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

特許第5259097号
(P5259097)

(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		
G06F 21/10	(2013.01)	G06F	21/22	110K
G06F 21/62	(2013.01)	G06F	21/24	163G
H04N 7/16	(2011.01)	G06F	21/24	166A
G09C 1/00	(2006.01)	H04N	7/16	Z
		G09C	1/00	660D

請求項の数 8　(全 16 頁)

(21)出願番号　特願2007-35314(P2007-35314)
(22)出願日　平成19年2月15日(2007.2.15)
(65)公開番号　特開2007-220125(P2007-220125A)
(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　60/773,341
(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　10-2006-0036825
(32)優先日　平成18年4月24日(2006.4.24)
(33)優先権主張国　韓国(KR)

前置審査

(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　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】複数のコンテンツ部分を含むコンテンツ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】
複数のコンテンツ部分を含む第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、
前記コンテンツ部分の使用制限情報によって前記コンテンツ部分を、コンテンツキーを利用して暗号化するステップと、
前記使用制限情報によって前記コンテンツ部分についてのライセンスを生成するステップと、
前記コンテンツ部分を復号化するのに必要な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、
前記コンテンツ部分を管理するための管理情報をコンテンツ部分別に生成するステップと、
前記コンテンツ部分、前記管理情報、前記ライセンスを含む第２コンテンツファイルを生成するステップと、を含み、
前記管理情報は、前記第２コンテンツファイル内にコンテンツ部分と区別されるヘッダ部分に含まれ、前記コンテンツ部分のそれぞれのコンテンツＩＤ、位置情報、前記コンテンツ部分についてのそれぞれのライセンスを探せるように前記コンテンツＩＤとマッピングされたマッピング情報を含み、
前記ライセンスは、当該コンテンツ部分についてのコンテンツＩＤ、前記当該コンテンツ部分についてのコンテンツキー及び前記当該コンテンツ部分についての使用規則を含み

、
前記プロテクションインフォメーションは、前記第２コンテンツファイルのコンテンツ部分内に周期的に挿入され、
前記プロテクションインフォメーションは、少なくとも一つのコンテンツ部分についてのマッピング情報と前記コンテンツ部分を暗号化するのに使用された暗号化パラメータを含むことを特徴とするインポート方法。
【請求項２】
前記コンテンツ部分は、相異なる使用制限情報を有することを特徴とする請求項１に記載のインポート方法。
【請求項３】
前記第１コンテンツを他のコンテンツと識別するための情報（ＰＲＯＧＲＭ＿ＩＤ）を生成するステップをさらに含むことを特徴とする請求項１に記載のインポート方法。
【請求項４】
前記プロテクションインフォメーションの識別情報を生成するステップをさらに含むことを特徴とする請求項１に記載のインポート方法。
【請求項５】
複数のコンテンツ部分を含む第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、
前記コンテンツ部分の使用制限情報によって前記コンテンツ部分を、コンテンツキーを利用して暗号化する暗号化部と、
前記使用制限情報によって前記コンテンツ部分についてのライセンスを生成するライセンス発給部と、
前記コンテンツ部分を復号化するのに必要な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手段と、
前記コンテンツ部分を管理するための管理情報を各コンテンツ部分別に生成する手段と、
前記コンテンツ部分、前記ライセンス、前記管理情報を含む第２コンテンツファイルを生成するファイル生成部と、を備え、
前記管理情報は、第２コンテンツファイル内にコンテンツ部分と区別されるヘッダ部分に含まれ、前記コンテンツ部分のそれぞれのコンテンツＩＤ、位置情報、前記コンテンツ部分についてのそれぞれのライセンスを探せるように前記コンテンツＩＤとマッピングされたマッピング情報を含み、
前記ライセンスは、当該コンテンツ部分についてのコンテンツＩＤ、前記当該コンテンツ部分についてのコンテンツキー及び前記当該コンテンツ部分についての使用規則を含み、
前記プロテクションインフォメーションは、前記第２コンテンツファイルのコンテンツ部分内に周期的に挿入され、
前記プロテクションインフォメーションは、少なくとも一つのコンテンツ部分についてのマッピング情報と前記コンテンツ部分を暗号化するのに使用された暗号化パラメータを含むことを特徴とするインポート装置。
【請求項６】
前記コンテンツ部分は、相異なる使用制限情報を有することを特徴とする請求項５に記載のインポート装置。
【請求項７】
前記第１コンテンツを他のコンテンツと識別するための情報（ＰＲＯＧＲＭ＿ＩＤ）を生成する手段をさらに備えることを特徴とする請求項５に記載のインポート装置。
【請求項８】
前記プロテクションインフォメーションの識別情報を生成する手段をさらに備えることを特徴とする請求項５に記載のインポート装置。

【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】
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、それによって複数の

ライセンスが必要となる。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であって、このようなコンテンツがインポートされてコンテンツファイルとして保存された場合、ユーザのドメインに属したデバイスが、このようなコンテンツファイルを利用するためには、コンテンツファイルを構成するトランスポートパケットをパージングして使用しようとするコンテンツファイルが、いくつのコンテンツ部分から構成されているかを把握し、各コンテンツ部分が何なるライセンスを必要とするかを判断して、当該ライセンスを獲得せねばならないので、時間遅延が起こるという問題がある。特に、このような時間遅延は、コンテンツを使用しようとするデバイスが、インポートされたコンテンツファイルをストリーミングで提供される場合にさらに問題となる。

【発明の開示】

【発明が解決しようとする課題】

【０００８】

本発明は、複数の使用制限情報を含むコンテンツをインポートして一つのコンテンツファイルに変換するとき、各コンテンツ部分の構造に関する情報、及び各コンテンツ部分を復号化して使用するために必要な情報の位置を予め知らせるヘッダをインポートされたコンテンツファイルに含ませるインポート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】

【０００９】

このような目的を達成するための本発明は、複数のコンテンツ部分を含む第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、（ａ）前記コンテンツ部分の使用制限情報によって前記コンテンツ部分を暗号化するステップと、（ｂ）前記使用制限情報によって前記コンテンツ部分についてのライセンスを生成するステップと、（ｃ）前記コンテンツ部分及びライセンスを備える第２コンテンツファイルを生成するステップと、を含むことを特徴とする。

【００１０】

このとき、前記暗号化されたコンテンツ部分のそれぞれを使用するために必要な情報は、前記第２コンテンツファイル内での前記暗号化されたコンテンツ部分のそれぞれの位置を表す第１情報、前記暗号化されたコンテンツ部分のそれぞれの復号化に使用される第２情報、及び前記複数の使用制限情報に基づいて前記コンテンツ部分のそれぞれについて規定された使用規則のうち少なくとも一つを含むことを特徴とする。

【００１１】

ここで、前記第１情報は、前記第２コンテンツファイル内で前記暗号化されたコンテンツ部分のそれぞれが開始する位置及び／または終了する位置を表す情報であり、前記第２情報は、前記暗号化されたコンテンツ部分のそれぞれの暗号化に使用された暗号化パラメータ及び／または前記暗号化されたコンテンツ部分のそれぞれを復号化できるコンテンツキーである。

【００１２】

また、本発明は、前記コンテンツ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。

【００１３】

また、本発明は、複数の使用制限情報を含む第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、前記複数の使用制限情報に基づいて前記第１コンテンツファイルに含まれたコンテンツ部分を適応的に暗号化する暗号化部と、前記暗号化されたコンテンツ部分のそれぞれを使用するために必要な情報の位置を提供するヘッダを生成するヘッダ生成部と、前記生成されたヘッダを備える第２コンテンツファイル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】

【００１４】

本発明によれば、ユーザのドメインに属するデバイスが、インポートされたコンテンツファイルのうち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を使用する場合、コンテンツファイルのトランスポートパケットをパージングせずとも、ヘッダ情報を分析するだけで、当該コンテンツファイルがいくつのコンテンツ部分から構成されているかを把握し、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予め獲得できるので、コンテンツを使用するために必要な準備時間を短縮させ、特に、ストリーミング方式で当該コンテンツファイルを提供されて再生する場合、コンテンツ部分が変わる区間で、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獲得するために時間が遅延されることを防止できる。

【００１５】

また、本発明によれば、インポートされたコンテンツファイルのヘッダに各コンテンツ部分の位置情報を挿入して各コンテンツ部分を使用するデバイスは、各コンテンツ部分に対応するライセンスを正確に適用できる。

【発明を実施するための最良の形態】

【００１６】

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。

【００１７】

図２は、本発明が適用されるデジタルコンテンツの保護環境を示す図である。図２に示すように、本発明が適用されるデジタルコンテンツの保護環境は、ＤＲＭシステム１００、ＨＤＣＰ（Ｈｉｇｈ Ｂａｎｄｗｉｄｔｈ Ｄｉｇｉｔａｌ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）システム１１０及びＤＴＣＰ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）システム１２０のような多様なコンテンツの保護システムと、これらによって保護される複数のデバイス２１ないし２３から構成される。

【００１８】

ＤＲＭシステム１００は、外部から受信されたコンテンツの権利を管理するためのシステムである。ＨＤＣＰシステム２００は、ＤＶＩ（デジタル ビデオ インターフェース）のような高帯域幅インターフェースを通じてデジタルディスプレイに出力されるコンテンツのコピーを防止するためのシステムである。ＤＴＣＰシステム３００は、ＩＥＥＥ（インスティチュート オブ エレクトリカル アンド エレクトロニクス エンジニアーズ）１３９４の規格に従うＵＳＢ（ユニバーサル シリアル バス）を通じて伝送されるコンテンツのコピーを防止するためのシステムである。前記のようなコンテンツ保護システム以外にも、ＣＡＳ（コンディショナル アクセス システム）システム、ＣＰＲＭ（Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ ｆｏｒ Ｒｅｃｏｒｄａｂｌｅ Ｍｅｄｉａ）システムのような他のコンテンツ保護システムがさらに含まれうる。

【００１９】

ＤＲＭシステム１００は、従来のコピー制御、ブロードキャストフラグなどによって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１００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１０を備える。

【００２０】

ここで、インポートとは、ＤＲＭシステム１００の規則に従ってコンテンツを構成するコンテンツ部分のそれぞれにライセンスを発給し、このコンテンツ部分を暗号化する過程であって、すなわち、ＤＲＭシステム１００の規則に従わないコンテンツファイルを、ＤＲＭシステム１００の規則に従うコンテンツファイルに変換する過程をいう。特に、コンテンツのどの部分が一つのコンテンツ部分であるかは、使用制限情報またはライセンスによって区別される。すなわち、コンテンツ部分のそれぞれは、相異なる使用制限情報またはライセンスを有する。一方、コンテンツファイルとは、コンテンツ部分及びそれらのそれぞれについてのコピー制御情報、またはライセンスなどを含むファイルを言うものであ

って、一つのコンテンツファイルは、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。したがって、コンテンツファイルという用語は、単純にコンテンツという用語と呼ばれてもよいということを、当業者ならば理解できるであろう。

【００２１】

本発明に係るコンテンツインポート装置１０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備えさせる。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。以下ではさらに詳細に説明する。

【００２２】

図３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。

【００２３】

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（３１０）、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（３２０）。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。

【００２４】

次いで、コンテンツキーを利用してコンテンツ部分を暗号化するが（３３０）、暗号化のために、ＡＥＳ－１２８－ＣＢＣや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。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及びパケットの一連番号情報が使用されるが、各コンテンツ部分に対してそれぞれ異なる値が使用される。本発明では、コンテンツファイルがＭＰＥＧ－２規格に従うトランスポートパケット（ＴＳ　Ｐａｃｋｅｔ）から構成されると仮定し、暗号化は、このトランスポートパケット単位で行われるが、コンテンツファイルを構成するトランスポートパケットのうち、メディアストリームを載せているトランスポートパケットの間に、周期的に各コンテンツ部分の暗号化に使用した暗号化方式及び暗号化パラメータを知らせるトランスポートパケットを挿入する。また、このようなトランスポートパケットには、当該コンテンツ部分を復号化するために必要なライセンスを探させうるマッピング情報も含まれるが、以下では、このようなトランスポートパケットに含まれた情報をＰＩ（プロテクション　インフォメーション）と称すことにする。ＰＩを含むトランスポートパケットであるＰＩパケットに関する詳細な説明は、図６を参照して後述する。

【００２５】

各コンテンツ部分についての暗号化が終われば、各コンテンツ部分についてのライセンスを発給する（３４０）。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うるが、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って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。

【００２６】

一方、コンテンツ部分についてのライセンスのそれぞれには、当該コンテンツについての使用規則も含まれるが、デバイスは、当該コンテンツ部分を復号化できるとしても、ラ

イセンスに含まれた使用規則を違反してはならない。このような使用規則は、インポートされる前にコンテンツファイルに含まれていた使用制限情報に基づいて新たに規定されるが、これについての詳細な説明は、図４を参照して後述する。

【００２７】

次いで、インポートされたコンテンツファイルに含ませるヘッダを生成するが（３５０）、このヘッダには、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デバイスをして予め各コンテンツ部分についてのライセンス及び復号化パラメータを得させる情報が含まれる。すなわち、デバイスは、このヘッダ情報を分析して、予め必要なライセンス及び復号化パラメータを獲得できる。各コンテンツ部分についてのライセンスも、このヘッダと共にパッケージングされることが望ましい。ヘッダに関する詳細な説明は、図７を参照して後述する。

【００２８】

ヘッダが生成されれば、ヘッダを備える第２コンテンツファイルを生成し（３６０）、ストレージに保存する（３７０）。すなわち、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、ユーザのドメイン内で全てのデバイスに、または特定デバイスの要請により配布される（３８０）。

【００２９】

図４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４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。特に、図４に示す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ついてのものである。

【００３０】

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。

【００３１】

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再生することを意味する。

【００３２】

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。

【００３３】

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。

【００３４】

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。デバイス範囲内でのコンテンツ部分のコピーを含むいかなる形態の使用も、コンテンツ部分の無制限再配布禁止に符合し、ドメイン範囲もユーザにより認識可能な特定の地域であるので、ドメイン範囲内でのコンテンツ部分のコピーを含むいかなる形態の使用も、コンテンツ部分の無制限再配布禁止に符合する。

【００３５】

図５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。図３での過程により、ユーザのドメインの外部から受信された第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の第２コンテンツファイルは、インポート装置に保存されている。ドメインに属するデバイスが、インポート装置に第２コンテンツファイルを要請し、それについての応答として第２コンテンツファイルを受信すれば（５１０）、ヘッダに含まれた情報を分析する（５２０）。前述のように、ヘッダを分析すれば、第２コンテンツファイルのトランスポートパケットをパージングせずとも、第２コンテンツファイルの構造及び第２コンテンツファイルを構成する各コンテンツ部分を復号化して使用するためのライセンス及び暗号化パラメータを予め獲得して復号化を準備することができる。すなわち、デバイスは、復号化しようとするコンテンツ部分に含まれたＰＩパケットを参照して、当該ライセンスを探すためのマッピング情報及び復号化パラメータを獲得する。また、マッピング情報を通じて当該ライセンスを探し、最終的にコンテンツ部分を構成する各トランスポートパケットを復号化することによって、所望のコンテンツ部分を使用できる。

【００３６】

図６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。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三つのコンテンツ部分から構成されると仮定する。図６に示すように、各コンテンツ部分には、周期的にＰＩを含むＰＩパケット６１０が挿入される。ＰＩパケット６１０は、ＣＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　６２０、ＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　６４０を含む。

【００３７】

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、ＣＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　６２０は、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、使用しようとするコンテンツ部分に該当するライセンスを探すために、三つのコンテンツ部分のうちどのコンテンツ部分であるかを知らせる。

【００３８】

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ＥＣＩＤ＿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。

【００３９】

ＥＮＣＲＹＰＴＩＯＮ　ＰＡＲＡＭＥＴＥＲ　６４０は、暗号化に使用された暗号化パラメータである。例えば、暗号化方式としてＡＥＳ－１２８－ＣＴＲが使用された場合、ＰＩパケットには、シリアル番号情報が含まれうる。

【００４０】

図７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ヘッダ構造を示す図である。図７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のヘッダは、ＰＲＯＧＲＡＭ＿ＩＤ　７０１及びＰＩ＿ＰＩＤ　７０２を含み、各コンテンツ部分別にＣＯＮＴＥＮＴ＿ＩＤ　７０３、ＣＯＮＴＥＮＴ＿ＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　７０４、ＣＯＮＴＥＮＴ＿ＳＴＡＲＴ＿ＰＯＩＮＴＥＲ　７０５、ＣＯＮＴＥＮＴ＿ＥＮＤ＿ＰＯＩＮＴＥＲ　７０６を含む。また、各コンテンツ部分に対応するライセンス７１０を含む。以下では、前記情報について詳細に説明する。

【００４１】

ＰＲＯＧＲＡＭ＿ＩＤ　７０１は、プログラムのタイトルを表す情報である。すなわち、Ｎ個のコンテンツ部分により完成する一つのプログラムを他のプログラムと区別させる識別子であり、ＤＲＭシステムで規定する政策によってその形態が決定されうる。

【００４２】

ＰＩ＿ＰＩＤ　７０２は、ＰＩパケットを探すためのインデックス情報である。各コンテンツ部分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によって、各パケットのヘッダに固有のパケットＩＤを有する。すなわち、各コンテンツ部分は、何れも別途のライセンスを有し、暗号化方式及び暗号化パラメータも相異なりうるが、一つのコンテンツファイルに含まれたトランスポートパケットのうち、ＰＩを含んでいるＰＩパケットのパケットＩＤは、あらゆるコンテンツ部分に対して同じであるので、ＰＩ＿ＰＩＤ　７０２を分析すれば、ＰＩパケットを探し出しうる。

【００４３】

ＣＯＮＴＥＮＴ＿ＩＤ　７０３は、各コンテンツ部分を区別するための識別子である。各コンテンツ部分は、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、当該コンテンツ部分のコンテンツＩＤが含んでいるので、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。

【００４４】

ＣＯＮＴＥＮＴ＿ＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　７０４は、図６で説明したように、ＰＩパケットを当該ライセンスとマッピングするための情報であるが、ＣＯＮＴＥＮＴ＿ＩＤ　７０３のサイズが、ＰＩパケットに挿入するには大き過ぎるので、その一部分のみをＰＩパケットに挿入し、図６に示すように、コンテンツファイルヘッダにも記録する。すなわち、デバイスは、ＰＩパケットに記録されたＣＯＮＴＥＮＴ＿ＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲを認知すれば、ヘッダを参照して当該コンテンツ部分のＣＯＮＴＥＮＴ＿ＩＤ　７０３が分かり、また、ＣＯＮＴＥＮＴ＿ＩＤ　７０３をマッピング情報として必要なライセンス７２０を探しうる。

【００４５】

ＣＯＮＴＥＮＴ＿ＳＴＡＲＴ＿ＰＯＩＮＴＥＲ　７０５及びＣＯＮＴＥＮＴ＿ＥＮＤ＿ＰＯＩＮＴＥＲ　７０６は、それぞれコンテンツ部分の開始位置及び終了位置を表す。この情報を分析すれば、いちいちトランスポートパケットを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がいくつのコンテンツ部分から構成されているかが分かり、各コンテンツ部分に対して獲得したライセンスを正確に適用できる。具現例によって、ＣＯＮＴＥＮＴ＿ＳＴＡＲＴ＿ＰＯＩＮＴＥＲ　７０５及びＣＯＮＴＥＮＴ＿ＥＮＤ＿ＰＯＩＮＴＥＲ　７０６のうちいずれか一つは省略してもよい。

【００４６】

ライセンス７２０には、コンテンツＩＤ　７２１、コンテンツキー７２２及び使用規則７２３が含まれる。コンテンツＩＤ　７２１は、コンテンツ部分のそれぞれに対して必要なライセンスをマッピングさせるためのマッピング情報である。例えば、図７において最初のコンテンツ部分を使用しようとするデバイスは、コンテンツＩＤ　７０３を知っていれば、同じコンテンツＩＤを有するライセンス７２０を検索して探しうる。すなわち、ＣＯＮＴＥＮＴ＿ＩＤ　７０３とコンテンツＩＤ　７２１とは同じ情報である。

【００４７】

コンテンツキー７２２は、当該コンテンツ部分の暗号化に使用した暗号化キーである。使用規則７２３は、インポートされる前のコンテンツファイルに含まれた使用制限情報に基づいて生成されたものであって、図４で既に説明したので、ここではそれについての詳細な説明は省略する。

【００４８】

図８は、本発明の一実施形態に係るコンテンツインポート装置の構造を示す図である。図８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８００は、受信部８０１、検出部８０２、使用規則決定部８０３、暗号化部８０４、ライセンス発給部８０５、ヘッダ生成部８０６、ファイル生成部８０７、保存部８０８及び送受信部８０９を備える。

【００４９】

受信部８０１は、ドメインの外部の多様な伝送チャンネルを通じて伝送ストリームを受信し、検出部８０２は、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。

【００５０】

使用規則決定部８０３は、検出部８０２で検出した使用制限情報に基づいてインポートされた後の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。

【００５１】

暗号化部８０４は、検出部８０２により検出されたコンテンツファイル、すなわち、未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、暗号化部８０４は、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であれば、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であれば、ドメインキーを利用して暗号化する。

【００５２】

ライセンス発給部８０５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備える。

【００５３】

ヘッダ生成部８０６は、インポートされたコンテンツファイルのヘッダを生成するが、

このヘッダには、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できるようにする情報が含まれる。また、図７に示すように、ヘッダには、各コンテンツ部分についてのライセンスも含まれることが望ましい。

【００５４】

ファイル生成部８０７は、暗号化されたコンテンツ部分にヘッダを付加してコンテンツファイルを生成する。このときに生成されたコンテンツファイルは、インポートされた後のコンテンツファイルである。保存部８０８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８０９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インポートされたコンテンツファイルを伝送する。

【００５５】

図９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を使用する過程を示すフローチャートである。

【００５６】

ステップ９１０で、インポートされたコンテンツファイルに含まれた保護情報からマッピング情報を解析する。このマッピング情報は、図７でのＣＯＮＴＥＮＴ＿ＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　７０４になりうる。

【００５７】

ステップ９２０では、マッピング情報を利用してコンテンツ部分の識別情報を解析する。コンテンツ部分の識別情報は、図７でのＣＯＮＴＥＮＴ＿ＩＤ　７０３になりうる。

【００５８】

ステップ９３０では、識別情報を利用してライセンスを解析する。詳細に説明すれば、識別情報に対応するライセンスを選択し、ライセンスに含まれた使用規則によってユーザの使用要請を処理する。すなわち、ユーザの使用要請が使用規則に符合する場合にのみコンテンツキーを解析する。

【００５９】

ステップ９４０では、保護情報及びライセンスを利用してコンテンツ部分についての復号化を行う。

【００６０】

図１０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を使用する装置の構造を示す図である。図１０に示すように、インポートされたコンテンツファイルを使用する装置１０００は、保存部１００１、マッピング情報解析部１００２、識別情報解析部１００３、ライセンス解析部１００４及び復号化部１００５を備える。

【００６１】

保存部１００１は、インポートされたファイルを保存し、マッピング情報解析部１００２は、インポートされたファイルのコンテンツ部分の間に周期的に含まれた保護情報からコンテンツ部分のマッピング情報を解析する。このマッピング情報は、図７でのＣＯＮＴＥＮＴ＿ＩＤ＿ＳＥＱＵＥＮＣＥ＿ＮＵＭＢＥＲ　７０４になりうる。

【００６２】

識別情報解析部１００３は、マッピング情報に該当する識別情報を解析する。識別情報は、図７でのＣＯＮＴＥＮＴ＿ＩＤ　７０３になりうる。

【００６３】

ライセンス解析部１００４は、識別情報を利用して当該コンテンツ部分のライセンスを解析する。すなわち、識別情報に対応するライセンスを選択し、ライセンスに含まれた使用規則を参照して、ユーザのコンテンツ使用要請を処理する。したがって、図示していないが、ライセンス解析部１００４は、識別情報に該当するライセンスを選択する手段、ユーザの要請をライセンスの使用規則と比較する手段、比較結果によってライセンスのコンテンツキーを解析する手段を備えることが望ましい。

【００６４】

復号化部１００５は、保護情報及びライセンスを利用してコンテンツ部分を復号化する。

【００６５】

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。

【００６６】

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、ハードディスク等）、光学的判読媒体（例えば、ＣＤ－ＲＯＭ、ＤＶＤなど）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。

【００６７】

以上、本発明についてその望ましい実施形態を中心に説明した。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を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全ての相違点は、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】

【００６８】

【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】本発明が適用されるデジタルコンテンツの保護環境を示す図である。

【図３】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４】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５】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６】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７】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ヘッダ構造を示す図である。

【図８】本発明の一実施形態に係るコンテンツインポート装置の構造を示す図である。

【図９】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を使用する過程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インポート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。

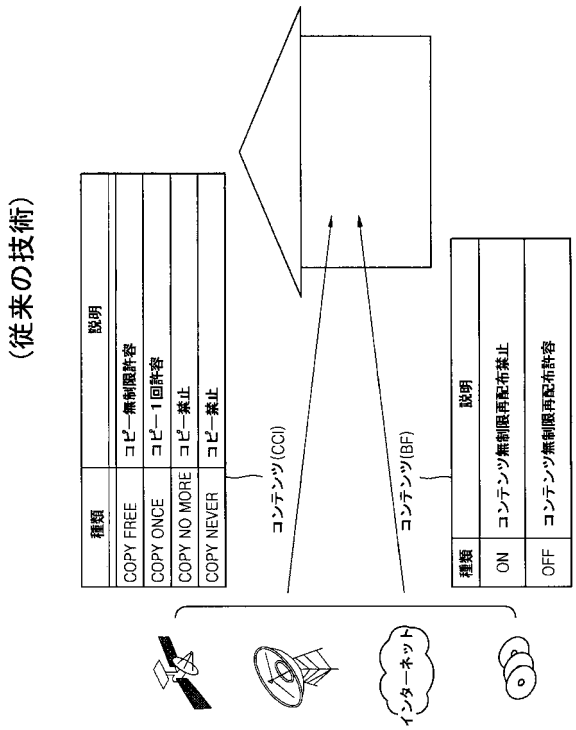
【符号の説明】

【００６９】

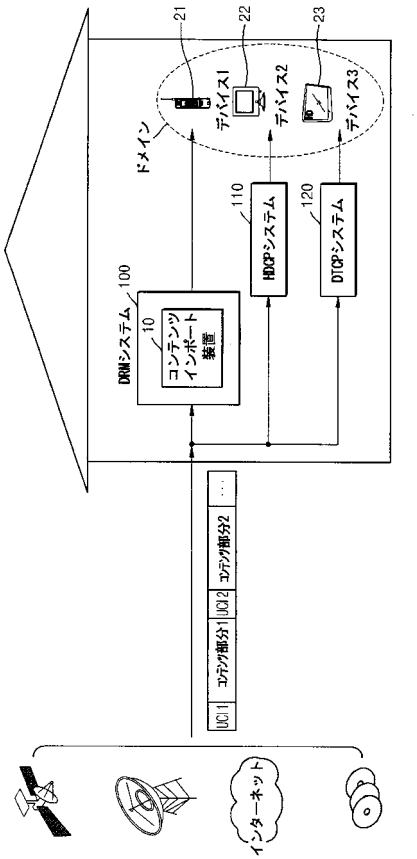
１０、８００　コンテンツインポート装置
２１、２２、２３　デバイス
４１　使用制限情報フィールド
４２　インポートフィールド
４３　使用範囲フィールド
４４　使用規則フィールド
１００　ＤＲＭシステム
１１０　ＨＤＣＰシステム
１２０　ＤＴＣＰシステム
８０１　受信部
８０２　検出部

８０３　使用規則決定部
８０４　暗号化部
８０５　ライセンス発給部
８０６　ヘッダ生成部
８０７　ファイル生成部
８０８　保存部
８０９　送受信部
１００１　保存部
１００２　マッピング情報解析部
１００３　識別情報解析部
１００４　ライセンス解析部
１００５　復号化部

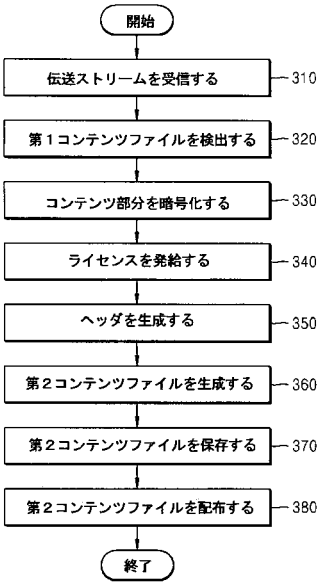
【図１】



【図２】



【図３】

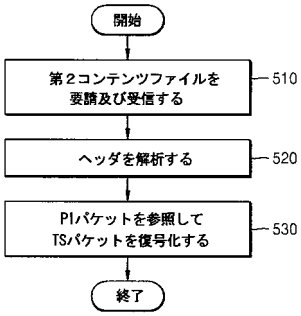


【図４】

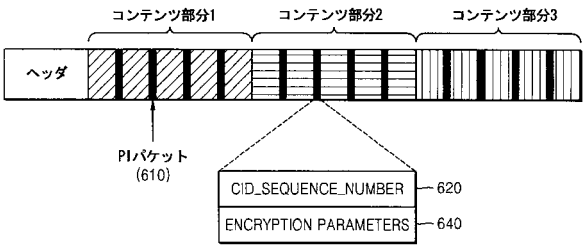
	UCI	Import	Bind Type	Usage Rule
CCI	COPY FREE	O	Device, Domain	All
	COPY ONCE	O	Device	M,S,P
	COPY NO MORE	N/A	–	–
	COPY NEVER	X	–	–
BF	ON	O	Device, Domain	All
	OFF	X	–	–

41 42 43 44

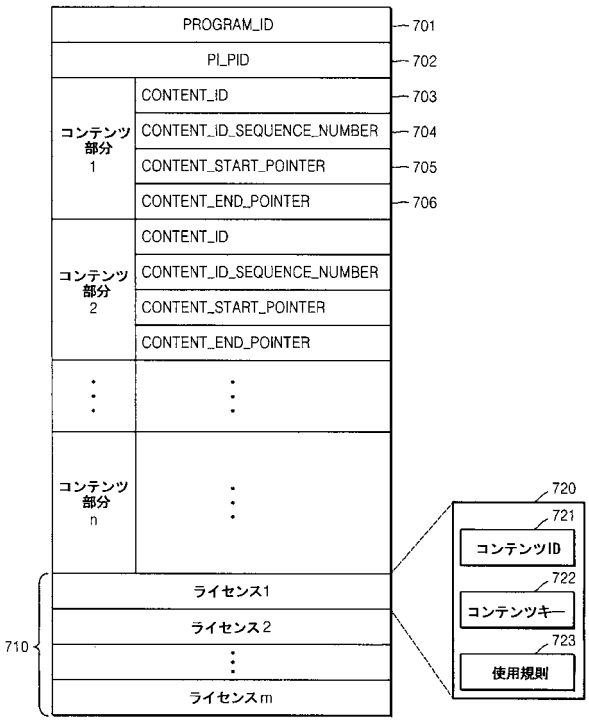
【図５】



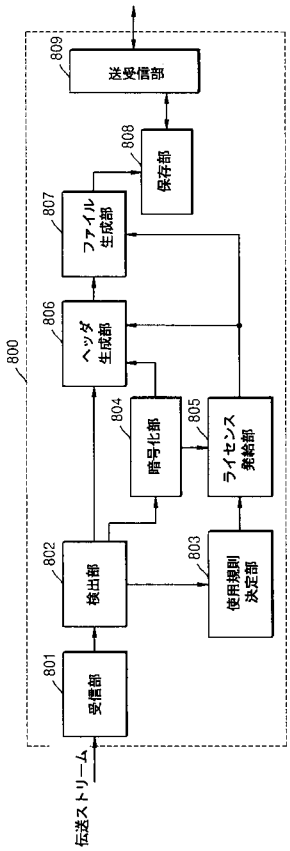
【図６】



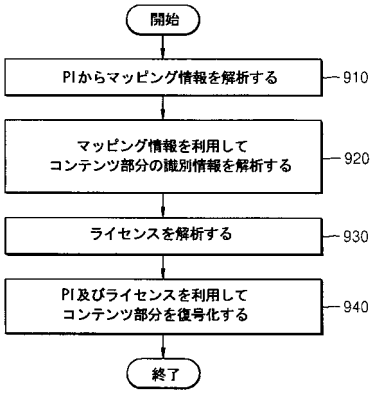
【図７】



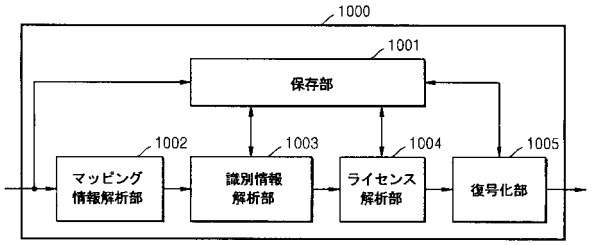
【図８】


800
809
送受信部
808
保存部
807
ファイル生成部
806
ヘッダ生成部
804
暗号化部
805
ライセンス発給部
802
検出部
803
使用規則決定部
801
受信部
伝送ストリーム

【図９】


開始
PIからマッピング情報を解析する
910
マッピング情報を利用して
コンテンツ部分の識別情報を解析する
920
ライセンスを解析する
930
PI及びライセンスを利用して
コンテンツ部分を復号化する
940
終了

【図１０】


1000
1001
保存部
1002
マッピング
情報解析部
1003
識別情報
解析部
1004
ライセンス
解析部
1005
復号化部

フロントページの続き

(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）
(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）

審査官　戸島　弘詩

(56)参考文献　特開２００３－０２２６０８（ＪＰ，Ａ）
国際公開第２００６／０３５７７７（WO，Ａ１）
特開２００３－３３１５０９（ＪＰ，Ａ）
特開２０００－３５０１８１（ＪＰ，Ａ）
国際公開第２００５／０１３６１６（WO，Ａ１）
特表２００７－５０１５６２（ＪＰ，Ａ）
国際公開第２００５／０３８６８１（WO，Ａ１）
特開平０９－２４５４３８（ＪＰ，Ａ）
特開平０９－１６０８９９（ＪＰ，Ａ）
特開２００１－２２９２８１（ＪＰ，Ａ）
特開２００１－１９７４１７（ＪＰ，Ａ）
特開平０８－２６３４４１（ＪＰ，Ａ）
特開２００４－１５８９３６（ＪＰ，Ａ）
特開２００５－２４４９４６（ＪＰ，Ａ）
特表２００５－５２５０１０（ＪＰ，Ａ）
米国特許出願公開第２００５／０２０４０３７（ＵＳ，Ａ１）
米国特許出願公開第２００７／０１６２４００（ＵＳ，Ａ１）
韓国公開特許第１０－２００３－０００６８１７（ＫＲ，Ａ）
特許第４６４２０２３（ＪＰ，Ｂ２）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／１０，２１／６０－２１／８８
Ｇ０９Ｃ１／００－５／００
Ｈ０４Ｋ１／００
Ｈ０４Ｌ９／００
Ｇ１１Ｂ２０／１０
Ｈ０４Ｎ５／９１，７／１０，７／１４－７／１７３，７／２０－７／２２