

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5259115号
(P5259115)

(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
GO 6 F 21/10 (2013.01) GO 6 F 21/22 1 1 O K
GO 6 F 21/62 (2013.01) GO 6 F 21/24 1 6 3 G
GO 6 F 21/24 1 6 6 A

請求項の数 4 (全 15 頁)

(21) 出願番号	特願2007-108360 (P2007-108360)	(73) 特許権者	390019839
(22) 出願日	平成19年4月17日 (2007.4.17)		三星電子株式会社
(62) 分割の表示	特願2007-35314 (P2007-35314) の分割		S a m s u n g E l e c t r o n i c s C o . , L t d .
原出願日	平成19年2月15日 (2007.2.15)		大韓民国京畿道水原市靈通区三星路129
(65) 公開番号	特開2007-220139 (P2007-220139A)		129, S a m s u n g - r o , Y e o n g t o n g - g u , S u w o n - s i , G y e o n g g i - d o , R e p u b l i c o f K o r e a
(43) 公開日	平成19年8月30日 (2007.8.30)	(74) 代理人	100107766
審査請求日	平成22年2月12日 (2010.2.12)		弁理士 伊東 忠重
(31) 優先権主張番号	60/773,341	(74) 代理人	100070150
(32) 優先日	平成18年2月15日 (2006.2.15)		弁理士 伊東 忠彦
(33) 優先権主張国	米国 (US)	(74) 代理人	100091214
(31) 優先権主張番号	10-2006-0036825		弁理士 大貫 進介
(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			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ファイルを記録した記録媒体

(57) 【特許請求の範囲】

【請求項 1】

コンテンツファイルを記録した記録媒体であって、
複数のコンテンツ部分と、
前記コンテンツ部分に対するライセンスと、
前記コンテンツ部分についての管理情報を有し、
前記複数のコンテンツ部分は、
前記コンテンツ部分内に周期的に挿入されているプロテクションインフォメーションを
含み、

前記プロテクションインフォメーションは、前記コンテンツ部分のマッピング情報及び
前記コンテンツ部分の復号化に必要な暗号化パラメータを含み、

前記コンテンツ部分の管理情報は、前記コンテンツファイル内で前記コンテンツ部分と
区別されるヘッダ部分に含まれ、前記コンテンツ部分のマッピング情報、前記コンテンツ
部分の ID 及び前記コンテンツ部分の位置情報を含み、

前記ライセンスは、前記コンテンツ部分の ID、前記コンテンツ部分のコンテンツキー
及び前記コンテンツ部分についての使用規則を含むことを特徴とするコンテンツファイルを
記録した記録媒体。

【請求項 2】

前記コンテンツファイルは、前記ヘッダに前記プロテクションインフォメーションを含
むパケットの識別情報をさらに含むことを特徴とする請求項 1 に記載の記録媒体。

10

20

【請求項 3】

前記コンテンツ部分は、MPEG-2 TSの形態に保存されることを特徴とする請求項 1 に記載の記録媒体。

【請求項 4】

前記コンテンツ部分のマッピング情報は、前記コンテンツ部分のコンテンツIDが簡略化された情報であることを特徴とする請求項 1 に記載の記録媒体。

【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、著作権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

10

20

30

40

50

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、いくつか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ことでその目的がある。

【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

10

20

30

40

50

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 packets 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。

10

【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。

20

【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。

30

【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(インスティテュートオブエレクトロニカルズ)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る。

40

【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

50

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、D R Mシステム 1 0 0 の規則に従わないコンテンツファイルを、D R Mシステム 1 0 0 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。

10

【 0 0 2 1 】

本発明に係るコンテンツインポート装置 1 0 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。

【 0 0 2 2 】

20

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。

【 0 0 2 3 】

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 (3 1 0)、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 (3 2 0)。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。

【 0 0 2 4 】

30

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 (3 3 0)、暗号化のために、A E S - 1 2 8 - C B C や A E S - 1 2 8 - C T R 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、A E S - 1 2 8 - C B C 方式ではイニシャルベクトル、A E S - 1 2 8 - C T R 方式では S A L T 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 M P E G - 2 規格に従うトランスポートパケット (T S P a c k e t) 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 P I (プロテクション インフォメーション) と称すことにする。P I を含むトランスポートパケットである P I 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。

40

【 0 0 2 5 】

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 (3 4 0)。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

50

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。

【 0 0 2 6 】

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、当該コンテンツ部分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。

10

【 0 0 2 7 】

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 (3 5 0)、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。

【 0 0 2 8 】

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 (3 6 0)、ストレージに保存する (3 7 0)。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 (3 8 0)。

20

【 0 0 2 9 】

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 4 1、インポートフィールド 4 2、使用範囲フィールド 4 3 及び使用規則フィールド 4 4 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。

【 0 0 3 0 】

30

使用制限情報フィールド 4 1 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 4 2 には、使用制限情報フィールド 4 1 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 4 3 には、使用制限情報フィールド 4 1 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 4 4 には、使用範囲フィールド 4 3 に記録された使用範囲別に、使用制限情報フィールド 4 1 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。

【 0 0 3 1 】

特に、使用規則フィールド 4 4 に記録された値のうち“オール (a l l)”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 4 4 に記録された値のうち“M”は、コンテンツ部分の移動 (M o v e) 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 4 4 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 (S t r e a m i n g) 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 4 4 に記録された値のうち“P”は、コンテンツ部分の再生 (P l a y) 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。

40

【 0 0 3 2 】

50

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__SEQU

10

20

30

40

50

ENCE__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。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に対応す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。

10

【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る。

20

【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。

30

【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パケットを探し出さる。

40

【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、CONT

50

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。

10

20

30

40

50

【 0 0 5 2 】

ライセンス発給部 8 0 5 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。

【 0 0 5 3 】

ヘッダ生成部 8 0 6 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。

10

【 0 0 5 4 】

ファイル生成部 8 0 7 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 8 0 8 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 8 0 9 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。

【 0 0 5 5 】

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。

20

【 0 0 5 6 】

ステップ 9 1 0 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` 7 0 4 になりうる。

【 0 0 5 7 】

ステップ 9 2 0 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` 7 0 3 になりうる。

【 0 0 5 8 】

ステップ 9 3 0 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。

30

【 0 0 5 9 】

ステップ 9 4 0 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。

【 0 0 6 0 】

図 1 0 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 1 0 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 1 0 0 0 は、保存部 1 0 0 1、マッピング情報解析部 1 0 0 2、識別情報解析部 1 0 0 3、ライセンス解析部 1 0 0 4 及び復号化部 1 0 0 5 を備える。

40

【 0 0 6 1 】

保存部 1 0 0 1 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 1 0 0 2 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` 7 0 4 になりうる。

【 0 0 6 2 】

識別情報解析部 1 0 0 3 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` 7 0 3 になりうる。

【 0 0 6 3 】

50

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

10

20

30

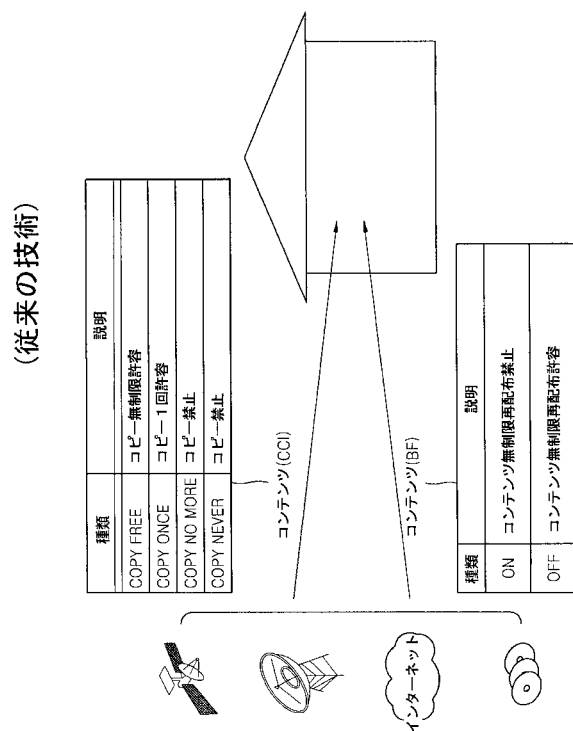
40

50

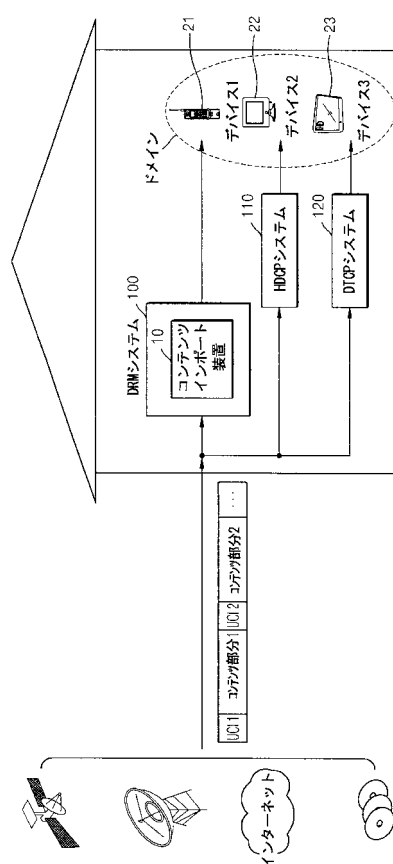
- 4 3 使用範囲フィールド
- 4 4 使用規則フィールド
- 1 0 0 D R M システム
- 1 1 0 H D C P システム
- 1 2 0 D T C P システム
- 8 0 1 受信部
- 8 0 2 検出部
- 8 0 3 使用規則決定部
- 8 0 4 暗号化部
- 8 0 5 ライセンス発給部
- 8 0 6 ヘッダ生成部
- 8 0 7 ファイル生成部
- 8 0 8 保存部
- 8 0 9 送受信部
- 1 0 0 1 保存部
- 1 0 0 2 マッピング情報解析部
- 1 0 0 3 識別情報解析部
- 1 0 0 4 ライセンス解析部
- 1 0 0 5 復号化部

10

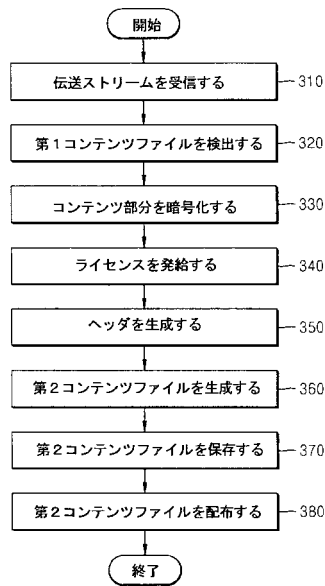
【図 1】



【図 2】



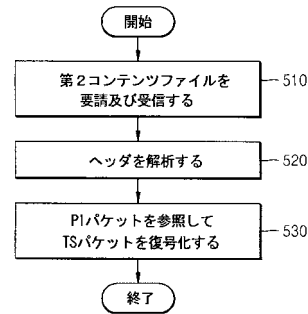
【図 3】



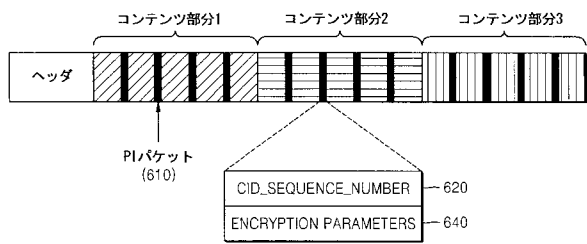
【図 4】

	41	42	43	44
	UCI	Import	Bind Type	Usage Rule
C C I	COPY FREE	O	Device, Domain	All
	COPY ONCE	O	Device	M,S,P
	COPY NO MORE	N/A	—	—
	COPY NEVER	X	—	—
B F	ON	O	Device, Domain	All
	OFF	X	—	—

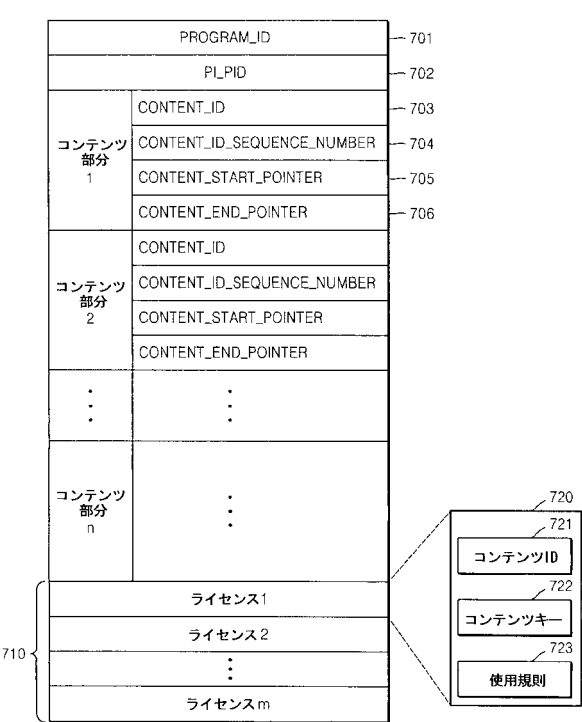
【図 5】



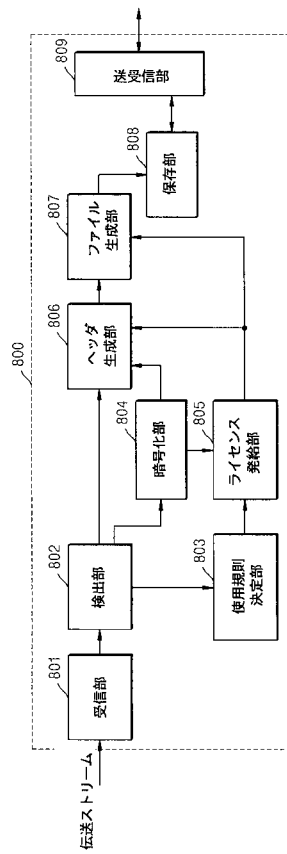
【図 6】



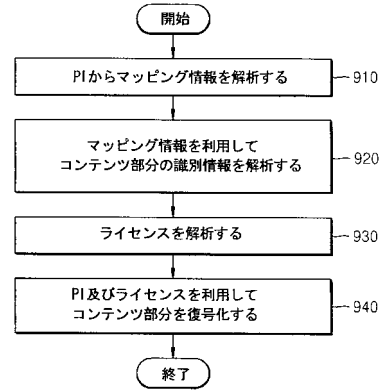
【図 7】



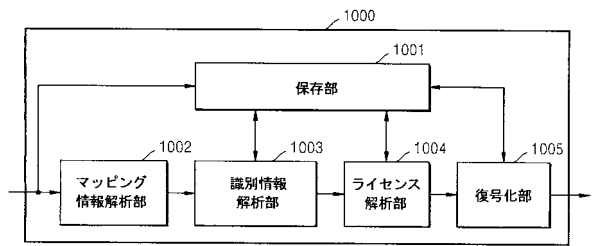
【図 8】



【図 9】



【図 10】



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)

特開2003-331509(JP,A)

特開2000-350181(JP,A)

国際公開第2005/013616(WO,A1)

特開2001-157172(JP,A)

国際公開第2006/035777(WO,A1)

米国特許出願公開第2005/0204037(US,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)

韓国公開特許第10-2003-0006817(KR,A)

特表2005-525010(JP,A)

特開平08-263441(JP,A)

特許第4642023(JP,B2)

米国特許出願公開第2007/0162400(US,A1)

特開2004-158936(JP,A)

特開2005-244946(JP,A)

(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