(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年10 月18 日 (18.10.2001)

PCT

(10) 国際公開番号
WO 01/78300 A1

(51) 国際特許分類[7]: H04L 9/00, G11B 20/10, 20/12

(21) 国際出願番号: PCT/JP01/02963

(22) 国際出願日: 2001 年4 月5 日 (05.04.2001)

(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2000-105328 2000 年4 月6 日 (06.04.2000) JP
特願2000-243205 2000 年8 月10 日 (10.08.2000) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35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): 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP]. 大石丈於 (OISHI, Tateo) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 小池 晃, 外 (KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).

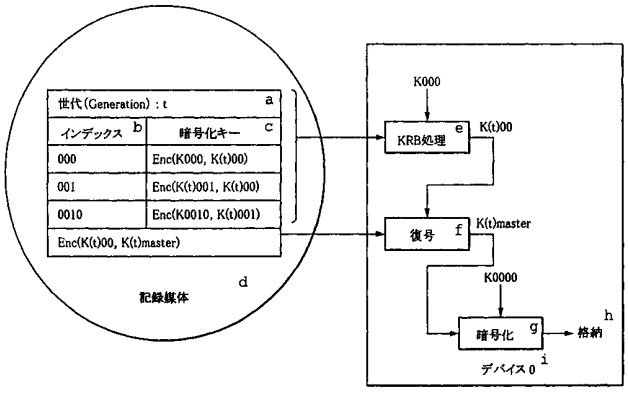
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

[続葉有]

(54) Title: INFORMATION RECORDING/REPRODUCING APPARATUS AND METHOD

(54) 発明の名称: 情報記録／再生装置及び方法



a...GENERATION
b...INDEX
c...CIPHERING KEY
d...RECORD MEDIUM
e...KRB PROCESSING
f...DECIPHERING
g...CIPHERING
h...STORING
i...DEVICE 0

(57) Abstract: Update of a master key and a media key is transmitted along with a key update block (KRB) through a key distribution system of tree structure. The KRB has a structure where devices constituting leaves of the tree have a leaf key and a limited node key and creates and distributes a specific key update block (KRB) to a group specified by a specific node, thereby limiting updateable devices. Any device not belonging to the group cannot decode the data, thus ensuring the safety of key distribution. Especially, in a system using a master key under generation control, an update master key is distributed by a KRB.

[続葉有]

WO 01/78300 A1

(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, 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:

ツリー構造の鍵配布構成により、マスターキー、メディアキーの更新をキー更新ブロック（ＫＲＢ）とともに送信する。ＫＲＢは、ツリーのリーフを構成するデバイスにリーフキー及び限定したノードキーを保有させた構成であり、特定のノードにより特定されるグループに特定のキー更新ブロック（ＫＲＢ）を生成して配布して、更新可能デバイスを限定することができる。グループに属さないデバイスは復号できず、キー配信の安全性が確保される。特に、世代管理を行ったマスターキーを使用するシステムにおいて、ＫＲＢによる更新マスターキーを配布する構成が実現される。

明細書

情報記録／再生装置及び方法

技術分野

本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体に関し、特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく押さえて、マスターキーあるいはメディアキー等の鍵更新におけるデータ配信の負荷を軽減することを可能とした構成を提供する。具体的には、各記録再生器機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体に関する。

背景技術

ディジタル信号処理技術の進歩、発展にともない、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み（システム）が

導入されている。

例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、又はコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行うことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗

号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。したがって、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、ディジタルデータを記録したＤＶＤ－ＲＯＭの再生を行えないことになり、不正コピーが防止されるようになっている。

しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

すなわち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

そこで、本出願人は、先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別するための情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受

けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、１つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

しかし、この方式においては、攻撃者が１つの機器の攻撃に成功し、マスターキーを取り出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

発明の開示

本発明は、上述の問題点を解決することを目的とするものであり、木構造の階

層的鍵配信方式を用いることにより、メッセージ量を小さく押さえて、新たな更新キーの配信の負荷を軽減することを可能とした構成を提供する。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

本発明の第１の側面は、記録媒体に情報を記録する情報記録装置において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する格納データの暗号化処理を実行する暗号処理手段を有し、前記暗号処理手段は、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する構成を有し、前記暗号化キー生成用データは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記暗号化キー生成用データの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、

該取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、第１の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第１の暗号化キーを生成して該第１の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第１の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、を選択的に実行する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに

基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の第２の側面は、記録媒体から情報を再生する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を実行する暗号処理手段を有し、前記暗号処理手段は、前記情報記録装置に内蔵した復号キー生成用データに基づいて復

号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する構成を有し、前記復号キー生成用データは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記復号キー生成用データの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記記録媒体に格納さ

れた第１の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第１の復号キーを生成して該第１の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、を選択的に実行する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記再生機器制限なしの復号処理において、情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーと、暗号データを記録した情報記録装置の識別子であるデバイスＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キーを生成し、前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復号キーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成する構成を有し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報

（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の第３の側面は、記録媒体に情報を記録する情報記録方法において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とする情報記録方法にある。

さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、さらに、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、第１の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第１の暗号化キーを生成して該第１の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第１の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、を選択的に実行することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記

録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成し、前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御することを特徴とする。

さらに、本発明の第４の側面は、記録媒体から情報を再生する情報再生方法であり、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、前記

更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とする情報再生方法にある。

さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記記録媒体に格納された第１の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第１の復号キーを生成して該第１の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、

を選択的に実行することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記再生機器制限なしの復号処理において、情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーと、暗号データを記録した情報記録装置の識別子であるデバイスＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キーを生成し、前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復号キーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、情報再生装置は、復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記復号処理ステップは、前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、データを構成するトラ

ンスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする。

さらに、本発明の第５の側面は、情報を記録可能な情報記録媒体であって、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を格納したことを特徴とする情報記録媒体にある。

さらに、本発明の情報記録媒体の一実施態様において、情報記録装置において記録媒体に格納するデータの暗号化処理に用いる暗号化キーを生成するための暗号化キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする。

さらに、本発明の情報記録媒体の一実施態様において、情報再生装置において記録媒体に格納された暗号データの復号処理に用いる復号キーを生成するための復号キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする。

さらに、本発明の情報記録媒体の一実施態様において、暗号化キー生成用データ又は復号キー生成用データに関する世代情報を格納した構成であることを特徴とする。

さらに、本発明の第６の側面は、情報記録媒体を製造する記録媒体製造装置であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を格納するメモリと、前記メモリ

に格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込み制御を実行する制御部と、を有することを特徴とする記録媒体製造装置にある。

さらに、本発明の記録媒体製造装置の一実施態様において、前記メモリには、さらに、記録媒体識別子と、暗号化された暗号化キー生成用データ又は暗号化された復号キー生成用データの少なくともいずれかを格納し、前記制御部は、前記記録媒体識別子、暗号化された暗号化キー生成用データ、又は暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする。

さらに、本発明の記録媒体製造装置の一実施態様において、前記メモリには、さらに、暗号化キー生成用データ又は復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする。

さらに、本発明の第７の側面は、記録媒体を製造する記録媒体製造方法であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）をメモリに格納するステップと、前記メモリに格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込みを実行するステップと、を有することを特徴とする記録媒体製造方法にある。

さらに、本発明の記録媒体製造方法の一実施態様において、前記メモリに、さらに、記録媒体識別子、暗号化された暗号化キー生成用データ、又は暗号化された復号キー生成用データの少なくともいずれかを格納し、前記記録媒体識別子、暗号化された暗号化キー生成用データ、又は暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込みを実行することを特徴とする。

さらに、本発明の記録媒体製造方法の一実施態様において、前記記録媒体製造方法において、前記メモリに、さらに、暗号化キー生成用データ又は復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込みを実行することを特徴とする。

さらに、本発明の第８の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とするプログラム提供媒体にある。

さらに、本発明の第９の側面は、記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

本発明の構成においては、ツリー（木）構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく抑えている。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。

また、本発明の１つの態様としては、記録媒体に記録するコンテンツの形式をＭＰＥＧ２ ＴＳパケット（ｐａｃｋｅｔ）とし、このパケットを記録装置が受信した時刻情報であるＡＴＳを付加して記録する。ＡＴＳは２４乃至３２ビットの

データであり、ある程度のランダム性がある。ここで、ＡＴＳはArrival Time Stamp（着信時刻スタンプ）の略である。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳパケットをＸ個記録することにし、その第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロックのデータを暗号化するブロックキーを生成する。

このようにすることにより、各ブロック毎に固有の鍵を用いて暗号化することができ、また鍵を格納する特別な領域も不要となり、記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなる。

さらに、ＴＳパケットにＡＴＳだけでなくコピー制限情報(ＣＣＩ：Copy Control Information)も付加して記録し、ＡＴＳとＣＣＩを用いてブロックキーを生成するようにすることも可能である。

なお、本発明の第８及び第９の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

図１は、本発明の情報記録再生装置の構成例（その１）を示すブロック図である。

図２は、本発明の情報記録再生装置の構成例（その２）を示すブロック図である。

図３Ａ及び図３Ｂは、本発明の情報記録再生装置のデータ記録処理フローを示す図である。

図４Ａ及び図４Ｂは、本発明の情報記録再生装置のデータ再生処理フローを示す図である。

図５は、本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

図６は、本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図７Ａ～図７Ｃは、本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

図８は、本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図９は、本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図１０は、本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

図１１は、本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

図１２Ａ及び図１２Ｂは、本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用されるキー更新ブロック（ＫＲＢ）の例を示す図である。

図１３は、本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理例を示す図である。

図１４は、本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（ＫＲＢ）を使用した復号処理フローを示す図である。

図１５は、本発明の情報記録再生装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。

図１６は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その１）である。

図１７は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その２）である。

図１８は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理を説明するフローチャートである。

図１９は、本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

図２０は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるタイトル固有キーの生成処理フローを示す図である。

図２１は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録時のタイトル固有キーの生成処理例を示す図である。

図２２は、本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

図２３は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

図２４は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理を説明するフローチャートである。

図２５は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

図２６は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ最盛時のタイトル固有キーの生成処理フローを示す図である。

図２７は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理例を示す図である。

図２８は、本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した復号処理フローを示す図である。

図２９は、本発明の情報記録再生装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。

図３０は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その１）である。

図３１は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その２）である。

図３２は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理を説明するフローチャートである。

図３３は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理時の暗号化処理を説明するブロック図である。

図３４は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理を説明するフローチャートである。

図３５は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理における再生可能性判定処理の詳細を示すフローチャートである。

図３６は、本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する構成とした記録再生装置構成を示すブロック図である。

図３７は、本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理について示すブロック図である。

図３８は、本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理フローを示す図である。

図３９は、本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理を説明する図である。

図４０Ａ及び図４０Ｂは、本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

図４１Ａ及び図４１Ｂは、本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

図４２は、本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

図４３は、本発明の情報記録再生装置において使用される情報記録媒体を製造する製造装置の構成を示すブロック図である。

図４４は、本発明の情報記録再生装置において使用される情報記録媒体を製造する製造処理の処理フローを示す図である。

図４５は、本発明の情報記録再生装置において使用されるキー更新ブロック（ＫＲＢ）のフォーマット例を示す図である。

図４６Ａ～図４６Ｃは、本発明の情報記録再生装置において使用されるキー更新ブロック（ＫＲＢ）のタグの構成を説明する図である。

発明を実施するための最良の形態

［システム構成］

図１は、本発明を適用した記録再生装置１００の一実施例構成を示すブロック図である。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ(Read Only Memory) １６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０、さらにトランスポート・ストリーム処理手段（ＴＳ処理手段）３００を有し、これらはバス１１０によって相互に接続されている。

入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１

４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale Integrated Curcuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、又は復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

ＲＯＭ１６０は、例えば、記録再生装置毎に固有の、あるいは複数の記録再生装置のグループ毎に固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。ドライブ１９０は、ディジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。また、プログラムをＲＯＭ１６０に、デバイスキーをメモリ１８０に記録する構成としてもよい。

記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱

可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、後段において図６以下を用いて詳細に説明するが、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体１９５に格納するためのデータ処理及び、記録媒体１９５からの再生処理時の出現タイミング制御処理を行う。

トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングはＭＰＥＧ２システムズで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御する。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、ＤＶＤ等の記録媒体１９５へのデータ記録時に、各トランスポートパケットの入力タイミングを表すＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）を付加して記録する。

本発明の記録再生装置１００は、上述のＡＴＳの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段１５０において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体１９５に格納する。さらに、暗号処理手段１５０は、記録媒体１９５に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

なお、図１に示す暗号処理手段１５０、ＴＳ処理手段３００は、理解を容易に

するため、別ブロックとして示してあるが、両機能を実行する１つのワンチップＬＳＩとして構成してもよく、また、両機能をソフトウェア又はハードウェアを組み合わせた構成によって実現する構成としてもよい。

本発明の記録再生装置の構成例としては図１に示す構成の他に図２に示す構成が可能である。図２に示す記録再生装置２００では、記録媒体２０５はドライブ装置としての記録媒体インタフェース（Ｉ／Ｆ）２１０から着脱が可能であり、この記録媒体２０５を別の記録再生装置に装着してもデータの読出し、書き込みが可能な構成としたものである。

［データ記録処理及びデータ再生処理］

次に、図１あるいは図２の記録再生装置における記録媒体に対するデータ記録処理及び記録媒体からのデータ再生処理について、図３及び図４のフローチャートを参照して説明する。外部からのディジタル信号のコンテンツを、記録媒体１９５に記録する場合においては、図３（Ａ）のフローチャートに従った記録処理が行われる。すなわち、ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ３０１において、入出力Ｉ／Ｆ１２０は、供給されるディジタルコンテンツを受信し、バス１１０を介して、ＴＳ処理手段３００に出力する。

ＴＳ処理手段３００は、ステップＳ３０２において、トランスポートストリームを構成する各トランスポートパケットにＡＴＳを付加したブロックデータを生成して、バス１１０を介して、暗号処理手段１５０に出力する。

暗号処理手段１５０は、ステップＳ３０３において、受信したディジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス１１０を介して、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０に出力する。暗号化コンテンツは、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０を介して記録媒体１９５に記録（Ｓ３０４）され、記録処理を終了する。なお、暗号処理手段１５０における暗号処理については後段で説明する。

なお、IEEE1394シリアルバスを介して接続した装置相互間で、ディジタルコンテンツを伝送するときの、ディジタルコンテンツを保護するための規格として、

本特許出願人であるソニー株式会社を含む５社によって、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められているが、このＤＴＣＰでは、コピーフリーでないディジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、ディジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたディジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

このＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２０は、ステップＳ３０１で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

ＤＴＣＰによるディジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたディジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたディジタルコンテンツを、そこに含まれるキーを用いて復号する。

なお、ＤＴＣＰによれば、正確には、キーの初期値と、ディジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.comのURL(Uniform Resource Locator)で特定されるＷｅｂページにおいて、インフォメイショナルバージョン(Informational Version)の取得が可能である。

次に、外部からのアナログ信号のコンテンツを、記録媒体１９５に記録する場合の処理について、図３（Ｂ）のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、

入出力Ｉ／Ｆ１４０は、ステップＳ３２１において、そのアナログコンテンツを受信し、ステップＳ３２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、ディジタル信号のコンテンツ（ディジタルコンテンツ）とする。

このディジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ３２３において、ＭＰＥＧエンコード、即ちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段１５０に供給される。

以下、ステップＳＳ３２４、Ｓ３２５、Ｓ３２６において、図３（Ａ）のステップＳ３０２、Ｓ３０３における処理と同様の処理が行われる。すなわち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

次に、記録媒体１９５に記録されたコンテンツを再生して、ディジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図４のフローに従って説明する。ディジタルコンテンツとして外部に出力する処理は図４（Ａ）のフローチャートに従った再生処理として実行される。すなわち、まず最初に、ステップＳ４０１において、ドライブ１９０又は記録媒体Ｉ／Ｆ２１０によって、記録媒体１９５に記録された暗号化コンテンツが読み出され、バス１１０を介して、暗号処理手段１５０に出力される。

暗号処理手段１５０では、ステップＳ４０２において、ドライブ１９０又は記録媒体Ｉ／Ｆ２１０から供給される暗号化コンテンツが復号処理され、復号データがバス１１０を介して、ＴＳ処理手段３００に出力される。

ＴＳ処理手段３００は、ステップＳ４０３において、トランスポートストリームを構成する各トランスポートパケットのＡＴＳから出力タイミングを判定し、ＡＴＳに応じた制御を実行して、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給する。入出力Ｉ／Ｆ１２０は、ＴＳ処理手段３００からのディジタルコンテンツを、外部に出力し、再生処理を終了する。なお、ＴＳ処理手段３００の処理、暗号処理手段１５０におけるディジタルコンテンツの復号処理については後述する。

なお、入出力Ｉ／Ｆ１２０は、ステップＳ４０４で、IEEE1394シリアルバスを

介してディジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、ディジタルコンテンツを暗号化して伝送する。

記録媒体１９５に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４（Ｂ）のフローチャートに従った再生処理が行われる。

すなわち、ステップＳ４２１、Ｓ４２２、Ｓ４２３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段１５０において得られた復号されたディジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

ＭＰＥＧコーデック１３０では、ステップＳ４２４において、ディジタルコンテンツがＭＰＥＧデコード、即ち伸長処理が実行され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ４２４において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたディジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換（Ｓ４２５）して、アナログコンテンツとする。そして、ステップＳ４２６に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

［データフォーマット］

次に、図５を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。１ブロックは、１９２＊Ｘ（エックス）バイト（例えばＸ＝３２）の大きさとなっている。

本発明では、ＭＰＥＧ２のＴＳ（トランスポート・ストリーム）パケット（１８８バイト）にＡＴＳを付加して１９２バイトとして、それをＸ個集めて１ブロックのデータとしている。ＡＴＳは２４乃至３２ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp（着信時刻スタンプ）の略である。ＡＴＳは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳ（トランスポート・ストリーム）パケットをＸ個記録する。本発明の構成では、

トランスポートストリームを構成する各ブロックの第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロック（セクタ）のデータを暗号化するブロックキーを生成する。

ランダム性のあるＡＴＳを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

なお、図５に示すブロック・シード（Block Seed）は、ＡＴＳを含む付加情報である。ブロック・シードは、さらにＡＴＳだけでなくコピー制限情報(ＣＣＩ：Copy Control Information)も付加した構成としてもよい。この場合、ＡＴＳとＣＣＩを用いてブロックキーを生成する構成とすることができる。

なお、本発明の構成においては、ＤＶＤ等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図５の最下段に示すように、ブロックの先頭のｍ（例えば、ｍ＝８又は１６）バイトは暗号化されずに平文（Unencrypted data）のまま記録され、残りのデータ（ｍ＋１バイト以降）が暗号化される。これは暗号処理が８バイト単位としての処理であるために暗号処理データ長（Encrypted data）に制約が発生するためである。なお、もし、暗号処理が８バイト単位でなく、例えば１バイト単位で行えるなら、ｍ＝４として、ブロックシード以外の部分をすべて暗号化してもよい。

［ＴＳ処理手段における処理］

ここで、ＡＴＳの機能について詳細に説明する。ＡＴＳは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

すなわち、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームの中から１つ又は幾つかのＴＶプログラム（コンテンツ）を取り出した時、その取り出したトランスポートストリームを構成するトランスポ

ートパケットは、不規則な間隔で現れる（図７（Ａ）参照）。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはＭＰＥＧ２システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングが制御される。したがって、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをＤＶＤ等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すＡＴＳを付加して記録する。

図６に、ディジタルインタフェース経由で入力されるトランスポートストリームをＤＶＤ等の記録媒体であるストレージメディアに記録する時のＴＳ処理手段３００において実行する処理を説明するブロック図を示す。端子６００からは、ディジタル放送等のディジタルデータとしてトランスポートストリームが入力される。図１又は図２においては、入出力Ｉ／Ｆ１２０を介して、あるいは入出力Ｉ／Ｆ１４０、ＭＰＥＧコーデック１３０を介して端子６００からトランスポートストリームが入力される。

トランスポートストリームは、ビットストリームパーサー(parser)６０２に入力される。ビットストリームパーサー６０２は、入力トランスポートストリームの中からＰＣＲ(Program Clock Reference)パケットを検出する。ここで、ＰＣＲパケットとは、ＭＰＥＧ２システムズで規定されているＰＣＲが符号化されているパケットである。ＰＣＲパケットは、１００ｍｓｅｃ以内の時間間隔で符号化されている。ＰＣＲは、トランスポートパケットが受信側に到着する時刻を２７ＭＨｚの精度で表す。

そして、２７ＭＨｚＰＬＬ６０３において、記録再生器が持つ２７ＭＨｚクロックをトランスポートストリームのＰＣＲにロック（Lock）させる。タイムスタンプ発生回路６０４は、２７ＭＨｚクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード（Block seed）付加回路

６０５は、トランスポートパケットの第１バイト目がスムージングバッファ６０６へ入力される時のタイムスタンプをＡＴＳとして、そのトランスポートパケットに付加する。

ＡＴＳが付加されたトランスポートパケットは、スムージングバッファ６０６を通って、端子６０７から、暗号処理手段１５０に出力され、後段で説明する暗号処理が実行された後、ドライブ１９０（図１）、記録媒体Ｉ／Ｆ２１０（図２）を介してストレージメディアである記録媒体１９５に記録される。

図７は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図７（Ａ）は、ある特定プログラム（コンテンツ）を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図７（Ａ）に示すように不規則なタイミングで現れる。

図７（Ｂ）は、ブロック・シード（Block Seed）付加回路６０５の出力を示す。ブロック・シード（Block Seed）付加回路６０５は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すＡＴＳを含むブロック・シード（Block Seed）を付加して、ソースパケットを出力する。図７（Ｃ）は記録媒体に記録されたソースパケットを示す。ソースパケットは、図７（Ｃ）に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

図８は、記録媒体１９５に記録されたトランスポートストリームを再生する場合のＴＳ処理手段３００の処理構成ブロック図を示している。端子８００からは、後段で説明する暗号処理手段において復号されたＡＴＳ付きのトランスポートパケットが、ブロック・シード（Block seed）分離回路８０１へ入力され、ＡＴＳとトランスポートパケットが分離される。タイミング発生回路８０４は、再生器が持つ２７ＭＨｚクロック８０５のクロックカウンター値に基づいた時間を計算する。

なお、再生の開始時において、一番最初のＡＴＳが初期値として、タイミング発生回路８０４にセットされる。比較器８０３は、ＡＴＳとタイミング発生回路８０４から入力される現在の時刻を比較する。そして、タイミング発生回路８０

４が発生する時間とＡＴＳが等しくなった時、出力制御回路８０２は、そのトランスポートパケットをＭＰＥＧコーデック１３０又はディジタル入出力Ｉ／Ｆ１２０へ出力する。

図９は、入力ＡＶ信号を記録再生器１００のＭＰＥＧコーデック１３０においてＭＰＥＧエンコードして、さらにＴＳ処理手段３００においてトランスポートストリームを符号化する構成を示す。したがって、図９は、図１又は、図２おけるＭＰＥＧコーデック１３０とＴＳ処理手段３００の両処理構成を併せて示すブロック図である。端子９０１からは、ビデオ信号が入力されており、それはＭＰＥＧビデオエンコーダ９０２へ入力される。

ＭＰＥＧビデオエンコーダ９０２は、入力ビデオ信号をＭＰＥＧビデオストリームに符号化し、それをバッファビデオストリームバッファ９０３へ出力する。また、ＭＰＥＧビデオエンコーダ９０２は、ＭＰＥＧビデオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ，符号化ビット量，デコードタイムスタンプである。ここで、ピクチャタイプは、Ｉ／Ｐ／Ｂピクチャ（picture）の情報である。また、デコードタイムスタンプは、ＭＰＥＧ２システムズで規定されている情報である。

端子９０４からは、オーディオ信号が入力されており、それはＭＰＥＧオーディオエンコーダ９０５へ入力される。ＭＰＥＧオーディオエンコーダ９０５は、入力オーディオ信号をＭＰＥＧオーディオストリームに符号化し、それをバッファ９０６へ出力する。また、ＭＰＥＧオーディオエンコーダ９０５は、ＭＰＥＧオーディオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量，デコードタイムスタンプである。

多重化スケジューラ９０８には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ９０８は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ９０８は、内部に２７ＭＨｚ精度の基準

時刻を発生するクロックを持ち、そして、ＭＰＥＧ２で規定されている仮想的なデコーダモデルであるＴ－ＳＴＤを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

パケット符号化制御情報がビデオパケットの場合、スイッチ９７６はａ側になり、ビデオストリームバッファ９０３からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

パケット符号化制御情報がオーディオパケットの場合、スイッチ９７６はｂ側になり、オーディオストリームバッファ９０６から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

パケット符号化制御情報がＰＣＲパケットの場合、トランスポートパケット符号化器９０９は、多重化スケジューラ９０８から入力されるＰＣＲを取り込み、ＰＣＲパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器９０９へは何も入力されない。

トランスポートパケット符号化器９０９は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器９０９は、間欠的にトランスポートパケットを出力する。到着（Arrival）タイムスタンプ（time stamp）計算手段９１０は、多重化スケジューラ９０８から入力されるＰＣＲに基づいて、トランスポートパケットの第１バイト目が受信側に到着する時刻を示すＡＴＳを計算する。

多重化スケジューラ９０８から入力されるＰＣＲは、ＭＰＥＧ２で規定されるトランスポートパケットの１０バイト目の受信側への到着時刻を示すので、ＡＴＳの値は、ＰＣＲの時刻から１０バイト前のバイトが到着する時刻となる。

ブロック・シード（Block Seed）付加回路９１１は、トランスポートパケット

符号化器９０９から出力されるトランスポートパケットにＡＴＳを付加する。ブロック・シード（Block seed）付加回路９１１から出力されるＡＴＳ付きのトランスポートパケットは、スムージングバッファ９１２を通って、暗号処理手段１５０へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体１９５へ格納される。

記録媒体１９５へ格納されるＡＴＳ付きのトランスポートパケットは、暗号処理手段１５０で暗号化される前に図７（Ｃ）に示すように間隔を詰めた状態で入力され、その後、記録媒体１９５に格納される。トランスポートパケットが間隔を詰めて記録されても、ＡＴＳを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

ところで、ＡＴＳの大きさは３２ビットに決まっているわけではなく、２４ビット乃至３１ビットでも構わない。ＡＴＳのビット長が長いほど、ＡＴＳの時間カウンターが一周する周期が長くなる。例えば、ＡＴＳが２７ＭＨｚ精度のバイナリーカウンターである場合、２４－ｂｉｔ長のＡＴＳが一周する時間は、約０．６秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、ＭＰＥＧ２の規定により、最大０．１秒と決められているからである。しかしながら、十分な余裕を見て、ＡＴＳを２４－ｂｉｔ以上にしてもよい。

このように、ＡＴＳのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図１０に示す。図１０の例１は、ＡＴＳを３２ビット分使用する例である。図１０の例２は、ＡＴＳを３０ビットとし、コピー制御情報（CCI）を２ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、ＳＣＭＳ：Serial Copy Management SystemやＣＧＭＳ：Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free）、１世代のみのコピーを許可する１世代コピー許可（One Generation Copy Allowed）、コピーを認めないコピー禁止（Copy Prohibited）などの情報が表せる。

図１０に示す例３は、ＡＴＳを２４ビットとし、ＣＣＩを２ビット使用し、さらに他の情報を６ビット使用する例である。他の情報としては、例えばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン（Macrovision）のオン／オフ（On/Off）を示す情報など、様々な情報を利用することが可能である。

［キー配信構成としてのツリー（木）構造について］

次に、図１又は図２に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図１１は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図１１の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図１１に示す木（ツリー）構造の各葉(リーフ：leaf)がそれぞれの記録再生装置に相当する。

各デバイス０～１５は、製造時（出荷時）に、予め定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）及び各リーフのリーフキーを自身で格納する。図１１の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

図１１に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図１１のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図１１のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの

共存構成の上に図１１に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図１１の点線で囲んだ部分、即ちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行う機関は、図１１の点線で囲んだ部分、即ちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図１１のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行うプロバイダ、決済機関等によってグループ毎に管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図１１から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。例えば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Kmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスターキー：Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデー

タであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１,Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

更新キーの配布処理ついて説明する。キーの更新は、例えば、図１２（Ａ）に示すキー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

図１２（Ａ）に示すキー更新ブロック（ＫＲＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１２の例は、図１１に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図１１から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

図１２（Ａ）のＫＲＢに示されるようにＫＲＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図１２（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図１２（Ａ）の上から２段目の暗号化キーＥｎ

ｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図１２（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００を取得し、以下、図１２（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒを得ることができる。なお、図１２（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図１１に示すツリー構造の上位段のノードキー：Ｋ０,ＫＲの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図１２（Ｂ）のキー更新ブロック（ＫＲＢ：Key Renewal Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

図１２（Ｂ）に示すＫＲＢは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図１１に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスターキー：Ｋ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を図１２（Ｂ）に示すＫＲＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス０，１，２はＫＲＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスターキーＫ（ｔ）masterを得ることが可能になる。

［ＫＲＢを使用したマスターキーの配布］

図１３に、ｔ時点でのマスターキーＫ（ｔ）masterを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のマスターキーＫ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master）と図１２（Ｂ）に示すＫＲＢとを記録媒体を介して受領したデバイス０の処理を示す。

図１３に示すように、デバイス０は、記録媒体に格納されている世代：t時点のＫＲＢと自分が予め格納しているノードキーＫ０００を用いて上述したと同様のＫＲＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新マスターキーＫ（ｔ）masterを復号して、後にそれを使用するために自分だけが持つリーフキーＫ００００で暗号化して格納する。なお、デバイス０が更新マスターキーＫ（ｔ）master を安全に自身内に格納できる場合、リーフキーＫ００００で暗号化する必要はない。

また、この更新マスターキーの取得処理を図１４のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー:Ｋ（ｃ）masterを与えられ、自身のメモリに安全に（具体的には例えば、自身のリーフキーで暗号化して）格納しているものとする。

更新マスターキーＫ（ｎ）masterとＫＲＢの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップＳ１４０１において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーＫ（ｎ）masterの時点（世代）番号：ｎ（これを、プレ（pre－recording）記録世代情報（Generation#n）と呼ぶことにする）を読み出す。記録媒体には、予め、マスターキーＫ（ｎ）masterの時点（世代）番号：ｎが記憶されている。また、自身が保持している暗号化マスターキーＣを読み出し、ステップＳ１４０２において、その暗号化マスターキーの世代：ｃと、プレ記録世代情報Generation#nが表す世代：ｎとを比較して、その世代の前後を判定する。

ステップＳ１４０２において、プレ記録世代情報Generation#nが表す世代：ｎの方が、自身のメモリに記憶された暗号化マスターキーＣの世代：ｃよりも後でない（新しくない）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代：ｃが、プレ記録世代情報Generation#nが表す世代：ｎと同一か、又は後の場合、ステップＳ１４０３乃至Ｓ１４０８をスキップして、マスターキ

ー更新処理を終了する。すなわち、この場合、自身のメモリに記憶されたマスターキーＫ（ｃ）master（暗号化マスターキーＣ）の更新は行う必要がないので、その更新は行われない。

一方、ステップＳ１４０２において、プレ記録世代情報Generation#nが表す世代：ｎの方が、メモリに記憶された暗号化マスターキーＣの世代：ｃよりも後である（新しい）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎよりも前の世代である場合、ステップＳ１４０３に進み、記録再生装置は、記録媒体から、キー更新ブロック（ＫＲＢ：Key Renewal Block)を読み出す。

ステップＳ１４０４において、記録再生装置は、ステップＳ１４０３で読み出したＫＲＢと、自身がメモリに格納しているリーフキー（図１１のデバイス０におけるＫ００００）及びノードキー（図１１のデバイス０におけるＫ０００,Ｋ００...）を用いて、プレ記録世代情報Generation#n（図１３におけるｔ）時点でのノード００の鍵Ｋ（ｔ）００を計算する。

ステップＳ１４０５では、ステップＳ１４０４においてＫ（ｔ）００を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク（排除）されていることを示すので、ステップＳ１４０６乃至Ｓ１４０８をスキップしてマスターキー更新処理を終了する。

Ｋ（ｔ）００を得られた場合、ステップＳ１４０６に進み、記録媒体からＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master)、即ち、Ｋ（ｔ）００を用いても時点でのマスターキーを暗号化した値を読み出す。そしてステップＳ１４０７において、この暗号文をＫ（ｔ）００を用いて復号してＫ（ｔ）masterを計算する。

ステップＳ１４０８では、自身のみが持つリーフキー（図１１のデバイス０におけるＫ００００）を用いてＫ（ｔ）masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

ところで、マスターキーは、時点（世代）０から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、

一方向性関数ｆを保持しており、その一方向性関数ｆに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

具体的には、例えば、記録再生装置に記憶されているマスターキーＭＫの世代が世代ｉ＋１であり、あるデータの再生に必要な（記録時に使用された）マスターキーＭＫの世代が世代ｉ－１である場合、マスターキーＫ（ｉ－１）masterは、記録再生装置において、一方向性関数ｆが２回用いられ、ｆ（ｆ（Ｋ（ｉ＋１）master））を計算することにより生成される。

また、記録再生装置に記憶されているマスターキーの世代が世代ｉ＋１であり、必要なマスターキーの世代が世代ｉ－２である場合、マスターキーＫ（ｉ－２）masterは、一方向性関数ｆを３回用いて、ｆ（ｆ（ｆ（Ｋ（ｉ＋１）master）））を計算することにより生成される。

ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、ＭＤ５(Message Digest 5)や、ＳＨＡ－１(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーＫ（０）master，Ｋ（１）master，Ｋ（２）master・・・，Ｋ（Ｎ）masterを、予め求めておく。すなわち、まず最初に、第Ｎ世代のマスターキーＫ（Ｎ）masterを設定し、そのマスターキーＫ（Ｎ）masterに、一方向性関数を１回ずつ適用しいくことで、それより前の世代のマスターキーＫ（Ｎ－１）master，Ｋ（Ｎ－２）master，・・・，Ｋ（１）master，Ｋ（０）masterを順次生成しておく。そして、世代の小さい（前の）マスターキーＫ（０）masterから順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第０世代のマスターキーＫ（０）masterを設定し、そのマスターキーＫ（０）masterから使用していく。すなわち、キー発行機関は、第１世代以降のマ

スターキーＫ（ｉ）masterが必要になったら、その１世代前のマスターキーＫ（ｉ－１）masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、Ｎ世代のマスターキーを、予め生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

次に、この記録再生装置がコンテンツを自身の記録媒体に記録する場合の、記録再生装置の処理について図１５のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

まず最初に、ステップＳ１５０１において、記録再生装置は、記録媒体から、プレ記録世代情報Generation#nを読み出す。また、自身のメモリが記憶している暗号化マスターキーＣの世代ｃを取得し、ステップＳ１５０２において、その暗号化マスターキーの世代ｃと、プレ記録世代情報Generation#nが表す世代ｎとを比較して、その世代の前後を判定する。

ステップＳ１５０２において、メモリに記憶された暗号化マスターキーＣの世代ｃが、プレ記録世代情報Generation#nが表す世代ｎ以後でないと判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代ｃが、プレ記録世代情報Generation#nが表す世代ｎよりも古い世代である場合、ステップＳ１５０３をスキップして、即ち、コンテンツデータの記録処理を行わずに終了する。

一方、ステップＳ１５０２において、自身の記録再生装置内のメモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎ以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎと同一か、又はそれよりも新しい場合、ステップＳ１５０３に進み、コンテンツデータの記録処理を行う。

［世代管理のなされたマスターキーによるコンテンツデータ暗号化及び記録処理］

以下、世代管理のなされたマスターキーによってコンテンツデータの暗号化処理を実行して、自己の記録媒体に格納する処理について説明する。なお、ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用したデータに基づいてブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。また、記録再生装置が記録媒体に記録したデータを他の再生機器において再生可能とする設定と再生不可能とする設定が可能な構成を例として説明する。

図１６、図１７の処理ブロック図及び図１８のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

図１６、図１７の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理の概要について説明する。

記録再生装置１６００は自身のメモリ１８０（図１，２参照）に格納しているマスターキー１６０１、デバイス識別子としてのデバイスＩＤ１６３１、デバイス固有キー１６３２を読み出す。マスターキー１６０１は、ライセンスを受けた記録再生装置に格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図１１に示す点線枠のグループに属するデバイスに共通なキーである。デバイスＩＤは記録再生装置１６００の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスＩＤは公開されていてもよい。デバイス固有キーは、その記録再生器１６００に固有の秘密鍵であり、予め個々の記録再生装置に応じて異なるように設定されて格納されたキーである。これらは予め記録再生装置１６００のメモリに格納されている。

記録再生装置１６００は例えば光ディスクである記録媒体１６２０に識別情報としてのディスクＩＤ（Disc ID）１６０３が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）１６０３を読出し（図１６に

相当）、記録されていなければ、暗号処理手段１５０においてランダムに、もしくは予め定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）１７０１を生成し、ディスクに記録する（図１７に相当）。ディスクＩＤ（Disc ID）１６０３はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生器１６００は、次にマスターキーとディスクＩＤを用いて、ディスク固有キー（Disc Unique Key）を生成１６０２する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、図１９に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

次に、記録毎の固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０（図１，２，参照）においてランダムに、もしくは予め定められた例えば乱数発生等の方法で生成１６０４し、ディスク１６２０に記録する。

さらに、このタイトル（データ）がデータ記録を実行した記録再生装置でのみ再生可能とする（機器制限あり）か、他の機器においても再生可能とする（再生機器制限なし）のいずれであるかを示すフラグ、即ち再生機器制限フラグ（Player Restriction Flag）を設定し１６３３、ディスク１６２０に記録する１６３５。さらに、機器識別情報としてのデバイスＩＤ取り出して１６３１、ディスク１６２０に記録する１６３４。

さらに、使用するマスターキーの世代番号、即ち、自身が格納するマスターキーの世代番号［記録時世代番号（Generation#n）］１６５０を取得して、これを記録媒体１６２０に記録時世代番号１６５１として格納する。

ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー１６０５、再生機器制限フラグ１６３５、デバイスＩＤ１６３４、マスターキーの世代番号

[記録時世代番号（Generation#n）]１６５１を格納することができる。

なお、記録媒体１６２０には、予め、プレ（pre－recording）世代番号が格納されており、プレ世代番号と同一又はプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

すなわち、再生機器制限をしない場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとからタイトル固有キー（Title Unique Key）を生成し、再生機器制限をする場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キーとからタイトル固有キー（Title Unique Key）を生成する。

このタイトル固有キー（Title Unique Key）生成の具体的な方法は、図２１に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー（Title Key）とディスク固有キー（Disc Unique Key）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキーとディスクＩＤ（Disc ID）とデバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。

なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー

(Master Key) とディスクＩＤ (Disc ID) とタイトルキー (Title Key) と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とディスクＩＤ (Disc ID) と、デバイスＩＤ (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

ところで、例えば上記の５ＣＤＴＣＰに規定される伝送フォーマットのひとつを使用した場合、データはＭＰＥＧ２のＴＳパケットで伝送される場合がある。例えば、衛星放送を受信したセットトップボックス (ＳＴＢ：Set Top Box) がこの放送を記録機に５ＣＤＴＣＰを用いて伝送する際に、ＳＴＢは衛星放送通信路で伝送されたＭＰＥＧ２　ＴＳパケットをIEEE1394上も伝送することが、データ変換の必要がなく望ましい。

記録再生装置１６００は記録すべきコンテンツデータをこのＴＳパケットの形で受信し、前述したＴＳ処理手段３００において、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ＡＴＳとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

ＡＴＳを付加したＴＳパケットをＸ個 (例えばＸ＝３２) 並べて、１ブロックのブロックデータが形成 (図５の上の図参照) され、図１６、１７の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第１～４バイトが分離され (セレクタ１６０８) て出力される３２ビットのＡＴＳを含むブロックシード (Block Seed) と、先に生成したタイトル固有キー (Title Unique Key) とから、そのブロックのデータを暗号化する鍵であるブロック・キー (Block Key) が生成１６０７される。

ブロック・キー (Block Key) の生成方法の例を図２２に示す。図２２では、いずれも３２ビットのブロック・シード (Block Seed) と、６４ビットのタイトル固有キー (Title Unique Key) とから、６４ビットのブロックキー (Block Key) を生成する例を２つ示している。

上段に示す例１は、鍵長６４ビット、入出力がそれぞれ６４ビットの暗号関数

を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

例２は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をＳＨＡ－１に入力し、その１６０ビットの出力を、例えば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図１６、１７の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第１～ｍバイト（例えばｍ＝８バイト）は分離（セレクタ１６０８）されて暗号化対象とせず、ｍ＋１バイト目から最終データまでを暗号化１６０９する。なお、暗号化されないｍバイト中にはブロック・シードとしての第１～４バイトも含まれる。セレクタ１６０８により分離された第ｍ＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化１６０９される。暗号化アルゴリズムとしては、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がＤＥＳのように８バイトであるときは、Ｘを例えば３２とし、ｍを例えば８の倍数とすることで、端数なくｍ＋１バイト目以降のブロックデータ全体が暗号化できる。

すなわち、１ブロックに格納するＴＳパケットの個数をＸ個とし、暗号アルゴリズムの入出力データサイズをＬバイトとし、ｎを任意の自然数とした場合、１９２＊Ｘ＝ｍ＋ｎ＊Ｌが成り立つようにＸ，ｍ、Ｌを定めることにより、端数処理が不要となる。

暗号化した第ｍ＋１バイト以降のブロックデータは暗号処理のされていない第１～ｍバイトデータとともにセレクタ１６１０により結合されて暗号化コンテンツ１６１２として記録媒体１６２０に格納される。

以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ＡＴＳを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。

上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、即ち再生可能となる条件となる。

さらに、ブロックキーは上述のように再生機器制限をしない場合は、デバイスＩＤに基づいて生成され、再生機器制限をする場合は、デバイス固有キーに基づいて生成される。これらの暗号化データは、再生機器制限をした場合は、そのデータを記録した機器でのみ再生可能となる。

すなわち、再生機器制限なしの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイスＩＤを含むデータに基づいて生成されるとともに、デバイスＩＤが記録媒体に格納される。したがって、記録媒体上のコンテンツを再生しようとする機器は、記録媒体からデバイスＩＤを取得可能であり、同様のブロックキーを生成することが可能となるのでブロックデータの復号が可能となる。しかし、再生機器制限ありの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイス固有キーを含むデータに基づいて生成される。このデバイス固有キーはデバイス毎に異なる秘密鍵であり、他の機器は、そのキーを取得することはできない。また、ブロックデータを暗号化して記録媒体に格納する場合、デバイス固有キーの記録媒体に対する書き込み処理は実行されない。したがって、他

の再生機器では、暗号化されたブロックデータを格納した記録媒体を装着しても、同一のデバイス固有キーを取得することができないので、ブロックデータを復号するための復号キーを生成することができず、復号不可能となり再生できない。なお、再生処理の詳細については後述する。

次に図１８に示すフローチャートに従って、データ記録処理にともなって実行されるＴＳ処理手段３００におけるＡＴＳ付加処理及び暗号処理手段１５０における暗号処理の処理の流れを説明する。図１８のＳ１８０１において、記録再生装置は自身のメモリ１８０に格納しているマスターキー、デバイス識別子としてのデバイスＩＤ、デバイス固有キーを読み出す。

Ｓ１８０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ１８０３でこのディスクＩＤを読出し、記録されていなければＳ１８０４で、ランダムに、もしくは予め定められた方法でディスクＩＤを生成し、ディスクに記録する。次に、Ｓ１８０５では、マスターキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

次にＳ１８０６に進み、その一回の記録毎の固有の鍵としてのタイトルキー（Title Key）、再生機器制限フラグ（Player Restriction Flag）、さらに、機器識別情報としてのデバイスＩＤ、マスターキーの世代番号を取り出してディスクに記録する。次にＳ１８０７で、上記のディスク固有キーとタイトルキーと、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）から、タイトル固有キーを生成する。

タイトル固有キーの生成の詳細フローを図２０に示す。暗号処理手段１５０は、ステップＳ２００１において、再生機器制限をするかしないかの判定を実行する。この判定は、記録再生器を使用するユーザによって入力された指示データ、あるいはコンテンツに付加された利用制限情報に基づいて判定する。

Ｓ２００１の判定がＮｏ、即ち、再生機器制限をしない場合は、ステップＳ２００２に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title K

ey）と、デバイスＩＤとから、タイトル固有キー（Title Unique Key）を生成する。

Ｓ２００１の判定がＹｅｓ、即ち、再生機器制限をする場合は、ステップＳ２００３に進みディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キーとから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

Ｓ１８０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ１８０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ１８１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ１８１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

次に、暗号処理手段１５０は、Ｓ１８１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ１８０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

Ｓ１８１３では、ブロックキーを用いてＳ１８１１で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

Ｓ１８１４で、暗号化したブロックデータを記録媒体に記録する。Ｓ１８１５で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ１８０８に戻って残りのデータの処理を実行する。

［世代管理のなされたマスターキーによるコンテンツデータ復号及び再生処理］

次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図２３の処理ブロック図と、図２４～図２６のフローチャートを用いて説明する。

図２３の処理ブロック図を参照しながら、図２４に示すフローチャートに従って、復号処理及び再生処理について、処理の流れを説明する。図２４のＳ２４０１において、記録再生装置２３００はディスク２３２０からディスクＩＤ２３０２とプレ（pre－recording）記録世代番号を読み出し、また自身のメモリからマスターキー２３０１、デバイス識別子としてのデバイスＩＤ２３３１、デバイス固有キー２３３２を読み出す。先の記録処理の説明から明らかなように、ディスクＩＤはディスクに予め記録されているか、そうでない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。

プレ（pre－recording）記録世代番号２３６０は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このプレ（pre－recording）世代番号と、データ記録時のマスターキーの世代番号、即ち記録時世代番号２３５０を比較して再生処理の可否を制御する。マスターキー２３０１は、ライセンスを受けた記録再生装置に格納され世代管理のなされた秘密キーであり、デバイスＩＤは記録再生装置固有の識別子、デバイス固有キーは、その記録再生器に固有の秘密鍵である。

記録再生装置２３００は、次に、Ｓ２４０２で、ディスクから読み出すべきデータのタイトルキー、さらに、このデータを記録した記録再生器のデバイスＩＤと、データに対応して設定された再生機器制限フラグ、データを記録したときに使用したマスターキーの世代番号（Generation #）、即ち記録時世代番号２３５０を読み出す。次に、Ｓ２４０３で読み出すべきデータが再生可能か否かを判定する。判定の詳細フローを図２５に示す。

図２５のステップＳ２５０１において、記録再生装置は、Ｓ２４０１で読み出したプレ世代番号と、Ｓ２４０２で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、プレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、プレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップＳ２４０４乃至

Ｓ２４０９をスキップして、再生処理を行わずに処理を終了する。したがって、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

すなわち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

一方、ステップＳ２５０１において、記録時世代番号が表す世代が、プレ記録世代番号が表す世代以後であると判定された場合、即ち、記録時世代情報が表す世代が、プレ記録世代番号が表す世代ｎと同一か、又は新しい世代であり、従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステップＳ２５０２に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーＣの世代情報を取得し、その暗号化マスターキーの世代と、暗号時世代情報が表す世代を比較して、その世代の前後を判定する。

ステップＳ２５０２において、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップＳ２４０４乃至Ｓ２４０９をスキップして、再生処理を行わずに処理を終了する。

一方、ステップＳ２５０２において、メモリに記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代と同一か、又はそれよりも新しい場合、ステップＳ２５０３に進み、読出しをしたいデータが再生機器制限されて記録されているかどうかを検査する。

ステップＳ２５０３では、読み出した再生機器制限フラグの示す再生機器制限情報が、「再生機器制限あり」の設定であるか否かを判定する。ありの場合は、

ステップＳ２５０４において、「記録媒体から読み出したデバイスＩＤと自己のデバイスＩＤが一致するか否か」を判定する。一致する場合は、再生可能と判定する。ステップＳ２５０３において、「再生機器制限あり」の設定でないと判定された場合も、再生可能と判定する。読み出した再生機器制限フラグが示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤと自己のデバイスＩＤが一致しない」場合は、再生不可能と判定する。

再生可能と判定された場合は、ステップＳ２４０４に進む。Ｓ２４０４では、ディスクＩＤ（Disc ID）とマスターキー（Master Key）を用いてディスク固有キー（Disc Unique Key）を生成２３０３する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、Ｓ２４０２で記録媒体から読み出した、そのデータの記録時世代番号が表す世代（時点）のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、前述した方法を用いて記録時世代番号が表す世代のマスターキーを作成し、それを用いてディスク固有キー（Disc Unique Key）を生成してもよい。

次に、Ｓ２４０５で、タイトル固有キーの生成を行う。タイトル固有キーの生成の詳細フローを図２６に示す。暗号処理手段１５０は、ステップＳ２６０１において、再生機器制限をするの設定であるか、しないの設定であるかの判定を実行する。この判定は、ディスクから読み出した再生機器制限フラグに基づいて実行される。

データを記録した記録再生器のデバイスＩＤ２３３４と、データに対応して設定された再生機器制限フラグ２３３５を読み出し、読み出した再生機器制限フラグ２３３５が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤ２３３４と自己のデバイスＩＤ２３３１が一致する」か、あるいは、読み出した再生機器制限フラグ２３３３が示す再生機器制限

情報が、「再生機器制限なし」である場合は、再生可能となり、読み出した再生機器制限フラグ２３３３が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤ２３３４と自己のデバイスＩＤ２３３１が一致しない」場合は、再生不可能となる。

再生不可能とされる場合は、データは、そのデータを記録した記録再生器固有のデバイス固有キーに基づいて生成されたブロックキーによって暗号化されており、そのデータを記録した記録再生器以外の記録再生器は同一のデバイス固有キーを保有しないので、データを復号するためのブロックキーを生成することができない場合である。

再生可能である場合は、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

すなわち、再生機器制限をしない設定である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとからタイトル固有キー（Title Unique Key）を生成し、再生機器制限をする設定である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、自己のデバイス固有キーとからタイトル固有キー（Title Unique Key）を生成する。このキー生成方法としては、ハッシュ関数SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

図２６のフローに従って説明する。Ｓ２６０１の判定がＮｏ、即ち、再生機器制限をしない設定である場合は、ステップＳ２６０２に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとから、タイトル固有キー（Title Unique Key）を生成する。

Ｓ２６０１の判定がＹｅｓ、即ち、再生機器制限をする場合は、ステップＳ２６０３に進みディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、自己の記録再生器の有するデバイス固有キーとから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

次にＳ２４０６でディスクから暗号化されて格納されている暗号化コンテンツ２３１２から順次ブロックデータ（Block Data）を読み出し、Ｓ２４０７で、ブロックデータの先頭の４バイトのブロック・シード（Block Seed）をセレクタ２３１０において分離して、ブロックシード（Block Seed）と、Ｓ２４０５で生成したタイトル固有キーを用いてブロックキーを生成する。

ブロック・キー（Block Key）の生成方法は、先に説明した図２２の構成を適用することができる。すなわち、３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する構成が適用できる。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、ブロックシード（Block Seed）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、次にＳ２４０８で、ブロックキー（Block Key）

を用いて暗号化されているブロックデータを復号２３０９し、セレクタ２３０８を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにＡＴＳが付加されており、先に説明したＴＳ処理手段３００において、ＡＴＳに基づくストリーム処理が実行される。その後、データは、使用、例えば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。ブロックキーを用いて暗号化されているブロックデータを復号し、Ｓ２４０９で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければＳ２４０６に戻り残りのデータを読み出す。

［記録媒体にのみ有効なメディアキーを使用した処理構成］

ところで、上記の実施例においては、キー更新ブロックＫＲＢ：Key Renewal Blockを用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うとしていた。

マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点及びそれ以前にこのシステムで記録されたデータを復号することが可能になる。但し、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

これに対し、記録媒体のＫＲＢ（Key Renewal Block）を用いて伝送する鍵として、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることも可能である。以下に、第２の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。但し、第１の実施例との変更部分のみを説明する。

図２７には、図１３と同様の例として、デバイス０が記録媒体に格納されている ｔ 時点のＫＲＢと自分が予め格納しているリーフキーＫ００００とノードキーＫ０００，Ｋ００を用いて更新ノードキーＫ（ｔ）００を生成し、それを用いて更

新メディアキー：Ｋ（ｔ）mediaを得る様子を示している。ここで得たＫ（ｔ）mediaは、その記録媒体のデータの記録、再生時に使用される。

なお、図２７におけるプレ記録世代番号（Generation #n)は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオプションとして設定される。

各記録再生装置は、例えば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図２８に示すフローチャートによってその記録媒体用のメディアキー：Ｋ（ｔ）mediaを計算し、後にその記録媒体へのアクセスに使用する。

図２８のステップＳ２８０１のＫＲＢの読みこみとＳ２８０２のＫＲＢの処理は、それぞれ図１４のステップＳ１４０３及びＳ１４０４と同様の処理である。

ステップＳ２８０３において記録再生装置はメディアキーＫ（ｔ）mediaをノードキー Ｋ（ｔ）００で暗号化した暗号文Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media)を記録媒体から読みこみ、ステップＳ２８０４でこれを復号してメディアキーを得る。もしこの記録再生装置が図１１に示すツリー構成のグループから排除、即ちリボークされていれば、メディアキーを入手できず、その記録媒体への記録及び再生が行えない。

次に、記録媒体へのデータの記録の処理を説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第１の実施例において図１５に示した、プレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図２９に示す処理フローのようになる。図２９の処理フローは、メディアキーの取得をＳ２９０１で判定し、取得された場合にのみ、ステップＳ２９０２においてコンテンサの記録処理を実行するものである。

［記録媒体にのみ有効なメディアキーを使用したデータの記録処理］

コンテンツデータの記録処理の様子を、図３０、３１のブロック図及び図３２のフローチャートを用いて説明する。

本実施例では、第１の実施例と同様、記録媒体として光ディスクを例とする。

この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている点も同様である。

図３０及び図３１は、それぞれ第１の実施例における図１６及び図１７に対応する図であり、マスターキー（Master Key）の代わりにメディアキー（Media Key）が使われている点が異なっており、また、マスターキーの世代を示す記録時世代番号（Generation #）を用いていない点が異なっている。図３０及び図３１の差異は、図１６、図１７の差異と同様ディスクＩＤの書き込みを実行するかしないかの差異である。

図３２はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、実施例１の図１８のフローチャートに対応する。以下、図３２の処理フローについて実施例１と異なる点を中心として説明する。

図３２のＳ３２０１において、記録再生装置３０００は自身のメモリに格納している機器識別情報（Device ID）、機器固有鍵（Device Unique Key）と、図２８のＳ２８０４で計算し、一時的に保存しているメディアキーＫ（ｔ）mediaを読み出す。

Ｓ３２０２において、記録再生装置は記録媒体（光ディスク）３０２０に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、Ｓ３２０３でこのディスクＩＤ（Disc ID）を読出し（図３０に相当）、記録されていなければ、Ｓ３２０４で、ランダムに、もしくは予め定められた方法でディスクＩＤ（Disc ID）を生成し、ディスクに記録する（図３１に相当）。ディスクＩＤ（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次にＳ３２０５に進む。

Ｓ３２０５では、Ｓ３２０１で読み出したメディアキーとディスクＩＤ（Disc ID）を用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、第１の実施例で使用した方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

次にＳ３２０６に進み、その一回の記録毎に固有の鍵：タイトルキー（Title

Key）をランダムに、あるいはあからじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル（データ）が、記録した機器でのみ再生できるもの（再生機器制限する）か、他の機器でも再生できる（再生機器制限しない）かを表す情報としての再生機器制限フラグ（Player Restriction Flag）と、記録機器が持つ機器識別情報（Device ID）をディスクに記録する。

ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、再生機器制限フラグ（Player Restriction Flag）、機器識別情報（Device ID）を格納することができる。

ステップＳ３２０７乃至Ｓ３２１５は図１８のＳ１８０７乃至Ｓ１８１５と同様であるため説明を省略する。

なお、上記の説明では、メディアキー（Media Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

［記録媒体にのみ有効なメディアキーを使用したデータの再生処理］

次に、上記のようにして記録されたデータを再生する処理の様子を図３３のブロック図と図３４のフローチャートを用いて説明する。

図３３は、第１の実施例における図２３に対応する図であり、マスターキー（Master Key）の代わりにメディアキー（Media Key）が使われ、そのため記録時

世代番号（Generation #）が省略されている点が異なっている。

図３４のＳ３４０１において、記録再生装置３４００は記録媒体であるディスク３４２０からディスクＩＤ（Disc ID）を、また自身のメモリから自己の機器識別情報としてデバイスＩＤ（Device ID）,自己の機器固有鍵であるデバイス固有キー（Device Unique Key）と、図２８のＳ２８０４で計算し一時的に保存しているメディアキーを読み出す。

なお、この記録媒体の挿入時に、図２８の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

次にＳ３４０２で、ディスクから読み出すべきデータのタイトルキー（Title Key）とこのデータを記録した機器のデバイスＩＤ（Device ID）とこのデータの再生機器制限フラグ（Player Restriction Flag）を読み出す。

次にＳ３４０３で、このデータが再生可能であるか否かを判断する。Ｓ３４０３の処理の詳細を図３５に示す。

ステップＳ３５０１ではメディアキー（Media Key）を得られたか否かを判定する。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップＳ３５０２に進む。ステップＳ３５０２及びＳ３５０３の処理は図２５のＳ２５０３及びＳ２５０４とそれぞれ同じであり、再生機器制限フラグ（Player Restriction Flag）が表す再生機器制限の状態が、「再生機器制限されている」であり、かつ、Ｓ３５０３で記録媒体から読み出した記録した機器のデバイスＩＤ（Device ID）と、Ｓ３４０１でメモリから読み出した自己のデバイスＩＤ（Device ID）により、「記録した機器が自分ではない」という２つの条件が重なった場合には「再生不可能」と判断し、ステップＳ３４０４乃至Ｓ３４０９をスキップして、再生処理を行わずに処理を終了し、一方それ以外の場合には「再生可能」と判断してＳ３４０４に進む。

ステップＳ３４０４乃至Ｓ３４０９の処理は、図２４のＳ２４０４乃至Ｓ２４０９と同様であるため、説明を省略する。

なお、上記の説明では、メディアキー（Media Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス

固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

上記のようにして、記録媒体へのデータの記録及び記録媒体からの再生が行える。

［記録再生装置による記録媒体へのキー更新ブロック（ＫＲＢ）格納処理］

ところで、上述した例では、キー更新ブロック：ＫＲＢ（Key Renewal Block）が記録媒体に予め格納されている例を示したが、図３６に示すように、記録再生装置３６００が入出力Ｉ／Ｆ１２０，１４０や、モデム３６０１等を介して他の機器から受信したＫＲＢ（Key Renewal Block）を、最初に記録媒体にデータを記録する際や、記録媒体にデータを記録するたび毎に記録媒体に記録するようにすることもできる。

すなわち、例えば第１の実施例において、図３７に示すように、記録再生装置は予め、入出力Ｉ／Ｆ１２０，１４０やモデム３６０１等を介してキー更新ブロック：ＫＲＢ（Key Renewal Block）とマスターキーをノードキーで暗号化した暗号文を入手し、自身の記憶手段であるメモリ１８０等に格納しておき、コンテンツデータの記録媒体に対する記録の際に、図３８に示すフローチャートに従って処理をする構成としてもよい。

図３８の処理フローについて説明する。ステップＳ３８０１において、データを記録しようとする記録媒体には既にキー更新ブロック：ＫＲＢ（Key Renewal Block）が記録されているか否かを検査する。既に記録媒体にキー更新ブロック：ＫＲＢ（Key Renewal Block）が記録されていた場合にはステップＳ３８０２をスキップして終了する（データの記録処理に進む）が、記録されていない場合には、ステップＳ３９０２に進み、図３９に示すように、自身の記憶手段、例えばメモ

リ１８０に格納しているキー更新ブロック：ＫＲＢ（Key Renewal Block）とマスターキーを暗号化した暗号文を記録媒体に記録する処理を実行する。その処理の実行の後に、コンテンツデータの記録処理に進む。

この方法は、マスターキーに特化したものではなく、例えば第２の実施例のようにメディアキーを用いる記録方法に適用することももちろん可能である。

［記録処理におけるコピー制御］

さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

すなわち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図１又は図２の記録再生装置の処理について、図４０及び図４１のフローチャートを参照して説明する。

まず、外部からのディジタル信号のコンテンツを、記録媒体に記録する場合においては、図４０（Ａ）のフローチャートに従った記録処理が行われる。図４０（Ａ）の処理について説明する。図１の記録再生器１００を例として説明する。ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ４００１において、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを受信し、ステップＳ４００２に進む。

ステップＳ４００２では、入出力Ｉ／Ｆ１２０は、受信したディジタルコンテンツが、コピー可能であるかどうかを判定する。すなわち、例えば、入出力Ｉ／Ｆ１２０が受信したコンテンツが暗号化されていない場合（例えば、上述のＤＴＣＰを使用せずに、平文のコンテンツが、入出力Ｉ／Ｆ１２０に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

また、記録再生装置１００がＤＴＣＰに準拠している装置であるとし、ＤＴＣ

Ｐに従って処理を実行するものとする。ＤＴＣＰでは、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

記録再生装置１００の入出力Ｉ／Ｆ１２０に供給される信号にＥＭＩが含まれ、そのＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

ステップＳ４００２において、コンテンツがコピー可能でないと判定された場合、ステップＳ４００３～Ｓ４００５をスキップして、記録処理を終了する。したがって、この場合には、コンテンツは、記録媒体１０に記録されない。

また、ステップＳ４００２において、コンテンツがコピー可能であると判定された場合、ステップＳ４００３に進み、以下、ステップＳ４００３～Ｓ４００５において、図３（Ａ）のステップＳ３０２、Ｓ３０３、Ｓ３０４における処理と同様の処理が行われる。すなわち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

なお、ＥＭＩは、入出力Ｉ／Ｆ１２０に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、ＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（例えば、ＤＴＣＰにおけるembedded CCIなど）も記録される。

この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

本発明の記録再生装置では、このＥＭＩやembedded CCIなどのコピー制御情報を、ＴＳパケットに付加する形で記録する。すなわち、図１０の例２や例３のように、ＡＴＳを２４ビット乃至３０ビット分と、コピー制御情報を加えた３２ビットを図５に示すように各ＴＳパケットに付加する。

外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図４０（Ｂ）のフローチャートにしたがった記録処理が行われる。図４０（Ｂ）の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ４０１１において、そのアナログコンテンツを受信し、ステップＳ４０１２に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

ここで、ステップＳ４０１２の判定処理は、例えば、入出力Ｉ／Ｆ１４０で受信した信号に、マクロビジョン(Macrovision)信号や、ＣＧＭＳ－Ａ(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。すなわち、マクロビジョン信号は、ＶＨＳ方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力Ｉ／Ｆ１４０で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

また、例えば、ＣＧＭＳ－Ａ信号は、ディジタル信号のコピー制御に用いられるＣＧＭＳ信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、１度だけコピーして良いもの(Copy-one-generation)、又はコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

したがって、ＣＧＭＳ－Ａ信号が、入出力Ｉ／Ｆ１４０で受信した信号に含まれ、かつ、そのＣＧＭＳ－Ａ信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

さらに、例えば、マクロビジョン信号も、ＣＧＭＳ－Ａ信号も、入出力Ｉ／Ｆ４で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能で

あると判定される。

ステップＳ４０１２において、アナログコンテンツがコピー可能でないと判定された場合、ステップＳ４０１３乃至Ｓ４０１７をスキップして、記録処理を終了する。したがって、この場合には、コンテンツは、記録媒体１０に記録されない。

また、ステップＳ４０１２において、アナログコンテンツがコピー可能であると判定された場合、ステップＳ４０１３に進み、以下、ステップＳ４０１３乃至Ｓ４０１７において、図３（Ｂ）のステップＳ３２２乃至Ｓ３２６における処理と同様の処理が行われ、これにより、コンテンツがディジタル変換、ＭＰＥＧ符号化、ＴＳ処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

なお、入出力Ｉ／Ｆ１４０で受信したアナログ信号に、ＣＧＭＳ－Ａ信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのＣＧＭＳ－Ａ信号も、記録媒体に記録される。すなわち、図１０で示したＣＣＩもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。但し、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

［再生処理におけるコピー制御］

次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図４１（Ａ）のフローチャートに従った再生処理が行われる。図４１（Ａ）の処理について説明する。まず最初に、ステップＳ４１０１、Ｓ４１０２、Ｓ４１０３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段１５０において復号処理がなされ、ＴＳ処理がなされる。各処理が実行されたディジタルコンテンツは、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。

入出力Ｉ／Ｆ１２０は、ステップＳ４１０４において、そこに供給されるディ

ジタルコンテンツが、後でコピー可能なものかどうかを判定する。すなわち、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩが含まれる場合、従って、コンテンツの記録時に、ＤＴＣＰの規格に従って、ＥＭＩが記録された場合には、そのＥＭＩ（記録されたＥＭＩ(Recorded EMI)）が、Copy-freelyであるときには、ディジタルコンテンツは、後でコピー可能なものであると判定される。また、ＥＭＩが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

なお、一般的には、記録されたＥＭＩが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのＥＭＩは記録時にNo-more-copiesに変換され、また、Copy-neverのＥＭＩを持つディジタルコンテンツは、記録媒体に記録されないからである。但し、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

ステップＳ４１０４において、コンテンツが、後でコピー可能なものであると判定された場合、ステップＳ４１０５に進み、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを、外部に出力し、再生処理を終了する。

また、ステップＳ４１０４において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップＳ４１０６に進み、入出力Ｉ／Ｆ１２０は、例えば、ＤＴＣＰの規格等に従って、ディジタルコンテンツを、そのディジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

すなわち、例えば、上述のように、記録されたＥＭＩが、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力Ｉ／Ｆ１２０は、ＤＴＣＰの規格に従い、相手の装置との間

で認証を相互に行い、相手が正当な装置である場合（ここでは、ＤＴＣＰの規格に準拠した装置である場合）には、ディジタルコンテンツを暗号化して、外部に出力する。

次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４１（Ｂ）のフローチャートに従った再生処理が行われる。図４１（Ｂ）の処理について説明する。ステップＳ４１１１乃至Ｓ４１１５において、図４（Ｂ）のステップＳ４２１乃至Ｓ４２５における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、ＴＳ処理、ＭＰＥＧデコード、Ｄ／Ａ変換が実行される。これにより得られるアナログコンテンツは、入出力Ｉ／Ｆ１４０で受信される。

入出力Ｉ／Ｆ１４０は、ステップＳ４１１６において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。すなわち、例えば、記録されていたコンテンツにＥＭＩなどのコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、コンテンツの記録時に、例えばＤＴＣＰの規格に従って、ＥＭＩ又はコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

また、ＥＭＩ又はコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ又はコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

さらに、例えば、入出力Ｉ／Ｆ１４０に供給されるアナログコンテンツにＣＧＭＳ－Ａ信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにＣＧＭＳ－Ａ信号が記録された場合には、そのＣＧＭＳ－Ａ信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

ステップＳ４１１６において、コンテンツが、後でコピー可能であると判定された場合、ステップＳ４１１７に進み、入出力Ｉ／Ｆ１４０は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

また、ステップＳ４１１６において、コンテンツが、後でコピー可能でないと判定された場合、ステップＳ４１１８に進み、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

すなわち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すＧＣＭＳ－Ａ信号を付加して、外部に出力する。また、例えば、記録されたＣＧＭＳ－Ａ信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力Ｉ／Ｆ４は、ＣＧＭＳ－Ａ信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

［データ処理手段の構成］

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。すなわち、例えば、暗号処理手段１５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にＴＳ処理手段３００も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、

そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図４２は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク４２０５やＲＯＭ４２０３に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体４２１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体４２１０は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体４２１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部４２０８で受信し、内蔵するハードディスク４２０５にインストールすることができる。

コンピュータは、ＣＰＵ(Central Processing Unit)４２０２を内蔵している。ＣＰＵ４２０２には、バス４２０１を介して、入出力インタフェース４２１１が接続されており、ＣＰＵ４２０２は、入出力インタフェース４２１０を介して、ユーザによって、キーボードやマウス等で構成される入力部４２０７が操作されることにより指令が入力されると、それに従って、ＲＯＭ(Read Only Memory)４２０３に格納されているプログラムを実行する。

あるいは、ＣＰＵ４２０２は、ハードディスク４２０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部４２０８で受信されてハードディスク４２０５にインストールされたプログラム、又はドライブ４２０９に装着されたリムーバブル記録媒体４２１０から読み出されてハードディスク４２０５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)４

２０４にロードして実行する。

これにより、ＣＰＵ４２０２は、上述したフローチャートに従った処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ４２０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース４２１１を介して、ＬＣＤ(Liquid CryStal Display)やスピーカ等で構成される出力部４２０６から出力、あるいは、通信部４２０８から送信、さらには、ハードディスク４２０５に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、１のコンピュータにより処理されるものであってもよいし、複数のコンピュータによって分散処理されるものであってもよい。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであってもよい。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図１及び図２に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。同様に、ＴＳ処理手段３００の処理もＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することが可能である。

［記録媒体の製造装置及び方法］

次に、上述した本発明の情報記録媒体を製造する本発明の情報記録媒体製造装置及び方法について説明する。

図４３には、記録媒体を製造するとともに、記録媒体に対してディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキーを記録するディスク製造装置の概略構成を示す。

この図４３に示すディスク製造装置は、図示しない組立工程により既に組み立てられている情報記録媒体に対して、ディスクＩＤ（Disk ID），キー更新ブロッ

ク：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキーを記録する。さらに、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）も併せて記録する。

ディスク製造装置４３００は、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキーを予め格納しているメモリ４３０２もしくはその他の記憶手段と、記録媒体４３５０に対する読み書きを行う記録媒体Ｉ／Ｆ４３０３と、他の装置とのＩ／Ｆとなる入出力Ｉ／Ｆ４３０４と、それらを制御する制御部４３０１、これらを接続するバス４３０５を備えている。

なお、図４３の構成では、メモリ４３０２及び記録媒体Ｉ／Ｆ４３０４は、当該製造装置に内蔵されている例を挙げているが、メモリ４３０２及び記録媒体Ｉ／Ｆ４３０３は外付けのものであってもよい。

上記のディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）は、例えば図示しない鍵発行センタにより発行されるものであり、上記内蔵あるいは外付けのメモリに予め格納されている。

上記メモリ４３０２に格納されているディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキーは、制御部４３０１の制御の下、記録媒体Ｉ／Ｆ４３０３を介して記録媒体に記録される。なお、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）についても記録する。

また、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）は、上述したようにメモリ４３０２に予め格納されているものを使用するだけでなく、例えば入出力Ｉ／Ｆ４３０４を介して鍵発行センタから送られてきたものを入手することも可能である。

図４４には、本発明の記録媒体製造方法として、上記記録媒体を製造するとと

もに、記録媒体に対してディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録する記録媒体製造方法における製造工程の流れを示す。

図４４において、記録媒体製造方法では、まず、ステップＳ４４０１の製造工程として、図示しない公知の組立工程によりＤＶＤ、ＣＤ等各種記録媒体が組み立てられる。

次に、ステップＳ４４０２の製造工程として、図４３の記録媒体製造装置により、製造された記録媒体に対して、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキーの記録処理を実行する。また、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録する。

以上のディスク製造処理プロセスにより、記録媒体は、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）及び、暗号化されたマスターキー又は暗号化されたメディアキーを記録した状態で製造工場から出荷される。また、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録した後、製造工場から出荷される。

［ＫＲＢのフォーマット］

図４５にキー更新ブロック（ＫＲＢ：Key Renewal Block）のフォーマット例を示す。バージョン４５０１は、キー更新ブロック（ＫＲＢ：Key Renewal Block）のバージョンを示す識別子である。デプス４５０２は、キー更新ブロック（ＫＲＢ：Key Renewal Block）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ４５０３は、キー更新ブロック（ＫＲＢ：Key Renewal Block）中のデータ部の位置を示すポインタであり、タグポインタ４５０４はタグ部の位置、署名ポインタ４５０５は署名の位置を示すポインタである。データ部４５０６は、例えば更新するノードキーを暗号化したデータを格納する。

タグ部４５０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図４６を用いて説明する。図４６では、データとして先に図１２（Ａ）で説明したキー更新ブロック

（ＫＲＢ）を送付する例を示している。この時のデータは、図４６の右の表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。

暗号化キーの最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図４６の左の階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図４６（ｃ）に示すデータ列、及びタグ列が構成される。ツリーのノードの処理の順序として同一段の幅方向を先に処理するｗｉｄｔｈ　ｆｉｒｓｔと、深さ方向を先に処理するｄｅｐｔｈ　ｆｉｒｓｔのいずれかを用いるのが好適である。

図４５に戻って、ＫＲＢフォーマットについてさらに説明する。署名（Signature）は、キー更新ブロック（ＫＲＢ）を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。ＫＲＢを受領したデバイスは署名検証によって正当なキー更新ブロック（ＫＲＢ）発行者が発行したキー更新ブロック（ＫＲＢ）であることを確認する。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

以上、説明したように、本発明の情報記録再生装置によれば、ツリー（木）構造の鍵配布構成により、マスターキーやメディアキーの更新データを更新ブロッ

ク（ＫＲＢ）とともに送信する構成としたので、鍵更新の必要なデバイスにのみ復号可能な構成とした伝送又は配布が可能となり、メッセージ量を小さく抑えることができる。さらに、ツリー構造によって規定される特定のグループにのみ復号可能な鍵をメッセージ量を少なくして配布可能であり、グループに属さない他のデバイスには復号できない構成とすることが可能であり、キー配信又は配布の安全性が確保される。

また、ツリー構造の鍵配信方式を用いて各記録再生装置に伝送する鍵の種類を、ツリーを構成する特定のグループによって規定されるシステムで共通に利用できるマスターキーとすることも、各記録媒体毎に固有のメディアキーとすることも可能であり、それぞれに固有のＫＲＢを生成してネットワーク配信、又はメディアを介して配布することにより、キー更新が容易にかつ安全に実行される。

このため、本発明によれば、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができる情報記録再生システムを構成することが可能である。

また、世代管理を行ったマスターキーを使用するシステムにおいて、ＫＲＢにより更新された新たな世代のマスターキーを配布する構成とすることにより、ＫＲＢとともに暗号化されて配布される更新マスターキーを更新可能なデバイスを特定した固有のキーブロックを構成可能であるので、従来のデバイス単位での認証処理等を実行することなく、安全に更新の必要なデバイスのみが復号可能な暗号化マスターキーを構成して安全に鍵更新が実行できる。

さらに、本発明の情報記録再生装置及び方法によれば、世代管理されたマスターキー、あるいはメディアキーによる暗号化処理のみならず、再生機器制限処理を可能とした暗号処理を実行して記録媒体に格納する構成としている。本構成によって、データを記録媒体に記録する際に、その機器でのみ再生できるようにする（再生機器制限する）場合には機器固有鍵（デバイス固有キー）をデータの暗号鍵に作用させ、そうでない（再生機器制限しない）場合には機器識別情報（デバイスＩＤ）をデータの暗号鍵に作用させて暗号化するようにする。さらに、記録した機器の機器識別情報と、再生機器制限したかしないかのどちらのモードで記録したかを表す情報（再生機器制限フラグ）を記録媒体に記録しておく構成と

したので、データの再生時に、再生機器制限されている場合には機器固有鍵を知っている記録した機器のみがデータを復号でき、再生機器制限されていない場合にはいずれの機器でも記録機器の機器識別情報を用いてデータを復号できるようになる。

また、各パケットの着信時刻に応じたランダム性のあるデータとして構成されるＡＴＳを用いてブロック・データを暗号化するブロックキーを生成する構成としたので、ブロック毎に異なる固有キーを生成することが可能となり、ブロック毎に暗号鍵を変更でき、暗号解析に対する強度を高めることができる。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

請求の範囲

１．　記録媒体に情報を記録する情報記録装置において、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

記録媒体に対する格納データの暗号化処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記情報記録装置に内蔵した暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する構成を有し、

前記暗号化キー生成用データは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報記録装置。

２．　前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第１項記載の情報記録装置。

３．　前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求の範囲第１項記載の情報記録装置。

４．　前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記暗号化キー生成用データの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する構成を有することを特徴とする請求の範囲第１項記載の情報記録装置。

５．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第４項記載の情報記録装置。

６．　前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求の範囲第１項記載の情報記録装置。

７．　前記情報記録装置は、さらに、

第１の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第１の暗号化キーを生成して該第１の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第１の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、

前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、

を選択的に実行する構成を有することを特徴とする請求の範囲第１項記載の情報記録装置。

８．　前記暗号処理手段は、

前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、

前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キ

ーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする請求の範囲第７項記載の情報記録装置。

９．　前記情報記録装置は、さらに、

間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、

前記暗号処理手段は、

前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、

前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする請求の範囲第１項記載の情報記録装置。

１０．　前記暗号処理手段は、

前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする請求の範囲第１項記載の情報記録装置。

１１．　前記情報記録装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求の範囲第１項記載の情報記録装置。

１２．　前記情報記録装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求の範囲第１項記載の情報記録装置。

１３．　記録媒体から情報を再生する情報再生装置において、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

記録媒体に格納された暗号データの復号処理を実行する暗号処理手段を有し、

前記暗号処理手段は、

前記情報記録装置に内蔵した復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する構成を有し、

前記復号キー生成用データは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報再生装置。

１４．　前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第１３項記載の情報再生装置。

１５．　前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求の範囲第１３項記載の情報再生装置。

１６．　前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記復号キー生成用データの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する構成を有することを特徴とする請求の範囲第１３項記載の情報再生装置。

１７．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第１６項記載の情報再生装

置。

１８．　前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成する構成であることを特徴とする請求の範囲第１３項記載の情報再生装置。

１９．　前記情報再生装置は、さらに、

前記記録媒体に格納された第１の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第１の復号キーを生成して該第１の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、

前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、

を選択的に実行する構成を有することを特徴とする請求の範囲第１３項記載の情報再生装置。

２０．　前記暗号処理手段は、

前記再生機器制限なしの復号処理において、

情報記録装置に格納された世代管理されたマスターキーを取得するとともに、

記録媒体から、

記録媒体固有の記録媒体識別子であるディスクＩＤと、

復号対象データに固有のタイトルキーと、

暗号データを記録した情報記録装置の識別子であるデバイスＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、

前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キ

ーを生成し、

前記再生機器制限ありの復号処理において、

情報記録装置に格納された世代管理されたマスターキーと、

情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、

記録媒体から、

記録媒体固有の記録媒体識別子であるディスクＩＤと、

復号対象データに固有のタイトルキーとを取得し、

前記マスターキー、ディスクＩＤ、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復号キーを生成する構成であることを特徴とする請求の範囲第１９項記載の情報再生装置。

２１．　前記情報再生装置は、

前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、

前記暗号処理手段は、

前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成する構成を有し、

前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする請求の範囲第１３項記載の情報再生装置。

２２．　前記暗号処理手段は、

前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする請求の範囲第１３項記載の情報再生装置。

２３．　前記情報再生装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする請求の範囲第１３項記載の情報再生装置。

２４．　前記情報再生装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする請求の範囲第１３項記載の情報再生装置。

２５．　記録媒体に情報を記録する情報記録方法において、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とする情報記録方法。

２６．　前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第２５項記載の情報記録方法。

２７．　前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求の範囲第２５項記載の情報記録方法。

２８．　前記情報記録方法において、

前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、

前記更新ステップは、

前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する更新データ取得ステップと、

を含むことを特徴とする請求の範囲第２５項記載の情報記録方法。

２９．　前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理ステップは、さらに、

前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求の範囲第２５項記載の情報記録方法。

３０．　前記暗号処理ステップは、

第１の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第１の暗号化キーを生成して該第１の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第１の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、

前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、

を選択的に実行することを特徴とする請求の範囲第２５項記載の情報記録方法。

３１．　前記暗号処理ステップは、

前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、

前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、

前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする請求の範囲第３０項記載の情報記録方法。

３２．　前記情報記録方法は、さらに、

間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、

前記暗号処理ステップは、

前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成し、

前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする請求の範囲第２５項記載の情報記録方法。

３３．　前記暗号処理ステップは、

前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行することを特徴とする請求の範囲第２５項記載の情報記録方法。

３４．　前記情報記録方法は、さらに、

データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御することを特徴とする請求の範囲第２５項記載の情報記録方法。

３５．　前記情報記録方法は、さらに、

コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御することを特徴とする請求の範囲第２５項記載の情報記録方法。

３６．　記録媒体から情報を再生する情報再生方法であり、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを

用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、

を有することを特徴とする情報再生方法。

３７．　前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第３６項記載の情報再生方法。

３８．　前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求の範囲第３６項記載の情報再生方法。

３９．　前記情報再生方法において、

前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、

前記更新ステップは、

前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する更新データ取得ステップと、

を含むことを特徴とする請求の範囲第３６項記載の情報再生方法。

４０．　前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記復号処理ステップは、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成することを特徴とする請求の範囲第３６項記載の情報再生方法。

４１．　前記情報再生方法は、さらに、

前記記録媒体に格納された第１の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第１の復号キーを生成して該第１の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、

前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、

を選択的に実行することを特徴とする請求の範囲第３６項記載の情報再生方法。

４２．　前記復号処理ステップは、

前記再生機器制限なしの復号処理において、

情報記録装置に格納された世代管理されたマスターキーを取得するとともに、

記録媒体から、

記録媒体固有の記録媒体識別子であるディスクＩＤと、

復号対象データに固有のタイトルキーと、

暗号データを記録した情報記録装置の識別子であるデバイスＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、

前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キーを生成し、

前記再生機器制限ありの復号処理において、

情報記録装置に格納された世代管理されたマスターキーと、

情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、

記録媒体から、

記録媒体固有の記録媒体識別子であるディスクＩＤと、

復号対象データに固有のタイトルキーとを取得し、

前記マスターキー、ディスクＩＤ、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復

号キーを生成することを特徴とする請求の範囲第４１項記載の情報再生方法。

４３．　前記情報再生方法において、

情報再生装置は、復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、

前記復号処理ステップは、

前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成し、

前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする請求の範囲第３６項記載の情報再生方法。

４４．　前記復号処理ステップは、

前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行することを特徴とする請求の範囲第３６項記載の情報再生方法。

４５．　前記情報再生方法は、さらに、

データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする請求の範囲第３６項記載の情報再生方法。

４６．　前記情報再生方法は、さらに、

コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする請求の範囲第３６項記載の情報再生方法。

４７．　情報を記録可能な情報記録媒体であって、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーによ

り暗号化したキー更新ブロック（ＫＲＢ）を格納したことを特徴とする情報記録媒体。

４８．　前記情報記録媒体は、さらに、

情報記録装置において記録媒体に格納するデータの暗号化処理に用いる暗号化キーを生成するための暗号化キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする請求の範囲第４７項記載の情報記録媒体。

４９．　前記情報記録媒体は、さらに、

情報再生装置において記録媒体に格納された暗号データの復号処理に用いる復号キーを生成するための復号キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする請求の範囲第４７項記載の情報記録媒体。

５０．　前記情報記録媒体は、さらに、暗号化キー生成用データ又は復号キー生成用データに関する世代情報を格納した構成であることを特徴とする請求の範囲第４７項記載の情報記録媒体。

５１．　情報記録媒体を製造する記録媒体製造装置であり、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を格納するメモリと、

前記メモリに格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込み制御を実行する制御部と、

を有することを特徴とする記録媒体製造装置。

５２．　前記メモリには、さらに、

記録媒体識別子と、暗号化された暗号化キー生成用データ又は暗号化された復号キー生成用データの少なくともいずれかを格納し、

前記制御部は、前記記録媒体識別子、暗号化された暗号化キー生成用データ、又は暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする請求の範囲第５１項記載の記録媒体製造装置。

５３．　前記メモリには、さらに、

暗号化キー生成用データ又は復号キー生成用データに関する世代情報を格納し、

前記制御部は、前記世代情報の前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする請求の範囲第５１項記載の記録媒体製造装置。

５４．　記録媒体を製造する記録媒体製造方法であり、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）をメモリに格納するステップと、

前記メモリに格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込みを実行するステップと、

を有することを特徴とする記録媒体製造方法。

５５．　前記記録媒体製造方法において、

前記メモリに、さらに、

記録媒体識別子、暗号化された暗号化キー生成用データ、又は暗号化された復号キー生成用データの少なくともいずれかを格納し、

前記記録媒体識別子、暗号化された暗号化キー生成用データ、又は暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込みを実行することを特徴とする請求の範囲第５４項記載の記録媒体製造方法。

５６．　前記記録媒体製造方法において、

前記メモリに、さらに、

暗号化キー生成用データ又は復号キー生成用データに関する世代情報を格納し、

前記制御部は、前記世代情報の前記記録媒体に対する書き込みを実行することを特徴とする請求の範囲第５４項記載の記録媒体製造方法。

５７．　記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを

用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とするプログラム提供媒体。

５８．　記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、

を有することを特徴とするプログラム提供媒体。

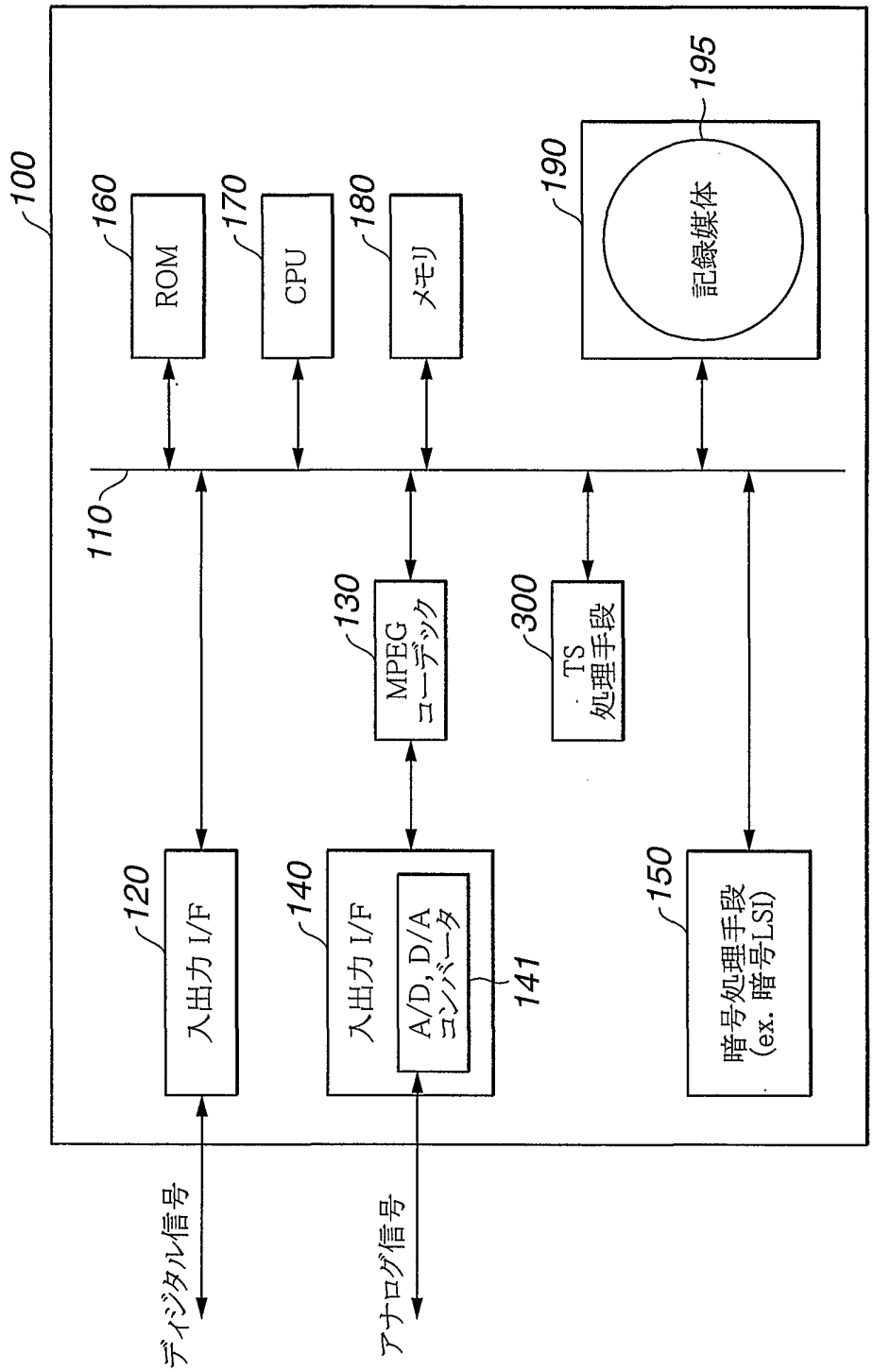

100
160
ROM
170
CPU
180
メモリ
190
記録媒体
195
110
130
MPEG
コーデック
300
TS
処理手段
120
入出力 I/F
140
入出力 I/F
A/D, D/A
コンバータ
141
150
暗号処理手段
(ex. 暗号LSI)
ディジタル信号
アナログ信号

FIG.1

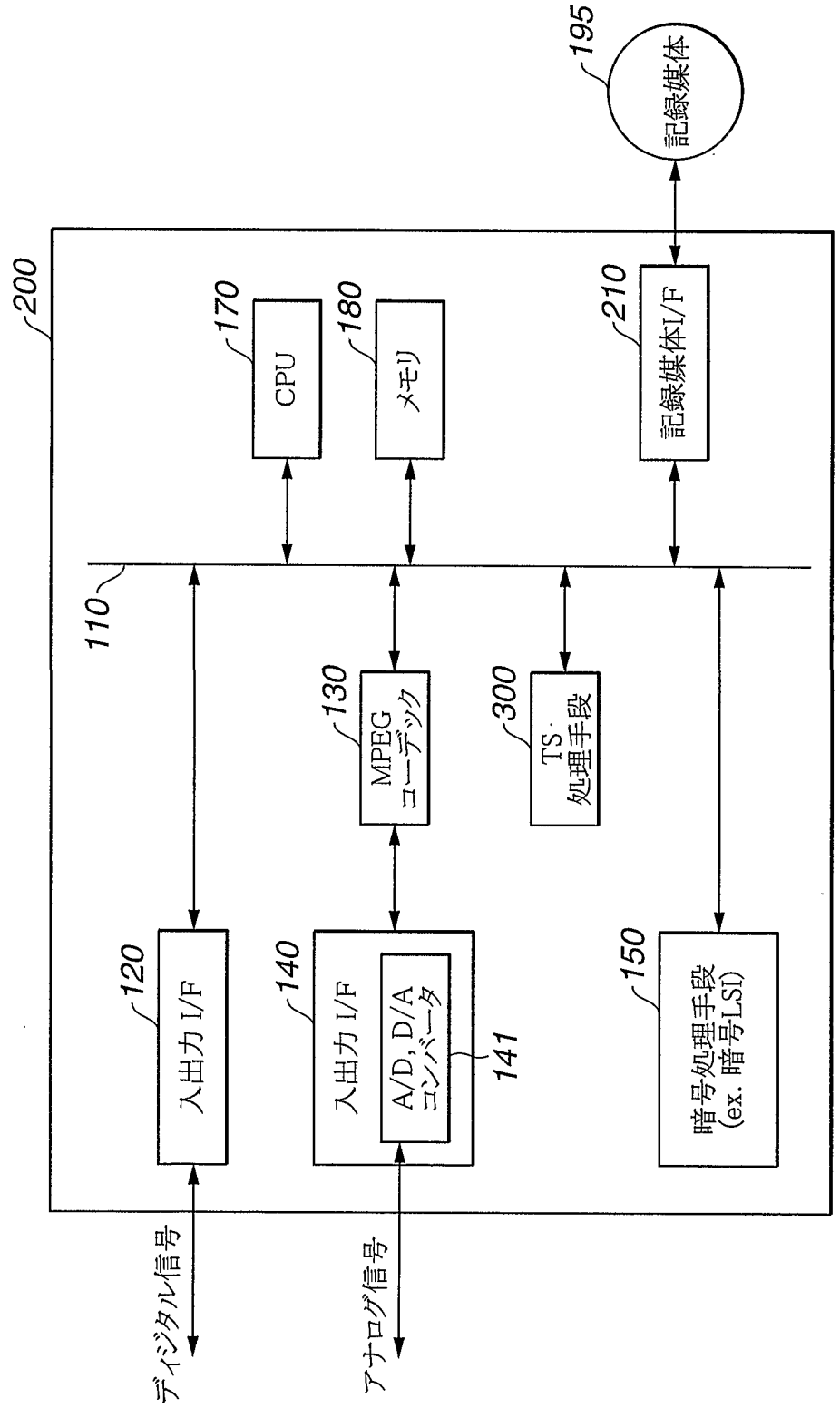

195
記録媒体
200
170
CPU
180
メモリ
210
記録媒体I/F
110
130
MPEG
コーデック
300
TS
処理手段
120
入出力 I/F
140
入出力 I/F
A/D, D/A
コンバータ
141
150
暗号処理手段
(ex. 暗号LSI)
ディジタル信号
アナログ信号

FIG.2

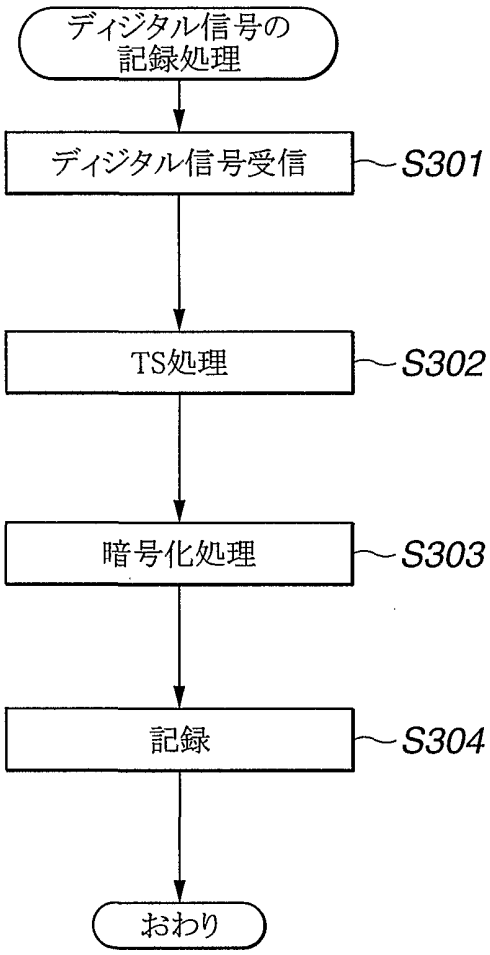

ディジタル信号の
記録処理
ディジタル信号受信
S301
TS処理
S302
暗号化処理
S303
記録
S304
おわり

FIG.3A

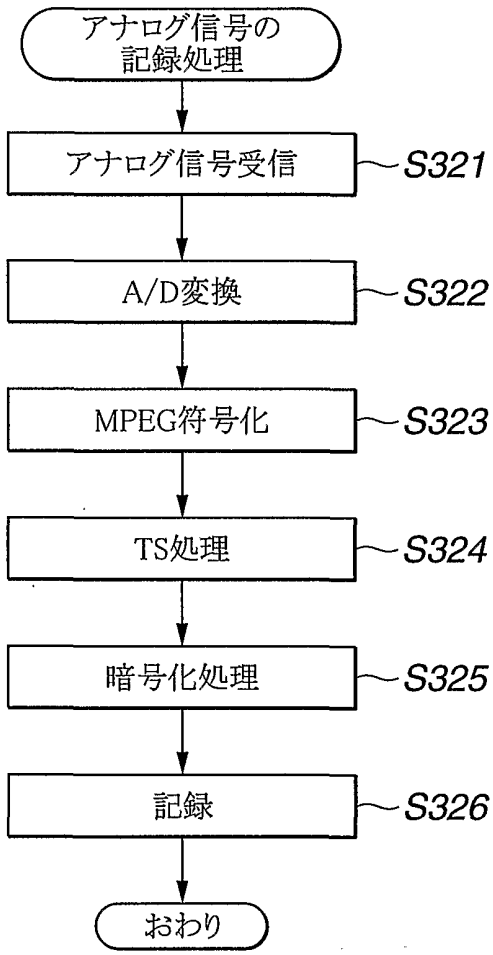

アナログ信号の
記録処理
アナログ信号受信
S321
A/D変換
S322
MPEG符号化
S323
TS処理
S324
暗号化処理
S325
記録
S326
おわり

FIG.3B

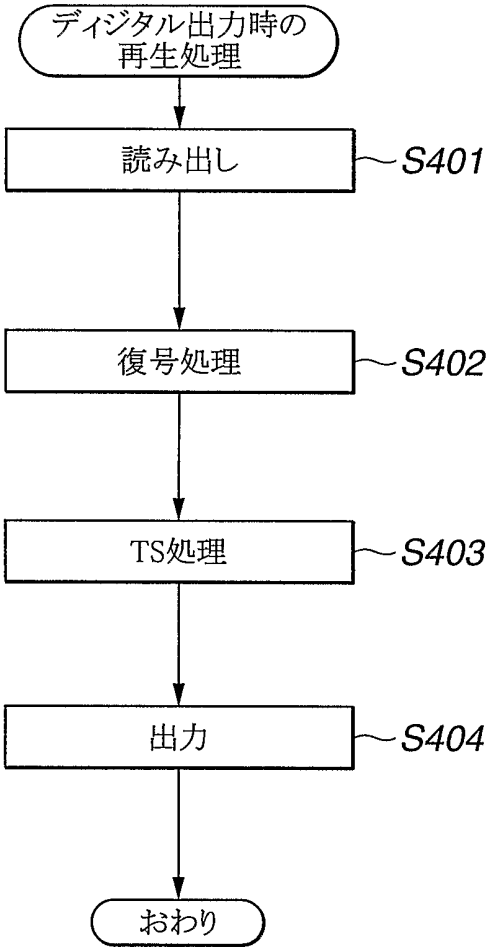

ディジタル出力時の
再生処理
読み出し
S401
復号処理
S402
TS処理
S403
出力
S404
おわり

FIG.4A

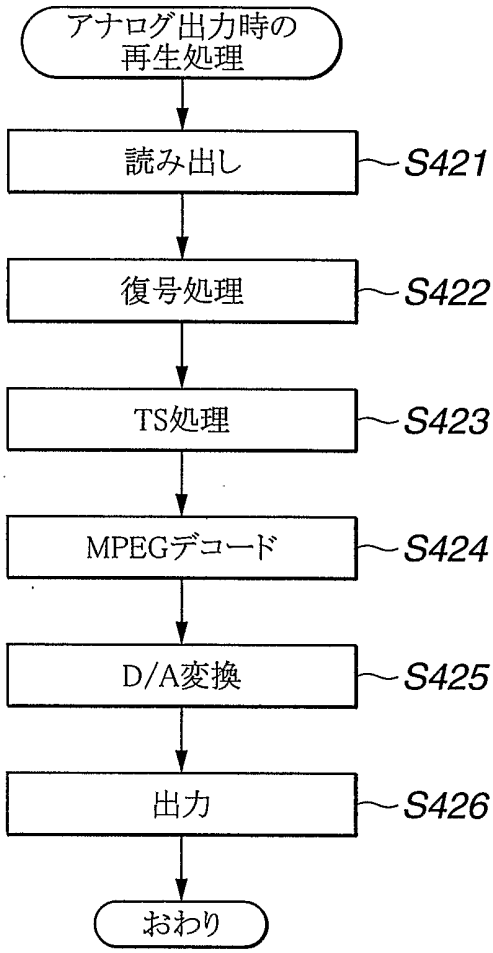

アナログ出力時の
再生処理
読み出し
S421
復号処理
S422
TS処理
S423
MPEGデコード
S424
D/A変換
S425
出力
S426
おわり

FIG.4B

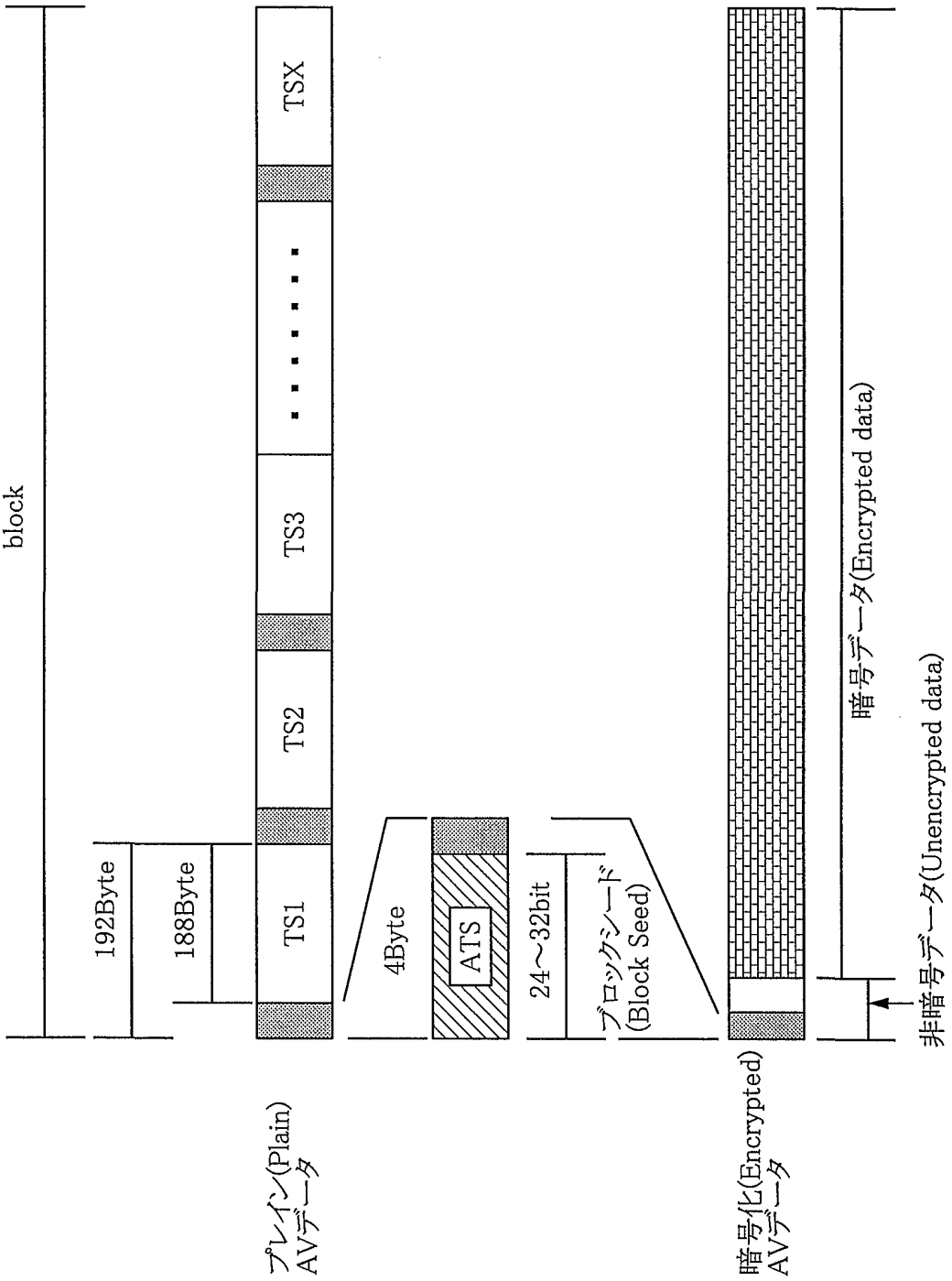

block
192Byte
188Byte
TS1
TS2
TS3
TSX
4Byte
ATS
24～32bit
ブロックシード
(Block Seed)
プレイン(Plain)
AVデータ
暗号化(Encrypted)
AVデータ
暗号データ(Encrypted data)
非暗号データ(Unencrypted data)

FIG.5

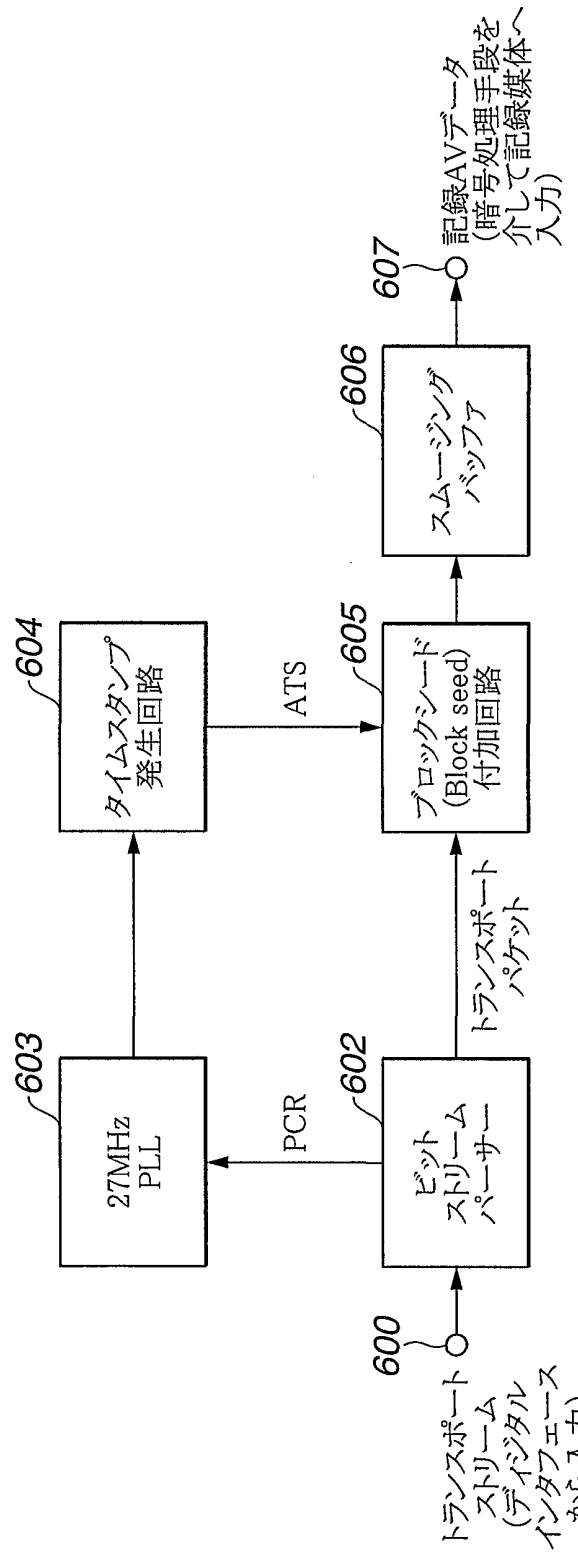

600
トランスポートストリーム(ディジタルインタフェースから入力)
602
ビットストリームパーサー
603
27MHz PLL
604
タイムスタンプ発生回路
605
ブロックシード(Block seed)付加回路
606
スムージングバッファ
607
記録AVデータ(暗号処理手段を介して記録媒体へ入力)
PCR
ATS
トランスポートパケット

FIG.6

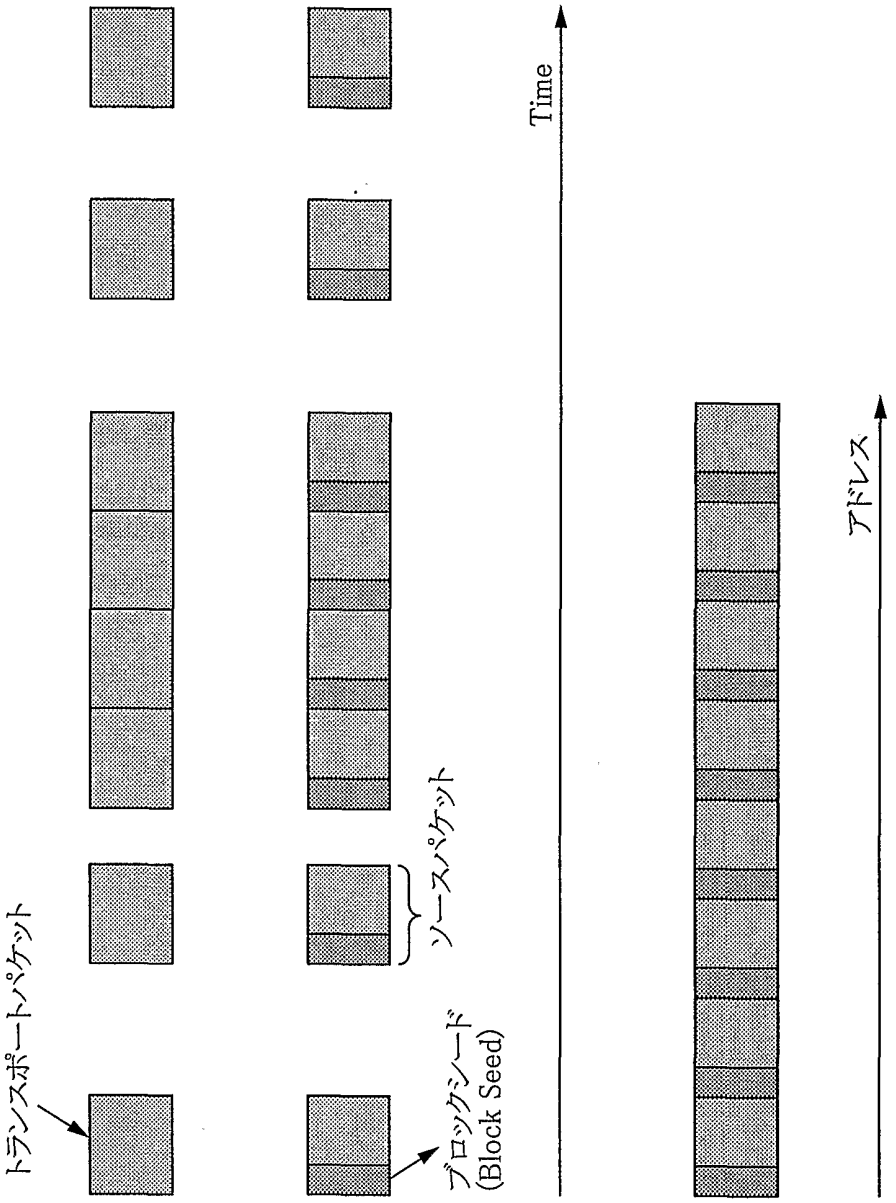


FIG.7A
入力トランスポート
ストリーム

FIG.7B
Block seed付加器
の出力

FIG.7C
記録媒体上のAV
データ

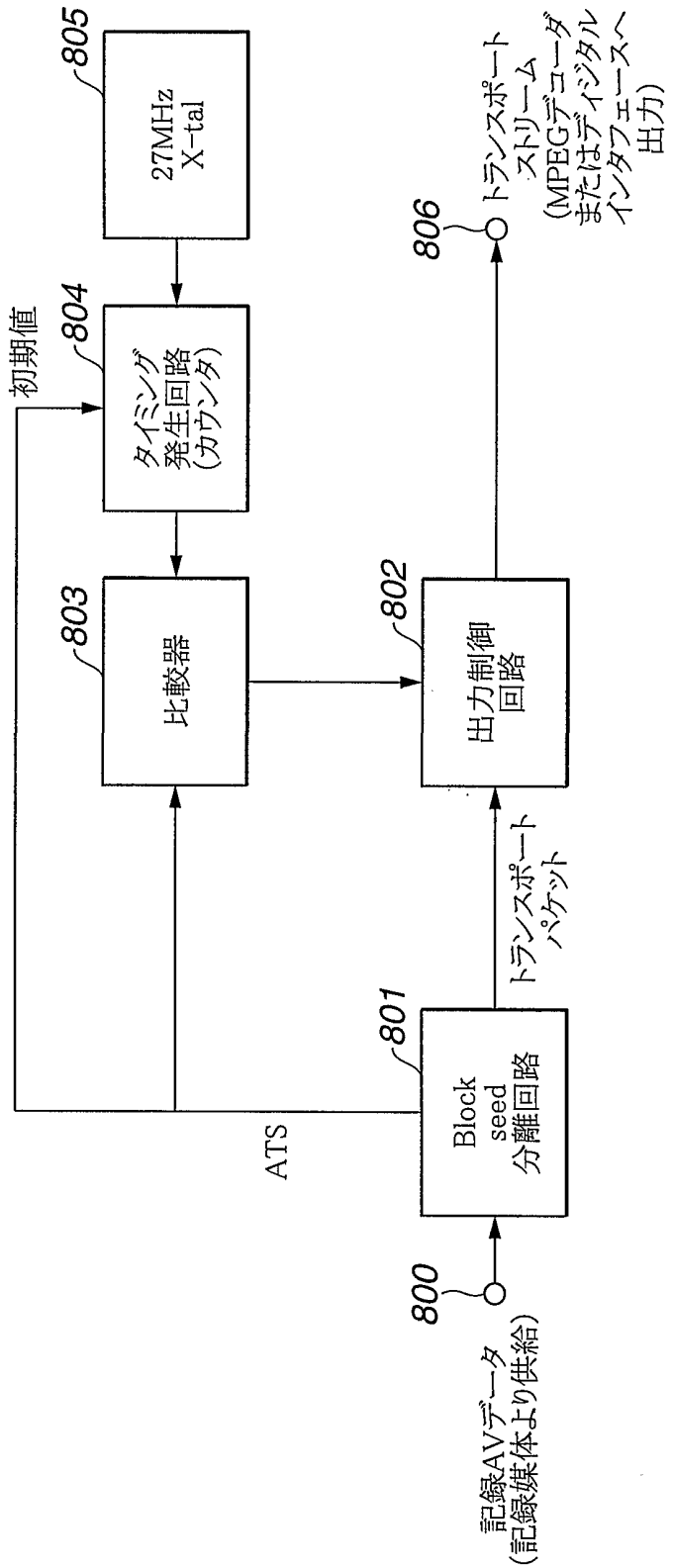

805
27MHz
X-tal
804
タイミング
発生回路
(カウンタ)
初期値
803
比較器
802
出力制御
回路
806
トランスポート
ストリーム
(MPEGデコーダ
またはディジタル
インタフェースへ
出力)
ATS
801
Block
seed
分離回路
トランスポート
パケット
800
記録AVデータ
(記録媒体より供給)

FIG.8

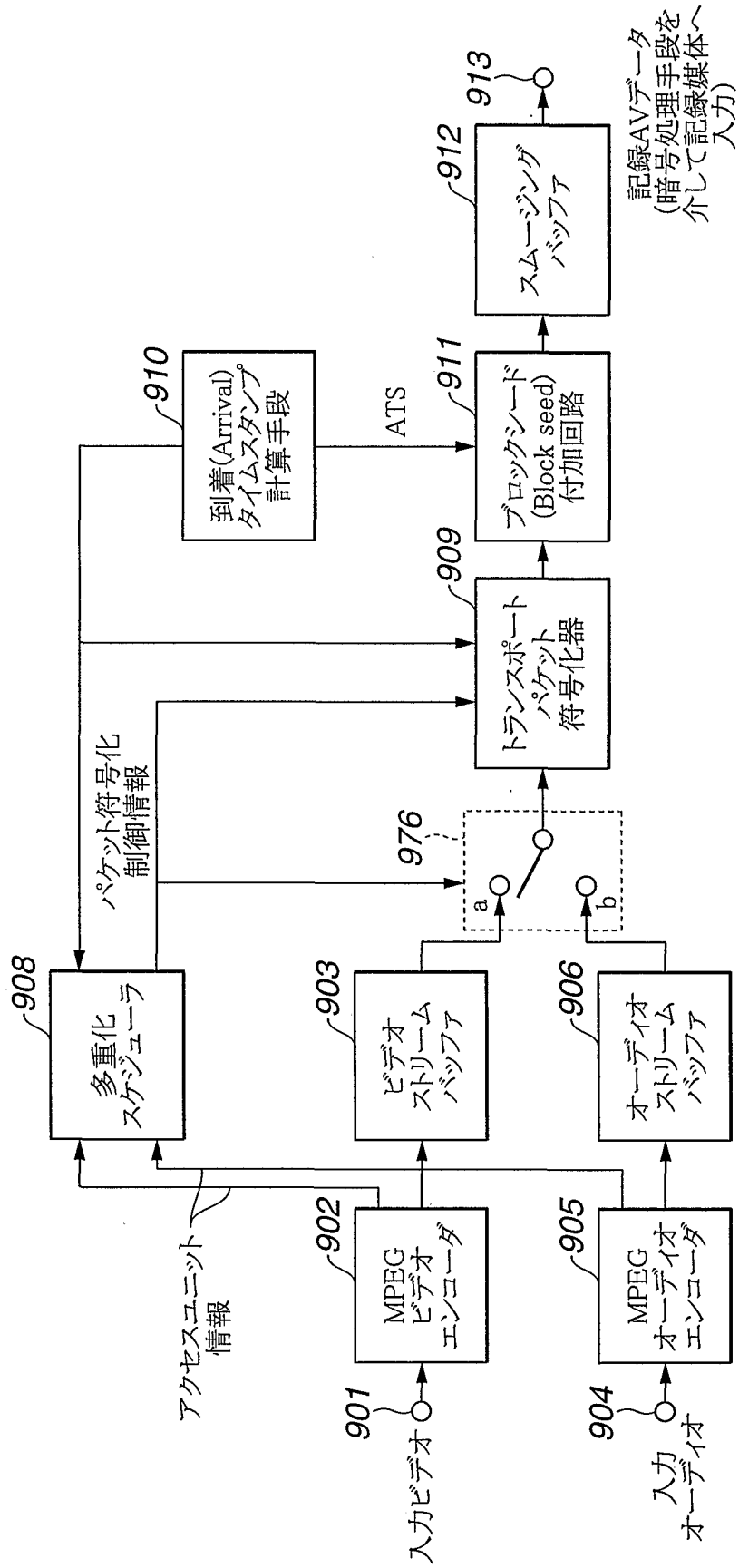

入力ビデオ
901
MPEG ビデオ エンコーダ
902
ビデオ ストリーム バッファ
903
入力 オーディオ
904
MPEG オーディオ エンコーダ
905
オーディオ ストリーム バッファ
906
アクセスユニット 情報
多重化 スケジューラ
908
パケット符号化 制御情報
トランスポート パケット 符号化器
909
976
a
b
到着(Arrival) タイムスタンプ 計算手段
910
ATS
ブロックシード (Block seed) 付加回路
911
スムージング バッファ
912
913
記録AVデータ (暗号処理手段を 介して記録媒体へ 入力)

FIG.9

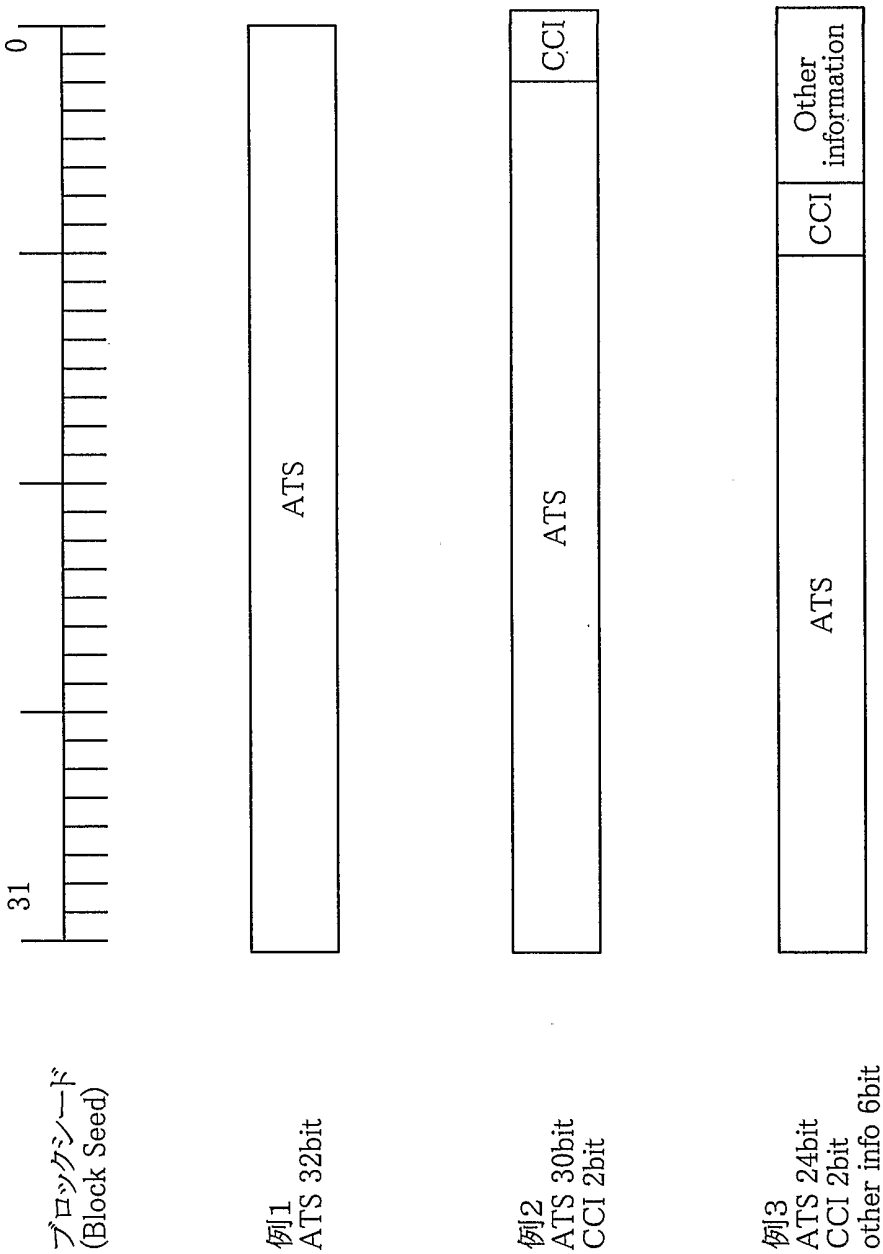

31
0
ブロックシード
(Block Seed)
例1
ATS 32bit
ATS
例2
ATS 30bit
CCI 2bit
ATS
CCI
例3
ATS 24bit
CCI 2bit
other info 6bit
ATS
CCI
Other information

FIG.10

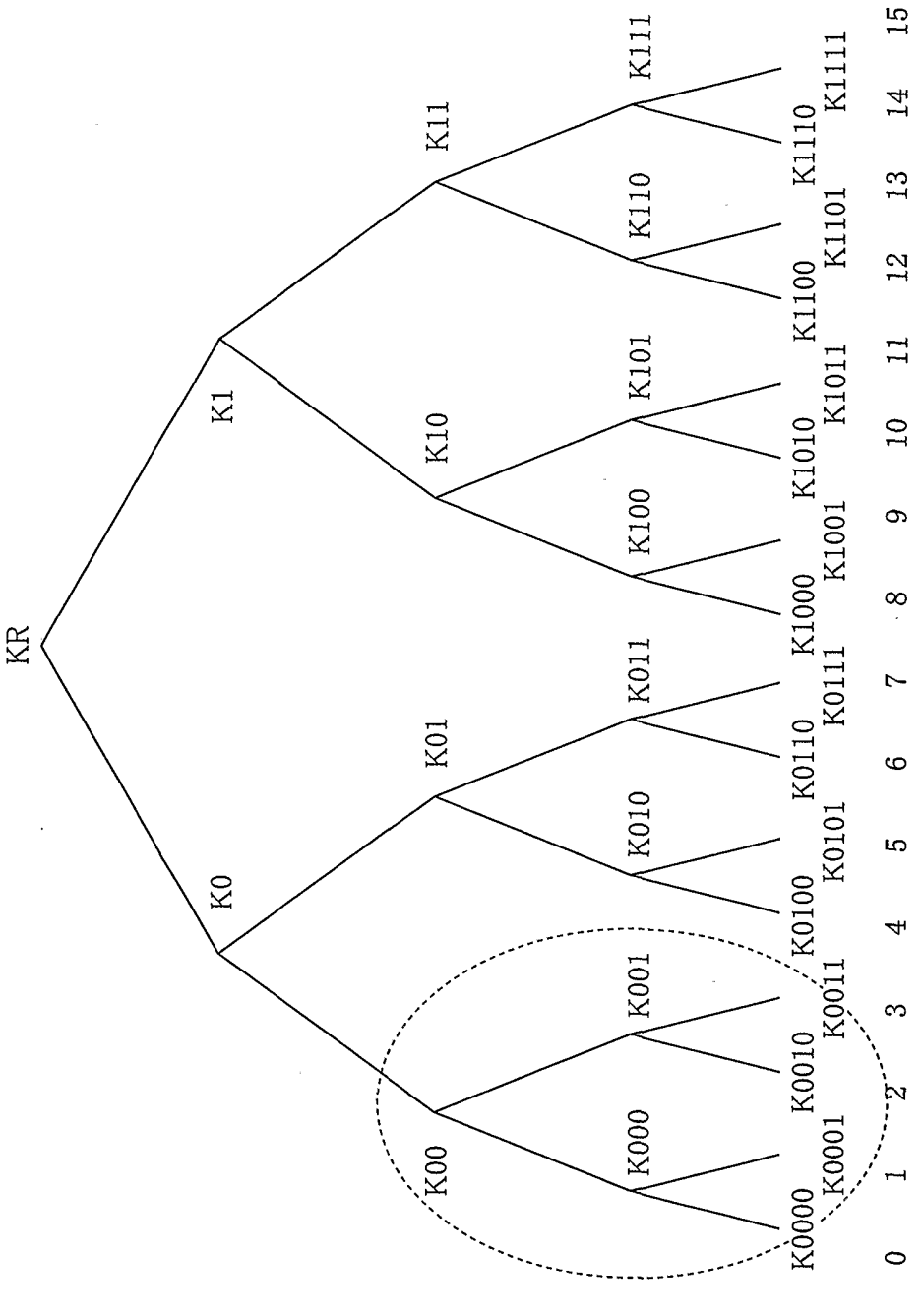

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

FIG.11

世代(Generation) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.12A

世代(Generation) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.12B

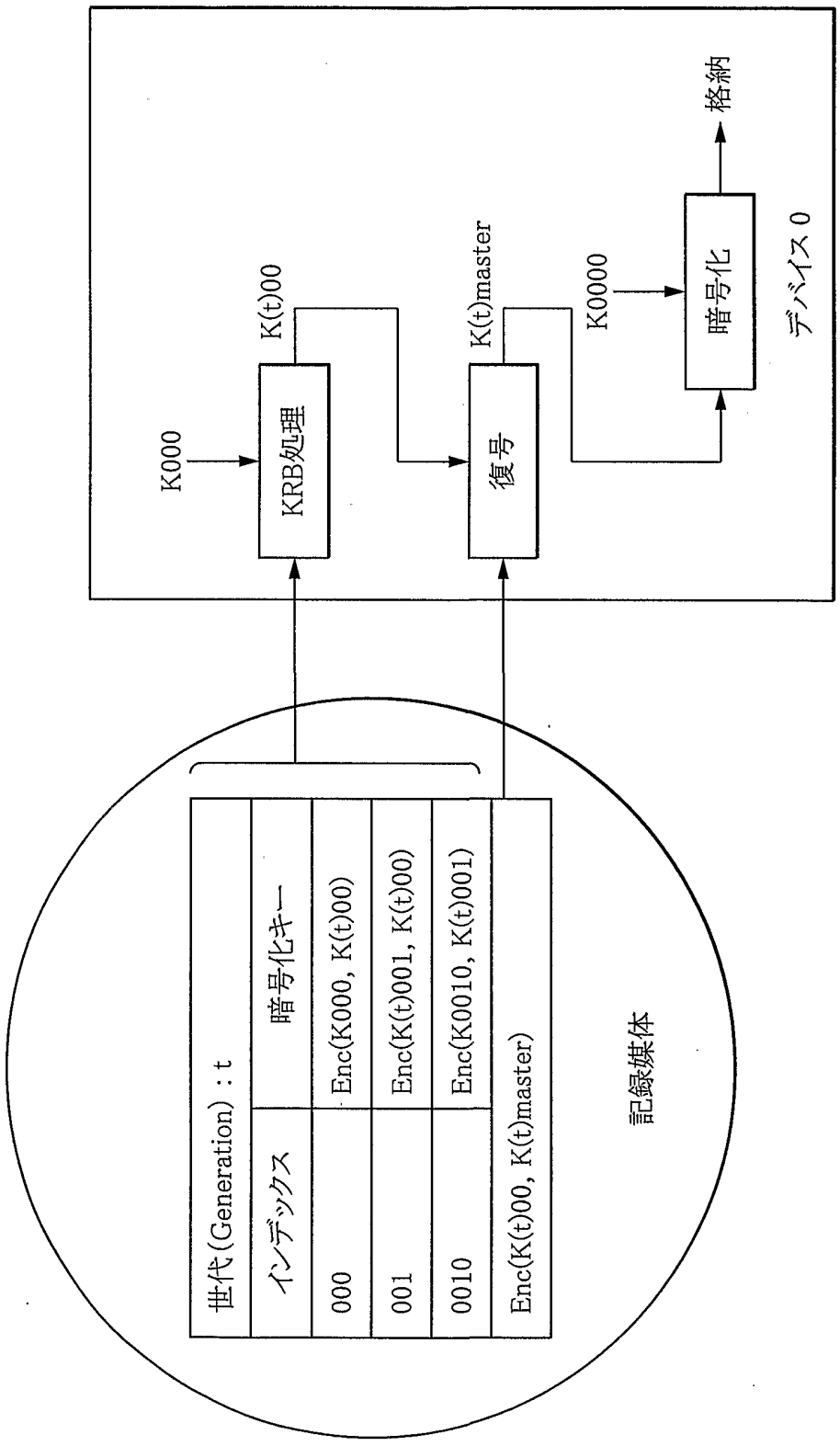

K000
KRB処理
K(t)00
復号
K(t)master
K0000
暗号化
格納
デバイス 0
記録媒体
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)

FIG.13

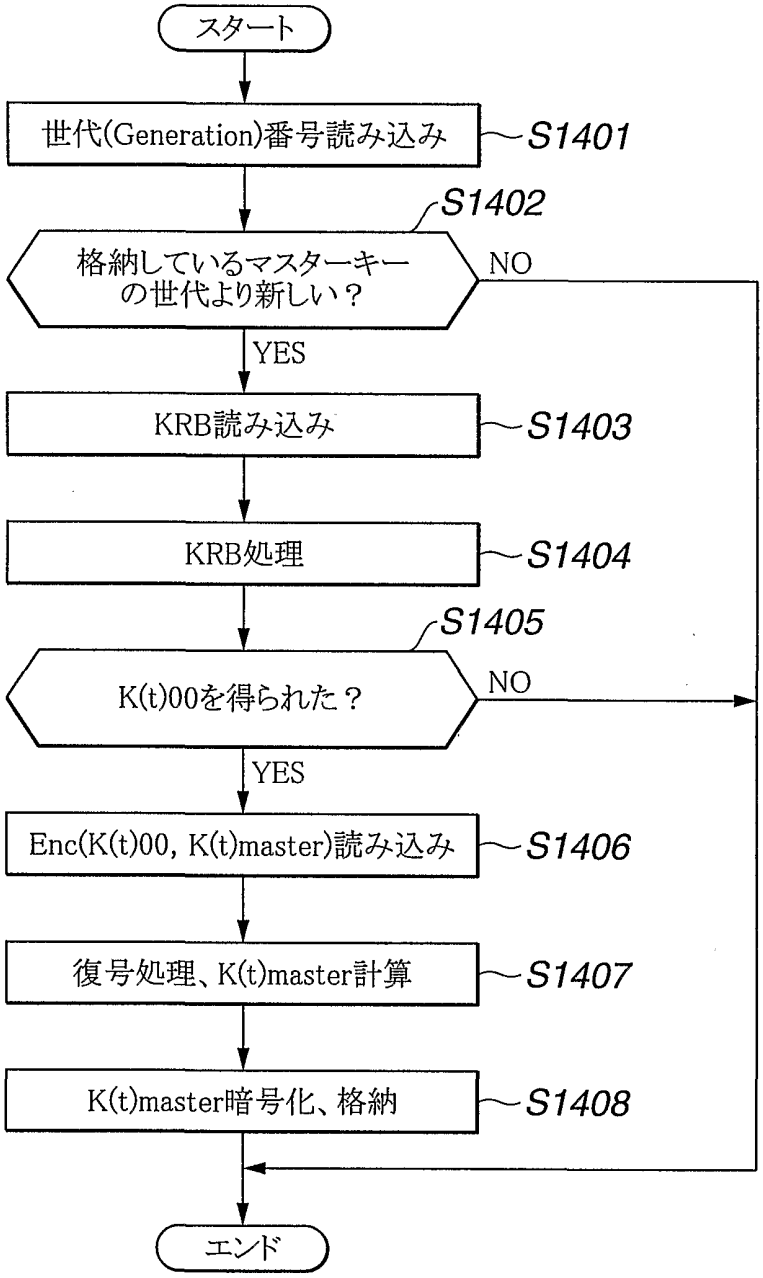

スタート
世代(Generation)番号読み込み
S1401
S1402
格納しているマスターキーの世代より新しい？
NO
YES
KRB読み込み
S1403
KRB処理
S1404
S1405
K(t)00を得られた？
NO
YES
Enc(K(t)00, K(t)master)読み込み
S1406
復号処理、K(t)master計算
S1407
K(t)master暗号化、格納
S1408
エンド

FIG.14

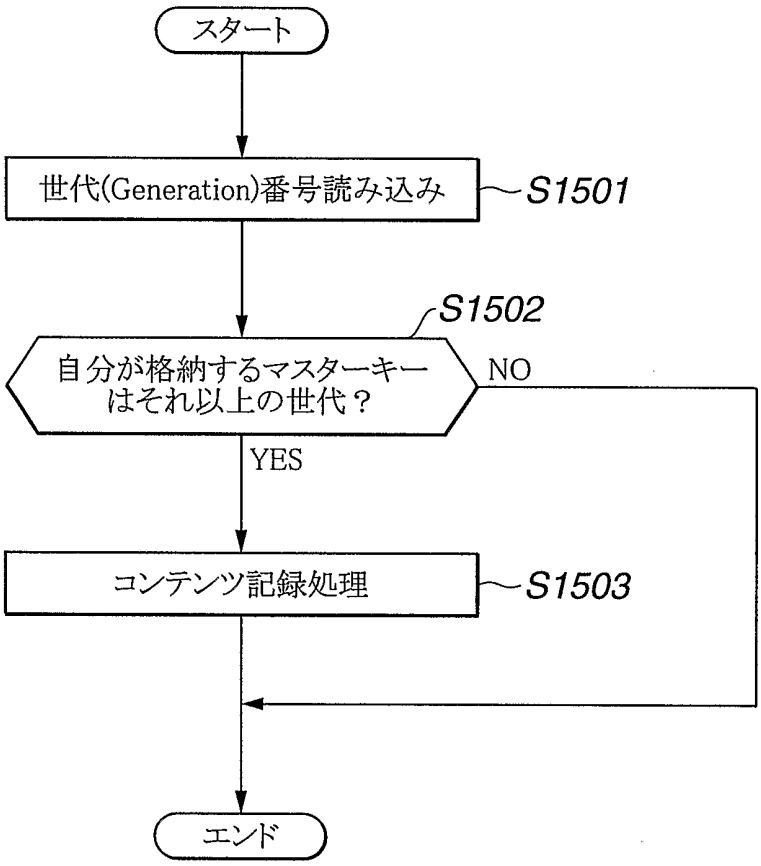

スタート
世代(Generation)番号読み込み
S1501
S1502
自分が格納するマスターキー
はそれ以上の世代？
NO
YES
コンテンツ記録処理
S1503
エンド

FIG.15

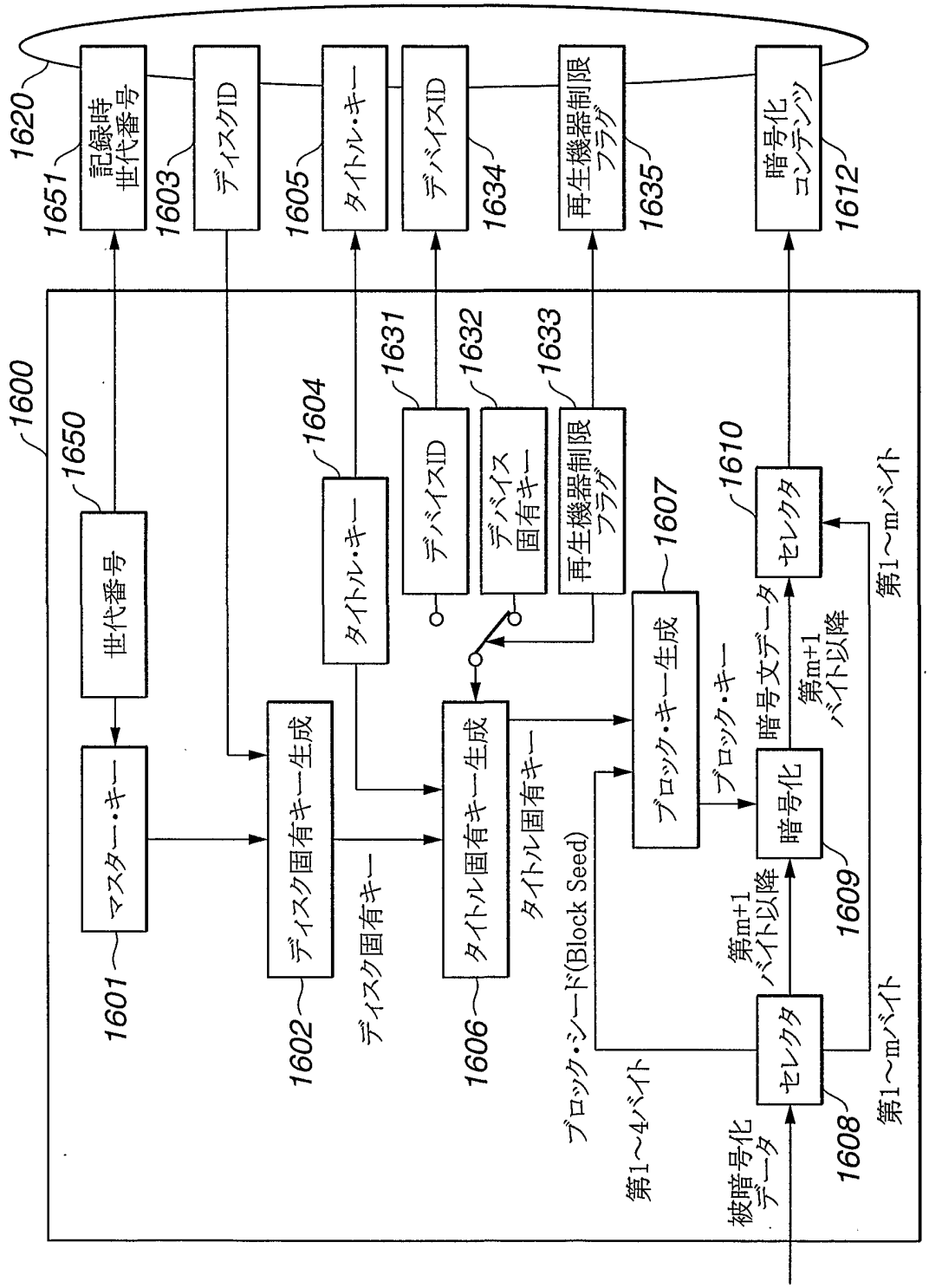

1600
1620
1651
記録時世代番号
1603
ディスクID
1605
タイトル・キー
1634
デバイスID
1635
再生機器制限フラグ
1612
暗号化コンテンツ
1650
世代番号
1601
マスター・キー
1602
ディスク固有キー生成
ディスク固有キー
1604
タイトル・キー
1631
デバイスID
1632
デバイス固有キー
1633
再生機器制限フラグ
1606
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
第1～4バイト
1607
ブロック・キー生成
1610
セレクタ
ブロック・キー
暗号文データ
第m+1バイト以降
第1～mバイト
第m+1バイト以降
暗号化
1609
セレクタ
1608
被暗号化データ
第1～mバイト

FIG.16

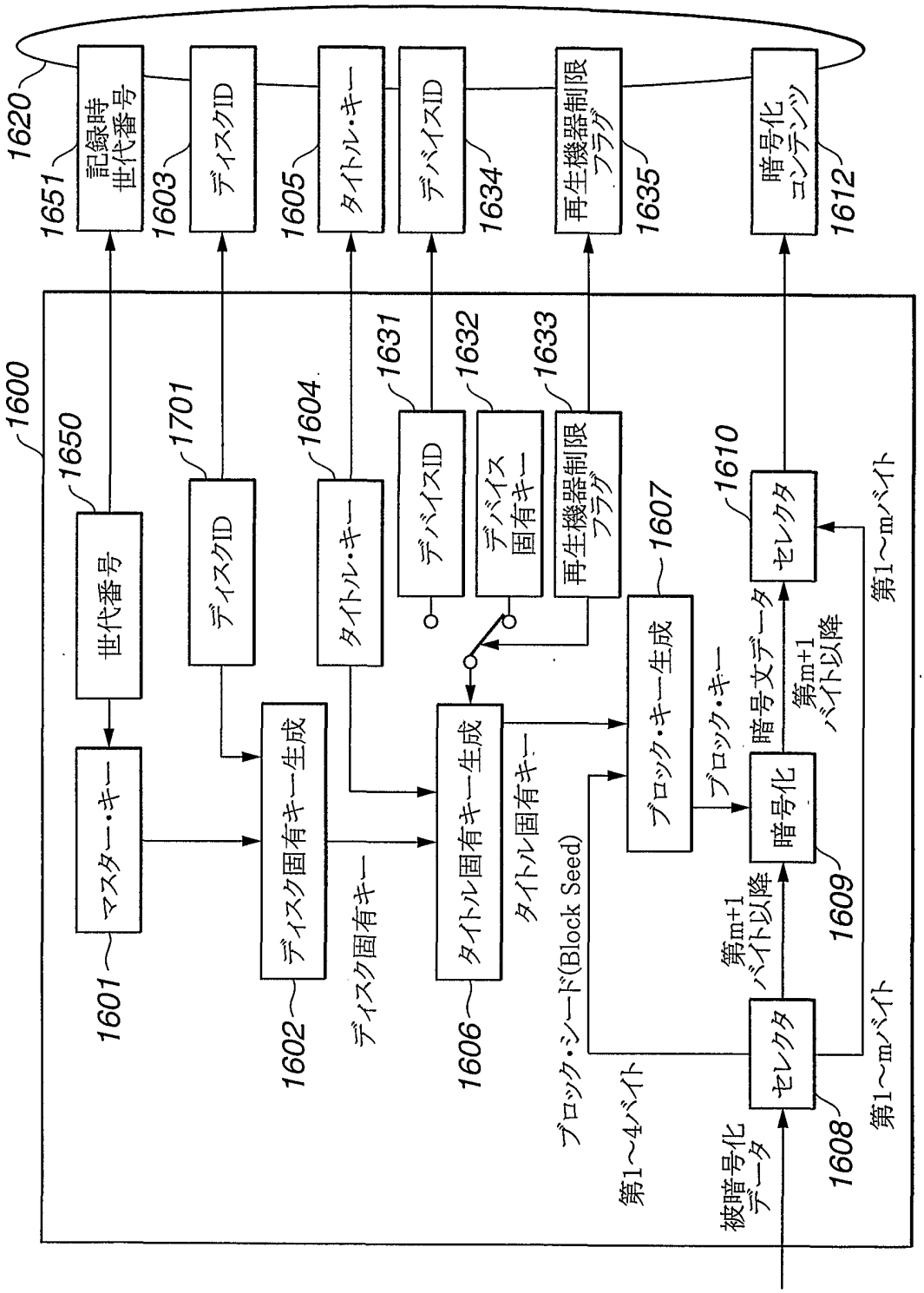

1600
1620
1651
記録時世代番号
1603
ディスクID
1605
タイトル・キー
1634
デバイスID
1635
再生機器制限フラグ
1612
暗号化コンテンツ
1650
世代番号
1701
ディスクID
1604
タイトル・キー
1631
デバイスID
1632
デバイス固有キー
1633
再生機器制限フラグ
1610
セレクタ
1601
マスター・キー
1602
ディスク固有キー生成
ディスク固有キー
1606
タイトル固有キー生成
タイトル固有キー
1607
ブロック・キー生成
ブロック・キー
暗号文データ
第m+1バイト以降
ブロック・シード(Block Seed)
第1～4バイト
第m+1バイト以降
暗号化
1609
第1～mバイト
セレクタ
1608
第1～mバイト
被暗号化データ

FIG.17

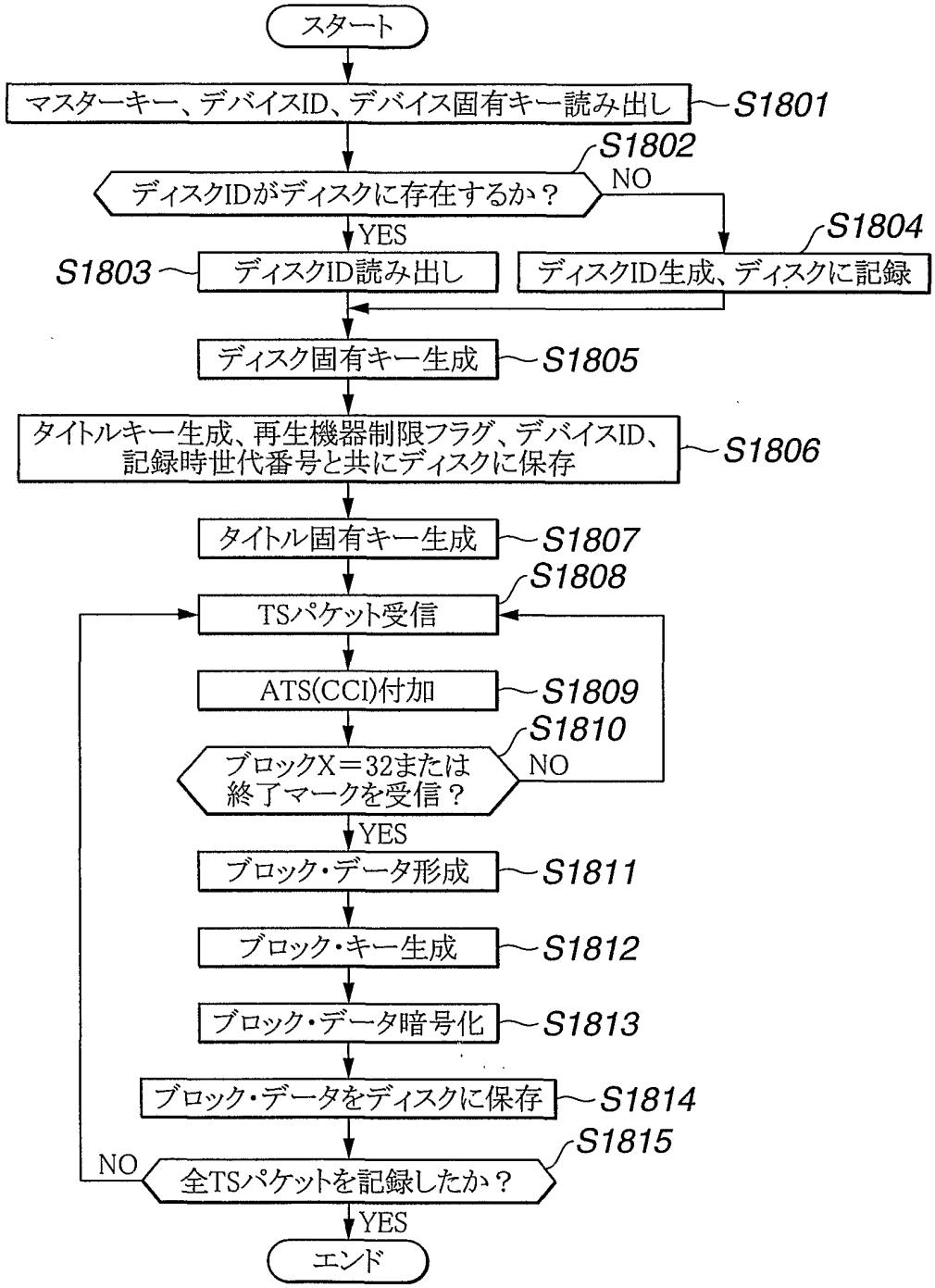

スタート
マスターキー、デバイスID、デバイス固有キー読み出し
S1801
S1802
ディスクIDがディスクに存在するか？
NO
YES
S1804
S1803
ディスクID読み出し
ディスクID生成、ディスクに記録
ディスク固有キー生成
S1805
タイトルキー生成、再生機器制限フラグ、デバイスID、
記録時世代番号と共にディスクに保存
S1806
タイトル固有キー生成
S1807
S1808
TSパケット受信
ATS(CCI)付加
S1809
S1810
ブロックX＝32または
終了マークを受信？
NO
YES
ブロック・データ形成
S1811
ブロック・キー生成
S1812
ブロック・データ暗号化
S1813
ブロック・データをディスクに保存
S1814
S1815
NO
全TSパケットを記録したか？
YES
エンド

FIG.18

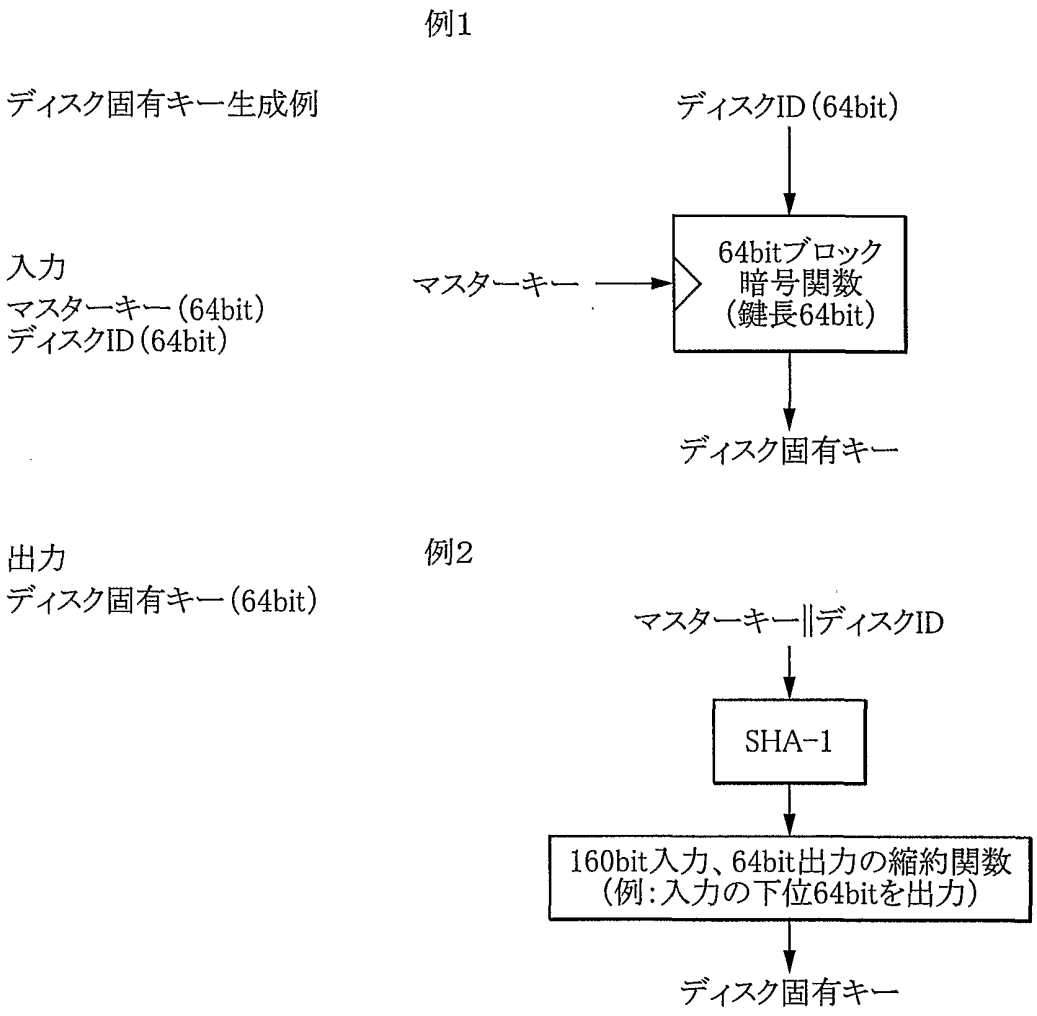

例1
ディスク固有キー生成例
ディスクID(64bit)
入力
マスターキー(64bit)
ディスクID(64bit)
マスターキー
64bitブロック
暗号関数
(鍵長64bit)
ディスク固有キー
出力
ディスク固有キー(64bit)
例2
マスターキー||ディスクID
SHA-1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
ディスク固有キー

FIG.19

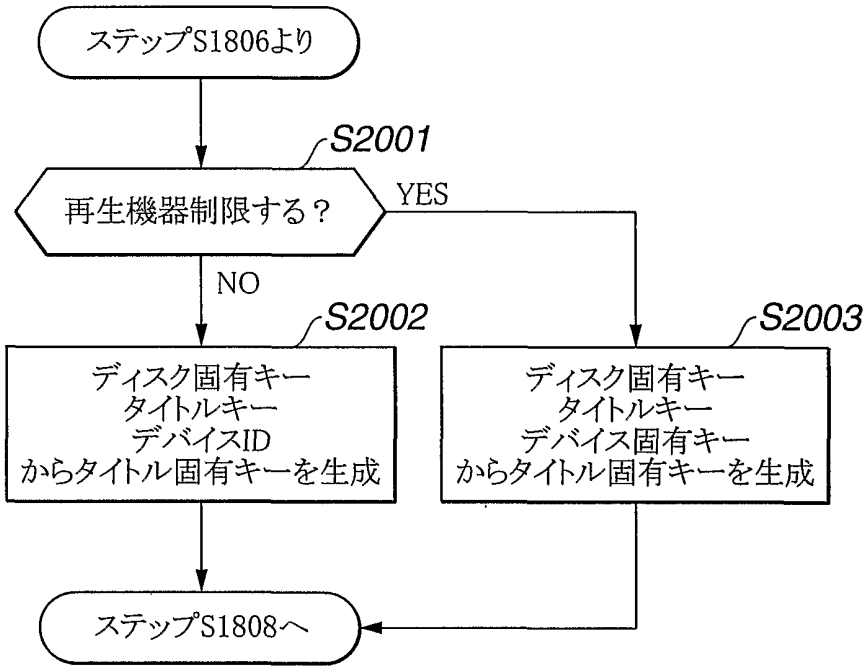

ステップS1806より
S2001
再生機器制限する？
YES
NO
S2002
ディスク固有キー
タイトルキー
デバイスID
からタイトル固有キーを生成
S2003
ディスク固有キー
タイトルキー
デバイス固有キー
からタイトル固有キーを生成
ステップS1808へ

FIG.20

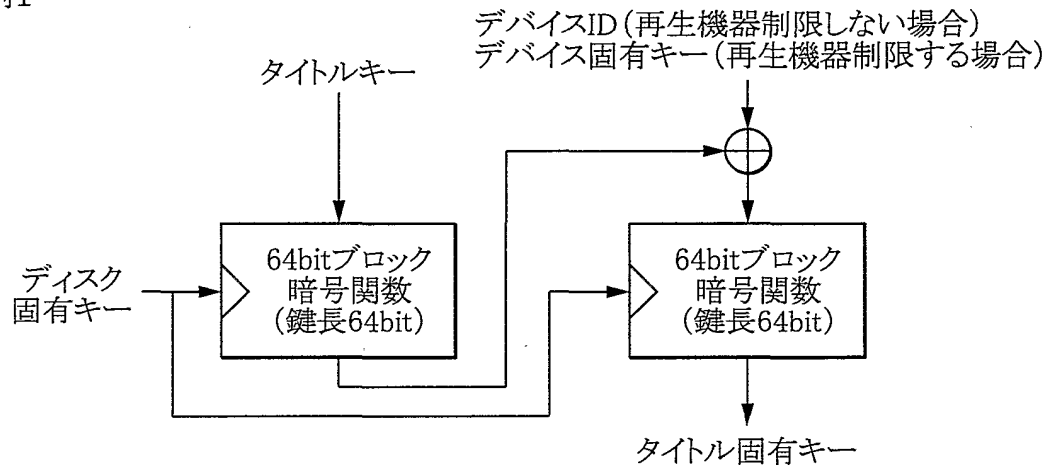
タイトル固有キー生成例

入力
ディスク固有キー(64bit)
タイトルキー(64bit)

ディスクID(64bit)または
デバイス固有キー(64bit)

出力
タイトル固有キー(64bit)

例1



例2

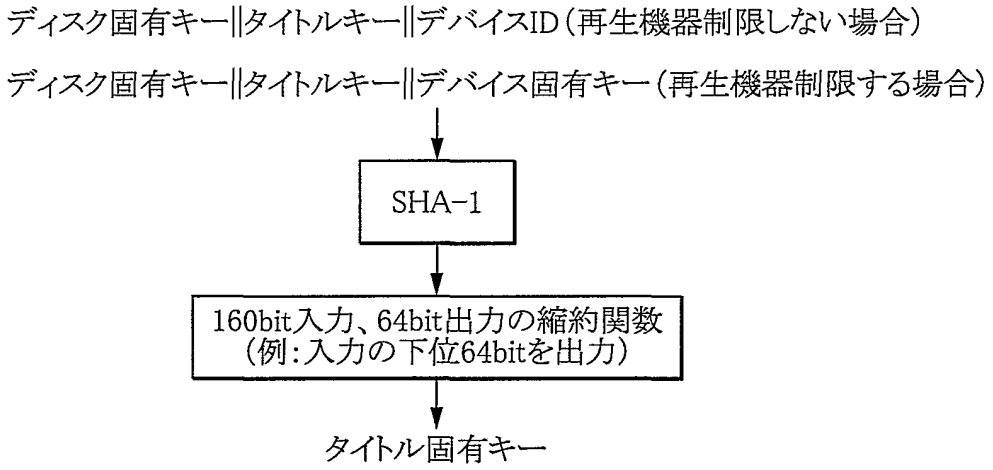


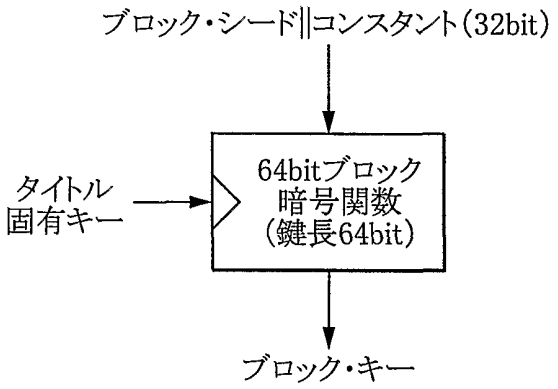
FIG.21

ブロック・キー生成例

入力
ブロック・シード(32bit)
タイトル固有キー(64bit)

出力
ブロック・キー(64bit)

例1



例2

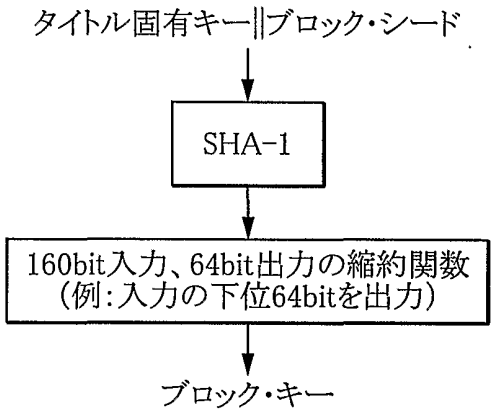


FIG.22

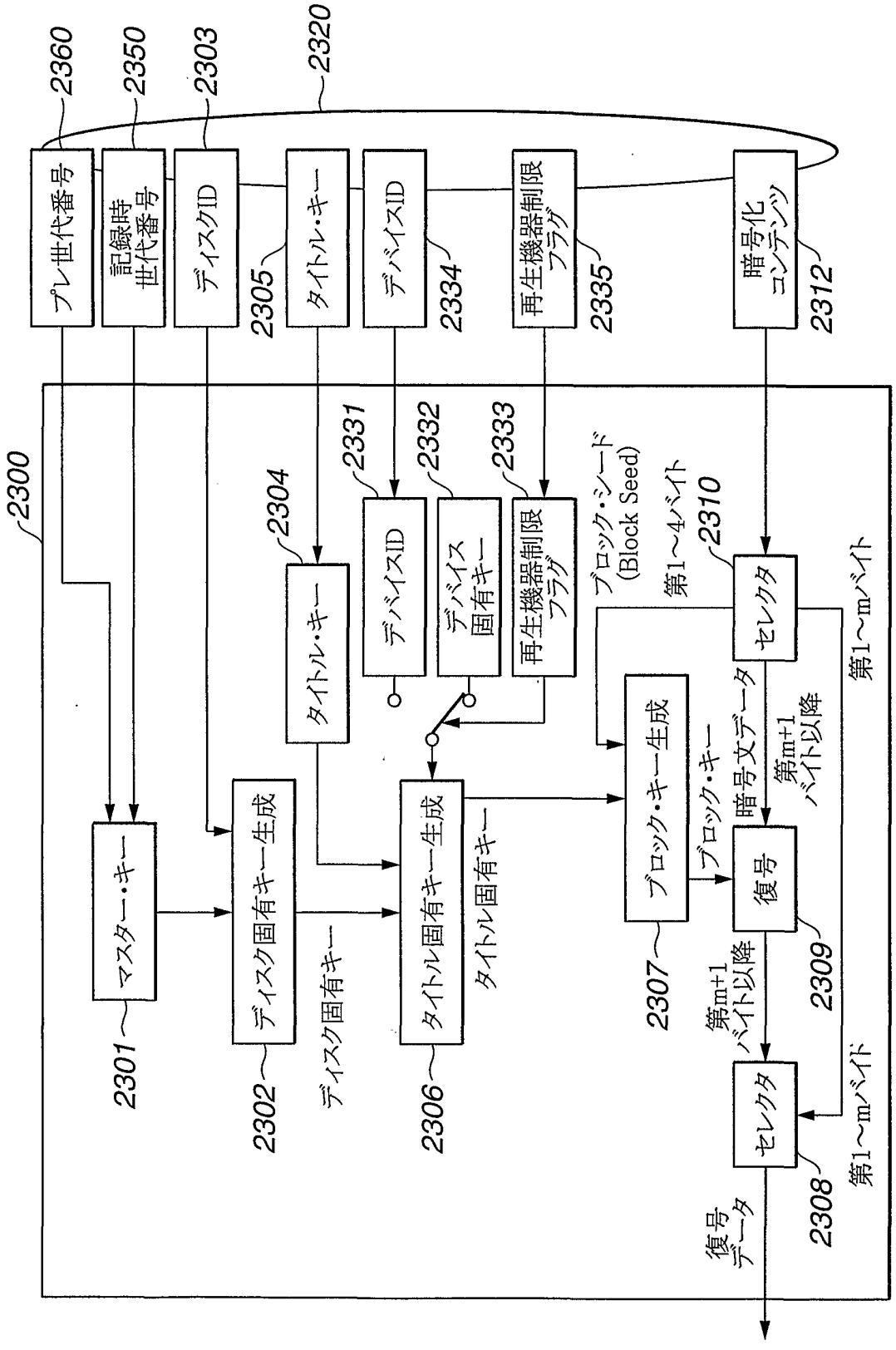

2360
2350
2303
2320
プレ世代番号
記録時世代番号
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
2305
2334
2335
2312
2300
2331
2332
2333
2304
デバイスID
デバイス固有キー
再生機器制限フラグ
タイトル・キー
ブロック・シード (Block Seed)
第1～4バイト
2310
セレクタ
マスター・キー
ディスク固有キー生成
タイトル固有キー生成
ブロック・キー生成
2301
2302
2306
2307
ディスク固有キー
タイトル固有キー
ブロック・キー
暗号文データ
復号
第m+1バイト以降
2309
第1～mバイト
第m+1バイト以降
セレクタ
2308
第1～mバイト
復号データ

FIG.23

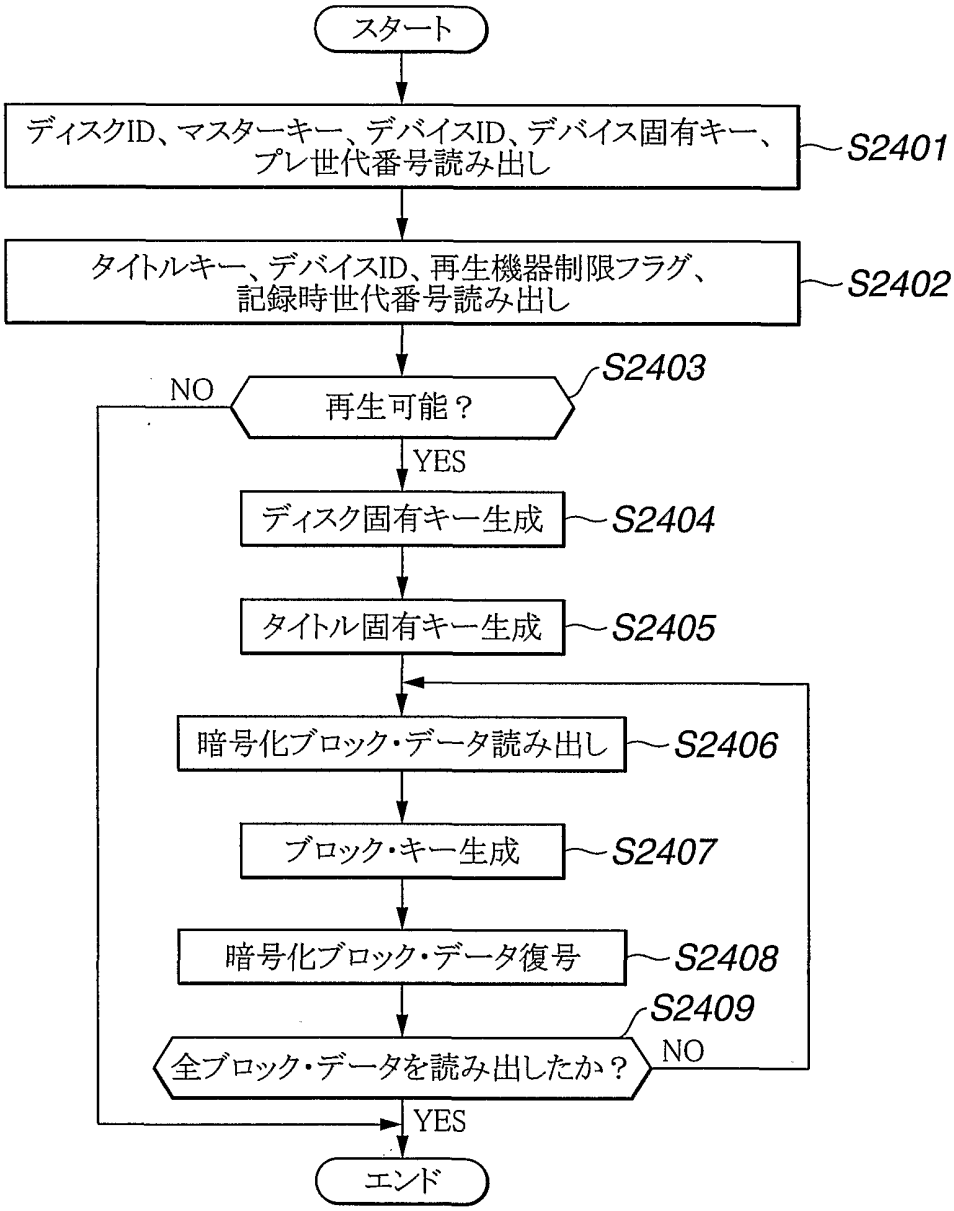

スタート
ディスクID、マスターキー、デバイスID、デバイス固有キー、プレ世代番号読み出し
S2401
タイトルキー、デバイスID、再生機器制限フラグ、記録時世代番号読み出し
S2402
再生可能？
S2403
NO
YES
ディスク固有キー生成
S2404
タイトル固有キー生成
S2405
暗号化ブロック・データ読み出し
S2406
ブロック・キー生成
S2407
暗号化ブロック・データ復号
S2408
全ブロック・データを読み出したか？
S2409
NO
YES
エンド

FIG.24

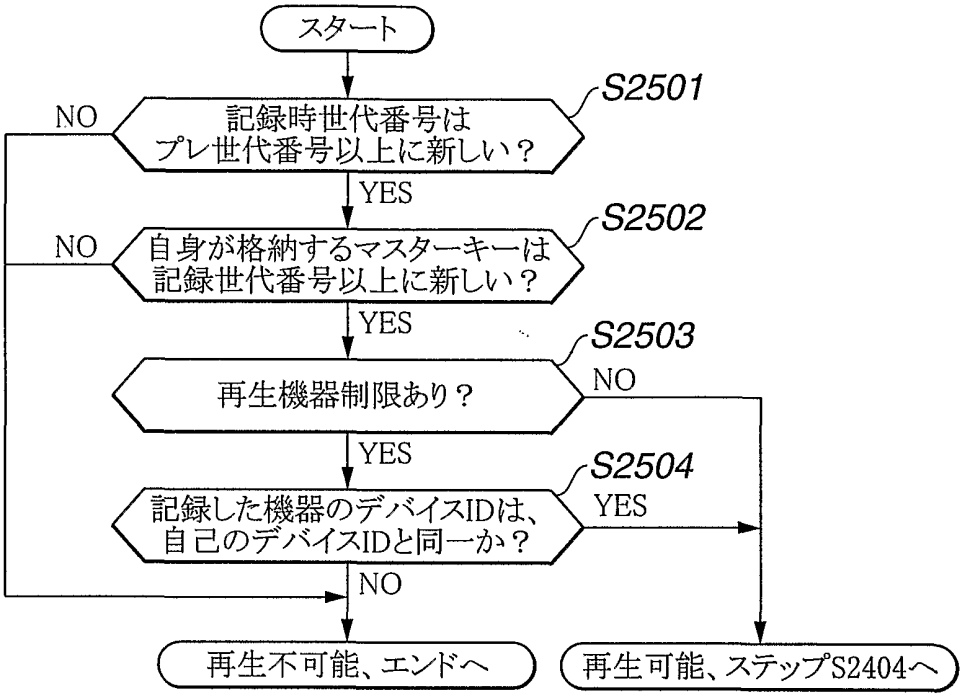

スタート
S2501
記録時世代番号は
プレ世代番号以上に新しい？
NO
YES
S2502
自身が格納するマスターキーは
記録世代番号以上に新しい？
NO
YES
S2503
再生機器制限あり？
NO
YES
S2504
記録した機器のデバイスIDは、
自己のデバイスIDと同一か？
YES
NO
再生不可能、エンドへ
再生可能、ステップS2404へ

FIG.25

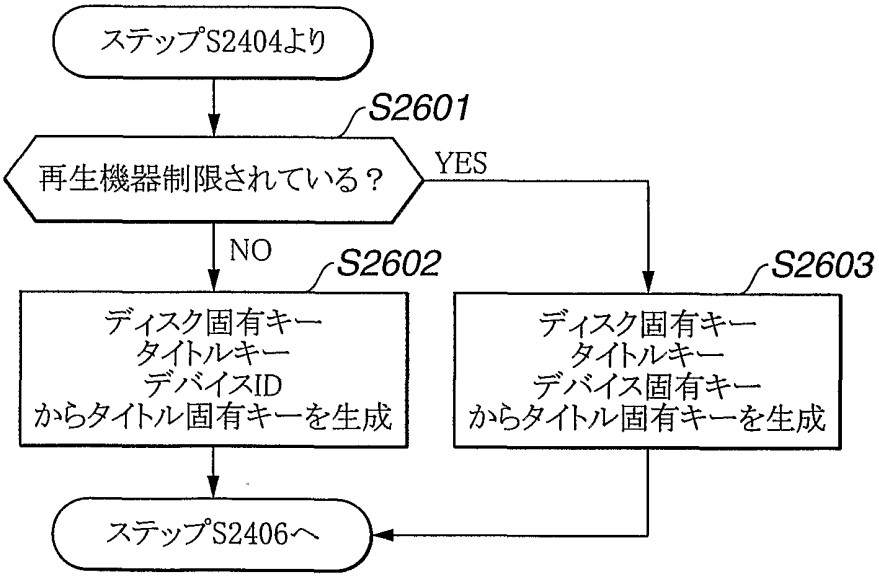

ステップS2404より
S2601
再生機器制限されている？
YES
NO
S2602
ディスク固有キー
タイトルキー
デバイスID
からタイトル固有キーを生成
S2603
ディスク固有キー
タイトルキー
デバイス固有キー
からタイトル固有キーを生成
ステップS2406へ

FIG.26

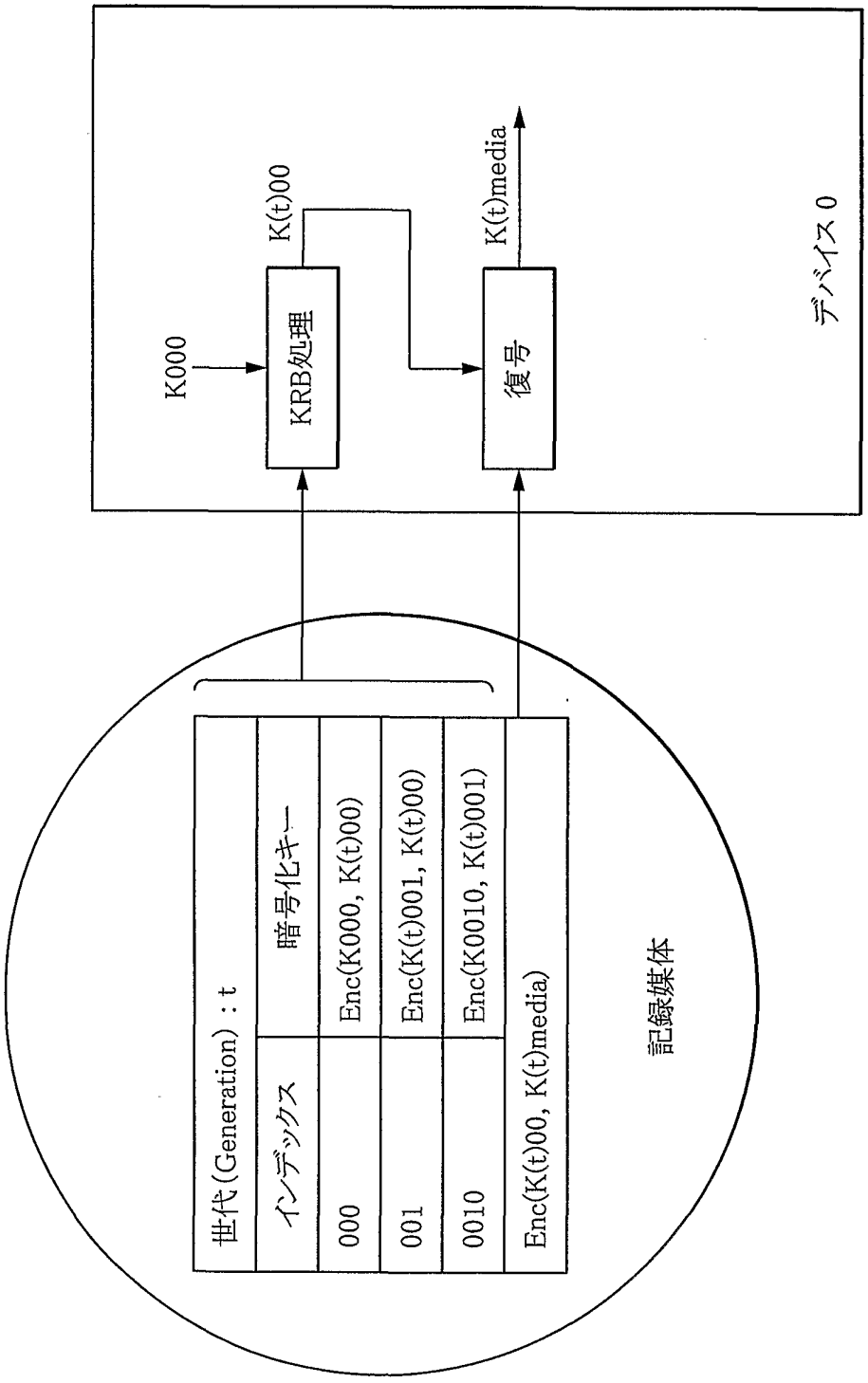

K000
KRB処理
K(t)00
復号
K(t)media
デバイス０
記録媒体
世代(Generation)：t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

FIG.27

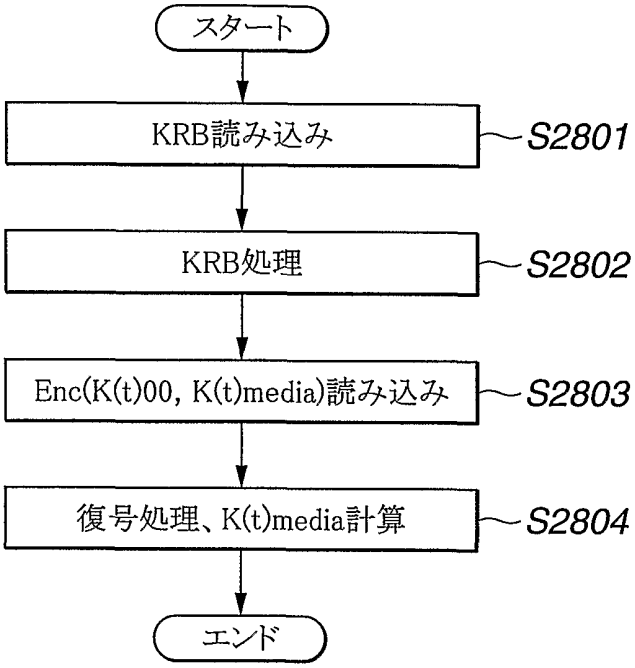

スタート
KRB読み込み
S2801
KRB処理
S2802
Enc(K(t)00, K(t)media)読み込み
S2803
復号処理、K(t)media計算
S2804
エンド

FIG.28

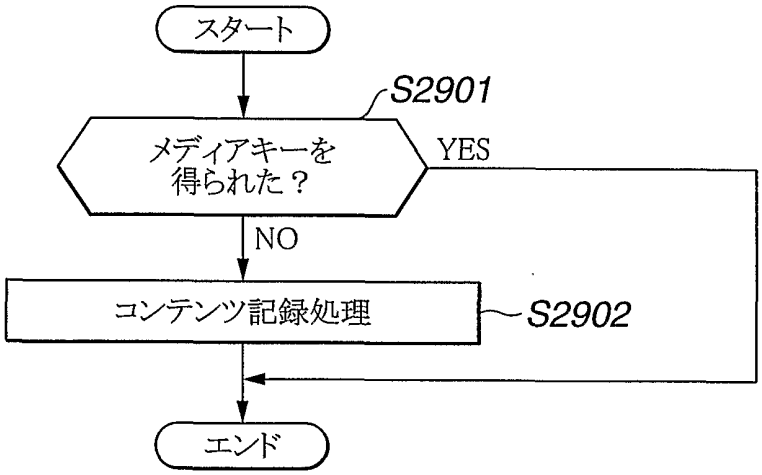

スタート
S2901
メディアキーを
得られた？
YES
NO
コンテンツ記録処理
S2902
エンド

FIG.29

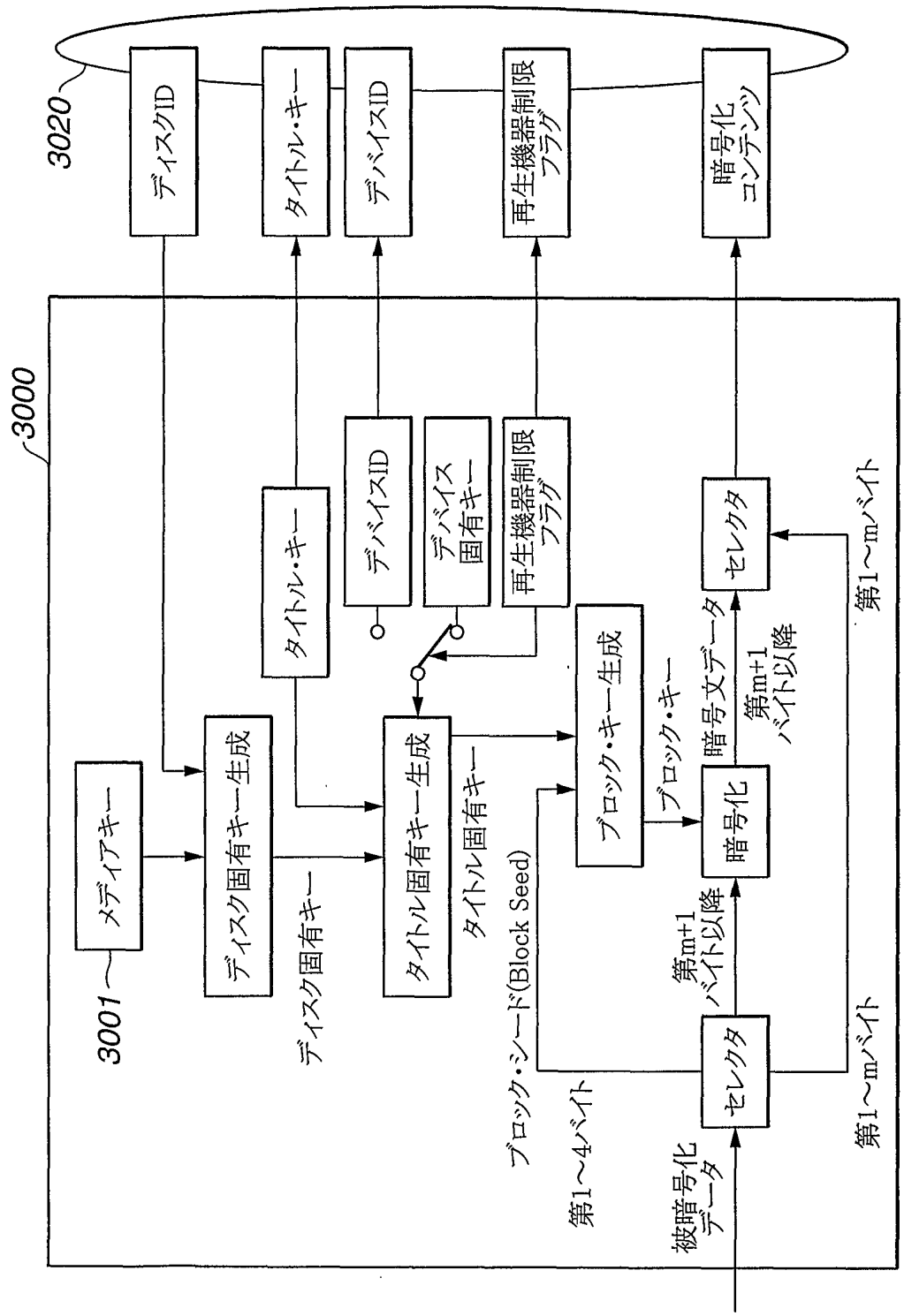

3020
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
3000
3001
メディアキー
ディスク固有キー生成
ディスク固有キー
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
タイトル固有キー生成
タイトル固有キー
ブロック・キー生成
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー
暗号化
暗号文データ
第m+1バイト以降
セレクタ
第1～mバイト
被暗号化データ
セレクタ
第m+1バイト以降
第1～mバイト

FIG.30

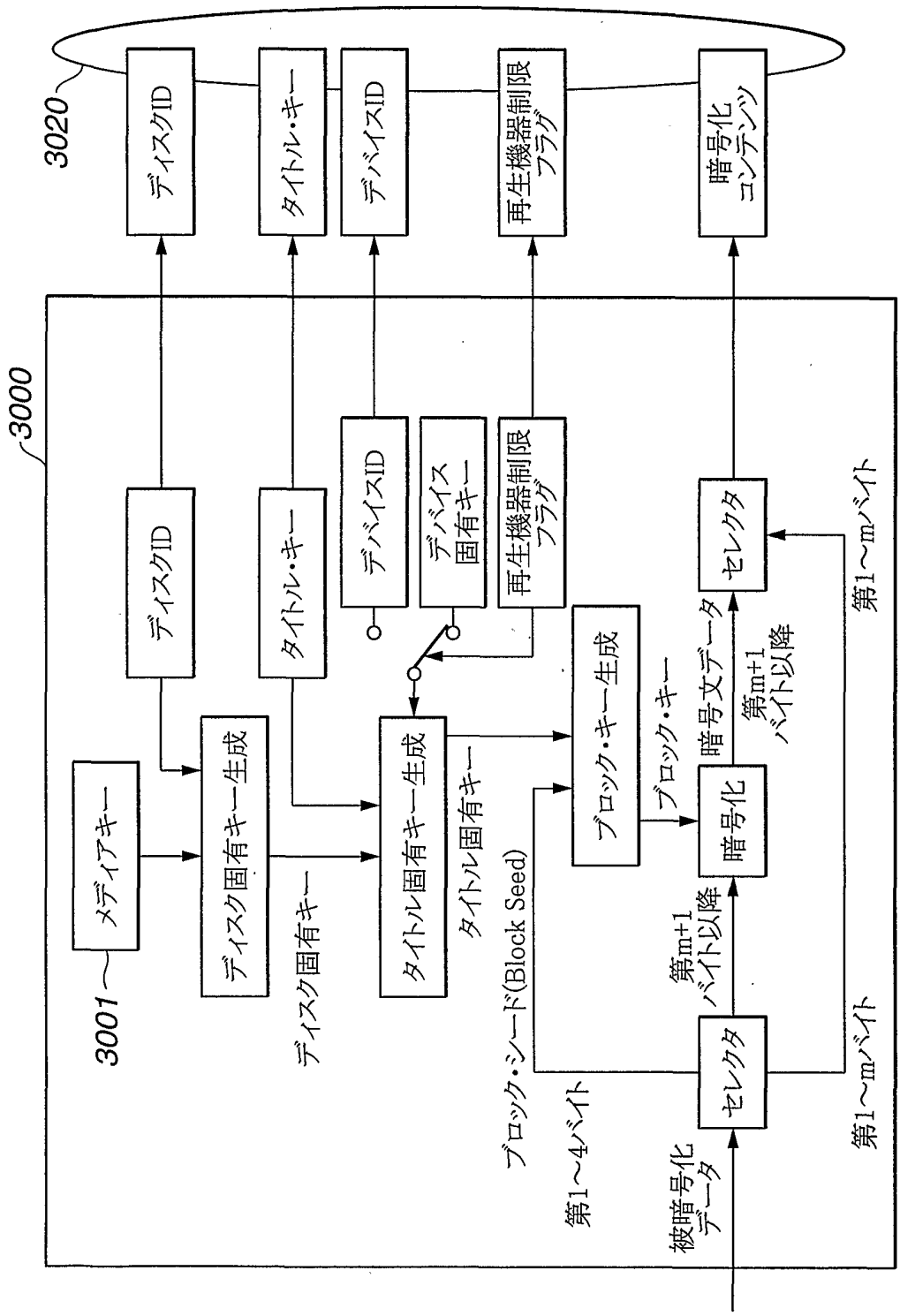

3020
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
3000
ディスクID
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
セレクタ
3001
メディアキー
ディスク固有キー生成
タイトル固有キー生成
ブロック・キー生成
暗号化
セレクタ
ディスク固有キー
タイトル固有キー
ブロック・シード(Block Seed)
ブロック・キー
暗号文データ
第m+1バイト以降
第1～4バイト
第m+1バイト以降
第1～mバイト
第1～mバイト
被暗号化データ

FIG.31

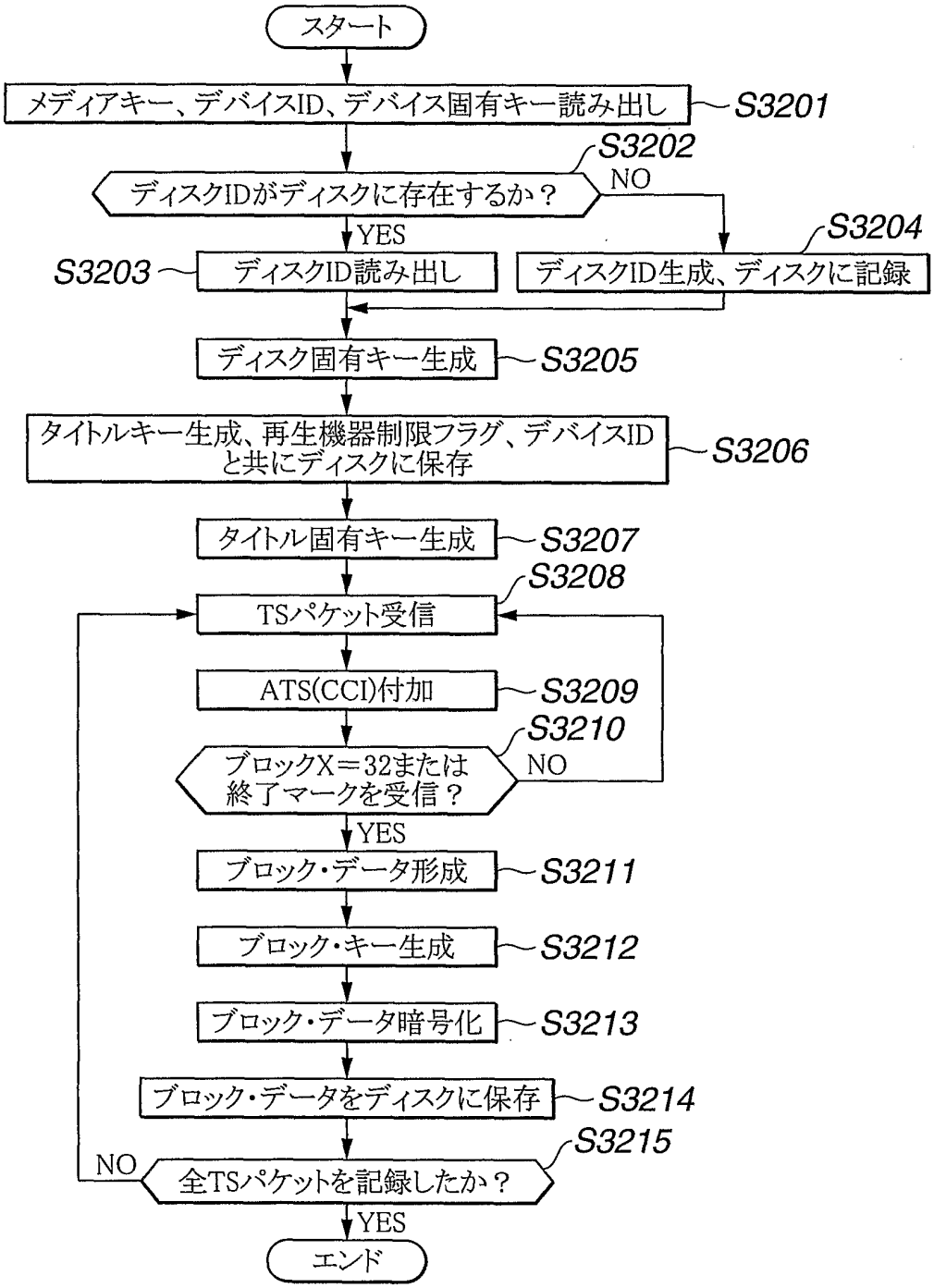

スタート
メディアキー、デバイスID、デバイス固有キー読み出し
S3201
S3202
ディスクIDがディスクに存在するか？
NO
YES
S3204
S3203
ディスクID読み出し
ディスクID生成、ディスクに記録
ディスク固有キー生成
S3205
タイトルキー生成、再生機器制限フラグ、デバイスID
と共にディスクに保存
S3206
タイトル固有キー生成
S3207
S3208
TSパケット受信
ATS(CCI)付加
S3209
S3210
ブロックX＝32または
終了マークを受信？
NO
YES
ブロック・データ形成
S3211
ブロック・キー生成
S3212
ブロック・データ暗号化
S3213
ブロック・データをディスクに保存
S3214
S3215
NO
全TSパケットを記録したか？
YES
エンド

FIG.32

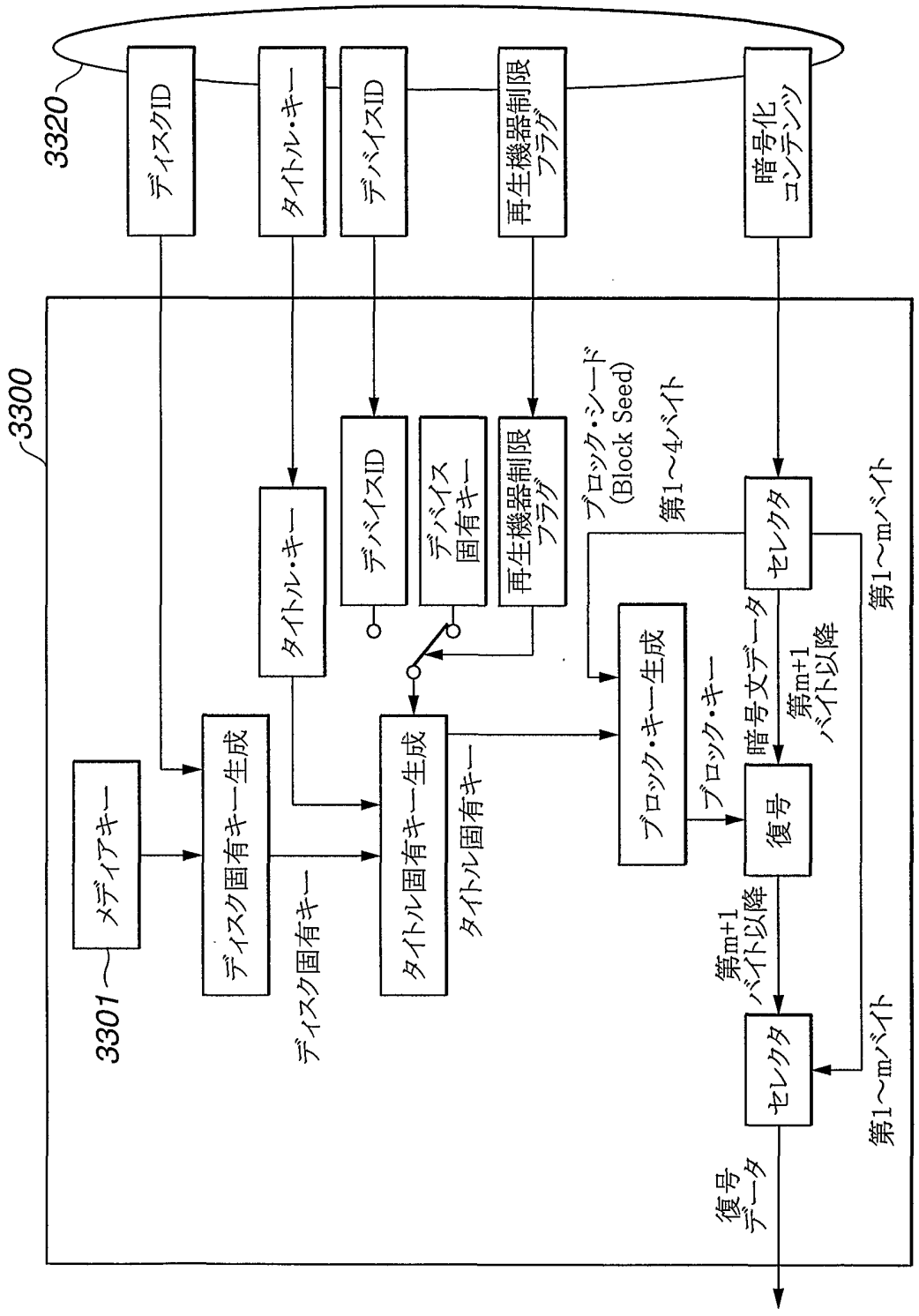

3320
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
3300
デバイスID
デバイス固有キー
再生機器制限フラグ
タイトル・キー
ブロック・シード (Block Seed)
第1～4バイト
セレクタ
第1～mバイト
メディアキー
3301
ディスク固有キー生成
タイトル固有キー生成
ブロック・キー生成
ディスク固有キー
タイトル固有キー
ブロック・キー
暗号文データ
第m+1バイト以降
復号
第m+1バイト以降
セレクタ
第1～mバイト
復号データ

FIG.33

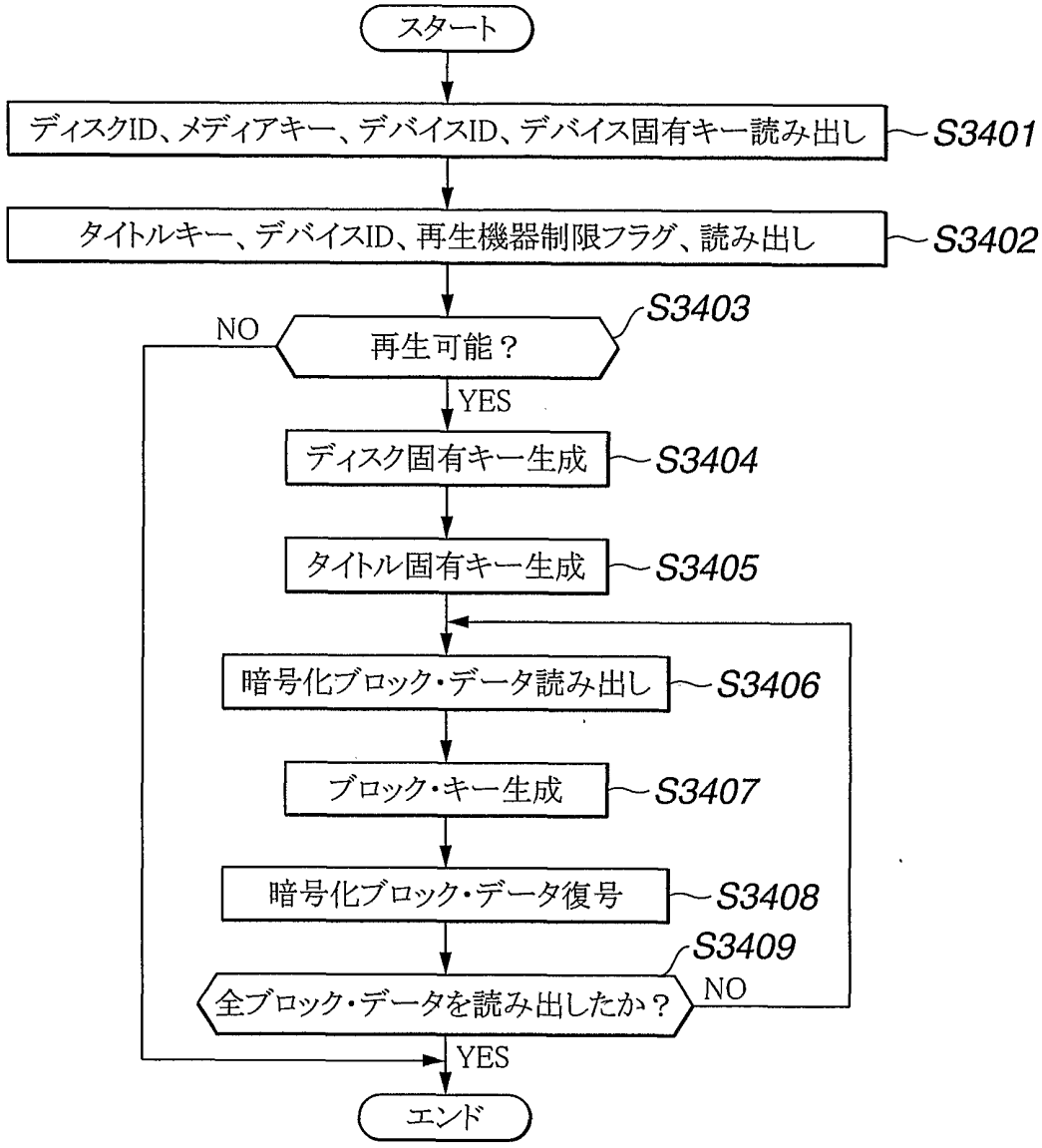

スタート
ディスクID、メディアキー、デバイスID、デバイス固有キー読み出し
S3401
タイトルキー、デバイスID、再生機器制限フラグ、読み出し
S3402
再生可能？
S3403
NO
YES
ディスク固有キー生成
S3404
タイトル固有キー生成
S3405
暗号化ブロック・データ読み出し
S3406
ブロック・キー生成
S3407
暗号化ブロック・データ復号
S3408
全ブロック・データを読み出したか？
S3409
NO
YES
エンド

FIG.34

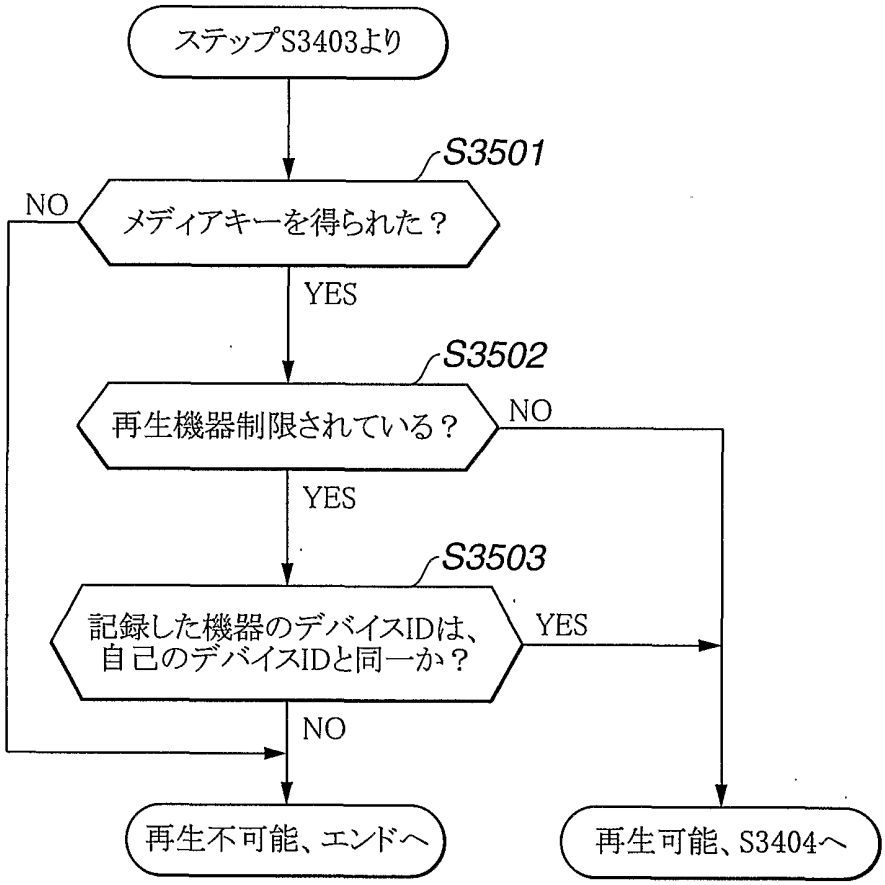

ステップS3403より
S3501
NO
メディアキーを得られた？
YES
S3502
再生機器制限されている？
NO
YES
S3503
記録した機器のデバイスIDは、
自己のデバイスIDと同一か？
YES
NO
再生不可能、エンドへ
再生可能、S3404へ

FIG.35

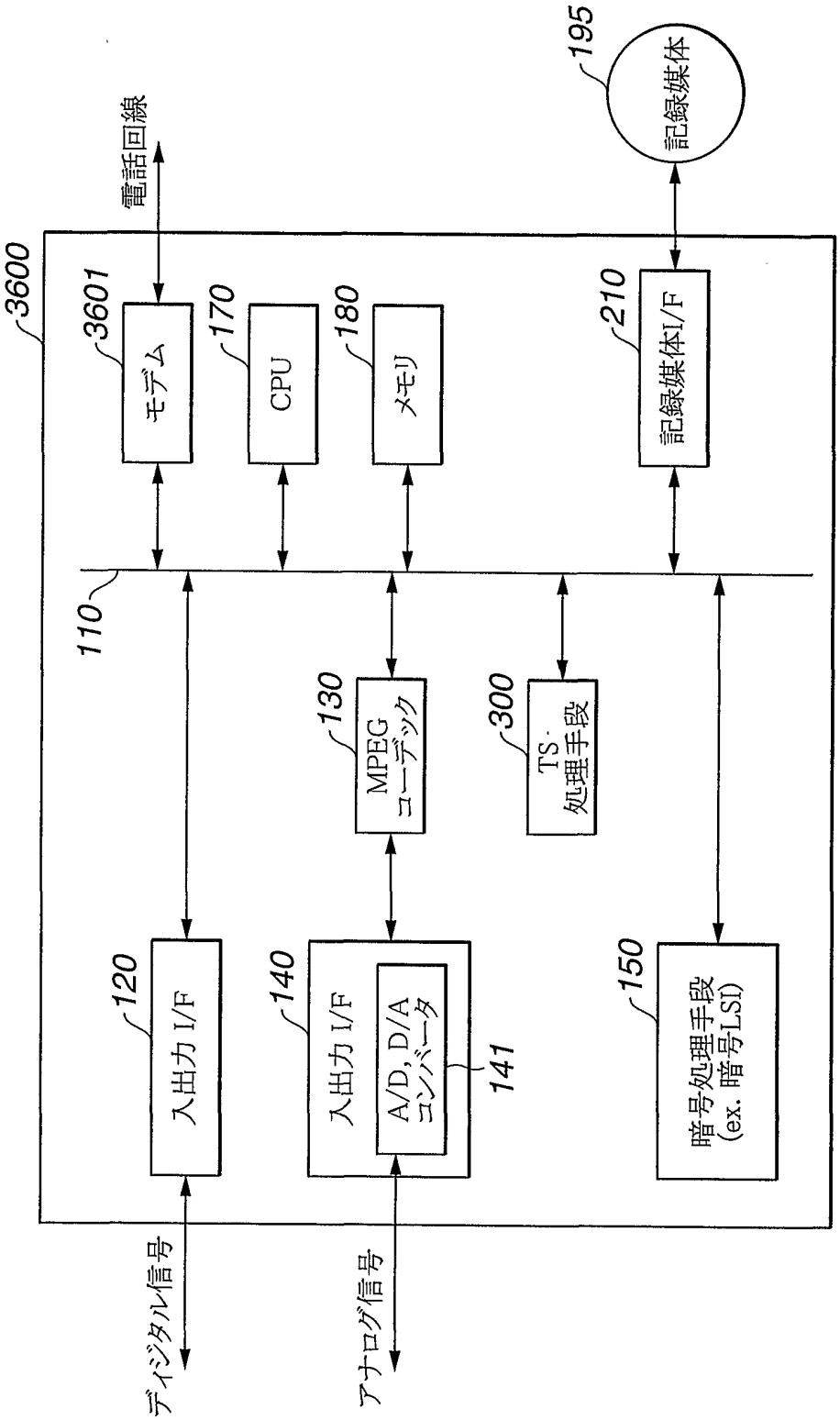

3600
3601
モデム
170
CPU
180
メモリ
210
記録媒体I/F
195
記録媒体
電話回線
110
130
MPEG
コーデック
300
TS
処理手段
120
入出力 I/F
140
入出力 I/F
A/D, D/A
コンバータ
141
150
暗号処理手段
(ex. 暗号LSI)
ディジタル信号
アナログ信号

FIG.36

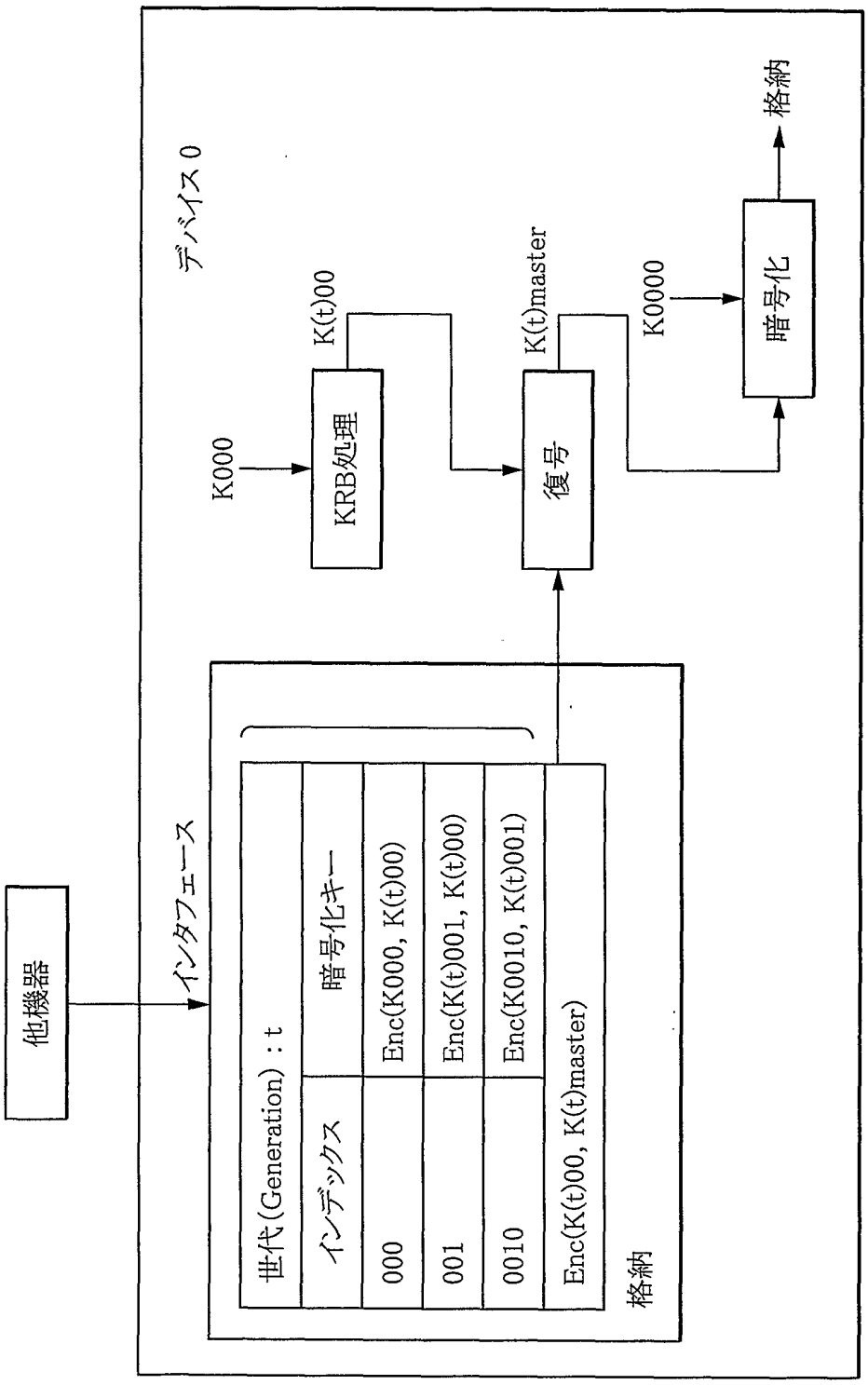

他機器
インタフェース
デバイス 0
K000
KRB処理
K(t)00
K(t)master
復号
K0000
暗号化
格納
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
格納

FIG.37

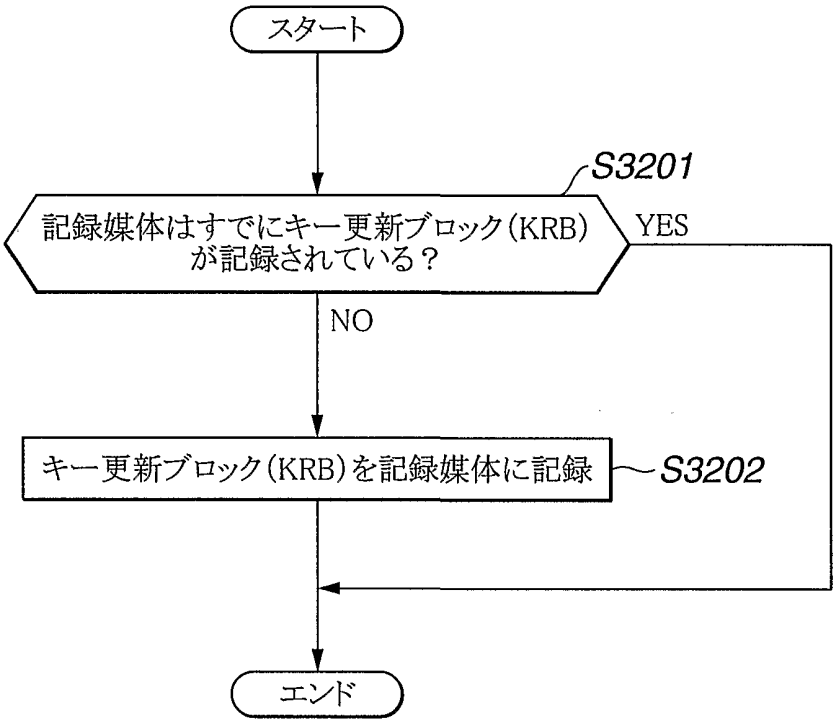

スタート
S3201
記録媒体はすでにキー更新ブロック(KRB)が記録されている？
YES
NO
キー更新ブロック(KRB)を記録媒体に記録
S3202
エンド

FIG.38

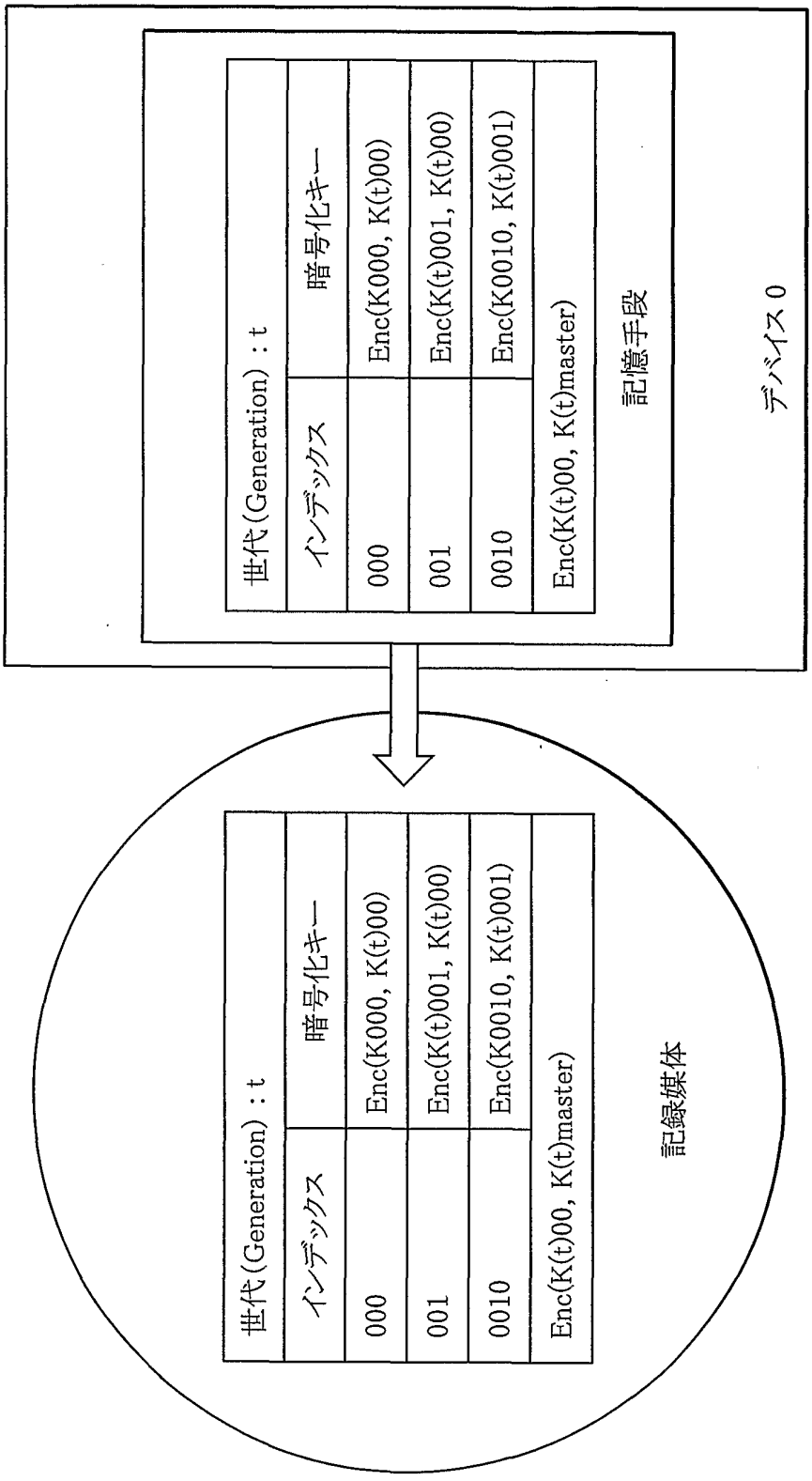

デバイス 0
記憶手段
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
記録媒体
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)

FIG.39

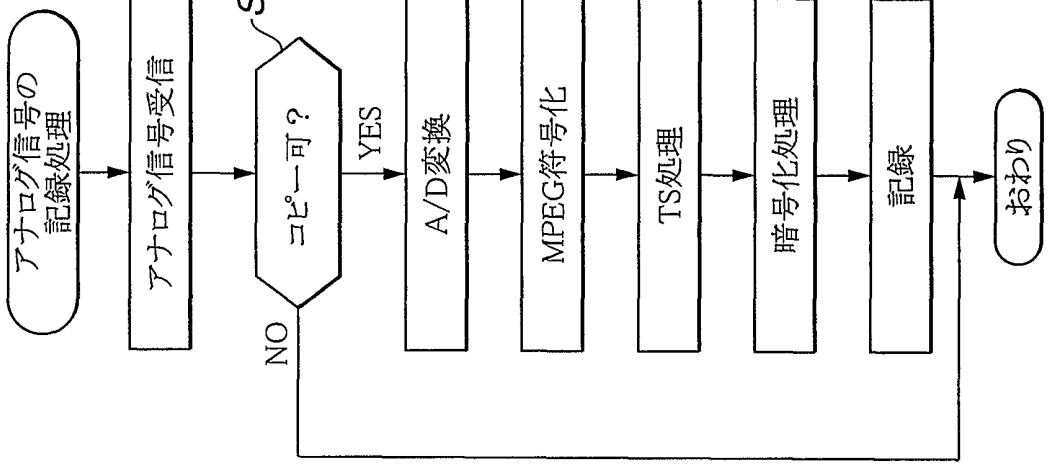


FIG.40B

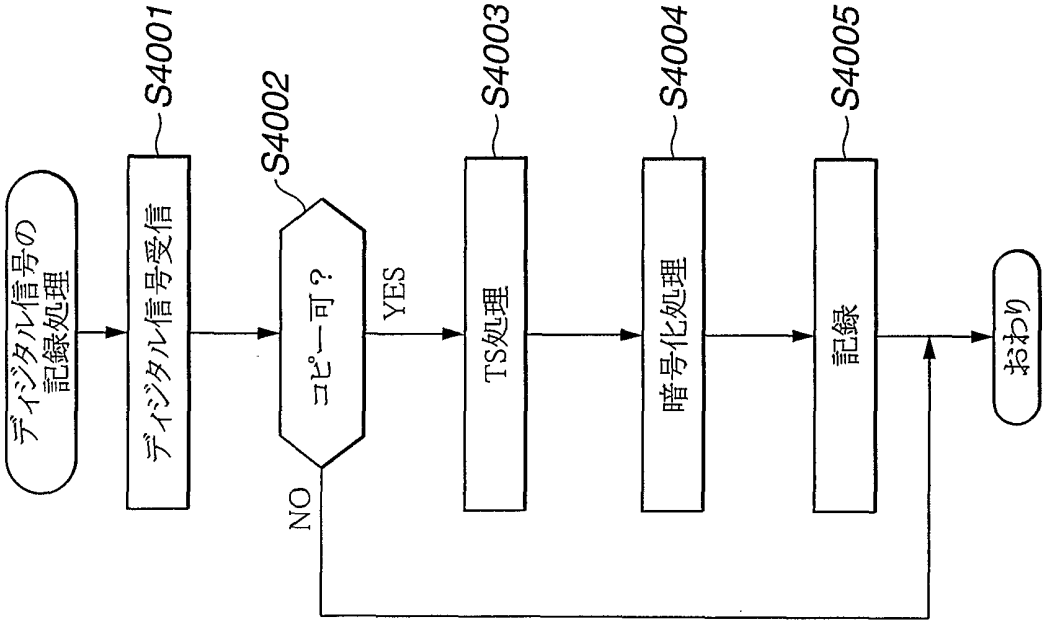


FIG.40A

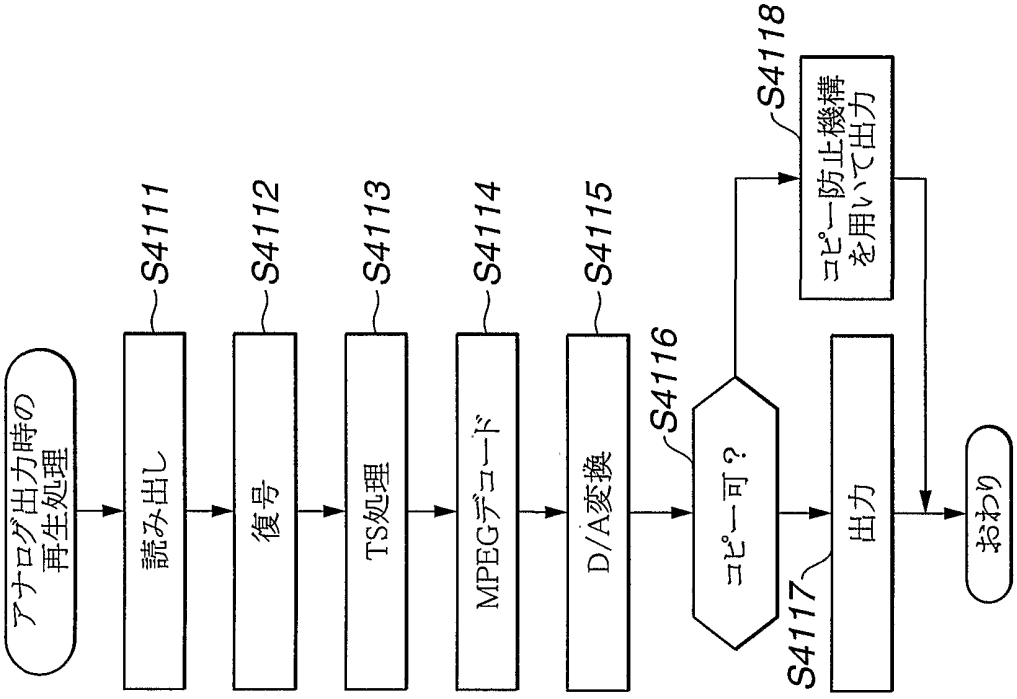


FIG.41B

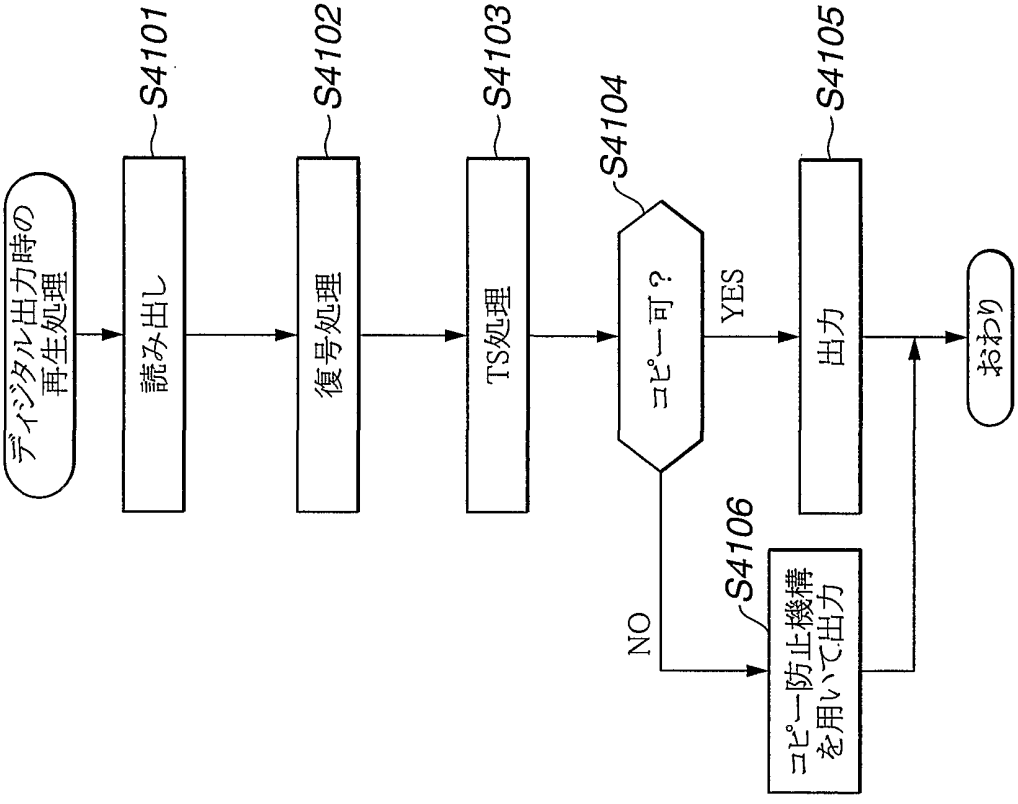


FIG.41A

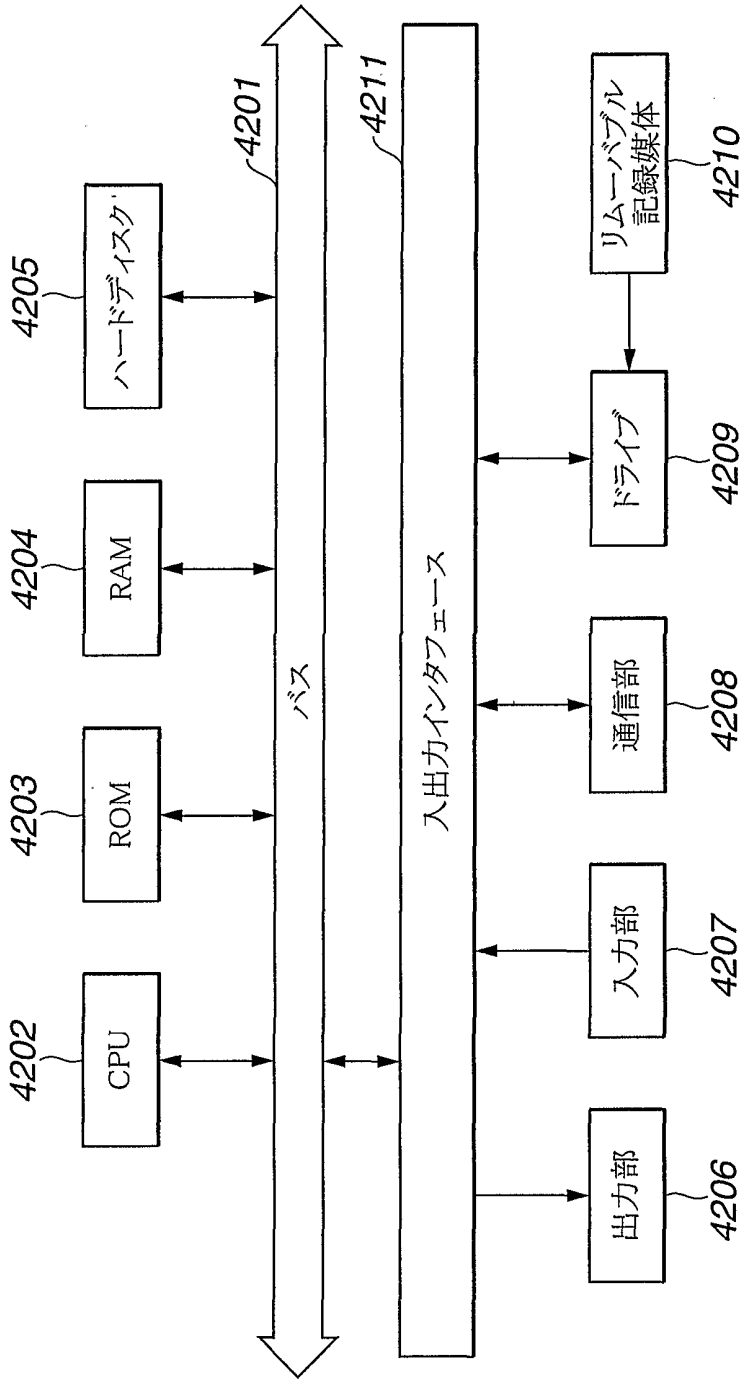

4201
4211
4205
ハードディスク
4204
RAM
4203
ROM
4202
CPU
バス
入出力インタフェース
リムーバブル記録媒体
4210
ドライブ
4209
通信部
4208
入力部
4207
出力部
4206

FIG.42

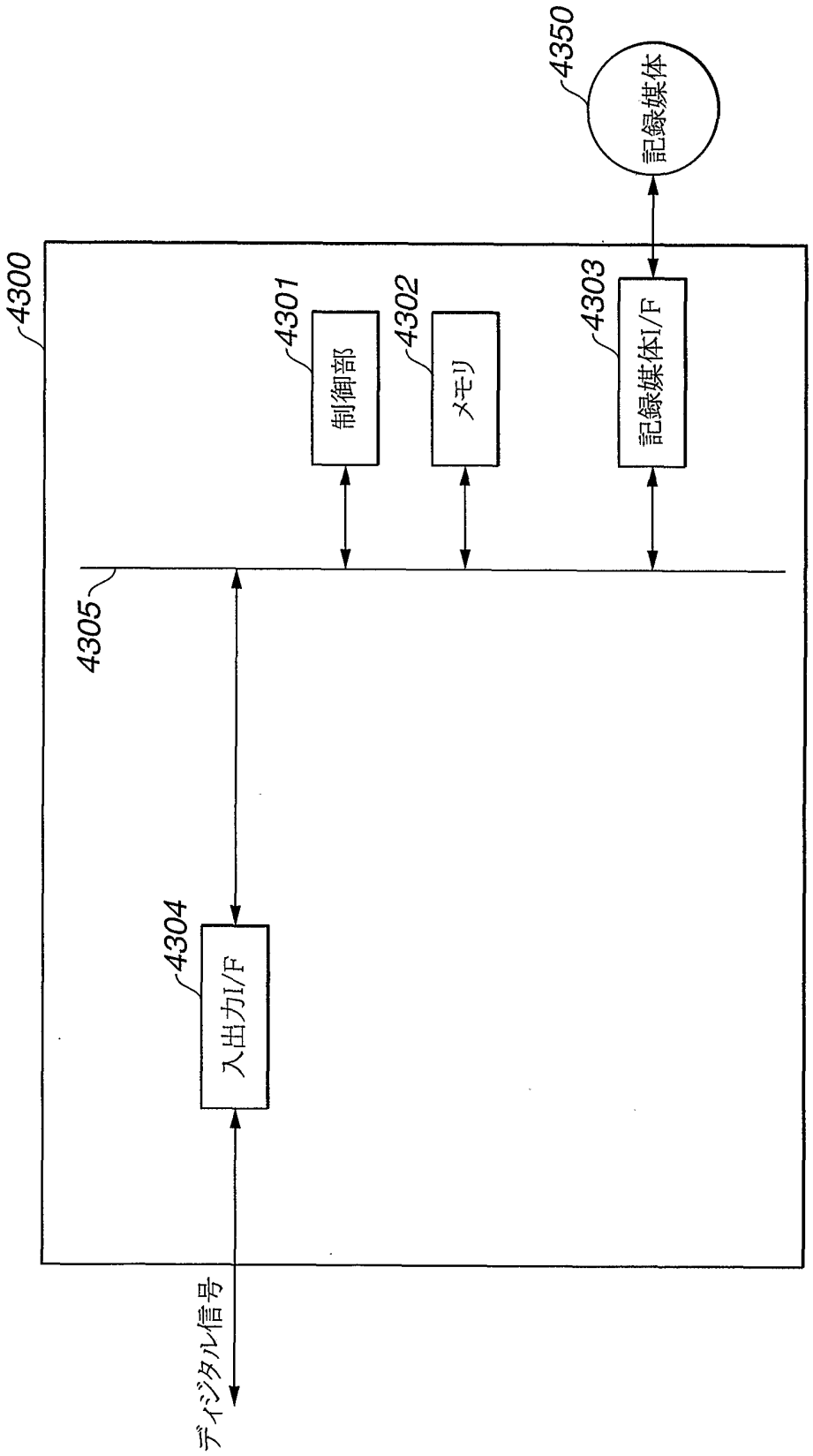

4350
記録媒体
4300
4301
制御部
4302
メモリ
4303
記録媒体I/F
4305
4304
入出力I/F
ディジタル信号

FIG.43

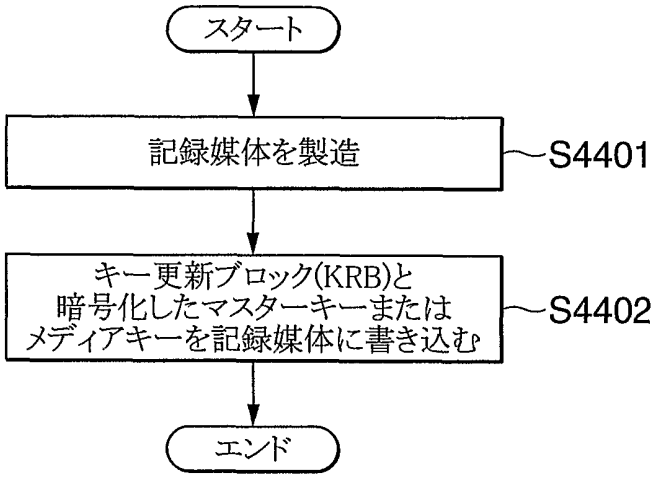

スタート
記録媒体を製造
S4401
キー更新ブロック(KRB)と
暗号化したマスターキーまたは
メディアキーを記録媒体に書き込む
S4402
エンド

FIG.44

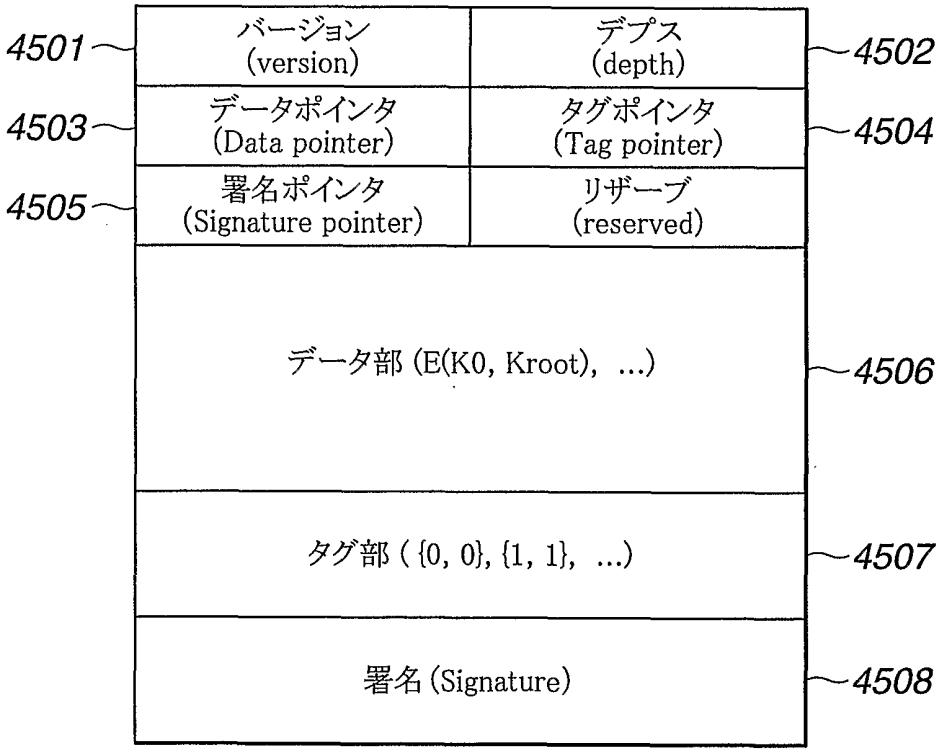

4501
バージョン
(version)
デプス
(depth)
4502
4503
データポインタ
(Data pointer)
タグポインタ
(Tag pointer)
4504
4505
署名ポインタ
(Signature pointer)
リザーブ
(reserved)
データ部 (E(K0, Kroot), ...)
4506
タグ部 ({0, 0}, {1, 1}, ...)
4507
署名 (Signature)
4508

FIG.45

FIG.46A

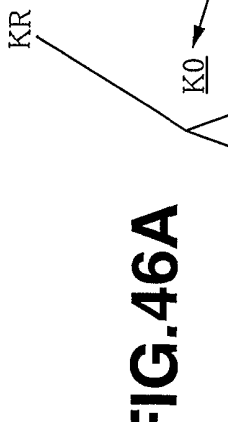


FIG.46B

キー更新ブロック(KRB：Key Renewal Block)

デバイス 0, 1, 2 にバージョン:tのノードキーを送付

トップノードアドレス：KR	
データ(暗号化キー)	タグ
Enc(K(t)0, K(t)R)	{0, 1}
Enc(K(t)00, K(t)0)	{0, 0}
Enc(K000, K(t)00)	{1, 1}
Enc(K(t)001, K(t)00)	{0, 1}
Enc(K0010, K(t)001)	{1, 1}

{Lタグ, Rタグ}
左(L) 右(R)それぞれの方向にデータがあれば0、なければ1

データ：Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ...

タグ：{0, 1}, {0, 0}, {1, 1}, ...

FIG.46C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/02963

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/00, G11B20/10, G11B20/12

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.Cl[7] H04L9/00, G11B20/10, G11B20/12

Documentation 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 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST DATABASE ON SCIENCE AND TECHNOLOGY key, tree, DVD

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 11-224461 A (Sony Corporation) 17 August 1999 (17.08.99) Full text (Family: none)	1-6,10-18,22-28,33-40,44-58 7-9,19-21,29-32,41-43
Y A	JP 11-187013 A (IBM Japan Ltd.) 09 July 1999 (09.07.99) Par. Nos. [0009]-[0011], [0017]-[0022] & CN 1224962 A	1-6,10-18,22-28,33-40,44-58 7-9,19-21,29-32,41-43
Y A	WALDVOGEL, M. et al. The VarsaKey Framework: Versatile Group Key Management. IEEE Journal on Selected Areas in Communications. September 1999, Vol.17, No.9, pp.1614-1631, especially pp.1616-1621	1-6,10-18,22-28,33-40,44-58 7-9,19-21,29-32,41-43
Y A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98, 1998, pp.68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	1-6,10-18,22-28,33-40,44-58 7-9,19-21,29-32,41-43

☒ 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 document 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	Date of mailing of the international search report
05 July, 2001 (05.07.01)	17 July, 2001 (17.07.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/02963

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 789361 A2 (Matsushita Electric Ind. Co., Ltd.) 13 August 1997 (13.08.97 column 40, line 42 to column 41 line 22 & JP 10-79174 A, column 42, lines 2-38; column 55, lines 31-42 & WO 97/14249 A1 & EP 800312 A1 & KR 98700776 A & KR 98004075 A & TW 346571 A & US 6047103 A	11,12,23,24, 34,35,45,46
A	JP 11-250570 A (Matsushita Electric Ind. Co., Ltd.) 17 September 1999 (17.09.99) column 13, line 17 to column 16 line 32 (Family: none)	1-58
A	JP 11-126425 A (Sony Corporation) 11 May, 1999 (11.05.99) Full text (Family: none)	1-58
A	JP 10-3256 A (Sony Corporation) 06 January 1998 (06.01.98) Full text (Family: none)	1-58
A	5C Digital Transmission Content Protection White Paper. Revision 1.0, 1998, p.3, 11, 12 (http://www.dtcp.com)	1-58
PA	Makoto TATEBAYASHI et al. "Kiroku Media no Contents Hogo System" 2000 nen Denshi Joho Tsushin Gakkai Kiso Kyoukai Society Taikai Kouen Ronbunshuu, 07 September 2000 (07.09.00), pp.367-368	1-58

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/02963

Box I Observations where certain claims were found unsearchable (Continuation of item 1 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 II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

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

The inventions of the claims of the present international application are divided into the following two groups.

1. The inventions of claims 1-46, 57, 58
2. The inventions of claims 47-56

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.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０２９６３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／００，Ｇ１１Ｂ２０／１０，Ｇ１１Ｂ２０／１２

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　Ｈ０４Ｌ９／００，Ｇ１１Ｂ２０／１０，Ｇ１１Ｂ２０／１２

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	１９７１－２００１年
日本国登録実用新案公報	１９９４－２００１年
日本国実用新案登録公報	１９９６－２００１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）

ＷＰＩ，ＪＩＣＳＴ科学技術文献データベース　key, tree, DVD

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 11-224461 A（ソニー株式会社） 17.8月.1999(17.08.99)，全頁を参照（ファミリーなし）	1-6，10-18，22-28，33-40，44-58
Ａ		7-9，19-21，29-32，41-43

☒ 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 ０５．０７．０１	国際調査報告の発送日 17.07.01
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

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9. 7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	1-6 ,10-18, 22-28,33-40, 44-58
A		7-9 ,19-21, 29-32,41-43
Y	WALDVOGEL, M. et al. The VersaKey Framework:Versatile Group Key Management. IEEE Journal on Selected Areas in Communications.	1-6.,10-18, 22-28,33-40, 44-58
A	Septemper 1999, Vol.17, No.9 ,p.1614-1631, especially pp.1616-1621	7-9 ,19-21, 29-32,41-43
Y	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98 ,1998 ,p.68-79	1-6 ,10-18, 22-28,33-40, 44-58
A	especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	7-9 ,19-21, 29-32,41-43
Y	EP 789361 A2 (MATSUSHITA ELECTRIC IND. CO. LTD.) 13.8月.1997(13.08.97) 第40欄第42行－第41欄第22行 & JP 10-79174 A, 第42欄第2-38行, 第55欄第31-42行 & WO 97/14249 A1 & EP 800312 A1 & KR 98700776 A & KR 98004075 A & TW 346571 A & US 6047103 A	11,12,23,24, 34,35,45,46
A	JP 11-250570 A (松下電器産業株式会社) 17.9月.1999(17.09.99), 第13欄第17行-第16欄第32行 (ファミリーなし)	1-58
A	JP 11-126425 A (ソニー株式会社) 11.5月.1999(11.05.99), 全頁を参照 (ファミリーなし)	1-58
A	JP 10-3256 A (ソニー株式会社) 6.1月.1998(06.01.98), 全頁を参照 (ファミリーなし)	1-58
A	5C Digital Transmission Content Protection White Paper. Revision 1.0, 1998, p.3, 11, 12 (http://www.dtcp.com)	1-58
PA	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-58

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０２９６３

第Ⅰ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（ＰＣＴ１７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Ⅱ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の国際調査機関は認めた。

この出願の発明は、下記の２群の発明に区分される。

1．請求の範囲 1-46, 57, 58
2．請求の範囲47-56

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ので、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ので、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。

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。