

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006 年 3 月 2 日 (02.03.2006)

PCT

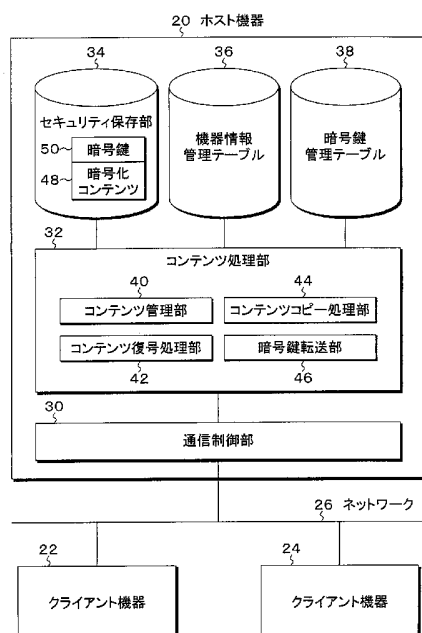
(10) 国際公開番号
WO 2006/022006 A1

- (51) 国際特許分類⁷: H04L 9/06 2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP2004/012266
- (22) 国際出願日: 2004 年 8 月 26 日 (26.08.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 山嶋 雅樹 (YAMASHIMA, Masaki) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP). 川井 修 (KAWAI, Osamu) [JP/JP]; 〒
- (74) 代理人: 竹内 進 (TAKEUCHI, Susumu); 〒1050003 東京都港区西新橋 3 丁目 2 番 4 7 号 清水ビル 8 階 Tokyo (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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

[続葉有]

(54) Title: CONTENT MANAGEMENT PROGRAM, METHOD, AND DEVICE

(54) 発明の名称: コンテンツ管理プログラム、方法及び装置



- 20... HOST DEVICE
34... SECURITY STORAGE UNIT
50... ENCRYPTION KEY
48... ENCRYPTED CONTENT
36... DEVICE INFORMATION MANAGEMENT TABLE
38... ENCRYPTION KEY MANAGEMENT TABLE
32... CONTENT PROCESSING UNIT
40... CONTENT MANAGEMENT UNIT
42... CONTENT DECODING PROCESSING UNIT
44... CONTENT COPY PROCESSING UNIT
46... ENCRYPTION KEY TRANSFER UNIT
30... COMMUNICATION CONTROL UNIT
26... NETWORK
22... CLIENT DEVICE
24... CLIENT DEVICE

(57) Abstract: An encrypted content having a use condition of copyright inhibiting copy in a device which has received the content and an encryption key are stored. The encrypted content is copied/transferred via a network to/from another device. The encryption key is transferred via the network so that is stored in one of the devices. Even when recording/storing a highly fine television broadcast signal received with a copyright use condition of copy once, an access flag is provided for controlling presence/absence of reproduction of the broadcast content for each broadcast content. When an original broadcast content is transcoded to a low resolution and transferred to another device, the access flag is turned on so as to enable reproduction.

[続葉有]



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, IT, LU, 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).

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。

添付公開書類:

— 国際調査報告書

(57) 要約: コンテンツを受信した装置でのコピーを禁止するような著作権の利用条件とした暗号化コンテンツとその暗号鍵を保存し、他の機器との間でネットワークを介して暗号化コンテンツをコピー転送すると共に何れか1つの機器に保存されるようにネットワークを介して暗号鍵を転送する。コピーワンスを著作権の利用条件として受信された高精細度テレビジョン放送信号を録画保存する場合にも放送コンテンツ毎に放送コンテンツの再生の有無を制御するアクセスフラグを設ける。オリジナルの放送コンテンツを低解像度にトランスコーディングして他の機器に転送した際には、そのアクセスフラグをオンして再生可能とする。

明 細 書

コンテンツ管理プログラム、方法及び装置

技術分野

- [0001] 本発明は、著作権に基づきユーザのアクセス権が付与されたコンテンツを管理するユビキタス環境におけるコンテンツ管理プログラム、方法及び装置に関し、特に、コンテンツを複数の機器間で転送しながら利用可能とするコンテンツ管理プログラム、方法及び装置に関する。

背景技術

- [0002] 現在、音楽、映像、ドキュメントなど様々なコンテンツがデジタル化されているが、デジタルデータ化されたことでコンテンツのコピーが容易にできるようになり、とりわけ深刻なのが不正コピーの問題である。
- [0003] 著作権侵害にあたる不正コピーが出回れば、配信業者や著作権保有者が損害を被るばかりでなく、消費者にも好ましくない影響を及ぼすことになる。このため価値の高いコンテンツに関しては著作権管理機能が実装されたデジタル著作権管理のシステム環境で運用されることが要求されてきている。
- [0004] 通常、デジタル著作権管理システムでは、コンテンツは暗号化され、暗号化コンテンツにアクセスする許可が与えられたアクセス権所有者に対しては、暗号化コンテンツとその暗号鍵が配布される。アクセス権所有者は、暗号化コンテンツと暗号鍵を一つの機器に保管し、アクセスする際には暗号鍵を使って暗号化コンテンツの復号を行い、コンテンツにアクセスする。
- [0005] また別の機器でコンテンツにアクセスしたい場合には、暗号化コンテンツと暗号鍵を別の機器に転送する必要があるが、コンテンツのコピー防止のため、少なくとも暗号鍵と暗号化コンテンツのペアが複数の機器に同時に保管されることのないように制御する仕組みが使用されている。

特許文献1:特開2000-134193

特許文献2:特開2000-285028

発明の開示

発明が解決しようとする課題

- [0006] しかしながら、このような従来のデジタル著作権管理システムにあつては、アクセス権所有者が必要に応じて異なる機器によって入手したコンテンツにアクセスしようと試みた場合、事前に暗号鍵とコンテンツのペアを機器に転送しておく必要があり、ユーザの使い勝手を阻害するものである。
- [0007] この問題に対する一つの解決策として、鍵管理を行うサーバ、即ち鍵管理サーバを利用する方法がある。アクセス権所有者は1つの暗号化コンテンツを複数の機器に保存しておく。コンテンツにアクセスする時点で、まず鍵管理サーバにアクセスし、鍵管理サーバから暗号鍵を機器に転送もしくは期限付きでコピーし、この暗号鍵を使って暗号化コンテンツを復号する。
- [0008] 暗号鍵を転送した場合は、使用終了後に鍵管理サーバに暗号鍵を戻す。期限付きでコピーする場合は、設定された期限が過ぎると暗号鍵は使用できなくなる。
- [0009] しかし、鍵管理サーバを利用する方法にあつては、鍵管理サーバが必ず必要であることと、コンテンツにアクセスする際には必ず鍵管理サーバとの通信が必要になるという問題がある。
- [0010] 一方、テレビ放送の分野にあつても、デジタル放送の開始に伴って不正コピーが簡単に作られてインターネットに流出する問題を防ぐため、日本におけるBSデジタル及び地上デジタル放送の番組は、2004年4月1日から1回限りの録画を許容する「コピーワンス」を実現するコピー制御信号CCI(Copy Control Information)を導入している。
- [0011] しかしながら、HDTV(High Definition Television)解像度でハードディスクドライブ等に受信録画したコンテンツは、1回目の録画によりコピー・ワンスとなってコピープロテクトがかかっており、携帯端末で視聴するため320×240画素のQVGA(Quarte Viedo Graphic Arry)の低解像度にトランスコーディングしてSDカードなどメモ리카ードに一度転送すると、元のHDTVコンテンツは転送の際に消去される。そのため、後にメモ리카ードのQVGAコンテンツをハードディスクドライブに戻しても、元のHDTV解像度に復帰させることができず、コピーワンスのプロテクトがかかったHDTV解像度の放送コンテンツが失われ、二度と再生できなくなる問題がある。

[0012] 本発明は、コピーワンスという著作権利用の制約を維持しつつ1つのコンテンツを複数の機器にコピーしてアクセス可能とするコンテンツ管理プログラム、方法及び装置を提供することを目的とする。

[0013] 本発明は、コピーワンスという利用制約を維持しつつ、コンテンツを低解像度に変換して他の機器に転送した後に、元に戻した際に元の解像度への復帰を可能とするコンテンツ管理プログラム、方法及びプログラム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

[0014] (コンテンツコピーと暗号鍵転送)

本発明は、ネットワークを介して他の機器と接続された装置のコンピュータにより実行されるコンテンツ管理プログラムを提供する。

[0015] 本発明のコンテンツ管理プログラムは、コンピュータに、

コンテンツを受信した装置でのコピーを禁止するような著作権の利用条件とした暗号化コンテンツとその暗号鍵をコンテンツ保存部に保存するコンテンツ保存ステップと、

暗号鍵により暗号化コンテンツを復号する復号ステップと、

他の機器との間でネットワークを介して暗号化コンテンツをコピー転送するコンテンツコピーステップと、

他の機器との間でネットワークを介して暗号鍵を転送する暗号鍵転送ステップと、
を実行させることを特徴とする。

[0016] ここで暗号鍵転送ステップは、コンテンツ保存部の暗号鍵をネットワークを介して他の機器にコピー転送した後に保存している暗号鍵を消去する。

[0017] 暗号鍵転送ステップは、コンテンツ毎に暗号鍵を保存している機器を暗号鍵管理テーブルに登録し、復号ステップは、暗号化コンテンツを復号する際に、管理テーブルから認識した暗号鍵を保存している機器に対する転送要求により暗号鍵を取得して暗号化コンテンツを復号する。

[0018] 暗号鍵転送ステップは、暗号鍵を他の機器に転送した際に、自己の暗号鍵管理テーブルを更新すると共に他の機器に転送情報を通知して暗号鍵管理テーブルを更新させる。

- [0019] ネットワークを介して接続された機器は、機器管理テーブルに登録された同一ユーザの保有する機器である。またネットワークを介して接続された機器は、機器管理テーブルに登録された他のユーザの保有する機器を含んでもよい。暗号化コンテンツは、著作権を有する音楽、映像、ドキュメントのいずれか、もしくはそれらの組合せである。
- [0020] 本発明は、ネットワークを介して他の機器と接続された装置のコンテンツ管理方法を提供する。
- [0021] 本発明のコンテンツ管理方法は、
コンテンツを受信した装置でのコピーを禁止するような著作権の利用条件とした暗号化コンテンツとその暗号鍵をコンテンツ保存部に保存するコンテンツ保存ステップと、
暗号鍵により暗号化コンテンツを復号する復号ステップと、
他の機器との間で前記ネットワークを介して暗号化コンテンツをコピー転送するコンテンツコピーステップと、
他の機器との間で前記ネットワークを介して暗号鍵を転送する暗号鍵転送ステップと、を備えたことを特徴とする。
- [0022] 本発明は、ネットワークを介して他の機器と接続されたコンテンツ管理装置を提供する。
- [0023] 本発明のコンテンツ管理装置は、コンテンツを受信した装置でのコピーを禁止するような著作権の利用条件とした暗号化コンテンツとその暗号鍵を保存するコンテンツ保存部と、暗号鍵により暗号化コンテンツを復号する復号部と、他の機器との間でネットワークを介して暗号化コンテンツをコピー転送するコンテンツコピー部と、他の機器との間でネットワークを介して暗号鍵を転送する暗号鍵転送部とを備えたことを特徴とする。
- [0024] (コンテンツ管理プログラム)
本発明は、放送受信されたコンテンツのコンテンツ管理プログラムを提供する。本発明のコンテンツ管理プログラムは、コンピュータに、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の可否を制御す

るアクセス情報を設定するアクセス情報設定ステップと、

アクセス情報が再生可を示している場合にコンテンツを再生し、アクセス情報が再生不可を示している場合はコンテンツの再生を禁止するコンテンツ再生ステップと、

コンテンツ保存部に保存されたコンテンツの解像度を変換して該変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、

コンテンツをコンテンツ保存部に保存した際にアクセス情報を再生可に設定し、変換後のコンテンツを他の機器に転送した際にアクセス情報を再生不可に設定して再生を禁止し、更に他の機器に転送された変換後のコンテンツが再生不可になった場合にアクセス情報を再生可に設定して再生可能とするアクセス情報制御ステップと、
を実行させることを特徴とする。

[0025] ここで解像度とは、画像（動画、静止画）データについては画素密度のことであり、また音声データの場合はビットレートのことである。

[0026] 更に本発明のコンテンツ管理プログラムは、コンピュータに、アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミーコンテンツ数を設け、ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止するダミーコンテンツ制限ステップを実行させることを特徴とする。

[0027] コンテンツ転送ステップは、コンテンツ保存部に保存されたコンテンツを転送先の機器に対応した低解像度のコンテンツに変換して変換後のコンテンツを転送する。

[0028] 本発明は、コピー録画装置のコンピュータで実行されるコンテンツ管理プログラムを提供する。

[0029] このプログラムは、コンピュータに、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の有無を制御するアクセス情報を設定するアクセス情報設定ステップと、
アクセス情報が再生可を示している場合にコンテンツを再生し、アクセス情報が再生不可を示している場合はコンテンツの再生を禁止するコンテンツ再生ステップと、
コンテンツ保存部に保存されたコンテンツの解像度を変換して変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、

他の機器から転送してきたコンテンツをコンテンツ保存部に保存した際にアクセス情報を再生可に設定して再生可能とし、コンテンツを別の他の機器に転送した際にアクセス情報を再生不可に設定して再生を禁止するアクセス情報制御ステップと、を実行させることを特徴とする。

[0030] この場合にもコンテンツ管理プログラムを、コンピュータに、更に、アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミーコンテンツ数を設け、ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止させるダミーコンテンツ制限ステップを実行させる。

[0031] コンテンツ転送ステップは、コンテンツ保存部に保存されたコンテンツの解像度を転送先の機器に対応した低解像度のコンテンツに変換して転送し、コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、コンテンツを含まない転送処理を実行する。

[0032] コンテンツ転送ステップは、コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、保存しているコンテンツをそのまま残すか又は消去する。

[0033] コンテンツ転送ステップは、コンテンツをネットワーク接続又は着脱自在な記憶媒体を介して他の機器に転送する。また他の機器で変換後のコンテンツが再生不可となる場合は、変換後のコンテンツが戻される。

[0034] 本発明の別の形態にあつては、放送信号を保存して再生する装置のコンピュータにより実行されるコンテンツ管理プログラムを提供する。

[0035] この場合の本発明のプログラムは、コンピュータに、
信号を受信して並列的に同じコンテンツを再生する複数のコーデックステップと
複数のコーデックステップで並列的に再生された複数の同じコンテンツをコンテンツ保存部に保存するコンテンツ保存ステップと、
コンテンツ保存部に保存された同じコンテンツ毎に設定されたアクセス情報の何れか1つをオンして対応するコンテンツを再生可能とすると共に、残りのアクセス情報を全てオフして対応するコンテンツの再生を禁止するフラグ制御ステップと、

複数の同じコンテンツの中でアクセス情報がオンしている前記コンテンツを選択して再生するコンテンツ再生ステップと、
を実行させることを特徴とする。

[0036] このような本発明のコンテンツ管理プログラムにおいて、コンテンツは、1回限りのコピーを著作権の利用条件として受信されたテレビジョン放送信号である。

[0037] (コンテンツ管理方法)

本発明のコンテンツ管理方法は、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の可否を制御するアクセス情報を設定するアクセス情報設定ステップと、
アクセス情報が再生可を示している場合に前記コンテンツを再生し、アクセス情報が再生不可を示している場合はコンテンツの再生を禁止するコンテンツ再生ステップと、
コンテンツ保存部に保存されたコンテンツの解像度を変換して変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、
コンテンツをコンテンツ保存部に保存した際にアクセス情報を再生可に設定し、変換後のコンテンツを他の機器に転送した際にアクセス情報を再生不可に設定して再生を禁止し、更に他の機器に転送された変換後のコンテンツが再生不可になった場合にアクセス情報を再生可に設定して再生可能とするアクセス情報制御ステップと、
を備えたことを特徴とする。

[0038] 本発明によるコンテンツ管理方法の別の形態にあつては、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の有無を制御するアクセス情報を設定するアクセス情報設定ステップと、
アクセス情報が再生可を示している場合にコンテンツを再生し、アクセス情報が再生不可を示している場合はコンテンツの再生を禁止するコンテンツ再生ステップと、
コンテンツ保存部に保存されたコンテンツの解像度を変換して変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、
他の機器から転送してきたコンテンツをコンテンツ保存部に保存した際にアクセス情報を再生可に設定して再生可能とし、コンテンツを別の他の機器に転送した際に

アクセス情報を再生不可に設定して再生を禁止するアクセス情報制御ステップと、
を備えたことを特徴とする。

- [0039] 本発明によるコンテンツ管理方法の別の形態にあつては、
信号を受信して並列的に同じコンテンツを再生する複数のコーデックステップと
複数のコーデックステップで並列的に再生された複数の同じコンテンツをコンテンツ
保存部に保存するコンテンツ保存ステップと、
コンテンツ保存部に保存された同じコンテンツ毎に設定されたアクセス情報の何れ
か1つをオンして対応するコンテンツを再生可能とすると共に、残りのアクセス情報を
全てオフして対応するコンテンツの再生を禁止するフラグ制御ステップと、
複数の同じコンテンツの中でアクセス情報がオンしている前記コンテンツを選択して
再生するコンテンツ再生ステップと、
を備えたことを特徴とする。

- [0040] (コンテンツ管理装置)
本発明はコンテンツ管理装置を提供する。本発明のコンテンツ管理装置は、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の可否を制御す
るアクセス情報を設定するアクセス情報設定部と、
アクセス情報が再生可を示している場合にコンテンツを再生し、アクセス情報が再
生不可を示している場合はコンテンツの再生を禁止するコンテンツ再生部と、
コンテンツ保存部に保存されたコンテンツの解像度を変換して変換後のコンテンツ
を他の機器に転送するコンテンツ転送部と、
コンテンツをコンテンツ保存部に保存した際にアクセス情報を再生可に設定し、変
換後のコンテンツを他の機器に転送した際にアクセス情報を再生不可に設定して再
生を禁止し、更に他の機器に転送された変換後のコンテンツが再生不可になった場
合にアクセス情報を再生可に設定して再生可能とするアクセス情報制御部と、
を備えたことを特徴とする。

- [0041] 本発明によるコンテンツ管理装置の他の形態にあつては、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の有無を制御す
るアクセス情報を設定するアクセス情報設定部と、

アクセス情報が再生可を示している場合にコンテンツを再生し、アクセス情報が再生不可を示している場合はコンテンツの再生を禁止するコンテンツ再生部と、
コンテンツ保存部に保存されたコンテンツの解像度を変換して変換後のコンテンツを他の機器に転送するコンテンツ転送部と、
他の機器から転送してきたコンテンツをコンテンツ保存部に保存した際にアクセス情報を再生可に設定して再生可能とし、コンテンツを別の他の機器に転送した際にアクセス情報を再生不可に設定して再生を禁止するアクセス情報制御部と、
を備えたことを特徴とする。

- [0042] 本発明によるコンテンツ管理装置の他の形態にあつては、
信号を受信して並列的に同じコンテンツを再生する複数のコーデックステップと
複数のコーデックステップで並列的に再生された複数の同じコンテンツを保存する
コンテンツ保存部と、
コンテンツ保存部に保存された同じコンテンツ毎に設定されたアクセス情報の何れか1つをオンして対応するコンテンツを再生可能とすると共に、残りのアクセス情報を全てオフして対応するコンテンツの再生を禁止するフラグ制御部と、
複数の同じコンテンツの中でアクセス情報がオンしている前記コンテンツを選択して再生するコンテンツ再生部と、
を備えたことを特徴とする。

- [0043] なお、本発明におけるコンテンツ管理方法及び装置の詳細は、コンテンツ管理プログラムの場合と基本的に同じになる。

発明の効果

- [0044] (コンテンツコピーと鍵転送)

本発明によれば、鍵管理サーバを必要とせずにアクセス権所有者はコンテンツにアクセスする機器だけで1回限りのコピーを許容するコピーワンスの制約条件が課された暗号化コンテンツを暗号鍵を使用して利用することができる。

- [0045] また暗号化コンテンツを複数の機器にコピーすると共に全ての機器で暗号鍵がどの機器に保存しているかを認識していることで、アクセス権所有者が使用する機器を変更した場合や機器を使用する場所を変更したような場合でも、他の機器に保存し

ている暗号鍵を自動取得して暗号化コンテンツにアクセスすることができ、コピーワンスの制約条件を維持しながら1つのコンテンツを複数の機器で同時利用とならない限り、自由にアクセスでき、コンテンツを利用する際の利便性を大幅に向上することができる。

[0046] (コンテンツ管理)

本発明のコンテンツ管理によれば、例えば受信録画したHDTV解像度のコンテンツは残したまま別の機器の低解像度に変換してコンテンツを保存しており、解像度の異なる同じ放送コンテンツを複数の機器に保存するが、1つの機器のみにつきアクセス情報を再生可に設定してコンテンツの利用を可能とし、他の全ての機器はアクセス情報を再生不可に設定しておくことで保存しているコンテンツの利用を禁止する。これによって複数の機器にコンテンツが保存されていても、利用できるコンテンツを1つに制限するためのコピーワンスのプロテクトがかかった録画保存状態を実質的に実現している。

[0047] また低解像度に変換したコンテンツを元に戻すと、オリジナルの高解像度のコンテンツが利用可能となる。この場合、低解像度から高解像度へのコンテンツの転送は行わず、アクセス情報を転送したと同じ状態を作り出すことで、元の高解像度のコンテンツを再生利用できるようにし、一度、受信録画した高解像度の放送コンテンツが低解像度化して他の機器に送ることで、失われることはない。

[0048] また受信録画装置に複数のコーデック機能が設けられている場合、同じHDTV解像度の放送を並列的に受信録画することとなり、それぞれ個別にコピーワンスの条件を満足しているため、そのままではコーデック数分のコンテンツが録画され、2以上のコピーされたことと同じになり、コピーワンスの条件が破られてしまう。そこで多重コーデックによる受信録画についても、それぞれに設定しているアクセスキーのうちの1つのみをオンとし、1回に利用できるのは1つの録画コンテンツとすることで、多重コーデックに対してもコピーワンスの録画条件を維持できる。

図面の簡単な説明

[0049] [図1]本発明が適用される機器ネットワーク環境の説明図；

[図2]本発明のコンテンツ管理機能を備えた機器のブロック図；

- [図3]図2の機器情報データベースの説明図；
- [図4]図2のコンテンツデータベースの説明図；
- [図5]本発明が適用されるコンピュータのハードウェア環境のブロック図；
- [図6]本発明による機器間でコピーワンスの利用条件の下に暗号鍵を利用して暗号化コンテンツをアクセスする処理のタイムチャート；
- [図7]図2のホスト機器処理のフローチャート；
- [図8]図2のクライアント機器処理のフローチャート；
- [図9]本発明による放送コンテンツ管理処理が適用される機器環境のブロック図；
- [図10]図9の高解像度装置と低解像度装置の機能構成のブロック図；
- [図11]図10における放送コンテンツの解像度変換を伴う転送処理の説明図；
- [図12]図11の放送コンテンツの転送処理のタイムチャート；
- [図13]図10の高解像度装置における録画転送処理のフローチャート；
- [図14]図10の低解像度装置における転送録画処理のフローチャート；
- [図15]図14に続く転送録画処理のフローチャート；
- [図16]SDメモリを用いて放送コンテンツを転送する機器環境の説明図；
- [図17]本発明の放送コンテンツ管理処理が適用される他の機器環境のブロック図；
- [図18]ダミーコンテンツ数を管理する図17の高解像度装置と中解像度装置の機能構成のブロック図；
- [図19]図17における放送コンテンツの解像度変換を伴う転送処理の説明図；
- [図20]図19に続く転送処理の説明図；
- [図21]図20に続く転送処理の説明図；
- [図22]図17の放送コンテンツの転送処理のタイムチャート；
- [図23]図18の高解像度装置における録画転送処理のフローチャート；
- [図24]図18の中解像度装置における転送録画処理のフローチャート；
- [図25]図24に続く録画転送処理のフローチャート；
- [図26]図18におけるダミーコンテンツカウント処理のフローチャート；
- [図27]高解像度側へ戻る際に低解像度側のコンテンツを残す図18における放送コンテンツの解像度変換を伴う転送処理の説明図；

[図28]図27に続く転送処理の説明図；

[図29]図28に続く転送処理の説明図；

[図30]図27乃至図29におけるダミーコンテンツカウント処理のフローチャート；

[図31]本発明による多重コーデックで録画する装置の機能構成のブロック図；

[図32]図31の多重コーデック処理のフローチャート；

発明を実施するための最良の形態

[0050] (コンテンツコピーと鍵転送)

図1は、本発明によるコンテンツ管理処理が適用されるネットワーク環境の説明図である。図1において、本発明のコンテンツ管理処理が適用される機器として、あるユーザが

保有しているパーソナルコンピュータ10、ポータブル音楽再生装置12及び車載用音楽再生装置14を例にとっており、これらの装置はインターネット16を介してそれぞれに通信することができ、また音楽販売サイト18から楽曲コンテンツを購入してダウンロードすることができる。

[0051] 図2は、本発明のコンテンツ管理機能を備えた機器のブロック図である。図2において、この例にあつてはホスト機器20に対しネットワーク26を介してクライアント機器22, 24が接続されている。ホスト機器20は例えば図1のパーソナルコンピュータ10であり、ユーザがインターネット16を介して例えば音楽販売サイト18から楽曲を購入することで楽曲の暗号化コンテンツと暗号キーを取得している機器である。

[0052] これに対しクライアント機器22, 24は例えば図1のポータブル音楽再生装置12や車載用音楽再生装置14であり、ホスト機器20としてのパーソナルコンピュータ10から楽曲などの暗号化コンテンツなどのコピーを取得して利用する機器である。

[0053] 尚、ホスト機器やクライアント機器の名称は相対的なものであり、最初にコンテンツを入手した機器を単にホスト機器といっているにすぎず、これによる限定は受けない。

[0054] ホスト機器20には通信制御部30、コンテンツ処理部32、セキュリティ保存部34、機器情報管理テーブル36及び暗号鍵管理テーブル38が設けられている。コンテンツ処理部32はコンテンツ処理プログラムの実行により実現されるアプリケーションであり

、コンテンツ管理部40、コンテンツ復号処理部42、コンテンツコピー処理部44及び暗号鍵転送部46を備えている。

[0055] コンテンツ管理部40は、図1に示したようにインターネット16を介して、例えば音楽販売サイト18からコピーワンスの楽曲を購入することで楽曲の暗号化コンテンツと暗号鍵を取得し、セキュリティ保存部34に暗号化コンテンツ48及び暗号鍵50として保存する。

[0056] コンテンツ復号処理部42はセキュリティ保存部34に暗号鍵50が保存されていることを条件に、暗号鍵50により暗号化コンテンツ48を復号して出力表示などの利用を行なう。

[0057] コンテンツコピー処理部44は、クライアント機器22, 24との間でネットワーク26を介してセキュリティ保存部34に保存している暗号化コンテンツ48をコピー転送して保存させる。暗号鍵転送部46はクライアント機器22, 24との間でネットワーク26を介してセキュリティ保存部34に保存している暗号鍵50を転送する。

[0058] ここでコンテンツコピー処理部44による暗号化コンテンツ48のコピー処理は、クライアント機器22, 24に対しセキュリティ保存部34から暗号化コンテンツ48を読み出してコピー転送した後、暗号化コンテンツ48は残しておく。

[0059] これに対し暗号鍵転送部46にあつては、セキュリティ保存部34から暗号鍵50を読み出して例えばクライアント機器22にコピー転送した後、セキュリティ保存部34の暗号鍵50を消去する。このような暗号鍵転送部46の処理によってホスト機器20及びクライアント機器22, 24のいずれかひとつにのみ暗号鍵50が保存された状態となり、これによって1回限りのコピーを許容するコピーワンスを著作権の利用条件としたコンテンツのアクセスを可能とする。

[0060] 図3は、図2のホスト機器20に設けた機器情報管理テーブル36の説明図である。

機

器情報管理テーブル36には本発明のコンテンツ管理処理が適用される機器名とネットワーク上の位置が登録されている。図2の例では機器名として機器20、機器22及び機器24が登録され、ネットワーク上の位置としてはアドレスa、アドレスb、アドレスcが登録されている。

- [0061] この機器情報管理テーブル36に登録される本発明のコンテンツ管理処理が適用される機器は、基本的には同じ利用者が保有する機器であるが、利用者が許諾すれば他人の保有する機器を機器情報管理テーブル36に登録し、本発明のコンテンツ管理処理の対象機器に含めることができる。このように他人の機器を機器情報管理テーブル36に登録した場合には、ある利用者が取得したコンテンツをコピーワンスの制約約条件のもとに第3者に貸してコンテンツを利用させるような使い方ができる。
- [0062] 図4は、図2のホスト機器20に設けた暗号鍵管理テーブル38の説明図である。暗号鍵管理テーブル38は本発明のコンテンツ管理処理が適用される複数の機器のどの位置に暗号鍵が存在するかを登録したテーブル情報である。暗号鍵管理テーブル38にあつては、この例ではコンテンツ名、鍵の保存機器名及び暗号化方式を登録するようにしている。
- [0063] ここでコンテンツ名にはコンテンツA、コンテンツB、コンテンツCの3つが登録されており、それぞれ保存機器名として機器20、機器22、機器24が登録され、更に暗号化方式として α 方式と β 方式が登録されている。暗号化方式として α 方式、 β 方式としては具体的には現在著作権対象となるコンテンツに利用されている公知の適宜の暗号方式が採用される。
- [0064] 再び図2を参照するに、クライアント機器22、24についても基本的にはホスト機器20と同じ機能構成を備えており、クライアント機器22、24としては自分自身でネットワーク経由で新たなコンテンツを取得せず、ホスト機器20からのコピー処理によりコンテンツを入手する点が損している。もちろんクライアント機器22、24が直接インターネット経由でコンテンツを取得した場合にはそのコンテンツについてはホスト機器20としての機能を持つこととなる。
- [0065] ホスト機器20における通信制御部30、コンテンツ処理部32及びセキュリティ保存部34、機器情報管理テーブル36及び暗号鍵管理テーブル38の部分は、暗号化コンテンツ及び暗号鍵の転送及び復号処理を行なうことから、第3者による不正アクセスから保護するため耐タンパーなモジュール(Tamper Resistant Module)或いはソフトウェアで構築されている。
- [0066] またネットワーク26を介して接続したホスト機器20とクライアント機器22、24の機器

間における暗号化コンテンツ及び暗号鍵の転送については、クライアント機器22、24をホスト機器20を構成するパーソナルコンピュータに例えばIEEE1394ポートを介して接続するような場合にはDTPC (Digital Transmission Content Protection)を使って暗号化してやり取りし、またネットワーク26を経由してLANを使用した場合にはSSL (Secure Socket Layer)やIPSEC (Ip security protocol)を使って暗号化している。

[0067] またホスト機器20とクライアント機器22、24の間のデータ転送に際しては、まず2つの機器間で相互認証と鍵交換を行なった後、例えばハイブリッド方式により暗号化して暗号化コンテンツ及び暗号鍵のデータ転送を行なう。

[0068] ハイブリッド方式による暗号化は、送信側で擬似乱数を発生してセッション鍵を作成し、このセッション鍵を最初の鍵交換で得られた受信先の公開鍵を使用して暗号化し、一方、送信するメッセージについてはセッション鍵で暗号化して結合した後、送信する。受信側にあつては暗号化されている秘密鍵(プライベート鍵)に基づいて受信した暗号化セッション鍵を復号し、復号したセッション鍵で受信した暗号化メッセージを復号することになる。

[0069] 図2におけるホスト機器20は、例えば図5のようなコンピュータのハードウェア資源により実現される。図5のコンピュータにおいて、CPU200のバス201にはRAM202、ハードディスクコントローラ(ソフト)204、フロッピーディスクドライバ(ソフト)210、CD-ROMドライバ(ソフト)214、マウスコントローラ218、キーボードコントローラ222、ディスプレイコントローラ226、通信用ボード230が接続される。

[0070] ハードディスクコントローラ204はハードディスクドライブ206を接続し、本発明のコンテンツ管理処理を実行するプログラムをローディングしており、コンピュータの起動時にハードディスクドライブ206から必要なプログラムを呼び出して、RAM202上に展開し、CPU200により実行する。

[0071] フロッピーディスクドライバ210にはフロッピーディスクドライブ(ハード)212が接続され、フロッピーディスク(R)に対する読み書きができる。CD-ROMドライバ214に対しては、CDドライブ(ハード)216が接続され、CDに記憶されたデータやプログラムを

読み込むことができる。

- [0072] マウスコントローラ218はマウス220の入力操作をCPU200に伝える。キーボードコントローラ222はキーボード224の入力操作をCPU200に伝える。ディスプレイコントローラ226は表示部228に対して表示を行う。通信用ボード230は無線を含む通信回線232を使用し、LANを介してネットワーク内の機器や外部のインターネット上の機器との間で通信を行う。
- [0073] 図6は、本発明による機器間でのワンコピーの利用条件のもとに暗号鍵を利用して暗号化コンテンツをアクセスする処理のタイムチャートである。図6において、まずホスト機器20はステップS1で暗号化コンテンツと暗号鍵をインターネット経由で例えば音楽配信サイトから購入して入力することにより保存する。
- [0074] 続いてステップS2でコンテンツメニューと暗号鍵管理テーブルを作成し、これを他の機器に配信する。これを受けてクライアント機器22はステップS101でホスト機器20から受信したコンテンツメニューと暗号鍵管理テーブルを保存する。続いてクライアント機器22においてステップS102でメニューからコンテンツを選択すると、ステップS103で暗号化コンテンツの保存の有無をチェックする。
- [0075] 暗号化コンテンツが保存されていないならばステップS104に進み、暗号化コンテンツのコピーをホスト機器20に要求する。これを受けてホスト機器20はステップS3で保存している暗号化コンテンツを要求元のクライアント機器22にコピー転送する。クライアント機器22はステップS105でコピー転送された暗号化コンテンツを保存する。もちろんステップS103でメニューにより選択された暗号化コンテンツが保存されていればステップS104, S105はスキップする。
- [0076] 次にステップS106で暗号鍵の保存の有無をチェックする。暗号鍵が保存されていないならば暗号鍵管理テーブルの参照により現在ホスト機器20に保存されていることを認識し、ステップS107でホスト機器20に対し暗号鍵の転送要求を行なう。
- [0077] この転送要求を受けてホスト機器20はステップS4で暗号鍵を読み出して、要求元のクライアント機器22に転送する。暗号鍵を転送した後、ホスト機器20はステップS5で保存している暗号鍵を消去し、暗号鍵管理テーブルを更新する。
- [0078] ホスト機器20から暗号鍵の転送を受けたクライアント機器22はステップS108で暗

号鍵を保存した後、自分の暗号鍵管理テーブルを更新する。この暗号鍵管理テーブルの更新にあつては暗号鍵の転送元または転送先のいずれかから他の機器に対し暗号鍵管理テーブルの更新結果を通知して更新させる。続いてステップS109で暗号化コンテンツを転送により取得して保存している暗号鍵により復号して出力する。

[0079] 図7は、図2のホスト機器20におけるホスト機器処理のフローチャートである。図7において、ステップS1で暗号化コンテンツと暗号鍵を入力して保存し、ステップS2でコンテンツメニューの生成と暗号鍵管理テーブルに対する保存位置登録を行う。

[0080] 次にステップS3で暗号化コンテンツのコピー要求の有無をチェックしており、コピー要求を受けるとステップS4に進み、要求機器に暗号化コンテンツをコピー転送する。

[0081] 続いてステップS5でホスト機器自身におけるコンテンツの利用要求の有無を判別しており、利用要求があるとステップS6で暗号鍵の保存の有無をチェックし、暗号鍵の保存がなければステップS7に進み、暗号鍵管理テーブルの参照で現在暗号鍵を保存している機器に対し暗号鍵の転送要求を行い、ステップS8で取得した暗号鍵を保存し暗号鍵管理テーブルを更新する。

[0082] そしてステップS9で暗号化コンテンツを暗号鍵により復号して出力する。ステップS6で暗号鍵の保存があればステップS7ーS8はスキップしステップS9に進む。

[0083] 次にステップS10で他の機器から暗号鍵転送要求があるか否かチェックしており、転送要求があればステップS11で保存している暗号鍵を読み出して転送し、保存している暗号鍵を消去する。続いてステップS12で暗号鍵管理テーブルの保存位置を更新する。このステップS3ーS12の処理をステップS13でホスト機器の停止指示があるまで繰り返す。

[0084] 図8は、図2のクライアント機器22, 24における処理を示したフローチャートである。図8において、ステップS1でコンテンツメニューを表示し、ステップS2でメニュー表示を見てコンテンツ選択があったか否かチェックする。

[0085] コンテンツの選択があればステップS3に進み、暗号化コンテンツが保存されているか否かチェックする。保存されていなければステップS4でホスト機器に対し暗号化コンテンツのコピー転送を要求して保存する。

[0086] 続いてステップS5で暗号鍵を保存しているか否かチェックし、保存していなければ

暗号鍵管理テーブルの参照で判明した保存機器に対しステップS6で暗号鍵の転送要求を行なう。ステップS7で転送要求先から暗号鍵を取得すると取得した暗号鍵を保存し暗号鍵管理テーブルを更新する。

[0087] そしてステップS8で暗号化コンテンツを暗号鍵で復号して出力する。ステップS5で暗号鍵を保存していた場合にはステップS6, S7の処理はスキップする。

[0088] 続いてステップS9で他の機器からの暗号鍵の転送要求の有無をチェックしており、転送要求があればステップS10で暗号鍵を要求機器に転送して保存している暗号鍵を消去し、ステップS11で暗号鍵管理テーブルを更新する。このステップS1～S11の処理をステップS12でクライアント機器に対し停止指示があるまで繰り返すことになる。

[0089] 尚、本発明のコンテンツ管理処理にあつては機器情報テーブルの登録している全ての機器が常時接続状態にあることが必要である。しかし、実際の使用状態にあつては特定の機器で電源が切られて常時接続でなくなる場合があり、この常時接続でなくなった機器に暗号鍵が保存されていたとすると、他の常時接続されている機器に暗号鍵を転送することができず、暗号化コンテンツを復号して利用することができない。

[0090] このため使用後は電源を切るような機器については、他の機器からの制御で電源を自動的に投入できるオートパワーアップコントロールの機能を設けておき、電源切り離しによる機器接続状態にあつては暗号鍵の転送要求を受けて自動的に電源投入が行われ転送要求に対し暗号鍵を読み出して転送させ、転送終了で電源を落とす処理機能を設けることが望ましい。

[0091] また機器の常時接続を可能とするため暗号鍵及び暗号化コンテンツの転送に必要な部分のみを常時電源供給による動作要求とし、それ以外の部分を電源スイッチなどによりオンオフできるようにしてもよい。

[0092] また本発明の対象となる機器としてはパーソナルコンピュータや車載端末以外にPDAや携帯電話などの適宜の利用者端末に適用できる。

[0093] またコピーワンスの利用条件でアクセスするコンテンツとしては音楽コンテンツ、映像コンテンツ、カラオケコンテンツ、地図コンテンツ、ゲームコンテンツ、電子ブックな

どあらゆるデジタルコンテンツを対象とする。

[0094] (放送コンテンツ)

図9は、本発明による放送コンテンツ管理処理が適用される機器環境のブロック図である。なお、この実施形態にあつては、コンテンツとして画像データを例にとつて画素密度で示される解像度を扱っているが、本発明が対象とするコンテンツには音楽データも含まれ、音楽データの場合の解像度はビットレートで示されることになる。

[0095] 図9において、この実施形態にあつては、高解像度装置100と低解像度装置104を、ネットワーク106を介して接続している。高解像度装置100は例えばハードディスクドライブHDD内蔵のHDTV録画装置であり、HDTVチューナ110とハードディスクドライブを用いたコンテンツ保存部112を備えており、コンテンツ保存部112にはHDTVチューナ110で受信再生したHDTVテレビジョン放送番組であるHDTVコンテンツ114が保存されている。

[0096] 低解像度装置104は例えばフラッシュメモリ120を内蔵したQVGA携帯端末であり、高解像度装置100に保存しているHDTVコンテンツ114を低解像度のQVGAコンテンツ122にトランスコーディングしたコンテンツを保存している。

[0097] このような本発明が適用される高解像度装置100及び低解像度装置104は、それぞれHDTV放送の受信録画における1回限りの録画を許容するワンスコピーのためのコピー制御情報(CCI)に基づくコピー制御のルールを遵守した機器であり、更に機器間でデジタル著作権保護のための通信を行うため、認証機関が発行した証明書を備えている。この証明書には、それぞれの公開鍵情報などが含まれている。

[0098] 高解像度装置100と低解像度装置104の間で行われる暗号化通信としては、例えばハイブリッド方式を採用している。ハイブリッド方式は機器間で相互認証を行った後に公開鍵をやり取りし、送信元は送信メッセージを擬似ランダム処理に発生したセッション鍵で暗号化して送り、このセッション鍵を相手方から受信した公開鍵で暗号化して送ることになる。

[0099] 受信側にあつては、秘密鍵に基づき暗号化セッション鍵からセッション鍵を復号し、復号したセッション鍵により暗号化メッセージを復号してメッセージを取り出すことになる。

- [0100] 図10は、図9の高解像度装置と低解像度装置の機能構成のブロック図である。図10において、高解像度装置100には、HDTVチューナ110及び放送コンテンツ保存部112に加え、通信制御部124とコンテンツ管理部126を設けている。
- [0101] コンテンツ管理部126はコンテンツ管理処理プログラムの実行により実現されるアプリケーションである。コンテンツ管理部126には、アクセスフラグ(アクセス情報設定部)設定部128、アクセスフラグ制御部(アクセス情報制御部)134、コンテンツ再生部136及びコンテンツ転送部138が設けられている。
- [0102] 高解像度装置100に対しネットワーク106を介して接続された低解像度装置104は、通信制御部242、コンテンツ管理部244及び放送コンテンツ保存部246を備えている。コンテンツ管理部244はコンテンツ管理プログラムの実行により実現される機能である。
- [0103] コンテンツ管理部244には、アクセスフラグ設定部248、アクセスフラグ制御部254、コンテンツ転送部258及びコンテンツ再生部256が設けられている。
- [0104] 高解像度装置100のコンテンツ管理部126に設けたアクセス情報設定部として機能するアクセスフラグ設定部128は、HDTVチューナ110で受信されたコピーワンスを著作権の利用条件とする高精細度テレビジョン放送信号を放送コンテンツ保存部112にHDTVコンテンツ114として保存する際に、放送コンテンツの再生の有無を制御するためのアクセスフラグ130を設定する。アクセスフラグ130はHDTVコンテンツ114の最初の保存の際に1(オン)にセットされる。このアクセスフラグ130のセットの制御はアクセスフラグ制御部134により行われる。
- [0105] コンテンツ再生部136は、放送コンテンツ保存部112に保存されているHDTVコンテンツ114を再生する際にアクセスフラグ130を参照し、アクセスフラグ130が1(再生可)にセットされている場合には再生処理を行い、アクセスフラグが0(再生不可)にセットされている場合はコンテンツの再生を禁止する。
- [0106] コンテンツ転送部138は、放送コンテンツ保存部112に保存しているオリジナルのHDTVコンテンツ114を解像度変換部140により、低解像度装置104におけるQVGAコンテンツにトランスコーディングして転送する。
- [0107] コンテンツ転送部138によりトランスコーディングしてコンテンツを転送した場合、ア

クセスフラグ制御部134は転送元となったHDTVコンテンツ114のアクセスフラグ130を0にリセットする。またアクセスフラグ制御部134は、低解像度装置104に転送したコンテンツが戻ってきた際には、アクセスフラグ130を1にセットして、HDTVコンテンツ114を再生可能とする。

[0108] 低解像度装置104側のコンテンツ管理部244に設けているアクセスフラグ設定部248、アクセスフラグ制御部254、コンテンツ再生部256及びコンテンツ転送部258の機能も、基本的に高解像度装置100のコンテンツ管理部126と同じである。

[0109] 相違点は、高解像度装置100からトランスコーディングされた低解像度のQVGAコンテンツ122の転送を受けて放送コンテンツ保存部246に保存し、これに伴いアクセスフラグ設定部248でアクセスフラグ164を設定し、保存の際にアクセスフラグ制御部254でアクセスフラグ164を1にセットし、コンテンツ再生部256による再生を可能としている点である。

[0110] またコンテンツ転送部258は、QVGAコンテンツ122より低い低解像度の装置に放送コンテンツを転送する際に、解像度変換部260でトランスコーディングを行って転送し、この転送に伴いアクセスフラグ制御部254はアクセスフラグ164を0にリセットすることになる。なおQVGAコンテンツより低い解像度の機器が存在しなければ、コンテンツ転送部258の機能は不要である。

[0111] 図11は、図10における放送コンテンツの解像度変換を伴う転送処理の説明図である。図11(A)は高解像度装置100におけるHDTVコンテンツの受信録画の状態であり、受信したHDTVコンテンツ114を保存すると共に、そのアクセスフラグ130を1にセットする。

[0112] 次に図11(B)のように、高解像度装置100から低解像度装置104にコンテンツを転送する場合には、高解像度装置100におけるHDTVコンテンツ114を例えばQVGAコンテンツ122にトランスコーディングして転送することで低解像度装置104に保存し、このとき転送元となる高解像度装置100のアクセスフラグ130は0にリセットし、転送先となる低解像度装置104のアクセスフラグ164は1にセットする。

[0113] この状態にあっては、高解像度装置100と低解像度装置104のそれぞれに解像度の異なる同一放送内容のコンテンツが別々に存在しているが、再生ができるのはアク

セスフラグ164が1となっている低解像度装置104のみであり、高解像度装置100にあってはアクセスフラグ130が0であることから再生ができず、これによってHDTVコンテンツの録画に要求されるコピーワンスのコピー制御ルールを維持することができる。

[0114] 図11(C)は、低解像度装置104から高解像度装置100にコンテンツを戻した場合の説明図である。低解像度装置104のQVGAコンテンツ122を高解像度装置100に戻す場合には、コンテンツの高解像度へのトランスコーディングは行わず、即ちコンテンツの転送を伴うことなく転送指示のみを高解像度装置100に送る転送処理を行う。

[0115] この高解像度側への転送により、低解像度装置104におけるアクセスフラグ164は0にリセットされ、高解像度装置100のアクセスフラグ130が1にセットされることで、転送先となった高解像度装置100においてのみコンテンツを再生することができる。

[0116] なお転送元となった低解像度装置104にあっては、転送後に保存しているQVGAコンテンツ122を残してもよいし消去してもよい。QVGAコンテンツ122を図示のように残す場合には、アクセスフラグ164は0にリセットする。またQVGAコンテンツ122を転送後に消去する場合には、アクセスフラグ164も消去すればよい。

[0117] 図12は、図11の放送コンテンツの転送処理のタイムチャートである。図12において、高解像度装置100にあっては、ステップS1でHDTVコンテンツの受信に基づく録画保存を行っており、録画保存が済むと、ステップS2でアクセスフラグを1にセットする。

[0118] 続いてステップS3で低解像度装置104に対する転送要求を判別すると、ステップS4に進み、低解像度のQVGAコンテンツにトランスコーディングした後、ステップS5で低解像度装置104との間に相互認証と鍵交換を行う。これに伴い低解像度装置104にあってはステップS101で相互認証と鍵交換を行う。

[0119] この相互認証と鍵交換は、例えば予め高解像度装置100及び低解像度装置104に持たせている認証機関が発行した証明書に基づいて行われる。相互認証に成功して鍵交換が済むと、ステップS6で高解像度装置100はトランスコーディングの済んだQVGAコンテンツを暗号化して低解像度装置104に送信する。

- [0120] この暗号化は例えばハイブリッド方式を採用していることから、擬似乱数として発生したセッション鍵によりQVGAコンテンツを暗号化し、またセッション鍵を低解像度装置104から通知された公開鍵で暗号化し、両者を結合して送信する。
- [0121] 低解像度装置104は、ステップS102で暗号化QVGAコンテンツを受信復号して保存する。この暗号化QVGAコンテンツの受信復号は、暗号化されたセッション鍵を自分の秘密鍵(プライベート鍵)に基づいて復号し、復号したセッション鍵で暗号化QVGAコンテンツを復号して保存することになる。
- [0122] 転送元となった高解像度装置100にあっては、ステップS6で暗号化送信が終了すると、ステップS7でアクセスフラグを0にリセットし、高解像度装置100におけるコンテンツの再生を禁止する。一方、転送先となった低解像度装置104にあっては、ステップS102で暗号化QVGAコンテンツを受信復号して保存した後、ステップS103でアクセスフラグを1にセットする。そしてステップS104でアクセスフラグが1にセットされていることを条件にQVGAコンテンツを再生することができる。
- [0123] 続いてステップS105で高解像度装置100に対する転送要求を判別すると、ステップS106で相互認証と鍵交換を行った後、ステップS107で転送指示のみを暗号化して送信する。そしてステップS108でQVGAコンテンツを残していることからアクセスフラグを0にリセットする。
- [0124] 高解像度装置100にあっては、ステップS8で低解像度装置104との間で相互認証と鍵交換を行った後、ステップS9で暗号化された転送指示を復号して認識し、ステップS10でアクセスフラグを1にセットし、これによってHDTVコンテンツの再生を可能とする。
- [0125] 図13は、図10の高解像度装置における録画転送処理のフローチャートである。図13において、ステップS1で録画放送番組の選択が行われると、ステップS2で高精度テレビジョン放送信号を受信再生し、HDTVコンテンツとして録画保存する。そしてステップS3でアクセスフラグを1にセットする。
- [0126] 続いてステップS4で再生要求を判別すると、ステップS5でアクセスフラグが1であれば、ステップS6に進み、保存しているHDTVコンテンツを読み出して再生出力を行う。アクセスフラグが0であった場合には、ステップS16でエラーメッセージを出力し

、再生出力は行わない。

- [0127] 続いてステップS7で転送要求を判別すると、ステップS8で転送先の機器との相互認証と鍵交換を行った後、ステップS9でHDTVコンテンツを転送先機器の低解像度例えばSDTV(標準テレビジョン)またはQVGAにトランスコーディングする。そしてステップS10でトランスコーディングした低解像度のコンテンツを暗号化して転送した後、ステップS11でアクセスフラグを0にリセットする。ステップS7で転送要求がなければ、ステップS8～S11はスキップする。
- [0128] 続いてステップS12で低解像度側からの転送要求を判別すると、ステップS13に進み、転送元との相互認証と鍵交換を行った後、コンテンツを伴わない転送処理を行う。そしてステップS14でアクセスフラグを1にセットしてHDTVコンテンツの再生を可能とする。このようなステップS1～S14の処理を、ステップS15で装置の停止指示があるまで繰り返す。
- [0129] 図14及び図15は、図10の低解像度装置における転送録画処理のフローチャートである。図14において、ステップS1で高解像度側からの転送要求を判別すると、ステップS2で暗号化コンテンツ例えばSDTVコンテンツを受信復号して保存し、ステップS3でアクセスフラグを1にセットする。
- [0130] ステップS4で再生要求を判別すると、ステップS5でアクセスフラグが1であることを条件に、ステップS6でSDTVコンテンツを読み出して再生出力を行う。アクセスフラグが0の場合にはステップS19に進み、エラーメッセージ出力を行って再生は行わない。
- [0131] ステップS7で低解像度側への転送要求を判別すると、ステップS8で転送先の機器との相互認証と鍵交換を行った後、ステップS9で保存コンテンツ(SDTV)を転送先の低解像度QVGAに変換し、ステップS10で変換したコンテンツを暗号化して転送し、ステップS11でアクセスフラグを0にリセットする。
- [0132] 続いて図15のステップS12で低解像度側からのコンテンツの転送要求があると、ステップS13に進み、転送元機器との相互認証と鍵交換を行って、コンテンツを伴わない転送処理を行った後、ステップS14でアクセスフラグを1にセットする。
- [0133] なおステップS7～S14の処理は、保存している放送コンテンツが最も低い解像度

であった場合には、それ以上のトランスコーディングはできないことから、ステップS7～S14の処理は行わない。

[0134] 次に図15のステップS15で高解像度側への転送要求を判別すると、ステップS16で転送先機器との相互認証と鍵交換を行って、コンテンツを伴わない転送処理を実行し、ステップS17でアクセスフラグを0にリセットする。このステップS1～S17の処理を、ステップS18で停止指示があるまで繰り返す。

[0135] 図16は本発明の放送コンテンツを転送する機器環境の他の実施形態の説明図であり、この実施形態にあつてはSDメモリを用いて放送コンテンツを機器間で転送するようにしている。

[0136] 図16において、高解像度装置100は、図9の場合と同様、HDTVチューナ110及び放送コンテンツ保存部112を備え、HDTVチューナ110で受信したHDTVコンテンツ114を保存している。

[0137] 一方、低解像度装置104はSDメモリ170のカードスロットに接続可能とした機器であり、高解像度装置100に保存しているHDTVコンテンツ114をQVGAコンテンツ122にトランスコーディングしてSDメモリ170に保存した後、このSDメモリ170を低解像度装置104のカードスロットに差し込んで転送保存することができる。

[0138] 図16の実施形態における高解像度装置100の機能構成は図10と同じであり、SDメモリ170に対する入出力アダプタを新たに備えている。また低解像度装置104についても図10と機能構成は同じであり、SDメモリ170の入出力アダプタを設けている点で異なるだけである。

[0139] 図17は本発明の放送コンテンツ管理処理が適用される他の機器環境のブロック図であり、この実施形態にあつては高解像度装置100、中解像度装置102及び低解像度装置104といった3つの機器間で放送コンテンツを転送する場合を例にとっている。

[0140] 図17において、高解像度装置100及び低解像度装置104は図8と同じである。また両者の間に中解像度装置102が設けられており、中解像度装置102としては例えばDVDレコーダなどの機器であり、DVD媒体116に高解像度装置100からトランスコーディングにより転送された中解像度のコンテンツとしてSDTVコンテンツ118を保

存している。

- [0141] SDTVコンテンツは標準テレビ放送コンテンツであり、NTSEテレビジョン放送信号やPALテレビジョン放送信号の解像度に対応している。この例では高解像度装置100はネットワーク106を介して中解像度装置102と接続し、中解像度装置102はネットワーク108を介して低解像度装置104と接続している。
- [0142] 更に図17の実施形態にあつては、放送コンテンツの再生を可能とするアクセスフラグに加え、放送コンテンツのコピー数の最大数を制限するダミーコンテンツ数を設定制御している。
- [0143] 図18は放送コンテンツのコピー数を制限するダミーコンテンツを管理する図17における高解像度装置100と中解像度装置102の機能構成のブロック図である。図18において、高解像度装置100は、通信制御部124、コンテンツ管理部126、HDTVチューナ110及び放送コンテンツ保存部112を備えている。
- [0144] コンテンツ管理部126には、アクセスフラグ設定部128、アクセスフラグ制御部134、コンテンツ再生部136及びコンテンツ転送部138が設けられており、基本的に図10の実施形態と同じである。これに加えて図18の実施形態にあつては、アクセスフラグ設定部128にダミーコンテンツ数132を設定している。
- [0145] ダミーコンテンツ数132の制御はダミーコンテンツ数の計数により実現される。ダミーコンテンツ数132は、図17においてオリジナルのHDTVコンテンツ114をトランスコーディングして中解像度装置102にSDTVコンテンツ118として保存し、更に中解像度装置102のSDTVコンテンツ118をトランスコーディングして低解像度装置104にQVGAコンテンツ122として保存した場合、3つの装置のうちのいずれか1つでアクセスフラグが1にセットされて再生可能となっており、残りの2つの装置ではアクセスフラグは0にリセットされて再生禁止されており、このアクセスフラグが0となって再生が禁止されているコンテンツの数をダミーコンテンツ数132は示している。
- [0146] 図18の中解像度装置102は、通信制御部142、コンテンツ管理部144及び放送コンテンツ保存部146を備える。コンテンツ管理部144にはアクセスフラグ設定部148、アクセスフラグ制御部154、コンテンツ再生部156、解像度変換部160を備えたコンテンツ転送部158が設けられている。

- [0147] この中解像度装置102の構成は基本的に図10に示した低解像度装置104の場合と同じであるが、新たにアクセスフラグ設定部148にダミーコンテンツ数152が設けられている。またコンテンツ転送部158の解像度変換部160としては、例えば図18に示すように、放送コンテンツ保存部146にSDTVコンテンツ118が保存されていることから、低解像度装置104にコンテンツを転送する際に、SDTVコンテンツ118をQVGAコンテンツ122にトランスコーディングすることになる。
- [0148] 図19、図20及び図21は、図17における放送コンテンツの解像度変換を伴う転送処理の説明図である。図19(A)は高解像度装置100においてHDTVコンテンツ114を受信録画した状態であり、このときアクセスフラグ130は1にセットされ、またダミーコンテンツ数132は0となっている。
- [0149] ダミーコンテンツ数132はアクセスフラグが1となっている装置以外の機器に保存しているコンテンツ数を示しており、この場合、中解像度装置102及び低解像度装置104のいずれにもトランスコーディングした同じ放送コンテンツは保存されていないことから、ダミーコンテンツ数132は0となっている。
- [0150] 次に図19(B)のように、高解像度装置100から中解像度装置102にコンテンツを転送する。この転送はHDTVコンテンツ114をSDTVコンテンツ118にトランスコーディングして転送することで保存し、転送元のアクセスフラグ130は0にリセットし、転送先のアクセスフラグ150を1にセットする。また転送先のダミーコンテンツ数152を1つカウントアップして1にする。
- [0151] このように高解像度側からのコンテンツの転送については、ダミーコンテンツ数は次式で求める。
- $$\begin{aligned}(\text{ダミーコンテンツ数}) &= (\text{転送元ダミーコンテンツ数}) + 1 \\ &= 0 + 1 = 1\end{aligned}$$
- [0152] 次に図20(C)のように、中解像度装置102から低解像度装置104にコンテンツを転送する。このコンテンツの転送は、中解像度装置102のSDTVコンテンツ118をQVGAコンテンツ122にトランスコーディングして転送することにより低解像度装置104に保存する。このコンテンツ転送により、転送元のアクセスフラグ150は0にリセットされ、転送先のアクセスフラグ164が1にセットされる。またダミーコンテンツ数は転送先

の低解像度装置104において

$$\begin{aligned}(\text{ダミーコンテンツ数}) &= (\text{転送元ダミーコンテンツ数}) + 1 \\ &= 1 + 1 = 2\end{aligned}$$

となる。

[0153] 次に図20(D)のように、低解像度装置104から中解像度装置102にコンテンツを戻す転送を説明する。低解像度装置104のQVGAコンテンツ122の高解像度となるSDTVコンテンツ118へのトランスコーディングは不可能であることから、コンテンツの転送は行わず、転送指示のメッセージのみを暗号化して中解像度装置102に転送する転送処理を行うことになる。

[0154] この実施形態にあつては、転送後に、転送元となる低解像度装置104のQVGAコンテンツ122、アクセスフラグ164及びダミーコンテンツ数166は消去するようにしている。高解像度側への転送により、転送先となった中解像度装置102にあつては、アクセスフラグ150を1にセットしてSDTVコンテンツ118の再生出力を可能とする。またダミーコンテンツ数152については次式で求める。

$$(\text{ダミーコンテンツ数}) = (\text{転送元コンテンツ数}) - 1$$

[0155] 図20(D)の場合には、

$$(\text{ダミーコンテンツ数}) = (\text{転送元コンテンツ数}) - 1 = 2 - 1 = 1$$

となる。

[0156] 図21は中解像度装置102から高解像度装置100にコンテンツを戻した場合の説明図である。この転送についても、コンテンツの実質的な転送は行わず、転送指示のみを転送する。また転送元となる中解像度装置102のSDTVコンテンツ118、アクセスフラグ150及びダミーコンテンツ数152は消去している。転送先となった高解像度装置100にあつては、アクセスフラグ130が1にセットされ、これによってHDTVコンテンツ114が再生可能となる。またダミーコンテンツ数132は

$$\begin{aligned}(\text{ダミーコンテンツ数}) &= (\text{転送元ダミーコンテンツ数}) - 1 \\ &= 1 - 1 = 0\end{aligned}$$

となる。

[0157] この図19乃至図21のコンテンツの機器間の転送で制御されるダミーコンテンツ数

については、コピー制限のための閾値を設定しておくことで、閾値を超えるコンテンツの転送保存を禁止することができる。例えばダミーコンテンツの閾値を閾値＝2に設定していると、図20(C)のように低解像度装置104に転送した際にダミーコンテンツ数166は2となり、更に別の装置に転送するとダミーコンテンツ数は3となって閾値を超えるため、コンテンツの転送保存を禁止することができる。

- [0158] これによってオリジナルのHDTVコンテンツ114からトランスコーディングされた低解像度の同じ放送内容のコンテンツが無制限に他の機器に実質的にコピーコンテンツとして保存されてしまうことを防止する。
- [0159] 図22は、図17における放送コンテンツの転送処理のタイムチャートである。図22において、高解像度装置100は、ステップS1でHDTVコンテンツを受信して録画保存し、ステップS2でアクセスフラグを1にセットし、ダミーコンテンツは0にセットする。
- [0160] ステップS3で転送要求を判別すると、ステップS4で低解像度のSDTVコンテンツにトランスコーディングした後、ステップS5で中解像度装置102との間で相互認証と鍵交換を行い、ステップS6でトランスコーディングしたSDTVコンテンツを暗号化して送信する。そしてステップS7でアクセスフラグを0にリセットする。
- [0161] 中解像度装置102にあっては、ステップS101で相互認証と鍵交換を行った後、ステップS102で暗号化SDTVコンテンツを受信復号して保存する。そしてステップS103でアクセスフラグを1にセットし、ダミーコンテンツ数は1にセットする。そしてステップS104でアクセスフラグが1であることを条件に、保存したSDTVコンテンツを再生することができる。
- [0162] 次に、ステップS105で低解像度装置104に対する転送要求を判別すると、ステップS106で低解像度のQVGAコンテンツにトランスコーディングした後、ステップS107で相互認証と鍵交換を行い、ステップS108でQVGAコンテンツを暗号化して送信し、ステップS109でアクセスフラグを0にリセットする。
- [0163] 低解像度装置104にあっては、ステップS201で相互認証と鍵交換を行った後、ステップS202で暗号化QVGAコンテンツを受信復号して保存した後、ステップS203でアクセスフラグを1にセットし、ダミーコンテンツ数は2にセットする。そしてステップS204でアクセスフラグが1であることを条件に、保存したQVGAコンテンツの再生を行

う。その後、低解像度装置104から中解像度装置102への戻し、中解像度装置102から高解像度装置100への戻しも、必要に応じて行われることになる。

- [0164] 図23は、図18の高解像度装置100における録画転送処理のフローチャートである。図23のステップS1〜S16の処理は、ダミーコンテンツ数を処理する以外は図13の画像転送処理と同じである。図23にあっては、ステップS3で録画保存後にダミーコンテンツ数を0にセットしている。またステップS14で低解像度側からの転送要求があった場合にダミーコンテンツ数を
- $$(\text{ダミーコンテンツ数}) = (\text{転送元ダミーコンテンツ数}) - 1$$
- としている点で相違しているだけである。

- [0165] 図24及び図25は、図18の中解像度装置102における録画転送処理のフローチャートである。この録画転送処理についても、図14に示した低解像度装置104における録画転送処理のフローチャートと基本的に同じであるが、ダミーコンテンツを求めている点と、ダミーコンテンツを閾値と比較して閾値を超えた場合に転送を禁止している点で相違している。

- [0166] また中解像度装置102にあっては、高解像度装置からトランスコーディングされたSDTVコンテンツを受信して保存し、更に低解像度装置104側に対しSDTVコンテンツをトランスコーディングしたQVGAコンテンツを転送するようにしている。

- [0167] 図24において、ステップS1で高解像度側から転送要求があると、ステップS2で暗号化コンテンツ即ちSDTVコンテンツを受信復号して保存し、ステップS3でアクセスフラグを1にセットし、ダミーコンテンツ数は転送元ダミーコンテンツ数に1を加えた値にセットする。

- [0168] ステップS4で再生要求があると、ステップS5でアクセスフラグが1であれば、ステップS6で保存したSDTVコンテンツを読み出して再生出力する。アクセスフラグが0であれば、ステップS20でエラーメッセージを出力し、再生は行わない。

- [0169] ステップS7で低解像度側への転送要求があると、ステップS8でダミーコンテンツ数が閾値に達したか否かチェックする。閾値未満であれば、ステップS9で転送先の機器との相互認証と鍵交換を行った後、ステップS10で、保存しているSDTVコンテンツを転送先の低解像度であるQVGAコンテンツにトランスコーディングした後、ステッ

プS11で暗号化して転送し、ステップS12でアクセスフラグを0にリセットする。ステップS8でダミーコンテンツ数が閾値に達していた場合には、コンテンツの転送処理は禁止され、ステップS21でエラーメッセージを出力して転送処理は行わない。

- [0170] ステップS13で低解像度側からのコンテンツの転送要求があると、ステップS14で転送元機器との相互認証と鍵交換を行って、コンテンツを伴わない転送処理を実行する。このコンテンツの戻りに対しては、ステップS15でアクセスフラグを1にセットした後、ダミーコンテンツ数は転送元のコンテンツから1を引いた値とする。
- [0171] 次に図25において、ステップS16で高解像度側への転送要求を判別すると、ステップS17で転送先機器との相互認証と鍵交換を行って、コンテンツを伴わない転送処理を実行する。そして、ステップS18でアクセスフラグを0にリセットする。このステップS18までの処理を、ステップS19で装置の停止指示があるまで繰り返す。
- [0172] なお図18の低解像度装置104における転送録画処理は、図24及び図25の中解像度装置102における転送録画処理と基本的に同じであり、ステップS2の受信復号する暗号化コンテンツがQVGAコンテンツである点が相違する。また低解像度側への転送については、保存しているQVGAコンテンツが最低解像度であれば、ステップS7〜S15, S21の処理は除くことになる。
- [0173] 図26は、図18の高解像度装置100、中解像度装置102及び低解像度装置104のそれぞれの処理で実行されるダミーコンテンツカウント処理をサブルーチンとして示したフローチャートである。図26において、ダミーコンテンツカウント処理は、ステップS1で高解像度側からの転送を判別すると、ステップS2で転送元ダミーコンテンツ数に1を加えた値をダミーコンテンツ数とする。またステップS3で低解像度側からの転送を判別した場合には、転送元ダミーコンテンツ数から1を引いた値をダミーコンテンツ数としている。
- [0174] 図27、図28及び図29は、高解像度側へ転送する際に低解像度側のコンテンツを残すようにした図18における放送コンテンツの解像度変換を伴う転送処理の説明図である。図27(A)は高解像度装置100にHDTVコンテンツ114を録画保存した状態であり、アクセスフラグ130は1、ダミーコンテンツ数132は0となっている。
- [0175] 図27(B)は高解像度装置100から中解像度装置102に転送した場合であり、HD

TVコンテンツ114をトランスコーディングして、SDTVコンテンツ118として中解像度装置102に保存している。この場合、転送元のアクセスフラグ130は0にリセットされ、転送先のアクセスフラグ150は1にセットされる。また転送先のダミーコンテンツ数は、転送元コンテンツ数に1を加えた値となる。

[0176] 即ち、高解像度側から低解像度側にコンテンツを転送する際のダミーコンテンツ数は、 $(\text{ダミーコンテンツ数}) = (\text{転送元ダミーコンテンツ数}) + 1$ となり、これは図19～図21に示した高解像度側への転送の際に低解像度側のコンテンツを消去する場合と同じである。

[0177] 図28(C)は中解像度装置102から低解像度装置104への転送であり、SDTVコンテンツ118をQVGAコンテンツ122にトランスコーディングして低解像度装置104に保存している。この場合、転送元のアクセスフラグ150は0にリセットされ、転送先のアクセスフラグ164が1にセットされる。また転送先のダミーコンテンツ数は2にセットされる。

[0178] 図28(D)は低解像度装置104から中解像度装置102にコンテンツを戻した場合の説明図である。高解像度側にコンテンツを戻す場合には、低解像度から高解像度へのトランスコーディングはできないことから、コンテンツの転送は行わず、転送指示のみを転送する。

[0179] この場合、転送元となる低解像度装置104についてQVGAコンテンツ122を残している。また転送元のアクセスフラグ164は0にリセットされ、転送先のアクセスフラグ150が1となる。またダミーコンテンツ数については、転送元のダミーコンテンツ数166は2であり、転送先のダミーコンテンツ数も2となっている。

[0180] 即ち、転送元となる低解像度側にコンテンツを残す場合のダミーコンテンツ数は $(\text{ダミーコンテンツ数}) = (\text{転送元ダミーコンテンツ数}) = 2$ とする。

[0181] 図29(D)は中解像度装置102から高解像度装置100にコンテンツを戻した場合であり、この場合にもコンテンツの転送は行わず、転送指示のみの転送となる。この場合、転送元のアクセスフラグ150は0にリセットされ、転送先のアクセスフラグ130が1にセットされる。また転送先のダミーコンテンツ数は、

(転送先のダミーコンテンツ数) = (転送元ダミーコンテンツ数) = 2
にセットされる。

[0182] この図27ー図29のように、コンテンツの転送を高解像度装置100から中解像度装置102、低解像度装置104と転送し、再び元に戻ってきた場合、図29(D)のように全ての装置におけるダミーコンテンツ数132, 152, 166の値が2となっている。

[0183] ここでダミーコンテンツ数の閾値を例えば「2」に設定した場合、図29(D)の装置以外にコンテンツを転送すると、転送先の装置においてダミーコンテンツ数は3となり、これは閾値を超えているためコンテンツの転送処理が禁止され、これ以上、他の機器にトランスコーディングしたコンテンツが保存されてしまうことを阻止できる。

[0184] 図30は図27乃至図29におけるダミーコンテンツカウント処理のフローチャートをサブルーチンとして示している。図30において、ステップS1で転送元ダミーカウント数が閾値未満であれば、ステップS2で高解像度側からの転送を判別すると、ステップS3で転送元ダミーコンテンツ数に1を加えた値をダミーコンテンツ数とする。またステップS4で低解像度側からの転送を判別した場合には、転送元ダミーコンテンツ数をそのままダミーコンテンツ数とする。

[0185] 一方、ステップS1で転送元ダミーコンテンツ数が閾値に達した場合には、ステップS2ーS4の処理はスキップし、ステップS5で転送元ダミーコンテンツ数をそのままダミーカウント数とする。

[0186] なお上記の実施形態にあつては、機器間で解像度を変化させるトランスコーディングをしてコンテンツを転送しているが、解像度を変えることなくコンテンツをそのまま転送するコピーについても、同様にアクセスフラグとダミーコンテンツ数を設定することで本発明のコンテンツ管理処理を適用することができる。

[0187] この場合にも、オリジナルのコピーが複数の機器に保存されていても、再生できるのはアクセスフラグが1にセットされた1つの機器のみであることから、コピーワンスによるコピー制御が維持できる。

[0188] (多重コーデック録画)

図31は、HDTVコンテンツを多重コーデックにより受信録画する装置の機能構成のブロック図である。図31において、録画装置300は、HDTVチューナ302、MPE

G2のHDTVコーデック304、H. 264のQVGAコーデック306、アクセスフラグ制御部308、310、放送コンテンツ保存部312及びコンテンツ再生部322を備えている。

[0189] HDTVコーデック304とQVGAコーデック306は、HDTVチューナ202によりコピーワンスのコピー制御条件の下に受信されたHDTV放送信号をMPEG2及びH. 264のそれぞれのコーデック方式により並列的に復号し、放送コンテンツ保存部312にHDTVコンテンツ314及びQVGAコンテンツ318として保存する。

[0190] アクセスフラグ制御部308、310は、HDTVコンテンツ314及びQVGAコンテンツ318に対し、それぞれアクセスフラグ316、320を設定し、例えばデフォルトで設定されたHDTVコンテンツ314のアクセスフラグ316を1にセットすることで再生可能とし、QVGAコンテンツ318についてはアクセスフラグ320を0にリセットすることで再生を禁止状態としている。

[0191] このデフォルトのアクセスフラグ316、320の設定状態は、ユーザが必要に応じて再生したいコンテンツの選択に応じて切り替わる。例えばデフォルトの保存状態についてユーザがQVGAコンテンツ318の再生を指示すると、そのアクセスフラグ320が1にセットされ、HDTVコンテンツ314のアクセスフラグ316が0にリセットされ、コンテンツ再生部322はアクセスフラグが1となった側のコンテンツを再生出力することになる。

[0192] これによって録画装置300がHDTVコーデック304とQVGAコーデック306という2つのコーデックを備えることで、同じHDTV受信放送を二重に復号して2つのコンテンツを保存しても、いずれか一方のアクセスフラグが1、残りのアクセスフラグが0となり、アクセスフラグが1となった1つの放送コンテンツしか再生できないため、多重コーデックによる複数コンテンツの保存であっても、コピーワンスによるコピー制御の制約条件を維持することができる。

[0193] 図32は、図31の多重コーデック処理のフローチャートである。図31において、ステップS1で録画要求があると、ステップS2で指定コーデックのアクセスフラグを1にセットし、残りを0にリセットする。続いてステップS3で多重コーデックの録画保存処理を行う。ステップS4で再生要求があれば、ステップS5でアクセスフラグをチェックし、アクセスフラグが1であれば、ステップS7で録画コンテンツの再生を行う。

- [0194] アクセスフラグが1でなかった場合には、ステップS6で対応するアクセスフラグを1にセットし、残りを0にリセットした後、ステップS7でアクセスフラグを1にセットした録画コンテンツを再生する。このステップS1〜S7の処理を、ステップS8で装置の停止指示があるまで繰り返すことになる。
- [0195] なお図31にあつては、録画装置300に2台のコーデックを設けて二重コーデック録画する場合を例にとっているが、3以上のコーデックを設けた場合についても同様に適用できる。
- [0196] 更に本発明の放送コンテンツの暗号化復号を含む処理を行う機器の処理部分については、耐タンパー処理機能を持ったハードウェアモジュールまたはソフトウェアを使用することで、不正アクセスに対する保護を図っている。
- [0197] また機器間の通信についても、例えばパーソナルコンピュータに対しDVD装置をDTCPポートで接続するような場合にはIEEE1394やDTTPCなどの暗号化通信を使用し、また機器間をLANで接続している場合にはSSLやIPsecなどのプロトコルで暗号化通信を行っている。
- [0198] なお本発明は上記の実施形態に限定されず、その目的と利点を損なうことのない適宜の変形を含み、更に上記の実施形態に示した数値による限定は受けない。

請求の範囲

- [1] ネットワークを介して他の機器と接続された装置のコンピュータに、
コンテンツを受信した装置でのコピーを禁止するような著作権の利用条件とした暗号化コンテンツとその暗号鍵をコンテンツ保存部に保存するコンテンツ保存ステップと、
前記暗号鍵により前記暗号化コンテンツを復号する復号ステップと、
他の機器との間で前記ネットワークを介して暗号化コンテンツをコピー転送するコンテンツコピーステップと、
他の機器との間で前記ネットワークを介して暗号鍵を転送する暗号鍵転送ステップと、を実行させることを特徴とするコンテンツ管理プログラム。
- [2] 請求の範囲1のコンテンツ管理プログラムに於いて、
前記暗号鍵転送ステップは、前記コンテンツ保存部の暗号鍵をネットワークを介して他の機器にコピー転送した後に保存している暗号鍵を消去することを特徴とするコンテンツ管理プログラム。
- [3] 請求の範囲1のコンテンツ管理プログラムに於いて、
前記暗号鍵転送ステップは、コンテンツ毎に前記暗号鍵を保存している機器を暗号鍵管理テーブルに登録し、
前記復号ステップは、前記暗号化コンテンツを復号する際に、前記管理テーブルから認識した暗号鍵を保存している機器に対する転送要求により前記暗号鍵を取得して前記暗号化コンテンツを復号することを特徴とするコンテンツ管理プログラム。
- [4] 請求の範囲1のコンテンツ管理プログラムに於いて、前記暗号鍵転送ステップは、
前記暗号鍵を他の機器に転送した際に、自己の暗号鍵管理テーブルを更新すると共に他の機器に転送情報を通知して暗号鍵管理テーブルを更新させることを特徴とするコンテンツ管理プログラム。
- [5] 請求の範囲1のコンテンツ管理プログラムに於いて、ネットワークを介して接続された機器は、機器管理テーブルに登録された同一ユーザの保有する機器であることを特徴とするコンテンツ管理プログラム。
- [6] 請求の範囲5のコンテンツ管理プログラムに於いて、ネットワークを介して接続され

た機器は、前記機器管理テーブルに登録された他のユーザの保有する機器を含むことを特徴とするコンテンツ管理プログラム。

- [7] 請求の範囲1のコンテンツ管理プログラムに於いて、前記暗号化コンテンツは、著作権を有する音楽、映像、ドキュメントのいずれか、もしくはそれらの組合せであることを特徴とするコンテンツ管理プログラム。
- [8] ネットワークを介して他の機器と接続された装置のコンテンツ管理方法に於いて、コンテンツを受信した装置でのコピーを禁止するような著作権の利用条件とした暗号化コンテンツとその暗号鍵をコンテンツ保存部に保存するコンテンツ保存ステップと、
前記暗号鍵により前記暗号化コンテンツを復号する復号ステップと、
他の機器との間で前記ネットワークを介して暗号化コンテンツをコピー転送するコンテンツコピーステップと、
他の機器との間で前記ネットワークを介して暗号鍵を転送する暗号鍵転送ステップと、を備えたことを特徴とするコンテンツ管理方法。
- [9] 請求の範囲8のコンテンツ管理方法に於いて、
前記暗号鍵転送ステップは、前記コンテンツ保存部の暗号鍵をネットワークを介して他の機器にコピー転送した後に保存している暗号鍵を消去することを特徴とするコンテンツ管理方法。
- [10] 請求の範囲8のコンテンツ管理方法に於いて、
前記暗号鍵転送ステップは、コンテンツ毎に前記暗号鍵を保存している機器を暗号鍵管理テーブルに登録し、
前記復号ステップは、前記暗号化コンテンツを復号する際に、前記管理テーブルから認識した暗号鍵を保存している機器に対する転送要求により前記暗号鍵を取得して前記暗号化コンテンツを復号することを特徴とするコンテンツ管理方法。
- [11] 請求の範囲8のコンテンツ管理方法に於いて、前記暗号鍵転送ステップは、前記暗号鍵を他の機器に転送した際に、自己の暗号鍵管理テーブルを更新すると共に他の機器に転送情報を通知して暗号鍵管理テーブルを更新させることを特徴とするコンテンツ管理方法。

- [12] 請求の範囲8のコンテンツ管理方法に於いて、ネットワークを介して接続された機器は、機器管理テーブルに登録された同一ユーザの保有する機器であることを特徴とするコンテンツ管理方法。
- [13] 請求の範囲12のコンテンツ管理方法に於いて、ネットワークを介して接続された機器は、前記機器管理テーブルに登録された他のユーザの保有する機器を含むことを特徴とするコンテンツ管理方法。
- [14] ネットワークを介して他の機器と接続されたコンテンツ管理装置に於いて、
コンテンツを受信した装置でのコピーを禁止するような著作権の利用条件とした暗号化コンテンツとその暗号鍵を保存するコンテンツ保存部と、
前記暗号鍵により前記暗号化コンテンツを復号する復号部と、
他の機器との間で前記ネットワークを介して暗号化コンテンツをコピー転送するコンテンツコピー部と、
他の機器との間で前記ネットワークを介して暗号鍵を転送する暗号鍵転送部と、
を備えたことを特徴とするコンテンツ管理装置。
- [15] 請求の範囲14のコンテンツ管理装置に於いて、
前記暗号鍵転送部は、前記コンテンツ保存部の暗号鍵をネットワークを介して他の機器にコピー転送した後に前記コンテンツ保存部の暗号鍵を消去することを特徴とするコンテンツ管理装置。
- [16] 請求の範囲14のコンテンツ管理装置に於いて、
前記暗号鍵転送部は、コンテンツ毎に前記暗号鍵を保存している機器を暗号鍵管理テーブルに登録し、
前記復号部は、前記暗号化コンテンツを復号する際に、前記管理テーブルから認識した暗号鍵を保存している機器に対する転送要求により前記暗号鍵を取得して前記暗号化コンテンツを復号することを特徴とするコンテンツ管理装置。
- [17] 請求の範囲14のコンテンツ管理装置に於いて、前記暗号鍵転送部は、前記暗号鍵を他の機器に転送した際に、自己の暗号鍵管理テーブルを更新すると共に他の機器に転送情報を通知して暗号鍵管理テーブルを更新させることを動要求により前記暗号鍵を取得して前記暗号化コンテンツを復号することを特徴とするコンテンツ管

理装置。

- [18] 請求の範囲14のコンテンツ管理装置に於いて、ネットワークを介して接続された機器は、機器管理テーブルに登録された同一ユーザの保有する機器であることを特徴とするコンテンツ管理装置。
- [19] 請求の範囲14のコンテンツ管理装置に於いて、ネットワークを介して接続された機器は、前記機器管理テーブルに登録された他のユーザの保有する機器を含むことを特徴とするコンテンツ管理装置。
- [20] コンピュータに、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の可否を制御するアクセス情報を設定するアクセス情報設定ステップと、
前記アクセス情報が再生可を示している場合に前記コンテンツを再生し、前記アクセス情報が再生不可を示している場合は前記コンテンツの再生を禁止するコンテンツ再生ステップと、
前記コンテンツ保存部に保存されたコンテンツの解像度を変換して該変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、
コンテンツを前記コンテンツ保存部に保存した際に前記アクセス情報を再生可に設定し、前記変換後のコンテンツを他の機器に転送した際に前記アクセス情報を再生不可に設定して再生を禁止し、更に前記他の機器に転送された前記変換後のコンテンツが再生不可になった場合に前記アクセス情報を再生可に設定して再生可能とするアクセス情報制御ステップと、
を実行させることを特徴とするコンテンツ管理プログラム。
- [21] 請求の範囲20のコンテンツ管理プログラムに於いて、前記コンピュータに、更に、前記アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミーコンテンツ数を設け、前記ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止するダミーコンテンツ制限ステップを実行させることを特徴とするコンテンツ管理プログラム。
- [22] 請求の範囲20のコンテンツ管理プログラムに於いて、前記コンテンツ転送ステップは、前記コンテンツ保存部に保存されたコンテンツを転送先の機器に対応した低解

像度のコンテンツに変換して変換後のコンテンツを転送することを特徴とするコンテンツ管理プログラム。

- [23] コンピュータに、
コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の有無を制御するアクセス情報を設定するアクセス情報設定ステップと、
前記アクセス情報が再生可を示している場合に前記コンテンツを再生し、前記アクセス情報が再生不可を示している場合は前記コンテンツの再生を禁止するコンテンツ再生ステップと、
前記コンテンツ保存部に保存されたコンテンツの解像度を変換して該変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、
他の機器から転送してきたコンテンツを前記コンテンツ保存部に保存した際に前記アクセス情報を再生可に設定して再生可能とし、前記コンテンツを別の他の機器に転送した際に前記アクセス情報を再生不可に設定して再生を禁止するアクセス情報制御ステップと、を実行させることを特徴とするコンテンツ管理プログラム。
- [24] 請求の範囲23のコンテンツ管理プログラムに於いて、前記コンピュータに、更に、前記アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミーコンテンツ数を設け、前記ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止させるダミーコンテンツ制限ステップを実行させることを特徴とするコンテンツ管理プログラム。
- [25] 請求の範囲23のコンテンツ管理プログラムに於いて、前記コンテンツ転送ステップは、前記コンテンツ保存部に保存されたコンテンツの解像度を転送先の機器に対応した低解像度のコンテンツに変換して転送し、前記コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、コンテンツを含まない転送処理を実行することを特徴とするコンテンツ管理プログラム。
- [26] 請求の範囲23のコンテンツ管理プログラムに於いて、前記コンテンツ転送ステップは、前記コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、保存しているコンテンツをそのまま残すか又は

消去することを特徴とするコンテンツ管理プログラム。

- [27] 請求の範囲20又23のコンテンツ管理プログラムに於いて、前記コンテンツ転送ステップは、前記コンテンツをネットワーク接続又は着脱自在な記憶媒体を介して他の機器に転送することを特徴とするコンテンツ管理プログラム。
- [28] 請求の範囲20又は23のコンテンツ管理プログラムに於いて、他の機器で変換後のコンテンツが再生不可となる場合は、該変換後のコンテンツが戻されることを特徴とするコンテンツ管理プログラム。
- [29] コンピュータに、
信号を受信して並列的に同じコンテンツを再生する複数のコーデックステップと
前記複数のコーデックステップで並列的に再生された複数の同じコンテンツをコンテンツ保存部に保存するコンテンツ保存ステップと、
前記コンテンツ保存部に保存された同じコンテンツ毎に設定されたアクセス情報の何れか1つをオンして対応するコンテンツを再生可能とすると共に、残りのアクセス情報を全てオフして対応するコンテンツの再生を禁止するフラグ制御ステップと、
前記複数の同じコンテンツの中でアクセス情報がオンしている前記コンテンツを選択して再生するコンテンツ再生ステップと、
を実行させることを特徴とするコンテンツ管理プログラム。
- [30] 請求の範囲20、23又は29のコンテンツ管理プログラムに於いて、前記コンテンツは、1回限りのコピーを著作権の利用条件として受信されたテレビジョン放送信号であることを特徴とするコンテンツ管理プログラム。
- [31] コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の可否を制御するアクセス情報を設定するアクセス情報設定ステップと、
前記アクセス情報が再生可を示している場合に前記コンテンツを再生し、前記アクセス情報が再生不可を示している場合は前記コンテンツの再生を禁止するコンテンツ再生ステップと、
前記コンテンツ保存部に保存されたコンテンツの解像度を変換して該変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、

コンテンツを前記コンテンツ保存部に保存した際に前記アクセス情報を再生可に設定し、前記変換後のコンテンツを他の機器に転送した際に前記アクセス情報を再生不可に設定して再生を禁止し、更に前記他の機器に転送された前記変換後のコンテンツが再生不可になった場合に前記アクセス情報を再生可に設定して再生可能とするアクセス情報制御ステップと、
を備えたことを特徴とするコンテンツ管理方法。

[32] 請求の範囲31のコンテンツ管理方法に於いて、更に、前記アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミーコンテンツ数を設け、前記ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止するダミーコンテンツ制限ステップを実行させることを特徴とするコンテンツ管理方法。

[33] 請求の範囲31のコンテンツ管理方法に於いて、前記コンテンツ転送ステップは、前記コンテンツ保存部に保存されたコンテンツを転送先の機器に対応した低解像度のコンテンツに変換して変換後のコンテンツを転送することを特徴とするコンテンツ管理方法。

[34] コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の有無を制御するアクセス情報を設定するアクセス情報設定ステップと、

前記アクセス情報が再生可を示している場合に前記コンテンツを再生し、前記アクセス情報が再生不可を示している場合は前記コンテンツの再生を禁止するコンテンツ再生ステップと、

前記コンテンツ保存部に保存されたコンテンツの解像度を変換して該変換後のコンテンツを他の機器に転送するコンテンツ転送ステップと、

他の機器から転送してきたコンテンツを前記コンテンツ保存部に保存した際に前記アクセス情報を再生可に設定して再生可能とし、前記コンテンツを別の他の機器に転送した際に前記アクセス情報を再生不可に設定して再生を禁止するアクセス情報制御ステップと、を備えたことを特徴とするコンテンツ管理方法。

[35] 請求の範囲34のコンテンツ管理方法に於いて、更に、前記アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミ

ーコンテンツ数を設け、前記ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止させるダミーコンテンツ制限ステップを実行させることを特徴とするコンテンツ管理方法。

[36] 請求の範囲34のコンテンツ管理方法に於いて、前記コンテンツ転送ステップは、前記コンテンツ保存部に保存されたコンテンツの解像度を転送先の機器に対応した低解像度のコンテンツに変換して転送し、前記コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、コンテンツを含まない転送処理を実行することを特徴とするコンテンツ管理方法。

[37] 請求の範囲34のコンテンツ管理方法に於いて、前記コンテンツ転送ステップは、前記コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、保存しているコンテンツをそのまま残すか又は消去することを特徴とするコンテンツ管理方法。

[38] 請求の範囲31又34のコンテンツ管理方法に於いて、前記コンテンツ転送ステップは、前記コンテンツをネットワーク接続又は着脱自在な記憶媒体を介して他の機器に転送することを特徴とするコンテンツ管理方法。

[39] 請求の範囲31又は34のコンテンツ管理方法に於いて、他の機器で変換後のコンテンツが再生不可となる場合は、該変換後のコンテンツが戻されることを特徴とするコンテンツ管理方法。

[40] 信号を受信して並列的に同じコンテンツを再生する複数のコーデックステップと前記複数のコーデックステップで並列的に再生された複数の同じコンテンツをコンテンツ保存部に保存するコンテンツ保存ステップと、

前記コンテンツ保存部に保存された同じコンテンツ毎に設定されたアクセス情報の何れか1つをオンして対応するコンテンツを再生可能とすると共に、残りのアクセス情報を全てオフして対応するコンテンツの再生を禁止するフラグ制御ステップと、

前記複数の同じコンテンツの中でアクセス情報がオンしている前記コンテンツを選択して再生するコンテンツ再生ステップと、
を備えたことを特徴とするコンテンツ管理方法。

- [41] 請求の範囲31、34又は40のコンテンツ管理方法に於いて、前記コンテンツは、1回限りのコピーを著作権の利用条件として受信されたテレビジョン放送信号であることを特徴とするコンテンツ管理方法。
- [42] コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の可否を制御するアクセス情報を設定するアクセス情報設定部と、
前記アクセス情報が再生可を示している場合に前記コンテンツを再生し、前記アクセス情報が再生不可を示している場合は前記コンテンツの再生を禁止するコンテンツ再生部と、
前記コンテンツ保存部に保存されたコンテンツの解像度を変換して該変換後のコンテンツを他の機器に転送するコンテンツ転送部と、
コンテンツを前記コンテンツ保存部に保存した際に前記アクセス情報を再生可に設定し、前記変換後のコンテンツを他の機器に転送した際に前記アクセス情報を再生不可に設定して再生を禁止し、更に前記他の機器に転送された前記変換後のコンテンツが再生不可になった場合に前記アクセス情報を再生可に設定して再生可能とするアクセス情報制御部と、
を備えたことを特徴とするコンテンツ管理装置。
- [43] 請求の範囲42のコンテンツ管理装置に於いて、更に、前記アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミーコンテンツ数を設け、前記ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止するダミーコンテンツ制限部を備えたことを特徴とするコンテンツ管理装置。
- [44] 請求の範囲42のコンテンツ管理装置に於いて、前記コンテンツ転送部は、前記コンテンツ保存部に保存されたコンテンツを転送先の機器に対応した低解像度のコンテンツに変換して変換後のコンテンツを転送することを特徴とするコンテンツ管理装置。
- [45] コンテンツ保存部に保存されたコンテンツ毎に、コンテンツの再生の有無を制御するアクセス情報を設定するアクセス情報設定部と、
前記アクセス情報が再生可を示している場合に前記コンテンツを再生し、前記アク

セス情報が再生不可を示している場合は前記コンテンツの再生を禁止するコンテンツ再生部と、

前記コンテンツ保存部に保存されたコンテンツの解像度を変換して該変換後のコンテンツを他の機器に転送するコンテンツ転送部と、

他の機器から転送してきたコンテンツを前記コンテンツ保存部に保存した際に前記アクセス情報を再生可に設定して再生可能とし、前記コンテンツを別の他の機器に転送した際に前記アクセス情報を再生不可に設定して再生を禁止するアクセス情報制御部と、

を備えたことを特徴とするコンテンツ管理装置。

[46] 請求の範囲45のコンテンツ管理装置に於いて、更に、前記アクセス情報を再生不可に設定した再生禁止状態で他の機器に保存されているコンテンツの数を示すダミーコンテンツ数を設け、前記ダミーコンテンツカウンタの値が所定閾値に達した場合に他の機器への転送処理を禁止させるダミーコンテンツ制限部を備えたことを特徴とするコンテンツ管理装置。

[47] 請求の範囲45のコンテンツ管理装置に於いて、前記コンテンツ転送部は、前記コンテンツ保存部に保存されたコンテンツの解像度を転送先の機器に対応した低解像度のコンテンツに変換して転送し、前記コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、コンテンツを含まない転送処理を実行することを特徴とするコンテンツ管理装置。

[48] 請求の範囲45のコンテンツ管理装置に於いて、前記コンテンツ転送部は、前記コンテンツ保存部に保存しているコンテンツを高解像度のコンテンツを保存している転送元の機器に戻す場合は、保存しているコンテンツをそのまま残すか又は消去することを特徴とするコンテンツ管理装置。

[49] 請求の範囲42又45のコンテンツ管理装置に於いて、前記コンテンツ転送部は、前記コンテンツをネットワーク接続又は着脱自在な記憶媒体を介して他の機器に転送することを特徴とするコンテンツ管理装置。

[50] 請求の範囲42又は45のコンテンツ管理装置に於いて、他の機器で変換後のコンテンツが再生不可となる場合は、該変換後のコンテンツが戻されることを特徴とするコ

ンテンツ管理装置。

- [51] 信号を受信して並列的に同じコンテンツを再生する複数のコーデックステップと
前記複数のコーデックステップで並列的に再生された複数の同じコンテンツを保存
するコンテンツ保存部と、

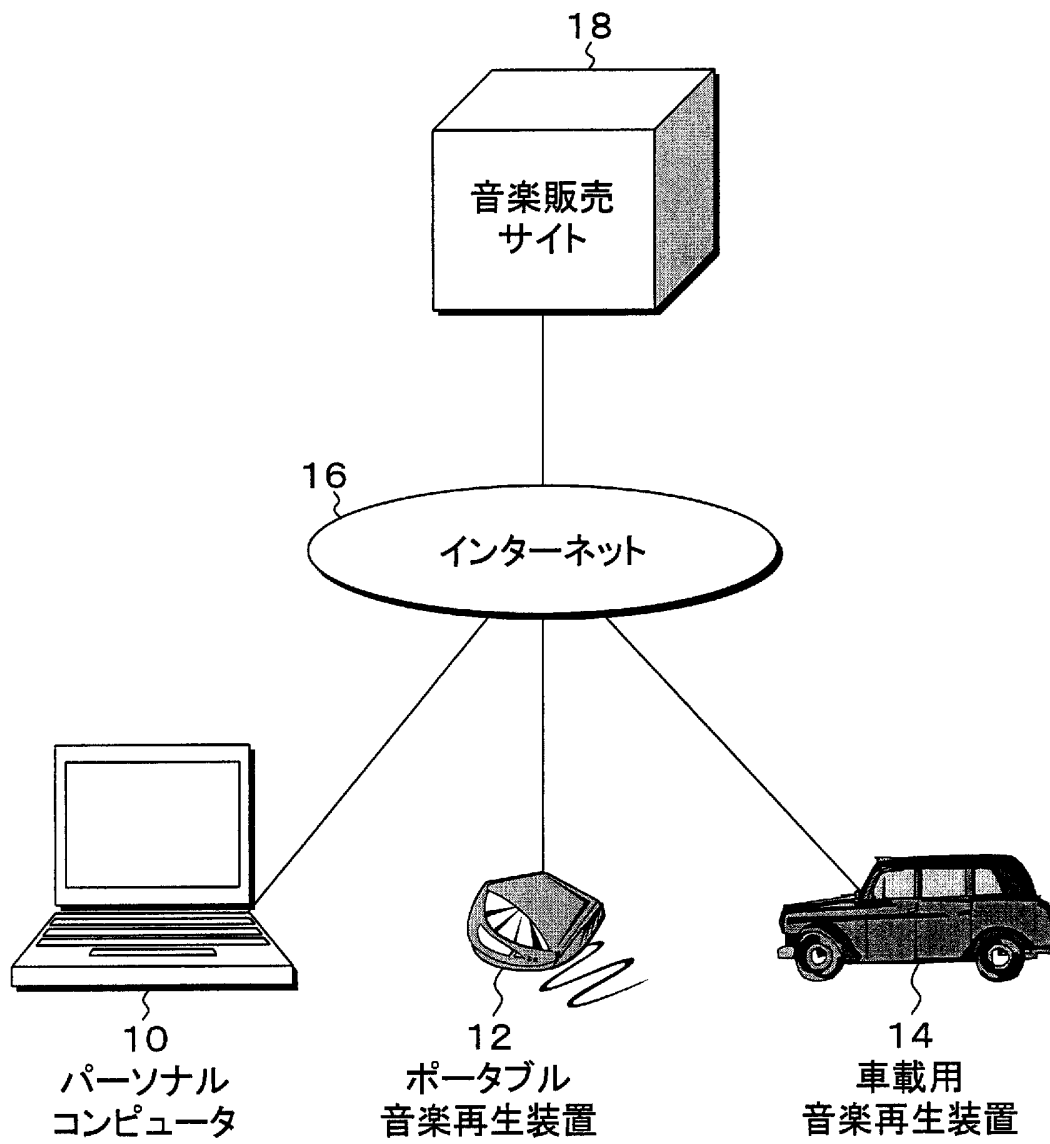
前記コンテンツ保存部に保存された同じコンテンツ毎に設定されたアクセス情報の
何れか1つをオンして対応するコンテンツを再生可能とすると共に、残りのアクセス情
報を全てオフして対応するコンテンツの再生を禁止するフラグ制御部と、

前記複数の同じコンテンツの中でアクセス情報がオンしている前記コンテンツを選
択して再生するコンテンツ再生部と、

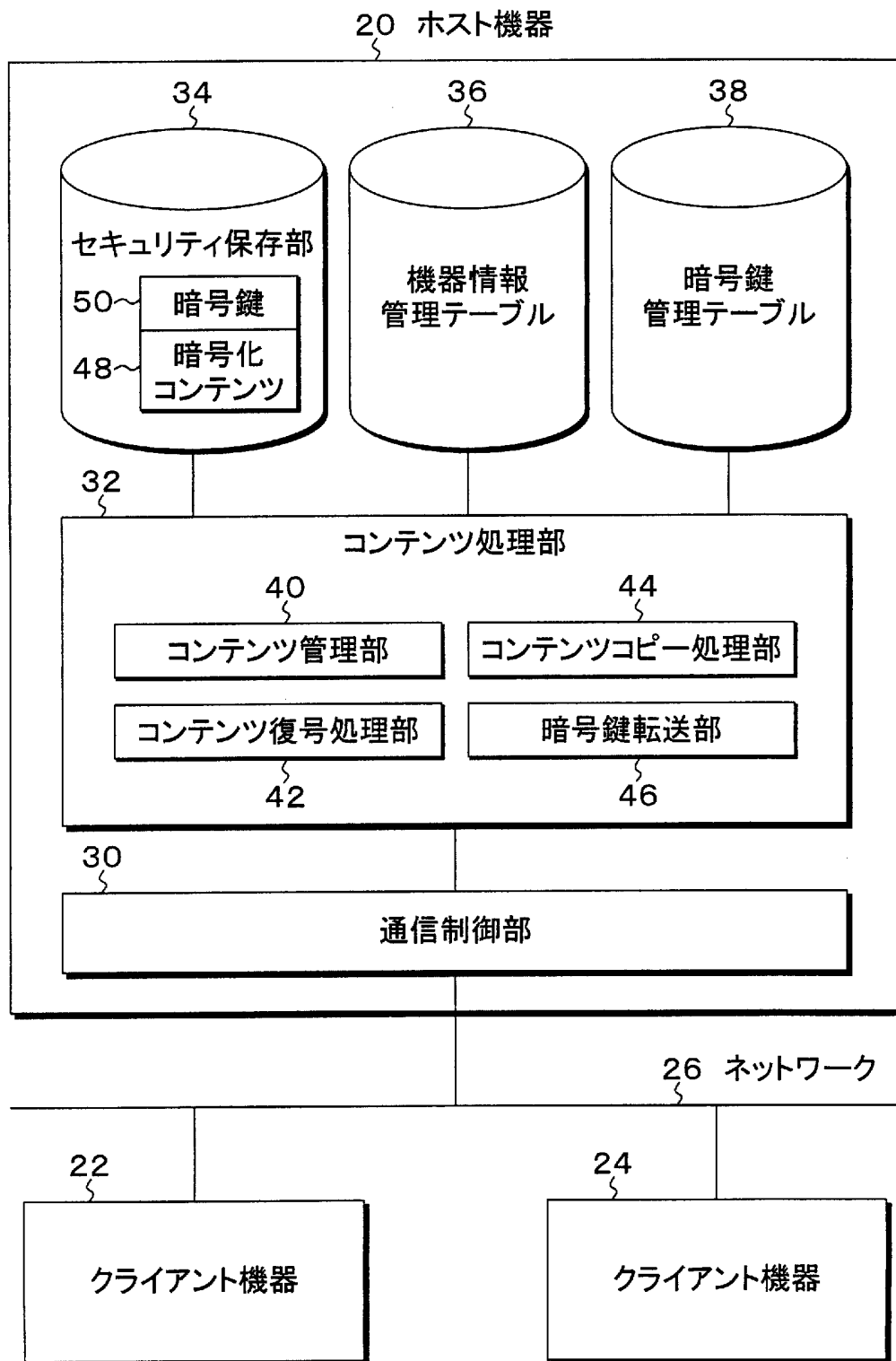
を備えたことを特徴とするコンテンツ管理装置。

- [52] 請求の範囲42、45又は51のコンテンツ管理装置に於いて、前記コンテンツは、1
回限りのコピーを著作権の利用条件として受信されたテレビジョン放送信号であるこ
とを特徴とするコンテンツ管理装置。

[図1]



[図2]



[図3]

36 機器情報テーブル

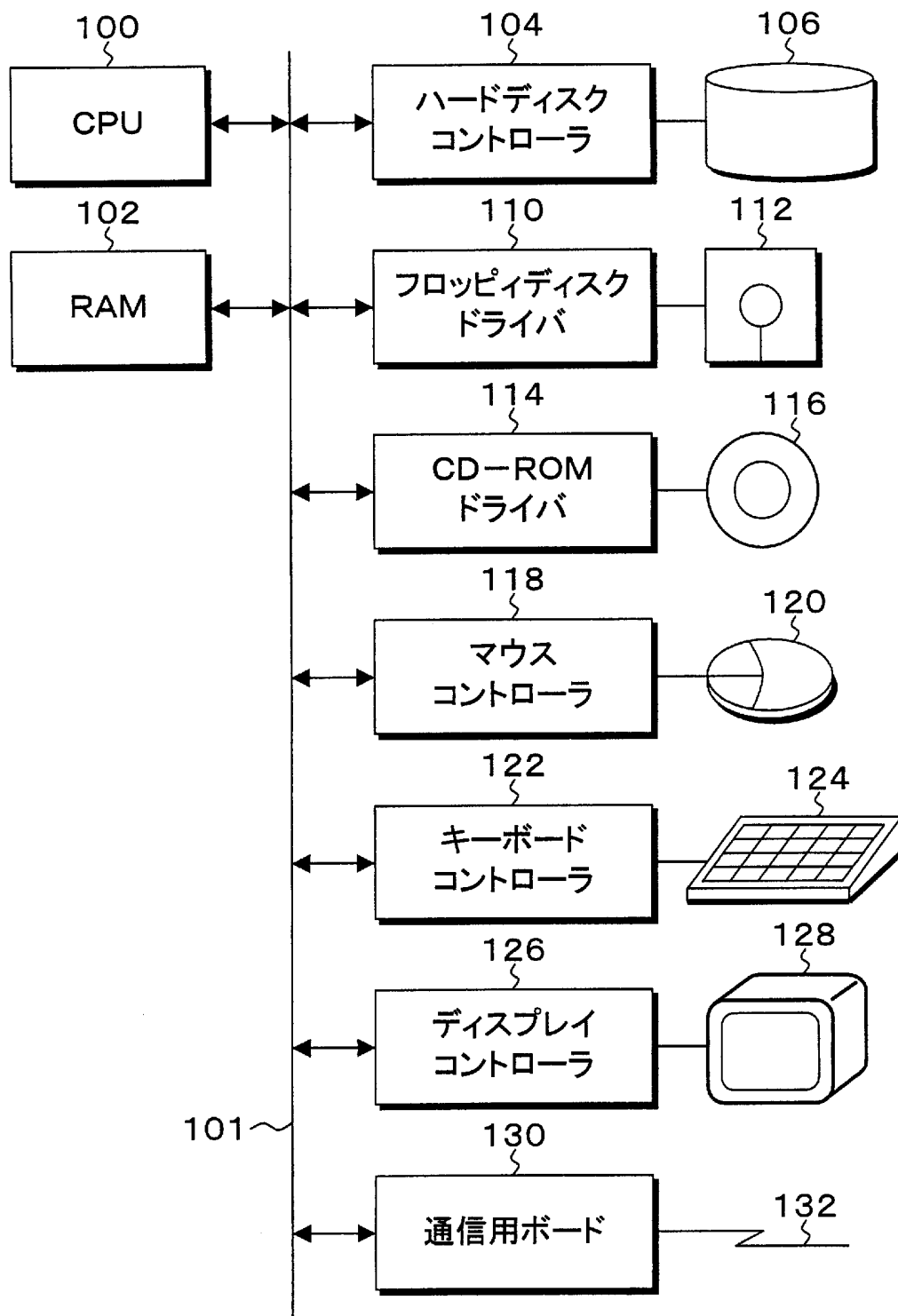
機器名	ネットワーク上の位置
機器20	アドレスa
機器22	アドレスb
機器24	アドレスc

[図4]

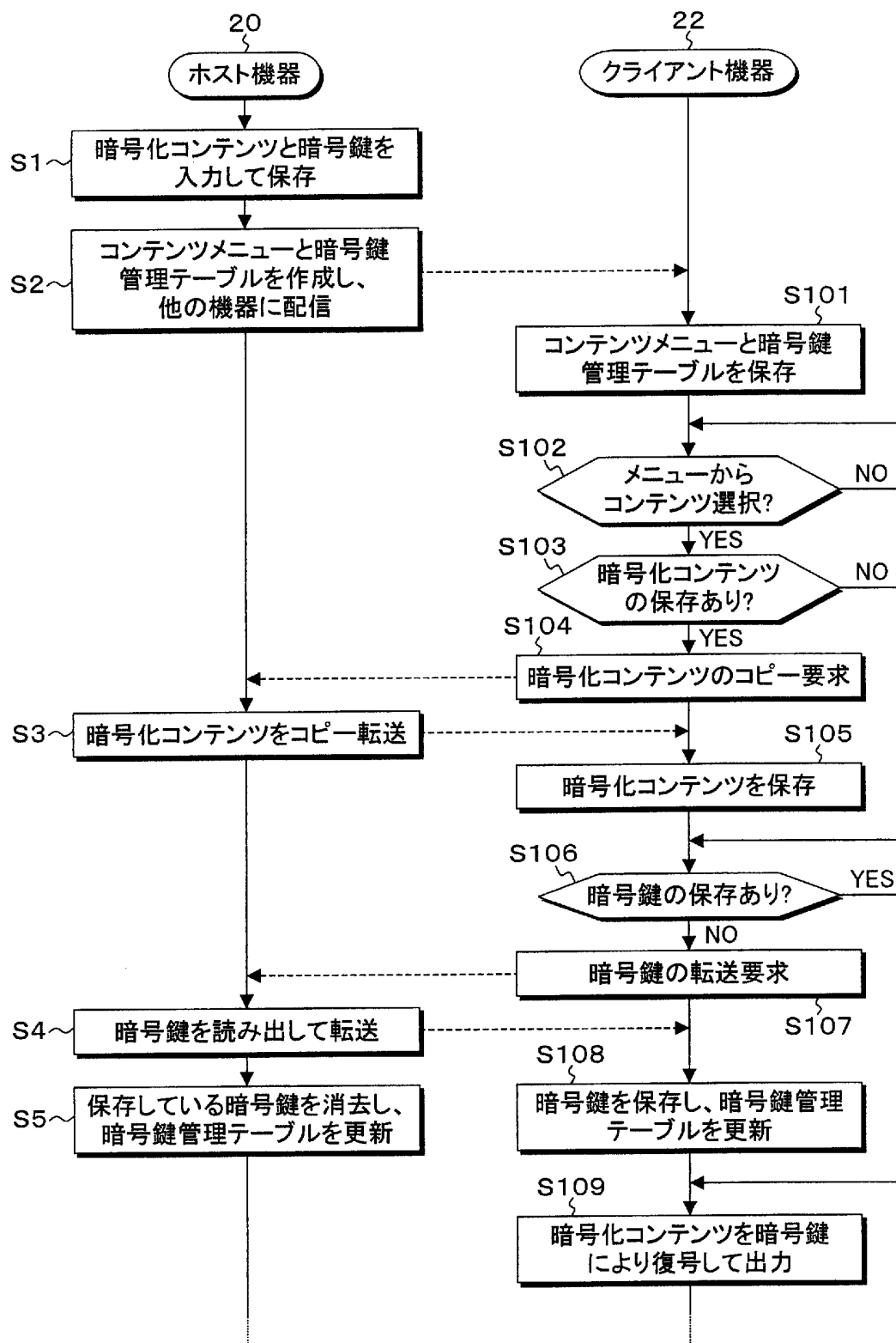
38 暗号鍵管理テーブル

コンテンツ名	鍵の保存機器名	暗号化方式
コンテンツA	機器20	α
コンテンツB	機器22	α
コンテンツC	機器24	β

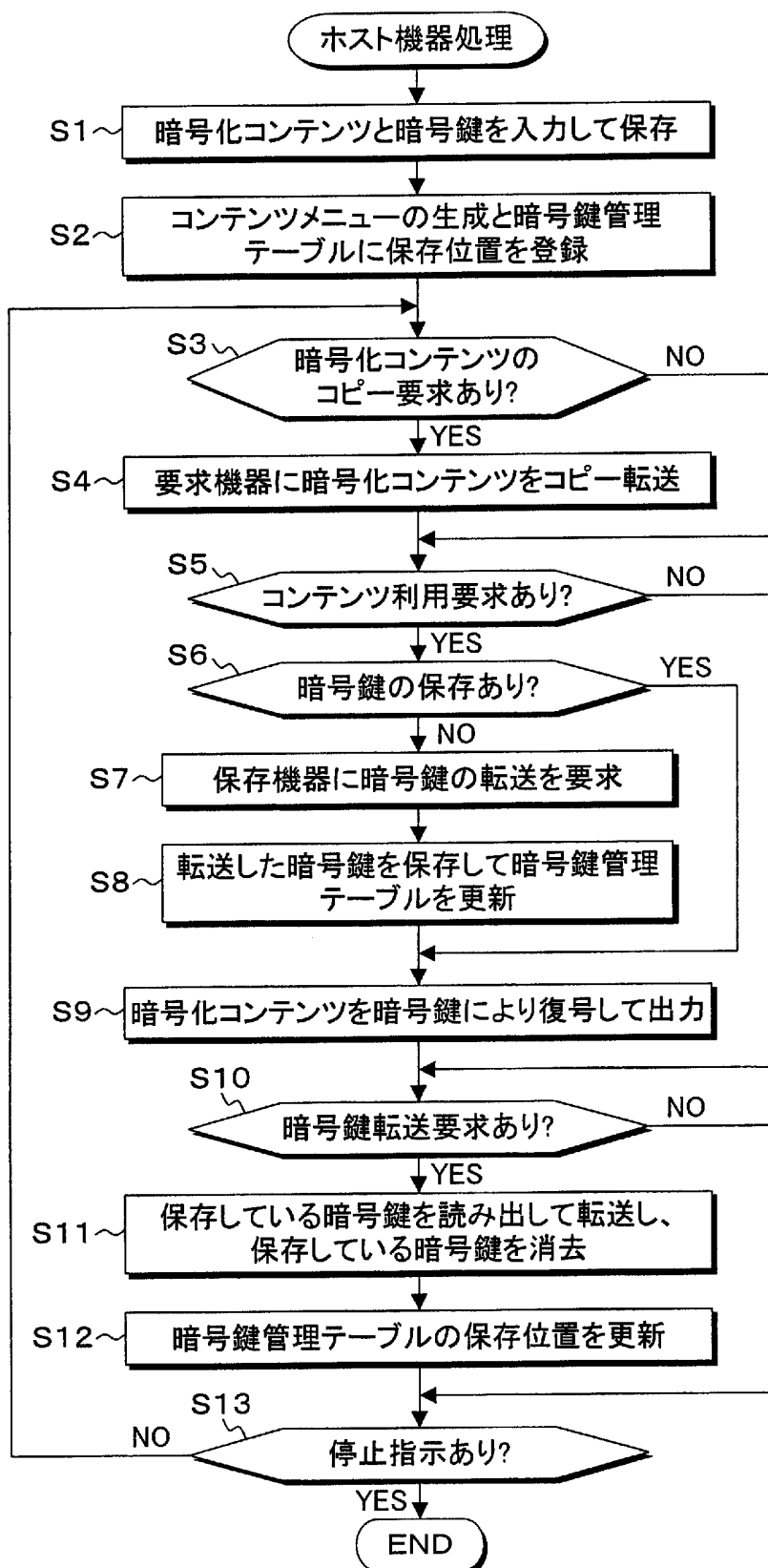
[図5]



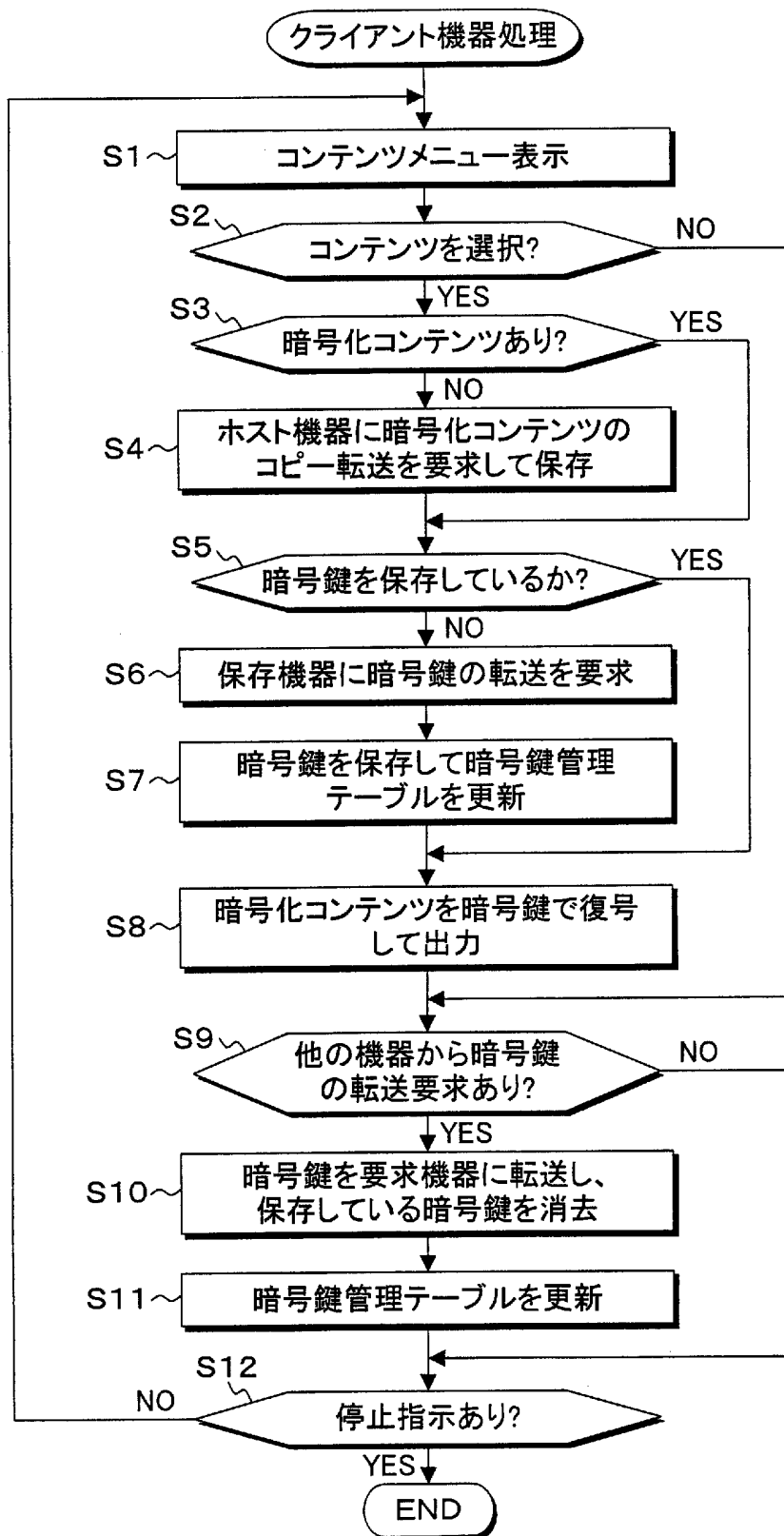
[図6]



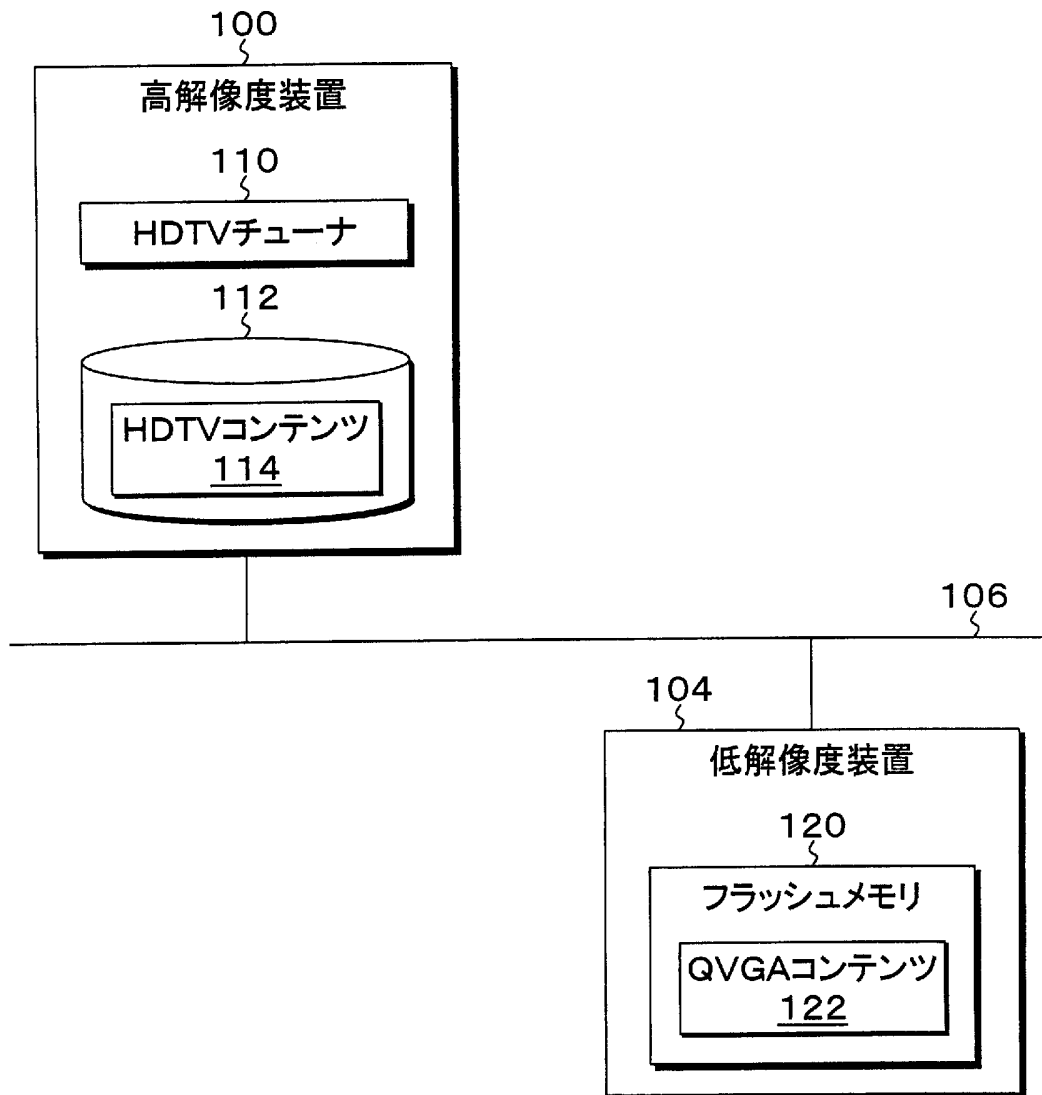
[図7]



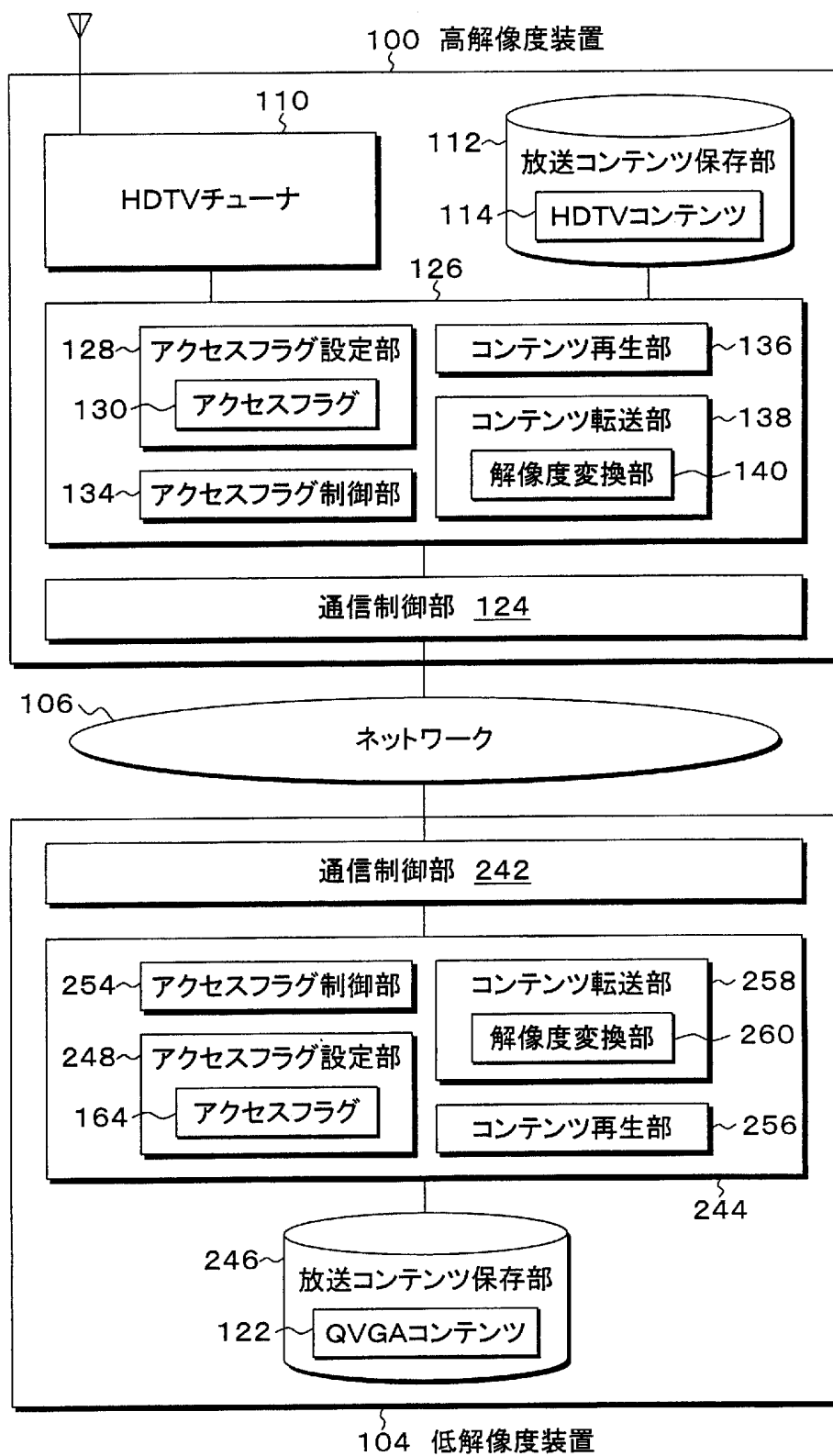
[図8]



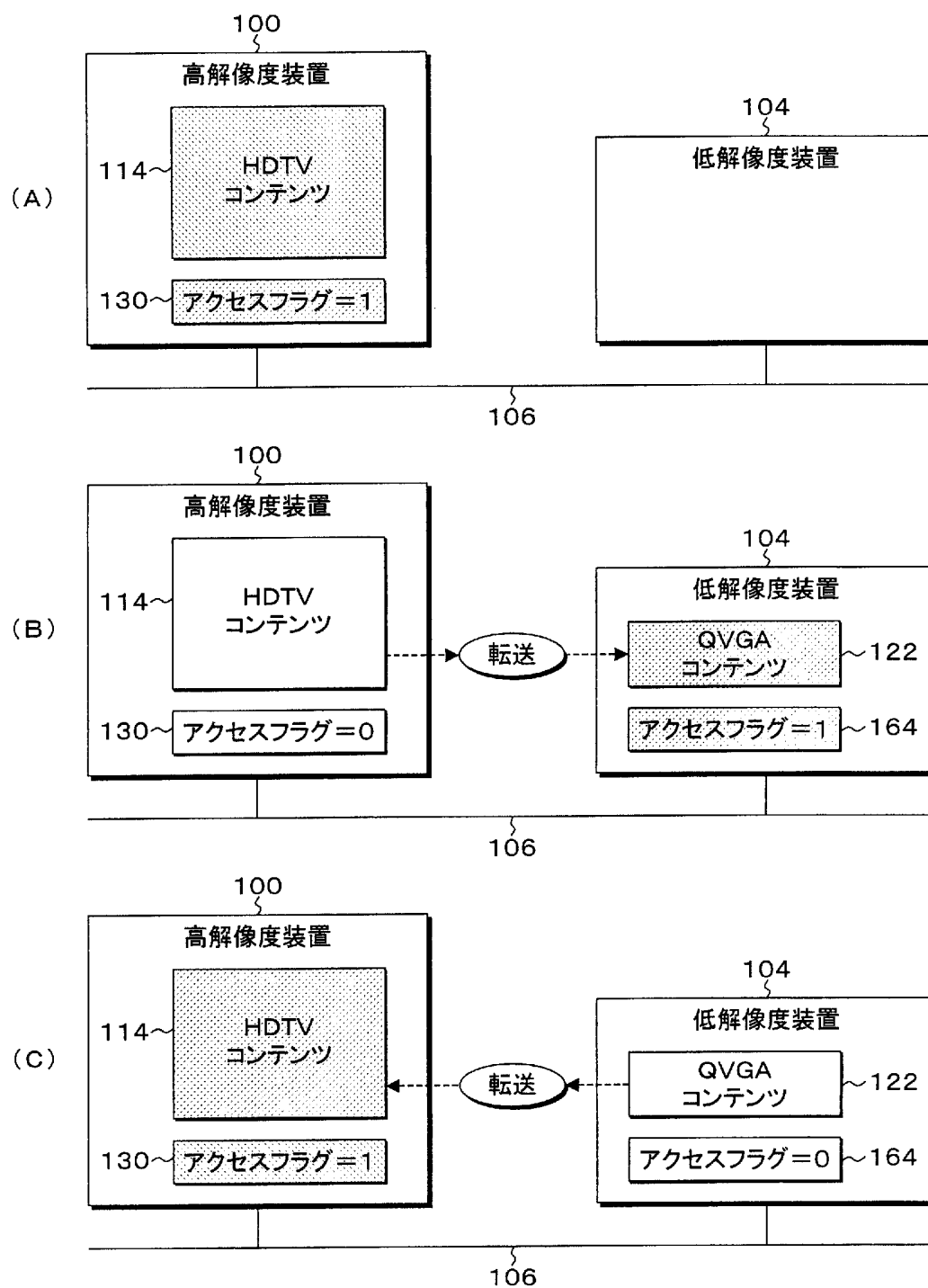
[図9]



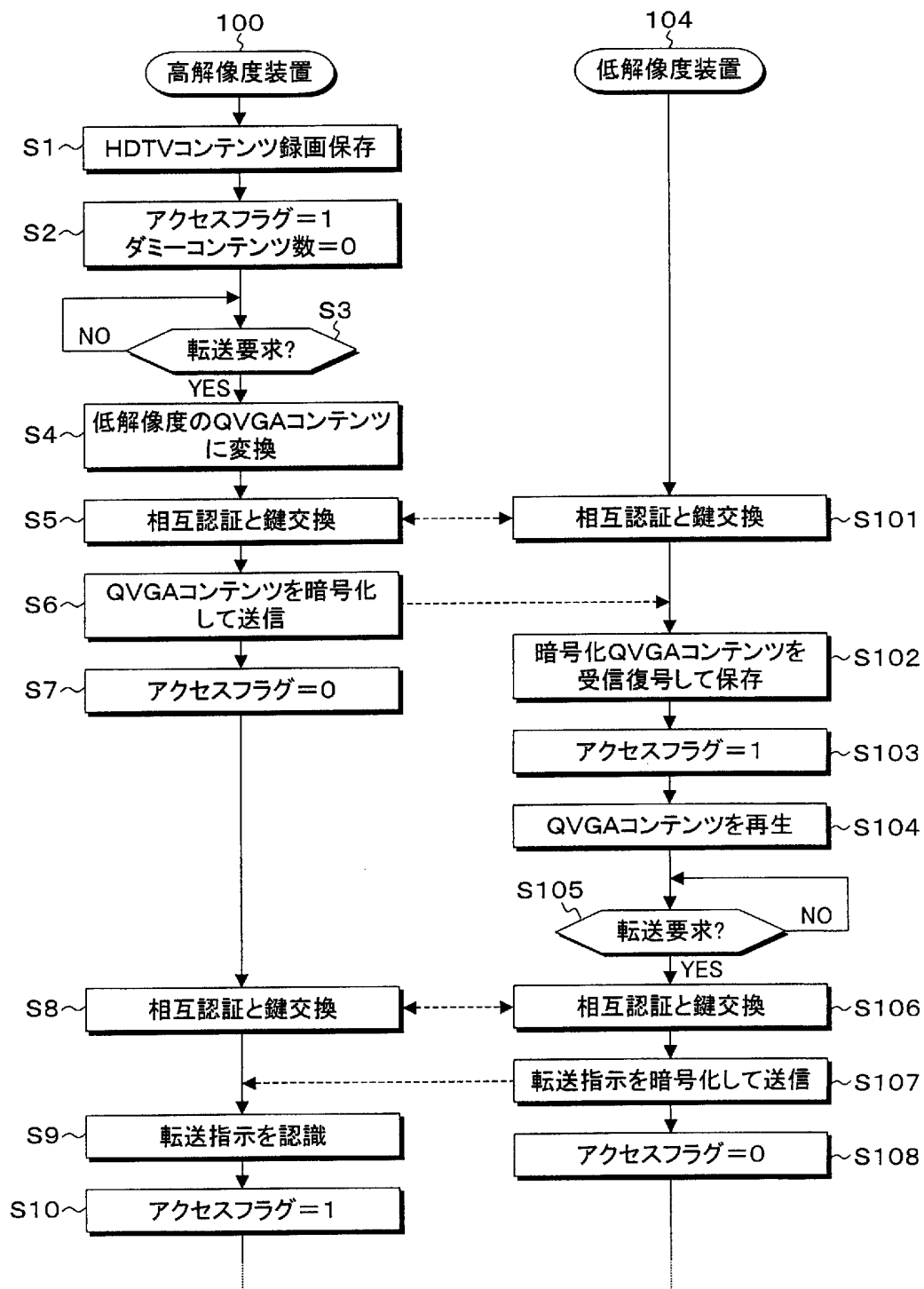
[図10]



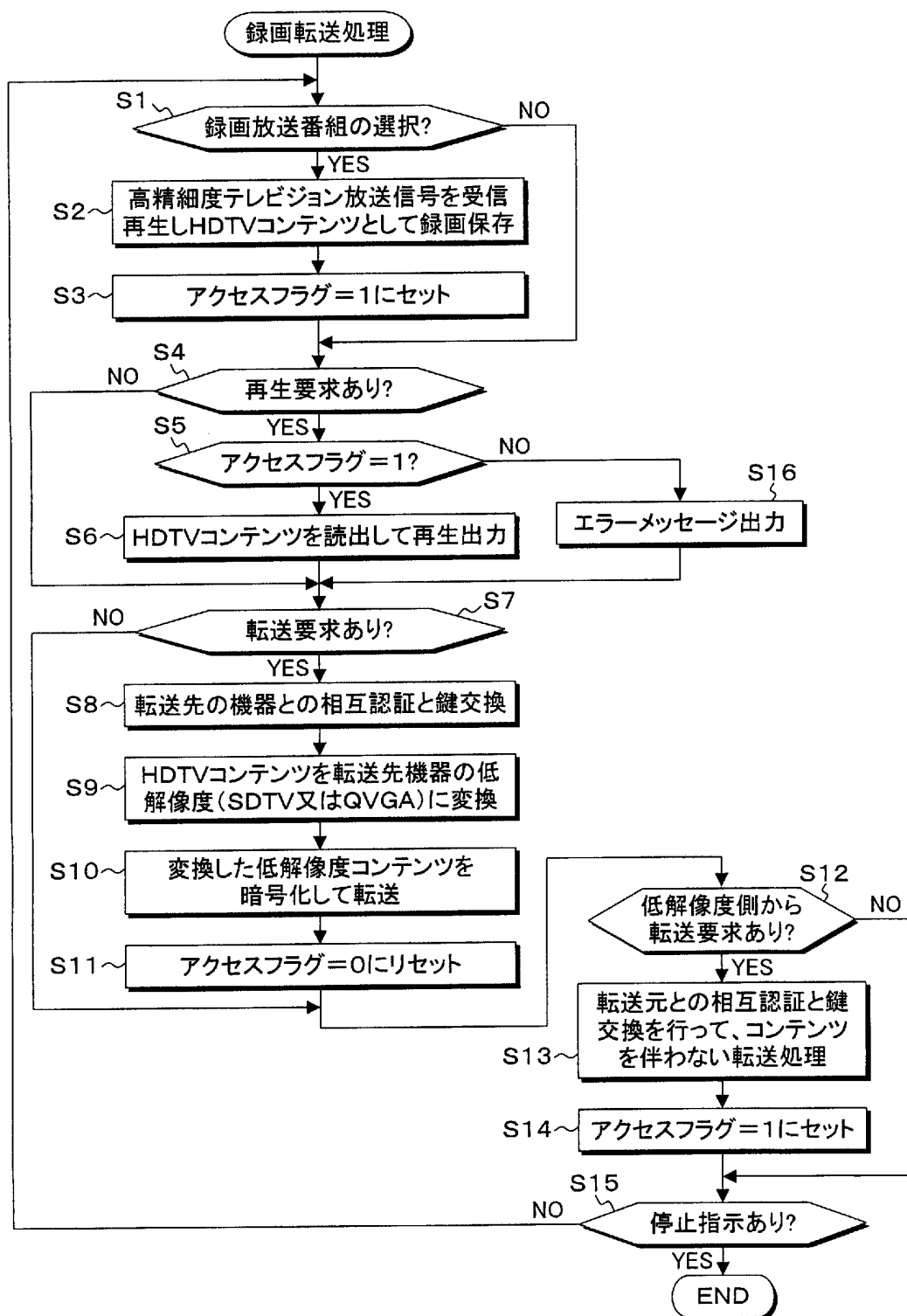
[図11]



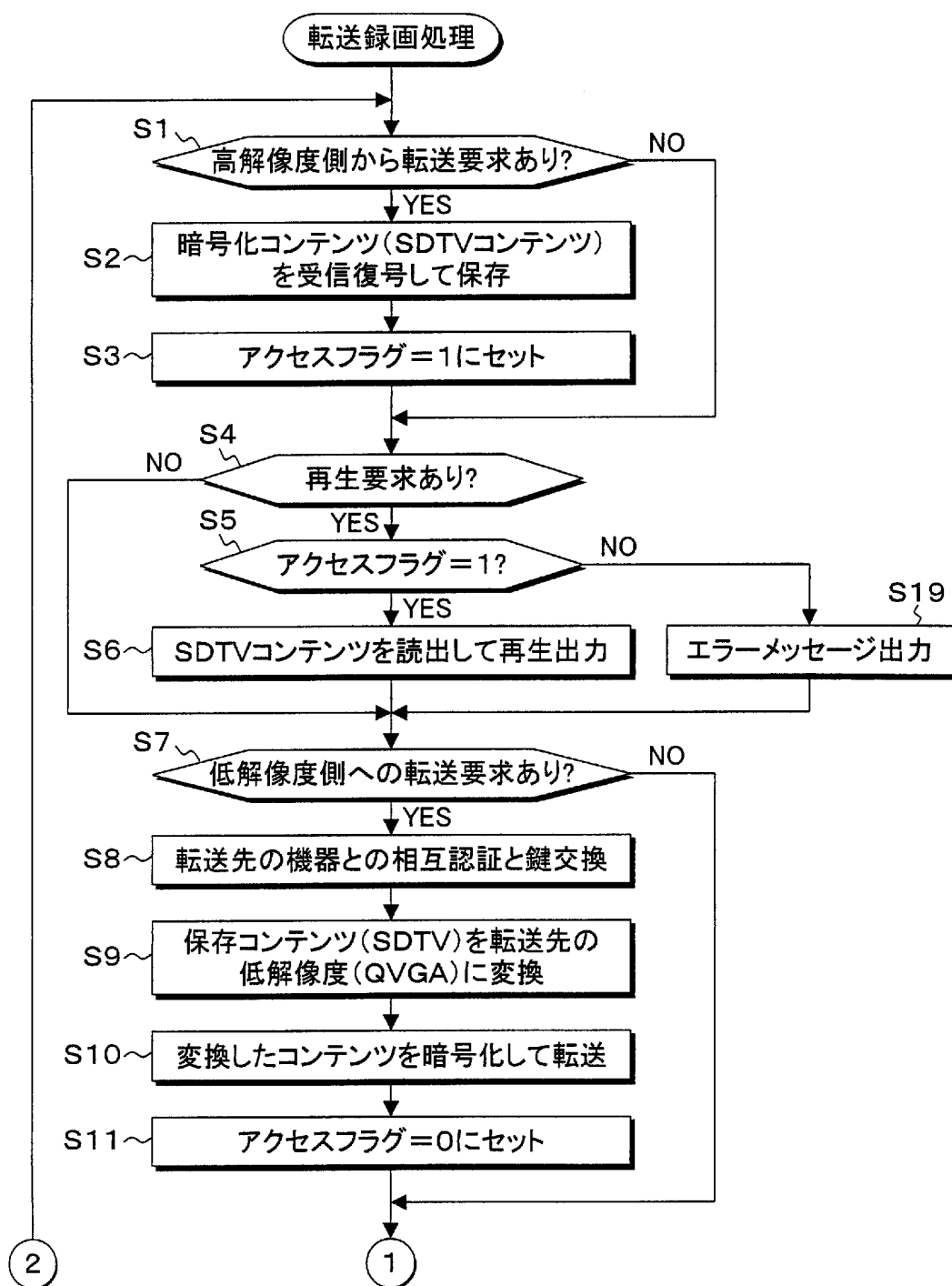
[図12]



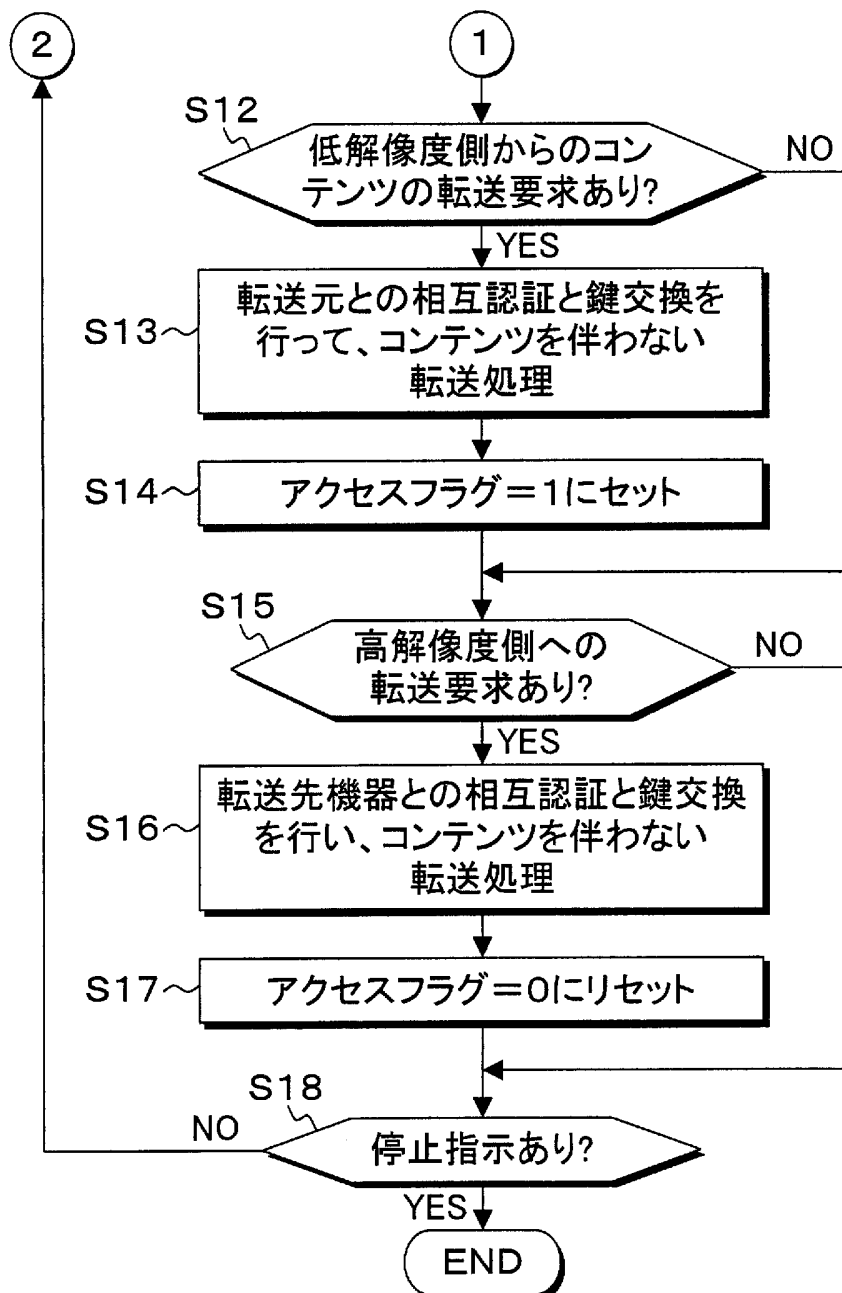
[図13]



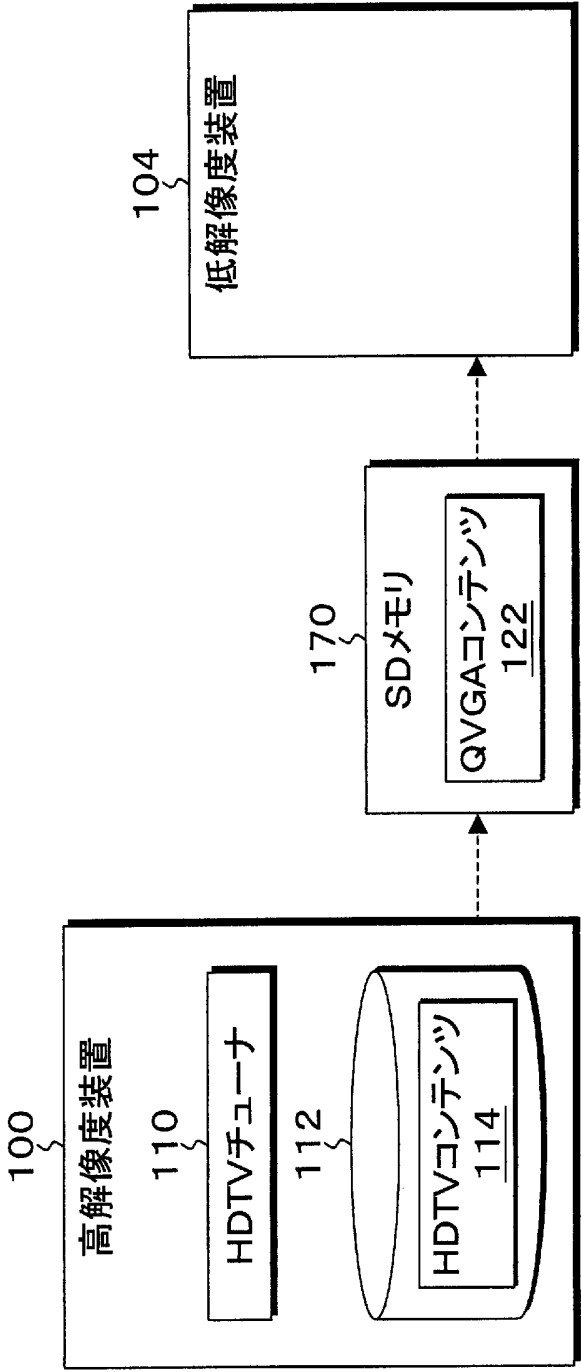
[図14]



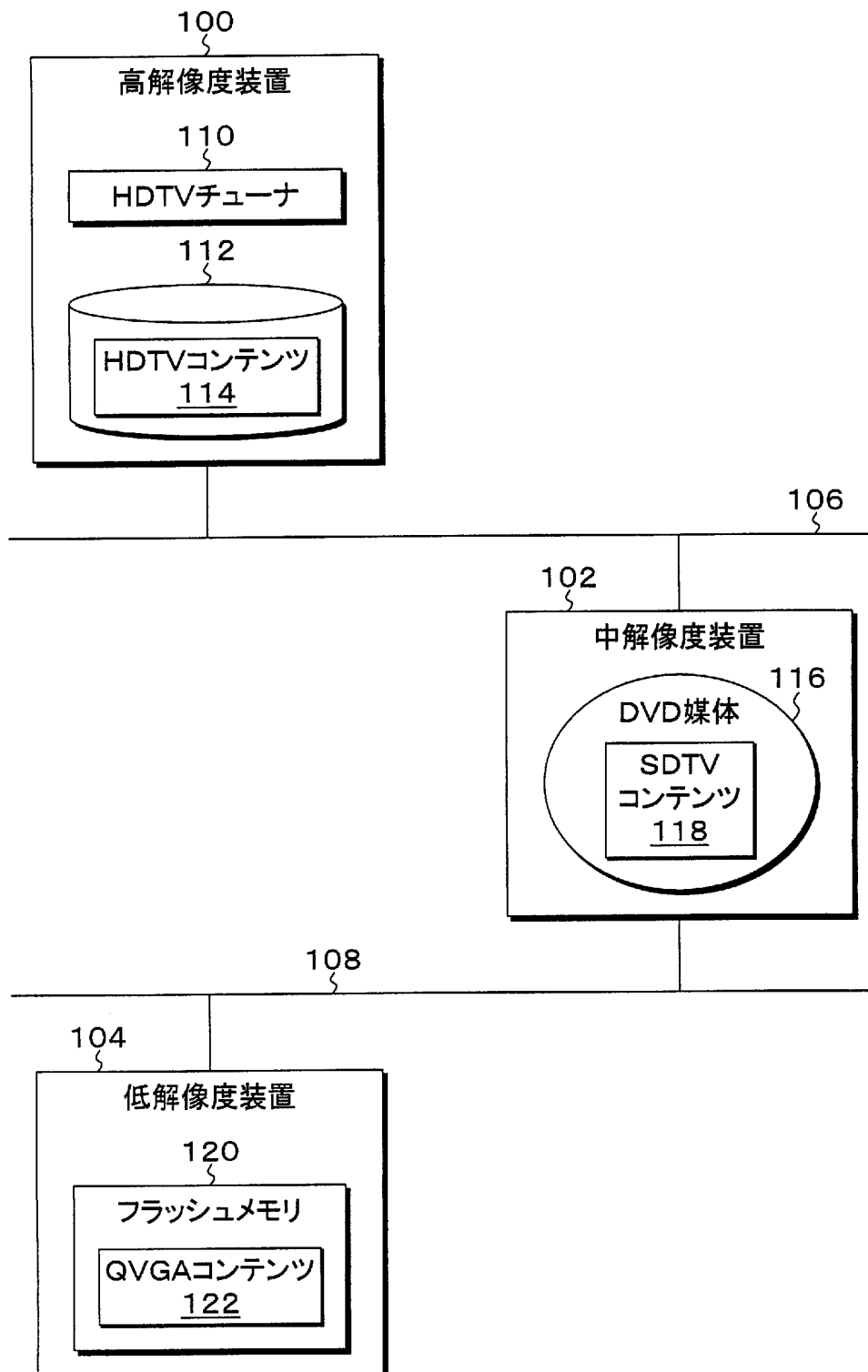
[図15]



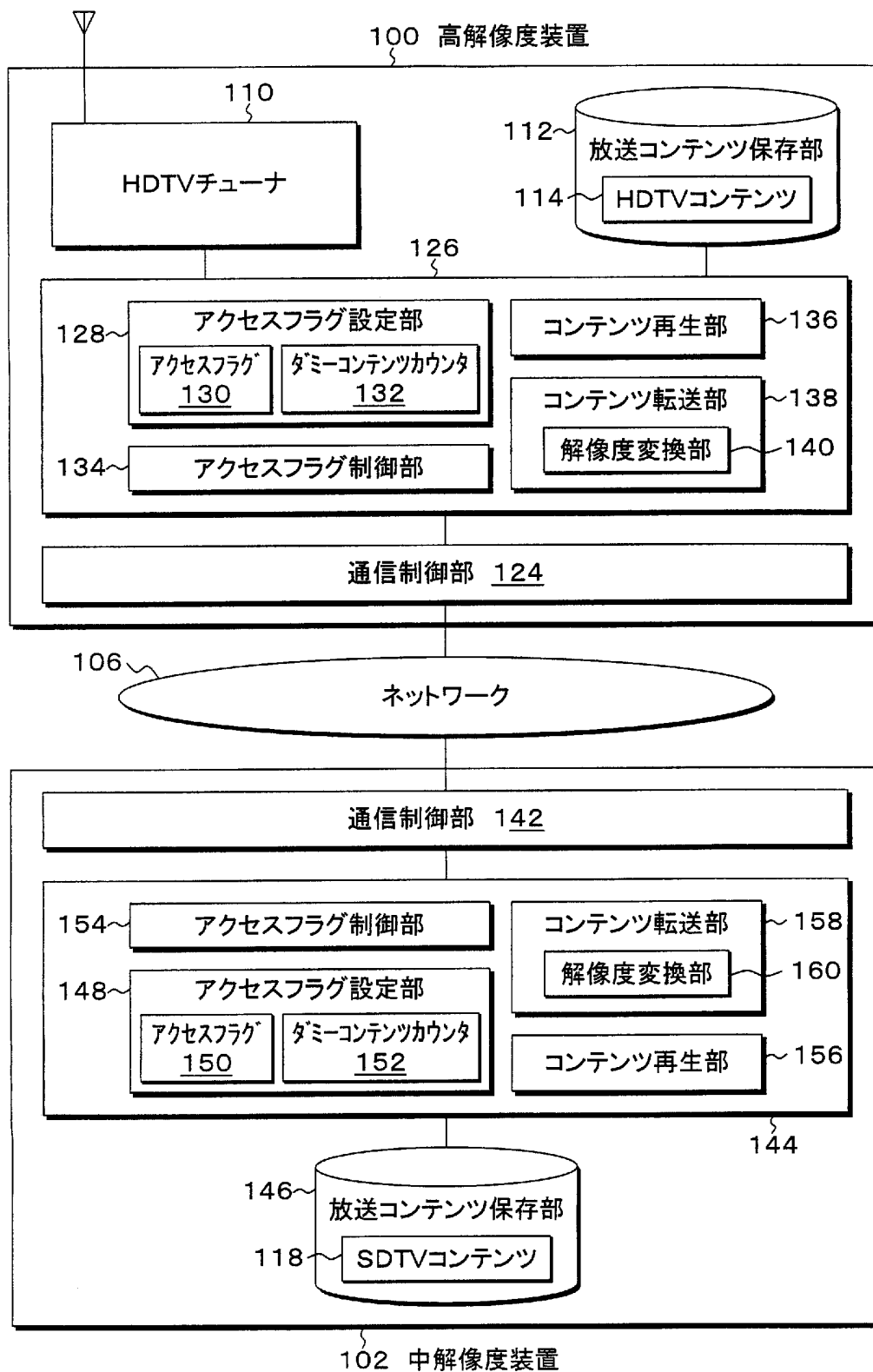
[図16]



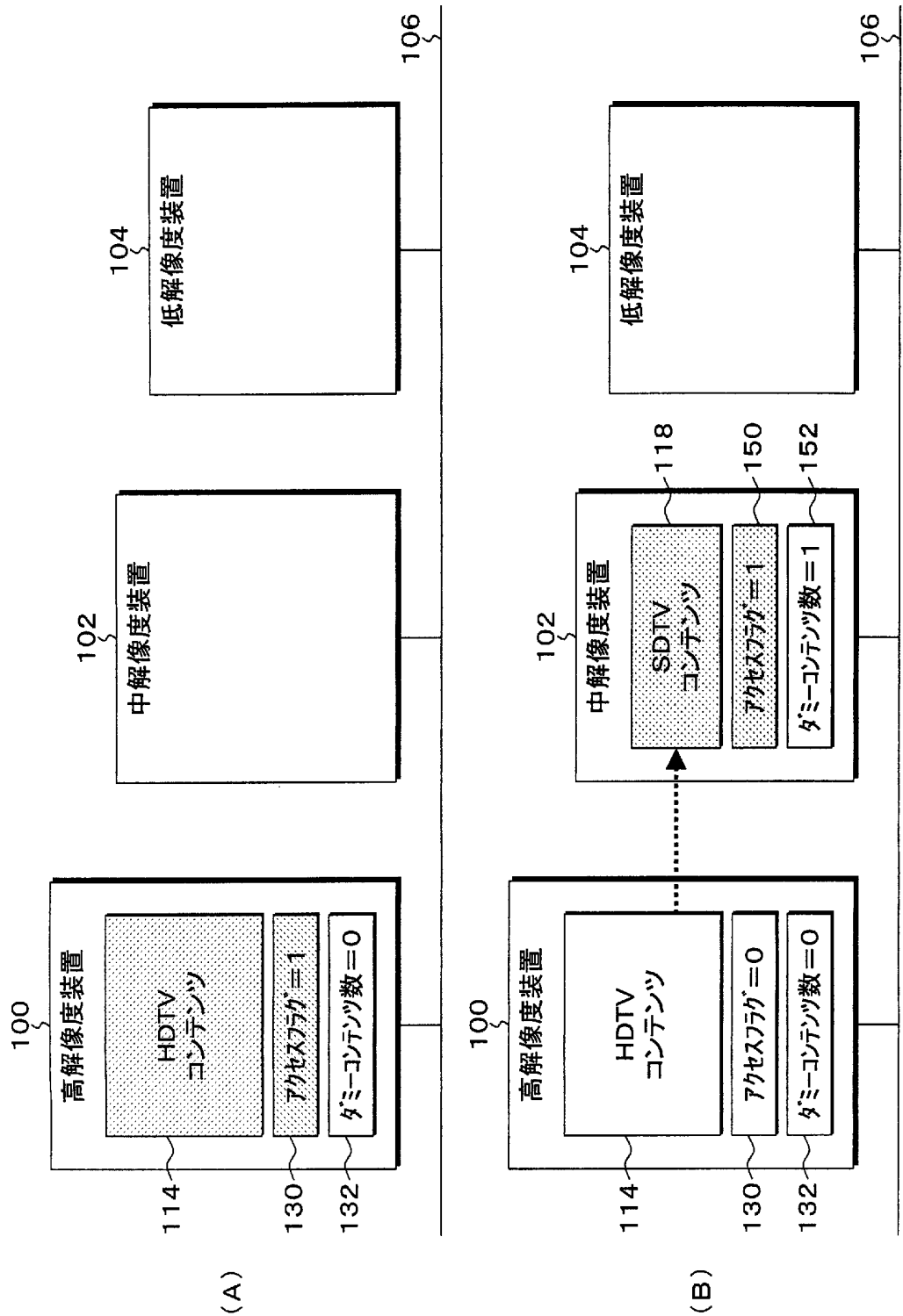
[図17]



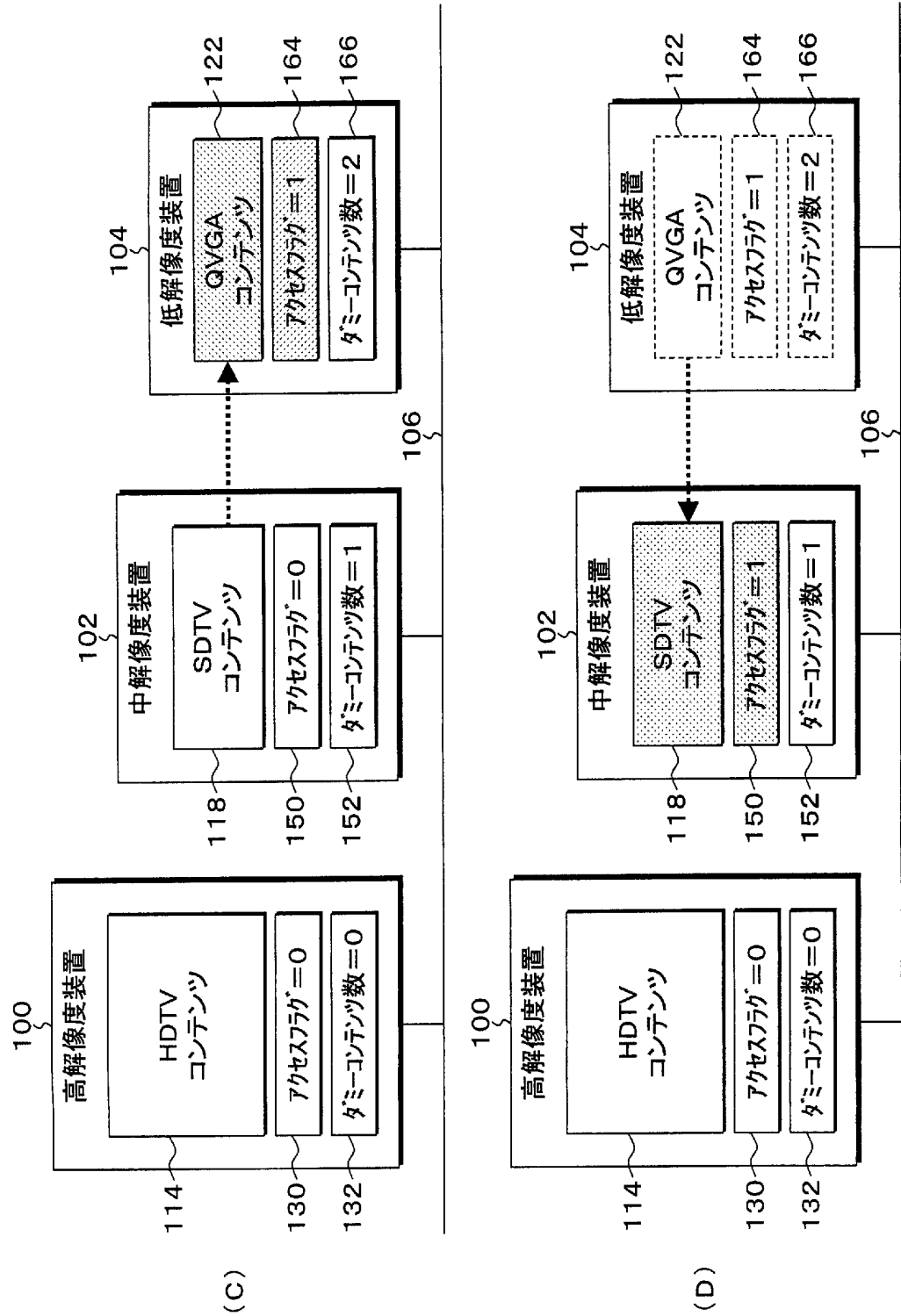
[図18]



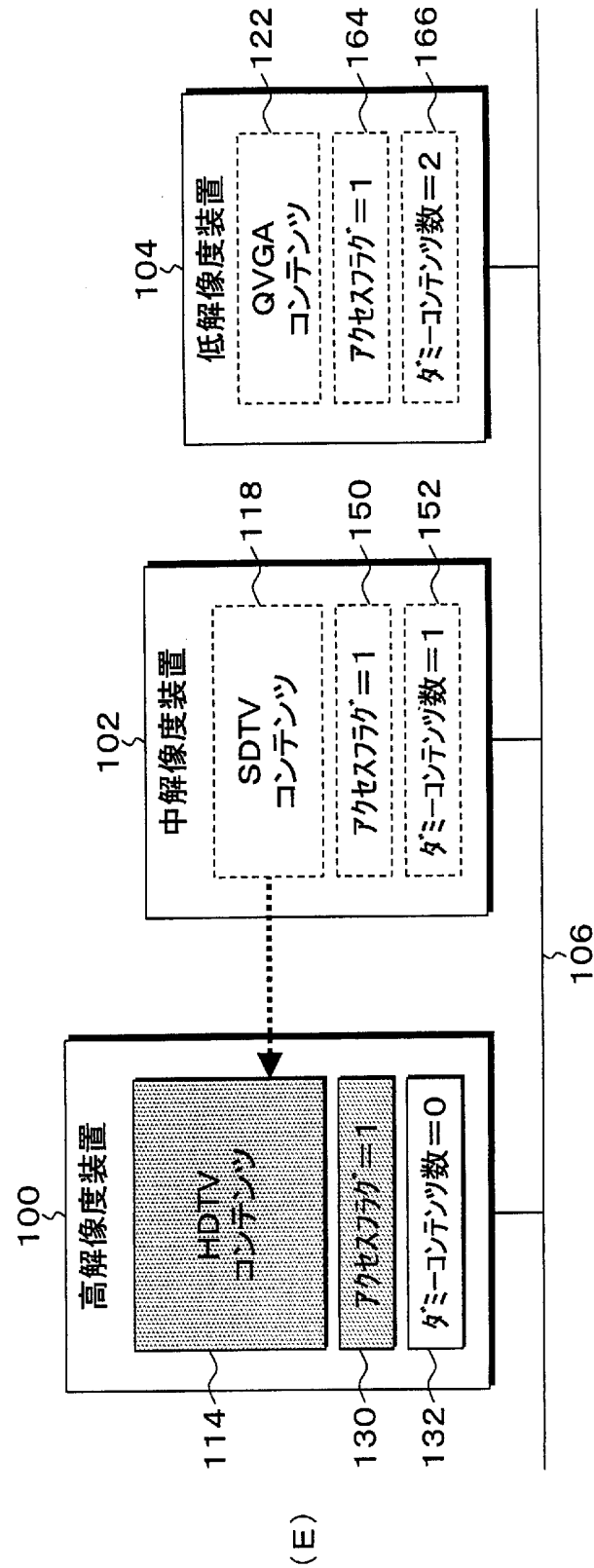
[図19]



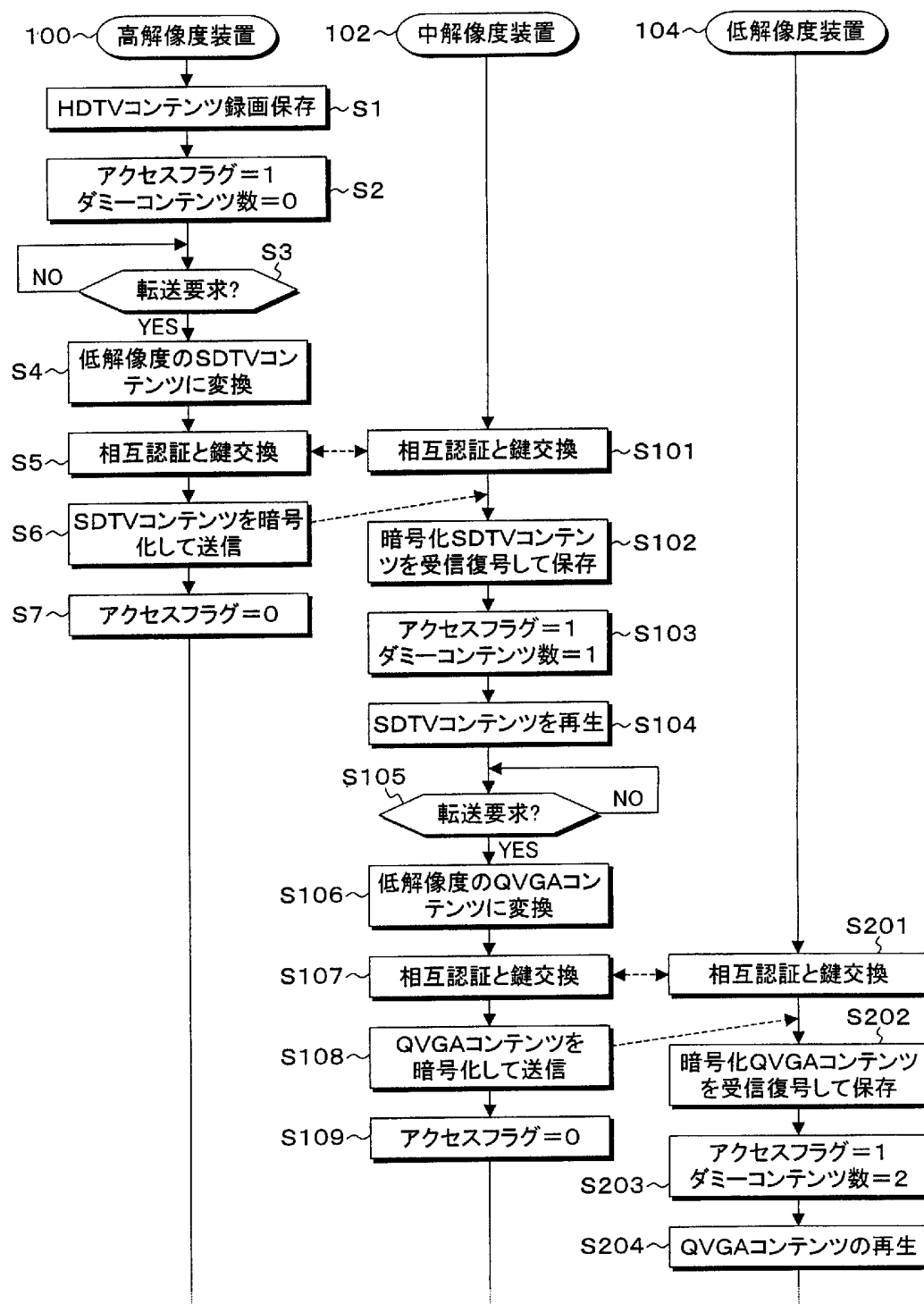
[図20]



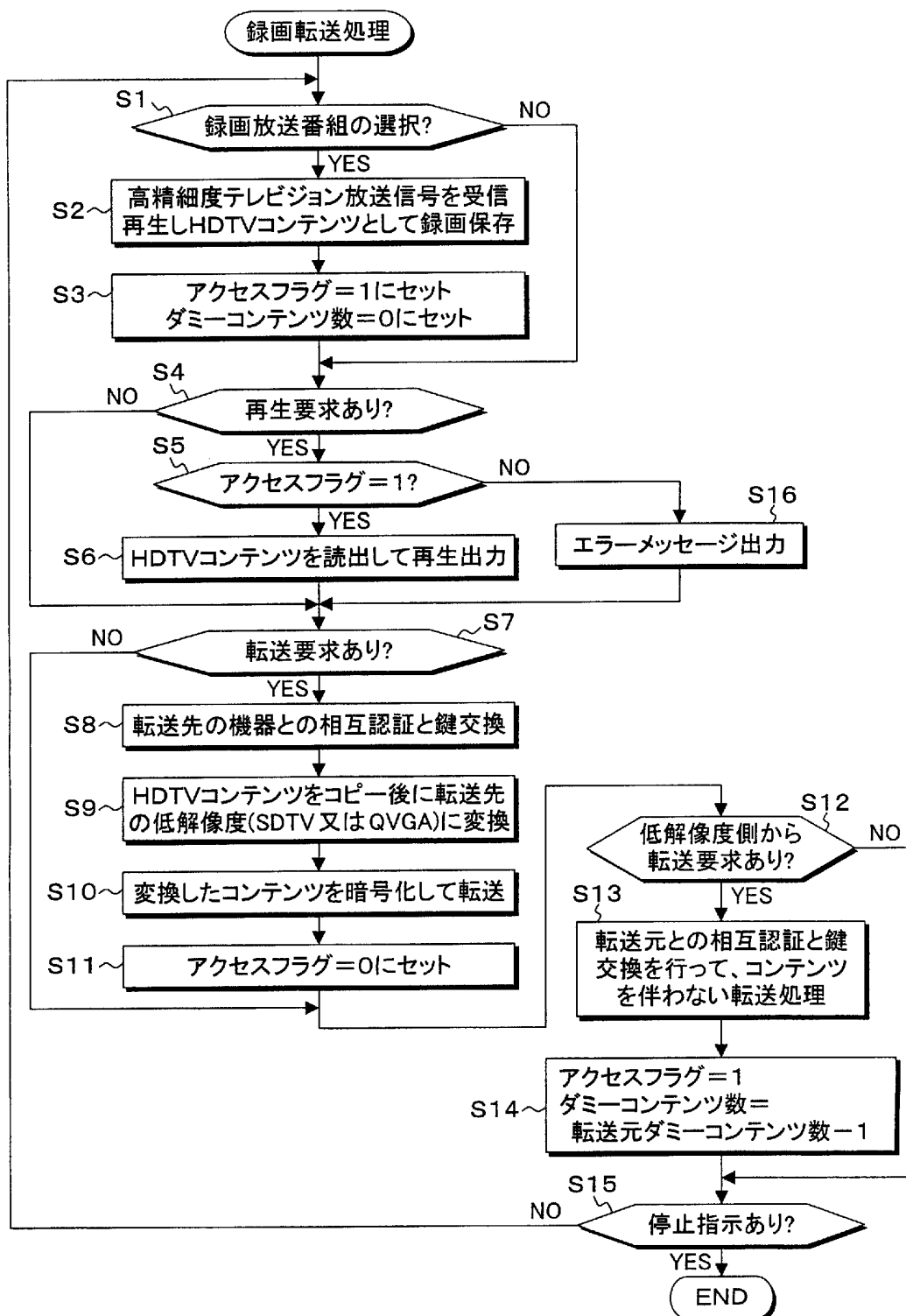
[図21]



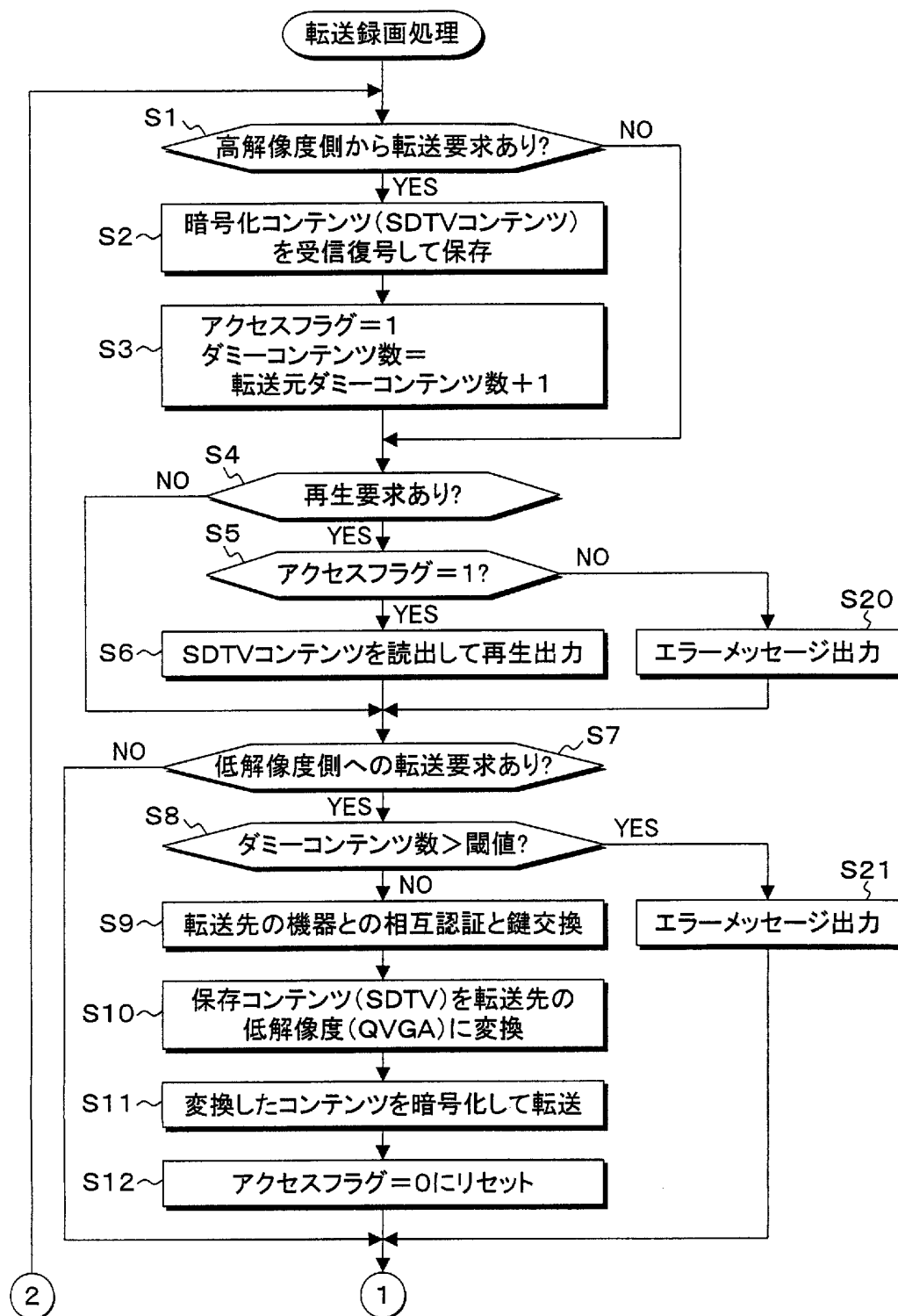
[図22]



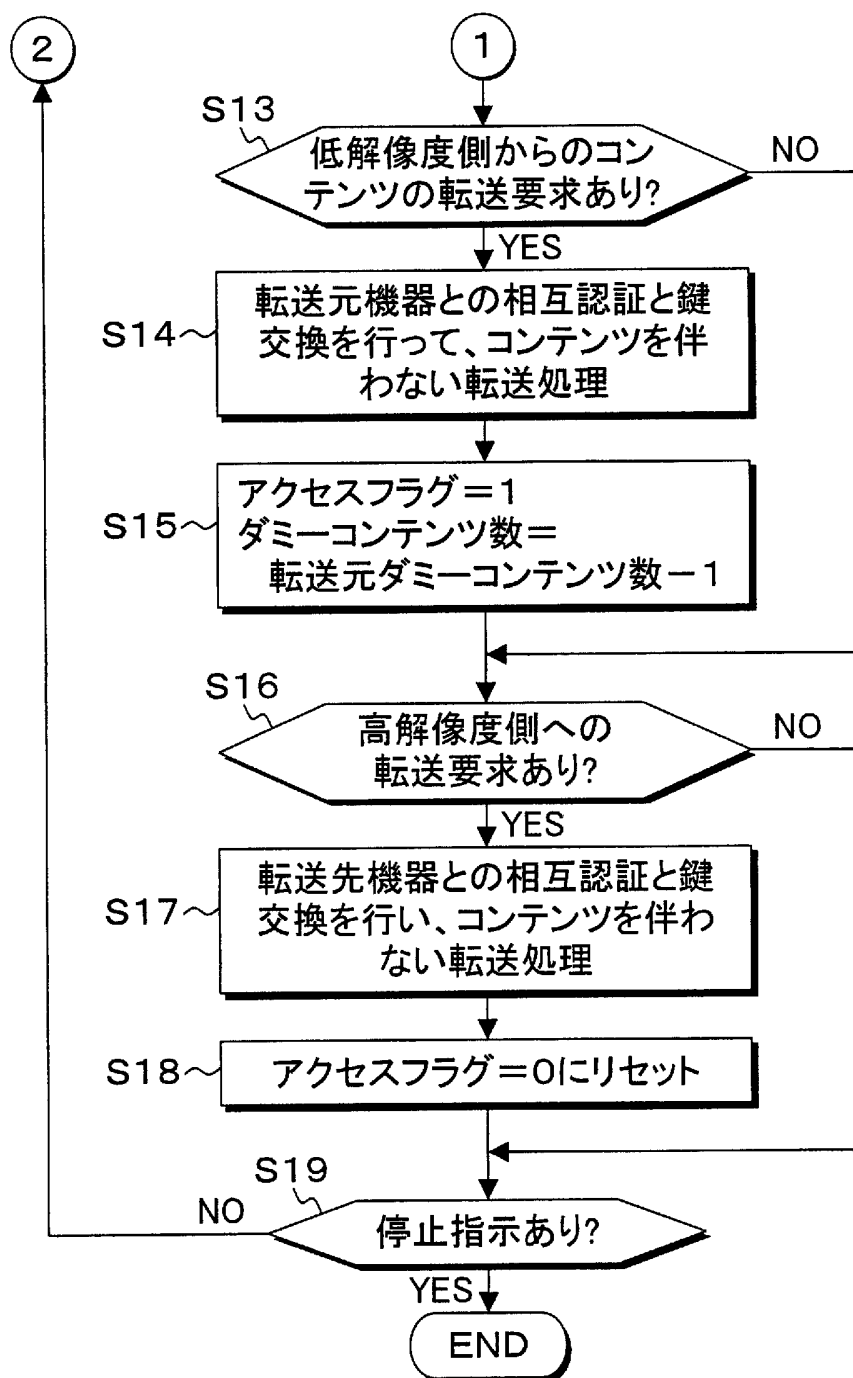
[図23]



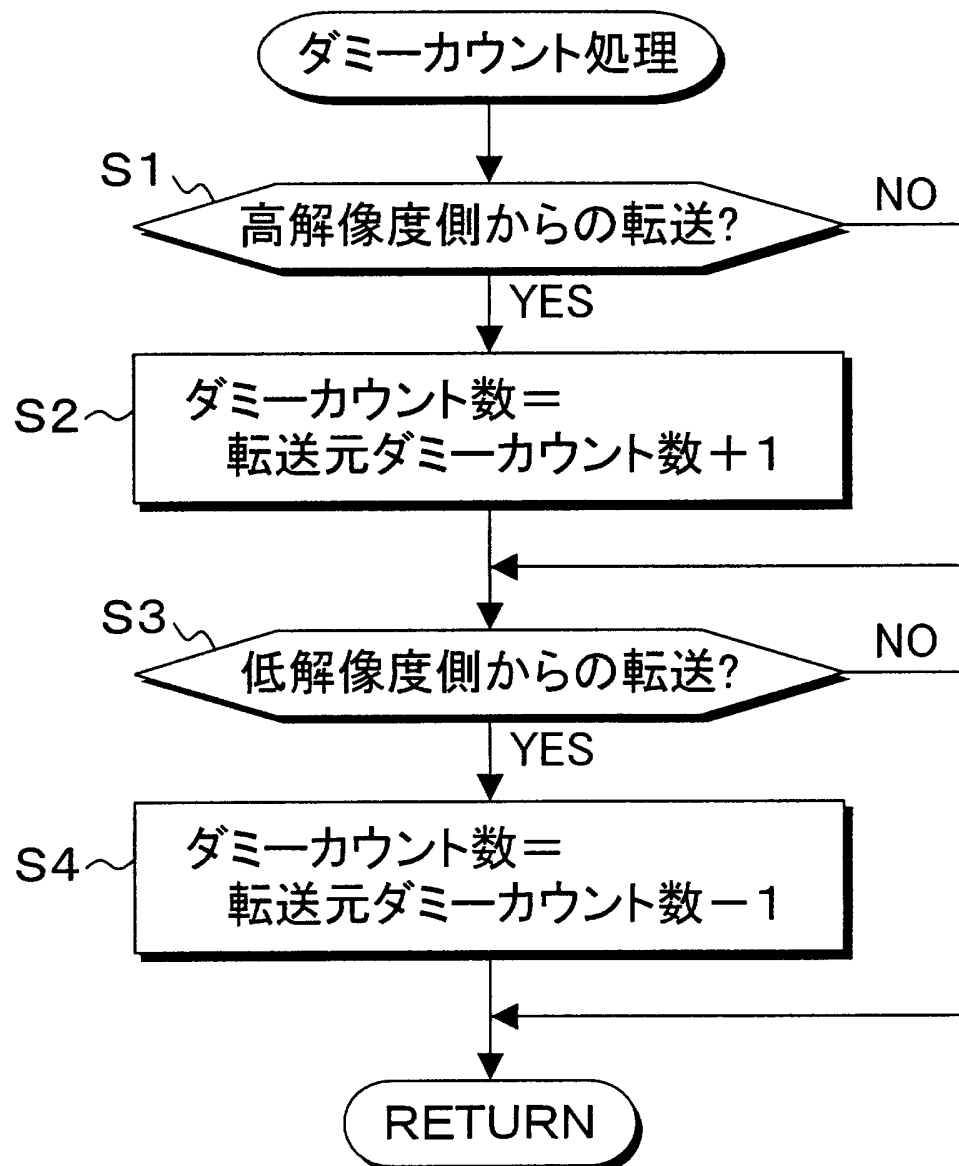
[図24]



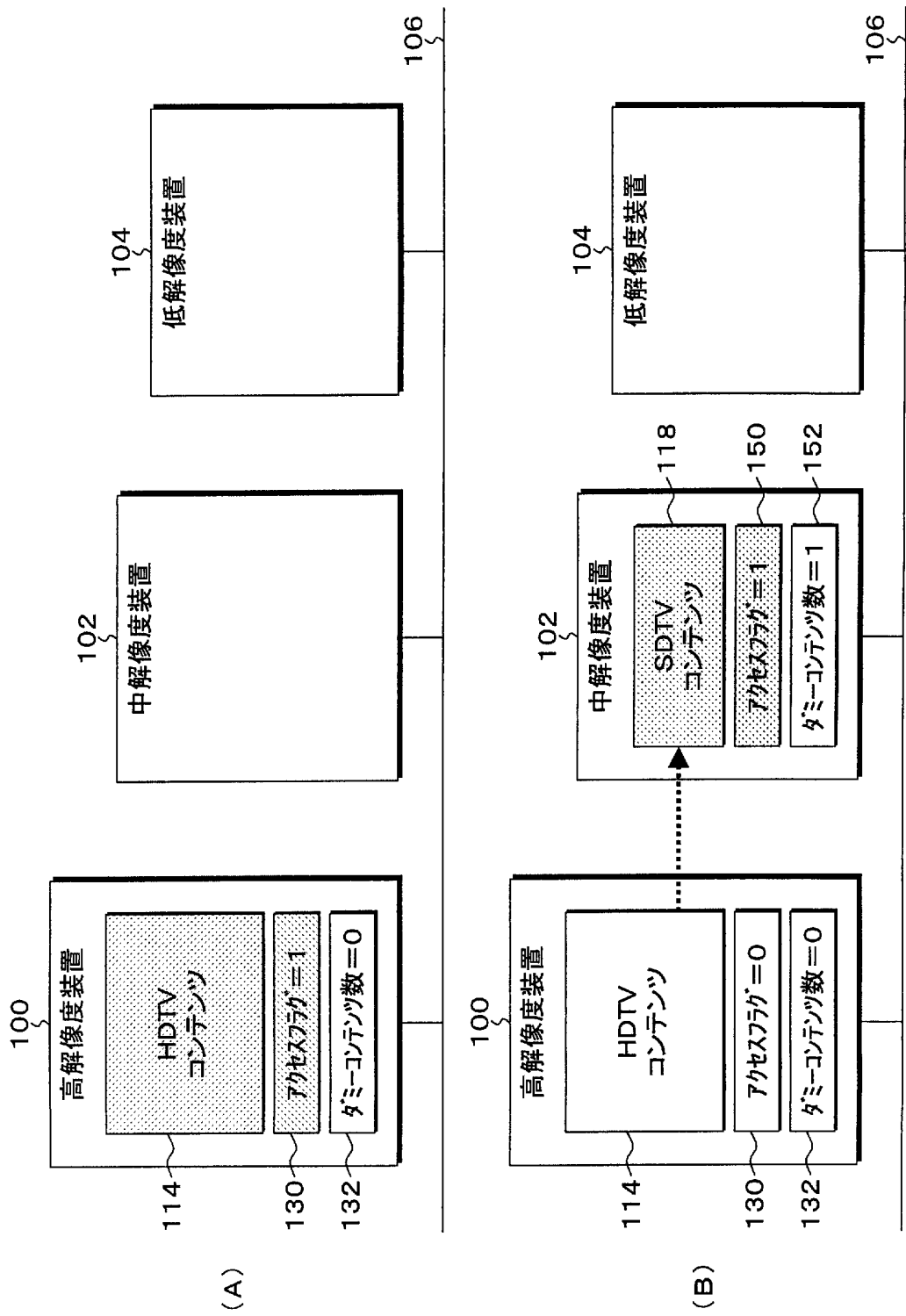
[図25]



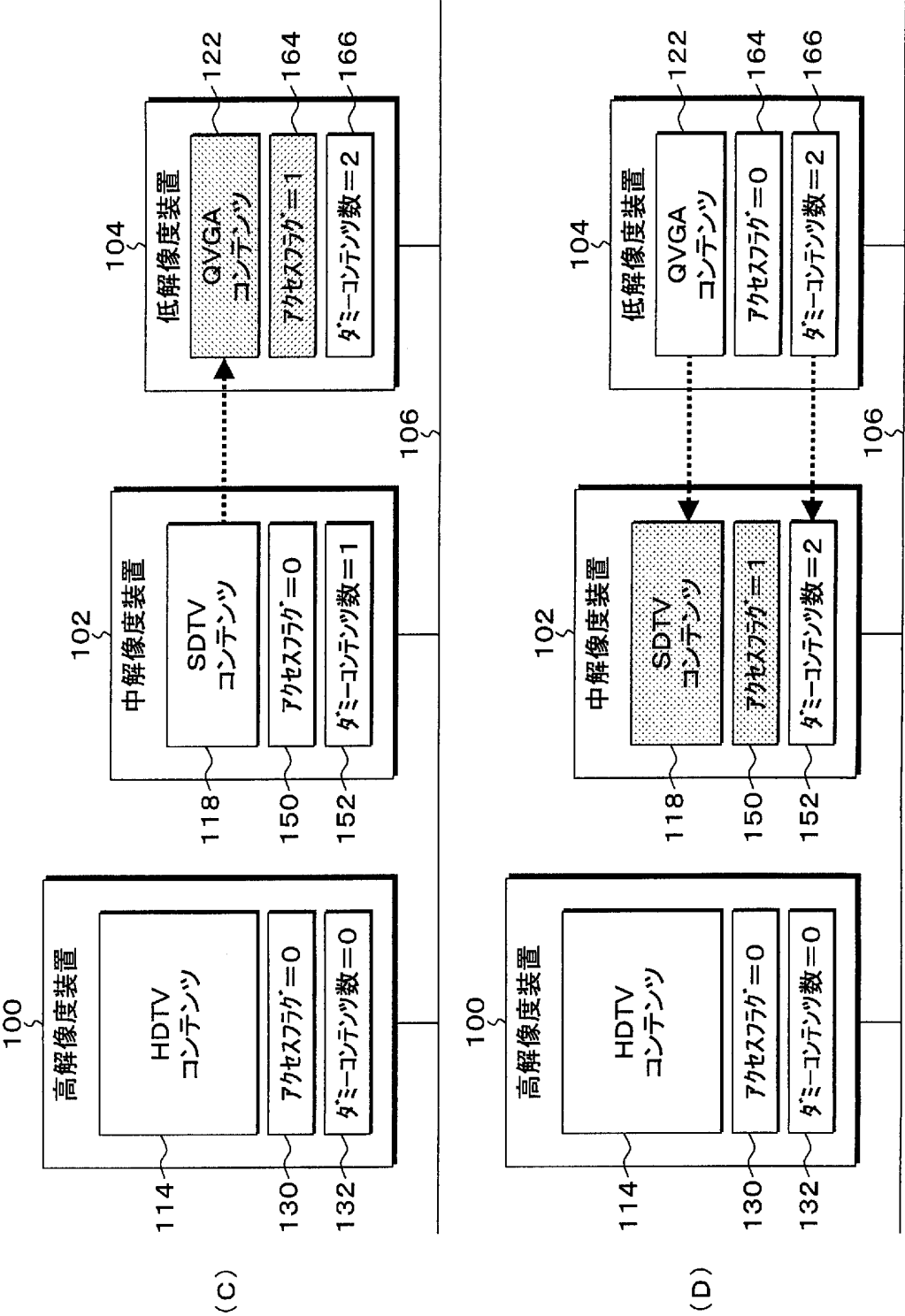
[図26]



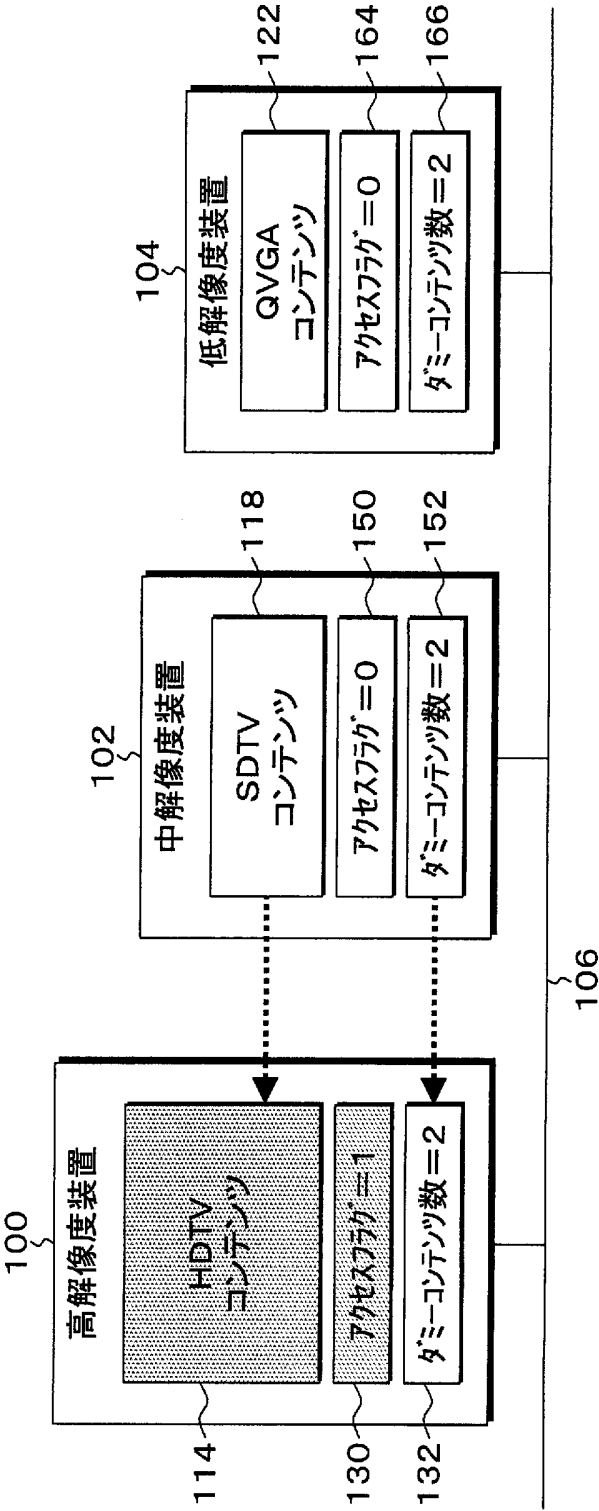
[図27]



[図28]

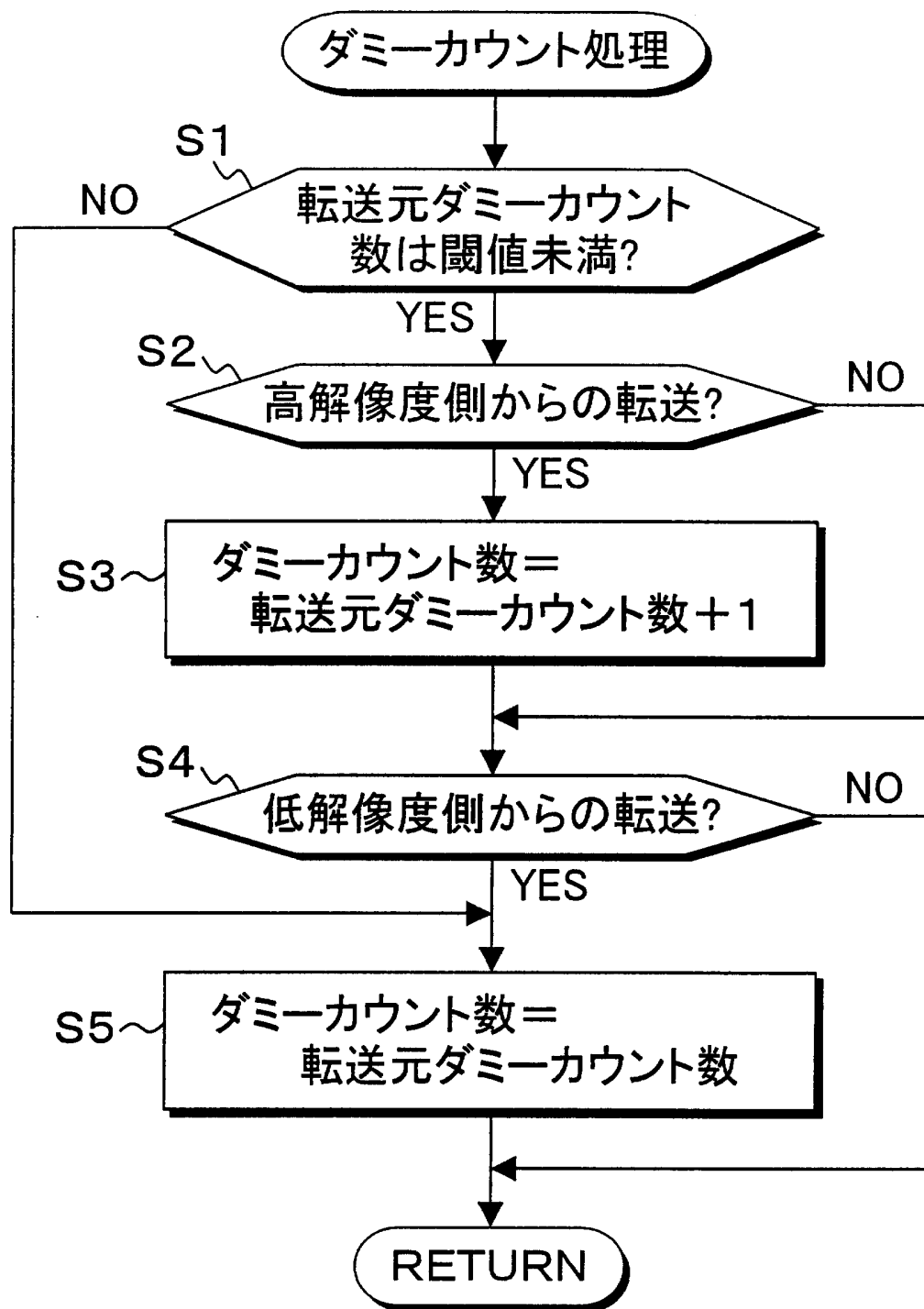


[図29]

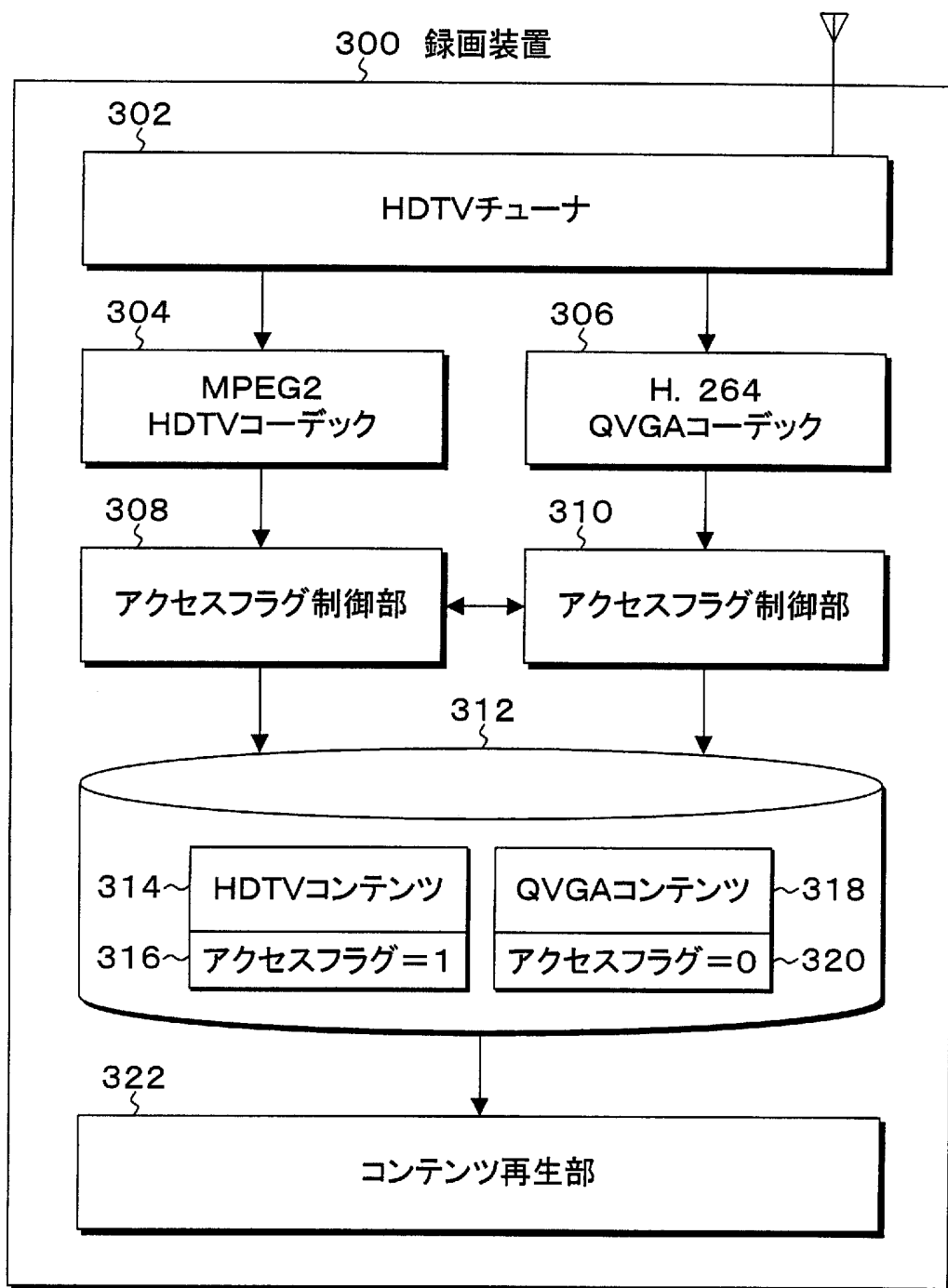


(E)

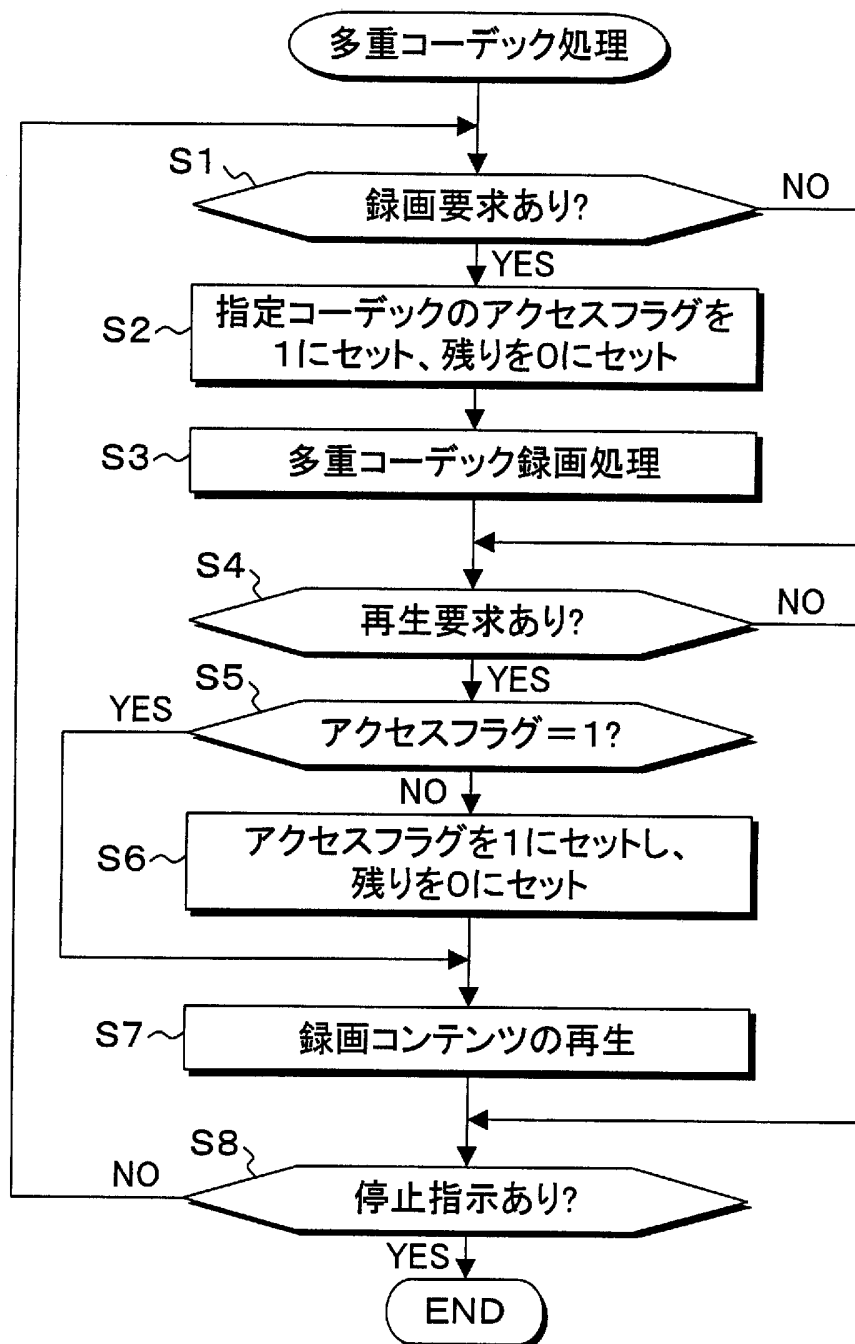
[図30]



[図31]



[図32]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/012266

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/06Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

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.
X	JP 2002-288377 A (Sanyo Electric Co., Ltd.), 04 October, 2002 (04.10.02),	1, 2, 4-9, 11-15, 17-19
Y	Par. Nos. [0084] to [0091], [0100] to [0104], [0128], [0379] to [0407] (Family: none)	3, 10, 16
Y	JP 2002-51037 A (Hitachi, Ltd.), 04 October, 2002 (04.10.02), Par. Nos. [0048] to [0052], [0064] to [0068] & US 2002/015497 A1	3, 10, 16

☐ 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
22 December, 2004 (22.12.04)Date of mailing of the international search report
18 January, 2005 (18.01.05)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/012266

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the present application are divided into the following four groups of inventions.

1. claims 1-19
 2. claims 20-22, 27, 28, 30-33, 38, 39, 41-44, 49, 50, 52
 3. claims 23-26, 34-37, 45-48
 4. claims 29, 40, 51
-
1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
 2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
 3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
 4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-19

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/06

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. Cl⁷ H04L9/06

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	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004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
X	JP 2002-288377 A (三洋電機株式会社) 2002. 10. 04, 第84-91, 100-104, 128, 379-407段落 (ファミリーなし)	1, 2, 4-9, 11-15, 17-19
Y		3, 10, 16
Y	JP 2002-51037 A (株式会社日立製作所) 2002. 10. 04, 第48-52, 64-68段落 & US 2002/015497 A1	3, 10, 16

☐ 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

の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

22. 12. 2004

国際調査報告の発送日

18. 1. 2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

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)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3597

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT 17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

本願の請求の範囲に係る発明は、以下の4群に分けられるものと認める。

1. 請求の範囲1-19
2. 請求の範囲20-22, 27, 28, 30-33, 38, 39, 41-44, 49, 50, 52
3. 請求の範囲23-26, 34-37, 45-48
4. 請求の範囲29, 40, 51

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☒ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

請求の範囲1-19

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。