(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4941607号
(P4941607)
(45)発行日　平成24年5月30日(2012.5.30)　(24)登録日　平成24年3月9日(2012.3.9)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　G06F 21/24 166A
G06F 21/22 (2006.01)　G06F 21/22 110L
G09C 1/00 (2006.01)　G09C 1/00 610A

請求項の数 10　(全 63 頁)

(21)出願番号　特願2011-152918 (P2011-152918)
(22)出願日　平成23年7月11日 (2011.7.11)
(62)分割の表示　特願2005-265476 (P2005-265476)の分割
原出願日　平成17年9月13日 (2005.9.13)
(65)公開番号　特開2011-216109 (P2011-216109A)
(43)公開日　平成23年10月27日 (2011.10.27)
審査請求日　平成23年7月11日 (2011.7.11)

早期審査対象出願

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100095496
弁理士　佐々木　榮二
(74)代理人　110000763
特許業務法人大同特許事務所

最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法

(57)【特許請求の範囲】
【請求項１】
コンテンツ再生処理を実行する情報処理装置であり、
再生対象となる入力コンテンツの構成データの一部を、変換テーブルに記録された変換データに置き換えるデータ変換処理を実行して再生コンテンツを生成する処理を実行するコンテンツ再生処理部と、
前記コンテンツ再生処理部に対して、前記データ変換処理において適用するパラメータを提供するパラメータ生成部とを有し、
前記コンテンツ再生処理部は、
コンテンツ再生区間情報であるクリップ情報に含まれ、コンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを取得し、
前記ＥＰマップ登録テーブルＩＤを適用した演算処理により、再生コンテンツの区分領域として設定されたセグメント毎に異なるパラメータ識別子を算出し、算出したパラメータ識別子を伴うパラメータ算出要求を前記パラメータ生成部に出力する構成を有し、
前記パラメータ生成部は、
前記コンテンツ再生部からのパラメータ算出要求に応じて、セグメント毎に異なるセグメント固有のパラメータを算出して前記コンテンツ再生部に提供し、
前記コンテンツ再生処理部は、
前記変換テーブルに記録された変換テーブルデータに対して、前記パラメータ生成部か

ら取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行する情報処理装置。

【請求項２】

前記コンテンツ再生処理部は、

前記ＥＰマップ登録テーブルＩＤに基づいて、前記セグメントに対応するパラメータ識別子を、下記算出式、すなわち、

（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ

ただし、

ＳＰ＿ＩＤ：パラメータ識別子、

ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、

Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、

上記式に従って算出する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記コンテンツ再生処理部は、

前記変換データを含む変換テーブルデータをコンテンツ中に含まれるパケットから取得して、前記パラメータ生成部から取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項４】

前記コンテンツ再生処理部は、

前記変換データを含む変換テーブルデータをコンテンツと異なる独立した変換テーブルデータから取得して、前記パラメータ生成部から取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項５】

情報記録媒体製造装置であり、

正当コンテンツ構成データと異なるブロークンデータを含むコンテンツと、

コンテンツの再生区間情報を記録したクリップ情報と、

前記ブロークンデータの置き換え対象となる変換データを、コンテンツの区分領域であるセグメント毎に異なるセグメント固有のパラメータによって演算または暗号化処理を施して記録した変換テーブルボディデータと、前記パラメータの識別情報としてのパラメータ識別子を記録したパラメータ識別子特定テーブルを含む変換テーブルと、

を生成するデータ処理部と、

前記ブロークンデータを含むコンテンツと、前記変換テーブルとを情報記録媒体に記録するデータ記録部と、

を有し、

前記パラメータ識別子は、

前記クリップ情報に含まれるコンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを適用した演算処理により算出可能な識別子である情報記録媒体製造装置。

【請求項６】

前記パラメータ識別子は、

前記ＥＰマップ登録テーブルＩＤを適用した下記算出式、すなわち、

（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ

ただし、

ＳＰ＿ＩＤ：パラメータ識別子、

ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、
Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、
上記式に従って算出可能な識別子である請求項５に記載の情報記録媒体製造装置。
【請求項７】
情報記録媒体であり、
一部のコンテンツ構成データが置き換えられて再生されるコンテンツと、
コンテンツの再生区間情報を記録したクリップ情報と、
前記コンテンツ構成データを複数に区分して設定されたセグメント毎に異なるセグメント固有のパラメータ識別子と、置き換えられる一部のコンテンツ構成データの置き換え対象となる変換データとを対応させて登録した変換テーブルとを格納し、
前記変換データは前記パラメータ識別子に対応するセグメント固有のパラメータに基づき演算または暗号化処理を施したデータであり、
前記パラメータ識別子は、
前記クリップ情報に含まれるコンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを適用した演算処理により算出可能な識別子であり、
前記情報記録媒体の記録コンテンツを再生する情報処理装置において、
前記ＥＰマップ登録テーブルＩＤを適用した演算処理による前記セグメント固有のパラメータ識別子を算出処理と、前記セグメント固有のパラメータ識別子に基づくパラメータ算出処理と、算出パラメータに基づく演算または暗号化処理を伴うコンテンツ再生を実行させることを可能とした情報記録媒体。
【請求項８】
前記パラメータ識別子は、
前記ＥＰマップ登録テーブルＩＤを適用した下記算出式、すなわち、
（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ
ただし、
ＳＰ＿ＩＤ：パラメータ識別子、
ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、
Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、
上記式に従って算出可能な識別子である請求項７に記載の情報記録媒体。
【請求項９】
情報処理装置において、コンテンツ再生処理を実行する情報処理方法であり、
コンテンツ再生処理部において、
コンテンツ再生区間情報であるクリップ情報に含まれ、コンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを取得し、
前記ＥＰマップ登録テーブルＩＤを適用した演算処理により、再生コンテンツの区分領域として設定されたセグメント毎に異なるパラメータ識別子を算出し、算出したパラメータ識別子を伴うパラメータ算出要求をパラメータ生成部に出力するステップと、
パラメータ生成部において、
前記コンテンツ再生部からのパラメータ算出要求に応じて、セグメント毎に異なるセグメント固有のパラメータを算出して前記コンテンツ再生部に提供するステップと、
前記コンテンツ再生処理部において、
再生対象となる入力コンテンツの構成データの一部を、変換テーブルに記録された変換データに置き換えるデータ変換処理を実行して再生コンテンツを生成する処理を実行するコンテンツ再生処理ステップであり、
前記変換テーブルに記録された変換テーブルデータに対して、前記パラメータ生成部から取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行して再生コンテンツを生成するコンテンツ再生処理ステップを実行す

る情報処理方法。
【請求項１０】
前記パラメータ識別子は、
前記ＥＰマップ登録テーブルＩＤに基づいて、下記算出式、すなわち、
（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ
ただし、
ＳＰ＿ＩＤ：パラメータ識別子、
ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、
Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、
上記式に従って算出可能な識別子である請求項９に記載の情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法に関する。さらに、詳細には、コンテンツ利用管理の要求される様々なコンテンツに対するデータ変換処理により、不正なコンテンツ利用を排除し、厳格なコンテンツ利用管理を実現する情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法に関する。
【背景技術】
【０００２】
音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）は、記録メディア、例えば、青色レーザを適用したＢｌｕ－ｒａｙディスク、あるいはＤＶＤ(Digital Versatile Disc)、ＭＤ(Mini Disc)、ＣＤ(Compact Disc)にデジタルデータとして格納することができる。特に、青色レーザを利用したＢｌｕ－ｒａｙディスクは、高密度記録可能なディスクであり大容量の映像コンテンツなどを高画質データとして記録することができる。
【０００３】
これら様々な情報記録媒体（記録メディア）にデジタルコンテンツが格納され、ユーザに提供される。ユーザは、所有するＰＣ（Personal Computer）、ディスクプレーヤ等の再生装置においてコンテンツの再生、利用を行う。
【０００４】
音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。
【０００５】
デジタル記録装置およ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可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをＣＤ－Ｒ等にコピーした、いわゆる海賊版ディスクの流通や、ＰＣ等のハードディスクに格納したコピーコンテンツの利用が蔓延しているといった問題が発生している。
【０００６】
ＤＶＤ、あるいは近年開発が進んでいる青色レーザを利用した記録媒体等の大容量型記録媒体は、１枚の媒体に例えば映画１本～数本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。
【０００７】
コンテンツの不正コピーを防止して著作権者の保護を図る１つの手法としてコンテンツ

の暗号化処理がある。しかし、コンテンツを暗号化しても、暗号鍵の漏洩が発生してしまうと、不正に復号されたコンテンツが流出するという問題が発生する。このような問題を解決する１つの構成を開示した従来技術として、特許文献１に記載の構成がある。特許文献１は、コンテンツの一部をダミーデータに置き換えて記録することで、コンテンツの不正再生を防止した構成を開示している。

【０００８】

コンテンツをダミーデータに置き換えたコンテンツの再生処理に際しては、ダミーデータを正常なコンテンツデータに再度、置き換える処理が必要になる。このデータ変換処理は、正常コンテンツの外部への漏洩を発生させることなく行なわれることが必要であり、またダミーデータの配置位置などや変換方法などの処理情報についても漏洩を防止することが好ましい。このような再生時の処理を、情報漏洩を防止し安全に実行する構成については、まだ検討すべき課題が多いというのが現状である。

【先行技術文献】

【特許文献】

【０００９】

【特許文献１】特開平１１－４５５０８号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

本発明は、このような状況に鑑みてなされたものであり、コンテンツ構成データの部分的な置き換えによってコンテンツを破壊し、効果的なコンテンツの不正利用防止を実現するとともに、再生処理において、情報漏洩を防止したセキュアなデータ処理を実現する情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法を提供することを目的とするものである。

【課題を解決するための手段】

【００１１】

本発明の第１の側面は、

コンテンツ再生処理を実行する情報処理装置であり、

再生対象となる入力コンテンツの構成データの一部を、変換テーブルに記録された変換データに置き換えるデータ変換処理を実行して再生コンテンツを生成する処理を実行するコンテンツ再生処理部と、

前記コンテンツ再生処理部に対して、前記データ変換処理において適用するパラメータを提供するパラメータ生成部とを有し、

前記コンテンツ再生処理部は、

コンテンツ再生区間情報であるクリップ情報に含まれ、コンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを取得し、

前記ＥＰマップ登録テーブルＩＤを適用した演算処理により、再生コンテンツの区分領域として設定されたセグメント毎に異なるパラメータ識別子を算出し、算出したパラメータ識別子を伴うパラメータ算出要求を前記パラメータ生成部に出力する構成を有し、

前記パラメータ生成部は、

前記コンテンツ再生部からのパラメータ算出要求に応じて、セグメント毎に異なるセグメント固有のパラメータを算出して前記コンテンツ再生部に提供し、

前記コンテンツ再生処理部は、

前記変換テーブルに記録された変換テーブルデータに対して、前記パラメータ生成部から取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行する情報処理装置にある。

【００１２】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツ再生処理部は、

前記ＥＰマップ登録テーブルＩＤに基づいて、前記セグメントに対応するパラメータ識別子を、下記算出式、すなわち、

（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ

ただし、

ＳＰ＿ＩＤ：パラメータ識別子、

ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、

Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、

上記式に従って算出する処理を実行する構成であることを特徴とする。

【００１３】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツ再生処理部は、前記変換データを含む変換テーブルデータをコンテンツ中に含まれるパケットから取得して、前記パラメータ生成部から取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行する構成であることを特徴とする。

【００１４】

さらに、本発明の情報処理装置の一実施態様において、前記コンテンツ再生処理部は、前記変換データを含む変換テーブルデータをコンテンツと異なる独立した変換テーブルデータから取得して、前記パラメータ生成部から取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行する構成であることを特徴とする。

【００１５】

さらに、本発明の第２の側面は、

情報記録媒体製造装置であり、

正当コンテンツ構成データと異なるブロークンデータを含むコンテンツと、

コンテンツの再生区間情報を記録したクリップ情報と、

前記ブロークンデータの置き換え対象となる変換データを、コンテンツの区分領域であるセグメント毎に異なるセグメント固有のパラメータによって演算または暗号化処理を施して記録した変換テーブルボディデータと、前記パラメータの識別情報としてのパラメータ識別子を記録したパラメータ識別子特定テーブルを含む変換テーブルと、

を生成するデータ処理部と、

前記ブロークンデータを含むコンテンツと、前記変換テーブルとを情報記録媒体に記録するデータ記録部と、

を有し、

前記パラメータ識別子は、

前記クリップ情報に含まれるコンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを適用した演算処理により算出可能な識別子である情報記録媒体製造装置にある。

【００１６】

さらに、本発明の情報記録媒体製造装置の一実施態様において、前記パラメータ識別子は、前記ＥＰマップ登録テーブルＩＤを適用した下記算出式、すなわち、

（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ

ただし、

ＳＰ＿ＩＤ：パラメータ識別子、

ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、

Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、

上記式に従って算出可能な識別子である。

【００１７】

さらに、本発明の第３の側面は、

情報記録媒体であり、

一部のコンテンツ構成データが置き換えられて再生されるコンテンツと、
コンテンツの再生区間情報を記録したクリップ情報と、
前記コンテンツ構成データを複数に区分して設定されたセグメント毎に異なるセグメント固有のパラメータ識別子と、置き換えられる一部のコンテンツ構成データの置き換え対象となる変換データとを対応させて登録した変換テーブルとを格納し、
前記変換データは前記パラメータ識別子に対応するセグメント固有のパラメータに基づき演算または暗号化処理を施したデータであり、
前記パラメータ識別子は、
前記クリップ情報に含まれるコンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを適用した演算処理により算出可能な識別子であり、
前記情報記録媒体の記録コンテンツを再生する情報処理装置において、
前記ＥＰマップ登録テーブルＩＤを適用した演算処理による前記セグメント固有のパラメータ識別子を算出処理と、前記セグメント固有のパラメータ識別子に基づくパラメータ算出処理と、算出パラメータに基づく演算または暗号化処理を伴うコンテンツ再生を実行させることを可能とした情報記録媒体にある。

【００１８】

さらに、本発明の情報記録媒体の一実施態様において、前記パラメータ識別子は、
前記ＥＰマップ登録テーブルＩＤを適用した下記算出式、すなわち、
（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ
ただし、
ＳＰ＿ＩＤ：パラメータ識別子、
ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、
Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、
上記式に従って算出可能な識別子である。

【００１９】

さらに、本発明の第４の側面は、
情報処理装置において、コンテンツ再生処理を実行する情報処理方法であり、
コンテンツ再生処理部において、
コンテンツ再生区間情報であるクリップ情報に含まれ、コンテンツ格納パケットのパケット識別情報を記録したＥＰマップに登録されたＥＰマップ登録テーブルの識別子であるＥＰマップ登録テーブルＩＤを取得し、
前記ＥＰマップ登録テーブルＩＤを適用した演算処理により、再生コンテンツの区分領域として設定されたセグメント毎に異なるパラメータ識別子を算出し、算出したパラメータ識別子を伴うパラメータ算出要求をパラメータ生成部に出力するステップと、
パラメータ生成部において、
前記コンテンツ再生部からのパラメータ算出要求に応じて、セグメント毎に異なるセグメント固有のパラメータを算出して前記コンテンツ再生部に提供するステップと、
前記コンテンツ再生処理部において、
再生対象となる入力コンテンツの構成データの一部を、変換テーブルに記録された変換データに置き換えるデータ変換処理を実行して再生コンテンツを生成する処理を実行するコンテンツ再生処理ステップであり、
前記変換テーブルに記録された変換テーブルデータに対して、前記パラメータ生成部から取得するセグメント固有のパラメータを適用した演算処理または暗号処理を実行し、該セグメントの構成データに対する置き換えデータとして適用される変換データを含むデータの復元処理を実行して再生コンテンツを生成するコンテンツ再生処理ステップを実行する情報処理方法にある。

【００２０】

さらに、本発明の情報処理方法の一実施態様において、前記パラメータ識別子は、前記ＥＰマップ登録テーブルＩＤに基づいて、下記算出式、すなわち、

（ＳＰ＿ＩＤ）＝（ＥＰ＿ｍａｐ＿ＩＤ）／Ｎ
ただし、
ＳＰ＿ＩＤ：パラメータ識別子、
ＥＰ＿ｍａｐ＿ＩＤ：ＥＰマップ登録テーブルＩＤ、
Ｎ：１セグメントに対応して設定されるＥＰマップ登録テーブル数、
上記式に従って算出可能な識別子である請求項９に記載の情報処理方法。

【００２１】

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。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００２２】

本発明の一実施例の構成によれば、本発明の一実施例の構成によれば、コンテンツの区分領域として設定されたセグメント毎に異なるパラメータによる演算または暗号処理によって変換データを復元、取得して、取得した変換データによって、コンテンツの一部データの置き換えを行いながらコンテンツ再生を実行する構成において、再生対象コンテンツのセグメントに含まれるパケットのＳＰＮ（ソースパケットナンバー）と、パラメータＩＤ（ＳＰ＿ＩＤ）を対応付けたテーブル、または、再生対象コンテンツのセグメントに含まれるパケットの情報を格納したＥＰマップの登録テーブル識別子（ＥＰマップ登録テーブルＩＤ）とパラメータＩＤを対応付けたテーブルに基づいて、セグメント対応のパラメータＩＤを取得して、取得したパラメータＩＤ（ＳＰ＿ＩＤ）をセキュアＶＭに通知して、シークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する構成としたので、各セグメントに対応するシークレットパラメータ（ＳＰ）を順次、セキュアＶＭから正確に受領して、正確なデータ変換を実行しながらコンテンツ再生を行なうことができる。

【００２３】

また、本発明の一実施例構成によれば、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、まず、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマップから、再生対象コンテンツデータに対応するＥＰマップを特定し、そのＥＰマップの登録テーブル識別子（ＥＰマップ登録テーブルＩＤ）に基づいて、パラメータＩＤ（ＳＰ＿ＩＤ）を、算出式を適用して求めるか、またはＥＰマップ登録テーブル数のカウントによって求め、取得したパラメータＩＤ（ＳＰ＿ＩＤ）をセキュアＶＭに通知して、シークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する構成としたので、特別なパラメータＩＤ特定テーブルを適用することなくパラメータＩＤ（ＳＰ＿ＩＤ）を取得して、各セグメントに対応するシークレットパラメータ（ＳＰ）を順次、セキュアＶＭから正確に受領して、正確なデータ変換を実行しながらコンテンツ再生を行なうことができる。

【図面の簡単な説明】

【００２４】

【図１】情報記録媒体の格納データおよびドライブ装置、情報処理装置の構成および処理について説明する図である。

【図２】情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットの設定例について説明する図である。

【図３】情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットとユニット鍵との対応について説明する図である。

【図４】情報記録媒体に記録されるコンテンツと、コンテンツ再生において必要となるデータ変換処理について説明する図である。

【図５】変換テーブルがコンテンツを含むトランスポートストリームパケット内に格納される場合のデータ構成について説明する図である。

【図６】情報記録媒体に格納されるコンテンツおよび変換テーブルの詳細について説明する図である。

【図７】変換テーブルに含まれる変換エントリのデータ構成を示す図である。
【図８】コンテンツを構成するＴＳパケット内の変換エントリを適用したデータ変換処理について説明する図である。
【図９】変換テーブル中の変換エントリを適用したデータ変換処理について説明する図である。
【図１０】再生（プレーヤ）アプリケーションと、セキュアＶＭとの間で実行される処理シーケンスについて説明する図である。
【図１１】再生（プレーヤ）アプリケーションと、セキュアＶＭ間の処理シーケンス中のタイトル初期化処理において実行される変換テーブルのコピー処理について説明する図である。
【図１２】セキュアＶＭにおける処理の受理、および拒否シーケンスについて説明する図である。
【図１３】コンテンツ再生処理の処理例について説明する図である。
【図１４】コンテンツ再生の際に実行するデータ変換処理について説明する図である。
【図１５】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例１の概要について説明する図である。
【図１６】ＥＰマップについて説明する図である。
【図１７】ＥＰマップについて説明する図である。
【図１８】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例１の処理シーケンスおよびＳＰ＿ＩＤ特定テーブルの構成例について説明する図である。
【図１９】変換テーブルの全体データ構成を示す図である。
【図２０】ＳＰ＿ＩＤ特定テーブルの構成例について説明する図である。
【図２１】変換テーブル内に含まれる変換テーブルボディのデータ構成を示す図である。
【図２２】変換テーブルボディ内に含まれる変換テーブルブロック（ＦＵＴブロック）のデータ構成を示す図である。
【図２３】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例１を適用した場合のコンテンツ再生シーケンスについて説明するフローチャートを示す図である。
【図２４】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例１を適用した場合の特殊再生におけるコンテンツ再生シーケンスについて説明するフローチャートを示す図である。
【図２５】処理例２におけるＳＰ＿ＩＤ特定テーブルの構成例について説明する図である。
【図２６】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例２を適用した場合のコンテンツ再生シーケンスについて説明するフローチャートを示す図である。
【図２７】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例２を適用した場合の特殊再生におけるコンテンツ再生シーケンスについて説明するフローチャートを示す図である。
【図２８】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例３の概要について説明する図である。
【図２９】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例３を適用した場合のコンテンツ再生シーケンスについて説明するフローチャートを示す図である。
【図３０】セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例３を適用した場合の特殊再生におけるコンテンツ再生シーケンスについて説明するフローチャートを示す図である。
【図３１】ホストとしてのアプリケーションを実行する情報処理装置のハードウェア構成例について説明する図である。
【発明を実施するための形態】
【００２５】
以下、図面を参照しながら本発明の情報処理装置、情報記録媒体製造装置、情報記録媒体、および方法の詳細について説明する。なお、説明は、以下の記載項目に従って行う。

１．情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要
２．コンテンツ管理ユニット（ＣＰＳユニット）について
３．変形データを含むコンテンツのデータ構成およびデータ変換処理の概要
４，再生（プレーヤ）アプリケーションとセキュアＶＭ間の処理
５．コンテンツ再生処理
６．セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理
（６．１）セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例１
（６．２）セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例２
（６．３）セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例３
７．情報処理装置の構成
８．情報記録媒体製造装置および情報記録媒体

【００２６】

［１．情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要］

まず、情報記録媒体の格納データと、ドライブおよびホストにおける処理の概要について説明する。図１に、コンテンツの格納された情報記録媒体１００、ドライブ１２０およびホスト１４０の構成を示す。ホスト１４０は、例えばＰＣ等の情報処理装置で実行されるデータ再生（または記録）アプリケーションであり、所定のデータ処理シーケンスに従ってＰＣ等の情報処理装置のハードウェアを利用した処理を行なう。

【００２７】

情報記録媒体１００は、例えば、Ｂｌｕ－ｒａｙディスク、ＤＶＤなどの情報記録媒体であり、正当なコンテンツ著作権、あるいは頒布権を持ついわゆるコンテンツ権利者の許可の下にディスク製造工場において製造された正当なコンテンツを格納した情報記録媒体（ＲＯＭディスクなど）、あるいはデータ記録可能な情報記録媒体（ＲＥディスクなど）である。なお、以下の実施例では、情報記録媒体の例としてディスク型の媒体を例として説明するが、本発明は様々な態様の情報記録媒体を用いた構成において適用可能である。

【００２８】

図１に示すように、情報記録媒体１００には、暗号化処理および一部データの置き換え処理の施された暗号化コンテンツ１０１と、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックとしてのＭＫＢ（Media Key Block）１０２、コンテンツ復号処理に適用するタイトル鍵を暗号化したデータ（Encrypted CPS Unit Key）等から構成されるタイトル鍵ファイル１０３、コンテンツのコピー・再生制御情報としてのＣＣＩ（Copy Control Information）等を含む使用許諾情報１０４、コンテンツ中の所定領域の置き換えデータに対応する変換データを登録した変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５の登録データによるデータ変換処理を実行するための処理命令を含むデータ変換処理プログラム１０６が格納されている。なお、図に示すデータ例は一例であり、格納データは、ディスクの種類などによって多少異なる。以下、これらの各種情報の概要について説明する。

【００２９】

（１）暗号化コンテンツ１０１

情報記録媒体１００には、様々なコンテンツが格納される。例えば高精細動画像データであるＨＤ（High Definition）ムービーコンテンツなどの動画コンテンツのＡＶ(Audio Visual)ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツである。これらのコンテンツは、特定のＡＶフォーマット規格データであり、特定のＡＶデータフォーマットに従って格納される。具体的には、例えばＢｌｕ－ｒａｙディスクＲＯＭ規格データとして、Ｂｌｕ－ｒａｙディスクＲＯＭ規格フォーマットに従って格納される。

【００３０】

さらに、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどが格納される場合もある。これらのコンテンツは、特定のＡＶデ

ータフォーマットに従わないデータフォーマットを持つデータとして格納される場合もある。

【００３１】

コンテンツの種類としては、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなど、様々なコンテンツが含まれ、これらのコンテンツには、情報記録媒体１００からのデータのみによって利用可能なコンテンツ情報と、情報記録媒体１００からのデータと、ネットワーク接続されたサーバから提供されるデータとを併せて利用可能となるコンテンツ情報など、様々な態様の情報が含まれる。情報記録媒体に格納されるコンテンツは、区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵（ＣＰＳユニット鍵またはユニット鍵（あるいはタイトル鍵と呼ぶ場合もある））が割り当てられ暗号化されて格納される。１つのユニット鍵を割り当てる単位をコンテンツ管理ユニット（ＣＰＳユニット）と呼ぶ。さらに、コンテンツは、構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデータとして設定され、復号処理のみでは正しいコンテンツ再生が実行されず、再生を行なう場合は、ブロークンデータを変換テーブルに登録されたデータに置き換える処理が必要となる。これらの処理は後段で詳細に説明する。

【００３２】

（２）ＭＫＢ

ＭＫＢ（Media Key Block）１０２は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。ＭＫＢ１０２は有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式を適用したものであり、ユーザデバイス（情報処理装置）が有効なライセンスを持つ場合にのみ、メディア鍵［Ｋｍ］の取得を可能とし、無効化（リボーク処理）されたユーザデバイスにおいては、メディア鍵［Ｋｍ］の取得が不可能となる。

【００３３】

ライセンスエンティティとしての管理センタはＭＫＢに格納する鍵情報の暗号化に用いるデバイス鍵の変更により、特定のユーザデバイスに格納されたデバイス鍵では復号できない、すなわちコンテンツ復号に必要なメディア鍵を取得できない構成を持つＭＫＢを生成することができる。従って、任意タイミングで不正デバイスを排除（リボーク）して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。コンテンツの復号処理については後述する。

【００３４】

（３）タイトル鍵ファイル

前述したように各コンテンツまたは複数コンテンツの集合は、コンテンツの利用管理のため、各々、個別の暗号鍵（タイトル鍵（ＣＰＳユニット鍵））を適用した暗号化がなされて情報記録媒体１００に格納される。すなわち、コンテンツを構成するＡＶ(Audio Visual)ストリーム、音楽データ、動画、静止画等の画像データ、ゲームプログラム、ＷＥＢコンテンツなどは、コンテンツ利用の管理単位としてのユニットに区分され、区分されたユニット毎に異なるタイトル鍵を生成して、復号処理を行なうことが必要となる。このタイトル鍵を生成するための情報がタイトル鍵データであり、例えばメディア鍵等によって生成された鍵で暗号化タイトル鍵を復号することによってタイトル鍵を得る。タイトル鍵データを適用した所定の暗号鍵生成シーケンスに従って、各ユニット対応のタイトル鍵が生成され、コンテンツの復号が実行される。

【００３５】

（４）使用許諾情報

使用許諾情報には、例えばコピー・再生制御情報（ＣＣＩ）が含まれる。すなわち、情報記録媒体１００に格納された暗号化コンテンツ１０１に対応する利用制御のためのコピー制限情報や、再生制限情報である。このコピー・再生制御情報（ＣＣＩ）は、コンテン

ツ管理ユニットとして設定されるＣＰＳユニット個別の情報として設定される場合や、複数のＣＰＳユニットに対応して設定される場合など、様々な設定が可能である。

【００３６】

（５）変換テーブル

前述したように、情報記録媒体１００に格納された暗号化コンテンツ１０１は、所定の暗号化が施されているとともに、コンテンツ構成データの一部が、正しいデータと異なるブロークンデータによって構成されている。コンテンツ再生に際しては、このブロークンデータを正しいコンテンツデータである変換データに置き換えるデータ上書き処理が必要となる。この変換データを登録したテーブルが変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５である。ブロークンデータはコンテンツ中に散在して多数設定され、コンテンツ再生に際しては、これらの複数のブロークンデータを変換テーブルに登録された変換データに置き換える（上書き）する処理が必要となる。この変換データを適用することにより、例えば、暗号鍵が漏洩しコンテンツの復号が不正に行なわれた場合であっても、コンテンツの復号のみでは、置き換えデータの存在によって正しいコンテンツの再生が不可能となり、不正なコンテンツ利用を防止することができる。

【００３７】

なお、変換テーブル１０５には、通常の変換データに加え、コンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報の構成ビットを解析可能としたデータを含む変換データが含まれる。具体的には、例えば、プレーヤ（ホストアプリケーションを実行する装置）の識別データとしてのプレーヤＩＤあるいはプレーヤＩＤに基づいて生成された識別情報が記録された「識別マークを含む変換データ」が含まれる。識別マークを含む変換データは、コンテンツの再生に影響を与えないレベルで、正しいコンテンツデータのビット値をわずかに変更したデータである。これらの変換データを利用した処理についての詳細は、後段で説明する。

【００３８】

なお、図１には、変換テーブル１０５を独立したデータファイルとして設定した例を示しているが、変換テーブルを独立ファイルとせずに、暗号化コンテンツ１０１の構成パケット中に散在させて含ませる構成としてもよい。これらの構成および処理については後段で説明する。

【００３９】

（６）データ変換処理プログラム

データ変換処理プログラム１０６は、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５の登録データによるデータ変換処理を実行するための処理命令を含むプログラムであり、コンテンツ再生を実行するホストによって利用される。図１におけるホスト１００のデータ変換処理部１５４において実行される。なお、上述した変換テーブル１０５は、データ変換処理プログラム１０６に含まれるデータとして設定してもよい。

【００４０】

ホストでは、データ変換処理を実行するバーチャルマシン（ＶＭ）を設定し、バーチャルマシン（ＶＭ）において、情報記録媒体１００から読み出したデータ変換処理プログラム１０６を実行して、変換テーブル（Ｆｉｘ－ｕｐ　Ｔａｂｌｅ）１０５の登録エントリを適用して、復号コンテンツに対して、その一部構成データのデータ変換処理を実行する。これらの処理の詳細については後述する。

【００４１】

次に、ホスト１４０とドライブ１２０の構成、処理の概要について、図１を参照して説明する。情報記録媒体１００に格納されたコンテンツの再生処理は、ドライブ１２０を介してホスト１４０にデータが転送されて実行される。

【００４２】

ホスト１４０には、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０が設定される。再生（プレーヤ）アプリケーション１５０は、コンテンツ再生処理部であり、コンテンツ再生処理において実行するドライブとの認証処理、コンテンツ復号、デコ

ード処理などの処理を実行する。セキュアＶＭ１６０は、例えば、コンテンツ再生処理部である再生（プレーヤ）アプリケーション１５０の実行するコンテンツ再生処理において実行するデータ変換処理において適用するパラメータを提供するパラメータ生成部として機能する。セキュアＶＭ１６０は、ホスト１４０内にバーチャルマシンとして設定される。バーチャルマシン（ＶＭ）は中間言語を直接解釈して実行する仮想コンピュータであり、プラットホームに依存しない中間言語での命令コード情報を情報記録媒体１００から読み出して解釈実行する。

【００４３】

再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間の情報伝達、あるいは処理要求は、再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理のシーケンスによって実行される。アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理のシーケンスによって、コンテンツ再生処理において実行するデータ変換処理において適用するパラメータの算出要求、およびパラメータ提供が行われる。これらの処理シーケンスの詳細については後段で説明する。

【００４４】

ホスト１４０の実行する主な処理について説明する。コンテンツの利用に先立ち、ドライブ１２０と、ホスト１４０間では相互認証処理が実行され、この認証処理の成立によって双方の正当性が確認された後、ドライブからホストに暗号化コンテンツが転送され、ホスト側でコンテンツの復号処理が行なわれ、さらに上述の変換テーブルによるデータ変換処理が実行されてコンテンツ再生が行なわれる。

【００４５】

ホスト１４０と、ドライブ１２０間において実行する相互認証においては、各機器またはアプリケーションが不正な機器またはアプリケーションとして登録されていないかを示す管理センタの発行したリボケーション（無効化）リストを参照して、正当性を判定する処理を実行する。

【００４６】

ドライブ１２０は、ホストの証明書（公開鍵証明書）のリボーク（無効化）情報を格納したホストＣＲＬ（Certificate Revocation List）を格納するためのメモリ１２２を有する。一方、ホスト１４０は、ドライブの証明書（公開鍵証明書）のリボーク（無効化）情報を格納したドライブＣＲＬ（Certificate Revocation List）を格納するためのメモリ１５２を有する。メモリは不揮発性メモリ（ＮＶＲＡＭ）であり、例えば、情報記録媒体１００から読み出されるＣＲＬがより新しいバージョンである場合には、それぞれのデータ処理部１２１，１５１は、メモリ１２２．１５２に新しいバージョンのホストＣＲＬまたはドライブＣＲＬを格納する更新処理を行なう。

【００４７】

ホストＣＲＬ、ドライブＣＲＬ等のＣＲＬは管理センタが逐次更新する。すなわち新たな不正機器が発覚した場合、その不正機器に対して発行された証明書のＩＤまたは機器ＩＤなどを新規エントリとし追加した更新ＣＲＬを発行する。各ＣＲＬにはバージョン番号が付与されており、新旧比較が可能な構成となっている。例えばドライブが装着した情報記録媒体から読み出されたＣＲＬが、ドライブ内のメモリ１２２に格納されたＣＲＬより新しい場合、ドライブは、ＣＲＬの更新処理を実行する。ホスト１４０も同様に、ドライブＣＲＬの更新を実行する。

【００４８】

ドライブ１２０のデータ処理部１２１は、このＣＲＬの更新処理の他、コンテンツ利用に際して実行されるホストとの認証処理、さらに、情報記録媒体からのデータ読み出し、ホストへのデータ転送処理などを実行する。

【００４９】

ホスト１４０の再生（プレーや）アプリケーション１５０は、例えばＰＣ等の情報処理装置で実行されるデータ再生（または記録）アプリケーションであり、所定のデータ処理シーケンスに従ってＰＣ等の情報処理装置のハードウェアを利用した処理を行なう。

【００５０】

ホスト１４０は、ドライブ１２０との相互認証処理や、データ転送制御などを実行するデータ処理部１５１、暗号化コンテンツの復号処理を実行する復号処理部１５３、前述の変換テーブル１０５の登録データに基づくデータ変換処理を実行するデータ変換処理部１５４、デコード（例えばＭＰＥＧデコード）処理を実行するデコード処理部１５５を有する。

【００５１】

データ処理部１５１は、ホスト－ドライブ間の認証処理を実行し、認証処理においては、不揮発性メモリ（ＮＶＲＡＭ）としてのメモリａ１５２に格納されたドライブＣＲＬを参照して、ドライブがリボークされたドライブでないことを確認する。ホストも、また、メモリａ１５２に新しいバージョンのドライブＣＲＬを格納する更新処理を行なう。

【００５２】

復号処理部１５３では、メモリｂ１５６に格納された各種情報、および、情報記録媒体１００からの読み取りデータを適用して、コンテンツの復号に適用する鍵を生成し、暗号化コンテンツ１０１の復号処理を実行する。データ変換処理部１５４は、情報記録媒体１００から取得されるデータ変換処理プログラムに従って、情報記録媒体１００から取得される変換テーブルに登録された変換データを適用してコンテンツの構成データの置き換え処理（上書き）を実行する。デコード処理部１５５は、デコード（例えばＭＰＥＧデコード）処理を実行する。

【００５３】

情報処理装置１５０のメモリｂ１５６には、デバイス鍵：Ｋｄや、相互認証処理に適用する鍵情報や復号に適用する鍵情報などが格納される。なお、コンテンツの復号処理の詳細については後述する。デバイス鍵：Ｋｄは、先に説明したＭＫＢの処理に適用する鍵である。ＭＫＢは有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵［Ｋｄ］に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵［Ｋｍ］の取得を可能とした鍵情報ブロックであり、暗号化コンテンツの復号に際して、情報処理装置１５０は、メモリｂ１５６に格納されたデバイス鍵：Ｋｄを適用してＭＫＢの処理を実行することになる。なお、コンテンツの復号処理の詳細については後述する。

【００５４】

［２．コンテンツ管理ユニット（ＣＰＳユニット）について］

前述したように、情報記録媒体に格納されるコンテンツは、ユニット毎の異なる利用制御を実現するため、ユニット毎に異なる鍵が割り当てられ暗号化処理がなされて格納される。すなわち、コンテンツはコンテンツ管理ユニット（ＣＰＳユニット）に区分されて、個別の暗号化処理がなされ、個別の利用管理がなされる。

【００５５】

コンテンツ利用に際しては、まず、各ユニットに割り当てられたＣＰＳユニット鍵（タイトル鍵とも呼ばれる）を取得することが必要であり、さらに、その他の必要な鍵、鍵生成情報等を適用して予め定められた復号処理シーケンスに基づくデータ処理を実行して再生を行う。コンテンツ管理ユニット（ＣＰＳユニット）の設定態様について、図２を参照して説明する。

【００５６】

図２に示すように、コンテンツは、（Ａ）インデックス２１０、（Ｂ）ムービーオブジェクト２２０、（Ｃ）プレイリスト２３０、（Ｄ）クリップ２４０の階層構成を有する。再生アプリケーションによってアクセスされるタイトルなどのインデックスを指定すると、例えばタイトルに関連付けられた再生プログラムが指定され、指定された再生プログラムのプログラム情報に従ってコンテンツの再生順等を規定したプレイリストが選択される

。
【００５７】
プレイリストには、再生対象データ情報としてのプレイアイテムが含まれる。プレイリストに含まれるプレイアイテムによって規定される再生区間としてのクリップ情報によって、コンテンツ実データとしてのＡＶストリームあるいはコマンドが選択的に読み出されて、ＡＶストリームの再生、コマンドの実行処理が行われる。なお、プレイリスト、プレイアイテムは多数、存在し、それぞれに識別情報としてのプレイリストＩＤ、プレイアイテムＩＤが対応付けられている。
【００５８】
図２には、２つのＣＰＳユニットを示している。これらは、情報記録媒体に格納されたコンテンツの一部を構成している。ＣＰＳユニット１，２７１、ＣＰＳユニット２，２７２の各々は、インデックスとしてのタイトルと、再生プログラムファイルとしてのムービーオブジェクトと、プレイリストと、コンテンツ実データとしてのＡＶストリームファイルを含むクリップを含むユニットとして設定されたＣＰＳユニットである。
【００５９】
コンテンツ管理ユニット（ＣＰＳユニット）１，２７１には、タイトル１，２１１とタイトル２，２１２、再生プログラム２２１，２２２、プレイリスト２３１，２３２、クリップ２４１、クリップ２４２が含まれ、これらの２つのクリップ２４１，２４２に含まれるコンテンツの実データであるＡＶストリームデータファイル２６１，２６２が、少なくとも暗号化対象データであり、原則的にコンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定される暗号鍵であるタイトル鍵（Ｋｔ１）（ＣＰＳユニット鍵とも呼ばれる）を適用して暗号化されたデータとして設定される。
【００６０】
コンテンツ管理ユニット（ＣＰＳユニット）２，２７２には、インデックスとしてアプリケーション１，２１３、再生プログラム２２４、プレイリスト２３３、クリップ２４３が含まれ、クリップ２４３に含まれるコンテンツの実データであるＡＶストリームデータファイル２６３がコンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定される暗号鍵である暗号鍵であるタイトル鍵（Ｋｔ２）適用して暗号化される。
【００６１】
例えば、ユーザがコンテンツ管理ユニット１，２７１に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）１，２７１に対応付けて設定された暗号鍵としてのタイトル鍵：Ｋｔ１を取得して復号処理を実行することが必要となる。コンテンツ管理ユニット２，２７２に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット（ＣＰＳユニット）２，２７２に対応付けて設定された暗号鍵としてのタイトル鍵：Ｋｔ２を取得して復号処理を実行することが必要となる。
【００６２】
ＣＰＳユニットの設定構成、およびタイトル鍵の対応例を図３に示す。図３には、情報記録媒体に格納される暗号化コンテンツの利用管理単位としてのＣＰＳユニット設定単位と、各ＣＰＳユニットに適用するタイトル鍵（ＣＰＳユニット鍵）の対応を示している。なお、予め後発データ用のＣＰＳユニットおよびタイトル鍵を格納して設定しておくことも可能である。例えばデータ部２８１が後発データ用のエントリである。
【００６３】
ＣＰＳユニット設定単位は、コンテンツのタイトル、アプリケーション、データグループなど、様々であり、ＣＰＳユニット管理テーブルには、それぞれのＣＰＳユニットに対応する識別子としてのＣＰＳユニットＩＤが設定される。
【００６４】
図３において、例えばタイトル１はＣＰＳユニット１であり、ＣＰＳユニット１に属する暗号化コンテンツの復号に際しては、タイトル鍵Ｋｔ１を生成し、生成したタイトル鍵Ｋｔ１に基づく復号処理を行なうことが必用となる。

【００６５】
このように、情報記録媒体１００に格納されるコンテンツは、ユニット毎の異なる利用制御を実現するため、ユニット毎に異なる鍵が割り当てられ暗号化処理がなされて格納される。各コンテンツ管理ユニット（ＣＰＳユニット）に対する個別の利用管理のために、各コンテンツ管理ユニット（ＣＰＳユニット）に対する使用許諾情報（ＵＲ：Ｕｓａｇｅ Ｒｕｌｅ）が設定されている。使用許諾情報は、前述したように、コンテンツに対する例えばコピー・再生制御情報（ＣＣＩ）を含む情報であり、各コンテンツ管理ユニット（ＣＰＳユニット）に含まれる暗号化コンテンツのコピー制限情報や、再生制限情報である。
【００６６】
なお、タイトル鍵の生成には、情報記録媒体に格納された様々な情報を適用したデータ処理が必要となる。これらの処理の具体例についは、後段で詳細に説明する。
【００６７】
［３．変形データを含むコンテンツのデータ構成およびデータ変換処理の概要］
次に、変形データを含むコンテンツの構成およびデータ変換処理の概要について説明する。情報記録媒体１００に含まれる暗号化コンテンツ１０１は、前述したように、構成データの一部が、正しいコンテンツデータと異なるデータによって置き換えられたブロークンデータとして設定され、復号処理のみでは正しいコンテンツ再生が実行されず、再生を行なう場合は、ブロークンデータを変換テーブルに登録された変換データに置き換える処理が必要となる。
【００６８】
図４を参照して、情報記録媒体に格納されるコンテンツの構成および再生処理の概要について説明する。情報記録媒体１００には例えば映画などのＡＶ（Audio Visual）コンテンツが格納される。これらのコンテンツは暗号化が施され、所定のライランスを持つ再生装置においてのみ取得可能な暗号鍵を適用した処理によって復号の後、コンテンツ再生が可能となる。具体的なコンテンツ再生処理については後段で説明する。情報記録媒体１００に格納されるコンテンツは、暗号化のみならず、コンテンツの構成データが変形データによって置き換えられた構成を持つ。
【００６９】
図４には、情報記録媒体１００に格納される記録コンテンツ２９１の構成例を示している。記録コンテンツ２９１は変形のされていない正常なコンテンツデータ２９２と、変形が加えられ破壊されたコンテンツであるブロークンデータ２９３によって構成される。ブロークンデータ２９３は、本来のコンテンツに対してデータ処理によって破壊が施されたデータである。従って、このブロークンデータを含むコンテンツ２９１を適用して正常なコンテンツ再生は実行できない。
【００７０】
コンテンツ再生を行なうためには、記録コンテンツ２９１に含まれるブロークンデータ２９３を正常なコンテンツデータに置き換える処理を行なって再生コンテンツ２９６を生成することが必要となる。各ブロークンデータ領域に対応する正常なコンテンツデータとしての変換用のデータ（変換データ）は、情報記録媒体１００に記録された変換テーブル（ＦＵＴ(Fix-Up Table)）１０５（図１参照）に登録された変換データ２９５を取得して、ブロークンデータ領域のデータを置き換える処理を実行して、再生コンテンツ２９６を生成して再生を実行する。変換テーブルの具体例、変換テーブルを利用した再生処理の詳細については後述する。
【００７１】
なお、再生コンテンツ２９６の生成に際しては、ブロークンデータ２９３を正常なコンテンツデータとしての変換データ２９７に置き換える処理に加え、記録コンテンツ２９１の一部領域を、コンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報（例えばプレーヤＩＤ）の構成ビットを解析可能としたデータを含む識別子設定変換データ２９８によって置き換える処理を行なう。例えば、不正にコピーされたコ

ンテンツが流出した場合、流出コンテンツ中の識別子設定変換データ２９８の解析によって、不正コンテンツの流出源を特定することが可能となる。

【００７２】

なお、変換データを格納した変換テーブルは、コンテンツと別ファイルとして設定して情報記録媒体に記録される。さらに、変換データを含む変換テーブルの一部データは、コンテンツの構成データ中の特定パケットに分散して記録される。すなわち、変換データは、図１に示す変換テーブル１０６に格納されるとともに、暗号化コンテンツ１０１にも分散記録され、重複して記録される。コンテンツ再生を実行する情報処理装置は、変換テーブル１０６に格納された変換データを取得してデータ置き換えを実行するか、あるいはコンテンツに分散は記録された変換ントリを取得してデータ置き換えを実行するかのいずれかの処理を行なう。

【００７３】

コンテンツの構成データ中の特定パケットに分散して変換データを含む変換テーブルの構成データである変換テーブルブロックを記録する構成とする場合は、例えば図５に示すような設定で変換テーブルブロックの構成データをコンテンツを含むトランスポートストリームパケット内に格納する。図５（ａ）にコンテンツデータの構成を示す。このコンテンツ構成は、復号されたトランスポートストリーム（ＴＳ）パケットからなるコンテンツデータを示している。トランスポートストリームは、所定バイト数のＴＳ（トランスポートストリーム）パケットから構成されている。これらのＴＳパケットの一部の複数パケットに、変換データを含む変換テーブルブロックの構成データが分割記録される。例えば、図に示すＴＳパケット３０７に記録される。変換テーブルブロックを格納するＴＳパケットとしては、例えばコンテンツ中に分散して設定されるＰＭＴ（プログラムマップテーブル）を含むＴＳパケットなどが利用される。

【００７４】

変換テーブルブロックには、復号コンテンツに対して置き換え処理を行なう変換データ（または識別子設定変換データ）とその変換データの記録位置が記録されている。記録位置情報としては、例えば、図５（ｂ）に示すように複数の記録位置がある場合、１つ目の変形パケットの位置は、変換テーブルブロックの構成データとしての変換エントリを含むＴＳパケット３０７からのオフセット、２つ目のパケットの変形パケットの位置は、最初の変形パケット３０８から後の変形パケット３０９への相対パケット位置を示すオフセット位置を記録する。

【００７５】

各変換テーブルブロックに記録された変換データは、例えば図５（ｂ）に示すように、各変換テーブルブロックの構成データとしての変換エントリを含むＴＳパケットの近傍位置に記録位置が設定される。

【００７６】

例えば、図５（ｂ）に示す例では、変換データの記録領域を持つパケット３０８，３０９は、変換テーブルブロックの構成データとしての変換エントリを含むパケット３０７の近傍に設定される。このような設定とすることで、コンテンツの復号、再生をリアルタイムで実行する場合、変換データによるデータ置き換え処理を復号処理後の連続処理として実行することが可能であり、変換テーブルの記録されたＴＳパケットの検出、解析処理によって、変換データを取得し、テーブルに記録された位置に対して変換データを書き込む（上書き）処理を効率的に実行することができる。

【００７７】

図６を参照して、情報記録媒体１００に格納されるデータ変換処理プログラム３００、変換テーブル（ＦＵＴ：Ｆｉｘ－Ｕｐ　Ｔａｂｌｅ）３０１、暗号化コンテンツ３０６の構成例について説明する。情報記録媒体１００に記録される変換テーブル３０１は、図６に示すように、シークレットパラメータＩＤ特定テーブル３０２と、変換テーブルボディ３０３ａを含む構成を持つ。

【００７８】

変換テーブルボディ３０３ａは、クリップ毎の変換テーブル集合３０３ｂとして設定され、各クリップ単位の変換テーブルは、複数の変換テーブルブロック１～Ｋ３０４によって構成され、さらに、各変換テーブルブロックは、複数の変換エントリ３０５を含む構成を持つ。これらの変換エントリの各々には、置き換えデータとして適用される変換データと変換データの記録位置情報が含まれる。

【００７９】

図７は、変換テーブブロックに含まれる１つの変換エントリ（FixUpEntry）のデータ構成例を示している。図７に示すように、変換エントリ（FixUpEntry）には以下のデータが含まれる。

type_indicator：タイプ識別子[00:変換なし，01b:変換データによる処理，10b,11b:識別子設定変換データによる処理]

FM_ID_bit_position：識別子設定変換データに対応するプレーヤＩＤの識別ビット位置

relative_SPN：変換データ適用パケット位置（プログラマブルマップテーブル（ＰＭＴ）格納パケットからのパケット数）

byte_position：パケット内の変換データ記録位置

overwrite_value：変換データ（識別子設定変換データも含む）

relative_SPN_2：第２変換データ適用パケット位置（ＰＭＴパケットからのパケット数）

byte_position_2：パケット内の変換データ記録位置（第２変換データ対応）

overwrite_value_2：第２変換データ（識別子設定変換データも含む）

これらのデータによって構成される。

【００８０】

変換テーブルは、コンテンツデータの一部の置き換え対象となる変換データと、該変換データのコンテンツに対する設定位置情報を記録した変換テーブルとして設定され、この変換テーブルを適用して、コンテンツ構成データの置き換え処理実行命令を含むデータ変換処理プログラムを実行して、データ変換が行われる。

【００８１】

図７に示す変換テーブブロックに含まれる変換エントリ（FixUpEntry）情報に含まれる情報［type_indicator］は、変換テーブルの登録情報が、

（ａ）ブロークンデータを正当なコンテンツデータに変換するための変換データに関する登録情報であるか、または、

（ｂ）再生装置又はコンテンツ再生アプリケーションの識別情報を埋めこむための識別子設定変換データに関する登録情報であるか、

上記（ａ）、（ｂ）のいずれの登録情報であるかを識別するタイプ識別子である。

【００８２】

変換テーブルの登録情報領域が、再生装置又はコンテンツ再生アプリケーションの識別情報を埋めこむための識別子設定変換データに関する登録情報領域である場合には、テーブル登録情報として、コンテンツ再生装置またはコンテンツ再生アプリケーションの識別情報に基づいて選択的に適用する変換データ、すなわち、識別子設定変換データが登録される。

【００８３】

登録情報［FM_ID_bit_position］は、複数ビットからなる再生装置又は再生アプリケーションの識別情報中、処理態様決定のために参照すべきビットの位置情報である。例えば、複数ビットからなる再生装置又は再生アプリケーションの識別情報中、処理態様決定のために参照すべきビットのビット値が１である場合、変換テーブルに登録された識別子設定変換データによってコンテンツ構成データの置き換えを実行し、参照すべきビットのビット値が０である場合には置き換えを実行しないといった処理態様が決定されてデータ変換が実行される。

【００８４】

なお、参照ビットが０の場合に変換を実行し、１の場合に変換を実行しないとする設定

も可能である。また参照ビットが０の場合の変換データと、１の場合の変換データをそれぞれ別の変換データとして設定し、参照ビットのビット値に応じて、適宜、変換データを選択して設定する構成としてもよい。

【００８５】

図６に示すように、暗号化コンテンツ３０６は、ＴＳパケットのストリームとして設定され、その一部に変換エントリが散在して格納されたパケット、すなわち変換エントリ格納パケット３０７ａ～３０７ｄが設定される。ＡＶストリームは、クリップ単位で区分され、クリップ単位の変換エントリが、コンテンツ中に分散記録される。

【００８６】

これらの分散記録データとして設定される各変換エントリには、図５を参照して説明したように、近傍の変換データが記録されている。暗号化コンテンツ３０６に分散記録された変換エントリと、変換テーブル３０１に含まれる変換エントリは同じものであり、コンテンツ再生を実行する情報処理装置は、再生（プレーヤ）アプリケーションの仕様に応じて、コンテンツに分散記録された変換エントリから変換データを取得してデータ置き換えを実行するか、あるいは、変換テーブル３０１中の変換エントリから変換データを取得してデータ置き換えを実行するかいずれか一方の処理を実行する。

【００８７】

コンテンツは、図６に示すように、所定データ単位ごとのセグメントとして区分されている。各変換データを含む変換エントリは、コンテンツの所定データ単位（セグメント単位）ごとに異なるパラメータ（ＳＰ：シークレットパラメータ）を適用した演算または暗号化処理が実行されている。

【００８８】

コンテンツ再生の際に実行するデータの置き換え処理としてのデータ変換処理を実行する情報処理装置は、各セグメントに対応するシークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）順次、取得して、各セグメント位置に対応する変換データを含む変換テーブルブロックに対して、取得パラメータ（ＳＰｎ）を適用した演算または暗号処理を実行して、変換データを取得する処理を行なう。

【００８９】

図６に示すシークレットパラメータ（ＳＰ）ＩＤ特定テーブル３０２は、どのコンテンツデータ位置にどのシークレットパラメータを適用すべきかのガイド情報を記録したテーブルである。このテーブルの詳細、および使用例については、後段で説明する。

【００９０】

図８、図９を参照して、変換データに基づくデータ置き換えの具体例について説明する。まず、図８を参照して、コンテンツに分散記録された変換データを含む変換テーブルブロック構成データを取得して、データ置き換えを実行する処理例について説明する。

【００９１】

図８（ａ）は、情報記録媒体１００に記録されたコンテンツ構成を示している。変換エントリを含む変換テーブルブロックの構成データが図に示すＴＳパケット３０７ａ～ｄに分散記録されている。

【００９２】

データ置き換え処理シーケンスについて、図８（ｂ）を参照して説明する。図８（ｂ）に示す処理は、ホストの再生（プレーヤ）アプリケーションの実行する処理である。図８（ｂ）には、コンテンツ構成データ中の、セグメントＩＤ＝Ｎ，Ｎ＋１に属するコンテンツのＴＳパケット列の一部を示している。

【００９３】

例えば、セグメントＩＤ＝Ｎに記録された変換エントリを含むパケット３１１には、シークレットパラメータ（ＳＰｘ）と排他論理和演算された結果データとしてのＸＯＲｅｄ変換エントリ３１５が格納されている。データ置き換え処理を実行するホストの再生（プレーヤ）アプリケーションは、ＸＯＲｅｄ変換エントリ３１５に対して、シークレットパラメータ（ＳＰｘ）３１６との排他論理和演算を実行して変換エントリ３１７を取得して

、変換エントリ３１７から変換データと記録位置情報を取得し、データ置き換え対象位置のパケット３１２ａ，ｂとの置き換え処理を実行する。

【００９４】

変換エントリ３１７を取得するための演算に適用するパラメータ（ＳＰｘ）は、セキュアＶＭ３２０から供給を受ける。例えば、再生（プレーヤ）アプリケーションは、コンテンツの各セグメントにおいて必要なシークレットパラメータ（ＳＰｎ）を取得するため、各セグメントに対応するシークレットパラメータ指定情報としてのシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得して、シークレットパラメータＩＤの通知を含むシークレットパラメータ算出要求を、セキュアＶＭに対する割り込み（ＩＮＴＲＰ）要求として出力する。セキュアＶＭは、再生（プレーヤ）アプリケーションからのシークレットパラメータ算出要求に応じて、ＳＰ＿ＩＤ対応のシークレットパラメータ（ＳＰｘ）を算出し、応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーションに提供する。

【００９５】

図８に示すように、セグメントが異なると、変換エントリを取得するための演算に適用するパラメータ（ＳＰｘ）は異なるパラメータとなる。例えば、１つのセグメントはコンテンツ再生時間として約１０秒程度に設定され、再生（プレーヤ）アプリケーションは、約１０秒の各セグメント毎に異なるパラメータをセキュアＶＭから受領して、変換エントリを復元して、復元した変換エントリから変換データを取得し、データ置き換え処理を実行する。

【００９６】

図９に、コンテンツ中に分散記録された変換テーブルブロックではなく、独立した変換テーブルブロックファイルとしての１クリップ分の変換テーブル３０３ｂから、ＸＯＲｅｄ変換エントリを取得して、演算または暗号処理を実行して、変換エントリを復元して、復元した変換エントリから変換データを抽出してデータ置き換えを行なう場合の処理例を示す。

【００９７】

図９（ａ）は、情報記録媒体１００に記録されたコンテンツ構成を示している。変換データを含む変換エントリが図に示すＴＳパケット３０７ａ～ｄに分散記録されているが、本例では、これらのデータは使用せず、情報記録媒体に独立に記録された変換テーブルの構成データとしての１クリップ分の変換テーブル３０３ｂを使用し、この１クリップ分の変換テーブル３０３ｂに格納された変換エントリを適用してデータ置き換えを実行する。

【００９８】

データ置き換え処理シーケンスについて、図９（ｂ）を参照して説明する。図９（ｂ）に示す処理は、ホストの再生（プレーヤ）アプリケーションの実行する処理である。図９（ｂ）には、コンテンツ構成データ中の、セグメントＩＤ＝Ｎ，Ｎ＋１に属するコンテンツのＴＳパケット列の一部を示している。

【００９９】

例えば、セグメントＩＤ＝Ｎについてのデータ置き換えを実行する場合、１クリップ分の変換テーブル３０３ｂに含まれるセグメントＩＤ＝Ｎに対応する変換エントリを取得する。しかし、この変換エントリｘ３１５は、コンテンツ中に分散記録された変換テーブルブロックと同様、シークレットパラメータ（ＳＰｘ）と排他論理和演算された結果データとしてのＸＯＲｅｄ変換エントリ３１５である。データ置き換え処理を実行するホストの再生（プレーヤ）アプリケーションは、ＸＯＲｅｄ変換エントリ３１５に対して、シークレットパラメータ（ＳＰｘ）３１６との排他論理和演算を実行して変換エントリ３１７を取得して、変換エントリ３１７から変換データと記録位置情報を取得し、データ置き換え対象位置のパケット３１２ａ，ｂとの置き換え処理を実行する。

【０１００】

変換エントリ３１７を取得するための演算に適用するパラメータ（ＳＰｘ）は、先に説明した処理例と、同様セキュアＶＭ３２０から供給を受ける。例えば、再生（プレーヤ）アプリケーションは、コンテンツの各セグメントにおいて必要なシークレットパラメータ

（ＳＰｎ）を取得するため、各セグメントに対応するシークレットパラメータ指定情報としてのシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得して、シークレットパラメータＩＤの通知を含むシークレットパラメータ算出要求を、セキュアＶＭに対する割り込み（ＩＮＴＲＰ）要求として出力する。セキュアＶＭは、再生（プレーヤ）アプリケーションからのシークレットパラメータ算出要求に応じて、ＳＰ＿ＩＤ対応のシークレットパラメータ（ＳＰｘ）を算出し、応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーションに提供する。

【０１０１】

図９に示すように、セグメントが異なると、変換エントリを取得するための演算に適用するパラメータ（ＳＰｘ）は異なるパラメータとなる。例えば、１つのセグメントはコンテンツ再生時間として約１０秒程度に設定され、再生（プレーヤ）アプリケーションは、約１０秒の各セグメント毎に異なるパラメータをセキュアＶＭから受領して、変換エントリを復元して、復元した変換エントリから変換データを取得し、データ置き換え処理を実行する。

【０１０２】

このように、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、各セグメント単位で、セキュアＶＭからシークレットパラメータを受領して、演算を実行して、変換テーブルブロックの構成データとしてり変換エントリの復元を実行し、復元した変換エントリを取得してデータ置き換えを行なう。なお、上述の処理例では、シークレットパラメータを適用した演算として排他論理和（ＸＯＲ）を例示したが、その他の演算処理を適用する設定としてもよい。またシークレットパラメータを適用した暗号処理等を実行する構成としてもよい。

【０１０３】

［４，再生（プレーヤ）アプリケーションとセキュアＶＭ間の処理］

上述した処理を実行する場合、再生（プレーヤ）アプリケーションは、コンテンツの再生を実行中、一定のセグメント単位で、異なるシークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を順次取得するため、セキュアＶＭに対して、セグメントの切り替わりの再生前に、シークレットパラメータを取得してデータ置き換えを行なうことになる。この場合に、再生（プレーヤ）アプリケーションは、セキュアＶＭに対してシークレットパラメータ指定情報としてのシークレットパラメータＩＤ（ＳＰ＿Ｉ）を通知して、必要なＳＰを特定する。このシークレットパラメータＩＤ（ＳＰ＿Ｉ）は、先に、図６を参照して説明したシークレットパラメータ（ＳＰ）ＩＤ特定テーブル３０２に記録されている。

【０１０４】

再生（プレーヤ）アプリケーションは、このシークレットパラメータ（ＳＰ）ＩＤ特定テーブル３０２を参照可能な状態に設定する処理が必要となる。再生アプリケーションと、セキュアＶＭ間において実行される一連の処理シーケンスについて、図１０を参照して説明する。

【０１０５】

先に、図１を参照して説明したように、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間の情報伝達、あるいは処理要求は、再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理のシーケンスによって実行される。

【０１０６】

図１０に示す処理シーケンスは、コンテンツを記録した情報記録媒体の挿入から、取り出しに至るまでに再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間において実行される処理の種類を示した図である。

【０１０７】

例えば、ステップＳ１１は、情報記録媒体（Ｄｉｓｃ）挿入時の処理として実行されるメディア初期化（Ｍｅｄｉａ　Ｉｎｉｔｉａｌｉｚｅ）処理であり、再生（プレーヤ）ア

プリケーション１５０は、最初の再生処理に必要となるコード情報を格納したコンテンツコードファイル（Ｃｏｎｔｅｎｔ　Ｃｏｄｅ　Ｆｉｌｅ）をメモリにロードして、実行を開始する。コンテンツコードファイル（Ｃｏｎｔｅｎｔ　Ｃｏｄｅ　Ｆｉｌｅ）は、再生（プレーヤ）アプリケーションのメーカー、モデル名などを特定する。

【０１０８】

例えば、セキュアＶＭ１６０は、取得したモデル名が、過去にセキュリティ問題が発生したことがあるモデルであるか否かを判定し、過去にセキュリティ問題が発生したことがあるモデルである場合、同様のセキュリティ問題が発生していないかをコンテンツコード（ＣｏｎｔｅｎｔＣｏｄｅ）の実行により調査する。例えば情報処理装置のＲＡＭ上の特定の値や、特定のデバイスの動作を調べて、正しい状態であるかを検査する。なお、モデルごとの調査プログラムは、最初にロードしたコンテンツコードファイルには入っていないことがあり、その場合は別の必要なコンテンツコードファイルへのアクセスを行う。セキュアＶＭ１６０による初期化処理が終了すると、応答（Ｃａｌｌ）が再生アプリケーション１５０に通知され、次のステップＳ１２に進む。

【０１０９】

ステップＳ１２では、タイトル初期化処理（Ｔｉｔｌｅ　Ｉｎｉｔｉａｌｉｚｅ）を実行する。タイトルは再生対象コンテンツの指定情報として適用され、ユーザの指定などに基づいて、特定の再生対象コンテンツに対応するタイトルが選択され、タイトル情報とともに、タイトル初期化処理要求が再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に出力される。

【０１１０】

セキュアＶＭ１６０は、タイトル再生に必要な全クリップ対応の変換データ情報を集めた変換テーブルをセキュアＶＭ１６０のメモリ上に生成し、再生（プレーヤ）アプリケーション１５０がテーブルを取得できるようにテーブルがストアされたメモリの位置を再生（プレーヤ）アプリケーション１５０に知らせる。なお、タイトル初期化中もステップＳ１１のメディア初期化と同様のセキュリティチェックを行うことが可能である。

【０１１１】

タイトル初期化処理において実行される、タイトル再生に必要な全クリップ対応の変換データ情報を集めた変換テーブルをセキュアＶＭ１６０のメモリ上に生成する処理例について、図１１を参照して説明する。図１１には、セキュアＶＭ１６０の利用可能なメモリ領域（例えば２ＭＢ）を示している。ここには、セキュアＶＭ１６０が、情報記録媒体から取得したデータ変換処理プログラムに含まれるコード情報としてのコンテンツコードが格納される。なお、このコンテンツコードには暗号化等の難読化処理のなされた変換テーブルが含まれる。

【０１１２】

再生（プレーヤ）アプリケーション１５０からのタイトル初期化要求が入力されると、セキュアＶＭ１６０は、コンテンツコードから、タイトル再生に必要な全クリップ対応の変換データ情報を集めた変換テーブルを、必要に応じて復号処理を行い、前述したＸＯＲｅｄ等の処理のなされた状態（マスク状態）でメモリに格納し、このメモリ格納位置を再生（プレーヤ）アプリケーション１５０に通知する。この通知処理は、再生（プレーヤ）アプリケーション１５０からのタイトル初期化要求（ＩＮＴＲＰ）に対する応答（Ｃａｌｌ）として実行される。

【０１１３】

再生（プレーヤ）アプリケーション１５０は、セキュアＶＭ１６０から、タイトル初期化要求（ＩＮＴＲＰ）に対する応答（Ｃａｌｌ）を受領すると、セキュアＶＭ１６０利用メモリ領域の変換テーブル格納領域から、必要なデータ部分を、再生（プレーヤ）アプリケーション１５０の利用可能なメモリ領域にコピーして格納する。例えば、先に、図６～図９を参照して説明したコンテンツのセグメント対応のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を取得するためのシークレットパラメータＩＤ（ＳＰ＿ＩＤ）特定テーブルを抽出して再生（プレーヤ）アプリケーション１５０の利用可能なメモリ領域にコピーして

格納する。

【０１１４】

先に、図８を参照して説明したコンテンツ中に分散記録された変換テーブルブロックから変換データを取得する処理を実行する再生（プレーヤ）アプリケーションである場合は、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）特定テーブルを取得するのみでよいが、図９を参照して説明したプレーヤ、すなわち、コンテンツ中に分散記録された変換テーブルブロックを利用しないプレーヤである場合は、このコピー処理において、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）特定テーブル、および、変換ントリを格納した変換テーブルブロックについても自己の利用可能なメモリ領域にコピーして格納する処理を実行する。図９を参照して説明したＸＯＲｅｄ変換テーブルブロックは、この処理によって再生（プレーヤ）アプリケーション１５０の利用可能なメモリ領域にコピーされた変換テーブルブロックである。

【０１１５】

図１０に戻り、再生（プレーヤ）アプリケーション１５０とセキュアＶＭ１６０間の処理シーケンスについて説明を続ける。ステップＳ１３は、シークレットパラメータ（ＳＰ）計算に（Ｃｏｍｐｕｔｅ＿ＳＰ）に対応する処理であり、再生（プレーヤ）アプリケーション１５０は、ＳＰ計算要求（ＩＮＴＲＰ）をセキュアＶＭ１６０に出力し、セキュアＶＭ１６０は計算結果（ＳＰ）を応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーション１５０に返す。再生（プレーヤ）アプリケーション１５０は、ＳＰ計算要求（ＩＮＴＲＰ）をセキュアＶＭ１６０に出力する場合、ＳＰ指定情報としてのＳＰ＿ＩＤを、例えばシークレットパラメータＩＤ（ＳＰ＿ＩＤ）特定テーブルから取得して通知する。

【０１１６】

なお、再生（プレーヤ）アプリケーション１５０は、ＳＰ指定情報としてのＳＰ＿ＩＤを取得してセキュアＶＭ１６０に通知する場合、コンテンツのセグメントに対応する正確なＳＰ＿ＩＤを選択することが必要である。このＳＰ＿ＩＤの選択処理の具体例については、後述する。なお、ステップＳ１３の処理は、各セグメントごとに繰り返して実行される。

【０１１７】

ステップＳ１４の処理は、シークレットパラメータの計算とは異なる再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する要求処理である。例えば、セキュリティチェックの実行などの要求処理であり、セキュアＶＭ１６０は、これらの要求があった場合、その要求に応じた処理を実行して、処理結果を応答（Ｃａｌｌ）として再生（プレーヤ）アプリケーション１５０に通知する。なお、この際の情報伝達には、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０の双方が書き込み読み取り可能なレジスタ、例えばプレイヤ・ステータスレジスタ、レジスタ（ＰＳＲ）が利用される。

【０１１８】

ステップＳ１５の処理は、情報記録媒体（Ｄｉｓｃ）取出の際のメディアファイナライズ（Ｍｅｄｉａ　Ｆｉｎａｌｉｚｅ）処理であり、コンテンツコード（Ｃｏｎｔｅｎｔ　Ｃｏｄｅ）の処理状況を、不揮発メモリに記録する。この処理によって、次回のディスク挿入時に過去のセキュリティチェックの情報を継続して使用することが可能となる。

【０１１９】

上述したように、再生（プレーヤ）アプリケーション１５０と、セキュアＶＭ１６０間の情報伝達、あるいは処理要求、応答は、再生（プレーヤ）アプリケーション１５０からセキュアＶＭ１６０に対する割り込み（ＩＮＴＲＰ）と、セキュアＶＭ１６０から再生（プレーヤ）アプリケーション１５０に対する応答（Ｃａｌｌ）処理によって実行される。

【０１２０】

この場合、セキュアＶＭ１６０は、再生（プレーヤ）アプリケーション１５０から入力する割り込み（ＩＮＴＲＰ）をすべて処理するのではなく、一定の条件に基づいて、ある処理を実行し、ある処理については拒否する。このセキュアＶＭ１６０における割り込み

処理要求（ＩＮＴＲＰ）の受理、拒否の態様について、図１２を参照して説明する。

【０１２１】

図に示すグラフ３２１は、セキュアＶＭにおけるモード遷移を示している。左から右に時間（ｔ）が経過している。まず、バックグラウンドモードにおいて、再生（プレーヤ）アプリケーションからの割り込み要求としてシークレットパラメータ（ＳＰ）算出要求が入力される。この時点で、セキュアＶＭは処理を実行しておらず、シークレットパラメータ（ＳＰ）算出要求を受理（Ａｃｃｅｐｔ）し、パラメータ算出モードに遷移して、パラメータ算出処理を実行する。

【０１２２】

さらに、このパラメータ算出モード期間に、再生（プレーヤ）アプリケーションからの割り込み要求を受けた場合、１番目の要求については受理し、連続して受領した割り込み要求については拒否（Ｉｇｎｏｒｅ）する。

【０１２３】

パラメータ算出モード期間において受領した最初の割り込み要求に対応する処理は、パラメータ算出モード期間の終了後のアプリケーション要求モードにおいて実行される。さらに、この期間において受けたシークレットパラメータ（ＳＰ）算出要求は、受理（Ａｃｃｅｐｔ）し、アプリケーション要求モードの終了後に、パラメータ算出モードに遷移して、パラメータ算出処理を実行する。このようにセキュアＶＭは、１種類の割り込み（ＩＮＴＲＰ）について、１つだけの未処理割り込みを保持する構成を持つ。２つ目移行の割り込み要求については拒否（Ｉｇｎｏｒｅ）する。

【０１２４】

［５．コンテンツ再生処理］

次に、図１３を参照して、ホストの実行するコンテンツ再生処理について説明する。図１３には、左から暗号化コンテンツの格納された情報記録媒体３３０、情報記録媒体３３０をセットし、データの読み取りを実行するドライブ３４０、ドライブとデータ通信可能に接続され、情報記録媒体３３０に格納されたコンテンツをドライブ３４０を介して取得して再生処理を実行する再生アプリケーションを実行するホスト３４５を示している。

【０１２５】

なお、図１３に示すホスト３４５は、コンテンツの復号、デコード、データ変換処理などを実行する再生（プレーヤ）アプリケーションブロック３５０と、シークレットパラメータ（ＳＰ）の算出処理などを実行するセキュアＶＭ３６０を有するセキュアＶＭ３６０ブロックを区分して示してある。

【０１２６】

情報記録媒体３３０には、ＭＫＢ（Media Key Block）３３１、タイトル鍵ファイル３３２、暗号化コンテンツ３３３、変換テーブル３３４、データ変換処理プログラム３３５が格納されている。ホスト３４５は、ＭＫＢの処理に適用するデバイス鍵３５１を保持している。

【０１２７】

図１３に示すホスト３４５がドライブ３４０を介して情報記録媒体３３０の格納コンテンツを取得して再生する処理シーケンスについて説明する。まず、情報記録媒体３３０の格納コンテンツの読み出しに先立ち、ホスト３４５とドライブ３４０は、ステップＳ１０１において、相互認証を実行する。この相互認証は、ホストおよびドライブがそれぞれ正当な機器またはアプリケーションソフトであるかを確認する処理である。この相互認証処理シーケンスとしては、様々な処理が適用可能である。相互認証処理によって、ドライブ３４０とホスト３４５は共通の秘密鍵としてのセッション鍵（Ｋｓ）を共有する。

【０１２８】

ステップＳ１０１において、ホストドライブ間の相互認証が実行され、セッション鍵（Ｋｓ）を共有した後、ホスト３４５の再生（プレーヤ）アプリケーション３５０は、ステップＳ１０２において、情報記録媒体３３０に記録されたＭＫＢ３３１を、ドライブを介して取得して、メモリに格納されたデバイス鍵３５１を適用したＭＫＢ３３１の処理を実

行して、ＭＫＢからメディア鍵（Ｋｍ）を取得する。

【０１２９】

前述したように、ＭＫＢ（Media Key Block）３３１は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックであり、有効なライセンスを持つ装置に格納されたデバイス鍵（Ｋｄ）に基づく処理（復号）によってのみ、コンテンツの復号に必要なキーであるメディア鍵（Ｋｍ）の取得を可能とした鍵情報ブロックである。

【０１３０】

次に、ステップＳ１０３において、ステップＳ１０２におけるＭＫＢ処理で取得したメディア鍵（Ｋｍ）を適用して、情報記録媒体３３０から読み取ったタイトル鍵ファイル３３２の復号を実行して、タイトル鍵（Ｋｔ）を取得する。情報記録媒体３３０に格納されるタイトル鍵ファイル３３２はメディア鍵によって暗号化されたデータを含むファイルであり、メディア鍵を適用した処理によってコンテンツ復号に適用するタイトル鍵（Ｋｔ）を取得することができる。なお、ステップＳ１０３の復号処理は、例えばＡＥＳ暗号アルゴリズムが適用される。

【０１３１】

次に、ホスト３４５の再生（プレーヤ）アプリケーション３５０は、ドライブ３４０を介して情報記録媒体３３０に格納された暗号化コンテンツ３３３を読み出して、トラックバッファ３５２に読み出しコンテンツを格納し、このバッファ格納コンテンツについて、ステップＳ１０４において、タイトル鍵（Ｋｔ）を適用した復号処理を実行し、復号コンテンツを取得する。

【０１３２】

復号コンテンツは、平文ＴＳバッファ３５３に格納する。（Ｐｌａｉｎ　ＴＳ）は復号された平文トランスポートストリームを意味する。ここで、平文ＴＳバッファ３５３に格納される復号コンテンツは、前述したブロークンデータを含むコンテンツであり、このままでは再生できず、所定のデータ変換（上書きによるデータ置き換え）を行なう必要がある。

【０１３３】

図１３に示す処理例では、暗号化コンテンツの構成データ中の特定パケットに分散されて記録された変換エントリを取得して、ここから変換データを抽出してデータ置き換えを行なう処理例である。すなわち、先に、図８を参照して説明したデータ変換処理に相当する。

【０１３４】

コンテンツ中に分割記録された変換エントリは、復号コンテンツに対して置き換え処理を行なう変換データ（または識別子設定変換データ）とその変換データの記録位置を記録したデータである。

【０１３５】

セキュアＶＭ３６１は、命令コード情報を含むデータ変換処理プログラム３３５を情報記録媒体３３０から読み出して、コンテンツ再生あるいは出力処理前および処理実行中に間欠的に、イベントハンドラ３５４の制御、プレーヤ情報３５５の入力に基づいて、情報記録媒体３３０にコンテンツとともに記録された変換テーブルを平文変換テーブルにするために必要なシークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を生成して出力する。この処理は間欠的に行なわれる。

【０１３６】

シークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）は、前述したように所定のコンテンツデータ単位に対応するセグメントごとに切り替わる演算または暗号処理パラメータであり、具体的には、例えば、排他論理和（ＸＯＲ）演算パラメータである。セキュアＶＭ３６１は、再生（プレーヤ）アプリケーションからの要求に応じて、演算処理または暗号処理によって変形された変換テーブルブロックの構成データである変換エントリを復元するために必要なパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を間欠的に生成して

出力する処理を実行する。

【０１３７】

再生（プレーヤ）アプリケーション３５０は、ステップＳ１０４において、変換エントリを含む暗号化コンテンツ３３３の復号が実行され、ステップＳ１０５におけるデマルチプレクサの処理によって、コンテンツ中に記録された変換テーブルの構成データである変換エントリが分離され、リアルタイムイベントハンドラ３５６の制御によって、ステップＳ１０６におけるテーブル復元＆データ変換処理が実行される。リアルタイムイベントハンドラ３５６の制御により、再生（プレーヤ）アプリケーション３５０は、セグメントの切り替えに応じたシークレットパラメータ算出要求をセキュアＶＭ３６１に割り込み（ＩＮＴＲＰ）として出力し、セキュアＶＭ３６１からセキュアパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を受領し、変換テーブルブロックの復号または演算を実行して平文変換テーブルブロックを取得し、取得した変換テーブルブロックに含まれる変換エントリを取得する。

【０１３８】

変換エントリには、変換データ、すなわち、

（ａ）変換データ

（ｂ）識別子設定変換データ

と、これらの変換データのコンテンツにおける記録位置指定情報が記録されており、再生（プレーヤ）アプリケーション３５０は、ステップＳ１０６において、指定位置に書き込むデータ変換処理をコンテンツ再生処理または外部出力処理に並行したリアルタイム処理として実行する。

【０１３９】

例えば、パラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）は所定のコンテンツ部分データ単位に対応する変換データとの排他論理和（ＸＯＲ）演算パラメータである場合、ステップＳ３０３におけるテーブル復元処理としては、

［変換テーブルブロック１］（ＸＯＲ）［ＳＰ１］、

［変換テーブルブロック２］（ＸＯＲ）［ＳＰ２］、

［変換テーブルブロック３］（ＸＯＲ）［ＳＰ３］、

：　　：

これらの排他論理和演算処理を実行して、変換テーブルブロックデータに含まれる変換エントリを取得する。なお、上記式において、［Ａ］（ＸＯＲ）［Ｂ］は、ＡとＢの排他論理和演算を意味するものとする。

【０１４０】

このように、情報記録媒体に記録されたコンテンツ３３３に含まれる変換テーブルブロックは、各コンテンツ部分に対応する変換データおよび変換データ位置情報を記録した変換エントリに分割されており、シークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）と排他論理和演算されて格納されている。このパラメータは、セキュアＶＭ３６１によって逐次、取得され出力される。

【０１４１】

ステップＳ１０６のテーブル復元＆データ変換処理においては、シークレットパラメータ（ＳＰ１，ＳＰ２，ＳＰ３・・・）を適用した演算または暗号処理よって取得した復元された変換エントリから変換データを取得して、コンテンツに含まれるブロークンデータを正当なコンテンツ構成データである変換データに置き換え、さらに、識別子設定変換データをコンテンツの一部データと入れ替えるデータ上書き処理を実行し、平文ＴＳバッファ３５３の格納データを変換処理済みデータに変更する。このデータ変換処理の概要について、図１４を参照して説明する。

【０１４２】

情報記録媒体に格納された暗号化コンテンツ３３３が、一旦、ホスト側のトラックバッファ３５２に格納される。図１４（１）に示すトラックバッファ格納データ４０１である。ホスト側の復号処理によって、トラックバッファ格納データ４０１としての暗号化コン

テンツの復号が実行されて、復号結果データが平文ＴＳバッファ３５３に格納される。図１４（２）に示す復号結果データ４０２である。

【０１４３】

復号結果データ４０２には、正常なコンテンツ構成データではない、ブロークンデータ４０３が含まれる。ホストのデータ変換処理部は、このブロークンデータ４０３を、正しいコンテンツ構成データとしての変換データ４０４に置き換える処理を実行する。この置き換え処理は、例えば平文ＴＳバッファ３５３に書き込み済みのデータに対する一部データの再書き込み（上書き）処理として実行される。

【０１４４】

さらに、ホストの実行するデータ変換処理は、ブロークンデータを正常なコンテンツデータである変換データに置き換える処理のみならず、図１４に示すように、識別子設定変換データ４０５によって、復号結果データ４０２の一部構成データを置き換える処理を実行する。

【０１４５】

識別子は、前述したようにコンテンツ再生装置またはコンテンツ再生アプリケーションを識別可能とした識別情報の構成ビットを解析可能としたデータである。具体的には例えば、ホストアプリケーションを実行するプレーヤとしての情報処理装置の識別情報（プレーヤＩＤ）の構成データまたは、プレーヤＩＤに基づいて生成される識別マークである。識別子設定変換データは、先に説明したようにコンテンツの再生に影響を与えないレベルで、正しいコンテンツデータのビット値をわずかに変更したデータである。

【０１４６】

識別子設定変換データ４０５は、コンテンツ中に多数設定され、これら複数の識別子設定変換データ４０５を集積して解析することで、例えばプレーヤＩＤが判別される。識別子設定変換データ４０５は、コンテンツとして通常再生可能なレベルで正常コンテンツデータの構成ビットを変更したデータであり、ＭＰＥＧビットストリーム解析によりビット（識別マーク構成ビット）判別が可能なデータである。

【０１４７】

情報記録媒体に格納される変換テーブルには、図１４に示す変換データ４０４、識別子設定変換データ４０５が多数登録されており、さらに、これらの書き込み位置情報についても登録されている。この変換テーブル格納情報に基づくデータ変換処理を実行することで、平文ＴＳバッファ３５３に格納されたデータは、図１４（３）に示す変換処理済みデータ４０６に置き換えられることになる。

【０１４８】

その後、変換済みのＴＳ（トランスポートストリーム）は、ネットワークなどを介して外部出力され、外部の再生機器において再生される。あるいは、ステップＳ１０７において、デマルチプレクサによる処理によって、トランスポートストリーム（ＴＳ）からエレメンタリストリーム（ＥＳ）への変換が実行され、さらに、デコード処理（ステップＳ１０８）が行なわれた後、ディスプレイスピーカを介して再生される。

【０１４９】

［６．セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理］

上述したように、情報記録媒体に記録されたコンテンツは、セグメントに区分されており、各セグメントにおいて必要となるデータ変換処理に際しては、セグメントごとに異なるシークレットパラメータ（ＳＰｎ）をセキュアＶＭから取得して、取得したシークレットパラメータを適用して変換エントリを含む変換テーブルブロックの復元をすることが必要となる。

【０１５０】

このセグメントごとに異なるシークレットパラメータ（ＳＰｎ）をセキュアＶＭから取得するため、再生（プレーヤ）アプリケーションは、各セグメントに対応するシークレットパラメータ識別子（ＳＰ＿ＩＤ）を取得して、取得したシークレットパラメータ識別子（ＳＰ＿ＩＤ）をセキュアＶＭに通知する。以下では、各セグメントに対応する正しいシ

ークレットパラメータ識別子（ＳＰ＿ＩＤ）を取得する手法に関する複数の処理例１～３について説明する。

【０１５１】

（６．１）セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例１

セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例１について説明する。本処理例においては、先に、図６を参照して説明したシークレットパラメータＩＤ特定テーブルに、コンテンツを構成するパケット（ＴＳパケット）の識別情報としてのＳＰＮ（ソースパケットナンバー）をＳＰ識別子（ＳＰ＿ＩＤ）に対応付けて登録する。

【０１５２】

コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、まず、再生対象コンテンツデータに対応するＳＰＮ（ソースパケットナンバー）を、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマップから取得する。さらに、ＥＰマップから取得したＳＰＮ（ソースパケットナンバー）に基づいて、シークレットパラメータＩＤ特定テーブルを検索して、取得ＳＰＮ（ソースパケットナンバー）に対応して設定されたＳＰ識別子（ＳＰ＿ＩＤ）を取得する。

【０１５３】

再生（プレーヤ）アプリケーションは、セキュアＶＭに対して、シークレットパラメータＩＤ特定テーブルから取得したＳＰ識別子（ＳＰ＿ＩＤ）を通知してシークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する。

【０１５４】

以下、図面を参照して、本処理例について詳細に説明する。図１５は、コンテンツ再生を実行するコンテンツ再生処理部、すなわち、再生（プレーヤ）アプリケーションによるコンテンツ再生処理を説明する図である。まず、コンテンツ再生に際して、再生（プレーヤ）アプリケーションはコンテンツの再生区間情報としてのクリップ情報を取得する。

【０１５５】

例えば図１５（ａ）に示すクリップ情報が選択される。クリップ情報は、コンテンツのパケット識別子情報を含むＥＰマップを複数含むデータとして設定される。各ＥＰマップには、例えば図１５（ｂ）に示す再生コンテンツとしてのＡＶストリームを構成する符号化データであるＭＰＥＧデータの符号化データ単位としてのＧＯＰ(Group Of Pictures)中のＩピクチャに関するパケット情報が含まれる。

【０１５６】

ＥＰマップ中に含まれるＩピクチャのパケット情報中には、ＳＰＮ（ソースパケットナンバー）が含まれる。例えば、１つのＧＯＰ(Group Of Pictures)は、図１５（ｃ）に示すように、１つのＩピクチャ４１１と複数のＰ，Ｂピクチャによって構成される。Ｉピクチャ４１１は、ＧＯＰ中の基準ピクチャとして設定される符号化データであり、Ｐ，Ｂピクチャは、Ｉピクチャ情報を参照情報として適用するピクチャ情報である。

【０１５７】

なお、ブロークンデータとして設定されるパケットはＴＳパケット単位であり、ＴＳパケットは、図に示すようにＩピクチャ４１１やＰ，Ｂピクチャの構成データとして設定される。すなわち、１つのＩピクチャ、またはＰ，Ｂピクチャは、多数のＴＳパケットに分散されて格納される。

【０１５８】

例えば、このＧＯＰ内のＩピクチャ４１１を構成するＴＳパケットの１つを変形データ（ブロークンデータ）として設定すると、ＭＰＥＧ符号化データの基準となるＩピクチャが壊れることになり、Ｉピクチャを参照情報として利用するＰピクチャやＢピクチャも復元（ＭＰＥＧ復号）ができなくなり、効果的なデータ破壊を行なうことができる。

【０１５９】

コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、データ変換によって、変換テーブルに記録された変換データを取得して、データ置き換えを実行する。なお、前述したように、データ置き換えは、ブロークンデータの置き換え用の変換データのみな

らず、識別子設定変換データについても実行される。

【０１６０】

前述したように、これらの変換データは、変換テーブルに登録されているが、セグメント毎に異なるシークレットパラメータ（ＳＰ）を適用した演算、あるいは暗号化が施されており、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、各セグメントに対応するシークレットパラメータをセキュアＶＭかせら取得しなければならない。

【０１６１】

本処理例では、再生（プレーヤ）アプリケーションは、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマップからＳＰＮ（ソースパケットナンバー）を取得し、取得したＳＰＮ（ソースパケットナンバー）に基づいて、シークレットパラメータＩＤ特定テーブルを検索して、再生予定のＳＰＮ（ソースパケットナンバー）に対応するＳＰ識別子（ＳＰ＿ＩＤ）を取得する。

【０１６２】

まず、図１６、図１７を参照してＥＰマップの詳細について説明する。図１６に示すように、ＥＰマップ（ＥＰ＿ｍａｐ）４１２は、クリップ情報ファィル（クリップインフォメーション）に含まれるデータである。ＥＰマップに基づくＩピクチャ位置の検出について、図１７参照して説明する。図１７（Ａ）はクリップＡＶストリームを示し、各矩形は１９２ビットソースパケットを示している。各ソースパケットにはタイムスタンプが設定され再生処理時間が規定されている。

【０１６３】

図１７（Ｂ）に、ソースパケットＮｏ．（Ｘ１）の詳細構成を示す。１つのソースパケットは、ＴＰ＿ｅｘｔｒａヘッダとトランスポートパケットとによって構成され、トランスポートパケットには、各種のヘッダ情報と、ＭＰＥＧ２実体データとしてのＩ－ＰＩＣＨ～のデータによって構成される。

【０１６４】

図１７（Ｃ）に示すクリップインフォメーションには、前述したようにＥＰマップが含まれる。ＥＰマップには、図に示すように、［ＰＴＳ＿ＥＰ　ｓｔａｒｔ］、［ＳＰＮ＿ＥＰ　ｓｔａｒｔ］、［Ｉ＿ｅｎｄ＿ｐｏｓｉｔｉｏｎ＿ｏｆｆｓｅｔ］の各データが含まれる。各データの意味は、以下の通りである。

PTS_EP_start：シーケンスヘッダを含むsource packetに対応するタイムスタンプ（プレゼンテーションタイムスタンプ）。

SPN_EP_start：シーケンスヘッダを含むsource packetの先頭アドレス。

I_end_position_offset：シーケンスヘッダを含むsource packetから、Ｉピクチャの終わりを含むsource packetのオフセット

これらのデータ関係を示すのが図１７（Ｄ）である。

【０１６５】

すなわち、図１７（Ｂ）に示すように、ソースパケットに含まれるデータの構成が規定されており、図１７（Ｃ）に示す［ＰＴＳ＿ＥＰ　ｓｔａｒｔ］、［ＳＰＮ＿ＥＰ　ｓｔａｒｔ］、［Ｉ＿ｅｎｄ＿ｐｏｓｉｔｉｏｎ＿ｏｆｆｓｅｔ］の各データをＥＰマップから求めることで、これらのデータに基づいて、ソースパケット中のＩピクチャ位置が求められることになる。

【０１６６】

本処理例では、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、再生対象コンテンツのデータに対応するＳＰＮ（ソースパケットナンバー）を、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマップから取得し、取得したＳＰＮ（ソースパケットナンバー）に基づいて、シークレットパラメータＩＤ特定テーブルを検索して、再生予定のＳＰＮ（ソースパケットナンバー）に対応するＳＰ識別子（ＳＰ＿ＩＤ）を取得する。

【０１６７】

図１８に、シークレットパラメータ（ＳＰ）ＩＤ特定テーブルのデータ構成例、および

、再生（プレーヤ）アプリケーションの実行するセキュアＶＭに対するＳＰ算出要求処理シーケンスを説明するフローチャートを示す。

【０１６８】

図１８に示すフローチャートの各ステップについて説明する。コンテンツを再生する再生（プレーヤ）アプリケーションは、まず、ステップＳ２０１において、再生予定のコンテンツの再生区間情報としてのクリップ情報を取得し、さらに、ステップＳ２０２において、クリップ情報に含まれるＥＰマップを取得する。さらに、ステップＳ２０３において、取得したＥＰマップから再生位置を示すソースパケットＮｏ．であるＳＰＮを取得する。

【０１６９】

例えば、ソースパケッナンバー：ＳＰＮ＝９４５１０００が取得されたとする。次に、ステップＳ２０４において、ＳＰ＿ＩＤ特定テーブルを参照する。なお、このＳＰ＿ＩＤ特定テーブルは、先に図６を参照して説明したように情報記録媒体に格納される変換テーブルの構成データであり、先に、図１０、図１１を参照して説明したように、再生アプリケーションの利用可能なメモリ領域にコピーされて格納されている。

【０１７０】

ＳＰ＿ＩＤ特定テーブルは、図１８に示すように、ＳＰ＿ＩＤと、ソースパケットナンバー（ＳＰＮ）の対応テーブルとして記録されている。図に示すＳＰ＿ＩＤ特定テーブルは、クリップに対応するＳＰ＿ＩＤ特定テーブルである。各ＳＰ＿ＩＤに対応して登録されたソースパケットナンバー（ＳＰＮ）は、コンテンツを構成する各セグメントの最初のパケットナンバーに相当する。

【０１７１】

図に示すＳＰ＿ＩＤ特定テーブルの例では、例えばＳＰ＿ＩＤ＝１２４が対応するコンテンツのセグメントは、パケットナンバー（ＳＰＮ）＝９３６２１５３～９４４４３１０であり、ＳＰ＿ＩＤ＝１２５が対応するセグメントは、パケットナンバー（ＳＰＮ）＝９４４４３１１～９５２８２５４となる。

【０１７２】

ステップＳ２０３において、再生アプリケーションがクリップ情報中のＥＰマップからソースパケッナンバー：ＳＰＮ＝９４５１０００を取得したとする。再生アプリケーションは、ステップＳ２０４において、ソースパケッナンバー：ＳＰＮ＝９４５１０００に対応するＳＰ＿ＩＤをＳＰ＿ＩＤ特定テーブルから取得する。

【０１７３】

図１８に示すＳＰ＿ＩＤ特定テーブルの例では、ソースパケッナンバー：ＳＰＮ＝９４５１０００は、ＳＰ＿ＩＤ＝１２５に対応するパケットナンバー（ＳＰＮ）＝９４４４３１１～９５２８２５４に属することになる。従って、ソースパケッナンバー：ＳＰＮ＝９４５１０００に対応するシークレットパラメータＩＤは、ＳＰ＿ＩＤ＝１２５となる。ステップＳ２０５では、このようにして、ソースパケッナンバー：ＳＰＮ＝９４５１０００に対応するシークレットパラメータＩＤ［ＳＰ＿ＩＤ＝１２５］を取得する。

【０１７４】

再生（プレーヤ）アプリケーションは、ステップＳ２０６において、取得したシークレットパラメータＩＤ［ＳＰ＿ＩＤ＝１２５］をセキュアＶＭに通知して、セグメント対応のシークレットパラメータ（ＳＰ）算出要求（ＩＮＴＲＰ）を実行して、セキュアＶＭからセグメント対応のシークレットパラメータ（ＳＰ）を取得する。

【０１７５】

本処理例において適用可能な変換テーブル、および、ＳＰ＿ＩＤ特定テーブルの構成例について図１９、図２０を参照して説明する。図１９は、変換テーブルの構成を示す図である。変換テーブルには、以下のデータが含まれる。

Number of Clips (= Nclip)：タイトル中で使用するクリップ数

FixUpTableBody_StartAddress：変換テーブル内の変換テーブルボディの開始アドレス

SPChangePositionTable()：ＳＰ＿ＩＤ特定テーブル

FixUpTableBody()：変換テーブルボディ

【０１７６】

本処理例では、ＳＰ＿ＩＤ特定テーブルは、図１８に示すように、シークレットパラメータ（ＳＰ）の変更されるパケットＮｏ．が記録されたテーブルとして設定される。すなわち、各セグメントの先頭パケットＮｏ．が各ＳＰ＿ＩＤに対応して記録される。

【０１７７】

変換テーブルに含まれるＳＰ＿ＩＤ特定テーブル［SPChangePositionTable］のデータ構成例を図２０に示す。ＳＰ＿ＩＤ特定テーブルは各クリップ毎に各クリップに含まれるＳＰ変更部に相当するパケット識別子としてのソースパケットナンバー（ＳＰＮ）を登録したテーブルとして設定される。ＳＰ＿ＩＤ特定テーブルには、以下のデータが含まれる。

Clip_ID：クリップＩＤ

Number of SP (= NSP)：セグメント（SP_segment）数

SP_segment_start_SPN：ＳＰ＿ＩＤに対応するセグメント（SP_segment）の先頭のソースパケットナンバー（ＳＰＮ）

【０１７８】

再生アプリケーションは、ＳＰ＿ＩＤに対応するセグメント（SP_segment）の先頭のソースパケットナンバー（ＳＰＮ）を取得して、再生予定のＳＰＮに対応したＳＰ＿ＩＤを取得することができる。

【０１７９】

図２１に、変換テーブルに含まれる変換テーブルボディ［FixUpTableBody］のデータ構成例を示す。変換テーブルボディは、各クリップごとに以下のデータを持つ。

Clip_ID：クリップの識別子（ＩＤ）(Clip_ID=1234の場合は01234.clpi、01234.m2tsのクリップファイルに対応する)

Number of SP (= NSP)：クリップ内のセグメント（SP_segment）数

さらに、各ＳＰ＿ＩＤ毎に

Start address of FUT block()：変換テーブルブロック（ＦＵＴブロック）のスタートアドレス

FUT block:変換テーブルブロック

これらのデータを格納している。

なお、各変換テーブルブロックは、図に示すように、１つのセグメント（SP_segment）に対応する変換エントリを全て含む設定となっている。

【０１８０】

１つの変換テーブルブロックのデータ構成例について図２２を参照して説明する。変換テーブルブロックは、先に説明したように、実際の置き換えデータとしての変換データと書き込み位置情報を含む変換エントリを格納したテーブルである。変換テーブルブロックには、以下のデータが記録される。

Number of FixUpEntry in this block (=NFixups)：この変換テーブルブロック（FUT block）内の変換エントリ（FixUpEntry）数＝この変換テーブルブロック（FUT block）に該当するセグメント（SP_segment）内にある、変換データ（FixUpデータ）を含むプログラムマップテーブル（ＰＭＴ）の数

さらに各変換エントリの各々について、

Base SPN for FixUpEntry：セグメント（SP_segment）内でI番目の変換エントリ（FixUpEntry）構造付きプログラムマップテーブル（ＰＭＴ）のソースパケットナンバー（ＳＰＮ）

FixUpEntry()：変換エントリ、セグメント（SP_segment）内でI番目の変換エントリ（FixUpEntry）構造付きプログラムマップテーブル（ＰＭＴ）内の変換エントリ（FixUpEntry）情報に一致する

これらのデータが含まれる。

【０１８１】

なお、変換エントリ（FixUpEntry）は、先に、図７を参照して説明したように、実際に置き換え対象となる変換データと、その変換データの記録位置情報が登録されているデータであり、再生（プレーヤ）アプリケーションは、変換エントリから、変換データと、その変換データの記録位置情報を取り出して、指定位置に、変換データを上書きしてデータ変換を実行する。

【０１８２】

次に、図２３に示すフローチャートを参照して、セグメント毎に異なるシークレットパラメータ（ＳＰ）を取得して変換データによるデータ置き換えを伴うコンテンツ再生処理シーケンスについて説明する。まず、ステップＳ４０１において、再生（プレーヤ）アプリケーションは、再生するタイトルを決定し、セキュアＶＭに対して、タイトル初期化命令を発行する。ステップＳ４０２では、セキュアＶＭは、タイトル初期化処理を実行し、タイトルに対応する変換テーブル（FixUpTable）の生成処理を実行する。これは、先に、図１０、図１１を参照して説明した処理であり、図１０に示すシーケンス図のステップＳ１２の処理に対応する。

【０１８３】

ステップＳ４０３において、再生（プレーヤ）アプリケーションは、変換テーブル（FixUpTable）から必要な情報を取得する。これは、先に、図１１を参照して説明した処理であり、セキュアＶＭのメモリ領域に格納された変換テーブルから、必要な情報を再生（プレーヤ）アプリケーションの利用可能なメモリ領域にコピーする処理として実行される。

【０１８４】

コンテンツのＴＳ（トランスポートストリーム）に多重化されたＦＵＴブロックから変換エントリを取り出してデータ変換を実行する再生（プレーヤ）アプリケーション、すなわち、先に図８を参照して説明した処理を実行する再生（プレーヤ）アプリケーションの場合は、シークレットパラメータ（ＳＰ）ＩＤ特定テーブルのみを自己のメモリ領域にコピーする。一方、コンテンツのＴＳ（トランスポートストリーム）に多重化されたＦＵＴブロックを利用せず、変換テーブルファイル内の変換テーブルブロックに記録された変換データを利用する再生（プレーヤ）アプリケーション、すなわち、先に図９を参照して説明した処理を実行する再生（プレーヤ）アプリケーション（ＦＵＴプリロード・タイプのプレーヤ）の場合は変換テーブル全体を、自己のメモリ領域にコピーする。

【０１８５】

次に、ステップＳ４０４において、再生（プレーヤ）アプリケーションは、タイトルに対応するクリップ情報を取得し、クリップ情報に含まれるＥＰマップから再生開始点に対応するソースパケットナンバー（ＳＰＮ）の値を取得する。

【０１８６】

次に、ステップＳ４０５において、ＥＰマップから取得したＳＰＮに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）から、再生点のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を特定する。この処理は、図１８を参照して説明した処理である。

【０１８７】

次に、ステップＳ４０６において、セキュアＶＭに対して、取得したシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を伝え、シークレットパラメータ（ＳＰ）値算出要求を出力する。この処理は、図１０を参照して説明したステップＳ１３の処理に相当する。

【０１８８】

次に、ステップＳ４０７において、再生（プレーヤ）アプリケーションは、セキュアＶＭにおいて算出したセグメント対応のシークレットパラメータ（ＳＰ）値を取得し、シークレットパラメータ（ＳＰ）に基づいて変換テーブルブロックの復元を実行して、復元した変換テーブルブロックに格納された変換エントリを取得し、変換エントリに記録された変換データおよびその記録位置に基づいて、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理を行い、ステップＳ４０８において、デコードおよび再生処理を実行する。

【０１８９】

さらに、次のセグメントに移行する場合は、ステップＳ４１０において、次の再生セグメントのＳＰＮをＥＰマップから取得し、ステップＳ４０５以下の処理を実行する。すなわち、ＥＰマップから取得したＳＰＮに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）からセグメント対応のＳＰ＿ＩＤを取得、取得したＳＰ＿ＩＤをセキュアＶＭに通知して、セグメント対応のＳＰ値を取得し、取得ＳＰ値に基づいて変換テーブルブロックを復元して、復元変換テーブルブロックから変換エントリ取得、変換エントリから変換データおよび記録位置を抽出して、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理をセグメント毎に実行する。

【０１９０】

これらの処理によって、各セグメントごとに異なるシークレットパラメータ（ＳＰ）を適用した処理が行なわれる。

【０１９１】

次に、図２４を参照して、ランダムアクセスなどの特殊再生処理を行なう場合の処理シーケンスについて説明する。なお図２４に示す処理は、タイトル初期化処理語の処理シーケンスのみを示している。すなわち、図２３に示す処理フローにおける処理ステップＳ４０１～Ｓ４０３が終了した後の処理を示している。

【０１９２】

まず、ステップＳ４２１において、再生（プレーヤ）アプリケーションは、ランダムアクセスなどの特殊再生処理の要求に応じて、クリップ情報からＥＰマップを取得し、取得ＥＰマップから再生開始点に対応するソースパケットナンバー（ＳＰＮ）の値を取得する。

【０１９３】

次に、ステップＳ４２２において、ＥＰマップから取得したＳＰＮに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）から、再生点のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を特定する。この処理は、図１８を参照して説明した処理である。

【０１９４】

次に、ステップＳ４２３において、セキュアＶＭに対して、取得したシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を伝え、シークレットパラメータ（ＳＰ）値算出要求を出力する。この処理は、図１０を参照して説明したステップＳ１３の処理に相当する。

【０１９５】

次に、ステップＳ４２４において、再生（プレーヤ）アプリケーションは、セキュアＶＭにおいて算出したセグメント対応のシークレットパラメータ（ＳＰ）値を取得し、シークレットパラメータ（ＳＰ）に基づいて変換テーブルブロックの復元を実行して、復元した変換テーブルブロックに格納された変換エントリを取得し、変換エントリに記録された変換データおよびその記録位置に基づいて、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理を行い、ステップＳ４２５において、デコードおよび再生処理を実行する。

【０１９６】

さらに、次のセグメントに移行する場合は、ステップＳ４３０において、次の再生セグメントのＳＰＮをＥＰマップから取得し、ステップＳ４２２以下の処理を実行する。すなわち、ＥＰマップから取得したＳＰＮに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）からセグメント対応のＳＰ＿ＩＤを取得、取得したＳＰ＿ＩＤをセキュアＶＭに通知して、セグメント対応のＳＰ値を取得し、取得ＳＰ値に基づいて変換テーブルブロックを復元して、復元変換テーブルブロックから変換エントリ取得、変換エントリから変換データおよび記録位置を抽出して、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理をセグメント毎に実行する。

【０１９７】

上述したように、本処理例では、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、まず、再生対象コンテンツデータのセグメントに対応するＳＰＮ（ソースパケットナンバー）を、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマ

ップから取得し、その後、取得したＳＰＮ（ソースパケットナンバー）に基づいて、シークレットパラメータＩＤ特定テーブルを検索して、取得ＳＰＮ（ソースパケットナンバー）に対応して設定されたＳＰ識別子（ＳＰ＿ＩＤ）を取得して、取得したＳＰ識別子（ＳＰ＿ＩＤ）をセキュアＶＭに通知して、シークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する構成としたので、各セグメントに対応するシークレットパラメータ（ＳＰ）を順次、セキュアＶＭから正確に受領して、正確なデータ変換を実行しながらコンテンツ再生を行なうことができる。

【０１９８】

（６．２）セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例２

次に、セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例２について説明する。本処理例においては、シークレットパラメータＩＤ特定テーブルを、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）と、ＥＰマップの登録テーブル識別情報（ＥＰマップ登録テーブルＩＤ）との対応データを格納した構成とする。

【０１９９】

コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、まず、再生対象コンテンツデータに対応するクリップ情報からＥＰマップを取得し、ＥＰマップに対応するＥＰマップの登録テーブル識別情報（ＥＰマップ登録テーブルＩＤ）に基づいて、シークレットパラメータＩＤ特定テーブルからＥＰマップ登録テーブルＩＤに対応して設定されたＳＰ識別子（ＳＰ＿ＩＤ）を取得する。

【０２００】

再生（プレーヤ）アプリケーションは、セキュアＶＭに対して、シークレットパラメータＩＤ特定テーブルから取得したＳＰ識別子（ＳＰ＿ＩＤ）を通知してシークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する。

【０２０１】

以下、図面を参照して、本処理例について詳細に説明する。図２５は、本処理例において適用するＳＰ＿ＩＤ特定テーブル［SPChangePositionTable］のデータ構成例を示す図である。なお、本処理例でも、変換テーブルの構成は先の処理例１と同様、図１９に示す構成を持つ。ＳＰ＿ＩＤ特定テーブル［SPChangePositionTable］のデータ構成のみが処理例１と異なる。

【０２０２】

図２５に示すＳＰ＿ＩＤ特定テーブルは、ＥＰマップ登録テーブルＩＤとシークレットパラメータＩＤ（ＳＰ＿ＩＤ）との対応データを格納している。具体的には、コンテンツの構成データとしてのセグメント(SP_segment)の先頭パケットの情報を含むＥＰマップのＥＰマップ登録テーブルＩＤと、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）との対応データを格納している。ＳＰ＿ＩＤ特定テーブルには、以下のデータが含まれる。

Clip_ID：クリップＩＤ

Number of SP (= NSP)：セグメント（SP_segment）数

SP_segment_start_EP_map_id：ＳＰ＿ＩＤに対応するセグメント（SP_segment）の先頭をＥＰマップ登録テーブルＩＤ（EP_map_id）で指定したものであり、この値を使って再生したいソースパケットナンバー（ＳＰＮ）に該当するＥＰマップ登録テーブルＩＤ（EP_map_id）からＳＰ＿ＩＤを取得することができる

【０２０３】

再生アプリケーションは、ＳＰ＿ＩＤに対応するセグメント（SP_segment）の先頭のパケットを含むＥＰマップの登録テーブルＩＤを取得して、ＥＰマップ登録テーブルＩＤに基づいて、図２５に示すＳＰ＿ＩＤ特定テーブルから、セグメント対応のＳＰ＿ＩＤを取得することができる。

【０２０４】

図２５に示すＳＰ＿ＩＤ特定テーブルを適用して、セグメント毎に異なるシークレットパラメータ（ＳＰ）を取得して変換データによるデータ置き換えを伴うコンテンツ再生処理シーケンスについて図２６に示すフローチャートを参照して説明する。

【０２０５】
まず、ステップＳ５０１において、再生（プレーヤ）アプリケーションは、再生するタイトルを決定し、セキュアＶＭに対して、タイトル初期化命令を発行する。ステップＳ５０２では、セキュアＶＭは、タイトル初期化処理を実行し、タイトルに対応する変換テーブル（FixUpTable）の生成処理を実行する。これは、先に、図１０、図１１を参照して説明した処理であり、図１０に示すシーケンス図のステップＳ１２の処理に対応する。
【０２０６】
ステップＳ５０３において、再生（プレーヤ）アプリケーションは、変換テーブル（FixUpTable）から必要な情報を取得する。これは、先に、図１１を参照して説明した処理であり、セキュアＶＭのメモリ領域に格納された変換テーブルから、必要な情報を再生（プレーヤ）アプリケーションの利用可能なメモリ領域にコピーする処理として実行される。
【０２０７】
コンテンツのＴＳ（トランスポートストリーム）に多重化されたＦＵＴブロックから変換エントリを取り出してデータ変換を実行する再生（プレーヤ）アプリケーション、すなわち、先に図８を参照して説明した処理を実行する再生（プレーヤ）アプリケーションの場合は、シークレットパラメータ（ＳＰ）ＩＤ特定テーブルのみを自己のメモリ領域にコピーする。一方、コンテンツのＴＳ（トランスポートストリーム）に多重化されたＦＵＴブロックを利用せず、変換テーブルファイル内の変換テーブルブロックに記録された変換データを利用する再生（プレーヤ）アプリケーション、すなわち、先に図９を参照して説明した処理を実行する再生（プレーヤ）アプリケーション（ＦＵＴプリロード・タイプのプレーヤ）の場合は変換テーブル全体を、自己のメモリ領域にコピーする。
【０２０８】
次に、ステップＳ５０４において、再生（プレーヤ）アプリケーションは、タイトルに対応するクリップ情報を取得し、クリップ情報に含まれるＥＰマップを決定し、決定したＥＰマップの登録テーブル識別情報としてのＥＰマップ登録テーブルＩＤの値を取得する。
【０２０９】
次に、ステップＳ５０５において、ＥＰマップ登録テーブルＩＤに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）から、再生点のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を特定する。図２５に示すシークレットパラメータＩＤ（ＳＰ＿ＩＤ）と、ＥＰマップの登録テーブル識別情報（ＥＰマップ登録テーブルＩＤ）との対応データを格納したＳＰ＿ＩＤ特定テーブルを利用する。
【０２１０】
次に、ステップＳ５０６において、セキュアＶＭに対して、取得したシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を伝え、シークレットパラメータ（ＳＰ）値算出要求を出力する。この処理は、図１０を参照して説明したステップＳ１３の処理に相当する。
【０２１１】
次に、ステップＳ５０７において、再生（プレーヤ）アプリケーションは、セキュアＶＭにおいて算出したセグメント対応のシークレットパラメータ（ＳＰ）値を取得し、シークレットパラメータ（ＳＰ）に基づいて変換テーブルブロックの復元を実行して、復元した変換テーブルブロックに格納された変換エントリを取得し、変換エントリに記録された変換データおよびその記録位置に基づいて、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理を行い、ステップＳ５０８において、デコードおよび再生処理を実行する。
【０２１２】
さらに、次のセグメントに移行する場合は、ステップＳ５１０において、次の再生セグメントの最初のパケットの情報を含むＥＰマップのＥＰマップ登録テーブルＩＤを取得し、ステップＳ５０５以下の処理を実行する。すなわち、取得したＥＰマップ登録テーブルＩＤに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）からＥＰマップ登録テーブルＩＤに対応付けられたＳＰ＿ＩＤを取得、取得したＳＰ＿ＩＤをセキュアＶ

Ｍに通知して、セグメント対応のＳＰ値を取得し、取得ＳＰ値に基づいて変換テーブルブロックを復元して、復元変換テーブルブロックから変換エントリ取得、変換エントリから変換データおよび記録位置を抽出して、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理をセグメント毎に実行する。

【０２１３】

これらの処理によって、各セグメントごとに異なるシークレットパラメータ（ＳＰ）を適用した処理が行なわれる。

【０２１４】

次に、図２７を参照して、ランダムアクセスなどの特殊再生処理を行なう場合の処理シーケンスについて説明する。なお図２７に示す処理は、タイトル初期化処理語の処理シーケンスのみを示している。すなわち、図２６に示す処理フローにおける処理ステップＳ５０１～Ｓ５０３が終了した後の処理を示している。

【０２１５】

まず、ステップＳ５２１において、再生（プレーヤ）アプリケーションは、ランダムアクセスなどの特殊再生処理の要求に応じて、クリップ情報の利用ＥＰマップを特定し、特定したＥＰマップの登録テーブル識別子（ＥＰマップ登録テーブルＩＤ）の値を取得する。

【０２１６】

次に、ステップＳ５２２において、取得したＥＰマップ登録テーブルＩＤに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）から、ＥＰマップ登録テーブルＩＤに対応する再生点のシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を特定する。

【０２１７】

次に、ステップＳ５２３において、セキュアＶＭに対して、取得したシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を伝え、シークレットパラメータ（ＳＰ）値算出要求を出力する。この処理は、図１０を参照して説明したステップＳ１３の処理に相当する。

【０２１８】

次に、ステップＳ５２４において、再生（プレーヤ）アプリケーションは、セキュアＶＭにおいて算出したセグメント対応のシークレットパラメータ（ＳＰ）値を取得し、シークレットパラメータ（ＳＰ）に基づいて変換テーブルブロックの復元を実行して、復元した変換テーブルブロックに格納された変換エントリを取得し、変換エントリに記録された変換データおよびその記録位置に基づいて、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理を行い、ステップＳ５２５において、デコードおよび再生処理を実行する。

【０２１９】

さらに、次のセグメントに移行する場合は、ステップＳ５３０において、次の再生セグメントの最初のパケットの情報を含むＥＰマップのＥＰマップ登録テーブルＩＤを取得し、ステップＳ５２２以下の処理を実行する。すなわち、取得したＥＰマップ登録テーブルＩＤに基づいて、ＳＰ＿ＩＤ特定テーブル（SPChangePositionTable ()）からＥＰマップ登録テーブルＩＤに対応付けられたＳＰ＿ＩＤを取得、取得したＳＰ＿ＩＤをセキュアＶＭに通知して、セグメント対応のＳＰ値を取得し、取得ＳＰ値に基づいて変換テーブルブロックを復元して、復元変換テーブルブロックから変換エントリ取得、変換エントリから変換データおよび記録位置を抽出して、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理をセグメント毎に実行する。

【０２２０】

上述したように、本処理例では、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、まず、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマップから、再生対象コンテンツデータのセグメントの開始位置に対応するパケット情報を格納したＥＰマップを特定し、そのＥＰマップの登録テーブル識別子（ＥＰマップ登録テーブルＩＤ）に基づいて、シークレットパラメータＩＤ特定テーブルを検索して、ＥＰマップ登録テーブルＩＤに対応して設定されたＳＰ識別子（ＳＰ＿ＩＤ）を取得して、取得し

たＳＰ識別子（ＳＰ＿ＩＤ）をセキュアＶＭに通知して、シークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する構成としたので、各セグメントに対応するシークレットパラメータ（ＳＰ）を順次、セキュアＶＭから正確に受領して、正確なデータ変換を実行しながらコンテンツ再生を行なうことができる。

【０２２１】

（６．３）セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例３

次に、セグメント対応のＳＰ識別子（ＳＰ＿ＩＤ）取得処理例３について説明する。本処理例においては、コンテンツに設定されるセグメントを、予め規定したＥＰマップ登録テーブル数に基づいて区分する設定とする。すなわち、ＥＰマップ登録テーブル数Ｎ個分に相当する再生開始位置を示すエントリポイントを持つコンテンツの区分領域を１セグメントとする。Ｎは１以上の整数である。

【０２２２】

コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、再生対象コンテンツデータに対応するクリップ情報からＥＰマップを取得し、ＥＰマップに基づいて、コンテンツを構成するＴＳパケットを順次取得して再生を行なう。先に、図１５を参照して説明したように、ＥＰマップは、ＧＯＰ毎に設定されており、再生（プレーヤ）アプリケーションは、クリップ情報に含まれるＥＰマップを取得して、再生パケットを抽出して再生処理を実行する。

【０２２３】

本処理例では、再生（プレーヤ）アプリケーションは、利用するＥＰマップに対応するＥＰマップ登録テーブルＩＤを適用して、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）を算出する。あるいは、再生（プレーヤ）アプリケーションは、利用するＥＰマップ登録テーブル数をカウントして、セグメント（Ｎ個のＥＰマップ登録テーブル数に対応）を構成するＥＰマップ登録テーブル数（Ｎ）になる毎に、セグメントの切り替えが発生すると判断して、変換テーブルブロックの復元に適用するシークレットパラメータ（ＳＰ）を切り替える処理を実行する。

【０２２４】

再生（プレーヤ）アプリケーションは、セキュアＶＭに対して、セグメント（ｎ個のＥＰマップ登録テーブル数に対応）に対応付けられるＥＰマップ登録テーブル数（ｎ）になる毎に、順次、インクリメントしたＳＰ識別子（ＳＰ＿ＩＤ）を通知してシークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する。

【０２２５】

以下、図面を参照して、本処理例について詳細に説明する。図２８は、本処理例において適用する（ａ）コンテンツ構成と、（ｂ）ＥＰマップ構成データを示している。（ａ）コンテンツ構成に示すように、コンテンツはＧＯＰによって区分され、各ＧＯＰ内のＩピクチャに関する情報がＥＰマップ登録テーブルにそれぞれ記録される。図２８（ｂ）のＥＰマップ構成データに示すように、ＥＰマップには、複数のＥＰマップ登録テーブルが記録され、各ＥＰマップ登録テーブルにＩピクチャについてのアドレス情報であるＳＰＮ（ソースパケットナンバー）と、ＰＴＳ（プレゼンテーションタイムスタンプ）が対応付けられて記録される。

【０２２６】

このように、ＥＰマップは、複数のＥＰマップ登録テーブルを１つのファイルに格納したデータ構成を有する。ＥＰマップに登録されるテーブルには、テーブル番号を有し、これらはＥＰマップ登録テーブルＩＤとして識別される。

【０２２７】

本処理例では、セグメントを、ＥＰマップ登録テーブルＮ個分のデータ領域として設定する。図２８に示す例では、Ｎ＝５とした設定であり、ＥＰマップ登録テーブル５個が１つのセグメントとして設定される。図２８（ａ）に示すコンテンツ中、ＧＯＰ０～ＧＯＰ４、すなわちＥＰマップ登録テーブル０～ＥＰマップ登録テーブル４が１つのセグメントとして区分され、以下、ＧＯＰ５～ＧＯＰ９、すなわちＥＰマップ登録テーブル５～ＥＰ

マップ登録テーブル９が次の１つのセグメントとして区分される。以下同様に５ＧＯＰ（＝５ＥＰマップ登録テーブル）が１セグメントとして設定される。

【０２２８】

この場合、図２８（ｂ）に示すように、ＥＰマップ登録テーブル０～４に対応するセグメントにおいて適用するシークレットパラメータの識別子（ＳＰ＿ＩＤ）は［０］に設定され、以降、

ＥＰマップ登録テーブル５～９：ＳＰ＿ＩＤ＝１、

ＥＰマップ登録テーブル１０～１４：ＳＰ＿ＩＤ＝２、

ＥＰマップ登録テーブル１４～１９：ＳＰ＿ＩＤ＝３、

このように、５つのＥＰマップ登録テーブル毎にシークレットパラメータの識別子（ＳＰ＿ＩＤ）は１ずつ増加する設定とされる。

【０２２９】

コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、利用するＥＰマップ登録テーブルに対応するＥＰマップ登録テーブルＩＤを適用して、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）を算出する。シークレットパラメータＩＤ（ＳＰ＿ＩＤ）は、以下の算出式によって算出される０以上の整数部分を抽出することによって決定される。

ＳＰ＿ＩＤ＝（ＥＰマップ登録テーブルＩＤ）／Ｎ

上記式において、Ｎは、１セグメント中のＥＰマップ登録テーブル数に相当する。図２８の例では、

ＥＰマップ登録テーブル０～４：ＳＰ＿ＩＤ＝０、

ＥＰマップ登録テーブル５～９：ＳＰ＿ＩＤ＝１、

ＥＰマップ登録テーブル１０～１４：ＳＰ＿ＩＤ＝２、

：

として算出される。

【０２３０】

あるいは、上記算出式を適用せず、再生（プレーヤ）アプリケーションは、利用するＥＰマップ登録テーブルの数をカウントして、セグメント（Ｎ個のＥＰマップ登録テーブルに対応）を構成するＥＰマップ登録テーブル数（Ｎ）になる毎に、セグメントの切り替えが発生すると判断して、変換テーブルブロックの復元に適用するシークレットパラメータ（ＳＰ）を切り替える処理を実行する構成としてもよい。

【０２３１】

図２８に示す設定例ではＮ＝５であるので、５つのＥＰマップ登録テーブル毎にセグメント切り替えが発生すると判断し、５つのＥＰマップのカウント毎にＳＰ＿ＩＤを１つずつ増加させて、ＳＰ＿ＩＤを決定して、決定したＳＰ＿ＩＤをセキュアＶＭに出力して、セグメント対応のシークレットパラメータを取得する。もちろんＮ＝５以外の整数単位でセグメントを設定しても構わないことは明らかである。ただし、再生装置の処理時間を考慮して、複数のＥＰマップ登録テーブルのエントリポイントの単位で設定することが望ましい。

【０２３２】

本処理例では、上記の算出式、あるいはＥＰマップ登録テーブルのカウントに基づいて、セグメント毎の異なるＳＰ＿ＩＤを求めることが可能となり、先に説明した処理例１，２のようにソースパケットナンバー、あるいはＥＰマップ登録テーブルＩＤに基づいてシークレットパラメータＩＤを取得するシークレットパラメータＩＤ特定テーブルを利用する必要がない。

【０２３３】

本処理例を適用した場合の、セグメント毎の異なるシークレットパラメータ（ＳＰ）の取得、および変換データによるデータ置き換えを伴うコンテンツ再生処理シーケンスについて図２９に示すフローチャートを参照して説明する。

【０２３４】

まず、ステップＳ６０１において、再生（プレーヤ）アプリケーションは、再生するタ

イトルを決定し、セキュアＶＭに対して、タイトル初期化命令を発行する。ステップＳ６０２では、セキュアＶＭは、タイトル初期化処理を実行し、タイトルに対応する変換テーブル（FixUpTable）の生成処理を実行する。これは、先に、図１０、図１１を参照して説明した処理であり、図１０に示すシーケンス図のステップＳ１２の処理に対応する。

【０２３５】

ステップＳ６０３において、再生（プレーヤ）アプリケーションは、変換テーブル（FixUpTable）から必要な情報を取得する。これは、先に、図１１を参照して説明した処理であり、セキュアＶＭのメモリ領域に格納された変換テーブルから、必要な情報を再生（プレーヤ）アプリケーションの利用可能なメモリ領域にコピーする処理として実行される。

【０２３６】

コンテンツのＴＳ（トランスポートストリーム）に多重化されたＦＵＴブロックから変換エントリを取り出してデータ変換を実行する再生（プレーヤ）アプリケーション、すなわち、先に図８を参照して説明した処理を実行する再生（プレーヤ）アプリケーションの場合は、シークレットパラメータ（ＳＰ）ＩＤ特定テーブルのみを自己のメモリ領域にコピーする。一方、コンテンツのＴＳ（トランスポートストリーム）に多重化されたＦＵＴブロックを利用せず、変換テーブルファイル内の変換テーブルブロックに記録された変換データを利用する再生（プレーヤ）アプリケーション、すなわち、先に図９を参照して説明した処理を実行する再生（プレーヤ）アプリケーション（ＦＵＴプリロード・タイプのプレーヤ）の場合は変換テーブル全体を、自己のメモリ領域にコピーする。

【０２３７】

次に、ステップＳ６０４において、再生（プレーヤ）アプリケーションは、タイトルに対応するクリップ情報を取得し、クリップ情報に含まれるＥＰマップを決定し、決定したＥＰマップの登録テーブル識別情報としてのＥＰマップ登録テーブルＩＤの値を取得する。

【０２３８】

次に、ステップＳ６０５において、ＥＰマップ登録テーブルＩＤに基づいて、ＳＰ＿ＩＤを算出する。例えば、１つのセグメントに含まれるＥＰマップ登録テーブル数をＮとしたとき、

ＳＰ＿ＩＤ＝（ＥＰマップ登録テーブルＩＤ）／Ｎ

によって、ＳＰ＿ＩＤを算出する。

【０２３９】

次に、ステップＳ６０６において、セキュアＶＭに対して、取得したシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を伝え、シークレットパラメータ（ＳＰ）値算出要求を出力する。この処理は、図１０を参照して説明したステップＳ１３の処理に相当する。

【０２４０】

次に、ステップＳ６０７において、再生（プレーヤ）アプリケーションは、セキュアＶＭにおいて算出したセグメント対応のシークレットパラメータ（ＳＰ）値を取得し、シークレットパラメータ（ＳＰ）に基づいて変換テーブルブロックの復元を実行して、復元した変換テーブルブロックに格納された変換エントリを取得し、変換エントリに記録された変換データおよびその記録位置に基づいて、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理を行い、ステップＳ６０８において、デコードおよび再生処理を実行する。

【０２４１】

さらに、次のセグメントに移行する場合は、ステップＳ６１０において、次の再生セグメントの最初のパケットの情報を含むＥＰマップのＥＰマップ登録テーブルＩＤを取得し、ステップＳ６０５以下の処理を実行する。すなわち、取得したＥＰマップ登録テーブルＩＤに基づいて、ＳＰ＿ＩＤを算出し、算出したＳＰ＿ＩＤをセキュアＶＭに通知して、セグメント対応のＳＰ値を取得し、取得ＳＰ値に基づいて変換テーブルブロックを復元して、復元変換テーブルブロックから変換エントリ取得、変換エントリから変換データおよび記録位置を抽出して、コンテンツのセグメント中のデータを変換データに置き換えるデ

ータ変換処理をセグメント毎に実行する。

【０２４２】

これらの処理によって、各セグメントごとに異なるシークレットパラメータ（ＳＰ）を適用した処理が行なわれる。なお、前述したように、ＥＰマップ登録テーブルＩＤを適用した算出式に基づいてＳＰ＿ＩＤを求めるのではなく、ＥＰマップ登録テーブル数をカウントして、ＳＰ＿ＩＤを求める設定としてもよい。

【０２４３】

次に、図３０を参照して、ランダムアクセスなどの特殊再生処理を行なう場合の処理シーケンスについて説明する。なお図３０に示す処理は、タイトル初期化処理語の処理シーケンスのみを示している。すなわち、図２９に示す処理フローにおける処理ステップＳ６０１～Ｓ６０３が終了した後の処理を示している。

【０２４４】

まず、ステップＳ６２１において、再生（プレーヤ）アプリケーションは、ランダムアクセスなどの特殊再生処理の要求に応じて、クリップ情報の利用ＥＰマップ登録テーブルを特定し、特定したＥＰマップ登録テーブルの識別子（ＥＰマップ登録テーブルＩＤ）の値を取得する。

【０２４５】

次に、ステップＳ６２２において、取得したＥＰマップ登録テーブルＩＤに基づいて、算出式、

ＳＰ＿ＩＤ＝（ＥＰマップ登録テーブルＩＤ）／Ｎ

によって、ＳＰ＿ＩＤを算出する。

【０２４６】

次に、ステップＳ６２３において、セキュアＶＭに対して、取得したシークレットパラメータＩＤ（ＳＰ＿ＩＤ）を伝え、シークレットパラメータ（ＳＰ）値算出要求を出力する。この処理は、図１０を参照して説明したステップＳ１３の処理に相当する。

【０２４７】

次に、ステップＳ６２４において、再生（プレーヤ）アプリケーションは、セキュアＶＭにおいて算出したセグメント対応のシークレットパラメータ（ＳＰ）値を取得し、シークレットパラメータ（ＳＰ）に基づいて変換テーブルブロックの復元を実行して、復元した変換テーブルブロックに格納された変換エントリを取得し、変換エントリに記録された変換データおよびその記録位置に基づいて、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理を行い、ステップＳ６２５において、デコードおよび再生処理を実行する。

【０２４８】

さらに、次のセグメントに移行する場合は、ステップＳ６３０において、次の再生セグメントの最初のパケットの情報を含むＥＰマップのＥＰマップ登録テーブルＩＤを取得し、ステップＳ６２２以下の処理を実行する。すなわち、取得したＥＰマップ登録テーブルＩＤに基づいて、ＳＰ＿ＩＤを算出、算出したＳＰ＿ＩＤをセキュアＶＭに通知して、セグメント対応のＳＰ値を取得し、取得ＳＰ値に基づいて変換テーブルブロックを復元して、復元変換テーブルブロックから変換エントリ取得、変換エントリから変換データおよび記録位置を抽出して、コンテンツのセグメント中のデータを変換データに置き換えるデータ変換処理をセグメント毎に実行する。なお、本例においても算出式を適用せずＥＰマップ登録テーブル数のカウントに基づいてＳＰ＿ＩＤを求める構成としてもよい。

【０２４９】

上述したように、本処理例では、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、まず、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマップから、再生対象コンテンツデータに対応するＥＰマップ登録テーブルを特定し、そのＥＰマップ登録テーブルの識別子（ＥＰマップ登録テーブルＩＤ）に基づいて、シークレットパラメータＩＤ（ＳＰ＿ＩＤ）を、算出式を適用して求めるか、またはＥＰマップ登録テーブル数のカウントによって求め、取得したＳＰ識別子（ＳＰ＿ＩＤ）をセキュアＶＭ

に通知して、シークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する構成としたので、特別なパラメータＩＤ特定テーブルを適用することなくＳＰ識別子（ＳＰ＿ＩＤ）を取得して、各セグメントに対応するシークレットパラメータ（ＳＰ）を順次、セキュアＶＭから正確に受領して、正確なデータ変換を実行しながらコンテンツ再生を行なうことができる。

【０２５０】

［７．情報処理装置の構成］

次に、図３１を参照して、上述した再生（プレーヤ）アプリケーションおよびセキュアＶＭの処理を実行する情報処理装置のハードウェア構成例について説明する。情報処理装置８００は、ＯＳやコンテンツ再生または記録アプリケーションプログラム、相互認証処理、コンテンツ再生に伴う様々な処理、例えば、上述したデータ変換処理などを含む各種プログラムに従ったデータ処理を実行するＣＰＵ８０９、プログラム、パラメータ等の記憶領域としてのＲＯＭ８０８、メモリ８１０、デジタル信号を入出力する入出力Ｉ／Ｆ８０２、アナログ信号を入出力し、Ａ／Ｄ，Ｄ／Ａコンバータ８０５を持つ入出力Ｉ／Ｆ８０４、ＭＰＥＧデータのエンコード、デコード処理を実行するＭＰＥＧコーデック８０３、ＴＳ（Transport Stream）・ＰＳ(Program Stream)処理を実行するＴＳ・ＰＳ処理手段８０６、相互認証、暗号化コンテンツの復号処理など各種の暗号処理を実行する暗号処理手段８０７、ハードディスクなどの記録媒体８１２、記録媒体８１２の駆動、データ記録再生信号の入出力を行なうドライブ８１１を有し、バス８０１に各ブロックが接続されている。

【０２５１】

情報処理装置（ホスト）８００は、例えばＡＴＡＰＩ－ＢＵＳ等の接続バスによってドライブと接続されている。変換テーブル、コンテンツなどをデジタル信号用入出力Ｉ／Ｆ８０２を介して入出力される。暗号化処理、復号処理は、暗号化処理手段８０７によって、例えば、ＡＥＳアルゴリズムなどを適用して実行される。

【０２５２】

なお、コンテンツ再生あるいは記録処理を実行するプログラムは例えばＲＯＭ８０８内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ８１０を使用する。

【０２５３】

ＲＯＭ８０８または記録媒体８１２には、例えば、管理センタの公開鍵、ホスト対応秘密鍵、ホスト対応の公開鍵証明書、さらに、リボケーションリストとしてのドライブＣＲＬなどが格納される。

【０２５４】

コンテンツ再生または外部出力に際しては、情報記録媒体から取得したデータ変換処理プログラムを適用して、暗号化コンテンツの復号と、変換テーブルの復元、変換テーブルの格納データに基づく変換データの書き込み処理など、先に説明した処理例の各処理シーケンスに従った処理を実行する。

【０２５５】

［８．情報記録媒体製造装置および情報記録媒体］

次に、情報記録媒体製造装置および情報記録媒体について説明する。すなわち、上述したコンテンツ再生処理において適用される情報記録媒体の製造装置、方法、および情報記録媒体について説明する。

【０２５６】

情報記録媒体製造装置は、例えば、先に図１を参照して説明した記録データを格納した情報記録媒体１００を製造する装置である。

情報記録媒体製造装置は、

正当コンテンツ構成データと異なるブロークンデータを含むコンテンツと、

ブロークンデータの置き換え対象となる変換データを、コンテンツの区分領域であるセグメントに対応して設定されるパラメータによって演算または暗号化処理を施して記録し

た変換テーブルボディデータと、パラメータの識別情報としてのパラメータ識別子を記録したパラメータ識別子特定テーブルを含む変換テーブルとを生成するデータ処理部と、ブロークンデータを含むコンテンツと、変換テーブルとを情報記録媒体に記録するデータ記録部とを有する。

【０２５７】

情報記録媒体製造装置の一実施例構成におけるデータ処理部の生成するパラメータ識別子特定テーブルの１つの例は、先に、図２０を参照して説明したパラメータ識別子と、コンテンツ構成データとしてのセグメントの先頭の位置にあるパケットのパケットナンバーを対応付けたテーブルである。

【０２５８】

あるいは、情報記録媒体製造装置の一実施例構成におけるデータ処理部の生成するパラメータ識別子特定テーブルのもう１つの例は、先に、図２５を参照して説明したパラメータ識別子と、コンテンツ構成データとしてのセグメントの先頭の位置にあるパケットの情報を含むＥＰマップの登録テーブル識別子としてのＥＰマップ登録テーブルＩＤを対応付けたテーブルである。

【０２５９】

このような、製造装置によって生成された情報記録媒体は、図１他を参照して説明したように、

（ａ）正当コンテンツ構成データと異なるブロークンデータを含むコンテンツと、

（ｂ）ブロークンデータの置き換え対象となる変換データを、コンテンツの区分領域であるセグメントに対応して設定されるパラメータによって演算または暗号化処理を施して記録した変換テーブルボディデータと、パラメータの識別情報としてのパラメータ識別子を記録したパラメータ識別子特定テーブルを含む変換テーブルと、

記録データとして格納した情報記録媒体となる。

【０２６０】

一実施例において、情報記録媒体に記録される変換テーブルは、先に、図２０を参照して説明したパラメータ識別子と、コンテンツ構成データとしてのセグメントの先頭の位置にあるパケットのパケットナンバーを対応付けたテーブルである。先に、図２５を参照して説明したパラメータ識別子と、コンテンツ構成データとしてのセグメントの先頭の位置にあるパケットの情報を含むＥＰマップの登録テーブル識別子としてのＥＰマップ登録テーブルＩＤを対応付けたテーブルである。

【０２６１】

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。

【０２６２】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０２６３】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、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。

【０２６４】

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、コンピュータに無線転送したり、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受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０２６５】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０２６６】

以上、説明したように、本発明の一実施例の構成によれば、コンテンツの区分領域として設定されたセグメント毎に異なるパラメータによる演算または暗号処理によって変換データを復元、取得して、取得した変換データによって、コンテンツの一部データの置き換えを行いながらコンテンツ再生を実行する構成において、再生対象コンテンツのセグメントに含まれるパケットのＳＰＮ（ソースパケットナンバー）と、パラメータＩＤ（ＳＰ＿ＩＤ）を対応付けたテーブル、または、再生対象コンテンツのセグメントに含まれるパケットの情報を格納したＥＰマップの登録テーブル識別子（ＥＰマップ登録テーブルＩＤ）とパラメータＩＤを対応付けたテーブルに基づいて、セグメント対応のパラメータＩＤを取得して、取得したパラメータＩＤ（ＳＰ＿ＩＤ）をセキュアＶＭに通知して、シークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する構成としたので、各セグメントに対応するシークレットパラメータ（ＳＰ）を順次、セキュアＶＭから正確に受領して、正確なデータ変換を実行しながらコンテンツ再生を行なうことができる。

【０２６７】

また、本発明の一実施例構成によれば、コンテンツ再生を実行する再生（プレーヤ）アプリケーションは、まず、コンテンツ再生区間情報としてのクリップ情報に記録されたＥＰマップから、再生対象コンテンツデータに対応するＥＰマップを特定し、そのＥＰマップの登録テーブル識別子（ＥＰマップ登録テーブルＩＤ）に基づいて、パラメータＩＤ（ＳＰ＿ＩＤ）を、算出式を適用して求めるか、またはＥＰマップ登録テーブル数のカウントによって求め、取得したパラメータＩＤ（ＳＰ＿ＩＤ）をセキュアＶＭに通知して、シークレットパラメータ算出要求（ＩＮＴＲＰ）を実行する構成としたので、特別なパラメータＩＤ特定テーブルを適用することなくパラメータＩＤ（ＳＰ＿ＩＤ）を取得して、各セグメントに対応するシークレットパラメータ（ＳＰ）を順次、セキュアＶＭから正確に受領して、正確なデータ変換を実行しながらコンテンツ再生を行なうことができる。

【符号の説明】

【０２６８】

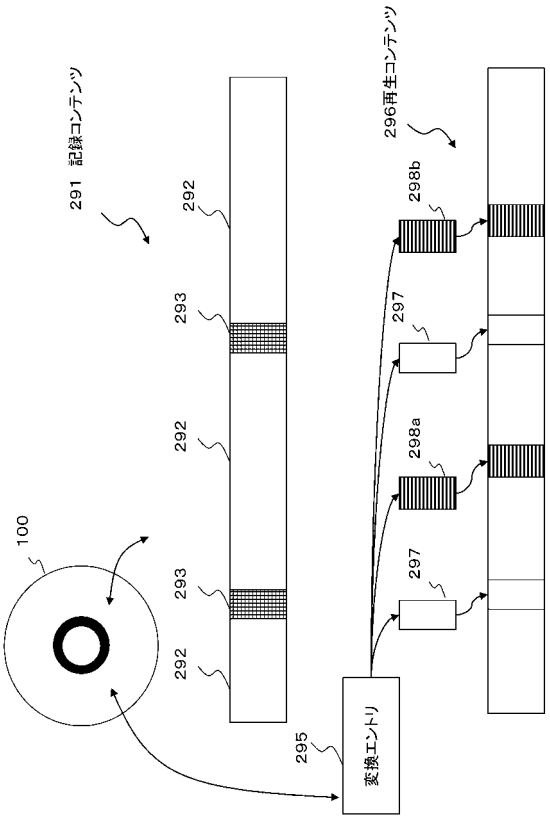
１００　情報記録媒体
１０１　暗号化コンテンツ
１０２　ＭＫＢ
１０３　タイトル鍵ファイル
１０４　使用許諾情報
１０５　変換テーブル
１０６　データ変換処理プログラム
１２０　ドライブ
１２１　データ処理部
１２２　メモリ
１４０　ホスト

１５０　再生（プレーヤアプリケーション）
１５１　データ処理部
１５２　メモリａ
１５３　復号処理部
１５４　データ変換処理部
１５５　デコード処理部
１５６　メモリｂ
１６０　セキュアＶＭ
２１０　インデックス
２２０　ムービーオブジェクト
２３０　プレイリスト
２４０　クリップ
２６１，２６２，２６３　ＡＶストリーム
２７１，２７２　コンテンツ管理ユニット（ＣＰＳユニット）
２８１　データ部
２９１　記録コンテンツ
２９２　コンテンツデータ
２９３　ブロークンデータ
２９５　変換エントリ
２９６　再生コンテンツ
２９７　変換データ
２９８　識別子設定変換データ
３００　データ変換処理プログラム
３０１　変換テーブル
３０２　シークレットパラメータ（ＳＰ）ＩＤ特定テーブル
３０３ａ　変換テーブルボティ
３０３ｂ　変換テーブル集合
３０４　変換テーブルブロック
３０５　変換エントリ
３０６　暗号化コンテンツ
３０７　ＴＳパケット
３０８，３０９　ＴＳパケット
３１１～３１４　パケット
３１５　ＸＯＲｅｄ変換エントリ
３１６　シークレットパラメータ
３１７　変換エントリ
３２０　セキュアＶＭ
３３０　情報記録媒体
３３１　ＭＫＢ
３３２　タイトル鍵ファイル
３３３　暗号化コンテンツ
３３４　変換テーブル
３３５　データ変換処理プログラム
３４０　ドライブ
３４５　ホスト
３５０　再生（プレーヤ）アプリケーション
３５１　デバイス鍵
３５２　トラックバッファ
３５３　平文ＴＳバッファ
３５４　イベントハンドラ

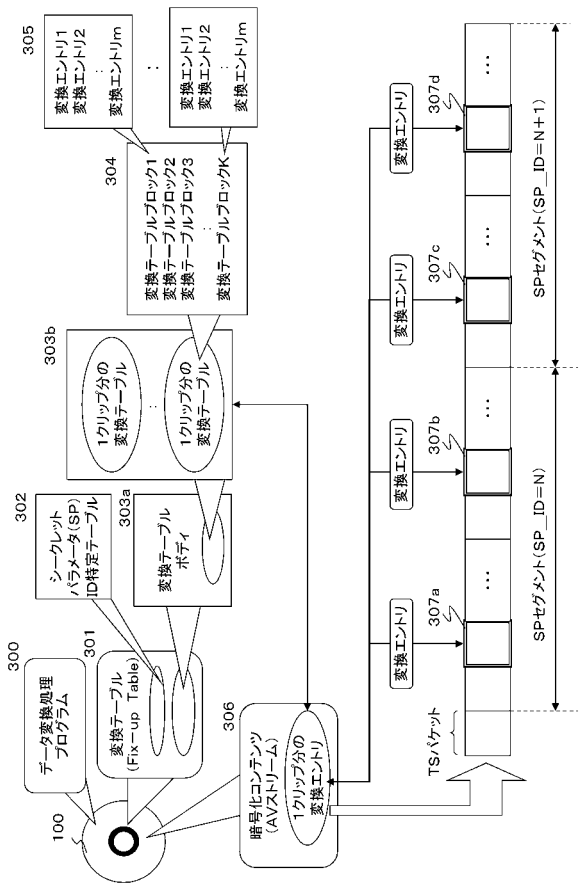
３５５　プレーヤ情報
３５６　リアルタイムイベントハンドラ
３６０　セキュアＶＭブロック
３６１　セキュアＶＭ
４０１　トラックバッファ格納データ
４０２　復号結果データ
４０３　ブロークンデータ
４０４　変換データ
４０５　識別子設定変換データ
４１１　Ｉピクチャ
４１２　ＥＰマップ
８００　情報処理装置
８０１　バス
８０２　入出力Ｉ／Ｆ
８０３　ＭＰＥＧコーデック
８０４　入出力Ｉ／Ｆ
８０５　Ａ／Ｄ，Ｄ／Ａコンバータ
８０６　ＴＳ・ＰＳ処理手段
８０７　暗号処理手段
８０８　ＲＯＭ
８０９　ＣＰＵ
８１０　メモリ
８１１　ドライブ
８１２　記録媒体

【図３】

【図４】



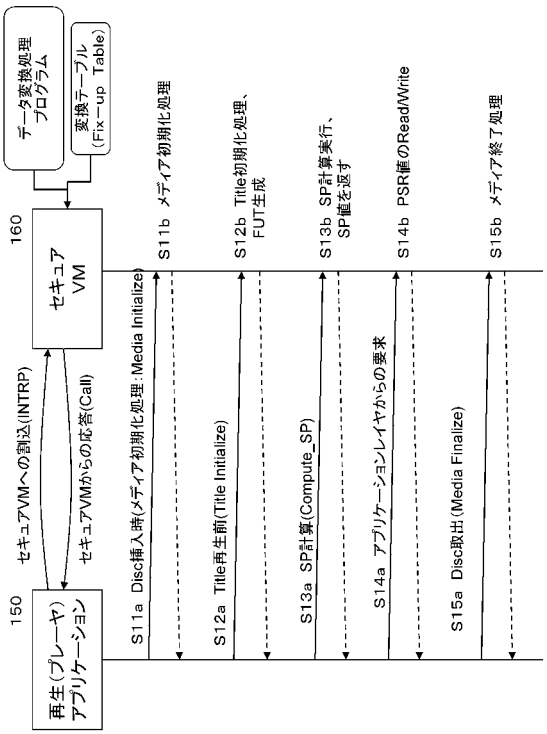
【図６】



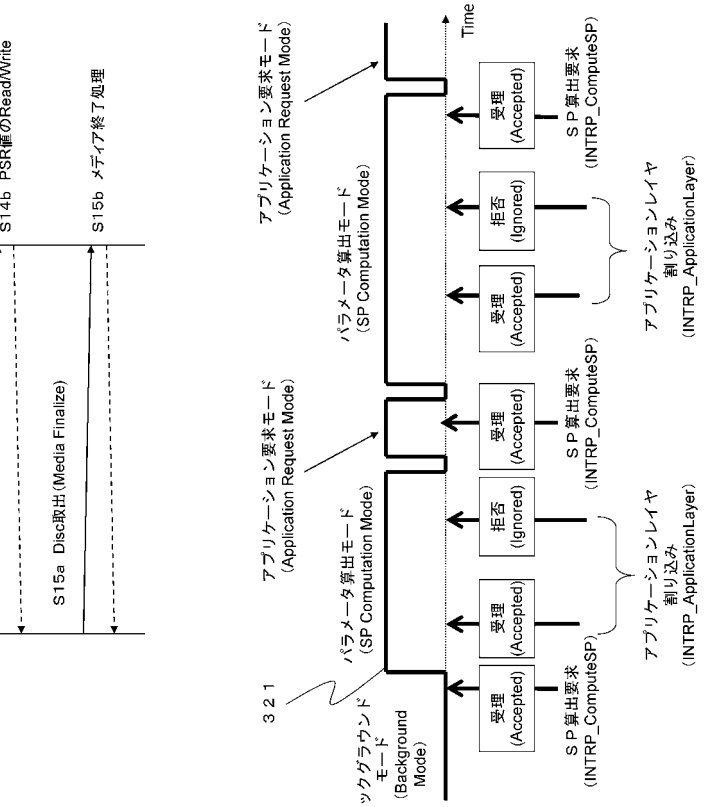
【図７】

FixUpEntry() {	Bits	Description
type_indicator	2	タイプ識別子[00:変換なし, 01b:変換データによる処理, 10b,11b:識別マーク入り変換データによる処理] 00b:no transform, 01b:transform, 10b and 11b:forensic
FM_ID_bit_position	6	識別マーク入り変換データに対応するプレーヤIDの識別ビット位置 Indicate bit position of Player ID for forensic (MSB is second bit of type_indicator)
relative_SPN	12	変換データ適用パケット位置(PMTパケットからのパケット数) Relative packet number from PMT to transformed packet
byte_position	8	パケット内の変換データ記録位置 Start byte position of transformed data in the packet (more than 5)
overwrite_value	5x8	変換データ Value to be overwritten
relative_SPN_2	12	第2変換データ適用パケット位置(PMTパケットからのパケット数) Relative packed number from PMT to second transformed packet
byte_position_2	8	パケット内の変換データ記録位置(第2変換データ対応) Start byte position of transformed data in the second packet
overwrite_value_2	5x8	第2変換データ Second value to be overwritten
}		

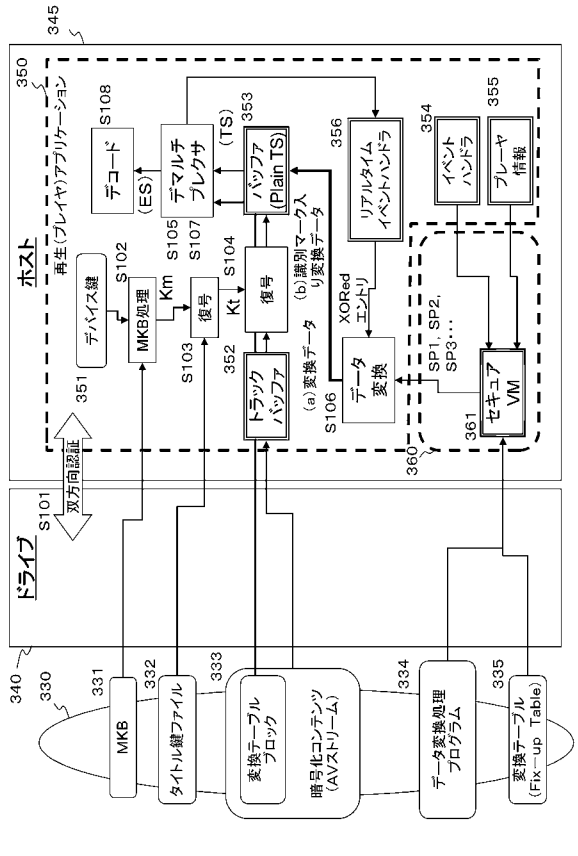
【図１０】



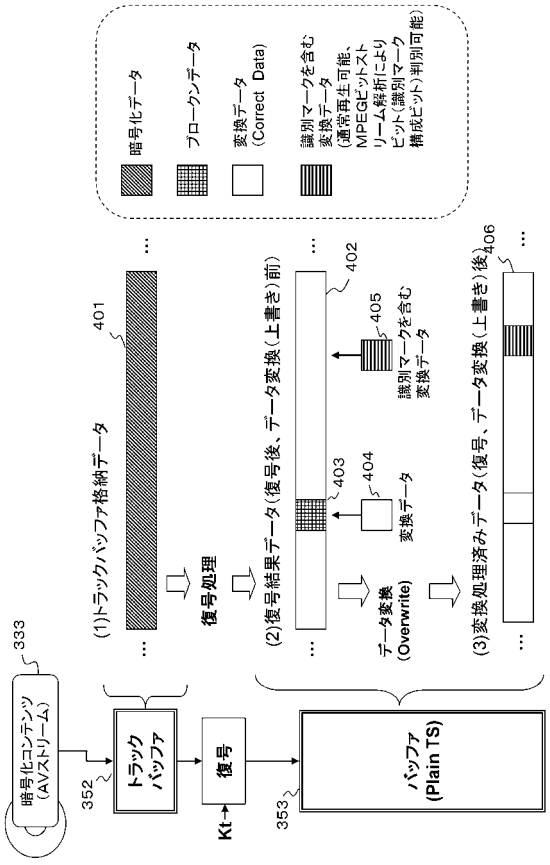
【図１２】



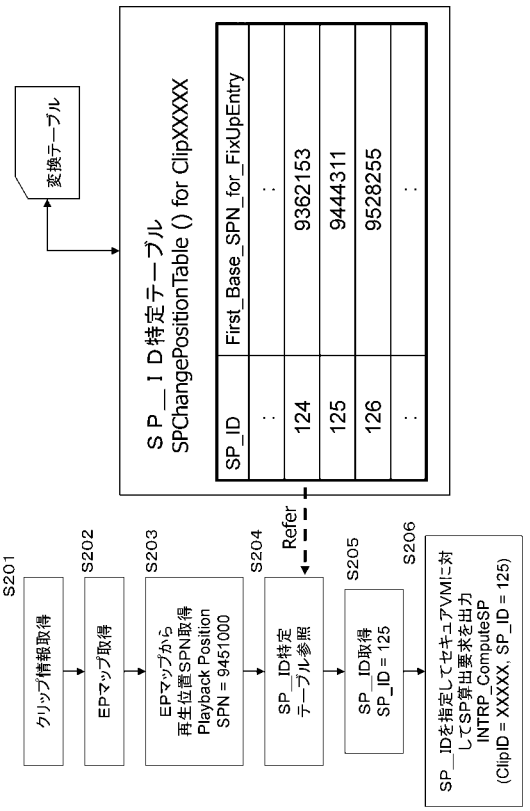
【図１３】



【図１４】



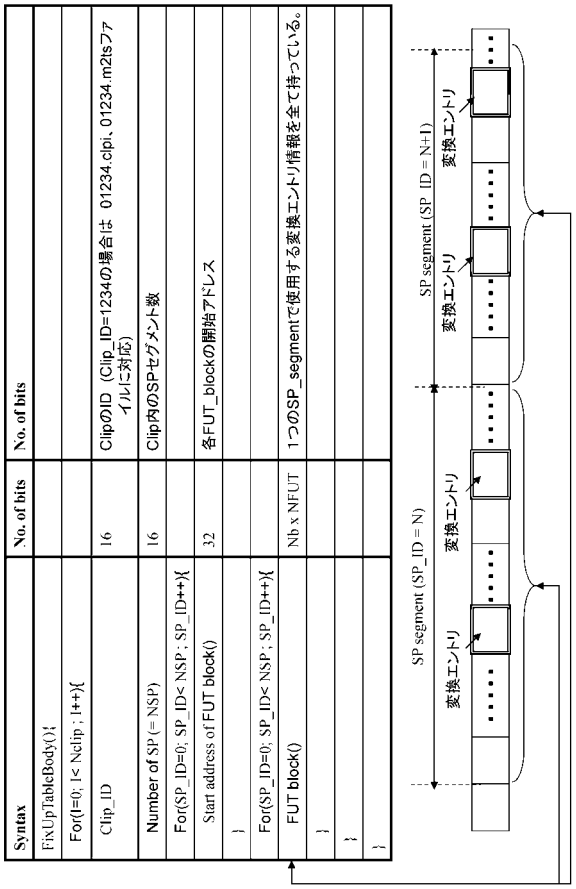
【図１８】



【図１９】

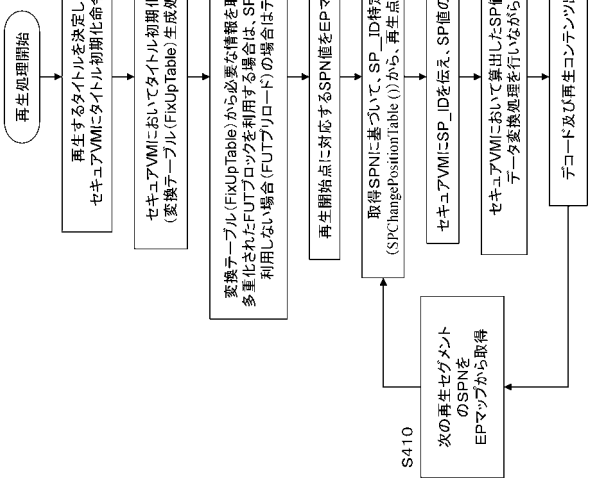
Syntax	No. of bits	定義
FixUpTable(){		
Number of Clips (=Nclip)	16	Title中で使用するClip数
FixUpTableBody_StartAddress	32	FixUpTable()内でのFixUpTableBody()の開始アドレス
SPChangePositionTable()		
FixUpTableBody()		
}		

【図２１】

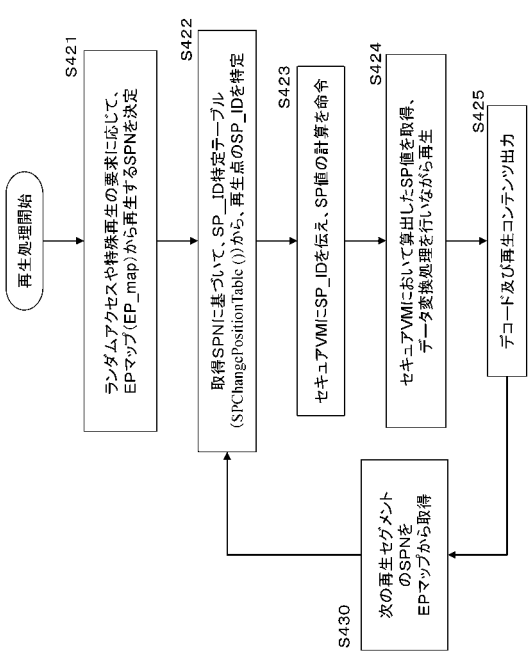


Syntax	No. of bits	No. of bits
FixUpTableBody(){		
For(I=0; I< Nclip ; I++){		
Clip_ID	16	ClipのID（Clip_ID=1234の場合は 01234.clpi、01234.m2tsファイルに対応）
Number of SP (= NSP)	16	Clip内のSPセグメント数
For(SP_ID=0; SP_ID< NSP ; SP_ID++){		
Start address of FUT block()	32	各FUT_blockの開始アドレス
}		
For(SP_ID=0; SP_ID< NSP ; SP_ID++){		
FUT block()	Nb x NFUT	1つのSP_segmentで使用する変換エントリ情報を全て持っている。
}		
}		
}		

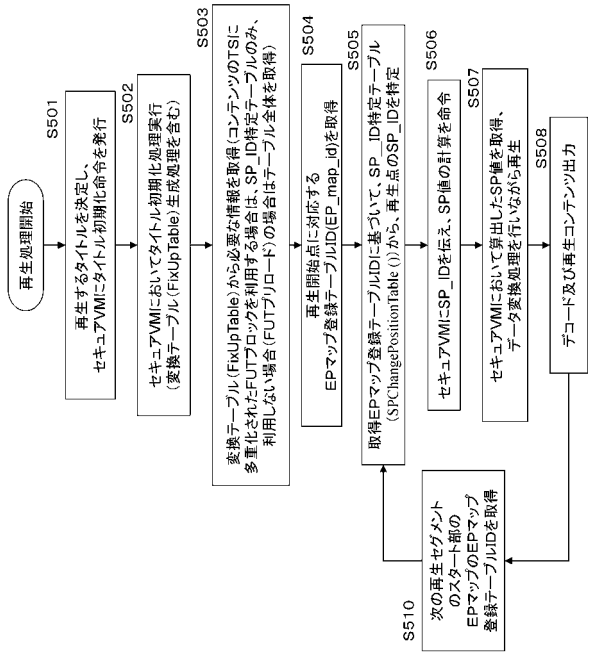
【図２３】



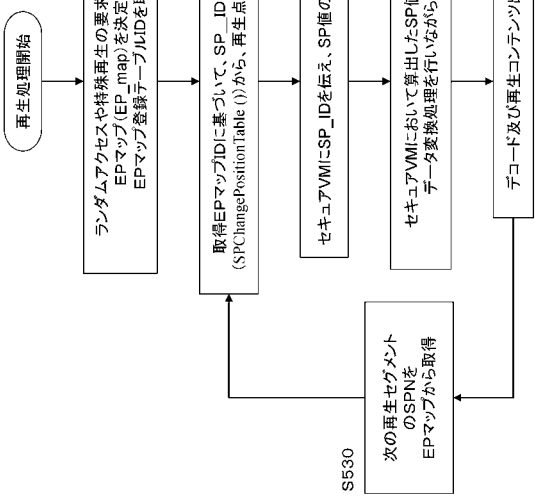
【図２４】



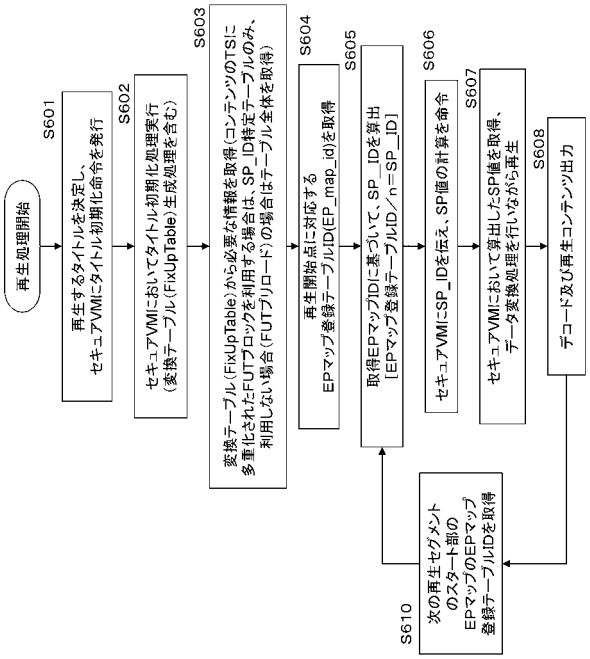
【図２６】



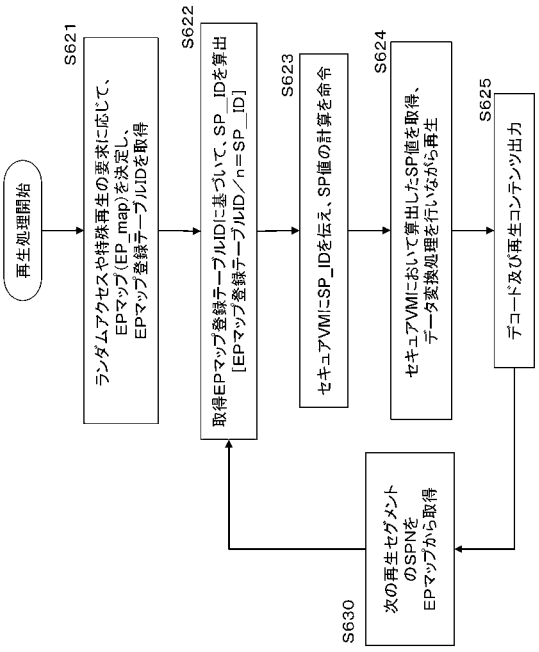
【図２７】



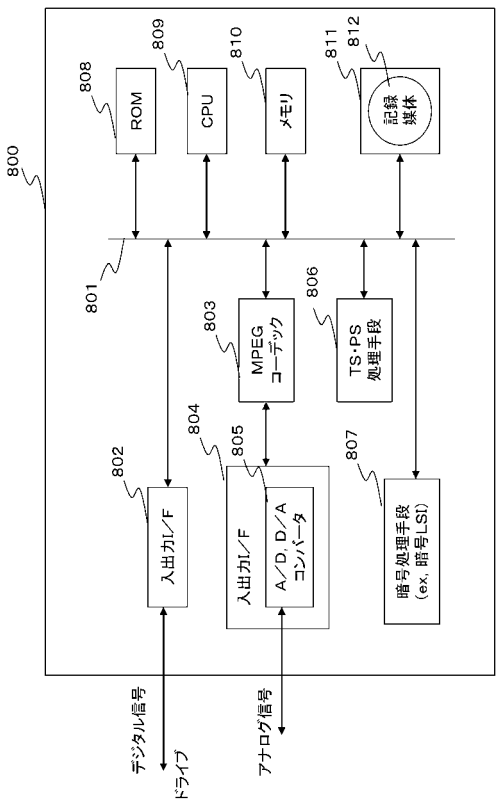
【図２９】



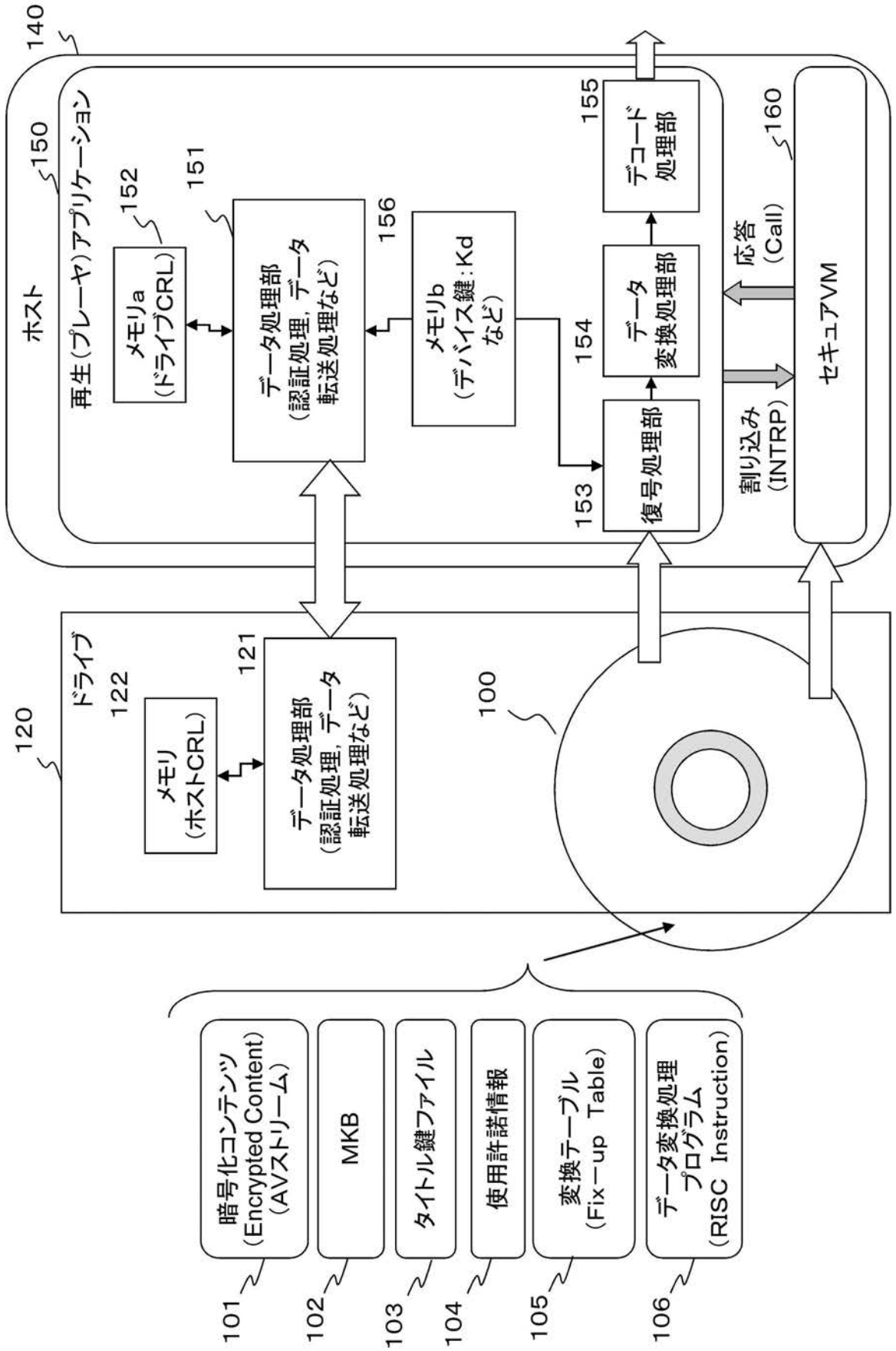
【図３０】



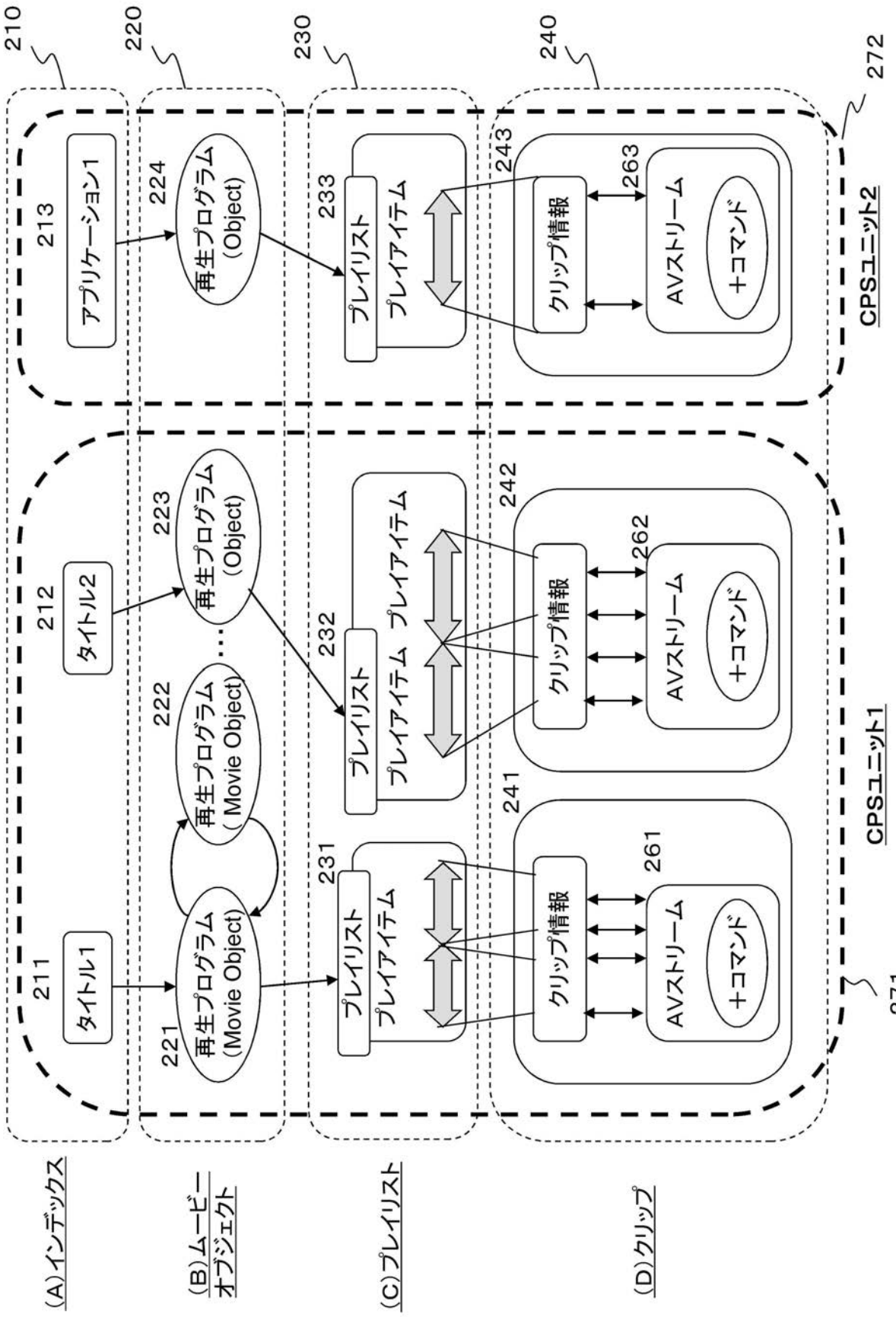
【図３１】



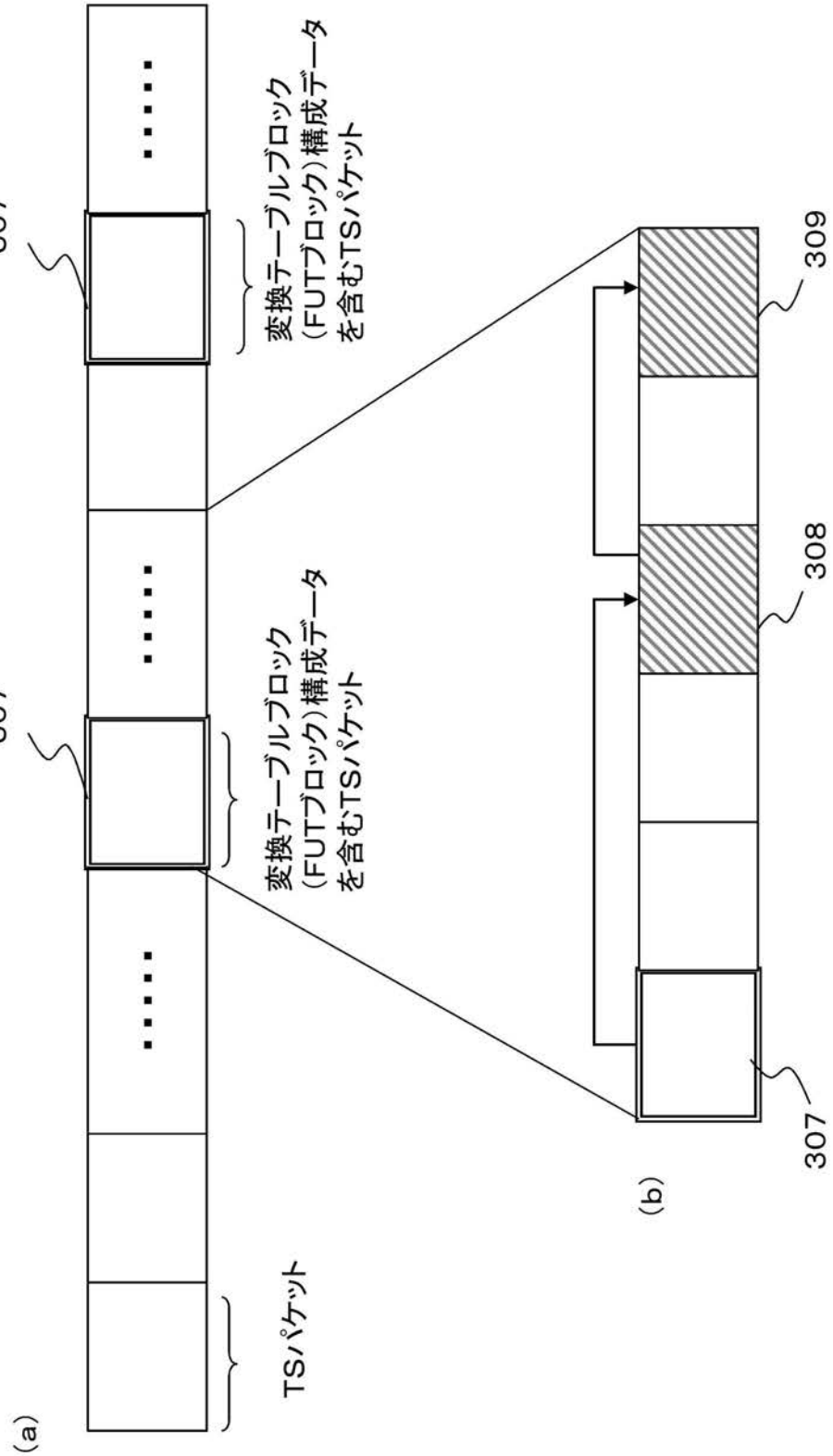
【図１】


140
ホスト
150
再生（プレーヤ）アプリケーション
152
メモリa
（ドライブCRL）
151
データ処理部
（認証処理，データ
転送処理など）
156
メモリb
（デバイス鍵：Kd
など）
155
デコード
処理部
154
データ
変換処理部
153
復号処理部
160
応答
（Call）
割り込み
（INTRP）
セキュアVM
120
ドライブ
122
メモリ
（ホストCRL）
121
データ処理部
（認証処理，データ
転送処理など）
100
101
暗号化コンテンツ
（Encrypted Content）
（AVストリーム）
102
MKB
103
タイトル鍵ファイル
104
使用許諾情報
105
変換テーブル
（Fix－up Table）
106
データ変換処理
プログラム
（RISC Instruction）

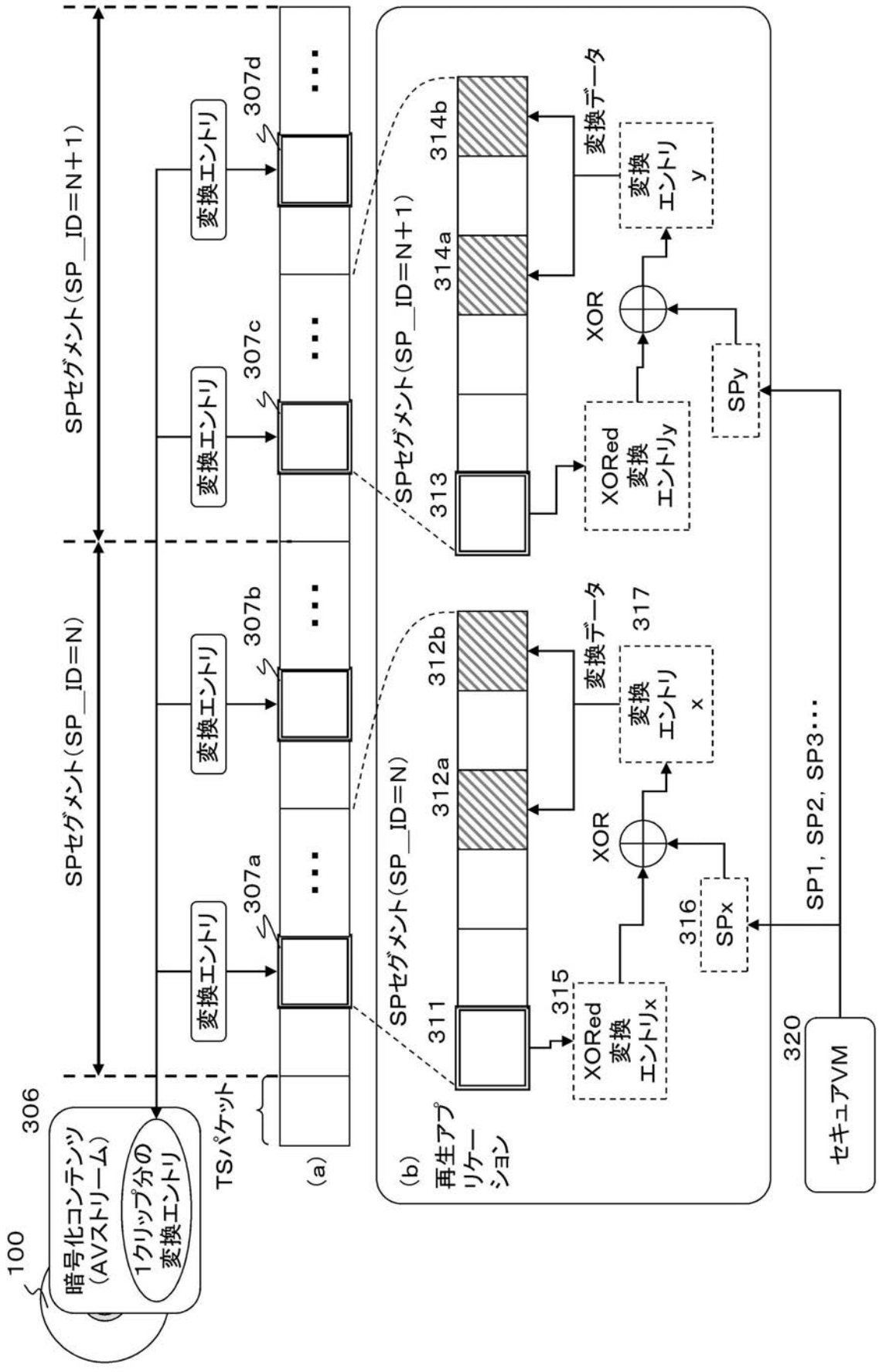
【図２】


210
220
230
240
272
アプリケーション1
213
再生プログラム (Object)
224
プレイリスト
233
プレイアイテム
クリップ情報
243
263
AVストリーム
＋コマンド
CPSユニット2
タイトル2
212
再生プログラム (Object)
223
再生プログラム (Movie Object)
222
プレイリスト
232
プレイアイテム
プレイアイテム
クリップ情報
242
262
AVストリーム
＋コマンド
タイトル1
211
再生プログラム (Movie Object)
221
プレイリスト
231
プレイアイテム
クリップ情報
241
261
AVストリーム
＋コマンド
CPSユニット1
271
(A)インデックス
(B)ムービーオブジェクト
(C)プレイリスト
(D)クリップ

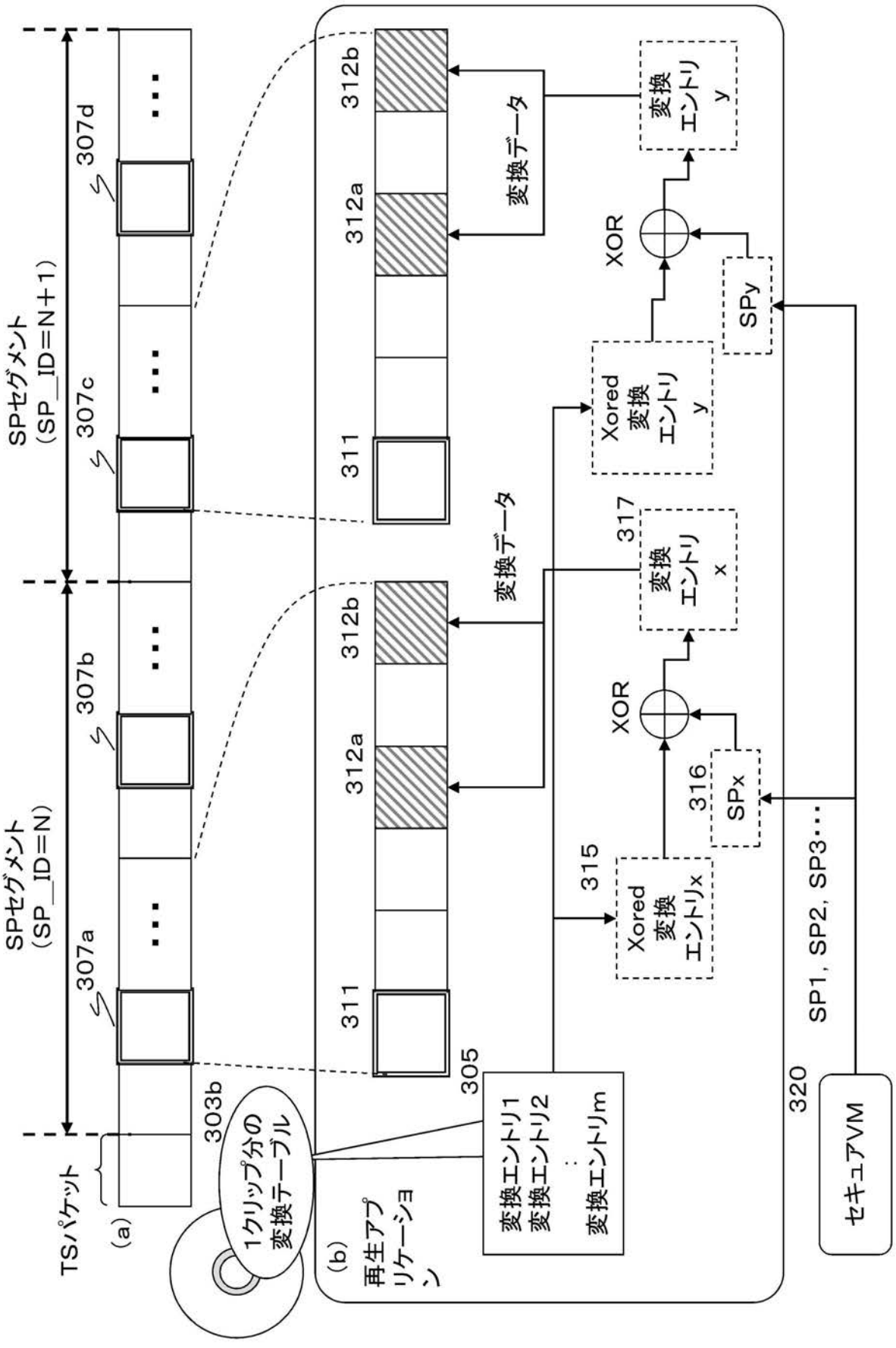
【図５】


(a)
TSパケット
変換テーブルブロック
(FUTブロック)構成データ
を含むTSパケット
307
307
変換テーブルブロック
(FUTブロック)構成データ
を含むTSパケット
(b)
309
308
307

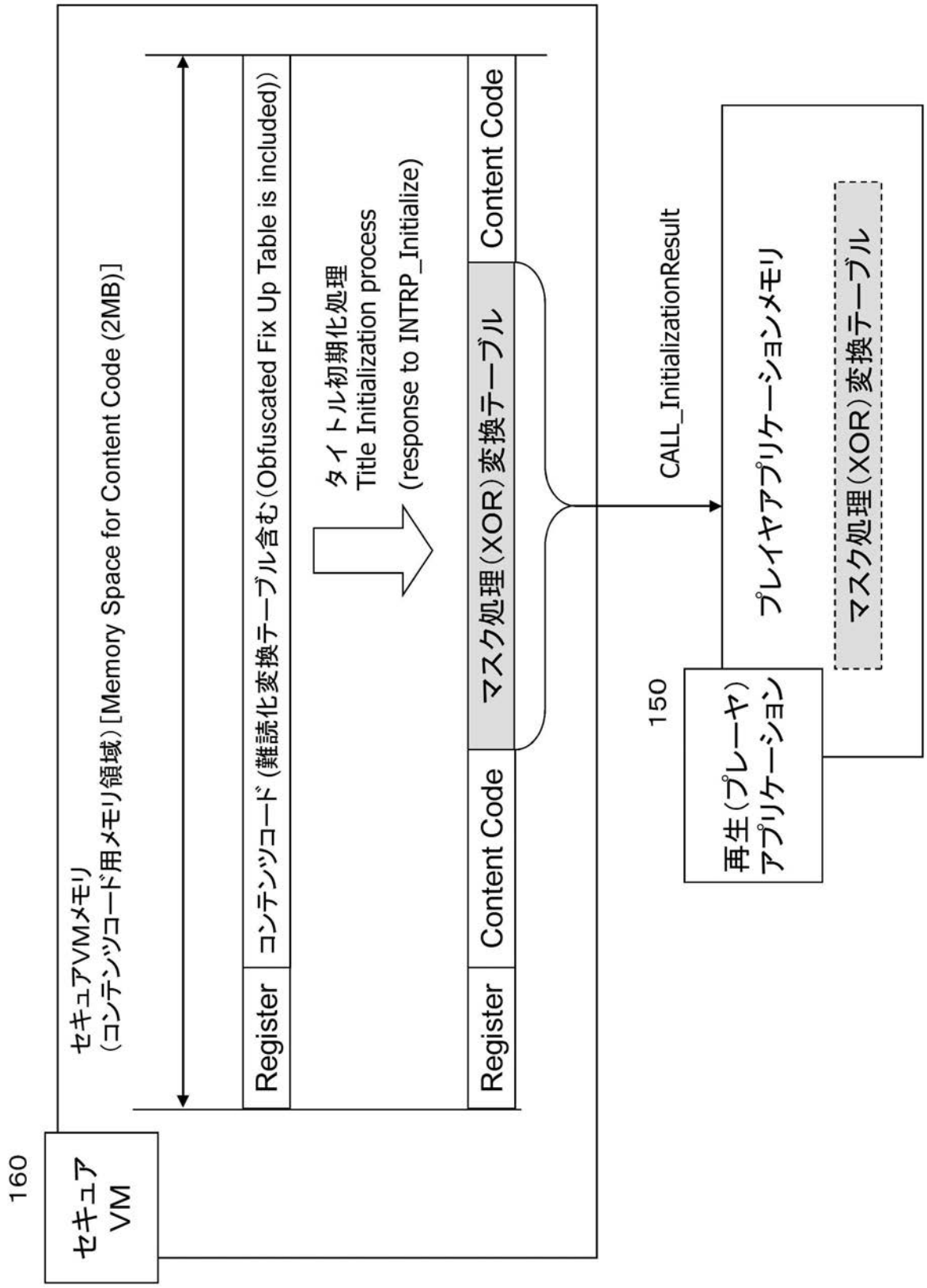
【図８】


100
306
暗号化コンテンツ
(AVストリーム)
1クリップ分の
変換エントリ
TSパケット
(a)
SPセグメント(SP_ID=N)
SPセグメント(SP_ID=N+1)
変換エントリ
307a
307b
307c
307d
(b)
再生アプリケーション
SPセグメント(SP_ID=N)
SPセグメント(SP_ID=N+1)
311
312a
312b
313
314a
314b
315
316
317
XORed 変換エントリx
XORed 変換エントリy
XOR
SPx
SPy
変換データ
変換エントリ x
変換エントリ y
SP1, SP2, SP3・・・
320
セキュアVM

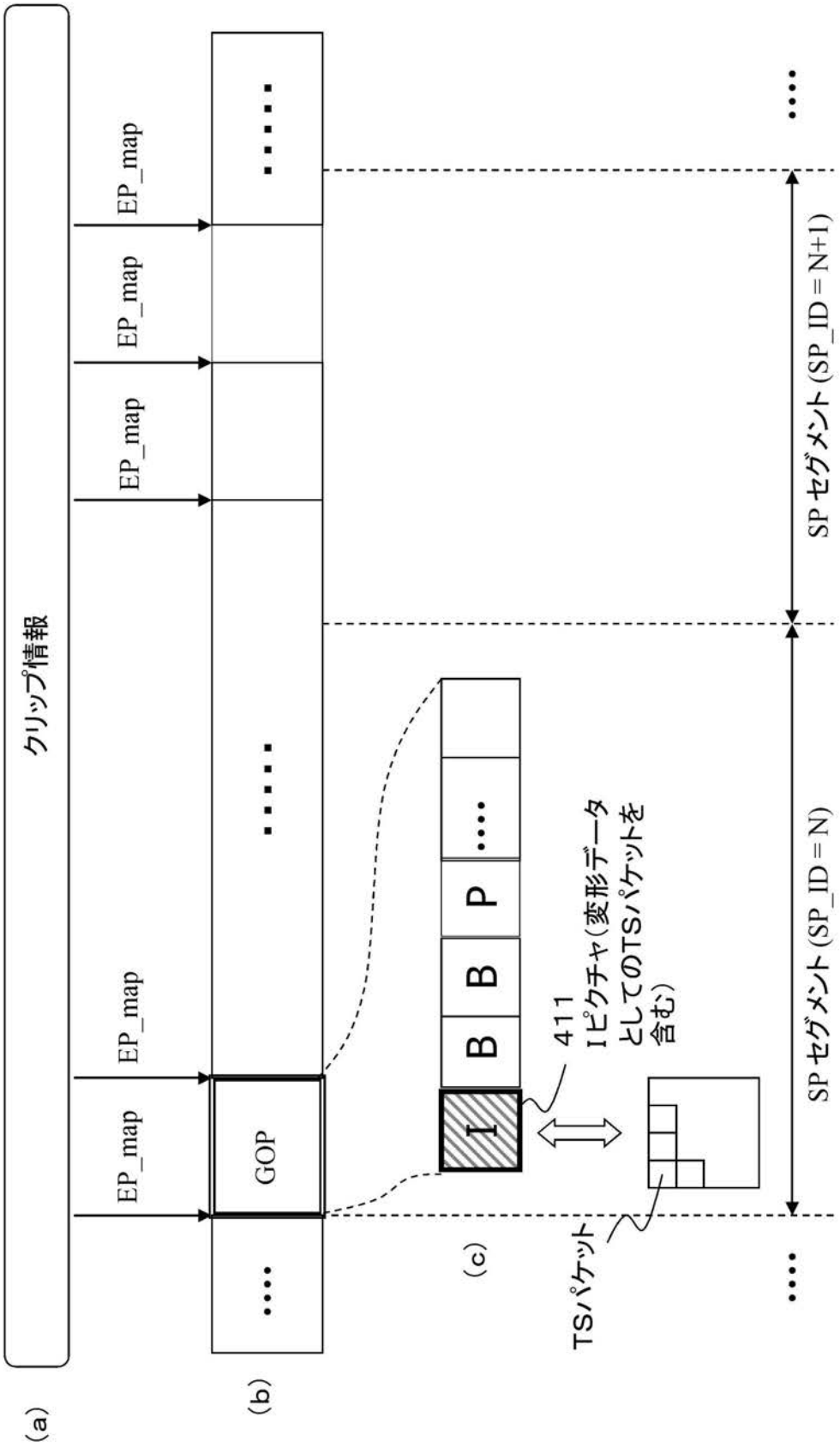
【図９】


SPセグメント
(SP_ID=N+1)
SPセグメント
(SP_ID=N)
TSパケット
(a)
307a
307b
307c
307d
303b
1クリップ分の
変換テーブル
(b)
再生アプリケーション
311
312a
312b
変換データ
変換エントリ1
変換エントリ2
:
変換エントリm
305
315
Xored
変換
エントリx
316
SPx
317
変換
エントリ
x
Xored
変換
エントリ
y
SPy
XOR
XOR
変換
エントリ
y
SP1, SP2, SP3･･･
320
セキュアVM

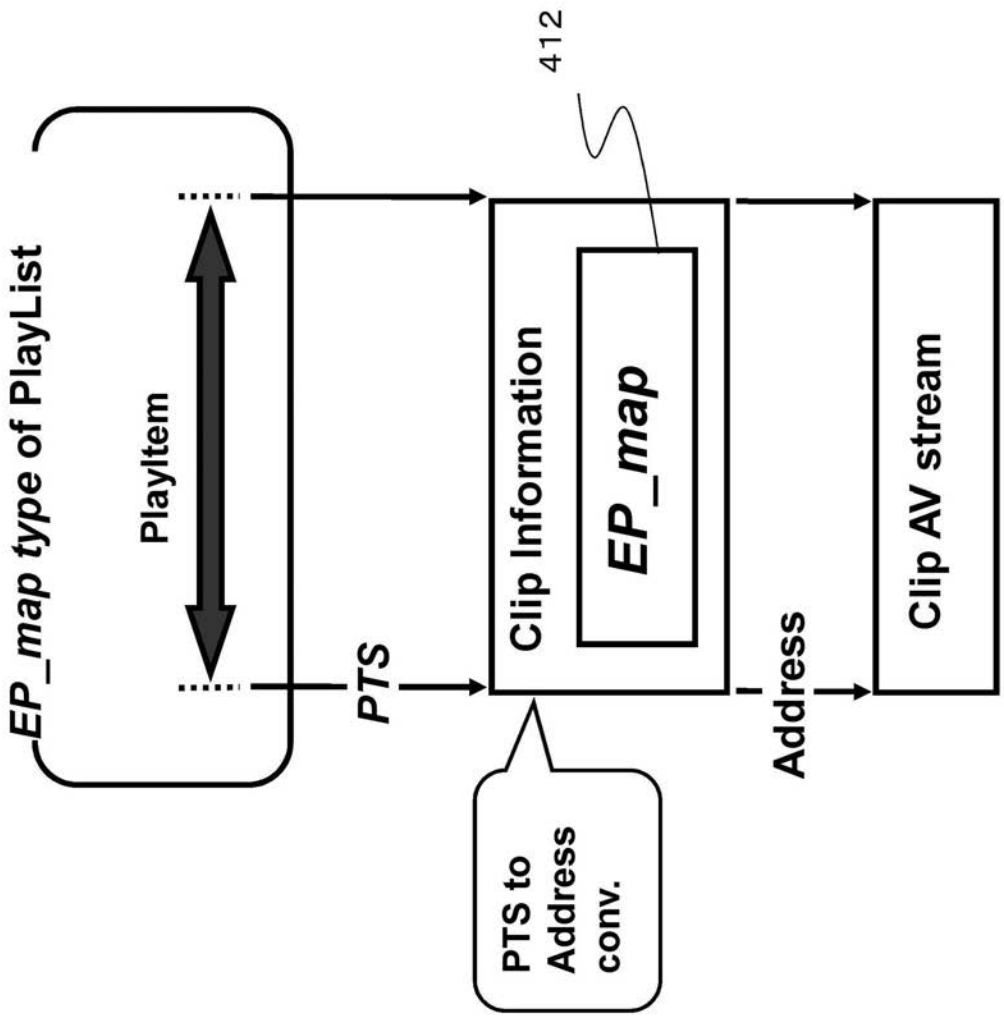
【図１１】


160
セキュア
VM
セキュアVMメモリ
(コンテンツコード用メモリ領域) [Memory Space for Content Code (2MB)]
Register
コンテンツコード (難読化変換テーブル含む (Obfuscated Fix Up Table is included))
Register
Content Code
Content Code
タイトル初期化処理
Title Initialization process
(response to INTRP_Initialize)
マスク処理（XOR）変換テーブル
CALL_InitializationResult
150
再生（プレーヤ）
アプリケーション
プレイヤアプリケーションメモリ
マスク処理（XOR）変換テーブル

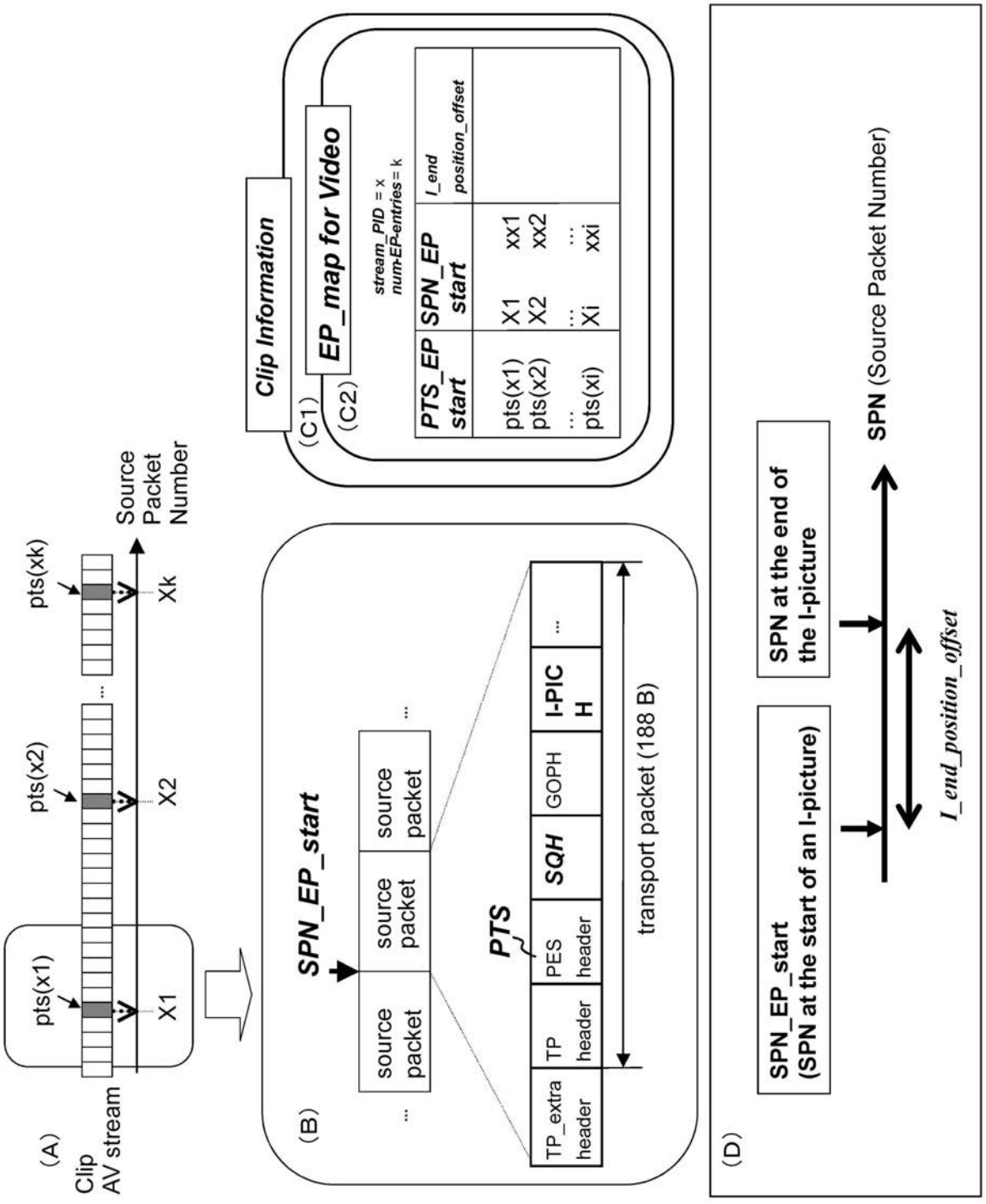
【図１５】


クリップ情報
EP_map
GOP
SP セグメント (SP_ID = N+1)
SP セグメント (SP_ID = N)
I
B
B
P
411
Iピクチャ（変形データとしてのTSパケットを含む）
TSパケット
(a)
(b)
(c)

【図１６】

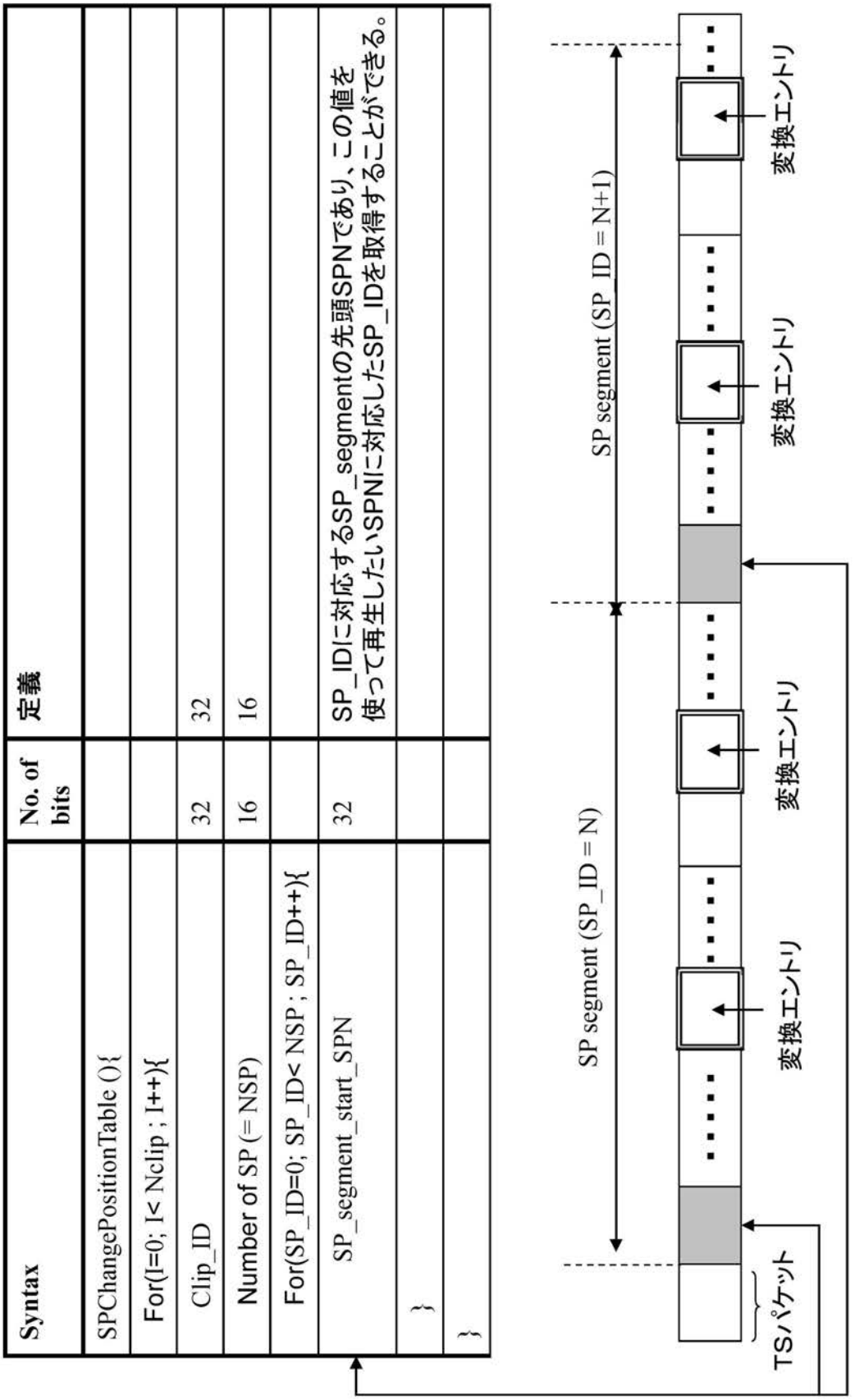

412
EP_map type of PlayList
PlayItem
PTS
Clip Information
EP_map
Address
Clip AV stream
PTS to Address conv.

【図１７】


(A)
Clip
AV stream
pts(x1)
pts(x2)
pts(xk)
X1
X2
Xk
Source
Packet
Number
(B)
SPN_EP_start
source packet
TP_extra header
TP header
PES header
PTS
SQH
GOPH
I-PIC H
transport packet (188 B)
Clip Information
(C1)
EP_map for Video
(C2)
stream_PID = x
num-EP-entries = k
PTS_EP start
SPN_EP start
I_end position_offset
pts(x1) X1 xx1
pts(x2) X2 xx2
pts(xi) Xi xxi
(D)
SPN_EP_start
(SPN at the start of an I-picture)
SPN at the end of the I-picture
SPN (Source Packet Number)
I_end_position_offset

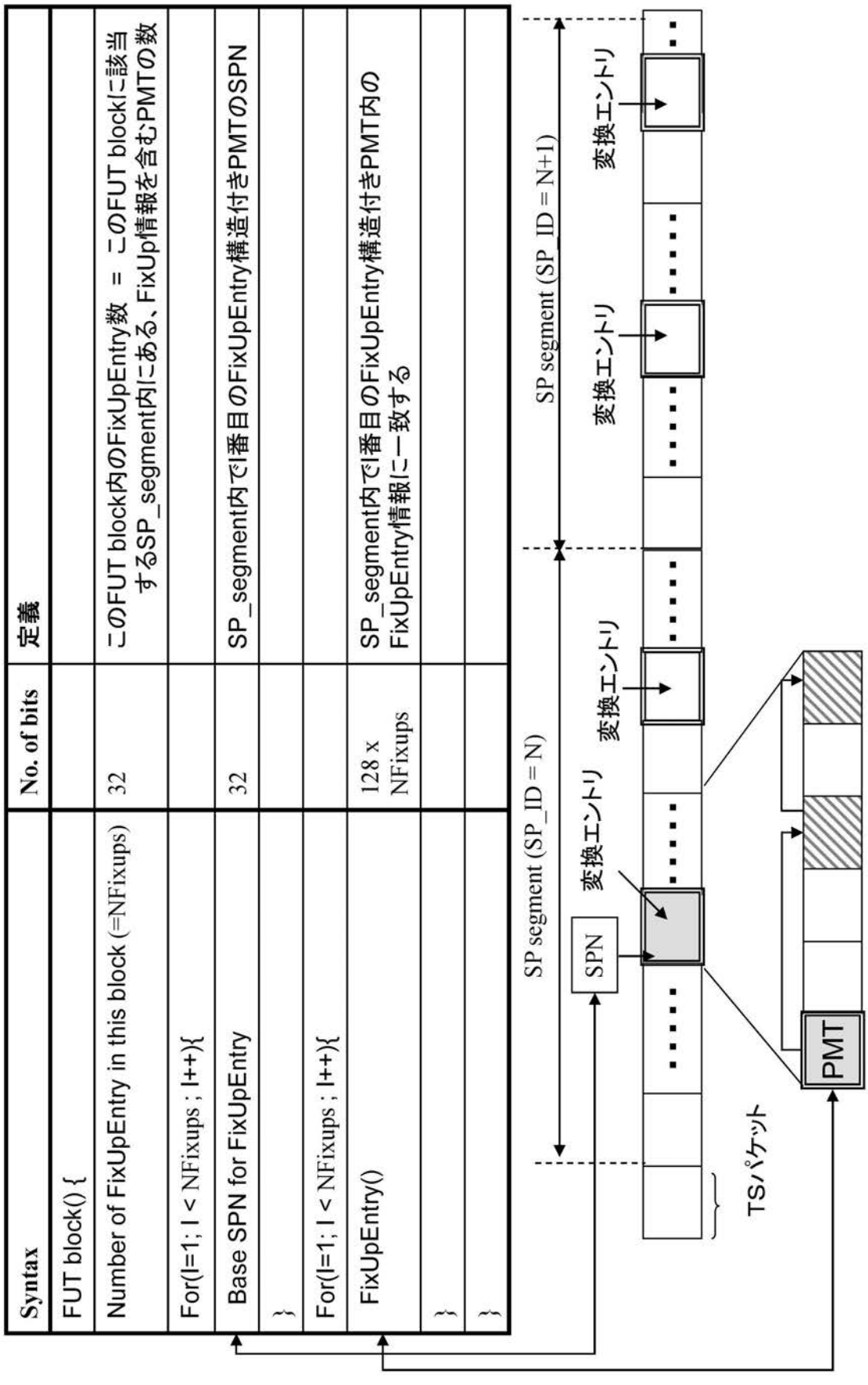
【図２０】

Syntax	No. of bits	定義
SPChangePositionTable (){		
For(I=0; I< Nclip ; I++){		
Clip_ID	32	32
Number of SP (= NSP)	16	16
For(SP_ID=0; SP_ID< NSP ; SP_ID++){		
SP_segment_start_SPN	32	SP_IDに対応するSP_segmentの先頭SPNであり、この値を使って再生したいSPNに対応したSP_IDを取得することができる。
}		
}		



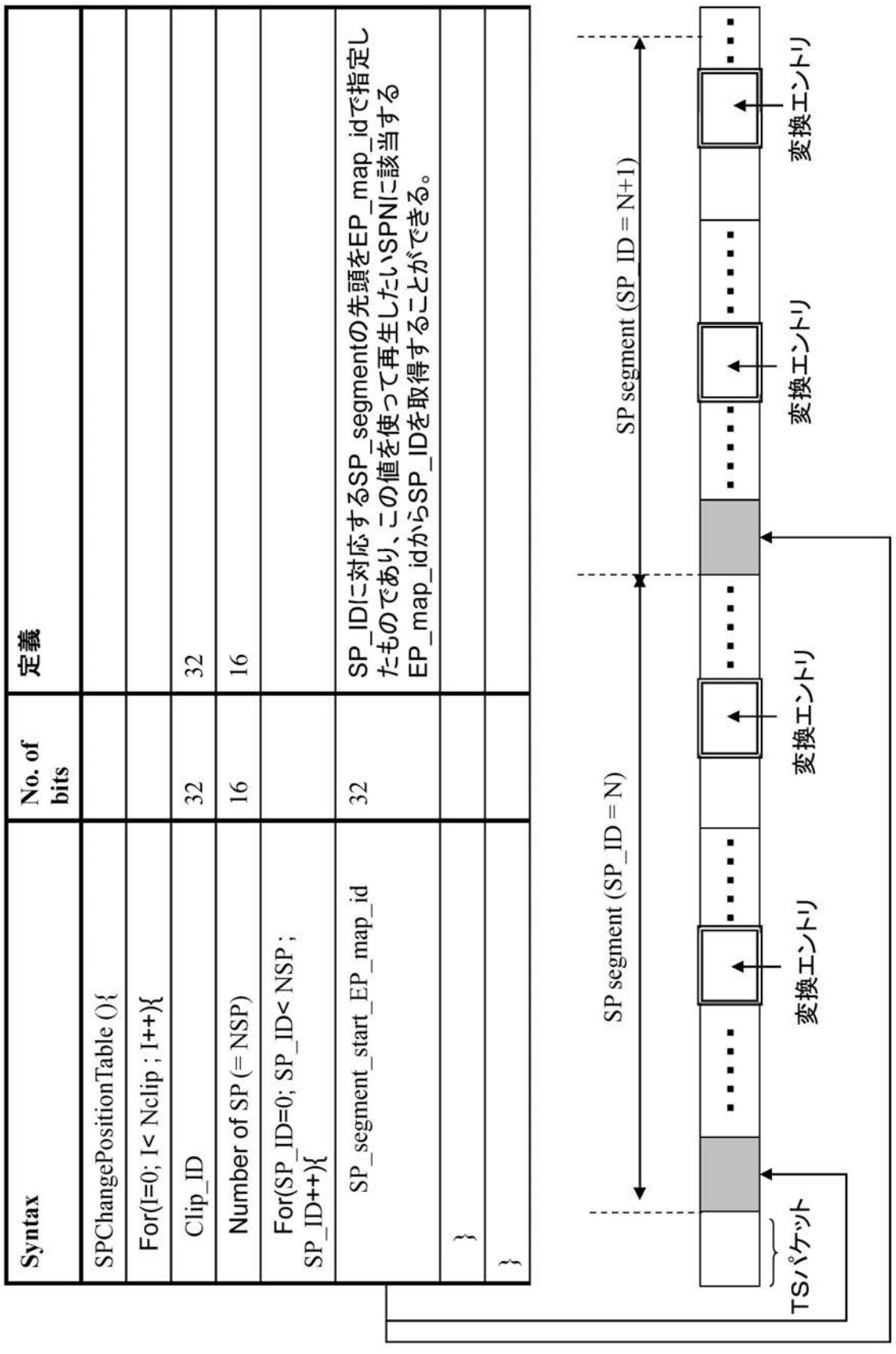
【図２２】

Syntax	No. of bits	定義
FUT block() {		
Number of FixUpEntry in this block (=NFixups)	32	このFUT block内のFixUpEntry数 = このFUT blockに該当するSP_segment内にある、FixUp情報を含むPMTの数
For(I=1; I < NFixups ; I++){		
Base SPN for FixUpEntry	32	SP_segment内でI番目のFixUpEntry構造付きPMTのSPN
}		
For(I=1; I < NFixups ; I++){		
FixUpEntry()	128 x NFixups	SP_segment内でI番目のFixUpEntry構造付きPMT内のFixUpEntry情報に一致する
}		
}		

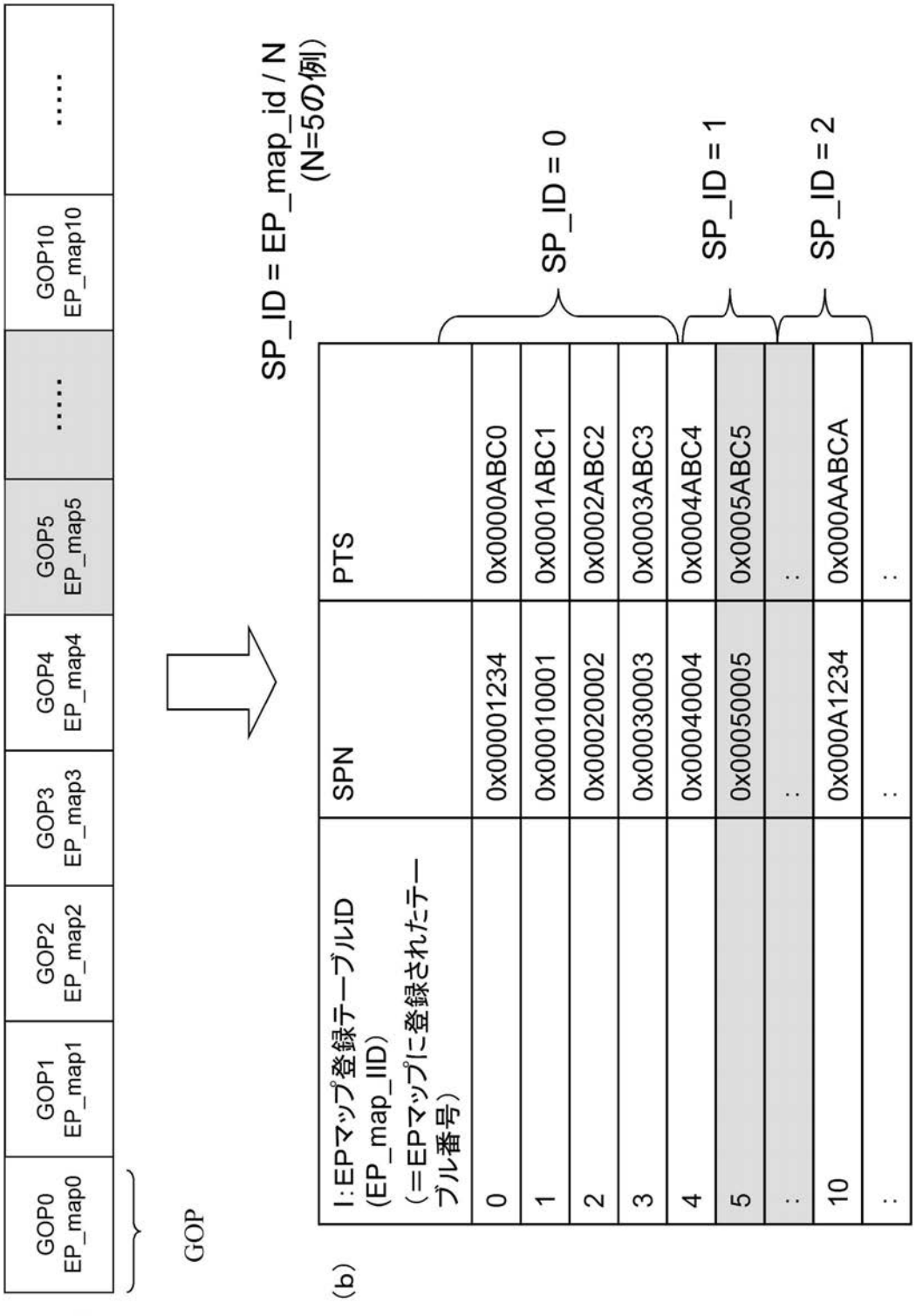


【図２５】

Syntax	No. of bits	定義
SPChangePositionTable (){		
For(I=0; I< Nclip ; I++){		
Clip_ID	32	32
Number of SP (= NSP)	16	16
For(SP_ID=0; SP_ID< NSP ; SP_ID++){		
SP_segment_start_EP_map_id	32	SP_IDに対応するSP_segmentの先頭をEP_map_idで指定したものであり、この値を使って再生したいSPNに該当するEP_map_idからSP_IDを取得することができる。
}		
}		



【図２８】



I:EPマップ登録テーブルID (EP_map_IID) (＝EPマップに登録されたテーブル番号)	SPN	PTS
0	0x00001234	0x0000ABC0
1	0x00010001	0x0001ABC1
2	0x00020002	0x0002ABC2
3	0x00030003	0x0003ABC3
4	0x00040004	0x0004ABC4
5	0x00050005	0x0005ABC5
:	:	:
10	0x000A1234	0x000AABCA
:	:	:

フロントページの続き

(72)発明者　高島　芳和
東京都港区港南１丁目７番１号　ソニー株式会社内

審査官　戸島　弘詩

(56)参考文献　特開２００５－２４２９７２（ＪＰ，Ａ）
特開平１１－４５５０８（ＪＰ，Ａ）
特開２００４－９５１１４（ＪＰ，Ａ）
特開２００５－２１６０２７（ＪＰ，Ａ）
特開２００３－１４３１３１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／２４
Ｇ０９Ｃ１／００－５／００
Ｈ０４Ｋ１／００
Ｈ０４Ｌ９／００
Ｇ１１Ｂ２０／１０