(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-518901
(P2006-518901A)
(43)公表日　平成18年8月17日(2006.8.17)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560B	5B017
G06Q 50/00	(2006.01)	G06F	17/60	142	
G06Q 30/00	(2006.01)	G06F	17/60	302E	
		G06F	17/60	ZEC	

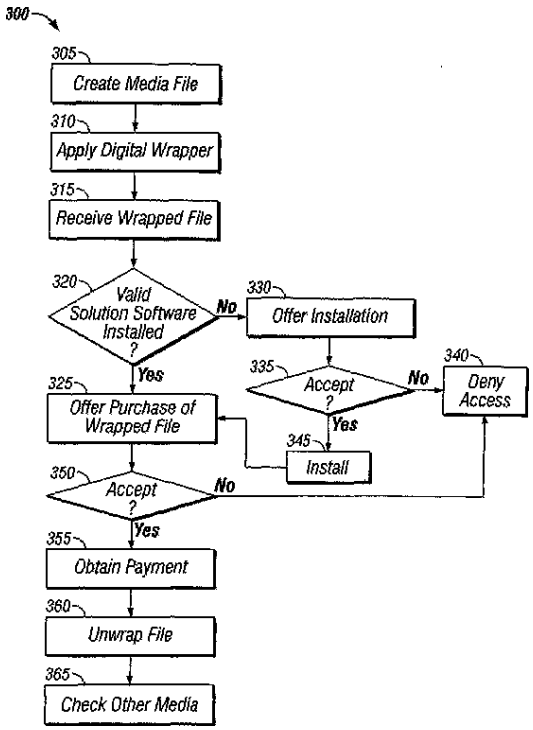
審査請求 未請求　予備審査請求 有　（全 68 頁）

(21)出願番号　特願2006-503101 (P2006-503101)
(86)(22)出願日　平成16年1月28日 (2004.1.28)
(85)翻訳文提出日　平成17年8月31日 (2005.8.31)
(86)国際出願番号　PCT/US2004/002356
(87)国際公開番号　WO2004/070538
(87)国際公開日　平成16年8月19日 (2004.8.19)
(31)優先権主張番号　60/444,581
(32)優先日　平成15年2月3日 (2003.2.3)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10/726,284
(32)優先日　平成15年12月2日 (2003.12.2)
(33)優先権主張国　米国 (US)

(71)出願人　505289638
テネシー、パシフィック、グループ、エル、エル、シー
アメリカ合衆国テネシー州３７０６５、フランクリン、フランクリン・ロウド　２３０番　スウィート１１－ＪＪ
(74)代理人　100073841
弁理士　真田　雄造
(74)代理人　100058136
弁理士　中島　宣彦
(74)代理人　100104053
弁理士　尾原　静夫
(72)発明者　ポウ，ラビン
アメリカ合衆国テクサス州７５２２５、ダラス、ヴィラノウヴァ　３３０１番
最終頁に続く

(54)【発明の名称】デジタルコンテンツの配布及び権利管理

(57)【要約】
デジタル権利を管理する技術とシステムが、デジタルコンテンツの許可されていないコピーからプロテクトし、コンテンツオーナーと配布者への支払を保証するために実装される。デジタルラッパーがデータファイルに対して適用され（３１０、１０２０）、正当な許可なしにアクセスすることを防止する（１３５、３４０、４４０）。データファイルへのアクセスの許可に関連する情報そして／またはそのデータファイルにアクセスするためのキーが蓄積され、ユーザ装置（２０５）の不揮発性のストレージエリア（２２０）に蓄積されたデータを用いて取り出される。ユーザ装置におけるソフトウェアが、ファイルを識別し（１１０、４１５）、そして、デジタルラッパーを認識されたファイルに対して適用する（３１０、４５５、１０２０）ために用いられる。さらに、そのソフトウェアは、そのファイルへのアクセスの許可に従ってそのファイルからデジタルラッパーを取り除くために用いられる（３６０、６８５、７７０）。そのデジタルラッパーに付随する情報を用いて、データファイルの配布者達の間で支払料または他のクレジットが配分



【特許請求の範囲】
【請求項１】
ユーザ装置においてデータファイルを検知し、前記データファイルは、正当な許可なしにそのデータファイルにアクセスできないようにするデジタルラッパーを備え、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータを用いて、前記データファイルへのアクセスの許可に関する情報をサーチし、
前記データファイルへのアクセスの許可がそのサーチにおいて見つかる場合には、そのデジタルラッパーを不能化する
ことを特徴とするデジタル権利管理方法。
【請求項２】
請求項１に記載のデジタル権利管理方法において、
前記データファイルは、メディアファイルを含む
ことを特徴とするデジタル権利管理方法。
【請求項３】
請求項１または請求項２に記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、前記ユーザ装置のライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項４】
請求項３に記載のデジタル権利管理方法において、
ライセンスデータベースが、前記ユーザ装置の不揮発性のストレージエリア内に配置されている
ことを特徴とするデジタル権利管理方法。
【請求項５】
請求項４に記載のデジタル権利管理方法において、
前記ユーザ装置の不揮発性のストレージエリアは、ベーシック入力／出力システム（ＢＩＯＳ）を含む
ことを特徴とするデジタル権利管理方法。
【請求項６】
請求項３乃至請求項５のいずれかに記載のデジタル権利管理方法において、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、ライセンスデータベースのロケーションを含む
ことを特徴とするデジタル権利管理方法。
【請求項７】
請求項３乃至請求項６のいずれかに記載のデジタル権利管理方法において、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、ライセンスデータベース用のアクセスキーを含み、そのアクセスキーは、前記ライセンスデータベースにアクセスするために必要である
ことを特徴とするデジタル権利管理方法。
【請求項８】
請求項３乃至請求項７のいずれかに記載のデジタル権利管理方法において、
前記ライセンスデータベースは、前記データファイル用のアクセスキーを含み、そのアクセスキーは、前記デジタルラッパーを不能化するために必要である
ことを特徴とするデジタル権利管理方法。
【請求項９】
先行するいずれかの請求項に記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、リモートサーバに関連するライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項１０】

請求項９に記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、ユーザ装置上のローカルデータベースが、そのデータファイルへのアクセスの許可に関する情報を有していないという判断に応答して、前記リモートサーバのライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項１１】
請求項９または請求項１０に記載のデジタル権利管理方法において、さらに、
中央サーバに対してユーザ装置の識別データを送信し、その識別データは、前記中央サーバがそのユーザ装置を認証できるように適用される
ことを特徴とするデジタル権利管理方法。
【請求項１２】
請求項１１に記載のデジタル権利管理方法において、
前記識別データは、前記ユーザ装置とそのユーザ装置に付随するユーザの少なくとも一つと関連しているデジタルキーを含む
ことを特徴とするデジタル権利管理方法。
【請求項１３】
先行するいずれかの請求項に記載のデジタル権利管理方法において、さらに、
前記データファイルへのアクセスの許可の購入のオファーを行い、
前記購入のオファーの受け入れを受信し、
そのオファーの受け入れに応答して、前記デジタルラッパーを不能化する
ことを特徴とするデジタル権利管理方法。
【請求項１４】
請求項１３に記載のデジタル権利管理方法において、さらに、
前記オファーの受け入れを中央サーバに送信し、
前記中央サーバから、そのオファーの受け入れに応じたメッセージを受信し、そのメッセージ中に含まれるデータは、前記デジタルラッパーを不能化するために用いられる
ことを特徴とするデジタル権利管理方法。
【請求項１５】
請求項１４に記載のデジタル権利管理方法において、さらに、
前記中央サーバに対して前記ユーザ装置の識別データを送信し、その識別データは、前記中央サーバがそのユーザ装置を認証できるように適用される
ことを特徴とするデジタル権利管理方法。
【請求項１６】
請求項１５に記載のデジタル権利管理方法において、さらに、
前記識別データは、前記ユーザ装置とそのユーザ装置に付随するユーザの少なくとも一つと関連しているデジタルキーを含む
ことを特徴とするデジタル権利管理方法。
【請求項１７】
請求項１３乃至請求項１６のいずれかに記載のデジタル権利管理方法において、さらに、
前記ユーザ装置において、前記データファイルへのアクセスの許可に関する情報を蓄積する
ことを特徴とするデジタル権利管理方法。
【請求項１８】
先行するいずれかの請求項に記載のデジタル権利管理方法において、さらに、
前記データファイルへのアクセスの許可がそのサーチの間に見つからない場合に、そして、そのデータファイルへのアクセスの許可の購入のオファーが受け入れられない場合に、そのデータファイルへのアクセスを拒否する
ことを特徴とするデジタル権利管理方法。
【請求項１９】

先行するいずれかの請求項に記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、前記ユーザ装置が前記デジタルラッパーを不能化するためのソフトウェアを備えているかを判断することを含み、その判断は、デジタルラッパー中に蓄積されている実行可能な命令を用いて行われる
ことを特徴とするデジタル権利管理方法。
【請求項２０】
ユーザ装置においてデータファイルを検知し、
ファイル認識アルゴリズムを用いてデータファイルを識別し、
ユーザ装置の不揮発性のストレージエリアに蓄積されているデータを用いて、そのデータファイルへのアクセスの許可に関する情報をサーチし、
データファイルへのアクセスの許可がそのサーチ中に見つかる場合に、データファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理方法。
【請求項２１】
請求項２０に記載のデジタル権利管理方法において、
ファイル認識アルゴリズムは、デジタルフィンガープリンティング検知技術を含む
ことを特徴とするデジタル権利管理方法。
【請求項２２】
請求項２０または請求項２１に記載のデジタル権利管理方法において、
データファイルは、メディアファイルを含む
ことを特徴とするデジタル権利管理方法。
【請求項２３】
請求項２０乃至請求項２２のいずれかに記載のデジタル権利管理方法において、
データファイルへのアクセスの許可に関する情報のサーチは、ユーザ装置のライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項２４】
請求項２０乃至請求項２３のいずれかに記載のデジタル権利管理方法において、
ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、ユーザ装置の不揮発性のストレージエリア内のライセンスデータベースのロケーションを識別する
ことを特徴とするデジタル権利管理方法。
【請求項２５】
請求項２０乃至請求項２４のいずれかに記載のデジタル権利管理方法において、
データファイルへのアクセスの許可に関する情報のサーチは、リモートサーバのライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項２６】
請求項２０乃至請求項２５のいずれかに記載のデジタル権利管理方法において、
データファイルへのアクセスの許可の購入のオファーを行い、
購入のオファーの受け入れを受信し、
そのオファーの受け入れに応答して、データファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理方法。
【請求項２７】
請求項２６に記載のデジタル権利管理方法において、さらに、
購入のオファーの受け入れに応答して、ユーザ装置において、データファイルへのアクセスの許可に関する情報を蓄積する
ことを特徴とするデジタル権利管理方法。
【請求項２８】
請求項２０乃至請求項２７のいずれかに記載のデジタル権利管理方法において、さらに、

データファイルに対してデジタルラッパーを適用し、そのデジタルラッパーは、識別されたファイルに付随する
ことを特徴とするデジタル権利管理方法。
【請求項２９】
ユーザ装置においてデータファイルを受信し、そのデータファイルは、そのデータファイルの少なくとも一人の配布者に関する情報を含むデジタルラッパーを有しており、
そのデータファイルへのアクセス権を購入するリクエストを受信し、
そのデジタルラッパーから少なくとも一人の配布者に関する情報を抽出し、
抽出された情報に基づいて、少なくとも一人の配布者に対してクレジットを配分する
ことを特徴とするデジタル権利の配布に関連する収益配分方法。
【請求項３０】
請求項２９に記載の収益配分方法において、
デジタルラッパーは、さらに、
データファイルへのアクセス権の購入についての、割り当てられたロイヤリティの配分に関する情報を含んでいる
ことを特徴とする収益配分方法。
【請求項３１】
請求項３０に記載の収益配分方法において、
抽出された情報は、独特のファイル識別子を含み、
その方法は、さらに、
その独特のファイル識別子を用いて、少なくとも一つの配布者情報とそのロイヤリティ配分情報を取り出す
ことを特徴とする収益配分方法。
【請求項３２】
請求項３１に記載の収益配分方法において、
取り出された情報は、ユーザ装置から離れて配置する中央データベースから取り出される
ことを特徴とする収益配分方法。
【請求項３３】
請求項２９乃至請求項３２のいずれかに記載の収益配分方法において、さらに、
購入のリクエストを中央サーバに送信し、その中央サーバのデータベース中にクレジットの配分を蓄積する
ことを特徴とする収益配分方法。
【請求項３４】
ユーザ装置のユーザを識別し、
その方法は、
ユーザ装置においてデータファイルを受信し、そのデータファイルは、そのデータファイルの少なくとも一人の配布者に関する情報を含むデジタルラッパーを有しており、
デジタルラッパーを修正してそのユーザの識別に関する情報を含むようにし、その修正されたデジタルラッパーを用いたそのデータファイルの検知は、そのユーザに対するクレジットの割り当てを可能とする
ことを特徴とするデジタル権利の配布に関連する収益配分方法。
【請求項３５】
請求項３４に記載の収益配分方法において、
そのデジタルラッパーは、正当な許可なしにデータファイルへアクセスできないようにするように適用される
ことを特徴とする収益配分方法。
【請求項３６】
請求項３４または請求項３５に記載の収益配分方法において、さらに、
修正されたデジタルラッパーを有するデータファイルを消費者に付随する装置に対して

送信し、
消費者装置からデータファイルへのアクセスを購入するリクエストを受信し、
受信されたリクエストに応答して、その消費者装置においてデジタルラッパーを不能化する
ことを特徴とする収益配分方法。
【請求項３７】
請求項３６に記載の収益配分方法において、さらに、
１または複数の配布者の間で、その消費者購入に対するクレジットを配分する
ことを特徴とする収益配分方法。
【請求項３８】
請求項３４乃至請求項３７のいずれかに記載の収益配分方法において、
ユーザの識別に関する情報は、そのユーザについての独特のユーザ識別子から成り、その独特のユーザ識別子は、中央サーバによって割り当てられる
ことを特徴とする収益配分方法。
【請求項３９】
請求項３４乃至請求項３８のいずれかに記載の収益配分方法において、
データファイルは、メディアファイルを含む
ことを特徴とする収益配分方法。
【請求項４０】
ユーザ装置からユーザ装置に関連する情報を収集し、そのユーザ装置に関する情報は、ユーザ装置についての独特の識別データを含んでおり、
その方法は、
収集された情報を用いてデジタルキーを生成し、
デジタルキーを蓄積し、
デジタルキーを暗号化し、
暗号化されたキーをユーザ装置上に蓄積するためにユーザ装置に対して送信し、
ユーザ装置から、暗号化されたキーとユーザ装置に関する情報を受信し、
受信された暗号化されたキー、受信された情報、そして蓄積されているデジタルキーのうち少なくとも２つを用いて、ユーザ装置を認証する
ことを特徴とするユーザ装置におけるデジタル権利管理助長方法。
【請求項４１】
請求項４０に記載のデジタル権利管理助長方法において、
ユーザ装置のユーザに関する識別情報を収集し、そのデジタルキーは、そのユーザに関する識別情報を用いて生成される
ことを特徴とするデジタル権利管理助長方法。
【請求項４２】
請求項４０または請求項４１に記載のデジタル権利管理助長方法において、
収集される情報は、ユーザ装置上に蓄積された実行可能コードに従って収集される
ことを特徴とするデジタル権利管理助長方法。
【請求項４３】
請求項４０乃至請求項４２のいずれかに記載のデジタル権利管理助長方法において、
デジタルキーは、中央サーバによって生成され、中央サーバにおいて蓄積される
ことを特徴とするデジタル権利管理助長方法。
【請求項４４】
請求項４０乃至請求項４３のいずれかに記載のデジタル権利管理助長方法において、
ユーザ装置の認証は、
暗号化されたキーを復号し、
暗号化されたキーを蓄積されているデジタルキーと比較する
ことを特徴とするデジタル権利管理助長方法。
【請求項４５】

請求項４０乃至請求項４４のいずれかに記載のデジタル権利管理助長方法において、
ユーザ装置の認証は、
受信されたユーザ装置に関する情報を用いてデジタルキーを生成し、
そのデジタルキーを蓄積されたデジタルキーと比較する
ことを特徴とするデジタル権利管理助長方法。
【請求項４６】
請求項４０乃至請求項４５のいずれかに記載のデジタル権利管理助長方法において、さらに、
ユーザ装置の認証に応答して、ライセンスデータベースへのアクセスを許可する
ことを特徴とするデジタル権利管理助長方法。
【請求項４７】
請求項４０乃至請求項４６のいずれかに記載のデジタル権利管理助長方法において、
ユーザ装置の認証に応答して、デジタルファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理助長方法。
【請求項４８】
請求項４０乃至請求項４７のいずれかに記載のデジタル権利管理助長方法において、
独特の識別データは、ユーザ装置の不揮発性のストレージエリアから抽出される
ことを特徴とするデジタル権利管理助長方法。
【請求項４９】
ユーザ装置の入力／出力システムを、試みられたファイル送信について監視し、
入力／出力システムを通じたデータファイルの送信の試みを検知し、
その送信が許可される前に、データファイルに対してデジタルラッパーを適用し、そのデジタルラッパーは、そのデータファイルへの許可されていないアクセスを防止するために適用される
ことを特徴とするデジタル権利管理助長方法。
【請求項５０】
請求項４９に記載のデジタル権利管理助長方法において、
そのデータファイルは、メディアファイルを含む
ことを特徴とするデジタル権利管理助長方法。
【請求項５１】
請求項４９または請求項５０に記載のデジタル権利管理助長方法において、さらに、
そのデータファイルを識別し、そのデジタルラッパーは、そのデータファイルのアイデンティティに基づいて適用される
ことを特徴とするデジタル権利管理助長方法。
【請求項５２】
請求項４９乃至請求項５１のいずれかに記載のデジタル権利管理助長方法において、
そのデジタルラッパーは、ユーザ装置上のデータベース中のデータファイルの識別子と合致するデータファイルのアイデンティティに基づいて適用される
ことを特徴とするデジタル権利管理助長方法。
【請求項５３】
請求項５１または請求項５２に記載のデジタル権利管理助長方法において、
データファイルの識別は、ファイル認識アルゴリズムの使用を含む
ことを特徴とするデジタル権利管理助長方法。
【請求項５４】
請求項４９乃至請求項５３のいずれかに記載のデジタル権利管理助長方法において、
デジタルラッパーは、そのデータファイルを識別する情報と、そのデータファイルの購入に対するクレジットの割り当てに関する情報を含む
ことを特徴とするデジタル権利管理助長方法。
【請求項５５】
第１のユーザ装置上においてデジタルファイルを識別し、そのデジタルファイルは、そ

の第１のユーザ装置上に蓄積されているライセンス情報に従うライセンスを受けており、
前記第１のユーザ装置から第２のユーザ装置に対するデジタルファイルのコピーのリクエストを受信し、
前記第２のユーザ装置に関連する情報であって、この第２のユーザ装置についての独特の識別データを含む情報を取得し、
前記第１のユーザ装置から前記第２のユーザ装置に対してデジタルファイルをコピーし、
前記第１のユーザ装置上にデータを蓄積し、そのデータは、コピーされたデジタルファイルを識別し、そして、前記第２のユーザ装置を識別する
ことを特徴とするデジタル権利管理方法。

【請求項５６】
請求項５５に記載のデジタル権利管理方法において、さらに、
前記第１のユーザ装置上に蓄積されたデータを中央データベースと同期させる
ことを特徴とするデジタル権利管理方法。

【請求項５７】
請求項５５または請求項５６に記載のデジタル権利管理方法において、さらに、
リクエストされたデジタルファイルのコピーは、ライセンス情報に基づいて許可されると判断する
ことを特徴とするデジタル権利管理方法。

【請求項５８】
請求項５５乃至請求項５７のいずれかに記載のデジタル権利管理方法において、
ライセンス情報は、そのデジタルファイルについてのデジタルラッパー中に含まれている
ことを特徴とするデジタル権利管理方法。

【請求項５９】
請求項５５乃至請求項５８のいずれかに記載のデジタル権利管理方法において、さらに、
第２のユーザ装置上に、そのデジタルファイルについてのライセンス情報を蓄積する
ことを特徴とするデジタル権利管理方法。

【請求項６０】
デジタル権利管理方法であって、
配布されるメディアファイルを識別し、
そのメディアファイルに関するアクセスルールを識別し、そのアクセスルールは、使用権限と使用料に関する情報を含み、
そのメディアファイルに対してデジタルラッパーを適用し、そのデジタルラッパーは、そのメディアファイルについての識別データとアクセスルールに関するデータを含み、そのデジタルラッパーは、そのメディアファイルへの許可されていないアクセスを防止するために適用される
ことを特徴とするデジタル権利管理方法。

【請求項６１】
請求項６０に記載のデジタル権利管理方法において、
デジタルラッパーは、そのメディアファイルへアクセスするライセンスを持っているユーザによって、そのメディアファイルの使用されるようにするために不能化される
ことを特徴とするデジタル権利管理方法。

【請求項６２】
請求項６０または請求項６１に記載のデジタル権利管理方法において、
デジタルラッパーは、さらに、そのメディアファイルの少なくとも一人の配布者に関する情報を含んでいる
ことを特徴とするデジタル権利管理方法。

【請求項６３】

デジタル権利管理方法であって、
ライセンス情報を用いてメディアファイルを符号化し、
許可されていないアクセスを防止するために、デジタルラッパーを用いて、そのメディアファイルをロックし、
ラップされたメディアファイルをユーザ装置上にロードし、
そのメディアファイルのアンロックを許可するためにそのユーザ装置上に命令をインストールし、その命令は、そのメディアファイルを識別し、そして、そのメディアファイル内に符号化されたライセンス情報に従って、そのメディアファイルを使用するライセンスを取得するためにリモートサーバに対してメッセージを送信し、
リモートサーバからメディアファイルへのアクセスのライセンスを受信し、
そのライセンスを用いて、ユーザ装置におけるメディアファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理方法。

【請求項６４】
請求項６３に記載のデジタル権利管理方法において、さらに、
ユーザ装置上に、メディアファイルへアクセスするライセンスを蓄積する
ことを特徴とするデジタル権利管理方法。

【請求項６５】
請求項６３または請求項６４に記載のデジタル権利管理方法において、さらに、
そのライセンスは、そのメディアファイルをアンロックするためのデータを含む
ことを特徴とするデジタル権利管理方法。

【請求項６６】
デジタル権利管理システムであって、
複数のデジタルファイルについての識別子を蓄積するために適用され、そして、デジタルファイルを使用するユーザライセンスを蓄積するために適用される中央データベースと、
ネットワークを介して、リモート装置からメッセージを受信し得る中央サーバとを備え、受信された各メッセージは、ユーザについてのユーザ識別子と、デジタルファイルについての識別情報を含み、
その中央サーバは、さらに、デジタルファイルを使用するライセンスについての支払情報を処理して、そのユーザについての、デジタルファイルを使用するライセンスに関する情報を蓄積し、
そのライセンス情報は、リモート装置を、そのユーザによってデジタルファイルが使用できるようにするために適用される
ことを特徴とするデジタル権利管理システム。

【請求項６７】
請求項６６に記載のデジタル権利管理システムにおいて、
中央サーバは、さらに、
リモート装置から１または複数のデジタルキーを受信し、リモート装置とユーザの少なくとも一つのアイデンティティを認証するために、ひとつまたは複数のデジタルキーを復号し得る
ことを特徴とするデジタル権利管理システム。

【請求項６８】
請求項６６または請求項６７に記載のデジタル権利管理システムにおいて、
中央サーバは、さらに、リモート装置を認証するために用いる装置特有のデータをリモート装置から受信し得る
ことを特徴とするデジタル権利管理システム。

【請求項６９】
請求項６６乃至請求項６８のいずれかに記載のデジタル権利管理システムにおいて、
リモート装置は、ユーザに付随するユーザ装置に対するデジタルファイルのストリーミ

ングをサポートするために適用されるサーバを含む
ことを特徴とするデジタル権利管理システム。
【請求項７０】
請求項６６乃至請求項６９のいずれかに記載のデジタル権利管理システムにおいて、
リモート装置は、ライセンス情報を蓄積する
ことを特徴とするデジタル権利管理システム。
【請求項７１】
請求項６６乃至請求項６８のいずれかに記載のデジタル権利管理システムにおいて、
リモート装置は、ユーザに付随するユーザ装置を含む
ことを特徴とするデジタル権利管理システム。
【請求項７２】
請求項７１に記載のデジタル権利管理システムにおいて、
中央サーバは、さらに、ユーザ装置から情報を受信し、ユーザとユーザ装置の少なくとも一つに関するデジタルキーを生成し、そのデジタルキーをユーザ装置に送信し、そのデジタルキーは、ライセンス情報、ライセンス情報を含むライセンスデータベース、そしてデジタルファイルのうち少なくとも一つにアクセスしうるように適用される
ことを特徴とするデジタル権利管理システム。
【請求項７３】
請求項６６乃至請求項７２のいずれかに記載のデジタル権利管理システムにおいて、
ライセンス情報は、デジタルファイルに対して適用されるデジタルラッパーを不能化するために用いられるデータを含む
ことを特徴とするデジタル権利管理システム。
【請求項７４】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
ユーザ装置においてデータファイルを検知し、そのデータファイルは、正当な許可なしにそのデータファイルにアクセスできないようにするデジタルラッパーを備え、
そのユーザ装置の不揮発性のストレージエリアに蓄積されているデータを用いて、そのデータファイルへのアクセスの許可に関する情報をサーチし、
そのデータファイルへのアクセスの許可がそのサーチにおいて見つかる場合には、そのデジタルラッパーを不能化する
ことを特徴とするアーティクル。
【請求項７５】
請求項７４に記載のアーティクルにおいて、
不揮発性のストレージエリアに蓄積されているデータは、ユーザ装置上のライセンスデータベースにアクセスするためのデジタルキーを含む
ことを特徴とするアーティクル。
【請求項７６】
請求項７４または請求項７５に記載のアーティクルにおいて、
ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、ライセンスデータベースのロケーション情報を含む
ことを特徴とするアーティクル。
【請求項７７】
請求項７４乃至請求項７６のいずれかに記載のアーティクルにおいて、
データファイルへのアクセスの許可は、デジタルラッパーを不能化するためのデジタルキーを含み、そのデジタルラッパーの不能化は、そのデジタルキーを用いて行われる
ことを特徴とするアーティクル。
【請求項７８】
請求項７４乃至請求項７７のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、

ユーザ装置のファイルインプットシステムを監視するオペレーションを実行させるための命令を記録し、
ユーザ装置におけるデータファイルの検知は、ファイルインプットシステムの監視結果によって実行される
ことを特徴とするアーティクル。
【請求項７９】
請求項７４乃至請求項７８のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
ユーザ装置において蓄積されている装置キーを検知し、
そのユーザ装置が許可された装置かを判断するために装置キーを認証するオペレーションを実行させるための命令を記録し、
デジタルラッパーの不能化は、ユーザ装置が許可された装置でない場合には実行されない
ことを特徴とするアーティクル。
【請求項８０】
請求項７４乃至請求項７９のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
データファイルへのアクセスの許可がユーザ装置において見つからない場合に、そのデータファイルへのアクセスの許可をリクエストするリクエストメッセージをリモートサーバに対して送信するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項８１】
請求項８０に記載のアーティクルにおいて、
リクエストメッセージは、データファイルへのアクセスの許可を購入するリクエストを含む
ことを特徴とするアーティクル。
【請求項８２】
請求項８０に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
リクエストメッセージに応答したレスポンスメッセージを受信し、そのレスポンスメッセージは、そのデータファイルへのアクセスの許可を含み、
レスポンスメッセージとともに含まれるデータファイルへのアクセスの許可を用いて、デジタルラッパーを不能化するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項８３】
請求項８０に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
データファイルへのアクセスの許可がサーチにおいて見つからない場合に、データファイルへのアクセスの許可の購入のオファーをユーザ装置のユーザに対して提供し、
購入のオファーの受け入れを受信し、
購入のオファーの受け入れの表示を蓄積するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項８４】
請求項８３に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
購入のオファーの受け入れの表示をリモートサーバに対して送信するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項８５】

ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
ユーザ装置においてデータファイルを検知し、
ファイル認識アルゴリズムを用いて、データファイルを識別し、
ユーザ装置の不揮発性のストレージエリア内に蓄積されているデータを用いて、そのデータファイルへのアクセスの許可に関する情報をサーチし、
そのデータファイルへのアクセスの許可がそのサーチにおいて見つかる場合には、そのデータファイルへのアクセスを許す
ことを特徴とするアーティクル。

【請求項８６】
請求項８５に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
ユーザ装置の入力システムを監視するオペレーションを実行させるための命令を記録し、
そのデータファイルの検知は、その監視の結果として生ずる
ことを特徴とするアーティクル。

【請求項８７】
請求項８５または請求項８６に記載のアーティクルにおいて、
不揮発性のストレージエリアに蓄積されているデータは、ユーザ装置上のライセンスデータベースにアクセスするためのデジタルキーを含む
ことを特徴とするアーティクル。

【請求項８８】
請求項８５乃至請求項８７のいずれかに記載のアーティクルにおいて、
不揮発性のストレージエリアに蓄積されているデータは、ライセンスデータベースのロケーション情報を含む
ことを特徴とするアーティクル。

【請求項８９】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
データファイルに適用されるデジタルラッパーから抽出される情報を受信し、抽出された情報は、データファイルの識別子を含み、
そのデータファイルへのアクセスの許可の購入のリクエストを受信し、
抽出された情報に基づいて、データファイルの少なくとも一人の配布者を識別し、
予め決められた配分構成に従って、識別された配布者にクレジットを配分する
ことを特徴とするアーティクル。

【請求項９０】
請求項８９に記載のアーティクルにおいて、
抽出された情報は、識別された配布者の各々の識別子を含む
ことを特徴とするアーティクル。

【請求項９１】
請求項８９または請求項９０に記載のアーティクルにおいて、
識別された配布者に対するクレジットの配分は、抽出された情報中のデータに従って行われる
ことを特徴とするアーティクル。

【請求項９２】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
ユーザ装置上にデータファイルを蓄積し、そのデータファイルは、そのデータファイルの少なくとも一人の配布者に関する情報を含むデジタルラッパーを有しており、
そのユーザ装置のユーザを識別し、

デジタルラッパーを修正してそのユーザの識別に関する情報を含むようにし、その修正されたデジタルラッパーを伴うそのデータファイルの検知は、そのユーザに対するクレジットの割り当てを可能とする
ことを特徴とするアーティクル。
【請求項９３】
請求項９２に記載のアーティクルにおいて、
デジタルラッパーは、さらに、
ユーザに対するクレジットの割り当て配分に関する情報を含んでいる
ことを特徴とするアーティクル。
【請求項９４】
請求項９２または請求項９３に記載のアーティクルにおいて、
デジタルラッパーは、そのデータファイルへのアクセスの正当な許可なしにそのデータファイルへアクセスできないようにし得る
ことを特徴とするアーティクル。
【請求項９５】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
ユーザ装置からユーザ装置に関連する情報を受信し、受信された情報は、ユーザ装置についての独特の識別データを含んでおり、
受信された情報を用いてデジタルキーを生成し、
デジタルキーを蓄積し、
デジタルキーを暗号化し、
暗号化されたキーをユーザ装置上に蓄積するためにユーザ装置に対して送信し、
ユーザ装置から、暗号化されたキーと、収集されたユーザ装置に関する情報を受信し、収集された情報は、ユーザ装置上に蓄積されている命令に従ってユーザ装置によって収集され、
受信された暗号化されたキー、収集された情報、そして蓄積されているデジタルキーのうち少なくとも２つを用いて、ユーザ装置を認証する
ことを特徴とするアーティクル。
【請求項９６】
請求項９５に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
ユーザ装置から、データファイルへのアクセス許可のリクエストを受信し、
データファイルへのアクセス許可をユーザ装置の認証に応じて送信するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項９７】
請求項９６に記載のアーティクルにおいて、
暗号化されたキーと収集された情報が、その許可のリクエストとともに受信される
ことを特徴とするアーティクル。
【請求項９８】
請求項９６または請求項９７に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
そのデータファイルへのアクセスの許可を示す表示を、そのユーザ装置の認証に応じて蓄積するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項９９】
請求項９５乃至請求項９８のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
ユーザ装置に付随するユーザの独特の識別子を受信し、

さらに、そのユーザの独特の識別子を用いてデジタルキーを生成するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項１００】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
ユーザ装置の入力／出力システムを、試みられたファイル送信について監視し、
入力／出力システムを通じたデータファイルの送信の試みを検知し、
その送信が許可される前に、データファイルに対してデジタルラッパーを適用し、そのデジタルラッパーは、そのデータファイルへの許可されていないアクセスを防止するために適用される
ことを特徴とするアーティクル。
【請求項１０１】
請求項１００に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
許可されていないコピーからプロテクトされているデータファイルを識別するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項１０２】
請求項１０１に記載のアーティクルにおいて、
許可されていないコピーからプロテクトされているデータファイルの識別は、ユーザ装置上に蓄積されているデータベース内にデータファイルの識別子を配置することを含む
ことを特徴とするアーティクル。
【請求項１０３】
請求項１０１または請求項１０２に記載のアーティクルにおいて、
許可されていないコピーからプロテクトされているデータファイルの識別は、
リモートサーバに対して、データファイルを識別するための情報を含むメッセージを送信し、
そのデータファイルが許可されていないコピーからプロテクトされていることを示す、そのメッセージに対するレスポンスを受信することを含む
ことを特徴とするアーティクル。
【請求項１０４】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
第１のユーザ装置上においてデジタルファイルを識別し、そのデジタルファイルは、その第１のユーザ装置上に蓄積されているライセンス情報に従うライセンスを受けており、
第１のユーザ装置から第２のユーザ装置に対するデジタルファイルのコピーのリクエストを受信し、
第２のユーザ装置に関連する情報であって、第２のユーザ装置についての独特の識別データを含む情報を取得し、
第１のユーザ装置から第２のユーザ装置に対してデジタルファイルをコピーし、
第１のユーザ装置上にデータを蓄積し、そのデータは、コピーされたデジタルファイルを識別し、そして、第２のユーザ装置を識別する
ことを特徴とするアーティクル。
【請求項１０５】
請求項１０４に記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、１または複数のプロセッサに、さらに、
ライセンス情報に従って、第２のユーザ装置に対するデジタルファイルのコピーが許されるかを確認するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。

【請求項１０６】
請求項１０４または請求項１０５に記載のアーティクルにおいて、
デジタルファイルのコピーのリクエストの受信は、第１のユーザ装置のファイル出力システムを通じたそのデジタルファイルのコピーの試みを示す表示を受信することを含む
ことを特徴とするアーティクル。
【請求項１０７】
請求項１０４乃至請求項１０６のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、１または複数のプロセッサに、さらに、
そのデータをリモートサーバに対して送信するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項１０８】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
配布されるメディアファイルを識別し、
そのメディアファイルに関するアクセスルールを識別し、そのアクセスルールは、使用権限と使用料に関する情報を含み、
そのメディアファイルに対してデジタルラッパーを適用し、そのデジタルラッパーは、そのメディアファイルについての識別データとアクセスルールに関するデータを含み、そのデジタルラッパーは、そのメディアファイルへの許可されていないアクセスを防止するために適用される
ことを特徴とするアーティクル。
【請求項１０９】
請求項１０８に記載のアーティクルにおいて、
メディアファイルの識別は、ファイル認識アルゴリズムを用いてそのメディアファイルを識別することを含む
ことを特徴とするアーティクル。
【請求項１１０】
請求項１０８または請求項１０９に記載のアーティクルにおいて、
そのメディアファイルについてのアクセスルールの識別は、リモートサーバからアクセスルールを受信することを含む
ことを特徴とするアーティクル。
【請求項１１１】
請求項１０８乃至請求項１１０のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
そのメディアファイルへのアクセスの許可を求めるリクエストをユーザから受信し、
そのメディアファイルへのアクセスの許可を求めるリクエストをリモートサーバに通知し、
ユーザによってそのメディアファイルへのアクセスができるようにするために、そのデジタルラッパーを不能化するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項１１２】
請求項１０８乃至請求項１１１のいずれかに記載のアーティクルにおいて、
メディアファイルについてのアクセスルールの識別は、
ユーザからアクセスルールを受信することを含む
ことを特徴とするアーティクル。
【請求項１１３】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記録したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
デジタルキーを受信し、

そのデジタルキーを不揮発性のメモリ内に蓄積し、
ライセンスデータベース内の少なくとも一つのデジタルファイルについてのライセンス情報を、揮発性のストレージエリア内に蓄積し、
特定のデジタルファイルへのアクセスの試みを識別し、
ライセンスデータベースがその特定のデジタルファイルに対するライセンスを識別するライセンス情報を含んでいる場合に、そのデジタルキーを用いてデジタルファイルへのアクセスを許す
ことを特徴とするアーティクル。
【請求項１１４】
請求項１１３に記載のアーティクルにおいて、
そのデジタルキーは、ユーザ装置に特有のデータを含み、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
ユーザ装置から識別情報を取り出し、
その識別情報と、ユーザ装置に特有のデータとを用いて、そのデジタルキーを認証するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項１１５】
請求項１１３または請求項１１４に記載のアーティクルにおいて、
そのデジタルキーは、ライセンスデータベースのロケーションデータを含み、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
そのデジタルキーからのロケーションデータを用いて、ライセンスデータベースにアクセスするオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項１１６】
請求項１１３乃至請求項１１５のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能なアーティクルは、ひとつまたは複数のプロセッサに、さらに、
ライセンスデータベースが、特定のデジタルファイルへのライセンスを識別するライセンス情報を含んでいない場合に、そのデジタルファイルへのアクセスを防止するオペレーションを実行させるための命令を記録する
ことを特徴とするアーティクル。
【請求項１１７】
請求項１１３乃至請求項１１６のいずれかに記載のアーティクルにおいて、
デジタルキーは、ライセンスデータベースとライセンス情報の少なくとも一つを復号するために必要なデータを含む
ことを特徴とするアーティクル。
【請求項１１８】
請求項１１３乃至請求項１１７のいずれかに記載のアーティクルにおいて、
ライセンス情報は、特定のデジタルファイルに適用されるデジタルラッパーを不能化するために必要なデータを含む
ことを特徴とするアーティクル。
【発明の詳細な説明】
【技術分野】
【０００１】
本説明は、デジタル権利管理に関し、特に、デジタルメディア（ｄｉｇｉｔａｌ　ｍｅｄｉａ）の許可されるライセンス（ａｕｔｈｏｒｉｚｅｄ　ｌｉｃｅｎｓｉｎｇ）と配布との実行に関する。
（関連出願）
【０００２】
本出願は、２０００年２月３日に出願された出願番号６０／４４４，５８１、発明の名称「デジタルメディアの配布及び権利管理」の米国仮出願、及び、２００３年１２月２日

に出願された出願番号１０／７２６，２８４、発明の名称「デジタルコンテンツの配布及び権利管理（Ｄｉｓｔｒｉｂｕｔｉｏｎ ａｎｄ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ ｏｆ Ｄｉｇｉｔａｌ Ｃｏｎｔｅｎｔ）」の米国仮出願の利益を主張している。

【背景技術】

【０００３】

音楽産業は、混乱の中にある。十年もの間、音楽会社は、作成したコンテンツ（ｃｏｎｔｅｎｔ）の物理的な配布を管理してきた。歴史上の初期においては、消費者は、このコンテンツの配布をコントロールできるようにするツールを与えられてきた。急速に拡大し、広く適用される技術は、現状に対して消費者によってなされる破壊的な変化をもたらした。無数のリーガルまたはイリーガルな解決法が、デジタル世界におけるコンテンツ配布についての本質的な難題に対して解答し、解決しようとしてきた。コンテンツのデジタル配布についての問題は、大いに音楽産業に関連しているものの、映画産業（ｍｏｔｉｏｎ ｐｉｃｔｕｒｅ ｉｎｄｕｓｔｒｙ）のような他の産業も同じ難題を被っている。

【０００４】

コンテンツクリエーター／オーナーと消費者双方を満足させる解決法はない。広く適用されている唯一のデジタル配布についての解決法は、様々なピアツーピアネットワークにおいて見受けられる。しかし、この解決法は、何百万もの消費者が音楽及び他の形式のコピーライトされたコンテンツを、ダウンロードするコンテンツに対して支払わずにダウンロードできるようにする。コンテンツのオーナーは、料金を収集することができない。この状況は、大きな収入の損失を引き起こす。

【０００５】

とりわけ、デジタルサブスクリプションサービスの承認を通じて、音楽会社のような多くのコンテンツ作成者は、デジタル配布が将来あることを確認する。これは、最も効率的かつ経済的な配布手段である。現在のところ、音楽産業は、この配布手段に十分取り組んではいない。デジタル配布は、また、他の産業において、多くのタイプのコンテンツに関して一般に行われている。他のタイプのコンテンツにおいて、音楽産業が直面しているこれらの問題と同様の問題が生じている。

【０００６】

例えば、音楽産業における近年のデジタル配布モデルは、偽った購入パターンに消費者を限定して、歌の選択を制限し、他の利用可能なオプションを制限する、。さらに、これらのモデルは、一般に、消費者のコンテンツに対する支払方法を制限し、モデルのいくつかは、基調をなす成果物における権利の侵害を防止することができない。

【発明の開示】

【０００７】

（発明の要旨）

デジタル権利を管理するシステム及び技術が提供される。発明者は、デジタルメディア及び他のコンテンツを保護する現在の技術は適していないと認識し、ユーザが正当にデジタルメディアと他のコンテンツにアクセスする機能を実質的に損なうことなく、デジタル権利をライセンスするためにプロセスを改善し得ることを認識した。さらに、そのようなプロセスは、そのようなコンテンツをプロモートし、配布するユーザに対して報酬を与えるメカニズムを提供し得る。

【０００８】

一つの一般的な側面において、デジタル権利の管理は、ユーザ装置上のデータファイルを検知することを含む。そのデータファイルは、有効な許可なしに（ｗｉｔｈｏｕｔ ｖａｌｉｄ ａｕｔｈｏｒｉｚａｔｉｏｎ）データファイルにアクセスできないようにするデジタルラッパー（ｄｉｇｉｔａｌ ｗｒａｐｐｅｒ）を含む。ユーザ装置の不揮発性のストレージエリアに蓄積されたデータを用いて、データファイルにアクセスする権限に関する情報のサーチが行われる。そのデジタルラッパーは、そのデータファイルにアクセスする権限がそのサーチにおいて見つかるなら動作しない。

【０００９】

実施例は、ひとつまたは複数の以下の特徴を有する。そのデータファイルは、メディアファイルであり得る。データファイルにアクセスする権限に関する情報のサーチが、ユーザ装置上のライセンスデータベースにおいて行われる。そのライセンスデータベースは、ユーザ装置の不揮発性のストレージエリアに配置されている。ユーザ装置の不揮発性のストレージエリアは、ベーシック入力／出力システム（ＢＩＯＳ）であり得る。ユーザ装置の不揮発性のストレージエリア（ｓｔｏｒａｇｅ　ａｒｅａ）に蓄積されたデータは、ライセンスデータベースのロケーションそして／またはライセンスデータベース用のアクセスキーとを備え得る。アクセスキーは、ライセンスデータベースにアクセスするために必要である。ライセンスデータベースは、データファイル用のアクセスキーを含み、そのアクセスキーは、そのラッパーを不能化するために必要である。そのデータファイルへのアクセスの許可（ａｕｔｈｏｒｉｚａｔｉｏｎ）に関連する情報のサーチが、ユーザ装置上のローカルデータベースが、そのデータファイルへのアクセスの許可に関する情報を持っていないとの判断に応答して、リモートサーバについてのライセンスデータベースにおいて行われる。

【００１０】

ユーザ装置の識別データは、中央サーバに送信され、その識別データが適用されて、その中央サーバがそのユーザ装置を認証（ｖａｌｉｄａｔｅ）できるようにする。その識別データは、ユーザ装置そして／またはそのユーザ装置に付随するユーザに関するデジタルキーを含んでいる。そのデータファイルへのアクセスの許可（ａｕｔｈｏｒｉｚａｔｉｏｎ）は、購入用にオファーされ、購入のオファーの受け入れが受信され得る。そのデジタルラッパーは、そのオファーの受け入れに応じて不能化される。そのオファーの受け入れは、中央サーバに送信され得る。中央サーバからのメッセージが、そのオファーの受け入れに対応して受信され、そして、そのメッセージ中に含まれるデータは、そのデジタルラッパーを不能化するために用いられる。そのユーザ装置の識別データは、中央サーバに対して送信され、その中央サーバがそのユーザ装置を認証できるようにする。その識別データは、ユーザ装置そして／またはそのユーザ装置に付随するユーザに関するデジタルキーを含み得る。そのデータファイルへのアクセスの許可についての情報は、ユーザ装置上に蓄積され得る。そのデータファイルへのアクセスは、そのデータファイルへのアクセスの許可がサーチにおいて見いだせなかった場合、及び、そのデータファイルへのアクセスの許可の購入のオファーが受け入れられなかった場合には、拒否され得る。そのデータファイルへのアクセスの許可に関する情報のサーチは、そのユーザ装置がそのデジタルラッパーを不能化するためのソフトウェアを含んでいるかを判断するための、デジタルラッパー中に蓄積されている実行可能な命令を用いることを含む。

【００１１】

別の一般的な側面においては、デジタルラッパーを含まないデータファイルがユーザ装置上で検知される。そのデータファイルは、ファイル認識アルゴリズムを用いて識別される。データファイルへのアクセスの許可に関する情報のサーチが、ユーザ装置の不揮発性のストレージエリアに蓄積されたデータを用いて行われる。そのデータファイルへのアクセスは、そのデータファイルへのアクセスの許可がそのサーチにおいて見つかった場合には、許される。

【００１２】

実施例は、ひとつまたは複数の以下の特徴を備える。ファイル認識アルゴリズムは、デジタルフィンガープリンティング検知技術を含んでいる。そのデータファイルは、メディアファイルであり得る。そのデータファイルへのアクセスの許可に関する情報のサーチは、ユーザ装置上のライセンスデータベースにおいて行われる。ユーザ装置の不揮発性のストレージエリアに蓄積されたデータは、ユーザ装置の揮発性のストレージエリア中のライセンスデータベースのロケーションを識別し得る。そのデータファイルへのアクセスの許可に関する情報のサーチは、リモートサーバのライセンスデータベースにおいて行われ得る。そのデータファイルへのアクセスの許可は、購入のオファーがなされる。購入のオファーの受け入れが受信されると、そのデータファイルへのアクセスが許される。そのデー

タファイルへのアクセスの許可に関する情報は、その購入のオファーの受け入れに応じて、そのユーザ装置上のデータベース中に蓄積される。その識別されたファイルに関するデジタルラッパーが、そのデータファイルに適用され得る。

【００１３】

別の一般的な側面においては、ユーザ装置上のデータファイルを受信することによって、また、そのデータファイルへのアクセスの許可の購入リクエストを受信することによって、デジタル権利の配布に対して、収益が配分される。そのデータファイルは、ひとつまたは複数のデータファイルの配布に関する情報を含むデジタルラッパーを有する。ひとつまたは複数の配布に関する情報が、デジタルラッパーから抽出され、抽出された情報に基づいて、ひとつまたは複数の配布者に対してクレジットが割り当てられる。

【００１４】

実施例は、ひとつまたは複数の以下の特徴を含む。デジタルラッパーは、さらに、ロイヤリティの割り当て配分に関する情報を含む。抽出された情報は、独特の（ｕｎｉｑｕｅ）ファイル識別子であり、その配布者の情報そして／またはロイヤリティ割り当て情報が、その独特のファイル識別子を用いて取り出される。その取り出された情報は、ユーザ装置とは離れて配置されている中央データベースから取り出され得る。購入のリクエストは、中央サーバに送信されることができ、そして、クレジットの割り当てが、その中央サーバのデータベース中に蓄積され得る。

【００１５】

デジタル権利の配布についての収益の配分に参加するため、データファイルが受信される装置のユーザが識別される。そのデータファイルは、そのデータファイルのひとつまたは複数の配布者に関する情報を有するデジタルラッパーを含んでいる。そのデジタルラッパーは、そのユーザの識別子に関する情報を含むように修正される。その修正されたデジタルラッパーを備えるデータファイルの検知は、クレジットのそのユーザへの割り当てを可能とする。そのデジタルラッパーは、適用されることによって、正当な許可なしにデータファイルにアクセスできないようにし得る。その修正されたデジタルラッパーを備えるデータファイルは、消費者の装置に送信され、そのデータファイルへのアクセスの購入リクエストが、その消費者の装置から受信される。その消費者の装置上のデジタルラッパーは、その受信されたリクエストに応じて不能化され得る。消費者の購入に対するクレジットが１または複数の配布者の間に配分される。そのユーザの識別子に関する情報は、中央サーバによって付与された独特のユーザ識別子である。

【００１６】

他の一般的な側面において、デジタル権利管理が、ユーザ装置に関する情報であって、そのユーザ装置用の独特の識別データを含む情報をユーザ装置から収集することによって、また、収集された情報を用いてデジタルキーを生成することによって、ユーザ装置上で実行される。そのデジタルキーは、蓄積され、暗号化され、その暗号化されたキーは、ユーザ装置に送信されて、ユーザ装置上に蓄積される。その暗号化されたキーとユーザ装置に関する情報は、順次受信され、そのユーザ装置はその受信された暗号化されたキー、受信された情報そして／または蓄積されているデジタルキーを用いて認証される。

【００１７】

実施例は、ひとつまたは複数の以下の特徴を含んでいる。そのユーザ装置のユーザに関する識別情報が収集され、デジタルキーが、そのユーザに関する識別情報を用いて生成される。その収集された情報は、そのユーザ装置上に蓄積された実行可能なコードに従って収集される。そのデジタルキーは、中央サーバによって生成され、中央サーバ上に蓄積される。そのユーザ装置の認証は、暗号化されたキーを復号し、その暗号化されたキーを、蓄積されたデジタルキーと比較することを含む。そのユーザ装置の認証は、また、受信されたユーザ装置に関する情報を用いてデジタルキーを生成し、そのデジタルキーを、蓄積されたデジタルキーと比較することを含む。ライセンスデータベースへのアクセスそして／またはデジタルファイルへのアクセスは、そのユーザ装置の認証に応じて許可される。その独特の識別データは、ユーザ装置の不揮発性のストレージエリアから抽出される。

【００１８】
他の一般的な側面においては、ユーザ装置の入力／出力システムが、ファイル転送を行うために監視される。入力／出力システムを通じたデータファイルの転送が検知され、デジタルラッパーがその転送が許可される前にそのデータファイルに適用される。そのデジタルラッパーは、データファイルへの許可されていないアクセスを防止するように適用される。
【００１９】
実施例は、ひとつまたは複数の以下の特徴を含んでいる。そのデータファイルは、識別され、そのデジタルラッパーは、ユーザ装置上のデータベース内のデータファイルの識別子と合致するデータファイルの識別子に基づいて適用される。そのデータファイルの識別は、ファイル認識アルゴリズムを用いて行われる。そのデジタルラッパーは、データファイルとそのデータファイルの購入に対するクレジットの割り当てに関する情報を識別する情報を含んでいる。
【００２０】
他の一般的な側面においては、デジタルファイルが第１のユーザ装置上で識別され、そのデジタルファイルが第１のユーザ装置上に蓄積されたライセンス情報に従って、ライセンスされる。第１のユーザ装置から第２のユーザ装置へのデジタルファイルのコピーリクエストが受信され、その第２のユーザ装置に関する情報であって、第２のユーザ装置用の独特の識別データを含む情報が取得される。そのデジタルファイルは、第１のユーザ装置から第２のユーザ装置にコピーされ、そのコピーされたデジタルファイルと第２のユーザ装置とを識別するデータが、第１のユーザ装置上に蓄積される。
【００２１】
実施例は、ひとつまたは複数の以下の特徴を含む。第１のユーザ装置上に蓄積されたデータは、中央データベースと同期し得る。ライセンス情報に基づいて、デジタルファイルのコピーリクエストの許可が判断される。そのライセンス情報は、そのデジタルファイル用のデジタルラッパーに含まれている。そのデジタルファイル用のライセンス情報は、第２のユーザ装置上に蓄積され得る。
【００２２】
他の一般的な側面においては、配布されるメディアファイルが識別される。使用権限と使用料に関する情報を含むアクセスルールであって、そのメディアファイルに関するアクセスルールが識別される。デジタルラッパーがそのメディアファイルに適用される。そのデジタルラッパーは、そのメディアファイル用の識別データとそのアクセスルールに関するデータを含み、そのメディアファイルへの許可されていないアクセスを防止するように適用される。
【００２３】
実施例は、ひとつまたは複数の以下の特徴を含む。そのデジタルラッパーは、そのメディアファイルにアクセスするライセンスを有するユーザがそのメディアファイルを使用できるように不能化される。そのデジタルラッパーは、さらに、ひとつまたは複数のメディアファイルの配布者に関する情報を含んでいる。
【００２４】
他の一般的な側面においては、メディアファイルは、ライセンシング情報を用いて符号化され、そのメディアファイルは、許可されていないアクセスを防止するためのデジタルラッパーを用いてロックされる。ラップされたメディアファイルは、ユーザ装置上にロードされる。メディアファイルのアンロックを許可するための命令がユーザ装置にインストールされる。その命令は、そのメディアファイルを識別し、メディアファイル中に符号化されているライセンシング情報に従って、メディアファイルの使用ライセンスを得るためのメッセージをリモートサーバに送信する。そのメディアファイルへのアクセスのライセンスが、そのリモートサーバから取得され、そのユーザ装置におけるそのメディアファイルへのアクセスが、そのライセンスを用いて許される。
【００２５】

実施例は、ひとつまたは複数の以下の特徴を含んでいる。そのメディアファイルにアクセスするライセンスは、ユーザ装置上に蓄積されている。そのライセンスは、そのメディアファイルをアンロックするためのデータを含んでいる。

【００２６】

他の一般的な側面においては、中央データベースが、デジタルファイルについての識別子を蓄積し、そのデジタルファイルを使用するユーザライセンスを蓄積するために適用される。中央サーバは、リモート装置からネットワークを介してメッセージを受信し得る。受信される各メッセージは、ユーザ用のユーザ識別子と、デジタルファイル用の識別情報を含んでいる。その中央サーバは、さらに、そのデジタルファイルを使用するライセンスに対する支払情報を処理し、そのデジタルファイルを使用するライセンスをそのユーザと関連づける情報を蓄積し、デジタルファイルのライセンス情報をリモート装置に送信する。そのライセンス情報は、そのリモート装置がそのユーザによるデジタルファイルの使用を許可させ得るように適用される。

【００２７】

実施例は、ひとつまたは複数の以下の特徴を含む。中央サーバは、さらに、リモート装置からひとつまたは複数のデジタルキーを受信し、ひとつまたは複数のデジタルキーを復号して、リモート装置とユーザの少なくともひとつのアイデンティティを認証する。その中央サーバは、さらに、リモート装置から、そのリモート装置を認証するのに用いる、装置特有のデータを受信し得る。そのリモート装置は、そのユーザのユーザ装置に対する、デジタルファイルのストリーミングをサポートするために適用されるサーバであってもよい。そのリモート装置は、そのライセンス情報を蓄積し得る。そのリモート装置は、そのユーザのユーザ装置であってもよい。その中央サーバは、さらに、ユーザ装置から情報を受信するために適用され、そのユーザそして／またはユーザ装置に関するデジタルキーを生成し、そのデジタルキーをそのユーザ装置に送信するために適用され得る。そのデジタルキーは、ライセンス情報、そのライセンス情報を含むライセンスデータベースそして／またはデジタルファイルに対するアクセスを可能にするために適用され得る。そのライセンス情報は、デジタルファイルに適用されるデジタルラッパーを不能化するのに用いるデータであってもよい。

【００２８】

説明した技術は、方法、システム、または、ひとつまたは複数のプロセッサを動作させる命令を記録したマシーン読み取り可能な媒体を含むアーティクル（ａｒｔｉｃｌｅ）として実装され得る。

【００２９】

ひとつまたは複数の実施例の詳細は、添付した図面と以下の描写によって説明される。他の特徴は、その説明と描写、そしてクレームから明らかである。

【発明を実施するための最良の形態】

【００３０】

ここで説明するシステムと技術は、デジタルメディアファイルの配布と権利管理用のコンピュータに実装されたシステムに関する。そのシステムと技術は、理論上任意のタイプの、音楽及び他の記録物、映画及びその他のビデオ、書籍及びその他の記述物を含む著作権デジタルファイル、そして、ファイナンシャル、法律上、医学上、ゲーミング、そしてソフトウェア産業におけるファイルといった他のファイルを支援するエンドツーエンドのプロセスを示す。以下の説明は、主に音楽ファイルについての技術の適用に焦点が当てられているが、その技術は、等しく他のタイプのデジタルファイルに適用可能である。同様に、その技術は、メディアファイルのコンテクストにおいて説明されているが、その技術は、また、マルチメディアファイルと他のタイプのデータファイルについて適用できる。そのシステムと技術は、コンテンツオーナーがそれらの作品の配布と使用の見返りを受け、デジタルメディアの売却そして／またはライセンシングによって生み出される収益への様々な参加レベルをオファーすることを保証する。

【００３１】

その技術は、「ラップされていない」（すなわち保護されていない）［ｕｎｗｒａｐｐｅｄ］形式で到着するメディアと同様に、「ラップされた」（保護された）［ｗｒａｐｐｅｄ］形式でユーザのコンピュータに到着するメディアについて動作する。メディア権利のオーナーは、所有権と支払に関する情報を持ったファイルをラップし得る。この情報には、独特のファイルＩＤが与えられ、中央データベースに蓄積される。そのファイルＩＤは、そのラッパーとともに蓄積され、転送される。そのラッパーを持たない歌または他の形式のデジタルメディアもまた識別される。一旦ファイルがそのシステムによって取得され、識別されると、（例えば、識別されたファイルを中央データベースに蓄積された独特のファイルＩＤと照合することによって）オーナーや支払リクエストといった情報が取り出される。説明されるソリューション（「ソリューションソフトウェア」）に従って提供される監視ソフトウェアは、自動的に、またはマニュアルでユーザがラップされたファイルにアクセスしようとするコンピュータまたは他の装置上にインストールされる。一旦インストールされると、そのコンピュータのファイル入力／出力（Ｉ／Ｏ）システムを通過するすべての将来のメディアが、利用可能であればファイルＩＤを用いることによって、または、ファイル識別ソフトウェアを用いることによって識別され得る。

【００３２】

ユーザＩＤが、各ユーザについて生成される。そのユーザＩＤは、そのコンピュータのＢＩＯＳのような、コンピュータ上の安全なエリア内に、装置に特有の情報とともに蓄積される。そのユーザＩＤは、暗号化されたまたは暗号化されていない形式で蓄積される。この情報は、ユーザが保有するライセンスと、関連する許諾についてのローカルデータベースにアクセスすることを許可するユーザ識別キーを示している。このローカルライセンスデータベースを参照することにより、そのコンピュータ上に蓄積されているソリューションソフトウェアは、ユーザが特定のファイルを使用可能かを判断でき、もしそうである場合は、そのファイルをアンラップする。そのファイルがラップされていなくても、そのファイルのアクセスまたは使用は、ローカルデータベースまたは中央データベースレベルに蓄積されているビジネスルールに従って許可または防止される。例えば、ビジネスルールは、あるタイプのファイルを、ローカルデータベースにおいてライセンスが見出せない場合には使用できなくする一方で、他のタイプのファイルを、ライセンスの必要なく使用できるようにする。ユーザは、多数の装置を持っていることが多いため、そのユーザのライセンスについての情報は、中央において蓄積され、そのユーザが、自分が有する１以上の装置において、ライセンスされた全てのメディアにアクセスすることを保証する。

【００３３】

ユーザは、個人または家族、世帯のメンバー、共有されたプライベート装置にアクセスする人物、またはビジネス体といった、関連する１セットの個人として定義される。さらに、情報がデータベースに蓄積されるものとして説明する場合、その情報は、多数のデータベースにおいて蓄積される。

【００３４】

ファイルは、他のユーザに向けられるか、さもなくばユーザ間で交換される。しかし、ファイルがライセンスを必要とし、新たなユーザがそのメディアファイルを購入しない場合、その新たなユーザは、そのファイルにアクセスできない。そのファイルの配布を促進するために、ユーザは、メディアファイルを「パスアロング」（電子的な送信）［ｐａｓｓ　ａｌｏｎｇ］するか、またはそのメディアファイルに興味を持っていると感じる他者（すなわち、新たな購入者によって生み出された収入の一部を受け取り得る者）にメディアファイルをリンクさせるインセンティブが与えられる。受領者達は、そのメディアファイルを購入（すなわちそのファイルにアクセスし得るように）するインセンティブを与えられ、さらに、彼らもまたその収入の分配を受けるように、そのメディアを送信する。収入の分配を受けることが許される配布レベル数は、無制限である。しかし、典型的には、収入の分配を受けることが許される配布レベル数は、限られている。特定のメディアファイルについての支払レベルの数は、コンテンツオーナーそして／またはそのメディアファイルをその後に配布する者によって設定される。支払レベルの最大数とそのような支払に

ついてのレートは、メディアファイルの独特のファイルＩＤの生成の際に、支払レートとともに設定される。新たなユーザがそのメディアファイルをライセンスされていなければ、彼／彼女は、他のユーザに購入のためにそのファイルを送信することができるが、そのファイルにアクセスすることはできない。

【００３５】

あるファイルは、購入され、またはそのファイルとともに送信される関連ファイルを必要とする、購入または送信用のルールを含んでいる。例えば、ある歌は、アルバムのような歌の集合の一部としてのみ売られることを必要とする。他の例は、予告編、広告、または他の関連マテリアルが、映画または配信されるテレビ番組に伴うことを必要とする。

【００３６】

段階的な水準を持つ配布技術に従って、正確に収益を分配することを支援するため、ユーザのコンピュータにおけるソリューションソフトウェアが、転売者と配布者がラップされたメディアファイルに彼らの識別子を付与し売るメカニズムを提供し、転売者と配布者を識別し得るようにして、その結果、彼らが配布チャネルを必要とする場所における販売に対して報酬を受けられるようにする。販売取引が特定のメディアファイルについて生じる度に、配布チャネルにおけるユーザの識別情報がラップされたメディアファイルから抽出され、誰がその収益の分配を受けられるかが決定される。全ての取引は、支払と分析のために中央で追跡される。中央追跡データベースは、転売者、（ラップされたファイルを送信するユーザを含む）配布者、そして、ラッパーなしに到着するファイルを送信するユーザについての支払を追跡し得る。この後者の状況は、例えば、ユーザが、標準のオーディオＣＤまたはＤＶＤから発せられる歌をシェアする時に生じ得る。参照するユーザのＩＤが、購入時に入力され、その結果、参照者と、関連する転売者と配布者達が報酬を受けられるようにする。

【００３７】

ファイルについてのライセンスが、ユーザの多数の装置を通じて認識される。ここで説明される方法と技術は、ユーザの多数の装置を通じた管理、分配、ライセンスの移動を提供する。

【００３８】

図１は、コンピュータといったユーザの装置にロードされるファイルに対するデジタル権利を管理するプロセス１００のフロー図である。ユーザ装置は、その装置が全てのファイル入力／出力を監視するためのＩ／Ｏポートとのソフトウェアインタフェースであって、コンピュータのために全ての入出力するトラフィックをスキャンし、そのシステムから入出力する全てのファイルをチェックする、ファイアウォールに似たソフトウェアインタフェースを備える。ファイルは、フロッピードライブ、イーサネットまたはＬＡＮコネクション、ダイアルアップコネクション、ＣＤ－ＲＯＭまたはＤＶＤドライブ、ＵＳＢポート、赤外線データポート、Ｂｌｕｅｔｏｏｔｈまたは他の無線コネクション、またはデータをそのユーザ装置と送受信する任意の他のメカニズムそして／またはプロトコルを含む、任意のタイプのＩ／Ｏポートを用いてその装置上にロードされる。

【００３９】

そのファイルがユーザ装置上にロードされると、そのファイルが検知される（ステップ１０５）。その検知されたファイルは、さらに、そのファイルを識別するためにファイル識別ソフトウェアを用いて調査される（ステップ１１０）。例えば、そのファイル識別ソフトウェアは、その受信されたファイルが知られた（例えばＭＰ３、ウィンドウメディア、または他のフォーマットでの）歌または映画かを判断する。このファイル識別は、その全てがグレースノート株式会社に譲渡され、ここにおいて参照として組み込まれている、ロバートらの２００２年７月３１日に出願された、公開番号２００３００２８７９６の米国特許出願において、また、ロバーツの、２００２年１０月２９日に出願された、公開番号２００３００４６２８３の米国特許出願そして／または、ウェルズらの２００２年７月２２日に出願された公開番号２００３００８６３４１の米国特許出願において記述された技術を実装するソフトウェアによって実行される。この技術は、デジタルファイルからデ

ジタルフィンガープリント（ｄｉｇｉｔａｌ　ｆｉｎｇｅｒｐｒｉｎｔ）を抽出し、抽出されたフィンガープリントを知られたデータベースと比較する。より具体的には、この技術は、メディアファイルタイプと（例えば、潜在的に保護された産物を示す）そのメディアファイルが関係する類似物を検知するアルゴリズムを用いることができる。一般に、これらのアルゴリズムは、そのファイル拡張子に基づいて単にそのファイルタイプを識別するのではなく、そのファイルの内部属性を調査する。関係のないと判断されるメディアファイルは、さらにそのファイルを解析することなく通過が許可される。

【００４０】

そのメディアファイルが関係しそうであるとされたら、追加的なアルゴリズムがその特定のメディアファイル（例えば特定の歌、映画、写真、記述作品など）を識別するために用いられる。特定のメディアファイルの識別を可能とするフィンガープリンティングデータは、中央サーバに蓄積され、インターネットコネクションを用いてアクセスされる。ファイルのいくつかは、対応するファイルタイプのものであるが、（例えば、そのメディアファイルがユーザによって生成されたレコードを示す場合や、デジタルフィンガープリントについての中央データベースへのアクセスができない場合には）認識されない。そのようなファイルへのアクセスは、制限なく認められるが、そのファイルについては、（例えば、ユーザ装置上において、その認識されていないファイルがアクセスされている旨の表示を格納することによって）認識されていない旨のフラグが立てられ、将来における処理を迅速にし、ソリューションソフトウェアが、そのメディアファイルがその後カタログ化され、または識別された場合（例えば、中央のデジタルフィンガープリントデータベースに対するインターネットコネクションが可能となった時）の後の使用において、そのメディアファイルを識別し得るようにする。そのファイルが連続して識別され、カタログ化され、制限された場合には、識別されないファイルがアクセスされた旨を示す蓄積された表示が、そのファイルの使用を継続するためのライセンスの購入を要求したり、または、そのファイルの使用についてのライセンス料を集めるために用いられる。ある実施例においては、限定された数のメディアファイル（例えば２０００の最も人気のある歌ファイル）が、迅速なアクセスのために、そのコンピュータ上にローカルに蓄積される。そのローカルに蓄積されたフィンガープリンティングデータは、定期的にその中央サーバから（例えば、歌ファイルの人気が変動するにつれて）更新される。

【００４１】

上記のファイル識別技術は、（例えばファイル名、拡張子、または他の属性を変更するなどして）そのファイルを偽造しようとする者がいる場合においても、また、そのファイルが圧縮形式または非圧縮形式で受信されようとも（例えば、圧縮情報をリードする標準プラクティスを用いて）、そのファイルを正確に識別できるようにする。そのような技術は、２％以下（１％以下の間違った否定と、１％以下の間違った肯定）という非常に小さいエラーレートを提供する。

【００４２】

デジタル権利管理の分野において知られている、透かし及びフィンガープリンティング技術といった、他のファイル識別技術もまた用いられる。ある場合には、複雑なファイル識別技術を用いて、そのファイルを識別する必要がなくなる。その代わりに、そのファイルは、そのファイル名に基づいて、または、そのファイル中にまたはそのファイルとともに含まれているファイルＩＤの属性を用いて識別され、改変できないように設計される。例えば、そのメディアファイルがラップされている場合、そのファイル識別ソフトウェアが、そのラッパーの検知動作を行い、そのラッパー中に埋め込まれているファイルＩＤ情報をリードする。こうして、ファイルは、そのファイルの隠された特徴（例えば、フィンガープリントまたは透かし）を用いて、または、（例えばファイルヘッダに格納されたファイル識別子などの）明示されたファイル特徴を用いて識別される。

【００４３】

一旦そのファイルが識別されると、そのファイルがそのユーザ装置における、そして／または特定のユーザによる使用のライセンスがなされているかが判断される（ステップ１

１５）。この判断は、（例えばユーザ装置上に）ローカルに、そして／または（例えば中央サーバにおいて）遠隔的に格納された、１または複数のライセンスデータベースを参照することによって行われる。ライセンスデータベース中のライセンス情報が正当であることを保証するため、１または複数の特殊キーが、その情報にアクセスし、そのライセンスデータベースをアンロックし、そして／またはそのユーザ、そのユーザ装置、そして／またはそのユーザ装置におけるライセンス自体を認証するために用いられるか、または、以下により詳細に説明するように、中央サーバへの通信がなされる。そのファイルがライセンスされたものなら、そのユーザは、そのファイルへのアクセスが許され、例えば、そのファイルをアンラップし、そのファイル中に含まれる歌または映画を再生し、または、無線または有線のコネクションを通じてそのファイルをユーザ装置にストリーミングすることが許可される（ステップ１２０）。そのライセンスは、どんなタイプのそのファイルのアクセスまたは使用が許されるかを特定する。

【００４４】

そのファイルがライセンスされていない場合、ライセンスの購入のオファーがそのユーザに対してなされる（ステップ１２５）。例えば、そのユーザは、購入することが可能なウェブサイトに向かうか、ユーザ装置のディスプレイスクリーン上にポップアップウィンドウが表示されて、そのユーザがそのファイルに対するライセンスの購入を望むか、またはそうでなければあるライセンスタームを受け入れるか、そして／またはそのユーザが購入できるウェブサイトに向かうかを尋ねる。その代わりとして、そのユーザは、ライセンスの購入に使われるある数のクレジットを予め購入することができるサービスを受ける。または、別の代わりとして、特定の期間内において使用されたライセンスされていないメディアの数がソリューションソフトウェアまたは他のソフトウェアによってローカルに監視され、この情報が、使用料またはレートの計算にシーケンシャルに用いられる。継続期間、使用及び配布制限、そして支払オプションといった、そのライセンスタームは、また、購入用のライセンスのオファーの一部として表示される。そして、そのユーザがそのライセンスを受け入れるかが（例えば、そのユーザが承諾ボタンやポップアップウィンドウにおけるディクラインボタンをクリックしたことを示す表示を受信することによって）判断される（ステップ１３０）。そのユーザがそのライセンスを受け入れない場合には、そのファイルへのアクセスが拒否される（ステップ１３５）。そのユーザがそのライセンスを受け入れる場合には、任意の支払タームに応ずる場合も含め、そのユーザは、そのファイルへのアクセスが許可され、そのファイルがライセンスされたことを示すライセンス情報と、任意の他の必要な情報が、ライセンスデータベース中に格納される（ステップ１４０）。

【００４５】

図２は、デジタル権利を管理する具体的システム２００のブロック図である。ユーザ装置２０５は、メモリ２１５そして／またはユーザ装置２０５に接続された他の記録媒体（図示せず）上に蓄積された命令を実行する、プロセッサ２１０を備える。そのユーザ装置は、ＢＩＯＳ（ベーシック入力／出力システム）２２０、または、ユーザ装置２０５についてのベーシック情報を蓄積する他の不揮発性のメモリを備える。そのユーザ装置２０５は、（２３０に示すように）、ファイルと他のデータが移動できるようにし、そして／またはユーザ装置２０５にコピー入出力できるようにする、ひとつまたは複数のＩ／Ｏポート２２５を備える。プロセッサ２１０は、メモリ２１５に蓄積された命令に従って、Ｉ／Ｏポート２２５を通過する、プロテクトされた（例えば、コピーライトされた）音楽、ビデオ、ソフトウェアまたは他のファイルを識別するためのファイルと他のデータを監視する。

【００４６】

メモリ２１５は、ユーザ装置２０５における、またはひとつまたは複数のユーザによる使用をライセンスされたファイルのライセンス情報を蓄積するローカルデータベース２３５を備える。ローカルデータベース２３５、またはローカルデータベースに含まれる情報に対するアクセスは、ソリューションソフトウェアを必要とし、また、ＢＩＯＳ２２０中

に蓄積されているひとつまたは複数のキーを用いる。そのようなキーは、ユーザそして／またはユーザ装置２０５に独特のものであり、そのローカルデータベース２３５へのアクセスプロセスは、ローカルデータベース２３５中に蓄積されたキーそして／またはライセンス情報が特定のユーザ装置２０５について正当な場合だけである。例えば、ユーザが別の装置上において、キーそして／またはライセンス情報の許可されていないコピーを行おうとする場合には、ユーザ装置にライセンスされたファイルへのアクセスは、新たな独特のキーがその別の装置のために生成され、その別の装置上にライセンス情報が蓄積されない限り、その別の装置上において拒否される。特定の装置上のライセンス情報は、将来更新され、使用権限を更新し、または、ファイルへアクセスできないようにする。そのような更新をおこなう場合の例は、古いコンピュータの非ライセンス化である。

【００４７】

ユーザ装置２０５は、ひとつまたは複数の無線ネットワーク、ＬＡＮ、ＷＡＮ、インターネット、電話ネットワーク、そしてデータ送信用の他の任意のネットワークを含む、ネットワーク２４５を通じて中央サーバ２４０に通信する。ユーザ装置２０５と中央サーバ２４０との間の通信は、セキュアソケットレイヤー（ＳＳＬ）といったセキュアなチャネルを用いて、そして／またはＰＧＰといった暗号化を用いて行われる。中央サーバ２４０は、デジタル権利管理システム２００をサポートするサービスを提供し、例えば、少なくとも部分的に、セキュアなコネクションを通じてユーザ装置２０５から通信された情報を用いてキーを生成し、定期的または新たなメディアをライセンスしようとする時にキー及びライセンス情報を認証する。さらに、中央サーバ２４０は、個別のユーザが持っているライセンスを蓄積及び識別し、キー認証情報を蓄積する中央ライセンスデータベース２５０へのアクセスを提供する。中央ライセンスデータベース２５０へのライセンス情報は、（ユーザ装置の揮発性メモリエリアにおける破壊が生じる場合には）冗長に蓄積され、別の装置におけるライセンスされたデータ条件を再生成し、ユーザ装置間におけるライセンスの送信を許可し、揮発性メモリエリアのない装置（例えば、いくつかのタイプのセル電話）を用いるユーザによるライセンス情報へのリモートアクセスを許可し、ライセンスされたデジタルファイルのストリーミングを許可する。

【００４８】

いくつかのセル電話といった、いくつかのタイプのユーザ装置２０５について、いくつかの機能が、ユーザ装置から離れたコンポーネントによって実行される。例えば、いくつかのセル電話は、ローカルにファイルとライセンス情報を蓄積することができるメモリを備えておらず、または、アプリケーションによっては、そうすることは望ましくない。そのような場合、デジタルファイル（例えば音楽またはビデオであるが、それに限定されない）は、無線コネクションを通じてユーザ装置にストリームされる。ローカルデータベース２３５は、無線ネットワーク中に配置され、そのユーザ装置が特定のファイルにアクセスするライセンスを有しているかの判断は、その無線ネットワーク中のサーバ上で実行される。

【００４９】

多くの場合、ローカルデータベース２３５は、ユーザ装置２０５に対してローカルである。しかし、いくつかの場合、ローカルデータベース２３５は（他の蓄積可能な手段とともに）、ネットワークドライブまたは他の外部ストレージ上に配置される。ネットワークドライブまたは外部ストレージがユーザ装置２０５にマップされまたは接続されている場合、付加的な情報がそのデジタルファイルを十分にセキュアにするために用いられる。特に、ネットワークドライブまたは外部ストレージに対してそのストレージロケーションを追跡するために書き込まれているデータを、記述することが望ましい。さらに、そのローカルデータベース２３５にアクセスする装置、そして／またはユーザを識別することが望ましい。

【００５０】

ローカルデータベース２３５がユーザについて生成され、そのロケーションデータがＢＩＯＳに書き込まれると、情報がネットワークドライブまたは外部ストレージに書き込ま

れる。ネットワークドライブまたは外部ストレージに書き込まれた情報は、ネットワークドライブまたは外部ストレージに接続されたユーザ装置またはマシーンを、独特のユーザＩＤそして／または装置ＩＤを用いて識別する。例えば、ファミリーシェアードサーバまたは他の共有ネットワークサーバの場合、そのドライブは、ネットワークドライブまたは外部ストレージ上の暗号化されたファイルに蓄積された、多数のユーザそして／または装置ＩＤ（またはその２つの組み合わせ）を有する。新たなマシーンがそのドライブに接続されると、その新たなマシーン用の識別情報が、そのネットワークドライブまたは外部ストレージ上の暗号化されたファイルに追加される。この識別情報は、中央において（例えば、中央サーバ２４０または中央データベース２５０において）追跡され、過剰な数のユーザまたはマシーンが同じメディアを使用してそのメディアのライセンスルールを揮発させることのないようにする。

【００５１】

図３は、ユーザ装置上に、プロテクトされたファイルをコントロールするソフトウェア（ソリューションソフトウェア）をインストールするプロセス３００のフロー図である。ソリューションソフトウェアは、キーの生成のための情報を収集し、中央サーバと通信し、そのファイルＩ／Ｏシステムを監視し、ローカルデータベースからのライセンス情報を蓄積し、および取り出し、（例えばグレースノートまたは他の技術を用いて）ファイルを識別し、ファイルをラップまたはアンラップし、そのライセンスの購入を実行することを含む、多くの様々な機能を実行する。そのソリューションソフトウェアは、様々な形でユーザ装置上にインストールされる。従来のダウンロードおよびソフトウェアインストールプロセスでは、ソリューションソフトウェアのインストールという１つの方法であった。そのインストールプロセスは、そのユーザ装置がラップされたファイルを受信した時に開始される。他の潜在的なインストールプロセスは、現在のピアツーピアのネットワークにそのソリューションソフトウェアによってラップされた歌を供給し、そのソリューションソフトウェアまたはソリューションソフトウェアを蓄積しているサーバへのリンクを、インスタントメッセージングまたは電子メールまたは別の代替手段を用いて送信する。図３中に示されるプロセス３００は、ラップされたファイルを受信した結果、開始されるインストールを示す。

【００５２】

最初に、データファイルが生成される（ステップ３０５）。例えば、そのデータファイルが歌である場合、そのデータファイルの生成は、その歌とアーティストをレコーディングしたアーティスト、ラベル、配布準備ができている歌を生成するために協働した出版者を含む。その代わりとして、独立したアーティストが自分で配布用の歌を生成し、出版する場合もある。その歌は、その後、歌をＣＤまたはＤＶＤといったデジタルソースまたはアナログソースから取るといったように、「リップ」され、その歌は、ＭＰ３ファイル、ウィンドウメディアファイル、リアルプレイヤーファイル、またはコンピュータまたはミュージック／メディアプレイヤー装置上でプレイバックするための他のメディアフォーマットで符号化される。

【００５３】

次に、デジタルラッパーがそのメディアファイルに適用される（ステップ３１０）。そのコンテンツオーナー（例えばレコードラベル、出版者、または独立のアーティスト）またはその配布チェーンの中の誰か他の者は、そのメディアファイルに対してそのデジタルラッパーを適用し、調整し、またはエンハンスする。そのデジタルラッパーは、所有権、使用権限、ロイヤリティフィー、そして送信される支出レベル（例えば、その配布チェーン周辺の個人に支払われる手数料）を特定するビジネスルールとともに、タイトル、作者／アーティスト、そして、ボリューム／コレクションといった属性を含む。この組み合わせられた情報に、「独特のファイルＩＤ」（ＵＦＩＤ）［Ｕｎｉｑｕｅ　Ｆｉｌｅ　ＩＤ］が与えられ、そして、中央のデータベース内に蓄積される（図２参照）。そのＵＦＩＤは、任意のそして全ての送信の間に、そのラッパー内に含められ、そして、そのメディアファイルを特定し、コピーライトオーナー支払イベント、ファイル使用データベース更新

、そして、消費者のパスアロング動作についてのマイクロ支払料の分配を開始させるメカニズムとして用いられる。そのソリューションソフトウェアは、ファイルとそのＵＦＩＤの正当性を認証して、ＵＦＩＤとラッパーが不正に変更されることを防止する。例えば、独特の埋め込まれたＩＤを備えないファイルに関して上述した認識技術が、抽出されるＩＤを生成することによってそのファイルを「認識」するために用いられる。その抽出されるＩＤは、対応する蓄積されたＩＤと照合され、そのファイルとその独特の埋め込まれた識別子が不正に変更されないようにする。

【００５４】

そのメディアファイルに関する情報に加えて、そのラッパーは、そのメディアファイルに対する許可されていないアクセスを防止する。言い換えると、そのラッパーは、そのユーザがライセンスを購入しない限りそのメディアファイルへアクセスできないようにする。要するに、そのラッパーはそのファイルを、基調となるメディアファイルにアクセスし得るキーを必要とする暗号化された形式にする。ソフトウェアアプリケーションを、それらが電子的に配布される時にプロテクトするために用いられる従来からのデジタルラッパーが、そのメディアファイルに対するラッパーとして用いられる。例えば、そのラッパーは、シマンテックコーポレーションのノートンアンチウィルスやアラディンソフトウェアのプリビレッジシステムといったソフトウェアの配布に用いられる、デジタルリバーから利用できるイーコマースラッパーと同じタイプである。一旦そのユーザが自分自身のためにまたはその装置のために購入すると、キーがそのメディアファイルをアンラップするために用いられる。そのキーは、中央サーバから受信される。

【００５５】

典型的には、ユーザ装置と中央サーバとの間の全ての通信は、２つの暗号化レベルを用いて発生する。最初に、送信が、ＳＳＬ／ＴＬＳ（セキュアＨＴＴＰとして知られているセキュアソケットレイヤ／トランスポートレイヤ）を介して暗号化される。第２に、送信されたキーは、公開キーとプライベートキーのペアとシンメトリックキーを介してセキュアにされる。ユーザ装置に特有の証明書が、インストールの際にユーザ装置に対して発行され、そのコンピュータが中央サーバと安心して通信し得るようにする。その証明書は、その送信者が、それがそうであると言っている者であることを示している。次に、中央サーバは、その公開キーを、送信コンピュータに対して送信する。送信コンピュータは、シンメトリックキーを用いて、送信したい情報を暗号化し、そして、そのシンメトリックキーを中央サーバの公開キーで暗号化する。中央サーバは、そのプライベートキーを用いて、そのシンメトリックキーをデコードし、そのシンメトリックキーを、受信された情報をデコードするために用いる。シンメトリックキーアルゴリズムの例は、ＤＥＳ（デジタル暗号化システム）、３ＤＥＳ（トリプルＤＥＳ）、そして、シンプル暗号複写アルゴリズムを含む。キーペア暗号化アルゴリズムのポピュラーな例は、ＰＧＰ（プリティグッドプライバシー）である。記述されている方法論は、情報を中央サーバからユーザの装置に対して送信するために、逆方向に用いられる。

【００５６】

一般に、各メディアファイルは、対応する独特のキーを持っており、特定のキーは、２またはそれ以上のメディアファイル間で共有される。セキュリティの改善のため、用いられる特定の暗号化方法は、各ファイルに対してユニークである。従って、多数の暗号化技術が用いられ、そのラッパーは、そのファイルをアンラップするために復号技術が用いられるソリューションソフトウェアに通知するための、暗号化技術の識別子を含んでいる。そのラッパーは、また、ユーザがそのラップされたファイルを開けようとする時にはいつも動作する実行可能なコンポーネントを含んでいる。とりわけ、その実行可能なコンポーネントは、そのユーザ装置上に、正当にインストールされたソリューションソフトウェアが存在するかを判断する。

【００５７】

その装置にローカルなライセンスデータベースは、暗号化され得る。この暗号化は、典型的には、上述したシンメトリックキーを用いる。セキュリティを改善するために、セキ

ュリティのレイヤが（上述したように）追加され、その暗号化スキームが中央サーバとの通信において、時とともに変更される。説明した技術は、そのシンメトリックキーを生成するために、データと暗号化シード値の組み合わせを利用する。これらの暗号化シードの要素は、そのローカルなユーザそして／または装置に特有の情報であって、その装置のハードウェアと不揮発性メモリに向けられる情報を含む情報を含んでいる。これは、そのシステムの、ローカルなマシーンに特有の暗号化を行う機能を向上させる。こうして、あるシステム用に生成された、暗号化および識別キーは、別のシステム上で使用することができない。

【００５８】

ラップされたファイルは、典型的には、上述したようにシンメトリックキーを用いて暗号化される。この暗号化されたコンテンツは、実行可能なラッパー内に蓄積される。従って、キーは、ラップされたファイルのプロテクト（例えばロック）とアンロック、ローカルデータベースのロックとアンロック、ユーザ装置と中央サーバそして／または中央データベースとの間の通信のプロテクト、そのユーザの認証、そのユーザ装置の中央のサーバに対する認証、そして、その中央サーバのユーザ装置に対する認証を含む、様々なセキュリティ機能のために用いられる。

【００５９】

ユーザ装置は、その後、物理的なまたは電子的なメディア配布技術を通じて、そのラップされたファイルを受信する（ステップ３１５）。例えば、ユーザは、そのコンピュータ上で、例えばＭｏｒｐｈｅｕｓ、ＫａＺａＡ、Ｎａｐｓｔｅｒ、Ｇｒｏｋｓｔｅｒなどといったピアツーピアのプラットフォームから、また、他の人から受信した電子メールにおいて、また、サイトがデジタルコンテンツの限定された配布者であるか否かによらず、ウェブサイト、電話または衛星ネットワークからのファイルアクセスおよびダウンロードプロセス（ＦＴＰまたはＨＴＴＰ）を通じて、または、インスタントメッセージを介したパーソンツーパーソンのファイル送信または他の直接のコネクト方法によって、または、ネットワークコネクション、ＣＤ－ＲＯＭまたはＣＤＲ、ＤＶＤ－Ｒ、Ｚｉｐディスクなどといった他のメディアを介して、そのラップされたファイルを受信する。

【００６０】

ユーザが（例えばそのファイル上にダブルクリックすることによって）そのラップされたファイルを開こうとしたり、また、アクセスしようとしたりすると、そのデジタルラッパーの実行可能なコンポーネントは、ユーザ装置上にソリューションソフトウェアの正当なインストールが既に存在するかを判断する（ステップ３２０）。ソリューションソフトウェアのインストールの間、中央のサーバは、そのユーザそして／または装置キーに関連する「独特のカスタマーＩＤ」（ＵＣＩＤ）を含む独特のキーを生成する。その独特のキーは、予め決められたアルゴリズムに従い、装置に特有の情報を含む多くのデータタイプと、ユーザ入力から収集されたデータと、ソリューションソフトウェアまたは中央のサーバによって生成されたデータと、ローカルデータベースアクセスとロケーション情報の組み合わせによって生成される。データまたは少なくともデータの一部は、ユーザ装置から中央サーバに対して送信され、その中央サーバは、その独特のキーを生成するためにその受信されたデータを用いる。中央サーバは、次に、この情報を暗号化して、その情報を、その情報がＢＩＯＳといった、ユーザ装置上のセキュアな不揮発性のエリアに蓄積されるユーザ装置に対して返す。とりわけ、その独特のキーは、その中央サーバが、その消費者を認識し、そのユーザがライセンスされたデータファイルを使用し、他の消費者に対してファイルを「プロモート」（パスアロング）することに対する支払を受けられるようにする。実行可能なソリューションソフトウェアとサポーティングファイルとを伴うユーザ装置上における独特のキーの存在は、そのユーザ装置上にそのソリューションソフトウェアが正当にインストールされたことを示す。一方、その独特のキーが存在するが、そのユーザが全てまたは一部のソフトウェアとサポーティングファイルを取り除いた場合、ソリューションソフトウェアの再インストールが必要となる。

【００６１】

従って、ユーザがラップされたメディアファイルにアクセスしようとする場合、そのソリューションソフトウェアは、そのソリューションソフトウェアがインストールされた場合にその独特のキーが書き込まれる、（「システムマネジメントＢＩＯＳ参照仕様バージョン２．３（セクション２．１－テーブル仕様）において定義されているように、（ＤＭＩとしても知られている）ＳＭＢＩＯＳ標準に書き込まれているＢＩＯＳデータテーブルのメモリリードを行うことによって、ＢＩＯＳをチェックして、正当な独特のキーが存在するかを調べる。その独特のキーが見つからない場合、そのラッパーの実行可能なコンポーネントは、そのソリューションソフトウェアはまだインストールされていないと判断する。その独特のキーがＢＩＯＳ中に存在する場合、その独特のキーがリードされて、中央データベースによって認証され、見つかった独特のキーが正当であることが保証される。その中央データベースは、その独特のキーを復号し、チェックサムを計算し、認証する。チェックサムの使用に代えて、クライアント装置と中央サーバとの間で交換される付加的なキーまたはハンドシェイクトークンを含む、他の認証方法が用いられる。ある状況または実施例において、その独特のキーの正当性の認証は、ユーザ装置上のソリューションソフトウェアによって行われる。その独特のキーとチェックサムが合致しない場合、そのラッパーの実行可能なコンポーネントは、正当なソリューションソフトウェアは現在インストールされていないと判断する。その独特のキーとチェックサムが照合する場合、正当なインストールが存在すると判断される。そのローカルシステムが、限られたプロセシングリソースしか持っていない（例えばセル電話内の）、いくつかの実施例において、正当なインストールのチェックプロセスは、その中央サーバにおいて実行される。

【００６２】

さらに、その独特のキーが、正当なインストールが存在することを示す場合、そのユーザ装置上に配置されたソリューションソフトウェアは、ＢＩＯＳ中に蓄積されている独特のキーに含まれているソリューションソフトウェア用の独特の識別情報に照らして認証される。例えば、ＢＩＯＳ中に蓄積されている独特のキーは、ユーザ装置上に配置されているソリューションソフトウェアのチェックサムおよびバージョンと比較される、暗号化形式で蓄積されていないソリューションソフトウェアのチェックサムとバージョンを含む。この情報が合致しない場合は、そのラッパーの実行可能なコンポーネントは、正当なソリューションソフトウェアが現在インストールされていないと判断する。さもなくば、正当なインストールが認識される。

【００６３】

図３には示されていないが、ラップされたファイルがそのユーザ装置上に既にライセンスされている（すなわち、そのファイルへのアクセスについてのライセンスが、既にローカルまたは中央ライセンスデータベースに蓄積されている）か、ファイルが、ラッパーなしに、既にユーザ装置上に存在する（例えば、そのファイルがソリューションソフトウェアがユーザ装置上にインストールされる前にＣＤからそのユーザ装置上にリップされる）状況が存在する。その後者の場合、そのユーザは、そのファイルへのアクセスをライセンスを与えられていることを想定している。そのファイルが既にユーザ装置上に存在するかを判断するため、そのユーザ装置に接続されているストレージ装置をスキャンして、そのユーザ装置上にどんなファイルが存在しているかを見つけることが必要である。既にユーザ装置上にライセンスされたファイル、または、既にそのユーザ装置上に存在するファイルの処理は、以下にさらに説明する。

【００６４】

そのラッパーの実行可能なコンポーネントが、正当なソリューションソフトウェアが現在インストールされていないと判断する場合、そのソリューションソフトウェアをインストールするオファーが、そのユーザ装置において提供される（ステップ３３０）。そのオファーは、例えば、ポップアップウィンドウ中で提供される。次に、（例えば、そのユーザがポップアップウィンドウ中でアクセプトボタンまたはディクラインボタンをクリックしたことの指示を受信することによって）、そのユーザがそのソリューションソフトウェアをインストールするオファーを受け入れるかが判断される（ステップ３３５）。ユーザ

がそのオファーを受け入れない場合、そのソリューションソフトウェアはインストールされず、そのラップされたメディアファイルへのアクセスは拒否される（ステップ３４０）。ユーザがオファーを受け入れた場合、ソリューションソフトウェアコードを蓄積している中央サーバから、または、そのラッパー中に含まれているコードから、ソリューションソフトウェアがインストールされる（ステップ３４５）。

【００６５】

一旦ソリューションソフトウェアがステップ３４５においてインストールされ、または、そのラッパーの実行可能なコンポーネントが、ステップ３２０において、ソリューションソフトウェアの正当なインストールが既に存在する（そして、ラップされたメディアファイルがそのユーザそして／またはユーザ装置によってライセンスされていると考えられる）なら、そのラップされたメディアファイルを購入またはライセンスするオファーがユーザ装置上に呈示される（ステップ３２５）。その代わりに、ユーザは、そのファイルの購入またはライセンスを実現できるウェブサイトに向かう。次に、そのユーザがその購入またはライセンスオファーを受け入れるかの判断がなされる（ステップ３５０）。もし受け入れないなら、そのラップされたファイルへのアクセスは拒否される（ステップ３４０）。

【００６６】

いくつかの実施例においては、ステップ３５０においてそのラップされたメディアファイルの購入またはライセンスのオファーが呈示されるまで、または、ステップ３５０において、そのユーザがその購入またはライセンスオファーを受け入れる後まで、そのソリューションソフトウェアはインストールされない。従って、そのラップされたメディアファイルの購入またはライセンスの提供（ステップ３２５）は、ステップ３２０においてソリューションソフトウェアの正当なインストールがユーザ装置上に見つかったかに関わらず、ステップ３４５においてそのソリューションソフトウェアのコピーがユーザ装置上に呈示される前に、ユーザ装置上に呈示される。そのような場合、そのソリューションソフトウェアは、ステップ３５０においてそのユーザがその購入またはライセンスオファーを受け入れるかの判断がされるとほぼ同時に、またはその後に、そのソリューションソフトウェアの別個のオファーと受け入れを必要とすることなくインストールされる。従って、ステップ３５０とほぼ同時にまたはステップ３５０の後に行われ、ステップ３３０と３３５は省略される。他の方法として、ステップ３３０と３３５は、プロセス３００の他のポイントにおいて行われる。

【００６７】

そのユーザが購入またはライセンスオファーを受け入れる場合、支払情報がユーザから取得されて、中央サーバに送信される（ステップ３５５）。その中央サーバは、以下にさらに説明するように、そのメディアファイルライセンスの販売と各特定の販売についての支払を受ける全ての者を追跡するマイクロ支払システムを備えている。この購入が、そのユーザがメディアファイルを購入した最初の時である場合、支払方法を含む請求情報と電話コンタクト情報を示す情報といった関連情報が入力される。さもなくば、そのユーザは、ログインして事前支払方法を用いるか、新たな支払方法を入力するかを選択できる。

【００６８】

その支払方法が処理される。その支払が失敗する場合、そのユーザは、異なる支払方法を入力して、再び試すことができる。そのユーザが再び試すことはしないことを選択し、または、オファーされた支払方法がどれも有効でない場合には、その取引はキャンセルされ、そのメディアファイルへのアクセスは、拒否される。しかし、支払が成功した場合には、そのメディアファイルはアンラップされ（ステップ３６０）、ライセンス情報が、ローカルデータベースそして／または中央サーバ中に適切に蓄積される。

【００６９】

一旦そのソリューションソフトウェアがユーザ装置上にインストールされると、そのソリューションソフトウェアは、任意のメディアファイルがプロテクトされたコンテンツを示しているかを判断するために、そのユーザ装置上の全てのメディアをチェックする（ス

テップ３６５）。このチェックは、ユーザ装置のメモリのコンテンツをスキャンすることによって、そして、知られたメディアファイルを識別するファイル識別技術を用いて行われる。次に、認識されたメディアファイルが、ラップされて、ユーザが、以下にさらに説明するように、自分自身のカタログ化されたライブラリをプロモートし、そして販売できるようにする。特定の実施例において、そのメディアファイルは、認識された時にラップされるか、ユーザがユーザ装置のＩ／Ｏシステムを通じてそのファイルを送信しようとするまでラップされない。さらに、ユーザは、ユーザがまだライセンスを持っていない任意の認識されたコンテンツについてのライセンスを購入するよう要求される。しかし、ある実施例においては、ソリューションソフトウェアがインストールされた時にユーザ装置上にすでに存在するファイルのライセンスの購入を要求することは望ましくない。なぜなら、そのユーザが合法的にそのファイルを所有しているか（例えば、そのユーザが、ソリューションソフトウェアがユーザ装置上にインストールされる前にそのファイルについて事前に支払をしているか）を判断できないからである。しかし、すでにユーザ装置上に存在しているファイルは、他の装置そして／または他のユーザに対して送信される時にラップされる。

【００７０】

図４は、ソリューションソフトウェアを備えるユーザ装置上に、デジタルラッパーなしに到着するコンテンツをラップするプロセス４００のフロー図である。最初に、図３に関して説明されるように、メディアファイルが生成される（ステップ４０５）。そのメディアファイルは、ソリューションソフトウェアを備えるユーザ装置上において、物理的または電子的なメディア配布技術を通じて、連続的に受信される（ステップ４１０）。そのソリューションソフトウェアは、そのファイルＩ／Ｏシステムを監視し、そのメディアファイルの受信を認識する。ファイル識別技術を用いて、そのソリューションソフトウェアは、例えば、メディアファイルからデジタルフィンガープリントを抽出し、そして、そのフィンガープリントを知られたメディアファイルのフィンガープリントと比較することによって、そのメディアファイルの識別を試みる（ステップ４１５）。そのメディアファイルが認識されたかの判断がされる（ステップ４２０）。認識されない場合、そのファイルは、コピーライトまたは他の権利によってプロテクトされていないと考えられ、そのメディアファイルへのアクセスが許される（ステップ４２５）。

【００７１】

そのファイルが認識された場合、そのメディアファイルが、既にそのユーザ装置上におけるそして／または特定のユーザによる使用のライセンスがなされているかが判断される（ステップ４３０）。一般に、ファイルが認識された時、ファイル識別技術が、そのメディアファイルに関する現存するＵＦＩＤを識別する。そのメディアファイルがユーザ装置上での使用がライセンスされているかを判断するため、ソリューションソフトウェアは、そのＵＦＩＤが、ライセンスされたメディアファイル用のＵＦＩＤを含んでいるローカルデータベース中に蓄積されているかを判断する。場合によっては、ユーザは、そのメディアファイルに対するライセンスを持っているが、そのライセンス情報はユーザ装置上に蓄積されていない場合がある。例えば、ユーザは、異なる装置を用いてライセンスを購入したかもしれない。メディアファイルについてのビジネスルールが特定の装置（すなわち、メディアファイルが元々ライセンスされていた装置）へのメディアファイルの使用を制限していないとすれば、または予め現在のユーザ装置におけるメディアファイルの使用を除外しているとすれば、そのメディアファイルへのアクセスは許される。従って、そのＵＦＩＤがそのローカルデータベース中に見つからなければ、中央のデータベースが、そのユーザがそのメディアファイルについてのライセンスを持っているかを判断するためにチェックされる。

【００７２】

そのメディアファイルがライセンスされていると判断された場合は、そのメディアファイルへのアクセスが許される（ステップ４２５）。ある場合には、正当なライセンスが存在すると判断され、そのファイルがそのユーザについてのライセンスデータベース中に含

まれていない場合においても、そのメディアファイルへのアクセスが許される。例えば、そのファイルがコンパクトディスク（ＣＤ）からユーザ装置上にロードされている場合、ソリューションソフトウェアは、そのＣＤが工場で作成されたものかを認識することができ、工場で作成されたものである場合は、そのファイルのコピーは合法的であるか、許されると判断するようプログラムされている。従って、そのソリューションソフトウェアは、オリジナルＣＤからのファイルのコピーを許し、オリジナルＣＤからコピーされるファイル用のライセンス情報を蓄積する（図１のステップ１４０参照）。しかし、そのソリューションソフトウェアは、また、ＣＤから受信されたファイルのさらなるコピーを防止するようにプログラムされている。特に、そのソリューションソフトウェアは、そのファイルが認識された時またはそのファイルがそのユーザ装置についてのＩ／Ｏシステムを通じて送信されていることを検知した時のいずれかの時に、ＣＤからコピーされたファイルをラップする。

【００７３】

そのメディアファイルがライセンスされていない場合には、そのユーザは、そのメディアファイルを使用するライセンスを購入する機会をオファーされる（ステップ４３５）。そのユーザが、ライセンスを購入しないと決めた場合は、そのメディアファイルへのアクセスは拒否される（ステップ４４０）。そのユーザがライセンスを購入することを決める場合には、支払情報がそのユーザから得られ、中央のサーバに対して送信される（ステップ４４５）。支払が成功した場合は、そのメディアファイルについてのライセンス情報が、ローカルデータベースそして／または中央のデータベース中に適切に蓄積される（ステップ４５０）。そのメディアファイルは、また、さらなる配布のためラップされ、そのメディアファイルがライセンスされていることを保証し、他者がそのメディアファイルにアクセスできる前に料金が適切に配布されることを保証する（ステップ４５５）。上述したように、そのメディアファイルは、直ちにラップされる。その代わりとして、そのメディアファイルは、そのユーザ装置上でアンラップされた形式のまま残り、ユーザがそのメディアファイルをそのユーザ装置についてのＩ／Ｏシステムを通じて送信しようとした時にだけラップされることもある。

【００７４】

図５は、ユーザ用のＵＣＩＤそして／またはそのユーザ装置に特有のキーを生成するプロセス５００のシグナリングおよびフロー図である。一般に、各ユーザは、一つのＵＣＩＤを持っており、そして、各ユーザ装置は、自分特有の装置キーを持っている。そのＵＣＩＤは、中央のサーバに蓄積されている、ユーザのライセンス情報にアクセスすることを目的としてそのユーザを識別するため、また、（ユーザが自分のＵＣＩＤをファイルラッパーに付加して、そのファイルを他の購入者に配布した時に）支払を識別することを目的としてファイルのソースを追跡するため、また、特定のユーザのあるユーザ装置を識別するために用いられる。特有の装置キーは、中央サーバがその特定の装置を識別できるようにするためと同様に、ローカルライセンスデータベースをアンロックし、そして／またはそのローカルデータベースにアクセスするために用いられる。そのＵＣＩＤと特有のユーザ装置キーは、また、一つを他に単に付加することによって、または、いくつかのタイプのコーディングアルゴリズムに従ってそのキーを混合することによって、組み合わせられたキーにマージされる。ＵＣＩＤとその特有のユーザ装置キーの組み合わせは、特定のユーザの特定のユーザ装置を識別するために（そして、例えば、その中央のサーバが、どの装置がライセンスされたファイルを有しているかを追跡できるようにするために）用いられる。

【００７５】

プロセス５００は、ユーザ装置５０５、ユーザ装置５０５用のＢＩＯＳ５１０、中央サーバ５１５、そして中央データベース５２０上でのオペレーションとそれらの間での通信を有する。ユーザ装置５０５上におけるソリューションソフトウェアのインストールが開始される（ステップ５２２）。その結果、ユーザ装置５０５は、中央サーバ５１５にソリューションソフトウェアのリクエスト５２４を送信する。リクエスト５２４に対する応答

において、ソリューションソフトウェアが中央サーバ５１５からユーザ装置５０５に対してダウンロード５２６される。リクエスト５２４を送信し、ダウンロード５２６を実行する代わりに、そのソリューションソフトウェアは、（例えば、ユーザ装置５０５上に配置されているファイルからまたはディスクから）ローカルにロードされる。そのユーザは、そのソリューションソフトウェア用のライセンスアグリーメントのタームと条件との受け入れを開始し、ライセンスアグリーメントの受け入れが受信される（ステップ５２８）。

【００７６】

ユーザ装置５０５上にロードされたソリューションソフトウェアは、ユーザに関連する情報を収集するのに必要な実行可能なコードを有している（ステップ５３０）。その情報のいくつかは自動的に収集され、他の情報は、ユーザによってマニュアルで入力される。例えば、ユーザは、独特のユーザ名または「ハンドル」、パスワード、電子メールアドレス、そして他のユーザ入力情報の入力を開始する。この情報は、ユーザのライセンスと中央データベース中に蓄積されている他の情報にアクセスするために、そして／または、多数のユーザによって共有されているユーザ装置５０５において、ユーザに特有のローカルデータベースにアクセスするために用いられる。自動的に収集された情報は、ユーザ装置に特有の情報（例えば、システムユニバーサルユーザＩＤ、ＣＰＵＩＤ、ＭＡＣアドレス、ＢＩＯＳブートブロック）とローカルデータベースについてのアクセスおよびロケーション情報を含んでいる。

【００７７】

ユーザ装置５０５上にロードされたソリューションソフトウェアは、また、ユーザ装置５０５と中央サーバ５１５との間のコネクションを確立するために必要な実行可能コードを含んでいる。典型的には、ユーザ装置５０５と中央サーバ５１５との間のインターネットコネクションは、自動的になされる。自動的にコネクションできない場合は、マニュアルプロセスが開始されて、ユーザに（モデム、ネットワークなどを用いて）コネクションを開始させる。インターネットコネクションがなされない場合は、そのインストールは中止となり、そのような場合、ステップ５３０において収集された情報は、その後にインターネットコネクションが可能となった時にＵＣＩＤと特定の装置キーとをインストールするために蓄積される。そのソリューションソフトウェアが中央サーバ５１５からインストールされている場合には、ソリューションソフトウェアのインストールは、ステップ５２２、５２４および５２６において中止される。インターネットコネクションが、セキュアソケットレイヤ（ＳＳＬ）といったセキュアなチャネルを介して行われる。

【００７８】

中央サーバ５１５に対して送信された情報は、このセキュアなチャネル上で送信され、その情報には、（ＳＳＬコネクションによって提供される暗号化に加えてＰＧＰを用いて）さらなる暗号化がなされる。中央サーバ５１５に送信されたメッセージは、成功または失敗コードを伴って返される。プログラムで決められたリーズナブルなタイムフレーム内に返答が受信されない送信メッセージは、失敗したと考えられる。確立されたコネクションを用いて、ステップ５３０において収集されたユーザ情報は、５３４において中央サーバ５１５に対して送信される。

【００７９】

中央サーバ５１５は、５３６において、中央データベース５２０をサーチして、そのユーザが既に知られているかを調べる。そのユーザが既に知られているかの判断は、１または複数のユーザ情報のデータアイテムと、中央データベース５２０において蓄積されている知られているデータアイテムとを比較することを含む。例えば、そのユーザの名前が既に中央のデータベース５２０に存在するがそのパスワードが合致しない場合、そのユーザは、正しいパスワードを用いてログインすることを促されるか、そして／またはそのユーザの名前が既に使用されていることを知らされる。

【００８０】

そのユーザがまだ知られていない場合、中央のサーバ５１５は、ＵＣＩＤそして／または装置キーを生成する（ステップ５３８）。ＵＣＩＤと装置キーは、受信された装置に特

有の情報、ユーザ入力から受信されたユーザ情報、受信されたローカルデータベースについてのアクセスおよびロケーション情報、中央サーバ５１５によって生成されたデータ、日付と時間に関する情報、または取引に関する他の情報を含む、様々な利用可能なデータアイテムから選択された、選択された数のデータアイテムの組み合わせによって生成される。上述したように、ＵＣＩＤは、特定の装置キーと組み合わせられて、組み合わせキーを生成する。どのデータアイテムが用いられ、どのようにしてデータアイテムが組合わせられるかは、中央サーバ５１５内に蓄積されたアルゴリズムによって決定される。中央サーバ５１５においてＵＣＩＤ、装置キーそして／または組み合わせキーを生成することによって、ＵＣＩＤ、装置キーそして／または組み合わせキーを生成するアルゴリズムは、セキュアに保持され、ユーザが偽のＵＣＩＤ、装置キー、組み合わせキーを生成できないようにする。さらに、ＵＣＩＤ、装置キー、組み合わせキーそして／またはＵＣＩＤ、装置キー、組み合わせキーを生成するアルゴリズムのリバースエンジニアリングは、さらに、ユーザ装置５０５から受信された、全てには満たないユーザの情報そして／またはそのＵＣＩＤの生成に用いられるいくつかのデータアイテムをランダムに選択することによって、そして、そのＵＣＩＤをユーザ装置５０５に送信する前にそのＵＣＩＤを暗号化することによって、防止される。

【００８１】

そのＵＣＩＤ、装置キー、組み合わせキーそして／または追加的なマシーン特有の情報は、他のユーザ情報とともに、中央データベース５２０中に５４０において蓄積される。ＵＣＩＤ、装置キーそして／または組み合わせキーは、また、暗号化され（ステップ５４２）、その暗号化されたＵＣＩＤ、装置キーそして／または組み合わせキーは、５４４において、その暗号化されたＵＣＩＤ、装置キーそして／または組み合わせキーをＢＩＯＳ５１０中に蓄積するユーザ装置５０５に対して送信される。そのキーは、パーツに分けられ、そのキーの様々なパーツは、そのＢＩＯＳ中のセパレートロケーション中に蓄積される。ＵＣＩＤ、装置キーそして／または組み合わせキーは、クライアントマシーンと中央サーバとの間のメッセージを暗号化するために連続的に用いられるパブリックキーを表している。ローカルライセンスデータベースがユーザ装置５０５において生成される（ステップ５４８）。例えば、ソリューションソフトウェアコードの一部は、ユーザ装置５０５上に暗号化されたライセンスデータベースを生成するように動作する。データベースそして／またはそのデータベース中に蓄積される情報を暗号化することによって、そのデータベース中に含まれる情報が、適切なキーが用いられない限りリードできないようにする。一般に、そのライセンスデータベースは、ユーザ装置５０５のハードドライブ上に、ＢＩＯＳ５１０中に蓄積されたロケーションポインタを持って生成されるが、そのライセンスデータベースは、また、ＢＩＯＳ５１０中にも生成される。１または複数のロケーションポインタを持つ暗号化されたＵＣＩＤと装置キーそして／または組み合わせキーは、拡張されたデータ構造を蓄積するために、デスクトップマネジメントインタフェース（ＤＭＩ）といった産業標準プロセスを用いて、そのＢＩＯＳ中に書き込まれる。

【００８２】

消費者は、多数の装置を持っていることが多く、ライセンスされたファイルを様々な装置上で使用することを望む。従って、ある状況では、プロセス５００が新たな装置上で既にＵＣＩＤを持っているユーザによって開始される。ＵＣＩＤ、ユーザネームとパスワード、そして／または他の識別情報に基づいて、中央サーバ５１５は、そのユーザが既にサーチ５３６において既に知られていると判断する。そのユーザは、また、他の装置にソリューションソフトウェアをインストールし、そして、自分のユーザネームとパスワードを用いてログインすることができる。その中央サーバ５１５は、新たなＵＣＩＤを生成することなく新たな装置キーを生成し（ステップ５３８）、そして、その組み合わせキーを新たな装置情報を用いて更新する。このようにして、その組み合わせキーは、ユーザによって所有されまたは使用される全ての装置についての、装置に特有の情報（例えば、特定の装置キー）を伴うＵＣＩＤを含んでいる。

【００８３】

その組み合わせキーが中央データベースによって受信されると、その組み合わせキーは、中央サーバによって、そのユーザを識別するために、そして、そのユーザ装置がそのユーザにとって新たな装置か既知の装置かを判断するために、（組み合わせキーのＵＣＩＤ部分を用いて）復号される。その装置が新たな装置である場合、その新たな装置が、登録されたユーザについての既知の装置のリストに追加され、その装置は、個々のファイル用のライセンス許諾内容（例えば、メディアファイルが追加的なライセンスの購入なしに使用される、異なる装置の数）に基づいて、データファイルを使用できる。そのＵＣＩＤそして／または更新された組み合わせキーは（新たな装置キーと同様に）、その装置がその特定のユーザに関連付けられるように、その新たな装置のＢＩＯＳに追加される。そのＵＣＩＤそして／または更新された組み合わせキーは、また、それらの装置がその中央サーバに接続した次の時に、そのユーザの別の装置のＢＩＯＳに追加される。特定の装置は、また、各ユーザがセパレートライセンスデータベースを持っており、そのセパレートデータベースがユーザネームとパスワードとを用いて区別されるような場合には、多数のユーザと関連付けられる。さらに、ソリューションソフトウェアを持っていないが、ローカルデータベース中のライセンスライブラリまたは中央データベース５２０と通信が許されている装置は、そのライセンスライブラリ中に配置するライセンス情報に基づいてライセンスされたファイルの使用を許可される。

【００８４】

ある場合においては、ユーザは、例えば、借りた装置を用いて一時的にライセンスされたファイルへのアクセスが許される。例えば、ユーザは、友人の家において音楽ファイルを聞きたい場合がある。そのような場合、装置が一時的に追加的な装置として（例えば、日／時の期限とともに）追加され、そのファイルは、その装置上での一時的なライセンスを許されるか、または、そのファイルは、ストリーミングフォーマットでその装置に対して提供される。しかし、ユーザが、他の者がライセンスにアクセスすることを許すことがないようにするため、ユーザは、ある時において同時期にログインする者に限定され、そして／またはそのような一時的なライセンスは、限られた時間においてまたはある時における一つの装置のみに限定される。

【００８５】

図６は、ユーザが既にメディアファイルについてのライセンスを持っている場合にメディアファイルにアクセスするプロセス６００のシグナリングおよびフロー図である。プロセス６００は、ユーザ装置６０５、ユーザ装置６０５についてのＢＩＯＳ６１０、ローカルデータベース６１５、中央サーバ６２０、そして中央データベース６２５におけるオペレーションまたはそれらの間での通信を有している。ユーザ装置６０５は、図３のステップ３１５において、ラップされたファイルを受信する。ユーザがそのラップされたファイルを開こうとすると、実行可能なラッパーコードがユーザ装置６０５上で動作する（ステップ６３０）。実行可能なコードは、ユーザ装置６０５にソリューションソフトウェアの正当なインストールがあるかのファーストチェックをさせる（ステップ６３５）。正当なインストールが見つかった場合、その実行可能なコードは、ユーザ装置６０５に、ソリューションソフトウェアがインストールされた時にキーが書き込まれるＤＮＩテーブルをメモリリードすることを含む、ＢＩＯＳ６１０中に正当なＵＣＩＤ、装置キー、そして／または組み合わせキーがあるかのチェックをさせる（ステップ６４０）。

【００８６】

正当なＵＣＩＤ、装置キーそして／または組み合わせキーが見つかった場合は、ユーザ装置６０５上のソリューションソフトウェアは、ファイルライセンスリクエスト６４２を送信することによって、ローカルデータベース６１５内のラップされたファイルへのライセンスがあるかをチェックする。このサーチは、デジタルラッパー中に含まれるメディアファイルのＵＦＩＤを識別し、そのＵＦＩＤをローカルデータベース６１５内に配置することによって行われる。ローカルデータベース６１５は、ＢＩＯＳ内に蓄積されている１または複数のキーからの独特のマシン情報を実際の独特のマシン情報と比較することによってアンロックされる。その情報が合致する場合は、ソリューションソフトウェアは、ラ

イセンス情報をリードするためにそのローカルデータベースを復号する。その情報が合致しない場合は、そのキーは、（例えば、そのライセンスデータベースの許可されていないコピーを別の装置に対して行うために）そのローカルデータベースを復号しようとする試みが失敗するように設計されており、そのような場合には、中央サーバ６２０にコンタクトして、許可を取得しまたはユーザ装置６０５を登録する必要がある（図５参照）。ローカルデータベース６２５そして／またはローカルデータベース６２５中に含まれるライセンス情報の復号は、ＢＩＯＳ中に蓄積されているデジタルキーを用いて、ローカルデータベース６２５とそのコンテンツをアンロックするために行われる。

【００８７】

ローカルデータベース６２５の復号が成功する場合、必要なライセンス情報または、そのファイルがユーザ装置６０５において現在ライセンスされていないことを示す表示を含むレスポンス６４４が、ユーザ装置６０５に対して返される。そのライセンス情報が返された場合、そのファイルへのアクセスは、許される（ステップ６８５）。一方、ローカルデータベース６２５にアクセスするためには、ユーザ装置６０５が許可された装置であるかを判断すること、そして／または正当なライセンスが存在するかを判断することが必要である。中央サーバ６２０そして／または中央データベースがアクセスされる時にはいつでも、その通信が正当な、許可されたユーザ装置６０５を含んでいることを保証するために、ユーザ装置において蓄積されているキーを中央データベース６２５内に蓄積されている情報に照らしてテストすることが必要である。以下のステップは、組み合わせキーのテストを説明している。組み合わせキーが用いられているが、他の実施例は、ＵＣＩＤ、装置キーそして／または他の情報を用いる。組み合わせキーがＢＩＯＳ６１０内に見つかった場合、その見つけられたキーが、６４５において中央サーバ６２０に対して送信され、付加的なマシン特有の情報（すなわち、その情報またはその組み合わせキーを元々生成するために用いられた情報）とともに認証される。中央サーバ６２０は、ＵＣＩＤを取得するために、その受信された組み合わせキーを復号し（ステップ６５０）、装置情報を埋め込む。中央サーバは、さらに、復号された組み合わせキーについてのチェックサムの計算を行う（ステップ６５５）。中央サーバは、次に、復号された組み合わせキーを中央データベース中に蓄積されている情報に照らして認証する（ステップ６６０）。その組み合わせキーの認証は、チェックサムを用いた計算を含む。その復号された組み合わせキー、ＵＣＩＤ、そしてマシーン情報が中央データベース内に蓄積されている情報と合致する場合には、実行の許可６６５がユーザ装置６０５に対して送信され、その組み合わせキーの認証が成功したことを示す。その組み合わせキーが偽のものであったり他の装置からコピーされたものであったりする場合には、その組み合わせキーと一緒に送信されたマシーン特有の情報は、復号されたキー内に含まれる情報そして中央サーバ内に蓄積されている情報と合致しない。

【００８８】

ローカルデータベース６２５に対してコネクトされた時に、１セッションに１回用いられる許可６６５に対するレスポンスにおいて、その実行可能なコードは、ユーザ装置６０５に、そのメディアファイル用のＵＦＩＤをローカルデータベース６１５中に配置することによって、ローカルデータベース６１５内のメディアファイルへのライセンスをサーチさせる（ステップ６７５）。もし、例えば、そのローカルに蓄積されているキー情報が破壊されたが許可６６５を通じて更新された場合には、このサーチは、（６４２における）オリジナルのサーチが成功しなかった場合でも成功する。そのＵＦＩＤがローカルデータベース６１５中に見つからない場合、ローカルデータベース６２５は、ＵＦＩＤについてサーチされる。そのＵＦＩＤがローカルデータベース６２５において見つかる場合には、６８０において、そのローカルデータベースは、ライセンス情報を用いて更新される。ライセンスが配置されているとすると、そのメディアファイルの使用は許可される（ステップ６８５）。例えば、ソリューションソフトウェアは、メディアプレイヤーアプリケーションが、リクエストされた音楽ファイルにアクセスできるようにする。ある実施例においては、一旦メディアファイルが特定のユーザ装置６０５において使用することが許された

場合、そのメディアファイルは、ラップされていない形式でユーザ装置６０５上に蓄積される。そのラッパーは、ソリューションソフトウェアが、そのメディアファイルがユーザ装置６０５から他の装置またはストレージ媒体に対してコピーされまたは移動されたことを検知した時に、そのソリューションソフトウェアによってのみ再び適用される。その検知の判断は、上述したように、ファイルＩ／Ｏシステムを監視することによって行われる。他の実施例においては、そのメディアファイルは、ラップされた形式でユーザ装置６０５上に蓄積され、そのメディアファイルが開かれるたびにローカルデータベース６１５内に蓄積されているライセンス情報を用いてアンラップされる。

【００８９】

図７は、ユーザがメディアファイル用のライセンスを持っていない場合にメディアファイルにアクセスするプロセス７００のシグナリングおよびフロー図である。プロセス７００は、ユーザ装置７０５、ローカルデータベース７１５、中央サーバ７２０、そして中央データベース７２５におけるオペレーションまたはそれらの間での通信を有している。プロセス７００は、そのユーザがメディアファイル用のライセンスを持っていないとの判断から開始される（ステップ７３０）。この判断は、図６のステップ６７５における、ライセンスのサーチの失敗の結果である。この判断に対するレスポンスにおいて、ユーザ装置７０５は、７３５において、中央サーバ７２０に対してライセンスが必要とされることを通知する。中央サーバ７２０は、ユーザ装置７０５上に表示される支払リクエスト７４０を返すか、ユーザは支払情報が得られるウェブサイトに向かう。ユーザ装置７０５は、ユーザから支払情報を受信し（ステップ７４５）、その支払情報を中央サーバ７２０に対して送信する。その支払情報については、どのくらいのライセンス料がコンテンツオーナーそして／またはそのメディアファイルを配布した１または複数のユーザに対して配分されるかを決定することを含む処理がなされる（ステップ７５５）。その中央データベース７２５は、７６０において、そのユーザがそのメディアファイルに対するライセンスを持っていることを示す情報を用いて更新される。中央データベース７２５は、また、支払配分情報を用いて更新される。さらに、ローカルデータベース７１５は、７６５において、そのユーザがそのメディアファイルへのライセンスを持っていることを示す情報を用いて更新される。その更新されたライセンス情報に基づいて、そのユーザは、ユーザ装置７０５上においてそのメディアファイルの使用が許される（ステップ７７０）。

【００９０】

いくつかの装置は、例えば、その装置がインターネットに対して簡単にはコネクトできない場合には、中央サーバと直接通信することはできない。メディアファイルは、そのメディアファイルがラッパーなしに他の装置に対してさらに送信されることがないような方法で、そのような装置に対して送信される。そのような状況においては、コンピュータコードの部分は、ファームウェア内にインストールされ、スモールローカルデータベースが、その装置の書き込み可能メモリ内にインストールされる。図８は、ユーザ装置８０５から第２の装置８１０に対してメディアファイルをコピーまたは移動させるプロセス８００のシグナリングおよびフロー図である。プロセス８００は、ユーザ装置８０５、第２の装置８１０、ローカルデータベース８１５、第２の装置データベース８２０、そして中央サーバ８２５におけるオペレーションまたはそれらの間での通信を有している。第２の装置８１０は、例えば、衛星接続カーオーディオシステム、ＭＰ３プレイヤー、または他のポータブル装置であり、ＩＥＥ１３９４ファイアワイヤまたはＵＳＢケーブルそしてそれらに限定されないケーブルを用いて、そのユーザ装置に対してコネクトし、または、無線コネクションを介して接続され得る。ソリューションソフトウェアのバージョンは、第２の装置８１０上に（例えば工場において）予めインストールされる。

【００９１】

メディアファイルの送信リクエストが、ユーザ装置８０５によって受信される（ステップ８３０）。レスポンス中において、ユーザ装置８０５は、８３５において、第２の装置８１０からの装置ＩＤをリクエストする。第２の装置は、装置ＩＤを伴う応答８４０を返す。ユーザ装置８０５は、そのメディアファイル用のラッパー中に含まれるビジネスルー

ルが、リクエストされた送信を許すかを確認する（ステップ８４５）。例えば、そのビジネスルールは、メディアファイルがコピーされ得る装置の数に制限を置いている。その送信が許可されるとすると、そのラップされたメディアファイルと、対応するライセンス情報が、８５０において第２の装置８１０に対して送信される。第２の装置８１０は、そのライセンス情報を第２の装置データベース８２０内に蓄積する（ステップ８５５）。そのライセンス情報は、予めインストールされたソリューションソフトウェアとともに、第２の装置８１０がそのラップされたメディアファイルにアクセスできるようにする。さらに、ユーザ装置８０５は、ローカルデータベース８１５内のローカルライセンス情報を更新する（ステップ８６０）。この更新は、そのメディアファイルのコピーが第２の装置８１０に対して送信されたことを示す情報を蓄積する。

【００９２】

続いて、８６５において、ユーザ装置８０５と中央サーバ８２５との間のコネクションが確立される。このコネクションは、新たなメディアファイルへアクセスする試み、ライセンス情報を配置する試み、または、ユーザ装置８０５がライセンスの使用を継続するために、定期的にローカルデータベース８１５内に蓄積されたライセンスを認証する要求へのレスポンスに応じて確立される。そのコネクションを用いて、ローカルデータベース中に蓄積されたライセンス更新は、８７０において中央サーバ８２５にアップロードされ（そして中央データベース中に蓄積され）、中央サーバがメディアファイルのコピーが置かれている装置を追跡し、そしてメディアファイルが、そのビジネスルールの下で許されるより多くの装置においてコピーされないようにできるようにする。中央サーバ８２５は、また、８７５において、ローカルデータベース８１５中に蓄積された現存するライセンスを認証する。

【００９３】

メディアファイルをユーザからユーザに配布することをサポートし、ユーザが他の者に対してメディアファイルを配布した結果生み出された利益を享受できるようにする技術が提供される。ユーザは、彼が所有しまたは楽しんでいるメディアファイルに関する他のユーザの情報を電子的に送信する。パスアロングの結果として販売が行われると、ユーザは、そのメディアファイルの販売そしてそのメディアファイルのその後の販売から生成される利益のあるパーセンテージを取得する。メディアファイルラッパーは、ユーザが、認識された再販売者と配布者からメディアファイルを受信した時にオリジナルの再販売者と配布者を識別する情報を、そのメディアファイルをさらに配布するユーザを識別する情報と同様に含んでいる。そのファイルに関するビジネスルールに基づいて、この情報は、再販売者とそのユーザが、メディアファイルが送信された時になされる購入の見返りを受けられるようにする。さらに、ファイルがアンラップされて送信または受信される場合、該当するユーザ、再販売者、そして配布者は、彼らの独特の識別子がその取引データ中に含まれている限り、見返りを受ける。例えば、購入者が該当するユーザを識別することが可能となり、そのような場合、中央サーバは、どのようにしてその該当ユーザがそのファイルを受信したかを判断し、誰がその利益の配分を受けるかを識別することを含む、配布チェーンの再構築を行う。

【００９４】

ビジネスルールは、そのメディアファイルをライセンスされていないユーザがまだそのメディアファイルの再配布から利益を受け得るかを決定する。例えば、ユーザは、再販売ポイントとして動作するサーバ上にファイルを収め、そのユーザが、自分が配布しているファイルについてのライセンスを持っていない場合においても、パスアロング参加料の支払を受ける。

【００９５】

誰かがファイルを友人に送信するプロセスを開始すると、そのソリューションソフトウェアは、そのメディアファイルの新たにラップされたバージョンを生成し、そのメディアファイルをパスアロングプロセスに供する。この新たなラッパーは、そのメディアファイル用のＵＦＩＤ、そのメディアファイルに適用されるビジネスルール、そして始めのユー

ザ（またはユーザ達）についてのＵＣＩＤを含んでおり、そのユーザ（またはユーザ達）が、受信ユーザによって購入された歌をプロモートした時に見返りを受け得るようにする。再販売者と配布者ＩＤ情報もまた、そのラッパー中に含まれている。ソリューションソフトウェアは、ユーザ装置がＣＤまたはＤＶＤをリップするために用いられた時にこの同じプロセスを実行する。例えば、ＣＤ上の歌がコンピュータ上にリップされる時は、その歌についてのライセンスがライセンスデータベース中にインストールされる。続いて、その歌がそのコンピュータのＩ／Ｏシステムを通じて送信される場合、ラッパーがその歌に適用される。そのラッパーは、リップされたファイル中に含まれる歌識別情報に基づいて、または、上述したファイル識別技術を用いて取得された識別情報に基づいて、その中央データベースから取り出される、ライセンス情報と支払情報を含んでいる。その歌がＣＤ上に焼かれる場合、ラップされたファイルがそのＣＤに対して書き込まれる。その代わりに、ソリューションソフトウェアは、再販売者と配布者の情報に関するＵＦＩＤとＵＣＩＤといったメディア情報ファイルをそのＣＤのＰＣ読み取り可能なエリア内に含むデュアルセッションＣＤを生成することができる。デュアルセッションＣＤフォーマットでは、従来のオーディオファイルがそのＣＤのオーディオセッションにおいて許可され、そのＣＤが従来のＣＤプレイヤー上で再生できるようにする。一方、そのファイルがそのソリューションソフトウェアがインストールされている装置中にロードされる場合、そのファイルは、ライセンスを必要とする。

【００９６】

図９は、パスアロング配布を実行する代表的なプロセス９００のフロー図を示す。最初に、ユーザ２は、ユーザ１からメディアファイルを受信する（ステップ９０５）。ユーザ２はユーザ１から受信したメディアファイルについてのライセンスを購入する（ステップ９１０）。その支払プロセスに関連して、そのメディアファイルに関するビジネスルールが調べられる（ステップ９１５）。この調査は、ユーザ装置、中央サーバ、または別のロケーションにおいて実行される。次に、ユーザ１は、そのビジネスルールによって特定される額の手数料を受け取る（ステップ９２０）。その手数料は、中央サーバによって管理されるマイクロ支払アカウントに与えられ、そのメディアファイルライセンスの将来の購入用としてユーザ１に与えられ、または、マイクロ支払システムを通じてユーザ１の銀行口座に置かれる。

【００９７】

続いて、ユーザ３がユーザ２からメディアファイルを受信する（ステップ９２５）。ユーザ３は、ユーザ２から受信したメディアファイルについてのライセンスを購入する（ステップ９３０）。支払プロセスに関連して、そのメディアファイルに関するビジネスルールが再び調査される（ステップ９３５）。ユーザ１とユーザ２は、次に、そのビジネスルールによって特定される額の手数料を受け取る（ステップ９４０）。従って、多数のレベルの支払がそのメディアファイルの配布に対して行われる。

【００９８】

ある実施例においては、中央サーバは、ユーザのパスアロング動作からの預金口座のような全てのアカウントを与え、追跡する。全てのアカウントホルダーは、追加的な音楽に対する支払において、または電子ファンド移送（ＥＦＴ）を介したマネタリーファンドとして送信される回収手段として、または他の適当な手段として、自分のファンドを追跡し、使用することができる。これは、ユーザ、再販売者、配布者、そしてレコード会社、出版社そしてアーティストといったコンテンツマネージャを含む収益ストリームに参加する全ての者に適用される。支払レベルの数と各レベルに対する支払額は、ファイルの所有権を持っている者（通常はコピーライトホルダーまたは出版者）によってＵＦＩＤの生成において設定され、ビジネスルールによって異なる。

【００９９】

図１０は、メディアファイルをラップするプロセス１０００のフロー図である。そのプロセスは、ラップされるメディアファイルの選択から開始される（ステップ１００５）。そのメディアファイルに関連するビジネスルールが特定される（ステップ１０１０）。そ

のビジネスルールは、支払情報とそのメディアファイルの使用とコピーの制限に関する情報を含んでいる。ＵＦＩＤがそのメディアファイルについて生成される（ステップ１０１５）。そのＵＦＩＤは、ビジネスルールを組み込み、そして／または中央データベース中に蓄積されているビジネスルールへのポインタとして役立つ。一般に、ＵＦＩＤは、作品の特定のコピーがラップされているかラップされていないかに関わらず、特定の作品（例えば、特定のアーティストによる特定のレコーディング）に関連している。従って、ファイル識別技術がメディアファイルを特定するために用いられる場合、認識されたメディアファイルはそのメディアファイルに対応する特定のＵＦＩＤを持っている。次に、そのＵＦＩＤを組み込んでいるラッパーがそのメディアファイルに適用される（ステップ１０２０）。そのラッパーは、ユーザが唯一そのメディアファイルに対するライセンスを用いてそのラッパーを取り除くことができるように、そのメディアファイルの暗号化を含む。ソリューションソフトウェアは、一般に、そのラッパーなしにファイルが移動するのを防止するが、ユーザが標準オーディオＣＤを焼いて、そのＣＤのコンテンツがその後別のコンピュータにリップされるような、ラッパーなしにファイルが移動される状況が存在する。ファイルがラッパーなしに移動される場合、そのファイルを識別して中央データベース中のＵＦＩＤとそのビジネスルールをルックアップするために認識技術が用いられ得る。

【０１００】

説明された技術は、デジタル電子回路、集積回路またはコンピュータハードウェア、ファームウェア、ソフトウェアまたはそれらの組み合わせにおいて実装される。その技術を実行する装置は、プログラマブルプロセッサによって実行されるマシーン読み取り可能なストレージ装置において明確に具体化されるソフトウェア製品（例えば、コンピュータプログラム製品）において実装され、プロセッシングオペレーションは、入力データ上で操作して出力を生成することによって説明された機能を実行する命令プログラムを実行するプログラマブルプロセッサによって実行され得る。その技術は、データストレージシステムからデータとの間で命令を送受信するために接続された、少なくとも一つのプログラマブルプロセッサ、少なくともひとつの入力装置、少なくとも一つの出力装置を含むプログラマブルシステムにおいて適切に実装され得る。各ソフトウェアプログラムは、高水準の手続言語またはオブジェクト指向のプログラミング言語、そして、望ましい場合には、アセンブリまたは機械言語において実装され、いずれの場合にも、その言語はコンパイル言語またはインタープリタされた言語である。

【０１０１】

適合するプロセッサは、例えば、一般的または特定の目的のマイクロプロセッサを含む。一般に、プロセッサは、リードオンリーメモリ、ランダムアクセスメモリ、そして／またはマシーン読み取り可能な信号（例えば、ネットワークコネクションを通じて受信されたデジタル信号）からデータと命令を受信する。一般に、コンピュータは、データファイルを蓄積するひとつまたは複数の大容量のストレージ装置を含んでおり、そのような装置は、内部のハードディスクと着脱可能なディスク、光磁気ディスク、そして光ディスクといった磁気ディスクを含んでいる。ソフトウェアプログラムの命令とデータを明確に具体化するために適したストレージ装置は、例えば、ＥＰＲＯＭ（電子的プログラマブルリードオンリーメモリ）、ＥＥＰＲＯＭ（電子的消去可能プログラマブルリードオンリーメモリ）といった半導体メモリ装置、フラッシュメモリ装置を、内部ハードディスクと着脱可能なディスクといった磁気ディスク、光磁気ディスク、そしてＣＤ－ＲＯＭディスクを含むあらゆる形式の不揮発性のメモリを含んでいる。上述した任意のものは、ＡＳＩＣＳ（アプリケーション特有の集積回路）によって拡張され、または組み込まれる。

【０１０２】

ある実施例においては、ファイルが表示され、再生され、または配信されているユーザ装置は、ソリューションソフトウェアそして／またはローカルライセンスデータベースを蓄積し得るローカルストレージ媒体またはメモリを持っていない。そのような場合、そのファイルは、そのユーザ装置に対して配信されるか、または、一時的にそのユーザ装置上に蓄積される。従って、ソリューションソフトウェアが動作し、そのファイルに対するア

クセスをコントロールするプロセッサは、リモートに配置される。そのようなリモートプロセッサは、情報をローカルに蓄積できないユーザ装置についてのプロキシとして役立つ。

【０１０３】

ユーザとのインタラクションを提供するため、その技術は、ユーザに対して情報を表示するためのモニタまたはＬＣＤ（リキッドクリスタルディスプレイ）スクリーンそして、キーボードそしてユーザがコンピュータシステム、または入力可能で音声やシンボルを通じて情報を提供できるマウスまたはトラックボールといったポインティング装置、またはブレイル入力出力システムといった他の手段を備えるコンピュータシステムにおいて実装される。コンピュータシステムは、コンピュータプログラムがユーザとインタラクトするグラフィカルユーザインタフェースを提供するようにプログラムされ得る。音声入出力といった新たな技術を用いれば、説明した技術を実装するビジュアルディスプレイは必要でなくなる。

【０１０４】

多くの実施例が説明された。しかし、様々な変形例があることが理解されるべきである。例えば、図１と図３から１０において示されるプロセスのステップは、再配置されるかそして／またはあるステップは省略され得る。従って、他の実施例は以下のクレームの範囲を逸脱しない。

【０１０５】

様々な描写における同様の参照シンボルは、同様の要素を示している。

【図面の簡単な説明】

【０１０６】

【図１】コンピュータといったユーザ装置にロードされるファイルに対するデジタル権利の管理プロセスのフロー図である。

【図２】デジタル権利を管理するシステム例のブロック図である。

【図３】ユーザ装置上に、プロテクトされたファイルへのアクセスをコントロールするソフトウェア（「ソリューションソフトウェア」）をインストールするプロセスのフロー図である。

【図４】ソリューションソフトウェアを備えるユーザ装置においてデジタルラッパーなしに到着するコンテンツをラップするプロセスのフロー図である。

【図５】ユーザ用の独特の顧客識別子そして／またはそのユーザ装置に特有のキーを生成するプロセスのシグナリング及びフロー図である。

【図６】ユーザが既にメディアファイルに対するライセンスを持っている場合に、メディアファイルにアクセスするプロセスのシグナリング及びフロー図である。

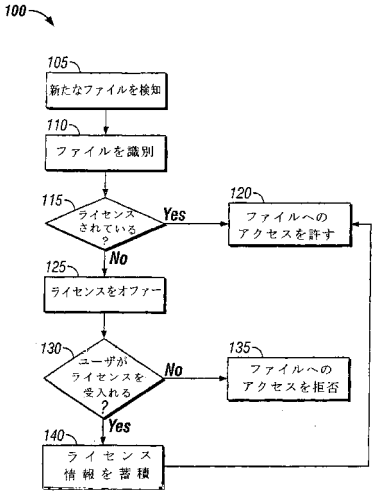
【図７】ユーザがメディアファイルについてライセンスを持っていない場合の、メディアファイルにアクセスするプロセスのシグナリング及びフロー図である。

【図８】ユーザ装置から第２の装置に対してメディアファイルをコピーまたは移動するプロセスのシグナリング及びフロー図である。

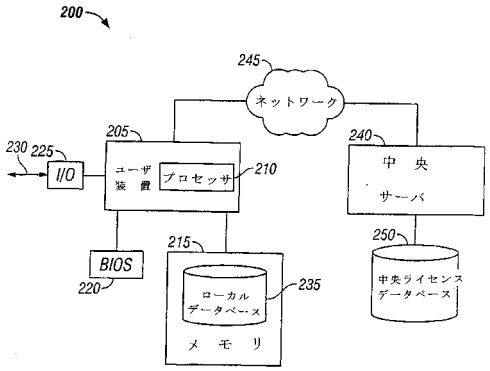
【図９】パスアロング配布を実行するプロセスを示すフロー図を示す。

【図１０】メディアファイルをラップするプロセスのフロー図である。

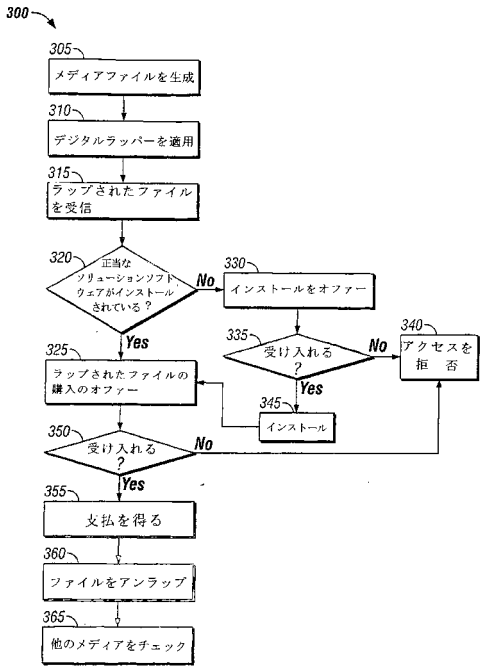
【図１】


100
105
新たなファイルを検知
110
ファイルを識別
115
ライセンスされている？
Yes
120
ファイルへのアクセスを許す
No
125
ライセンスをオファー
130
ユーザがライセンスを受入れる？
No
135
ファイルへのアクセスを拒否
Yes
140
ライセンス情報を蓄積

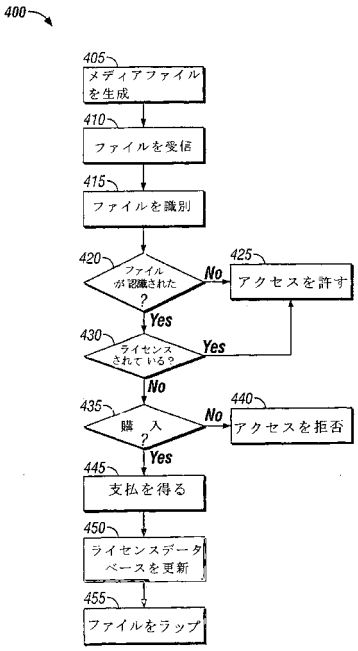
【図２】


200
245
ネットワーク
205
230
225
I/O
ユーザ装置
プロセッサ
210
240
中央サーバ
250
中央ライセンスデータベース
BIOS
220
215
ローカルデータベース
235
メモリ

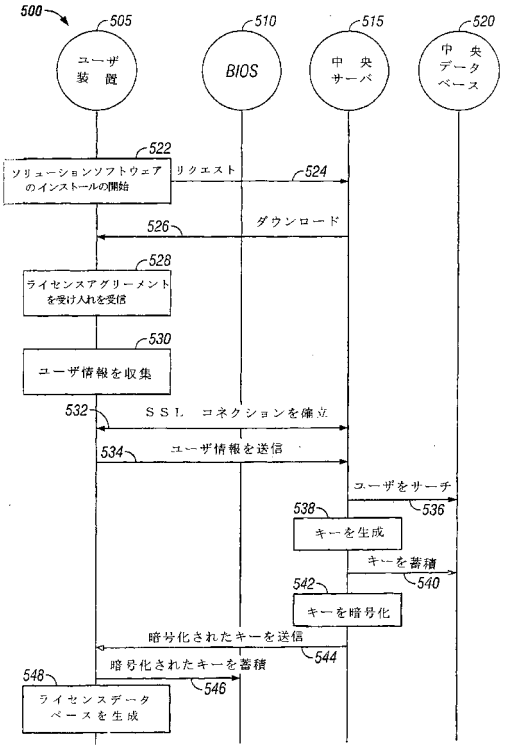
【図３】


300
305
メディアファイルを生成
310
デジタルラッパーを適用
315
ラップされたファイルを受信
320
正当なソリューションソフトウェアがインストールされている？
No
330
インストールをオファー
Yes
335
受け入れる？
No
340
アクセスを拒否
Yes
325
ラップされたファイルの購入のオファー
345
インストール
350
受け入れる？
No
Yes
355
支払を得る
360
ファイルをアンラップ
365
他のメディアをチェック

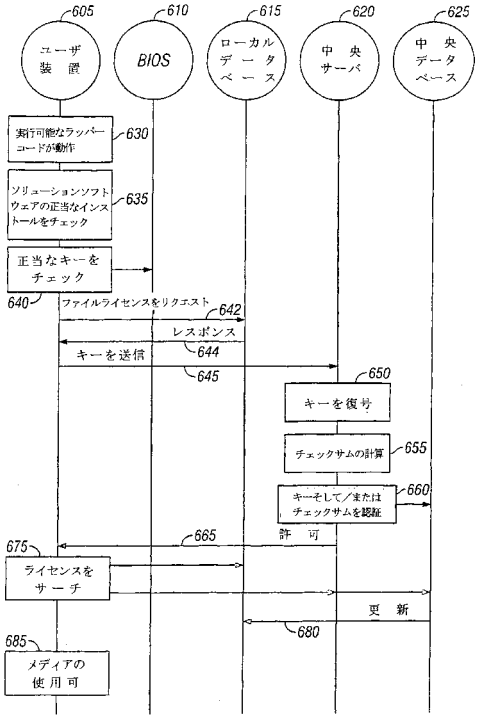
【図４】


400
405
メディアファイルを生成
410
ファイルを受信
415
ファイルを識別
420
ファイルが認識された？
No
425
アクセスを許す
Yes
430
ライセンスされている？
Yes
No
435
購入？
No
440
アクセスを拒否
Yes
445
支払を得る
450
ライセンスデータベースを更新
455
ファイルをラップ

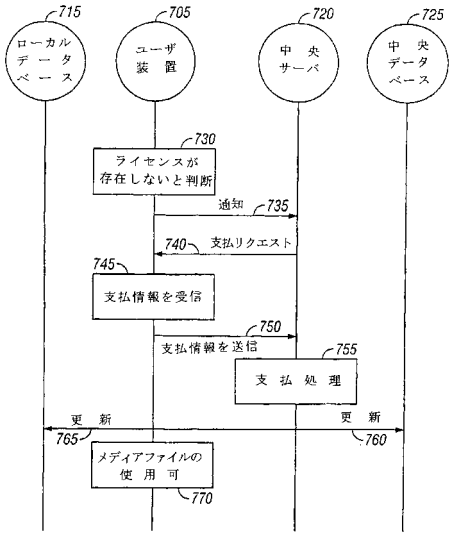
【図５】


500
505
ユーザ装置
510
BIOS
515
中央サーバ
520
中央データベース
522
ソリューションソフトウェアのインストールの開始
リクエスト
524
ダウンロード
526
528
ライセンスアグリーメントを受け入れを受信
530
ユーザ情報を収集
532
ＳＳＬ　コネクションを確立
534
ユーザ情報を送信
ユーザをサーチ
536
538
キーを生成
キーを蓄積
540
542
キーを暗号化
暗号化されたキーを送信
544
暗号化されたキーを蓄積
546
548
ライセンスデータベースを生成

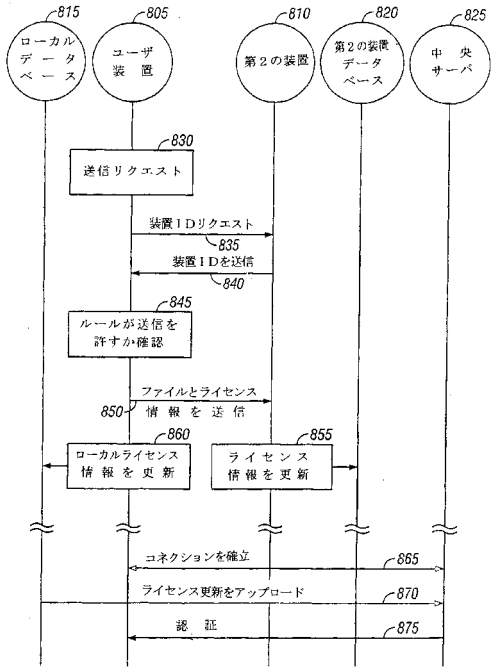
【図６】


605
ユーザ装置
610
BIOS
615
ローカルデータベース
620
中央サーバ
625
中央データベース
実行可能なラッパーコードが動作
630
ソリューションソフトウェアの正当なインストールをチェック
635
正当なキーをチェック
640
ファイルライセンスをリクエスト
642
レスポンス
644
キーを送信
645
650
キーを復号
チェックサムの計算
655
キーそして／またはチェックサムを認証
660
許可
665
675
ライセンスをサーチ
更新
680
685
メディアの使用可

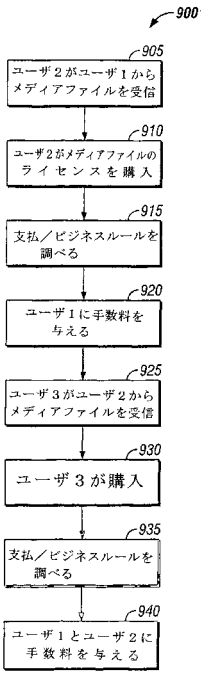
【図７】


715
ローカルデータベース
705
ユーザ装置
720
中央サーバ
725
中央データベース
730
ライセンスが存在しないと判断
通知
735
740
支払リクエスト
745
支払情報を受信
750
支払情報を送信
755
支払処理
更新
765
更新
760
メディアファイルの使用可
770

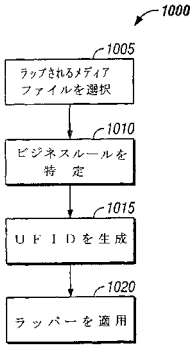
【図８】


815
ローカルデータベース
805
ユーザ装置
810
第２の装置
820
第２の装置データベース
825
中央サーバ
830
送信リクエスト
装置ＩＤリクエスト
835
装置ＩＤを送信
840
845
ルールが送信を許すか確認
ファイルとライセンス情報を送信
850
860
ローカルライセンス情報を更新
855
ライセンス情報を更新
コネクションを確立
865
ライセンス更新をアップロード
870
認証
875

【図９】



【図１０】



【手続補正書】
【提出日】平成17年2月14日(2005.2.14)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ユーザ装置においてデータファイルを検知し、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータを用いて、前記データファイルへのアクセスの許可に関する情報をサーチし、
前記データファイルへのアクセスの許可に関する情報は、ライセンスデータベース中に含まれ、前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、アクセスキーを含み、そのアクセスキーは、前記ライセンスデータベースへのアクセスに必要であり、前記ユーザ装置とは別の装置を用いて前記ライセンスデータベースにアクセスできないように構成されており、
前記データファイルへのアクセスの許可がそのサーチの間に見つかる場合には、前記データファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理方法。
【請求項２】
請求項１に記載のデジタル権利管理方法において、
デジタルラッパーは、正当な許可なしにデータファイルへアクセスできないようにし、
そのデータファイルへアクセスできるようにすることは、前記デジタルラッパーを不能化することを含む

ことを特徴とするデジタル権利管理方法。
【請求項３】
請求項１または請求項２に記載のデジタル権利管理方法において、
前記データファイルは、メディアファイルを含む
ことを特徴とするデジタル権利管理方法。
【請求項４】
請求項１乃至請求項３のいずれかに記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、前記ユーザ装置のライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項５】
請求項４に記載のデジタル権利管理方法において、
前記ライセンスデータベースが、前記ユーザ装置の不揮発性のストレージエリア内に配置されている
ことを特徴とするデジタル権利管理方法。
【請求項６】
請求項５に記載のデジタル権利管理方法において、
前記ユーザ装置の不揮発性のストレージエリアは、ベーシック入力／出力システム（ＢＩＯＳ）を含む
ことを特徴とするデジタル権利管理方法。
【請求項７】
請求項３乃至請求項６のいずれかに記載のデジタル権利管理方法において、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、前記ライセンスデータベースのロケーションを含む
ことを特徴とするデジタル権利管理方法。
【請求項８】
請求項３乃至請求項７のいずれかに記載のデジタル権利管理方法において、
アクセスキーは、前記ユーザ装置から収集された複数のデータアイテムから抽出されたデータを組み合わせることによって生成される
ことを特徴とするデジタル権利管理方法。
【請求項９】
請求項３乃至請求項８のいずれかに記載のデジタル権利管理方法において、
前記ライセンスデータベースは、前記データファイルについてのアクセスキーを含み、前記アクセスキーは、前記ラッパーを不能化するために必要である
ことを特徴とするデジタル権利管理方法。
【請求項１０】
先行するいずれかの請求項に記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、リモートサーバのライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項１１】
請求項１０に記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、前記ユーザ装置上のローカルデータベースが、前記データファイルへのアクセスの許可に関する情報を有していないという判断に応答して、前記リモートサーバの前記ライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項１２】
請求項１０または請求項１１に記載のデジタル権利管理方法において、さらに、
前記中央サーバに対して前記ユーザ装置の識別データを送信し、前記識別データは、前

記中央サーバが前記ユーザ装置を認証できるように適用される
ことを特徴とするデジタル権利管理方法。
【請求項１３】
請求項１２に記載のデジタル権利管理方法において、
前記識別データは、前記ユーザ装置と、このユーザ装置に付随するユーザの少なくともひとつと関連しているデジタルキーを含む
ことを特徴とするデジタル権利管理方法。
【請求項１４】
先行するいずれかの請求項に記載のデジタル権利管理方法において、さらに、
前記データファイルへのアクセスの許可の購入のオファーを行い、
この購入のオファーの受け入れを受信し、
このオファーの受け入れに応答して、前記デジタルラッパーを不能化する
ことを特徴とするデジタル権利管理方法。
【請求項１５】
請求項１４に記載のデジタル権利管理方法において、さらに、
前記オファーの受け入れを中央サーバに送信し、
この中央サーバから、そのオファーの受け入れに応じたメッセージを受信し、そのメッセージ中に含まれるデータは、前記デジタルラッパーを不能化するために用いられる
ことを特徴とするデジタル権利管理方法。
【請求項１６】
請求項１５に記載のデジタル権利管理方法において、さらに、
前記中央サーバに対して前記ユーザ装置の識別データを送信し、この識別データは、前記中央サーバが前記ユーザ装置を認証できるように適用される
ことを特徴とするデジタル権利管理方法。
【請求項１７】
請求項１６に記載のデジタル権利管理方法において、さらに、
前記識別データは、前記ユーザ装置とこのユーザ装置に付随するユーザの少なくとも一つと関連しているデジタルキーを含む
ことを特徴とするデジタル権利管理方法。
【請求項１８】
先行するいずれかの請求項に記載のデジタル権利管理方法において、さらに、
前記データファイルへのアクセスの許可がそのサーチの間に見つからない場合に、そして、
前記データファイルへのアクセスの許可の購入のオファーが受け入れられない場合に、前記データファイルへのアクセスを拒否する
ことを特徴とするデジタル権利管理方法。
【請求項１９】
先行するいずれかの請求項に記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、前記ユーザ装置が前記デジタルラッパーを不能化するためのソフトウェアを備えているかを判断することを含み、その判断は、前記デジタルラッパー中に蓄積されている実行可能な命令を用いて行われる
ことを特徴とするデジタル権利管理方法。
【請求項２０】
請求項１に記載のデジタル権利管理方法において、さらに、
ファイル認識アルゴリズムを用いて前記データファイルを識別する
ことを特徴とするデジタル権利管理方法。
【請求項２１】
請求項２０に記載のデジタル権利管理方法において、
前記ファイル認識アルゴリズムは、デジタルフィンガープリンティング検知技術を含む

ことを特徴とするデジタル権利管理方法。
【請求項２２】
請求項２０または請求項２１に記載のデジタル権利管理方法において、
前記データファイルは、メディアファイルを含む
ことを特徴とするデジタル権利管理方法。
【請求項２３】
請求項２０乃至請求項２２のいずれかに記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、前記ユーザ装置のライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項２４】
請求項２０乃至請求項２３のいずれかに記載のデジタル権利管理方法において、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、前記ユーザ装置の不揮発性のストレージエリア内の前記ライセンスデータベースのロケーションを識別する
ことを特徴とするデジタル権利管理方法。
【請求項２５】
請求項２０乃至請求項２４のいずれかに記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可に関する情報のサーチは、リモートサーバに関連するライセンスデータベース中で行われる
ことを特徴とするデジタル権利管理方法。
【請求項２６】
請求項２０乃至請求項２５のいずれかに記載のデジタル権利管理方法において、
前記データファイルへのアクセスの許可の購入のオファーを行い、
この購入のオファーの受け入れを受信し、
このオファーの受け入れに応答して、前記データファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理方法。
【請求項２７】
請求項１３乃至請求項１６、または請求項２６のいずれかに記載のデジタル権利管理方法において、さらに、
前記購入のオファーの受け入れに応答して、前記ユーザ装置において、前記データファイルへのアクセスの許可に関する情報を蓄積する
ことを特徴とするデジタル権利管理方法。
【請求項２８】
請求項２０乃至請求項２７のいずれかに記載のデジタル権利管理方法において、さらに、
前記データファイルに対してデジタルラッパーを適用し、このデジタルラッパーは、識別されたファイルと関連する
ことを特徴とするデジタル権利管理方法。
【請求項２９】
ユーザ装置においてデータファイルを受信し、前記データファイルは、このデータファイルの少なくとも一人の配布者に関する情報を含むデジタルラッパーを有しており、
前記データファイルへのアクセス権を購入するリクエストを受信し、
前記デジタルラッパーから少なくとも一人の配布者に関する情報を抽出し、
この抽出された情報に基づいて、少なくとも一人の配布者に対してクレジットを配分する
ことを特徴とするデジタル権利の配布に関連する収益配分方法。
【請求項３０】
請求項２９に記載の収益配分方法において、
前記デジタルラッパーは、さらに、

前記データファイルへのアクセス権の購入についての、割り当てられたロイヤリティの配分に関する情報を含んでいる
ことを特徴とする収益配分方法。
【請求項３１】
請求項３０に記載の収益配分方法において、
抽出された情報は、独特のファイル識別子を含み、
その方法は、さらに、
その独特のファイル識別子を用いて、少なくとも一つの配布者情報とそのロイヤリティ配分情報を取り出す
ことを特徴とする収益配分方法。
【請求項３２】
請求項３１に記載の収益配分方法において、
取り出された情報は、前記ユーザ装置から離れて配置する中央データベースから取り出される
ことを特徴とする収益配分方法。
【請求項３３】
請求項２９乃至３２のいずれかに記載の収益配分方法において、さらに、
購入のリクエストを中央サーバに送信し、この中央サーバに関連するデータベース中にクレジットの配分を蓄積する
ことを特徴とする収益配分方法。
【請求項３４】
ユーザ装置のユーザを識別することを含むデジタル権利の配布に関連する収益配分方法において、
前記ユーザ装置においてデータファイルを受信し、このデータファイルは、このデータファイルの少なくとも一人の配布者に関する情報を含むデジタルラッパーを有しており、
前記デジタルラッパーを修正して前記ユーザの識別に関する情報を含むようにし、その修正されたデジタルラッパーを用いた前記データファイルの検知は、前記ユーザに対するクレジットの割り当てを可能とする
ことを特徴とする収益配分方法。
【請求項３５】
請求項３４に記載の収益配分方法において、
前記デジタルラッパーは、正当な許可なしに前記データファイルへアクセスできないようにするのに適している
ことを特徴とする収益配分方法。
【請求項３６】
請求項３４または請求項３５に記載の収益配分方法において、さらに、
前記修正されたデジタルラッパーを有するデータファイルを消費者に付随する装置に対して送信し、
この消費者に付随する装置から前記データファイルへのアクセスを購入するリクエストを受信し、
受信されたリクエストに応答して、前記消費者に付随する装置において前記デジタルラッパーを不能化する
ことを特徴とする収益配分方法。
【請求項３７】
請求項３６に記載の収益配分方法において、さらに、
ひとつまたは複数の配布者の間で、前記消費者購入に対するクレジットを配分する
ことを特徴とする収益配分方法。
【請求項３８】
請求項３４乃至請求項３７のいずれかに記載の収益配分方法において、
前記ユーザの識別に関する情報は、このユーザについての独特のユーザ識別子から成り

、その独特のユーザ識別子は、中央サーバによって割り当てられる
ことを特徴とする収益配分方法。
【請求項３９】
請求項３４乃至請求項３８のいずれかに記載の収益配分方法において、
前記データファイルは、メディアファイルを含む
ことを特徴とする収益配分方法。
【請求項４０】
ユーザ装置からこのユーザ装置に関連する情報を収集し、前記ユーザ装置に関する情報は、このユーザ装置についての独特の識別データを含んでいる、
ユーザ装置におけるデジタル権利管理助長方法において、
収集された情報を用いてデジタルキーを生成し、
前記デジタルキーを蓄積し、
前記デジタルキーを暗号化し、
暗号化されたキーを前記ユーザ装置上に蓄積するためにこのユーザ装置に対して送信し、
前記ユーザ装置から、暗号化されたキーとこのユーザ装置に関する情報を受信し、
受信された暗号化されたキー、受信された情報、そして蓄積されているデジタルキーのうち少なくとも２つを用いて、前記ユーザ装置を認証する
ことを特徴とするユーザ装置におけるデジタル権利管理助長方法。
【請求項４１】
請求項４０に記載のデジタル権利管理助長方法において、
前記ユーザ装置のユーザに関する識別情報を収集し、前記デジタルキーは、そのユーザに関する識別情報を用いて生成される
ことを特徴とするデジタル権利管理助長方法。
【請求項４２】
請求項４０または請求項４１に記載のデジタル権利管理助長方法において、
収集される情報は、ユーザ装置上に蓄積された実行可能コードに従って収集される
ことを特徴とするデジタル権利管理助長方法。
【請求項４３】
請求項４０乃至請求項４２のいずれかに記載のデジタル権利管理助長方法において、
前記デジタルキーは、中央サーバによって生成され、この中央サーバにおいて蓄積される
ことを特徴とするデジタル権利管理助長方法。
【請求項４４】
請求項４０乃至請求項４３のいずれかに記載のデジタル権利管理助長方法において、
前記ユーザ装置の認証は、
前記暗号化されたキーを復号し、
前記暗号化されたキーを蓄積されているデジタルキーと比較することから成る
ことを特徴とするデジタル権利管理助長方法。
【請求項４５】
請求項４０乃至請求項４４のいずれかに記載のデジタル権利管理助長方法において、
前記ユーザ装置の認証は、
受信された前記ユーザ装置に関する情報を用いてデジタルキーを生成し、
このデジタルキーを蓄積されたデジタルキーと比較することから成る
ことを特徴とするデジタル権利管理助長方法。
【請求項４６】
請求項４０乃至請求項４５のいずれかに記載のデジタル権利管理助長方法において、さらに、
前記ユーザ装置の認証に応答して、ライセンスデータベースへのアクセスを許可する
ことを特徴とするデジタル権利管理助長方法。

【請求項４７】
請求項４０乃至請求項４６のいずれかに記載のデジタル権利管理助長方法において、
前記ユーザ装置の認証に応答して、デジタルファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理助長方法。
【請求項４８】
請求項４０乃至請求項４７のいずれかに記載のデジタル権利管理助長方法において、
前記独特の識別データは、前記ユーザ装置の不揮発性のストレージエリアから抽出される
ことを特徴とするデジタル権利管理助長方法。
【請求項４９】
ユーザ装置の入力／出力システムを、試みられたファイル送信について監視し、
前記入力／出力システムを通じたデータファイルの送信の試みを検知し、
その試みられた送信が許可される前に、前記データファイルに対して前記デジタルラッパーを適用し、このデジタルラッパーは、前記データファイルへの許可されていないアクセスを防止するために適用される
ことを特徴とするデジタル権利管理方法。
【請求項５０】
請求項４９に記載のデジタル権利管理方法において、
前記データファイルは、メディアファイルを含む
ことを特徴とするデジタル権利管理方法。
【請求項５１】
請求項４９または請求項５０に記載のデジタル権利管理方法において、さらに、
前記データファイルを識別し、前記デジタルラッパーは、前記データファイルのアイデンティティに基づいて適用される
ことを特徴とするデジタル権利管理方法。
【請求項５２】
請求項４９乃至請求項５１のいずれかに記載のデジタル権利管理方法において、
前記デジタルラッパーは、前記ユーザ装置上のデータベース中の前記データファイルの識別子と合致するデータファイルのアイデンティティに基づいて適用される
ことを特徴とするデジタル権利管理方法。
【請求項５３】
請求項５１または請求項５２に記載のデジタル権利管理方法において、
前記データファイルの識別は、ファイル認識アルゴリズムの使用を含む
ことを特徴とするデジタル権利管理方法。
【請求項５４】
請求項４９乃至請求項５３のいずれかに記載のデジタル権利管理方法において、
前記デジタルラッパーは、前記データファイルを識別する情報と、前記データファイルの購入に対するクレジットの割り当てに関する情報とを含む
ことを特徴とするデジタル権利管理方法。
【請求項５５】
第１のユーザ装置上においてデジタルファイルを識別し、前記デジタルファイルは、前記第１のユーザ装置上に蓄積されているライセンス情報に従うライセンスを受けており、
前記第１のユーザ装置から第２のユーザ装置に対する前記デジタルファイルのコピーのリクエストを受信し、
前記第２のユーザ装置に関連する情報であって、前記第２のユーザ装置についての独特の識別データを含む情報を取得し、
前記第１のユーザ装置から前記第２のユーザ装置に対して前記デジタルファイルをコピーし、
前記第１のユーザ装置上にデータを蓄積し、前記データは、コピーされた前記デジタルファイルを識別し、前記第２のユーザ装置を識別する

ことを特徴とするデジタル権利管理方法。
【請求項５６】
請求項５５に記載のデジタル権利管理方法において、さらに、
前記第１のユーザ装置上に蓄積されたデータを中央データベースと同期させる
ことを特徴とするデジタル権利管理方法。
【請求項５７】
請求項５５または請求項５６に記載のデジタル権利管理方法において、さらに、
リクエストされた前記デジタルファイルのコピーは、前記ライセンス情報に基づいて許可されると判断する
ことを特徴とするデジタル権利管理方法。
【請求項５８】
請求項５５乃至請求項５７のいずれかに記載のデジタル権利管理方法において、
前記ライセンス情報は、前記デジタルファイルについてのデジタルラッパー中に含まれている
ことを特徴とするデジタル権利管理方法。
【請求項５９】
請求項５５乃至請求項５８のいずれかに記載のデジタル権利管理方法において、さらに、
前記第２のユーザ装置上に、前記デジタルファイルについての前記ライセンス情報を蓄積する
ことを特徴とするデジタル権利管理方法。
【請求項６０】
配布されるメディアファイルを識別し、
このメディアファイルに関するアクセスルールを識別し、そのアクセスルールは、使用権利と使用料に関する情報を含み、
前記メディアファイルに対してデジタルラッパーを適用し、このデジタルラッパーは、前記メディアファイルについての識別データとアクセスルールに関するデータを含み、前記デジタルラッパーは、前記メディアファイルへの許可されていないアクセスを防止するのに適する
ことを特徴とするデジタル権利管理方法。
【請求項６１】
請求項６０に記載のデジタル権利管理方法において、
前記デジタルラッパーは、前記メディアファイルへアクセスするライセンスを持っているユーザによって、このメディアファイルの使用に対して不能化される
ことを特徴とするデジタル権利管理方法。
【請求項６２】
請求項６０または請求項６１に記載のデジタル権利管理方法において、
前記デジタルラッパーは、さらに、前記メディアファイルの少なくとも一人の配布者に関する情報を含んでいる
ことを特徴とするデジタル権利管理方法。
【請求項６３】
ライセンス情報を用いてメディアファイルを符号化し、
許可されていないアクセスを防止するために、デジタルラッパーを用いて、そのメディアファイルをロックし、
ラップされたメディアファイルをユーザ装置上にロードし、ラップされたメディアファイルは、ラップされたメディアファイルのアンロックを許す命令の取得についての情報を含み、
前記ラップされたメディアファイルへのアクセスの試みを検知し、
前記ラップされたメディアファイルへのアクセスの試みに応答して、そして、その命令の取得についての情報を用いて、前記ユーザ装置上にその命令をロードし、

前記メディアファイルのアンロックを許可するために前記ユーザ装置上に命令をインストールし、この命令は、前記メディアファイルを識別し、そして、前記メディアファイル内に符号化されたライセンス情報に従って、前記メディアファイルを使用するライセンスを取得するためにリモートサーバに対してメッセージを送信し、
前記リモートサーバから前記メディアファイルへのアクセスのライセンスを受信し、
このライセンスを用いて、前記ユーザ装置における前記メディアファイルへのアクセスを許可する
ことを特徴とするデジタル権利管理方法。
【請求項６４】
請求項６３に記載のデジタル権利管理方法において、さらに、
前記ユーザ装置上に、前記メディアファイルへアクセスするライセンスを蓄積する
ことを特徴とするデジタル権利管理方法。
【請求項６５】
請求項６３または請求項６４に記載のデジタル権利管理方法において、さらに、
前記ライセンスは、前記メディアファイルをアンロックするためのデータを含む
ことを特徴とするデジタル権利管理方法。
【請求項６６】
複数のデジタルファイルについての識別子を蓄積するために適用され、そして、前記デジタルファイルを使用するユーザライセンスを蓄積するために適用される中央データベースと、
ネットワークを介して、リモート装置からメッセージを受信するように動作できる中央サーバとを備え、受信された各メッセージは、ユーザについてのユーザ識別子と、デジタルファイルについての識別情報を含み、
前記中央サーバは、さらに、前記リモート装置からひとつまたは複数のデジタルキーを受信し、前記リモート装置とユーザの少なくとも一つのアイデンティティを認証するために、前記ひとつまたは複数のデジタルキーを復号し、前記デジタルファイルを使用するライセンスについての支払情報を処理して、前記ユーザについての、前記デジタルファイルを使用するライセンスに関する情報を蓄積し、前記デジタルファイルについてのライセンス情報を前記リモート装置に対して送信し、
前記ライセンス情報は、前記リモート装置を、そのユーザによって前記デジタルファイルが使用できるようにするために適用される
ことを特徴とするデジタル権利管理システム。
【請求項６７】
請求項６６に記載のデジタル権利管理システムにおいて、
前記中央サーバは、さらに、前記リモート装置を認証するために用いる装置特有のデータをこのリモート装置から受信するように動作できる
ことを特徴とするデジタル権利管理システム。
【請求項６８】
請求項６６乃至請求項６７のいずれかに記載のデジタル権利管理システムにおいて、
前記リモート装置は、ユーザに付随するユーザ装置に対するデジタルファイルのストリーミングをサポートするために適用されるサーバを含む
ことを特徴とするデジタル権利管理システム。
【請求項６９】
請求項６６乃至請求項６８のいずれかに記載のデジタル権利管理システムにおいて、
リモート装置は、ライセンス情報を蓄積する
ことを特徴とするデジタル権利管理システム。
【請求項７０】
請求項６６乃至請求項６７のいずれかに記載のデジタル権利管理システムにおいて、
前記リモート装置は、ユーザに付随する前記ユーザ装置を含む
ことを特徴とするデジタル権利管理システム。

【請求項７１】
請求項７０に記載のデジタル権利管理システムにおいて、
前記中央サーバは、さらに、前記ユーザ装置から情報を受信し、ユーザと前記ユーザ装置の少なくともひとつに関するデジタルキーを生成し、このデジタルキーを前記ユーザ装置に送信し、このデジタルキーは、ライセンス情報、このライセンス情報を含むライセンスデータベース、そして前記デジタルファイルのうち少なくともひとつにアクセスしうるように適用される
ことを特徴とするデジタル権利管理システム。
【請求項７２】
請求項６６乃至請求項７１のいずれかに記載のデジタル権利管理システムにおいて、
前記ライセンス情報は、前記デジタルファイルに対して適用されるデジタルラッパーを不能化するために適用されるデータを含む
ことを特徴とするデジタル権利管理システム。
【請求項７３】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を蓄積したマシーン読み取り可能なアーティクルであって、そのオペレーションは、
ユーザ装置においてデータファイルを検知し、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータを用いて、前記データファイルへのアクセスの許可に関する情報をサーチし、前記データファイルへのアクセスの許可に関する情報は、ライセンスデータベース中に含まれ、前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、アクセスキーを含み、このアクセスキーは、前記ライセンスデータベースにアクセスするために必要であり、また、前記ユーザ装置とは別の装置を用いて前記ライセンスデータベースへアクセスできないように構成され、
前記データファイルへのアクセスの許可がそのサーチの間に見つかる場合には、前記データファイルへのアクセスを許可する
ことを特徴とするアーティクル。
【請求項７４】
請求項７３に記載のアーティクルにおいて、
前記データファイルは、正当な許可なしにこのデータファイルへアクセスできないようにするデジタルラッパーを含み、
前記データファイルへアクセスできるようにすることは、前記デジタルラッパーを不能化することを含む
ことを特徴とするアーティクル。
【請求項７５】
請求項７３または請求項７４に記載のアーティクルにおいて、
前記ユーザ装置の不揮発性のストレージエリアに蓄積されているデータは、前記ライセンスデータベースのロケーション情報を含み、前記ライセンスデータベースは、前記ユーザ装置において蓄積される
ことを特徴とするアーティクル。
【請求項７６】
請求項７３乃至請求項７５のいずれかに記載のアーティクルにおいて、
前記データファイルへのアクセスの許可は、前記デジタルラッパーを不能化するためのデジタルキーを含み、このデジタルラッパーの不能化は、前記デジタルキーを用いて行われる
ことを特徴とするアーティクル。
【請求項７７】
請求項７３乃至請求項７６のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
ユーザ装置のファイルインプットシステムを監視するオペレーションを実行させるため

の命令を記憶し、
前記ユーザ装置における前記データファイルの検知は、前記ファイルインプットシステムの監視結果によって実行される
ことを特徴とするアーティクル。
【請求項７８】
請求項７３乃至請求項７７のいずれかに記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記ユーザ装置において蓄積されている装置キーを検知し、
前記ユーザ装置が許可された装置かを判断するために前記装置キーを認証するオペレーションを実行させるための命令を記憶し、
前記デジタルラッパーの不能化は、前記ユーザ装置が許可された装置でない場合には実行されない
ことを特徴とするアーティクル。
【請求項７９】
請求項７３乃至請求項７８のいずれかに記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記データファイルへのアクセスの許可が前記ユーザ装置において見つからない場合に、前記データファイルへのアクセスの許可をリクエストするリクエストメッセージをリモートサーバに対して送信するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項８０】
請求項７９に記載のアーティクルにおいて、
前記リクエストメッセージは、前記データファイルへのアクセスの許可を購入するリクエストを含む
ことを特徴とするアーティクル。
【請求項８１】
請求項７９に記載のアーティクルにおいて、
マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記リクエストメッセージに応答したレスポンスメッセージを受信し、前記レスポンスメッセージは、前記データファイルへのアクセスの許可を含み、
前記レスポンスメッセージとともに含まれる前記データファイルへのアクセスの許可を用いて、前記デジタルラッパーを不能化するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項８２】
請求項７３乃至請求項８１のいずれかに記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記データファイルへのアクセスの許可がサーチの間に見つからない場合に、前記データファイルへのアクセスの許可の購入のオファーを前記ユーザ装置のユーザに対して提供し、
購入のオファーの受け入れを受信し、
購入のオファーの受け入れの表示を蓄積するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項８３】
請求項８２に記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記購入のオファーの受け入れの表示をリモートサーバに対して送信するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。

【請求項８４】
請求項７３に記載のアーティクルにおいて、
前記命令は、ひとつまたは複数のプロセッサに、さらに、
ファイル認識アルゴリズムを用いて前記データファイルを識別するオペレーションを実行させる
ことを特徴とするアーティクル。
【請求項８５】
請求項８４に記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記ユーザ装置の入力システムを監視するオペレーションを実行させるための命令を記憶し、
前記データファイルの検知は、前記監視の結果として生ずる
ことを特徴とするアーティクル。
【請求項８６】
請求項８４または請求項８５に記載のアーティクルにおいて、
前記不揮発性のストレージエリアに蓄積されているデータは、前記ユーザ装置上のライセンスデータベースにアクセスするためのデジタルキーを含む
ことを特徴とするアーティクル。
【請求項８７】
請求項８４乃至請求項８６のいずれかに記載のアーティクルにおいて、
前記不揮発性のストレージエリアに蓄積されているデータは、前記ライセンスデータベースのロケーション情報を含む
ことを特徴とするアーティクル。
【請求項８８】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記憶したマシーン読み取り可能な媒体を備えたアーティクルにおいて、そのオペレーションは、
データファイルに適用されるデジタルラッパーから抽出される情報を受信し、この抽出された情報は、前記データファイルの識別子を含み、
前記データファイルへのアクセスの許可の購入のリクエストを受信し、
前記抽出された情報に基づいて、前記データファイルの少なくとも一人の配布者を識別し、
予め決められた配分構成に従って、前記識別された配布者にクレジットを配分する
ことを特徴とするアーティクル。
【請求項８９】
請求項８８に記載のアーティクルにおいて、
前記抽出された情報は、前記識別された配布者の各々の識別子を含む
ことを特徴とするアーティクル。
【請求項９０】
請求項８８または請求項８９に記載のアーティクルにおいて、
前記識別された配布者に対するクレジットの配分は、前記抽出された情報中のデータに従って行われる
ことを特徴とするアーティクル。
【請求項９１】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記憶したマシーン読み取り可能な媒体を備えたアーティクルであって、そのオペレーションは、
ユーザ装置上にデータファイルを蓄積し、このデータファイルは、このデータファイルの少なくとも一人または複数の配布者に関する情報を含むデジタルラッパーを有しており、
前記ユーザ装置のユーザを識別し、
前記デジタルラッパーを修正して前記ユーザの識別に関する情報を含むようにし、この

修正されたデジタルラッパーを伴う前記データファイルの検知は、前記ユーザに対するクレジットの割り当てを可能とする
ことを特徴とするアーティクル。
【請求項９２】
請求項９１に記載のアーティクルにおいて、
前記デジタルラッパーは、さらに、
前記ユーザに対するクレジットの割り当て配分に関する情報を含んでいる
ことを特徴とするアーティクル。
【請求項９３】
請求項９１または請求項９２に記載のアーティクルにおいて、
前記デジタルラッパーは、前記データファイルへのアクセスの正当な許可なしにこのデータファイルへアクセスできないようにし得る
ことを特徴とするアーティクル。
【請求項９４】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記憶したマシーン読み取り可能な媒体を備えたアーティクルにおいて、そのオペレーションは、
ユーザ装置からこのユーザ装置に関連する情報を受信し、受信された情報は、前記ユーザ装置についての独特の識別データを含んでおり、
受信された情報を用いてデジタルキーを生成し、
前記デジタルキーを蓄積し、
前記デジタルキーを暗号化し、
前記暗号化されたキーを前記ユーザ装置上に蓄積するためにこのユーザ装置に対して送信し、
前記ユーザ装置から、暗号化されたキーと、収集された前記このユーザ装置に関する情報を受信し、収集された情報は、前記ユーザ装置上に蓄積されている命令に従ってこのユーザ装置によって収集され、
前記受信された暗号化されたキー、収集された情報、そして蓄積されているデジタルキーのうち少なくとも２つを用いて、前記ユーザ装置を認証する
ことを特徴とするアーティクル。
【請求項９５】
請求項９４に記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記ユーザ装置から、データファイルへのアクセス許可のリクエストを受信し、
前記データファイルへのアクセス許可を前記ユーザ装置の認証に応じて送信するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項９６】
請求項９５に記載のアーティクルにおいて、
前記暗号化されたキーと収集された情報とが、その許可のリクエストに関連して受信される
ことを特徴とするアーティクル。
【請求項９７】
請求項９５または請求項９６に記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記データファイルへのアクセスの許可を示す表示を、前記ユーザ装置の認証に応じて蓄積するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項９８】
請求項９４乃至請求項９７のいずれかに記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、

前記ユーザ装置に付随するユーザの独特の識別子を受信し、
さらに、このユーザの独特の識別子を用いて前記デジタルキーを生成するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項９９】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記憶したマシーン読み取り可能な媒体を備えたアーティクルにおいて、そのオペレーションは、
ユーザ装置の入力／出力システムを、試みられたファイル送信について監視し、
前記入力／出力システムを通じたデータファイルの送信の試みを検知し、
この試みられた送信が許可される前に、前記データファイルに対してデジタルラッパーを適用し、このデジタルラッパーは、前記データファイルへの許可されていないアクセスを防止するために適用される
ことを特徴とするアーティクル。
【請求項１００】
請求項９９に記載のアーティクルにおいて、
マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
許可されていないコピーからプロテクトされているデータファイルを識別するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項１０１】
請求項１００に記載のアーティクルにおいて、
許可されていないコピーからプロテクトされている前記データファイルの識別は、前記ユーザ装置上に蓄積されているデータベース内に前記データファイルの識別子を配置することを含む
ことを特徴とするアーティクル。
【請求項１０２】
請求項１００または請求項１０１に記載のアーティクルにおいて、
許可されていないコピーからプロテクトされている前記データファイルの識別は、
リモートサーバに対して、前記データファイルを識別するための情報を含むメッセージを送信し、
前記データファイルが許可されていないコピーからプロテクトされていることを示す、前記メッセージに対するレスポンスを受信することを含む
ことを特徴とするアーティクル。
【請求項１０３】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記憶したマシーン読み取り可能な媒体を備えたアーティクルでにおいて、そのオペレーションは、
第１のユーザ装置上においてデジタルファイルを識別し、このデジタルファイルは、前記第１のユーザ装置上に蓄積されているライセンス情報に従うライセンスを受けており、
前記第１のユーザ装置から第２のユーザ装置に対する前記デジタルファイルのコピーのリクエストを受信し、
前記第２のユーザ装置に関連する情報であって、この第２のユーザ装置についての独特の識別子データを含む情報を取得し、
前記第１のユーザ装置から前記第２のユーザ装置に対して前記デジタルファイルをコピーし、
前記第１のユーザ装置上にデータを蓄積し、このデータは、コピーされた前記デジタルファイルを識別し、そして、前記第２のユーザ装置を識別する
ことを特徴とするアーティクル。
【請求項１０４】
請求項１０３に記載のアーティクルにおいて、
前記マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、

前記ライセンス情報に従って、前記第２のユーザ装置に対する前記デジタルファイルのコピーが許されるかを確認するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項１０５】
請求項１０３または請求項１０４に記載のアーティクルにおいて、
前記デジタルファイルのコピーのリクエストの受信は、前記第１のユーザ装置のファイル出力システムを通じた前記デジタルファイルのコピーの試みを示す表示を受信することを含む
ことを特徴とするアーティクル。
【請求項１０６】
請求項１０３乃至請求項１０５のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記データをリモートサーバに対して送信するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項１０７】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記憶したマシーン読み取り可能な媒体を備えたアーティクルにおいて、そのオペレーションは、
メディアファイルを識別し、
前記メディアファイルに関するアクセスルールを識別し、このアクセスルールは、使用権利と使用料に関する情報を含み、
前記メディアファイルに対してデジタルラッパーを適用し、このデジタルラッパーは、前記メディアファイルについての識別データと前記アクセスルールに関するデータとを含み、前記デジタルラッパーは、前記メディアファイルへの許可されていないアクセスを防止するために適用される
ことを特徴とするアーティクル。
【請求項１０８】
請求項１０７に記載のアーティクルにおいて、
前記メディアファイルの識別は、ファイル認識アルゴリズムを用いて前記メディアファイルを識別することを含む
ことを特徴とするアーティクル。
【請求項１０９】
請求項１０７または請求項１０８に記載のアーティクルにおいて、
前記メディアファイルについてのアクセスルールの識別は、リモートサーバからアクセスルールを受信することを含む
ことを特徴とするアーティクル。
【請求項１１０】
請求項１０７乃至請求項１０９のいずれかに記載のアーティクルにおいて、
マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記メディアファイルへのアクセスの許可を求めるリクエストをユーザから受信し、
前記メディアファイルへのアクセスの許可を求めるリクエストをリモートサーバに通知し、
前記ユーザによって前記メディアファイルへのアクセスができるようにするために、前記デジタルラッパーを不能化するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項１１１】
請求項１０７乃至請求項１１０のいずれかに記載のアーティクルにおいて、
前記メディアファイルについてのアクセスルールの識別は、
ユーザからアクセスルールを受信することを含む
ことを特徴とするアーティクル。

【請求項１１２】
ひとつまたは複数のプロセッサにオペレーションを実行させる命令を記憶したマシーン読み取り可能な媒体を備えたアーティクルにおいて、そのオペレーションは、
デジタルキーを受信し、
このデジタルキーを不揮発性のメモリ内に蓄積し、
ライセンスデータベース内の少なくとも一つのデジタルファイルについてのライセンス情報を、揮発性のストレージエリア内に蓄積し、前記デジタルキーが、前記ライセンスデータベースのロケーションデータを含み、
特定のデジタルファイルへのアクセスの試みを識別し、
前記ライセンスデータベースが前記特定のデジタルファイルに対するライセンスを識別するライセンス情報を含んでいる場合に、前記デジタルキーを用いて前記デジタルファイルへのアクセスを許す
ことを特徴とするアーティクル。
【請求項１１３】
請求項１１２に記載のアーティクルにおいて、
前記デジタルキーは、ユーザ装置に特有のデータを含み、
マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記ユーザ装置から識別情報を取り出し、
前記識別情報と、前記ユーザ装置に特有のデータとを用いて、前記デジタルキーを認証するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項１１４】
請求項１１２または請求項１１３に記載のアーティクルにおいて、
マシーン読み取り可能な媒体は、ひとつまたは複数のプロセッサに、さらに、
前記ライセンスデータベースが、特定のデジタルファイルへのライセンスを識別するライセンス情報を含んでいない場合に、前記デジタルファイルへのアクセスを防止するオペレーションを実行させるための命令を記憶する
ことを特徴とするアーティクル。
【請求項１１５】
請求項１１２乃至請求項１１４のいずれかに記載のアーティクルにおいて、
前記デジタルキーは、前記ライセンスデータベースと前記ライセンス情報との少なくとも一つを復号するために必要なデータを含む
ことを特徴とするアーティクル。
【請求項１１６】
請求項１１２乃至請求項１１５のいずれかに記載のアーティクルにおいて、
前記ライセンス情報は、特定のデジタルファイルに適用されるデジタルラッパーを不能化するために必要なデータを含む
ことを特徴とするアーティクル。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/002356

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 October 2004	10/11/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Anticoli, C

9

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/002356

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/161718 A1 (COLEY CHRISTOPHER D ET AL) 31 October 2002 (2002-10-31)	1,2, 7-19,21, 22, 25-39, 60-63, 66-74, 77-93, 108, 110-112
Y	paragraph '0041! - paragraph '0049!	3-6,20, 23,24, 64,65, 75,76, 109
	paragraph '0065! paragraph '0079! paragraph '0087! - paragraph '0090! paragraph '0106! paragraph '0109!	
Y	US 6 108 420 A (ALLAN DAVID IAN ET AL) 22 August 2000 (2000-08-22) abstract column 3, line 5 - line 56	20,109
Y	WO 02/086803 A (RHOADS GEOFFREY B ; DIGIMARC CORP (US); HIATT R STEPHEN (US); LEVY KEN) 31 October 2002 (2002-10-31) abstract paragraph '0003! - paragraph '0014!	3-6,23, 24,64, 65,75,76
Y	WO 01/41027 A (KOVAC MARIO ; ORSULIC JOSKO (HR); RUNJE DAVOR (HR); UZELAC TOMISLAV (H) 7 June 2001 (2001-06-07) abstract	3-6,23, 24,64, 65,75,76
X	US 4 796 220 A (WOLFE EVERETT W) 3 January 1989 (1989-01-03) column 3, line 1 - line 25 column 6, line 4 - column 7, line 56	40-48, 95-99, 113-118
A	US 5 490 216 A (RICHARDSON III FREDERIC B) 6 February 1996 (1996-02-06) column 2, line 50 - column 3, line 32 column 6, line 60 - column 7, line 7	40-48, 95-99, 113-118
X	US 6 189 099 B1 (BEHAR YAACOV ET AL) 13 February 2001 (2001-02-13) column 1, line 30 - line 62	40-48, 95-99, 113-118
	-/--	

9

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/002356

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 563 946 A (NAGDA JAGDISH ET AL) 8 October 1996 (1996-10-08) column 8, line 28 - line 62 column 19, line 18 - column 20, line 32	49,100
Y	EP 1 096 382 A (IONTAS LTD) 2 May 2001 (2001-05-02) paragraph '0003! paragraph '0028!	49-59, 100-107
Y	WO 02/052388 A (ALDRIDGE JANE LESLEY ; GAFFNEY PHILIP MICHAEL (GB); INTERNET EXTRA LTD) 4 July 2002 (2002-07-04) page 1, line 8 - line 14 claim 1	49-59, 100-107
X	US 6 282 653 B1 (HIMMEL MARIA AZUA ET AL) 28 August 2001 (2001-08-28)	55,104
Y	column 1, line 5 - column 5, line 8 column 19, line 18 - column 20, line 32	49-59, 100-107
P,Y	US 2003/236978 A1 (EVANS GLENN F ET AL) 25 December 2003 (2003-12-25) paragraph '0004! - paragraph '0005!	49-59, 100-107

9

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2004/002356

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/US2004 /002356

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-39, 60-94, 108-112

managing digital rights by using a digital wrapper and a license database

1.1. claims: 29-39

allocating proceeds in connection with a distribution of digital rights

---

2. claims: 40-48, 95-99, 113-118

facilitating digital rights management by generating a digital key

---

3. claims: 49-59, 100-107

managing digital rights when transferring files

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/002356

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002161718 A1	31-10-2002	US 2001011253 A1	02-08-2001
US 6108420 A	22-08-2000	AU 6492198 A	30-10-1998
		CA 2285392 A1	15-10-1998
		WO 9845768 A1	15-10-1998
		CN 1255209 T	31-05-2000
		EP 0974084 A1	26-01-2000
		JP 2002503365 T	29-01-2002
WO 02086803 A	31-10-2002	US 2002186844 A1	12-12-2002
		WO 02086803 A1	31-10-2002
WO 0141027 A	07-06-2001	AU 1943801 A	12-06-2001
		WO 0141027 A1	07-06-2001
US 4796220 A	03-01-1989	NONE	
US 5490216 A	06-02-1996	AU 678985 B2	19-06-1997
		AU 4811393 A	12-04-1994
		WO 9407204 A1	31-03-1994
		CA 2145068 A1	31-03-1994
		CN 1103186 A	31-05-1995
		EP 0689697 A1	03-01-1996
		NZ 255971 A	26-05-1997
US 6189099 B1	13-02-2001	US 6216230 B1	10-04-2001
		US 6401205 B1	04-06-2002
		US 6425084 B1	23-07-2002
US 5563946 A	08-10-1996	DE 69528408 D1	07-11-2002
		DE 69528408 T2	03-07-2003
		EP 0679977 A1	02-11-1995
		JP 7295798 A	10-11-1995
		JP 2002251325 A	06-09-2002
EP 1096382 A	02-05-2001	EP 1096382 A2	02-05-2001
		IE 20000864 A1	29-05-2002
WO 02052388 A	04-07-2002	WO 02052388 A2	04-07-2002
US 6282653 B1	28-08-2001	CA 2268377 A1	15-11-1999
		CN 1292896 T	25-04-2001
		CZ 20004231 A3	12-06-2002
		DE 69809800 D1	09-01-2003
		DE 69809800 T2	04-12-2003
		EP 1076845 A1	21-02-2001
		ES 2184347 T3	01-04-2003
		WO 9960461 A1	25-11-1999
		JP 2002516426 T	04-06-2002
		PL 343928 A1	10-09-2001
US 2003236978 A1	25-12-2003	BR 0302113 A	08-09-2004
		CA 2428953 A1	24-12-2003
		CN 1471021 A	28-01-2004
		EP 1376302 A2	02-01-2004
		JP 2004062886 A	26-02-2004
		NO 20032887 A	29-12-2003
		PL 360755 A1	29-12-2003

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No
PCT/US2004/002356

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003236978 A1		ZA 200303975 A	25-03-2004

Form PCT/ISA/210 (patent family annex) (January 2004)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
フロッピー
イーサネット
Ｂｌｕｅｔｏｏｔｈ

(72)発明者 エドマンスン，ブラッド
アメリカ合衆国テネシー州３７０６４、フランクリン、ワイルドフロウア・コート ６０５番
(72)発明者 ジァウォースキ，デイヴ
アメリカ合衆国テネシー州３７０２７、ブレントウッド、セワード・ロウド ５１１６番
(72)発明者 ヌイエンス，ジョウズェフ
アメリカ合衆国テネシー州３７０２７、ブレントウッド、ササフラス・プレイス ５４０９番
(72)発明者 ルーイス，スカット
アメリカ合衆国キャリフォーニア州９５７４２、エルドラド・ヒルズ、ヒルヴュー・コート ６４５番

Ｆターム(参考) 5B017 AA07 BA06 BB07 BB09 CA16

【要約の続き】
される（９２０、９４０）。