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

特許第5319620号
(P5319620)

(45)発行日　平成25年10月16日(2013.10.16)　(24)登録日　平成25年7月19日(2013.7.19)

(51)Int.Cl.		F I		
G06F 21/10	(2013.01)	G06F	21/22	110K
G06F 21/33	(2013.01)	G06F	21/22	110M
G06F 21/62	(2013.01)	G06F	21/20	133
G06Q 50/10	(2012.01)	G06F	21/24	163E
H04L 9/08	(2006.01)	G06F	21/24	166A

請求項の数 28　外国語出願　(全 32 頁)　最終頁に続く

(21)出願番号	特願2010-157194(P2010-157194)
(22)出願日	平成22年7月9日(2010.7.9)
(65)公開番号	特開2011-18342(P2011-18342A)
(43)公開日	平成23年1月27日(2011.1.27)
審査請求日	平成22年9月7日(2010.9.7)
(31)優先権主張番号	12/460,003
(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	12/460,009
(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)
(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)

(73)特許権者　504399716
ディズニー　エンタープライゼス　インコーポレイテッド
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
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100134005
弁理士　澤田　達也
(74)代理人　100134577
弁理士　石川　雅章

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】
メモリとプロセッサとを有するキー集中収納場所（CKR）による、コンテンツへのアクセスの認可を提供するための使用方法であって、
該方法は、
前記プロセッサにより、第１のキーを用いて復号するための第１に暗号化した第２のキー、暗号化メタデータ及びコンテンツＩＤ（識別子）を含むキー情報ファイルを前記コンテンツの受信なしで受信するステップと、
前記プロセッサにより、前記キー情報ファイルを前記メモリに保存するステップであって、前記CKRは前記コンテンツを保存しないステップと、
前記プロセッサにより、前記第１に暗号化した第２のキーを、前記第１のキーを用いて復号して、前記第２のキーを取り戻すステップと、
前記プロセッサにより、コンテンツＩＤを含むキー要求をディストリビュータから受信するステップと、
前記プロセッサにより、第３のキーを用いて前記第２のキーを暗号化して、第２に暗号化した第２のキーを生成するステップと、
前記プロセッサにより、前記キー要求の受信に応答して、前記第２に暗号化した第２のキーを、前記ディストリビュータへ送信するステップと、を有する、方法。
【請求項２】
前記プロセッサにより、前記キー要求の受信に応答して、前記第３のキーを用いて前記

第２のキーを暗号化する、請求項１に記載の方法。
【請求項３】
前記プロセッサにより、前記第３のキーを生成するステップと、
前記プロセッサにより、前記第３のキーをディストリビュータキーデータベースに保存するステップと、
前記プロセッサにより、前記第２に暗号化した第２のキーを、前記ディストリビュータへ送信する前に、前記第３のキーを、前記ディストリビュータへ送信するステップとを、さらに有する、請求項１に記載の方法。
【請求項４】
前記プロセッサにより、前記第３のキーを用いて前記第２のキーを暗号化する前に、前記第３のキーを前記ディストリビュータから受信するステップと、
前記プロセッサにより、前記第３のキーをディストリビュータキーデータベースに保存するステップとを、さらに有する、請求項１に記載の方法。
【請求項５】
前記プロセッサにより、前記第３のキーを用いて前記第２のキーを暗号化する前に、前記第３のキーを第三者から受信するステップと、
前記プロセッサにより、前記第３のキーをディストリビュータキーデータベースに保存するステップとを、さらに有する、請求項１に記載の方法。
【請求項６】
前記第三者は認証オーソリティを含む、請求項５に記載の方法。
【請求項７】
前記キー情報ファイルは、ユニバーサル一意識別子（ＵＵＩＤ）及び国際標準視聴覚番号（ＩＳＡＮ）をさらに含む、請求項１に記載の方法。
【請求項８】
前記CKRはディストリビュータデータベースをさらに含み、前記プロセッサにより前記キー要求の受信に応答して、前記方法は、前記プロセッサにより、前記ディストリビュータが前記第２のキーを受信することを認可されているかどうかを確定するステップを、さらに有する、請求項１に記載の方法。
【請求項９】
前記キー要求は、消費者情報、取引の種類及び装置情報の内の少なくとも1つを、さらに含む、請求項１に記載の方法。
【請求項１０】
前記CKRはトランザクションデータベースをさらに含み、前記プロセッサにより前記キー要求の受信に応答して、前記方法は、前記プロセッサにより、前記消費者情報に関係する消費者が前記コンテンツＩＤに関係する前記コンテンツを使用することを認可されているかどうかを確定するステップを、さらに有する、請求項９に記載の方法。
【請求項１１】
前記CKRは消費者データベースをさらに含み、前記プロセッサにより前記キー要求の受信に応答して、前記方法は、前記プロセッサにより、消費者が前記コンテンツＩＤに関係する前記コンテンツを使用することを、前記取引の種類が認可しているかどうかを確定するステップを、さらに有する、請求項９に記載の方法。
【請求項１２】
前記CKRは装置データベースをさらに含み、前記プロセッサにより前記キー要求の受信に応答して、前記方法は、前記プロセッサにより、前記キー要求に関係する装置が前記コンテンツＩＤに関係する前記コンテンツを使用することを認可されているかどうかを確定するステップを、さらに有する、請求項９に記載の方法。
【請求項１３】
前記キー要求は、前記コンテンツＩＤに関係する前記コンテンツに関係するコードを、さらに含む、請求項１に記載の方法。
【請求項１４】

前記第２に暗号化した第２のキーの前記プロセッサによる送信は、前記第２に暗号化した第２のキーを有するキー情報ファイル及び前記コンテンツＩＤにより参照される前記コンテンツについての情報を含む、請求項１に記載の方法。

【請求項１５】

コンテンツへのアクセスの認可を提供するためのキー集中収納場所（CKR）であって、

該キー集中収納場所は、

第１のキーを有するメモリと、

該メモリと通信するプロセッサとを備え、

該プロセッサは、

前記第１のキーを用いて復号するための第１に暗号化した第２のキー、暗号化メタデータ及びコンテンツＩＤ（識別子）を含むキー情報ファイルを前記コンテンツの受信なしで受信し、

前記キー情報ファイルを前記メモリに保存し、前記CKRは前記コンテンツを保存しないで、

前記第１に暗号化した第２のキーを、前記メモリから取り戻した前記第１のキーを用いて復号して、第２のキーを取り戻し、

コンテンツＩＤを含むキー要求をディストリビュータから受信し、

第３のキーを用いて前記第２のキーを暗号化して、第２に暗号化した第２のキーを生成し、

前記キー要求の受信に応答して、前記第２に暗号化した第２のキーを、前記ディストリビュータへ送信するように構成される、キー集中収納場所。

【請求項１６】

前記プロセッサは、前記キー要求の受信に応答して、前記第３のキーを用いて前記第２のキーを暗号化するように構成される、請求項１５に記載のキー集中収納場所。

【請求項１７】

前記プロセッサは、

前記第３のキーを生成し、

前記第３のキーを前記メモリ内のディストリビュータキーデータベースに保存し、

前記第２に暗号化した第２のキーを、前記ディストリビュータへ送信する前に、前記第３のキーを、前記ディストリビュータへ送信するように、さらに構成される、請求項１５に記載のキー集中収納場所。

【請求項１８】

前記プロセッサは、

前記第３のキーを用いて前記第２のキーを暗号化する前に、前記第３のキーを前記ディストリビュータから受信し、

前記第３のキーを前記メモリ内のディストリビュータキーデータベースに保存するように、さらに構成される、請求項１５に記載のキー集中収納場所。

【請求項１９】

前記プロセッサは、

前記第３のキーを用いて前記第２のキーを暗号化する前に、前記第３のキーを第三者から受信し、

前記第３のキーを前記メモリ内のディストリビュータキーデータベースに保存するように、さらに構成される、請求項１５に記載のキー集中収納場所。

【請求項２０】

前記第三者は認証オーソリティを含む、請求項１９に記載のキー集中収納場所。

【請求項２１】

前記キー情報ファイルは、ユニバーサル一意識別子（ＵＵＩＤ）及び国際標準視聴覚番号（ＩＳＡＮ）をさらに含む、請求項１５に記載のキー集中収納場所。

【請求項２２】

前記メモリはディストリビュータデータベースをさらに含み、前記キー要求の受信に応

答して、前記プロセッサは、前記ディストリビュータが前記第２のキーを受信することを認可されているかどうかを確定するように、さらに構成される、請求項１５に記載のキー集中収納場所。
【請求項２３】
前記キー要求は、消費者情報、取引の種類及び装置情報の内の少なくとも1つを、さらに含む、請求項１５に記載のキー集中収納場所。
【請求項２４】
前記メモリは消費者データベースをさらに含み、前記キー要求の受信に応答して、前記プロセッサは、前記消費者情報に関係する消費者が前記コンテンツＩＤに関係する前記コンテンツを使用することを認可されているかどうかを確定するように、さらに構成される、請求項２３に記載のキー集中収納場所。
【請求項２５】
前記メモリはトランザクションデータベースをさらに含み、前記キー要求の受信に応答して、前記プロセッサは、消費者が前記コンテンツＩＤに関係する前記コンテンツを使用することを、前記取引の種類が認可しているかどうかを確定するように、さらに構成される、請求項２３に記載のキー集中収納場所。
【請求項２６】
前記メモリは装置データベースをさらに含み、前記キー要求の受信に応答して、前記プロセッサは、前記キー要求に関係する装置が前記コンテンツＩＤに関係する前記コンテンツを使用することを認可されているかどうかを確定するように、さらに構成される、請求項２３に記載のキー集中収納場所。
【請求項２７】
前記キー要求は、前記コンテンツＩＤに関係する前記コンテンツに関係するコードを、さらに含む、請求項１５に記載のキー集中収納場所。
【請求項２８】
前記プロセッサは、前記第２に暗号化した第２のキーを有するキー情報ファイル及び前記コンテンツＩＤにより参照される前記コンテンツについての情報を含むことにより、前記第２に暗号化した第２のキーを送信するように、構成される、請求項１５に記載のキー集中収納場所。
【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変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図である。

【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】

【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ャ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】

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を生成するシステムを示す。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、プリペアラー（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。プリペアラー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ャ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（ユーアールエル）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、プリペアラー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。

【００１０】

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、プリペアラー１３０又は他の第三者を用いることができる。

【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ＩＤ１１１及びタイトルＩＤ１１６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ＩＤ１１６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（ＵＵＩＤ）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。

【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ー１３０の汎用ファイルパッケージャ１３５へ送ることができる。このプリペアラー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ー１３０へ届けるために、物理的媒体に書き込むことができる。

【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及びプリペアラー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、プリペアラー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、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及びプリペアラー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。

【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ャ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の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１１５に直接アクセスしないで、なお、タイトル１１５を見て聴いて楽しむことができる。

【００１５】

タイトルキー１３２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ー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１３２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ーを提供する。

【００１６】

キー収納箱１６０によるアクセスのために、タイトルキー１３２をプリペアラー１３０から安全に送るために、認証オーソリティ１２０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１６０によっても生成することができ、認可証は認証オーソリティ１２０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、２０４８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１２１に含まれる。認可証１２１からキー収納箱公開キー１２２を検索することにより、汎用ファイルパッケージャ１３５は、キー収納箱公開キー１２２を用いてタイトルキー１３２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１６５のオーナーであるキー収納箱１６０のみが、暗号化タイトルキー１５２を復号することができるような、暗号化タイトルキー１５２が得られる。認証

オーソリティ１２０は、認可証１２１内に設けられたキー収納箱公開キー１２２が、キー収納箱１６０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。

【００１７】

認証オーソリティ１２０は、例えば、Ｘ．５０９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１２０の同一性を検証するために、プリペアラー１３０は、認証オーソリティ１２０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１２０が、認証されたプリペアラー、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．５０９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。

【００１８】

このようにして、キー収納箱１６０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。プリペアラーＡＰＩ１６１により、プリペアラー１３０のようなコンテンツプリペアラーは、暗号化タイトルキーをキー情報ファイル１５０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１５２のような暗号化タイトルキー、暗号化データ１５３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ＩＤ１１１及びタイトルＩＤ１１６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１６２のようなデータベースに保存することができる。プリペアラー１３０がプリペアラーＡＰＩ１６１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ー（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・セキュリティー（HTTPS）を用いてキー収納箱１６０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。

【００１９】

前に論じたように、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る。キー収納箱１６０は、対応する秘密キーであるキー収納箱秘密キー１６５のオーナーであるため、キー情報データベース１６２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ＡＰＩ１６１及びプロバイダーＡＰＩ１５７により受信してメモリ１５９内にあるリクエストを解釈するためのプロセッサ１５８を用いて、キー収納箱１６０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ＡＰＩ１５７により、メディア・ディストリビュータ１７０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１６２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１５１のような書き換えられたキー情報ファイルを生成する。

【００２０】

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１７０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１７５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１６０にディストリビュータ公開キーデータベース１６６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１６０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１２２と同様に、認証オーソリティ１２０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。

【００２１】

キー収納箱１６０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１６３、トランザクションデータベース１６４、ディストリビュータデータベース１６７、販売データベース１６８及びプリペアラーデータベース１６９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交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１６４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１６０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１６７は、キー収納箱１６０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え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１６３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ャ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ＩＤ１１６、メタデータ１１７及びキー収納箱ＵＲＬ１４６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ＵＲＬ１４６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ＵＲＬ１４６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ＵＲＬ１４６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ＩＤ１１６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ＩＤ１１６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。

【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、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１７

５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。

【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。

【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ことの決定ができるか、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シング、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ー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て、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。

【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。

【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。

【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。

【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２８０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、又は代わりの識別子を作成し、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。

【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、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。

【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。

【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ム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ー及び小さい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、メディアコンテナー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、もたらす。

【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にそのままで直接コピーされる。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３

７０ｂ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。

【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。

【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に、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。

【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。

【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。

【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。
【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て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。
【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、その入力は、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）７２０×４８０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、特別の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】
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ＩＤ２８１、ディストリビュータＩＤ２７１、共有クライアントＩＤ２８６、消費者ＩＤ２８４、タイトルＩＤ２１６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】
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２８

５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ＡＰＩ２５６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】

図５のフローチャート５００のステップ５４０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４ａ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】

図５のフローチャート５００のステップ５５０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】

図５のフローチャート５００のステップ５６０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、プリペアラー１３０の汎用ファイルパッケージャ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。プリペアラー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、プリペアラー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、プリペアラー１３０の汎用ファイルパッケージャ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、プリペアラー１３０の汎用ファイルパッケージャ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、エー・イー・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て、速い復号時間を有する合理的に強いセキュリティーを提供する。
【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、プリペアラー１３０の汎用ファイルパッケージャ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】
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、プリペアラー１３０の汎用ファイルパッケージャ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。

【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、プリペアラー１３０の汎用ファイルパッケージャ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のプリペアラー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、プリペアラー１３０を認証プリペアラーとして認証を行い、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。

【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、プリペアラー１３０の汎用ファイルパッケージャ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。

【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７０

０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。

【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。

【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。

【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すために、キー収納箱１６０からのタイトルＩＤ１１６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。

【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に応答して、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。

【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。

【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。

【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に応答して、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、フローチャート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に応答して、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。

【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、フローチャート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に関係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。

【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、フローチャート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に応答して起動され、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。

【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。

【符号の説明】

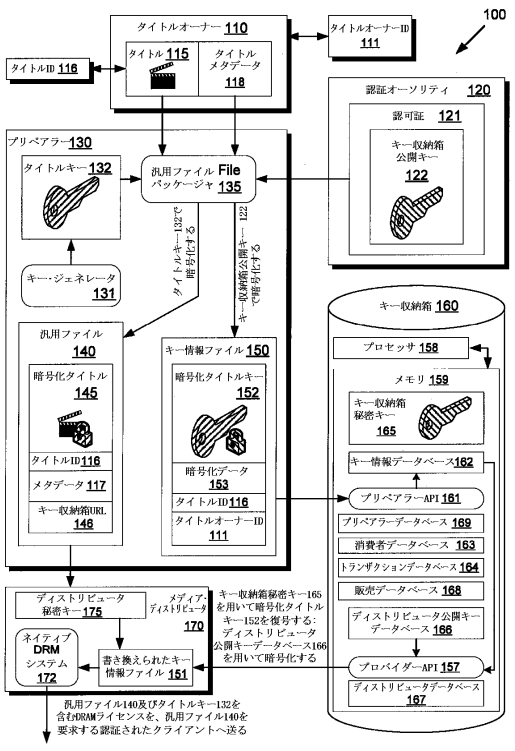
【００９２】

１１０　タイトルオーナー
１１１、２１１　タイトルオーナーＩＤ
１１５　タイトル
１１６、２１６、３１６　タイトルＩＤ
１１７、２１７、３１７　メタデータ
１１８　タイトルメタデータ
１２０　認証オーソリティ
１２１　認可証
１２２　キー収納箱公開キー
１３０　プリペアラー
１３１　キー・ジェネレータ
１３２　タイトルキー
１３５　汎用ファイルパッケージャ
１４０、２４０、３４０、４４０　汎用ファイル
１４５、２４５、３４５　暗号化タイトル
１４６、２４６、３４６　キー収納箱ＵＲＬ
１５０　キー情報ファイル
１５１、２５１　書き換えられたキー情報ファイル
１５２、２５２　暗号化タイトルキー
１５３　暗号化データ
１５７　プロバイダーＡＰＩ
１５８　プロセッサ

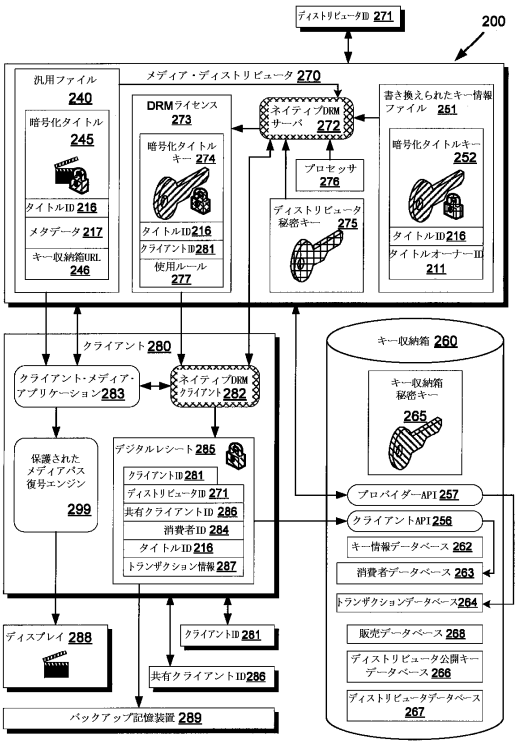
１５９　メモリ
１６０、２６０、３６０、４６０　キー収納箱
１６１　プリペアラーＡＰＩ
１６２　キー情報データベース
１６３　消費者データベース
１６４　トランザクションデータベース
１６５、２６５　キー収納箱秘密キー
１６６　ディストリビュータ公開キーデータベース
１６７　ディストリビュータデータベース
１６８　販売データベース
１６９　プリペアラーデータベース
１７０　メディア・ディストリビュータ
１７２　ネイティブDRMシステム
１７５　ディストリビュータ秘密キー
２５６　クライアントＡＰＩ
２５７　プロバイダーＡＰＩ
２６２　キー情報データベース
２６３　消費者データベース
２６４　トランザクションデータベース
２６６　ディストリビュータ公開キーデータベース
２６７　ディストリビュータデータベース
２６８　販売データベース
２７０、３７０ａ、３７０ｂ、４７０　メディア・ディストリビュータ
２７１　ディストリビュータＩＤ
２７２、３７２ａ、３７２ｂ　ネイティブDRMサーバ
２７３、３７３ａ、３７３ｂ、４７３　DRMライセンス
２７４、３７４ａ、３７４ｂ　暗号化タイトルキー
２７５　ディストリビュータ秘密キー
２７６　プロセッサ
２７７　使用ルール
２８０、３８０ａ、３８０ｂ、４８０　クライアント
２８１、３８１　クライアントＩＤ
２８２、３８２ａ、３８２ｂ　ネイティブDRMクライアント
２８３、４８３、４８３ａ　クライアント・メディア・アプリケーション
２８４　消費者ＩＤ
２８５　デジタルレシート
２８６、３８６　共有クライアントＩＤ
２８７　トランザクション情報
２８８、４８８　ディスプレイ
２８９、４８９　バックアップ記憶装置
２９９　保護されたメディアパス復号エンジン
３６２　キー情報データベース
３６３　消費者データベース
３６４　トランザクションデータベース
３６８　販売データベース
３６６　ディストリビュータ公開キーデータベース
３６７　ディストリビュータデータベース
３６９　プリペアラーデータベース
３５７　プロバイダーＡＰＩ
３９０、４９０　共有クライアントＩＤ検証サーバ

４４０ａ　汎用ファイル（HD）
４４０ｂ　汎用ファイル（SD）
４７３ａ　DRMライセンス（HD）
４７３ｂ　DRMライセンス（SD）
４８０ａ　クライアント（ノートブックパソコン）
４８０ｂ　クライアント（携帯メディアプレイヤー）
４８５　保護デジタルレシート
４８８ａ　ディスプレイ（HD 1280×720）
４８８ｂ　ディスプレイ（SD 720×480）
４９１　メディアディスク
４９２　メディアボックスコード

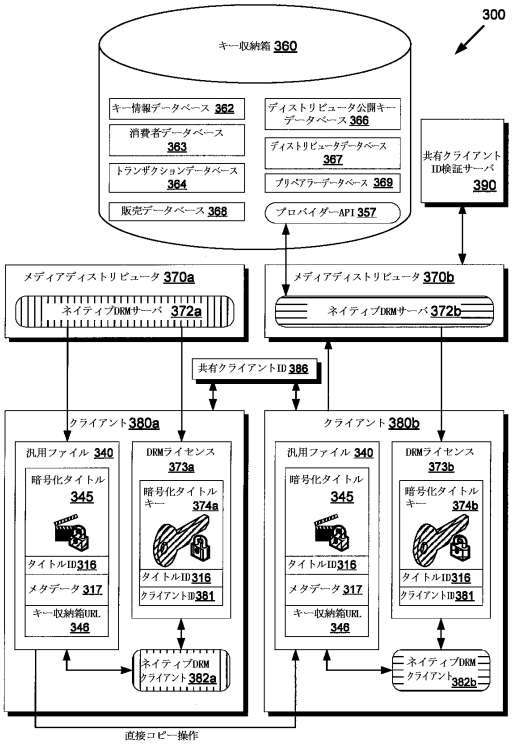
【図１】



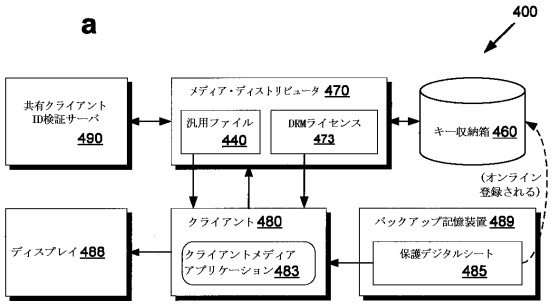
【図２】



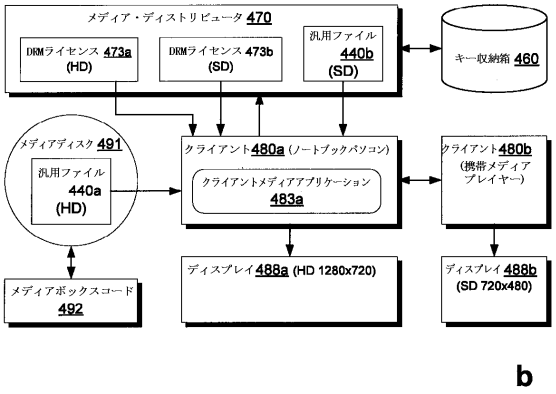
【図３】



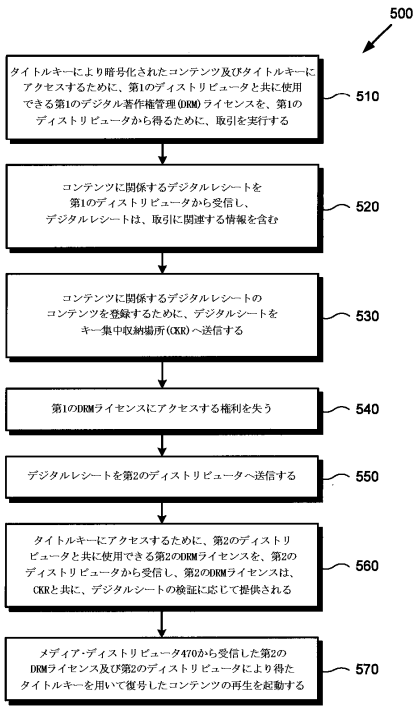
【図４ａ】



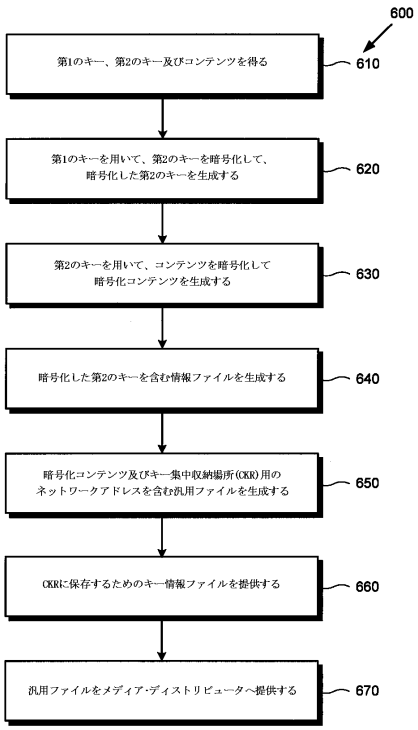
【図４ｂ】



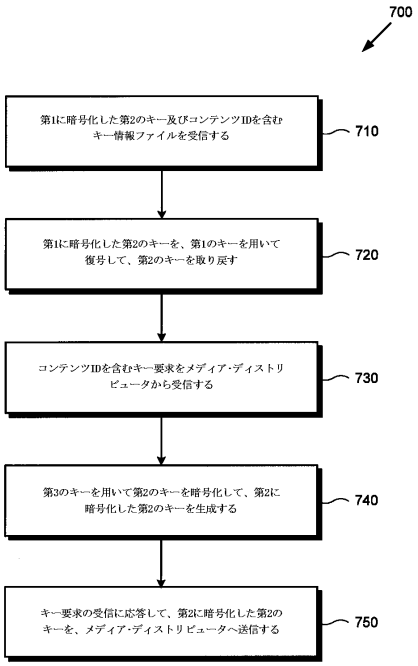
【図５】



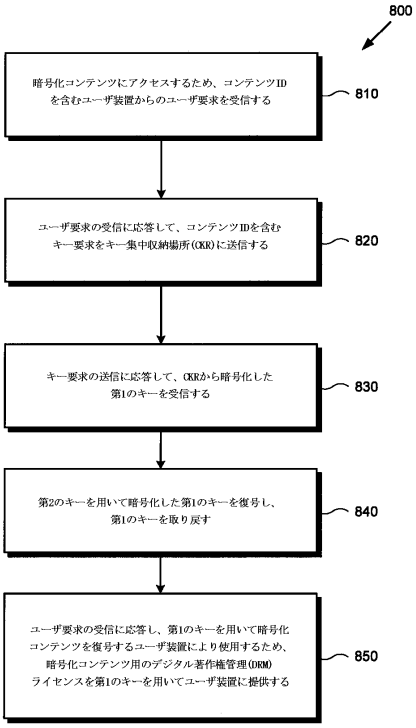
【図６】



【図７】


700
第1に暗号化した第2のキー及びコンテンツIDを含むキー情報ファイルを受信する
710
第1に暗号化した第2のキーを、第1のキーを用いて復号して、第2のキーを取り戻す
720
コンテンツIDを含むキー要求をメディア・ディストリビュータから受信する
730
第3のキーを用いて第2のキーを暗号化して、第2に暗号化した第2のキーを生成する
740
キー要求の受信に応答して、第2に暗号化した第2のキーを、メディア・ディストリビュータへ送信する
750

【図８】


800
暗号化コンテンツにアクセスするため、コンテンツIDを含むユーザ装置からのユーザ要求を受信する
810
ユーザ要求の受信に応答して、コンテンツIDを含むキー要求をキー集中収納場所(CKR)に送信する
820
キー要求の送信に応答して、CKRから暗号化した第1のキーを受信する
830
第2のキーを用いて暗号化した第1のキーを復号し、第1のキーを取り戻す
840
ユーザ要求の受信に応答し、第1のキーを用いて暗号化コンテンツを復号するユーザ装置により使用するため、暗号化コンテンツ用のデジタル著作権管理(DRM)ライセンスを第1のキーを用いてユーザ装置に提供する
850

フロントページの続き

(51)Int.Cl.	FI		
	G06Q	50/10	140
	H04L	9/00	601B
	H04L	9/00	601E

(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 アルノー ロバート
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
(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 特表２００６－５００６５２（ＪＰ，Ａ）
特開２００４－３５０２７１（ＪＰ，Ａ）
特表２００７－５３１１２７（ＪＰ，Ａ）
特開２００５－０５６４１８（ＪＰ，Ａ）
米国特許出願公開第２００６／０２２９９９２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／１０
Ｇ０６Ｆ ２１／３３
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｑ ５０／１０
Ｈ０４Ｌ ９／０８