(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5259098号
(P5259098)

(45)発行日　平成25年8月7日(2013.8.7)　(24)登録日　平成25年5月2日(2013.5.2)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
H04N 7/16	(2011.01)	H04N	7/16	Z
G06F 21/62	(2013.01)	H04L	9/00	601E
G06F 21/10	(2013.01)	G06F	21/24	166A
		G06F	21/22	110E

請求項の数 12　(全 19 頁)

(21)出願番号　特願2007-35315(P2007-35315)
(22)出願日　平成19年2月15日(2007.2.15)
(65)公開番号　特開2007-221791(P2007-221791A)
(43)公開日　平成19年8月30日(2007.8.30)
審査請求日　平成22年2月12日(2010.2.12)
(31)優先権主張番号　60/773,340
(32)優先日　平成18年2月15日(2006.2.15)
(33)優先権主張国　米国(US)
(31)優先権主張番号　10-2006-0037718
(32)優先日　平成18年4月26日(2006.4.26)
(33)優先権主張国　韓国(KR)

(73)特許権者　390019839
三星電子株式会社
Ｓａｍｓｕｎｇ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｃｏ．，Ｌｔｄ．
大韓民国京畿道水原市霊通区三星路１２９　１２９，Ｓａｍｓｕｎｇ－ｒｏ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】トランスポートストリームをインポートする方法及び装置

(57)【特許請求の範囲】

【請求項１】

暗号化部と、ＰＩ生成部と、ヘッダ生成部と、ライセンス発給部と、ファイル生成部とを含む、コンテンツをインポートする装置において、コンテンツをインポートする方法において、

前記暗号化部が、前記コンテンツの使用制限情報によって前記コンテンツを暗号化するステップと、

前記ＰＩ生成部が、前記暗号化方式によって前記コンテンツを復号化するための情報を含むプロテクションインフォメーションを生成するステップと、

前記ヘッダ生成部が、前記コンテンツについてのＩＤ情報を含む前記コンテンツのヘッダを生成するステップと、

前記ライセンス発給部が、前記使用制限情報によって前記コンテンツについてのライセンスを生成するステップと、

前記ファイル生成部が、前記コンテンツ、プロテクションインフォメーション、コンテンツのヘッダ及びライセンスを結合するステップとを含み、

プロテクションインフォメーションはコンテンツに周期的に挿入され、プロテクションインフォメーションそれぞれは該当ライセンスを探すために必要なマッピング情報を含むことを特徴とするコンテンツのインポート方法。

【請求項２】

前記プロテクションインフォメーションは、前記暗号化方式がＡＥＳ－１２８－ＣＴＲ

である場合、前記コンテンツのシリアル番号を含み、前記コンテンツのヘッダは、前記コンテンツのＳＡＬＴ値をさらに含むことを特徴とする請求項１に記載のコンテンツのインポート方法。

【請求項３】

前記コンテンツのヘッダは、前記暗号化方式がＡＥＳ－１２８－ＣＢＣである場合、前記コンテンツのイニシャルベクトルを含むことを特徴とする請求項２に記載のコンテンツのインポート方法。

【請求項４】

前記プロテクションインフォメーションは、前記コンテンツのＩＤ情報に対応するマッピング情報を含み、前記ライセンスは、前記コンテンツのＩＤ情報を含むことを特徴とする請求項１に記載のコンテンツのインポート方法。

【請求項５】

前記結合ステップは、

前記プロテクションインフォメーションを前記コンテンツにＰＭＴパケットと同じ周期で挿入することを特徴とする請求項１に記載のコンテンツのインポート方法。

【請求項６】

前記プロテクションインフォメーションは、暗号化されないことを特徴とする請求項１に記載のコンテンツのインポート方法。

【請求項７】

コンテンツをインポートする装置において、

前記コンテンツの使用制限情報によって前記コンテンツを暗号化する暗号化部と、

前記暗号化方式によって前記コンテンツを復号化するための情報を含むプロテクションインフォメーションを生成するＰＩ生成部と、

前記コンテンツについてのＩＤ情報を含む前記コンテンツのヘッダを生成するヘッダ生成部と、

前記使用制限情報によって前記コンテンツについてのライセンスを生成するライセンス発給部と、

前記コンテンツ、プロテクションインフォメーション、コンテンツのヘッダ及びライセンスを結合するファイル生成部とを備え、

プロテクションインフォメーションはコンテンツに周期的に挿入され、プロテクションインフォメーションそれぞれは該当ライセンスを探すために必要なマッピング情報を含むことを特徴とするコンテンツインポート装置。

【請求項８】

前記プロテクションインフォメーションは、前記暗号化方式がＡＥＳ－１２８－ＣＴＲである場合、前記コンテンツのシリアル番号を含み、前記コンテンツのヘッダは、前記コンテンツのＳＡＬＴ値をさらに含むことを特徴とする請求項７に記載のコンテンツインポート装置。

【請求項９】

前記コンテンツのヘッダは、前記暗号化方式がＡＥＳ－１２８－ＣＢＣである場合、前記コンテンツのイニシャルベクトルを備えることを特徴とする請求項８に記載のコンテンツインポート装置。

【請求項１０】

前記プロテクションインフォメーションは、前記コンテンツのＩＤ情報に対応するマッピング情報を含み、前記ライセンスは、前記コンテンツのＩＤ情報を含むことを特徴とする請求項７に記載のコンテンツのインポート方法。

【請求項１１】

前記ファイル生成部は、前記プロテクションインフォメーションをＰＭＴパケットと同じ周期で前記コンテンツに挿入することを特徴とする請求項７に記載のコンテンツインポート装置。

【請求項１２】

前記プロテクションインフォメーションは、暗号化しないことを特徴とする請求項１１に記載のコンテンツインポート装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、デジタルコンテンツの保護に係り、特に、ＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）システムでのデジタルコンテンツの保護に関する。

【背景技術】

【０００２】

アナログ時代からデジタル時代に切り換わるにつれて、多くのコンテンツがデジタルで製作されている。アナログコンテンツは、そのコピーに多くの努力及び時間がかかるが、デジタルコンテンツは、そのコピーが容易かつ迅速に行われる。また、アナログコンテンツは、そのコピーの回数に比例してその品質が低下するが、デジタルコンテンツは、そのコピーの回数に関係なく、同じ品質を維持する。これにより、デジタルコンテンツの保護への必要性が持ち上げられ、デジタルコンテンツの保護に関する多様な研究が多くの企業によって行われている。

【０００３】

図１は、従来のデジタルコンテンツの保護環境を示す図である。図１に示すように、従来のデジタルコンテンツの保護環境では、多様なブロードキャスト伝送チャンネルを通じて伝送ストリームを受信し、これに含まれた情報を利用してコンテンツを保護しようとした。

【０００４】

特に、米国ケーブルラボ（Ｃａｂｌｅ　Ｌａｂｓ）という団体は、コンテンツのコピーを制御するために、コンテンツにコピー制御情報（ＣＣＩ）を添付するようにした。コピー制御情報とは、コンテンツのコピー回数を制限する２ビットの情報を言い、その種類には、コピーフリー（ｃｏｐｙ　ｆｒｅｅ、００）、コピーワンス（ｃｏｐｙ　ｏｎｃｅ、０１）、コピーノーモア（ｃｏｐｙ　ｎｏ　ｍｏｒｅ、１０）及びコピーネバー（ｃｏｐｙ　ｎｅｖｅｒ、１１）がある。コピーフリーは、コンテンツの無制限コピーが許容されることを表し、コピーワンスは、コンテンツの一回コピーのみが許容されることを表す。コピーワンスであるコンテンツがコピーされれば、このコンテンツは、コピーノーモアとなる。コピーネバーは、コンテンツのコピー禁止を表す。

【０００５】

また、米国の連邦通信委員会（Ｆｅｄｅｒａｌ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｃｏｍｍｉｓｓｉｏｎ：ＦＣＣ）は、米国内で放送されるＨＤ（Ｈｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ）級デジタルコンテンツに対して、コンテンツの無制限再配布を禁止するために、コンテンツにブロードキャストフラグを添付するようにした。ブロードキャストフラグとは、コンテンツの無制限再配布の禁止如何を表す１ビットの情報を言い、その種類には、ブロードキャストフラグオン（１）及びブロードキャストフラグオフ（０）がある。ブロードキャストフラグオンは、コンテンツの無制限再配布が許容されないことを表し、ブロードキャストフラグオフは、コンテンツの無制限再配布が許容されることを表す。その他にも、多様な使用制限情報が存在しうる。

【０００６】

一般的に、ユーザが多様な伝送チャンネルを通じて受信された多様な種類のコンテンツを利用するためには、各コンテンツを利用する度に、著作者から当該ライセンスを獲得せねばならないという面倒さが生じるが、ユーザが伝送チャンネルを通じて受信されたコンテンツを、ユーザのＤＲＭシステムを通じてインポートして、ユーザのＤＲＭシステムの規則に従うコンテンツファイルに変換し、本来の使用制限情報を遵守する範囲内で自体的にライセンスを発給すれば、インポートされたコンテンツファイルを自身のデバイスまたはドメインを通じて自由に利用できる。

【０００７】

ここで、インポートとは、ユーザのＤＲＭシステムの規則によって外部から受信されたコンテンツのそれぞれのライセンスを発給し、このコンテンツを暗号化する過程であって、すなわち、ユーザのＤＲＭシステムで規定する使用規則に従わないコンテンツファイルを、ユーザのＤＲＭシステムが規定する使用規則に従うように変換する過程を言い、ライセンスは、当該コンテンツを復号化して使用するために必要なものであって、コンテンツキー及び使用規則などを含む。また、コンテンツファイルとは、一つのコンテンツ、すなわち、一つの放送プログラムを構成する単位であって、使用制限情報またはライセンスなどを含みうる。

【０００８】

図２は、従来の技術によってインポートされたコンテンツファイルの構造を示す図である。図２に示すように、コンテンツに関するメタ情報は、一般的にコンテンツヘッダに記録される。

【０００９】

一方、伝送チャンネルを通じて受信された一つのコンテンツファイル、すなわち、一つの独立的なプログラムが複数のコンテンツ部分から構成される場合、各コンテンツ部分は、別途のコンテンツキーで暗号化され、それにより、複数のライセンスが必要となる。ここで、コンテンツ部分とは、一つのプログラムを構成するが、それぞれ相異なる使用制限情報を有するものを言う。

【００１０】

一般的に、インポートを行うＤＲＭシステムは、まず、コンテンツファイルのヘッダを生成し、受信されたペイロードパケットを暗号化した後、ヘッダとパッケージングすることによって図２のようなコンテンツファイルを生成するが、複数のコンテンツ部分から構成されたコンテンツをインポートする場合には、ヘッダのサイズが既に固定されているので、外部から受信されるコンテンツの使用制限情報が変わる度に、関連した復号化情報をヘッダに全て記録することは難しいという問題が生じる。

【００１１】

また、図２のような構造を有するコンテンツファイルは、デバイスが中間部分からストリーミングを通じて受信する場合、時間が遅延されるという問題が生じるが、これは、図３Ａ及び図３Ｂを参照して説明する。一般的に、ＭＰＥＧ－２トランスポートパケットから構成されるコンテンツの暗号化には、ＡＥＳ－１２８－ＣＴＲ方式またはＡＥＳ－１２８－ＣＢＣ方式などが使用されるが、図３Ａには、ＡＥＳ－１２８－ＣＴＲ方式を示した。

【００１２】

図３Ａに示すように、ＡＥＳ－１２８－ＣＴＲ方式では、暗号化パラメータであるＳＡＬＴとシリアル番号とを組合わせてカウンタ値を算出し、ＡＥＳアルゴリズムによって、このカウンタ値でコンテンツキーを暗号化することによってキーストリームを形成するが、コンテンツをキーストリームとＸＯＲ演算することによって、ＡＥＳ－１２８－ＣＴＲ方式による暗号化が完了する。ここで、暗号化は、コンテンツを１２８ビット、すなわち、１６バイトサイズの暗号化ブロック単位で分けて行い、カウンタ値は、暗号化ブロックに順に割り当てられる番号であるので、次の暗号化ブロックのカウンタ値は、以前暗号化ブロックのカウンタ値より１がさらに多くなる。

【００１３】

図３Ｂには、ＡＥＳ－１２８－ＣＢＣ方式による暗号化方式を示すが、図３Ｂに示すように、暗号化パラメータとして使用されるイニシャルベクトルを、暗号化ブロック（Ｐｌａｉｎ
Ｔｅｘｔ）とＸＯＲ演算し、その結果値を、ＡＥＳアルゴリズムを利用してコンテンツキーで暗号化すれば、一つの暗号化ブロックについての暗号化が完了するが、次のブロックの暗号化には、暗号化パラメータとしてイニシャルベクトルが使用されるものではなく、以前のステップで暗号化されたブロックを使用する。

【００１４】

結局、図３Ａ及び図３Ｂで説明したところによれば、ＡＥＳ－１２８－ＣＴＲ方式またはＡＥＳ－１２８－ＣＢＣ方式により暗号化されたコンテンツファイルを、ドメインに属するデバイスが、中間部分からストリーミングを通じて受信する場合、デバイスは、当該部分のトランスポートパケットの復号化に必要な暗号化パラメータを得るために、前部分のトランスポートパケットと関連した演算を全て行わねばならないので、時間が遅延されるという問題が生じる。

【発明の開示】

【発明が解決しようとする課題】

【００１５】

本発明は、トランスポートストリームコンテンツをインポートしてコンテンツファイルを生成することにおいて、コンテンツファイルのペイロードに周期的に復号化のために必要な情報を挿入して、インポート過程及び復号化過程での効率を高める装置及び方法を提供するところにその目的がある。

【課題を解決するための手段】

【００１６】

このような目的を達成するための本発明は、第１コンテンツファイルを第２コンテンツファイルにインポートする方法において、前記第１コンテンツファイルのペイロードパケットを暗号化するステップと、前記暗号化されたペイロードパケットを復号化するために必要な情報を含む保護情報パケットを生成するステップと、前記生成された保護情報パケットを前記第１コンテンツファイルのペイロードパケットの間に周期的に挿入して、前記第２コンテンツファイルのペイロードを生成するステップと、を含むことを特徴とする。

【００１７】

このとき、前記保護情報パケットは、前記第１コンテンツファイルのペイロードパケットと同じフォーマットを有することが望ましく、前記フォーマットは、ＭＰＥＧ－２トランスポートパケットでありうる。

【００１８】

また、前記ペイロードの生成ステップは、前記保護情報パケットがＰＭＴ（プログラムマップ　テーブル）パケットと同じ周期を有するように挿入することが望ましい。

【００１９】

また、前記インポート方法は、前記第２コンテンツファイルを構成するパケットのうち、前記保護情報パケットを識別させるインデックス情報を含むヘッダを生成するステップと、前記生成されたヘッダを前記第２コンテンツファイルのペイロードに付加するステップとをさらに含みうる。

【００２０】

また、本発明は、前記コンテンツのインポート方法をコンピュータで実行させるためのプログラムを記録したコンピュータで読み取り可能な記録媒体を提供する。

【００２１】

また、本発明は、第１コンテンツファイルを第２コンテンツファイルにインポートする装置において、前記第１コンテンツファイルのペイロードパケットを暗号化する暗号化部と、前記暗号化されたペイロードパケットを復号化するために必要な情報を含む保護情報パケットを生成する保護情報パケット生成部と、前記生成された保護情報パケットを前記第１コンテンツファイルのペイロードパケットの間に周期的に挿入して、前記第２コンテンツファイルのペイロードを生成するファイル生成部とを備えることを特徴とする。

【発明の効果】

【００２２】

本発明によれば、インポート装置がドメインの外部から受信されたコンテンツのインポート中、コンテンツに含まれた使用制限情報が変更されても、効率的なパッケージングが可能であり、ドメインに属するデバイスは、インポートされたコンテンツファイルを中間部分からストリーミングを通じて受信する場合にも、時間遅延なしに迅速に当該部分のトランスポートパケットを復号化できる。また、ＭＰＥＧ－２トランスポートパケットを処

理できるデバイスでは、追加的な装備なしに既存の出コーディング装備を利用して、本発明によってインポートされたコンテンツファイルを解析できる。

【発明を実施するための最良の形態】

【００２３】

以下、添付された図面を参照して本発明の望ましい実施形態を詳細に説明する。

【００２４】

図４は、本発明の一実施形態によってインポートされたコンテンツファイルの構造を示す図である。図４に示すように、本発明の一実施形態によってインポートされたコンテンツファイルは、ファイルヘッダ２１０にＣＯＮＴＥＮＴ　ＩＤ　２１１、ＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　２１２及びＰＩ　ＰＩＤ　２１３を備える。

【００２５】

また、ペイロードには、ペイロードパケットを復号化するために必要な情報を含むパケットが周期的に挿入されているが、以下では、このようなパケットをＰＩ（プロテクション　インフォメーション）パケットと称す。このようなＰＩパケットは、ペイロードの他のパケットと同様に、ＭＰＥＧ－２トランスポートパケットのフォーマットに従うことが望ましい。もし、別途のフォーマットを有するならば、インポートされたコンテンツファイルを利用しようとするデバイスは、ＰＩパケットを解析するための別途のモジュールを備えねばならない。

【００２６】

このように、ＰＩパケットをペイロードに周期的に挿入することによって、インポート装置は、複数の使用制限情報を含むコンテンツの受信中に使用制限情報が変わっても、その度に関連情報をＰＩパケットに含ませてペイロードに挿入すればよいので、パッケージング作業が効率的になり、コンテンツを使用しようとするデバイスがコンテンツの中間部分からストリーミングを通じて受信する場合にも、当該部分を復号化するために必要なＰＩパケットを迅速に探しうるだけでなく、探したＰＩパケットのシリアル番号を利用して、当該部分のトランスポートパケットを復号化するために必要なカウンタ値を迅速に演算できる。

【００２７】

一方、デバイスがトランスポートパケットから構成されたコンテンツを再生するためには、ＰＭＴパケットを参照せねばならないので、ＰＩパケットは、ＰＭＴパケットと同じ周期（一般的に、０.７秒）で挿入されることが望ましい。

【００２８】

図４に示すように、ＰＩパケット２２０は、ＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　２２２を含む。ＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　２２２は、インポートされたコンテンツファイルのペイロードパケットがＡＥＳ－１２８－ＣＴＲ方式で暗号化された場合、暗号化パラメータとして使用されたシリアル番号である。すなわち、コンテンツファイルを利用しようとするデバイスは、ＰＩパケット２２０に含まれたシリアル番号をＳＡＬＴとＸＯＲ演算して、基本カウンタを探した後、これを基礎として次のＰＩパケットが表れる前までのペイロードパケットの暗号化ブロックを復号化できる。

【００２９】

一方、ヘッダ２１０のＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　２１２は、暗号化がＡＥＳ－１２８－ＣＢＣ方式により行われた場合、イニシャルベクトル、ＡＥＳ－１２８－ＣＴＲ方式により行われた場合、ＳＡＬＴに該当する。もちろん、ＰＩパケットでこのような情報も全て含みうるが、イニシャルベクトルやＳＡＬＴは、一つのコンテンツ内で変更される確率がシリアル番号に比べて相対的に少なく、また、ＭＰＥＧ－２トランスポートパケットは、ペイロードに保存できるデータの最大値が１８４バイトに限定されるためである。

【００３０】

ＣＯＮＴＥＮＴ　ＩＤ　２１１は、コンテンツを他のコンテンツと区別するための識別子である。ＤＲＭシステムが保存する各コンテンツは、それぞれ異なるライセンスを必要

とするが、各ライセンスは、当該コンテンツのコンテンツＩＤを含んでいるので、コンテンツＩＤは、各コンテンツを当該ライセンスに対応させるマッピング情報として活用される。

【００３１】

ＰＩ　ＰＩＤ　２１３は、ＰＩパケットを探すためのインデックス情報である。コンテンツファイルのペイロードを構成するトランスポートパケットは、各パケットに含まれる情報の種類によって、パケットヘッダに固有のパケットＩＤを有する。したがって、コンテンツファイルを利用しようとするデバイスは、ファイルヘッダを読み取って、どのトランスポートパケットがＰＩパケットであるかが分かる。

【００３２】

以上では、一つのコンテンツに一つの使用制限情報が含まれた場合のインポート方法について説明した。しかし、場合によって、一つのコンテンツには、複数の使用制限情報が含まれ、このようなコンテンツをインポートして、複数のコンテンツ部分から構成されたコンテンツファイルが生成されうる。以下では、複数の使用制限情報を含むコンテンツをインポートする方法について説明する。

【００３３】

図５は、複数の使用制限情報を含むコンテンツをインポートする環境を説明するための図である。図５に示すデジタルコンテンツの保護環境は、ＤＲＭシステム５００によりインポートされたコンテンツファイルを提供される複数のデバイス５１ないし５３から構成される。

【００３４】

ＤＲＭシステム５００は、従来のコピー制御、ブロードキャストフラグなどにより保護されるコンテンツを、コンテンツ製作者及びコンテンツ供給者の保安要求を遵守すると同時に、コンテンツユーザの自由な使用要求をさらに十分に満足させるように設計されたＤＲＭシステム５００の規則に従うコンテンツにインポートするコンテンツインポート装置５０を備える。

【００３５】

本発明に係るコンテンツインポート装置５０は、複数の使用制限情報を含むコンテンツ、すなわち、複数のコンテンツ部分から構成されたコンテンツが受信されれば、これをインポートして、コンテンツファイルを生成する過程でインポートされた後のコンテンツファイルをして、各コンテンツ部分についての位置情報、ライセンスマッピング情報などが記録されたヘッダを含ませる。ユーザのドメインに属するデバイスが、このような方式でインポートされたコンテンツファイルを使用する場合、ヘッダを分析して、予め各コンテンツファイルを使用するための使用規則やライセンスなどを獲得して準備できるので、時間遅延を防止できる。また、前述のように、インポートされたコンテンツファイルのペイロードには、ＰＩパケットが周期的に挿入される。このようにインポートされたコンテンツファイルを、そのコンテンツファイルを再生しようとするデバイスが要請すれば、ＤＲＭシステム５００は、使用規則を参照して当該コンテンツファイルのコンテンツ部分を分配し、各コンテンツ部分を受信したデバイスは、ファイルヘッダを分析して必要なライセンスを探した後、自身のデバイスキーまたはドメインキーを利用して、ライセンスに含まれたコンテンツキーを獲得し、再びコンテンツキーを利用して各コンテンツ部分を復号化できる。このとき、ＤＲＭシステム５００がコンテンツファイルの提供時に参照する使用規則は、インポートなる前のコンテンツファイルに含まれた使用制限情報によって規定されるが、図６を参照してこれを説明する。

【００３６】

図６は、本発明の一実施形態によって使用制限情報を使用規則に変換したマッピングテーブルである。図６に示すように、本発明の一実施形態に係るマッピングテーブルは、使用制限情報フィールド４１、インポートフィールド４２、使用範囲フィールド４３及び使用規則フィールド４４から構成される。このようなマッピングテーブルは、コンテンツを構成するコンテンツ部分のうち何れか一つに関するものであってもよく、一つの使用制限

情報のみを有する一つのコンテンツファイルに関するものであってもよい。以下では、前者の場合を仮定して説明する。

【００３７】

使用制限情報フィールド４１には、コンテンツ部分の使用制限情報が記録される。インポートフィールド４２には、使用制限情報フィールド４１に記録された使用制限情報を有するコンテンツ部分のインポート可否を表す値が記録される。使用範囲フィールド４３には、使用制限情報フィールド４１に記録された使用制限情報を基盤とする使用範囲が記録される。使用規則フィールド４４には、使用範囲フィールド４３に記録された使用範囲別に、使用制限情報フィールド４１に記録された使用制限情報を基盤とする使用規則が記録される。

【００３８】

特に、使用規則フィールド４４に記録された値のうち“オール（ａｌｌ）”は、コンテンツ部分についての全ての種類の使用が可能であることを表す。また、使用規則フィールド４４に記録された値のうち“Ｍ”は、コンテンツ部分の移動（Ｍｏｖｅ）を表す。コンテンツ部分の移動とは、何れか一つのデバイスに保存されたコンテンツ部分が、このデバイスから削除されると同時に、他のデバイスに保存されることを意味する。また、使用規則フィールド４４に記録された値のうち“Ｓ”は、コンテンツ部分のストリーミング（Ｓｔｒｅａｍｉｎｇ）を表す。コンテンツ部分のストリーミングとは、何れか一つのデバイスに保存されたコンテンツ部分が他のデバイスに一時的に出力されるが、本来のデバイスでコンテンツ部分を継続的に保存していることを意味する。また、使用規則フィールド４４に記録された値のうち“Ｐ”は、コンテンツ部分の再生（Ｐｌａｙ）を表す。コンテンツ部分の再生とは、何れか一つのデバイスがコンテンツ部分を他のデバイスに伝達せずに直接的に再生することを意味する。

【００３９】

コピーフリーは、コンテンツ部分の無制限コピーが許容されることを表すので、使用制限情報がコピーフリーである場合には、使用範囲フィールド４３にデバイス、ドメインが記録され、使用規則フィールド４４に“オール”が記録される。一方、コピーワンスは、コンテンツ部分の一回コピーのみが許容されることを表すので、使用制限情報がコピーワンスである場合には、使用範囲フィールド４３にデバイスが記録され、使用規則フィールド４４に“Ｍ、Ｓ、Ｐ”が記録される。

【００４０】

コンテンツ部分の使用例としては、前記の移動、ストリーミング、再生以外にも、コピーなどがある。コンテンツ部分のコピーとは、本実施形態によってインポートされたコンテンツ部分をコピーすることを意味する。ところが、コンテンツインポート装置１０がコンテンツ部分をインポートするためには、コンテンツ部分コピーが前提されねばならず、その結果、本実施形態によってインポートされたコンテンツ部分をコピーするならば、２回のコピーが行われる。したがって、コンテンツインポート装置１０は、コピーワンスであるコンテンツ部分をインポートすることはできるが、本実施形態によってインポートされたコンテンツ部分をコピーするように許容することはできない。これが、使用制限情報がコピーワンスである場合に、使用規則フィールド４４に“Ｍ、Ｓ、Ｐ”のみが記録される理由である。

【００４１】

ブロードキャストフラグオンは、コンテンツ部分の無制限再配布が許容されないことを表すので、ブロードキャストフラグがブロードキャストフラグオンである場合には、使用範囲フィールド４３にデバイス、ドメインが記録され、使用規則フィールド４４に“オール”が記録される。

【００４２】

以上では、コンテンツに含まれた使用制限情報がコピー制御情報またはブロードキャストフラグである場合を例としてマッピングテーブルを
説明したが、この他にも多様な使用制限情報が存在し、それにより、マッピングテーブル

が変わりうるということは、当業者にとっては明らかなことである。

【００４３】

図７は、複数の使用制限情報を含むコンテンツが、本発明の一実施形態によってインポートされた後のコンテンツファイルの構造を示す図である。本実施形態では、インポートされたコンテンツファイルが全部三つのコンテンツ部分から構成されると仮定する。すなわち、三つのコンテンツ部分は、それぞれ異なるコンテンツキーを利用して暗号化され、各コンテンツキーを利用するためには、相異なるライセンスが要求される。

【００４４】

図７に示すように、各コンテンツ部分には、周期的にＰＩパケット６１０が挿入され、ＰＩパケット６１０には、ＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６２０、ＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　６４０を含む。

【００４５】

ＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６２０は、各コンテンツ部分を使用するために必要なライセンスを探すためのマッピング情報である。すなわち、ヘッダ６００には、ＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６０２及びＣＯＮＴＥＮＴ　ＩＤ　６０１を含んでおり、ライセンスも、当該コンテンツ部分についてのコンテンツＩＤを含んでいるので、各コンテンツ部分を使用しようとするデバイスは、当該コンテンツ部分のＰＩパケット６１０を探して、ＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６２０のみ分かれば、あらゆるコンテンツ部分に対して生成されたライセンスのうち必要なライセンスを探しうる。

【００４６】

一般的に、ＤＲＭシステムでは、コンテンツを管理するために、各コンテンツごとにコンテンツＩＤを与えるが、ＰＩパケット６１０にＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６２０の代わりに当該コンテンツのコンテンツＩＤを挿入してもマッピング情報として使用されうる。一般的に、コンテンツＩＤは、ＤＲＭシステムの政策によってその形態が定められうるが、場合によってそのサイズがＭＰＥＧ－２トランスポートパケットのペイロードに含まれうるデータの最大サイズである１８４バイトより大きくなりうるので、ＰＩパケットでは、コンテンツＩＤの代わりに、コンテンツＩＤに比べてそのデータのサイズは小さいが、各コンテンツＩＤに対応しうるマッピング情報として、ＣＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　６２０を使用することが望ましい。例えば、コンテンツＩＤが“ｕｒｎ：ｍａｒｌｉｎ：ｂｒｏａｄｃａｓｔ：１－０：ｃａｂｌｅ：０３３０２００６：０００１”である場合、ＣＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　６２０は、“ｃａｂｌｅ：０３３０２００６：０００１”のように構成されうる。本実施形態では、ライセンスを探すためのマッピング情報として、コンテンツＩＤの一部分から構成されるＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６２０を例としたが、各コンテンツＩＤと対応しうる情報ならば、いかなる形態の値でもＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６２０を代替できるであろう。

【００４７】

ＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　６４０は暗号化に使用された暗号化パラメータとして、前述のように、ＡＥＳ－１２８－ＣＴＲの暗号化方式を使用した場合、ＰＩパケットは、シリアル番号を含むことが望ましい。各ＰＩパケットに含まれたシリアル番号を基準としてその値を順次に増加させれば、次のＰＩパケットが表れる前までの暗号化されたトランスポートパケットの暗号化ブロックについてのシリアル番号が決定され、結局、当該暗号化ブロックのカウンタ値が分かるので、トランスポートパケットの復号化が可能になる。

【００４８】

一方、ヘッダ６００には、ＣＯＮＴＥＮＴ　ＩＤ　６０１、ＥＮＣＲＹＰＴＩＯＮＰＡＲＡＭＥＴＥＲ　６０２、ＰＩ　ＰＩＤ　６００及びＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６０４が含まれる。前述のように、ここでのＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　６０２は、ＡＥＳ－１２８－ＣＢＣ方式で使用されるイニシャルベクトルまた

はＡＥＳ－１２８－ＣＴＲ方式で使用されるＳＡＬＴになりうる。一方、ＣＯＮＴＥＮＴ　ＩＤ　６０１及びＣＩＤ　ＳＥＱＵＥＮＣＥ　ＮＵＭＢＥＲ　６０４は、各コンテンツ部分ごとに別途に存在し、ヘッダには、その他にも各コンテンツ部分の開始点及び終了点を表す位置情報などがさらに含まれうる。

【００４９】

図８は、本発明の一実施形態によってドメイン内のデバイスがインポートされたコンテンツを利用する過程を示すフローチャートである。

【００５０】

本発明によって、ユーザのドメインの外部からインポートされたコンテンツファイルを、ドメインに属するデバイスがインポート装置に要請し、それについての応答として当該コンテンツファイルを受信すれば（８１０）、受信されたコンテンツファイルのヘッダに含まれた情報を分析する（８２０）。前述のように、本発明によってインポートされたコンテンツファイルのヘッダには、ＰＩパケットを探しうるインデックス情報が含まれているので、デバイスは、ヘッダを分析することによってペイロードからＰＩパケットを容易に探し、ＰＩパケットを参照して必要な暗号化パラメータ及びライセンスを獲得した後、それらを利用して迅速にトランスポートパケットを復号化できる（８３０）。

【００５１】

図９は、本発明の一実施形態によってコンテンツをインポートする方法を示すフローチャートである。

【００５２】

本発明の一実施形態に係るコンテンツインポート装置は、ケーブル、衛星放送チャンネルなどの伝送チャンネルを通じて伝送ストリームを受信し、伝送ストリームから一つのプログラムを構成する第１コンテンツファイルを検出する（９００）。このとき、第１コンテンツファイルは、複数のコンテンツ部分から構成され、各コンテンツ部分のうち相異なる使用制限情報を有するコンテンツ部分が少なくとも２つ以上存在すると仮定する。

【００５３】

次いで、第１コンテンツファイルのペイロードを構成するパケットを暗号化するが（９０５）、暗号化のために、ＡＥＳ－１２８－ＣＢＣ及びＡＥＳ－１２８－ＣＴＲ方式が使用され、その他にも多様な方式が使用されうる。前述のように、暗号化に使用される暗号化パラメータは、ＡＥＳ－１２８－ＣＢＣ方式では、イニシャルベクトル、ＡＥＳ－１２８－ＣＴＲ方式では、ＳＡＬＴ及びシリアル番号である。

【００５４】

各コンテンツ部分についての暗号化が終了すれば、各コンテンツ部分についてのライセンスを発給する（９１０）。各コンテンツ部分についてのライセンスには、当該コンテンツ部分の暗号化に使用したコンテンツキーが暗号化されて含まれている。コンテンツキーの暗号化には、当該コンテンツ部分の使用範囲によってデバイスキーまたはドメインキーが使用されてもよいが、当該コンテンツ部分が特定のデバイスでのみ使用されねばならない場合には、デバイスキーで暗号化され、当該コンテンツ部分がドメイン内のデバイスにより共有されうるドメインキーで暗号化される。また、各ライセンスには、当該コンテンツ部分とマッピングさせるためのマッピング情報が含まれる。

【００５５】

次いで、各コンテンツ部分の暗号化に使用した暗号化パラメータ及びライセンスマッピング情報を含むＰＩパケットを生成して、メディア情報を含むトランスポートパケットの間に周期的に挿入して（９１５）、第２コンテンツファイルのペイロードを生成し、各コンテンツ部分の位置情報と、ＰＩパケットのパケットＩＤ及びＳＡＬＴなどの暗号化パラメータとを含むファイルヘッダを生成する（９２０）。ＰＩパケットをＰＭＴパケットと同じ周期で配置することが望ましいということは前述した通りである。

【００５６】

ペイロード及びヘッダが生成されれば、生成されたペイロードとヘッダとをパッケージングして第２コンテンツファイルを生成した後（９２５）、保存する（９３０）。保存さ

れた第２コンテンツファイルは、第１コンテンツファイルがインポートされた後のコンテンツファイルであり、インポート装置は、ユーザのドメイン内であらゆるデバイスに、または特定デバイスの要請に応答して第２コンテンツファイルを配布する（９３５）。

【００５７】

図１０は、本発明の一実施形態によってコンテンツをインポートする装置の構造を示す図である。本実施形態では、インポートするコンテンツが複数の使用制限情報を含むと仮定する。図１０に示すように、本発明の一実施形態に係るコンテンツインポート装置９５０は、検出部９５１、使用規則決定部９５２、ヘッダ生成部９５３、暗号化部９５４、ＰＩパケット生成部９５５、ライセンス発給部９５６、ファイル生成部９５７、保存部９５８及び送受信部９５９を備える。

【００５８】

検出部９５１は、ドメインの外部の多様な伝送チャンネルを通じて受信された伝送ストリームから一つのプログラムを構成するコンテンツファイルを検出し、また、各コンテンツ部分についての使用制限情報を検出する。前述のように、使用制限情報の例としては、コピー制御情報、ブロードキャストフラグなどがありうる。

【００５９】

使用規則決定部９５２は、検出部９５１で検出した使用制限情報に基づいて、コンテンツ部分のそれぞれについての使用規則を決定する。

【００６０】

暗号化部９５４は、検出部９５１により検出されたコンテンツファイル、すなわち、まだインポートされる前のコンテンツファイルに含まれた各コンテンツ部分を該当する使用制限情報によって別途のコンテンツキーを利用して暗号化する。また、各コンテンツ部分の暗号化に使用したコンテンツキーは、デバイスキーまたはドメインキーを利用して暗号化する。暗号化されたコンテンツ部分が特定のデバイスでのみ使用されねばならない場合ならば、当該デバイスのデバイスキーを利用して暗号化し、ドメイン内のあらゆるデバイスにより共有されてもよい場合ならば、ドメインキーを利用して暗号化する。

【００６１】

ライセンス発給部９５６は、コンテンツ部分のそれぞれについて別途のライセンスを発給するが、前述のように、ライセンスは、デバイスがコンテンツ部分を使用するために必要なものであって、各ライセンスは、当該コンテンツ部分についての使用規則及び暗号化されたコンテンツキーを含む。

【００６２】

ヘッダ生成部９５３は、インポートされた後のコンテンツファイルに使用するファイルヘッダを生成するが、このヘッダには、ドメインのデバイスがインポートされたコンテンツファイルを使用しようとするとき、各トランスポートパケットを全てパージングせずとも、インポートされたコンテンツファイルの構造を把握し、各コンテンツ部分についてのライセンスを予め獲得させうる情報が含まれる。このような情報には、ＰＩパケットのパケットＩＤ、各コンテンツ部分についての位置情報、ＳＡＬＴやイニシャルベクトルのような暗号化パラメータ及びライセンスマッピング情報などが含まれる。また、各コンテンツ部分についてのライセンスもヘッダに含まれることが望ましい。

【００６３】

ＰＩパケット生成部９５５は、所定数の暗号化されたトランスポートパケットを復号化するために必要な情報を含むＰＩパケットを生成する。前述のように、このような情報には、ライセンスマッピング情報及びＡＥＳ－１２８－ＣＴＲ方式で暗号化されたトランスポートパケットを復号化するためのシリアル番号などが含まれる。ＰＩパケットは暗号化されない。

【００６４】

ファイル生成部９５７は、ＰＩパケットを、メディア情報を含んでいるトランスポートパケットの間に周期的に配置して、インポートされたコンテンツファイルのペイロードを生成し、ヘッダ生成部９５３で生成したファイルヘッダをペイロードに付加してコンテン

ツファイルを生成する。このとき、生成されたコンテンツファイルは、インポートされたコンテンツファイルである。保存部９５８は、インポートされたコンテンツファイルを保存し、送受信部９５９は、ユーザのドメインに属するデバイスの要請を受信すれば、それについての応答として保存されたコンテンツファイルを伝送する。

【００６５】

図１１は、本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＴＲ方式により暗号化されたコンテンツファイルを使用する方法を示すフローチャートである。

【００６６】

ステップ１１０１で、ＰＩパケットからシリアルナンバー及びマッピング情報を解析して抽出する。

【００６７】

ステップ１１０２で、コンテンツファイルのヘッダに含まれたＳＡＬＴ値と、ステップ１１０１で抽出したシリアルナンバーとを利用してカウンタ値を生成する。

【００６８】

ステップ１１０３で、マッピング情報を利用してコンテンツＩＤを選択する。

【００６９】

ステップ１１０４で、選択されたコンテンツＩＤを利用してライセンスを選択する。選択されたライセンスは、選択されたコンテンツＩＤを含んでいるので、コンテンツＩＤを利用して適切なライセンスを選択できる。

【００７０】

ステップ１１０５で、選択されたライセンスからコンテンツキーを解析して抽出する。

【００７１】

ステップ１１０６で、コンテンツキー及びカウンタ値を利用してコンテンツファイルの復号化を行う。

【００７２】

図１２は、本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＴＲ方式により暗号化されたコンテンツファイルを使用する装置の構造を示す図である。

【００７３】

本発明によってインポートされたコンテンツが入力されれば、シリアルナンバー解析部１２０１は、ＰＩパケットから入力されたコンテンツのシリアルナンバーを解析し、カウンタ値生成部１２０４は、シリアルナンバーとコンテンツファイルヘッダに含まれたＳＡＬＴ値とを利用してカウンタ値を生成する。

【００７４】

一方、マッピング情報解析部１２０２は、ＰＩパケットからマッピング情報を解析し、コンテンツＩＤ選択部１２０３は、マッピング情報解析部１２０２から伝達されたマッピング情報を利用してコンテンツＩＤを選択する。ライセンス選択部１２０５は、コンテンツＩＤ選択部１２０３により選択されたコンテンツＩＤを利用して適切なライセンスを選択し、コンテンツキー解析部１２０７は、ライセンス選択部１２０５が選択したライセンスからコンテンツキーを解析する。

【００７５】

復号化部１２０６は、カウンタ値生成部１２０４から伝達されたカウンタ値と、コンテンツする解析部１２０７から伝達されたコンテンツキーとを利用して暗号化されたコンテンツの復号化を行う。

【００７６】

図１３は、本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＢＣ方式により暗号化されたコンテンツファイルを使用する方法を示すフローチャートである。

【００７７】

ステップ１３０１で、ＰＩパケットから暗号化されたコンテンツについてのイニシャルベクトル及びマッピング情報を解析して抽出する。

【００７８】

ステップ１３０２で、マッピング情報を利用してコンテンツＩＤを選択する。

【００７９】

ステップ１３０３で、選択されたコンテンツＩＤを利用して適切なライセンスを選択する。

【００８０】

ステップ１３０４で、選択されたライセンスから暗号化されたコンテンツを復号化するためのコンテンツキーを解析する。

【００８１】

ステップ１３０５で、コンテンツキー及びイニシャルベクトルを利用して暗号化されたコンテンツの復号化を行う。

【００８２】

図１４は、本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＢＣ方式により暗号化されたコンテンツファイルを使用する装置の構造を示す図である。

【００８３】

イニシャルベクトル解析部１４０１は、入力されたコンテンツファイルのＰＩパケットからイニシャルベクトルを解析して抽出する。

【００８４】

マッピング情報解析部１４０２は、入力されたコンテンツファイルのＰＩパケットからマッピング情報を解析して抽出し、コンテンツＩＤ選択部１４０３は、抽出されたマッピング情報を利用してコンテンツＩＤを選択する。ライセンス選択部１４０６は、選択されたコンテンツＩＤを利用して適切なライセンスを選択し、コンテンツキー解析部１４０５は、選択されたライセンスからコンテンツキーを解析して抽出する。

【００８５】

復号化部１４０４は、コンテンツキー及びイニシャルベクトルを利用して暗号化されたコンテンツを復号化する。

【００８６】

一方、前述の本発明の実施形態は、コンピュータで実行されうるプログラムで作成可能であり、コンピュータで読み取り可能な記録媒体を利用して前記プログラムを動作させる汎用のディジタルコンピュータで具現されうる。

【００８７】

前記コンピュータで読み取り可能な記録媒体は、マグネチック記録媒体（例えば、ＲＯＭ、フロッピー（登録商標）ディスク、ハードディスクなど）、光学的判読媒体（例えば、ＣＤ－ＲＯＭ、ＤＶＤ等）及びキャリアウェーブ（例えば、インターネットを介した伝送）のような記録媒体を含む。

【００８８】

以上、本発明についてその望ましい実施形態を中心として説明した。当業者は、本発明が本発明の本質的な特性から逸脱しない範囲で変形された形態で具現されうるということが理解できるであろう。したがって、開示された実施形態は、限定的な観点ではなく、説明的な観点で考慮されねばならない。本発明の範囲は、前述の説明ではなく、特許請求の範囲に示されており、それと同等な範囲内にあるあらゆる相違点は、本発明に含まれたものと解釈されねばならない。

【図面の簡単な説明】

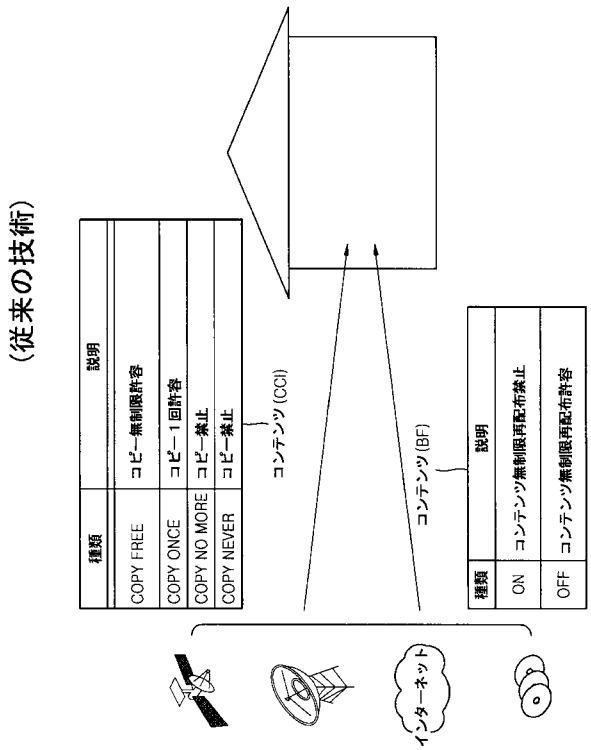
【００８９】

【図１】従来のデジタルコンテンツの保護環境を示す図である。

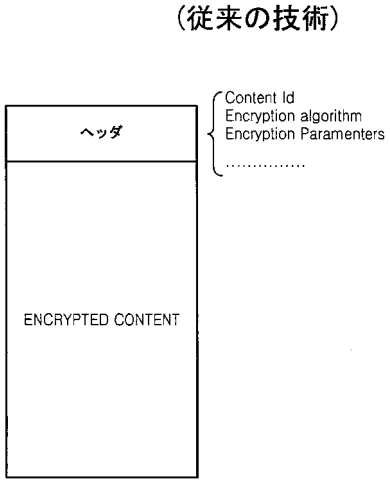
【図２】従来の技術によってインポートされたコンテンツファイルの構造を示す図である。

【図３Ａ】ＡＥＳによる暗号化方式を説明するための図である。
【図３Ｂ】ＡＥＳによる暗号化方式を説明するための図である。
【図４】本発明の一実施形態によってインポートされたコンテンツファイルの構造を示す図である。
【図５】複数の使用制限情報を含むコンテンツをインポートする環境を説明するための図である。
【図６】使用制限情報を使用規則に変換したマッピングテーブルである。
【図７】複数の使用制限情報を含むコンテンツが、本発明の一実施形態によってインポートされた後のコンテンツファイルの構造を示す図である。
【図８】本発明の一実施形態によってドメイン内のデバイスがインポートされたコンテンツを利用する過程を示すフローチャートである。
【図９】本発明の一実施形態によってコンテンツをインポートする方法を示すフローチャートである。
【図１０】本発明の一実施形態によってコンテンツをインポートする装置の構造を示す図である。
【図１１】本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＴＲ方式により暗号化されたコンテンツファイルを使用する方法を示すフローチャートである。
【図１２】本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＴＲ方式により暗号化されたコンテンツファイルを使用する装置の構造を示す図である。
【図１３】本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＢＣ方式により暗号化されたコンテンツファイルを使用する方法を示すフローチャートである。
【図１４】本発明の一実施形態によってインポートされたコンテンツのうち、ＡＥＳ－１２８－ＣＢＣ方式により暗号化されたコンテンツファイルを使用する装置の構造を示す図である。
【符号の説明】
【００９０】
５００　ＤＲＭシステム
５１、５２、５３　デバイス
９５０　コンテンツインポート装置
９５１　検出部
９５２　使用規則決定部
９５３　ヘッダ生成部
９５４　暗号化部
９５５　ＰＩパケット生成部
９５６　ライセンス発給部
９５７　ファイル生成部
９５８　保存部
９５９　送受信部
１２０１　シリアルナンバー解析部
１２０２、１４０２　マッピング情報解析部
１２０３、１４０３　コンテンツＩＤ選択部
１２０４　カウンタ値生成部
１２０５、１４０６　ライセンス選択部
１２０６　復号化部
１２０７、１４０５　コンテンツキー解析部
１４０１　イニシャルベクトル解析部
１４０４　復号化部

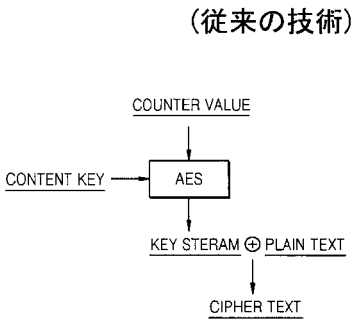
【図１】



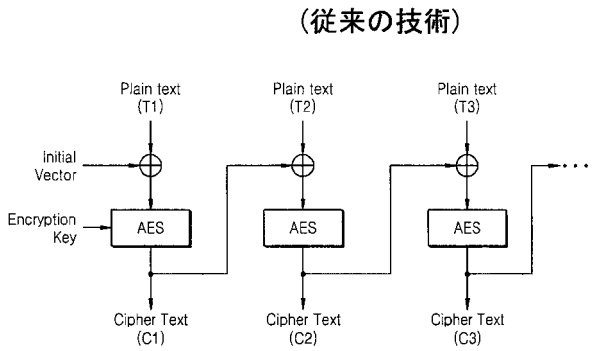
【図２】



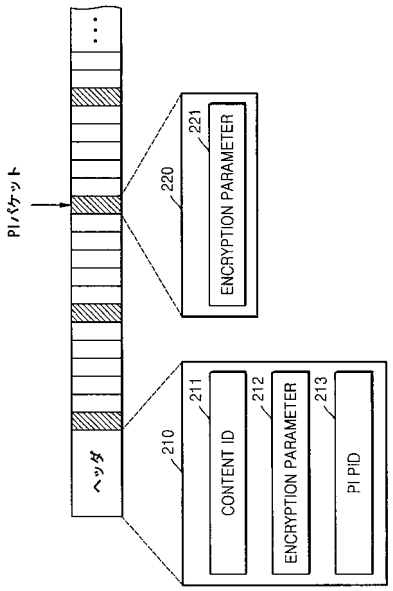
【図３Ａ】



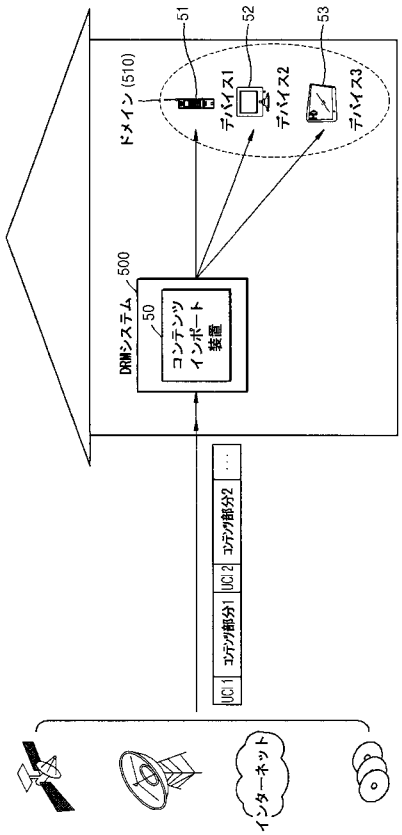
【図３Ｂ】



【図４】



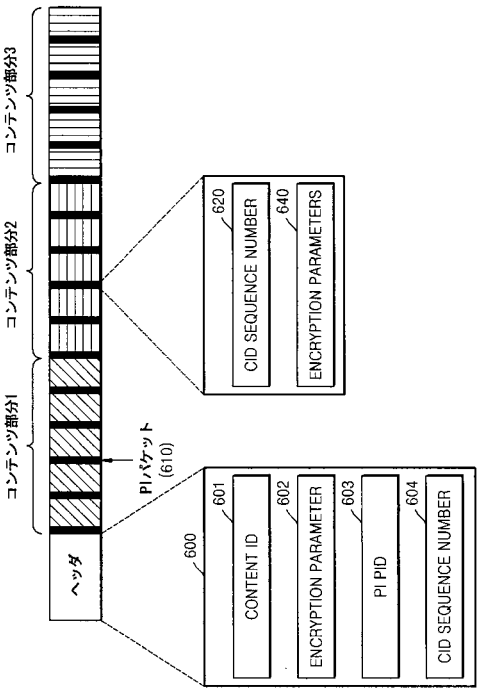
【図５】



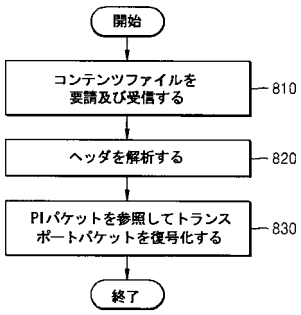
【図６】

		41	42	43	44
	UCI		Import	Bind Type	Usage Rule
CCI	COPY FREE		O	Device, Domain	All
	COPY ONCE		O	Device	M,S,P
	COPY NO MORE		N/A	-	-
	COPY NEVER		X	-	-
BF	ON		O	Device, Domain	All
	OFF		X	-	-

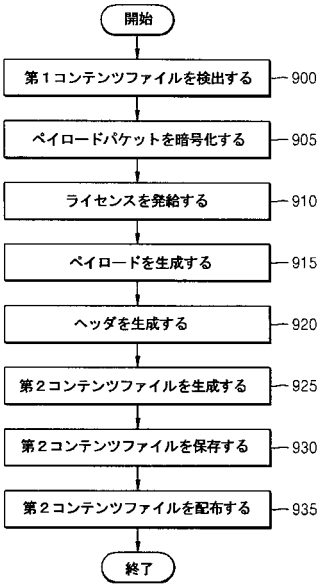
【図７】



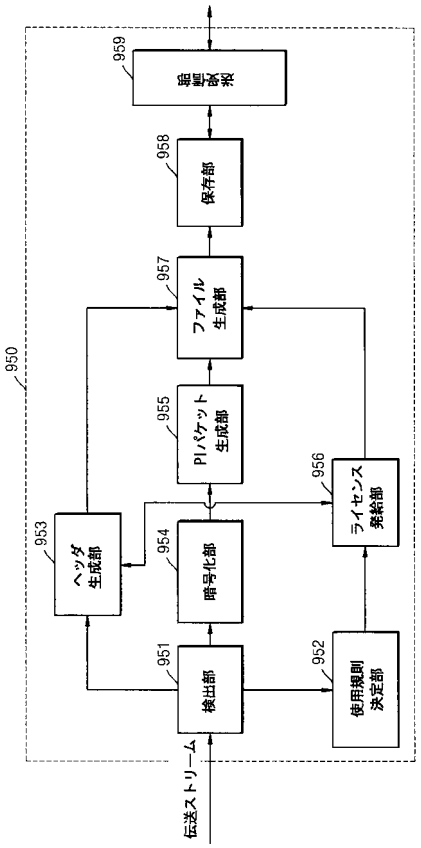
【図８】



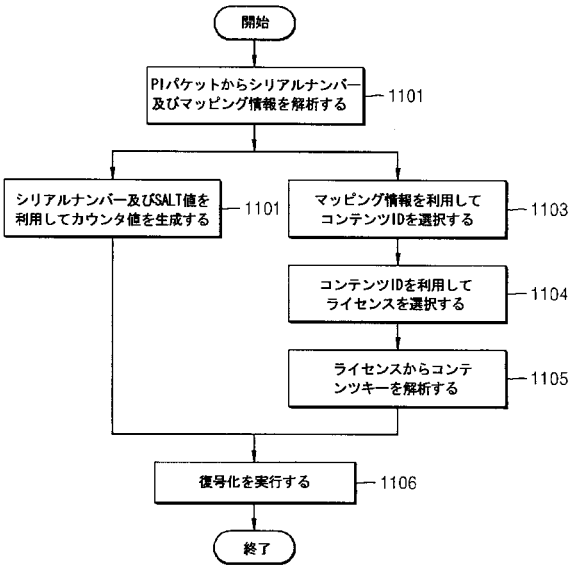
【図９】



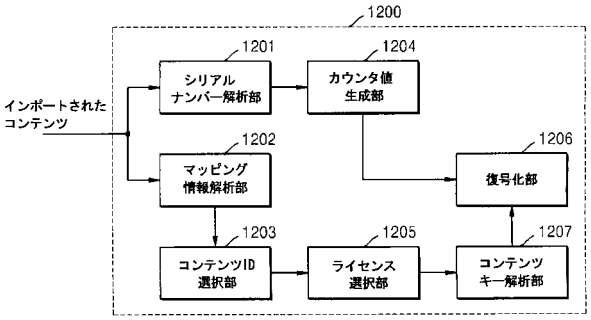
【図１０】



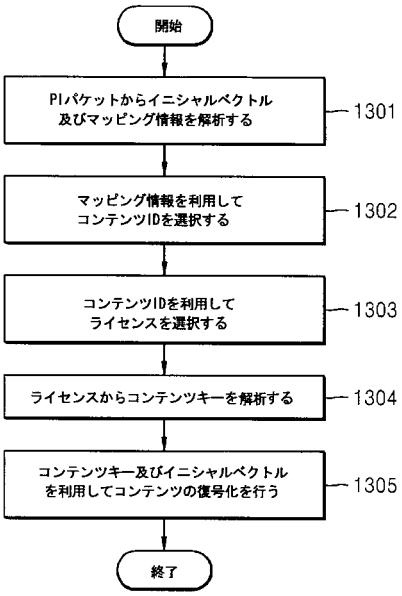
【図１１】



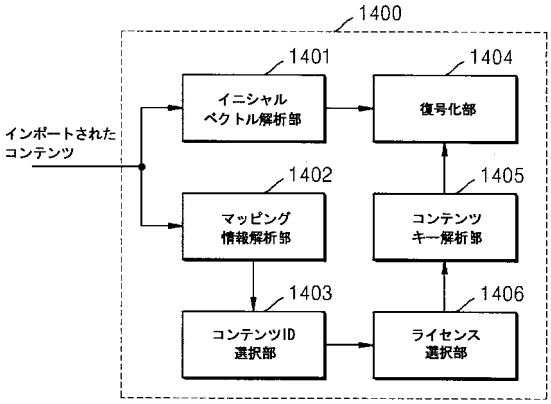
【図１２】



【図１３】


開始
PIパケットからイニシャルベクトル及びマッピング情報を解析する
1301
マッピング情報を利用してコンテンツIDを選択する
1302
コンテンツIDを利用してライセンスを選択する
1303
ライセンスからコンテンツキーを解析する
1304
コンテンツキー及びイニシャルベクトルを利用してコンテンツの復号化を行う
1305
終了

【図１４】


1400
1401
イニシャルベクトル解析部
1404
復号化部
インポートされたコンテンツ
1402
マッピング情報解析部
1405
コンテンツキー解析部
1403
コンテンツID選択部
1406
ライセンス選択部

フロントページの続き

(72)発明者　金　奉　禪
大韓民国京畿道城南市盆唐区金谷洞　青率マウル住公９團地アパート９０３棟４１１号（番地なし）
(72)発明者　尹　映　善
大韓民国京畿道水原市勸善区勸善洞　常緑アパート５１１棟７０４号（番地なし）

審査官　金沢　史明

(56)参考文献　特開２００３－１４１８１６（ＪＰ，Ａ）
特開２００４－３０３１１１（ＪＰ，Ａ）
特開２００３－１０００１９（ＪＰ，Ａ）
特表２００５－５１３８３９（ＪＰ，Ａ）
特開平０７－２８８７９８（ＪＰ，Ａ）
特開２００２－３７４５１１（ＪＰ，Ａ）
特開２００４－３６２５４６（ＪＰ，Ａ）
特開２００１－０８６１１０（ＪＰ，Ａ）
特開２００３－１３４１０６（ＪＰ，Ａ）
国際公開第２００５／０９９１６９（WO，Ａ１）
国際公開第２００５／０４３８９９（WO，Ａ１）
特開２００３－０９２７５２（ＪＰ，Ａ）
特開２００４－２２８７５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００－　９／３８
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／１０
Ｇ０６Ｆ　２１／６２