CONTENT USING SYSTEM

TECHNICAL FIELD

The present invention relates to a system for using digital contents, such as images, video and audio, that have been distributed via communication, a broadcast, etc., and in particular relates to control over the use of contents when contents are written onto an external storage medium.

BACKGROUND ART

In recent years, systems in which digital contents, such as music, video, images, and games, are distributed via the Internet or a digital broadcast and then used have reached the implementation stage.

As can be understood from the patent documents #1 to #3 listed below, in a conventional content using system, a content that has been distributed via a broadcast is bound to a network so that the content can be shared within the network and used. Here, the "binding" of a content to a network refers to a condition where only authorized terminals on the network are able to use the content. Putting this another way, if a content is bound to the network, even if a different, non-authorized terminal is connected to the network, such terminal will not be able to use the content. Additionally, if a content that has been bound to a network is moved to another network, terminals on this other network will not be able to use the content.

As one example, when a content that has been encrypted and then distributed is imported into a network (such as a home network), the content can be bound to the network by having terminals on the network use the encrypted content without conversion and by converting the encryption of the encryption key

for the content. Here, "converting the encryption" refers to a process where the encryption key for the content is re-encrypted using an encryption key (hereinafter called a "network key") that has been shared on the network in advance.

When a content that has been bound to the network is used, an appliance on the network that stores the network key can use the shared network key to decrypt the content encryption key that has been re-encrypted and then use the decrypted content encryption key to decrypt the encrypted content.

On the other hand, an appliance that does not store the network key cannot decrypt the content encryption key and so is unable to decrypt the encrypted content.

With the content using systems described in the patent documents #1 to #3 listed below, limitations are imposed on the usage of contents as follows. Once a content has been bound to a network, the generation of copies of a content and the content encryption key on storage media, such as hard disk drives, on the network is unlimited for such data in a state where the data is bound to the network. However, the number of network appliances that may use (for example, reproduce) the content is limited.

Patent Document #1
Japanese Laid-Open Patent Application No. 11-331805
Patent Document #2
The specification of USP 5,878,135
Patent Document #3
The specification of USP 6,016,348

With the background art listed above, in reality it is not possible to write a content outside the network with the content in a state where the content is not bound to the network. In spite of this, there are demands from users who wish to write ("move" or

"export") a content that has been bound to the network to an external storage medium such as a DVD-RAM, D-VHS, an SD (Secure Digital) Card, etc., and then use the content.

In this way, there is the problem that conventional content using systems do not consider the writing of unbound contents, so are unable to satisfy the user demands described above.

With such conventional systems, even if it were possible to write a content in an unbound state, there would be the risk of it being possible to make an unlimited number of copies of the content onto storage media. This leads to problems regarding copyright protection for the content.

The present invention was conceived in view of the above problems with the background art, and has an object of providing a content using system that provides, for contents that have been bound to a network, a favorable balance between the conflicting aims of satisfying the above user demands and providing copyright protection.

Putting this another way, it is an object of the present invention to provide a content using system that can provide sufficient copyright protection while satisfying the demands of users regarding the writing of contents, which have been bound to a network, onto a storage medium.

DISCLOSURE OF THE INVENTION

According to a first aspect of the present invention, there is provided a content using system in which a content is used on a network to which a plurality of apparatuses are connected, comprising: a binding unit that is provided in at least one of the plurality of apparatuses and is operable to bind the content to the network by putting the content in a state where only the apparatuses on the network can use the content; an ID issuing unit that is provided in at least one of the plurality of apparatuses and is operable to issue a content ID that

corresponds to the content that has been bound by the binding unit; a bind removing unit that is provided in at least one of the plurality of apparatuses and is operable to put the content that has been bound by the binding unit in an unbound state; a writing unit that is provided in at least one of the plurality of apparatuses and is operable to write the content that has been put in the unbound state by the bind removing unit onto a storage medium; a table unit that is provided in at least one of the plurality of apparatuses and is operable to store a table showing the content ID of the content written by the writing unit; and a suppressing unit that is provided in at least one of the plurality of apparatuses and is operable to obtain the content ID of the content to be written by the writing unit and to suppress writing of the content by the writing unit based on a content of the table.

With the above construction, each content that is bound to the network is assigned a content ID, and is managed using the writing table for contents, so that the unlimited writing of contents by the writing unit may be suppressed. That is, the writing of contents in a state where the contents are not bound to the network may be limited. As one example, it may be possible to sufficiently protect the copyright of a content while satisfying the demands of individual users who wish to write a content that has been bound to a home network onto a storage medium, so that it may be possible to strike a favorable balance between the conflicting aims of users regarding personal use and of the copyright holder.

Here, the suppressing unit may be operable to obtain the content ID of the content to be written by the writing unit, to add, if the obtained content ID has not been already recorded in the table, the content ID to the table without suppressing the writing of the content by the writing unit, and to suppress the writing of the content by the writing unit if the obtained content ID is present in the table.

With the above construction, if the content ID is already present in the table, the suppressing unit may suppress the writing of the content by the writing unit, so that the writing of each content by the writing unit may be permitted once and then prohibited for the second time onwards.

Here, the suppressing unit may be operable to obtain the content ID of the content to be written by the writing unit, to add, if the obtained content ID is not present in the table, the obtained content ID to the table and "1" as a number of writes by the writing unit, and to suppress the writing by the writing unit if the obtained content ID is present in the table and the number of writes has reached a predetermined maximum number.

With the above construction, the suppressing unit may suppress the writing by the writing unit when the content ID is present in the is table and the number of writes has reached a maximum number, so that writing by the writing unit may be permitted within a range of the maximum number for each content and prohibited when the range is exceeded. One value may be set in advance as the maximum number, or the maximum number may be set for each content, so that the balance between the conflicting aims of users and the copyright holder can be set flexibly.

Here, the binding unit may be operable to bind the content to the network by encrypting a content key for decrypting the content using a network key that is shared in advance with the plurality of apparatuses.

With the above construction, it may not be necessary to re-encrypt the content itself using the network key, so that the processing load of binding a content may be reduced.

Here, the plurality of apparatuses may include one content importing apparatus and at least one content using apparatus, the content importing apparatus may include the binding unit and the ID issuing unit, and each of the content using apparatuses may include the

table unit, the bind removing unit, the writing unit, and the suppressing unit.

With the above construction, the processing for the binding of a content and the generation of a content ID may be concentrated in the content importing apparatus, only one of which is present on the network.

Here, the content using apparatuses may further include: a notifying unit operable to notify, when a write has been performed by the writing unit, other content using apparatuses of at least the content ID; and an updating unit operable to update a table stored in the table unit when a notification is received from another content using apparatus.

With the above construction, the content of the table may be easily made to match in a plurality of content using apparatuses on the network.

Here, the content using system may include one content importing apparatus and at least one content using apparatus, wherein the content importing apparatus may include the binding unit, the ID issuing unit, the table unit and the suppressing unit, and each of the content using apparatuses may include the bind removing unit, and the writing unit.

With the above construction, the processing for the binding of a content, the generation of a content ID, the managing of the table, and the suppressing of writing may be concentrated in the content importing apparatus, only one of which is present on the network. Each content using apparatus may only need to perform writes in accordance with the suppressing unit in the content importing apparatus, so that managing the table may create no load for individual content importing apparatuses.

The content using method and content using program of the example embodiments have the same construction, operation and effects as those described above.

According to a second aspect of the present invention, there is provided a content using system including a content importing apparatus and at least one content using apparatus that share a network key, where a content is bound to a network by encrypting content key information, which includes a content key required to decrypt the content, using the network key, the content importing apparatus including: an obtaining unit operable to obtain a content and encrypted content key information, which includes the content key for the content, from the outside; an ID generating unit operable to generate a content ID for identifying the content obtained by the obtaining unit; and an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key, and each content using apparatus including: a first decrypting unit operable to decrypt the re-encrypted content key information using the network key; a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit; a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium; a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing of the content by the writing unit when the number of times has reached a predetermined maximum number of times.

According to a third aspect of the present invention, there is provided a content using system including a content importing

apparatus and at least one content using apparatus that share a network key, where a content is bound to a network by encrypting content key information, which includes a content key required to decrypt the content, using the network key, the content importing apparatus including: an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside; an ID generating unit operable to generate a content ID for identifying the obtained content; an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key; a table storing unit operable to store a table that records the content ID of a content that has been written onto a storage medium by a content using apparatus; a table managing unit operable to use, when a write permission judgement request has been received from a content using apparatus, the table to judge whether writing of a content is permitted and to update the table based on a judgement result; and a content ID receiving unit operable to receive the write permission judgement request from the content using apparatus and to transmit the judgement result obtained from the table managing unit, and the content using apparatuses each including: a first decrypting unit operable to decrypt the re-encrypted content key information using the network key; a content ID transmitting unit operable to transmit to the content importing apparatus a write permission judgement request including the content ID included in the decrypted content key information and to receive the judgement result; a second decrypting unit operable to decrypt the content using the content key included in the content key information decrypted by the first decrypting unit only when the received judgement result shows that the writing is permitted; and

a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium.

According to a fourth aspect of the present invention, there is provided a content using system including a content importing apparatus and at least one content using apparatus that share a network key, where a content is bound to the network by encrypting content key information, which includes a content key required to decrypt the content, using the network key, the content importing apparatus including: an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside; an ID generating unit operable to generate a content ID for identifying the obtained content; an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key; a first table storing unit operable to store a table that records the content ID of a content that has been written onto a storage medium by a content using apparatus; a table managing unit operable to use, when a write permission judgement request has been received from a content using apparatus, the table to judge whether writing of a content is permitted and to update the table based on a judgement result; and a table transmitting unit operable to receive synchronization information from a content using apparatus and to transmit the table to the content using apparatus, and each content using apparatus including: first decrypting unit operable to decrypt the re-encrypted content key information using an encryption key that has been shared in advance on the network and to output the content key; a table receiving unit operable to transmit synchronization information for the table that includes at least a content ID to the content importing apparatus and to receive the table; a second table storing unit operable to store the table; a table managing unit operable to update the

table in the second table storing unit using the table received from the content importing apparatus and to judge whether writing of a content is permitted using the table; a second decrypting unit operable to decrypt the encrypted content using the content key only when a judgement result of the table managing unit shows that writing is permitted; and a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium.

According to a fifth aspect of the present invention, there is provided a content using system including a content importing apparatus and at least one content using apparatus that share a network key and also a content writing apparatus that is connected to at least one of the at least one content using apparatuses and writes a content onto a storage medium, where a content is bound to the network by encrypting content key information, which includes a content key required to decrypt the content, using the network key, the content importing apparatus including: an obtaining unit operable to obtain a content and encrypted content key information, which includes the content key for the content, from the outside; an ID generating unit operable to generate a content ID for identifying the obtained content; and an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key, each content using apparatus including: a first decrypting unit operable to decrypt the re-encrypted content key information using the network key; and a second decrypting unit operable to decrypt the content using the content key included in the decrypted content key information, and the content writing apparatus including: a writing unit operable to write a content onto a storage medium; a table storing unit operable to store a table for recording a content ID of the content written on the storage

medium by the writing unit; and a table managing unit operable to judge whether writing of a content is permitted using the table and to control the writing unit in accordance with a judgement result.

According to a sixth aspect of the present invention, there is provided a content using system in which a content importing apparatus and at least one content using apparatus are connected to a network, the content importing apparatus including: an encryption converting unit operable to convert encryption by decrypting encrypted content key information, generating secret information for influencing a content key, and re-encrypting the content key information using an encryption key that is shared in advance on the network and the secret information; and an output request processing unit operable to receive a content output request from a content using apparatus and to transmit a request response including at least the secret information, and the content using apparatus including: an output requesting unit operable to transmit an output request, which includes at least an output destination of a content, to the content importing apparatus, to receive the request response, and to obtain the secret information; a first decrypting unit operable to decrypt the re-encrypted content key information using an encryption key shared in advance on the network and the secret information; a control unit operable to output content output control information for controlling a selecting unit; a second decrypting unit operable to decrypt the encrypted content using the content key; a selecting unit operable to select an output destination of the content based on the content output control information; and at least one output unit operable to output the content.

According to a seventh aspect of the present invention, there is provided a content using apparatus that uses a content that has been bound to a network by encrypting content key information, which includes a content key required to decrypt the content, using a network key, the content using apparatus comprising: a first

decrypting unit operable to decrypt the re-encrypted content key information using the network key; a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit; a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium; a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing of the content by the writing unit when the number of times has reached a predetermined maximum number of times.

According to an eighth aspect of the present invention, there is provided a content importing apparatus that binds a content to a network to which a plurality of apparatuses that share a network key are connected by encrypting content key information, which includes a content key required to decrypt the content, using the network key, the content importing apparatus including: an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside; an ID generating unit operable to generate a content ID for identifying the content obtained by the obtaining unit; and an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key, wherein the content ID is used to manage writing

of the content, which has been bound to the network, onto a storage medium in an unbound state.

According to a ninth aspect of the present invention, there is provided a content using method of using a content on a network to which a plurality of apparatuses are connected, the method comprising: a binding step which is performed in at least one of the plurality of apparatuses and in which a content is bound to the network by putting the content in a state where only apparatuses on the network can use the content; an ID issuing step which is performed in at least one of the plurality of apparatuses and in which a content ID that corresponds to the content that has been bound to the network in the binding step is issued; a judging step which is performed in at least one of the plurality of apparatuses and in which a content ID of a content, which has been bound to the network and is to be written in an unbound state, is obtained, a table in which content IDs of contents that have already been written is recorded is referred to in a memory, and a judgement of whether writing the content is permitted is made; a bind removing step which is performed in at least one of the plurality of apparatuses and in which the content that has been bound to the network by the binding unit is put in an unbound state when the judgement in the judging step is that writing is permitted; and a writing step which is performed in at least one of the plurality of apparatuses and in which the content put in the unbound state in the bind removing step is written onto a storage medium.

According to a tenth aspect of the present invention, there is provided a content using method performed by an apparatus that uses a content that has been bound to a network by encrypting content key information, which includes a content key that is required to decrypt the content, using a network key, the content using method comprising: a first decrypting step of decrypting the encrypted content key information using the network key; a second decrypting

step of decrypting the content using the content key in the content key information decrypted in the first decrypting step; a judging step of obtaining a content ID of a content, which has been bound to the network and is to be written in an unbound state, referring to a table, in which content IDs of contents that have already been written is recorded, in a memory, and judging whether writing the content is permitted; and a writing step of putting the bound content into an unbound state and writing the content in the unbound state onto a storage medium when the judging step has judged that writing is permitted.

According to an eleventh aspect of the present invention, there is provided a content using program for a content using system that includes a content importing apparatus and at least one content using apparatus that share a network key, where a content is bound to the network by encrypting content key information, which includes a content key required to decrypt the content, using a network key, the content using program including a first program that is executed by the content importing apparatus and a second program that is executed by a content using apparatus, the first program having a computer function as: an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside; an ID generating unit operable to generate a content ID for identifying the content obtained by the obtaining unit; and an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key, and the second program having a computer function as: a first decrypting unit operable to decrypt the re-encrypted content key information using the network key; a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit; a writing unit operable to write the

content decrypted by the second decrypting unit on a storage medium; a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing by the writing unit when the number of times has reached a predetermined maximum number of times.

According to a twelfth aspect of the present invention, there is provided a content using program executed by an apparatus that uses a content that has been bound to a network by encrypting content key information, which includes a content key that is required to decrypt the content, using a network key, the program having a computer function as: a first decrypting unit operable to decrypt the encrypted content key information using the network key; a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit; a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium; a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing by the writing unit when the number of times has reached a predetermined maximum number of times.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows the overall construction of a content using system according to the embodiments of the present invention.

FIG. 2 shows the overall construction of a content using system according to the embodiments of the present invention.

FIG. 3 is a functional block diagram showing the constructions of a content importing apparatus and a content using apparatus according to the first embodiment.

FIG. 4 shows the composition of the ECM section and the ECM according to the first embodiment.

FIG. 5 shows the composition of the moved content list according to the first embodiment.

FIG. 6 is a flowchart showing the content importing process of the content importing apparatus according to the first embodiment.

FIG. 7 is a flowchart showing the content writing process of the content using apparatus according to the first embodiment.

FIG. 8 is a flowchart showing the content reproducing process of the content using apparatus according to the first embodiment.

FIG. 9 is a flowchart showing the generation of scramble IDs and the recording process in the content writing process of the content using apparatus according to the first embodiment.

FIG. 10 is a flowchart showing the write resume process of the content using apparatus according to the first embodiment.

FIG. 11 is a functional block diagram showing the constructions of the content importing apparatus and the content using apparatus according to the second embodiment.

FIG. 12 is a flowchart showing the moved content list synchronization process performed between the content using apparatuses according to the second embodiment.

FIG. 13 shows the composition of the moved content list of a

first content using apparatus according to the second embodiment.

FIG. 14 shows the composition of the moved content list of a second content using apparatus according to the second embodiment.

FIG. 15 shows the write synchronization information according to the second embodiment.

FIG. 16 is a functional block diagram showing the constructions of the content importing apparatus and the content using apparatus according to the third embodiment.

FIG. 17 shows the compositions of the PMT and of the content_id_descriptor in which the content ID is written according to the third embodiment.

FIG. 18 is a flowchart showing the content importing process of the content importing apparatus according to the third embodiment.

FIG. 19 shows the composition of the moved content list according to the third embodiment.

FIG. 20 is a flowchart showing the content writing process of the content using apparatus according to the third embodiment.

FIG. 21 is a functional block diagram showing the constructions of the content importing apparatus and the content using apparatus according to the third embodiment.

FIG. 22 is a flowchart showing the content writing process of the content using apparatus according to the fourth embodiment.

FIG. 23 is a flowchart showing the moved content list synchronization process performed between the content importing apparatus and the content using apparatus according to the fourth embodiment.

FIG. 24 is a functional block diagram showing the constructions of the content importing apparatus and the content using apparatus according to the fifth embodiment.

FIG. 25 is a flowchart showing the content importing process

of the content importing apparatus according to the fifth embodiment.

FIG. 26 is a flowchart showing the content writing process of the content using apparatus according to the fifth embodiment.

FIG. 27 is a functional block diagram showing the constructions of the content importing apparatus, the content using apparatus, and the recording apparatus according to the sixth embodiment.

FIG. 28 is a flowchart showing the content write process of the content using apparatus and the recording apparatus according to the sixth embodiment.

BEST MODE FOR CARRYING OUT THE PRESENT INVENTION

First Embodiment

The following describes a first embodiment of the present invention in detail with reference to the attached drawings.

FIG. 1 shows the overall construction of a content using system 1 according to the first embodiment of the present invention.

In this content using system, contents that are distributed via a digital broadcast are used by appliances that are connected to a network. This content using system 1 is composed of a content importing apparatus 100 that imports contents, a storage apparatus 90, a plurality of content using apparatuses 110-1, 110-2, 110-3, etc., that use contents, and a network 120 that connects these appliances.

The content importing apparatus 100 imports a content from a broadcast wave and binds the content to the network 120 by decrypting encrypted content key information that includes at least an encryption key for the content (hereinafter called the "content key") and re-encrypting the content key information using an encryption key (hereinafter called the "network key") that has been shared in advance on the network 120. This is to say, the content

importing apparatus 100 "converts the encryption of" the content key information.

As one example, as shown in FIG. 2, the content importing apparatus 100 is an STB (Set Top Box) for receiving digital broadcasts and performs a process that (i) receives a content subject to access control according to CAS (Conditional Access System) and an encrypted ECM (Entitlement Control Message) that includes the content key as access key information, (ii) reconstructs the ECM section, (iii) decrypts the encrypted ECM, (iv) re-encrypts the ECM using the network key, and (v) outputs the content and the re-encrypted ECM to the network 120. It should be noted that, ECM is realized using a "private" section defined according to the MPEG-2 Systems, and has a construction like that shown in FIG. 4. It should be noted that MPEG-2 Systems is defined according to the international standard ISO/IEC 13818-1.

The ECM section shown in FIG. 4 is constructed so as to include a section header, an ECM payload, and a section tailer (for error correction). As one example of the content of the ECM payload, the ECM section shown in this drawing has a version number, copy control information, a content key, variable-length private data, and tampering detection data. The version number shows the ECM version. The copy control information shows whether copying is permitted ("COPY FREE", "NETWORK COPY", "COPY NEVER" etc.) for the content. The content key is also called the scrambling key, and is used for encrypting and decrypting the content. The private data includes any freely-chosen data that is of variable length. The tampering detection data is set for detecting any tampering with the ECM. It should be noted that the encrypted part of the ECM is the entire ECM payload, which is encrypted using a work key or the like that is distributed via an EMM (Entitlement Management Message).

The copy control information described above is set by the

copyright holder or the content provider/service provider, etc. Here "COPY NEVER" means that copying is not permitted and that the content can only be reproduced, with the content not being bound to the network. "NETWORK COPY" means that copies can be freely made only within a private network, with the content being bound to the network. "COPY FREE" means that copies can be freely made, with it being possible to bind the content to the network, although this is not necessary.

In the present embodiment, the content provider/service provider can set the maximum number of writes(copies), the write(output) destination, and the write(output) path, etc., in the private data described above. Such information is used as conditions for controlling the writing and reproduction/displaying of contents that have been bound to the network.

The storage apparatus 90 stores the content that has been imported by the content importing apparatus 100 and the content key information whose encryption has been converted. That is, the storage apparatus 90 stores the content in a state where the content is bound to the network.

As one example, the storage apparatus 90 is the home server shown in FIG. 2, includes a hard disk drive, and can be accessed by appliances on the network.

The content using apparatuses 110-1, 110-2, 110-3, etc., obtain the content and the content key information whose encryption has been converted from the content importing apparatus 100 or the storage apparatus 90, decrypt the encrypted content key using the network key that has already been obtained to extract the content key, decrypt the content using the content key, and then use the content. Also, in the present content using system 1, the plurality of content using apparatuses 110-1, 110-2, 110-3, etc., can connect to the network 120.

As one example, as shown in FIG. 2, the content using

apparatuses 110-1, 110-2, 110-3, etc., may be appliances such as a digital TV 110-1, a D-VHS 110-2, a DVD recorder 110-3, and a PC 110-4, etc., that display a content and store the content onto a removable medium such as a D-VHS tape, a DVD-RAM, and an SD memory card. Alternatively, the content using apparatuses 110 may be appliances that combine any of these functions.

The network 120 is a network that connects the content importing apparatus 100 and the content using apparatuses 110-1, 110-2, 110-3, etc. to one another, and is realized for example by an IEEE 1394 bus, IEEE 802.3 (10/100 Base-T), or Bluetooth.

FIG. 3 is a functional block diagram showing the constructions of the content importing apparatus 100 and a content using apparatus 110 shown in FIG. 1. This content using system is constructed so that contents that have been bound to the network can be identified individually and limitations are imposed on the writing of contents in a state where the contents are not bound to the network. It should be noted that in FIG. 3, the single content using apparatus 110 is used to represent the content using apparatuses 110-1, 110-2, 110-3, etc. that have the same construction. The storage apparatus 90 and the network 120 are also shown in FIG. 3.

The content importing apparatus 100 includes an input unit 101, a separating unit 102, a content key information encryption conversion unit 103, a content ID generating unit 104, and a multiplexing unit 105.

The input unit 101 imports an MPEG-2 transport stream ("TS") of a digital broadcast as an input stream. The transport stream is constructed by packet-multiplexing a content, an ECM, an EMM, PSI (Program Specific Information), etc. and can be identified by the PIDs (Packet IDs) of the header parts of the transport stream packets (TS packets).

The separating unit 102 separates the transport stream

imported by the input unit 101 into the content, the ECM, etc.

More specifically, the separating unit 102 refers to PSI called a PMT (Program Map Table) and obtains the elementary PIDs that compose the stream. After this, the separating unit 102 executes a process that refers to the PIDs in the header parts of the TS packets and separates the packets of the content and the ECM, etc.

The content key information encryption conversion unit 103 reconstructs the ECM section from the ECM packets received from the separating unit 102, extracts the ECM, and converts the encryption of the ECM. That is, the content key information encryption conversion unit 103 decrypts the encrypted ECM and uses the network key described above to re-encrypt the decrypted ECM.

More specifically, the ECM is distributed in a state where the ECM has been encrypted using the work key of the CAS and then multiplexed in the broadcast wave. The content key information encryption conversion unit 103 decrypts the encrypted ECM using the work key of the CAS, requests the content ID generating unit 104 to issue a content ID, inserts the content ID, which has been generated by the content ID generating unit 104 in accordance with this request, into the decrypted ECM, and then re-encrypts the ECM using the network key. It should be noted that the work key is usually distributed via an EMM that is multiplexed into the broadcast wave before the distribution of a content, so that the content key information encryption conversion unit 103 can obtain the work key in advance.

In this way, by inserting the content ID into an ECM that includes the content key which is the encryption key for a content, the content and the content ID can be securely bound. Here, the units for the assigning of content IDs may be events that are identified by the separating unit 102. Here, an "event" is a content that corresponds to one broadcast program. In this case, the

content key information encryption conversion unit 103 identifies an event by obtaining event information such as an event_id from an EIT (Event Information Table) in the SI (Service Information) in a TS, and requests the generation of content IDs in such event units.

Based on the request from the content key information encryption conversion unit 103, the content ID generating unit 104 issues a unique content ID. More specifically, the content ID generating unit 104 has an internal counter and on receiving a request for the issuing of a content ID from the content key information encryption conversion unit 103, performs a process that assigns the present counter value as a content ID and increments the counter.

The multiplexing unit 105 performs a process that multiplexes the content received from the separating unit 102 and the encrypted ECM received from the content key information encryption conversion unit 103 to reconstruct a transport stream.

The storage apparatus 90 stores the transport stream outputted from the multiplexing unit 105.

On the other hand, the content using apparatus 110 includes a separating unit 111, a content key information decrypting unit 112, a moved content list managing unit 113, a moved content list storing unit 114, a content output control unit 115, a content decrypting unit 116, a content output selecting unit 117, and a content display unit 118 and a content writing unit 119 as content outputting units.

The separating unit 111 operates as follows. When a content display request or a content writing request has been received in the content using apparatus 110 from the user, the separating unit 111 separates the content and the re-encrypted ECM from a transport stream obtained from the content importing apparatus 100 or the storage apparatus 90.

The content key information decrypting unit 112 receives the re-encrypted ECM from the separating unit 111 and decrypts the

re-encrypted ECM using the network key. When doing so, if the user has made a content writing request, the content key information decrypting unit 112 transfers the decrypted content key to the content decrypting unit 116 only when it has been judged by the moved content list managing unit 113 that the write is permitted. More specifically, the content key information decrypting unit 112 decrypts the re-encrypted ECM using the network key and transfers the content ID included in the ECM to the moved content list managing unit 113. The content key information decrypting unit 112 then receives a judgement result from the moved content list managing unit 113 showing whether the writing of the content with that content ID is permitted or prohibited, and when the judgement result is "permitted", transfers the decrypted content key to the content decrypting unit 116. In this way, the moved content list managing unit 113 judges whether writing is permitted or prohibited for individual contents, so that it is not possible to unlimitedly output contents in an unbound state to the outside.

When a content display request has been received from the user, the processing of the content key information decrypting unit 112 is the same as when a content writing request has been received. However, the judgement result received from the moved content list managing unit 113 is a judgement result regarding the reproduction/display of the content and not a judgement result regarding whether writing is permitted or prohibited.

The moved content list managing unit 113 performs a judgement as to whether the outputting of a content is permitted or prohibited based on a moved content list (hereinafter "MCL") that is stored in the moved content list storing unit 114 and updates the MCL. Here, the MCL is a list that includes at least the content IDs of contents that have already been written. The judgements as to whether the outputting of contents is permitted include judgements as to whether the writing of a content is permitted and judgements

as to whether the reproduction/display of a content is permitted.

More specifically, when a content ID has been received from the data I/O control circuit 12, the moved content list managing unit 113 judges whether the writing of a content is permitted according to processes such as (A) and (B) below.

(A) The moved content list managing unit 113 judges whether the received content ID is already registered in the MCL and when the content ID has not been registered, adds the content ID to the MCL and permits the writing. When the content has already been registered, the moved content list managing unit 113 prohibits the writing. In this case, it is possible to permit the writing of the content only once, with the second and subsequent writings of the content being prohibited. In this case, the MCL is a content ID list of contents that have already been written once. The non-registration of a content ID in the MCL is the condition (writing condition) for writing a content.

(B) The moved content list managing unit 113 judges that the received content ID has already been registered in the MCL. When the content ID has not been registered, the moved content list managing unit 113 registers the content ID in the MCL, and judges whether the writing of the content is permitted or prohibited in accordance with a predetermined writing condition or the MCL. When the content ID has been registered, the moved content list managing unit 113 judges whether the writing of the content is permitted or prohibited in accordance with the writing condition corresponding to the content ID. Here, the writing conditions may be a permitted number of writes for a content, a write destination (the kind of storage medium for the write), a writing path (analog output/digital output, etc.) and the like. In this case, the writing of each content is limited in accordance with the writing conditions for

each content. The number of permitted writes for a content may be the number of content using apparatuses 110 that share the network key in the network 120, for example.

The moved content list managing unit 113 judges whether the reproduction/display of a content is permitted or prohibited in the same way as the processes (A) and (B) above, though such judgements are made according to content reproduction/display conditions, not content writing conditions.

The moved content list managing unit 113 also securely manages a hash value of the MCL stored in the moved content list storing unit 114. This is used to detect whether or not the MCL has been tampered with and so ensures the authenticity of the MCL in a case where the MCL is stored in a non-secure region of a hard disk drive or the like. Accordingly, whenever the content of the MCL is updated, the moved content list managing unit 113 calculates the hash value for the MCL and manages the calculation result. As one example of a method for securely managing the hash value, the hash value may be stored inside a security module, which is tamper-resistant hardware.

In addition, the moved content list managing unit 113 manages the maximum size of the MCL and/or a threshold relating to the number of content IDs or the size of the MCL. Here, in a case where a threshold for the maximum number of content IDs or a maximum number of bytes that can be written in the MCL is provided and this threshold for the MCL is reached, control is performed to delete the information for the oldest content IDs in the MCL. More specifically, the moved content list managing unit 113 manages a pointer that shows the next writing position for the MCL and when an upper limit for the MCL is reached, the pointer is returned to the start of the MCL, so that it is possible to delete information starting from the oldest content ID.

Alternatively, by writing the time and date when a content

was accessed as the information for each content in the MCL, deletion (overwriting) can be performed starting from the information with the lowest access frequency.

Alternatively, instead of automatically deleting information as described above, the information to be deleted from the MCL may be selected by the user and then deleted by a user operation.

The moved content list storing unit 114 stores the MCL and is realized by a hard disk drive or the like.

The content output control unit 115 outputs content output control information for controlling the outputting of a content to the content output selecting unit 117. More specifically, based on a content display request or a content write request from the user, the content output control unit 115 generates content output control information indicating an outputting of the content to the content display unit 118 or an outputting of the content to the content writing unit 119 and transmits the content output control information to the content output selecting unit 117.

The content decrypting unit 116 decrypts the encrypted content. More specifically, the content decrypting unit 116 performs a process that uses the content key obtained from the content key information decrypting unit 112 to successively decrypt TS packets of the content that have been encrypted using the content key.

The content output selecting unit 117 controls the transfer destination of the content based on the content output control information obtained from the content output control unit 115. More specifically, the content output selecting unit 117 performs a process that transmits, when the content output control information shows "display", the content to the content display unit 118 and transmits, when the content output control information shows a write to a storage medium, the content to the content writing unit 119.

The content display unit 118 reconstructs an MPEG-2 elementary stream from the TS packets of the content, decodes the MPEG-2 elementary stream, and outputs the content to a monitor.

The content writing unit 119 performs the processing required to write the content and a process that writes the content onto a storage medium. More specifically, the content writing unit 119 performs a process that converts the encryption of the content to bind the content to the medium and converts the format, etc.

FIG. 5 shows one example of the data construction of the MCL that is stored by the moved content list storing unit 114 and is managed by the moved content list managing unit 113. This MCL is a list in which contents that have been written by the content writing unit 119 and contents subjected to reproduction/display by the content display unit 118 are written. As shown in the drawing, the MCL includes a number of writes, write destinations, and a write path corresponding to each content ID. The number of writes shows the number of times writing on a storage medium has been performed for each content by the content writing unit 119. The write destination shows the storage medium, such as a DVD-RAM, D-VHS, and an SD card, for which writing is permitted. The write path shows the output state, such as analog output, digital output (compressed/uncompressed), and output image quality (SD(Standard Definition)/HD(High Definition)). The moved content list managing unit 113 may obtain information such as the write destinations and write paths from the private data in the ECM shown in FIG. 4 and set the information in the MCL or may obtain such information from information (such as the content, ECM, and PSI/SI) included in a broadcast wave and set the obtained information in the MCL, or may even set values that are stored in advance in the present content using system.

From an MCL with the above construction, it is possible to know the number of times a content has already been written, so

that the moved content list managing unit 113 can limit the writing of a content within a range stipulated by a maximum number of writes for each single content.

The operation of the content using system 1 with the construction described above is explained below using the flowcharts shown in FIGS. 6 and 7.

FIG. 6 is a flowchart showing the content importing process of the content importing apparatus 100.

The input unit 101 receives a transport stream from a broadcast wave (step S401).

The separating unit 102 obtains the transport stream from the input unit 101, refers to the PIDs of the TS packets, and separates the TS packets of a content and the TS packets of an ECM and the like (step S402). The PIDs showing the TS packets of the content and the ECM are written in the PMT, so that by referring to the PMT, the separating unit 102 separates these TS packets.

The content key information encryption conversion unit 103 obtains the TS packets of the ECM, reconstructs the ECM section, and decrypts the encrypted ECM using the work key (step S403). In addition, when the copy control information of the decrypted ECM is "COPY NEVER", the content key information encryption conversion unit 103 does not bind the content to the network and so does not perform the processing below (though reproduction/display of the content is permitted). When the copy control information is "NETWORK COPY", the content key information encryption conversion unit 103 performs the processing described below. When the copy control information is "COPY FREE", it may not be necessary to bind the content to the network, though the content key information encryption conversion unit 103 may bind the content to the network with the number of writes set at "unlimited".

The content key information encryption conversion unit 103 sends a content ID generation request to the content ID generating

unit 104. The content ID generating unit 104 receives this request and generates a content ID (step S404).

The content ID generating unit 104 sends the generated content ID to the content key information encryption conversion unit 103. The content key information encryption conversion unit 103 embeds the obtained content ID in the ECM (step S405). More specifically, the content ID generating unit 104 generates a content ID using the counter that is stored internally and transmits this content ID to the content key information encryption conversion unit 103. The content key information encryption conversion unit 103 sets the received content ID in a specified field in the ECM. As one example, a method where the content ID is inserted into the private data part of the ECM shown in FIG. 4 may be used.

The content key information encryption conversion unit 103 re-encrypts the ECM using the network key (step S406). More specifically, the content key information encryption conversion unit 103 internally stores an encryption key that has been shared in advance on the network and uses this encryption key to re-encrypt the ECM in which the content ID has been embedded. In addition, the content key information encryption conversion unit 103 converts the encrypted ECM into TS packets and transfers these TS packets to the multiplexing unit 105.

The multiplexing unit 105 multiplexes the TS packets of the content received from the separating unit 102 and the TS packets of the ECM, whose encryption has been converted, received from the content key information encryption conversion unit 103 (step S407).

After multiplexing, the content and ECM are stored in the storage apparatus 90. Alternatively, the content and ECM are inputted into the content using apparatus 110 at the same time as the content and ECM are stored in the storage apparatus 90.

In this way, in the content importing apparatus 100, the

encryption of the ECM is converted, thereby generating a content that has been bound to the network, and a content ID is set in the ECM which is multiplexed with the content.

On the other hand, FIG. 7 is a flowchart showing the content writing process of the content using apparatus 110.

In the separating unit 111, the content and the ECM are separated from either a transport stream received from the content importing apparatus 100 or a transport stream that has been read from the storage apparatus 90 (step S501). More specifically, the separating unit 111 performs a process that refers to the PIDs that are in the header parts of the TS packets in the transport stream and separates the TS packets corresponding to the respective PIDs.

The content key information decrypting unit 112 receives the TS packets of the ECM from the separating unit 111, reconstructs the ECM section, and obtains the re-encrypted ECM. The content key information decrypting unit 112 then decrypts the encrypted part of the ECM using the network key that is obtained in advance (step S502).

The content key information decrypting unit 112 reads the content ID that has been embedded in the decrypted ECM (step S503). In order to confirm whether writing is permitted for the present content, the content key information decrypting unit 112 transfers the read content ID to the moved content list managing unit 113.

The moved content list managing unit 113 reads the MCL from the moved content list storing unit 114 (step S504). The moved content list managing unit 113 first obtains conditions such as the write destination and the write path of the content from information (such as the content, the ECM and the PSI/SI) included in the transport stream or from parameters that are set in advance in the system and then confirms whether the write destination and the write path indicated by the user satisfy the conditions (step S505).

As one example, when the user indicates "D-VHS" as the write destination, and a write destination that is provided in advance in the content using apparatus 110 is "D-VHS", the content can be written to D-VHS, but when the write destination that is provided in advance in the content using apparatus 110 is "SD card", such writing to D-VHS is not possible. This is also the case for the write path, so that unless the write path indicated by the user satisfies the write path provided in advance in the content using apparatus 110, the content cannot be written onto a storage medium.

In addition, the moved content list managing unit 113 judges whether the content ID received from the content key information decrypting unit 112 is present in the MCL (step S506). It should be noted that when there is no MCL in the moved content list storing unit 114 (a pre-initialization state), an MCL is generated (initialization is performed).

When the judgement in step S506 is "NO", which is to say, when a content ID is not present in the MCL, the moved content list managing unit 113 performs a process that updates the MCL and stores the MCL in the moved content list storing unit 114 (step S507). In this case, it is judged that writing is permitted for the present content.

In order to record the writing of the content, the moved content list managing unit 113 adds the content ID, the number of writes, the write destination, and the write path to the MCL, recalculates the hash of the MCL, and stores the MCL in the moved content list storing unit 114, in addition to replacing the hash value stored in the moved content list managing unit 113 with the recalculated hash value for the MCL.

The content key information decrypting unit 112 extracts the content key from the ECM and transfers the content key to the content decrypting unit 116, and also instructs the content output control unit 115 to transfer the content to the content writing unit

119 via the confirmed write destination and write path (step S508). Accordingly, the content output control unit 115 controls the content output selecting unit 117 to write the content on the indicated write destination and write path.

The content decrypting unit 116 decrypts (descrambles) the TS packets obtained from the separating unit 111 using the content key obtained from the content key information decrypting unit 112 (step S509).

The content output selecting unit 117 transfers, according to control by the content output control unit 115, the content to the content writing unit 119 using the indicated write destination and write path.

The content writing unit 119 writes the content onto a storage medium (step S510). More specifically, the content writing unit 119 encrypts the content in a suitable manner, changes the format, etc., in accordance with the storage medium, such as a DVD-RAM or D-VHS, and then writes the content onto the storage medium.

When the judgement in step S506 is "YES", which is to say, when the content ID is present in the MCL, the moved content list managing unit 113 judges whether writing is permitted or prohibited using the information in the MCL that is related to this content ID (step S511). More specifically, since a number of writes, a write destination, a write path, etc., are recorded in the MCL for each content ID, the moved content list managing unit 113 refers to this information and confirms whether writing is permitted.

As one example, when the permitted number of writes for each content is "3", if the content ID of the content to be written is "CONTENT-ID-11111" in FIG. 5, the number of writes is "1", meaning that two more writes are possible, so that the moved content list managing unit 113 judges that the write is possible. When doing so, the content of the MCL relating to the write destination and the write path is "-", which is to say, that there are

no limitations over the write destination and the write path, so that writing can be performed for the write destination and the write path indicated by the user. When the content ID is "CONTENT-ID-22222" and the write destination indicated by the user is "DVD-RAM", in the MCL the number of writes is "2" and the write destination is "DVD-RAM", so that the moved content list managing unit 113 judges that the write is permitted. If, at this point, the write destination indicated by the user is "SD CARD" for example, even though the maximum number of writes has not been reached, the limitation over the write destination is not satisfied, so the moved content list managing unit 113 judges that the write is not permitted. In the same way, when the content ID is "CONTENT-ID-88888" and the write path indicated by the user is "Digital (SD)", the limitations on the number of writes and the write path are both satisfied, so that the moved content list managing unit 113 judges that the write is permitted, but when the write path indicated by the user is "Digital (HD)", the limitation on the write path is not satisfied, so that the moved content list managing unit 113 judges that the write is not permitted. In addition when the content ID is "CONTENT-ID-77777", the number of writes has already reached "3", so that the moved content list managing unit 113 judges that the write is not permitted.

When the judgement in step S511 is "YES", which is to say, the moved content list managing unit 113 has judged that the write is permitted, the moved content list managing unit 113 updates and stores the MCL (step S507). The detailed processing from step S507 onwards is as was described above, so that description of such has been omitted.

When the judgement in step S511 is "NO", which is to say, the moved content list managing unit 113 has judged that the write is prohibited, the content writing process is terminated.

In this way, in the content using system 1, when a content ID

is assigned to a content that has been bound to the network and the content is written, the writing is confirmed using the MCL so that it is possible to impose limitations on the writing of contents.

Also, while FIG. 7 is a flowchart showing the content writing process in the content using apparatus 110, FIG. 8 is a flowchart showing the content reproduction (display) process.

In FIG. 8, the processing in steps S601 to S606 are the same as in the content writing process shown in FIG. 7, so that description of such has been omitted.

When the judgement of the moved content list managing unit 113 in step S606 is "NO", which is to say, when the present content ID is not present in the MCL, the present content has not been written, so that the moved content list managing unit 113 judges that the reproduction process is permitted, so that the content key information decrypting unit 112 performs a process that extracts the content key from the ECM and transfers the content key to the content decrypting unit 116 (step S608).

The content decrypting unit 116 decrypts (descrambles) the TS packets obtained from the separating unit 111 using the content key obtained from the content key information decrypting unit 112 (step S609).

The content output selecting unit 117 transfers the content to the content display unit 118 for displaying the content, based on control by the content output control unit 115.

The content display unit 118 outputs the content to a TV set or the like (step S610).

When the judgement of the moved content list managing unit 113 in step S606 is "YES", which is to say, the present content ID is present in the MCL, the moved content list managing unit 113 confirms whether reproduction is permitted or prohibited using the information in the MCL relating to the present content ID (step S607). More specifically, the moved content list managing unit 113

confirms whether the number of writes has reached the maximum number of writes, and judges that reproduction is permitted when the maximum number of writes has not been reached and that reproduction is prohibited when the maximum number of writes has been reached.

When the judgement in step S607 is "YES", which is to say, when reproduction is permitted, the processing in steps S608 onwards is executed.

When the judgement in step S607 is "NO", which is to say, when reproduction is prohibited, the content reproduction process is terminated.

In this way, in the present content using system 1, even for a content that has been written on a storage medium, there is the possibility that a copy of the content is present on the network, so that during the display (reproduction) process for a written content also, the MCL is used to confirm whether reproduction of the content is permitted, thereby imposing limitations on the usage of the content.

However, there can be cases where the writing process is interrupted (fails) due to the power being cut off or the user canceling the process, for example. For this reason, the present content using system 1 is designed so as to be able to resume the writing process. More specifically, in FIG. 3, the content key information decrypting unit 112 assigns IDs (hereinafter referred to as "scramble IDs") in scramble units (for example, the units in which the content key included in the ECM is updated), with the content decrypting unit 116 receiving the content key and this scramble ID and storing up to what point the content has been transferred to the content writing unit 119, which is to say, up to what point the writing of the content onto a storage medium has succeeded. When the process is cancelled, and the writing process is resumed, the content decrypting unit 116 transfers the stored scramble ID to the content

key information decrypting unit 112 so that the processing can be resumed from the scramble ID.

This process is described below using the flowcharts shown in FIGS. 9 and 10.

FIG. 9 is a flowchart showing the process for writing a content onto a storage medium. This drawing shows the processing from the start of a write up to an interruption (a "cancel" or a "pause") and then up to the end.

Once the writing process for a content is commenced, the moved content list managing unit 113 provisionally registers the content ID of the content being written (step S701).

The content key information decrypting unit 112 checks whether a writing process interruption (cancel) cause has occurred (step S702). When the process has not been interrupted, the content key information decrypting unit 112 executes step S703, while when the process has been interrupted, the content writing process is terminated. When the power is cut off, the processing obviously ends.

In step S703, it is judged whether the content has been outputted in an entire scramble unit. When the content has not been outputted in an entire scramble unit, step S704 is executed, while when the content has been outputted in an entire scramble unit, step S709 is executed.

The content key information decrypting unit 112 assigns a scramble ID to each scramble unit (step S704). More specifically, by uniformly assigning IDs to each scramble unit, the content decrypting unit 116 and/or the content writing unit 119 can use these IDs to recognize how far the writing has progressed. The last scramble ID to be assigned is stored inside the content key information decrypting unit 112 as the last transmitted scramble ID.

The content key information decrypting unit 112 reads the content key from the ECM and transfers the content key and

scramble ID to the content decrypting unit 116 (step S705). Here, in consideration of a case where the writing processes for a plurality of contents are interrupted, the content ID of the content to be written may be transferred together with the scramble ID.

The content decrypting unit 116 receives the content key and the scramble ID (step S706).

The content decrypting unit 116 decrypts the encrypted content using the content key and internally stores the scramble ID of a scramble unit for which writing has been completed (step S707).

The content writing unit 119 writes the content (step S708).

When it has been judged in step S703 that an entire scramble unit has been outputted, the moved content list managing unit 113 properly registers the content ID of the content being written in the MCL (step S709).

It should be noted that while the scramble ID is described as being internally stored when the content that has been encrypted is decrypted by the content decrypting unit 116, the scramble ID may be internally stored when notification that the content has been written and is successfully stored in the storage medium is received from the content writing unit 119.

FIG. 10 shows the processing that restarts (resumes) the process after the process has been interrupted.

The processing in FIG. 10 commences when a content ID that has been provisionally registered in the MCL is discovered, when a resume request is received from the user, etc.

In this drawing, the content decrypting unit 116 transmits the stored scramble ID to the content key information decrypting unit 112 (step S801).

The content key information decrypting unit 112 receives the scramble ID (step S802).

The content key information decrypting unit 112 compares

the last transmitted scramble ID that is stored with the scramble ID received from the content decrypting unit 116 (step S803). More specifically, the content key information decrypting unit 112 finds the difference between the scramble ID received from the content decrypting unit 116 and the last transmitted scramble ID, and by judging that the difference is equal to or below a threshold value set in advance, prevents illegal writes from being performed.

When the judgement in step S803 is "YES", which is to say, the difference is equal to or below the threshold value, the resumption of the writing process is permitted and the content writing process is resumed (step S804). It should be noted that the operation following the resumption of the content writing_process was described with reference to FIG. 9, and so description of such is omitted here.

When the judgement in step S803 is "NO", which is to say, the difference is above the threshold value, the content writing process is cancelled (step S805).

In this way, in the present content using system 1, when a content is written, scramble IDs are assigned to indicate the progress of the write, so that if the power is cut off during a write or the user interrupts the write, the write can be safely resumed without the security being compromised.

Second Embodiment

The following describes a second embodiment of the present invention, with reference to the attached drawings.

FIG. 11 is a block diagram showing the construction of a content using system 2 according to the second embodiment of the present invention. It should be noted that in FIG. 11, construction elements that are the same as in the content using system 1 of the first embodiment shown in FIG. 3 have already been described with reference to FIG. 3, so that such construction elements have been

given the same reference numerals as in FIG. 3 and description of such has been omitted.

The content using system 2 shown in FIG. 11 is characterized as follows. While the content importing apparatus 100 has the same construction as in the content using system 1 of the first embodiment of the present invention, each content using apparatus 110a further comprises a moved content list synchronizing unit 901 and communicates with other content using apparatuses 110a that are connected to the network so that the MCL is synchronized between a plurality of content using apparatuses 110a.

The moved content list synchronizing unit 901 synchronizes the MCL by transmitting and receiving synchronization information for the MCL to and from other content using apparatuses 110a and notifies the moved content list managing unit 113 of the result. More specifically, at the timing when a content is written and the MCL is updated, the moved content list managing unit 113 transfers synchronization information for the updated content ID to the moved content list synchronizing unit 901. The moved content list synchronizing unit 901 transmits this synchronization information to the other content using apparatuses 110a connected to the network. The moved content list synchronizing unit 901 of each of the other content using apparatuses 110a that receive this synchronization information transfers the synchronization information to the moved content list managing unit 113 and by reflecting this information in the MCL in the moved content list storing unit 114, the synchronization of the MCLs in different content using apparatuses 110a is ensured. As one example, the synchronizing information (synchronization information) is information that has been recorded in the MCL and includes the content ID of the content that has been written. As one example of the synchronization method, synchronization information may be broadcast on the network.

FIG. 12 shows a sequence when the moved content list

synchronizing unit 901 synchronizes the MCL with the moved content list synchronizing units 901 of other content using apparatuses 110a connected to the network. In this drawing, the updating source of the MCL (the content using apparatus 110a that updates the MCL and broadcasts the synchronization information) is set as the first content using apparatus 110α while the updating destination (the content using apparatus 110a that receives the broadcast synchronization information and updates the MCL) is set as a second content using apparatus 110β. It should be noted that there may be a plurality of content using apparatuses 110a that correspond to the updating destination for the MCL, with the second content using apparatus 110β being used to represent these content using apparatuses 110a in the following explanation.

When writing a content, the moved content list managing unit 113 of the first content using apparatus 110α obtains the content ID from the content key information decrypting unit 112 and updates the MCL read from the moved content list storing unit 114 (step S1001). More specifically, when the content with the content ID "CONTENT-ID-12345" is written, as shown in FIG. 13, information (Content ID, number of writes, etc.) relating to the content ID "CONTENT-ID-12345" is added to the MCL stored in the first content using apparatus 110α. At this point, as shown in FIG. 14, the MCL stored in the second content using apparatus 110β has not been notified of the writing of the content with the content ID "CONTENT-ID-12345" by the first content using apparatus 110α, so that there is no record for "CONTENT-ID-12345" in this MCL.

It should be noted that in the MCL shown in FIG. 13, the number of writes that have been performed (the number of writes) and the maximum number of writes that are permitted (maximum number of writes) are recorded as the information relating to the number of writes of a content. Accordingly, when the reproduction of a content is controlled, the reproduction of the content is

permitted so long as the number of writes is yet to reach the maximum number of writes, though once the maximum number of writes has been reached, control is performed so as to prohibit the reproduction of the content. The number of writes is recorded as the number of writes that have been performed, but it is possible to alternatively record the remaining number of permitted writes, with this number being decreased every time a write is performed. In this case, the writing and reproduction of a content become prohibited when the number of writes reaches zero.

The moved content list managing unit 113 of the first content using apparatus 110α notifies the moved content list synchronizing unit 901 of information relating to the updated content ID (step S1002). More specifically, the moved content list managing unit 113 of the first content using apparatus 110α notifies the moved content list synchronizing unit 901 of the entire record with the content ID "CONTENT-ID-12345" in the MCL of the first content using apparatus 110α shown in FIG. 13.

The moved content list synchronizing unit 901 of the first content using apparatus 110α generates the synchronization information from the information relating to the content ID "CONTENT-ID-12345" received from the moved content list managing unit 113 (step S1003). The synchronization information 1301 shown in FIG. 15 is one example of this synchronization information. The synchronization information 1301 is composed of the information described below.

The session ID (SESSION-ID) is set for each content using apparatus 110a every time the synchronization information is generated. More specifically, the session ID is an ID which is realized by a counter to which "1" is added every time synchronization information is generated.

The content using apparatus ID (TERMINAL-ID) is internally stored in the content using apparatus 110a and is an ID for

identifying the content using apparatus 110a. As one example, when two content using apparatuses 110a simultaneously write a content with the same content ID and synchronization information is broadcast by both content using apparatuses 110a, these content using apparatus IDs are used as information for distinguishing between the two content using apparatuses 110a.

The content ID (CONTENT-ID) is the content ID of the content that has been written.

The number of writes, the write destination and write path are all fundamentally the same as in the information in the MCL. It should be noted that the MCL itself may be used as the synchronization information, though the synchronization information 1301 shown in FIG. 15 is used as the synchronization information in the explanation below.

Next, the moved content list synchronizing unit 901 of the first content using apparatus 110α transmits the generated synchronization information 1301 (step S1004). More specifically, the moved content list synchronizing unit 901 of the first content using apparatus 110α broadcasts the synchronization information 1301 on the network.

The moved content list synchronizing unit 901 of the second content using apparatus 110β receives the broadcast synchronization information 1301 and requests the moved content list managing unit 113 to read the MCL (step S1005).

The MCL is read from the moved content list storing unit 114 and the moved content list managing unit 113 of the second content using apparatus 110β calculates the hash of the MCL, compares the calculated value with the value stored by the moved content list managing unit 113 to confirm the authenticity of the MCL, and transfers the content of the MCL to the moved content list synchronizing unit 901 (step S1006). It should be noted that when an MCL is not present in the moved content list storing unit 114, the

moved content list managing unit 113 generates (initializes) the MCL.

The moved content list synchronizing unit 901 of the second content using apparatus 110β confirms the session ID and the content using apparatus ID, etc., compares the content of the MCL received from the moved content list managing unit 113 with the synchronization information 1301, and judges whether the synchronization information 1301 should be reflected in the MCL (step S1007). More specifically, the moved content list synchronizing unit 901 judges whether the content of the synchronization information 1301 is not included in the content of the MCL or whether the content of the MCL has not been updated.

When the judgement in step S1007 is "YES", which is to say, when the moved content list synchronizing unit 901 judges that it is necessary to update the MCL, the moved content list synchronizing unit 901 notifies the moved content list managing unit 113 of the content of the synchronization information 1301 and the moved content list managing unit 113 updates the MCL using the content of the synchronization information 1301 (step S1008). More specifically, the content of the MCL stored by the second content using apparatus 110β shown in FIG. 14 is synchronized so as to match the content of the MCL stored by the first content using apparatus 110α shown in FIG. 13.

The moved content list managing unit 113 of the second content using apparatus 110β recalculates the hash of the MCL, internally stores the hash value, and writes the MCL into the moved content list storing unit 114 (step S1009).

When the judgement in step S1007 is "NO", which is to say, when the moved content list synchronizing unit 901 judges that it is not necessary to update the MCL, the present synchronization process is terminated. More specifically, it is possible for the synchronization information 1301 to the repeatedly broadcast a

plurality of times, so that a process is performed that refers to the session ID of the synchronization information 1301 and the content using apparatus ID of the synchronization information transmission source and discards unnecessary synchronization information 1301 when the same synchronization information 1301 has been received a plurality of times.

It should be noted that the content importing process of the content importing apparatus 100, the content writing process of the content using apparatus 110a, and the content reproduction process of the content using apparatus 110a are the same as in the first embodiment, and since these processes have already been described, description of such is omitted here.

In this way, with the present content using system 2, the MCL is synchronized between a plurality of content using apparatuses 110a on a network. This means that while in the content using system 1 shown in the first embodiment of the present invention, limitations such as the permitted number of content writes are imposed separately for content using apparatuses 110a, in the content using system 2, limitations can be imposed on the entire network, which is to say, on all of a plurality of content using apparatuses 110a.

Third Embodiment

The following describes a third embodiment of the present invention with reference to the attached drawings.

FIG. 16 is a block diagram showing the construction of a content using system 3 according to the third embodiment of the present invention. It should be noted that in FIG. 16 construction elements that are the same as in the content using system 1 of the first embodiment shown in FIG. 3 have already been described with reference to FIG. 3, so that such construction elements have been given the same reference numerals as in FIG. 3 and description of

such has been omitted.

Compared to the content using system 1 of the first embodiment of the present invention, the content using system 3 shown in FIG. 16 is characterized as follows. The content importing apparatus 100 further includes a moved content list managing unit 1401, a moved content list storing unit 1402 and a content ID receiving unit 1403, while a content using apparatus 110b includes the separating unit 111, the content key information decrypting unit 112, the content output control unit 115, the content decrypting unit 116, the content output selecting unit 117, the content display unit 118 and the content writing unit 119 as content output units, and a content ID transmitting unit 1404. The content importing apparatus 100 manages the MCL, so that when the content using apparatus 110b writes a content or displays (reproduces) a content, the content using apparatus 110b inquires to the content importing apparatus 100 whether the writing is permitted or prohibited and the writing and display of the content is controlled based on the result of a judgement by the content importing apparatus 100 as to whether the writing is permitted or prohibited.

All of the content IDs that have been assigned to contents that have been imported into the content using system 3 are registered in the MCL managed by the content using system 3, and in the MCL, only the content IDs of contents that have been written are marked. This means that the content ID generating unit 104 generates a content ID whenever a content is newly imported and that it is necessary to inform the moved content list managing unit 1401 of the new content ID.

The moved content list managing unit 1401 of the content importing apparatus 100 reads the MCL stored in the moved content list storing unit 1402, refers to the MCL, and performs an update process and the like. More specifically, the moved content list managing unit 1401 performs processing that receives a content ID

to be registered in the content ID generating unit 104 from the content ID generating unit 104 and registers the content ID in the MCL, etc. When the content ID of a content to be written is received from the content using apparatus 110b, the moved content list managing unit 1401 judges whether a write is permitted or prohibited, and updates the MCL. Also, when an MCL is not stored in the moved content list storing unit 1402, an MCL is newly generated and initialized. It should be noted that the methods for calculating the hash of the MCL and securely managing the hash value are the same as those described in the first embodiment of the present invention, so that description of such is omitted here.

The moved content list storing unit 1402 in the content importing apparatus 100 is the part that stores the MCL and is realized by a hard disk drive or the like.

The content ID receiving unit 1403 in the content importing apparatus 100 performs a process that receives the content ID of a content to be written or reproduced from the content ID transmitting unit 1404 of a content using apparatus 110b, transfers the content ID to the moved content list managing unit 1401, and transmits the judgement result, which shows that the writing is permitted or prohibited, received from the moved content list managing unit 1401 to the content ID transmitting unit 1404 of the content using apparatus 110b.

The content ID transmitting unit 1404 in the content using apparatus 110b performs a process that receives the content ID of the content to be written or reproduced from the content key information decrypting unit 112, transmits the content ID to the content ID receiving unit 1403 of the content importing apparatus 100, receives the judgement result, which shows that the writing is permitted or prohibited, and transfers the judgement result to the content key information decrypting unit 112.

The content using system 1 of the first embodiment of the

present invention and the content using system 2 of the second embodiment of the present invention are examples where the content ID is set in the ECM, though in this embodiment the content ID is set in information aside from the ECM (content key information). As examples of such information aside from the ECM, a method where the content ID is set in the PMT or a method where the content ID is set as a private section and the content is pointed to from the PMT by a PID may be used. As one example of setting the content ID in the PMT, FIG. 17 shows a case where a content_id_descriptor, which is defined so that a content ID can be set, is inserted in a first loop part of a descriptor part of the PMT. Any desired descriptor that can be defined on a system-by-system basis can be set in the descriptor part of the PMT, and a digital copy control descriptor in which information relating to digital copying is written and a CA descriptor or the like may be inserted in this PMT descriptor part. In the present content using system, a content_id_descriptor is newly defined in this descriptor part, and the content ID is set in a content_id field in this content_id_descriptor. The decision as to whether this descriptor is set in the first loop part or in the second loop part can be made freely in each system, but the descriptor is normally set in the first loop part when there are parameters for each program, and in the second loop part when there are parameters for each elementary stream. The following describes an example where the content ID is inserted in the PMT.

However, when the content ID is inserted somewhere aside from the ECM as described above, there is the risk of the content ID being illegally replaced or tampered with, so that it is necessary to securely bind the content and the content ID. This means that when the content key information encryption conversion unit 103 in the content importing apparatus 100 converts the encryption of the ECM, the conversion of the encryption is performed with the content

ID having been associated to the ECM so that the content and the content ID are securely bound. As specific examples, a method where the result of an XOR (Exclusive OR) taken for the network key and the content ID or the result of linking the network key and the content ID is used as the encryption key for re-encrypting the ECM, a method where a hash is calculated for the content ID using a hash algorithm, such as SHA-1, and the resulting hash value is inserted in the ECM, or a method where the ECM is encrypted using the content ID and then encrypted using the network key may be used. The following describes an example where an XOR is taken for the network key and the content ID and the result is used as an encryption key for re-encrypting the ECM.

The operation of the content using system 3 with the construction described above is described below with reference to FIGS. 18 and 20.

FIG. 18 is a flowchart showing the content importing process of the content importing apparatus 100.

The input unit 101 receives a transport stream from a broadcast wave (step S1501).

The separating unit 102 receives the transport stream from the input unit 101, refers to the PIDs of the TS packets, and separates the TS packets of the content and the TS packets of the ECM (step S1502). The PIDs showing the TS packets of the content and the ECM are written in the PMT, so that the separating unit 102 refers to the PMT when separating the TS packets. Also, in order to generate the content ID, the separating unit 102 separates the SI information. As one example, this information is an EIT (Event Information Table) in which event information is written and a TOT (Time Offset Table) in which the present time is written.

The content key information encryption conversion unit 103 receives the TS packets of the ECM, reconstructs the ECM section, and decrypts the encrypted ECM using the work key (step S1503).

The content key information encryption conversion unit 103 sends a content ID generation request and the data (information on the EIT, TOT, etc.) that has been distributed together with the content to the content ID generating unit 104, with the content ID generating unit 104 receiving this information and request and generating a content ID (step S1504). Here, as one example, the content ID generating unit 104 generates the content ID from the service_id of the EIT and the present time in the TOT. In this case, content IDs are assigned in units of time. In addition, if at this point the content ID is generated in association with a unique ID that is internally stored in the content importing apparatus 100, it is possible to generate a content ID that is globally unique. The content ID that is generated in this way is transferred to the moved content list managing unit 1401 in order to update the MCL and is transferred to the multiplexing unit 105 in order to generate a content_id_descriptor in which the content ID is written. Also, in order to securely bind the content and the content ID, the content ID is transferred to the content key information encryption conversion unit 103.

On receiving the content ID, etc., from the content ID generating unit 104, the moved content list managing unit 1401 reads the MCL from the moved content list storing unit 1402 (step S1505) and registers the content ID received from the content ID generating unit 104 (step S1506). It should be noted that when the MCL is not present in the moved content list storing unit 1402, an MCL is generated and initialized.

Here, the MCL is composed as shown in FIG. 19. In the MCL shown in FIG. 19, the number of writes is registered as the number of times a content has been written onto a storage medium so far. In addition, a maximum number of writes per unit time (maximum times/period), an interval ("penalty period") for performing control so that the writing of a content is prohibited for a fixed period

following the writing of the content and a time showing when a previous write was performed (previous write time) are recorded in the MCL. As one example, for the content with the content ID "CONTENT-ID-11111", the MCL shows that one write has been performed and the maximum number of writes per unit time is set at "2/Day", so that it is possible to write the content twice during a single day and this content may be written one further time. The penalty period is set at "1 hour", so that control is performed to impose a penalty so that the writing of the content onto a storage medium is prohibited for one hour following the previous write time "22:22:22", which is to say, until "23:22:22". It should be noted that in the present embodiment, the maximum number of writes per unit time and the penalty period are set separately for each content, though it is possible to set such parameters in each MCL and to set common restrictions for all of the contents on an MCL basis.

In the present embodiment, the number of writes is incremented (with the number of writes of contents that have not been written remaining at zero) as the process for marking contents that have been written, so that it is possible to distinguish between contents that have been written and contents that have never been written.

The moved content list managing unit 1401 writes the updated MCL in the moved content list storing unit 1402 (step S1507).

The content key information encryption conversion unit 103 uses the content ID and the network key received from the content ID generating unit 104 to re-encrypt the decrypted ECM (step S1508). More specifically, the content key information encryption conversion unit 103 takes an XOR for the content ID and an encryption key that is internally stored and has been shared in advance on the network, and re-encrypts the ECM using the result of the XOR. In addition, the content key information encryption

conversion unit 103 converts the re-encrypted ECM into TS packets and transfers the TS packets to the multiplexing unit 105.

The multiplexing unit 105 multiplexes the TS packets of the content received from the separating unit 102 and the TS packets of the ECM, whose encryption has been converted, received from the content key information encryption conversion unit 103. The multiplexing unit 105 also generates a content_id_descriptor from the content ID received from the content ID generating unit 104 and inserts this content_id_descriptor into the descriptor part of the PMT (step S1509).

In this way, in the content importing apparatus 100, the encryption of the ECM is converted so as to generate a content that is bound to the network, the content ID is set in the PMT, and the re-encrypted ECM is multiplexed with the content. The content ID of the imported content is also registered in the MCL.

On the other hand, FIG. 20 is a flowchart showing the content writing process performed by the content using apparatus 110b. Since a process that enquires to the content importing apparatus 100 to see whether the writing of the content is permitted or prohibited is also performed, the processing of the content importing apparatus 100 is also shown in the drawing.

In the separating unit 111, the content and the ECM are separated from the transport stream received from the content importing apparatus 100. The separating unit 111 also separates the PMT, obtains the content ID from the content_id_descriptor of the descriptor part in the PMT, and notifies the content key information decrypting unit 112 (step S1701).

The content key information decrypting unit 112 transfers the content ID received from the separating unit 111 to the content ID transmitting unit 1404 and the content ID transmitting unit 1404 transmits the content ID to the content importing apparatus 100 (step S1702).

The content ID receiving unit 1403 of the content importing apparatus 100 receives the content ID (step S1703) and transfers the received content ID to the moved content list managing unit 1401.

The moved content list managing unit 1401 reads the MCL from the moved content list storing unit 1402 (step S1704).

The moved content list managing unit 1401 judges whether the external writing of the content is permitted or prohibited based on the content ID and the MCL (step S1705). More specifically, the moved content list managing unit 1401 performs a process that refers to the maximum number of writes per unit time and the penalty time for the content ID that are registered in the MCL and judges whether the limitations are satisfied.

When the judgement in step S1705 is "YES", which is to say, the judgement result is that the write is permitted, the moved content list managing unit 1401 adds one to the number of writes in the MCL, updates the MCL, and stores the MCL in the moved content list storing unit 1402 (step S1706). The moved content list managing unit 1401 also transmits the judgement result to the content ID receiving unit 1403.

When the judgement in step S1705 is "NO", which is to say, the judgement result is that the write is prohibited, the moved content list managing unit 1401 transmits the judgement result to the content ID receiving unit 1403.

The content ID receiving unit 1403 of the content importing apparatus 100 transmits the judgement result about the writing that has been received from the moved content list managing unit 1401 to the content using apparatus 110b (step S1707).

The content ID transmitting unit 1404 of the content using apparatus 110b receives the judgement result showing whether the writing is permitted from the content using apparatus 110b and transfers the judgement result to the content key information

decrypting unit 112 (step S1708).

The content key information decrypting unit 112 determines whether the writing process for the content is to be performed, in accordance with the judgement result showing whether the writing is permitted (step S1709).

When the judgement in step S1709 is "YES", which is to say, when the judgement result shows that the writing is permitted, the content key information decrypting unit 112 obtains the re-encrypted ECM from the separating unit 111, takes an XOR for the network key and the content ID, and uses the result to decrypt the ECM (step S1710).

The content key information decrypting unit 112 obtains the content key from the ECM and transfers the content key to the content decrypting unit 116, in addition to instructing the content output control unit 115 to transfer the content in question to the content writing unit 119 (step S1711). By doing so, the content output control unit 115 controls the content output selecting unit 117 so as to write the content.

The content decrypting unit 116 decrypts (descrambles) the TS packets obtained from the separating unit 111 using the content key obtained from the content key information decrypting unit 112 (step S1712).

Based on control by the content output control unit 115, the content output selecting unit 117 transfers the content to the content writing unit 119 in order to write the content (step S1713).

The content writing unit 119 writes the content onto a storage medium (step S1714). More specifically, the content writing unit 119 encrypts the content in a suitable method for a storage medium, such as a DVD-RAM or D-VHS, converts the format, and writes the content onto the storage medium.

When the judgement in step S1709 is "NO", which is to say, when the judgement result shows that the writing is prohibited, the

content key information decrypting unit 112 cancels the content writing process.

In this way, in the present content using system 3, a content ID is assigned to a content bound to the network and at the same time the content ID is registered in the MCL that is managed in the content importing apparatus 100. When writing a content, the content using apparatus 110b enquires to the content importing apparatus 100 as to whether the writing is permitted or prohibited and the content importing apparatus 100 uses the MCL to judge whether the writing is permitted or prohibited, thereby imposing limitations on the writing of contents.

The content reproduction (display) process in the content using apparatus 110b is performed with the same processing flow as was shown in FIG. 20, and so description of such is omitted. However, it is necessary to amend the procedure so that the processing in step S1706 is never performed and the processing in step S1712 has the content output selecting unit 117 transfer, in accordance with an instruction from the content output control unit 115, the content to the content display unit 118 so that the content is reproduced.

Fourth Embodiment

The following describes a fourth embodiment of the present invention with reference to the attached drawings.

FIG. 21 is a block diagram showing the construction of a content using system 4 according to the fourth embodiment of the present invention. It should be noted that in FIG. 21 construction elements that are the same as in the content using system 3 of the third embodiment shown in FIG. 16 have already been described with reference to FIG. 16, so that such construction elements have been given the same reference numerals as in FIG. 16 and

description of such has been omitted.

Compared to the content using system 3 of the third embodiment of the present invention, the content using system 4 shown in FIG. 21 is characterized as follows. The content importing apparatus 100 has a moved content list transmitting unit 1801 in place of the content ID receiving unit 1403 and the content using apparatus 110c has a moved content list receiving unit 1802 in place of the content ID transmitting unit 1404 and also includes a moved content list managing unit 1803 and a moved content list storing unit 1804. The content importing apparatus 100 manages the MCL and the content using apparatus 110c receives a copy of the MCL from the content importing apparatus 100 and controls the writing and displaying of contents based on the received MCL.

When the MCL stored in the moved content list storing unit 1402 has been updated, the moved content list transmitting unit 1801 in the content importing apparatus 100 transmits the MCL to the content using apparatus 110c. More specifically, the MCL is transmitted to every content using apparatus 110c when (1) a content ID has been registered in the MCL due to the content importing apparatus 100 newly importing a content or (2) when a content has been written by a content using apparatus 110c, the content ID of the written content has been received from the content using apparatus 110c and marking has been performed for the content ID in question in the MCL to indicate the write. Here, the MCL may be broadcast as one example of the transmission method.

When a content has been written, the moved content list receiving unit 1802 in the content using apparatus 110c performs a process that transmits the content ID of the written content to the content importing apparatus 100 and, when the MCL has been updated in the content importing apparatus 100, receives the new MCL whose version number has been updated.

The moved content list managing unit 1803 in the content

using apparatus 110c manages the MCL in the moved content list storing unit 1804. More specifically, when a content has been written, the moved content list managing unit 1803 performs a process that transfers the content ID of the written content to the moved content list receiving unit 1802, receives the MCL that has been received by the moved content list receiving unit 1802, and updates the MCL in the moved content list storing unit 1804.

The moved content list storing unit 1804 in the content using apparatus 110c is the unit that stores the MCL and is realized by a hard disk drive or the like.

The following describes, with reference to the flowcharts in FIGS. 22 and 23, the processing that synchronizes the MCL between the content importing apparatus 100 and the content using apparatus 110c in the content using system 4 constructed as described above. It should be noted that the processing performed when a content is imported by the content importing apparatus 100 is the same as the operation shown in FIG. 18 and described in the third embodiment, and so description of such is omitted here.

FIG. 22 is a flowchart showing the content writing process of the content using apparatus 110c.

The separating unit 111 separates the content and the ECM from the transport stream received from the content importing apparatus 100. The separating unit 111 also separates the PMT, obtains the content ID from the content_id_descriptor of the descriptor part of the PMT, and notifies the content key information decrypting unit 112 (step S1901).

The content key information decrypting unit 112 transfers the content ID obtained from the separating unit 111 to the moved content list managing unit 1803 and the moved content list managing unit 1803 reads the MCL from the moved content list storing unit 1804 (step S1902). At this point, if no MCL is stored in the moved content list storing unit 1804, the moved content list

managing unit 1803 generates an MCL.

The moved content list managing unit 1803 searches the MCL to see if the content ID received from the content key information decrypting unit 112 is present (step S1903).

When the judgement in step S1903 is "NO", which is to say, when the content ID is not present in the MCL, the moved content list managing unit 1803 temporarily stores the content ID for transmission to the content importing apparatus 100 (step S1904).

The content key information decrypting unit 112 receives TS packets for the ECM from the separating unit 111, reconstructs the ECM section, and obtains the re-encrypted ECM. The content key information decrypting unit 112 takes an XOR for the network key and the content ID and decrypts the encrypted part of the ECM using the result of the XOR (step S1905).

The content key information decrypting unit 112 extracts the content key from the ECM, transfers the content key to the content decrypting unit 116, and also instructs the content output control unit 115 to transfer the content in question to the content writing unit 119 (step S1906). Accordingly, the content output control unit 115 controls the content output selecting unit 117 to write the content.

The content decrypting unit 116 decrypts (descrambles) the TS packets obtained from the separating unit 111 using the content key obtained from the content key information decrypting unit 112 (step S1907).

The content output selecting unit 117 transfers, based on the control of the content output control unit 115, the content to the content writing unit 119 in order to write the content (step S1908).

The content writing unit 119 writes the content onto a storage medium (step S1909). More specifically, the content writing unit 119 changes the format or encrypts the content, etc., using a suitable method for the storage medium, such as a DVD-RAM or

D-VHS, and then writes the content onto the storage medium.

When the judgement in step S1903 is "YES", which is to say, the judgement result is that the content ID is present in the MCL, the information in the MCL relating to the content ID is used to confirm whether the writing is permitted or prohibited (step S1910). More specifically, since the number of writes, maximum writes per unit time, etc., are recorded for each content ID in the MCL, the moved content list managing unit 1803 refers to such information and confirms whether the write is permitted.

When the judgement in step S1910 is "YES", which is to say, the judgement result is that the write is permitted, the content ID is temporarily stored in the moved content list managing unit 1803 (step S1904). The processing in step S1904 onwards is the same as the processing described above and so description of such has been omitted.

When the judgement in step S1910 is "NO", which is to say, the judgement result is that the write is prohibited, the content writing process is cancelled (step S1911).

FIG. 23 is a flowchart showing the process that transmits the content ID, which has been temporarily stored in the moved content list managing unit 1803 of the content using apparatus 110c as shown by step S1904 in FIG. 22, to the content importing apparatus 100 and so synchronizes the MCL between the content importing apparatus 100 and the content using apparatus 110c. It should be noted that in FIG. 23 the content using apparatus 110c that has written the content represents a plurality of content using apparatuses 110c, with the other content using apparatuses 110c also performing a process that receives and synchronizes the MCL.

The content ID of the content that has been written, which is stored in the moved content list managing unit 1803 of the content using apparatus 110c, is transferred to the moved content list receiving unit 1802 and is transmitted via the network to the content

importing apparatus 100 (step S2001).

The moved content list transmitting unit 1801 of the content importing apparatus 100 receives the content ID (step S2002) and transfers the content ID to the moved content list managing unit 1401.

The moved content list managing unit 1401 reads the MCL in the moved content list storing unit 1402 (step S2003), adds the received content ID to the MCL or updates the entry for this content ID, and updates the MCL in the moved content list storing unit 1402 (step S2004). At this point, the version number of the MCL is updated. The moved content list managing unit 1401 transfers the updated MCL to the moved content list transmitting unit 1801.

The moved content list transmitting unit 1801 transfers the updated MCL to the content using apparatuses 110c (step S2005). As one example, the moved content list transmitting unit 1801 may broadcast the MCL to every content using apparatus 110c.

The moved content list receiving unit 1802 of the content using apparatus 110c receives the updated MCL (step S2006) and transfers the received MCL to the moved content list managing unit 1803.

The moved content list managing unit 1803 refers to the version number of the received MCL and compares this with the version number of the stored MCL (step S2007).

When the judgement in step S2007 is "YES", which is to say, the received MCL is a newer version, the moved content list managing unit 1803 replaces the MCL in the moved content list storing unit 1804 with the received MCL (step S2008). It should be noted that when no MCL is stored in the moved content list storing unit 1804, the moved content list managing unit 1803 unconditionally writes the received MCL into the moved content list storing unit 1804.

When the judgement in step S2007 is "NO", which is to say,

the received MCL is not a newer version, the moved content list managing unit 1803 discards the received MCL.

In this way, in the present content using system 4 a content ID is assigned to a content that has been bound to the network and at the same time the content ID is registered in the MCL that is managed in the content importing apparatus 100. This MCL is transmitted to the content using apparatus 110c and when a content is to be written, the MCL that is stored in each content using apparatus 110c is used to judge whether the write is permitted or prohibited, thereby imposing limitations on the writing of contents.

Fifth Embodiment

The following describes a fifth embodiment of the present invention with reference to the attached drawings.

FIG. 24 is a block diagram showing the construction of a content using system 5 according to the fifth embodiment of the present invention. It should be noted that in FIG. 24 construction elements that are the same as in the content using system 1 of the first embodiment shown in FIG. 3 have already been described with reference to FIG. 3, so that such construction elements have been given the same reference numerals as in FIG. 3 and description of such has been omitted.

In the content using systems of the first to fourth embodiments of the present invention described above, when the content that is imported by the content importing apparatus 100, the content key information is re-encrypted using only an encryption key that has been shared in advance on the network, so that it is possible to use the content in real time and to use the content after first recording the content onto a storage unit, such as a hard disk drive, that is connected on the network. This means that when the content is written, limitations can be imposed on the writing using the MCL.

On the other hand, in the content using system 5 shown in the fifth embodiment of the present invention, when the content importing apparatus 100 imports a content, secret information is generated, the content key information is re-encrypted by making use of this secret information, and when a content is written (reproduced), the content using apparatus 110d indicates the output destination and obtains the secret information from the content importing apparatus 100, and so becomes able to write (reproduce) the content. This is to say, a mode is provided for indicating the output destination of the content from the content using apparatus 110d to the content importing apparatus 100 and, in accordance with the output destination, then writing the content onto the storage medium in real time or reproducing the content. Here, when an output request has been received from the content using apparatus 110d, the content importing apparatus 100 confirms the write, thereby imposing a limitation over the writing of contents.

The content using system 5 shown in FIG. 24 is characterized as follows. The content importing apparatus 100 includes the input unit 101, the separating unit 102, the content key information encryption conversion unit 103, the multiplexing unit 105, and an output request processing unit 2101, and the content using apparatus 110d includes the separating unit 111, the content key information decrypting unit 112, the content output control unit 115, the content decrypting unit 116, the content output selecting unit 117, the content display unit 118 and the content writing unit 119 as content outputting units, and an output request unit 2102. The content key information encryption conversion unit 103 of the content importing apparatus 100 generates secret information with an arbitrary timing and uses an encryption key (network key) that has been shared in advance on the network and the secret information to encrypt the content key information. The output

request unit 2102 of the content using apparatus 110d transmits an output request to the content importing apparatus 100 as an output request for the writing or reproduction of a content and the output request processing unit 2101 of the content importing apparatus 100 transmits the secret information as the request response. The output request unit 2102 of the content using apparatus 110d obtains the secret information from the request response, and the content key information decrypting unit 112 decrypts the content key information using the network key and the secret information and decrypts the content using the content key obtained from the content key information. The content output selecting unit 117 switches the output of the content in accordance with the output destination.

In the first embodiment of the present invention, the content key information encryption conversion unit 103 of the content importing apparatus 100 converts the encryption of the ECM using the network key, but in the present embodiment, when a content is imported, secret information is generated at arbitrary timing and the ECM is re-encrypted using the network key and the secret information. As the timing for generating the secret information, as examples the secret information may be generated for each program (event) and/or for each content and when new secret information is generated, the previous secret information is deleted. In this way, by using a method whether secret information is stored for only a period during which the secret information is valid, the content that is outputted can be identified.

The output request processing unit 2101 of the content importing apparatus 100 transmits, as the output request for a content from the content using apparatus 110d, the output destination for a content and a challenge that is used for authentication, generates a response from the challenge, and transmits the response and the secret information to the content

using apparatus 110d as the request response.

The output request unit 2102 of the content using apparatus 110d transmits, to the content importing apparatus 100, an output destination in accordance with whether the content is to be written or to be reproduced and a challenge that is used for authentication. The output request unit 2102 receives the response and the secret information transmitted from the content importing apparatus 100 as the response to the output request and authenticates the response. Only when the authentication succeeds does the output request unit 2102 perform processing that transfers the secret information to the content key information decrypting unit 112. It should be noted that the details of the challenge-response authentication are not described in this embodiment, though the authentication process may be performed using the same method as the challenge-response that is used in CHAP (Challenge Handshake Authentication Protocol) or SSL (Secure Socket Layer).

The operation of the content using system 5 constructed as described above is described below using the flowcharts shown in FIGS. 25 and 26.

FIG. 25 is a flowchart showing the processing when a content is imported by the content importing apparatus 100.

The input unit 101 receives a transport stream from the broadcast wave (step S2201).

The separating unit 102 receives the transport stream from the input unit 101, refers to the PIDs of the TS packets, and separates the TS packets of the content and the TS packets of the ECM (step S2202). To make it possible for the content key information encryption conversion unit 103 to identify an event, the separating unit 102 separates the EIT packets and transfers the EIT packets to the content key information encryption conversion unit 103.

The content key information encryption conversion unit 103

receives the TS packets of the ECM, reconstructs the ECM section, and decrypts the encrypted ECM using the work key (step S2203). The content key information encryption conversion unit 103 also reconstructs the EIT from the received TS packets of the EIT and obtains the event information.

The content key information encryption conversion unit 103 generates secret information in event units (step S2204). More specifically, the content key information encryption conversion unit 103 generates, for each event, secret information of a fixed byte length using a random number.

The content key information encryption conversion unit 103 uses the generated secret information and the network key to re-encrypt the ECM (step S2205). More specifically, the content key information encryption conversion unit 103 uses a certain encryption algorithm, such as AES (Advanced Encryption Standard), and the generated secret information to encrypt the content key part of the ECM. In addition, the content key information encryption conversion unit 103 encrypts the entire ECM using the network key. The content key information encryption conversion unit 103 converts the re-encrypted ECM into TS packets and transfers the packets to the multiplexing unit 105.

The multiplexing unit 105 multiplexes TS packets of the content that have been received from the separating unit 102 with TS packets of the ECM, whose encryption has been converted, that have been received from the content key information encryption conversion unit 103 (step S2206).

In this way, the content importing apparatus 100 generates secret information and uses the network key and this secret information to convert the encryption of the ECM, resulting in the content being processed so that the content cannot be used without first obtaining the secret information.

On the other hand, FIG. 26 is a flowchart showing the content

writing process in the content using apparatus 110d.

When the output request unit 2102 of the content using apparatus 110 directly writes a content that is broadcast in real time, the output request unit 2102 generates a challenge (such as a random number) for performing an authentication process with the content importing apparatus 100, and transmits the challenge data and an output destination of the content (which indicates the content writing unit 119, etc.) to the content importing apparatus 100 as an output request (step S2301).

The output request processing unit 2101 of the content importing apparatus 100 receives the challenge and the output destination as the output request from the content using apparatus 110d (step S2302).

The output request processing unit 2101 judges whether the outputting of the content is permitted or prohibited (step S2303). More specifically, the output request processing unit 2101 confirms the output destination (the write destination) in the output request, compares the output destination with the limitations on the write destination that are defined for the system or by copy control information written in the broadcast wave, and determines whether the write is permitted or prohibited. When a challenge/response procedure is performed with a certain content using apparatus 110d, a limitation can be imposed on the writing of a content by not having the output request processing unit 2101 receive a challenge from other content using apparatuses 110d on the network or by receiving challenges from the content using apparatuses 110d only until a predetermined number of challenges has been reached.

When the judgement in step S2303 is "YES", which is to say, when the output request processing unit 2101 has judged that the outputting is permitted, the output request processing unit 2101 generates a response from the challenge and sets the response and the secret information in a message as a request response (step

S2304).

When the judgement in step S2303 is "NO", which is to say, when the output request processing unit 2101 has judged that the outputting is prohibited, the output request processing unit 2101 generates an error message showing that the outputting is prohibited and sets this in a message as a request response.

The output request processing unit 2101 transmits the request response to the content using apparatus 110d (step S2305).

The output request unit 2102 of the content using apparatus 110d receives the request response (step S2306) and authenticates the response (step S2307).

When the judgement in step S2307 is "YES", which is to say, when the authentication process has succeeded, the output request unit 2102 obtains the secret information and transfers the secret information to the content key information decrypting unit 112 (step S2308).

When the judgement in step S2307 is "NO", which is to say, when the authentication process has failed, the output request unit 2102 does not obtain the secret information and the content writing process is terminated.

The content key information decrypting unit 112 decrypts the re-encrypted ECM using the network key and also uses the secret information to decrypt the encrypted part of the content key (step S2309). The content key information decrypting unit 112 also indicates the write destination and the write path, etc., for the content to the content output control unit 115.

The content key information decrypting unit 112 transfers the decrypted content key to the content decrypting unit 116 (step S2310).

The content decrypting unit 116 decrypts the encrypted content received from the separating unit 111 using the content key received from the content key information decrypting unit 112 (step

S2311).

The content output selecting unit 117 selects to output the content to the content writing unit 119 in accordance with the content output control information (the write destination and the write path, etc., for the content) received from the content output control unit 115 (step S2312).

The content writing unit 119 outputs the content to the storage medium (step S2313).

In this way, the present content using system 5 is provided with a mode for outputting a content in real time to a storage medium (or reproducing the content) and by re-encrypting the content key information using secret information, which is generated when the content is imported, and a network key, only content using apparatuses 110d that have been able to obtain the secret information can use the content. This is to say, if the content importing apparatus 100 performs control so as to transfer the secret information to only a limited number of content using apparatuses 110d, there is no need to store or manage the MCL, which has the advantages of high security and of making it possible to simplify the construction. As one example, if copying is only allowed once for a content (such as when the copy control information is "NETWORK COPY"), when the content is imported, it is possible to impose a limitation by having the content importing apparatus 100 refer to the copy control information, convert the encryption of the content key information in this mode, and transfer the secret information to only one content using apparatus 110d, so that only one copy can be generated from the network.

It should be noted that the present embodiment describes an example where the content importing apparatus 100 encrypts the content key information using the secret information, which is generated when the content is imported, and the network key, which is an encryption key that is shared on the network in advance,

though provided that the encryption key for encrypting the content key information is shared by at least the content importing apparatus 100 and the content using apparatus 110, the present embodiment is not limited to the above example.

Sixth Embodiment

The following describes a sixth embodiment of the present invention with reference to the attached drawings.

FIG. 27 is a block diagram showing the construction of a content using system 6 according to the sixth embodiment of the present invention. It should be noted that in FIG. 27 construction elements that are the same as in the content using system 1 of the first embodiment shown in FIG. 3 have already been described with reference to FIG. 3, so that such construction elements have been given the same reference numerals as in FIG. 3 and description of such has been omitted.

Compared to the content using system 1 of the first embodiment of the present invention, the content using system 6 shown in FIG. 27 is characterized as follows. The content using system 6 further includes a recording apparatus 2401 for recording a content onto a recording medium. While the construction of the content importing apparatus 100 is the same as that of the content importing apparatus 100 in the first embodiment of the present invention, the content using apparatus 110e does not include the moved content list managing unit 113, the moved content list storing unit 114 and the content writing unit 119. The recording apparatus 2401 includes a content writing unit 2402, a moved content list managing unit 2403, and a moved content list storing unit 2404. The recording apparatus 2401 manages the MCL, and when a content and a content ID received from the content using apparatus 110e are to be written on a storage medium, the recording apparatus 2401 uses the MCL to judge whether the writing

of the content is permitted and controls the writing of the content based on the result of this judgement.

The recording apparatus 2401 can be an apparatus, such as a DVD-RAM recorder or an SD CARD writer/reader that writes a content onto a storage medium.

The content writing unit 2402 performs the processing required to write a content onto a storage medium and writes the content onto the storage medium.

The moved content list storing unit 2404 is the part that stores the MCL and is realized by a hard disk drive or the like.

The moved content list managing unit 2403 manages the MCL stored in the moved content list storing unit 2404. More specifically, the moved content list managing unit 2403 performs a read/write process for the MCL that reads the MCL from the moved content list storing unit 2404, updates the MCL, and writes the MCL back into the moved content list storing unit 2404, and also receives a content ID of a content to be written onto a storage medium from the content writing unit 2402 and uses the MCL to judge whether to allow the writing of the MCL onto the storage medium.

The following describes, with reference to the flowchart shown in FIG. 28, the operation of the content using system 6 constructed as described above.

It should be noted that the content importing process performed by the content importing apparatus 100 is the same as in the first embodiment of the present invention and has already been described, so that the description of such is omitted here.

FIG. 28 is a flowchart showing the content writing process of the content using apparatus 110e and the recording apparatus 2401.

The separating unit 111 separates the content and the ECM from the transport stream received from the content importing apparatus 100 (step S2501).

The content key information decrypting unit 112 receives the TS packets of the ECM from the separating unit 111, reconstructs the ECM section, and so obtains the re-encrypted ECM. The content key information decrypting unit 112 decrypts the re-encrypted part of the ECM using a network key that has been obtained in advance (step S2502).

The content key information decrypting unit 112 extracts the content key from the ECM and transfers the content key to the content decrypting unit 116 (step S2503). The content key information decrypting unit 112 also transmits the information such as the write destination and the write path to the content output control unit 115 so that the content output control unit 115 can control the content output selecting unit 117 to output to the recording apparatus 2401. In addition, the recording apparatus 2401 reads, from the ECM, the content ID that is used to judge whether the writing of a content is permitted or prohibited and transfers the content ID to the content output control unit 115. The content output control unit 115 transfers the content ID, the write destination, and the write path to the content output selecting unit 117 as content output control information.

The content decrypting unit 116 decrypts (descrambles) the TS packets obtained from the separating unit 111 using the content key obtained from the content key information decrypting unit 112 (step S2504).

The content output selecting unit 117 switches to outputting to the recording apparatus 2401 based on the content output control information from the content output control unit 115 (step S2505) and transmits the content and the content output control information (step S2506).

The content writing unit 2402 of the recording apparatus 2401 receives the content and the content output control information from the content using apparatus 110e (step S2507).

The received content output control information is transferred to the moved content list managing unit 2403.

The moved content list managing unit 2403 reads the MCL from the moved content list storing unit 2404 (step S2508) and judges whether the write is prohibited or permitted (step S2509). This judgement as to whether the write is prohibited or permitted is performed using the same method as described in the first embodiment, and so description of such is omitted here.

When the judgement in step S2509 is "YES", which is to say, when the write has been judged to be permitted, the MCL is updated and is stored in the moved content list storing unit 2404 (step S2510). The content writing unit 2402 is also instructed to commence the content writing process.

The content writing unit 2402 writes the content onto the storage medium (step S2511).

It should be noted that when the judgement in step S2509 is "NO", which is to say, when the write has been judged to be prohibited, the content writing process is terminated.

In this way, in the present content using system 6, the MCL is managed in the recording apparatus 2401 and the MCL is used when writing a content to judge whether the write is permitted or prohibited, so that limitations can be imposed on the writing of contents by each recorder.

It should be noted that if there is a generation unit that uniformly increases or uniformly decreases the content ID, the generation method of the content ID is not limited to the methods described in the first to fourth and sixth embodiments of the present invention. The content ID may be generated using a unique random number.

The content IDs may be assigned in scramble units for the contents. Alternatively, content IDs may be assigned in units in which button operations (user actions) for reproduction and

recording, etc., are made by users. As specific examples, such unit may be from when the user indicates the start of recording until when the user indicates the end of recording or from the selection of a channel by the user until the selection of another channel.

The first to fourth and sixth embodiments of the present invention show examples where content IDs are generated by the content ID generating unit 104 of the content importing apparatus 100, though it is possible to omit the content ID generating unit 104 and to use information that is assigned in advance to input data (such as data (the EIT, etc.) that is distributed together with the content) as the content IDs. More specifically, in the case of a digital broadcast, the service_id and the event_id that are set in the EIT may be used without amendment as the content IDs. Alternatively, when content IDs have been assigned to contents on the transmission side, such content IDs may be used.

The embodiments describe examples where a content is associated with the content key information using the multiplexing unit 105, though such associating is not limited to this method. Instead of separating and multiplexing, the content and content key information may be associated by any method.

In the above embodiments, between the content importing apparatus 100 and the content using apparatus 110, between a plurality of content using apparatuses 110, and between the content using apparatus 110 and the recording apparatus 2401, the content ID is transmitted and received in order to confirm the MCL, synchronization information for the MCL is transmitted and received, the content is transmitted and received, and content output control information is transmitted and received, though encryption may be performed for such communication to stop such data from being replaced or being tampered with.

At least the content key information encryption conversion unit 103 and the content ID generating unit 104 in the content

importing apparatus 100 and the content key information decrypting unit 112, the moved content list managing unit 113, the moved content list storing unit 114, and the content output control unit 115 of the content using apparatus 110 are parts that perform processing which relates to security, so that these units may be realized by modules, such as security modules, with tamper-free constructions.

Also, the first and fourth embodiments of the present invention show an example where the content using apparatus 110 includes a content display unit 118 and a content writing unit 119, though the content using apparatus 110 does not need to include both of these units, and the content using apparatus 110 may include only a content display unit 118 or the content using apparatus 110 may include only a content writing unit 119. In this case, one or both of the content output control unit 115 and the content output selecting unit 117 can also be omitted.

The first to sixth embodiments of the present invention are examples where an MPEG content, which has been multiplexed according to MPEG-2 Systems, is imported from a digital broadcast, though this is not a limitation for the present invention and it should be obvious that the present invention can be applied to a case where contents of any format are imported from a communication medium, such as the Internet, and/or a recording medium, such as a packaged medium.

In the above embodiments, examples that include, for outputting a content, a display unit for reproducing and displaying a content on a monitor and a writing unit for writing on a storage medium are described, though the present invention is not limited to these and the content may be outputted to a digital bus such as an IEEE 1394 bus. Here, it is possible to use a construction where it is judged whether the outputting of the content to the digital bus is permitted or prohibited in the same way as for the writing units in

the above embodiments.

In addition, in the content using apparatuses in each of the above embodiments, the content writing units may have a construction where in addition to the writing of a content in a state where the content is not bound to the network, the user may be able to select a writing of the content in a bound state.

Also each of the above embodiments may be constructed so that when the size of the MCL reaches the maximum size and content IDs can no longer be added, the content ID to be deleted from the MCL is determined according to a random number.

Additionally, in each of the above embodiments, the maximum number of writes, the write destination, and the write path can be set as the write conditions in the ECM, but it is possible to use a construction where information that shows whether writing is permitted or prohibited is set somewhere aside from the ECM in the transport stream.

Finally, the content importing apparatuses in each of the above embodiments may be physically integrated with any of the content using apparatuses.

INDUSTRIAL APPLICABILITY

The content using system of the present invention is composed of a content importing apparatus that is connected to a network and at least one content using apparatus. The content importing apparatus includes a content ID issuing unit that issues a content ID and a content key information encryption converting unit that converts the encryption of content key information using a network key that is shared in advance on the network. The content using apparatus includes a content key information decrypting unit that decrypts the content key information, whose encryption has been converted, using the network key, a moved content list storing unit for storing a moved content list (MCL) in which the content IDs

of contents that have been written onto a storage medium are written, and a moved content list managing unit that judges whether the writing of a content is permitted or prohibited based on the MCL. The present invention is utilized in a content using system, a content using method, a content using apparatus, and a content using program that write a content in accordance with the above judgement of whether the writing is permitted or prohibited.

CLAIMS

1. A content using system in which a content is used on a network to which a plurality of apparatuses are connected, comprising:

a binding unit that is provided in at least one of the plurality of apparatuses and is operable to bind the content to the network by putting the content in a state where only the apparatuses on the network can use the content;

an ID issuing unit that is provided in at least one of the plurality of apparatuses and is operable to issue a content ID that corresponds to the content that has been bound by the binding unit;

a bind removing unit that is provided in at least one of the plurality of apparatuses and is operable to put the content that has been bound by the binding unit in an unbound state;

a writing unit that is provided in at least one of the plurality of apparatuses and is operable to write the content that has been put in the unbound state by the bind removing unit onto a storage medium;

a table unit that is provided in at least one of the plurality of apparatuses and is operable to store a table showing the content ID of the content written by the writing unit; and

a suppressing unit that is provided in at least one of the plurality of apparatuses and is operable to obtain the content ID of the content to be written by the writing unit and to suppress writing of the content by the writing unit based on a content of the table.

2. A content using system according to Claim 1,

wherein the suppressing unit is operable to obtain the content ID of the content to be written by the writing unit, to add, if the obtained content ID has not been already recorded in the table, the

content ID to the table without suppressing the writing of the content by the writing unit, and to suppress the writing of the content by the writing unit if the obtained content ID is present in the table.

3. A content using system according to Claim 1,

wherein the suppressing unit is operable to obtain the content ID of the content to be written by the writing unit, to add, if the obtained content ID is not present in the table, the obtained content ID to the table and "1" as a number of writes by the writing unit, and to suppress the writing by the writing unit if the obtained content ID is present in the table and the number of writes has reached a predetermined maximum number.

4. A content using system according to Claim 3,

wherein the binding unit is operable to bind the content to the network by encrypting a content key for decrypting the content using a network key that is shared in advance with the plurality of apparatuses.

5. A content using system according to Claim 4,

wherein the plurality of apparatuses include one content importing apparatus and at least one content using apparatus,

the content importing apparatus includes the binding unit and the ID issuing unit, and

each of the content using apparatuses includes the table unit, the bind removing unit, the writing unit, and the suppressing unit.

6. A content using system according to Claim 5,

wherein the content using apparatuses further include:

a notifying unit operable to notify, when a write has been performed by the writing unit, other content using apparatuses of at

least the content ID; and

an updating unit operable to update a table stored in the table unit when a notification is received from another content using apparatus.

7. A content using system according to Claim 4,

including one content importing apparatus and at least one content using apparatus,

wherein the content importing apparatus includes the binding unit, the ID issuing unit, the table unit and the suppressing unit, and

each of the content using apparatuses includes the bind removing unit, and the writing unit.

8. A content using system according to Claim 4,

including one content importing apparatus and at least one content using apparatus,

wherein the content importing apparatus includes the binding unit, the ID issuing unit, and the table unit, and

each of the content using apparatuses includes the bind removing unit, the writing unit, and the suppressing unit.

9. A content using system according to Claim 8,

wherein each content using apparatus further includes a second table unit operable to store a copy of the table by obtaining a content of the table stored in the table unit of the content importing apparatus, and

the suppressing unit suppresses the writing of the content based on the copy of the table.

10. A content using system according to Claim 4,

wherein the ID issuing unit is one of (a) to (e):

(a) a unit operable to generate and issue the content ID using

a counter;

(b) a unit operable to generate and issue the content ID by uniformly incrementing or uniformly decrementing;

(c) a unit operable to generate and issue the content ID using a random value that generates a unique value;

(d) a unit operable to generate and issue the content ID based on data distributed together with the content; and

(e) a unit operable to obtain and issue the content ID from data distributed together with the content.

11. A content using system according to Claim 4,

wherein the ID issuing unit is operable to generate a content ID that is associated with an ID for identifying the content importing apparatus.

12. A content using system according to Claim 4,

wherein the ID issuing unit is operable to generate the content ID for each content that corresponds to a broadcast program.

13. A content using system according to Claim 4,

wherein the table includes information showing a write destination of a content for each content ID, and

the suppressing unit is operable to suppress the writing when the write destination shown by the information differs from a write destination into which the writing unit is to write the content.

14. A content using system according to Claim 4,

wherein the table includes information showing a write path of a content for each content ID, and

the suppressing unit is operable to suppress the writing when the write path shown by the information differs from a write path in

which the writing unit is to write the content.

15. A content using system according to Claim 4,

wherein the table includes information showing a permitted number of writes per unit time for the content , and

the suppressing unit is operable to suppress the writing when a number of writes of a content per unit time by the writing unit exceeds the permitted number of writes per unit time.

16. A content using system according to Claim 4,

wherein the table includes information showing a time interval from a writing of a content until a next permitted writing of the content, and

the suppressing unit is operable to suppress the writing by the writing unit when an interval for writes by the writing unit is shorter than the time interval.

17. A content using system according to Claim 4,

wherein a hash value of the table is securely managed by the table unit.

18. A content using system according to Claim 4,

wherein the table unit stores a threshold value for deleting content IDs that have been recorded in the table and deletes, when a number of content IDs that have been recorded in the table has reached the threshold value, at least one content ID from the table.

19. A content using system according to Claim 18,

wherein the table further records time and date information showing a time and date at which each content ID was registered, and

when the number of content IDs that have been recorded in

the table has reached the threshold value, the table unit determines a content ID to be deleted based on the time and date information.

20. A content using system according to Claim 18,

wherein the table further includes access information for contents, and

when the number of content IDs that have been recorded in the table has reached the threshold value, the table unit determines a content ID to be deleted based on the access information.

21. A content using system according to Claim 18,

wherein the table unit generates a random number when the number of content IDs that have been recorded in the table has reached the threshold value and determines a content ID to be deleted based on the random number.

22. A content using system including a content importing apparatus and at least one content using apparatus that share a network key, where a content is bound to a network by encrypting content key information, which includes a content key required to decrypt the content, using the network key,

the content importing apparatus including:

an obtaining unit operable to obtain a content and encrypted content key information, which includes the content key for the content, from the outside;

an ID generating unit operable to generate a content ID for identifying the content obtained by the obtaining unit; and

an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key,

and each content using apparatus including:

a first decrypting unit operable to decrypt the re-encrypted content key information using the network key;

a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit;

a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium;

a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and

a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing of the content by the writing unit when the number of times has reached a predetermined maximum number of times.

23. A content using system according to Claim 22,

wherein at least one content using apparatus further includes a reproducing unit operable to reproduce the content that has been decrypted by the second decrypting unit, and

the suppressing unit is operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress reproduction by the reproduction unit when the number of times has reached a predetermined maximum number of times.

24. A content using system according to Claim 22,

wherein each content using apparatus further includes a table synchronizing unit operable to synchronize the table with tables of other content using apparatuses, and

when the table is updated, the table synchronizing unit transmits synchronization information including at least the content ID to table synchronizing units of other content using apparatuses, and when synchronization information is received from a table synchronizing unit in another content using apparatus, the table synchronizing unit updates the table in the table storing unit.

25. A content using system including a content importing apparatus and at least one content using apparatus that share a network key, where a content is bound to a network by encrypting content key information, which includes a content key required to decrypt the content, using the network key,

the content importing apparatus including:

an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside;

an ID generating unit operable to generate a content ID for identifying the obtained content;

an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key;

a table storing unit operable to store a table that records the content ID of a content that has been written onto a storage medium by a content using apparatus;

a table managing unit operable to use, when a write permission judgement request has been received from a content using apparatus, the table to judge whether writing of a content is

permitted and to update the table based on a judgement result; and

a content ID receiving unit operable to receive the write permission judgement request from the content using apparatus and to transmit the judgement result obtained from the table managing unit, and

the content using apparatuses each including:

a first decrypting unit operable to decrypt the re-encrypted content key information using the network key;

a content ID transmitting unit operable to transmit to the content importing apparatus a write permission judgement request including the content ID included in the decrypted content key information and to receive the judgement result;

a second decrypting unit operable to decrypt the content using the content key included in the content key information decrypted by the first decrypting unit only when the received judgement result shows that the writing is permitted; and

a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium.

26. A content using system including a content importing apparatus and at least one content using apparatus that share a network key, where a content is bound to the network by encrypting content key information, which includes a content key required to decrypt the content, using the network key,

the content importing apparatus including:

an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside;

an ID generating unit operable to generate a content ID for identifying the obtained content;

an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by

the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key;

a first table storing unit operable to store a table that records the content ID of a content that has been written onto a storage medium by a content using apparatus;

a table managing unit operable to use, when a write permission judgement request has been received from a content using apparatus, the table to judge whether writing of a content is permitted and to update the table based on a judgement result; and

a table transmitting unit operable to receive synchronization information from a content using apparatus and to transmit the table to the content using apparatus,

and each content using apparatus including:

a first decrypting unit operable to decrypt the re-encrypted content key information using an encryption key that has been shared in advance on the network and to output the content key;

a table receiving unit operable to transmit synchronization information for the table that includes at least a content ID to the content importing apparatus and to receive the table;

a second table storing unit operable to store the table;

a table managing unit operable to update the table in the second table storing unit using the table received from the content importing apparatus and to judge whether writing of a content is permitted using the table;

a second decrypting unit operable to decrypt the encrypted content using the content key only when a judgement result of the table managing unit shows that writing is permitted; and

a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium.

27. A content using system including a content importing

apparatus and at least one content using apparatus that share a network key and also a content writing apparatus that is connected to at least one of the at least one content using apparatuses and writes a content onto a storage medium, where a content is bound to the network by encrypting content key information, which includes a content key required to decrypt the content, using the network key,

the content importing apparatus including:

an obtaining unit operable to obtain a content and encrypted content key information, which includes the content key for the content, from the outside;

an ID generating unit operable to generate a content ID for identifying the obtained content; and

an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key,

each content using apparatus including:

a first decrypting unit operable to decrypt the re-encrypted content key information using the network key; and

a second decrypting unit operable to decrypt the content using the content key included in the decrypted content key information, and

the content writing apparatus including:

a writing unit operable to write a content onto a storage medium;

a table storing unit operable to store a table for recording a content ID of the content written on the storage medium by the writing unit; and

a table managing unit operable to judge whether writing of a content is permitted using the table and to control the writing unit in accordance with a judgement result.

28. A content using system according to Claim 22,

wherein the first decrypting unit is operable to generate an ID by uniformly incrementing or uniformly decrementing a value in desired units and to transmit the ID to the second decrypting unit,

the second decrypting unit is operable to record the received ID and transmit the ID to the first decrypting unit when a write process is to be resumed, and

the first decrypting unit compares the received ID with a most recently generated ID and permits a resumption of the write process only when a difference between the IDs is a certain value or below.

29. A content using system in which a content importing apparatus and at least one content using apparatus are connected to a network,

the content importing apparatus including:

an encryption converting unit operable to convert encryption by decrypting encrypted content key information, generating secret information for influencing a content key, and re-encrypting the content key information using an encryption key that is shared in advance on the network and the secret information; and

an output request processing unit operable to receive a content output request from a content using apparatus and to transmit a request response including at least the secret information,

and the content using apparatus including:

an output requesting unit operable to transmit an output request, which includes at least an output destination of a content, to the content importing apparatus, to receive the request response, and to obtain the secret information;

a first decrypting unit operable to decrypt the re-encrypted content key information using an encryption key shared in advance

on the network and the secret information;

a control unit operable to output content output control information for controlling a selecting unit;

a second decrypting unit operable to decrypt the encrypted content using the content key;

a selecting unit operable to select an output destination of the content based on the content output control information; and

at least one output unit operable to output the content.

30. A content using apparatus that uses a content that has been bound to a network by encrypting content key information, which includes a content key required to decrypt the content, using a network key,

the content using apparatus comprising:

a first decrypting unit operable to decrypt the re-encrypted content key information using the network key;

a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit;

a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium;

a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and

a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing of the content by the writing unit when the number of times has reached a predetermined maximum number of times.

31. A content importing apparatus that binds a content to a network to which a plurality of apparatuses that share a network key are connected by encrypting content key information, which includes a content key required to decrypt the content, using the network key,

the content importing apparatus including:

an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside;

an ID generating unit operable to generate a content ID for identifying the content obtained by the obtaining unit; and

an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key,

wherein the content ID is used to manage writing of the content, which has been bound to the network, onto a storage medium in an unbound state.

32. A content using method of using a content on a network to which a plurality of apparatuses are connected,

the method comprising:

a binding step which is performed in at least one of the plurality of apparatuses and in which a content is bound to the network by putting the content in a state where only apparatuses on the network can use the content;

an ID issuing step which is performed in at least one of the plurality of apparatuses and in which a content ID that corresponds to the content that has been bound to the network in the binding step is issued;

a judging step which is performed in at least one of the plurality of apparatuses and in which a content ID of a content, which has been bound to the network and is to be written in an unbound state, is obtained, a table in which content IDs of contents that have already been written is recorded is referred to in a memory, and a judgement of whether writing the content is permitted is made;

a bind removing step which is performed in at least one of the plurality of apparatuses and in which the content that has been bound to the network by the binding unit is put in an unbound state when the judgement in the judging step is that writing is permitted; and

a writing step which is performed in at least one of the plurality of apparatuses and in which the content put in the unbound state in the bind removing step is written onto a storage medium.

33. A content using method performed by an apparatus that uses a content that has been bound to a network by encrypting content key information, which includes a content key that is required to decrypt the content, using a network key,

the content using method comprising:

a first decrypting step of decrypting the encrypted content key information using the network key;

a second decrypting step of decrypting the content using the content key in the content key information decrypted in the first decrypting step;

a judging step of obtaining a content ID of a content, which has been bound to the network and is to be written in an unbound state, referring to a table, in which content IDs of contents that have already been written is recorded, in a memory, and judging whether writing the content is permitted; and

a writing step of putting the bound content into an unbound

state and writing the content in the unbound state onto a storage medium when the judging step has judged that writing is permitted.

34. A content using program for a content using system that includes a content importing apparatus and at least one content using apparatus that share a network key, where a content is bound to the network by encrypting content key information, which includes a content key required to decrypt the content, using a network key, the content using program including a first program that is executed by the content importing apparatus and a second program that is executed by a content using apparatus,

the first program having a computer function as:

an obtaining unit operable to obtain a content and encrypted content key information, which includes a content key for the content, from the outside;

an ID generating unit operable to generate a content ID for identifying the content obtained by the obtaining unit; and

an encryption converting unit operable to convert encryption by decrypting the encrypted content key information obtained by the obtaining unit, adding the content ID to the decrypted content key information, and re-encrypting the content key information using the network key,

and the second program having a computer function as:

a first decrypting unit operable to decrypt the re-encrypted content key information using the network key;

a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit;

a writing unit operable to write the content decrypted by the second decrypting unit on a storage medium;

a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the

first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and

a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing by the writing unit when the number of times has reached a predetermined maximum number of times.

35. A content using program executed by an apparatus that uses a content that has been bound to a network by encrypting content key information, which includes a content key that is required to decrypt the content, using a network key,

the program having a computer function as:

a first decrypting unit operable to decrypt the encrypted content key information using the network key;

a second decrypting unit operable to decrypt the content using the content key in the content key information decrypted by the first decrypting unit;

a writing unit operable to write the content decrypted by the second decrypting unit onto a storage medium;

a table storing unit operable to store a table in which the content ID included in the content key information decrypted by the first decrypting unit is associated with a number of times the content corresponding to the content ID has been written by the writing unit; and

a suppressing unit operable to obtain the content ID of the content to be written by the writing unit, to refer, in the table, to the number of times the content corresponding to the content ID has been written, and to suppress writing by the writing unit when the number of times has reached a predetermined maximum number of

times.