

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 8 月 29 日 (29.08.2002)

PCT

(10) 国際公開番号
WO 02/067256 A1

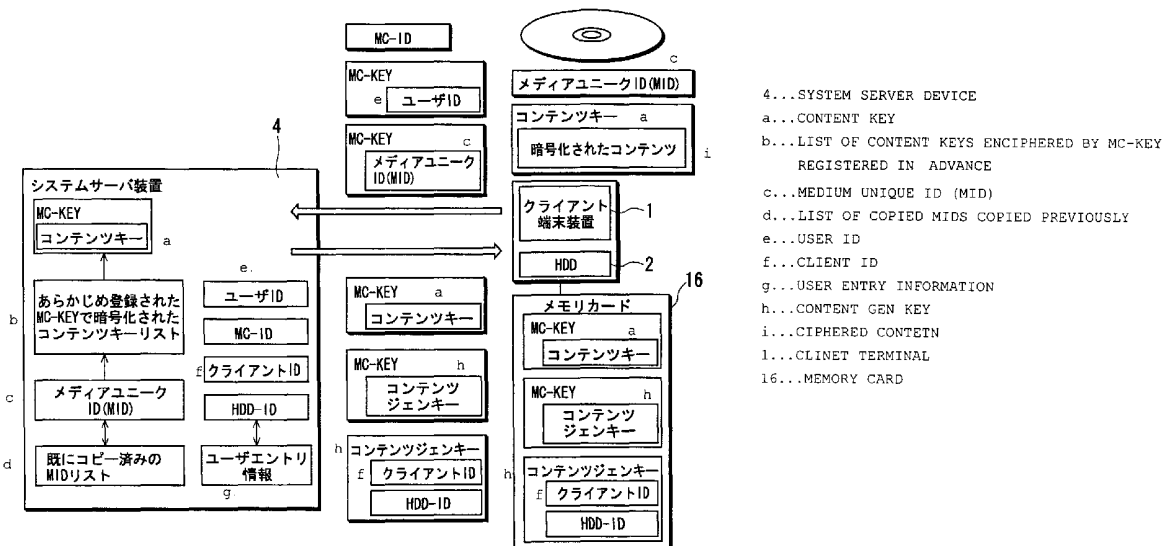
- (51) 国際特許分類: G11B 20/10, G06F 9/06, 12/14, 15/00
- (21) 国際出願番号: PCT/JP02/01452
- (22) 国際出願日: 2002 年 2 月 20 日 (20.02.2002)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2001-44358 2001 年 2 月 20 日 (20.02.2001) JP
特願2002-41890 2002 年 2 月 19 日 (19.02.2002) JP
- (71) 出願人: 株式会社ソニー・コンピュータエンタテインメント (SONY COMPUTER ENTERTAINMENT INC.) [JP/JP]; 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 Tokyo (JP).
- (72) 発明者: 島田 宗毅 (SHIMADA, Muneki); 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・

コンピュータエンタテインメント内 Tokyo (JP). 岡本伸一 (OKAMOTO, Shinichi); 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内 Tokyo (JP). 吉森 正治 (YOSHIMORI, Masaharu); 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内 Tokyo (JP). 犬井 努 (INUI, Tsutomu); 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内 Tokyo (JP). 島川 恵三 (SHIMAKAWA, Keiso); 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内 Tokyo (JP). 岡田 豊史 (OKADA, Toyoshi); 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内 Tokyo (JP). 九保 亮 (KUBO, Makoto); 〒107-0052 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内 Tokyo (JP). 中村 光宏 (NAKAMURA, Mitsuhiro); 〒107-0052

[続葉有]

(54) Title: COMPUTER PROGRAM COPY MANAGEMENT SYSTEM

(54) 発明の名称: コンピュータプログラムのコピー管理システム



(57) Abstract: An ID (MID) is given to an optical disk, a content is enciphered by using a content key, and the ciphered content is recorded. A system server device manages, as user entry information, the client ID of a client terminal, the HDD-ID of an HDD, and MC-ID of a memory card all of which a user has. When the user copies a content, the user sends the MID of the optical disk and the MC-ID to the system server device. The system server device collates the MC-ID with the user entry information to identify the user and sends as a reply the content key used when the content is enciphered. The user decipheres the content recorded in an optical disk by means of the sent content key and copies it in an HDD. Thus, only the authenticated user who has a storage medium is permitted to copy the content.

[続葉有]



東京都 港区 赤坂 7 丁目 1 番 1 号 株式会社ソニー・
コンピュータエンタテインメント内 Tokyo (JP).

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

(74) 代理人: 米山 尚志 (YONEYAMA, Hisashi); 〒160-0022
東京都 新宿区 新宿 6 丁目 2 9 番 8 号 新宿福智ビル
5 階 Tokyo (JP).

添付公開書類:
— 国際調査報告書
— 補正書・説明書

(81) 指定国 (国内): AU, BR, CA, CN, IN, KR, MX, NZ, RU,
SG.

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

(57) 要約:

各光ディスク毎に I D (MID) を付すと共に、コンテンツを Content-Key で暗号化して記録しておく。また、システムサーバ装置は、ユーザが所有するクライアント端末装置のクライアント I D, H D D の HDD-ID、及びメモ리카ードの MC-ID 等をユーザエントリ情報として管理する。ユーザはコンテンツのコピーを行う際に、光ディスクの MID と共に MC-ID をシステムサーバ装置側に送付する。システムサーバ装置は、MC-ID をユーザエントリ情報と照合してユーザを特定し、コンテンツの暗号化の際に用いた Content-Key を返送する。ユーザ側では、この返送された Content-Key を用いて光ディスクに記録されているコンテンツを復号化し H D D にコピーする。これにより、記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーを許可することができる。

明細書

コンピュータプログラムのコピー管理システム

技術分野

- 5 本発明は、例えばゲームコンテンツ、映画コンテンツ、音楽コンテンツ、アプリケーションプログラム等のコンピュータプログラムのコピー管理を行うコピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、クライアント端末装置の情報処理プログラム、管理サーバ装置の情報処理プログラム、及びコピー管理方法に関する。
- 10

背景技術

- 15 今日において、例えばCD-ROM、DVD-ROM或いは半導体メモリ等の記憶媒体に記憶されているゲームコンテンツに基づいてビデオゲームを実行するビデオゲーム機が広く普及している。

- ユーザは、所望のゲームコンテンツが記憶された記憶媒体を購入し、この記憶媒体をビデオゲーム機で再生してビデオゲームを行う。大抵の場合、ユーザは、徐々に新しいビデオゲームを買い揃えていく。このため、月日と共にユーザの手元には各ゲームコンテンツが記憶された記憶媒体が蓄積されていくこととなる。
- 20

- しかし、ビデオゲーム機には、記憶媒体の再生機構が1基のみ設けられている場合が多い。このため、異なるビデオゲームを行う場合には、ビデオゲーム機に現在装着されている記憶媒体を取
- 25

り出し、これから行おうとするゲームコンテンツが記憶された記憶媒体を新たに装着し直すという、大変面倒な作業を必要としていた。

5 本件出願人は、例えば数十G（ギガ）オーダーの大容量のハードディスクドライブ（HDD）を内蔵或いは外付け可能としたビデオゲーム機を開示している。

このビデオゲーム機の場合、各記憶媒体に記憶されているゲームコンテンツをそれぞれHDDにコピーし、このHDDから所望のゲームコンテンツを再生して利用することができる。このHDD
10 Dを用いることにより、ビデオゲーム機の再生機構に記憶媒体を着脱する手間を省略することができる。

ここで、ゲームコンテンツ等のコンピュータプログラムは、そのコンピュータプログラムが記憶されたソフトウェアを購入する等して正当に入手したユーザのみが使用可能なはずである。
15 しかし、記憶媒体に記憶されたコンピュータプログラムを二次記憶媒体にコピー可能とした場合、一つの記憶媒体に記憶されているコンピュータプログラムを、複数のユーザがそれぞれ二次記憶媒体にコピーして使用する不正コピーが懸念される。

本発明は、正当なユーザに対してのみ、コンピュータプログラムのコピーを可能とするコピー管理を行うことで、コンテンツの不正使用の防止等を図ったコピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、クライアント端末
20 装置の情報処理プログラム、管理サーバ装置の情報処理プログラム、及びコピー管理方法の提供を目的とする。

発明の開示

本発明は、暗号化鍵で暗号化したコンテンツを記憶させた記憶媒体に対して固有の識別番号を付してユーザに配布する。ユーザ
5 がコンテンツのコピーを行う際に使用するデバイスにも識別番号が付されている。

上記デバイスは、コンテンツのコピーを行う際に、上記記憶媒体の識別番号、及びデバイスの識別番号を管理サーバ装置に送信する。管理サーバ装置は、各ユーザが使用するデバイスの識別番号
10 が登録されたデータベースを有している。管理サーバ装置は、データベースに登録されているデバイスの識別番号と、ユーザのデバイスから送信されたデバイスの識別番号とを照合してユーザを特定する。管理サーバ装置は、この照合を行うことでユーザが特定された際に、記憶媒体に記憶されているコンテンツを復号
15 化するための復号化鍵をユーザのデバイスに送信する。

ユーザのデバイスは、この管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してコンテンツのコピーを行う。

これにより、記憶媒体の持ち主である正規のユーザにのみ、コ
20 ンテンツのコピーを許可することができ、コンテンツの不正コピーを防止することができる。

図面の簡単な説明

図 1 は、本発明の第 1 の実施の形態のコピー管理システムのシステム構成を示すブロック図である。
25

図 2 は、コピー管理システムを構成するクライアント端末装置

及びハードディスクドライブ（HDD）の外観を示す斜視図である。

図3は、クライアント端末装置の電氣的な構成を示すブロック図である。

5 図4は、コンテンツキー（Content-Key）で暗号化されたコンテンツが記憶された、このコピー管理システムに用いられる光ディスクを説明するための図である。

図5は、コピー管理システムにおけるユーザ登録の流れを示すフローチャートである。

10 図6は、ユーザ登録時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

図7は、コピー管理システムにおける、光ディスクに個別に付されたメディアユニークID（MID）の登録動作と、コンテンツキー（Content-Key）の取得動作を示すフローチャートである。

15 図8は、光ディスクに個別に付されたメディアユニークID（MID）の登録時、及びコンテンツキー（Content-Key）の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

図9は、コピー管理システムにおけるコピー実行時の流れを示すフローチャートである。

25 図10は、コピー実行時にクライアント端末装置、メモリカード及びハードディスクドライブの間で送受信される各情報を示す模式図である。

図 1 1 は、コピー管理システムにおける、ハードディスクドライブにコピーしたコンテンツの再生動作を示すフローチャートである。

図 1 2 は、ハードディスクドライブにコピーしたコンテンツの再生時に、クライアント端末装置、メモ리카ード及びハードディスクドライブの間で送受信される情報を示す模式図である。

図 1 3 は、クライアント端末装置或いはハードディスクドライブの修理或いは交換に対するコピー管理システムの対応を説明するための模式図である。

図 1 4 は、メモ리카ードの破損或いは紛失に対するコピー管理システムの対応を説明するための模式図である。

図 1 5 は、光ディスクに個別に付されたメディアユニーク I D (M I D) の登録時、及びコンテンツキー (C o n t e n t - K e y) の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示す、本発明の第 2 の実施の形態となるコピー管理システムの模式図である。

発明を実施するための最良の形態

本発明は、コンピュータプログラムのコピー管理を行うコピー管理システムに適用することができる。

コンピュータプログラムとしては、例えばゲームコンテンツ、音楽コンテンツ、映画コンテンツ、アプリケーションプログラム等がある。また、コンピュータプログラムが記憶された記憶媒体としては、DVD-ROM、CD-ROM等の光ディスクの他、半導体メモリがある。また、コンピュータプログラムのコピー先となる二次記憶媒体としては、ハードディスク (H D) , DVD

ー R A M や光磁気ディスク（M O ）等がある。

以下、上記ゲームコンテンツ、音楽コンテンツ、映画コンテンツ、アプリケーションプログラム等を総称して、単に「コンテンツ」ということとする。

5 コピー管理システムの全体構成

まず、図 1 に本発明の第 1 の実施の形態となるコピー管理システムの全体構成を示す。この図 1 に示すように、この第 1 の実施の形態のコピー管理システムは、光ディスクに記憶されているコンテンツの再生機能（実行機能）、及びネットワークを介した通信機能を備えたクライアント端末装置 1 を有している。

このクライアント端末装置 1 には、光ディスクに記憶されたコンテンツをコピーするためのハードディスクドライブ 2（H D D）が接続されている。

また、このクライアント端末装置 1 には、インターネット 5 などのネットワークとの接続を図るための通信モデム 6 が接続されている。

なお、通信モデム 6 は、この図 1 に示すようにクライアント端末装置 1 に対して外付けのかたちで設けてもよい。また、通信モデム 6 は、クライアント端末装置 1 に内蔵のかたちで設けてもよい。

また、コピー管理システムは、ユーザエントリ情報が記憶されたデータベース 3 を備えたシステムサーバ装置 4 を有している。このシステムサーバ装置 4 と上記クライアント端末装置 1 とが、例えばインターネット 5 等のネットワークを介して相互に接続されることでこの第 1 の実施の形態のコピー管理システムが構成されている。

クライアント端末装置の構成

図 2 に、クライアント端末装置 1 の外観の斜視図を示す。この図 2 示すように、クライアント端末装置 1 の前面側には、コントローラ接続部 7 A, 7 B と、メモ리카ード装着部 8 A, 8 B が設けられている。

また、このクライアント端末装置 1 の前面側には、U S B 対応機器 (U S B : Universal Serial Bus) が接続される 2 つの U S B 接続端子 9 と、例えば最大 4 0 0 M b p s のデータ転送速度に対応可能な I E E E 1 3 9 4 接続端子 1 0 とが設けられている。

また、このクライアント端末装置 1 の前面側には、光ディスクが装着されるトレイ型のディスク装着部 1 1 が設けられている。また、このクライアント端末装置 1 の前面側には、コンテンツの実行動作や再生動作をリセットするためのリセットボタン 1 2 と、光ディスク装着部 1 1 のトレイの出し入れを操作するためのトレイ操作ボタン 1 3 とが設けられている。

クライアント端末装置 1 の背面側には、電源スイッチ、音声映像出力端子 (A V マルチ出力端子)、P C カードスロット、光デジタル出力端子、A C 電源入力端子等が設けられている。

A V マルチ出力端子は、A V ケーブル 1 7 を介してモニタ用のテレビジョン受像機 1 8 に接続される。クライアント端末装置 1 から出力される映像信号や音声信号は、この A V マルチ出力端子及び A V ケーブル 1 7 を介してモニタ用のテレビジョン受像機 1 8 に供給される。これにより、上記コンテンツの映像がテレビジョン受像機 1 8 に表示される。また、上記コンテンツの音声はテレビジョン受像機のスピーカ装置を介して発音される。

コントローラ接続部 7 A、7 B には、コントローラケーブル 1

5 を介してそれぞれコントローラ 1 4 が接続される。

メモ리카ード装着部 8 A、8 B には、ゲームデータのセーブ（記憶）及び読み出しを行うセーブ用のメモ리카ード等が装着される。

ハードディスクドライブの構成

- 5 次に、図 2 において、クライアント端末装置 1 の上面部に載置されている筐体がハードディスクドライブ 2（以下、HDD 2 という）である。この HDD 2 は、内部に例えば 40 GB 等の大容量のハードディスクが設けられている。この HDD 2 には、十数枚分の DVD-ROM に記憶されたゲームコンテンツをコピー
- 10 可能となっている。

- HDD 2 の前面側には、電源投入時に点灯駆動される電源ランプ 20 と、ハードディスクへの書き込みに連動して点灯駆動される書き込み表示ランプ 21 とが設けられている。HDD 2 の背面側には、少なくとも電源スイッチ及びデータ入出力端子が設けら
- 15 れている。

- HDD 2 をクライアント端末装置 1 に接続する場合、クライアント端末装置 1 の背面側に設けられた上記 PC カードスロットに PC カードを挿入する。この状態で、PC カードに接続ケーブルの一端を接続する。接続ケーブルの他端は、HDD 2 のデータ
- 20 入出力端子に接続する。これにより、クライアント端末装置 1 と HDD 2 とが、電氣的に相互に接続される。

- なお、この例においては、HDD 2 はクライアント端末装置 1 とは別体で、クライアント端末装置 1 に対して外付けすることとした。しかし、この HDD 2 を、クライアント端末装置 1 に内蔵
- 25 するかたちで設けてもよい。

また、クライアント端末装置 1 と HDD 2 とを PC カードと接

続ケーブルを介して接続することとした。しかし、HDD 2 の背面側（或いは前面側でもよい。）にUSB 接続端子やIEEE 1394 接続端子等の接続端子を設け、この接続端子を介してHDD 2 をクライアント端末装置 1 に接続するようにしてもよい。

5 クライアント端末装置の電氣的構成

次に、図 3 はクライアント端末装置 1 のブロック図である。この図 3 に示すように、クライアント端末装置 1 は、CPU 30 と、グラフィックプロセッサ 31（GPU）と、I/O プロセッサ 32（IOP）を有している。

- 10 また、クライアント端末装置 1 は、CD-ROM や DVD-ROM 等の光ディスクの再生制御を行う光ディスク制御部 33 と、サウンドプロセッサユニット 34（SPU）とを有している。

- また、クライアント端末装置 1 は、CPU 30 や IOP 32 が実行するオペレーティングシステムプログラムが格納された M
15 ASK-ROM 35 と、CPU 30 のワークエリアや光ディスクから読み出されたデータを一時的に格納するバッファとして機能する RAM 36 とを有している。

- また、クライアント端末装置 1 は、光ディスク制御部 33 の R
F アンプ 37 を介して供給される光ディスクからの再生出力に
20 対して、例えば誤り訂正処理（CRC 処理）等を施して出力する CD/DVD DSP 38 を有している。

- また、クライアント端末装置 1 は、光ディスク制御部 33 のスピ
ンドルモータの回転制御、光ピックアップのフォーカス／トラッ
キング制御、ディスクトレイのローディング制御等を行うドライ
25 バ 39 及びメカコントローラ 40 を有している。

また、クライアント端末装置 1 は、上記 PC カードが接続される

カード型コネクタ 4 1 を有している。

これらの各部は、主にバスライン 4 2 , 4 3 等を介してそれぞれ相互に接続されている。

5 なお、DVD-ROMに記憶された映画コンテンツの再生は、メモリカードに記憶されたDVDドライバソフトウェアに基づいて行われる。或いは、映画コンテンツの再生は、クライアント端末装置 1 内に内蔵された半導体メモリ 4 4 (DVD Player ROM) に焼き付けられたDVDドライバソフトウェアに基づいて行われる。

10 MASK-ROM 3 5 には、オペレーティングシステムプログラムが記憶されている。CPU 3 0 は、このMASK-ROM 3 5 に記憶されているオペレーティングシステムプログラムに基づいて、クライアント端末装置 1 全体の動作を制御する。

15 また、MASK-ROM 3 5 には、コントローラ接続部 7 A , 7 B と、メモリカード装着部 8 A , 8 B 、及びカード型コネクタ 4 1 に接続されるコントローラ 1 4 , メモリカード 1 6 及びHDD 2 等のハードウェア識別番号 (ハードウェア ID) も記憶されている。IOP 3 2 は、このMASK-ROM 3 5 に記憶されているハードウェア IDに基づいて、コントローラ 1 4 , メモリカード 1 6 及びHDD 2 等のハードウェアと通信を行い、各接続端子 7 A , 7 B , 8 A , 8 B 及びカード型コネクタ 4 1 等に接続されたハードウェアを特定して認識する。

20 なお、ハードウェア ID は、クライアント端末装置 1 全体で一つの ID 、メモリカード 1 6 全体で一つの ID 、及びHDD 2 全体で一つの ID 等のように、いわば各ハードウェアに対して総称的に付された ID を意味している。

これに対して、後述するクライアント I D , M C - I D 及び H D D - I D は、各クライアント端末装置 1 毎、各メモリカード 1 6 毎、及び各 H D D 2 毎にそれぞれ付された各ハードウェア固有の I D となっている。

- 5 GPU 3 1 は、CPU 3 0 からの描画指示に従って描画を行い、描画された画像を図示しないフレームバッファに格納する。また、GPU 3 1 は、座標変換等の処理を行うジオメトリトランスファエンジンとしての機能を有している。

- この GPU 3 1 は、例えば光ディスクに記録されているゲーム
10 コンテンツがいわゆる 3 D グラフィックを利用する場合に、三角形形状のポリゴンの集合で仮想的な 3 次元オブジェクトを構成する。そして、GPU 3 1 は、この 3 次元オブジェクトを仮想的なカメラ装置で撮影することで得られる画像を生成するための諸計算を行う。すなわち、GPU 3 1 は、レンダリングを行う場合
15 における透視変換処理（3 次元オブジェクトを構成する各ポリゴンの頂点を仮想的なカメラスクリーン上に投影した場合における座標値の計算）等を行う。

- また、GPU 3 1 は、CPU 3 0 からの描画指示に従って、必要に応じてジオメトリトランスファエンジンを利用しながら、フ
20 レームバッファに対して描画を行う。そして、この描画した画像に対応するビデオ信号（v i s u a l o u t）を出力する。

- 一方、SPU 3 4 は、適応予測符号化された音声データを再生する A D P C M 復号機能と、サウンドバッファに記憶されている波形データを再生することで、効果音等の音声信号を再生して出
25 力（a u d i o o u t）する再生機能と、サウンドバッファに記憶されている波形データを変調させて再生する変調機能等を

備えている。この S P U 3 4 は、いわゆるサンプリング音源として動作する。S P U 3 4 は、C P U 3 0 からの指示により、サウンドバッファに記憶されている波形データに基づき楽音，効果音等の音声信号を発生する。

- 5 このようなクライアント端末装置 1 は、電源が投入されると、C P U 3 0 及び I O P 3 2 が、M A S K - R O M 3 5 から C P U 3 0 用のオペレーティングシステムプログラム及び I O P 3 2 用のオペレーティングシステムプログラムをそれぞれ読み出す。

- 10 C P U 3 0 は、C P U 3 0 用のオペレーティングシステムプログラムによりクライアント端末装置 1 の各部を統括的に制御する。

I O P 3 2 は、I O P 3 2 用のオペレーティングシステムプログラムによりコントローラ 1 4，メモ리카ード 1 6、及び H D D 2 等との間のデータの入出力を制御する。

- 15 C P U 3 0 は、C P U 3 0 用のオペレーティングシステムプログラムに基づいて、動作確認等の初期化処理を行った後、光ディスク制御部 3 3 を制御し、光ディスクに記録されているコンテンツを再生制御する。

- 20 再生したコンテンツがビデオゲームのゲームコンテンツである場合、C P U 3 0 は、I O P 3 2 を介してコントローラ 1 4 から受け付けたプレーヤからの指示（コマンド）に従って、G P U 3 1 や S P U 3 4 を制御し、ゲームコンテンツの画像の表示や効果音，楽音等の発声を制御する。

- 25 再生したコンテンツが映画コンテンツの場合、C P U 3 0 は、I O P 3 2 を介してコントローラ 1 4 から受け付けたプレーヤからの指示に従って、G P U 3 1 や S P U 3 4 を制御し、映画コ

ンテンツの映像の表示や音声の発声等を制御する。

コピー管理動作

このようなコピー管理システムは、光ディスクに記憶されているコンテンツがHDD2にコピーされる際に、以下のように管理
5 する。

インストーラのインストール

まず、このコピー管理システムは、光ディスクに記憶されているコンテンツをHDD2にコピーする際に、クライアント端末装置1でコピー制御用のアプリケーションプログラム（インストー
10 ラ）を実行する必要がある。この例の場合、インストーラは、コンテンツと共に光ディスクに記憶されている。クライアント端末装置1は、コンテンツのコピーを行う前にインストーラのインストールを行う。

インストーラのインストールを行う場合、ユーザは、インストーラが記憶されている光ディスクをクライアント端末装置1に装着する。クライアント端末装置1のCPU30は、この光ディスクが装着されると自動的に（オートラン）、或いはユーザのコントローラ14の操作に従って光ディスクに記憶されているイン
15 ストーラを読み出し、これをメモ리카ード16或いはRAM36に記憶制御する。

このメモ리카ード16或いはRAM36に記憶されたインストーラは、ユーザが光ディスクに記憶されているコンテンツのコピーを指定した際に、CPU30により実行される。CPU30は、このインストーラを実行することで、コンテンツのコピー制
25 御を行う。

なお、インストーラは、システム業者側でインストーラのみ記

- 憶された光ディスクを製造し、これをユーザに配布するようにしてもよい。或いは、システム業者側でインストーラが記憶されたメモリカードを製造し、これをユーザに配布するようにしてもよい。この場合、インストーラのインストール作業を省略可能とすることができる。或いは、インストーラが記憶されたROMをクライアント端末装置1内に設けてもよい。この場合でも、インストーラのインストール作業を省略可能とすることができる。

コンテンツの暗号化

- 光ディスクに記憶されたコンテンツには、図4に示すように各コンテンツ毎に異なる対称鍵（コンテンツキー：Content-
Key）を用いて暗号化処理が施されている。また、光ディスクには、このように暗号化処理されたコンテンツの他、各光ディスク毎に固有となる「Media unique ID（メディア
ユニークID：MID）」が記憶されている。

ユーザ登録

- 次に、この第1の実施の形態のコピー管理システムにおいては、光ディスクからHDD2にコンテンツのコピーを行う場合、各メモリカード16に固有に付された「メモリカードID（MC-ID）」を用いてシステムサーバ装置4にユーザ登録を行う。このユーザ登録が行われない場合には、コンテンツのコピーは許可されない。

- 図5は、ユーザがシステムサーバ装置4に対してユーザ登録を行うまでの流れを示すフローチャートである。図6は、このユーザ登録によりクライアント端末装置1とシステムサーバ装置4との間で送受信される情報を示す当該コピー管理システムの模式図である。

この図 5 及び図 6 を用いてユーザ登録動作を説明する。図 5 のフローチャートは、ユーザがクライアント端末装置 1 のメイン電源を投入することでスタートとなる。

ステップ S 1 では、ユーザがインターネット 5 を介して自分の
5 クライアント端末装置 1 をシステムサーバ装置 4 に接続する。

具体的には、このクライアント端末装置 1 には、図 1 に示したようにインターネット接続用の通信モデム 6 が接続（或いは内蔵）されている。ユーザによりインターネット接続が指定されると、図 3 に示す CPU 3 0 は、所定の WWW ブラウザに基づいて
10 動作し、この通信モデム 6 を介して当該クライアント端末装置 1 とシステムサーバ装置 4 との間の通信回線の確立を図る。これにより、このユーザ登録の行程がステップ S 2 に進む。

ステップ S 2 では、CPU 3 0 が、クライアント端末装置 1 に装着されたメモリカードの識別番号（MC-ID）、クライアント
15 ト端末装置 1 毎に付された固有の識別番号（クライアント ID）及び HDD 2 毎に付された固有の識別番号（HDD-ID）をシステムサーバ装置 4 に送信制御する。

具体的には、システムサーバ装置 4 とクライアント端末装置 1 との通信回線が確立されると、CPU 3 0 は、クライアント端末
20 装置 1、HDD 2 及びメモリカード 1 6 とそれぞれ通信を行う。CPU 3 0 は、この通信により、クライアント端末装置 1 に固有に付された識別番号（クライアント ID）、HDD 2 に固有に付された識別番号（HDD-ID）、及びクライアント端末装置 1 に装着されたメモリカード 1 6 に固有に付された識別番号（MC
25 -ID）をそれぞれ取得する。CPU 3 0 は、これらの識別番号を、図 6 に示すようにシステムサーバ装置 4 側に送信する。これ

により、このユーザ登録の行程がステップ S 3 に進む。

なお、クライアント端末装置 1 とシステムサーバ装置 4 との間においては、例えば S S L (Secure Sockets Layer) 等の通信
5 プロトコルに基づいて情報が暗号化されて送受信されるようにな
っており、通信の安全性が確保されている。

また、この例においては、C P U 3 0 は、各デバイスと通信を行
うことで、クライアント I D、H D D - I D 及び M C - I D を取得してシ
ステムサーバ装置 4 側に送信することとした。しかし、
クライアント端末装置 1、H D D 2 及びメモ리카ード 1 6 には、
10 クライアント I D、H D D - I D 及び M C - I D がそれぞれ各筐
体にユーザが視認可能なかたちで貼り付けられている。このため、
ユーザが、このクライアント I D、H D D - I D 及び M C - I D
を見て、コントローラ 1 4 を操作して手動で各 I D の入力を行い、
システムサーバ装置 4 側に送信するようにしてもよい。

15 次に、ステップ S 3 では、システムサーバ装置 4 が、このユー
ザから送信されたメモ리카ードの識別番号 (M C - I D) が有効
な I D であるか否かを判別する。このユーザ登録行程は、このス
テップ S 3 において、システムサーバ装置 4 が、ユーザから送信
された M C - I D が有効な I D であると判別した場合にステッ
20 プ S 4 に進み、ユーザから送信された M C - I D が無効な I D
であると判別した場合にステップ S 7 に進む。

具体的には、システムサーバ装置 4 は、全てのクライアント端
末装置 1 のクライアント I D、全ての H D D 2 の H D D - I D、
及び全てのメモ리카ード 1 6 の M C - I D を記憶したデータベ
25 ース 3 を有している。

システムサーバ装置 4 は、ユーザからクライアント端末装置 1、

H D D 2 及びメモリカード 1 6 の各固有の I D が送信されると、まず、ユーザから送信されたメモリカード 1 6 の固有の I D である M C - I D と、データベース 3 に登録されている各 M C - I D とを照合し、ユーザから送信されたメモリカード 1 6 の M C - I D と同じ M C - I D がデータベース 3 に登録されているか否かを判別する。

すなわち、システムサーバ装置 4 は、ユーザから送信されたメモリカード 1 6 の M C - I D は、データベース 3 に正規に登録されている M C - I D と同じであるか否かを判別する。

10 ユーザから送信されたメモリカード 1 6 の M C - I D が、データベース 3 に正規に登録されているいずれの M C - I D ととも一致しなかった場合には、システムサーバ装置 4 は、このユーザ登録のアクセスを、不正なユーザ登録のアクセスと判断する。この場合、システムサーバ装置 4 は、ステップ S 7 において、例えば
15 「このメモリカードではユーザ登録を行うことはできません。」等のユーザ登録を拒否するメッセージをクライアント端末装置 1 側に返信する（無効通知）。これにより、ユーザ登録が中断されたかたちで、このユーザ登録行程が終了することとなる。

一方、ユーザから送信されたメモリカード 1 6 の M C - I D が、
20 データベース 3 に正規に登録されているいずれかの M C - I D と一致した場合、システムサーバ装置 4 は、ステップ S 4 において、現在、システムサーバ装置 4 にアクセスしているユーザの固有の I D であるユーザ I D （U s e r I D）を、例えば乱数等を用いて形成する。

25 そして、システムサーバ装置 4 は、図 6 に示すようにそのユーザのクライアント I D , H D D - I D 及び M C - I D と共に、上

記ユーザの固有のIDであるユーザID (User ID)、及び後に説明するMC-Keyを一纏めにし、これを「ユーザエントリ情報」としてシステムサーバ装置4のデータベース3に登録する。

- 5 このように、当該実施の形態のコピー管理システムは、各ユーザが所有するクライアント端末装置1, HDD2及びメモリカード16の3つのIDの組み合わせで各ユーザを特定してデータベース3に登録する。

10 クライアント端末装置1, HDD2及びメモリカード16の3つのIDが、異なるユーザ間で全て一致するということは有り得ないため、この3つのIDに基づいてユーザ登録を行うことにより、ユーザを確実に特定してユーザ登録を行うことができる。これにより、後述する光ディスクに記録されたコンテンツの不正コピーを、より強力に防止することができる。

- 15 なお、ユーザ登録の際に、「MC-IDのみ」、「クライアントIDのみ」、「HDD-IDのみ」、「MC-IDとクライアントID」、「MC-IDとHDD-ID」、或いは「クライアントIDとHDD-ID」をシステムサーバ装置4側に送信してユーザ登録を行うようにしてもよい。これらの場合でも、各IDはそれぞれ固有のIDであるため、異なるユーザ間で重複することはなく、ユーザを略々確実に特定してユーザ登録を行うことができる。

25 次に、ユーザ登録の行程がステップS5に進むと、システムサーバ装置4は、ユーザ登録が正規に完了した証として、上記ステップS4で形成したユーザエントリ情報のうち、ユーザID (User ID) をMC-Keyで暗号化し、これをクライアント端末装置1側に返信する。

MC-Key

ここで、上記「MC-Key」は、クライアント端末装置 1 とシステムサーバ装置 4 との間で送受信する情報を暗号化するための鍵情報である。この MC-Key は、MC-ID と共にメモリカード 16 内に予め記憶されている。

MC-ID は、ユーザが視認可能なようにメモリカード 16 の筐体に張り付けられているのであるが、この MC-Key はユーザが視認できないようにメモリカード 16 内に記憶されている。また、この MC-Key は、ユーザがメモリカード 16 内に記憶されている情報を再生した場合でも、表示や出力が行われることのない秘密性の高い情報となっている。このため、この MC-Key は、ユーザレベルでは、認識することはできないようになっている。

また、システムサーバ装置 4 のデータベース 3 には、全てのメモリカード 16 の MC-ID と共に、各メモリカード 16 に記憶された MC-Key が記憶されている。システムサーバ装置 4 は、MC-Key が必要となったときに、このデータベース 3 から MC-Key を読み出して参照する。このため、クライアント端末装置 1 からシステムサーバ装置 4 に対して MC-Key が送信されることはない。

このように、MC-Key は、ユーザレベルでは認識することができず、また、クライアント端末装置 1 とシステムサーバ装置 4 との間で送受信されることの無い、秘密性の高い情報となっている。

クライアント端末装置 1 とシステムサーバ装置 4 との間における MC-Key の送受信を不要とすることで、MC-Key が

第三者に傍受される不都合を防止することができる。

システムサーバ装置 4 は、ユーザ I D (U s e r I D) を返信する際、予めデータベース 3 に記憶されている M C - K e y の中から、現在アクセスされているユーザのメモリカード 1 6 に対応する M C - K e y を選択する。そして、この選択した M C - K e y を用いてユーザ I D (U s e r I D) を暗号化してクライアント端末装置 1 に返信する。

この M C - K e y は、上記ユーザ I D (U s e r I D)、メディアユニーク I D (m e d i a u n i q u e I D (M I D))、コンテンツキー (C o n t e n t - K e y)、及び C o n t e n t - G e n - K e y をそれぞれ復号化する際に用いられる。

M I D は、各光ディスク毎に固有に付されている I D である。コンテンツキーは、光ディスクに記録されたコンテンツを暗号化処理する際に用いられた暗号鍵である。C o n t e n t - G e n - K e y は、H D D 2 にコピーされるコンテンツに対して再暗号化処理を施す際に用いられる暗号鍵である。

クライアント端末装置 1 は、光ディスクから再生したコンテンツを、上記コンテンツキーを用いて復号化する。そして、クライアント端末装置 1 は、この復号化したコンテンツを、上記 C o n t e n t - G e n - K e y を用いて再暗号化処理して H D D 2 にコピーするようになっている。詳しくは後述する。

次に、ユーザ登録行程がステップ S 6 に進むと、クライアント端末装置 1 が、システムサーバ装置 4 側から返信されたユーザ I D (U s e r I D) をメモリカード 1 6 に記憶制御する。これにより、この図 5 のフローチャートに示すユーザ登録の全行程が

終了する。そして、この時点において、メモ리카ード16には、図6に示すように予め記憶されているMC-ID及びMC-Keyと共に、MC-Keyで暗号化されたユーザID (User ID) が記憶されることとなる。

5 メディアユニークIDの登録とコンテンツキーの取得

次に、光ディスクに記録されているコンテンツを何回でもHDD2にコピー可能とすると、MC-ID, MC-Key及びユーザID (User ID) が記録されたメモ리카ード16を他のユーザに貸与するだけで、この他のユーザも光ディスクに記録されているコンテンツをこの他のユーザのHDDに不正にコピーすることが可能となり好ましいことではない。

このコピー管理システムの場合、コンテンツをHDD2にコピーする際、ユーザがクライアント端末装置1を介して各光ディスク毎に付された固有のメディアユニークID (media unique ID (MID)) をシステムサーバ装置4側に送信する。システムサーバ装置4は、ユーザから送信されたメディアユニークIDを登録すると共に、暗号化されたコンテンツを復号化するためのコンテンツキーをユーザに送信する。クライアント端末装置1は、光ディスクに記録されているコンテンツを、コンテンツキーを用いて復号化してHDD2にコピーする。このため、このコンテンツキーを受信するということは、システムサーバ装置4からクライアント端末装置1に対して、コンテンツのコピーが許諾されたことを意味する。

システムサーバ装置4は、クライアント端末装置1から受信したメディアユニークIDに対して、過去にコンテンツキーの送信が行われていないことを確認したうえで、コンテンツキーの送信

を行う。これにより、同じメディアユニーク I D に対するコンテンツキーの送信を、1 回のみに制限することができる。

例えば、あるユーザが自分で購入した光ディスクに記憶されているコンテンツを、自分の H D D 2 にコピーした後に、この光ディスクを他のユーザに貸与したとする。他のユーザは、H D D 2 にコンテンツをコピーする際に、貸与された光ディスクのメディアユニーク I D をシステムサーバ装置 4 に送信する。しかし、システムサーバ装置 4 側には、その光ディスクのメディアユニーク I D に対して、コンテンツキーの送信が行われたことを示す履歴が残っている。この場合、システムサーバ装置 4 は、他のユーザに対してコンテンツキーの配信は行わない。コンテンツキーを入手することができない他のユーザは、コンテンツを H D D 2 にコピーすることはできない。このコピー管理システムは、このようにしてコンテンツの不正コピーを防止している。

図 7 のフローチャートに、メディアユニーク I D (M I D) の登録とユーザがコンテンツキーを取得するまでの流れを示す。また、図 8 に、メディアユニーク I D の登録の際、及びコンテンツキーの取得の際に、クライアント端末装置 1 とシステムサーバ装置 4 との間で送受信される各情報を示す。

この図 7 及び図 8 を用いてメディアユニーク I D (M I D) の登録とコンテンツキーの取得動作を説明する。この図 7 のフローチャートに示すメディアユニーク I D (M I D) の登録とコンテンツキーの取得行程（登録取得行程）は、ユーザが前述のユーザ登録を正規に終了させていることを前提として実行される。

まず、ステップ S 1 1 では、クライアント端末装置 1 が、システムサーバ装置 4 との間の通信回線の確立を図る。これにより、

この登録取得行程がステップ S 1 2 に進む。

なお、この例においては、前述のユーザ登録終了後に、クライアント端末装置 1 とシステムサーバ装置 4 との間で確立された通信回線を一旦切断し、この登録取得行程の実行時に、再度、クライアント端末装置 1 とシステムサーバ装置 4 との間の通信回線を確立する説明となっている。

しかし、前述のユーザ登録に続けて、クライアント端末装置 1 とシステムサーバ装置 4 との間で確立された通信回線を切断することなく、この登録取得行程を実行するようにしてもよい。この場合、この登録取得行程は、ステップ S 1 1 をスキップして、スタートからステップ S 1 2 に進むこととなる。

次にステップ S 1 2 では、クライアント端末装置 1 が、前述のように取得したユーザ ID (User ID) 及び MC-ID をシステムサーバ装置 4 に送信する。また、クライアント端末装置 1 は、このユーザ ID 及び MC-ID と共に、これから HDD 2 にコピーするコンテンツが記憶された光ディスクに対して固有に付されているメディアユニーク ID (MID) をシステムサーバ装置 4 側に送信する。

具体的には、CPU 30 は、メモ리카ード 16 と通信を行い、図 8 に示すように MC-ID をシステムサーバ装置 4 側に送信する。また、CPU 30 は、前述のように MC-Key で暗号化されたユーザ ID をメモ리카ード 16 から読み出してシステムサーバ装置 4 側に送信する。また、CPU 30 は、光ディスク制御部 33 を制御して光ディスクから再生したメディアユニーク ID (MID) を MC-Key で暗号化し、これをシステムサーバ装置 4 側に送信する。

なお、これらの各情報と共に、クライアント I D 及び H D D - I D をシステムサーバ装置 4 側に送信するようにしてもよい。クライアント I D 及び H D D - I D は、上記 M C - I D と共にユーザの特定に用いることができる。M C - I D , クライアント I D
5 及び H D D - I D の 3 つの I D を用いてユーザを特定することで、M C - I D のみでユーザの特定を行う場合よりも、より正確にユーザを特定することができる。

また、クライアント端末装置 1 とシステムサーバ装置 4 との間で送受信される情報は、例えば S S L (Secure Sockets Layer)
10 等の通信プロトコルに基づいて暗号化されて送受信される。これにより、クライアント端末装置 1 とシステムサーバ装置 4 との間では、安全性の高い通信を行うことができる。

次に、ステップ S 1 3 では、システムサーバ装置 4 が、クライアント端末装置 1 側から送信されたユーザ I D (U s e r I
15 D) が有効な I D であるか否かを判別する。このステップ S 1 3 において、システムサーバ装置 4 が、ユーザ I D は有効であると判別した場合、この登録取得行程がステップ S 1 4 に進む。これに対して、このステップ S 1 3 において、システムサーバ装置 4 が、ユーザ I D は無効であると判別した場合、この登録取得行程
20 はステップ S 1 7 に進む。

具体的には、システムサーバ装置 4 は、クライアント端末装置 1 側から送信された M C - I D (及びクライアント I D , H D D - I D) に基づいてデータベース 3 を参照し、この M C - I D に対応する M C - K e y を読み出す。そして、システムサーバ装置
25 4 は、この M C - K e y に基づいて、M C - K e y で暗号化されて送信されたユーザ I D (U s e r I D) 及びメディアユニー

ク I D (M I D) をそれぞれ復号化する。

前述のように、システムサーバ装置 4 側のデータベース 3 には、ユーザエントリ情報としてユーザ I D (U s e r I D) , M C - I D , クライアント I D 及び H D D - I D 等が記憶されている。

- 5 このため、システムサーバ装置 4 は、M C - I D (クライアント I D 及び H D D - I D) に基づいてデータベース 3 内のユーザ情報を検索する。そして、システムサーバ装置 4 は、このユーザ情報内のユーザ I D (U s e r I D) と、現在システムサーバ装置 4 側にアクセスしてきているユーザのユーザ I D (U s e r I D) とを照合する。

システムサーバ装置 4 は、上記両者が一致した場合には、現在システムサーバ装置 4 側にアクセスしてきているユーザは正規のユーザであると判断する。これにより、この登録取得行程がステップ S 1 4 に進む。

- 15 これに対して、システムサーバ装置 4 は、データベース 3 のユーザ情報内のユーザ I D (U s e r I D) と、現在システムサーバ装置 4 側にアクセスしてきているユーザのユーザ I D (U s e r I D) とが不一致の場合、そのユーザ I D (U s e r I D) は無効と判断する。そして、システムサーバ装置 4 は、ステップ S 1 7 において、例えば「ユーザ I D が無効です。ユーザ登録をして下さい。」等の再度のユーザ登録を促すメッセージをクライアント端末装置 1 側に返信する (無効通知) 。これにより、この登録取得行程が中断されたかたちで終了することとなる。

- 25 次に、ステップ S 1 4 では、システムサーバ装置 4 が、現在アクセスしてきているユーザの光ディスクに記録されているコンテンツは、過去にコピーされた履歴があるか否かを判別する。

具体的には、このコピー管理システムの場合、データベース 3 に、各光ディスクにそれぞれ付されているメディアユニーク I D (M I D) が全て登録されている。システムサーバ装置 4 は、コンテンツのコピーが行われた際に、データベース 3 のメディアユニーク I D (M I D) に対してフラグを立てることで、コピーの履歴を残すようになっている。

このため、システムサーバ装置 4 は、メディアユニーク I D (M I D) を復号化すると、そのメディアユニーク I D (M I D) に対してフラグが立っているか否かを検出する。これにより、そのメディアユニーク I D (M I D) を有する光ディスクから過去にコンテンツのコピーが行われたか否かを判別することができる。

そのメディアユニーク I D (M I D) のフラグが立っていない場合、そのメディアユニーク I D (M I D) が付された光ディスクから過去にコンテンツのコピーは行われていないことを意味する。このため、システムサーバ装置 4 は、データベース 3 内におけるそのメディアユニーク I D (M I D) のフラグを立てる。また、システムサーバ装置 4 は、このフラグを立てたメディアユニーク I D (M I D) を、そのユーザのユーザエントリ情報に登録して、この登録取得行程をステップ S 1 5 に進める。

これに対して、そのメディアユニーク I D (M I D) のフラグが立っている場合、過去にそのメディアユニーク I D (M I D) が付された光ディスクからコンテンツのコピーが行われていることを意味する。このため、システムサーバ装置 4 は、ステップ S 1 7 において、例えば「このメディアからコンテンツのコピーをすることはできません。」等のコンテンツのコピーを拒否するメッセージをクライアント端末装置 1 側に返信する（無効通知）。

これにより、この登録取得行程が中断されたかたちで終了することとなる。

次にステップ S 1 5 は、過去に、そのユーザの光ディスクからコンテンツのコピーが行われていない場合に進むステップである。この場合、システムサーバ装置 4 は、そのユーザのメモ리카ード 1 6 の M C - K e y を用いて、光ディスクに記録されているコンテンツを暗号化したコンテンツキー (C o n t e n t - K e y) の暗号化を行う。そして、この暗号化したコンテンツキーをクライアント端末装置 1 側に送信する。このコンテンツキーの送信は、システムサーバ装置 4 側からユーザに対して、光ディスクに記録されているコンテンツのコピーが許可されたことを意味する。

M C - K e y は、そのユーザが所有するメモ리카ード 1 6 に対して固有に付されている。このため、このコンテンツキーを復号化して使用することができるユーザを、その M C - K e y が記憶されたメモ리카ード 1 6 を有するユーザのみに限定することができる。従って、上記コンテンツキーを正規のユーザに対してのみ、安全に送信することができる。

また、システムサーバ装置 4 は、データベース 3 に記憶されているユーザエントリ情報に基づいて、そのユーザが使用しているクライアント端末装置 1 のクライアント I D 及び H D D 2 の H D D - I D を読み出す。システムサーバ装置 4 は、これら各 I D を、例えば乱数を用いて形成した「コンテンツジェンキー (C o n t e n t - G e n - K e y) 」で暗号化してクライアント端末装置 1 側に返信する。

さらに、システムサーバ装置 4 は、クライアント I D 及び H D

D-I Dを暗号化する際に用いたコンテンツジェンキー（Content-Gen-Key）を、上記MC-Keyで暗号化してクライアント端末装置1側に返信する。

後に説明するが、クライアント端末装置1は、システムサーバ装置4から返信されたクライアントIDと、当該クライアント端末装置1のクライアントIDとを照合する。また、クライアント端末装置1は、システムサーバ装置4から送信されたHDD-IDと、当該クライアント端末装置1に接続されているHDD2のHDD-IDとを照合する。そして、クライアント端末装置1は、上記2つのクライアントIDと、上記2つのHDD-IDとが、それぞれ一致することを確認してコンテンツのコピーを行うようになっている。

このため、システムサーバ装置4からユーザのクライアント端末装置1に対して、予め登録されているクライアントID及びHDD-IDを返信することにより、予めデータベース3に登録されているそのユーザのクライアント端末装置1とHDD2の組み合わせでのみ、コンテンツのコピー可能とすることができる。

さらに、システムサーバ装置4は、クライアントID及びHDD-IDを暗号化したコンテンツジェンキーを、そのユーザが所有するメモリカード16に固有に付されたMC-Keyを用いて暗号化してユーザのクライアント端末装置1に返信する。これにより、コンテンツジェンキーを復号化して使用することができるユーザを、そのMC-Keyが記憶されたメモリカード16を有するユーザのみに限定することができる。従って、上記コンテンツジェンキーを正規のユーザに対してのみ、安全に送信することができる。

次に、ステップ S 1 6 では、クライアント端末装置 1 が、システムサーバ装置 4 側から返信された M C - K e y で暗号化されたコンテンツキー (C o n t e n t - K e y)、M C - K e y で暗号化されたコンテンツジェンキー (C o n t e n t - G e n -
5 K e y)、及びコンテンツジェンキー (C o n t e n t - G e n - K e y) で暗号化されたクライアント I D 及び H D D - I D をそれぞれメモ리카ード 1 6 に記憶制御する。これにより、この FIG. 7 のフローチャートに示す登録取得行程が終了する。

このように、このコピー管理システムは、過去にコピー履歴の
10 無いメディアユニーク I D (M I D) を有する光ディスクに記憶されたコンテンツのみコピーの許可を行う。これにより、各光ディスクに記憶されたコンテンツのコピーを 1 回に制限することができる。このため、過去にコンテンツのコピーが行われた光ディスクを貸与された第三者は、その貸与された光ディスクからコ
15 ンテンツのコピーを行うことはできない。従って、1 枚の光ディスクから多数のユーザがコンテンツのコピーを行う不正使用を防止することができる。

コンテンツのコピー

次に、ユーザは、このコンテンツキー (C o n t e n t - K e
20 y) を取得することで、光ディスクに記録されているコンテンツを H D D 2 にコピーすることが可能となる。

図 9 はこのコピー行程の流れを示すフローチャート、FIG. 1 0 はこのコンテンツのコピーが行われる際に、クライアント端末装置 1 , H D D 2 及びメモ리카ード 1 6 の間で取り扱う情報を模式的に示した図である。この図 9 及び図 1 0 を用いてコンテンツの
25 コピー行程の説明を行う。

まず、図 9 のフローチャートは、前述のメディアユニーク I D の登録を終了し、コンテンツキーを取得したユーザが、クライアント端末装置 1 を操作してコンテンツのコピーを指定することでスタートとなる。

5 ステップ S 2 1 では、クライアント端末装置 1 の I O P 3 2 が、それぞれ M C - K e y で暗号化されたコンテンツキー (C o n t e n t - K e y) 及びコンテンツジェンキー (C o n t e n t - G e n - K e y) をメモリカード 1 6 から読み出し、これらを C P U 3 0 に供給する。

10 前述のように、M C - K e y は、システムサーバ装置 4 及びこのクライアント端末装置 1 でそれぞれ保持している。このため、C P U 3 0 は、この保持している M C - K e y を用いて、上記暗号化されているコンテンツキー (C o n t e n t - K e y) 及びコンテンツジェンキー (C o n t e n t - G e n - K e y) を復
15 号化処理する。そして、C P U 3 0 は、この復号化したコンテンツキー及びコンテンツジェンキーを R A M 3 6 に記憶制御する。これにより、このコピー行程がステップ S 2 2 に進む。

20 ステップ S 2 2 では、I O P 3 2 が、コンテンツジェンキー (C o n t e n t - G e n - K e y) で暗号化されたクライアント I D 及び H D D - I D をメモリカード 1 6 から読み出し、これらを C P U 3 0 に供給する。C P U 3 0 は、先に復号化したコンテンツジェンキー (C o n t e n t - G e n - K e y) を用いてこのクライアント I D 及び H D D - I D を復号化する。

25 また、このステップ S 2 2 では、C P U 3 0 が、上記復号化したクライアント I D と当該クライアント端末装置 1 に付されたクライアント I D とを照合する。また、C P U 3 0 は、上記復号

化したHDD-IDと、当該クライアント端末装置1に接続されたHDD2のHDD-IDとを照合する。

次に、ステップS23では、CPU30が、上記各クライアントID、及び上記各HDD-IDがそれぞれ一致するか否かを判別する。両者が一致する場合はコンテンツのコピーを実行すべくこのコピー行程がステップS24に進む。両者が不一致の場合はこのコピー行程がステップS28に進む。

メモ리카ード16から復号化されたクライアントID及びHDD-IDが、そのクライアント端末装置1のクライアントID及びHDD-IDと一致しないということは、前述のコンテンツキー(Content-Key)の取得が、正規のユーザのクライアント端末装置1及びHDD2に基づいて行われていないことを示す。

すなわち、この場合、正規ユーザからメモ리카ード16を貸与された不正ユーザが、コンテンツのコピーを行おうとしていることを示している。

このため、CPU30は、例えば「コピーを行うことはできません。」等のコンテンツのコピーを拒否するメッセージをユーザに対して表示制御する。これにより、中断されたかたちでこのコピー行程が終了することとなる。

次に、ステップS24は、クライアント端末装置1が、上記各クライアントID及び上記各HDD-IDの一致を検出した際に実行するステップである。この場合、CPU30は、光ディスク制御部33により光ディスクから再生されたコンテンツを、RAM36に記憶されているコンテンツキー(Content-Key)を用いて復号化する。また、CPU30は、

この復号化したコンテンツを、R A M 3 6 に記憶されているコンテンツジェンキー (C o n t e n t - G e n - K e y) で再暗号化してH D D 2 に供給する。

次に、ステップ S 2 5 では、H D D 2 が、図 1 0 に示すように
5 上記コンテンツジェンキーで再暗号化されたコンテンツをハードディスクに保存 (コピー) する。

次に、ステップ S 2 6 ではクライアント端末装置 1 の C P U 3 0 が H D D 2 と通信を行うことで、コンテンツのコピーが完了したか否かを判別する。コピーが完了していない場合、C P U 3 0
10 は、前述のステップ S 2 4 及びステップ S 2 5 の動作を繰り返し実行制御することで、コンテンツのコピーが完了するまでの間、H D D 2 に対してコンテンツの供給を行う。コンテンツのコピーが完了すると、このコピー行程がステップ S 2 7 に進む。

ステップ S 2 7 では、コンテンツのコピーが完了したため、I
15 O P 3 2 が、メモ리카ード 1 6 に記憶されているコンテンツキー (C o n t e n t - K e y) を消去する。これにより、このコピー行程が終了する。

このように、クライアント端末装置 1 は、コンテンツキー (C o n t e n t - K e y) で暗号化されて光ディスクに記憶されているコンテンツを、システムサーバ装置 4 から発行されたコンテンツキーで復号化してH D D 2 にコピーする。そして、このコンテンツのコピー後に、メモ리카ード 1 6 内に記憶されているコンテンツキー (システムサーバ装置 4 から発行されたコンテンツキー) を消去する。

25 前述のように、過去にコンテンツのコピーが行われた光ディスクに対しては、データベース 3 にコピー履歴が残るため、システ

ムサーバ装置 4 は、原則的にコンテンツキーの再発行は行わない。
このため、一度コンテンツのコピーが行われた光ディスクを貸与
された第三者からのコピー申請は、システムサーバ装置 4 が、上
記データベースのコピー履歴に基づいて拒否する。そして、シス
5 テムサーバ装置 4 は、この第三者に対しては、コンテンツキーを
送信しない。

上記第三者は、コンテンツキーを取得することができないため、
貸与された光ディスクに記憶されているコンテンツを復号化す
ることができない。このため、上記第三者がコンテンツを H D D
10 等の二次記憶媒体にコピーすることができたとしても、コンテ
ンツを復号化することができないことから、該コンテンツを使用す
ることができない。従って、このコピー管理システムは、コンテ
ンツの不正使用を防止することができる。

コピーされたコンテンツの再生

15 次に、このように H D D 2 にコピーされたコンテンツは、ユー
ザが繰り返し再生して利用することができるようになっている。

図 1 1 に、H D D 2 に保存されたコンテンツの再生行程の流れ
を示すフローチャートを示す。また、図 1 2 にこの再生行程にお
いて、クライアント端末装置 1 , H D D 2 及びメモ리카ード 1 6
20 の間で取り扱われる情報の模式図を示す。

図 1 1 のフローチャートは、前述のコンテンツのコピーを正規に
終了させたユーザが、コンテンツの再生を指定することでスター
トとなる。

ステップ S 3 1 では、クライアント端末装置 1 の I O P 3 2 が、
25 上記 M C - K e y で暗号化されたコンテンツジェンキー (C o n
t e n t - G e n - K e y) をメモ리카ード 1 6 から読み出し、

これをCPU30に供給する。CPU30は、このコンテンツジェンキーを、クライアント端末装置1側で保持しているMC-Keyを用いて復号化して再生する。

次に、ステップS32では、IOP32が、コンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-IDをメモリカード16から読み出し、これをCPU30に供給する。CPU30は、先に復号化したコンテンツジェンキーを用いて、この暗号化されたクライアントID及びHDD-IDを復号化する。

次に、ステップS33では、CPU30が、当該クライアント端末装置1に付されているクライアントIDと、上記コンテンツジェンキーで復号化したクライアントIDとを照合する。

また、CPU30は、当該クライアント端末装置1に接続されているHDD2のHDD-IDと、上記コンテンツジェンキーで復号化したHDD-IDとを照合する。

上記各クライアントID及び上記各HDD-IDが一致しないということは、他のユーザのメモリカード16、他のユーザのクライアント端末装置1、或いは他のユーザのHDD2が用いられていることを示す。このため、CPU30は、ステップS35において、例えば「コンテンツを再生することはできません。」等のコンテンツの再生を拒否するメッセージをユーザに表示する。これにより、中断されるかたちでこのコンテンツの再生行程が終了することとなる。

このように、このコピー管理システムにおいては、HDD2にコピーされたコンテンツを再生する際にも、クライアントID及びHDD-IDの照合を行う。例えば、正規のユーザが所有する

メモ리카ード16とコンテンツが保存されたHDD2が、第三者に貸与された場合を考える。第三者は、自分のクライアント端末装置に対して、この貸与されたメモ리카ード16とHDD2を接続して、該HDD2内に記憶されているコンテンツの再生を行うこととなる。

しかし、メモ리카ード16内に記憶されているクライアントIDは、正規のユーザのクライアントIDである。このため、第三者のクライアント端末装置のクライアントIDと、メモ리카ード16に記憶されているクライアントIDとが一致しないことから、第三者のクライアント端末装置において、HDD2に記憶されているコンテンツの再生は拒否される。このため、メモ리카ード16とHDD2が貸与された場合でも、HDD2にコピーされているコンテンツの使用を防止することができる。

次に、上記各クライアントID及び上記各HDD2がそれぞれ一致した場合、CPU30は、先に復号化したコンテンツジェンキーを用いてHDD2のコンテンツを復号化し、これをRAM36に記憶する。これにより、このコンテンツの再生行程が終了する。

RAM36に記憶されたコンテンツが、例えばビデオゲームのゲームコンテンツであった場合、CPU30は、このゲームコンテンツに基づいて動作する。そして、CPU30は、例えばビデオゲームのキャラクタを表示制御し、効果音やBGM等を発音制御する。これにより、ユーザは、光ディスクからHDD2にコピーしたゲームコンテンツに基づいてビデオゲームを楽しむことができる。

光ディスクからゲームコンテンツを直接的に再生してビデオ

ゲームを行う場合、新たなビデオゲームを行う毎に光ディスクの着脱作業が必要である。しかし、このように各光ディスクに記録されたゲームコンテンツをHDD2にコピーしておくことにより、新たなビデオゲームを行う毎に必要なとなっていた光ディスクの着脱作業を省略することができる。このため、新たなビデオゲームをスムーズに開始可能とすることができる。

なお、光ディスクからコンテンツのコピーが終了した後は、メモ리카ード16に記憶されているコンテンツキーが消去されるため、コンテンツの再コピーは行うことができない。しかし、メモ리카ード16に記憶されているコンテンツジェンキーは、コピー完了後も消去されることはない。このため、コンテンツジェンキーで暗号化されてHDD2にコピーされたコンテンツは、このメモ리카ード16に記憶されているコンテンツジェンキーを用いて繰り返し復号化して再生可能である。

15 デバイスの修理、交換に対する対応

次に、このコピー管理システムの場合、システムサーバ装置4は、クライアントID、HDD-ID、MC-ID等（以下、一括してデバイスIDという）と、ユーザIDとをユーザエントリ情報として一括して管理する。しかし、クライアント端末装置1やHDD2等のデバイスを破損等により交換した場合、この交換したデバイスのデバイスIDが、ユーザエントリ情報として登録されているデバイスIDとは異なるものとなる。従って、デバイスの交換を行うと、正規のユーザであるにも拘わらず、その交換したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

一方、このコピー管理システムの場合、デバイスIDの固有性

を確保することでコンテンツの不正使用を防止するようになっている。このため、クライアント端末装置 1 や H D D 2 等のデバイスを修理により復元した場合でも、この修理後のデバイスに対して、修理前に付されていたデバイス I D とは異なる新たなデバイス I D を付し、修理前のデバイスと修理後のデバイスとを明確に区別して管理することが好ましい。

ただ、このように修理後のデバイスに対して新たなデバイス I D を付すと、前述のデバイスの交換時と同様に、正規のユーザであるにも拘わらず、その修理したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

このコピー管理システムは、デバイスの修理及び交換により新たなデバイス I D を用いることで懸念される上記不都合を、以下のように防止している。

クライアント端末装置及びH D D の修理，交換に対する対応

図 1 3 に、このコピー管理システムにおけるクライアント端末装置及びH D D の修理，交換に対する対応を説明するための模式図を示す。この図 1 3 中、×印が描かれているクライアント端末装置 1 或いはH D D 2 は、破損したデバイスを示している。

この図 1 3 において、デバイスが破損した場合、ユーザは、その破損したデバイスを、メモ리카ード 1 6 と共に、このコピー管理システムを管理する管理者側のリペアセンターに送付する。

すなわち、この場合メモ리카ード 1 6 は破損していないのであるが、メモ리카ード 1 6 にはコンテンツジェンキー (C o n t e n t - G e n - K e y) やコンテンツジェンキー (C o n t e n t - G e n - K e y) で暗号化されたクライアント I D 及びH D D - I D (以下、各 I D を一括してデバイス I D という) が記憶

されている。このため、デバイスが破損した場合でも、この破損したデバイスと共にメモリカード16を上記リペアセンターに送付（或いは持ち込み）するようになっている。

リペアセンターでは、故障したデバイスが送付されると、この
5 デバイスが正常に動作するように修理，交換等すると共に、この修理，交換等したデバイスに対して新たなデバイスIDを付与する。

具体的には、クライアント端末装置1のクライアントIDは、例えば上記ハードウェアIDやオペレーティングシステムプログラムと共にMASK-ROM35に記憶されている。また、H
10 HDD2内にも上記MASK-ROM35と同様のMASK-ROMが設けられており、HDD-IDは、このMASK-ROMに記憶されている。このため、リペアセンターでは、デバイスの修理を行った場合には、この修理を行う前に設けられていたMA
15 SK-ROMを取り外し、新たなクライアントID或いはHDD-IDが記憶されたMASK-ROMに交換することで、新たなクライアントID或いはHDD-IDの付与を行う。

なお、デバイス自体を新品のデバイスに交換する場合は、この新品のデバイスのMASK-ROM内に、故障したデバイスとは
20 異なるデバイスIDが記憶されているため、上記修理時のようなMASK-ROMの交換は行わない。

次に、リペアセンターのオペレータは、故障したデバイスと共に送付されたメモリカード16のMC-IDを再生する。オペレータは、リペアセンターに設けられている端末装置を介して上記
25 システムサーバ装置4のデータベース3にアクセスし、上記メモリカード16から再生したMC-IDに基づいて、上記データベ

ース 3 に記憶されているユーザエントリ情報を参照する。そして、オペレータは、端末装置を操作して、このデータベース 3 に記憶されているユーザエントリ情報のうち、デバイス ID を、新たに付与したデバイス ID に修正登録する。また、オペレータは、端末装置を介してデータベース 3 を操作し、コピー済みのコンテンツに対して立てられている上記フラグを降ろす。

また、オペレータは、端末装置を操作して、メモ리카ード 16 内に記憶されている、MC-Key で暗号化されたコンテンツジェンキー (Content-Gen-Key) と、コンテンツジェンキー (Content-Gen-Key) で暗号化されたデバイス ID (クライアント ID 及び HDD-ID) とをそれぞれ消去する。そして、このメモ리카ード 16 を、修理、交換等したデバイスと共にユーザに返送 (或いは手渡し) する。

これにより、ユーザのデバイス (クライアント端末装置 1, HDD 2 及びメモ리카ード 16) の状態は、図 5 及び図 6 を用いて説明したユーザ登録行程が終了した直後の状態 (=コンテンツのコピーを行う直前の状態) に戻ることとなる。

このメモ리카ード 16 とデバイスが返送されたユーザは、図 7 及び図 8 を用いて説明したメディアユニーク ID (MID) の登録とコンテンツキー (Content-Key) の取得を再度行うようにクライアント端末装置 1 を操作する。

クライアント端末装置 1 は、ユーザの操作に対応してシステムサーバ装置 4 にアクセスし、メディアユニーク ID (MID) の登録を行う。そして、クライアント端末装置 1 は、この登録によりシステムサーバ装置 4 から取得したコンテンツキー (Content-Key) を用いて光ディスクに記憶されているコンテン

ツをHDD2に再コピーする。

これにより、デバイスの修理や交換によりデバイスIDを新たに付与した場合でも、正規のユーザであれば、新たなデバイスIDに基づいてコンテンツのコピーや再生を実行可能とすることができる。

また、コピー管理システム側では、修理や交換により復元したデバイスに対して新たなデバイスIDを付すことにより、修理前のデバイスと修理後のデバイスとを明確に区別して管理することができる。

10 メモ리카ードの破損、紛失に対する対応

次に、このコピー管理システムの場合、メモ리카ード16の破損、或いは紛失に対しては、以下のように対処する。図14に、このコピー管理システムにおけるメモ리카ード16の破損、紛失に対する対応を説明するための模式図を示す。この図14中、点線の枠で囲んで示すメモ리카ード16が、破損或いは紛失したメモ리카ード16を示している。

メモ리카ード16が破損或いは紛失した場合、ユーザは、この図14に示すように、インターネット5を介してクライアント端末装置1をシステムサーバ装置4に接続し、システムサーバ装置4に対してメモ리카ードの再発行を申請する。

この申請がなされるとシステムサーバ装置4は、ユーザIDの入力画面データをクライアント端末装置1側に送信する。これにより、ユーザのクライアント端末装置1は、テレビジョン受像機18にユーザIDの入力画面を表示制御する。

ユーザは、この入力画面に対してユーザIDの入力を行う。しかし、この場合、メモ리카ード16が破損或いは紛失しているた

め、メモリカード16からユーザID (U s e r I D) を読み出すことはできない。このため、ユーザは、ユーザIDが発行された際にメモ帳等を書き写しておいたユーザIDを見て、ユーザIDの入力を行う。クライアント端末装置1は、この入力されたユーザIDをシステムサーバ装置4に送信する。

次にシステムサーバ装置4は、このユーザから送信されたユーザIDに対応するユーザエントリ情報をデータベース3から参照する。これにより、システムサーバ装置4は、破損或いは紛失したメモリカード16のMC-ID及びMC-Keyと共に、コンテンツジェンキー (C o n t e n t - G e n - K e y) やそのメモリカード16でコピーされたコンテンツ等を認識することができる。

次に、システムサーバ装置4は、新たなMC-IDを有するメモリカード16 newに対して、新たなMC-Key (N e w - M C - K e y) と、このN e w - M C - K e yで新たに暗号化したコンテンツジェンキー (C o n t e n t - G e n - K e y) と、このコンテンツジェンキー (C o n t e n t - G e n - K e y) で暗号化したクライアントID及びHDD-IDを記録し直す。また、システムサーバ装置4は、データベース3に記憶されているユーザエントリ情報が、この新たなメモリカード16 N e wに対応したユーザエントリ情報となるように、MC-IDやMC-Key等の書き換えを行う。

なお、この場合、メモリカード16が破損或いは紛失した場合であり、ユーザのクライアント端末装置1及びHDD2は正常に動作している。このため、コンテンツジェンキー (C o n t e n t - G e n - K e y) で暗号化されるクライアントID及びHDD

D-I Dとしては、元のデバイス I Dがそのまま用いられる。

次に、リペアセンターは、このメモリカード 1 6 n e wを、例えば郵送等によりユーザ側に物理的に送付する。前述のように、システムサーバ装置 4 側ではこのメモリカード 1 6 n e w内の
5 各情報の書き換えと共に、データベース 3 のユーザエントリ情報の書き換えを行っている。このため、送付されたメモリカード 1 6 n e wを受け取ったユーザは、このメモリカード 1 6 n e w, クライアント端末装置 1 及び H D D 2 の組み合わせのシステムを用いて、以前と同様に、コンテンツのコピーや、コピーしたコ
10 ンテンツの再生等を行うことができる。

以上の説明から明らかなように、この第 1 の実施の形態のコピー管理システムは、システム管理者が、コンテンツキーで暗号化処理を施したコンテンツを、メディアユニーク I D (M I D) が付された光ディスクに記憶させてユーザに配布する。

15 ユーザは、コンテンツのコピーを行う際に、システムサーバ装置 4 に対して光ディスクの M I Dを送信する。また、ユーザは、自分が使用しているデバイスのデバイス I D (クライアント I D , H D D - I D , M C - I D 等) をシステムサーバ装置 4 に送信する。

20 システムサーバ装置 4 は、各ユーザが使用しているデバイスのデバイス I Dに関連付けて、過去にコンテンツのコピーが行われた光ディスクの M I Dをデータベース 3 に記憶している。システムサーバ装置 4 は、ユーザからコンテンツのコピー申請がなされた際に、ユーザが使用しているデバイス I Dと光ディスクの M I
25 Dに基づいてデータベース 3を参照する。システムサーバ装置 4 は、データベース 3内に同じ M I Dが登録されていないことを条件

として、コンテンツを復号化するためのコンテンツキーを、ユーザのクライアント端末装置 1 に送信する。

クライアント端末装置 1 は、このコンテンツキーを用いて光ディスクに記憶されているコンテンツを復号化して H D D 2 にコピーする。

このコピー管理システムは、データベース 3 内に登録されている M I D と同じ M I D を掲示してコピー申請がなされた場合は、上記コンテンツキーの配信は行われぬ。このため、このコピー管理システムは、コンテンツのコピーを 1 回に制限することができる、コンテンツの不正コピーを防止することができる。

第 2 の実施の形態

次に本発明の第 2 の実施の形態となるコピー管理システムの説明をする。上述の第 1 の実施の形態のコピー管理システムは、ユーザが自分のクライアント端末装置 1 をシステム管理者側のシステムサーバ装置 4 に直接的に接続してユーザ登録を行い、コンテンツキー (C o n t e n t - K e y) 等を取得してコンテンツのコピーを行うものであった。

この第 2 の実施の形態のコピー管理システムは、ユーザのクライアント端末装置 1 とシステム管理者側のシステムサーバ装置 4 との間に、第 3 者が管理する第 3 者管理サーバ装置が設けられている。ユーザはこの第 3 者管理サーバ装置を介してコンテンツキー (C o n t e n t - K e y) 等の取得を行う。第 3 者管理サーバ装置は、このコンテンツキー (C o n t e n t - K e y) 等の提供に対する課金を行う。

第 2 の実施の形態の構成

図 1 5 に、この第 2 の実施の形態となるコピー管理システムの

システム構成図を示す。この図 15 は、光ディスクからコンテンツをコピーする際にコンテンツキー (Content-Key) を取得する流れを示している。

この図 15 において、システムサーバ装置 4 と第 3 者管理サーバ装置 50 とは、例えば専用回線や、公衆回線を専用回線のように利用可能な VPN (Virtual Private Network) 等により相互に接続されている。

また、システムサーバ装置 4 はインターネット 5 には接続されておらず、この第 3 者管理サーバ装置 50 がインターネット 5 に接続されている。このため、ユーザは、システムサーバ装置 4 に対して直接的にアクセスすることはできず、この第 3 者管理サーバ装置 50 を介して間接的にシステムサーバ装置 4 にアクセスすることとなる。

第 2 の実施の形態の動作

次に、この第 2 の実施の形態のコピー管理システムの動作説明をする。この第 2 の実施の形態のコピー管理システムの場合、光ディスクからコンテンツのコピーを行おうとするユーザは、インターネット 5 を介して自分のクライアント端末装置 1 を第 3 者管理サーバ装置 50 に接続する。そして、ユーザは、クライアント端末装置 1 を介して、MC-ID, ユーザ ID (User ID), メディアユニーク ID (MID) を第 3 者管理サーバ装置 50 側に送信する。また、ユーザは、クライアント端末装置 1 を介して、第 3 者管理サーバ装置 50 用のアカウント情報 (例えばユーザ名やパスワード等) を第 3 者管理サーバ装置 50 に送信する。

クライアント端末装置 1 は、MC-ID 及びアカウント情報を

そのまま第3者管理サーバ装置50に送信する。また、クライアント端末装置1は、ユーザID (User ID) 及び光ディスクのメディアユニークID (MID) をMC-Keyで暗号化し、これらを第3者管理サーバ装置50に送信する。

- 5 第3者管理サーバ装置50は、クライアント端末装置1から送信された各情報のうち、アカウント情報を抽出して取得する。また、第3者管理サーバ装置50は、専用回線（或いは上記VPN）を介してMC-ID, MC-Keyで暗号化されたユーザID (User ID)、及びMC-Keyで暗号化されたメディアユニークID (MID) をシステムサーバ装置4に送信する。

- システムサーバ装置4は、このMC-ID, ユーザID及びMIDを受信すると、前述と同様に暗号化されて光ディスクに記録されているコンテンツを復号化するためのコンテンツキー (Content-Key) をMC-Keyで暗号化して第3者管理サーバ装置50に返信する。また、システムサーバ装置4は、コンテンツジェンキー (Content-Gen-Key) をMC-Keyで暗号化して第3者管理サーバ装置50に返信する。さらにシステムサーバ装置4は、このコンテンツジェンキー (Content-Gen-Key) でユーザのクライアントID及びHDD-IDを暗号化して第3者管理サーバ装置50に返信する。

- 第3者管理サーバ装置50は、このMC-Keyで暗号化されたコンテンツキー (Content-Key), MC-Keyで暗号化されたコンテンツジェンキー (Content-Gen-Key)、及びコンテンツジェンキー (Content-Gen-Key) で暗号化されたユーザのクライアントID, HDD-IDを、それぞれインターネット5を介してユーザのクライアン

ト端末装置 1 に転送する。

第 3 者管理サーバ装置 50 は、コンテンツキー (Content Key) を提供した代償として、先にクライアント端末装置 1 から送信された第 3 者管理サーバ装置 50 用のアカウント情報に基づいて、そのユーザに対する課金を行う。

クライアント端末装置 1 は、第 3 者管理サーバ装置 50 から送信された上記コンテンツキー、コンテンツジェンキー、クライアント ID、及び HDD-ID をメモリカード 16 に記憶制御して、前述のようにコンテンツのコピー、及びコピーしたコンテンツの再生に用いる。

第 3 者管理サーバ装置 50 側には、例えばユーザのクレジットカードの番号や、プリペイドされた金額情報が予め登録されている。このため、第 3 者管理サーバ装置 50 は、コンテンツキーの提供と引き替えに課金した金額をクレジットカード会社に請求して回収する。或いは第 3 者管理サーバ装置 50 は、プリペイドされている残金から課金分の金額を減算して回収する。

このように回収された金銭は、例えばシステムサーバ装置 4 の管理者と第 3 者管理サーバ装置 50 の管理者との間において、所定の割合で分配されることとなる。

このようにこの第 2 の実施の形態のコピー管理システムは、クライアント端末装置 1 とシステムサーバ装置 4 との間に第 3 者管理サーバ装置 50 を設けて構成する。ユーザはこの第 3 者管理サーバ装置 50 を介してシステムサーバ装置 4 にアクセスしてコンテンツキー (Content Key) の配布を請求する。第 3 者管理サーバ装置 50 は、このコンテンツキー (Content Key) をユーザに配布して課金を行う。

これにより、このコピー管理システムは、第3者（第3者管理サーバ装置50の管理者）が介在するコピー管理システムという新規なコピー管理システムを提供することができる他、上述の第1の実施の形態のコピー管理システムと同じ効果を得ることができる。

また、このコピー管理システムは、コンテンツキーをユーザに配布した際に課金を行うことで、光ディスク等を介して、或いは所定のネットワークを介してコンテンツを無償でユーザに配布することができる。

10 なお、このコピー管理システムにおいて、光ディスクにMIDを付すことなくユーザに配布し、ユーザからコピーの申請があった際に、システムサーバ装置4或いは第3者管理サーバ装置50が、そのユーザに対してコンテンツキーを配布して課金を行うようにしてもよい。

15 また、この第2の実施の形態のコピー管理システムは、第3者管理サーバ装置50が課金を行うこととしたが、これは、システムサーバ装置4が課金を行うようにしてもよい。

最後に、本発明は一例として説明した上述の各実施の形態に限定されることはない。このため、上述の各実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論である。

例えば、上述の各実施の形態の説明では、クライアント端末装置1は、デバイス識別情報として、クライアントID、HDD-ID及びMC-IDをシステムサーバ装置4に送信することとした。しかし、クライアント端末装置1からクライアントIDのみをシステムサーバ装置4に送信してもよい。同様に、クライア

ント端末装置 1 から H D D - I D のみをシステムサーバ装置 4 に送信してもよい。同様に、クライアント端末装置 1 から M C - I D のみをシステムサーバ装置 4 に送信してもよい。

また、クライアント端末装置 1 からクライアント I D 及び H D
5 D - I D をシステムサーバ装置 4 に送信してもよい。同様に、クライアント端末装置 1 からクライアント I D 及び M C - I D をシステムサーバ装置 4 に送信してもよい。同様に、クライアント端末装置 1 から H D D - I D 及び M C - I D をシステムサーバ装置 4 に送信してもよい。

10 すなわち、上述の各実施の形態のコピー管理システムは、システムサーバ装置 4 側で、コンテンツのコピーが行われる記憶媒体と、コンテンツのコピーに使用されるデバイスとを関連付けてコピー管理を行うことで不正コピーを防止する。このため、クライアント端末装置 1 からシステムサーバ装置 4 に送信されるデバ
15 イス識別情報としては、ユーザを特定可能な識別情報であればよい。

また、上述の各実施の形態の説明では、メモリカード 1 6 を用いることとしたが、このコピー管理システムの場合、必ずしもメモリカード 1 6 は必要としない。メモリカード 1 6 を用いない場
20 合は、メモリカード 1 6 に記憶される上記コンテンツキーやコンテンツジェンキー等は、H D D 2 やクライアント端末装置 1 に内蔵されているメモリに記憶させればよい。

産業上の利用の可能性

25 本発明は、コンピュータプログラムのコピー管理を行うコピー管理システムに適用することができる。

請求の範囲

1. 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付され、管理者側からユーザに配布される記憶媒体と、

上記記憶媒体に記憶されているコンテンツを、上記暗号化鍵に対応する復号化鍵を用いて復号化して二次記憶媒体にコピーするコピー機能を有し、該コンテンツのコピーを行う際に、上記記憶媒体の媒体識別情報と共に、所定かつ固有のデバイス識別情報を送信するユーザの端末装置と、

上記記憶媒体の媒体識別番号を受信した際に、上記デバイス識別情報を有するユーザの端末装置に対して、上記コンテンツの復号化鍵を送信する管理サーバ装置と
を備えるコピー管理システム。

15

2. 請求項1に記載のコピー管理システムであって、

上記管理サーバ装置は、一つの媒体識別情報に対して1回のみ復号化鍵の送信を行うこと
を特徴とするコピー管理システム。

20

3. 請求項1又は請求項2に記載のコピー管理システムであって、

上記端末装置は、上記端末装置の識別情報、上記コンテンツのコピーを行うコピー手段に固有に付された識別情報、及び外付けの半導体メモリに固有に付された識別番号のうち、いずれか1つ
或いは複数を組み合わせ、上記デバイス識別情報として送信すること

25

を特徴とするコピー管理システム。

4. 請求項1から請求項3のうち、いずれか一項に記載のコピー管理システムであって、

5 上記管理サーバ装置は、上記デバイス識別情報で上記復号化鍵を暗号化して送信し、

上記端末装置は、自己のデバイス識別情報で、上記暗号化された復号化鍵を復号化して用いること

を特徴とするコピー管理システム。

10

5. 請求項1から請求項4のうち、いずれか一項に記載のコピー管理システムであって、

上記端末装置は、上記コンテンツの復号化後に、上記復号化鍵を削除すること

15 を特徴とするコピー管理システム。

6. 請求項1から請求項5のうち、いずれか一項に記載のコピー管理システムであって、

20 上記管理サーバ装置は、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信し、

上記端末装置は、上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーし、上記再暗号化鍵を記憶手段に記憶し、上記記憶手段に記憶した再暗号化鍵を用いて、上記コピーされたコンテンツを復号化して再生すること

25 を特徴とするコピー管理システム。

7. 請求項 1 から請求項 6 のうち、いずれか一項に記載のコピー管理システムであって、

上記管理サーバ装置は、各ユーザのデバイス識別情報に関連付けして上記復号化鍵を送信済みの媒体識別情報をデータベース
5 に記憶することで上記復号化鍵の配信管理を行い、

上記管理サーバ装置は、修理或いは交換によりユーザのデバイス識別情報が変更された場合、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えること

10 を特徴とするコピー管理システム。

8. 請求項 1 から請求項 7 のうち、いずれか一項に記載のコピー管理システムであって、

上記管理サーバ装置は、復号化鍵の送信を行った端末装置を有
15 するユーザに対して所定の課金処理を行うこと
を特徴とするコピー管理システム。

9. 請求項 1 から請求項 8 のうち、いずれか一項に記載のコピー管理システムであって、

20 上記ユーザの端末装置と上記管理サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記復号化鍵をユーザの端末装置に送信した際に、ユーザに対する課金処理を行う仲介サーバ装置を備えること

を特徴とするコピー管理システム。

25

10. 暗号化鍵で暗号化されたコンテンツが記憶されると共に、

固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、

上記復号化処理したコンテンツをコピーするステップと

をコンピュータに実行させるクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

11. 請求項10に記載のクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、

上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理すること

を特徴とするクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

12. 請求項10又は請求項11に記載のクライアント端末装置
5 の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

上記コンテンツのコピー後に、上記復号化鍵を削除するステップをコンピュータに実行させることを特徴とするクライアント
端末装置の情報処理プログラムが記憶されたコンピュータ読み
10 取り可能な記憶媒体。

13. 請求項10から請求項12のうち、いずれか一項に記載の
クライアント端末装置の情報処理プログラムが記憶されたコン
ピュータ読み取り可能な記憶媒体であって、

- 15 上記管理サーバ装置から送信される、上記コピーするコン
テンツを再暗号化するための再暗号化鍵を受信するステップと、

上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再
暗号化してコピーするステップと、

上記再暗号化鍵を記憶手段に記憶するステップと、

- 20 コンテンツを再生する際に、上記記憶手段に記憶されている再
暗号化鍵を用いて上記コピーされたコンテンツを復号化して再
再生するステップと

をコンピュータに実行させることを特徴とするクライアント
端末装置の情報処理プログラムが記憶されたコンピュータ読み

- 25 取り可能な記憶媒体。

14. 請求項10から請求項13のうち、いずれか一項に記載のクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

上記媒体識別情報及びデバイス識別情報を送信するステップ
5 では、該デバイス識別情報として、ユーザが使用する端末装置に
対して固有に付されている識別情報、上記コンテンツがコピーさ
れる二次記憶装置に対して固有に付されている識別情報、或いは
上記端末装置に対して外付けされるメモリに対して固有に付さ
れている識別情報のうち、いずれかの識別情報或いは複数の識別
10 情報を送信すること

を特徴とするクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

15 15. ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップと

25 をコンピュータに実行させる管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

16. 請求項15に記載の管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

上記復号化鍵の送信を行った媒体識別情報を、該送信を行った
5 ユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップ

をコンピュータに実行させることを特徴とする管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

10

17. 請求項15又は請求項16に記載の管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

上記復号化鍵を送信するステップは、ユーザのデバイスのデバ
15 イス識別情報で、上記復号化鍵を暗号化して送信すること

を特徴とする管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

18. 請求項15から請求項17のうち、いずれか一項に記載の
20 管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信すること

を特徴とする管理サーバ装置の情報処理プログラムが記憶さ
25 れたコンピュータ読み取り可能な記憶媒体。

19. 請求項15から請求項18のうち、いずれか一項に記載の管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

- 5 修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップ

- 10 をコンピュータに実行させることを特徴とする管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

20. 請求項15から請求項19のうち、いずれか一項に記載の管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

- 15 上記復号化鍵の送信を行ったユーザに対して課金を行うステップ

をコンピュータに実行させることを特徴とする管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

20

21. 請求項15から請求項20のうち、いずれか一項に記載の管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、

- 25 上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされ

る二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信すること

- 5 を特徴とする管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

22. 固有のデバイス識別番号が付されたユーザのデバイスで、固有の媒体識別情報が付された記憶媒体に暗号化鍵で暗号化されて記憶されているコンテンツのコピーを行う際に、上記デバイスから上記デバイス識別情報及び上記媒体識別情報を管理サーバ装置に送信し、
- 10

- コンテンツのコピーが行われた記憶媒体の媒体識別情報が、各ユーザのデバイスのデバイス識別情報に関連付けされた状態で
- 15
- 登録されるデータベースに、上記ユーザのデバイスから送信された媒体識別情報が登録されているか否かを上記管理サーバ装置が検出し、

- 上記データベースに、上記媒体識別情報が未登録であった場合に、上記管理サーバ装置からユーザのデバイスに対して、上記コ
- 20
- ンテンツを復号化するための復号化鍵を送信する
- コピー管理方法。

23. 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を
- 25
- 読み出し、

ユーザが上記コンテンツのコピーを行う際に使用するデバイ

スに対して固有に付されたデバイス識別情報を読み出し、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信し、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信し、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理し、

上記復号化処理したコンテンツをコピーする

クライアント端末装置の情報処理方法。

10

24. ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信し、

15 各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出し、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信する

20 管理サーバ装置の情報処理方法。

25 25. 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、

5 少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、

10 上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、

上記復号化処理したコンテンツをコピーするステップと

をコンピュータに実行させるクライアント端末装置の情報処理プログラム。

15 26. ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

20 各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、

25 上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップと

をコンピュータに実行させる管理サーバ装置の情報処理プロ

グラム。

補正書の請求の範囲

[2002年7月19日 (19. 07. 02) 国際事務局受理：出願当初の請求の範囲
1-18は補正された；出願当初の請求の範囲
19-26は取り下げられた。(8頁)]

1. (補正後) 所定のコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体と、

- 5 上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第1の記憶装置にコピーするコピー機能を有し、上記記憶媒体の媒体識別情報と共に、当該端末装置に付された固有の装置識別情報を送信するユーザ端末装置と、

上記媒体識別情報及び上記装置識別情報を受信した際に、該装置識別
10 情報に対応するユーザ端末装置に対して、該媒体識別情報に対応するコンテンツのコピーを許可するコピー許可情報を送信するサーバ装置と
を有するコピー管理システム。

2. (補正後) 請求項1記載のコピー管理システムであって、

- 15 上記サーバ装置は、一つの媒体識別情報に対して1回のみ上記コピー許可情報の送信を行うこと
を特徴とするコピー管理システム。

3. (補正後) 請求項1又は請求項2記載のコピー管理システムであって、

- 20 上記ユーザ端末装置は、当該ユーザ端末装置自体に固有に付された端末識別情報、上記第1の記憶装置の第1の装置識別情報、及びユーザ端末装置を構成する第2の記憶装置に固有に付された第2の装置識別情報のうち、いずれか1つ或いは複数を組み合わせて上記装置識別情報としてサーバ装置に送信すること

- 25 を特徴とするコピー管理システム。

4. (補正後) 請求項 1 から請求項 3 のうち、いずれか一項記載のコピー管理システムであって、

上記サーバ装置は、上記装置識別情報で暗号化した上記コピー許可情報を送信し、

- 5 上記ユーザ端末装置は、上記サーバ装置に送信した装置識別情報で、上記暗号化されたコピー許可情報を復号化して用いることを特徴とするコピー管理システム。

5. (補正後) 請求項 1 から請求項 4 のうち、いずれか一項記載のコピー管理システムであって、

上記ユーザ端末装置は、上記コンテンツのコピー後に、上記コピー許可情報を削除すること

を特徴とするコピー管理システム。

- 15 6. (補正後) 請求項 1 から請求項 5 のうち、いずれか一項記載のコピー管理システムであって、

上記サーバ装置は、上記コピーするコンテンツを暗号化するための暗号化鍵を送信し、

- 20 上記ユーザ端末装置は、上記コンテンツを上記暗号化鍵で暗号化して上記第 1 の記憶装置にコピーすると共に、上記暗号化鍵を所定の記憶手段に記憶し、該記憶手段に記憶した暗号化鍵を用いて、上記第 1 の記憶装置にコピーされたコンテンツを復号化して再生すること
- を特徴とするコピー管理システム。

- 25 7. (補正後) 請求項 1 から請求項 6 のうち、いずれか一項記載のコピー管理システムであって、

上記サーバ装置は、上記コピー許可情報の送信が終了した媒体識別情報を、各ユーザのユーザ端末装置に付されている固有の装置識別情報に関連付けてデータベースに記憶し、修理或いは交換によりユーザ端末装置固有の識別情報が変更された場合、上記データベースに登録されてい

5 る装置識別情報を変更された装置識別情報に書き換えること

を特徴とするコピー管理システム。

8. (補正後) 請求項 1 から請求項 7 のうち、いずれか一項記載のコピー管理システムであって、

10 上記サーバ装置は、上記コピー許可情報の送信を行ったユーザ端末装置を有するユーザに対して所定の課金処理を行うこと

を特徴とするコピー管理システム。

9. (補正後) 請求項 1 から請求項 8 のうち、いずれか一項記載のコピー管理システムであって、

15 上記ユーザ端末装置と上記サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記コピー許可情報をユーザ端末装置に送信した際に、該ユーザに対する課金処理を行う仲介サーバ装置を有すること

を特徴とするコピー管理システム。

20

10. (補正後) 記憶されている所定のコンテンツ及び固有の媒体識別情報のうち、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するユーザ端末装置を構成する装置に対して固有に付された装置識別情報を読み出すステップと、

25

少なくとも上記読み出した媒体識別情報及び装置識別情報を、所定の

サーバ装置に送信するステップと、

上記媒体識別情報及び装置識別情報を送信することで、上記サーバ装置から送信される、上記コンテンツのコピーを許可するコピー許可情報を受信するステップと、

- 5 上記受信したコピー許可情報を用いて、上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第1の記憶装置にコピーするステップと

を有するユーザ端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

10

11. (補正後) 請求項10記載の記憶媒体であって、

上記コピー許可情報は、上記送信した装置識別情報で暗号化されており、

上記受信したコピー許可情報を、上記送信した装置識別情報で復号化

- 15 するステップを有すること

を特徴とする記憶媒体。

12. (補正後) 請求項10又は請求項11記載の記憶媒体であって、

上記コンテンツのコピー後に、上記コピー許可情報を削除するステップ

- 20 を有すること

を特徴とする記憶媒体。

13. (補正後) 請求項10から請求項12のうち、いずれか一項記載の記憶媒体であって、

- 25 上記サーバ装置から送信される、上記コピーするコンテンツを暗号化するための暗号化鍵を受信するステップと、

上記コンテンツを、上記暗号化鍵で暗号化してコピーするステップと、
上記暗号化鍵を記憶手段に記憶するステップと、

上記コピーされたコンテンツを再生する際に、上記記憶手段に記憶されている暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップと

を有することを特徴とする記憶媒体。

14. (補正後) 請求項10から請求項13のうち、いずれか一項記載の記憶媒体であって、

- 10 上記媒体識別情報及び装置識別情報を送信するステップでは、ユーザ端末装置自体に固有に付された端末識別情報、上記第1の記憶装置の第1の装置識別情報、及びユーザ端末装置を構成する第2の記憶装置に固有に付された第2の装置識別情報のうち、いずれか1つ或いは複数を組み合わせて上記装置識別情報として上記サーバ装置に送信すること
- 15 を特徴とする記憶媒体。

15. (補正後) ユーザ端末装置から送信される、該ユーザ端末装置を構成する装置に固有に付された装置識別情報、及び所定のコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記受信した媒体識別情報が、上記受信した装置識別情報に関連付けされて登録されているか否かを検出するステップと、

- 25 上記受信した媒体識別情報の未登録が検出された際に、上記受信した装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコ

ピーを許可するコピー許可情報を送信するステップと

を有するサーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

- 5 16. (補正後) 所定のコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、
- ユーザが上記コンテンツのコピーを行う際に使用するユーザ端末装置を構成する装置に対して固有に付された装置識別情報を読み出すステップと、

- 10 少なくとも上記読み出した媒体識別情報及び装置識別情報を、所定のサーバ装置に送信するステップと、

上記媒体識別情報及び装置識別情報を送信することで、上記サーバ装置から送信される、上記コンテンツのコピーを許可するコピー許可情報を受信するステップと、

- 15 上記受信したコピー許可情報を用いて、上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第1の記憶装置にコピーするステップと

を有するユーザ端末装置の情報処理プログラム。

- 20 17. (補正後) ユーザ端末装置から送信される、該ユーザ端末装置を構成する装置に固有に付された装置識別情報、及び所定のコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

- 対応する装置識別情報に関連付けされた状態で、コンテンツのコピー
- 25 が行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記受信した媒体識別情報が、上記受信した装置識別情報に関連付けされ

て登録されているか否かを検出するステップと、

上記受信した媒体識別情報の未登録が検出された際に、上記受信した装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可情報を送信するステップと

5 を有するサーバ装置の情報処理プログラム。

18. (補正後) 固有の媒体識別情報が付された記憶媒体に記憶されているコンテンツのコピーを行う際に、該媒体識別情報と共に、ユーザ端末装置を構成する装置に固有に付された装置識別情報を、該ユーザ端末装置からサーバ装置に送信し、

上記サーバ装置において、対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記送信された媒体識別情報が、上記送信された装置識別情報に関連付けされて登録されているか否かを検出し、

15 上記データベースに、上記媒体識別情報が未登録であった場合に、上記サーバ装置から、上記送信された装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可情報を送信する

コピー管理方法。

20

19. (削除)

20. (削除)

25 21. (削除)

2 2 . (削 除)

2 3 . (削 除)

5

2 4 . (削 除)

2 5 . (削 除)

10 2 6 . (削 除)

条約 19 条に基づく説明書

請求の範囲第 1 項は、ユーザ端末装置は、複数の装置で構成され、そのうちの第 1 の記憶装置が、記憶媒体に記憶されているコンテンツのコピーを行う旨と、ユーザ端末装置に付された固有の装置識別情報（ユーザ端末装置を構成する全ての装置の装置識別情報、或いはユーザ端末装置を構成する一部の装置の装置識別情報の両方を含む概念である。）、及び記憶媒体に固有に付されている媒体識別情報がユーザ端末装置からサーバ装置に対して送信された際に、該サーバ装置からユーザ端末装置に送信される「コピー許可情報」に基づいて、上記コンテンツのコピーが行われる旨を明確化したものである。

請求の範囲第 3 項は、上記ユーザ端末装置は第 1, 第 2 の記憶装置を含む複数の装置で構成され、当該ユーザ端末装置から上記サーバ装置に送信される装置識別情報としては、当該ユーザ端末装置を構成する一つ或いは複数の装置の装置識別情報が送信される旨を明確化したものである。

請求の範囲第 10 項は、ユーザ端末装置で実行されるコンピュータプログラムの各ステップが記憶された記憶媒体において、装置識別情報を読み出すステップでは、ユーザ端末装置を構成する複数の装置にそれぞれ固有に付されている装置識別情報のうち、全部の装置識別情報、或いは一部の装置識別情報を読み出し、これを媒体識別情報と共にサーバ装置に送信し、これら各情報を送信することでサーバ装置から送信されるコピー許可情報に基づいて、記憶媒体に記憶されているコンテンツを第 1 の記憶装置にコピーすることを明確化したものである。

請求の範囲第 14 項は、上記ユーザ端末装置は第 1, 第 2 の記憶装置を含む複数の装置で構成され、上記装置識別情報を送信するステップでは、当該ユーザ端末装置を構成する一つ或いは複数の装置の装置識別情報を送信する旨を明確化したものである。

請求の範囲第 15 項は、サーバ装置で実行されるコンピュータプログラムの各ステップが記憶された記憶媒体において、ユーザ端末装置から送信される、当該ユーザ端末装置を構成する複数の装置にそれぞれ固有に付されている装置識別情報のうち、全部の装置識別情報、或いは一部の装置識別情報を、媒体識別情報と共に受信し、この受信により記憶媒体に記憶されているコンテンツのコピーを許可するコピー許可情報をユーザ端末装置に送信する旨を明確化したものである。

請求の範囲第 16 項は、ユーザ端末装置で実行されるコンピュータプログラムにお

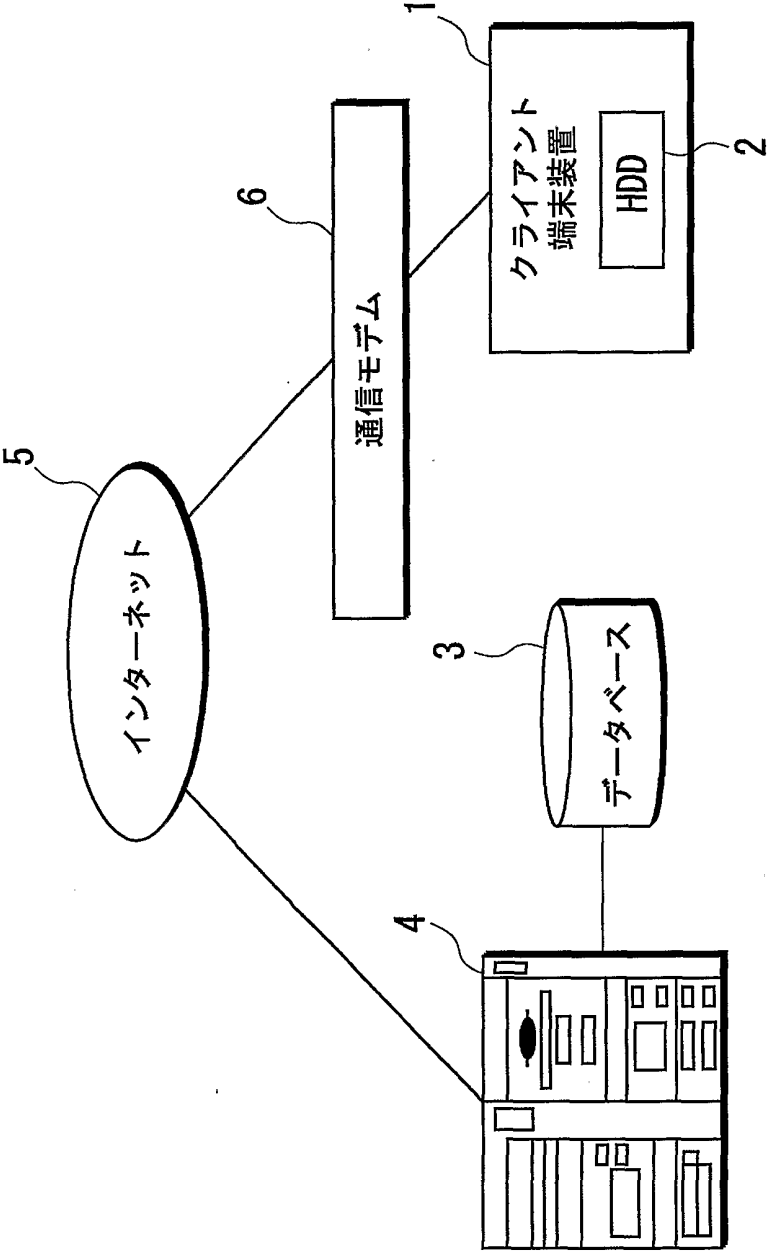
いて、装置識別情報を読み出すステップでは、ユーザ端末装置を構成する複数の装置にそれぞれ固有に付されている装置識別情報のうち、全部の装置識別情報、或いは一部の装置識別情報を読み出し、これを媒体識別情報と共にサーバ装置に送信し、これら各情報を送信することでサーバ装置から送信されるコピー許可情報に基づいて、記憶媒体に記憶されているコンテンツを第1の記憶装置にコピーすることを明確化したものである。

請求の範囲第17項は、サーバ装置で実行されるコンピュータプログラムにおいて、ユーザ端末装置から送信される、当該ユーザ端末装置を構成する複数の装置にそれぞれ固有に付されている装置識別情報のうち、全部の装置識別情報、或いは一部の装置識別情報を、媒体識別情報と共に受信し、この受信により記憶媒体に記憶されているコンテンツのコピーを許可するコピー許可情報をユーザ端末装置に送信する旨を明確化したものである。

請求の範囲第18項は、ユーザ端末装置は、複数の装置で構成され、そのうちの第1の記憶装置が、記憶媒体に記憶されているコンテンツのコピーを行う旨と、ユーザ端末装置に付された固有の装置識別情報（ユーザ端末装置を構成する全ての装置の装置識別情報、或いはユーザ端末装置を構成する一部の装置の装置識別情報の両方を含む概念である。）、及び記憶媒体に固有に付されている媒体識別情報がユーザ端末装置からサーバ装置に対して送信された際に、該サーバ装置からユーザ端末装置に対して「コピー許可情報」を送信することで、記憶媒体に記憶されているコンテンツのコピー管理を行う旨を明確化したものである。

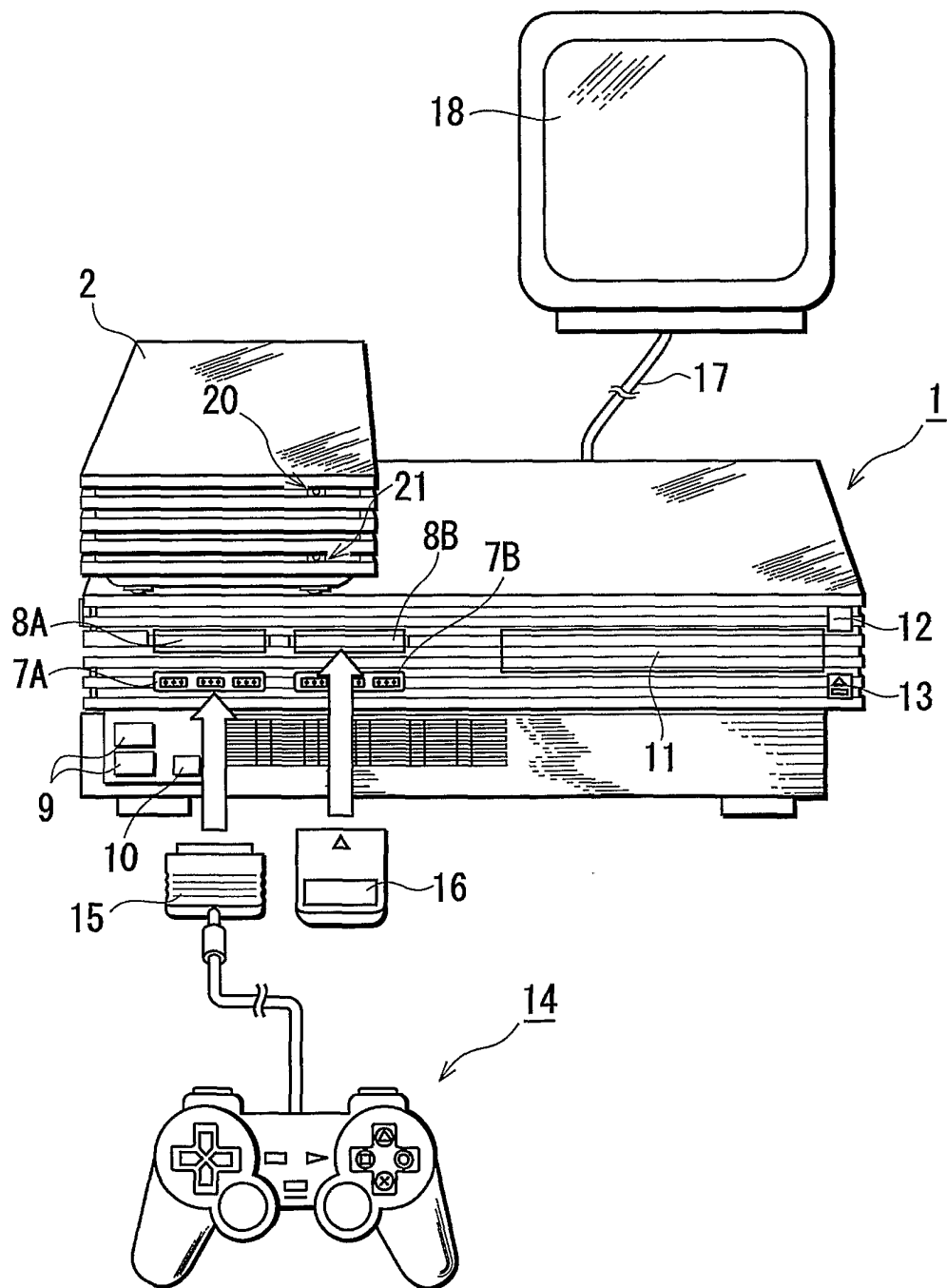
請求の範囲第19項から第26項は削除した。

図1



2/15

図2



3/15

図3

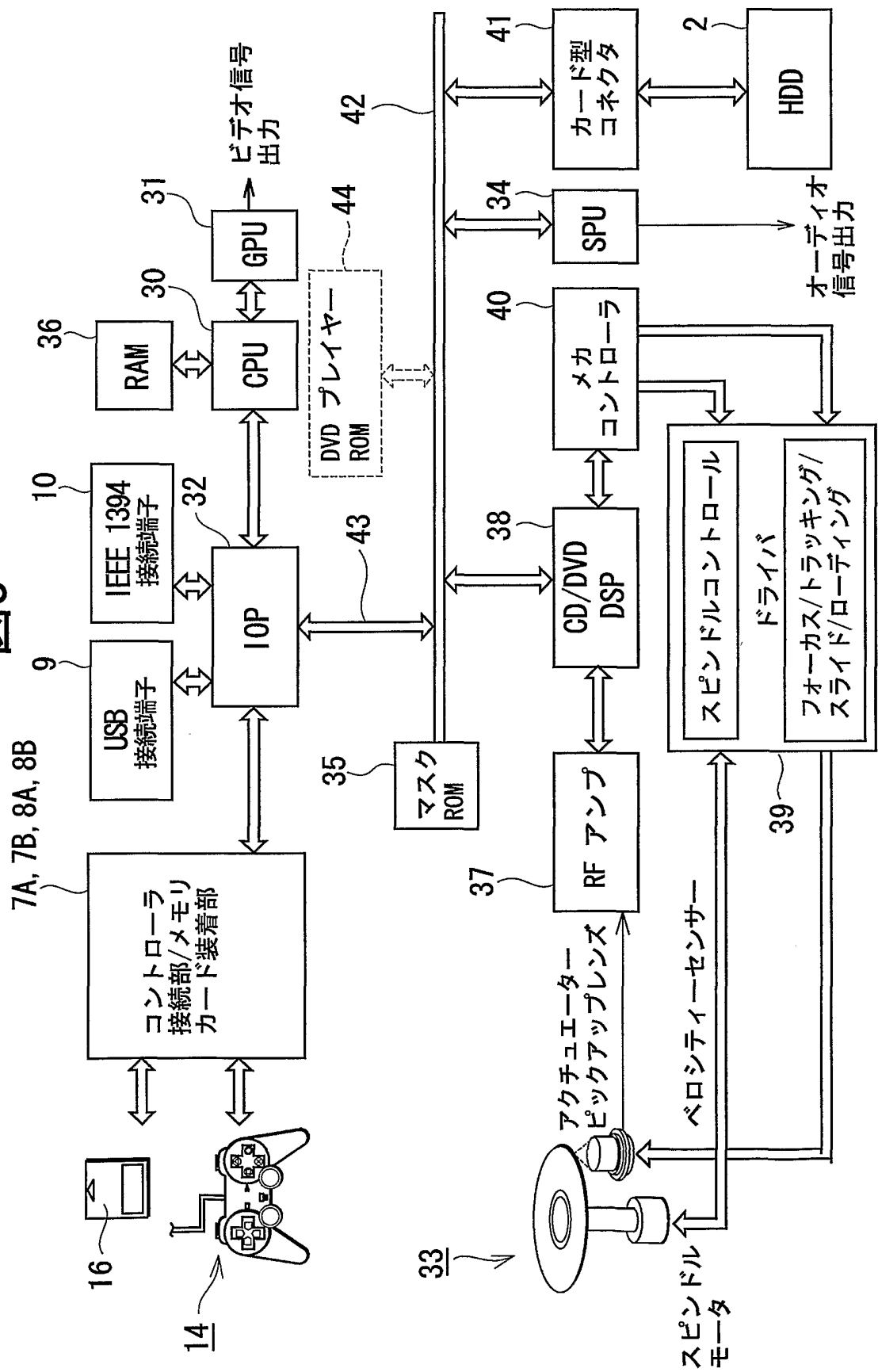
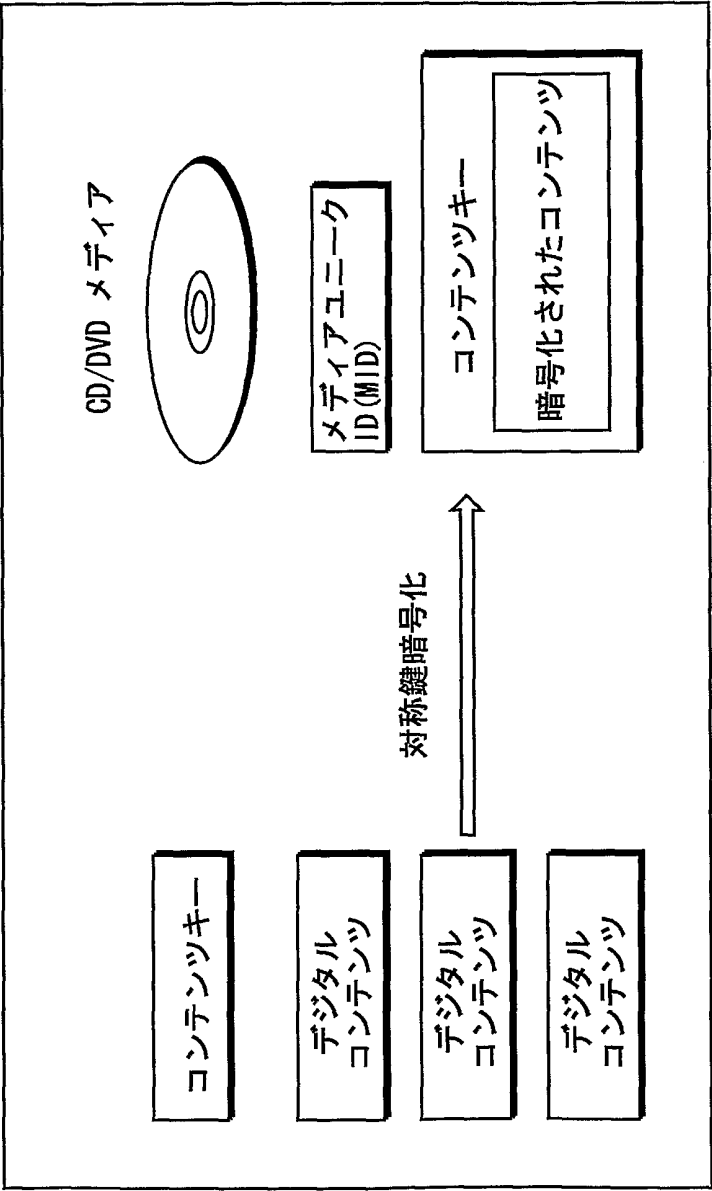


図4



5/15

図5

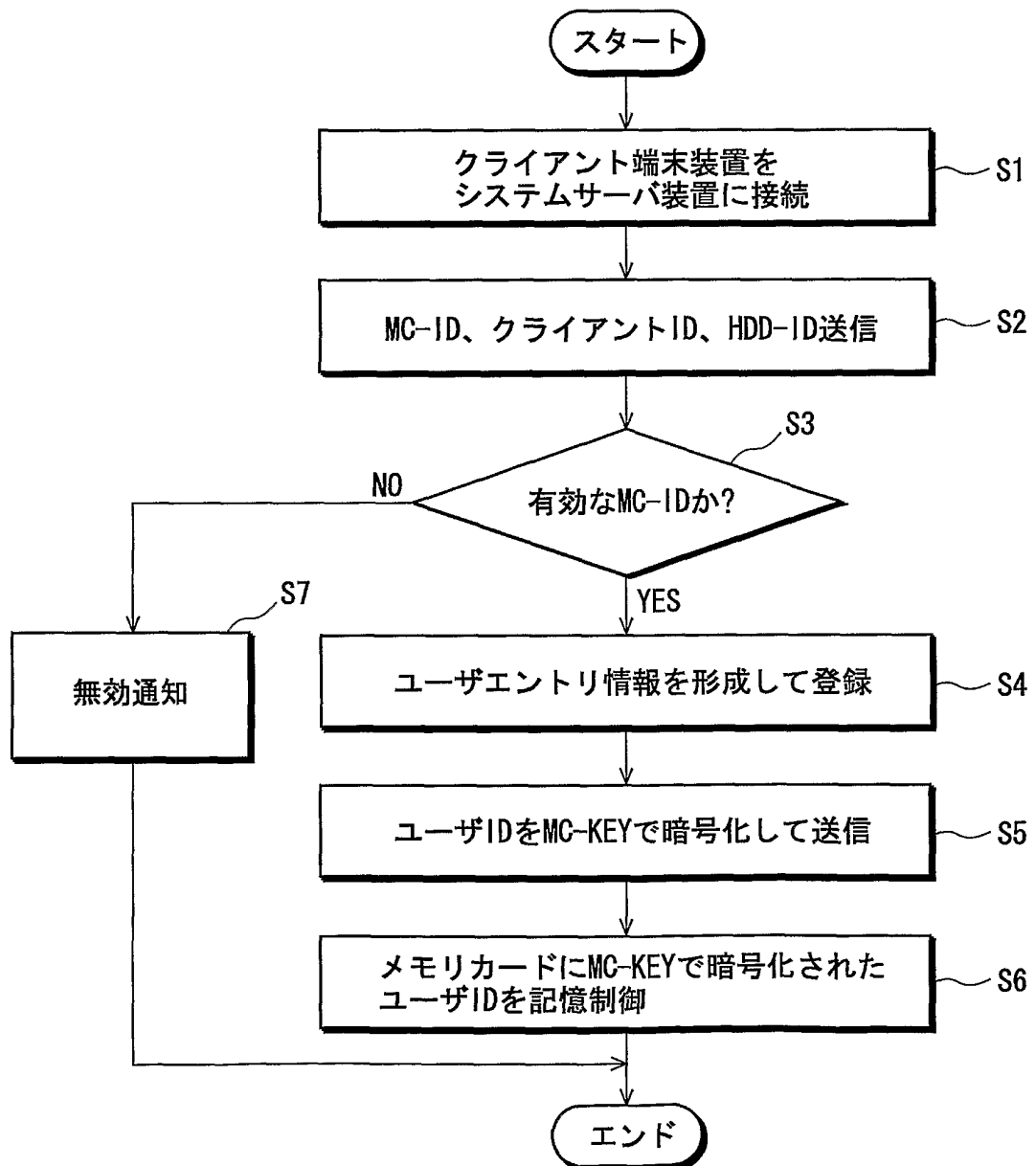
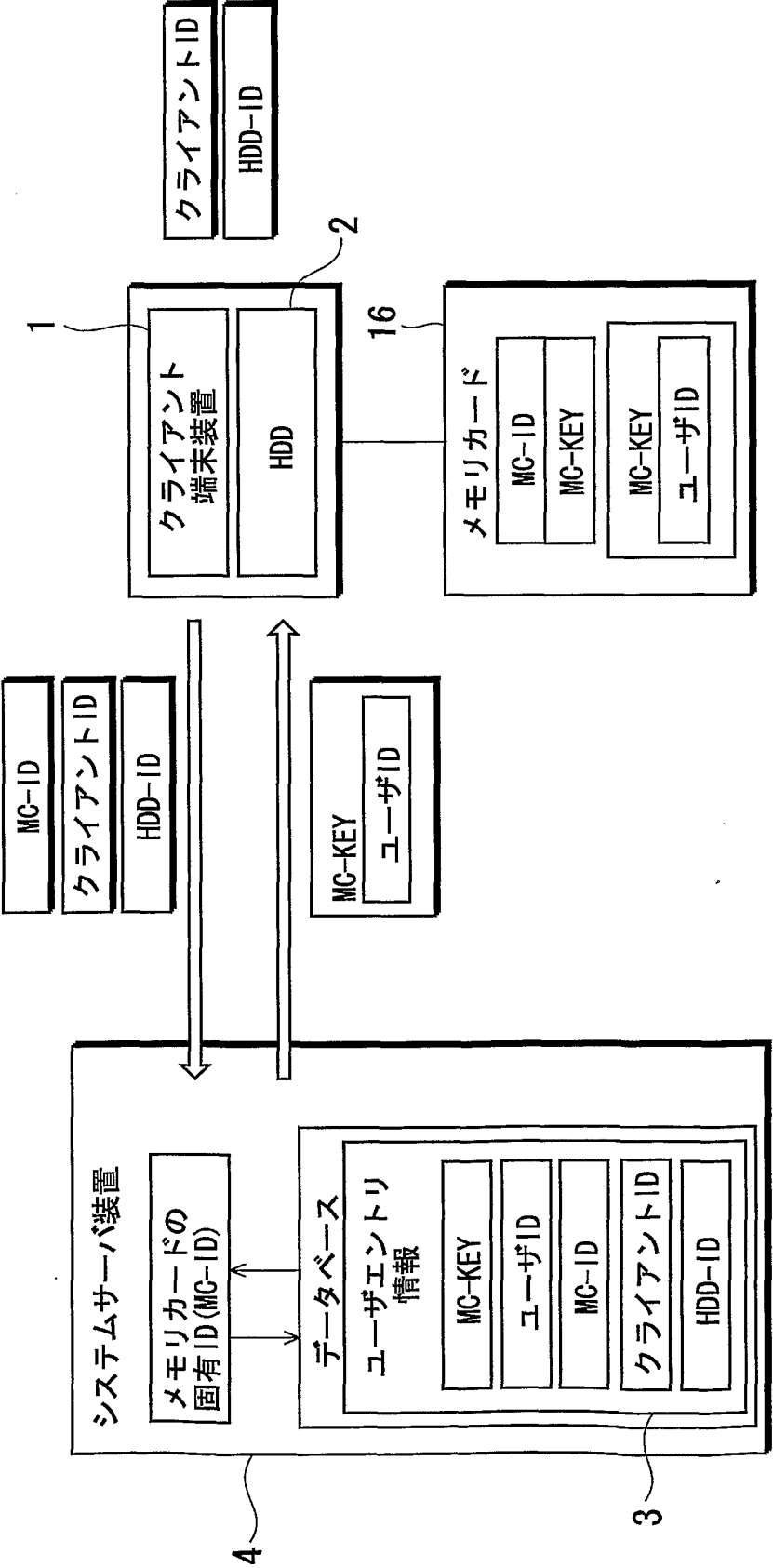
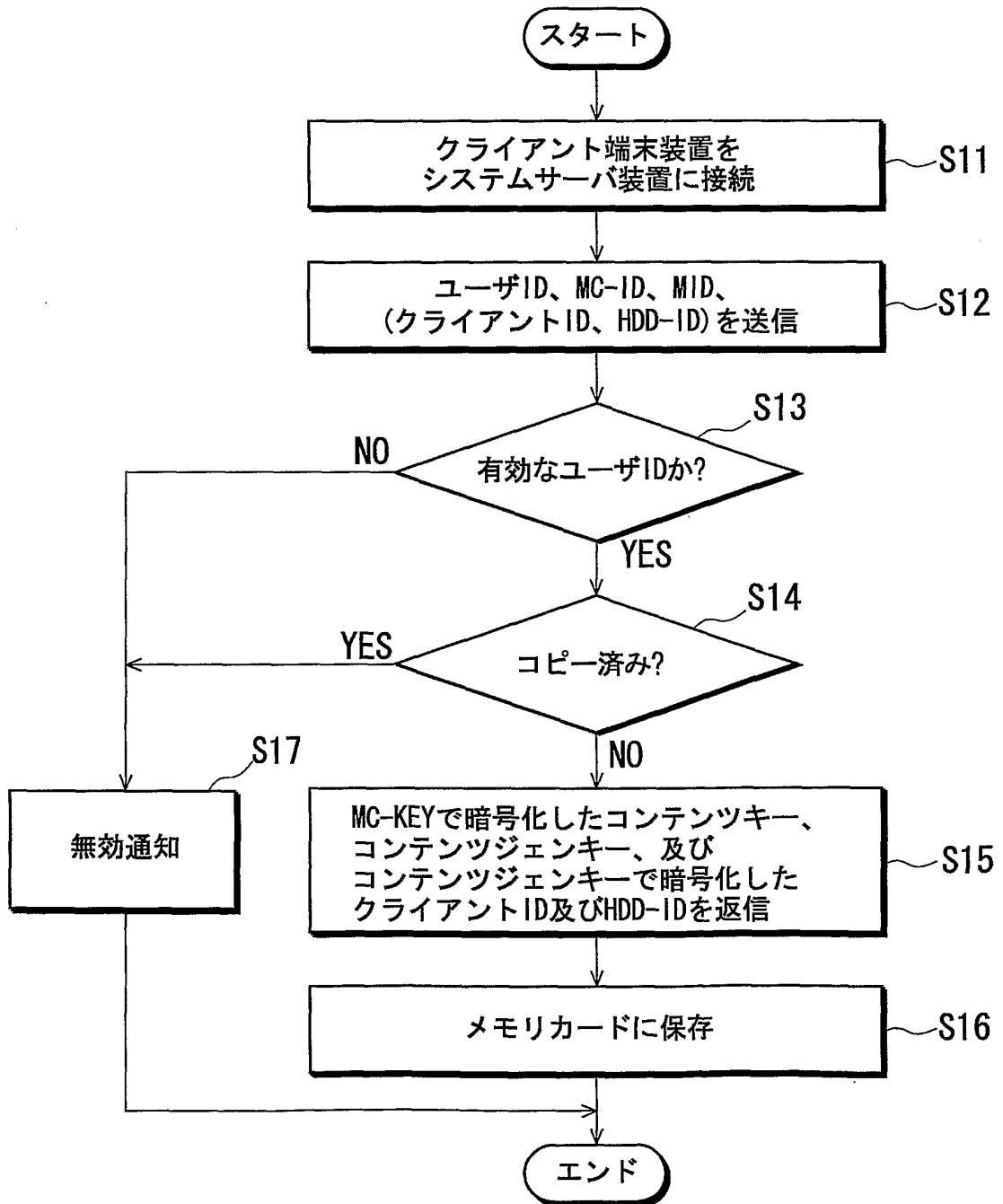


図6



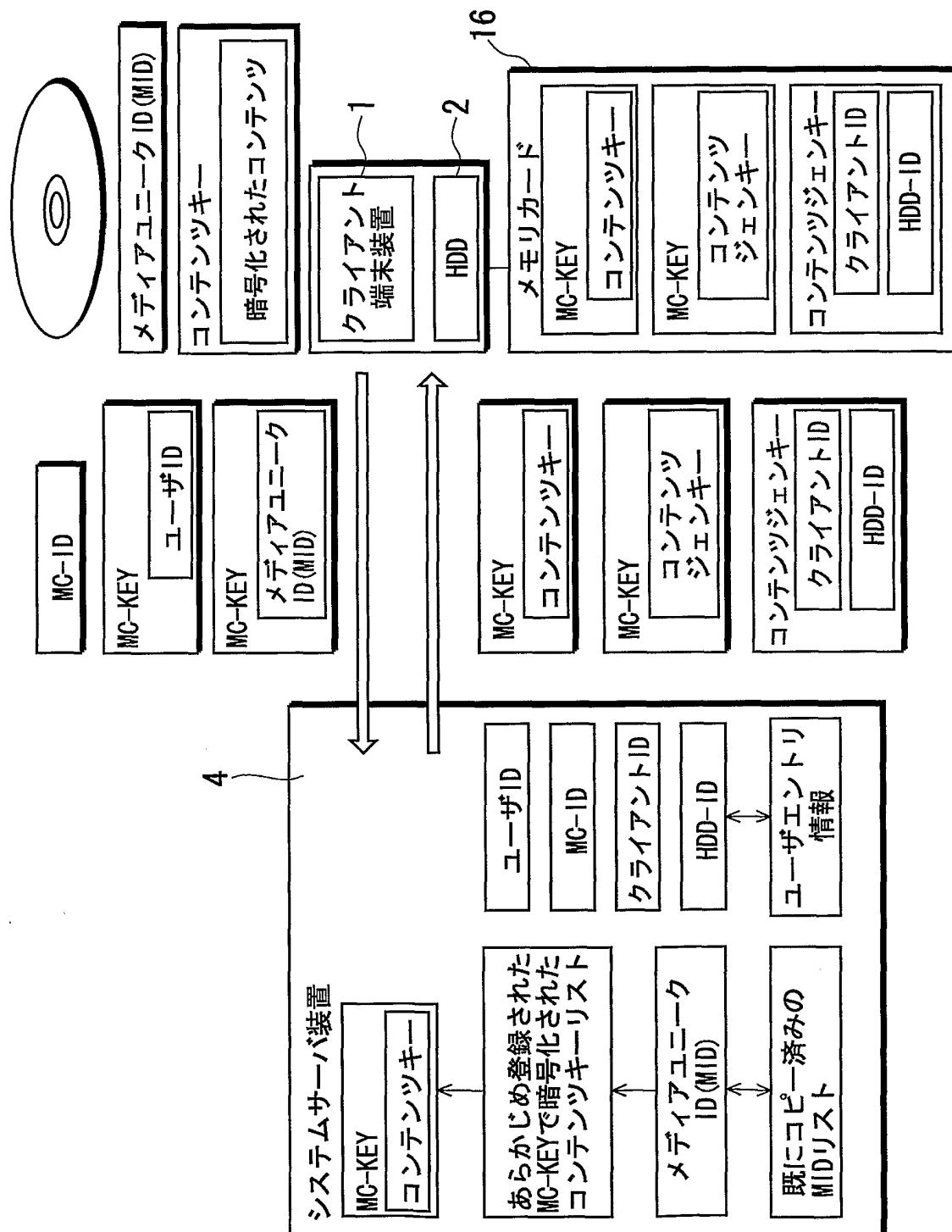
7/15

図7



8/15

図8



9/15

図9

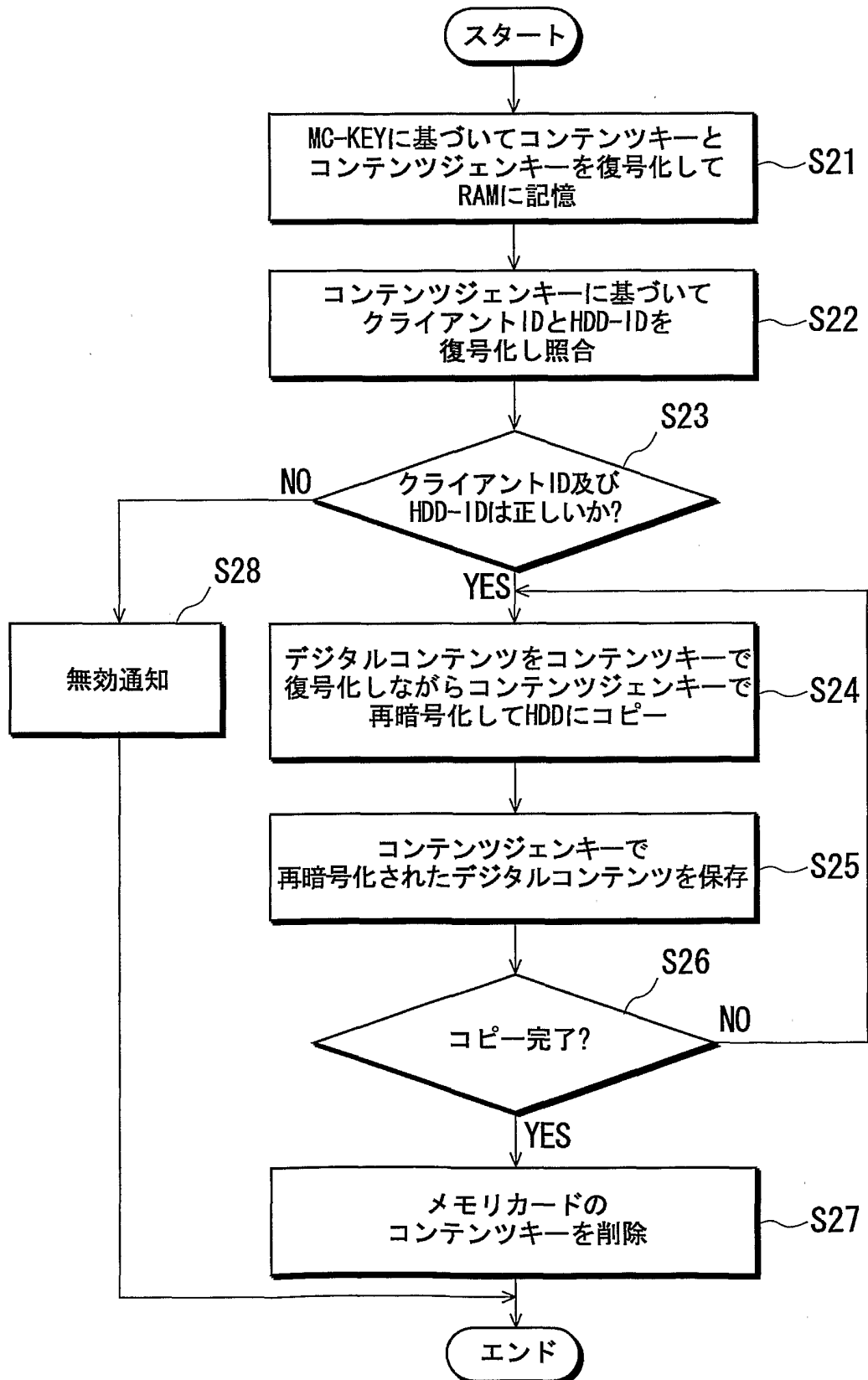
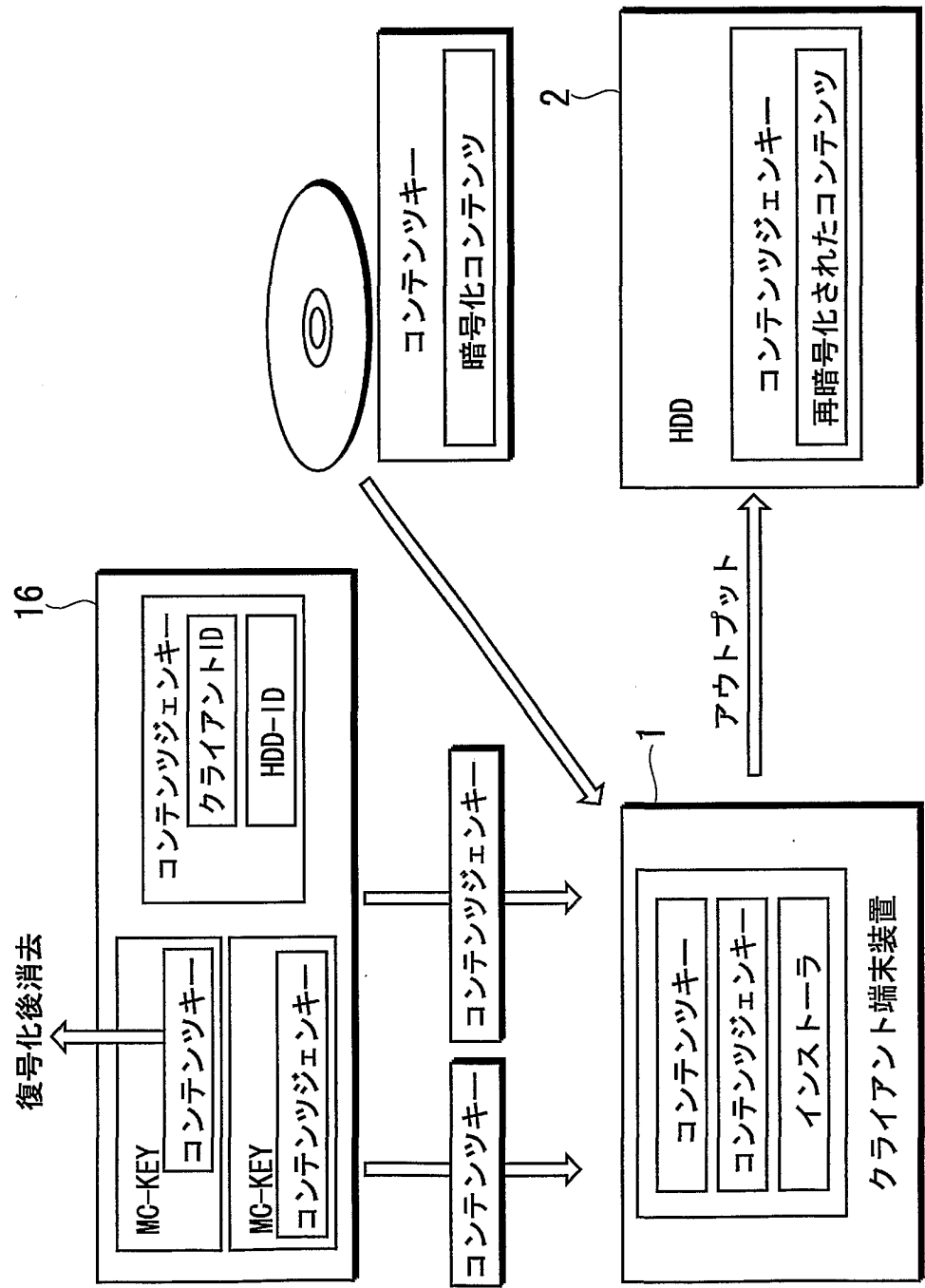


図10



11/15

図11

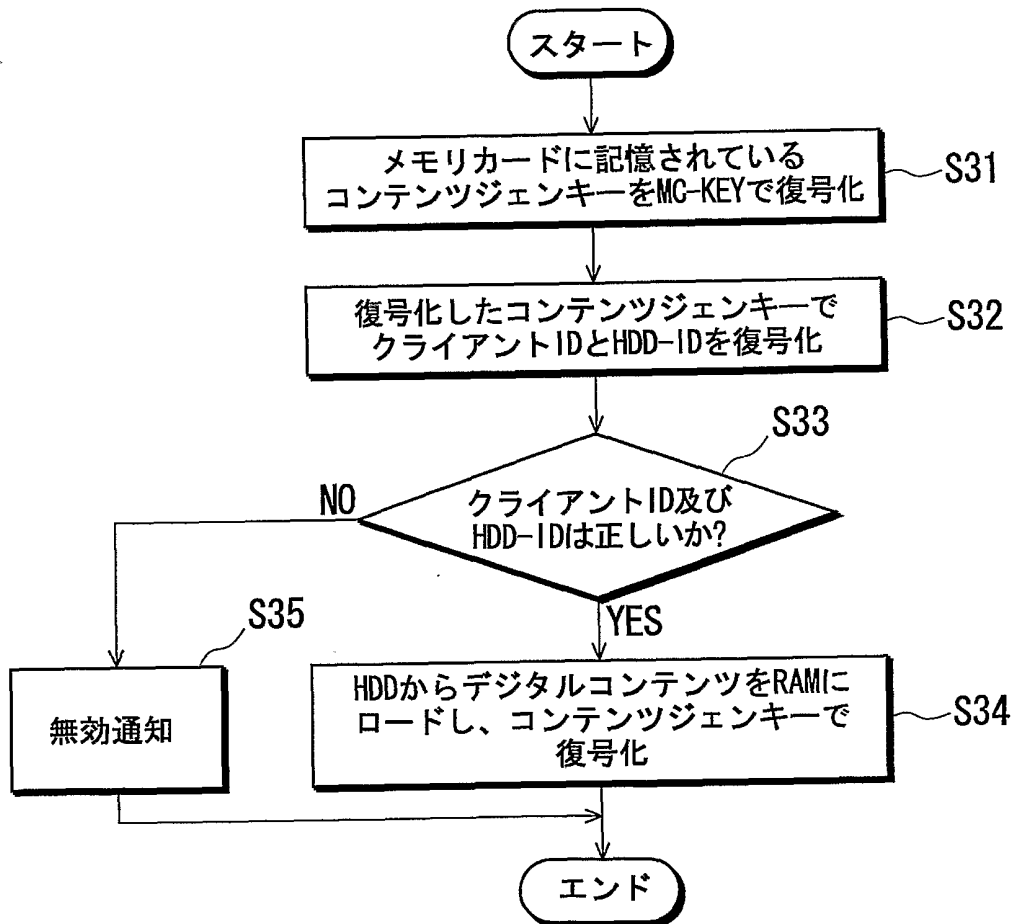
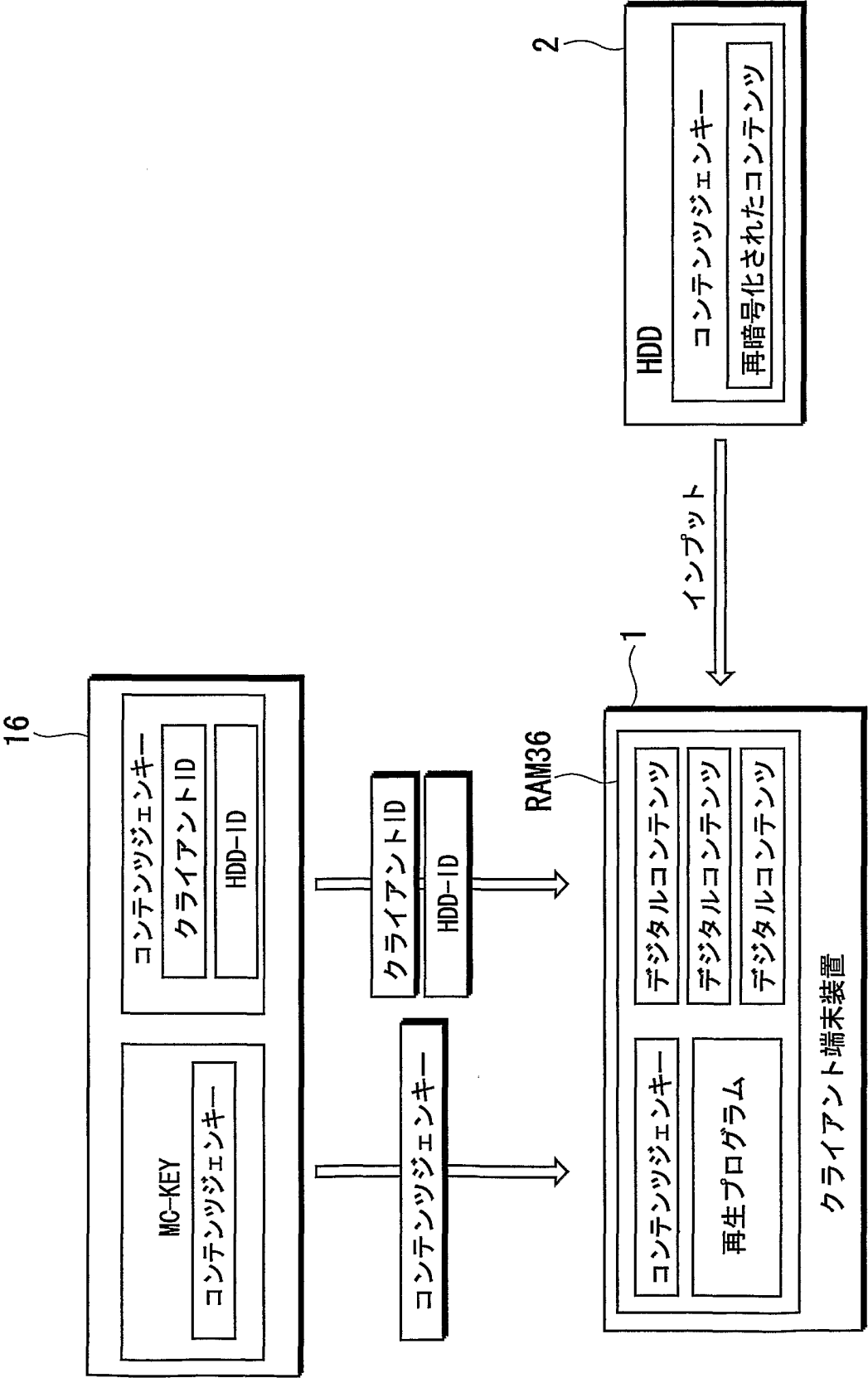


図12



13/15

図13

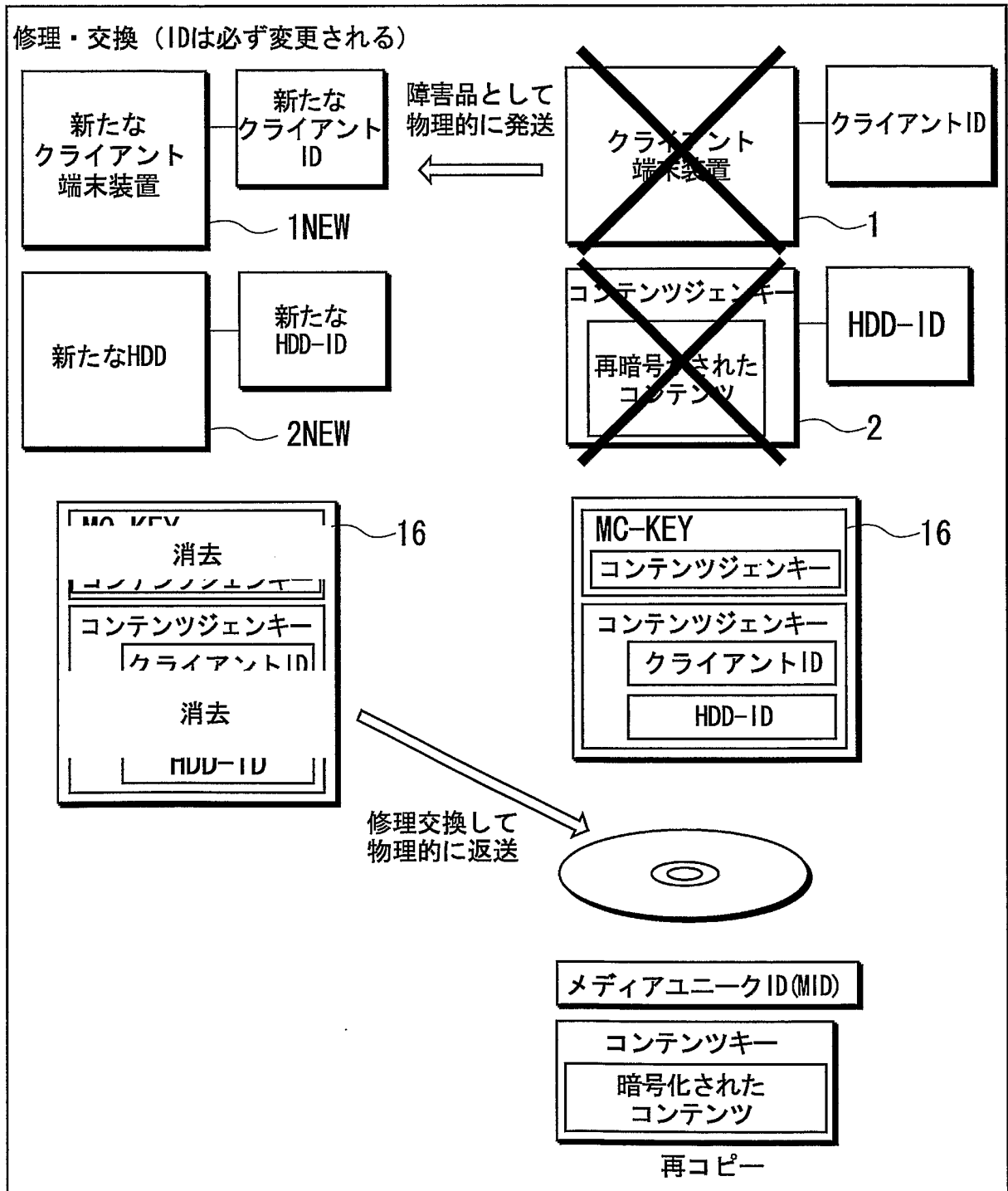
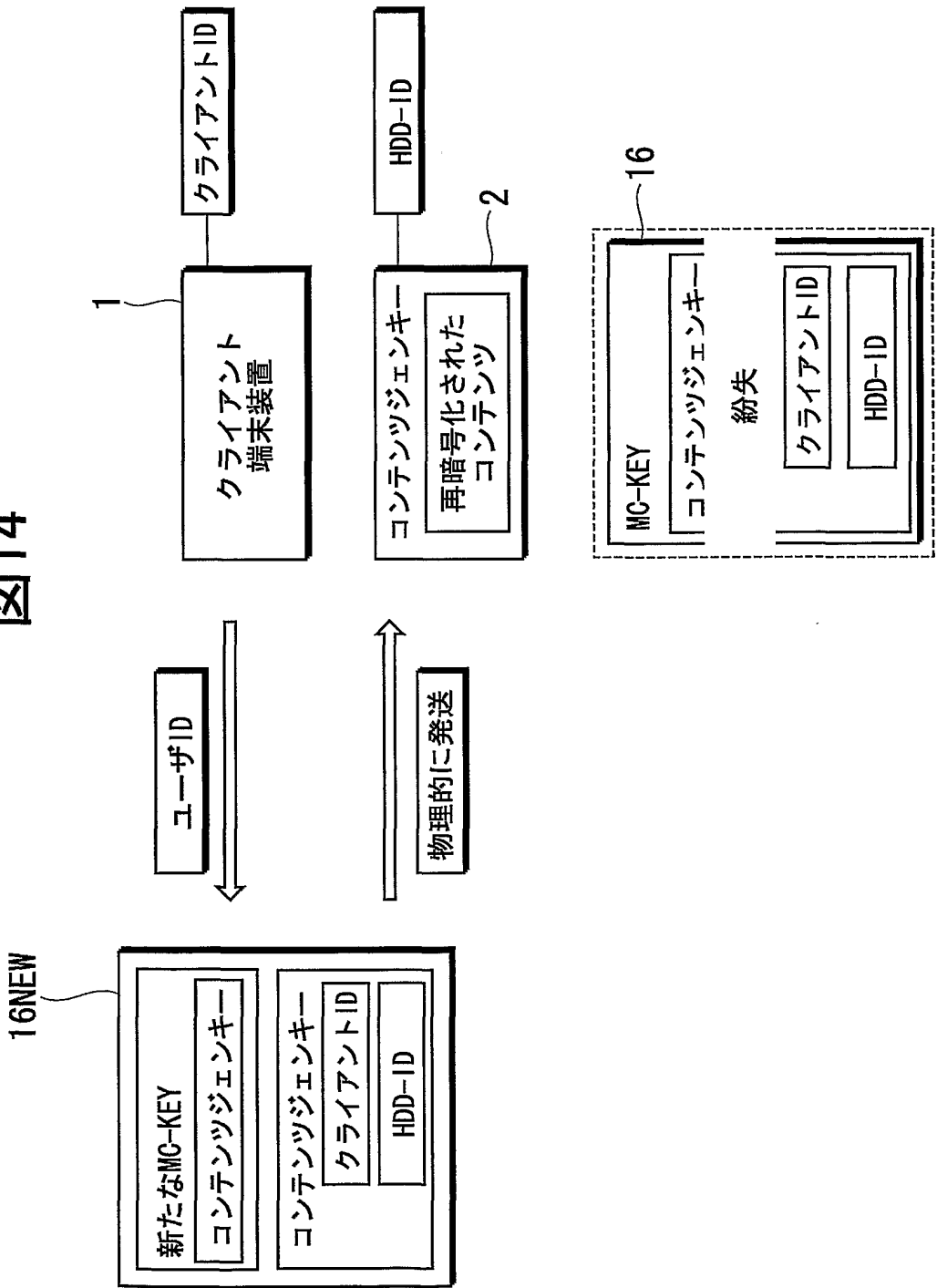
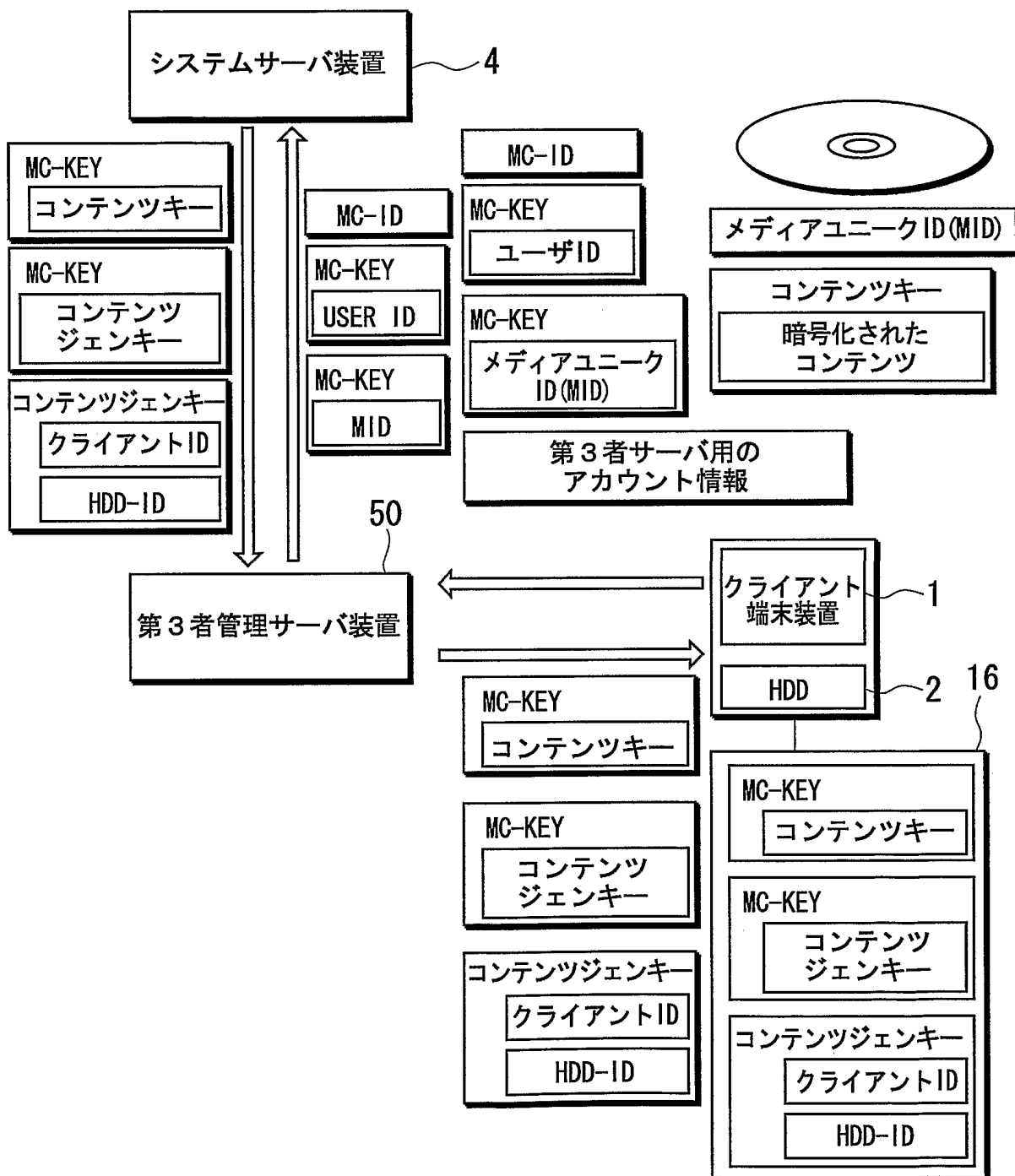


図14



15/15

図15



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/01452

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G11B20/10, G06F9/06, G06F12/14, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G11B20/10, G06F9/06, G06F12/14, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-83297 A (Fujitsu Ltd.), 13 March, 1998 (13.03.98), All pages; full text & EP 809244 A2 & CN 1166029 A & US 5805699 A & KR 236697 B	1-26
Y	YOSHIO, "Kogata Memory Card de Ongaku Chosakuken O Mamoru", Nikkei Electronics, Nikkei Business Publications, Inc., 22 March, 1999 (22.03.99), No.739, pages 49 to 53	1-26
Y	EDA, IMAI, "Pasocon ID Sengen", Nikkei Electronics, Nikkei Business Publications, Inc., 05 April, 1999 (05.04.99), No.740, pages 97 to 113	1-26

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
07 May, 2002 (07.05.02)

Date of mailing of the international search report
21 May, 2002 (21.05.02)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/01452

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Mary Foley, "Mirosoft and piracy: Try, try again", ZDNet News, [online], 11 January, 2001 (11.01.01), [retrieved on 07 May, 2002 (07.05.02)], Retrieved from the Internet: <URL: http://zdnet.com.com/2100-11-527150.html>	1-26
Y	Mary Foley, "Whistler Shin β Ban, Interface Kairyo shi Iho Copy Boshi no Shinkino mo", ZDNet Japan, [online], 09 January, 2001 (09.01.01), [retrieved on 07 May 2002 (07.05.02)], Retrieved from the Internet: <URL: http://www.zdnet.co.jp/news/0101/09/e_whistler.html>	1-26
Y	JP 2000-305853 A (Victor Company Of Japan, Ltd.), 02 November, 2000 (02.11.00), All pages; full text & EP 1047062 A2 & CN 1271907 A	1-26
Y	JP 9-134330 A (Fujitsu Ltd.), 20 May, 1997 (20.05.97), All pages; full text & EP 773490 A1 & US 5857021 A	1-26
Y	MOTOIKE, KIYONO, "DVD o Mochiita Contents Ryutsu Service", Matsushita Technical Journal, Matsushita Electric Industrial Co., Ltd., 18 October, 1998 (18.10.98), Vol.44, No.5, pages 25 to 33	2,5,8,9, 12,20
Y	JP 9-97174 A (Mitsubishi Electric Corp.), 08 April, 1997 (08.04.97), All pages; full text (Family: none)	15-22,24,26

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl ⁷ G11B 20/10 G06F 9/06 G06F12/14 G06F15/00		
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl ⁷ G11B 20/10 G06F 9/06 G06F12/14 G06F15/00		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1926 - 1996 日本国公開実用新案公報 1971 - 2002 日本国登録実用新案公報 1994 - 2002 日本国実用新案登録公報 1996 - 2002		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-83297 A (富士通株式会社) 1998.03.13, 全頁, 全文 & EP 809244 A2 & CN 1166029 A & US 5805699 A & KR 236697 B	1-26
Y	芳尾, " 小型メモリ・カードで音楽著作権を守る", 日経エレクトロニクス, 日経BP社, 1999.03.22, no.739, p.49-53	1-26
Y	枝, 今井, " パソコンID宣言", 日経エレクトロニクス, 日経BP社, 1999.04.05, no.740, p.97-113	1-26
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 07.05.02	国際調査報告の発送日 21.05.02	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 原 秀人  5 N 3 0 4 4 電話番号 03-3581-1101 内線 3585	

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	Mary Foley, "Microsoft and piracy: Try, try again", ZDNet News, [online], 2001.01.11, [retrieved on 2002-05-07], Retrieved from the Internet: <URL: http://zdnet.com.com/2100-11-527150.html>	1-26
Y	Mary Foley, "Whistler新β版, インタフェース改良し違法コピー防 止の新機能も", ZDNet Japan, [online], 2001.01.09, [retrieved on 2002-05-07], Retrieved from the Internet: <URL: http://www.zdnet.co.jp/news/0101/09/e_whistler.html>	1-26
Y	JP 2000-305853 A (日本ビクター株式会社) 2000.11.02, 全頁, 全文 & EP 1047062 A2 & CN 1271907 A	1-26
Y	JP 9-134330 A (富士通株式会社) 1997.05.20, 全頁, 全文 & EP 773490 A1 & US 5857021 A	1-26
Y	本池, 清野, "DVDを用いたコンテンツ流通サービス", Matsushita Technical Journal, 松下電器産業株式会社, 1998.10.18, Vol.44, No.5, p.25-33	2, 5, 8, 9, 12, 20
Y	JP 9-97174 A (三菱電機株式会社) 1997.04.08, 全頁, 全文 (ファミリーなし)	15-22, 24, 26