【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成19年3月15日(2007.3.15)

【公表番号】特表2006-518901(P2006-518901A)
【公表日】平成18年8月17日(2006.8.17)
【年通号数】公開・登録公報2006-032
【出願番号】特願2006-503101(P2006-503101)
【国際特許分類】
Ｇ０６Ｆ　21/24　(2006.01)
Ｇ０６Ｑ　50/00　(2006.01)
Ｇ０６Ｑ　30/00　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　５６０Ｂ
Ｇ０６Ｆ　17/60　１４２
Ｇ０６Ｆ　17/60　３０２Ｅ
Ｇ０６Ｆ　17/60　ＺＥＣ

【手続補正書】
【提出日】平成19年1月26日(2007.1.26)
【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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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ないし請求項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】
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５０】
請求項４９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、
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５２】
請求項４９ないし請求項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５３】
請求項４９ないし請求項５２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５４】
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５５】
請求項５４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５６】
請求項５４または請求項５５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５７】
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５８】
請求項５７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５９】
請求項５７または請求項５８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６０】
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６１】
請求項６０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６２】
請求項６０または請求項６１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６３】
請求項６０ないし請求項６２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６４】
請求項６０または請求項６１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６５】
請求項６４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６６】
請求項６０ないし請求項６５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６７】
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６８】
請求項６７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６９】
請求項６７または請求項６８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７０】
請求項６７ないし請求項６９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７１】
請求項６７ないし請求項７０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７２】
請求項６７ないし請求項７１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７３】
請求項６７ないし請求項７２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７４】
請求項７３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７５】
請求項７３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７６】
請求項６７ないし請求項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７７】
請求項７６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７８】
請求項６７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７９】
請求項７８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８０】
請求項７８または請求項７９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８１】
請求項７８ないし請求項８０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８２】
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８３】
請求項８２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８４】
請求項８２または請求項８３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、
前記デジタルキーからのロケーションデータを使用するライセンスデータベースにアクセスし、
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８６】
請求項８５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、
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８８】
請求項８５ないし請求項８７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８９】
請求項８５ないし請求項８８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。