

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5552176号
(P5552176)

(45) 発行日 平成26年7月16日(2014.7.16)

(24) 登録日 平成26年5月30日(2014.5.30)

(51) Int.Cl.	F I
G06F 21/62 (2013.01)	G06F 21/24 166A
G06F 21/70 (2013.01)	G06F 21/02
G06F 21/10 (2013.01)	G06F 21/22 110A
H04L 9/14 (2006.01)	H04L 9/00 641

請求項の数 22 外国語出願 (全 31 頁)

(21) 出願番号	特願2013-32536 (P2013-32536)	(73) 特許権者	504399716
(22) 出願日	平成25年2月21日(2013.2.21)		ディズニー エンタープライゼス インコーポレイテッド
(62) 分割の表示	特願2010-157194 (P2010-157194)の分割		アメリカ合衆国 カリフォルニア州 91521 バーバンク サウス ブエナ ヴィスタ ストリート 500
原出願日	平成22年7月9日(2010.7.9)	(74) 代理人	100147485
(65) 公開番号	特開2013-101697 (P2013-101697A)		弁理士 杉村 憲司
(43) 公開日	平成25年5月23日(2013.5.23)	(74) 代理人	100134577
審査請求日	平成25年2月25日(2013.2.25)		弁理士 石川 雅章
(31) 優先権主張番号	12/460,003	(72) 発明者	アルノー ロバート
(32) 優先日	平成21年7月10日(2009.7.10)		アメリカ合衆国 カリフォルニア州 91501 バーバンク イースト ハーバード ロード 1052
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	12/460,009		
(32) 優先日	平成21年7月10日(2009.7.10)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 相互運用キー収納箱

(57) 【特許請求の範囲】

【請求項1】

コンテンツに係るデジタルレシートのオンライン登録のための方法であって、
該方法は、

前記コンテンツを、第1のディストリビュータから得るために、取引を実行するステップと、

前記コンテンツに係る前記デジタルレシートを前記第1のディストリビュータから受信し、前記デジタルレシートは、前記取引に関連する情報を含むステップと、

前記コンテンツに係る前記デジタルレシートのオンライン登録のために、前記デジタルレシートをキー収納場所へ送信するステップと、

前記デジタルレシートを第2のディストリビュータへ送信するステップと、

前記コンテンツを再生するために、DRMライセンスを、前記第2のディストリビュータから受信し、前記DRMライセンスは、前記キー収納場所を用いて、送信された前記デジタルレシートの前記第2のディストリビュータの検証に応じて与えられるステップと、を有する、方法。

【請求項2】

前記デジタルレシートは、消費者に関するデータを含む、請求項1に記載の方法。

【請求項3】

前記デジタルレシートは、前記第1のディストリビュータに関するデータを含む、請求項1に記載の方法。

10

20

【請求項 4】

前記デジタルレシートは、取引の種類及び取引の日付を含む前記取引に関するデータを含む、請求項 1 に記載の方法。

【請求項 5】

前記デジタルレシートは、前記コンテンツに関するメタデータを含む、請求項 1 に記載の方法。

【請求項 6】

前記デジタルレシートは、前記キー収納場所に関するデータを含む、請求項 1 に記載の方法。

【請求項 7】

前記キー収納場所から、オンライン登録プロセスの成功又は失敗を示す戻り値を受信するステップを、さらに有する、請求項 1 に記載の方法。

10

【請求項 8】

前記デジタルレシートの一部は、前記デジタルレシートを受信する前に、さらに暗号化される、請求項 1 に記載の方法。

【請求項 9】

前記デジタルレシートの一部は、前記デジタルレシートを受信する前に、さらにデジタル署名される、請求項 1 に記載の方法。

【請求項 10】

前記デジタルレシートの暗号化部分は、前記キー収納場所の公開キーを用いて暗号化される、請求項 8 に記載の方法。

20

【請求項 11】

前記デジタルレシートの前記キー収納場所への送信は、前記第 1 のディストリビュータにより行われる、請求項 1 に記載の方法。

【請求項 12】

前記コンテンツを再生するために、第 1 のデジタル著作権管理 (DRM) ライセンスを、前記第 1 のディストリビュータから得るステップを、さらに有する、請求項 1 に記載の方法。

【請求項 13】

前記送信されたデジタルレシートの有効性を検証するために、前記キー収納場所は、前記デジタルレシートに含まれる前記情報に 1 つ以上の業務ルールを、さらに適用する、請求項 1 に記載の方法。

30

【請求項 14】

前記送信するステップは、さらにユーザの認証情報を送信するステップを有し、前記第 2 のディストリビュータは、前記送信されたデジタルレシートの有効性を検証するために、前記ユーザの認証情報を、さらに認証する、請求項 1 に記載の方法。

【請求項 15】

前記送信するステップは、さらにユーザの認証情報を送信するステップを有し、前記キー収納場所は、前記送信されたデジタルレシートの有効性を検証するために、前記ユーザの認証情報を、さらに認証する、請求項 1 に記載の方法。

40

【請求項 16】

前記ユーザの認証情報は、前記第 1 のディストリビュータ及び前記第 2 のディストリビュータを含む多数のディストリビュータと共に、認証するために、用いることができ、前記キー収納場所は、第三者認証サーバに対して、前記ユーザの認証情報を検証することにより、前記送信されたデジタルレシートの有効性を、さらに検証する、請求項 15 に記載の方法。

【請求項 17】

前記第 2 のディストリビュータは、同じユーザの認証情報を用いて認証されたデジタルレシートの追加のオンライン登録のために、前記キー収納場所に、さらにクエリーを行い、前記第 2 のディストリビュータからの受信は、前記追加のオンライン登録に係るコ

50

ンテンツ用のタイトルキーにアクセスするために、前記第2のディストリビュータと共に用いることができる追加のDRMライセンスを、さらに含む、請求項16に記載の方法。

【請求項18】

前記DRMライセンスを受信する前に、前記第2のディストリビュータから前記DRMライセンスにアクセスするために、さらに取引を行うステップを、さらに有する、請求項1に記載の方法。

【請求項19】

コンテンツに係るデジタルレシートのオンライン登録のための方法であって、
該方法は、
前記コンテンツを、第1のディストリビュータから得るために、取引を実行するステップと、

10

前記コンテンツに係る前記デジタルレシートを前記第1のディストリビュータから受信し、前記デジタルレシートは、前記取引に関連する情報を含むステップと、

前記コンテンツに係る前記デジタルレシートのオンライン登録のために、前記デジタルレシートをキー収納場所へ送信するステップと、

前記取引の証明を提供するために、前記デジタルレシートを前記キー収納場所へ再送信するステップと、

前記キー収納場所から、前記キー収納場所に応答して、タイトルキーにアクセスして、オンライン登録を有する再送信された前記デジタルレシートの有効性を検証し、それにより、前記取引の前記証明を確認するステップと、

20

前記キー収納場所からアクセスした前記タイトルキーを用いて復号した前記コンテンツの再生を起動するステップとを、有する、方法。

【請求項20】

コンテンツに係るデジタルレシートのオンライン登録のための方法であって、
該方法は、
前記コンテンツを、第1のディストリビュータから得るために、取引を実行するステップと、

前記コンテンツに係る前記デジタルレシートを前記第1のディストリビュータから受信し、前記デジタルレシートは、前記取引に関連する情報を含むステップと、

前記コンテンツに係る前記デジタルレシートのオンライン登録のために、前記デジタルレシートをキー収納場所へ送信するステップと、

30

前記取引の証明を提供するために、前記デジタルレシートを前記キー収納場所へ再送信するステップと、

前記キー収納場所により示された複数のディストリビュータから第3のディストリビュータを選択し、前記複数のディストリビュータは、前記デジタルレシートに係る前記コンテンツに対して配信特権を有する前記キー収納場所により検証される、ステップと、

前記コンテンツを再生するためのDRMライセンスを前記第3のディストリビュータから受信し、前記DRMライセンスは、前記キー収納場所に応答して、与えられて、前記オンライン登録を有する再送信された前記デジタルレシートの有効性を、前記第3のディストリビュータへ転送し、それにより、前記取引の前記証明を確認するステップとを、有する、方法。

40

【請求項21】

前記再送信するステップは、さらにユーザの認証情報を送信するステップを有し、前記キー収納場所は、前記ユーザの認証情報が前記再送信されたデジタルレシートの有効性を検証することを、さらに認証する、請求項20に記載の方法。

【請求項22】

前記再送信するステップは、さらにユーザの認証情報を送信するステップを有し、前記第3のディストリビュータは、前記ユーザの認証情報が前記再送信されたデジタルレシートの有効性を検証することを、さらに認証する、請求項20に記載の方法。

50

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は一般的にデジタルメディアに関する。特に、本発明はデジタルメディアについてのデジタル著作権管理に関する。

【背景技術】**【0002】**

デジタルメディア配信がはやってきて、多くの消費者にとって小売りの物理メディアを購入するための実行可能な代替になっているけれども、消費者が無条件で、デジタルメディアを完全に受け入れることができる前に、なお重大な障害がある。これらの条件のうち10の多くは、異なる再生装置又はサービスプロバイダーと、メディアファイルが新しいフォーマット又は防護機構により将来動作不可能になる可能性との間の制限された相互運用を中心に展開する。例えば、競合するデジタルメディア配信チャンネルは、互換性がないメディアフォーマット及び専用のデジタル著作権管理(DRM)システムを用いることができるため、経営不振又は会社のオーナーの交代によるビデオの販売の打ち切り又は終了により、消費者に、もはや使用できないメディアファイルを残す結果となる。

【0003】

従って、オリジナルの使用配信チャンネル及びオリジナルのメディアファイルフォーマットにかかわらず、配信マーケットの変更に生き延びて、継続サービスを消費者に提供できる相互運用保護コンテンツの必要性がある。このようにして、消費者は、サービスプロバイダーを容易に変更でき、多種多様の再生装置にわたって保護メディアを使用でき、保護コンテンツの再生が将来保証されることを確信することができる。同様に、コンテンツ製作者は、発展し得る持続可能なビジネスモデルとして、保護メディアのデジタル配信に依存することを確信することができる。しかしながら、単一のDRMの方法論を単に定めることによる最も直接的な方法で、このような相互運用を保証するために、多くの既存のDRMシステム及び配信チャンネルは、市場での熱意がほとんど見出されない命題である、確立され証明された運用手続きを根本的に変更する必要がある。その上、これは、脆弱性の単一の安全性ポイントを作り出す。

【発明の概要】**【発明が解決しようとする課題】****【0004】**

従って、特にキー管理について、既存のデジタル著作権管理枠組み、配信モデル及び消費モデルに対する最小限の破壊的变化を必要とする方法で、デジタルメディアを異なるサービスプロバイダー及びメディア装置にわたって相互運用する方法を、提供することにより、従来の技術の欠点及び欠陥を克服する必要性がある。

【課題を解決するための手段】**【0005】**

本発明によれば、実質的には、少なくとも1つの図面に示され、及び/又は図面に関連して説明され、特許請求の範囲にもっと完全に記載されているように、相互運用キー収納箱のためのシステム及び方法が提供される。

【0006】

本発明の特徴及び利点は、以下の詳細な説明及び添付図面をレビューした後に、当業者にはもっと容易に明らかになるであろう。

【図面の簡単な説明】**【0007】**

【図1】本発明の一実施形態による、相互運用キー収納箱とともに使用するためのファイルを生成するシステムを示す図である。

【図2】本発明の一実施形態による、相互運用キー収納箱とともに使用するためのデジタルレシートをクライアントに提供するシステムを示す図である。

【図3】本発明の一実施形態による、異なるDRMシステム間の相互運用のための相互運用

10

20

30

40

50

キー収納箱により、保護されたデジタル著作権管理（DRM）ライセンスを得るためのシステムを示す図である。

【図4a】本発明の一実施形態による、オリジナルの発行メディア・ディストリビュータと無関係に相互運用キー収納箱を用いて保護メディアを再生するためのシステムを示す図である。

【図4b】本発明の一実施形態による、相互運用キー収納箱を用いて二次保護メディアを取り戻すためのシステムを示す図である。

【図5】コンテンツに係るデジタルレシートのオンライン登録がキー集中収納場所（CKR）を用いて使用でき、最初のディストリビュータとは無関係に、コンテンツの相互運用再生を可能にする、本発明の一実施形態によるステップを説明するフローチャートを示す図である。

10

【図6】メディアコンテンツがメディア・ディストリビュータに配信される、本発明の一実施形態によるステップを説明するフローチャートを示す図である。

【図7】キー集中収納場所（CKR）がコンテンツのアクセスの認可をメディア・ディストリビュータに提供することができる、本発明の一実施形態によるステップを説明するフローチャートを示す図である。

【図8】メディア・ディストリビュータが、キー集中収納場所（CKR）からのコンテンツのアクセスの認可へのアクセスを得ることができる、本発明の一実施形態によるステップを説明するフローチャートを示す図である。

【発明を実施するための形態】

20

【0008】

本出願は、相互運用キー収納箱とともに使用するための汎用ファイルパッケージ用のシステム及び方法を対象としたものである。以下の説明は本発明の実施に関する具体的な情報を含む。当業者は、本発明が本出願で具体的に述べる方法とは異なる方法で実施できることを認識するであろう。その上、本発明の特定な細部のいくつかは、本発明を曖昧にしないため述べないものとする。本出願で記載しない特定な細部は、当業者の知識の範囲内である。本出願の図面及び付随の詳細な説明は、本発明の単なる例示的な実施形態を対象としたものである。簡潔にするために、本発明の原理を用いる本発明の他の実施形態は、本出願において具体的に記載せず、また、本図面においても具体的に例示していない。

【0009】

30

図1は、本発明の一実施形態による相互運用キー収納箱とともに使用するためのファイル生成システムを示す。図1の環境100は、タイトルオーナー110、タイトルオーナーID（識別子）111、タイトルID（識別子）116、認証オーソリティ120、プリペアラ（Preparer）130、キー収納箱160及びメディア・ディストリビュータ170を含む。タイトルオーナー110は、タイトル115及びタイトルメタデータ118を含む。認証オーソリティ120は認可証121を含む。認可証121はキー収納箱公開キー122を含む。プリペアラ130は、キー・ジェネレータ131、タイトルキー132、汎用ファイルパッケージ135、汎用ファイル140及びキー情報ファイル150を含む。汎用ファイル140は、タイトルID116、メタデータ117、暗号化タイトル145及びキー収納箱URL（ユアールエル）146を含む。キー情報ファイル150は、タイトルオーナーID111、タイトルID116、暗号化データ153及び暗号化タイトルキー152を含む。キー収納箱160は、プロセッサ158及びメモリ159を含む。メモリ159は、プリペアラAPI（応用プログラムインターフェース）161、キー情報データベース162、消費者データベース163、トランザクションデータベース164、キー収納箱秘密キー165、ディストリビュータ公開キーデータベース166、ディストリビュータデータベース167及びプロバイダーAPI157を含む。メディア・ディストリビュータ170は、書き換えられたキー情報ファイル151、ディストリビュータ秘密キー175及びネイティブDRM（デジタル著作権管理）システム172を含む。

40

【0010】

50

タイトルオーナー 110 は、個々のアーティスト又は作曲家、メディア・グループ、映画撮影所、アニメーション・スタジオ、テレビ・スタジオ又は映画配給会社のようなプロデューサー、放送局、著作権者、著者又はタイトル 115 の譲受人を含むことができる。それから、タイトル 115 は、楽曲又は曲集、ラジオ番組、ビデオクリップ、全編の映画又はアニメーション、ドラマ又はテレビ番組のシリーズ物の1回放映分、インタラクティブなビデオゲーム又は任意の他のタイプの視聴覚の作品又はコンテンツのような独創的なメディアの作品又はプロジェクトを含むことができる。それから、タイトルメタデータ 118 は、人間が読めるタイトル名、特定のメディアカテゴリ、コンテンツのジャンル、メディアフォーマット、視聴率及びタイトル 115 をカタログに載せて同定するために役立つ情報を提供するような、タイトル 115 をもっと詳細に説明するために提供することができる。図 1 では、タイトルメタデータ 118 は、タイトルオーナー 110 により提供されるが、代替の実施形態は、タイトルメタデータ 118 を生成するため、代わりに、プリペアラ 130 又は他の第三者を用いることができる。

10

【0011】

さらに、タイトルオーナー 110 及びタイトル 115 は、それぞれタイトルオーナー ID 111 及びタイトル ID 116 により、各々、一意的に同定される。これらの識別子も、タイトルメタデータ 118 の中に含むことができる。一意的な識別子を選択するための任意の適切なアルゴリズム採用することができるけれども、タイトル ID 116 は、可能な場合は国際標準視聴覚番号 (ISAN)、及びセキュア・ハッシュ・アルゴリズム 1 (SHA-1) のような暗号関数に基づくユニバーサル一意識別子 (UID) の組み合わせに、特に適している。このようにして、種々異なるタイトルオーナーは、お互いにコミュニケーションを取り合わずに、なお、一意性の強力な保証を持ってタイトル ID を生成することができる。代替的に、中央集権的機構は、全ての識別子のデータベースを維持することにより、一意性を保証する一意識別子を要求する当事者へ配信することができる。

20

【0012】

一旦、上記識別子、メタデータ及びタイトルファイルが整うと、タイトルオーナー 110 は、一般公衆に役立つ配信チャンネルに集積するため、それらをプリペアラ 130 の汎用ファイルパッケージ 135 へ送ることができる。このプリペアラ 130 への送付は、好ましくは、第三者の情報漏れの恐れを緩和する安全な方法で、任意の適切な通信手段により、行うことができる。例えば、安全なファイル転送プロトコル (FTP)、セキュア・ソケット・レイヤー (SSL)、セキュア・シェル (SSH) 又は別のプロトコルのような様々な保護インターネットプロトコルを利用することができる。代替的に、データは、郵便で又は本人が直接にプリペアラ 130 へ届けるために、物理的媒体に書き込むことができる。

30

【0013】

符号化及び配信のためのタイトルの準備プロセスは、効率化又は他の理由のため、第三者機関へ外部委託できるので、図 1 では、タイトルオーナー 110 及びプリペアラ 130 は、別個の構成要素として示される。しかしながら、代替の実施形態は、プリペアラ 130 の機能も担うタイトルオーナー 110 を有することができる、より小さいメディアユニットの操作にはもっと便利にすることができる。この場合、タイトルオーナー 110 及びプリペアラ 130 は、同一の親により所有され、それらの機能は、単一のサーバ又はコンピュータクラスターに統合することができる。

40

【0014】

キー・ジェネレータ 131 は、暗号化によりコンテンツの保護をサポートするために、汎用ファイルパッケージ 135 へ暗号化キーを提供する。タイトル 115 に対するいくつかの種類 of 保護を適用しなければ、消費者は保護されないメディアファイルに直接アクセスするため、ライセンス期間を施行し、無認可のコピーを防ぐことが困難になる。従って、図 1 に示すように、キー・ジェネレータ 131 は、タイトル 115 を暗号化したり復号したりするために、対称の暗号化キー、タイトルキー 132 を生成する。適切な DRM ライセンスを有する認可されたメディアアプリケーションに対するタイトルキー 132 へ

50

のアクセスを制限することにより、消費者は、保護されない形でタイトル 1 1 5 に直接アクセスしないで、なお、タイトル 1 1 5 を見て聴いて楽しむことができる。

【 0 0 1 5 】

タイトルキー 1 3 2 用のより長いキーの長さ及びより強い暗号化アルゴリズムは、アクセス規制回避技術に対してより大きいセキュリティを提供することができるけれども、復号複雑性も重要な対抗考慮すべき事項をもたらす。この対抗考慮すべき事項は、限られたバッテリー寿命、メモリ及び処理リソースを有するモバイル機器にとって特に重大である。従って、タイトルキー 1 3 2 を暗号化するために、エー・イー・エス (AES) のようなバランスのとれた妥協を選択することができて、速い復号時間を有する合理的に強いセキュリティを提供する。

10

【 0 0 1 6 】

キー収納箱 1 6 0 によるアクセスのために、タイトルキー 1 3 2 をプリペアラ 1 3 0 から安全に送るために、認証オーソリティ 1 2 0 により生成された非対称の暗号化キー対を図 1 に示すように用いる。その暗号化キー対はキー収納箱 1 6 0 によっても生成することができ、認証は認証オーソリティ 1 2 0 により発行される。公開及び秘密のキー対は、例えば、公開キー暗号化基準 # 1 (PKCS # 1) に従って、2 0 4 8 ビットの RSA キーを用いる。キー対の公開キーは、デジタル認可証 1 2 1 に含まれる。認可証 1 2 1 からキー収納箱公開キー 1 2 2 を検索することにより、汎用ファイルパッケージ 1 3 5 は、キー収納箱公開キー 1 2 2 を用いてタイトルキー 1 3 2 を暗号化することができて、対応するキー収納箱秘密キー 1 6 5 のオーナーであるキー収納箱 1 6 0 のみが、暗号化タイトルキー 1 5 2 を復号することができるような、暗号化タイトルキー 1 5 2 が得られる。認証オーソリティ 1 2 0 は、認可証 1 2 1 内に設けられたキー収納箱公開キー 1 2 2 が、キー収納箱 1 6 0 として知られる構成要素に適切に結合することを保証する、図 1 の信頼できる第三者としての機能を果たす。

20

【 0 0 1 7 】

認証オーソリティ 1 2 0 は、例えば、X . 5 0 9 第 3 版認証基準に準拠することができる。認証オーソリティ 1 2 0 の同一性を検証するために、プリペアラ 1 3 0 は、認証オーソリティ 1 2 0 のような信頼できる第三者の同一性を保証する、あらかじめ組み込まれた一組の認可証も有することができる。相互認証も、認証オーソリティ 1 2 0 が、認証されたプリペアラ、メディア・ディストリビュータ又はサービスプロバイダー、及び他の関係者に応答するように、実装することができる。図 1 では、単一の認証オーソリティのみを示しているが、代替の実施形態は、認証オーソリティの階層的システムを用いることができ、又は、同等の中程度の信頼網のような X . 5 0 9 以外の代替の信頼できるシステムを用いることができる。

30

【 0 0 1 8 】

このようにして、キー収納箱 1 6 0 は、キー情報ファイル内に暗号化された形でタイトルキーを保持するキー集中収納場所 (CKR) としての機能を果たす。プリペアラ A P I 1 6 1 により、プリペアラ 1 3 0 のようなコンテンツプリペアラは、暗号化タイトルキーをキー情報ファイル 1 5 0 のようなキー情報ファイルコンテナに提出することができる。暗号化タイトルキー 1 5 2 のような暗号化タイトルキー、暗号化データ 1 5 3 のような暗号化データ又はメタデータ、並びにタイトルオーナー I D 1 1 1 及びタイトル I D 1 1 6 のような関連するコンテンツ情報を含むこれらのキー情報ファイルは、キー情報データベース 1 6 2 のようなデータベースに保存することができる。プリペアラ 1 3 0 がプリペアラ A P I 1 6 1 にアクセスするために、標準ウェブサービスは、キー交換のための PKCS # 3 に準拠するディフィエ・ヘルマン (Diffie Hellman) を有するトランスポート層セキュリティ (TLS) を用いたシンプル・オブジェクト・アクセス・プロトコル (SOAP) 及びハイパーテキスト転送プロトコル・セキュリティ (HTTPS) を用いてキー収納箱 1 6 0 により、さらすことができる。異なるパラメータを用いる安全な通信又は改良型のこの同じ方法は、図 1 及び以下の図に示す他の通信経路に対しても用いることができる。さらに、入ってくるインターネットプロトコル (IP) アドレスレンジ又はメディアアクセ

40

50

ス制御 (MAC) アドレスレンジを周知の値に制限するようなセキュリティー対策も、認可されないアクセスに対してさらに防護するために、実装することができる。

【 0 0 1 9 】

前に論じたように、暗号化タイトルキー 1 5 2 は、キー収納箱公開キー 1 2 2 を用いて暗号化される。キー収納箱 1 6 0 は、対応する秘密キーであるキー収納箱秘密キー 1 6 5 のオーナーであるため、キー情報データベース 1 6 2 に提出された全てのタイトルキーを、上記のやり方で自由に復号してアクセスできる。プリペアラー A P I 1 6 1 及びプロバイダー A P I 1 5 7 により受信してメモリ 1 5 9 内にあるリクエストを解釈するためのプロセッサ 1 5 8 を用いて、キー収納箱 1 6 0 は、サービスプロバイダー又はコンテンツプロバイダーとしても呼ばれる認証されたプリペアラー及びメディア・ディストリビュータ用の強固なキーの保存及び配信サービスを提供することができる。他の方向において、プロバイダー A P I 1 5 7 により、メディア・ディストリビュータ 1 7 0 のような認証されたディストリビュータは、これらの暗号化された形のタイトルキーがそれ自体の非対称キー対を用いて、消費者へメディア・アプリケーション及び装置を配るための DRM ライセンスを安全に生成することを要求することができる。このように、キー情報データベース 1 6 2 からの元のキー情報ファイルは、復号され、暗号化され、又は書き換えられて、各特定のメディア・ディストリビュータに適用可能な暗号化キーを用いて、書き換えられたキー情報ファイル 1 5 1 のような書き換えられたキー情報ファイルを生成する。

10

【 0 0 2 0 】

図 1 では、このキー情報ファイルの書き換えは、メディア・ディストリビュータ 1 7 0 のような各ディストリビュータが、ディストリビュータ秘密キー 1 7 5 のようなそれ自体の対応する秘密キーを所有すると共に、キー収納箱 1 6 0 にディストリビュータ公開キーデータベース 1 6 6 内の全てのメディア・ディストリビュータの公開キーを集めさせることにより、可能となる。メディア・ディストリビュータは、標準公開キー基盤 (PKI) アプローチを用いてそれ自体のキー対を生成できる。しかしながら、代替の実施形態は、キー収納箱 1 6 0 が、公開 / 秘密キー対を生成し、安全な通信チャンネルを用いて、各メディア・ディストリビュータに秘密キーを提供するような、代替の暗号化の手筈を用いることができる。前述のキー収納箱公開キー 1 2 2 と同様に、認証オーソリティ 1 2 0 又は別の信頼できる第三者を利用して、公開キーとその関連する参照同一性との間の正当な結合を保証する信頼できる認証を提供することができる。

20

30

【 0 0 2 1 】

キー収納箱 1 6 0 に示すように、いくつかの追加のデータベースが、消費者データベース 1 6 3、トランザクションデータベース 1 6 4、ディストリビュータデータベース 1 6 7、販売データベース 1 6 8 及びプリペアラーデータベース 1 6 9 を含み、利用することができる。これらのデータベースは、キー収納箱側から様々な業務ルールを実装するために利用することができ、それにより、消費者及び関連する権利により行われるメディア・トランザクションを記録し、消費者の認証データを記録し、様々な業務契約に従って認証されたプロバイダー及びメディア・ディストリビュータのみがキー収納箱と通信することができることを保証する。例えば、成功したオンライン・トランザクション毎の後に、トランザクションデータベース 1 6 4 に記録を保存し、販売の日時、支払代金、レンタルか購入かの種類、買い戻し、又は予約、提供された買い戻しコードが多数回使用されたかどうか、消費者、クライアント、装置 ID (識別子) 及びその他の詳細のような関連する識別子を示すことができる。従って、キー収納箱 1 6 0 は、レンタル期間、買い戻しカウント限界、必要に応じて他の業務ルールを執行することができる。ディストリビュータデータベース 1 6 7 は、キー収納箱 1 6 0 が、異種コンテンツライセンス契約で、いくつかの異なる関連の又は非関連のメディア・ディストリビュータをサポートすることができるので、どのメディア・ディストリビュータがどのキー情報ファイルにアクセスするのに権限を与られているかを追跡することができる。消費者データベース 1 6 3 は、さらに図 2 で論じるように、消費者が、特定のメディア・ディストリビュータに制限されずに、保護されたメディアファイルにアクセスし開錠することを可能にする権利の収納場所として役立

40

50

つことができ、かつ、消費者が、唯一のディストリビュータ又は開いたID (Open ID) のようなより開いたフレームワークからの専用の認証スキームのような、単一の又は多数の認証スキームを用いて多数のディストリビュータにわたって認証することを可能にする認証情報も含むことができる。追加的に又は代替的に、キー収納箱 160 は、図 1 に示していない装置データベースを含むことができ、装置データベースは、特定の消費者よりも特定の装置への結合に基づくモデルを可能にするか、又は、消費者と装置との両方への結合に基づくモデルを可能にし、特定の消費者に関連することができるメディア装置のリストを作る。一般的に言えば、装置データベースは、消費者データベース 163 と同様に機能し、消費者データベース 163 に関連している。販売データベース 168 は、例えば、タイトルを、レンタル、予約及び購入のような多数のビジネスモデルをサポートする特別の使用ルールと関連付けることができる。プリペアラーデータベース 169 は、認証されたメディアプリペアラーのみが、キー情報ファイルをキー収納箱 160 にアップロードすることができることを保証することができる。

【0022】

キー情報ファイル 150 から汎用ファイル 140 へ焦点を切り替えると、汎用ファイル 140 も、メディア・ディストリビュータへの配信のために、最終的には消費者への配信のために、汎用ファイルパッケージ 135 により生成される。「汎用ファイル」の名称は、たとえメディア・ディストリビュータが異なるDRMシステムを用いても、同一のファイルが、消費者へ配信され、CKR、キー収納箱 160 を用いて異なるメディア・ディストリビュータにわたって、相互運用されるという特性を説明する。図 1 に示すように、タイトル 115 はタイトルキー 132 を用いて暗号化されて、暗号化タイトル 145 が作られ、タイトルID 116、メタデータ 117 及びキー収納箱URL 146 を含むデータの同定を伴う。メタデータ 117 は、例えば、タイトルメタデータ 118 の成分を含むことができる。キー収納箱URL 146 は、暗号化タイトル 145 がキー情報ファイル 150 に保存されたタイトルキー 132 を用いて復号することができるように、関連するキー情報ファイル 150 を保存するキー収納箱がどこで見つけられるかを指示するポインター又はネットワークアドレスとしての機能を果たす。図 1 の場合、キー収納箱URL 146 は、キー収納箱 160 を指し示す。なお、キー収納箱URL は、キー収納箱の通信を柔軟にリダイレクトするために、単に、URLリダイレクトを用いるリダイレクトサーバを指し示せばよい。さらに、URL形式が、SOAPを用いるインターネットによってアクセス可能なウェブサービスにつなぐために、選択されるが、代替のネットワークアドレス指定プロトコルも同様に用いることができる。汎用ファイル 140 の成分は、MPEG-4パート14又はMP4コンテナファイルのような標準コンテナフォーマットに埋め込むことができる。さらに、タイトル 115 が非圧縮フォーマットで提供されるならば、プリペアラー 130 は、例えば、MPEG-4パート10又はH.264を用いてタイトル 115 を暗号化する前に、ビデオ及び音声圧縮をすることができる。汎用ファイル 140 は、生成された後に、メディア・ディストリビュータ 170 へ送ることができる。

【0023】

一旦、メディア・ディストリビュータ 170 が汎用ファイル 140 を受信すると、メディア・ディストリビュータ 170 は、直ちに、キー収納箱URL 146 から関連するキー情報ファイルを要求することができるか、又は、消費者又はクライアントが実際に汎用ファイル 140 を要求するまで、キー情報ファイルの要求を遅らすことができる。どちらの場合も、メディア・ディストリビュータ 170 は、前に論じたように、例えば、HTTPSによるSOAPを用いて問い合わせを行い、タイトルID 116 と関係があり関連するキー情報ファイルに含まれる情報を要求する。それから、キー収納箱 160 は、同一のタイトルID 116 を有するキー情報ファイル 150 を見つけるために、キー情報データベース 162 を検索し、ファイルを配信する許可が与えられるべきかどうかを決定する全ての関連する業務ロジックルールを適用し、許可が与えられるべき決定がなされるならば、書き換えられたキー情報ファイル 151 を与えることができる。書き換えられたキー情報ファイル 151 は、暗号化タイトルキー 152 が、キー収納箱 160 の公開キーであるキー収納箱

10

20

30

40

50

公開キー 122 ではなく、メディア・ディストリビュータ 170 の公開キーにより暗号化されることを除いて、キー情報ファイル 150 に類似して見える。前に論じたように、書き換えステップは、全てのメディア・ディストリビュータの公開キーを、前もってディストリビュータ公開キーデータベース 166 に収集するキー収納箱 160 によりサポートすることができる。

【0024】

新しく書き換えられたキー情報ファイル 151 をキー収納箱から常に検索することを避けるために、メディア・ディストリビュータは、キー収納箱のリソースに不必要に負担させることを避けるために、書き換えられたキー情報ファイルのローカルキャッシュを保存することができる。キャッシュに格納されたキー情報ファイルを更新するために、以前のキー情報のアクセスは、キー収納箱から定期的に又はオン・デマンドで要求することができるので、変更の要求は発生する。代替的に、キー収納箱は、更新情報をメディア・ディストリビュータへ積極的に送ることができる。

10

【0025】

一旦、メディア・ディストリビュータ 170 が、キー情報ファイル 151 及び汎用ファイル 140 を共に書き換えると、メディア・ディストリビュータ 170 は、ディストリビュータ秘密キー 175 及びネイティブ DRM システム 172 とともに、それらを使用することができる。メディア・ディストリビュータ 170 に対しすでに適所にある既存の DRM システムのインフラストラクチャーに対する、もしあれば、わずかな修正をもって、保護された方法で、メディアファイルをクライアントにサービスすることができる。メディア・ディストリビュータ 170 は、それ自体の秘密キーであるディストリビュータ秘密キー 175 を用いることができ、書き換えられたキー情報ファイル 151 からタイトルキー 132 にアクセスし、そのタイトルキー 132 をネイティブ DRM システム 172 へ供給する。それから、ネイティブ DRM システム 172 は、使用ルール及びそれ自体のセキュリティープロトコルを用いて暗号化されたタイトルキー 132 を含む適切な DRM ライセンスを生成することができる。一旦、消費者が汎用ファイル 140 及びネイティブ DRM ライセンスを受け取ると、消費者は、使用ルールにより許可されるように、汎用ファイル 140 内に含まれるメディアを使うことができる。

20

【0026】

このようにして、汎用ファイルフォーマット及び相互運用キー収納箱の採用に入る障壁は、メディア・ディストリビュータに参加し、より広い配信チャンネルの採用を促し、強化した相互運用の全ての利点を消費者に与えるために、最小にされる。以下に図 2 で説明するように、デジタル配信されたメディアに関するアドレスの相互運用及び可用性の懸念を助けることにより、かつ、消費者の制御内のデジタルレシートを提供することにより、消費者は、デジタル配信により制限されるよりも権限を与えられると感じることができ、ひいては、より売り上げが伸び、消費者がより満足することができる。

30

【0027】

タイトルオーナー 110、タイトル 115、認証オーソリティ 120、プリペアラー 130、キー収納箱 160 及びメディア・ディストリビュータ 170 は、図 1 では、単一のインスタンスのみを有しているけれども、代替の実施形態は、各構成要素のいくつかのインスタンスを含むことができる。例えば、汎用ファイル 140 は、いくつかの異なるタイトルを、編集物の一部、アルバム又は代替のトラックとして、カプセル化することができる。同様に、キー情報ファイル 150 は、いくつかの関連するタイトルキーを保存することができる。キー収納箱も、特定の組織的なニーズに適合するように、拡大縮小することができる。例えば、多くの映画設備を有する大きいスタジオ及び下位部門は、スタジオ部門毎に別個のキー収納箱を専用にするものの決定ができるか、又は、全ての部門が 1 つの大きい統合されたキー収納箱により供給されることを選ぶことができる。代替的に、より小さいスタジオでは特に、いくつかの異なるスタジオ又は会社は、単一のキー収納箱を共有することができ、又は、キー収納箱の操作及びメンテナンスを第三者事業体に外注することができる。別の可能性は、第三者により操作され、キー情報ファイルを集中キー収納

40

50

箱に服従させるスタジオを有する、1つの大きい集中キー収納箱である。上記のように、URLリダイレクトも、柔軟なキー収納箱のリダイレクト用に用いることができ、サーバの負荷バランス、高速移動及び他の機能を可能にする。キー収納箱も、適切な契約及びセキュリティ手続きが整っていれば、他のキー収納箱と情報を共有することができる。言い換えれば、キー収納箱は、要望通り、集中化又は分散化することができるが、大きいキー情報データベースにアクセスする集中キー収納箱が、多数のメディア・ディストリビュータと取引を有するクライアントに、もっと効率的なサービスを提供することができる。

【0028】

図2は、本発明の一実施形態による相互運用キー収納箱とともに使用するためのデジタルレシートをクライアントに提供するシステムを示す。図2の環境200は、キー収納箱260、メディア・ディストリビュータ270、ディストリビュータID271、クライアント280、クライアントID281、共有クライアントID286、ディスプレイ288及びバックアップ記憶装置289を含む。キー収納箱260は、キー情報データベース262、消費者データベース263、トランザクションデータベース264、キー収納箱秘密キー265、ディストリビュータ公開キーデータベース266、ディストリビュータデータベース267、販売データベース268、クライアントAPI256及びプロバイダーAPI257を含む。図2では、プリペアラーとの双方向通信はないため、図1のプリペアラーAPI161及びプリペアラーデータベース169は、図2では簡単のために省略されているが、なお、キー収納箱260内に存在し得る。メディア・ディストリビュータ270は、汎用ファイル240、書き換えられたキー情報ファイル251、ネイティブDRMサーバ272、DRMライセンス273、ディストリビュータ秘密キー275及びプロセッサ276を含む。汎用ファイル240は、タイトルID216、メタデータ217、暗号化タイトル245及びキー収納箱URL246を含む。書き換えられたキー情報ファイル251は、タイトルオーナーID211、タイトルID216及び暗号化タイトルキー252を含む。DRMライセンス273は、タイトルID216、暗号化タイトルキー274、クライアントID281及び使用ルール277を含む。クライアント280は、ネイティブDRMクライアント282、クライアント・メディア・アプリケーション283、保護されたメディアパス復号エンジン299及びデジタルレシート285を含む。デジタルレシート285は、タイトルID216、ディストリビュータID271、クライアントID281、共有クライアントID286、消費者ID284及びトランザクション情報287を含む。なお、図2に関し、キー収納箱260は図1のキー収納箱160に対応し、メディア・ディストリビュータ270は図1のメディア・ディストリビュータ170に対応する。図2のキー収納箱260は、図1のキー収納箱160のように、プロセッサ又はメモリを示していないけれども、それらは、キー収納箱260のAPIの動作及び他の論理演算をサポートするために存在すると見なすことができる。

【0029】

図2は、焦点を、図1のタイトルオーナー及びプリペアラーから、図2のメディア・ディストリビュータ及びクライアントへ移す。もっと具体的に言うと、どのようにして消費者又はクライアントが、図1で導入された汎用ファイル、キー情報ファイル及びCKR又はキー収納箱のコンセプトを用いて、ディスプレイ288上に結果として生ずる再生用のメディアファイルに、実際にアクセスすることができるかを、図2は例示する。さらに、図2は、デジタルレシート285として示すデジタルレシートのコンセプトを導入し、デジタルレシートのコンセプトは、例えば、たとえ、クライアントが、もともと検索され、保護されていたメディアファイルをなくしたとしても、又は、たとえ、クライアントが、メディア・ディストリビュータを替えたとしても、保護されるメディアコンテンツを復活させるための、購入証明書又は取引証明書としての機能を果たすことができる。

【0030】

汎用ファイル240及び書き換えられたキー情報ファイル251のコンテンツは、図1の対応する汎用ファイル140及び書き換えられたキー情報ファイル151により、いく

10

20

30

40

50

らか詳細に、すでに説明した。書き換えられたキー情報ファイル251は、書き換えステップ用のキー収納箱260とともに、図1のタイトルオーナー110に類似の事業体のような、メディア・ディストリビュータ270と配信契約を有する事業体により、メディア・ディストリビュータ270へ供給することができた。メディア・ディストリビュータ270のプロセッサ276は、ネイティブDRMサーバ272と共の使用用に暗号化タイトルキー252を復号するため、ディストリビュータ秘密キー275と共に使用することができる。プロセッサ276で実行するネイティブDRMサーバ272は、それから、図2に示す全ての入力を用いることができ、汎用ファイル240を要求する認証されたクライアントへの配信のために、DRMライセンス273を生成する。暗号化タイトルキー274は、ネイティブDRMサーバ272により提供され、メディア・ディストリビュータ270の暗号化パートナーをキー収納箱260からクライアント280へ効果的に変更する保護システムを用いて、保護することができる。このステップは、特定のメディア・ディストリビュータに対して書き換えられたキー情報ファイルを提供するキー収納箱260に類似の追加の書き換えステップのように見なすことができるが、メディア・ディストリビュータ270を備えて、代わりにDRMライセンス273に特定のクライアント用の書き換えられたタイトルキーを提供する。

10

【0031】

DRMライセンス273を調べるに、汎用ファイル240を復号するために使用できる対応するタイトルキーである暗号化タイトルキー274が含まれている。DRMライセンス273は、DRMライセンスが適用するクライアントの同定情報、すなわち、クライアントID281も含み、かつ、関連するメディアタイトル又は汎用ファイルの同定情報、すなわち、タイトルID216も含む。図2に示すように、ディストリビュータID271、共有クライアントID286、消費者ID284、使用ルール277及びトランザクション情報287のような追加の情報も、DRMライセンス273に埋め込むことができる。

20

【0032】

クライアント280に移動するに、クライアント280は、パソコン、メディアプレーヤー、セットトップボックス、ビデオゲーム機器、携帯電話、ポータブルメディアプレーヤー又はメディア・ディストリビュータ270とインターフェースをとる任意の他の装置を含むことができる。クライアント280は、ブラウジング、購買、再生及びメディア・ディストリビュータ270により提供されるデジタルメディアとその他のトランザクション用のクライアント・メディア・アプリケーション283を含むことができる。消費者がクライアント280上での再生用のデジタル取引により、汎用ファイル240を購入、レンタル又は他の方法で得ることを決定した後で、メディア・ディストリビュータ270は、金融機関とインターフェースをとることにより、取引を処理することができ、合意した金額を請求し、又は前払いのポイント又は他の通貨の合意した金額を内部的に差し引き、上記のように、DRMライセンス273を生成し、汎用ファイル240及びDRMライセンス273を共に、ネイティブDRMサーバ272により、クライアント280へ提供する。さらに、デジタル取引の記録は、キー収納箱260のプロバイダーAPI257により、トランザクションデータベース264に入れることができる。

30

【0033】

クライアント280が汎用ファイル240及びDRMライセンス273を共に受信した後、クライアント280は、ネイティブDRMクライアント282とともに、DRMライセンス273を用いることができ、音声コンテンツ用のスピーカーも含むことができるディスプレイ288へ出力する保護されたメディアパス復号エンジン299を用いる再生により使用するため、汎用ファイル240内の暗号化タイトル245を復号する。従って、消費者は、要求したメディアをディスプレイ288で見ることができる。

40

【0034】

汎用ファイル240及びDRMライセンス273が、クライアント280に暗号化タイトル245を再生させ、ネイティブDRMクライアント282が、ネイティブDRMサーバ272とインターフェースをとることができる間に、上記1つ以上の構成要素がクライアント2

50

80に欠けており、ユーザは完全に異なるクライアントを使用する必要があり、又は、ユーザは異なるメディア・ディストリビュータを使用する必要がある状況があり得る。この不測の事態に備えるために、メディア・ディストリビュータ270は、クライアント280に安全なデジタルレシート285を提供することもできる。消費者が上記の状況に対処する場合、汎用ファイルを再取得するため、新たなDRMライセンスを得るため、又は、状況に応じて両方とも得るための購入証明書として、デジタルレシート285を、検索することができ、代替のメディア・ディストリビュータ又はキー収納箱260へ渡すことができる。

【0035】

図2に示すように、クライアント280は、バックアップ記憶装置289にコピーすることにより、デジタルレシート285を積極的に保護し、バックアップ記憶装置289は、ユニバーサル・シリアル・バス(USB)記憶装置を含むことができ、デジタルレシートを消費者データベース263へ入れるため、クライアントAPI256により、関連するCKR又はキー収納箱260を用いて記録する。例えば、ウェブインターフェースを提供することができて、クライアントAPI256により、デジタルレシートをキー収納箱260へ直接アップロードすることを可能にし、クライアントAPI256は、プロバイダーAPI257と同様にHTTPSにより保護されたSOAPウェブサービスをさらすことができる。第三者は、例えば、オンラインバックアップサービスの提供又はウェブアクセス可能な電子メールサーバにより、バックアップ記憶装置289を提供しメンテナンスすることができる。特に、デジタルレシートが、登録した電子メールアドレスにより、ユーザへ提供される場合、ユーザの電子メールアカウントは、バックアップ保存場所として、デジタルレシートの代わりになる。

【0036】

代替的に、ユーザがデジタル取引を完了させた後、クライアント・メディア・アプリケーション283は、ユーザがデジタルレシートをオンラインで自動的にキー収納箱260に記録することを促すことができる。それから、キー収納箱260は、デジタルレシートの記録プロセスの成功か失敗かのいずれかを示す、戻り値をクライアント280へ提供することができる。

【0037】

デジタルレシート285は、デジタルレシートの作成に導くユーザの同一性に関連するいくつかのフィールドを含む。クライアントID281は、ネイティブDRMクライアント282及びネイティブDRMサーバ272により実装された特定のDRMシステムに関連する消費者又は装置を同定する。消費者ID284及びディストリビュータID271は、特殊のメディア・ディストリビュータに関連する特定の消費者を示し、一方、選択成分である共有クライアントID286は、ユーザを一般的な意味でグローバルに同定することができる。共有クライアントID286は、単一のメディア・ディストリビュータよりも、いくつかのメディア・ディストリビュータにわたって認証するために、使用できる開いたID(OpenID)のような外部のユーザ認証システムに結び付けることができる。全てのユーザがこのような共有クライアントIDを所有することはできないため、そのようなユーザに対して省略することができ、又は代替の識別子を作成し、ユーザに提供できる。しかしながら、共有クライアントID286が提供される場合、キー収納箱260は、メディア・ディストリビュータにかかわらず、消費者に帰属せしめられるべき消費者データベース263内の全てのレシートを同定することができ、いくつかの異なるメディア・ディストリビュータにわたって沢山のメディア収集物を有するユーザにとって、有用であることが証明できる。

【0038】

デジタルレシート285は、デジタルレシートを作りだす取引に関連するいくつかのフィールドを含む。タイトルID216は、デジタルレシートにより参照される特殊な汎用ファイルを示し、一方、トランザクション情報287は、取引の日付、取引の種類又は販売のような取引に関する特殊な情報、及び、タイトルID216により参照されるコンテ

10

20

30

40

50

ンツに関するメタデータを含むことができる。取引の日付は、取引が発生した特定の年月日及び時刻を含むことができ、一方、取引の種類は、例えば、取引が全額購買、レンタル、定期会員プランの一部、又は別の種類の取引を含むかどうかを示すことができる。メタデータは、タイトル、ジャンル分類、視聴率及び他のデータのような図1のメタデータ117に類似の情報を含むことができる。デジタルレシート285は、キー収納箱URL又は代替的にURLの形式でデジタルレシート285を記録するために用いるサーバについての情報、又は類似の参照データのようなキー収納箱260に関する情報も選択的に含むことができる。デジタルレシート285に保存されるデータの大多数は、暗号化で保護することができるのに、トランザクション情報287のタイトルメタデータ部分は、暗号化されないプレーンテキスト形式で示すことができ、デジタルレシートがユーザにより容易に同定されることを可能にする。図2に示すように、デジタルレシート285の部分は、キー収納箱260の公開キーを用いて暗号化し、キー収納箱260は、暗号化した部分を復号するために、キー収納箱秘密キー265を用いることができるが、キー収納箱260により使用可能な他の保護方法も利用することができる。なお、デジタルレシート285の部分も、配信するメディア・ディストリビュータ270により、デジタルに署名することができて、キー収納箱260は、デジタルレシート285が、認証されたメディア・ディストリビュータにより、正当に発行されたことを確認することができる。

10

【0039】

一旦、デジタルレシート285が、安全に、バックアップ記憶装置289及びキー収納箱260の消費者データベース263に保存されると、クライアント280のユーザは、汎用ファイル240の喪失、DRMライセンス273の喪失、及び、クライアント280及び/又はメディア・ディストリビュータ270の喪失又は変更から保護される。ユーザは、単に、バックアップ記憶装置289からデジタルレシート285を検索する必要があり、それをキー収納箱260、メディア・ディストリビュータ270又はキー収納箱260と確立した関係を有する別のメディア・ディストリビュータのいずれかへ、再提出する。一旦、デジタルレシート285が、キー収納箱260へ直接提出され、又は送られると、キー収納箱260は、必要に応じて、キー収納箱秘密キー265を用いてデジタルレシート285の暗号化部分を復号し、及び/又はメディア・ディストリビュータ270の公開キーを用いて上記の署名を認証し、デジタルレシート285を認証することができる。クエリー又は要求を是認又は否認するために任意の関連する業務ルールを処理することができる。クエリー又は要求が是認される場合、メディア・ディストリビュータは対応するキー情報ファイルを検索することができ、汎用ファイル240の再送を認証し、及び/又はユーザ用のタイトルキーを含む新たなDRMライセンスを生成する。

20

30

【0040】

ユーザの観点から、全てのメディア・ディストリビュータが、任意の提出されたデジタルレシートに対して、任意の要求されたキー情報ファイルを提供することが望ましく、異なるメディア・ディストリビュータとタイトルオーナーとの間の限定配信契約により、任意の単一のメディア・ディストリビュータにより配信できるキー情報ファイルの範囲を制限することができる。具体的には、ディストリビュータデータベース267が、クエリーを行うメディア・ディストリビュータの同一性に従って、特定のキー情報ファイルに対するアクセス権を決めることができる。メディア・ディストリビュータ270の場合、これはディストリビュータID271に対応し、ディストリビュータID271は、プロバイダーAPI257によりキー収納箱260との確実な通信を確立する前に、HTTPS又はTLSのハンドシェイキング手続きの一部として、提供することができる。

40

【0041】

さらに、一方では、ユーザは、全てのメディア・ディストリビュータが汎用ファイル240のダウンロードの提供をすることを好むのに、あるいは、自由なメディア・ディストリビュータ用の新たなDRMライセンスの生成により、サーバ及びネットワークのメンテナンスのような費用、消費者サービス及び配信契約も考慮しなければならない。従って、いくつかのメディア・ディストリビュータは、デジタルレシートにより無料の再活性化を提

50

供できるのに、他のメディア・ディストリビュータは、帯域幅、サーバメンテナンス、消費者サポート、並びに配信権及びコンテンツライセンスの取得及び更新の費用をカバーするために、デジタルレシートを清算するための料金を請求することができる。これらの考慮は、CKR、キー収納箱260の中核キーの保存及び配信機能に柔軟に独立して、キー収納箱260により又は個々のメディア・ディストリビュータにより実行される業務ルールの範囲内でカプセル化することができる。

【0042】

図3は、本発明の一実施形態による、異なるDRMシステム間の相互運用のための相互運用キー収納箱により、保護されたデジタル著作権管理(DRM)ライセンスを得るためのシステムを示す。図3の環境300は、キー収納箱360、メディア・ディストリビュータ370a、370b、クライアント380a、380b、共有クライアントID386、共有クライアントID検証サーバ390を含む。キー収納箱360は、キー情報データベース362、消費者データベース363、トランザクションデータベース364、ディストリビュータ公開キーデータベース366、ディストリビュータデータベース367、販売データベース368、プリペアラーデータベース369、及びプロバイダーAPI357を含む。メディア・ディストリビュータ370aはネイティブDRMサーバ372aを含む。メディア・ディストリビュータ370bはネイティブDRMサーバ372bを含む。クライアント380aは、汎用ファイル340、DRMライセンス373a、ネイティブDRMクライアント382aを含む。汎用ファイル340は、タイトルID316、メタデータ317、暗号化タイトル345及びキー収納箱URL346を含む。DRMライセンス373aは、タイトルID316、暗号化タイトルキー374a、クライアントID381を含む。クライアント380bは、汎用ファイル340、DRMライセンス373b、ネイティブDRMクライアント382bを含む。DRMライセンス373bは、タイトルID316、暗号化タイトルキー374b、クライアントID381を含む。なお、図3に関して、キー収納箱360は、図2のキー収納箱260に対応し、メディア・ディストリビュータ370a、370bは、メディア・ディストリビュータ270に対応し、クライアント380a、380bは、クライアント280に対応する。

【0043】

異なるメディア・ディストリビュータ間の相互運用のためのデジタルレシートを用いるコンセプトは、上記の図2でいくらか詳細に説明したが、図3は、異なるメディア・ディストリビュータ間の相互運用の代替方法を示し、たとえ、異なるメディア・ディストリビュータが異なるDRMシステム又はスキーマを用いるとしても、汎用ファイルが、異なるクライアント間で単にコピーされて、新たなクライアントに適用可能な新たなDRMライセンスを得るために、用いられる。

【0044】

例えば、クライアント380aのユーザは、既に汎用ファイル340を購入したと仮定すると、関連するDRMライセンスの取得ももたらす。さらに、購入記録が、購入者のIDである共有クライアントID386を含み、トランザクションデータベース364に記録される。前に論じたように、共有クライアントID386は、開いたID(Open ID)のような同一性スキーマを用いることができる。ネイティブDRMクライアント382a及びネイティブDRMサーバ372aによりサポートされるDRMシステム又はスキーマを用いることにより、クライアント380aクライアント380aのユーザは、クライアント380aで、暗号化タイトル345を、容易に使用し、再生し、楽しむことができる。しかしながら、クライアント380aのユーザは、メディアの使用のための異なるクライアント又は装置を有することができ、いくつかのクライアントは、他のクライアントよりも、ある状況に対してもっと適している。例えば、クライアント380aは、ユーザのパソコンを表わすことができ、一方、クライアント380bは、ユーザのビデオゲーム機器を表わすことができる。例えば、パソコンが、金属性のコンピュータスピーカ及び小さいLCD画面を有する部屋にたまたま追いやられる一方、ビデオゲーム機器が、リビングルーム内の最高級ホームシアターシステムにたまたま接続される場合、ユーザは、クライアント380a

よりも、クライアント380bで汎用ファイル340を見ることを望む。代替的には、ユーザが、ビジネス旅行で飛行中に汎用ファイル340を見たい場合、クライアント380bは、ユーザの携帯メディア装置を表わすことができる。

【0045】

従来技術では、専用のクローズドシステムのDRMフォーマットは、完全な相互運用を妨げる非互換性を導入する傾向があるので、異なるDRMシステムを用いる異なる装置間のメディアファイルの転送は困難又は不可能であった。DRM相互運用の難題に加えて、メディアコンテナフォーマット及び圧縮アルゴリズムは、異なるプラットフォームで再生可能でない保護されないコンテンツさえも、もたらず。

【0046】

しかしながら、図3に示すように、汎用ファイルコンセプトの導入は、デジタルメディア消費者間のこの懸念に主として対処するのに役立つことができる。図3に示すように、汎用ファイル340をクライアント380aから購入後に、クライアント380a及びクライアント380b内の汎用ファイル340の2つのインスタンス間の同一のコンテンツにより証明されるように、汎用ファイル340はクライアント380bにそのまま直接コピーされる。代替的に、汎用ファイル340は、クライアント380bにコピーされる前に、USB記憶装置のような中間の記憶場所に最初にコピーすることができる。DRMライセンス373aは、ネイティブDRMクライアント382a及びネイティブDRMサーバ372aによりサポートされるDRMシステムと共にのみ機能するため、DRMライセンス373aは、クライアント380bには役に立たない。しかしながら、キー収納箱360の支援により、クライアント380bは、クライアント380b及びメディア・ディストリビュータ370bがネイティブDRMサーバ372b及びネイティブDRMクライアント382bによりサポートされる異なるDRMシステムを用いるけれども、メディア・ディストリビュータ370bからDRMライセンス373bを得ることができる。

【0047】

汎用ファイル340を受信後に、クライアント380bは、DRMライセンス373bのために、メディア・ディストリビュータ370bのクエリーを行うことができる。クライアント380bは、ユーザ名及びパスワードのような共有クライアントID386に関連する同定認証情報を提供することもできる。メディア・ディストリビュータ370bは、同定認証情報を共有クライアントID検証サーバ390へ中継することにより、それから、ユーザの同一性を検証することができる。

【0048】

一旦、クライアント380bの同一性が確認されると、メディア・ディストリビュータ370bは、プロバイダーAPI357によりキー収納箱360にクエリーを行うことができ、共有クライアントID386により同定されたユーザが、汎用ファイル340に関連する権利を有するかどうかを確認する。従って、キー収納箱360は、トランザクションデータベース364を調べることができ、共有クライアントID386を用いて同定された同じユーザによる汎用ファイル340の購入を含む、メディア・ディストリビュータ370aとの前の取引の存在を確認する。トランザクションデータベース364が、共有クライアントID386及び汎用ファイル340に関連するマッチング結果がないこと、又は取引の種類が購入ではなく単なるレンタルであることを、代わりにレポートする場合、キー収納箱360は、処理を中断することができ、認可が否認されたことを返すことができる。ディストリビュータデータベース367は、メディア・ディストリビュータ370bが、汎用ファイル340と関係がある関連するキー情報ファイルをキー情報データベース362から配信することの合意に達しているかどうかの決定をすることも調べることができる。さらに、前に論じたように、様々な業務ルールをキー収納箱360により実行することができる。例えば、汎用ファイルの配信乱用を防ぐために、ケースバイケースで消費者サービスにより対処される5つより多い同時に機能するDRMライセンスを必要とするユーザと共に、5つの異なるクライアントの大域的限界を、同定可能なユーザに結び付く任意の単一の購入に対してサポートすることができる。同様に、5つの異なる同一性の

10

20

30

40

50

大域的限界を同一の消費者を同定するためにサポートすることができる。

【0049】

キー収納箱360が、トランザクションデータベース364内の適格取引を確認し、任意のかつ全ての他の業務ルールを満たすと仮定すれば、キー収納箱360は、キー情報データベース362から関係するキー情報ファイルを検索することができ、上記のように、メディア・ディストリビュータ370bの公開キーを用いて、メディア・ディストリビュータ370bに書き換えられたキー情報ファイルを提供する。メディア・ディストリビュータ370bは、それから、書き換えられたキー情報ファイルを用いることができ、ネイティブDRMサーバ372bを用いてDRMライセンス373bを生成し、クライアント380b内のネイティブDRMクライアント382bへDRMライセンス373bを提供する。従って、クライアント380bのユーザは、汎用ファイル340を再びダウンロードしなければならないよりも、もっと小さいダウンロードサイズを有するDRMライセンス373bを検索することにより、汎用ファイル340を使用することができ、最高級ホームシアターシステム又は携帯メディア装置で、ほとんど即時に再生し、ユーザが汎用ファイル340を楽しむことを可能にする。

10

【0050】

代替的に、中間物としてのメディア・ディストリビュータによりデジタルレシートをルーティングする代わりに、クライアント380bは、キー収納箱360が登録したメディアを要求するための直接のクライアントインターフェースを提供する場合、デジタルレシートをキー収納箱360へ直接再送信することができる。個々のキー収納箱は、その自由裁量により、この機能を提供することができる。前に論じたように、デジタルレシートは、取引の証拠として機能し、従って、キー収納箱360へ再送信して戻すことができ、オリジナルのメディア又はオリジナルの取引により許可されたライセンスにアクセスする。キー収納箱360がクライアント380bからのこのような直接の要求をサポートする場合、かつ、キー収納箱360が、上記で詳説したように、クライアント380bが要求された登録メディアにアクセスする特権を与えられていることを確定する場合、キー収納箱360は、クライアント380bを、要求された登録メディアを供給することが可能な適切なメディア・ディストリビュータに向けることができる。

20

【0051】

例えば、キー収納箱360は、ディストリビュータデータベース367を用いて特権のあるメディア・ディストリビュータのリストを最初に確定することができて、例えば汎用ファイル340のような要求された登録メディアに対する配信権又は配信特権を有する全ての第三者メディア・ディストリビュータを見出す。それから、クライアント380bのユーザは、プロバイダーのリストから、特定の第三者メディア・ディストリビュータにリダイレクトされるように、選択することを促される。クライアント380bのユーザが、例えば、メディア・ディストリビュータ370bのような特定の第三者メディア・ディストリビュータにリダイレクトされた後に、キー収納箱360は、メディア・ディストリビュータ370bに、クライアント380bのユーザが、要求された汎用ファイル340及び/又は任意の関係するDRMライセンスを検索することが認証される検証を送ることができる。以前の通り、この検証は、消費者データベース363内の登録デジタルレシートに対し提出されたデジタルレシートを検証すること、及び、任意の適用可能な業務ルールを適用することを含むことができる。その後、あたかもユーザがデジタルレシートをCKRの代わりにメディア・ディストリビュータへ提出するかのよう、プロセスは正常のように続く。従って、メディア・ディストリビュータ370bは、それゆえ、汎用ファイル340を使用するために、DRMライセンス373bをクライアント380bへ提供することができる。

30

40

【0052】

さらに、汎用ファイル340を共同使用し、異なるDRMライセンスを得るプロセスは、関係する汎用ファイルを再ダウンロードする必要はなく、友人及び仲間が推薦したメディアファイルを提供するために、使用することができる。例えば、クライアント380aの

50

ユーザは、多分、USB記憶装置により、クライアント380bのユーザに汎用ファイル340のコピーを提供することができる。しかしながら、クライアント380bは、クライアント380aのユーザの秘密のログイン詳細を知らないため、クライアント380bは、共有クライアントID386用のログイン認証情報を提供できず、クライアント380bのユーザが、コピーした汎用ファイル340のオリジナル購入者のクライアント380aのユーザと同一ではないことを、メディア・ディストリビュータ370bが確認することを可能にする。代わりに、メディア・ディストリビュータ370bは、即時再生のためロック解除する汎用ファイル340用のDRMライセンスを得るために、新たな取引を実行するための販売を表示することができる。さらに、2つの別個のメディア・ディストリビュータを図3に示すけれども、このプロセスは、同一のメディア・ディストリビュータを用いるクライアントにも適用することができる。

10

【0053】

図3に示すように、各メディア・ディストリビュータは、たとえ異なるDRMシステム又はスキーマが用いられようとも、特定のメディアタイトルに対して、厳密に同一の汎用ファイルを提供することができる。主要権利情報センターとしての機能を有するキー収納箱360及びプロバイダーに渡ってユニークなユーザを検証する共有クライアントID検証サーバ390を用いて、メディア・ディストリビュータは、最小の追加の努力及び既存のDRMシステムのリエンジニアリングで、相互運用の解決法を提供することができる。これは、コピーした汎用ファイルを再生するのに必要な新たなDRMライセンスの迅速な検索のみにより、ユーザが異なる装置及びメディア・ディストリビュータ間で汎用ファイルを容易に移植することを可能にする。

20

【0054】

図4aは、本発明の一実施形態による、オリジナルの発行メディア・ディストリビュータと無関係に相互運用キー収納箱を用いて保護メディアを再生するためのシステムを示す。図4aの環境400は、キー収納箱460、メディア・ディストリビュータ470、クライアント480、ディスプレイ488、バックアップ記憶装置489、共有クライアントID検証サーバ490を含む。メディア・ディストリビュータ470は汎用ファイル440及びDRMライセンス473を含む。クライアント480はクライアントメディア・アプリケーション483を含む。バックアップ記憶装置489はデジタルレシート485を含む。なお、図4aに関し、キー収納箱460は図2のキー収納箱260に対応し、メディア・ディストリビュータ470はメディア・ディストリビュータ270に対応し、クライアント480はクライアント280に対応し、バックアップ記憶装置489はバックアップ記憶装置289に対応する。

30

【0055】

前に論じたように、ユーザが、自発的に又は非自発的に、購入した汎用ファイル及び関係するDRMライセンスへのアクセスを失う状況があり得る。自発的喪失は、クライアント装置又はメディア・ディストリビュータの変更を含むことができる。非自発的喪失は、故障したハードディスクドライブのようなハードウェアの突発故障又は間違っただけファイルを削除するようなユーザの誤りを含むことができる。各デジタル取引は、図2に示すように、ユーザ制御下の必須のデジタルレシートを伴うため、ユーザは、オリジナルのメディア・ディストリビュータと無関係に、このような緊急時対応策に完全な自由裁量を有する。例えば、ユーザがデジタルレシートをオンラインで関係するキー収納箱に勤勉に登録し、安全なバックアップに保持する場合、ユーザは、関係する汎用ファイル及びDRMライセンスへのアクセスを取り戻すために、単に、デジタルレシートを再提出する必要がある。

40

【0056】

例えば、クライアント480のユーザが、ハードディスクドライブの突発故障により、損害を被ると仮定する。ユーザは、クライアント480のハードディスクドライブを交換し、メディア・ディストリビュータ470と再びインターフェースで接続するために、クライアントメディア・アプリケーション483を再度インストールする。ハードディスクドライブは汎用ファイルのユーザのメディアライブラリ及びDRMライセンスを保存するた

50

め、クライアント480のユーザは、ユーザの前のメディアライブラリへのアクセスを取り戻すことを求める。幸いなことに、ユーザは、デジタルレシートのコピーをバックアップ記憶装置489内に保持し、バックアップ記憶装置489は、前に論じたように、USB記憶装置又はオンライン電子メールプロバイダーを含むことができる。さらに、図4aに示すように、ユーザは、デジタルレシート485がキー収納箱460のユーザ認証データベース内に保存することができるように、デジタルレシート485をオンラインでキー収納箱460に登録した。

【0057】

従って、クライアント480のユーザは、メディア・ディストリビュータ470で検証するためのユーザ認証情報と共に、又は代替的に、共有クライアントID検証サーバ490で検証するための共有ユーザ認証情報と共に、バックアップ記憶装置489から検索されたデジタルレシート485をメディア・ディストリビュータ470へ、提供するにすぎない。メディア・ディストリビュータ470は、キー収納箱460と情報を交換後、汎用ファイル440及びDRMライセンス473をクライアント480へ提供して戻すことができる。さらに、メディア・ディストリビュータ470は、クライアント480により提供され、メディア・ディストリビュータ470又は共有クライアントID検証サーバ490により正当に検証されたユーザ認証情報にマッチングする、キー収納箱460内の適切に登録されたデジタルレシートを有する任意の他の汎用ファイル及びDRMライセンスのバッチ転送も提供することができる。このバッチ転送は、ハードウェアの突発故障後の場合である、いくつかのデジタルレシートを提出しなければならない場合に、ユーザにかなりの時間及び労力を省くことができる。いくつかの業務ルールがこのモデルに関与して、乱用の可能性に取り組み、システムが適切に機能することを確保し、又は、追加のサービスを消費者に提供する。

【0058】

さらに、この同じ機構が、お気に入りのメディア・ディストリビュータの故障又は再構成に対して一種の保護手段をユーザに提供することができる。例えば、クライアント480が、通常、ひいきにしているメディア・ディストリビュータが、突然、廃業した場合、クライアント480のユーザは、デジタルレシートのバックアップを保持し、デジタルレシートをキー収納箱460に登録している限り、ユーザは、図4aのメディア・ディストリビュータ470のような別のメディア・ディストリビュータに容易に移動することができる。このようにして、DRMで保護されるデジタルメディアの永続性に関する多くの長年のユーザの懸念は、有効に解決することができる。

【0059】

図4bは、本発明の一実施形態による、相互運用キー収納箱を用いて二次保護メディアを取り戻すためのシステムを示す。図4bの環境400は、キー収納箱460、メディア・ディストリビュータ470、クライアント480a、480b、ディスプレイ488a、488b、メディアディスク491、メディアボックスコード492を含む。メディア・ディストリビュータ470は汎用ファイル440b及びDRMライセンス473a、473bを含む。クライアント480aはクライアントメディア・アプリケーション483aを含む。メディアディスク491は汎用ファイル440aを含む。なお、図4bに関し、キー収納箱460は図2のキー収納箱260に対応し、メディア・ディストリビュータ470はメディア・ディストリビュータ270に対応し、クライアント480a、480bはクライアント280に対応し、ディスプレイ488a、488bはディスプレイ288に対応する。

【0060】

これまでの汎用ファイルの議論は、一般的にオンラインデジタル配信に制限されてきたけれども、汎用ファイルは、物理的小売りメディアをもつアプリケーションも同様に有することができる。例えば、メディアディスク491は、小売りチャンネルにより購入したブルーレイ・ディスクを含むことができる。標準ブルーレイ動画データを保存することの他に、対応する汎用ファイルは、パソコンで使用するため、又は携帯メディア装置用にも

10

20

30

40

50

含むことができる。メディアボックスコード492は、内張り又は隠しスクラッチパネル内にプリントされたユニークな数字又は英数字の列を含むことができ、それらを、適用可能なDRMライセンスを検索することにより、再生用に汎用ファイル440aを取り戻すために用いることができる。この意味で、キー収納箱460は、業務ルールを用いる任意の単一のメディアボックスコードに対する、取り戻し数を制限することができるので、メディアボックスコード492は、匿名のユーザ識別子として機能することができる。

【0061】

従って、ノートブックパソコンであるクライアント480aのユーザは、メディアディスク491をブルーレイ・ディスクドライブに入れることができ、そこで、ユーザは、汎用ファイル440aを取り戻すかどうか促される。ユーザが「ハイ」と答えるならば、ユーザは、メディアボックスコード492に入力することを促され、その入力、汎用ファイル440aに含まれる任意の識別メタデータと共にメディア・ディストリビュータ470へ送られる。それから、メディア・ディストリビュータ470は、メディアボックスコード492が有効かどうか、及び/又は、メディアボックスコード492が取り戻し数の最大値に達したかどうかを確認するために、キー収納箱460と情報を交換することができる。例えば、キー収納箱460での業務ルールは、各有効なメディアボックスコードが最大3回の取り戻し数のみ設けることができ、無差別の汎用ファイルの共用の乱用の可能性を防ぐことができる。キー収納箱460が肯定的に答えるならば、メディア・ディストリビュータ470は、DRMライセンス473aを提供することができ、クライアント480aのユーザは、映画をノートブックパソコンのディスプレイ488aで、最大解像度で見ることができる。

【0062】

さらに、メディアディスク491の強力なセールスポイントは、映画をメディアディスク491から様々な携帯装置へコピーする機能を含むことである。従って、クライアント480aは、標準解像度ディスプレイの携帯装置で再生するため、映画の標準解像度(SD)720x480版をさらに要求することができる。同じメディアボックスコード492及び汎用ファイル440aからの同じメタデータを用いて、メディア・ディストリビュータ470は、キー収納箱460に、携帯装置用の特別な標準解像度版のキーファイルのクエリーを行うことができ、そのキーファイルは正当に戻されて汎用ファイル440b及びDRMライセンス473bを生成するために用いられ、それらは、クライアント480bへ送られてディスプレイ488bで、再生することができる。その上、ボックスコードの取り戻しは、クライアント又は消費者IDに関係付けることができ、前にオンライン取引で行ったように、キー収納箱460の関連データベース内に記録することができる。代替的に、一般のメディア装置用に既にフォーマットされた様々な汎用ファイルを、対応するDRMライセンスのみがダウンロード時間を減少して検索される必要があるように、メディアディスク491に埋め込むことができる。

【0063】

図5は、コンテンツに関係するデジタルレシートのオンライン登録がキー集中収納場所(CKR)を用いて使用でき、最初のディストリビュータとは無関係に、コンテンツの相互運用再生を可能にする、本発明の一実施形態によるステップを説明するフローチャートを示す。当業者に明らかなある種の詳細及び特徴は、フローチャート500から省略してある。例えば、ステップは、従来技術で知られるように、1つ以上のサブステップを含むことができ、特別な装置及び材料を含むことができる。フローチャート500に示すステップ510から570は、本発明の一実施形態を説明するのに十分であるが、本発明の他の実施形態は、フローチャート500に示すものと異なるステップを用いることができる。

【0064】

図5のフローチャート500のステップ510及び図5の環境200を参照するに、フローチャート500のステップ510は、クライアント280が、暗号化タイトルキー274の非暗号化バージョンに対応するタイトルキー、すなわち、図1のタイトルキー132により暗号化された暗号化タイトル245を含む汎用ファイル240、及び、暗号化タ

10

20

30

40

50

イトルキー 274 の非暗号化バージョンにアクセスするために、メディア・ディストリビュータ 270 と共に使用できる DRM ライセンス 273 を、メディア・ディストリビュータ 270 から得るために、取引を実行することを含む。この手続きは、既にいくらか詳細に、しかし、簡潔に論じたが、クライアント 280 は、クライアント・メディア・アプリケーション 283 を用い、デジタル店頭をブラウズし、取引を開始するため汎用ファイル 240 を選択する。それに応じて、メディア・ディストリビュータ 270 は、キー収納箱 260、ネイティブ DRM サーバ 272 及びネイティブ DRM クライアント 282 と情報をやりとりすることにより、汎用ファイル 240 及び関係する DRM ライセンス 273 を、クライアント 280 へ提供する。

【0065】

10

図 5 のフローチャート 500 のステップ 520 及び図 5 の環境 200 を参照するに、フローチャート 500 のステップ 520 は、クライアント 280 が、暗号化タイトル 245 に関係するデジタルレシート 285 を受信し、デジタルレシート 285 は、ステップ 510 の取引に関連する情報を含むことを含む。図 2 に示すように、この情報は、クライアント ID 281、ディストリビュータ ID 271、共有クライアント ID 286、消費者 ID 284、タイトル ID 216 及びトランザクション情報 287 を含むが、代替の実施形態は、他のデータ配置を用いることができる。さらに、図 2 に示すように、デジタルレシート 285 の部分は、キー収納箱 260 の公開キーにより暗号化されて提供される。

【0066】

20

図 5 のフローチャート 500 のステップ 530 及び図 2 の環境 200 を参照するに、フローチャート 500 のステップ 530 は、クライアント 280 が、デジタルレシート 285 を消費者データベース 263 内にオンライン登録するために、ステップ 520 で受信したデジタルレシート 285 をキー収納箱 260 へ送信することを含む。図 2 に示すように、クライアント 280 は、キー収納箱 260 のクライアント API 256 を用いてデジタルレシート 285 を転送し、HTTPS による SOAP によりアクセスできるウェブサービスをさらすことができる。

【0067】

30

図 5 のフローチャート 500 のステップ 540 及び図 4 a の環境 400 を参照するに、フローチャート 500 のステップ 540 は、クライアント 480 が、ステップ 510 で検索した DRM ライセンス 273 に対応する DRM ライセンス 473 にアクセスする権利を失うことを含む。前に論じたように、これは、メディア・ディストリビュータ又はクライアントの変更による自発的失権であり得るが、又は、例えば、データ損失をもたらすハードウェア故障による非自発的失権であり得る。どちらの場合も、クライアント 480 は、ステップ 540 の後では、もはや直接、DRM ライセンス 473 にアクセスしない。しかしながら、クライアント 480 は、図 4 a に示すアクセス状態に反して、ステップ 510 で検索した汎用ファイル 240 に対応する汎用ファイル 440 への直接アクセスをなお、保有することができる。

【0068】

40

図 5 のフローチャート 500 のステップ 550 及び図 4 a の環境 400 を参照するに、フローチャート 500 のステップ 550 は、クライアント 480 が、デジタルレシート 485 をメディア・ディストリビュータ 470 へ送信し、デジタルレシート 485 がステップ 520 で検索したデジタルレシート 285 に対応し、メディア・ディストリビュータ 470 が、ステップ 510 ~ 520 の間にアクセスしたメディア・ディストリビュータ 270 とは異なる構成要素であることを含む。ステップ 550 の後、メディア・ディストリビュータ 470 は、同じデジタルレシート 485 のオンライン登録の事前の証拠のため、キー収納箱 460 にクエリーを行うことにより、デジタルレシート 485 の妥当性を注意深く調べることができる。キー収納箱 460 は、新たな DRM ライセンスを生成するための関連するキー情報ファイルを提供する前に、様々な業務ルールも適用することができる。

【0069】

50

図 5 のフローチャート 500 のステップ 560 及び図 4 a の環境 400 を参照するに、

フローチャート500のステップ560は、クライアント480が、汎用ファイル440の復号用のタイトルキーにアクセスするために、メディア・ディストリビュータ470と共に使用できるDRMライセンス473を、メディア・ディストリビュータ470から受信し、そのタイトルキーが、暗号化タイトル245用にステップ510で用いたタイトルキーと同じであることを含む。前に論じたように、ステップ550の後、ステップ560を進めることができるように、関連するキー情報ファイルを提供する前に、クライアント480の同一性、メディア・ディストリビュータ470の認証、及び任意の適用可能な業務ルールも検証することができる。

【0070】

図5のフローチャート500のステップ570及び図4aの環境400を参照するに、フローチャート500のステップ570は、クライアント480のクライアントメディア・アプリケーション483が、ステップ560のメディア・ディストリビュータ470から受信したDRMライセンス473を用いることにより得たタイトルキーを用いて復号した汎用ファイル440の再生をディスプレイ488に起動することを含む。ステップ560の最後で、クライアント480は、汎用ファイル440及びDRMライセンス473の両方にアクセスするので、クライアント480は、汎用ファイル440内の暗号化タイトルを復号するためDRMライセンス473に埋め込まれたタイトルキーにアクセスするために、クライアントメディア・アプリケーション483及びメディア・ディストリビュータ470により実装されたネイティブDRM解決手段を用いれば十分であり、汎用ファイル440は、クライアント480のユーザが見るために、使用されてディスプレイ488へ出力される。

【0071】

図6は、メディアコンテンツがメディア・ディストリビュータに配信される、本発明の一実施形態によるステップを説明するフローチャートを示す。当業者に明らかなある種の詳細及び特徴は、フローチャート600から省略してある。例えば、ステップは、従来技術で知られるように、1つ以上のサブステップを含むことができ、特別の装置及び材料を含むことができる。フローチャート600に示すステップ610から670は、本発明の一実施形態を説明するのに十分であるが、本発明の他の実施形態は、フローチャート600に示すものと異なるステップを用いることができる。

【0072】

図6のフローチャート600のステップ610及び図1の環境100を参照するに、フローチャート600のステップ610は、プリペアラ－130の汎用ファイルパッケージ135が、第1のキーであるキー収納箱公開キー122、第2のキーであるタイトルキー132及びタイトル115を得ることを含む。図1に示すように、キー収納箱公開キー122は、信頼できる第三者である認証オーソリティ120から検索され、認可証121は、キー収納箱公開キー122とキー収納箱160との間の結合を認証するために用いられる。しかしながら、標準公開キー基盤(PKI)付きアプローチ又は標準公開キー基盤(PKI)の無いアプローチも用いることができる。プリペアラ－130自体が、キー・ジェネレータ131を用いてタイトルキー132を生成することができる。タイトル115は、デジタル又は物理的手段により、しっかりと検索することができるタイトルオーナー110から検索される。前記のように、タイトルオーナー110は、プリペアラ－130と同じ構成要素により所有されることも可能である。

【0073】

図6のフローチャート600のステップ620及び図1の環境100を参照するに、フローチャート600のステップ620は、プリペアラ－130の汎用ファイルパッケージ135が、ステップ610で得たキー収納箱公開キー122を用いて、ステップ610で得たタイトルキー132を暗号化して暗号化タイトルキー152を生成することを含む。暗号化タイトルキー152は、キー収納箱秘密キー165を用いてのみ復号することができるため、キー収納箱160がキー収納箱秘密キー165の秘密を保護する限り、キー収納箱160のみが暗号化タイトルキー152からタイトルキー132にアクセスするこ

とができる。前に論じたように、公開キー暗号化基準 # 1 (PKCS # 1) に従って、2048ビットのRSAキーを、ステップ620の非対称のキーの暗号化のために用いることができる。

【0074】

図6のフローチャート600のステップ630及び図1の環境100を参照するに、フローチャート600のステップ630は、プリペアラ-130の汎用ファイルパッケージ135が、ステップ610で得たタイトルキー132を用いて、ステップ610で得たタイトル115を暗号化して暗号化タイトル145を生成することを含む。前に論じたように、ステップ630の対称キーの暗号化用に、エ-イ-エス(AES)のようなバランスのとれた妥協を用いることができ、速い復号時間を有する合理的に強いセキュリ

10

【0075】

図6のフローチャート600のステップ640及び図1の環境100を参照するに、フローチャート600のステップ640は、プリペアラ-130の汎用ファイルパッケージ135が、ステップ620で生成した暗号化タイトルキー152を含むキー情報ファイル150を生成することを含む。図1に示すように、キー情報ファイル150は、キー情報データベース162内のキー情報ファイル150の索引付け及び検索に役立つために、様々なメタデータ並びにタイトルオーナーID111及びタイトルID116のような同定情報も含むことができる。

【0076】

20

図6のフローチャート600のステップ650及び図1の環境100を参照するに、フローチャート600のステップ650は、プリペアラ-130の汎用ファイルパッケージ135が、ステップ630で生成した暗号化タイトル145及びキー集中収納場所(CKR)であるキー収納箱160用のキー収納箱URL146を含む汎用ファイル140を生成することを含む。キー収納箱URL146は、キー収納箱160を指し示すネットワークアドレスを表わし、前に論じたように、リダイレクトサーバも中間物として用いることができる。図1は、ウェブベースのHTTPSによるSOAPとインターフェースをとるためのネットワークアドレスとしてURLを用いるけれども、代替の実施形態は、確実な方法でネットワークアドレスに達する他のプロトコルを用いることができる。汎用ファイル140で示すように、汎用ファイル140の同定及びカタログ作成に役立つために、タイトルID116及びメタデータ117のような追加のメタデータ及び同定情報も、汎用ファイル140内に含むことができる。

30

【0077】

図6のフローチャート600のステップ660及び図1の環境100を参照するに、フローチャート600のステップ660は、プリペアラ-130の汎用ファイルパッケージ135が、キー収納箱160のキー情報データベース162に保存するためのキー情報ファイル150を提供することを含む。図1に示すように、これは、キー収納箱160のプリペアラ-API161によるHTTPSによりさらされるSOAPウェブベースを用いることによりできる。キー収納箱160が、プリペアラ-130を認証プリペアラ-として認証を行い、キー情報ファイル150を受け入れた後に、キー情報ファイル150は、メディア・ディストリビュータによる今後の検索用にキー情報データベース162内に保存することができ、キー情報ファイル150は、検索するメディア・ディストリビュータに対応するディストリビュータ公開キーデータベース166を用いることにより、書き換えられた形で準備される。この場合、各メディア・ディストリビュータは、自体の秘密/公開キー対を生成し、公開キーをキー収納箱160へ配信するが、前に論じたように、キー収納箱160も、秘密/公開キー対を生成し、公開キーをメディア・ディストリビュータへ配信することができる。

40

【0078】

図6のフローチャート600のステップ670及び図1の環境100を参照するに、フローチャート600のステップ670は、プリペアラ-130の汎用ファイルパッケージ

50

ャ135が、汎用ファイル140をメディア・ディストリビュータ170へ提供することを含む。ステップ670の前には、両当事者の間に適切な配信の配置が存在すべきである。もっと具体的に言えば、メディア・ディストリビュータ170は、タイトル115を配信する合意をタイトルオーナー110から得るべきであり、キー収納箱160のディストリビュータデータベース167は、メディア・ディストリビュータ170がキー収納箱160から対応するキー情報ファイル150にアクセスすることの許可を与えるべきである。単一のメディア・ディストリビュータのみが図1に示されるけれども、代替の実施形態では、タイトルオーナー110は、いくつかのメディア・ディストリビュータが、プリペアラーにより生成された汎用ファイルを各異なるメディア・ディストリビュータへ送信することの合意を得ることができる。タイトル115をプリペアラー130へ提供するタイトルオーナー110と同様に、汎用ファイル140は、物理的に又はデジタルに、任意の適切な確実な通信方法で、メディア・ディストリビュータ170へ提供することができる。一旦、汎用ファイル140がメディア・ディストリビュータ170のような認証されたメディア・ディストリビュータへ配信されると、汎用ファイル140は、デジタル店舗又は他の提示方法により、クライアント又はユーザに要求するのに役立つことができる。

10

【0079】

図7は、キー集中収納場所(CKR)がコンテンツのアクセスの認可をメディア・ディストリビュータに提供することができる、本発明の一実施形態によるステップを説明するフローチャートを示す。当業者に明らかなある種の詳細及び特徴は、フローチャート700から省略してある。例えば、ステップは、従来技術で知られるように、1つ以上のサブステップを含むことができ、特別の装置及び材料を含むことができる。フローチャート700に示すステップ710から750は、本発明の一実施形態を説明するのに十分であるが、本発明の他の実施形態は、フローチャート700に示すものと異なるステップを用いることができる。

20

【0080】

図7のフローチャート700のステップ710及び図1の環境100を参照するに、フローチャート700のステップ710は、キー収納箱160が、暗号化タイトルキー152、タイトルID116及びタイトルオーナーID111を含むキー情報ファイル150を受信することを含む。図1に示すように、ステップ710は、プリペアラー130による使用のためのプリペアラーAPI161により、HTTPSによるSOAPウェブベースをさらすことにより、達成することができる。一旦、キー収納箱160が、キー情報ファイル150を受信すると、メディア・ディストリビュータによる今後の検索のために、キー収納箱160は、キー情報データベース162内にキー情報ファイル150のカタログを作ることができる。

30

【0081】

図7のフローチャート700のステップ720及び図1の環境100を参照するに、フローチャート700のステップ720は、キー収納箱160が、ステップ710で受信したキー情報ファイル150内の暗号化タイトルキー152を、キー収納箱秘密キー165を用いて復号してタイトルキー132を取り戻すことを含む。暗号化タイトルキー152は、キー収納箱公開キー122を用いて暗号化されたため、キー収納箱160は、キー収納箱160が既に復号用にメモリ159内に有するキー収納箱秘密キー165を用いれば十分である。

40

【0082】

図7のフローチャート700のステップ730及び図1の環境100を参照するに、フローチャート700のステップ730は、キー収納箱160が、タイトルID116を含むキー要求をメディア・ディストリビュータ170から受信することを含む。例えば、メディア・ディストリビュータ170は、汎用ファイル140を供給する要求をクライアントから受信する。しかしながら、汎用ファイル140を再生することができるために、キー情報ファイル150も復号する必要がある。汎用ファイル140は、タイトルID116を含むので、メディア・ディストリビュータ170は、クライアントからの要求を満た

50

すために、キー収納箱 160 からのタイトル ID 116 にマッチするキー情報ファイルを要求することができる。

【0083】

図7のフローチャート700のステップ740、図1の環境100及び図2の環境200を参照するに、フローチャート700のステップ740は、キー収納箱160が、ステップ720で復号したタイトルキー132を、ディストリビュータ公開キーデータベース166に保存されたプロバイダーの公開キーを用いて暗号化して、書き換えられたキー情報ファイル251の暗号化タイトルキー252を生成することを含み、プロバイダーの公開キーは、ディストリビュータ秘密キー175を含む秘密/公開非対称キー対の公開部分に対応する。このプロバイダーの公開キーは、認証オーソリティ120のような信頼できる第三者により前もってキー収納箱160へ提供されている。ステップ740は、図2の書き換えられたキー情報ファイル251に対応する書き換えられたキー情報ファイル151へ、キー情報ファイル150を「書き換える」。本明細書で用いる用語「書き換える」は、ディストリビュータ秘密キー275を有する関連のメディア・ディストリビュータ270のみが、書き換えられたキー情報ファイル251からオリジナルのタイトルキー132にアクセスすることができるように、暗号化タイトルキー152としてキー収納箱公開キー122により暗号化されることから、暗号化タイトルキー252としてプロバイダーの公開キーにより暗号化されることへ、タイトルキー132が移行するという意味である。

10

【0084】

図7のフローチャート700のステップ750及び図1の環境100を参照するに、フローチャート700のステップ750は、キー収納箱160が、キー要求を受信するステップ730に回答して、書き換えられたキー情報ファイル151内に含まれる暗号化タイトルキーに対応するステップ740で生成した暗号化タイトルキー252を、メディア・ディストリビュータ170へ送信することを含む。ステップ750の後、メディア・ディストリビュータ170は、ネイティブDRMシステム172内で汎用ファイル140のアクセス及び再生ができるように統合するため、オリジナルのタイトルキー132にアクセスするために、ディストリビュータ秘密キー175を用いることができる。

20

【0085】

図8は、メディア・ディストリビュータが、キー集中収納場所(CKR)からのコンテンツのアクセスの認可へのアクセスを得ることができる、本発明の一実施形態によるステップを説明するフローチャートを示す。当業者に明らかなある種の詳細及び特徴は、フローチャート800から省略してある。例えば、ステップは、従来技術で知られるように、1つ以上のサブステップを含むことができ、特別の装置及び材料を含むことができる。フローチャート800に示すステップ810から850は、本発明の一実施形態を説明するのに十分であるが、本発明の他の実施形態は、フローチャート800に示すものと異なるステップを用いることができる。

30

【0086】

図8のフローチャート800のステップ810及び図2の環境200を参照するに、フローチャート800のステップ810は、メディア・ディストリビュータ270が、汎用ファイル240内の暗号化タイトル245にアクセスするため、タイトルID216を含むクライアント280からのユーザ要求を受信することを含む。例えば、クライアント・メディア・アプリケーション283は、電子商取引店舗をクライアント280のユーザに示すために、メディア・ディストリビュータ270と通信することができる。クライアント280のユーザは、電子商取引店舗をブラウズすることができ、タイトルID216又は汎用ファイル240内の暗号化タイトル245により同定されるデジタルメディアを見るためのライセンスを購入する契約を有効とすることができる。この契約は、それから、ユーザ要求として、メディア・ディストリビュータ270に送信するために、送られる。

40

【0087】

図8のフローチャート800のステップ820及び図2の環境200を参照するに、フ

50

ローチャート800のステップ820は、メディア・ディストリビュータ270が、ステップ810に 응답して、タイトルID216を含むキー要求をキー収納箱260に送信することを含む。プロバイダーAPI257を用いることにより、メディア・ディストリビュータ270は、タイトルID216に対応するキー情報ファイルのキー要求をキー収納箱260に送信することができる。クライアントAPI256と同様に、プロバイダーAPI257は、HTTPS上のSOAPによるウェブサービスにより、外部へさらすことができる。

【0088】

図8のフローチャート800のステップ830及び図2の環境200を参照するに、ローチャート800のステップ830は、メディア・ディストリビュータ270が、ステップ820に 응답して、暗号化タイトルキー252を含む書き換えられたキー情報ファイル251を受信することを含む。書き換えられたキー情報ファイル251は、ステップ820で確立した同じ確実な接続を用いて受信することができる。書き換えられたキー情報ファイル251内の暗号化タイトルキー252は、メディア・ディストリビュータ270の公開キーを用いて暗号化されるので、ディストリビュータ秘密キー275は、暗号化タイトルキー252を復号するために、直ちに、用いることができる。

10

【0089】

図8のフローチャート800のステップ840及び図2の環境200を参照するに、ローチャート800のステップ840は、メディア・ディストリビュータ270が、ステップ830で受信した書き換えられたキー情報ファイル251の暗号化タイトルキー252を復号し、図1のタイトルキー132に対応するタイトルキーを取り戻すことを含む。このタイトルキーは、汎用ファイル240内のタイトルID216に関する暗号化タイトル245を復号するために、最終的に用いることができる。

20

【0090】

図8のフローチャート800のステップ850及び図2の環境200を参照するに、ローチャート800のステップ850は、メディア・ディストリビュータ270が、汎用ファイル240の暗号化タイトル245用のDRMライセンス273をクライアント280に提供することを含み、DRMライセンス273は、ステップ840のタイトルキーをネイティブDRMサーバ272により保護される暗号化タイトルキー274として用いる。ステップ850は、ステップ810に 응답して起動され、ネイティブDRMクライアント282を用いてDRMライセンス273から取り戻し可能なステップ840のタイトルキーを用いて、暗号化タイトル245を復号するクライアント280により使用される。クライアント280がDRMライセンス273を受信後、クライアント280は、ネイティブDRMクライアント282を用いて、暗号化タイトルキー274からの保護を取り除くことができ、ステップ840のタイトルキーにアクセスして汎用ファイル240内の暗号化タイトル245を復号する。復号後、クライアント280は、例えば、クライアント280のユーザがステップ810で要求したコンテンツを楽しむことができるように、復号したコンテンツを、ディスプレイ288で再生するために、保護されたメディアパス復号エンジン299に向けることができる。

30

【0091】

本発明の上記の記載から、本発明の範囲から逸脱することなく、本発明の概念を実施するために、様々な技術を使用できることは明白である。更に、本発明を特定の実施形態を特別に参照して説明したが、本発明の精神及び範囲から逸脱することなく、形式及び細部を変更できることを当業者は認めるであろう。そのようなものとして、記載された実施形態は、全ての点において、例示的であり、限定的でないとして考慮されるべきである。本発明は、ここに記載された特定の実施形態に限定されず、本発明の範囲から逸脱することなく、多くの再配置、修正及び置換ができる。

40

【符号の説明】

【0092】

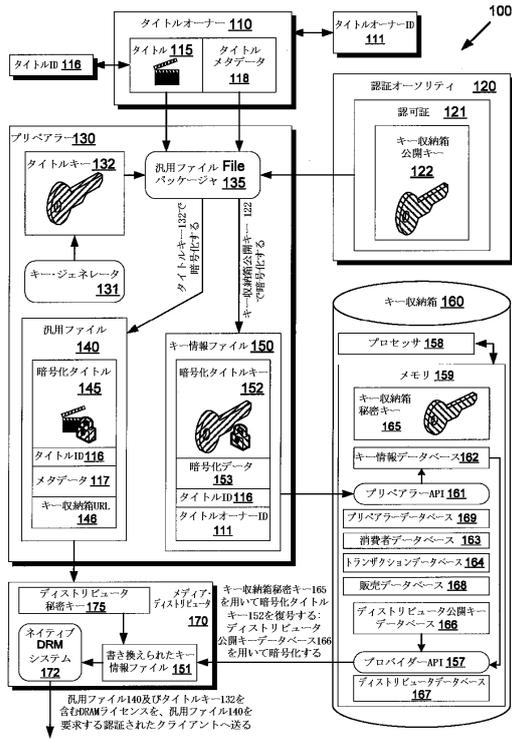
110 タイトルオーナー

50

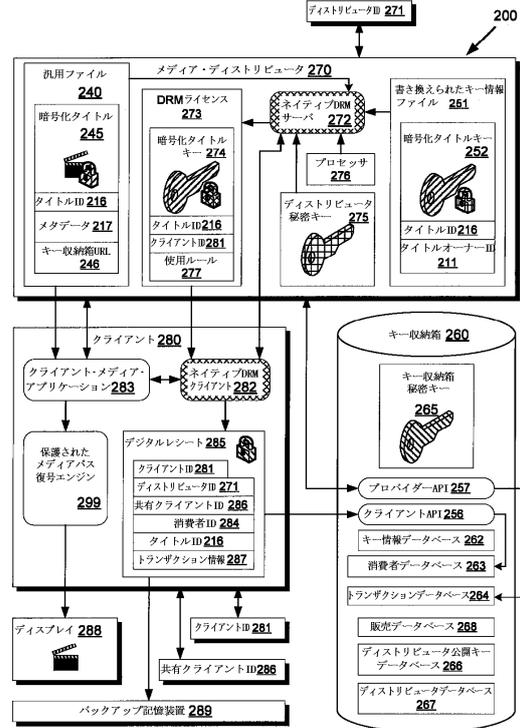
1 1 1、 2 1 1	タイトルオーナー I D	
1 1 5	タイトル	
1 1 6、 2 1 6、 3 1 6	タイトル I D	
1 1 7、 2 1 7、 3 1 7	メタデータ	
1 1 8	タイトルメタデータ	
1 2 0	認証オーソリティ	
1 2 1	認可証	
1 2 2	キー収納箱公開キー	
1 3 0	プリペアラー	
1 3 1	キー・ジェネレータ	10
1 3 2	タイトルキー	
1 3 5	汎用ファイルパッケージ	
1 4 0、 2 4 0、 3 4 0、 4 4 0	汎用ファイル	
1 4 5、 2 4 5、 3 4 5	暗号化タイトル	
1 4 6、 2 4 6、 3 4 6	キー収納箱 URL	
1 5 0	キー情報ファイル	
1 5 1、 2 5 1	書き換えられたキー情報ファイル	
1 5 2、 2 5 2	暗号化タイトルキー	
1 5 3	暗号化データ	
1 5 7	プロバイダー A P I	20
1 5 8	プロセッサ	
1 5 9	メモリ	
1 6 0、 2 6 0、 3 6 0、 4 6 0	キー収納箱	
1 6 1	プリペアラー A P I	
1 6 2	キー情報データベース	
1 6 3	消費者データベース	
1 6 4	トランザクションデータベース	
1 6 5、 2 6 5	キー収納箱秘密キー	
1 6 6	ディストリビュータ公開キーデータベース	
1 6 7	ディストリビュータデータベース	30
1 6 8	販売データベース	
1 6 9	プリペアラーデータベース	
1 7 0	メディア・ディストリビュータ	
1 7 2	ネイティブDRMシステム	
1 7 5	ディストリビュータ秘密キー	
2 5 6	クライアント A P I	
2 5 7	プロバイダー A P I	
2 6 2	キー情報データベース	
2 6 3	消費者データベース	
2 6 4	トランザクションデータベース	40
2 6 6	ディストリビュータ公開キーデータベース	
2 6 7	ディストリビュータデータベース	
2 6 8	販売データベース	
2 7 0、 3 7 0 a、 3 7 0 b、 4 7 0	メディア・ディストリビュータ	
2 7 1	ディストリビュータ I D	
2 7 2、 3 7 2 a、 3 7 2 b	ネイティブDRMサーバ	
2 7 3、 3 7 3 a、 3 7 3 b、 4 7 3	DRMライセンス	
2 7 4、 3 7 4 a、 3 7 4 b	暗号化タイトルキー	
2 7 5	ディストリビュータ秘密キー	
2 7 6	プロセッサ	50

2 7 7	使用ルール	
2 8 0、3 8 0 a、3 8 0 b、4 8 0	クライアント	
2 8 1、3 8 1	クライアント I D	
2 8 2、3 8 2 a、3 8 2 b	ネイティブDRMクライアント	
2 8 3、4 8 3、4 8 3 a	クライアント・メディア・アプリケーション	
2 8 4	消費者 I D	
2 8 5	デジタルレシート	
2 8 6、3 8 6	共有クライアント I D	
2 8 7	トランザクション情報	
2 8 8、4 8 8	ディスプレイ	10
2 8 9、4 8 9	バックアップ記憶装置	
2 9 9	保護されたメディアパス復号エンジン	
3 6 2	キー情報データベース	
3 6 3	消費者データベース	
3 6 4	トランザクションデータベース	
3 6 8	販売データベース	
3 6 6	ディストリビュータ公開キーデータベース	
3 6 7	ディストリビュータデータベース	
3 6 9	プリペアラーデータベース	
3 5 7	プロバイダー A P I	20
3 9 0、4 9 0	共有クライアント I D 検証サーバ	
4 4 0 a	汎用ファイル (HD)	
4 4 0 b	汎用ファイル (SD)	
4 7 3 a	DRMライセンス (HD)	
4 7 3 b	DRMライセンス (SD)	
4 8 0 a	クライアント (ノートブックパソコン)	
4 8 0 b	クライアント (携帯メディアプレイヤー)	
4 8 5	保護デジタルレシート	
4 8 8 a	ディスプレイ (HD 1280 x 720)	
4 8 8 b	ディスプレイ (SD 720 x 480)	30
4 9 1	メディアディスク	
4 9 2	メディアボックスコード	

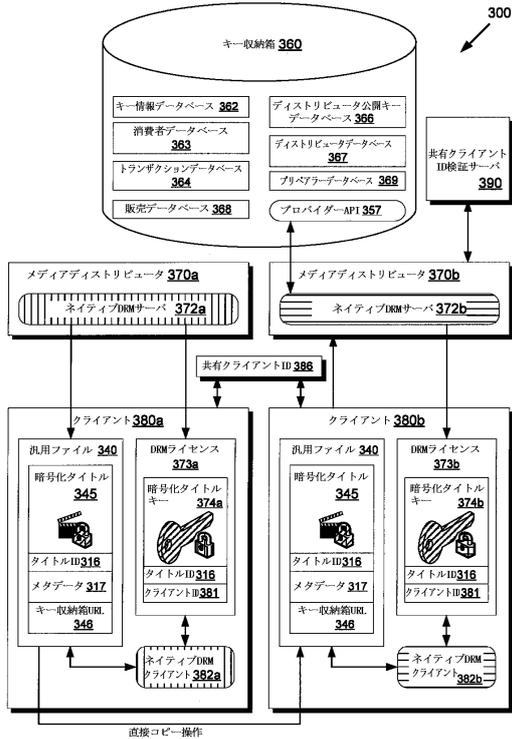
【図1】



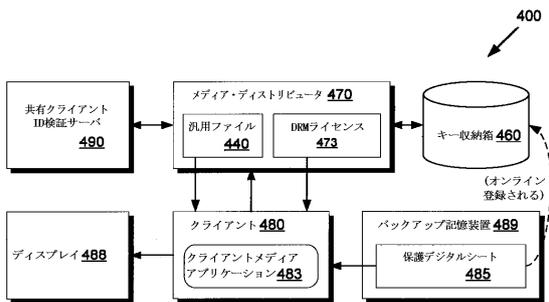
【図2】



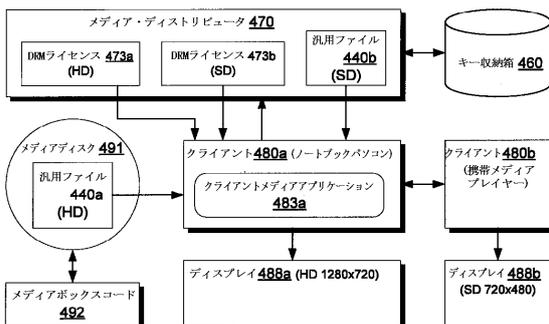
【図3】



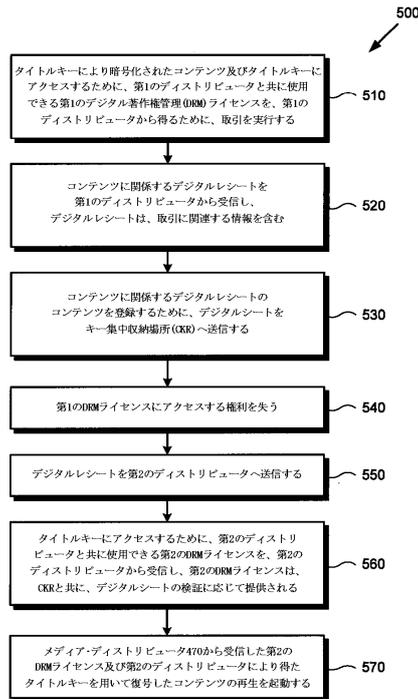
【図4a】



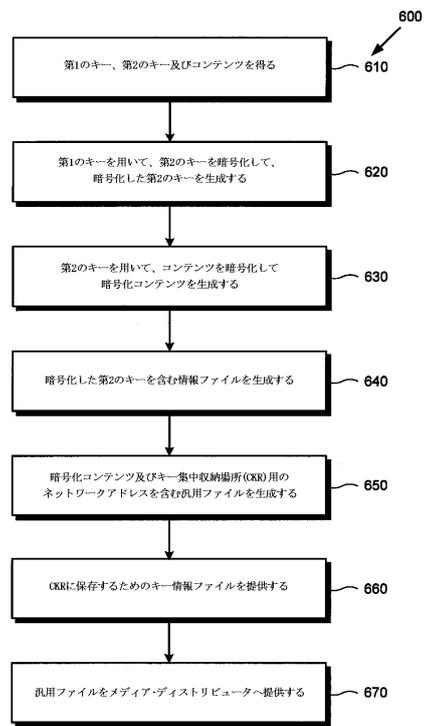
【図4b】



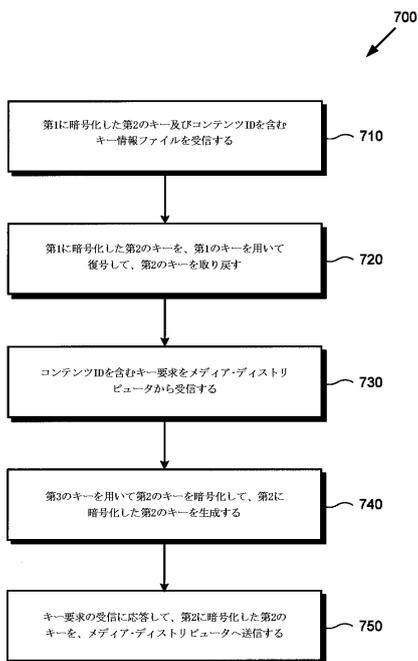
【図5】



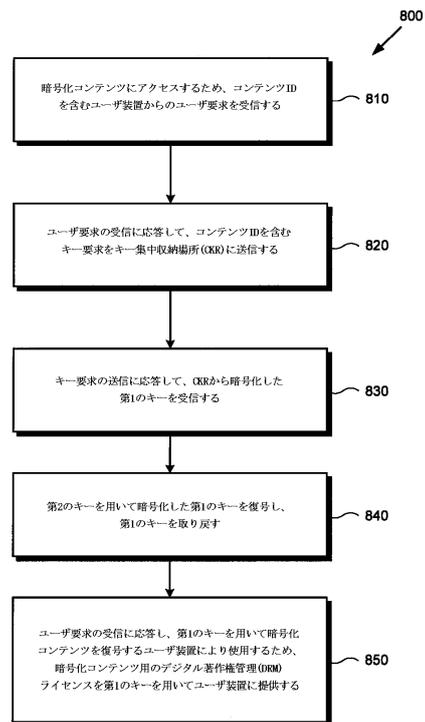
【図6】



【図7】



【図8】



フロントページの続き

- (31)優先権主張番号 12/460,002
(32)優先日 平成21年7月10日(2009.7.10)
(33)優先権主張国 米国(US)
(31)優先権主張番号 12/460,004
(32)優先日 平成21年7月10日(2009.7.10)
(33)優先権主張国 米国(US)

(72)発明者 スコット エフ ワットソン
アメリカ合衆国 カリフォルニア州 90292 マリーナ デル レイ イーストウィンド 6
ナンバー 310

審査官 和田 財太

- (56)参考文献 鈴木裕利(外2名), ネットワーク上の電子的著作権管理システム(ECMS)の構造のモデル化と特徴分析, 情報処理学会研究報告(99 - EIP - 4), 日本, 社団法人情報処理学会, 1999年 5月22日, Vol. 99, No. 46, p. 9 - p. 16

- (58)調査した分野(Int.Cl., DB名)
G06F 21/62
G06F 21/10
G06F 21/70
H04L 9/14