブ２２、ＵＳＢポート２３、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及びホストバス１４を介してＣＰＵ１１に接続されている。
【００４４】
通信部２５は、ネットワーク２が接続され、ＣＰＵ１１、又はＨＤＤ２１から供給されたデータ（例えば、登録の要求、又はコンテンツの送信要求など）を、所定の方式のパケットに格納して、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、受信したパケットに格納されているデータ（例えば、認証鍵、又はコンテンツなど）をＣＰＵ１１、ＲＡＭ１３、又はＨＤＤ２１に出力する。
【００４５】
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２６のＣＰＵ３２は、外部バス１６、ブリッジ１５及びホストバス１４を介してパーソナルコンピュータ１のＣＰＵ１１と共働し、各種の処理を実行する。ＲＡＭ３３は、ＣＰＵ３２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３４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。ＲＯＭ３６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）３５は、計時動作を実行し、時刻情報を提供する。半導体ＩＣは、セキュアな環境に設計されており、外部からの悪意なアクセスに対して耐性をもっている。なお、この機能は、ソフトウェアプログラムで構成されていてもよい。
【００４６】
通信部２５及びアダプタ２６は、外部バス１６、ブリッジ１５及びホストバス１４を介してＣＰＵ１１に接続されている。
【００４７】
次に、図３を参照して、ポータブルデバイス６の構成を説明する。
【００４８】
電源回路５２は、乾電池５１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、ＣＰＵ５３～表示部６７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。
【００４９】
ＵＳＢコントローラ５７は、ＵＳＢコネクタ５６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含むデータを、内部バス５８を介して、ＣＰＵ５３に供給する。

【００５０】

パーソナルコンピュータ１から転送されるデータは、１パケット当たり６４バイトのデータから構成され、１２Ｍｂｉｔ／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。

【００５１】

ポータブルデバイス６に転送されるデータは、ヘッダ及びコンテンツから構成される。ヘッダには、コンテンツＩＤ、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ともに、再生制限処理等に必要な利用条件情報等が格納されている。コンテンツは、ＡＴＲＡＣ３などの符号化方式で符号化され、暗号化されている。

【００５２】

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、コンテンツのデータ長（例えば、３３，６３６，１３８バイトなど）を表す。

【００５３】

コンテンツ鍵は、暗号化されているコンテンツ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。

【００５４】

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２３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。

【００５５】

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。

【００５６】

コンテンツＩＤは、コンテンツに対応した、コンテンツを特定するためのＩＤである。

【００５７】

コーデックＩＤは、コンテンツ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。

【００５８】

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、又は作曲者名などをＡＳＣＩＩコードに変換したデータである。

【００５９】

ポータブルデバイス６が、パーソナルコンピュータ１からコンテンツとともにコンテンツの書き込み命令を受信した場合、ＲＡＭ５４又はＲＯＭ５５から読み出したメインプログ

ラムを実行するＣＰＵ５３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６０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６１に書き込ませる。

【００６０】

フラッシュメモリ６１は、約６４ＭＢｙｔｅの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ６１には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

【００６１】

なお、フラッシュメモリ６１は、ポータブルデバイス６にメモリカードとして着脱可能とすることができるようにしてもよい。

【００６２】

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６２を介してＣＰＵ５３に供給されると、ＣＰＵ５３は、フラッシュメモリコントローラ６０に、フラッシュメモリ６１から、再生用コードとコンテンツとを読み出させ、ＤＳＰ５９に転送させる。

【００６３】

ＤＳＰ５９は、フラッシュメモリ６１から転送された再生用コードに基づいてコンテンツを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３中においてＤ１で示す）をディジタル／アナログ変換回路６３に供給する。

【００６４】

ＤＳＰ５９は、内部に設けられた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５９ＡからのマスタークロックＭＣＬＫを基に、コンテンツ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ビットクロックＢＣＬＫ、並びに、フレーム単位のＬチャンネルクロックＬＣＬＫ及びＲチャンネルクロックＲＣＬＫからなる動作クロックＬＲＣＬＫをディジタルアナログ変換回路６３に供給する。

【００６５】

ＤＳＰ５９は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをディジタルアナログ変換回路６３に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、ディジタルアナログ変換回路６３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。

【００６６】

同様に、ＣＰＵ５３及びＵＳＢコントローラ５７も、水晶でなる発振子５３Ａ又は５７Ａがそれぞれ外付けされ、発振子５３Ａ又は５７Ａ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。

【００６７】

このように構成することで、ポータブルデバイス６は、ＣＰＵ５３，ＤＳＰ５９，ＵＳＢコントローラ５７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ともに小型化することができる。

【００６８】

ディジタルアナログ変換回路６３は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路６４に供給する。増幅回路６４は、音声信号を増幅して、ヘッドフォンジャック６５を介して、ヘッドフォンに音声信号を供給する。

【００６９】

このように、ポータブルデバイス６は、再生／停止ボタンが押圧操作されたとき、ＣＰＵ５３の制御に基づいてフラッシュメモリ６１に記憶されているコンテンツ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、コンテンツの再生を停止する。

【００７０】

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、ＣＰＵ５３の制御に基づいて停止した位置からコンテンツの再生を再開する。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。

【００７１】

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コンテンツを再生せず、１曲目から再生する。

【００７２】

また、ポータブルデバイス６のＣＰＵ５３は、ＬＣＤコントローラ６８を制御して、表示部６７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、音量及び乾電池５１の残量等の情報を表示させる。

【００７３】

さらに、ポータブルデバイス６は、ＥＥＰＲＯＭ６８に、フラッシュメモリ８０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６１のブロック位置及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。

【００７４】

因みに、本実施の形態においては、コンテンツは、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。

【００７５】

フラッシュメモリ６１にＦＡＴが格納される場合、例えば、１曲目のコンテンツがＣＰＵ５３の制御によりフラッシュメモリ６１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６１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６１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６１（１曲目と同一の領域）に書き込まれる。

【００７６】

このように、ＦＡＴは、フラッシュメモリ６１へのコンテンツの書き込みのたびに書き換えられ、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。

【００７７】

ＦＡＴがフラッシュメモリ６１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６１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６１に規定されている書換えの回数に達してしまい、フラッシュメモリ６１の書換えができなくなってしまう。

【００７８】

そこで、ポータブルデバイス６は、ＦＡＴをＥＥＰＲＯＭ６８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６１の書換えの頻度を少なくしている。

【００７９】

書換えの回数の多いＦＡＴをＥＥＰＲＯＭ６８に記憶させることにより、ＦＡＴをフラッシュメモリ６１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、ＣＰＵ５３は、ＥＥＰＲＯＭ６８にＦＡＴを追記するように書き込ませるので、ＥＥＰＲＯＭ６８の同一の領域の書換えの頻度を少なくして、ＥＥＰＲＯＭ６８が短期間で書換え不能になることを防止する。

【００８０】

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５７からＣＰＵ５３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。

【００８１】

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。
【００８２】
ＣＰＵ５３は、ＵＳＢ接続されたとき、ＤＳＰ５９のコンテンツ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。
【００８３】
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。
【００８４】
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。
【００８５】
つぎに、パーソナルコンピュータ１にインストールされた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の機能について説明する。
【００８６】
図４は、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の機能の構成を示す図である。
【００８７】
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、コピー管理プログラム１３３、移動管理プログラム１３４、暗号方式変換プログラム１３５、圧縮方式変換プログラム１３６、暗号化プログラム１３７、利用条件変換プログラム１３９、利用条件管理プログラム１４０、認証プログラム１４１、復号プログラム１４２、ＰＤ用ドライバ１４３、購入用プログラム１４４及び購入用プログラム１４５などの複数のプログラムで構成されている。
【００８８】
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、又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。
【００８９】
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、ＥＭＤの登録の際に、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（４－１，４－２，４－３）のとの接続を選択して、購入用アプリケーション１１５、又は購入用プログラム１４４，１４５に、ＥＭＤサーバ４（４－１，４－２，４－３）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。
【００９０】
チェックイン／チェックアウト管理プログラム１３２は、チェックイン又はチェックアウトの設定、及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１６２－１～１６２－Ｎに基づいて、コンテンツファイル１６１－１～１６１－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にチェックアウトするか、又はポータブルデバイス６に記憶されているコンテンツをチェックインする。
【００９１】

チェックイン／チェックアウト管理プログラム１３２は、チェックイン又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１６２－１～１６２－Ｎに格納されている利用条件情報を更新する。

【００９２】

コピー管理プログラム１３３は、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１６２－１～１６２－Ｎに基づいて、コンテンツファイル１６１－１～１６１－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にコピーするか、又はポータブルデバイス６からコンテンツをコンテンツデータベース１１４にコピーする。

【００９３】

移動管理プログラム１３４は、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１６２－１～１６２－Ｎに基づいて、コンテンツファイル１６１－１～１６１－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に移動するか、又はポータブルデバイス６からコンテンツをコンテンツデータベース１１４に移動する。

【００９４】

暗号方式変換プログラム１３５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１１５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、購入用プログラム１４４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を、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１６１－１～１６１－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。

【００９５】

圧縮方式変換プログラム１３６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１１５がＥＭＤサーバ４－１から受信したコンテンツの圧縮の方式、購入用プログラム１４４がＥＭＤサーバ４－２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１１４が記録しているコンテンツファイル１６１－１～１６１－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。

【００９６】

暗号化プログラム１３７は、例えばＣＤから読み取られ、録音プログラム１１３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１１４が記録しているコンテンツファイル１６１－１～１６１－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。

【００９７】

圧縮／伸張プログラム１３８は、例えばＣＤから読み取られ、録音プログラム１１３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１１４が記録しているコンテンツファイル１６１－１～１６１－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。圧縮／伸張プログラム１３８は、符号化されているコンテンツを伸張（復号）する。

【００９８】

利用条件変換プログラム１３９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１１５がＥＭＤサーバ４－１から受信したコンテンツの利用条件情報（いわゆる、Ｕｓａｇｅ　Ｒｕｌｅ）、購入用プログラム１４４がＥＭＤサーバ４－２から受信したコンテンツの利用条件情報を、コンテンツデータベース１１４が記録している利用条件ファイル１６２－１～１６２－Ｎに格納されている利用条件情報と同一のフォーマットに変換する。

【００９９】

利用条件管理プログラム１４０は、コンテンツのコピー、移動、チェックイン、又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１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに格納されている利用条件情報に対応するハッシュ値を基に、利用条件情報の改竄を検出する。利用条件管理プログラム１４０は、コンテンツのコピー、移動、チェックイン、又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１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに格納されてい

る利用条件情報を更新に対応して、利用条件情報に対応するハッシュ値を更新する。

【０１００】

認証プログラム１４１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及びコンテンツ管理プログラム１１１と購入用プログラム１４４との相互認証の処理を実行する。また、認証プログラム１４１は、ＥＭＤサーバ４－３と購入用プログラム１４５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。

【０１０１】

認証プログラム１４１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１４１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１４１に記憶される。

【０１０２】

復号プログラム１４２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１６１－１～１６１－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。

【０１０３】

ＰＤ用ドライバ１４３は、ポータブルデバイス６に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス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にコンテンツ又はポータブルデバイス６に所定の処理を実行させるコマンドを供給する。

【０１０４】

購入用プログラム１４４は、コンテンツ管理プログラム１１１ととも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、又は所定のＣＤに記録されて供給される。購入用プログラム１４４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。

【０１０５】

購入用プログラム１４４は、例えば、シャッフルされているインストラクション、又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、購入用プログラム１４４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。

【０１０６】

購入用プログラム１４４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、購入用プログラム１４４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。

【０１０７】

購入用プログラム１４５は、コンテンツ管理プログラム１１１ととも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、購入用プログラム１４５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。

【０１０８】

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１８３－１～１８３－Ｋ、又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又はマウス１９への操作を基に、コンテンツ管理プログラム１１１にチェックイン又はチェックアウトなどの処理の実行を指示する。

【０１０９】

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１６１－１～１６１－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。

【０１１０】

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１６１－１～１６１－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。

【０１１１】

画像ファイル１８３－１～１８３－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１６１－１～１６１－Ｎに対応する画像、又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。

【０１１２】

以下、画像ファイル１８３－１～１８３－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。

【０１１３】

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１６１－１～１６１－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。

【０１１４】

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から認証用鍵及び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に認証用鍵及びＥＭＤ選択プログラム１３１を供給する。

【０１１５】

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又はマウス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。

【０１１６】

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又は５－２にＣＤに対応するデータ（例えば、アルバム名、又はアーティスト名など）又は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又は５－２からＣＤに対応するデータ又は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。

【０１１７】

録音プログラム１１３は、受信したＣＤに対応するデータ又は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。

【０１１８】

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。

【０１１９】

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１６１－１～１６１－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１６１－１～１６１－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情報を、コンテンツが格納されているコンテンツファイル１６１－１～１６１－Ｎにそれぞれ対応する利用条件ファイル１６２－１～１６２－Ｎ

のいずれかに格納する（ＨＤＤ２１に記録する）。
【０１２０】
コンテンツデータベース１１４は、コンテンツファイル１６１－１～１６１－Ｎ又は利用条件ファイル１６２－１～１６２－Ｎをレコードとして記録してもよい。
【０１２１】
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情報は、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情報は、利用条件ファイル１６２－Ｎに格納されている。
【０１２２】
以下、コンテンツファイル１６１－１～１６１－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１６２－１～１６２－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。
【０１２３】
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、又は所定のＣＤ－ＲＯＭ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。
【０１２４】
次に、表示データファイル１８２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１６１－１～１６１－Ｎとの対応付けについて説明する。
【０１２５】
コンテンツファイル１６１－１～１６１－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、又はフィルタリングパッケージのいずれかである。
【０１２６】
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）、又は一枚の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、又は追加した情報の変更）することができる。
【０１２７】
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。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。
【０１２８】
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１８１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又はＷＷＷサーバ５などからネットワーク２を介して供給され、又は所定の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１８１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。
【０１２９】
フィルタリングデータは、所定のコンテンツを選択する、又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－ＰＯＰ（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～今週の日本のポップス１０位のコンテンツを特定することができる。

【０１３０】

フィルタリングデータファイル１８１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、又は曲名に”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。

【０１３１】

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２２１（コンテンツ用表示データ２２１に使用者が設定したデータを含む）、又は履歴データ１８４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。

【０１３２】

ドライバ１１７は、コンテンツ管理プログラム１１１などの制御の基に、音声入出力インターフェース２４を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム１１１に供給するか、若しくはコンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツをデジタルデータとして出力するか、又は、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツに対応するアナログ信号を出力する。

【０１３３】

図５は、表示操作指示プログラム１１２を起動させたとき、操作指示プログラム１１２がディスプレイ２０に表示させる表示操作指示ウィンドウの例を示す図である。

【０１３４】

表示操作指示ウィンドウには、録音プログラム１１３を起動させるためのボタン２０１、ＥＭＤ選択プログラム１３１を起動させるためのボタン２０２、チェックイン又はチェックアウトの処理の設定を行うフィールドを表示させるためのボタン２０３、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン２０４等が配置されている。

【０１３５】

ボタン２０５が選択されているとき、フィールド２１１には、オリジナルパッケージに対応するデータが表示される。ボタン２０６が選択されているとき、フィールド２１１には、マイセレクトパッケージに対応するデータが表示される。

ボタン２０７が選択されているとき、フィールド２１１には、フィルタリングパッケージに対応するデータが表示される。

【０１３６】

フィールド２１１に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、又はアーティスト名などである。

【０１３７】

例えば、図５においては、パッケージ名称”ファースト”及びアーティスト名”Ａ太郎”、パッケージ名称”セカンド”及びアーティスト名”Ａ太郎”などがフィールド２１１に表示される。

【０１３８】

フィールド２１２には、フィールド２１１で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド２１２に表示されるデータは、例えば、曲名、演奏時間、又はチェックアウト可能回数などである。

【０１３９】

例えば、図５においては、パッケージ名称”セカンド”に対応するパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”及びチェックアウト可能回数（例えば、８分音符の１つがチェックアウト１回に相当し、８分音符が２つでチェックアウト２回を示す）、並びに曲名”北

の墓場”及びチェックアウト可能回数（８分音符が１つでチェックアウト１回を示す）などがフィールド２１２に表示される。

【０１４０】

このように、フィールド２１２に表示されるチェックアウト可能回数としての１つの８分音符は、対応するコンテンツが１回チェックアウトできることを示す。

【０１４１】

フィールド２１２に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が０である。（ただし、パーソナルコンピュータ１はそのコンテンツを再生することができる。））ことを示す。また、フィールド２１２に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限がない（何度でも、チェックアウトできる）ことを示している。

【０１４２】

なお、チェックアウト可能回数は、図５に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

【０１４３】

また、表示操作指示ウィンドウには、選択されているパッケージ又はコンテンツに対応付けられている画像等（図４の画像ファイル１８３－１～１８３－Ｋのいずれかに対応する）を表示させるフィールド２０８が配置されている。ボタン２０９は、選択されているコンテンツを再生する（コンテンツに対応する音声をスピーカ４５に出力させる）とき、クリックされる。

【０１４４】

ボタン２０５が選択され、フィールド２１１に、オリジナルパッケージに対応するデータが表示されている場合、フィールド２１２に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、選択されている曲名に対応する、コンテンツデータベース１１４に格納されている所定のコンテンツを消去させる。

【０１４５】

録音プログラム１１３が表示させるウィンドウのボタン（後述するボタン２５５）が選択されて（アクティブにされて）いる場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス６に記憶されているコンテンツの曲名を表示するフィールド２１３を表示する。

【０１４６】

録音プログラム１１３が表示させるウィンドウのボタンが選択されている場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、コンテンツデータベース１１４に記録した、ＣＤから読み出したコンテンツを予め指定されているポータブルデバイス６にチェックアウトさせる。

【０１４７】

フィールド２１３にはコンテンツの曲名に対応させて、フィールド２１３の最も左に、そのコンテンツがパーソナルコンピュータ１にチェックインできるか否かを示す記号が表示される。例えば、フィールド２１３の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできる（すなわち、パーソナルコンピュータ１からチェックアウトされた）ことを示している。フィールド２１３の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできない（すなわち、パーソナルコンピュータ１からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

【０１４８】

表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス６に記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス６に記憶されているコンテンツが属するパーケージ）の名称を表示するフィールド２１４、フィールド２１３を閉じるためのボタン２１０及びチェックイン又はチェックアウトを実行させるボタン２１５を表示する。

【０１４９】

更に、表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、フィールド２１２で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン２１６、フィールド２１３で選択された曲名に対応するコンテンツのチェックインを設定するボタン２１７、フィールド２１３に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン２１８及びチェックイン又はチェックアウトの設定を取り消すボタン２１９を配置させる。

【０１５０】

ボタン２１６乃至２１９の操作によるチェックイン又はチェックアウトの設定だけでは、パーソナルコンピュータ１は、チェックイン又はチェックアウトの処理を実行しない。

【０１５１】

ボタン２１６乃至２１９の操作によるチェックイン又はチェックアウトの設定をした後、ボタン２１５がクリックされたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１にチェックイン又はチェックアウトの処理を実行させる。すなわち、ボタン２１５がクリックされたとき、表示操作指示プログラム１１２は、チェックイン又はチェックアウトの設定に基づき、コンテンツ管理プログラム１１１に、ポータブルデバイス６にコンテンツを送信させるか、又はチェックインに対応する所定のコマンド（例えば、ポータブルデバイス６が記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツ又はコマンドに対応する利用条件ファイル１６２に格納されている利用条件情報を更新させる。

【０１５２】

チェックイン又はチェックアウトが実行されたとき、表示操作指示プログラム１１２は、送信したコンテンツ又は送信されたコマンドに対応して、履歴データファイル１８４に格納されている履歴データを更新する。履歴データは、チェックイン又はチェックアウトされたコンテンツを特定する情報、又はそのコンテンツがチェックイン又はチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス６の名称などから成る。

【０１５３】

チェックイン又はチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックイン又はチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックイン又はチェックアウトの処理の回数を減らして、チェックイン又はチェックアウトに必要な時間全体（設定及び実行を含む）を短くすることができる。

【０１５４】

図６は、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。

【０１５５】

例えば、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１１３は、フィールド２５１に、”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１１３は、フィールド２５２に、例えば、”クワイ”などのアーティスト名を表示する。

【０１５６】

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１１３は、フィールド２５３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１１３は、フィールド２５３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。

【０１５７】

録音プログラム１１３が所定のＣＤの情報を受信した後、録音プログラム１１３は、ＨＤＤ２１の所定のディレクトリにＣＤの情報を格納する。

【０１５８】

ボタン２５４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１１３は、始めに、ＨＤＤ２１の所定のディレクトリを検索する。録音プログラム１１３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。

【０１５９】

録音プログラム１１３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２５６がクリックされたとき、録音プログラム１１３は、ドライブ２２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の情報とともにコンテンツ管理プログラム１１１に供給する。コンテンツ管理プログラム１１１の圧縮／伸張プログラム１３８は、録音プログラム１１３から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム１３７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１３９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情報を生成する。

【０１６０】

コンテンツ管理プログラム１１１は、圧縮され、暗号化されたコンテンツを利用条件情報とともに、コンテンツデータベース１１４に供給する。

【０１６１】

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から受信したコンテンツに対応するコンテンツファイル１６１及び利用条件ファイル１６２を生成して、コンテンツファイル１６１にコンテンツを格納するとともに、利用条件ファイル１６２に利用条件情報を格納する。

【０１６２】

コンテンツ管理プログラム１１１は、コンテンツデータベース１１４にコンテンツ及びコンテンツに対応する利用条件情報が格納されたとき、録音プログラム１１３から受信したＣＤの情報及び利用条件情報を表示操作指示プログラム１１２に供給する。

【０１６３】

表示操作指示プログラム１１２は、録音の処理でコンテンツデータベース１１４に格納されたコンテンツに対応する利用条件情報及びＣＤの情報を基に、表示データファイル１８２に格納する表示用のデータを生成する。

【０１６４】

録音プログラム１１３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１１４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にチェックアウトさせるか否かの設定を行うボタン２５５が配置されている。

【０１６５】

例えば、ボタン２５５がクリックされたとき、録音プログラム１１３は、ポータブルデバイス６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の選択をしたとき、選択されたポータブルデバイス６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。

【０１６６】

このように、録音プログラム１１３が表示させるウィンドウのボタン２５５をアクティブにしておくだけで、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、パーソナルコンピュータ１は、予め指定されているポータブルデバイス６に、ＣＤから読み出したコンテンツをチェックアウトさせることができる。

【０１６７】

（２）異なるフォーマット間での取り扱い

ところで、音楽コンテンツを提供するコンテンツ配信業者は、数多く存在し、それぞれの配信業者毎に、そのコンテンツの暗号化方式や圧縮方式、さらに、利用条件情報のフォーマットが異なっている。従って、一般にユーザは、提供を受けたいコンテンツの配信業者毎に、再生やチェックイン／チェックアウト用のコンテンツ管理アプリケーションやポータブルデバイスを購入しなければならなかった。そのため、ユーザは、１つのパーソナルコンピュータ上に格納されている音楽コンテンツを、１つの管理アプリケーションやポータブルデバイスで取り扱うことができなかった。

【０１６８】

そこで、本システムでは、このように配信業者毎にフォーマットが異なるコンテンツを、パーソナルコンピュータ１上で統一的に取り扱っている。

【０１６９】

以下、この音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて、図７を参照して説明する。

【０１７０】

ネットワーク２に接続された複数のＥＭＤサーバは、例えば音楽提供会社Ａから提供される音楽コンテンツを配信するＥＭＤサーバ（Ａ）４－１、音楽提供会社Ｂから提供される音楽コンテンツを配信するＥＭＤサーバ（Ｂ）４－２、音楽提供会社Ｘから提供される音楽コンテンツを配信するＥＭＤサーバ（Ｘ）４－３であるものとする。各ＥＭＤサーバ４（４－１，４－２，４－３）は、各社独自にラインナップがされた音楽コンテンツを、ユーザが持つパーソナルコンピュータ１にネットワーク２を介して提供を行う。また、各ＥＭＤサーバ４（４－１，４－２，４－３）では、音楽コンテンツの暗号化方式、利用条件（ Usage Rule ）情報のフォーマット、音楽コンテンツの圧縮方式、音楽コンテンツの課金方式等が各社独自の方式が採用されそれぞれ異なる方式により音楽コンテンツを配信している。

【０１７１】

パーソナルコンピュータ１には、音楽コンテンツの再生や管理等を行うためのアプリケーションソフトウェアとして、ＥＭＤサーバ（Ａ）４－１から音楽コンテンツの購入や管理や再生を行う再生用アプリケーション（Ａ）３１１と、ＥＭＤサーバ（Ｂ）４－２から音楽コンテンツの購入や管理や再生を行う再生用アプリケーション（Ｂ）３１２と、音楽コンテンツをポータブルデバイス（Ａ）６－１に転送するデバイスドライバ（Ａ）３１３と、音楽コンテンツをポータブルデバイス（Ｂ）６－２に転送するデバイスドライバ（Ｂ）３１４とがインストールされている。なお、この図７で示す再生用アプリケーション３１１，３１２は、図４で示した購入用アプリケーションプログラム１１５及びドライバ１１７に対応するものである。

【０１７２】

また、パーソナルコンピュータ１には、ＨＤＤ２１内に格納されている全ての音楽コンテンツの包括的な管理を行う包括管理ユニット（Ｘ）３１５がインストールされている。この包括管理ユニット（Ｘ）３１５は、さらに、ＥＭＤ用受信インターフェース３１６，ＥＭＤ用送信インターフェース３１７，ＰＤ用ドライバ３１８により構成されている。

【０１７３】

また、ここでは、ポータブルデバイス（Ａ）６－１は音楽提供会社Ａに対応した専用の装置であり、ポータブルデバイス（Ｂ）６－２は音楽提供会社Ｂに対応した専用の装置であり、ポータブルデバイス（Ｘ）６－３は音楽提供会社Ｘに対応した専用の装置であるものとする。なお、ここでは、メモリカード内に格納した音楽コンテンツは、各音楽提供会社

独自の暗号化方式で暗号化されており、また、その圧縮方式や利用条件情報のフォーマットも異なる。そのため、例えば他のデバイスドライバ等と直接接続して、音楽コンテンツを転送することはできないようになっているものとする。

【０１７４】

再生用アプリケーション（Ａ）３１１は、ＥＭＤサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ，コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション（Ａ）３１１は、対応しているＥＭＤサーバに対してのみ接続処理を行うようになっている。ここでは、再生用アプリケーション（Ａ）３１１は、ＥＭＤサーバ（Ａ）４－１に対応した処理を行い、他のＥＭＤサーバに対して接続処理を行うことができない。また、再生用アプリケーション（Ａ）３１１は、ＥＭＤサーバ（Ａ）４－１と接続した際の認証処理、ポータブルデバイス（Ａ）６－１と接続した際の認証処理、ＨＤＤ２１に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション（Ａ）３１１は、例えば、ＥＭＤサーバ（Ａ）４－１からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ＨＤＤ２１に格納する。なお、暗号化処理の方式は、各再生用アプリケーションでそれぞれ独自の方式を採用している。そのため、パーソナルコンピュータ１内の同一のＨＤＤ２１に格納されている音楽コンテンツであっても、専用の再生用アプリケーションでなければ、他の再生用アプリケーションでは暗号を解読することができないようになっている。

【０１７５】

また、再生用アプリケーション（Ａ）３１１は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション（Ａ）３１１は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を１回分デクリメントする等の処理を行う。

【０１７６】

また、再生用アプリケーション（Ａ）３１１は、自己がＨＤＤ２１上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット（Ｘ）３１５のＥＭＤ用受信インターフェース３１６に送信する。

【０１７７】

再生用アプリケーション（Ｂ）３１２は、ＥＭＤサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ，コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション（Ｂ）３１２は、対応しているＥＭＤサーバに対してのみ接続処理を行うようになっている。具体的には、再生用アプリケーション（Ｂ）３１２は、ＥＭＤサーバ（Ｂ）４－２に対応した処理を行い、他のＥＭＤサーバに対して接続処理を行うことができない。また、再生用アプリケーション（Ｂ）３１２は、ＥＭＤサーバ（Ｂ）４－２と接続した際の認証処理、ポータブルデバイス（Ｂ）６－２と接続した際の認証処理、ＨＤＤ２１に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション（Ｂ）３１２は、例えば、ＥＭＤサーバ（Ｂ）４－２からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ＨＤＤ２１に格納する。

【０１７８】

また、再生用アプリケーション（Ｂ）３１２は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション（Ｂ）３１２は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を１回分デクリメントする等の処理を行う。

【０１７９】

また、再生用アプリケーション（Ｂ）３１２は、自己がＨＤＤ２１上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット（Ｘ）３１５のＥＭＤ用受信インターフェース３１６に送信する。

【０１８０】
デバイスドライバ（Ａ）３１３は、ポータブルデバイス（Ａ）６－１への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ（Ａ）３１３は、ポータブルデバイス（Ａ）６－１に音楽コンテンツを転送する。
【０１８１】
デバイスドライバ（Ｂ）３１４は、ポータブルデバイス（Ｂ）６－２への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ（Ｂ）３１４は、ポータブルデバイス（Ｂ）６－２に音楽コンテンツを転送する。
【０１８２】
包括管理ユニット（Ｘ）３１５は、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツの提供を受ける音楽提供会社Ｘ専用のアプリケーションソフトウェアであるとともに、デバイスドライバ（Ａ）３１３及びデバイスドライバ（Ｂ）３１４や、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２との間で音楽コンテンツ及び利用条件情報の転送を行って、パーソナルコンピュータ１内の音楽コンテンツを包括的に管理を行う管理ソフトウェアでもある。
また、自己が管理を行う音楽コンテンツを、携帯型の音楽再生装置である専用のポータブルデバイス（Ｘ）６－３に転送することができる。
【０１８３】
なお、この包括管理ユニット（Ｘ）１１５は、図４に示したコンテンツ管理プログラム１１１に対応する処理を行う。
【０１８４】
ＰＤ用ドライバ３１８は、ポータブルデバイス（Ｘ）６－３との接続用のインターフェースモジュールで、このポータブルデバイス（Ｘ）６－３との間における認証処理や暗号化処理を行う。また、ＰＤ用ドライバ３１８は、他のポータブルデバイス８，９に音楽コンテンツ等を転送する場合には、デバイスドライバ（Ａ）３１３やデバイスドライバ（Ｂ）３１４を介して音楽コンテンツ及び利用条件情報を転送する。
【０１８５】
ＥＭＤ用受信インターフェース３１６は、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２からの音楽コンテンツ及び利用条件情報の受信、ＥＭＤサーバ（Ｘ）４－３からネットワーク２を介して転送された音楽コンテンツ及び利用条件情報の受信、及び、ＰＤ用ドライバ３１８との間での音楽コンテンツ及び利用条件情報の送受信を行う。
【０１８６】
ＥＭＤ用受信インターフェース３１６は、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２から音楽コンテンツ及び利用条件情報を受信する場合には、相互認証処理、暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換等を行う。暗号化方式、利用条件情報、圧縮方式の変換は、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２が用いている方式から、包括管理ユニット（Ｘ）３１５が用いている方式に変換される。ここで包括管理ユニット（Ｘ）３１５が用いている方式を、以下、統一転送プロトコルと呼ぶ。そして、ＥＭＤ用受信インターフェース３１６は、このように統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、ＰＤ用ドライバ３１８を介してデバイスドライバ（Ａ）３１３やデバイスドライバ（Ｂ）３１４に送信する。また、ＥＭＤ用受信インターフェース３１６は、統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、ＰＤ用ドライバ３１８を介して、ポータブルデバイス（Ｘ）６－３に送信する。
【０１８７】
このように、ＥＭＤサーバ（Ａ）４－１及びＥＭＤサーバ（Ｂ）４－２から提供される音楽コンテンツは、一旦再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２によりダウンロードされ、音楽コンテンツの暗号化方式、圧縮方式、利用条

件情報が、統一転送プロトコルに変換されて、包括管理ユニット（Ｘ）３１５に転送される。包括管理ユニット（Ｘ）３１５は、ＥＭＤサーバ（Ａ）４－１、ＥＭＤサーバ（Ｂ４－２）、ＥＭＤサーバ（Ｘ）４－３からダウンロードされたそれぞれのコンテンツ提供会社の音楽コンテンツを統括的に管理を行うことができる。

【０１８８】

また、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの複製（コピー）、移動（ムーブ）、チェックイン、チェックアウトの機能を有している。

【０１８９】

ＥＭＤ用受信インターフェース３１６は、ユーザからの複製命令、移動命令に従い、例えば、再生用アプリケーション（Ａ）３１１や再生用アプリケーション（Ｂ）３１２によって管理されている音楽コンテンツを、包括管理ユニット（Ｘ）３１５に複製や移動する処理を行う。この際に、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットの変換を行って、統一転送プロトコルとする。

【０１９０】

また、ユーザからのＣＤリッピング命令やチェックイン命令に従い、コンパクトディスク等の外部メディアやポータブルデバイス６（６－１，６－２，６－３）に格納されている音楽コンテンツを、包括管理ユニット（Ｘ）３１５に複製やチェックインする処理を行う。この際に、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

【０１９１】

また、ユーザからのチェックアウト命令に従い、包括管理ユニット（Ｘ）３１５により管理されている音楽コンテンツを、ポータブルデバイス（Ｘ）６－３に記録する処理を行う。この際に、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。また、この際に、利用条件のチェックアウト可能回数を１減少させる。

【０１９２】

また、包括管理ユニット（Ｘ）３１５では、図８に示すように、アプリケーション層の下位レイヤに統一転送プロトコルを設けて、このレイヤにおいて他の再生用アプリケーションとのデータ転送を行っている。そして、包括管理ユニット（Ｘ）３１５は、この統一転送プロトコルの更に下位レイヤをｈｔｔｐ（ hiper Text Transfer Protocol ）として、ＥＭＤサーバ（Ｘ）４－３とのデータ送受信を行っている。

【０１９３】

以上のような構成の音楽コンテンツ配信システムでは、ＥＭＤサーバ（Ａ）４－１及びＥＭＤサーバ（Ｂ）４－２から配信された音楽コンテンツを、包括管理ユニット（Ｘ）３１５が取得し、再生や管理を行うようになっている。そして、ＥＭＤサーバ（Ｘ）４－３、ＥＭＤサーバ（Ａ）４－１及びＥＭＤサーバ（Ｂ）４－２から配信された音楽コンテンツを、ポータブルデバイス（Ｘ）６－３へ転送できるようになっている。

【０１９４】

このように音楽コンテンツ配信システムでは、包括管理ユニット（Ｘ）３１５を中心として、各再生用アプリケーション及びデバイスドライバの間で、転送する音楽コンテンツの暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換が行われ、統一転送プロトコルを用いて音楽コンテンツの転送が行われる。そのため、例えば、再生用アプリケーション（Ａ）３１１によりＥＭＤサーバ（Ａ）４－１からダウンロードした音楽コンテンツ並びに再生用アプリケーション（Ｂ）３１２によりＥＭＤサーバＢ４－２からダウンロードした音楽コンテンツを、包括管理ユニット（Ｘ）３１５に転送することができる。このため、例えば音楽提供会社Ａからのみ提供されるアーチストの音楽コンテンツを、ポータブルデバイス

（Ｘ）６－３に転送することができる。すなわち、この音楽コンテンツ配信システムでは、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、音楽コンテンツの圧縮方式等を、統一転送プロトコルに変換するので、パーソナルコンピュータ１のハードディスク内に格納されている様々な方式の音楽コンテンツを、包括管理ユニット（Ｘ）３１５やポータブルデバイス（Ｘ）６－３により再生を行うことができる。特に、音楽コンテンツ配信システムでは、転送の際に、暗号化方式及び利用条件情報を変換するので、音楽コンテンツの著作権の保護を図りつつ、その音楽コンテンツの取り扱いの自由度を大きくすることができる。

【０１９５】

すなわち、音楽コンテンツ配信システムでは、音楽コンテンツの再生や制御を行う再生用アプリケーション間で、少なくとも暗号化方式と利用条件情報の変換を行って、音楽コンテンツ及び利用条件情報の転送を行う。このことにより、音楽コンテンツ配信システムでは、複数の再生用アプリケーションが存在してもパーソナルコンピュータ１内の例えばＨＤＤ２１に格納されている音楽コンテンツを自由に移動させることができ、統一的な音楽コンテンツの管理をすることができる。また、音楽コンテンツとともに利用条件情報も転送するので、１つの音楽コンテンツに対して利用条件が重複したりすることがなく、音楽コンテンツの著作権も確実に保護することができる。

【０１９６】

（３）利用条件情報

（一般的に用いられる利用条件情報の説明）

つぎに、再生用アプリケーション（Ａ）３１１に用いられる利用条件情報のフォーマットの一例について説明をする。

【０１９７】

再生用アプリケーション（Ａ）３１１では、例えば、図９（ａ）に示すような表形式で記述された利用条件情報が用いられている。

【０１９８】

表の左欄には、利用条件のポリシーが列方向に記述され、右欄には各ポリシーの具体的な値が記述される。例えば、ポリシーとして、再生開始可能日（ｆｒｏｍ）、再生終了日（ｔｏ）、１回の再生に対する価格（ｐａｙ／ｐｌａｙ）等が記述される。このような利用条件情報は、図９（ｂ）に示すように各音楽コンテンツに付加された状態で、ＥＭＤサーバ（Ａ）４－１から配信される。再生用アプリケーション（Ａ）３１１は、記述されているポリシー及びその値に従い、音楽コンテンツの制御を行う。例えば、利用条件情報に、再生開始可能日（ｆｒｏｍ）が９９年１０月２５日、再生終了日（ｔｏ）が９９年１１月２４日、１回の再生に対する価格（ｐａｙ／ｐｌａｙ）がｙｅｓ／１０円と記述されているとする。この場合、その音楽コンテンツは、９９年１０月２５日から再生が可能とされ、それ以前にユーザから再生命令があっても、再生を禁止する。また、その音楽コンテンツは、９９年１１月２４日まで再生が可能とされ、それ以後となると、その音楽コンテンツを消去する。また、その音楽コンテンツは、１回の再生の度に１０円の課金を行うように設定されており、例えば、ユーザが再生した回数を別途ログ情報として保管しておき、そのログ情報をＥＭＤサーバ（Ａ）４－１にアップロードして、視聴したユーザに対して視聴した回数分だけの課金処理を行う。

【０１９９】

（包括管理ユニット（Ｘ）３１５が用いている利用条件情報の説明）

つぎに、包括管理ユニット（Ｘ）３１５が用いている利用条件情報について説明する。以下説明をする利用条件情報は、ＥＭＤサーバ（Ｘ）４－３からダウンロードされる音楽コンテンツに付加されており、上記包括管理ユニット（Ｘ）３１５がその音楽コンテンツの制御を行う際に用いられる。また、この利用条件情報は、再生用アプリケーション（Ａ）３１１と包括管理ユニット（Ｘ）３１５との間、及び、再生用アプリケーション（Ｂ）３１２と包括管理ユニット（Ｘ）３１５との間で、音楽コンテンツの転送をする際の統一フォーマットとして用いられる。以下、この利用条件情報を、統一利用条件情報と称する。

【０２００】
統一利用条件情報は、図１０に示すように、インデックスファイル３３１、オートマトンファイル３３２と、パラメータファイル３３３と、履歴ファイル３３４とから構成される。各ファイルは、ＸＭＬ(eXtensible Markup Language)言語で記述されている。
【０２０１】
インデックスファイル３３１には、各ファイルのリファレンス情報等が記述されている。
【０２０２】
オートマトンファイル３３２には、図１１に示すように、利用条件がオートマトンで記述されたオートマトン記述部３４１と、コンテンツ鍵による認証コード（ＭＡＣ:Message Authentication Code）３４２、コンテンツ提供者の署名（Ｓｉｇ）３４３、この署名を検証するための認証書（Ｃｅｒｔ）３４４が付加されている。ここで、コンテンツ鍵をK_C、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれK^{-1}_E, K^{1}_Eとする。
【０２０３】
オートマトン記述部３４１は、tuple列で記述されたExtended State Machineにより音楽コンテンツの動作状態が記述される。
【０２０４】
具体的には、オートマトン記述部３４１では、現在の音楽コンテンツの動作状態の集合をＱとし、音楽コンテンツのイベントを表す入力シンボルの集合をΣとし、状態遷移した後の音楽コンテンツの動作状態の集合をＱ′を以下のように表す。
Ｑ′＝｛ｄ｜ｄ＝δ（ｑ，α）｜ｑ　Ｑ，α　Σ，δ：Ｑ×Σ→Ｑ｝
この式に示すように、状態遷移した後の状態Ｑ′の集合は、ｄとして表される。このｄは、変数ｑ、αをもった関数δによって定義される。ｑは、音楽コンテンツの動作状態の集合Ｑのなかの１つの動作状態を示している。αは、イベントの集合Σのなかの１つのイベントを示している。そして、関数δは、Ｑ及びΣのべき集合のＱへの写像である。
【０２０５】
そして、以上のＱ，Σ，Ｑ′に基づき、各tupleを
｛〈ｑ，α，ｄ〉｜ｑ，ｄ　Ｑ，α　Σ｝
として表す。なお、〈ｑ，α，ｄ〉は、ｑ、α、ｄの順列のある組み合わせを示している。
【０２０６】
ここで、Σには、再生（Play）,複製（copy）,支払い金額（pay Y）,再生開始可能日時（from YMD）,再生終了日時（to YMD）,使用可能日数（in Ddays）,ヌルイベント（ε）といったイベントが、以下のように記述される。
Σ＝｛Play,copy,pay Y,from YMD,to YMD,in Ddays,ε｝
このようにオートマトン記述部３４１は、以上のように記述される。
【０２０７】
このオートマトン記述部３４１への具体的な記述例について説明をする。
【０２０８】
例えば、図１２に示すような音楽コンテンツの動作遷移を示すオートマトンのtuple列による記述例を、図１３に示す。
【０２０９】
このオートマトンは、以下に説明するような状態遷移をする。
【０２１０】
まず、初期状態ｑ０から、状態ｑ１及び状態ｑ５に遷移する。状態ｑ１及び状態ｑ５以降は、それぞれ並行して動作する。
【０２１１】
状態ｑ１で、所定金額（例えば１０円）の支払いイベント（ｐａｙ１０）が発生すると状態ｑ２へ遷移する。状態ｑ２で、プレイイベント（ｐｌａｙ）が発生すると状態ｑ１へ遷移する。すなわち、このオートマトンでは、１０円の支払いがされると、音楽コンテンツ

が１回だけ再生が可能となることを示している。また、状態ｑ１で、所定金額（例えば１０００円）の支払いイベント（ａ．ｐａｙ１０００）が発生すると状態ｑ３へ遷移する。状態ｑ３では、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ３に遷移する。すなわち、このオートマトンでは、１０００円の支払いがされると、音楽コンテンツが回数に制限無く再生が可能となることを示している。また、状態ｑ１で、一回の再生金額（例えば１０円）のｎ倍の金額の支払いイベント（ｐａｙ１０×ｎ）が発生すると、状態ｑ４へ遷移する。状態ｑ４へ遷移してから、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ４に遷移する。そして、この状態ｑ４で、ｎ回のプレイイベントが発生すると、状態ｑ１に遷移する。すなわち、このオートマトンでは、１０×ｎ円の支払いがされると、音楽コンテンツがｎ回再生が可能となることを示している。

【０２１２】

また、状態ｑ５で、所定金額（例えば１００円）の支払いイベント（ｐａｙ１００）が発生すると状態ｑ６へ遷移する。状態ｑ６で、コピーイベント（ｃｏｐｙ）が発生すると状態ｑ５へ遷移する。また、状態ｑ６で、コピーイベント（ｃｏｐｙ）が発生すると、状態ｑ８へ遷移する。状態ｑ８で、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ８に遷移する。また、この状態ｑ８で、コピーイベント（ｃｏｐｙ）が発生すると、状態ｑ９に遷移する。状態ｑ９では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンでは、１００円の支払いがされると音楽コンテンツを他のデバイスへ１回コピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

【０２１３】

また、状態ｑ５で、所定金額（例えば２０００円）の支払いイベント（ａ．ｐａｙ２０００）が発生すると状態ｑ７へ遷移する。状態ｑ７では、コピーイベント（ｃｏｐｙ）が発生すると、再度この状態ｑ７に遷移する。また、状態ｑ７で、コピーイベント（ｃｏｐｙ）が発生すると、状態ｑ８へ遷移する。状態ｑ８で、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ８に遷移する。また、この状態ｑ８で、コピーイベント（ｃｏｐｙ）が発生すると、状態ｑ９に遷移する。状態ｑ９では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンでは、２０００円の支払いがされると、音楽コンテンツを他のデバイスへ回数制限無くコピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

【０２１４】

そして、以上のように状態遷移をするオートマトンをtuple列で記述すると、図１３に示すようになる。

【０２１５】

また、オートマトン記述部３４１は、音楽コンテンツの動作を更新するため、動作状態の並列合成を記述しても良い。例えば、動作a_0と動作a_1との並列合成は、tuple列で以下のように表される。

〈q_0，α，a_0．q_0〉

〈q_0，α，a_1．q_0〉

また、オートマトン記述部３４１には、状態遷移に伴うアクションを記述してもよい。例えば、アクションは、tupleで以下のように表される。

〈q_0，α，q_1；ａｃｔｉｏｎ〉

このアクションは、予め定義した変数を用いた関数として表される。また、変数は、ＩＤとスコープと初期値とからなる。スコープには、その音楽コンテンツ、アルバム、システム全体等のクラスがある。例えば、アルバム（ａ）の買い取りの値段を表す変数をｎとし、ａ．ｎ：＝１０００のように記述する。このように変数に対するアクションが記述されたオートマトン記述部３４１の一例を以下に示す。

〈q_0，ｐａｙ１００，q_1，ａ．ｎ：＝ａ．ｎ－１００〉・・・（１）
〈q_0，ｐａｙ（ａ．ｎ），q_1，ａ．ｎ：＝０〉　・・・（２）
〈q_1，ｐｌａｙ，q_2〉　・・・（３）
この例は、１つの音楽コンテンツの買い取り値段｛式（１）｝が、アルバム買い取り｛式（２）｝の値段に影響を及ぼすことを示している。

【０２１６】
以上のようなオートマトン記述部３４１は、図１４に示すように、エントリーＩＤ３４５と、コンテンツＩＤ３４６と、バージョン情報３４７と、変数情報３４８と、tuple列３４９とから構成される。

【０２１７】
以上のように記述フォーマットが定められたオートマトン記述部３４１の具体例について説明をする。

【０２１８】
なお、以下にオートマトンの記述で用いられているイベント及びコマンドは、ＸＭＬの仕様に基づいて規定されたＤＴＤ（ Document Type Definition ）で定義されている。例えば、図１５に示すように、再生動作（play）、複製動作（copy）、再生権購入（pay-for-play）、複製権購入（pay-for-copy）、アルバム再生権購入（pay-for-album-play）、アルバム複製権購入（pay-for-album-copy）、使用可能開始日（from）、使用終了日（to）、ヌル動作（null）がイベントとして、ＤＴＤによって定義されている。

【０２１９】
図１６は、音楽コンテンツが１９９９年９月１日から再生が可能であることを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２０】
この図１６に示す記述は、図１７に示すようなオートマトンとなる。このオートマトンは、初期状態の状態ｑ１と、状態ｑ２とから構成される。状態ｑ１で、日付が使用可能開始日（ｆｒｏｍ）の１９９９年９月１日となると、状態ｑ２へ遷移する。そして、状態ｑ２で、再生イベント（ｐｌａｙ）が発生すると、音楽コンテンツの再生を行い、再度状態ｑ２へ遷移する。このようにこのオートマトンは、音楽コンテンツを、１９９９年９月１日から再生を可能とするように制御している。

【０２２１】
図１８は、音楽コンテンツが１９９９年１０月３１日まで再生が可能であることを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２２】
この図１８に示す記述は、図１９に示すようなオートマトンとなる。このオートマトンは、初期状態の状態ｑ１と、終端状態の状態ｅｎｄとから構成される。
状態２で、再生イベント（ｐｌａｙ）が発生すると、音楽コンテンツの再生を行い、再度状態ｑ２へ遷移する。また、状態２で、使用終了日（ｔｏ）の１９９９年１０月３１日となると、状態ｅｎｄへ遷移する。状態ｅｎｄとなると、どの状態へも遷移せずイベントも発生しない。このように、このオートマトンは、音楽コンテンツを、１９９９年１０月３１日まで再生を可能とするように制御している。

【０２２３】
図２０は、音楽コンテンツの再生可能期間が１９９９年９月１日から１９９９年１０月３１日までであって、且つ、その再生可能回数が１６回であることを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２４】
この図２０に示す記述は、図２１に示すようなオートマトンとなる。このオートマトンは、初期状態の状態ｑ１と、状態ｑ２と、終端状態の状態ｅｎｄとから構成される。状態ｑ１で、使用可能開始日（ｆｒｏｍ）の１９９９年９月１日となると、状態ｑ２へ遷移する。そして、状態ｑ２で、再生イベント（ｐｌａｙ）が発生すると、音楽コンテンツの再生を行い、再度状態ｑ２へ遷移する。また、状態２で、使用終了日（ｔｏ）の１９９９年１

０月３１日となるか、或いは、１６回再生イベント（ｐｌａｙ×１６）が発生すると、状態ｅｎｄへ遷移する。状態ｅｎｄとなると、どの状態へも遷移せずイベントも発生しない。このようにこのオートマトンは、音楽コンテンツの再生期間を１９９９年９月１日から１９９９年１０月３１日までとし、且つ、その再生回数を１６回に制御している。

【０２２５】

図２２は、音楽コンテンツの再生回数を１６回に制限することを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２６】

つぎに、パラメータファイル３３３には、図２３に示すように、パラメータ記述部３５１、コンテンツ鍵による認証コード３５２、コンテンツ提供者の署名３５３、この署名を検証するための認証書３５４が付加されている。ここで、コンテンツ鍵をK_C、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれK^{-1}_E，K^{1}_Eとする。

【０２２７】

また、パラメータファイル３３３は、上記オートマトンファイル３３２を作成したコンテンツ提供者とは別のコンテンツ提供者（例えば、コンテンツ小売業者やコンテンツ中間業者等の二次提供者）により書き換えることが可能である。書き換えられたパラメータファイル３３３は、図２４に示すように、それぞれの提供者や中間業者等に与えられたユニークなエンティティＩＤ５５が付加される。

ここで、K'_Cは、二次提供者のコンテンツ鍵で、$K'_C = H(K_C, \text{ＥｎｔｉｔｙＩＤ})$となる。なお、ここで、Ｈは、一方向ハッシュ関数である。二次提供者のコンテンツ鍵K'_Cは、一次提供者のコンテンツ鍵K_Cから作成される。一次提供者と二次提供者とは、その認証書により区別される。

【０２２８】

パラメータファイル３３３を検証する方法としては、コンテンツ鍵が得られていればＭＡＣにより行い、安全性等の理由でコンテンツ鍵が得られない場合には署名と証明書により検証する。

【０２２９】

ＭＡＣにより検証するプロトコルは以下のようになる。コンテンツの一次提供者をＳ、二次提供者をＡ、端末をＢとする。Ｓ→Ａは、ＳからＡへの伝送を示しており、Ｓ→Ｂは、ＳからＢへの伝送を示しており、Ａ→Ｂは、ＡからＢへの伝送を示している。また、ID_Aは、デバイスＡのＩＤを示している。

【０２３０】

$$S \rightarrow A: \quad K'_C = H(K_C, ID_A)$$

$$S \rightarrow B: \quad X = E_{Ks}(K_C)$$

$$A \rightarrow B: \quad ID_A, \text{Parameters}, M = MACK'_C(\text{Parameters})$$

$$B: \quad M \quad MAC_{K'_C}(\text{Parameters}) \ ?$$

このパラメータ記述部３５１には、上記オートマトンファイル３１のオートマトン部４１に記述された値の変更のための関数の係数が記述される。例えば、図１３に示した例において、オートマトン部４１では、例えば、以下のように音楽コンテンツの価格が関数となる場合がある。

〈q_0，ｐａｙ（f_1（１０））， q_1〉

〈q_1，ｐａｙ（f_2（１０）×ｎ）， q_2〉

この場合、上記関数f_1及びf_2を、例えば、以下のように定める。

$f_1(n) = 0.9n$

$f_2(n) = 90 + 0.1n$

このように関数を定めることによって、例えば、一次提供者が価格のデフォルト値を定め、二次提供者がパラメータファイル３３３を書き換えて、価格を変更することができる。

【０２３１】
以上のようなパラメータ記述部３５１は、図２５に示すように、エントリーＩＤ３５６と、コンテンツＩＤ３５７と、係数情報３５８とから構成される。
【０２３２】
履歴ファイル３３４は、オートマトン記述部３４１に記述内容に基づき動作する音楽コンテンツの動作の軌跡を記述するファイルである。この履歴ファイル３３４には、上記オートマトン記述４１のｔｕｐｌｅ内のステータスと変数を記録する。例えば、上述した図１３に例において、２回再生を行った場合には、
〈q_0，q_1，q_0，q_1〉
となり、これにより以下のような動作の軌跡を得ることができる。
〈ｐａｙ１０，ｐｌａｙ，ｐａｙ１０，ｐｌａｙ〉
これを集計して、例えば、包括管理ユニット（Ｘ）３１５にアップロード等すれば、ユーザの支払い金額を計算することができる。
【０２３３】
以上のように音楽コンテンツ配信システムでは、ポリシー自体及びその具体的な値をプログラム化したオートマトンによって利用条件情報を記述しているので、コンテンツの利用条件の記載の自由度を高めることができる。
【０２３４】
（４）破壊された音楽コンテンツ等のリストア及び再ダウンロード
つぎに、包括管理ユニット（Ｘ）３１５による音楽コンテンツのバックアップについて説明をする。
【０２３５】
まず、包括管理ユニット（Ｘ）３１５の音楽コンテンツの鍵管理方法について、図２６を用いて説明する。
【０２３６】
包括管理ユニット（Ｘ）３１５は、パーソナルコンピュータ１内のＨＤＤ２１に、音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎを格納している。また、包括管理ユニット（Ｘ）３１５は、各音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎに対応するコンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎも格納している。コンテンツ鍵Ｋｃは、音楽コンテンツＣに対して一対一の関係となっている。また、各音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎには、それぞれの識別するためのコンテンツＩＤが付加されている。このコンテンツＩＤを、ＣＩＤ１，ＣＩＤ２，ＣＩＤ３・・・ＣＩＤｎとする。
【０２３７】
音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎは、コンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎにより暗号化され、Ｅ（Ｋｃ１，Ｃ１），Ｅ（Ｋｃ２，Ｃ２），Ｅ（Ｋｃ３，Ｃ３）・・・Ｅ（Ｋｃｎ，Ｃｎ）とされた状態でパーソナルコンピュータ１のＨＤＤ２１内に記録されている。ここで、Ｅ（Ｋ，Ｃ）は、鍵ＫでコンテンツＣを暗号化していることを示す。通常、コンテンツＩＤは、音楽コンテンツＣのヘッダなどに記録されて音楽コンテンツＣとともに暗号化されているか、或いは、ＭＡＣが音楽コンテンツＣに付加された状態とされており、音楽コンテンツ本体と切り離しができないようになっている。
【０２３８】
また、コンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎは、ストレージ鍵ＫＳにより暗号化され、Ｅ（ＫＳ，Ｋｃ１），Ｅ（ＫＳ，Ｋｃ２），Ｅ（ＫＳ，Ｋｃ３）・・・Ｅ（ＫＳ，Ｋｃｎ）とされた状態でパーソナルコンピュータ１のＨＤＤ２１上に記録されている。このストレージ鍵ＫＳは、いわゆる耐タンパ性を有しており、通常のユーザからは参照することができない記録領域に保存されている。
【０２３９】
以上のように鍵管理が行われる包括管理ユニット（Ｘ）３１５では、例えば、音楽コンテンツＣ１の再生を行う場合には、ストレージ鍵ＫＳを用いてコンテンツ鍵Ｋｃ１の暗号を解除し、続いて、このコンテンツ鍵Ｋｃ１を用いて、音楽コンテンツＣ１の暗号を解除す

る。このことにより、包括管理ユニット（Ｘ）３１５は、音楽コンテンツＣ１の再生を行うことができる。

【０２４０】

また、以上のように鍵管理が行われる包括管理ユニット（Ｘ）３１５では、例えば、音楽コンテンツＣ１をＨＤＤ２１からポータブルデバイス（Ｘ）６－３に移動（ＭＯＶＥ）する場合には、ポータブルデバイス（Ｘ）６－３との間で相互認証を行い、認証が完了するとストレージ鍵ＫＳを用いてコンテンツ鍵Ｋｃ１の暗号を解除し、続いて、セッション鍵によりコンテンツ鍵Ｋｃ１を暗号化し、暗号化したコンテンツ鍵Ｋｃ１及び暗号化した音楽コンテンツＣ１をポータブルデバイス（Ｘ）６－３に転送する。そして、コンテンツ鍵Ｋｃ１と音楽コンテンツＣ１をともにＨＤＤ２１から消去をする。このことにより、包括管理ユニット（Ｘ）３１５は、音楽コンテンツＣ１をポータブルデバイス（Ｘ）６－３に移動することができる。

【０２４１】

つぎに、ＨＤＤ２１が破壊した場合など、音楽コンテンツやコンテンツ鍵をＨＤＤ２１から再生することができなくなったときにおける音楽コンテンツの復元方法について説明する。

【０２４２】

まず、通常時において、包括管理ユニット（Ｘ）３１５は、暗号化した音楽コンテンツＣ及びコンテンツ鍵Ｋｃのバックアップデータを、ＨＤＤ２１内や他の記録媒体等に保存しておく。

【０２４３】

また、通常時において、包括管理ユニット（Ｘ）３１５は、ＥＭＤサーバ（Ｘ）４－３からダウンロードした音楽コンテンツの購入記録と、ＨＤＤ２１内に記憶している全ての音楽コンテンツのコンテンツＩＤのリストとを、使用ログ情報として管理する。このログ情報は、音楽コンテンツをＥＭＤサーバ（Ｘ）４－３からダウンロードしたときや、ポータブルデバイス（Ｘ）６－３への移動等の音楽コンテンツの制御を行ったときに、更新するようにする。また、ログ情報は、ＨＤＤ２１の別領域や他の記録媒体に格納しておく。包括管理ユニット（Ｘ）３１５は、このログ情報を、定期的、或いは、アクセスした度に、ＥＭＤサーバ（Ｘ）４－３にアップロードする。

【０２４４】

そして、包括管理ユニット（Ｘ）３１５のＨＤＤ２１に格納されている音楽コンテンツＣやコンテンツ鍵Ｋｃが破壊されてしまった場合には、以下に示すような処理が行われる。

【０２４５】

音楽コンテンツＣやコンテンツ鍵Ｋｃが破壊されてしまった場合、包括管理ユニット（Ｘ）３１５は、まず、ＥＭＤサーバ（Ｘ）４－３にアクセスを行って、ユーザ認証を行う。

【０２４６】

続いて、ＥＭＤサーバ（Ｘ）４－３は、認証したユーザのユーザＩＤから、包括管理ユニット（Ｘ）３１５の使用ログ情報を参照して、整合検証値ＩＣＶ（Integrity Check Value）を生成する。この整合検証値ＩＣＶは、使用ログ情報に記述されている音楽コンテンツＣのコンテンツＩＤであるＣＩＤと、包括管理ユニット（Ｘ）３１５のストレージ鍵ＫＳとに基づき、以下のように生成される。

ＩＣＶ＝Ｈ（ＫＳ，ＣＩＤ１｜｜ＣＩＤ２｜｜・・・｜｜ＣＩＤｎ）

ここで、Ｈ（Ｋ，Ｄａｔａ）は、一方向ハッシュ関数で、鍵Ｋによりその値が変化するものである。

【０２４７】

続いて、ＥＭＤサーバ（Ｘ）４－３は、生成した整合検証値ＩＣＶを、包括管理ユニット（Ｘ）３１５に送信する。

【０２４８】

続いて、包括管理ユニット（Ｘ）３１５は、音楽コンテンツＣ又はコンテンツ鍵Ｋｃがバックアップされていれば、そのバックアップデータをリストアして、音楽コンテンツＣ又

はコンテンツ鍵ＫｃをＨＤＤ２１内に保存する。また、音楽コンテンツＣ又はコンテンツ鍵Ｋｃがバックアップされていなければ、ＥＭＤサーバ（Ｘ）４－３から破壊された音楽コンテンツＣ又はコンテンツ鍵Ｋｃを再配信してもらう。このとき、ＥＭＤサーバ（Ｘ）４－３は、ユーザの購入履歴を参照して、以前に購入しているコンテンツであれば、課金処理を行わない。

【０２４９】

包括管理ユニット（Ｘ）３１５は、以上の処理を行い、破壊された音楽コンテンツＣ又はコンテンツ鍵Ｋｃを復活させる。

【０２５０】

そして、包括管理ユニット（Ｘ）３１５は、復活された音楽コンテンツＣ又はコンテンツ鍵Ｋｃの再生や制御を行う場合には、上記整合検証値ＩＣＶによりその音楽コンテンツのＣＩＤをチェックするようにする。このように、整合検証値ＩＣＶを用いて復活させた音楽コンテンツＣ又はコンテンツ鍵Ｋｃをチェックすることにより、例えば、ある音楽コンテンツＣｉをポータブルデバイス（Ｘ）６－３に移動してＨＤＤ２１上からは消去されている場合に、悪意のあるユーザが暗号化された音楽コンテンツＣｉであるＥ（Ｋｃｉ，Ｃｉ）を覚えておきリストアしたとしても、それらのデータは再生をすることもまた移動等の制御をすることもできない。

【０２５１】

なお、音楽コンテンツＣ及びコンテンツ鍵Ｋｃではなく、ストレージ鍵ＫＳが破壊されている場合には、包括管理ユニット（Ｘ）３１５の再インストールを行う。この場合であっても、ＥＭＤサーバ（Ｘ）４－３にユーザ登録をするとともにログ情報をアップロードしておけば、上述した方法でリストアや再ダウンロードをすることができる。

【０２５２】

このように、音楽コンテンツ配信システムでは、例えば、ハードディスクのクラッシュ等により、音楽コンテンツが破壊されてしまった場合であっても、著作権を保護しながら、復元することができる。例えば、その音楽コンテンツが正規に購入したものであれば、無料で復活させることができる。

【０２５３】

（５）包括管理ユニットのマスター鍵及び認証鍵等の配布方法

包括管理ユニット（Ｘ）３１５とポータブルデバイス（Ｘ）６－３との間では、ポータブルデバイス（Ｘ）６－３の固有のＩＤ及び認証鍵（ＭＧ－ＩＤ／ＩＫ）と、包括管理ユニット（Ｘ）３１５の固有のマスター鍵（ＯＭＧ－ＭＫ）とを用いて、相互認証が行われる。

【０２５４】

包括管理ユニット（Ｘ）３１５とポータブルデバイス（Ｘ）６－３との間で、相互認証が行われると、包括管理ユニット（Ｘ）３１５からポータブルデバイス（Ｘ）６－３へ音楽コンテンツを送信（チェックアウト）したり、ポータブルデバイス（Ｘ）６－３から包括管理ユニット（Ｘ）３１５への音楽コンテンツの返却（チェックイン）をしたりできるようになる。なお、包括管理ユニット（Ｘ）３１５は、パーソナルコンピュータ１のＨＤＤ２１内に暗号化した音楽コンテンツを保存しており、また、ポータブルデバイス（Ｘ）６－３は、内部のメモリカード等の記憶媒体に暗号化した音楽コンテンツを保存する。そのため、包括管理ユニット（Ｘ）３１５からポータブルデバイス（Ｘ）６－３へ音楽コンテンツを送信する場合には、パーソナルコンピュータ１のＨＤＤ２１上の音楽コンテンツが、ポータブルデバイス（Ｘ）６－３に装着されたメモリカード上に転送されることとなる。また、ポータブルデバイス（Ｘ）６－３から包括管理ユニット（Ｘ）３１５へ音楽コンテンツを送信する場合には、ポータブルデバイス（Ｘ）６－３に装着されたメモリカード上の音楽コンテンツが、パーソナルコンピュータ１のＨＤＤ２１上に転送されることとなる。

【０２５５】

ポータブルデバイス（Ｘ）６－３は、ＩＤ情報（ＭＧ－ＩＤ）、複数世代分の認証鍵（Ｍ

Ｇ－ＩＫ）及び複数世代分のマスター鍵（ＯＭＧ－ＭＫ）を工場出荷時から予め保持している。ポータブルデバイス（Ｘ）６－３には、後に外部からこれらの鍵等は供給されない。ポータブルデバイス（Ｘ）６－３は、必要に応じて、認証鍵（ＭＧ－ＩＫ）及びマスター鍵（ＯＭＧ－ＭＫ）の世代を更新する。
ポータブルデバイス（Ｘ）６－３は、世代更新された最も新しい世代の認証鍵及びマスター鍵で相互認証を行い、旧世代の認証鍵及びマスター鍵では、相互認証を行わない。以下、ポータブルデバイス（Ｘ）６－３は、第０世代から第９９世代の１００世代分の認証鍵（ＭＧ－ＩＫ［０－９９］）及びマスター鍵（ＯＭＧ－ＭＫ［０－９９］）を保持しているものとする。なお、第ｉ世代の認証鍵を（ＭＧ－ＩＫ［ｉ］）と示し、第ｉ世代のマスター鍵を（ＯＭＧ－ＭＫ［ｉ］）と示す。

【０２５６】
また、包括管理ユニット（Ｘ）３１５は、マスター鍵（ＯＭＧ－ＭＫ）を保持することによって、オーディオ用コンパクトディスク等からパーソナルコンピュータ１内に音楽コンテンツを転送して、保存することができる。また、包括管理ユニット（Ｘ）３１５は、マスター鍵（ＯＭＧ－ＭＫ）を保持することによって、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツをダウンロードして、パーソナルコンピュータ１内に保存することができる。

【０２５７】
ここで、包括管理ユニット（Ｘ）３１５では、コンパクトディスクから音楽コンテンツを転送することはできるがＥＭＤサーバ（Ｘ）４－３からは音楽コンテンツをダウンロードすることができないマスター鍵（ＯＭＧ－ＭＫ）と、コンパクトディスクからもＥＭＤサーバ（Ｘ）４－３からも音楽コンテンツを転送することができるマスター鍵（ＯＭＧ－ＭＫ）とが異なったものとなっている。以下、コンパクトディスクから音楽コンテンツを転送することはできるがＥＭＤサーバ（Ｘ）４－３からは音楽コンテンツをダウンロードすることができない鍵のことを、リッピング専用鍵ともいい、コンパクトディスクからもＥＭＤサーバ（Ｘ）４－３からも音楽コンテンツを転送することができる鍵のことをＥＭＤ鍵ともいう。

【０２５８】
なお、本例では、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）がリッピング専用鍵となっており、第１世代以後のマスター鍵（ＯＭＧ－ＭＫ［１～９９］）がＥＭＤ鍵となっている。

【０２５９】
つぎに、リッピング専用鍵を用いた処理の手順について説明する。

【０２６０】
包括管理ユニット（Ｘ）３１５がＣＤ－ＲＯＭからインストールされる場合には、図２７に示すように、包括管理ユニット（Ｘ）３１５のインストールソフトウェアが格納されたＣＤ－ＲＯＭ３６１とともに、ポータブルデバイス（Ｘ）６－３と、フロッピーディスク３６２とが例えばセットで販売される。フロッピーディスク３６２には、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ），第０世代の認証鍵（ＭＧ－ＩＫ［０］），第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）が格納されている。

【０２６１】
続いて、販売されたポータブルデバイス（Ｘ）６－３等を使用可能とするには、まず、ＣＤ－ＲＯＭ３６１をパーソナルコンピュータ１に装着する（ステップＳ１１）。続いて、このＣＤ－ＲＯＭ３６１から包括管理ユニット（Ｘ）３１５をパーソナルコンピュータ１にインストールする（ステップＳ１２）。すると、包括管理ユニット（Ｘ）３１５がパーソナルコンピュータ１のハードディスク内に格納されることとなる（ステップＳ１３）。続いて、フロッピーディスク３６２に格納されているポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とをパーソナルコンピュータ１に保存する（ステップＳ１４）。

【０２６２】

このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のハードディスク内に格納することができるようになる（ステップＳ１５）。なお、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）は、リッピング専用鍵なので、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツをダウンロードできないようになっている。

【０２６３】

また、ポータブルデバイス（Ｘ）６－３は、世代更新がされていく１００世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第０世代とされている。このため、第０世代の認証鍵及びマスター鍵を保持している包括管理ユニット（Ｘ）３１５と、ポータブルデバイス（Ｘ）６－３との相互認証が可能となる。したがって、音楽ＣＤ３６３等により提供される音楽コンテンツを、ポータブルデバイス（Ｘ）６－３のメモリーカードに格納することができるようになる（ステップＳ１６）。

【０２６４】

一方、包括管理ユニット（Ｘ）３１５がネットワークを介して提供される場合には、図２８に示すように、ポータブルデバイス（Ｘ）６－３とともに、インターネット上のＥＭＤ登録サーバ３のアドレス、ユーザＩＤ及びパスワード等が提供される。

【０２６５】

続いて、販売されたポータブルデバイス（Ｘ）６－３等を使用可能とするには、まず、ユーザＩＤ及びパスワードを用いてネットワーク上のＥＭＤ登録サーバ３にアクセスをする（ステップＳ２１）。続いて、ＥＭＤ登録サーバ３は、ユーザＩＤ及びパスワードの認証を行う（ステップＳ２２）。続いて、認証に問題がなければ、ＥＭＤ登録サーバ３は、包括管理ユニット（Ｘ）３１５のインストールソフトウェアと、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とを、パーソナルコンピュータ１に送信する（ステップＳ２３）。続いて、パーソナルコンピュータ１は、包括管理ユニット（Ｘ）３１５のインストールソフトウェアを起動して、包括管理ユニット（Ｘ）３１５をインストールするとともに、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とをＨＤＤ２１に保存する（ステップＳ２４）。すると、ハードディスクには、包括管理ユニット（Ｘ）３１５が格納されることとなる（ステップＳ２５）。

【０２６６】

このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のＨＤＤ２１内に格納することができるようになる（ステップＳ２６）。なお、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）は、リッピング専用鍵なので、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツをダウンロードできないようになっている。

【０２６７】

また、ポータブルデバイス（Ｘ）６－３は、世代更新がされていく１００世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第０世代とされている。このため、第０世代の認証鍵及びマスター鍵を保持している包括管理ユニット（Ｘ）３１５と、ポータブルデバイス（Ｘ）６－３との相互認証が可能となる。したがって、音楽ＣＤ３６３等により提供される音楽コンテンツを、ポータブルデバイス（Ｘ）６－３のメモリカード内に格納することができるようになる（ステップＳ２７）。

【０２６８】

なお、以上の図２７及び図２８に示した方法に限られず、包括管理ユニット（Ｘ）３１５及びリッピング専用の第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）をＣＤ－ＲＯＭ３６１に格納しておき、ポータブルデバイス（Ｘ）６－３との認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ）をネットワークを介して提供しても良い。

【０２６９】

つぎに、リッピング専用鍵をＥＭＤ鍵に鍵に更新して、ＥＭＤサーバ（Ｘ）４－３からダ

ウンロードした音楽コンテンツを取り扱えるようにする処理の手順について説明する。
【０２７０】
包括管理ユニット（Ｘ）３１５は、図２７又は図２８に示した手順により、ＣＤ－ＲＯＭ等のリムーバブルメディアやインターネット等のネットワークを介して提供され、パーソナルコンピュータ１内のＨＤＤ２１にインストールされている。このとき包括管理ユニット（Ｘ）３１５は、リッピング専用である第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）と、認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ［０］）とを保持しており、ポータブルデバイス（Ｘ）６－３の鍵の世代もデフォルトのままである。
【０２７１】
まず、パーソナルコンピュータ１は、図２９に示すように、ユーザＩＤ及びパスワードを用いてネットワーク上のＥＭＤ登録サーバ３にアクセスをする（ステップＳ３１）。続いて、ＥＭＤ登録サーバ３は、ユーザＩＤ及びパスワードの認証を行う（ステップＳ３２）。続いて、認証に問題がなければ、ＥＭＤ登録サーバ３は、パーソナルコンピュータ１のＩＤ情報（ＯＭＧ－ＩＤ）を登録し、包括管理ユニット（Ｘ）３１５がＥＭＤサーバ（Ｘ）４－３と接続するための公開鍵（ＯＭＧ－ＰＫ）、秘密鍵（ＯＭＧ－ＫＳ）及び公開鍵の認証書（Ｃｅｒｔ［ＰＫ］）を生成する（ステップＳ３３）。続いて、ＥＭＤ登録サーバ３は、生成した公開鍵（ＯＭＧ－ＰＫ）、秘密鍵（ＯＭＧ－ＫＳ）及び公開鍵の認証書（Ｃｅｒｔ［ＰＫ］）を、パーソナルコンピュータ１に送信する（ステップＳ３４）。
【０２７２】
続いて、ＥＭＤ登録サーバ３は、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ），第ｉ世代の認証鍵（ＭＧ－ＩＫ［ｉ］），第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）をパーソナルコンピュータ１に送信する（ステップＳ３５）。続いて、パーソナルコンピュータ１の包括管理ユニット（Ｘ）３１５は、受信したＩＤ情報（ＭＧ－ＩＤ），第ｉ世代の認証鍵（ＭＧ－ＩＫ［ｉ］），第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）に基づき、これらの鍵を第ｉ世代に世代更新する（ステップＳ３６）。続いて、包括管理ユニット（Ｘ）３１５は、ポータブルデバイス（Ｘ）６－３との間で認証を行う（ステップＳ３７）。ポータブルデバイス（Ｘ）６－３は、認証がされると、自己の鍵の世代を第ｉ世代に更新する（ステップＳ３８）。
【０２７３】
このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のハードディスク内に格納することができるとともに、ＥＭＤサーバ（Ｘ）４－３からダウロードした音楽コンテンツをパーソナルコンピュータ１のＨＤＤ２１に格納することができるようになる。
【０２７４】
つぎに、ＥＭＤ鍵等の世代更新をする手順について説明する。
【０２７５】
包括管理ユニット（Ｘ）３１５は、第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）と、認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ［ｉ］）とを保持しており、ポータブルデバイス（Ｘ）６－３の鍵の世代も第ｉ世代となっている。
【０２７６】
まず、図３０に示すように、パーソナルコンピュータ１が何らかの処理のため、ＥＭＤ登録サーバ３にアクセスすると、ＥＭＤ登録サーバ３は、包括管理ユニット（Ｘ）３１５のＩＤを認証して、第（ｉ＋ｋ）世代の認証鍵（ＭＧ－ＩＫ［ｉ＋ｋ］）及び第（ｉ＋ｋ）世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ＋ｋ］）をパーソナルコンピュータ１に送信する（ステップＳ４１）。続いて、パーソナルコンピュータ１の包括管理ユニット（Ｘ）３１５は、受信した認証鍵及びマスター鍵を、第（ｉ＋ｋ）世代に更新する（ステップＳ４２）。続いて、包括管理ユニット（Ｘ）３１５は、ポータブルデバイス（Ｘ）６－３と認証を行う（ステップＳ４３）。ポータブルデバイス（Ｘ）６－３は、認証がされると、自己の鍵の世代を第ｉ世代から第（ｉ＋ｋ）世代に更新する（ステップＳ４４）。
【０２７７】

また、図３１に示すように、一方、ポータブルデバイス（Ｘ）６－３が用いている認証鍵等の世代が第（ｉ＋ｋ）世代となっており、包括管理ユニット（Ｘ）３１５が保持している認証鍵等の世代が第ｉ世代となっている場合には、ポータブルデバイス（Ｘ）６－３と包括管理ユニット（Ｘ）３１５との認証が行われると、認証失敗となる（ステップＳ５１）。認証を失敗すると、包括管理ユニット（Ｘ）３１５は、ＥＭＤ登録サーバ３に対して、鍵要求を行う（ステップＳ５２）。鍵要求があると、ＥＭＤ登録サーバ３は、包括管理ユニット（Ｘ）３１５のＩＤを認証して、第（ｉ＋ｋ）世代の認証鍵（ＭＧ－ＩＫ［ｉ＋ｋ］）及び第（ｉ＋ｋ）世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ＋ｋ］）を送信する（ステップＳ５３）。続いて、包括管理ユニット（Ｘ）３１５は、受信した認証鍵及びマスター鍵を、第（ｉ＋ｋ）世代に更新する（ステップＳ５４）。続いて、包括管理ユニット（Ｘ）３１５は、ポータブルデバイス（Ｘ）６－３と認証を行う（ステップＳ５５）。

【０２７８】

このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のハードディスク内に格納することができるとともに、ＥＭＤサーバ（Ｘ）４－３からダウンロードした音楽コンテンツをパーソナルコンピュータ１のＨＤＤ２１に格納することができるようになる（ステップＳ３８）。

【０２７９】

以上のように、音楽コンテンツ配信システムでは、包括管理ユニット（Ｘ）３１５及びポータブルデバイス（Ｘ）６－３が用いるマスター鍵及び認証鍵を、リッピング専用の鍵とサーバ接続鍵とに分け、さらに、サーバ接続鍵をネットワークを介してダウンロードするようにしている。このため、音楽コンテンツ配信システムでは、サーバから配信された音楽コンテンツの安全性が高まり、例えば、リッピング専用の鍵が破られたとしても、サーバからダウンロードされる音楽コンテンツを破ることができない。

【０２８０】

また、音楽コンテンツ配信システムでは、包括管理ユニット（Ｘ）３１５及びポータブルデバイス（Ｘ）６－３が用いるマスター鍵及び認証鍵を、世代更新させて用いている。さらに、包括管理ユニット（Ｘ）３１５は、マスター鍵及び認証鍵がネットワークを介して供給され、世代更新を行う。このため、音楽コンテンツの安全性が高まる。

【０２８１】

【発明の効果】

本発明によれば、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元又は再配信されたコンテンツデータの再生及び／又は制御を行う。

【０２８２】

このことにより、本発明では、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態の音楽コンテンツ配信システムの構成を示す図である。

【図２】上記音楽コンテンツ配信システムにおけるパーソナルコンピュータの構成を示す図である。

【図３】上記音楽コンテンツ配信システムにおけるポータブルデバイスの構成を示す図である。

【図４】上記パーソナルコンピュータの機能について説明する図である。

【図５】表示操作指示ウィンドウの一例を示す図である。

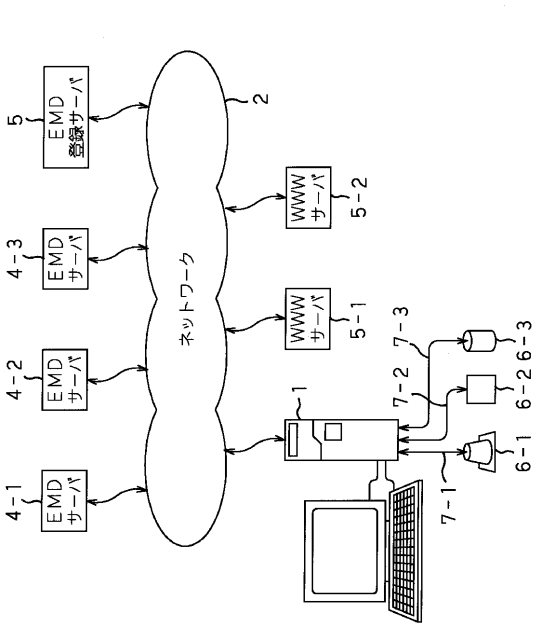
【図６】録音プログラムがディスプレイに表示させる表示例を示す図である。

【図７】上記音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて説明するための図である。

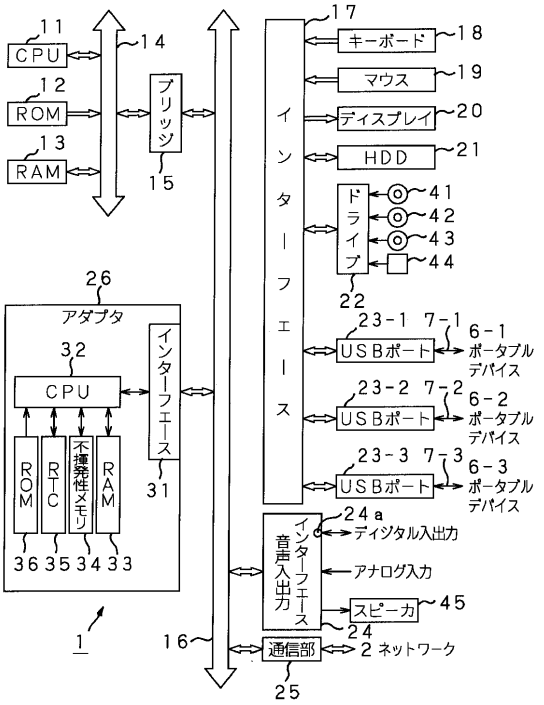
【図８】統一転送プロトコルレイヤとアプリケーションレイヤとの関係を説明する図であ

る。
【図９】一般的に用いられる利用条件情報のフォーマットを説明する図である。
【図１０】包括管理ユニットで用いられる統一利用条件情報を構成するファイルを説明する図である。
【図１１】上記統一利用条件情報のオートマトンファイルの構成を説明する図である。
【図１２】上記オートマトンファイルのオートマトン記述部に記述される音楽コンテンツの動作遷移を示すオートマトンの一例を説明する図である。
【図１３】上記オートマトンをｔｕｐｌｅ列で表現した図である。
【図１４】上記オートマトン記述部の構成を説明する図である。
【図１５】ＸＭＬの仕様に基づいて規定されたＤＴＤで定義されているイベントとコマンドとを示す図である。
【図１６】上記オートマトン記述部の第１の記述例を示す図である。
【図１７】上記第１の記述例の状態遷移図である。
【図１８】上記オートマトン記述部の第２の記述例を示す図である。
【図１９】上記第２の記述例の状態遷移図である。
【図２０】上記オートマトン記述部の第３の記述例を示す図である。
【図２１】上記第３の記述例の状態遷移図である。
【図２２】上記オートマトン記述部の第４の記述例を示す図である。
【図２３】上記統一利用条件情報のパラメータファイルの構成を説明する図である。
【図２４】上記パラメータファイルを更新した場合の構成を説明する図である。
【図２５】上記パラメータファイルのパラメータ記述部の構成を説明する図である。
【図２６】上記包括管理ユニットによるコンテンツの管理方法について説明する図である。
【図２７】包括管理ユニットがＣＤ－ＲＯＭからインストールされる場合の処理手順について説明する図である。
【図２８】包括管理ユニットがネットワークからダウンロードされてインストールされる場合の処理手順について説明する図である。
【図２９】リッピング鍵からＥＭＤ鍵に更新する更新手順について説明する図である。
【図３０】ＥＭＤ鍵を更新する手順の第１の例について説明する図である。
【図３１】ＥＭＤ鍵を更新する手順の第２の例について説明する図である。
【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、４ＥＭＤサーバ、６　ポータブルデバイス、７　ＵＳＢインターフェース、２１ハードディスク、３１１，３１２　再生用アプリケーション、３１３，３１４デバイスドライバ、３１５　包括管理ユニット、３１６　ＥＭＤ用受信インターフェース、３１７　ＥＭＤ用送信インターフェース、３１８　ＰＤドライバ

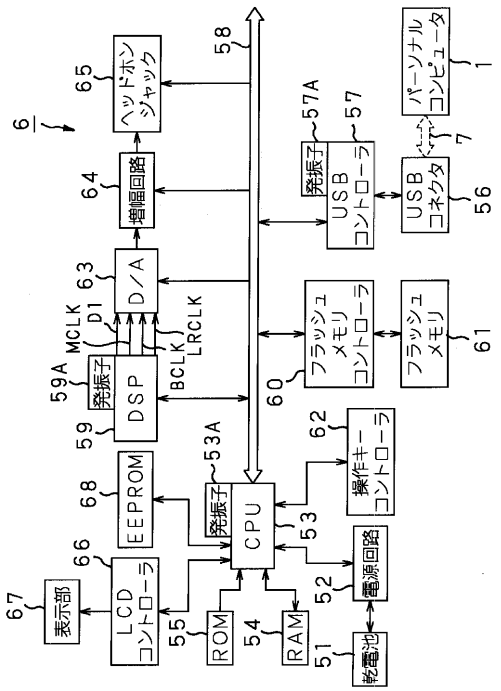
【図１】


ネットワーク
EMD 登録サーバ
EMD サーバ
WWW サーバ
CPU
ROM
RAM
フラッシュメモリ
インターフェース
キーボード
マウス
ディスプレイ
HDD
ライブラリ
USBポート
ポータブルデバイス
ディジタル入出力
アナログ入力
スピーカ
音声入出力インターフェース
通信部

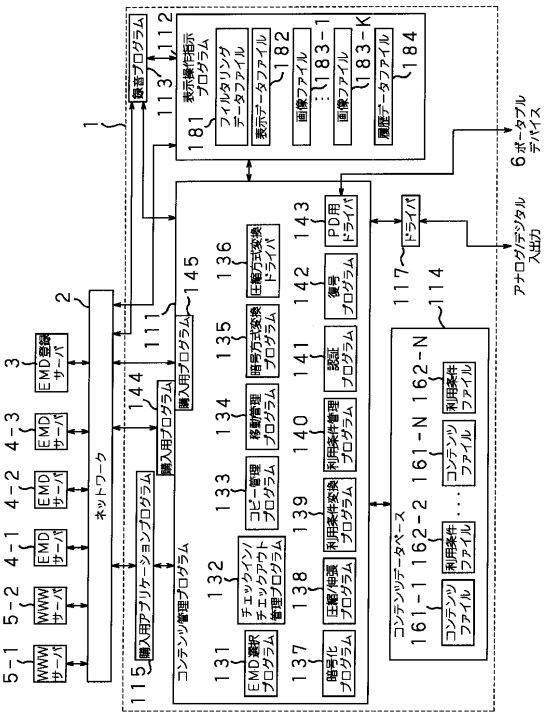
【図２】


CPU
ROM
RAM
バス
インターフェース
キーボード
マウス
ディスプレイ
HDD
ライブラリ
USBポート
ポータブルデバイス
アダプタ
ディジタル入出力
アナログ入力
スピーカ
音声入出力インターフェース
通信部
ネットワーク

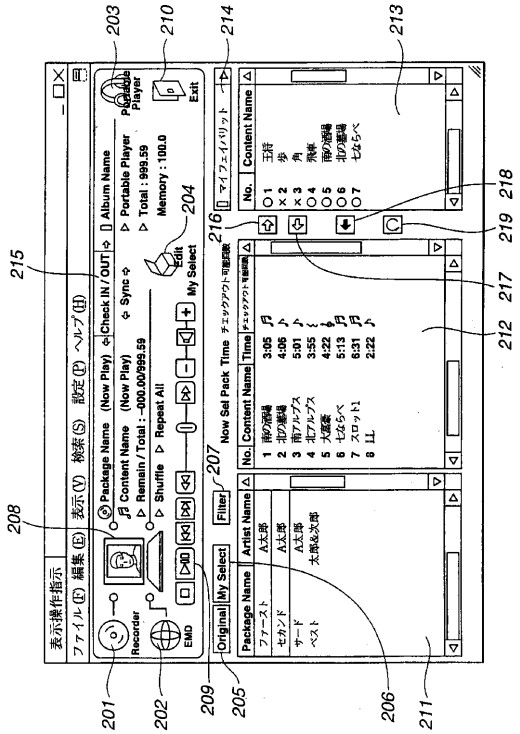
【図３】


CPU
ROM
RAM
EEPROM
DSP
D/A
増幅回路
ヘッドホンジャック
LCDコントローラ
表示部
乾電池
電源回路
操作キーコントローラ
フラッシュメモリコントローラ
フラッシュメモリ
USBコントローラ
USBコネクタ
パーソナルコンピュータ
発振子
MCLK
BCLK
LRCLK

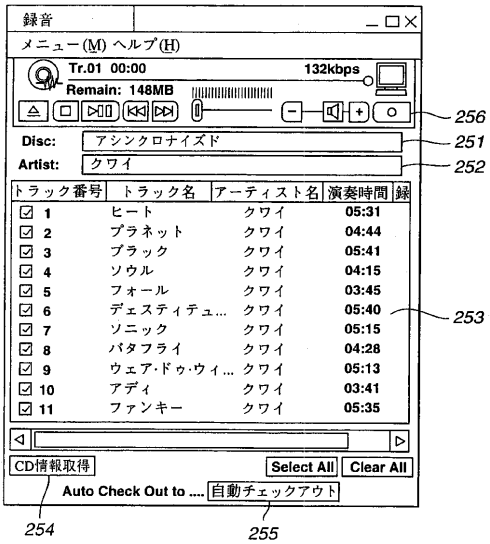
【図４】


ネットワーク
WWWサーバ
EMDサーバ
EMD登録サーバ
購入用アプリケーションプログラム
コンテンツ管理プログラム
購入用プログラム
着音プログラム
表示操作指示プログラム
フィルタリングデータファイル
表示データファイル
画像ファイル
履歴データファイル
コンテンツデータベース
コンテンツファイル
利用条件ファイル
ドライバ
PD用ドライバ
ポータブルデバイス
アナログディジタル入出力

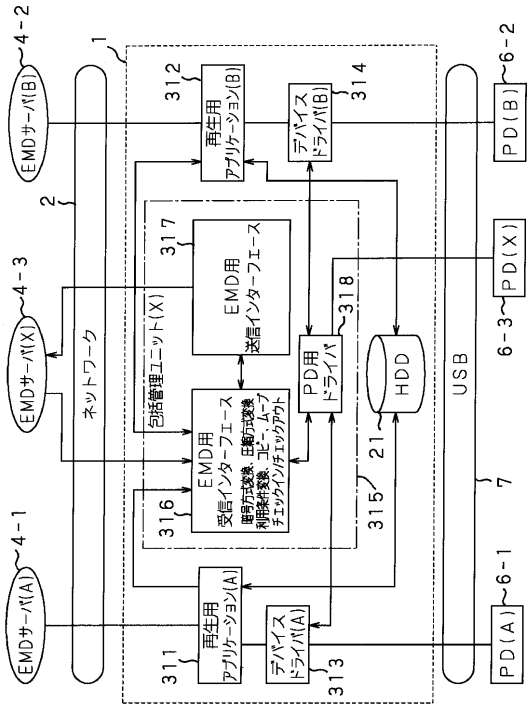
【図５】


201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219

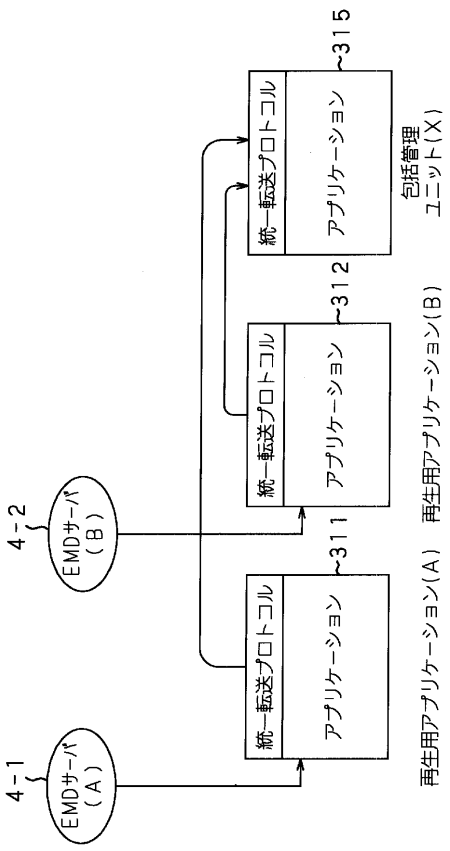
【図６】


録音
メニュー(M) ヘルプ(H)
Tr.01 00:00
132kbps
Remain: 148MB
Disc: アシンクロナイズド
Artist: クワイ
トラック番号 トラック名 アーティスト名 演奏時間 録
1 ヒート クワイ 05:31
2 プラネット クワイ 04:44
3 ブラック クワイ 05:41
4 ソウル クワイ 04:15
5 フォール クワイ 03:45
6 デェスティテュ... クワイ 05:40
7 ソニック クワイ 05:15
8 バタフライ クワイ 04:28
9 ウェア・ドゥ・ウィ... クワイ 05:13
10 アディ クワイ 03:41
11 ファンキー クワイ 05:35
CD情報取得
Select All
Clear All
Auto Check Out to .... 自動チェックアウト
251
252
253
254
255
256

【図７】


EMDサーバ(A) 4-1
EMDサーバ(X) 4-3
EMDサーバ(B) 4-2
ネットワーク
1
2
再生用アプリケーション(A) 311
デバイスドライバ(A) 313
再生用アプリケーション(B) 312
デバイスドライバ(B) 314
包括管理ユニット(X) 317
EMD用送信インターフェース
EMD用受信インターフェース 316
PD用ドライバ 318
HDD 21
USB 7
PD(A) 6-1
PD(X) 6-3
PD(B) 6-2
315

【図８】


EMDサーバ(A) 4-1
EMDサーバ(B) 4-2
統一転送プロトコル
アプリケーション 311
統一転送プロトコル
アプリケーション 312
統一転送プロトコル
アプリケーション 315
再生用アプリケーション(A)
再生用アプリケーション(B)
包括管理ユニット(X)

【図９】

(a)

ポリシー	値
from	99/10/25
to	99/11/24
pay/play	yes/10円

(b)

コンテンツ
利用条件情報

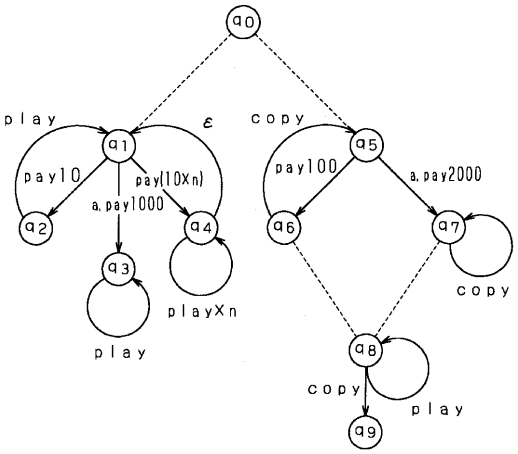
【図１０】

インデックスファイル	～331
オートマトンファイル	～332
パラメータファイル	～333
履歴ファイル	～334

【図１１】

Automaton	～341
MAC_{Kc}(Automaton)	～342
$Sig_{K_E^{-1}}$(Automaton)	～343
Cert(K_E^1)	～344

【図１２】



【図１３】

$\langle q_1, pay10, q_2 \rangle$
$\langle q_1, a.pay1000, q_3 \rangle$
$\langle q_1, pay(10 \times n), q_4 \rangle$
$\langle q_2, play, q_1 \rangle$
$\langle q_3, play, q_3 \rangle$
$\langle q_4, play \times n, q_4 \rangle$
$\langle q_4, \varepsilon, q_1 \rangle$
$\langle q_5, pay100, q_6 \rangle$
$\langle q_5, a.pay2000, q_7 \rangle$
$\langle q_6, copy, q_5 \rangle$
$\langle q_7, copy, q_7 \rangle$
$\langle q_8, play, q_8 \rangle$
$\langle q_8, copy, q_9 \rangle$

【図１４】

Entity ID	～345
Content ID	～346
Automaton Version	～347
Variables	～348
Tuples	～349
Automaton Version	～347
Variables	～348
Tuples	～349
⋮	

【図１５】

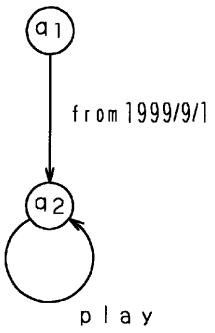
```
〈!ENTITY % event" (
    play                    |
    copy                    |
    pay-for-play            |
    pay-for-copy            |
    pay-for-album-play      |
    pay-for-album-copy      |
    from                    |
    to                      |
    null
)"〉

〈!ENTITY % command" (
    drop                |
    dup                 |
    swap                |
    add                 |
    subtract            |
    multiply            |
    divide              |
    remainder           |
    upper               |
    lower               |
    equal               |
    less                |
    greater             |
    less-equal          |
    greater-equal       |
    and                 |
    or                  |
    not                 |
    bit-and             |
    bit-or              |
    bit-xor             |
    bit-not
)"〉
```

【図１６】

Content playable from 1999/9/1

```
〈automaton〉

  〈!—This usage rule system has one Right Unit.
   Initial state is q1--〉
  〈initial-right-unit state="q1"/〉

  〈node state="q1"〉
    〈!—If after 1999/9/1, transfer to q2--〉
    〈rule event="from" next-state="q2"〉
      〈arguments〉
        〈integer value="time:19990901"/〉
      〈/arguments〉
    〈/rule〉
  〈/node〉

  〈node state="q2"〉
    〈!--Playable--〉
    〈rule event="play" next-state="q2"/〉
  〈/node〉

〈/automaton〉
```

【図１７】

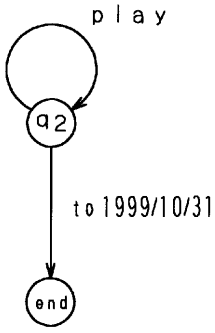


【図１８】

Content playable unil 1999/10/31

```
〈automaton〉

  〈!--This Usage Rule System has one Right Unit.
   Initial state is q2--〉
  〈initial-right-unit state="q2"/〉

  〈node state="q2"〉
    〈!—If after 1999/10/31, transfer to end--〉
    〈rule event="to" next-state="end"〉
      〈arguments〉
        〈integer value="time:19991031"/〉
      〈/arguments〉
    〈/rule〉

    〈!--Playable--〉
    〈rule event="play" next-state="q2"〉
    〈/rule〉
  〈/node〉

  〈!—Unusable state--〉
  〈node state="end"/〉

〈/automaton〉
```

【図１９】

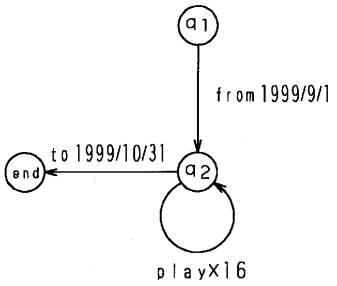


【図２０】

Content playable 16times 1999/9/1 to 1999/10/31

```
<automaton>

  <!-Define counter variables for playable numbers. Initial value is 16-->
  <define-variable name="count" initial-value="16"/>

  <!-This Usage Rule System has one Right Unit. Initial state is q1-->
  <initial-right-unit state="q1"/>

  <node state="q1">
    <!-From 1999/9/1 transfer to q2-->
    <rule event="from" next-state="q2">
      <arguments>
        <integer value="time 19990901"/>
      </arguments>
    </rule>
  </node>

  <node state="q2">
    <!-From 1999/10/31 transfer to end-->
    <rule event="to" next-state="end">
      <arguments>
        <integer value="time 19991031"/>
      </arguments>
    </rule>

    <rule event="play" next-state="q2">
      <!-playable only for "count" numbers-->
      <arguments>
        <variable name="count"/>
        <command name="load"/>
      </arguments>
      <!-If this rule is selected, the "count" number decrements by one-->
      <action>
        <variable name="count"/>
        <command name="load"/>
        <integer value="1"/>
        <command name="subtract"/>
        <variable name="count"/>
        <command name="store"/>
      </action>
    </rule>
  </node>

  <!-Unusable state-->
  <node state="end"/>

</automaton>
```

【図２１】

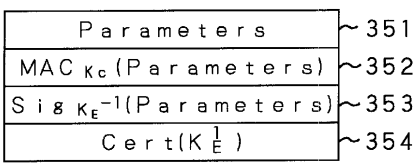


【図２２】

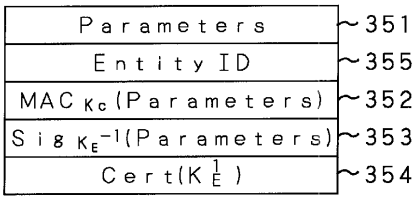
Content playable less than and/or equal to 16times

```
<automaton>

  <!-Define valuable counter for playable numbers.
   Initial value is 16-->
  <define-variable name="count" initial-value="16"/>

  <!--Usage Rule System has one Right Unit.
   Initial state is q2-->
  <initial-right-unit state="q1"/>

  <node state="q2">
    <rule event="play" next-state="q2">
      <!-"Count" number of times playable-->
      <arguments>
        <variable name="count"/>
        <command name="load"/>
      </arguments>
      <!-If this rule is selected, "count"
       number decrements by one-->
      <action>
        <variable name="count"/>
        <command name="load"/>
        <integer value "1"/>
        <command name="subtract"/>
        <variable name="count"/>
        <command name="store"/>
      </action>
    </rule>
  </node>

</automaton>
```

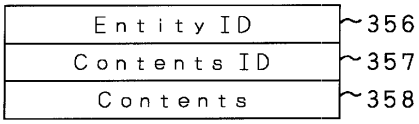
【図２３】



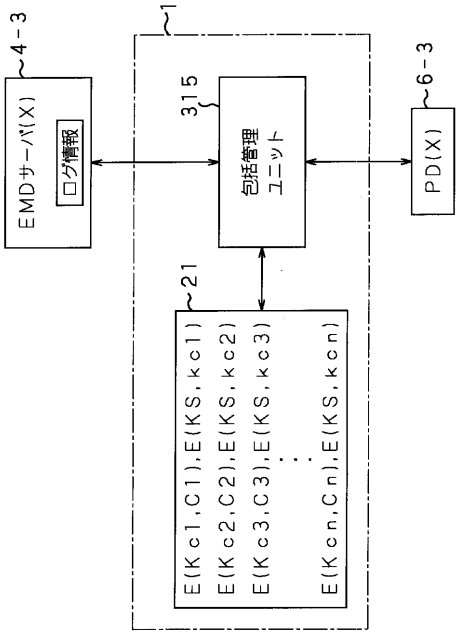
【図２４】



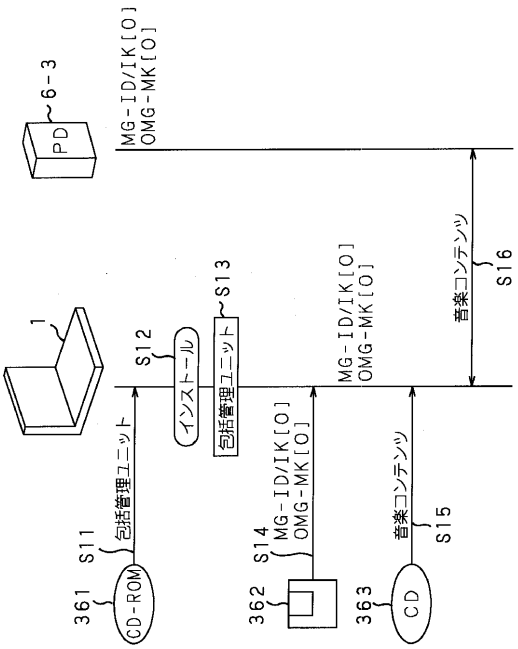
【図２５】



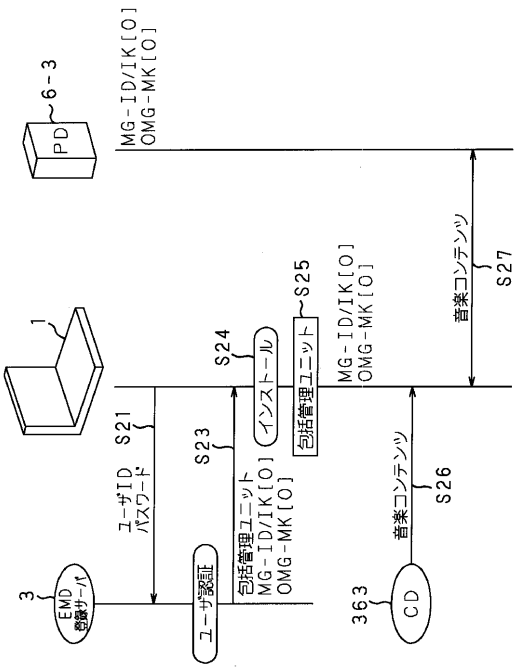
【図２６】



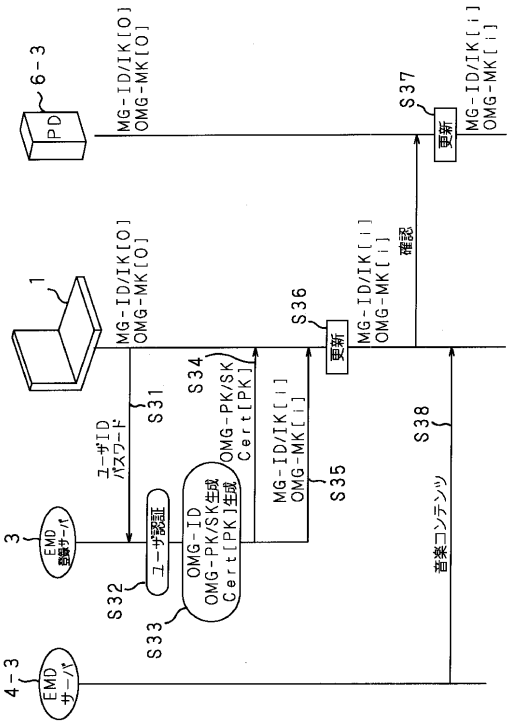
【図２７】



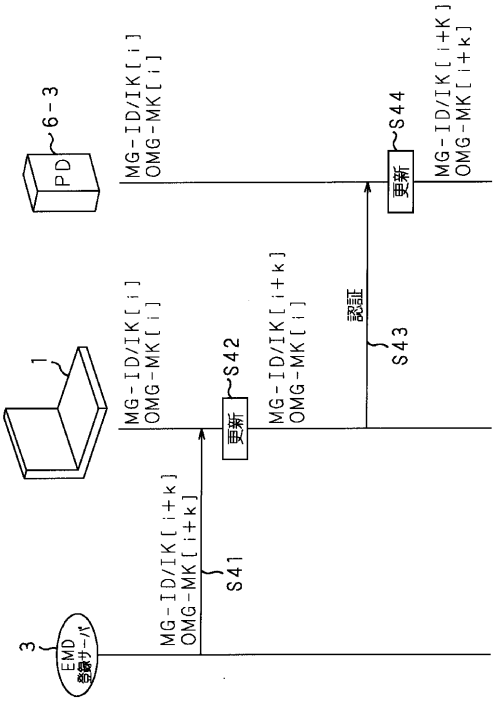
【図２８】



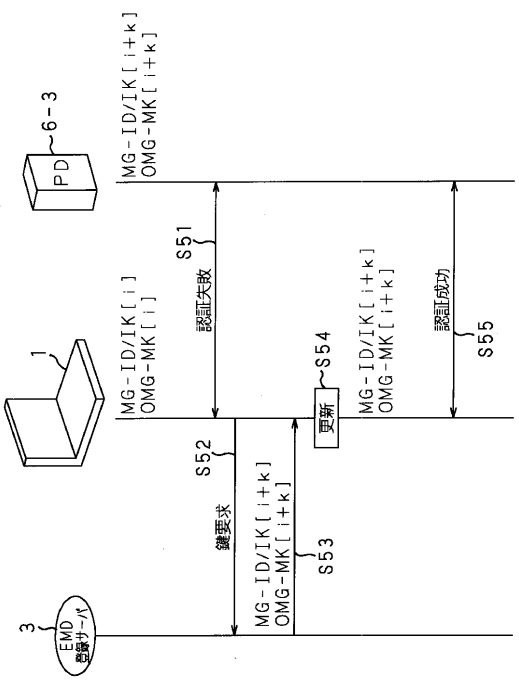
【図２９】



【図３０】


6-3
PD
MG-ID/IK[i]
OMG-MK[i]
S44
更新
MG-ID/IK[i+K]
OMG-MK[i+k]
1
MG-ID/IK[i]
OMG-MK[i]
S42
更新
MG-ID/IK[i+k]
OMG-MK[i]
認証
S43
MG-ID/IK[i+k]
OMG-MK[i+k]
S41
3
EMD
鍵サーバ

【図３１】


6-3
PD
MG-ID/IK[i+k]
OMG-MK[i+k]
S51
認証失敗
1
MG-ID/IK[i]
OMG-MK[i]
S54
更新
MG-ID/IK[i+k]
OMG-MK[i+k]
認証成功
S55
S52
鍵要求
MG-ID/IK[i+k]
OMG-MK[i+k]
S53
3
EMD
鍵サーバ

フロントページの続き

(72)発明者　田辺　充
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(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
(72)発明者　佐藤　一郎
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　海老原　宗毅
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　阿部　潤

(56)参考文献　特開平１０－２２２０６３（ＪＰ，Ａ）
特開平０７－１３１４５２（ＪＰ，Ａ）
特開平０８－３０７５５８（ＪＰ，Ａ）
特開平１１－０８５５０４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q　30/00