

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5203376号
(P5203376)

(45) 発行日 平成25年6月5日 (2013.6.5)

(24) 登録日 平成25年2月22日 (2013.2.22)

(51) Int. Cl.

F I

G O 6 F 21/10 (2013.01)
H O 4 N 7/167 (2011.01)G O 6 F 21/22 1 1 O J
H O 4 N 7/167 Z

請求項の数 6 (全 12 頁)

(21) 出願番号 特願2009-531963 (P2009-531963)
 (86) (22) 出願日 平成19年10月10日 (2007.10.10)
 (65) 公表番号 特表2010-506325 (P2010-506325A)
 (43) 公表日 平成22年2月25日 (2010.2.25)
 (86) 国際出願番号 PCT/IB2007/054120
 (87) 国際公開番号 W02008/044210
 (87) 国際公開日 平成20年4月17日 (2008.4.17)
 審査請求日 平成22年10月8日 (2010.10.8)
 (31) 優先権主張番号 06122191.7
 (32) 優先日 平成18年10月12日 (2006.10.12)
 (33) 優先権主張国 欧州特許庁 (EP)

前置審査

(73) 特許権者 590000248
 コーニンクレッカ フィリップス エレク
 トロニクス エヌ ヴィ
 オランダ国 5 6 2 1 ベーアー アイン
 ドーフェン フルーネヴァウツウェッハ
 1
 (74) 代理人 100087789
 弁理士 津軽 進
 (74) 代理人 100122769
 弁理士 笛田 秀仙
 (74) 代理人 100145654
 弁理士 矢ヶ部 喜行

最終頁に続く

(54) 【発明の名称】 ライセンスに固有な認可領域

(57) 【特許請求の範囲】

【請求項 1】

電子クライアント装置において暗号化されたコンテンツ情報を処理する方法であって、
 前記電子クライアント装置の処理ユニットが、暗号化されたコンテンツ情報を処理するス
 テップであって、前記コンテンツ情報が、領域内で配信する権利に関するライセンスを有
 し、前記ライセンスがコンテンツ鍵を含むステップ、
 前記電子クライアント装置の復号化ユニットが、前記暗号化されたコンテンツ情報を復号
 するステップであって、前記復号は、前記コンテンツ鍵並びに領域の構成及び領域の方針
 条件によって可能にされ、前記領域の構成及び領域の方針条件は、前記ライセンスの機
 能的部分であるステップ、
 を有し、前記処理ユニットによる前記処理するステップが、
 前記領域の構成及び領域の方針条件に従って、前記コンテンツ情報の配信の制御を行使す
 るステップ、
 前記ライセンスから派生した前記コンテンツ情報を配信する更なる権利を有する更なるラ
 イセンスであって、前記コンテンツ鍵とは異なる他のコンテンツ鍵を有する更なるライセ
 ンスを生成するステップ、
 前記更なるライセンスを他のクライアント装置に結び付けるステップ、
 前記他のクライアント装置によって用いられるように、前記コンテンツ情報を配信する前
 記更なる権利を有する前記更なるライセンスを提供するステップ、
 を有し、

10

20

前記コンテンツ鍵がコンテンツの高品質のレベルの復号を可能にし、前記他のコンテンツ鍵がコンテンツの低品質のレベルの復号を可能にする、
方法。

【請求項 2】

前記更なるライセンスが前記コンテンツ鍵を有する請求項 1 に記載の方法。

【請求項 3】

前記領域の方針が、機械処理可能な言語で少なくとも部分的に表現されている、請求項 1 に記載の方法。

【請求項 4】

最初に言及された前記権利から前記更なる権利が派生することを可能にするステップを含む、請求項 1 に記載の方法。

【請求項 5】

暗号化されたコンテンツ情報を処理する処理ユニットであって、前記コンテンツ情報が、領域内で配信する権利に関するライセンスを有し、前記ライセンスがコンテンツ鍵を含む処理ユニット、

前記暗号化されたコンテンツ情報を復号する復号化ユニットであって、前記復号は、前記コンテンツ鍵並びに領域の構成及び領域の方針条件によって可能にされ、前記領域の構成及び領域の方針条件は、前記ライセンスの機能的部分である復号化ユニット、
を有し、前記処理ユニットが、

前記領域の構成及び領域の方針条件に従って、前記コンテンツ情報の配信の制御を行使し、

前記ライセンスから派生した前記コンテンツ情報を配信する更なる権利を有する更なるライセンスであって、前記コンテンツ鍵とは異なる他のコンテンツ鍵を有する更なるライセンスを生成し、

前記更なるライセンスを他のクライアント装置に結び付け、

前記他のクライアント装置によって用いられるように、前記コンテンツ情報を配信する前記更なる権利を有する前記更なるライセンスを提供し、

前記コンテンツ鍵がコンテンツの高品質のレベルの復号を可能にし、前記他のコンテンツ鍵がコンテンツの低品質のレベルの復号を可能にする、

電子クライアント装置。

【請求項 6】

コンピュータによって読み込まれて実行され、請求項 1 から請求項 4 のいずれか一項に記載の方法の各ステップを前記コンピュータに実行させて、前記コンピュータを前記電子クライアント装置として機能させる、ソフトウェア。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は電子システムでコンテンツ情報のデータ処理を可能にする方法に関する。本発明は、データ処理システム、及び斯様な方法で用いられるソフトウェアに更に関する。

【背景技術】

【0002】

近年、複数の種々異なるタイプのコンテンツ保護システムが、急速なペースで増大した。これらのシステムのいくつかは、コンテンツを違法にコピーすることから保護するのみである。他のシステムは、ユーザがコンテンツにアクセスすることを禁じている。第1のカテゴリは、コピープロテクション (CP) システムと呼ばれている。CPシステムは、伝統的に家電 (CE) 製品に対してフォーカスされた。この種のコンテンツ保護は、一般に安価な態様で実行されることができ、コンテンツ・プロバイダとの双方向性の連関を必要としない。コンテンツ保護のいくつかの例は、コンテンツ・スクランブル・システム (CSS)、DVD ROM ディスクの保護システム、及び DTCP (IEEE 1394 接続のための保護システム) である。アクセスを禁止することに関する、コンテンツ保護システムの第2のカテゴリは、

複数の名前の下に公知である。テレビ放送界では、これらのシステムは、条件付きアクセス（CA）システムとして一般に知られており、インターネットでは、これらはデジタル権利管理（DRM）システムとして一般に知られている。

【 0 0 0 3 】

ホームネットワークは、（例えば、イーサネット、IEEE 1394、BlueTooth、802.11b、802.11g、等の）ネットワーク技術を使用して相互接続する一連の装置として規定されることができる。ネットワーク技術は、種々異なる装置が通信することを可能にするにもかかわらず、装置が相互運用するには十分ではない。相互運用のためには、装置は、ネットワーク内の他の装置に存在する機能を発見し、アドレスできることを必要とする。この機能は、ホームネットワークを行うミドルウェアによって供される。ホームネットワークを行うミドルウェアの例は、Jini、HAVi、UPnP、及びAVCである。

10

【発明の概要】

【発明が解決しようとする課題】

【 0 0 0 4 】

認可領域の概念は、（彼等の著作権が保護されていることを望む）コンテンツ・オーナーの利益、及び（コンテンツの無制限の使用を望む）コンテンツ消費者の利益の両方に貢献する解決策を見出すことを意図する。基本的な原理は、認可領域とも呼ばれる、制御されたネットワーク環境を持つことである。コンテンツは比較的自由に、しかし、認可された領域内でのみ使われることができる。一般に、認可領域は、家庭環境又はホームネットワークに集中している。もちろん、他のシナリオも可能である。ユーザは、例えば、装置で記憶されたオーディオ及び／又はビデオを再生するための携帯機器を、彼（女）と一緒に旅行に持っていくことができ、自宅で彼（女）の個人のオーディオ／ビデオ・システムで記憶された、追加のコンテンツにアクセスするか、又はダウンロードするために、彼（女）のホテルの部屋で当該携帯機器を使用する。当該携帯機器は地理的にはホームネットワーク外にあるにもかかわらず、機能的には、このユーザの認可された領域の一部に留まる。この態様にて、認可領域は、当該領域に帰属している装置によるコンテンツへのアクセスを可能にするシステムであるが、しかし他のいかなる装置によるアクセスもできない。

20

【 0 0 0 5 】

認可領域等の使用に対するより広範な紹介については、例えば、S.A.F.A. van den Heuvel、W. Jonker、F.L.A.J. Kamperman、P.J. Lenoirによる論文、Secure Content Management in authorized domains、フィリップス・リサーチ、オランダ、IBC 2002会議刊行、2002年9月12日～16日開催、頁474を参照されたい。

30

【 0 0 0 6 】

認可領域の概念をある程度実行する様々な提案が存在する。

【 0 0 0 7 】

既知の実施例の一つのタイプは、装置ベースの認可領域である。斯様なシステムの例は、SmartRight（Thomson Multimedia社）、xCP、及びNetdigital権利管理、NetDRM（Panasonic社）である。装置ベースの認可領域の更なる例は、例えば、ここでも参照されて組み込まれる、フィリップス・エレクトロニクス社の国際特許公開公報 WO 03/098931（出願人整理番号NL020455）で説明されており、また、米国特許公開公報US 20050210261として刊行されてもいる。

40

【 0 0 0 8 】

一般的な装置ベースの認可領域は、特定の一連の装置、及びコンテンツによって形成されている。この特定の一連の装置のみが、当該領域にあるコンテンツにアクセス、使用等することが許容されている。同じ領域内に存在する、同じ特定の一連の装置をもつ、異なるユーザ間の区別がない。

【 0 0 0 9 】

装置ベースの認可領域システムの欠点は、当該システムが、ユーザが望むか又は必要とする柔軟性を一般に供しないという点である。何故ならばユーザは、特定の限られた一連

50

の装置に対して限定されるからである。この態様では、ユーザは、いつでもどこでも、彼（女）が選択した場所、時間に、ユーザが得た権利を行使することが出来ない。例えば、ユーザが友人の家を訪問している場合、友人の装置からは、当該ユーザが合法的に購入したコンテンツに、彼（女）はアクセスをすることができない。友人の装置は、この特定のユーザのコンテンツを有する領域と一緒に形成する特定の及び限定された一連の装置には、一般的に、含まれない。

【 0 0 1 0 】

既知の実施例の別のタイプは、人ベースの認可領域である。ここでは、認可領域は、（上で説明された、装置ベースで認可された領域におけるような装置の代わりに）人及びコンテンツに基づく。斯様なシステムの例は、例えば、ここでも参照して組み込まれる、国際特許公開公報 WO 04/038568（出願人整理番号NL021063）で説明されており、また、米国特許公開公報 US 20060021065として刊行されてもいる。説明されているシステムにおいて、コンテンツは、領域にグループ分けされた人に結びつけられる。

10

【 0 0 1 1 】

一般的な人ベースの認可領域では、アクセスは、その認可領域に対して結び付けられたコンテンツに対して行われることができる。しかしながら、特定の、及び限定された一連のユーザのみが、アクセスを許される。これらのユーザは、どのような準拠した装置をも使うことができる。人ベースの認可領域での領域の管理は、装置ベースの認可領域における領域の管理より、一般に容易である。

【 0 0 1 2 】

20

しかしながら、人ベースのシステムは人の識別を必要とし、これはユーザにとって必ずしも便利ではなく、又はユーザによって好まれない。更に、認可されたユーザの自宅への訪問客は、ユーザのコンテンツにアクセスしたくなくろう。彼（女）がその領域に対する個人識別子をもたないので、彼（女）が当該コンテンツにアクセスすることは可能ではない。当該領域に属している自宅の装置は、訪問客がその領域にあるコンテンツにアクセスすることが好ましい。

【課題を解決するための手段】

【 0 0 1 3 】

これ故、複合型の認可領域に対するニーズがあり、これは装置ベースの領域同様、人ベースの領域とも共通する態様をもつ。斯様な複合型の認可領域は、両方の長所を組み合わせることを意図している。人ベース及び装置ベースの複合型の認可領域は、ここでも参照して組み込まれる国際特許公開公報 WO 05/010879（出願人整理番号NL030926）で提案されており、米国でも、出願番号10/565,663にて出願されている。この文書では、認可領域を規定するために、二つの異なるアプローチを組み合わせた認可領域が開示されている。装置ベースのアプローチと人ベースのアプローチとの間の接続部分は、いわゆる領域識別子（Domain Identifier）である。装置は、領域-装置証明書（DDC）を介して、好ましくは一緒にグループ化される；即ち、人は、領域-ユーザ証明書（DUC）を介して、好ましくは別々にグループ化され；コンテンツは、人に直接又は間接的にリンクされる。

30

【 0 0 1 4 】

しかしながら、コンテンツが、例えば、デジタル権利管理配達システム及び/又はCAシステムからこの認可領域にインポートされるとき（一般には、この動作は装置を介して実施される）、コンテンツがどの人に割り当てられなければならないかは直接明らかではない。言い換えると、システムは、コンテンツがリンクされるべき人についての追加の情報を、インポート時に必要とする。

40

【 0 0 1 5 】

これ故、コンテンツをインポートするときに必要とされる追加の情報が容易に、及び/又は直接入手できる、認可領域を作成する単純な方法に対するニーズがある。これは、ここでも参照され組み込まれる、国際特許公開公報 WO 05/093544（出願人整理番号NL040315）で提案されている認可領域によって達成される。この刊行物では、認可領域を生成する方法が、以下のステップと共に提案されている：即ち、認可領域を識別している領域識

50

別子が、独自に選択されるステップと、ユーザが、当該領域識別子に対して結び付けられるステップと、コンテンツ項目が、ユーザに対して結び付けられるステップと、装置が、ユーザに対して結び付けられるステップとである。コンテンツ項目の各々、装置の各々、及びユーザの各々を認可領域に対して結び付けられるというよりはむしろ、ユーザのみが認可領域に対して結び付けられ、コンテンツ項目及び装置は、順に、ユーザに対して結び付けられる。

【 0 0 1 6 】

上記のように、種々異なる認可領域が、システムの領域の構成及び領域の方針によって区別される。例えば、認可領域は、一つの領域識別子にリンクされた、一例では多くても10台の装置のセット（組）として規定されることができ、当該一連の装置は、無制限のセットのコンテンツに結び付けられている、一例では最大五つのユーザ・アカウントにリンクされる。装置及びユーザ・アカウントの最大数に加え、領域の方針は頻度の制限を含むことができる。当該頻度の制限は、時間単位当たりの限定された回数の構成の変更を認め、又は、特定のコンテンツ若しくは特定の場所に対する領域の機能を限定する近接制御を可能にする。

10

【 0 0 1 7 】

現行のシステムでは、明白な区別が、コンテンツの権利と、領域の構成及び領域の方針との間になされている。これは、DRMライセンスが、認可領域内にあるコンテンツの配信をアドレスする権利表現を含まないことを意味する。場合によっては、ライセンスは領域の方針を規定して、これを取り扱う（例えば、OMA DRMなどの）管理者とのリンクを含む。

20

【 0 0 1 8 】

発明者は、ここで、領域の構成及び領域の方針の記述（又は条件）が、ライセンスの機能部分であるシステムを提案する。領域の構成条件は、許容される領域の構成、即ち、可能な領域の構造を決定する。当該条件は、コンテンツ又は権利が、特定の領域内に配信されることができるとする条件を決定する。例えば、領域の構成は、後述されているライセンスの近接規則に基づいている。領域の方針は、領域の構成の内容の方針を決定する。領域のサイズに対する（数値的な）制限を効果的に提起するのは、一組の変数又は関数でもよい。例えば、ライセンスの近接規則に基づく領域の構成のために、領域の方針は、ライセンスの複製又はコンテンツのコピーが作られる前に、少なくとも五つのライセンスが近接していなければならないことを示す。

30

【 0 0 1 9 】

本発明を理解するために、領域の方針及び領域の構成条件をライセンスに入れないことから起こる以下の問題を考慮する。

【 0 0 2 0 】

第1の問題は、いくつかのシステムでは、認可領域の方針が特定の技術に組み込まれているという点である。これは、認可領域に対して、単一の構成が全システムに対して規定されていることを意味する。問題は、しばしば、これが消費者に単一の、一体化された経験を供する点である。しかしながら、領域の構成は、コンテンツのオーナー及びコンテンツの配信者のビジネス・モデルに直接関係していることが判明する。異なるタイプのコンテンツは、異なる領域の構成及び領域の方針を必要とする。更に、種々異なる領域の構成及び領域の方針は、消費者を引きつけるための競争の手段である。関係するすべての当事者に合うビジネス・モデルを見つけることに関するもので、これらの方針の標準化は、これ故、極めて困難である。これらの困難さはDRMシステムの標準化を非常に妨げ、これによって、DRMシステムの良好な市場導入を妨げる。

40

【 0 0 2 1 】

第2の問題は、いくつかのシステムでは、サービス・プロバイダが領域の管理及び（方針の）行使を行う点である。これは、顧客とコンテンツ・プロバイダとの間に、長期の依存関係を確立する。これらの場合、特定の（インターネット）サービスへのリンク（URL）が、ライセンスに組み込まれている。コンテンツを販売する当事者は、このサービスを

50

一般的に運営する。このサービスは、大きな一連の領域を維持し、伴われた方針を行使する。このサービス・アプローチは、全システムに対して単一の領域の方針をもつという問題を迂回する。しかしながら、このアプローチは、顧客とサービス・プロバイダとの間に長期の依存をもたらす。これも、いくつかの欠点につながる。第1の欠点は、顧客のコンテンツを配信するため、そして長期的には、顧客のコンテンツをレンダリングするために、顧客がサービス・プロバイダの継続した存在に依存する点である。第2の欠点は、サービス・プロバイダが、コンテンツの使用（配信）の過程で、いくつかの知見を得ることができる点である。消費者の観点からは、これはプライバシーの侵害と考え得る。第3の欠点として、コンテンツの配信者が領域管理のインフラストラクチャを構築しなければならない点、当該インフラストラクチャが十分に長い期間存在することを保証しなければならない点、コンテンツの配信者にとって負担となる。この種の領域管理は、単にコンテンツを販売したいだけのコンテンツの配信者にとっては、あまり興味がない。

10

【 0 0 2 2 】

これ故、発明者は、コンテンツ（認可領域）の配信の行使は、コンテンツの権利（再生、コピー、描画、印刷等）が行使されるのと類似の態様にて行われることを提案する。コンテンツ・プロバイダは、配信する権利（領域の構成条件及び領域の方針条件）を規定し、これらの条件と共にコンテンツを販売する。ある意味では、コンテンツは、コンテンツの権利と配信する権利との組合せで購入される。消費者側のDRMのクライアントは、コンテンツの権利及び配信する権利を行使する。

【 0 0 2 3 】

20

したがって、本発明は、例えばユーザが、ユーザの、例えばCE機器、ホームネットワーク、又は電子装置、又は別のDRMクライアントなどのデータ処理システムでコンテンツ情報をデータ処理することを可能にする方法に関し、コンテンツ情報は、領域内に配信する権利があるライセンスを有する。データ処理を可能にするステップは、例えばユーザが起動したシステム制御を通じて、ライセンスの機能部分である、領域の構成及び領域の方針条件に従った（及び、ライセンスの場合は、通信又は配信も、このように、ライセンスの機能部分として配信される）システムを介し、コンテンツ情報の配信を行うステップを含む。好ましくは、システム制御を行うステップは、ライセンスにコンテンツ情報を配信する権利を供するステップを含み、当該権利は、システムによって行使可能である。実施例では、データ処理を可能にするステップは、システムを通じコンテンツ情報への条件付きのアクセスを、システム制御を介して行うステップを更に含む。例えば、コンテンツ情報は暗号化され、制御を行うステップは、暗号化されたコンテンツ情報を解読するための鍵を、ライセンスと共に供するステップを含む。他の実施例では、領域の構成条件及び領域の方針条件が、配信する権利を記述している専用の機械でデータ処理可能な言語で、少なくとも部分的に表現されている。他の実施例では、前述のライセンスを供するステップは、更なるライセンスにコンテンツ情報を配信する、システムによって行使可能な更なる権利を供することを可能にするステップを含む。好ましくは、当該更なる権利は、最初に言及した権利から派生する。

30

【 0 0 2 4 】

本発明は、コンテンツ情報をデータ処理するためのデータ処理システムにも関し、添付の請求項で更に特定された斯様なシステム上にインストールするためのソフトウェアに関する。

40

【 0 0 2 5 】

本発明は、添付の図面を参照し、例の態様にて更に詳細に説明される。

【図面の簡単な説明】

【 0 0 2 6 】

【図 1】本発明のDRMシステムを例示している機能線図を示す。

【図 2】本発明のDRMシステムのクライアントがもつライセンスから、別のDRMのクライアントがもつ派生ライセンスを導き出す過程を例示している機能線図を示す。

【図 3】本発明のDRMのクライアントを例示しているブロック図を示す。

50

【 0 0 2 7 】

図全体にわたって、同一の参照番号は、類似か、又は対応する特徴を示す。

【 発明を実施するための形態 】

【 0 0 2 8 】

上記のように、本発明は、幾つかある特徴のなかで特に、ユーザがコンテンツ情報をデータ処理することができるようなサービスを提供することを意図する。当該サービスは、ユーザによるコンテンツ情報への条件付きのアクセスの制御、及びユーザによるコンテンツ情報の配信の制御の両方を好ましくは組み合わせた制御を、実行する。

【 0 0 2 9 】

コンテンツ・プロバイダが配信する権利を規定することを可能にするために、新規の、又は拡張された権利表現言語（REL）が、必要とされる。このRELは、配信する権利を記述するために、構文及びソフトウェアの動作を含む。斯様な配信する権利の例は、以下の要素を含む：

- 装置の数の計数：ライセンスの複製がどれくらい多くの異なる数の装置上に存在するかを指し示す。

- 装置の計数方法：どのように装置の計数が管理されるべきか、又は減じられるべきかの方法を示す。例としては、

- マスター：一つのライセンスからのみ、複製が作られることができる。当該ライセンスは、ムーブ（移動）ができない。

- 可動マスター：一つのマスターライセンスからのみ、複製が作られることができる。これまでに作られたライセンスの複製を無効にせずに、このライセンスは、更に移動することができる。

- 最初：ライセンスの最初の事例が、マスターから、又は別の複製から作られた複製の数を追跡する。

- 分割：装置の計数が二つ（又はより多く）の計数に分割され、この結果、当該二つ（又はより多く）の計数の合計が装置の計数に等しい。例えば、装置の計数5は、一つのライセンスに対して装置の計数3、及び他のライセンスに対して装置の計数2に分割されることができる。

- 減算：複製が作られる場合（及び、複製が作られる前に）、装置の計数は（数値が正である場合）、1だけ減じられる。装置の計数がゼロである場合、更なる複製は作ることができない。これは、多くても2の（装置のカウント数）のべき乗個の複製が作られ得ることを意味する。

- 複製の近接：ライセンスの交換を望む2台の装置は、お互いに空間的に近接していなければならないことを示す。

- ライセンスの近接：コンテンツの再生は、特定の数のライセンスが近接している時にのみ可能であることを示す。このように、「近接」する装置への近接度が測定される。一定数のこれら近接する装置がコンテンツ部分に対する有効なライセンスをもっているとき、ライセンスは「本物」と評価し、そして当該コンテンツは再生されることができる。このことは、コンテンツが、互いに近接する装置のグループ内（例えば、1軒の家の中にある装置）で使用されることを強制する。旅行の間に使用される（そして、他の装置に接続されていない）携帯機器は、斯様なコンテンツを再生することを許可されないであろう。

- ムーブの許可：1台の装置から別の装置へと、ライセンスがムーブすることができることを示している。

- 含有：領域の制約を有する別のライセンスを参照すること。基準となるライセンス及び手元にあるライセンスの両方が満たされる場合、複製を作ることが許可される。「含有された」ライセンスに含まれる規則に付随する状態は、無視される。例えば、「含有された」ライセンスが、複製は10台の装置に許可されると告知すると、このライセンスは「親」ライセンスを含んだ他のライセンスにかかわりなく、10台の装置へ複製されることができる。子ライセンスは親ライセンスから継承されるので、子ライセンスは如何なる配信する権利も必要としないであろう。

10

20

30

40

50

- 拡張：領域の制約を有する別のライセンスを参照すること。基準となるライセンス及び手元にあるライセンスの両方が満たされる場合、複製を作ることが許可される。「拡張」ライセンスに含まれる規則に付随する状態が、考慮される。例えば、「拡張」ライセンスが、複製は10台の装置に許容されると告知すると、次に、「拡張」ライセンスを参照しているすべてのライセンスが（例えば、多くても10台の）一連の同一の装置を通じて配信されなければならない。このメカニズムは、限られた一連の装置上にあるコンテンツの結び付けを可能にする。
- 複製の認証：複製が新規の装置に作られることができる前に、ユーザ認証が行われなければならない。
- 再生認証：コンテンツが再生されることができるよう前に、ユーザ認証が行われなければならない。
- 認証のタイムアウト：装置が、このライセンスに対する特定のユーザを認証する時間を限定する。
- 複製の頻度：どれくらい多くの複製が時間単位当たりで作成されることができるようについて規定する。
- ムーブの頻度：ライセンスが、時間単位当たり何回移動することができるようについて規定する。
- 子の権利：ライセンスの複製を取得せねばならない（配信及び使用の）権利一式を記述する。この権利の使用例は、タイムアウトを複製上に設定するか、又は複製を現行のライセンスに含めるか、若しくは延在させることである。
- コピー品質の劣化：コピーされたコンテンツは、減じられた音質レベルで再生されることができるようのみである。これは、アナログのコピーの性質を模倣している。次の（孫）コピーは許可されてもよいし、又は許可されなくてもよいが、許可される場合でも、更なる劣化を示すだろう。

【0030】

上で説明された権利の例は、多くの異なる領域の方針をすでに考慮に入れている。これらの方針の記述は、従来の方針及び従来の構成とはいくらか異なる。これは、より旧来の領域の構成及び領域の方針が、システムの全体的な概観と共に記述されているのに対して、ライセンス毎の領域の方針が、ライセンスの観点から記述されているという事実の結果である。

【0031】

また、配信する権利の表現のための専用言語が、XML又は別の適切なマークアップ言語を使用して実行することができる点に留意する。

【0032】

明確な配信する権利をもつDRMシステムの一般的な構造は、既存のDRMシステムと類似している。主要な違いは、DRMのクライアントによって行われる部分においてである。これらのクライアントは、本発明では、配信する権利を行使する追加の機能一式を持つ。これらの配信する権利は、ライセンスに含まれている従来の権利一式に加えられる。これを図1に示す。

【0033】

図1は、本発明のDRMシステム100のさまざまな概念を例示している線図である。システム100は、特定のクライアント108に対してライセンス104を発行するサービス・プロバイダ102を有する。サービス・プロバイダ102は、特定のクライアントの装置108に、暗号化されたコンテンツ情報106も供給する。ライセンス104は、クライアント108がコンテンツ情報106を解読し、再生することを可能にする、コンテンツ鍵110を含む。ライセンス104は、クライアント108に供されたコンテンツ106の使用領域を特定している、明確な配信する権利112も有する。クライアント108は、システム100の使用時に、配信する権利112を行使する。クライアントの装置108は、システムの殆どの方針決定を、局所的に扱うことができる。しかしながら、いくつかの方針決定は、装置108、及びライセンス104が複製される全ての他の装置114、116、、、118の協力を要する、状態管理の形態を必要とする。こ

れが、（上記で「装置のカウント」の個所で説明されたように）ライセンス（又は拡張ライセンス）の複製の使用を可能にした計数装置をもつ一般的な事例である。さらにまた、いくつかの方針決定は、近接条件の下で、装置の連関を必要とする。

【0034】

全体の（即ち、複数の装置が関与する）状態管理が必要なときには、装置108、114、116、及び118の中の特定の1台が、当該状態の所有者として選ばれる。これは、サービス・プロバイダ102からライセンス104の最初の事例を受信した装置108であり得る。ライセンス104の複製においては、状態の所有者、この事例では装置108が、明確に言及される。DRMのクライアント、例えば、全体の状態にアクセスすることが必要な装置114-118は、指定された、状態の所有者、即ち装置108と連絡をとることが必要とされる。代替的なアプローチは、装置108及び装置114-118に存在しているライセンス104の種々異なる複製の状態を同期させようと試みるプロトコル（例えば、ピア・ツー・ピア）を加えることである。10
斯様なプロトコルは、ベストエフォート（最善努力式）ベースで良く機能する。これは、異なるDRMのクライアント108、114-118の間で、状態が一時的に矛盾していてもよいが、しかし、これは、領域の方針によっては受け入れられてもよいことを意味する。オプションとしては、両方の技法（状態の所有者及び同期プロトコル）をDRMのクライアント108、及び114-118に埋め込んで、配信する権利の言語に方針選択オプションを加えることである。

【0035】

DRMのクライアント108、114-118が状態を管理する代わりに、当該状態はオンラインサービス、例えば、サービス・プロバイダ102又は別の信頼のおける当事者によって、代替的に管理されることができる。これは技術的な観点からは、より簡単な解決策であるが、しかし、これも外部のサービスへの依存を誘発する。しかしながら、このアプローチは、異なる領域の方針が単一のシステムの中で共存することを依然として可能にする。さらに、サービスが機能しなくなると、異なるサービスが義務を引き継ぐことができる。斯様な場合には、ライセンスは、新規のサービスが領域を設定するために必要なすべての方針の10
情報を含む。

【0036】

確実にライセンスの配信を制御するために、好適な態様は、個々のライセンスの各々を特定のDRMのクライアントに結びつけることである。これは、ライセンスが暗号化され、10
ライセンスが意図するDRMのクライアントによって解読されることのみができることを意味する。これは、すでにライセンス領域の一部である一連の装置には見えない未知の場所へ、ライセンスが複製されることを防止する。これはまた、ライセンスが異なる場所で複数回挿入されることを防止する。代替のアプローチは、ライセンスを暗号化するのではなく、ライセンスが配信される安全な経路を確立することである。当該経路は信頼のあるDRMのクライアント間にのみ確立されるので、これによって、未知の装置に対する権利の配信を防止する。

【0037】

ライセンスが複製されると、複製の出所であるDRMのクライアントは、調節（変更）された権利をもつ新規のライセンスを作成し、この新規のライセンスを、複製が作られた他のDRMのクライアントに結び付ける。これは、DRMのクライアントがライセンスの複製を生成することができ、そして、変更することができることを意味する。代替のアプローチは、オリジナルのライセンスを送り、別のデータ構造内で、当該ライセンスの状態を示すことである。いずれの場合においても、DRMのクライアントは、彼自身がライセンスの発行人になる。これは、従来のDRMのクライアントの役目では、通常、無いようなものである。40

【0038】

図2は、DRMのクライアント202が持つライセンス206から、派生したライセンス204を作成している、DRMのクライアント202を示す。派生ライセンス204は、別のDRMのクライアント208によって使われ、当初のライセンス206で指定された権利212によって調整（変更）50

され、当該権利に基づいた派生権利210を含む。この例では、ライセンス206及び派生ライセンス204は、クライアント202及び208がコンテンツ216にアクセスするために、両方とも同じ暗号鍵214を含んでいる。代替のシナリオでは、派生ライセンス204は、ライセンス206に含まれるものとは異なる代わりの別の鍵（図示せず）を含んでもよい。例えば、派生ライセンス204は、コンテンツ216の低品質のレベルのみを解読する鍵を含むが、ライセンス206に含まれる鍵は、当該コンテンツ216の高品質のレベルの解読を可能にする。

【0039】

代替のシナリオ、例えば、Coralアーキテクチャ（<http://www.coral-interop.org>を参照）に基づいたシナリオでは、DRMのクライアント202は、権利斡旋サービス（図示せず）と置き換えられることができる。このサービスの目的は、ライセンス発行人によって発行された一連の権利から派生したライセンスを、（例えば、ライセンスと考えられることができる、権利トークンの形態で）発行することである。派生ライセンスは、第1のライセンスが発行されたDRMシステムとは異なってもよいDRMシステムでのライセンスである。この派生は、方針に非常に左右される。方針を当初のライセンスに置くことによって、完全なシステムに向けて標準化される必要はない。

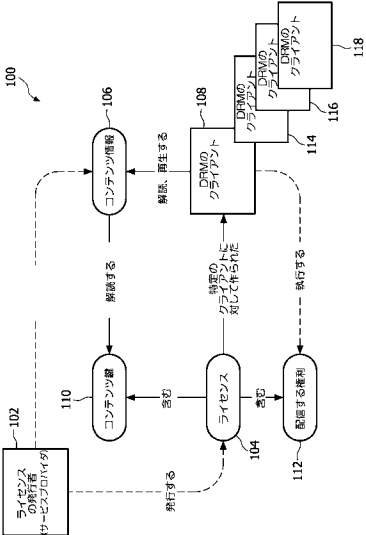
【0040】

図3は、本発明で言うところの機能を例示している、DRMのクライアント300のブロック図である。クライアント300は、上記のように、ライセンス302が関係するコンテンツ情報の使用領域を指示している特定の権利304を有するライセンス302を受信した。当該権利はクライアント300に、クライアント300を介したコンテンツ情報の配信のコントロールを可能にする制御コードとして、例えばメモリ306内にインストールされる。この目的のために、インタフェース310を介したネットワーク（図1及び図2には更に示されていない）上での他のクライアントとの連関において、クライアント300は、制御コードで表現されたこれらの権利304を行使するコントローラ308をもつ。

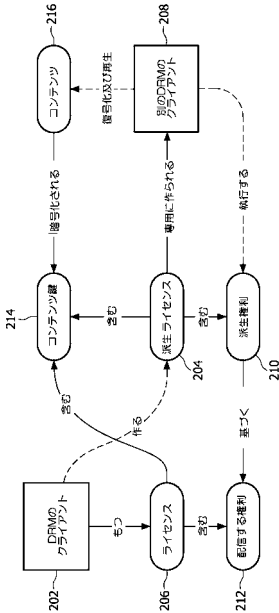
【0041】

本発明は、将来のDRMシステム、又は現在開発中の斯様なシステムに適用されることができる。本システムがやっかいな方針の議論を迂回するので、当該システムは、本発明の利益を得ることができる領域モデルを標準化することを可能にする。例えば、異なるDRMシステムの間を仲介するサービス・フレームワークにおいて、このアプローチは異なるコンテンツ項目に対するコンテンツの交換方針を記述するために用いることができ、複数の領域モデルが同じ技術的なフレームワークの範囲内に共存することを可能にする。これは、製造業者がDRMを実行することができる仕様を開発することを可能にし、この結果、当該DRMは、種々異なる製造業者からの装置の範囲を横断して動作することができる。

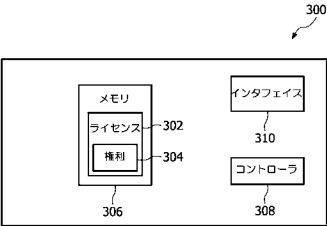
【図 1】



【図 2】



【図 3】



フロントページの続き

(72)発明者 レウーツェル ヨハン ジー エイチ
オランダ国 5 6 5 6 アーエー アインドーフエン ハイ テック キャンパス 4 4

審査官 和田 財太

(56)参考文献 特表 2 0 0 5 - 5 1 7 2 2 2 (J P , A)
国際公開第 0 4 / 0 3 8 5 6 8 (W O , A 1)
国際公開第 0 5 / 0 9 3 5 4 4 (W O , A 1)
特開 2 0 0 5 - 2 2 8 3 4 7 (J P , A)
特開 2 0 0 6 - 1 2 9 3 2 3 (J P , A)
特表 2 0 0 4 - 5 3 2 4 9 5 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)
G06F 21/10
H04N 7/167