UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	080379-000110US
First Inventor	RACZ, Patrick
Title	DATA STORAGE AND ACCESS SYSTEMS
Filed via USPTO Website.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form** (e.g., PTO/SB/17)
   (Submit an original and a duplicate for fee processing)
2. ☒ **Applicant claims small entity status.**
   See 37 CFR 1.27.
3. ☒ **Specification** [*Total Pages* (incl cover sheet) 50]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. ☒ **Drawing(s)** *(35 U.S.C.113)* [*Total Sheets* 17]
5. **Oath or Declaration** [*Total Sheets* _____]
   a. ☐ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63 (d))
   (for a continuation/divisional with Box 18 completed)
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☒ **Application Data Sheet.** See 37 CFR 1.76
7. ☐ **CD-ROM** or **CD-R** in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a. - c. are required)
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria, VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. ☐ **Assignment Papers** (cover sheet (PTO-1595) & document(s))
   Name of Assignee _____
10. ☐ **37 CFR 3.73(b) Statement** *(when there is an assignee)* ☐ **Power of Attorney**
11. ☐ **English Translation Document** *(if applicable)*
12. ☐ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of foreign patent documents, publications, & other information
13. ☐ **Preliminary Amendment**
14. ☐ **Return Receipt Postcard** (MPEP 503)
    (Should be specifically itemized)
15. ☐ **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. ☐ **Nonpublication Request** under 35 U.S.C. 122 (b)(2)(B)(i).
    Applicant must attach form PTO/SB/35 or its equivalent.
17. ☐ Other: _____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☒ No Fee Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: 11/336,758

Prior application information: *Examiner* Steve S. PAIK *Art Unit:* 2876

19. CORRESPONDENCE ADDRESS

☒ The address associated with Customer Number: **20350** *OR* ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature		Date	January 15, 2008
Name (Print/Type)	Jason D. Lohr	Registration No. (Attorney/Agent)	48,163

61257843 v1

CONTINUATION PATENT APPLICATION

DATA STORAGE AND ACCESS SYSTEMS

Inventor(s): Patrick RACZ, a citizen of the United Kingdom, residing at
19 Royal Square, Saint Heller, Jersey JE1 4WA

Entity: Small

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200

DATA STORAGE AND ACCESS SYSTEMS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. Patent Application No. 11/336,758, filed on January 19, 2006; which is a continuation of U.S. Patent Application No. 10/111,716, filed on September 17, 2002, which application is a national stage application under 35 U.S.C. 371, claiming the priority of international PCT Application No. GB00/04110, filed on October 25, 2000; which claims priority to UK Application No. 9925227.2 filed on October 25, 1999, each of which is incorporated by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

[0002] This invention is generally concerned with data storage and access systems. More particularly, it relates to a portable data carrier for storing and paying for data and to computer systems for providing access to data to be stored. The invention also includes corresponding methods and computer programs. The invention is particularly useful for managing stored audio and video data, but may also be applied to storage and access of text and software, including games, as well as other types of data.

[0003] One problem associated with the increasingly wide use of the internet is the growing prevalence of so-called data pirates. Such pirates obtain data either by unauthorized or legitimate means and then make this data available essentially world-wide over the internet without authorization. Data can be a very valuable commodity, but once it has been published on the internet it is difficult to police access to and use of it by internet users who may not even realize that it is pirated. This is a particular problem with audio recordings, and, once the bandwidth becomes available, is also likely to be evident with video.

[0004] Over the past three or four years compressed audio sources have become increasingly widely available on web pages. One widely used audio data compression format is MP3 (MPEG - Audio Layer 3 of the MPEG1 compression algorithm), which is an internationally defined standard including a definition of compressed audio information such as speech or music. It relies on psycho-acoustic properties of human hearing to achieve very large data compression factors. It is thus feasible to download usefully long passages of music in a practically convenient short time. Pirate data suppliers have not been slow to realize the potential of this, and many unauthorized websites have sprung up offering popular

industry considerable concern and there is an urgent need to find a way to address the problem of data piracy.

SUMMARY OF THE INVENTION

[0005] According to the present invention there is therefore provided a method of providing portable data comprising providing a portable data storage device comprising downloaded data storage means and payment validation means; providing a terminal for internet access; coupling the portable data storage device to the terminal; reading payment information from the payment validation means using the terminal; validating the payment information; and downloading data into the portable storage device from a data supplier.

[0006] Another aspect of the invention provides a corresponding mobile data retrieval device for retrieving and outputting data such as stored music and/or noise from the data storage device.

[0007] The payment validation means is, for example, means to validate payment with an external authority such as a bank or building society. The combination of the payment validation means with the data storage means allows the access to the downloaded data which is to be stored by the data storage means, to be made conditional upon checked and validated payment being made for the data. Binding the data access and payment together allows the legitimate owners of the data to make the data available themselves over the internet without fear of loss of revenue, thus undermining the position of data pirates.

[0008] A further advantage of the system is that it allows users under the age of 18 to make internet purchases. Currently internet users pay for goods and/or services by credit card. Since credit cards cannot legitimately be used by persons under the age of 18 (at least in the UK), a significant fraction of adventurous internet users are excluded from e-commerce, one of the most significant predicted uses of the internet. In one embodiment of the invention, however, the payment validation means comprises e-cash; that is, the payment validation means stores transaction value information on a cash value of transactions validatable by the data storage means. In simple terms, the data storage means can be a card which is charged up to a desired cash value (if necessary limited to a maximum value) at a suitable terminal. This might be an internet access terminal but could, more simply, be a device to accept the data storage card and to receive and count money deposited by the user to charge the card, writing update cash value information onto the card. More sophisticated ways of updating the cash value on the card are also possible, such as direct bank transfer. Since, with this type

of embodiment, the data storage means is, essentially, precharged with cash rather than acting as a credit card, it can be used by young people without the risk of their incurring large debts.

[0009] In one embodiment the data storage means is powered by the retrieval device when it is connected to the device and retains a memory of the downloaded data when it is unpowered. This can be achieved by the use of Flash RAM or, more generally, any form of programmable read-only memory. Alternatively the data storage means may incorporate a rechargeable cell or capacitor and store information in battery backed-up static RAM.

[0010] The downloaded data may be entered into the data storage device by means of an interface such as a magnetically or capacitatively coupled connection or an optical connection, but preferably the interface comprises contacts for direct electrical connection to the storage means. The payment validation means may likewise have one of a variety of interfaces but again preferably comprises a set of electrical contacts. The payment validation means could, however, comprise a magnetic or holographic data-strip such as is known for use with credit cards and phone cards. The interface to receive the downloaded data may be separate from the interface to the payment validation means, to facilitate separate and simultaneous access to both these systems. In other embodiments a single interface may serve for both data storage and payment. Advantageously the payment validation means includes a memory storing information to identify the person who is paying for the downloaded data.

[0011] For additional security the downloaded data may be encrypted. In this case data decryption may be necessary at some stage, either in the data storage means or in the retrieval device or in an information delivering apparatus such as a data access terminal. Alternatively the data decryption function can be shared amongst one or more of these devices. The skilled person will be aware of a range of suitable encryption/decryption techniques, including Pretty Good Privacy (Registered Trade Mark) and PKI (Public Key Infrastructure). Normally when the downloaded data is encrypted a decryption key must be supplied. This can be generated automatically by the data access terminal or data access service provider or it can be entered by the user into the data access terminal or into the mobile data retrieval device.

[0012] The data storage means and/or the retrieval device can be provided with access control means to prevent unauthorized access to the downloaded data. Additionally or alternatively, use control means can be provided to stop or provide only limited access of the user to the downloaded data in accordance with the amount paid. These access and use

control functions may in some embodiments be combined, permitted use controlling access or permitted access controlling use. Thus, for example, a complete set of data information relating to a particular topic, a particular music track, or a particular software package might be downloaded, although access to part of the data set might thereafter be controlled by payments made by a user at a later stage. In this way, a user could pay to enable an extra level on a game or to enable further tracks of an album.

[0013] In embodiments where the access or use control means is responsive to the payment validation means, access or use control information may be stored with the downloaded data or in a separate storage area, for example in the payment validation means. The user's access to the downloaded data could advantageously be responsive to the payment validation means, for example, by means of a control line coupling the payment validation means with a memory access or decryption control element.

[0014] In one embodiment the data storage means comprises an electronic memory card or smart card and the mobile data retrieval device is provided with a slot to receive the card. Preferably the card is a push-fit within the retrieval device, and retention of the card may be effected by pressure from electrical interface connections and/or resilience of the housing, or by using a resilient retaining means. In a preferred embodiment the retrieval device includes an audio output and a display, to play a downloaded track and to show information about the track and/or an accompanying video.

[0015] To download data onto the data storage means the user can employ a data access terminal coupled to the internet. The terminal can directly validate payment; for example in the case of a smart card charged with electronic cash it can deduct a cash value from the card. Alternatively it can communicate with a bank or other financial services provider to control payment. In a preferred embodiment, however, the terminal connects to a data access service provider which provides a portal to other sites and which validates payment and then forwards data from a data supplier to the user's local access terminal. The data access service provider may alternatively forward payment validation information and/or information from the payment validation authority to the data supplier for control by the supplier of the data supplied. Thus, access to the payment validation system and/or data for downloading may be entirely controlled by the data supplier.

[0016] Data held on the data storage means may advantageously include data relating to the user's or payer's usage of the system. This information may include, for example,

information on a user's spending pattern, information on data suppliers used and information on the downloaded data. This information may be accessed by the data supplier and/or data access service provider and can be used for targeted marketing or loyalty-based incentive schemes such as air miles or the like.

[0017] The data access terminal may be a conventional computer or, alternatively, it may be a mobile phone. Wireless Application Protocol (WAP) and i-mode allow mobile phones to efficiently access the internet and this allows a mobile phone to be used to download data to the data storage means, advantageously, directly. The data storage means can, if desired, incorporate the functionality of a mobile phone SIM (Subscriber Identity Module) card, which cards already include a user identification means, to allow user billing through the phone network operator.

[0018] In a preferred embodiment the downloaded data is MP3 or other encoded audio data, but the system finds more general application for other data types. For example, download data can include software, and particularly games, share price information, current news information, transport timetable information, weather information and catalog shopping information. The downloaded information may also include compressed video data. The storage capacity of the data storage means is adaptable to suit the type of data intended to be downloaded; for example, 32 megabytes is sufficient for CD quality music, but for video it is preferable that the data storage means has a capacity of 128 megabytes or greater.

[0019] In another aspect, the invention provides a portable data carrier comprising an interface for reading and writing data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; non-volatile payment data memory, coupled to the interface, for providing payment data to an external device.

[0020] These features allow the data carrier to store both payment data and content data, thus providing the advantages outlined above. Depending upon the payment system used, the payment data memory may also store code for validating or confirming a payment to an external payment system. The payment data will normally be linked to a card or card holder identification data for payment by the card holder. The non-volatile memory ensures that stored content and payment data is retained in the data carrier when the data carrier is not receiving power from an external source. Thus "non-volatile" encompasses, for example, low-power memory whose contents are retained by a battery back-up system. In one embodiment the payment data memory comprises EEPROM and the content data memory

comprises Flash memory, but other types of content data memory, such as optical, for example, holographic, data memory can also be used. The data carrier may also be integrated into other apparatus, such as a mobile communications device.

[0021] Preferably, the portable data carrier further comprises a program store for storing code implementable by a processor; and a processor, coupled to the content data memory, the payment data memory, the interface and to the program store for implementing code in the program store, wherein the code comprises code to output payment data from the payment data memory to the interface and code to provide external access to the data memory.

[0022] Normally, the (content) data memory allows both write and read access for both storing and retrieving data, but in some embodiments the content data memory may be read-only memory (ROM). In such embodiments, content may be pre-loaded onto the carrier and payment may then be made for permission to access the pre-loaded data.

[0023] Preferably, the data carrier also stores a record of access made to the content data and updates this in response to external access, preferably read access, made to the data memory. The carrier may also store content use rules pertaining to allowed use of stored data items. These use rules may be linked to payments made from the card to provide payment options such as access to buy content data outright; rental access to content data for a time period or for a specified number of access events; and/or rental/purchase, for example where rental use is provided together with an option to purchase content data at the reduced price after rental access has expired.

[0024] Thus where the data carrier stores, for example, music, the purchase outright option may be equivalent to the purchase of a compact disc (CD), preferably with some form of content copy protection such as digital watermarking. In this example, the rental or subscription payment option may be a pay-per-play option, and with this option payment may either be before or after access to the stored data so that the carrier may operate in either a debit or credit payment mode.

[0025] The portability of the data carrier potentially allows it to be used to access content or, in the example, play music without the need to be linked to a communications system or to be on-line to the internet. By providing a use record memory on the data carrier, use of the stored data can be tracked while ff-line and then any necessary payment can be made when the data carrier is next coupled to a communication system. This allows the data carrier to operate in a credit mode. In a debit mode, the additional storage of use rules facilitates the

regulation of access to content data stored on the carrier without the need for further exchange of payment/use data with an external system to validate the use.

[0026] By combining digital rights management with content data storage using a single carrier, the stored content data becomes mobile and can be accessed anywhere while retaining control over the stored data for the data content provider or data copyright owner. Preferably, the data carrier also stores access control data, such as a user ID and a password, as the stored data may be valuable. The access control data may be combined with access control to the payment data, which is typically by means of a PIN (Personal Identification Number) to simplify access to valued content stored on the carrier.

[0027] In one embodiment the stored content data is encrypted and a unique password or PIN and/or biometric data is required for decryption. The data carrier may be arranged so that the content is erased after a predetermined number of incorrect access attempts. Additionally or alternatively, a permanently stored flag may be set and/or a hardware modification (such as a fusable link) may be made to prevent the data carrier from functioning for further data storage/retrieval. Preferably, however, access to any stored value/payment data is nevertheless retained.

[0028] Supplementary data may also be stored on the carrier in association with stored content data. This supplementary data may comprise customer reward management data and/or advertising data. The supplementary data may comprise a pointer to an external data source from which data is downloaded either to the data carrier or to a data access device or content player, so that advertising or other data can be displayed when reviewing or accessing the stored content.

[0029] Additional data security and/or a mechanism for rewarding operators at different levels in the data supply chain may be provided using a content synthesis function. The content synthesis function combines partial content information from two or more sources to provide content data items for storage and/or output. Thus, for example, a first percentage of a content data item could be provided by a content retailer, while a remaining percentage could be provided by an on-line data supplier. This would provide an incentive for a user to register with a content retailer or distributor as well as with an on-line system owner and so could encourage the use of existing retailers and could provide a mechanism for paying commission to such retailers. The two portions of data combined to provide a content data item could comprise encryption data and a key but preferably comprise separate parts of a

complete data item, for example, least significant bits and most significant bits or high frequencies and low frequencies (for audio). This arrangement also facilitates customer reward and loyalty management.

[0030] In one embodiment the data carrier further comprises memory for storing data for accessing a mobile communications network, for example to receive content data over the network. For such an embodiment, the data carrier may replace a SIM (Subscriber Identity Module) card in a mobile communications device, thus providing a single card for both network access and valued content retrieval and storage. Additionally or alternatively the card may also store the web address of a data supplier from whom data may be downloaded onto the carrier.

[0031] The data memory for storing content data may be optic, magnetic or semiconductor memory, but preferably comprises Flash memory. Preferably, the data memory has a large capacity for storing large data files such as compressed video data. Preferably, the data memory is partitioned for lock access, that is, for read and/or write access to blocks of, for example, 1K, 4K, 16K or 64K databytes for faster data access, particularly where the stored content data will normally be accessed serially, as is normally the case with audio and video data. Preferably the card is configured as an IC card or smart card and has a credit card-type format, although other formats such as the "memory stick" format may also be used. This provides a small and convenient portable format and facilitates removable interfacing with a variety of devices.

[0032] The invention also provides a related method of controlling access to data on a data carrier, the data carrier comprising non-volatile data memory and non-volatile parameter memory storing use status data and use rules, the method comprising receiving a data access request; reading the use status data and use rules from memory; and evaluating the use status data using the use rules to determine whether access to the stored data is permitted.

[0033] According to another aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a pointer to a data provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item

from the requester; code to receive from the communications interface payment data comprising data relating to payment for the requested data item; code responsive to the request and to the received payment data, to read data for the requested data item from a content provider; and code to transmit the read data to the requester over the communications interface.

[0034] The computer system is operated by a data supplier or data supply "system owner" for providing content data to the data carrier described above. The payment data received may either be data relating to an actual payment made to the data supplier, or it may be a record of a payment made to an e-payment system relating either to a payment to the data supplier, or to a payment to a third party. The data from the content provider, preferably without permanent (local) storage of the forwarded data, improves data security as the content provider retains control over a content data item, and the data supplier, a copy of a data item, is unable to supply data for the item without the content provider's assistance. The computer system may provide temporary storage for a requested data item, for example using a disk cache, but preferably the computer system does not store a complete data item, even temporarily.

[0035] Preferably, the computer system includes payment distribution information so that when payment is made for a data item, the payment can be distributed for reimbursing royalties and making other payments. Typically a large fraction of the payment for a data item will be transferred to a copyright owner or "content provider" for the item while smaller payments will go to the artist and/or publisher and/or retailer/distributor. Payment may be made directly by the computer system to the computer systems of other relevant parties using, for example, a signature-transporting type e-payment system. Alternatively, the computer system can issue appropriate instructions to a third party e-payment system for making the transfers. The computer system allows automatic distribution of payments either before, during or after content data download, or after content data access by a user. Instructions for distributing the payments may be issued substantially simultaneously, thereby avoiding long delays in the payment of some parties; for example, it can presently take a year or more for an artist generating content to be paid by conventional methods.

[0036] Preferably, the computer system also stores content data item access rule data, for downloading in association with a content data item. The rule data may be stored by a content provider but is preferably held by the computer system, and links a content identifier

with an access rule, typically based upon a required payment value, as outlined above in the context of the data carrier. Normally, each content data item will have an associated access rule, but a single rule may apply to a large number of data items. The computer system also, preferably, stores requester reward data for customer reward/loyalty management. This data may again comprise one or more rules linking a payment value and/or content data item type to a specified reward, such as a number of air miles or retailer value points. The computer system preferably also keeps a record of an identified user's or data's carriers content item downloads and payments for market research purposes.

[0037] The computer system, in one embodiment, also stores access control data, such as an access request identity and password which can be employed, for example, to create an extranet of system users, which again can be linked to stored access record data for marketing purposes. When further linked to content item type data, such an arrangement can be used to construct a club of users of content data items of a particular type, for example country and western or rock and roll music. As described in connection with the portable data carrier, the computer system may also comprise content synthesis code for additional data security and for more secure management of payment distributions.

[0038] The invention also provides a related method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; reading the requested data from a content provider responsive to the received payment data; and transmitting the read data to the requester.

[0039] According to a further aspect of the present invention, there is provided a data access terminal for retrieving data from a data supplier and providing the retrieved data to a data carrier, the terminal comprising a first interface for communicating with the data supplier; a data carrier interface for interfacing with the data carrier; a program store storing code implementable by a processor; and a processor, coupled to the first interface, the data carrier interface and to the program store for implementing the stored code, the code comprising: code to read payment data from the data carrier and to forward the payment data to a payment validation system; code to receive payment validation data from the payment validation system; code responsive to the payment validation data to retrieve data from the data supplier and to write the retrieved data into the data carrier.

[0040] This terminal can be used for retrieving data from the above-described computer system and for downloading the retrieved data to the above-described portable data carrier. As with the data supply computer system, it is preferable that there is no (local) storage of content item data forwarded from the data supplier to the data carrier. The data access terminal is not restricted to use with the above-described status supplier and could, for example, retrieve data for downloading to the data carrier from a local data source, such as a CD (Compact Disc) or DVD (Digital Versatile Disc), or from a third party such as a cable TV company.

[0041] The terminal reads payment data from the data carrier and transmits this to a payment validation system for validating the data and authorizing the payment. This may be part of the data supplier's computer system or it may be a separate system such as an e-payment system. Thus, the terminal operates with a data carrier storing payment (validation) data and, in some embodiments, additional payment validation code for validating payment to the payment validation system. Again, the terminal is preferably configured to provide a data item use rule to the carrier in conjunction with a data item. As before, the data item use rule will normally be dependent upon payment value information embodied in the payment data read from the data carrier. The terminal is preferably also configured for user input of access control data. This access control data may be forwarded to the data carrier for access permission verification and/or it may be passed to the data supplier computer system for a similar purpose. The terminal may be configured to warn a user of content access or data carrier function inhibition after a predetermined number of access requests have been refused. The terminal may also incorporate content synthesis code as described above.

[0042] The terminal may comprise code to output supplementary data when downloading data to the data carrier. Identity data on the data carrier can be used to retrieve the supplementary data, or a pointer to the supplementary data, from the data supplier computer system, or the supplementary data or a pointer thereto can be retrieved directly from the data carrier. Preferably, however, identification data on the card is used to retrieve characterizing data such as card user preference data from the data supplier computer system, and this characterizing data is then used by the terminal to retrieve and output supplementary data to a terminal user. When the terminal is associated with a contact distributor or retailer, the supplementary data may be retrieved over a network associated with the retailer/distributor such as a local area network (LAN), wide area network (WAN) or extranet.

[0043] The invention also provides a method of providing data from a data supplier to a data carrier, the method comprising reading payment data from the data carrier; forwarding the payment data to a payment validation system; retrieving data from the data supplier; and writing the retrieved data into the date carrier.

[0044] The payment validation system may be part of the data supplier's computer systems or it may be a separate e-payment system. In one embodiment the method further comprises receiving payment validation data from the payment validation system; and transmitting at least a portion of the payment validation data to the data supplier. Alternatively the payment validation system may comprise a payment processor at the data supplier or at a destination retrieved from the data supplier. The payment processor may also provide payment distribution data for distributing a payment represented by the payment data.

[0045] In a further aspect, the invention provides a data access device for retrieving stored data from a data carrier, the device comprising a user interface; a data carrier interface; a program store storing code implementable by a processor; and a processor coupled to the user interface, to the data carrier interface and to the program store for implementing the stored code, the code comprising code to retrieve use status data indicating a use status of data stored on the carrier, and use rules data indicating permissible use of data stored on the carrier; code to evaluate the use status data using the use rules data to determine whether access is permitted to the stored data; and code to access the stored data when access is permitted.

[0046] The data access device uses the use status data and use rules to determine what access is permitted to data stored on the data carrier. As described above, the use rules will normally be dependent upon payments made for data stored on the data carrier, but may also comprise access control employing a user identification and password. Since a single data carrier may have more than one user, the use status and use rules may be selected dependent upon a user identity. The data access device may also be configured to present supplementary data when presenting the content data, retrieved as described above, from the card, from a remote computer system or from some other source such as a cable TV network or off-air.

[0047] The invention also provides a related method of controlling access to data from a data carrier, comprising retrieving use status data from the data carrier indicating past use of the stored data; retrieving use rules from the data carrier; evaluating the use status data using

the use rules to determine whether access to data stored on the carrier is permitted; and permitting access to the data on the data carrier dependent on the result of said evaluating.

[0048] According to a further aspect of the invention there is provided a data access system comprising a data supply computer system for forwarding data from a data provider to a data access terminal; a electronic payment system for confirming an electronic payment; a data access terminal for communicating with the data supply system to write data from the data supply system onto a data carrier; and a data carrier for storing data from the data supply system and payment data; wherein data is forwarded from the data provider to the data carrier on validation of payment data provided from the data carrier to the electronic payment system.

[0049] In a further aspect of the invention, there is provided a portable data carrier comprising an interface for sending and receiving data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; and a digital rights management processor for controlling access to the stored data.

[0050] In a further aspect of the invention, there is provided a portable data carrier comprising an interface for sending and receiving data from and to the carrier; non-volatile data memory, coupled to the interface, for storing data on the carrier; and an access control processor; wherein the data memory is partitioned as data blocks and the access control processor controls external access to the data blocks.

[0051] In a further aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a resource locator; a data provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item; code, responsive to the request and to the received payment data, to output the item data to the requester over the communication interface; wherein said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and further

comprising code to output payment data for a data item for making payments for the item when the item is supplied to a requester.

[0052] In a further aspect of the invention, there is provided a computer system for providing data to a data requester, the system comprising a communication interface; a data access data store for storing records of data items available from the system, each record comprising a data item description and a printer location data identifying an electronic address for a provider for the data item; a program store storing code implementable by a processor; a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item; code responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein the data access data store further comprises data item access rule data for output to the requester with a data item; and further comprising code to select access rule data for output with a data item in response to the payment data.

[0053] In a yet further aspect of the invention, there is provided a method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; transmitting the requested data to the requester; reading payment distribution information from a data store; and outputting payment data to a payment system for distributing the payment for the requested data.

[0054] In a still further aspect of the invention, there is provided a method of providing data to a data requester comprising receiving a request for a data item from the requester; receiving payment data from the requester relating to payment for the requested data; transmitting the requested data to the requester; and transmitting data access rule data to the requester with the read data.

[0055] These and other aspects of the invention will now be further described, by way of example only, with reference to the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0056] Figure 1 shows a data access device a) from the top; b) from the front; and c) from the side;

[0057] Figure 2 shows, conceptually, a portable data carrier;

[0058] Figures 3a and b show exemplary data access terminals;

[0059] Figures 4a and b show, respectively, a logical signal path between elements of a conceptual data access system; and a physical representation of a conceptual data access system;

[0060] Figure 5 shows a content provision system;

[0061] Figure 6 shows a data supply computer system;

[0062] Figure 7 shows a variety of data access terminals;

[0063] Figure 8 shows a schematic diagram of components of a data access terminal;

[0064] Figure 9 shows a schematic diagram of components of a data carrier;

[0065] Figure 10 shows a schematic diagram of components of a data access device;

[0066] Figures 11a and 11b are flow diagrams of a data carrier registration process;

[0067] Figures 12a-c and 12d-e show, respectively, a flow diagram of data access using a data access terminal; and a flow diagram of data supply using a data supply computer system; and

[0068] Figure 13 shows a flow diagram of data retrieval using a data access device.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0069] Referring to Figure 1, this shows a data access device for playing MP3 audio (10) with operator controls (12) and LCD display (14). The outline of a smart card data storage device is shown at (16). The operator controls allow a user to select and play tracks, while track information and still or video images are provided on display (14). A slot (18) is provided in the front of the device to receive a smart card-type data storage means. This smart card occupies space (20) and interfaces with resilient contacts (24); it is held in the data retrieval device against the contacts, by resilient housing element (22).

[0070] Referring now to Figure 2, this shows a portable data carrier (30) suitable for use with the device of Figure 1. The data storage means is based on a standard smart card; it is plastic, about the size of a standard credit card, and has some flexibility. On the card (30) are two sets of contacts, contacts (32) for interfacing with the payment validation means and

contacts (34) for interfacing with the memory for storing downloaded data (although in other embodiments, a single set of contacts may be used for both). The surface of the card can be embellished with suitable graphics.

[0071] In one embodiment the smart card retains all its useable functionality as specified for standard Electronics Point of Sale Systems (EPOSS) and, if desired, the memory for storing the downloaded data can be electrically separate from this. However, it may be preferable to provide interaction between the standard smart card device and the data memory in order to accomplish the access control/decryption functions described above.

[0072] Referring now to Figure 3, an example of a data access terminal is shown at (40). This has a screen (42) and a slot (44) to receive the data carrier (30). Alternatively the data carrier may interface to the terminal via the data access device (10) and an interface (46) to the terminal (40). In Figure 3b a dedicated terminal (50) has a slot (52) to receive the data carrier, a display (54) and controls (56). Coins can be inserted into the terminal at (58) and notes at (60) to charge the data carrier with cash.

[0073] Referring now to Figure 4a, this illustrates conceptually the logical connections and data flow between data processing systems involved in payment validation, and data download to the carrier (30). A user connects the data carrier (30) to terminal (40) and logs on to a data web page of data supply service provider (60). Either terminal (40) or service provider (60) then communicates via data paths (62) with a payment validation authority (70) to check and authorize the user's or payer's payment. In the case of electronic cash the terminal (40) may immediately validate the payment information, updating the service provider and/or payment validation authority (70) at a later stage. The logical connection (64) between the terminal and the service provider is preferably made over the internet.

[0074] The service provider may provide a direct portal to data providers (80) or may collect information from data suppliers (80) and provide a "front end" to present data from the suppliers to the terminal user. Alternatively, data supply service provider (60) may regulate direct access between terminal (40) and data providers (80), as shown by links (66), by communicating with the terminal and the data providers to provide communication regulation information to, for example, instruct data suppliers about what information the user of terminal (40) should have access to.

[0075] In a preferred embodiment, service provider (60) pays royalties at an agreed rate - for example, 10 pence per track or 10 pence per minute - to a computer system owned by a

company or entity in the recording industry, such as a content provider or copyright owner, a content publisher or a content creator, and the user of terminal (40) effectively pays the service provider. Billing can also be regulated by bandwidth and/or data download time.

[0076] Preferably the service provider (60) monitors the user's access to the system and either stores or forwards to data providers (80), or downloads to the data carrier (30), usage information. In a preferred embodiment the service provider sends information via terminal (40) to data carrier (30) which can be used to determine incentives to be provided to users of the system.

[0077] Figure 4b shows a conceptual physical configuration of the system of Figure 4a in which a plurality of terminals (40), a plurality of service providers (60) and a plurality of data providers (80) all interact via the internet. The physical embodiment of the system is not critical and a skilled person will understand that the terminals, data processing systems and the like can all take a variety of forms.

[0078] Referring now to Figure 5, this shows a conceptual illustration of a content provision system 100. Content creators 104a, b generate or receive content data from artist terminals 102a-d and store content data in databases 106a, b. The content data stored in databases 106a, b may comprise audio data, such as music, video data, such as films or TV programs, text, such as literary works, software, such as games software, or other data. Content creators 104a, b are coupled to communications network 101 for communicating created content data over the network. Also coupled to communications network 101 are content publishers 110a and 110b, each of which is coupled to an associated stored content database, 112a and 112b respectively. The content publishers make their stored content available for controlled access using communications network 101. In some instances, for example where the content data comprises computer games, the functions of content creator and content publisher may be provided by a single entity. Also although conceptually illustrated as blocks in Figure 5, the content creator and content publisher typically each comprise a client server computer network.

[0079] The communications network 101 is typically a private communications network, such as an extranet, with security controlled access to entities connected to the network. Physically the network may comprise an internet protocol network or it may comprise, or consist of, dedicated point-to-point links. Thus, for example, a content creator 104 may be

directly linked to a content publisher 110 and/or to other entities shown in Figure 5 such as a content provider or content distributor.

[0080] The content provision system includes a plurality of content providers 108a-e, each coupled to the communications network 101. In the illustrated system, the content provider's own copyright in stored content data accessible over communications network 101 and may, in practice, also perform a content publication function. Five content providers own the copyright in over 80% of all world-wide music sales. The content providers are coupled to stored content databases 106 and 112 via communications network 101, for supplying stored content data.

[0081] A gateway server 114 is also coupled to communications network 101 to link the communications network to other networks such as the internet and/or mobile communications networks. Gateway server 114 provides security and access control functions and firewalls. A second gateway, content distributor WAN gatewayn 116, is also shown attached to communications network 101. This provides similar security and firewall functions and coupled communications network 101 to distributor WAN (wide area network) 117. Gateway 116 has logical access to one or more of a content creator, content publisher and content provider for accessing stored content data. Content distributor gateway 116 may be owned by a chain of record stores and provide content access terminals 118, coupled to WAN 117, in separate retail outlets. Content access terminals 118 have access, via gateway 116, to stored content accessible over communications network 101.

[0082] Referring now to Figure 6, this shows a data supply computer system 120. In this embodiment, three content access terminals 118a-c, e-payment systems 121a, b, and content access web server 124 are all coupled to internet 142. Data supply system 120 is coupled to the content provision system 100 illustrated in Figure 5. Where communications network 101 of Figure 5 is an extranet, this extranet physically operates over internet 142; where communications network 101 does not partly operate via internet 142, a connection to internet 142 is established via gateway server 114 as shown in Figure 5. In this way content access terminals 118a-c are provided with controlled access to the stored content data of content provision system 100.

[0083] E-payment systems 121a and 121b are coupled to banks 122a, b and c, d respectively. These provide an e-payment system according to, for example, MONDEX, Proton, and/or Visa cash compliant standards. Preferably at least one of e-payment systems

121a, b operates a so-called "open purse" system in which the value is stored as a publicly verifiable digital signature issued by the e-payment system. In such a signature-transporting arrangement, payment data may be validated using public keys and thus payment authentication need not be performed by the e-payment system but may instead be performed by, for example, a data access terminal or data supply system computer, using payment management code. The authenticated signatures, which in effect perform a similar role to checks, are submitted to the relevant e-payment system after authentication for verification and reimbursement or transfer of monetary value. With such a system payments may be made anonymously and thus payer identification is not essential. Data carriers, such as data cards, may be issued with stored value or without value, in which latter case value (that is, a publicly verifiable digital signature) may be written onto the card during an on-line transaction.

[0084] In alternative embodiments, a data carrier such as the smart Flash card described below may be used to create value bearing digital signatures as is well-known to those familiar with e-money.

[0085] Content access web server 124 is also coupled to internet 142 for providing content access terminals 118a-c with access to content data. Content access web server 124 is typically owned by a content data supply "system owner" who acts as an intermediary between a content access terminal user and a content provider, forwarding content data provided (directly or indirectly) by a content provider to a content access terminal and then to a stored content data carrier. Web server 124 is coupled to web server code storage 126 storing Java code for generating web pages for interpretation by web browsers on content access terminals 111a-c. The web pages provide the content download, value add, CRM (customer reward management) value check/spend and website link functions described below.

[0086] Web server 124 is coupled to payment processor 128, Digital Rights Management (DRM) processor 130, access control processor 132, and content distribution processor 134. Payment processor 128 includes payment management code storage 128a and is coupled to payment record data store 136. Access control processor 132 includes access control code storage 132a and is coupled to access control data store 138. DRM processor 130 includes DRM code storage 130a and is coupled to content access and DRM data store 140. Content distribution processor 134 includes CRM (customer reward management) and payment

distribution management code storage 134a and is also coupled to content access and DRM data store 140. As shown in Figure 6, processors 128-134 are all in communication with one another.

[0087] Processors 128, 130, 132 and 134 may comprise separate application programs or a single computer program and may operate on a single physical computer, on which web server 124 may also be provided, or may operate on separate computers. Likewise data stores 136, 138 and 140 may comprise a single physical data store or may be distributed over a plurality of physical devices and may even be at physically remote locations from processors 128-134 and coupled to these processors via internet 142.

[0088] Web server 124 communicates with processors 128-134 by means of a CGI (common gateway interface) script and the code associated with processors 128-134 may be written in any conventional computer language such as C, C++, or Perl. However, in other embodiments one or more of the processors may be coupled to web server 124 via internet 142 and owned and operated by a separate entity, such as a financial institution. In this case conventional secure web-based communications may be operated between web server 124 and the relevant processor. In particular, payment processor 128 may be operated by one of the e-payment system providers 128a, b.

[0089] Payment management code 128a issues and authenticates payment data and stores an audit record in payment record data store 136. Access control code 132a stores identification data (of a user or card) together with registration data provided by a user when registering with the system owner. This data comprises a user password for accessing stored content and/or payment data; user characterizing data, for example characterizing user preferences, for marketing purposes; data indicating an e-payment system to use; and in some embodiments, further general user related data such as card level data for identifying the provision of "gold" level services to selected users. A copy of the password is stored with the content data on the portable data carrier, as described further below. Alternatively, one or both of the access control data store and portable data carrier may simply store data for verifying a user-entered password.

[0090] Content access and DRM data store 140 stores data related to content access and content use, but does not itself store content data items; these are instead provided via content provision system 100 described above. Data store 140 stores a plurality of records each comprising a data item identifier, a data item description, a data item type or genre, and

location data comprising one or more pointers to a location or locations from where the data item can be downloaded. Associated with a data item is also a table of use rule data comprising a list of values (i.e. content data item prices) and corresponding levels of permitted usage. Thus a value of £1 might permit ten plays of a music track, while the value of £10 might permit an unlimited number of plays of the track and copying of the track for personal use.

[0091] Also associated with a data item is a table of payment distribution data comprising a list of recipients and corresponding fractions of the data item value each is to receive. Typically, the main recipient will be the copyright owner of the data item and other recipients will be selected from the content creator, the artist or artists, the system owner, the content publisher, and the retailer/distributor. The payment distribution proportions may be dependent upon the payment value, in which case a plurality of sets of payment distribution figures may be associated with each data item, each set of distribution figures corresponding to a payment value range. The payment data and distribution data is here termed DRM (Digital Rights Management) data.

[0092] Further associated with a data item is a table of CRM (Customer Reward Management) data, linked to the user rule data, comprising CRM rules to specify, for one or more data item use levels, a quantity of reward points and one or more recipients for the reward points (the recipients may include the card user and the retailer/distributor).

[0093] The CRM and payment distribution code 134a operates with content access and DRM data store 140 to inform a system user of the description and value of a data item, to access and download a data item from the content provider system to a content access terminal, to provide content use rules with the data item, and to provide instructions either to payment processor 128 or to e-payment system 121 to distribute payments for the data item to the recipients identified by the data store 140 and to distribute CRM reward points.

[0094] The access control data store 138 holds a secure key, such as a secret "public" key in a public key cryptography system, for the system owner to authenticate its identity to a content provider. This data is held securely with other sensitive data in the access control data store 138. As is described in more detail below, when data supply system 120 receives a request for a content data item from a content access terminal 118, it looks up a location from which the data item is available using content access and DRM data store 140 and then determines the identity of the corresponding content provider. This identity is either stored in

content access and DRM data store 140 or, as there are relatively few content providers, it may be hard written in DRM code 130a. DRM code 130 then requests access control processor 132 to provide the secure system owner identifier from access control data store 138 to the relevant content provider and sets up a trusted connection between the content provider and content access web server 124 for downloading the data item to a content access terminal 118 and then to a portable data carrier.

[0095] Referring now to Figure 7, this shows a variety of content access terminals for accessing data supply computer system 120 over internet 142. The terminals are provided with an interface to a portable data carrier or "smart Flash card" (SFC) as generally described with reference to Figure 2 and as described in more detail below. In most embodiments of the terminal the SFC interface allows the smart Flash card data carrier to be inserted into and removed from the terminal, but in some embodiments the data carrier may be integral with the terminal.

[0096] Referring now to the specific embodiments illustrated in Figure 7, a simple content access terminal may comprise a home personal computer 144 with SFC interface 144a. In another embodiment, a mobile communications device 152 is provided with a smart Flash card interface 152a and is coupled to internet 142 via radio tower 150, mobile communications system 148 and mobile communications internet gateway 146.

[0097] In another embodiment, a smart Flash card interface is provided to a so-called "set top box" (STB) 154. The set top box is, in effect, a receiver for television programs received on video input 154b, which may comprise a satellite TV signal, a cable TV signal or an off-air TV signal. The video signal is provided from the set top box to television 156 or to some other home entertainment device such as a personal computer (not shown). In another embodiment, content access terminals 166 and 168 each with respective SFC interfaces 166a and 168a are coupled to a retailer local area network (LAN) 160 connected to internet 142 via retailer LAN server 158. DVD player 164 is also coupled to LAN 160. In a further embodiment a smart Flash card interface 170a is provided for a CD/DVD player 170.

[0098] In these latter three embodiments, content data for storage on the smart Flash card may be retrieved from broadcast video and/or a CD or DVD. In this case, the computer data supply system 120 illustrated in Figure 6 may be used to provide use rule data for the content data stored on the smart Flash card, and to pay for data downloaded onto the card; the content data may be captured before or after the data supply system 120 is accessed to enable use of

the stored data, but in a preferred embodiment content data written to the card from a supplier other than the content data supply computer system is not accessible to a user until corresponding use rule data has been downloaded from computer system 120, which will normally be after receiving payment for the downloaded data.

[0099] Referring now to Figure 8, this shows a schematic diagram of one embodiment of a data access terminal 170. The terminal comprises a general purpose computer including an audio/visual interface 184, a keyboard 186 and a pointing device 188 for providing an interface to the user. The terminal has an internet interface 176, for example a modem, and optionally a LAN/WAN interface 174 for connecting the terminal to a retailer or distributor LAN or WAN. The terminal also has an optional video input 178 for receiving broadcast video data and a media input device 180, such as a CD or DVD drive. Further communications I/O ports 182 may also be provided. A portable data carrier or smart Flash card interface 190 is provided for interfacing to a smart Flash card. Optionally, a cash input and verification system 192, such as is conventionally used in an automatic teller machine (ATM), may also be incorporated within the content access terminal. The terminal has working memory 194 such as RAM and program memory 196 which can comprise any conventional storage device such as RAM, ROM or a disk drive. Program code in program memory 196 may also be stored on removable disk 198. A processor 200 loads and implements program code stored in program memory 196. All the components of the terminal are linked by a data and communications bus 172.

[0100] More specifically, processor 200 loads and implements cash payment management code 200a for managing cash input data from cash input and verification system 192, for adding value to a smart Flash card. Processor 200 also implements a web browser 200b for accessing system owner web pages and data exchange interface 200c for exchanging data between a smart Flash card interface to the terminal and data supply system 120.

[0101] Processor 200 also implements off-line contents retrieval code 200d for retrieving data for storage on a smart Flash card from media input device 180 and/or video input 178 and/or LAN/WAN interface 174. The processor implements a content sampler 200e for outputting small extracts of content data items to a user via audio/visual interface 184. Such data item samples may be stored with the content description data in content access data store 140. The processor also implements a smart Flash card interface driver 200f, user interface

code 200g and additional communication drivers 200h for driving LAN/WAN interface 174 and/or comms I/O ports 182.

[0102] Referring now to Figure 9, this shows a schematic diagram of components of a portable data carrier 202, in the embodiment shown a so-called "smart Flash card". In this context, "smart Flash card" refers to an IC card similar in size to a plastic payment card incorporating a processor and Flash data memory, preferably of large capacity. For further details on smart cards, reference may be made to the ISO (International Standards Organization) series of standards, including ISO 7810, ISO 7811, ISO 7812, ISO 7813, ISO 7816, ISO 9992 and ISO 10102, which are hereby incorporated by reference.

[0103] Referring in more detail to Figure 9, a data and communications bus 204 links components of the card which include a processor 210, working memory 212, timing and control logic 208 and an external interface which may have contacts (ISO 7816) or be contactless (ISO 10536) for providing external access to a bus 204 for reading data from and writing data to the card 202. Also coupled to bus 204 are permanent program memory 216, non-volatile data memory 218 and non-volatile (Flash) content data memory 214. Non-volatile data memory 218 may comprise EEPROM and permanent program memory 216 may comprise ROM, for example, mask-programmed ROM. All the components of Figure 9 are mounted on a single substrate, in a preferred embodiment bearing contacts for external interface 206.

[0104] Processor 200 loads and implements program code from permanent program memory 216. This code comprises operating system code for providing the card with a basic operating system for at least external communications; payment management code for supplying payment data from non-volatile data memory 218 to pay for downloaded content; DRM (Digital Rights Management) and security code, including code to implement content data use rules and code for password controlled access to data and program functions; CRM code for implementing CRM-related rules; and content synthesis code for combining stored content data with additional data provided via external interface 206 for synthesizing complete content item data.

[0105] Non-volatile data memory 218 stores data including card identity data, access control data, including password data for validating a user password, access record data for storing a record of access attempts and their outcomes, and content supply data such as system owner website addresses and retailer/distributor website addresses.

[0106] Data memory 218 further stores card value data comprising e-money such as publicly verifiable digital signatures, and payment data for storing a payment audit trail including payment amounts and data on to whom payments have been made. The memory 218 also stores RFM (Recency Frequency Monetary) data to provide a record of transactions for market research and customer reward purposes, and CRM data storing customer reward points. Data memory 218 also stores an index of content data items stored in Flash memory 214 and associated content use rules, as well as DRM and royalty data for maintaining an audit trail of use history for rights management tracking. Optionally, data memory 218 may also store supply chain data specifying a supply chain route through which data has been obtained from a content provider, which may be used for rewarding supply chain intermediaries, for example on a commission or reward points basis.

[0107] Content data memory 214 preferably comprises at least 100 MB of data storage, partitioned as data blocks of a size selected to match the stored content type. For storing video data, Flash memory 214 preferably comprises > 1 GB data storage and the data blocks into which the data memory is partitioned are larger.

[0108] Referring now to Figure 10, this shows a schematic diagram of a data access device 220, such as a portable audio/video player. The data access device 220 comprises a conventional dedicated computer system including a processor 238, permanent program memory 236, such as ROM, working memory 234, such as RAM, and timing and control logic 226 all coupled by a data and communications bus 222. Also coupled to the bus are an audio interface 228, a display 230 and user controls 232, for providing a user interface. A smart Flash card interface 224 is coupled to bus 222 for interfacing with a smart Flash card for retrieving and playing stored content data.

[0109] Permanent program memory 236 stores program code for implementation by processor 238; this code may also be provided on a data carrier such as a ROM chip or disk 240. Processor 238 implements an SFC interface 238a, a user interface 238b, a content player 238d for retrieving stored content data from a smart Flash card interfaced to the device and for outputting audio and/or video data derived from the retrieved content data (which may comprise compressed audio and/or video data) to a user of the device.

[0110] Processor 238 also implements use control 238c for controlling access to and use of contents stored on the smart Flash card by the content access device user. Use control routine 238c and/or DRM and security code in permanent memory 216 on the smart Flash card may

also implement digital watermarking and other Secure Digital Music Initiative (SDMI) content protection code as specified in the SDMI portable device specification, part one, version 1.0 (see www.sdmi.org) which is hereby incorporated by reference.

[0111] Figures 11a and 11b show a flow diagram of a process for registering a data carrier or smart Flash card with a data supplier or system owner operating a data supply system as illustrated in Figure 6. A smart Flash card may be issued entirely blank, that is, with no prestored content or value, with prestored value but no prestored content, with prestored content but not prestored value (the content being provided free) or with both prestored value and prestored content. Thus, for example, a user may purchase a card with stored value but no stored content over the counter at a retailer. The process of Figures 11a and 11b illustrates the registration of a card with neither prestored content nor prestored value. As illustrated the registration process records user registration data in the access control data store 138 of Figure 6 and writes value data onto the blank card.

[0112] At step S10 a smart Flash card is inserted into a content access terminal smart Flash card interface. The system owner web page is then loaded onto the content access terminal and displayed to the user (step S11). User registration data is then entered into the content access terminal (step S12) and transmitted to the system owner (S13). The user registration data may include a user identity, a preferred e-payment system to use and, optionally, a content access PIN or password, and a service level (for example bronze, silver or gold). The optional password may be a password required by the e-payment system for validation of a payment by the user with the card or it may be a password to protect unauthorized access to content on a smart Flash card to protect stored data in the event, for example, of the card being stolen. A single password may serve both these functions. The content access terminal web browser is configured so that all sensitive data passing between the terminal and the system owner is securely transmitted, for example by using a conventional encryption system such as PKI (Public Key Infrastructure).

[0113] At step S14 a payment request is received from the system owner at the content access terminal and displayed to the user. At step S15 the user enters payment data into the content access terminal and this payment data is transmitted to the system owner, for adding value to the card. This may, for example, be a credit card transaction as is conventionally used for purchase over the internet. Card value data and a card value access code is then received by the content access terminal from the system owner at step S16. The card value

corresponds to the payment made by the user and the value access code may be a password entered by the user at step S12 or may comprise a password for PIN created by payment processor 128 or e-payment system 121 as illustrated in Figure 6. In a preferred embodiment, the user pays the system owner and the system owner then directly provides digital signature data representing value to the content access terminal for writing onto the smart Flash card.

[0114] At step S17, card registration data is received from the system owner by the content access terminal and written onto the smart Flash card. This card registration data comprises user identity data, access control data, payment system specifying data, system owner access data, such as a system owner web page address and other dial-up information. At this stage other data may be entered by the user and written onto the card, including, for example, user preference data, retail outlet and CRM data (alternatively user preference data may be captured at step S12). At step S18 the card value data and card value access code received at step S16 is written onto the card and output to the user visually and, optionally, as a printed record. The card is then available for use, at step S19.

[0115] Figure 11b shows the corresponding registration steps performed by the system owner's data supply system 120. At step S20, a request for a smart card registration web page is received from a content access device and, at step S21, transmitted to the device. User registration data is then received, at step S22, from the content access terminal and stored in content access control data store 138. The system owner's computer system then transmits, at step S23, a payment request to the content access terminal and receives, at step S24, payment data in reply, this payment is then authenticated, at step S25, with an e-payment system such as payment system 121 a or b illustrated in Figure 6, and after verification the payment processor 128 of the computer system transmits, at step S26, value data and a value access code to the content access terminal, for writing onto the smart Flash card. The payment processor then updates the payment record data store 136 with data relating to the transaction (step S27) and, at step S28, retrieves card registration data previously written into the access control data store and transmits this registration data to the content access terminal. At step S29 the transaction is then complete.

[0116] Referring now to Figures 12a-c, these illustrate a flow chart for downloading data to a smart Flash card using a data access terminal. At step S30 the smart Flash card is inserted into the content access terminal and the user then enters, at step S31, their password for gaining access to the functionality of the smart Flash card. At step S32, the content access

terminal transmits the password to the smart card for verification and the terminal checks, at step S33, whether access is permitted. If access is not permitted a warning is displayed by the terminal, at step S34, and an access denied count is implemented. A threshold count is then read from the card together with a count of the total number of times access to the card has been denied (step S35). At step S36 the terminal checks whether the total number of denied accesses is within three of the card threshold, and if it is not, returns to step S31, while if it is, it proceeds to step S37 where the terminal displays a warning that a further denied access is likely to result in erasure of content stored on the card. At step S38 the terminal then checks whether its count of denied accesses is greater than its threshold value, returning to step S31 if not, and displaying an access refused message at step S39 if the total number of permitted accesses has been exceeded. The system then waits at step S39 for removal of the smart Flash card from the content access terminal.

[0117] If access is permitted at step S33, the terminal loads outline CRM data from the card (step S40) and loads retail data, such as targeted advertising, from the retailer LAN/WAN (step S41). At step S42, the terminal then displays a menu of options, retail data such as advertising or CRM-related data and outline CRM data, such as a total number of reward points earned, on the content access terminal. Many options include download content (from a system owner), add monetary value (to the card), check/spend CRM value stored on the card, follow website links, and exit. At step S43, the user inputs a menu option which, in the illustrated flow chart, is the download option. The system thus passes to step S44 and loads the system owner's content access web page onto the content access terminal and displays this to the user.

[0118] At step S45, the user enters a content search request, which is transmitted to the system owner content distributor processor 134. Content search results are received back from the content distribution processor, including a content identifier, a brief description, and content cost data for at least one payment option, and these results are displayed on the user on the content access terminal. The user then selects one or more content items at step S47 and the selection is transmitted to the content distribution processor 134 where further content cost data and purchase option data is retrieved from data store 140. At step S48, this content cost and purchase data (including use rule data) is received from the system owner and displayed to the terminal user. The user then selects, at step S49, a purchase option and confirms a purchase request or, alternatively, selects "exit" to return to the menu display of step S42. After one or more content items have been selected, together with a purchase

option, hard value and CRM data is read from the smart Flash card at step S50, and at step S51 a check is made to determine whether the monetary and/or CRM (reward points) value stored on the smart Flash card is sufficient to purchase the selected purchase data items. If the card value is insufficient, a warning is displayed at step S52 and the system returns to the menu display at step S42. If the card value is sufficient, at step S53 the content access terminal transmits a payment request to the smart Flash card.

[0119] Payment for the data item or items requested may either be made directly to the system owner or may be made to an e-payment system such as e-payment systems 121a and 121b of Figure 6, with these systems then forwarding payment confirmation data to the system owner computer system. Alternatively, the content access terminal may transmit data to the card to set up a transaction directly with a content provider who, being the copyright owner, would normally receive the majority of the payment.

[0120] At step S54, payment data for making a payment to the system owner is received from the smart Flash card by the content access terminal and forwarded to an e-payment system such as e-payment system 121 in Figure 6. Payment record data, validating payment by the card to the system owner, is then received back from the e-payment system at step S55 by the content access terminal and forwarded to the card for updating payment data on the card. In alternative embodiments, payment data from the card may be provided directly to the system owner's data supply computer for authentication and, optionally, further validation with an e-payment system by the system owner's computer.

[0121] Distribution of the payment received by the system owner from the card is performed by the system owner's computer system, as described elsewhere. Such payment distribution will normally provide a small percentage of the total payment to a "owner" or operator of the content access terminal, such as a retailer, distributor, or in other embodiments, mobile communications network operator or cable TV network operator.

[0122] In the presently described embodiment, payment record data received in step S55 is transmitted to the system owner to confirm payment by the card and thus it is the content access terminal, in the described embodiment, which authenticates a payment before confirming that the payment has been made to the system owner.

[0123] In step S56, together with the payment record data, purchase request and card registration data is transmitted to the system owner to identify one or more content data items for purchase and to identify the purchaser. Then, at step S57, the content access terminal sets

up a transaction between the system owner data supply computer and the smart Flash card for download of the identified content items requested from the data supplier to the smart Flash card. The download is preferably arranged so that there is no permanent storage of downloaded data on the content access terminal (although temporary storage in a disk cache may be permissible), and there is further preferably no temporary storage on the content access terminal of complete data for a content data item. This provides data security and reassurance to the content providers.

[0124] In the same way as with card registration described with regard to Figure 11, a secure and trusted link is set up between the content access terminal and/or the smart Flash card and the data supply computer in a conventional manner as is well known to those skilled in the art (for example, using public key data encryption). The data transaction may be set up directly between the smart Flash card and the data supply computer, in which case the content access terminal has no access to unencrypted content data, or it may be set up between the content access terminal and the data supply computer, in which case unencrypted data is written by the content access terminal to the smart Flash card. Standard transmission protocols are used to ensure complete transmission of a content data item, for example by re-transmitting blocks of data which are not correctly received.

[0125] Also at step S57, one or more content access rules is received from the system owner data supply computer and written to the smart Flash card so that each content data item has an associated use rule to specify under what conditions a user of the smart Flash card is allowed access to the content data item.

[0126] At step S58 the content access terminal receives CRM data from the content distribution processor 134 of the system owner, for example specifying a number of reward points earned by downloading the selected content items. This CRM data will normally be written to the smart Flash card (step S59), but may additionally or alternatively be stored in the content access terminal or in a data store of the content access terminal owner so that the reward points are held by the distributor/retailer/cable TV operator. Finally, also at step S59, a complete record of details of the transactions between the smart Flash card and the content access terminal, the smart Flash card and the system owner, the smart Flash card and the e-payment system, and the content access terminal and the e-payment system and/or data supply computer is recorded on the smart Flash card to provide an audit trial. The system then returns to the menu display at step S42.

[0127] The add monetary value menu option provided by the menu operates in a similar manner to that described with regard to steps S15 and S16 of Figure 11a and steps S24 to S27 of Figure 11b. In embodiments of the system in which the smart Flash card operates either in a debit (pre-pay) or credit mode, operating mode data may be loaded from the card together with outlying CRM data at step S40. If the card is operating in a credit mode then, at step S41, the content access terminal reads content use data records from the card and proceeds correspondingly to steps S47 and S48 to determine the value of the content accessed and then proceeds according to steps S15 and S16 of Figure 11a and steps S24 to S27 of Figure 11b to retrieve payment for the accessed content from the card owner. Where enhanced access control features are provided, access control data read from the smart Flash card or entered into the content access terminal at step S31 is used, in step S44, to access the system owner content access webpage and, in some embodiments, to set up a secure connection between the content access terminal and system owner data supply computer at step S44.

[0128] Referring now to Figures 12d and 12e, these show steps in a process implemented on the system owner's data supply computer for providing content data to a content access terminal and thence to a data carrier such as a smart Flash card. At step S60 the system owner's content access web page is requested by a content access terminal and transmitted to the requesting terminal. A search request for searching for a content data item is received, at step S61, from the content access terminal, and at step S62 content distribution processor 134 of the content supply system searches content access and DRM data store 140 and transmits the search results to the content access terminal. The search results will normally comprise a content item identifier, a content item description, optionally a content item sample, and at least one content item price, for example for a default payment option. The search results may comprise a set of content data items, either selected by type or artist or comprising some predetermined selection in a similar manner to a compilation of tracks on a CD.

[0129] At step S63 content item selection data identifying one or more content items is retrieved from the content access terminal, and at step S64 content item purchase data for the selected content items is retrieved from content access and DRM data store 140. This purchase data will normally include, for each selected content item, one or more prices and purchase options. Purchase option data may simply comprise one of a set of standard options, for example "1" to purchase outright, "2" to rent for a period of time, "3" to rent for a number of plays, and "4" to rent with a final purchase option. The purchase option data may also indicate when a content item is available free.

[0130] At step S65 the content purchase data is transmitted to the content access terminal, and at step S66 payment record data, indicating a payment made from the smart Flash card to the system owner, purchase request data, card registration data and, optionally, access control data, is received from the content access terminal. The payment record data confirms a payment for the requested data items, the purchase request data specifies the payment option selected for the selected content items, and the card registration data provides data for keeping records of the transaction and providing reward points; the access control data may be required for additional data security. At step S67 the payment record data, in the described embodiment of the system, is validated with an e-payment system such as e-payment system 121 of Figure 6. As illustrated in the flow chart, the data supply system computer checks with the e-payment system that a payment has in fact been made to the system owner. In other embodiments of the system, payment may be made directly to the system owner, and either concurrently with the content access and download process, or at some later stage, payment data received from the smart Flash card may be verified with the e-payment system for reimbursement of the system owner.

[0131] At step S68, payment distribution data is read from the content access data store 140. This data will indicate how payment made by the card for the data is to be distributed among recipients. In one embodiment, recipient's payment fractions are specified in general terms in the content access data store, for example copyright owner 0.90, system owner 0.01, retailer/distributor 0.02, publisher 0.02, creator 0.05. Identification of who is the relevant copyright owner is stored in the data store together with the content item identifier, but may be selected from more than one possible content provider for the data item, and identification of who is the relevant retailer/distributor may be determined from, for example, content access identity information received from the content access terminal when the system owner content access web page is accessed at step S60. At step S69, payments are then distributed in accordance with the payment distribution data, either by direct distribution of value-bearing digital signatures to the relevant parties, or by issuing a payment distribution instruction to e-payment system 121. Preferably the data supply system stores records of individual card payments and, at intervals, combines the payment distribution data for a plurality of individual records to output payment data for distributing the total payment received by the data supply system from a batch of individual payments.

[0132] At step S70, content access rules for the purchased level of service are read from the content access data store. These rules could, for example, specify that only a predetermined

number of accesses to the content are permitted, for example 10 plays. Alternatively, the rules could provide access for, say, one month from the download date. Other rules may provide unlimited plays but only on specified players, for example set top boxes owned by a particular cable TV network (as determined by content access device identification data provided to a smart Flash card from a content access device). A content provider identification for the requested content data is also read from the content access data store at step S70 together with CRM data for issuing reward points.

[0133] At step S71, content access rules for the requested content data items are retrieved from data store 140 and transmitted to the content access terminal. Then, at step S72, DRM processor 130 of the data supply system transmits a transaction request and authentication data to the content provider identified in step S70. This request identifies the system owner data supply system to the content provider in a secure manner, either by means of physical security, such as a dedicated connection from the system owner data supply system to the content provider, or by means of an electronically secure connection such as an encryption connection. Then, at step S73, the content access web server 124 receives protected content from the content provider, comprising the data items requested by the content access terminal, and transmits this protected content to the content access terminal. The content is preferably protected by data encryption but may be protected in other ways, for example, by digital watermarking or simply by the large number of other transactions taking place at any one time over the internet. The data supply system computer, at this point, essentially acts as a transparent data forwarder, forwarding data from the content provider to the content access terminal, which itself is preferably effectively transparent, using data exchange interface 200c to transmit the protected content data directly to the smart Flash card. As described with regard to Figure 12d, the content download protocol includes error protection and transmission retry protocols to ensure substantially error-free data transmission.

[0134] Once content has been downloaded to the content access terminal (and, hence, to the smart Flash card) at step S74 a record of the purchase data and content accessed is written to payment record data store 136, to provide an audit trail. Then, at step S75, updated CRM data is written to the content access data store 140, using rules stored in the content access data store, in conjunction with a record of the downloaded data items, to calculate the CRM data (i.e. reward points). The updated CRM data is then also transmitted to the content access terminal, where it can be forwarded to the smart Flash card. Then, at step S76, the process ends.

[0135] Referring now to Figure 13, this shows a flow chart for user access of stored data on a smart Flash card using a data access device such as the MP3 player of Figure 1. At step S77 the smart Flash card is inserted into the player and, at step S78, the user enters a password into the player, which is transmitted to the smart Flash card for validation (this step is optional). If access to stored data on the card is permitted, the process proceeds to step S79 where an index of content data items stored on the card is loaded from the card and displayed together with a menu. The menu provides options including access content, check value (stored on the card), check CRM data (such as reward points) stored on the card, and play options (such as no video, repeat play, random play, and the like). If the user wishes to access content data items stored on the smart Flash card, a user selection of such items is entered into the player at step S80, for example using cursor keys or a pointer; additionally or alternatively a default play option may be provided to, for example, play the most recently downloaded data.

[0136] At step S81 content use status data for the selected content items is loaded from the smart Flash card together with associated content use rules. Then, at step S82, the use rules and present use status for each selected content item are compared and the result is displayed together with a content play menu. The content play menu may comprise a simple list of the selected content items with items not available for access highlighted in, for example, red. Alternatively, more detailed content access permission data may be displayed such as the purchased contents use for a content data item, the actual use of the data item made so far, and the available remaining use. Then, at step S83, the player determines whether content use is permitted. If use is not permitted, the process returns to step S79 to re-display the menu; if content use is permitted the system proceeds to step S84.

[0137] At step S84 the selected content data items whose use is permitted are retrieved sequentially from the card, decoded as necessary, and the decoded audio and/or video data is made available to the user, for example, by providing audio output at a headphone socket on the player and displaying video output on the player display. Preferably, the player also retrieves supplementary data stored in association with a content data item, such as advertising data, or for a web-enabled player, hot links to web sites for sale of goods or services, particularly those related to the accessed content data item or those identified to appeal to users accessing the data item (such as pop group merchandizing or Harley Davidson (trade mark) motor bikes for rock music/video).

[0138] Preferably, the player is provided with "pause" and "continue" functions and corresponding user controls. When "pause" is selected the process passes to step S85 and writes a record to the smart Flash card comprising data specifying how much use has been made of the accessed content data item. In the case of music or video data, this may comprise start and end time markers or simply a play duration time (the start time being predetermined, for example at the start of the data item). In the case of a game the partial use data may comprise an elapsed play time or a number of lives left. In the case of a data item providing a service such as access to stock and share prices, or weather information, or a share dealing service, the partial use information may comprise a status record indicating the status of an interrupted transaction. When the "continue" function is selected on the player the process returns to step S84.

[0139] To allow for the smart Flash card being removed from the player between pause and continue events, a check may be made at step S78, by reading a partial use status data from the card, to determine whether a content data item was left in a pause state when the card was last used. If such a pause state is determined to exist for a content data item, the process may then jump directly to step S85 to allow a user to resume or continue with the content data item and proceed directly to step S84.

[0140] Once play is complete the process moves to step S85 where updated content use data is written to the smart Flash card. This updated use data provides a record of the use of a content made in step S84. This record can then be used in steps S81 to S83 to determine, on a subsequent occasion, whether further use of the content data item is permitted. Finally, at step S86, customer reward management reward rules are loaded from the smart Flash card together with CRM data stored on the card. The CRM data is then updated, using the CRM reward rules, to reflect the use of content data items made in step S84 and the updated data is written back to the smart Flash card.

[0141] In one embodiment the CRM reward rules are determined by the content access terminal owner (retailer/distributor/cable or mobile network operator) and are written onto the card when registering the card. The updated CRM data may then be accessed by a content access terminal for spending or other use when the smart Flash card is next inserted into a content access terminal. Once the CRM data has been updated, the process returns to step S79 to display the content index and menu.

[0142] The specific embodiments of the invention described above use communication over the internet and web-based technology but this is not essential, and the invention may be implemented using any electronic communications network, such as a wide area network, local area network, wireless network, or conventional land line network. Likewise, the invention is applicable to the internet, intranets, extranets, and other internet protocol networks.

[0143] The skilled person will understand that many variants to the system are possible and the invention is not limited to the described embodiments but encompasses modifications which lie within the spirit and scope of the present invention.

WHAT IS CLAIMED IS:

1. A method of providing portable data comprising:

providing a portable data storage device comprising downloaded data storage means and payment validation means;

providing a terminal for internet access;

coupling the portable data storage device to the terminal;

reading payment information from the payment validation means using the terminal;

validating the payment information; and

downloading data into the portable storage device from a data supplier.

2. A method as claimed in claim 1 further comprising

writing updated payment information into the payment validation means.

3. A method as claimed in claim 1 or 2 further comprising

communicating a result of the payment information validating to the data supplier.

4. A method as claimed in any one of claims 1 to 3 further comprising controlling access by the terminal to data from the data supplier using a control data processing system coupled to the Internet.

5. A method as claimed in claim 4 wherein the control data processing system performs said validating of the payment information.

6. A method as claimed according to any one of claims 1 to 5 wherein said coupling is performed by a mobile data retrieval device comprising:

a removable data storage means;

data access means, to access downloaded data on the data storage means;

storage interface means adapted to couple the data storage and data access means; and

data output means to output data derived from the downloaded data, to a user of the device.

7. A method as claimed in claims 1 to 6 further comprising

writing into the data storage device data relating to past use made of the downloaded data including data identifying downloaded data items; and/or data identifying data suppliers used; and/or data characterizing a user spending pattern.

8. A method as claimed in claims 1 to 7 wherein said portable data storage device comprises an electronic memory card or smart card.

9. A method as claimed in any one of claims 1 to 8 wherein the downloaded data comprises compressed audio and/or video data.

10. A portable data carrier comprising:

an interface for reading and writing data from and to the carrier;

non-volatile data memory, coupled to the interface, for storing data on the carrier;

non-volatile payment data memory, coupled to the interface, for providing payment data to an external device.

11. A portable data carrier as claimed in claim 10, further comprising a program store storing code implementable by a processor; and

a processor, coupled to the content data memory, the payment data memory, the interface and to the program store for implementing code in the program store,

wherein the code comprises code to output payment data from the payment data memory to the interface and code to provide external access to the data memory.

12. A portable data carrier as claimed in claim 11, further comprising non-volatile use record memory, coupled to the processor, for storing a record of access made to the data memory and code to update the use record memory in response to external access made to the data memory.

13. A portable data carrier as claimed in claim 12, further comprising non-volatile use rule memory, coupled to the processor for storing data use rules, and wherein the code further comprises code for storing at least one data item in the data memory and at least one corresponding use rule in the use rule memory and code to provide external access to the data item in accordance with the use rule.

14. A portable data carrier as claimed in claim 11, 12 or 13, further comprising a non-volatile access control memory coupled to the processor, for storing access control data and wherein said code to provide external access to the data memory includes code to receive access request data from the interface, code to determine access permission using the stored access control data and code to provide external access to the data memory in response to the result of the determination.

15. A portable data carrier as claimed in claim 14, further comprising non-volatile access record data memory, coupled to the processor, for storing a record of requests for external access to the data memory and wherein said code further comprises code to compare said access record data and said access request data and to erase stored content data in response to a result of said comparison.

16. A portable data carrier as claimed in any one of claims 11 to 15, configured for storing supplementary data in said data memory and further comprising code to output the supplementary data from the interface in addition to the stored data, in response to an external request to read the data memory.

17. A portable data carrier as claimed in any one of claims 11 to 16 further comprising data synthesis code to receive a first portion of data from the interface and to combine the first portion with a second portion of data stored in the data memory and to store the result in the data memory.

18. A portable data carrier as claimed in any one of claims 10 to 17, further comprising non-volatile communications parameter memory for storing data for accessing a communications network to receive data from the communications network for storage in the data memory.

19. A portable data carrier as claimed in any one of claims 10 to 18, wherein the data memory is partitioned for access on a block-by-block basis, each block comprising a plurality of data bytes read or written as a set.

20. A portable data carrier as claimed in any one of claims 10 to 19 wherein said data memory has a capacity of greater than 1 MByte, more preferably > 100 MBytes, and most preferably > 1 GByte.

21. A portable data carrier as claimed in any one of claims 10 to 20 substantially configured as an IC card or smart card.

22. A method of controlling access to data on a data carrier, the data carrier comprising non-volatile data memory and non-volatile parameter memory storing use status data and use rules, the method comprising:

receiving a data access request;

reading the use status data and use rules from memory; and

evaluating the use status data using the use rules to determine whether access to the stored data is permitted.

23. A method as claimed in claim 22 wherein said parameter memory further stores payment data and further comprising selecting a said use rule dependent upon said payment data.

24. A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and a pointer to a data provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester;

code to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code responsive to the request and to the received payment data, to read data for the requested data item from a content provider; and

code to transmit the read data to the requester over the communications interface.

25. A computer system as claimed in claim 24, wherein said data access data store further comprises payment distribution information indicating to whom payments

should be made for a data item; and further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

26. A computer system as claimed in claim 24 or 25, wherein said data access data store further comprises data item access rule data for output to the requester with said data item.

27. A computer system as claimed in claim 26, further comprising code to select access rule data for output with a data item in response to said payment data.

28. A computer system as claimed in claim 27, wherein said data access data store further comprises requester reward data associated with a said data item, and said code further comprises code to update said reward data in response to said payment data.

29. A computer system as claimed in any one of claims 24 to 28, further comprising an access control data store coupled to said processor for storing access control data comprising a requester identifier, corresponding requester system access data and payment system data for identifying a payment system for use by the requester.

30. A computer system as claimed in any one of claims 24 to 29, further comprising content synthesis code to generate substantially complete item data from partial item data provided from two or more sources.

31. A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

reading the requested data from a content provider responsive to the received payment data; and

transmitting the read data to the requester.

32. A method of providing data to a data requester as claimed in claim 31 further comprising:

reading payment distribution information from a data store; and

outputting payment data to a payment system for distributing the payment for the requested data.

33. A method of providing data to a data requester as claimed in claim 31 or 32 further comprising:

transmitting data access rule data to requester with the read data.

34. A method of providing data to a data requester as claimed in claim 33 further comprising:

selecting said access rule data dependent upon said payment data.

35. A data access terminal for retrieving data from a data supplier and providing the retrieved data to a data carrier, the terminal comprising:

a first interface for communicating with the data supplier;

a data carrier interface for interfacing with the data carrier;

a program store storing code implementable by a processor; and

a processor, coupled to the first interface, the data carrier interface and to the program store for implementing the stored code, the code comprising:

code to read payment data from the data carrier and to forward the payment data to a payment validation system;

code to receive payment validation data from the payment validation system;

code responsive to the payment validation data to retrieve data from the data supplier and to write the retrieved data into the data carrier.

36. A data access terminal as claimed in claim 35 further comprising code to transmit at least a portion of the payment validation data to the data supplier or to a destination received from the data supplier.

37. A data access terminal as claimed in claim 35 or 36 further comprising code to retrieve from the data supplier and output to a user stored data identifier data and associated value data and use rule data for a data item available from the data supplier.

38. A data access terminal as claimed in claim 37 further comprising code to write use rule data for a data item into the data carrier with the associated data item.

39. A data access terminal as claimed in claim 37 or 38 further comprising code to read a stored value from the data carrier, code to compare said stored value with said value data; and code to provide a modified output to a user of one or more of said stored data

identifier data, said value data and said use rule data, in response to a result of the comparison.

40. A data access terminal according to any one of claims 35 to 39 further comprising code for user input of access control data, code to output the access control data to the data carrier, code to receive access permission data from the card, and code to output data to the user in response to the received access permission data.

41. A data access terminal as claimed in claim 40 further comprising code to output a data erasure warming in response to the received access permission data.

42. A data access terminal according to any one of claims 35 to 41 further comprising code to read reward data from the data carrier and to write modified reward data to the data carrier in response to said retrieval of data from the data supplier.

43. A data access terminal according to any one of claims 35 to 42 further comprising:

code to read identity data from the data carrier;

code to transmit the identity data to the data supplier;

code to receive user characterizing data from the data supplier;

code to retrieve supplementary data in response to said characterizing data; and

code to output the supplementary data.

44. A data access terminal according to any one of claims 35 to 43 further comprising a cash input device coupled to the processor, to provide cash input value data; and code to update payment data in the data carrier, in accordance with the cash input value data.

45. A data access terminal according to any one of claims 35 to 44 integrated with a mobile communication device, a personal computer, an audio/video player, and/or a cable or satellite television interface device.

46. A method of providing data from a data supplier to a data carrier, the method comprising:

reading payment data from the data carrier;

forwarding the payment data to a payment validation system;

retrieving data from the data supplier; and

writing the retrieved data into the date carrier.

47. A method of providing data from a data supplier according to claim 46 further comprising:

receiving payment validation data from the payment validation system; and

transmitting at least a portion of the payment validation data to the data supplier.

48. A method of providing data as claimed in claim 47, wherein the payment validation system comprises a payment processor at the data supplier.

49. A method of providing data as claimed in claim 46, 47 or 48, further comprising:

retrieving from the data supplier a stored data item identifier and associated value data and use rule data; and

writing use rule data for the data item into the data carrier.

50. A method of providing data as claimed in claim 48 or 49, further comprising:

reading a stored value from the data carrier;

comparing the stored value with said value data; and

outputting to a user information indicating the result of said comparing.

51. A data access device for retrieving stored data from a data carrier, the device comprising:

a user interface;

a data carrier interface;

a program store storing code implementable by a processor; and

a processor coupled to the user interface, to the data carrier interface and to the program store for implementing the stored code, the code comprising:

code to retrieve use status data indicating a use status of data stored on the carrier, and use rules data indicating permissible use of data stored on the carrier;

code to evaluate the use status data using the use rules data to determine whether access is permitted to the stored data; and

code to access the stored data when access is permitted.

52. A data access device according to claim 51, further comprising code to write updated use status data to the carrier after user access to the stored data.

53. A data access device as claimed in claim 51 or 52, further comprising user access control code to input user access data, to transmit the user access data to the carrier, and to receive from the carrier user access permission data.

54. A data access device according to claim 53, further comprising code to select the use status and use rules data using the user access data.

55. A data access device as claimed in claim 53 or 54, further comprising code to retrieve and output supplementary data to the user.

56. A data access device according to any one of claims 51 to 55 wherein said use rules permit partial use of a data item stored on the carrier and further comprising code to write partial use status data to the data carrier when only part of a stored data item has been accessed.

57. A data access device according to any one of claims 51 to 56 wherein the device is portable and the data carrier interface is configured for interfacing with a removable data carrier.

58. A data access device according to claim 57 configured to interface with the data carrier of any one of claims 10 to 21.

59. A method of controlling access to data from a data carrier, comprising:

retrieving use status data from the data carrier indicating past use of the stored data;

retrieving use rules from the data carrier;

evaluating the use status data using the use rules to determine whether access to data stored on the carrier is permitted; and

permitting access to the data on the data carrier dependent on the result of said evaluating.

60. A method of controlling access according to claim 59, further comprising:

writing updated use status data to the carrier after an access attempt.

61. A method of controlling access according to claim 60, wherein said use rules permit partial access to a data item and wherein said writing writes a record of what part of the data item has been accessed when only part of the data item has been accessed.

62. A method of controlling access according to any one of claims 59 to 61, further comprising:

inputting a user access data;

selecting the use rules dependent upon the user access data.

63. A data access system comprising a data supply computer system for forwarding data from a data provider to a data access terminal; a electronic payment system for confirming an electronic payment; a data access terminal for communicating with the data supply system to write data from the data supply system onto a data carrier; and a data carrier for storing data from the data supply system and payment data; wherein data is forwarded from the data provider to the data carrier on validation of payment data provided from the data carrier to the electronic payment system.

64. A data access system according to claim 63 further comprising a payment distribution store and wherein the electronic payment system makes payments according to data in the payment distribution store associated with the forwarded data on confirmation of the payment and/or provision of the forwarded data to the card.

65. A data access system according to claim 63 or 64 further comprising a data use rule data store and wherein data use rule data is provided to the data carrier with the forwarded data for controlling user access to the forwarded data.

66. A data access system according to claim 65 wherein the data use rule data is selected dependent upon the payment data.

67. A portable data carrier comprising:

an interface for sending and receiving data from and to the carrier;

non-volatile data memory, coupled to the interface, for storing data on the carrier; and

a digital rights management processor for controlling access to the stored data.

68. A portable data carrier comprising:

an interface for sending and receiving data from and to the carrier;

non-volatile data memory, coupled to the interface, for storing data on the carrier; and

an access control processor;

wherein the data memory is partitioned as data blocks and the access control processor controls external access to the data blocks.

69. A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and a resource locator a data provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code, responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and

further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

70. A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and location data identifying an electronic address for a provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises data item access rule data for output to the requester with a said data item; and

further comprising code to select access rule data for output with a data item in response to said payment data.

71. A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

transmitting the requested data to the requester;

reading payment distribution information from a data store; and

outputting payment data to a payment system for distributing the payment for the requested data.

72. A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

transmitting the requested data to the requester; and

transmitting data access rule data to requester with the read data.

73. A computer program to, when running, carry out the method of any preceding method claim.

74. A computer readable medium carrying the computer program of claim 73.

DATA STORAGE AND ACCESS SYSTEMS

ABSTRACT OF THE DISCLOSURE

Data storage and access systems are described for downloading and paying for data such as audio and video data, text, software, games and other types of data. A portable data carrier has an interface for sending and receiving data, non-volatile data memory for storing received content data and non-volatile payment validation memory for providing payment validation data to an external device. The carrier may also store a record of access made to the stored content, and content use rules for controlling access to the stored content. Preferred embodiments store further access control data and supplementary data such as hot links to web sites and/or advertising data. A complementary data access terminal, data supply computer system and data access device are also described. The combination of payment data and stored content data and, in preferred embodiments, use rule data, helps reduce the risk of unauthorized access to data such as compressed music and video data, especially over the Internet.

61257267 v1

Fig. 1

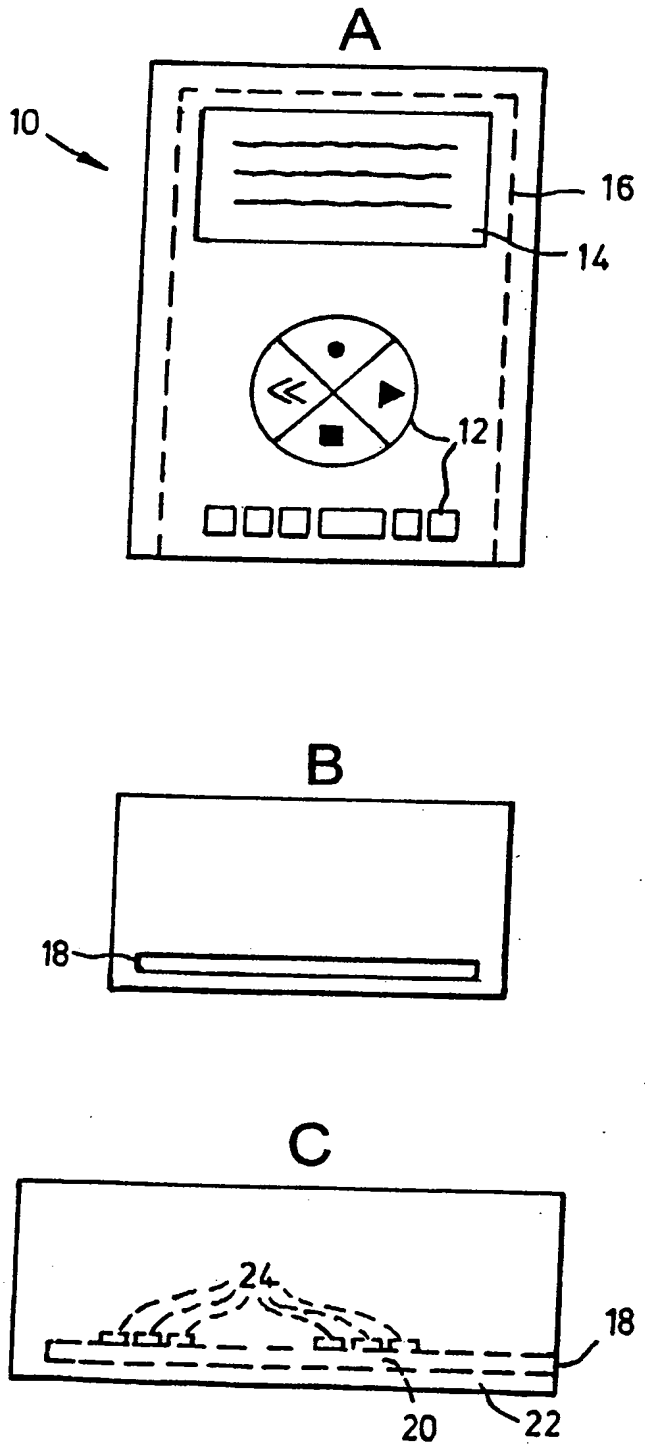


Fig. 2

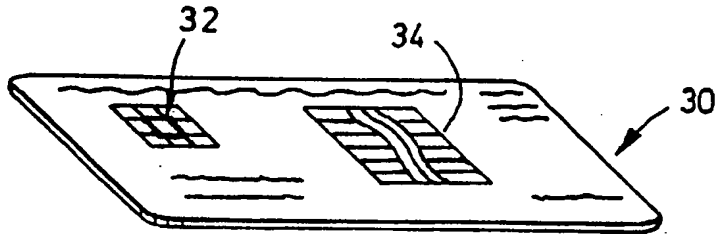


Fig. 3

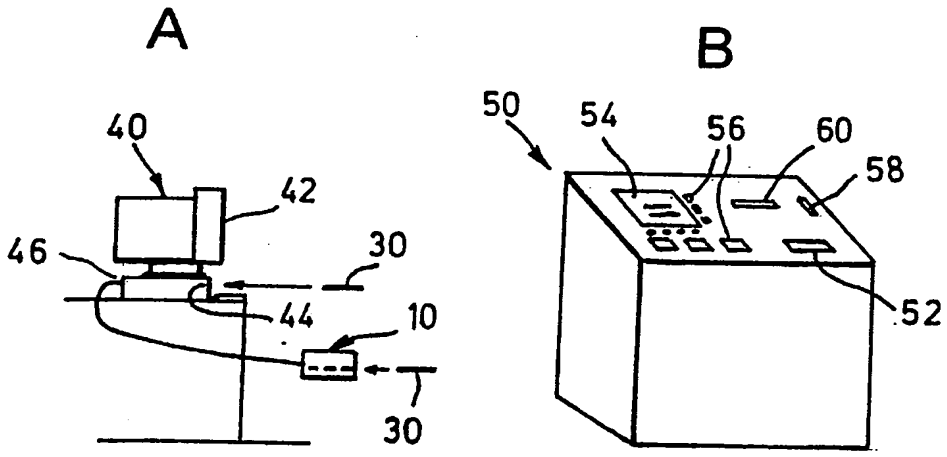
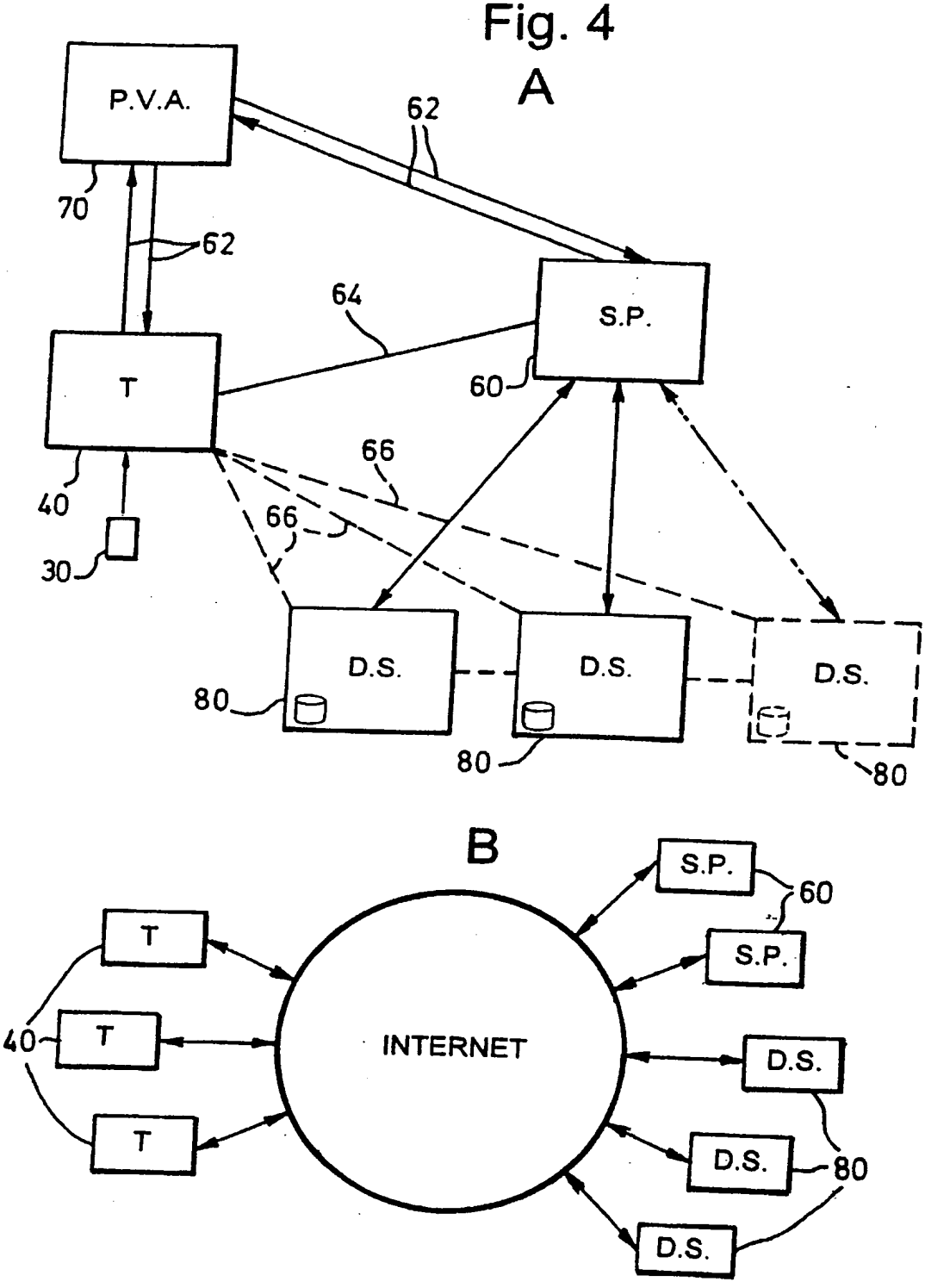


Fig. 4


A
P.V.A.
62
70
62
64
S.P.
T
60
66
40
66
30
D.S.
D.S.
D.S.
80
80
80
B
S.P.
60
S.P.
T
T
INTERNET
40
D.S.
T
D.S.
80
D.S.

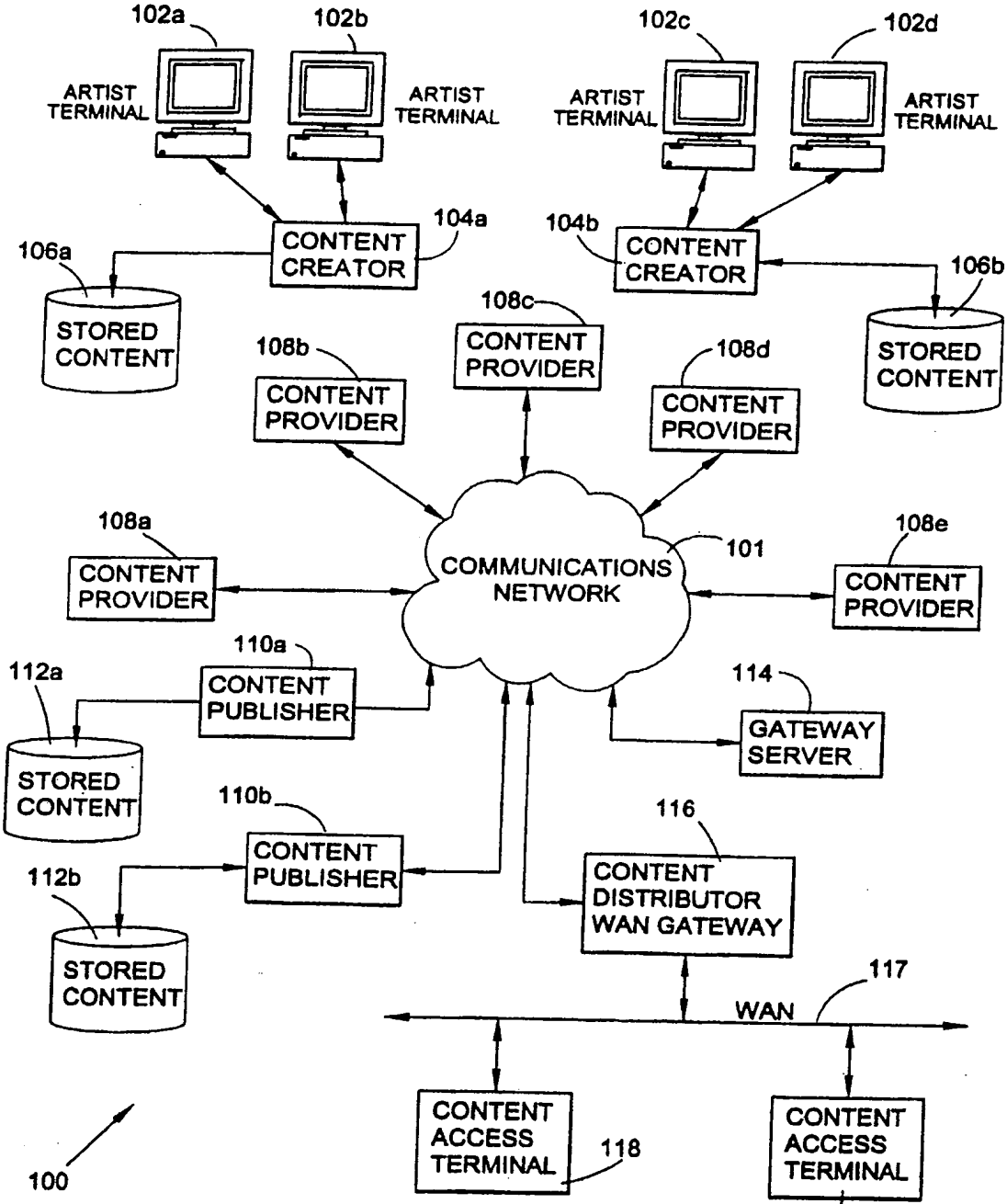

102a
102b
102c
102d
ARTIST TERMINAL
ARTIST TERMINAL
ARTIST TERMINAL
ARTIST TERMINAL
CONTENT CREATOR
104a
CONTENT CREATOR
104b
106a
STORED CONTENT
106b
STORED CONTENT
108c
CONTENT PROVIDER
108b
CONTENT PROVIDER
108d
CONTENT PROVIDER
108a
CONTENT PROVIDER
COMMUNICATIONS NETWORK
101
108e
CONTENT PROVIDER
110a
CONTENT PUBLISHER
112a
STORED CONTENT
114
GATEWAY SERVER
110b
CONTENT PUBLISHER
116
CONTENT DISTRIBUTOR WAN GATEWAY
112b
STORED CONTENT
117
WAN
CONTENT ACCESS TERMINAL
118
CONTENT ACCESS TERMINAL
118
100

Fig. 5

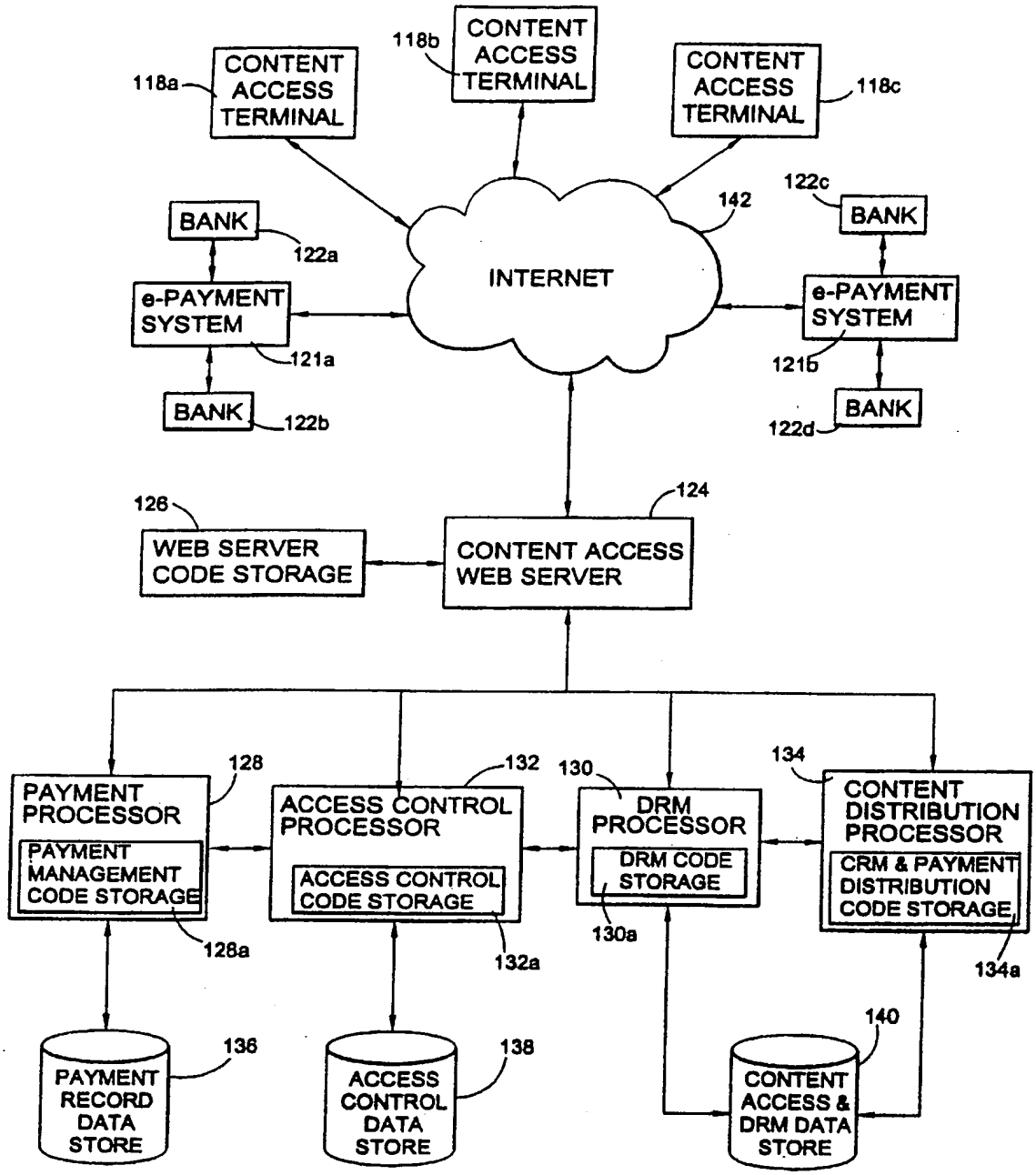

CONTENT ACCESS TERMINAL
118a
CONTENT ACCESS TERMINAL
118b
CONTENT ACCESS TERMINAL
118c
INTERNET
142
BANK
122a
BANK
122c
e-PAYMENT SYSTEM
121a
e-PAYMENT SYSTEM
121b
BANK
122b
BANK
122d
126
WEB SERVER CODE STORAGE
CONTENT ACCESS WEB SERVER
124
PAYMENT PROCESSOR
PAYMENT MANAGEMENT CODE STORAGE
128
128a
ACCESS CONTROL PROCESSOR
ACCESS CONTROL CODE STORAGE
132
132a
DRM PROCESSOR
DRM CODE STORAGE
130
130a
CONTENT DISTRIBUTION PROCESSOR
CRM & PAYMENT DISTRIBUTION CODE STORAGE
134
134a
PAYMENT RECORD DATA STORE
136
ACCESS CONTROL DATA STORE
138
CONTENT ACCESS & DRM DATA STORE
140
120

Fig.6

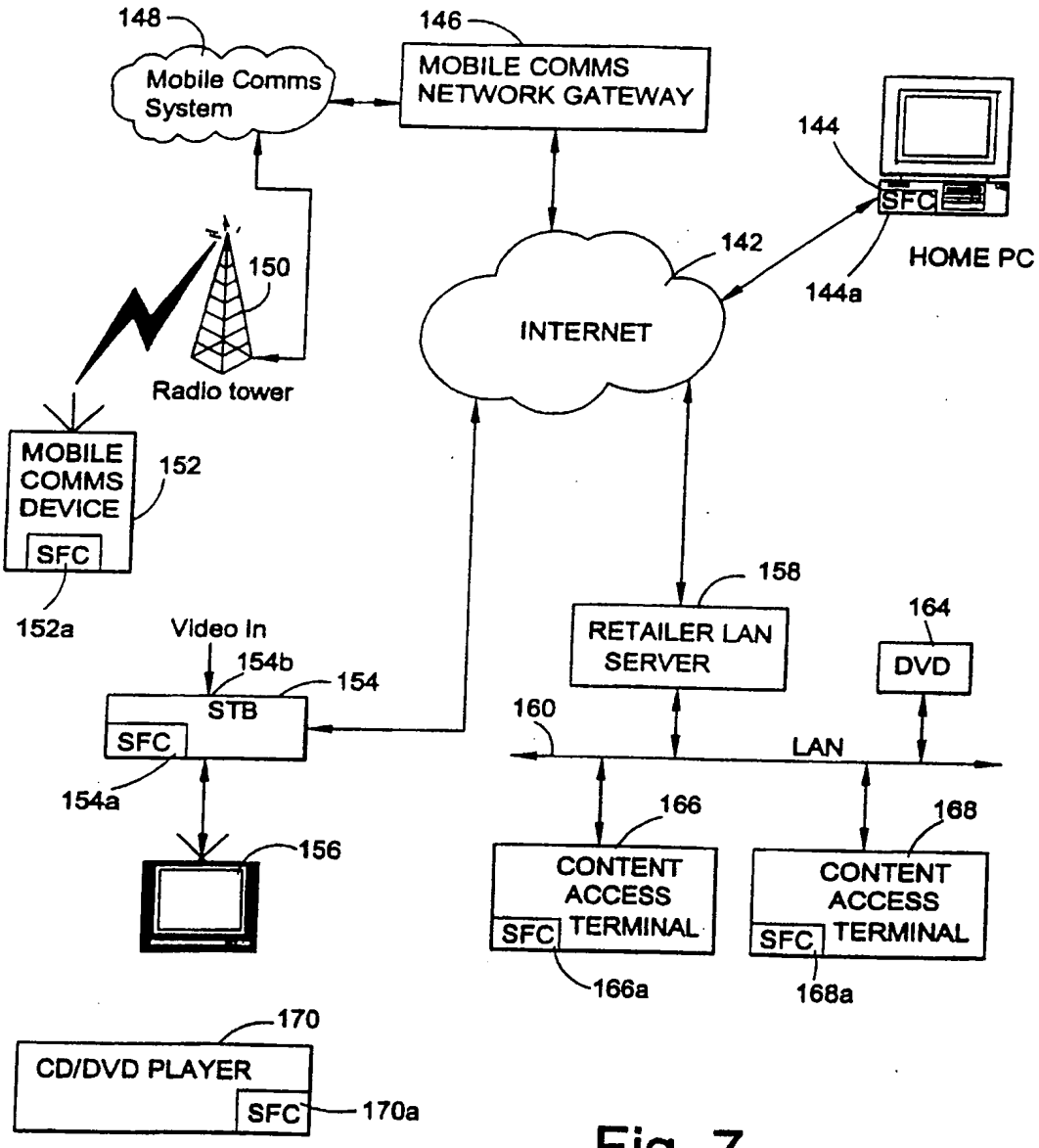

148
Mobile Comms System
146
MOBILE COMMS NETWORK GATEWAY
144
SFC
HOME PC
144a
142
INTERNET
150
Radio tower
MOBILE COMMS DEVICE
SFC
152
152a
Video In
154b
154
STB
SFC
154a
156
158
RETAILER LAN SERVER
164
DVD
160
LAN
166
CONTENT ACCESS TERMINAL
SFC
166a
168
CONTENT ACCESS TERMINAL
SFC
168a
170
CD/DVD PLAYER
SFC
170a

Fig. 7

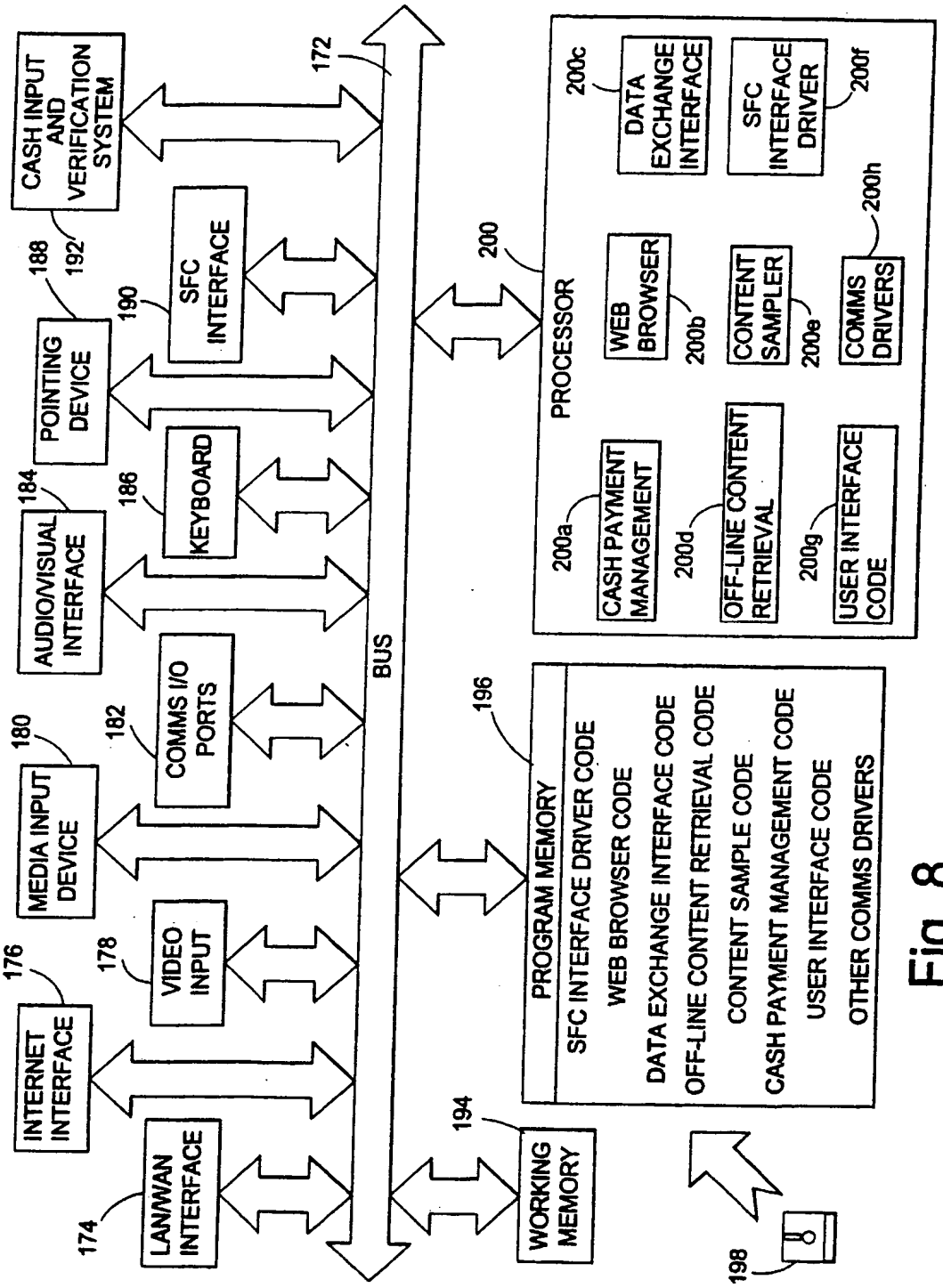

CASH INPUT AND VERIFICATION SYSTEM
192
188
POINTING DEVICE
190
SFC INTERFACE
172
BUS
184
AUDIO/VISUAL INTERFACE
186
KEYBOARD
180
MEDIA INPUT DEVICE
182
COMMS I/O PORTS
176
INTERNET INTERFACE
178
VIDEO INPUT
174
LAN/WAN INTERFACE
194
WORKING MEMORY
196
PROGRAM MEMORY
SFC INTERFACE DRIVER CODE
WEB BROWSER CODE
DATA EXCHANGE INTERFACE CODE
OFF-LINE CONTENT RETRIEVAL CODE
CONTENT SAMPLE CODE
CASH PAYMENT MANAGEMENT CODE
USER INTERFACE CODE
OTHER COMMS DRIVERS
198
200
PROCESSOR
200a
CASH PAYMENT MANAGEMENT
200b
WEB BROWSER
200c
DATA EXCHANGE INTERFACE
200d
OFF-LINE CONTENT RETRIEVAL
200e
CONTENT SAMPLER
200f
SFC INTERFACE DRIVER
200g
USER INTERFACE CODE
200h
COMMS DRIVERS

Fig. 8

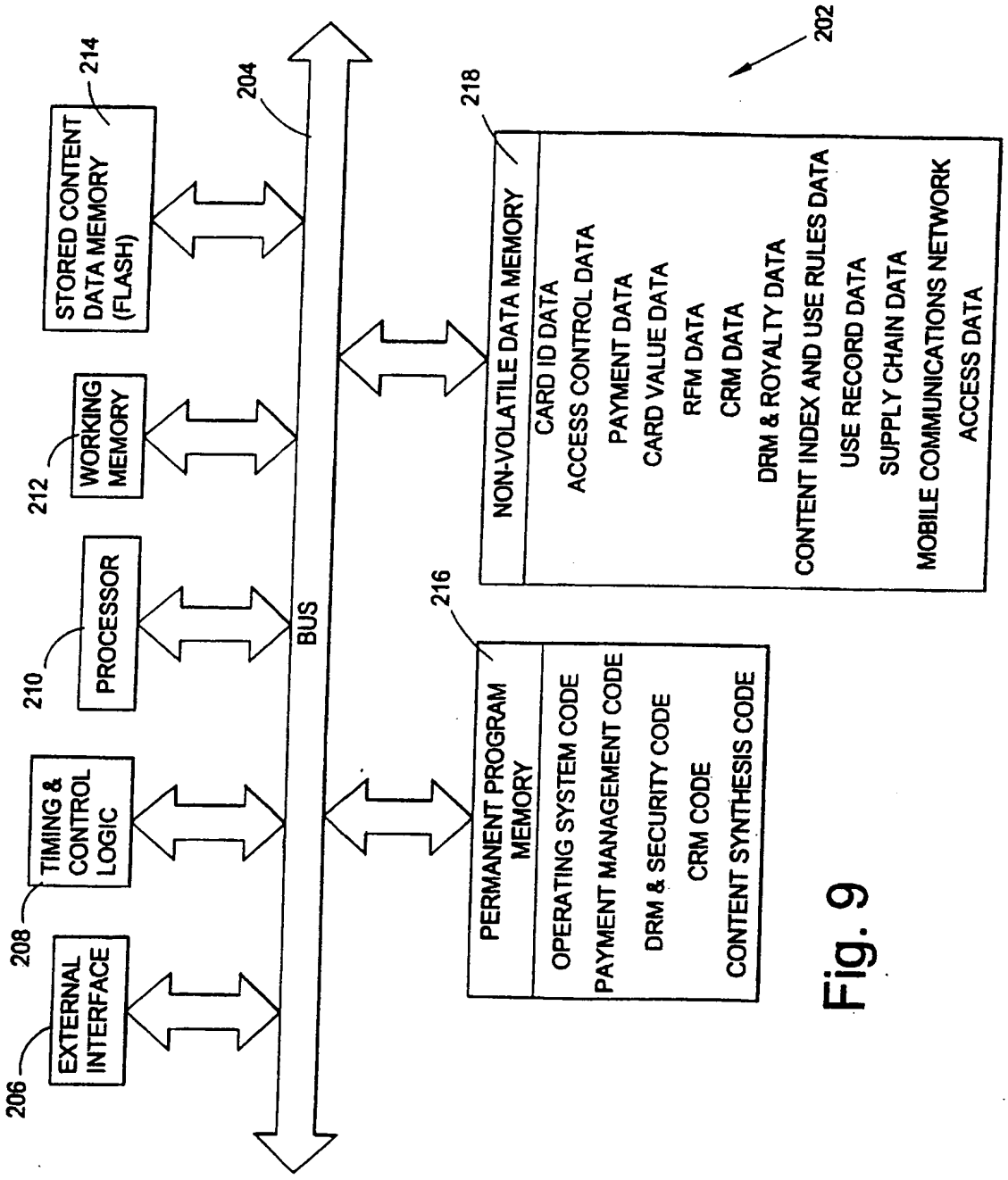

202
204
206
208
210
212
214
216
218
EXTERNAL INTERFACE
TIMING & CONTROL LOGIC
PROCESSOR
WORKING MEMORY
STORED CONTENT DATA MEMORY (FLASH)
BUS
PERMANENT PROGRAM MEMORY
OPERATING SYSTEM CODE
PAYMENT MANAGEMENT CODE
DRM & SECURITY CODE
CRM CODE
CONTENT SYNTHESIS CODE
NON-VOLATILE DATA MEMORY
CARD ID DATA
ACCESS CONTROL DATA
PAYMENT DATA
CARD VALUE DATA
RFM DATA
CRM DATA
DRM & ROYALTY DATA
CONTENT INDEX AND USE RULES DATA
USE RECORD DATA
SUPPLY CHAIN DATA
MOBILE COMMUNICATIONS NETWORK
ACCESS DATA

Fig. 9

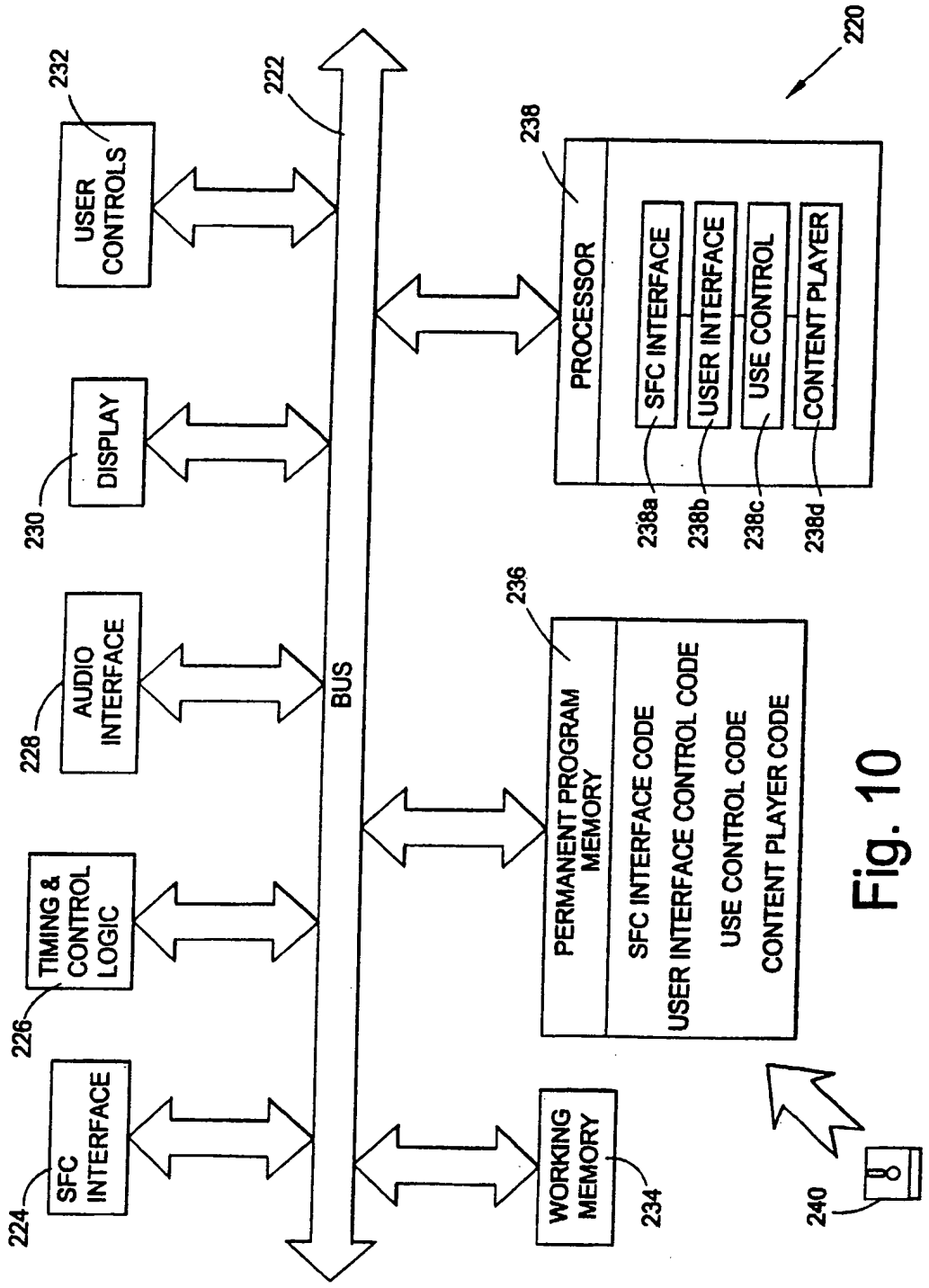

220
232
USER CONTROLS
222
238
PROCESSOR
SFC INTERFACE
USER INTERFACE
USE CONTROL
CONTENT PLAYER
238a
238b
238c
238d
230
DISPLAY
228
AUDIO INTERFACE
BUS
236
PERMANENT PROGRAM MEMORY
SFC INTERFACE CODE
USER INTERFACE CONTROL CODE
USE CONTROL CODE
CONTENT PLAYER CODE
226
TIMING & CONTROL LOGIC
224
SFC INTERFACE
WORKING MEMORY
234
240

Fig. 10

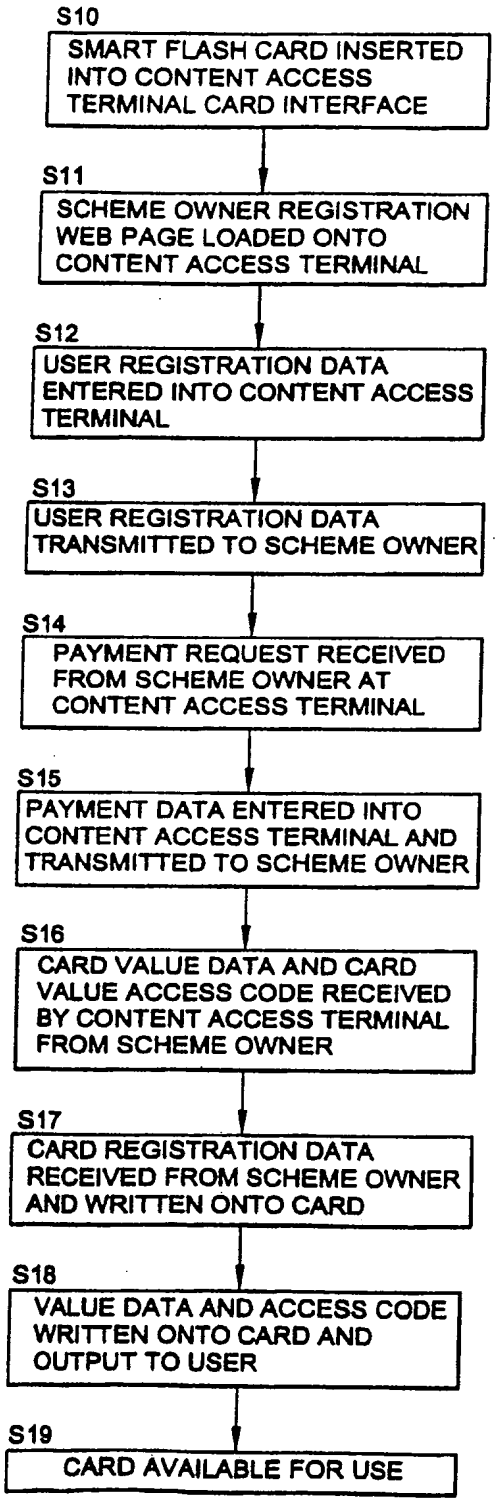

S10
SMART FLASH CARD INSERTED INTO CONTENT ACCESS TERMINAL CARD INTERFACE
S11
SCHEME OWNER REGISTRATION WEB PAGE LOADED ONTO CONTENT ACCESS TERMINAL
S12
USER REGISTRATION DATA ENTERED INTO CONTENT ACCESS TERMINAL
S13
USER REGISTRATION DATA TRANSMITTED TO SCHEME OWNER
S14
PAYMENT REQUEST RECEIVED FROM SCHEME OWNER AT CONTENT ACCESS TERMINAL
S15
PAYMENT DATA ENTERED INTO CONTENT ACCESS TERMINAL AND TRANSMITTED TO SCHEME OWNER
S16
CARD VALUE DATA AND CARD VALUE ACCESS CODE RECEIVED BY CONTENT ACCESS TERMINAL FROM SCHEME OWNER
S17
CARD REGISTRATION DATA RECEIVED FROM SCHEME OWNER AND WRITTEN ONTO CARD
S18
VALUE DATA AND ACCESS CODE WRITTEN ONTO CARD AND OUTPUT TO USER
S19
CARD AVAILABLE FOR USE

Fig11a

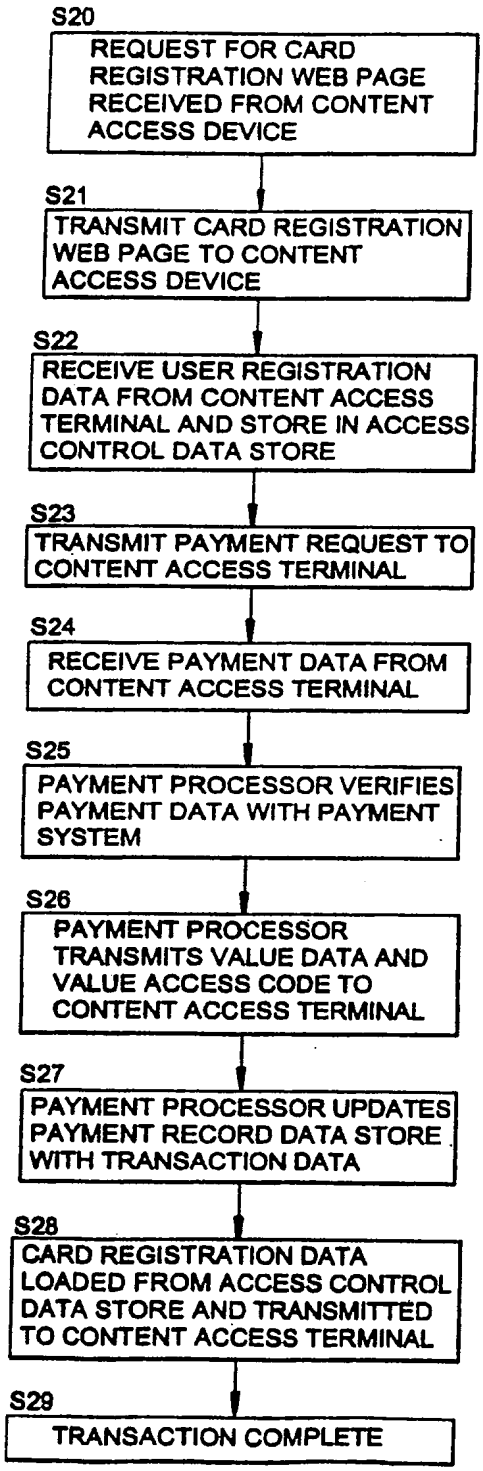

S20
REQUEST FOR CARD REGISTRATION WEB PAGE RECEIVED FROM CONTENT ACCESS DEVICE
S21
TRANSMIT CARD REGISTRATION WEB PAGE TO CONTENT ACCESS DEVICE
S22
RECEIVE USER REGISTRATION DATA FROM CONTENT ACCESS TERMINAL AND STORE IN ACCESS CONTROL DATA STORE
S23
TRANSMIT PAYMENT REQUEST TO CONTENT ACCESS TERMINAL
S24
RECEIVE PAYMENT DATA FROM CONTENT ACCESS TERMINAL
S25
PAYMENT PROCESSOR VERIFIES PAYMENT DATA WITH PAYMENT SYSTEM
S26
PAYMENT PROCESSOR TRANSMITS VALUE DATA AND VALUE ACCESS CODE TO CONTENT ACCESS TERMINAL
S27
PAYMENT PROCESSOR UPDATES PAYMENT RECORD DATA STORE WITH TRANSACTION DATA
S28
CARD REGISTRATION DATA LOADED FROM ACCESS CONTROL DATA STORE AND TRANSMITTED TO CONTENT ACCESS TERMINAL
S29
TRANSACTION COMPLETE

Fig.11b

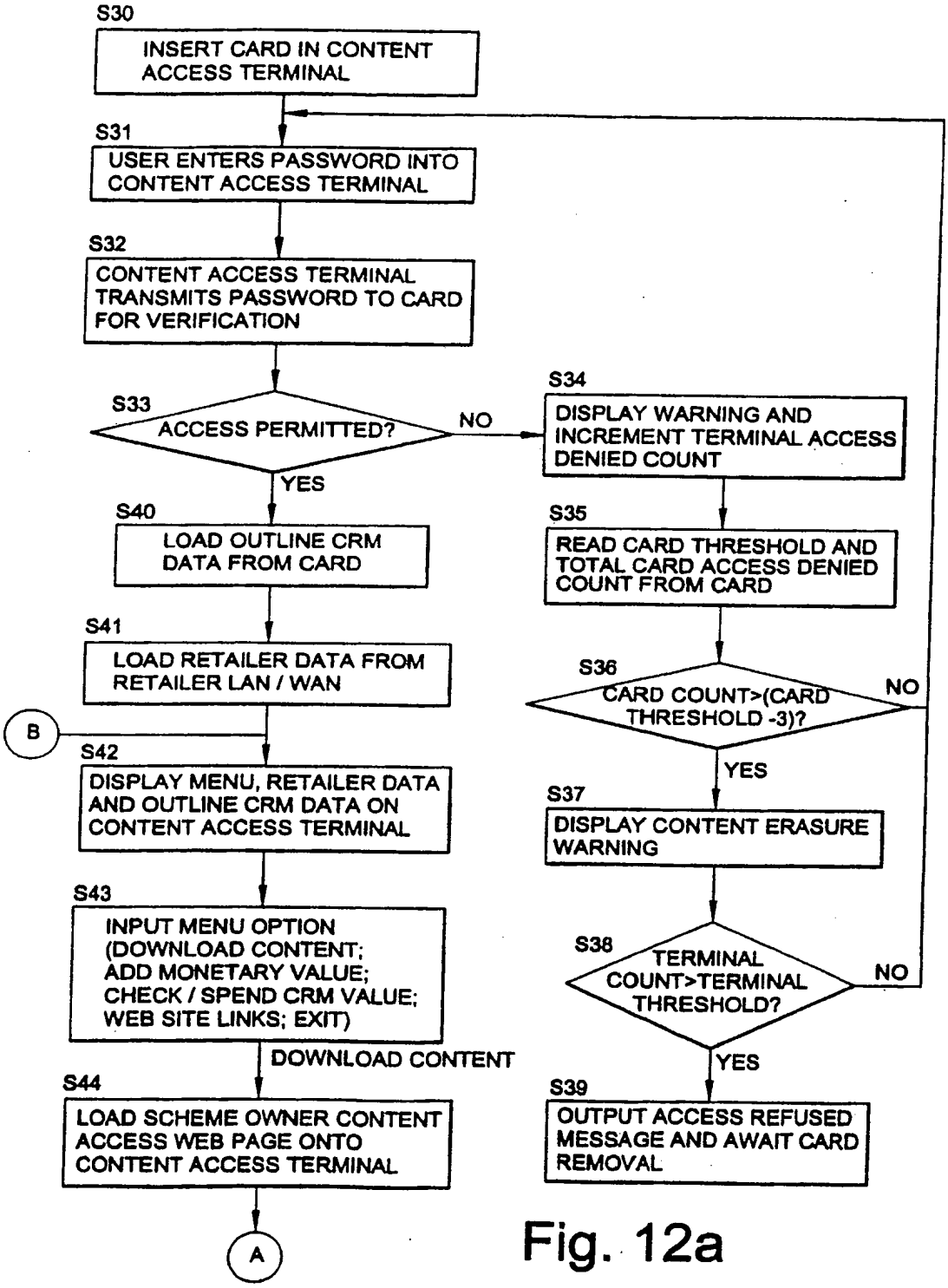

S30
INSERT CARD IN CONTENT ACCESS TERMINAL
S31
USER ENTERS PASSWORD INTO CONTENT ACCESS TERMINAL
S32
CONTENT ACCESS TERMINAL TRANSMITS PASSWORD TO CARD FOR VERIFICATION
S33
ACCESS PERMITTED?
NO
YES
S34
DISPLAY WARNING AND INCREMENT TERMINAL ACCESS DENIED COUNT
S35
READ CARD THRESHOLD AND TOTAL CARD ACCESS DENIED COUNT FROM CARD
S36
CARD COUNT>(CARD THRESHOLD -3)?
NO
YES
S37
DISPLAY CONTENT ERASURE WARNING
S38
TERMINAL COUNT>TERMINAL THRESHOLD?
NO
YES
S39
OUTPUT ACCESS REFUSED MESSAGE AND AWAIT CARD REMOVAL
S40
LOAD OUTLINE CRM DATA FROM CARD
S41
LOAD RETAILER DATA FROM RETAILER LAN / WAN
B
S42
DISPLAY MENU, RETAILER DATA AND OUTLINE CRM DATA ON CONTENT ACCESS TERMINAL
S43
INPUT MENU OPTION (DOWNLOAD CONTENT; ADD MONETARY VALUE; CHECK / SPEND CRM VALUE; WEB SITE LINKS; EXIT)
DOWNLOAD CONTENT
S44
LOAD SCHEME OWNER CONTENT ACCESS WEB PAGE ONTO CONTENT ACCESS TERMINAL
A

Fig. 12a

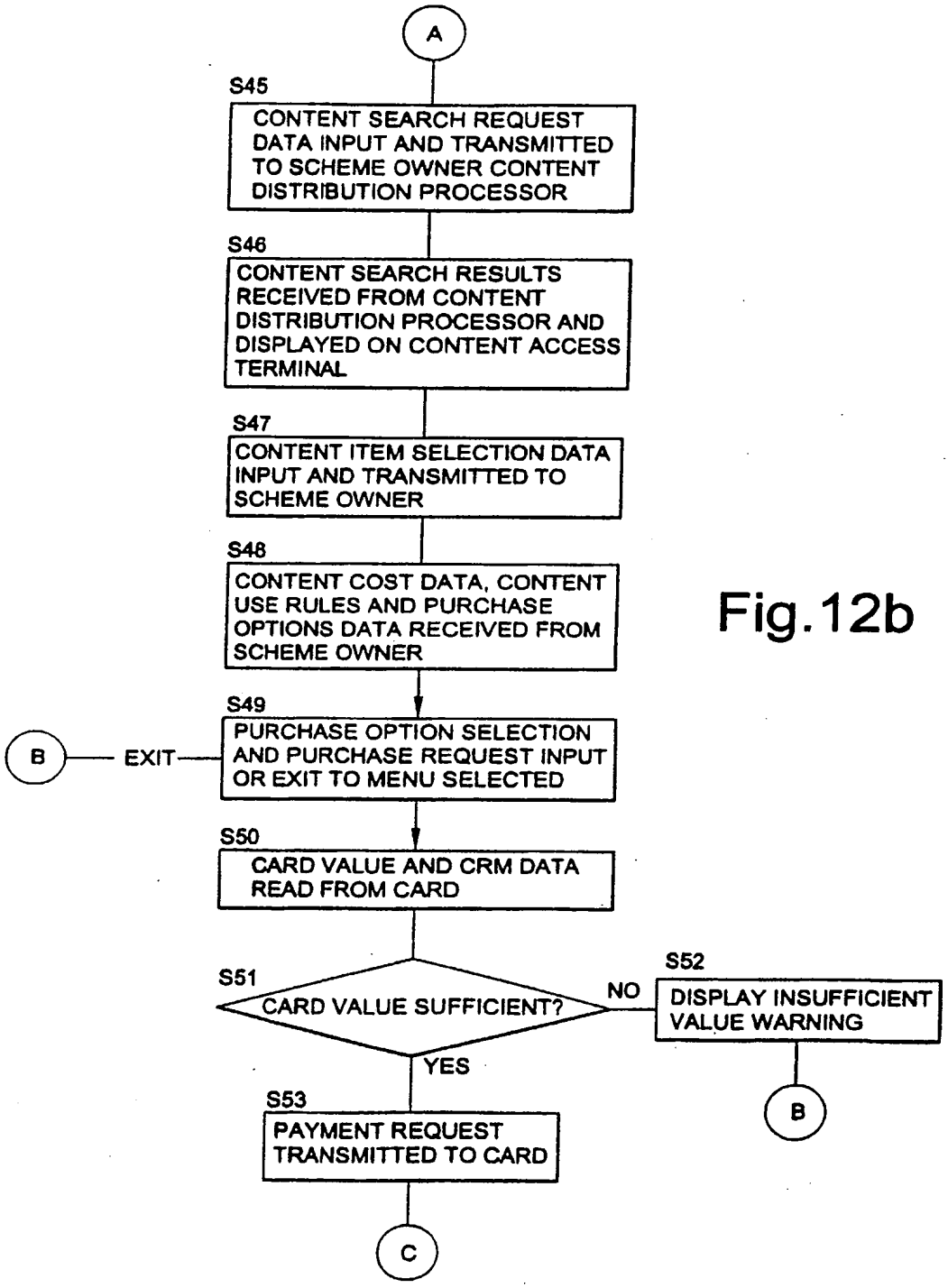

A
S45
CONTENT SEARCH REQUEST DATA INPUT AND TRANSMITTED TO SCHEME OWNER CONTENT DISTRIBUTION PROCESSOR
S46
CONTENT SEARCH RESULTS RECEIVED FROM CONTENT DISTRIBUTION PROCESSOR AND DISPLAYED ON CONTENT ACCESS TERMINAL
S47
CONTENT ITEM SELECTION DATA INPUT AND TRANSMITTED TO SCHEME OWNER
S48
CONTENT COST DATA, CONTENT USE RULES AND PURCHASE OPTIONS DATA RECEIVED FROM SCHEME OWNER
S49
B
EXIT
PURCHASE OPTION SELECTION AND PURCHASE REQUEST INPUT OR EXIT TO MENU SELECTED
S50
CARD VALUE AND CRM DATA READ FROM CARD
S51
CARD VALUE SUFFICIENT?
NO
S52
DISPLAY INSUFFICIENT VALUE WARNING
B
YES
S53
PAYMENT REQUEST TRANSMITTED TO CARD
C

Fig.12b

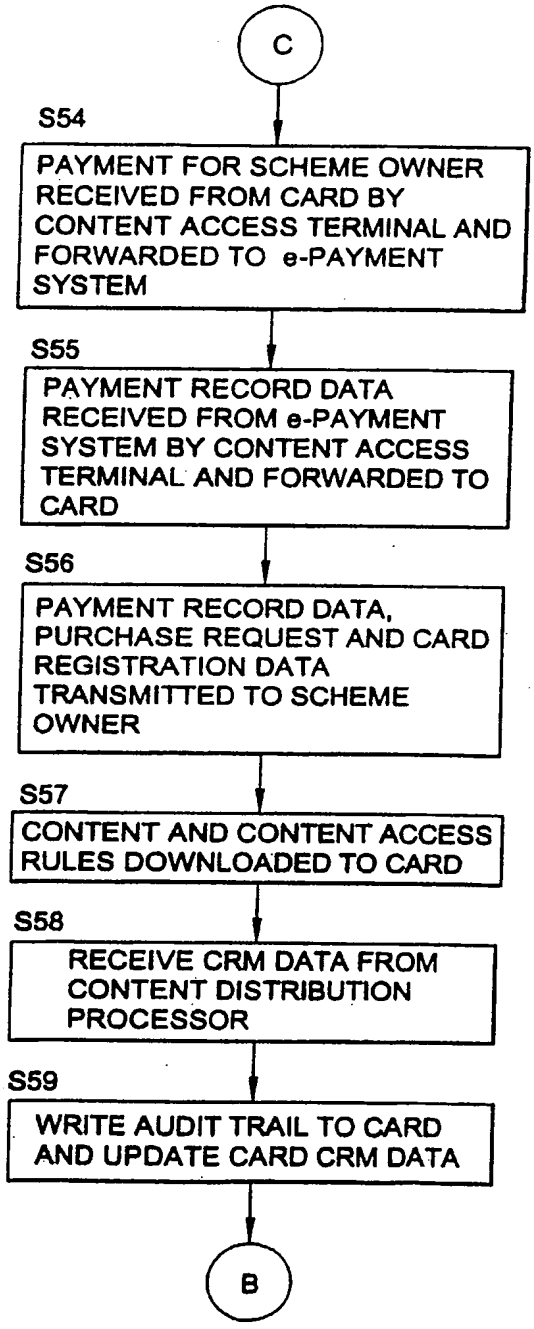

C
S54
PAYMENT FOR SCHEME OWNER RECEIVED FROM CARD BY CONTENT ACCESS TERMINAL AND FORWARDED TO e-PAYMENT SYSTEM
S55
PAYMENT RECORD DATA RECEIVED FROM e-PAYMENT SYSTEM BY CONTENT ACCESS TERMINAL AND FORWARDED TO CARD
S56
PAYMENT RECORD DATA, PURCHASE REQUEST AND CARD REGISTRATION DATA TRANSMITTED TO SCHEME OWNER
S57
CONTENT AND CONTENT ACCESS RULES DOWNLOADED TO CARD
S58
RECEIVE CRM DATA FROM CONTENT DISTRIBUTION PROCESSOR
S59
WRITE AUDIT TRAIL TO CARD AND UPDATE CARD CRM DATA
B

Fig.12c

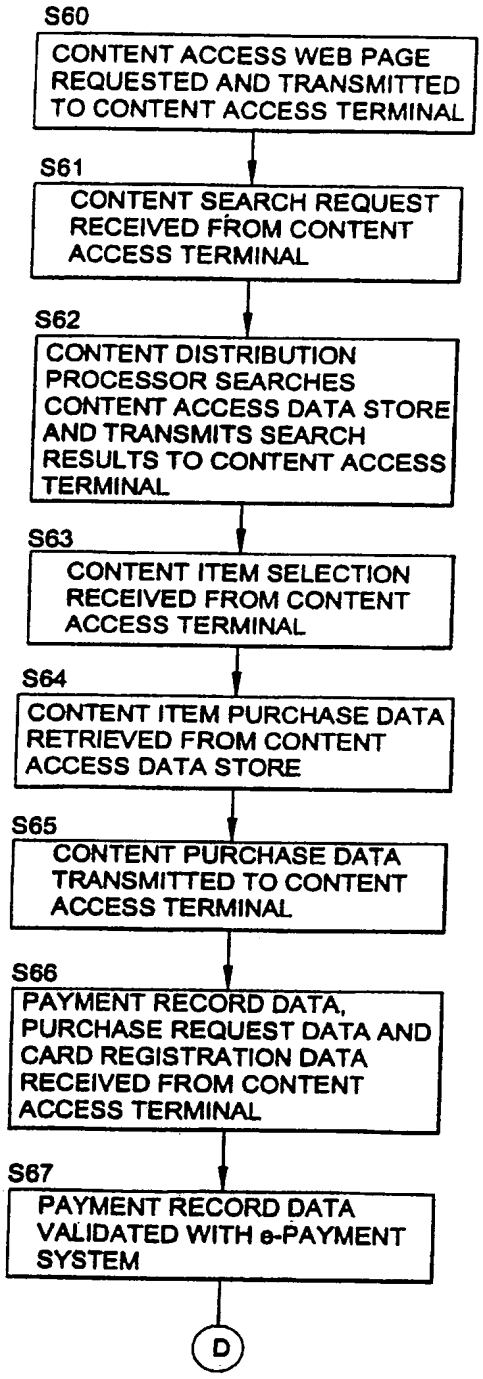

S60
CONTENT ACCESS WEB PAGE REQUESTED AND TRANSMITTED TO CONTENT ACCESS TERMINAL
S61
CONTENT SEARCH REQUEST RECEIVED FROM CONTENT ACCESS TERMINAL
S62
CONTENT DISTRIBUTION PROCESSOR SEARCHES CONTENT ACCESS DATA STORE AND TRANSMITS SEARCH RESULTS TO CONTENT ACCESS TERMINAL
S63
CONTENT ITEM SELECTION RECEIVED FROM CONTENT ACCESS TERMINAL
S64
CONTENT ITEM PURCHASE DATA RETRIEVED FROM CONTENT ACCESS DATA STORE
S65
CONTENT PURCHASE DATA TRANSMITTED TO CONTENT ACCESS TERMINAL
S66
PAYMENT RECORD DATA, PURCHASE REQUEST DATA AND CARD REGISTRATION DATA RECEIVED FROM CONTENT ACCESS TERMINAL
S67
PAYMENT RECORD DATA VALIDATED WITH e-PAYMENT SYSTEM
D

Fig. 12d

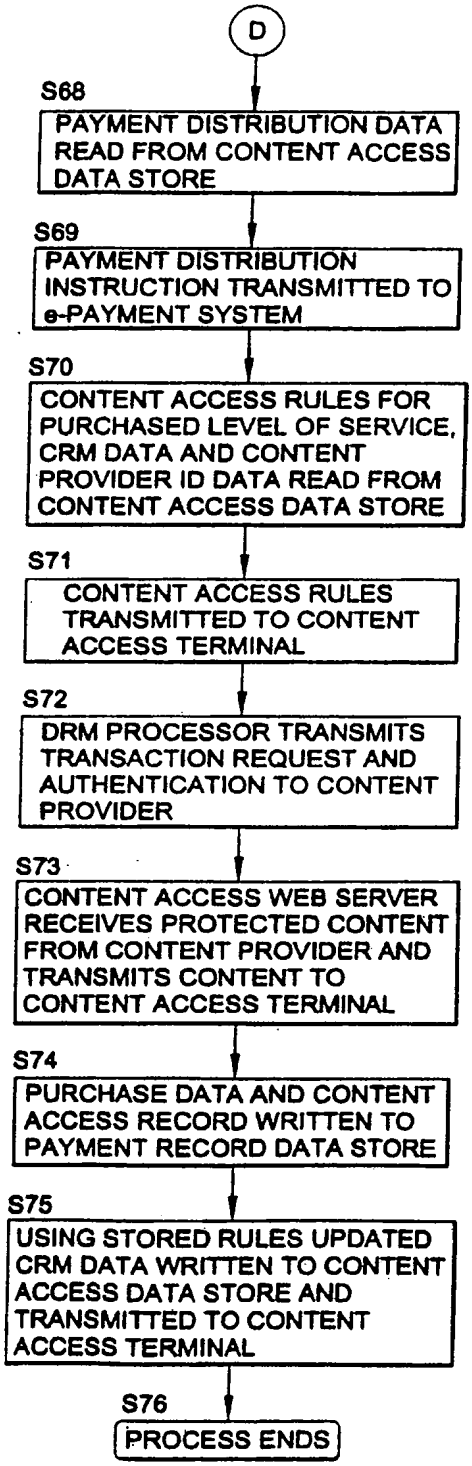

D
S68
PAYMENT DISTRIBUTION DATA READ FROM CONTENT ACCESS DATA STORE
S69
PAYMENT DISTRIBUTION INSTRUCTION TRANSMITTED TO e-PAYMENT SYSTEM
S70
CONTENT ACCESS RULES FOR PURCHASED LEVEL OF SERVICE, CRM DATA AND CONTENT PROVIDER ID DATA READ FROM CONTENT ACCESS DATA STORE
S71
CONTENT ACCESS RULES TRANSMITTED TO CONTENT ACCESS TERMINAL
S72
DRM PROCESSOR TRANSMITS TRANSACTION REQUEST AND AUTHENTICATION TO CONTENT PROVIDER
S73
CONTENT ACCESS WEB SERVER RECEIVES PROTECTED CONTENT FROM CONTENT PROVIDER AND TRANSMITS CONTENT TO CONTENT ACCESS TERMINAL
S74
PURCHASE DATA AND CONTENT ACCESS RECORD WRITTEN TO PAYMENT RECORD DATA STORE
S75
USING STORED RULES UPDATED CRM DATA WRITTEN TO CONTENT ACCESS DATA STORE AND TRANSMITTED TO CONTENT ACCESS TERMINAL
S76
PROCESS ENDS

Fig. 12e

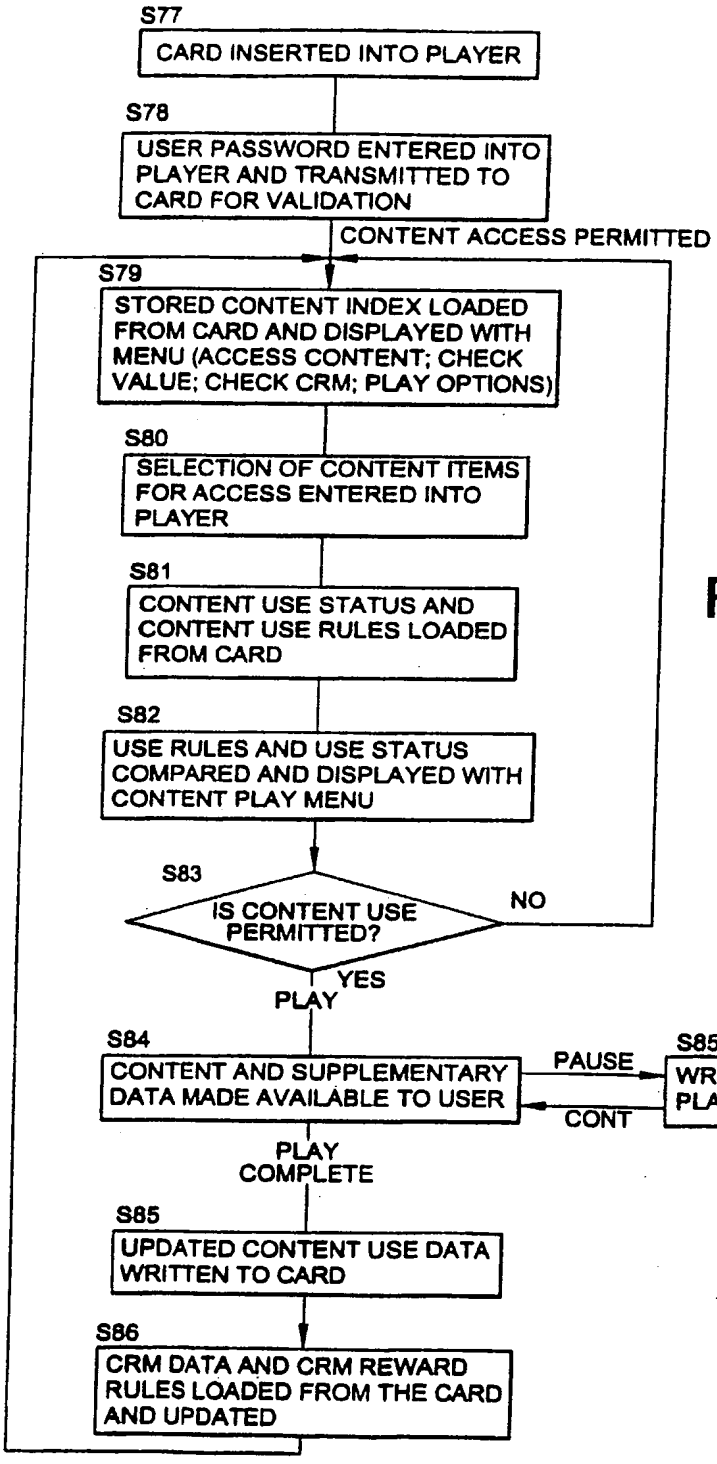

S77
CARD INSERTED INTO PLAYER
S78
USER PASSWORD ENTERED INTO PLAYER AND TRANSMITTED TO CARD FOR VALIDATION
CONTENT ACCESS PERMITTED
S79
STORED CONTENT INDEX LOADED FROM CARD AND DISPLAYED WITH MENU (ACCESS CONTENT; CHECK VALUE; CHECK CRM; PLAY OPTIONS)
S80
SELECTION OF CONTENT ITEMS FOR ACCESS ENTERED INTO PLAYER
S81
CONTENT USE STATUS AND CONTENT USE RULES LOADED FROM CARD
S82
USE RULES AND USE STATUS COMPARED AND DISPLAYED WITH CONTENT PLAY MENU
S83
IS CONTENT USE PERMITTED?
NO
YES
PLAY
S84
CONTENT AND SUPPLEMENTARY DATA MADE AVAILABLE TO USER
PAUSE
CONT
S85
WRITE/READ CARDS PLAY STATUS DATA
PLAY COMPLETE
S85
UPDATED CONTENT USE DATA WRITTEN TO CARD
S86
CRM DATA AND CRM REWARD RULES LOADED FROM THE CARD AND UPDATED

Fig. 13

Application Data Sheet

Application Information

Application number::	
Filing Date::	January 15, 2008
Application Type::	Regular
Subject Matter::	Utility
Title::	DATA STORAGE AND ACCESS SYSTEMS
Attorney Docket Number::	080379-000110US
Request for Early Publication::	No
Request for Non-Publication::	No
Suggested Drawing Figure::	1
Total Drawing Sheets::	17
Small Entity?::	No
Petition included?::	No
Secrecy Order in Parent Appl.::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	United Kingdom
Status::	Full Capacity
Given Name::	Patrick
Middle Name::	
Family Name::	RACZ
City of Residence::	Saint Heller
State or Province of Residence::	
Country of Residence::	Jersey
Street of Mailing Address::	19 Royal Street
City of Mailing Address::	Saint Heller
State or Province of mailing address::	

Country of mailing address:: Jersey

Postal or Zip Code of mailing address:: JE1 4WA

Correspondence Information

Correspondence Customer Number:: 20350

Representative Information

Representative Customer Number:: 20350

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	11/336,758	01/19/06
11/336,758	Continuation of	10/111,716	09/17/02

Foreign Priority Information

Country::	Application number::	Filing Date::
PCT	GB00/04110	10/25/00
United Kingdom	9925227.2	11/25/99

Assignee Information

Assignee Name::

Street of mailing address::

City of mailing address::

State or Province of mailing address::

Country of mailing address::

Postal or Zip Code of mailing address::

Electronic Acknowledgement Receipt

EFS ID:	2720640
Application Number:	12014558
International Application Number:	
Confirmation Number:	1812
Title of Invention:	DATA STORAGE AND ACCESS SYSTEMS
First Named Inventor/Applicant Name:	Patrick RACZ
Customer Number:	20350
Filer:	Jason Donald Lohr/Sherri Hale
Filer Authorized By:	Jason Donald Lohr
Attorney Docket Number:	080379-000110US
Receipt Date:	15-JAN-2008
Filing Date:	
Time Stamp:	17:42:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1		080379_000110US_NO_FEE_CON_APP.pdf	3299253 458ea1069944afb42c70abf3668a885a146b52a0	yes	70

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal of New Application	1	1
	Specification	2	38
	Claims	39	50
	Abstract	51	51
	Drawings-only black and white line drawings	52	68
	Application Data Sheet	69	70

Warnings:	
Information:	
Total Files Size (in bytes):	3299253

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/07 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

Substitute for Form PTO-1360

(For use with Form PTO/SB/06)

Application Number	Filing Date
12/014,558	1/15/08

Applicant(s)

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT		*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend		Indep	Depend	Indep	Depend	Indep	Depend
1	1						51	1					
2		1					52		1				
3		2					53		2				
4		(1)					54		2				
5		(1)					55		(1)				
6		(1)					56		(1)				
7		(1)					57		(1)				
8		(1)					58		(1)				
9		(1)					59	1					
10	1						60		1				
11		1					61		1				
12		1					62		3				
13		1					63	1					
14		3					64		-1				
15		3					65		2				
16		(1)					66		2				
17		(1)					67	1					
18		(1)					68	1					
19		(1)					69	1					
20		(1)					70	1					
21		(1)					71	1					
22	1						72	1					
23		1					73		(1)				
24	1						74		(1)				
25		1					75						
26		2					76						
27		2					77						
28		2					78						
29		(1)					79						
30		(1)					80						
31	1						81						
32		1					82						
33		1					83						
34		1					84						
35	1						85						
36		1					86						
37		2					87						
38		2					88						
39		(1)					89						
40		(1)					90						
41		(1)					91						
42		(1)					92						
43		(1)					93						
44		(1)					94						
45		(1)					95						
46	1						96						
47		1					97						
48		1					98						
49		3					99						
50		(1)					100						
Total Indep	16						Total Indep						
Total Depend	76						Total Depend						
Total Claims	92						Total Claims						

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/014,558	01/15/2008	Patrick RACZ	080379-000110US

CONFIRMATION NO. 1812

20350
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

FORMALITIES LETTER

OC000000028098525

Date Mailed: 02/06/2008

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  *Applicant must submit $**75** to complete the basic filing fee for a small entity.*
- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of $**3350** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**65** for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this notice.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is $**3850** for a small entity
- $**75** Statutory basic filing fee.
- $**65** Surcharge.
- The application search fee has not been paid. Applicant must submit $**255** to complete the search fee.

- The application examination fee has not been paid. Applicant must submit $**105** to complete the examination fee for a small entity in compliance with 37 CFR 1.27.
- Total additional claim fee(s) for this application is $**3350**
  - $**1365** for **13** independent claims over 3.
  - $**1800** for **72** total claims over 20.
  - $**185** for multiple dependent claim surcharge.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/fly/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/014,558	01/15/2008	2876	0.00	080379-000110US	74	16

CONFIRMATION NO. 1812

20350
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

FILING RECEIPT

Date Mailed: 02/06/2008

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Patrick RACZ, Residence Not Provided;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 11/336,758 01/19/2006 PAT 7,334,720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB00/04110 10/25/2000

Foreign Applications

UNITED KINGDOM 9925227.2 11/25/1999

If Required, Foreign Filing License Granted: 02/04/2008

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/014,558**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

DATA STORAGE AND ACCESS SYSTEMS

Preliminary Class

235

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on September 5, 2008.

TOWNSEND and TOWNSEND and CREW LLP

By: Sheri Hall

PATENT
Attorney Docket No.: 080379-000110US
Client Reference No.: USP81421Z

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 1812
Patrick RACZ	Examiner:
Application No.: 12/014,558	Art Unit: 2876
Filed: January 15, 2008	TRANSMITTAL LETTER – RESPONSE TO NOTICE OF MISSING PARTS
For: DATA STORAGE AND ACCESS SYSTEMS	
Customer No.: 20350	

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to the Notice to File Missing Parts of Nonprovisional Application, dated February 6, 2008, enclosed are the following to be made of record in the above-identified application:

1) Executed Declaration
2) Petition to Extend Time
3) Preliminary Amendment

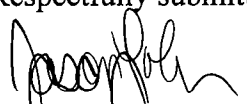
Please charge Deposit Account No. 20-1430 for the following fees:

Small Entity:	(a)	Utility Filing Fee	$155

(b)	Utility Search Fee		$255
(c)	Utility Examination Fee		$105
(d)	Application Size Fee		$0
(e)	Excess Claims Fees (§ 1.16(b), (c)):		
	71 - 20 = 51	x $25 =	$1,275
	16 - 3 = 13	x $105 =	$1,365
(f)	Multiple Dependent Claims		
(g)	Missing Parts Surcharge		$65
TOTAL FEES TO BE CHARGED			$3220

The Commissioner is hereby authorized to charge any additional fees associated with this paper or during the pendency of this application, or credit any overpayment, to Deposit Account No. 20-1430.

Respectfully submitted,



Jason D. Lohr
Reg. No. 48,163

Customer No. 20350

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 415 576-0300
JDL:slh

61494098 v1

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2008** *(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)*	Docket Number (Optional) 080379-000110US
Application Number 12/014,558	Filed January 15, 2008
For DATA STORAGE AND ACCESS SYSTEMS	
Art Unit 2876	Examiner

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$120	$60	$
☐ Two months (37 CFR 1.17(a)(2))	$460	$230	$
☐ Three months (37 CFR 1.17(a)(3))	$1050	$525	$
☐ Four months (37 CFR 1.17(a)(4))	$1640	$820	$
☒ Five months (37 CFR 1.17(a)(5))	$2230	$1115	$ 1115

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 20-1430. I have enclosed a duplicate copy of this sheet.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

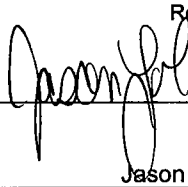
I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration Number 48,163

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____



Signature — September 5, 2008 (Date)

Jason D. Lohr, Reg. No. 48,163 (Typed or printed name) — 925 472 5000 (Telephone Number)

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☐ Total of _____ forms are submitted.

61494070 v1

PTO/SB/01 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☐ Declaration Submitted With Initial Filing OR ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16(e)) required)

Attorney Docket Number	080379-000000US
First Named Inventor	HULST, Hermen-ard
COMPLETE IF KNOWN	
Application Number	10/111,716
Filing Date	October 25, 2000
Art Unit	
Examiner Name	

As the below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original and first inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

DATA STORAGE AND ACCESS SYSTEMS

(Title of the Invention)

the specification of which

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 10/25/00 as United States Application Number or PCT International Application Number 10/111,716 and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
9925227.2	Great Britain	10/25/1999	☐	☐	☒ Not
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

PTO/SB/01 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☒ Customer Number or Bar Code Label	20350	OR ☐ Correspondence address below	
Name			
Address			
City		State	ZIP
Country	Telephone		Fax

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: ☐ A petition has been filed for this unsigned inventor

Hermen-ard Given Name (first and middle [if any])		HULST Family Name or Surname	
Inventor's Signature			Date June 12th 2002
Amsterdam Residence: City	State	Netherlands Country	Dutch Citizenship
Van Tuyll van Serooskerkenweg 75hs Mailing Address			
Amsterdam City	State	1076 JG ZIP	Netherlands Country

NAME OF SECOND INVENTOR: ☐ A petition has been filed for this unsigned inventor

Patrick Sandor Given Name (first and middle [if any])		RACZ Family Name or Surname	
Inventor's Signature			Date 12/5/02
St. Heller, Jersey Residence: City	State	Great Britain Country	GB Citizenship
19 Royal Square Mailing Address			
St. Heller, Jersey City	State	JE1 4WA ZIP	Great Britain Country

☐ Additional Inventors are being named on the ____ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on September 5, 2008.

TOWNSEND and TOWNSEND and CREW LLP

By: Sherri Hall

PATENT
Attorney Docket No.: 080379-000110US
Client Ref. No.: USP81421Z

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 1812
Patrick RACZ	Examiner: unassigned
Application No.: 12/014,558	Technology Center/Art Unit: 2876
Filed: January 15, 2008	PRELIMINARY AMENDMENT
For: DATA STORAGE AND ACCESS SYSTEMS	
Customer No.: 20350	

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Prior to examination of the above-referenced application, please enter the following amendments and remarks:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 16 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Original) A method of providing portable data comprising:

providing a portable data storage device comprising downloaded data storage means and payment validation means;

providing a terminal for internet access;

coupling the portable data storage device to the terminal;

reading payment information from the payment validation means using the terminal;

validating the payment information; and

downloading data into the portable storage device from a data supplier.

2. (Original) A method as claimed in claim 1 further comprising

writing updated payment information into the payment validation means.

3. (Currently Amended) A method as claimed in claim 1 ~~or 2~~ further comprising communicating a result of the payment information validating to the data supplier.

4. (Currently Amended) A method as claimed in ~~any one of claims~~ claim 1 ~~to~~ ~~3~~ further comprising controlling access by the terminal to data from the data supplier using a control data processing system coupled to the Internet.

5. (Original) A method as claimed in claim 4 wherein the control data processing system performs said validating of the payment information.

6. (Currently Amended) A method as claimed according to ~~any one of claims~~ claim 1 ~~to 5~~ wherein said coupling is performed by a mobile data retrieval device comprising:

a removable data storage means;

data access means, to access downloaded data on the data storage means;

storage interface means adapted to couple the data storage and data access means; and

data output means to output data derived from the downloaded data, to a user of the device.

7. (Currently Amended) A method as claimed in ~~claims~~ claim 1 ~~to 6~~ further comprising

writing into the data storage device data relating to past use made of the downloaded data including data identifying downloaded data items; and/or data identifying data suppliers used; and/or data characterizing a user spending pattern.

8. (Currently Amended) A method as claimed in ~~claims~~ claim 1 ~~to 7~~ wherein said portable data storage device comprises an electronic memory card or smart card.

9. (Currently Amended) A method as claimed in ~~any one of claims~~ claim 1 ~~to 8~~ wherein the downloaded data comprises compressed audio and/or video data.

10. (Original) A portable data carrier comprising:

an interface for reading and writing data from and to the carrier;

non-volatile data memory, coupled to the interface, for storing data on the carrier;

non-volatile payment data memory, coupled to the interface, for providing payment data to an external device.

11. (Original) A portable data carrier as claimed in claim 10, further comprising a program store storing code implementable by a processor; and

a processor, coupled to the content data memory, the payment data memory, the interface and to the program store for implementing code in the program store,

wherein the code comprises code to output payment data from the payment data memory to the interface and code to provide external access to the data memory.

12. (Original) A portable data carrier as claimed in claim 11, further comprising non-volatile use record memory, coupled to the processor, for storing a record of access made to the data memory and code to update the use record memory in response to external access made to the data memory.

13. (Original) A portable data carrier as claimed in claim 12, further comprising non-volatile use rule memory, coupled to the processor for storing data use rules, and wherein the code further comprises code for storing at least one data item in the data memory and at least one corresponding use rule in the use rule memory and code to provide external access to the data item in accordance with the use rule.

14. (Currently Amended) A portable data carrier as claimed in claim 11, ~~12 or 13,~~ further comprising a non-volatile access control memory coupled to the processor, for storing access control data and wherein said code to provide external access to the data memory includes code to receive access request data from the interface, code to determine access permission using the stored access control data and code to provide external access to the data memory in response to the result of the determination.

15. (Original) A portable data carrier as claimed in claim 14, further comprising non-volatile access record data memory, coupled to the processor, for storing a record of requests for external access to the data memory and wherein said code further comprises code to compare said access record data and said access request data and to erase stored content data in response to a result of said comparison.

16. (Currently Amended) A portable data carrier as claimed in ~~any one of claims~~ claim 11, ~~to 15,~~ configured for storing supplementary data in said data memory and further comprising code to output the supplementary data from the interface in addition to the stored data, in response to an external request to read the data memory.

17. (Currently Amended) A portable data carrier as claimed in ~~any one of claims~~ claim 11 ~~to 16~~ further comprising data synthesis code to receive a first portion of data

from the interface and to combine the first portion with a second portion of data stored in the data memory and to store the result in the data memory.

18. (Currently Amended) A portable data carrier as claimed in ~~any one of claims~~ claim 10, ~~to 17,~~ further comprising non-volatile communications parameter memory for storing data for accessing a communications network to receive data from the communications network for storage in the data memory.

19. (Currently Amended) A portable data carrier as claimed in ~~any one of claims~~ claim 10, ~~to 18,~~ wherein the data memory is partitioned for access on a block-by-block basis, each block comprising a plurality of data bytes read or written as a set.

20. (Currently Amended) A portable data carrier as claimed in ~~any one of claims~~ claim 10 ~~to 19~~ wherein said data memory has a capacity of greater than 1 MByte, more preferably > 100 MBytes, and most preferably > 1 GByte.

21. (Currently Amended) A portable data carrier as claimed in ~~any one of claims~~ claim 10 ~~to 20~~ substantially configured as an IC card or smart card.

22. (Original) A method of controlling access to data on a data carrier, the data carrier comprising non-volatile data memory and non-volatile parameter memory storing use status data and use rules, the method comprising:

receiving a data access request;

reading the use status data and use rules from memory; and

evaluating the use status data using the use rules to determine whether access to the stored data is permitted.

23. (Original) A method as claimed in claim 22 wherein said parameter memory further stores payment data and further comprising selecting a said use rule dependent upon said payment data.

24. (Original) A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and a pointer to a data provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester;

code to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code responsive to the request and to the received payment data, to read data for the requested data item from a content provider; and

code to transmit the read data to the requester over the communications interface.

25. (Original) A computer system as claimed in claim 24, wherein said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

26. (Currently Amended) A computer system as claimed in claim 24, ~~or 25,~~ wherein said data access data store further comprises data item access rule data for output to the requester with said data item.

27. (Original) A computer system as claimed in claim 26, further comprising code to select access rule data for output with a data item in response to said payment data.

28. (Original) A computer system as claimed in claim 27, wherein said data access data store further comprises requester reward data associated with a said data item, and said code further comprises code to update said reward data in response to said payment data.

29. (Currently Amended) A computer system as claimed in ~~any one of claims~~ claim 24, ~~to 28,~~ further comprising an access control data store coupled to said processor for storing access control data comprising a requester identifier, corresponding requester system access data and payment system data for identifying a payment system for use by the requester.

30. (Currently Amended) A computer system as claimed in ~~any one of claims~~ claim 24, ~~to 29,~~ further comprising content synthesis code to generate substantially complete item data from partial item data provided from two or more sources.

31. (Original) A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

reading the requested data from a content provider responsive to the received payment data; and

transmitting the read data to the requester.

32. (Original) A method of providing data to a data requester as claimed in claim 31 further comprising:

reading payment distribution information from a data store; and

outputting payment data to a payment system for distributing the payment for the requested data.

33. (Currently Amended) A method of providing data to a data requester as claimed in claim 31 ~~or 32~~ further comprising:

transmitting data access rule data to requester with the read data.

34. (Original) A method of providing data to a data requester as claimed in claim 33 further comprising:

selecting said access rule data dependent upon said payment data.

35. (Original) A data access terminal for retrieving data from a data supplier and providing the retrieved data to a data carrier, the terminal comprising:

a first interface for communicating with the data supplier;

a data carrier interface for interfacing with the data carrier;

a program store storing code implementable by a processor; and

a processor, coupled to the first interface, the data carrier interface and to the program store for implementing the stored code, the code comprising:

code to read payment data from the data carrier and to forward the payment data to a payment validation system;

code to receive payment validation data from the payment validation system;

code responsive to the payment validation data to retrieve data from the data supplier and to write the retrieved data into the data carrier.

36. (Original) A data access terminal as claimed in claim 35 further comprising code to transmit at least a portion of the payment validation data to the data supplier or to a destination received from the data supplier.

37. (Currently Amended) A data access terminal as claimed in claim 35 ~~or 36~~ further comprising code to retrieve from the data supplier and output to a user stored data identifier data and associated value data and use rule data for a data item available from the data supplier.

38. (Original) A data access terminal as claimed in claim 37 further comprising code to write use rule data for a data item into the data carrier with the associated data item.

39. (Currently Amended) A data access terminal as claimed in claim 37 ~~or 38~~ further comprising code to read a stored value from the data carrier, code to compare said stored value with said value data; and code to provide a modified output to a user of one or more of said stored data identifier data, said value data and said use rule data, in response to a result of the comparison.

40. (Currently Amended) A data access terminal according to ~~any one of claims~~ claim 35 ~~to 39~~ further comprising code for user input of access control data, code to output the access control data to the data carrier, code to receive access permission data from the card, and code to output data to the user in response to the received access permission data.

41. (Original) A data access terminal as claimed in claim 40 further comprising code to output a data erasure warming in response to the received access permission data.

42. (Currently Amended) A data access terminal according to ~~any one of claims~~ claim 35 ~~to 41~~ further comprising code to read reward data from the data carrier and to write modified reward data to the data carrier in response to said retrieval of data from the data supplier.

43. (Currently Amended) A data access terminal according to ~~any one of claims~~ claim 35 ~~to 42~~ further comprising:

code to read identity data from the data carrier;

code to transmit the identity data to the data supplier;

code to receive user characterizing data from the data supplier;

code to retrieve supplementary data in response to said characterizing data; and

code to output the supplementary data.

44. (Currently Amended) A data access terminal according to ~~any one of claims~~ claim 35 ~~to 43~~ further comprising a cash input device coupled to the processor, to provide

cash input value data; and code to update payment data in the data carrier, in accordance with the cash input value data.

45. (Currently Amended) A data access terminal according to ~~any one of claims~~ claim 35 ~~to 44~~ integrated with a mobile communication device, a personal computer, an audio/video player, and/or a cable or satellite television interface device.

46. (Original) A method of providing data from a data supplier to a data carrier, the method comprising:

reading payment data from the data carrier;

forwarding the payment data to a payment validation system;

retrieving data from the data supplier; and

writing the retrieved data into the date carrier.

47. (Original) A method of providing data from a data supplier according to claim 46 further comprising:

receiving payment validation data from the payment validation system; and

transmitting at least a portion of the payment validation data to the data supplier.

48. (Original) A method of providing data as claimed in claim 47, wherein the payment validation system comprises a payment processor at the data supplier.

49. (Currently Amended) A method of providing data as claimed in claim 46, ~~47 or 48,~~ further comprising:

retrieving from the data supplier a stored data item identifier and associated value data and use rule data; and

writing use rule data for the data item into the data carrier.

50. (Currently Amended) A method of providing data as claimed in claim 48, ~~or 49,~~ further comprising:

reading a stored value from the data carrier;

comparing the stored value with said value data; and

outputting to a user information indicating the result of said comparing.

51. (Original) A data access device for retrieving stored data from a data carrier, the device comprising:

a user interface;

a data carrier interface;

a program store storing code implementable by a processor; and

a processor coupled to the user interface, to the data carrier interface and to the program store for implementing the stored code, the code comprising:

code to retrieve use status data indicating a use status of data stored on the carrier, and use rules data indicating permissible use of data stored on the carrier;

code to evaluate the use status data using the use rules data to determine whether access is permitted to the stored data; and

code to access the stored data when access is permitted.

52. (Original) A data access device according to claim 51, further comprising code to write updated use status data to the carrier after user access to the stored data.

53. (Currently Amended) A data access device as claimed in claim 51, ~~or 52,~~ further comprising user access control code to input user access data, to transmit the user access data to the carrier, and to receive from the carrier user access permission data.

54. (Original) A data access device according to claim 53, further comprising code to select the use status and use rules data using the user access data.

55. (Currently Amended) A data access device as claimed in claim 53, ~~or 54,~~ further comprising code to retrieve and output supplementary data to the user.

56. (Currently Amended) A data access device according to ~~any one of claims~~ claim 51 ~~to 55~~ wherein said use rules permit partial use of a data item stored on the carrier and

further comprising code to write partial use status data to the data carrier when only part of a stored data item has been accessed.

57. (Currently Amended) A data access device according to ~~any one of claims~~ claim 51 ~~to 56~~ wherein the device is portable and the data carrier interface is configured for interfacing with a removable data carrier.

58. (Cancel)

59. (Original) A method of controlling access to data from a data carrier, comprising:

retrieving use status data from the data carrier indicating past use of the stored data;

retrieving use rules from the data carrier;

evaluating the use status data using the use rules to determine whether access to data stored on the carrier is permitted; and

permitting access to the data on the data carrier dependent on the result of said evaluating.

60. (Original) A method of controlling access according to claim 59, further comprising:

writing updated use status data to the carrier after an access attempt.

61. (Original) A method of controlling access according to claim 60, wherein said use rules permit partial access to a data item and wherein said writing writes a record of what part of the data item has been accessed when only part of the data item has been accessed.

62. (Currently Amended) A method of controlling access according to ~~any one of claims~~ claim 59, ~~to 61,~~ further comprising:

inputting a user access data;

selecting the use rules dependent upon the user access data.

63. (Original) A data access system comprising a data supply computer system for forwarding data from a data provider to a data access terminal; a electronic payment system for confirming an electronic payment; a data access terminal for communicating with the data supply system to write data from the data supply system onto a data carrier; and a data carrier for storing data from the data supply system and payment data; wherein data is forwarded from the data provider to the data carrier on validation of payment data provided from the data carrier to the electronic payment system.

64. (Original) A data access system according to claim 63 further comprising a payment distribution store and wherein the electronic payment system makes payments according to data in the payment distribution store associated with the forwarded data on confirmation of the payment and/or provision of the forwarded data to the card.

65. (Currently Amended) A data access system according to claim 63 ~~or 64~~ further comprising a data use rule data store and wherein data use rule data is provided to the data carrier with the forwarded data for controlling user access to the forwarded data.

66. (Original) A data access system according to claim 65 wherein the data use rule data is selected dependent upon the payment data.

67. (Original) A portable data carrier comprising:

an interface for sending and receiving data from and to the carrier;

non-volatile data memory, coupled to the interface, for storing data on the carrier; and

a digital rights management processor for controlling access to the stored data.

68. (Original) A portable data carrier comprising:

an interface for sending and receiving data from and to the carrier;

non-volatile data memory, coupled to the interface, for storing data on the carrier; and

an access control processor;

wherein the data memory is partitioned as data blocks and the access control processor controls external access to the data blocks.

69. (Original) A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and a resource locator a data provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code, responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and

further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

70. (Original) A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and location data identifying an electronic address for a provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises data item access rule data for output to the requester with a said data item; and

further comprising code to select access rule data for output with a data item in response to said payment data.

71. (Original) A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

transmitting the requested data to the requester;

reading payment distribution information from a data store; and

outputting payment data to a payment system for distributing the payment for the requested data.

72. (Original) A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

transmitting the requested data to the requester; and

transmitting data access rule data to requester with the read data.

Claims 73 - 74. (Canceled)

REMARKS/ARGUMENTS

Before this Preliminary Amendment, claims 1-74 were pending in the present application. This Amendment amends claims 3-4, 6-9, 14, 16-21, 26, 29-30, 33, 37, 39-40, 42-45, 49-50, 53, 55-57, 62, and 65; and cancels claims 58 and 73-74, leaving pending in the application claims 1-57 and 59-72. Consideration of the claims as amended is respectfully requested.

I. Amendment to the Claims

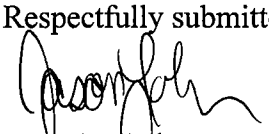
The claims are amended simply to remove multiple dependencies. The amendments thus are supported by the specification and do not add new matter.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 925-472-5000.

Respectfully submitted,



Jason D. Lohr
Reg. No. 48,163

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 415-576-0300
Attachments
JDL:slh
61493771 v1

Electronic Patent Application Fee Transmittal

Application Number:	12014558
Filing Date:	15-Jan-2008
Title of Invention:	DATA STORAGE AND ACCESS SYSTEMS
First Named Inventor/Applicant Name:	Patrick RACZ
Filer:	Jason Donald Lohr/Sherri Hale
Attorney Docket Number:	080379-000110US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	255	255
Utility Examination Fee	2311	1	105	105
Pages:				
Claims:				
Claims in excess of 20	2202	51	25	1275
Independent claims in excess of 3	2201	13	105	1365
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Late filing fee for oath or declaration	2051	1	65	65
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 5 months with $0 paid	2255	1	1115	1115
Miscellaneous:				
		Total in USD ($)		**4255**

Electronic Acknowledgement Receipt

EFS ID:	3898418
Application Number:	12014558
International Application Number:	
Confirmation Number:	1812
Title of Invention:	DATA STORAGE AND ACCESS SYSTEMS
First Named Inventor/Applicant Name:	Patrick RACZ
Customer Number:	20350
Filer:	Jason Donald Lohr/Sherri Hale
Filer Authorized By:	Jason Donald Lohr
Attorney Docket Number:	080379-000110US
Receipt Date:	05-SEP-2008
Filing Date:	15-JAN-2008
Time Stamp:	17:58:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$4255
RAM confirmation Number	3226
Deposit Account	201430
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		080379_000110US_RNTFMP_DEC_EOT_PAMD.pdf	792640 440093bf998799056d6c6795591d0ae4abe26b5e	yes	21

Multipart Description/PDF files in .zip description

Document Description	Start	End
Applicant Response to Pre-Exam Formalities Notice	1	2
Extension of Time	3	3
Oath or Declaration filed	4	5
Preliminary Amendment	6	21

Warnings:

Information:

2	Fee Worksheet (PTO-06)	fee-info.pdf	41719 a5546f1eed23a178aa589d82b24a8372474b901d	no	2

Warnings:

Information:

Total Files Size (in bytes):	834359

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/014,558	01/15/2008	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 09/05/2008

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 70	Minus	** 92	= 0	X $25 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 16	Minus	***16	= 0	X $105 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/STELLA LITTLE/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/014,558	01/15/2008	2876	3140	080379-000110US	71	16

CONFIRMATION NO. 1812

UPDATED FILING RECEIPT

20350
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

OC000000032052632

Date Mailed: 09/15/2008

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Hermen-ard Hulst, Amsterdam, NETHERLANDS;
Patrick RACZ, St. Heller, NJ;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 11/336,758 01/19/2006 PAT 7,334,720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB00/04110 10/25/2000

Foreign Applications

UNITED KINGDOM 9925227.2 11/25/1999

If Required, Foreign Filing License Granted: 02/04/2008

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/014,558**

Projected Publication Date: 12/25/2008

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

DATA STORAGE AND ACCESS SYSTEMS

Preliminary Class

235

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/014,558	01/15/2008	Hermen-ard Hulst	080379-000110US

CONFIRMATION NO. 1812

20350
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

PUBLICATION NOTICE

Title:DATA STORAGE AND ACCESS SYSTEMS

Publication No.US-2008-0314974-A1
Publication Date:12/25/2008

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	12/014,558
Filing Date	January 15, 2008
First Named Inventor	Hulst, Hermen-ard
Art Unit	2887
Examiner Name	Thien Minh Le
Attorney Docket Number	080379-000110US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	US 5,226,145	07-06-1993	Moronaga et al.	
	2.	US 5,367,150	11-22-1994	Kitta et al.	
	3.	US-5,406,619	04-11-1995	Akhteruzzaman et al.	
	4.	US 5,457,746	10-10-1995	Dolphin	
	5.	US 5,588,146	12-24-1996	Leroux	
	6.	US 5,677,953	10-14-1997	Dolphin	
	7.	US 5,703,951	12-30-1997	Dolphin	
	8.	US 5,754,654	05-19-1998	Hiroya et al.	
	9.	US 5,794,202	08-11-1998	Kim	
	10.	US 5,809,241	09-15-1998	Hanel et al.	
	11.	US 5,847,372	12-08-1998	Kreft	
	12.	US 5,889,860	03-30-1999	Eller et al.	
	13.	US 5,901,330	05-04-1999	Sun et al.	
	14.	US 5,918,213	06-29-1999	Bernard et al.	
	15.	US 5,923,884	07-13-1999	Peyret et al.	
	16.	US 6,012,634	01-11-2000	Brogan et al.	
	17.	US 6,078,917	06-20-2000	Paulsen et al.	
	18.	US 6,119,945	09-19-2000	Muller et al.	
	19.	US-6,202,056	03-13-2001	Nuttall	
	20.	US-6,385,731	05-07-2002	Ananda	
	21.	US 6,424,975	07-23-2002	Walter et al.	
	22.	US 6,442,570	08-27-2002	Wu	
	23.	US 6,473,829	10-29-2002	Dahman et al.	
	24.	US 6,510,236	01-21-2003	Crane et al.	
	25.	US-6,553,413	04-22-2003	Leighton et al.	
	26.	US-6,574,643	06-03-2003	Walter et al.	
	27.	US-6,999,936	02-14-2006	Sehr	
	28.	US-7,044,362	05-16-2006	Yu	
	29.	US-7,083,081	08-01-2006	McGee et al.	
	30.	US-7,334,720	02-26-2008	Hulst et al.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/014,558
				Filing Date	January 15, 2008
				First Named Inventor	Hulst, Hermen-ard
				Art Unit	2887
(Use as many sheets as necessary)				Examiner Name	Thien Minh Le
Sheet	2	of	2	Attorney Docket Number	080379-000110US

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document			Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		Country Code[3]	Number[4]	Kind Code[5] (*if known*)				
	31.	EP	0 195 098		10-03-1990	FPDC, Inc.		☐
	32.	EP	0 542 298		04-22-1998	Hitachi, Ltd.		☐
	33.	EP	0 713 198	A2	05-22-1996	Nederland PTT		☐
	34.	EP	0 823 694	A1	02-11-1998	Citibank NA		☐
	35.	EP	0 843 449	A2	05-07-1998	Sunhawk Corp. Inc.		☐
	36.	EP	0 914 001	A1	05-06-1999	Canal Plus SA		☐
	37.	WO	98/19237	A1	05-07-1998	Schulumberger Technologies, Inc.		☐
	38.	WO	98/33343		07-30-1998	Sonera OY et al.		☐
	39.	WO	98/37526		08-27-1998	Mondex Int. Ltd.		☐

NON PATENT LITERATURE DOCUMENTS

Examiner Initials *	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
			☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	5140484
Application Number:	12014558
International Application Number:	
Confirmation Number:	1812
Title of Invention:	DATA STORAGE AND ACCESS SYSTEMS
First Named Inventor/Applicant Name:	Hermen-ard Hulst
Customer Number:	20350
Filer:	Jason Donald Lohr/Linda Lim
Filer Authorized By:	Jason Donald Lohr
Attorney Docket Number:	080379-000110US
Receipt Date:	13-APR-2009
Filing Date:	15-JAN-2008
Time Stamp:	13:03:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Transmittal.pdf	56923 f2f9a21014616b2a87997d855826c9e5394d1099	no	1

Warnings:	
Information:	

2	Transmittal Letter	IDS_Cover_Letter.pdf	73682 2da610ca4df463062acfed384c876c84bd91ef1d	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Filed (SB/08)	IDS.pdf	117653 dfc78864936a54d2d247329a5eb113fd2cec3f9a	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
			Total Files Size (in bytes):	248258	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/21 (02-09)

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	12/014,558
Filing Date	January 15, 2008
First Named Inventor	Hulst, Hermen-ard
Art Unit	2887
Examiner Name	Thien Minh Le
Attorney Docket Number	080379-000110US

Total Number of Pages in This Submission: 5

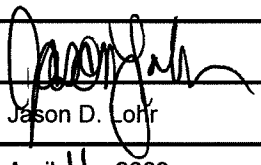
ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☒ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please identify below):

Information Disclosure Statement Form PTO/SB/08A&B (2 pages)

Remarks The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Townsend and Townsend and Crew LLP		
Signature			
Printed name	Jason D. Lohr		
Date	April 11, 2009	Reg. No.	48,163

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on the date shown below.

Signature	Linda Lim		
Typed or printed name	Linda Lim	Date	April 13, 2009

61895154 v1

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on April 13, 2009.

TOWNSEND and TOWNSEND and CREW LLP

By: Linda Lin

PATENT
Attorney Docket No.: 080379-000110US
Client Reference No.: USP81421Z

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Hermen-ard Hulst et al.

Application No.: 12/014,558

Filed: January 15, 2008

For: DATA STORAGE AND ACCESS SYSTEMS

Customer No.: 20350

Confirmation No.: 1812

Examiner: Thien Minh Le

Art Unit: 2887

INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR §1.97 and §1.98

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

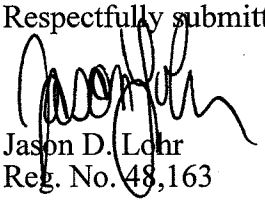
The references cited on attached form PTO/SB/08A and PTO/SB/08B are being called to the attention of the Examiner. A copy of reference number 28 is not enclosed. However, in accordance with 37 CFR §1.98(d), copies of the remaining references can be found in Application No. 11/336,758, filed January 19, 2006 (Attorney Docket No. 080379-000100US). It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

Some of the references cited in this IDS were cited in an Office Action mailed on November 6, 2006, in related U.S. Patent Application No. 11/336,758. Copies of the Office Actions in U.S. Patent Application No. 11/336,758 are available on PAIR and are believed to be readily accessible to the Examiner.

As provided for by 37 CFR §1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement. However, if a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,



Jason D. Lohr
Reg. No. 48,163

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 415-576-0300
JDL:lml
61895050 v1

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/014,558
				Filing Date	January 15, 2008
				First Named Inventor	RACZ, Patrick
(Use as many sheets as necessary)				Art Unit	2876
				Examiner Name	Le, Thien Minh
Sheet	1	of	1	Attorney Docket Number	080379-000110US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-6,658,568 B1	12-02-2003	Ginter et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of U.S. Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	5681124
Application Number:	12014558
International Application Number:	
Confirmation Number:	1812
Title of Invention:	DATA STORAGE AND ACCESS SYSTEMS
First Named Inventor/Applicant Name:	Hermen-ard Hulst
Customer Number:	20350
Filer:	Jason Donald Lohr/Jessie Kelly
Filer Authorized By:	Jason Donald Lohr
Attorney Docket Number:	080379-000110US
Receipt Date:	10-JUL-2009
Filing Date:	15-JAN-2008
Time Stamp:	15:42:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SIDS_080379_000110_071009.pdf	108021 e69ed5f47f52c17a3a45f7dcdd909aad753cfabd	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Filed (SB/08)	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	108021	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on July 10, 2009.

TOWNSEND and TOWNSEND and CREW LLP

By: Jessie M. Kelly

PATENT
Attorney Docket No.: 080379-000110US
Client Reference No.: PN759544USB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Patrick RACZ

Application No.: 12/014,558

Filed: January 15, 2008

For: DATA STORAGE AND ACCESS SYSTEMS

Customer No.: 20350

Confirmation No.: 1812

Examiner: Le, Thien Minh

Art Unit: 2876

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR §1.97 and §1.98

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

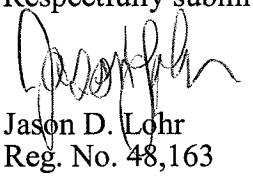
The reference cited on attached form PTO/SB/08A is being called to the attention of the Examiner. A copy of the reference is not enclosed. It is respectfully requested that the cited reference be expressly considered during the prosecution of this application, and the reference be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR §1.97(g) and (h), no inference should be made that the information and reference cited are prior art merely because they are in this statement and no

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement. However, if a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,



Jason D. Lohr
Reg. No. 48,163

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 925-472-8895
JDL:jmk
62119616 v1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/014,558	01/15/2008	Hermen-ard Hulst	080379-000110US	1812

20350 7590 01/21/2010

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
LE, THIEN MINH	

ART UNIT	PAPER NUMBER
2887	

MAIL DATE	DELIVERY MODE
01/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	12/014,558	HULST ET AL.	
	Examiner	Art Unit	
	THIEN M. LE	2887	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *1* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/5/2008*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57 and 59-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *1-57 and 59-72* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 January 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/10/2009; 4/13/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The preliminary amendment filed on 9/5/2008 has been entered. Claims 58 and 73-74 have been canceled. Claims 1-57 and 59-72 remain for examination.

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-9, drawn to a method of providing portable data, classified in class 235, subclass 487.

II. Claims 10-21, 51-57, 67, and 68 drawn to a portable data carrier, classified in class 23, subclass 379.

III. Claims 22, 23, 35-50, and 59-62 drawn to a method and an apparatus of controlling access to data, classified in class 235, subclass 382.

IV. Claims 24-34, 63-66, and 69-72 drawn to a system controlled by data beating records, classified in class 235, subclass 375.

2. The inventions are distinct, each from the other because of the following reasons: Inventions Group I - Group IV are related as product and process of use. The inventions can be shown to be distinct if either or both of the following can be shown: (1) the process for using the product as claimed can be practiced with another materially different product or (2) the product as claimed can be used in a materially different process of using that product (MPEP § 806.05(h)). In the instant case the process for using the product claimed can be practiced with materially different product. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Groups II, III, or IV restriction for examination purposes as indicated is proper.

3. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim

remaining in the application. Any amendment of inventorship must be accompanied by a petition under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to THIEN M. LE whose telephone number is (571)272-2396. The examiner can normally be reached on Monday - Friday from 7:30am - 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve S. Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thien M. Le/
Primary Examiner, Art Unit 2887

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12014558	HULST ET AL.
	Examiner	Art Unit
	THIEN M LE	2887

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/19/2010								
	1	÷								
	2	÷								
	3	÷								
	4	÷								
	5	÷								
	6	÷								
	7	÷								
	8	÷								
	9	÷								
	10	÷								
	11	÷								
	12	÷								
	13	÷								
	14	÷								
	15	÷								
	16	÷								
	17	÷								
	18	÷								
	19	÷								
	20	÷								
	21	÷								
	22	÷								
	23	÷								
	24	÷								
	25	÷								
	26	÷								
	27	÷								
	28	÷								
	29	÷								
	30	÷								
	31	÷								
	32	÷								
	33	÷								
	34	÷								
	35	÷								
	36	÷								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12014558	HULST ET AL.
	Examiner	Art Unit
	THIEN M LE	2887

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/19/2010								
	37	÷								
	38	÷								
	39	÷								
	40	÷								
	41	÷								
	42	÷								
	43	÷								
	44	÷								
	45	÷								
	46	÷								
	47	÷								
	48	÷								
	49	÷								
	50	÷								
	51	÷								
	52	÷								
	53	÷								
	54	÷								
	55	÷								
	56	÷								
	57	÷								
	58	-								
	59	÷								
	60	÷								
	61	÷								
	62	÷								
	63	÷								
	64	÷								
	65	÷								
	66	÷								
	67	÷								
	68	÷								
	69	÷								
	70	÷								
	71	÷								
	72	÷								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12014558	HULST ET AL.
	Examiner	Art Unit
	THIEN M LE	2887

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	01/19/2010								
	73	-								
	74	-								

PTO/SB/08a (06-09)

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	12/014,558
				Filing Date	January 15, 2008
				First Named Inventor	RACZ, Patrick
				Art Unit	2887
(Use as many sheets as necessary)				Examiner Name	Le, Thien Minh
Sheet	1	of	1	Attorney Docket Number	080379-000110US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-6,658,568 B1	12-02-2003	Ginter et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature	/Thien Le/	Date Considered	01/19/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of U.S. Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

62119616 v1 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.L./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1812

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/014,558	01/15/2008 RULE	235	2887	080379-000110US

APPLICANTS

Hermen-ard Hulst, Amsterdam, NETHERLANDS;
Patrick RACZ, St. Heller, NJ;

**** CONTINUING DATA ***************************

This application is a CON of 11/336,758 01/19/2006 PAT 7,334,720
which is a CON of 10/111,716 09/17/2002 ABN
which is a 371 of PCT/GB00/04110 10/25/2000

**** FOREIGN APPLICATIONS ***************************

UNITED KINGDOM 9925227.2 11/25/1999

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
02/04/2008

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/ Thien M. Le/ Examiner's Signature	☐ Initials	NETHERLANDS	17	71	16

ADDRESS

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834
UNITED STATES

TITLE

DATA STORAGE AND ACCESS SYSTEMS

FILING FEE RECEIVED		
3140	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

PTO/SB/08A&B (02-09)

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	12/014,558
Filing Date	January 15, 2008
First Named Inventor	Hulst, Hermen-ard
Art Unit	2887
Examiner Name	Thien Minh Le
Attorney Docket Number	080379-000110US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	US 5,226,145	07-06-1993	Moronaga et al.	
	2.	US 5,367,150	11-22-1994	Kitta et al.	
	3.	US-5,406,619	04-11-1995	Akhteruzzaman et al.	
	4.	US 5,457,746	10-10-1995	Dolphin	
	5.	US 5,586,146	12-24-1996	Leroux	
	6.	US 5,677,953	10-14-1997	Dolphin	
	7.	US 5,703,951	12-30-1997	Dolphin	
	8.	US 5,754,654	05-19-1998	Hiroya et al.	
	9.	US 5,794,202	08-11-1998	Kim	
	10.	US 5,809,241	09-15-1998	Hanel et al.	
	11.	US 5,847,372	12-08-1998	Kreft	
	12.	US 5,889,860	03-30-1999	Eller et al.	
	13.	US 5,901,330	05-04-1999	Sun et al.	
	14.	US 5,918,213	06-29-1999	Bernard et al.	
	15.	US 5,923,884	07-13-1999	Peyret et al.	
	16.	US 6,012,634	01-11-2000	Brogan et al.	
	17.	US 6,078,917	06-20-2000	Paulsen et al.	
	18.	US 6,119,945	09-19-2000	Muller et al.	
	19.	US-6,202,056	03-13-2001	Nuttall	
	20.	US-6,385,731	05-07-2002	Ananda	
	21.	US 6,424,975	07-23-2002	Walter et al.	
	22.	US 6,442,570	08-27-2002	Wu	
	23.	US 6,473,829	10-29-2002	Dahman et al.	
	24.	US 6,510,236	01-21-2003	Crane et al.	
	25.	US-6,553,413	04-22-2003	Leighton et al.	
	26.	US-6,574,643	06-03-2003	Walter et al.	
	27.	US-6,999,936	02-14-2006	Sehr	
	28.	US-7,044,362	05-16-2006	Yu	
	29.	US-7,083,081	08-01-2006	McGee et al.	
	30.	US-7,334,720	02-26-2008	Hulst et al.	

Examiner Signature	/Thien Le/	Date Considered	01/19/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

61895050 v1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.L./

PTO/SB/08A&B (02-09)

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	12/014,558
Filing Date	January 15, 2008
First Named Inventor	Hulst, Hermen-ard
Art Unit	2887
Examiner Name	Thien Minh Le
Attorney Docket Number	080379-000110US

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document			Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		Country Code[3]	Number[4]	Kind Code[5] (*if known*)				
	31.	EP	0 195 098		10-03-1990	FPDC, Inc.		☐
	32.	EP	0 542 298		04-22-1998	Hitachi, Ltd.		☐
	33.	EP	0 713 198	A2	05-22-1996	Nederland PTT		☐
	34.	EP	0 823 694	A1	02-11-1998	Citibank NA		☐
	35.	EP	0 843 449	A2	05-07-1998	Sunhawk Corp. Inc.		☐
	36.	EP	0 914 001	A1	05-06-1999	Canal Plus SA		☐
	37.	WO	98/19237	A1	05-07-1998	Schulumberger Technologies, Inc.		☐
	38.	WO	98/33343		07-30-1998	Sonera OY et al.		☐
	39.	WO	98/37526		08-27-1998	Mondex Int. Ltd.		☐

NON PATENT LITERATURE DOCUMENTS

Examiner Initials *	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
			☐

Examiner Signature	/Thien Le/	Date Considered	01/19/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

61895050 v1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.L./

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on 06/18/10.

TOWNSEND and TOWNSEND and CREW LLP

By: /Anna Marie Arante/

PATENT
Attorney Docket No.: 080379-000110US
Client Ref. No.: PN759544USB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 1812
Hermen-ard Hulst	Examiner: Le, Thien Minh
Application No.: 12/014,558	Technology Center/Art Unit: 2876
Filed: January 15, 2008	AMENDMENT
For: DATA STORAGE AND ACCESS SYSTEMS	
Customer No.: 20350	

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

In response to the Office Action mailed January 21, 2010, please enter the following amendments and remarks. The Applicants file herewith a petition for an extension of time to the present date, with payment of the appropriate fees.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

Claims 1 – 23. (Cancelled)

24. (Original) A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and a pointer to a data provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester;

code to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code responsive to the request and to the received payment data, to read data for the requested data item from a content provider; and

code to transmit the read data to the requester over the communications interface.

25. (Original) A computer system as claimed in claim 24, wherein said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

26. (Previously Presented) A computer system as claimed in claim 24, wherein said data access data store further comprises data item access rule data for output to the requester with said data item.

27. (Original) A computer system as claimed in claim 26, further comprising code to select access rule data for output with a data item in response to said payment data.

28. (Original) A computer system as claimed in claim 27, wherein said data access data store further comprises requester reward data associated with a said data item, and said code further comprises code to update said reward data in response to said payment data.

29. (Previously Presented) A computer system as claimed in claim 24, further comprising an access control data store coupled to said processor for storing access control data comprising a requester identifier, corresponding requester system access data and payment system data for identifying a payment system for use by the requester.

30. (Previously Presented) A computer system as claimed in claim 24, further comprising content synthesis code to generate substantially complete item data from partial item data provided from two or more sources.

31. (Original) A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

reading the requested data from a content provider responsive to the received payment data; and

transmitting the read data to the requester.

32. (Original) A method of providing data to a data requester as claimed in claim 31 further comprising:

reading payment distribution information from a data store; and

outputting payment data to a payment system for distributing the payment for the requested data.

33. (Previously Presented) A method of providing data to a data requester as claimed in claim 31 further comprising:

transmitting data access rule data to requester with the read data.

34. (Original) A method of providing data to a data requester as claimed in claim 33 further comprising:

selecting said access rule data dependent upon said payment data.

Claims 35 – 62. (Cancelled)

63. (Original) A data access system comprising a data supply computer system for forwarding data from a data provider to a data access terminal; a electronic payment system for confirming an electronic payment; a data access terminal for communicating with the data supply system to write data from the data supply system onto a data carrier; and a data carrier for storing data from the data supply system and payment data; wherein data is forwarded from the data provider to the data carrier on validation of payment data provided from the data carrier to the electronic payment system.

64. (Original) A data access system according to claim 63 further comprising a payment distribution store and wherein the electronic payment system makes payments according to data in the payment distribution store associated with the forwarded data on confirmation of the payment and/or provision of the forwarded data to the card.

65. (Previously Presented) A data access system according to claim 63 further comprising a data use rule data store and wherein data use rule data is provided to the data carrier with the forwarded data for controlling user access to the forwarded data.

66. (Original) A data access system according to claim 65 wherein the data use rule data is selected dependent upon the payment data.

Claims 67 – 68. (Cancelled)

69. (Original) A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and a resource locator a data provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code, responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises payment distribution information indicating to whom payments should be made for a data item; and

further comprising code to output payment data for a data item for making payments for the item when the item is supplied to a said requester.

70. (Original) A computer system for providing data to a data requester, the system comprising:

a communication interface;

a data access data store for storing records of data items available from the system, each record comprising a data item description and location data identifying an electronic address for a provider for the data item;

a program store storing code implementable by a processor;

a processor coupled to the communications interface, to the data access data store, and to the program store for implementing the stored code, the code comprising:

code to receive a request for a data item from the requester to receive from the communications interface payment data comprising data relating to payment for the requested data item;

code responsive to the request and to the received payment data to output the item data to the requester over the communication interface; wherein

said data access data store further comprises data item access rule data for output to the requester with a said data item; and

further comprising code to select access rule data for output with a data item in response to said payment data.

71. (Original) A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

transmitting the requested data to the requester;

reading payment distribution information from a data store; and

outputting payment data to a payment system for distributing the payment for the requested data.

72. (Original) A method of providing data to a data requester comprising:

receiving a request for a data item from the requester;

receiving payment data from the requester relating to payment for the requested data;

transmitting the requested data to the requester; and

transmitting data access rule data to requester with the read data.

Claims 73-74. (Cancelled)

REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed January 21, 2010. claims 1-57 and 59-72 were pending in the present application. This Amendment cancels claims 1-23, 35-57, 59-62 and 67-68, without adding or amending any claims, leaving pending in the application claims 24-34, 63-66, and 69-72. Consideration of the elected claims is respectfully requested.

I. Restriction of the Claims.

The claims are subjected to restriction under 35 U.S.C. §121 as allegedly being drawn to groups classified as:

Group I: Claims 1-9, as being drawn to a method of providing portable data;

Group II: Claims 10-21, 51-57, 67 and 68, as being drawn to a portable data carrier;

Group III: Claims 22, 23, 35-50, and 59-62, as being drawn to a method and an apparatus of controlling access to data; and

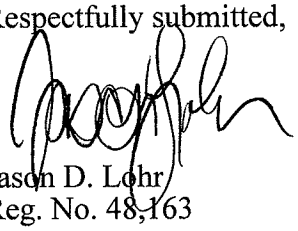
Group IV: Claims 24-34, 63-66, and 69-72, as being drawn to a system controlled by data beating records.

Although Applicants do not necessarily agree with these groupings and/or the need for restriction, Applicants hereby elect to prosecute the claims of Group IV without traverse. Applicants reserve the right to present the non-elected claims in one or more subsequent continuing applications. Applicants hereby cancel the claims of Groups I-III, and request consideration and examination of the claims of Group IV (claims 24-34, 63-66 and 69-72).

CONCLUSION

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 925-472-5000.

Respectfully submitted,



Jason D. Lohr
Reg. No. 48,163

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 415-576-0300
Attachments
JDL:atm

Electronic Patent Application Fee Transmittal

Application Number:	12014558
Filing Date:	15-Jan-2008
Title of Invention:	DATA STORAGE AND ACCESS SYSTEMS
First Named Inventor/Applicant Name:	Hermen-ard Hulst
Filer:	Jason Donald Lohr/Anna Marie Arante
Attorney Docket Number:	080379-000110US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 4 months with $0 paid	2254	1	865	865

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**865**

Electronic Acknowledgement Receipt

EFS ID:	7850362
Application Number:	12014558
International Application Number:	
Confirmation Number:	1812
Title of Invention:	DATA STORAGE AND ACCESS SYSTEMS
First Named Inventor/Applicant Name:	Hermen-ard Hulst
Customer Number:	20350
Filer:	Jason Donald Lohr/Anna Marie Arante
Filer Authorized By:	Jason Donald Lohr
Attorney Docket Number:	080379-000110US
Receipt Date:	18-JUN-2010
Filing Date:	15-JAN-2008
Time Stamp:	19:59:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$865
RAM confirmation Number	5800
Deposit Account	201430
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2010_06_18_AMENDMENT_EXT_080379_000110US.pdf	383644 0e9aa0b8635feca357362d562166630d1abcb2a4	yes	9

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Extension of Time	1	1
Response to Election / Restriction Filed	2	2
Claims	3	7
Applicant Arguments/Remarks Made in an Amendment	8	9

Warnings:

Information:

2	Fee Worksheet (PTO-875)	fee-info.pdf	30318 93da90a6233e6dfd55556ca7d6041695429e6275	no	2

Warnings:

Information:

Total Files Size (in bytes):	413962

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2009** *(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)*	Docket Number (Optional) 080379-000110US
Application Number 12/014,558	Filed January 15, 2008
For DATA STORAGE AND ACCESS SYSTEMS	
Art Unit 2876	Examiner Le, Thien Minh

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$130	$65	$
☐ Two months (37 CFR 1.17(a)(2))	$490	$245	$
☐ Three months (37 CFR 1.17(a)(3))	$1110	$555	$
☒ Four months (37 CFR 1.17(a)(4))	$1730	$865	$ 865
☐ Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

☒ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 20-1430.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

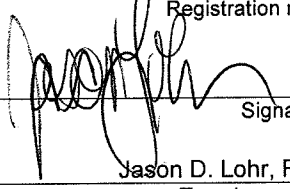
I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration Number 48,163

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____



Signature — 06/18/10 (Date)

Jason D. Lohr, Reg. No. 48,163 (Typed or printed name) — (925) 472-5000 (Telephone Number)

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☒ Total of 1 form is submitted.

62725141 v1

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/014,558	01/15/2008	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 06/18/2010

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 19	Minus	** 92	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 7	Minus	***16	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/ANGELA WHITE/

Substitute for form 1449/PTO				*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application Number**	12/014,558
				Filing Date	January 15, 2008
				First Named Inventor	HULST, Hermen-ard
				Art Unit	2876
(Use as many sheets as necessary)				Examiner Name	Le, Thien Minh
Sheet	1	of	1	Attorney Docket Number	080379-000110US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-5,845,281 A	12-01-1998	Benson et al.	
	2	US-5,933,498 A	08-03-1999	Schneck et al.	
	3	US-6,018,720 A	01-25-2000	Fujimoto	Corresponds to JP 11-53184

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]	Number[4]	Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	4	JP	10-269291	A	10-09-1998	Sony Corp.		☒
	5	JP	11-53184	A	02-26-1999	Seta:KK	Corresponds to US 6,018,720	☒
	6	JP	11-212785	A	08-06-1999	Casio Comput. Co. Ltd.		☒
	7	JP	11-213010	A	08-06-1999	Planet Computer:KK		☒
	8	JP	11-272762	A	10-08-1999	Hitachi Ltd.		☒

NON PATENT LITERATURE DOCUMENTS

Examiner Initials *	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[6]
			☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of U.S. Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

62773286 v1

(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10－269291

(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
	9/06	５５０		9/06	５５０Ｚ
	15/00	３３０		15/00	３３０Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｆ
Ｈ０４Ｌ	9/08		Ｃ０６Ｆ	15/21	Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全 36 頁）　最終頁に続く

(21)出願番号　特願平9－74185

(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

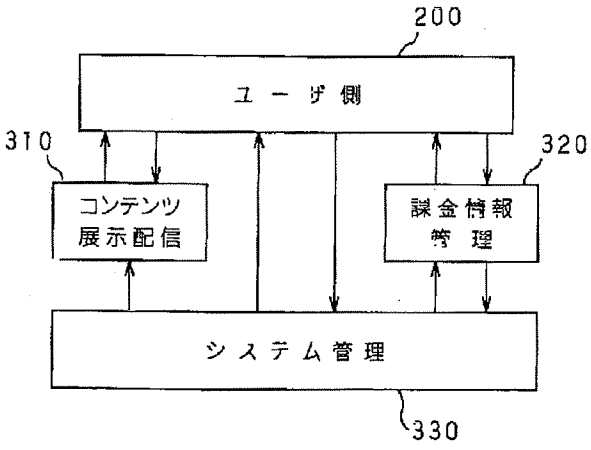
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　ディジタルコンテンツ配付管理システム

(57)【要約】

【課題】　通信のレスポンスを向上させることが可能な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にする。

【解決手段】　一定の地域のユーザ側２００に対する課金情報を管理する課金情報管理機関３２０と、ディジタルコンテンツを展示，配信するコンテンツ展示配信機関３１０と、ディジタルコンテンツの加工と、コンテンツ展示配信機関３１０に対する上記加工したディジタルコンテンツの配信と、課金情報管理機関３２０からの情報収集及び収益配分と、全体のセキュリティ管理配分とを行うシステム管理機関３３０とからなり、課金情報管理機関３２０とコンテンツ展示配信機関３１０とシステム管理機関３３０とは、それぞれ独立にユーザ側２００との間でデータ通信を行う。



【特許請求の範囲】
【請求項１】　一定の地域の利用者端末装置に対する課金情報を管理する課金情報管理手段と、
ディジタルコンテンツを展示，配信するコンテンツ展示配信手段と、
少なくとも、上記ディジタルコンテンツの加工と、上記コンテンツ展示配信手段に対する上記加工したディジタルコンテンツの配信と、上記課金情報管理手段からの情報収集及び収益配分と、全体のセキュリティ管理配分とを行うシステム管理手段とからなり、
上記課金情報管理手段とコンテンツ展示配信手段とシステム管理手段とは、それぞれ独立に上記利用者端末装置との間でデータ通信を行うことを特徴とするディジタルコンテンツ配付管理システム。
【請求項２】　上記システム管理手段は、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手段と、上記加工したディジタルコンテンツを上記コンテンツ展示配信手段に配信するコンテンツ配信手段と、上記加工されたディジタルコンテンツの復号化に使用するコンテンツ鍵を暗号化し上記利用者端末装置に送信するコンテン鍵送信手段と、利用者端末装置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暗号化して上記課金情報管理手段に送信する課金情報暗号化手段とを少なくとも有してなり、上記課金情報管理手段は、上記利用者端末装置からの要求に応じて上記暗号化された課金情報を当該利用者端末装置に送信する課金情報送信手段と、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手段とを少なくとも有してなり、
上記コンテンツ展示配信手段は、上記利用者端末装置からのディジタルコンテンツ送信要求に応じて、上記加工したディジタルコンテンツを送信するコンテンツ送信手段を少なくとも有してな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システム。
【請求項３】　上記課金情報管理手段とコンテンツ展示配信手段とシステム管理手段とが、それぞれ独立に上記利用者端末装置との間でデータ通信を行う際に使用する暗号化方式若しくは暗号鍵は、それぞれ独自であることを特徴とする請求項２記載のディジタルコンテンツタ配信管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばディジタルコンテンツを利用者端末装置に配付すると共にそれらの管理を行うディジタルコンテンツ配付管理システムに関する。
【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】ところで、上述の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、システム側に通信が集中し、ユーザに対して満足のいくレスポンスが得られないおそれがある。
【０００４】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、通信のレスポンスを向上させることが可能なディジタルデータ配信管理システムを提供することを目的とする。
【０００５】
【課題を解決するための手段】本発明によれば、一定の地域の利用者端末装置に対する課金情報を管理する機能

と、ディジタルコンテンツを展示，配信する機能と、ディジタルコンテンツの加工、上記ディジタルコンテンツ展示配信機能に対する上記加工したディジタルコンテンツの配信、課金情報管理機能からの情報収集及び収益配分、全体のセキュリティ管理配分を行う機能とからなり、利用者端末装置と各機能との間のデータ通信はそれぞれ独立に行うことにより、上述した課題を解決する。

【０００６】

【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。

【０００７】先ず、本発明のディジタルコンテンツ配付管理システム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。

【０００８】図１にはシステム全体の概略的な構成を示す。

【０００９】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。

【００１０】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。

【００１１】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。

【００１２】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。

【００１３】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。

【００１４】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。

【００１５】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。

【００１６】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。

【００１７】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。

【００１８】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。

【００１９】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。

【００２０】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。

【００２１】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。

【００２２】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。

【００２３】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。

【００２４】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。

【００２５】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。

【００２６】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。

【００２７】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。

【００２８】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。

【００２９】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。

【００３０】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。

【００３１】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。

【００３２】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。

【００３３】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。

【００３４】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。

【００３５】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。

【００３６】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。

【００３７】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。

【００３８】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。

【００３９】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。

【００４０】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。

【００４１】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。

【００４２】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。

【００４３】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。

【００４４】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。

【００４５】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。

【００４６】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。

【００４７】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。

【００４８】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。

【００４９】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。

【００５０】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。

【００５１】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。

【００５２】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。

【００５３】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。

【００５４】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。

【００５５】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。

【００５６】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。

【００５７】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。

【００５８】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。

【００５９】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。

【００６０】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。

【００６１】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。

【００６２】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。

【００６３】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。

【００６４】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。

【００６５】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。

【００６６】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。

【００６７】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。

【００６８】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。

【００６９】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。

【００７０】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。

【００７１】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。

【００７２】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。

【００７３】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。

【００７４】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。

【００７５】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。

【００７６】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。
【００７７】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。
【００７８】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。
【００７９】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。
【００８０】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。
【００８１】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。
【００８２】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。
【００８３】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。
【００８４】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。
【００８５】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。
【００８６】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。
【００８７】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。
【００８８】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。
【００８９】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。
【００９０】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。
【００９１】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。
【００９２】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。
【００９３】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。

【００９４】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。

【００９５】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。

【００９６】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。

【００９７】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１００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。

【００９８】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。

【００９９】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。

【０１００】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。

【０１０１】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。

【０１０２】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。

【０１０３】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。

【０１０４】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。

【０１０５】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。

【０１０６】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。

【０１０７】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。

【０１０８】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。

【０１０９】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。

【０１１０】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。

【０１１１】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。

【０１１２】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。

【０１１３】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。

【０１１４】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。

【０１１５】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。

【０１１６】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。

【０１１７】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。

【０１１８】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。

【０１１９】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。

【０１２０】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。

【０１２１】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。

【０１２２】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。

【０１２３】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。

【０１２４】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。

【０１２５】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。

【０１２６】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。

【０１２７】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。

【０１２８】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。

【０１２９】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。

【０１３０】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。

【０１３１】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。

【０１３２】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。

【０１３３】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。

【０１３４】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。

【０１３５】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。

【０１３６】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。

【０１３７】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。

【０１３８】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。

【０１３９】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。

【０１４０】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。

【０１４１】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。

【０１４２】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。

【０１４３】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。

【０１４４】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。

【０１４５】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。

【０１４６】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。

【０１４７】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。

【０１４８】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。

【０１４９】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。

【０１５０】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。

【０１５１】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。

【０１５２】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。

【０１５３】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。

【０１５４】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。

【０１５５】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。

【０１５６】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。

【０１５７】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。

【０１５８】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。

【０１５９】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。

【０１６０】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。

【０１６１】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。

【０１６２】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。

【０１６３】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。

【０１６４】次に、ユーザ端末５０は、ステップＳＴ１

３３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。

【０１６５】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。

【０１６６】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。

【０１６７】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。

【０１６８】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。

【０１６９】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。

【０１７０】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。

【０１７１】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。

【０１７２】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。

【０１７３】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。

【０１７４】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。

【０１７５】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。

【０１７６】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。

【０１７７】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。

【０１７８】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。

【０１７９】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。

【０１８０】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。

【0181】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。

【0182】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。

【0183】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。

【0184】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。

【0185】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。

【0186】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lcm（X，Y）の単位に分割する。

【0187】次に、上記最小公倍数lcm（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lcm（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。

【0188】当該復号化処理により得られた最小公倍数lcm（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。

【0189】その後、この最小公倍数lcm（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lcm（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。

【0190】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。

【0191】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lcm（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。

【0192】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。

【0193】上述のフローチャートでは、最小公倍数l

ｃｍ（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。

【０１９４】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。

【０１９５】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。

【０１９６】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。

【０１９７】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１ｃｍは１．２８Ｋとなる。

【０１９８】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。

【０１９９】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。

【０２００】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。

【０２０１】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。

【０２０２】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。

【０２０３】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。

【０２０４】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。

【０２０５】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。

【０２０６】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。

【０２０７】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。

【０２０８】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。

【０２０９】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。

【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、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。

【０２１１】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。

【０２１２】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。

【０２１３】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。

【０２１４】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。

【０２１５】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。

【０２１６】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。

【０２１７】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。

【０２１８】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。

【０２１９】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。

【０２２０】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。

【０２２１】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。

【０２２２】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。

【０２２３】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。

【０２２４】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）。

【０２２５】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。

【０２２６】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。

【０２２７】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。

【０２２８】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。

【０２２９】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。

【０２３０】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。

【０２３１】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。

【０２３２】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。

【０２３３】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。

【０２３４】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。

【０２３５】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。

【０２３６】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。

【０２３７】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。

【０２３８】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。

【０２３９】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。

【０２４０】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。

【０２４１】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。

【０２４２】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。

【０２４３】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。

【０２４４】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。

【０２４５】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。

【０２４６】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。

【０２４７】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。

【０２４８】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。

【０２４９】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。

【０２５０】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。

【０２５１】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。

【０２５２】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。

【０２５３】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。

【０２５４】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。

【0255】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。

【0256】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。

【0257】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。

【0258】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。

【0259】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。

【0260】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。

【0261】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。

【0262】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。

【0263】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。

【0264】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。

【0265】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。

【0266】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。

【0267】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。

【0268】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。

【0269】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。

【0270】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。

【0271】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。

【0272】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。

【０２７３】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。

【０２７４】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。

【０２７５】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。

【０２７６】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。

【０２７７】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。

【０２７８】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。

【０２７９】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。

【０２８０】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。

【０２８１】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。

【０２８２】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。

【０２８３】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。

【０２８４】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。

【０２８５】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。

【０２８６】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。

【０２８７】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。

【0288】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。

【0289】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。

【0290】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。

【0291】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。

【0292】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。

【0293】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。

【0294】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。

【0295】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。

【0296】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。

【0297】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。

【0298】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。

【０２９９】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。

【０３００】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。

【０３０１】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。

【０３０２】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。

【０３０３】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。

【０３０４】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。

【０３０５】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。

【０３０６】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。

【０３０７】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。

【０３０８】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。

【０３０９】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。

【０３１０】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。

【０３１１】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。

【０３１２】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。

【０３１３】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。

【０３１４】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。

【０３１５】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。

【０３１６】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。

【０３１７】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。

【０３１８】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。

【０３１９】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。

【０３２０】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。

【０３２１】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。

【０３２２】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。

【0323】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。

【0324】

【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、一定の地域の利用者端末装置に対する課金情報を管理する機能と、ディジタルコンテンツを展示，配信する機能と、ディジタルコンテンツの加工、上記ディジタルコンテンツ展示配信機能に対する上記加工したディジタルコンテンツの配信、課金情報管理機能からの情報収集及び収益配分、全体のセキュリティ管理配分を行う機能とからなり、利用者端末装置と各機能との間のデータ通信はそれぞれ独立に行うことにより、通信のレスポンスを向上させることが可能となる。

【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。

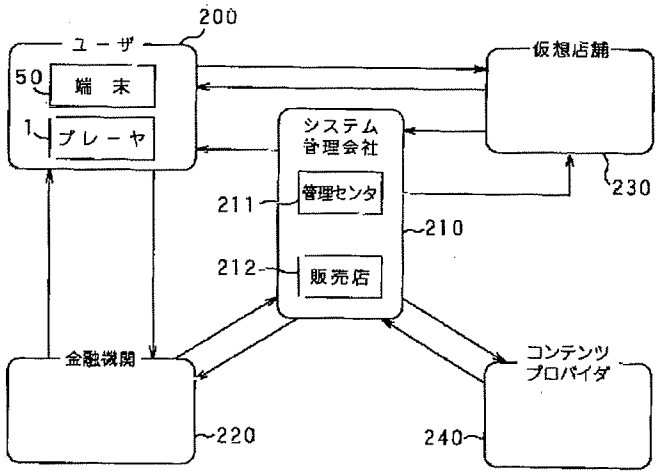
【図27】セキュリティＩＤとしての乱数を発生する具体的構成を示すブロック回路図である。

【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。

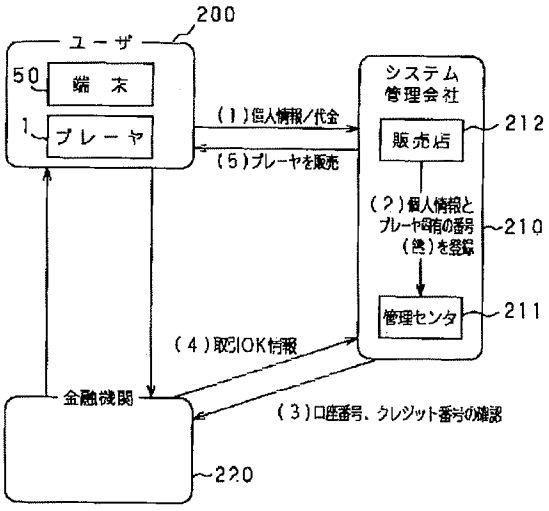
【図29】受信文から乱数が取り出されて正当性の確認がなされる様子を説明するための図である。

【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

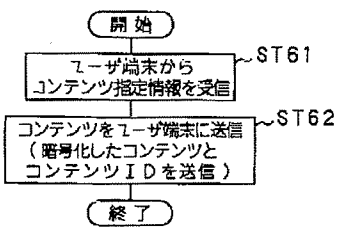
【図１】



【図４】

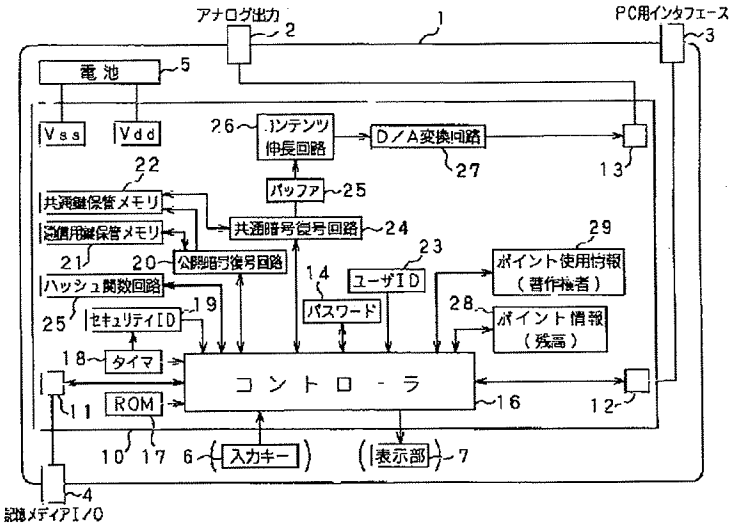


【図１４】

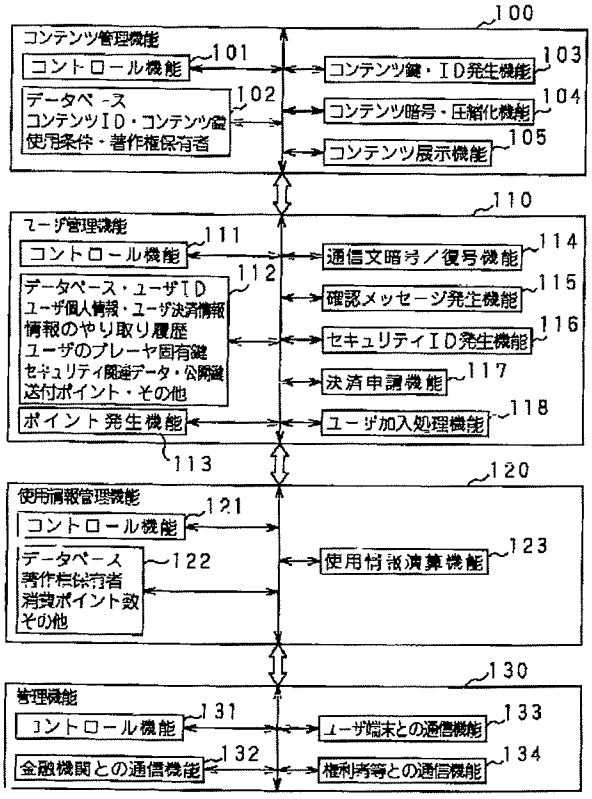


コンテンツ入手時の管理センタのフローチャート

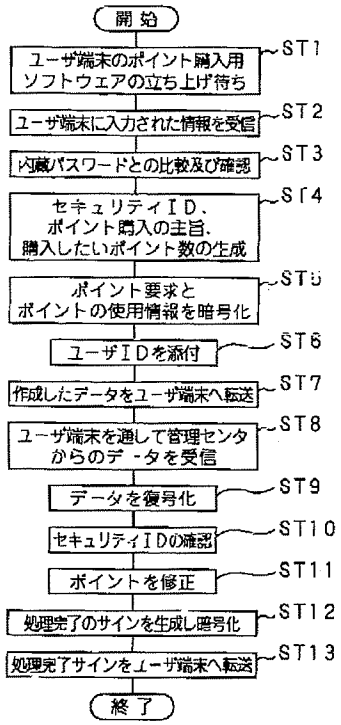
【図2】



【図3】

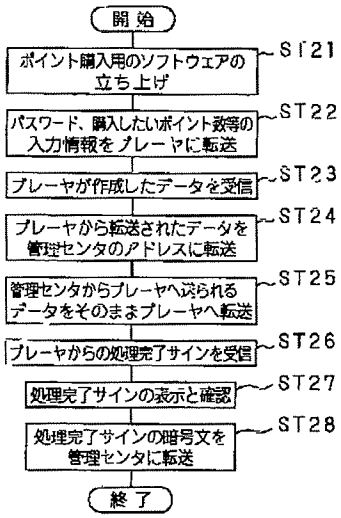


【図8】



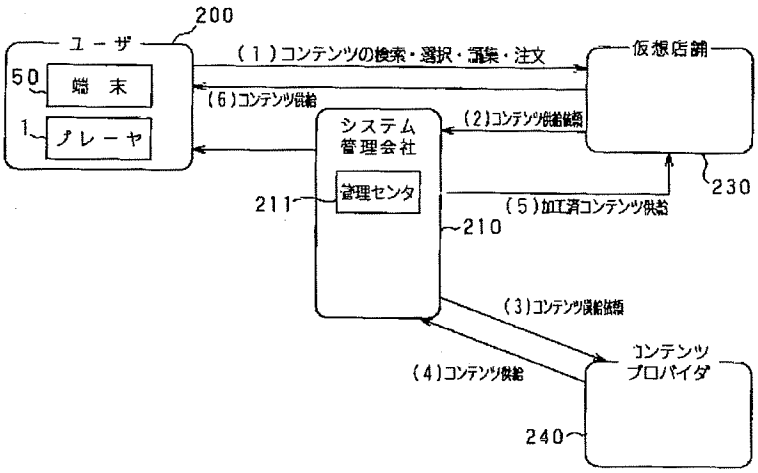
ポイント購入時のプレーヤのフローチャート

【図9】

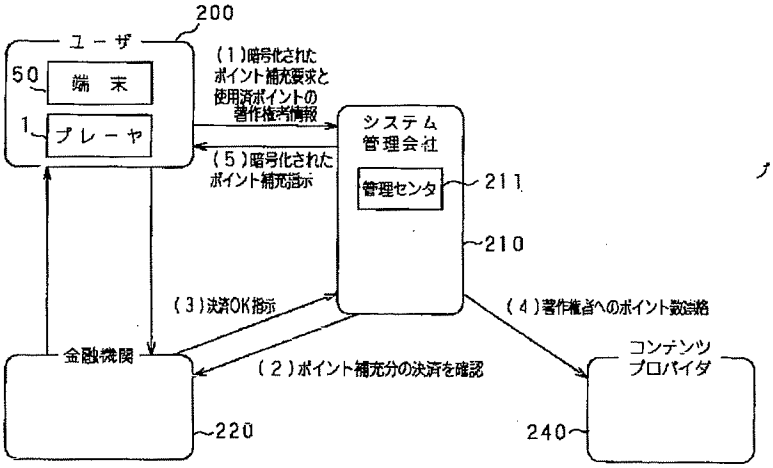


ポイント購入時のユーザ端末のフローチャート

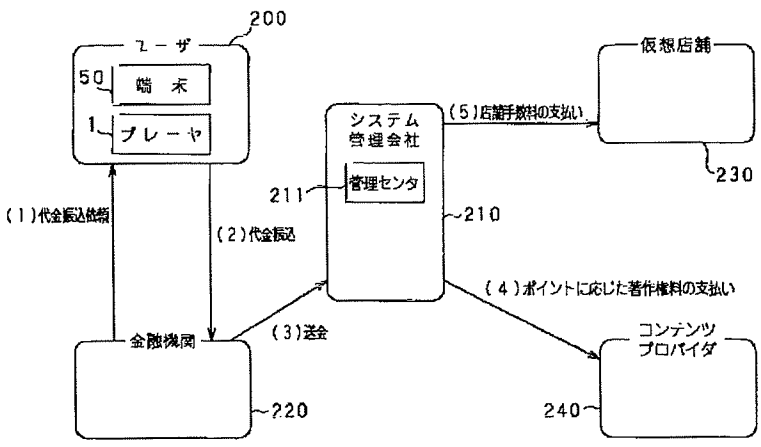
【図5】



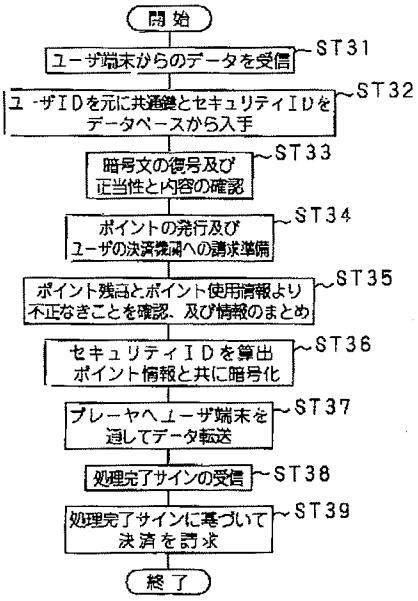
【図6】



【図7】

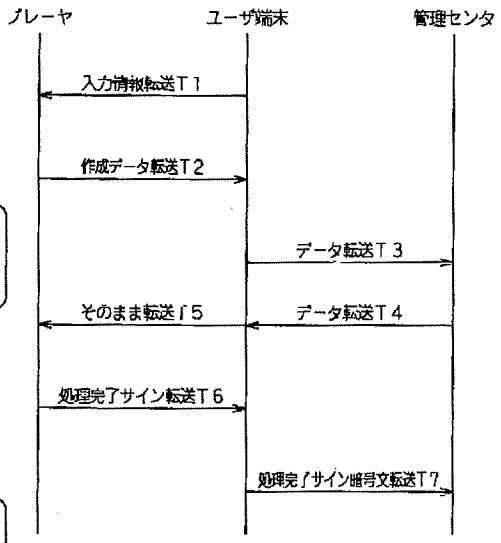


【図10】



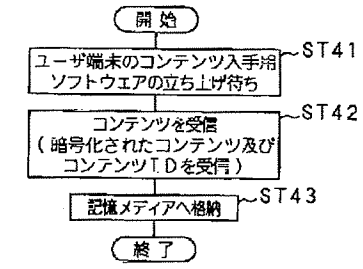
ポイント購入時の管理センタのフローチャート

【図11】



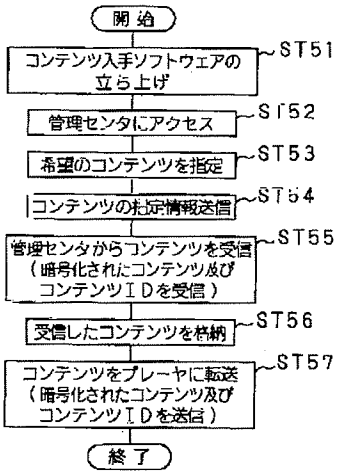
ポイント購入時のシーケンス

【図12】



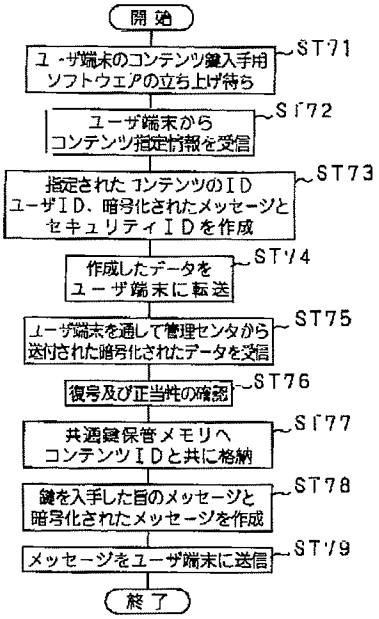
コンテンツ入手時のプレーヤのフローチャート

【図13】



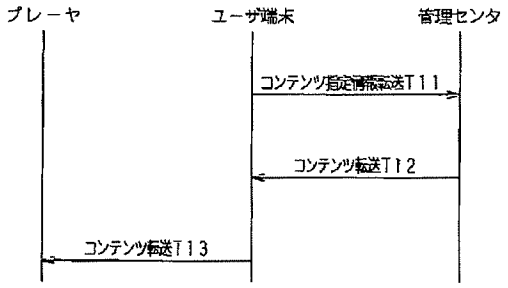
コンテンツ入手時のユーザ端末のフローチャート

【図16】



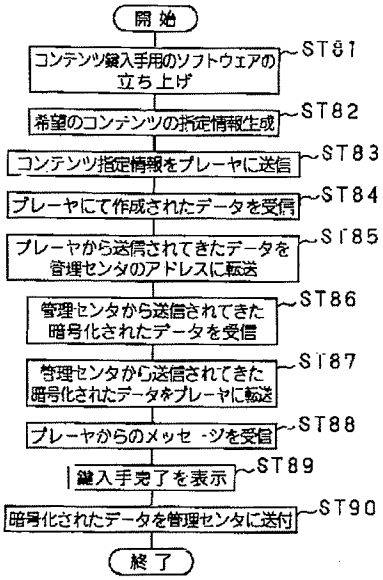
コンテンツ鍵・入手時のプレーヤのフローチャート

【図15】



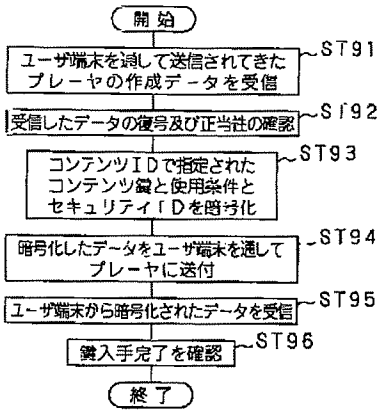
コンテンツ入手時のシーケンス

【図17】



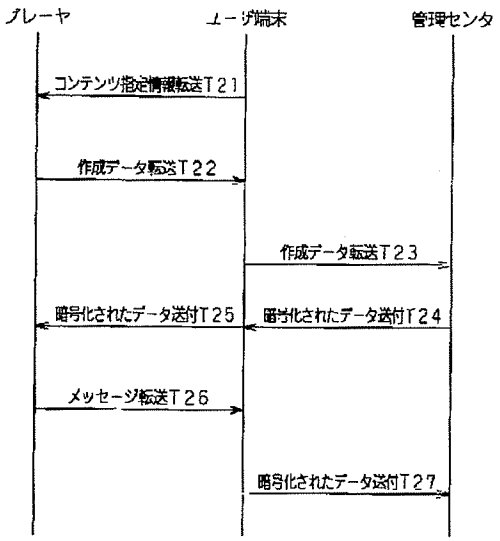
コンテンツ鍵・使用条件入手時のユーザ端末のフローチャート

【図18】



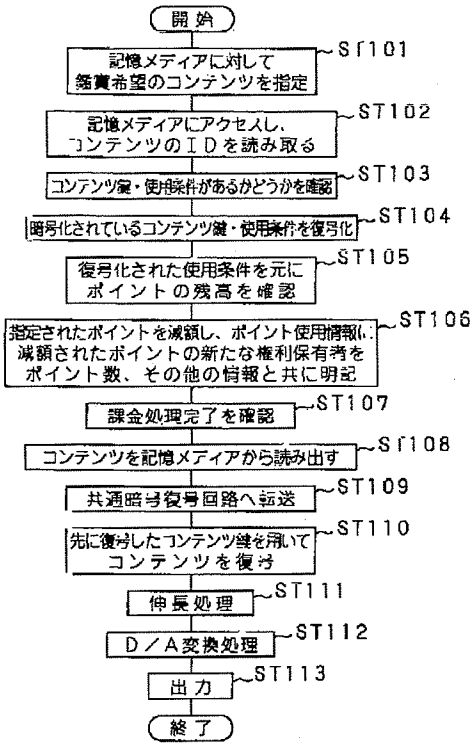
コンテンツ鍵・使用条件入手時の管理センタのフローチャート

【図19】



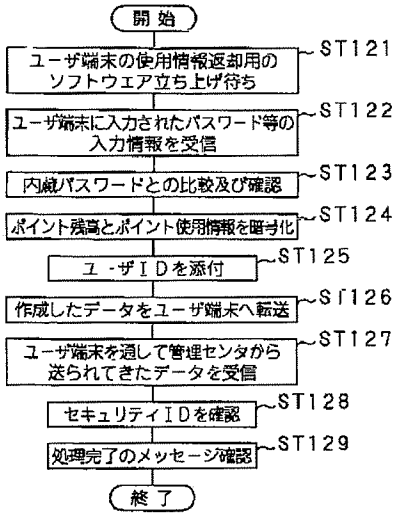
コンテンツ鍵・使用条件入手時のシーケンス

【図20】



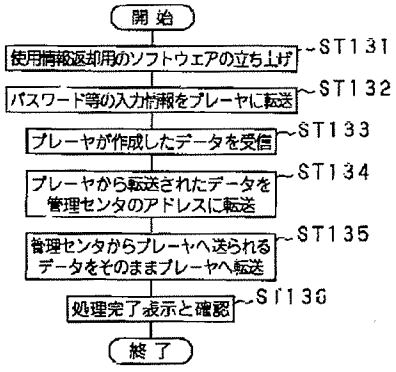
コンテンツ録音時のプレーヤのフローチャート

【図21】



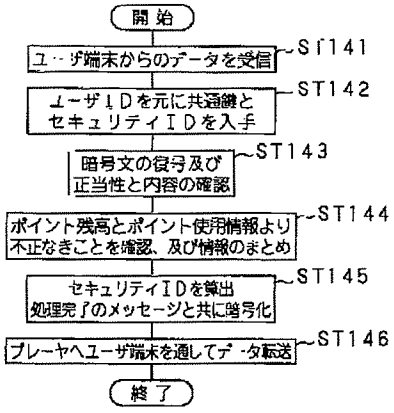
使用情報返却時のプレーヤのフローチャート

【図22】



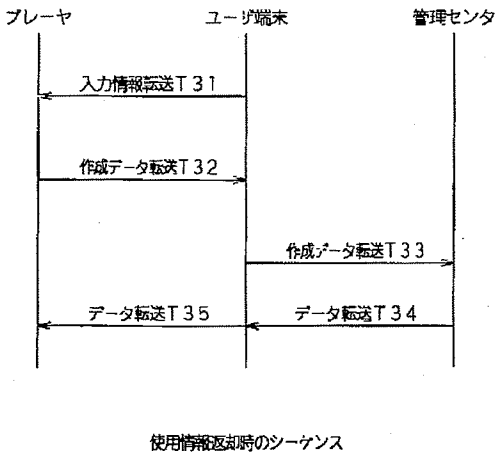
使用情報返却時のユーザ端末のフローチャート

【図23】



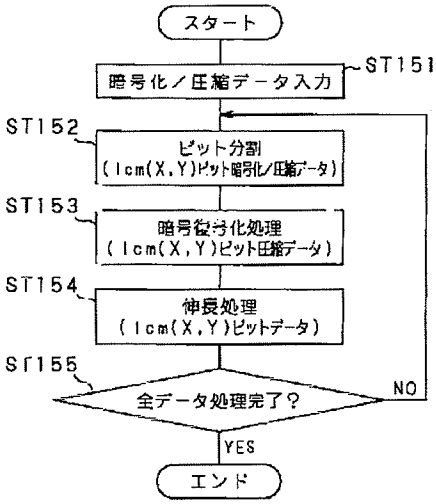
使用情報返却時の管理センタのフローチャート

【図24】

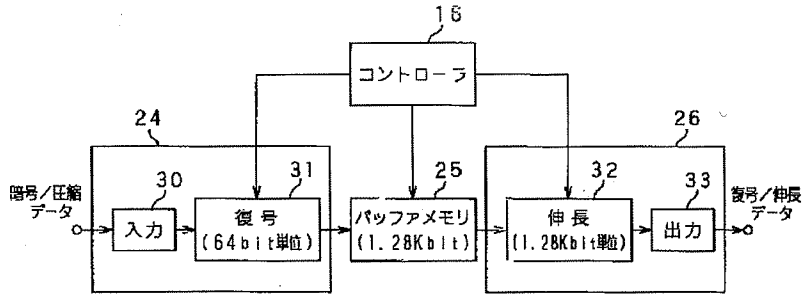


使用情報返却時のシーケンス

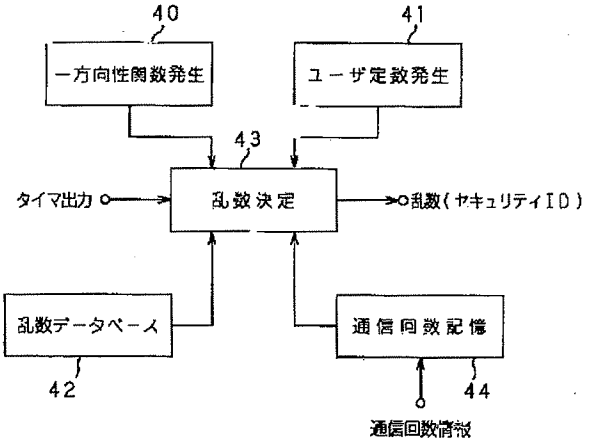
【図25】



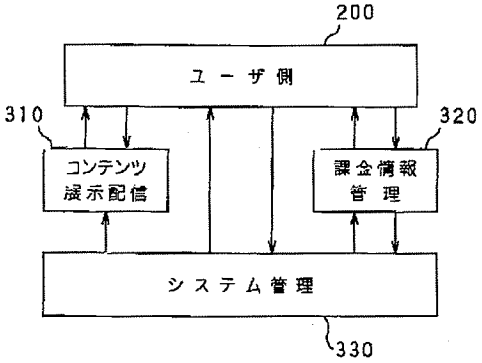
【図26】



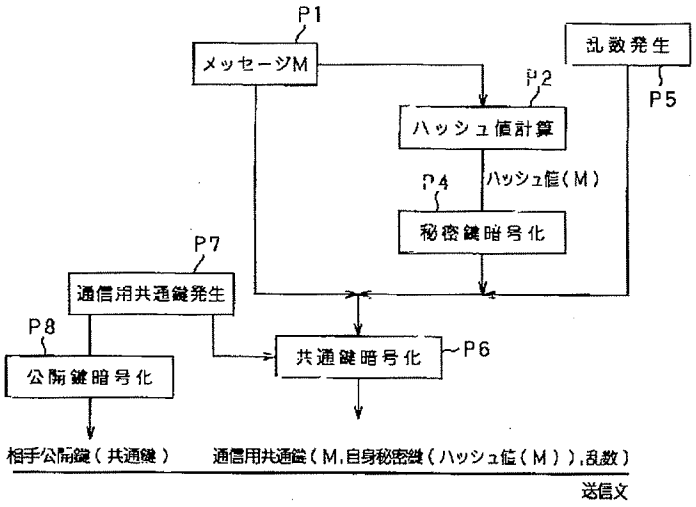
【図27】



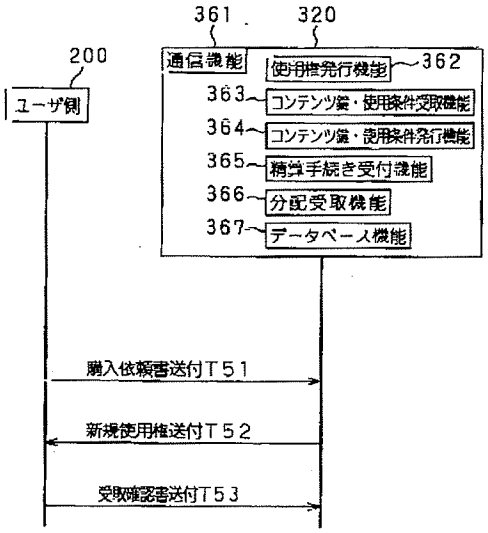
【図30】



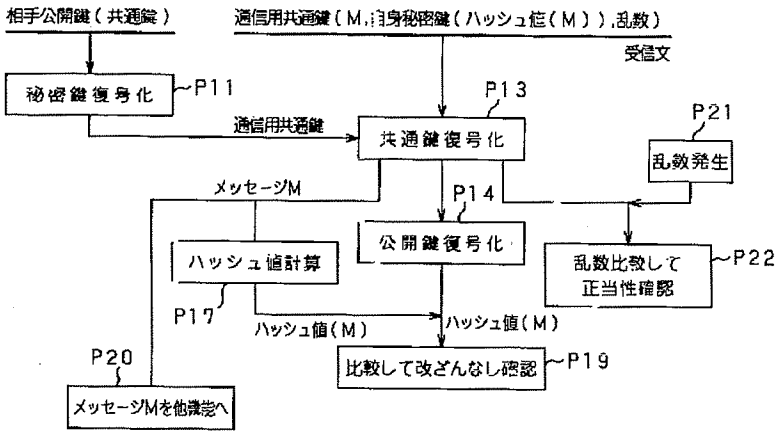
【図28】



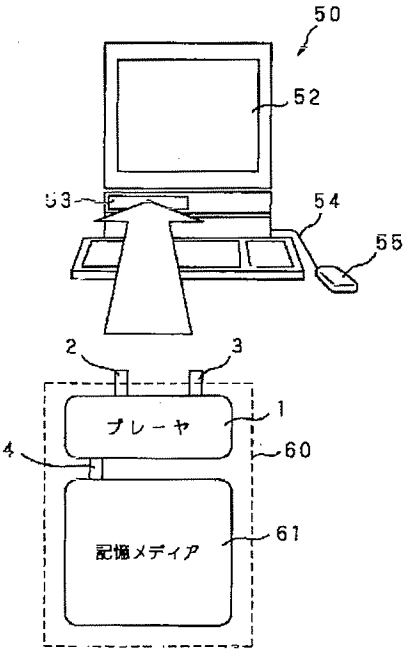
【図32】



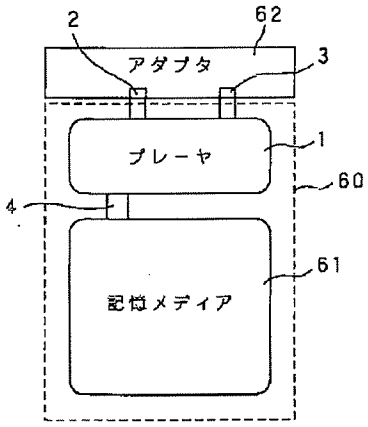
【図29】



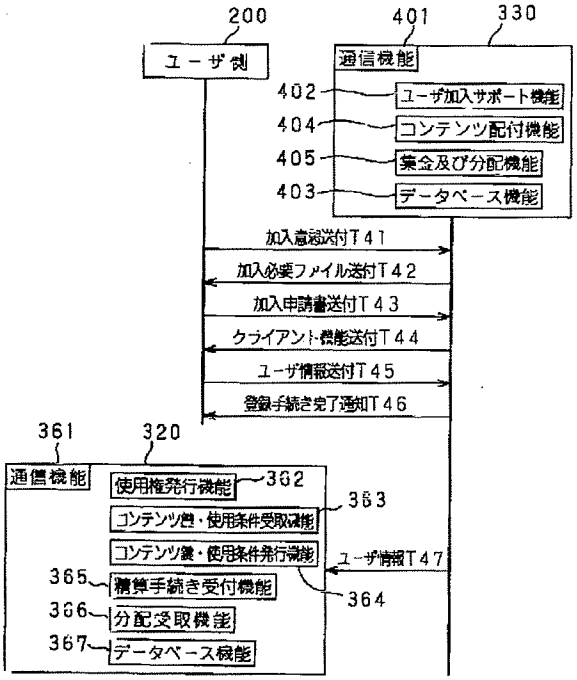
【図39】



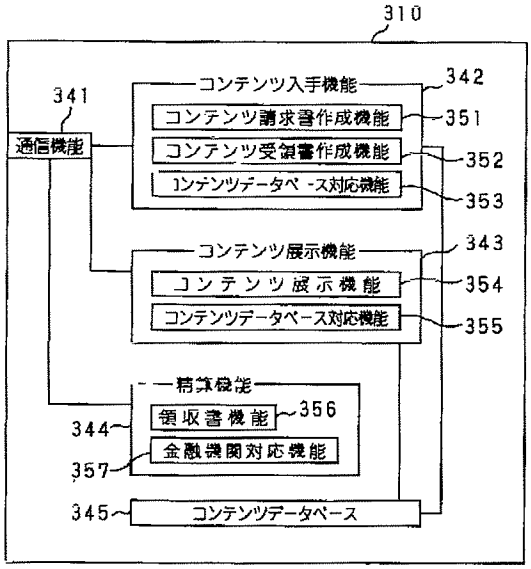
【図40】



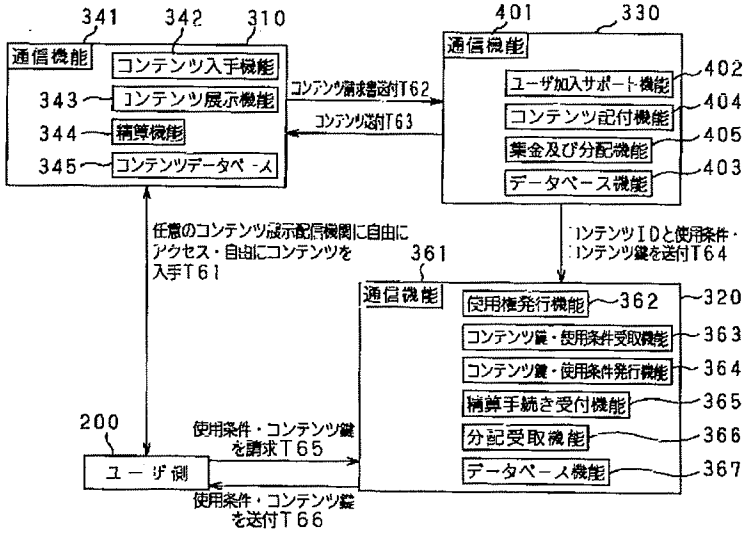
【図31】


200
401
330
ユーザ側
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
364
365
精算手続き受付機能
366
分配受取機能
367
データベース機能

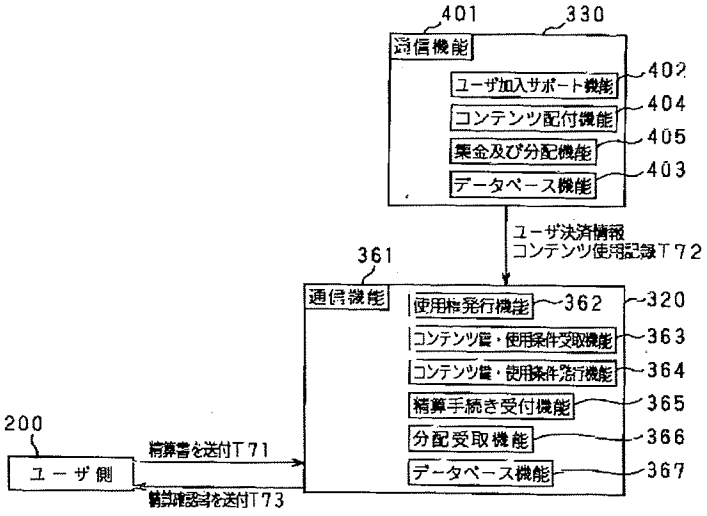
【図35】


310
341
通信機能
コンテンツ入手機能
342
コンテンツ請求書作成機能
351
コンテンツ受領書作成機能
352
コンテンツデータベース対応機能
353
コンテンツ展示機能
343
コンテンツ展示機能
354
コンテンツデータベース対応機能
355
精算機能
領収書機能
356
344
金融機関対応機能
357
345
コンテンツデータベース

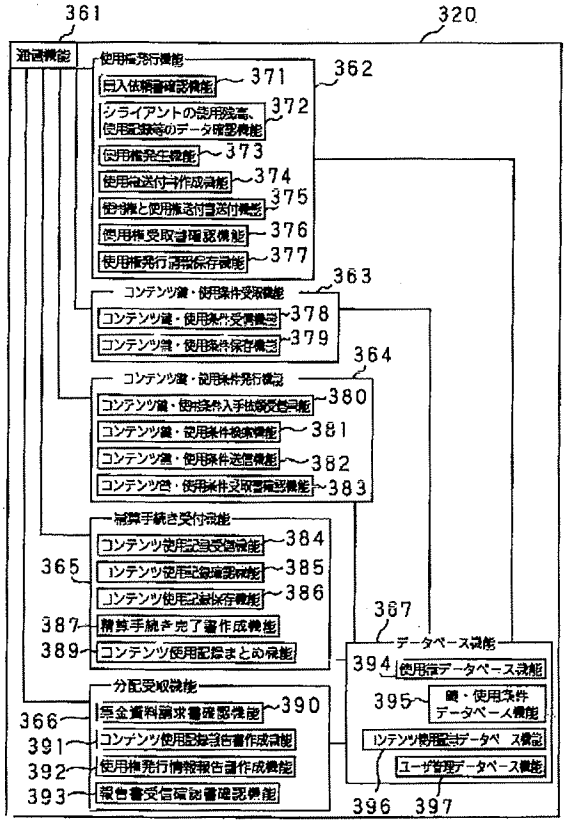
【図33】


341
342
310
401
330
通信機能
コンテンツ入手機能
通信機能
ユーザ加入サポート機能
402
343
コンテンツ展示機能
コンテンツ請求書送付T62
コンテンツ送付T63
コンテンツ配付機能
404
344
精算機能
集金及び分配機能
405
345
コンテンツデータベース
データベース機能
403
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
分記受取機能
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

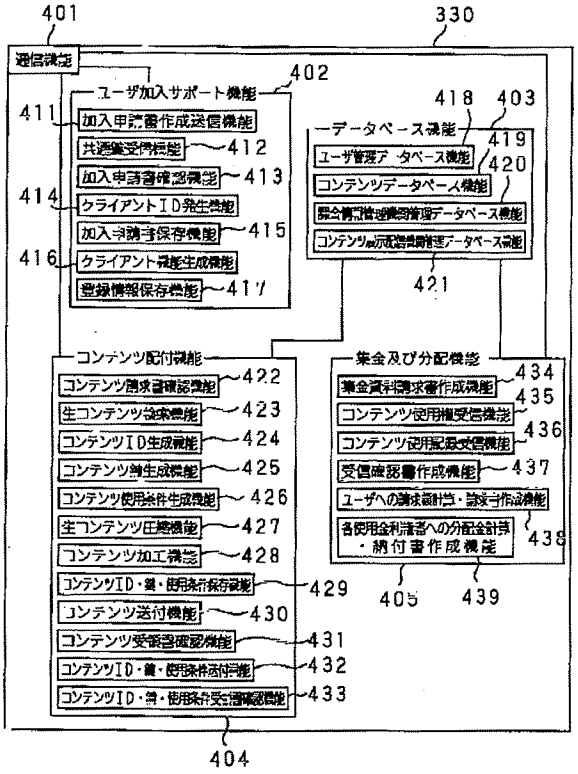
【図34】


401
330
通信機能
ユーザ加入サポート機能
402
コンテンツ配付機能
404
集金及び分配機能
405
データベース機能
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

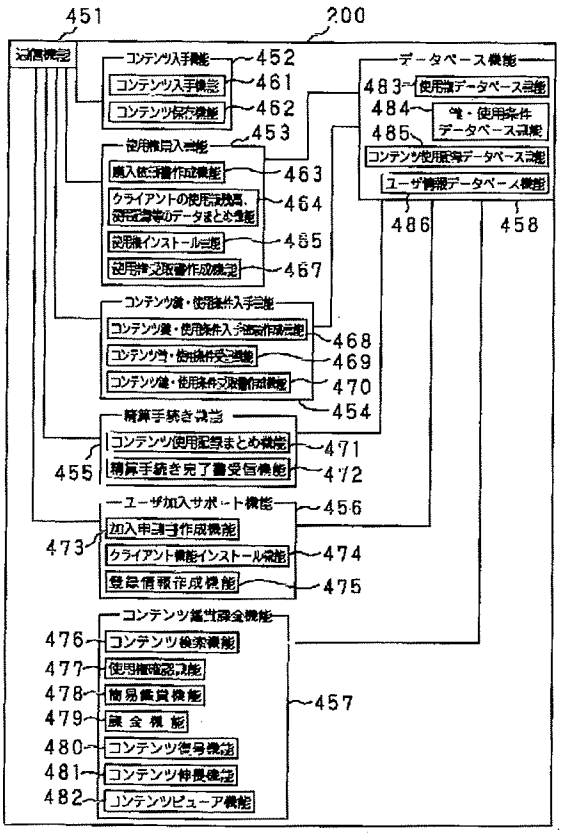
【図36】


361
320
通信機能
使用権発行機能
362
371
372
373
374
375
376
377
コンテンツ鍵・使用条件受取機能
363
378
379
コンテンツ鍵・使用条件発行機能
364
380
381
382
383
精算手続き受付機能
384
365
385
386
387
388
389
分配受取機能
390
366
391
392
393
367
データベース機能
394
使用権データベース機能
395
鍵・使用条件データベース機能
ユーザ管理データベース機能
396
397

【図37】


401
330
通信機能
ユーザ加入サポート機能
402
411
加入申請書作成送信機能
共通鍵受信機能
412
加入申請書確認機能
413
414
クライアントID発生機能
加入申請書保存機能
415
416
クライアント識別生成機能
登録情報保存機能
417
418
403
データベース機能
419
ユーザ管理データベース機能
420
コンテンツデータベース機能
421
コンテンツ配付機能
コンテンツ請求書確認機能
422
生コンテンツ検索機能
423
コンテンツID生成機能
424
コンテンツ鍵生成機能
425
コンテンツ使用条件生成機能
426
生コンテンツ圧縮機能
427
コンテンツ加工機能
428
コンテンツID・鍵・使用条件保存機能
429
コンテンツ送付機能
430
コンテンツ受領書確認機能
431
コンテンツID・鍵・使用条件送付機能
432
コンテンツID・鍵・使用条件受領確認機能
433
404
集金及び分配機能
集金資料請求書作成機能
434
コンテンツ使用権受信機能
435
コンテンツ使用記録送信機能
436
受信確認書作成機能
437
ユーザへの請求額計算・請求書作成機能
各使用金利清算への分配金計算・納付書作成機能
438
405
439

【図38】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04L 12/14		H04L 9/00	601E
		11/02	F

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-269291

(43)Date of publication of application : 09.10.1998

(51)Int.Cl.	G06F 17/60	G06F 9/06	G06F 15/00
	G09C 1/00	H04L 9/08	H04L 12/14

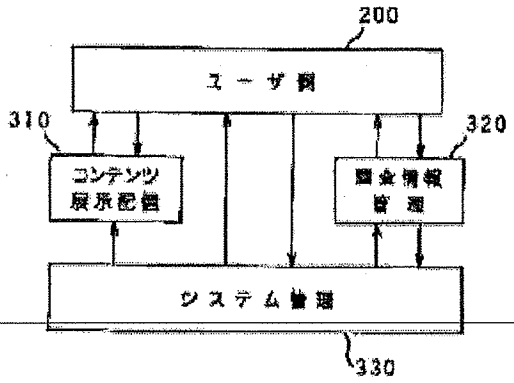
(21)Application number : 09-074185

(22)Date of filing : 26.03.1997

(71)Applicant : SONY CORP

(72)Inventor : MAARI KOUICHI

(54) DIGITAL CONTENT DISTRIBUTION MANAGING SYSTEM



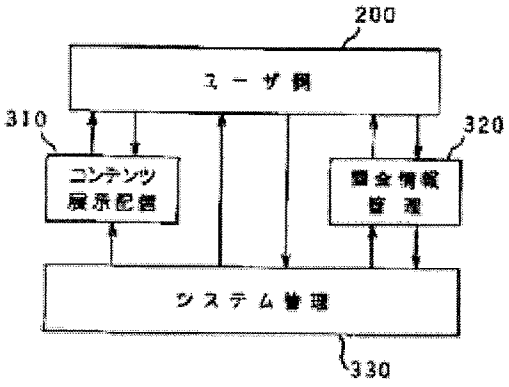
(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a digital data distribution managing system that can improve the response of communications by making a charging information managing means, a content exhibition distribution means and a system managing means respectively and independently execute data communications with a user terminal equipment.

SOLUTION: The configuration at a system side against a user side 200 is divided into a content exhibition distributing institution 310 provided with a function for exhibiting and distributing the digital contents, a charging information managing institution 320 provided with a function for managing user charging information and a system managing institution 330 provided with a function for generating data, such as enciphering the digital contents, etc., for distributing generated data to the content exhibiting distributing institution 310, for collecting information from the charging information managing institution 320, for distributing profit and for managing the security of the whole system. And, the respective institutions 310, 320 and 330 are made to be able to communicate with the user side 200 respectively and independently. Therefore, communications are prevented from being concentrated and the communication response is improved.

4) DIGITAL CONTENT DISTRIBUTION MANAGING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a digital data distribution managing system that can improve the response of communications by making a charging information managing means, a content exhibition distribution means and a system managing means respectively and independently execute data communications with a user terminal equipment.
SOLUTION: The configuration at a system side against a user side 200 is divided into a content exhibition distributing institution 310 provided with a function for exhibiting and distributing the digital contents, a charging information managing institution 320 provided with a function for managing user charging information and a system managing institution 330 provided with a function for generating data, such as enciphering the digital contents, etc., for distributing generated data to the content exhibiting distributing institution 310, for collecting information from the charging information managing institution 320, for distributing profit and for managing the security of the whole system. And, the respective institutions 310, 320 and 330 are made to be able to communicate with the user side 200 respectively and independently. Therefore, communications are prevented from being concentrated and the communication response is improved.



TECHNICAL FIELD
[Field of the Invention]This invention distributes digital contents among a user-terminal device, for example, and it relates to the digital contents distribution managerial system which performs those managements.

PRIOR ART
[Description of the Prior Art]Facilitate circulation of digital contents, such as a computer program, audio information, a video data, delve into a latent demand, and as a technique advantageous to a market expansion, For example, a technique like the software management method indicated to JP,H6-19707,B, the software use managing system indicated to JP,H6-28030,B, and the software management method indicated to JP,H6-95302,B exists. The software management method indicated to above-mentioned JP,H6-19707,B enables it to grasp the Assessment on Search Report by Designated Searching Authority of software according to a software right holder etc. when using software, such as a computer program which is intangible property, and a video data. The software use managing system indicated to JP,H6-28030,B, Use of software, such as a computer program which is intangible property, and a video data, is faced, Buy an onerous program (after buying, it can be used for free), attach a price, provide the data in which the amount of money which can be purchased is shown in the computer system, and in the case of onerous program purchase. Register with a table as a name of the available software in a same system, and. When reducing the

data in which the amount of money concerned which can be purchased is shown by a software price and erasing registered software from this table, it is made to carry out renewal of an increase of the data in which the amount of money in which this purchase is possible is shown according to a situation. The software management method indicated to above-mentioned JP,H6-95302,B, In order to collect a utilization charge when using software, such as a computer program which is intangible property, and a video data, according to actual utilization quantity (using frequency or utilization time) per onerous program, It is effective in the system in the case of carrying out "recording a user identification signal and a fee" with discernment of the used program, and a program right holder being able to grasp the utilization charge of a program which he owns by collecting these records, and collecting the program utilization charges according to the utilization quantity of the program.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention]By the way, in the system which distributes digital contents using the above networks, Communication concentrates on the system side in the time of a user obtaining digital contents from the system side, and the case of the fee collection accompanying use of digital contents, and there is a possibility that a satisfying response may not be obtained to a user.

[0004]Then, this invention is made in view of such a situation, and is a thing.

It is providing the digital data distribution managerial system which can raise the purpose.

EFFECT OF THE INVENTION

[Effect of the Invention]The function to manage the accounting information to the user-terminal device of a fixed area by this invention by the above explanation so that clearly, The function which exhibits digital contents and is distributed, and processing of digital contents, It consists of a function to perform the information gathering and profit distribution from the distribution of digital contents to the above-mentioned digital content display distribution function processed [above-mentioned], and an accounting information controlling function, and the whole security management distribution, and the data communications between a user-terminal device and each function are performed independently, respectively.

Therefore, it becomes possible to raise a communicative response.

MEANS

[Means for Solving the Problem]A function to manage accounting information to a user-terminal device of a fixed area according to this invention, A function which exhibits digital contents and is distributed, and processing of digital contents, Distribution of digital contents to the above-mentioned digital content display distribution function processed [above-mentioned], Consisting of a function to perform information gathering and profit distribution from an accounting information controlling function, and the whole security management distribution, data communications between a user-terminal device and each function solve SUBJECT mentioned above by carrying out independently, respectively.

[0006]

[Embodiment of the Invention]Hereafter, the desirable embodiment of this invention is described, referring to Drawings.

[0007]First, before giving the concrete contents of the digital contents distribution managerial system of this invention, and explanation of composition, in order to make these understanding easy, the outline composition of the whole system and the operation method of a system with which this invention is applied are briefly explained using each figure from drawing 1 to drawing 7.
[0008]The rough composition of the whole system is shown in drawing 1.
[0009]In this drawing 1, user side 200 assumes that the digital contents playback device (it will be hereafter called the player 1) and what is called a personal computer (it will be hereafter called the user terminal 50) of this invention are held.
[0010]Although the user terminal 50 is the usual personal computer, The various software which is used for this invention and which is mentioned later is stored as application software, and while, it comes to connect the loudspeaker which is the display device and sound emission means which are displaying means, a keyboard, a mouse which are information input means, etc. Via a network, the system management company 210 and connection are possible for the user terminal 50 concerned, and it has an interface means between the players 1, and data transmission and reception are possible for it.
[0011]The player 1 has composition as shown in drawing 2.
[0012]Although detailed explanation of the composition of this drawing 2 is mentioned later, The player 1 concerned as the main components of the processing route of digital contents, It has the common key encryptosystem decoder circuit 24 which decrypts the digital contents enciphered using a contents key, the expansion circuit 26 which is the expansion means which elongate the digital contents compressed, and the D/A conversion circuit 27 which changes digital data into an analog signal at least. The decryption told to below is solving encryption.
[0013]The information which shows the right information data and the operating condition of digital contents which this player 1 uses. (These information is hereafter called point usage information) The possession money data which is needed when using digital contents, Namely, as the main components treating the billing data (it is hereafter called point information) etc. which are reduced whenever it uses digital contents, It has at least the point usage information storing memory 29 which stores the above-mentioned point usage information, and the point information storing memory 28 which stores the above-mentioned point information.
[0014]This player 1 as composition for storing the various keys used for encryption and decryption which are mentioned later The common key storage memory 22 and the key storage memory 21 for communication, It has the common code decoder circuit 24 and the open code decoder circuit 20 as composition for performing encryption and decryption using the key stored in these. This player 1 as composition relevant to the above-mentioned encryption and decryption, It also has the security ID generating circuit 19 and the timer 18 which generate the random number interlocked with the host computer of the system management company 210, and generate security ID, and the hash function circuit 25 grade which generates what is called a hash value mentioned later.
[0015]In addition, the player 1 concerned is provided with the controller 16 which is a control means which performs digital contents, various kinds of data in addition to this, and control of each component based on the program stored in ROM17, and the cell 5 as operation power at the time of carrying.
[0016]Here, as for each main components of the player 1 of drawing 2, it is desirable on security to comprise one chip of IC (integrated circuit) or LSI (large scale integration circuit). In this drawing 2, 1 chip making of each main components is

carried out into the integrated circuit 10. The player 1 concerned is equipped with three terminals (the analog output terminal 2, the Interface Division terminal 3 for PC, and the I/O terminal 4 for archive media) as an object for Interface Division with the exterior, and these each terminal is connected to the terminals 13, 12, and 11 in which the integrated circuit 10 corresponds, respectively. These each terminal is possible also for also unifying and newly providing another terminal, and is not scrupulous in particular.

[0017]The system management company 210 consists of the control center 211 which manages the whole system, and the store 212 which sells the above-mentioned player 1, and via the virtual online shop 230 between the user terminals 50 of user side 200, Transmission and reception of the information about supply of digital contents which is mentioned later, processing of the digital contents which compress and encipher the contents which the content provider 240 holds, the supply of digital contents processed [above-mentioned], the information transmission and reception between the financial institutions 220, etc. are performed. Between the system management company 210 and the financial institution 220, the exchange of the check of the account number of user side 200, a credit number, a name, a contact, etc., the information on the ability to trade between user side 200, etc., etc. are performed. Processing of actual price transfer etc. is performed between the financial institution 220 and user side 200. The store 212 does not necessarily need to be included in the system management company 210, and may be a sales agent.

[0018]The control center 211 of the above-mentioned system management company 210 has composition as shown, for example in drawing 3. Although detailed explanation of the composition of this drawing 3 is mentioned later, As the main components, manage digital contents and Processing treatment, such as the exhibition, encryption, and compression, The contents managing functional block 100 which has each function which is the key information used for encryption and decryption of digital contents, such as a contents key and generating of ID, Manage User Information and Encryption and decryption of correspondence (a message, point information, etc.), The user management functional block 110 provided also with the user subscription processing function part 118 which performs user subscription processing besides each function, such as generating of a confirmation message, generating of security ID, a settlement-of-accounts application between the financial institutions 230, generating of the point, etc., It has at least the usage information controlling-function block 120 which manages point usage information etc., and the controlling-function block 130 which manages the whole system and has a communication function.

[0019]An example of the actual operation method of the system constituted like drawing 1 mentioned above is explained using drawing 4 - drawing 7. The following operation methods are procedures which user side 200, the system management company 210, the financial institution 220, and content provider 240 grade actually follow.

[0020]The procedure of the purchase of the player 1 in explanation of the operation method of this system, the procedure from search of digital contents to installation of the digital contents to the memory medium for player 1, The procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making the digital contents concerned usable and the procedure of distribution of the fee collection price collected from the user with appreciation of digital contents are explained in order.

[0021]First, as a procedure at the time of the purchase of the player 1, as shown in (1) of drawing 4, and (5), user side 200 actually purchases the above-mentioned player 1 from the above-mentioned store 212 by the shop front or mail order.
[0022]Personal information (a name, a contact, etc.) and settlement information (a bank account, a credit number, etc.) which were provided from above-mentioned user side 200 at the time of sale of the above-mentioned player 1 at this time as the above-mentioned store 212 was shown in (2) of drawing 4, The number (a player inherent key etc. are included) peculiar to the player 1 which sold [above-mentioned] is registered into the control center 211 of the system management company 210.
[0023]As shown in (3) of drawing 4, the control center 211 checks an account number, a credit number, etc. which were provided from above-mentioned user side 200 to the financial institution 220, and as shown in (4) of drawing 4, it acquires the information on the purport that it can trade from the financial institution 220.
[0024]User side 200 [next,] which purchased the above-mentioned player 1 as a procedure to installation of the digital contents from search of digital contents to the memory medium for player 1, Using the user terminal 50 provided with the interface means with the player 1 concerned, as shown in (1) of drawing 5, search of the digital contents of hope, selection, edit, an order, etc. are performed. Processing from the search at this time to an order is performed to the virtual online shop 230 where the user terminal 50 was connected via the network using the retrieval software stored as application software.
[0025]The virtual online shop 230 is a store which the control center 211 has provided virtually on a network, for example, and the information which shows the contents of two or more contents, for example is exhibited by this virtual online shop 230. User side 200 will place an order for desired contents based on these information provided in the virtual online shop 230. As information which shows the contents of the contents exhibited by the virtual online shop 230, When contents are video datas, such as a movie, for example, titles and advertisements, such as the movie concerned, Images, such as one scene in the movie concerned, etc. can be considered, and when contents are audio information, a track name, an artist name, the number phrase (what is called an intro) of the beginning of the music concerned, etc. can be considered. Therefore, when the above-mentioned virtual online shop 230 is accessed with the user terminal 50 of user side 200. The order of contents will be performed because the contents of two or more contents of the above-mentioned virtual online shop 230 are exhibited virtually and choose a desired thing out of these display objects on the user terminal 50 concerned.
[0026]When there are an order of digital contents, etc. from the user terminal 50 of above-mentioned user side 200, the above-mentioned virtual online shop 230 performs the supply request of digital contents to the control center 211, as shown in (2) of drawing 5.
[0027]The control center 211 which received the supply request of the digital contents concerned performs the distribution request of the digital contents which had the above-mentioned supply request to the content provider 240. Thereby, the content provider 240 concerned supplies the digital contents which had the above-mentioned distribution request as shown in (4) of drawing 5 to the control center 211.
[0028]The control center 211 performs encryption and compression using predetermined compression technology to the digital contents rationed by the above-mentioned content provider 240, and. The virtual-online-shop name etc. which supply charge amount and contents when right holder information and the contents concerned, such as ID (content ID) of the contents concerned and an owner of a

copyright of these contents, are used to user side 200 are added to these digital contents compressed and enciphered. The charge amount to contents is determined a priori by the content provider 240.
[0029]The contents processed in the above-mentioned control center 211 are sent to the virtual online shop 230, and as shown in (5) of drawing 5, as shown in (6) of drawing 5, they are further supplied to the user terminal 50 of user side 200 via this virtual online shop 230. By this, contents will be supplied to the player 1 from the above-mentioned user terminal 50, and these contents will be stored in the player 1 concerned.
[0030]It is also possible to carry out to this drawing 5 a priori about flowing to (2) - (5). That is, it not only may exhibit the information which shows the contents of two or more above-mentioned contents, but it may prepare beforehand for the virtual online shop 230 the digital contents corresponding to these exhibitions processed [above-mentioned].
[0031]Next, in the procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making usable the digital contents installed in the player 1 as mentioned above. First, with the user terminal 50, shortage of the point information stored in the player 1 is checked, and a supplement demand of point information is made from the user terminal 50 concerned.
[0032]At this time, as shown in (1) of drawing 6, from the user terminal 50 concerned, the supplement request of the point information enciphered by the player 1 is transmitted to the control center 211. Simultaneously, it is read from the player 1, is enciphered and is sent to the control center 211 via the user terminal 50, a right holder's information, i.e., point usage information, corresponding to the already used digital contents, such as an owner of a copyright. Thus, transmission of point usage information was made to be performed simultaneously with the supplement request of point information, in order that user side 200 might save the time and effort which accesses the control center 211 only for transmission to the control center 211 of the point usage information concerned. Of course, it is not necessary to necessarily perform transmission of this point usage information simultaneously with the purchase of point information, and may carry out independently.
[0033]The control center 211 which received the supplement request and point usage information of point information which were enciphered [above-mentioned] recognizes the replenishing amount of point information and the contents of point usage information which user side 200 is demanding by decoding the code concerned. The control center 211 concerned checks [of drawing 6] whether as shown in (2), the settlement of accounts for the point supplement concerned is possible to the financial institution 220. From the financial institution 220 concerned, a check accounts can be settled by investigating the account of user side 200 in the financial institution 220 will send directions of the settlement of accounts O.K. to the control center 211, as shown in (3) of drawing 6.
[0034]The control center 211 at this time connects the point usage number which will be paid to right holders, such as an owner of a copyright, to the content provider 240, i.e., the amount of money, as shown in (4) of drawing 6.
[0035]Then, in the control center 211, the letter missive of point supplementary information is enciphered, and with security ID, by making this into point supplement directions information, as shown in (5) of drawing 6, it sends to the user terminal 50. The above-mentioned point supplement directions information sent to the player 1 from this user terminal 50, It is decrypted in the player 1 concerned and supplement of

the point information on the point information storing memory 28 and deletion of right holder information, including the copyright information etc. which were connected to the above place from the point usage information storing memory 29, are further performed after the check of security ID.

[0036]Next, the fee collection price collected from the user with appreciation of digital contents, That is, in the procedure of distribution of the price which will be charged directly to a user's account according to the usage information of a point, first, as shown in (1) of drawing 7, a price transfer request is made from the financial institution 220 to user side 200. When a price transfer request in particular is not made when there is sufficient balance for the account of user side 200 at this time, and there is not sufficient balance for an account, as shown in (2) of drawing 7, transfer of a price is made from user side 200 to the financial institution 220.

[0037]The financial institution 220 deducts a prescribed fee, and as shown in (3) of drawing 7, it remits the price received from user side 200 to the control center 211. That is, in the control center 211, the charge of contents processing, a financial fee, system management expense, etc. are collected from the above-mentioned price remitted from the financial institution 220. The control center 211 concerned pays the content provider 240 the royalty according to the point used previously, as shown in (4) of drawing 7, and as shown in (5) of drawing 7, it pays a store fee to the virtual online shop 230. The content provider 240 who received the above-mentioned royalty pays each owner of a copyright a royalty, and the virtual online shop 230 which received the above-mentioned store fee pays the fee for every virtual online shop to each virtual online shop.

[0038]Thus, the price paid from user side 200, Based on said point usage information, it is distributed to a royalty, a store fee, a contents processing fee, a settlement-of-accounts fee, and a system management fee, the above-mentioned royalty -- the content provider 240 -- the above-mentioned store fee -- the above-mentioned virtual online shop 230 -- pay the system management company 210 a contents processing fee, a settlement-of-accounts fee is paid to a system management company and the financial institution 220, and a system management fee is paid to the system management company 210.

[0039]Here, in the case of the data transmission and reception between the systems of this embodiment, i.e., the data transmission and reception between the control center 211 and the player 1, in order to secure the safety of data communications, the data encryption and decryption which communicate are performed. According to this invention embodiment, it can respond as a method of encryption and decryption to both a common key encryption system and a public-key crypto system.

[0040]In the embodiment of the invention, the common key encryption system is adopted from a point of processing speed as a cipher system in the case of transmission of the variety of information of the above-mentioned digital contents, the above-mentioned point usage information, point information, a message and security ID, and others. The common keys used for encryption and decryption of these varieties of information differ corresponding to each information, respectively. The common key used for decryption of the enciphered information which is transmitted from the control center 211 in the player 1 of said drawing 2 is kept by said common key storage memory 22, Said common code decoder circuit 24 decrypts the information enciphered from the above-mentioned control center 211 using the common key currently kept in this common key storage memory 22.

[0041]The cipher system adopted by whether the player inherent key which is a peculiar key of said player 1 deals with which method as a cipher system in the case

of transmission of the above-mentioned common key used for encryption and decryption of the above-mentioned variety of information on the other hand changes. That is, when the above-mentioned player inherent key supports the common key encryption system, the above-mentioned common key will be enciphered using the player inherent key concerned, and the enciphered common key concerned will be decrypted using the above-mentioned player inherent key. On the other hand, when the above-mentioned player inherent key supports the public-key crypto system, the public key of the partner point is used for encryption of the above-mentioned common key, and the secret key of the side which decrypts, respectively is used for decryption of the enciphered above-mentioned common key.

[0042]For example, in the case where the above-mentioned common key (for example, session key mentioned later) is sent to the control center 211 from the above-mentioned player 1, When the above-mentioned player inherent key supports the common key encryption system, In the above-mentioned player 1, the above-mentioned common key encryptosystem decoder circuit 24 enciphers the above-mentioned common key using the player inherent key which the key storage memory 21 for communication is keeping, and the common key enciphered [above-mentioned] is decrypted in the control center 211 using the player inherent key which the control center 211 concerned is keeping. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the control center 211 from the above-mentioned player 1 for example, The above-mentioned public-key-encryption decoder circuit 20 enciphers the above-mentioned common key in the public key of the control center 211 which the ** key storage memory 21 for communication of the above-mentioned player 1 is keeping, and the common key enciphered [above-mentioned] is decrypted in the control center 211 using the secret key which the control center 211 concerned is keeping.

[0043]On the contrary, when the above-mentioned common key (for example, contents key) is sent to the player 1, for example from the above-mentioned control center 211 and the above-mentioned player inherent key supports the common key encryption system. The above-mentioned common key is enciphered with the player inherent key which the above-mentioned control center 211 is keeping, and said common code decoder circuit 24 decrypts the common key enciphered [above-mentioned] using the player inherent key currently kept by the above-mentioned key storage memory 21 for communication in the player 1. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the player 1 from the above-mentioned control center 211 for example, The above-mentioned common key is enciphered in the public key of the player 1 which the above-mentioned control center 211 is keeping, and said open code decoder circuit 20 decrypts the common key enciphered [above-mentioned] using the player inherent key, i.e., the secret key, which are kept by the above-mentioned key storage memory 21 for communication in the player 1.

[0044]The cipher system of the player inherent key itself [which was mentioned above] is determined by whether delivery (delivery to the player 1 from the system management company 210) of the player inherent key concerned is easy. That is, since the common key encryption system is more advantageous in cost, if delivery of a player inherent key is easy, a common key encryption system will be adopted, but when delivery of the player inherent key concerned is difficult, it is a high cost, but a public-key crypto system is adopted. In mounting a player inherent key in hardware and mounting a common key encryption system in software, it adopts a public-key crypto system.

[0045]Hereafter, in an embodiment of the invention, the example which adopts the above-mentioned public-key crypto system will be given and explained in consideration of the compatibility in the case of mounting in software as a cipher system of a player inherent key itself. Namely, in the case where transmission of said common key is performed between the above-mentioned control center 211 and the player 1, When a common key (session key) is enciphered by the above-mentioned player 1 side, encryption is made using the public key of the control center 211, and the common key enciphered [above-mentioned] using the above-mentioned player inherent key (namely, secret key) is decrypted in the control center 211. On the contrary, when a common key (contents key) is enciphered by the above-mentioned control center 211 side, encryption is made in the public key of a player and the common key enciphered [above-mentioned] using the above-mentioned player inherent key (namely, secret key) is decrypted in the player 1.
[0046]Actual operation of the above-mentioned player 1, the user terminal 50, and the control center 211 which constitute the system employed using each procedure and a cipher system which were mentioned above is explained in order below.
[0047]First, it explains, referring to said drawing 2 and drawing 3 for flowing into the processing in the player 1 at the time of the point supplement, i.e., point purchase, which were mentioned above, the user terminal 50, and the control center 10 using drawing 11 from drawing 8.
[0048]The flow of the processing in the player 1 at the time of purchasing the point is shown in drawing 8.
[0049]In this drawing 8, starting of the software for point purchase beforehand installed in the user terminal 50, i.e., a personal computer, is performed by step ST1, It is waiting for the controller 16 of the player 1 in the meantime until the software for the point purchase concerned rises.
[0050]If the software for the above-mentioned point purchase rises, the controller 16 of the player 1 will receive the information inputted into the above-mentioned user terminal 50 from the user terminal 50 concerned in step ST2. An input request is made from the user terminal 50 concerned to the user who operates the above-mentioned user terminal 50 according to the software for the above-mentioned point purchase, and the information inputted into the user terminal 50 at this time is information, including a password, a point information number to purchase, etc.
[0051]The information from these user terminals 50 is received by the controller 16 via the terminal 12 of the integrated circuit 10 by which 1 chip making was carried out into the interface terminal 3 for PC of the player 1, and the player 1 concerned. The controller 16 which received the information from the user terminal 50 concerned, In step ST3, comparison with the password which the password storing memory 14 in the integrated circuit 10 of the player 1 concerned stores, and the password in the information which received [above-mentioned] is performed, and the above-mentioned receiving password checks that it is the right.
[0052]The above-mentioned password the right and the checked controller 16, At the same time it generates the information on the purport that he would like to purchase the point in step ST4 (main point of point purchase), and a point information number to purchase and other information, Security ID is generated from the security ID generating circuit 19, and these information is made to encipher by the common code decoder circuit 24 in the following step ST5. The controller 16 reads user ID from the user ID storing memory 23 in step ST6 next, It adds to the information which enciphered [above-mentioned] the user ID concerned, and the data which added and created the user ID concerned in step ST7 is further transmitted to the user terminal

50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50, the above-mentioned prepared data will be sent to the control center 211.

[0053]Since the common key encryption system is adopted as encryption of the above-mentioned prepared data at this time as mentioned above, generation of a common key is performed in advance of transmission of the prepared data concerned. For this reason, in the above-mentioned controller 16, a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation means, for example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto system here, in the above-mentioned controller 16. The public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken out, and it sends to the above-mentioned open code decoder circuit 20 at the same time it sends the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concerned, encryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus, with user ID, the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data.

[0054]As mentioned above, when also performing transmission of point usage information with a demand of point information, the controller 16 reads point usage information including said right holder information from the point usage information storing memory 29, and these also make the above-mentioned common code decoder circuit 26 send and encipher it. This enciphered point usage information is transmitted with the above-mentioned prepared data. Simultaneously with transmission of point usage information, it is also possible to transmit the balance of point information similarly.

[0055]Then, the controller 16 receives the data which has been sent from the control center 211 through the user terminal 50 in step ST8 and which is enciphered. The data sent from this control center 211 is the data in which the point information and information, including security ID etc., according to the above-mentioned point information number previously transmitted from the player 1 concerned to purchase were enciphered using the same common key as the above-mentioned session key.

[0056]If the data from the above-mentioned control center 211 is received, in step ST9, it sends the data concerned to the above-mentioned common code decoder circuit 24, and the controller 16 will read said common key which was generated previously and kept in the common key storage memory 22, and, similarly will send it to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, the data enciphered from the above-mentioned control center 211 using the above-mentioned common key is decrypted.

[0057]Next, security ID of the data in which the above-mentioned controller 16 was decrypted [above-mentioned] in step ST10, the point information which checked by comparison with security ID from the above-mentioned security ID generating circuit 19, and was stored in the above-mentioned point information storing memory 28 in step ST11 after the check -- the above -- it corrects for the newly sent point information.

[0058]After processing of correction of the above-mentioned point information, etc. is completed, the controller 16 generates the sign of processing completion, sends it to

the above-mentioned common code decoder circuit 24 with the common key read from the above-mentioned common key storage memory 22, and is made to encipher by the common code decoder circuit 24 concerned in step ST12. Then, the controller 16 transmits the sign of the enciphered processing completion concerned to the user terminal 50 via the terminals 12 and 3 in step ST13, and sends it to the control center 211.

[0059]By the above, the flow of the processing in the player 1 in the case of point purchase is completed.

[0060]Next, the flow of the processing in the user terminal 50 at the time of the above-mentioned point purchase is explained using drawing 9.

[0061]In this drawing 9, the user terminal 50 starts the software for point purchase in step ST21. When the software for point purchase concerned rises, in this user terminal 50. The input request of information, including the password mentioned above to the user who operates the user terminal 50 concerned in step ST22 according to the software for the above-mentioned point purchase, a point size to purchase, etc., is performed, If these information is inputted from a user, the inputted information concerned will be transmitted to the above-mentioned player 1 like step ST2 of said drawing 8.

[0062]Next, the user terminal 50 will transmit the data transmitted from the player 1 concerned in step ST24, if the data created like step ST7 of said drawing 8 from the above-mentioned player 1 in step ST23 is received, the address 211, i.e., the control center, which are registered beforehand.

[0063]If the user terminal 50 after performing the above-mentioned data transfer has the data return from waiting and the control center 211 in the return from the control center 211, it will transmit the data from the control center 211 concerned to the player 1 as it is in step ST25.

[0064]If the sign of processing completion is received like step ST13 of said drawing 8 from the above-mentioned player 1 in step ST26, in order to tell a user about processing of the point purchase concerned etc. having been completed, the user terminal 50 concerned, The sign of processing completion is displayed on a display in step ST27, and a user is made to check.

[0065]Then, the user terminal 50 concerned transmits the cryptogram of the sign of the processing completion sent from the above-mentioned player 1 to the control center 211.

[0066]By the above, the flow of the processing in the user terminal 50 in the case of point purchase is completed.

[0067]Next, the flow of the processing in the control center 211 at the time of point purchase is explained using drawing 10.

[0068]In this drawing 10, the control center 211 like step ST31, The data enciphered [above-mentioned] from the player 1 transmitted via the user terminal 50 by the communication function section 133 of the controlling-function block 130 by which the whole is controlled like step ST7 of said drawing 8 and step ST24 of drawing 9 in the control function part 131 is received. When this data is received, the user management functional block 110 of the control center 211, Based on the user ID attached to the received data concerned, a common key comes to hand from the database section 112 under control of the control function part 111 like step ST32, and security ID comes to hand from the security ID generating function part 116.

[0069]The common key at this time is said session key beforehand sent from said player 1, and this session key is enciphered and sent with a public-key crypto system as mentioned above. Therefore, at the time of decoding of this session key enciphered.

In the user management functional block 110 of the control center 211 concerned, the secret key of the public-key crypto system of the above-mentioned control center 211 is taken out, and the session key enciphered [above-mentioned] with this secret key is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerned, decryption of a session key enciphered [above-mentioned] using the public key of the above-mentioned control center 211 is performed. Thus, the obtained session key (common key) is stored in the above-mentioned database section 112.

[0070]If the common key corresponding to the above-mentioned user ID comes to hand from the above-mentioned database section 112 and security ID comes to hand from the security ID generating function part 116, as shown in step ST33, In the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211, Further in [decrypt the data enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common key, and] the control function part 111, Comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned security ID generating function part 116 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed.

[0071]In the control center 211 which checked the justification of the above-mentioned access origin. Like step ST34, by the point generating function part 113 of the user management functional block 110. The point information according to the contents of the data sent from the above-mentioned user terminal 50 is published, and the claim preparations to a user's settlement-of-accounts organization (financial institution 220) are made by the settlement-of-accounts claim function part 117.

[0072]Like step ST35, in the control function part 111, the control center 211 checks that there is no injustice in the balance and point usage information of point information from the player 1, and performs the conclusion of information for next processing. That is, a check and conclusion of whether there is any unjust use are performed from the balance of point information, and the number of the actually used point information. It is better to perform this check and conclusion desirably, although it must not carry out.

[0073]In the user management functional block 110 of the control center 211, like step ST36 after processing of above-mentioned step ST35 again, In the security ID generating function part 115, new security ID to the above-mentioned player 1 (user) is computed based on a random number generation, and above-mentioned security ID is enciphered with the above-mentioned point information in the control function part 110 further, for example. Encryption at this time is also performed using said session key (common key) sent beforehand from said player 1.

[0074]An end of the above-mentioned encryption will transmit the data which enciphered [above-mentioned] to the player 1 via the user terminal 50 under control of the control function part 131 like step ST25 of said drawing 9, and step ST8 of drawing 8 in the communication function section 133 of the controlling-function block 130 of the control center 211.

[0075]Then, in the communication function section 133 of the control center 211, like step ST38, When the processing completion sign from the user terminal 50 shown in step ST28 of said drawing 9 is received and decrypted, in the settlement-of-accounts claim function part 117 of the user management functional block 110 of the control center 211, like step ST39, The financial institution 220 is asked for settlement of accounts based on the processing completion sign concerned. The settlement-of-

accounts claim to this financial institution 220 is performed from the communication function section 132 of the controlling-function block 130.
[0076]By the above, the flow of the processing in the control center 211 in the case of point purchase is completed.
[0077]From drawing 8 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 10, and the control center 211 can be expressed, as shown in drawing 11.
[0078]That is, in this drawing 11, input, such as said password and a point size, is transmitted from the user terminal 50 to the player 1 by the input transmission T1 like step ST2 of said drawing 8, and step ST22 of drawing 9.
[0079]In the prepared data transmission T2, the data created from the player 1 by said player 1 to the user terminal 50 is transmitted like step ST7 of said drawing 8, and step ST23 of drawing 9. In data transfer T3, the data which said player 1 created from the user terminal 50 to the control center 211 is transmitted like step ST24 of said drawing 9, and step ST31 of drawing 10.
[0080]In the data transfer T4, the data enciphered from the control center 211 to the user terminal 50 in the control center 211 is transmitted like step ST37 of said drawing 10, and step ST25 of drawing 9. In the transmission T5, the data from the control center 211 is transmitted to the user terminal 50 by the player 1 as it is like step ST25 of said drawing 9, and step ST8 of drawing 8.
[0081]In the processing completion sign transmission T6, the processing completion sign from the player 1 is transmitted to the user terminal 50 like step ST13 of said drawing 8, and step ST26 of drawing 9. In processing completion sign cryptogram transmission, the processing completion sign enciphered from the player 1 is transmitted to the control center 211 like step ST28 of said drawing 9, and step ST38 of drawing 10.
[0082]Next, it explains from drawing 12 flowing into the processing in the player 1 at the time of acquisition of the digital contents mentioned above, the user terminal 50, and the control center 211 using drawing 15, referring to drawing 2 and drawing 3.
[0083]The flow of the processing in the player 1 at the time of acquisition of digital contents is shown in drawing 12.
[0084]In this drawing 12, it is waiting for the controller 16 until starting of the software for digital contents acquisition beforehand installed in the user terminal 50, i.e., a personal computer, is performed like step ST41.
[0085]If the software for the above-mentioned digital contents acquisition rises, the controller 16 will receive the data which contains digital contents from the control center 211 via the user terminal 50 like step ST42. It has at least the digital contents enciphered with the contents key (a different common key for every contents) as having mentioned above the data received via the terminals 3 and 12 from the user terminal 50 at this time, and the content ID corresponding to the digital contents concerned. therefore, in order to use these enciphered digital contents, a contents key comes to hand from the control center 211 -- if it kicks, it will not become. The method of acquisition of this contents key is mentioned later.
[0086]The controller 16 which received the data from this user terminal 50 stores this data, i.e., the enciphered digital contents, in the memory medium connected to the I/O terminal 4 for memory media via the terminal 11 of the integrated circuit 10. Although various kinds of storages, such as a rewritable optical disc and semiconductor memory, can be considered as this memory medium, the thing in which random access is possible is desirable.

[0087]By the above, the flow of the processing in the player 1 at the time of acquisition of digital contents is completed.
[0088]Next, the flow of the processing in the user terminal 50 at the time of acquisition of digital contents is explained using drawing 13.
[0089]In this drawing 13, the user terminal 50 starts the software for digital contents acquisition in step ST51. If the software concerned rises, in this user terminal 50, the control center 211 of the address beforehand registered in step ST52 according to the software for the above-mentioned digital contents acquisition will be accessed.
[0090]At this time, the control center 211 concerned is exhibiting two or more digital contents using said virtual online shop 230. From the user terminal 50, the digital contents of the request according to the selection operation of the user out of two or more digital contents currently exhibited by this virtual online shop 230 in step ST53 are specified. That is, the user terminal 50 transmits the specification information on the contents for specifying the digital contents of the request in the digital contents exhibited by the virtual online shop 230 like step ST54 to the control center 211.
[0091]If the data which consists of data returned from the control center 211 according to the above-mentioned contents designation information, i.e., said enciphered digital contents, and content ID like step ST55 is received, The user terminal 50 concerned once stores the above-mentioned data in storing means, such as an inside, for example, a hard disk, and a memory, like step ST56.
[0092]Then, the user terminal 50 transmits the stored data (digital contents and content ID which were enciphered) concerned to the player 1 like step ST42 of said drawing 12.
[0093]By the above, the flow of the processing in the user terminal 50 at the time of acquisition of digital contents is completed.
[0094]Next, the flow of the processing in the control center 211 at the time of digital contents acquisition is explained using drawing 14.
[0095]The control center 211 shown in drawing 3 is making the virtual online shop 230 mentioned above exhibit two or more contents here. In the contents managing functional block 100 of control center 211 **, said virtual online shop 230 is generated and, specifically, two or more above-mentioned digital contents are exhibited to this virtual online shop 230.
[0096]Thus, in the state where digital contents are exhibited to the virtual online shop 230, contents designation information is received from the user terminal 50 like step ST61 of drawing 14 step ST54 of said drawing 13.
[0097]If the above-mentioned contents designation information is received from the user terminal 50 concerned, the control function part 101 of the contents managing functional block 100 will send this contents designation information to the controlling-function block 130. The control function part 131 of the controlling-function block 130 lets the communication function section 134 for right holders pass, and transmits the contents designation information received from the above-mentioned control controlling-function block 100 to said content provider 240. Thereby from the content provider 240 concerned, the digital contents demanded in the above-mentioned contents designation information are transmitted. The digital contents which came to hand from the above-mentioned content provider 240 are sent to the contents managing functional block 100 from the controlling-function block 130, and are inputted into this contents code and compression-ized function part 104. At this time, the control function part 101 sends the contents key which is generated in a contents key and the ID generating function part 103, and is stored in the database 102 to above-mentioned contents code and compression-ized function part 104. In this

contents code and compression-ized function part 104, encryption using the above-mentioned contents key is given to the above-mentioned digital contents, and further predetermined compression processing is performed. The control function part 101 adds the content ID taken out from the database 102 to the digital contents by which above encryption and compression processing were carried out, and sends it to the controlling-function block 130. As predetermined compression processing in case digital contents are audio signals, For example, like what is called ATRAC (Adaptive TRansform Acoustic Coding) that is the art currently used in what is called MD (mini disc: trademark) produced commercially in recent years, processing which carries out highly efficient compression of the audio information in consideration of human being's aural characteristic was made into an example -- it can mention.

[0098]Then, as shown in step ST62 of drawing 14, the control section 131 of the controlling-function block 130 transmits the digital contents to which it let the communication function section 133 with a user terminal pass, and it enciphered [above-] and processed [compression-], and content ID was added to the above-mentioned user terminal 50.

[0099]The flow of the processing in the control center 211 at the time of digital contents acquisition is above.

[0100]From drawing 12 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 14, and the control center 211 can be expressed, as shown in drawing 15.

[0101]That is, in this drawing 15, said contents designation information is transmitted from the user terminal 50 to the control center 211 like step ST54 of said drawing 13 by the input transmission T11. In the contents transfer T12, the digital contents and content ID which were enciphered are transmitted to the user terminal 50 like step ST62 of said drawing 14 from the control center 211.

[0102]In the contents transfer T13, the digital contents and content ID which were once stored in the user terminal 50 and which were enciphered [above-mentioned] are transmitted to the player 1 like step ST57 of said drawing 13, and step ST42 of drawing 12.

[0103]Next, it explains from drawing 16 flowing into the processing in the contents key which is needed when using the digital contents mentioned above, the player 1 at the time of acquisition of the service condition and the user terminal 50, and the control center 211 using drawing 19, referring to drawing 2 and drawing 3.

[0104]The flow of the processing in the player 1 at the time of acquisition of a contents key and a service condition is shown in drawing 16.

[0105]In step ST71 of this drawing 16, in the controller 16 of the player 1, it is waiting until starting of the software the contents key beforehand installed in the user terminal 50 and for service-condition acquisition is performed.

[0106]If the above-mentioned contents key of the above-mentioned user terminal 50 and the software for service-condition acquisition rise, the information inputted into the user terminal 50 according to the software concerned will be received like step ST72 via said interface terminal 3 for PC, and the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is information for requiring a contents key required to solve encryption of digital contents to appreciate. In this example, the specification information on the digital contents which use this contents key is used as demand information on the above-mentioned contents key.

[0107]The controller 16 which received this contents designation information from the above-mentioned user terminal 50, ID of the digital contents specified in the contents designation information concerned and security ID from the security ID generating circuit 19 are created, and this created data is made to encipher by the common code decoder circuit 24 in step ST73. The controller 16 adds the user ID read from the user ID storing memory 23 to the created data concerned, and transmits it to the user terminal 50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50, the above-mentioned prepared data will be sent to the control center 211.
[0108]Since the common key encryption system is adopted also as encryption of the prepared data at this time as mentioned above, in advance of transmission of the prepared data concerned, generation of a common key is performed to it. For this reason, in the above-mentioned controller 16, a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation means, for example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto system, in the above-mentioned controller 16. The public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken out, and it sends to the above-mentioned open code decoder circuit 20 at the same time it sends the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concerned, encryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus, the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data.
[0109]Then, the controller 16 receives the enciphered data which has been sent from the control center 211 via the user terminal 50 in step ST75 so that it may mention later. The above-mentioned contents key, a service condition, security ID, etc. are enciphered as mentioning later the data sent from the control center 211 at this time.
[0110]If the data enciphered from the above-mentioned control center 211 is received, in the player 1, the data enciphered [above-mentioned] will be decrypted like step ST76, and the justification of the data will be checked. That is, the controller 16 evaluates the justification by checking security ID of the data decrypted [above-mentioned] by comparison with security ID from the above-mentioned security ID generating circuit 19.
[0111]Here, encryption is made with a public-key crypto system so that a contents key may be mentioned later, and about a service condition and security ID, encryption is made with the common key encryption system. Therefore, in order to decrypt the contents key concerned enciphered, The secret key of a public-key crypto system is required, and since the player inherent key is used as a secret key as mentioned above in the player 1 of this embodiment, the player inherent key concerned is taken out from the key storage memory 21 for communication. This player inherent key is sent to the open code decoder circuit 20 with the contents key enciphered [above-mentioned]. In this open code decoder circuit 20, the contents key enciphered [above-mentioned] is decrypted using the above-mentioned player inherent key. The contents key decrypted in this way is kept by the common key storage memory 22. On the other hand, in decrypting the service condition and security ID which are enciphered with the above-mentioned common key encryption system, These data is sent to the above-mentioned common code decoder circuit 24, and said common key

which was generated previously and kept in the common key storage memory 22 is read, and, similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, the above-mentioned service condition and security ID are decrypted using the above-mentioned common key. The service condition decrypted in this way is stored in the point usage information storing memory 29. It is important here that the decrypted contents key and the service condition concerned are not taken out from the exterior of the player 1 concerned, the controller 16 specifically formed in the integrated circuit 10 of drawing 2 or the common key storage memory 22, and the point usage information storing memory 29 outside.

[0112]The controller 16 makes the contents key which decoded [above-mentioned] store in the above-mentioned common key storage memory 22 with the above-mentioned content ID like step ST77 after the check of the above-mentioned justification.

[0113]Then, the controller 16 creates the message which shows that the above-mentioned contents key came to hand in step ST78, This message is sent to the common key encryptosystem decoder circuit 24 like the above-mentioned, and said common key which was generated beforehand and kept in the common key storage memory 22 is read, and, similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, a message is enciphered using the above-mentioned common key.

[0114]After encryption of the message concerned is completed, the controller 16 transmits this enciphered message to the user terminal 50 via the terminals 12 and 3 like step ST79. This enciphered message is made to transmit to the control center 211 after that.

[0115]By the above, the flow of the processing in the player 1 at the time of a contents key and service-condition acquisition is completed.

[0116]Next, the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is explained using drawing 17.

[0117]In this drawing 17, the user terminal 50 starts the software for a contents key and service-condition acquisition in step ST81. If the designation input demand of the contents of hope is performed and specification of contents is made from a user to the user who will operate the user terminal 50 concerned in step ST82 with this user terminal 50 according to the above-mentioned software if the software concerned rises, that specification information will be generated. The user terminal 50 transmits the specification information on the above-mentioned contents to the player 1 in the above-mentioned step ST83.

[0118]Next, if the data created and transmitted by the above-mentioned player 1 like step ST74 of said drawing 16 in step ST84 is received, the user terminal 50, The data transmitted from the player 1 concerned in step ST85 is transmitted to the control center 211 where the address is registered beforehand.

[0119]The user terminal 50 after performing a data transfer to the above-mentioned control center 211, If there is return of the data in which the contents key and service condition specified by the above-mentioned content ID from the control center 211 in waiting and step ST86, security ID, etc. were enciphered, the return from the control center 211, The data from the control center 211 concerned is transmitted to the player 1 as it is in step ST87.

[0120]The user terminal 50 after performing a data transfer to the above-mentioned player 1, The return from the player 1 in waiting and step ST88 like step ST79 of said drawing 16 from the player 1, If there is return of the message as which it was

enciphered that the above-mentioned contents key came to hand, it will indicate that the above-mentioned contents key acquisition was completed to the display device connected to the user terminal 50 concerned in step ST89, and a user will be told.
[0121]Then, the message which was returned from the above-mentioned player 1 and which was enciphered [above-mentioned] is sent to the control center 211 in step ST90.
[0122]By the above, the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is completed.
[0123]Next, the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is explained using drawing 18.
[0124]In this drawing 18, the communication function section 133 with the user terminal of the control center 211, The encryption data of the content ID transmitted to the user terminal 50 from the player 1 via ** in step ST91 like step ST74 of said drawing 16 and step ST85 of drawing 17, user ID, a message, and security ID is received. This received data is sent to the user management functional block 110.
[0125]The control function part 111 of the user management functional block 110 concerned, Based on the user ID added to the encryption data which received [above-mentioned], the common key for solving the encryption concerned is taken out from the database section 112, and the above-mentioned encryption data is decoded using this common key in a correspondence code and the function decoding part 114. The control function part 111 checks the justification of the data which was received [above-mentioned] and decrypted using the user ID and security ID from the security ID generating function part 116 which were read from the database section 112.
[0126]The common key at this time is said session key beforehand sent from said player 1, and this session key is enciphered and sent with a public-key crypto system as mentioned above. Therefore, at the time of decoding of this session key enciphered. Like the above-mentioned, in the control center 211 concerned, the secret key of the public-key crypto system of the above-mentioned control center 211 is taken out, and the session key enciphered [above-mentioned] is decrypted using a secret key in a correspondence code / the function decoding part 114 concerned. Thus, the obtained session key (common key) is stored in the above-mentioned database section 112.
[0127]When the justification of the data which received [above-mentioned] is checked, the control function part 111, The contents key and service condition which were specified in the above-mentioned content ID to the contents managing functional block 100 are required, The control function part 101 of the contents managing functional block 100 which received the demand concerned reads the contents key and service condition which were specified in the above-mentioned content ID from the database section 102, and transmits them to the user management functional block 110. The control function part 111 sends these contents keys and a service condition to a correspondence code / function decoding part 114 with security ID, as shown in step ST93.
[0128]Here, encryption is made with the public-key crypto system mentioned above about the contents key, and encryption is made with the common key encryption system mentioned above about a service condition and security ID. Therefore, when enciphering the contents key concerned, the public key (public key beforehand stored corresponding to the player 1) of user side 200 is taken out from said database section 112 based on the above-mentioned user ID, and it is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerned, the above-mentioned contents key is enciphered using the above-mentioned public key. On the other hand, when enciphering the above-mentioned

service condition and security ID, the common key (session key) specified by the above-mentioned user ID is taken out from the above-mentioned database section 112, and it is sent to a correspondence code / function decoding part 114. In the correspondence code / function decoding part 114 at this time, the above-mentioned service condition and security ID are enciphered using the above-mentioned common key.

[0129]The contents key, the service condition, and security ID which were enciphered [above-mentioned] are sent to the controlling-function block 130, and are transmitted to the user terminal 50 from the communication function section 133 with a user terminal like step ST94. The data transmitted to this user terminal 50 will be sent to the player 1 via the user terminal 50 like step ST87 of said drawing 17, and step ST75 of drawing 16.

[0130]Reception of the encryption message which the control center 211 was generated by the player 1 like step ST79 of said drawing 16, and step ST90 of drawing 17, and was transmitted via the user terminal 50 Then, waiting, When the above-mentioned communication function section 133 receives the encryption message which the above-mentioned player 1 generated like step ST95, the control center 211 concerned, Like step ST96, the encryption message concerned is decrypted with a common key, and it checks that the above-mentioned player 1 has obtained the contents key and the service condition from the decoding message.

[0131]By the above, the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is completed.

[0132]From drawing 16 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 18, and the control center 211 can be expressed, as shown in drawing 19.

[0133]That is, in this drawing 19, said contents designation information is transmitted from the user terminal 50 to the player 1 like step ST83 of said drawing 17 by the contents-designation-information transmission T21. In the prepared data transmission T22, the data created by the player 1 is transmitted to the user terminal 50 like above step ST74. In the prepared data transmission T23, the data created by the above-mentioned player 1 from the user terminal 50 concerned is transmitted to the control center 211. In the enciphered data sending T24, the data enciphered in the control center 211 is sent to the user terminal 50 like step ST94 of said drawing 18, and the enciphered data concerned is further sent to the player 1 by the enciphered data sending T25.

[0134]In the message transfer T26, like step ST79 of said drawing 16, In the data sending T27 as which the data which enciphered the message which shows the completion of contents key acquisition was transmitted to the user terminal 50 from the player 1, and was enciphered further, the message enciphered from the above-mentioned player 1 is sent to the control center 211 from the user terminal 50.

[0135]Next, in the player 1 which received point information, digital contents, and a contents key as mentioned above, it explains flowing into the processing at the time of actually appreciating digital contents using the user terminal 50 using drawing 20, referring to drawing 2.

[0136]Here, it is assumed that the memory medium said digital contents were remembered to be is connected to the terminal 4 of the player 1.

[0137]In this state, the digital contents which wish to appreciate from the user terminal 50 are specified to the player 1 concerned like step ST101. At this time, the

specification concerned is made, when a user operates the user terminal 50, for example.
[0138]Like step ST102, according to the contents designation information from the above-mentioned user terminal 50, the controller 16 of the player 1 performs access to the above-mentioned memory medium, and reads ID of contents at this time.
[0139]Based on the content ID read in the above-mentioned memory medium, the above-mentioned controller 16 like step ST103, It accesses to said common key storage memory 22, and it checks whether the contents key is stored, and accesses to said point usage information storing memory 29, and it is checked whether the service condition is stored.
[0140]When it checks here that the above-mentioned contents key and the service condition are not stored in the above-mentioned common key storage memory 22 or the point usage information storing memory 29, the controller 16, The information on the purport that the contents key concerned etc. do not exist to the user terminal 50 is sent, and this displays the message which stimulates acquisition of the above-mentioned contents key etc. on said display device from the user terminal 50. In this case, it carries out like the flow chart for contents key acquisition mentioned above, and a contents key etc. come to hand. Thus, when a contents key etc. newly come to hand, as mentioned above in step ST104, the contents key which are enciphered is decrypted.
[0141]Next, the controller 16 checks whether there is any enough balance of the point information stored in the point information storing memory 28 based on the service condition decrypted [above-mentioned], as shown in step ST105. When the balance of the above-mentioned point information stored in the above-mentioned point information storing memory 28 is insufficient, The information on the purport that the balance of the point information concerned is insufficient is sent from the controller 16 to the user terminal 50, and, thereby, the user terminal 50 displays the message which stimulates acquisition of the above-mentioned point information on said display device. In this case, it carries out like a flow chart for point access to information which was mentioned above, and point information comes to hand.
[0142]When actually appreciating digital contents, here the controller 16, According to the digital contents concerned to appreciate, a point information number is reduced from the above-mentioned point information storing memory 28 like step ST106, Furthermore, the new point usage information according to the condition of use of the point information concerned is stored in the point usage information storing memory 29 (point usage information is updated). Thus, as point usage information newly stored to the point usage information storing memory 29, they are the right holder information corresponding to the digital contents which appreciated [above-mentioned], including owner of a copyright etc., information, other information on the reduced point information number, etc.
[0143]Then, the controller 16 will read digital contents from a memory medium, if it checks that the processing for fee collection of the cut of these point information, new storing of point usage information, etc. has been completed like step ST107.
[0144]Since the digital contents read from this memory medium are enciphered, the controller 16 transmits the digital contents enciphered [above-mentioned] to the common code decoder circuit 24 like step ST109.
[0145]In this common code decoder circuit 24, the digital contents enciphered [above-mentioned] are decrypted like step ST110 using the contents key which decrypts previously and is kept by the common key storage memory 22 based on the directions from the controller 16.

[0146]Since predetermined compression processing is made as mentioned above, these digital contents the controller 16, The digital contents by which the above-mentioned code was decrypted and by which compression processing is carried out [above-mentioned] are made to transmit to the expansion circuit 26 from the above-mentioned common code decoder circuit 24 like step ST111, and the elongation processing corresponding to the above-mentioned predetermined compression processing is made to perform here.
[0147]Then, the elongated digital contents concerned, Like step ST112, it is changed into an analog signal in the D/A conversion circuit 27, and is outputted outside (for example, user terminal 50 grade) like step ST113 via the terminal 13 of the integrated circuit 10, and the analog output terminal 2 of the player 1 concerned.
[0148]By the above, the flow of the processing in the player 1 at the time of contents appreciation is completed, and the appreciation of digital contents of a user is attained.
[0149]Next, the point usage information newly stored in the point usage information storing media 29 of said player 1 with appreciation of digital contents which were mentioned above, It explains flowing into the processing in the player 1 at the time of returning to the control center 211, the user terminal 50, and the pipe center 310 using drawing 24 from drawing 21, referring to drawing 2 and drawing 3.
[0150]The flow of the processing in the player 1 at the time of point usage information return is shown in drawing 21.
[0151]In this drawing 21, it waits for the controller 16 until starting of the software for point usage information return beforehand installed in the user terminal 50 is performed, as shown in step ST121.
[0152]If the software for the above-mentioned point usage information return of the above-mentioned user terminal 50 rises, the information inputted into the user terminal 50 according to the software concerned will be received like step ST122 via said interface terminal 3 for PC, and the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is a password etc. which are entered by the user.
[0153]The controller 16 which received this contents designation information from the above-mentioned user terminal 50, The password supplied from the user terminal 50 concerned in step ST123 is compared with the password stored in the password storing memory 14, and the password concerned carries out the right check of how.
[0154]When it is checked that it is a right password in the check of the above-mentioned password, the controller 16, The balance of the point information stored in the point information storing memory 28 and the point usage information stored in the point usage information storing memory 29 are read like step ST124, respectively, and these information is enciphered.
[0155]After the balance of the above-mentioned point information and encryption of point usage information are completed, the controller 16 is attached to the data which read user ID from the user ID storing memory 23, and enciphered [above-mentioned] like step ST125.
[0156]The data in which this user ID was attached is transmitted to the user terminal 50 via the terminal 12 and the interface terminal 3 for PC like step ST126 from the controller 16. This data is transmitted to the control center 211 after that.
[0157]As mentioned above also in the encryption at this time, the common key encryption system is adopted. That is, in advance of transmission of the data concerned, generation of a common key is performed like the above-mentioned, it is enciphered with said public-key crypto system (encryption using the public key of the

control center 211), and this generated common key is sent to the control center 211 with user ID.
[0158]After transmitting data to the user terminal 50 as mentioned above, the controller 16 waits to transmit the data later mentioned from the above-mentioned control center 211 via the user terminal 50.
[0159]When the data from the above-mentioned control center 211 is received like step ST127, here in the player 1. The received data enciphered using the common key encryption system are decrypted like step ST127 using a common key like the above-mentioned, and the justification of the data is checked. That is, the controller 16 evaluates the justification by checking security ID of the data decrypted [above-mentioned] by comparison with security ID from the above-mentioned security ID generating circuit 19.
[0160]The message of the processing completion enciphered using the above-mentioned common key is also contained in the data transmitted from the above-mentioned control center 211. Therefore, the controller 16 after the check of above-mentioned security ID is completed, Send the processing completion message enciphered [above-mentioned] to the common code decoder circuit 24, the decryption using a common key is made to perform here, and it is checked that processing in the above-mentioned control center 211 has been completed by receiving this decrypted processing completion message.
[0161]By the above, the flow of the processing in the player 1 at the time of point usage information return is completed.
[0162]Next, the flow of the processing in the user terminal 50 at the time of point usage information return is explained using drawing 22.
[0163]In this drawing 22, the user terminal 50 starts the software for point usage information return in step ST131. When the software concerned rises, in this user terminal 50. If input requests, such as a password, are performed and the input of a password is made from a user to the user who operates the user terminal 50 concerned in step ST132 according to the above-mentioned software, the password will be transmitted to the player 1.
[0164]Next, if the data created and transmitted by the above-mentioned player 1 like step ST126 of said drawing 21 in step ST133 is received, the user terminal 50, The data transmitted from the player 1 concerned in step ST134 is transmitted to the control center 211 where the address is registered beforehand.
[0165]The user terminal 50 after performing a data transfer to the above-mentioned control center 211 will transmit the data concerned to the player 1 as it is, if the data in which the return from the control center 211 is sent from the control center 211 to the player 1 in waiting and step ST135 is received.
[0166]The user terminal 50 after performing a data transfer to the above-mentioned player 1 performs the display for making a user know that processing was completed to a display device, and receives the check from a user.
[0167]By the above, the flow of the processing in the user terminal 50 at the time of point usage information return is completed.
[0168]Next, the flow of the processing in the control center 211 at the time of point usage information return is explained using drawing 23.
[0169]In the communication function section 133 with the user terminal of the control center 211, the data of the point usage information etc. which have been transmitted by step ST126 of said drawing 21 and step ST134 of drawing 22 from the player 1 via said user terminal 50 is received like step ST141.

[0170]When this data is received, the user management functional block 110 of the control center 211, The common key which is beforehand received from the database section 112 like the above-mentioned, and is stored under control of the control function part 111 like step ST142 based on the user ID attached to the received data concerned comes to hand, and security ID comes to hand.
[0171]If the common key and security ID corresponding to the above-mentioned user ID come to hand from the above-mentioned database section 112, as shown in step ST143, In the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211, Further in [decrypt the data of the point usage information etc. which were enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common key, and] the control function part 111, Comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned database section 112 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed.
[0172]The data after the check of the above-mentioned justification and the contents is transmitted to the usage information controlling-function block 120. The control function part 121 of this usage information controlling-function block 120, As shown in step ST144, it is checked whether there is any injustice in use of above-mentioned user side 200 using the information stored in the database section 122 using the balance and point usage information of point information which have been sent from the above-mentioned player 1. Simultaneously, when [concerned / unjust] it comes and things are checked, the operation which summarizes the balance and point usage information of point information in the usage information calculation function part 123 is performed.
[0173]Then, the control function part 111 of the user management functional block 110 controls the security ID generating function part 116, makes security ID compute, controls the confirmation message generating function part 115 further, and makes the message of processing completion generate, as shown in step ST145. These security ID and a processing completion message are enciphered using said common key in the correspondence code / function decoding part 114 of the user management functional block 110.
[0174]The data which was enciphered [above-mentioned] and generated will be sent to the user terminal 50 from the communication function section 133 with a user terminal, as shown in step ST146, and it will be transmitted to the player 1 from the user terminal 50 concerned like step ST135 of said drawing 22, and step ST127 of drawing 21.
[0175]By the above, the flow of the processing in the control center 211 at the time of point usage information return is completed.
[0176]From drawing 21 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 23, and the control center 211 can be expressed, as shown in drawing 24.
[0177]That is, in this drawing 24, the input of said password is transmitted from the user terminal 50 to the player 1 like step ST132 of said drawing 22 by the input transmission T31. In the prepared data transmission T32, the data which the player 1 created is transmitted to the user terminal 50 like step ST126 of said drawing 21. In the prepared data transmission T33, the data created by the above-mentioned player 1 is transmitted to the control center 211 from the above-mentioned user terminal 50 like step ST134 of said drawing 22. In the data transfer T34, the data created in the

control center 211 is transmitted to the user terminal 50 like step ST146 of said drawing 23. In the data transfer T35, the data created in the control center 211 is transmitted to the player 1 via the user terminal 50 like step ST127 of said drawing 21.

[0178]Actual operation of the player 1 of the system of this embodiment, the user terminal 50, and the control center 211 serves as a flow which was mentioned above.

[0179]So far, although the flow of processing of the whole in the system of this embodiment has been explained, operation of each of the principal part of the system of this embodiment is explained in detail after this.

[0180]First, explanation about operation of the encryption and compression in this invention embodiment, and extension and decryption is given.

[0181]Like the system of an embodiment mentioned above, when distributing digital contents using a network, in order to stop the data volume, compression/extension art is used, and encryption/compression technology is used for anti-copying or fee collection. That is, compressing digital contents and carrying out encryption processing further by the distribution side (an above-mentioned example the control center 211 side), is performed. When distributing the digital contents (encryption/compressed data) generated at the transmitting side (control center 211 side) like an above-mentioned example using a network, In a receiver (an above-mentioned example player 1), decrypting, after receiving the digital contents which were above-enciphered and were compressed, elongating further, and restoring digital contents is performed. The turn of processing of the above-mentioned encryption, compression and decryption, and extension may interchange.

[0182]When copyright etc. exist in the above-mentioned digital contents, when the above-mentioned receiver elongates the above-mentioned digital contents with the above-mentioned decryption, it will be charged according to intention of the above-mentioned owner of a copyright etc. Although this fee collection is performed by mainly purchasing, the key, i.e., the contents key, of decryption, it is in the method of purchasing this contents key variously.

[0183]Here, as mentioned above, when procedure which compresses digital contents, is enciphered, is decrypted and is elongated is followed, the user who had bad faith, for example can obtain comparatively easily the compressed data decrypted [above-mentioned]. Namely, the compressed data of digital contents, Generally capacity is large, therefore For example, since not an internal memory but the ** value of a common contents playback device of a receiver are accumulated in external memory in many cases, It is because it is easy to take out unjustly the digital contents compressed [above-mentioned] by the connection section with direct or external memory from this external memory.

[0184]What cannot be processed if the algorithm of the expansion system to compression is hidden like the key of a code general to the algorithm of an expansion system, respectively being opened to the public in many cases does not exist. And as compared with the digital contents by which the encryption distributed from the above-mentioned transmitting side and compression were made, **** which distributes the compression digital contents which did not change in data volume, therefore were decrypted [above-mentioned] with bad faith is also easy for the compression digital contents decrypted [above-mentioned]. Namely, according to the method which is enciphered and distributes digital contents after compressing [above-mentioned]. The danger that the compression digital contents which can elongate anyone easily will be distributed further in the place which a theft is easily

carried out to a user with bad faith, and intention of an owner of a copyright etc. does not reach for this reason, or will be elongated is large.
[0185]So, in the embodiment of the invention, in order to make it possible to raise the safety of the digital contents distributed using a network in view of such a situation, in the player 1 of above-mentioned drawing 2, processing as shown in the flow chart of the following drawing 25 is performed.
[0186]Namely, in the decoding processing in the common code decoder circuit 24 of the player 1 of drawing 2, and the elongation processing in the above-mentioned expansion circuit 26. The data of the digital contents by which compression processing was carried out with the encryption read from said memory medium like step ST151, First, it divides into the unit of the least common multiple lcm (X, Y) of the batch X bit of the algorithm of decoding processing, and the algorithm batch Y bit of elongation processing.
[0187]Next, as the data of digital contents in which the above-mentioned encryption divided into the unit of the above-mentioned least common multiple lcm (X, Y) and compression processing are made is shown in step ST152, decoding processing is performed by the above-mentioned common code decoder circuit 24 for every unit of the least common multiple lcm (X, Y) concerned.
[0188]As the data of digital contents in which the unit of the least common multiple lcm (X, Y) obtained by the decoding processing concerned is compressed is shown in step ST154, elongation processing is performed to all the compressed data for the unit concerned in the above-mentioned expansion circuit 26.
[0189]Then, the decryption and elongation processing for every unit of this least common multiple lcm (X, Y) are continued until the processing about all the data of digital contents by which compression processing was carried out with the above-mentioned encryption is completed. . Namely, judgment whether the decryption and elongation processing for every unit of the least common multiple lcm (X, Y) were completed to all the data of digital contents should do to be shown in step ST155. When not having completed and it returned and completes to step ST152, the flow chart of the processing concerned is completed.
[0190]The digital contents by which all the data was decrypted and elongated by this will be obtained.
[0191]Although the decoding data of the above-mentioned least-common-multiple lcm (X, Y) unit will exist, the data volume of the decoding data concerned also has little processing of the flow chart of drawing 25 in the player 1 concerned. For this reason, a possibility of being stolen like [in the case of saving at external memory which can be saved at an internal memory with high safety even if comparatively expensive, therefore was mentioned above] will become very low.
[0192]In the above-mentioned player 1 in this embodiment, the buffer memory 25 of drawing 2 is formed as an internal memory for securing the above-mentioned safety between the above-mentioned common code decoder circuit 24 and the expansion circuit 26. That is, this buffer memory 25 is formed in the integrated circuit 10 of one chip, and it is hard to be accessed from the outside, therefore data is not taken out outside.
[0193]In an above-mentioned flow chart, are made to perform decryption and elongation processing to all the data for the unit of the least common multiple lcm (X, Y), and as specific constitution for it, For example, the data of digital contents is first divided into the batch X bit of the algorithm of decoding processing like composition of being shown in drawing 26, By performing decoding processing to the data of this X bit, gathering the data in which the X bit concerned by which decoding processing

was carried out is compressed after that by the algorithm batch Y bit of elongation processing, and elongating the compressed data of the Y bit concerned. It is made to realize the decryption and elongation processing in the unit of the least common multiple lcm (X, Y) as mentioned above.
[0194]The common code decoder circuit 24 of the player 1 which realizes this consists of the input part 30 and the code decoding part 31, and the above-mentioned expansion circuit 26 consists of the expanding part 32 and the outputting part 33. Said buffer memory 25 is formed between these common code decoder circuit 24 and the expansion circuit 26.
[0195]If encryption processing to the above-mentioned digital contents is performed as a more concrete example here for example, using the DES (Data Encription Standard) code, The encryption processing concerned and decoding processing corresponding to it will be performed by 64 bitwises.
[0196]In the case of the elongation processing to the compressed digital contents, it changes also with the compression ratios and sampling frequencies, but under the present circumstances, it is processed per 1K - 2 K bits/channel in many cases. Here, it is assumed that it is processed for every 1.28K bit for convenience.
[0197]Therefore, in the case of the system using the above-mentioned DES cipher system and the compression expansion system for every above-mentioned 1.28K bit, the above-mentioned least common multiple lcm is set to 1.28K.
[0198]Said digital contents enciphered and compressed are inputted into the input part 30 of the basis of such conditions, and the common code decoder circuit 24 of drawing 26. In the input part 31 concerned, the digital contents which were enciphered [above-mentioned] and compressed are divided into [every batch X bit of the algorithm of the above-mentioned decoding processing], i.e., 64 bits, data, and are outputted to the code decoding part 31.
[0199]In this code decoding part 32, decoding processing of the above-mentioned X bit, i.e., 64 bits, data is carried out concerned every 64 bits. The 64 bits [which was obtained by the decryption in this every 64 bits] data compressed is sent to the buffer memory 25.
[0200]When the compressed data for the algorithm batch Y bit of elongation processing, i.e., a 1.28K bit, accumulates according to the directions from said controller 16, the buffer memory 25 concerned, The compressed data for the 1.28K bit concerned is outputted collectively, and this compressed data is sent to the expanding part 32 of the above-mentioned expansion circuit 26.
[0201]The above-mentioned expanding part 26 elongates the compressed data for the 1.28K bit inputted [above-mentioned], and outputs it to the outputting part 33.
[0202]The controller 16 controls processing of the decoding section 31, and processing of the expanding part 32, monitoring the data volume which accumulated in the buffer memory 25.
[0203]If 20 pieces (= 1280/64) are parallel in decoding processing if it is this case, and it processes, it will become a more nearly high-speed processing system.
[0204]In addition, when performing not hardware constitutions like said drawing 2 or drawing 26 but processing mentioned above with the programmable device, the controller 16 will process based on a decoded program or an extension program, corresponding to the situation of the buffer memory 25.
[0205]Although the digital contents enciphered after compressing were supplied to the player 1 and the example elongated after decrypting these digital contents compressed and enciphered was given by the player 1 by above-mentioned

explanation, Even if it is a case where the compressed digital contents are elongated and decrypted after enciphering, the same effect as **** can be acquired.
[0206]The algorithm of compression / extension, and encryption/decryption is not limited, and this invention is effective to any methods.
[0207]Thus, according to this invention, the safety of the digital contents distributed using a network improves.
[0208]Next, explanation about generating operation of said security ID is given.
[0209]As point information comes to hand beforehand and being mentioned above like this embodiment in the case of a method which reduces the point information concerned according to appreciation of digital contents, After the control center 211 on a network performs checks as arbitrary after receiving communication of a purchase request of the point information from the user terminal 50 of user side 200 as financial institution 220 and others, it enciphers the point information and sends it to the player 1 of user side 200 via a network.
[0210]In the case of a method which obtains point information beforehand and reduces the point information concerned like this embodiment according to appreciation of digital contents, between the control center 211 and the player 1 (user terminal 50), an exchange of the data same each time as the degree of the purchase of point information -- carrying out (for example, the information of "the point information on 3000 cyclotomies" corresponding to "3000 supplement demand of the point information on a cyclotomy" and it which were enciphered is exchanged) -- it is based on those who have bad faith, for example. The amount-of-money supplement depended for what is called "impersonating" to the financial institution 220 serves as a problem. "Impersonating" to the financial institution which says here means what a person with the above-mentioned bad faith impersonates an original user (this embodiment user side 200), and obtains point information unjustly.
[0211]Namely, if the data same each time as the degree of the purchase of point information is exchanged, For example, a person with bad faith robs a communication line of the data concerned, and the same data is generated, In the case as the destination is made into itself (person with bad faith) to the control center 211 and acquisition of point information was requested. A person with the bad faith concerned can obtain point information, and the claim of the purchase price of this point information has further a possibility that the problem that it will be made by original user side 200 may occur.
[0212]Then, in order to prevent such injustice, in the system of this invention embodiment, the random number generated by the random number generation function which has interlocked beforehand by both a receiver (player 1 side) and the distribution side (control center 211 side) is used for the improvement in safety. According to this embodiment, said security ID is generated as the above-mentioned random number. What is necessary is to initialize the timer 18, for example and just to synchronize operation between both, for example in the cases, such as a user's registration procedure, in order to interlock a random number generation among both.
[0213]That is, the operation at the time of the player 1, for example, point access to information, from the control center 211 at the time of using this random number (security ID) serves as the following flows.
[0214]The data sent from the control center 211 to the player 1 is made with the data which consists of security ID generated [above-mentioned] with the point information enciphered using the common key (session key) which came to hand beforehand from the player 1 as mentioned above at the time of the purchase of point information.

[0215]The controller 16 of the player 1 is sent to the common code decoder circuit 24, as the data received from the control center 211 concerned was mentioned above, and it performs decoding processing here using said common key. By this, the point information and security ID which have been sent from the control center 211 will be obtained.
[0216]Then, the controller 16 of the player 1 compares security ID sent from the above-mentioned control center 211 with security ID generated in the own security ID generating circuit 19. In this comparison, the controller 16 stores in said point information storing memory 28 the point information sent from the above-mentioned control center 211, only when security ID from the control center 211 and security ID which the above itself generated are in agreement.
[0217]By this, only the player 1 of valid-user side 200 can obtain point information. the malicious person who in other words has the player 1 of valid-user side 200, and the same player -- said -- impersonating, even if it is going to obtain point information unjustly, Since security ID of the player which the person of the bad faith concerned has, and security ID sent from the above-mentioned control center 211 are not in agreement, the person with this bad faith will not get said inaccurate point access to information depended for impersonating.
[0218]Of course, security ID generated in the player 1 of user side 200, The security ID generating circuit 19 provided in the integrated circuit 10 of the player 1 concerned occurs, and since it is what cannot be taken out outside, a person with bad faith cannot steal the security ID concerned.
[0219]Although some are various in the composition which generates the random number as above-mentioned security ID, the example is shown in drawing 27. The composition of this drawing 27 is one example of the security ID generating circuit 19 of said drawing 2.
[0220]In this drawing 27, the one-way function generating part 40 generates what is called a one-way nature function. The inverse function is far difficult for calculation with a function with the above-mentioned one-way nature function comparatively easy to calculate. It receives by secret communication etc. beforehand and this one-way function can also be saved at the one-way function generating part 40 concerned. The one-way function generating part 40 can also be made to generate the above-mentioned one-way function by making into an input function the hour entry from the timer 18 established in the integrated circuit 10 of said drawing 2. The above-mentioned one-way function is sent to the random number deciding part 43.
[0221]The number generating part 41 of users generates the predetermined number of users defined for every user. This number of users is beforehand sent by secret communication etc., and is saved at the number generating part 41 of users concerned. The user ID which said user ID storing memory 23 stores, for example can also be used for this number of users.
[0222]The random number database 42 stores a random number, and stores 99 random numbers.
[0223]The time communication storage parts store 44 memorizes the time communication information sent, for example from the controller 16. This time communication information is information which shows the time communication between the player 1 and the control center 211.
[0224]These one-way functions, the number of users, and time communication information are sent to the random number deciding part 43. The random number deciding part 43 concerned generates the random number of the range beforehand memorized by the random number database section 42 from the above-mentioned

one-way function and the number of users, for example based on the hour entry from said timer 18 (for example, 99 pieces).
[0225]Namely, if the above-mentioned time communication information is the communication which is the 1st time in this random number deciding part 43, The 99th random number is taken out from the above-mentioned random number database section 42, and if for example, time communication information is the communication which is the n-th time, the 100-n-th random numbers will be picked out from the above-mentioned random number database 42, and this taken-out random number is outputted as said security ID.
[0226]The composition of this security ID generating has the same thing in the player 1 and the control center 211.
[0227]When finishing using all the random numbers stored in the random number database section 42, In the above-mentioned random number deciding part 42, 100 pieces - the 199th random number are calculated, or secret communication of a new random number and unidirectional function is carried out, and it re-stores in the random number database section 42, or, on the other hand, reconstructs to the tropism function generation part 40.
[0228]Although a random number (security ID) is generated and he is trying to improve the safety for every communication in the explanation mentioned above, According to this embodiment, since he is also trying to generate programmably a common key (session key) different each time whenever it communicates between user side 200 and the control center 211 side as mentioned above, safety is improved further.
[0229]Here, the above-mentioned random number is inserted about the transmission sentences (for example, message etc.) actually transmitted, and signs that encryption by a session key is made, and signs that a random number is taken out from a receiving sentence and the check of justification is made are explained using drawing 28 and drawing 29. He is also trying to add a signature (digital signature) to a transmission sentence in the example of these drawing 28 and drawing 29.
[0230]In this drawing 28, first, as a flow which enciphers said common key with a public-key crypto system, and transmits, it generates as a common key which uses said session key for communication, and this common key is enciphered by the public key of a receiver to the public-key-encryption chemically-modified degree P8 by the common key generating process P7 for communication. This enciphered common key is sent to a receiver.
[0231]On the other hand, as a flow in the case of enciphering the message as a transmission sentence with a common key encryption system, and transmitting, in the message generation distance P1, the message M is generated and a random number (said security ID) is generated at the random number generation process P5, for example. These messages M and a random number are sent to the common key encryptosystem chemically-modified degree P6. In the common key encryptosystem chemically-modified [this] degree P6, the above-mentioned message M and a random number are enciphered using the common key by which it was generated at the above-mentioned common key generating process P7 for communication.
[0232]When adding the above-mentioned digital signature, the above-mentioned message M is sent to the hash value calculation process P2. In the hash value calculation process P2 concerned, what is called a hash value is calculated from the above-mentioned message M. A hash value is address information called for by a hash method, and a hash method performs a predetermined operation to some contents (keyword) of data (in this case, the message M), and uses that result for it as

an address. The hash value (M) generated from this message is sent to the secret key cryptosystem chemically-modified degree P4 as a digital signature. In the secret key cryptosystem chemically-modified [this] degree P4, the above-mentioned digital signature is enciphered with the secret key of the transmitting side. This enciphered digital signature is sent to the common key encryptosystem chemically-modified degree P6. This enciphers the above-mentioned digital signature in the common key encryptosystem chemically-modified degree P6 using the common key by which it was generated at the above-mentioned common key generating process P7 for communication.

[0233]These messages M, a digital signature, and a random number are transmitted to a receiver.

[0234]Next, the flow of processing by the receiver corresponding to drawing 28 is explained using drawing 29.

[0235]In this drawing 29, the common key transmitted from the above-mentioned transmitting side is first decrypted with the secret key of the receiver concerned at the secret key decryption process P11 as a flow which decrypts said common key with a public-key crypto system.

[0236]At the common key decoding process 13, the message M transmitted [above-mentioned] is decrypted using the common key decrypted at the above-mentioned secret key decryption process P11 as a flow which, on the other hand, decrypts the message M enciphered with said common key encryption system. This decrypted message M will be sent to other processes by the other functional transmission processes P20.

[0237]The hash value which decodes a digital signature and which flowed and was decrypted at the above-mentioned common key decryption process P13 is decrypted using the public key of the transmitting side at the public key decryption process P14. Simultaneously, in the hash value calculation process P17, a hash value is calculated from the above-mentioned message M. The check of the hash value decrypted by these public key decryption process P14 and the hash value calculated by the above-mentioned hash value calculation process P17 being compared, and not being altered by the comparison process P19, is performed.

[0238]About the transmitted random number, the random number decrypted at the above-mentioned common key decryption process P13 and the random number generated at the random number generation process P21 of the receiver concerned are compared by the just exact private seal process P22, and the check of justification is performed.

[0239]By the way, in the system of this embodiment shown in drawing 1 mentioned above, the system management company 210, the virtual online shop 230, and the content provider 240 are formed as a system side to user side 200. The financial institution 220 of drawing 1 is an external bank etc., for example.

[0240]The control center 210 of the above-mentioned system management company 210, Exhibition of digital contents and management of distribution in the virtual online shop 230, between the financial institutions 220 -- the main work by the side of systems, such as collection of the accounting information of user side 200, or a variety of information, distribution and those managements, encryption of the digital contents from the content provider 240, and a security management of the information to treat, -- all are performed mostly.

[0241]However, in the system which distributes digital contents using a network which was mentioned above, In the time of the user side obtaining digital contents from the system side, and the case of the fee collection accompanying use of digital

contents, communication will concentrate on the system side and there is a possibility that a satisfying response may no longer be obtained to the user side.
[0242]So, in other embodiments of this invention, it makes it possible to prevent concentration of communication which was mentioned above and to raise a communicative response by the function of the system management company 210, and more specifically dividing the function of the control center 211 as follows.
[0243]Namely, the content exhibiting distributing institution 310 which has a function which exhibits digital contents and distributes the composition by the side of the system to user side 200 in other embodiments of this invention as shown in drawing 30, Accounting information control machine Seki 320 which has the function to manage the accounting information of the user of a fixed area, It divides into the data generation of enciphering digital contents, distribution of generated data to the above-mentioned content exhibiting distributing institution 310, the information gathering from above-mentioned accounting information control machine Seki 320, division of earnings, and the system management organization 330 that has the function to perform the security management and others of the whole system, User side 200 and communication are independently attained for each organization 310,320,330, respectively.
[0244]In composition like this drawing 30, the content exhibiting distributing institution 310 is scattered on the network in the world, two or more arrangement is possible for it, and if even communication charges are paid, it can access user side 200 to the content exhibiting distributing institution 310 of every area. For example, when user side 200 wants for digital contents to come to hand, the above-mentioned content exhibiting distributing institution 310 is accessed from user side 200, and digital contents come to hand. Digital contents [which were enciphered by the system management organization 330], i.e., user, side 200 will be the digital contents at this time in the state which can be transmitted directly using a network.
[0245]Holding not much many users installs accounting information control machine Seki 320 for a moderate number of every users undesirably therefore on safety management in order to treat accounting information. However, since the attack point (accounting information control machine Seki 320) from the 3rd person with bad faith will be increased and it will be traded off if it installs not much mostly, optimizing is desirable. For example, when user side 200 performs communication about fee collection, it accesses from user side 200 to above-mentioned accounting information control machine Seki 320.
[0246]The above-mentioned system management organization 330 Subscription to a user's system, and registration of means of settlement, Profits distribution to the profits beneficiary of the collection of money from a user, said right holder, the content exhibiting distributing institution 310, and accounting information control machine Seki 320 grade, etc. raise security by carrying out by summarizing management of important information on security. However, as for the system management organization 330 concerned, it is desirable not to necessarily establish one place in the world and to install in a certain settled unit, for example, the unit of a country etc. For example, when user side 200 performs important communication on [, such as subscription to this system, and registration of means of settlement,] security, it carries out by accessing from user side 200 to the above-mentioned system management organization 330. The system management organization 330 concerned which obtained information performs profits distribution to the collection of money and the profits beneficiary from the user concerned collectively from above-mentioned accounting information control machine Seki 320. It is supplied to the

system management organization 330 concerned, the source data, i.e., the contents, which an owner of a copyright etc. have, they are changed into the digital contents by which encryption etc. were made here, and are distributed to the above-mentioned content exhibiting distributing institution 310.
[0247]As mentioned above, by distributing the function by the side of a system to the three organizations 310,320,330, and making direct access of it possible between user side 200 and each organization 310,320,330, communicative concentration is prevented and it becomes possible to raise a communicative response. According to the content exhibiting distributing institution 310, it can respond also to a thing like what is called an existing virtual Mall, and it is effective also in sales promotion and attractive for a user. By dividing accounting information control machine Seki 320 independently, it is useful for the dishonesty prevention which conspired with exhibition and the selling function of contents. In order that a fixed number may obstruct the user who manages, the controlling function who receives unjustly is also more effective.
[0248]In the system of other embodiments of this invention shown in drawing 30 mentioned above below, It explains that the accounting information accompanying the information flow at the time of acquisition of the contents key subscription to a user's system, the purchase of point information, and for decoding of the enciphered digital contents, etc., the flow in the case of circulation of the information for contents and contents appreciation, and use of contents flows.
[0249]First, the principal part of the flow of the time of subscription to a user's system is explained using drawing 31.
[0250]In the case of the subscription registration to a user's system, the following procedures depended on the user subscription support functional block 402 of the system management organization 330 follow, and registering operation is performed at it.

[0251]From user side 200 [1], i.e., said player, and the user terminal 50, the information which shows the intention of subscription to a system is first sent via a network like the subscription intention sending T41 to the system management organization 330. The information on the above-mentioned subscription intention of having been inputted into the communication function block 401 of the system management organization 330 is sent to the user subscription support functional block 402.
[0252]Reception of the above-mentioned subscription intention information of the user subscription support functional block 402 concerned will send the information on a file required for subscription to user side 200 via the communication function block 401 like the subscription required file sending T42.
[0253]In user side 200, creation of the subscription request according to a predetermined format is performed based on the subscription required file sent from the above-mentioned system management organization 330. The drawn-up subscription request concerned is sent to the system management organization 330 like the subscription request sending T43.
[0254]The user subscription support functional block 402 which received the above-mentioned subscription request sends the information which explains the function of a client to user side 200 like the client function sending T44.
[0255]From user side who received information on client function concerned 200, User Information, such as users' information, for example, an account number and a

credit number which were mentioned above, a name, and a contact, is sent to the system management organization 330 like the User Information sending T45.
[0256]The user subscription support functional block 402 which received sending of the User Information concerned notifies the information on the purport that the registration procedure of subscription was completed to user side 200 like the registration procedure completion notification T46.
[0257]The user subscription support functional block 402 of the system management organization 330 transmits User Information to accounting information control machine Seki 320 via the communication function block 401 like the User Information sending T47 after the completion of procedure of this user subscription registration. Accounting information control machine Seki 320 which received this User Information saves the User Information concerned at the database function block 367.
[0258]By the above, the main flows of the time of subscription to a user's system are completed. The explanation about other composition currently mentioned to this drawing 31 is mentioned later.
[0259]Next, the principal part of the flow of the information at the time of acquisition of the key the purchase of point information and for decoding of the enciphered digital contents, etc. is explained using drawing 32. Since the information on the contents key the purchase of the above-mentioned point information and for decoding of the enciphered digital contents is information for using contents, it is made to simplify these and to call it royalty information by the following explanation.
[0260]When a user obtains the important information (here royalty of contents) used by a system, access is made from user side 200 to accounting information control machine Seki 320 where the assignment in its duty is beforehand made for every user side 200. To access of an acquisition demand of the contents royalty information sent from above-mentioned user side 200, the royalty issuing function block 362 of accounting information control machine Seki 320 corresponds, and issue of a royalty is performed according to the following procedures.
[0261]First, from user side 200, the information on the purport that he would like to purchase a royalty is sent to accounting information control machine Seki 320 like the purchase written request sending T51. The information on the purport that he would like to purchase a royalty is information on the purchase written request which followed the predetermined format by user side 200. Thus, the information on the above-mentioned purchase written request inputted into the communication function block 361 of this accounting information control machine Seki 320 is sent to the royalty issuing function block 362 via a network.
[0262]In the royalty issuing function block 362 concerned, if the information on the above-mentioned purchase written request is received, it will carry out based on User Information saved at the database function block 367, the information on a new royalty will be generated, and the information on the royalty concerned will be sent to user side 200 like the new royalty sending T52.
[0263]If the receipt of the information on the above-mentioned new royalty is checked, user side 200 will draw up the receipt written confirmation according to a predetermined format, and will send it to the royalty issuing function block 362 of accounting information control machine Seki 320 like the receipt written confirmation sending T53.
[0264]By the above, the main flows of the time of the purchase of a royalty are completed. The explanation about other composition currently mentioned to this drawing 32 is mentioned later.

[0265]Next, the principal part of the flow in the case of circulation of the information for contents and contents appreciation (here, they are a service condition and a contents key) is explained using drawing 33.
[0266]First, the contents acquisition functional block 342 of the content exhibiting distributing institution 310 charges digital contents to the system management organization 330 like the contents bill sending T62.
[0267]In the contents distribution functional block 404, the system management organization 330 which received the contents bill concerned is processed so that the demanded contents can be circulated. That is, in this contents distribution functional block 404, the digital contents (enciphered digital contents) of the state which can be sent to user side 200 are generated. These processed digital contents are sent to the content exhibiting distributing institution 310 like the contents sending 63.
[0268]In the content exhibiting distributing institution 310 concerned, the digital contents processed [above-mentioned] are saved at the contents database functional block 345.
[0269]In the contents distribution functional block 404 of the system management organization 330. The contents key for decoding the contents enciphered as content ID and a service condition as information for contents appreciation is sent to accounting information control machine Seki 320 like the information sending T64 for contents appreciation.
[0270]In accounting information control machine Seki 320, a contents key and the service-condition receipt functional block 363 receive the information for the above-mentioned contents appreciation, and it is saved at the database function block 367.
[0271]Next, like the contents acquisition request T61, user side 200 is accessed to the content exhibiting distributing institution 310, and obtains contents. Namely, the content exhibiting distributing institution 310, reading the enciphered digital contents which are saved at the contents database functional block 354, if the demand of acquisition of contents is made from above-mentioned user side 200 via the communication function block 341 -- the read digital contents concerned -- user side 200 -- sending .
[0272]Then, user side 200 is accessed to accounting information control machine Seki 320 by the information claim T65 for contents appreciation, and obtains the information for contents appreciation like the information sending T66 for contents appreciation. Namely, via the communication function block 361 in accounting information control machine Seki 320, If the request for a service condition and a contents key is made as information for contents appreciation from above-mentioned user side 200, a contents key and a service condition will be published from a contents key and the service-condition issuing function block 364, and these will be sent to user side 200 via the communication function block 361.
[0273]By the above, the flow in the case of circulation of the information for contents and contents appreciation is completed. The explanation about other composition currently mentioned to this drawing 33 is mentioned later.
[0274]Next, the principal part of the flow of balancing account, i.e., balancing account of a contents usage fee, when contents are actually appreciated is explained using drawing 34.
[0275]First, after appreciation of contents is performed in user side 200, from concerned user side 200, point usage information, i.e., use record of contents, is sent to accounting information control machine Seki 320 like the statement-of-accounts sending T71 as mentioned above. Thus, if sending of the above-mentioned contents use record is received from above-mentioned user side 200 via the communication

function block 361, the contents use record concerned will be received with the balancing account procedure reception functional block 365 of accounting information control machine Seki 320, and the balancing account written confirmation corresponding to this will be published. Similarly the balancing account written confirmation concerned is sent to user side 200 via the communication function block 361 like the balancing account written confirmation sending T73. Thereby, user side 200 can know that balancing account was performed.
[0276]Next, the balancing account procedure reception functional block 365 of accounting information control machine Seki 320 makes royalty issuing information publish from the royalty issuing function block 362. This royalty issuing information is sent to the system management organization 330 via the communication function block 361 as user settlement of accounts and the contents use record sending T74 with the contents use record sent from above-mentioned user side 200.
[0277]The system management organization 330 summarizes the information sent from accounting information control machine Seki 320 currently distributed in various places with collection of money and the distribution frame block 405, totals the amount of collection of money, a collection-of-money place, and the distribution destination of money, and settles them through a actual financial institution.
[0278]By the above, the flow of balancing account of a contents usage fee is completed. The explanation about other composition currently mentioned to this drawing 34 is mentioned later.
[0279]In explanation to drawing 34, from above-mentioned drawing 30, the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, the system management organization 330, and user side 200, In the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, and the system management organization 330, it cannot be overemphasized that a data encryption and decryption are performed like the above-mentioned. Also in this encryption and decryption, any of a public-key crypto system and a common key encryption system may be used, as mentioned above, a public-key crypto system can be used as a cipher system of a contents key or a common key, and a common key encryption system can be used as cipher systems, such as a message and various kinds of documents. It is also possible to use the technique of the improvement in security using said random number, the encryption at the time of treating contents, and least-common-multiple-ization of a compressive batch with these encryption.
[0280]Next, the concrete composition of each organizations 310, 320, and 330 mentioned above is explained briefly.
[0281]First, the composition of the content exhibiting distributing institution 310 is explained using drawing 35.
[0282]In this drawing 35, the content exhibiting distributing institution 310 concerned, The communication function block 341 which divides roughly and takes charge of the communication function between user side 200 and the system management organization 330, It consists of the contents acquisition functional block 342 which takes charge of the acquisition function of contents, the content display functional block 343 which takes charge of the exhibition function of contents, the balancing account functional block 344 which takes charge of balancing account, and the contents database functional block 345 which saves contents.
[0283]The contents bill creation function part 351 which takes charge of creation of a bill in case the above-mentioned contents acquisition functional block 342 charges

contents to the system management organization 330, The contents receipt creation function part 352 which takes charge of creation of a receipt when contents are received from the system management organization 330, It consists of the function part 353 corresponding to a contents database which takes charge of correspondence with these **** and ** contents, and the contents saved at the contents database functional block 345.
[0284]The content display function part 354 which takes charge of the function for which the above-mentioned content display functional block 343 actually exhibits contents to virtual online shop, It consists of the function part 355 corresponding to a contents database which takes charge of correspondence with the contents currently these-exhibited and the contents saved at the above-mentioned contents database functional block 345.
[0285]The above-mentioned balancing account functional block 344 consists of the receipt issuing function part 356 which takes charge of the function to publish a receipt, and the function part 357 corresponding to the financial institution which takes charge of correspondence between the financial institutions 220.
[0286]Next, the composition of accounting information control machine Seki 320 is explained using drawing 36.
[0287]In this drawing 36, accounting information control machine Seki 320 concerned, The communication function block 361 which divides roughly and takes charge of the communication function between user side 200 and the system management organization 330, The royalty issuing function block 362 which takes charge of the function to publish a royalty, A contents key, and the contents key and service-condition receipt functional block 363 which take charge of the receipt of a service condition, A contents key, and the contents key and service-condition issuing function block 364 which take charge of issue of a service condition, It consists of the balancing account procedure reception functional block 365 which takes charge of the receptionist function of balancing account procedure, the distribution receipt functional block 366 which takes charge of the function of a receipt as distribution, and the database function block 376.
[0288]The purchase written request acknowledgement function part 371 in which the above-mentioned royalty issuing function block 362 takes charge of the acknowledgement function of a purchase written request, The point-data acknowledgement function part 372 which takes charge of the check of the data of the balance (balance of point information) of the royalty of client, i.e., user, side 200, use record (point usage information), etc., The royalty generating function part 373 which takes charge of the function to generate a royalty, and the royalty invoice creation function part 374 which takes charge of the function which draws up the invoice of a royalty, It consists of a royalty, the sending function part 375 which takes charge of the function to actually send a royalty invoice, the royalty receipt acknowledgement function part 376 which takes charge of the check of the receipt document of a royalty, and the royalty issuing information preservation function part 377 which takes charge of the function to save the information on the published royalty.
[0289]Above-mentioned contents key and service-condition receipt functional block 363 consist of a contents key, the receipt function part 378 which takes charge of the receipt of a service condition, and a contents key and the preservation function part 379 which saves a service condition.
[0290]Above-mentioned contents key and service-condition issuing function block 364, A contents key and the receiving function part 380 which takes charge of the function to receive the acquisition request of a service condition, The search service

part 381 which takes charge of the function which searches and discovers a contents key and a service condition from the database function block 367, It consists of the transmitting-function part 382 which takes charge of the function to encipher and send a contents key and a service condition, and a contents key and the acknowledgement function part 383 which takes charge of the acknowledgement function of the receipt document of a service condition.
[0291]The contents use record receiving function part 384 which takes charge of the function which the above-mentioned balancing account procedure reception functional block 365 receives the contents use record (point usage information) enciphered, and is decrypted, The contents use record acknowledgement function part 385 which takes charge of the check of contents use record, The contents use record-keeping function part 386 which takes charge of the function in which the database function block 367 saves contents use record, It consists of the completion document creation function part 387 which takes charge of the function which draws up the completion document of balancing account procedure, and the conclusion function part 389 which takes charge of the function to edit contents use record collectively.
[0292]The bill acknowledgement function part 390 which takes charge of the acknowledgement function of the request-for-information document which charges the data at the time of the above-mentioned distribution receipt functional block 366 collecting money, The use record report writer feature part 391 which takes charge of the function which draws up the report of the contents use record submitted to the system management organization 330, It consists of the royalty issue report writer feature part 392 which takes charge of the function which draws up the report of the royalty issuing information submitted to the system management organization 330, and the written confirmation acknowledgement function part 393 which takes charge of the acknowledgement function of the confirmation-of-receipt document of a report.
[0293]The royalty database function part 394 which takes charge of the function in which the database function block 367 saves the data of a royalty, A contents key, and the contents key and royalty database function part 395 which take charge of the function to save the data of a service condition, It consists of the user management data base function part 397 which saves the information about the contents use recording data base function part 396 which saves contents use record, and a user.
[0294]Next, the composition of the system management organization 330 is explained using drawing 37.
[0295]In this drawing 37, the system management organization 330 concerned, The communication function block 401 which divides roughly and takes charge of the communication function between user side 200, the content exhibiting distributing institution 310, and accounting information control machine Seki 320, It consists of the user subscription support functional block 402 which performs the support in the case of user subscription, the contents distribution functional block 404 which takes charge of distribution of contents, the database function block 403, and collection of money and the collection-of-money **** distribution frame block 405 which takes charge of the function of distribution.
[0296]The above-mentioned user subscription support functional block 402, Creation of a subscription request, and the subscription request creation transmitting-function part 411 which takes charge of transmission, The common key receiving function part 412 which takes charge of the function which receives and decrypts the enciphered common key, The subscription request acknowledgement function part 413 which takes charge of the acknowledgement function of the subscription request transmitted from user side 200, The ID generating function part 414 which takes charge of the

function to generate client ID, i.e., user ID, The subscription request preservation function part 415 which takes charge of the function to save a subscription request at the database function block 403, It consists of the client function generation function part 416 which generates a client function, and the registration information preservation function part 417 which takes charge of the function to save registration information at the database function block 403.
[0297]The user management data base function part 418 to which the database function block 403 carries out preservation management of a user's information, The contents database function part 419 which saves contents, and the accounting information control machine Seki database function part 420 which carries out preservation management of the information on accounting information control machine Seki 320, It consists of the content-exhibiting-distributing-institution database function part 421 which carries out preservation management of the information of the content exhibiting distributing institution 310.
[0298]The bill acknowledgement function part 422 in which the contents distribution functional block 404 takes charge of the acknowledgement function of the bill of contents, The content retrieval function part 423 which takes charge of the function to search ready-mixed concrete TENTSU (source data), i.e., the contents before processing, from the contents database function part 419 of the database function block 403, The content ID generation function part 424 which generates content ID, and the contents key generation function part 425 which generates a contents key, The contents service-condition generation function part 426 which generates a contents service condition, The contents compression function part 427 which compresses ready-mixed concrete TENTSU, i.e., the contents before processing, The preservation function part 429 which takes charge of the function to save the contents processing function part 428 which enciphers contents, and content ID, a contents key and a service condition at the contents database function part 419 of the database function block 403, The contents sending function part 430 which takes charge of the function to send contents via the communication function block 401, and the contents receipt acknowledgement function part 431 which takes charge of the function to check the receipt of contents, Content ID, a contents key, and ID, key and service-condition sending function part 432 that take charge of the function to send a service condition via the communication function block 401, It consists of content ID, a contents key, and ID, key and service-condition receipt acknowledgement function part 433 that take charge of the function to check the receipt of a service condition.
[0299]The request-for-information document creation function part 434 which makes out the bill of the data which use collection of money and the distribution frame block 405 for collection of money, The contents royalty receiving function part 435 which takes charge of the function to receive a contents royalty via the communication function block 401, The contents use record receiving function part 436 which takes charge of the function to receive contents use record via the communication function block 401, The confirmation-of-receipt document creation function part 437 which takes charge of the function which draws up the written confirmation of reception, It consists of the calculation and the bill creation function part 438 which makes out the bill which performs the calculation of the amount billed and the creation of a bill which are charged to a user, calculation of the dividend at the time of distributing the use gold collected by use to a right holder, and the calculation and the form-for-payment creation function part 439 which perform creation of a form for payment.
[0300]next -- being concerned -- others -- the composition of user side 200 corresponding to the system of an embodiment is explained using drawing 38. This

drawing 38 expresses each function of said player 1 and the user terminal 50 collectively.

[0301]In this drawing 38, the composition of concerned user side 200, The communication function block 451 which will take charge of the communication function between the system management organization 330, the content exhibiting distributing institution 310, and accounting information control machine Seki 320 if it divides roughly, The contents acquisition functional block 452 which takes charge of acquisition of contents, The royalty purchasing function block 453 which takes charge of the purchase of royalties, such as point information, a contents key, a service condition, A contents key, and the contents key and service-condition acquisition functional block 454 which take charge of acquisition of a service condition, The balancing account procedure functional block 455 which takes charge of balancing account procedure, and the user subscription support functional block 456 which takes charge of the function which supports subscription to a system, It consists of appreciation of contents, the contents appreciation accounting function block 457 which takes charge of the function of fee collection, and the database function block 458.

[0302]The above-mentioned contents acquisition functional block 452 consists of the contents acquisition function part 461 which takes charge of the function which actually obtains contents, and the contents preservation function part 462 which takes charge of the function in which contents are made to save at a memory medium.

[0303]The purchase written request creation function part 463 in which the royalty purchasing function block 453 draws up the purchase written request of a royalty, The conclusion function part 464 which takes charge of the conclusion of the data of the balance (point balance) of the royalty of a client (user), use record (point usage information), etc., It consists of the royalty installation function part 465 which takes charge of the function which installs each information as a royalty, and the royalty receipt document creation function part 467 which draws up a royalty receipt document.

[0304]A contents key and the service-condition acquisition functional block 454, It consists of a contents key, the acquisition written request creation function part 468 which draws up the acquisition written request of a service condition, a contents key and the receiving function part 469 which takes charge of reception of a service condition, and a contents key and the receipt document creation function part 470 which draws up the receipt document of a service condition.

[0305]The balancing account procedure functional block 455 consists of the conclusion function part 471 which performs the conclusion of contents use record (point usage information), and the completion document receiving function part 472 which takes charge of reception of the completion document of balancing account procedure.

[0306]The above-mentioned user subscription support functional block 456, It consists of the subscription request creation function part 473 which takes charge of creation of a subscription request, the client function installation function part 474 which takes charge of installation of a client function, i.e., initialization of a user's player 1, and the registration information creation function part 475 which takes charge of the function which creates registration information.

[0307]The content retrieval function part 476 which takes charge of search of the contents by which the contents appreciation accounting function block 457 was saved at the memory medium, The royalty acknowledgement function part 477 which takes charge of the check of a royalty, and the simple contents appreciation function part

478 which reproduces contents in [when choosing contents, for example] simple, The accounting function part 479 which manages accounting information (point information), and the contents function decoding part 480 which decrypts the contents enciphered, It consists of the contents extension function part 481 which elongates the contents compressed, and the contents viewer function part 482 for enabling recognition of the contents of the contents saved at the memory medium, for example.
[0308]The royalty database function part 483 where the database function block 458 saves the data of a royalty, It consists of a contents key, the contents key and service-condition database function part 484 which save a service condition, the contents use recording data base function part 485 which saves contents use record, and the user information data base function part 486 which saves User Information.
[0309]Next, the player 1 of each embodiment which was mentioned above, and the concrete using form of the user terminal 50 are explained using drawing 39 and drawing 40.
[0310]As shown in drawing 39, the player 1 is arranged after said analog output terminal 2, the interface terminal 3 for PC, and the I/O terminal 4 for memory media have projected out of the case of the player 1, and the memory medium 61 is connected to the above-mentioned I/O terminal 4 for memory media. For example in the case 60, these players 1 and the memory medium 61 are formed so that storage is possible, and they are made as [arrange / for example at the end side of this case 60 / the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC].
[0311]The case 60 where this player 1 and memory medium 61 were stored, From the side by which the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC are arranged, it is formed in the input/output port 53 of the personal computer 50 as the above-mentioned user terminal 50 so that insertion connecting may be possible.
[0312]Although the personal computer 50 concerned has the general composition which equipped the computer body with the display device 52, the keyboard 54, and the mouse 55, In the above-mentioned input/output port 53, the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC, and the corresponding interface are formed. Therefore, only by inserting in the input/output port 53 of the above-mentioned personal computer 50 the case 60 where the above-mentioned player 1 and the memory medium 61 were stored, The analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC come to be connected with the above-mentioned personal computer 50.
[0313]Although he is trying to form an interface [in the input/output port 53 of the personal computer 50 / terminal / 3 / for PC / the analog output terminal 2 of the above-mentioned player 1, and / interface] in the example of above-mentioned drawing 39, For example, as shown in drawing 40, it is also possible to arrange the adapter 62 which can respond to the interface of the general-purpose input/output port of the personal computer 50 between the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC.
[0314]In the system of an embodiment of the invention since it has stated above, Since digital contents are enciphered with the contents key which is a common key of a system, If it is the user (player 1) who registered with the system of this embodiment, if only it can copy these enciphered contents freely and a contents key comes to hand, appreciation of these contents is also possible. Therefore, installation to this contents memory medium (enciphered contents) can also be performed easily. On the other hand, since the enciphered digital contents cannot be decoded, the right

of the copyright of contents or the right holder of the contents concerned is protected by the terminal unit which is not based on this embodiment system.
[0315]an embodiment of the invention, while according to the system filling up point information with a prepaid system (charge advance payment method) and reducing point information at the time of contents appreciation, Since he is trying to collect the usage information of the point, recovery of an appreciation price is possible for right holders (owner of a copyright etc.), a contents selling store, etc. with the right about a used point.
[0316]Since encryption is given in the case of an exchange of the data of point information or point usage information as mentioned above, security nature is improving. For example, since it shall trade after checking that use the random number (security ID) which interlocked by the system and player side, and both are in agreement, as mentioned above even if the completely same thing as the last data is forged and it tries to steal the point information for fee collection, it is safe.
[0317]1 chip making of the main components of a player is carried out, and it is difficult to take out key information and the decrypted digital contents outside. This player 1 equips player 1 the very thing with the tamper resistance function, in order to prevent the data usurpation by destruction of the player 1 concerned.
[0318]As mentioned above, according to the embodiment of the invention, the digital contents distributing system with high security top intensity is built.
[0319]As above-mentioned digital contents, various kinds of things other than digital audio information, such as a digital video data, can be mentioned. When dynamic-image-data (audio information is also included) use is carried out as the above-mentioned digital video data, as the technique of said compression, compression methods, such as MPEG (Moving Picture Image CodingExperts Group), can be used, for example. The above-mentioned MPEG, In WG(Working Group) 11 of SC(Sub Committee) 29 of JTC(Joint Technical Committee)1 of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). It is a common name of the packed video coding mode, and there are MPEG1, MPEG 2, MPEG4, etc.
[0320]As the technique of the above-mentioned encryption, as mentioned above, the enciphering method currently called what is called DES (Data Encryption Standard) can be used. DES is the standard cipher system (cryptographic algorithm) which NIST (National Institute of Standards and Technology) in the U.S. announced in 1976. Data conversion is performed for every 64-bit data block, and, specifically, the conversion using a function is repeated 16 times. The above-mentioned digital contents, point information, etc. are enciphered with what is called a common key system using the DES concerned. It is a method which becomes the same [the key (decode key data) for decrypting with the key data (encryption key data) for enciphering] as that of the above-mentioned common key system.
[0321]What is called an EEPROM (electrically eliminable ROM) can be used for the common key storage memory 22 of the player 1 of said drawing 1, the key storage memory 21 for communication, the point usage information storing memory 29, and point information storing memory 28 grade, for example.
[0322]As a memory medium, the memory medium of recording media, such as a hard disk, a floppy disk, a magneto-optical disc, and a phase-change optical disk, or semiconductor memory (IC card etc.) can be used for others, for example.
[0323]In addition, although selection, a check, etc. were performed in the above-mentioned embodiment using the keyboard 54 of the user terminal 50, and the mouse 55 and the display device 52 on the occasions, such as content confirmation etc. of the

contents exhibited by selection and the virtual online shop 230 of contents, It is also possible to simplify a function to these keyboards, or a mouse and a display device, and to give the player 1. namely, . Like drawing 2, it is also possible to form the input key part 6 and the indicator 7 in the player 1.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a system configuration figure showing the entire configuration of the digital contents distribution system of an embodiment of the invention.

[Drawing 2]It is a block circuit diagram showing specific constitution of the player corresponding to the system of an embodiment of the invention.

[Drawing 3]It is a block circuit diagram showing specific constitution of the control center corresponding to the system of an embodiment of the invention.

[Drawing 4]It is a figure used for explanation of the procedure at the time of the purchase of a player in the system of this embodiment.

[Drawing 5]It is a figure used for explanation of the procedure to installation of the digital contents from search of digital contents to the memory medium for players in the system of this embodiment.

[Drawing 6]It is a figure used for explanation of the procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for fee collection in the system of an embodiment.

[Drawing 7]It is a figure used for explanation of the procedure of distribution of a fee collection price in the system of an embodiment.

[Drawing 8]It is a flow chart which shows the flow of the processing in the player at the time of point purchase in the system of an embodiment.

[Drawing 9]It is a flow chart which shows the flow of the processing in the user terminal at the time of point purchase in the system of an embodiment.

[Drawing 10]It is a flow chart which shows the flow of the processing in the control center at the time of point purchase in the system of an embodiment.

[Drawing 11]It is a figure showing the sequence of the information transmission and reception at the time of point purchase in the system of an embodiment.

[Drawing 12]It is a flow chart which shows the flow of the processing in the player at the time of acquisition of digital contents in the system of an embodiment.

[Drawing 13]It is a flow chart which shows the flow of the processing in the user terminal at the time of acquisition of digital contents in the system of an embodiment.

[Drawing 14]It is a flow chart which shows the flow of the processing in the control center at the time of acquisition of digital contents in the system of an embodiment.

[Drawing 15]It is a figure showing the sequence of the information transmission and reception at the time of acquisition of digital contents in the system of an embodiment.

[Drawing 16]It is a flow chart which shows the flow of the processing in the player at the time of acquisition of a contents key and a service condition in the system of an embodiment.

[Drawing 17]It is a flow chart which shows the flow of the processing in a contents key and the user terminal at the time of acquisition of a service condition in the system of an embodiment.

[Drawing 18]It is a flow chart which shows the flow of the processing in the control center at the time of acquisition of a contents key and a service condition in the system of an embodiment.

[Drawing 19]It is a figure showing the sequence of the information transmission and reception at the time of acquisition of a contents key and a service condition in the system of an embodiment.
[Drawing 20]It is a flow chart which shows the flow of the processing at the time of actually appreciating digital contents using a player and a user terminal in the system of an embodiment.
[Drawing 21]It is a flow chart which shows the flow of the processing in the player at the time of point usage information return in the system of an embodiment.
[Drawing 22]It is a flow chart which shows the flow of the processing in the user terminal at the time of point usage information return in the system of an embodiment.
[Drawing 23]It is a flow chart which shows the flow of the processing in the control center at the time of point usage information return in the system of an embodiment.
[Drawing 24]It is a figure showing the sequence of the information transmission and reception at the time of point usage information return in the system of an embodiment.
[Drawing 25]It is a flow chart which shows the flow of the processing at the time of performing decryption and extension in the least common multiple of the batch of encryption and compression.
[Drawing 26]It is a block circuit diagram showing the composition which performs encryption, decryption for every unit of the least common multiple of a compressive batch, and elongation processing.
[Drawing 27]It is a block circuit diagram showing specific constitution which generates the random number as security ID.
[Drawing 28]When enciphering a common key with a public-key crypto system and transmitting, it is a figure for explaining signs that a random number is inserted.
[Drawing 29]It is a figure for explaining signs that a random number is taken out from a receiving sentence and the check of justification is made.
[Drawing 30]It is a figure used for explanation of each organization when the function by the side of a system is divided.
[Drawing 31]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the flow of the time of subscription to a user's system.
[Drawing 32]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the information flow at the time of acquisition of the key the purchase of point information, and for decoding of the enciphered digital contents, etc.
[Drawing 33]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the flow in the case of circulation of the information for contents and contents appreciation.
[Drawing 34]In the embodiment which divided the function by the side of a system, it is a figure for explaining the principal part of the flow of balancing account when contents are actually appreciated.
[Drawing 35]In the embodiment which divided the function by the side of a system, it is a block diagram showing the composition of content exhibiting distributing institution.
[Drawing 36]In the embodiment which divided the function by the side of a system, it is a block diagram showing the composition of accounting information control machine Seki.

[Drawing 37]In the embodiment which divided the function by the side of a system, it is a block diagram showing the composition of a system management organization.
[Drawing 38]In the embodiment which divided the function by the side of a system, it is a block diagram showing users' composition.
[Drawing 39]It is a figure used for explanation of an example of the concrete using form of a player and a user terminal.
[Drawing 40]It is a figure used for explanation of other examples of the concrete using form of a player and a user terminal.
[Description of Notations]
1 A player, 2 analog output terminals, the interface terminal for 3 PC, 4 The I/O terminal for memory media, and 16 A controller and 19 Security ID generating circuit, 20 An open code decoder circuit and 21 The key storage memory for communication, and 22 Common key storage memory, 23 A user ID storing memory and 24 A common code decoder circuit and 25 Buffer memory, 26 An expansion circuit, 27 D/A conversion circuits, 50 user terminals, and a 100 contents-managing functional block, A 110 user-management functional block and 120 [A financial institution and 230 / Virtual online shop and 240 / Content provider] A usage information controlling-function block and 130 A controlling-function block and 200 The user side, 210 system management companies, 211 control centers, and 220

DETAILED DESCRIPTION
[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention distributes digital contents among a user-terminal device, for example, and it relates to the digital contents distribution managerial system which performs those managements.
[0002]
[Description of the Prior Art]Facilitate circulation of digital contents, such as a computer program, audio information, a video data, delve into a latent demand, and as a technique advantageous to a market expansion, For example, a technique like the software management method indicated to JP,H6-19707,B, the software use managing system indicated to JP,H6-28030,B, and the software management method indicated to JP,H6-95302,B exists. The software management method indicated to above-mentioned JP,H6-19707,B enables it to grasp the Assessment on Search Report by Designated Searching Authority of software according to a software right holder etc. when using software, such as a computer program which is intangible property, and a video data. The software use managing system indicated to JP,H6-28030,B, Use of software, such as a computer program which is intangible property, and a video data, is faced, Buy an onerous program (after buying, it can be used for free), attach a price, provide the data in which the amount of money which can be purchased is shown in the computer system, and in the case of onerous program purchase. Register with a table as a name of the available software in a same system, and. When reducing the data in which the amount of money concerned which can be purchased is shown by a software price and erasing registered software from this table, it is made to carry out renewal of an increase of the data in which the amount of money in which this purchase is possible is shown according to a situation. The software management method indicated to above-mentioned JP,H6-95302,B, In order to collect a utilization charge when using software, such as a computer program which is intangible property, and a video data, according to actual utilization quantity (using frequency or utilization time) per onerous program, It is effective in the system in the case of

carrying out "recording a user identification signal and a fee" with discernment of the used program, and a program right holder being able to grasp the utilization charge of a program which he owns by collecting these records, and collecting the program utilization charges according to the utilization quantity of the program.
[0003]
[Problem(s) to be Solved by the Invention]By the way, in the system which distributes digital contents using the above networks, Communication concentrates on the system side in the time of a user obtaining digital contents from the system side, and the case of the fee collection accompanying use of digital contents, and there is a possibility that a satisfying response may not be obtained to a user.
[0004]Then, this invention is made in view of such a situation, and is a thing.
It is providing the digital data distribution managerial system which can raise the purpose.

[0005]
[Means for Solving the Problem]A function to manage accounting information to a user-terminal device of a fixed area according to this invention, A function which exhibits digital contents and is distributed, and processing of digital contents, Distribution of digital contents to the above-mentioned digital content display distribution function processed [above-mentioned], Consisting of a function to perform information gathering and profit distribution from an accounting information controlling function, and the whole security management distribution, data communications between a user-terminal device and each function solve SUBJECT mentioned above by carrying out independently, respectively.
[0006]
[Embodiment of the Invention]Hereafter, the desirable embodiment of this invention is described, referring to Drawings.
[0007]First, before giving the concrete contents of the digital contents distribution managerial system of this invention, and explanation of composition, in order to make these understanding easy, the outline composition of the whole system and the operation method of a system with which this invention is applied are briefly explained using each figure from drawing 1 to drawing 7.
[0008]The rough composition of the whole system is shown in drawing 1.
[0009]In this drawing 1, user side 200 assumes that the digital contents playback device (it will be hereafter called the player 1) and what is called a personal computer (it will be hereafter called the user terminal 50) of this invention are held.
[0010]Although the user terminal 50 is the usual personal computer, The various software which is used for this invention and which is mentioned later is stored as application software, and while, it comes to connect the loudspeaker which is the display device and sound emission means which are displaying means, a keyboard, a mouse which are information input means, etc. Via a network, the system management company 210 and connection are possible for the user terminal 50 concerned, and it has an interface means between the players 1, and data transmission and reception are possible for it.
[0011]The player 1 has composition as shown in drawing 2.
[0012]Although detailed explanation of the composition of this drawing 2 is mentioned later, The player 1 concerned as the main components of the processing route of digital contents, It has the common key encryptosystem decoder circuit 24 which decrypts the digital contents enciphered using a contents key, the expansion circuit 26 which is the expansion means which elongate the digital contents

compressed, and the D/A conversion circuit 27 which changes digital data into an analog signal at least. The decryption told to below is solving encryption.
[0013]The information which shows the right information data and the operating condition of digital contents which this player 1 uses. (These information is hereafter called point usage information) The possession money data which is needed when using digital contents, Namely, as the main components treating the billing data (it is hereafter called point information) etc. which are reduced whenever it uses digital contents, It has at least the point usage information storing memory 29 which stores the above-mentioned point usage information, and the point information storing memory 28 which stores the above-mentioned point information.
[0014]This player 1 as composition for storing the various keys used for encryption and decryption which are mentioned later The common key storage memory 22 and the key storage memory 21 for communication, It has the common code decoder circuit 24 and the open code decoder circuit 20 as composition for performing encryption and decryption using the key stored in these. This player 1 as composition relevant to the above-mentioned encryption and decryption, It also has the security ID generating circuit 19 and the timer 18 which generate the random number interlocked with the host computer of the system management company 210, and generate security ID, and the hash function circuit 25 grade which generates what is called a hash value mentioned later.
[0015]In addition, the player 1 concerned is provided with the controller 16 which is a control means which performs digital contents, various kinds of data in addition to this, and control of each component based on the program stored in ROM17, and the cell 5 as operation power at the time of carrying.
[0016]Here, as for each main components of the player 1 of drawing 2, it is desirable on security to comprise one chip of IC (integrated circuit) or LSI (large scale integration circuit). In this drawing 2, 1 chip making of each main components is carried out into the integrated circuit 10. The player 1 concerned is equipped with three terminals (the analog output terminal 2, the Interface Division terminal 3 for PC, and the I/O terminal 4 for archive media) as an object for Interface Division with the exterior, and these each terminal is connected to the terminals 13, 12, and 11 in which the integrated circuit 10 corresponds, respectively. These each terminal is possible also for also unifying and newly providing another terminal, and is not scrupulous in particular.
[0017]The system management company 210 consists of the control center 211 which manages the whole system, and the store 212 which sells the above-mentioned player 1, and via the virtual online shop 230 between the user terminals 50 of user side 200, Transmission and reception of the information about supply of digital contents which is mentioned later, processing of the digital contents which compress and encipher the contents which the content provider 240 holds, the supply of digital contents processed [above-mentioned], the information transmission and reception between the financial institutions 220, etc. are performed. Between the system management company 210 and the financial institution 220, the exchange of the check of the account number of user side 200, a credit number, a name, a contact, etc., the information on the ability to trade between user side 200, etc., etc. are performed. Processing of actual price transfer etc. is performed between the financial institution 220 and user side 200. The store 212 does not necessarily need to be included in the system management company 210, and may be a sales agent.
[0018]The control center 211 of the above-mentioned system management company 210 has composition as shown, for example in drawing 3. Although detailed

explanation of the composition of this drawing 3 is mentioned later, As the main components, manage digital contents and Processing treatment, such as the exhibition, encryption, and compression, The contents managing functional block 100 which has each function which is the key information used for encryption and decryption of digital contents, such as a contents key and generating of ID, Manage User Information and Encryption and decryption of correspondence (a message, point information, etc.), The user management functional block 110 provided also with the user subscription processing function part 118 which performs user subscription processing besides each function, such as generating of a confirmation message, generating of security ID, a settlement-of-accounts application between the financial institutions 230, generating of the point, etc., It has at least the usage information controlling-function block 120 which manages point usage information etc., and the controlling-function block 130 which manages the whole system and has a communication function.

[0019]An example of the actual operation method of the system constituted like drawing 1 mentioned above is explained using drawing 4 - drawing 7. The following operation methods are procedures which user side 200, the system management company 210, the financial institution 220, and content provider 240 grade actually follow.

[0020]The procedure of the purchase of the player 1 in explanation of the operation method of this system, the procedure from search of digital contents to installation of the digital contents to the memory medium for player 1, The procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making the digital contents concerned usable and the procedure of distribution of the fee collection price collected from the user with appreciation of digital contents are explained in order.

[0021]First, as a procedure at the time of the purchase of the player 1, as shown in (1) of drawing 4, and (5), user side 200 actually purchases the above-mentioned player 1 from the above-mentioned store 212 by the shop front or mail order.

[0022]Personal information (a name, a contact, etc.) and settlement information (a bank account, a credit number, etc.) which were provided from above-mentioned user side 200 at the time of sale of the above-mentioned player 1 at this time as the above-mentioned store 212 was shown in (2) of drawing 4, The number (a player inherent key etc. are included) peculiar to the player 1 which sold [above-mentioned] is registered into the control center 211 of the system management company 210.

[0023]As shown in (3) of drawing 4, the control center 211 checks an account number, a credit number, etc. which were provided from above-mentioned user side 200 to the financial institution 220, and as shown in (4) of drawing 4, it acquires the information on the purport that it can trade from the financial institution 220.

[0024]User side 200 [next,] which purchased the above-mentioned player 1 as a procedure to installation of the digital contents from search of digital contents to the memory medium for player 1, Using the user terminal 50 provided with the interface means with the player 1 concerned, as shown in (1) of drawing 5, search of the digital contents of hope, selection, edit, an order, etc. are performed. Processing from the search at this time to an order is performed to the virtual online shop 230 where the user terminal 50 was connected via the network using the retrieval software stored as application software.

[0025]The virtual online shop 230 is a store which the control center 211 has provided virtually on a network, for example, and the information which shows the contents of two or more contents, for example is exhibited by this virtual online shop 230. User

side 200 will place an order for desired contents based on these information provided in the virtual online shop 230. As information which shows the contents of the contents exhibited by the virtual online shop 230, When contents are video datas, such as a movie, for example, titles and advertisements, such as the movie concerned, Images, such as one scene in the movie concerned, etc. can be considered, and when contents are audio information, a track name, an artist name, the number phrase (what is called an intro) of the beginning of the music concerned, etc. can be considered. Therefore, when the above-mentioned virtual online shop 230 is accessed with the user terminal 50 of user side 200. The order of contents will be performed because the contents of two or more contents of the above-mentioned virtual online shop 230 are exhibited virtually and choose a desired thing out of these display objects on the user terminal 50 concerned.

[0026]When there are an order of digital contents, etc. from the user terminal 50 of above-mentioned user side 200, the above-mentioned virtual online shop 230 performs the supply request of digital contents to the control center 211, as shown in (2) of drawing 5.

[0027]The control center 211 which received the supply request of the digital contents concerned performs the distribution request of the digital contents which had the above-mentioned supply request to the content provider 240. Thereby, the content provider 240 concerned supplies the digital contents which had the above-mentioned distribution request as shown in (4) of drawing 5 to the control center 211.

[0028]The control center 211 performs encryption and compression using predetermined compression technology to the digital contents rationed by the above-mentioned content provider 240, and. The virtual-online-shop name etc. which supply charge amount and contents when right holder information and the contents concerned, such as ID (content ID) of the contents concerned and an owner of a copyright of these contents, are used to user side 200 are added to these digital contents compressed and enciphered. The charge amount to contents is determined a priori by the content provider 240.

[0029]The contents processed in the above-mentioned control center 211 are sent to the virtual online shop 230, and as shown in (5) of drawing 5, as shown in (6) of drawing 5, they are further supplied to the user terminal 50 of user side 200 via this virtual online shop 230. By this, contents will be supplied to the player 1 from the above-mentioned user terminal 50, and these contents will be stored in the player 1 concerned.

[0030]It is also possible to carry out to this drawing 5 a priori about flowing to (2) - (5). That is, it not only may exhibit the information which shows the contents of two or more above-mentioned contents, but it may prepare beforehand for the virtual online shop 230 the digital contents corresponding to these exhibitions processed [above-mentioned].

[0031]Next, in the procedure of balancing account at the time of using purchase and the digital contents concerned of the point information for the fee collection for making usable the digital contents installed in the player 1 as mentioned above. First, with the user terminal 50, shortage of the point information stored in the player 1 is checked, and a supplement demand of point information is made from the user terminal 50 concerned.

[0032]At this time, as shown in (1) of drawing 6, from the user terminal 50 concerned, the supplement request of the point information enciphered by the player 1 is transmitted to the control center 211. Simultaneously, it is read from the player 1, is enciphered and is sent to the control center 211 via the user terminal 50, a right

holder's information, i.e., point usage information, corresponding to the already used digital contents, such as an owner of a copyright. Thus, transmission of point usage information was made to be performed simultaneously with the supplement request of point information, in order that user side 200 might save the time and effort which accesses the control center 211 only for transmission to the control center 211 of the point usage information concerned. Of course, it is not necessary to necessarily perform transmission of this point usage information simultaneously with the purchase of point information, and may carry out independently.

[0033]The control center 211 which received the supplement request and point usage information of point information which were enciphered [above-mentioned] recognizes the replenishing amount of point information and the contents of point usage information which user side 200 is demanding by decoding the code concerned. The control center 211 concerned checks [of drawing 6] whether as shown in (2), the settlement of accounts for the point supplement concerned is possible to the financial institution 220. From the financial institution 220 concerned, a check accounts can be settled by investigating the account of user side 200 in the financial institution 220 will send directions of the settlement of accounts O.K. to the control center 211, as shown in (3) of drawing 6.

[0034]The control center 211 at this time connects the point usage number which will be paid to right holders, such as an owner of a copyright, to the content provider 240, i.e., the amount of money, as shown in (4) of drawing 6.

[0035]Then, in the control center 211, the letter missive of point supplementary information is enciphered, and with security ID, by making this into point supplement directions information, as shown in (5) of drawing 6, it sends to the user terminal 50. The above-mentioned point supplement directions information sent to the player 1 from this user terminal 50, It is decrypted in the player 1 concerned and supplement of the point information on the point information storing memory 28 and deletion of right holder information, including the copyright information etc. which were connected to the above place from the point usage information storing memory 29, are further performed after the check of security ID.

[0036]Next, the fee collection price collected from the user with appreciation of digital contents, That is, in the procedure of distribution of the price which will be charged directly to a user's account according to the usage information of a point, first, as shown in (1) of drawing 7, a price transfer request is made from the financial institution 220 to user side 200. When a price transfer request in particular is not made when there is sufficient balance for the account of user side 200 at this time, and there is not sufficient balance for an account, as shown in (2) of drawing 7, transfer of a price is made from user side 200 to the financial institution 220.

[0037]The financial institution 220 deducts a prescribed fee, and as shown in (3) of drawing 7, it remits the price received from user side 200 to the control center 211. That is, in the control center 211, the charge of contents processing, a financial fee, system management expense, etc. are collected from the above-mentioned price remitted from the financial institution 220. The control center 211 concerned pays the content provider 240 the royalty according to the point used previously, as shown in (4) of drawing 7, and as shown in (5) of drawing 7, it pays a store fee to the virtual online shop 230. The content provider 240 who received the above-mentioned royalty pays each owner of a copyright a royalty, and the virtual online shop 230 which received the above-mentioned store fee pays the fee for every virtual online shop to each virtual online shop.

[0038]Thus, the price paid from user side 200, Based on said point usage information, it is distributed to a royalty, a store fee, a contents processing fee, a settlement-of-accounts fee, and a system management fee, the above-mentioned royalty -- the content provider 240 -- the above-mentioned store fee -- the above-mentioned virtual online shop 230 -- pay the system management company 210 a contents processing fee, a settlement-of-accounts fee is paid to a system management company and the financial institution 220, and a system management fee is paid to the system management company 210.
[0039]Here, in the case of the data transmission and reception between the systems of this embodiment, i.e., the data transmission and reception between the control center 211 and the player 1, in order to secure the safety of data communications, the data encryption and decryption which communicate are performed. According to this invention embodiment, it can respond as a method of encryption and decryption to both a common key encryption system and a public-key crypto system.
[0040]In the embodiment of the invention, the common key encryption system is adopted from a point of processing speed as a cipher system in the case of transmission of the variety of information of the above-mentioned digital contents, the above-mentioned point usage information, point information, a message and security ID, and others. The common keys used for encryption and decryption of these varieties of information differ corresponding to each information, respectively. The common key used for decryption of the enciphered information which is transmitted from the control center 211 in the player 1 of said drawing 2 is kept by said common key storage memory 22, Said common code decoder circuit 24 decrypts the information enciphered from the above-mentioned control center 211 using the common key currently kept in this common key storage memory 22.
[0041]The cipher system adopted by whether the player inherent key which is a peculiar key of said player 1 deals with which method as a cipher system in the case of transmission of the above-mentioned common key used for encryption and decryption of the above-mentioned variety of information on the other hand changes. That is, when the above-mentioned player inherent key supports the common key encryption system, the above-mentioned common key will be enciphered using the player inherent key concerned, and the enciphered common key concerned will be decrypted using the above-mentioned player inherent key. On the other hand, when the above-mentioned player inherent key supports the public-key crypto system, the public key of the partner point is used for encryption of the above-mentioned common key, and the secret key of the side which decrypts, respectively is used for decryption of the enciphered above-mentioned common key.
[0042]For example, in the case where the above-mentioned common key (for example, session key mentioned later) is sent to the control center 211 from the above-mentioned player 1, When the above-mentioned player inherent key supports the common key encryption system, In the above-mentioned player 1, the above-mentioned common key encryptosystem decoder circuit 24 enciphers the above-mentioned common key using the player inherent key which the key storage memory 21 for communication is keeping, and the common key enciphered [above-mentioned] is decrypted in the control center 211 using the player inherent key which the control center 211 concerned is keeping. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the control center 211 from the above-mentioned player 1 for example, The above-mentioned public-key-encryption decoder circuit 20 enciphers the above-mentioned common key in the public key of the control center 211 which the ** key

storage memory 21 for communication of the above-mentioned player 1 is keeping, and the common key enciphered [above-mentioned] is decrypted in the control center 211 using the secret key which the control center 211 concerned is keeping.
[0043]On the contrary, when the above-mentioned common key (for example, contents key) is sent to the player 1, for example from the above-mentioned control center 211 and the above-mentioned player inherent key supports the common key encryption system. The above-mentioned common key is enciphered with the player inherent key which the above-mentioned control center 211 is keeping, and said common code decoder circuit 24 decrypts the common key enciphered [above-mentioned] using the player inherent key currently kept by the above-mentioned key storage memory 21 for communication in the player 1. When the above-mentioned player inherent key similarly supports the public-key crypto system when the above-mentioned common key is sent to the player 1 from the above-mentioned control center 211 for example, The above-mentioned common key is enciphered in the public key of the player 1 which the above-mentioned control center 211 is keeping, and said open code decoder circuit 20 decrypts the common key enciphered [above-mentioned] using the player inherent key, i.e., the secret key, which are kept by the above-mentioned key storage memory 21 for communication in the player 1.
[0044]The cipher system of the player inherent key itself [which was mentioned above] is determined by whether delivery (delivery to the player 1 from the system management company 210) of the player inherent key concerned is easy. That is, since the common key encryption system is more advantageous in cost, if delivery of a player inherent key is easy, a common key encryption system will be adopted, but when delivery of the player inherent key concerned is difficult, it is a high cost, but a public-key crypto system is adopted. In mounting a player inherent key in hardware and mounting a common key encryption system in software, it adopts a public-key crypto system.
[0045]Hereafter, in an embodiment of the invention, the example which adopts the above-mentioned public-key crypto system will be given and explained in consideration of the compatibility in the case of mounting in software as a cipher system of a player inherent key itself. Namely, in the case where transmission of said common key is performed between the above-mentioned control center 211 and the player 1, When a common key (session key) is enciphered by the above-mentioned player 1 side, encryption is made using the public key of the control center 211, and the common key enciphered [above-mentioned] using the above-mentioned player inherent key (namely, secret key) is decrypted in the control center 211. On the contrary, when a common key (contents key) is enciphered by the above-mentioned control center 211 side, encryption is made in the public key of a player and the common key enciphered [above-mentioned] using the above-mentioned player inherent key (namely, secret key) is decrypted in the player 1.
[0046]Actual operation of the above-mentioned player 1, the user terminal 50, and the control center 211 which constitute the system employed using each procedure and a cipher system which were mentioned above is explained in order below.
[0047]First, it explains, referring to said drawing 2 and drawing 3 for flowing into the processing in the player 1 at the time of the point supplement, i.e., point purchase, which were mentioned above, the user terminal 50, and the control center 10 using drawing 11 from drawing 8.
[0048]The flow of the processing in the player 1 at the time of purchasing the point is shown in drawing 8.

[0049]In this drawing 8, starting of the software for point purchase beforehand installed in the user terminal 50, i.e., a personal computer, is performed by step ST1, It is waiting for the controller 16 of the player 1 in the meantime until the software for the point purchase concerned rises.
[0050]If the software for the above-mentioned point purchase rises, the controller 16 of the player 1 will receive the information inputted into the above-mentioned user terminal 50 from the user terminal 50 concerned in step ST2. An input request is made from the user terminal 50 concerned to the user who operates the above-mentioned user terminal 50 according to the software for the above-mentioned point purchase, and the information inputted into the user terminal 50 at this time is information, including a password, a point information number to purchase, etc.
[0051]The information from these user terminals 50 is received by the controller 16 via the terminal 12 of the integrated circuit 10 by which 1 chip making was carried out into the interface terminal 3 for PC of the player 1, and the player 1 concerned. The controller 16 which received the information from the user terminal 50 concerned, In step ST3, comparison with the password which the password storing memory 14 in the integrated circuit 10 of the player 1 concerned stores, and the password in the information which received [above-mentioned] is performed, and the above-mentioned receiving password checks that it is the right.
[0052]The above-mentioned password the right and the checked controller 16, At the same time it generates the information on the purport that he would like to purchase the point in step ST4 (main point of point purchase), and a point information number to purchase and other information, Security ID is generated from the security ID generating circuit 19, and these information is made to encipher by the common code decoder circuit 24 in the following step ST5. The controller 16 reads user ID from the user ID storing memory 23 in step ST6 next, It adds to the information which enciphered [above-mentioned] the user ID concerned, and the data which added and created the user ID concerned in step ST7 is further transmitted to the user terminal 50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50, the above-mentioned prepared data will be sent to the control center 211.
[0053]Since the common key encryption system is adopted as encryption of the above-mentioned prepared data at this time as mentioned above, generation of a common key is performed in advance of transmission of the prepared data concerned. For this reason, in the above-mentioned controller 16, a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation means, for example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto system here, in the above-mentioned controller 16. The public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken out, and it sends to the above-mentioned open code decoder circuit 20 at the same time it sends the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concerned, encryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus, with user ID, the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data.

[0054]As mentioned above, when also performing transmission of point usage information with a demand of point information, the controller 16 reads point usage information including said right holder information from the point usage information storing memory 29, and these also make the above-mentioned common code decoder circuit 26 send and encipher it. This enciphered point usage information is transmitted with the above-mentioned prepared data. Simultaneously with transmission of point usage information, it is also possible to transmit the balance of point information similarly.
[0055]Then, the controller 16 receives the data which has been sent from the control center 211 through the user terminal 50 in step ST8 and which is enciphered. The data sent from this control center 211 is the data in which the point information and information, including security ID etc., according to the above-mentioned point information number previously transmitted from the player 1 concerned to purchase were enciphered using the same common key as the above-mentioned session key.
[0056]If the data from the above-mentioned control center 211 is received, in step ST9, it sends the data concerned to the above-mentioned common code decoder circuit 24, and the controller 16 will read said common key which was generated previously and kept in the common key storage memory 22, and, similarly will send it to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, the data enciphered from the above-mentioned control center 211 using the above-mentioned common key is decrypted.
[0057]Next, security ID of the data in which the above-mentioned controller 16 was decrypted [above-mentioned] in step ST10, the point information which checked by comparison with security ID from the above-mentioned security ID generating circuit 19, and was stored in the above-mentioned point information storing memory 28 in step ST11 after the check -- the above -- it corrects for the newly sent point information.
[0058]After processing of correction of the above-mentioned point information, etc. is completed, the controller 16 generates the sign of processing completion, sends it to the above-mentioned common code decoder circuit 24 with the common key read from the above-mentioned common key storage memory 22, and is made to encipher by the common code decoder circuit 24 concerned in step ST12. Then, the controller 16 transmits the sign of the enciphered processing completion concerned to the user terminal 50 via the terminals 12 and 3 in step ST13, and sends it to the control center 211.
[0059]By the above, the flow of the processing in the player 1 in the case of point purchase is completed.
[0060]Next, the flow of the processing in the user terminal 50 at the time of the above-mentioned point purchase is explained using drawing 9.
[0061]In this drawing 9, the user terminal 50 starts the software for point purchase in step ST21. When the software for point purchase concerned rises, in this user terminal 50. The input request of information, including the password mentioned above to the user who operates the user terminal 50 concerned in step ST22 according to the software for the above-mentioned point purchase, a point size to purchase, etc., is performed, If these information is inputted from a user, the inputted information concerned will be transmitted to the above-mentioned player 1 like step ST2 of said drawing 8.
[0062]Next, the user terminal 50 will transmit the data transmitted from the player 1 concerned in step ST24, if the data created like step ST7 of said drawing 8 from the

above-mentioned player 1 in step ST23 is received, the address 211, i.e., the control center, which are registered beforehand.
[0063]If the user terminal 50 after performing the above-mentioned data transfer has the data return from waiting and the control center 211 in the return from the control center 211, it will transmit the data from the control center 211 concerned to the player 1 as it is in step ST25.
[0064]If the sign of processing completion is received like step ST13 of said drawing 8 from the above-mentioned player 1 in step ST26, in order to tell a user about processing of the point purchase concerned etc. having been completed, the user terminal 50 concerned, The sign of processing completion is displayed on a display in step ST27, and a user is made to check.
[0065]Then, the user terminal 50 concerned transmits the cryptogram of the sign of the processing completion sent from the above-mentioned player 1 to the control center 211.
[0066]By the above, the flow of the processing in the user terminal 50 in the case of point purchase is completed.
[0067]Next, the flow of the processing in the control center 211 at the time of point purchase is explained using drawing 10.
[0068]In this drawing 10, the control center 211 like step ST31, The data enciphered [above-mentioned] from the player 1 transmitted via the user terminal 50 by the communication function section 133 of the controlling-function block 130 by which the whole is controlled like step ST7 of said drawing 8 and step ST24 of drawing 9 in the control function part 131 is received. When this data is received, the user management functional block 110 of the control center 211, Based on the user ID attached to the received data concerned, a common key comes to hand from the database section 112 under control of the control function part 111 like step ST32, and security ID comes to hand from the security ID generating function part 116.
[0069]The common key at this time is said session key beforehand sent from said player 1, and this session key is enciphered and sent with a public-key crypto system as mentioned above. Therefore, at the time of decoding of this session key enciphered. In the user management functional block 110 of the control center 211 concerned, the secret key of the public-key crypto system of the above-mentioned control center 211 is taken out, and the session key enciphered [above-mentioned] with this secret key is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerned, decryption of a session key enciphered [above-mentioned] using the public key of the above-mentioned control center 211 is performed. Thus, the obtained session key (common key) is stored in the above-mentioned database section 112.
[0070]If the common key corresponding to the above-mentioned user ID comes to hand from the above-mentioned database section 112 and security ID comes to hand from the security ID generating function part 116, as shown in step ST33, In the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211, Further in [decrypt the data enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common key, and] the control function part 111, Comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned security ID generating function part 116 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed.
[0071]In the control center 211 which checked the justification of the above-mentioned access origin. Like step ST34, by the point generating function part 113 of

the user management functional block 110. The point information according to the contents of the data sent from the above-mentioned user terminal 50 is published, and the claim preparations to a user's settlement-of-accounts organization (financial institution 220) are made by the settlement-of-accounts claim function part 117.
[0072]Like step ST35, in the control function part 111, the control center 211 checks that there is no injustice in the balance and point usage information of point information from the player 1, and performs the conclusion of information for next processing. That is, a check and conclusion of whether there is any unjust use are performed from the balance of point information, and the number of the actually used point information. It is better to perform this check and conclusion desirably, although it must not carry out.
[0073]In the user management functional block 110 of the control center 211, like step ST36 after processing of above-mentioned step ST35 again, In the security ID generating function part 115, new security ID to the above-mentioned player 1 (user) is computed based on a random number generation, and above-mentioned security ID is enciphered with the above-mentioned point information in the control function part 110 further, for example. Encryption at this time is also performed using said session key (common key) sent beforehand from said player 1.
[0074]An end of the above-mentioned encryption will transmit the data which enciphered [above-mentioned] to the player 1 via the user terminal 50 under control of the control function part 131 like step ST25 of said drawing 9, and step ST8 of drawing 8 in the communication function section 133 of the controlling-function block 130 of the control center 211.
[0075]Then, in the communication function section 133 of the control center 211, like step ST38, When the processing completion sign from the user terminal 50 shown in step ST28 of said drawing 9 is received and decrypted, in the settlement-of-accounts claim function part 117 of the user management functional block 110 of the control center 211, like step ST39, The financial institution 220 is asked for settlement of accounts based on the processing completion sign concerned. The settlement-of-accounts claim to this financial institution 220 is performed from the communication function section 132 of the controlling-function block 130.
[0076]By the above, the flow of the processing in the control center 211 in the case of point purchase is completed.
[0077]From drawing 8 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 10, and the control center 211 can be expressed, as shown in drawing 11.
[0078]That is, in this drawing 11, input, such as said password and a point size, is transmitted from the user terminal 50 to the player 1 by the input transmission T1 like step ST2 of said drawing 8, and step ST22 of drawing 9.
[0079]In the prepared data transmission T2, the data created from the player 1 by said player 1 to the user terminal 50 is transmitted like step ST7 of said drawing 8, and step ST23 of drawing 9. In data transfer T3, the data which said player 1 created from the user terminal 50 to the control center 211 is transmitted like step ST24 of said drawing 9, and step ST31 of drawing 10.
[0080]In the data transfer T4, the data enciphered from the control center 211 to the user terminal 50 in the control center 211 is transmitted like step ST37 of said drawing 10, and step ST25 of drawing 9. In the transmission T5, the data from the control center 211 is transmitted to the user terminal 50 by the player 1 as it is like step ST25 of said drawing 9, and step ST8 of drawing 8.

[0081]In the processing completion sign transmission T6, the processing completion sign from the player 1 is transmitted to the user terminal 50 like step ST13 of said drawing 8, and step ST26 of drawing 9. In processing completion sign cryptogram transmission, the processing completion sign enciphered from the player 1 is transmitted to the control center 211 like step ST28 of said drawing 9, and step ST38 of drawing 10.
[0082]Next, it explains from drawing 12 flowing into the processing in the player 1 at the time of acquisition of the digital contents mentioned above, the user terminal 50, and the control center 211 using drawing 15, referring to drawing 2 and drawing 3.
[0083]The flow of the processing in the player 1 at the time of acquisition of digital contents is shown in drawing 12.
[0084]In this drawing 12, it is waiting for the controller 16 until starting of the software for digital contents acquisition beforehand installed in the user terminal 50, i.e., a personal computer, is performed like step ST41.
[0085]If the software for the above-mentioned digital contents acquisition rises, the controller 16 will receive the data which contains digital contents from the control center 211 via the user terminal 50 like step ST42. It has at least the digital contents enciphered with the contents key (a different common key for every contents) as having mentioned above the data received via the terminals 3 and 12 from the user terminal 50 at this time, and the content ID corresponding to the digital contents concerned. therefore, in order to use these enciphered digital contents, a contents key comes to hand from the control center 211 -- if it kicks, it will not become. The method of acquisition of this contents key is mentioned later.
[0086]The controller 16 which received the data from this user terminal 50 stores this data, i.e., the enciphered digital contents, in the memory medium connected to the I/O terminal 4 for memory media via the terminal 11 of the integrated circuit 10. Although various kinds of storages, such as a rewritable optical disc and semiconductor memory, can be considered as this memory medium, the thing in which random access is possible is desirable.
[0087]By the above, the flow of the processing in the player 1 at the time of acquisition of digital contents is completed.
[0088]Next, the flow of the processing in the user terminal 50 at the time of acquisition of digital contents is explained using drawing 13.
[0089]In this drawing 13, the user terminal 50 starts the software for digital contents acquisition in step ST51. If the software concerned rises, in this user terminal 50, the control center 211 of the address beforehand registered in step ST52 according to the software for the above-mentioned digital contents acquisition will be accessed.
[0090]At this time, the control center 211 concerned is exhibiting two or more digital contents using said virtual online shop 230. From the user terminal 50, the digital contents of the request according to the selection operation of the user out of two or more digital contents currently exhibited by this virtual online shop 230 in step ST53 are specified. That is, the user terminal 50 transmits the specification information on the contents for specifying the digital contents of the request in the digital contents exhibited by the virtual online shop 230 like step ST54 to the control center 211.
[0091]If the data which consists of data returned from the control center 211 according to the above-mentioned contents designation information, i.e., said enciphered digital contents, and content ID like step ST55 is received, The user terminal 50 concerned once stores the above-mentioned data in storing means, such as an inside, for example, a hard disk, and a memory, like step ST56.

[0092]Then, the user terminal 50 transmits the stored data (digital contents and content ID which were enciphered) concerned to the player 1 like step ST42 of said drawing 12.
[0093]By the above, the flow of the processing in the user terminal 50 at the time of acquisition of digital contents is completed.
[0094]Next, the flow of the processing in the control center 211 at the time of digital contents acquisition is explained using drawing 14.
[0095]The control center 211 shown in drawing 3 is making the virtual online shop 230 mentioned above exhibit two or more contents here. In the contents managing functional block 100 of control center 211 **, said virtual online shop 230 is generated and, specifically, two or more above-mentioned digital contents are exhibited to this virtual online shop 230.
[0096]Thus, in the state where digital contents are exhibited to the virtual online shop 230, contents designation information is received from the user terminal 50 like step ST61 of drawing 14 step ST54 of said drawing 13.
[0097]If the above-mentioned contents designation information is received from the user terminal 50 concerned, the control function part 101 of the contents managing functional block 100 will send this contents designation information to the controlling-function block 130. The control function part 131 of the controlling-function block 130 lets the communication function section 134 for right holders pass, and transmits the contents designation information received from the above-mentioned control controlling-function block 100 to said content provider 240. Thereby from the content provider 240 concerned, the digital contents demanded in the above-mentioned contents designation information are transmitted. The digital contents which came to hand from the above-mentioned content provider 240 are sent to the contents managing functional block 100 from the controlling-function block 130, and are inputted into this contents code and compression-ized function part 104. At this time, the control function part 101 sends the contents key which is generated in a contents key and the ID generating function part 103, and is stored in the database 102 to above-mentioned contents code and compression-ized function part 104. In this contents code and compression-ized function part 104, encryption using the above-mentioned contents key is given to the above-mentioned digital contents, and further predetermined compression processing is performed. The control function part 101 adds the content ID taken out from the database 102 to the digital contents by which above encryption and compression processing were carried out, and sends it to the controlling-function block 130. As predetermined compression processing in case digital contents are audio signals, For example, like what is called ATRAC (Adaptive TRansform Acoustic Coding) that is the art currently used in what is called MD (mini disc: trademark) produced commercially in recent years, processing which carries out highly efficient compression of the audio information in consideration of human being's aural characteristic was made into an example -- it can mention.
[0098]Then, as shown in step ST62 of drawing 14, the control section 131 of the controlling-function block 130 transmits the digital contents to which it let the communication function section 133 with a user terminal pass, and it enciphered [above-] and processed [compression-], and content ID was added to the above-mentioned user terminal 50.
[0099]The flow of the processing in the control center 211 at the time of digital contents acquisition is above.
[0100]From drawing 12 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow

of processing of drawing 14, and the control center 211 can be expressed, as shown in drawing 15.
[0101]That is, in this drawing 15, said contents designation information is transmitted from the user terminal 50 to the control center 211 like step ST54 of said drawing 13 by the input transmission T11. In the contents transfer T12, the digital contents and content ID which were enciphered are transmitted to the user terminal 50 like step ST62 of said drawing 14 from the control center 211.
[0102]In the contents transfer T13, the digital contents and content ID which were once stored in the user terminal 50 and which were enciphered [above-mentioned] are transmitted to the player 1 like step ST57 of said drawing 13, and step ST42 of drawing 12.
[0103]Next, it explains from drawing 16 flowing into the processing in the contents key which is needed when using the digital contents mentioned above, the player 1 at the time of acquisition of the service condition and the user terminal 50, and the control center 211 using drawing 19, referring to drawing 2 and drawing 3.
[0104]The flow of the processing in the player 1 at the time of acquisition of a contents key and a service condition is shown in drawing 16.
[0105]In step ST71 of this drawing 16, in the controller 16 of the player 1, it is waiting until starting of the software the contents key beforehand installed in the user terminal 50 and for service-condition acquisition is performed.
[0106]If the above-mentioned contents key of the above-mentioned user terminal 50 and the software for service-condition acquisition rise, the information inputted into the user terminal 50 according to the software concerned will be received like step ST72 via said interface terminal 3 for PC, and the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is information for requiring a contents key required to solve encryption of digital contents to appreciate. In this example, the specification information on the digital contents which use this contents key is used as demand information on the above-mentioned contents key.
[0107]The controller 16 which received this contents designation information from the above-mentioned user terminal 50, ID of the digital contents specified in the contents designation information concerned and security ID from the security ID generating circuit 19 are created, and this created data is made to encipher by the common code decoder circuit 24 in step ST73. The controller 16 adds the user ID read from the user ID storing memory 23 to the created data concerned, and transmits it to the user terminal 50 via the above-mentioned terminal 12 and the interface terminal 3 for PC. From this user terminal 50, the above-mentioned prepared data will be sent to the control center 211.
[0108]Since the common key encryption system is adopted also as encryption of the prepared data at this time as mentioned above, in advance of transmission of the prepared data concerned, generation of a common key is performed to it. For this reason, in the above-mentioned controller 16, a session key is generated as the above-mentioned common key from the security ID generating circuit 19 which is a random number generation means, for example. This common key (session key) will be sent from the player 1 to the control center 211 in advance of transmission of the above-mentioned prepared data. Since the common key concerned is that by which a code is carried out as mentioned above with a public-key crypto system, in the above-mentioned controller 16. The public key of the control center 211 currently beforehand kept by the key storage memory 21 for communication is taken out, and it sends to the above-mentioned open code decoder circuit 20 at the same time it sends

the session key which is the above-mentioned common key to the open code decoder circuit 20. Thereby by the open code decoder circuit 20 concerned, encryption of the above-mentioned common key (session key) is performed using the public key of the above-mentioned control center 211. Thus, the enciphered session key is sent to the control center 211 in advance of transmission of the above-mentioned prepared data.
[0109]Then, the controller 16 receives the enciphered data which has been sent from the control center 211 via the user terminal 50 in step ST75 so that it may mention later. The above-mentioned contents key, a service condition, security ID, etc. are enciphered as mentioning later the data sent from the control center 211 at this time.
[0110]If the data enciphered from the above-mentioned control center 211 is received, in the player 1, the data enciphered [above-mentioned] will be decrypted like step ST76, and the justification of the data will be checked. That is, the controller 16 evaluates the justification by checking security ID of the data decrypted [above-mentioned] by comparison with security ID from the above-mentioned security ID generating circuit 19.
[0111]Here, encryption is made with a public-key crypto system so that a contents key may be mentioned later, and about a service condition and security ID, encryption is made with the common key encryption system. Therefore, in order to decrypt the contents key concerned enciphered, The secret key of a public-key crypto system is required, and since the player inherent key is used as a secret key as mentioned above in the player 1 of this embodiment, the player inherent key concerned is taken out from the key storage memory 21 for communication. This player inherent key is sent to the open code decoder circuit 20 with the contents key enciphered [above-mentioned]. In this open code decoder circuit 20, the contents key enciphered [above-mentioned] is decrypted using the above-mentioned player inherent key. The contents key decrypted in this way is kept by the common key storage memory 22. On the other hand, in decrypting the service condition and security ID which are enciphered with the above-mentioned common key encryption system, These data is sent to the above-mentioned common code decoder circuit 24, and said common key which was generated previously and kept in the common key storage memory 22 is read, and, similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, the above-mentioned service condition and security ID are decrypted using the above-mentioned common key. The service condition decrypted in this way is stored in the point usage information storing memory 29. It is important here that the decrypted contents key and the service condition concerned are not taken out from the exterior of the player 1 concerned, the controller 16 specifically formed in the integrated circuit 10 of drawing 2 or the common key storage memory 22, and the point usage information storing memory 29 outside.
[0112]The controller 16 makes the contents key which decoded [above-mentioned] store in the above-mentioned common key storage memory 22 with the above-mentioned content ID like step ST77 after the check of the above-mentioned justification.
[0113]Then, the controller 16 creates the message which shows that the above-mentioned contents key came to hand in step ST78, This message is sent to the common key encryptosystem decoder circuit 24 like the above-mentioned, and said common key which was generated beforehand and kept in the common key storage memory 22 is read, and, similarly it sends to the common code decoder circuit 24. In the common code decoder circuit 24 concerned, a message is enciphered using the above-mentioned common key.

[0114]After encryption of the message concerned is completed, the controller 16 transmits this enciphered message to the user terminal 50 via the terminals 12 and 3 like step ST79. This enciphered message is made to transmit to the control center 211 after that.
[0115]By the above, the flow of the processing in the player 1 at the time of a contents key and service-condition acquisition is completed.
[0116]Next, the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is explained using drawing 17.
[0117]In this drawing 17, the user terminal 50 starts the software for a contents key and service-condition acquisition in step ST81. If the designation input demand of the contents of hope is performed and specification of contents is made from a user to the user who will operate the user terminal 50 concerned in step ST82 with this user terminal 50 according to the above-mentioned software if the software concerned rises, that specification information will be generated. The user terminal 50 transmits the specification information on the above-mentioned contents to the player 1 in the above-mentioned step ST83.
[0118]Next, if the data created and transmitted by the above-mentioned player 1 like step ST74 of said drawing 16 in step ST84 is received, the user terminal 50, The data transmitted from the player 1 concerned in step ST85 is transmitted to the control center 211 where the address is registered beforehand.
[0119]The user terminal 50 after performing a data transfer to the above-mentioned control center 211, If there is return of the data in which the contents key and service condition specified by the above-mentioned content ID from the control center 211 in waiting and step ST86, security ID, etc. were enciphered, the return from the control center 211, The data from the control center 211 concerned is transmitted to the player 1 as it is in step ST87.
[0120]The user terminal 50 after performing a data transfer to the above-mentioned player 1, The return from the player 1 in waiting and step ST88 like step ST79 of said drawing 16 from the player 1, If there is return of the message as which it was enciphered that the above-mentioned contents key came to hand, it will indicate that the above-mentioned contents key acquisition was completed to the display device connected to the user terminal 50 concerned in step ST89, and a user will be told.
[0121]Then, the message which was returned from the above-mentioned player 1 and which was enciphered [above-mentioned] is sent to the control center 211 in step ST90.
[0122]By the above, the flow of the processing in the user terminal 50 at the time of a contents key and service-condition acquisition is completed.
[0123]Next, the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is explained using drawing 18.
[0124]In this drawing 18, the communication function section 133 with the user terminal of the control center 211, The encryption data of the content ID transmitted to the user terminal 50 from the player 1 via ** in step ST91 like step ST74 of said drawing 16 and step ST85 of drawing 17, user ID, a message, and security ID is received. This received data is sent to the user management functional block 110.
[0125]The control function part 111 of the user management functional block 110 concerned, Based on the user ID added to the encryption data which received [above-mentioned], the common key for solving the encryption concerned is taken out from the database section 112, and the above-mentioned encryption data is decoded using this common key in a correspondence code and the function decoding part 114. The control function part 111 checks the justification of the data which was received [

above-mentioned] and decrypted using the user ID and security ID from the security ID generating function part 116 which were read from the database section 112.
[0126]The common key at this time is said session key beforehand sent from said player 1, and this session key is enciphered and sent with a public-key crypto system as mentioned above. Therefore, at the time of decoding of this session key enciphered. Like the above-mentioned, in the control center 211 concerned, the secret key of the public-key crypto system of the above-mentioned control center 211 is taken out, and the session key enciphered [above-mentioned] is decrypted using a secret key in a correspondence code / the function decoding part 114 concerned. Thus, the obtained session key (common key) is stored in the above-mentioned database section 112.
[0127]When the justification of the data which received [above-mentioned] is checked, the control function part 111, The contents key and service condition which were specified in the above-mentioned content ID to the contents managing functional block 100 are required, The control function part 101 of the contents managing functional block 100 which received the demand concerned reads the contents key and service condition which were specified in the above-mentioned content ID from the database section 102, and transmits them to the user management functional block 110. The control function part 111 sends these contents keys and a service condition to a correspondence code / function decoding part 114 with security ID, as shown in step ST93.
[0128]Here, encryption is made with the public-key crypto system mentioned above about the contents key, and encryption is made with the common key encryption system mentioned above about a service condition and security ID. Therefore, when enciphering the contents key concerned, the public key (public key beforehand stored corresponding to the player 1) of user side 200 is taken out from said database section 112 based on the above-mentioned user ID, and it is sent to a correspondence code / function decoding part 114. In a correspondence code / the function decoding part 114 concerned, the above-mentioned contents key is enciphered using the above-mentioned public key. On the other hand, when enciphering the above-mentioned service condition and security ID, the common key (session key) specified by the above-mentioned user ID is taken out from the above-mentioned database section 112, and it is sent to a correspondence code / function decoding part 114. In the correspondence code / function decoding part 114 at this time, the above-mentioned service condition and security ID are enciphered using the above-mentioned common key.
[0129]The contents key, the service condition, and security ID which were enciphered [above-mentioned] are sent to the controlling-function block 130, and are transmitted to the user terminal 50 from the communication function section 133 with a user terminal like step ST94. The data transmitted to this user terminal 50 will be sent to the player 1 via the user terminal 50 like step ST87 of said drawing 17, and step ST75 of drawing 16.
[0130]Reception of the encryption message which the control center 211 was generated by the player 1 like step ST79 of said drawing 16, and step ST90 of drawing 17, and was transmitted via the user terminal 50 Then, waiting, When the above-mentioned communication function section 133 receives the encryption message which the above-mentioned player 1 generated like step ST95, the control center 211 concerned, Like step ST96, the encryption message concerned is decrypted with a common key, and it checks that the above-mentioned player 1 has obtained the contents key and the service condition from the decoding message.

[0131]By the above, the flow of the processing in the control center 211 at the time of a contents key and service-condition acquisition is completed.
[0132]From drawing 16 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 18, and the control center 211 can be expressed, as shown in drawing 19.
[0133]That is, in this drawing 19, said contents designation information is transmitted from the user terminal 50 to the player 1 like step ST83 of said drawing 17 by the contents-designation-information transmission T21. In the prepared data transmission T22, the data created by the player 1 is transmitted to the user terminal 50 like above step ST74. In the prepared data transmission T23, the data created by the above-mentioned player 1 from the user terminal 50 concerned is transmitted to the control center 211. In the enciphered data sending T24, the data enciphered in the control center 211 is sent to the user terminal 50 like step ST94 of said drawing 18, and the enciphered data concerned is further sent to the player 1 by the enciphered data sending T25.
[0134]In the message transfer T26, like step ST79 of said drawing 16, In the data sending T27 as which the data which enciphered the message which shows the completion of contents key acquisition was transmitted to the user terminal 50 from the player 1, and was enciphered further, the message enciphered from the above-mentioned player 1 is sent to the control center 211 from the user terminal 50.
[0135]Next, in the player 1 which received point information, digital contents, and a contents key as mentioned above, it explains flowing into the processing at the time of actually appreciating digital contents using the user terminal 50 using drawing 20, referring to drawing 2.
[0136]Here, it is assumed that the memory medium said digital contents were remembered to be is connected to the terminal 4 of the player 1.
[0137]In this state, the digital contents which wish to appreciate from the user terminal 50 are specified to the player 1 concerned like step ST101. At this time, the specification concerned is made, when a user operates the user terminal 50, for example.
[0138]Like step ST102, according to the contents designation information from the above-mentioned user terminal 50, the controller 16 of the player 1 performs access to the above-mentioned memory medium, and reads ID of contents at this time.
[0139]Based on the content ID read in the above-mentioned memory medium, the above-mentioned controller 16 like step ST103, It accesses to said common key storage memory 22, and it checks whether the contents key is stored, and accesses to said point usage information storing memory 29, and it is checked whether the service condition is stored.
[0140]When it checks here that the above-mentioned contents key and the service condition are not stored in the above-mentioned common key storage memory 22 or the point usage information storing memory 29, the controller 16, The information on the purport that the contents key concerned etc. do not exist to the user terminal 50 is sent, and this displays the message which stimulates acquisition of the above-mentioned contents key etc. on said display device from the user terminal 50. In this case, it carries out like the flow chart for contents key acquisition mentioned above, and a contents key etc. come to hand. Thus, when a contents key etc. newly come to hand, as mentioned above in step ST104, the contents key which are enciphered is decrypted.

[0141]Next, the controller 16 checks whether there is any enough balance of the point information stored in the point information storing memory 28 based on the service condition decrypted [above-mentioned], as shown in step ST105. When the balance of the above-mentioned point information stored in the above-mentioned point information storing memory 28 is insufficient, The information on the purport that the balance of the point information concerned is insufficient is sent from the controller 16 to the user terminal 50, and, thereby, the user terminal 50 displays the message which stimulates acquisition of the above-mentioned point information on said display device. In this case, it carries out like a flow chart for point access to information which was mentioned above, and point information comes to hand.
[0142]When actually appreciating digital contents, here the controller 16, According to the digital contents concerned to appreciate, a point information number is reduced from the above-mentioned point information storing memory 28 like step ST106, Furthermore, the new point usage information according to the condition of use of the point information concerned is stored in the point usage information storing memory 29 (point usage information is updated). Thus, as point usage information newly stored to the point usage information storing memory 29, they are the right holder information corresponding to the digital contents which appreciated [above-mentioned], including owner of a copyright etc., information, other information on the reduced point information number, etc.
[0143]Then, the controller 16 will read digital contents from a memory medium, if it checks that the processing for fee collection of the cut of these point information, new storing of point usage information, etc. has been completed like step ST107.
[0144]Since the digital contents read from this memory medium are enciphered, the controller 16 transmits the digital contents enciphered [above-mentioned] to the common code decoder circuit 24 like step ST109.
[0145]In this common code decoder circuit 24, the digital contents enciphered [above-mentioned] are decrypted like step ST110 using the contents key which decrypts previously and is kept by the common key storage memory 22 based on the directions from the controller 16.
[0146]Since predetermined compression processing is made as mentioned above, these digital contents the controller 16, The digital contents by which the above-mentioned code was decrypted and by which compression processing is carried out [above-mentioned] are made to transmit to the expansion circuit 26 from the above-mentioned common code decoder circuit 24 like step ST111, and the elongation processing corresponding to the above-mentioned predetermined compression processing is made to perform here.
[0147]Then, the elongated digital contents concerned, Like step ST112, it is changed into an analog signal in the D/A conversion circuit 27, and is outputted outside (for example, user terminal 50 grade) like step ST113 via the terminal 13 of the integrated circuit 10, and the analog output terminal 2 of the player 1 concerned.
[0148]By the above, the flow of the processing in the player 1 at the time of contents appreciation is completed, and the appreciation of digital contents of a user is attained.
[0149]Next, the point usage information newly stored in the point usage information storing media 29 of said player 1 with appreciation of digital contents which were mentioned above, It explains flowing into the processing in the player 1 at the time of returning to the control center 211, the user terminal 50, and the pipe center 310 using drawing 24 from drawing 21, referring to drawing 2 and drawing 3.

[0150]The flow of the processing in the player 1 at the time of point usage information return is shown in drawing 21.
[0151]In this drawing 21, it waits for the controller 16 until starting of the software for point usage information return beforehand installed in the user terminal 50 is performed, as shown in step ST121.
[0152]If the software for the above-mentioned point usage information return of the above-mentioned user terminal 50 rises, the information inputted into the user terminal 50 according to the software concerned will be received like step ST122 via said interface terminal 3 for PC, and the terminal 12 of the integrated circuit 10. The input supplied from the above-mentioned user terminal 50 at this time is a password etc. which are entered by the user.
[0153]The controller 16 which received this contents designation information from the above-mentioned user terminal 50, The password supplied from the user terminal 50 concerned in step ST123 is compared with the password stored in the password storing memory 14, and the password concerned carries out the right check of how.
[0154]When it is checked that it is a right password in the check of the above-mentioned password, the controller 16, The balance of the point information stored in the point information storing memory 28 and the point usage information stored in the point usage information storing memory 29 are read like step ST124, respectively, and these information is enciphered.
[0155]After the balance of the above-mentioned point information and encryption of point usage information are completed, the controller 16 is attached to the data which read user ID from the user ID storing memory 23, and enciphered [above-mentioned] like step ST125.
[0156]The data in which this user ID was attached is transmitted to the user terminal 50 via the terminal 12 and the interface terminal 3 for PC like step ST126 from the controller 16. This data is transmitted to the control center 211 after that.
[0157]As mentioned above also in the encryption at this time, the common key encryption system is adopted. That is, in advance of transmission of the data concerned, generation of a common key is performed like the above-mentioned, it is enciphered with said public-key crypto system (encryption using the public key of the control center 211), and this generated common key is sent to the control center 211 with user ID.
[0158]After transmitting data to the user terminal 50 as mentioned above, the controller 16 waits to transmit the data later mentioned from the above-mentioned control center 211 via the user terminal 50.
[0159]When the data from the above-mentioned control center 211 is received like step ST127, here in the player 1. The received data enciphered using the common key encryption system are decrypted like step ST127 using a common key like the above-mentioned, and the justification of the data is checked. That is, the controller 16 evaluates the justification by checking security ID of the data decrypted [above-mentioned] by comparison with security ID from the above-mentioned security ID generating circuit 19.
[0160]The message of the processing completion enciphered using the above-mentioned common key is also contained in the data transmitted from the above-mentioned control center 211. Therefore, the controller 16 after the check of above-mentioned security ID is completed, Send the processing completion message enciphered [above-mentioned] to the common code decoder circuit 24, the decryption using a common key is made to perform here, and it is checked that

processing in the above-mentioned control center 211 has been completed by receiving this decrypted processing completion message.
[0161]By the above, the flow of the processing in the player 1 at the time of point usage information return is completed.
[0162]Next, the flow of the processing in the user terminal 50 at the time of point usage information return is explained using drawing 22.
[0163]In this drawing 22, the user terminal 50 starts the software for point usage information return in step ST131. When the software concerned rises, in this user terminal 50. If input requests, such as a password, are performed and the input of a password is made from a user to the user who operates the user terminal 50 concerned in step ST132 according to the above-mentioned software, the password will be transmitted to the player 1.
[0164]Next, if the data created and transmitted by the above-mentioned player 1 like step ST126 of said drawing 21 in step ST133 is received, the user terminal 50, The data transmitted from the player 1 concerned in step ST134 is transmitted to the control center 211 where the address is registered beforehand.
[0165]The user terminal 50 after performing a data transfer to the above-mentioned control center 211 will transmit the data concerned to the player 1 as it is, if the data in which the return from the control center 211 is sent from the control center 211 to the player 1 in waiting and step ST135 is received.
[0166]The user terminal 50 after performing a data transfer to the above-mentioned player 1 performs the display for making a user know that processing was completed to a display device, and receives the check from a user.
[0167]By the above, the flow of the processing in the user terminal 50 at the time of point usage information return is completed.
[0168]Next, the flow of the processing in the control center 211 at the time of point usage information return is explained using drawing 23.
[0169]In the communication function section 133 with the user terminal of the control center 211, the data of the point usage information etc. which have been transmitted by step ST126 of said drawing 21 and step ST134 of drawing 22 from the player 1 via said user terminal 50 is received like step ST141.
[0170]When this data is received, the user management functional block 110 of the control center 211, The common key which is beforehand received from the database section 112 like the above-mentioned, and is stored under control of the control function part 111 like step ST142 based on the user ID attached to the received data concerned comes to hand, and security ID comes to hand.
[0171]If the common key and security ID corresponding to the above-mentioned user ID come to hand from the above-mentioned database section 112, as shown in step ST143, In the correspondence code / function decoding part 114 of the user management functional block 110 of the control center 211, Further in [decrypt the data of the point usage information etc. which were enciphered / above-mentioned / from the above-mentioned player 1 using the above-mentioned common key, and] the control function part 111, Comparison with security ID in the decrypted data concerned and security ID read from the above-mentioned database section 112 performs content confirmation of whether to be a user with the just user side 200 (player 1) who has accessed.
[0172]The data after the check of the above-mentioned justification and the contents is transmitted to the usage information controlling-function block 120. The control function part 121 of this usage information controlling-function block 120, As shown in step ST144, it is checked whether there is any injustice in use of above-mentioned

user side 200 using the information stored in the database section 122 using the balance and point usage information of point information which have been sent from the above-mentioned player 1. Simultaneously, when [concerned / unjust] it comes and things are checked, the operation which summarizes the balance and point usage information of point information in the usage information calculation function part 123 is performed.

[0173]Then, the control function part 111 of the user management functional block 110 controls the security ID generating function part 116, makes security ID compute, controls the confirmation message generating function part 115 further, and makes the message of processing completion generate, as shown in step ST145. These security ID and a processing completion message are enciphered using said common key in the correspondence code / function decoding part 114 of the user management functional block 110.

[0174]The data which was enciphered [above-mentioned] and generated will be sent to the user terminal 50 from the communication function section 133 with a user terminal, as shown in step ST146, and it will be transmitted to the player 1 from the user terminal 50 concerned like step ST135 of said drawing 22, and step ST127 of drawing 21.

[0175]By the above, the flow of the processing in the control center 211 at the time of point usage information return is completed.

[0176]From drawing 21 mentioned above, the sequence of the information transmission and reception between the player 1 and the user terminal 50 in the flow of processing of drawing 23, and the control center 211 can be expressed, as shown in drawing 24.

[0177]That is, in this drawing 24, the input of said password is transmitted from the user terminal 50 to the player 1 like step ST132 of said drawing 22 by the input transmission T31. In the prepared data transmission T32, the data which the player 1 created is transmitted to the user terminal 50 like step ST126 of said drawing 21. In the prepared data transmission T33, the data created by the above-mentioned player 1 is transmitted to the control center 211 from the above-mentioned user terminal 50 like step ST134 of said drawing 22. In the data transfer T34, the data created in the control center 211 is transmitted to the user terminal 50 like step ST146 of said drawing 23. In the data transfer T35, the data created in the control center 211 is transmitted to the player 1 via the user terminal 50 like step ST127 of said drawing 21.

[0178]Actual operation of the player 1 of the system of this embodiment, the user terminal 50, and the control center 211 serves as a flow which was mentioned above.

[0179]So far, although the flow of processing of the whole in the system of this embodiment has been explained, operation of each of the principal part of the system of this embodiment is explained in detail after this.

[0180]First, explanation about operation of the encryption and compression in this invention embodiment, and extension and decryption is given.

[0181]Like the system of an embodiment mentioned above, when distributing digital contents using a network, in order to stop the data volume, compression/extension art is used, and encryption/compression technology is used for anti-copying or fee collection. That is, compressing digital contents and carrying out encryption processing further by the distribution side (an above-mentioned example the control center 211 side), is performed. When distributing the digital contents (encryption/compressed data) generated at the transmitting side (control center 211 side) like an above-mentioned example using a network, In a receiver (an above-

mentioned example player 1), decrypting, after receiving the digital contents which were above-enciphered and were compressed, elongating further, and restoring digital contents is performed. The turn of processing of the above-mentioned encryption, compression and decryption, and extension may interchange.
[0182]When copyright etc. exist in the above-mentioned digital contents, when the above-mentioned receiver elongates the above-mentioned digital contents with the above-mentioned decryption, it will be charged according to intention of the above-mentioned owner of a copyright etc. Although this fee collection is performed by mainly purchasing, the key, i.e., the contents key, of decryption, it is in the method of purchasing this contents key variously.
[0183]Here, as mentioned above, when procedure which compresses digital contents, is enciphered, is decrypted and is elongated is followed, the user who had bad faith, for example can obtain comparatively easily the compressed data decrypted [above-mentioned]. Namely, the compressed data of digital contents, Generally capacity is large, therefore For example, since not an internal memory but the ** value of a common contents playback device of a receiver are accumulated in external memory in many cases, It is because it is easy to take out unjustly the digital contents compressed [above-mentioned] by the connection section with direct or external memory from this external memory.
[0184]What cannot be processed if the algorithm of the expansion system to compression is hidden like the key of a code general to the algorithm of an expansion system, respectively being opened to the public in many cases does not exist. And as compared with the digital contents by which the encryption distributed from the above-mentioned transmitting side and compression were made, **** which distributes the compression digital contents which did not change in data volume, therefore were decrypted [above-mentioned] with bad faith is also easy for the compression digital contents decrypted [above-mentioned]. Namely, according to the method which is enciphered and distributes digital contents after compressing [above-mentioned]. The danger that the compression digital contents which can elongate anyone easily will be distributed further in the place which a theft is easily carried out to a user with bad faith, and intention of an owner of a copyright etc. does not reach for this reason, or will be elongated is large.
[0185]So, in the embodiment of the invention, in order to make it possible to raise the safety of the digital contents distributed using a network in view of such a situation, in the player 1 of above-mentioned drawing 2, processing as shown in the flow chart of the following drawing 25 is performed.
[0186]Namely, in the decoding processing in the common code decoder circuit 24 of the player 1 of drawing 2, and the elongation processing in the above-mentioned expansion circuit 26. The data of the digital contents by which compression processing was carried out with the encryption read from said memory medium like step ST151, First, it divides into the unit of the least common multiple lcm (X, Y) of the batch X bit of the algorithm of decoding processing, and the algorithm batch Y bit of elongation processing.
[0187]Next, as the data of digital contents in which the above-mentioned encryption divided into the unit of the above-mentioned least common multiple lcm (X, Y) and compression processing are made is shown in step ST152, decoding processing is performed by the above-mentioned common code decoder circuit 24 for every unit of the least common multiple lcm (X, Y) concerned.
[0188]As the data of digital contents in which the unit of the least common multiple lcm (X, Y) obtained by the decoding processing concerned is compressed is shown in

step ST154, elongation processing is performed to all the compressed data for the unit concerned in the above-mentioned expansion circuit 26.
[0189]Then, the decryption and elongation processing for every unit of this least common multiple lcm (X, Y) are continued until the processing about all the data of digital contents by which compression processing was carried out with the above-mentioned encryption is completed. . Namely, judgment whether the decryption and elongation processing for every unit of the least common multiple lcm (X, Y) were completed to all the data of digital contents should do to be shown in step ST155. When not having completed and it returned and completes to step ST152, the flow chart of the processing concerned is completed.
[0190]The digital contents by which all the data was decrypted and elongated by this will be obtained.
[0191]Although the decoding data of the above-mentioned least-common-multiple lcm (X, Y) unit will exist, the data volume of the decoding data concerned also has little processing of the flow chart of drawing 25 in the player 1 concerned. For this reason, a possibility of being stolen like [in the case of saving at external memory which can be saved at an internal memory with high safety even if comparatively expensive, therefore was mentioned above] will become very low.
[0192]In the above-mentioned player 1 in this embodiment, the buffer memory 25 of drawing 2 is formed as an internal memory for securing the above-mentioned safety between the above-mentioned common code decoder circuit 24 and the expansion circuit 26. That is, this buffer memory 25 is formed in the integrated circuit 10 of one chip, and it is hard to be accessed from the outside, therefore data is not taken out outside.
[0193]In an above-mentioned flow chart, are made to perform decryption and elongation processing to all the data for the unit of the least common multiple lcm (X, Y), and as specific constitution for it, For example, the data of digital contents is first divided into the batch X bit of the algorithm of decoding processing like composition of being shown in drawing 26, By performing decoding processing to the data of this X bit, gathering the data in which the X bit concerned by which decoding processing was carried out is compressed after that by the algorithm batch Y bit of elongation processing, and elongating the compressed data of the Y bit concerned. It is made to realize the decryption and elongation processing in the unit of the least common multiple lcm (X, Y) as mentioned above.
[0194]The common code decoder circuit 24 of the player 1 which realizes this consists of the input part 30 and the code decoding part 31, and the above-mentioned expansion circuit 26 consists of the expanding part 32 and the outputting part 33. Said buffer memory 25 is formed between these common code decoder circuit 24 and the expansion circuit 26.
[0195]If encryption processing to the above-mentioned digital contents is performed as a more concrete example here for example, using the DES (Data Encription Standard) code, The encryption processing concerned and decoding processing corresponding to it will be performed by 64 bitwises.
[0196]In the case of the elongation processing to the compressed digital contents, it changes also with the compression ratios and sampling frequencies, but under the present circumstances, it is processed per 1K - 2 K bits/channel in many cases. Here, it is assumed that it is processed for every 1.28K bit for convenience.
[0197]Therefore, in the case of the system using the above-mentioned DES cipher system and the compression expansion system for every above-mentioned 1.28K bit, the above-mentioned least common multiple lcm is set to 1.28K.

[0198]Said digital contents enciphered and compressed are inputted into the input part 30 of the basis of such conditions, and the common code decoder circuit 24 of drawing 26. In the input part 31 concerned, the digital contents which were enciphered [above-mentioned] and compressed are divided into [every batch X bit of the algorithm of the above-mentioned decoding processing], i.e., 64 bits, data, and are outputted to the code decoding part 31.
[0199]In this code decoding part 32, decoding processing of the above-mentioned X bit, i.e., 64 bits, data is carried out concerned every 64 bits. The 64 bits [which was obtained by the decryption in this every 64 bits] data compressed is sent to the buffer memory 25.
[0200]When the compressed data for the algorithm batch Y bit of elongation processing, i.e., a 1.28K bit, accumulates according to the directions from said controller 16, the buffer memory 25 concerned, The compressed data for the 1.28K bit concerned is outputted collectively, and this compressed data is sent to the expanding part 32 of the above-mentioned expansion circuit 26.
[0201]The above-mentioned expanding part 26 elongates the compressed data for the 1.28K bit inputted [above-mentioned], and outputs it to the outputting part 33.
[0202]The controller 16 controls processing of the decoding section 31, and processing of the expanding part 32, monitoring the data volume which accumulated in the buffer memory 25.
[0203]If 20 pieces (= 1280/64) are parallel in decoding processing if it is this case, and it processes, it will become a more nearly high-speed processing system.
[0204]In addition, when performing not hardware constitutions like said drawing 2 or drawing 26 but processing mentioned above with the programmable device, the controller 16 will process based on a decoded program or an extension program, corresponding to the situation of the buffer memory 25.
[0205]Although the digital contents enciphered after compressing were supplied to the player 1 and the example elongated after decrypting these digital contents compressed and enciphered was given by the player 1 by above-mentioned explanation, Even if it is a case where the compressed digital contents are elongated and decrypted after enciphering, the same effect as **** can be acquired.
[0206]The algorithm of compression / extension, and encryption/decryption is not limited, and this invention is effective to any methods.
[0207]Thus, according to this invention, the safety of the digital contents distributed using a network improves.
[0208]Next, explanation about generating operation of said security ID is given.
[0209]As point information comes to hand beforehand and being mentioned above like this embodiment in the case of a method which reduces the point information concerned according to appreciation of digital contents, After the control center 211 on a network performs checks as arbitrary after receiving communication of a purchase request of the point information from the user terminal 50 of user side 200 as financial institution 220 and others, it enciphers the point information and sends it to the player 1 of user side 200 via a network.
[0210]In the case of a method which obtains point information beforehand and reduces the point information concerned like this embodiment according to appreciation of digital contents, between the control center 211 and the player 1 (user terminal 50), an exchange of the data same each time as the degree of the purchase of point information -- carrying out (for example, the information of "the point information on 3000 cyclotomies" corresponding to "3000 supplement demand of the point information on a cyclotomy" and it which were enciphered is exchanged) -- it is

based on those who have bad faith, for example. The amount-of-money supplement depended for what is called "impersonating" to the financial institution 220 serves as a problem. "Impersonating" to the financial institution which says here means what a person with the above-mentioned bad faith impersonates an original user (this embodiment user side 200), and obtains point information unjustly.
[0211]Namely, if the data same each time as the degree of the purchase of point information is exchanged, For example, a person with bad faith robs a communication line of the data concerned, and the same data is generated, In the case as the destination is made into itself (person with bad faith) to the control center 211 and acquisition of point information was requested. A person with the bad faith concerned can obtain point information, and the claim of the purchase price of this point information has further a possibility that the problem that it will be made by original user side 200 may occur.
[0212]Then, in order to prevent such injustice, in the system of this invention embodiment, the random number generated by the random number generation function which has interlocked beforehand by both a receiver (player 1 side) and the distribution side (control center 211 side) is used for the improvement in safety. According to this embodiment, said security ID is generated as the above-mentioned random number. What is necessary is to initialize the timer 18, for example and just to synchronize operation between both, for example in the cases, such as a user's registration procedure, in order to interlock a random number generation among both.
[0213]That is, the operation at the time of the player 1, for example, point access to information, from the control center 211 at the time of using this random number (security ID) serves as the following flows.
[0214]The data sent from the control center 211 to the player 1 is made with the data which consists of security ID generated [above-mentioned] with the point information enciphered using the common key (session key) which came to hand beforehand from the player 1 as mentioned above at the time of the purchase of point information.
[0215]The controller 16 of the player 1 is sent to the common code decoder circuit 24, as the data received from the control center 211 concerned was mentioned above, and it performs decoding processing here using said common key. By this, the point information and security ID which have been sent from the control center 211 will be obtained.
[0216]Then, the controller 16 of the player 1 compares security ID sent from the above-mentioned control center 211 with security ID generated in the own security ID generating circuit 19. In this comparison, the controller 16 stores in said point information storing memory 28 the point information sent from the above-mentioned control center 211, only when security ID from the control center 211 and security ID which the above itself generated are in agreement.
[0217]By this, only the player 1 of valid-user side 200 can obtain point information. the malicious person who in other words has the player 1 of valid-user side 200, and the same player -- said -- impersonating, even if it is going to obtain point information unjustly, Since security ID of the player which the person of the bad faith concerned has, and security ID sent from the above-mentioned control center 211 are not in agreement, the person with this bad faith will not get said inaccurate point access to information depended for impersonating.
[0218]Of course, security ID generated in the player 1 of user side 200, The security ID generating circuit 19 provided in the integrated circuit 10 of the player 1 concerned

occurs, and since it is what cannot be taken out outside, a person with bad faith cannot steal the security ID concerned.
[0219]Although some are various in the composition which generates the random number as above-mentioned security ID, the example is shown in drawing 27. The composition of this drawing 27 is one example of the security ID generating circuit 19 of said drawing 2.
[0220]In this drawing 27, the one-way function generating part 40 generates what is called a one-way nature function. The inverse function is far difficult for calculation with a function with the above-mentioned one-way nature function comparatively easy to calculate. It receives by secret communication etc. beforehand and this one-way function can also be saved at the one-way function generating part 40 concerned. The one-way function generating part 40 can also be made to generate the above-mentioned one-way function by making into an input function the hour entry from the timer 18 established in the integrated circuit 10 of said drawing 2. The above-mentioned one-way function is sent to the random number deciding part 43.
[0221]The number generating part 41 of users generates the predetermined number of users defined for every user. This number of users is beforehand sent by secret communication etc., and is saved at the number generating part 41 of users concerned. The user ID which said user ID storing memory 23 stores, for example can also be used for this number of users.
[0222]The random number database 42 stores a random number, and stores 99 random numbers.
[0223]The time communication storage parts store 44 memorizes the time communication information sent, for example from the controller 16. This time communication information is information which shows the time communication between the player 1 and the control center 211.
[0224]These one-way functions, the number of users, and time communication information are sent to the random number deciding part 43. The random number deciding part 43 concerned generates the random number of the range beforehand memorized by the random number database section 42 from the above-mentioned one-way function and the number of users, for example based on the hour entry from said timer 18 (for example, 99 pieces).
[0225]Namely, if the above-mentioned time communication information is the communication which is the 1st time in this random number deciding part 43, The 99th random number is taken out from the above-mentioned random number database section 42, and if for example, time communication information is the communication which is the n-th time, the 100-n-th random numbers will be picked out from the above-mentioned random number database 42, and this taken-out random number is outputted as said security ID.
[0226]The composition of this security ID generating has the same thing in the player 1 and the control center 211.
[0227]When finishing using all the random numbers stored in the random number database section 42, In the above-mentioned random number deciding part 42, 100 pieces - the 199th random number are calculated, or secret communication of a new random number and unidirectional function is carried out, and it re-stores in the random number database section 42, or, on the other hand, reconstructs to the tropism function generation part 40.
[0228]Although a random number (security ID) is generated and he is trying to improve the safety for every communication in the explanation mentioned above, According to this embodiment, since he is also trying to generate programmably a

common key (session key) different each time whenever it communicates between user side 200 and the control center 211 side as mentioned above, safety is improved further.

[0229]Here, the above-mentioned random number is inserted about the transmission sentences (for example, message etc.) actually transmitted, and signs that encryption by a session key is made, and signs that a random number is taken out from a receiving sentence and the check of justification is made are explained using drawing 28 and drawing 29. He is also trying to add a signature (digital signature) to a transmission sentence in the example of these drawing 28 and drawing 29.

[0230]In this drawing 28, first, as a flow which enciphers said common key with a public-key crypto system, and transmits, it generates as a common key which uses said session key for communication, and this common key is enciphered by the public key of a receiver to the public-key-encryption chemically-modified degree P8 by the common key generating process P7 for communication. This enciphered common key is sent to a receiver.

[0231]On the other hand, as a flow in the case of enciphering the message as a transmission sentence with a common key encryption system, and transmitting, in the message generation distance P1, the message M is generated and a random number (said security ID) is generated at the random number generation process P5, for example. These messages M and a random number are sent to the common key encryptosystem chemically-modified degree P6. In the common key encryptosystem chemically-modified [this] degree P6, the above-mentioned message M and a random number are enciphered using the common key by which it was generated at the above-mentioned common key generating process P7 for communication.

[0232]When adding the above-mentioned digital signature, the above-mentioned message M is sent to the hash value calculation process P2. In the hash value calculation process P2 concerned, what is called a hash value is calculated from the above-mentioned message M. A hash value is address information called for by a hash method, and a hash method performs a predetermined operation to some contents (keyword) of data (in this case, the message M), and uses that result for it as an address. The hash value (M) generated from this message is sent to the secret key cryptosystem chemically-modified degree P4 as a digital signature. In the secret key cryptosystem chemically-modified [this] degree P4, the above-mentioned digital signature is enciphered with the secret key of the transmitting side. This enciphered digital signature is sent to the common key encryptosystem chemically-modified degree P6. This enciphers the above-mentioned digital signature in the common key encryptosystem chemically-modified degree P6 using the common key by which it was generated at the above-mentioned common key generating process P7 for communication.

[0233]These messages M, a digital signature, and a random number are transmitted to a receiver.

[0234]Next, the flow of processing by the receiver corresponding to drawing 28 is explained using drawing 29.

[0235]In this drawing 29, the common key transmitted from the above-mentioned transmitting side is first decrypted with the secret key of the receiver concerned at the secret key decryption process P11 as a flow which decrypts said common key with a public-key crypto system.

[0236]At the common key decoding process 13, the message M transmitted [above-mentioned] is decrypted using the common key decrypted at the above-mentioned secret key decryption process P11 as a flow which, on the other hand, decrypts the

message M enciphered with said common key encryption system. This decrypted message M will be sent to other processes by the other functional transmission processes P20.
[0237]The hash value which decodes a digital signature and which flowed and was decrypted at the above-mentioned common key decryption process P13 is decrypted using the public key of the transmitting side at the public key decryption process P14. Simultaneously, in the hash value calculation process P17, a hash value is calculated from the above-mentioned message M. The check of the hash value decrypted by these public key decryption process P14 and the hash value calculated by the above-mentioned hash value calculation process P17 being compared, and not being altered by the comparison process P19, is performed.
[0238]About the transmitted random number, the random number decrypted at the above-mentioned common key decryption process P13 and the random number generated at the random number generation process P21 of the receiver concerned are compared by the just exact private seal process P22, and the check of justification is performed.
[0239]By the way, in the system of this embodiment shown in drawing 1 mentioned above, the system management company 210, the virtual online shop 230, and the content provider 240 are formed as a system side to user side 200. The financial institution 220 of drawing 1 is an external bank etc., for example.
[0240]The control center 210 of the above-mentioned system management company 210, Exhibition of digital contents and management of distribution in the virtual online shop 230, between the financial institutions 220 -- the main work by the side of systems, such as collection of the accounting information of user side 200, or a variety of information, distribution and those managements, encryption of the digital contents from the content provider 240, and a security management of the information to treat, -- all are performed mostly.
[0241]However, in the system which distributes digital contents using a network which was mentioned above, In the time of the user side obtaining digital contents from the system side, and the case of the fee collection accompanying use of digital contents, communication will concentrate on the system side and there is a possibility that a satisfying response may no longer be obtained to the user side.
[0242]So, in other embodiments of this invention, it makes it possible to prevent concentration of communication which was mentioned above and to raise a communicative response by the function of the system management company 210, and more specifically dividing the function of the control center 211 as follows.
[0243]Namely, the content exhibiting distributing institution 310 which has a function which exhibits digital contents and distributes the composition by the side of the system to user side 200 in other embodiments of this invention as shown in drawing 30, Accounting information control machine Seki 320 which has the function to manage the accounting information of the user of a fixed area, It divides into the data generation of enciphering digital contents, distribution of generated data to the above-mentioned content exhibiting distributing institution 310, the information gathering from above-mentioned accounting information control machine Seki 320, division of earnings, and the system management organization 330 that has the function to perform the security management and others of the whole system, User side 200 and communication are independently attained for each organization 310,320,330, respectively.
[0244]In composition like this drawing 30, the content exhibiting distributing institution 310 is scattered on the network in the world, two or more arrangement is

possible for it, and if even communication charges are paid, it can access user side 200 to the content exhibiting distributing institution 310 of every area. For example, when user side 200 wants for digital contents to come to hand, the above-mentioned content exhibiting distributing institution 310 is accessed from user side 200, and digital contents come to hand. Digital contents [which were enciphered by the system management organization 330], i.e., user, side 200 will be the digital contents at this time in the state which can be transmitted directly using a network.

[0245]Holding not much many users installs accounting information control machine Seki 320 for a moderate number of every users undesirably therefore on safety management in order to treat accounting information. However, since the attack point (accounting information control machine Seki 320) from the 3rd person with bad faith will be increased and it will be traded off if it installs not much mostly, optimizing is desirable. For example, when user side 200 performs communication about fee collection, it accesses from user side 200 to above-mentioned accounting information control machine Seki 320.

[0246]The above-mentioned system management organization 330 Subscription to a user's system, and registration of means of settlement, Profits distribution to the profits beneficiary of the collection of money from a user, said right holder, the content exhibiting distributing institution 310, and accounting information control machine Seki 320 grade, etc. raise security by carrying out by summarizing management of important information on security. However, as for the system management organization 330 concerned, it is desirable not to necessarily establish one place in the world and to install in a certain settled unit, for example, the unit of a country etc. For example, when user side 200 performs important communication on [, such as subscription to this system, and registration of means of settlement,] security, it carries out by accessing from user side 200 to the above-mentioned system management organization 330. The system management organization 330 concerned which obtained information performs profits distribution to the collection of money and the profits beneficiary from the user concerned collectively from above-mentioned accounting information control machine Seki 320. It is supplied to the system management organization 330 concerned, the source data, i.e., the contents, which an owner of a copyright etc. have, they are changed into the digital contents by which encryption etc. were made here, and are distributed to the above-mentioned content exhibiting distributing institution 310.

[0247]As mentioned above, by distributing the function by the side of a system to the three organizations 310,320,330, and making direct access of it possible between user side 200 and each organization 310,320,330, communicative concentration is prevented and it becomes possible to raise a communicative response. According to the content exhibiting distributing institution 310, it can respond also to a thing like what is called an existing virtual Mall, and it is effective also in sales promotion and attractive for a user. By dividing accounting information control machine Seki 320 independently, it is useful for the dishonesty prevention which conspired with exhibition and the selling function of contents. In order that a fixed number may obstruct the user who manages, the controlling function who receives unjustly is also more effective.

[0248]In the system of other embodiments of this invention shown in drawing 30 mentioned above below, It explains that the accounting information accompanying the information flow at the time of acquisition of the contents key subscription to a user's system, the purchase of point information, and for decoding of the enciphered

digital contents, etc., the flow in the case of circulation of the information for contents and contents appreciation, and use of contents flows.
[0249]First, the principal part of the flow of the time of subscription to a user's system is explained using drawing 31.
[0250]In the case of the subscription registration to a user's system, the following procedures depended on the user subscription support functional block 402 of the system management organization 330 follow, and registering operation is performed at it.

[0251]From user side 200 [1], i.e., said player, and the user terminal 50, the information which shows the intention of subscription to a system is first sent via a network like the subscription intention sending T41 to the system management organization 330. The information on the above-mentioned subscription intention of having been inputted into the communication function block 401 of the system management organization 330 is sent to the user subscription support functional block 402.
[0252]Reception of the above-mentioned subscription intention information of the user subscription support functional block 402 concerned will send the information on a file required for subscription to user side 200 via the communication function block 401 like the subscription required file sending T42.
[0253]In user side 200, creation of the subscription request according to a predetermined format is performed based on the subscription required file sent from the above-mentioned system management organization 330. The drawn-up subscription request concerned is sent to the system management organization 330 like the subscription request sending T43.
[0254]The user subscription support functional block 402 which received the above-mentioned subscription request sends the information which explains the function of a client to user side 200 like the client function sending T44.
[0255]From user side who received information on client function concerned 200, User Information, such as users' information, for example, an account number and a credit number which were mentioned above, a name, and a contact, is sent to the system management organization 330 like the User Information sending T45.
[0256]The user subscription support functional block 402 which received sending of the User Information concerned notifies the information on the purport that the registration procedure of subscription was completed to user side 200 like the registration procedure completion notification T46.
[0257]The user subscription support functional block 402 of the system management organization 330 transmits User Information to accounting information control machine Seki 320 via the communication function block 401 like the User Information sending T47 after the completion of procedure of this user subscription registration. Accounting information control machine Seki 320 which received this User Information saves the User Information concerned at the database function block 367.
[0258]By the above, the main flows of the time of subscription to a user's system are completed. The explanation about other composition currently mentioned to this drawing 31 is mentioned later.
[0259]Next, the principal part of the flow of the information at the time of acquisition of the key the purchase of point information and for decoding of the enciphered digital contents, etc. is explained using drawing 32. Since the information on the contents key the purchase of the above-mentioned point information and for decoding

of the enciphered digital contents is information for using contents, it is made to simplify these and to call it royalty information by the following explanation.
[0260]When a user obtains the important information (here royalty of contents) used by a system, access is made from user side 200 to accounting information control machine Seki 320 where the assignment in its duty is beforehand made for every user side 200. To access of an acquisition demand of the contents royalty information sent from above-mentioned user side 200, the royalty issuing function block 362 of accounting information control machine Seki 320 corresponds, and issue of a royalty is performed according to the following procedures.
[0261]First, from user side 200, the information on the purport that he would like to purchase a royalty is sent to accounting information control machine Seki 320 like the purchase written request sending T51. The information on the purport that he would like to purchase a royalty is information on the purchase written request which followed the predetermined format by user side 200. Thus, the information on the above-mentioned purchase written request inputted into the communication function block 361 of this accounting information control machine Seki 320 is sent to the royalty issuing function block 362 via a network.
[0262]In the royalty issuing function block 362 concerned, if the information on the above-mentioned purchase written request is received, it will carry out based on User Information saved at the database function block 367, the information on a new royalty will be generated, and the information on the royalty concerned will be sent to user side 200 like the new royalty sending T52.
[0263]If the receipt of the information on the above-mentioned new royalty is checked, user side 200 will draw up the receipt written confirmation according to a predetermined format, and will send it to the royalty issuing function block 362 of accounting information control machine Seki 320 like the receipt written confirmation sending T53.
[0264]By the above, the main flows of the time of the purchase of a royalty are completed. The explanation about other composition currently mentioned to this drawing 32 is mentioned later.
[0265]Next, the principal part of the flow in the case of circulation of the information for contents and contents appreciation (here, they are a service condition and a contents key) is explained using drawing 33.
[0266]First, the contents acquisition functional block 342 of the content exhibiting distributing institution 310 charges digital contents to the system management organization 330 like the contents bill sending T62.
[0267]In the contents distribution functional block 404, the system management organization 330 which received the contents bill concerned is processed so that the demanded contents can be circulated. That is, in this contents distribution functional block 404, the digital contents (enciphered digital contents) of the state which can be sent to user side 200 are generated. These processed digital contents are sent to the content exhibiting distributing institution 310 like the contents sending 63.
[0268]In the content exhibiting distributing institution 310 concerned, the digital contents processed [above-mentioned] are saved at the contents database functional block 345.
[0269]In the contents distribution functional block 404 of the system management organization 330. The contents key for decoding the contents enciphered as content ID and a service condition as information for contents appreciation is sent to accounting information control machine Seki 320 like the information sending T64 for contents appreciation.

[0270]In accounting information control machine Seki 320, a contents key and the service-condition receipt functional block 363 receive the information for the above-mentioned contents appreciation, and it is saved at the database function block 367.
[0271]Next, like the contents acquisition request T61, user side 200 is accessed to the content exhibiting distributing institution 310, and obtains contents. Namely, the content exhibiting distributing institution 310, reading the enciphered digital contents which are saved at the contents database functional block 354, if the demand of acquisition of contents is made from above-mentioned user side 200 via the communication function block 341 -- the read digital contents concerned -- user side 200 -- sending .
[0272]Then, user side 200 is accessed to accounting information control machine Seki 320 by the information claim T65 for contents appreciation, and obtains the information for contents appreciation like the information sending T66 for contents appreciation. Namely, via the communication function block 361 in accounting information control machine Seki 320, If the request for a service condition and a contents key is made as information for contents appreciation from above-mentioned user side 200, a contents key and a service condition will be published from a contents key and the service-condition issuing function block 364, and these will be sent to user side 200 via the communication function block 361.
[0273]By the above, the flow in the case of circulation of the information for contents and contents appreciation is completed. The explanation about other composition currently mentioned to this drawing 33 is mentioned later.
[0274]Next, the principal part of the flow of balancing account, i.e., balancing account of a contents usage fee, when contents are actually appreciated is explained using drawing 34.
[0275]First, after appreciation of contents is performed in user side 200, from concerned user side 200, point usage information, i.e., use record of contents, is sent to accounting information control machine Seki 320 like the statement-of-accounts sending T71 as mentioned above. Thus, if sending of the above-mentioned contents use record is received from above-mentioned user side 200 via the communication function block 361, the contents use record concerned will be received with the balancing account procedure reception functional block 365 of accounting information control machine Seki 320, and the balancing account written confirmation corresponding to this will be published. Similarly the balancing account written confirmation concerned is sent to user side 200 via the communication function block 361 like the balancing account written confirmation sending T73. Thereby, user side 200 can know that balancing account was performed.
[0276]Next, the balancing account procedure reception functional block 365 of accounting information control machine Seki 320 makes royalty issuing information publish from the royalty issuing function block 362. This royalty issuing information is sent to the system management organization 330 via the communication function block 361 as user settlement of accounts and the contents use record sending T74 with the contents use record sent from above-mentioned user side 200.
[0277]The system management organization 330 summarizes the information sent from accounting information control machine Seki 320 currently distributed in various places with collection of money and the distribution frame block 405, totals the amount of collection of money, a collection-of-money place, and the distribution destination of money, and settles them through a actual financial institution.

[0278]By the above, the flow of balancing account of a contents usage fee is completed. The explanation about other composition currently mentioned to this drawing 34 is mentioned later.
[0279]In explanation to drawing 34, from above-mentioned drawing 30, the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, the system management organization 330, and user side 200, In the data transmission and reception between the content exhibiting distributing institution 310, accounting information control machine Seki 320, and the system management organization 330, it cannot be overemphasized that a data encryption and decryption are performed like the above-mentioned. Also in this encryption and decryption, any of a public-key crypto system and a common key encryption system may be used, as mentioned above, a public-key crypto system can be used as a cipher system of a contents key or a common key, and a common key encryption system can be used as cipher systems, such as a message and various kinds of documents. It is also possible to use the technique of the improvement in security using said random number, the encryption at the time of treating contents, and least-common-multiple-ization of a compressive batch with these encryption.
[0280]Next, the concrete composition of each organizations 310, 320, and 330 mentioned above is explained briefly.
[0281]First, the composition of the content exhibiting distributing institution 310 is explained using drawing 35.
[0282]In this drawing 35, the content exhibiting distributing institution 310 concerned, The communication function block 341 which divides roughly and takes charge of the communication function between user side 200 and the system management organization 330, It consists of the contents acquisition functional block 342 which takes charge of the acquisition function of contents, the content display functional block 343 which takes charge of the exhibition function of contents, the balancing account functional block 344 which takes charge of balancing account, and the contents database functional block 345 which saves contents.
[0283]The contents bill creation function part 351 which takes charge of creation of a bill in case the above-mentioned contents acquisition functional block 342 charges contents to the system management organization 330, The contents receipt creation function part 352 which takes charge of creation of a receipt when contents are received from the system management organization 330, It consists of the function part 353 corresponding to a contents database which takes charge of correspondence with these **** and ** contents, and the contents saved at the contents database functional block 345.
[0284]The content display function part 354 which takes charge of the function for which the above-mentioned content display functional block 343 actually exhibits contents to virtual online shop, It consists of the function part 355 corresponding to a contents database which takes charge of correspondence with the contents currently these-exhibited and the contents saved at the above-mentioned contents database functional block 345.
[0285]The above-mentioned balancing account functional block 344 consists of the receipt issuing function part 356 which takes charge of the function to publish a receipt, and the function part 357 corresponding to the financial institution which takes charge of correspondence between the financial institutions 220.
[0286]Next, the composition of accounting information control machine Seki 320 is explained using drawing 36.

[0287]In this drawing 36, accounting information control machine Seki 320 concerned, The communication function block 361 which divides roughly and takes charge of the communication function between user side 200 and the system management organization 330, The royalty issuing function block 362 which takes charge of the function to publish a royalty, A contents key, and the contents key and service-condition receipt functional block 363 which take charge of the receipt of a service condition, A contents key, and the contents key and service-condition issuing function block 364 which take charge of issue of a service condition, It consists of the balancing account procedure reception functional block 365 which takes charge of the receptionist function of balancing account procedure, the distribution receipt functional block 366 which takes charge of the function of a receipt as distribution, and the database function block 376.
[0288]The purchase written request acknowledgement function part 371 in which the above-mentioned royalty issuing function block 362 takes charge of the acknowledgement function of a purchase written request, The point-data acknowledgement function part 372 which takes charge of the check of the data of the balance (balance of point information) of the royalty of client, i.e., user, side 200, use record (point usage information), etc., The royalty generating function part 373 which takes charge of the function to generate a royalty, and the royalty invoice creation function part 374 which takes charge of the function which draws up the invoice of a royalty, It consists of a royalty, the sending function part 375 which takes charge of the function to actually send a royalty invoice, the royalty receipt acknowledgement function part 376 which takes charge of the check of the receipt document of a royalty, and the royalty issuing information preservation function part 377 which takes charge of the function to save the information on the published royalty.
[0289]Above-mentioned contents key and service-condition receipt functional block 363 consist of a contents key, the receipt function part 378 which takes charge of the receipt of a service condition, and a contents key and the preservation function part 379 which saves a service condition.
[0290]Above-mentioned contents key and service-condition issuing function block 364, A contents key and the receiving function part 380 which takes charge of the function to receive the acquisition request of a service condition, The search service part 381 which takes charge of the function which searches and discovers a contents key and a service condition from the database function block 367, It consists of the transmitting-function part 382 which takes charge of the function to encipher and send a contents key and a service condition, and a contents key and the acknowledgement function part 383 which takes charge of the acknowledgement function of the receipt document of a service condition.
[0291]The contents use record receiving function part 384 which takes charge of the function which the above-mentioned balancing account procedure reception functional block 365 receives the contents use record (point usage information) enciphered, and is decrypted, The contents use record acknowledgement function part 385 which takes charge of the check of contents use record, The contents use record-keeping function part 386 which takes charge of the function in which the database function block 367 saves contents use record, It consists of the completion document creation function part 387 which takes charge of the function which draws up the completion document of balancing account procedure, and the conclusion function part 389 which takes charge of the function to edit contents use record collectively.
[0292]The bill acknowledgement function part 390 which takes charge of the acknowledgement function of the request-for-information document which charges

the data at the time of the above-mentioned distribution receipt functional block 366 collecting money, The use record report writer feature part 391 which takes charge of the function which draws up the report of the contents use record submitted to the system management organization 330, It consists of the royalty issue report writer feature part 392 which takes charge of the function which draws up the report of the royalty issuing information submitted to the system management organization 330, and the written confirmation acknowledgement function part 393 which takes charge of the acknowledgement function of the confirmation-of-receipt document of a report.
[0293]The royalty database function part 394 which takes charge of the function in which the database function block 367 saves the data of a royalty, A contents key, and the contents key and royalty database function part 395 which take charge of the function to save the data of a service condition, It consists of the user management data base function part 397 which saves the information about the contents use recording data base function part 396 which saves contents use record, and a user.
[0294]Next, the composition of the system management organization 330 is explained using drawing 37.
[0295]In this drawing 37, the system management organization 330 concerned, The communication function block 401 which divides roughly and takes charge of the communication function between user side 200, the content exhibiting distributing institution 310, and accounting information control machine Seki 320, It consists of the user subscription support functional block 402 which performs the support in the case of user subscription, the contents distribution functional block 404 which takes charge of distribution of contents, the database function block 403, and collection of money and the collection-of-money **** distribution frame block 405 which takes charge of the function of distribution.
[0296]The above-mentioned user subscription support functional block 402, Creation of a subscription request, and the subscription request creation transmitting-function part 411 which takes charge of transmission, The common key receiving function part 412 which takes charge of the function which receives and decrypts the enciphered common key, The subscription request acknowledgement function part 413 which takes charge of the acknowledgement function of the subscription request transmitted from user side 200, The ID generating function part 414 which takes charge of the function to generate client ID, i.e., user ID, The subscription request preservation function part 415 which takes charge of the function to save a subscription request at the database function block 403, It consists of the client function generation function part 416 which generates a client function, and the registration information preservation function part 417 which takes charge of the function to save registration information at the database function block 403.
[0297]The user management data base function part 418 to which the database function block 403 carries out preservation management of a user's information, The contents database function part 419 which saves contents, and the accounting information control machine Seki database function part 420 which carries out preservation management of the information on accounting information control machine Seki 320, It consists of the content-exhibiting-distributing-institution database function part 421 which carries out preservation management of the information of the content exhibiting distributing institution 310.
[0298]The bill acknowledgement function part 422 in which the contents distribution functional block 404 takes charge of the acknowledgement function of the bill of contents, The content retrieval function part 423 which takes charge of the function to search ready-mixed concrete TENTSU (source data), i.e., the contents before

processing, from the contents database function part 419 of the database function block 403, The content ID generation function part 424 which generates content ID, and the contents key generation function part 425 which generates a contents key, The contents service-condition generation function part 426 which generates a contents service condition, The contents compression function part 427 which compresses ready-mixed concrete TENTSU, i.e., the contents before processing, The preservation function part 429 which takes charge of the function to save the contents processing function part 428 which enciphers contents, and content ID, a contents key and a service condition at the contents database function part 419 of the database function block 403, The contents sending function part 430 which takes charge of the function to send contents via the communication function block 401, and the contents receipt acknowledgement function part 431 which takes charge of the function to check the receipt of contents, Content ID, a contents key, and ID, key and service-condition sending function part 432 that take charge of the function to send a service condition via the communication function block 401, It consists of content ID, a contents key, and ID, key and service-condition receipt acknowledgement function part 433 that take charge of the function to check the receipt of a service condition.

[0299]The request-for-information document creation function part 434 which makes out the bill of the data which use collection of money and the distribution frame block 405 for collection of money, The contents royalty receiving function part 435 which takes charge of the function to receive a contents royalty via the communication function block 401, The contents use record receiving function part 436 which takes charge of the function to receive contents use record via the communication function block 401, The confirmation-of-receipt document creation function part 437 which takes charge of the function which draws up the written confirmation of reception, It consists of the calculation and the bill creation function part 438 which makes out the bill which performs the calculation of the amount billed and the creation of a bill which are charged to a user, calculation of the dividend at the time of distributing the use gold collected by use to a right holder, and the calculation and the form-for-payment creation function part 439 which perform creation of a form for payment.

[0300]next -- being concerned -- others -- the composition of user side 200 corresponding to the system of an embodiment is explained using drawing 38. This drawing 38 expresses each function of said player 1 and the user terminal 50 collectively.

[0301]In this drawing 38, the composition of concerned user side 200, The communication function block 451 which will take charge of the communication function between the system management organization 330, the content exhibiting distributing institution 310, and accounting information control machine Seki 320 if it divides roughly, The contents acquisition functional block 452 which takes charge of acquisition of contents, The royalty purchasing function block 453 which takes charge of the purchase of royalties, such as point information, a contents key, a service condition, A contents key, and the contents key and service-condition acquisition functional block 454 which take charge of acquisition of a service condition, The balancing account procedure functional block 455 which takes charge of balancing account procedure, and the user subscription support functional block 456 which takes charge of the function which supports subscription to a system, It consists of appreciation of contents, the contents appreciation accounting function block 457 which takes charge of the function of fee collection, and the database function block 458.

[0302]The above-mentioned contents acquisition functional block 452 consists of the contents acquisition function part 461 which takes charge of the function which actually obtains contents, and the contents preservation function part 462 which takes charge of the function in which contents are made to save at a memory medium.
[0303]The purchase written request creation function part 463 in which the royalty purchasing function block 453 draws up the purchase written request of a royalty, The conclusion function part 464 which takes charge of the conclusion of the data of the balance (point balance) of the royalty of a client (user), use record (point usage information), etc., It consists of the royalty installation function part 465 which takes charge of the function which installs each information as a royalty, and the royalty receipt document creation function part 467 which draws up a royalty receipt document.
[0304]A contents key and the service-condition acquisition functional block 454, It consists of a contents key, the acquisition written request creation function part 468 which draws up the acquisition written request of a service condition, a contents key and the receiving function part 469 which takes charge of reception of a service condition, and a contents key and the receipt document creation function part 470 which draws up the receipt document of a service condition.
[0305]The balancing account procedure functional block 455 consists of the conclusion function part 471 which performs the conclusion of contents use record (point usage information), and the completion document receiving function part 472 which takes charge of reception of the completion document of balancing account procedure.
[0306]The above-mentioned user subscription support functional block 456, It consists of the subscription request creation function part 473 which takes charge of creation of a subscription request, the client function installation function part 474 which takes charge of installation of a client function, i.e., initialization of a user's player 1, and the registration information creation function part 475 which takes charge of the function which creates registration information.
[0307]The content retrieval function part 476 which takes charge of search of the contents by which the contents appreciation accounting function block 457 was saved at the memory medium, The royalty acknowledgement function part 477 which takes charge of the check of a royalty, and the simple contents appreciation function part 478 which reproduces contents in [when choosing contents, for example] simple, The accounting function part 479 which manages accounting information (point information), and the contents function decoding part 480 which decrypts the contents enciphered, It consists of the contents extension function part 481 which elongates the contents compressed, and the contents viewer function part 482 for enabling recognition of the contents of the contents saved at the memory medium, for example.
[0308]The royalty database function part 483 where the database function block 458 saves the data of a royalty, It consists of a contents key, the contents key and service-condition database function part 484 which save a service condition, the contents use recording data base function part 485 which saves contents use record, and the user information data base function part 486 which saves User Information.
[0309]Next, the player 1 of each embodiment which was mentioned above, and the concrete using form of the user terminal 50 are explained using drawing 39 and drawing 40.
[0310]As shown in drawing 39, the player 1 is arranged after said analog output terminal 2, the interface terminal 3 for PC, and the I/O terminal 4 for memory media have projected out of the case of the player 1, and the memory medium 61 is

connected to the above-mentioned I/O terminal 4 for memory media. For example in the case 60, these players 1 and the memory medium 61 are formed so that storage is possible, and they are made as [arrange / for example at the end side of this case 60 / the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC].

[0311]The case 60 where this player 1 and memory medium 61 were stored, From the side by which the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC are arranged, it is formed in the input/output port 53 of the personal computer 50 as the above-mentioned user terminal 50 so that insertion connecting may be possible.

[0312]Although the personal computer 50 concerned has the general composition which equipped the computer body with the display device 52, the keyboard 54, and the mouse 55, In the above-mentioned input/output port 53, the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC, and the corresponding interface are formed. Therefore, only by inserting in the input/output port 53 of the above-mentioned personal computer 50 the case 60 where the above-mentioned player 1 and the memory medium 61 were stored, The analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC come to be connected with the above-mentioned personal computer 50.

[0313]Although he is trying to form an interface [in the input/output port 53 of the personal computer 50 / terminal / 3 / for PC / the analog output terminal 2 of the above-mentioned player 1, and / interface] in the example of above-mentioned drawing 39, For example, as shown in drawing 40, it is also possible to arrange the adapter 62 which can respond to the interface of the general-purpose input/output port of the personal computer 50 between the analog output terminal 2 of the above-mentioned player 1 and the interface terminal 3 for PC.

[0314]In the system of an embodiment of the invention since it has stated above, Since digital contents are enciphered with the contents key which is a common key of a system, If it is the user (player 1) who registered with the system of this embodiment, if only it can copy these enciphered contents freely and a contents key comes to hand, appreciation of these contents is also possible. Therefore, installation to this contents memory medium (enciphered contents) can also be performed easily. On the other hand, since the enciphered digital contents cannot be decoded, the right of the copyright of contents or the right holder of the contents concerned is protected by the terminal unit which is not based on this embodiment system.

[0315]an embodiment of the invention, while according to the system filling up point information with a prepaid system (charge advance payment method) and reducing point information at the time of contents appreciation, Since he is trying to collect the usage information of the point, recovery of an appreciation price is possible for right holders (owner of a copyright etc.), a contents selling store, etc. with the right about a used point.

[0316]Since encryption is given in the case of an exchange of the data of point information or point usage information as mentioned above, security nature is improving. For example, since it shall trade after checking that use the random number (security ID) which interlocked by the system and player side, and both are in agreement, as mentioned above even if the completely same thing as the last data is forged and it tries to steal the point information for fee collection, it is safe.

[0317]1 chip making of the main components of a player is carried out, and it is difficult to take out key information and the decrypted digital contents outside. This

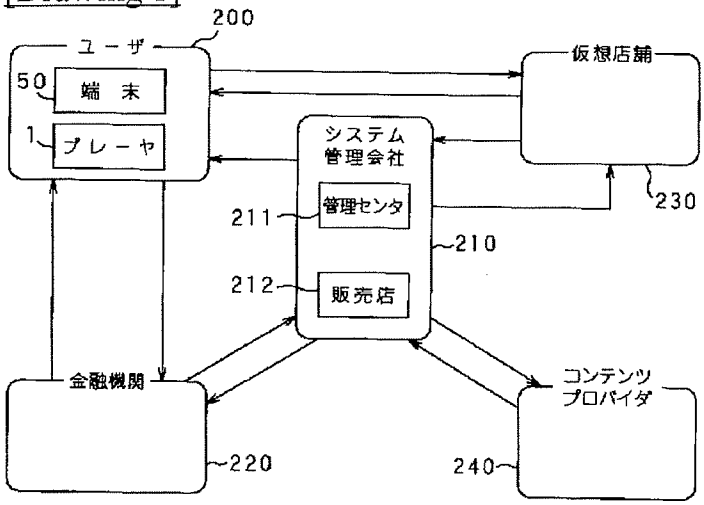
player 1 equips player 1 the very thing with the tamper resistance function, in order to prevent the data usurpation by destruction of the player 1 concerned.
[0318]As mentioned above, according to the embodiment of the invention, the digital contents distributing system with high security top intensity is built.
[0319]As above-mentioned digital contents, various kinds of things other than digital audio information, such as a digital video data, can be mentioned. When dynamic-image-data (audio information is also included) use is carried out as the above-mentioned digital video data, as the technique of said compression, compression methods, such as MPEG (Moving Picture Image CodingExperts Group), can be used, for example. The above-mentioned MPEG, In WG(Working Group) 11 of SC(Sub Committee) 29 of JTC(Joint Technical Committee)1 of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). It is a common name of the packed video coding mode, and there are MPEG1, MPEG 2, MPEG4, etc.
[0320]As the technique of the above-mentioned encryption, as mentioned above, the enciphering method currently called what is called DES (Data Encryption Standard) can be used. DES is the standard cipher system (cryptographic algorithm) which NIST (National Institute of Standards and Technology) in the U.S. announced in 1976. Data conversion is performed for every 64-bit data block, and, specifically, the conversion using a function is repeated 16 times. The above-mentioned digital contents, point information, etc. are enciphered with what is called a common key system using the DES concerned. It is a method which becomes the same [the key (decode key data) for decrypting with the key data (encryption key data) for enciphering] as that of the above-mentioned common key system.
[0321]What is called an EEPROM (electrically eliminable ROM) can be used for the common key storage memory 22 of the player 1 of said drawing 1, the key storage memory 21 for communication, the point usage information storing memory 29, and point information storing memory 28 grade, for example.
[0322]As a memory medium, the memory medium of recording media, such as a hard disk, a floppy disk, a magneto-optical disc, and a phase-change optical disk, or semiconductor memory (IC card etc.) can be used for others, for example.
[0323]In addition, although selection, a check, etc. were performed in the above-mentioned embodiment using the keyboard 54 of the user terminal 50, and the mouse 55 and the display device 52 on the occasions, such as content confirmation etc. of the contents exhibited by selection and the virtual online shop 230 of contents, It is also possible to simplify a function to these keyboards, or a mouse and a display device, and to give the player 1. namely, . Like drawing 2, it is also possible to form the input key part 6 and the indicator 7 in the player 1.
[0324]
[Effect of the Invention]The function to manage the accounting information to the user-terminal device of a fixed area by the above explanation according to this invention so that clearly, The function which exhibits digital contents and is distributed, and processing of digital contents, The distribution of digital contents to the above-mentioned digital content display distribution function processed [above-mentioned], It consists of a function to perform the information gathering and profit distribution from an accounting information controlling function, and the whole security management distribution, and it becomes possible by carrying out independently, respectively to raise a communicative response of the data communications between a user-terminal device and each function.

CLAIMS
[Claim(s)]
[Claim 1]A digital contents distribution managerial system which is provided with the following and characterized by the above-mentioned accounting information management tool, a content display distribution means, and a system management means performing data communications between the above-mentioned user-terminal devices independently, respectively.
An accounting information management tool which manages accounting information to a user-terminal device of a fixed area.
A content display distribution means which exhibits digital contents and is distributed. At least, it is processing of the above-mentioned digital contents.
A system management means which performs distribution of digital contents to the above-mentioned content display distribution means processed [above-mentioned], information gathering and profit distribution from the above-mentioned accounting information management tool, and the whole security management distribution.

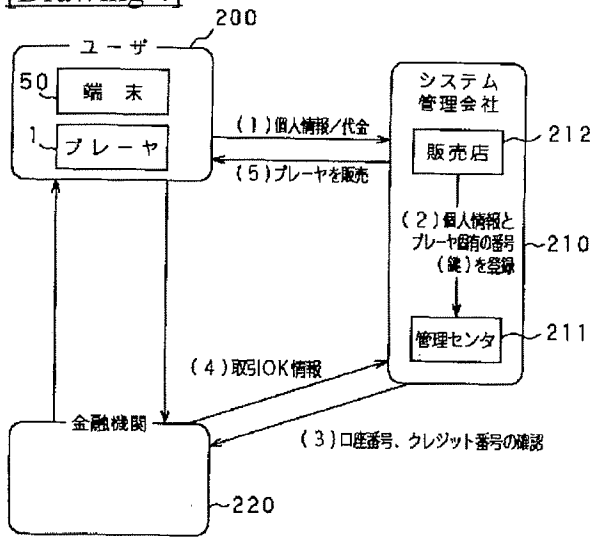
[Claim 2]A digital contents processing means which the above-mentioned system management means enciphers digital contents using a contents key for every digital contents concerned, and is compressed, A contents distribution means to distribute digital contents which processed [above-mentioned] it to the above-mentioned content display distribution means, The Cong Teng key transmitting means which enciphers a contents key used for decryption of digital contents processed [above-mentioned], and transmits to the above-mentioned user-terminal device, A contents usage information reception means which receives and decrypts enciphered contents usage information which has been transmitted from a user-terminal device, It has at least an accounting information encoding means which enciphers accounting information reduced whenever it decrypts digital contents processed [above-mentioned], and transmits to the above-mentioned accounting information management tool, An accounting information transmitting means which transmits accounting information by which the above-mentioned accounting information management tool was enciphered [above-mentioned] according to a demand from the above-mentioned user-terminal device to the user-terminal device concerned, Have at least a use gold dispensing means which distributes use gold collected based on the above-mentioned contents usage information to a right holder of the above-mentioned digital contents, and the above-mentioned content display distribution means according to a digital contents Request to Send from the above-mentioned user-terminal device, The digital contents distribution managerial system according to claim 1 which has at least a contents transmitting means which transmits digital contents which processed [above-mentioned] it, and is characterized by things.
[Claim 3]The above-mentioned accounting information management tool, a content display distribution means, and a system management means, The digital KONTEN ivy distribution managerial system according to claim 2, wherein a cipher system or an encryption key used when performing data communications between the above-mentioned user-terminal devices independently, respectively is original respectively.

DRAWINGS

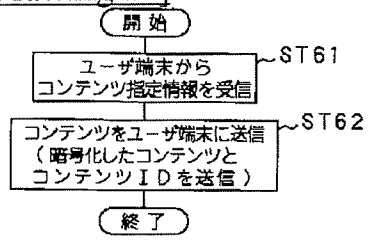
[Drawing 1]



[Drawing 4]

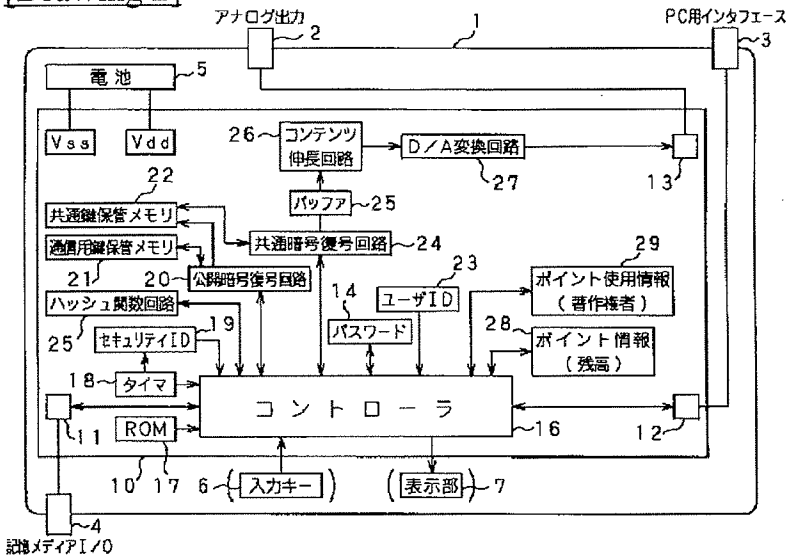


[Drawing 14]

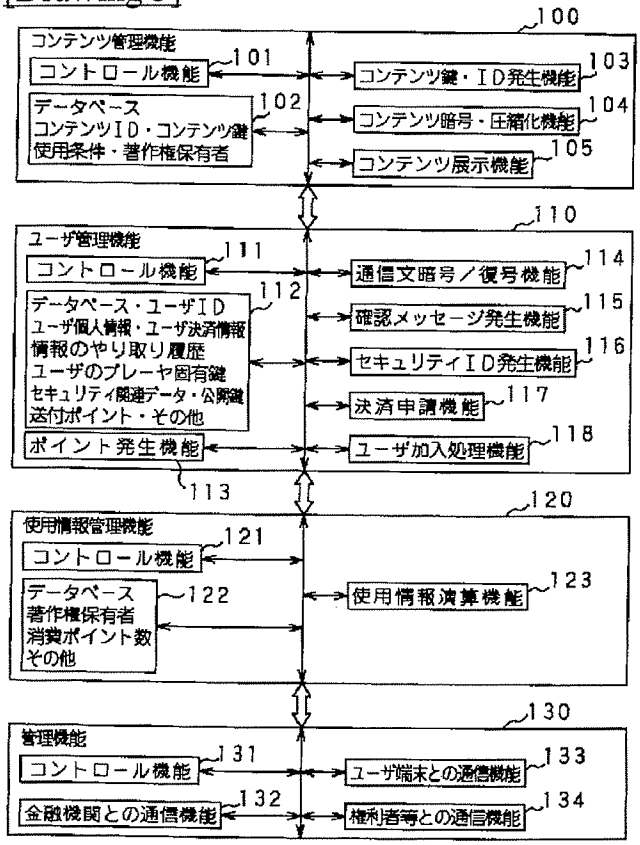


コンテンツ入手時の管理センタのフローチャート

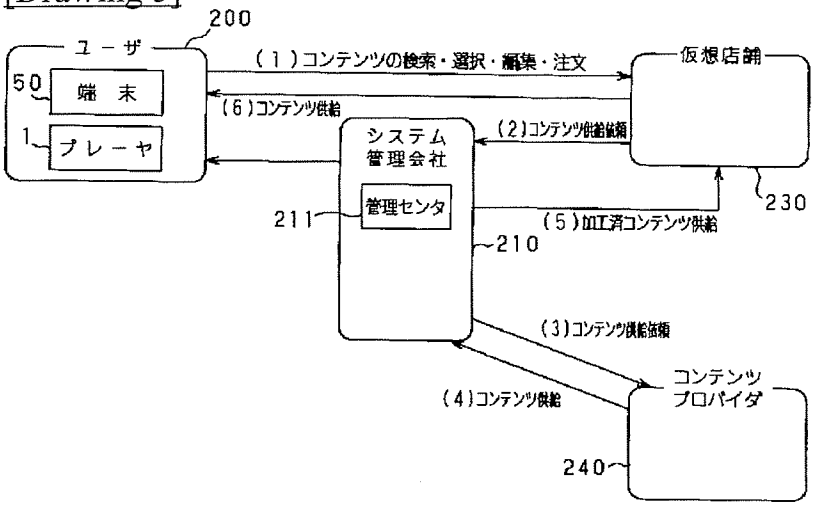
[Drawing 2]



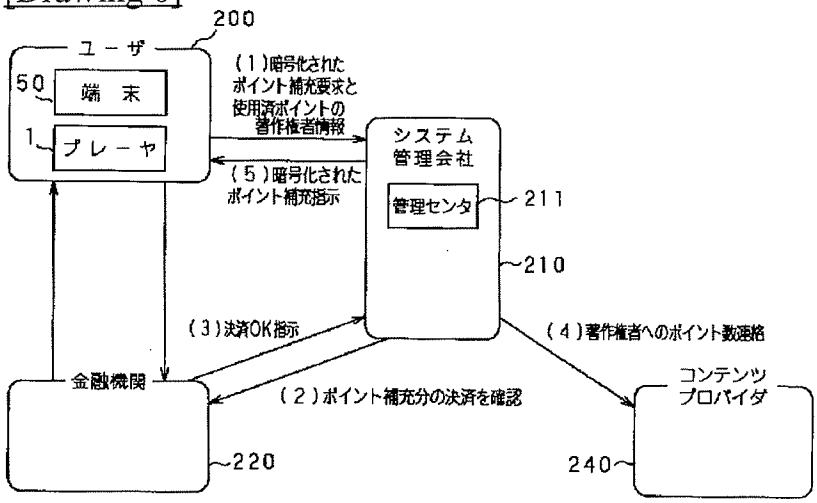
[Drawing 3]



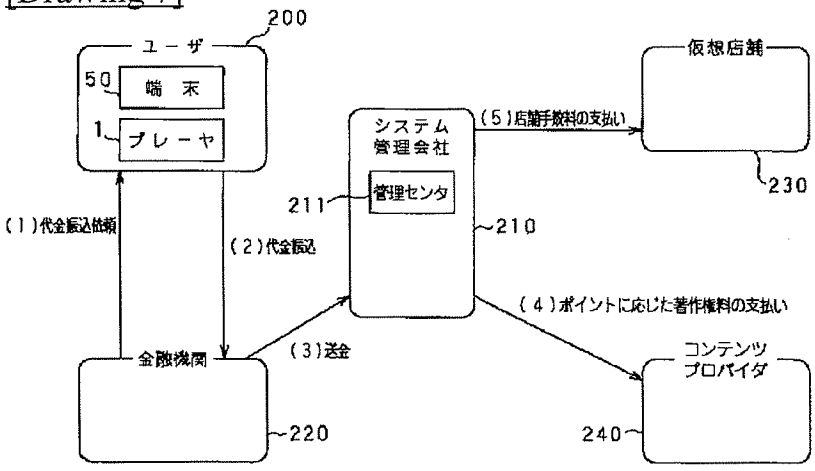
[Drawing 5]



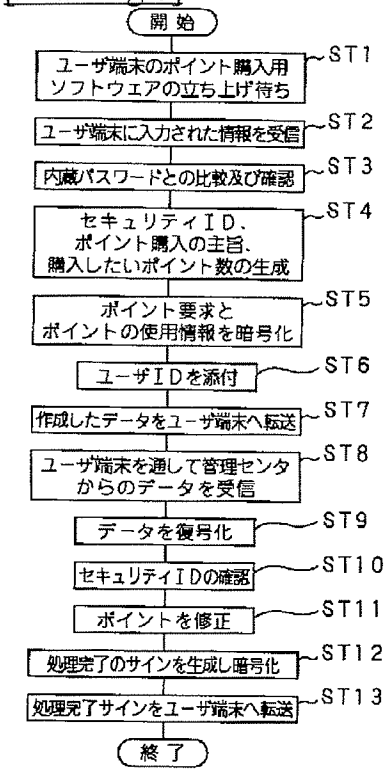
[Drawing 6]



[Drawing 7]

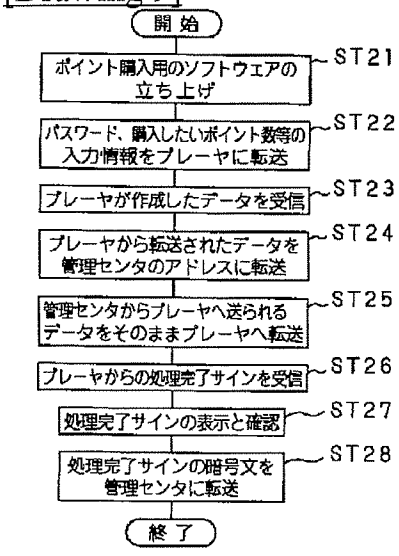


[Drawing 8]



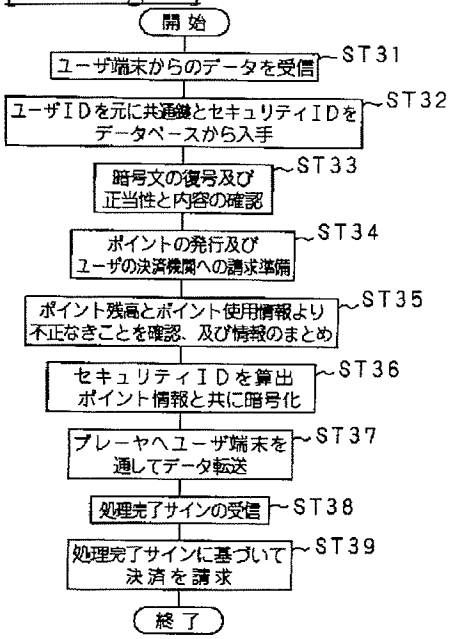
ポイント購入時のプレーヤのフローチャート

[Drawing 9]



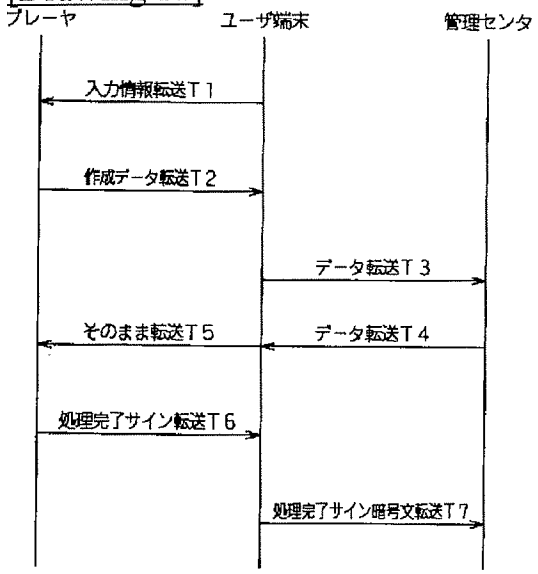
ポイント購入時のユーザ端末のフローチャート

[Drawing 10]



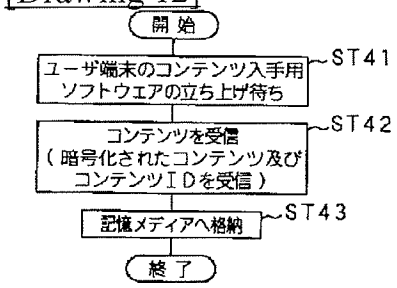
ポイント購入時の管理センタのフローチャート

[Drawing 11]



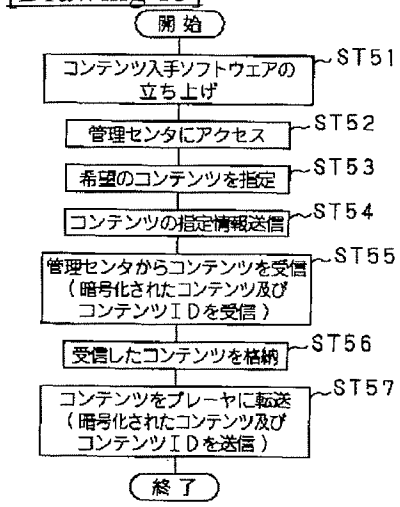
ポイント購入時のシーケンス

[Drawing 12]



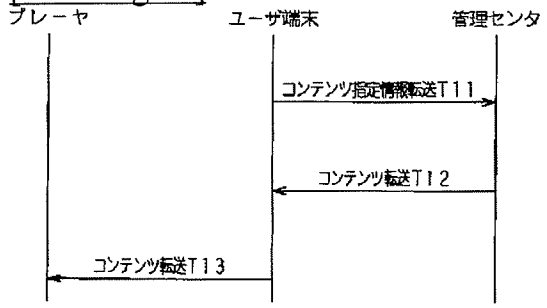
コンテンツ入手時のプレーヤのフローチャート

[Drawing 13]



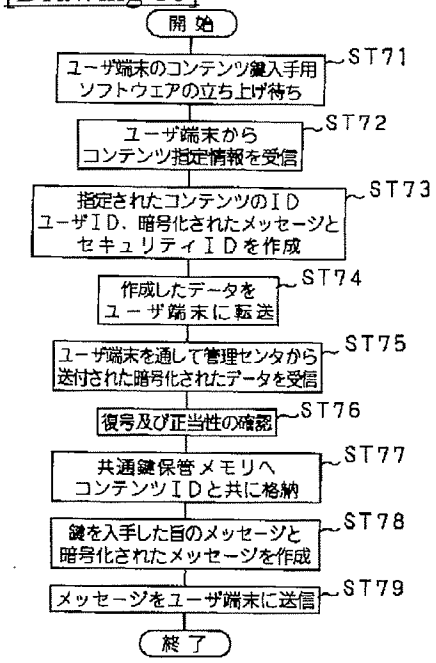
コンテンツ入手時のユーザ端末のフローチャート

[Drawing 15]



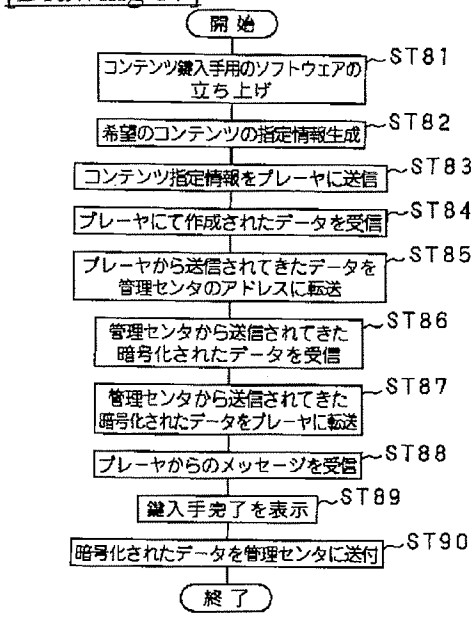
コンテンツ入手時のシーケンス

[Drawing 16]



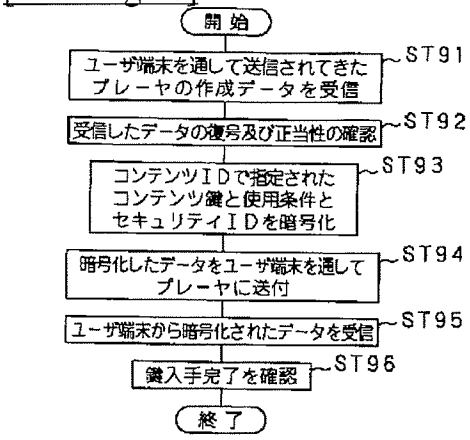
コンテンツ鍵・入手時のプレーヤのフローチャート

[Drawing 17]



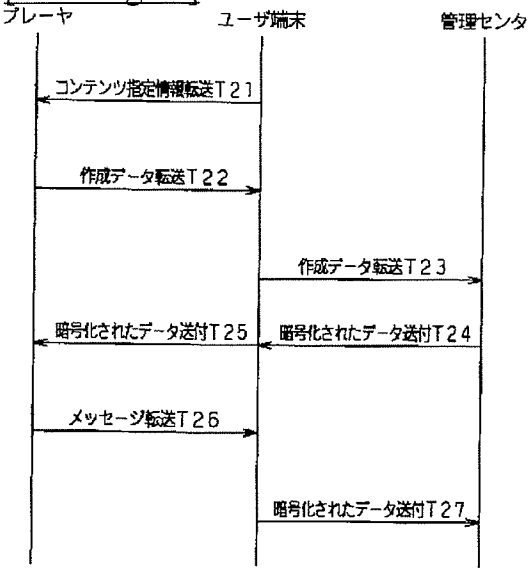
コンテンツ鍵・使用条件入手時のユーザ端末のフローチャート

[Drawing 18]



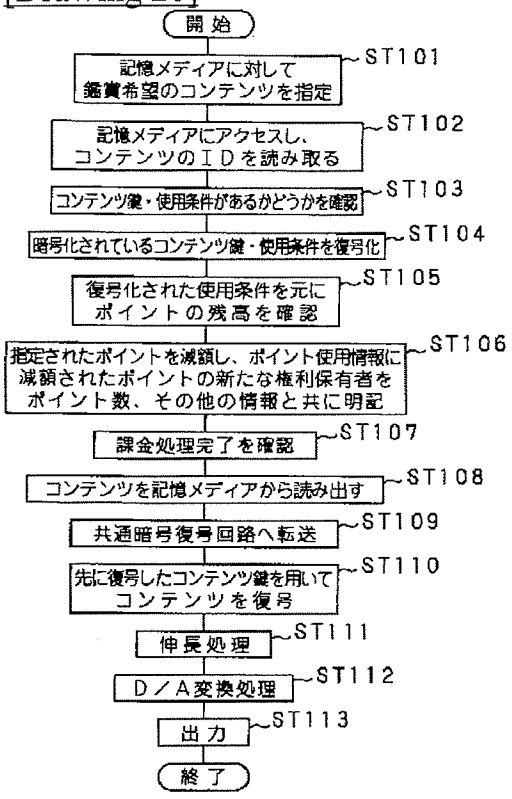
コンテンツ鍵・使用条件入手時の管理センタのフローチャート

[Drawing 19]



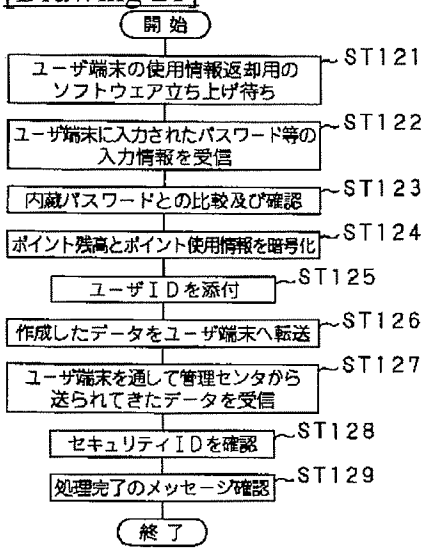
コンテンツ鍵・使用条件入手時のシーケンス

[Drawing 20]



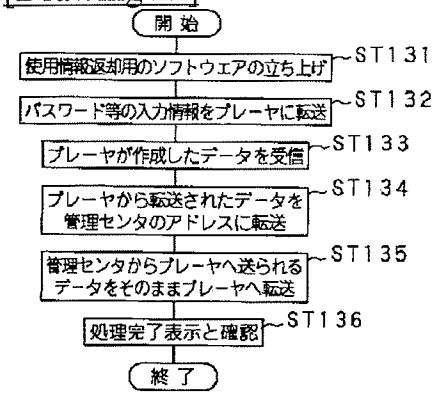
コンテンツ鑑賞時のプレーヤのフローチャート

[Drawing 21]



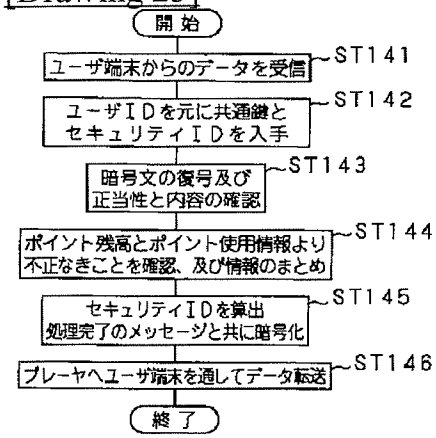
使用情報返却時のプレーヤのフローチャート

[Drawing 22]



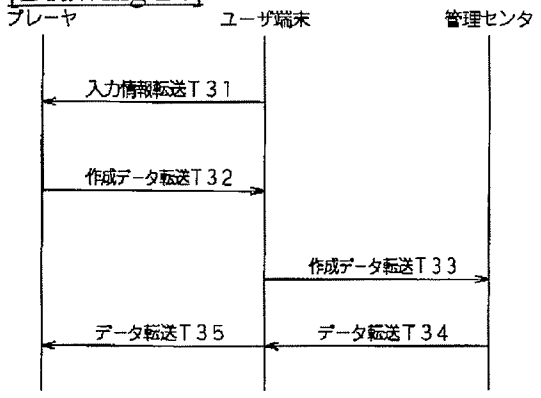
使用情報返却時のユーザ端末のフローチャート

[Drawing 23]



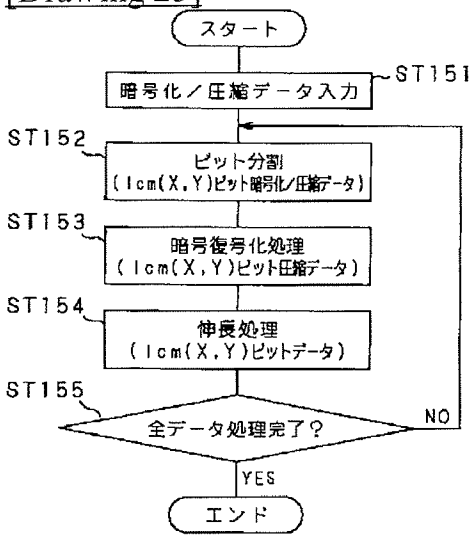
使用情報返却時の管理センタのフローチャート

[Drawing 24]

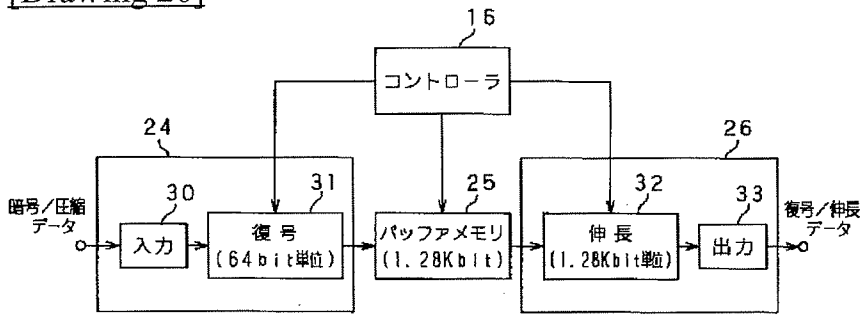


使用情報返却時のシーケンス

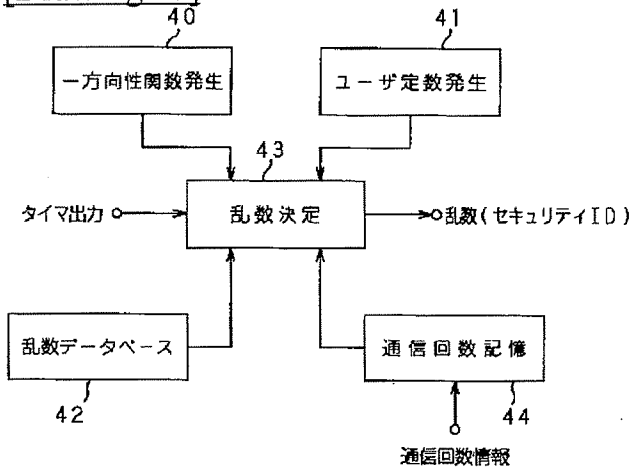
[Drawing 25]



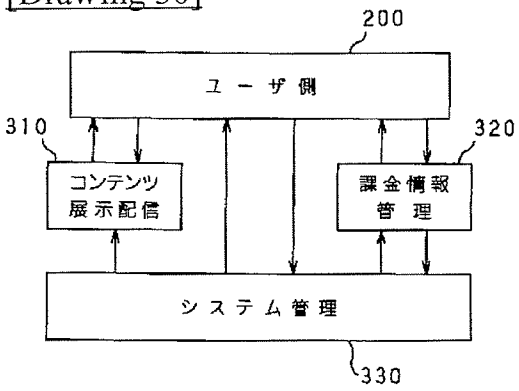
[Drawing 26]



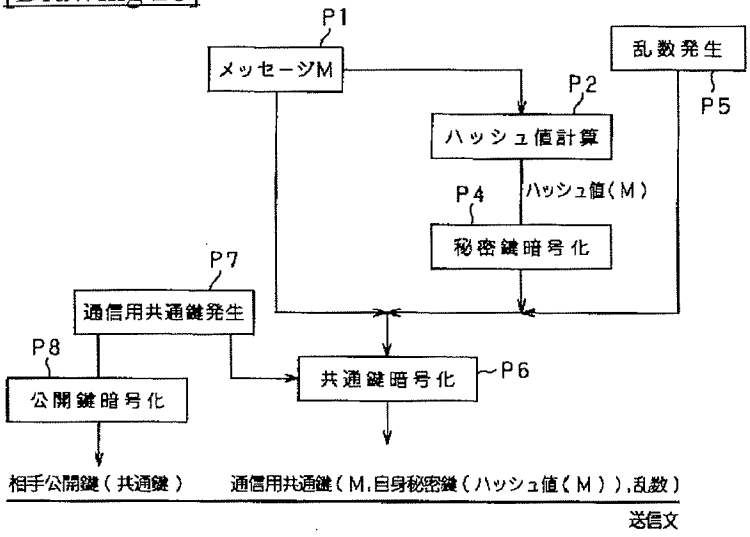
[Drawing 27]



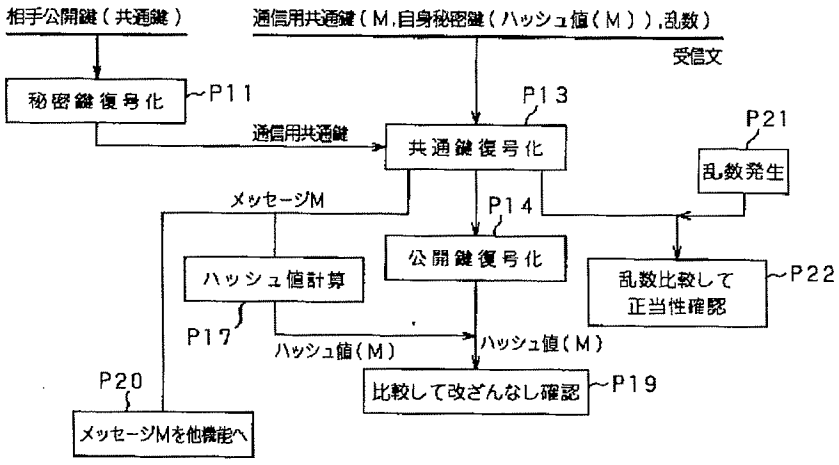
[Drawing 30]



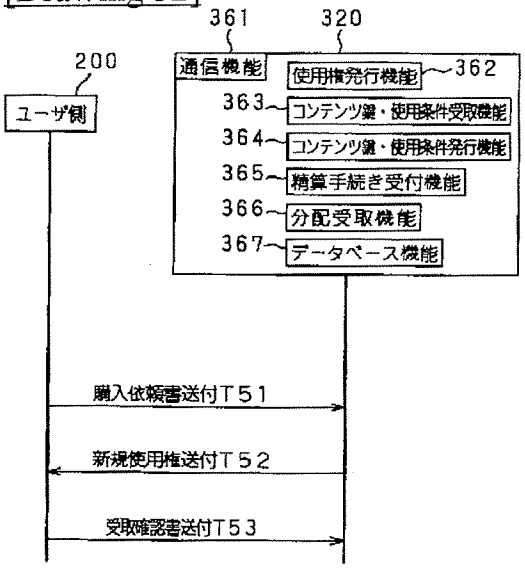
[Drawing 28]



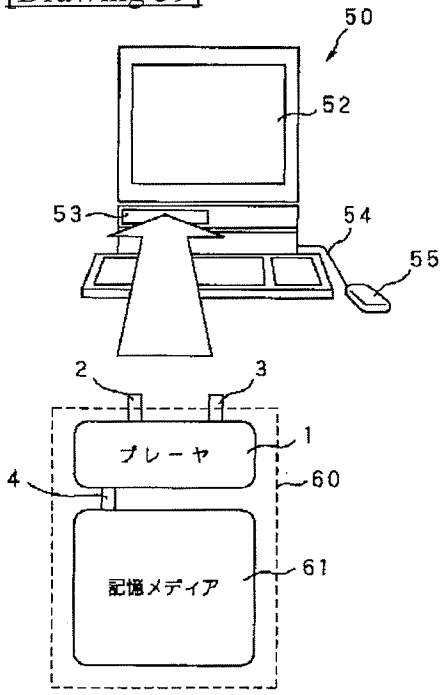
[Drawing 29]



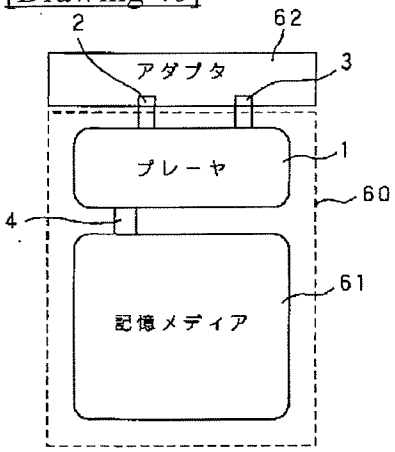
[Drawing 32]



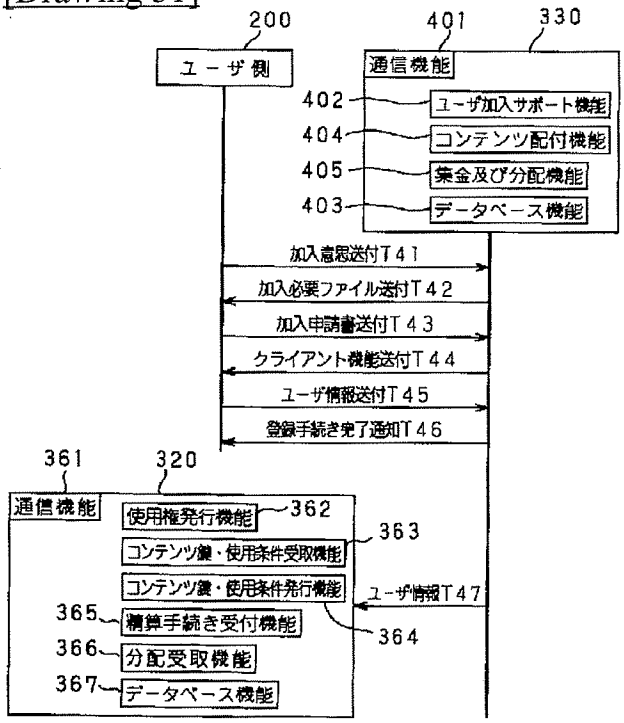
[Drawing 39]



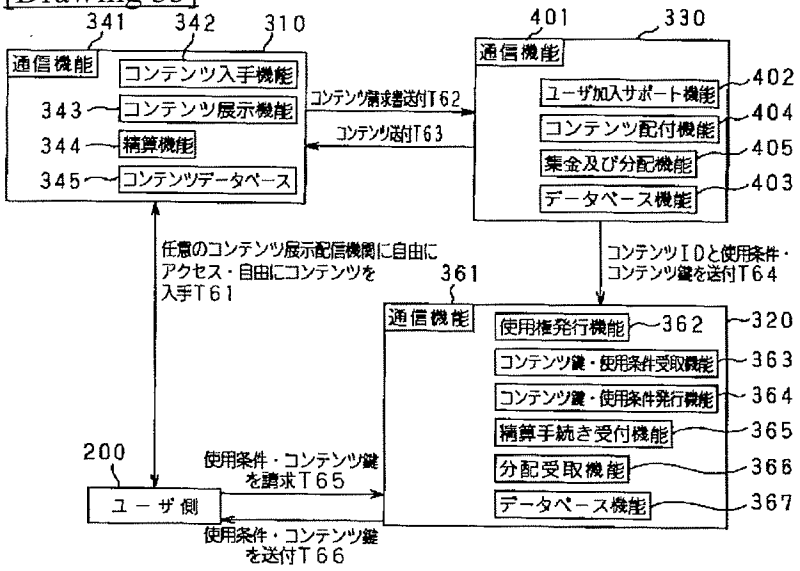
[Drawing 40]



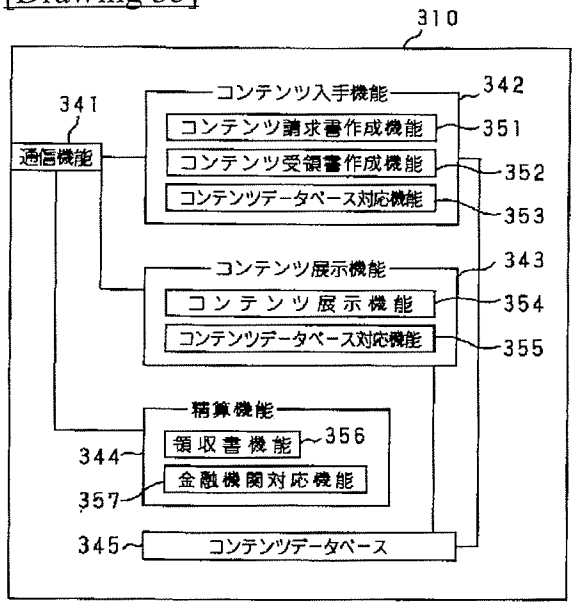
[Drawing 31]



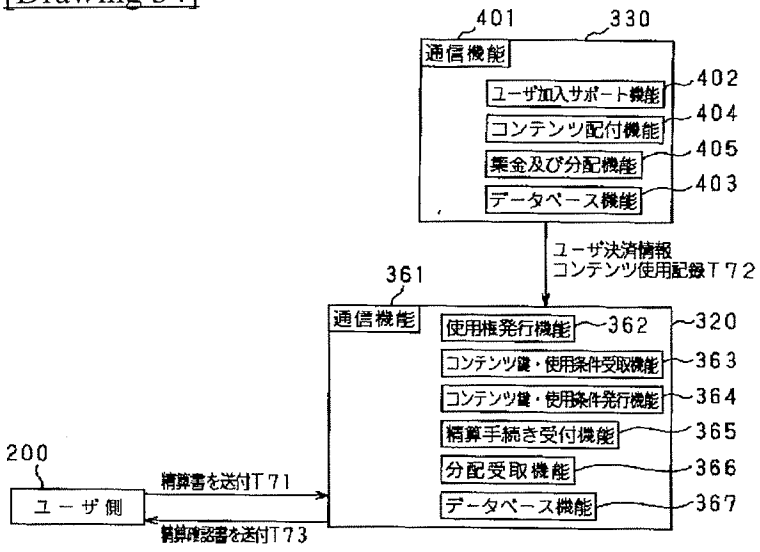
[Drawing 33]



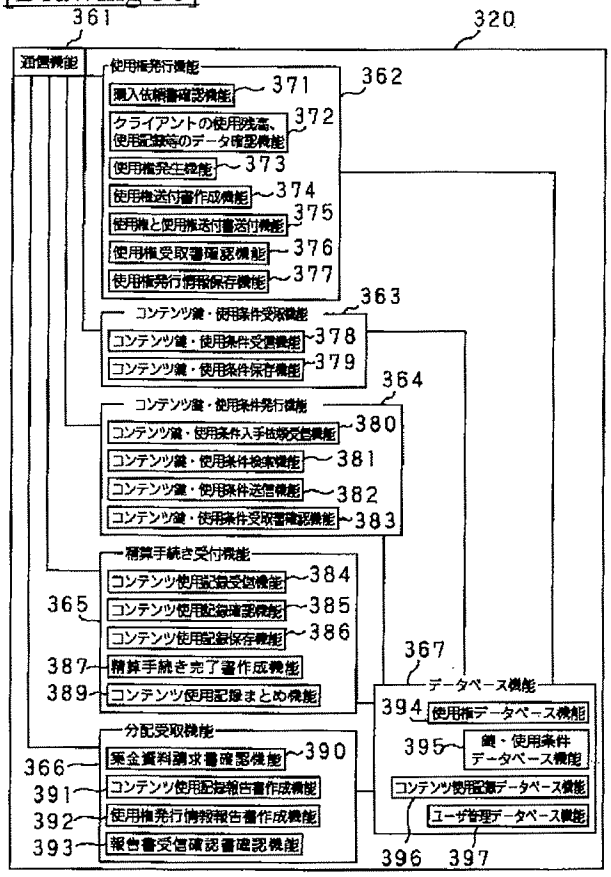
[Drawing 35]



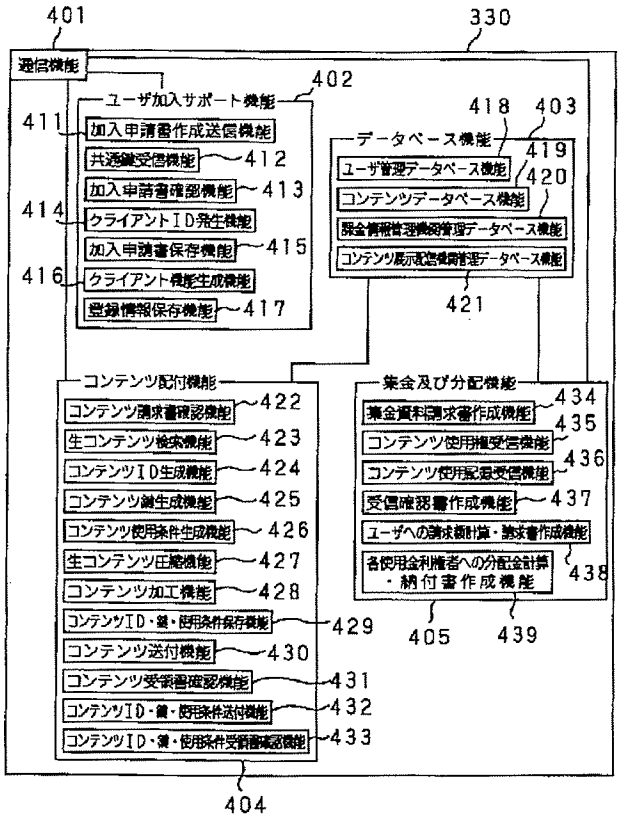
[Drawing 34]



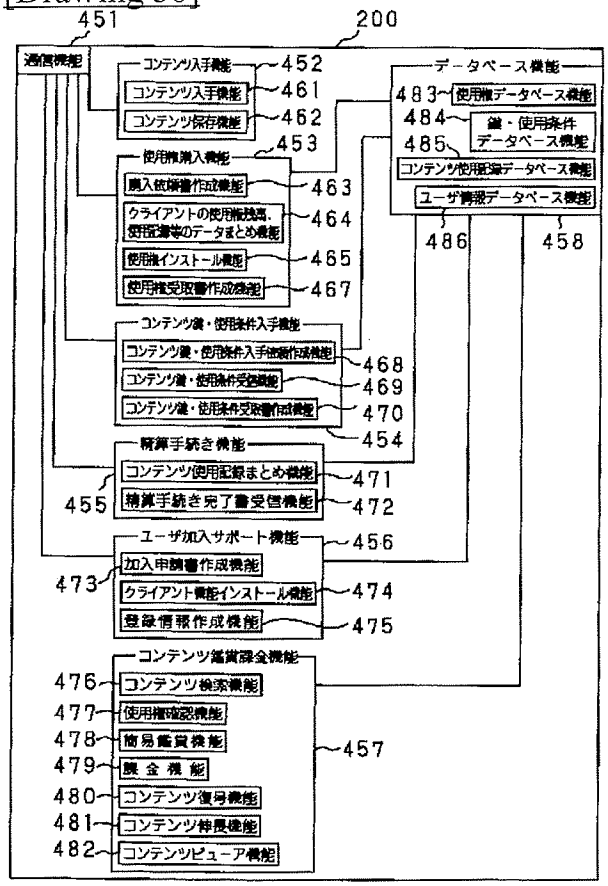
[Drawing 36]



[Drawing 37]


401
330
通信機能
402
ユーザ加入サポート機能
411
加入申請書作成送信機能
共通鍵受信機能
412
加入申請書確認機能
413
414
クライアントID発生機能
加入申請書保存機能
415
416
クライアント機能生成機能
登録情報保存機能
417
418
403
データベース機能
419
ユーザ管理データベース機能
420
コンテンツデータベース機能
課金情報管理機関管理データベース機能
コンテンツ展示配信機関管理データベース機能
421
コンテンツ配付機能
コンテンツ請求書確認機能
422
生コンテンツ検索機能
423
コンテンツID生成機能
424
コンテンツ鍵生成機能
425
コンテンツ使用条件生成機能
426
生コンテンツ圧縮機能
427
コンテンツ加工機能
428
コンテンツID・鍵・使用条件保存機能
429
コンテンツ送付機能
430
コンテンツ受領書確認機能
431
コンテンツID・鍵・使用条件送付機能
432
コンテンツID・鍵・使用条件受領書確認機能
433
404
集金及び分配機能
集金資料請求書作成機能
434
コンテンツ使用権受信機能
435
コンテンツ使用配分受信機能
436
受信確認書作成機能
437
ユーザへの請求額計算・請求書作成機能
各使用金利権者への分配金計算・納付書作成機能
438
405
439

[Drawing 38]


451
200
通信機能
コンテンツ入手機能
452
コンテンツ入手機能
461
コンテンツ保存機能
462
使用権購入機能
453
購入依頼書作成機能
463
クライアントの使用権残高、使用記録等のデータまとめ機能
464
使用権インストール機能
465
使用権受取書作成機能
467
コンテンツ鍵・使用条件入手機能
コンテンツ鍵・使用条件入手依頼作成機能
468
コンテンツ鍵・使用条件受取機能
469
コンテンツ鍵・使用条件受取書作成機能
470
454
精算手続き機能
コンテンツ使用記録まとめ機能
471
455
精算手続き完了書受信機能
472
ユーザ加入サポート機能
456
加入申請書作成機能
473
クライアント機能インストール機能
474
登録情報作成機能
475
コンテンツ鑑賞課金機能
476
コンテンツ検索機能
477
使用権確認機能
478
簡易鑑賞機能
479
課金機能
480
コンテンツ復号機能
481
コンテンツ特長機能
482
コンテンツビューア機能
457
データベース機能
483
使用権データベース機能
484
鍵・使用条件データベース機能
485
コンテンツ使用記録データベース機能
ユーザ情報データベース機能
486
458

(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11－53184

(43)公開日　平成11年(1999)２月26日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｈ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ａ
					６７３Ｅ

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）

(21)出願番号　特願平9－214318

(22)出願日　平成９年(1997)８月８日

(71)出願人　391065769
株式会社セタ
東京都大田区西蒲田７丁目35番１号

(72)発明者　富士本　淳
東京都大田区西蒲田七丁目35番１号　株式会社セタ内

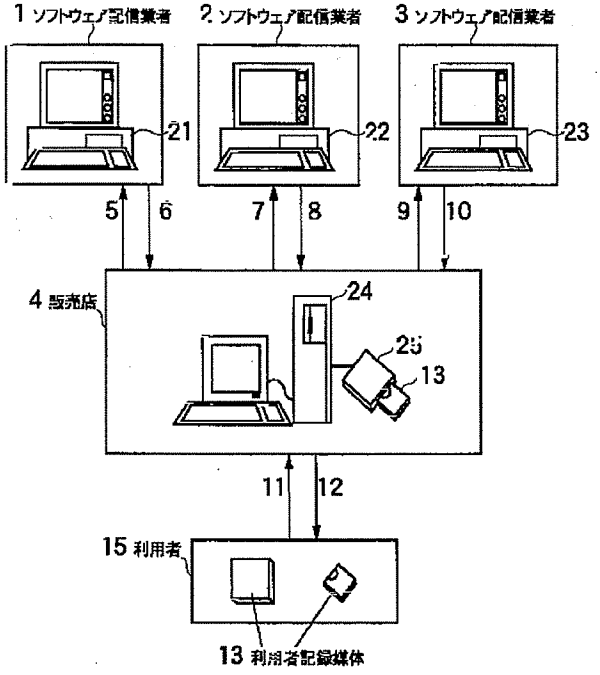
(74)代理人　弁理士　油井　透　（外１名）

(54)【発明の名称】　データ配信方法および装置

(57)【要約】

【課題】　ゲームソフトの書換えに使用する書換え可能な記録媒体に、利用者の個別データ、課金データなどの付加データも記録し、ソフトウェア配信業者のコンピュータと照合することで、セキュリティの高いシステムを簡単に構築する。

【解決手段】　販売店４でゲームソフトを書換える利用者記録媒体１３を購入し、そこに一定額の現金データを入金する。このとき利用者の固有データも書き込む。販売店４のコンピュータ２４からゲームソフトを要求すると、利用者記録媒体１３のデータが通信系５、７、９によりソフトウェア配信業者１～３に送られて、配信業者のコンピュータ２１～２３に記録されている過去の付加データと照合される。一致すると配信業者から通信系６、８、１０を利用してゲームソフトが販売店４に配信され利用者記録媒体１３に記録される。同時にゲームソフトに関する付加データが、利用者記録媒体１３とソフトウェア配信業者１～３のコンピュータ２１～２３に記録される。



【特許請求の範囲】
【請求項１】利用者の要求に応じて情報提供者から利用者にソフトウェアが配信されるデータ配信方法において、
利用者固有のデータおよび課金データを含む上記ソフトウェアに関連する付加データが記録されている書換え可能な利用者記録媒体を用い、利用者記録媒体の利用者固有データに該当する付加データを情報提供者のコンピュータから検索し、
情報提供者のコンピュータに記憶されている付加データと利用者記録媒体に記憶されている付加データとを照合し、
付加データが合致しないとき配信処理を中止し、
付加データが合致したとき利用者の要求するソフトウェアに対する課金処理を含む配信処理を行ない、この配信処理により情報提供者から利用者に配信されてきたソフトウェアと、上記課金処理した課金データを含む上記ソフトウェアに関する付加データを利用者記録媒体に記録するとともに、利用者からは直接アクセスできないようにデータ管理されている情報提供者のコンピュータにも上記付加データを記録するようにしたデータ配信方法。
【請求項２】利用者がサービス供与条件を満たしたとき、情報提供者から利用者にサービスを供与するために、情報提供者のコンピュータから利用者記録媒体に所定の金額を入金し、その記録が情報提供者のコンピュータにも記録されるようにした請求項２に記載のデータ配信方法。
【請求項３】上記利用者記録媒体が光磁気ディスクである請求項１または２に記載のデータ配信方法。
【請求項４】利用者の要求に応じて情報提供者から利用者にデータを配信する通信系と、
通信系により情報提供者から配信されるデータのうち、利用者の要求するソフトウェアを記録する主データ領域と、利用者固有のデータおよび課金データを含む上記ソフトウェアに関連する付加データを記録する付加データ領域とを備えた書換え可能な利用者記録媒体と、
利用者記録媒体の付加データ領域に記録された付加データと同一のデータを記録する情報提供者側の記録手段と、
情報提供者の記録手段に記録された付加データに対して情報提供者からの書換えは許容し、利用者からの書換えを規制する手段と、
利用者記録媒体の利用者固有データに該当する付加データを情報提供者の記録手段から検索し、情報提供者の記録手段の付加データと利用者記録媒体の付加データとを照合し、合致したときソフトウェアの配信処理を続行し、合致しないときソフトウェアの配信処理を中止する照合手段と、
照合手段の照合結果によりソフトウェアの配信処理が続行される時、配信されるソフトウェアに応じて課金処理したうえで、情報提供者から利用者に配信されてくるソフトウェアを利用者記録媒体の主データ領域に記録させるとともに、利用者記録媒体の付加データ領域と情報提供者側の記録手段とに課金データを含む付加データを記録させる手段とを備えたデータ配信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はデータ配信方法および装置に係り、特に書換え可能な記録媒体を利用してデータの配信と課金を同時に行うものに関する。
【０００２】
【従来の技術】現金の代りに使用する代表的なカードとして、プリペイドカード、クレジットカード、ＩＣカードがある。
【０００３】プリペイドカードは、インクの代りに磁気を使って必要な情報を書き込んだ一種の回数券であり、磁気カードに記録されている購入金額の分だけ利用でき、利用しきれば使用できなくなる仕組みである。たとえばパチンコカードやテレホンカード、イオカードなどがある。不正使用に対する有効な対策がないのが現状である。
【０００４】クレジットカードは、このカードを取り扱う加盟店で使用でき、商品代金の支払や返済を一定期間猶予し、商品代金を銀行口座から自動引き落としで決済するものである。不正使用を防ぐためにオーソリゼーションを必要とする。有線電話回線、無線電話回線、衛星放送などを利用して、付加価値データおよび各種制御データを入手するためのシステム利用料金の課金方法は、このクレジットカードによる決済が一般的である。
【０００５】ＩＣカードは、ＩＣに記憶装置であるメモリ部とマイクロプロセッサ部を設けて、カード自体にデータ作成や判断などの論理的な処理機能を持たせたものである。電子マネーなどがこれにあたる。カードに埋め込まれたＩＣにより、真贋のチェック機能や、転送された電子マネーデータを格納しておく書換え可能な記憶機能がある。書換え可能な記憶機能があるので、利用者以外からもＩＣカードに入金させることもできる。
【０００６】
【発明が解決しようとする課題】しかし上述した従来のカード方式には、これらのカードを使ってソフトウェアを配信しようとする場合、つぎのような問題があった。
【０００７】(1) プリペイドカード
①利用者の個別データが、管理コンピュータと連動していなかったため、プリペイドカード自体の偽造に弱い。実際にパチンコカードで偽造が顕在化していることは周知である。
【０００８】②専用のカードリーダなどの読取機が必要なため、小形化、省電力化、低価格化ができない。
【０００９】③データを再充填できないので、カード内の現金データまたは度数データを使いきってしまうと

再利用することができなくなる。

【００１０】④自動販売機の形で設置されているソフトウェア販売機でソフトウェアを購入する時に、また通信対局ゲームや通信を利用して画像情報や音楽情報を取得する通信利用型ソフトウェアを購入する時に、それらのソフトウェアとは別個にプリペイドカードを購入する必要があり、利用者から見て非常に不便である。

【００１１】(2) クレジットカード

①利用者がクレジットカードの所持者に限定されてしまうので、利用者の拡大という点で障害となる。

【００１２】②クレジットカードの契約が面倒である等の理由で、利用者の拡大において障害となっている。

【００１３】③ソフトウェアの販売状況を、有線電話網または無線電話網の通信系を利用し、ソフトウェアを配信する業者のコンピュータと通信する機能がないために、販売／売上管理ができない。

【００１４】(3) ＩＣカード

ＩＣカードはデータ作成や判断などの論理的な処理機能を持たせてあるので、上述したプリペイドカードやクレジットカードのような欠点はない。しかし、つぎの点で問題がある。

【００１５】①個人データなど種々の秘匿する必要のあるデータが多数含まれるので、セキュリティを確保するために、高度な暗号技術やコピー防止技術を必要とする。

【００１６】②システムが非常に大掛かりとなるうえ、ＩＣカードの構造も複雑になる。

【００１７】③記憶容量が小さいので、ゲームソフトのような大容量のプログラムを記録させることが困難である。

【００１８】④まだ実験段階で、簡易かつ安価に実現することは難しい。

【００１９】特に、ゲーム業界においては、ネットワークを通じてソフトウェアの配信を既に始めているが、上述したように(1) ～(3) の方式では、現金データを使って配信業者から配信されたソフトウェアを簡易かつ安全に配信することができない。

【００２０】本発明の課題は、利用者の要求に応じて情報提供者から利用者にソフトウェアを配信するデータ配信技術において、上述した従来技術の問題点を解消して、書換え可能な記録媒体を使用しながら、簡易かつ安全に配信することができるデータ配信方法および装置を提供することにある。

【００２１】

【課題を解決するための手段】請求項１に記載のデータ配信方法は、利用者の要求に応じて情報提供者から利用者にソフトウェアが配信されるデータ配信方法において、利用者固有のデータおよび課金データを含む上記ソフトウェアに関連する付加データが記録されている書換え可能な利用者記録媒体を用い、利用者記録媒体の利用者固有データに該当する付加データを情報提供者のコンピュータから検索し、情報提供者のコンピュータに記憶されている付加データと利用者記録媒体に記憶されている付加データとを照合し、付加データが合致しないとき配信処理を中止し、付加データが合致したとき利用者の要求するソフトウェアに対する課金処理を含む配信処理を行ない、この配信処理により情報提供者から利用者に配信されてきたソフトウェアと、上記課金処理した課金データを含む上記ソフトウェアに関する付加データを利用者記録媒体に記録するとともに、利用者からは直接アクセスできないようにデータ管理されている情報提供者のコンピュータにも上記付加データを記録するようにしたものである。

【００２２】プリペイドカードの偽造問題の原因は、プリペイドカード内の課金データ（使用可能度数）の管理を一切行なわず、単にプリペイドカード内の課金（使用可能度数）が０になったら、そのプリペイドカードは使用済みであると認識した点に止まっていたことである。本発明は、この課題を解決する手法として、偽造を防止するのではなく、付加データの管理を行なうことにより、偽造した書換え可能な記録媒体を使用時に発見するようにしたものである。

【００２３】本発明によれば、利用者の書換え可能な利用者記録媒体に正規の付加データが記録されるときは、同時に情報提供者のコンピュータにも同一内容の付加データが記録される。したがって、情報提供者のコンピュータとは関係なく、利用者記録媒体に不正にデータを書込んだり、利用者記録媒体を偽造したりした場合には、情報提供者のコンピュータには不正データないし利用者記録媒体と同一の付加データが記録されていないので、利用者記録媒体と情報提供者のコンピュータとに記録される過去のデータは不一致となる。その結果、付加データを照合することにより、偽造またはデータの改ざんされた利用者記録媒体の不正使用を有効に防止することができる。

【００２４】また、利用者記録媒体に書込まれるソフトウェアに関連する付加データは、ソフトウェアを配信する情報提供者のコンピュータに、ソフトウェアの購入と同時に記録されて蓄積していくので、ソフトウェアの販売／売上管理ができる。またゲームなどのソフトウェアと課金データを含む付加データとの双方を１枚の利用者記録媒体に記録するようにしたので、従来のようにソフトウェアウェア用の記録媒体と、ソフトウェア購入用のプリペイドカードとを別個に購入する必要がなく、１枚の利用者記録媒体を購入するだけで用が足りる。

【００２５】また、だれでも購入できる利用者記録媒体を採用すると、クレジットカードのような契約加入を必要とせず、利用者記録媒体を正規に購入するだけで誰でもデータ配信サービスを受けることができるので、利用者の拡大を図ることができる。

【００２６】請求項２に記載のデータ配信方法は、上記発明において、利用者がサービス供与条件を満たしたとき、情報提供者から利用者にサービスを供与するために、情報提供者のコンピュータから利用者記録媒体に所定の金額を入金し、その記録が情報提供者のコンピュータにも記録されるようにしたものである。

【００２７】利用者はソフトウェアなどの商品を購入するだけであるから、プリペイドカードを使用して購入するような場合、プリペイドカードは減額されるだけである。しかし書換え可能な利用者記録媒体を使用したこの発明では、情報提供者のコンピュータから自由に利用者記録媒体に対してアクセスできるから、上記サービスに見合った金額を利用者記録媒体に入金して課金データを増額することができる。

【００２８】請求項３に記載のデータ配信方法は、上記発明において、上記利用者記録媒体を光磁気ディスクで構成したものである。

【００２９】利用者記録媒体を光磁気ディスクで構成すると、既存のパソコンに内蔵または外付けされた光磁気ディスクドライブで書込み、読み取りができるので、カードリーダなどの専用機を必要とせず、データ配信システムを安価に構成することができる。

【００３０】請求項４に記載のデータ配信方法は、利用者の要求に応じて情報提供者から利用者にデータを配信する通信系と、通信系により情報提供者から配信されるデータのうち、利用者の要求するソフトウェアを記録する主データ領域と、利用者固有のデータおよび課金データを含む上記ソフトウェアに関連する付加データを記録する付加データ領域とを備えた書換え可能な利用者記録媒体と、利用者記録媒体の付加データ領域に記録された付加データと同一のデータを記録する情報提供者側の記録手段と、情報提供者の記録手段に記録された付加データに対して情報提供者からの書換えは許容し、利用者からの書換えを規制する手段とを備える。

【００３１】さらに利用者記録媒体の利用者固有データに該当する付加データを情報提供者の記録手段から検索し、情報提供者の記録手段の付加データと利用者記録媒体の付加データとを照合し、合致したときソフトウェアの配信処理を続行し、合致しないときソフトウェアの配信処理を中止する照合手段と、照合手段の照合結果によりソフトウェアの配信処理が続行される時、配信されるソフトウェアに応じて課金処理したうえで、情報提供者から利用者に配信されてくるソフトウェアを利用者記録媒体の主データ領域に記録させるとともに、利用者記録媒体の付加データ領域と情報提供者側の記録手段とに課金データを含む付加データを記録させる手段とを備えたものである。

【００３２】情報提供者側の記録手段に記録された付加データは、利用者からの書換えが規制されているので、たとえ利用者が利用者記録媒体の付加データを不正に変更し得たとしても、利用者は情報提供者側の記録手段の付加データまでは変更することはできない。したがって利用者記録媒体が書換え可能であっても、利用者記録媒体を不正に書換えて使用することはできない。利用者記録媒体の付加データ領域に記録された付加データと同一内容のデータを情報提供者側の記録手段に記録するだけの簡単な構造で、書換え可能な利用者記録媒体を使っても、偽造や改ざんによる利用者記録媒体の不正使用を防止することができる。

【００３３】

【発明の実施の形態】以下に本発明のデータ配信方法および装置を、情報提供者であるソフトウェア配信業者によって通信系を通じて配信されるゲームソフト販売に適用した実施の形態について説明する。

【００３４】システム構成図

本システムは、情報提供者であるソフトウェアを配信する配信業者から販売店に来店した利用者にゲームソフトを配信するに際して、販売店のコンピュータにセットしたリムーバブルの利用者記録媒体に、ゲームソフトを記録するに止めず、ゲームソフトの購入内容や課金データをも記録するようにして、その購入内容や課金データを通信系を利用して、ソフトウェアを配信する配信業者のコンピュータにも記録する。配信業者のコンピュータに記録されている過去の記録と利用者記録媒体の記録とを照合して不正使用を防止するようにしたものである。

【００３５】図１はソフトウェア販売システムのブロック図である。ソフトウェア配信業者１、２、３は、それぞれ独自のソフトウェア・プログラム、画像データ、音声データ、その他機械の動作を制御または拡張するための付加価値データなどのゲームに関する主データを配信する。ソフトウェア配信業者１、２、３内のコンピュータ２１、２２、２３から一般公衆回線、ＣＡＴＶ等を使用した有線や、光通信、音波、衛星放送等を使用した無線などの下りの通信系６、８、１０を介して、業者独自の主データを販売店４のコンピュータ２４に配信する。この時、配信するデータ量が非常に膨大等になる場合には、ＣＤ－ＲＯＭなどの記録媒体を利用し直接販売店４に配送し、販売店のコンピュータ２４に書込んでもよい。コンピュータ２１、２２、２３は、これらに記録されたデータを独自に管理しているので、利用者からネットワークを通じて直接アクセスしてきても、上記データを改ざんしたり、ダウンロードすることは実質的に不可能になっている。具体的には、コンピュータ２１～２３にそれぞれ独自で非公開のデータベースを構築し、それらのデータベースは販売店４のコンピュータ２４の書込み機番号と対応づけられており、登録されている販売店４以外からはアクセスできないようになっている。

【００３６】ここでは販売店４のコンピュータ２４に、業者１～３のコンピュータ２１～２３との間で通信を行う通信機能だけをもたせている。また、販売店４のコン

ピュータ２４は、利用者の集まりやすい場所、例えばコンビニエンス・ストア等商店の店内や店頭に設置したり、また販売するソフトウェアの内容に合せた商店に設置する。

【００３７】利用者１５は、書換え可能な利用者記録媒体１３を販売店４で購入するか、または既に購入してある汎用の利用者記録媒体１３を販売店４に持ち込み（符号１１）、購入したいゲームソフトを販売店４のコンピュータ２４を使って、指定した配信元の業者１～３内のコンピュータ２１～２３と通信接続する。業者内コンピュータ２１～２３と販売店コンピュータ２４との間でデータ通信を行ない、業者１～３から配信された所望のゲームソフトを利用者記録媒体１３に書込む。利用者はゲームソフトの書込まれた利用者記録媒体１３を持ち帰り（符号１２）、ゲーム本体にそのまま装着してプレイすることになる。利用者記録媒体１３に残っている金額の範囲内で、利用者はゲームに飽きたら上記方法でゲームソフトを何度でも書換えることができる。上記利用者記録媒体１３は最も普及している光磁気ディスクとしている。

【００３８】図２に示すように、利用者記録媒体１３の記憶領域Ｚはソフトウェア、データ等の書換え領域Ｚ１、個別データ領域Ｚ２、課金データ領域Ｚ３から構成される。書換え領域Ｚ１で本発明の主データ領域を構成し、個別データ領域Ｚ２および課金データ領域Ｚ３で付加データ領域を構成する。利用者が配信業者から取得しようとするゲーム機やパソコンを利用した通信対局ゲーム、または画像データ、音楽データ等のデータが書換え領域Ｚ１に書き込まれるが、それ以外の情報は付加データとして個別データ領域Ｚ２および課金データ領域Ｚ３に書き込まれる。ここで個別データ領域は商品管理台帳に相当し、また課金データ領域は通帳に相当する。

【００３９】利用者がソフトウェアを購入するために、販売店コンピュータ２４の書込み機２５に利用者記録媒体１３をセットすると、販売店コンピュータ２４は、配信業者１～３から配信されてきたゲームソフトを利用者記録媒体１３の書換え領域Ｚ１に書き込むとともに、個別データ領域Ｚ２および課金データ領域Ｚ３に付加データを書き込む。この利用者記録媒体１３への書込みを行うと同時に、利用者記録媒体１３内に書込まれた個別データおよび課金データと同一のデータを販売店コンピュータ２４から上りの通信系５、７、９を介してソフトウェアを配信する業者１～３のコンピュータ２１～２３にも送り、当該業者コンピュータ２１～２３に同一内容の個別データおよび課金データを記録する。

【００４０】配信業者１～３は利用者１５の利用者記録媒体１３の課金データを参照して、課金データ内の残高より配信ソフトウェアの金額を減算して決済処理する。また個別データをも参照して、加算、照合などの他の決済処理もおこなう。

【００４１】上記通信系の課金システムは、衛星放送やインターネット上などの不特定多数の利用者に対する付加価値データの配信などの際に利用できる。なお、本発明の情報提供者側の記録手段、規制する手段、照合手段、記録させる手段は、情報提供者側のコンピュータ２１～２３で構成される。

【００４２】利用者記録媒体に記録される個別データ、課金データ

(1) 個別データ

図３は利用者１５の書換え可能な利用者記録媒体１３の記憶領域Ｚ内の一部を個別データ領域Ｚ２として割当て、個別データを記憶したデータフォーマット例である。

【００４３】個別データ領域データフォーマットとして、購入ソフトウェアの名称Ａ１、購入ソフトウェアの金額Ａ２、購入した店舗Ａ３、購入した日時Ａ４、コンピュータからなる書込み機の番号Ａ５を１ブロックとする。ソフトウェアを購入する毎に１ブロック（Ｂ１～Ｂ５）、（Ｃ１～Ｃ５）単位で追加していく。これにより過去の個別データが更新されることなく蓄積記録される。なおこれら個別データ領域のデータフォーマットは目的に応じて仕様を定めることで機能拡張が可能である。

【００４４】①個別データ例

１９９７年４月１０日１６時２５分にザーコンビニ蒲田店で「最強将棋１９９７」を５，８００円で購入した場合のＡ１からＡ５の個別データとして、領域Ａ１には購入したソフトウェアの名称として「最強将棋１９９７」を、Ａ２には購入したソフトウェアの金額として５，８００円を簡略化した「５８００」を、Ａ３には購入した販売店の名称として「ザーコンビニ蒲田店」を、Ａ４には購入した日時（１９９７年４月１０日１６時２５分）を簡略化した「９７０４１０１６２５」を、Ａ５には購入した販売店の書込み機番号「００００２５３７」をそれぞれ記憶する。

【００４５】②１９９７年５月５日１１時３８分に丸大デパート新宿店で「ベストゴルフ長野県」を４，９００円で購入した場合のＢ１からＢ５の個別データとして、領域Ｂ１には購入したソフトの名称として「ベストゴルフ長野県」を、Ｂ２には購入したソフトの金額として４，９００円を簡略化した「４９００」を、Ｂ３には購入した販売店（店舗）の名称として「丸大デパート新宿店」を、Ｂ４には購入した日時（１９９７年５月５日１１時３８分）を簡略化した「９７０５０５１１３８」を、Ｂ５には購入した販売店の書込み機の番号「０００００２７１」をそれぞれ記憶する。

【００４６】③１９９７年６月２０日２１時５７分に四越デパート渋谷店で「麻雀リーチ一発」を５，５００円で購入したばあいのＣ１からＣ５の個別データとして、領域Ｃ１には購入したソフトの名称として「麻雀リーチ

一発」を、Ｃ２には購入したソフトの金額として５，５００円を簡略化した「５５００」を、Ｃ３には購入した販売店の名称として「四越デパート渋谷店」を、Ｃ４には購入した日時（１９９７年６月２０日２１時５７分）を簡略化した「９７０６２０２１５７」を、Ｃ５には購入した販売店の書込み機の番号「００００５９６３」とそれぞれ記憶する。

【００４７】(2) 課金データ

図４は利用者１５の書換え可能な利用者記録媒体１３の記憶領域Ｚ内の一部を課金データ領域Ｚ３として割当て、課金データを記憶した使用例である。

【００４８】課金データ領域データフォーマットとして、課金データと金額課金データとを含ませる。課金データは利用者の固有データであり、購入者の利用者ＩＤＤ１、暗証番号Ｄ２、生年月日Ｄ３、性別Ｄ４からなる。金額課金データは、課金日時Ｅ１、入金額Ｅ２、出金額Ｅ３、残高Ｅ４、課金店舗Ｅ５とからなる。金額課金データＥ１～Ｅ５を１ブロックとして、入出金する毎に１ブロック（Ｆ１～Ｆ５）、（Ｇ１～Ｇ５）、（Ｈ１～Ｈ５）単位で追加していく。これにより過去の個別データが更新されることなく蓄積記録される。なおこれら課金データ領域のデータフォーマットも目的に応じて仕様を定めることで機能拡張が可能である。

【００４９】①課金データ例

領域Ｄ１には、購入者の利用者ＩＤ番号として「ＳＴ７８１２４９」を登録する。これは所有者個人に定めた固有のＩＤである。領域Ｄ２には、暗証番号として本人の意思により決定した暗証番号「７２９８」が登録される。領域Ｄ３には、購入者の生年月日、例えば昭和３４年２月２３日である場合には西暦に直した「１９５９．２．２３」が登録される。領域Ｄ４には購入者の性別として男性の場合は「０」を、女性の場合は「１」を登録する。

【００５０】②１９９７年４月１０日１６時２０分にザーコンビニ蒲田店で２０，０００円の課金額を購入（入金）した場合のＥ１からＥ５の課金データとして、Ｅ１には課金の日時１９９７年４月１０日１６時２０分を簡略化した「９７０４１０１６２０」を、Ｅ２には入金額２０，０００円を簡略化した「２００００」を、Ｅ３には出金額として０円を簡略化した「０」を、Ｅ４には残高として２０，０００円を簡略化した「２００００」をそれぞれ記憶する。

【００５１】③１９９７年４月１０日１６時２５分にザーコンビニ蒲田店で５，８００円のソフトウェアを購入した場合のＦ１からＦ５の課金データとして、Ｆ１には課金の日時１９９７年４月１０日１６時２５分を簡略化した「９７０４１０１６２５」を、Ｆ２には入金額として０円を簡略化した「０」を、Ｅ３には出金額としてソフトウェアウェーハ購入金額の５，８００円を簡略化した「５８００」を、Ｆ４には購入後の残高としてＥ４＋Ｆ２－Ｆ３＝１４，２００円を簡略化した「１４２００」をそれぞれ記憶する。

【００５２】④１９９７年５月５日１１時３８分に丸大デパート新宿店で４，９００円のソフトウェアを購入した場合のＧ１からＧ５の課金データとして、Ｇ１には課金の日時１９９７年５月５日１１時３８分を簡略化した「９７０５１１３８」を、Ｇ２には入金額として０円を簡略化した「０」を、Ｇ３には出金額としてソフトウェア購入金額の４，９００円を簡略化した「４９００」を、Ｇ４には購入後の残高としてＦ４＋Ｇ２－Ｇ３＝９，３００円を簡略化した「９３００」をそれぞれ記憶する。

【００５３】⑤１９９７年６月２０日２１時５７分に四越デパート渋谷店で５，５００円のソフトウェアを購入した場合のＨ１からＨ５の課金データとして、Ｈ１には課金の日時１９９７年６月２０日２１時５７分を簡略化した「９７０６２０２１５７」を、Ｈ２には入金額として０円を簡略化した「０」を、Ｈ３には出金額としてソフトウェア購入金額の５，５００円を簡略した「５５００」を、Ｈ４を購入後の残高としてＧ４＋Ｈ２－Ｈ３＝３，８００円を簡略化した「３８００」をそれぞれ記憶する。

【００５４】データの流れ

販売店に設置したコンピュータ２４と配信業者１～３に設置したコンピュータ２１～２３間を結ぶ通信系５～１０を利用してソフトウェアを配信するとともに、現金データを含むデータをやりとりする。配信業者１～３はソフトウェア購入者の利用者記録媒体１３から送られてくるデータについて過去の記録と照合し、合致したら処理を続行し、合致しなかったら処理を中止し、しかるべき措置をとる。

【００５５】(1) 偽造発見の仕組み

販売店４を介して利用者記録媒体１３の付加データ領域Ｚ２、Ｚ３に付加データを正規に書込むときは、同時に配信業者１～３側に設置されたコンピュータ２１～２３にも同一内容の付加データが書込まれる。したがってソフトウェア配信業者１～３のコンピュータ２１～２３には登録された全ての利用者の利用者記録媒体１３の課金データが記録されている。利用者記録媒体１３への不正な書込みがない限り、利用者記録媒体１３とコンピュータ２１～２３との付加データの内容は一致している。

【００５６】さて図５に示すように、ステップ１０１で利用者記録媒体１３内の課金データのＩＤ番号より、ソフトウェア配信業者１～３のコンピュータ２１～２３内の課金データからＩＤ番号に該当する課金データを検索し、利用者記録媒体１３に記録されている課金データとの照合を行う。ステップ１０２で照合した結果、データが合致する場合はステップ１０３に進み、課金データは正常であると判断され、課金処理を含む配信処理に移行する。データが合致しない場合はステップ１０４に進

み、課金データは異常であると判断され配信処理を中止する。必要な場合は利用者記録媒体１３を販売店コンピュータ２４の書込み機から強制的に排出したり、配信業者１～３が利用者記録媒体１３の不正使用者を特定して、しかるべき措置をとったりする。

【００５７】(2) 照合後の流れ

正しい照合結果がでると、ソフトウェア配信業者１～３は利用者が所望するゲームソフトをネットワークを利用して販売店に配信する。このとき課金データ内の生年月日（Ｄ３）（図４）を参照して、もし配信層に年齢制限のあるゲームソフトの場合で年齢制限にひっかかったときは、規制して配信を中止する。必要に応じて、その旨のメッセージをコンピュータ２４から出力させてもよい。

【００５８】配信を受けたゲームソフトは販売店４のコンピュータ２４により利用者記録媒体１３内の書換え領域Ｚ１に記録される。また利用者記録媒体１３の個別データ領域Ｚ２および課金データ領域Ｚ３に前述した必要なデータを記録する。このときソフトウェア配信業者１～３のコンピュータ２１～２３の個別データ領域Ｚ２および課金データ領域Ｚ３にも、通信系５、７、９を介して同じデータを記録する。

【００５９】このように本実施の形態は、利用者から直接アクセスすることが不可能なソフトウェア配信業者のコンピュータに、利用者記録媒体に記録された同一の付加データを記憶するようにしている。このため利用者側の付加データと情報提供者側の付加データとの照合により、利用者記録媒体の偽造や改ざん更にはデータの二重使用も確認できるので、記録媒体が書換え可能な媒体であっても、偽造に強く、信頼性を向上できる。

【００６０】また販売店では、カードリーダのような専用機を必要とせず、光磁気ディスクドライブを装着した既存のパソコンが使用できるので、システムを安価に構築することができる。特に光磁気ディスクは容量が大きいので、ＩＣカードと異なり、大容量のゲームソフトを制約なしに記録できる。また残金が許す限りゲームソフトの書換えは何度でもできる。また、光磁気ディスクの購入に際して、クレジットカードのような面倒で時間のかかる契約を必要としないので、利用者の拡大が図れる。しかも、１枚の光磁気ディスクにソフトウェアと付加データとを書込むようにしたので、ゲームソフトとソフト購入用のカードとを同時に購入できることになり、別個に購入する場合に比較して、利用者にとって非常に便利になる。

【００６１】利用者記録媒体に記録された個別データなどの付加データは、ソフトウェア配信業者のコンピュータにも記録されるので、クレジットカードと異なり、ソフトウェアの販売／売上管理ができ、リアルタイムで販売状況を把握することもできる。このシステムはＰＯＳ端末を導入するよりも安価であり、しかもＰＯＳと同等のシステムを構築できる。

【００６２】また、利用者記録媒体はプリペイドカードと異なり書換え可能であり、そこに付加データを再充填できる付加データ領域を設けたので、通常は減算されるのみであるが、加算することもできるようになる。例えばソフトウェアを配信している業者から、アンケートのお礼や、抽選による賞品、または他人からの譲渡によって、利用者記録媒体内の付加データとして、存在する付加データに、利用権利を加算することが可能となる。このように、情報を提供する側が、自由に利用者に対して、そのサービスの利用権を加算することができる。

【００６３】また、利用者記録媒体は、利用者記録媒体内の現金データを使いきってしまっても、現金データを書き込めば同じ利用者記録媒体を何度でも利用できるので、資源の有効利用が図れる。

【００６４】そして、利用料金の請求をクレジットカードを所持している人物に限定していた従来方式のものに比べて、利用者記録媒体内に付加データとして書き込まれた付加データを利用するようにしたので、クレジットの枠を取り外すことができる。このように通信にからむ課金システムとして、クレジットカードや、プリペイドカード以外に、安全かつ簡易に付加データを参照できる。特に、付加データをブロック単位で追加して過去の支払い記録を全て残すようにし、残高を除いてデータ内容を更新しないようにしたので、データが改ざんされても、過去の記録と照合することで、データの改ざんなどを簡単に発見できる。

【００６５】なお、上記実施の形態では課金データを照合するようにしたが、付加データの全てについて照合するようにしてもよい。また、ソフトウェア配信業者のコンピュータで照合して販売店での不正も防止するようにしたが、そのようなおそれがなければ、販売店に照合機能をもたせることも可能である。例えば、販売店４のコンピュータ２４に、登録された全ての利用者の利用者記録媒体１３の課金データを記録する。利用者記録媒体１３内の課金データのＩＤ番号より、販売店４のコンピュータ２４内の課金データからＩＤ番号に該当する課金データを検索し、利用者記録媒体１３に記録されている課金データとの照合を行うようにする。

【００６６】また、大規模化を想定してネットワークを導入しているが、ネットワークを使わない小規模なシステムも構築することは可能である。

【００６７】書換え可能な利用者記録媒体としては、ゲームカセット、フロッピーディスク、磁気ディスク、光磁気ディスク（ＭＯ）、光ディスク、リムーバブルハードディスク（ｚｉｐ、ｊａｚ、ＰＤと呼ばれているものを含む）、または将来予想される大容量のＩＣメモリカード等がある。

【００６８】また、①販売するソフトウェアや、②付加価値データの内容によって時間課金のものや、③付加価

値データの量による課金のもの、④また付加価値データの質による課金のものなど、課金基準が違うものに対しても一つのステムで、総合的、簡易かつ安全に管理することができる。またセキュリティを高めるために付加データを暗号化してもよい。

【００６９】また上記実施形態では利用者記録媒体の記録領域を個別データ領域と課金データ領域とに分け、データを一部重複させるようにしたが、データ付加領域としてまとめてデータの重複を避けるようにしてもよい。また配信するソフトウェアはゲームソフトに限定されないことはもちろんである。

【００７０】

【発明の効果】請求項１に記載の発明によれば、

(1) 利用者側から直接アクセスできない情報提供者のコンピュータにも利用者記録媒体の付加データが記録されているため、利用者記録媒体が偽造されたり、利用者記録媒体が書換え可能であるため勝手に書換えられたりしても、利用者記録媒体の付加データと情報提供者のコンピュータの付加データとを照合することにより、その不正使用を有効に防止することができ、その結果ソフトウェアを簡易かつ安全に配信することができる。

【００７１】(2) 利用者記録媒体を購入するだけで入会することができ、クレジットカードのように契約加入を必要としないので、利用者の拡大を図ることができる。

【００７２】(3) １枚の利用者記録媒体にソフトウェアと課金データを含む付加データとを記録できるようにして、ソフトウェアの入れ物と現金の機能とをもたせたので、１枚の利用者記録媒体を購入するだけで、ソフトウェアの購入が可能となり、利用者の手続の簡素化が図れる。

【００７３】(4) 利用者記録媒体の付加データを情報提供者側のコンピュータにも記録するようにして、情報提供者が利用者記録媒体に記録された付加データを管理できるようにしたので、付加データにソフトウェア内容や課金データを含めれば、配信されるソフトウェアの販売／売上管理が容易にできる。

【００７４】請求項２に記載の発明によれば、利用者記録媒体は書換え可能だから、一方的に利用者記録媒体の価値ないし権利を減らしていくにとどまらず、利用者記録媒体に入金して増額することにより、情報提供者側から利用者にサービスを供与していくこともできる。

【００７５】請求項３に記載の発明によれば、利用者記録媒体に光磁気ディスクを使用すれば、既存のパソコンを利用でき、システムを安価に構築できる。

【００７６】請求項４に記載の発明によれば、利用者が購入しようとするソフトウェアを記録させる利用者記録媒体に付加データ領域を増設して、付加データ領域に課金データやソフトウェア関連データなどの付加データを記録させるとともに、この付加データを同時に情報提供者側の記録手段にも記録させて、両付加データを管理するという簡単な構造で、信頼性の高いデータ配信システムを構築することができる。

【図面の簡単な説明】

【図１】実施形態によるシステム構成図。

【図２】実施形態による利用者記録媒体内の記憶領域の割当て図。

【図３】実施形態による個別データ領域のデータフォーマットおよびデータ例を示す図。

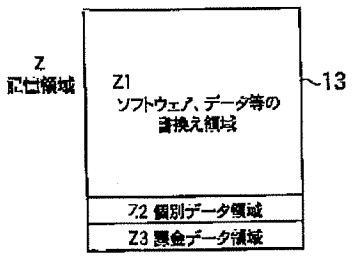
【図４】実施形態による課金データ領域のデータフォーマットおよびデータ例を示す図。

【図５】利用者記録媒体の偽造発見のフロー図。

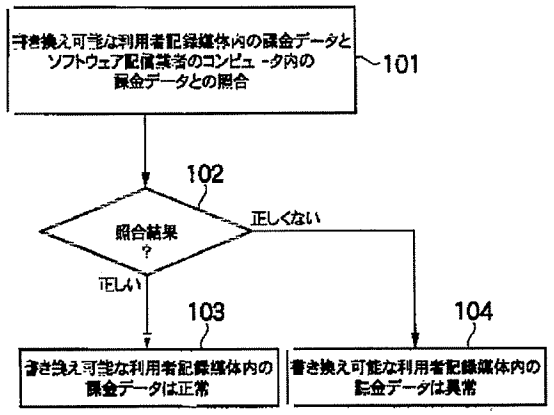
【符号の説明】

１～３　　ソフトウェア配信業者
４　　販売店
５～１０　　通信系
１３　　利用者記録媒体
１５　　利用者
２１～２３　　配信業者側のコンピュータ
２４　　販売店側のコンピュータ

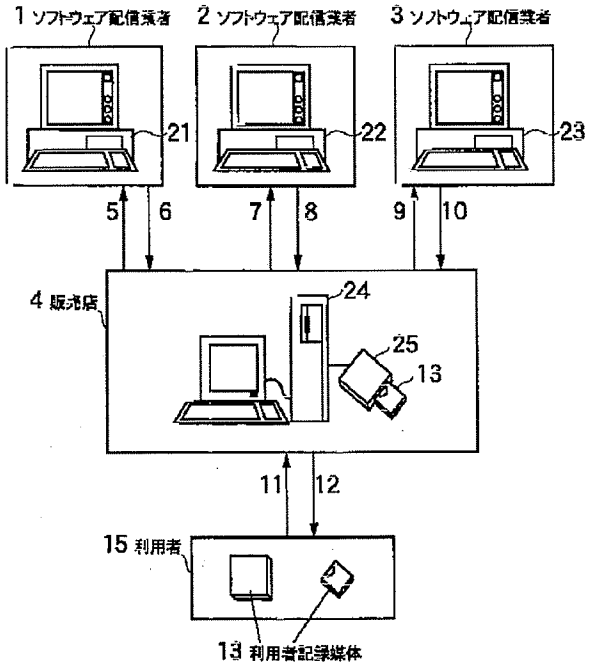
【図２】



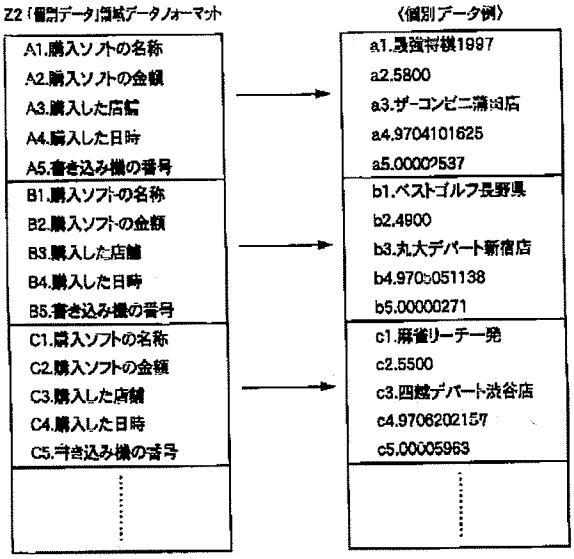
【図５】



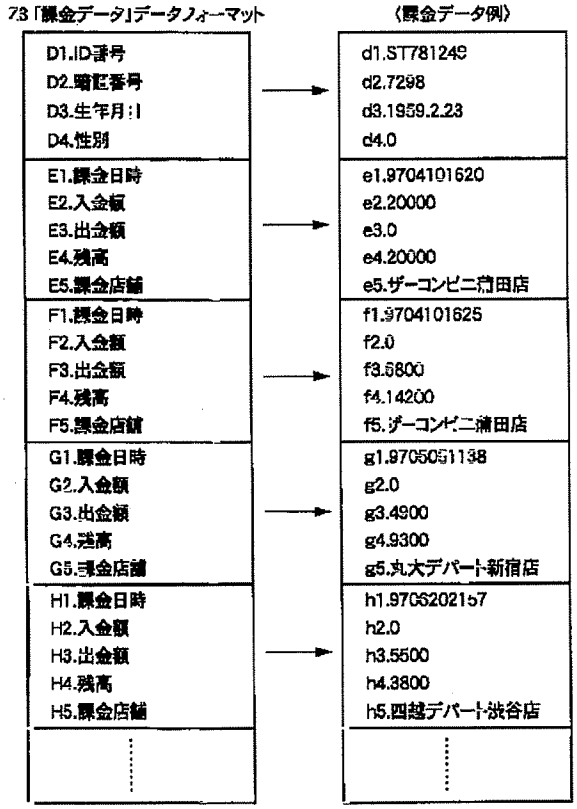
【図１】


1 ソフトウェア配信業者
2 ソフトウェア配信業者
3 ソフトウェア配信業者
21
22
23
5
6
7
8
9
10
4 販売店
24
25
13
11
12
15 利用者
13 利用者記録媒体

【図３】


Z2「個別データ」領域データフォーマット
A1.購入ソフトの名称
A2.購入ソフトの金額
A3.購入した店舗
A4.購入した日時
A5.書き込み機の番号
B1.購入ソフトの名称
B2.購入ソフトの金額
B3.購入した店舗
B4.購入した日時
B5.書き込み機の番号
C1.購入ソフトの名称
C2.購入ソフトの金額
C3.購入した店舗
C4.購入した日時
C5.書き込み機の番号
〈個別データ例〉
a1.最強将棋1997
a2.5800
a3.ザーコンビニ蒲田店
a4.9704101625
a5.00002537
b1.ベストゴルフ長野県
b2.4900
b3.丸大デパート新宿店
b4.9705051138
b5.00000271
c1.麻雀リーテー発
c2.5500
c3.四越デパート渋谷店
c4.9706202157
c5.00005963

【図４】


Z3「課金データ」データフォーマット
D1.ID番号
D2.暗証番号
D3.生年月日
D4.性別
E1.課金日時
E2.入金額
E3.出金額
E4.残高
E5.課金店舗
F1.課金日時
F2.入金額
F3.出金額
F4.残高
F5.課金店舗
G1.課金日時
G2.入金額
G3.出金額
G4.残高
G5.課金店舗
H1.課金日時
H2.入金額
H3.出金額
H4.残高
H5.課金店舗
〈課金データ例〉
d1.ST781249
d2.7298
d3.1959.2.23
d4.0
e1.9704101620
e2.20000
e3.0
e4.20000
e5.ザーコンビニ荏田店
f1.9704101625
f2.0
f3.5800
f4.14200
f5.ザーコンビニ蒲田店
g1.9705051138
g2.0
g3.4900
g4.9300
g5.丸大デパート新宿店
h1.9706202157
h2.0
h3.5500
h4.3800
h5.四越デパート渋谷店

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-053184
(43)Date of publication of application : 26.02.1999

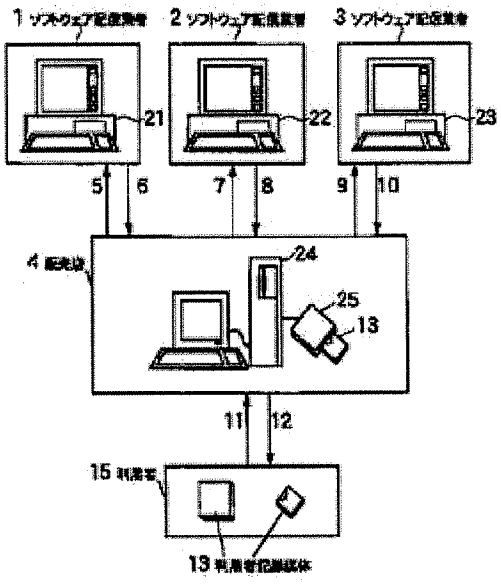
(51)Int.Cl. G06F 9/06
G09C 1/00
H04L 9/32

(21)Application number : 09-214318
(22)Date of filing : 08.08.1997

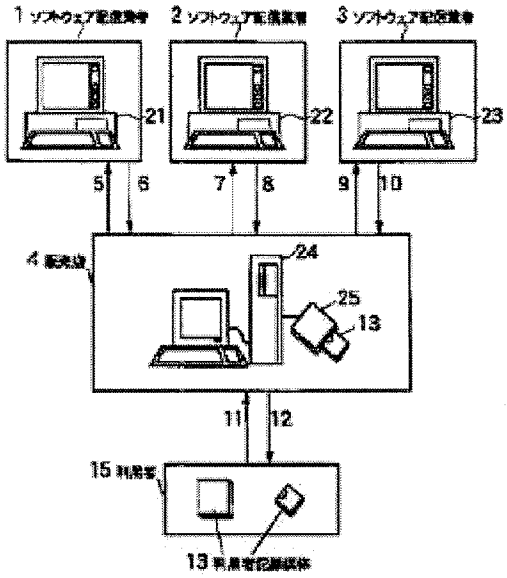
(71)Applicant : SETA:KK
(72)Inventor : FUJIMOTO ATSUSHI

(54) DATA DISTRIBUTION METHOD AND DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To easily construct a system with high security by recording additional data like individual data, charging data of a user as well in a rewritable recording medium used for rewriting of game software and collating the additional data with a computer of a software distributor.
SOLUTION: A user recording medium 13 to rewrite the game software is purchased at a store 4 and a fixed amount of cash data is deposited in the user recording medium 13. In this case, intrinsic data of the user is also written in the user recording medium 13. When the game software is requested from a computer 24 of the store 4, data of the user recording medium 13 is transmitted to software distributors 1 to 3 by communication systems 5, 7, 9 and collated with the past additional data recorded in computers 21 to 23 of the distributors. When the data of the user recording medium 13 coincides with the past additional data, the game software is distributed from the distributors to the store 4 by using communication systems 6, 8, 10 and recorded in the user recording medium 13. The additional data regarding the game software is simultaneously recorded in the user recording medium 13 and the computers 21 to 23 of the software distributors 1 to 3.



DATA DISTRIBUTION METHOD AND DEVICE



(57)Abstract:
PROBLEM TO BE SOLVED: To easily construct a system with high security by recording additional data like individual data, charging data of a user as well in a rewritable recording medium used for rewriting of game software and collating the additional data with a computer of a software distributor.
SOLUTION: A user recording medium 13 to rewrite the game software is purchased at a store 4 and a fixed amount of cash data is deposited in the user recording medium 13. In this case, intrinsic data of the user is also written in the user recording medium 13. When the game software is requested from a computer 24 of the store 4, data of the user recording medium 13 is transmitted to software distributors 1 to 3 by communication systems 5, 7, 9 and collated with the past additional data recorded in computers 21 to 23 of the distributors. When the data of the user recording medium 13 coincides with the past additional data, the game software is distributed from the distributors to the store 4 by using communication systems 6, 8, 10 and recorded in the user recording medium 13. The additional data regarding the game software is simultaneously recorded in the user recording medium 13 and the computers 21 to 23 of the software distributors 1 to 3.

TECHNICAL FIELD

[Field of the Invention]This invention relates to what starts a data distribution method and a device, especially performs distribution and fee collection of data simultaneously using a rewritable recording medium.

PRIOR ART

[Description of the Prior Art]As a typical card used instead of cash, there are a prepaid card, a credit card, and an IC card.

[0003]A prepaid card is a kind of coupon ticket which wrote in required information using magnetism instead of ink.

It is the structure it will become impossible to use if only the part of the purchased amount currently recorded on the magnetic card can be used and it has used.

For example, there are a pachinko card, a telephone card, an IO card, etc. The actual condition is that there is no effective measure to an unauthorized use.

[0004]A credit card can be used by the member's store which deals with this card, carries out fixed time postponement of the payment and payment of a commodity price, and settles a commodity price by automatic accounts transfer from a bank account. Authorization is needed in order to prevent an unauthorized use. The charging method of a system utilization charge for added value data and various control data to come to hand using a wired telephone line, a radio telephone network, satellite broadcasting, etc. has the common settlement of accounts by this credit card.

[0005]An IC card provides the memory part and microprocessor part which are memory storage in IC, and gives logical processing capabilities, such as data creation and judgment, to the card itself. Electronic money etc. hit this. By IC embedded on the card, the check function of truth or falsehood and the rewritable memory storage function which stores the transmitted electronic money data occur. Since a rewritable memory storage function occurs, an IC card can also be made to pay also from other than a user.

EFFECT OF THE INVENTION

[Effect of the Invention]Since the attached data of the user recording medium is recorded also on the computer of the information provider who cannot carry out direct access from the (1) user side according to the invention according to claim 1, Since a user recording medium is forged, or a user recording medium is rewritable, even if it is rewritten by the kitchen, By comparing the attached data of a user recording medium, and the attached data of an information provider's computer, the unauthorized use can be prevented effectively and, as a result, software can be distributed simply and safely.

[0071](2) It can register as a club member only by purchasing a user recording medium, and since contract subscription is not needed like a credit card, a user's expansion can be aimed at.

[0072](3) Since the receptacle of software and the function of cash were given to it as software and the attached data containing billing data could be recorded on the user recording medium of one sheet, only by purchasing the user recording medium of one sheet, the purchase of software is attained and simplification of a user's procedure can be attained.

[0073](4) Since the information provider enabled it to manage the attached data recorded on the user recording medium as the attached data of a user recording medium was recorded also on the computer by the side of an information provider, If the contents of software and billing data are included in attached data, sale/sales management of the software distributed can be performed easily.

[0074]According to the invention according to claim 2, since a user recording medium is rewritable, it can also supply a user with service from the information provider side by not remaining for on the other hand reducing the value thru/or the right of a user recording medium on a target, but paying a user recording medium, and increasing.

[0075]According to the invention according to claim 3, if a magneto-optical disc is used for a user recording medium, the existing personal computer can be used and a system can be built cheaply.

[0076]According to the invention according to claim 4, an attached data field is extended to the user recording medium on which the software which a user is going to purchase is made to record, While making attached data, such as billing data and software associated data, record on an attached data field, this attached data can be made to be able to record also on the recording device by the side of an information provider simultaneously, and a reliable data distribution system can be built with an easy structure of managing both attached data.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention]However, when it was going to distribute software using these cards, the following problems were among the conventional card systems mentioned above.

[0007](1) Since the prepaid card ** user's individual data was not being interlocked with a management computer, it is weak to forgery of the prepaid card itself. It is well-known that forgery is actually actualizing with the pachinko card.
[0008]** Since readers, such as a card reader for exclusive use, are required, miniaturization, power-saving, and low-pricing cannot be performed.
[0009]** When the cash data or frequency data in a card is exhausted, it becomes impossible to reuse, since it cannot be re-filled up with data.
[0010]** When purchasing software with the software vending machine currently installed in the form of the vending machine, communication -- a game -- when purchasing the communication use type software which acquires picture information and music information using a game or communication, it is necessary to purchase a prepaid card separately from those software, it sees from a user, and is dramatically inconvenient.
[0011](2) Since a credit card ** user will be limited to the possessor of a credit card, it becomes an obstacle in respect of a user's expansion.
[0012]** For the Reasons of it being troublesome and being, the contract of the credit card has been an obstacle in a user's expansion.
[0013]** The communication system of a wire telephone network or a radio telephone network is used for the sales situation of software, and since there is no function which communicates with the computer of the contractor who distributes software, sale/sales management cannot be performed.
[0014](3) Since the IC card IC card has given logical processing capabilities, such as data creation and judgment, there is no fault like the prepaid card and credit card which were mentioned above. However, there is a problem the following point.
[0015]** Since much data of versatility, such as personal data, which needs to be kept secret is contained, in order to secure security, need advanced encoding technology and anti-copying art.
[0016]** A system becomes very large-scale, and also the structure of an IC card also becomes complicated.
[0017]** Since the storage capacity is small, it is difficult to make a mass program like game software record.
[0018]** It is still difficult to realize simply and cheaply by the experimental stage.
[0019]It is (1) as it mentioned above especially, although distribution of software was already begun through the network in the game industry. In the method of - (3), the software distributed by the distribution contractor using cash data cannot be distributed simply and safely.
[0020]In the data distribution art in which SUBJECT of this invention distributes software to a user from an information provider according to a user's demand, It is in providing the data distribution method and device which can be distributed simply and safely, canceling the problem of the conventional technology mentioned above and using a rewritable recording medium.

MEANS
[Means for Solving the Problem]In a data distribution method with which software is distributed to a user from an information provider according to a user's demand as for the data distribution method according to claim 1, A rewritable user recording medium with which attached data relevant to the above-mentioned software containing data and billing data peculiar to a user is recorded is used, Attached data applicable to user proper data of a user recording medium is searched from an information provider's computer, Attached data memorized by an information

provider's computer and attached data memorized by user recording medium are compared, When attached data does not agree, stop message distribution processing, and message distribution processing including accounting to software which a user demands when attached data agrees is performed, While recording attached data about software distributed to a user by this message distribution processing from an information provider, and the above-mentioned software containing billing data which carried out [above-mentioned] accounting on a user recording medium, From a user, the above-mentioned attached data is recorded also on an information provider's computer by which data management is carried out so that direct access cannot be carried out.

[0022]When a cause of the forged problem of a prepaid card does not manage any billing data (usable frequency) in a prepaid card but fee collection (usable frequency) in a prepaid card is only set to 0, it is having stopped at a point recognized that the prepaid card is used. It is made for this invention to discover a forged rewritable recording medium at the time of use by managing attached data as the technique of solving this SUBJECT, rather than preventing forgery.

[0023]According to this invention, when regular attached data is recorded on a user recording medium which a user can rewrite, attached data of an identical content is simultaneously recorded also on an information provider's computer. Therefore, when data is unjustly written in a user recording medium or a user recording medium is forged regardless of an information provider's computer. Since incorrect data thru/or the same attached data as a user recording medium are not recorded on an information provider's computer, data of the past recorded on a user recording medium and an information provider's computer becomes inharmonious. As a result, an unauthorized use of a user recording medium with which forgery or data was altered can be effectively prevented by comparing attached data.

[0024]Since attached data relevant to software written in a user recording medium is recorded on a computer of an information provider who distributes software simultaneously with the purchase of software and is accumulated, it can perform sale/sales management of software. Since both sides of software, such as a game, and attached data containing billing data were recorded on a user recording medium of one sheet, It is not necessary to purchase separately a recording medium for software wear, and a prepaid card for software purchase like before, and purchasing a user recording medium of one sheet only serves the purpose.

[0025]Since anyone can receive data distribution service only by not needing contract subscription like a credit card, but purchasing a user recording medium regularly if a user recording medium which anyone can purchase is adopted, a user's expansion can be aimed at.

[0026]When a user fulfills service supply conditions in the above-mentioned invention, in order to supply a user with service from an information provider, the data distribution method according to claim 2, A user recording medium receives a predetermined amount of money from an information provider's computer, and the record is recorded also on an information provider's computer.

[0027]Since a user only purchases products, such as software, when purchasing using a prepaid card, a prepaid card is only reduced. However, in this invention that uses a rewritable user recording medium, since it can access to an information provider's computer to a user recording medium freely, a user recording medium can receive the amount of money corresponding to the above-mentioned service, and billing data can be increased.