

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006年5月11日 (11.05.2006)

PCT

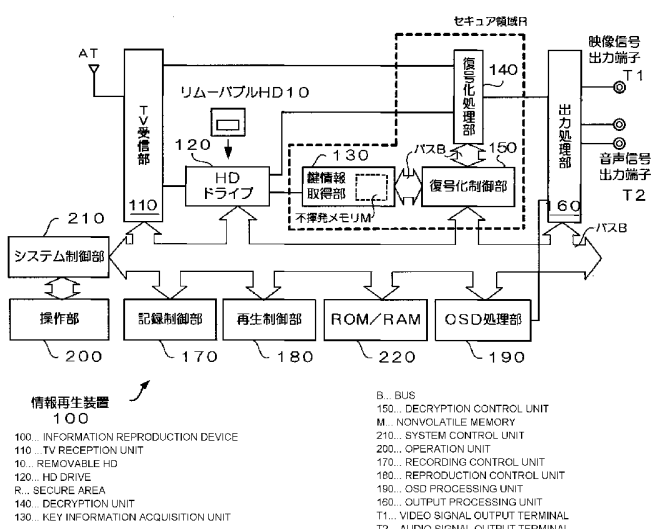
(10) 国際公開番号
WO 2006/049083 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) G11B 20/10 (2006.01)
G06F 21/24 (2006.01)
- (21) 国際出願番号: PCT/JP2005/019809
- (22) 国際出願日: 2005年10月27日 (27.10.2005)
- (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2004-319209 2004年11月2日 (02.11.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): パイオニア株式会社 (PIONEER CORPORATION) [JP/JP]; 〒1538654 東京都目黒区目黒一丁目4番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 竹村到 (TAKEMURA, Itaru) [JP/JP]; 〒3598522 埼玉県所沢市花園四丁目2610番地 パイオニア株式会社 所沢工場内 Saitama (JP).
- (74) 代理人: 石川泰男, 外 (ISHIKAWA, Yasuo et al.); 〒1050014 東京都港区芝二丁目17番11号 パーク芝ビル 2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, 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, 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).

/ 続葉有 /

(54) Title: KEY INFORMATION PROVIDING METHOD, INFORMATION REPRODUCTION DEVICE, AND KEY INFORMATION PROVIDING DEVICE

(54) 発明の名称: 鍵情報提供方法、情報再生装置、および、鍵情報提供装置



(57) Abstract: When transferring an encrypted content, key information for decrypting the encrypted content is distributed into a plurality of information, which are successively transmitted. After one distributed information is transmitted, the one transmitted information is erased before the next information is transmitted. Since there is no case that the key information is simultaneously present at the transmission side and the reception side, even if a failure occurs during transfer of the key information, the encrypted content cannot be decrypted by either side, thereby protecting the copyright.

(57) 要約:

暗号化コンテンツを転送する際に、当該暗号化コンテンツを復号するための鍵情報を複数の情報に分散し、順次送信する。分散された一の情報を送信した後、次の情報を送信する前に、送信された一の情報を消去する。送信側と受信側で同時に鍵情報が存在することがないので、鍵情報の転送中に障害が生じたとしても、双方で暗号化コンテンツを復号することはできず、著作権を保護することができる。



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。

明 細 書

鍵情報提供方法、情報再生装置、および、鍵情報提供装置

技術分野

- [0001] 本発明は、暗号化されたコンテンツデータを復号する際に用いる著作権の保護が考慮された鍵情報の提供処理に関する技術分野に属する。

背景技術

- [0002] 近年、インターネット等の通信ネットワークに関する技術の発達により、携帯用電話機等を用いた個人向けの携帯通信端末装置により、映像データをはじめとする様々な情報の閲覧、取得および提供など各ユーザが容易に情報を利用することができるようになっている。
- [0003] このような情報の授受においては、すべての情報がデジタル信号により行われるため、音楽データや映像データの授受を行った場合に、データの授受による音質や画質の劣化をほとんど生じさせることなく、データの複製を行うことが可能となっている。したがって、様々な媒体で提供される音楽データや映像データにおいて、著作権者の権利が存在する場合には、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。
- [0004] 一方、著作権保護の目的を最優先して、様々な媒体で提供される音楽データや映像データの複製などのデータの授受を禁止すると、適法にコンテンツデータを購入したユーザが個人的に使用する場合であっても複製を行うことができなくなるので、著作権の保護が過度になりすぎるとともに、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、その機会を喪失することになりかねず、かえって不利益が生ずることとなる。
- [0005] このような状況下において、従来、コンテンツデータの所有に対してではなく、利用に対して著作権保護を実現する超流通システムと呼ばれる著作権管理に着目した流通システムが提案されている。
- [0006] 具体的には、この超流通システムは、コンテンツデータが通信回線に代表されるネットワークやCD (Compact Disc)、DVD (Digital Versatile Disc) の記録媒体など様々

な経路で提供される一方、当該コンテンツデータを利用する際に、当該コンテンツデータの復号または再生管理を行うためのライセンスと呼ばれる鍵情報を用いるようになっている。この超流通システムは、この鍵情報を用いてコンテンツデータの利用を管理し、かつ、著作権の保護を行うようになっている(例えば、非特許文献1)。

非特許文献1: 森亮一、河原正治、大瀧保広「超流通 知的財産権処理のための電子技術」情報処理、社団法人情報処理学会、1996年12月、第37巻、第2号、pp. 155-161

発明の開示

発明が解決しようとする課題

[0007] しかしながら、このような流通システムにあつては、ライセンスの情報を示す鍵情報もまたデジタル情報であるため、当該鍵情報の授受に關して的確な方法を構築する必要がある。すなわち、このような流通システムにおいて、不正に鍵情報が取得され、または、使用されると、コンテンツデータの著作権保護を的確に行うことができないのみならず、当該流通システムを構築することができない。

[0008] 本発明は、上記の課題に鑑み、その一例として、鍵情報を授受に關して当該鍵情報を暗号化しつつ、段階的に送受信することによつて的確に鍵情報の授受を行うことができるとともに、強固な著作権の保護を行うことができる鍵情報提供方法を提供することにある。

課題を解決するための手段

[0009] 上記の課題を解決するために、請求項1に記載の発明は、暗号化されたデータを復号するための鍵情報を記憶する第1記憶手段から当該第1記憶手段とは異なる第2記憶手段に提供する鍵情報提供方法であつて、前記第1記憶手段にて前記鍵情報から複数の送信情報を生成する生成工程と、前記生成された各送信情報を他の送信情報と異なるタイミングにて段階的に前記第1記憶手段から第2記憶手段に順次送信する送信工程と、前記第2記憶手段にて前記送信された各送信情報を順次受信する受信工程と、前記第2記憶手段にて送信情報を受信した後に、当該送信情報を用いて前記鍵情報を復元する復元工程と、を含み、前記送信工程においては、前記第1記憶手段が一の送信情報を送信した後であつて、未だ前記第2記憶手段に

送信されていない他の送信情報を送信する前に、当該送信された送信情報を消去する構成を有している。

[0010] また、請求項9に記載の発明は、暗号化されたデータを復号するための鍵情報を記録する記憶手段から当該鍵情報を取得して当該データを再生する情報再生装置であって、

前記記憶手段にて前記鍵情報を暗号化する際に用いる複数の送信情報を生成させ、当該生成された各送信情報を他の送信情報とは異なるタイミングにて段階的に当該記憶手段から順次送信させる送信制御手段と、前記送信された各送信情報を受信する受信手段と、前記送信情報を受信した後に、当該送信情報を用いて前記鍵情報を復元する復元手段と、前記復元された鍵情報に基づいて暗号化されたデータを復号し、当該コンテンツデータを再生する再生手段と、を備え、前記送信制御手段が、前記一の送信情報を受信した後であって、未だ記憶手段から送信されていない他の一の送信情報を受信する前に、当該送信された送信情報を前記記憶手段から消去させる構成を有している。

[0011] また、請求項12に記載の発明は、暗号化されたデータを復号するための鍵情報を、当該データを再生する情報再生装置に提供する鍵情報提供装置であって、前記鍵情報が予め記憶される記憶手段と、前記鍵情報を暗号化する際に用いる複数の送信情報を生成する生成手段と、前記生成された各送信情報を他の送信情報と異なるタイミングにて段階的に前記記憶手段から他の記憶手段に順次送信する送信手段と、前記一の送信情報を送信した後であって、未だ送信していない他の送信情報を送信する前に、当該送信された送信情報を消去する消去手段と、を備える構成を有している。

図面の簡単な説明

[0012] [図1]本願に係る情報記録再生装置の構成を示すブロック図である。

[図2]第1実施形態におけるライセンス鍵情報の提供処理を説明するための図である。

[図3]第1実施形態におけるリムーバブルHDおよび鍵情報取得部におけるライセンス鍵情報の存在と再生可能状態を示す表である。

[図4]第1実施形態の再生制御部におけるコンテンツデータの再生開始処理の動作を示すフローチャートである。

[図5]第1実施形態のHDドライブおよび復号化制御部におけるライセンス鍵情報提供処理の動作を示すフローチャート(I)である。

[図6]第1実施形態のHDドライブおよび復号化制御部におけるライセンス鍵情報提供処理の動作を示すフローチャート(II)である。

[図7]共有鍵情報に基づいてライセンス鍵情報を暗号化して転送する処理を説明するための図(I)である。

[図8]共有鍵情報に基づいてライセンス鍵情報を暗号化して転送する処理を説明するための図(II)である。

[図9]第1実施形態の情報記録再生装置におけるライセンス鍵情報提供処理のその他の例を説明するための図である。

[図10]第2実施形態のライセンス鍵情報転送処理において用いる秘密分散法を説明するための図(I)である。

[図11]第2実施形態のライセンス鍵情報転送処理において用いる秘密分散法を説明するための図(II)である。

[図12]第2実施形態におけるライセンス鍵情報の提供処理を説明するための図である。

[図13]第2実施形態におけるリムーバブルHDおよび鍵情報取得部におけるライセンス鍵情報の存在と再生可能状態を示す表である。

[図14]第2実施形態のHDドライブおよび復号化制御部におけるライセンス鍵情報提供処理の動作を示すフローチャート(I)である。

[図15]第2実施形態のHDドライブおよび復号化制御部におけるライセンス鍵情報提供処理の動作を示すフローチャート(II)である。

[図16]第2実施形態の情報記録再生装置におけるライセンス鍵情報提供処理のその他の例を説明するための図である。

符号の説明

[0013] 10 … リムーバブルHD

- 100 … 情報記録再生装置
- 110 … TV受信部
- 120 … HDドライブ
- 130 … 鍵情報取得部
- 140 … 復号化処理部
- 150 … 復号化制御部
- 160 … 出力処理部
- 170 … 記録制御部
- 180 … 再生制御部
- 190 … OSD処理部
- 200 … 操作部
- 210 … システム制御部
- 220 … ROM/RAM

発明を実施するための最良の形態

- [0014] 以下、本願の実施の形態について、図面を参照しながら説明する。
- [0015] なお、以下に説明する実施の形態は、音声データと映像データを含むコンテンツデータが記録され、持ち運び可能なハードディスク(以下、リムーバブルHDという。)を有し、当該リムーバブルHDによってコンテンツデータおよび鍵情報の授受を行うことが可能な情報再生装置に対して、本願のライセンス鍵情報提供方法および情報再生装置を適用した場合の実施の形態である。
- [0016] また、本実施形態では、コンテンツデータそのものについては、著作権保護のための管理を行わず、この鍵情報を管理することによってコンテンツデータの視聴制御を行う超流通と呼ばれる流通システムに属する情報記録再生装置として説明する。
- [0017] [第1実施形態]
- 始めに、図1～図9を用いて本願に係る情報記録再生装置の第1実施形態について説明する。
- [0018] まず、図1を用いて本実施形態の情報記録再生装置の構成および動作について説明する。なお、図1は、本実施形態における情報記録再生装置の構成を示すブロ

ック図である。

- [0019] 本実施形態の情報記録再生装置100は、リムーバブルHD10によって、または、所定の放送局から送信された放送波によって提供された暗号化されたコンテンツデータ(以下、暗号化コンテンツデータという。)を、当該リムーバブルHD10にて提供されたコンテンツデータの配信元から供給される鍵情報(以下、ライセンス鍵情報という。)を用いて復号化の処理を実行し(以下、復号化処理という。)、外部に接続されたモニタなどの外部装置に復号化されたコンテンツデータを出力するようになっている。
- [0020] 特に、本実施形態の情報記録再生装置100は、ライセンス鍵情報をリムーバブルHD10から取得する際に、当該情報記録再生装置100内とリムーバブルHD10それぞれに、暗号化コンテンツデータを復号可能なライセンス鍵を存在させないために、当該ライセンス鍵情報を段階的に授受するようになっている。
- [0021] すなわち、超流通などの流通システムでは、暗号化コンテンツデータは複写記録、または、移動記録を行う際にその記録における回数または記録禁止などの記録制限が無いので、ライセンス鍵情報さえあれば、何れの装置においても暗号化コンテンツデータの再生が可能になる。したがって、本実施形態の情報記録再生装置100は、一のライセンス鍵情報が複数の装置または記録媒体に存在することなく、的確に当該各ライセンス鍵情報の授受を行わせるために、各装置間または各装置と記録媒体の間において当該ライセンス鍵情報の段階的な授受を行い、各ライセンス鍵情報を管理するようになっている。
- [0022] このような本実施形態の情報記録再生装置100は、図1に示すように、アンテナATを介して暗号化コンテンツデータを放送波として受信するTV受信部110と、リムーバブルHD10を装着するHDDドライブ120と、リムーバブルHD10からライセンス鍵情報を取得する鍵情報取得部130と、取得されたライセンス鍵情報に基づいて暗号化コンテンツデータを復号化する復号化処理部140と、コンテンツデータの復号化の処理の制御を行う復号化制御部150と、復号化されたコンテンツデータを所定の信号に変換し、外部装置に出力する出力処理部160と、を備え、受信されたまたはリムーバブルHD10に記録された暗号化コンテンツデータを復号化して図示しない外部装置に出力するようになっている。

- [0023] なお、本実施形態において、鍵情報取得部130、復号化处理部140および復号化制御部150は、バスBにより接続され、所定の操作にのみによってアクセスすることができる物理的に隔離された領域であるセキュア領域Rに配設されるようになっている。したがって、鍵情報取得部130において取得されたライセンス鍵情報は、当該セキュア領域Rより外部には、本実施形態におけるライセンス鍵の提供方法以外の方法では出力されることなく、また、復号化处理されたコンテンツデータは、復号された信号としては出力処理部160以外に出力されることはない。
- [0024] また、この情報記録再生装置100は、受信されたコンテンツデータの記録制御を行う記録制御部170と、復号化制御部150と連動し、暗号化コンテンツデータの再生制御を行う再生制御部180と、出力する映像信号に対してOSD(On screen Display)処理を行うOSD処理部190と、暗号化コンテンツデータの記録および再生を行うために各種の設定操作を行う操作部200と、各部を制御するシステム制御部210と、各部を制御する際に用いるROM/RAM220と、を有し、システム制御部210は、復号化制御部150を含む各部とバスBにより接続されている。
- [0025] なお、例えば、本実施形態のリムーバブルHD10は、本発明の第1記憶手段および変換手段を構成し、鍵情報取得部130は、第2記憶手段、受信手段および復元手段を構成する。また、例えば、本実施形態の復号化处理部140および出力処理部160は、本発明の再生手段を構成する。さらに、例えば、本実施形態のシステム制御部210は、本発明の送信制御制御手段を構成する。
- [0026] TV受信部110は、アンテナATを介して各放送局から送信された放送波、例えば、BS(Broadcasting Satellite)デジタル放送などの所定のデジタル形式を有する放送波を受信するようになっており、ユーザの選択した受信帯域に同調して受信された信号波を暗号化コンテンツデータに復調し、復調された暗号化コンテンツデータをHDドライブ120または復号化处理部140に出力するようになっている。
- [0027] HDドライブ120は、リムーバブルHD10を着脱可能にするための構造を有するとともに、例えば、iVDR(Information Versatile Disc for Removable usage)などの規格に準拠したHD用ドライブインターフェースを有している。また、このHDドライブ120は、再生制御部180または記録制御部170の制御の下、リムーバブルHD10から読み

出す暗号化コンテンツデータまたはライセンス鍵情報のデータに関する入出力の切り換え、および、それに伴うHDの記録再生の制御を行うようになっている。

[0028] また、本実施形態のHDドライブ120は、リムーバブルHD10からライセンス鍵情報を鍵情報取得部130に出力する際に、再生制御部180の制御の下、復号化制御部150と連動し、リムーバブルHD10に記憶されているライセンス鍵情報の暗号化を行わせつつ、鍵情報取得部130においてライセンス鍵情報を復号化することが可能な複数の情報(以下、暗号化情報または送信情報という。)を生成させ、生成された各暗号化情報を段階的に鍵情報取得部130に出力するようになっている。

[0029] なお、本実施形態のHDドライブ120の詳細については、特に、暗号化情報の生成および送信に関する処理(以下、暗号化情報送信処理という。)の詳細については、後述する。また、このHDドライブ120は、装着されたリムーバブルHD10にTV受信部110において受信された暗号化コンテンツデータを記録に関して所定の処理を行うようになっている。

[0030] 鍵情報取得部130には、復号化制御部150の制御の下、ライセンス鍵情報をリムーバブルHD10から取得する際に、HDドライブ120と連動しつつ、HDドライブ120から出力された複数の暗号化情報が順次入力されるようになっており、この鍵情報取得部130は、全ての暗号化情報を受信した後に、当該全ての暗号化情報を用いてライセンス鍵情報を生成するようになっている。そして、この鍵情報取得部130は、生成されたライセンス鍵情報を、復号化制御部150を介して復号化処理部140に出力するようになっている。

[0031] また、鍵情報取得部130は、内部に不揮発性メモリMを有し、暗号化情報その他の当該リムーバブルHD10から送信されたライセンス鍵情報の提供にあたり必要な情報を当該不揮発性メモリMに記憶するようになっている。

[0032] なお、本実施形態における復号化処理部140の詳細について、特に、暗号化情報の受信およびライセンス鍵情報の生成に関する処理(以下、暗号化情報受信処理という。)の詳細については、後述する。また、本実施形態では、上述の暗号化情報送信処理および暗号化情報受信処理を含めてライセンス鍵情報提供処理という。

[0033] 復号化処理部140には、HDドライブ120またはTV受信部110から出力された暗

号化コンテンツデータと、鍵情報取得部130において生成されたライセンス鍵情報と、が入力されるようになっている。この復号化処理部140は、復号化制御部150の制御の下、ライセンス鍵情報に基づいてTV受信部110から出力された、または、リムーバブルHD10から読み出された暗号化コンテンツデータを復号化するようになっており、復号化されたコンテンツデータを出力処理部160に出力するようになっている。

[0034] 復号化制御部150は、再生制御部180の制御の下、鍵情報取得部130および復号化処理部140の各部を制御するようになっている。具体的には、復号化制御部150は、鍵情報取得部130における暗号化情報の受信制御および暗号化情報に基づくライセンス鍵情報の生成制御と、復号化処理部140における暗号化コンテンツデータの復号化処理の制御を行うようになっている。

[0035] 出力処理部160には、復号化処理部140において復号化されたコンテンツデータが入力されるようになっており、この出力処理部160は、入力されたコンテンツデータを所定の信号に変換し、図示しない外部装置に出力するようになっている。

[0036] 具体的には、本実施形態の出力処理部160は、再生制御部180の制御の下、復号化されたコンテンツデータを音声データと映像データに分離するとともに、これらの各データに対してデコード処理など所定の処理を行うことによって、コンテンツデータにおける映像データおよび音声データを生成するようになっている。また、この出力処理部160は、デコードされた映像データおよび音声データをNTSC形式の信号形式に変換するとともに、当該変換された映像信号に対して、OSD処理部190によって生成され、入力された表示データを重畳するようになっている。そして、この出力処理部160は、表示データが重畳された映像信号および信号形式が変換された音声信号を映像信号出力端子T1および音声信号出力端子T2を介して接続された図示しない外部装置に出力するようになっている。

[0037] なお、例えば、本実施形態では、音声を拡声する機能を有するモニタが外部装置として接続されるようになっており、出力処理部160から出力された映像信号または音声信号は、当該モニタによって拡声され、および、表示させるようになっている。

[0038] 記録制御部170は、システム制御部210を介して操作部200から入力された記録指示が入力されるようになっており、この記録制御部170は、システム制御部210の

制御の下、入力された記録指示に基づいて、HDドライブ120を制御し、リムーバブルHD10にTV受信部110から出力された暗号化コンテンツデータを記録するようになっている。

- [0039] 再生制御部180には、システム制御部210を介して操作部200から入力された再生指示が入力されるようになっており、この再生制御部180は、システム制御部210の制御の下、入力された再生指示に基づいてTV受信部110、HDドライブ120、復号化制御部150および出力処理部160を制御し、ライセンス鍵情報の取得制御を行い、暗号化コンテンツデータを復号化して再生させる再生制御を行うようになっている。
- [0040] 特に、この再生制御部180は、HDドライブ120および復号化制御部150を連動させ、リムーバブルHD10に記憶されているライセンス鍵情報を鍵情報取得部130に転送させるためのライセンス鍵情報提供処理の制御、当該取得させたライセンス鍵情報に基づいて、暗号化コンテンツデータを復号化処理させる制御、および、復号化されたコンテンツデータを所定の信号に変換させ外部装置へ出力させる制御の各制御を行うようになっている。
- [0041] なお、本実施形態の再生制御部180におけるライセンス鍵情報提供処理を含むコンテンツデータの再生開始を行うための処理(以下、再生開始処理という。)の動作の詳細については後述する。
- [0042] OSD処理部190は、再生制御部180の制御の下、文字情報等の外部装置に出力される映像信号に対して重畳するための表示データを生成し、当該生成された文字情報などの表示データを出力処理部160に出力するようになっている。
- [0043] 操作部200は、各種確認ボタン、選択ボタンおよび数字キー等の多数のキーを有するリモートコントロール装置および当該リモートコントロール装置から送信された信号を受光する受光部、または、各種確認ボタン、選択ボタンおよび数字キー等の多数のキーを有する操作パネルにより構成されている。そして、この操作部200は、コンテンツデータの受信、リムーバブルHD10への当該コンテンツデータの記録または当該リムーバブルHD10に記録されたコンテンツデータの再生を行う際の各種の指示のために用いられるようになっている。

- [0044] システム制御部210は、受信装置用ROM／RAM220に格納される制御プログラムを読み出して各処理を実行するとともに、当該ROM／RAM220に処理中のデータを一時的に保持するようになっており、TV受信部110において受信された、または、HDドライブ120に装着されたリムーバブルHD10に記録された暗号化コンテンツデータの再生制御、および、HDドライブ120に装着されたリムーバブルHD10に暗号化コンテンツデータを記録する暗号化コンテンツデータの記録制御を行うようになっている。特に、本実施形態のシステム制御部210は、再生制御部180を制御しつつ、復号化コンテンツデータの再生にあたり、ライセンス鍵情報提供処理の制御を統括的に行うようになっている。
- [0045] 次に、図2および図3を用いて、本実施形態のHDドライブ120および鍵情報取得部130のライセンス鍵情報の提供処理について説明する。なお、図2は、本実施形態におけるライセンス鍵情報の提供処理を説明するための図であり、図3は、本実施形態のリムーバブルHD10および鍵情報取得部130におけるライセンス鍵情報の存在と再生可能状態を示す表である。
- [0046] 本実施形態のHDドライブ120は、リムーバブルHD10から鍵情報取得部130にライセンス鍵情報を送信する際に、リムーバブルHD10を制御し、
- (1) 鍵情報取得部130との認証制御(状態1)、
 - (2) 乱数の発生制御(乱数情報の生成制御(状態2))、
 - (3) ライセンス鍵情報の暗号化制御(状態3)、
 - (4) 暗号化されたライセンス鍵情報の送信制御および削除制御(状態4、状態5)
 - (5) 乱数情報の暗号化制御(状態6)
 - (6) 暗号化された乱数情報の送信制御および削除制御(状態7、状態8)を行い、
- リムーバブルHD10から鍵情報取得部130にライセンス鍵情報を暗号化させつつ、出力させるようになっている。ただし、上述のまたは後述するカッコ内の状態は図3における各状態を示す。
- [0047] 具体的には、HDドライブ120は、図2に示すように、再生制御部180の制御の下、復号化制御部150を介して鍵情報取得部130と連動し、リムーバブルHD10と当該鍵情報取得部130との認証を行わせるとともに、当該リムーバブルHD10に鍵情報

取得部130と共通するライセンス鍵情報とは異なる鍵情報(以下、共通鍵情報という。)を保持させるようになっている(状態1)。すなわち、HDドライブ120は、リムーバブルHD10に鍵情報取得部130に格納された鍵情報と同一の鍵情報を共通鍵情報として保持させるようになっている。

[0048] また、このHDドライブ120は、リムーバブルHD10と鍵情報取得部130との認証が行われると、当該リムーバブルHD10内において、所定の処理に基づいて乱数を発生させるようになっており(状態2)、当該発生させた乱数に基づいて当該リムーバブルHD10に記憶されているライセンス鍵情報を所定の暗号化処理により暗号化させるようになっている(状態3)。そして、このHDドライブ120は、リムーバブルHD10から暗号化されたライセンス鍵情報(以下、暗号化鍵情報という。)を第1の暗号化情報として鍵情報取得部130に送信制御するようになっている(状態4)。

[0049] なお、本実施形態では、HDドライブ120は、リムーバブルHD10に暗号化鍵情報が生成されると暗号化鍵情報の基になったライセンス鍵情報を消滅させるようになっている。また、当該暗号化鍵情報が生成される際に、当該暗号化鍵情報は、リムーバブルHD10内に記憶されるとともに、発生させた乱数は、乱数情報として当該リムーバブルHD10内に記憶されるようになっている。

[0050] さらに、HDドライブ120は、暗号化鍵情報の送信の後に、鍵情報取得部130から暗号化鍵情報を受信した旨を示す受信確認情報が送信されてくると、リムーバブルHD10に当該リムーバブルHD10に記憶されている暗号化鍵情報を消去させるようになっている(状態5)。そして、このHDドライブ120は、リムーバブルHD10に、当該リムーバブルHD10内に記憶されている乱数情報を共通鍵情報に基づいて暗号化させ(状態6)、リムーバブルHD10から当該暗号化された乱数情報(以下、暗号化乱数情報という。)を鍵情報取得部130に送信制御するようになっている(状態7)。

[0051] 最後に、HDドライブ120は、暗号化乱数情報の送信の後に、鍵情報取得部130から暗号化乱数情報を受信した旨を示す受信確認情報が送信されてくると、リムーバブルHD10に当該リムーバブルHD10に記憶されている暗号化鍵情報を消去させるようになっている(状態8および状態9)。

[0052] 一方、鍵情報取得部130は、リムーバブルHD10からライセンス鍵情報を受信する

際に、

- (1)リムーバブルHD10との認証制御(状態1～状態3)、
- (2)暗号化鍵情報の受信(状態4～状態6)、
- (3)暗号化乱数情報の受信(状態7、状態8)、
- (4)暗号化乱数情報の復号化とライセンス鍵情報の復元(状態9)を行い、

リムーバブルHD10から送信された暗号化鍵情報を受信し、当該暗号化鍵情報を復号化し、ライセンス鍵情報の復元を行うようになっている。ただし、上述のまたは後述するかっこ内の状態は図3における各状態を示す。

[0053] 具体的には、鍵情報取得部130は、図2に示すように、復号化制御部150の制御の下、再生制御部180を介してHDDドライブ120と連動し、リムーバブルHD10との認証を行うようになっており、リムーバブルHD10と共通する共通鍵情報を内部の不揮発性メモリMに記憶するようになっている(状態1～状態3)。すなわち、鍵情報取得部130は、リムーバブルHD10に格納された鍵情報と同一の鍵情報を共通鍵情報として不揮発性メモリMに保持するようになっている。

[0054] また、この鍵情報取得部130は、リムーバブルHD10との認証が行われ、最初に送信されてきた暗号化鍵情報を受信すると、当該暗号化鍵情報を不揮発性メモリMに格納し、当該暗号化鍵情報を受信した旨を示す受信確認情報をリムーバブルHD10に送信するようになっている(状態4～状態6)。

[0055] なお、本実施形態では、リムーバブルHD10に送信する受信確認情報にてリムーバブルHD10に格納されている暗号化鍵情報の消去指示となる。また、鍵情報取得部130は、暗号化鍵情報を受信した際に、当該暗号化鍵情報を正確に受信していない場合には、受信確認情報を送信せず、再送指示または所定のエラー処理を行うようになっている。

[0056] さらに、鍵情報取得部130は、暗号化鍵情報の受信の後に、リムーバブルHD10から暗号化乱数情報が送信されてくると、当該暗号化乱数情報を不揮発性メモリMに格納し、当該暗号化乱数情報を受信した旨を示す受信確認情報をリムーバブルHD10に送信するようになっている(状態7、状態8)。

[0057] なお、本実施形態では、暗号化鍵情報を受信する際と同様に、リムーバブルHD1

0に送信する受信確認情報にてリムーバブルHD10に格納されている暗号化乱数情報の消去指示となる。また、鍵情報取得部130は、暗号化乱数情報を受信した際に、当該暗号化乱数情報を正確に受信していない場合には、受信確認情報を送信せず、再送指示または所定のエラー処理を行うようになっている。

[0058] 最後に、鍵情報取得部130は、暗号化乱数情報の受信の後に、当該暗号化乱数情報を共通化鍵情報に基づいて復号化するとともに、復号化された乱数情報に基づいて暗号化鍵情報を復号化し、ライセンス鍵情報を復元するようになっている(状態9)。そして、この鍵情報取得部130は、上述のように、復元されたライセンス鍵情報を復号化処理部140に出力するようになっている。

[0059] 本実施形態では、このようにリムーバブルHD10およびHDDドライブ120と鍵情報取得部130とが暗号化情報送信処理および暗号化情報受信処理を行うようになっている。すなわち、図3に示す表のように、リムーバブルHD10と鍵情報取得部130では、それぞれ、状態1～状態9において、ライセンス鍵情報(または暗号化鍵情報)、乱数情報(または暗号化鍵情報)および共通鍵情報の三種類の情報を同時に有することがないので、ライセンス鍵情報は常に一の装置でのみ存在することとなる。したがって、本実施形態では、リムーバブルHD10および鍵情報取得部130において、ライセンス鍵情報(暗号化されていない状態のライセンス鍵情報)が、それぞれ個々の部材に存在することがないので、一のライセンス鍵情報では、同時に複数のコンテンツデータを復号化することができないようになっている。

[0060] 次に、図4を用いて本実施形態の再生制御部180におけるライセンス鍵情報提供処理を含むコンテンツデータの再生開始処理の動作について説明する。なお、図4は、本実施形態の再生制御部180におけるコンテンツデータの再生開始処理の動作を示すフローチャートである。

[0061] 以下の動作において、予めリムーバブルHD10がHDDドライブ120に装着されるとともに、当該リムーバブルHD10には再生の対象となる暗号化コンテンツデータを復号化するライセンス鍵情報が記憶されているものとし、再生の対象となるコンテンツデータは予めリムーバブルHD10に記録されているものとする。

[0062] まず、操作部200を操作することによって、リムーバブルHD10に記録されたコンテ

ンツデータを再生すべきことが指示され、再生制御部180にシステム制御部210を介して当該指示が入力されると、当該再生制御部180は、当該指示を検出し(ステップS11)、当該再生制御部180は、HDドライブ120と復号化制御を連動させてライセンス鍵情報提供処理を実行する(ステップS12)。

[0063] 具体的には、再生制御部180は、HDドライブ120および復号化制御部150にライセンス鍵情報提供処理を実行する旨の指示を出力し、HDドライブ120および復号化処理部140は、当該指示に基づいて暗号化送信処理または暗号化受信処理の制御を開始する。

[0064] なお、本実施形態におけるHDドライブ120および復号制御部のライセンス鍵情報提供処理の動作、すなわち、暗号化送信処理部および暗号化受信処理部の詳細については、後述する。

[0065] 次いで、再生制御部180は、適正にライセンス鍵情報提供処理を行うことができたか否かを判断し(ステップS13)、適正にライセンス鍵情報提供処理を行うことができなかったと判断すると、再度、当該ライセンス鍵情報提供処理を行うか否かを判断する(ステップS14)。

[0066] このとき、再生制御部180は、OSD処理部190および出力処理部160を制御して、再度ライセンス鍵情報提供処理を行うか否かの表示を行い、操作部200にて入力された指示に基づいて当該判断を行う。

[0067] 次いで、再生制御部180が、再度、ライセンス鍵情報提供処理を行うと判断した場合には、当該再生制御部180は、ステップS12の処理に移行させ、ライセンス鍵情報提供処理を中止すると判断した場合には、コンテンツデータを再生させずに本動作を終了させる。

[0068] 一方、再生制御部180が、適正にライセンス鍵情報提供処理を行うことができた判断した場合には、当該再生制御部180は、復号化制御部150を介して復号化処理部140と、HDドライブ120を制御して、リムーバブルHD10に記憶されている暗号化コンテンツデータの再生開始の指示を行い(ステップS15)、本動作を終了させる。

[0069] なお、再生制御部180から各部に再生開始の指示が為されると、暗号化コンテンツデータの再生が実行される。具体的には、HDドライブ120が、リムーバブルHD10

から暗号化コンテンツデータを順次読み出すとともに復号処理部140に出力し、復号化処理部140は、入力された暗号化コンテンツデータを鍵情報取得部130が取得したライセンス鍵情報に基づいて順次復号処理を行う。また、出力処理部160は、復号化処理されたコンテンツデータを順次所定の映像信号および音信号に変換して外部装置に出力する。

[0070] 次に、図5および図6を用いて、本実施形態のHDドライブ120および復号化制御部150におけるライセンス鍵情報提供処理の動作について説明する。なお、図5および図6は、本実施形態のHDドライブ120および復号化制御部150におけるライセンス鍵情報提供処理の動作を示すフローチャートである。

[0071] 本動作では、ライセンス鍵情報を送信するリムーバブルHD10内における暗号化送信処理と、ライセンス鍵情報を受信する鍵情報取得部130における暗号化受信処理と、を各処理毎の動作として個々のフローチャートにて説明する。

[0072] また、本動作において、HDドライブ120および復号化制御部150は、再生制御部180の指示に基づいて暗号化送信処理および暗号化受信処理の制御を開始するものとし、暗号化送信処理を基準として各処理の説明を行う。

[0073] まず、HDドライブ120および復号化制御部150に、再生制御部180からのライセンス鍵情報提供処理を実行する旨の指示が入力されると、当該HDドライブ120および復号化制御部150は、互いに連動し、リムーバブルHD10と鍵情報取得部130の認証を実行させ(ステップS111、ステップS211)、リムーバブルHD10と鍵情報取得部130との認証が適正に実行された否かを判断する(ステップS112、ステップS212)。

[0074] このとき、HDドライブ120および復号化制御部150が、リムーバブルHD10と鍵情報取得部130の認証が適正に実行されていないと判断すると、当該HDドライブ120および復号化制御部150は、本動作を終了させる。

[0075] 一方、HDドライブ120および復号化制御部150が、リムーバブルHD10と鍵情報取得部130の認証が適正に実行されたことを判断すると、HDドライブ120および復号化制御部150は、リムーバブルHD10または鍵情報取得部130には共有鍵情報を保持させる(ステップS113、ステップS213)。

- [0076] このとき、復号化制御部150は、共有鍵情報を鍵情報取得部130内部の不揮発性メモリMに格納し、リムーバブルHD10から送信される暗号化鍵情報の受信待機を行う(ステップS214)。
- [0077] 次いで、HDドライブ120は、リムーバブルHD10に、所定の処理により乱数を乱数情報として当該リムーバブルHD10内にて発生させるとともに(ステップS114)、当該発生させた乱数情報に基づいてライセンス鍵情報を暗号化させ、暗号化鍵情報を暗号化情報として当該リムーバブルHD10内にて生成させる(ステップS115)。
- [0078] 次いで、HDドライブ120は、生成された暗号化鍵情報である暗号化情報をリムーバブルHD10から読み出して鍵情報取得部130に送信し、鍵情報取得部130から送信される受信確認情報の受信を待機する(ステップS116)。
- [0079] このとき、鍵情報取得部130がHDドライブ120を介してリムーバブルHD10から暗号化鍵情報を受信すると(ステップS215)、復号化制御部150は、当該鍵情報取得部130に受信された暗号化鍵情報の有効性を判断し(ステップS216)、有効でないと判断された場合に、復号化制御部150は本動作を終了させる。
- [0080] なお、復号化制御部150によって本動作が終了すると、再生制御部180は、当該終了の通知(以下、終了通知という。)を受け取り、当該終了通知に基づいてHDドライブ120の暗号化送信処理も強制的に終了させる。
- [0081] 一方、鍵情報取得部130が、受信された暗号化鍵情報が有効であると判断した場合には、復号化制御部150は、鍵情報取得部130に暗号化鍵情報を受信した旨を示す受信確認情報、すなわち、消去指示の情報(以下、消去指示情報という。)をHDドライブ120に送信させる(ステップS217)。
- [0082] 次いで、HDドライブ120は、鍵情報取得部130から送信された受信確認情報を受信すると(ステップS117)、HDドライブ120は、当該受信された受信確認情報が有効か否か、すなわち、鍵情報取得部130において有効に暗号化鍵情報の受信ができたか否かを判断し(ステップS118)、当該受信確認情報が有効でない場合には、本動作を終了させる。
- [0083] なお、HDドライブ120によって本動作が終了すると、再生制御部180は、当該終了通知を受け取り、当該終了通知に基づいて復号化制御部150の暗号化受信処理

も強制的に終了させる。

- [0084] 一方、HDドライブ120が、鍵情報取得部130にて適正に暗号化鍵情報が取得されたと判断すると、当該HDドライブ120は、リムーバブルHD10を制御して当該リムーバブルHD10に記憶されている暗号化鍵情報を消去させる(ステップS119)。
- [0085] 次いで、HDドライブ120は、リムーバブルHD10に、当該リムーバブルHD10に保持されている共通鍵情報に基づいてステップS114にて生成された乱数情報を暗号化させ、暗号化乱数情報を暗号化情報として当該リムーバブルHD10内にて生成させる(ステップS120)。
- [0086] 次いで、HDドライブ120は、生成された暗号化乱数情報である暗号化情報をリムーバブルHD10から読み出して鍵情報取得部130に送信し、鍵情報取得部130から送信される受信確認情報の受信を待機する(ステップS121)。
- [0087] このとき、鍵情報取得部130がHDドライブ120を介してリムーバブルHD10から暗号化乱数情報を受信すると(ステップS218)、復号化制御部150は、当該鍵情報取得部130に受信された暗号化乱数情報の有効性を判断し(ステップS219)、有効でないと判断された場合に、復号化制御部150は本動作を終了させる。
- [0088] なお、復号化制御部150によって本動作が終了すると、上述のステップS215の処理と同様に、再生制御部180は、終了通知を受け取り、当該終了通知に基づいてHDドライブ120の暗号化送信処理も強制的に終了させる。
- [0089] 次いで、鍵情報取得部130が、受信された暗号化乱数情報が有効であると判断した場合には、復号化制御部150は、当該鍵情報取得部130に、暗号化乱数情報を受信した旨を示す受信確認情報をHDドライブ120に送信させる(ステップS220)。
- [0090] 次いで、HDドライブ120は、鍵情報取得部130から送信された受信確認情報を受信すると(ステップS122)、HDドライブ120は、当該受信された受信確認情報が有効か否か、すなわち、鍵情報取得部130において有効に暗号化鍵情報の受信ができたか否かを判断し(ステップS123)、当該受信確認情報が有効でない場合には、本動作を終了させる。
- [0091] なお、HDドライブ120によって本動作が終了すると、再生制御部180は、当該終了通知を受け取り、当該終了通知に基づいて復号化制御部150の暗号化受信処理

も強制的に終了させる。

- [0092] 次いで、HDドライブ120が、鍵情報取得部130にて適正に暗号化乱数情報が取得されたと判断すると、当該HDドライブ120は、リムーバブルHD10を制御して当該リムーバブルHD10に記憶されている暗号化乱数情報を消去させ(ステップS124)、本動作を終了させる。
- [0093] 他方、復号化制御部150は、鍵情報取得部130に、受信された暗号化乱数情報および暗号化鍵情報を復号化させるとともに(ステップS221)、当該復号化されたライセンス鍵情報の有効性を判断させ(ステップS222)、当該復号化されたライセンス鍵情報が有効でないと判断された場合に、復号化制御部150は本動作を終了させる。
- [0094] なお、復号化制御部150によって本動作が終了すると、再生制御部180は、当該終了通知を受け取り、当該終了通知に基づいてHDドライブ120の暗号化送信処理も強制的に終了させる。
- [0095] 一方、鍵情報取得部130が復号化されたライセンス鍵情報が有効であると判断すると、復号化制御部150は、ライセンス鍵情報提供処理が適正に終了した旨を再生制御部180に通知し(ステップS223)、本動作を終了させる。
- [0096] 以上本実施形態によれば、情報記録再生装置100は、暗号化されたコンテンツデータを復号するための鍵情報を記憶するリムーバブルHD10から当該リムーバブルHD10とは異なる鍵情報取得部130に提供するライセンス鍵情報提供処理を行う場合であって、ライセンス鍵情報を暗号化する際に用いる複数の暗号化情報を生成する生成処理と、生成された各暗号化情報を他の暗号化情報と異なるタイミングにて段階的にリムーバブルHD10から鍵情報取得部130に順次送信する送信処理と、鍵情報取得部130にて送信された各暗号化情報を順次受信する受信処理と、鍵情報取得部130にて全ての暗号化情報を受信した後に、当該全ての暗号化情報を用いてライセンス鍵情報を生成する生成処理と、を含み、送信処理においては、リムーバブルHD10が一の暗号化情報を送信した後であって、未だ情報取得部に送信されていない他の暗号化情報を送信する前に、当該送信された暗号化情報を消去する構成を有している。
- [0097] この構成により、本実施形態の情報記録再生装置100は、生成された各暗号化情

報を他の暗号化情報と異なるタイミングにて段階的にリムーバブルHD10から鍵情報取得部130に順次送信するとともに、鍵情報取得部130にて送信された各暗号化情報を順次受信し、鍵情報取得部130にて全ての暗号化情報が受信された後に、当該全ての暗号化情報を用いてライセンス鍵情報を生成する。そして、本実施形態の情報記録再生装置100は、リムーバブルHD10が一の暗号化情報が送信された後であって、未だ鍵情報取得部130に送信されていない他の暗号化情報が送信される前に、当該送信された暗号化情報を消去する。

[0098] したがって、本実施形態のライセンス鍵情報提供処理では、暗号化コンテンツデータを部材間において転送する場合であっても、各部材にて暗号化コンテンツデータと当該暗号化コンテンツデータを復号するためのライセンス鍵情報と同時に存在することがないので、すなわち、暗号化コンテンツデータとライセンス鍵情報が同時に存在する部材は常に一つであるので、一つライセンス鍵情報からは常に一の暗号化コンテンツデータの再生のみ可能となる。

[0099] また、例えば、図7に示すライセンス鍵情報を提供する方法であっては、認証により共通鍵情報の共有が行われた後に、共通鍵情報にてライセンス鍵情報を暗号化して送信し、当該暗号化されたライセンス鍵情報の送信後に、当該ライセンス鍵情報を消去するようになっているので、当該ライセンス鍵情報が消去される直前には、または、不正行為によりライセンス鍵情報が消去されなければ、複数の部材においてそれぞれ暗号化されたコンテンツデータを復号化することができてしまう。なお、図7は、共有鍵情報に基づいてライセンス鍵情報を暗号化して転送する処理を説明するための図(I)である。

[0100] さらに、例えば、図8に示すライセンス鍵情報を提供する方法であっては、認証により共通鍵情報の共有が行われた後に、共通鍵情報にてライセンス鍵情報を暗号化して送信し、当該暗号化されたライセンス鍵情報の送信後に、提供された側の部材からの受信の有無に関係なく、当該ライセンス鍵情報を消去するようになるので、暗号化されたライセンス鍵情報の転送中に転送処理が中止に成った場合、または、転送される側の部材が適切にライセンス鍵情報を受信することができなかった場合には、各部材の情報を集約したとしてもライセンス鍵情報の復号化を行うことができない。な

お、図8は、共有鍵情報に基づいてライセンス鍵情報を暗号化して転送する処理を説明するための図(II)である。

- [0101] 一方、例えば、超流通システムに関する規定の一つであるARIB (Association of Radio Industries and Business／社団法人電波産業会)にてデジタル放送におけるコンテンツ保護規定により策定されている規格 (ARIB Technical Report B-15) では、コンテンツデータのムーブ (転送記録) に関して、ムーブ処理の途中において、ムーブ処理におけるコンテンツデータを転送する側 (ムーブ元) および当該ムーブ処理におけるコンテンツデータが転送される側 (ムーブ先) の双方の装置に同時に、所定の時間、すなわち、1分を越える時間的長さを有するコンテンツデータが再生可能な状態であってはならないことが規定されている。このため、図7および図8に示すライセンス鍵情報を提供する方法など、この条件を満たさない提供方法では、超流通システムを構築することができない。
- [0102] 一方、本実施形態のライセンス鍵情報提供処理では、上述のように、暗号化コンテンツデータとライセンス鍵情報が同時に存在する部材は常に一つであるので、転送側および転送される側の双方の部材に同時に、暗号化コンテンツデータを復号可能なライセンス鍵情報が存在しないこととなり、当該規格を満たすこととなる。
- [0103] 以上のように、本実施形態のライセンス鍵情報提供処理では、一つライセンス鍵情報からは常に一の暗号化コンテンツデータの再生のみ可能となるとともに、ライセンス鍵情報の転送中の障害に強く、さらに、上述の超流通システムに代表される著作権保護を強固に行うシステムにおいても条件を満たすことができるので、的確にライセンス鍵情報の授受を行うことができるとともに、コンテンツデータの著作権保護を強固にかつ的確に行うことができる。
- [0104] なお、本実施形態の情報記録再生装置100は、ライセンス鍵情報提供処理において、リムーバブルHD10と鍵情報取得部130間において単に暗号化鍵情報および暗号化乱数情報の授受を行うようになっているが、各暗号化情報の転送におけるセキュリティを高めるために、各暗号化情報の送受信および受信確認情報の送受信に関して、各情報が発信者から発信され、途中で改ざんなどが行なわれていないことを示すためのデジタル署名の方法を用いるようにしてもよい。

- [0105] この場合には、図9に示すように各暗号化情報および受信確認情報の送信時に、リムーバブルHD10または鍵情報取得部130は、当該リムーバブルHD10または鍵情報取得部130におけるデジタル署名を署名情報として生成して添付し、各情報の受信後に当該添付された署名情報を用いて情報を送信したリムーバブルHD10または鍵情報取得部130の署名を検証する。そして、デジタル署名が承認された場合に、当該各情報を受信したリムーバブルHD10または鍵情報取得部130デジタル署名を署名情報として生成して添付する。
- [0106] また、本実施形態の情報記録再生装置100には、ライセンス鍵情報がリムーバブルHD10にて提供されるようになっているが、DVDなどのその他の可搬型記録媒体によって提供されるようにしてもよい。
- [0107] また、本実施形態の情報記録再生装置100には、ライセンス鍵情報がリムーバブルHD10にて提供されるようになっているが、インターネットなどの通信回線を介して、パーソナルコンピュータやハードディスクレコーダなどの他の情報再生装置、または、情報記録再生装置100から提供されるようにしてもよい。
- [0108] この場合に、ライセンス鍵情報を提供する情報記録装置は、通信回線を介して暗号化鍵情報および暗号化乱数情報を順次段階的にライセンス鍵情報を提供する装置に送信しつつ、消去する。
- [0109] 〔第2実施形態〕
次に、図10～図14を用いて本願に係る情報記録再生装置の第2実施形態について説明する。
- [0110] 本実施形態では、第1実施形態におけるライセンス鍵情報転送処理において、乱数情報を用いてライセンス鍵情報を送信する点に代えて、ライセンス鍵情報から当該ライセンス鍵情報を一意に決定する複数の鍵情報に分散し、当該分散された鍵情報（以下、分散鍵情報という。）を用いてライセンス鍵情報を提供する点に特徴がある。その他の構成は、第1実施形態と同様であり、同一の部材には同一番号を付してその説明を省略するとともに、本実施形態におけるライセンス鍵情報提供処理の前提となる再生開始処理は、第1実施形態と同様の動作となるため、その説明を省略する。
- [0111] なお、本実施形態では、ライセンス鍵情報転送処理における分割鍵情報を生成す

る方法として、秘密分散法と呼ばれる情報分割方式を用いる。

[0112] まず、図10および図11を用いて本実施形態のライセンス鍵情報転送処理において用いる秘密分散処理について説明する。なお、図10および図11は、本実施形態のライセンス鍵情報転送処理において用いる秘密分散処理を説明するための図である。

[0113] 秘密分散処理とは、ライセンス鍵情報を複数の分散情報に符号化する処理をいい、この秘密分散処理は、分散された各分散情報一つ一つから全体の情報、すなわち、ライセンス鍵情報を知ることはできないようになっており、ライセンス鍵情報の漏洩等から高い安全性を維持できるようになっている。

[0114] 例えば、図10に示すように、 $X-Y$ 平面上の直線の方程式($y=ax+b$)を算出の対象となる情報とすると、各座標の情報からは、直線の方程式を算出することができない。例えば、 (x_1, y_1) からは($y=ax+b$)を算出することができない。しかしながら、2点の座標、例えば、 (x_1, y_1) (x_3, y_3) からは($y=ax+b$)を算出することができる。すなわち、 $X-Y$ 平面上の直線($y=ax+b$)の情報は、2点以上の座標の情報から算出することができる。したがって、ライセンス鍵情報が $X-Y$ 平面上の直線($y=ax+b$)の情報とすると、複数の座標情報を分散情報として生成すれば、各分散情報ではライセンス鍵情報を算出することができないが、複数の分散情報を取得すれば、ライセンス鍵情報を算出すること、すなわち、ライセンス鍵情報を復元することができるようになっている。

[0115] 本実施形態では、この原理を用いてライセンス鍵情報に秘密分散処理(分散)を行うとともに、当該ライセンス鍵情報を復元する際には、当該各分散情報を取得し、当該各分散情報に基づいて秘密分散処理(統合)を行い、ライセンス鍵情報を復元する際に必要となる情報を他の部材に提供するようになっている。

[0116] なお、図11は、ライセンス鍵情報が $X-Y$ 平面上の2次曲線の方程式($y=ax^2+bx+c$)の情報とした場合の秘密分散処理を説明するための図であり、この場合には、3点以上の座標情報から当該2次曲線の方程式($y=ax^2+bx+c$)、すなわち、ライセンス鍵情報を復元することができることを示している。

[0117] また、本実施形態では、符号化された各分散情報に対して共通鍵情報に基づいて

更に暗号化するようになっており、ライセンス鍵情報の漏洩を高度に防止するようになっている。

- [0118] 次に、図12および図13を用いて、本実施形態のHDドライブ120および鍵情報取得部130のライセンス鍵情報の提供処理について説明する。なお、図12は、本実施形態におけるライセンス鍵情報の提供処理を説明するための図であり、図13は、本実施形態のリムーバブルHD10および鍵情報取得部130におけるライセンス鍵情報の存在と再生可能状態を示す表である。
- [0119] 本実施形態のHDドライブ120は、第1実施形態と同様に、リムーバブルHD10からHDライセンス鍵情報を鍵情報取得部130に出力する際に、再生制御部180の制御の下、復号化制御部150と連動し、リムーバブルHD10に記憶されているライセンス鍵情報を所定の処理により複数の情報、すなわち、分散情報を生成させ、当該各分散情報に対して暗号化を行わせつつ、鍵情報取得部130においてライセンス鍵情報を復号化するために必要な複数の暗号化情報を生成させ、生成された各暗号化情報を段階的に鍵情報取得部130に出力するようになっている。
- [0120] 本実施形態のHDドライブ120は、リムーバブルHD10から鍵情報取得部130にライセンス鍵情報を送信する際に、リムーバブルHD10を制御し、
- (1) 鍵情報取得部130との認証制御(状態1)、
 - (2) ライセンス鍵情報を秘密分散処理(分散)によって二つの鍵情報に分割させ、二つの鍵情報の生成を行わせる生成制御(状態2)、
 - (3) 分割された第1の鍵情報(以下、第1鍵情報という。)の暗号化制御(状態3)、
 - (4) 暗号化された第1鍵情報(以下、暗号化第1鍵情報という。)の送信制御および削除制御(状態4、状態5)
 - (5) 分割された第2の鍵情報(以下、第2鍵情報という。)の暗号化制御(状態6)、
 - (6) 暗号化された第2鍵情報(以下、暗号化第2鍵情報という。)の送信制御および削除制御(状態7、状態8)を行い、
- リムーバブルHD10から鍵情報取得部130にライセンス鍵情報を暗号化させつつ、出力させるようになっている。ただし、上述のまたは後述するカッコ内の状態は図13における各状態を示す。

- [0121] 具体的には、HDドライブ120は、図12に示すように、再生制御部180の制御の下、復号化制御部150を介して鍵情報取得部130と連動し、リムーバブルHD10と当該鍵情報取得部130との認証を行わせるとともに、当該リムーバブルHD10に鍵情報取得部130と共通する共通鍵情報を保持させるようになっている(状態1)。
- [0122] また、このHDドライブ120は、リムーバブルHD10と鍵情報取得部130との認証が行われると、当該リムーバブルHD10内において、ライセンス鍵情報に対して秘密分散処理(分散)を行い、ライセンス鍵情報から第1鍵情報と第2鍵情報を生成するようになり(状態2)、共通鍵情報に基づいて当該生成された第1鍵情報を所定の暗号化処理により暗号化させるようになっている(状態3)。そして、このHDドライブ120は、リムーバブルHD10から暗号化された第1鍵情報である暗号化第1鍵情報を第1の暗号化情報として鍵情報取得部130に送信制御するようになっている(状態4)。
- [0123] さらに、HDドライブ120は、暗号化第1鍵情報の送信の後に、鍵情報取得部130から暗号化第1鍵情報を受信した旨を示す受信確認情報が送信されてくると、リムーバブルHD10に当該リムーバブルHD10に記憶されている暗号化第1鍵情報を消去させるようになっている(状態5)。そして、このHDドライブ120は、リムーバブルHD10に、当該リムーバブルHD10内に記憶されている第2鍵情報を共通鍵情報に基づいて暗号化させ(状態6)、リムーバブルHD10から当該暗号化された第2鍵情報である暗号化第2鍵情報を鍵情報取得部130に送信制御するようになっている(状態7)。
- [0124] 最後に、HDドライブ120は、暗号化第2鍵情報の送信の後に、鍵情報取得部130から暗号化第2鍵情報を受信した旨を示す受信確認情報が送信されてくると、リムーバブルHD10に当該リムーバブルHD10に記憶されている暗号化第2鍵情報を消去させるようになっている(状態8および状態9)。
- [0125] 一方、本実施形態の鍵情報取得部130には、第1実施形態と同様に、復号化制御部150の制御の下、ライセンス鍵情報をリムーバブルHD10から取得する際に、HDドライブ120と連動しつつ、HDドライブ120から出力された複数の暗号化情報が順次入力されるようになっており、この鍵情報取得部130は、全ての暗号化情報を受信

した後に、当該全ての暗号化情報を用いてライセンス鍵情報を生成するようになっている。そして、この鍵情報取得部130は、生成されたライセンス鍵情報を、復号化制御部150を介して復号化処理部140に出力するようになっている。

[0126] また、鍵情報取得部130は、内部に不揮発性メモリMを有し、暗号化情報その他の当該リムーバブルHD10から送信されたライセンス鍵情報の提供にあたり必要な情報を当該不揮発性メモリMに記憶するようになっている。

[0127] 本実施形態の鍵情報取得部130は、リムーバブルHD10からライセンス鍵情報を受信する際に、

- (1)リムーバブルHD10との認証制御(状態1～状態3)、
- (2)暗号化第1鍵情報の受信(状態4～状態6)、
- (3)暗号化第2鍵情報の受信(状態7、状態8)、および、
- (4)暗号化第1鍵情報および暗号化第2鍵情報の復号化とライセンス鍵情報の復元(状態9)を行い、

リムーバブルHD10から送信された暗号化第1鍵情報および暗号化第2鍵情報を受信し、当該ライセンス鍵情報の復元を行うようになっている。ただし、上述のまたは後述するかっこ内の状態は図13における各状態を示す。

[0128] 具体的には、鍵情報取得部130は、図12に示すように、復号化制御部150の制御の下、再生制御部180を介してHDドライブ120と連動し、リムーバブルHD10との認証を行うようになっており、リムーバブルHD10と共通する共通鍵情報を内部の不揮発性メモリMに記憶するようになっている(状態1～状態3)。すなわち、鍵情報取得部130は、リムーバブルHD10に格納された鍵情報と同一の鍵情報を共通鍵情報として不揮発性メモリMに保持するようになっている。

[0129] また、この鍵情報取得部130は、リムーバブルHD10との認証が行われ、最初に送信されてきた暗号化第1鍵情報を受信すると、当該暗号化第1鍵情報を不揮発性メモリMに格納し、当該暗号化第1鍵情報を受信した旨を示す受信確認情報をリムーバブルHD10に送信するようになっている(状態4～状態6)。

[0130] なお、本実施形態では、リムーバブルHD10に送信する受信確認情報にてリムーバブルHD10に格納されている暗号化第1鍵情報の消去指示となる。また、鍵情報

取得部130は、暗号化第1鍵情報を受信した際に、当該暗号化第1鍵情報を正確に受信していない場合には、受信確認情報を送信せず、再送指示または所定のエラー処理を行うようになっている。

[0131] さらに、鍵情報取得部130は、暗号化第1鍵情報の受信の後に、リムーバブルHD10から暗号化第2鍵情報が送信されてくると、当該暗号化第2鍵情報を不揮発性メモリMに格納し、当該暗号化第2鍵情報を受信した旨を示す受信確認情報をリムーバブルHD10に送信するようになっている(状態7、状態8)。

[0132] なお、本実施形態では、暗号化第1鍵情報を受信する際と同様に、リムーバブルHD10に送信する受信確認情報にてリムーバブルHD10に格納されている暗号化第2鍵情報の消去指示となる。また、鍵情報取得部130は、暗号化第2鍵情報を受信した際に、当該暗号化第2鍵情報を正確に受信していない場合には、受信確認情報を送信せず、再送指示または所定のエラー処理を行うようになっている。

[0133] 最後に、鍵情報取得部130は、暗号化第2鍵情報の受信の後に、暗号化第1鍵情報および暗号化第2鍵情報をそれぞれ共通化鍵情報に基づいて復号化するとともに(状態9)、復号化された第1鍵情報および第2鍵情報に基づいて秘密分散処理を行い、ライセンス鍵情報を復元するようになっている(状態9)。そして、この鍵情報取得部130は、上述のように、復元されたライセンス鍵情報を復号化処理部140に出力するようになっている。

[0134] 本実施形態では、このようにリムーバブルHD10およびHDDドライブ120と鍵情報取得部130とが暗号化情報送信処理および暗号化情報受信処理を行うようになっている。すなわち、図13に示す表のように、リムーバブルHD10と鍵情報取得部130では、状態1～状態10において、第1鍵情報(または暗号化第1鍵情報)、第2鍵情報(または暗号化第2鍵情報)および共通鍵情報の三種類の情報を同時に有することがないので、ライセンス鍵情報は常に一の装置でのみ存在することとなる。したがって、本実施形態では、リムーバブルHD10および鍵情報取得部130において、ライセンス鍵情報(暗号化されていない状態のライセンス鍵情報)が、それぞれ個々に存在することがないので、一のライセンス鍵情報では、同時に複数のコンテンツデータを復号化することができないようになっている。

- [0135] 次に、図14および図15を用いて、本実施形態のHDドライブ120および復号化制御部150におけるライセンス鍵情報提供処理の動作について説明する。なお、図14および図15は、本実施形態のHDドライブ120および復号化制御部150におけるライセンス鍵情報提供処理の動作を示すフローチャートである。
- [0136] 本動作では、第1実施形態と同様に、ライセンス鍵情報を送信するリムーバブルHD10内における暗号化送信処理と、ライセンス鍵情報を受信する鍵情報取得部130における暗号化受信処理と、各処理毎の動作として個々のフローチャートにて説明する。
- [0137] また、本動作において、HDドライブ120および復号化制御部150は、再生制御部180の指示に基づいて暗号化送信処理および暗号化受信処理の制御を開始するものとし、暗号化送信処理を基準として各処理の説明を行う。
- [0138] まず、HDドライブ120および復号化制御部150に、再生制御部180からのライセンス鍵情報提供処理を実行する旨の指示が入力されると、当該HDドライブ120および復号化制御部150は、互いに連動し、リムーバブルHD10と鍵情報取得部130の認証を実行させ(ステップS311、ステップS411)、リムーバブルHD10と鍵情報取得部130との認証が適正に実行された否かを判断する(ステップS312、ステップS412)。
- [0139] このとき、HDドライブ120および復号化制御部150が、リムーバブルHD10と鍵情報取得部130の認証が適正に実行されていないと判断すると、当該HDドライブ120および復号化制御部150は、本動作を終了させる。
- [0140] 一方、HDドライブ120および復号化制御部150が、リムーバブルHD10と鍵情報取得部130の認証が適正に実行されたことを判断すると、HDドライブ120および復号化制御部150は、リムーバブルHD10または鍵情報取得部130には共有鍵情報を保持させる(ステップS313、ステップS413)。
- [0141] このとき、復号化制御部150は、共有鍵情報を内部の不揮発性メモリMに格納し、リムーバブルHD10から送信される暗号化鍵情報の受信待機を行う(ステップS414)。
- [0142] 次いで、HDドライブ120は、リムーバブルHD10に、秘密分散処理を実行させ、ラ

イセンス鍵情報から第1鍵情報および第2鍵情報を生成させるとともに(ステップS314)、共通鍵情報に基づいて第1鍵情報を暗号化させ、第1鍵情報を暗号化情報として当該リムーバブルHD10内にて生成させる(ステップS315)。なお、このとき、リムーバブルHD10は、第1鍵情報および第2鍵情報を生成した後に、秘密分散処理の基になったライセンス鍵情報を消去する。

[0143] 次いで、HDドライブ120は、生成された暗号化第1鍵情報である暗号化情報をリムーバブルHD10から読み出して鍵情報取得部130に送信し、鍵情報取得部130から送信される受信確認情報の受信を待機する(ステップS316)。

[0144] このとき、鍵情報取得部130がHDドライブ120を介してリムーバブルHD10から暗号化第1鍵情報を受信すると(ステップS415)、復号化制御部150は、当該鍵情報取得部130に受信された暗号化第1鍵情報の有効性を判断し(ステップS416)、有効でないと判断された場合に、復号化制御部150は本動作を終了させる。

[0145] なお、復号化制御部150によって本動作が終了すると、再生制御部180は、当該終了の通知(以下、終了通知という。)を受け取り、当該終了通知に基づいてHDドライブ120の暗号化送信処理も強制的に終了させる。

[0146] 一方、鍵情報取得部130が、受信された暗号化第1鍵情報が有効であると判断した場合には、復号化制御部150は、鍵情報取得部130に暗号第1化鍵情報を受信した旨を示す受信確認情報、すなわち、消去指示情報をHDドライブ120に送信させる(ステップS417)。

[0147] 次いで、HDドライブ120は、鍵情報取得部130から送信された受信確認情報を受信すると(ステップS317)、HDドライブ120は、当該受信された受信確認情報が有効か否か、すなわち、鍵情報取得部130において有効に暗号化鍵情報の受信ができたか否かを判断し(ステップS318)、当該受信確認情報が有効でない場合には、本動作を終了させる。

[0148] なお、HDドライブ120によって本動作が終了すると、再生制御部180は、当該終了通知を受け取り、当該終了通知に基づいて復号化制御部150の暗号化受信処理も強制的に終了させる。

[0149] 一方、HDドライブ120が、鍵情報取得部130にて適正に暗号化第1鍵情報が取得

されたと判断すると、当該HDドライブ120は、リムーバブルHD10を制御して当該リムーバブルHD10に記憶されている暗号化第1鍵情報を消去させる(ステップS319)。

[0150] 次いで、HDドライブ120は、リムーバブルHD10に、当該リムーバブルHD10に保持されている共通鍵情報に基づいてステップS114にて生成された第2鍵情報を暗号化させ、暗号化第2情報を暗号化情報として当該リムーバブルHD10内にて生成させる(ステップS320)。

[0151] 次いで、HDドライブ120は、生成された暗号化第2鍵情報である暗号化情報をリムーバブルHD10から読み出して鍵情報取得部130に送信し、鍵情報取得部130から送信される受信確認情報の受信を待機する(ステップS321)。

[0152] このとき、鍵情報取得部130がHDドライブ120を介してリムーバブルHD10から暗号化第2鍵情報を受信すると(ステップS418)、復号化制御部150は、当該鍵情報取得部130に受信された暗号化第2鍵情報の有効性を判断し(ステップS419)、有効でないと判断された場合に、復号化制御部150は本動作を終了させる。

[0153] なお、復号化制御部150によって本動作が終了すると、上述のステップS415の処理と同様に、再生制御部180は、終了通知を受け取り、当該終了通知に基づいてHDドライブ120の暗号化送信処理も強制的に終了させる。

[0154] 次いで、鍵情報取得部130が、受信された暗号化第2鍵情報が有効であると判断した場合には、復号化制御部150は、当該鍵情報取得部130に、暗号化第2鍵情報を受信した旨を示す受信確認情報、をHDドライブ120に送信させる(ステップS420)。

[0155] 次いで、HDドライブ120は、鍵情報取得部130から送信された受信確認情報を受信すると(ステップS322)、HDドライブ120は、当該受信された受信確認情報が有効か否か、すなわち、鍵情報取得部130において有効に暗号化第2鍵情報の受信ができたか否かを判断し(ステップS323)、当該受信確認情報が有効でない場合には、本動作を終了させる。

[0156] なお、HDドライブ120によって本動作が終了すると、再生制御部180は、当該終了通知を受け取り、当該終了通知に基づいて復号化制御部150の暗号化受信処理

も強制的に終了させる。

- [0157] 次いで、HDドライブ120が、鍵情報取得部130にて適正に暗号化第2鍵情報が取得されたと判断すると、当該HDドライブ120は、リムーバブルHD10を制御して当該リムーバブルHD10に記憶されている暗号化第2鍵情報を消去させ(ステップS324)、本動作を終了させる。
- [0158] 他方、復号化制御部150は、鍵情報取得部130に、受信された暗号化第1鍵情報および暗号化第2鍵情報を共通鍵情報に基づいて復号化させるとともに(ステップS421)、当該復号化された第1鍵情報および第2鍵情報を用いて秘密分散処理における統合処理を行い、ライセンス鍵情報を復元する(ステップS422)。
- [0159] 次いで、復号化制御部150は、鍵情報取得部130に、復元されたライセンス鍵情報の有効性を判断させ(ステップS423)、当該復号化されたライセンス鍵情報が有効でないと判断された場合に、復号化制御部150は本動作を終了させる。
- [0160] なお、復号化制御部150によって本動作が終了すると、再生制御部180は、当該終了通知を受け取り、当該終了通知に基づいてHDドライブ120の暗号化送信処理も強制的に終了させる。
- [0161] 一方、鍵情報取得部130が復号化されたライセンス鍵情報が有効であると判断すると、復号化制御部150は、ライセンス鍵情報提供処理が適正に終了した旨を再生制御部180に通知し(ステップS424)、本動作を終了させる。
- [0162] 以上本実施形態によれば、情報記録再生装置100は、暗号化されたコンテンツデータを復号するための鍵情報を記憶するリムーバブルHD10から当該リムーバブルHD10とは異なる鍵情報取得部130に提供するライセンス鍵情報提供処理を行う場合であって、ライセンス鍵情報を暗号化する際に用いる複数の暗号化情報を生成する生成処理と、生成された各暗号化情報を他の暗号化情報と異なるタイミングにて段階的にリムーバブルHD10から鍵情報取得部130に順次送信する送信処理と、鍵情報取得部130にて送信された各暗号化情報を順次受信する受信処理と、鍵情報取得部130にて全ての暗号化情報を受信した後に、当該全ての暗号化情報を用いてライセンス鍵情報を生成する生成処理と、を含み、送信処理においては、リムーバブルHD10が一の暗号化情報を送信した後であって、未だ情報取得部に送信されて

いない他の暗号化情報を送信する前に、当該送信された暗号化情報を消去する構成を有している。

[0163] この構成により、本実施形態の情報記録再生装置100は、生成された各暗号化情報を他の暗号化情報と異なるタイミングにて段階的にリムーバブルHD10から鍵情報取得部130に順次送信するとともに、鍵情報取得部130にて送信された各暗号化情報を順次受信し、鍵情報取得部130にて全ての暗号化情報が受信された後に、当該全ての暗号化情報を用いてライセンス鍵情報を生成する。そして、本実施形態の情報記録再生装置100は、リムーバブルHD10が一の暗号化情報が送信された後であって、未だ鍵情報取得部130に送信されていない他の暗号化情報が送信される前に、当該送信された暗号化情報を消去する。

[0164] したがって、本実施形態のライセンス鍵情報提供処理では、第1実施形態と同様に、暗号化コンテンツデータを部材間において転送する場合であっても、各部材にて暗号化コンテンツデータと当該暗号化コンテンツデータを復号するためのライセンス鍵情報と同時に存在することがないので、すなわち、暗号化コンテンツデータとライセンス鍵情報が同時に存在する部材は常に一つであるので、一つライセンス鍵情報からは常に一の暗号化コンテンツデータの再生のみ可能となる。

[0165] 例えば、第1実施形態と同様に、図7および図8に示すライセンス鍵情報を提供する方法によってもライセンス鍵情報の授受を行うことができるが、これらのライセンス鍵情報を提供する方法では、当該ライセンス鍵情報が消去される直前には、複数の部材においてそれぞれ暗号化されたコンテンツデータを復号化することができてしまう、または、ライセンス鍵情報の転送処理中に、何らかの障害により転送処理が中止された場合には、転送状況(ライセンス鍵情報の各部材の状態)においては、ライセンス鍵情報の復号化を行うことができない。

[0166] さらに、例えば、超流通システムに関する規定の一つであるARIB (Association of Radio Industries and Business/ 社団法人電波産業会)にてデジタル放送におけるコンテンツ保護規定により策定されている規格 (ARIB Technical Report B-15) では、コンテンツデータのムーブ (転送記録) に関して、ムーブ処理の途中において、ムーブ処理におけるコンテンツデータを転送する側 (ムーブ元) および当該ムーブ処理にお

けるコンテンツデータが転送される側(ムーブ先)の双方の装置に同時に、所定の時間、すなわち、1分を越える時間的長さを有するコンテンツデータが再生可能な状態であってはならないことが規定されている。このため、図7および図8に示すライセンス鍵情報を提供する方法など、この条件を満たさない提供方法では、超流通システムを構築することができない。

[0167] 一方、本実施形態のライセンス鍵情報提供処理では、上述のように、暗号化コンテンツデータとライセンス鍵情報が同時に存在する部材は常に一つであるので、転送側および転送される側の双方の部材に同時に、暗号化コンテンツデータを復号可能なライセンス鍵情報が存在しないこととなり、当該規格を満たすこととなる。

[0168] 以上のように、本実施形態のライセンス鍵情報提供処理では、一つライセンス鍵情報からは常に一の暗号化コンテンツデータの再生のみ可能となるとともに、ライセンス鍵情報の転送中の障害に強く、さらに、上述の超流通システムに代表される著作権保護を強固に行うシステムにおいても条件を満たすことができるので、的確にライセンス鍵情報の授受を行うことができるとともに、コンテンツデータの著作権保護を強固にかつ的確に行うことができる。

[0169] なお、本実施形態の情報記録再生装置100は、ライセンス鍵情報提供処理において、リムーバブルHD10と鍵情報取得部130間において単に暗号化第1鍵情報および暗号化第2鍵情報の授受を行うようになっているが、各暗号化情報の転送におけるセキュリティを高めるために、各暗号化情報の送受信および受信確認情報の送受信に関して、各情報が発信者から発信され、途中で改ざんなどが行なわれていないことを示すためのデジタル署名の方法を用いるようにしてもよい。

[0170] この場合には、図16に示すように各暗号化情報および受信確認情報の送信時に、リムーバブルHD10または鍵情報取得部130は、当該リムーバブルHD10または鍵情報取得部130におけるデジタル署名を署名情報として生成して添付し、各情報の受信後に当該添付された署名情報を用いて情報を送信したリムーバブルHD10または鍵情報取得部130の署名を検証する。そして、デジタル署名が承認された場合に、当該各情報を受信したリムーバブルHD10または鍵情報取得部130デジタル署名を署名情報として生成して添付する。

- [0171] また、本実施形態の情報記録再生装置100には、ライセンス鍵情報がリムーバブルHD10にて提供されるようになっているが、DVDなどのその他の可搬型記録媒体によって提供されるようにしてもよい。
- [0172] また、本実施形態の情報記録再生装置100には、ライセンス鍵情報がリムーバブルHD10にて提供されるようになっているが、インターネットなどの通信回線を介して、パーソナルコンピュータやハードディスクレコーダなどの他の情報再生装置、または、情報記録再生装置100から提供されるようにしてもよい。
- [0173] この場合に、ライセンス鍵情報を提供する情報記録装置は、通信回線を介して暗号化鍵情報および暗号化乱数情報を順次段階的にライセンス鍵情報を提供する装置に送信しつつ、消去する。
- [0174] また、本実施形態のライセンス鍵情報転送処理では、ライセンス鍵情報から二つの鍵情報を生成して暗号化し、転送するようになっているが、勿論、ライセンス鍵情報から3以上の鍵情報を生成して暗号化し、転送するようによい。

請求の範囲

- [1] 暗号化されたデータを復号するための鍵情報を記憶する第1記憶手段から当該第1記憶手段とは異なる第2記憶手段に提供する鍵情報提供方法であって、
前記第1記憶手段にて前記鍵情報から複数の送信情報を生成する生成工程と、
前記生成された各送信情報を他の送信情報と異なるタイミングにて段階的に前記第1記憶手段から第2記憶手段に順次送信する送信工程と、
前記第2記憶手段にて前記送信された各送信情報を順次受信する受信工程と、
前記第2記憶手段にて送信情報を受信した後に、当該送信情報を用いて前記鍵情報を復元する復元工程と、
を含み、
前記送信工程においては、前記第1記憶手段が一の送信情報を送信した後であって、未だ前記第2記憶手段に送信されていない他の送信情報を送信する前に、当該送信された送信情報を消去することを特徴とする鍵情報提供方法。
- [2] 請求項1に記載の鍵情報提供方法において、
前記生成工程は、
任意の情報を発生させる発生工程と、
前記発生された任意の情報に基づいて前記鍵情報を暗号化することによって第1の送信情報を生成する第1暗号化情報生成工程と、
前記第1記憶手段および前記第2記憶手段にて共通する暗号化処理によって前記任意の情報を暗号化することによって第2の送信情報を生成する第2暗号化情報生成工程と、
を含むことを特徴とする鍵情報提供方法。
- [3] 請求項2に記載の鍵情報提供方法において、
前記復元工程は、
前記第1の送信情報と前記第2の送信情報を用いて前記鍵情報を復元することを特徴とする鍵情報提供方法。
- [4] 請求項3に記載の鍵情報提供方法において、
前記送信工程においては、前記第2記憶手段における前記送信された前記第1の

送信情報または前記第2の送信情報を受信した旨を示す受信確認の情報を受信した後に、直前に第2記憶手段に送信された前記送信情報を消去することを特徴とする鍵情報提供方法。

- [5] 請求項1に記載の鍵情報提供方法において、
前記生成工程は、
前記鍵情報を複数の情報に分散し、当該鍵情報を消去する分散工程と、
前記第1記憶手段および前記第2記憶手段にて共通する暗号化処理によって前記分散された各情報を示す分散情報を暗号化し、前記複数の送信情報を生成する暗号化工程と、
を含むことを特徴とする鍵情報提供方法。
- [6] 請求項4に記載の鍵情報提供方法において、
前記復元工程は、
前記複数の送信情報を用いて前記鍵情報を復元することを特徴とする鍵情報提供方法。
- [7] 請求項6に記載の鍵情報提供方法において、
前記送信工程においては、前記第2記憶手段における前記送信された送信情報を受信した旨を示す受信確認の情報を受信した後に、直前に第2記憶手段に送信された前記送信情報の基となる前記分散情報を消去することを特徴とする鍵情報提供方法。
- [8] 請求項1乃至7の何れか一項に記載の鍵情報提供方法において、
前記送信工程においては、前記各送信情報を前記第2記憶手段に送信する際に、当該各送信情報の転送中に改ざんなどが行なわれていないことを示す署名情報を添付して当該各送信情報を送信することを特徴とする鍵情報提供方法。
- [9] 暗号化されたデータを復号するための鍵情報を記録する記憶手段から当該鍵情報を取得して当該データを再生する情報再生装置であって、
前記記憶手段にて前記鍵情報を暗号化する際に用いる複数の送信情報を生成させ、当該生成された各送信情報を他の送信情報とは異なるタイミングにて段階的に当該記憶手段から順次送信させる送信制御手段と、

前記送信された各送信情報を受信する受信手段と、
前記送信情報を受信した後に、当該送信情報を用いて前記鍵情報を復元する復元手段と、
前記復元された鍵情報に基づいて暗号化されたデータを復号し、当該コンテンツデータを再生する再生手段と、

を備え、

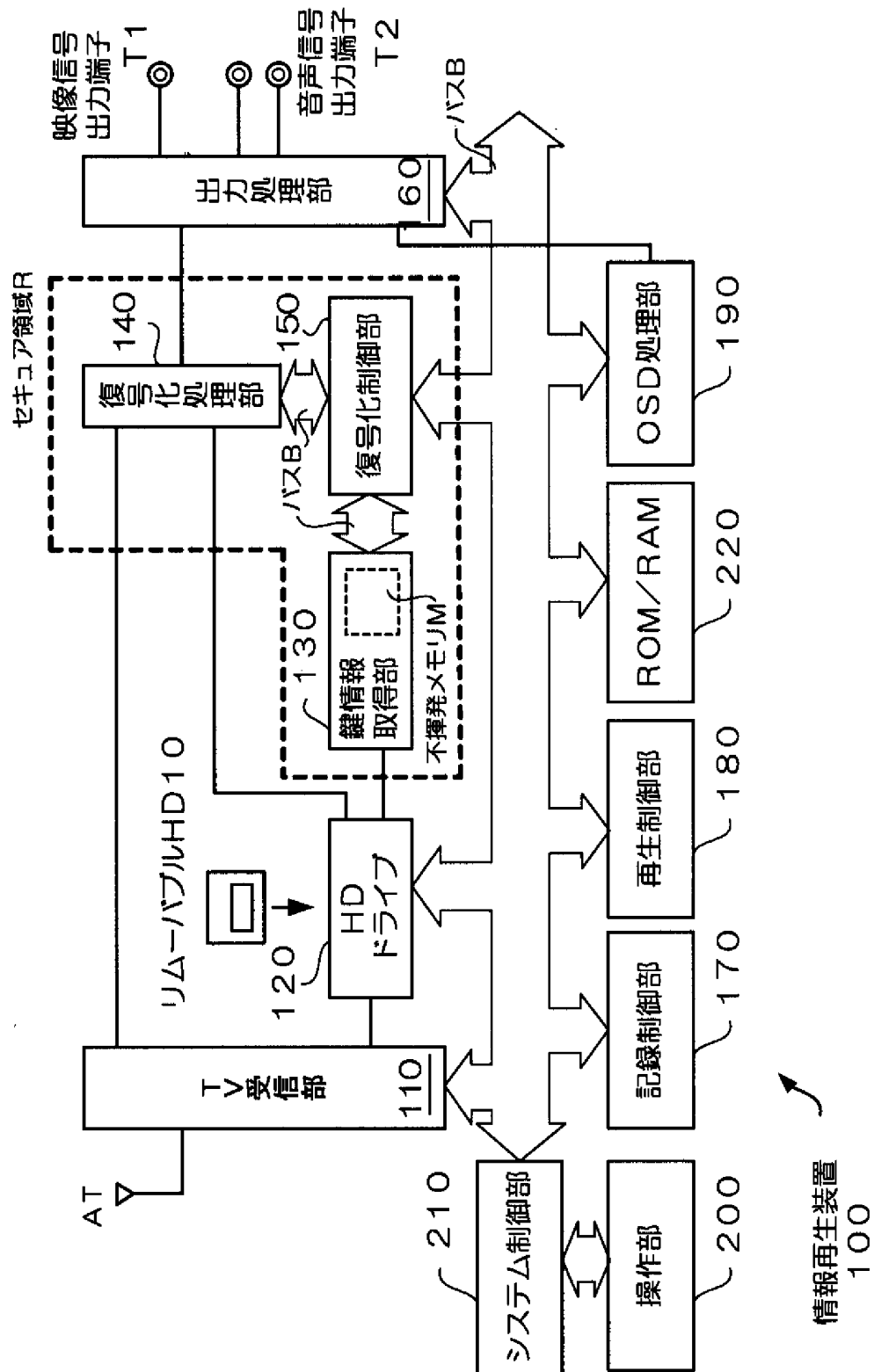
前記送信制御手段が、前記一の送信情報を受信した後であって、未だ記憶手段から送信されていない他の一の送信情報を受信する前に、当該送信された送信情報を前記記憶手段から消去させることを特徴とする情報再生装置。

[10] 請求項9に記載の情報再生装置であって、
前記記憶手段が、当該情報再生装置に搭載されていることを特徴とする情報再生装置。

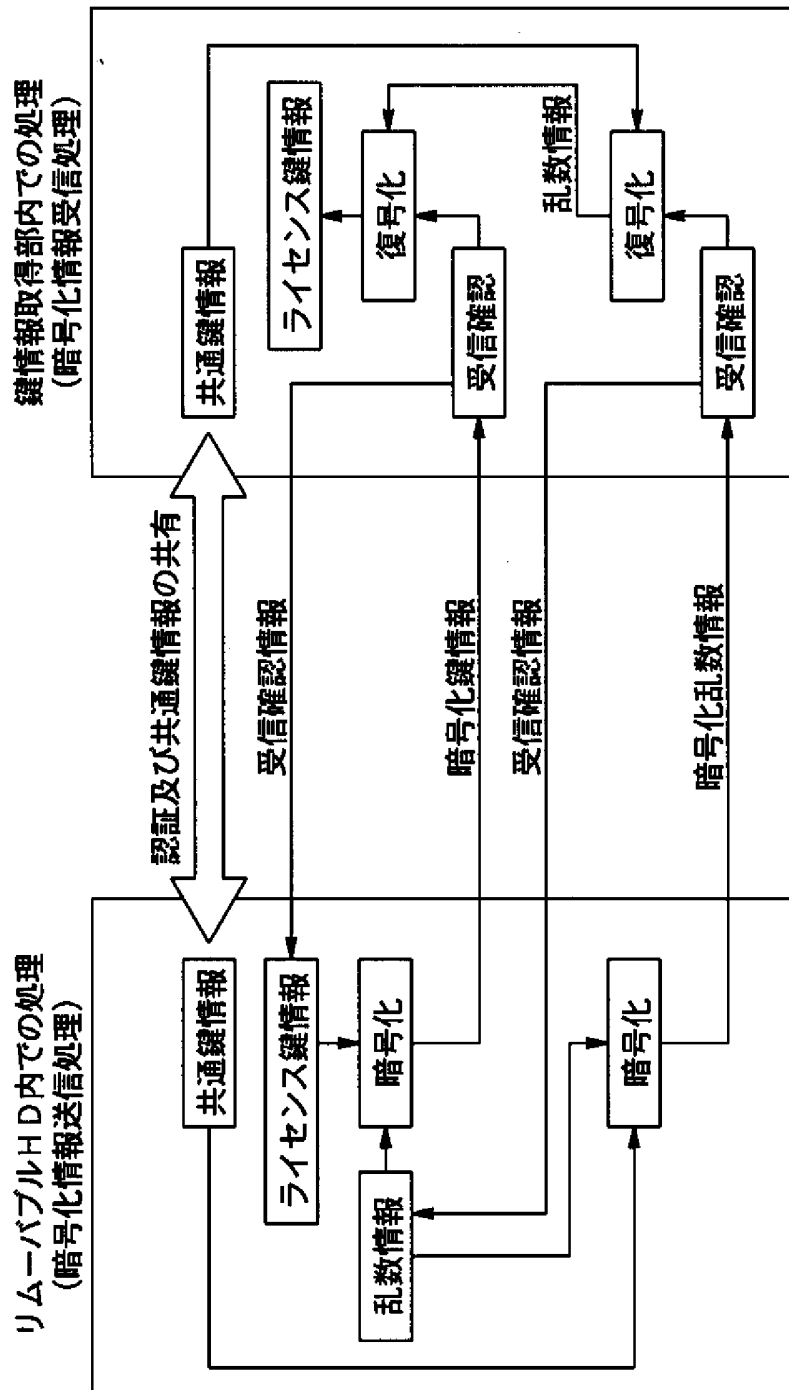
[11] 請求項9または10に記載の情報再生装置であって、
前記記憶手段が、当該情報再生装置とは異なる装置に搭載されるとともに、
前記受信手段が、通信回線を介して前記鍵情報を受信することを特徴とする情報再生装置。

[12] 暗号化されたデータを復号するための鍵情報を、当該データを再生する情報再生装置に提供する鍵情報提供装置であって、
前記鍵情報が予め記憶される記憶手段と、
前記鍵情報を暗号化する際に用いる複数の送信情報を生成する生成手段と、
前記生成された各送信情報を他の送信情報と異なるタイミングにて段階的に前記記憶手段から他の記憶手段に順次送信する送信手段と、
前記一の送信情報を送信した後であって、未だ送信していない他の送信情報を送信する前に、当該送信された送信情報を消去する消去手段と、
を備えることを特徴とする鍵情報提供装置。

[図1]



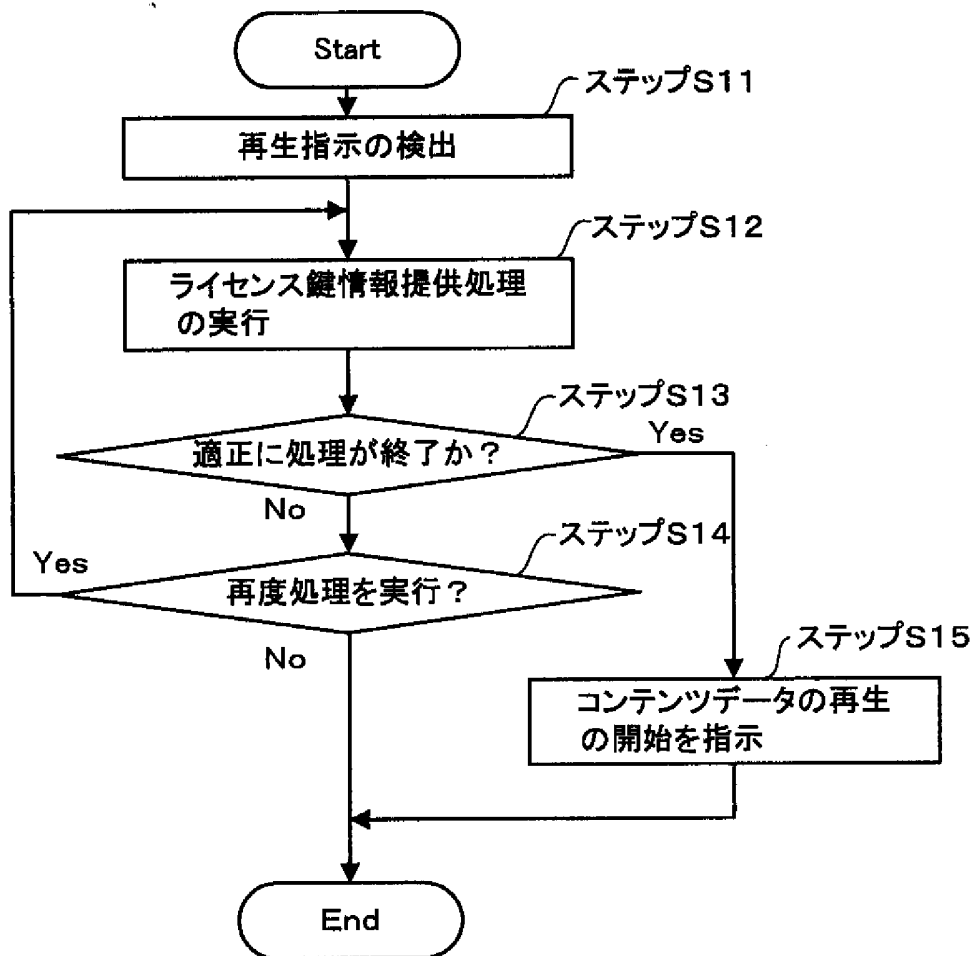
[図2]



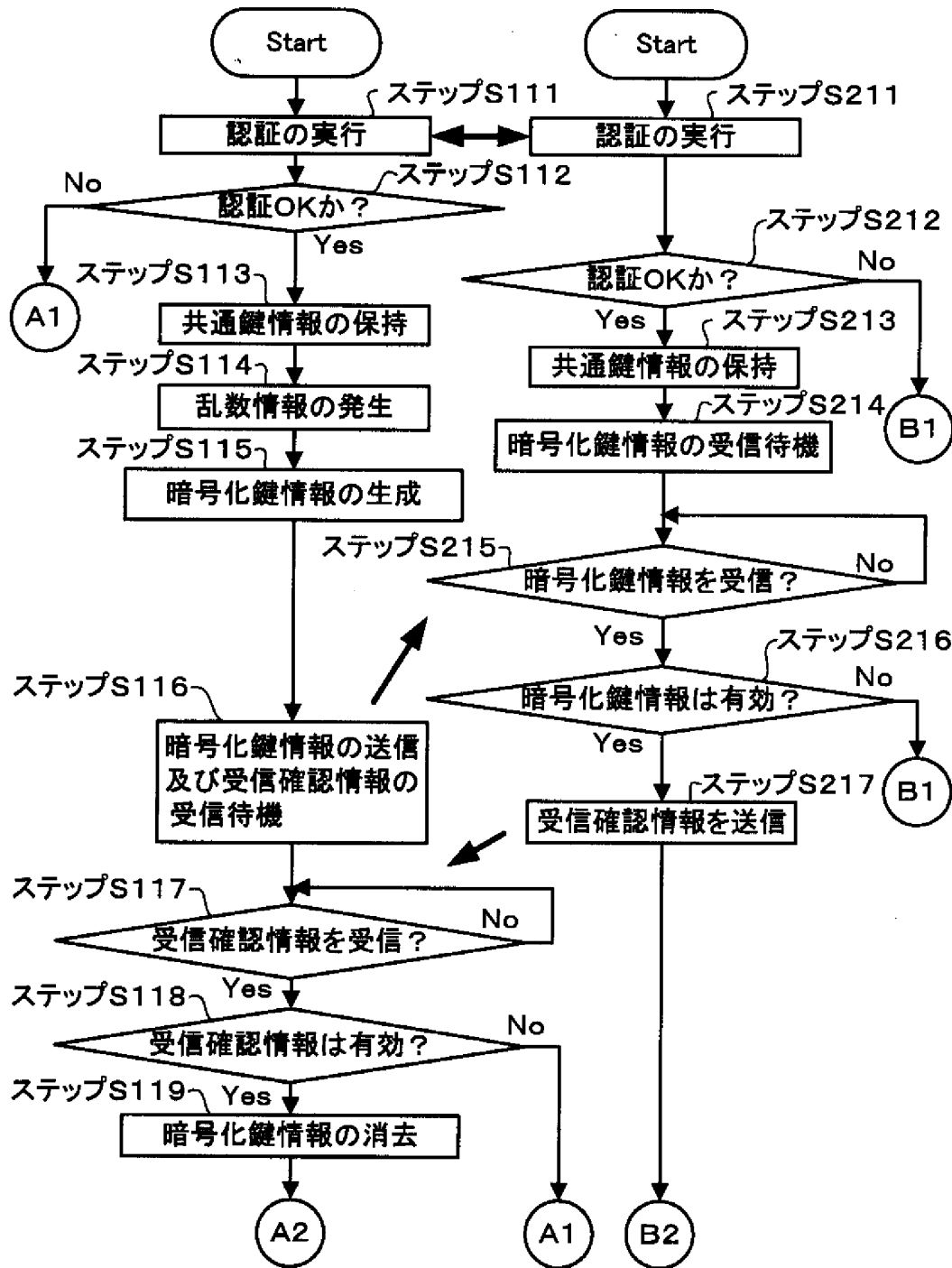
[図3]

	リムーバブルHD		鍵情報取得部	
	再生可能状態	リムーバブルHDに存在する情報	再生可能状態	鍵情報取得部に存在する情報
状態1	YES	ライセンス鍵情報、共通鍵情報	NO	共通鍵情報
状態2	YES	ライセンス鍵情報、共通鍵情報、乱数情報	NO	共通鍵情報
状態3	YES	暗号化鍵情報、共通鍵情報、乱数情報	NO	共通鍵情報
状態4	YES	暗号化鍵情報、共通鍵情報、乱数情報	NO	共通鍵情報、暗号化鍵情報
状態5	NO	共通鍵情報、乱数情報	NO	共通鍵情報、暗号化鍵情報
状態6	NO	共通鍵情報、暗号化乱数情報	NO	共通鍵情報、暗号化鍵情報
状態7	NO	共通鍵情報、暗号化乱数情報	YES	共通鍵情報、暗号化鍵情報、暗号化乱数情報
状態8	NO	共通鍵情報	YES	共通鍵情報、暗号化鍵情報、暗号化乱数情報
状態9	NO	共通鍵情報	YES	共通鍵情報、ライセンス鍵情報

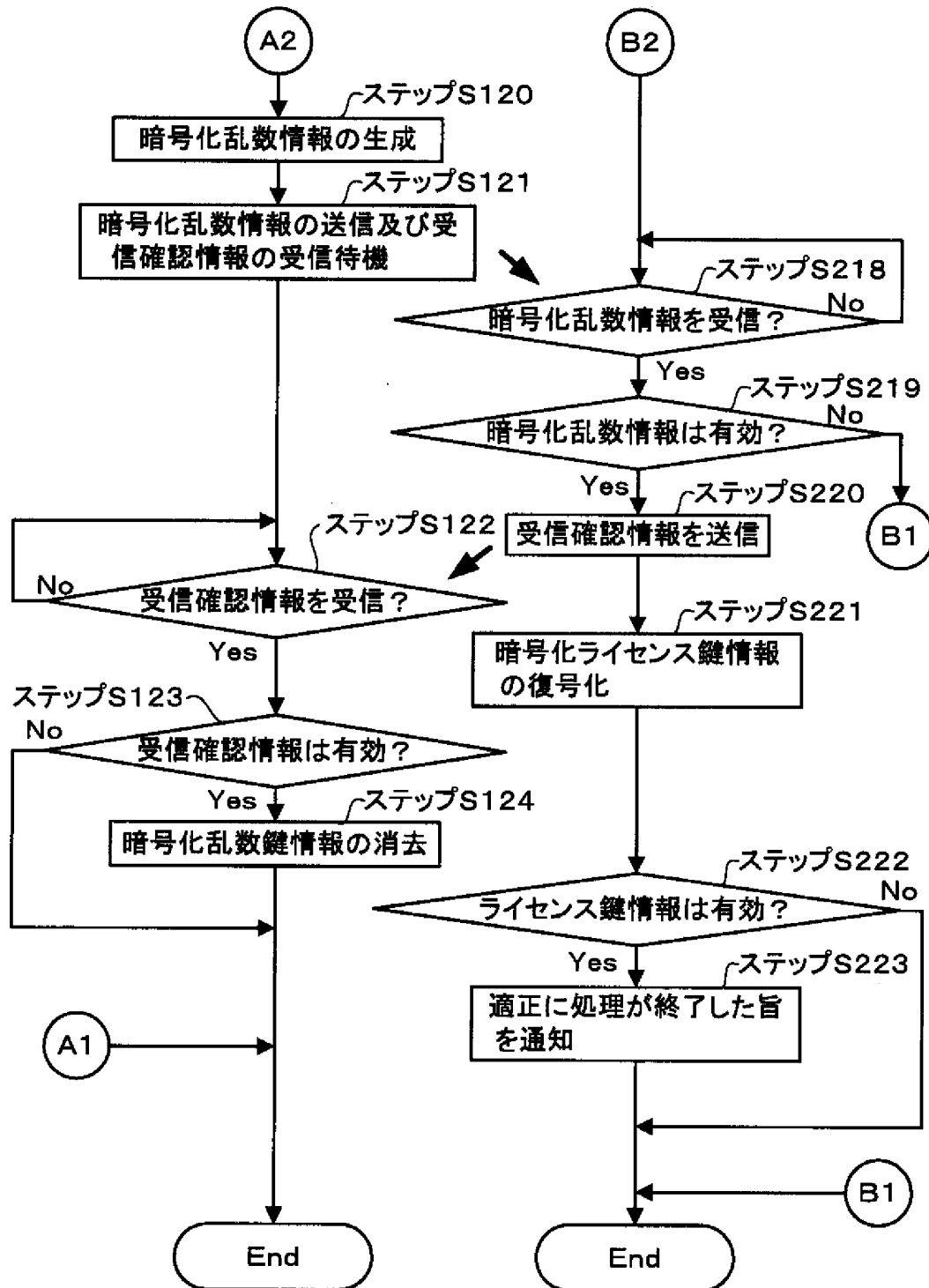
[図4]



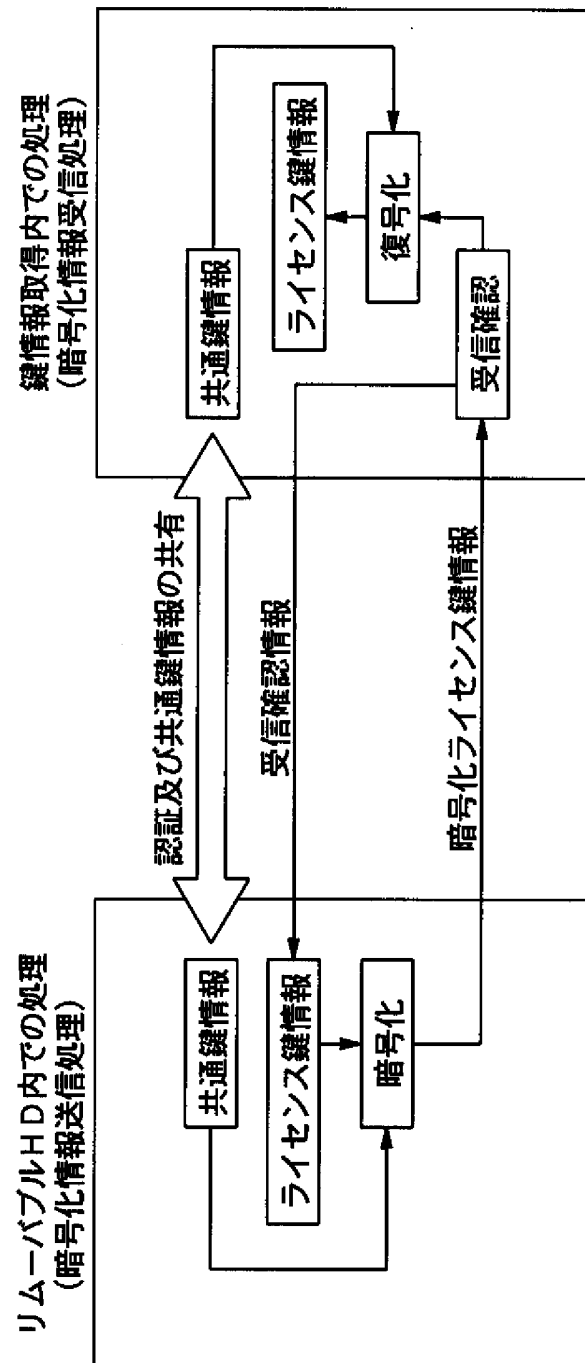
[図5]



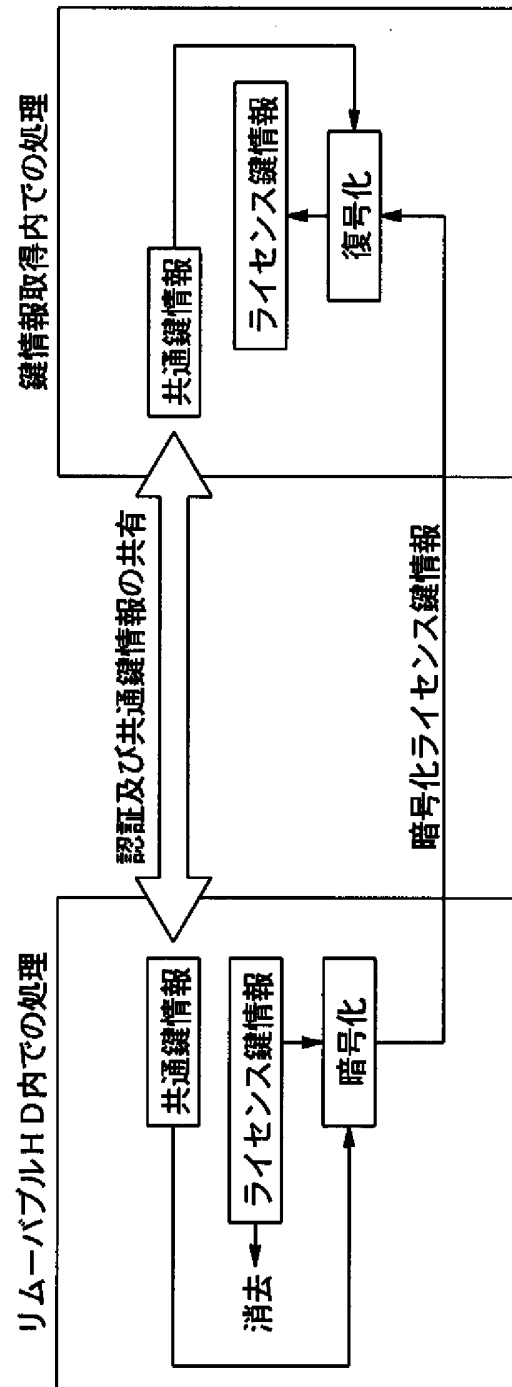
[図6]



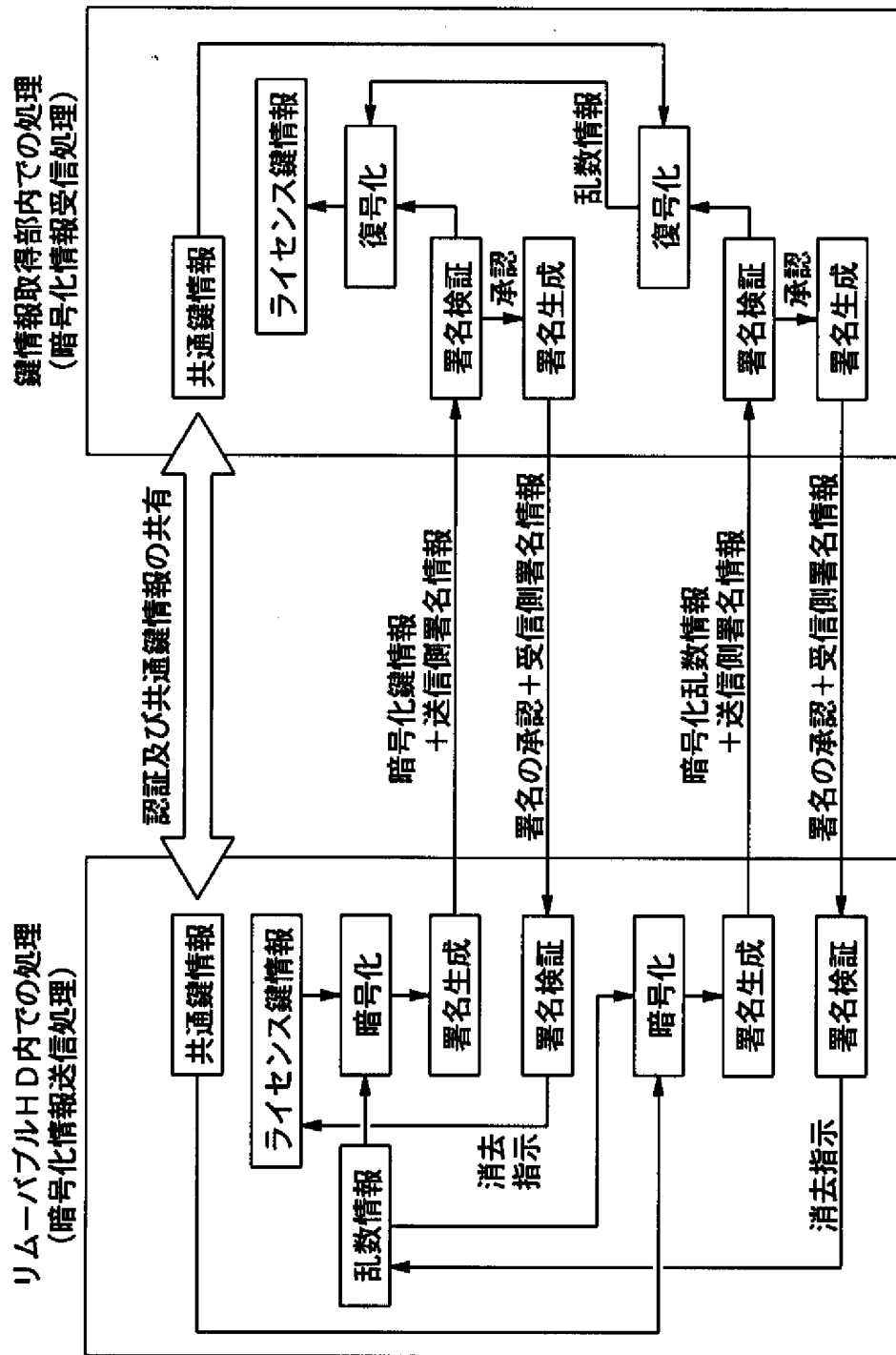
[図7]



[図8]



[図9]

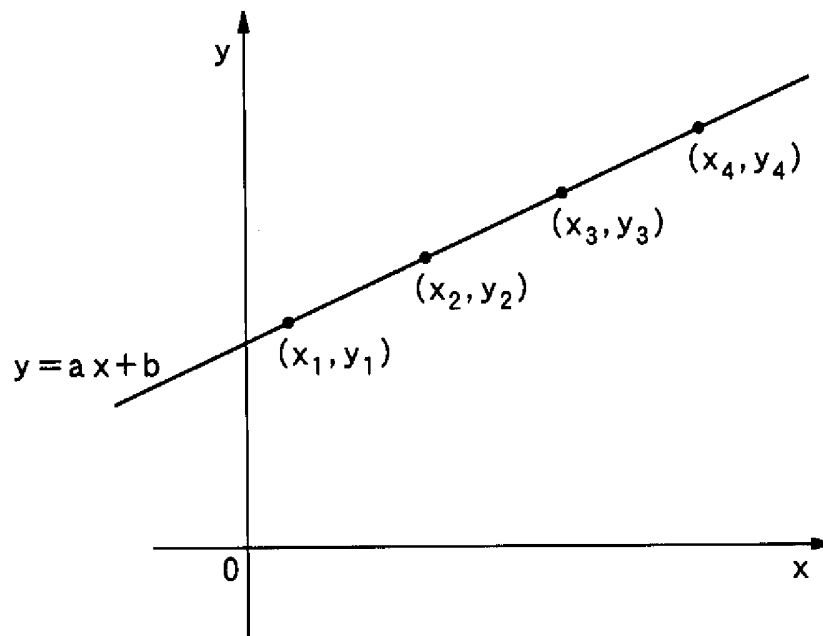


[図10]

$$\begin{array}{cccc} (x_1, y_1) & (x_2, y_2) & (x_3, y_3) & (x_4, y_4) \\ y_1 = ax_1 + b & y_2 = ax_2 + b & y_3 = ax_3 + b & y_4 = ax_4 + b \end{array}$$

a, b

任意の2点から直線の方程式が一意に決定

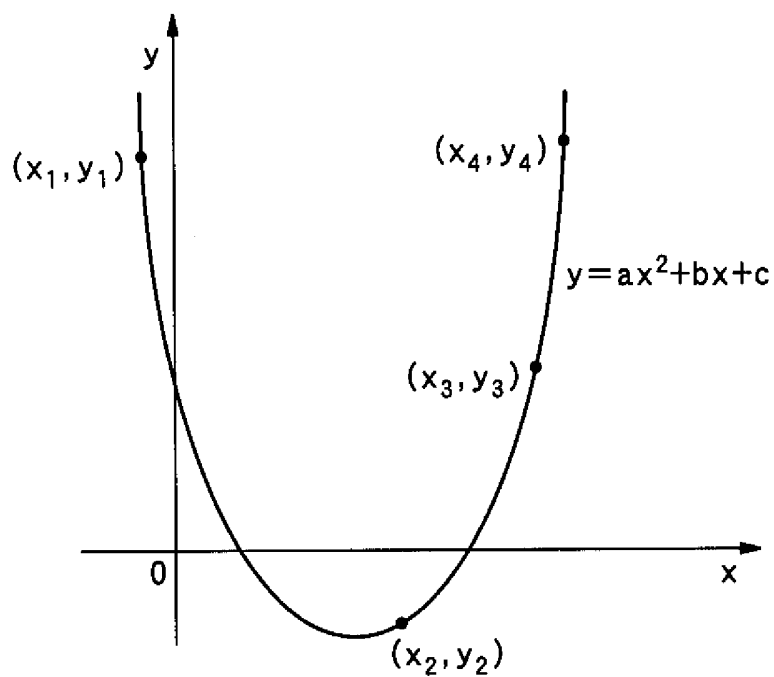


[図11]

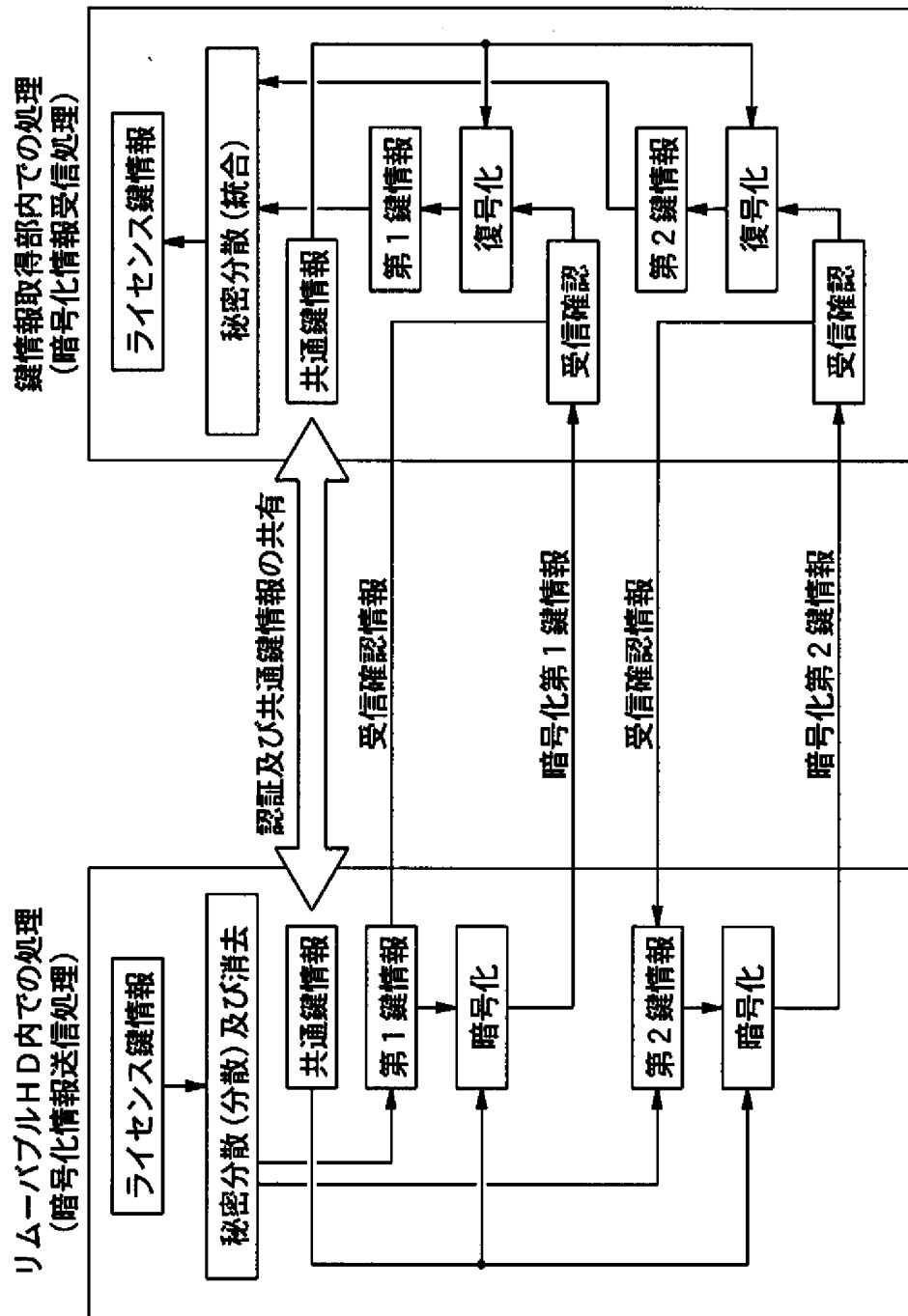
$$\begin{array}{cccc}
 (x_1, y_1) & (x_2, y_2) & (x_3, y_3) & (x_4, y_4) \\
 y_1 = ax_1^2 + bx_1 + c & y_2 = ax_2^2 + bx_2 + c & y_3 = ax_3^2 + bx_3 + c & y_4 = ax_4^2 + bx_4 + c
 \end{array}$$

a, b

任意の 3 点から 2 次曲線の方程式が一意に決定

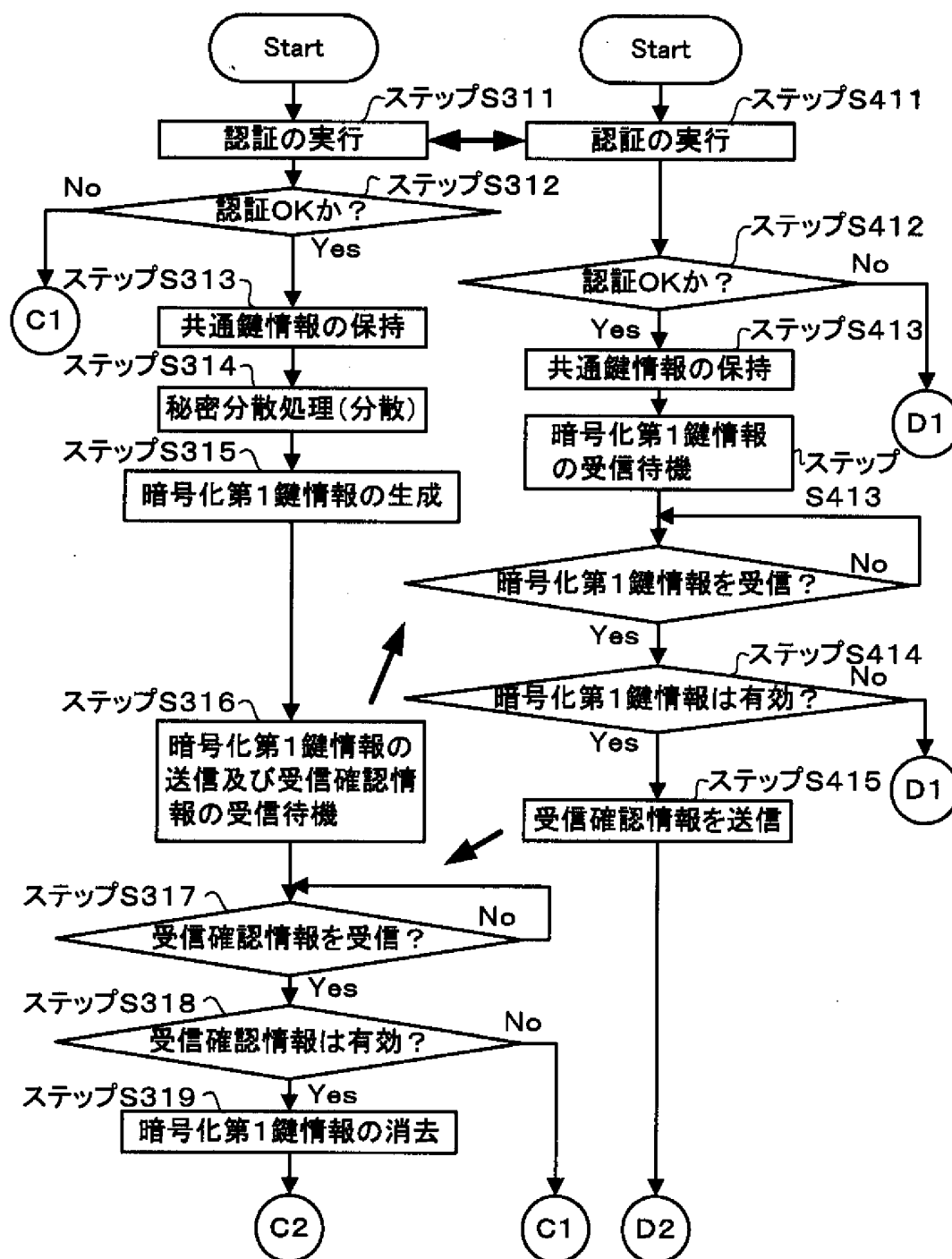


[図12]

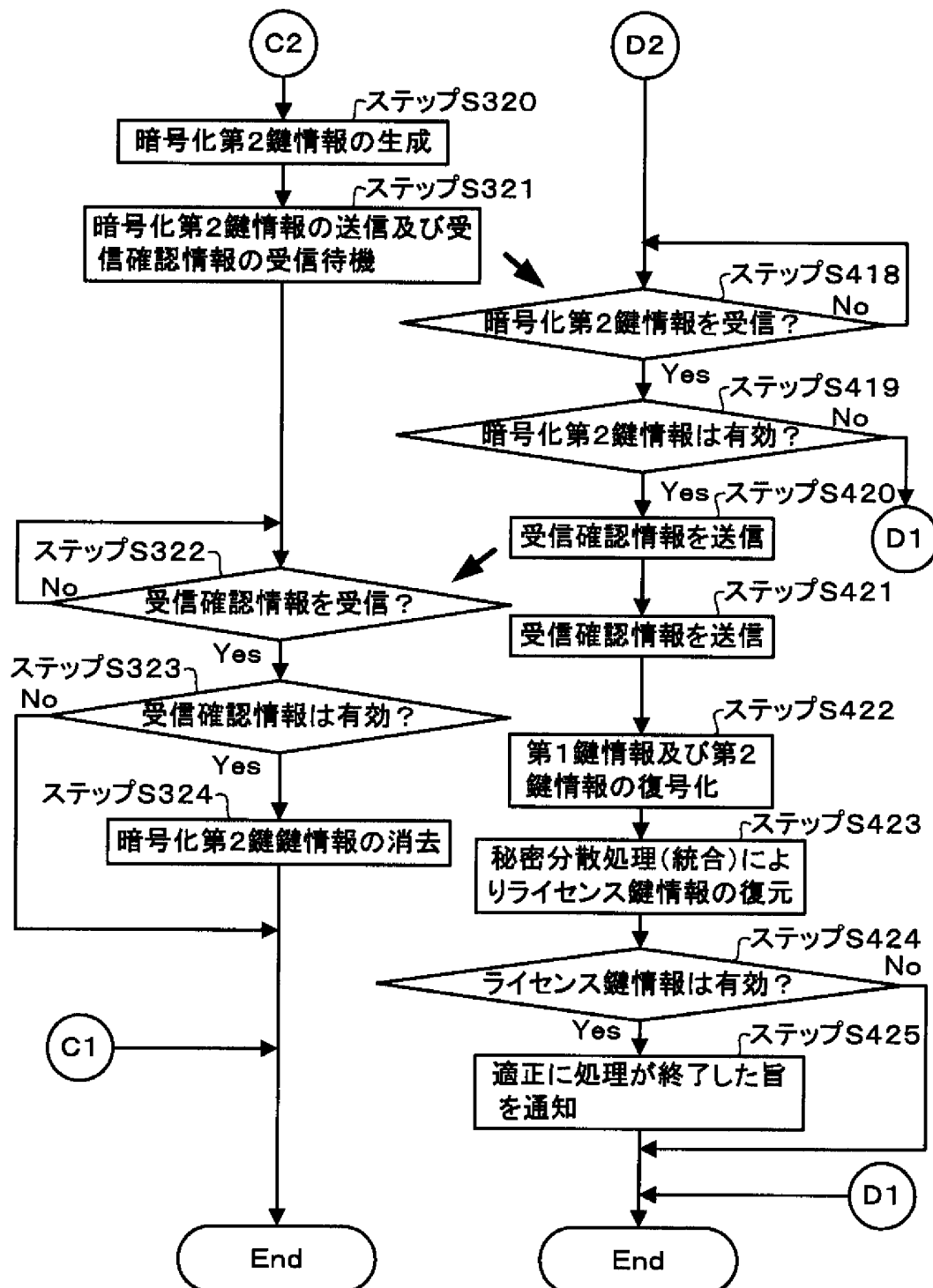


[図13]

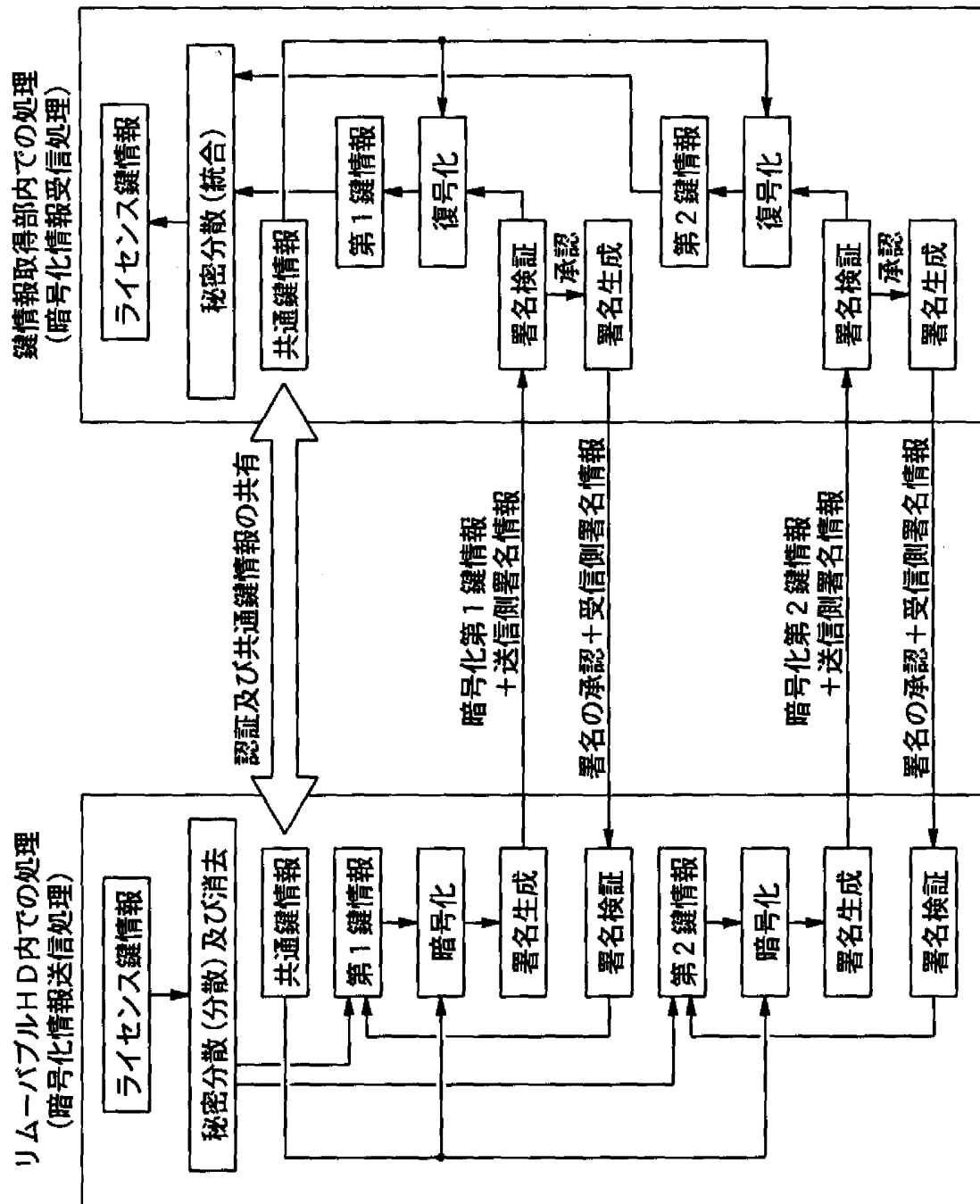
	リムーバブルHD		鍵情報取得部	
	再生可能状態	リムーバブルHDに存在する情報	再生可能状態	鍵情報取得部に存在する情報
状態1	YES	ライセンス鍵情報、共通鍵情報	NO	共通鍵情報
状態2	YES	共通鍵情報、第1鍵情報、第2鍵情報	NO	共通鍵情報
状態3	YES	共通鍵情報、暗号化第1鍵情報、第2鍵情報	NO	共通鍵情報
状態4	YES	共通鍵情報、暗号化第1鍵情報、第2鍵情報	NO	共通鍵情報、暗号化第1鍵情報
状態5	NO	共通鍵情報、第2鍵情報	NO	共通鍵情報、暗号化第1鍵情報
状態6	NO	共通鍵情報、暗号化第2鍵情報	NO	共通鍵情報、暗号化第1鍵情報
状態7	NO	共通鍵情報、暗号化第2鍵情報	YES	共通鍵情報、暗号化第1鍵情報、暗号化第2情報
状態8	NO	共通鍵情報	YES	共通鍵情報、暗号化第1鍵情報、暗号化第2情報
状態9	NO	共通鍵情報	YES	共通鍵情報、第1鍵情報、第2鍵情報
状態10	NO	共通鍵情報	YES	共通鍵情報、ライセンス鍵情報



[図15]



[図16]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/019809

A. CLASSIFICATION OF SUBJECT MATTER H04L9/08(2006.01), G06F21/24(2006.01), G11B20/10(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) H04L9/08(2006.01), G06F21/24(2006.01), G11B20/10(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 2003-323342 A (Matsushita Electric Industrial Co., Ltd.), 14 November, 2003 (14.11.03), Particularly, Par. Nos. [0161] to [0170], [0104] to [0109] (Family: none)	1-12
Y	JP 2000-138673 A (Sony Corp.), 16 May, 2000 (16.05.00), Particularly, Par. Nos. [0231] to [0242] & AU 9961231 A & EP 1039392 A1 & CN 1289421 A & KR 2001033171 A	1-12
Y	JP 2004-140808 A (Kabushiki Kaisha Denon), 13 May, 2004 (13.05.04), Particularly, Par. Nos. [0043] to [0054], [0211] & US 2004/057582 A1 & EP 1404132 A1	1-12
☐ 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 07 February, 2006 (07.02.06)		Date of mailing of the international search report 14 February, 2006 (14.02.06)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04L9/08(2006.01), G06F21/24(2006.01), G11B20/10(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. H04L9/08(2006.01), G06F21/24(2006.01), G11B20/10(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 2003-323342 A (松下電器産業株式会社) 2003.11.14 (ファミリーなし) 特に第 161-170, 104-109 段落	1-12
Y	JP 2000-138673 A (ソニー株式会社) 2000.05.16 & AU 9961231 A & EP 1039392 A1 & CN 1289421 A & KR 2001033171 A 特に第 231-242 段落	1-12
Y	JP 2004-140808 A (株式会社デノン) 2004.05.13 & US 2004/057582 A1 & EP 1404132 A1 特に第 43-54, 211 段落	1-12

☐ 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

07.02.2006

国際調査報告の発送日

14.02.2006

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)

中里 裕正

電話番号 03-3581-1101 内線 3546

5 S

9364