(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－269289

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	17/60		Ｃ０６Ｆ	15/21	３３０
	1/00	３７０		1/00	３７０Ｆ
	9/06	５５０		9/06	５５０Ｚ
	15/00	３３０		15/00	３３０Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｃ０９Ｃ	1/00	６６０Ｆ

審査請求　未請求　請求項の数37　ＯＬ　（全 39 頁）　最終頁に続く

(21)出願番号　特願平9－74182

(22)出願日　平成９年(1997)３月26日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　真有　浩一
東京都品川区北品川６丁目７番35号　ソニー株式会社内

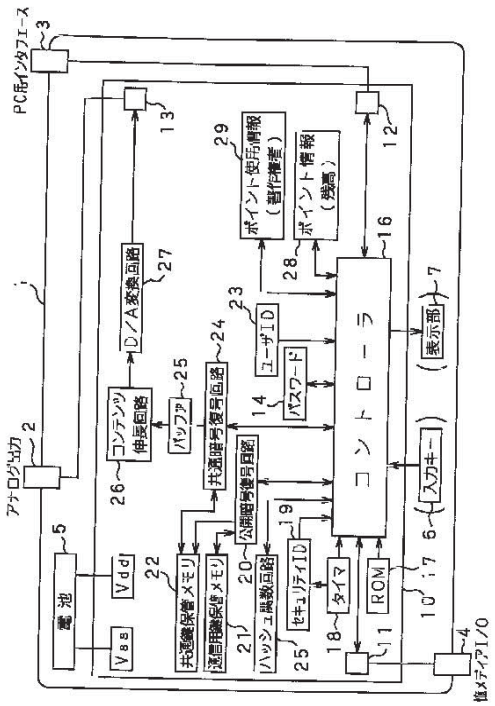
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　ディジタルコンテンツ配付管理方法、ディジタルコンテンツ再生方法及び装置

(57)【要約】

【課題】　簡単に持ち運びができて何時でも何処でもディジタルコンテンツを楽しむことを可能とし、ディジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築する。

【解決手段】　暗号化されたコンテンツ鍵を復号化し、セッション鍵を暗号化する公開暗号復号回路２０と、コンテンツ鍵やセッション鍵を保管する共通鍵保管メモリ２２と、公開暗号方式の鍵情報を保管する通信用鍵保管メモリ２１と、ポイント情報を格納するポイント情報格納メモリ２９と、ポイント使用情報を格納するポイント使用情報格納メモリ２８と、暗号化ディジタルコンテンツの復号化し、暗号化ポイント情報の復号化、ポイント使用情報の暗号化を行う共通暗号復号回路２４と、圧縮ディジタルコンテンツを伸長する伸長回路２６と、ディジタルコンテンツをＤ／Ａ変換するＤ／Ａ変換回路２７とを、１チップ化する。



【特許請求の範囲】
【請求項１】　ディジタルコンテンツを、当該ディジタルコンテンツ毎のコンテンツ鍵を用いて暗号化すると共に、圧縮するディジタルコンテンツ加工工程と、
上記加工したディジタルコンテンツを、通信相手側からのディジタルコンテンツ送信要求に応じて送信するコンテンツ送信工程と、
上記加工されたディジタルコンテンツの復号化に使用するコンテンツ鍵を暗号化し、通信相手側からのコンテンツ鍵送信要求に応じて送信するコンテン鍵送信工程と、
上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報を暗号化し、通信相手側からの課金情報送信要求に応じて送信する課金情報送信工程と、
通信相手側から送信されてきた暗号化されたコンテンツ使用情報を受信して復号化するコンテンツ使用情報受信工程と、
上記コンテンツ使用情報に基づいて徴収した利用金を、上記ディジタルコンテンツの権利者に対して分配する利用金分配工程とを有してなることを特徴とするディジタルコンテンツ配付管理方法。
【請求項２】　上記コンテンツ鍵は共通鍵であることを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。
【請求項３】　上記コンテンツ鍵を通信相手側の公開鍵を用いて暗号化することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。
【請求項４】　通信相手側から送信されてきた暗号化された共通鍵を受信して復号化する共通鍵復号化工程を有することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。
【請求項５】　上記共通鍵はセッション鍵であることを特徴とする請求項４記載のディジタルコンテンツ配付管理方法。
【請求項６】　上記課金情報送信工程では、課金情報を上記共通鍵を用いて暗号化することを特徴とする請求項４記載のディジタルコンテンツ配付管理方法。
【請求項７】　上記コンテンツ使用情報受信工程では、上記暗号化されたコンテンツ使用情報の復号化に上記共通鍵を用いることを特徴とする請求項４記載のディジタルコンテンツ配付管理方法。
【請求項８】　上記コンテンツ使用情報受信工程では、上記通信相手側からの上記課金情報の送信要求に伴って当該通信相手側から送信されてくる上記暗号化されたコンテンツ使用情報を受信することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。
【請求項９】　上記課金情報送信工程では、上記課金情報と共にコンテンツの使用条件を示す情報を送信することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。
【請求項１０】　暗号化及び圧縮処理によって加工されたディジタルコンテンツを受信して格納するコンテンツ受信工程と、
上記加工されたディジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を生成するコンテンツ鍵要求情報生成工程と、
上記コンテンツ鍵要求情報を暗号化して送信するコンテンツ鍵要求情報送信工程と、
上記コンテンツ鍵の要求に応じて送信されてきたコンテンツ鍵を受信するコンテンツ鍵受信工程と、
上記コンテンツ鍵に施されている暗号化を復号化するコンテンツ鍵復号化工程と、
上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管工程と、
上記加工されたディジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化工程と、
上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を生成する課金情報要求情報生成工程と、
上記課金情報要求情報を暗号化して送信する課金情報要求情報送信工程と、
上記課金情報の要求に応じて送信されてきた課金情報を受信すると共に当該課金情報に施されている暗号化を復号化して格納する課金情報受信工程と、
上記加工されたディジタルコンテンツを伸長するコンテンツ伸長工程と、
上記加工されたディジタルコンテンツの復号化に応じたコンテンツ使用情報を生成して格納するコンテンツ使用情報格納工程と、
上記コンテンツ使用情報を暗号化して送信するコンテンツ使用情報送信工程とを有することを特徴とするディジタルコンテンツ再生方法。
【請求項１１】　コンテンツ使用情報格納工程では、上記格納されている課金情報の残高を確認し、上記加工されたディジタルコンテンツの復号化に応じて上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。
【請求項１２】　上記復号化及び伸長がなされたディジタルコンテンツをディジタル／アナログ変換するディジタル／アナログ変換工程を有することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。
【請求項１３】　上記コンテンツ受信工程では、上記加工されたディジタルコンテンツを外部記憶媒体に格納することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。
【請求項１４】　上記コンテンツ鍵は共通鍵であることを特徴とする請求項１０記載のディジタルコンテンツ再生方法。
【請求項１５】　上記コンテンツ鍵復号化工程では、上

記コンテンツ鍵を固有の秘密鍵を用いて復号化することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１６】　共通鍵を発生し、当該共通鍵を暗号化して送信する共通鍵送信工程を有することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１７】　上記共通鍵送信工程では、上記共通鍵としてセッション鍵を生成することを特徴とする請求項１６記載のディジタルコンテンツ再生方法。

【請求項１８】　上記課金情報要求情報送信工程では、上記課金情報要求情報を上記共通鍵を用いて暗号化することを特徴とする請求項１６記載のディジタルコンテンツ再生方法。

【請求項１９】　上記コンテンツ使用情報送信工程では、上記コンテンツ使用情報の暗号化に上記共通鍵を用いることを特徴とする請求項１６記載のディジタルコンテンツ再生方法。

【請求項２０】　上記コンテンツ使用情報送信工程では、上記課金情報要求情報生成工程による上記課金情報の要求に伴って、上記暗号化したコンテンツ使用情報を送信することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項２１】　上記課金情報受信工程では、上記課金情報と共に暗号化されて送信されてくるコンテンツの使用条件を示す情報をも受信することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項２２】　データ通信を行うデータ通信手段と、暗号化及び圧縮処理によって加工されたディジタルコンテンツを受信して記憶媒体に記憶させるコンテンツ記憶制御手段と、
暗号化されたコンテンツ鍵を復号化するコンテンツ鍵復号化手段と、
上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管手段と、
上記加工されたディジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化手段と、
上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報に施されている暗号化を復号化する課金情報復号化手段と、
上記復号化された課金情報を格納する課金情報格納手段と、
上記加工されたディジタルコンテンツを伸長するコンテンツ伸長手段と、
上記加工されたディジタルコンテンツの復号化に応じたコンテンツ使用情報を生成するコンテンツ使用情報生成手段と、
上記コンテンツ使用情報を格納するコンテンツ使用情報格納手段と、
上記コンテンツ使用情報を暗号化するコンテンツ使用情報暗号化手段とを有することを特徴とするディジタルコンテンツ再生装置。

【請求項２３】　上記加工されたディジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を暗号化するコンテンツ鍵要求情報暗号化手段と、
上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を暗号化する課金情報要求情報暗号化手段とを有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２４】　コンテンツ使用情報生成手段は、上記課金情報格納手段に格納されている課金情報の残高を確認し、上記加工されたディジタルコンテンツの復号化に応じて、上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２５】　上記復号化及び伸長がなされたディジタルコンテンツをディジタル／アナログ変換するディジタル／アナログ変換手段を有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２６】　上記コンテンツ記憶制御手段は、上記加工されたディジタルコンテンツを外部記憶媒体に記憶させることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２７】　上記コンテンツ鍵は共通鍵であることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２８】　装置固有の鍵を保管する固有鍵格保管段を有し、
上記コンテンツ鍵復号化手段では、上記固有鍵保管手段に保管している装置固有の秘密鍵を用いて、上記暗号化されているコンテンツ鍵を復号化することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２９】　共通鍵を発生する共通鍵発生手段と、上記共通鍵を暗号化する共通鍵暗号化手段とを有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項３０】　上記共通鍵発生手段は、上記共通鍵としてセッション鍵を生成することを特徴とする請求項２９記載のディジタルコンテンツ再生装置。

【請求項３１】　上記課金情報復号化手段は、上記課金情報を上記共通鍵を用いて復号化することを特徴とする請求項２９記載のディジタルコンテンツ再生装置。

【請求項３２】　上記コンテンツ使用情報暗号化手段は、上記コンテンツ使用情報を上記共通鍵を用いて暗号化することを特徴とする請求項２９記載のディジタルコンテンツ再生装置。

【請求項３３】　上記コンテンツ使用情報暗号化手段は、上記課金情報要求情報暗号化手段による上記課金情

報要求情報の暗号化に伴って、上記コンテンツ使用情報の暗号化を行うを有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。
【請求項３４】　上記課金情報復号化工程では、上記課金情報と共に暗号化されているコンテンツの使用条件を示す情報をも復号化することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。
【請求項３５】　携帯可能に構成されてなることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。
【請求項３６】　カード状の筐体を有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。
【請求項３７】　集積回路化してなることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばオーディオデータやビデオデータ等のディジタルコンテンツを配布し、それらディジタルコンテンツの利用量に応じて課金するシステムに好適なディジタルコンテンツ配付管理方法、並びにディジタルコンテンツ再生方法及び装置に関する。
【０００２】
【従来の技術】コンピュータプログラムやオーディオデータ、ビデオデータ等のディジタルコンテンツの流通を簡便化し、潜在需要を掘り下げ、市場拡大に有利な手法としては、例えば特公平６－１９７０７号公報に記載されるソフトウェア管理方式、特公平６－２８０３０号公報に記載されるソフトウェア利用管理方式、特公平６－９５３０２号公報に記載されるソフトウェア管理方式のような手法が存在する。上記特公平６－１９７０７号公報に記載されたソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、ソフトウェアの利用状況をソフトウェア権利者別などによって把握できるようにしたものである。また、特公平６－２８０３０号公報に記載されるソフトウェア利用管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムを買い取り（買い取った後は無料で使用できる）価格を付し、コンピュータシステム内には購入可能な金額を示すデータを設けておき、有償プログラム購入の際は、同システムにある利用可能なソフトウェアの名称としてテーブルに登録すると共に、当該購入可能金額を示すデータをソフトウェア価格分だけ減じ、また登録済みソフトウェアを該テーブルから抹消する際には状況に応じて該購入可能な金額を示すデータを増加更新するようにしたものである。また、上記特公平６－９５３０２号公報に記載されるソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムにつき実際の利用量（利用回数または利用時間など）に応じて利用料金を徴収するために、利用されたプログラムの識別と「利用者識別符号と料金とを記録」しておき、該記録を回収することでプログラム権利者が自分の所有するプログラムの利用料金を把握でき、プログラムの利用量に応じたプログラム利用料金を回収する場合のシステムで有効なものである。
【０００３】
【発明が解決しようとする課題】ところが、上述したディジタルコンテンツをネットワークを使って配信するシステムは、パーソナルコンピュータ上だけでの運用を考慮しており、したがって、簡単に持ち運びができ、何時でも、また何処でも上記ディジタルコンテンツを楽しむといったシステムは存在しない。
【０００４】一方、上述した各公報記載の手法は、潜在需要を掘り下げ、市場拡大に有利であるが、ディジタルコンテンツのコピー或いは不当な使用への防御として不十分であり、且つ経済的なシステムとは言い難い。
【０００５】そこで、本発明はこのような状況に鑑みてなされたものであり、簡単に持ち運びができて何時でも何処でもディジタルコンテンツを楽しむことを可能とし、また、ディジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築することをも可能にするディジタルコンテンツ配付管理方法、並びにディジタルコンテンツ再生方法及び装置を提供することを目的とする。
【０００６】
【課題を解決するための手段】本発明によれば、ディジタルコンテンツの配付側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手側から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしており、一方、ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報の生成を行い、このコンテンツ使用情報を配付側に送信するようにし、また本発明のディジタルコンテンツ再生装置は、携帯可能となされていることにより、上述した課題を解決する。
【０００７】
【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。
【０００８】先ず、本発明のディジタルコンテンツ配付方法、ディジタルコンテンツ再生方法及び装置の具体的内容及び構成の説明を行う前に、これらの理解を容易にするために、本発明が適用されるシステム全体の概略構成及びシステムの運用方法について図１から図７までの各図を用いて簡単に説明する。

【０００９】図１にはシステム全体の概略的な構成を示す。

【００１０】この図１において、ユーザ側２００は、本発明のディジタルコンテンツ再生装置（以下、プレーヤ１と呼ぶことにする）及びいわゆるパーソナルコンピュータ（以下、ユーザ端末５０と呼ぶことにする）を保有しているものとする。

【００１１】ユーザ端末５０は、通常のパーソナルコンピュータであるが、本発明に使用する後述する各種ソフトウェアをアプリケーションソフトとして格納してなると共に、表示手段であるディスプレイ装置と放音手段であるスピーカ、及び情報入力手段であるキーボードやマウス等が接続されてなるものである。当該ユーザ端末５０は例えばネットワークを介してシステム管理会社２１０と接続可能であり、また、プレーヤ１との間のインターフェイス手段を有し、データ送受が可能である。

【００１２】プレーヤ１は例えば図２に示すような構成を有するものである。

【００１３】この図２の構成の詳細な説明については後述するが、当該プレーヤ１は、ディジタルコンテンツの処理経路の主要構成要素として、暗号化されているディジタルコンテンツをコンテンツ鍵を用いて復号化する共通鍵暗号復号回路２４と、圧縮されているディジタルコンテンツを伸長する伸長手段である伸長回路２６と、ディジタルデータをアナログ信号に変換するＤ／Ａ変換回路２７とを少なくとも有する。なお、以下に言う復号化とは、暗号化を解くことである。

【００１４】また、このプレーヤ１は、使用するディジタルコンテンツの権利情報及び使用状況を示す情報（以下、これら情報をポイント使用情報と呼ぶ）や、ディジタルコンテンツを使用する際に必要となる保有金額データ、すなわちディジタルコンテンツを使用する毎に減額される課金データ（以下、ポイント情報と呼ぶ）等を扱う主要構成要素として、上記ポイント使用情報を格納するポイント使用情報格納メモリ２９と、上記ポイント情報を格納するポイント情報格納メモリ２８とを少なくとも備えている。

【００１５】さらに、このプレーヤ１は、後述するような暗号化及び復号化に使用する各種鍵を格納するための構成として共通鍵保管メモリ２２及び通信用鍵保管メモリ２１と、これらに格納された鍵を用いて暗号化や復号化を行うための構成として共通暗号復号回路２４及び公開暗号復号回路２０を有している。また、このプレーヤ１は、上記暗号化及び復号化に関連する構成として、システム管理会社２１０のホストコンピュータと連動した乱数を発生してセキュリティＩＤを生成するセキュリティＩＤ発生回路１９及びタイマ１８や、後述するいわゆるハッシュ値を発生するハッシュ関数回路２５等をも有している。

【００１６】その他、当該プレーヤ１は、ディジタルコンテンツやその他各種のデータ及び各構成要素の制御をＲＯＭ１７に格納されたプログラムに基づいて行う制御手段であるコントローラ１６と、携帯時の動作電源としての電池５を備えている。

【００１７】ここで、図２のプレーヤ１の各主要構成要素は、セキュリティ上、ＩＣ（集積回路）或いはＬＳＩ（大規模集積回路）の１チップで構成されることが望ましい。この図２では、各主要構成要素が集積回路１０内に１チップ化されている。当該プレーヤ１には、外部とのインターフェイス用として３つの端子（アナログ出力端子２と、ＰＣ用インターフェイス端子３と、記録メディア用Ｉ／Ｏ端子４）を備え、これら各端子が集積回路１０のそれぞれ対応する端子１３、１２、１１に接続されている。なお、これら各端子は統合することも、また新たに別の端子を設けることも可能であり、特にこだわるものではない。

【００１８】システム管理会社２１０は、システム全体を管理する管理センタ２１１と、上記プレーヤ１を販売する販売店２１２とからなり、仮想店舗２３０を介してユーザ側２００のユーザ端末５０との間で、後述するようなディジタルコンテンツの供給に関する情報の送受、コンテンツプロバイダ２４０が保有するコンテンツを圧縮及び暗号化するディジタルコンテンツの加工、上記加工したディジタルコンテンツの供給、金融機関２２０との間の情報送受等を行う。なお、システム管理会社２１０と金融機関２２０との間では、ユーザ側２００の口座番号やクレジット番号，名前や連絡先等の確認や、ユーザ側２００との間で取引可能かどうかの情報等のやり取りなどが行われる。金融機関２２０とユーザ側２００との間では、実際の代金振込等の処理が行われる。また、販売店２１２は、必ずしもシステム管理会社２１０内に含まれる必要はなく、販売代理店であってもよい。

【００１９】上記システム管理会社２１０の管理センタ２１１は、例えば図３に示すような構成を有するものである。この図３の構成の詳細な説明については後述するが、主要構成要素として、ディジタルコンテンツを管理し、その展示、暗号化及び圧縮等の加工処理、ディジタルコンテンツの暗号化及び復号化に使用する鍵情報であるコンテンツ鍵やＩＤの発生等の各機能を有するコンテンツ管理機能ブロック１００と、ユーザ情報を管理し、通信文（メッセージやポイント情報等）の暗号化及び復号化、確認メッセージの発生、セキュリティＩＤの発生、金融機関２３０との間での決済申請、ポイントの発生等の各機能の他、ユーザ加入処理等を行うユーザ加入処理機能部１１８をも備えたユーザ管理機能ブロック１１０と、ポイント使用情報等を管理する使用情報管理機能ブロック１２０と、システム全体を管理し、通信機能を有する管理機能ブロック１３０とを、少なくとも有してなる。

【００２０】上述した図１のように構成されるシステム

の実際の運用方法の一例を、図４～図７を用いて説明する。なお、以下の運用方法は、ユーザ側２００やシステム管理会社２１０，金融機関２２０，コンテンツプロバイダ２４０等が実際に行う手順である。

【００２１】このシステムの運用方法の説明では、プレーヤ１の購入の手順、ディジタルコンテンツの検索からプレーヤ１用の記憶メディアに対するディジタルコンテンツのインストールまでの手順、当該ディジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順、ディジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金の分配の手順について順番に説明する。

【００２２】先ず、プレーヤ１の購入時の手順としては、図４の（１）及び（５）に示すように、ユーザ側２００が実際に店頭或いは通信販売等により、上記販売店２１２から上記プレーヤ１を購入する。

【００２３】このとき、上記販売店２１２は、図４の（２）に示すように、上記プレーヤ１の販売時に上記ユーザ側２００から提供された個人情報（名前や連絡先等）及び決済情報（銀行口座、クレジット番号等）と、上記販売したプレーヤ１固有の番号（プレーヤ固有鍵等を含む）とをシステム管理会社２１０の管理センタ２１１に登録する。

【００２４】管理センタ２１１は、図４の（３）に示すように、金融機関２２０に対して、上記ユーザ側２００から提供された口座番号やクレジット番号等の確認を行い、図４の（４）に示すように金融機関２２０から取引可能である旨の情報を得る。

【００２５】次に、ディジタルコンテンツの検索からプレーヤ１用の記憶メディアへのディジタルコンテンツのインストールまでの手順として、上記プレーヤ１を購入したユーザ側２００は、当該プレーヤ１とのインターフェイス手段を備えたユーザ端末５０を使って、図５の（１）に示すように、希望のディジタルコンテンツの検索，選択，編集，注文等を行う。このときの検索から注文までの処理は、ユーザ端末５０がアプリケーションソフトとして格納している検索ソフトを用い、例えばネットワークを介して接続された仮想店舗２３０に対して行う。

【００２６】仮想店舗２３０は、例えば管理センタ２１１がネットワーク上の仮想的に設けている店舗であり、この仮想店舗２３０には、例えば複数のコンテンツの内容を示す情報が展示されている。ユーザ側２００は、仮想店舗２３０にて提供されているこれらの情報に基づいて、所望のコンテンツの注文を行うことになる。なお、仮想店舗２３０に展示されるコンテンツの内容を示す情報としては、例えばコンテンツが映画等のビデオデータである場合には当該映画等のタイトルや広告、当該映画中の１シーン等の映像などが考えられ、また、コンテンツがオーディオデータである場合は曲名やアーティスト名、当該曲の最初の数フレーズ（いわゆるイントロ）等が考えられる。したがって、ユーザ側２００のユーザ端末５０にて上記仮想店舗２３０をアクセスした場合には、当該ユーザ端末５０上に上記仮想店舗２３０の複数のコンテンツの内容が仮想的に展示され、これら展示物の中から所望のものを選択することでコンテンツの注文が行われることになる。

【００２７】上記ユーザ側２００のユーザ端末５０からディジタルコンテンツの注文等があったとき、上記仮想店舗２３０は、図５の（２）に示すように管理センタ２１１に対してディジタルコンテンツの供給依頼を行う。

【００２８】当該ディジタルコンテンツの供給依頼を受け取った管理センタ２１１は、コンテンツプロバイダ２４０に対して上記供給依頼のあったディジタルコンテンツの配給依頼を行う。これにより、当該コンテンツプロバイダ２４０は、図５の（４）に示すように上記配給依頼のあったディジタルコンテンツを管理センタ２１１に配給する。

【００２９】管理センタ２１１は、上記コンテンツプロバイダ２４０から配給されたディジタルコンテンツに対して暗号化及び所定の圧縮方式を用いた圧縮を施すと共に、この圧縮及び暗号化されたディジタルコンテンツに対して、当該コンテンツのＩＤ（コンテンツＩＤ）とこのコンテンツの著作権者等の権利者情報と当該コンテンツを使用したときの課金額とコンテンツをユーザ側２００に供給する仮想店舗名等とを付加する。なお、コンテンツに対する課金額は、コンテンツプロバイダ２４０にて事前に決定される。

【００３０】上記管理センタ２１１にて加工されたコンテンツは、図５の（５）に示すように、仮想店舗２３０に送られ、さらにこの仮想店舗２３０を介して、図５の（６）のようにユーザ側２００のユーザ端末５０に供給される。これにより、プレーヤ１には、上記ユーザ端末５０からコンテンツが供給され、このコンテンツが当該プレーヤ１に格納されることになる。

【００３１】なお、この図５に（２）～（５）までの流れについては、事前に行っておくことも可能である。すなわち、仮想店舗２３０には、上記複数のコンテンツの内容を示す情報を展示するだけでなく、これら展示に対応した上記加工されたディジタルコンテンツを予め用意しておくようにしても良い。

【００３２】次に、上述のようにしてプレーヤ１にインストールされたディジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順では、先ず、ユーザ端末５０によってプレーヤ１に格納されているポイント情報の不足が確認されて、当該ユーザ端末５０からポイント情報の補充要求がなされる。

【００３３】このとき、図６の（１）のように、当該ユ

ーザ端末５０からは、プレーヤ１にて暗号化されたポイント情報の補充依頼が、管理センタ２１１に対し転送される。また同時に、既に使用したディジタルコンテンツに対応する著作権者等の権利者の情報すなわちポイント使用情報がプレーヤ１から読み出されて暗号化され、ユーザ端末５０を介して管理センタ２１１に送られる。このように、ポイント情報の補充依頼と同時にポイント使用情報の転送が行われるようにしたのは、当該ポイント使用情報の管理センタ２１１への送信のみのために、ユーザ側２００が管理センタ２１１にアクセスする手間を省くためである。勿論、このポイント使用情報の転送は、必ずしもポイント情報の購入と同時に行う必要はなく、独立に行っても良い。

【００３４】上記暗号化されたポイント情報の補充依頼及びポイント使用情報を受け取った管理センタ２１１は、当該暗号を解読することでユーザ側２００が要求しているポイント情報の補充量とポイント使用情報の内容を認識する。さらに、当該管理センタ２１１は、金融機関２２０に対して図６の（２）のように当該ポイント補充分の決済が可能かどうかの確認を行う。金融機関２２０にて、ユーザ側２００の口座を調べることによって、決済可能であることが確認されると、当該金融機関２２０から図６の（３）のように決済ＯＫの指示が管理センタ２１１に送られることになる。

【００３５】また、このときの管理センタ２１１は、図６の（４）に示すように、コンテンツプロバイダ２４０に対して著作権者等の権利者に支払われることになるポイント使用数、すなわち金額を連絡する。

【００３６】その後、管理センタ２１１では、ポイント補充情報の命令書を暗号化し、これをセキュリティＩＤと共にポイント補充指示情報として、図６の（５）に示すようにユーザ端末５０に送る。このユーザ端末５０からプレーヤ１に送られた上記ポイント補充指示情報は、当該プレーヤ１において復号化され、さらにセキュリティＩＤの確認後に、ポイント情報格納メモリ２８へのポイント情報の補充と、ポイント使用情報格納メモリ２９からの上記先に連絡した著作権情報等の権利者情報の削除とが行われる。

【００３７】次に、ディジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金、すなわちポイントの使用情報に応じてユーザの口座から引き落とされることになる代金の分配の手順では、先ず図７の（１）のようにユーザ側２００に対して代金振り込み依頼が金融機関２２０からなされる。このとき、ユーザ側２００の口座に十分な残高がある場合には、特に代金振り込み依頼はなされず、口座に十分な残高がない場合には、図７の（２）のようにユーザ側２００から金融機関２２０に対して代金の振り込みがなされる。

【００３８】金融機関２２０は、所定の手数料を差し引いて、図７の（３）のように、ユーザ側２００から受け取った代金を管理センタ２１１に対して送金する。すなわち管理センタ２１１では、金融機関２２０から送金された上記代金から、コンテンツ加工料と金融手数料とシステム管理費等を徴収する。また、当該管理センタ２１１は、先に使用されたポイントに応じた著作権料を、図７の（４）のようにコンテンツプロバイダ２４０に対して支払うと共に、仮想店舗２３０に対しては図７の（５）のように店舗手数料を支払う。上記著作権料を受け取ったコンテンツプロバイダ２４０は著作権料を各著作権者に支払い、上記店舗手数料を受け取った仮想店舗２３０は仮想店舗毎の手数料を各仮想店舗に対して支払う。

【００３９】このように、ユーザ側２００から支払われた代金は、前記ポイント使用情報に基づいて、著作権料と店舗手数料とコンテンツ加工手数料と決済手数料とシステム管理手数料とに分配され、上記著作権料はコンテンツプロバイダ２４０に、上記店舗手数料は上記仮想店舗２３０に、コンテンツ加工手数料はシステム管理会社２１０に、決済手数料はシステム管理会社と金融機関２２０に、システム管理手数料はシステム管理会社２１０に支払われる。

【００４０】ここで、本実施の形態のシステム間でのデータ送受、すなわち管理センタ２１１とプレーヤ１との間のデータ送受の際には、データ通信の安全性を確保するために、通信するデータの暗号化及び復号化が行われる。本発明実施の形態では、暗号化及び復号化の方式として共通鍵暗号方式及び公開鍵暗号方式の何れにも対応可能となっている。

【００４１】本発明の実施の形態では、上記ディジタルコンテンツ、上記ポイント使用情報、ポイント情報、メッセージやセキュリティＩＤ、その他の各種情報の伝送の際の暗号方式としては、処理速度の点から共通鍵暗号方式を採用している。これら各種情報の暗号化及び復号化に使用する共通鍵は、それぞれ各情報に対応して異なるものである。前記図２のプレーヤ１では、管理センタ２１１から伝送されてくる暗号化された情報の復号化に使用する共通鍵が前記共通鍵保管メモリ２２に保管され、この共通鍵保管メモリ２２に保管している共通鍵を用いて、前記共通暗号復号回路２４が、上記管理センタ２１１からの暗号化された情報の復号化を行う。

【００４２】一方、上記各種情報の暗号化や復号化に使用する上記共通鍵の伝送の際の暗号方式としては、前記プレーヤ１の固有の鍵であるプレーヤ固有鍵が何れの方式に対応しているかによって採用される暗号方式が変わるものである。すなわち、上記プレーヤ固有鍵が共通鍵暗号方式に対応している場合、上記共通鍵は当該プレーヤ固有鍵を用いて暗号化され、また当該暗号化された共通鍵は上記プレーヤ固有鍵を用いて復号化されることになる。これに対して、上記プレーヤ固有鍵が公開鍵暗号方式に対応している場合、上記共通鍵の暗号化には相手

先の公開鍵が用いられ、暗号化された上記共通鍵の復号化にはそれぞれ復号化を行う側の秘密鍵が用いられる。

【００４３】例えば上記プレーヤ１から管理センタ２１１に上記共通鍵（例えば後述するセッション鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記プレーヤ１では通信用鍵保管メモリ２１が保管しているプレーヤ固有鍵を用いて上記共通鍵暗号復号回路２４が上記共通鍵を暗号化し、管理センタ２１１では当該管理センタ２１１が保管しているプレーヤ固有鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。同じく、上記プレーヤ１から管理センタ２１１に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記プレーヤ１の通信用用鍵保管メモリ２１が保管している管理センタ２１１の公開鍵にて上記公開鍵暗号復号回路２０が上記共通鍵を暗号化し、管理センタ２１１では当該管理センタ２１１が保管している秘密鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。

【００４４】逆に、例えば上記管理センタ２１１からプレーヤ１に上記共通鍵（例えばコンテンツ鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記管理センタ２１１が保管しているプレーヤ固有鍵にて上記共通鍵が暗号化され、プレーヤ１では上記通信用鍵保管メモリ２１にて保管しているプレーヤ固有鍵を用いて、前記共通暗号復号回路２４が上記暗号化されてる共通鍵の復号化を行う。同じく、上記管理センタ２１１からプレーヤ１に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記管理センタ２１１が保管しているプレーヤ１の公開鍵にて上記共通鍵が暗号化され、プレーヤ１では上記通信用鍵保管メモリ２１にて保管しているプレーヤ固有鍵すなわち秘密鍵を用いて、前記公開暗号復号回路２０が上記暗号化されてる共通鍵の復号化を行う。

【００４５】上述したようなプレーヤ固有鍵自身の暗号方式は、当該プレーヤ固有鍵の配送（システム管理会社２１０からプレーヤ１への配送）が容易か否かによって決定されている。すなわち、コスト的には共通鍵暗号方式の方が有利であるので、プレーヤ固有鍵の配送が容易であれば共通鍵暗号方式を採用するが、当該プレーヤ固有鍵の配送が困難であるときにはコスト高であるが公開鍵暗号方式を採用する。プレーヤ固有鍵をハードウェアに実装する場合には共通鍵暗号方式を、ソフトウェアに実装する場合には公開鍵暗号方式を採用する。

【００４６】以下、本発明の実施の形態では、プレーヤ固有鍵自身の暗号方式としてソフトウェアに実装する場合の互換性を考慮して、上記公開鍵暗号方式を採用する例を挙げて説明することにする。すなわち、上記管理センタ２１１とプレーヤ１との間で前記共通鍵の伝送が行われる場合において、上記プレーヤ１側で共通鍵（セッション鍵）が暗号化されるときには管理センタ２１１の公開鍵を用いて暗号化がなされ、管理センタ２１１では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。逆に、上記管理センタ２１１側で共通鍵（コンテンツ鍵）が暗号化されるときには、プレーヤの公開鍵にて暗号化がなされ、プレーヤ１では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。

【００４７】前述したような各手順と暗号方式を用いて運用されるシステムを構成する上記プレーヤ１とユーザ端末５０と管理センタ２１１の実際の動作を、以下に順番に説明する。

【００４８】先ず、上述したポイント補充すなわちポイント購入時のプレーヤ１、ユーザ端末５０、管理センタ１０における処理の流れについて、図８から図１１を用い、前記図２及び図３を参照しながら説明する。

【００４９】図８には、ポイントを購入する際のプレーヤ１における処理の流れを示している。

【００５０】この図８において、ステップＳＴ１では、ユーザ端末５０すなわちパーソナルコンピュータに予めインストールされているポイント購入用のソフトウェアの立ち上げが行われ、この間のプレーヤ１のコントローラ１６は、当該ポイント購入用のソフトウェアが立ち上がるまで待っている。

【００５１】上記ポイント購入用のソフトウェアが立ち上がると、ステップＳＴ２にて、プレーヤ１のコントローラ１６は、上記ユーザ端末５０に入力された情報を、当該ユーザ端末５０から受信する。このときのユーザ端末５０に入力される情報とは、上記ポイント購入用のソフトウェアに従って、上記ユーザ端末５０を操作するユーザに対して当該ユーザ端末５０から入力要求がなされるものであり、例えばパスワードや購入したいポイント情報数等の情報である。

【００５２】これらユーザ端末５０からの情報は、プレーヤ１のＰＣ用インターフェース端子３及び当該プレーヤ１内に１チップ化された集積回路１０の端子１２を介して、コントローラ１６に受信される。当該ユーザ端末５０からの情報を受信したコントローラ１６は、ステップＳＴ３にて、当該プレーヤ１の集積回路１０内のパスワード格納メモリ１４が格納するパスワードと、上記受信した情報中のパスワードとの比較を行い、上記受信パスワードが正しいかどうかの確認を行う。

【００５３】上記パスワードが正しいと確認したコントローラ１６は、ステップＳＴ４にて、ポイントを購入したい旨の情報（ポイント購入の主旨）と購入したいポイント情報数その他の情報を生成すると同時に、セキュリティＩＤ発生回路１９からセキュリティＩＤを発生させ、次のステップＳＴ５にてこれらの情報を共通暗号復号回路２４にて暗号化させる。コントローラ１６は、次

にステップＳＴ６にて、ユーザＩＤ格納メモリ２３からユーザＩＤを読み出し、当該ユーザＩＤを上記暗号化した情報に付加し、さらに、ステップＳＴ７にて、当該ユーザＩＤを付加して作成したデータを上記端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送する。このユーザ端末５０からは、上記作成データが管理センタ２１１に送られることになる。

【００５４】このとき、上記作成データの暗号化には前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ１６では、上記共通鍵として、例えば乱数発生手段であるセキュリティＩＤ発生回路１９からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だって、プレーヤ１から管理センタ２１１に対して送られることになる。ここで、当該共通鍵は前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ１６では、上記共通鍵であるセッション鍵を公開暗号復号回路２０に送ると同時に、通信用鍵保管メモリ２１に予め保管されている管理センタ２１１の公開鍵を取り出して上記公開暗号復号回路２０に送る。これにより当該公開暗号復号回路２０では、上記管理センタ２１１の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵はユーザＩＤと共に、上記作成データの伝送に先だって管理センタ２１１に送られている。

【００５５】なお、前述したように、ポイント情報の要求と共にポイント使用情報の転送も行う場合、コントローラ１６は、ポイント使用情報格納メモリ２９から前記権利者情報等を含むポイント使用情報を読み出し、これらも上記共通暗号復号回路２６に送って暗号化させる。この暗号化したポイント使用情報は、上記作成データと共に伝送される。また、ポイント使用情報の転送と同時に、ポイント情報の残高をも同様にして転送することも可能である。

【００５６】その後、コントローラ１６は、ステップＳＴ８にて、ユーザ端末５０を通して管理センタ２１１から送られてきた暗号化されているデータを受信する。この管理センタ２１１から送られてきたデータは、先に当該プレーヤ１から転送した上記購入したいポイント情報数に応じたポイント情報とセキュリティＩＤ等の情報が、上記セッション鍵と同じ共通鍵を用いて暗号化されたデータである。

【００５７】コントローラ１６は、上記管理センタ２１１からのデータを受信すると、ステップＳＴ９にて、当該データを上記共通暗号復号回路２４に送ると共に、先に発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いて上記管理センタ２１１からの暗号化されたデータを復号化する。

【００５８】次に、上記コントローラ１６は、ステップＳＴ１０にて、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認し、その確認後、ステップＳＴ１１にて、上記ポイント情報格納メモリ２８に格納されていたポイント情報を、上記新たに送られてきたポイント情報にて修正する。

【００５９】上記ポイント情報の修正等の処理が終了すると、コントローラ１６は、ステップＳＴ１２にて、処理完了のサインを生成し、上記共通鍵保管メモリ２２から読み出した共通鍵と共に上記共通暗号復号回路２４に送り、当該共通暗号復号回路２４にて暗号化させる。その後、コントローラ１６は、ステップＳＴ１３にて当該暗号化された処理完了のサインを、端子１２及び３を介してユーザ端末５０に転送し、管理センタ２１１に送る。

【００６０】以上により、ポイント購入の際のプレーヤ１における処理の流れが終了する。

【００６１】次に、上記ポイント購入時のユーザ端末５０における処理の流れを、図９を用いて説明する。

【００６２】この図９において、ユーザ端末５０は、ステップＳＴ２１にて、ポイント購入用のソフトウェアの立ち上げを行う。当該ポイント購入用ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ２２にて、上記ポイント購入用のソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して上述したパスワードや購入したいポイント数等の情報の入力要求を行い、ユーザからこれらの情報が入力されると、当該入力された情報を前記図８のステップＳＴ２のように上記プレーヤ１に転送する。

【００６３】次に、ユーザ端末５０は、ステップＳＴ２３にて、上記プレーヤ１から前記図８のステップＳＴ７のように作成されたデータを受信すると、ステップＳＴ２４にて、当該プレーヤ１から転送されたデータを、予め登録されているアドレスすなわち管理センタ２１１へ転送する。

【００６４】上記データの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、管理センタ２１１からのデータ返送があると、ステップＳＴ２５にて当該管理センタ２１１からのデータをそのままプレーヤ１に転送する。

【００６５】当該ユーザ端末５０は、ステップＳＴ２６にて、上記プレーヤ１から前記図８のステップＳＴ１３のように処理完了のサインを受信すると、当該ポイント購入等の処理が終了したことをユーザに知らせるために、ステップＳＴ２７にて処理完了のサインをディスプレイに表示し、ユーザに確認させる。

【００６６】その後、当該ユーザ端末５０は、上記プレーヤ１から送られてきた処理完了のサインの暗号文を管

理センタ２１１に転送する。

【００６７】以上により、ポイント購入の際のユーザ端末５０における処理の流れが終了する。

【００６８】次に、ポイント購入時の管理センタ２１１における処理の流れを、図１０を用いて説明する。

【００６９】この図１０において、管理センタ２１１は、ステップＳＴ３１のように、コントロール機能部１３１にて全体が制御される管理機能ブロック１３０の通信機能部１３３によって、前記図８のステップＳＴ７及び図９のステップＳＴ２４のようにユーザ端末５０を介して転送されたプレーヤ１からの上記暗号化されたデータを受信する。このデータを受信すると、管理センタ２１１のユーザ管理機能ブロック１１０は、ステップＳＴ３２のように、コントロール機能部１１１の制御の元で、当該受信したデータに添付されたユーザＩＤに基づいて、データベース部１１２から共通鍵を入手すると共にセキュリティＩＤ発生機能部１１６からセキュリティＩＤを入手する。

【００７０】なお、この時の共通鍵は、前記プレーヤ１から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、当該管理センタ２１１のユーザ管理機能ブロック１１０において、上記管理センタ２１１の公開鍵暗号方式の秘密鍵が取り出され、この秘密鍵と上記暗号化されているセッション鍵とが通信文暗号／復号機能部１１４に送られる。当該通信文暗号／復号機能部１１４では、上記管理センタ２１１の公開鍵を用いて上記暗号化されたセッション鍵の復号化が行われる。このようにして得られたセッション鍵（共通鍵）が上記データベース部１１２に格納されている。

【００７１】上記データベース部１１２から上記ユーザＩＤに対応する共通鍵を入手すると共にセキュリティＩＤ発生機能部１１６からセキュリティＩＤを入手すると、ステップＳＴ３３に示すように、管理センタ２１１のユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４において、上記共通鍵を用いて、上記プレーヤ１からの上記暗号化されたデータの復号化を行い、さらにコントロール機能部１１１において、当該復号化したデータ中のセキュリティＩＤと上記セキュリティＩＤ発生機能部１１６から読み出したセキュリティＩＤとの比較によって、アクセスしてきたユーザ側２００（プレーヤ１）が正当な使用者であるかどうかの内容確認を行う。

【００７２】上記アクセス元の正当性を確認した管理センタ２１１では、ステップＳＴ３４のように、ユーザ管理機能ブロック１１０のポイント発生機能部１１３にて、上記ユーザ端末５０から送られてきたデータの内容に応じたポイント情報の発行を行い、また、決済請求機能部１１７にて、ユーザの決済機関（金融機関２２０）への請求準備を行う。

【００７３】さらに、管理センタ２１１は、ステップＳＴ３５のように、例えばコントロール機能部１１１において、プレーヤ１からのポイント情報の残高とポイント使用情報に不正が無いことを確認し、後の処理のために情報のまとめを行う。すなわち、ポイント情報の残高と実際に使用したポイント情報の数とから不正な使用がないかどうかの確認とまとめとを行う。なお、この確認とまとめは、必ず行わなければならないものではないが、望ましくは行った方が良い。

【００７４】管理センタ２１１のユーザ管理機能ブロック１１０ではまた、上記ステップＳＴ３５の処理の後、ステップＳＴ３６のように、セキュリティＩＤ発生機能部１１５において上記プレーヤ１（ユーザ）への新たなセキュリティＩＤを例えば乱数発生に基づいて算出し、さらに、例えばコントロール機能部１１０にて、上記セキュリティＩＤを上記ポイント情報と共に暗号化する。このときの暗号化も前記プレーヤ１から予め送られてきている前記セッション鍵（共通鍵）を用いて行う。

【００７５】上記暗号化が終了すると、管理センタ２１１の管理機能ブロック１３０の通信機能部１３３では、コントロール機能部１３１の制御の元、上記暗号化したデータを前記図９のステップＳＴ２５及び図８のステップＳＴ８のようにユーザ端末５０を介してプレーヤ１に転送する。

【００７６】その後、管理センタ２１１の通信機能部１３３において、ステップＳＴ３８のように、前記図９のステップＳＴ２８に示したユーザ端末５０からの処理完了サインを受信して復号化すると、管理センタ２１１のユーザ管理機能ブロック１１０の決済請求機能部１１７では、ステップＳＴ３９のように、当該処理完了サインに基づいて金融機関２２０に決済を請求する。この金融機関２２０に対する決済請求は、管理機能ブロック１３０の通信機能部１３２から行われる。

【００７７】以上により、ポイント購入の際の管理センタ２１１における処理の流れが終了する。

【００７８】上述した図８から図１０の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１１に示すように表すことができる。

【００７９】すなわちこの図１１において、入力情報転送Ｔ１では、前記図８のステップＳＴ２及び図９のステップＳＴ２２のように、ユーザ端末５０からプレーヤ１に対して、前記パスワードやポイント数等の入力情報が転送される。

【００８０】作成データ転送Ｔ２では、前記図８のステップＳＴ７及び図９のステップＳＴ２３のように、プレーヤ１からユーザ端末５０に対して、前記プレーヤ１にて作成したデータが転送される。また、データ転送Ｔ３

では、前記図９のステップＳＴ２４及び図１０のステップＳＴ３１のように、ユーザ端末５０から管理センタ２１１に対して、前記プレーヤ１が作成したデータが転送される。

【００８１】データ転送Ｔ４では、前記図１０のステップＳＴ３７及び図９のステップＳＴ２５のように、管理センタ２１１からユーザ端末５０に対して、管理センタ２１１にて暗号化したデータが転送される。また、転送Ｔ５では、前記図９のステップＳＴ２５及び図８のステップＳＴ８のように、管理センタ２１１からのデータをユーザ端末５０がそのままプレーヤ１に転送される。

【００８２】処理完了サイン転送Ｔ６では、前記図８のステップＳＴ１３及び図９のステップＳＴ２６のように、プレーヤ１からの処理完了サインがユーザ端末５０に転送される。さらに、処理完了サイン暗号文転送では、前記図９のステップＳＴ２８及び図１０のステップＳＴ３８のように、プレーヤ１からの暗号化された処理完了サインが管理センタ２１１に転送される。

【００８３】次に、上述したディジタルコンテンツの入手時のプレーヤ１、ユーザ端末５０、管理センタ２１１における処理の流れについて、図２及び図３を参照しながら、図１２から図１５を用いて説明する。

【００８４】図１２には、ディジタルコンテンツの入手時のプレーヤ１における処理の流れを示している。

【００８５】この図１２において、コントローラ１６は、ステップＳＴ４１のように、ユーザ端末５０すなわちパーソナルコンピュータに予めインストールされているディジタルコンテンツ入手用のソフトウェアの立ち上げが行われるまで待っている。

【００８６】上記ディジタルコンテンツ入手用のソフトウェアが立ち上がると、コントローラ１６は、ステップＳＴ４２のように、ユーザ端末５０を介して管理センタ２１１からディジタルコンテンツを含むデータを受信する。このときユーザ端末５０から端子３及び１２を介して受信するデータは、前述したようにコンテンツ鍵（コンテンツ毎に異なる共通鍵）で暗号化されたディジタルコンテンツと、当該ディジタルコンテンツに対応するコンテンツＩＤとを少なくとも有してなる。したがって、この暗号化されたディジタルコンテンツを使用するには、コンテンツ鍵を管理センタ２１１から入手しなければならない。このコンテンツ鍵の入手の方法については後述する。

【００８７】このユーザ端末５０からのデータを受信したコントローラ１６は、このデータすなわち暗号化されたディジタルコンテンツを、集積回路１０の端子１１を介し、記憶メディア用Ｉ／Ｏ端子４に接続されている記憶メディアに格納する。なお、この記憶メディアとしては、書き換え可能な光ディスクや半導体メモリ等の各種の記憶媒体が考えられるが、ランダムアクセス可能なものが望ましい。

【００８８】以上により、ディジタルコンテンツの入手時のプレーヤ１における処理の流れが終了する。

【００８９】次に、ディジタルコンテンツの入手時のユーザ端末５０における処理の流れを、図１３を用いて説明する。

【００９０】この図１３において、ユーザ端末５０は、ステップＳＴ５１にて、ディジタルコンテンツ入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ５２にて、上記ディジタルコンテンツ入手用のソフトウェアに従い、予め登録されているアドレスの管理センタ２１１にアクセスする。

【００９１】このとき、当該管理センタ２１１は、前記仮想店舗２３０を用いて複数のディジタルコンテンツを展示している。ユーザ端末５０からは、ステップＳＴ５３にて、この仮想店舗２３０に展示されている複数のディジタルコンテンツのなかから、ユーザの選択操作に応じた所望のディジタルコンテンツが指定される。すなわち、ユーザ端末５０は、ステップＳＴ５４のように、仮想店舗２３０に展示されたディジタルコンテンツの中の所望のディジタルコンテンツを指定するためのコンテンツの指定情報を管理センタ２１１に送信する。

【００９２】ステップＳＴ５５のように、上記コンテンツ指定情報に応じて管理センタ２１１から返送されたデータ、すなわち前記暗号化されたディジタルコンテンツ及びコンテンツＩＤからなるデータを受信すると、当該ユーザ端末５０は、ステップＳＴ５６のように、内部の例えばハードディスクやメモリ等の格納手段に上記データを一旦格納する。

【００９３】その後、ユーザ端末５０は、当該格納したデータ（暗号化されたディジタルコンテンツ及びコンテンツＩＤ）を、前記図１２のステップＳＴ４２のようにプレーヤ１に転送する。

【００９４】以上により、ディジタルコンテンツの入手時のユーザ端末５０における処理の流れが終了する。

【００９５】次に、ディジタルコンテンツ入手時の管理センタ２１１における処理の流れを、図１４を用いて説明する。

【００９６】ここで、図3に示す管理センタ２１１は、前述した仮想店舗２３０に複数のコンテンツを展示させている。具体的には、管理センタ２１１ののコンテンツ管理機能ブロック１００において、前記仮想店舗２３０を生成しており、この仮想店舗２３０に上記複数のディジタルコンテンツの展示を行っている。

【００９７】このように仮想店舗２３０にディジタルコンテンツを展示している状態で、図１４のステップＳＴ６１のように、前記図１３のステップＳＴ５４にてユーザ端末５０からコンテンツ指定情報を受信する。

【００９８】当該ユーザ端末５０から上記コンテンツ指定情報を受信すると、コンテンツ管理機能ブロック１０

０のコントロール機能部１０１は、このコンテンツ指定情報を管理機能ブロック１３０に送る。管理機能ブロック１３０のコントロール機能部１３１は、上記コントロール管理機能ブロック１００から受け取ったコンテンツ指定情報を、権利者用の通信機能部１３４を通して、前記コンテンツプロバイダ２４０に転送する。これにより当該コンテンツプロバイダ２４０からは、上記コンテンツ指定情報にて要求されたディジタルコンテンツが転送されてくる。上記コンテンツプロバイダ２４０から入手したディジタルコンテンツは、管理機能ブロック１３０からコンテンツ管理機能ブロック１００に送られ、このコンテンツ暗号・圧縮化機能部１０４に入力される。このとき、コントロール機能部１０１は、コンテンツ鍵・ＩＤ発生機能部１０３にて発生されてデータベース１０２に格納されているコンテンツ鍵を、上記コンテンツ暗号・圧縮化機能部１０４に送る。このコンテンツ暗号・圧縮化機能部１０４では、上記ディジタルコンテンツに対して上記コンテンツ鍵を用いた暗号化を施し、さらに所定の圧縮処理を施す。コントロール機能部１０１は、上記暗号化及び圧縮処理されたディジタルコンテンツに対して、データベース１０２から取り出したコンテンツＩＤを付加し、管理機能ブロック１３０に送る。なお、ディジタルコンテンツがオーディオ信号である場合の所定の圧縮処理としては、例えば近年製品化されているいわゆるＭＤ（ミニディスク：商標）にて使用されている技術である、いわゆるＡＴＲＡＣ（Adaptive TRansform Acoustic Coding）のように、人間の聴覚特性を考慮してオーディオデータを高能率圧縮する処理を一例とした挙げることができる。

【００９９】その後、図１４のステップＳＴ６２に示すように、管理機能ブロック１３０のコントロール部１３１は、ユーザ端末との通信機能部１３３を通して、上記暗号化及び圧縮処理されてコンテンツＩＤが付加されたディジタルコンテンツを、上記ユーザ端末５０に送信する。

【０１００】ディジタルコンテンツ入手時の管理センタ２１１における処理の流れは以上である。

【０１０１】上述した図１２から図１４の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１５に示すように表すことができる。

【０１０２】すなわちこの図１５において、入力情報転送Ｔ１１では、前記図１３のステップＳＴ５４のように、ユーザ端末５０から管理センタ２１１に対して、前記コンテンツ指定情報が転送される。コンテンツ転送Ｔ１２では、管理センタ２１１から、前記図１４のステップＳＴ６２のように、暗号化されたディジタルコンテンツとコンテンツＩＤがユーザ端末５０に転送される。

【０１０３】コンテンツ転送Ｔ１３では、前記図１３のステップＳＴ５７及び図１２のステップＳＴ４２のように、ユーザ端末５０に一旦格納された上記暗号化されたディジタルコンテンツとコンテンツＩＤがプレーヤ１に転送される。

【０１０４】次に、上述したディジタルコンテンツを使用する際に必要となるコンテンツ鍵とその使用条件の入手時のプレーヤ１、ユーザ端末５０、管理センタ２１１における処理の流れについて、図２及び図３を参照しながら、図１６から図１９を用いて説明する。

【０１０５】図１６には、コンテンツ鍵及び使用条件の入手時のプレーヤ１における処理の流れを示している。

【０１０６】この図１６のステップＳＴ７１では、プレーヤ１のコントローラ１６において、ユーザ端末５０に予めインストールされているコンテンツ鍵及び使用条件入手用のソフトウェアの立ち上げが行われるまで待っている。

【０１０７】上記ユーザ端末５０の上記コンテンツ鍵及び使用条件入手用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末５０に入力された情報が、ステップＳＴ７２のように、前記ＰＣ用インターフェース端子３及び集積回路１０の端子１２を介して受信される。このときの上記ユーザ端末５０から供給される入力情報は、鑑賞したいディジタルコンテンツの暗号化を解くのに必要なコンテンツ鍵を要求するための情報である。なお、この例では、上記コンテンツ鍵の要求情報として、このコンテンツ鍵を使用するディジタルコンテンツの指定情報を用いている。

【０１０８】このコンテンツ指定情報を上記ユーザ端末５０から受信したコントローラ１６は、ステップＳＴ７３にて、当該コンテンツ指定情報にて指定されたディジタルコンテンツのＩＤと、セキュリティＩＤ発生回路１９からのセキュリティＩＤとを作成し、この作成したデータを共通暗号復号回路２４にて暗号化させる。また、コントローラ１６は、当該作成したデータにユーザＩＤ格納メモリ２３から読み出したユーザＩＤを付加し、上記端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送する。このユーザ端末５０からは、上記作成データが管理センタ２１１に送られることになる。

【０１０９】このときの作成データの暗号化にも、前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ１６では、上記共通鍵として、例えば乱数発生手段であるセキュリティＩＤ発生回路１９からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だって、プレーヤ１から管理センタ２１１に対して送られることになる。当該共通鍵は、前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ１６では、上記共通鍵であるセッション鍵を公開暗号復号回路２０に送ると同時に、通信用鍵保管メモリ２１に予

め保管されている管理センタ２１１の公開鍵を取り出して上記公開暗号復号回路２０に送る。これにより当該公開暗号復号回路２０では、上記管理センタ２１１の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵が、上記作成データの伝送に先だって管理センタ２１１に送られている。

【０１１０】その後、コントローラ１６は、ステップＳＴ７５にて、後述するようにユーザ端末５０を介して管理センタ２１１から送付されてきた暗号化されたデータを受信する。このときの管理センタ２１１から送られてきたデータは、後述するように上記コンテンツ鍵と使用条件とセキュリティＩＤ等が暗号化されたものである。

【０１１１】上記管理センタ２１１からの暗号化されたデータを受信すると、プレーヤ１では、ステップＳＴ７６のように、上記暗号化されたデータを復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ１６は、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認することによる正当性の評価を行う。

【０１１２】ここで、コンテンツ鍵については後述するように公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティＩＤについては共通鍵暗号方式にて暗号化がなされている。したがって、当該暗号化されているコンテンツ鍵を復号化するには、公開鍵暗号方式の秘密鍵が必要であり、本実施の形態のプレーヤ１では前述したようにプレーヤ固有鍵を秘密鍵として使用することにしているので、当該プレーヤ固有鍵が通信用鍵保管メモリ２１から取り出される。このプレーヤ固有鍵は、上記暗号化されたコンテンツ鍵と共に公開暗号復号回路２０に送られる。この公開暗号復号回路２０では、上記暗号化されているコンテンツ鍵を上記プレーヤ固有鍵を用いて復号化する。このように復号化されたコンテンツ鍵は、共通鍵保管メモリ２２に保管される。一方、上記共通鍵暗号方式にて暗号化されている使用条件とセキュリティＩＤを復号化する場合には、これらのデータを上記共通暗号復号回路２４に送ると共に、先に発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いて上記使用条件とセキュリティＩＤを復号化する。このように復号化された使用条件は、ポイント使用情報格納メモリ２９に格納される。なお、ここで重要なのは、当該復号化されたコンテンツ鍵・使用条件は、当該プレーヤ１の外部、具体的には図２の集積回路１０内に設けられたコントローラ１６や共通鍵保管メモリ２２、ポイント使用情報格納メモリ２９から外部には取り出されないことである。

【０１１３】上記正当性の確認後、コントローラ１６は、ステップＳＴ７７のように、上記復号したコンテンツ鍵を上記コンテンツＩＤと共に上記共通鍵保管メモリ２２に格納させる。

【０１１４】その後、コントローラ１６は、ステップＳＴ７８にて、上記コンテンツ鍵を入手した旨を示すメッセージを作成し、このメッセージを前述同様に共通鍵暗号復号回路２４に送り、予め発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いてメッセージを暗号化する。

【０１１５】当該メッセージの暗号化が終了すると、コントローラ１６は、ステップＳＴ７９のように、この暗号化されたメッセージを端子１２及び３を介してユーザ端末５０に送信する。この暗号化されたメッセージは、その後、管理センタ２１１に転送させる。

【０１１６】以上により、コンテンツ鍵・使用条件入手時のプレーヤ１における処理の流れが終了する。

【０１１７】次に、コンテンツ鍵・使用条件入手時のユーザ端末５０における処理の流れを、図１７を用いて説明する。

【０１１８】この図１７において、ユーザ端末５０は、ステップＳＴ８１にて、コンテンツ鍵・使用条件入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ８２にて、上記ソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して、希望のコンテンツの指定入力要求を行い、ユーザからコンテンツの指定がなされると、その指定情報を生成する。ユーザ端末５０は、上記ステップＳＴ８３にて、上記コンテンツの指定情報をプレーヤ１に対して送信する。

【０１１９】次に、ユーザ端末５０は、ステップＳＴ８４にて、前記図１６のステップＳＴ７４のように上記プレーヤ１にて作成されて転送されたデータを受信すると、ステップＳＴ８５にて、当該プレーヤ１から転送されたデータを、予めアドレスが登録されている管理センタ２１１へ転送する。

【０１２０】上記管理センタ２１１に対してデータの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、ステップＳＴ８６にて、管理センタ２１１から上記コンテンツＩＤで指定されたコンテンツ鍵・使用条件とセキュリティＩＤ等が暗号化されたデータの返送があると、ステップＳＴ８７にて当該管理センタ２１１からのデータをそのままプレーヤ１に転送する。

【０１２１】上記プレーヤ１に対してデータの転送を行った後のユーザ端末５０は、プレーヤ１からの返送を待ち、ステップＳＴ８８にて、プレーヤ１から前記図１６のステップＳＴ７９のように、上記コンテンツ鍵を入手した旨の暗号化されたメッセージの返送があると、ステップＳＴ８９にて当該ユーザ端末５０に接続されたディスプレイ装置に対して上記コンテンツ鍵入手が完了した旨の表示を行ってユーザに知らせる。

【０１２２】その後、上記プレーヤ１から返送された上記暗号化されたメッセージを、ステップＳＴ９０にて、管理センタ２１１に送付する。

【０１２３】以上により、コンテンツ鍵・使用条件入手時のユーザ端末５０における処理の流れが終了する。

【０１２４】次に、コンテンツ鍵・使用条件入手時の管理センタ２１１における処理の流れを、図１８を用いて説明する。

【０１２５】この図１８において、管理センタ２１１のユーザ端末との通信機能部１３３は、ステップＳＴ９１にて、前記図１６のステップＳＴ７４及び図１７のステップＳＴ８５のようにユーザ端末５０にてを介してプレーヤ１から送信されてきたコンテンツＩＤ，ユーザＩＤ、メッセージ、セキュリティＩＤの暗号化データを受信する。この受信したデータは、ユーザ管理機能ブロック１１０に送られる。

【０１２６】当該ユーザ管理機能ブロック１１０のコントロール機能部１１１は、上記受信した暗号化データに付加されたユーザＩＤに基づいて、当該暗号化を解くための共通鍵をデータベース部１１２から取り出し、通信文暗号・復号機能部１１４ではこの共通鍵を用いて上記暗号化データを復号する。また、コントロール機能部１１１は、データベース部１１２から読み出したユーザＩＤとセキュリティＩＤ発生機能部１１６からのセキュリティＩＤとを用いて、上記受信して復号化したデータの正当性を確認する。

【０１２７】なお、この時の共通鍵は、前記プレーヤ１から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、前述同様に当該管理センタ２１１において、上記管理センタ２１１の公開鍵暗号方式の秘密鍵が取り出され、当該通信文暗号／復号機能部１１４にて上記暗号化されているセッション鍵が当該秘密鍵を用いて復号化される。このようにして得られたセッション鍵（共通鍵）が上記データベース部１１２に格納されている。

【０１２８】上記受信したデータの正当性を確認すると、コントロール機能部１１１は、コンテンツ管理機能ブロック１００に対して上記コンテンツＩＤにて指定されたコンテンツ鍵と使用条件を要求し、当該要求を受けたコンテンツ管理機能ブロック１００のコントロール機能部１０１は、上記コンテンツＩＤにて指定されたコンテンツ鍵と使用条件とをデータベース部１０２から読み出してユーザ管理機能ブロック１１０に転送する。コントロール機能部１１１は、ステップＳＴ９３に示すように、これらコンテンツ鍵と使用条件はセキュリティＩＤと共に通信文暗号／復号機能部１１４に送る。

【０１２９】ここで、コンテンツ鍵については前述した公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティＩＤについては前述した共通鍵暗号方式にて暗号化がなされる。したがって、当該コンテンツ鍵を暗号化する時には、前記データベース部１１２からユーザ側２００の公開鍵（プレーヤ１に対応して予め格納されている公開鍵）が上記ユーザＩＤに基づいて取り出されて通信文暗号／復号機能部１１４に送られる。当該通信文暗号／復号機能部１１４では、上記公開鍵を用いて上記コンテンツ鍵を暗号化する。一方、上記使用条件及びセキュリティＩＤを暗号化する時には、上記データベース部１１２から上記ユーザＩＤで指定された共通鍵（セッション鍵）が取り出されて通信文暗号／復号機能部１１４に送られる。このときの通信文暗号／復号機能部１１４では、上記使用条件及びセキュリティＩＤを上記共通鍵を用いて暗号化する。

【０１３０】上記暗号化されたコンテンツ鍵と使用条件及びセキュリティＩＤは、管理機能ブロック１３０に送られ、ステップＳＴ９４のように、ユーザ端末との通信機能部１３３からユーザ端末５０に送信される。このユーザ端末５０に送信されたデータは、前記図１７のステップＳＴ８７及び図１６のステップＳＴ７５のようにユーザ端末５０を介してプレーヤ１に送付されることになる。

【０１３１】その後、管理センタ２１１は、前記図１６のステップＳＴ７９及び図１７のステップＳＴ９０のようにプレーヤ１にて生成されてユーザ端末５０を介して送信された暗号化メッセージの受信を待ち、ステップＳＴ９５のように上記通信機能部１３３が上記プレーヤ１が生成した暗号化メッセージを受信すると、当該管理センタ２１１は、ステップＳＴ９６のように、当該暗号化メッセージを共通鍵で復号化し、その復号メッセージから上記プレーヤ１がコンテンツ鍵と使用条件を入手したことを確認する。

【０１３２】以上により、コンテンツ鍵・使用条件入手時の管理センタ２１１における処理の流れが終了する。

【０１３３】上述した図１６から図１８の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１９に示すように表すことができる。

【０１３４】すなわちこの図１９において、コンテンツ指定情報転送Ｔ２１では、前記図１７のステップＳＴ８３のように、ユーザ端末５０からプレーヤ１に対して、前記コンテンツ指定情報が転送される。作成データ転送Ｔ２２では、前記のステップＳＴ７４のように、プレーヤ１にて作成されたデータがユーザ端末５０に転送される。作成データ転送Ｔ２３では、当該ユーザ端末５０から上記プレーヤ１にて作成されたデータが管理センタ２１１に転送される。暗号化されたデータ送付Ｔ２４では、前記図１８のステップＳＴ９４のように、管理センタ２１１にて暗号化されたデータがユーザ端末５０に送付され、さらに、暗号化されたデータ送付Ｔ２５では、

当該暗号化されたデータがプレーヤ１に送付される。

【０１３５】メッセージ転送Ｔ２６では、前記図１６のステップＳＴ７９のように、コンテンツ鍵入手完了を示すメッセージを暗号化したデータがプレーヤ１からユーザ端末５０に転送され、さらに暗号化されたデータ送付Ｔ２７では、上記プレーヤ１からの暗号化されたメッセージが、ユーザ端末５０から管理センタ２１１に送付される。

【０１３６】次に、上述したようにしてポイント情報とディジタルコンテンツとコンテンツ鍵とを受け取ったプレーヤ１において、ユーザ端末５０を用いてディジタルコンテンツを実際に鑑賞する際の処理の流れについて、図２を参照しながら図２０を用いて説明する。

【０１３７】ここで、プレーヤ１の端子４には、前記ディジタルコンテンツが記憶された記憶メディアが接続されているとする。

【０１３８】この状態で、ステップＳＴ１０１のように、当該プレーヤ１に対して、ユーザ端末５０から鑑賞を希望するディジタルコンテンツが指定される。このとき、当該指定は、例えばユーザ端末５０をユーザが操作することによりなされる。

【０１３９】このとき、プレーヤ１のコントローラ１６は、ステップＳＴ１０２のように、上記ユーザ端末５０からのコンテンツ指定情報に応じて、上記記憶メディアに対するアクセスを行い、コンテンツのＩＤを読み取る。

【０１４０】上記コントローラ１６は、ステップＳＴ１０３のように、上記記憶メディアから読み取ったコンテンツＩＤに基づき、前記共通鍵保管メモリ２２に対してアクセスを行い、コンテンツ鍵が格納されているかどうかを確認すると共に、前記ポイント使用情報格納メモリ２９に対してアクセスを行い、使用条件が格納されているかどうかを確認する。

【０１４１】ここで、上記共通鍵保管メモリ２２やポイント使用情報格納メモリ２９内に、上記コンテンツ鍵と使用条件が格納されていないことを確認したとき、コントローラ１６は、ユーザ端末５０に対して当該コンテンツ鍵等が存在しない旨の情報を送り、これによりユーザ端末５０からは上記コンテンツ鍵等の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合は、前述したコンテンツ鍵入手用のフローチャートのようにしてコンテンツ鍵等を入手する。このように、新たにコンテンツ鍵等を入手した場合には、ステップＳＴ１０４にて前述したように、その暗号化されているコンテンツ鍵等を復号化する。

【０１４２】次に、コントローラ１６は、ステップＳＴ１０５に示すように、上記復号化された使用条件を元に、ポイント情報格納メモリ２８に格納されているポイント情報の残高が足りているかどうかを確認する。上記ポイント情報格納メモリ２８に格納された上記ポイント情報の残高が足りないときには、コントローラ１６からユーザ端末５０に対して当該ポイント情報の残高が足りない旨の情報が送られ、これによりユーザ端末５０は、上記ポイント情報の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合、前述したようなポイント情報入手用のフローチャートのようにしてポイント情報を入手する。

【０１４３】ここで、実際にディジタルコンテンツの鑑賞を行うとき、コントローラ１６は、ステップＳＴ１０６のように、当該鑑賞するディジタルコンテンツに応じて上記ポイント情報格納メモリ２８からポイント情報数を減額し、さらに当該ポイント情報の使用状態に応じた新たなポイント使用情報を、ポイント使用情報格納メモリ２９に格納する（ポイント使用情報の更新を行う）。このようにポイント使用情報格納メモリ２９に対して新たに格納されるポイント使用情報としては、上記鑑賞したディジタルコンテンツに対応する権利者情報（著作権者等）と減額されたポイント情報数の情報その他の情報などである。

【０１４４】その後、コントローラ１６は、ステップＳＴ１０７のように、これらポイント情報の減額やポイント使用情報の新たな格納等の課金用処理が完了したことを確認すると、記憶メディアからディジタルコンテンツを読み出す。

【０１４５】この記憶メディアから読み出されたディジタルコンテンツは暗号化されているため、コントローラ１６は、ステップＳＴ１０９のように、上記暗号化されたディジタルコンテンツを共通暗号復号回路２４に転送する。

【０１４６】この共通暗号復号回路２４では、ステップＳＴ１１０のように、コントローラ１６からの指示に基づいて、先に復号化して共通鍵保管メモリ２２に保管されているコンテンツ鍵を用いて、上記暗号化されているディジタルコンテンツの復号化を行う。

【０１４７】また、このディジタルコンテンツは前述したように所定の圧縮処理がなされているため、コントローラ１６は、ステップＳＴ１１１のように、上記暗号が復号化された上記圧縮処理されているディジタルコンテンツを、上記共通暗号復号回路２４から伸長回路２６に転送させ、ここで上記所定の圧縮処理に対応する伸長処理を行わせる。

【０１４８】その後、当該伸長されたディジタルコンテンツは、ステップＳＴ１１２のように、Ｄ／Ａ変換回路２７にてアナログ信号に変換され、ステップＳＴ１１３のように、集積回路１０の端子１３と当該プレーヤ１のアナログ出力端子２とを介して外部（例えばユーザ端末５０等）に出力される。

【０１４９】以上により、コンテンツ鑑賞時のプレーヤ１における処理の流れが終了し、ユーザはディジタルコンテンツの鑑賞が可能となる。

【０１５０】次に、上述したようなディジタルコンテンツの鑑賞に伴って前記プレーヤ１のポイント使用情報格納メディア２９に新たに格納されたポイント使用情報を、管理センタ２１１に返却する際の、プレーヤ１、ユーザ端末５０、管センタ３１０における処理の流れについて、図２と図３を参照しながら、図２１から図２４を用いて説明する。

【０１５１】図２１には、ポイント使用情報返却時のプレーヤ１における処理の流れを示している。

【０１５２】この図２１において、コントローラ１６は、ステップＳＴ１２１に示すように、ユーザ端末５０に予めインストールされているポイント使用情報返却用のソフトウェアの立ち上げが行われるまで待つ。

【０１５３】上記ユーザ端末５０の上記ポイント使用情報返却用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末５０に入力された情報が、ステップＳＴ１２２のように、前記ＰＣ用インターフェース端子３及び集積回路１０の端子１２を介して受信される。このときの上記ユーザ端末５０から供給される入力情報は、ユーザにより入力されるパスワード等である。

【０１５４】このコンテンツ指定情報を上記ユーザ端末５０から受信したコントローラ１６は、ステップＳＴ１２３にて、当該ユーザ端末５０から供給されたパスワードと、パスワード格納メモリ１４に格納されているパスワードとを比較して、当該パスワードが正しいどうかの確認をする。

【０１５５】上記パスワードの確認において正しいパスワードであると確認されたとき、コントローラ１６は、ステップＳＴ１２４のように、ポイント情報格納メモリ２８に格納されているポイント情報の残高と、ポイント使用情報格納メモリ２９に格納されているポイント使用情報とをそれぞれ読み出し、これら情報を暗号化する。

【０１５６】上記ポイント情報の残高とポイント使用情報の暗号化が終了すると、コントローラ１６は、ステップＳＴ１２５のように、ユーザＩＤ格納メモリ２３からユーザＩＤを読み出して上記暗号化したデータに添付する。

【０１５７】このユーザＩＤが添付されたデータは、ステップＳＴ１２６のように、コントローラ１６から端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送される。このデータはその後管理センタ２１１に転送される。

【０１５８】なお、このときの暗号化にも前述したように共通鍵暗号方式が採用されている。すなわち、当該データの伝送に先立ち、前述同様に共通鍵の生成が行われ、この生成された共通鍵が前記公開鍵暗号方式にて暗号化（管理センタ２１１の公開鍵を用いた暗号化）され、ユーザＩＤと共に管理センタ２１１に送られている。

【０１５９】上述のようにしてユーザ端末５０にデータを転送した後、コントローラ１６は、上記管理センタ２１１から後述するデータがユーザ端末５０を介して転送されてくるのを待つ。

【０１６０】ここで、ステップＳＴ１２７のように上記管理センタ２１１からのデータを受信すると、プレーヤ１では、ステップＳＴ１２７のように、共通鍵暗号方式を使用して暗号化されている受信データを、前述同様に共通鍵を用いて復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ１６は、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認することによる正当性の評価を行う。

【０１６１】また、上記管理センタ２１１から転送されてくるデータには、上記共通鍵を用いて暗号化された処理完了のメッセージも含まれている。したがって、上記セキュリティＩＤの確認が終了した後のコントローラ１６は、上記暗号化された処理完了メッセージを共通暗号復号回路２４に送り、ここで共通鍵を用いた復号化を行わせ、この復号化した処理完了メッセージを受け取ることで、上記管理センタ２１１での処理が完了したことを確認する。

【０１６２】以上により、ポイント使用情報返却時のプレーヤ１における処理の流れが終了する。

【０１６３】次に、ポイント使用情報返却時のユーザ端末５０における処理の流れを、図２２を用いて説明する。

【０１６４】この図２２において、ユーザ端末５０は、ステップＳＴ１３１にて、ポイント使用情報返却用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ１３２にて、上記ソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して、パスワード等の入力要求を行い、ユーザからパスワードの入力がなされると、そのパスワードをプレーヤ１に転送する。

【０１６５】次に、ユーザ端末５０は、ステップＳＴ１３３にて、前記図２１のステップＳＴ１２６のように上記プレーヤ１にて作成されて転送されたデータを受信すると、ステップＳＴ１３４にて、当該プレーヤ１から転送されたデータを、予めアドレスが登録されている管理センタ２１１へ転送する。

【０１６６】上記管理センタ２１１に対してデータの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、ステップＳＴ１３５にて、管理センタ２１１からプレーヤ１に対して送られるデータを受信すると、当該データをそのままプレーヤ１に転送する。

【０１６７】上記プレーヤ１に対してデータの転送を行った後のユーザ端末５０は、処理が完了した旨をユーザに知らしめるための表示をディスプレイ装置に行い、ユーザからの確認を受ける。

【０１６８】以上により、ポイント使用情報返却時のユ

ーザ端末５０における処理の流れが終了する。

【０１６９】次に、ポイント使用情報返却時の管理センタ２１１における処理の流れを、図２３を用いて説明する。

【０１７０】管理センタ２１１のユーザ端末との通信機能部１３３において、ステップＳＴ１４１のように、前記図２１のステップＳＴ１２６及び図２２のステップＳＴ１３４によって前記ユーザ端末５０を介してプレーヤ１から送信されてきたポイント使用情報等のデータを受信する。

【０１７１】このデータを受信すると、管理センタ２１１のユーザ管理機能ブロック１１０は、ステップＳＴ１４２のように、コントロール機能部１１１の制御の元で、当該受信したデータに添付されたユーザＩＤに基づいて、データベース部１１２から前述同様に予め受け取って格納している共通鍵を入手すると共にセキュリティＩＤを入手する。

【０１７２】上記データベース部１１２から上記ユーザＩＤに対応する共通鍵とセキュリティＩＤを入手すると、ステップＳＴ１４３に示すように、管理センタ２１１のユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４において、上記共通鍵を用いて、上記プレーヤ１からの上記暗号化されたポイント使用情報等のデータの復号化を行い、さらにコントロール機能部１１１において、当該復号化したデータ中のセキュリティＩＤと上記データベース部１１２から読み出したセキュリティＩＤとの比較によって、アクセスしてきたユーザ側２００（プレーヤ１）が正当な使用者であるかどうかの内容確認を行う。

【０１７３】上記正当性と内容の確認後のデータは、使用情報管理機能ブロック１２０に転送される。この使用情報管理機能ブロック１２０のコントロール機能部１２１は、ステップＳＴ１４４に示すように、上記プレーヤ１から送られてきたポイント情報の残高とポイント使用情報とを用い、データベース部１２２に格納されている情報を用いて上記ユーザ側２００の使用に不正がないかどうかの確認を行う。同時に、当該不正なきことを確認した場合には、使用情報演算機能部１２３においてポイント情報の残高とポイント使用情報をまとめる演算を行う。

【０１７４】その後、ステップＳＴ１４５に示すように、ユーザ管理機能ブロック１１０のコントロール機能部１１１は、セキュリティＩＤ発生機能部１１６を制御してセキュリティＩＤを算出させ、さらに確認メッセージ発生機能部１１５を制御して処理完了のメッセージを生成させる。これらセキュリティＩＤと処理完了メッセージは、ユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４にて前記共通鍵を用いて暗号化される。

【０１７５】上記暗号化されて生成されたデータは、ステップＳＴ１４６に示すように、ユーザ端末との通信機能部１３３からユーザ端末５０に送られ、前記図２２のステップＳＴ１３５と図２１のステップＳＴ１２７のように当該ユーザ端末５０からプレーヤ１に転送されることになる。

【０１７６】以上により、ポイント使用情報返却時の管理センタ２１１における処理の流れが終了する。

【０１７７】上述した図２１から図２３の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図２４に示すように表すことができる。

【０１７８】すなわちこの図２４において、入力情報転送Ｔ３１では、前記図２２のステップＳＴ１３２のように、ユーザ端末５０からプレーヤ１に対して、前記パスワード等の入力情報が転送される。作成データ転送Ｔ３２では、前記図２１のステップＳＴ１２６のように、プレーヤ１が作成したデータがユーザ端末５０に転送される。作成データ転送Ｔ３３では、前記図２２のステップＳＴ１３４のように、上記プレーヤ１にて作成されたデータが上記ユーザ端末５０から管理センタ２１１に転送される。データ転送Ｔ３４では、前記図２３のステップＳＴ１４６のように、管理センタ２１１にて作成されたデータが、ユーザ端末５０に転送される。データ転送Ｔ３５では、前記図２１のステップＳＴ１２７のように、管理センタ２１１にて作成されたデータがユーザ端末５０を介してプレーヤ１に転送される。

【０１７９】本実施の形態のシステムのプレーヤ１とユーザ端末５０と管理センタ２１１の実際の動作は、上述したような流れとなる。

【０１８０】ここまでは、本実施の形態のシステムにおける全体の処理の流れを説明してきたが、これ以降は、本実施の形態のシステムの主要部の個々の動作を詳細に説明する。

【０１８１】先ず、本発明実施の形態における暗号化及び圧縮と、伸長及び復号化の動作についての説明を行う。

【０１８２】上述した実施の形態のシステムのように、ネットワークを使ってディジタルコンテンツを配信する際には、そのデータ量を抑えるために圧縮／伸長技術を使用し、コピー防止或いは課金のために暗号化／圧縮技術が使われる。すなわち、配信側（上述の例では管理センタ２１１側）でディジタルコンテンツを圧縮し、さらに暗号化処理することが行われる。上述の例のように送信側（管理センタ２１１側）にて生成されたディジタルコンテンツ（暗号化／圧縮データ）をネットワークを使って配信するとき、受信側（上述の例ではプレーヤ１）では上記暗号化及び圧縮されたディジタルコンテンツを受信後に復号化し、さらに伸長してディジタルコンテンツを復元することが行われる。なお、上記暗号化と圧縮、復号化と伸長の処理の順番は入れ替わる場合もあ

る。

【０１８３】上記ディジタルコンテンツに著作権等が存在する場合、上記受信側は、上記ディジタルコンテンツを上記復号化と伸長する際に、上記著作権者等の意思に従い、課金されることになる。この課金は、主として復号化の鍵すなわちコンテンツ鍵を購入することにより行われるが、このコンテンツ鍵を購入する方法には種々ある。

【０１８４】ここで、上述したように、ディジタルコンテンツを圧縮して暗号化し、復号化して伸長するような処理手順に従った場合、例えば悪意を持ったユーザは上記復号化済みの圧縮データを比較的簡単に入手することができることになる。すなわちディジタルコンテンツの圧縮データは、一般に容量が大きく、したがって例えば受信側の一般的なコンテンツ再生装置の内部メモリではなく、安価が外部メモリに蓄積される場合が多いため、この外部メモリから直接、或いは外部メモリとの接続部分で上記圧縮されたディジタルコンテンツを不正に取り出すことが容易だからである。

【０１８５】また、圧縮に対する伸長方式のアルゴリズムは公開されている場合が多く、また伸長方式のアルゴリズムには一般的な暗号の鍵のようにそれぞれ隠しておけば処理できないようなものも存在していない。しかも、上記復号化された圧縮ディジタルコンテンツは、上記送信側から配信された暗号化と圧縮とがなされたディジタルコンテンツと比較して、データ量的に変わらず、したがって、上記復号化された圧縮ディジタルコンテンツを悪意を持って配信するののも容易である。すなわち、上記圧縮した後に暗号化されてディジタルコンテンツを配信する方式によると、誰でも容易に伸長できる圧縮ディジタルコンテンツが、悪意を持ったユーザに容易に盗難され、このため著作権者等の意思の届かないところでさらに配信されたり、伸長されたりする危険性が大きい。

【０１８６】そこで、本発明の実施の形態では、このような状況に鑑み、ネットワークを使って配信するディジタルコンテンツの安全性を向上させることを可能にするため、上記図２のプレーヤ１において、以下の図２５のフローチャートに示すような処理を行っている。

【０１８７】すなわち図２のプレーヤ１の共通暗号復号回路２４における復号化処理と上記伸長回路２６における伸長処理では、前記記憶メディアから読み出された暗号化と圧縮処理されたディジタルコンテンツのデータを、ステップＳＴ１５１のように、先ず、復号化処理のアルゴリズムの処理単位Ｘビットと、伸長処理のアルゴリズム処理単位Ｙビットとの最小公倍数１ｃｍ（Ｘ，Ｙ）の単位に分割する。

【０１８８】次に、上記最小公倍数１ｃｍ（Ｘ，Ｙ）の単位に分割された上記暗号化と圧縮処理がなされているディジタルコンテンツのデータは、ステップＳＴ１５２に示すように、当該最小公倍数１ｃｍ（Ｘ，Ｙ）の単位毎に、上記共通暗号復号回路２４にて復号化処理が行われる。

【０１８９】当該復号化処理により得られた最小公倍数１ｃｍ（Ｘ，Ｙ）の単位の圧縮されているディジタルコンテンツのデータは、ステップＳＴ１５４に示すように、当該単位分の全ての圧縮データに対して上記伸長回路２６にて伸長処理が行われる。

【０１９０】その後、この最小公倍数１ｃｍ（Ｘ，Ｙ）の単位毎の復号化及び伸長処理は、上記暗号化と圧縮処理されたディジタルコンテンツの全データについての処理が終了するまで続けられる。すなわち、ステップＳＴ１５５に示すように、最小公倍数１ｃｍ（Ｘ，Ｙ）の単位毎の復号化及び伸長処理がディジタルコンテンツの全データに対して完了したか否かの判断がなされ、完了していない時にはステップＳＴ１５２に戻り、完了したときに当該処理のフローチャートが終了する。

【０１９１】これにより全データの復号化及び伸長されたディジタルコンテンツが得られることになる。

【０１９２】なお、当該プレーヤ１における図２５のフローチャートの処理でも、上記最小公倍数１ｃｍ（Ｘ，Ｙ）単位の復号化データは存在することになるが、当該復号化データのデータ量は少ない。このため、比較的高価でも安全性の高い内部メモリに保存することができるようになり、したがって前述したような外部メモリに保存する場合のように盗まれる可能性は非常に低いものとなる。

【０１９３】また、本実施の形態における上記プレーヤ１では、上記安全性を確保するための内部メモリとして、図２のバッファメモリ２５が上記共通暗号復号回路２４と伸長回路２６との間に設けられている。すなわちこのバッファメモリ２５は、１チップの集積回路１０内に設けられており、外部からアクセスされ難く、したがってデータが外部に取り出されることはない。

【０１９４】上述のフローチャートでは、最小公倍数１ｃｍ（Ｘ，Ｙ）の単位分の全てのデータに対して復号化及び伸長処理を行うようにしており、このための具体的構成としては、例えば図２６に示す構成のように、最初に復号化処理のアルゴリズムの処理単位Ｘビットにディジタルコンテンツのデータを分割し、このＸビットのデータに復号化処理を施し、その後当該復号化処理されたＸビットの圧縮されているデータを、伸長処理のアルゴリズム処理単位Ｙビット分まとめ、当該Ｙビットの圧縮データを伸長することで、上述のように最小公倍数１ｃｍ（Ｘ，Ｙ）の単位での復号化及び伸長処理を実現するようにしている。

【０１９５】このことを実現するプレーヤ１の共通暗号復号回路２４は、入力部３０と暗号復号部３１とからなり、上記伸長回路２６は、伸長部３２と出力部３３とからなる。これら共通暗号復号回路２４と伸長回路２６の

間に前記バッファメモリ２５が設けられている。
【０１９６】ここで、より具体的な例として、上記ディジタルコンテンツに対する暗号化処理が例えばＤＥＳ（Data Encription Standard）暗号を用いて行われているのであれば、当該暗号化処理とそれに対応する復号化処理は、６４ビット単位で行われることになる。
【０１９７】また、圧縮されたディジタルコンテンツに対する伸長処理の場合、その圧縮率やサンプリング周波数によっても異なるが、現状では１Ｋ～２Ｋビット／チャンネル単位で処理される場合が多い。ここでは、便宜的に１．２８Ｋビット毎に処理されると仮定する。
【０１９８】したがって、上記ＤＥＳ暗号化方式と上記１．２８Ｋビット毎の圧縮伸長方式を用いたシステムの場合、上記最小公倍数ｌｃｍは１．２８Ｋとなる。
【０１９９】このような条件のもと、図２６の共通暗号復号回路２４の入力部３０には、前記暗号化されて圧縮されたディジタルコンテンツが入力される。当該入力部３１では、上記暗号化されて圧縮されたディジタルコンテンツを、上記復号化処理のアルゴリズムの処理単位Ｘビット、すなわち６４ビットづつのデータに分割して暗号復号部３１に出力する。
【０２００】この暗号復号部３２では、上記Ｘビットすなわち６４ビットのデータを、当該６４ビット毎に復号化処理する。この６４ビット毎の復号化により得られた６４ビットの圧縮されているデータは、バッファメモリ２５に送られる。
【０２０１】当該バッファメモリ２５は、前記コントローラ１６からの指示に従い、伸長処理のアルゴリズム処理単位Ｙビット、すなわち１．２８Ｋビット分の圧縮データがたまった時点で、当該１．２８Ｋビット分の圧縮データを一括して出力し、この圧縮データが上記伸長回路２６の伸長部３２に送られる。
【０２０２】上記伸長部２６は、上記入力された１．２８Ｋビット分の圧縮データを伸長して出力部３３に出力する。
【０２０３】また、コントローラ１６は、バッファメモリ２５にたまったデータ量をモニタしながら、復号化部３１の処理と伸長部３２の処理をコントロールする。
【０２０４】なお、このケースであれば、復号化処理を２０個（＝１２８０／６４）並列で処理すれば、より高速な処理システムになる。
【０２０５】その他、前記図２や図２６のようなハードウェア構成ではなく、プログラマブルデバイスにて上述した処理を行う場合には、バッファメモリ２５の状況に応じて、例えばコントローラ１６が復号化プログラム或いは伸長プログラムに基づいて処理を行うことになる。
【０２０６】上述の説明では、圧縮した後に暗号化したディジタルコンテンツがプレーヤ１に供給され、プレーヤ１ではこの圧縮及び暗号化されたディジタルコンテンツを復号化した後に伸長する例を挙げたが、暗号化した後に圧縮されたディジタルコンテンツを伸長して復号化する場合であっても、上述同様の効果を得ることができる。
【０２０７】また、本発明は、圧縮／伸長並びに暗号化／復号化のアルゴリズムが限定されることはなく、いかなる方式に対しても有効である。
【０２０８】このように、本発明によれば、ネットワークを使って配信するディジタルコンテンツの安全性が向上する。
【０２０９】次に、前記セキュリティＩＤの発生動作についての説明を行う。
【０２１０】本実施の形態のように、ポイント情報を予め入手しておき、ディジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、前述したように、ネットワーク上の管理センタ２１１は、ユーザ側２００のユーザ端末５０からのポイント情報の購入依頼の通信を受けた後に、金融機関２２０その他と任意の確認を行った後、そのポイント情報を暗号化して、ユーザ側２００のプレーヤ１にネットワーク経由で送る。
【０２１１】本実施の形態のように、ポイント情報を予め入手しておき、ディジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、管理センタ２１１とプレーヤ１（ユーザ端末５０）との間で、ポイント情報の購入の度に、毎回同じようなデータのやり取りを行う（例えば暗号化された「３０００円分のポイント情報の補充要求」及びそれに対応した「３０００円分のポイント情報」といった情報のやりとりを行う）と、例えば悪意を持つ者による、金融機関２２０へのいわゆる「成り済まし」による金額補充が問題点となる。なお、ここに言う金融機関への「成り済まし」とは、上記悪意を持った者が本来のユーザ（本実施の形態ではユーザ側２００）に成り済まして、不正にポイント情報を入手するようなことを言う。
【０２１２】すなわち、ポイント情報の購入の度に毎回同じようなデータのやり取りを行っていると、例えば悪意を持った者が当該データを通信回線から盗み出して同じデータを生成し、管理センタ２１１に対して送り先を自分（悪意を持った者）にしてポイント情報の入手を依頼したような場合、当該悪意を持った者がポイント情報を入手できることになり、さらにこのポイント情報の購入代金の請求は本来のユーザ側２００になされることになるという問題が発生するおそれがある。
【０２１３】そこで、こういった不正を防止するために、本発明実施の形態のシステムでは、予め受信側（プレーヤ１側）と配信側（管理センタ２１１側）の両者で連動している乱数発生機能により発生させられた乱数を安全性向上のために使用している。本実施の形態では、上記乱数として前記セキュリティＩＤを発生している。なお、両者間で乱数発生を連動させるには、例えばユーザの登録手続きなどの際に、例えばタイマ１８を初期化

するなどして、両者間の動作を同期させれば良い。

【０２１４】すなわち、この乱数（セキュリティＩＤ）を用いた場合の管理センタ２１１からプレーヤ１への例えばポイント情報入手時の動作は、以下のような流れとなる。

【０２１５】ポイント情報の購入時、管理センタ２１１からプレーヤ１に対して送られるデータは、前述したように例えばプレーヤ１から予め入手した共通鍵（セッション鍵）を用いて暗号化されたポイント情報と上記発生されたセキュリティＩＤからなるデータとなされる。

【０２１６】プレーヤ１のコントローラ１６は、当該管理センタ２１１から受け取ったデータを前述したように共通暗号復号回路２４に送り、ここで前記共通鍵を用いて復号化処理を行う。これにより、管理センタ２１１から送られてきたポイント情報とセキュリティＩＤとが得られることになる。

【０２１７】その後、プレーヤ１のコントローラ１６は、上記管理センタ２１１から送られてきたセキュリティＩＤと、自身のセキュリティＩＤ発生回路１９にて発生したセキュリティＩＤとを比較する。この比較において、コントローラ１６は、管理センタ２１１からのセキュリティＩＤと、上記自身が発生したセキュリティＩＤとが一致したときのみ、上記管理センタ２１１から送られてきたポイント情報を、前記ポイント情報格納メモリ２８に格納する。

【０２１８】これにより、正当なユーザ側２００のプレーヤ１のみがポイント情報を入手できることになる。言い換えれば、正当なユーザ側２００のプレーヤ１と同じようなプレーヤを持っている悪意の者が、前記成り済ましによって不正にポイント情報を入手しようとしても、当該悪意の者が持っているプレーヤのセキュリティＩＤと上記管理センタ２１１から送られてきたセキュリティＩＤとは一致しないため、この悪意を持った者は前記成り済ましによる不正なポイント情報入手ができないことになる。

【０２１９】勿論、ユーザ側２００のプレーヤ１で発生するセキュリティＩＤは、当該プレーヤ１の集積回路１０内に設けられたセキュリティＩＤ発生回路１９によって発生されるものであり、外部には取り出せないものであるため、悪意を持った者が当該セキュリティＩＤを盗むことはできない。

【０２２０】上記セキュリティＩＤとしての乱数を発生する構成には種々のものがあるが、その一例を図２７に示す。この図２７の構成は、前記図２のセキュリティＩＤ発生回路１９の一具体例である。

【０２２１】この図２７において、一方向関数発生部４０は、いわゆる一方向性関数を発生する。なお、上記一方向性関数とは、比較的計算が簡単な関数で逆関数がはるかに計算が困難なものである。この一方向関数は、予め秘密通信等で受け取って当該一方向関数発生部４０に保存しておくことも可能である。なお、一方向関数発生部４０は、前記図２の集積回路１０内に設けられたタイマ１８からの時間情報を入力関数として上記一方向関数を発生するようにすることも可能である。上記一方向関数は、乱数決定部４３に送られる。

【０２２２】また、ユーザ定数発生部４１は、ユーザ毎に定められた所定のユーザ定数を発生する。このユーザ定数は、予め秘密通信等で送付されて当該ユーザ定数発生部４１に保存されるものである。なお、このユーザ定数は、例えば前記ユーザＩＤ格納メモリ２３が格納するユーザＩＤを用いることもできる。

【０２２３】乱数データベース４２は、乱数を格納するものであり、例えば９９個の乱数を格納している。

【０２２４】通信回数記憶部４４は、例えばコントローラ１６から送られてくる通信回数情報を記憶するものである。この通信回数情報とは、プレーヤ１と管理センタ２１１との間の通信回数を示す情報である。

【０２２５】これら一方向関数とユーザ定数と通信回数情報は、乱数決定部４３に送られる。当該乱数決定部４３は、例えば前記タイマ１８からの時間情報に基づき、上記一方向関数とユーザ定数から、予め乱数データベース部４２に記憶された範囲の乱数を発生させる（例えば９９個）。

【０２２６】すなわち、この乱数決定部４３では、上記通信回数情報が例えば１回目の通信であれば、９９個目の乱数を上記乱数データベース部４２から取り出し、また例えば通信回数情報がｎ回目の通信であれば１００－ｎ個目の乱数を上記乱数データベース４２から取り出し、この取り出した乱数を前記セキュリティＩＤとして出力する。

【０２２７】このセキュリティＩＤ発生の構成は、プレーヤ１と管理センタ２１１とで同じものを有している。

【０２２８】なお、乱数データベース部４２に格納している全ての乱数を使い終わったときには、上記乱数決定部４２において１００個～１９９個目の乱数を計算するか、或いは新たな乱数や１方向性関数を秘密通信するなどして、乱数データベース部４２に再格納したり、一方向性関数発生部４０に再構築する。

【０２２９】また、上述した説明では、乱数（セキュリティＩＤ）を発生させて通信毎の安全性を高めるようにしているが、本実施の形態では、前述のようにユーザ側２００と管理センタ２１１側との間で通信を行う毎に、毎回異なる共通鍵（セッション鍵）をプログラマブルに発生させるようにもしているので、さらに安全性が高められている。

【０２３０】ここで、実際に送信される送信文（例えばメッセージ等）について上記乱数が挿入されると共に、セッション鍵による暗号化がなされる様子と、受信文から乱数が取り出されて正当性の確認がなされる様子を図２８と図２９を用いて説明する。なお、これら図２８、

図２９の例では、送信文に署名（ディジタル署名）を付加するようにもしている。

【０２３１】この図２８において、先ず、前記共通鍵を公開鍵暗号方式にて暗号化して送信する流れとして、通信用共通鍵発生工程Ｐ７では前記セッション鍵を通信用に用いる共通鍵として発生し、この共通鍵は公開鍵暗号化工程Ｐ８にて受信側の公開鍵で暗号化される。この暗号化された共通鍵は、受信側に送られる。

【０２３２】一方、送信文としてのメッセージを共通鍵暗号方式にて暗号化して送信する場合の流れとして、例えばメッセージ生成行程Ｐ１ではメッセージＭが生成されると共に、乱数発生工程Ｐ５にて乱数（前記セキュリティＩＤ）が発生される。これらメッセージＭと乱数は、共通鍵暗号化工程Ｐ６に送られる。この共通鍵暗号化工程Ｐ６では、上記通信用共通鍵発生工程Ｐ７にて発生した共通鍵を用いて、上記メッセージＭと乱数を暗号化する。

【０２３３】さらに、上記ディジタル署名を付加する場合、上記メッセージＭはハッシュ値計算工程Ｐ２に送られる。当該ハッシュ値計算工程Ｐ２では、上記メッセージＭからいわゆるハッシュ値が計算される。なお、ハッシュ値とはハッシュ法にて求められるアドレス情報であり、ハッシュ法とはデータ（この場合はメッセージＭ）の内容の一部（キーワード）に所定の演算を施し、その結果をアドレスとして使用するものである。このメッセージから生成されたハッシュ値（Ｍ）はディジタル署名として、秘密鍵暗号化工程Ｐ４に送られる。この秘密鍵暗号化工程Ｐ４では、送信側の秘密鍵で上記ディジタル署名を暗号化する。この暗号化されたディジタル署名は、共通鍵暗号化工程Ｐ６に送られる。これにより共通鍵暗号化工程Ｐ６では、上記通信用共通鍵発生工程Ｐ７にて発生した共通鍵を用いて、上記ディジタル署名を暗号化する。

【０２３４】これらメッセージＭとディジタル署名と乱数が受信側に送信される。

【０２３５】次に、図２９を用いて、図２８に対応する受信側での処理の流れを説明する。

【０２３６】この図２９において、先ず、前記共通鍵を公開鍵暗号方式にて復号化する流れとして、秘密鍵復号化工程Ｐ１１では、上記送信側から送信されてきた共通鍵を当該受信側の秘密鍵で復号化する。

【０２３７】一方、前記共通鍵暗号方式にて暗号化されたメッセージＭを復号化する流れとして、共通鍵復号工程１３では、上記送信されてきたメッセージＭを上記秘密鍵復号化工程Ｐ１１にて復号化した共通鍵を用いて復号化する。この復号化されたメッセージＭは、他機能送信工程Ｐ２０にて他の工程に送られることになる。

【０２３８】また、ディジタル署名を復号する流れでは、上記共通鍵復号化工程Ｐ１３にて復号化されたハッシュ値が、公開鍵復号化工程Ｐ１４にて送信側の公開鍵を用いて復号化される。同時に、ハッシュ値計算工程Ｐ１７では、上記メッセージＭからハッシュ値を計算する。これら公開鍵復号化工程Ｐ１４により復号化されたハッシュ値と上記ハッシュ値計算工程Ｐ１７にて計算されたハッシュ値とは、比較工程Ｐ１９にて比較され、改竄されていないことの確認が行われる。

【０２３９】さらに、送信された乱数については、上記共通鍵復号化工程Ｐ１３にて復号化された乱数と、当該受信側の乱数発生工程Ｐ２１にて発生された乱数とが、正当正確認工程Ｐ２２にて比較され、正当性の確認が行われる。

【０２４０】ところで、前述した図１に示した本実施の形態のシステムでは、ユーザ側２００に対するシステム側として、システム管理会社２１０と仮想店舗２３０とコンテンツプロバイダ２４０とが設けられている。なお、図１の金融機関２２０は、例えば外部の銀行等である。

【０２４１】上記システム管理会社２１０の管理センタ２１０は、仮想店舗２３０におけるディジタルコンテンツの展示や配信の管理、金融機関２２０との間でユーザ側２００の課金情報や各種情報の収集，分配及びそれらの管理、コンテンツプロバイダ２４０からのディジタルコンテンツの暗号化、扱う情報のセキュリティ管理など、システム側の主要な作業のほぼ全てを行っている。

【０２４２】しかし、上述したようなネットワークを使ってディジタルコンテンツを配信するシステムにおいて、ユーザ側がシステム側からディジタルコンテンツを入手する際や、ディジタルコンテンツの使用に伴う課金の際には、システム側に通信が集中することになり、ユーザ側に対して満足のいくレスポンスが得られなくなるおそれがある。

【０２４３】そこで、本発明の他の実施の形態では、システム管理会社２１０の機能、より具体的には管理センタ２１１の機能を、以下のように分割することで、上述したような通信の集中を防ぎ、通信のレスポンスを向上させることを可能にしている。

【０２４４】すなわち、本発明の他の実施の形態では、図３０に示すように、ユーザ側２００に対するシステム側の構成を、ディジタルコンテンツを展示，配信する機能を有するコンテンツ展示配信機関３１０と、一定の地域のユーザの課金情報を管理する機能を有する課金情報管理機関３２０と、ディジタルコンテンツを暗号化する等のデータ生成と上記コンテンツ展示配信機関３１０への生成データの配信と上記課金情報管理機関３２０からの情報収集と収益分配とシステム全体のセキュリティ管理その他を行う機能を有するシステム管理機関３３０とに分割し、各機関３１０，３２０，３３０がそれぞれ独立にユーザ側２００と通信可能になされている。

【０２４５】この図３０のような構成において、コンテンツ展示配信機関３１０は、世界中のネットワーク上に

散らばって複数配置可能なものであり、ユーザ側２００は通信費さえ支払えばどの地域のコンテンツ展示配信機関３１０へでもアクセスできる。例えばユーザ側２００がディジタルコンテンツを入手したい場合には、ユーザ側２００から上記コンテンツ展示配信機関３１０にアクセスして、ディジタルコンテンツを入手する。このときのディジタルコンテンツは、システム管理機関３３０によって暗号化等されたディジタルコンテンツ、すなわちユーザ側２００にネットワークを使って直接送信可能な状態になされたものである。

【０２４６】また、課金情報管理機関３２０は、課金情報を扱うため、余り多くのユーザを抱え込むことは安全性管理上好ましくなく、したがって、適度な数のユーザ毎に設置する。但し、あまり多く設置すると、悪意を持った第３者からの攻撃ポイント（課金情報管理機関３２０）を増やすことになり、トレードオフになるので、最適化することが望ましい。例えばユーザ側２００が課金に関する通信を行う場合には、ユーザ側２００から上記課金情報管理機関３２０に対してアクセスする。

【０２４７】上記システム管理機関３３０は、ユーザのシステムへの加入や決済方法の登録、ユーザからの集金や前記権利者，コンテンツ展示配信機関３１０，課金情報管理機関３２０等の利益受益者への利益配付など、セキュリティ上重要な情報の管理をまとめて行うことで、セキュリティを向上させる。但し、当該システム管理機関３３０は世界に１箇所のみ設けるわけではなく、あるまとまった単位、例えば国などの単位で設置するのが望ましい。例えば、ユーザ側２００がこのシステムへの加入や決済方法の登録などセキュリティ上重要な通信を行う場合には、ユーザ側２００から上記システム管理機関３３０に対してアクセスして行う。当該ユーザからの集金と利益受益者への利益配付は上記課金情報管理機関３２０から情報を入手した当該システム管理機関３３０がまとめて行う。また、著作権者等が有するソースデータすなわちコンテンツは、当該システム管理機関３３０に供給され、ここで暗号化等がなされたディジタルコンテンツに変換され、上記コンテンツ展示配信機関３１０に配信される。

【０２４８】上述のように、システム側の機能を例えば３つの機関３１０，３２０，３３０に振り分け、ユーザ側２００と各機関３１０，３２０，３３０との間で直接アクセス可能とすることにより、通信の集中を防ぎ、通信のレスポンスを向上させることが可能となる。また、コンテンツ展示配信機関３１０によれば、既存のいわゆるバーチャルモールのようなものにも対応でき、販売促進にも有効であり、ユーザにとって魅力のあるものになる。課金情報管理機関３２０を別に分けることにより、コンテンツの展示や販売機能と結託した不正防止に役立つ。また、管理するユーザを一定の数に抑えられるため、不正に対する管理機能もより効果的である。

【０２４９】以下に、上述した図３０に示した本発明の他の実施の形態のシステムにおいて、ユーザのシステムへの加入、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用のコンテンツ鍵等の入手時の情報の流れ、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れ、コンテンツの使用に伴う課金情報の流れについて説明する。

【０２５０】先ず、図３１を用いて、ユーザのシステムへの加入時の流れの主要部を説明する。

【０２５１】ユーザのシステムへの加入登録の際には、システム管理機関３３０のユーザ加入サポート機能ブロック４０２による以下の手順の従って登録作業が行われる。

【０２５２】ユーザ側２００すなわち前記プレーヤ１及びユーザ端末５０からは、先ず加入意思送付Ｔ４１のように、システムへの加入の意思を示す情報が、システム管理機関３３０に対してネットワークを介して送付される。システム管理機関３３０の通信機能ブロック４０１に入力された上記加入意思の情報は、ユーザ加入サポート機能ブロック４０２に送られる。

【０２５３】当該ユーザ加入サポート機能ブロック４０２は、上記加入意思情報を受信すると、加入必要ファイル送付Ｔ４２のように、加入に必要なファイルの情報を通信機能ブロック４０１を介してユーザ側２００に送られる。

【０２５４】ユーザ側２００では、上記システム管理機関３３０から送られてきた加入必要ファイルに基づいて、所定のフォーマットに従った加入申請書の作成が行われる。当該作成された加入申請書は、加入申請書送付Ｔ４３のように、システム管理機関３３０に送付される。

【０２５５】上記加入申請書を受け取ったユーザ加入サポート機能ブロック４０２は、クライアント機能送付Ｔ４４のように、クライアントの機能を解説する情報を、ユーザ側２００に送付する。

【０２５６】当該クライアント機能の情報を受け取ったユーザ側２００からは、ユーザ情報送付Ｔ４５のように、ユーザ側の情報、例えば前述したような口座番号やクレジット番号，名前や連絡先等のユーザ情報を、システム管理機関３３０に送付する。

【０２５７】当該ユーザ情報の送付を受けたユーザ加入サポート機能ブロック４０２は、登録手続き完了通知Ｔ４６のように、加入の登録手続きが完了した旨の情報を、ユーザ側２００に通知する。

【０２５８】また、このユーザ加入登録の手続き完了後、システム管理機関３３０のユーザ加入サポート機能ブロック４０２は、ユーザ情報送付Ｔ４７のように、通信機能ブロック４０１を介して、課金情報管理機関３２０に対してユーザ情報を転送する。このユーザ情報を受け取った課金情報管理機関３２０は、当該ユーザ情報を

データベース機能ブロック３６７に保存する。
【０２５９】以上により、ユーザのシステムへの加入時の主な流れが終了する。なお、この図３１に挙げられている他の構成についての説明は後述する。
【０２６０】次に、図３２を用いて、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明する。なお、上記ポイント情報の購入や暗号化されたディジタルコンテンツの復号用のコンテンツ鍵の情報は、コンテンツを使用するための情報であるので、以下の説明では、これらを簡略化して使用権情報と呼ぶことにする。
【０２６１】ユーザがシステムで使用する重要な情報（ここでは、コンテンツの使用権）を入手する際は、予めユーザ側２００毎に担当割当がなされている課金情報管理機関３２０に対し、ユーザ側２００からアクセスがなされる。上記ユーザ側２００から送られてくるコンテンツ使用権情報の入手要求のアクセスに対しては、課金情報管理機関３２０の使用権発行機能ブロック３６２が対応し、以下の手順に従って使用権の発行が行われる。
【０２６２】先ず、ユーザ側２００からは、購入依頼書送付Ｔ５１のように、使用権を購入したい旨の情報が課金情報管理機関３２０に対して送付される。使用権を購入したい旨の情報は、ユーザ側２００によって所定のフォーマットに従った購入依頼書の情報である。このようにネットワークを介し、この課金情報管理機関３２０の通信機能ブロック３６１に入力された上記購入依頼書の情報は、使用権発行機能ブロック３６２に送られる。
【０２６３】当該使用権発行機能ブロック３６２では、上記購入依頼書の情報を受け取ると、データベース機能ブロック３６７に保存されたユーザ情報を元にして、新しい使用権の情報を生成し、新規使用権送付Ｔ５２のように、当該使用権の情報をユーザ側２００に対して送付する。
【０２６４】ユーザ側２００は、上記新規使用権の情報の受取を確認すると、所定のフォーマットに従った受取確認書を作成し、受取確認書送付Ｔ５３のように、課金情報管理機関３２０の使用権発行機能ブロック３６２に送付する。
【０２６５】以上により、使用権の購入時の主な流れが終了する。なお、この図３２に挙げられている他の構成についての説明は後述する。
【０２６６】次に、図３３を用いて、コンテンツとコンテンツ鑑賞用の情報（ここでは使用条件とコンテンツ鍵）の流通の際の流れの主要部を説明する。
【０２６７】先ず、コンテンツ展示配信機関３１０のコンテンツ入手機能ブロック３４２は、コンテンツ請求書送付Ｔ６２のように、システム管理機関３３０に対して、ディジタルコンテンツを請求する。
【０２６８】当該コンテンツ請求書を受け取ったシステム管理機関３３０は、コンテンツ配布機能ブロック４０４において、要求されたコンテンツを流通できるように加工する。すなわち、このコンテンツ配布機能ブロック４０４では、ユーザ側２００に送付可能な状態のディジタルコンテンツ（暗号化されたディジタルコンテンツ）を生成する。この加工されたディジタルコンテンツは、コンテンツ送付６３のように、コンテンツ展示配信機関３１０に送られる。
【０２６９】当該コンテンツ展示配信機関３１０では、上記加工されたディジタルコンテンツを、コンテンツデータベース機能ブロック３４５に保存する。
【０２７０】また、システム管理機関３３０のコンテンツ配布機能ブロック４０４では、コンテンツ鑑賞用の情報として、コンテンツＩＤと使用条件と暗号化されたコンテンツを復号するためのコンテンツ鍵とを、コンテンツ鑑賞用情報送付Ｔ６４のように、課金情報管理機関３２０に送付する。
【０２７１】課金情報管理機関３２０では、上記コンテンツ鑑賞用の情報を、コンテンツ鍵・使用条件受取機能ブロック３６３にて受理し、データベース機能ブロック３６７に保存する。
【０２７２】次に、ユーザ側２００は、コンテンツ入手依頼Ｔ６１のように、コンテンツ展示配信機関３１０に対してアクセスし、コンテンツを入手する。すなわち、コンテンツ展示配信機関３１０は、通信機能ブロック３４１を介して上記ユーザ側２００からコンテンツの入手の要求がなされると、コンテンツデータベース機能ブロック３５４に保存している暗号化されたディジタルコンテンツを読み出し、当該読み出したディジタルコンテンツをユーザ側２００の送付する。
【０２７３】その後、ユーザ側２００は、コンテンツ鑑賞用情報請求Ｔ６５にて課金情報管理機関３２０に対してアクセスし、コンテンツ鑑賞用情報送付Ｔ６６のようにコンテンツ鑑賞用の情報を入手する。すなわち、課金情報管理機関３２０では、通信機能ブロック３６１を介して、上記ユーザ側２００からコンテンツ鑑賞用の情報として使用条件とコンテンツ鍵の請求がなされると、コンテンツ鍵・使用条件発行機能ブロック３６４からコンテンツ鍵と使用条件とを発行し、これらを通信機能ブロック３６１を介してユーザ側２００に送付する。
【０２７４】以上により、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れが終了する。なお、この図３３に挙げられている他の構成についての説明は後述する。
【０２７５】次に、図３４を用いて、コンテンツが実際に鑑賞されたときの精算、すなわちコンテンツ使用料金の精算の流れの主要部を説明する。
【０２７６】先ず、ユーザ側２００にてコンテンツの鑑賞が行われた後、当該ユーザ側２００からは、精算書送付Ｔ７１のように、例えば前述のようにしてポイント使用情報すなわちコンテンツの使用記録が課金情報管理機

関３２０に対して送付される。このように通信機能ブロック３６１を介して上記ユーザ側２００から上記コンテンツ使用記録の送付を受けると、課金情報管理機関３２０の精算手続き受付機能ブロック３６５にて当該コンテンツ使用記録を受け取り、これに対応する精算確認書を発行する。当該精算確認書は、精算確認書送付Ｔ７３のように、同じく通信機能ブロック３６１を介してユーザ側２００に送付される。これにより、ユーザ側２００は精算が行われたことを知ることができる。

【０２７７】次に、課金情報管理機関３２０の精算手続き受付機能ブロック３６５は、使用権発行機能ブロック３６２から使用権発行情報を発行させる。この使用権発行情報は、上記ユーザ側２００から送られてきたコンテンツ使用記録と共に、通信機能ブロック３６１を介し、ユーザ決済・コンテンツ使用記録送付Ｔ７４としてシステム管理機関３３０に送付される。

【０２７８】システム管理機関３３０は、集金及び分配機能ブロック４０５にて、各地に分散している課金情報管理機関３２０から送付されてきた情報をまとめ、集金額と集金先とお金の分配先を集計し、実際の金融機関を通して決済する。

【０２７９】以上により、コンテンツ使用料金の精算の流れが終了する。なお、この図３４に挙げられている他の構成についての説明は後述する。

【０２８０】上述の図３０から図３４までの説明において、コンテンツ展示配信機関３１０、課金情報管理機関３２０、システム管理機関３３０とユーザ側２００との間のデータ送受や、コンテンツ展示配信機関３１０、課金情報管理機関３２０とシステム管理機関３３０との間のデータ送受においても、前述同様にデータの暗号化と復号化が行われていることは言うまでもない。またこの暗号化と復号化においても、公開鍵暗号方式と共通鍵暗号方式の何れを用いても良いし、前述したようにコンテンツ鍵や共通鍵の暗号化方式としては公開鍵暗号方式を使用し、メッセージや各種の書類等の暗号化方式としては共通鍵暗号方式を使用することができる。また、これら暗号化と共に前記乱数を用いたセキュリティ向上の手法や、コンテンツを扱う際の暗号化と圧縮の処理単位の最小公倍数化を使用することも可能である。

【０２８１】次に、上述した各機関３１０、３２０、３３０の具体的な構成について簡単に説明する。

【０２８２】先ず、図３５を用いてコンテンツ展示配信機関３１０の構成の説明を行う。

【０２８３】この図３５において、当該コンテンツ展示配信機関３１０は、大別して、ユーザ側２００とシステム管理機関３３０との間の通信機能を担当する通信機能ブロック３４１と、コンテンツの入手機能を担当するコンテンツ入手機能ブロック３４２と、コンテンツの展示機能を担当するコンテンツ展示機能ブロック３４３と、精算を担当する精算機能ブロック３４４と、コンテンツを保存するコンテンツデータベース機能ブロック３４５とからなる。

【０２８４】上記コンテンツ入手機能ブロック３４２は、システム管理機関３３０に対してコンテンツを請求するときの請求書の作成を担当するコンテンツ請求書作成機能部３５１と、システム管理機関３３０からコンテンツを受け取ったときの受領書の作成を担当するコンテンツ受領書作成機能部３５２と、これらあつかったコンテンツとコンテンツデータベース機能ブロック３４５に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部３５３とからなる。

【０２８５】上記コンテンツ展示機能ブロック３４３は、実際に仮想店舗にコンテンツを展示する機能を担当するコンテンツ展示機能部３５４と、これら展示しているコンテンツと上記コンテンツデータベース機能ブロック３４５に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部３５５とからなる。

【０２８６】上記精算機能ブロック３４４は、領収書を発行する機能を担当する領収書発行機能部３５６と、金融機関２２０との間の対応を担当する金融機関対応機能部３５７とからなる。

【０２８７】次に、図３６を用いて、課金情報管理機関３２０の構成の説明を行う。

【０２８８】この図３６において、当該課金情報管理機関３２０は、大別して、ユーザ側２００とシステム管理機関３３０との間の通信機能を担当する通信機能ブロック３６１と、使用権を発行する機能を担当する使用権発行機能ブロック３６２と、コンテンツ鍵と使用条件の受け取りを担当するコンテンツ鍵・使用条件受取機能ブロック３６３と、コンテンツ鍵と使用条件の発行を担当するコンテンツ鍵・使用条件発行機能ブロック３６４と、精算手続きの受け付け機能を担当する精算手続き受付機能ブロック３６５と、分配と受け取りの機能を担当する分配受取機能ブロック３６６と、データベース機能ブロック３７６とからなる。

【０２８９】上記使用権発行機能ブロック３６２は、購入依頼書の確認機能を担当する購入依頼書確認機能部３７１と、クライアントすなわちユーザ側２００の使用権の残高（ポイント情報の残高）や使用記録（ポイント使用情報）等のデータの確認を担当するポイントデータ確認機能部３７２と、使用権を発生する機能を担当する使用権発生機能部３７３と、使用権の送付書を作成する機能を担当する使用権送付書作成機能部３７４と、使用権と使用権送付書を実際に送付する機能を担当する送付機能部３７５と、使用権の受け取り書の確認を担当する使用権受取確認機能部３７６と、発行した使用権の情報を保存する機能を担当する使用権発行情報保存機能部３７７とからなる。

【０２９０】上記コンテンツ鍵・使用条件受取機能ブロック３６３は、コンテンツ鍵と使用条件の受取を担当す

る受取機能部３７８と、コンテンツ鍵と使用条件を保存する保存機能部３７９とからなる。

【０２９１】上記コンテンツ鍵・使用条件発行機能ブロック３６４は、コンテンツ鍵と使用条件の入手依頼を受信する機能を担当する受信機能部３８０と、コンテンツ鍵と使用条件をデータベース機能ブロック３６７から検索して探し出す機能を担当する検索機能部３８１と、コンテンツ鍵と使用条件を暗号化して送付する機能を担当する送信機能部３８２と、コンテンツ鍵と使用条件の受取書の確認機能を担当する確認機能部３８３とからなる。

【０２９２】上記精算手続き受付機能ブロック３６５は、暗号化されているコンテンツ使用記録（ポイント使用情報）を受信して復号化する機能を担当するコンテンツ使用記録受信機能部３８４と、コンテンツ使用記録の確認を担当するコンテンツ使用記録確認機能部３８５と、コンテンツ使用記録をデータベース機能ブロック３６７の保存する機能を担当するコンテンツ使用記録保存機能部３８６と、精算手続きの完了書を作成する機能を担当する完了書作成機能部３８７と、コンテンツ使用記録をまとめて編集する機能を担当するまとめ機能部３８９とからなる。

【０２９３】上記分配受取機能ブロック３６６は、集金を行う際の資料を請求する資料請求書の確認機能を担当する請求書確認機能部３９０と、システム管理機関３３０に対して提出するコンテンツ使用記録の報告書を作成する機能を担当する使用記録報告書作成機能部３９１と、システム管理機関３３０に対して提出する使用権発行情報の報告書を作成する機能を担当する使用権発行報告書作成機能部３９２と、報告書の受信確認書の確認機能を担当する確認書確認機能部３９３とからなる。

【０２９４】データベース機能ブロック３６７は、使用権のデータを保存する機能を担当する使用権データベース機能部３９４と、コンテンツ鍵と使用条件のデータを保存する機能を担当するコンテンツ鍵・使用権データベース機能部３９５と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部３９６と、ユーザに関する情報を保存するユーザ管理データベース機能部３９７とからなる。

【０２９５】次に、図３７を用いて、システム管理機関３３０の構成の説明を行う。

【０２９６】この図３７において、当該システム管理機関３３０は、大別して、ユーザ側２００、コンテンツ展示配信機関３１０、及び課金情報管理機関３２０との間の通信機能を担当する通信機能ブロック４０１と、ユーザ加入の際のサポートを行うユーザ加入サポート機能ブロック４０２と、コンテンツの配布を担当するコンテンツ配布機能ブロック４０４と、データベース機能ブロック４０３と、集金と分配の機能を担当する集金及ぶ分配機能ブロック４０５とからなる。

【０２９７】上記ユーザ加入サポート機能ブロック４０２は、加入申請書の作成と送信を担当する加入申請書作成送信機能部４１１と、暗号化された共通鍵を受信して復号化する機能を担当する共通鍵受信機能部４１２と、ユーザ側２００から送信されてきた加入申請書の確認機能を担当する加入申請書確認機能部４１３と、クライアントＩＤすなわちユーザＩＤを発生する機能を担当するＩＤ発生機能部４１４と、加入申請書をデータベース機能ブロック４０３に保存する機能を担当する加入申請書保存機能部４１５と、クライアント機能を生成するクライアント機能生成機能部４１６と、登録情報をデータベース機能ブロック４０３に保存する機能を担当する登録情報保存機能部４１７とからなる。

【０２９８】データベース機能ブロック４０３は、ユーザの情報を保存管理するユーザ管理データベース機能部４１８と、コンテンツを保存するコンテンツデータベース機能部４１９と、課金情報管理機関３２０の情報を保存管理する課金情報管理機関データベース機能部４２０と、コンテンツ展示配信機関３１０の情報を保存管理するコンテンツ展示配信機関データベース機能部４２１とからなる。

【０２９９】コンテンツ配信機能ブロック４０４は、コンテンツの請求書の確認機能を担当する請求書確認機能部４２２と、生コンテンツすなわち加工前のコンテンツ（ソースデータ）をデータベース機能ブロック４０３のコンテンツデータベース機能部４１９から検索する機能を担当するコンテンツ検索機能部４２３と、コンテンツＩＤを生成するコンテンツＩＤ生成機能部４２４と、コンテンツ鍵を生成するコンテンツ鍵生成機能部４２５と、コンテンツ使用条件を生成するコンテンツ使用条件生成機能部４２６と、生コンテンツすなわち加工前のコンテンツを圧縮するコンテンツ圧縮機能部４２７と、コンテンツの暗号化を行うコンテンツ加工機能部４２８と、コンテンツＩＤとコンテンツ鍵と使用条件とをデータベース機能ブロック４０３のコンテンツデータベース機能部４１９に保存する機能を担当する保存機能部４２９と、コンテンツを通信機能ブロック４０１を介して送付する機能を担当するコンテンツ送付機能部４３０と、コンテンツの受領書を確認する機能を担当するコンテンツ受領書確認機能部４３１と、コンテンツＩＤとコンテンツ鍵と使用条件を通信機能ブロック４０１を介して送付する機能を担当するＩＤ・鍵・使用条件送付機能部４３２と、コンテンツＩＤとコンテンツ鍵と使用条件の受領書を確認する機能を担当するＩＤ・鍵・使用条件受領書確認機能部４３３とからなる。

【０３００】集金及び分配機能ブロック４０５は、集金に使用する資料の請求書を作成する資料請求書作成機能部４３４と、コンテンツ使用権を通信機能ブロック４０１を介して受信する機能を担当するコンテンツ使用権受信機能部４３５と、コンテンツ使用記録を通信機能ブロ

ック４０１を介して受信する機能を担当するコンテンツ使用記録受信機能部４３６と、受信の確認書を作成する機能を担当する受信確認書作成機能部４３７と、ユーザへ請求する請求額の計算と請求書の作成を行う請求書の作成を行う計算・請求書作成機能部４３８と、使用により集金した使用金を権利者に分配する際の分配金の計算と納付書の作成を行う計算・納付書作成機能部４３９とからなる。

【０３０１】次に、当該他の実施の形態のシステムに対応するユーザ側２００の構成を、図３８を用いて説明する。なお、この図３８は、前記プレーヤ１とユーザ端末５０の各機能をまとめて表している。

【０３０２】この図３８において、当該ユーザ側２００の構成は、大別すると、システム管理機関３３０、コンテンツ展示配信機関３１０、及び課金情報管理機関３２０との間の通信機能を担当する通信機能ブロック４５１と、コンテンツの入手を担当するコンテンツ入手機能ブロック４５２と、ポイント情報やコンテンツ鍵、使用条件等の使用権の購入を担当する使用権購入機能ブロック４５３と、コンテンツ鍵と使用条件の入手を担当するコンテンツ鍵・使用条件入手機能ブロック４５４と、精算手続きを担当する精算手続き機能ブロック４５５と、システムへの加入をサポートする機能を担当するユーザ加入サポート機能ブロック４５６と、コンテンツの鑑賞と課金の機能を担当するコンテンツ鑑賞課金機能ブロック４５７と、データベース機能ブロック４５８とからなる。

【０３０３】上記コンテンツ入手機能ブロック４５２は、実際にコンテンツを入手する機能を担当するコンテンツ入手機能部４６１と、コンテンツを記憶メディアに保存させる機能を担当するコンテンツ保存機能部４６２とからなる。

【０３０４】使用権購入機能ブロック４５３は、使用権の購入依頼書を作成する購入依頼書作成機能部４６３と、クライアント（ユーザ）の使用権の残高（ポイント残高）や使用記録（ポイント使用情報）等のデータのまとめを担当するまとめ機能部４６４と、使用権としての各情報をインストールする機能を担当する使用権インストール機能部４６５と、使用権受取書を作成する使用権受取書作成機能部４６７とからなる。

【０３０５】コンテンツ鍵・使用条件入手機能ブロック４５４は、コンテンツ鍵と使用条件の入手依頼書を作成する入手依頼書作成機能部４６８と、コンテンツ鍵と使用条件の受信を担当する受信機能部４６９と、コンテンツ鍵と使用条件の受取書を作成する受取書作成機能部４７０とからなる。

【０３０６】精算手続き機能ブロック４５５は、コンテンツ使用記録（ポイント使用情報）のまとめを行うまとめ機能部４７１と、精算手続きの完了書の受信を担当する完了書受信機能部４７２とからなる。

【０３０７】上記ユーザ加入サポート機能ブロック４５６は、加入申請書の作成を担当する加入申請書作成機能部４７３と、クライアント機能のインストールすなわちユーザのプレーヤ１の初期化を担当するクライアント機能インストール機能部４７４、登録情報を作成する機能を担当する登録情報作成機能部４７５とからなる。

【０３０８】コンテンツ鑑賞課金機能ブロック４５７は、記憶メディアに保存されたコンテンツの検索を担当するコンテンツ検索機能部４７６と、使用権の確認を担当する使用権確認機能部４７７と、例えばコンテンツの選択を行うときに簡易的にコンテンツを再生する簡易コンテンツ鑑賞機能部４７８と、課金情報（ポイント情報）の管理を行う課金機能部４７９と、暗号化されているコンテンツを復号化するコンテンツ復号機能部４８０と、圧縮されているコンテンツを伸長するコンテンツ伸長機能部４８１と、例えば記憶メディアに保存されているコンテンツの内容を認識可能にするためのコンテンツビューア機能部４８２とからなる。

【０３０９】データベース機能ブロック４５８は、使用権のデータを保存する使用権データベース機能部４８３と、コンテンツ鍵と使用条件を保存するコンテンツ鍵・使用条件データベース機能部４８４と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部４８５と、ユーザ情報を保存するユーザ情報データベース機能部４８６とからなる。

【０３１０】次に、上述したような各実施の形態のプレーヤ１とユーザ端末５０の具体的な使用形態について、図３９と図４０を用いて説明する。

【０３１１】図３９に示すように、プレーヤ１は、前記アナログ出力端子２とＰＣ用インターフェース端子３と記憶メディア用Ｉ／Ｏ端子４がプレーヤ１の筐体外に突き出た状態で配置されており、上記記憶メディア用Ｉ／Ｏ端子４には、記憶メディア６１が接続されるようになっている。また、これらプレーヤ１と記憶メディア６１は、例えばケース６０内に収納可能に形成されており、このケース６０の例えば一端側に上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が配置されるようになされている。

【０３１２】このプレーヤ１及び記憶メディア６１が収納されたケース６０は、上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が配置される側から、上記ユーザ端末５０としてのパーソナルコンピュータ５０の入出力ポート５３に挿入接続可能なように形成されている。

【０３１３】当該パーソナルコンピュータ５０は、コンピュータ本体に、ディスプレイ装置５２とキーボード５４とマウス５５とを備えた一般的な構成を有するものであるが、上記入出力ポート５３内には上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３と対応したインターフェースが形成されている。したが

って、上記プレーヤ１及び記憶メディア６１が収納されたケース６０を上記パーソナルコンピュータ５０の入出力ポート５３に挿入するだけで、上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が上記パーソナルコンピュータ５０と接続されるようになる。

【０３１４】上記図３９の例では、パーソナルコンピュータ５０の入出力ポート５３内に、上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３と対応したインターフェースを形成するようにしているが、例えば図４０に示すように、パーソナルコンピュータ５０の汎用入出力ポートのインターフェースに対応できるアダプタ６２を、上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３の間に配置することも可能である。

【０３１５】以上述べてきたことから、本発明の実施の形態のシステムにおいては、ディジタルコンテンツはシステムの共通鍵であるコンテンツ鍵にて暗号化されているので、本実施の形態のシステムに登録したユーザ（プレーヤ１）であれば、この暗号化されたコンテンツを自由にコピーでき、コンテンツ鍵を入手しさえすればこのコンテンツの鑑賞も可能である。したがって、このコンテンツ（暗号化されたコンテンツの）記憶メディアへのインストールも簡単に行える。一方、本実施の形態システムに準拠していない端末装置では、暗号化されたディジタルコンテンツを復号できないので、コンテンツの著作権や当該コンテンツの権利者の権利は保護される。

【０３１６】また、本発明の実施の形態システムによれば、ポイント情報をプリペイド方式（料金前払い方式）により補充することにし、コンテンツ鑑賞時にポイント情報が減額されるようにするとともに、そのポイントの使用情報を収集するようにしているので、使用済みのポイントに関する権利をもつ権利者（著作権者等）及びコンテンツ販売店舗等は、鑑賞代金の回収が可能である。

【０３１７】さらに、ポイント情報やポイント使用情報のデータのやりとりの際には、前述したように暗号化が施されているので、セキュリティ性が向上している。例えば全く前回のデータと同じものを偽造して課金用のポイント情報を盗もうとしても、前述したように、システム側とプレーヤ側とで連動した乱数（セキュリティＩＤ）を使用し、両者が一致していることを確認してから取引を行うものとしているので、安全である。

【０３１８】またさらに、プレーヤの主要構成要素は１チップ化されており、鍵情報や復号化されたディジタルコンテンツを外部に取り出すことが困難となっている。このプレーヤ１は、当該プレーヤ１の破壊によるデータ横取りを防ぐためにプレーヤ１自体にタンパーレジスタンス機能を備えている。

【０３１９】上述したように、本発明の実施の形態によれば、セキュリティ上強度の高いディジタルコンテンツ配信システムが構築されている。

【０３２０】なお、上述のディジタルコンテンツとしては、ディジタルオーディオデータの他に、ディジタルビデオデータ等の各種のものを挙げることができる。上記ディジタルビデオデータとして動画像データ（オーディオデータも含む）使用した場合、前記圧縮の手法としては、例えばＭＰＥＧ（Moving Picture Image CodingExperts Group）等の圧縮手法を使用できる。なお、上記ＭＰＥＧは、ＩＳＯ（国際標準化機構）とＩＥＣ（国際電気標準会議）のＪＴＣ（Joint Technical Committee）１のＳＣ（Sub Committee）２９のＷＧ（Working Group）１１においてまとめられた動画像符号化方式の通称であり、ＭＰＥＧ１，ＭＰＥＧ２，ＭＰＥＧ４等がある。

【０３２１】さらに、上記暗号化の手法としては、前述したように、例えばいわゆるＤＥＳ（Data Encryption Standard）と呼ばれている暗号化手法を使用することができる。なお、ＤＥＳとは、米国のＮＩＳＴ（National Institute of Standards and Technology）が１９７６年に発表した標準暗号方式（暗号アルゴリズム）である。具体的には、６４ビットのデータブロック毎にデータ変換を行うものであり、関数を使った変換を１６回繰り返す。上記ディジタルコンテンツやポイント情報等は、当該ＤＥＳを用い、いわゆる共通鍵方式にて暗号化されている。なお、上記共通鍵方式とは、暗号化するための鍵データ（暗号鍵データ）と復号化するための鍵（復号鍵データ）が同一となる方式である。

【０３２２】また、前記図１のプレーヤ１の共通鍵保管メモリ２２や通信用鍵保管メモリ２１、ポイント使用情報格納メモリ２９、ポイント情報格納メモリ２８等には、例えばいわゆるＥＥＰＲＯＭ（電気的に消去可能なＲＯＭ）を使用できる。

【０３２３】他に記憶メディアとしては、例えばハードディスクやフロッピィディスク、光磁気ディスク，相変化型光ディスク等の記録媒体、或いは半導体メモリ（ＩＣカード等）の記憶メディアを使用できる。

【０３２４】その他、上述の実施の形態では、コンテンツの選択や仮想店舗２３０に展示されたコンテンツの内容確認等の際には、ユーザ端末５０のキーボード５４やマウス５５、ディスプレイ装置５２を使用して選択、確認等を行っていたが、これらキーボードやマウス、ディスプレイ装置に機能を簡略化して、プレーヤ１に持たせることも可能である。すなわち。図２のように、入力キー部６や表示部７をプレーヤ１に設けることも可能である。

【０３２５】

【発明の効果】以上の説明で明らかなように、本発明によれば、簡単に持ち運びができて何時でも何処でもディジタルコンテンツを楽しむことが可能であり、また、ディジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築す

ることをも可能である。

【図面の簡単な説明】

【図１】本発明の実施の形態のディジタルコンテンツ配布システムの全体構成を示すシステム構成図である。

【図２】本発明の実施の形態のシステムに対応するプレーヤの具体的構成を示すブロック回路図である。

【図３】本発明の実施の形態のシステムに対応する管理センタの具体的構成を示すブロック回路図である。

【図４】本実施の形態のシステムにおいてプレーヤの購入時の手順の説明に用いる図である。

【図５】本実施の形態のシステムにおいてディジタルコンテンツの検索からプレーヤ用の記憶メディアへのディジタルコンテンツのインストールまでの手順の説明に用いる図である。

【図６】実施の形態のシステムにおいて課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順の説明に用いる図である。

【図７】実施の形態のシステムにおいて課金代金の分配の手順の説明に用いる図である。

【図８】実施の形態のシステムにおいてポイント購入時のプレーヤにおける処理の流れを示すフローチャートである。

【図９】実施の形態のシステムにおいてポイント購入時のユーザ端末における処理の流れを示すフローチャートである。

【図１０】実施の形態のシステムにおいてポイント購入時の管理センタにおける処理の流れを示すフローチャートである。

【図１１】実施の形態のシステムにおいてポイント購入時の情報送受のシーケンスを示す図である。

【図１２】実施の形態のシステムにおいてディジタルコンテンツの入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図１３】実施の形態のシステムにおいてディジタルコンテンツの入手時のユーザ端末における処理の流れを示すフローチャートである。

【図１４】実施の形態のシステムにおいてディジタルコンテンツの入手時の管理センタにおける処理の流れを示すフローチャートである。

【図１５】実施の形態のシステムにおいてディジタルコンテンツの入手時の情報送受のシーケンスを示す図である。

【図１６】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図１７】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のユーザ端末における処理の流れを示すフローチャートである。

【図１８】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の管理センタにおける処理の流れを示すフローチャートである。

【図１９】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の情報送受のシーケンスを示す図である。

【図２０】実施の形態のシステムにおいてプレーヤとユーザ端末を用いてディジタルコンテンツを実際に鑑賞する際の処理の流れを示すフローチャートである。

【図２１】実施の形態のシステムにおいてポイント使用情報返却時のプレーヤにおける処理の流れを示すフローチャートである。

【図２２】実施の形態のシステムにおいてポイント使用情報返却時のユーザ端末における処理の流れを示すフローチャートである。

【図２３】実施の形態のシステムにおいてポイント使用情報返却時の管理センタにおける処理の流れを示すフローチャートである。

【図２４】実施の形態のシステムにおいてポイント使用情報返却時の情報送受のシーケンスを示す図である。

【図２５】暗号化と圧縮の処理単位の最小公倍数にて復号化と伸長を行う際の処理の流れを示すフローチャートである。

【図２６】暗号化と圧縮の処理単位の最小公倍数の単位毎の復号化及び伸長処理を行う構成を示すブロック回路図である。

【図２７】セキュリティＩＤとしての乱数を発生する具体的構成を示すブロック回路図である。

【図２８】共通鍵を公開鍵暗号方式にて暗号化して送信する際に乱数が挿入される様子を説明するための図である。

【図２９】受信文から乱数が取り出されて正当性の確認がなされる様子を説明するための図である。

【図３０】システム側の機能を分割したときの各機関の説明に用いる図である。

【図３１】システム側の機能を分割した実施の形態において、ユーザのシステムへの加入時の流れの主要部を説明するための図である。

【図３２】システム側の機能を分割した実施の形態において、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明するための図である。

【図３３】システム側の機能を分割した実施の形態において、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れの主要部を説明するための図である。

【図３４】システム側の機能を分割した実施の形態において、コンテンツが実際に鑑賞されたときの精算の流れの主要部を説明するための図である。

【図３５】システム側の機能を分割した実施の形態において、コンテンツ展示配信機関の構成を示すブロック図である。

【図３６】システム側の機能を分割した実施の形態にお

いて、課金情報管理機関の構成を示すブロック図である。

【図３７】システム側の機能を分割した実施の形態において、システム管理機関の構成を示すブロック図である。

【図３８】システム側の機能を分割した実施の形態において、ユーザ側の構成を示すブロック図である。

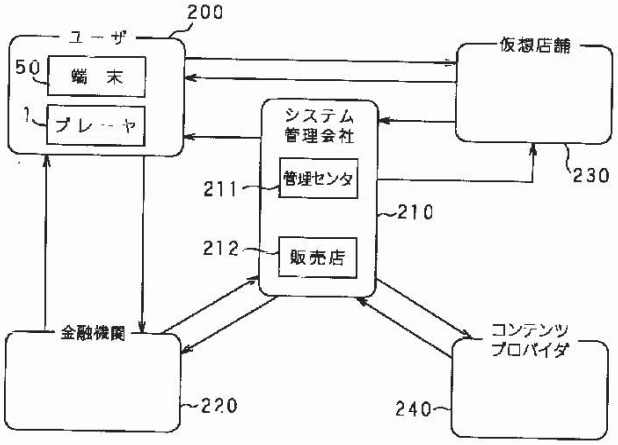
【図３９】プレーヤとユーザ端末の具体的な使用形態の一例の説明に用いる図である。

【図４０】プレーヤとユーザ端末の具体的な使用形態の他の例の説明に用いる図である。

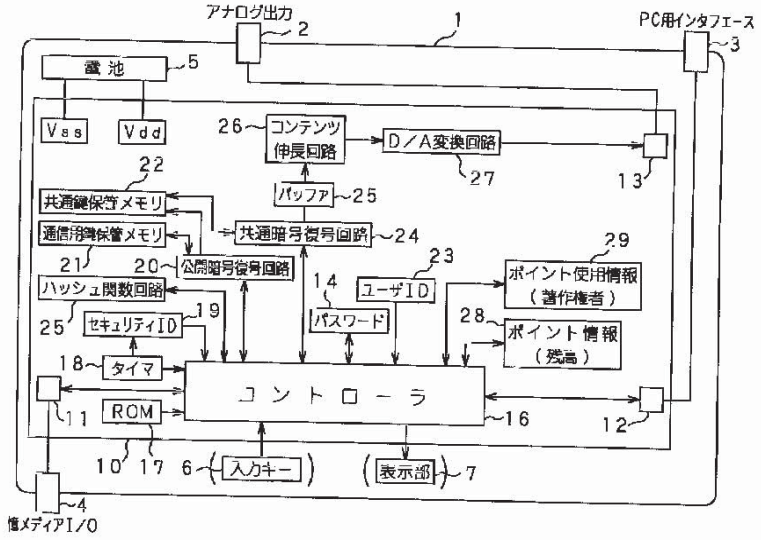
【符号の説明】

１　プレーヤ、　２　アナログ出力端子、　３　ＰＣ用インターフェース端子、　４　記憶メディア用Ｉ／Ｏ端子、　１６　コントローラ、　１９　セキュリティＩＤ発生回路、　２０　公開暗号復号回路、　２１　通信用鍵保管メモリ、２２　共通鍵保管メモリ、　２３　ユーザＩＤ格納メモリ、　２４　共通暗号復号回路、　２５　バッファメモリ、　２６　伸長回路、　２７　Ｄ／Ａ変換回路、　５０　ユーザ端末、　１００　コンテンツ管理機能ブロック、　１１０ユーザ管理機能ブロック、　１２０　使用情報管理機能ブロック、　１３０　管理機能ブロック、　２００　ユーザ側、　２１０　システム管理会社、　２１１管理センタ、　２２０　金融機関、　２３０　仮想店舗、　２４０　コンテンツプロバイダ

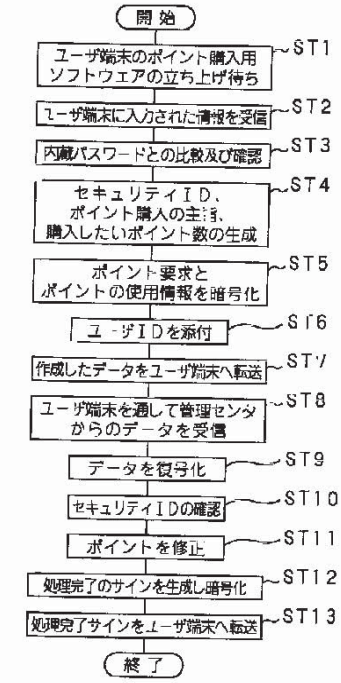
【図１】



【図２】

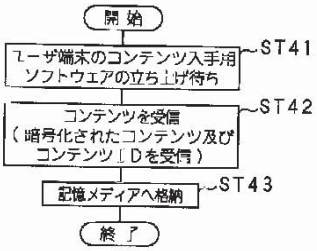


【図８】



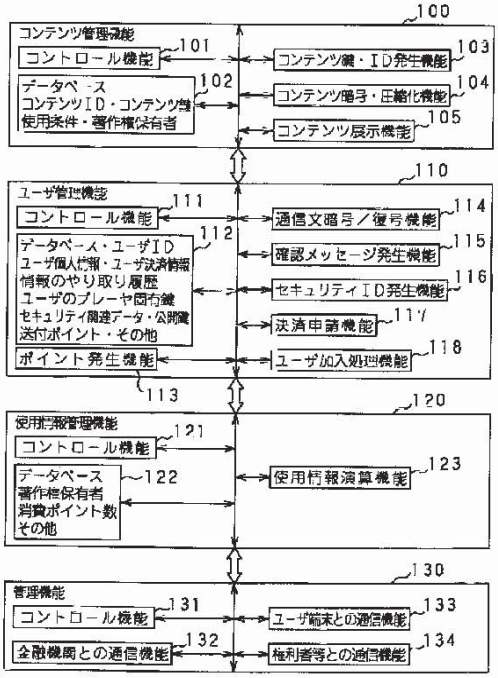
ポイント購入時のプレーヤのフローチャート

【図１２】

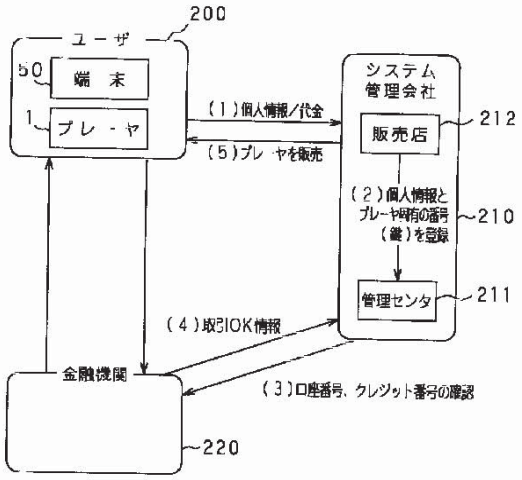


コンテンツ入手時のプレーヤのフローチャート

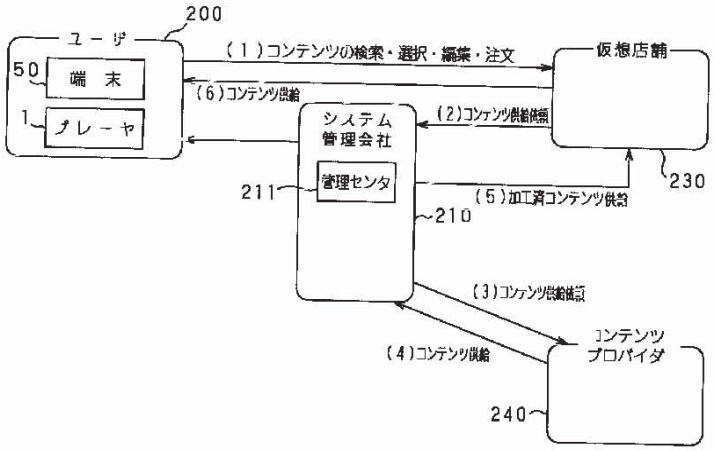
【図3】



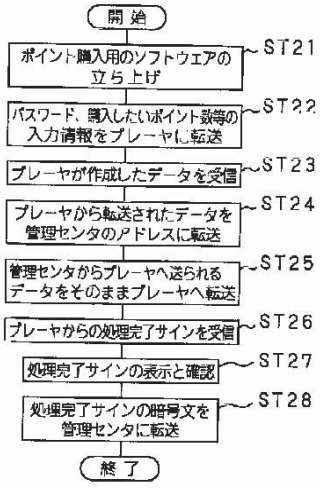
【図4】



【図5】

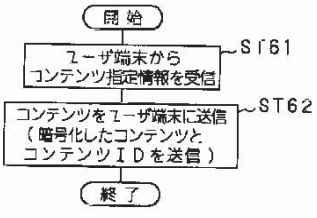


【図9】



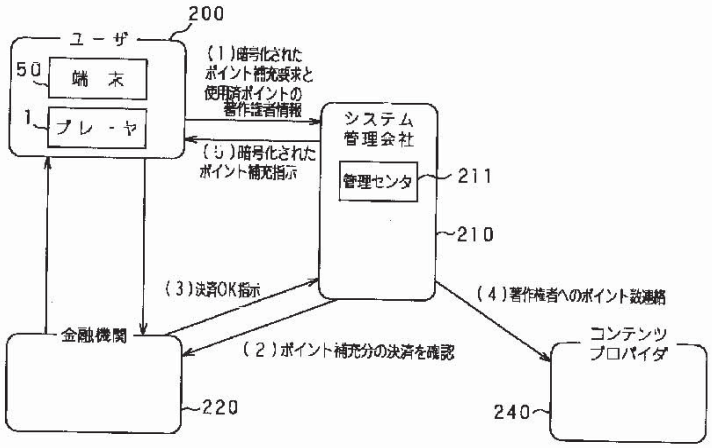
ポイント購入時のユーザ端末のフローチャート

【図14】

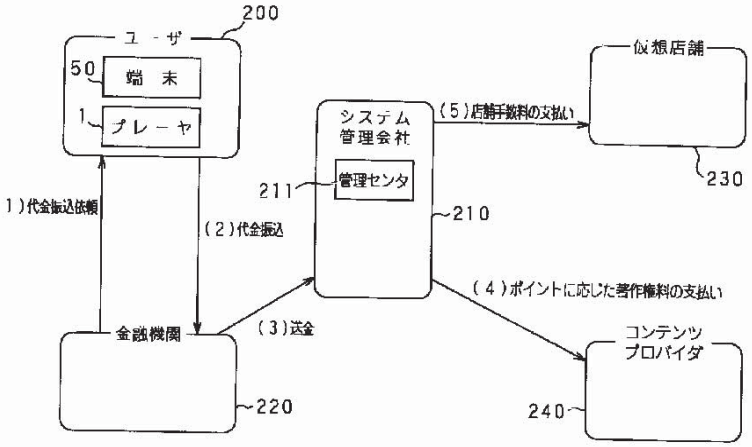


コンテンツ入手時の管理センタのフローチャート

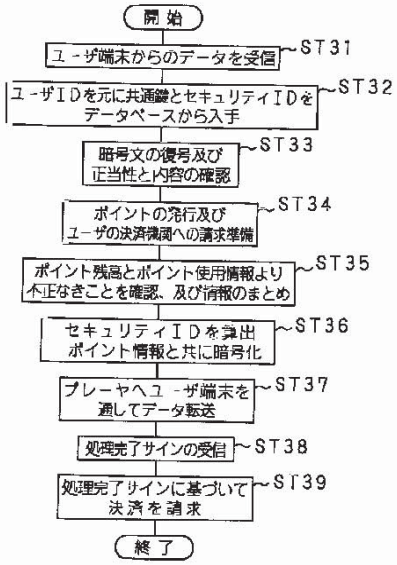
【図6】



【図7】

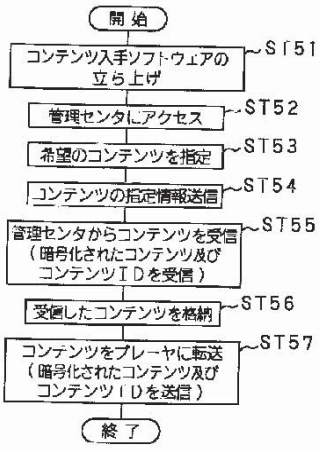


【図10】



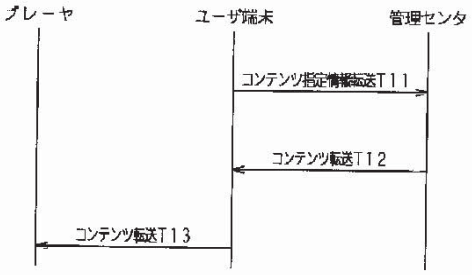
ポイント購入時の管理センタのフローチャート

【図13】



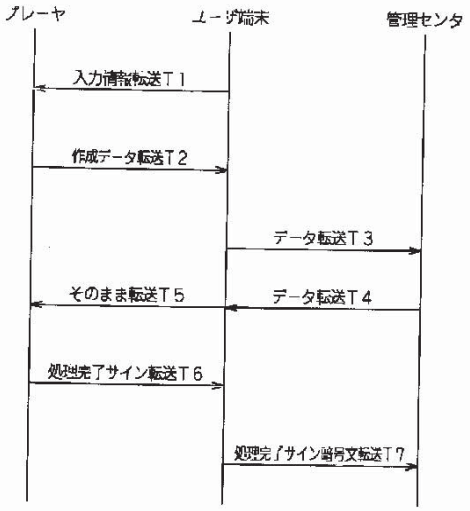
コンテンツ入手時のユーザ端末のフローチャート

【図15】



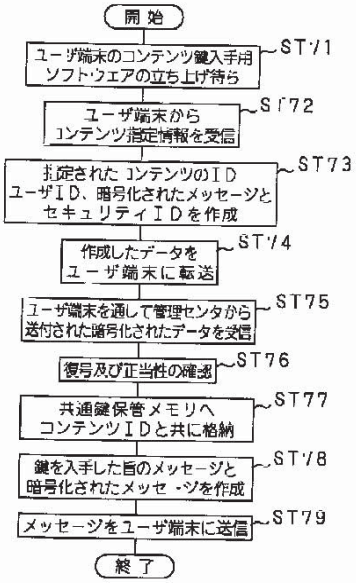
コンテンツ入手時のシーケンス

【図１１】



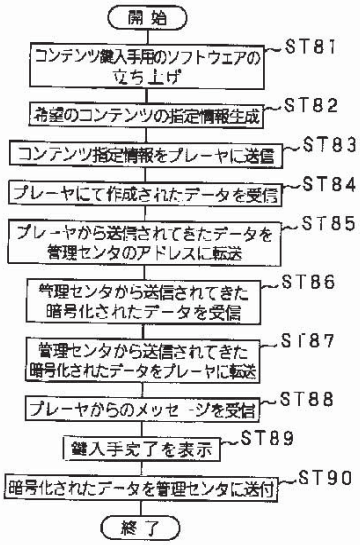
ポイント購入時のシーケンス

【図１６】



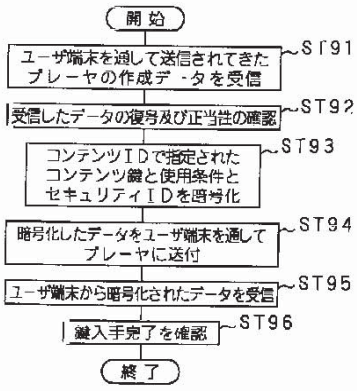
コンテンツ鍵・入手時のプレーヤのフローチャート

【図１７】



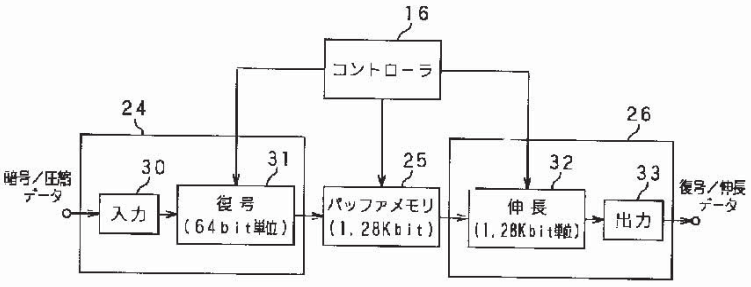
コンテンツ鍵・使用条件入手時のユーザ端末のフローチャート

【図１８】

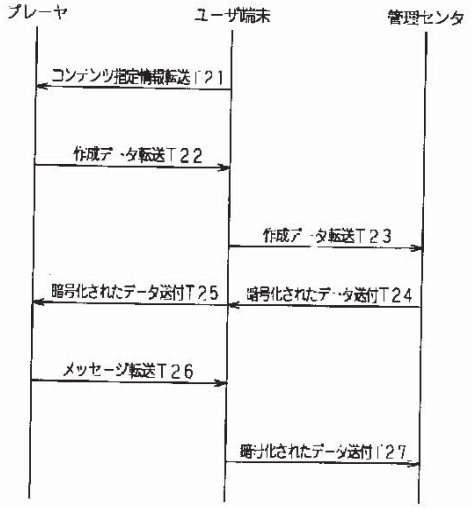


コンテンツ鍵・使用条件入手時の管理センタのフローチャート

【図２６】

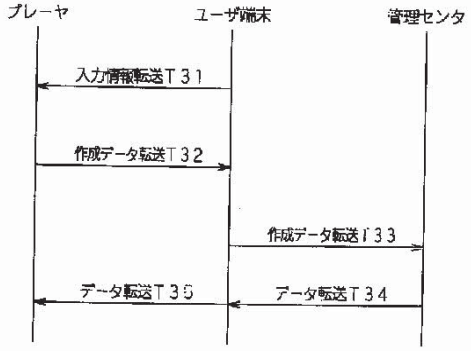


【図19】



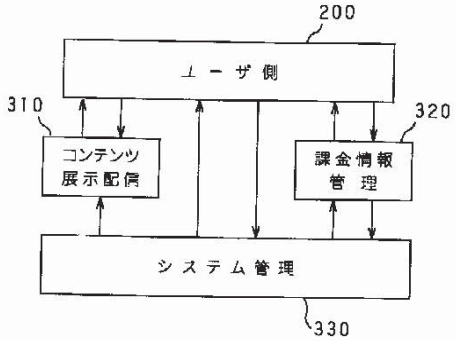
コンテンツ鍵・使用条件入手時のシーケンス

【図24】

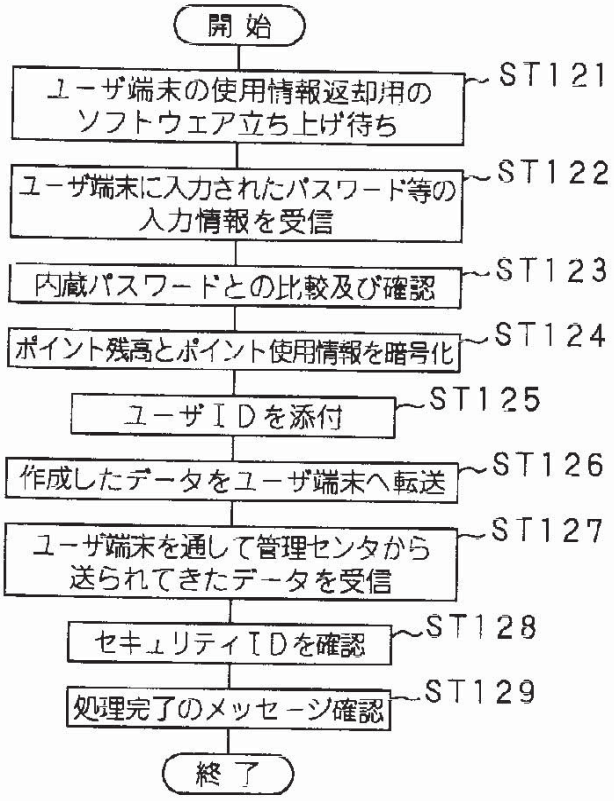


使用情報返却時のシーケンス

【図30】

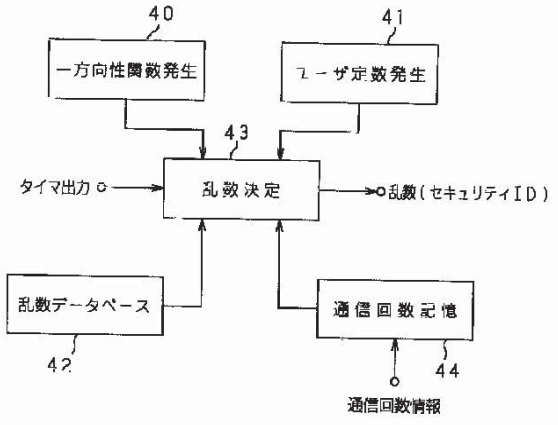


【図21】

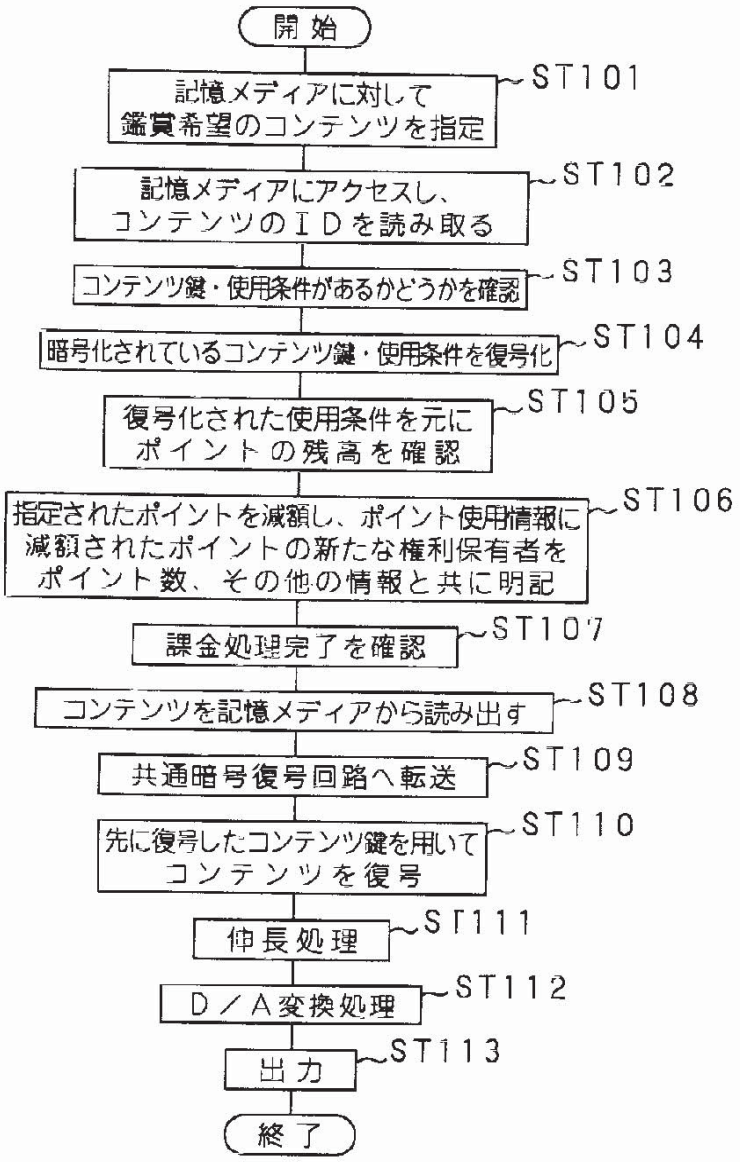


使用情報返却時のプレーヤのフローチャート

【図27】

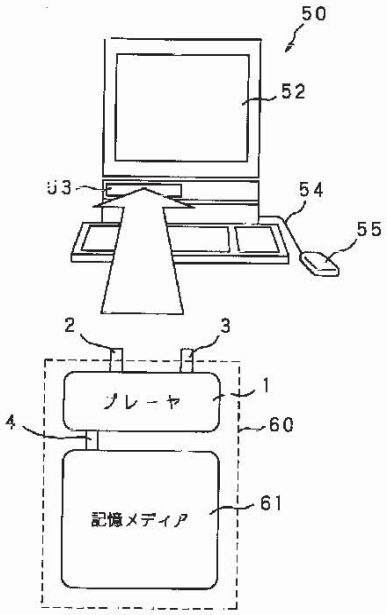


【図20】

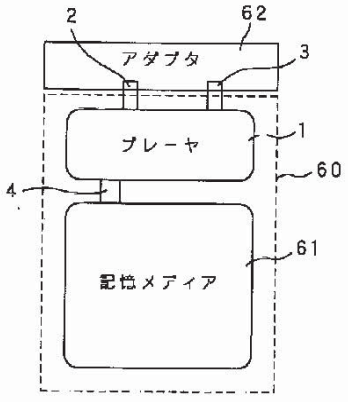


コンテンツ鑑賞時のプレーヤのフローチャート

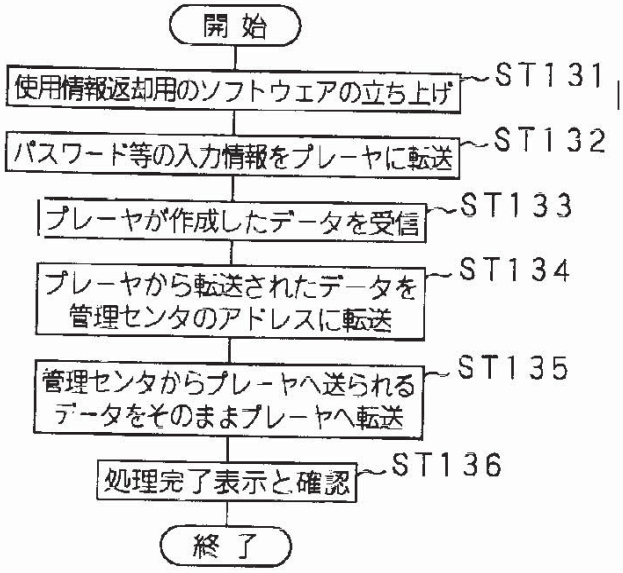
【図39】



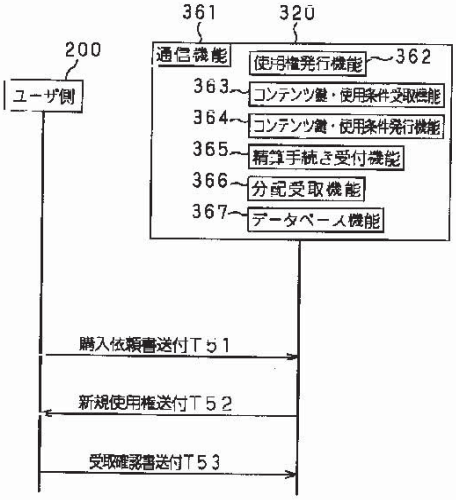
【図40】



【図22】

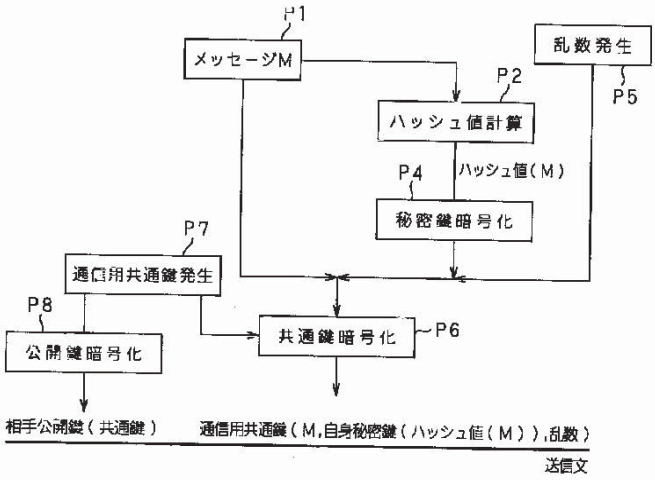


【図32】

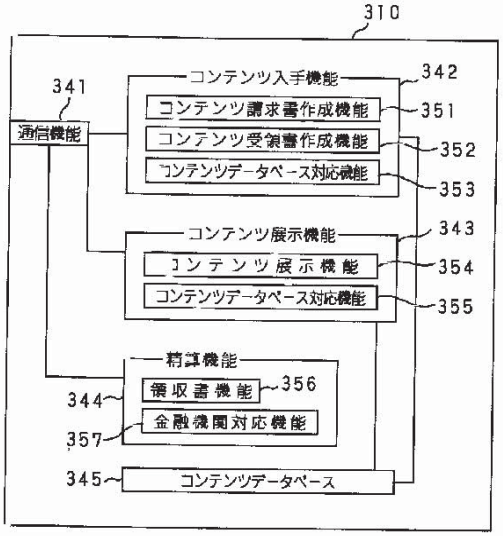


使用情報返却時のユーザ端末のフローチャート

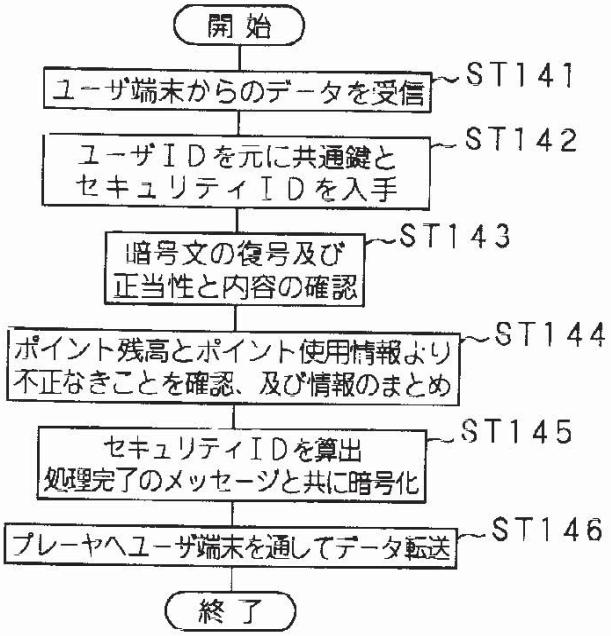
【図28】



【図35】

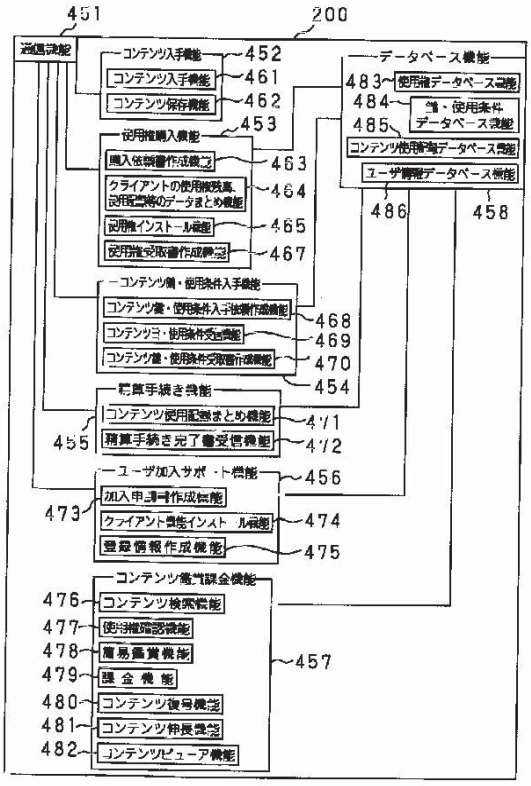


【図23】

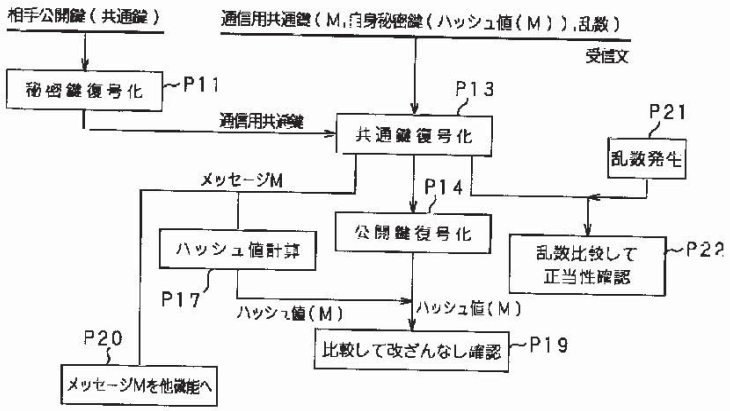


使用情報返却時の管理センタのフローチャート

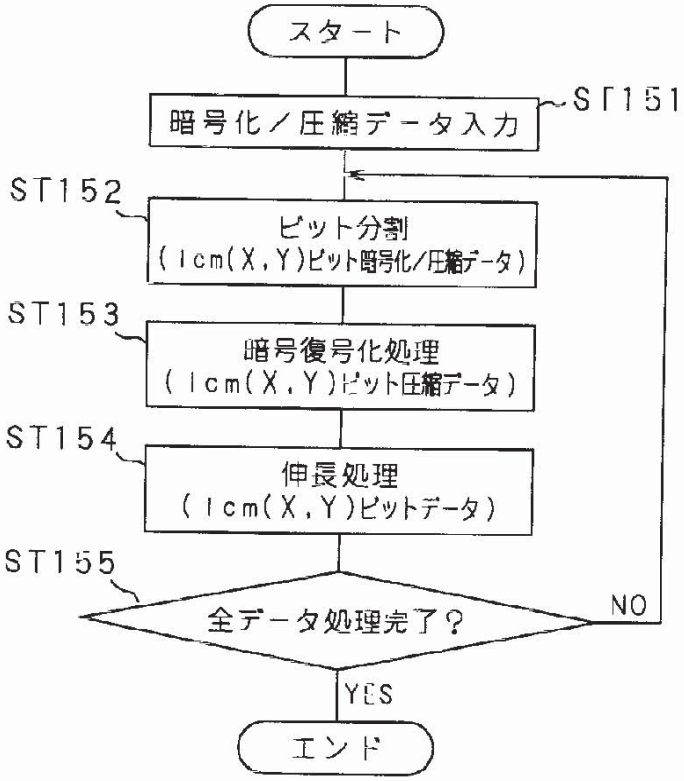
【図38】



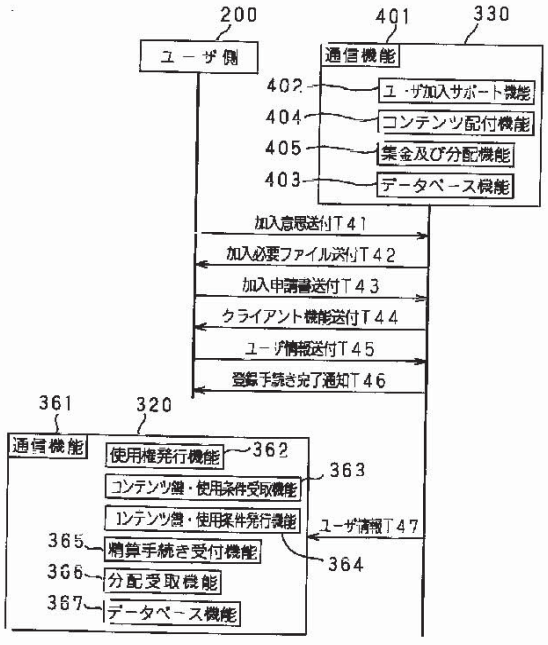
【図29】



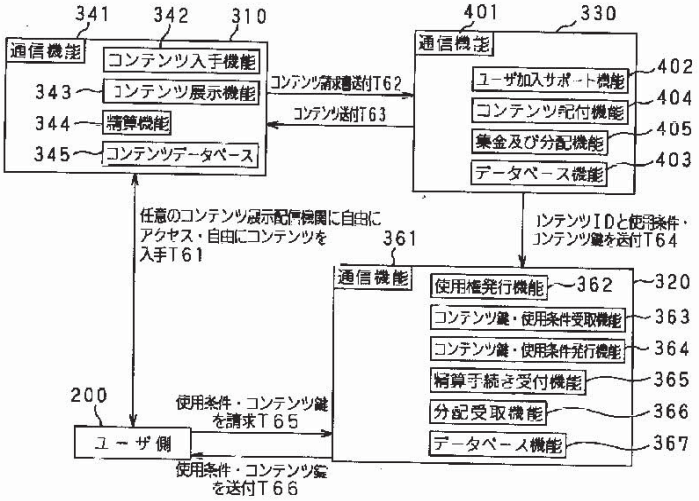
【図25】


スタート
暗号化／圧縮データ入力
ST151
ST152
ピット分割
（1cm(X,Y)ビット暗号化/圧縮データ）
ST153
暗号復号化処理
（1cm(X,Y)ビット圧縮データ）
ST154
伸長処理
（1cm(X,Y)ビットデータ）
ST155
全データ処理完了？
NO
YES
エンド

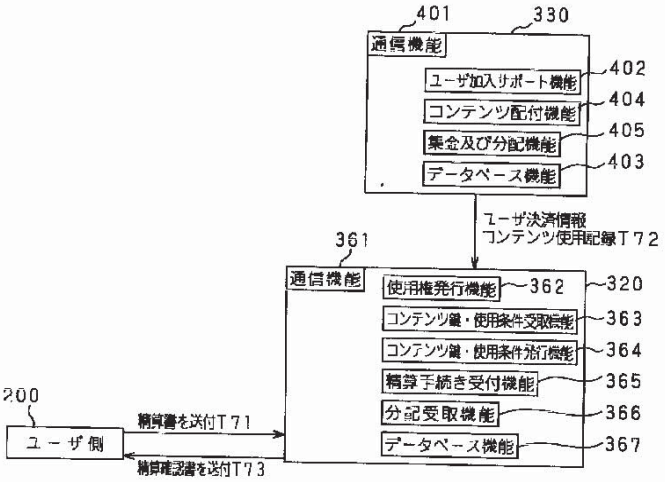
【図31】


200
ユーザ側
401
330
通信機能
402
ユーザ加入サポート機能
404
コンテンツ配付機能
405
集金及び分配機能
403
データベース機能
加入意思送付T41
加入必要ファイル送付T42
加入申請書送付T43
クライアント機能送付T44
ユーザ情報送付T45
登録手続き完了通知T46
361
320
通信機能
使用権発行機能
362
363
コンテンツ鍵・使用条件受取機能
コンテンツ鍵・使用条件発行機能
ユーザ情報T47
365
精算手続き受付機能
364
366
分配受取機能
367
データベース機能

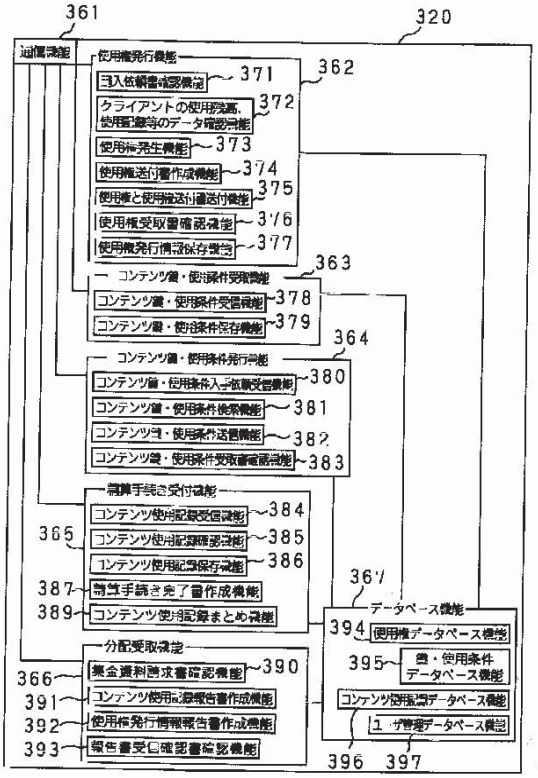
【図33】


341
342
310
401
330
通信機能
コンテンツ入手機能
コンテンツ展示機能
精算機能
コンテンツデータベース
コンテンツ請求書送付T62
コンテンツ送付T63
ユーザ加入サポート機能
コンテンツ配付機能
集金及び分配機能
データベース機能
402
404
405
403
343
344
345
任意のコンテンツ展示配信機関に自由にアクセス・自由にコンテンツを入手T61
コンテンツIDと使用条件・コンテンツ鍵を送付T64
361
通信機能
使用権発行機能
362
320
コンテンツ鍵・使用条件受取機能
363
コンテンツ鍵・使用条件発行機能
364
精算手続き受付機能
365
分配受取機能
366
データベース機能
367
200
ユーザ側
使用条件・コンテンツ鍵を請求T65
使用条件・コンテンツ鍵を送付T66

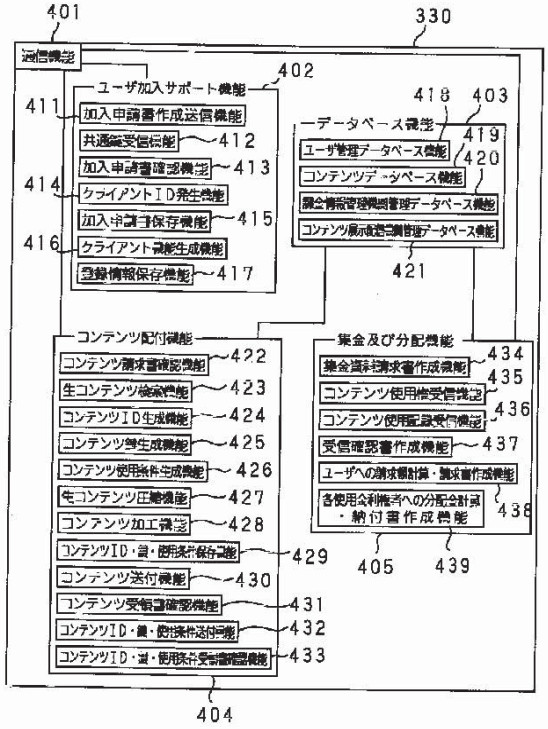
【図34】


401
330
通信機能
ユーザ加入サポート機能
コンテンツ配付機能
集金及び分配機能
データベース機能
402
404
405
403
ユーザ決済情報コンテンツ使用記録T72
361
通信機能
使用権発行機能
362
320
コンテンツ鍵・使用条件受取機能
363
コンテンツ鍵・使用条件発行機能
364
精算手続き受付機能
365
分配受取機能
366
データベース機能
367
200
ユーザ側
精算書を送付T71
精算確認書を送付T73

【図36】



【図37】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04L 9/08		H04M 15/00	Z
12/14		G06F 15/21	Z
H04M 15/00		H04L 9/00	601E
			601A
		11/02	F

(19) Japanese Patent Office (JP)

(12) Publication of Unexamined Patent Application (A)

(11) Publication Number: H10-269289

(43) Date of Publication: October 9, 1998

(51) Int. Cl.[6]	Identification Code	FI		
G06F 17/60		G06F	15/21	330
1/00	370		1/00	370 F
9/06	550		9/06	550 Z
15/00	330		15/00	330 Z
G09C 1/00	660	G09C	1/00	660 F
H04L 9/08		H04M	15/00	Z
12/14		G06F	15/21	Z
H04M 15/00		H04L	9/00	601 E
				601 A
			11/02	F

Examination Request Status: Not Yet Requested. No. of Claims: 37, OL (39 pages total)

(21) Application number: H09-74182

(22) Date of Application: March 26, 1997

(71) Applicant: 000002185

Sony Corporation

6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo

(72) Inventor: Koichi MAARI

C/O Sony Corporation,

6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo

(74) Agent: Akira KOIKE, Attorney (and two others)

(54) [Title of the Invention] METHOD OF CONTROLLING DIGITAL CONTENT DISTRIBUTION, A METHOD OF REPRODUCING DIGITAL CONTENT, AND AN APPARATUS USING THE SAME

(57) [Abstract]
[Problem]

To build a system that is portable, enables digital content to be enjoyed anywhere and anytime, provides adequate protection against copying and unauthorized use of the digital content, and is economical.

[Resolution Means]

A public-key encryption/decryption circuit 20 for decrypting an encrypted content key and encrypting a session key; a common key storage memory 22 for storing the content key and the session key; a communication key storage memory 21 for storing key information for a public-key encryption system; a point information storage memory 29 for storing point information; a point usage information storage memory 28 for storing point usage information; a common key encryption/decryption circuit 24 for decrypting encrypted digital content, decrypting encrypted point information, and encrypting point usage information; a decompressing circuit 26 for decompressing compressed digital content; and a D/A conversion circuit 27 for subjecting digital content to digital-to-analog conversion are integrated on a single chip.

What is Claimed is:

[Claim 1]

A method for controlling digital content distribution, the method comprising steps of:

digital content manipulation for encrypting and compressing digital content using a content key for each piece of relevant digital content;

content transmission for transmitting the manipulated digital content in accordance with a digital content transmission request from a communication partner;

content key transmission for encrypting a content key for use in decrypting the manipulated digital content and transmitting same in accordance with a content key transmission request from a communication partner;

billing information transmission for encrypting billing information that is decremented each time the manipulated digital content is decrypted and transmitting same in accordance with a billing information transmission request from a communication partner;

content usage information reception for receiving and decrypting encrypted content usage information transmitted from a communication partner; and

usage fee distribution for distributing a usage fee, which is collected on the basis of the content usage information, to a proprietor of the digital content.

[Claim 2]

The method for controlling digital content distribution according to claim 1, wherein the content key is a common key.

[Claim 3]

The method for controlling digital content distribution according to claim 1, wherein the content key is encrypted using a public key of a communication partner.

[Claim 4]

The method for controlling digital content distribution according to claim 1 comprising a step of common key decryption for receiving and decrypting an encrypted common key transmitted from a communication partner.

[Claim 5]

The method for controlling digital content distribution according to claim 4, wherein the common key is a session key.

[Claim 6]

The method for controlling digital content distribution according to claim 4, wherein billing information is encrypted using the common key in the billing information transmission step.

[Claim 7]

The method for controlling digital content distribution according to claim 4,

wherein the common key is used in decrypting the encrypted content usage information in the content usage information receiving step.

[Claim 8]

The method for controlling digital content distribution according to claim 1, wherein the encrypted content usage information transmitted from the communication partner in connection with the billing information transmission request from the communication partner is received in the content usage information receiving step.

[Claim 9]

The method for controlling digital content distribution according to claim 1, wherein information indicating a content use condition is transmitted together with the billing information in the billing information transmission step.

[Claim 10]

A method for reproducing digital content, the method comprising steps of:

content reception for receiving and storing digital content manipulated using encryption and compression processing;

content key request information generation for generating content key request information for requesting a content key required for decrypting the manipulated digital content;

content key request information transmission for encrypting and transmitting the content key request information;

content key reception for receiving a content key sent in accordance with the content key request;

content key decryption for decrypting the encryption that has been applied to the content key;

content key storage for storing either the encrypted content key or the post-decryption content key;

content decryption for decrypting the manipulated digital content using the content key;

billing information request information generation for generating billing information request information for requesting billing information that is decremented each time the manipulated digital content is decrypted;

billing information request information transmission for encrypting and transmitting the billing information request information;

billing information reception for receiving billing information transmitted in accordance with the billing information request, decrypting the encryption applied to the billing information, and storing same;

content decompression for decompressing the manipulated digital content;

content usage information storage for generating and storing content usage

information that corresponds to the decryption of the manipulated digital content; and

content usage information transmission for encrypting and transmitting the content usage information.

[Claim 11]

The method for reproducing digital content according to claim 10, wherein, in the content usage information storage step, a balance in the stored billing information is confirmed, the stored billing information is decremented in accordance with the decryption of the manipulated digital content, and content usage information including at least an amount of the billing information decrement is generated.

[Claim 12]

The method for reproducing digital content according to claim 10, comprising a step of digital/analog conversion for subjecting the decrypted and decompressed digital content to digital-to-analog conversion.

[Claim 13]

The method for reproducing digital content according to claim 10, wherein the manipulated digital content is stored in an external storage medium in the content reception step.

[Claim 14]

The method for reproducing digital content according to claim 10, wherein the content key is a common key.

[Claim 15]

The method for reproducing digital content according to claim 10, wherein the content key is decrypted using a unique secret key in the content key decryption step.

[Claim 16]

The method for reproducing digital content according to claim 10, comprising a step of common key transmission for generating a common key, and encrypting and transmitting the common key.

[Claim 17]

The method for reproducing digital content according to claim 16, wherein a session key is generated as the common key in the common key transmission step.

[Claim 18]

The method for reproducing digital content according to claim 16, wherein the billing information request information is encrypted using the common key in the billing information request information transmission step.

[Claim 19]

The method for reproducing digital content according to claim 16, wherein the common key is used in the encryption of the content usage information in the

content usage information transmission step.

[Claim 20]

The method for reproducing digital content according to claim 10, wherein, in the content usage information transmission step, the encrypted content usage information is transmitted in connection with the billing information request resulting from the billing information request information generation step.

[Claim 21]

The method for reproducing digital content according to claim 10, wherein information indicating a use condition for content encrypted and transmitted together with the billing information is also received in the billing information reception step.

[Claim 22]

A digital content reproducing apparatus, comprising:

data communication means for performing data communications;

content storage control means for receiving digital content manipulated using encryption and compression processing and storing same in a storage medium;

content key decryption means for decrypting an encrypted content key; content key storage means for storing either the encrypted content key or the post-decryption content key;

content decryption means for decrypting the manipulated digital content using the content key;

billing information decryption means for decrypting the encryption applied to billing information that is decremented each time the manipulated digital content is decrypted;

billing information storage means for storing the decrypted billing information; content decompression means for decompressing the manipulated digital content;

content usage information generation means for generating content usage information that corresponds to the decryption of the manipulated digital content;

content usage information storage means for storing the content usage information; and

content usage information encryption means for encrypting the content usage information.

[Claim 23]

The digital content reproducing apparatus according to claim 22, comprising:

content key request information encryption means for encrypting content key request information for requesting a content key required for the decryption of the manipulated digital content; and

billing information request information encryption means for encrypting

billing information request information for requesting billing information that is decremented each time the manipulated digital content is decrypted.

[Claim 24]

The digital content reproducing apparatus according to claim 22, wherein the content usage information generation means check a balance of billing information stored in the billing information storage means, decrement the stored billing information in accordance with the decryption of the manipulated digital content, and generate content usage information including at least an amount of the billing information decrement.

[Claim 25]

The digital content reproducing apparatus according to claim 22, comprising digital/analog conversion means for subjecting the decrypted and decompressed digital content to digital-to-analog conversion.

[Claim 26]

The digital content reproducing apparatus according to claim 22, wherein the content storage control means store the manipulated digital content in an external storage medium.

[Claim 27]

The digital content reproducing apparatus according to claim 22, wherein the content key is a common key.

[Claim 28]

The digital content reproducing apparatus according to claim 22, comprising unique key storage means for storing an apparatus-unique key, wherein in the content key decryption step, the encrypted content key is decrypted using an apparatus-unique secret key stored in the unique key storage means.

[Claim 29]

The digital content reproducing apparatus according to claim 22, comprising common key generation means for generating a common key, and common key encryption means for encrypting the common key.

[Claim 30]

The digital content reproducing apparatus according to claim 29, wherein the common key generation means generate a session key as the common key.

[Claim 31]

The digital content reproducing apparatus according to claim 29, wherein the billing information decryption means decrypt the billing information using the common key.

[Claim 32]

The digital content reproducing apparatus according to claim 29, wherein the

content usage information encryption means encrypt the content usage information using the common key.

[Claim 33]

The digital content reproducing apparatus according to claim 22, wherein the content usage information encryption means encrypt the content usage information in connection with the encryption of the billing information request information by the billing information request information encryption means.

[Claim 34]

The digital content reproducing apparatus according to claim 22, wherein information indicating a use condition for encrypted content is also decrypted together with the billing information in the billing information decryption step.

[Claim 35]

The digital content reproducing apparatus according to claim 22 which is configured to be portable.

[Claim 36]

The digital content reproducing apparatus according to claim 22 comprising a card-shaped enclosure.

[Claim 37]

The digital content reproducing apparatus according to claim 22 comprising an integrated circuit.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention]

The present invention generally relates to a digital content distribution control method suitable for a system for distributing digital content such as audio data and video data, for example, and for billing according to a usage quantity of the digital content, a digital content reproducing method, and an apparatus using the digital content reproducing method.

[0002]

[Background Art]

A software control method disclosed in Japanese Examined Patent Application Publication No. H6-19707, a software usage control method disclosed in Japanese Examined Patent Application Publication No. H6-28030, and a software control method disclosed in Japanese Examined Patent Application Publication No. H6-95302, for example, are known as advantageous techniques for simplifying the distribution of digital content such as computer programs, audio data, video data, and the like, exploiting potential demand for digital content, and expanding the market for this field. The software control method disclosed in Japanese Examined Patent Application Publication No. H6-19707 is designed so that, when using software such as computer programs and video data, which are intangible assets, it is possible for software proprietors and the like to ascertain the usage status of the software. Furthermore, the software usage control method disclosed in Japanese Examined Patent Application Publication No. H6-28030 is designed so that, when using software such as computer programs, video data, and the like, which are intangible assets, purchase prices are set for paid programs (available for use free-of-charge after purchase), and data indicating an amount of money available for purchase of paid programs is provided in a computer system. When purchasing a paid program, these programs are registered in a table as the names of software programs available in this computer system, and data indicating the amount of money available to purchase paid programs is decremented by the price of the purchased software. When deleting registered software from this table, the data indicating the amount of money available to purchase paid programs is incremented and updated in accordance with the circumstances. In addition, the software control method disclosed in Japanese Examined Patent Application Publication No. H6-95302 is designed to be effective in a system in a case where, in order to collect utilization fees according to the actual amount of usage (the number of times or the length of time used, or the like) for a paid program when using software such as computer programs, video data, and the like, which are intangible assets, the identifications of the programs that were used,

"user identification codes, and fees are recorded" in advance, and, by retrieving this record, the program proprietor is able to ascertain the utilization fees for the programs owned by the program proprietor and to collect the utilization fees in accordance with the usage of the programs.

[0003]

[Problems to be Solved by the Invention]

However, the above-mentioned system for distributing digital content through a network is considered to be operated only on personal computers. Therefore, there is no system that is portable with ease and allows the digital content to be enjoyed anytime and anywhere.

[0004]The above-mentioned disclosed technique is advantageous in exploiting potential demands for digital content and expanding the market. However, this technique is insufficient in protecting digital content from illegal duplication or unauthorized use and provides no economical system.

[0005]

Accordingly, the present invention was conceived in light of the foregoing, and an object thereof is to provide a method of controlling digital content distribution, and a method and apparatus for reproducing digital content that make it possible to build a system that is portable, enables digital content to be enjoyed anywhere and anytime, provides adequate protection against the copying and unauthorized use of the digital content, and is economical.

[0006]

[Means to Solve the Problem]

According to the present invention, the digital content distributing side manipulates digital contents by encrypting and compressing the same, transmits the manipulated digital content, an encrypted content key, and encrypted billing information to a communication partner, and distributes to digital content proprietors the digital content usage fees collected based on digital content usage information received from the communication partner. On the other hand, the digital content reproducing side decrypts and decompresses the manipulated digital content for reproduction by the content key. At the same time, the reproducing side decrements the billing information according to the use of the content and generates content usage information to be transmitted to the content distributing side. Additionally, the digital content reproducing apparatus associated with the present invention is made portable. The present invention thereby solves the above-mentioned problems.

[0007]

[Description of the Preferred Embodiments]

The preferred embodiments of the present invention will be described below

while referring to the drawings.

[0008]

Before describing specific contents and constitutions of a digital content distributing method, a digital content reproducing method, and a digital content reproducing apparatus according to the present invention, an outline constitution of an entire system to which the present invention is applied and an operating method of this system will be described for easier understanding of the above-mentioned distributing method, reproducing method and reproducing apparatus with reference to FIGS. 1 through 7.

[0009]

FIG. 1 shows a schematic constitution of the entire system.

[0010]

In FIG. 1, it is assumed that a user 200 has a digital content reproducing apparatus (hereafter referred to as a player 1) associated with the present invention and a so-called personal computer (hereafter referred to as a user terminal 50).

[0011]

The user terminal 50 is an ordinary personal computer that stores various software as application software, to be described later, for use in the present invention and connects to a display device providing display means, a speaker serving as sounding means, and a keyboard and a mouse serving as information inputting means. The user terminal 50 can be connected to a system administration company 210 through a network, for example, and also has interface means between the user terminal and the player 1 that allows data to be transferred.

[0012]

The player 1 has a constitution as shown in FIG. 2, for example.

[0013]

Details of the constitution shown in FIG. 2 will be described later. The player 1, as a main component of the processing route through which digital content flows, at least has a common key encryption/decryption circuit 24 for decrypting encrypted digital content by use of a content key, a decompressing circuit 26 serving as decompressing means for decompressing compressed digital content, and a D/A converting circuit 27 for converting digital data into an analog signal. It should be noted that the term decryption as used hereinbelow refers to undoing encryption.

[0014]

This player 1, as a main component for handling proprietary information and information indicating the usage status of digital content to be used (these pieces of information are hereafter referred to as point usage information) and data on an amount of money that must be held to use the digital content, namely billing data to

be decremented every time the digital content is used (hereafter referred to as point information), has at least a point usage information storage memory 29 for storing the point usage information and a point information storage memory 28 for storing the point information.

[0015]

Further, the player 1 has a common key storage memory 22 and a communication key storage memory 21 as a constitution for storing various keys to be used for encryption and decryption to be described later and a common key encryption/decryption circuit 24 and a public-key encryption/decryption circuit 20 as a constitution for performing encryption and decryption by use of the keys stored in these memories. Still further, the player 1 has, as a constitution associated with the above-mentioned encryption and decryption, a security ID generating circuit 19 for generating random numbers to generate a security ID in operative association with a host computer of a system administration company 210, a timer 18, and a hash function circuit 25 for generating a so-called hash value to be described later.

[0016]

In addition, the player 1 has a controller 16 serving as control means for controlling, based on a program stored in a ROM 17, the digital content, various data, and components, and a battery 5 as operating power for the system when used in portable state.

[0017]

Herein, it is desirable, in terms of security, that the components of the player 1 shown in FIG. 2 be configured of a single chip of IC (Integrated Circuit) or LSI (Large Scale Integration). The components shown in FIG. 2 are all mounted on an integrated circuit 10. The player 1 has three terminals (an analog output terminal 2, a PC interface terminal 3, and a recording medium I/O terminal 4) as interfaces with the outside. These terminals are connected to terminals 13, 12, and 11 of the integrated circuit 10 respectively. It should be noted that these terminals may be integrated or may be provided as additional separate terminals.

[0018]

The system administration company 210 is composed of an administration center 211 that administers the overall system and a store 212 for selling the player 1, transfers information associated with the supply of digital content to be described later with the user terminal 50 of the user 200 through a virtual store 230, manipulates digital content that compresses and encrypts content owned by a content provider 240, supplies the encrypted digital content, and transfers information with a financial organization 220. Furthermore, information such as the bank account number, credit card number, name, contact address, and the like for the user 200 is confirmed and

exchanged between the system administration company 210 and the financial organization 220 to determine whether or not a transaction is possible with the user 200. Processing such as the actual paying of fees and like is performed between the finance organization 220 and the user 200. It should be noted that the store 212 is not necessarily included in the system administration company 210, and the store may be an outside agent.

[0019]

The administration center 211 of the system administration company 210 has a constitution as shown in FIG. 3, for example. Details of the constitution shown in FIG. 3 will be described later. The administration center 211 at least has, as main components, a content administration function block 100 having functions for controlling digital content, displaying the digital content, performing manipulation processing such as encryption, compression, and the like, and generating a content key and ID which are key information for use in the encryption and decryption; a user administration function block 110 having functions for control of user information, encryption and decryption of a communication statement (including a message, point information, and the like), generating a confirmation message and a security ID, exchanging settlement information with the financial organization 230, generating points, and the like, and provided with a user subscription processing function 118 for processing user subscriptions and the like; a usage information administration function block 120 for controlling point usage information and the like; and an administration function block 130 for controlling the entire system and having a communication function.

[0020]

The following describes an example of the method described above of actually operating the system constituted as shown in FIG. 1, with reference to FIGS. 4 through 7. It should be noted that the operation method below is a procedure to be actually followed by the user 200, the system administration company 210, the financial organization 220, the content provider 240, and the like.

[0021]

The description of the method of operating the system will be made in the order, starting with a procedure of purchasing the player 1, followed by a procedure of operations from searching for digital content to installing the digital content into a storage medium of the player 1, a procedure of purchasing billing point information for making the digital content available and, if the digital content has been used, settling the fee for the usage, and finally a procedure of distributing fees collected from the user for the viewed digital content.

[0022]

In the procedure of purchasing the player 1, the user 200 purchases the player 1 from the store 212 by actually going to the store, by mail order, or the like, as shown in (1) and (5) of FIG. 4.

[0023]

As shown in (2) of FIG. 4, the store 212 registers into the administration center 211 of the system administration company 210 personal information (name, contact information, and the like) and settlement information (bank account number, credit number, and the like) obtained from the user 200 and the player-unique number of the player 1 (including the player-unique key and the like) at the purchase of the player 1.

[0024]

The administration center 211 confirms the bank account number, credit card number, and the like provided by the user 200 with the financial organization 220 as shown in (3) of FIG. 4, and obtains information from the financial organization 220 as to the possibility of a transaction as shown in (4) of FIG.4.

[0025]

Subsequently, in the procedure of operations from searching for digital content through installing the obtained digital content into the recording medium of the player 1, the user 200 who purchased the player 1 performs search, selection, editing, and order of a desired digital content by use of the user terminal 50 having the interface means for interfacing with the player 1 as shown in (1) of FIG. 5. The processing operations during this time from search through order are performed in relation to the virtual store 230 connected through a network, for example by use of search software stored in the user terminal 50 as application software.

[0026]

The virtual store 230 denotes a store that the administration center 211 virtually installs on the network, for example. In this virtual store 230, for example, information indicative of a plurality of contents are exhibited. Based on this information provided by the virtual store 230, the user 200 orders a desired content. The information indicative of the contents exhibited in the virtual store 230 includes, if the content is video data of a movie for example, the title, advertisement, or one scene of the movie, and the like, for example. If the content is audio data, the information includes the title, the name of the artist, or first several phrases (so-called intro) of the music, for example. Therefore, when the user terminal 50 of the user 200 accesses the virtual store 230, the plurality of contents of the virtual store 230 are virtually displayed on the user terminal 50, and the user 200 selects a desired one from the exhibited contents to place an order.

[0027]

When digital content is ordered from the user terminal 50 of the user 200, the virtual store 230 sends a request to the administration center 211 for supplying the ordered content as shown in (2) of FIG. 5.

[0028]

The administration center 211 that receives the request for supplying the digital content sends a request to the content provider 240 for distributing the requested content. In this manner, the content provider 240 distributes the requested digital content to the administration center 211 as shown in (4) of FIG. 5.

[0029]

The administration center 211 encrypts and compresses digital content distributed by the content provider 240 according to a predetermined compressing scheme and attaches, to this encrypted and compressed digital content, the ID of this content (the content ID), proprietor information such as copyright holder or the like for the content, the amount of fee to be billed when this content is used, the name of the virtual store that supplies this content to the user 200, and the like. It should be noted that the fee to be billed for the content is determined by the content provider 240 in advance.

[0030]

The content manipulated at the administration center 211 is transmitted to the virtual store 230 as shown in (5) of FIG. 5 and further supplied from the virtual store 230 to the user terminal 50 of the user 200 as shown in (6) of FIG. 5. In this manner, the desired content is supplied from the user terminal 50 to the player 1 and these contents are stored within that player 1.

[0031]

Note that the process flow shown in (2) through (5) of FIG. 5 can also be performed in advance. Namely, the virtual store 230 may not only exhibit information showing details of the plurality of contents but may also be made to prepare in advance the manipulated digital content corresponding to this display.

[0032]

Subsequently, in the above-mentioned procedure of purchasing billing point information for making available the digital content installed in the player 1 and of settling the fee if this digital content is used, the user terminal 50 confirms the shortage of the point information stored in the player 1 and sends a request from that user terminal 50 for replenishment of the point information.

[0033]

At this moment, as shown in (1) of FIG. 6, a request for replenishing the point information encrypted by the player 1 is transferred from the user terminal 50 to the administration center 211. At the same time, information about a proprietor,

such as a copyright holder or the like, corresponding to digital content that has already been used, that is point usage information, is read out from the player 1, encrypted, and transmitted to the administration center 211 through the user terminal 50. Thus, the point usage information is transferred concurrently with the point information replenishment request, thereby saving the user 200 from accessing the administration center 211 only to transmit the point usage information to the administration center 211. Of course, the point usage information need not be transferred concurrently with purchasing of the point information, and the point usage information may be transferred independently.

[0034]

The administration center 211 receiving the encrypted point information replenishment request and point usage information decrypts the cryptograph to recognize the point information replenishment quantity requested by the user 200 and the contents of the point usage information. Further, the administration center 211 confirms with the financial organization 220 to see if the point replenishment can be settled or not as shown in (2) of FIG. 6. The financial organization 220 checks the account of the user 200, and if settlement is permissible, a settlement OK instruction is sent from the financial organization 220 to the administration center 211 as shown in (3) of FIG. 6.

[0035]

Moreover, at the same time, the administration center 211 notifies the content provider 240 of a point usage count, namely an amount of money, to be paid to the proprietor such as the copyright holder or the like as shown in (4) of FIG. 6.

[0036]

Thereafter, the administration center 211 encrypts a point replenishment information directive, and transmits this directive together with a security ID to the user terminal 50 as point replenishment instruction information as shown in (5) of FIG. 6. The point replenishment instruction information sent from the user terminal 50 to the player 1 is decrypted within that player 1. After the security ID is confirmed, the point information to be stored in the point information storage memory 28 is replenished and the notified proprietary information such as the copyright information and the like is deleted from the point usage information storage memory 29

[0037]

Subsequently, in the procedure of distributing the fee billed for viewing digital content, namely the fee to be drawn from the user account according to the point usage information, the financial organization 220 sends a request to the user 200 for sending the fee as shown in (1) of FIG. 7. At this moment, if there is an enough balance on the account of the user 200, the financial organization does not specially

ask the user to send the fee. On the other hand, if there is not enough balance, the user 200 sends the fee to the financial organization 220 as shown in (2) of FIG. 7.
[0038]

The financial organization 220 subtracts a predetermined commission from the fee received from the user 200 and then sends the money to the administration center 211 as shown in (3) of FIG. 7. Namely, the administration center 211 collects the content manipulation fee, finance charge, system administration fee, and the like from the amount of money received from the financial organization 220. Moreover, the administration center 211 pays the copyright fee according to the point used to the content provider 240 as shown in (4) of FIG. 7 and a store commission to the virtual store 230 as shown in (5) of FIG. 7. The content provider 240 receiving the copyright fee pays the copyright fee to each copyright holder. The virtual store 230 receiving the store commission pays the commission per virtual store to each virtual store.
[0039]

As described, the fee paid by the user 200 is divided into the copyright fee, the store commission, the content manipulation commission, the settlement commission, and the system administration commission based on the point usage information. The copyright fee is paid to the content provider 240. The store commission is paid to the virtual store 230. The content manipulation commission is paid to the system administration company 210. The settlement commission is paid to the system administration company and the financial organization 220. The system administration commission is paid to the system administration company 210.
[0040]

It should be noted here that, in transferring data between the system of this embodiment, namely between the administration center 211 and the player 1, the data to be transferred is encrypted and decrypted to ensure the security of data communication. The preferred embodiment of the present invention is compatible with either a common key encryption system or a public-key encryption system.
[0041]

From the standpoint of processing speed, a common key encryption method is used in the preferred embodiment of the present invention as the encryption method when transferring the digital content, the point usage information, point information, messages, security IDs, and various other types of information. Different common keys are required for encryption and decryption of these various pieces of information. In the player 1 of FIG. 2, the common keys to be used for decryption of encrypted information received from the administration center 211 are stored in the common key storage memory 22. The common key encryption/decryption circuit 24 decrypts the

encrypted information received from the administration center 211 by use of the common keys stored in this common key storage memory 22.

[0042]

On the other hand, as method of encryption when transmitting the common keys to be used for encryption and decryption of the various pieces of information, the encryption to be used varies depending on which type of encryption a player-unique key that is a unique key for the player 1 corresponds to. Namely, if the player-unique key corresponds to common key encryption, the common keys are encrypted by use of the player-unique key and the encrypted common keys are decrypted by use of the player-unique key. In contrast, if the player-unique key corresponds to public-key encryption, the common keys are encrypted by the public key of the other party and the encrypted common keys are decrypted by the secret key of the decrypting party.

[0043]

For example, when the common key (for example, a session key to be described later) is transmitted from the player 1 to the administration center 211, if the player-unique key corresponds to common key encryption, the common key encryption/decryption circuit 24 in the player 1 encrypts the common key by use of the player-unique key stored in the communication key storage memory 21. The administration center 211 decrypts the encrypted common key by use of the player-unique key stored in the administration center 211. Likewise, in transmission of the common key from the player 1 to the administration center 211, if the player-unique key corresponds to public-key encryption, for example, the public-key encryption/decryption circuit 20 encrypts the common key by use of the public key of the administration center 211 stored in the communication key storage memory 21 in the player 1. The administration center 211 decrypts the encrypted common key by use of the secret key stored in the administration center 211.

[0044]

Conversely, in transmission of the common key (for example, a content key) from the administration center 211 to the player 1, if the player-unique key corresponds to common key encryption, the common key is encrypted by use of the player-unique key stored in the administration center 211. In the player 1, the common key encryption/decryption circuit 24 decrypts the encrypted common key by use of the player-unique key stored in the communication key storage memory 21. Likewise, in transmission of the common key from the administration center 211 to the player 1, if the player-unique key corresponds to public-key encryption, for example, the common key is encrypted by use of the public key of player 1 stored in the administration center 211 and the public-key encryption/decryption circuit 20

decrypts the encrypted common key by use of the player-unique key stored in the communication key storage memory 21 in the player 1, that is, the secret key.
[0045]

The encryption method of the player-unique key itself as mentioned above is determined by whether sending (from the system administration company 210 to the player 1) of that player-unique key is easy or not. Namely, because common key encryption is more advantageous in cost, if sending of the player-unique key is easy, common key encryption is used, however, if sending of the player-unique key is difficult, public-key encryption is used although higher in cost. When implementing the player-unique key in hardware, common key encryption is used. When implementing the player-unique key in software, public-key encryption is used.
[0046]

An example in which the public-key encryption method is used in the preferred embodiment of the present invention will be given and described below taking into account compatibility in a case where the player-unique key itself is to be implemented in software as the encryption method. Namely, in transmission of the common key between the administration center 211 and the player 1, if the common key (the session key) is encrypted by the player 1, the encryption is performed by use of the public key of the administration center 211. The administration center 211 decrypts the encrypted common key by use of the player-unique key (namely the secret key). Conversely, if the common key (content key) is encrypted by the administration center 211, the encryption is performed by use of the public key of the player and the player 1 decrypts the encrypted common key by use of the player-unique key (namely the secret key).
[0047]

The following describes sequentially the actual operations of the player 1, the user terminal 50, and the administration center 211 that constitute a system operated by use of the above-mentioned procedures and encryption method.
[0048]

First, a processing flow in the player 1, the user terminal 50, and the administration center 10 at point replenishing or point purchasing will be described, using FIGS. 8 through 11, with reference to FIGS. 2 and 3.
[0049]

FIG. 8 shows a processing flow in the player 1 at point purchasing.
[0050]

Referring to FIG. 8, software installed in the user terminal 50, or a personal computer, for point purchasing is started in step ST1, during which the controller 16 of the player 1 waits until the software for point purchasing starts up.

[0051]

When the software for point purchasing gets started, the controller 16 of the player 1 receives from the user terminal 50 the information inputted in the user terminal 50 in step ST2. The information inputted in the user terminal 50 is what the user operating the user terminal 50 is required by the user terminal 50 to input according to the software for point purchasing described above. For example, this information includes a password, information about a point information count to be purchased, and the like.

[0052]

The information from the user terminal 50 is received by the controller 16 through the PC interface terminal 3 of the player 1 and the terminal 12 of the integrated circuit 10 mounted on one chip in the player 1. The controller 16 receiving the information from the user terminal 50 compares a password stored in the password storage memory 14 in the integrated circuit 10 of the player 1 with a password contained in the received information in step ST3 to confirm whether the received password is valid.

[0053]

If the received password is found valid, the controller 16 generates information indicating intention to purchase a point (intention of point purchasing), information about the point to be purchased, and other information in step ST4. At the same time, the controller 16 causes the security ID generating circuit 19 to generate a security ID and, in step ST5, causes the common key encryption/decryption circuit 24 to encrypt these pieces of information. In the next step ST6, the controller 16 reads the user ID from the user ID storage memory 23, adds the user ID to the encrypted information, and, in step ST7, transfers the resultant data to the user terminal 50 through the terminal 12 and the PC interface terminal 3. This generated data is then sent from the user terminal 50 to the administration center 211.

[0054]

At this time, because common key encryption is used for encryption of the generated data as described above, the common key is generated before the generated data is transmitted. Therefore, the controller 16 causes the security ID generating circuit 19, which is a random number generating means, for example, to generate a session key. Moreover, this common key (the session key) is sent from the player 1 to the administration center 211 before the transmission of the generated data. Because the common key is encrypted by public-key encryption as described above, the controller 16 sends the session key, which is the common key, to the public-key encryption/decryption circuit 20 and, at the same time, takes the public key of the

administration center 211, which is stored in advance in the communication key storage memory 21, and sends this public key to the public-key encryption/decryption circuit 20. Consequently, the public-key encryption/decryption circuit 20 encrypts the common key (the session key) by use of the public key of the administration center 211. The session key thus encrypted is sent to the administration center 211 along with the user ID before the transmission of the generated data.

[0055]

It should be noted that, as described above, if the point usage information is transferred concurrently with the request for point information, the controller 16 reads the point usage information including the proprietor information and the like from the point usage information storage memory 29 and causes the common key encryption/decryption circuit 26 to encrypt the point usage information. The encrypted point usage information is transmitted along with the generated data. The balance of the point information may also be transferred in the same manner concurrently with the transfer of the point usage information.

[0056]

Thereafter, in step ST8, the controller 16 receives the encrypted data coming from the administration center 211 through the user terminal 50. This data sent from the administration center 211 is data obtained by first encrypting the point information corresponding to the point information count to be purchased that is transferred from the player 1 and information including the security ID, and the like, by use of the same common key as the session key.

[0057]

When the data is received from the administration center 211, the controller 16 sends the received data to the common key encryption/decryption circuit 24 in step ST9 and, at the same time, reads the common key generated in advance and stored in the common key storage memory 22 and sends this common key to the common key encryption/decryption circuit 24. The common key encryption/decryption circuit 24 decrypts the encrypted data coming from the administration center 211 by use of the common key.

[0058]

Subsequently, in step ST10, the controller 16 confirms the security ID of the decrypted data by comparing the same with the security ID coming from the security ID generating circuit 19. Then after the confirmation, in step ST11, the controller 16 updates the point information stored in the point information storage memory 28 with the newly sent point information.

[0059]

When the processing for updating the point information and the like has been

completed, the controller 16, in step ST12, generates a processing completion sign, sends the sign to the common key encryption/decryption circuit 24 along with the common key read from the common key storage memory 22, and causes the common key encryption/decryption circuit 24 to encrypt the sign. Thereafter, in step ST13, the controller 16 transfers the processing completion sign that has been encrypted to the user terminal 50 through the terminals 12 and 3, and the sign is sent to the administration center 211.

[0060]

Thus, the processing flow in the player 1 for point purchasing is completed.

[0061]

The following describes a processing flow in the user terminal 50 for point purchasing with reference to FIG. 9.

[0062]

As shown in FIG. 9, the user terminal 50 starts up the software for point purchasing in step ST21. When the software for point purchasing starts up, the user terminal 50 sends a request to the user operating this user terminal 50 to input the password and the information such as a point count to be purchased and the like according to the software for point purchasing in step ST22. When these pieces of information have been inputted by the user, the inputted information is transferred to the player 1 as with step ST2 shown in FIG. 8.

[0063]

Thereafter, in step ST23, the user terminal 50 receives the data generated as shown in step ST7 shown in FIG. 8 from the player 1. In step ST24, the data transferred from the player 1 is sent to the address registered in advance, namely the administration center 211.

[0064]

The user terminal 50, after transferring the data, waits for a return from the administration center 211. When the data is returned from the administration center 211, the data returned from the administration center 211 is transferred to the player 1 without change in step ST25.

[0065]

In step ST26, when the user terminal 50 receives the processing completion sign from the player 1 as with step ST13 of FIG. 8, the processing completion sign is displayed on the display device in step ST27 to notify the user of completion of the processing such as point purchasing and the like.

[0066]

Thereafter, the user terminal 50 sends the cryptograph of the processing completion sign sent from the player 1 to the administration center 211.

[0067]

Thus, the processing flow in the user terminal 50 when purchasing a point is completed.

[0068]

The following describes a processing flow in the administration center 211 when point purchasing with reference to FIG. 10.

[0069]

As shown in FIG. 10, the administration center 211 receives the encrypted data from the player 1 transferred through the user terminal 50, as shown in step ST7 of FIG. 8 and in step ST24 of FIG. 9, through a communication function 133 of the administration function block 130 controlled by the control function 131 as shown in step ST31. The user administration function block 110 of the administration center 211 receiving this data obtains the common key from a database 112 and the security ID from a security ID generating function 116 based on the user ID attached to the received data under the control of a control function 111, as indicated by step ST32.

[0070]

Note that the common key at this moment is a session key sent from the player 1 in advance. This session key was encrypted by public-key encryption as described above. Therefore, at decryption of this encrypted session key, the user administration function block 110 of the administration center 211 takes out the secret key of public-key encryption of the administration center 211 and sends this secret key and the encrypted session key to a communication statement encryption/decryption function 114. The communication statement encryption/decryption function 114 decrypts the encrypted session key by use of the public key of the administration center 211. The session key (the common key) thus obtained is stored in the database 112.

[0071]

When the common key corresponding to the user ID is obtained from the database 112 and the security ID is obtained from the security ID generating function 116, as shown in step ST33, the communication statement encryption/decryption function 114 of the user administration function block 110 in the administration center 211 decrypts the encrypted data from the player 1 by use of the common key. Further, the control function 111 compares the security ID attached to the decrypted data with the security ID read from the security ID generating function 116 to confirm whether the user 200 (the player 1) that made the access is an authorized user or not.

[0072]

The administration center 211, upon confirming that the accessing party is authorized, causes a point generating function 113 of the user administration function

block 110 to issue point information, as indicated in step ST34, according to the data sent from the user terminal 50 and causes a settlement billing function 117 to prepare billing for the settlement organization (the financial organization 220) of the user.
[0073]

Furthermore, as in step ST35, the administration center 211 causes the control function block 111, for example, to confirm that here is no illegality in the balance of the point information and the point usage information sent from the player 1 and reorganizes the information for later processing. Namely, it is confirmed from the balance of the point information and the actually used point information count that there is no illegal use, and the information is reorganized. It should be noted that the confirmation and reorganization need not always be performed, however, these are preferably performed.
[0074]

After the processing of step ST35, the user administration function block 110 of the administration center 211, as indicated by step ST36, causes the security ID generating function 115 to compute a new security ID for the player 1 (the user) based on random number generation, for example, and causes the control function 110 to encrypt the security ID along with the point information. The encryption at this time is also performed by use of the session key (the common key) sent from the player 1 in advance.
[0075]

When the encryption has been completed, the communication function 133 of the administration function block 130 in the administration center 211 sends the decrypted data to the player 1 through the user terminal 50 under the control of the control function 131 as indicated by step ST25 of FIG. 9 and step ST8 of FIG. 8.
[0076]

Thereafter, as indicated by step ST38, the communication function 133 of the administration center 211 receives the processing completion sign from the user terminal 50 shown in step ST28 of FIG. 9 and decrypts the received sign. In step ST39, the settlement billing function 117 of the user administration function block 110 in the administration center 211 sends a request to the financial organization 220 for settlement according to the decrypted processing completion sign. The settlement request to the financial organization 220 is issued from the communication function 132 of the administration function block 130.
[0077]

Thus, the processing flow in the administration center 211 for point purchasing is completed.
[0078]

The sequence of information transfer between the player 1, the user terminal 50, and the administration center 211 in the processing flow shown in FIGS. 8 through 10 can be represented as shown in FIG. 11.

[0079]

Namely, as shown in FIG. 11, in an input information transfer operation T1, the input information such as the password and the point count is transferred from the user terminal 50 to the player 1 as shown in step ST2 of FIG. 8 and step ST22 of FIG. 9.

[0080]

In a generated data transfer operation T2, the data generated by the player 1 is transferred from the player 1 to the user terminal 50 as shown in step ST7 of FIG. 8 and step ST23 of FIG. 9. Moreover, in a data transfer operation T3, the data generated by the player 1 is transferred from the user terminal 50 to the administration center 211 as shown in step ST24 of FIG. 9 and step ST31 of FIG. 10.

[0081]

In a data transfer operation T4, the data encrypted by the administration center 211 is transferred from the administration center 211 to the user terminal 50 as shown in step ST37 of FIG. 10 and step ST25 of FIG. 9. In a transfer operation T5, the data coming from the administration center 211 is transferred by the user terminal 50 to the player 1 without change as shown in step ST25 of FIG. 9 and step ST8 of FIG. 8.

[0082]

In a processing completion sign transfer operation T6, the processing completion sign is transferred from the player 1 to the user terminal 50 as shown in step ST13 of FIG. 8 and step ST26 of FIG. 9. Further, in a processing completion sign cryptograph transfer, the encrypted processing completion sign is transferred from the player 1 to the administration center 211 as shown in step ST28 of FIG. 9 and step ST38 of FIG. 10.

[0083]

The following describes a processing flow in the player 1, the user terminal 50, and the administration center 211 when obtaining the above-mentioned digital content, using FIGS. 12 through 15, with reference to FIGS. 2 and 3 .

[0084]

FIG. 12 shows a processing flow in the player 1 when obtaining digital content.

[0085]

As shown in FIG. 12 the controller 16, as in step ST41, waits until the software for obtaining digital content installed on the user terminal 50, or the personal

computer, has started up.

[0086]

When the software for obtaining digital content is started, the controller 16 receives data including digital content from the administration center 211 through the user terminal 50, as in step ST42. The data to be received at this time from the user terminal 50 through the terminal 3 and 12 has at least the digital content encrypted by the content key (a specific common key for each specific content) and the content ID corresponding to the digital content. Therefore, use of this encrypted digital content requires that the content key be obtained from the administration center 211. A method of obtaining the content key will be described later.

[0087]

The controller 16, upon receiving the data from the user terminal 50, stores this data, namely the encrypted digital content, into a storage medium connected to the storage medium I/O terminal 4 through the terminal 11 of the integrated circuit 10. It should be noted that this storage medium may be a rewritable optical disk, a semiconductor memory device, or the like, and preferably, this storage medium is a device allowing random access.

[0088]

Thus, the processing flow in the player 1 for obtaining digital content is completed.

[0089]

The following describes a processing flow in the user terminal 50 for obtaining digital content with reference to FIG. 13.

[0090]

As shown in FIG. 13, in step ST51, the user terminal 50 starts up the software for obtaining digital content. When this software is started up, the user terminal 50 accesses, in step S52, the administration center 211 having a registered address according to the software for obtaining digital content.

[0091]

At this moment, the administration center 211 is displaying a plurality of digital contents by use of the virtual store 230. In step ST53, the user selects a desired digital content through the user terminal 50 from among the plurality of digital contents displayed in the virtual store 230. Namely, as in step ST54, the user terminal 50 sends content specification information for specifying a desired digital content from among the digital content displayed in the virtual store 230 to the administration center 211.

[0092]

In step ST55, when the data returned from the administration center 211

according to the above-mentioned content specification information, namely the data composed of the encrypted digital content and the content ID, is received, the user terminal 50 temporarily stores the received data in an internal storage means such as hard disk, memory device, or the like, as in step ST56.

[0093]

Thereafter, the user terminal 50 transfers the stored data (the encrypted digital content and the content ID) to the player 1 as shown in step ST42 of FIG. 12.

[0094]

Thus, the processing flow in the user terminal 50 for obtaining digital content is completed.

[0095]

The following describes a processing flow in the administration center 211 for obtaining digital content with reference to FIG. 14.

[0096]

At this point, the administration center 211 shown in FIG. 3 is displaying a plurality of contents in the virtual store 230 described above. To be more specific, the virtual store 230 is generated in the content administration function block 100 of the administration center 211. The plurality of digital contents are displayed in the generated virtual store 230.

[0097]

In a situation in which digital content is on display in a virtual store 230 like this, as in step ST61 of FIG. 14, content specification information is received from the user terminal 50 in accordance with step ST54 of FIG. 13.

[0098]

When the content specification information is received from the user terminal 50, the control function 101 of the content administration function block 100 sends the received content specification information to the administration function block 130. The control function 131 of the administration function block 130 transfers the content specification information received from the control administration function block 100 [sic] to the content provider 240 through the communication function 134 for the proprietor. Thus, the digital content requested by the content specification information comes from this content provider 240. The digital content obtained from the content provider 240 is then transferred from the administration function block 130 to the content administration function block 100 to be inputted in this content encryption and compressing function 104. At this moment, the control function 101 sends the content key generated by the content key and ID generating function 103 and stored in the database 102 to the content encryption and compressing function 104. The content encryption and compressing function 104 encrypts the

digital content by use of the content key and compression processes the encrypted digital content in a predetermined manner. The control function 101 attaches the content ID taken from the database 102 to the encrypted and compression processed digital content and sends the result to the administration function block 130. It should be noted that, if the digital content is an audio signal, ATRAC (Adaptive TRansform Acoustic Coding), for example, is used for compression processing of the digital content. ATRAC is a technology for use in compressing data stored in a recently available storage medium called MD (Mini Disc, trademark). ATRAC considers the human auditory characteristic to compression process audio data highly efficiently.

[0099]

Thereafter, as shown in step ST62 of FIG. 14, the control block 131 of the administration function block 130 transmits the encrypted and compression processed digital content to which a content ID has been attached to the user terminal 50 through the communication function 133 interfacing with the user terminal.

[0100]

This completes the processing flow in the administration center 211 for obtaining digital content.

[0101]

The sequence of transferring information between the player 1, user terminal 50, and the administration center 211 in the processing flow shown in FIGS. 12 through 14 can be represented as shown in FIG. 15.

[0102]

Namely, in FIG. 15, in an input information transfer operation T11, as in step ST54 of FIG. 13, the content specification information is transferred from the user terminal 50 to the administration center 211. In a content transfer operation T12, the encrypted digital content and the content ID are transferred from the administration center 211 to the user terminal 50, as in step ST62 of FIG. 14.

[0103]

In a content transfer operation T13, the content ID and the encrypted digital content once stored in the user terminal 50 are transferred to the player 1, as in step ST57 of FIG. 13 and step ST42 of FIG. 12.

[0104]

The following describes a processing flow in the player 1, the user terminal 50, and the administration center 211 for obtaining a content key necessary for using the above-mentioned digital content and a use condition of the content key, using FIGS. 16 through 19, with reference to FIGS. 2 and 3.

[0105]

FIG. 16 shows a processing flow in the player 1 for obtaining the content key and the use condition.

[0106]

In step ST71 of FIG. 16, the controller 16 of the player 1 waits for the software installed in advance on the user terminal 50 for obtaining the content key and the use condition to start up.

[0107]

When the software of the user terminal 50 for obtaining the content key and the use condition has started up, information inputted in the user terminal 50 according to the software is received through the PC interface terminal 3 and the terminal 12 of the integrated circuit 10, as in step ST72. The input information supplied from the user terminal 50 is information for requesting a content key necessary for undoing the encryption of the encrypted digital content to be viewed. Note that in this example, for the content key requesting information, information for specifying the digital content that uses this content key is used.

[0108]

The controller 16 that receives the content specification information from the user terminal 50 generates the ID of the digital content specified by the content specification information and the security ID that comes from the security ID generating circuit 19 in step ST73 and causes the common key encryption/decryption circuit 24 to encrypt this generated data. Moreover, the controller 16 adds the user ID read from the user ID storage memory 23 to this generated data and sends the resultant data to the user terminal 50 through the terminal 12 and the PC interface terminal 3. This generated data is then sent from the user terminal 50 to the administration center 211.

[0109]

At this moment, because common key encryption is also used for encryption of the generated data, a common key is generated before the data is transmitted. Therefore, the controller 16 causes the security ID generating circuit 19, which is a random number generating means, for example, to generate a session key. Moreover, this common key (the session key) is sent from the player 1 to the administration center 211 before the transmission of the generated data. Because this common key is encrypted by public-key encryption as described above, the controller 16 sends the session key, which is the common key, to the public-key encryption/decryption circuit 20 and, at the same time, takes the public key of the administration center 211 from the communication key storage memory 21 to send this public key to the public-key encryption/decryption circuit 20. Consequently, the public-key encryption/decryption circuit 20 encrypts the common key (the session key) by use of

the public key of the administration center 211. Thus, the session key thus encrypted is sent to the administration center 211 before transmission of the generated data.
[0110]

Thereafter, in step ST75, the controller 16 receives the encrypted data sent from the administration center 211 through the user terminal 50 as will be described later. The data transmitted from the administration center 211 at this time is data in which the content key, use condition, security ID and the like have been encrypted as will be described later.
[0111]

When the encrypted data has been received from the administration center 211, the player 1 decrypts the encrypted data and confirms the validity of the data, as in step ST76. Namely, the controller 16 confirms the validity by comparing the security ID of the decrypted data with the security ID from the security ID generating circuit 19.
[0112]

Herein, the content key is encrypted by public-key encryption and the use condition and security ID are encrypted by common key encryption as will be described. Therefore, in order to decrypt the encrypted content key, a secret key of public-key encryption is required. In the player 1 of the present embodiment, because a player-unique key is used as the secret key as described above, the player-unique key is taken from the communication key storage memory 21. This player-unique key is sent to the public-key encryption/decryption circuit 20 along with the encrypted content key. The public-key encryption/decryption circuit 20 decrypts the encrypted content key by use of the player-unique key. The decrypted content key is stored in the common key storage memory 22. On the other hand, in order to decrypt the use condition and security ID encrypted by common key encryption, these pieces of data are sent to the common key encryption/decryption circuit 24 and the common key is read from the common key storage memory 22 to send to the common key encryption/decryption circuit 24. The common key encryption/decryption circuit 24 decrypts the use condition and security ID by use of the common key. The decrypted use condition is stored in the point usage information memory 29. It should be noted here that the decrypted content key and use condition are not taken outside the player 1, specifically, these pieces of data are not taken outside the controller 16, the common key storage memory 22, and the point usage information storage memory 29 that are mounted on the integrated circuit 10 shown in FIG. 2.
[0113]

After confirming the validity, the controller 16 stores the decrypted content

key in the common key storage memory 22 along with the content ID, as in step ST77.

[0114]

Thereafter, in step ST78, the controller 16 generates a message indicating that the content key has been obtained, sends this message to the common key encryption/decryption circuit 24, reads out the common key that was stored in advance in the common key storage memory 22, and sends this common key to the common key encryption/decryption circuit 24. The common key encryption/decryption circuit 24 encrypts the message by use of this common key.

[0115]

When the encryption of the message has been completed, the controller 16 sends the encrypted message to the user terminal 50 through the terminals 12 and 3, as in step ST79. This encrypted message is then transferred to the administration center 211.

[0116]

Thus, the processing flow in the player 1 for obtaining the content key and the use condition is completed.

[0117]

The following describes a processing flow in the user terminal 50 for obtaining a content key and a use condition with reference to FIG. 17.

[0118]

In FIG. 17, the user terminal 50 starts up the software for obtaining the content key and the use condition, in step ST81. When this software has started up, the user terminal 50 sends a request to the user operating the user terminal 50 to specify a desired content according to the software in step ST82. When the user specifies the desired content, the user terminal 50 generates the specification information. The user terminal 50 sends the content specification information to the player 1, in step ST83.

[0119]

Subsequently, in step ST84, when the data generated by the player 1 is received, as in step ST74 of FIG. 16, the user terminal 50 transfers, in step ST85, the data received from the player 1 to the administration center 211 the address of which has been registered in advance.

[0120]

The user terminal 50, after transferring the data to the administration center 211, waits for the return of data from the administration center 211, and in step ST86, when data in which the content key, use condition, security ID, and the like specified for the content key have been encrypted is returned from the administration center 211,

in step ST87, the data from the administration center 211 is transferred without change to the player 1.

[0121]

The user terminal 50, after transferring the data to the player 1, waits for the return of data from the player 1, and in step ST88, when an encrypted message to the effect that the content key has been acquired is returned from the player 1 as in step ST79 of FIG. 16, the user is notified thereof, in step ST89, by a display to the effect that the content key acquisition has been completed, which is carried out on the display device connected to the user terminal 50.

[0122]

Thereafter, the encrypted message returned from the player 1 is sent to the administration center 211 in step ST90.

[0123]

Thus, the processing flow in the user terminal 50 for obtaining the content key and the use condition is completed.

[0124]

The following describes a processing flow in the administration center 211 for obtaining a content key and a use condition with reference to FIG. 18.

[0125]

In FIG. 18, the administration center 211 communication function 133 interfacing with the user terminal, in step ST91, receives the encrypted data of the content ID, user ID, message, and security ID transmitted from the player 1 through the user terminal 50 as in step ST74 of FIG. 16 and step ST85 of FIG. 17. The received data is then sent to the user administration function block 110.

[0126]

The control function 111 of the user administration function block 110 retrieves the common key for undoing the encryption from the database 112 on the basis of the user ID attached to the received encrypted data, and decrypts this encrypted data by the communication statement encryption/decryption function 114 by use of this common key. Moreover, the control function 111 confirms the validity of the decrypted data by use of the user ID read from the database 112 and the security ID read from the security ID generating function 116.

[0127]

Note that the common key at this moment is a session key sent from the player 1 in advance. This session key was encrypted by public-key encryption as described above. Therefore, at decryption of this encrypted session key, the secret key based on public-key encryption of the administration center 211 is taken into the administration center 211, as described above. The encrypted session key is

decrypted by the communication statement encryption/decryption function 114 by use of this secret key. The session key (the common key) thus obtained is stored in the database 112.

[0128]

When the validity of the received data has been confirmed, the control function 111 sends a request to the content administration function block 100 for the content key and use condition specified by the content ID. The control function 101 of the requested content administration function block 100 reads the content key and use condition specified in the content ID from the database 102 and transfers the content key and use condition to the user administration function block 110 As shown in step ST93, the control function 111 sends the content key and use condition to the communication statement encryption/decryption function 114 along with the security ID.

[0129]

At this point, the content key is encrypted based on public-key encryption and the use condition and the security ID are encrypted based on common key encryption as described above. Therefore, at the time of encryption of the content key, the public key of the user 200 (the public key stored in advance corresponding to the player 1) is taken from the database 112 based on the user ID and this public key is sent to the communication statement encryption/decryption function 114. Using this public key, the communication statement encryption/decryption function 114 encrypts the content key. On the other hand, at the time of encryption of the use condition and the security ID, the common key (the session key) specified by the user ID is taken from the database 112 and this common key is sent to the communication statement encryption/decryption function 114. The communication statement encryption/decryption function 114 encrypts the use condition and the security ID by use of the common key.

[0130]

The encrypted content key, use condition, and security ID are sent to the administration function block 130 and then transmitted from the communication function 133 to the user terminal 50 as in step ST94. The data sent to the user terminal 50 is then sent to the player 1 through the user terminal 50 as in step ST87 of FIG. 17 and step ST75 of FIG. 16.

[0131]

Thereafter, the administration center 211 waits to receive the encrypted message generated in the player 1 and sent through the user terminal 50 as in step ST79 of FIG. 16 and step ST90 of FIG. 17. When the communication function 133 receives the encrypted message generated by the player 1 as in step ST95, the

administration center 211 decrypts the encrypted message by use of the common key, and confirms that the player 1 has obtained the content key and the use condition as in step ST96.

[0132]

Thus, the operation flow in the administration center 211 for obtaining the content key and the use condition is completed.

[0133]

The sequence of information transfer between the player 1, the user terminal 50, and the administration center 211 in the processing flow shown in FIGS. 16 through 18 is represented as shown in FIG. 19.

[0134]

Namely, referring to FIG. 19, in a content specification information transfer operation T21, the content specification information is transferred from the user terminal 50 to the player 1 as in step ST83 of FIG. 17. In a generated data transfer operation T22, the data generated by the player 1 is transferred to the user terminal 50 as in step ST74. In a generated data transfer operation T23, the data generated by the player 1 is transferred from the user terminal 50 to the administration center 211. In an encrypted data sending operation T24, the data encrypted by the administration center 211 is sent to the user terminal 50 as in step ST94 of FIG. 18. Furthermore, in an encrypted data sending operation T25, this encrypted data is sent to the player 1.

[0135]

In a message transfer operation T26, data obtained by encrypting a message indicating that the content key has been obtained is transferred from the player 1 to the user terminal 50 as in step ST79 of FIG. 16. In an encrypted data sending operation T27, the encrypted message coming from the player 1 is sent from the user terminal 50 to the administration center 211.

[0136]

The following describes a processing flow in the player 1 that has received the point information, the digital content, and the content key as described above for actually viewing the received digital content by use of the user terminal 50, using FIG. 20, with reference to FIG. 2.

[0137]

It is assumed here that the terminal 4 of the player 1 is connected to a storage medium in which the digital content is stored.

[0138]

In this state, the user terminal 50 specifies the digital content to be viewed in the player 1, as in step ST101. At this moment, this specification is made by the user operating the user terminal 50, for example.

[0139]

At this moment, as in step ST102, the controller 16 of the player 1 accesses the storage medium according to the content specification information coming from the user terminal 50 to read the ID of the content.

[0140]

The controller 16, as in step ST103, accesses the common key storage memory 22, based on the content ID read from the storage medium, to confirm whether the content key is stored and, at the same time, accesses the point usage information storage memory 29 to confirm whether the use condition is stored.

[0141]

At this point, if the content key and the use condition are not confirmed to be stored in the common key storage memory 22 and the point usage information storage memory 29 respectively, the controller 16 sends information to the user terminal 50 indicating that the content key and the like do not exist. Based on this information, a message is displayed on the display device from the user terminal 50 prompting to obtain the content key and the like. In this case, the content key and the like are obtained as shown in the flowchart of obtaining the content key as described above. Thus, if the content key and the like are newly obtained, the encrypted content key and the like are decrypted as described above in step ST104.

[0142]

Subsequently, as shown in step ST105, based on the decrypted use condition, the controller 16 confirms whether there is a sufficient balance of the point information stored in the point information storage memory 28. If the balance of the point information stored in the point information storage memory 28 is insufficient, the controller 16 sends information to the user terminal 50 indicating that the balance of the point information is insufficient. Based on this information, the user terminal 50 displays a message on the display device, prompting obtaining the point information. In this case, the point information is obtained as indicated in the flowchart of obtaining the point information as described above.

[0143]

At this point, when actually viewing the digital content, the controller 16 decrements the point information count from the point information storage memory 28 according to the digital content to be viewed, as in step ST106, and stores the new point usage information corresponding to the usage state of this point information into the point usage information storage memory 29 (updates the point usage information). The point usage information to be newly stored thus in the point usage information storage memory 29 includes proprietor information (copyright holder and the like) corresponding to the viewed digital content, information about the decremented point

information count, and the like.

[0144]

Thereafter, as in step ST107, the controller 16 confirms that the billing processing of decrementing the point information, newly storing the point usage information, and the like has been completed and then reads the digital content from the storage medium.

[0145]

Because the digital content read from the storage medium is encrypted, the controller 16 transfers this encrypted digital content to the common key encryption/decryption circuit 24, as in step ST109.

[0146]

Based on the instruction given by the controller 16, as in step ST110, the common key encryption/decryption circuit 24 decrypts the encrypted digital content by use of the content key decrypted and stored in advance in the common key storage memory 22.

[0147]

Moreover, because this digital content is compression processed in a predetermined manner as described above, the controller 16, as in step ST111, transfers the decrypted but still compression processed digital content from the common key encryption/decryption circuit 24 to the decompressing circuit 26, and the decompression processing corresponding to the compression processing is performed there.

[0148]

Thereafter, as in step ST112, the decompressed digital content is converted by the D/A conversion circuit 27 into an analog signal. The analog signal is outputted outside (for example, to the user terminal 50) through the terminal 13 of the integrated circuit 10 and the analog output terminal 2 of the player 1, as in step ST113.

[0149]

Thus, the processing flow in the player 1 for viewing digital content is completed, allowing the user to view the digital content.

[0150]

The following describes a processing flow in the player 1, the user terminal 50, and the administration center 310 for returning the point usage information newly stored in the point usage information storage medium 29 of the player 1 to the administration center 211 at the above-mentioned digital content viewing, using FIGS. 21 through 24, with reference to FIGS. 2 and 3.

[0151]

FIG. 21 shows a processing flow in the player 1 at returning the point usage information.

[0152]

In FIG. 21, as shown in step ST121, the controller 16 waits until the software installed in advance in the user terminal 50 for returning point usage information starts up.

[0153]

When the software of the user terminal 50 for returning point usage information has started up, information inputted in the user terminal 50 according to the software is received through the PC interface terminal 3 and the terminal 12 of the integrated circuit 10, as in step ST122. The input information supplied from the user terminal 50 at this time includes a password and the like to be inputted by the user.

[0154]

In step ST123, the controller 16 that has received this content specification information from the user terminal 50 compares the password supplied from the user terminal 50 with the password stored in the password storage memory 14 to confirm whether the supplied password is valid or not.

[0155]

If the password is found valid during the password confirmation, the controller 16 reads the balance of the point information stored in the point information storage memory 28 and the point usage information stored in the point usage information storage memory 29, as in step ST124, and encrypts these pieces of information.

[0156]

When the balance of the point information and the point usage information have been encrypted, the controller 16 reads the user ID from the user ID storage memory 23 and attaches this user ID to the encrypted data, as in the step ST125.

[0157]

The data attached with the user ID is transferred from the controller 16 to the user terminal 50 through the terminal 12 and the PC interface terminal 3, as in step ST126. This data is then transferred to the administration center 211.

[0158]

It should be noted that the encryption at this time is also based on common key encryption as described above. Namely, before transmission of the data, the common key is generated as described above, this generated common key is encrypted by public-key encryption (by encryption using the public key of the administration center 211), and the encrypted common key is sent to the administration center 211 along with the user ID.

[0159]

After the data is transferred to the user terminal 50 as described above, the controller 16 waits until the data to be described later comes from the administration center 211 through the user terminal 50.

[0160]

At this point, when the data from the administration center 211 has been received, as in step ST127, the player 1 decrypts, using the common key, the received data encrypted by use of common key encryption and confirms the validity of the decrypted data, as in step ST127 [sic - step 128?]. Namely, the controller 16 confirms the validity by comparing the security ID of the decrypted data with the security ID from the security ID generating circuit 19.

[0161]

Moreover, the data transferred from the administration center 211 includes a processing completion message encrypted by use of the common key indicating. Therefore, the controller 16, after confirming the validity of the security ID, sends the encrypted processing completion message to the common key encryption/decryption circuit 24, causes this circuit to decrypt the message by use of the common key, and receives the message with decryption processing completed, thereby confirming that the processing in the administration center 211 has been completed.

[0162]

Thus, the processing flow in the player 1 for returning the point usage information is completed.

[0163]

The following describes a processing flow in the user terminal 50 for returning point usage information with reference to FIG. 22.

[0164]

In FIG. 22, the user terminal 50 starts up the software for returning point usage information, as in step ST131. When this software starts up, the user terminal 50 sends a request in step 132, according to the software, to the user of the user terminal 50 to input a password and the like. When the password is inputted by the user, that password is transferred to the player 1.

[0165]

Subsequently, in step ST133, when the data generated by the player 1 is received, as in step ST126 of FIG. 21, the user terminal 50 transfers, in step ST134, the data received from the player 1 to the administration center 211 the address of which has been registered in advance.

[0166]

The user terminal 50, after transferring the data to the administration center

211, waits for return from the administration center 211. When the data sent from the administration center 211 to the player 1 is received, that data is transferred to the player 1 directly in step ST135.

[0167]

The user terminal 50, after transferring the data to the player 1, displays a processing completion message to the user on the display device and receives confirmation from the user.

[0168]

Thus, the processing flow in the user terminal 50 for returning the point usage information is completed.

[0169]

The following describes a processing flow in the administration center 211 for returning point usage information with reference to FIG. 23.

[0170]

As in step ST141, the communication function 133 of the administration center 211 interfacing the user terminal receives the data including point usage information and the like from the player 1 through the user terminal 50 in step ST126 of FIG. 21 and step ST134 of FIG. 22.

[0171]

When this data is received, as in step ST142, the user administration function block 110 of the administration center 211 obtains, from the database 112, the common key received and stored in advance, as well as the security ID based on the user ID attached to the received data under the control of the control function 111.

[0172]

When the common key and the security ID corresponding to the user ID have been obtained from the database 112, as shown in step ST143, the data including the encrypted point usage information coming from the player 1 is decrypted in the communication statement encryption/decryption function 114 of the user administration function block 110 in the administration center 211 by use of the common key. Further, in the control function 111, the security ID in the decrypted data is compared with the security ID read from the database 112 to confirm whether the accessing user 200 (the player 1) is valid or not.

[0173]

After the validity and data contents have been confirmed, the data is transferred to the usage information administration function block 120. A control function 121 of the usage information administration function block 120, as shown in step ST144, uses the point information balance and point usage information sent from the player 1 to confirm whether use by the user 200 is illegal or not using the

information stored in the database 122. At the same time, an operation for summarizing the point information balance and point usage information is carried out in a usage information operation function 123 when it has been confirmed that no illegality is involved.

[0174]

Thereafter, as shown in step ST145, the control function 111 of the user administration function block 110 controls the security ID generating function 116 to compute the security ID, and controls a confirmation message generating function 115 to generate a processing completion message. The security ID and the processing completion message are encrypted by the communication statement encryption/decryption function 114 of the user administration function block 110 by use of the common key.

[0175]

As shown in step ST146, the generated encrypted data is sent from the communication function 133 to the user terminal 50 and then sent from the user terminal 50 to the player 1, as in step ST135 of FIG. 22 and step ST127 of FIG. 21.

[0176]

Thus, the processing flow in the administration center 211 for returning the point usage information is completed.

[0177]

The sequence of information transfer between the player 1, the user terminal 50, and the administration center 211 in the processing flow of FIGS. 21 through 23 described above can be represented as shown in FIG. 24.

[0178]

Namely, in FIG. 24, in an input information transfer operation T31, input information such as the password and the like is transferred from the user terminal 50 to the player 1 as in step ST132 of FIG. 22. In a generated data transfer operation T32, the data generated by the player 1 is transferred to the user terminal 50 as in step ST126 of FIG. 21. In a generated data transfer operation T33, the data generated by the player 1 is transferred from the user terminal 50 to the administration center 211 as in step ST134 of FIG. 22. In a data transfer operation T34, the data generated by the administration center 211 is transferred to the user terminal 50 as in step ST146 of FIG. 23. In a data transfer operation T35, the data generated by the administration center 211 is transferred to the player 1 through the user terminal 50 as in step ST127 of FIG. 21.

[0179]

The actual operations of the player 1, the user terminal 50, and the administration center 211 of the system of the present embodiment flow as described

above.

[0180]

So far, the entire processing flow in the system of the present embodiment has been described. However, in the following, the operation of each main component of the system of the present embodiment will be described in detail.

[0181]

First, encryption and compressing operations and decompressing and decryption operations in the present embodiment of the invention will be described.

[0182]

When digital content is distributed using a network as in the system of the preferred embodiment described above, compression/decompression techniques are used to reduce the amount of this data, and encryption/compression techniques are used for protection against copying and/or for billing. Namely, the distributing side (in the above-mentioned example, the administration center 211) compresses and then performs encryption processing on digital content. When the digital content (encrypted and compressed data) generated by the distributing side (the administration center 211) as with the above-mentioned example is distributed through a network, the receiving side (in the above-mentioned example, the player 1) receives the encrypted and compressed digital content and then decrypts and decompresses the digital content. It should be noted that the order in which encryption and compressing are performed and the order in which decryption and decompressing are performed may be altered in some cases.

[0183]

If the digital content includes a copyright or the like, the receiving side is billed according to the intention of the holder of the copyright before decrypting and decompressing the digital content. This billing is performed mainly by purchasing the key for decryption, namely the content key, however, there are various methods by which this content key is purchased.

[0184]

Herein, if the processing procedure in which digital content is compressed and encrypted and then decrypted and decompressed as mentioned above is followed, a malicious user, for example, can obtain the decrypted and compressed data with comparative ease. That is, the capacity of the compressed data of the digital content generally is large, and therefore, for example, this compressed data is often stored in an inexpensive external memory rather than in the internal memory of an ordinary content playback device of the receiving side. For this reason, it is easy to illegally remove the compressed digital content either directly from the external memory or through the part that connects to the external memory.

[0185]

Moreover, the algorithms for decompressing the compressed data are made public in many cases. In addition, these decompressing algorithms are not ones that cannot be processed if hidden like general encryption keys. Furthermore, compared to the encrypted and compressed digital content distributed from the transmission side, the decrypted compressed digital content does not differ as far as the volume of the data, and therefore, it is easy to maliciously distribute the decrypted compressed digital content. That is, according to a system that distributes digital content that has been encrypted after being compressed, there is a serious risk of the compressed digital content, which anyone can easily decompress, being easily stolen by a user having malicious intent, and being distributed and decompressed yet again in places the copyright holders never intended.

[0186]

Therefore, in this embodiment of the present invention, in consideration of this situation, in order to allow the security of the digital content distributed through a network to be enhanced, the processing indicated by the flowchart shown in FIG. 25 is performed in the player 1 of FIG. 2.

[0187]

Namely, in the decryption processing by the common key encryption/decryption circuit 24 of the player 1 shown in FIG. 2 and the decompression processing by the decompressing circuit 26, the data of encryption and compression processed digital content read from the storage medium is first divided into units of least common multiple lcm(X,Y) of processing unit X bits of a decryption algorithm and processing unit Y bits of a decompression algorithm, as in step ST151.

[0188]

Subsequently, decryption processing is performed on the data of the encrypted and compressed digital content divided into least common multiple lcm(X,Y) units by the common key encryption/decryption circuit 24 in units of the least common multiple lcm(X,Y) as shown in step ST152.

[0189]

Regarding the digital content data compressed in units of the least common multiple lcm (X, Y) obtained by the decryption process, as shown in step ST154, decompression processing is performed by the decompressing circuit 26 for all the units of compressed data.

[0190]

Thereafter, the decryption and decompression processing in units of this least common multiple lcm(X,Y) are repeated until the processing of all data of the

encrypted and compressed digital content has been completed. Namely, as shown in step ST155, it is determined whether decryption and decompression processing in units of least common multiple lcm(X,Y) have been completed on all data of the digital content. If the decryption and decompression processing are not completed, the process returns to step ST152, while if the decryption and decompression processing have been completed, the processing shown in the flowchart comes to an end

[0191]

Thus, the digital content with all data decrypted and decompressed can be obtained.

[0192]

It should be noted that, in the processing by the player 1 shown in the flowchart of FIG. 25, the decrypted data in units of least common multiple lcm(X,Y) exists, but the data quantity of this decrypted data is small. Thus, it is possible to store the data in relatively high priced but highly secure internal memory, thereby making the likelihood of the data being stolen extremely low, as when stored in the external memory described above.

[0193]

Moreover, in the player 1 of the present embodiment, a buffer memory 25 shown in FIG. 2 is provided as an internal memory for ensuring the data security between the common key encryption/decryption circuit 24 and the decompressing circuit 26. That is, this buffer memory 25 is provided in a single-chip integrated circuit 10, and is difficult to access from the outside, thereby preventing the data from being taken out.

[0194]

In the flowchart described above, the constitution is such that decryption and decompression processing are carried out for all data in units of the least common multiple lcm (X,Y). As a specific constitution, for example as shown in FIG. 26, first, the digital content data is divided into X bits, which is the unit of processing of the decryption process algorithm, the decryption process is performed on this X-bit data, the compressed data of the decryption processed X-bits is then reorganized into Y-bit parts, which is the unit of processing of the decompression process algorithm, and decryption and decompression processing in units of the least common multiple lcm (X,Y) are realized as described above by decompressing the Y-bit compressed data.

[0195]

The common key encryption/decryption circuit 24 of the player 1 for realizing the processing is composed of an input block 30 and an

encryption/decryption block 31, and the decompressing circuit 26 is composed of a decompression block 32 and an output block 33. The buffer memory 25 is arranged between the common key encryption/decryption circuit 24 and the decompressing circuit 26.

[0196]

As a more specific example, if the encryption processing for the digital content is performed herein using DES (Data Encryption Standard) encryption for example, this encryption processing and the corresponding decryption processing are performed in units of 64 bits.

[0197]

The decompression processing for compressed digital content is currently often performed in units of 1K to 2K bits/channel, although this depends on a compression ratio and a sampling frequency thereof. It is assumed here for the sake of convenience that the decompression processing is performed in units of 1.28K bits.

[0198]

Therefore, in a system using the DES encryption method and the compression/decompression method in units of 1.28K bits, the least common multiple lcm becomes 1.28K.

[0199]

Under such conditions, the encrypted and compressed digital content is inputted in the input block 30 of the common key encryption/decryption circuit 24 of FIG. 26. In the input block 31 [sic], the encrypted and compressed digital content is divided into X bits of processing units of the algorithm of the decryption processing, namely 64 bits of data, which are then outputted to the encryption/decryption block 31.

[0200]

The encryption/decryption block 32 [sic] does decryption processing on the X-bit data, namely the 64-bit data, in units of 64 bits. The 64 bit compressed data that is obtained by this 64-bit decryption is sent to the buffer memory 25.

[0201]

According to an instruction from the controller 16, the buffer memory 25 outputs in a batch the 1.28K bits of compressed data when Y bits of processing unit of the algorithm of decompression processing, namely 1.28K bits of compressed data have been accumulated. This compressed data is sent to the decompression block 32 of the decompressing circuit 26.

[0202]

The decompressing circuit 26 decompresses the inputted 1.28K bits of compressed data and outputs this decompressed data to the output block 33.

[0203]

Moreover, the controller 16 controls the processing in the decryption block 31 and the processing in the decompression block 32 while monitoring the amount of data accumulated in the buffer memory 25

[0204]

It should be noted that, in this case, performing the decryption processing in units of 20 (=1280/64) concurrently provides a faster processing system.

[0205]

In addition, unlike the hardware constitutions as shown in FIGS. 2 and 26, if the processing is performed based on a programmable device, the controller 16 for example, performs the processing based on a decryption program or a decompression program according to the status of the buffer memory 25.

[0206]

In the description made so far, the example in which the compressed and then encrypted digital content is supplied to the player 1 and the player 1 decrypts and then decompresses this digital content was used. However, the same effect as described above can be obtained by decompressing and decrypting the encrypted and then compressed digital content.

[0207]

Moreover, the present invention is not limited to compression/decompression and encryption/decryption algorithms, and is valid for all sorts of methods.

[0208]

Thus, according to the present invention, the security of digital content transferred through a network is enhanced.

[0209]

The following describes the operation of generating the security ID.

[0210]

In the method, such as in the present embodiment, in which point information is obtained in advance and the obtained point information is decremented according to the viewing of digital content, as described above, the administration center 211 on the network receives a request for point information purchase from the user terminal 50 of the user 200, makes a desired confirmation with the financial organization 220 and others, encrypts that point information, and sends the encrypted point information to the player 1 of the user 200 through the network.

[0211]

In the method, such as in the present embodiment, in which point information is obtained in advance and the obtained point information is decremented according to the viewing of digital content, transfer of similar data (for example, encrypted

information "request for replenishment of 3,000 yen of point information" and corresponding information "3,000 yen of point information") between the administration center 211 and the player 1 (the user terminal 50) every time point information is purchased poses a problem of money replenishment based on so-called "spoofing" the financial organization 220 by a malicious person, for example. "Spoofing" the financial organization herein denotes that a malicious person disguises himself as an authentic user (the user 200 in the present embodiment) to illegally obtain point information, for example.

[0212]

Namely, if similar data is transferred every time point information is purchased, for example, a malicious person could tap that data from the communication line, generate the similar data, and send a request to the administration center 211 to send point information to that malicious person. In this case, there is a risk that the malicious person can get point information, and furthermore, that the fee for the obtained point information will be billed to the authentic user 200.

[0213]

At that point, in order to prevent such an illegal act, the system according to the present embodiment uses random numbers generated by a random number generating capability operatively associated with both the receiving side (the player 1) and the distributing side (the administration center 211) in order to increase the security. In the present embodiment, the security ID is generated as these random numbers. It should be noted that the random number generation can be operatively associated between the receiving side and the distributing side by synchronizing the operations of both side by initializing the timer 18, for example, at the user registration sequence, for example.

[0214]

Namely, an operation of obtaining point information, for example, by the player 1 from the administration center 211 by use of this random number (the security ID) is performed as follows.

[0215]

Data to be sent from the administration center 211 to the player 1 when purchasing point information includes point information encrypted by the common key (the session key) previously obtained from the player 1 and the security ID generated as described above, for example.

[0216]

The controller 16 of the player 1 sends the data received from the administration center 211 to the common key encryption/decryption circuit 24 as

described above for the decryption processing by use of the common key. Thus, the point information and the security ID sent from the administration center 211 can be obtained.

[0217]

Thereafter, the controller 16 of the player 1 compares the security ID sent from the administration center 211 with the security ID generated by the security ID generating circuit 19 of the controller 16. If a match is found between the security ID from the administration center 211 and the security ID generated by the security ID generating circuit 19 of the controller 16, the point information sent from the administration center 211 is stored in the point information storage memory 28.

[0218]

Thus, only the player 1 of the approved user 200 can obtain the point information. In other words, even if a malicious person, who has the same kind of player as the player 1 of an authorized user 200, attempts to obtain point information illegally using the spoofing, the security ID of the player possessed by the malicious person will not match the security ID sent from the administration center 211, therefore making it impossible for this person with malicious intent to illegally obtain the point information by spoofing.

[0219]

Of course, the security ID generated by the player 1 of the user 200 is generated in the security ID generating circuit 19 installed in the integrated circuit 10 of the player 1, and cannot be accessed from the outside, and therefore a malicious person cannot steal this security ID.

[0220]

Various constitutions are available that generate a random number as the security ID. One of these constitutions is shown in FIG. 27 as an example. The constitution shown in FIG. 27 is a specific example of the security ID generating circuit 19 shown in FIG. 2.

[0221]

In FIG. 27, a unidirectional function generating circuit 40 generates a so-called unidirectional function. The unidirectional function is a function that is comparatively easy to calculate, however, calculating the inverse function is far more difficult. This unidirectional function can also be received in advance by confidential communication or the like and can be stored in the unidirectional function generating circuit 40. It should be noted that the unidirectional function generating circuit 40 can also be adapted to generate the unidirectional function by use of time information from the timer 18 in the integrated circuit 10 of FIG. 2 as an input function. The unidirectional function is then sent to a random number decision

circuit 43.

[0222]

Moreover, a user constant generating circuit 41 generates a predetermined user constant specified for each user. This user constant is sent in advance by confidential communication or the like and stored in the user constant generating circuit 41. It should be noted that, for this user constant, the user ID stored in the user ID storage memory 23 can be used, for example.

[0223]

A random number database 42 stores random numbers. For example, 99 random numbers are stored.

[0224]

A communication count storage circuit 44 stores communication count information sent from the controller 16, for example. The communication count information is information indicating the number of times communication has been made between the player 1 and the administration center 211.

[0225]

The unidirectional function, user constant, and communication count information are sent to the random number decision circuit 43. The random number decision circuit 43, based on the time information received from the timer 18, for example, generates random numbers in a range (for example, 99 random numbers) stored in the random number database 42 from the unidirectional function and user constant.

[0226]

Namely, if the communication count information indicates a first communication, for example, the random number decision circuit 43 takes the 99th random number from the random number database 42. Moreover, if the communication count information indicates an nth communication, for example, the random number decision circuit 43 takes the 100-nth random number from the random number database 42. The obtained random number is then outputted as the security ID.

[0227]

The constitution of this security ID generation is the same on both the player 1 and the administration center 211.

[0228]

Note that, when the random numbers stored in the random number database 42 have all been used, 100th to 199th random numbers are newly computed in the random number decision circuit 42 [sic] or new random numbers or unidirectional functions are sent by confidential communication or the like, and these are stored in

the random number database 42 or the unidirectional functions are incorporated in the unidirectional function generating circuit 40.

[0229]

Moreover, in the above description, the security of every communication is enhanced by generating random numbers (the security ID). However, in the present embodiment, a different common key (a session key) is programmably generated every time communication is made between the user 200 and the administration center 211, thereby enhancing the security still further.

[0230]

The following describes a manner in which a random number is inserted in a send statement (for example, a message or the like) to be actually transmitted, and in which this statement is encrypted by the session key, and a manner in which the random number is taken out of the received statement to confirm the validity, with reference to FIGS. 28 and 29. It should be noted that, in the examples of FIGS. 28 and 29, a signature (namely, a digital signature) is attached to the send statement.

[0231]

In FIG. 28, first, as the flow for encrypting and transmitting the common key using public-key encryption, the session key is generated as a common key for use in communications in a communication common key generating process P7, and this common key is encrypted by the receiving side public key in a public-key encryption process P8. The encrypted common key is then sent to the receiving side.

[0232]

Meanwhile, as the flow when a message is encrypted using common key encryption and transmitted as a send statement, for example, a message M is generated in a message generating process P1, and, in addition, a random number (the security ID) is generated in a random number generating process P5. The message M and the random number are sent to common key encryption process P6. In this common key encryption process P6, the message M and the random number are encrypted by use of the common key generated in the communication common key generating process P7.

[0233]

Furthermore, if the digital signature is to be attached, the message M is sent to a hash value computing process P2. In the hash value computing process P2, a so-called hash value is computed from the message M. It should be noted that a hash value is address information obtained by a hashing method. In the hashing method, a predetermined computation is performed on one part (a keyword) of data (in this case, the message M) and the result thereof is used as an address. A hash value (M) obtained from this message is sent to secret key encryption process P4 as a digital

signature. In this secret key encryption process P4, the digital signature is encrypted by the secret key of the sending side. The encrypted digital signature is sent to common key encryption process P6. In the common key encryption process P6, the digital signature is encrypted by use of the common key generated in the communication common key generating process P7.

[0234]

The message M, digital signature, and random number are sent to the receiving side.

[0235]

The following describes a processing flow in the receiving side corresponding to FIG. 28, using FIG. 29.

[0236]

In FIG. 29, first, as the process flow for decryption of the common key by public key encryption, the common key sent from the sending side is decrypted by the secret key of the receiving side in secret key decryption process P11.

[0237]

Meanwhile, as the flow for decryption of the message M encrypted using the common key encryption method, in a common key decryption process P13, the sent message M is decrypted by the secret key decryption process P11 using the decrypted common key. This decrypted message M is sent to another process by an other function transmission process P20.

[0238]

Moreover, in the flow for decrypting a digital signature, a hash value decrypted by the common key decryption process P13 is decrypted by a public key decryption process P14 using the sending side public key. At the same time, in a hash value computing process P17, a hash value is computed from the message M. The hash value decrypted by the public key decryption process P14 and the hash value computed by the hash value computing process P17 are compared by a comparing process P19 to confirm that there has been no tampering.

[0239]

In addition, regarding the sent random numbers, a random number decrypted by the common key decryption process P13 and a random number generated by a receiving side random number generating process P21 are compared by a validity confirming process P22 to confirm that they are valid.

[0240]

Now then, in the system of the present embodiment shown in the above-mentioned FIG. 1, as the system for the user 200, a system administration company 210, a virtual store 230, and a content provider 240 are provided.

Furthermore, the financial organization 220 of FIG.1, for example, is an external bank or the like.

[0241]

The administration center 210 [sic] of the system administration company 210 performs almost all of the important system tasks, such as managing the display and distribution of the digital content in the virtual store 230, collecting, distributing, and managing user 200 billing information and various other information between the user 200 and the financial organization 220, encrypting digital content from the content provider 240, managing security for the information that is handled, and the like.

[0242]

However, in a system that uses a network to distribute digital content such as that described above, communications will become concentrated on the system side when the user is obtaining digital content from the system and when billing for the use of the digital content, raising fears that the user will not be able to obtain a satisfactory response.

[0243]

Accordingly, in another embodiment of the present invention, it is possible to prevent the concentration of communications as described above and to enhance communication response by dividing up the functions of the system administration company 210, more specifically, the functions of the administration center 211, as follows.

[0244]

That is, in another preferred embodiment of the present invention, as shown in FIG. 30, the constitution of the system for the user 200 is divided into a content display and distribution organization 310 having functions for displaying and distributing digital content, a billing information administration organization 320 having functions for managing the billing information of users in fixed regions, and a system administration organization 330 having functions for managing security for the entire system, such as generating data for the encryption of digital content and the like, distributing the generated data to the content display and distribution organization 310, collecting information from the billing information administration organization 320, and distributing revenues. Each of the organizations 310, 320, and 330 is able to communicate with the user 200 independently.

[0245]

In a constitution like that in FIG. 30, a plurality of content display and distribution organizations 310 can be dispersedly arranged over a worldwide network, making it possible for the user 200 to access a content display and distribution

organization 310 in any region as long as the communications charges are paid. For example, when the user 200 wants to obtain digital content, access is made from the user 200 to the content display and distribution organization 310 to obtain the digital content. The digital content at this time has been encrypted and the like by the system administration organization 330, that is, the digital content has been placed in a state capable of being transmitted directly to the user 200 using the network.
[0246]

Moreover, the billing information administration organization 320 handles billing information, and therefore, from the standpoint of security management, preferably should not take on too many users. Therefore, a billing information administration organization 320 is established for each of a moderate number of users. However, it is preferable that this number be optimized since the trade-off is an increase in a number of attack points (billing information administration organizations 320) for third-parties harboring malicious intent. For example, when the user 200 carries out communications related to billing, the user 200 accesses the billing information administration organization 320.
[0247]

The system administration organization 330 improves security by collectively managing information that is important from the standpoint of security, such as subscriptions to the user system, the registration of settlement methods, the collection of money from users, and the distribution of profits to the proprietors, the content display and distribution organizations 310, the billing information administration organizations 320, and other such profit recipients, and the like. However, the system administration organization 330 need not be provided in only one location in the world; rather it is preferable that it be established in certain coherent units, for example, in units such as countries or the like. For example, when the user 200 is to carry out a communication that is important from the standpoint of security, such as subscribing to this system, registering a settlement method, or the like, the user 200 does so by accessing the system administration organization 330. The collection of money from the relevant user and the distribution of profits to the profit recipients are performed collectively by the system administration organization 330, which obtains the information from the billing information administration organization 320. Furthermore, the source data, that is, the content possessed by the copyright holder and the like is supplied to the system administration organization 330, converted to encrypted digital content at this point, and distributed to the content display and distribution organization 310.
[0248]

For example, by allocating the system functions to the three organizations

310, 320, and 330, and enabling the user 200 to directly access each of the organizations 310, 320 and 330 as described above, it becomes possible to prevent the concentration of communications and to improve communication response. Furthermore, the content display and distribution organization 310 also makes it possible to deal with things that already exist, such as so-called virtual malls, and is effective for sales promotion as well, making it attractive to users. Separating the billing information administration organization 320 is beneficial for preventing fraud in collusion with content display and sales functions. Moreover, because the users being managed are held to a fixed number, administrative functions aimed at fraud are also more effective.

[0249]

The flow of information when a user subscribes to the system, purchases point information, obtains a content key for use in decrypting encrypted digital content, and the like, the flow when distributing content and information for viewing the content, and the flow of billing information according to content use in the system of another preferred embodiment of the present invention shown in FIG. 30 will be explained below.

[0250]

First, the important portions of the flow when a user subscribes to the system will be explained using FIG. 31.

[0251]

When a user subscribes to the system and is registered, the registration operation is performed by a user subscription support function block 402 of the system administration organization 330 in accordance with the following procedures.

[0252]

First of all, information indicating an intention to subscribe to the system, such as a subscription intention sending operation T41, is sent from the user 200, that is, the player 1 and user terminal 50, to the system administration organization 330 through the network. The subscription intention information, which was inputted into a communication function block 401 of the system administration organization 330, is sent to the user subscription support function block 402.

[0253]

The user subscription support function block 402, upon receiving the subscription intention information, sends file information that is required for subscription, such as a file required for subscription sending operation T42, to the user 200 through the communication function block 401.

[0254]

On the basis of the file required for subscription sent from the system

administration organization 330, the user 200 prepares a subscription application in accordance with a prescribed format. The prepared subscription application is sent to the system administration organization 330, such as in subscription application sending operation T43.

[0255]

The user subscription support function block 402, upon receiving the subscription application, sends information explaining the client function to the user 200, such as in client function sending operation T44.

[0256]

The user 200, upon receiving the client function information, sends to the system administration organization 330 user information, such as a user information sending operation T45, including, for example, the above-mentioned bank account number, credit card number, name, contact address, and the like.

[0257]

The user subscription support function block 402, upon receiving the user information that was sent, notifies the user 200 of information indicating that the subscription registration procedure has been completed, such as a registration procedure complete notification T46.

[0258]

Furthermore, after this user subscription registration procedure has been completed, the user subscription support function block 402 of the system administration organization 330 transfers the user information, such as a user information sending operation T47, to the billing information administration organization 320 through the communication function block 401. The billing information administration organization 320, which receives this user information, stores the user information in a database function block 367.

[0259]

Thus, the main flow at the time a user subscribes to the system is completed. Furthermore, the other constitutions included in FIG. 31 will be explained later.

[0260]

Hereafter, the main portions of the flow of information when purchasing point information, obtaining a key for decrypting encrypted digital content, and the like will be explained using FIG. 32. Furthermore, information on the purchase of point information and/or a content key for decrypting encrypted digital content is information needed for using content, and as such, this information will be abbreviated as use right information in the explanation that follows.

[0261]

When a user obtains important information for use in the system (as used

here, a content use right), the user 200 accesses the billing information administration organization 320, which has been assigned in advance to be in charge of each of the users 200. A use right issuing function block 362 of the billing information administration organization 320 responds to the access requesting content use right information sent from the user 200, and issues a use right in accordance with the following procedure.

[0262]

First, the user 200 sends the billing information administration organization 320 information, such as a purchase request sending operation T51, indicating a desire to purchase a use right. The information indicating that the user desires to purchase a use right is purchase request information from the user 200 conforming to a prescribed format. The purchase request information, which is inputted to a communication function block 361 of the billing information administration organization 320 through the network, is sent to a use right issuing function block 362.

[0263]

The use right issuing function block 362, upon receiving the purchase request information, generates new use right information based on the user information stored in a database function block 367, and sends the use right information to the user 200, such as a new use right sending operation T52.

[0264]

The user 200, upon confirming the receipt of the new use right, prepares a receipt confirmation in accordance with a prescribed format, and sends this receipt confirmation to the use right issuing function block 362 of the billing information administration organization 320, such as a receipt confirmation sending operation T53.

[0265]

Thus, the main flow at the time of use right purchase is completed. Furthermore, the other constitutions included in FIG. 32 will be explained later.

[0266]

Hereafter, the main portions of the flow when distributing content and information for viewing the content (as used here, a use condition and a content key) will be explained using FIG. 33.

[0267]

First, a content obtaining function block 342 of the content display and distribution organization 310 sends a bill to the system administration organization 330 for digital content, such as a content bill sending operation T62.

[0268]

The system administration organization 330, which receives the content bill, manipulates the requested content in a content distributing function block 404 so that it can be distributed. That is, the content distributing function block 404 generates digital content that is in a state capable of being sent to the user 200 (encrypted digital content). This manipulated digital content is sent to the content display and distribution organization 310, such as in a content sending operation T63.

[0269]

The content display and distribution organization 310 stores the manipulated digital content in a content database function block 345.

[0270]

Furthermore, as content-viewing information, the content distributing function block 404 of the system administration organization 330 sends a content ID, use condition, and content key for decrypting encrypted content to the billing information administration organization 320, such as in an information for viewing content sending operation T64 .

[0271]

The billing information administration organization 320 receives the content viewing information in a content key/use condition receiving function block 363, and stores this information in the database function block 367.

[0272]

Subsequently, the user 200 accesses the content display and distribution organization 310 and obtains content, such as in a content-obtaining request T61. That is, the content display and distribution organization 310, upon receiving a request to obtain content from the user 200 through a communication function block 341, reads out encrypted digital content stored in a content database function block 354, and sends the digital content that has been read out to the user 200.

[0273]

Thereafter, the user 200 accesses the billing information administration organization 320 using an information for viewing content request T65 and obtains content viewing information, such as in an information for viewing content sending operation T66. That is, the billing information administration organization 320, upon receiving a request from the user 200 for a use condition and content key as content viewing information from the user through the communication function block 361, issues the content key and use condition from the content key/use condition issuing function block 364 and sends the same to the user 200 through the communication function block 361.

[0274]

Thus, the flow when distributing content and content viewing information is

completed. Furthermore, the other constitutions included in FIG. 33 will be explained later.

[0275]

Hereafter, the main portion of the flow of a settlement when content has actually been viewed, that is, content use fee settlement will be explained using FIG. 34.

[0276]

First, after the user 200 has viewed the content, the user 200, for example, sends point usage information, that is, a record of content usage as described above, to the billing information administration organization 320, such as a settlement statement sending operation T71. Upon receiving the content usage record that has been sent from the user 200 through the communication function block 361 in this manner, a settlement procedure accepting function block 365 of the billing information administration organization 320 receives the content usage record and issues a settlement confirmation corresponding thereto. The settlement confirmation is sent to the user 200 through the same communication function block 361, such as a settlement confirmation sending operation T73. This makes it possible for the user 200 to learn that settlement has been performed.

[0277]

Subsequently, a settlement procedure accepting function block 365 of the billing information administration organization 320 issues information for issuing a use right from a use right issuing function block 362. This use right issuing information is sent, together with a content usage record sent from the user 200, to the system administration organization 330 through the communication function block 361 such as a user settlement/content usage record sending operation T74.

[0278]

The system administration organization 330, using a collection and distribution function block 405, summarizes the information sent from the billing information administration organizations 320 scattered in various regions, tabulates the collection amounts and collection destinations with the money distribution destinations, and settles accounts through an actual financial institution.

[0279]

Thus, the flow of the settlement of content usage fees comes to an end. Furthermore, the other constitutions included in FIG. 34 will be explained later.

[0280]

In the above explanations from FIG. 30 to FIG. 34, it goes without saying that encryption and decryption are performed the same as described above in the sending and receiving of data between the user 200 and the content display and

distribution organization 310, the billing information administration organization 320, and the system administration organization 330 and/or the sending and receiving of data between the content display and distribution organization 310, the billing information administration organization 320, and the system administration organization 330. Moreover, either a public-key encryption system or a common key encryption system may be used in this encryption and decryption, and as was described above, the public-key encryption system can be used as the encryption system for the content key and the common key, and the common key encryption system can be used as the encryption system for messages, various documents, and the like. Furthermore, it is also possible to use procedures for improving security by using the random number together with these encryptions, and the least common multiple as the processing unit for encryption and compressing when handling content.

[0281]

Hereafter, the specific constitutions of the organizations 310, 320, and 330 will be briefly explained.

[0282]

First, the constitution of the content display and distribution organization 310 will be explained using FIG. 35.

[0283]

In FIG. 35, the content display and distribution organization 310 broadly includes: a communication function block 341 that is in charge of communication functions with the user 200 and the system administration organization 330; a content obtaining function block 342 that is in charge of content obtaining functions; a content displaying function block 343 that is in charge of content displaying functions; a settlement function block 344 that is in charge of settlements; and a content database function block 345 for storing content.

[0284]

The content obtaining function block 342 includes: a content bill request generating function 351 that is in charge of generating a bill request when billing the system administration organization 330 for content; a content receipt generating function 352 that is in charge of generating a receipt when content has been received from the system administration organization 330; and a content database corresponding function 353 that is in charge of making sure the handled content corresponds to the content being stored in the content database function block 345.

[0285]

The content displaying function block 343 includes: a content displaying function 354 that is in charge of functions for actually displaying content in virtual

stores; and a content database corresponding function 355 that is in charge of making sure the displayed content corresponds to the content being stored in the content database function block 345.

[0286]

The settlement function block 344 includes: a receipt issuing function 356 that is in charge of functions for issuing receipts; and a financial organization corresponding function 357 that is in charge of correspondence with the financial organization 220.

[0287]

Hereafter, the constitution of the billing information administration organization 320 will be explained using FIG. 36.

[0288]

In FIG. 36, the billing information administration organization 320 broadly includes: a communication function block 361 that is in charge of communication functions with the user 200 and the system administration organization 330; a use right issuing function block 362 that is in charge of functions for issuing use rights; a content key/use condition receiving function block 363 that is in charge of receiving a content key and a use condition; a content key/use condition issuing function block 364 that is in charge of issuing a content key and a use condition; a settlement procedure accepting function block 365 that is in charge of functions for accepting a settlement procedure; a distribution and receiving function block 366 that is in charge of distributing and receiving functions; and a database function block 376.

[0289]

The use right issuing function block 362 includes: a purchase request confirming function 371 that is in charge of functions for confirming a purchase request; a point data confirming function 372 that is in charge of confirming data, such as the use right balance (point information balance) of a client, that is, a user 200, a usage record (point usage information), and the like; a use right generating function 373 that is in charge of functions for generating use rights; a use right sending notice generating function 374 that is charge of functions for generating a use right sending notice; a sending function 375 that is in charge of functions for actually sending a use right and a use right sending notice; a use right reception confirming function 376 that is in charge of confirming a use right receipt; and use right issue information storing function 377 that is in charge of functions for storing information on issued use rights.

[0290]

The content key/use condition receiving function block 363 includes: a receiving function 378 that is in charge of receiving a content key and a use condition; and a storing function 379 for storing content keys and use conditions.

[0291]

The content key/use condition issuing function block 364 includes: a receiving function 380 that is in charge of functions for receiving requests to obtain content keys and use conditions; a searching function 381 that is in charge of functions for searching for and retrieving content keys and use conditions from the database function block 367; a sending function 382 that is in charge of functions for encrypting and sending content keys and use conditions; and a confirming function 383 that is in charge of functions for confirming the receipt of content keys and use conditions.

[0292]

The settlement procedure accepting function block 365 includes: a content usage record receiving function 384 that is in charge of functions for receiving and decrypting encrypted content usage records (point usage information); a content usage record confirming function 385 that is in charge of confirming content usage records; a content usage record storing function 386 that is in charge of functions for storing content usage records in the database function block 367; a completion notice generating function 387 that is in charge of functions for generating completion notices for settlement procedures; and a summarizing function 389 that is in charge of functions for collectively editing content usage records.

[0293]

The distribution and receiving function block 366 includes: a bill confirming function 390 that is in charge of functions for confirming document bills for billing for documents when carrying out collection; a usage record report generating function 391 that is in charge of functions for generating content usage record reports to be submitted to the system administration organization 330; a use right issue report generating function 392 that is in charge of functions for generating use right issue information reports to be submitted to the system administration organization 330; and a certificate confirming function 393 that is in charge of functions for confirming a certificate of report reception.

[0294]

The database function block 367 includes: a use right data function 394 that is in charge of functions for storing use right data; a content key/use right database function 395 that is in charge of functions for storing content key and use condition data; a content usage record database function 396 for storing content usage records; and a user administration database function 397 for storing information related to users.

[0295]

Hereafter, the constitution of the system administration organization 330 will

be explained using FIG. 37.

[0296]

In FIG. 37, the system administration organization 330 broadly includes: a communication function block 401 that is in charge of functions for communicating with the user 200, the content display and distribution organization 310, and the billing information administration organization 320; a user subscription support function block 402 that provides support at the time of user subscription; a content distributing function block 404 that is in charge of the distribution of content; a database function block 403; and a collection and distribution function block 405 that is in charge of money collection and distribution functions.

[0297]

The user subscription support function block 402 includes: a subscription application generating and sending function 411 that is in charge of generating and sending subscription applications; a common key receiving function 412 that is in charge of functions for receiving and decrypting encrypted common keys; a subscription application confirming function 413 that is in charge of functions for confirming subscription applications sent from users 200; an ID generating function 414 that is in charge of functions for generating client IDs, that is, user IDs; a subscription application storing function 415 that is in charge of functions for storing subscription applications in the database function block 403; a client function generating function 416 for generating client functions; and a registration information storing function 417 that is in charge of functions for storing registration information in the database function block 403.

[0298]

The database function block 403 includes: a user administration database function 418 for storing and managing user information; a content database function 419 for storing content; a billing information administration organization database function 420 for storing and managing billing information administration organization 320 information; and a content display and distribution organization database function 421 for storing and managing content display and distribution organization 310 information.

[0299]

The content distributing function block 404 includes: a bill confirming function 422 that is in charge of functions for confirming content bills; a content searching function 423 that is in charge of functions for searching raw content, that is, content prior to manipulation (source data) from the content database function 419 of the database function block 403; a content ID generating function 424 for generating content IDs; a content key generating function 425 for generating content keys; a

content use condition generating function 426 for generating content use conditions; a content compressing function 427 for compressing raw content, that is, content prior to manipulation; a content manipulating function 428 for encrypting content; a storing function 429 that is in charge of functions for storing content IDs, content keys, and use conditions in the content database function 419 of the database function block 403; a content sending function 430 that is in charge of functions for sending content through the communication function block 401; a content receipt confirming function 431 that is in charge of functions for confirming content receipts; an ID/key/use condition sending function 432 that is in charge of functions for sending content IDs, content keys, and use conditions through the communication function block 401; and an ID/key/use condition receipt confirming function 433 that is in charge of functions for confirming receipts for content IDs, content keys, and use conditions.

[0300]

The collection and distribution function block 405 includes: a document bill generating function 434 for generating document bills for use in collection; a content use right receiving function 435 that is in charge of functions for receiving content use rights through the communication function block 401; a content usage record receiving function 436 that is in charge of functions for receiving content usage records through the communication function block 401; a reception confirmation generating function 437 that is in charge of functions for generating reception confirmations; a calculating and bill generating function 438 for calculating charges to be billed to users and generating bills; and a calculating and delivery notice generating function 439 for calculating dividends when distributing usage fees collected in accordance with usage to proprietors and generating delivery notices.

[0301]

Hereafter, the constitution of the user 200 corresponding to the system of the other preferred embodiment will be explained using FIG. 38. Furthermore, FIG. 38 collectively represents the functions of the player 1 and user terminal 50.

[0302]

In FIG. 38, the constitution of the user 200 side broadly includes: a communication function block 451 that is in charge of functions for communicating with the system administration organization 330, the content display and distribution organization 310, and the billing information administration organization 320; a content obtaining function block 452 that is in charge of obtaining content; a use right purchasing function block 453 that is in charge of purchasing point information, content keys, use conditions, and other such use rights; a content key/use condition obtaining function block 454 that is in charge of obtaining content keys and use conditions; a settlement procedure function block 455 that is in charge of settlement

procedures; a user subscription support function block 456 that is in charge of functions for supporting subscriptions to the system; a content-viewing billing function block 457 that is in charge of functions for billing for viewing content; and a database function block 458.

[0303]

The content obtaining function block 452 includes: a content obtaining function 461 that is in charge of functions for actually obtaining content; and a content storing function 462 that is in charge of functions for storing content in storage media.

[0304]

The use right purchasing function block 453 includes: a purchase request generating function 463 for generating purchasing requests for use rights; a summarizing function 464 that is in charge of summarizing data, such as a client (user) use right balance (point balance), usage records (point usage information), and the like; a use right installing function 465 that is in charge of functions for installing various information as use rights; and a use right receipt generating function 467 for generating a use right receipt.

[0305]

The content key/use condition obtaining function block 454 includes: an obtain request generating function 468 for generating requests for obtaining content keys and use conditions; a receiving function 469 that is in charge of receiving content keys and use conditions; and a receipt generating function 470 for generating receipts for content keys and use conditions.

[0306]

The settlement procedure function block 455 includes: a summarizing function 471 for summarizing content usage records (point usage information); and a completion notice receiving function 472 that is in charge of receiving completion notices for settlement procedures.

[0307]

The user subscription support function block 456 includes: a subscription application generating function 473 that is in charge of generating a subscription application; a client function installing function 474 that is in charge of installing the client functions, that is, initializing the player 1 of the user; and a registration information generating function 475 that is in charge of functions for generating registration information.

[0308]

The content viewing billing function block 457 includes: a content searching function 476 that is in charge of searching for content stored in storage media; a use

right confirming function 477 that is in charge of confirming use rights; a simplified content viewing function 478 for simply playing back content when, for example, content is being selected; a billing function 479 for managing billing information (point information); a content decryption function 480 for decrypting encrypted content; a content decompressing function 481 for decompressing compressed content; and a content viewer function 482 for making the details of content stored, for example, in storage media recognizable.

[0309]

The database function block 458 includes: a use right database function 483 for storing use right data; a content key/use condition database function 484 for storing content keys and use conditions; a content usage record database function 485 for storing content usage records; and a user information database function 486 for storing user information.

[0310]

Hereafter, the specific utilization configurations of the player 1 and user terminal 50 of the respective preferred embodiments as described above will be explained using FIGS. 39 and 40.

[0311]

As shown in FIG. 39, the analog output terminal 2, PC interface terminal 3, and storage medium I/O terminal 4 of the player 1 are arranged in a state protruding out from the player 1 enclosure, and a storage medium 61 is connected through the storage medium I/O terminal 4. Furthermore, the player 1 and storage medium 61 are formed, for example, so as to be able to be housed inside a case 60, and the analog output terminal 2 and PC interface terminal 3 of the player 1 are arranged, for example, at one end of this case 60.

[0312]

The case 60 in which the player 1 and storage medium 61 are housed is formed so as to be insertably connected to the input/output port 53 of the personal computer 50 serving as the user terminal 50 from the side on which the analog output terminal 2 and PC interface terminal 3 of the player 1 are arranged.

[0313]

The personal computer 50 has an ordinary constitution including a computer main unit with a display device 52, a keyboard 54, and a mouse 55, and interfaces corresponding to the player 1 analog output terminal 2 and PC interface terminal 3 are formed inside the input/output port 53. Therefore, the player 1 analog output terminal 2 and PC interface terminal 3 are connected to the personal computer 50 by simply inserting the case 60 housing the player 1 and storage medium 61 into the input/output port 53 of the personal computer 50.

[0314]

In the example of FIG. 39, interfaces corresponding to the player 1 analog output terminal 2 and PC interface terminal 3 are formed inside the input/output port 53 of the personal computer 50, however, for example, as shown in FIG. 40, it is also possible to arrange an adapter 62, which is capable of supporting a general-purpose input/output port interface of the personal computer 50, between the player 1 analog output terminal 2 and PC interface terminal 3.

[0315]

Based on the description given above, in a system of the preferred embodiment of the present invention, because digital content is encrypted using the content key, which is the system common key, as long as a user (player 1) is registered in the system of the preferred embodiment, the user can freely copy this encrypted content, and is able to view this content by simply obtaining the content key. Therefore, this content (encrypted content) can be easily installed in the storage medium. Alternatively, because a terminal device that does not conform to the system of the preferred embodiment is not able to decrypt the encrypted digital content, the content copyrights and the rights of the content proprietors are protected.

[0316]

Furthermore, according to the system according to the preferred embodiment of the present invention, point information is replenished using a prepaid system (a prepayment system) and point information is decremented when the content is viewed, and use information regarding these points is collected. Therefore it is possible for the proprietors (copyright holders, and the like) who hold the rights to used points, the content stores, and the like to collect viewing charges.

[0317]

In addition, security is improved since the previously described encryption is performed when point information and point usage information data are exchanged. For example, even if someone were to attempt to steal point information for billing by forging data that is exactly the same as previous data, as described above, interlinked random numbers (security IDs) are used by the system side and the player side and a transaction is carried out after confirming that the two random numbers match, thereby making it safe.

[0318]

In addition to that, the major components of the player are integrated onto a single chip, making it impossible to extract the key information and decrypted digital content to the outside. The player 1 is provided with a tamper-resistance function in the player 1 itself to prevent data from being stolen by destroying the player 1.

[0319]

As mentioned above, according to the preferred embodiments of the present invention, a high-security digital content distribution system is built.

[0320]

Furthermore, examples of the digital content can include various types of digital video data in addition to digital audio data. When using moving picture image data (including audio data) as the digital video data, for example, the Moving Picture Image Coding Experts Group (MPEG) and other such compression techniques can be used as the compression technique. Furthermore, the above-mentioned MPEG is the vernacular term for the video encryption system compiled in Working Group (WG) 11 of Sub-Committee (SC) 29 of the Joint Technical Committee (JTC) 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and includes MPEG 1, MPEG 2, MPEG 4, and the like.

[0321]

Furthermore, as was described above, for example, the encryption technique called the Data Encryption Standard (DES) can be used as the encryption technique. Note that DES is the standard encryption technique (encryption algorithm) announced in 1976 by the National Institute of Standards and Technology (NIST) of the United States. Specifically, DES performs data conversion for each 64-bit block of data, and repeats the conversion, which uses a function, 16 times. The digital content, point information, and the like are encrypted by using a so-called common key technique using the DES. Furthermore, the common key technique is a technique in which the key data for encryption (encryption key data) and the key for decryption (decryption key data) are the same.

[0322]

Moreover, for example, so-called Electrically Erasable Programmable Read-Only Memory (EEPROM) can be used in the common key storage memory 22, communication key storage memory 21, point usage information storage memory 29, point information storage memory 28, and the like of the player 1 of FIG. 1.

[0323]

Other storage media available includes recording media such as a hard disk, a floppy disk, a magneto-optical disk, and phase-alternating magneto-optical disk, and storage media such as a semiconductor memory (IC card and the like).

[0324]

In the above-mentioned preferred embodiments, the keyboard 54, the mouse 55, and the display device 52 of the user terminal 50 are used to select content or check content displayed in the virtual store 230. However the keyboard, mouse, and display device may be simplified in function and installed on the player 1. Namely,

the input section 6 and the display section 7 may be provided on the player 1, as in FIG. 2.

[0325]

[Effects of the Invention]

As is clear from the above explanation, according to the present invention, it is possible to build a system that is portable and enables digital content to be enjoyed anywhere and anytime, and also provides adequate protection against the copying and unauthorized use of the digital content and is economical.

[Brief Description of the Drawings]

FIG. 1 is a configuration diagram illustrating an entire constitution of a digital content distributing system according to an embodiment of the present invention.

FIG. 2 is a block circuit diagram illustrating a specific constitution of a player of the system according to an embodiment of the present invention.

FIG. 3 is a block circuit diagram illustrating a specific constitution of an administration center of the system according to an embodiment of the present invention.

FIG. 4 is a diagram for describing a procedure in which the player is purchased in the system according to an embodiment.

FIG. 5 is a diagram for describing a procedure for processing to be performed from digital content search to installation of digital content on a storage medium for the player in the system according to an embodiment.

FIG. 6 is a diagram for describing a procedure of purchasing point information for charging and of settlement to be made when digital content concerned has been used in the system according to an embodiment.

FIG. 7 is a diagram for describing a procedure of distributing charged fees in the system according to an embodiment.

FIG. 8 is a flowchart illustrating a processing flow in the player at the time of point purchase in the system according to an embodiment.

FIG. 9 is a flowchart illustrating a processing flow at a user terminal at the time of point purchase in the system according to an embodiment.

FIG. 10 is a flowchart illustrating a processing flow at an administration center at the time of point purchase in the system according to an embodiment.

FIG. 11 is a diagram illustrating a sequence of information transfer at the time of point purchase in the system according to an embodiment.

FIG. 12 is a flowchart illustrating a processing flow at the player at the time of acquiring digital content in the system according to an embodiment.

FIG. 13 is a flowchart illustrating a processing flow at the user terminal at the

time of acquiring digital content in the system according to an embodiment.

FIG. 14 is a flowchart illustrating a processing flow at the administration center at the time of acquiring digital content in the system according to an embodiment.

FIG. 15 is a diagram illustrating a sequence of information transfer to be performed when acquiring digital content in the system according to an embodiment.

FIG. 16 is a flowchart illustrating a processing flow at the player at the time of acquiring a content key and a condition of use in the system according to an embodiment.

FIG. 17 is a flowchart illustrating a processing flow at the user terminal at the time of acquiring a content key and a condition of use in the system according to an embodiment.

FIG. 18 is a flowchart illustrating a processing flow at the administration center at the time of acquiring a content key and a condition of use in the system according to an embodiment.

FIG. 19 is a diagram illustrating a sequence of information transfer to be performed at the time of acquiring a content key and a condition of use in the system according to an embodiment of the present invention

FIG. 20 is a flowchart illustrating a processing flow in which digital content is actually viewed by use of the player and the user terminal in the system according to an embodiment.

FIG. 21 is a flowchart illustrating a processing flow at the player at the time of returning point usage information in the system according to an embodiment.

FIG. 22 is a flowchart illustrating a processing flow at the user terminal at the time of returning point usage information in the system according to an embodiment.

FIG. 23 is a flowchart illustrating a processing flow at the administration center at the time of returning point usage information in the system according to an embodiment.

FIG. 24 is a diagram illustrating a sequence for information transfer at the time of returning point usage information in the system according to an embodiment.

FIG. 25 is a flowchart illustrating a processing flow of performing decryption and decompression by the least common multiple of the processing unit of encryption and compression.

FIG. 26 is a block circuit diagram illustrating a constitution for performing decryption and decompression per unit of the least common multiple of the processing unit of encryption and compression.

FIG. 27 is a block circuit diagram illustrating a specific constitution for generating random numbers as a security ID.

FIG. 28 is a diagram for illustrating an operation in which random numbers are inserted when encrypting a common key by public key encryption to transmit the encrypted common key.

FIG. 29 is a diagram for illustrating an operation in which random numbers are extracted from a received statement for confirming validity.

FIG. 30 is a diagram for describing each organization when the system functionality is divided.

FIG. 31 is diagram for describing a main portion of a processing flow at the time of user subscription to the system in an embodiment in which the system functionality is divided.

FIG. 32 is a diagram for describing a main portion of an information flow at the time of purchasing point information and acquiring a key for decrypting encrypted digital content in the embodiment in which the system functionality is divided.

FIG. 33 is a diagram for describing a main portion of a processing flow of distributing content and information for viewing the content in the embodiment in which the system functionality is divided.

FIG. 34 is a diagram for describing a main portion of a flow of fee settlement when content has been actually viewed in the embodiment in which the system functionality is divided.

FIG. 35 is a block diagram illustrating a constitution of a content display distributing organization in the embodiment in which the system functionality is divided.

FIG. 36 is a block diagram illustrating a constitution of a billing information control organization in the embodiment in which the system functionality is divided.

FIG. 37 is a block diagram illustrating a constitution of a system control organization in the embodiment in which the system functionality is divided.

FIG. 38 is a block diagram illustrating a constitution of the user side in the embodiment in which the system functionality is divided.

FIG. 39 is a diagram for describing one example of a specific usage form of the player and the user terminal.

FIG. 40 is a diagram for describing another example of a specific usage form of the player and the user terminal.

[Reference Numerals]

1 Player

2 Analog output terminal

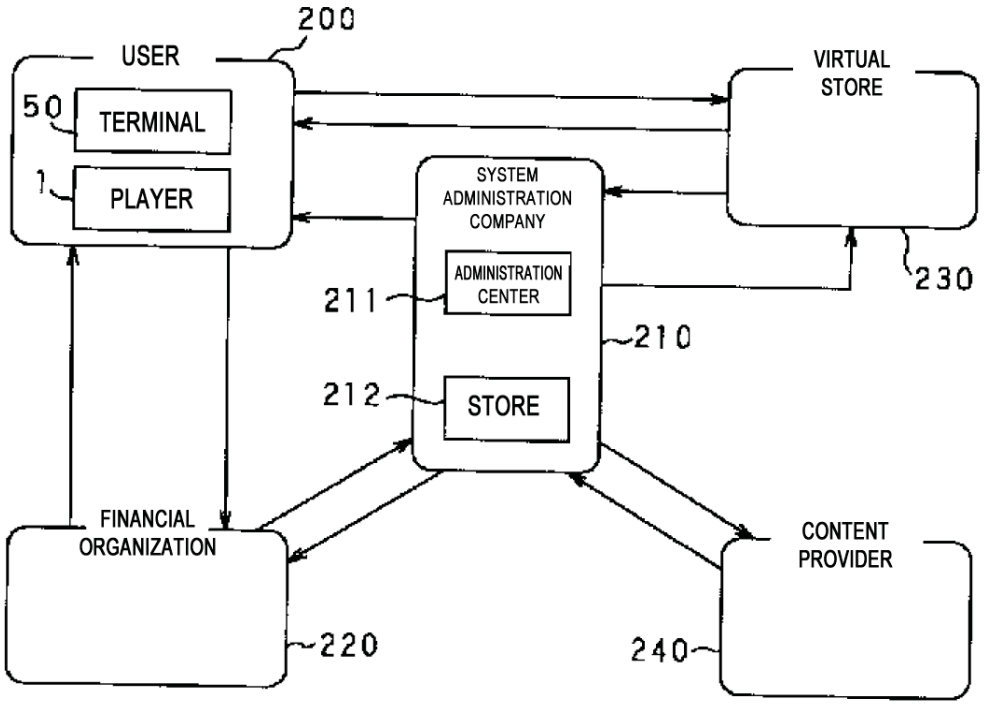
3 PC interface terminal

4 Storage medium I/O terminal

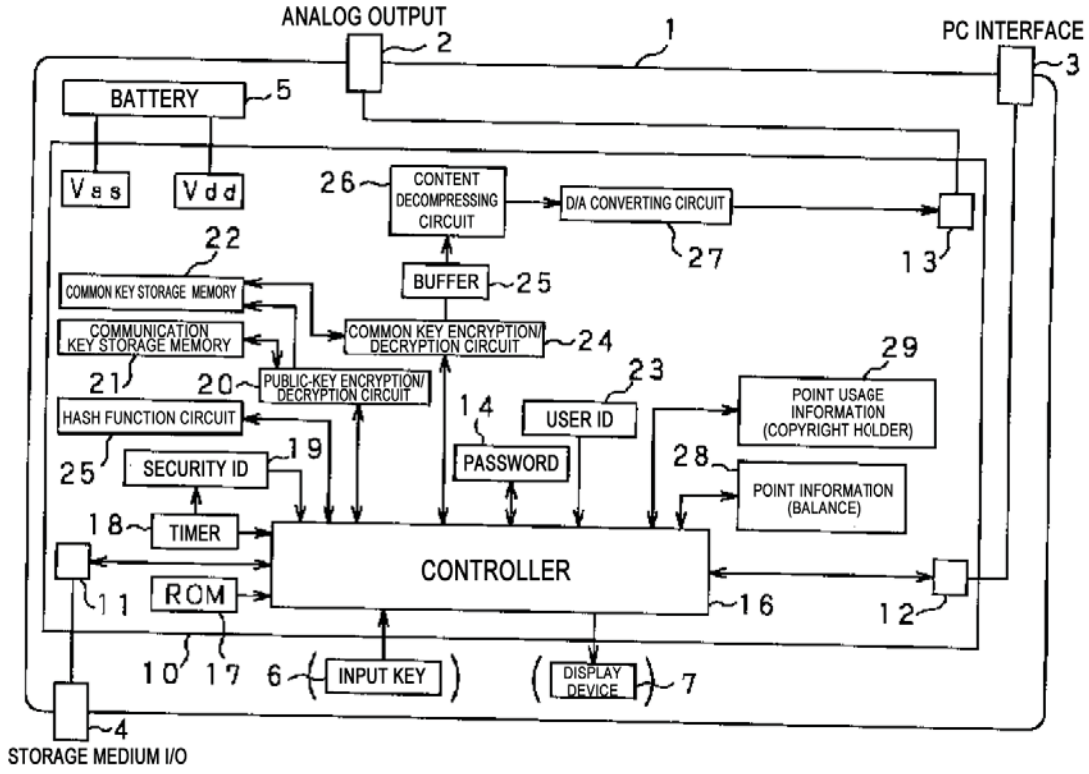
16 Controller

19 Security ID generation circuit
20 Public-key encryption/decryption circuit
21 Communication key storage memory
22 Common key storage memory
23 User ID storage memory
24 Common key encryption/decryption circuit
25 Buffer memory
26 decompressing circuit
27 D/A conversion circuit
50 User terminal
100 Content administration function block
110 User administration function block
120 Usage information administration function block
130 Administration function block
200 User side
210 System administration company
211 Administration center
220 Financial organization
230 Virtual store
240 Content provider

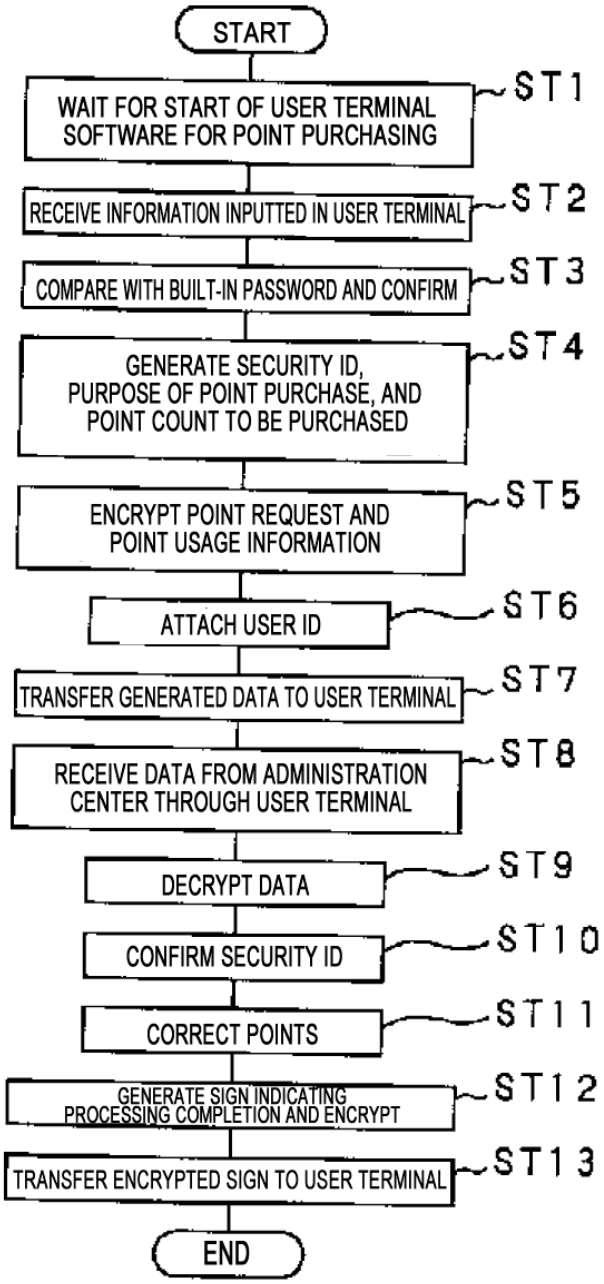
[FIG. 1]


200
USER
50
TERMINAL
1
PLAYER
VIRTUAL STORE
230
SYSTEM ADMINISTRATION COMPANY
ADMINISTRATION CENTER
211
210
212
STORE
FINANCIAL ORGANIZATION
220
CONTENT PROVIDER
240

[FIG. 2]

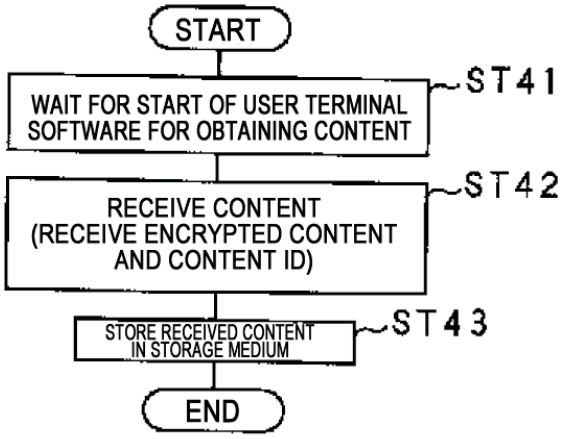

ANALOG OUTPUT
2
1
PC INTERFACE
3
BATTERY
5
Vss
Vdd
26
CONTENT DECOMPRESSING CIRCUIT
D/A CONVERTING CIRCUIT
27
13
22
BUFFER
25
COMMON KEY STORAGE MEMORY
COMMUNICATION KEY STORAGE MEMORY
COMMON KEY ENCRYPTION/ DECRYPTION CIRCUIT
24
29
21
20
PUBLIC-KEY ENCRYPTION/ DECRYPTION CIRCUIT
23
HASH FUNCTION CIRCUIT
14
USER ID
POINT USAGE INFORMATION (COPYRIGHT HOLDER)
25
SECURITY ID
19
PASSWORD
28
POINT INFORMATION (BALANCE)
18
TIMER
CONTROLLER
11
ROM
16
12
10
17
6
INPUT KEY
DISPLAY DEVICE
7
4
STORAGE MEDIUM I/O

[FIG. 8]



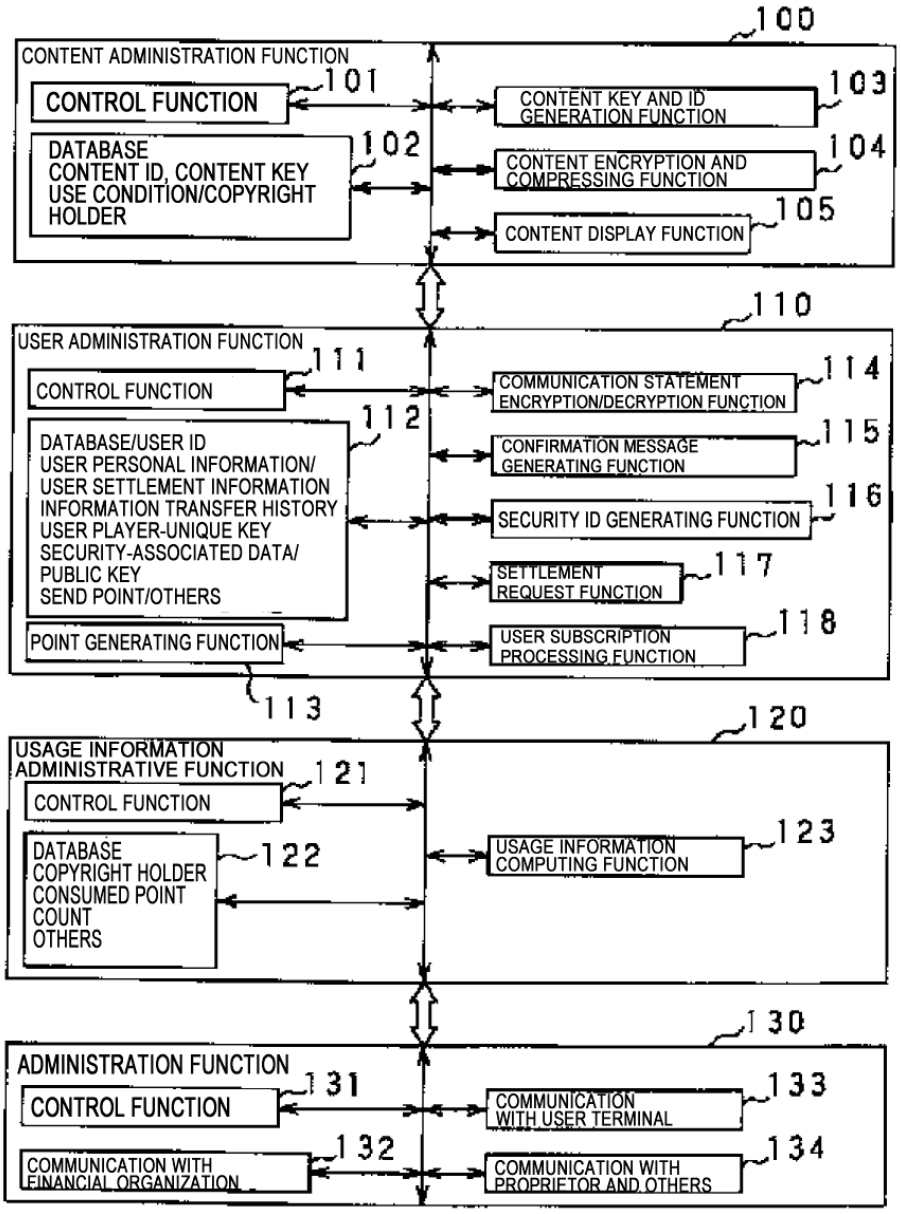
FLOWCHART FOR PLAYER WHEN PURCHASING POINTS

[FIG. 12]

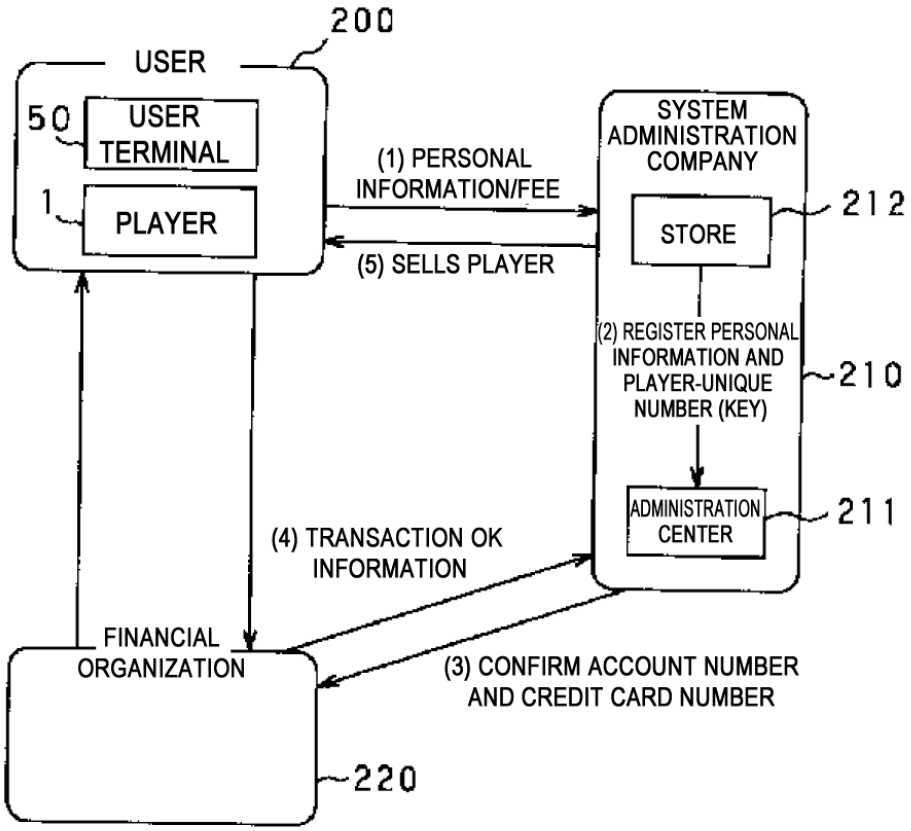


FLOWCHART FOR PLAYER WHEN OBTAINING CONTENT

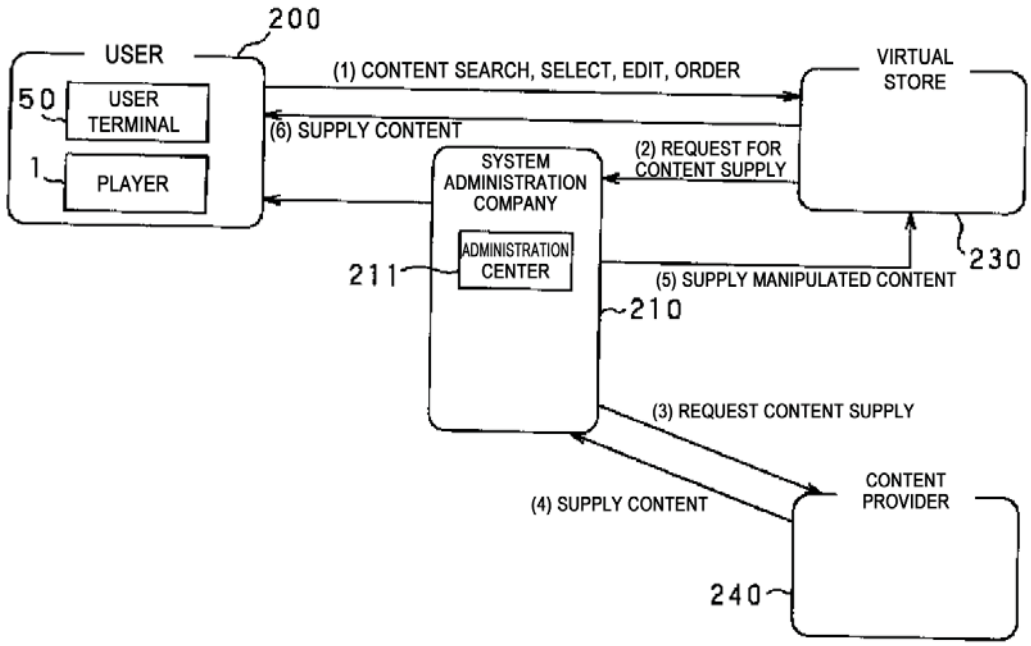
[FIG. 3]


100
CONTENT ADMINISTRATION FUNCTION
101
CONTROL FUNCTION
102
DATABASE
CONTENT ID, CONTENT KEY
USE CONDITION/COPYRIGHT
HOLDER
103
CONTENT KEY AND ID GENERATION FUNCTION
104
CONTENT ENCRYPTION AND COMPRESSING FUNCTION
105
CONTENT DISPLAY FUNCTION
110
USER ADMINISTRATION FUNCTION
111
CONTROL FUNCTION
112
DATABASE/USER ID
USER PERSONAL INFORMATION/
USER SETTLEMENT INFORMATION
INFORMATION TRANSFER HISTORY
USER PLAYER-UNIQUE KEY
SECURITY-ASSOCIATED DATA/
PUBLIC KEY
SEND POINT/OTHERS
113
POINT GENERATING FUNCTION
114
COMMUNICATION STATEMENT ENCRYPTION/DECRYPTION FUNCTION
115
CONFIRMATION MESSAGE GENERATING FUNCTION
116
SECURITY ID GENERATING FUNCTION
117
SETTLEMENT REQUEST FUNCTION
118
USER SUBSCRIPTION PROCESSING FUNCTION
120
USAGE INFORMATION ADMINISTRATIVE FUNCTION
121
CONTROL FUNCTION
122
DATABASE
COPYRIGHT HOLDER
CONSUMED POINT
COUNT
OTHERS
123
USAGE INFORMATION COMPUTING FUNCTION
130
ADMINISTRATION FUNCTION
131
CONTROL FUNCTION
132
COMMUNICATION WITH FINANCIAL ORGANIZATION
133
COMMUNICATION WITH USER TERMINAL
134
COMMUNICATION WITH PROPRIETOR AND OTHERS

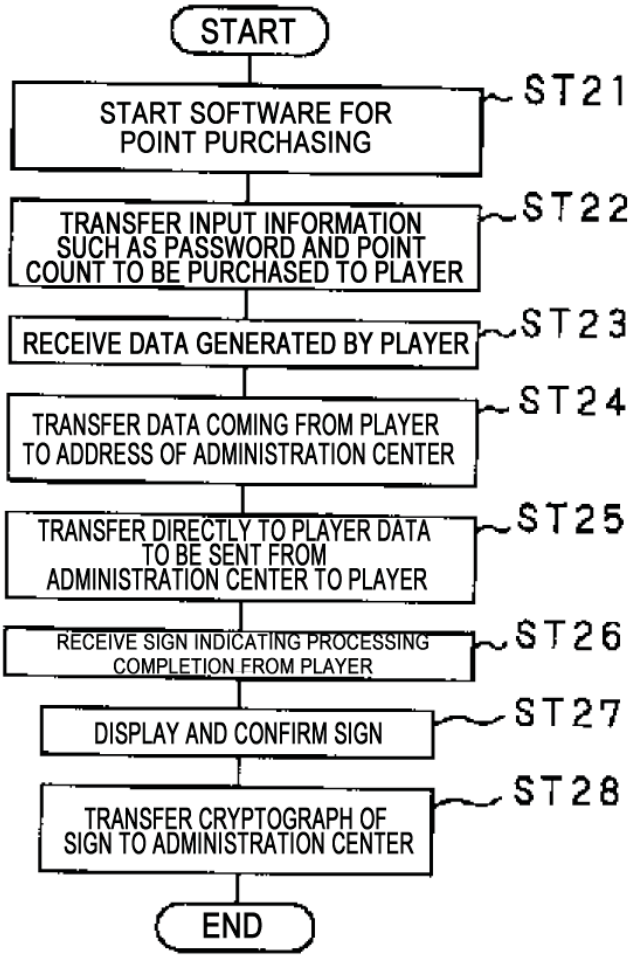
[FIG. 4]


200
USER
50
USER TERMINAL
1
PLAYER
(1) PERSONAL INFORMATION/FEE
(5) SELLS PLAYER
SYSTEM ADMINISTRATION COMPANY
212
STORE
(2) REGISTER PERSONAL INFORMATION AND PLAYER-UNIQUE NUMBER (KEY)
210
ADMINISTRATION CENTER
211
(4) TRANSACTION OK INFORMATION
FINANCIAL ORGANIZATION
(3) CONFIRM ACCOUNT NUMBER AND CREDIT CARD NUMBER
220

[FIG. 5]

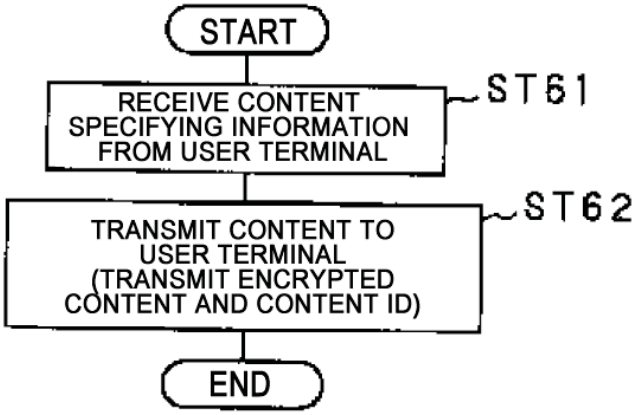

200
USER
50
USER TERMINAL
1
PLAYER
(1) CONTENT SEARCH, SELECT, EDIT, ORDER
(6) SUPPLY CONTENT
VIRTUAL STORE
(2) REQUEST FOR CONTENT SUPPLY
SYSTEM ADMINISTRATION COMPANY
ADMINISTRATION CENTER
211
230
(5) SUPPLY MANIPULATED CONTENT
210
(3) REQUEST CONTENT SUPPLY
(4) SUPPLY CONTENT
CONTENT PROVIDER
240

[FIG. 9]



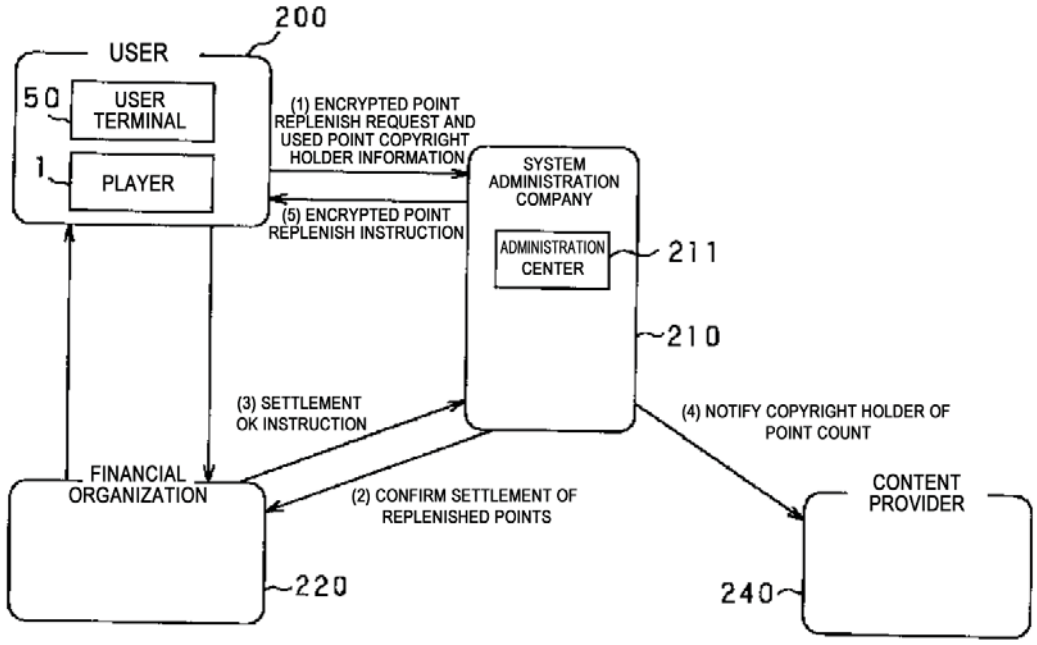
FLOWCHART FOR USER TERMINAL WHEN PURCHASING POINTS

[FIG. 14]

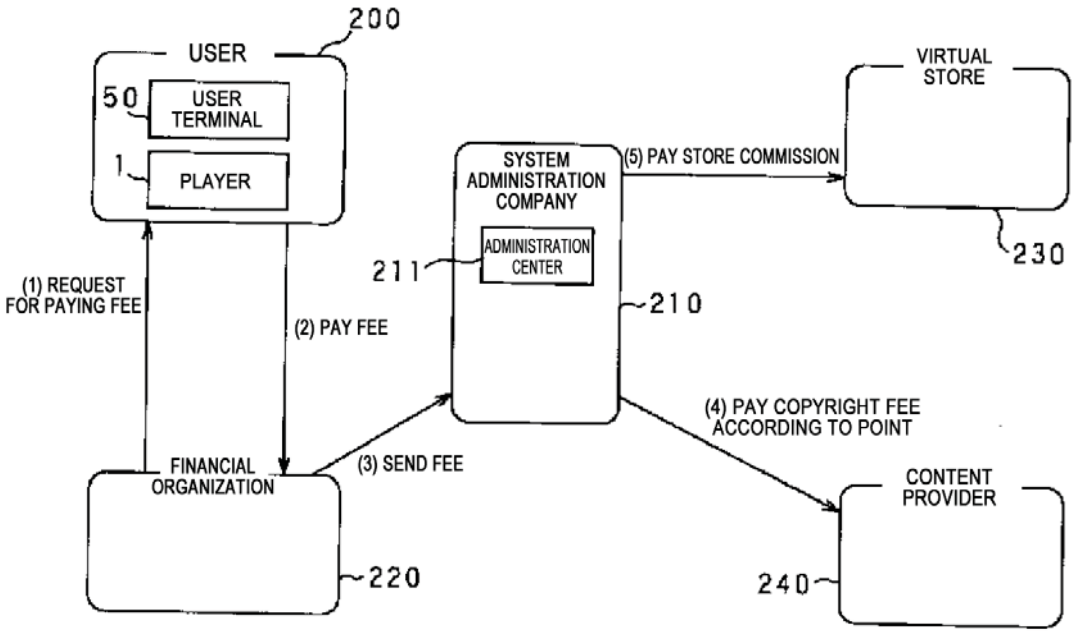


FLOWCHART FOR ADMINISTRATION CENTER WHEN PURCHASING CONTENT

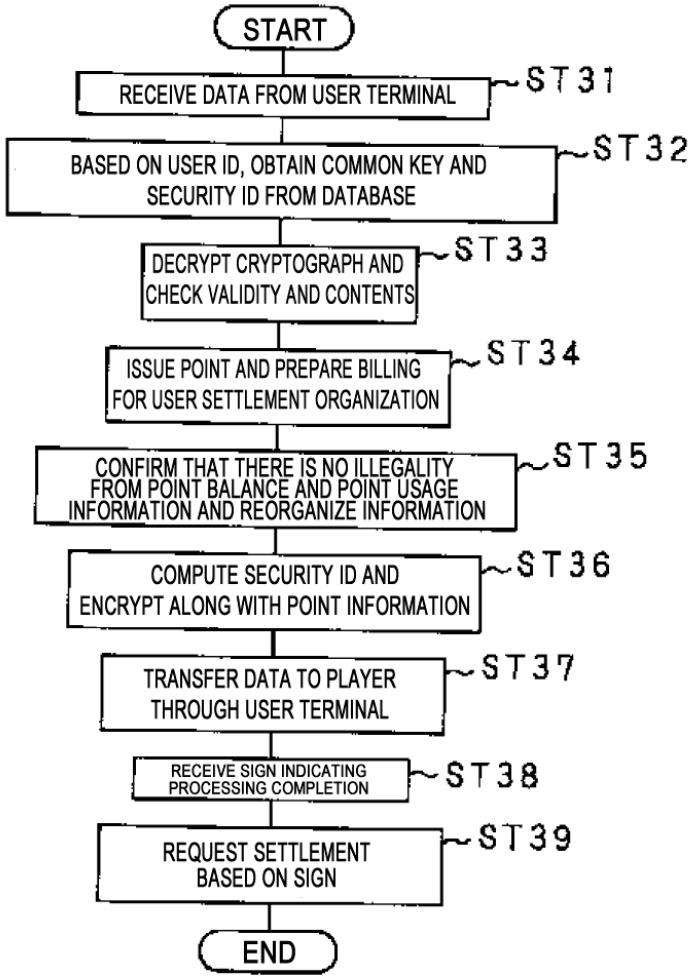
[FIG. 6]



[FIG. 7]

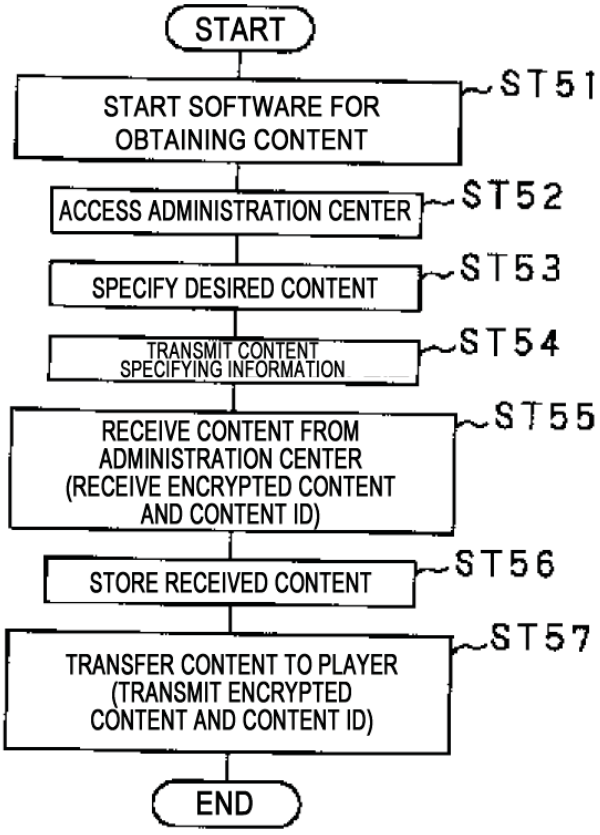

200
USER
50
USER TERMINAL
1
PLAYER
(1) REQUEST FOR PAYING FEE
(2) PAY FEE
FINANCIAL ORGANIZATION
220
(3) SEND FEE
SYSTEM ADMINISTRATION COMPANY
211
ADMINISTRATION CENTER
210
(5) PAY STORE COMMISSION
VIRTUAL STORE
230
(4) PAY COPYRIGHT FEE ACCORDING TO POINT
CONTENT PROVIDER
240

[FIG. 10]



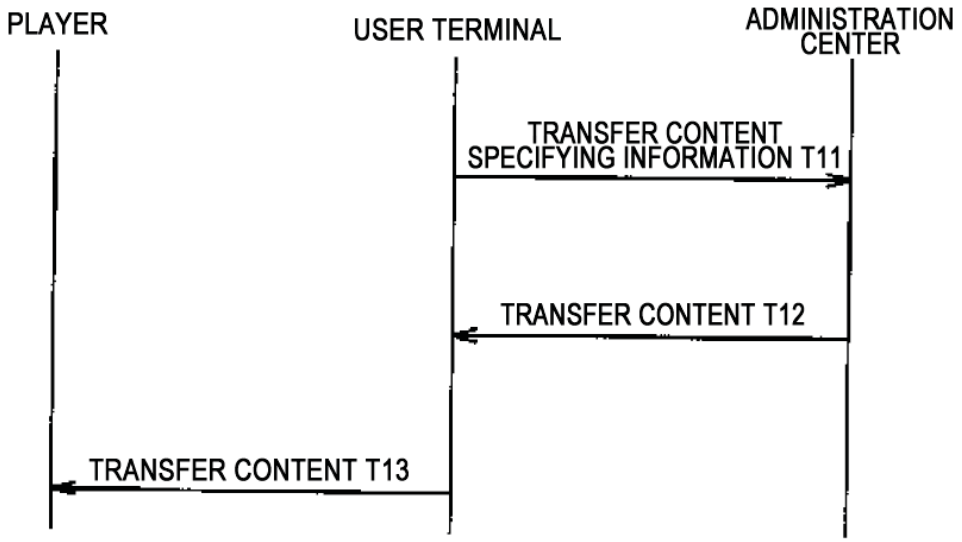
FLOWCHART FOR ADMINISTRATION CENTER WHEN PURCHASING POINTS

[FIG. 13]



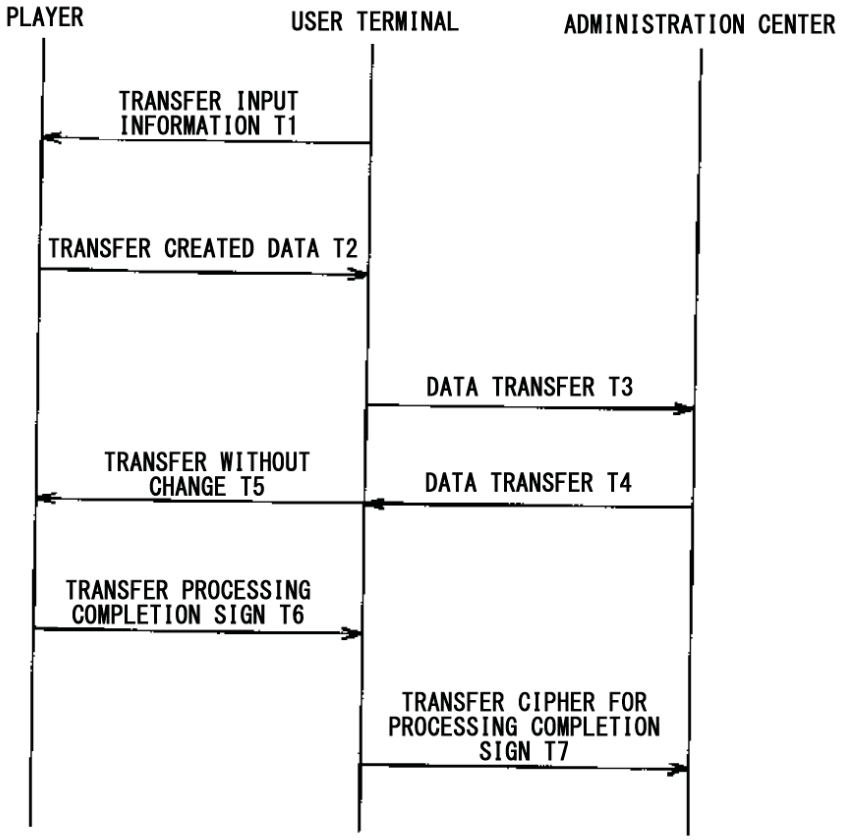
FLOWCHART FOR USER TERMINAL WHEN OBTAINING CONTENT

[FIG. 15]



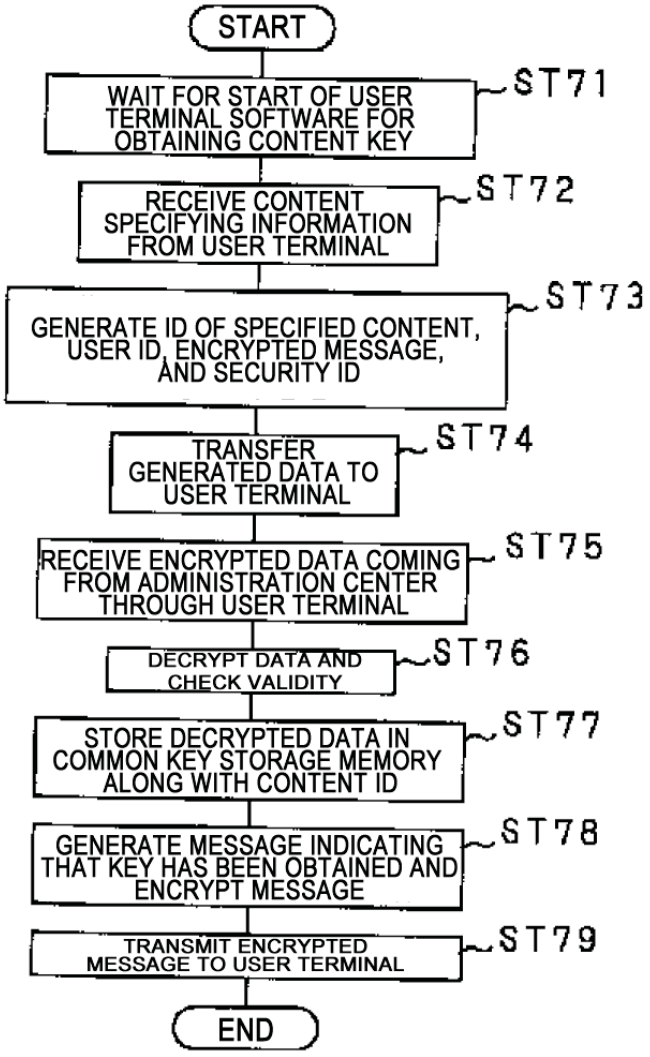
SEQUENCE WHEN OBTAINING CONTENT

[FIG. 11]



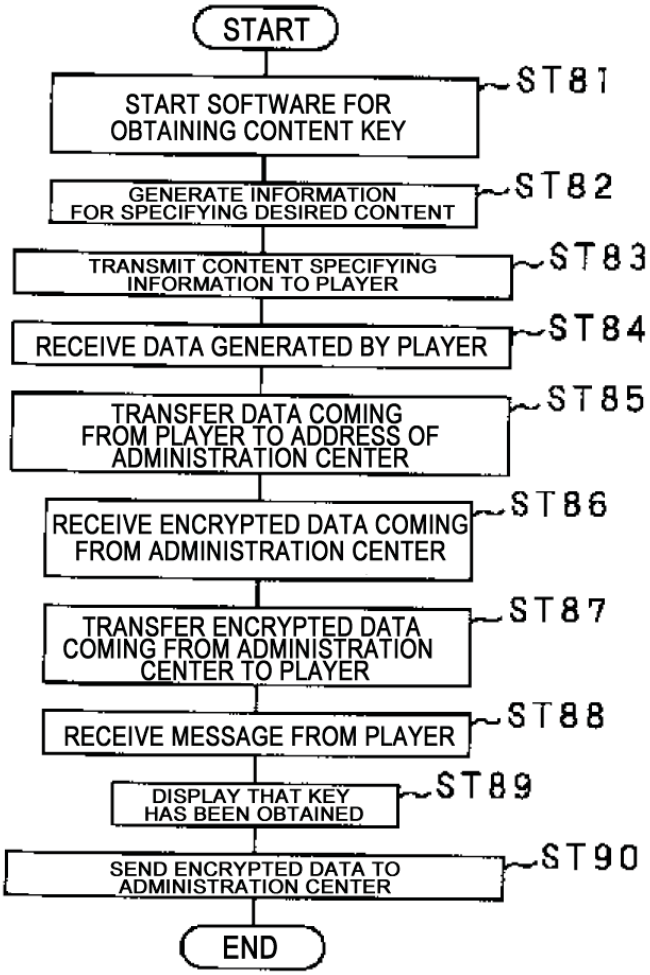
SEQUENCE WHEN PURCHASING POINTS

[FIG. 16]



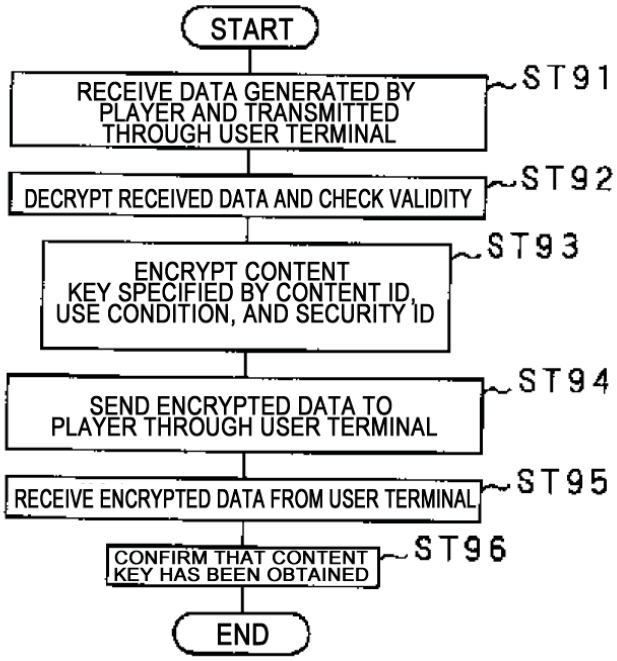
FLOWCHART FOR PLAYER WHEN OBTAINING CONTENT KEY

[FIG. 17]



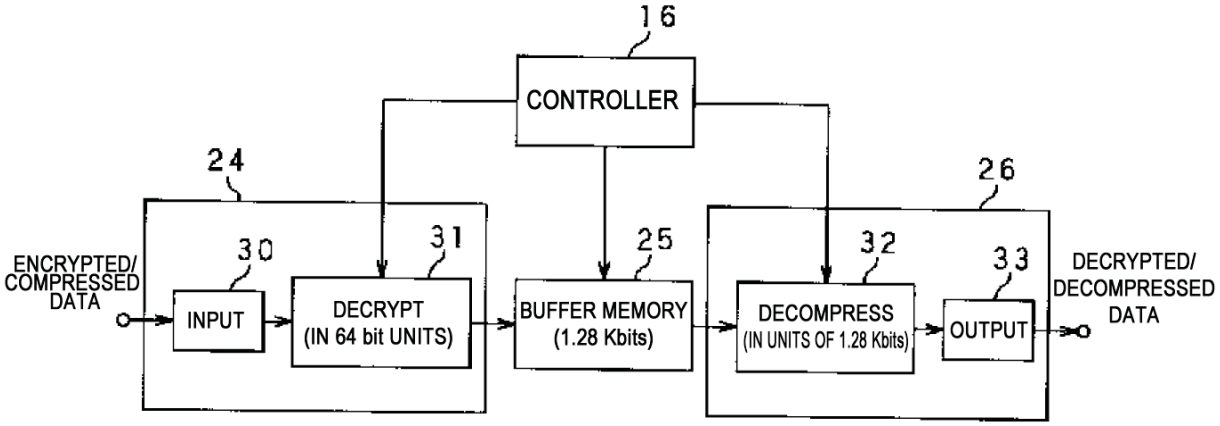
FLOWCHART FOR USER TERMINAL WHEN OBTAINING CONTENT KEY/USE CONDITION

[FIG. 18]

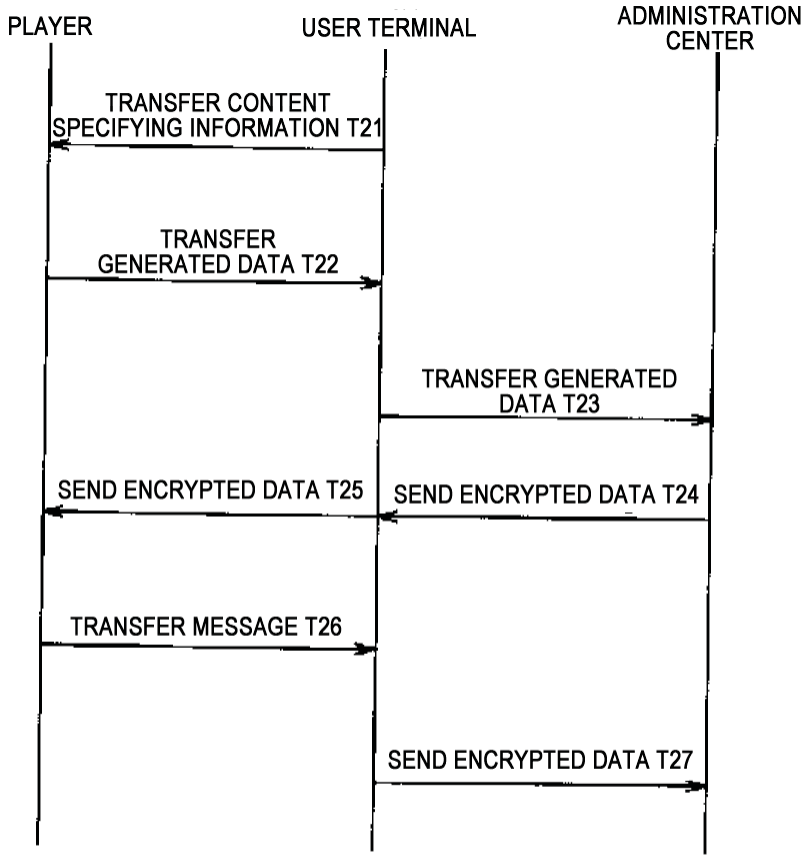


FLOWCHART FOR ADMINISTRATION CENTER WHEN OBTAINING CONTENT KEY/USE CONDITION

[FIG. 26]

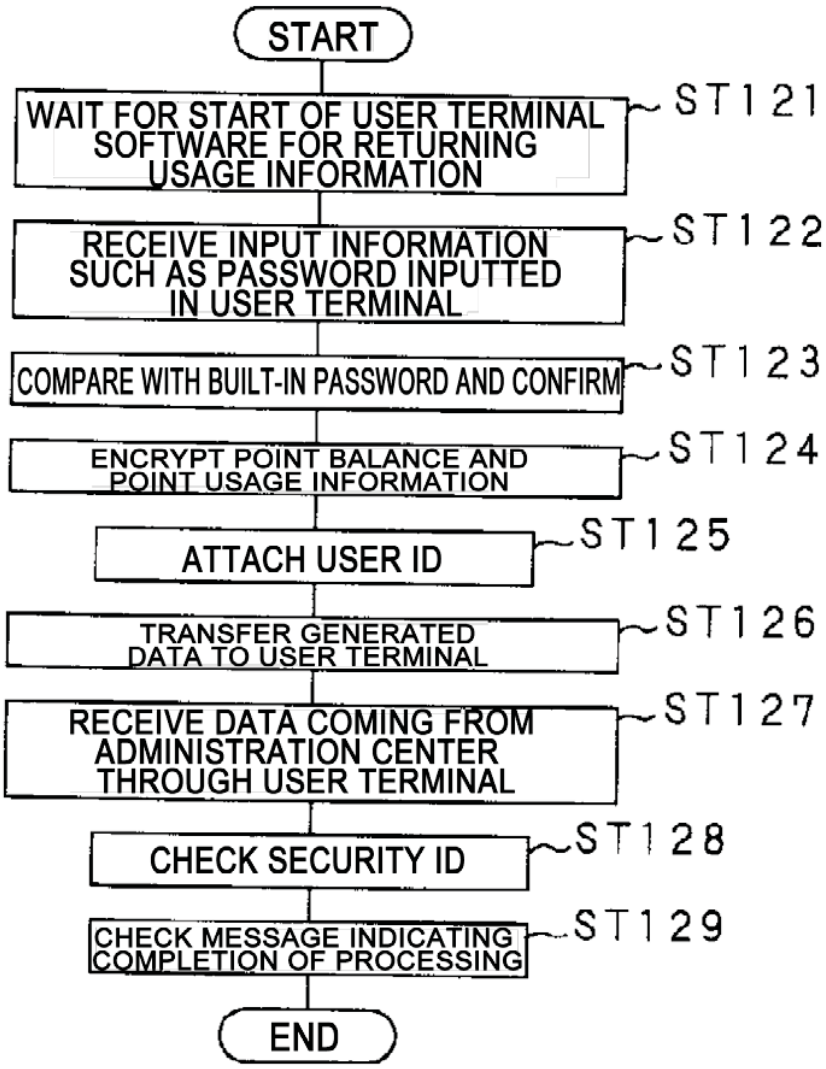


[FIG. 19]



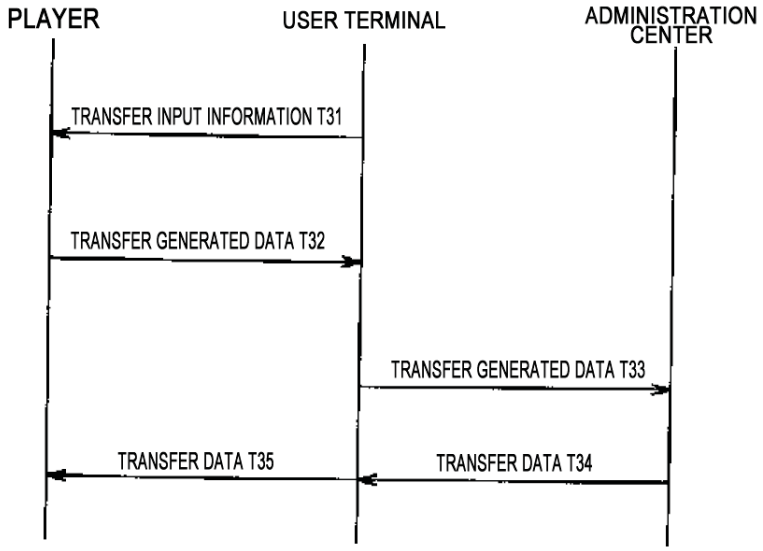
SEQUENCE WHEN OBTAINING CONTENT KEY/USE CONDITION

[FIG. 21]



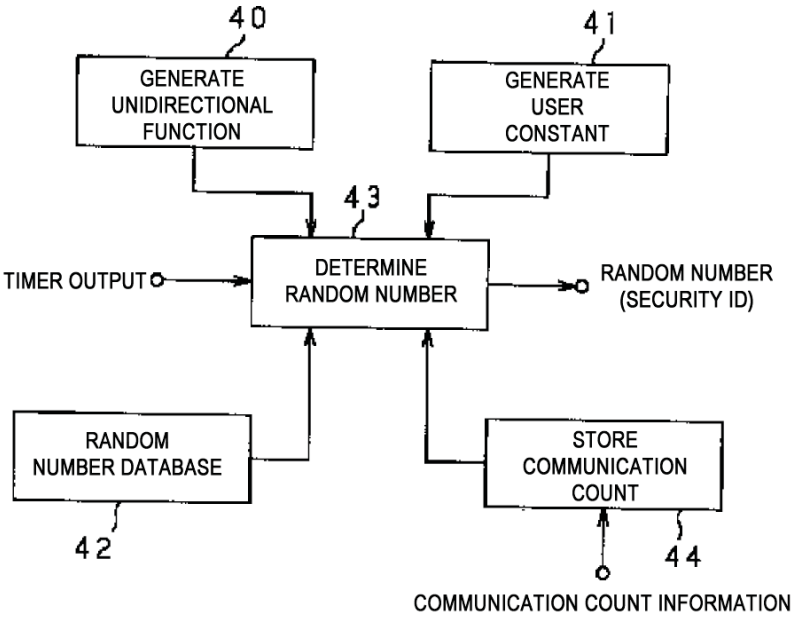
FLOWCHART FOR PLAYER WHEN RETURNING USAGE INFORMATION

[FIG. 24]

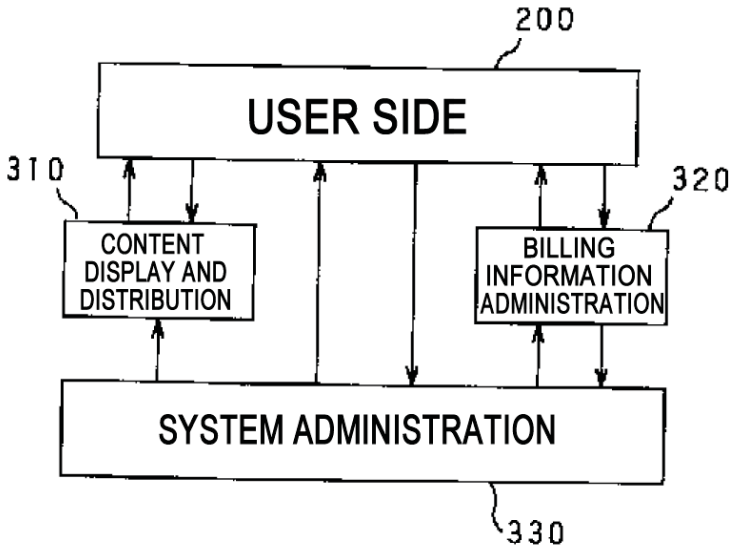


SEQUENCE WHEN RETURNING USAGE INFORMATION

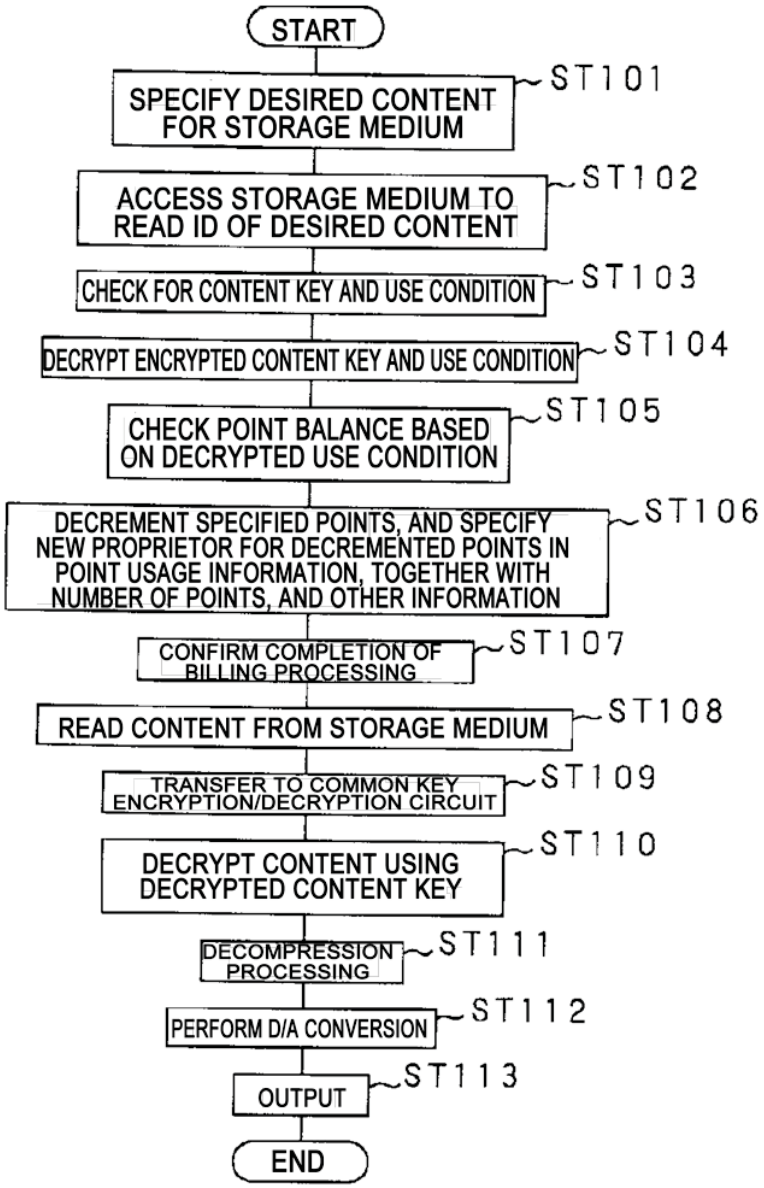
[FIG. 27]



[FIG. 30]

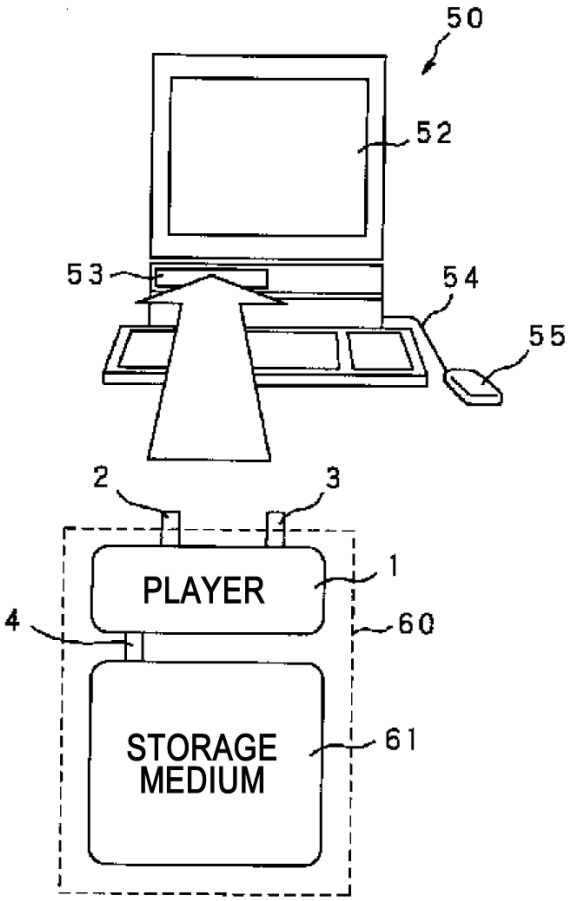

200
USER SIDE
310
320
CONTENT DISPLAY AND DISTRIBUTION
BILLING INFORMATION ADMINISTRATION
SYSTEM ADMINISTRATION
330

[FIG. 20]

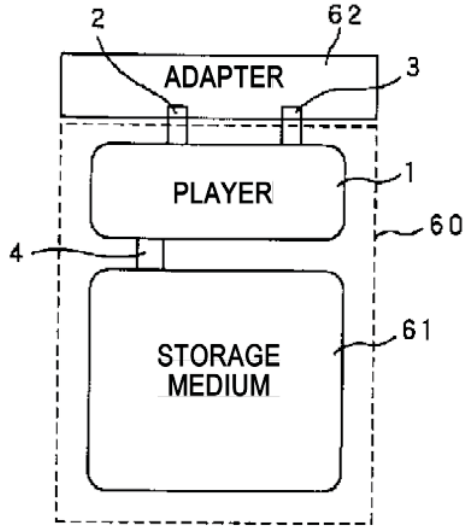


FLOWCHART FOR PLAYER WHEN VIEWING CONTENT

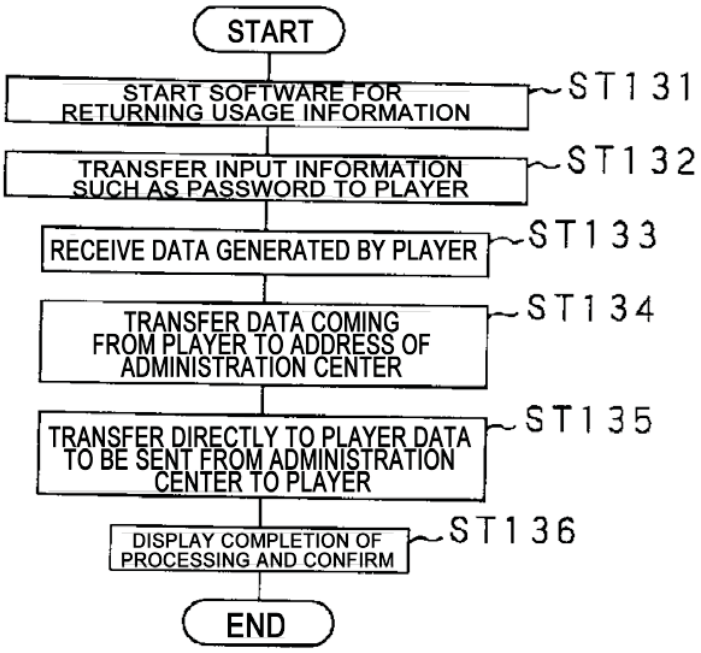
[FIG. 39]


50
52
53
54
55
2
3
PLAYER
1
4
60
STORAGE MEDIUM
61

[FIG. 40]

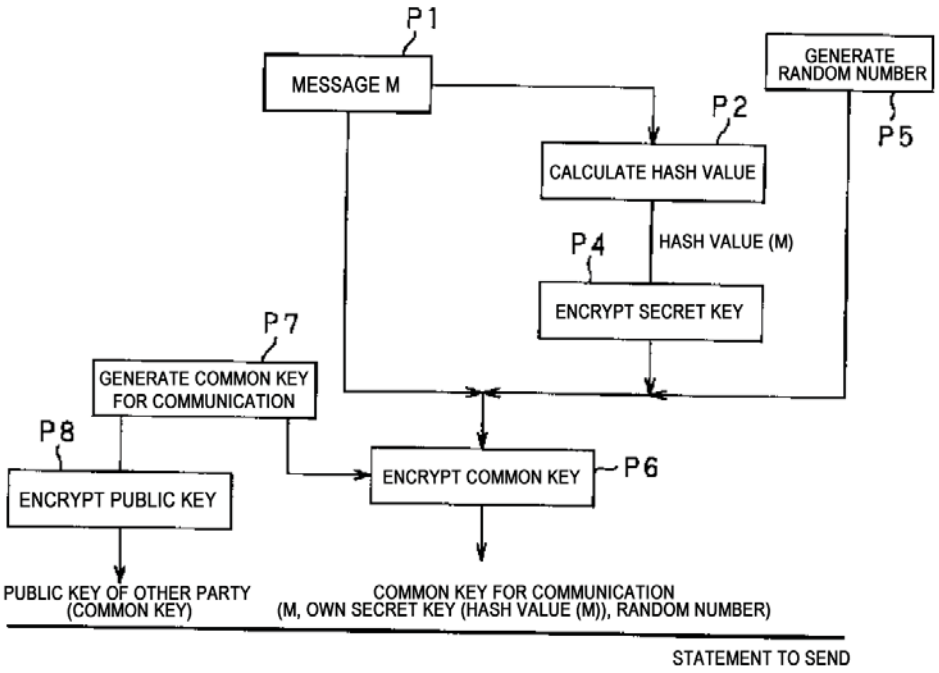

2
62
ADAPTER
3
PLAYER
1
60
4
STORAGE MEDIUM
61

[FIG. 22]

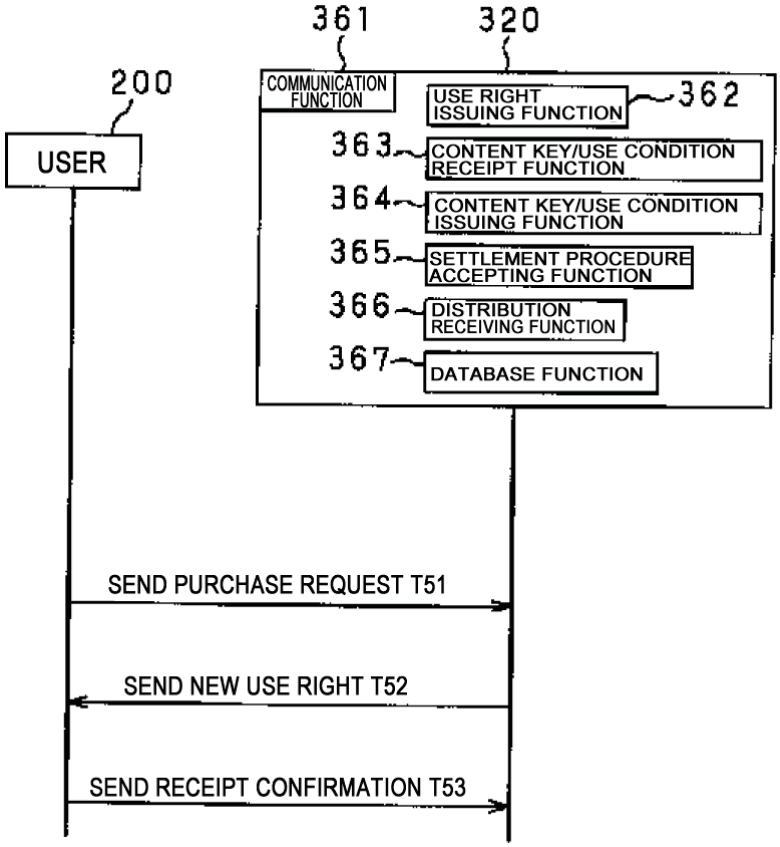


FLOWCHART FOR USER TERMINAL WHEN RETURNING USAGE INFORMATION

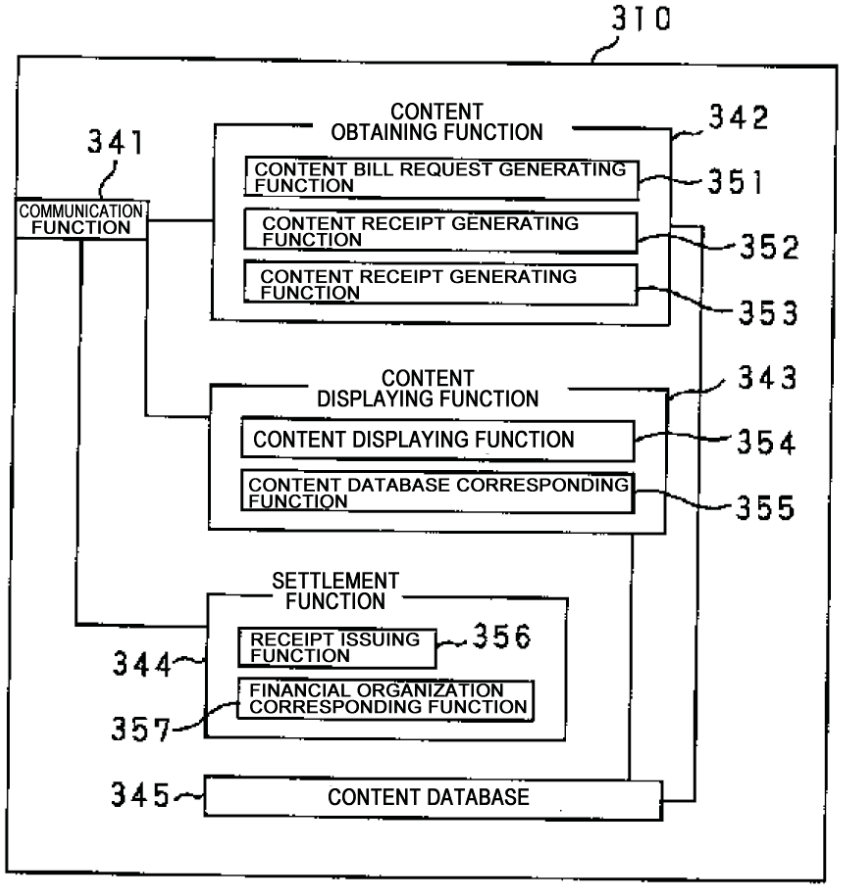
[FIG. 28]



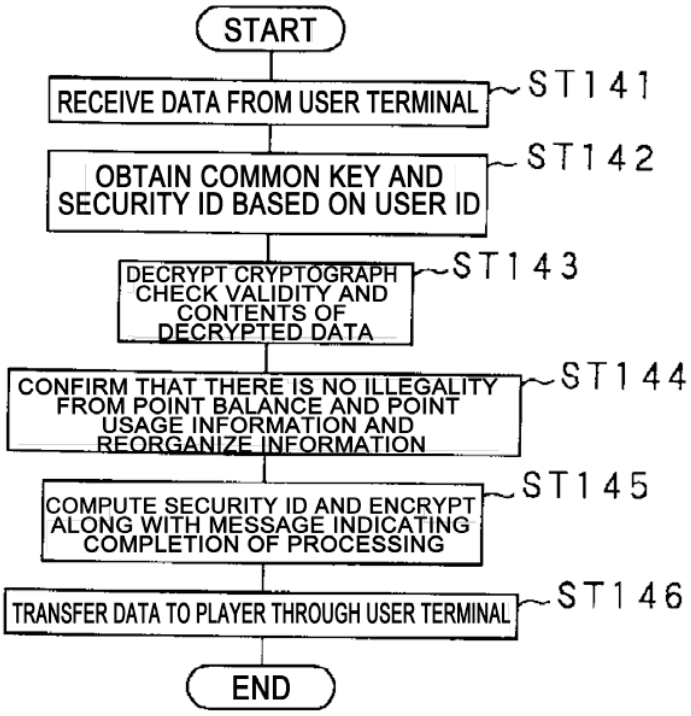
[FIG. 32]


361
320
200
USER
COMMUNICATION FUNCTION
USE RIGHT ISSUING FUNCTION
362
363
CONTENT KEY/USE CONDITION RECEIPT FUNCTION
364
CONTENT KEY/USE CONDITION ISSUING FUNCTION
365
SETTLEMENT PROCEDURE ACCEPTING FUNCTION
366
DISTRIBUTION RECEIVING FUNCTION
367
DATABASE FUNCTION
SEND PURCHASE REQUEST T51
SEND NEW USE RIGHT T52
SEND RECEIPT CONFIRMATION T53

[FIG. 35]

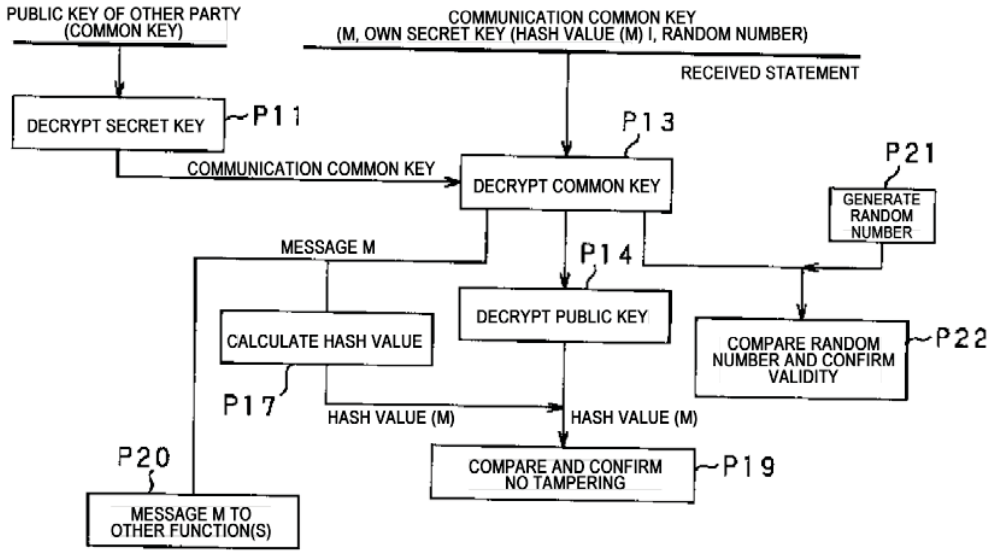

310
341
COMMUNICATION FUNCTION
CONTENT OBTAINING FUNCTION
342
CONTENT BILL REQUEST GENERATING FUNCTION
351
CONTENT RECEIPT GENERATING FUNCTION
352
CONTENT RECEIPT GENERATING FUNCTION
353
CONTENT DISPLAYING FUNCTION
343
CONTENT DISPLAYING FUNCTION
354
CONTENT DATABASE CORRESPONDING FUNCTION
355
SETTLEMENT FUNCTION
RECEIPT ISSUING FUNCTION
356
344
FINANCIAL ORGANIZATION CORRESPONDING FUNCTION
357
345
CONTENT DATABASE

[FIG. 23]

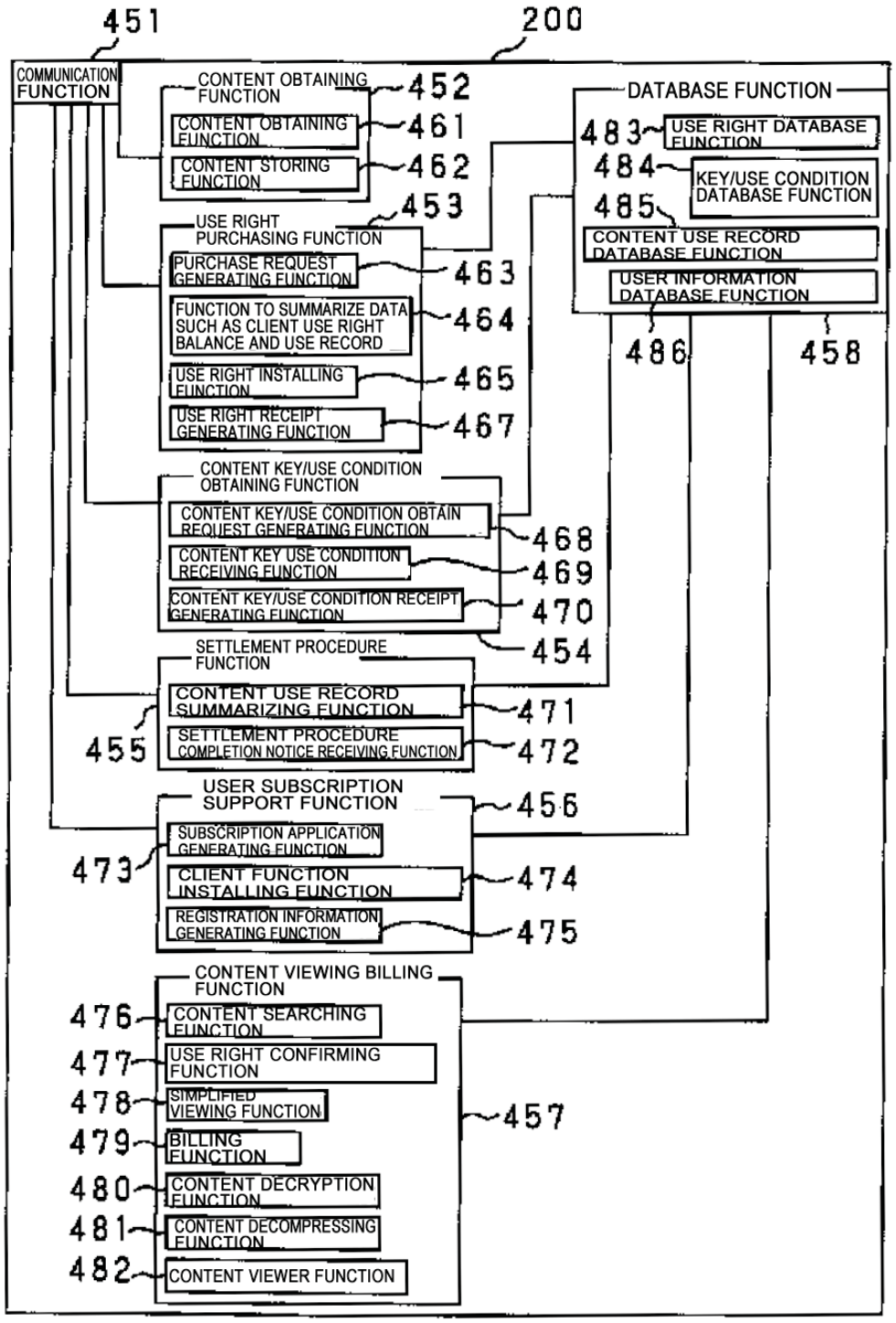


FLOWCHART FOR ADMINISTRATION CENTER WHEN RETURNING USAGE INFORMATION

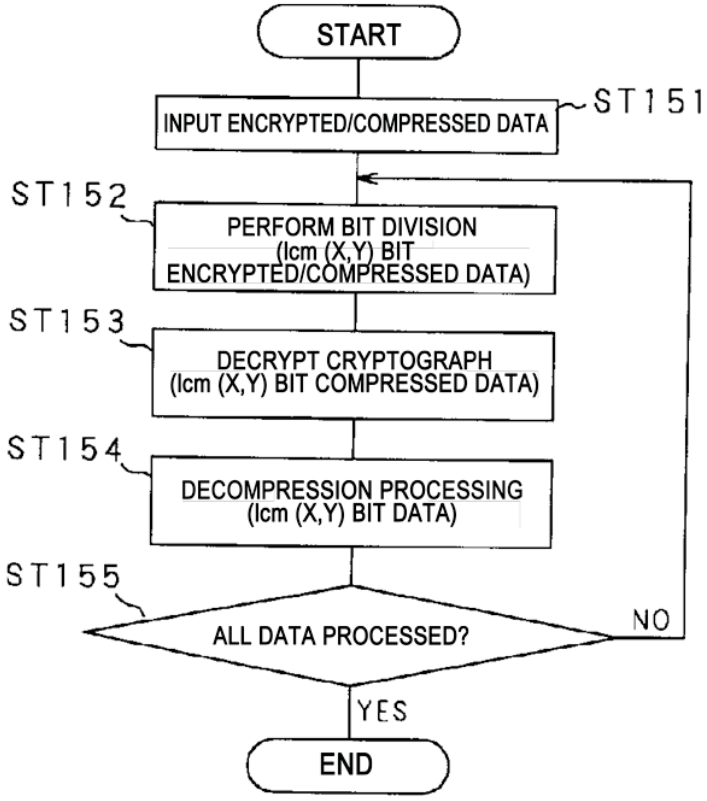
[FIG. 29]



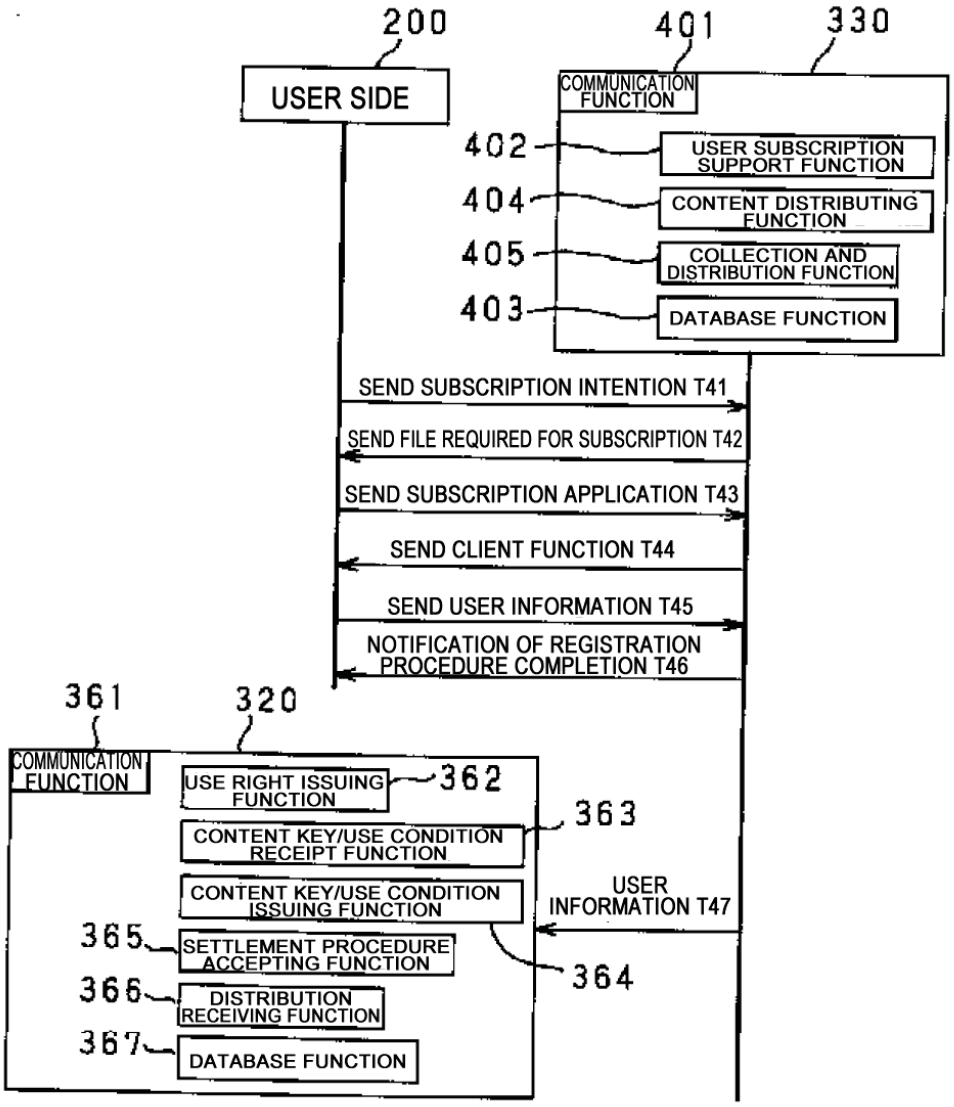
[FIG. 38]


451
200
COMMUNICATION FUNCTION
CONTENT OBTAINING FUNCTION
452
CONTENT OBTAINING FUNCTION
461
CONTENT STORING FUNCTION
462
USE RIGHT PURCHASING FUNCTION
453
PURCHASE REQUEST GENERATING FUNCTION
463
FUNCTION TO SUMMARIZE DATA SUCH AS CLIENT USE RIGHT BALANCE AND USE RECORD
464
USE RIGHT INSTALLING FUNCTION
465
USE RIGHT RECEIPT GENERATING FUNCTION
467
CONTENT KEY/USE CONDITION OBTAINING FUNCTION
CONTENT KEY/USE CONDITION OBTAIN REQUEST GENERATING FUNCTION
468
CONTENT KEY USE CONDITION RECEIVING FUNCTION
469
CONTENT KEY/USE CONDITION RECEIPT GENERATING FUNCTION
470
454
SETTLEMENT PROCEDURE FUNCTION
CONTENT USE RECORD SUMMARIZING FUNCTION
471
455
SETTLEMENT PROCEDURE COMPLETION NOTICE RECEIVING FUNCTION
472
USER SUBSCRIPTION SUPPORT FUNCTION
456
SUBSCRIPTION APPLICATION GENERATING FUNCTION
473
CLIENT FUNCTION INSTALLING FUNCTION
474
REGISTRATION INFORMATION GENERATING FUNCTION
475
CONTENT VIEWING BILLING FUNCTION
476
CONTENT SEARCHING FUNCTION
477
USE RIGHT CONFIRMING FUNCTION
478
SIMPLIFIED VIEWING FUNCTION
479
BILLING FUNCTION
480
CONTENT DECRYPTION FUNCTION
481
CONTENT DECOMPRESSING FUNCTION
482
CONTENT VIEWER FUNCTION
457
DATABASE FUNCTION
483
USE RIGHT DATABASE FUNCTION
484
KEY/USE CONDITION DATABASE FUNCTION
485
CONTENT USE RECORD DATABASE FUNCTION
USER INFORMATION DATABASE FUNCTION
486
458

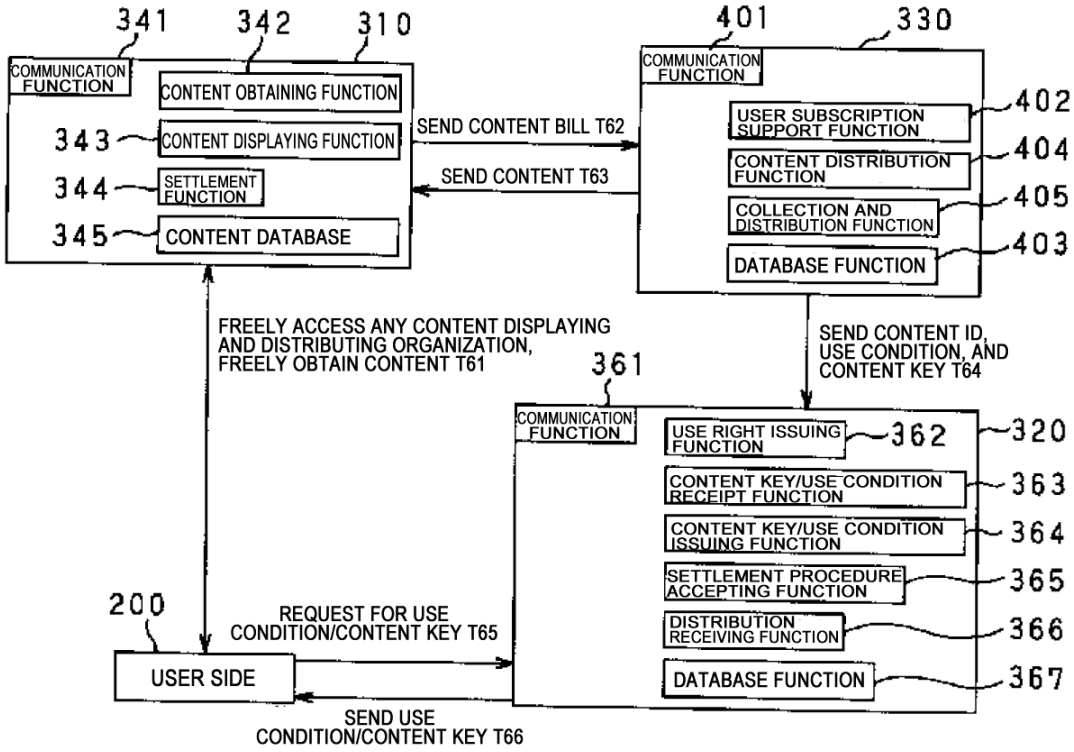
[FIG. 25]


START
INPUT ENCRYPTED/COMPRESSED DATA
ST151
ST152
PERFORM BIT DIVISION (lcm (X,Y) BIT ENCRYPTED/COMPRESSED DATA)
ST153
DECRYPT CRYPTOGRAPH (lcm (X,Y) BIT COMPRESSED DATA)
ST154
DECOMPRESSION PROCESSING (lcm (X,Y) BIT DATA)
ST155
ALL DATA PROCESSED?
NO
YES
END

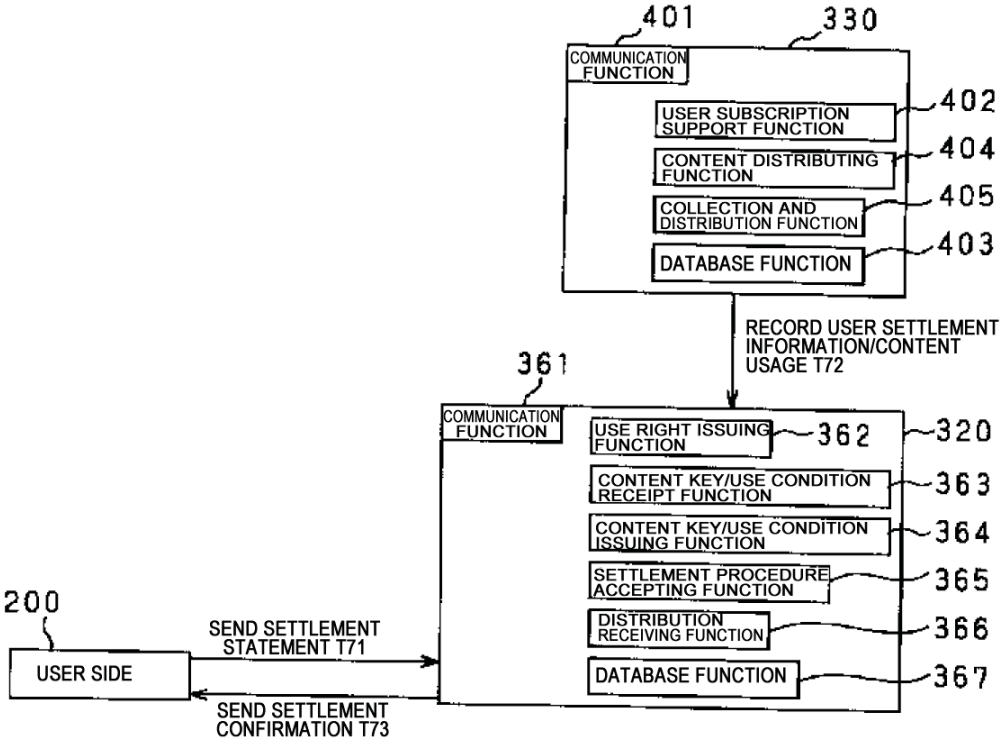
[FIG. 31]


200
USER SIDE
401
COMMUNICATION FUNCTION
330
402
USER SUBSCRIPTION SUPPORT FUNCTION
404
CONTENT DISTRIBUTING FUNCTION
405
COLLECTION AND DISTRIBUTION FUNCTION
403
DATABASE FUNCTION
SEND SUBSCRIPTION INTENTION T41
SEND FILE REQUIRED FOR SUBSCRIPTION T42
SEND SUBSCRIPTION APPLICATION T43
SEND CLIENT FUNCTION T44
SEND USER INFORMATION T45
NOTIFICATION OF REGISTRATION PROCEDURE COMPLETION T46
361
320
COMMUNICATION FUNCTION
USE RIGHT ISSUING FUNCTION
362
CONTENT KEY/USE CONDITION RECEIPT FUNCTION
363
CONTENT KEY/USE CONDITION ISSUING FUNCTION
USER INFORMATION T47
365
SETTLEMENT PROCEDURE ACCEPTING FUNCTION
364
366
DISTRIBUTION RECEIVING FUNCTION
367
DATABASE FUNCTION

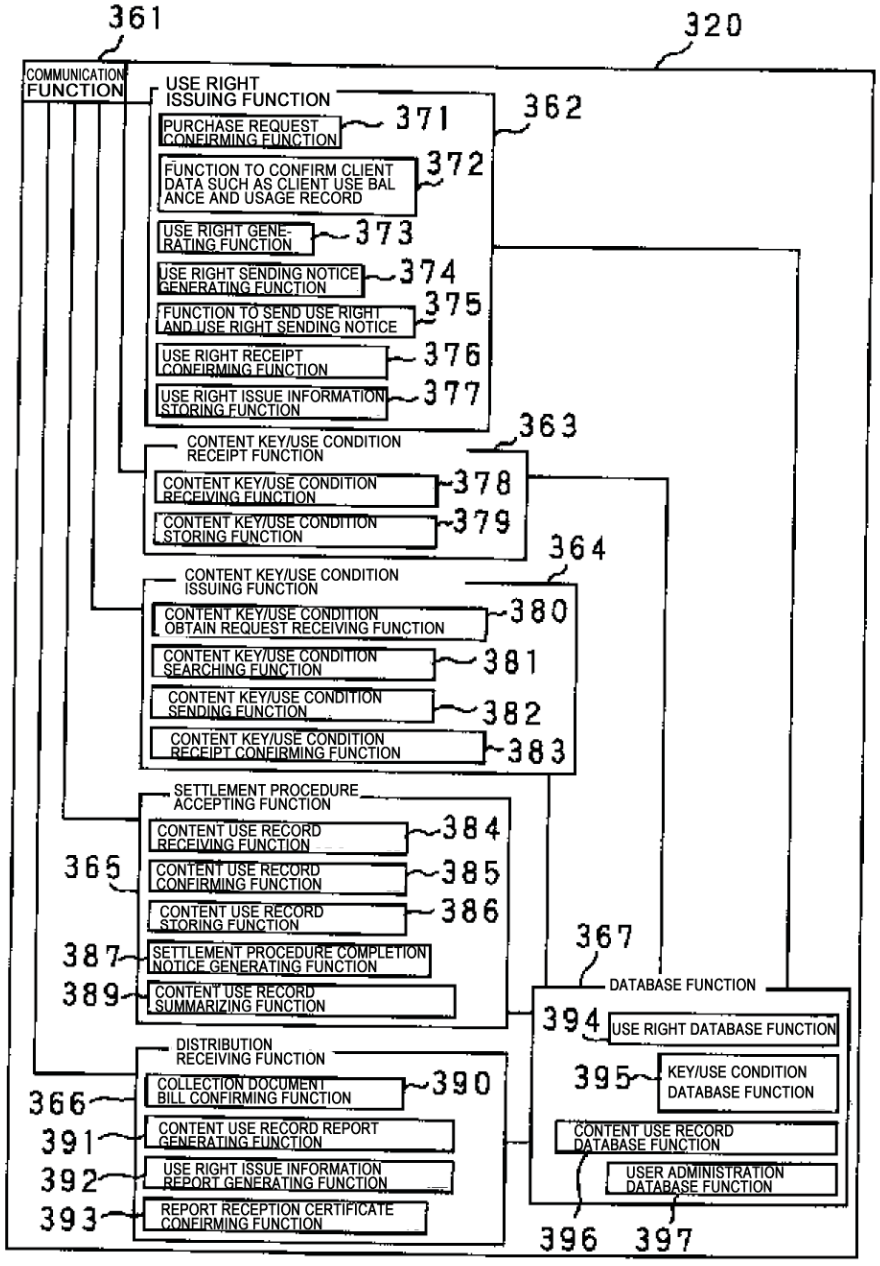
[FIG. 33]


341
342
310
401
330
COMMUNICATION FUNCTION
CONTENT OBTAINING FUNCTION
343
CONTENT DISPLAYING FUNCTION
344
SETTLEMENT FUNCTION
345
CONTENT DATABASE
SEND CONTENT BILL T62
SEND CONTENT T63
COMMUNICATION FUNCTION
USER SUBSCRIPTION SUPPORT FUNCTION
402
CONTENT DISTRIBUTION FUNCTION
404
COLLECTION AND DISTRIBUTION FUNCTION
405
DATABASE FUNCTION
403
FREELY ACCESS ANY CONTENT DISPLAYING AND DISTRIBUTING ORGANIZATION, FREELY OBTAIN CONTENT T61
SEND CONTENT ID, USE CONDITION, AND CONTENT KEY T64
361
COMMUNICATION FUNCTION
USE RIGHT ISSUING FUNCTION
362
320
CONTENT KEY/USE CONDITION RECEIPT FUNCTION
363
CONTENT KEY/USE CONDITION ISSUING FUNCTION
364
SETTLEMENT PROCEDURE ACCEPTING FUNCTION
365
DISTRIBUTION RECEIVING FUNCTION
366
DATABASE FUNCTION
367
200
USER SIDE
REQUEST FOR USE CONDITION/CONTENT KEY T65
SEND USE CONDITION/CONTENT KEY T66

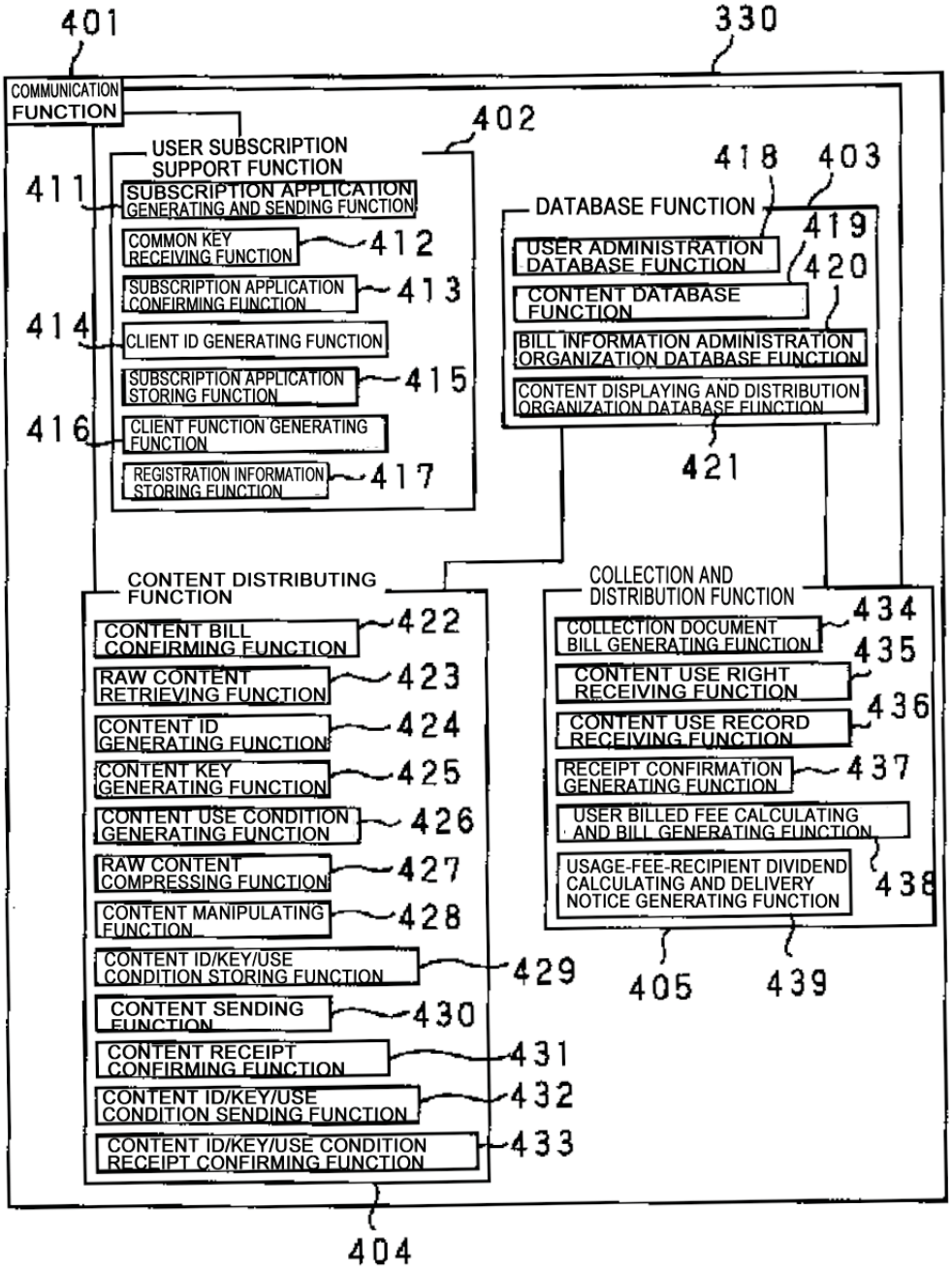
[FIG. 34]


401
330
COMMUNICATION FUNCTION
USER SUBSCRIPTION SUPPORT FUNCTION
402
CONTENT DISTRIBUTING FUNCTION
404
COLLECTION AND DISTRIBUTION FUNCTION
405
DATABASE FUNCTION
403
RECORD USER SETTLEMENT INFORMATION/CONTENT USAGE T72
361
COMMUNICATION FUNCTION
USE RIGHT ISSUING FUNCTION
362
320
CONTENT KEY/USE CONDITION RECEIPT FUNCTION
363
CONTENT KEY/USE CONDITION ISSUING FUNCTION
364
SETTLEMENT PROCEDURE ACCEPTING FUNCTION
365
DISTRIBUTION RECEIVING FUNCTION
366
DATABASE FUNCTION
367
200
USER SIDE
SEND SETTLEMENT STATEMENT T71
SEND SETTLEMENT CONFIRMATION T73

[FIG. 36]


361
320
COMMUNICATION FUNCTION
USE RIGHT ISSUING FUNCTION
362
PURCHASE REQUEST CONFIRMING FUNCTION
371
FUNCTION TO CONFIRM CLIENT DATA SUCH AS CLIENT USE BALANCE AND USAGE RECORD
372
USE RIGHT GENERATING FUNCTION
373
USE RIGHT SENDING NOTICE GENERATING FUNCTION
374
FUNCTION TO SEND USE RIGHT AND USE RIGHT SENDING NOTICE
375
USE RIGHT RECEIPT CONFIRMING FUNCTION
376
USE RIGHT ISSUE INFORMATION STORING FUNCTION
377
CONTENT KEY/USE CONDITION RECEIPT FUNCTION
363
CONTENT KEY/USE CONDITION RECEIVING FUNCTION
378
CONTENT KEY/USE CONDITION STORING FUNCTION
379
CONTENT KEY/USE CONDITION ISSUING FUNCTION
364
CONTENT KEY/USE CONDITION OBTAIN REQUEST RECEIVING FUNCTION
380
CONTENT KEY/USE CONDITION SEARCHING FUNCTION
381
CONTENT KEY/USE CONDITION SENDING FUNCTION
382
CONTENT KEY/USE CONDITION RECEIPT CONFIRMING FUNCTION
383
SETTLEMENT PROCEDURE ACCEPTING FUNCTION
365
CONTENT USE RECORD RECEIVING FUNCTION
384
CONTENT USE RECORD CONFIRMING FUNCTION
385
CONTENT USE RECORD STORING FUNCTION
386
387
SETTLEMENT PROCEDURE COMPLETION NOTICE GENERATING FUNCTION
389
CONTENT USE RECORD SUMMARIZING FUNCTION
367
DATABASE FUNCTION
394
USE RIGHT DATABASE FUNCTION
395
KEY/USE CONDITION DATABASE FUNCTION
CONTENT USE RECORD DATABASE FUNCTION
USER ADMINISTRATION DATABASE FUNCTION
396
397
DISTRIBUTION RECEIVING FUNCTION
366
COLLECTION DOCUMENT BILL CONFIRMING FUNCTION
390
391
CONTENT USE RECORD REPORT GENERATING FUNCTION
392
USE RIGHT ISSUE INFORMATION REPORT GENERATING FUNCTION
393
REPORT RECEPTION CERTIFICATE CONFIRMING FUNCTION

[FIG. 37]


401
330
COMMUNICATION FUNCTION
402
USER SUBSCRIPTION SUPPORT FUNCTION
411
SUBSCRIPTION APPLICATION GENERATING AND SENDING FUNCTION
COMMON KEY RECEIVING FUNCTION
412
SUBSCRIPTION APPLICATION CONFIRMING FUNCTION
413
414
CLIENT ID GENERATING FUNCTION
SUBSCRIPTION APPLICATION STORING FUNCTION
415
416
CLIENT FUNCTION GENERATING FUNCTION
REGISTRATION INFORMATION STORING FUNCTION
417
418
403
DATABASE FUNCTION
419
USER ADMINISTRATION DATABASE FUNCTION
420
CONTENT DATABASE FUNCTION
BILL INFORMATION ADMINISTRATION ORGANIZATION DATABASE FUNCTION
CONTENT DISPLAYING AND DISTRIBUTION ORGANIZATION DATABASE FUNCTION
421
CONTENT DISTRIBUTING FUNCTION
CONTENT BILL CONFIRMING FUNCTION
422
RAW CONTENT RETRIEVING FUNCTION
423
CONTENT ID GENERATING FUNCTION
424
CONTENT KEY GENERATING FUNCTION
425
CONTENT USE CONDITION GENERATING FUNCTION
426
RAW CONTENT COMPRESSING FUNCTION
427
CONTENT MANIPULATING FUNCTION
428
CONTENT ID/KEY/USE CONDITION STORING FUNCTION
429
CONTENT SENDING FUNCTION
430
CONTENT RECEIPT CONFIRMING FUNCTION
431
CONTENT ID/KEY/USE CONDITION SENDING FUNCTION
432
CONTENT ID/KEY/USE CONDITION RECEIPT CONFIRMING FUNCTION
433
404
COLLECTION AND DISTRIBUTION FUNCTION
434
COLLECTION DOCUMENT BILL GENERATING FUNCTION
435
CONTENT USE RIGHT RECEIVING FUNCTION
436
CONTENT USE RECORD RECEIVING FUNCTION
437
RECEIPT CONFIRMATION GENERATING FUNCTION
USER BILLED FEE CALCULATING AND BILL GENERATING FUNCTION
USAGE-FEE-RECIPIENT DIVIDEND CALCULATING AND DELIVERY NOTICE GENERATING FUNCTION
438
405
439