

**(12) INTERNATIONAL APPLICATION PUBLISHED IN ACCORDANCE WITH THE
PATENT COOPERATION TREATY**

(19) WORLD INTELLECTUAL PROPERTY ORGANIZATION

WIPO | PCT

International Bureau

(43) International Publication Date:
13 July 2006 (13.07.2006)

(10) International Publication No.:
WO 2006/073040 A1

(51) International Patent Classification:

G06F 21/24 (2006.01)
G11B 20/10 (2006.01)
G11B 27/00 (2006.01)
H04N 5/91 (2006.01)
H04N 7/167 (2006.01)
H04N 7/173 (2006.01)

(21) International Application No.:
PCT/JP2005/022772

(22) International Filing Date:
12 December 2005 (12.12.2005)

(25) Filing Language: Japanese

(26) Publication Language: Japanese

(30) Priority Data:
JP 2005-003152 7 January 2005
(07.01.2005) JP

(71) Applicants (All Except US):
MATSUSHITA ELECTRIC INDUSTRIAL CO.,
LTD. **[JP]/[JP]**; 1006, Kadoma, Kadoma-
shi, Osaka 5718501 (JP).

(72) Inventors; and

(75) Inventors/Applicants (US Only): ITO,
Yoshikatsu; HARADA, Shunji; TSUSAKA,
Yuko; FUJIOKA, Soichiro; OHMORI, Motoji;
NAKANO, Toshihisa.

(74) Agent: NAKAJIMA, Shiro et. al.; Yodogawa
5-Bankan 6F, 3-2-1, Toyosaki, Kita-ku,
Osaka-shi 5310072 (JP).

(81) Designated Countries (*unless indicated
otherwise, for every available national
registration*): AE, AG, AL, AM, AT, AU, AZ, BA,
BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR,
CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS,
JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR,
LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW,
MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL,
PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, YU, ZA, ZM, ZW.

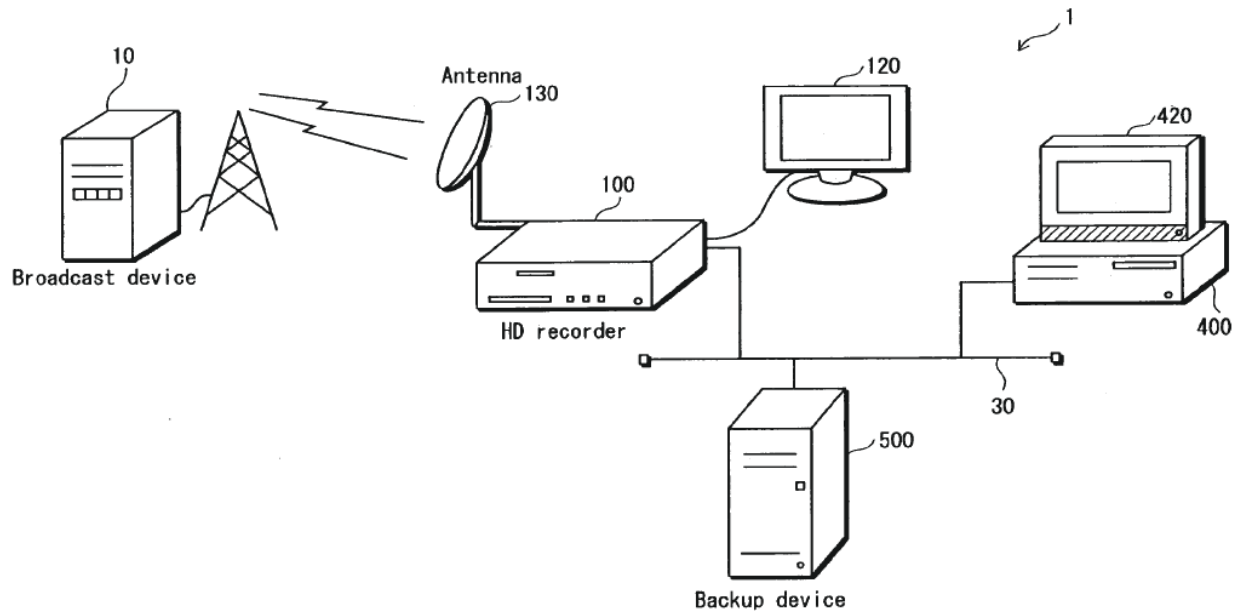
(84) Designated Countries (*unless indicated
otherwise, for every available regional
registration*): ARIPO (BW, GH, GM, KE, LS,
MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW);
Eurasia (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM);
Europe (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV,
MC, NL, PL, PT, RO, SE, SI, SK, TR); OAPI (BF,
BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR,
NE, SN, TD, TG)

Appended Documentation:

- International Search Report
*For two-letter codes and other abbreviations,
refer to "Guidance Notes on Codes and
Abbreviations" appearing at the start of every
regular issue of the PCT Gazette.*

(54) Title of the Invention: BACKUP SYSTEM, RECORDING AND PLAYBACK DEVICE, BACKUP DEVICE, BACKUP METHOD, PROGRAM, AND INTEGRATED CIRCUIT

(57) Abstract: It is inconvenient for users that Copy Once content cannot be copied to external devices even for backup purposes, but allowing copying for backup purposes poses the risk of unauthorized copying. The present invention provides an HD recorder 100 that transmits content to a backup device 500 and, at the same time, sets an expiration time for the content stored in the HD recorder 100 itself. The content stored in the HD recorder 100 is then deleted when the expiration time passes.



Description

BACKUP SYSTEM, RECORDING AND PLAYBACK DEVICE, BACKUP DEVICE, BACKUP METHOD, PROGRAM, AND INTEGRATED CIRCUIT

Technical Field

[0001] The present invention relates to technique for generating a backup of digital content while taking copyright protection of digital content into consideration.

Background Art

[0002] In recent years, digital broadcasting has been started to broadcast digital content. Since digital content experiences very little degradation with use, copy control information (CCI) indicating whether or not copies can be produced and the number of copies that can be produced is added to protect copyrights. CCI often indicates that copying is allowed only once (Copy Once). When content containing a CCI indicating Copy Once is recorded on a recording medium, the CCI added to this content is rewritten to a (No More Copies) CCI indicating that further copying is prohibited. Content that contains a CCI indicating No More Copies may not be copied, but is permitted to be moved (MOVE) to another medium.

[0003] Even when a CCI has been added to content, there are still incidents of fraudulent activities such as manipulating content stored in a hard disc drive (HDD) using, for example, a personal computer when the hard disc recorder ("HD recorder" below) has been turned off. To prevent unauthorized duplication, a technique has been used to detect unauthorized use of content by adding an assigned one-way function in advance to content stored on an HDD to calculate and store the fraud detection information. When power is turned on to the HD recorder, the content stored on the HDD is assigned to a one-way function to generate verification information, and content abuse is detected by comparing the generated verification information with the stored fraud detection information.

[0004] Another technique improves user convenience by temporarily storing content and deleting the content when a predetermined amount of time has elapsed or when the content has been played back, thereby realizing shifted playback of content that includes CCI indicating that copying is not permitted. However, since HDDs have large capacities and random access, users can store content broadcasted via digital broadcasting in HD recorders without worrying about storage capacity, and can watch the stored content by performing simple operations.

Disclosure of the Invention

Technical Problem

[0005] While HDDs are convenient, the rate of failure increases with frequency of use because they read and write information by performing spin and seek operations. If the HDD fails, data may be lost. To prevent such data loss due to HDD failure, backing up content to other storage media or recording devices is considered effective. However, if the content containing a CCI indicating Copy Once is moved to another medium, the content stored in the HD recorder will be deleted even if moved for the purpose of backup, which is an inconvenience for the user.

[0006] In addition, if content is allowed to be duplicated for backup purposes, the content may be illegally duplicated by malicious users, creating the problem of inadequate protection of copyright holders' rights. In view of this problem, it is an object of the present invention to provide a backup system, recording and playback device, backup device, backup method, integrated circuit, backup program, and recording medium that enable content to be backed up while balancing copyright protection with user convenience.

Solution to Problem

[0007] In order to realize this object, the present invention is a backup system comprising a recording and playback device for recording and playing back content, and a backup device, wherein the recording and playback device comprises: a storage means for storing the content; a receiving means for receiving

an instruction to back up the content; a content transmitting means for reading the content from the storage means and transmitting the read out content to the backup device upon receiving an instruction; a writing means for writing to the storage means, in association with the content, period information indicating a period during which playback of the content to be backed up is permitted upon receiving an instruction; and a playback control means for permitting playback of the content within the period indicated by the period information, and prohibiting playback of the content when the period indicated by the period information has ended, and wherein the backup device comprises: a content receiving means for receiving the content from the recording and playback device; and a backup storage means for storing the received content.

[0008] In the present specification, "backup" means storing a copy of content in a backup device in case the content stored in a legitimate device is lost due to mishandling or failure. A recording and playback device normally uses its own stored content, and if content stored by the recording and playback device is lost, the back-up device is used to obtain a copy and recover the lost content. Here, "cases of loss of content" which may be subject to recovery include not only the cases of a failure of the recording and playback device or the network to which the recording and playback device is connected, but also deletion due to insufficient memory in the recording and playback device, malfunctioning of the recording and playback device, and intentional deletion by the user. However, if content is lost due to a move to another recording medium, etc., the recording and playback device cannot retrieve the content from the back-up device.

Effects of the Invention

[0009] In the configuration described above, content is transmitted to a backup device and period information indicating the period during which playback of the content subject to backup is permitted is associated with the content and written to the storage means. In the recording and playback device, the period during which the content stored in the storage means can be played back is limited to the period indicated by the period information, allowing the user to view the content while protecting the rights of the copyright holder. As a result, content can be backed up as a failure countermeasure while balancing copyright protection with user convenience.

[0010] The present invention is also a recording and playback device for recording and playing back content, the recording and playback device comprising: a storage means for storing the content; a receiving means for receiving an instruction to back up the content; a content transmitting means for reading the content from the storage means and transmitting the read out content to the backup device upon receiving an instruction if backup of the read out content is permitted; a writing means for writing to the storage means, in association with the content, period information indicating a period during which playback of the content to be backed up is permitted upon receiving an instruction; and a playback control means for permitting playback of the content within the period indicated by the period information, and prohibiting playback of the content when the period indicated by the period information has ended.

[0011] In this configuration, the content is sent to the backup device, and period information indicating the period during which playback of the content that is being backed up is permitted is associated with the content and written to the storage means. When the playback control means determines that the period indicated by the period information has ended, it prohibits playback of the content, thereby limiting the period during which the content stored in the storage means can be played back to the period indicated by the period information. Therefore, content can be backed up as a failure countermeasure while balancing copyright protection and user convenience.

[0012] The recording and playback device further comprises: an extension requesting means for transmitting to the backup device an extension request requesting permission to extend the period indicated by the period information; and an extension means for receiving extension permission information indicating permission for extension from the backup device and extending the period indicated by the period information. In this configuration, the extension means receives extension permission information indicating permission for extension from the backup device and extends the period indicated by the period information. This allows the user to view content stored in the recording playback device even after the period indicated by the period information at the time of backup has ended.

[0013] Also, the recording and playback device sends the extension request to the backup device and extends the period information when it receives extension permission information. Here, it is assumed that the backup device is configured to send extension permission information only when the extension request meets certain conditions, such as being sent from a device that complies with a specific standard. In this way, it is possible to limit the devices that can extend the aforementioned period information to only those devices that satisfy the specified conditions.

[0014] In the recording and playback device, the extension requesting means transmits the extension request at a predetermined time prior to the end of the period indicated by the period information. In this configuration, the extension requesting means sends an extension request at a point in time before the end of the period indicated by the period information, so that the period during which viewing of the content is permitted by the recording and playback device is not interrupted.

[0015] In the recording and playback device, the extension requesting means repeatedly transmits the extension request within the period indicated by the period information at regular intervals. In this configuration, if transmission fails due to some kind of malfunction, the extension requesting means can reliably extend the period indicated by the period information by repeatedly transmitting the extension request.

[0016] In the recording and playback device, the extension means receives extension permission information indicating a period later than the period indicated by the period information stored in the storage means, and extends the period information by rewriting the period indicated by the period information to the period indicated by the received extension permission information. In this configuration, the extension means can quickly and easily extend the period information by simply replacing the period indicated by the period information with the period indicated by the received extension permission information.

[0017] The extension means constituting the recording and playback device stores the extension time in advance and extends the period information by adding the extended time to the period indicated by the expiration information. In a home network, internal LAN, etc., the backup device receives extension requests from each device connected to the network, determines whether to allow an extension, and sends the extension permission information.

[0018] In this configuration, the extension means extends the period information by adding the extension time stored in advance to the period indicated by the expiration information. In this way, by performing the operation of adding the extended period to the period in the recording and playback device, processing performed by the backup device can be reduced. Also, in the present invention, because the calculations performed for the management and extension of the effective period are performed by the recording and playback device, the backup device does not require a clock protected from external operations.

[0019] In the recording and playback device, the period information indicates the end of the period during which playback of the content stored in the storage means is permitted, and the playback control means permits playback of the content if the current time is prior to a point in time indicated by the period information, and prohibits playback of the content if the current time is after the point in time indicated by the period information.

[0020] In this configuration, the playback control means can easily determine whether to permit or prohibit playback of content by comparing the current time with the end time. In the recording and playback device, the period information includes permission time indicating the length of time during which playback of the content stored in the storage means is permitted, and the start time indicating the start time of the period during which playback of the content is permitted, and the playback control means acquires the elapsed time from the start time, and permits playback of the content if the acquired elapsed time is less than or equal to the permitted time, and prohibits playback of the content if the elapsed time from the start time exceeds the permitted time.

[0021] In this configuration, the period information indicates the permission time, which is the length of time during which playback of the content stored in the storage means is permitted, and the start

time, which is the start point of the period during which playback of the content is permitted. The period indicated by the period information is considered to be a period extending from the time at which the content was backed up to the backup device. The writing means can easily obtain the start time and write it to the storage means by obtaining the current time when the instruction is received and setting the current time as the start time.

[0022] In the recording and playback device, the playback control means prohibits playback of the content by deleting the content from the storage means. In this configuration, the playback control means can reliably prohibit playback of the content after the period indicated by the expiration information has ended in order to delete the content from the storage means.

[0023] In the recording and playback device of the present invention, the recording and playback device further comprises: a restore instruction acquiring means for acquiring a restore instruction indicating acquisition of the content stored in the backup device; a restore requesting means for transmitting to the backup device a request to transmit the content stored in the backup device upon acquiring a restore instruction; and a restore means for receiving the content from the backup device and writing the received content to the storage means, wherein the writing means further writes period information indicating the period during which playback of the content written by the restore means is permitted to the storage means in association with the content when the content is written.

[0024] In this configuration, the restore means receives the content from the backup device and writes the received content to the storage means. This allows users to view the content again. Also, upon receiving the content, the writing means writes period information indicating the period during which playback of the content written by the restore means is permitted, in association with the content, to the storage means. This makes it possible for the recording and playback device to limit the period during which the acquired content can be played back.

[0025] In the recording and playback device, the content stored in the storage means is configured to include encrypted copyrighted material generated by encrypting digital copyrighted material based on an encryption key and a decryption key used to decrypt the encrypted copyrighted material, and the playback control means prohibits playback of the content by deleting the decryption key included in the content.

[0026] In this configuration, the encrypted copyrighted material included in the content is generated by encrypting digital copyrighted material with an encryption key. Therefore, even if the encrypted copyrighted material is copied by an unauthorized user, the digital copyrighted material cannot be generated without the decryption key, thereby preventing unauthorized playback of the content. The recording and playback device further comprises: a restore instruction acquiring means for acquiring a restore instruction indicating acquisition of the encryption key stored in the backup device; a restore requesting means for transmitting a request to the backup device for transmission of the decryption key stored in the backup device when a restore instruction is acquired; and a restore means for receiving the decryption key from the backup device and writing the received decryption key to the storage means, wherein the writing means further writes period information indicating the period during which playback of the content stored in the storage means is permitted, in association with the content, to the storage means when the decryption key is written.

[0027] In this configuration, the restore means receives the decryption key and writes the received decryption key to the storage means. This allows the user to view the content stored in the recording and playback device again. In addition, because the writing means writes period information indicating the period during which playback of the content stored in the storage means is permitted to the storage means in association with the content, the playback period of the content can be limited in the recording and playback device.

[0028] In the recording and playback device, the content stored in the storage means includes encrypted copyrighted material generated by encrypting digital copyrighted material using an encryption key, and an encrypted key generated by encrypting a decryption key used to decrypt the encrypted copyrighted material using a unique key specific to the recording and playback device, and the playback control means prohibits playback of the content by deleting the encrypted key from the storage means.

[0029] In this configuration, the content stored in the storage means includes an encrypted key generated by encrypting the decryption key using the unique key, and encrypted digital copyrighted material encrypted using the encryption key. Therefore, even if the content is copied, it cannot be played back without the unique key, thereby preventing unauthorized playback of the content by third parties.

[0030] In the recording and playback device, the content stored in the storage means includes backup information indicating whether backup is permitted or prohibited, the content transmitting means determines whether the backup information indicates permission for backup, and transmits the content when it is determined that permission has been granted, and the writing means determines whether the backup information indicates permission for backup, and writes the period information when it is determined that permission has been granted.

[0031] In this configuration, the content is provided with backup information indicating whether backup is possible, which is added in advance by the creator, and the content transmitting means transmits the content only when the backup information indicates that backup is permitted. As a result, the intentions of the creator of the content can be reflected in regard to backup of the content.

[0032] The content transmitting means constituting the recording and playback device encrypts the content using a communication key and securely transmits the encrypted content. This configuration prevents unauthorized third parties from eavesdropping on the content. The recording and playback device further comprises a detection information storage means for storing detection information generated by performing a predetermined operation on the content, and an anti-tampering means for reading the content from the storage means, performing the predetermined operation on the read out content to generate inspection information, comparing the generated inspection information with the detection information, and prohibiting the use of content determined to be inconsistent.

[0033] In this configuration, the unauthorized use preventing means compares the detection information and the inspection information generated by the same operation. When a one-way function is used in this operation and there is any change to the content, the detection information will not match the inspection information. This makes it possible to easily detect tampering with the content and prevent playback of content that has been tampered with by malicious third parties.

[0034] In the recording and playback device, the backup device stores different content in response to a backup instruction from a device other than the recording and playback device, wherein the recording and playback device further comprises: a restore instruction acquiring means for acquiring a restore instruction indicating acquisition of the other content; a content requesting means for transmitting to the backup device a transmission request for the other content upon acquiring the restore instruction; and a restore means for receiving the other content from the backup device and writing the received other content to the storage means, and wherein the writing means further writes period information indicating the period during which playback of the other content is permitted to the storage means in association with the other content upon receiving the other content.

[0035] In this configuration, the restore means receives the other content from the backup device and writes the received other content to the storage means. In this way, for example, devices belonging to the same network, such as a home network or an internal LAN, can share the same content. This allows users to view the same content from any device installed in different rooms, improving user convenience.

[0036] Also, when the other content is written to the storage means, the writing means writes period information indicating the period during which playback of the other content is permitted to the storage means in association with the other content. This makes it possible to limit the period during which the content can be played back on each device that has the content. The present invention is also a backup device for backing up content, the backup device comprising: a storage device that stores the content; an extension request receiving means for receiving an extension request requesting permission to extend the period of time during which the content stored in the recording playback device may be played back; a determining means for determining whether or not to grant the extension; and a permission means for outputting extension permission information indicating permission for the extension to the recording and playback device when it has been determined that permission is to be granted.

[0037] In this configuration, when the determining means determines that an extension should be permitted, the permission means outputs extension permission information indicating that an extension has been permitted. This enables only devices that meet specified conditions receive extended playback period information for the content, while unauthorized devices that do not meet the conditions cannot receive extended playback period information. Therefore, playback of the content can be stopped after the period indicated by the period information has expired on devices that do not meet the conditions.

[0038] The storage means constituting the backup device further stores identification information indicating the content in association with the content, the extension receiving means receives the extension request including the content identification information indicating the content stored in the recording and playback device, and the determining means compares the content identification information with the identification information stored in the storage means, and grants permission if they match.

[0039] In this configuration, the determining means determines that permission is granted if the content identification information matches the identification information stored in the storage means. Therefore, when content stored in the backup device is moved and no longer backed up as a failure countermeasure, the period indicated by the period information is not be extended, and upon expiration of the period, playback of the content on the recording and playback device is no longer impossible. In this way, viewing of both content moved by malicious users from the backup device and content stored in the recording and playback device can be prevented.

[0040] In the backup device, the extension request includes device identification information indicating the recording and playback device that outputted the extension request, and the determining means stores in advance one or more pieces of permitted device identification information indicating a specific device, and grants the request if the device identification information included in the received extension request matches any of the pieces of permitted device identification information.

[0041] In this configuration, the determining means determines that permission should be granted if the device identification information included in the received extension request matches any of the pieces of permission device identification information stored in advance that indicates a specific device. This makes it possible to extend period information only for specific devices, thereby extending the period during which the content may be played back, while preventing the extension of the period during which the content may be played back on other devices.

[0042] In the backup device, the storage means further stores detection information generated by performing a predetermined operation on the content in association with the content, and the determining means reads the content from the storage means, performs the predetermined operation on the read out content to generate verification information, compares the generated verification information with the detection information, and grants the extension if they match.

[0043] In this configuration, the determining means compares the verification information generated by performing the same operation on the content with the detection information stored in the storage means, and permits an extension if they match. If a one-way function is used in this operation, tampering with the content can be easily detected. Therefore, if the content backed up by the backup device has been tampered with, the recording and playback device will not allow the playback period for the content to be extended, and the period during which the content can be played back can be limited.

[0044] In the backup device, the permission means outputs the permission information indicating a period later than the period indicated by the period information. In this configuration, since the permission means outputs the extended period information as extended permission information, the recording and playback device can quickly extend the period by replacing the period information with the extended period information.

[0045] Also, because the backup device sets the extended period information, this makes it possible to manage the period during which playback of the content of each device is permitted in a unified manner in the backup device. The backup device further comprises: a restore receiving means for receiving a transmission request for content stored in the storage means; a restore determining means for determining whether or not to transmit the content; and a restore transmitting means for reading the

content from the storage means and transmitting the read out content when it is determined that the content is to be transmitted.

[0046] In this configuration, when the restore determining means determines that transmission is to be performed, the restore transmission means reads the content from the storage means and transmits the read out content. Therefore, devices that meet the specified conditions can obtain the content, and users can enjoy viewing the content. Also, playback of the content on devices that do not meet the specified conditions can be prevented.

[0047] In the backup device, the transmission request includes restore device identification information indicating the restore device that is the transmission source of the transmission request, and the restore determining means stores one or more pieces of permitted device identification information indicating a specific device in advance, and determines that the content is to be transmitted if the restore device identification information matches any of the pieces of permitted device identification information.

[0048] In this configuration, the restore determining means determines that the content may be transmitted if the restore device identification information is included in the permission device identification information stored in advance. This makes it possible to limit devices that can obtain the content to only those devices that have been set in advance. In the backup device, the permitted device identification information indicates the backup device that transmitted the instruction to backup the content stored in the storage means, and the restore determining means determines that the content is to be transmitted if the restore device identification information and the permitted device identification information match.

[0049] In this configuration, devices capable of acquiring the content can be limited to the backup source device that sent an instruction to back up the content stored in the storage means. In the backup device of the present invention, the restore determining means has a copy count indicating the total number of devices storing content that is identical to the content stored in the storage means and permitted to be played by the backup device, and a copy permission count indicating the upper limit of the number of copies, and the content is permitted to be transmitted if the copy count is less than the copy permission count.

[0050] In this configuration, the restore determining means determines that the content may be transmitted if the copy count is less than the copy permission count. Therefore, the total number of devices having the same content can be limited to less than the number of permitted copies. The backup device further comprises: a period information storage means for associating and storing device identification information indicating the device that stores the content that is the same as the content stored in the storage means and that is permitted to be played by the backup device, and copying period information indicating the period during which playback of the content is permitted on the device; and a copy count management means for subtracting one from the copy count when the period indicated by the copy period information ends.

[0051] In this configuration, when the period indicated by the copy period information ends, a copy number managing means in the backup device subtracts one from the copy number. Therefore, when the period during which viewing of the content is permitted on a device ends, the backup device can output the content to other devices. In the backup device, the content stored in the storage means includes, in advance, the copy permission count, and the determining means obtains the copy permission count from the content.

[0052] In this configuration, because the creator of the content can generate content that includes any number of copy permissions, the determining means can perform a determination that reflects the intention of the creator of the content by using the number of copy permissions obtained from the content. The restore transmitting means constituting the backup device encrypts the content using a communication key and securely transmits the encrypted content.

[0053] This configuration prevents unauthorized third parties from eavesdropping on the content. In the backup device, the recording and playback device outputs a startup instruction information to the backup device to instruct the device to start up prior to an extension request, and the backup device

further comprises a power control means for starting the supply of power to each circuit comprising the backup device upon receipt of the startup instruction.

[0054] The backup device is designed to store content for disaster recovery purposes, so it preferably operates for short periods of time. In this configuration, when the power control means receives a start instruction, it starts supplying power to each circuit that constitutes the backup device. This makes it possible to shorten the operating time of the backup device and reduces the probability of failure of the hard disc unit constituting the storage means.

Brief Description of the Drawings

[0055]

[FIG. 1] FIG. 1 is a configuration diagram showing the configuration of the backup system 1 in the first embodiment.

[FIG. 2] FIG. 2 is a block diagram showing the configuration of the HD recorder 100.

[FIG. 3] FIG. 3 shows an example of information stored in the information storage unit 110.

[FIG. 4] FIG. 4 shows the details in a content management table 121.

[FIG. 5] FIG. 5 is a block diagram showing the configuration of the control unit 107.

[FIG. 6] FIG. 6 is an example of a menu screen 181 and a playback list screen 211 displayed on the monitor 120.

[FIG. 7] FIG. 7 is an example of an initial setting screen 191 and a restore information screen 221 displayed on the monitor 120.

[FIG. 8] FIG. 8 is a block diagram showing the configuration of the backup device 500.

[FIG. 9] FIG. 9 shows an example of information stored in the content storage unit 510.

[FIG. 10] FIG. 10 is an example of information stored in the secure information storage unit 511.

[FIG. 11] FIG. 11 shows the details in a backup management table 521.

[FIG. 12] FIG. 12 is a flowchart showing operations performed by the HD recorder 100.

[FIG. 13] FIG. 13 is a flowchart showing the recording process performed by the HD recorder 100.

[FIG. 14] FIG. 14 is a flowchart showing the recording process performed by the HD recorder 100. This is a continuation of FIG. 13.

[FIG. 15] FIG. 15 is a flowchart showing the content playback process.

[FIG. 16] FIG. 16 is a flowchart showing the restore process performed by the HD recorder 100 and the backup device 500.

[FIG. 17] FIG. 17 is a flowchart showing the restore process performed by the HD recorder 100 and the backup device 500. This is a continuation of FIG. 16.

[FIG. 18] FIG. 18 is a flowchart showing the backup process performed by the HD recorder 100 and the backup device 500.

[FIG. 19] FIG. 19 is a flowchart showing the backup process performed by the HD recorder 100 and the backup device 500. This is a continuation of FIG. 18.

[FIG. 20] FIG. 20 is a flowchart showing the backup process performed by the HD recorder 100 and the backup device 500. This is a continuation of FIG. 18.

[FIG. 21] FIG. 21 is a flowchart showing the expiration time extension process performed by the HD recorder 100 and the backup device 500.

[FIG. 22] FIG. 22 is a flowchart showing the expiration time extension process performed by the HD recorder 100 and the backup device 500. This is a continuation of FIG. 21.

[FIG. 23] FIG. 23 is a flowchart showing the expiration time extension process performed by the HD recorder 100 and the backup device 500. This is a continuation of FIG. 21.

[FIG. 24] FIG. 24 is a flowchart showing the device authentication process performed by the HD recorder 100 and the backup device 500.

[FIG. 25] FIG. 25 is a flowchart showing the device authentication process performed by the HD recorder 100 and the backup device 500. This is a continuation of FIG. 24.

Reference Numbers

[0056]

1: Backup system
10: Broadcast device
100: HD recorder
101: Transmission/reception unit
102: Authentication unit
103: Input unit
104: Playback control unit
105: Decoding unit
106: Key generating unit
107: Control unit
108: Unique information storage unit
109: Encryption processing unit
110: Information storage unit
112: Input/output unit
113: Secure storage unit
114: Broadcast receiving unit
120: Monitor
400: HD recorder
500: Backup device
501: Transmission/reception unit
502: Authentication unit
503: Power supply unit
504: Unique information storage unit
507: Control unit
509: Encryption processing unit
510: Content storage unit
511: Secure information storage unit
512: Input unit
513: Display unit

Best Mode for Carrying Out the Invention

[0057] 1. First Embodiment

The backup system 1 in the first embodiment of the present invention will now be described with reference to the drawings.

1.1 Summary of the Backup System 1

The backup system 1 of the present invention comprises a hard disc recorder (HD recorder below) 100, an HD recorder 400, and a backup device 500, as shown in Figure 1. The HD recorder 100, HD recorder 400, and backup device 500 are connected to a LAN (Local Area Network) 30.

[0058] The HD recorder 100 receives broadcast signals transmitted from the broadcasting device 10, acquires video and audio content, and stores the acquired content. The HD recorder 100 can be used as an external recording medium such as a DVD and can acquire content from the external recording media. The HD recorder 100 transmits the stored content to the backup device 500 based on a user operation and sets an expiration time for the stored content itself.

[0059] The backup device 500 receives content from the HD recorder 100 and stores the received content. When the expiration time approaches, the HD recorder 100 requests the backup device 500 to extend the expiration time. The backup device 500 receives a request for extension of the expiration time of content from the HD recorder 100, confirms that the content corresponding to the received request is stored normally, and grants permission for extension of the expiration time to the HD recorder 100.

[0060] When the extension is permitted by the backup device 500, the HD recorder 100 extends its own stored expiration time. If an extension is not permitted, or if communication with the backup device 500 is not possible, for example, due to a malfunction of the LAN 30, the HD recorder 100 deletes content whose expiration time has expired. After deletion, depending on the user operation performed, the HD recorder 100 retrieves the backed-up content from backup device 500 and resets the expiration time.

[0061] The HD recorder 100 can also acquire content sent by the HD recorder 400 to the backup device 500, not just content sent by the HD recorder 100 itself to the backup device 500. The HD recorder 400, like the HD recorder 100, receives, stores, and plays back content including broadcast programs, and transmits the received content to the backup device 500.

1.2 HD Recorder 100 and HD Recorder 400

The HD recorder 100, as shown in Figure 2, comprises a transmission/reception unit 101, an authentication unit 102, an input unit 103, a playback control unit 104, a decoding unit 105, a key generating unit 106, a control unit 107, a unique information storage unit 108, an encryption processing unit 109, an information storage unit 110, an input/output unit 112, a secure storage unit 113, a broadcast receiving unit 114, and an antenna 130.

[0062] The HD recorder 100 is a computer system comprising, specifically, a microprocessor, RAM, and ROM, with computer programs stored in the RAM and ROM. The HD recorder 100 realizes some of its functions from the microprocessor operating in accordance with a computer program. Note that the configuration and operation of the HD Recorder 400 are the same as those of the HD Recorder 100, so further explanation has been omitted.

(1) Unique information storage unit 108

The unique information storage unit 108 is composed of ROM and stores device identifier 115 "ID_A" and device-specific key 116 "Keypad." The unique information storage unit 108 is also equipped with a protection mechanism that protects it from access by external devices.

[0063] Device identifier 115 "ID_A" is information that uniquely identifies the HD recorder 100. Device-specific key 116 "Key_A" is key information specific to HD recorder 100. These are written to the unique information storage unit 108 when the HD recorder 100 is shipped.

(2) Information storage unit 110

The information storage unit 110 is composed of a hard disc unit and, in one example, contains a backup history table 131, and content files 134, 139, etc., as shown in FIG. 3. Each content file includes a content ID, encrypted content, and an encryption key. The content ID is identification information that

uniquely identifies the encrypted content. The encrypted content is obtained from the broadcast device 10 or external recording media using a content key. The content is generated by applying an encryption algorithm E1 to the content. Here, the content is composed of image data and audio data compressed using a compression method such as MPEG2.

[0064] The encrypted content key is generated by applying encryption algorithm E1 to the content key used for encrypting the content, using the device-specific key 116 "Key_A" stored in the unique information storage unit 108. Content keys and content have a one-to-one correspondence. The encryption algorithm E1 in one example is DES (Data Encryption Standard).

[0065] For example, content file 134 includes content ID 136 "A001," encrypted content 137, and encrypted content key 138 "Enc(Key_A,Key_1a)." Here, content ID 136 "A001" is identification information indicating encrypted content 137. Encrypted content 137 is generated by applying encryption algorithm E1 to content including video using content key "Key_1a." Encrypted content key 138 "Enc(Key_A,Key_1a)" is generated by applying encryption algorithm E1 to content key "Key_1a" using device-specific key 116 "Key_A" stored in unique information storage unit 108. Content key "Key_1a" corresponds one-to-one with the content that forms the basis of encrypted content 137.

[0066] The backup history table 131 contains the date and time when HD recorder 100 performed backup to the backup device 500, and the content IDs of each content file stored in the information storage unit 110 at that time. It also stores image data such as menu screens and initial settings screens.

(3) Secure storage unit 113

The secure storage unit 113 is configured to include flash memory and is protected from access by external devices.

[0067] The secure storage unit 113, for example, has the content management table 121 shown in FIG. 4. The content management table 121 includes content information 122, 123, 124, etc., as shown in FIG. 4. Each piece of content information management information consists of a content ID, title, recording date and time, hash value, type, compression method, expiration time, backup flag, and priority level, and corresponds in a one-to-one manner with the content files stored in the information storage unit 110.

[0068] A content ID is information that identifies encrypted content contained in the corresponding content file, and is the same as the content ID contained in the corresponding content file. The title is a name that indicates the corresponding encrypted content, and is not written when the content on which the encrypted content is based is acquired from the broadcast device 10 or the external recording medium.

[0069] The recording date and time indicate the date and time when the content that is the source of the encrypted content included in the corresponding content file was obtained from the broadcast device 10 or the recording medium. Type is information that indicates the acquisition source of the content. Examples include "broadcast program," which indicates that the content was received from a broadcast device 10, and "photo," which indicates that the content is image data captured by a digital camera or similar device. The compression method refers to the name of the compression method used to compress the video and audio that make up the content.

[0070] A hash value is generated by combining the encrypted content contained in the corresponding content file with the encrypted content key and assigning it into a hash function. The hash function used here is SHA-1, for example. The expiration time indicates the date and time when the corresponding encrypted content can no longer be used in the HD recorder 100.

[0071] The backup flag is a flag that indicates whether the corresponding encrypted content has been backed up to the backup device 500, and has a value of "1" or "0." Here, "1" indicates that a backup has been made, and "0" indicates that no backup has been made. The priority level is information that indicates the priority level for content storage, and takes a value of "1" or "2." When writing new encrypted content to the information storage unit 110, if there is insufficient free space in the information storage unit 110, the control unit 107 deletes content files corresponding to content

information with priority level "2" to secure storage space. Even if the free space in the information storage unit 110 is insufficient, content files corresponding to content information with priority level "1" are not deleted. Priority level is automatically set to "1" when content is acquired, but can be changed by a user operation.

[0072] Content information 122, for example, corresponds to content file 134 stored in information storage unit 110. Content ID 151 "A001" is identification information indicating encrypted content 137, and is the same as content ID 136 "A001." The title 152 "Tabloid Show" is the name entered by the user for encrypted content 137. The recording date and time 153 "04.10.10.17:00" indicates that the content was encrypted and generated from encrypted content 137 obtained at 17:00 on October 10, 2004. Hash value 154 "01a" is generated by assigning the combination of encrypted content 137 and encrypted content key 138 "Enc(Key_A,Key_1a)" into a hash function. The expiration time 157 "04.12.15.17" indicates that the corresponding encrypted content 137 can be decrypted and played back on the HD recorder 100 until 17:00 on December 15, 2004.

(4) Antenna 130, broadcast receiving unit 114, decoding unit 105

The antenna 130 receives broadcast signals transmitted from broadcast device 10.

[0073] The broadcast receiving unit 114 is equipped with a tuner, a modem unit, a transport decoder, etc., and selects one broadcast from the broadcast signals received by the antenna 130, converts the selected broadcast signals into digital signals, and generates TS (transport stream) packets. Successively generated TS packets are outputted to the decoding unit 105 in the order in which they were generated. In addition, a recording instruction is received from the control unit 107 indicating that the currently received content is to be recorded. When a recording instruction is received, the generated TS packets are outputted to the control unit 107 in the order in which they were generated. The output of TS packets is continued until an end notification is received from the control unit 107.

[0074] Here, the content acquired by the HD recorder 100 from broadcast device 10 is composed of multiple TS packets. In the following explanation, unless necessary, TS packets that compose the content will not be mentioned and will simply be referred to as "content." The decoding unit 105, in response to instructions from the control unit 107, decompresses the content acquired by the broadcast reception unit 114 and the content generated by the encryption processing unit 109 (described later) using the compression method of each content, such as MPEG (Moving Picture Experts Group) 2 or JPEG (Joint Photographic Experts Group) to generate image data and audio data, and the generated image data and audio data are outputted to the playback control unit 104.

[0075] MPEG2 and JPEG are well-known techniques, so further explanation has been omitted.

(5) Transmission/reception unit 101

The transmission/reception unit 101 is connected to the LAN 30 and transmits and receives information between the control unit 107, the authentication unit 102, and external devices. Here, external device refers to the backup device 500.

(6) Authentication unit 102

The authentication unit 102 stores, in advance, a secret key SK_A unique to the HD recorder 100, a public key certificate Cert_A, a public key PK_CA of the certifying authority, and a CRL (Certificate Revocation List). The public key certificate Cert_A certifies the validity of the public key PK_A corresponding to the private key SK_A, and consists of a certificate identification number, the public key PK_A, and the signature data of the certifying authority. The signature data of the certifying authority is generated by applying a signature generating algorithm S to the public key PK_A using a private key SK_CA of the certifying authority. The signature generating algorithm S can be, for example, an Elgamal signature over a finite field. Elgamal signatures are well known, so further explanation has not been provided here.

[0076] Here, the certifying authority is an impartial third-party organization that issues public key certificates for each device that constitutes the backup system 1 in the first embodiment. CRL contains

the certificate identification numbers of invalid public key certificates. The public key PK_CA of the certifying authority is a public key that corresponds to the private key SK_CA of the certifying authority. The authentication unit 102 performs device authentication in accordance with DTCP (Digital Transmission Content Protection) between external devices and the control unit 107 based on instructions from the control unit 107. If authentication fails, communication between the control unit 107 and external devices is prohibited. If authentication is successful, a common session key is generated between the external device and the control unit 107, and the generated session key is outputted to the control unit 107. The device authentication operation will be explained later in greater detail.

(7) Input unit 103

The input unit 103 includes buttons such as a power button, a recording button, a menu button, and a selection button, as well as a remote controller receiving circuit.

[0077] Button operations and remote controller operations performed by the user are received, and operation instruction information indicating the received button operations and remote controller operations are outputted to the control unit 107.

(8) Key generating unit 106 and encryption processing unit 109

The key generating unit 106 receives a content key generating instruction from the control unit 107. When a content key generating instruction is received, a pseudo-random number is generated, and a 56-bit content key is generated using the generated pseudo-random number. The generated content key is outputted to the control unit 107. Any method may be used to generate the content key.

[0078] The encryption processing unit 109 receives plaintext information and a key from the control unit 107 and is instructed to perform encryption. It also receives ciphertext and a key from the control unit 107 and is instructed to perform decryption. When instructed to perform encryption, the received plain text is encrypted using the received key and encryption algorithm E1 to generate ciphertext, which is then outputted to the control unit 107. When instructed to perform decryption, the received ciphertext is decrypted using the received key by applying decryption algorithm D1 to generate decrypted text, and the generated decrypted text is outputted to the control unit 107.

[0079] The combination of plaintext and key received by the encryption processing unit 109 can be, for example, content and a content key, or a content key and a device-specific key "Key_A." In addition, the combination of the ciphertext and key received by the encryption processing unit 109 can be encrypted content and a content key, or an encrypted content key and a device-specific key "Key_A." The decryption algorithm D1 is an algorithm that decrypts ciphertext generated by an encryption algorithm E1.

(9) Control unit 107

The control unit 107 comprises a secure clock 117, a main control unit 118, and an expiration time management unit 119, as shown in FIG. 5.

[0080] (a) Secure clock 117

The secure clock 117 is a clock that measures the passage of time and keeps the current time. The current time includes the date, day of the week, and time. The secure clock 117 is also equipped with a protection mechanism that protects it from external manipulation.

[0081] (b) Expiration time management unit 119

The expiration time management unit 119 stores the extension execution time "24 hours" in advance. The extended execution time of "24 hours" is the criterion for determining whether to request an extension of the expiration time of encrypted content stored in the HD Recorder 100. Here, the expiration time management unit 119 requests an extension of the expiration time to the backup device 500 if the time remaining until expiration is less than "24 hours."

[0082] The expiration time management unit 119 receives an expiration time extension instruction from the main control unit 118 to extend the expiration time of each content. It also receives a deletion instruction indicating the deletion of expired content.

(b-1) Expiration time extension processing

Upon receiving an expiration time extension instruction, the expiration time management unit 119 selects content information constituting content management table 121 stored in the secure storage unit 113 one by one in order and performs the following processing on the selected content information.

[0083] The expiration time management unit 119 reads the expiration time from the selected content information. Here, if no expiration time is written in the selected content information, processing moves on to the next piece of content information. After reading the expiration time, the expiration time management unit 119 obtains the current time from the secure clock. The difference between the expiration time read and the current time is calculated. Here, calculated difference is called the remaining time.

[0084] If the calculated remaining time is equal to or greater than the extension execution time of "24 hours," the expiration time management unit 119 terminates processing of the selected content information and moves on to processing the next piece of content information. If the calculated remaining time is less than the update execution time of "24 hours," the expiration time management unit 119 sends a start instruction instructing the backup device 500 to start up via the transmission/reception unit 101. Next, the expiration time management unit 119 receives a startup notification indicating that the backup device 500 has started up. Here, if a startup notification is not received within a specified time, the processing of the selected content information is terminated, and processing of the next content information is started.

[0085] When the startup notification is received, the expiration time management unit 119 instructs the authentication unit 102 to perform device authentication with the backup device 500. When device authentication by authentication unit 102 is successful, the session key generated during device authentication is received from the authentication unit 102. In the following processing, the expiration time management unit 119 encrypts and decrypts information sent and received to and from the backup device 500 using the session key to perform confidential communication. However, for the sake of simplicity, explanation of these encryption and decryption processes has been omitted.

[0086] If device authentication by the authentication unit 102 fails, processing of the selected content information is terminated, and processing of the next piece of content information is started. When the authentication unit 102 receives the session key, the expiration time management unit 119 reads the content ID included in the selected content information, reads the device identifier 115 "ID_A" from the unique information storage unit 108, and sends the read out content ID, device identifier, and extension request for extending the expiration to the backup device 500 via the transmission/reception unit 101.

[0087] Next, the expiration time management unit 119 receives an error notification indicating that it cannot accept a new expiration time or extension request from the backup device 500 via the transmission/reception unit 101. When an error notification is received, the expiration time management unit 119 terminates processing of the selected content information and moves on to processing the next piece of content information. When a new expiration time is received, the expiration time management unit 119 updates the expiration time contained in the selected content information based on the received expiration time and moves on to processing the next piece of content information.

[0088] When this processing has been completed for all content information, an extension end notification indicating the extension of the expiration time has ended is outputted to the main control unit 118.

(b-2) Deletion process

When the expiration time management unit 119 receives a deletion instruction from the main control unit 118, it selects content information constituting the content management table 121 stored in the

secure storage unit 113 one by one in sequential order, and performs the following processing on the selected content information.

[0089] The expiration time management unit 119 reads the expiration time from the selected content information. Here, if no expiration time is written in the selected content information, processing moves on to the next piece of content information. After reading the expiration time, the expiration time management unit 119 obtains the current time from the secure clock 117. The read out expiration time is compared with the current time, and if the current time is earlier than the expiration time, the unit proceeds to processing of the next piece of content information.

[0090] If the current time is later than the expiration time, the expiration time management unit 119 reads the content ID included in the selected content information and deletes the content file containing the content ID that matches the read out content ID from the information storage unit 110. Next, the selected content information is deleted, and processing moves on to the next piece of content information. When this processing has been completed for all content information, a deletion completion notification indicating that deletion of expired content has been completed is outputted to the main control unit 118.

[0091] (c) Main control unit 118

The main control unit 118 stores the extension time for extending the expiration time of the encrypted content stored in advance in the information storage unit 110. Here, the extension time "2 hours 00 minutes" is stored. In addition, a time interval of "30 minutes" for deleting expired content is stored. These settings are configured when the HD recorder 100 is shipped.

[0092] The main control unit 118 receives operation instruction information from the input unit 103 and controls various processes in accordance with the received operation instruction information. Specifically, when operation instruction information is received indicating that the recording button has been pressed, control of the recording process described in (c1) below is performed. When the main control unit 118 receives operation instruction information indicating that the menu button has been pressed, a menu screen 181 is generated based on image data stored in the information storage unit 110, the generated menu screen 181 is outputted to the playback control unit 104, and an instruction is given to display the menu screen 181. FIG. 6 (a) shows an example of the menu screen 181 displayed here. The menu screen 181 includes a playlist display button 182, a restore button 183, a timer reservation button 184, a track list display button 185, a content list button 186, a dubbing settings button 187, an initial settings button 188, and a content management button 189. The user selects a button by moving the cursor to that button using the direction keys and pressing the select button.

[0093] When the operation instruction information indicating the selection of the playback list display button 182 is received, the main control unit 118 controls performance of the playback process described in (c2) below. When operation instruction information indicating selection of the initial settings button 188 is received, the initial setting process described in (c3) below is performed. When operation instruction information is received indicating the selection of restore button 183, the restore process described in (c-4) below is executed.

[0094] When operation instruction information is received indicating the selection of other buttons, the main control unit 118 performs various processes such as accepting timer reservations, displaying program tables, and inputting/outputting information from external recording media, depending on the selected button. In addition, the main control unit 118 periodically monitors the secure clock 117, and when it determines that the time indicated by the secure clock 117 is the extended time of "2 hours 00 minutes," it outputs an expiration time extension instruction to the expiration time management unit 119.

[0095] In addition, the main control unit 118 keeps time using the secure clock 117 and outputs a deletion instruction indicating deletion of expired content to the expiration time management unit 119 every 30 minutes. The following is an explanation of the main control unit 118 performing (c-1) recording processing controls, (c-2) playback processing controls, (c-3) initial setting processing, (c-4) restore processing, and (c-5) backup processing.

[0096] (c-1) Recording processing controls

When the main control unit 118 receives from the input unit 103 operation instruction information indicating that the recording button has been pressed, the main control unit generates a new content ID and adds content information including the generated content ID to the content management table 121 stored in the secure storage unit 113. At this point, the current time is written as the recording date and time of the added content information, "broadcast program" is written as the type, "MPEG2" is written as the compression method, "0" is selected as the backup flag, and "1" is selected as the priority level.

[0097] Next, the main control unit 118 outputs a content key generating instruction to the key generating unit 106 and receives a content key from the key generating unit 106. When the content key is received, the main control unit 118 generates a new content file in the information storage unit 110. Next, the main control unit 118 outputs a recording instruction to the broadcast receiving unit 114 and receives content from the broadcast receiving unit 114. The received content key and content are outputted to the encryption processing unit 109, which is instructed to encrypt the content. The encrypted content is received from the encryption processing unit 109. The main control unit 118 writes the received encrypted content to the newly generated content file in the information storage unit 110.

[0098] As already mentioned, the content outputted from the broadcast receiving unit 114 consists of multiple TS packets, and the main control unit 118 receives the content in TS packet units, issues an encryption instruction, and writes the encrypted content repeatedly until it receives operation instruction information indicating that the stop button has been pressed. In parallel with this repeated operation, the main control unit 118 monitors the free capacity of the information storage unit 110. If it is determined that there is insufficient free space, content information with a priority level of "2" is selected from the content information that constitutes the content management table 121, the content information corresponding to the selected content information is deleted from the information storage unit 110, and the selected content information is deleted from the content management table 121.

[0099] If there is no content with a priority level of "2" in the content information that constitutes content management table 121, that is, if there is no content that can be deleted in information storage unit 110, the main control unit 118 notifies the user, for example, with a flashing light, that the storage capacity is insufficient and that recording will be stopped. When the memory capacity of the information storage unit 110 is insufficient and recording is interrupted, or when the main control unit 118 receives an operation instruction indicating that the stop button has been pressed on the input unit 103, the main control unit 118 outputs an end notification indicating the end of recording to the broadcast receiving unit 114.

[0100] Next, the main control unit 118 reads the device-specific key 116 "Key_A" from the unique information storage unit 108, outputs the read out device-specific key 116 "Key_A" and the content key to the encryption processing unit 109, and gives an instruction to encrypt the content key. An encrypted content key is received from the encryption processing unit 109, and the received encrypted content key and the generated content ID are written to the generated content file.

[0101] Next, the main control unit 118 reads the encrypted content and the encrypted content key from the generated content file, combines the read out encrypted content and the encrypted content key, assigns them into the hash function, and generates a 160-bit hash value. The calculated hash value is written to the added content information.

(c-2) Playback processing controls

When the playlist display button 182 is selected by a user button operation, the main control unit 118 generates a playlist screen 211 using the image data stored in the information storage unit 110 and the titles and recording dates and times of each piece of content information constituting the content management table 121, and outputs the display of the generated playlist screen 211 to the playback control unit 104. The playlist screen 211 shown in FIG. 6 (b) is the playlist screen 211 displayed here.

[0102] The playback list screen 211 includes content buttons 212, 213, 214, and 215, and each content button corresponds to content information 122, 123, 124, and 125 that constitutes the content

management table 121. Next, the content button selected by the user is accepted. When the user selects one of the content buttons, the main control unit 118 reads the content ID corresponding to the selected content button from the secure storage unit 113. In information storage unit 110, a content file containing a content ID that matches the read content ID is detected. The encrypted content and encryption key is read from the detected content file, and the read out encrypted content and encryption key are combined and assigned to the hash function to calculate a hash value.

[0103] The main control unit 118 reads the hash value included in the content information corresponding to the selected content button, compares the read hash value with the calculated hash value, and if they do not match, generates an error screen indicating that the selected content cannot be played. The main control unit 118 outputs the generated error screen to the playback control unit 104, gives an instruction to display the error screen, and stops playback of the content.

[0104] If the read hash value and the calculated hash value match, the main control unit 118 reads the device-specific key 116 "Key_A" from the device-unique information storage unit 108, outputs the read device-specific key 116 "Key_A" and the read out encrypted content key to the encryption processing unit 109, and gives an instruction to decrypt the encrypted content key. Next, the main control unit 118 receives the content key from the encryption processing unit 109. When the content key is received, the encrypted content is read from the detected content file, the read out encrypted content and the received content key are outputted to the encryption processing unit 109, an instruction is given to decrypt the encrypted content. Next, the main control unit 118 receives the content from the cryptographic processing unit 109 and outputs the received content to the decoding unit 105.

(c-3) Initial setting processing

When the menu screen 181 shown in FIG. 6 (a) is displayed on the monitor 120, and operation instruction information is received indicating the selection of the initial setting button 188, the main control unit 118 generates the initial setting screen 191 and instructs the playback control unit 104 to display the generated initial setting screen 191. FIG. 7 (a) shows the initial setup screen 191 displayed here. The initial setup screen 191 includes settings 192, 193, 194, and 196. When the user selects a setting, the corresponding setting box is displayed. FIG. 7 (a) shows setting boxes 197 to 201 corresponding to setting 196 "Backup."

[0105] The main control unit 118 receives input operations performed by the user in setting boxes 197 to 201. Here, "All" is entered in setting box 197 to indicate that all content, regardless of type, is to be backed up. In setting box 198, "Sunday 0:30" is entered as the schedule for sending encrypted content to the backup device 500 for backup purposes.

[0106] Setting box 199 contains "New only," which indicates that only new encrypted content that has not been backed up from the encrypted content stored in information storage unit 110 is to be backed up. Setting box 201 contains "Manual" indicating that the restoration of content backed up to the backup device 500 is to be started by a user operation. In the following explanation, the HD recorder 100 acquiring encrypted content backed up in the backup device 500 is referred to as "restoring."

[0107] Next, the main control unit 118 receives operation instruction information indicating that the select button has been pressed on the input unit 103 and stores the settings entered in each setting box. Also, although not depicted in detail, when the user places the cursor over buttons 192 to 194, the device accepts input for settings related to the channel, image quality, and disc, and stores the inputted settings when the select button is pressed.

(c-4) Restore processing

When the menu screen 181 shown in FIG. 6 (a) is displayed on the monitor 120 and operation instruction information indicating selection of the restore button 183 is received, the main control unit 118 sends a startup instruction to the backup device 500 via the transmission/reception unit 101.

[0108] If, within the specified time, the main control unit 118 does not receive startup notification indicating normal startup from the backup device 500 via the transmission/reception unit 101, the main control unit 118 generates an error screen notifying the user that restoration is not possible due to a

communication failure with the backup device 500. The generated error screen is displayed on the monitor 120 via the playback control unit 104, and subsequent processing is stopped.

[0109] If, within a specified time, the main control unit 118 receives startup notification from the backup device 500 via the transmission/reception unit 101, the main control unit 118 instructs the authentication unit 102 to perform device authentication with the backup device 500. If device authentication by the authentication unit 102 fails, the main control unit 118 generates an error screen notifying the user that restoration is not possible due to failure to communicate with backup device 500, displays the generated error screen on the monitor 120 via the playback control unit 104, and stops subsequent processing.

[0110] If device authentication is successful, the main control unit 118 receives a session key from the authentication unit 102. The main control unit 118 performs confidential communication using a common key encryption method with the session key received during the exchange of information with the backup device 500. For the sake of brevity, the following explanation omits details regarding encryption and decryption of confidential communication. The main control unit 118 reads the device identifier 115 "ID_A" from the unique information storage unit 108, sends a restore information request containing information on restorable encrypted content, and sends the read out device identifier 115 "ID_A" to the backup device 500 via the transmission/reception unit 101.

[0111] Next, the main control unit 118 receives, via the transmission/reception unit 101, the content ID, title, and recording date and time corresponding to each piece of encrypted content stored in the backup device 500 from the backup device 500. The received content ID, title, and recording date and time are temporarily stored, and the image data stored in the information storage unit 110 is used together with the received title and recording date and time to generate the restore information screen 221 shown in FIG. 7 (b), which is displayed on the monitor 120 via the playback control unit 104.

[0112] The restore information screen 221 displays content buttons 222 to 225. The main control unit 118 receives operation instruction information indicating the selection of one of the content buttons from the input unit 103 and reads out the content ID corresponding to the received operation instruction information. Next, the main control unit 118 sends the read out content ID and a restore request for the encrypted content indicated by the content ID to the backup device 500 via the transmission/reception unit 101.

[0113] Next, the encrypted content, a content key, and an expiration time are received from the backup device 500 via the transmission/reception unit 101. A new content file is generated by the information storage unit 110, and the content button selected by the user, the corresponding content ID, and the received encrypted content are written to the generated content file. Next, the main control unit 118 reads the device-specific key 116 "Key_A" from the secure storage unit 113, outputs the read device-specific key 116 "Key_A" and the received content key to the encryption processing unit 109, and issues an instruction for content key encryption. When the encryption processing unit 109 receives the encrypted content key, it writes the received encrypted content key to the newly generated content file.

[0114] Next, the main control unit 118 reads the encrypted content and the encrypted content key from the newly generated content file in the information storage unit 110, combines the read out encrypted content and the encrypted content key, assigns them into the hash function, and calculates a hash value. When the hash value is calculated, the main control unit 118 generates a content report containing the content ID corresponding to the content button selected by the user, the title, the recording date and time, the expiration time, and the calculated hash value, and adds the generated content report to the content management table 121. At this point, backup flag "1" and priority level "2" are written to the added content information, and the restore process is ended.

[0115] During any of this processing, when an error notification indicating that restoration is not possible is received from the backup device 500, an error screen indicating that restoration has failed is generated, and the generated error screen is displayed on the monitor 120 via the playback control unit 104. Here, the user performs an operation to select the content to be restored, and the selected content is retrieved from the backup device 500. However, the state of the information storage unit 110 may be restored to the state just prior to performing the backup using the backup history table 131. In this case, the main control unit 118 reads the dates on which a backup was performed from the backup history table 131

and displays the read out dates on the monitor 120. The user selects one of the displayed dates. The main control unit 118 reads the content ID stored in the backup history table 131 corresponding to the selected date. Content IDs that are not included in content management table 121 are extracted from the read out content IDs, the extracted content IDs are sent to the backup device 500, and a request for the encrypted content corresponding to the transmitted content IDs is transmitted.

(c-5) Backup processing

The main control unit 118 stores settings related to backup operations performed by the user. Storage of the settings entered in the initial setting screen 191 described above will be explained.

[0116] The main control unit 118 periodically monitors the time, and when it determines that the current time is "Sunday 0:30," it selects one piece of content information at a time in the order specified in the content management table 121 stored in the secure storage unit 113, and performs the following processing on the selected content information. The backup flag contained in the selected content information is read. If the read out backup flag is "0," the unit proceeds to processing the next content information.

[0117] If the value is not "0," the main control unit 118 detects the content file corresponding to the selected content information in the information storage unit 110 based on the content ID included in the selected content information. The encrypted content and the encrypted content key contained in the detected content file are read from the information storage unit 110, the read out encrypted content and the encrypted content key are combined and assigned to the hash function, and a hash value is calculated. The calculated hash value is compared with the hash value contained in the selected content information. If they do not match, the unit processes the next piece of content information.

[0118] If they match, the main control unit 118 sends a start instruction to the backup device 500 via the transmission/reception unit 101. If the startup notification is not received from the backup device 500 via the transmission/reception unit 101 within the specified time, the main control unit 118 stops the subsequent processing. When a startup notification is received via the transmission/reception unit 101 within the specified time, the main control unit 118 instructs the authentication unit 102 to perform device authentication with the backup device 500. If device authentication by the authentication unit 102 fails, the main control unit 118 stops subsequent processing.

[0119] If device authentication by the authentication unit 102 is successful, the main control unit 118 receives a session key from the authentication unit 102. The main control unit 118 performs confidential communication using a common key encryption method with the session key received during the exchange of information with the backup device 500. For the sake of brevity, the following explanation omits details regarding encryption and decryption of confidential communication.

[0120] The main control unit 118 reads the device-specific key 116 "Key_A" from the device-unique information storage unit 108, outputs the read device-specific key 116 "Key_A" and the encrypted content key read out from the information storage unit 110 to the encryption processing unit 109, and gives an instruction to decrypt the encrypted content key. The main control unit 118 receives the content key from the encryption processing unit 109. When the content key is received, the encrypted content contained in the detected content file is read out, the device identifier 115 "ID_A" is read out from the unique information storage unit 108, and the content ID, title, and recording date and time contained in the selected content information are read out from the secure storage unit 113. Next, the main control unit 118 sends a backup request indicating a backup, and the read out device identifier 115 "ID_A," content ID, title, recording date and time, content key, and encrypted content to the backup device 500 via the transmission/reception unit 101.

[0121] Next, the main control unit 118 receives an error notification indicating that the backup request cannot be accepted or an expiration time from the backup device 500 via the transmission/reception unit 101. When an error notification is received, the main control unit 118 stops subsequent processing. When an expiration time is received, the main control unit 118 writes the received expiration time to the selected content information and changes the backup flag to "1." Next, a priority level of "2" is written and the unit processes the next piece of content information.

[0122] When all of this processing has been completed for all content information, the main control unit 118 reads the content ID from each piece of content information included in the content management table 121, and writes the read out content IDs and the current date to the backup history table 131. Note that when the backup button provided on the input unit 103 is pressed by the user, the main control unit 118 starts the backup processing regardless of the backup schedule set in the initial setting process.

(10) Playback control unit 104 and monitor 120

The playback control unit 104 comprises a video signal processing unit and an audio signal processing unit. The playback control unit 104 receives video data and audio data from the decoding unit 105. The image signal processing unit generates video signals from the received video data. Vertical synchronization signals, horizontal synchronization signals, and generated video signals are outputted to the monitor 120. Also, video signals are generated from screen data and outputted to the monitor 120 based on instructions from the control unit 107.

[0123] The audio signal processing unit generates analog audio signals from the received audio data and outputs the generated analog audio signals to the monitor 120. The monitor 120 has a built-in speaker, receives horizontal synchronization signals, vertical synchronization signals, and video signals from the video signal processing unit, and displays video based on the received horizontal synchronization signals, vertical synchronization signals, and video signals. In addition, the speaker receives analog audio signals from the audio signal processing unit, converts the received analog audio signals into audio, and outputs them.

(11) Input/output unit 112

The input/output unit 112 can be, for example, equipped with a recording medium such as a DVD or memory card. The control unit 107 reads information recorded on the recording medium and writes information to the recording medium.

1.3 Backup device 500

The backup device 500 comprises a transmission/reception unit 501, an authentication unit 502, a power supply unit 503, a control unit 507, an encryption processing unit 509, a unique information storage unit 504, a content storage unit 510, a secure information storage unit 511, an input unit 512, and a display unit 513, as shown in FIG. 8.

[0124] The backup device 500 is a computer system specifically comprising a microprocessor, RAM, and ROM. The RAM and ROM store computer programs, and the microprocessor operates in accordance with the computer programs, thereby enabling the backup device 500 to perform some of its functions.

(1) Unique information storage unit 504

The unique information storage unit 504 is composed of ROM and stores the device-specific key 516 "Key_C" as shown in Figure 8. The device-specific key 516 "Key_C" is key data specific to the backup device 500 and is written to the backup device 500 at the time of shipment.

[0125] (2) Content storage unit 510

The content storage unit 510 is composed of a hard disc unit and, in one example, stores content files 529, 534, 539, etc. shown in FIG. 9. Each content file includes a content ID, encrypted content, and an encrypted content key. The content ID is identification information corresponding to the encrypted content. Encrypted content is generated by applying encryption algorithm E1 to content using a content key. The encrypted content key is generated by applying encryption algorithm E1 to the content key used for encrypting the content, using the device-specific key 516 "Key_C" stored in the unique information storage unit 508.

[0126] For example, content file 529 includes content ID 531 "A001," encrypted content 532, and encrypted content key 533 "Enc(Key_C,Key_1a)." Content ID 531 "A001" is information that uniquely

identifies encrypted content 532, which is the same as content ID 136 "A001" stored in the information storage unit 110 of the HD recorder 100. Encrypted content 532 is generated by applying encryption algorithm E1 to content using content key "Key_1a." Encrypted content 532 is the same as encrypted content 137 stored in the information storage unit 110 of the HD recorder 100.

[0127] Encrypted content key 533 "Enc(Key_C,Key_1a)" is generated by applying encryption algorithm E1 to content key "Key_1a" using device-specific key 516 "Key_C" stored in the unique information storage unit 504.

(3) Secure information storage unit 511

The secure information storage unit 511 is configured to include flash memory. The secure information storage unit 511 is also equipped with a protection mechanism to protect it from access from external devices.

[0128] The secure information storage unit 511 stores, for example, the backup management table 521 and the authorization device identification information 551 as shown in FIG. 10. The backup management table 521 is configured to include backup information 522, 523, 524, 525, etc., as shown in FIG. 11. Each backed up piece of information consists of a content ID, title, recording date and time, backup source device identifier, and hash value. Each piece of content information has a one-to-one correspondence with a content file stored in the content storage unit 510.

[0129] The content ID is identical to the content ID contained in the corresponding content file and is identification information that indicates encrypted content. The title is the name of the corresponding encrypted content. The recording date and time are the date and time when the content that is the source of the encrypted content was obtained from HD Recorder 100 or HD Recorder 400, the broadcast device 10, or an external recording medium. The backup source device identifier is the device identifier of the device that requested backup of the encrypted content contained in the corresponding content file. A hash value is generated by combining the encrypted content contained in the corresponding content file with the encrypted content key and assigning it into a hash function.

[0130] Permitted device identification information 551 is configured to include identification information on a device that receives instructions such as backup requests from the backup device 500. In the present embodiment, this includes device identifier 552 "ID_A," indicating the HD recorder 100 forming the backup system 1, and device identifier 553 "ID_B," indicating the HD recorder 400.

(4) Power supply unit 503

The power supply unit 503 obtains power from an external power source and supplies the obtained power to each circuit constituting the backup device 500 in accordance with instructions from the control unit 507.

[0131] Usually, the power supply unit 503 supplies power only to the transmission/reception unit 501 and the control unit 507. The power supply unit 503 receives a power supply start instruction from the control unit 507. When the power supply start instruction is received, the power supply to other units is started. The power supply is also stopped by a stop instruction from the control unit 507. When the power supply is stopped, the power supply to all units other than the transmission/reception unit 501 and the control unit 507 is stopped.

[0132] (5) Transmission/reception unit 501

The transmission/reception unit 501 is connected to the LAN 30 and exchanges information with external devices connected to the LAN 30 as well as the control unit 507 and the authentication unit 502. Here, the external devices are HD recorder 100 and HD recorder 400.

(6) Authentication unit 502

The authentication unit 502 stores in advance a secret key SK_C specific to the backup device 500, a public key certificate Cert_C, a public key PK_CA of the certifying authority, and a CRL. The public key

certificate Cert_C certifies the validity of the public key PK_C corresponding to the private key SK_C, and consists of a certificate identification number, the public key PK_C, and the signature data of the certifying authority. The signature data of the certifying authority is generated by applying a signature generating algorithm S to at least the public key PK_C using the private key SK_CA of the certifying authority.

[0133] The CRL contains the certificate identification numbers of invalid public key certificates. The public key PK_CA of the certifying authority is the public key that corresponds to the private key SK_CA of the certifying authority. The authentication unit 502 performs device authentication in accordance with DTCP between external devices and the control unit 507 based on instructions from the control unit 507. If authentication fails, communication between the control unit 507 and external devices is prohibited. If authentication is successful, a common session key is generated between the external device and the control unit 507, and the generated session key is outputted to the control unit 507. The device authentication operations will be explained in greater detail later.

[0134] (7) Encryption processing unit 509

The encryption processing unit 509 receives plain text and a key from the control unit 507 and is instructed to encrypt the plain text. It also receives cipher text and a key from the control unit 507 and is instructed to decrypt the cipher text. When instructed to perform encryption, the received plain text is encrypted using the received key and encryption algorithm E1 to generate ciphertext, which is then outputted to the control unit 507.

[0135] When instructed to perform decryption, the received ciphertext is decrypted using the received key by applying decryption algorithm D1 to generate decrypted text, and the generated decrypted text is outputted to the control unit 107. The combination of plain text and the key received by the encryption processing unit 509 is, for example, the content key and the device-specific key "Key_C." In addition, the combination of ciphertext and the key received by the encryption processing unit 509 is the encrypted content key and the device-specific key "Key_C."

[0136] (8) Control unit 507

The control unit 507 stores the viewing period "240 hours." The viewing period is the time during which the HD recorder 100 and the HD recorder 400 can use the encrypted content that has been backed up. In addition, the control unit 507 is provided with a secure clock that cannot be operated by external device, although this is not shown in the figure.

[0137] The control unit 507 receives a start-up instruction from an external device via the transmission/reception unit 501. The external device is the HD recorder 100 or the HD recorder 400. Upon receiving the start-up instruction, the unit instructs the power supply unit 503 to start supplying power. Next, a startup notification indicating that the backup device 500 has been started is sent to the external device via the transmission/reception unit 501.

[0138] Next, the control unit 507 instructs the authentication unit 502 to perform device authentication with the external device. If the device authentication performed by the authentication unit 502 fails, the control unit 507 instructs the power supply unit 503 to stop supplying power. If the device authentication performed by the authentication unit 502 succeeds, the control unit 507 receives a session key from the authentication unit 502. In the following processing, the control unit 507 uses the session key received to perform common key encryption with the external device to enable confidential communication, but details of the encryption and decryption for confidential communication are omitted.

[0139] Next, the control unit 507 receives a device identifier, a backup request, a content ID, a content key, a title, a recording date and time, and encrypted content from an external device via the transmission/reception unit 501. Alternatively, it receives a device identifier, an extension request, and a content ID. Alternatively, it receives a device identifier and a restore information request.

(a) Backup processing

When the device identifier, backup request, content ID, content key, title, recording date and time, and encrypted content are received, the control unit 507 confirms that the received device identifier is included in the authorized device identifier information 551 stored in the secure information storage unit 511. If not included, an error notification is sent via the transmission/reception unit 501 to indicate that a backup request cannot be accepted by the external device. Next, an instruction is given to the power supply unit 503 to stop supplying power.

[0140] If the received device identifier is included in the authorized device identifier information 551 stored in the secure information storage unit 511, the device-specific key 516 "Key_C" is read from the device-unique information storage unit 504. The read out device-specific key 516 "Key_C" and the received content key are outputted to the encryption processing unit 509, and an instruction is given to encrypt the content key. Next, the control unit 507 receives the encrypted content key from the encryption processing unit 509, generates a content file containing the received content ID, the encrypted content, and the encrypted content key, and writes the generated content file to the content storage unit 510.

[0141] Next, the control unit 507 reads the encrypted content and the encrypted content key included in the content file written to the content storage unit 510, combines the read out encrypted content and the encrypted content key, and assigns the combined data in a hash function to generate a 160-bit hash value. Next, the control unit 507 generates backup information consisting of the received content ID, title, recording date and time, device identifier, and calculated hash value, and adds the generated backup information to the backup management table 521. Here, the received device identifier is used as the backup source device identifier.

[0142] Next, the control unit 507 acquires the current time from the secure clock, adds the viewing period "240 hours" to the acquired current time, and calculates the expiration time. Next, the calculated expiration time is transmitted to the external device via the transmission/reception unit 501. When transmission is complete, the control unit 507 instructs the power supply unit 503 to stop supplying power.

(b) Expiration time extension processing

When the device identifier, extension request, and content ID are received via the transmission/reception unit 501, the control unit 507 confirms that the received device identifier matches one of the device identifiers included in the authorized device identifier information 551 stored in the secure information storage unit 511. If they do not match, an error notification indicating that an extension request cannot be accepted is sent to the external device via the transmission/reception unit 501. Next, the power supply 503 is instructed to stop supplying power.

[0143] If the received device identifier matches any of the device identifiers included in the authorized device identifier information 551, the control unit 507 selects backup information that includes the same content ID as the received content ID. Next, the control unit 507 detects a content file containing the same content ID as the received content ID from the content storage unit 510, and reads the encrypted content and the encrypted content key included in the detected content file. The decrypted content and the decryption key are combined and assigned in the hash function to calculate a hash value.

[0144] The control unit 507 compares the calculated hash value with the hash value included in the selected backup information, and if they do not match, the control unit 507 outputs an error notification indicating that the extension request cannot be accepted to the external device via the transmission/reception unit 501. If they are the same, the control unit 507 acquires the secure clock time, and adds a viewing period of "240 hours" to the current time to calculate the expiration time. Next, the calculated expiration time is transmitted to the external device via the transmission/reception unit 501.

[0145] (c) Restore processing

Upon receiving the device identifier and a restore information request from the external device, the control unit 507 confirms that the received device identifier is included in the permitted device information 551 stored in the secure information storage unit 511. If it is not included, an error

notification indicating that the restore information request cannot be accepted is sent to the external device via the transmission/reception unit 501. Next, the power supply unit 503 is instructed to stop supplying power.

[0146] If the received device identifier is included in the permitted device identification information 551, the control unit 507 reads all backup information contained in the backup management table 521 stored in the secure information storage unit 511, including the content ID, title, and recording time. The read out content ID, title and recording time are sent to the external device via the transmission/reception unit 501. Next, the control unit 507 receives the content ID and the restore request from the external device via the transmission/reception unit 501. Upon receiving the content ID and the restore request, the control unit 507 selects backup information including the same content ID as the received content ID from the backup management table 521.

[0147] Next, the control unit 507 detects the content file corresponding to the selected backup information based on the received content ID. The encrypted content and the encrypted content key are read from the detected content file. The read out encrypted content and encrypted content key are combined and assigned in a hash function to calculate a hash value. The calculated hash value is compared with the hash value contained in the selected backup information.

[0148] If they do not match, the control unit 507 sends an error notification to the external device via the transmission/reception unit 501, indicating that the restore request cannot be accepted. Next, the power supply unit 503 is instructed to stop supplying power. If they match, the control unit 507 reads the device-specific key 516 "Key_C" from the unique information storage unit 504, and outputs the read out encrypted content key and the device-specific key 516 "Key_C" to the encryption processing unit 509, and gives an instruction to decrypt the encrypted content key. Next, the content key is received from the encryption processing unit 509. Upon receiving the content key, the control unit 507 reads the encrypted content from the detected content file.

[0149] Next, the control unit 507 acquires the current time for the secure clock and calculates the expiration time by adding the viewing period "240 hours" to the acquired current time. The read out encrypted content, the received content key and the calculated expiration time are sent to the external device via the transmission/reception unit 501. When transmission is completed, the control unit 507 instructs the power supply unit 503 to stop supplying power.

[0150] (9) Input unit 512 and display unit 513

The input unit 512 accepts input of information and instructions from the operator and outputs the received information and operation instruction information corresponding to the received instructions to the control unit 507. The display unit 513 displays information under the control of the control unit 507.

1.4 Operation of the Backup System 1

The operation of the backup system 1 is described below.

[0151] (1) Operation of the HD recorder 100

The operation of the HD recorder 100 will now be described using the flowchart shown in FIG. 12. For the sake of brevity, the explanation starts at step S111. The main control unit 118 stores the settings related to backups set by the initial setup screen 191 shown in FIG. 7, namely, content type "All", backup schedule "Sunday 0:30", backup mode "New Only", and restore mode "Manual".

[0152] The control unit 107 of the HD recorder 100 compares the current time indicated by the secure clock 117 with its own stored extended time "2:00" (step S111), and if it determines that the current time is "2:00" (YES in step S111), the expiration time extension process is performed (step S112). If it is determined that the current time is not "2:00" (NO in step S111), step S112 is not performed and the program moves to step S113.

[0153] Next, the control unit 107 compares the current time with the stored backup schedule "Sunday 0:30." If it determines that the current time is "Sunday 0:30" (YES in step S113), it performs backup

processing (step S114). If it is determined that the current time is not "Sunday 0:30" (NO in step S113), the process moves to step S115.

[0154] Next, if the elapsed time since the last expired content deletion process exceeds "30 minutes" (YES in step S115), the control unit 107 again compares the expiration time in each piece of content information in the content management table 121 to the current time, and the content information and corresponding content files whose expiration time has expired are deleted from the information storage unit 110, and the content information is deleted from the content management table 121 (step S116).

[0155] If the elapsed time is less than "30 minutes" (NO in step S115), the control unit 107 does not process step S116 and moves to step S117. Next, when the power button is pressed by the user (YES in step S117), the control unit 107 accepts button operations and remote controller operations performed by the user via the input unit 103 (step S118) and performs the processing based on the received button operations.

[0156] If the power button is not pressed (NO in step S117), the unit returns to step S111 and continues monitoring the current time. When the recording button is pressed in step S118, the control unit 107 executes the recording process (step S122). When the recording process is completed, the system returns to step S118 to receive user operations.

[0157] If the power button is pressed in step S118, the unit returns to step S111 to continue monitoring the time. If another button is pressed in step S118, other processing is performed (step S123). In step S118, upon receiving the pressing of the menu button, the control unit 107 displays the menu screen 181 shown in FIG. 6 (a) on the monitor 120 (step S121) and receives the selection performed by the user (step S124).

[0158] When the initial setting button 188 is selected (step S124), the control unit 107 displays the initial setting screen 191 shown in FIG. 7 (a) on the monitor 120 (step S126) and accepts the settings based on user button operations (step S127). When the settings have been received, the unit returns to Step S118. When the playback list display button 182 is selected in step S124, playback processing is performed (step S129). When the playback process is completed, the unit returns to step S118.

[0159] If the restore button 183 is selected in step S124, the control unit 107 performs the restore process (step S131). When the restore process is completed, the unit returns to step S118. If another button is selected, other processing is performed (step S181) and the unit returns to step S118.

(2) Recording process by the HD recorder 100

The recording processing performed by the HD recorder 100 is described below using the flowchart shown in FIG. 13. This is the details in step S122 of FIG. 12.

[0160] Upon receiving operation instruction information indicating the pressing of the recording button, the control unit 107 generates a new content ID (step S151) and adds the content information including the generated content ID to the content management table 121 (step S153). The current time is written in the recording date and time of the added content information (Step S154), and "broadcast program" is written in the type (Step S156). "MPEG2" is written to the compression method (Step S157), "0" to the backup flag (Step S158), and "1" to the priority level (Step S161).

[0161] Next, the control unit 107 instructs the key generating unit 106 to generate a content key. The key generating unit 106 generates the content key and outputs the generated content key to the control unit 107 (step S162). Next, the control unit 107 generates a new content file in the information storage unit 110 (step S163). Next, recording instructions are outputted to the broadcast receiving unit 114. The broadcasting receiving unit 114 receives content via the antenna 130 (step S164) and outputs the received content in TS packet units to the control unit 107.

[0162] The processing in steps S164 through S168 below is repeated until the stop button is pressed by the user, and when the stop button is pressed (YES in step S166), the process moves to step S171. First, the control unit 107 outputs the content received from the broadcasting receiving unit 114 and the content key received from the key generating unit 106 to the encryption processing unit 109, and

gives an instruction to encrypt the content. The encryption processing unit 109 encrypts the content using the received content key and outputs the generated encrypted content to the control unit 107 (step S167).

[0163] The control unit 107 writes the encrypted content generated by the encryption processing unit 109 to the content file generated in the information storage unit 110 (step S168) and returns to step S164. When the stop button is pressed (YES in step S166), the control unit 107 reads the device-specific key 116 "Key_A" from the unique information storage unit 108 (step S171), outputs the read out device-specific key 116 "Key_A" and the content key to the encryption processing unit 109, and gives an instruction to encrypt the content key. The encryption processing unit 109 encrypts the content key using the received device-specific key 116 "Key_A" to generate an encrypted content key. The generated encrypted content key is outputted to the control unit 107 (step S172).

[0164] The control unit 107 receives the encrypted content key from the encryption processing unit 109 and writes the received encrypted content key and the generated content ID to the content file (Step S173). Next, the control unit 107 combines the encrypted content with the encrypted content key and assigns it to a hash function to calculate a hash value (step S174). The calculated hash value is written to the added content information (step S176).

[0165] In parallel with steps S164 to S168, the control unit 107 executes steps S181 to S189. First, the control unit 107 monitors the free capacity of the information storage unit 110 (step S181). If it is determined that there is sufficient free capacity (YES in step S181) and the stop button is not pressed by the user (NO in step S182), the system returns to step S181 and continues monitoring the free capacity. If the stop button is pressed by the user (YES in step S182), the control unit 107 moves to step S171.

[0166] If it is determined that there is insufficient free space (NO in step S181), the control unit 107 sequentially selects the content information contained in the content management table 121 stored in the secure storage unit 113 from the top (step S184). At this time, if the processing of steps S187 to 189 has been completed for all content information included in the content management table 121, that is, if there is no deletable content in the information storage unit 110 (YES in step S186), the control unit 107 notifies the user with a flashing light, etc. that the storage capacity is insufficient, and moves to step S171.

[0167] If NO in step S186, the control unit 107 reads the priority level included in the selected content information and determines whether or not the read out priority level is "2" (step S187). If the priority level is not "2" (NO in step S187), the unit returns to step S184 to select the next piece of content information. If the priority level is "2" (YES in step S187), the content file corresponding to the selected content information is detected in the information storage unit 110 based on the content ID included in the selected content information, and the detected content file is deleted from the information storage unit 110 (step S188). Next, the selected content information is deleted from the content management table 121 (step S189) and the unit returns to step S181.

[0168] (3) Operation of the HD recorder 100 during playback

The operation of the HD recorder 100 during playback will now be described using the flowchart shown in FIG. 15. This is the details of step S129 in FIG. 12. When the playback list display button 182 on the menu screen 181 shown in FIG. 6 is selected by the user, the control unit 107 generates a playback list screen 211 as shown in FIG. 6 (b) and displays the generated playback list screen 211 on the monitor 120 (step S201).

[0169] Next, content selection by the user is accepted via the input unit 103 (step S202). In the following description, the user selects content button 212. The control unit 107 reads the content ID "A001" contained in the content information 122 corresponding to the selected content button 212 from the secure storage unit 113 (step S203), and the corresponding content file 134 is detected in the information storage unit 110 based on the read out content ID "A001" (step S204). The encrypted content 137 and the encrypted content key 138 "Enc(Key_A,Key_1a)" are read from the detected content file 134 (Step S205). The read out encrypted content 137 and the encrypted content key 138

"Enc(Key_A,Key_1a)" are combined and assigned to a hash function to calculate a hash value (step S206).

[0170] Next, the control unit 107 reads the hash value "01a" from the content information 122 including the content ID "A001" (step S207). The calculated hash value is compared with the read out hash value (step S208), and if they do not match (NO in step S208), an error screen is generated indicating that the selected content cannot be played, the generated error screen is displayed (step S209), and playback processing ends.

[0171] If the calculated hash value matches the read out hash value (YES in step S208), the control unit 107 reads the device-specific key 116 "Key_A" from the unique information storage unit 108, outputs the encrypted content key 138 "Enc(Key_A,Key_1a)" and the read device-specific key 116 "Key_A" to the encryption processing unit 109, and gives an instruction to decrypt the encrypted content key 138 "Enc(Key_A,Key_1a)."

[0172] The encryption processing unit 109 receives the encrypted content key "Enc(Key_A,Key_1a)" and the device-specific key 116 "Key_A" from the control unit 107. Using the received device-specific key 116 "Key_A", the encrypted content key "Enc(Key_A,Key_1a)" is decrypted to generate the content key "Key_1a", and the generated content key "Key_1a" is outputted to the control unit 107 (Step S211).

[0173] The control unit 107 receives the content key "Key_1a" from the encryption processing unit 109. Upon receiving the content key "Key_1a", the encrypted content 137 is read from the content file 134 (step S212), and the read out encrypted content 137 and the content key "Key_1a" are outputted to the encryption processing unit 109, which is instructed to decrypt the encrypted content.

[0174] The encryption processing unit 109 decrypts the encrypted content using the content key "Key_1a" according to the instructions of the control unit 107, generates the content, and outputs the generated content to the control unit 107 (Step S213). The control unit 107 receives content from the encryption processing unit 109 and outputs the received content to the playback control unit 104. The playback control unit 104 receives the content from the control unit 107, decompresses the received content to generate image and audio signals (step S214), and outputs the generated image and audio signals to the monitor 120. The monitor 120 plays back the video and audio (step S216).

[0175] (4) Restore processing performed by the HD recorder 100 and the backup device 500

The flowchart shown in FIG. 16 and FIG. 17 describes the restore processing performed by the HD recorder 100 and the backup device 500. This is the details of step S131 in FIG. 12. When the restore button 183 on the menu screen 181 shown in FIG. 6 is selected by the user, the control unit 107 sends a startup instruction to the backup device 500 via the transmission/reception unit 101 (step S231).

[0176] The control unit 507 of the backup device 500 receives a startup instruction via the transmission/reception unit 501 and instructs the power supply unit 503 to start supplying power. The power supply unit 503 starts supplying power to each of the units comprising the backup device 500 (step S232). Next, the control unit 507 sends a startup notification to the HD recorder 100 via the transmission/reception unit 501 (step S233).

[0177] If the control unit 107 of the HD recorder 100 does not receive a startup notification from the backup device 500 within a predetermined time (NO in step S234) via the transmission/reception unit 101, it generates an error screen indicating that restoration is not possible and displays the generated error screen on the monitor 120 via the playback control unit 104 (step S236). If the startup notification is received within the predetermined time (YES in step S234), the authentication unit 102 is instructed to authenticate the device with the backup device 500. The authentication unit 102 performs device authentication with the backup device 500 under the direction of the control unit 107 (step S237).

[0178] If device authentication by the authentication unit 102 is a failure (NO in step S239), the control unit 107 moves to step S236. If the device authentication is successful (YES in step S239), the device identifier 115 "ID_A" is read from the unique information storage unit 108 (step S241), and the read out device identifier 115 "ID_A" and the restore information request are sent to the backup device 500 via the transmission/reception unit 101 (step S244).

[0179] If device authentication with the HD recorder 100 fails (NO in step S242), the control unit 507 in the backup device 500 instructs the power supply unit 503 to stop supplying power, and the power supply unit 503 stops supplying power to all units except the transmission/reception unit 501 and the control unit 507 (step S243). If the device authentication with the HD recorder 100 is successful (YES in step S242), a restore information request and the device identifier "ID_A" is received from the HD recorder 100 via the transmission/reception unit 501. It is then determined whether or not the received device identifier "ID_A" is registered in the permitted device identification information 551 stored in the secure information storage unit 511 (step S246). If it is determined that it is not registered (NO in step S246), the control unit 507 moves to step S263.

[0180] When it is determined that the content ID, title, and recording date and time are registered (step S246, YES), the content ID, title, and recording date and time are read from each piece of backup information comprising the backup management table 521 (step S247), and the read out content ID, title, and recording date and time are sent to the HD recorder 100 via the transmission/reception unit 501 (step S248). The control unit 107 of the HD recorder 100 receives the content ID, title and recording date and time from the backup device 500 via the transmission/reception unit 101. The received title and recording date and time are used to generate the restore information screen 221 shown in FIG. 7 (step S251), and the generated restore information screen 221 is displayed on the monitor 120 via the playback control unit 104 (step S252).

[0181] The control unit 107 receives the user selection of content to be restored via the input unit 103 (step S253). The control unit 107 reads the content ID corresponding to the selected content button (Step S254) and sends the read out content ID and the restore request to the backup device 500 via the transmission/reception unit 101 (Step S256).

[0182] The control unit 507 comprising the backup device 500 receives the restore request and content ID via the transmission/reception unit 501. Upon receiving the restore request, the control unit 507 selects backup information including the received content ID from the backup management table 521 stored in the secure information storage unit 511 (step S257). Next, the control unit 507 detects the content file corresponding to the selected backup information in the content storage unit 510 based on the received content ID, and reads the encrypted content and encrypted content key contained in the detected content file (Step S259). The control unit 507 combines the read out encrypted content and the encrypted content key and assigns them to a hash function to calculate a hash value (step S260).

[0183] Next, the hash value contained in the selected backup information is read (step S261), and the calculated hash value is compared with the read out hash value. If they do not match (NO in step S262), the control unit 507 generates an error notification indicating that the request to restore the content corresponding to the received content ID cannot be accepted, and sends a generated error notification to the HD recorder 100 via the transmission/reception unit 501 (step S263). Here, upon receipt of the error notification, the control unit 107 of the HD recorder 100 displays an error screen on the monitor notifying the user that restoration is not possible, and terminates the restoration process.

[0184] Next, the control unit 507 instructs the power supply unit 503 to stop supplying power. The power supply unit 503 receives an instruction from the control unit 507 and stops supplying power to all units except the transmission/reception unit 501 and the control unit 507 (step S264). If the calculated hash value and the read hash value match (YES in step S262), the control unit 507 reads the device-specific key 516 "Key_C" from the unique information storage unit 504 (step S266), and outputs the read out device-specific key 516 "Key_C" and the encrypted content key to the encryption processing unit 509, which is instructed to decrypt the encrypted content key. The encryption processing unit 509 decrypts the encrypted content key using the device-specific key 516 "Key_C" to generate a content key, and outputs the generated content key to the control unit 507 (Step S267).

[0185] The control unit 507 receives the content key from the encryption processing unit 509, and then reads the encrypted content contained in the detected content file (step S268). Next, the control unit 507 obtains the current time from the secure clock, and calculates the expiration time by adding the viewing period "240 hours" to the obtained current time (Step S269). The read out encrypted content, the received content key, and the calculated expiration time are then transmitted to the HD recorder 100 via the transmission/reception unit 501 (step S271). After transmission, the control unit 507

instructs the power supply unit 503 to stop supplying power, and the power supply unit 503 receives an instruction from the control unit 507 and stops supplying power to all units except the transmission/reception unit 501 and the control unit 507 (step S272).

[0186] The control unit 107 in the HD recorder 100 receives the encrypted content, content key, and expiration time from the backup device 500 via the transmission/reception unit 101. Upon receiving the encrypted content, content key, and expiration time, a new content file is generated in the information storage unit 110, and the received encrypted content and content ID are written to the generated content file (Step S274).

[0187] Next, the device-specific key 116 "Key_A" is read from the unique information storage unit 108 (step S276), and the read out device-specific key 116 "Key_A" and the received content key are outputted to the encryption processing unit 109, which is instructed to encrypt the content key. The encryption processing unit 109 receives the device-specific key 116 "Key_A" and the content key from the control unit 107. The received device-specific key "Key_A" is used to encrypt the content key, an encrypted content key is generated, and the generated encrypted content key is outputted to the control unit 107 (Step S277).

[0188] The control unit 107 receives the encrypted content key from the encryption processing unit 109 and writes the received encrypted content key to the content file generated in the information storage unit 110 (Step S278). Next, the control unit 107 combines the received encrypted content and the received encrypted content key and assigns them to a hash function to calculate a hash value (step S279).

[0189] The control unit 107 adds content information including the selected content button and corresponding content ID, title, recording date and time, received expiration time, and calculated hash value to the content management table 121 (step S281). Next, "1" is written to the back-up flag of the added content information (Step S284), and "2" is written to the priority level (Step S286).

[0190] (5) Backup processing performed by the HD recorder 100 and the backup device 500

The backup processing performed by the HD recorder 100 and the backup device 500 will now be explained using the flowcharts shown in FIG. 18 to FIG. 20. This is the details of step S114 in FIG. 12. At the current time backup schedule indicated by the secure clock 117, when the time is set by the user as "Sunday 0:30" arrives, the control unit 107 selects one piece of content information at a time in sequential order from the content management table 121 stored in the secure storage unit 113 (step S301). At this point, if all content information has been selected and there is no new content information to select (YES in step S302), the backup process is ended. If all content information has not been selected (step S302, NO), the control unit 107 determines whether the backup flag included in the selected content information is "0," that is, whether the content corresponding to the selected content information has already been backed up (step S303). If the backup flag is not "0" (NO in step S303), the unit returns to step S301 and selects the next piece of content information.

[0191] If the backup flag is "0" (YES in step S303), the control unit 107 reads the selected content information and the content ID (step S304), and detects the content file corresponding to the selected content information based on the read out content ID (step S306). The encrypted content and encrypted content key from the detected content files are read from the information storage unit 110 (step S307).

[0192] The control unit 107 combines the read out encrypted content and the encrypted content key, assigns them to a hash function, and calculates the hash value (step S308). Next, the hash value contained in the selected content information is read out (step S309), and the read out hash value is compared with the calculated hash value (step S311). If they do not match, the unit returns to step S301 and moves on to processing the next piece of content information.

[0193] When the read out hash value and the calculated hash value match, the control unit 107 sends a start instruction to the backup device 500 via the transmission/reception unit 101 (step S313). The control unit 507 in the backup device 500 receives the start instruction from the HD recorder 100 via the transmission/reception unit 501 and instructs the power supply unit 503 to start supplying power.

The power supply unit 503 starts supplying power to each unit of the backup device 500 according to instructions from the control unit 507 (step S316).

[0194] The control unit 507 sends a start notification to the HD recorder 100 via the transmission/reception unit 501 (step S317). If the control unit 107 of the HD recorder 100 does not receive a startup notification from the backup device 500 within a specified time (NO in step S318), it terminates the backup process. When a startup notification is received within the specified time via the transmission/reception unit 101 (YES in step S318), the control unit 107 instructs the authentication unit 102 to perform device authentication with the backup device 500.

[0195] The authentication unit 102 performs device authentication with the backup device 500 (step S321) based on instructions from the control unit 107. If device authentication by the authentication unit 102 fails (NO in step S322), the control unit 107 terminates the backup process. If the device authentication is successful (YES in step S322), the control unit 107 reads the device-specific key 116 "Key_A" from the device-unique information storage unit 108, outputs the read out device-specific key 116 "Key_A" and the encrypted content key included in the selected content information to the encryption processing unit 109, and gives an instruction to decrypt the encrypted content key. The encryption processing unit 109 receives the instruction from the control unit 107, decrypts the encrypted content key using the received device-specific key 116 "Key_A", generates a content key, and outputs the generated content key to the control unit 107 (step S323).

[0196] The control unit 107 receives the content key from the encryption processing unit 109. When the content key is received, the content ID, title, and recording date and time included in the selected content information are read (step S324). Next, the control unit 107 reads the device identifier 115 "ID_A" from the unique information storage unit 108 and reads the encrypted content corresponding to the selected content information from the information storage unit 110 (step S326). The backup request and the read out device identifier 115 "ID_A", the content ID, the title, the recording date and time, the encrypted content, and the received content key are transmitted via the transmission/reception unit 101 to the backup device 500 (step S327).

[0197] If device authentication with the HD recorder 100 fails (NO in step S328), the control unit 507 instructs the power supply unit 503 to stop supplying power, and the power supply unit 503 stops supplying power to all units other than the transmission/reception unit 501 and the control unit 507 (step S329). If device authentication is successful (YES in step S328), the control unit 507 receives the backup request, device identifier "ID_A," content ID, title, recording date and time, encrypted content, and content key from the HD recorder 100 via the transmission/reception unit 101. It is then determined whether the received device identifier "ID_A" is registered in the authorized device identification information 551 stored in the secure information storage unit 511 (step S331). If it is determined that it is not registered (NO in step S331), the control unit 507 sends an error notification indicating that the backup request cannot be accepted to the HD recorder 100 via the transmission/reception unit 501 (step S332) and stops the power supply to each circuit constituting the backup device 500 via the power supply unit 503 (step S333). At this point, HD recorder 100, which received the error notification, terminates the backup process.

[0198] When it is determined that the received device identifier "ID_A" is registered in the authorized device identifier information 551 (YES in step S331), the device-specific key 516 "Key_C" is read from the unique information storage unit 504, and the read out device-specific key 516 "Key_C" and the received content key are outputted to the encryption processing unit 509, with an instruction to encrypt the content key. The encryption processing unit 509 encrypts the content key using the device-specific key 516 "Key_C" received in accordance with the instructions from the control unit 507, generates an encrypted content key, and outputs the generated encrypted content key to the control unit 507 (step S336).

[0199] The control unit 507 receives the encrypted content key from the encryption processing unit 509. When the encrypted content key is received, a new content file is generated in the content storage unit 510, and the received content ID, the encrypted content, and the encrypted content key received from the encryption processing unit 509 are written to the generated content file (step S337). Next, the control unit 507 combines the received encrypted content and the received encrypted content key, assigns them to the hash function, and calculates the hash value (step S339). Backup information is

generated containing the received content ID, title, recording date and time, device identifier "ID_A," and calculated hash value, and the generated backup information is added to the backup management table 521 (step S341). Here, the received device identifier "ID_A" is set as the backup source device identifier.

[0200] The control unit 507 obtains the secure clock time, adds the viewing period "240 hours" to the obtained current time to calculate the expiration time (step S342), and transmits the calculated expiration time to the HD recorder 100 via the transmission/reception unit 501 (step S343). When transmission is complete, the power supply to each circuit constituting the backup device 500 is stopped via the power supply unit 503 (step S344).

[0201] The control unit 107 of the HD recorder 100 receives the expiration time from the backup device 500 via the transmission/reception unit 101 and writes the received expiration time to the selected content information (step S346). Next, the control unit 107 changes the backup flag of the selected content information to "1" (step S347), changes the priority level to "2" (step S348), and returns to step S301.

[0202] (6) Extending the expiration time of the HD Recorder 100

The extension of the expiration time by the HD recorder 100 will now be explained using the flowchart in FIG. 21. This is the details of step S112 in FIG. 12. When the time indicated by the secure clock 117 reaches the preset extension time "2:00," the main control unit 118 that constitutes the control unit 107 outputs an expiration time extension instruction to the expiration time management unit 119.

[0203] The expiration time management unit 119 receives the expiration time extension instruction and selects the content information constituting the content management table 121 stored in the secure storage unit 113 one by one in sequential order (step S361). At this point, if all content information has been selected and there is no new content information to select (YES in step S362), the expiration time extension process is terminated.

[0204] If all content information has not been selected (NO in step S362), the expiration time management unit 119 reads the expiration time of the selected content information (step S363). Here, an expiration time is written to the selected content information, and if there is no expiration time (NO in step S366), the process returns to step S361 to select the next piece of content information. If an expiration time is written in the selected content information (YES in step S366), the expiration time management unit 119 then obtains the current time from the secure clock 117 (step S367) and calculates the remaining time by calculating the difference between the read out expiration time and the obtained current time (step S368).

[0205] The expiration time management unit 119 compares the calculated remaining time with the extension execution time of "24 hours" and, if it determines that the remaining time is 24 hours or more (NO in step S371), returns to step S361 and moves on to processing the next piece of content information. When it is determined that the calculated remaining time is less than 24 hours (YES in step S371), the expiration time management unit 119 sends a start instruction to the backup device 500 via the transmission/reception unit 101 (step S372). The control unit 507 of the backup device 500 receives a start instruction via the transmission/reception unit 501 and instructs the power supply unit 503 to start supplying power. The power supply unit 503 starts supplying power to each unit of the backup device 500 (step S373).

[0206] Next, the control unit 507 sends a startup notification to the HD recorder 100 via the transmission/reception unit 501 (step S374). If the deadline management unit 119 of the HD recorder 100 does not receive a startup notification from the backup device 500 via the transmission/reception unit 101 within a specified time (NO in step S376), it returns to step S361.

[0207] When a startup notification is received within the specified time (YES in step S376), the expiration time management unit 119 instructs the authentication unit 102 to perform device authentication with the backup device 500. The authentication unit 102 performs device authentication with the backup device 500 (step S381) based on instructions from the expiration time management

unit 119, which constitutes the control unit 107. If device authentication by the authentication unit 102 fails (NO in step S382), the expiration time management unit 119 returns to step S361.

[0208] If device authentication is successful (YES in step S382), the expiration time management unit 119 reads the device identifier 115 "ID_A" from the unique information storage unit 108 and reads the content ID from the selected content information (step S383). Next, the expiration time management unit 119 sends an extension request and the read out device identifier 115 "ID_A" and content ID to the backup device 500 via the transmission/reception unit 101 (step S386).

[0209] When device authentication with the HD recorder 100 fails (NO in step S389), the control unit 507 of backup device 500 instructs the power supply unit 503 to stop supplying power, and power supply unit 503 stops supplying power to all units other than the transmission/reception unit 501 and the control unit 507 (step S391). If device authentication with the HD recorder 100 is successful (YES in step S389), the control unit 507 receives the extension request, the device identifier "ID_A," and the content ID via the transmission/reception unit 501.

[0210] Next, the control unit 507 determines whether the received device identifier "ID_A" is included in the authorized device identification information 551 stored in the secure information storage unit 511 (step S392). If it is determined that it is not included (NO in step S392), the control unit 507 sends an error notification to the HD recorder 100 via the transmission/reception unit 501 (step S393) and instructs the power supply unit 503 to stop supplying power. The power supply unit 503 stops supplying power to all units other than the transmission/reception unit 501 and the control unit 507 (step S394). At this point, if an error notification is received, the expiration time management unit 119 of the HD recorder 100 transitions the processing to step S361.

[0211] In step S392, if it is determined that the received device identifier "ID_A" is included in the permitted device identification information 551 (step S392 YES), the control unit 507 selects backup information including the received content ID from the backup management table 521 stored in the secure information storage unit 511 (step S396). Next, the control unit 507 detects the selected content information and the corresponding content file based on the received content ID, reads the encrypted content and the encrypted content key from the detected content file (step S397), combines the read out encrypted content and the encrypted content key, and assigns them to the hash function to calculate the hash value (step S398).

[0212] Next, the control unit 507 reads out the hash value included in the selected backup information (step S401) and compares the read hash value with the calculated hash value (step S402). If they do not match (NO in step S402), the control unit 507 sends an error notification to the HD recorder 100 via the transmission/reception unit 501 (step S403) and instructs the power supply unit 503 to stop supplying power. The power supply unit 503 stops supplying power to all units other than transmission/reception unit 501 and the control unit 507 (step S404). At this point, if an error notification is received, the expiration time management unit 119 of the HD recorder 100 transitions the processing to step S361.

[0213] If the read hash value and the calculated hash value match (YES in step S402), the control unit 507 obtains the current time from the secure clock, adds the viewing period "240 hours" to the obtained current time, and calculates the expiration time (step S406). Next, the control unit 507 transmits the calculated expiration time to the HD recorder 100 via the transmission/reception unit 501 (step S407). When the expiration time has been sent, the control unit 507 instructs the power supply unit 503 to stop supplying power. The power supply unit 503 stops supplying power to all units other than the transmission/reception unit 501 and the control unit 507 (step S408).

[0214] The expiration time management unit 119 receives the expiration time from the backup device 500 via the transmission/reception unit 101. The expiration time included in the selected content information (step S411) is updated based on the received expiration time, and the processing moves to step S361.

(7) Device authentication

The device authentication operation performed between the HD recorder 100 and the backup device 500 will now be explained using FIG. 24 and FIG. 25.

[0215] Note that this is just one example of a device authentication method, and other authentication methods and key sharing methods may be used. Here, $\text{Gen}()$ is the key generating function, and Y is a system-specific parameter. The key generating function $\text{Gen}()$ satisfies the relationship $\text{Gen}(x, \text{Gen}(z, Y)) = \text{Gen}(z, \text{Gen}(x, Y))$. Since the key generating function can be performed using any technique known in the art, the details are not provided here.

[0216] The authentication unit 102 of the HD recorder 100 reads the public key certificate Cert_A (step S501) and transmits the read out public key certificate Cert_A to the backup device 500 via the transmission/reception unit 101 (step S502). The authentication unit 502 of the backup device 500 that received the public key certificate Cert_A performs signature verification by applying the signature verifying algorithm V to the signature data Sig_CA of the certifying authority included in the public key certificate Cert_A using the public key PK_CA of the certifying authority (step S503). Here, signature verifying algorithm V is an algorithm that verifies signature data generated by signature generating algorithm S . If the signature verification fails (NO in step S504), the process is terminated.

[0217] If the signature verification result is successful (YES in step S504), the authentication unit 502 reads the CRL (step S505) and determines whether the certificate identification number ID_a included in the public key certificate Cert_A is registered in the read out CRL (step S506). If it is determined that it is registered (YES in step S506), the processing is terminated. If it is determined that it is not registered (NO in step S506), the authentication unit 502 reads the public key certificate Cert_C (step S507) and transmits the read out public key certificate Cert_C to the HD recorder 100 (step S508).

[0218] The authentication unit 102 of the HD recorder 100 that received the public key certificate Cert_C performs signature verification by applying the signature verifying algorithm V to the signature data Sig_CA of the certifying authority included in the public key certificate Cert_C using the public key PK_CA of the certifying authority (step S509). If the signature verification fails (NO in step S510), the processing is terminated. If the signature verification is successful (YES in step S510), the authentication unit 102 reads the CRL (step S511) and determines whether the certificate identification number ID_b included in the public key certificate Cert_C is registered in the read out CRL (step S512). If it is determined that it is registered (YES in step S512), the processing is terminated. If it is determined that it is not registered (NO in step S512), the processing is continued.

[0219] The authentication unit 502 of the backup device 500 generates a random number Cha_C (step S513) and transmits the generated random number Cha_C to the HD recorder 100 (step S514). The authentication unit 102 of the HD recorder 100 receives a random number Cha_C , applies a signature generating algorithm S to the received random number Cha_C using the secret key SK_A of the HD recorder 100 to generate signature data Sig_A (step S515), and transmits the generated signature data Sig_A to the backup device 500 (step S516).

[0220] When the authentication unit 502 of the backup device 500 receives the signature data Sig_A , it performs signature verification on the received signature data Sig_A by applying the signature verifying algorithm V using the public key PK_A of the HD recorder 100 received in the public key certificate Cert_A (step S517). If the signature verification result is determined to be a failure (NO in step S518), the process is terminated. If the signature verification result is determined to be a success (YES in step S518), the process continues.

[0221] The authentication unit 102 of the HD recorder 100 generates a random number Cha_A (step S519) and transmits the generated random number Cha_A to the backup device 500 (step S520). The backup device 500 receives a random number Cha_A , applies signature generating algorithm S to the received random number Cha_A using the secret key SK_B of the backup device 500 to generate signature data Sig_C (step S521), and transmits the generated signature data Sig_C to the HD recorder 100 (step S522).

[0222] When the HD recorder 100 receives the signature data Sig_C , it performs signature verification on the received signature data Sig_C by applying the signature verifying algorithm V to the signature data Sig_C using the public key PK_B of the backup device 500 received in the public key certificate

Cert_C (step S523). If the signature verification result is determined to be a failure (NO in step S524), the processing is terminated. If the signature verification result is determined to be successful (YES in step S524), the authentication unit 102 then generates a random number "a" (step S525), generates $\text{Key_a} = \text{Gen}(a, Y)$ using the generated random number "a" (step S526), and transmits the generated Key_a to the backup device 500 (step S527).

[0223] When the authentication unit 502 of the backup device 500 receives Key_a, it generates a random number "c" (step S528), generates $\text{Key_c} = \text{Gen}(c, Y)$ using the generated random number "c" (step S529), and transmits the generated Key_c to the HD recorder 100 (step S530). Also, the generated random number "c" and the received Key_a are used to generate $\text{Key_ac} = \text{Gen}(c, \text{Key_A}) = \text{Gen}(c, \text{Gen}(a, Y))$ and this is used as the session key (step S531).

[0224] The HD recorder 100 receives Key_c and uses generated random number "a" and the received Key_c to generate $\text{Key_ac} = \text{Gen}(a, \text{Key_c}) = \text{Gen}(a, \text{Gen}(c, Y))$, which is used as the session key (step S532).

1.5 Summary, Results

As explained above, in the backup system 1 of the present invention, the HD recorder 100 sends encrypted content stored in the information storage unit 110 to the backup device 500 and requests backup, and the backup device 500 backs up the received encrypted content. At this time, an expiration time is set for the encrypted content stored in the HD recorder 100, which is the source of the encrypted content. The HD recorder 100 requests an extension of the expiration time from backup device 500 before the expiration time arrives.

[0225] If the backup device 500 cannot communicate for some reason, such as a power failure, the expiration time cannot be extended, and when the expiration time arrives, the HD recorder 100 deletes the encrypted content whose expiration time has been reached from the information storage unit 110. Once deleted, encrypted content stored in the backup device 500 can be retrieved by user operations.

[0226] The backup device 500 stores permitted device identification information in advance, and backup requests, extension requests, and restore requests are accepted from devices with a device identifier registered in the permitted identification information. In this way, after the backup device 500 has backed up encrypted content, the HD recorder 100 stores the encrypted content until the expiration time, allowing the user to view the content by performing simple operations.

[0227] When the expiration time arrives, the HD recorder 100 deletes the stored encrypted content, thereby preventing the indefinite existence of copies of the encrypted content and protecting the rights of the copyright holder of the content. In the backup system 1, the backup device 500 also stores the backed up content requested by the HD recorder 400. The HD recorder 100 can also retrieve and play back backed up content at the instruction of the HD recorder 400, further improving convenience for the user.

[0228] The backup device 500 receives startup instructions from the HD recorder 100 and supplies power to the units that constitute the backup device 500 only during certain processing. Thus, the operating time of the hard disc unit comprising the content storage unit 510 can be minimized and the risk of failure of the hard disc unit can be reduced.

2. Modified Examples

While the present invention was described using a certain embodiment, the invention is of course not limited to this embodiment. The following examples are also encompassed by the present invention.

[0229] (1) In the first embodiment, the expiration time management unit 119 may delete only the encrypted content key from the information storage unit 110 in the content file containing the encrypted content after the expiration time. Here, the expiration management unit 119 deletes only the encrypted content key from the information storage unit 110, and deletes the hash value and expiration time from the corresponding content information.

[0230] With the playback list screen 211 displayed on the monitor, if there is no hash value in the content information corresponding to the content button selected by the user, the main control unit 118 reads the content ID contained in the content information and sends, via the transmission/reception unit 101, a content key request and the read out content ID to the backup device 500.

[0231] The backup device 500 receives the content key request and sends the corresponding content key and expiration time to the HD recorder 100. The main control unit 118 of the HD recorder 100 receives the content key and expiration time, instructs the encryption processing unit 109 to generate an encrypted content key, and writes the generated encrypted content key to the information storage unit 110. Next, the content information corresponding to the selected content button and the encrypted content contained in the corresponding content file are read from the information storage unit 110, a hash value is generated based on the read out encrypted content and generated encrypted content key, and the generated hash value and the received expiration time are written to the content information. Thereafter, the encrypted content is decrypted and played back in the same manner as in the control of the generation processing described above.

(2) In Modified Example (1) above, only the hash value and expiration time of the content information whose expiration time cannot be updated may be deleted.

[0232] In this case, the main control unit 118 sends an expiration time request to the backup device 500 instead of a content key request. The received expiration time is written to the content information only when an expiration time can be received from the backup device 500, and the hash value is calculated anew from the encrypted content corresponding to the content information and the encrypted content key.

(3) In the first embodiment above, the backup device 500 calculates the expiration time and sends the calculated expiration time to the HD recorder 100.

[0233] For example, in the backup process, instead of sending an expiration time, the backup device 500 sends a completion notification to the HD recorder 100 indicating that the backup was completed successfully. When the main control unit 118 of the HD recorder 100 receives the completion notification, it obtains the current time from the secure clock 117 and calculates the expiration time by adding the viewing period "240 hours" to the obtained current time.

[0234] In the expiration time extension process, instead of the expiration time, the backup device 500 also sends an extension permission to the HD recorder 100 indicating that the expiration time can be extended. When the expiration management unit 119 of the HD recorder 100 receives extension permission, it obtains the current time from the secure clock 117 and calculates the expiration time by adding the viewing period "240 hours" to the obtained current time.

[0235] Instead of using the current time, the viewing period "240 hours" may be added to the expiration time included in each piece of content information, and the result of the addition may be used as the new expiration time. In this case, the control unit 507 comprising the backup device 500 is no longer required to have a secure clock.

(4) In the embodiment above, the HD recorder 100 extends the expiration time and deletes expired content based on the expiration time included in each piece of content information, but it may also manage each piece of content by the start time of the period during which the encrypted content is allowed to be played and the period during which it is allowed to be played.

[0236] In this case, each piece of content information comprising the content management table 121 includes, instead of the expiration time, a start time of the period during which the content is allowed to be played. The main control unit 118 stores "240 hours" as the period during which content playback is permitted. In the backup process, the backup device 500 sends a backup completion notification indicating that it has successfully backed up the content instead of the expiration time.

[0237] The main control unit 118 receives a backup completion notification from the backup device 500 via the transmission/reception unit 101, obtains the current time from the secure clock 117, and writes the obtained current time to the content information as the start time. In the expiration time extension

process, the expiration time management unit 119 obtains the current time from the secure clock 117, and if the time elapsed from the start time is 216 hours or more, it sends an extension request to the backup device 500.

[0238] In the deletion process, the expiration time management unit 119 obtains the current time from the secure clock 117, and if the start time is more than 240 hours from the elapsed time, the corresponding content file is deleted from the information storage unit 110 and the content information is deleted. In this configuration, the control unit 507 comprising the backup device 500 is no longer required to have a secure clock.

(5) In the first embodiment and modified examples, the HD recorder 100 sends an extension request to the backup device 500 when the time until the expiration time of each piece of encrypted content is less than 24 hours, but it may send extension requests periodically regardless of the time until the expiration time arrives.

(6) Also, instead of using an expiration time, the content may be managed based on the number of viewings.

[0239] For example, each piece of content information in the content management table 121 includes a number of valid viewings instead of an expiration time. Each time content is played, the control unit 107 subtracts one from the valid number of viewings included in the content information corresponding to the played content. In the backup process and the expiration time extension process, the backup device 500 transmits the number of viewings "3" instead of the expiration time. The control unit 107 of the HD recorder 100 uses the received number of viewings "3" as the valid number of viewings.

[0240] The HD recorder 100 deletes content information with a valid number of views of "0" as well the content file corresponding to this content information.

(7) In the first embodiment, the backup device 500 stores the permitted device identification information 551 in advance, and devices with device identifiers registered in the permitted device identification information 551 have restore requests accepted by the backup device 500, but it is also possible to determine whether to accept restore requests based on a copied content count.

[0241] For ease of explanation, the encrypted content stored in the backup device 500 is simply referred to here as "content," while the encrypted content stored in playback devices, including the HD recorder 100, is referred to as copied content. Also, other devices with content storage and playback functions are connected to the backup system 1 in addition to HD recorders 100 and 400.

[0242] Specifically, the control unit 507 of the backup device 500 stores the allowable copy count "3," which is the number of copies allowed to exist of each content. The backup information in the backup management table 521 stored in the secure information storage unit 511 includes a copy count indicating the number of copies of each content that currently exist. The secure information storage unit 511 also stores a plurality of copy management tables. Each copy management table consists of a plurality of pieces of copy information, and each piece of copy information consists of a content ID, a device identifier, and an expiration time. The content ID is identical to the content IDs included in the backup management table 521. The device identifier is information that identifies the external device that has a copy of content indicated by the content ID. The expiration time is the expiration time of the copied content on the external device indicated by the device identifier.

[0243] (7-a) Backup processing

In the backup processing described in the first embodiment, when the control unit 507 receives a backup request from the HD recorder 100, it writes content, adds backup information, and calculates the expiration time, as explained above in the first embodiment. At this time, "1" is written to the copy count of the added backup information.

[0244] Next, the control unit 507 generates copy information consisting of the received content ID, the received device identifier, and the calculated expiration time, and adds the generated copy information

to the copy management table. After adding the copy information, the calculated expiration time is sent to the HD recorder 100.

(7-b) Copy deletion

During control of the recording process by the main control unit 118 of the HD recorder 100, as already mentioned, the main control unit 118 deletes content information including priority level "2" and the corresponding encrypted content from the information storage unit 110 when free space in the information storage unit 110 is insufficient.

[0245] At this time, the main control unit 118 sends a copy deletion notification indicating the deletion of copied content, the content ID corresponding to the copied content to be deleted, and the device identifier "ID_A" of the HD recorder 100 itself to the backup device 500. The control unit 507 of the backup device 500 receives the copy deletion notification, the content ID, and the device identifier "ID_A" from the HD recorder 100. When the copy deletion notification is received, the copied information including the received content ID and the device identifier "ID_A" is deleted, and one is subtracted from the copy count in the backup information including the received content ID.

[0246] (7-c) Restore processing

When the control unit 507 of the backup device 500 receives a restore request from an external device in the restore process described above, it reads the copy count in the backup information including the content ID received with the restore request. If the copy count is "3," an error notification indicating that the restore request cannot be accepted is sent to the HD recorder 100.

[0247] If the read out copy count is less than the permissible copy count of "3," the control unit 507 verifies the hash value, generates a content key, and calculates the expiration time, etc. using the procedures described in the first embodiment. After calculating the expiration time, one is added to the copy count contained in the backup information including the received content ID in the backup control table 521. Next, the control unit 507 generates copy information consisting of the received content ID, device identifier, and calculated expiration time, and adds the generated copy information to the copy management table.

[0248] Next, the content, content key, and expiration time are sent to the external device.

(7-d) Verification of the expiration time by the backup device 500

In the process of extending the expiration time, the control unit 507 selects copy information including the received content ID and device identifier, and rewrites the expiration time of the selected copy information with the newly calculated expiration time.

[0249] The control unit 507 stores the verification time at which the expiration time in each piece of copy information is verified. At the time of verification, the control unit 507 selects one piece of copy information comprising the copy control table, reads the expiration time contained in the selected copy information, and compares the read out expiration time with the current time. If the current time is past the expiration time, copy count in the backup information containing the content ID included in the selected copy information is reduced by 1. Next, the control unit 507 deletes the selected content information.

[0250] If the current time has not passed the expiration time, the copy count is not reduced and the copy information is not deleted. The control unit 507 verifies the expiration time in all pieces of backup information using the same procedure.

(8) Modified example (7) assumes that the backup device 500 stores the permissible copy count in advance.

[0251] For example, a predetermined bit in a TS packet that constitutes the content may contain the permissible copy count, and in the backup process, the backup device 500 may decrypt any one TS packet of the received encrypted content with the received content key to extract the permissible copy

count, which is stored in association with the received content ID. In addition to the permissible copy count, information indicating whether or not backup generation is permitted may also be included in the content. The control unit 107 of the HD recorder 100 extracts information indicating whether or not backup generation is permitted from the received content and stores the extracted information (called backup information) in association with the content ID.

[0252] If the backup process indicates permission to generate backup information corresponding to the encrypted content to be backed up, the encrypted content is sent to the backup device 500 according to the procedure as described in the first embodiment. If the backup information corresponding to the encrypted content to be backed up indicates that backup is prohibited, the transmission is terminated.

[0253] In particular, when the backup process described above is initiated by the user pressing the backup button, the backup information indicating the prohibition of backups and the title of the corresponding encrypted content is displayed on the monitor 120 to notify the user that backup of the displayed content is prohibited. In this way, the intention of the copyright holder of the content can be reflected with respect to backup and copied content generation.

(9) In the first embodiment, the encrypted content and the encrypted content key may be combined and assigned to a hash function to calculate a hash value assigned only to an encrypted content key.

(10) In the embodiment and modified examples, the same key is used for encryption and decryption by adopting a symmetric key encryption method for content and content key encryption, but the present invention is not limited to this. For example, a public key encryption method such as RSA or elliptic curve cryptography may be used, and different keys may be used for encryption and decryption.

[0254] Specifically, when a public key encryption method is used for content encryption, the key generating unit 106 of the HD recorder 100 generates a pair of content encryption keys and content decryption keys instead of a single content key in the content recording process described using FIG. 13. The control unit 107 outputs the content received via the broadcast receiving unit 114 and the content encryption key generated by the key generating unit 106 to the encryption processing unit 109 with an instruction to encrypt the content. When instructed to encrypt content, the encryption processing unit 109 applies an encryption algorithm according to a public key encryption method to the content using the content encryption key to generate encrypted content. When recording is stopped when the stop button is pressed or insufficient space is available in the information storage unit 110, the encryption processing unit 109 encrypts the content decryption key using the device-specific key "Key_A" instead of the content key, and generates an encrypted content key.

[0255] Afterward, the encryption processing unit 109 performs encryption and decryption by employing a symmetric key encryption method for encryption of the content decryption key and decryption of the encrypted content key, and by employing a public key encryption method for decryption of the encrypted content.

(11) The embodiments and modified examples are not limited to the configuration described above, in which the backup device 500 and the HD recorder 100 are connected by a LAN 30. A backup device built into the HD recorder 100, for example, is also encompassed by the invention.

(12) The content storage unit 510 of the backup device 500 has been described as comprising a hard disc unit, but it may also comprise a removable optical disc and an input/output unit for writing and reading information to and from the optical disc. In this case, the user removes or inserts an optical disc, when necessary.

[0256] It may also consist of a plurality of optical discs and a disc changer that automatically replaces these discs.

(13) The invention may be a method as shown above. It may also be a computer program that implements this methods by means of a computer, and digital signals composing the computer program.

[0257] The present invention may also be devised by recording the computer program or digital signals on a computer-readable recording medium, such as a flexible disk, hard disk, CD-ROM, MO, DVD, DVD-

ROM, DVD-RAM, BD (Blu-ray Disc), semiconductor memory, etc. The present invention may also be a computer program or digital signals recorded on these recording media.

[0258] The present invention may also transmit the computer program or digital signals via telecommunication lines, wireless or wired communication lines, networks such as the internet, data broadcasting, etc. The present invention may also be a computer system with a microprocessor and memory, in which the memory stores the computer program, and the microprocessor operates according to the computer program.

[0259] The present invention may also be embodied in an independent computer system by recording the program or digital signals on a recording medium and transferring it, or by transferring the program or digital signals via a network, etc.

(14) Some or all of the components in each of the devices above may be composed of a single system LSI (large-scale integrated circuit). A system LSI is a super multi-functional LSI manufactured by integrating multiple components on a single chip. Specifically, it is a computer system consisting of a microprocessor, ROM, RAM, and other components. The computer program is stored in the RAM. The system LSI realizes its functions by operating in accordance with the computer program.

[0260] The term "system LSI" is used for integrated circuits, and may refer to integrated circuits (IC), LSI, super-LSI, or ultra-LSI, depending on the degree of integration. Instead of a system LSI, it may be composed of a field-programable gate array (FPGA) or complex programmable logic device (CPLD, also known as a reconfigurable LSI) that can be programmed after being built into a product.

If a new technology is developed in the future that substitutes for the functions of the integrated circuits described above, the new technology may be used to realize some or all of the components that constitute each device.

(15) The embodiments and modified examples may be combined.

Industrial Applicability

[0261] The invention can be used operationally, continuously, and repeatedly in industries that generate, distribute, broadcast, and use digital content and in industries that manufacture and sell electronic devices that generate, distribute, play, edit, etc., content.

Claims

[1] A backup system comprising a recording and playback device for recording and playing back content, and a backup device, wherein the recording and playback device comprises:
a storage means for storing the content;
a receiving means for receiving an instruction to back up the content;
a content transmitting means for reading the content from the storage means and transmitting the read out content to the backup device upon receiving an instruction;
a writing means for writing to the storage means, in association with the content, period information indicating a period during which playback of the content to be backed up is permitted upon receiving an instruction; and
a playback control means for permitting playback of the content within the period indicated by the period information, and prohibiting playback of the content when the period indicated by the period information has ended, and
wherein the backup device comprises:
a content receiving means for receiving the content from the recording and playback device; and
a backup storage means for storing the received content.

[2] A recording and playback device for recording and playing back content, the recording and playback device comprising:
a storage means for storing the content;
a receiving means for receiving an instruction to back up the content;
a content transmitting means for reading the content from the storage means and transmitting the read out content to the backup device upon receiving an instruction if backup of the read out content is permitted;
a writing means for writing to the storage means, in association with the content, period information indicating a period during which playback of the content to be backed up is permitted upon receiving an instruction; and
a playback control means for permitting playback of the content within the period indicated by the period information, and prohibiting playback of the content when the period indicated by the period information has ended.

[3] The recording and playback device according to claim 2, further comprising:
an extension requesting means for transmitting to the backup device an extension request requesting permission to extend the period indicated by the period information; and
an extension means for receiving extension permission information indicating permission for extension from the backup device and extending the period indicated by the period information.

[4] The recording and playback device according to claim 3, wherein the extension requesting means transmits the extension request at a predetermined time prior to the end of the period indicated by the period information.

[5] The recording and playback device according to claim 3, wherein the extension requesting means repeatedly transmits the extension request within the period indicated by the period information at regular intervals.

[6] The recording and playback device according to claim 3, wherein the extension means receives extension permission information indicating a period later than the period indicated by the period information stored in the storage means, and extends the period information by rewriting the period indicated by the period information to the period indicated by the received extension permission information.

[7] The recording and playback device according to claim 3, wherein the extension means stores the extension time in advance and extends the period information by adding the extended time to the period indicated by the expiration information.

[8] The recording and playback device according to claim 3, wherein the period information indicates the end of the period during which playback of the content stored in the storage means is permitted,

and the playback control means permits playback of the content if the current time is prior to the point in time indicated by the period information, and prohibits playback of the content if the current time is after the point in time indicated by the period information.

[9] The recording and playback device according to claim 3, wherein the period information includes permission time indicating the length of time during which playback of the content stored in the storage means is permitted, and the start time indicating the start time of the period during which playback of the content is permitted, and the playback control means acquires the elapsed time from the start time, and permits playback of the content if the acquired elapsed time is less than or equal to the permitted time, and prohibits playback of the content if the elapsed time from the start time exceeds the permitted time.

[10] The recording and playback device according to claim 2, wherein the playback control means prohibits playback of the content by deleting the content from the storage means.

[11] The recording and playback device according to claim 10, the recording and playback device further comprising:

a restore instruction acquiring means for acquiring a restore instruction indicating acquisition of the content stored in the backup device;

a restore requesting means for transmitting to the backup device a request to transmit the content stored in the backup device upon acquiring a restore instruction; and

a restore means for receiving the content from the backup device and writing the received content to the storage means,

wherein the writing means further writes period information indicating the period during which playback of the content written by the restore means is permitted to the storage means in association with the content when the content is written.

[12] The recording and playback device according to claim 2, wherein the content stored in the storage means is configured to include encrypted copyrighted material generated by encrypting digital copyrighted material based on an encryption key and a decryption key used to decrypt the encrypted copyrighted material, and

the playback control means prohibits playback of the content by deleting the decryption key included in the content.

[13] The recording and playback device according to claim 12, further comprising:

a restore instruction acquiring means for acquiring a restore instruction indicating acquisition of the encryption key stored in the backup device;

a restore requesting means for transmitting a request to the backup device for transmission of the decryption key stored in the backup device when a restore instruction is acquired; and

a restore means for receiving the decryption key from the backup device and writing the received decryption key to the storage means,

wherein the writing means further writes period information indicating the period during which playback of the content stored in the storage means is permitted, in association with the content, to the storage means when the decryption key is written.

[14] The recording and playback device according to claim 2, wherein the content stored in the storage means includes encrypted copyrighted material generated by encrypting digital copyrighted material using an encryption key, and an encrypted key generated by encrypting a decryption key used to decrypt the encrypted copyrighted material using a unique key specific to the recording and playback device, and the playback control means prohibits playback of the content by deleting the encrypted key from the storage means.

[15] The recording and playback device according to claim 2, wherein the content stored in the storage means includes backup information indicating whether backup is permitted or prohibited, the content transmitting means determines whether the backup information indicates permission for backup, and transmits the content when it is determined that permission has been granted, and the writing means determines whether the backup information indicates permission for backup, and writes the period information when it is determined that permission has been granted.

[16] The recording and playback device according to claim 2, wherein the content transmitting means encrypts the content using a communication key and securely transmits the encrypted content.

[17] The recording and playback device according to claim 2, further comprising a detection information storage means for storing detection information generated by performing a predetermined operation on the content, and an anti-tampering means for reading the content from the storage means, performing the predetermined operation on the read out content to generate inspection information, comparing the generated inspection information with the detection information, and prohibiting the use of content determined to be inconsistent.

[18] The recording and playback device according to claim 2, wherein the backup device stores different content in response to a backup instruction from a device other than the recording and playback device, wherein the recording and playback device further comprises:
a restore instruction acquiring means for acquiring a restore instruction indicating acquisition of the other content;
a content requesting means for transmitting to the backup device a transmission request for the other content upon acquiring the restore instruction; and
a restore means for receiving the other content from the backup device and writing the received other content to the storage means, and
wherein the writing means further writes period information indicating the period during which playback of the other content is permitted to the storage means in association with the other content upon receiving the other content.

[19] A backup device for backing up content, the backup device comprising:
a storage device that stores the content;
an extension request receiving means for receiving an extension request requesting permission to extend the period of time during which the content stored in the recording playback device may be played back;
a determining means for determining whether or not to grant the extension; and
a permission means for outputting extension permission information indicating permission for the extension to the recording and playback device when it has been determined that permission is to be granted.

[20] The backup device according to claim 19, wherein the storage means further stores identification information indicating the content in association with the content,
the extension receiving means receives the extension request including the content identification information indicating the content stored in the recording and playback device, and
the determining means compares the content identification information with the identification information stored in the storage means, and grants permission if they match.

[21] The backup device according to claim 19, wherein the extension request includes device identification information indicating the recording and playback device that outputted the extension request, and
the determining means stores in advance one or more pieces of permitted device identification information indicating a specific device, and grants the request if the device identification information included in the received extension request matches any of the pieces of permitted device identification information.

[22] The backup device according to claim 19, wherein the storage means further stores detection information generated by performing a predetermined operation on the content in association with the content, and the determining means reads the content from the storage means, performs the predetermined operation on the read out content to generate verification information, compares the generated verification information with the detection information, and grants the extension if they match.

[23] The backup device according to claim 19, wherein the permission means outputs the permission information indicating a period later than the period indicated by the period information.

[24] The backup device according to claim 19, wherein the backup device further comprises:
a restore receiving means for receiving a transmission request for content stored in the storage means;

a restore determining means for determining whether or not to transmit the content; and
a restore transmitting means for reading the content from the storage means and transmitting the read out content when it is determined that the content is to be transmitted.

[25] The backup device according to claim 24, wherein the transmission request includes restore device identification information indicating the restore device that is the transmission source of the transmission request, and the restore determining means stores one or more pieces of permitted device identification information indicating a specific device in advance, and determines that the content is to be transmitted if the restore device identification information matches any of the pieces of permitted device identification information.

[26] The backup device according to claim 25, wherein the permitted device identification information indicates the backup device that transmitted the instruction to back up the content stored in the storage means, and
the restore determining means determines that the content is to be transmitted if the restore device identification information and the permitted device identification information match.

[27] The backup device according to claim 24, wherein the restore determining means has a copy count indicating the total number of devices storing content that is identical to the content stored in the storage means and permitted to be played by the backup device, and a copy permission count indicating the upper limit of the number of copies, and the content is permitted to be transmitted if the copy count is less than the copy permission count.

[28] The backup device according to claim 27, wherein the backup device further comprises:
a period information storage means for associating and storing device identification information indicating the device that stores the content that is the same as the content stored in the storage means and that is permitted to be played by the backup device, and copying period information indicating the period during which playback of the content is permitted on the device; and
and a copy count management means for subtracting one from the copy count when the period indicated by the copy period information ends.

[29] The backup device according to claim 27, wherein the content stored in the storage means includes, in advance, the copy permission count, and the determining means obtains the copy permission count from the content.

[30] The backup device according to claim 24, wherein the restore transmitting means encrypts the content using a communication key and securely transmits the encrypted content.

[31] The backup device according to claim 19, wherein the recording and playback device outputs a startup instruction information to the backup device to instruct the device to start up prior to an extension request, and
the backup device further comprises a power control means for starting the supplying power to each circuit comprising the backup device upon receipt of the startup instruction.

[32] A backup method used in a recording and playback device for recording and playing back content, the recording and playback device having a storage means that stores the content, and the backup method comprising:

a receiving step of receiving an instruction to back up the content;

a content transmitting step for reading the content from the storage means and transmitting the read out content to the backup device upon receiving an instruction if backup of the read out content is permitted;

a writing step of writing to the storage means, in association with the content, period information indicating a period during which playback of the content to be backed up is permitted upon receiving an instruction; and

a playback control step of permitting playback of the content within the period indicated by the period information, and prohibiting playback of the content when the period indicated by the period information has ended.

[33] An integrated circuit for use in a recording and playback device that records and plays back content, the integrated circuit comprising:

a storage means for storing the content;

a receiving means for receiving an instruction to back up the content;

a content transmitting means for reading the content from the storage means and transmitting the read out content to the backup device upon receiving an instruction if backup of the read out content is permitted;

a writing means for writing to the storage means, in association with the content, period information indicating a period during which playback of the content to be backed up is permitted upon receiving an instruction; and

a playback control means for permitting playback of the content within the period indicated by the period information, and prohibiting playback of the content when the period indicated by the period information has ended.

[34] A backup program executed in a recording and playback device that records and plays back content, the recording and playback device having a storage means that stores the content, and the backup program comprising:

a receiving step of receiving an instruction to back up the content;

a content transmitting step for reading the content from the storage means and transmitting the read out content to the backup device upon receiving an instruction if backup of the read out content is permitted;

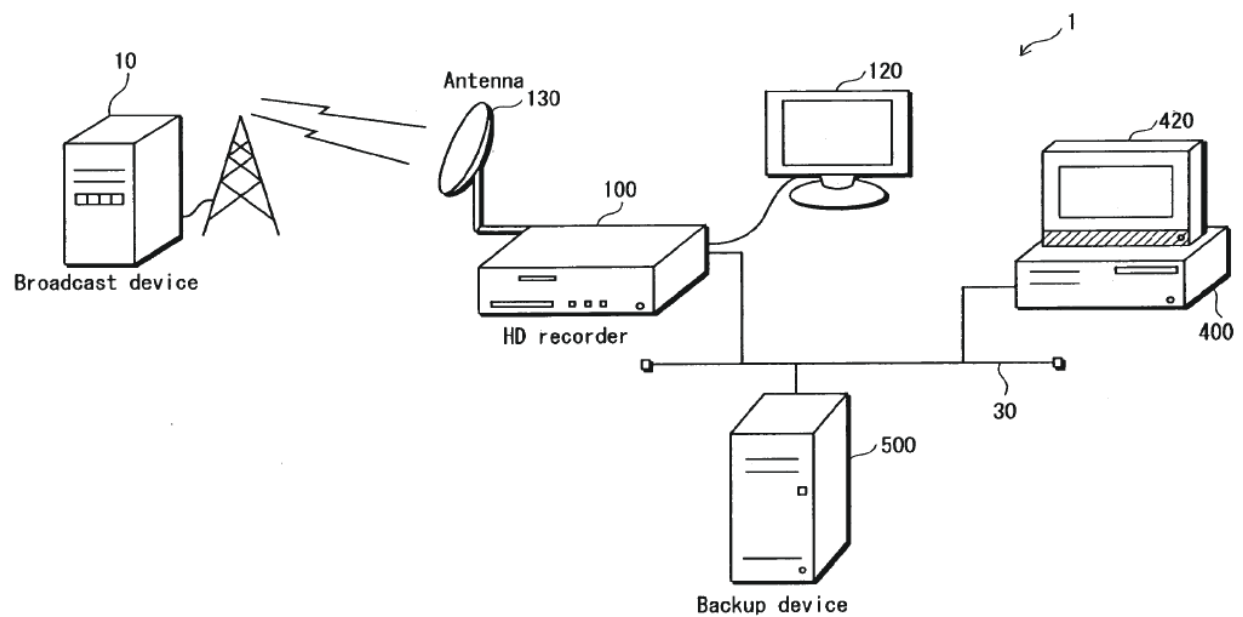
a writing step of writing to the storage means, in association with the content, period information indicating a period during which playback of the content to be backed up is permitted upon receiving an instruction; and

a playback control step of permitting playback of the content within the period indicated by the period information, and prohibiting playback of the content when the period indicated by the period information has ended.

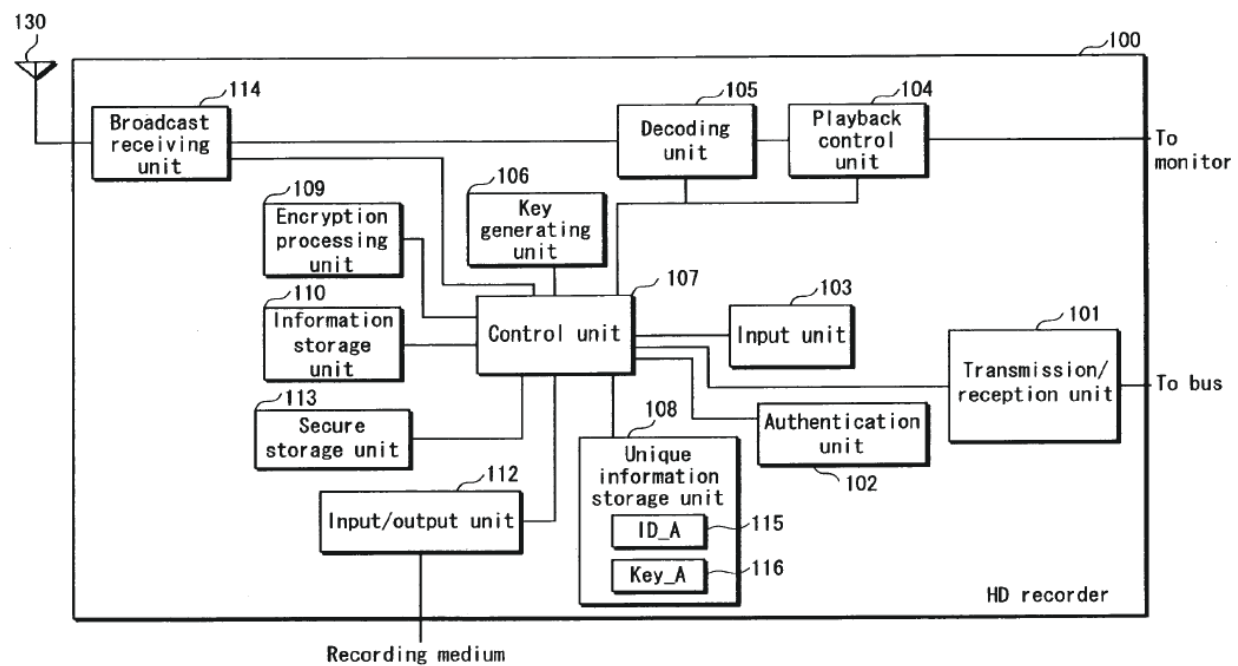
[35] The backup program according to claim 34, wherein the backup program is recorded on a computer-readable recording medium.

1/23

[FIG. 1]

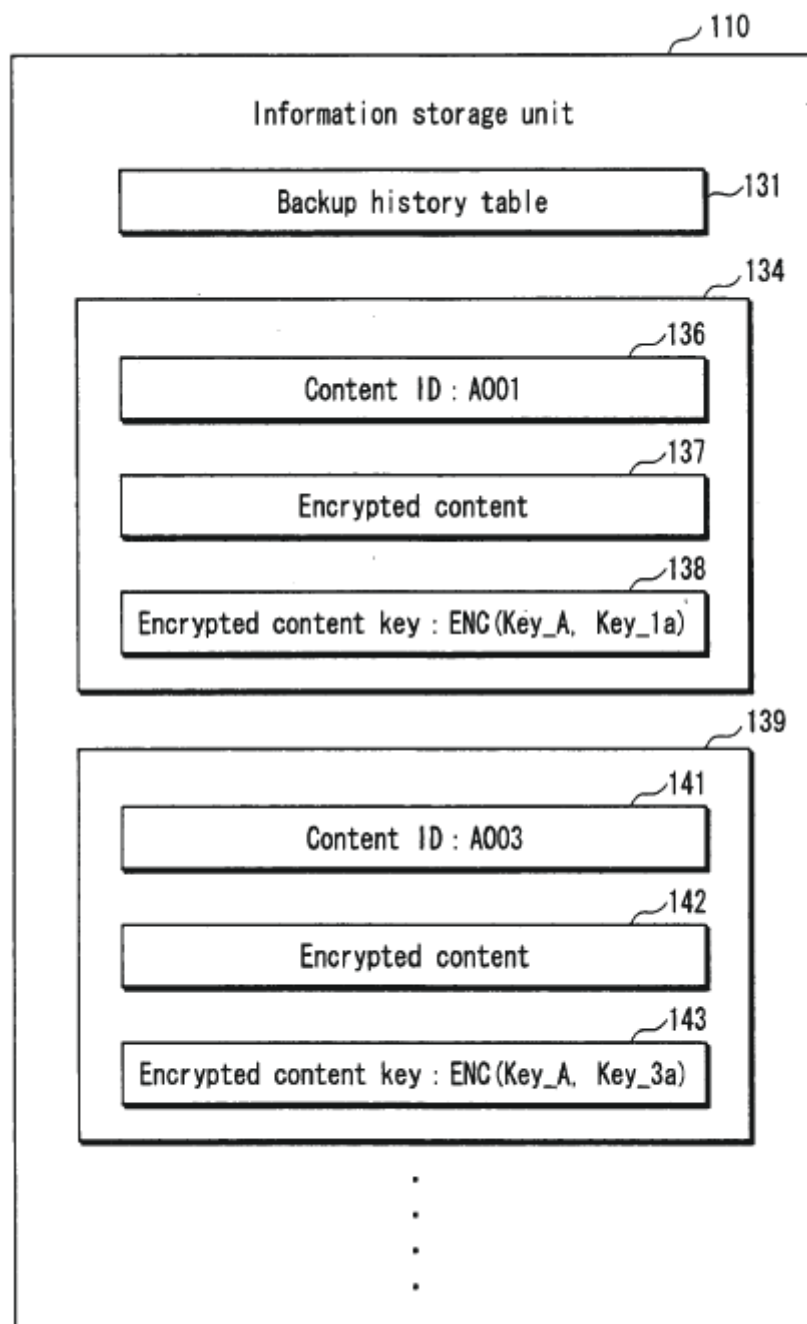


[FIG. 2]



[FIG. 3]

2/23

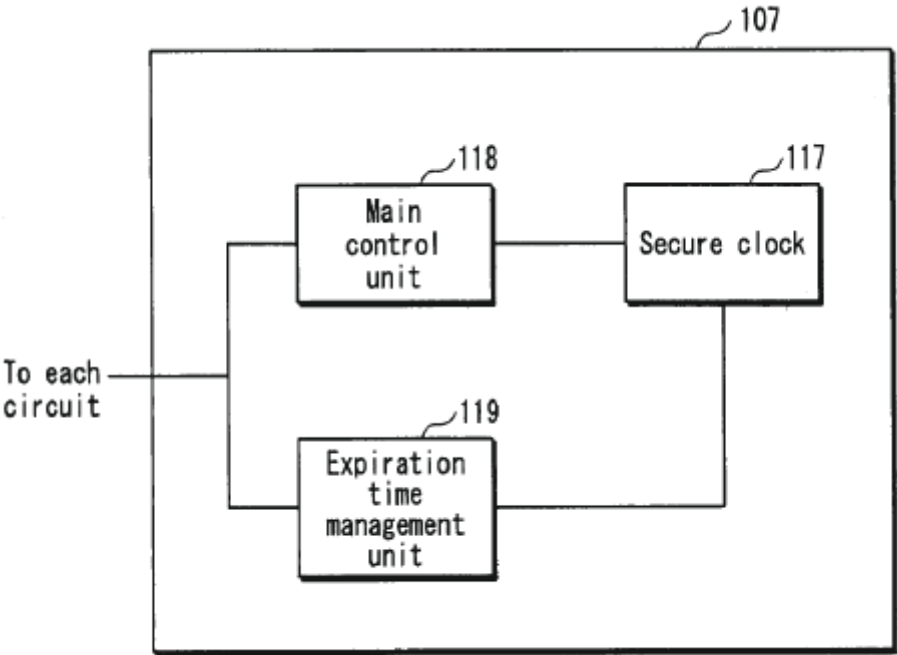


[FIG. 4]

3/23

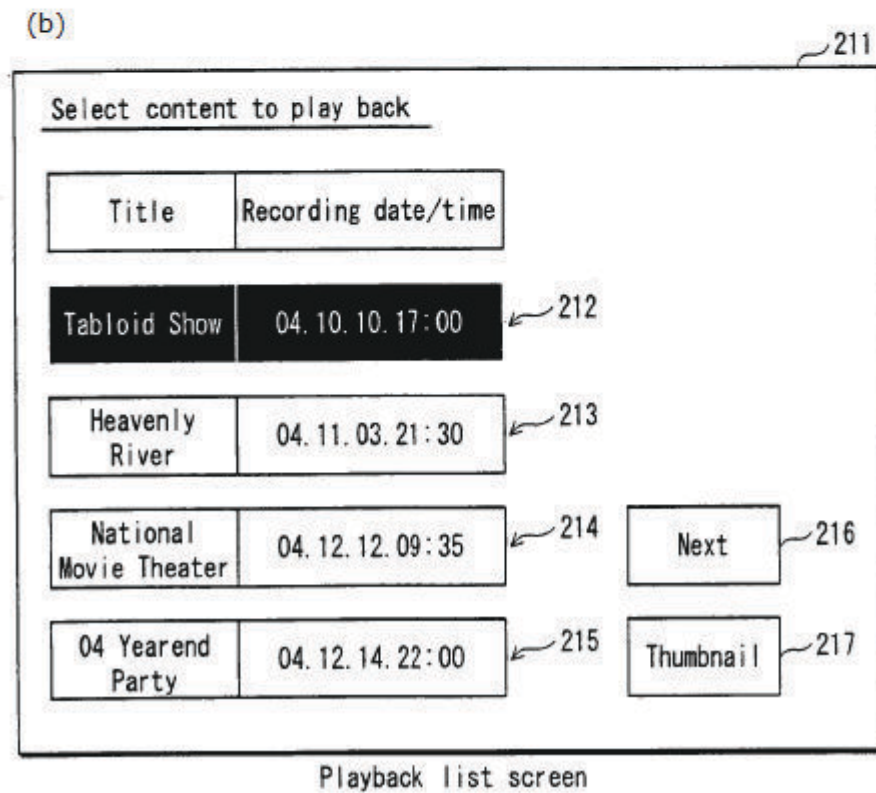
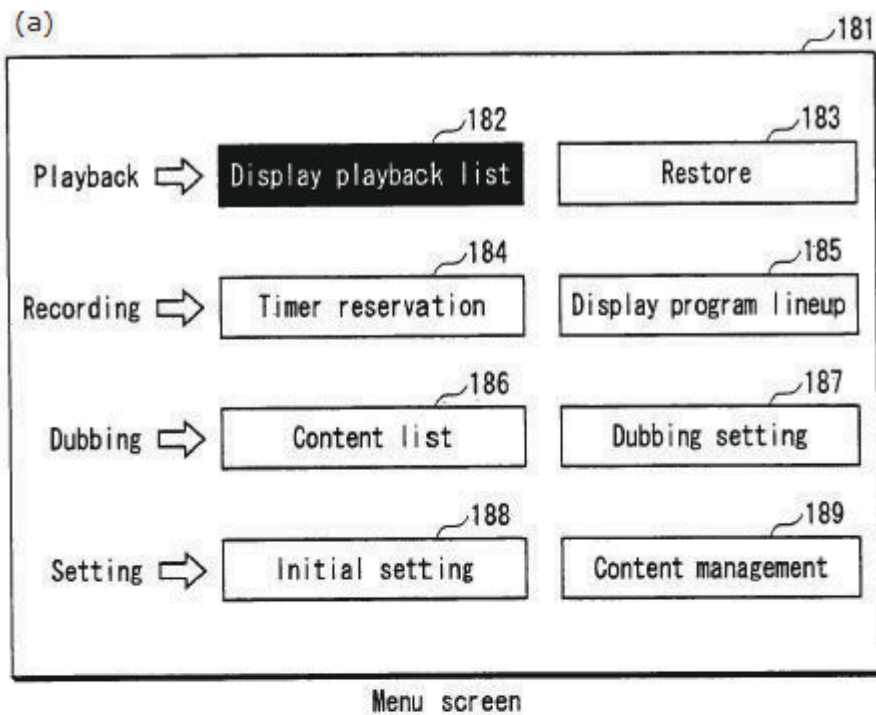
Content information								
Content ID	Title	Recording date/time	Hash value	Type	Compression method	Expiration time	Backup flag	Priority
A001	Tabloid Show	04. 10. 10. 17:00	01a	Broadcast program	MPEG2	04. 12. 15. 17	1	2
A003	04 Yearend Party	04. 12. 12. 09:35	03a	Photo	JPEG	04. 12. 14. 21	1	1
A004	Cat Diary	04. 12. 14. 22:00	04a	Broadcast program	MPEG2	—	0	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

[FIG. 5]



[FIG. 6]

4/23



[FIG. 7]

5/23

(a)

191

Initial setting

192 Channel

193 Image quality

194 Disk

196 Backup

Content type All 197

Backup schedule Sunday 0:30 198

Backup mode Only new 199

Restore mode Manual 201

Initial setting screen

(b)

221

Select content to restore

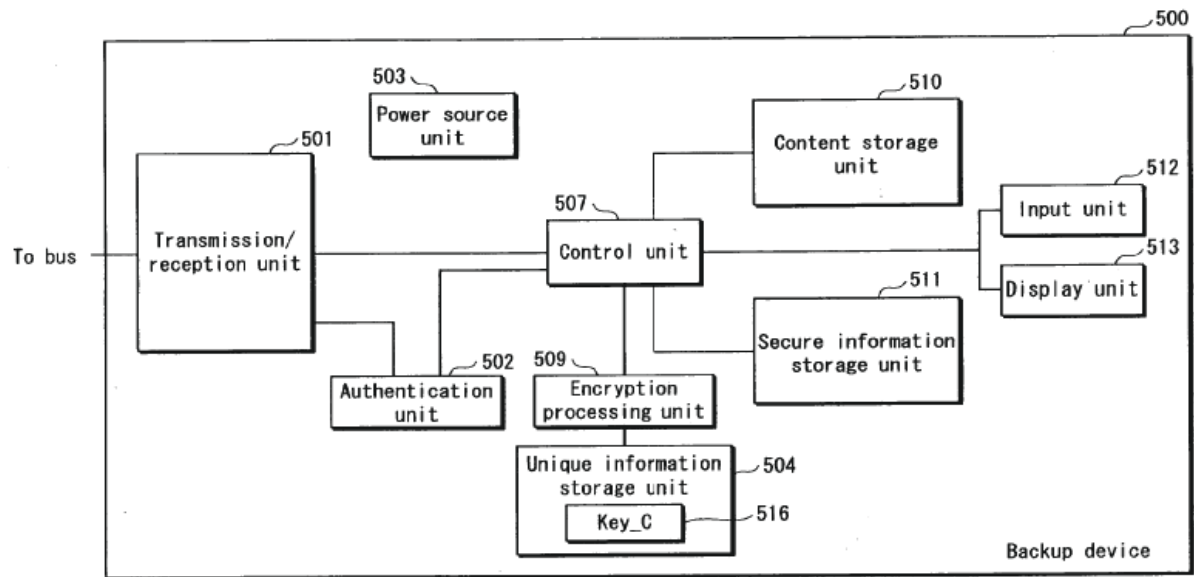
Title	Recording date/time	Recording device
Tabloid Show	04.10.10.17:00	Device A
Heavenly River	04.11.03.21:30	Device A
National Movie Theater	04.12.12.09:35	Device B
04 Yearend Party	04.12.14.22:00	Device A

Next

Restore information screen

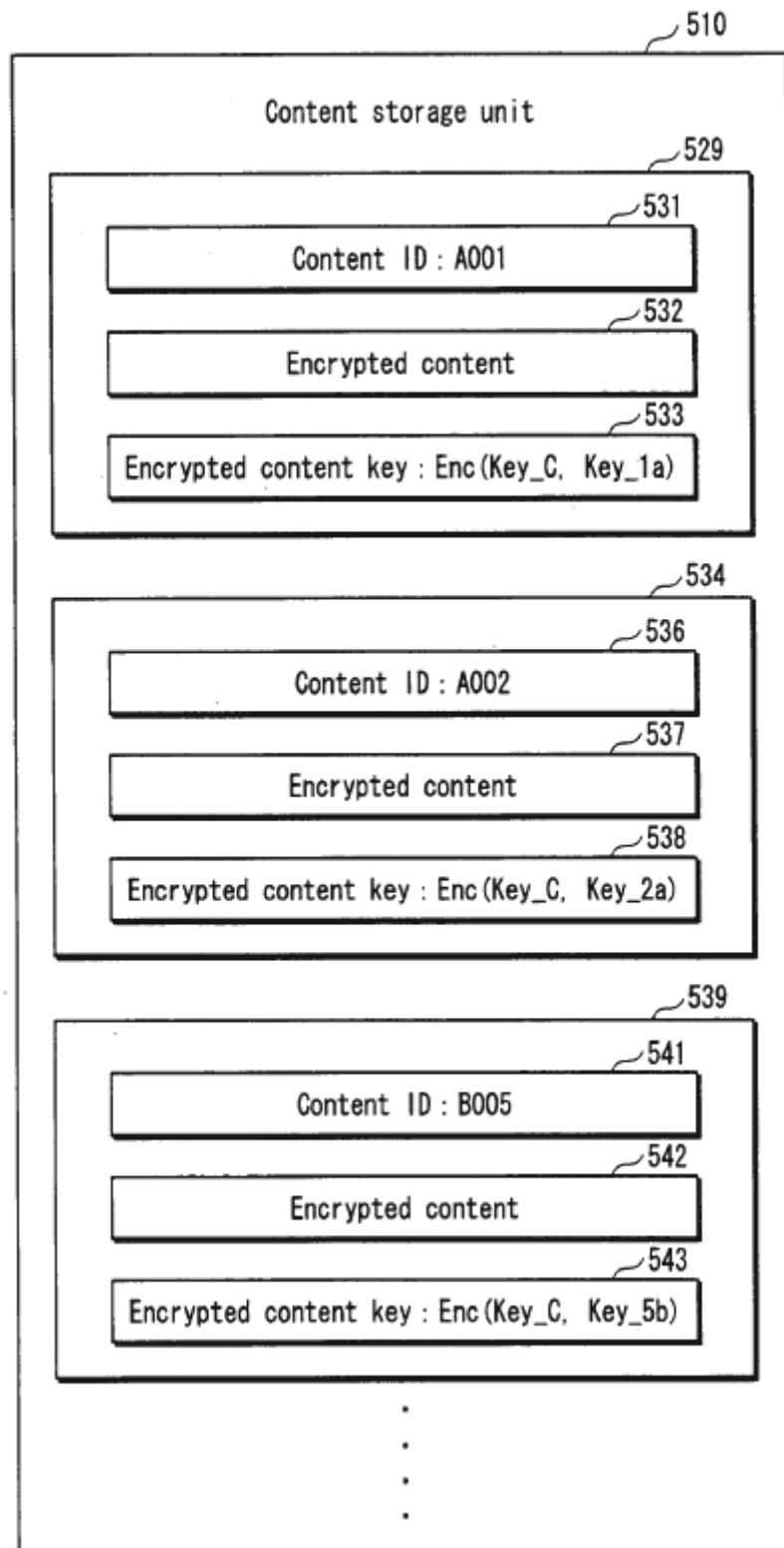
[FIG. 8]

6/23



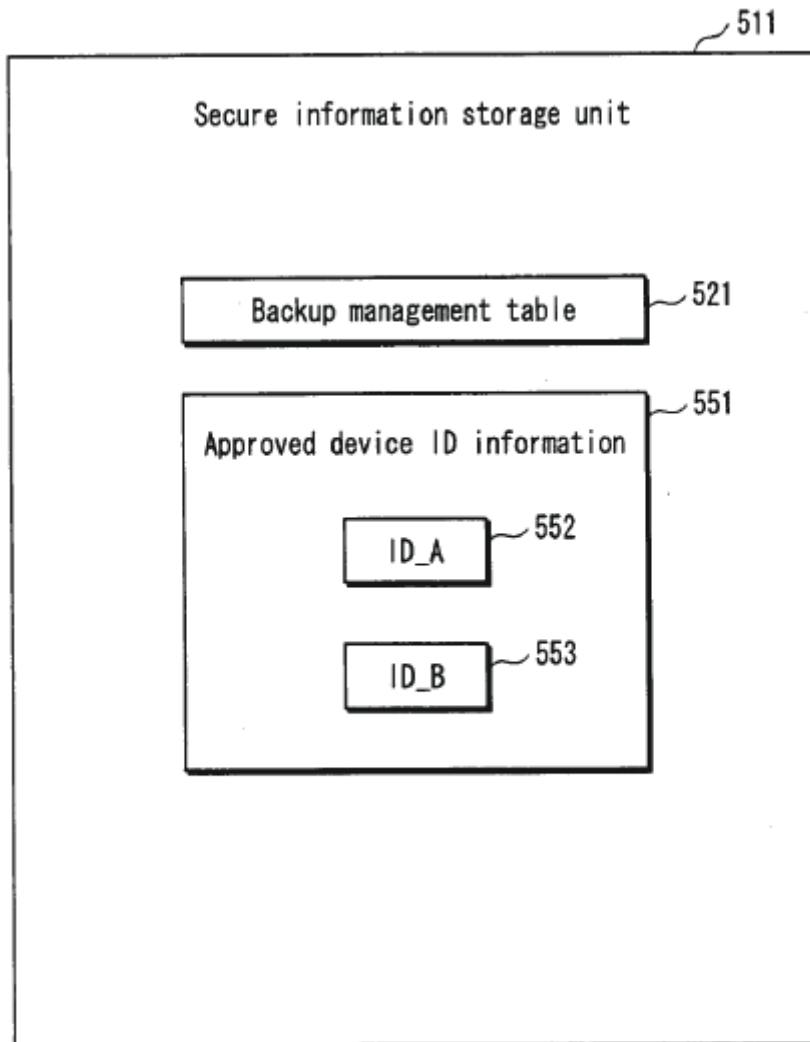
[FIG. 9]

7/23



[FIG. 10]

8/23



[FIG. 11]

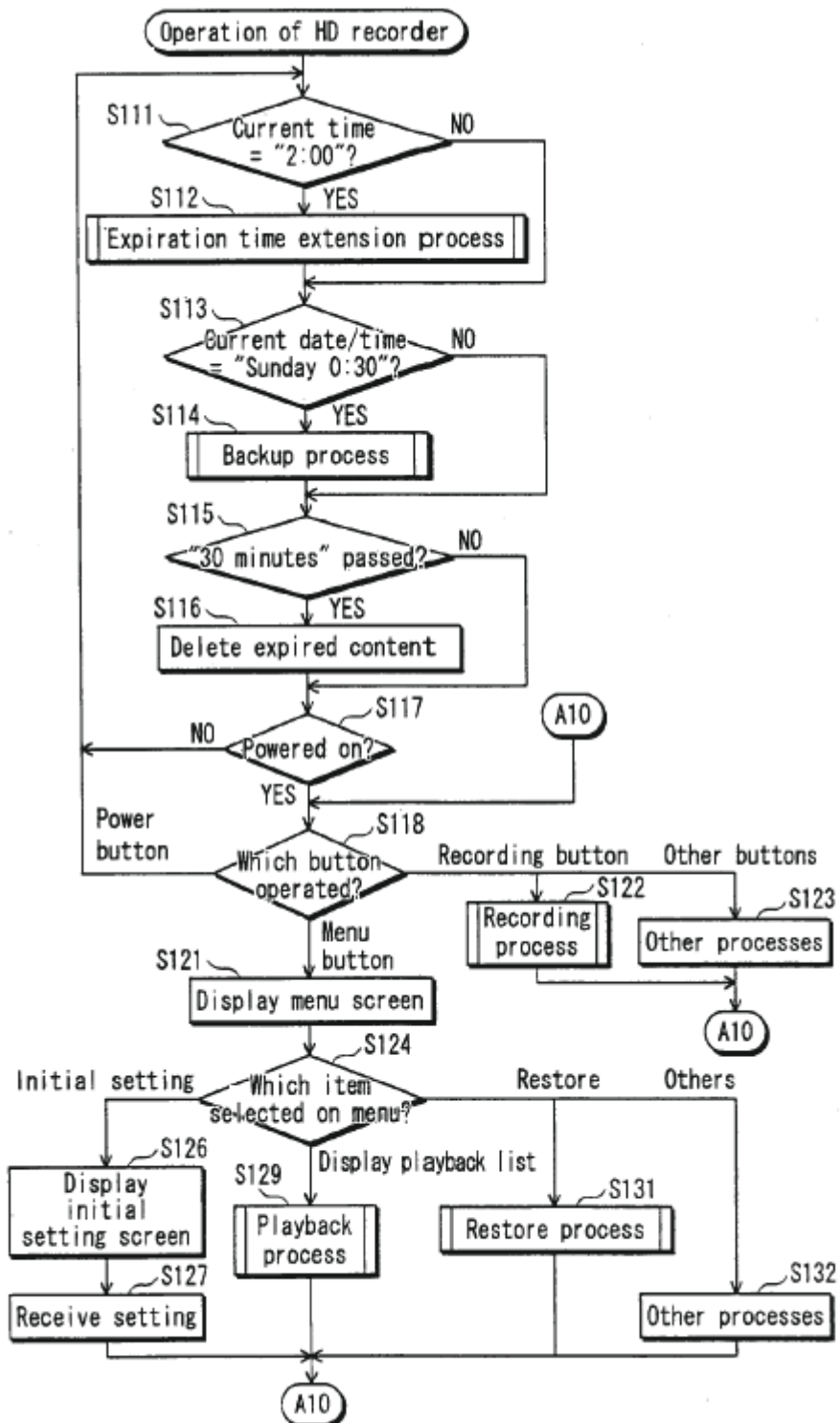
9/23

521

Backup information				
561 Content ID	562 Title	563 Recording date/time	564 Backup source device ID	565 Hash value
522 A001	Tabloid Show	04. 10. 10. 17:00	ID_A	01c
523 A002	Heavenly River	04. 11. 03. 21:30	ID_A	02c
524 B005	National Movie Theater	04. 12. 12. 09:35	ID_B	05c
525 A003	04 Yearend Party	04. 12. 14. 22:00	ID_A	03c
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

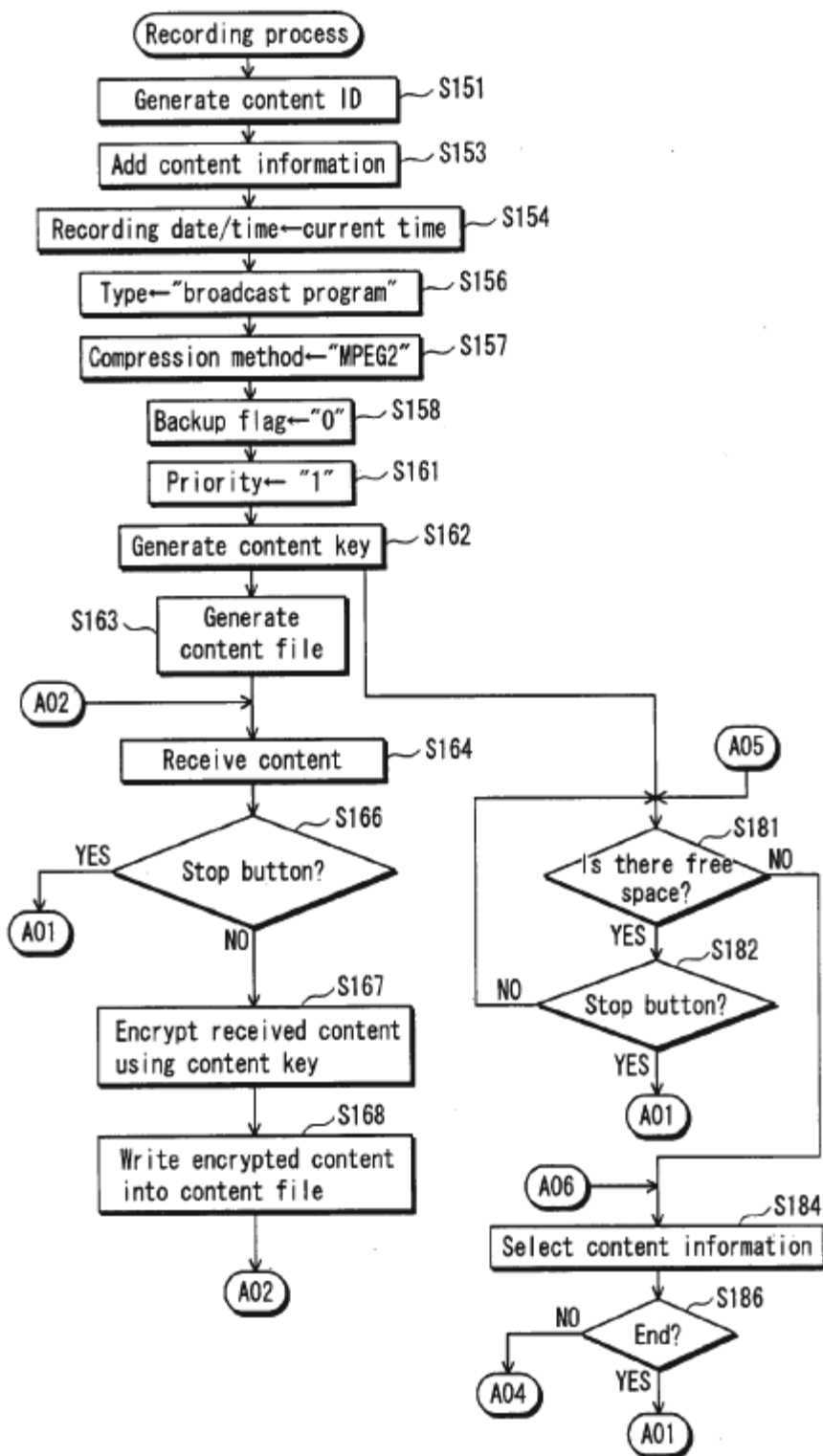
[FIG. 12]

10/23



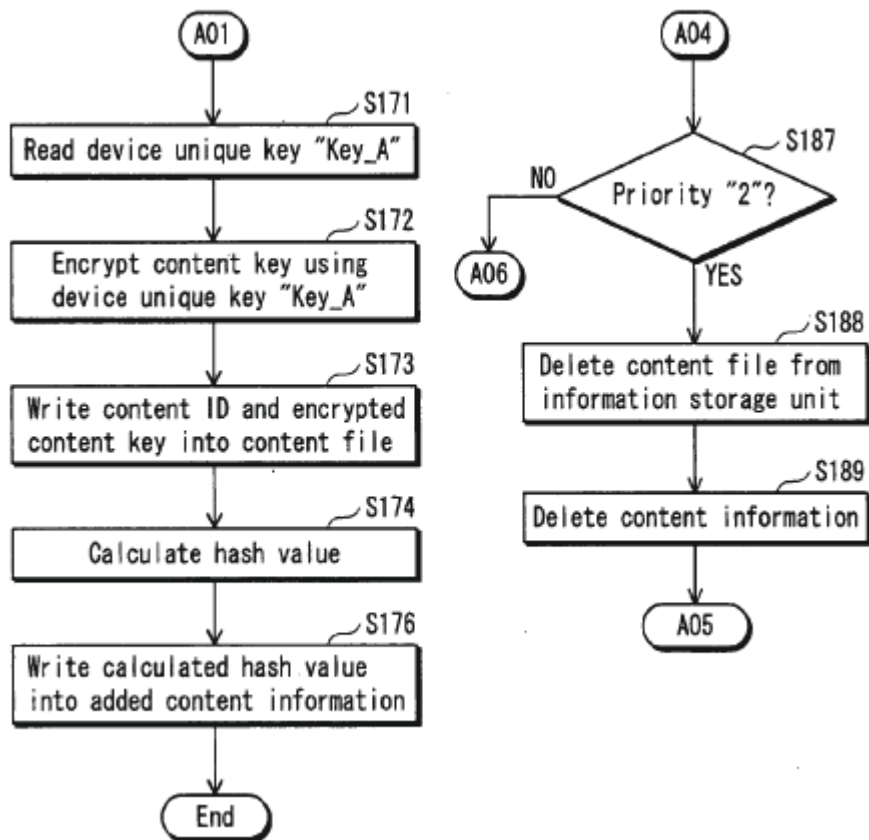
[FIG. 13]

11/23



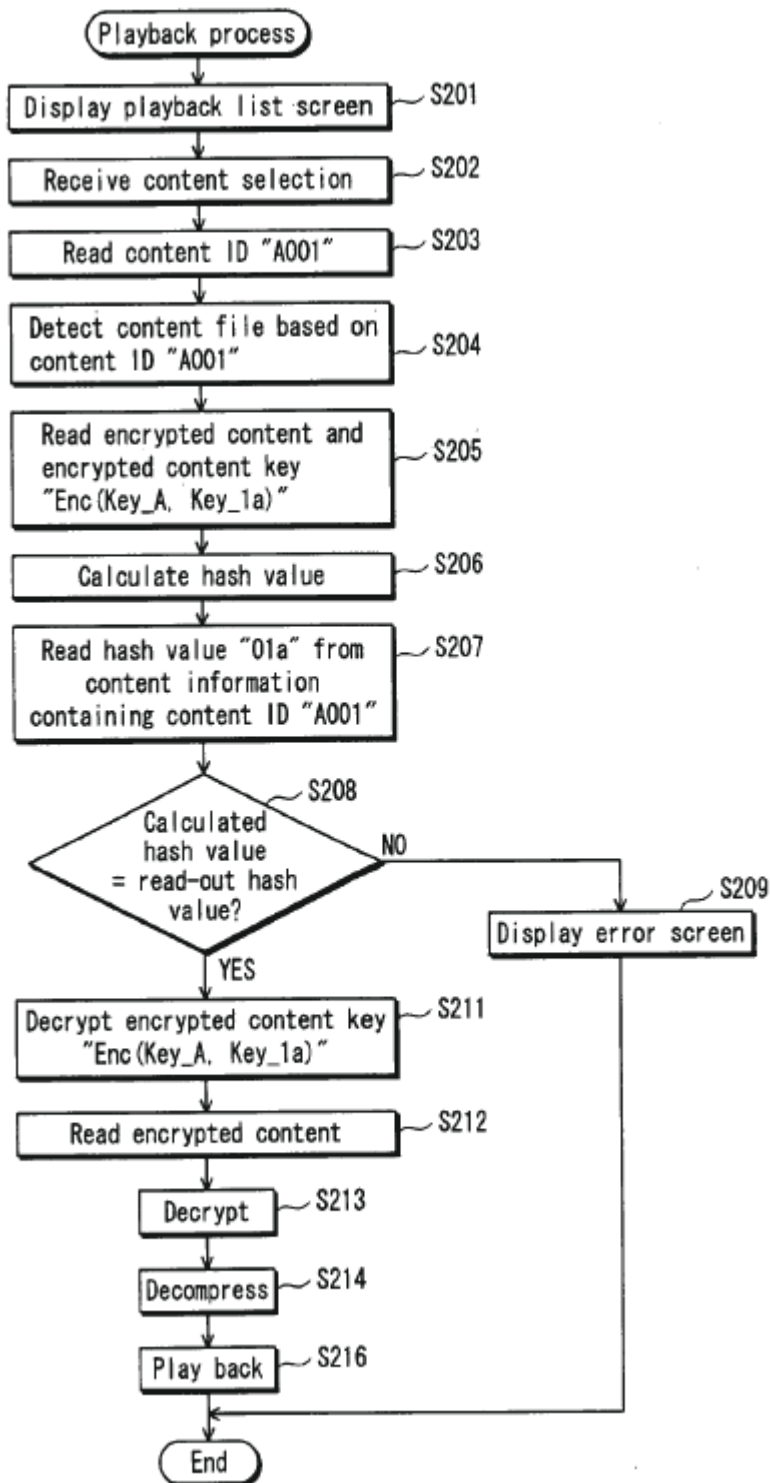
[FIG. 14]

12/23



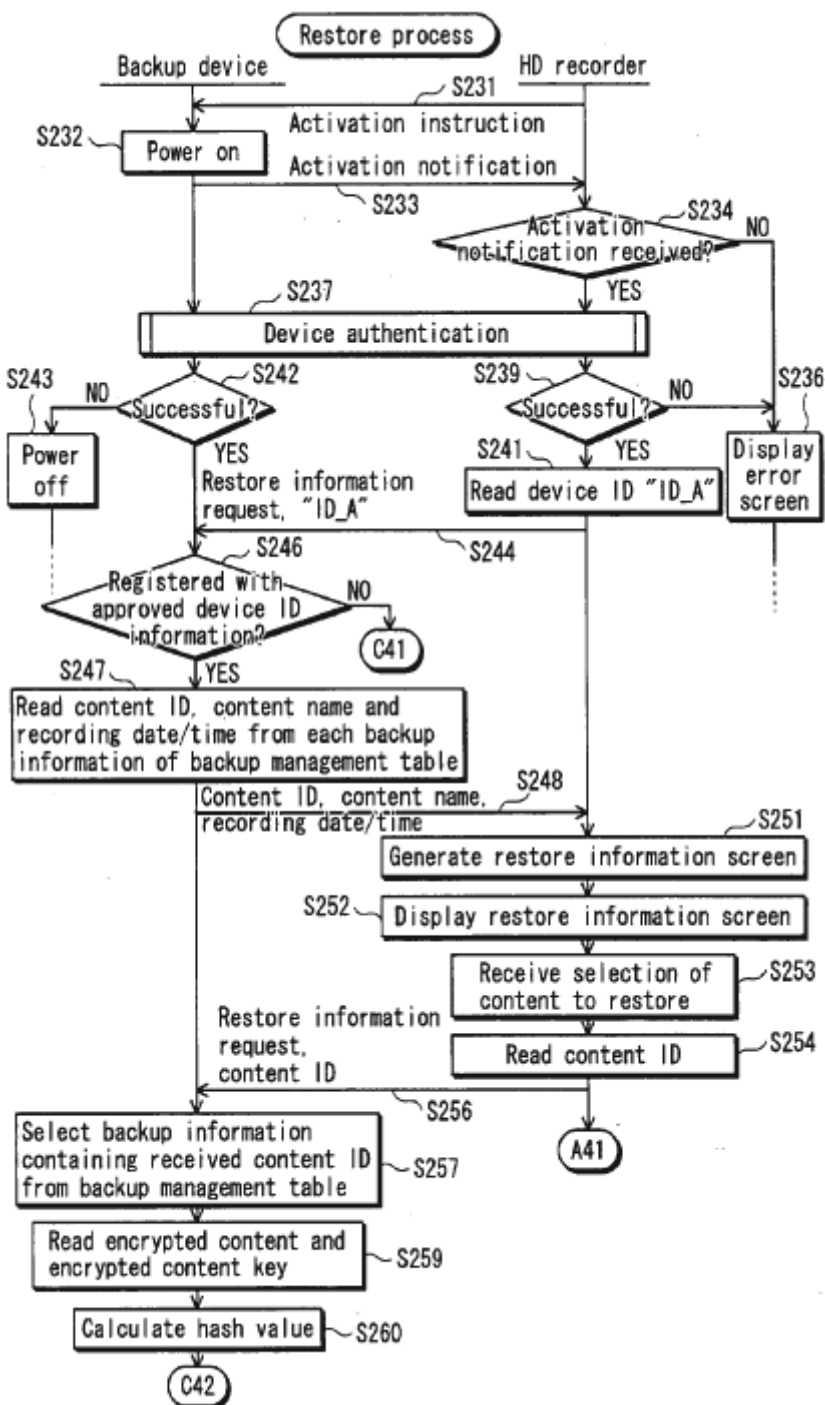
[FIG. 15]

13/23



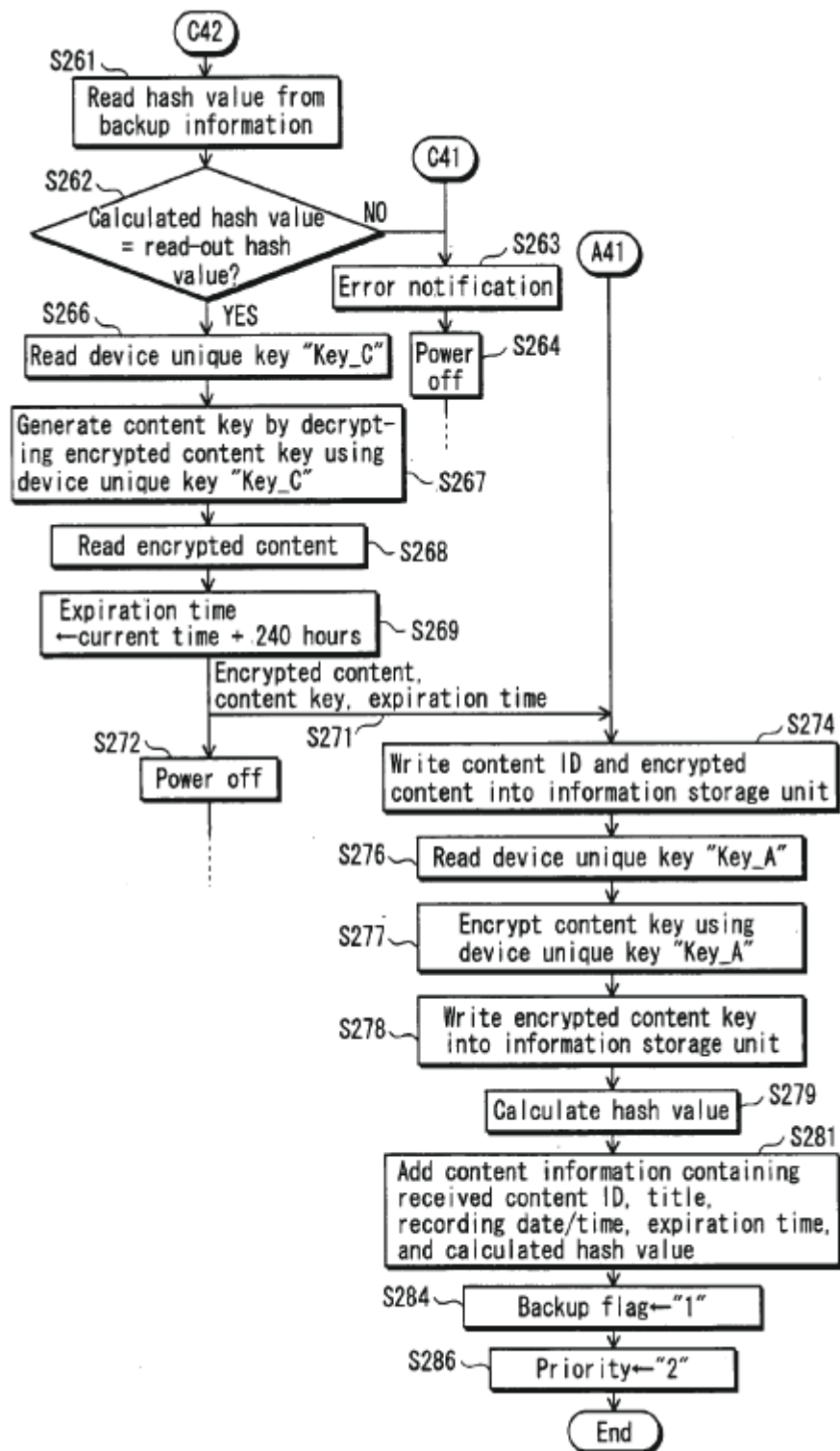
[FIG. 16]

14/23



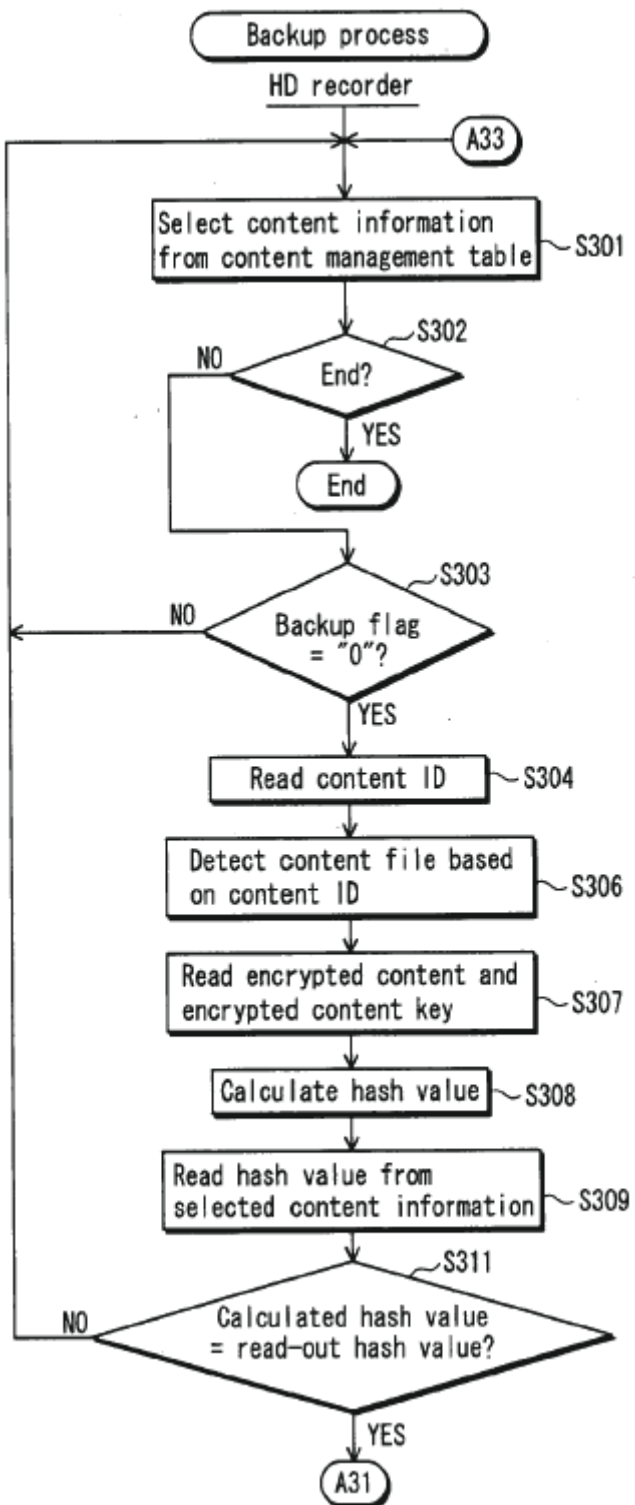
[FIG. 17]

15/23



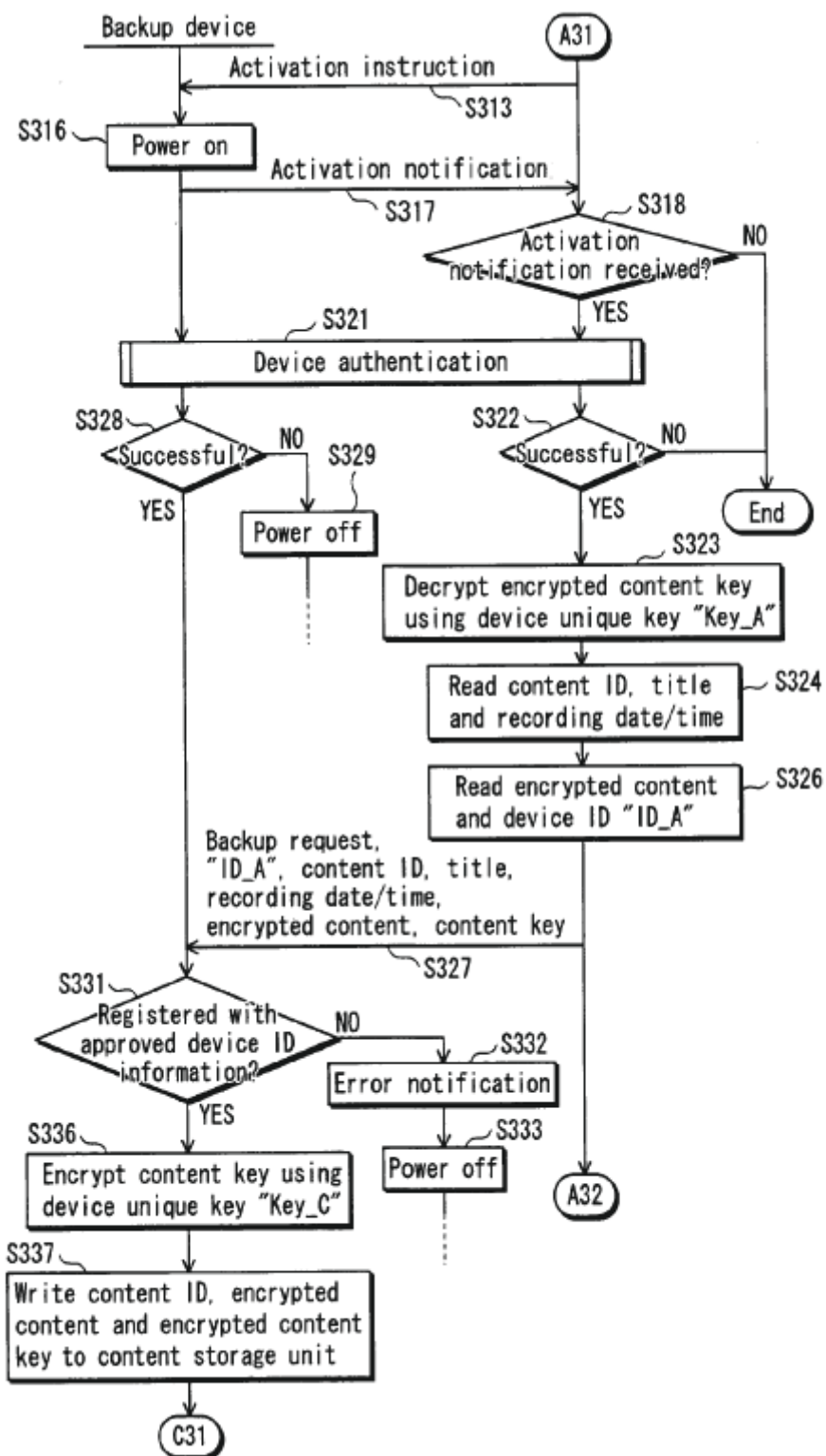
[FIG. 18]

16/23



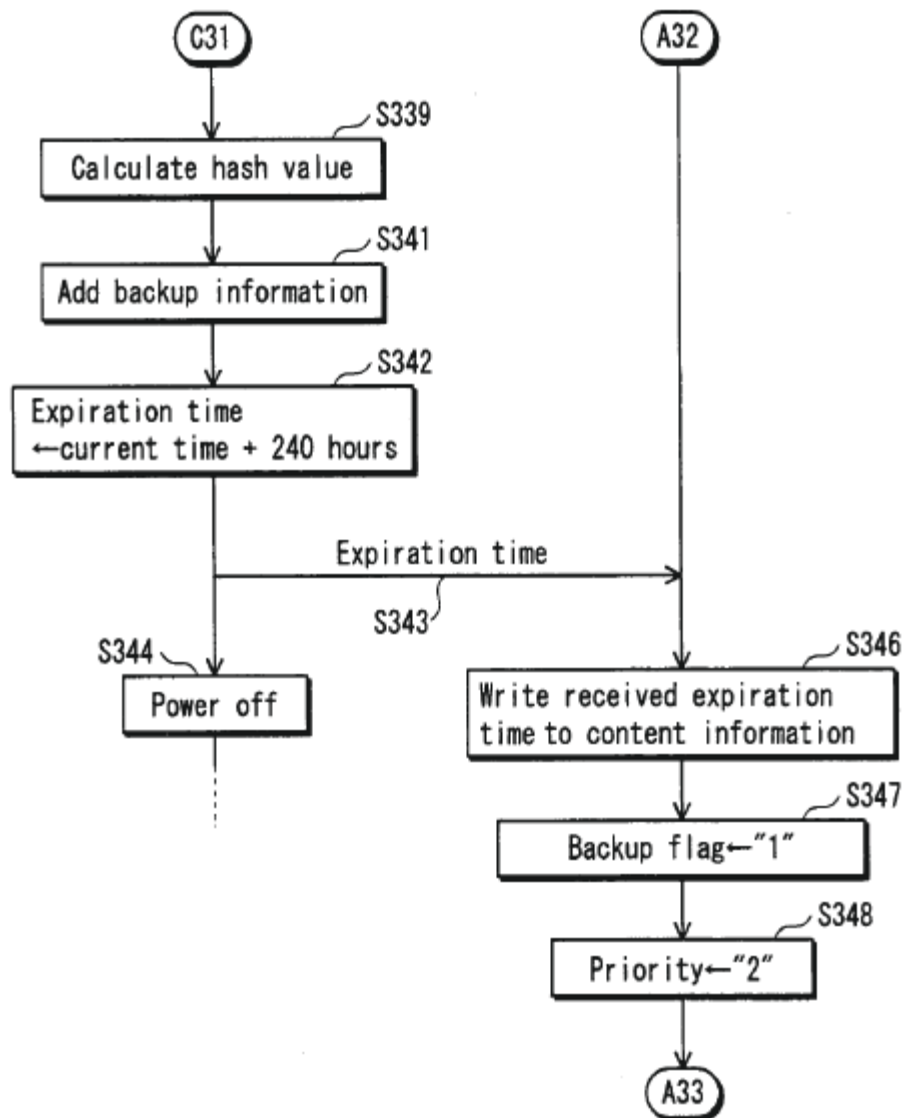
[FIG. 19]

17/23



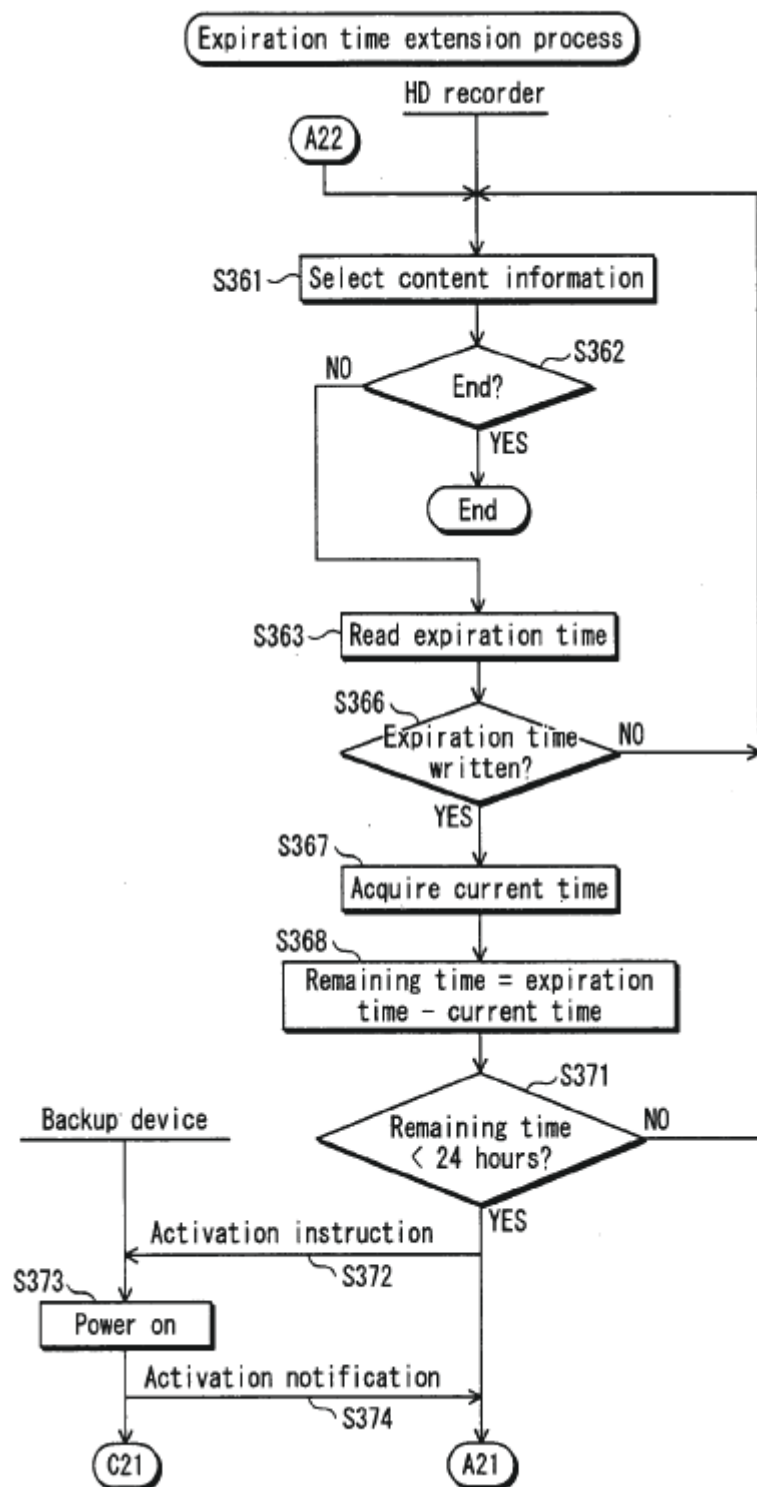
[FIG. 20]

18/23



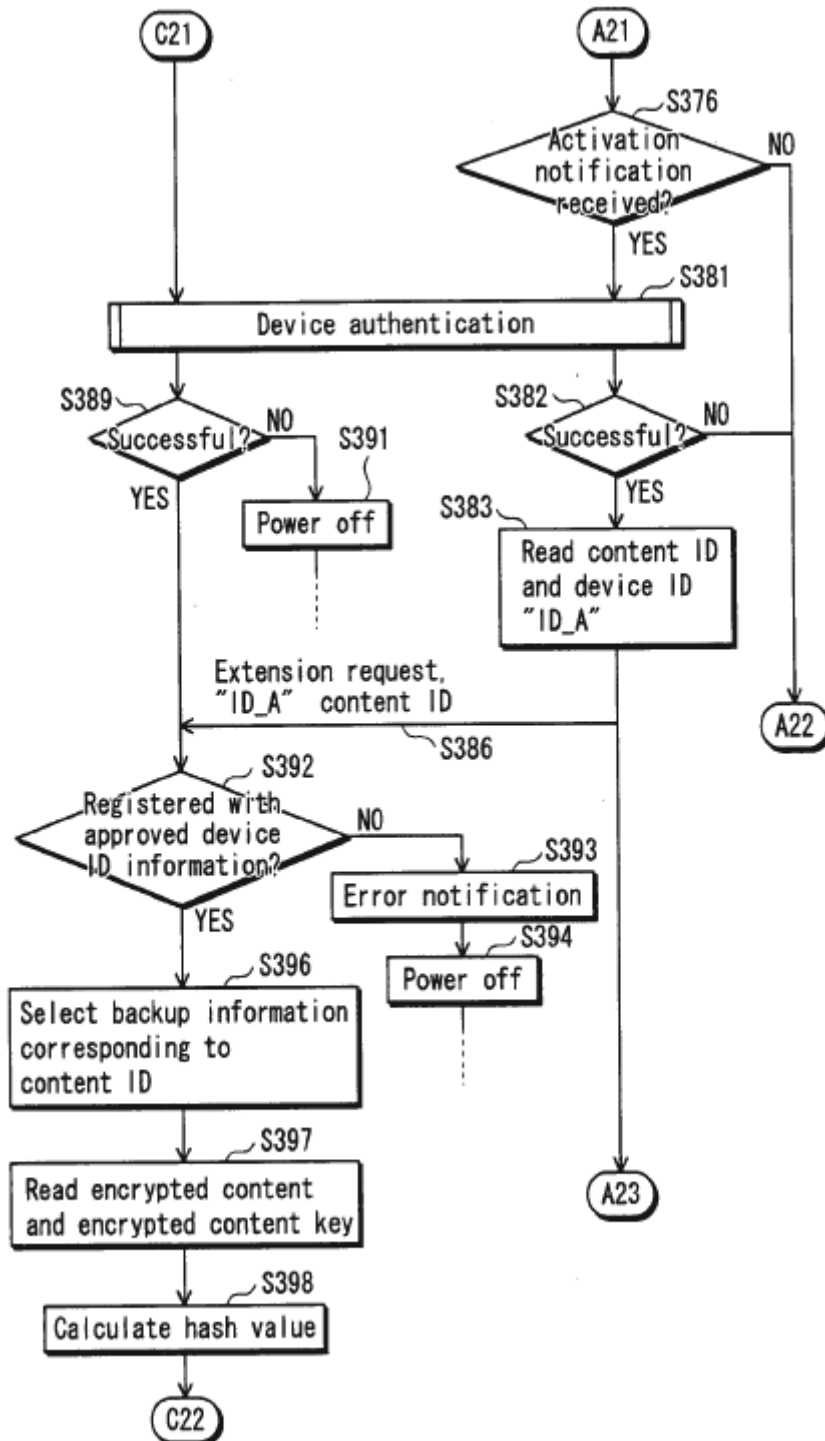
[FIG. 21]

19/23



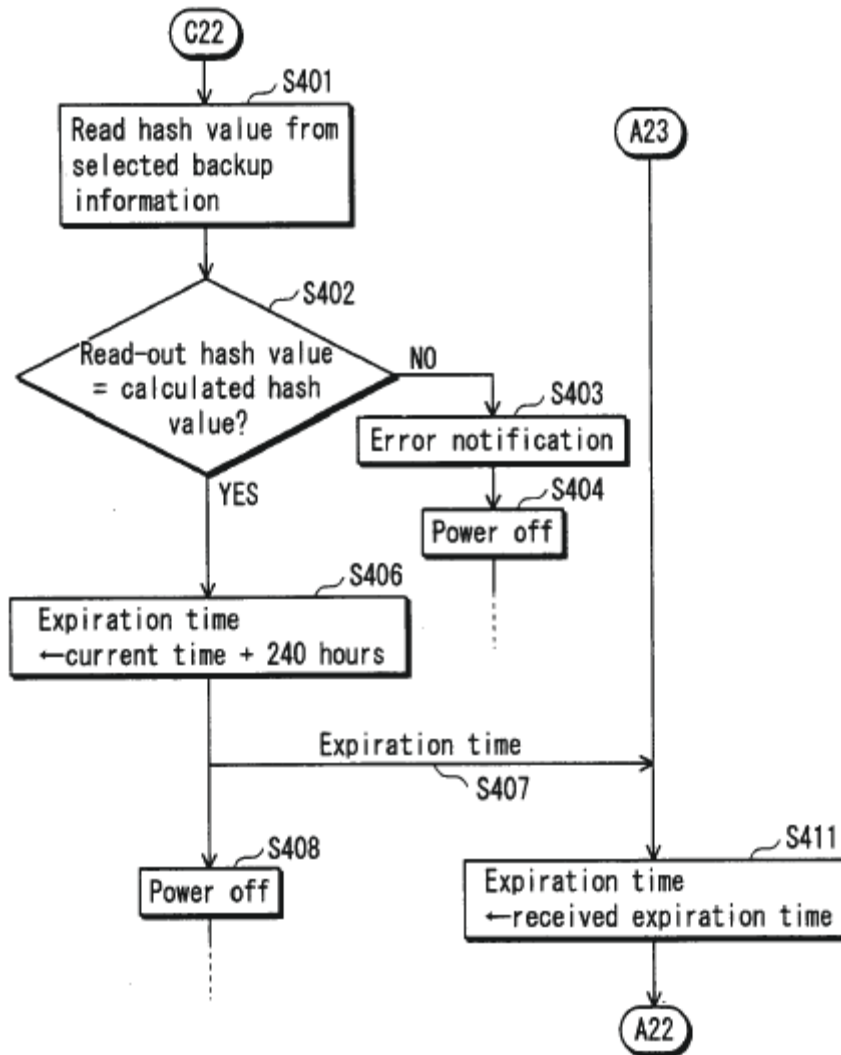
[FIG. 22]

20/23



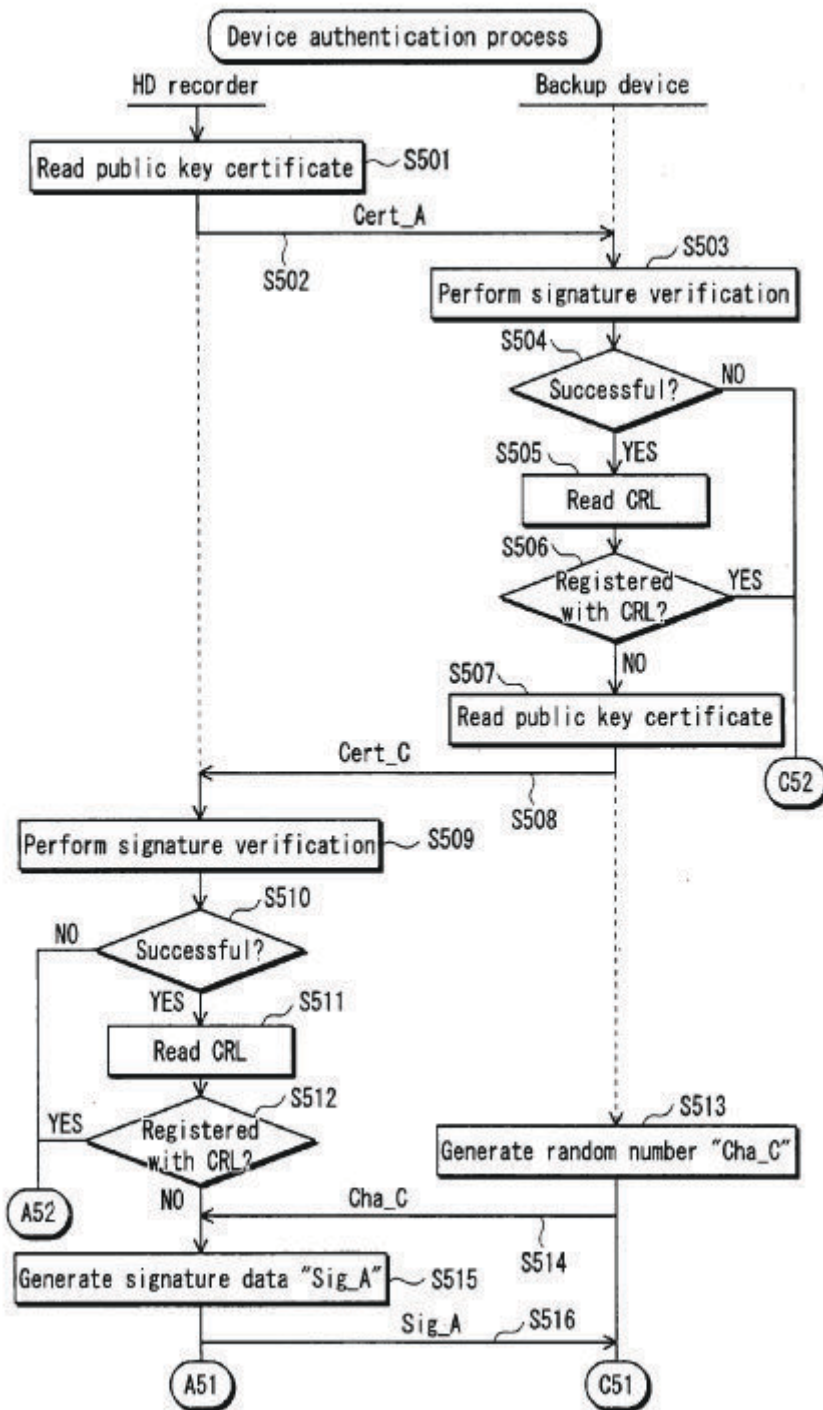
[FIG. 23]

21/23



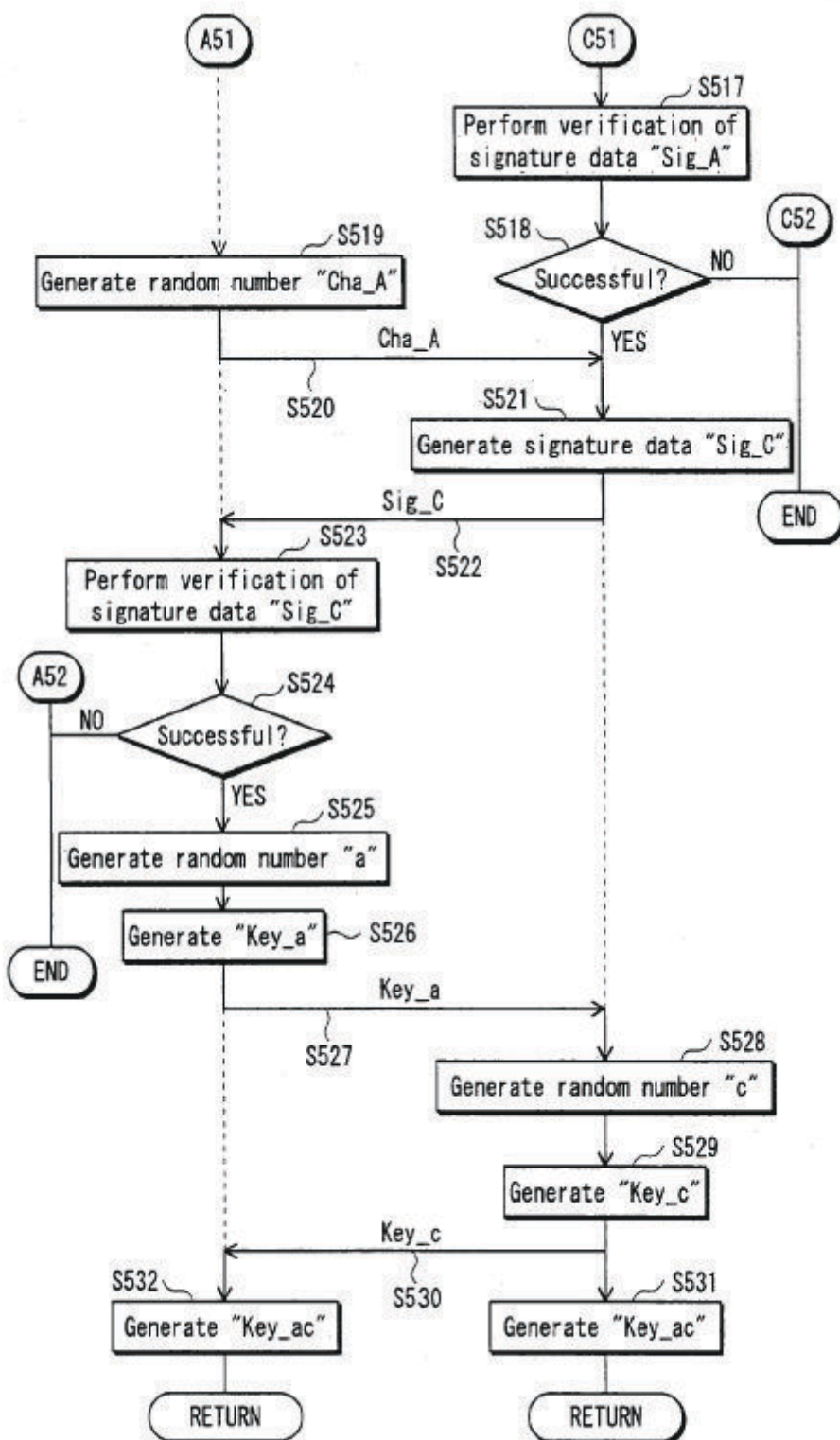
[FIG. 24]

22/23



[FIG. 25]

23/23



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022772

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)

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

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-186751 A (Matsushita Electric Industrial Co., Ltd.), 04 July, 2003 (04.07.03), Par. No. [0298] (Family: none)	19-25, 27-31
Y	JP 11-203127 A (Casio Computer Co., Ltd.), 30 July, 1999 (30.07.99), Abstract (Family: none)	19-25, 27-31
A	JP 8-263440 A (Xerox Corp.), 11 October, 1996 (11.10.96), Par. Nos. [0081] to [0083], [0176] to [0180] & US 5715403 A & EP 0715244 A1	1-35

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 February, 2006 (14.02.06)

Date of mailing of the international search report
21 February, 2006 (21.02.06)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022772

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-14221 A (Victor Company Of Japan, Ltd.), 19 January, 2001 (19.01.01), Par. Nos. [0022] to [0023] & EP 1049087 A2	1-35
A	JP 2004-54988 A (Sony Corp.), 19 February, 2004 (19.02.04), Abstract (Family: none)	1-35
A	JP 2003-30054 A (Sharp Corp.), 31 January, 2003 (31.01.03), Full text; all drawings (Family: none)	1-35

Form PCT/ISA/210 (continuation of second sheet) (April 2005)



TRANSLATION CERTIFICATION

Date: April 22, 2025

To whom it may concern:

I, Frank McGee, personally performed this translation. I am a translator fluent in the Japanese and English languages, on behalf of Morningside, do solemnly and sincerely declare that the following is, to the best of my knowledge and belief, a true and correct translation of the document(s) listed below in a form that best reflects the intention and meaning of the original text.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code

The document is designated as:

- WO2006073040A1

Frank McGee

QUESTEL CONFIDENTIAL

4001 S 700 East, Suite 500 #B17
Salt Lake City, UT 84107

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006年7月13日 (13.07.2006)

PCT

(10) 国際公開番号
WO 2006/073040 A1

(51) 国際特許分類:

G06F 21/24 (2006.01) H04N 5/91 (2006.01)
G11B 20/10 (2006.01) H04N 7/167 (2006.01)
G11B 27/00 (2006.01) H04N 7/173 (2006.01)

Yoshikatsu). 原田 俊治 (HARADA, Shunji). 津坂 優子 (TSUSAKA, Yuko). 藤岡 総一郎 (FUJIOKA, Soichiro). 大森 基司 (OHMORI, Motoji). 中野 稔久 (NAKANO, Toshihisa).

(21) 国際出願番号: PCT/JP2005/022772

(22) 国際出願日: 2005年12月12日 (12.12.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:

特願2005-003152 2005年1月7日 (07.01.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真 1006番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてののみ): 井藤 好克 (ITO,

(74) 代理人: 中島 司朗, 外 (NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目2番1号淀川5番館6F Osaka (JP).

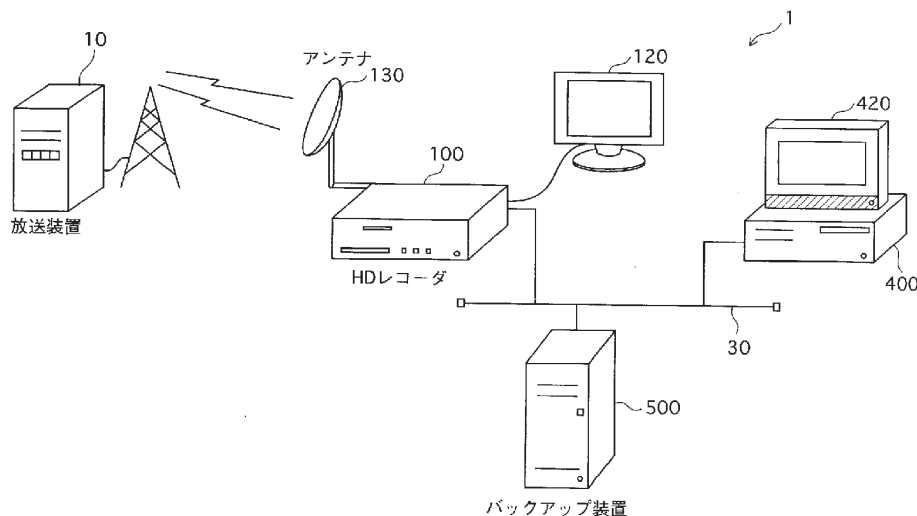
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,

[続葉有]

(54) Title: BACKUP SYSTEM, RECORDING/REPRODUCTION DEVICE, BACKUP DEVICE, BACKUP METHOD, PROGRAM, AND INTEGRATED CIRCUIT

(54) 発明の名称: バックアップシステム、記録再生装置、バックアップ装置、バックアップ方法、プログラム及び集積回路



(57) Abstract: It is impossible to copy a CopyOnce content in an external device even for backup because there is a danger of unauthorized copy if copy for backup is enabled. There is provided an HD recorder (100) for transmitting a content to a backup device (500) and setting an expiration date for the content stored in the HD recorder (100) itself and deleting the content stored in itself upon expiration.

[続葉有]



SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

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

(57) 要約: バックアップが目的であっても、Copy Onceのコンテンツを外部機器などに、複製することができず、利用者にとって不便であるが、バックアップのために複製を認めると、不正に複製される危険性がある。本発明は、HDレコーダ100は、コンテンツをバックアップ装置500へ送信し、同時に、HDレコーダ100自身の記憶しているコンテンツに有効期限を設け、有効期限の過ぎると、自身の記憶しているコンテンツを削除するHDレコーダ100を提供する。

明 細 書

バックアップシステム、記録再生装置、バックアップ装置、バックアップ方法、プログラム及び集積回路

技術分野

[0001] 本発明は、デジタルコンテンツの著作権保護を考慮しつつ、デジタルコンテンツのバックアップを生成する技術に関する。

背景技術

[0002] 近年、デジタルコンテンツを放送する、デジタル放送が開始されている。デジタルコンテンツは、使用に伴う劣化が少ないので、著作権を保護するために、コピー生成の可否及び生成を許可されるコピーの数を示すコピー制御情報(CCI:Copy Control Information)が付加されている。このCCIは、1度だけコピーを許可すること(Copy Once)を示すことが多い。Copy Onceを示すCCIを含むコンテンツを、記録媒体に記録すると、このコンテンツに付加されているCCIは、以後のコピーを禁止することを示す(No More Copy)CCIに書き換えられる。No More Copyを示すCCIを含むコンテンツは、コピーすることはできないが、他の媒体へ移動(MOVE)することは、許可されている。

[0003] CCIが付加されたコンテンツであっても、例えば、ハードディスクレコーダ(以下HDレコーダ)の電源OFF時に、パソコンなどを使用してHDD(ハードディスクドライブ)に記憶されているコンテンツを操作するような不正が行われることがある。このような不正な複製を防ぐために、従来から、予めHDDに記憶されているコンテンツを1方向関数に代入して、不正検出情報を算出して記憶しておき、HDレコーダに電源が投入された際に、HDDに記憶しているコンテンツを1方向関数に代入して、検証情報を生成し、生成した検証情報と記憶している不正検出情報とを比較することで、コンテンツの不正使用を検出する技術が存在する。

[0004] また、コンテンツを一時的に記憶し、所定時間が経過した場合又は再生された場合に、前記コンテンツを消去することで、コピー不可を示すCCIを含むコンテンツのシフト再生を実現し、利用者の利便性を向上させる技術もある。

一方で、HDDは、大容量でランダムアクセスが可能であるため、利用者は、記憶容量を気にせずにデジタル放送により放送されるコンテンツを、HDレコーダに記憶させ、簡単な操作で、記憶されているコンテンツを視聴することができる。

発明の開示

発明が解決しようとする課題

[0005] しかし、HDDは、便利である反面、回転動作、シーク動作を伴って、情報の書き込み及び読み出しを行うため、利用頻度に応じて故障の発生率が上昇する。HDDが、故障すれば、データが消失してしまう恐れがある。このような、HDDの故障によるデータ消失を防止するために、他の記憶媒体、記録装置などにコンテンツをバックアップすることが有効であると考えられる。しかし、バックアップが目的であっても、Copy Onceを示すCCIを含むコンテンツを、他の媒体にMOVEすると、HDレコーダに記憶されていたコンテンツは削除されてしまい、利用者にとっての利便性が損なわれるという問題がある。

[0006] また、バックアップのためにコンテンツの複製を許可すれば、悪意のある利用者により、コンテンツが不正に複製される可能性があり、著作権者の権利を十分に保護できないという問題が発生する。

本発明は、このような問題を鑑みてなされたものであり、著作権の保護と利用者にとっての利便性とを調整しつつ、コンテンツをバックアップすることができるバックアップシステム、記録再生装置、バックアップ装置、バックアップ方法、集積回路、バックアッププログラム、記録媒体を提供することを目的とする。

課題を解決するための手段

[0007] 上記の目的を達成するために、本発明は、コンテンツの記録及び再生をする記録再生装置とバックアップ装置とからなるバックアップシステムであって、前記記録再生装置は、前記コンテンツを記憶している記憶手段と、前記コンテンツのバックアップの指示を受け付ける受付手段と、前記指示を受け付けると、前記コンテンツを前記記憶手段から読み出し、読み出した前記コンテンツをバックアップ装置へ送信するコンテンツ送信手段と、前記指示を受け付けると、前記バックアップの対象である前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前

記記憶手段へ書き込む書込手段と、前記期間情報により示される期間内は、前記コンテンツの再生を許可し、前記期間情報により示される期間が終了すると、前記コンテンツの再生を禁止する再生制御手段とを備え、前記バックアップ装置は、前記記録再生装置から、前記コンテンツを受信するコンテンツ受信手段と、受信した前記コンテンツを記憶するバックアップ記憶手段とを備えることを特徴とする。

- [0008] 本明細書において、「バックアップ」とは、誤操作や障害により、正当な機器の記憶しているコンテンツが消失した場合に備え、バックアップ装置にコンテンツのコピーを記憶させることである。記録再生装置は、通常時は、自身の記憶しているコンテンツを使用し、当該記録再生装置の記憶しているコンテンツが消失した場合、バックアップ装置からコピーを取得し、消失したコンテンツを復旧する。「コンテンツが消失した場合」には、記録再生装置や当該記録再生装置の接続されているネットワーク上の障害、記録再生装置のメモリ不足による削除、誤操作のみならず、利用者の意思によって削除された場合も、復旧の対象になり得るものとする。ただし、他の記録媒体などに、MOVEしたことによりコンテンツが消失した場合、記録再生装置は、バックアップ装置からコンテンツを取得することはできない。

発明の効果

- [0009] 上記の構成によると、前記コンテンツを前記バックアップ装置へ送信するとともに、バックアップの対象となった前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込むので、前記記録再生装置において、前記記憶手段に記憶されている前記コンテンツを再生できる期間が、前記期間情報の示す期間内に限定され、著作権者の権利を保護しつつ、利用者は、前記コンテンツを視聴することができる。従って、著作権の保護と利用者にとっての利便性を調整しつつ、障害対策用にコンテンツをバックアップすることができる。
- [0010] また、本発明は、コンテンツの記録及び再生を行う記録再生装置でもあり、前記コンテンツを記憶している記憶手段と、前記コンテンツのバックアップの指示を受け付ける受付手段と、前記指示を受け付けると、前記コンテンツを前記記憶手段から読み出し、読み出した前記コンテンツのバックアップが許可されていれば、読み出した前記コンテンツをバックアップ装置へ送信するコンテンツ送信手段と、前記指示を受け付け

ると、前記バックアップの対象である前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込む書込手段と、前記期間情報により示される期間内は、前記コンテンツの再生を許可し、前記期間情報により示される期間が終了すると、前記コンテンツの再生を禁止する再生制御手段とを備えることを特徴とする。

[0011] この構成によると、前記コンテンツを前記バックアップ装置へ送信するとともに、バックアップの対象となった前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込み、前記再生制御手段が、前記期間情報により示される期間が終了すると、前記コンテンツの再生を禁止するので、前記記憶手段に記憶されている前記コンテンツを再生できる期間が、前記期間情報の示す期間内に限定される。従って、著作権の保護と利用者にとっての利便性のバランスをとりつつ、障害対策用にコンテンツをバックアップすることができる。

[0012] 前記記録再生装置は、さらに、前記バックアップ装置へ、前記期間情報の示す期間の延長許可を求める延長要求を送信する延長要求手段と、前記バックアップ装置から前記延長の許可を示す延長許可情報を受信し、前記期間情報の示す期間を延長する延長手段とを備える。

この構成によると、前記延長手段は、前記バックアップ装置から前記延長の許可を示す延長許可情報を受信し、前記期間情報の示す期間を延長する。これにより、利用者は、バックアップ当初の前記期間情報の示す期間の終了後も、前記記録再生装置に記憶されているコンテンツを視聴することができる。

[0013] また、前記記録再生装置は、前記バックアップ装置に前記延長要求を送信し、延長許可情報を受信した場合に、期間情報を延長する。ここで、前記バックアップ装置において、前記延長要求が所定の条件、例えば、特定の規格に準拠した機器から送信されたものであること、を満たしている場合にのみ延長許可情報を送信するように設定すると想定する。このようにすれば、前記期間情報を延長することができる機器を、所定の条件を満たす機器にのみ限定することができる。

[0014] 前記記録再生装置において、前記延長要求手段は、前記期間情報の示す期間の終了する時点よりも所定時間前に、前記延長要求を送信することを特徴とする。

この構成では、前記延長要求手段は、前記期間情報の示す期間の終了する時点よりも所定時間前の時点に、前記延長要求を送信するため、前記記録再生装置において、コンテンツの視聴を許可される期間が途切れることがない。

[0015] 前記記録再生装置において、前記延長要求手段は、前記期間情報の示す期間内に、定期的に前記延長要求手段要求を繰り返し送信することを特徴とする。

この構成によると、何らかの不具合により、送信が失敗した場合でも、前記延長要求手段は、繰り返し前記延長要求を送信するため、確実に、前記期間情報の示す期間を延長することができる。

[0016] 前記記録再生装置において、前記延長手段は、前記記憶手段に記憶されている前記期間情報よりも後の期間を示す前記延長許可情報を受信し、前記期間情報の示す期間を受信した前記延長許可情報の示す期間に書き換えることにより、前記期間情報を延長することを特徴とする。

この構成によると、前記延長手段は、前記期間情報の示す期間を、受信した前記延長許可情報の示す期間に置き換えるだけで、迅速かつ容易に、前記期間情報を延長することができる。

[0017] 前記記録再生装置を構成する前記延長手段は、予め、延長時間を記憶しており、前記延長時間を前記期限情報の示す期間に付加することにより、前記期間情報を延長することを特徴とする。

ホームネットワーク、社内LANなどを想定した場合、前記バックアップ装置は、ネットワークに接続された各機器から、前記延長要求を受信し、延長を許可するか否かを判定し、延長許可情報を送信する。

[0018] 上記の構成では、前記延長手段は、予め、記憶している延長時間を、前記期限情報の示す期間に付加することにより、前記期間情報を延長する。このように、前記記録再生装置において、前記期間に前記延長期間を付加する演算を行うことで、バックアップ装置の実行する処理を軽減することができる。さらに、本発明では、有効期間の管理及び延長に関する演算を当該記録再生装置が行うため、バックアップ装置が、外部の操作から保護された時計を備える必要がない。

[0019] 前記期間情報は、前記記憶手段に記憶されている前記コンテンツの再生が許可さ

れる期間の終了する時点を示し、前記記録再生装置を構成する前記再生制御手段は、現在時刻が前記期間情報の示す時点より前であれば、前記コンテンツの再生を許可し、現在時刻が前記期間情報の示す時点よりも後であれば、前記コンテンツの再生を禁止することを特徴とする。

[0020] この構成によると、前記再生制御手段は、現在時刻と前記終了時刻とを比較することにより、容易に前記コンテンツの再生の許可及び禁止を決定することができる。

前記期間情報は、前記記憶手段に記憶されている前記コンテンツの再生が許可される時間長を示す許可時間と、前記コンテンツの再生が許可される期間の開始時点を示す開始時刻であり、前記記録再生装置は、前記再生制御手段が、前記開始時刻からの経過時間を取得し、取得した前記経過時間が前記許可時間以下であれば、前記コンテンツの再生を許可し、前記開始時間からの経過時間が前記許可時間を超えていれば、前記コンテンツの再生を禁止することを特徴とする。

[0021] この構成によると、前記期間情報は、前記記憶手段に記憶されている前記コンテンツの再生が許可される時間長を示す許可時間と、前記コンテンツの再生が許可される期間の開始時点を示す開始時刻である。前記期間情報の示す期間は、前記バックアップ装置へ、前記コンテンツをバックアップした時点から、所定時間の間であると考えられる。書込手段は、前記指示を受け付けた時点の現在時刻を取得し、取得した現在時刻を開始時刻とすることによって、容易に、前記開始時刻を取得し、前記記憶手段に書き込むことができる。

[0022] 前記記録再生装置において、前記再生制御手段は、前記記憶手段から前記コンテンツを削除することによって、前記コンテンツの再生を禁止することを特徴とする。

この構成では、前記再生制御手段は、前記記憶手段から前記コンテンツを削除するため、前記期限情報の示す期間の終了後の前記コンテンツの再生を、確実に、禁止することができる。

[0023] 本発明の記録再生装置は、さらに、前記バックアップ装置の記憶している前記コンテンツの取得を示すリストア指示を取得するリストア指示取得手段と、前記リストア指示を取得すると、前記バックアップ装置へ、前記バックアップ装置の記憶している前記コンテンツの送信要求を送信するリストア要求手段と、前記バックアップ装置から、

前記コンテンツを受信し、受信した前記コンテンツを前記記憶手段に書き込むリストア手段とを備え、前記コンテンツが書き込まれると、前記書込手段は、さらに、前記リストア手段により書き込まれた前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段に書き込むことを特徴とする。

[0024] この構成によると、前記リストア手段は、前記バックアップ装置から、前記コンテンツを受信し、受信した前記コンテンツを前記記憶手段に書き込む。これにより、利用者は、再度、前記コンテンツを視聴できるようになる。

さらに、前記コンテンツを受信すると、前記書込手段は、前記リストア手段の書き込んだ前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段に書き込むため、前記記録再生装置において、取得した前記コンテンツを再生できる期間を限定することができる。

[0025] 前記記録再生装置において、前記記憶手段に記憶されている前記コンテンツは、暗号鍵に基づいて、デジタル著作物を暗号化して生成された暗号化著作物と前記暗号化著作物の復号に用いられる復号鍵とを含んで構成され、前記再生制御手段は、前記コンテンツに含まれる前記復号鍵を削除することによって、前記コンテンツの再生を禁止することを特徴とする。

[0026] この構成では、前記コンテンツに含まれる暗号化著作物は、デジタル著作物を暗号鍵により暗号化して生成されているため、不正な利用者により、前記暗号化著作物が複製された場合でも、前記復号鍵がなければ、前記デジタル著作物を生成することができず、前記コンテンツの不正な再生を防止することができる。

前記記録再生装置は、さらに、前記バックアップ装置の記憶している前記復号鍵の取得を示すリストア指示を取得するリストア指示取得手段と、前記リストア指示を取得した場合に、前記バックアップ装置へ、前記バックアップ装置の記憶している前記復号鍵の送信要求を送信するリストア要求手段と、前記バックアップ装置から、前記復号鍵を受信し、受信した前記復号鍵を前記記憶手段に書き込むリストア手段とを備え、前記復号鍵が書き込まれると、前記書込手段は、さらに、前記記憶手段に記憶されている前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段に書き込むことを特徴とする。

- [0027] この構成では、前記リストア手段は、前記復号鍵を受信し、受信した復号鍵を前記記憶手段に書き込む。これにより、利用者は、再び前記記録再生装置に記憶されているコンテンツを視聴することができる。また、前記書込手段は、前記記憶手段の記憶している前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段に書き込むため、前記記録再生装置において、前記コンテンツの再生が許可される期間を限定することができる。
- [0028] 本発明の記録再生装置において、前記記憶手段に記憶されている前記コンテンツは、暗号鍵を用いてデジタル著作物を暗号化して生成された暗号化著作物と、前記暗号化著作物の復号に用いられる復号鍵を当該記録再生装置に固有の固有鍵を用いて暗号化して生成された暗号化鍵とを含み、前記再生制御手段は、前記記憶手段から前記暗号化鍵を削除することにより前記コンテンツの再生を禁止することを特徴とする。
- [0029] この構成によると、前記記憶手段の記憶している前記コンテンツは、前記固有鍵を用いて、前記復号鍵を暗号化して生成された暗号化鍵と、前記暗号鍵を用いて前記デジタル著作物を暗号化した前記暗号化著作物とを含む。従って、前記コンテンツが複製された場合でも、前記固有鍵がなければ前記コンテンツを再生することができないため、第三者による不正なコンテンツの再生を防止することができる。
- [0030] 前記記憶手段に記憶されている前記コンテンツは、バックアップの許可又は禁止を示すバックアップ情報を含んでおり、前記記録再生装置を構成する前記コンテンツ送信手段は、前記バックアップ情報がバックアップの許可を示しているか否かを判断し、許可を示していると判断すると、前記コンテンツを送信し、前記書込手段は、前記バックアップ情報がバックアップの許可を示しているか否かを判断し、許可を示していると判断すると、前記期間情報を書き込むことを特徴とする。
- [0031] この構成では、前記コンテンツは、作成者により予め、バックアップの可否を示すバックアップ情報が付加されており、前記コンテンツ送信手段は、前記バックアップ情報がバックアップの許可を示している場合にのみ、前記コンテンツを送信する。従って、前記コンテンツのバックアップに関して、前記コンテンツの作成者の意思を反映することができる。

[0032] 前記記録再生装置を構成する前記コンテンツ送信手段は、通信鍵を用いて前記コンテンツを暗号化し、暗号化された前記コンテンツを、安全に送信することを特徴とする。

この構成により、不正な第三者による、前記コンテンツの盗聴を防止することができる。

前記記録再生装置は、さらに、前記コンテンツに所定の演算を施して生成された検出情報を記憶している検出情報記憶手段と、前記記憶手段から前記コンテンツを読み出し、読み出した前記コンテンツに前記所定の演算を施して検査情報を生成し、生成した検査情報と前記検出情報とを比較し、一致しないと判定された前記コンテンツの使用を禁止する不正禁止手段とを備えることを特徴とする。

[0033] この構成によると、前記不正禁止手段は、同一の演算により生成された前記検出情報と前記検査情報とを比較する。この演算に、一方向関数を用いると、前記コンテンツに一部でも変更があれば、前記検出情報は前記検査情報と一致しない。

従って、前記コンテンツの改ざんを容易に検出可能であり、悪意のある第三者により、不正に改ざんされたコンテンツの再生を防止することができる。

[0034] 前記バックアップ装置は、前記記録再生装置以外の機器によるバックアップの指示に応じて別のコンテンツを記憶しており、前記記録再生装置は、さらに、前記別のコンテンツの取得を示すリストア指示を取得するリストア指示取得手段と、前記リストア指示を取得すると、前記別のコンテンツの送信要求を前記バックアップ装置へ送信するコンテンツ要求手段と、前記バックアップ装置から、前記別のコンテンツを受信し、受信した前記別のコンテンツを前記記憶手段に書き込むリストア手段とを備え、前記別のコンテンツを受信すると、前記書込手段は、さらに、前記別のコンテンツの再生が許可される期間を示す期間情報を、前記別のコンテンツと対応付けて、前記記憶手段へ書き込むことを特徴とする。

[0035] この構成によると、リストア手段は、前記バックアップ装置から、前記別のコンテンツを受信し、受信した前記別のコンテンツを前記記憶手段に書き込むため、例えば、ホームネットワーク、社内LANといった同一のネットワークに属する機器の間で、同一のコンテンツを共有することができる。これにより、利用者は、異なる部屋に設置した

何れの機器からでも、同一のコンテンツを視聴することが可能になり、利用者の利便性が向上する。

[0036] また、前記別のコンテンツが前記記憶手段に書き込まれると、前記書込手段は、前記別のコンテンツの再生が許可される期間を示す期間情報を、前記別のコンテンツと対応付けて、前記記憶手段へ書き込むため、前記コンテンツを有する各機器において、前記コンテンツを再生できる期間を限定することができる。

また、本発明は、コンテンツをバックアップするバックアップ装置であって、前記コンテンツを記憶している記憶手段と、記録再生装置から、当該記録再生装置の記憶しているコンテンツの再生が許可される期間を示す期間情報の延長の許可を求める延長要求を受信する延長受付手段と、前記延長を許可するか否かを判定する判定手段と、許可すると判定する場合に前記延長の許可を示す延長許可情報を、前記記録再生装置へ出力する許可手段とを備えることを特徴とする。

[0037] この構成では、前記判定手段により前記延長を許可すると判定する場合に、前記許可手段は、前記延長の許可を示す延長許可情報を出力する。これにより、所定の条件を満たす装置のみが前記コンテンツの再生に係る期間情報を延長することが可能になり、条件を満たさない不正な機器は、期間情報を延長できない。従って、条件を満たさない機器において、期間情報の示す期間が終了後の、前記コンテンツの再生を停止させることができる。

[0038] 前記バックアップ装置を構成する前記記憶手段は、さらに、前記コンテンツを示す識別情報を前記コンテンツと対応して記憶しており、前記延長受付手段は、前記記録再生装置の記憶している前記コンテンツを示すコンテンツ識別情報を含む前記延長要求を受信し、前記判定手段は、前記コンテンツ識別情報と、前記記憶手段の記憶している前記識別情報とを比較し、両者が一致すれば、許可すると判定することを特徴とする。

[0039] この構成では、前記判断手段は、前記コンテンツ識別情報と前記記憶手段の記憶している識別情報とが一致すれば、許可すると判定する。従って、前記バックアップ装置に記憶されている前記コンテンツが、MOVEされ、もはや、障害対策用のバックアップではなくなると、前記期間情報の示す期間は延長されず、前記期間が終了す

ると、前記記録再生装置での、前記コンテンツの再生は不可能になる。このようにすることで、悪意のある利用者により前記バックアップ装置からMOVEされたコンテンツと、前記記録再生装置の有するコンテンツの両方が視聴可能になることを防止する。

[0040] 前記延長要求は、当該延長要求を出力した前記記録再生装置を示す装置識別情報を含んでおり、前記バックアップ装置において、前記判定手段は、予め、特定の機器を示す1以上の許可装置識別情報を記憶しており、受信した前記延長要求に含まれる前記装置識別情報が、前記許可装置識別情報の何れかと一致すれば、許可すると判定することを特徴とする。

[0041] この構成では、前記判定手段は、受信した前記延長要求に含まれる前記装置識別情報が、予め記憶している特定の機器を示す許可装置識別情報のいずれかと一致すれば、許可すると判定する。これにより、特定の機器においてのみ、前記期間情報を延長し、前記コンテンツの再生の許可される期間を延長することが可能であり、その他の機器において、前記コンテンツの再生の許可される期間の延長することができない。

[0042] 前記バックアップ装置において、前記記憶手段は、さらに、前記コンテンツに所定の演算を施して生成された検出情報を前記コンテンツと対応して記憶しており、前記判定手段は、前記記憶手段から、前記コンテンツを読み出し、読み出した前記コンテンツに前記所定の演算を施して検証情報を生成し、生成した検証情報と前記検出情報とを比較し、一致すれば、前記延長を許可すると判定することを特徴とする。

[0043] この構成では、前記判定手段は、前記コンテンツに同一の演算を施して生成された検証情報と前記記憶手段の記憶している前記検出情報とを比較し、一致すれば、前記延長を許可する。前記演算に、一方向関数を用いれば、前記コンテンツの改ざんが容易に前記コンテンツの改ざんを容易に検出することができる。従って、前記バックアップ装置がバックアップしているコンテンツが不正に改ざんされた場合、前記記録再生装置において、前記コンテンツの再生が許可される期間の延長は許可されず、前記コンテンツの再生可能な期間を限定することができる。

[0044] 前記バックアップ装置において、前記許可手段は、前記期間情報により示される期間よりも、後の期間を示す前記延長許可情報を出力することを特徴とする。

この構成によると、前記許可手段が、前記延長許可情報として、前記延長後期間情報を出力するため、前記記録再生装置においては、前記期間情報を、前記延長後期間情報に置き換えることにより、迅速に延長することができる。

[0045] また、バックアップ装置が、前記延長後期間情報を設定するため、バックアップ装置において、各機器の前記コンテンツの再生が許可される期間を、一括管理することができる。

前記バックアップ装置は、さらに、前記記憶手段の記憶している前記コンテンツの送信要求を受信するリストア受信手段と、前記コンテンツを送信するか否かを判定するリストア判定手段と送信すると判定されると、前記記憶手段から前記コンテンツを読み出し、読み出した前記コンテンツを送信するリストア送信手段とを備えることを特徴とする。

[0046] この構成では、前記リストア判定手段により、送信すると判定されると、前記リストア送信手段は、前記記憶手段から前記コンテンツを読み出し、読み出した前記コンテンツを送信する。従って、所定の条件を満たしている機器は、前記コンテンツを取得し、利用者は、前記コンテンツの視聴を楽しむことができる。また、所定の条件を満たさない機器での前記コンテンツの再生を防止することができる。

[0047] 前記送信要求は、当該送信要求の送信元であるリストア機器を示すリストア機器識別情報を含んでおり、前記バックアップ装置において、前記リストア判定手段は、予め、特定の機器を示す1以上の許可装置識別情報を記憶しており、前記リストア機器識別情報が、前記許可装置識別情報の何れかと一致すれば、前記コンテンツを送信すると判定することを特徴とする。

[0048] この構成によると、前記リストア判定手段は、前記リストア機器識別情報が、予め記憶している許可装置識別情報に含まれる場合、前記コンテンツを送信すると判定する。従って、前記コンテンツを取得できる機器を、予め、設定されている特定の機器のみに限定することができる。

前記許可装置識別情報は、前記記憶手段の記憶している前記コンテンツのバックアップを指示したバックアップ元装置を示しており、前記バックアップ装置において、前記リストア判定手段は、前記リストア機器識別情報と前記許可装置識別情報とが一

致すれば、前記コンテンツを送信すると判定することを特徴とする。

- [0049] この構成によると、前記コンテンツを取得できる機器を、前記記憶手段の記憶している前記コンテンツのバックアップを指示したバックアップ元装置のみに限定することができる。

本発明のバックアップ装置において、前記リストア判定手段は、前記記憶手段に記憶されている前記コンテンツと同一で、前記バックアップ装置により再生を許可されたコンテンツを記憶している機器の総数を示すコピー数と、前記コピー数の上限を示すコピー許可数とを有し、前記コピー数が前記コピー許可数未満であれば、前記コンテンツを送信すると判定することを特徴とする。

- [0050] この構成では、前記リストア判定手段は、前記コピー数が前記コピー許可数未満であれば、前記コンテンツを送信すると判定する。従って、前記コンテンツと同一のコンテンツを有する機器の総数を前記コピー許可数未満に限定することができる。

前記バックアップ装置は、さらに、前記記憶手段に記憶されている前記コンテンツと同一であり、前記バックアップ装置により再生を許可されたコンテンツを記憶している機器を示す機器識別情報と、前記機器において前記コンテンツの再生が許可される期間を示すコピー期間情報とを対応付けて記憶している期間情報記憶手段と、前記コピー期間情報の示す期間が終了すると、前記コピー数から1減算するコピー数管理手段を備えることを特徴とする。

- [0051] この構成では、前記コピー数管理手段前記バックアップ装置は、前記コピー期間情報の示す期間が終了すると、前記コピー数から1減算する。従って、ある機器において、前記コンテンツの視聴が許可される期間が終了すると、前記バックアップ装置は、他の機器に前記コンテンツを出力することができる。

前記バックアップ装置において、前記記憶手段の記憶している前記コンテンツは、予め、前記コピー許可数を含んでおり、前記判定手段は、前記コンテンツから前記コピー許可数を取得することを特徴とする。

- [0052] 前記コンテンツの作成者は、任意のコピー許可数を含むコンテンツを生成することができるため、この構成によると、前記判定手段は、前記コンテンツから取得した前記コピー許可数を使用することにより、前記コンテンツの作成者の意思を反映した判定を

行うことができる。

前記バックアップ装置を構成する前記リストア送信手段は、通信鍵を用いて前記コンテンツを暗号化し、安全に、暗号化コンテンツを送信する。

[0053] この構成により、不正な第三者による前記コンテンツの盗聴を防止することができる。

また、前記記録再生装置は、前記延長要求に先立って、前記バックアップ装置へ、起動を指示する起動指示情報を出し、前記バックアップ装置は、さらに、前記起動指示を受信すると、当該バックアップ装置を構成する各回路へ電力供給を開始する電力制御手段を備えることを特徴とする。

[0054] バックアップ装置は、障害発生対策用にコンテンツを保持するという役割上、その動作時間は短いほうが望ましい。上記の構成によると、電力制御手段は、前記起動指示を受信すると、当該バックアップ装置を構成する各回路へ電力供給を開始する。従って、前記バックアップ装置の動作時間を短縮し、前記記憶手段を構成するハードディスクユニットの故障の発生確率を低下させることができる。

図面の簡単な説明

[0055] [図1]実施の形態1のバックアップシステム1の構成を示す構成図である。

[図2]HDレコーダ100の構成を示すブロック図である。

[図3]情報記憶部110に記憶されている情報の一例を示す。

[図4]コンテンツ管理表121の詳細を示す。

[図5]制御部107の構成を示すブロック図である。

[図6]モニタ120に表示されるメニュー画面181及び再生リスト画面211の一例である。

[図7]モニタ120に表示される初期設定画面191及びリストア情報画面221の一例である。

[図8]バックアップ装置500の構成を示すブロック図である。

[図9]コンテンツ記憶部510に記憶されている情報の一例を示す。

[図10]セキュア情報記憶部511に記憶されている情報の一例を示す。

[図11]バックアップ管理表521の詳細を示す。

[図12]HDレコーダ100の動作を示すフローチャートである。

[図13]HDレコーダ100による録画処理を示すフローチャートである。

[図14]HDレコーダ100による録画処理を示すフローチャートである。図13から続く。

[図15]コンテンツの再生処理を示すフローチャートである。

[図16]HDレコーダ100及びバックアップ装置500によるリストア処理を示すフローチャートである。

[図17]HDレコーダ100及びバックアップ装置500によるリストア処理を示すフローチャートである。図16から続く。

[図18]HDレコーダ100及びバックアップ装置500によるバックアップ処理を示すフローチャートである。

[図19]HDレコーダ100及びバックアップ装置500によるバックアップ処理を示すフローチャートである。図18から続く。

[図20]HDレコーダ100及びバックアップ装置500によるバックアップ処理を示すフローチャートである。図18から続く。

[図21]HDレコーダ100及びバックアップ装置500による有効期限延長処理を示すフローチャートである。

[図22]HDレコーダ100及びバックアップ装置500による有効期限延長処理を示すフローチャートである。図21から続く。

[図23]HDレコーダ100及びバックアップ装置500による有効期限延長処理を示すフローチャートである。図21から続く。

[図24]HDレコーダ100及びバックアップ装置500による機器認証処理を示すフローチャートである。

[図25]HDレコーダ100及びバックアップ装置500による機器認証処理を示すフローチャートである。図24から続く。

符号の説明

- [0056]
- | | |
|-----|------------|
| 1 | バックアップシステム |
| 10 | 放送装置 |
| 100 | HDレコーダ |

- 101 送受信部
- 102 認証部
- 103 入力部
- 104 再生制御部
- 105 デコード部
- 106 鍵生成部
- 107 制御部
- 108 固有情報記憶部
- 109 暗号処理部
- 110 情報記憶部
- 112 入出力部
- 113 セキュア記憶部
- 114 放送受信部
- 120 モニタ
- 400 HDレコーダ
- 500 バックアップ装置
- 501 送受信部
- 502 認証部
- 503 電源部
- 504 固有情報記憶部
- 507 制御部
- 509 暗号処理部
- 510 コンテンツ記憶部
- 511 セキュア情報記憶部
- 512 入力部
- 513 表示部

発明を実施するための最良の形態

[0057] 1. 実施の形態1

本発明に係る実施の形態1のバックアップシステム1について、図を用いて以下に説明する。

1. 1 バックアップシステム1の概要

本発明のバックアップシステム1は、図1に示すようにハードディスクレコーダ(以下HDレコーダ)100、HDレコーダ400及びバックアップ装置500から構成される。HDレコーダ100、HDレコーダ400及びバックアップ装置500は、LAN(Local Area Network)30により接続されている。

[0058] HDレコーダ100は、放送装置10から送信される放送波を受信することにより、映像及び音声からなるコンテンツを取得し、取得したコンテンツを記憶する。また、HDレコーダ100は、DVDなどの、外部記録メディアを装着され、装着された外部記録メディアから、コンテンツを取得することもできる。

HDレコーダ100は、利用者の操作に基づいて、記憶しているコンテンツをバックアップ装置500へ送信するとともに、自身の記憶しているコンテンツに有効期限を設定する。

[0059] バックアップ装置500は、HDレコーダ100からコンテンツを受け取り、受け取ったコンテンツを記憶する。

また、HDレコーダ100は、有効期限が近づくと、バックアップ装置500に、有効期限の延長を要求する。

バックアップ装置500は、HDレコーダ100から、コンテンツの有効期限の延長の要求を受け取り、受け取った要求に該当するコンテンツが正常に記憶されていることを確認し、HDレコーダ100に対して、有効期限の延長を許可する。

[0060] バックアップ装置500により、延長が許可されると、HDレコーダ100は、自身の記憶している有効期限を延長する。延長が許可されない場合及びLAN30の不具合などによりバックアップ装置500と通信できなかった場合、HDレコーダ100は、有効期限が過ぎたコンテンツを削除する。削除した後、利用者の操作などにより、HDレコーダ100は、バックアップ装置500にバックアップされているコンテンツを、バックアップ装置500から取得し、改めて有効期限を設定する。

[0061] さらに、HDレコーダ100は、HDレコーダ100自身がバックアップ装置500に送信

したコンテンツだけでなく、HDレコーダ400がバックアップ装置500に送信したコンテンツを取得することも出来る。

HDレコーダ400は、HDレコーダ100と同様に、放送番組を含むコンテンツを受信し、記憶し、再生し、バックアップ装置500へ、受信したコンテンツを送信する。

1. 2 HDレコーダ100及びHDレコーダ400

HDレコーダ100は、図2に示すように、送受信部101、認証部102、入力部103、再生制御部104、デコード部105、鍵生成部106、制御部107、固有情報記憶部108、暗号処理部109、情報記憶部110、入出力部112、セキュア記憶部113、放送受信部114及びアンテナ130から構成される。

[0062] HDレコーダ100は、具体的にはマイクロプロセッサ、RAM、ROMを含んで構成されるコンピュータシステムであって、前記RAM及びROMにはコンピュータプログラムが記憶されている。前記マイクロプロセッサが前記コンピュータプログラムに従って動作することにより、HDレコーダ100はその機能の一部を達成する。

なお、HDレコーダ400の構成及び動作は、HDレコーダ100と同様であるので、説明を省略する。

(1) 固有情報記憶部108

固有情報記憶部108は、ROMから構成され、装置識別子115「ID__A」と装置固有鍵116「Key__A」とを記憶している。また、固有情報記憶部108は、保護機構を備えており、外部機器によるアクセスから保護されている。

[0063] 装置識別子115「ID__A」は、HDレコーダ100を一意に示す情報である。装置固有鍵116「Key__A」は、HDレコーダ100に固有の鍵情報である。これらは、予め、HDレコーダ100の出荷時に固有情報記憶部108に書き込まれている。

(2) 情報記憶部110

情報記憶部110は、ハードディスクユニットから構成され、一例として、図3に示すように、バックアップ履歴表131、コンテンツファイル134、139・・・を記憶している。各コンテンツファイルは、コンテンツIDと暗号化コンテンツと、暗号化コンテンツ鍵とを含む。コンテンツIDは、暗号化コンテンツを一意に識別する識別情報である。暗号化コンテンツは、コンテンツ鍵を用いて、放送装置10又は外部記録メディアから取得した

コンテンツに暗号化アルゴリズムE1を施して生成されたものである。ここで、コンテンツは、MPEG2などの圧縮方式により圧縮された画像データ、音声データを含んで構成される。

[0064] 暗号化コンテンツ鍵は、固有情報記憶部108の記憶している装置固有鍵116「Key__A」を用いて、コンテンツの暗号化に使用されたコンテンツ鍵に暗号化アルゴリズムE1を施して生成されたものである。コンテンツ鍵とコンテンツとは1対1に対応する。ここで、暗号化アルゴリズムE1は、一例としてDES(Data Encryption Standard)などである。

[0065] 例えば、コンテンツファイル134は、コンテンツID136「A001」、暗号化コンテンツ137、暗号化コンテンツ鍵138「Enc(Key__A, Key__1a)」を含んでおり、コンテンツID136「A001」は、暗号化コンテンツ137を示す識別情報である。暗号化コンテンツ137は、コンテンツ鍵「Key__1a」を用いて、映像を含むコンテンツに、暗号化アルゴリズムE1を施して生成されたものである。暗号化コンテンツ鍵138「Enc(Key__A, Key__1a)」は、固有情報記憶部108の記憶している装置固有鍵116「Key__A」を用いて、コンテンツ鍵「Key__1a」に暗号化アルゴリズムE1を施して生成されたものである。コンテンツ鍵「Key__1a」は、暗号化コンテンツ137の基になるコンテンツと1対1に対応する。

[0066] バックアップ履歴表131は、HDレコーダ100が、バックアップ装置500にバックアップを行った日時と、このとき、情報記憶部110に記憶されている各コンテンツファイルのコンテンツIDとを対応付けて含んでいる。

このほかにも、メニュー画面、初期設定画面などの各種画像データを記憶している。

(3) セキュア記憶部113

セキュア記憶部113は、フラッシュメモリを含んで構成され、外部機器によるアクセスから保護されている。

[0067] セキュア記憶部113は、一例として、図4に示すコンテンツ管理表121を記憶している。コンテンツ管理表121は、図4に示すように、複数のコンテンツ情報122、123、124・・・を含む。各コンテンツ情報管理情報は、コンテンツID、タイトル、録画日時、ハッシュ値、種類、圧縮方式、有効期限、バックアップフラグ及び優先度から構成され、

情報記憶部110に記憶されているコンテンツファイルと1対1に対応する。

- [0068] コンテンツIDは、対応するコンテンツファイルに含まれる暗号化コンテンツを識別する情報であり、対応するコンテンツファイルに含まれるコンテンツIDと同一である。

タイトルは、対応する暗号化コンテンツを示す名称であり、暗号化コンテンツの基になるコンテンツを放送装置10又は外部記録メディアから取得した時点では、書き込まれていない。

- [0069] 録画日時は、対応するコンテンツファイルに含まれる暗号化コンテンツの元になるコンテンツを、放送装置10又は記録メディアから取得した日付と時刻を示す。種類は、コンテンツの入手経路を示す情報であり、一例として、放送装置10から受信したコンテンツであることを示す「放送番組」、デジタルカメラなどによって撮影された画像データであることを示す「写真」などである。圧縮方式は、コンテンツを構成する映像、音声の圧縮に使用されている圧縮方式の名称である。

- [0070] ハッシュ値は、対応するコンテンツファイルに含まれる暗号化コンテンツと、暗号化コンテンツ鍵とを結合して、ハッシュ関数に代入して生成されたものである。ここで使用するハッシュ関数は、一例としてSHA-1である。

有効期限は、対応する暗号化コンテンツをHDレコーダ100において利用することが出来る期間の終了する年月日及び時刻を示している。

- [0071] バックアップフラグは、対応する暗号化コンテンツがバックアップ装置500にバックアップされているか否かを示すフラグであり、「1」又は「0」の値をとる。「1」は、バックアップされていることを示し、「0」はバックアップされていないことを示す。

優先度は、コンテンツの保存の優先度を示す情報であり、「1」又は「2」の値をとる。新たな暗号化コンテンツを情報記憶部110に書き込む際に、情報記憶部110の空き容量が不足している場合、制御部107は、優先度「2」を含むコンテンツ情報と対応するコンテンツファイルを削除し、記憶容量を確保する。情報記憶部110の空き容量が不足しても、優先度「1」を含むコンテンツ情報と対応するコンテンツファイルは、削除されない。優先度は、コンテンツ取得時に自動的に「1」に設定されるが、利用者の操作により、変更される。

- [0072] 例えば、コンテンツ情報122は、情報記憶部110に記憶されているコンテンツファイ

ル134と対応している。コンテンツID151「A001」は、暗号化コンテンツ137を示す識別情報であり、コンテンツID136「A001」と同一である。タイトル152「ワイドショー」は、暗号化コンテンツ137に対して利用者が入力した名称である。また、録画日時153「04. 10. 10. 17:00」は、暗号化コンテンツ137が、2004年10月10日17時に取得されたコンテンツを暗号化して生成されたことを示している。ハッシュ値154「01a」は、暗号化コンテンツ137と暗号化コンテンツ鍵138「Enc (Key__A, Key__1a)」との結合物をハッシュ関数に代入して生成されたものである。また、有効期限157「04 . 12. 15. 17」は、対応する暗号化コンテンツ137をHDレコーダ100において、復号して再生することができる期限が、2004年12月15日17時までであることを示している。

(4) アンテナ130、放送受信部114、デコード部105

アンテナ130は、放送装置10から送信される放送波を受信する。

[0073] 放送受信部114は、チューナー、変復調部、トランスポートデコーダなどを備えており、アンテナ130の受信した放送波から1つの放送波を選択し、選択した放送波をデジタル信号に変換し、TS (トランスポートストリーム) パケットを生成する。次に生成したTSパケットを、生成した順にデコード部105へ出力する。

また、制御部107から、現在受信中のコンテンツを記録することを示す録画指示を受け取る。録画指示を受け取ると、生成したTSパケットを、生成した順に、連続的に制御部107へ出力する。制御部107から終了通知を受け取るまで、TSパケットの出力を継続する。

[0074] ここで、HDレコーダ100が放送装置10から取得するコンテンツは、複数のTSパケットを含んで構成される。以下の説明において、特に必要がない限り、コンテンツを構成するTSパケットについては、言及せず、単にコンテンツと呼ぶ。

デコード部105は、制御部107の指示により、放送受信部114の取得したコンテンツ及び暗号処理部109 (後述する) により生成されたコンテンツを、各コンテンツの圧縮方式に応じて、MPEG (Moving Picture Experts Group) 2、JPEG (Joint Photographic Experts Group) などの方式に従って伸長して画像データ及び音声データを生成し、生成した画像データ及び音声データを再生制御部104へ出力

する。

[0075] MPEG2、JPEGについては、公知の技術であるので、説明を省略する。

(5)送受信部101

送受信部101は、LAN30と接続されており、制御部107及び認証部102と外部機器との間で、情報の送受信を行う。ここで、外部機器とは、バックアップ装置500である。

(6)認証部102

認証部102は、予め、HDレコーダ100に固有の秘密鍵SK__A、公開鍵証明書Cert__A、認証局の公開鍵PK__CA及びCRL(Certificate Revocation List)を記憶している。公開鍵証明書Cert__Aは、秘密鍵SK__Aと対応する公開鍵PK__Aの正当性を証明するものであり、証明書識別番号、前記公開鍵PK__A、認証局の署名データを含んで構成される。認証局の署名データは、認証局の秘密鍵SK__CAを用いて、少なくとも、公開鍵PK__Aに署名生成アルゴリズムSを施して生成されたものである。署名生成アルゴリズムSは、一例として、有限体上のElgamal署名である。Elgamal署名については、公知であるので説明を省略する。

[0076] ここで、認証局は、公正な第三者機関であり、実施の形態1のバックアップシステム1を構成する各機器の公開鍵証明書を発行する。

CRLは、無効になった公開鍵証明書の証明書識別番号を含む。

認証局の公開鍵PK__CAは、認証局の秘密鍵SK__CAと対になる公開鍵である。

認証部102は、制御部107の指示により外部機器との間で、DTCP(Digital Transmission Content Protection)に従った機器認証を行い、認証が失敗した場合、制御部107と外部機器との通信を禁止する。認証が成功であった場合、外部機器との間で共通のセッション鍵を生成し、生成したセッション鍵を制御部107へ出力する。機器認証の動作については、後に詳細に説明する。

(7)入力部103

入力部103は、電源ボタン、録画ボタン、メニューボタン、選択ボタンなどの各種ボタン及びリモートコントローラの受信回路を備える。

[0077] 利用者によるボタン操作及びリモートコントローラの操作を受け付け、受け付けた、

ボタン操作及びリモートコントローラの操作を示す操作指示情報を制御部107へ出力する。

(8) 鍵生成部106及び暗号処理部109

鍵生成部106は、制御部107からコンテンツ鍵の生成指示を受け取る。コンテンツ鍵の生成指示を受け取ると、擬似乱数を生成し、生成した擬似乱数を用いて56ビット長のコンテンツ鍵を生成する。生成したコンテンツ鍵を制御部107へ出力する。コンテンツ鍵の生成方法は、他の方法を用いても良い。

[0078] 暗号処理部109は、制御部107から平文の情報と鍵とを受け取り、暗号化を指示される。また、制御部107から暗号文と鍵とを受け取り、復号を指示される。

暗号化を指示されると、受け取った鍵を用いて、受け取った平文に暗号化アルゴリズムE1を施して、暗号文を生成し、生成した暗号文を制御部107へ出力する。

復号を指示されると、受け取った鍵を用いて受け取った暗号文に、復号アルゴリズムD1を施して復号文を生成し、生成した復号文を制御部107へ出力する。

[0079] 暗号処理部109の受け取る平文と鍵との組み合わせは、一例として、コンテンツとコンテンツ鍵、コンテンツ鍵と装置固有鍵「Key__A」である。また、暗号処理部109の受け取る暗号文と鍵との組み合わせは、暗号化コンテンツとコンテンツ鍵、暗号化コンテンツ鍵と装置固有鍵「Key__A」である。

復号アルゴリズムD1は、暗号化アルゴリズムE1により生成された暗号文を復号するアルゴリズムである。

(9) 制御部107

制御部107は、図5に示すように、セキュアクロック117、主制御部118、期限管理部119から構成される。

[0080] (a) セキュアクロック117

セキュアクロック117は、時間の経過を計測し、現在時刻を算出する時計である。算出される、現在時刻は、年月日、曜日、時刻を含む。

また、セキュアクロック117は、保護機構を備えており、外部の操作から保護されている。

[0081] (b) 期限管理部119

期限管理部119は、予め、延長実行時間「24時間」を記憶している。延長実行時間「24時間」は、HDレコーダ100の記憶している暗号化コンテンツの有効期限の延長を要求するか否かを判断する基準であり、ここでは、期限管理部119は、有効期限が切れるまでの時間が「24時間」未満であれば、バックアップ装置500へ有効期限の延長を要求する。

- [0082] 期限管理部119は、主制御部118から、各コンテンツの有効期限の延長を指示する有効期限延長指示を受け取る。また、有効期限切れのコンテンツの削除を示す削除指示を受け取る。

(b-1)有効期限延長処理

有効期限延長指示を受け取ると、期限管理部119は、セキュア記憶部113に記憶されているコンテンツ管理表121を構成するコンテンツ情報を1つずつ順番に選択し、選択したコンテンツ情報について、以下に説明する処理を行う。

- [0083] 期限管理部119は、選択したコンテンツ情報から、有効期限を読み出す。ここで、選択したコンテンツ情報に、有効期限が書き込まれていなければ、次のコンテンツ情報の処理に移る。

有効期限を読み出すと、期限管理部119は、次に、セキュアクロックから、現在時刻を取得する。読み出した有効期限と取得した現在時刻との差を算出する。ここで、算出される差を残り時間と呼ぶ。

- [0084] 算出した残り時間が、延長実行時間「24時間」以上であれば、期限管理部119は、選択したコンテンツ情報に関する処理を終了し、次の、コンテンツ情報の処理に移る。

算出した残り時間が、更新実行時間「24時間」未満であれば、期限管理部119は、送受信部101を介して、バックアップ装置500へ、起動を示す起動指示を送信する。

次に、期限管理部119は、バックアップ装置500から、起動したことを示す起動通知を受け取る。ここで、一定時間以内に起動通知を受信しなければ、選択したコンテンツ情報に関する処理を終了し、次の、コンテンツ情報の処理に移る。

- [0085] 起動通知を受け取ると、期限管理部119は、認証部102へ、バックアップ装置500との機器認証を指示する。認証部102による機器認証が成功すると、認証部102か

ら機器認証において生成されたセッション鍵を受け取る。以下の処理において、期限管理部119は、セッション鍵を用いて、バックアップ装置500との間で送受信する情報を暗号化及び復号し、秘密通信を行うが、簡略化のため、これらの暗号化及び復号の処理についての説明を省略する。

[0086] 認証部102による機器認証が失敗すると、選択したコンテンツ情報に関する処理を終了し、次の、コンテンツ情報の処理に移る。

認証部102からセッション鍵を受け取ると、期限管理部119は、選択したコンテンツ情報に含まれるコンテンツIDを読み出し、固有情報記憶部108から装置識別子115「ID_A」を読み出し、読み出したコンテンツIDと装置識別子と、有効期限の延長を要求する延長要求とを、送受信部101を介して、バックアップ装置500へ送信する。

[0087] 次に、期限管理部119は、送受信部101を介して、バックアップ装置500から新たな有効期限又は、延長要求を受け付けられないことを示すエラー通知を受信する。

エラー通知を受信すると、期限管理部119は、選択したコンテンツ情報に関する処理を終了し、次の、コンテンツ情報の処理に移る。

新たな有効期限を受信すると、期限管理部119は、受け取った有効期限により、選択したコンテンツ情報に含まれる有効期限を更新し、次のコンテンツ情報の処理に移る。

[0088] 全てのコンテンツ情報について、上記の処理が終了すると、有効期限の延長が終了したことを示す延長終了通知を主制御部118へ出力する。

(b-2) 削除処理

期限管理部119は、主制御部118から、削除指示を受け取ると、セキュア記憶部113に記憶されているコンテンツ管理表121を構成するコンテンツ情報を1つずつ順番に選択し、選択したコンテンツ情報について、以下に説明する処理を行う。

[0089] 期限管理部119は、選択したコンテンツ情報から、有効期限を読み出す。ここで、選択したコンテンツ情報に、有効期限が書き込まれていなければ、次のコンテンツ情報の処理に移る。

有効期限を読み出すと、期限管理部119は、次に、セキュアクロック117から、現在時刻を取得する。読み出した有効期限と取得した現在時刻とを比較し、現在時刻が

有効期限よりも前の時点を示していれば、そのまま次のコンテンツ情報の処理に移る。

- [0090] 現在時刻が有効期限よりも後の時点を示していれば、期限管理部119は、選択したコンテンツ情報に含まれるコンテンツIDを読み出し、情報記憶部110上で、読み出したコンテンツIDと一致するコンテンツIDを含むコンテンツファイルを削除する。次に、選択したコンテンツ情報を削除し、次のコンテンツ情報の処理に移る。

全てのコンテンツ情報について、上記の処理が終了すると、有効期限切れのコンテンツの削除処理が終了したことを示す削除終了通知を主制御部118へ出力する。

- [0091] (c)主制御部118

主制御部118は、予め、情報記憶部110に記憶されている暗号化コンテンツの有効期限の延長を行う延長時刻を記憶している。ここでは、延長時刻「2時00分」を記憶している。また、有効期限切れのコンテンツの削除を実行する時間間隔「30分」を記憶している。これらは、HDレコーダ100の出荷時に設定されている。

- [0092] 主制御部118は、入力部103から、各種の操作指示情報を受け取り、受け取った操作指示情報に応じて、各種の処理を制御する。

具体的には、録画ボタンの押下を示す操作指示情報を受け取ると、以下に説明する(c-1)録画処理の制御を行う。

メニューボタンの押下を示す操作指示情報を受け取ると、主制御部118は、情報記憶部110に記憶されている画像データを基に、メニュー画面181を生成し、生成したメニュー画面181を再生制御部104へ出力し、メニュー画面181の表示を指示する。図6(a)は、ここで表示されるメニュー画面181の一例である。メニュー画面181は、再生リスト表示ボタン182、リストアボタン183、タイマー予約ボタン184、番組表表示ボタン185、コンテンツリストボタン186、ダビング設定ボタン187、初期設定ボタン188及びコンテンツ管理ボタン189を含む。利用者は、方向キーにより、いずれかのボタンにカーソルを合わせ、決定ボタンを押下することにより、いずれかのボタンを選択する。

- [0093] 再生リスト表示ボタン182の選択を示す操作指示情報を受け取ると、主制御部118は、以下に説明する(c-2)再生処理の制御を行う。また、初期設定ボタン188の選

択を示す操作指示情報を受け取ると、以下に説明する(c-3)初期設定処理を行う。
リストアボタン183の選択を示す操作指示情報を受け取ると、以下に説明する(c-4)
)リストア処理を実行する。

[0094] その他のボタンの選択を示す操作指示情報を受け取った場合、主制御部118は、それぞれの、ボタンに応じて、タイマー予約の受付、番組表の表示、外部記録メディアからの情報の入出力など、各種の処理を行う。

また、主制御部118は、セキュアクロック117を定期的に監視し、セキュアクロック117の示す時刻が延長時刻である「2時00分」とであると判断すると、期限管理部119へ有効期限延長指示を出力する。

[0095] また、主制御部118は、セキュアクロック117を用いて時間を計測し、「30分」毎に、期限管理部119へ有効期限切れのコンテンツの削除を示す削除指示を出力する。

以下に、主制御部118が行う(c-1)録画処理の制御、(c-2)再生処理の制御、(c-3)初期設定処理、(c-4)リストア処理及び(c-5)バックアップ処理について説明する。

[0096] (c-1)録画処理の制御

入力部103から、録画ボタンの押下を示す操作指示情報を受け取ると、主制御部118は、新たにコンテンツIDを生成し、セキュア記憶部113に記憶されているコンテンツ管理表121に、生成したコンテンツIDを含むコンテンツ情報を追加する。このとき、追加したコンテンツ情報の録画日時として現在時刻を書き込み、種類として「放送番組」を書き込み、圧縮方式に「MPEG2」、バックアップフラグ「0」、優先度に「1」を書き込む。

[0097] 次に、主制御部118は、鍵生成部106へ、コンテンツ鍵の生成指示を出力し、鍵生成部106からコンテンツ鍵を受け取る。コンテンツ鍵を受け取ると、主制御部118は、情報記憶部110内に新たにコンテンツファイルを生成する。

次に、主制御部118は、放送受信部114へ録画指示を出力し、放送受信部114からコンテンツを受け取る。受け取ったコンテンツ鍵とコンテンツとを暗号処理部109へ出力し、コンテンツの暗号化を指示する。暗号処理部109から、暗号化コンテンツを受け取る。主制御部118は、情報記憶部110内に新たに生成したコンテンツファイル

へ、受け取った暗号化コンテンツを書き込む。

- [0098] 既に述べたように、ここで、放送受信部114から出力されるコンテンツは、複数のTSパケットから構成されており、主制御部118は、ストップボタンの押下を示す操作指示情報を受け取るまで、TSパケット単位でコンテンツを受け取り、暗号化を指示し、暗号化コンテンツを書き込むことを繰り返す。

この繰返しと並行して、主制御部118は、情報記憶部110の空き容量を監視している。空き容量が不足していると判断した場合、コンテンツ管理表121を構成するコンテンツ情報のうち、優先度が「2」であるものを選択し、選択したコンテンツ情報と対応するコンテンツファイルを情報記憶部110から削除し、選択したコンテンツ情報をコンテンツ管理表121から削除する。

- [0099] コンテンツ管理表121を構成するコンテンツ情報のうち、優先度が「2」のものが存在しない場合、つまり、情報記憶部110上に、削除しても良いコンテンツが存在しない場合、主制御部118は、利用者に、例えば、ランプを点滅させるなどして、記憶容量が不足しており、録画を中止する事を通知する。

情報記憶部110の記憶容量が不足し録画を中断する場合又は、入力部103からストップボタンの押下を示す操作指示情報を受け取った場合、主制御部118は、放送受信部114に録画終了を示す終了通知を出力する。

- [0100] 次に、主制御部118は、固有情報記憶部108から装置固有鍵116「Key__A」を読み出し、読み出した装置固有鍵116「Key__A」とコンテンツ鍵とを暗号処理部109へ出力し、コンテンツ鍵の暗号化を指示する。暗号処理部109から暗号化コンテンツ鍵を受け取り、受け取った暗号化コンテンツ鍵と生成したコンテンツIDとを、生成したコンテンツファイルへ書き込む。

- [0101] 次に、主制御部118は、暗号化コンテンツと暗号化コンテンツ鍵とを、生成したコンテンツファイルから読み出し、読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、160ビット長のハッシュ値を生成する。追加したコンテンツ情報に算出したハッシュ値を書き込む。

(c-2) 再生処理の制御

利用者のボタン操作により、再生リスト表示ボタン182が選択されると、主制御部11

8は、情報記憶部110に記憶されている画像データと、コンテンツ管理表121を構成する各コンテンツ情報のタイトル及び録画日時とを用いて再生リスト画面211を生成し、生成した再生リスト画面211の表示を再生制御部104へ出力する。図6(b)に示す再生リスト画面211は、ここで表示される再生リスト画面211である。

- [0102] 再生リスト画面211は、コンテンツボタン212、213、214及び215を含んでおり、各コンテンツボタンは、コンテンツ管理表121を構成するコンテンツ情報122、123、124及び125とそれぞれ対応している。

次に、利用者の操作によるコンテンツボタンの選択を受け付ける。

利用者によりいずれかのコンテンツボタンが選択されると、主制御部118は、選択されたコンテンツボタンと対応するコンテンツ情報に含まれるコンテンツIDをセキュア記憶部113から読み出す。情報記憶部110において、読み出したコンテンツIDと一致するコンテンツIDを含むコンテンツファイルを検出する。検出したコンテンツファイルから、暗号化コンテンツと暗号化コンテンツ鍵とを読み出し、読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合し、ハッシュ関数に代入し、ハッシュ値を算出する。

- [0103] 主制御部118は、選択されたコンテンツボタンと対応するコンテンツ情報に含まれるハッシュ値を読み出し、読み出したハッシュ値と算出したハッシュ値とを比較し、両者が一致しなければ、選択されたコンテンツを再生できないことを示すエラー画面を生成する。主制御部118は、生成したエラー画面を再生制御部104へ出力し、エラー画面の表示を指示し、コンテンツの再生を中止する。

- [0104] 読み出したハッシュ値と算出したハッシュ値とが一致すれば、主制御部118は、固有情報記憶部108から、装置固有鍵116「Key_A」を読み出し、読み出した装置固有鍵116「Key_A」と読み出した暗号化コンテンツ鍵とを暗号処理部109へ出力し、暗号化コンテンツ鍵の復号を指示する。

次に、主制御部118は、暗号処理部109から、コンテンツ鍵を受け取る。コンテンツ鍵を受け取ると、検出したコンテンツファイルから暗号化コンテンツを読み出し、読み出した暗号化コンテンツと受け取ったコンテンツ鍵とを暗号処理部109へ出力し、暗号化コンテンツの復号を指示する。次に、主制御部118は、暗号処理部109から、コ

ンテンツを受け取り、受け取ったコンテンツをデコード部105へ出力する。

(c-3) 初期設定処理

図6(a)に示すメニュー画面181がモニタ120に表示された状態で、初期設定ボタン188の選択を示す操作指示情報を受け取ると、主制御部118は、初期設定画面191を生成し、生成した初期設定画面191の表示を、再生制御部104へ指示する。図7(a)は、ここで表示される初期設定画面191である。初期設定画面191は、設定項目192、193、194及び196を含む。利用者の操作により、いずれかの設定項目にカーソルが合わせられると、設定項目に対応する設定ボックスが表示される。図7(a)では、設定項目196「バックアップ」に対応する設定ボックス197～201が表示されている。

- [0105] 主制御部118は、設定ボックス197～201への、利用者による入力操作を受け付ける。ここでは、設定ボックス197には、コンテンツの種類を問わず全てのコンテンツをバックアップすることを示す「全て」が入力されている。

設定ボックス198には、バックアップのために、バックアップ装置500へ暗号化コンテンツを送信するスケジュールとして、「日曜 0時30分」が入力されている。

- [0106] 設定ボックス199には、情報記憶部110に記憶されている暗号化コンテンツのうち、バックアップされていない新規の暗号化コンテンツのみをバックアップの対象とすることを示す「新規のみ」が入力されている。

設定ボックス201には、バックアップ装置500にバックアップされているコンテンツのリストアを開始する方法として、利用者の操作によって開始することを示す「手動」が入力されている。以下の説明において、バックアップ装置500にバックアップされている暗号化コンテンツをHDレコーダ100が取得することをリストアと呼ぶ。

- [0107] 次に、主制御部118は、入力部103から決定ボタンの押下を示す操作指示情報を受け取り、各設定ボックスに入力された設定事項を記憶する。

また、具体的には図示していないが、利用者がボタン192～194にカーソルを合わせることにより、チャンネル、画質、ディスクに関する設定の入力を受け付け、決定ボタンの押下により入力された設定事項を記憶する。

(c-4) リストア処理

図6(a)に示すメニュー画面181がモニタ120に表示された状態で、リストアボタン183の選択を示す操作指示情報を受け取ると、主制御部118は、送受信部101を介して、バックアップ装置500へ、起動指示を送信する。

[0108] 所定時間以内に、送受信部101を介してバックアップ装置500から、正常に起動したことを示す起動通知を受信しなかった場合、主制御部118は、バックアップ装置500との通信に失敗したためリストアできないことを利用者に通知するエラー画面を生成する。再生制御部104を介してモニタ120に生成したエラー画面を表示し、以下の処理を中止する。

[0109] 所定時間以内に、送受信部101を介してバックアップ装置500から、起動通知を受信したとすると、主制御部118は、認証部102へ、バックアップ装置500との機器認証を指示する。認証部102による機器認証が失敗であった場合、主制御部118は、バックアップ装置500との通信に失敗したため、リストアできないことを利用者に通知するエラー画面を生成し、再生制御部104を介してモニタ120に生成したエラー画面を表示し、以下の処理を中止する。

[0110] 機器認証が成功であった場合、主制御部118は、認証部102から、セッション鍵を受け取る。主制御部118は、バックアップ装置500との間の情報の送受信において、受け取ったセッション鍵を共通鍵暗号方式により秘密通信を行う。説明の簡略化のため、以下の説明では、秘密通信に係る暗号化及び復号の処理についての記載を省略する。

主制御部118は、固有情報記憶部108から装置識別子115「ID__A」を読み出し、リストア可能な暗号化コンテンツの情報を要求するリストア情報要求と読み出した装置識別子115「ID__A」とを送受信部101を介してバックアップ装置500へ送信する。

[0111] 次に、主制御部118は、送受信部101を介して、バックアップ装置500から、バックアップ装置500の記憶している暗号化コンテンツそれぞれに対応するコンテンツID、タイトル及び録画日時を受信する。受信したコンテンツID、タイトル及び録画日時を一時的に記憶し、情報記憶部110に記憶されている画像データと受信したタイトル及び録画日時とを用いて、図7(b)に示すリストア情報画面221を生成し、再生制御部1

04を介してモニタ120に生成したリストア情報画面221を表示する。

[0112] リストア情報画面221には、複数のコンテンツボタン222～225が表示されている。

主制御部118は、入力部103から、いずれかのコンテンツボタンの選択を示す操作指示情報を受け取り、受け取った操作指示情報と対応するコンテンツIDを読み出す。次に、主制御部118は、読み出したコンテンツIDと、コンテンツIDの示す暗号化コンテンツのリストアを要求するリストア要求とを、送受信部101を介して、バックアップ装置500へ送信する。

[0113] 次に、送受信部101を介して、バックアップ装置500から、暗号化コンテンツとコンテンツ鍵と有効期限とを受信する。情報記憶部110に新たなコンテンツファイルを生成し、生成したコンテンツファイルに、利用者により選択されたコンテンツボタンと対応するコンテンツIDと受信した暗号化コンテンツとを書き込む。

次に、主制御部118は、セキュア記憶部113から装置固有鍵116「Key__A」を読み出し、読み出した装置固有鍵116「Key__A」と受信したコンテンツ鍵とを暗号処理部109へ出力し、コンテンツ鍵暗号化を指示する。暗号処理部109から暗号化コンテンツ鍵を受け取ると、新たに生成したコンテンツファイルに受け取った暗号化コンテンツ鍵を書き込む。

[0114] 次に、主制御部118は、情報記憶部110上に新たに生成したコンテンツファイルから暗号化コンテンツと暗号化コンテンツ鍵とを読み出し、読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出する。ハッシュ値を算出すると、主制御部118は、利用者により選択されたコンテンツボタンと対応するコンテンツID、タイトル、録画日時、有効期限及び算出したハッシュ値を含むコンテンツ情報を生成し、生成したコンテンツ情報をコンテンツ管理表121に追加する。このとき、追加したコンテンツ情報にバックアップフラグ「1」及び優先度「2」を書き込み、リストア処理を終了する。

[0115] これらの処理の途中で、バックアップ装置500から、リストアできないことを示すエラー通知を受け取ると、リストアに失敗したことを示すエラー画面を生成し、再生制御部104を介して、生成したエラー画面をモニタ120に表示する。

ここでは、利用者の操作により、リストアするコンテンツを選択し、選択されたコンテ

ンツをバックアップ装置500から取得しているが、バックアップ履歴表131を利用して、情報記憶部110の状態を、バックアップを行った直後の状態に戻してもよい。この場合、主制御部118は、バックアップ履歴表131からバックアップを行った日付を読み出し、読み出した日付をモニタ120に表示する。利用者は、表示された日付のいずれかを選択する。主制御部118は、バックアップ履歴表131に、選択された日付と対応して記憶されているコンテンツIDを読み出す。読み出したコンテンツIDのうち、コンテンツ管理表121に含まれていないコンテンツIDのみを抽出し、抽出したコンテンツIDをバックアップ装置500に送信し、送信したコンテンツIDと対応する暗号化コンテンツの送信を要求する。

(c-5)バックアップ処理

主制御部118は、利用者の操作によるバックアップに関する設定を記憶している。ここでは、上記の初期設定画面191において、入力された設定事項を記憶しているとして説明する。

[0116] 主制御部118は、定期的に時刻を監視しており、現在時刻が「日曜 0時30分」であると判断すると、セキュア記憶部113に記憶されているコンテンツ管理表121を構成するコンテンツ情報を一つずつ順番に選択し、選択されたコンテンツ情報について以下の処理を行う。

選択されたコンテンツ情報に含まれるバックアップフラグを読み出す。読み出したバックアップフラグが「0」であれば、次のコンテンツ情報の処理へ移る。

[0117] 「0」でなければ、主制御部118は、選択したコンテンツ情報に含まれるコンテンツIDを基に、情報記憶部110上で、選択したコンテンツ情報と対応するコンテンツファイルを検出する。検出したコンテンツファイルに含まれる暗号化コンテンツと暗号化コンテンツ鍵とを情報記憶部110から読み出し、読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出する。算出したハッシュ値と選択したコンテンツ情報に含まれるハッシュ値とを比較する。両者が一致しなければ、次のコンテンツ情報の処理へ移る。

[0118] 両者が一致すれば、主制御部118は、送受信部101を介して、バックアップ装置500へ、起動指示を送信する。所定時間以内に、送受信部101を介してバックアップ

装置500から、起動通知を受信しなければ、主制御部118は、以降の処理を中止する。

所定時間以内に、送受信部101を介して起動通知を受信すると、主制御部118は、認証部102へ、バックアップ装置500との機器認証を指示する。認証部102による機器認証が失敗であった場合、主制御部118は、以降の処理を中止する。

[0119] 認証部102による機器認証が成功であれば、主制御部118は、認証部102から、セッション鍵を受け取る。主制御部118は、バックアップ装置500との間の情報の送受信において、受け取ったセッション鍵を用いた共通鍵暗号方式により、秘密通信を行う。説明の簡略化のため、以下の説明では、秘密通信に係る暗号化及び復号の処理についての記載を省略する。

[0120] 主制御部118は、固有情報記憶部108から装置固有鍵116「Key__A」を読み出し、読み出した装置固有鍵116「Key__A」と情報記憶部110から読み出した暗号化コンテンツ鍵とを暗号処理部109へ出力し、暗号化コンテンツ鍵の復号を指示する。

主制御部118は、暗号処理部109からコンテンツ鍵を受け取る。コンテンツ鍵を受け取ると、検出したコンテンツファイルに含まれる暗号化コンテンツを読み出し、固有情報記憶部108から装置識別子115「ID__A」を読み出し、セキュア記憶部113から、選択したコンテンツ情報に含まれるコンテンツID、タイトル及び録画日時を読み出す。次に、主制御部118は、バックアップを指示するバックアップ要求、読み出した装置識別子115「ID__A」、コンテンツID、タイトル、録画日時、コンテンツ鍵及び暗号化コンテンツを、送受信部101を介して、バックアップ装置500へ送信する。

[0121] 次に、主制御部118は、送受信部101を介してバックアップ装置500から、バックアップ要求を受け付けられないことを示すエラー通知又は有効期限を受信する。

エラー通知を受信した場合、主制御部118は、以降の処理を中止する。

有効期限を受信した場合、主制御部118は、選択したコンテンツ情報に受信した有効期限を書き込み、バックアップフラグを「1」に変更する。次に、優先度に「2」を書き込み、次のコンテンツ情報の処理に移る。

[0122] 全てのコンテンツ情報について、上記の処理が終了すると、主制御部118は、コンテンツ管理表121に含まれる各コンテンツ情報から、コンテンツIDを読み出し、読み

出したコンテンツIDと現在の日付とを、バックアップ履歴表131に書き込む。

なお、利用者により入力部103の備えるバックアップボタンが押下されると、主制御部118は、初期設定処理において、設定されたバックアップスケジュールとは無関係に、上記のバックアップ処理を開始する。

(10)再生制御部104及びモニタ120

再生制御部104は、画像信号処理部と音声信号処理部とを含んで構成される。再生制御部104は、デコード部105から画像データ及び音声データを受け取る。画像信号処理部は、受け取った画像データから画像信号を生成する。垂直同期信号、水平同期信号及び生成した画像信号をモニタ120へ出力する。また、制御部107の指示により、各種の画面データから、画像信号を生成し、モニタ120へ出力する。

[0123] 音声信号処理部は、受け取った音声データからアナログ音声信号を生成し、生成したアナログ音声信号をモニタ120へ出力する。

モニタ120は、スピーカを内蔵しており、画像信号処理部から、水平同期信号、垂直同期信号及び画像信号を受け取り、受け取った水平同期信号、垂直同期信号及び画像信号に基づいて、画像を表示する。また、スピーカは、音声信号処理部から、アナログ音声信号を受け取り、受け取ったアナログ音声信号を音声に変換し、出力する。

(11)入出力部112

入出力部112は、一例として、DVD、メモ리카ードといった記録メディアを装着される。制御部107の指示により、記録メディアに記録されている情報の読み出し及び記録メディアへの情報の書き込みを行う。

1. 3 バックアップ装置500

バックアップ装置500は、図8に示すように、送受信部501、認証部502、電源部503、制御部507、暗号処理部509、固有情報記憶部504、コンテンツ記憶部510、セキュア情報記憶部511、入力部512及び表示部513から構成される。

[0124] バックアップ装置500は、具体的にはマイクロプロセッサ、RAM、ROMを含んで構成されるコンピュータシステムである。RAM及びROMには、コンピュータプログラムが記憶されており、マイクロプロセッサが前記コンピュータプログラムに従って動作す

ることにより、バックアップ装置500は、その機能の一部を達成する。

(1)固有情報記憶部504

固有情報記憶部504は、ROMから構成され、図8に示すように装置固有鍵516「Key_C」を記憶している。装置固有鍵516「Key_C」は、バックアップ装置500に固有の鍵データであり、バックアップ装置500の出荷時に書き込まれる。

[0125] (2)コンテンツ記憶部510

コンテンツ記憶部510は、ハードディスクユニットから構成され、一例として、図9に示すようにコンテンツファイル529、534、539・・・を記憶している。

各コンテンツファイルは、コンテンツID、暗号化コンテンツ及び暗号化コンテンツ鍵を含む。コンテンツIDは、暗号化コンテンツと対応する識別情報である。暗号化コンテンツは、コンテンツ鍵を用いて、コンテンツに暗号化アルゴリズムE1を施して生成されたものである。暗号化コンテンツ鍵は、固有情報記憶部508の記憶している装置固有鍵516「Key_C」を用いて、コンテンツの暗号化に使用されたコンテンツ鍵に暗号化アルゴリズムE1を施して生成されたものである。

[0126] 例えば、コンテンツファイル529は、コンテンツID531「A001」、暗号化コンテンツ532、暗号化コンテンツ鍵533「Enc(Key_C, Key_1a)」を含む。

コンテンツID531「A001」は、暗号化コンテンツ532を一意に識別する情報であり、これは、HDレコーダ100の情報記憶部110に記憶されているコンテンツID136「A001」と同一である。暗号化コンテンツ532は、コンテンツ鍵「Key_1a」を用いて、コンテンツに、暗号化アルゴリズムE1を施して、生成されたものである。暗号化コンテンツ532は、HDレコーダ100の情報記憶部110に記憶されている暗号化コンテンツ137と同一のものである。

[0127] 暗号化コンテンツ鍵533「Enc(Key_C, Key_1a)」は、固有情報記憶部504の記憶している装置固有鍵516「Key_C」を用いて、コンテンツ鍵「Key_1a」に暗号化アルゴリズムE1を施して生成されたものである。

(3)セキュア情報記憶部511

セキュア情報記憶部511は、フラッシュメモリ含んで構成される。また、セキュア情報記憶部511は、保護機構を備えており、外部機器によるアクセスから保護されている

。

[0128] セキュア情報記憶部511は、一例として、図10に示すように、バックアップ管理表521及び許可装置識別情報551を記憶している。

バックアップ管理表521は、図11に示すように、複数のバックアップ情報522、523、524、525・・・を含んで構成される。各バックアップ情報は、コンテンツID、タイトル、録画日時、バックアップ元装置識別子及びハッシュ値から構成される。各コンテンツ情報は、コンテンツ記憶部510に記憶されているコンテンツファイルと1対1に対応している。

[0129] コンテンツIDは、対応するコンテンツファイルに含まれるコンテンツIDと同一であり、暗号化コンテンツを示す識別情報である。タイトルは、対応する暗号化コンテンツの名称である。

録画日時は、HDレコーダ100又はHDレコーダ400が、放送装置10又は外部記録メディアから、暗号化コンテンツのもとになるコンテンツを取得した時点の日付と時刻である。バックアップ元装置識別子は、対応するコンテンツファイルに含まれる暗号化コンテンツのバックアップを要求した装置の装置識別子である。ハッシュ値は、対応するコンテンツファイルに含まれる暗号化コンテンツと暗号化コンテンツ鍵とを結合し、ハッシュ関数に代入して生成されたものである。

[0130] 許可装置識別情報551は、バックアップ装置500が、バックアップ要求など各種の指示を受け付ける機器の識別情報を含んで構成される。本実施の形態では、バックアップシステム1を形成するHDレコーダ100を示す装置識別子552「ID_A」及びHDレコーダ400を示す装置識別子553「ID_B」を含んでいる。

(4)電源部503

電源部503は、外部電源から電力を取得し、制御部507の指示に従って、取得した電力を、バックアップ装置500を構成する各回路へ供給する。

[0131] 通常時、電源部503は、送受信部501及び制御部507のみへ、電力を供給している。

電源部503は、制御部507から、電力供給開始を指示される。電力供給開始を指示されると、その他の各部への電力供給を開始する。また、制御部507から電力供給

の停止を指示される。電力供給の停止を指示されると、送受信部501及び制御部507以外の各部への電力供給を停止する。

[0132] (5)送受信部501

送受信部501は、LAN30と接続されており、LAN30に接続されている外部機器と制御部507及び認証部502との間の各種の情報の送受信を行う。ここで、外部機器とは、HDレコーダ100及びHDレコーダ400である。

(6)認証部502

認証部502は、予め、バックアップ装置500に固有の秘密鍵SK__C、公開鍵証明書Cert__C、認証局の公開鍵PK__CA及びCRLを記憶している。公開鍵証明書Cert__Cは、秘密鍵SK__Cと対応する公開鍵PK__Cの正当性を証明するものであり、証明書識別番号、前記公開鍵PK__C、認証局の署名データを含んで構成される。認証局の署名データは、認証局の秘密鍵SK__CAを用いて、少なくとも、公開鍵PK__Cに署名生成アルゴリズムSを施して生成されたものである。

[0133] CRLは、無効になった公開鍵証明書の証明書識別番号を含む。

認証局の公開鍵PK__CAは、認証局の秘密鍵SK__CAと対になる公開鍵である。

認証部502は、制御部507の指示により外部機器との間で、DTCPに従った機器認証を行い、認証が失敗した場合、制御部507と外部機器との通信を禁止する。認証が成功であった場合、外部機器との間で共通のセッション鍵を生成し、生成したセッション鍵を制御部507へ出力する。機器認証の動作については、後に詳細に説明する。

[0134] (7)暗号処理部509

暗号処理部509は、制御部507から平文と鍵を受け取り、平文の暗号化を指示される。また、制御部507から暗号文と鍵を受け取り、暗号文の復号を指示される。

暗号化を指示されると、受け取った鍵を用いて、受け取った平文に暗号化アルゴリズムE1を施して、暗号文を生成し、生成した暗号文を制御部507へ出力する。

[0135] 復号を指示されると、受け取った鍵を用いて受け取った暗号文に、復号アルゴリズムD1を施して復号文を生成し、生成した復号文を制御部107へ出力する。

暗号処理部509の受け取る平文と鍵との組み合わせは、一例として、コンテンツ鍵

と装置固有鍵「Key__C」である。また、暗号処理部509の受け取る暗号文と鍵との組み合わせは、暗号化コンテンツ鍵と装置固有鍵「Key__C」である。

[0136] (8)制御部507

制御部507は、視聴時間「240時間」を記憶している。視聴時間は、バックアップの対象となった暗号化コンテンツを、HDレコーダ100及びHDレコーダ400が利用できる時間である。

また、制御部507は、具体的には図示していないが、外部から操作することが出来ないセキュアクロックを備えている。

[0137] 制御部507は、送受信部501を介して外部機器から、起動を指示する起動指示を受け取る。外部機器とは、HDレコーダ100又はHDレコーダ400である。

起動指示を受け取ると、電源部503へ、電力供給開始を指示する。次に、送受信部501を介して、外部機器へ、バックアップ装置500が起動したことを示す起動通知を送信する。

[0138] 次に、制御部507は、認証部502へ外部機器との機器認証を指示する。認証部502による機器認証が失敗であった場合、電源部503へ電力供給の停止を指示する。

認証部502による機器認証が成功であった場合、認証部502からセッション鍵を受け取る。以下の処理において、制御部507は、受け取ったセッション鍵を用いた共通鍵暗号方式により、外部機器との間で秘密通信を実現するが、秘密通信に係る暗号化及び復号の処理についての説明を省略する。

[0139] 次に、制御部507は、送受信部501を介して、外部機器から、装置識別子とバックアップ要求とコンテンツIDとコンテンツ鍵とタイトルと録画日時と暗号化コンテンツとを受信する。又は、装置識別子と延長要求とコンテンツIDとを受信する。又は、装置識別子とリストア情報要求とを受信する。

(a)バックアップ処理

装置識別子とバックアップ要求とコンテンツIDとコンテンツ鍵とタイトルと録画日時と暗号化コンテンツとを受信すると、制御部507は、受信した装置識別子が、セキュア情報記憶部511に記憶されている許可装置識別情報551に含まれていることを確認する。含まれていなければ、送受信部501を介して、外部機器へ、バックアップ要求

を受け付けられないことを示すエラー通知を送信する。次に、電源部503へ電力供給の停止を指示する。

- [0140] 受信した装置識別子が、セキュア情報記憶部511に記憶されている許可装置識別情報551に含まれていれば、固有情報記憶部504から装置固有鍵516「Key_C」を読み出す。読み出した装置固有鍵516「Key_C」と受信したコンテンツ鍵とを暗号処理部509へ出力し、コンテンツ鍵の暗号化を指示する。

次に、制御部507は、暗号処理部509から、暗号化コンテンツ鍵を受け取り、受信したコンテンツIDと暗号化コンテンツと暗号化コンテンツ鍵とを含むコンテンツファイルを生成し、生成したコンテンツファイルをコンテンツ記憶部510へ書き込む。

- [0141] 次に、制御部507は、コンテンツ記憶部510に書き込んだコンテンツファイルに含まれる暗号化コンテンツと暗号化コンテンツ鍵とを読み出し、読み出した暗号化コンテンツと暗号化コンテンツ鍵との結合物をハッシュ関数に代入し、160ビットのハッシュ値を生成する。

次に、制御部507は、受信したコンテンツID、タイトル、録画日時、装置識別子及び算出したハッシュ値からなるバックアップ情報を生成し、生成したバックアップ情報をバックアップ管理表521に追加する。ここで、受信した装置識別子をバックアップ元装置識別子とする。

- [0142] 次に、制御部507は、セキュアクロックから現在時刻を取得し、取得した現在時刻に視聴時間「240時間」を加算して有効期限を算出する。次に、算出した有効期限を、送受信部501を介して、外部機器へ送信する。

送信が完了すると、制御部507は、電源部503へ電力供給の停止を指示する。

(b)有効期限の延長処理

送受信部501を介して、装置識別子と延長要求とコンテンツIDとを受信すると、制御部507は、受信した装置識別子が、セキュア情報記憶部511に記憶されている許可装置識別情報551に含まれる装置識別子のいずれかと一致することを確認する。一致しなければ、送受信部501を介して、外部機器へ、延長要求を受け付けられないことを示すエラー通知を送信する。次に、電源部503へ電力供給の停止を指示する。

[0143] 受信した装置識別子が、許可装置識別情報551に含まれる装置識別子のいずれかと一致すれば、制御部507は、受信したコンテンツIDと同一のコンテンツIDを含むバックアップ情報を選択する。

次に、制御部507は、コンテンツ記憶部510から、受信したコンテンツIDと同一のコンテンツIDを含むコンテンツファイルを検出し、検出したコンテンツファイルに含まれる暗号化コンテンツと暗号化コンテンツ鍵とを読み出す。読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出する。

[0144] 算出したハッシュ値と選択したバックアップ情報に含まれるハッシュ値とを比較し、両者が一致しなかった場合、制御部507は、延長要求を受け付けられないことを示すエラー通知を、送受信部501を介して外部機器へ出力する。

両者が一致する場合、制御部507は、セキュアクロックから現在時刻を取得し、取得した現在時刻に、視聴時間「240時間」を加算して有効期限を算出する。次に、算出した有効期限を、送受信部501を介して、外部機器へ送信する。

[0145] (c)リストア処理

外部機器から、装置識別子とリストア情報要求とを受信すると、制御部507は、受信した装置識別子が、セキュア情報記憶部511に記憶されている許可装置識別情報551に含まれていることを確認する。含まれていなければ、送受信部501を介して、外部機器へ、リストア情報要求を受け付けられないことを示すエラー通知を送信する。次に、電源部503へ電力供給の停止を指示する。

[0146] 受信した装置識別子が、許可装置識別情報551に含まれていれば、制御部507は、セキュア情報記憶部511の記憶しているバックアップ管理表521に含まれる全てのバックアップ情報からコンテンツIDとタイトルと録画時刻とを読み出す。読み出したコンテンツIDとタイトルと録画時刻とを、送受信部501を介して外部機器へ送信する。

次に、制御部507は、送受信部501を介して外部機器から、コンテンツIDとリストア要求とを受信する。コンテンツIDとリストア要求とを受信すると、バックアップ管理表521から、受信したコンテンツIDと同一のコンテンツIDを含むバックアップ情報を選択する。

[0147] 次に、制御部507は、受信したコンテンツIDを基に、選択したバックアップ情報と対

応するコンテンツファイルを検出する。検出したコンテンツファイルから暗号化コンテンツと暗号化コンテンツ鍵とを読み出す。読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出する。算出したハッシュ値と選択したバックアップ情報に含まれるハッシュ値とを比較する。

[0148] 両者が一致しなければ、制御部507は、送受信部501を介して、外部機器へ、リストア要求を受け付けられないことを示すエラー通知を送信する。次に、電源部503へ電力供給の停止を指示する。

両者が一致すれば、制御部507は、固有情報記憶部504から装置固有鍵516「Key__C」を読み出し、読み出した暗号化コンテンツ鍵と装置固有鍵516「Key__C」とを暗号処理部509へ出力し、暗号化コンテンツ鍵の復号を指示する。次に、暗号処理部509から、コンテンツ鍵を受け取る。コンテンツ鍵を受け取ると、制御部507は、検出したコンテンツファイルから暗号化コンテンツを読み出す。

[0149] 次に、制御部507は、セキュアクロックから現在時刻を取得し、取得した現在時刻に視聴時間「240時間」を加算して有効期限を算出する。読み出した暗号化コンテンツと、受け取ったコンテンツ鍵と算出した有効期限とを、送受信部501を介して、外部機器へ送信する。

送信が完了すると、制御部507は、電源部503へ、電力供給の停止を指示する。

[0150] (9)入力部512及び表示部513

入力部512は、操作者による情報及び指示の入力を受け付け、受け付けた情報及び受け付けた指示に応じた操作指示情報を制御部507へ出力する。

表示部513は、制御部507の制御により、各種情報を表示する。

1. 4 バックアップシステム1の動作

以下に、バックアップシステム1の動作について説明する。

[0151] (1)HDLレコーダ100の動作

HDLレコーダ100の動作について、図12に示すフローチャートを用いて説明する。説明の便宜上、ステップS111から説明を始める。なお、主制御部118は、図7に示す初期設定画面191により設定されたバックアップに関する設定事項、コンテンツの種類「全て」、バックアップスケジュール「日曜 0:30」、バックアップモード「新規のみ

」、リストアモード「手動」を記憶している。

[0152] HDレコーダ100の制御部107は、セキュアクロック117の示す現在時刻と自身の記憶している延長時刻「2:00」とを比較し(ステップS111)、現在時刻が「2:00」であると判断すると(ステップS111のYES)、有効期限の延長処理を行う(ステップS112)。現在時刻が「2:00」でないと判断すると(ステップS111のNO)、ステップS112は行わず、ステップS113へ移る。

[0153] 次に、制御部107は、現在時刻と記憶しているバックアップスケジュール「日曜0:30」とを比較し、現在時刻が「日曜0:30」であると判断すると(ステップS113のYES)、バックアップ処理を行う(ステップS114)。

現在時刻が「日曜0:30」でないと判断すると(ステップS113のNO)、ステップS115へ処理を移す。

[0154] 次に、直前に有効期限切れのコンテンツ削除処理を行ってからの経過時間が「30分」を超えていれば(ステップS115のYES)、制御部107は、再び、コンテンツ管理表121の各コンテンツ情報に含まれる有効期限と、現在時刻とを比較し、有効期限の終了しているコンテンツ情報と対応するコンテンツファイルを情報記憶部110から削除し、前記コンテンツ情報をコンテンツ管理表121から削除する(ステップS116)。

[0155] 経過時間が「30分」未満であれば(ステップS115のNO)、制御部107は、ステップS116の処理は行わず、ステップS117へ処理を移す。

次に、利用者の操作により電源ボタンが押下されると(ステップS117のYES)、制御部107は、入力部103を介して、利用者によるボタン操作及びリモートコントローラの操作を受け付け(ステップS118)、受け付けたボタン操作に応じて各種の処理を行う。

[0156] 電源ボタンを押下されなければ(ステップS117のNO)、ステップS111へ戻り、現在時刻の監視を続ける。

ステップS118において、録画ボタンが押下されると、制御部107は、録画処理を実行する(ステップS122)。録画処理が終了すると、ステップS118へ戻り、利用者の操作を受け付ける。

[0157] また、ステップS118において、電源ボタンが押下されると、ステップS111へ戻り、

時刻の監視を続ける。

ステップS118において、その他のボタンが押下されると、その他の処理を行う(ステップS123)。

ステップS118において、メニューボタンの押下を受け付けると、制御部107は、モニタ120に、図6(a)に示すメニュー画面181を表示し(ステップS121)、利用者による選択を受け付ける(ステップS124)。

[0158] 初期設定ボタン188が選択されると(ステップS124)、制御部107は、モニタ120に、図7(a)に示す初期設定画面191を表示し(ステップS126)、利用者のボタン操作による、各種の設定を受け付ける(ステップS127)。設定の受付が終了すると、ステップS118へ戻る。

ステップS124において、再生リスト表示ボタン182が選択されると、再生処理を行う(ステップS129)。再生処理が終了すると、ステップS118へ戻る。

[0159] ステップS124において、リストアボタン183が選択されると、制御部107は、リストア処理を行う(ステップS131)。リストア処理が終了すると、ステップS118へ戻る。また、その他のボタンが選択されると、その他の処理を行い(ステップS181)、ステップS118へ戻る。

(2) HDレコーダ100による録画処理

以下に、HDレコーダ100による録画処理について、図13に示すフローチャートを用いて説明する。これは、図12のステップS122の詳細である。

[0160] 録画ボタンの押下を示す操作指示情報を受け取ると、制御部107は、新たなコンテンツIDを生成し(ステップS151)、生成したコンテンツIDを含むコンテンツ情報をコンテンツ管理表121に追加する(ステップS153)。追加したコンテンツ情報の録画日時に現在時刻を書き込み(ステップS154)、種類に「放送番組」を書き込む(ステップS156)。また、圧縮方式に「MPEG2」を書き込み(ステップS157)、バックアップフラグに「0」を書き込み(ステップS158)、優先度に「1」を書き込む(ステップS161)。

[0161] 次に、制御部107は、鍵生成部106へコンテンツ鍵の生成を指示する。鍵生成部106は、コンテンツ鍵を生成し、生成したコンテンツ鍵を制御部107へ出力する(ステップS162)。

次に、制御部107は、情報記憶部110に新たなコンテンツファイルを生成する(ステップS163)。次に、放送受信部114へ録画指示を出力する。放送受信部114は、アンテナ130を介して、コンテンツを受信し(ステップS164)、受信したコンテンツをTSパケット単位で制御部107へ出力する。

- [0162] 利用者により、ストップボタンが押下されるまで以下のステップS164～ステップS168の処理を繰返し、ストップボタンが押下されると(ステップS166のYES)、ステップS171へ処理を移す。

まず、制御部107は、放送受信部114から受け取ったコンテンツと鍵生成部106から受け取ったコンテンツ鍵とを暗号処理部109へ出力し、コンテンツの暗号化を指示する。暗号処理部109は、受け取ったコンテンツ鍵を用いて、コンテンツを暗号化し、生成した暗号化コンテンツを制御部107へ出力する(ステップS167)。

- [0163] 制御部107は、暗号処理部109により生成された暗号化コンテンツを、情報記憶部110に生成したコンテンツファイルへ書き込み(ステップS168)、ステップS164へ戻る。

ストップボタンが押下されると(ステップS166のYES)、制御部107は、固有情報記憶部108から、装置固有鍵116「Key__A」を読み出し(ステップS171)、読み出した装置固有鍵116「Key__A」とコンテンツ鍵とを暗号処理部109へ出力し、コンテンツの鍵の暗号化を指示する。暗号処理部109は、受け取った装置固有鍵116「Key__A」を用いてコンテンツ鍵を暗号化し、暗号化コンテンツ鍵を生成する。生成した暗号化コンテンツ鍵を制御部107へ出力する(ステップS172)。

- [0164] 制御部107は、暗号処理部109から暗号化コンテンツ鍵を受け取り、受け取った暗号化コンテンツ鍵と生成したコンテンツIDとを、コンテンツファイルへ書き込む(ステップS173)。

次に、制御部107は、暗号化コンテンツと暗号化コンテンツ鍵と結合してハッシュ関数に代入し、ハッシュ値を算出する(ステップS174)。追加したコンテンツ情報に算出したハッシュ値を書き込む(ステップS176)。

- [0165] ステップS164～ステップS168と並行して、制御部107は、ステップS181～ステップS189を実行する。まず、制御部107は、情報記憶部110の空き容量を監視する(

ステップS181)。空き容量が充分あると判断し(ステップS181のYES)、利用者によりストップボタンが押下されなければ(ステップS182のNO)、ステップS181へ戻り空き容量の監視を続ける。利用者により、ストップボタンが押下された場合(ステップS182のYES)、制御部107は、ステップS171へ処理を移す。

[0166] 空き容量が不足していると判断した場合(ステップS181のNO)、制御部107は、セキュア記憶部113に記憶されているコンテンツ管理表121に含まれるコンテンツ情報を先頭から順次選択する(ステップS184)。このとき、コンテンツ管理表121に含まれる全てのコンテンツ情報について、ステップS187~189の処理を終えている場合、つまり、削除可能なコンテンツが情報記憶部110に存在しない場合(ステップS186のYES)、制御部107は、ランプを点滅させるなどして、利用者に記憶容量が不足していることを通知し、ステップS171へ処理を移す。

[0167] ステップS186のNOの場合、制御部107は、選択したコンテンツ情報に含まれる優先度を読み出し、読み出した優先度が、「2」であるか否かを判定する(ステップS187)。優先度「2」でなければ(ステップS187のNO)、ステップS184に戻り、次のコンテンツ情報を選択する。

優先度「2」であれば(ステップS187のYES)、選択したコンテンツ情報に含まれるコンテンツIDを基に、情報記憶部110において、選択したコンテンツ情報と対応するコンテンツファイルを検出し、検出したコンテンツファイルを情報記憶部110から削除する(ステップS188)。次に、選択したコンテンツ情報を、コンテンツ管理表121から削除し(ステップS189)、ステップS181へ戻る。

[0168] (3)HDレコーダ100の再生時の動作

以下に、図15に示すフローチャートを用いてHDレコーダ100の再生時の動作について説明する。これは、図12のステップS129の詳細である。

利用者により、図6に示すメニュー画面181の再生リスト表示ボタン182が選択されると、制御部107は、図6(b)に示すような再生リスト画面211を生成し、生成した再生リスト画面211をモニタ120へ表示する(ステップS201)。

[0169] 次に、入力部103を介して、利用者によるコンテンツの選択を受け付ける(ステップS202)。以下の説明において、利用者がコンテンツボタン212を選択した場合につ

いて説明する。

制御部107は、選択されたコンテンツボタン212と対応するコンテンツ情報122に含まれるコンテンツID「A001」をセキュア記憶部113から読み出し(ステップS203)、読み出したコンテンツID「A001」を基に、情報記憶部110上で、コンテンツ情報122と対応するコンテンツファイル134を検出する(ステップS204)。検出したコンテンツファイル134から暗号化コンテンツ137と暗号化コンテンツ鍵138「Enc(Key__A, Key__1a)」を読み出す(ステップS205)。読み出した暗号化コンテンツ137と暗号化コンテンツ鍵138「Enc(Key__A, Key__1a)」とを結合してハッシュ関数に代入し、ハッシュ値を算出する(ステップS206)。

[0170] 次に、制御部107は、コンテンツID「A001」を含むコンテンツ情報122からハッシュ値「01a」を読み出す(ステップS207)。算出したハッシュ値と読み出したハッシュ値とを比較し(ステップS208)、両者が一致しない場合(ステップS208のNO)、選択されたコンテンツの再生が出来ないことを示すエラー画面を生成し、生成したエラー画面を表示し(ステップS209)、再生処理を終了する。

[0171] 算出したハッシュ値と読み出したハッシュ値とが一致する場合(ステップS208のYES)、制御部107は、固有情報記憶部108から装置固有鍵116「Key__A」を読み出し、暗号化コンテンツ鍵138「Enc(Key__A, Key__1a)」と読み出した装置固有鍵116「Key__A」とを暗号処理部109へ出力し、暗号化コンテンツ鍵138「Enc(Key__A, Key__1a)」の復号を指示する。

[0172] 暗号処理部109は、制御部107から暗号化コンテンツ鍵「Enc(Key__A, Key__1a)」と装置固有鍵116「Key__A」とを受け取る。受け取った装置固有鍵116「Key__A」を用いて、暗号化コンテンツ鍵「Enc(Key__A, Key__1a)」を復号してコンテンツ鍵「Key__1a」を生成し、生成したコンテンツ鍵「Key__1a」を制御部107へ出力する(ステップS211)。

[0173] 制御部107は、暗号処理部109からコンテンツ鍵「Key__1a」を受け取る。コンテンツ鍵「Key__1a」を受け取ると、コンテンツファイル134から、暗号化コンテンツ137を読み出し(ステップS212)、読み出した暗号化コンテンツ137とコンテンツ鍵「Key__1a」とを暗号処理部109へ出力し、暗号化コンテンツの復号を指示する。

[0174] 暗号処理部109は、制御部107の指示に従って、コンテンツ鍵「Key__1a」を用いて暗号化コンテンツを復号し、コンテンツを生成し、生成したコンテンツを制御部107へ出力する(ステップS213)。

制御部107は、暗号処理部109からコンテンツを受け取り、受け取ったコンテンツを再生制御部104へ出力する。再生制御部104は、制御部107からコンテンツを受け取り、受け取ったコンテンツを伸長して画像信号及び音声信号を生成し(ステップS214)、生成した画像信号及び音声信号をモニタ120へ出力し、モニタ120は、画像及び音声を再生する(ステップS216)。

[0175] (4)HDレコーダ100及びバックアップ装置500によるリストア処理

図16～17に示すフローチャートを用いて、HDレコーダ100及びバックアップ装置500によるリストア処理について説明する。これは、図12のステップS131の詳細である。

利用者により、図6に示すメニュー画面181のリストアボタン183が選択されると、制御部107は、送受信部101を介して、バックアップ装置500へ起動指示を送信する(ステップS231)。

[0176] バックアップ装置500の制御部507は、送受信部501を介して起動指示を受信し、電源部503へ電力供給開始を指示する。電源部503は、バックアップ装置500を構成する各部への電力供給を開始する(ステップS232)。

次に、制御部507は、送受信部501を介して、HDレコーダ100へ起動通知を送信する(ステップS233)。

[0177] HDレコーダ100の制御部107は、送受信部101を介して、所定時間以内にバックアップ装置500から、起動通知を受信しなければ(ステップS234のNO)、リストアできないことを示すエラー画面を生成し、再生制御部104を介して生成したエラー画面をモニタ120へ表示する(ステップS236)。

所定時間以内に起動通知を受信すると(ステップS234のYES)、認証部102へバックアップ装置500との機器認証を指示する。認証部102は、制御部107の指示により、バックアップ装置500との間で機器認証を行う(ステップS237)。

[0178] 認証部102による機器認証が失敗であれば(ステップS239のNO)、制御部107は

、ステップS236へ処理を移す。

機器認証が成功であれば(ステップS239のYES)、固有情報記憶部108から装置識別子115「ID_A」を読み出し(ステップS241)、送受信部101を介して、読み出した装置識別子115「ID_A」とリストア情報要求を、バックアップ装置500へ送信する(ステップS244)。

- [0179] HDレコーダ100との機器認証が失敗すると(ステップS242のNO)、バックアップ装置500の制御部507は、電源部503へ電力供給の停止を指示し、電源部503は、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS243)。

HDレコーダ100との機器認証が成功であると(ステップS242のYES)、次に、送受信部501を介して、HDレコーダ100からリストア情報要求と装置識別子「ID_A」を受信する。受信した装置識別子「ID_A」が、セキュア情報記憶部511に記憶されている許可装置識別情報551に登録されているか否かを判断する(ステップS246)。登録されていないと判断すると(ステップS246のNO)、制御部507は、ステップS263へ処理を移す。

- [0180] 登録されていると判断すると(ステップS246のYES)、バックアップ管理表521を構成する各バックアップ情報からコンテンツID、タイトル及び録画日時を読み出し(ステップS247)、読み出したコンテンツID、タイトル及び録画日時を送受信部501を介して、HDレコーダ100へ送信する(ステップS248)。

HDレコーダ100の制御部107は、送受信部101を介して、バックアップ装置500からコンテンツID、タイトル及び録画日時を受信する。受信したタイトル及び録画日時を用いて図7に示すリストア情報画面221を生成し(ステップS251)、生成したリストア情報画面221を再生制御部104を介してモニタ120に表示する(ステップS252)。

- [0181] 制御部107は、入力部103を介して、利用者によるリストアするコンテンツの選択を受け付ける(ステップS253)。

制御部107は、選択されたコンテンツボタンと対応するコンテンツIDを読み出し(ステップS254)、読み出したコンテンツIDとリストア要求とを、送受信部101を介してバ

ックアップ装置500へ送信する(ステップS256)。

- [0182] バックアップ装置500を構成する制御部507は、送受信部501を介して、リストア要求及びコンテンツIDを受信する。リストア要求を受信すると、制御部507は、セキュア情報記憶部511に記憶されているバックアップ管理表521から受信したコンテンツIDを含むバックアップ情報を選択する(ステップS257)。

次に、制御部507は、受信したコンテンツIDを基に、コンテンツ記憶部510において、選択したバックアップ情報と対応するコンテンツファイルを検出し、検出したコンテンツファイルに含まれる暗号化コンテンツ及び暗号化コンテンツ鍵を読み出す(ステップS259)。制御部507は、読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出する(ステップS260)。

- [0183] 次に、選択したバックアップ情報に含まれるハッシュ値を読み出し(ステップS261)、算出したハッシュ値と読み出したハッシュ値とを比較し、両者が一致しない場合(ステップS262のNO)、制御部507は、受信したコンテンツIDと対応するコンテンツのリストア要求を受け付けられないことを示すエラー通知を生成し、生成したエラー通知を、送受信部501を介してHDレコーダ100へ送信する(ステップS263)。ここで、エラー通知を受信すると、HDレコーダ100の制御部107は、リストアできないことを通知するエラー画面をモニタに表示し、リストア処理を終了する。

- [0184] 次に、制御部507は、電源部503へ、電力供給の停止を指示する。電源部503は、制御部507の指示を受け取り、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS264)。

算出したハッシュ値と読み出したハッシュ値とが一致すると判断すると(ステップS262のYES)、制御部507は、固有情報記憶部504から装置固有鍵516「Key_C」を読み出し(ステップS266)、読み出した装置固有鍵516「Key_C」と暗号化コンテンツ鍵とを暗号処理部509へ出力し、暗号化コンテンツ鍵の復号を指示する。暗号処理部509は、制御部507の指示により、装置固有鍵516「Key_C」を用いて、暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、生成したコンテンツ鍵を制御部507へ出力する(ステップS267)。

- [0185] 制御部507は、暗号処理部509からコンテンツ鍵を受け取り、次に、検出したコンテ

ンツファイルに含まれる、暗号化コンテンツを読み出す(ステップS268)。

次に、制御部507は、セキュアクロックから現在時刻を取得し、取得した現在時刻に視聴時間「240時間」を加算して有効期限を算出する(ステップS269)。送受信部501を介して、HDレコーダ100へ読み出した暗号化コンテンツと受け取ったコンテンツ鍵と算出した有効期限とを送信する(ステップS271)。送信すると、制御部507は、電源部503へ、電力供給の停止を指示し、電源部503は、制御部507の指示を受け取り、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS272)。

[0186] HDレコーダ100の制御部107は、送受信部101を介して、バックアップ装置500から、暗号化コンテンツとコンテンツ鍵と有効期限とを受信する。暗号化コンテンツとコンテンツ鍵と有効期限とを受信すると、情報記憶部110上に新たにコンテンツファイルを生成し、受信した暗号化コンテンツと、コンテンツIDとを、生成したコンテンツファイルへ書き込む(ステップS274)。

[0187] 次に、固有情報記憶部108から、装置固有鍵116「Key__A」を読み出し(ステップS276)、読み出した装置固有鍵116「Key__A」と受信したコンテンツ鍵とを暗号処理部109へ出力し、コンテンツ鍵の暗号化を指示する。暗号処理部109は、制御部107から装置固有鍵116「Key__A」とコンテンツ鍵とを受け取る。受け取った装置固有鍵「Key__A」を用いてコンテンツ鍵を暗号化し、暗号化コンテンツ鍵を生成し、生成した暗号化コンテンツ鍵を制御部107へ出力する(ステップS277)。

[0188] 制御部107は、暗号処理部109から暗号化コンテンツ鍵を受け取り、受け取った暗号化コンテンツ鍵を情報記憶部110上に生成したコンテンツファイルへ書き込む(ステップS278)。

次に、制御部107は、受信した暗号化コンテンツと受け取った暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出する(ステップS279)。

[0189] 制御部107は、選択されたコンテンツボタンと対応するコンテンツIDと、タイトルと、録画日時と、受信した有効期限と、算出したハッシュ値とを含むコンテンツ情報をコンテンツ管理表121に追加する(ステップS281)。追加したコンテンツ情報のバックアップフラグに「1」を書き込み(ステップS284)、優先度「2」を書き込む(ステップS286)

。

[0190] (5)HDレコーダ100及びバックアップ装置500によるバックアップ処理

HDレコーダ100及びバックアップ装置500によるバックアップ処理について、図18～20に示すフローチャートを用いて説明する。これは、図12のステップS114の詳細である。

セキュアクロック117の示す現在時刻が、バックアップスケジュールとして、利用者により設定された「日曜 0:30」になると、制御部107は、セキュア記憶部113に記憶されているコンテンツ管理表121を構成するコンテンツ情報を1つずつ順番に選択する(ステップS301)。このとき、全てのコンテンツ情報を選択し終えており、新たに選択すべきコンテンツ情報が存在しなければ(ステップS302のYES)、バックアップ処理を終了する。全てのコンテンツ情報を選択し終えていなければ(ステップS302のNO)、制御部107は、選択したコンテンツ情報に含まれるバックアップフラグが「0」であるか否か、すなわち選択したコンテンツ情報と対応するコンテンツは、既にバックアップされているか否かを判断する(ステップS303)。バックアップフラグが「0」でない場合(ステップS303のNO)、ステップS301へ戻り、次のコンテンツ情報を選択する。

[0191] バックアップフラグが「0」である場合(ステップS303のYES)、制御部107は、選択したコンテンツ情報からコンテンツIDを読み出し(ステップS304)、読み出したコンテンツIDを基に、選択したコンテンツ情報と対応するコンテンツファイルを検出する(ステップS306)。検出したコンテンツファイルから暗号化コンテンツ及び暗号化コンテンツ鍵を、情報記憶部110から読み出す(ステップS307)。

[0192] 制御部107は、読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出する(ステップS308)。次に、選択したコンテンツ情報に含まれるハッシュ値を読み出し(ステップS309)、読み出したハッシュ値と算出したハッシュ値とを比較する(ステップS311)。両者が一致しない場合、ステップS301に戻り、次のコンテンツ情報の処理に移る。

[0193] 読み出したハッシュ値と算出したハッシュ値とが一致する場合、制御部107は、送受信部101を介して、バックアップ装置500へ起動指示を送信する(ステップS313)

。

バックアップ装置500の制御部507は、送受信部501を介して、HDレコーダ100から起動指示を受信し、電源部503へ電力供給の開始を指示する。電源部503は、制御部507の指示により、バックアップ装置500を構成する各部へ電力供給を開始する(ステップS316)。

[0194] 制御部507は、送受信部501を介して、HDレコーダ100へ起動通知を送信する(ステップS317)。

HDレコーダ100の制御部107は、所定時間以内にバックアップ装置500から起動通知を受信しなければ(ステップS318のNO)、バックアップ処理を終了する。

送受信部101を介して、所定時間以内に起動通知を受信すると(ステップS318のYES)、制御部107は、認証部102へバックアップ装置500との機器認証を指示する。

[0195] 認証部102は、制御部107の指示により、バックアップ装置500と機器認証を行う(ステップS321)。認証部102による機器認証が失敗であれば(ステップS322のNO)、制御部107は、バックアップ処理を終了する。

機器認証が成功であれば(ステップS322のYES)、制御部107は、固有情報記憶部108から装置固有鍵116「Key__A」を読み出し、読み出した装置固有鍵116「Key__A」と選択したコンテンツ情報に含まれる暗号化コンテンツ鍵とを暗号処理部109へ出力し、暗号化コンテンツ鍵の復号を指示する。暗号処理部109は、制御部107の指示を受け、受け取った装置固有鍵116「Key__A」を用いて、暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、生成したコンテンツ鍵を制御部107へ出力する(ステップS323)。

[0196] 制御部107は暗号処理部109からコンテンツ鍵を受け取る。コンテンツ鍵を受け取ると、選択したコンテンツ情報に含まれるコンテンツID、タイトル、録画日時を読み出す(ステップS324)。

次に、制御部107は、固有情報記憶部108から装置識別子115「ID__A」を読み出し、情報記憶部110から選択したコンテンツ情報と対応する暗号化コンテンツを読み出す(ステップS326)。送受信部101を介して、バックアップ要求と読み出した装置識別子115「ID__A」とコンテンツIDとタイトルと録画日時と暗号化コンテンツと受

け取ったコンテンツ鍵とをバックアップ装置500へ送信する(ステップS327)。

- [0197] HDレコーダ100との機器認証が失敗であれば(ステップS328のNO)、制御部507は、電源部503へ電力供給の停止を指示し、電源部503は、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS329)。

機器認証が成功であれば(ステップS328のYES)、制御部507は、送受信部101を介して、HDレコーダ100から、バックアップ要求と装置識別子「ID__A」とコンテンツIDとタイトルと録画日時と暗号化コンテンツとコンテンツ鍵とを受信する。受信した装置識別子「ID__A」が、セキュア情報記憶部511に記憶されている許可装置識別情報551に登録されているか否かを判断する(ステップS331)。登録されていないと判断すると(ステップS331のNO)、制御部507は、送受信部501を介して、バックアップ要求を受け付けられないことを示すエラー通知を、HDレコーダ100へ送信し(ステップS332)、電源部503を介して、バックアップ装置500を構成する各回路への電力供給を停止する(ステップS333)。ここで、エラー通知を受け取ったHDレコーダ100は、バックアップ処理を終了する。

- [0198] 受信した装置識別子「ID__A」が、許可装置識別情報551に登録されていると判断すると(ステップS331のYES)、固有情報記憶部504から装置固有鍵516「Key__C」を読み出し、読み出した装置固有鍵516「Key__C」と受信したコンテンツ鍵とを暗号処理部509へ出力し、コンテンツ鍵の暗号化を指示する。暗号処理部509は、制御部507の指示に従って、受け取った装置固有鍵516「Key__C」を用いて、コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、生成した暗号化コンテンツ鍵を、制御部507へ出力する(ステップS336)。

- [0199] 制御部507は、暗号処理部509から、暗号化コンテンツ鍵を受け取る。暗号化コンテンツ鍵を受け取ると、コンテンツ記憶部510上に新たなコンテンツファイルを生成し、生成したコンテンツファイルに、受信したコンテンツIDと暗号化コンテンツと暗号処理部509から受け取った暗号化コンテンツ鍵とを書き込む(ステップS337)。

次に、制御部507は、受信した暗号化コンテンツと受け取った暗号化コンテンツ鍵とを結合し、ハッシュ関数に代入してハッシュ値を算出する(ステップS339)。受信したコンテンツID、タイトル、録画日時、装置識別子「ID__A」及び算出したハッシュ値

を含むバックアップ情報を生成し、生成したバックアップ情報をバックアップ管理表521に追加する(ステップS341)。ここで、受信した装置識別子「ID__A」をバックアップ元装置識別子とする。

[0200] 制御部507は、セキュアクロックから現在時刻を取得し、取得した現在時刻に視聴時間「240時間」を加算して有効期限を算出し(ステップS342)、算出した有効期限を、送受信部501を介してHDレコーダ100へ送信する(ステップS343)。送信が完了すると、電源部503を介して、バックアップ装置500を構成する各回路への電力供給を停止する(ステップS344)。

[0201] HDレコーダ100の制御部107は、送受信部101を介して、バックアップ装置500から有効期限を受け取り、受け取った有効期限を選択したコンテンツ情報に書き込む(ステップS346)。

次に、制御部107は、選択したコンテンツ情報のバックアップフラグを「1」に変更し(ステップS347)、優先度を「2」に変更し(ステップS348)、ステップS301へ戻る。

[0202] (6)HDレコーダ100の有効期限延長動作

HDレコーダ100による有効期限の延長動作について、図21のフローチャートを用いて説明する。これは、図12のステップS112の詳細である。

セキュアクロック117の示す時刻が、予め、設定されている延長時刻「2:00」になると、制御部107を構成する主制御部118は、期限管理部119へ、有効期限延長指示を出力する。

[0203] 期限管理部119は、有効期限延長指示を受け取り、セキュア記憶部113に記憶されているコンテンツ管理表121を構成するコンテンツ情報を1つずつ、順番に選択する(ステップS361)。このとき、全てのコンテンツ情報を選択し終えており、新たに選択すべきコンテンツ情報が存在しない場合(ステップS362のYES)、有効期限延長の処理を終了する。

[0204] 全てのコンテンツ情報を選択し終えていない場合(ステップS362のNO)、期限管理部119は、選択したコンテンツ情報から有効期限を読み出す(ステップS363)。ここで、選択したコンテンツ情報に有効期限が書き込まれていない場合(ステップS366のNO)、ステップS361に戻り、次のコンテンツ情報を選択する。

選択したコンテンツ情報に、有効期限が書き込まれていれば(ステップS366のYES)、期限管理部119は、次に、セキュアクロック117から現在時刻を取得し(ステップS367)、読み出した有効期限と取得した現在時刻との差を算出して残り時間を算出する(ステップS368)。期限管理部119は、算出した残り時間と延長実行時間「24時間」とを比較し、残り時間が24時間以上であると判断すると(ステップS371のNO)、ステップS361へ戻り、次のコンテンツ情報の処理に移る。

- [0205] 算出した残り時間が、24時間未満であると判断すると(ステップS371のYES)、期限管理部119は、送受信部101を介してバックアップ装置500へ、起動指示を送信する(ステップS372)。

バックアップ装置500の制御部507は、送受信部501を介して起動指示を受け取り、電源部503へ電力供給開始を指示する。電源部503は、バックアップ装置500を構成する各部への電力供給を開始する(ステップS373)。

- [0206] 次に、制御部507は、送受信部501を介して、HDレコーダ100へ起動通知を送信する(ステップS374)。

HDレコーダ100の期限管理部119は、送受信部101を介して、所定時間以内にバックアップ装置500から、起動通知を受信しなければ(ステップS376のNO)、ステップS361へ戻る。

- [0207] 所定時間以内に起動通知を受信すると(ステップS376のYES)、期限管理部119は、認証部102へバックアップ装置500との機器認証を指示する。認証部102は、制御部107を構成する期限管理部119の指示により、バックアップ装置500との間で機器認証を行う(ステップS381)。

認証部102による機器認証が失敗であれば(ステップS382のNO)、期限管理部119は、ステップS361へ戻る。

- [0208] 機器認証が成功であれば(ステップS382のYES)、期限管理部119は、固有情報記憶部108から装置識別子115「ID_A」を読み出し、選択したコンテンツ情報からコンテンツIDを読み出す(ステップS383)。

次に、期限管理部119は、送受信部101を介して、延長要求と読み出した装置識別子115「ID_A」とコンテンツIDとを、バックアップ装置500へ送信する(ステップS

386)。

- [0209] HDレコーダ100との機器認証が失敗すると(ステップS389のNO)、バックアップ装置500の制御部507は、電源部503へ電力供給の停止を指示し、電源部503は、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS391)。

HDレコーダ100との機器認証が成功であると(ステップS389のYES)、制御部507は、送受信部501を介して、延長要求と装置識別子「ID_A」とコンテンツIDとを受信する。

- [0210] 次に、制御部507は、受信した装置識別子「ID_A」が、セキュア情報記憶部511に記憶されている許可装置識別情報551に含まれているか否かを判断する(ステップS392)。含まれていないと判断すると(ステップS392のNO)、制御部507は、送受信部501を介してHDレコーダ100へ、エラー通知を送信し(ステップS393)、電源部503へ電力供給の停止を指示する。電源部503は、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS394)。ここで、エラー通知を受信した場合、HDレコーダ100の期限管理部119は、ステップS361へ処理を移す。

- [0211] ステップS392において、受信した装置識別子「ID_A」が、許可装置識別情報551に含まれていると判断すると(ステップS392のYES)、制御部507は、セキュア情報記憶部511に記憶されているバックアップ管理表521から、受信したコンテンツIDを含むバックアップ情報を選択する(ステップS396)。

次に、制御部507は、受信したコンテンツIDを基に、選択したコンテンツ情報と対応するコンテンツファイルを検出し、検出したコンテンツファイルから暗号化コンテンツと暗号化コンテンツ鍵とを読み出し(ステップS397)、読み出した暗号化コンテンツと暗号化コンテンツ鍵とを結合し、ハッシュ関数に代入してハッシュ値を算出する(ステップS398)。

- [0212] 次に、制御部507は、選択したバックアップ情報に含まれるハッシュ値を読み出し(ステップS401)、読み出したハッシュ値と算出したハッシュ値とを比較する(ステップS402)。両者が一致しない場合(ステップS402のNO)、制御部507は、送受信部501を介してHDレコーダ100へ、エラー通知を送信し(ステップS403)、電源部503へ

電力供給の停止を指示する。電源部503は、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS404)。ここで、エラー通知を受信した場合、HDレコーダ100の期限管理部119は、ステップS361へ処理を移す。

- [0213] 読み出したハッシュ値と算出したハッシュ値とが一致する場合(ステップS402のYES)、制御部507は、セキュアクロックから現在時刻を取得し、取得した現在時刻に視聴時間「240時間」を加算して有効期限を算出する(ステップS406)。

次に、制御部507は、算出した有効期限を、送受信部501を介してHDレコーダ100へ送信する(ステップS407)。有効期限を送信すると、制御部507は、電源部503へ電力供給の停止を指示する。電源部503は、送受信部501及び制御部507以外の各部への電力供給を停止する(ステップS408)。

- [0214] 期限管理部119は、送受信部101を介して、バックアップ装置500から有効期限を受信する。受信した有効期限により、選択したコンテンツ情報に含まれる有効期限を更新し(ステップS411)、ステップS361へ処理を移す。

(7)機器認証

HDレコーダ100とバックアップ装置500との間の機器認証の動作について図24～図25を用いて説明する。

- [0215] なお、この機器認証の方法は一例であり、他の認証方法、鍵共有方法を用いてもよい。ここで、 $\text{Gen}()$ を鍵生成関数とし、 Y をシステム固有のパラメータとする。鍵生成関数 $\text{Gen}()$ は、 $\text{Gen}(x, \text{Gen}(z, Y)) = \text{Gen}(z, \text{Gen}(x, Y))$ の関係を満たすものとする。鍵生成関数は任意の公知技術で実施可能なため、詳細についてここでは説明しない。

- [0216] HDレコーダ100の認証部102は、公開鍵証明書 Cert_A を読み出し(ステップS501)、送受信部101を介して、読み出した公開鍵証明書 Cert_A をバックアップ装置500へ送信する(ステップS502)。

公開鍵証明書 Cert_A を受信したバックアップ装置500の認証部502は、認証局の公開鍵 PK_CA を用いて、公開鍵証明書 Cert_A に含んで受信した認証局の署名データ Sig_CA に署名検証アルゴリズム V を施して署名検証する(ステップS503)。ここで、署名検証アルゴリズム V は、署名生成アルゴリズム S により生成された署名

データを検証するアルゴリズムである。署名検証の結果が失敗であれば(ステップS504のNO)、処理を終了する。

- [0217] 署名検証の結果が成功であれば(ステップS504のYES)、認証部502は、CRLを読み出し(ステップS505)、公開鍵証明書Cert__Aに含んで受信した証明書識別番号ID__aが読み出したCRLに登録されているか否かを判断する(ステップS506)。

登録されていると判断すると(ステップS506のYES)、処理を終了する。

登録されていないと判断すると(ステップS506のNO)、認証部502は、公開鍵証明書Cert__Cを読み出し(ステップS507)、読み出した公開鍵証明書Cert__CをHDレコーダ100に送信する(ステップS508)。

- [0218] 公開鍵証明書Cert__Cを受信したHDレコーダ100の認証部102は、認証局の公開鍵PK__CAを用いて、公開鍵証明書Cert__Cに含んで受信した認証局の署名データSig__CAに署名検証アルゴリズムVを施して署名検証する(ステップS509)。署名検証の結果が失敗であれば(ステップS510のNO)処理を終了する。

署名検証の結果が成功であれば(ステップS510のYES)、認証部102は、CRLを読み出し(ステップS511)、公開鍵証明書Cert__Cに含んで受信した証明書識別番号ID__bが読み出したCRLに登録されているか否かを判断する(ステップS512)。

登録されていると判断すると(ステップS512のYES)、処理を終了する。登録されていないと判断すると(ステップS512のNO)、処理を継続する。

- [0219] バックアップ装置500の認証部502は、乱数Cha__Cを生成し(ステップS513)、生成した乱数Cha__CをHDレコーダ100に送信する(ステップS514)。

HDレコーダ100の認証部102は、乱数Cha__Cを受信し、HDレコーダ100の秘密鍵SK__Aを用いて、受信した乱数Cha__Cに署名生成アルゴリズムSを施して署名データSig__Aを生成し(ステップS515)、生成した署名データSig__Aをバックアップ装置500へ送信する(ステップS516)。

- [0220] バックアップ装置500の認証部502は、署名データSig__Aを受信すると、公開鍵証明書Cert__Aに含んで受信したHDレコーダ100の公開鍵PK__Aを用いて、受信した署名データSig__Aに、署名検証アルゴリズムVを施して署名検証する(ステップS517)。署名検証の結果が失敗であると判断すると(ステップS518のNO)処理を

終了する。署名検証の結果が成功であると判断すると(ステップS518のYES)、処理を続ける。

[0221] HDレコーダ100の認証部102は、乱数Cha__Aを生成し(ステップS519)、生成した乱数Cha__Aをバックアップ装置500に送信する(ステップS520)。

バックアップ装置500は、乱数Cha__Aを受信し、バックアップ装置500の秘密鍵SK__Bを用いて、受信した乱数Cha__Aに署名生成アルゴリズムSを施して署名データSig__Cを生成し(ステップS521)、生成した署名データSig__CをHDレコーダ100へ送信する(ステップS522)。

[0222] HDレコーダ100は、署名データSig__Cを受信すると、公開鍵証明書Cert__Cに含んで受信したバックアップ装置500の公開鍵PK__Bを用いて、受信した署名データSig__Cに、署名検証アルゴリズムVを施して署名検証する(ステップS523)。署名検証の結果が失敗であると判断すると(ステップS524のNO)、処理を終了する。署名検証の結果が成功であると判断すると(ステップS524のYES)、認証部102は、次に、乱数「a」を生成し(ステップS525)、生成した乱数「a」を用いて $Key_a = Gen(a, Y)$ を生成し(ステップS526)、生成したKey__aをバックアップ装置500へ送信する(ステップS527)。

[0223] バックアップ装置500の認証部502は、Key__aを受信すると、乱数「c」を生成し(ステップS528)、生成した乱数「c」を用いて $Key_c = Gen(c, Y)$ を生成し(ステップS529)、生成したKey__cをHDレコーダ100へ送信する(ステップS530)。

また、生成した乱数「c」と受信したKey__aとを用いて、 $Key_ac = Gen(c, Key_A) = Gen(c, Gen(a, Y))$ を生成し、これをセッション鍵とする(ステップS531)。

[0224] HDレコーダ100は、Key__cを受信し、生成した乱数「a」と受信したKey__cとから $Key_ac = Gen(a, Key_c) = Gen(a, Gen(c, Y))$ を生成し、これをセッション鍵とする(ステップS532)。

1.5 まとめ・効果

以上、説明してきたように、本発明のバックアップシステム1において、HDレコーダ100は、情報記憶部110に記憶している暗号化コンテンツをバックアップ装置500へ送信してバックアップを要求し、バックアップ装置500は、受信した暗号化コンテンツ

をバックアップする。このとき、暗号化コンテンツの送信元であるHDレコーダ100に記憶されている暗号化コンテンツには、有効期限を設定する。HDレコーダ100は、有効期限が切れる前に、バックアップ装置500に有効期限の延長を要求する。

[0225] バックアップ装置500と通信できなかったなどの理由で、有効期限の延長ができず、有効期限が切れると、HDレコーダ100は、情報記憶部110から有効期限の切れた暗号化コンテンツを削除する。

また、いったん削除された後で、利用者の操作などにより、バックアップ装置500に記憶されている暗号化コンテンツを取得することができる。

[0226] バックアップ装置500は、予め、許可装置識別情報を記憶しており、許可識別情報に登録されている装置識別子を有する装置からのバックアップの要求、延長要の要求及びリストアの要求を受け付ける。

このようにして、バックアップ装置500が暗号化コンテンツをバックアップした後も、有効期限が切れるまでは、HDレコーダ100が、当該暗号化コンテンツを記憶しているため、利用者は、簡単な操作でコンテンツを視聴することが可能である。

[0227] また、有効期限が切れるとHDレコーダ100は、記憶している暗号化コンテンツを削除することで、前記暗号化コンテンツのコピーが無期限に存在することを防止し、コンテンツの著作権者の権利を保護することができる。

本発明のバックアップシステム1においては、バックアップ装置500は、HDレコーダ400からバックアップを要求されたコンテンツも記憶している。HDレコーダ100は、HDレコーダ400の指示によりバックアップされたコンテンツを取得し再生することもできるため、利用者にとっての利便性をより向上させることができる。

[0228] また、バックアップ装置500は、HDレコーダ100からの起動指示を受け、各種の処理を行う間のみ、バックアップ装置500を構成する各部への電力供給を行う。従って、コンテンツ記憶部510を構成するハードディスクユニットの動作時間を最小限に抑制し、ハードディスクユニットの故障の危険性を抑制することができる。

2. 変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれ

る。

- [0229] (1)実施の形態1において、期限管理部119は、有効期限が過ぎた暗号化コンテンツを含むコンテンツファイルを、情報記憶部110から削除しているが、暗号化コンテンツ鍵のみを削除するとしてもよい。

この場合、期限管理部119は、情報記憶部110から暗号化コンテンツ鍵のみを削除し、対応するコンテンツ情報に含まれるハッシュ値と有効期限とを削除する。

- [0230] 再生リスト画面211をモニタに表示した状態で、利用者のボタン操作により、選択されたコンテンツボタンと対応するコンテンツ情報にハッシュ値が存在しない場合、主制御部118は、コンテンツ情報に含まれるコンテンツIDを読み出し、送受信部101を介して、バックアップ装置500へコンテンツ鍵要求と読み出したコンテンツIDとを送信する。

- [0231] バックアップ装置500は、コンテンツ鍵要求を受信し、HDレコーダ100へ該当するコンテンツ鍵と有効期限とを送信する。

HDレコーダ100の主制御部118は、コンテンツ鍵と有効期限とを受信し、暗号処理部109へ指示して、暗号化コンテンツ鍵を生成し、生成した暗号化コンテンツ鍵を情報記憶部110に書き込む。次に、選択されたコンテンツボタンと対応するコンテンツ情報と対応するコンテンツファイルに含まれる暗号化コンテンツを情報記憶部110から、読み出し、読み出した暗号化コンテンツと生成された暗号化コンテンツ鍵とを基にハッシュ値を生成し、生成したハッシュ値と受信した有効期限とをコンテンツ情報に書き込む。以下、上記の生成処理の制御と同様にして、暗号化コンテンツを復号し、再生する。

(2)上記の変形例(1)において、有効期限を更新できなかったコンテンツ情報のハッシュ値及び有効期限のみを削除するとしても良い。

- [0232] この場合、主制御部118は、コンテンツ鍵の要求に代わって、有効期限の要求をバックアップ装置500へ送信する。バックアップ装置500から、有効期限を受信できた場合にのみ、受信した有効期限をコンテンツ情報に書き込み、コンテンツ情報と対応する暗号化コンテンツ及び暗号化コンテンツ鍵から改めてハッシュ値を算出する。

(3)上記の実施の形態1では、バックアップ装置500が有効期限を算出し、算出した

有効期限をHDレコーダ100へ送信しているが、HDレコーダ100において、有効期限を算出するとしても良い。

- [0233] 例えば、バックアップ処理において、バックアップ装置500は、有効期限を送信する代わりに、正常にバックアップが終了したことを示す完了通知をHDレコーダ100へ送信する。

HDレコーダ100の主制御部118は、完了通知を受信すると、セキュアクロック117から現在時刻を取得し、取得した現在時刻に視聴時間「240時間」を加算して有効期限を算出する。

- [0234] また、有効期限の延長処理においてもバックアップ装置500は、有効期限に代わって、有効期限の延長が可能であることを示す延長許可をHDレコーダ100に送信する。

HDレコーダ100の、期限管理部119は、延長許可を受信すると、セキュアクロック117から現在時刻を取得し、取得した現在時刻に視聴時間「240時間」を加算して有効期限を算出する。

- [0235] また、現在時刻に代わって、各コンテンツ情報に含まれる有効期限に視聴時間「240時間」を加算し、加算結果を新たな有効期限としてもよい。

このような構成の場合、バックアップ装置500を構成する制御部507は、セキュアクロックを有する必要がなくなる。

(4) 上記の実施の形態では、HDレコーダ100は、各コンテンツ情報に含まれる有効期限を基に、有効期限の延長及び、有効期限切れのコンテンツの削除を行っているが、暗号化コンテンツの再生を許可される期間の開始日時及び許可される期間により、各コンテンツを管理しても良い。

- [0236] この場合、コンテンツ管理表121を構成する各コンテンツ情報は、有効期限に代わって、コンテンツの再生を許可される期間の開始日時を含む。

主制御部118は、コンテンツの再生が許可される期間「240時間」を記憶している。

バックアップ処理において、バックアップ装置500は、有効期限に代わって、正常にコンテンツをバックアップしたことを示すバックアップ完了通知を送信する。

- [0237] 主制御部118は、送受信部101を介してバックアップ装置500からバックアップ完

了通知を受け取り、セキュアクロック117から現在時刻を取得し、取得した現在時刻を開始日時として、コンテンツ情報に書き込む。

有効期限の延長処理において、期限管理部119は、セキュアクロック117から現在時刻を取得し、開始日時からの経過時間が216時間以上であれば、バックアップ装置500に、延長要求を送信する。

[0238] 削除処理において、期限管理部119は、セキュアクロック117から現在時刻を取得し、開始日時からの経過時間が240時間以上であれば、該当するコンテンツファイルを情報記憶部110から削除し、コンテンツ情報を削除する。

このような構成の場合、バックアップ装置500を構成する制御部507は、セキュアクロックを有する必要がなくなる。

(5) 上記の実施の形態1及び変形例では、HDレコーダ100は、各暗号化コンテンツの有効期限が失効するまでの時間が24時間未満になると、バックアップ装置500へ延長要求を送信しているが、有効期限が失効するまでの時間にかかわらず、定期的に延長要求を送信するとしても良い。

(6) また、有効期限に代わって、視聴回数によって、コンテンツを管理しても良い。

[0239] 例えば、コンテンツ管理表121の各コンテンツ情報には、有効期限に代わって、有効視聴回数が含まれる。コンテンツを再生するたびに、制御部107は、再生されたコンテンツと対応するコンテンツ情報に含まれる有効視聴数から1減算する。

バックアップ処理及び有効期限延長処理において、バックアップ装置500は、有効期限に代わって、視聴回数「3」を送信する。HDレコーダ100の制御部107は、受信した視聴回数「3」を、有効視聴回数とする。

[0240] また、HDレコーダ100は、有効視聴回数「0」のコンテンツ情報とこのコンテンツ情報に対応するコンテンツファイルとを削除する。

(7) 実施の形態1では、バックアップ装置500は、予め、許可装置識別情報551を記憶しており、許可装置識別情報551登録されている装置識別子を有する機器からのリストア要求を受け付けるとしているが、コピーコンテンツの数に応じてリストア要求を受け付けるか否かを判断してもよい。

[0241] 説明の便宜上、ここでは、バックアップ装置500の記憶している暗号化コンテンツを

単に「コンテンツ」と呼び、HDレコーダ100を初めとする再生機器に記憶されている暗号化コンテンツをコピーコンテンツと呼ぶ。また、バックアップシステム1には、HDレコーダ100及び400以外にも、コンテンツの記憶及び再生機能を備えた機器が接続されている。

[0242] 具体的には、バックアップ装置500の制御部507は、各コンテンツ、それぞれに存在の許されるコピーコンテンツの数である、許容コピー数「3」を記憶している。また、セキュア情報記憶部511に記憶されているバックアップ管理表521を構成する各バックアップ情報には、現在存在するコピーコンテンツの数を示すコピー数が含まれる。

セキュア情報記憶部511は、さらに、複数のコピー管理表を記憶している。各コピー管理表は、複数のコピー情報から構成され各コピー情報は、コンテンツID、装置識別子、有効期限からなる。コンテンツIDは、バックアップ管理表521に含まれるコンテンツIDのいずれかと同一である。装置識別子は、コンテンツIDの示すコピーコンテンツを有する外部機器を識別する情報である。有効期限は、装置識別子の示す外部機器の有するコピーコンテンツの有効期限である。

[0243] (7-a)バックアップ処理

実施の形態1において説明したバックアップ処理では、制御部507は、HDレコーダ100から、バックアップ要求を受信すると、実施の形態1において説明したように、コンテンツの書き込み、バックアップ情報の追加、有効期限の算出などを行う。このとき、追加したバックアップ情報のコピー数には「1」を書き込む。

[0244] 次に、制御部507は、受信したコンテンツIDと受信した装置識別子と算出した有効期限とからなるコピー情報を生成し、生成したコピー情報をコピー管理表に追加する。コピー情報を追加した後、算出した有効期限を、HDレコーダ100へ送信する。

(7-b)コピー削除

HDレコーダ100の主制御部118による録画処理の制御において、既に述べたように、主制御部118は、新たなコンテンツを録画する際に、情報記憶部110の空き容量が不足すると、優先度「2」を含むコンテンツ情報と対応する暗号化コンテンツを情報記憶部110から削除する。

[0245] このとき、主制御部118は、コピーコンテンツの削除を示すコピー削除通知と削除

するコピーコンテンツと対応するコンテンツIDとHDレコーダ100自身の装置識別子「ID__A」をバックアップ装置500へ送信する。

バックアップ装置500の制御部507は、HDレコーダ100からコピー削除通知とコンテンツIDと装置識別子「ID__A」とを受信する。コピー削除通知を受信すると、受信したコンテンツIDと装置識別子「ID__A」とを含むコピー情報を削除し、受信したコンテンツIDを含むバックアップ情報のコピー数から1を減じる。

[0246] (7-c) リストア処理

バックアップ装置500の制御部507は、上記に説明したリストア処理において、外部機器からリストア要求を受信すると、リストア要求と共に受信したコンテンツIDを含むバックアップ情報からコピー数を読み出す。読み出したコピー数が、許容コピー数「3」であれば、リストア要求を受け付けられないことを示すエラー通知をHDレコーダ100へ送信する。

[0247] 読み出したコピー数が、許容コピー数「3」未満であれば、制御部507は、実施の形態1において説明した手順で、ハッシュ値の検証、コンテンツ鍵の生成、有効期限の算出などを行う。有効期限を算出した後、バックアップ管理表521中の受信したコンテンツIDを含むバックアップ情報に含まれるコピー数に1加算する。次に、制御部507は、受信したコンテンツIDと装置識別子と算出した有効期限とからなるコピー情報を生成し、生成したコピー情報をコピー管理表に追加する。

[0248] 次に、コンテンツとコンテンツ鍵と有効期限とを外部機器に送信する。

(7-d) バックアップ装置500による有効期限の検証

有効期限の延長の処理において、制御部507は、受信したコンテンツIDと装置識別子とを含むコピー情報を選択し、選択したコピー情報の有効期限を、新たに算出した有効期限書き換える。

[0249] 制御部507は、各コピー情報に含まれる有効期限の検証を行う検証時刻を記憶している。検証時刻になると、制御部507は、コピー管理表を構成するコピー情報を1つ選択し、選択したコピー情報に含まれる有効期限を読み出し、読み出した有効期限と現在時刻を比較する。現在時刻が有効期限を過ぎている場合、選択したコピー情報に含まれるコンテンツIDを含むバックアップ情報のコピー数を1減じる。次に、制

御部507は、選択したコンテンツ情報を削除する。

- [0250] 現在時刻が有効期限を過ぎていなければ、コピー数の減算及びコピー情報の削除は行わない。

制御部507は、全てのバックアップ情報について、同様の手順で有効期限の検証を行う。

(8)変形例(7)では、許容コピー数をバックアップ装置500が予め記憶しているとしたが、放送されるコンテンツに許容コピー数が含まれていてもよい。

- [0251] 例えば、コンテンツを構成するTSパケットの所定のビットに許容コピー数が含まれており、バックアップ装置500は、バックアップ処理において、受信した暗号化コンテンツのいずれか一つのTSパケットを受信したコンテンツ鍵で復号して許容コピー数を抽出し、抽出したコピー数を受信したコンテンツIDと対応付けて記憶する。

また、許容コピー数に限らず、バックアップの生成を許可するか否かを示す情報もコンテンツに含まれていても良い。HDレコーダ100の制御部107は、受信したコンテンツから、バックアップの生成を許可するか否かを示す情報を抽出し、抽出した情報(バックアップ情報と呼ぶ)とコンテンツIDとを対応付けて記憶する。

- [0252] バックアップの処理の際に、バックアップの対象となる暗号化コンテンツと対応するバックアップ情報が、バックアップの生成の許可を示していれば、実施の形態1において、説明したような手順で暗号化コンテンツをバックアップ装置500へ送信する。バックアップの対象となる暗号化コンテンツと対応するバックアップ情報が、バックアップの禁止を示していれば、送信を中止する。

- [0253] 特に、利用者によるバックアップボタンの押下により、上述のバックアップ処理を開始した場合、バックアップの禁止を示すバックアップ情報と対応する暗号化コンテンツのコンテンツのタイトルをモニタ120に表示し、表示されているコンテンツのバックアップが禁じられていることを利用者に通知する。

このようにすることで、バックアップ及びコピーコンテンツの生成に関して、コンテンツの著作権者の意思を反映することができる。

(9)実施の形態1では、暗号化コンテンツと暗号化コンテンツ鍵とを結合してハッシュ関数に代入し、ハッシュ値を算出しているが、暗号化コンテンツ鍵のみを代入しても

良い。

(10) 上記の実施の形態及び変形例では、コンテンツ及びコンテンツ鍵の暗号化には、共通鍵暗号方式を採用し暗号化と復号化に同一の鍵を用いているが、これに限定されるものではない。例えば、RSA、楕円曲線暗号といった公開鍵暗号方式を採用し、暗号化と復号に異なる鍵を用いてもよい。

[0254] 具体的に、コンテンツの暗号化に公開鍵暗号方式を採用する場合、図13を用いて説明したコンテンツの録画処理において、HDレコーダ100の鍵生成部106は、1個のコンテンツ鍵に代わって、1対のコンテンツ暗号鍵とコンテンツ復号鍵とを生成する。制御部107は、放送受信部114を介して受信したコンテンツと、鍵生成部106により生成されたコンテンツ暗号鍵を暗号処理部109へ出力してコンテンツの暗号化を指示する。暗号処理部109は、コンテンツの暗号化を指示されると、コンテンツ暗号鍵を用いて、コンテンツに、公開鍵暗号方式に従う暗号化アルゴリズムを施して暗号化コンテンツを生成する。ストップボタンの押下又は情報記憶部110の空き容量不足により、録画を停止する時、暗号処理部109は、コンテンツ鍵に代わって、コンテンツ復号鍵を装置固有鍵「Key__A」を用いて暗号化し、暗号化コンテンツ鍵を生成する。

[0255] 以後、暗号処理部109は、コンテンツ復号鍵の暗号化及び暗号化コンテンツ鍵の復号には、共通鍵暗号方式を採用し、暗号化コンテンツの復号には、公開鍵暗号方式を採用して、暗号化及び復号の処理を行う。

(11) 上記の実施の形態及び変形例では、バックアップ装置500とHDレコーダ100とがLAN30により接続されている例について説明してきたが、この構成に限るものではない。他の例として、バックアップ装置がHDレコーダ100に内蔵されている場合も、本発明に含まれる。

(12) バックアップ装置500のコンテンツ記憶部510は、ハードディスクユニットから構成されるとして説明してきたが、着脱可能な光ディスクと、光ディスクへの情報の書き込み及び読み出しを行う入出力部を含んで構成されるとしても良い。この場合、利用者は、必要に応じて、光ディスクを着脱する。

[0256] また、複数の光ディスクと、これらを自動的に交換するディスクチェンジャを含んで

構成されるとしても良い。

(13) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0257] また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0258] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0259] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(14) 上記の各装置を構成する構成要素の一部又は全部は、1個のシステムLSI (Large Scale Integration: 大規模集積回路) から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。

[0260] なお、上記では、システムLSIとしたが、集積度の違いによって、IC (Integrated Circuit)、LSI、スーパーLSI、ウルトラLSIと呼ばれる集積回路であってもよい。

また、システムLSIに代わって、製品に組み込んだ後にプログラムすることが可能なFPGA(Field Programmable Gate Array)、CPLD(Complex Programmable Logic Device、リコンフィギュラブルLSIともいう)により構成されていてもよい。さらに、今後、上記の集積回路の機能を代替する新技術が開発された場合、その新技術によって、各装置を構成する構成要素の一部又は全部を実現してもよい。

(15) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0261] 本発明は、デジタルコンテンツを生成し、配布し、放送し、使用する産業及びコンテンツを生成する機器、配布する機器、再生、編集などを行う各種の電器機器を製造、販売する産業において、経営的、継続的、反復的に利用することができる。

請求の範囲

- [1] コンテンツの記録及び再生をする記録再生装置とバックアップ装置とからなるバックアップシステムであって、
- 前記記録再生装置は、
- 前記コンテンツを記憶している記憶手段と、
- 前記コンテンツのバックアップの指示を受け付ける受付手段と、
- 前記指示を受け付けると、前記コンテンツを前記記憶手段から読み出し、読み出した前記コンテンツをバックアップ装置へ送信するコンテンツ送信手段と、
- 前記指示を受け付けると、前記バックアップの対象である前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込む書込手段と、
- 前記期間情報により示される期間内は、前記コンテンツの再生を許可し、前記期間情報により示される期間が終了すると、前記コンテンツの再生を禁止する再生制御手段とを備え、
- 前記バックアップ装置は、
- 前記記録再生装置から、前記コンテンツを受信するコンテンツ受信手段と、
- 受信した前記コンテンツを記憶するバックアップ記憶手段と
- を備えることを特徴とするバックアップシステム。
- [2] コンテンツの記録及び再生を行う記録再生装置であって、
- 前記コンテンツを記憶している記憶手段と、
- 前記コンテンツのバックアップの指示を受け付ける受付手段と、
- 前記指示を受け付けると、前記コンテンツを前記記憶手段から読み出し、読み出した前記コンテンツのバックアップが許可されていれば、読み出した前記コンテンツをバックアップ装置へ送信するコンテンツ送信手段と、
- 前記指示を受け付けると、前記バックアップの対象である前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込む書込手段と、
- 前記期間情報により示される期間内は、前記コンテンツの再生を許可し、前記期間

情報により示される期間が終了すると、前記コンテンツの再生を禁止する再生制御手段と

を備えることを特徴とする記録再生装置。

[3] 前記記録再生装置は、さらに、

前記バックアップ装置へ、前記期間情報の示す期間の延長許可を求める延長要求を送信する延長要求手段と、

前記バックアップ装置から前記延長の許可を示す延長許可情報を受信し、前記期間情報の示す期間を延長する延長手段と

を備えることを特徴とする請求項2に記載の記録再生装置。

[4] 前記延長要求手段は、前記期間情報の示す期間の終了する時点よりも所定時間前に、前記延長要求を送信する

ことを特徴とする請求項3に記載の記録再生装置。

[5] 前記延長要求手段は、前記期間情報の示す期間内に、定期的に前記延長要求手段要求を繰返し送信する

ことを特徴とする請求項3に記載の記録再生装置。

[6] 前記延長手段は、前記記憶手段に記憶されている前記期間情報よりも後の期間を示す前記延長許可情報を受信し、前記期間情報の示す期間を受信した前記延長許可情報の示す期間に書き換えることにより、前記期間情報を延長する

ことを特徴とする請求項3に記載の記録再生装置。

[7] 前記延長手段は、予め、延長時間を記憶しており、前記延長時間を前記期限情報の示す期間に付加することにより、前記期間情報を延長する

ことを特徴とする請求項3に記載の記録再生装置。

[8] 前記期間情報は、前記記憶手段に記憶されている前記コンテンツの再生が許可される期間の終了する時点を示し、

前記再生制御手段は、現在時刻が前記期間情報の示す時点より前であれば、前記コンテンツの再生を許可し、現在時刻が前記期間情報の示す時点よりも後であれば、前記コンテンツの再生を禁止する

ことを特徴とする請求項3に記載の記録再生装置。

- [9] 前記期間情報は、前記記憶手段に記憶されている前記コンテンツの再生が許可される時間長を示す許可時間と、前記コンテンツの再生が許可される期間の開始時点を示す開始時刻であり、
- 前記再生制御手段は、前記開始時刻からの経過時間を取得し、取得した前記経過時間が前記許可時間以下であれば、前記コンテンツの再生を許可し、前記開始時間からの経過時間が前記許可時間を超えていれば、前記コンテンツの再生を禁止することを特徴とする請求項3に記載の記録再生装置。
- [10] 前記再生制御手段は、前記記憶手段から前記コンテンツを削除することによって、前記コンテンツの再生を禁止する
- ことを特徴とする請求項2に記載の記録再生装置。
- [11] 前記記録再生装置は、さらに、
- 前記バックアップ装置の記憶している前記コンテンツの取得を示すリストア指示を取得するリストア指示取得手段と、
- 前記リストア指示を取得すると、前記バックアップ装置へ、前記バックアップ装置の記憶している前記コンテンツの送信要求を送信するリストア要求手段と、
- 前記バックアップ装置から、前記コンテンツを受信し、受信した前記コンテンツを前記記憶手段に書き込むリストア手段とを備え、
- 前記コンテンツが書き込まれると、前記書込手段は、さらに、前記リストア手段により書き込まれた前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段に書き込む
- ことを特徴とする請求項10に記載の記録再生装置。
- [12] 前記記憶手段に記憶されている前記コンテンツは、
- 暗号鍵に基づいて、デジタル著作物を暗号化して生成された暗号化著作物と前記暗号化著作物の復号に用いられる復号鍵とを含んで構成され、
- 前記再生制御手段は、前記コンテンツに含まれる前記復号鍵を削除することによって、前記コンテンツの再生を禁止する
- ことを特徴とする請求項2に記載の記録再生装置。
- [13] 前記記録再生装置は、さらに、

前記バックアップ装置の記憶している前記暗号鍵の取得を示すリストア指示を取得するリストア指示取得手段と、

前記リストア指示を取得した場合に、前記バックアップ装置へ、前記バックアップ装置の記憶している前記復号鍵の送信要求を送信するリストア要求手段と、

前記バックアップ装置から、前記復号鍵を受信し、受信した前記復号鍵を前記記憶手段に書き込むリストア手段とを備え、

前記復号鍵が書き込まれると、前記書込手段は、さらに、前記記憶手段に記憶されている前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段に書き込む

ことを特徴とする請求項12に記載の記録再生装置。

[14] 前記記憶手段に記憶されている前記コンテンツは、

暗号鍵を用いてデジタル著作物を暗号化して生成された暗号化著作物と、

前記暗号化著作物の復号に用いられる復号鍵を当該記録再生装置に固有の固有鍵を用いて暗号化して生成された暗号化鍵とを含み、

前記再生制御手段は、前記記憶手段から前記暗号化鍵を削除することにより前記コンテンツの再生を禁止する

ことを特徴とする請求項2に記載の記録再生装置。

[15] 前記記憶手段に記憶されている前記コンテンツは、バックアップの許可又は禁止を示すバックアップ情報を含んでおり、

前記コンテンツ送信手段は、前記バックアップ情報がバックアップの許可を示しているか否かを判断し、許可を示していると判断すると、前記コンテンツを送信し、

前記書込手段は、前記バックアップ情報がバックアップの許可を示しているか否かを判断し、許可を示していると判断すると、前記期間情報を書き込む

ことを特徴とする請求項2に記載の記録再生装置。

[16] 前記コンテンツ送信手段は、通信鍵を用いて前記コンテンツを暗号化し、暗号化された前記コンテンツを、安全に送信する

ことを特徴とする請求項2に記載の記録再生装置。

[17] 前記記録再生装置は、さらに、

前記コンテンツに所定の演算を施して生成された検出情報を記憶している検出情報記憶手段と、

前記記憶手段から前記コンテンツを読み出し、読み出した前記コンテンツに前記所定の演算を施して検査情報を生成し、生成した検査情報と前記検出情報とを比較し、一致しないと判定された前記コンテンツの使用を禁止する不正禁止手段と

を備えることを特徴とする請求項2に記載の記録再生装置。

- [18] 前記バックアップ装置は、前記記録再生装置以外の機器によるバックアップの指示に応じて別のコンテンツを記憶しており、

前記記録再生装置は、さらに、

前記別のコンテンツの取得を示すリストア指示を取得するリストア指示取得手段と、

前記リストア指示を取得すると、前記別のコンテンツの送信要求を前記バックアップ装置へ送信するコンテンツ要求手段と、

前記バックアップ装置から、前記別のコンテンツを受信し、受信した前記別のコンテンツを前記記憶手段に書き込むリストア手段とを備え、

前記別のコンテンツを受信すると、前記書込手段は、さらに、前記別のコンテンツの再生が許可される期間を示す期間情報を、前記別のコンテンツと対応付けて、前記記憶手段へ書き込む

ことを特徴とする請求項2に記載の記録再生装置。

- [19] コンテンツをバックアップするバックアップ装置であって、

前記コンテンツを記憶している記憶手段と、

記録再生装置から、当該記録再生装置の記憶しているコンテンツの再生が許可される期間を示す期間情報の延長の許可を求める延長要求を受信する延長受付手段と、

前記延長を許可するか否かを判定する判定手段と、

許可すると判定する場合に前記延長の許可を示す延長許可情報を、前記記録再生装置へ出力する許可手段と

を備えることを特徴とするバックアップ装置。

- [20] 前記記憶手段は、さらに、前記コンテンツを示す識別情報を前記コンテンツと対応し

て記憶しており、

前記延長受付手段は、前記記録再生装置の記憶している前記コンテンツを示すコンテンツ識別情報を含む前記延長要求を受信し、

前記判定手段は、前記コンテンツ識別情報と、前記記憶手段の記憶している前記識別情報とを比較し、両者が一致すれば、許可すると判定する

ことを特徴とする請求項19に記載のバックアップ装置。

- [21] 前記延長要求は、当該延長要求を出力した前記記録再生装置を示す装置識別情報を含んでおり、

前記判定手段は、予め、特定の機器を示す1以上の許可装置識別情報を記憶しており、受信した前記延長要求に含まれる前記装置識別情報が、前記許可装置識別情報の何れかと一致すれば、許可すると判定する

ことを特徴とする請求項19に記載のバックアップ装置。

- [22] 前記記憶手段は、さらに、前記コンテンツに所定の演算を施して生成された検出情報を前記コンテンツと対応して記憶しており、

前記判定手段は、前記記憶手段から、前記コンテンツを読み出し、読み出した前記コンテンツに前記所定の演算を施して検証情報を生成し、生成した検証情報と前記検出情報とを比較し、一致すれば、前記延長を許可すると判定する

ことを特徴とする請求項19に記載のバックアップ装置。

- [23] 前記許可手段は、前記期間情報により示される期間よりも、後の期間を示す前記延長許可情報を出力する

ことを特徴とする請求項19に記載のバックアップ装置。

- [24] 前記バックアップ装置は、さらに、前記記憶手段の記憶している前記コンテンツの送信要求を受信するリストア受信手段と、

前記コンテンツを送信するか否かを判定するリストア判定手段と

送信すると判定されると、前記記憶手段から前記コンテンツを読み出し、読み出した前記コンテンツを送信するリストア送信手段と

を備えることを特徴とする請求項19に記載のバックアップ装置。

- [25] 前記送信要求は、当該送信要求の送信元であるリストア機器を示すリストア機器識別

情報を含んでおり、

前記リストア判定手段は、予め、特定の機器を示す1以上の許可装置識別情報を記憶しており、前記リストア機器識別情報が、前記許可装置識別情報の何れかと一致すれば、前記コンテンツを送信すると判定する

ことを特徴とする請求項24に記載のバックアップ装置。

- [26] 前記許可装置識別情報は、前記記憶手段の記憶している前記コンテンツのバックアップを指示したバックアップ元装置を示しており、

前記リストア判定手段は、前記リストア機器識別情報と前記許可装置識別情報とが一致すれば、前記コンテンツを送信すると判定する

ことを特徴とする請求項25に記載のバックアップ装置。

- [27] 前記リストア判定手段は、前記記憶手段に記憶されている前記コンテンツと同一で、前記バックアップ装置により再生を許可されたコンテンツを記憶している機器の総数を示すコピー数と、前記コピー数の上限を示すコピー許可数とを有し、

前記コピー数が前記コピー許可数未満であれば、前記コンテンツを送信すると判定する

ことを特徴とする請求項24に記載のバックアップ装置。

- [28] 前記バックアップ装置は、さらに、

前記記憶手段に記憶されている前記コンテンツと同一であり、前記バックアップ装置により再生を許可されたコンテンツを記憶している機器を示す機器識別情報と、前記機器において前記コンテンツの再生が許可される期間を示すコピー期間情報とを対応付けて記憶している期間情報記憶手段と、

前記コピー期間情報の示す期間が終了すると、前記コピー数から1減算するコピー数管理手段を備える

ことを特徴とする請求項27に記載のバックアップ装置。

- [29] 前記記憶手段の記憶している前記コンテンツは、予め、前記コピー許可数を含んでおり、前記判定手段は、前記コンテンツから前記コピー許可数を取得する

ことを特徴とする請求項27に記載のバックアップ装置。

- [30] 前記リストア送信手段は、通信鍵を用いて前記コンテンツを暗号化し、安全に、暗号

化コンテンツを送信する

ことを特徴とする請求項24に記載のバックアップ装置。

- [31] 前記記録再生装置は、前記延長要求に先立って、前記バックアップ装置へ、起動を指示する起動指示情報を出力し、

前記バックアップ装置は、さらに、前記起動指示を受信すると、当該バックアップ装置を構成する各回路へ電力供給を開始する電力制御手段を備える

ことを特徴とする請求項19に記載のバックアップ装置。

- [32] コンテンツの記録及び再生を行う記録再生装置において用いられるバックアップ方法であって、

前記記録再生装置は、前記コンテンツを記憶している記憶手段を備え、

前記バックアップ方法は、

前記コンテンツのバックアップの指示を受け付ける受付ステップと、

前記指示を受け付けると、前記コンテンツを前記記憶手段から読み出し、読み出した前記コンテンツのバックアップが許可されていれば、読み出した前記コンテンツをバックアップ装置へ送信するコンテンツ送信ステップと、

前記指示を受け付けると、前記バックアップの対象である前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込む書込ステップと、

前記期間情報により示される期間内は、前記コンテンツの再生を許可し、前記期間情報により示される期間が終了すると、前記コンテンツの再生を禁止する再生制御ステップと

を備えることを特徴とするバックアップ方法。

- [33] コンテンツの記録及び再生を行う記録再生装置に搭載される集積回路であって、

前記コンテンツを記憶している記憶手段と、

前記コンテンツのバックアップの指示を受け付ける受付手段と、

前記指示を受け付けると、前記コンテンツを前記記憶手段から読み出し、読み出した前記コンテンツのバックアップが許可されていれば、読み出した前記コンテンツをバックアップ装置へ送信するコンテンツ送信手段と、

前記指示を受け付けると、前記バックアップの対象である前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込む書込手段と、

前記期間情報により示される期間内は、前記コンテンツの再生を許可し、前記期間情報により示される期間が終了すると、前記コンテンツの再生を禁止する再生制御手段と

を備えることを特徴とする集積回路。

[34] コンテンツの記録及び再生を行う記録再生装置において、実行されるプログラムであって、

前記記録再生装置は、前記コンテンツを記憶している記憶手段を備え、

前記バックアッププログラムは、

前記コンテンツのバックアップの指示を受け付ける受付ステップと、

前記指示を受け付けると、前記コンテンツを前記記憶手段から読み出し、読み出した前記コンテンツのバックアップが許可されていれば、読み出した前記コンテンツをバックアップ装置へ送信するコンテンツ送信ステップと、

前記指示を受け付けると、前記バックアップの対象である前記コンテンツの再生が許可される期間を示す期間情報を、前記コンテンツと対応付けて前記記憶手段へ書き込む書込ステップと、

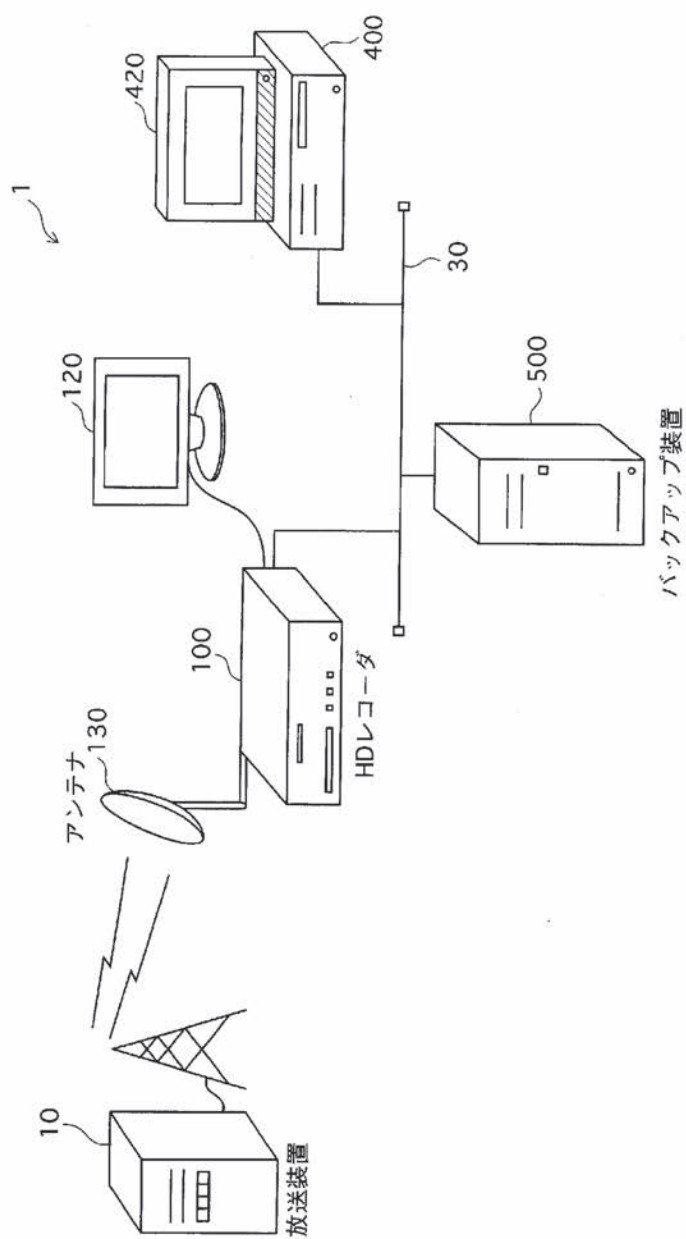
前記期間情報により示される期間内は、前記コンテンツの再生を許可し、前記期間情報により示される期間が終了すると、前記コンテンツの再生を禁止する再生制御ステップと

を備えることを特徴とするバックアッププログラム。

[35] 前記バックアッププログラムは、コンピュータにより読み取り可能な記録媒体に記録されていること

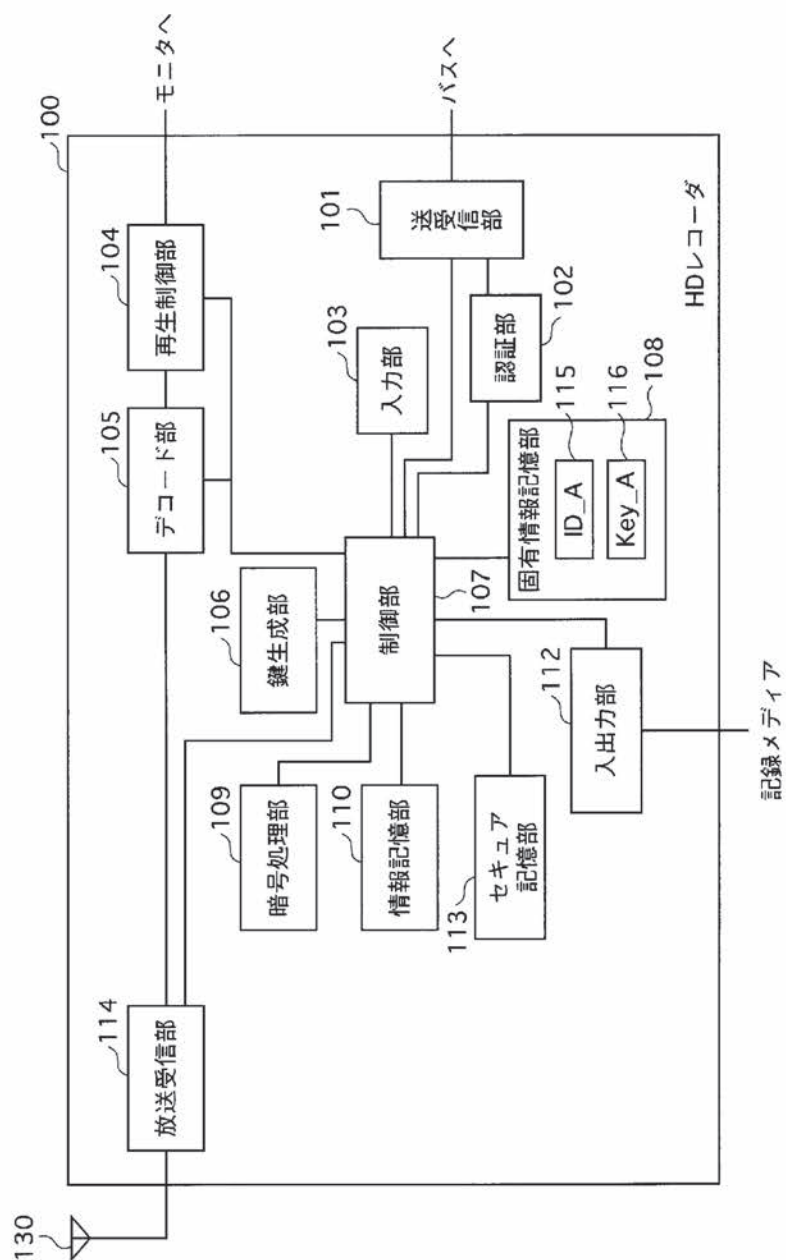
を特徴とする請求項34に記載のバックアッププログラム。

[図1]

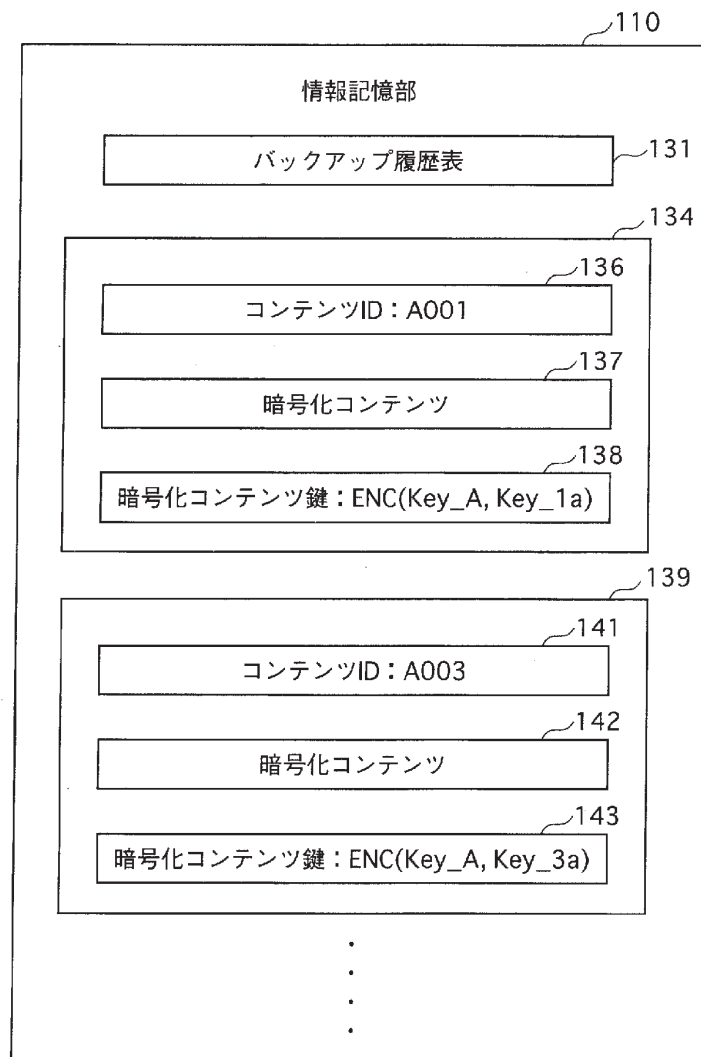


2/25

[図2]



[図3]



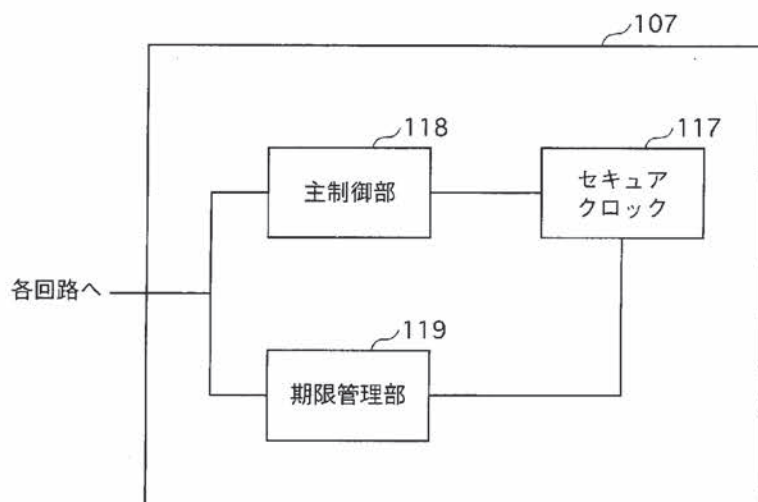
4/25

[図4]

121

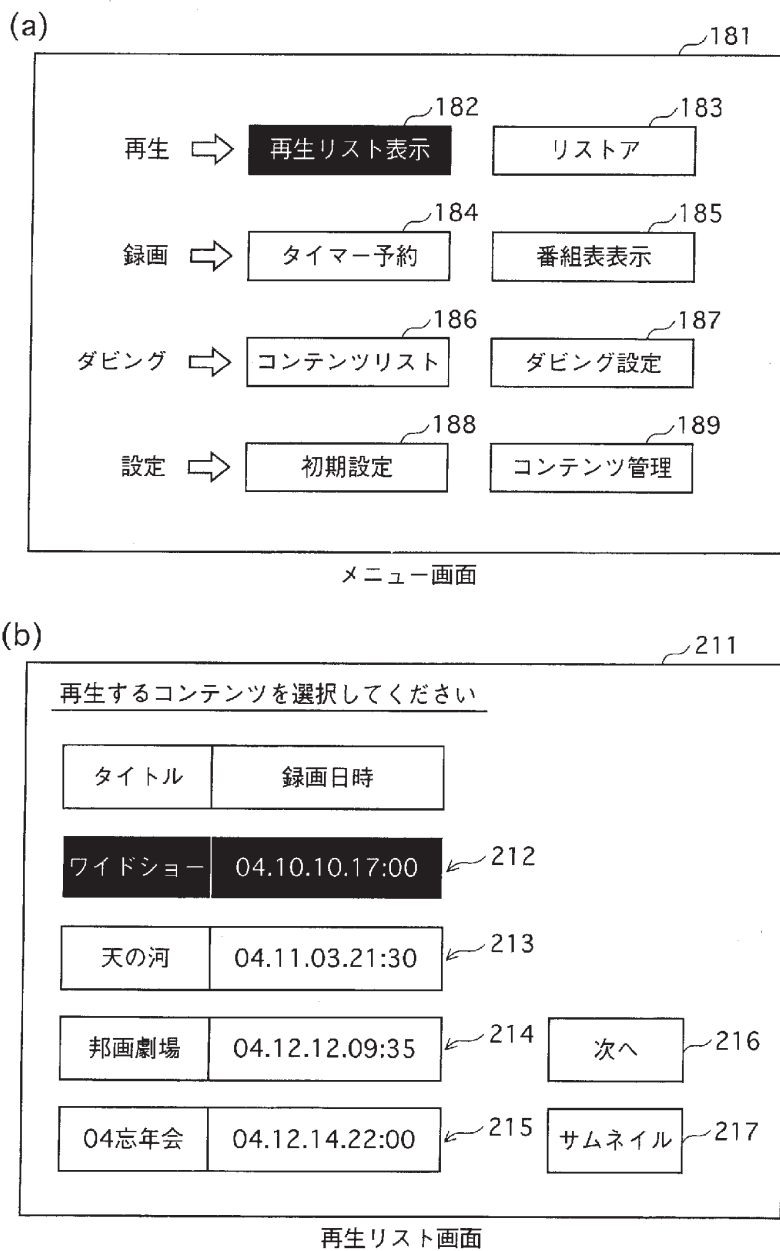
151	152	153	154	155	156	157	158	159
コンテンツID	タイトル	録画日時	ハッシュ値	種類	圧縮方式	有効期限	バックアップフラグ	優先度
A001	ワイドショー	04.10.10.17:00	01a	放送番組	MPEG2	04.12.15.17	1	2
A003	04忘年会	04.12.12.09:35	03a	写真	JPEG	04.12.14.21	1	1
A004	猫日記	04.12.14.22:00	04a	放送番組	MPEG2	—	0	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

[図5]



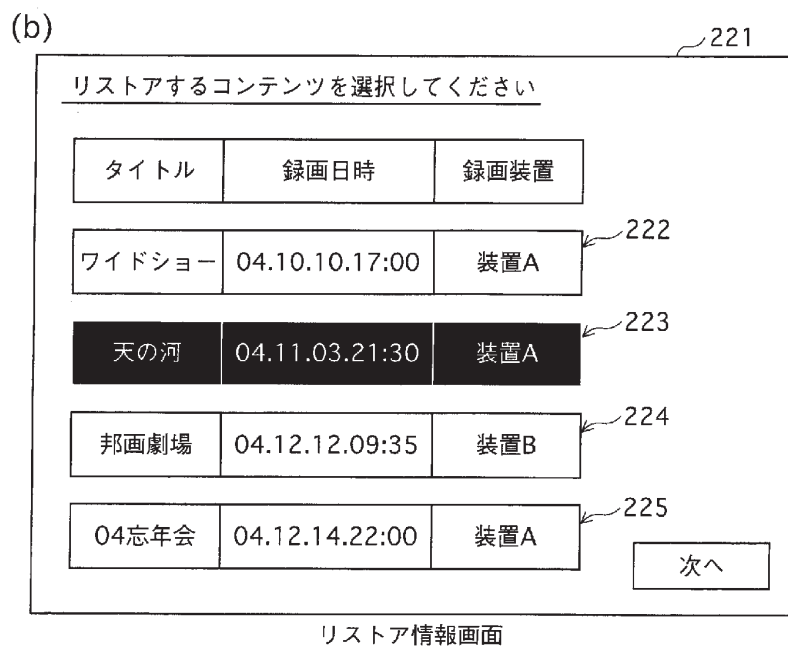
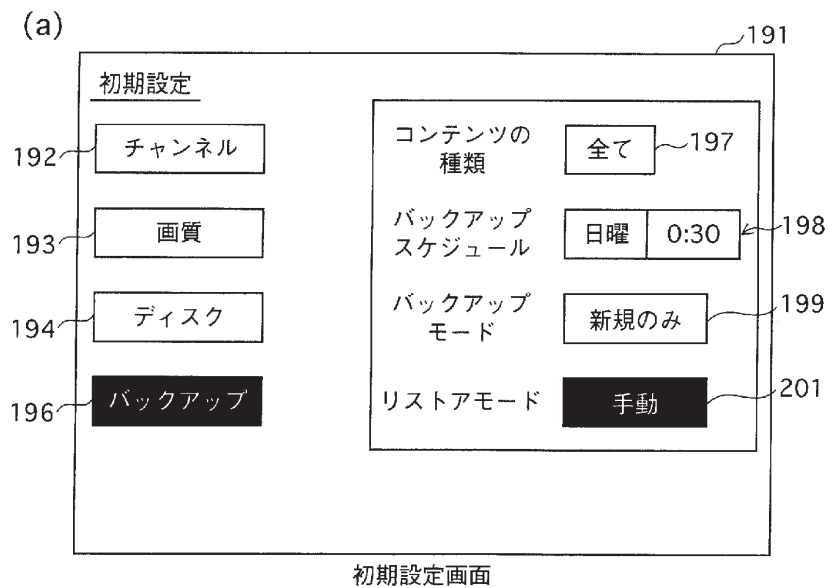
6/25

[[図6]



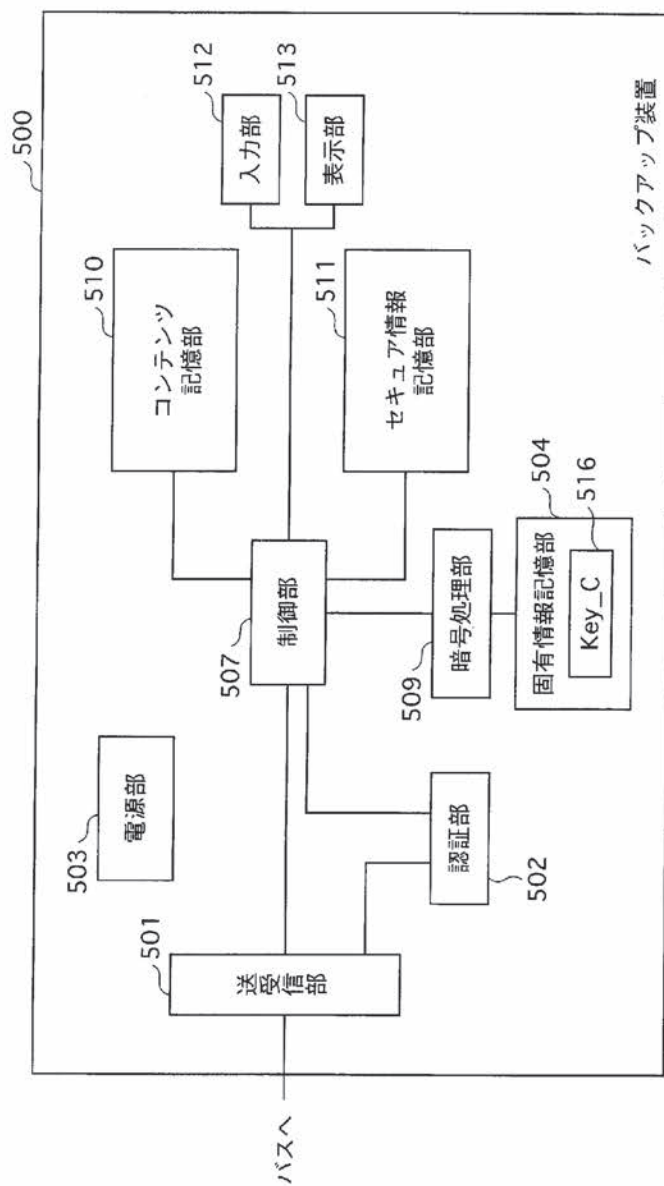
7/25

[図7]



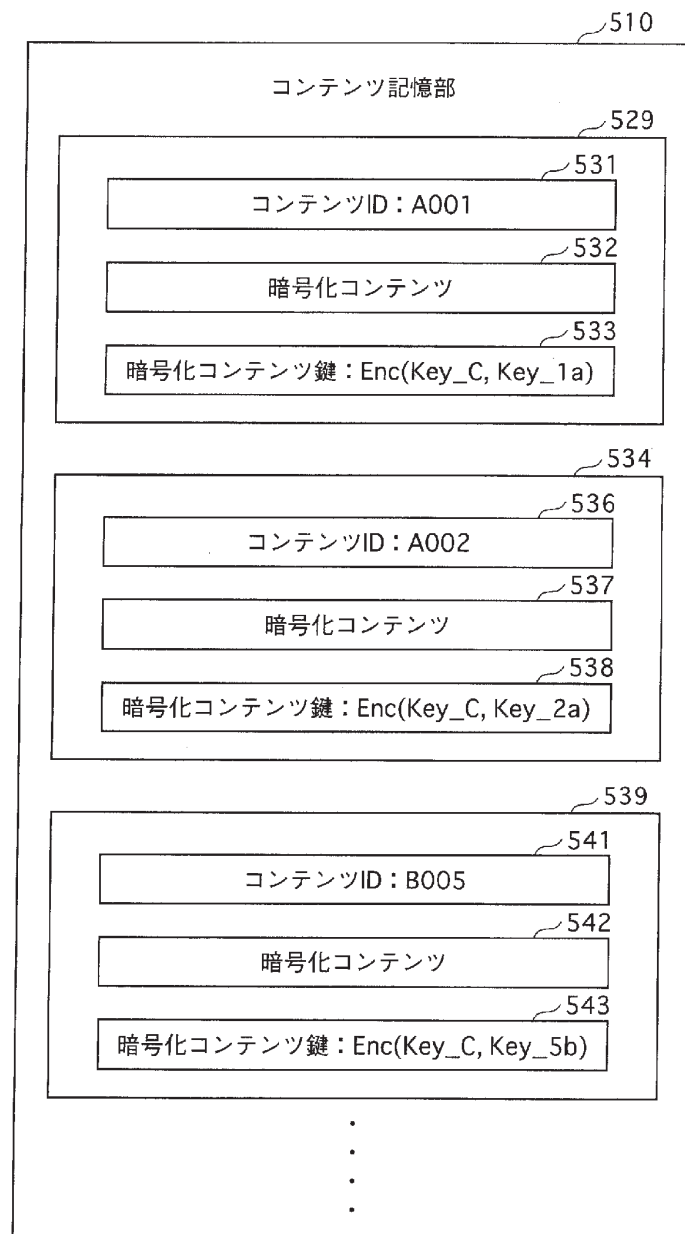
8/25

[図8]



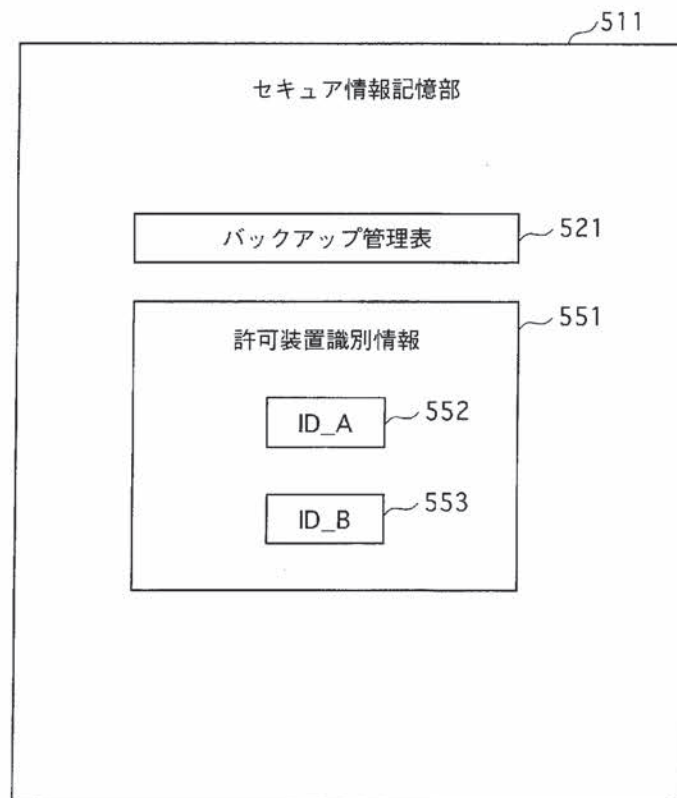
9/25

[図9]



10/25

[図10]



11/25

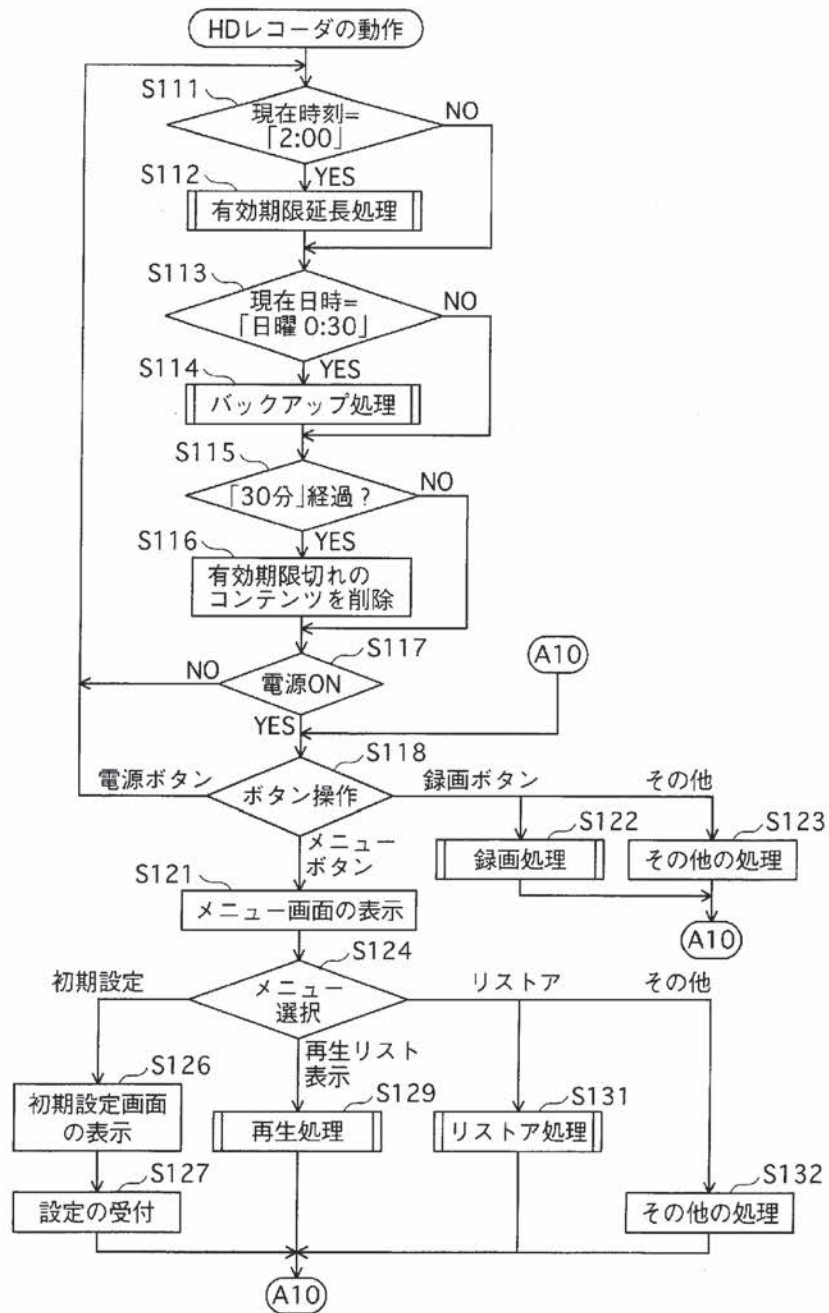
[図11]

521

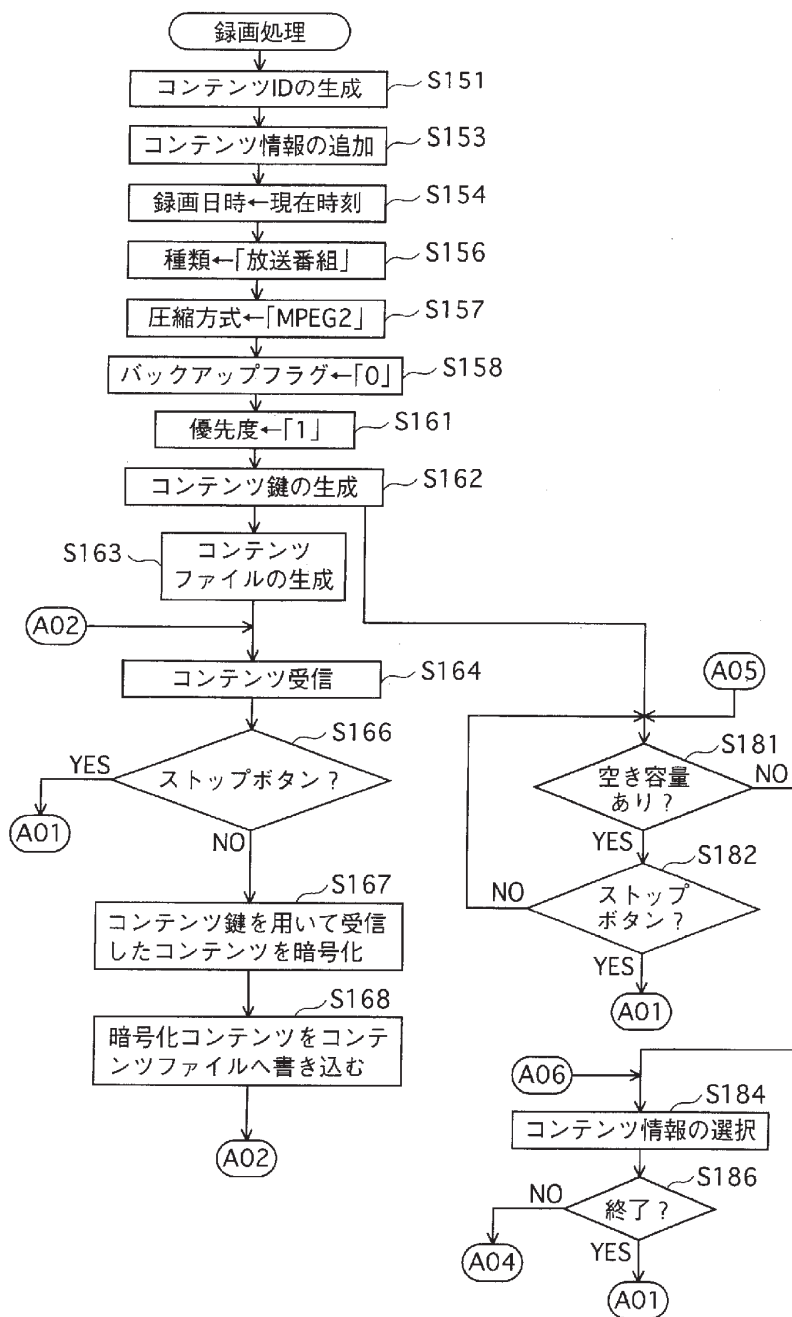
バックアップ情報				
561	562	563	564	565
コンテンツID	タイトル	録画日時	バックアップ 元装置識別子	ハッシュ値
522 A001	ワイドショー	04.10.10.17:00	ID_A	01c
523 A002	天の河	04.11.03.21:30	ID_A	02c
524 B005	邦画劇場	04.12.12.09:35	ID_B	05c
525 A003	04忘年会	04.12.14.22:00	ID_A	03c
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

12/25

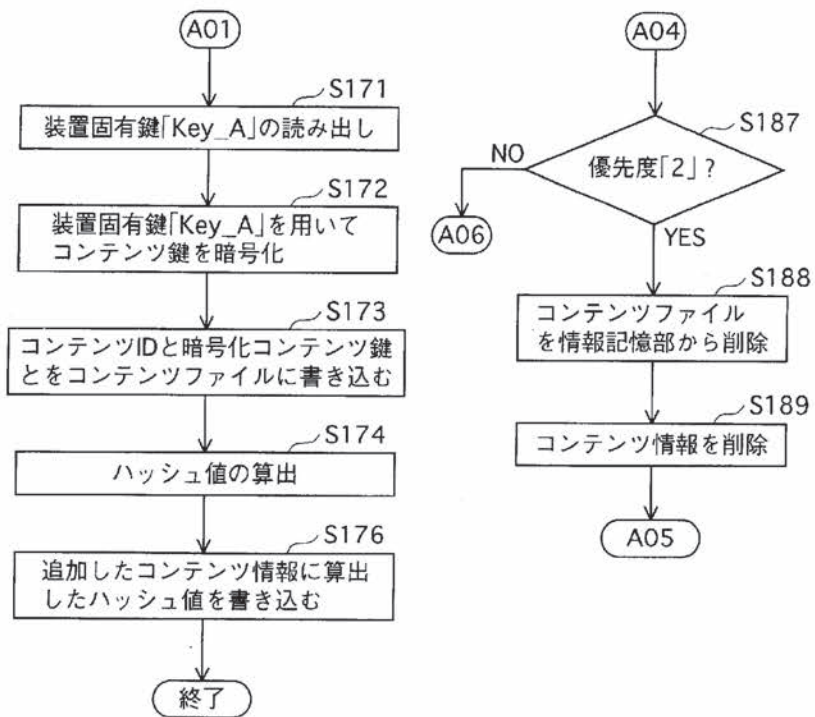
[図12]



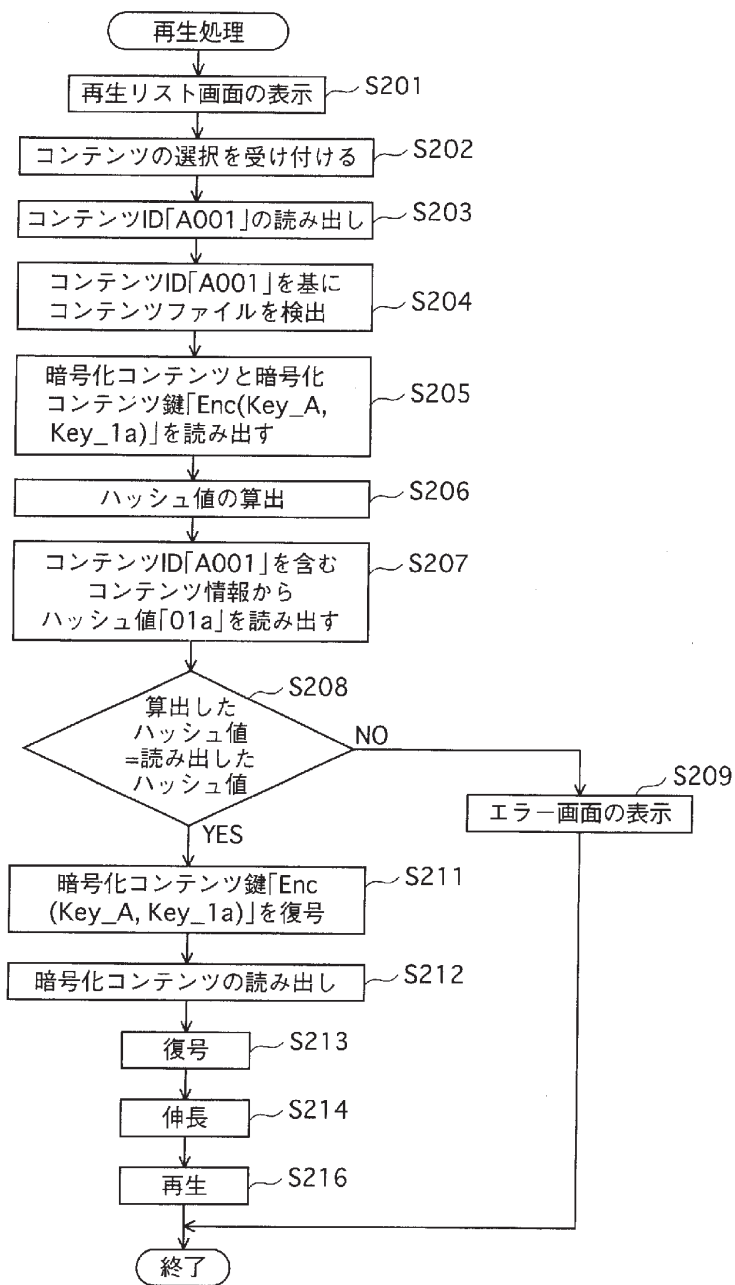
[図13]



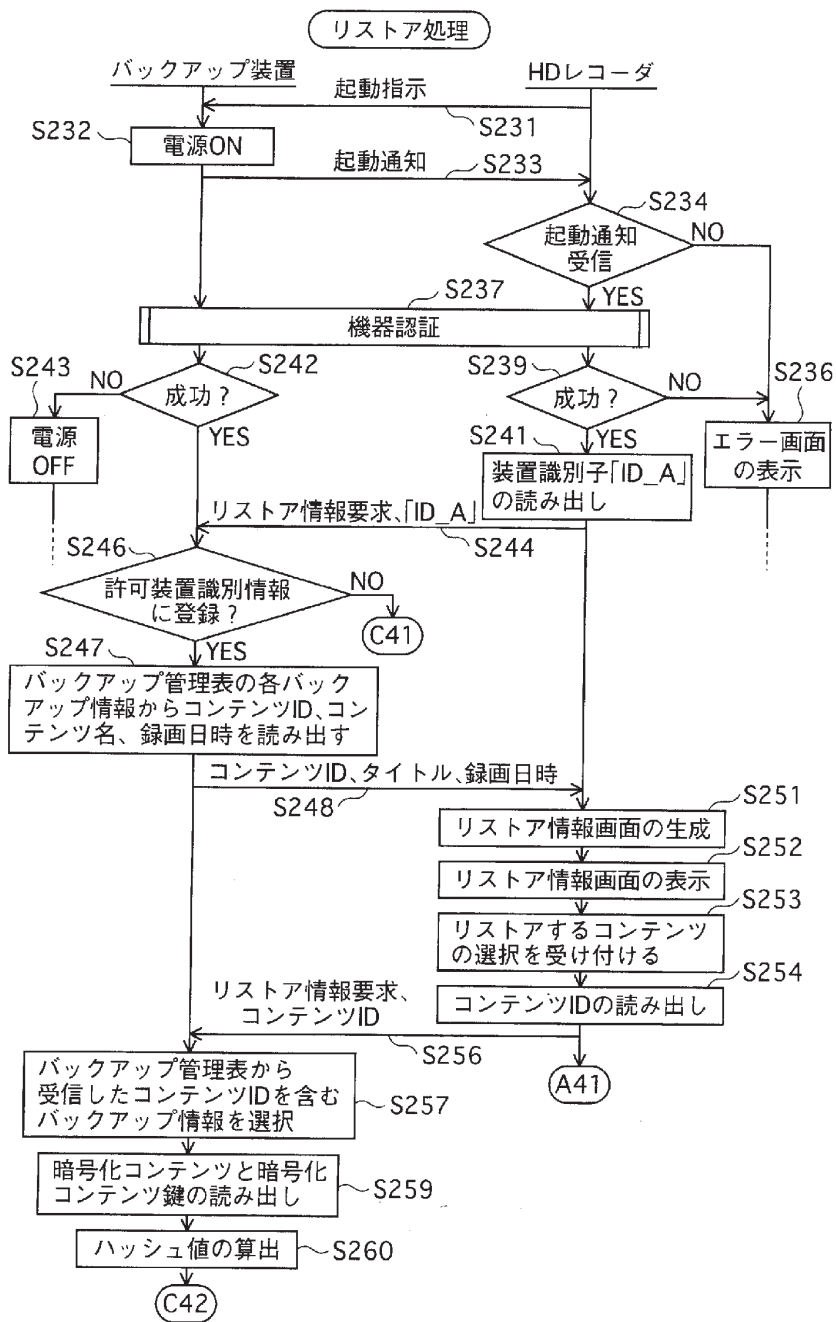
[図14]



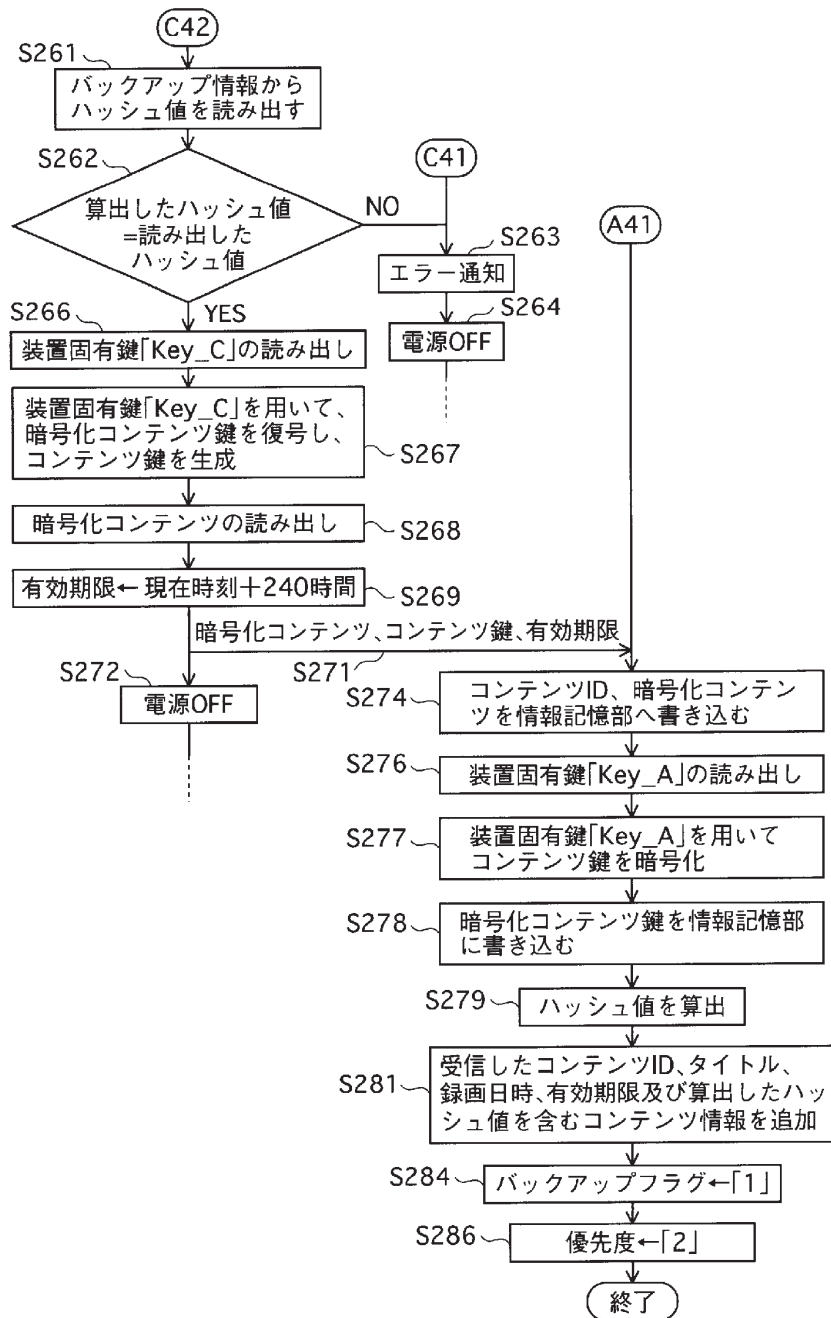
[図15]



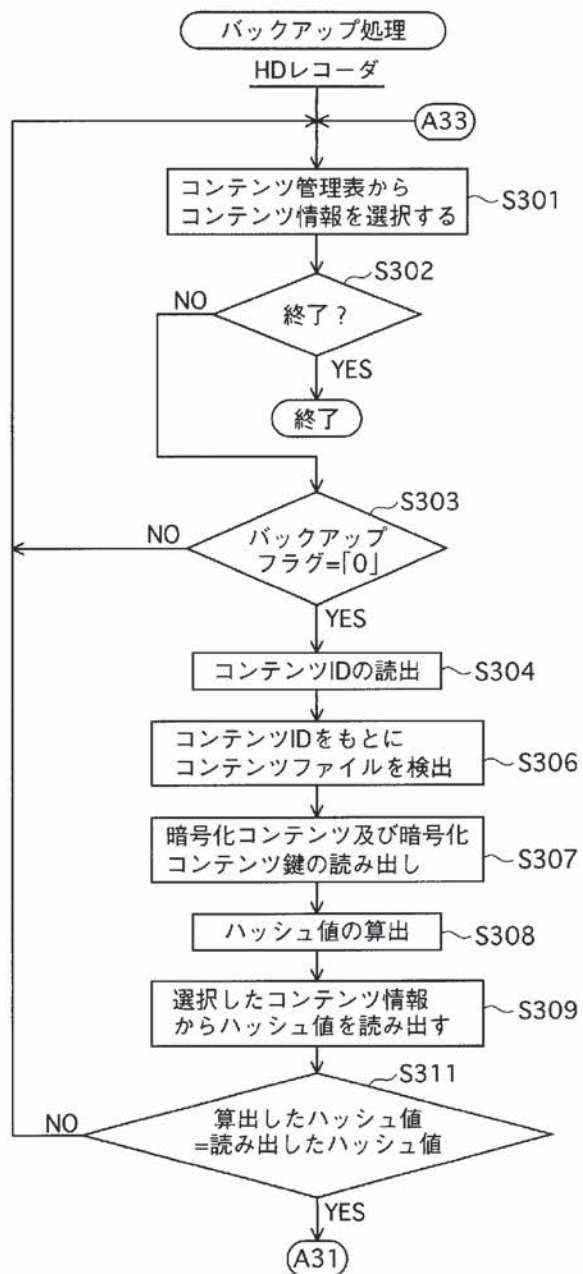
[図16]



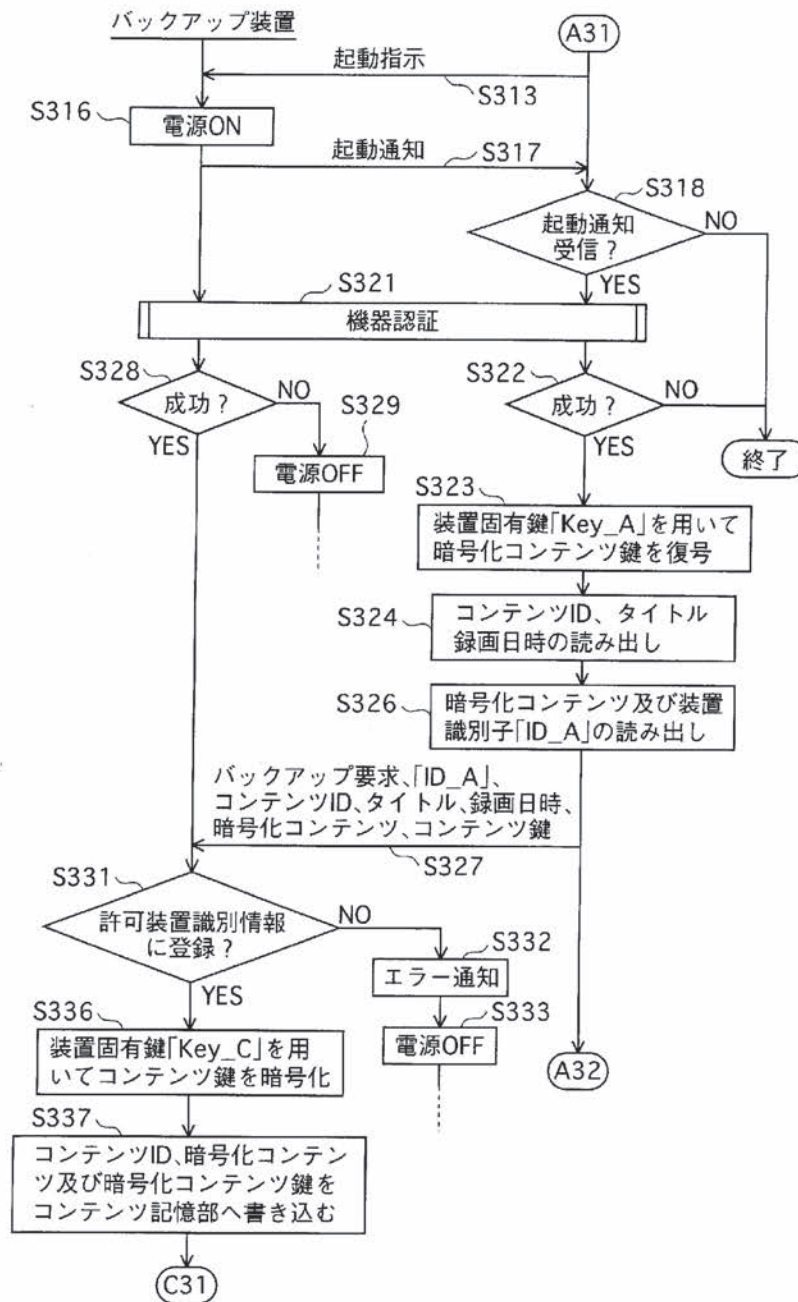
[図17]



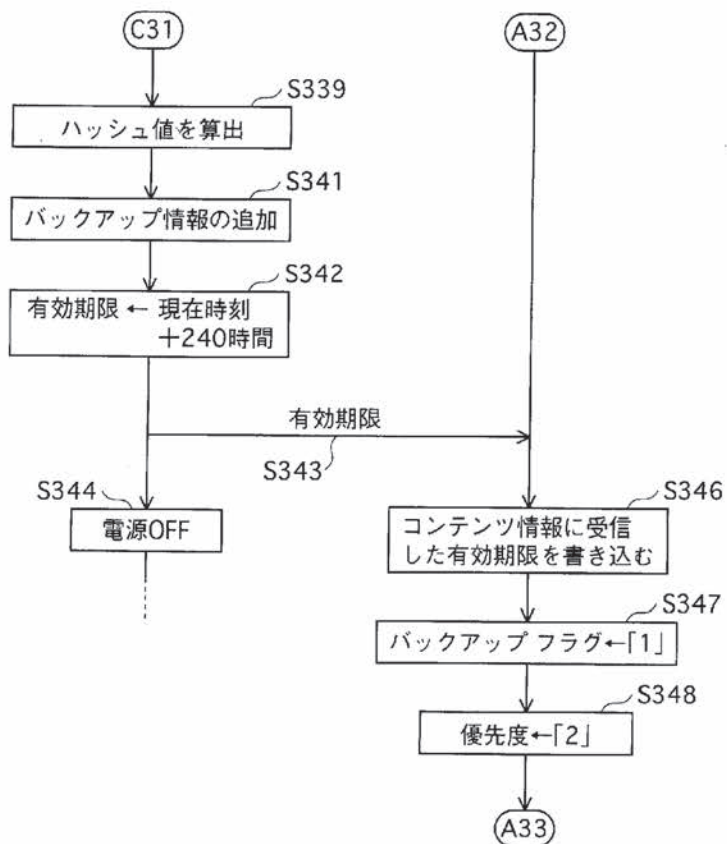
[図18]



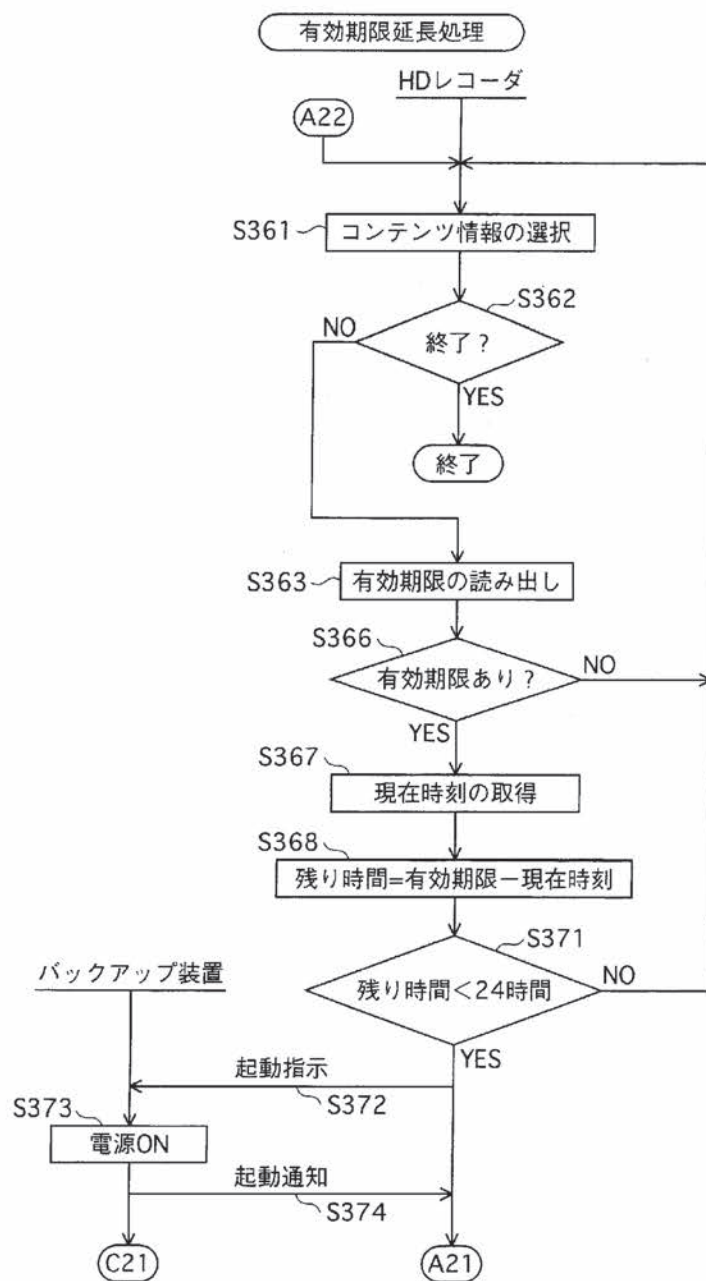
[図19]



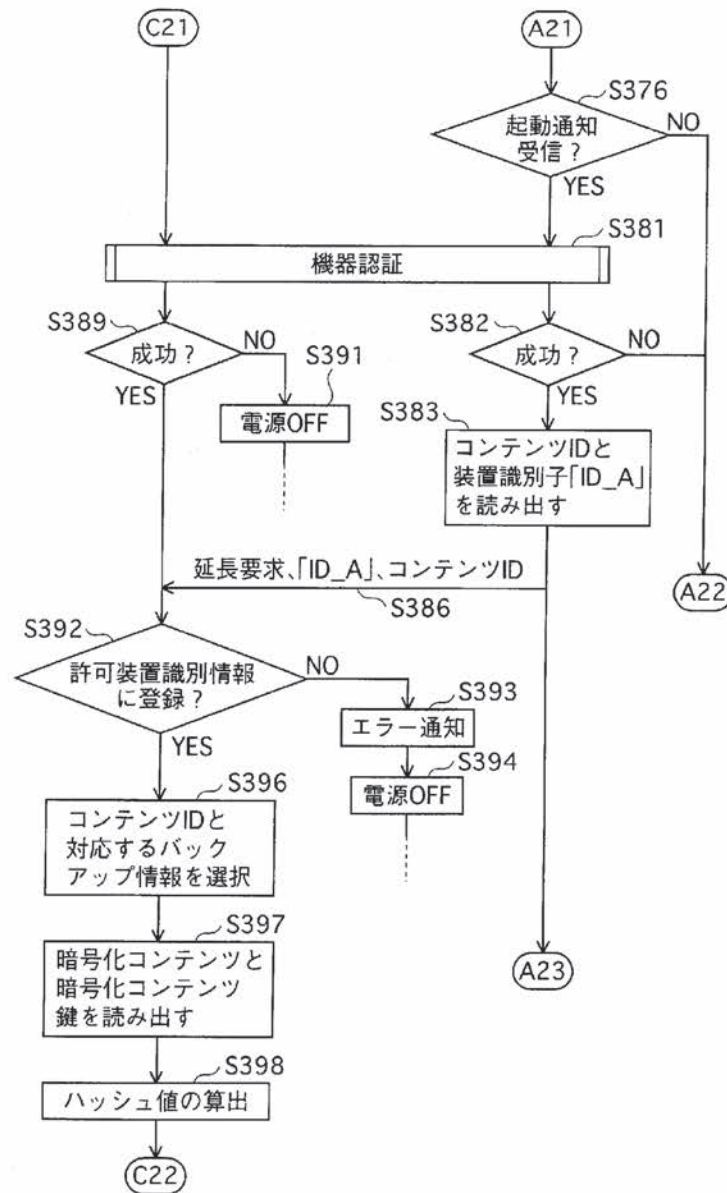
[図20]



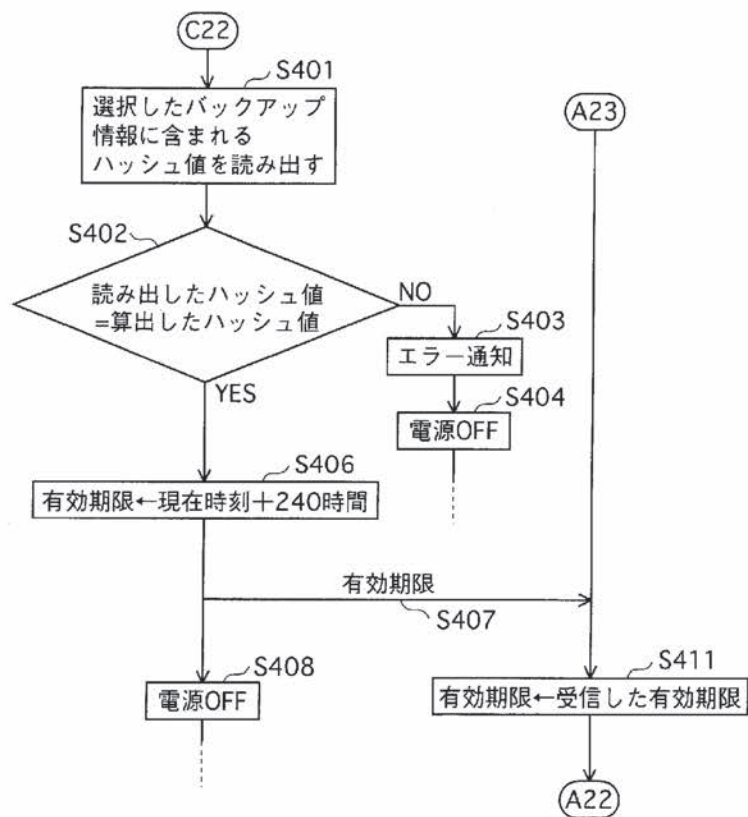
[図21]



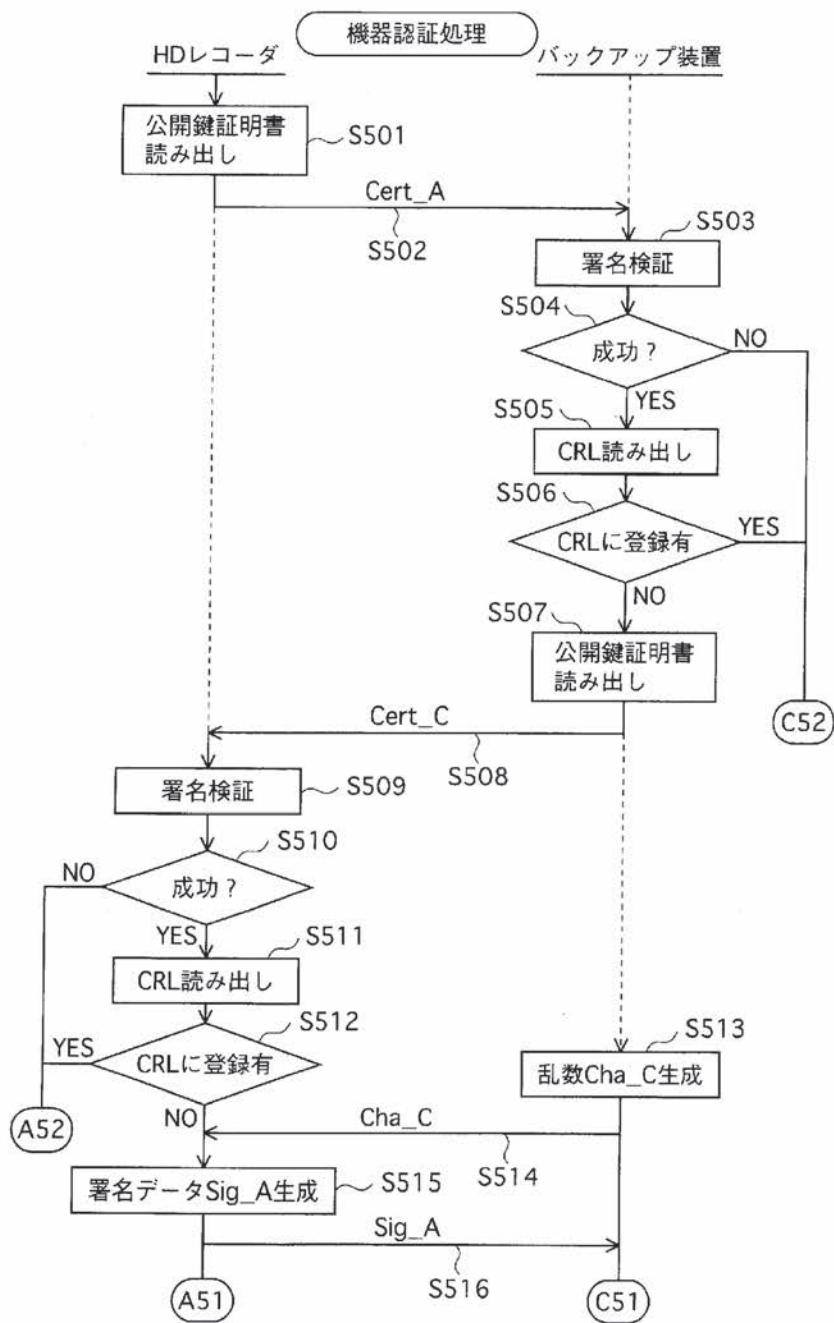
[図22]



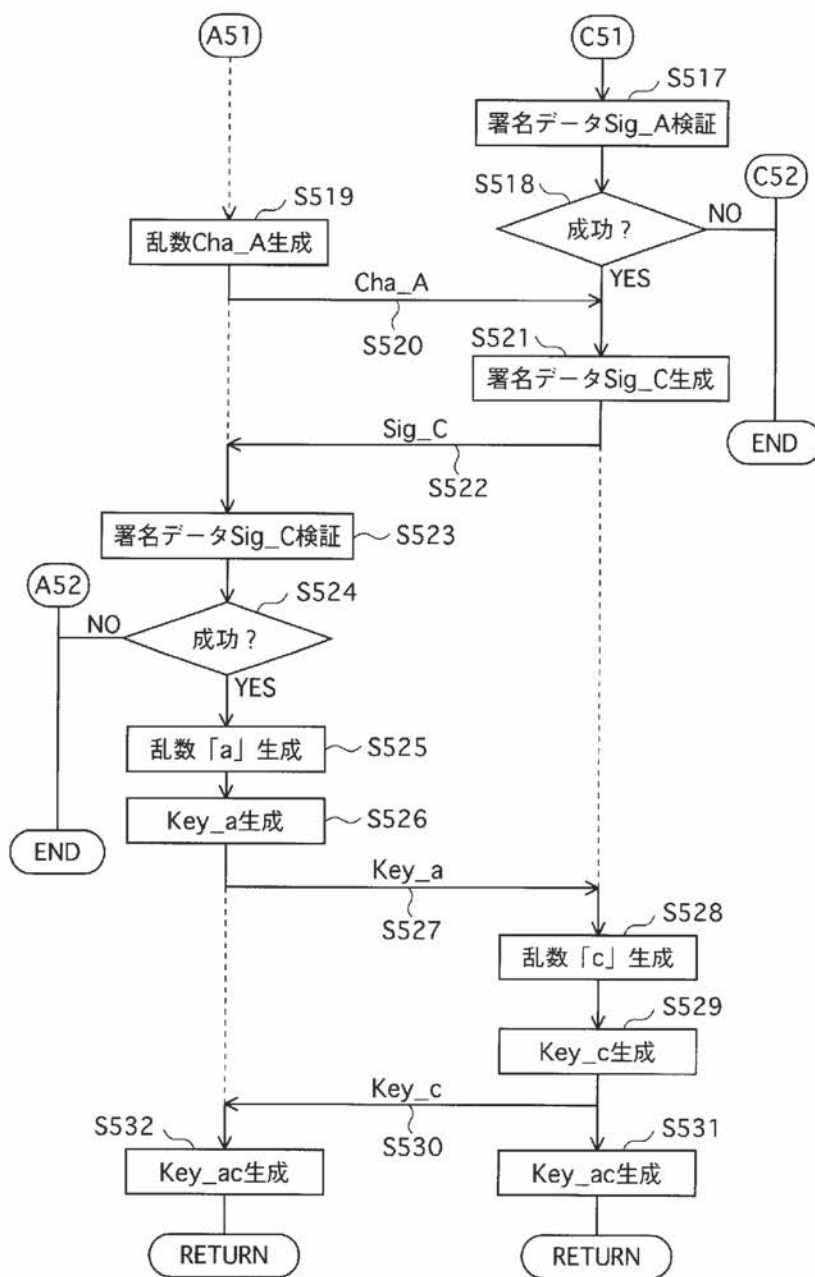
[図23]



[図24]



[図25]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022772

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-186751 A (Matsushita Electric Industrial Co., Ltd.), 04 July, 2003 (04.07.03), Par. No. [0298] (Family: none)	19-25, 27-31
Y	JP 11-203127 A (Casio Computer Co., Ltd.), 30 July, 1999 (30.07.99), Abstract (Family: none)	19-25, 27-31
A	JP 8-263440 A (Xerox Corp.), 11 October, 1996 (11.10.96), Par. Nos. [0081] to [0083], [0176] to [0180] & US 5715403 A & EP 0715244 A1	1-35

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 February, 2006 (14.02.06)

Date of mailing of the international search report
21 February, 2006 (21.02.06)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022772

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-14221 A (Victor Company Of Japan, Ltd.), 19 January, 2001 (19.01.01), Par. Nos. [0022] to [0023] & EP 1049087 A2	1-35
A	JP 2004-54988 A (Sony Corp.), 19 February, 2004 (19.02.04), Abstract (Family: none)	1-35
A	JP 2003-30054 A (Sharp Corp.), 31 January, 2003 (31.01.03), Full text; all drawings (Family: none)	1-35

A. 発明の属する分野の分類 (国際特許分類 (IPC))			
Int.Cl. G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)			
B. 調査を行った分野			
調査を行った最小限資料 (国際特許分類 (IPC))			
Int.Cl. G06F21/24 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01), H04N5/91 (2006.01), H04N7/167 (2006.01), H04N7/173 (2006.01)			
最小限資料以外の資料で調査を行った分野に含まれるもの			
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2006年 日本国実用新案登録公報 1996-2006年 日本国登録実用新案公報 1994-2006年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
Y	JP 2003-186751 A (松下電器産業株式会社) 2003.07.04, 【0298】 (ファミリーなし)	19-25, 27-31	
Y	JP 11-203127 A (カシオ計算機株式会社) 1999.07.30, 【要約】 (ファミリーなし)	19-25, 27-31	
A	JP 8-263440 A (ゼロックス コーポレーション) 1996.10.11, 【0081】 - 【0083】, 【0176】 - 【0180】 & US 5715403 A & EP 0715244 A1	1-35	
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献			
国際調査を完了した日 14.02.2006		国際調査報告の発送日 21.02.2006	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 平井 誠 電話番号 03-3581-1101 内線 3546	5S 9071

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2001-14221 A (日本ビクター株式会社) 2001. 01. 19, 【0022】 －【0023】, EP 1049087 A2	1-35
A	JP 2004-54988 A (ソニー株式会社) 2004. 02. 19, 【要約】(ファミリーなし)	1-35
A	JP 2003-30054 A (シャープ株式会社) 2003. 01. 31, 全文, 全図 (ファミリーなし)	1-35