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

特許第4790021号
(P4790021)

(45)発行日　平成23年10月12日(2011.10.12)　(24)登録日　平成23年7月29日(2011.7.29)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520D
G06K 17/00	(2006.01)	G06F	12/14	530C
G06K 19/073	(2006.01)	G06F	12/14	560C
G06K 19/07	(2006.01)	G06K	17/00	E
H04L 9/32	(2006.01)	G06K	17/00	B

請求項の数 14　(全 17 頁)　最終頁に続く

(21)出願番号　特願2008-538830 (P2008-538830)
(86)(22)出願日　平成18年11月10日 (2006.11.10)
(65)公表番号　特表2009-516243 (P2009-516243A)
(43)公表日　平成21年4月16日 (2009.4.16)
(86)国際出願番号　PCT/KR2006/004717
(87)国際公開番号　WO2007/055539
(87)国際公開日　平成19年5月18日 (2007.5.18)
審査請求日　平成20年5月2日 (2008.5.2)
(31)優先権主張番号　10-2005-0108263
(32)優先日　平成17年11月11日 (2005.11.11)
(33)優先権主張国　韓国 (KR)

(73)特許権者　502032105
エルジー　エレクトロニクス　インコーポレイティド
大韓民国，ソウル　１５０－７２１，ヨンドゥンポ－ク，ヨイド－ドン，２０
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】ＳＲＭのデジタル著作権管理方法及び装置

(57)【特許請求の範囲】
【請求項１】
ＳＲＭ（Ｓｅｃｕｒｅ　Ｒｅｍｏｖａｂｌｅ　Ｍｅｄｉａ）の権利を管理する方法であって、前記方法は、端末により実行され、
前記方法は、
前記端末により、権利発行サーバからトリガメッセージを受信することと、
前記端末により、前記トリガメッセージに含まれるＳＲＭデバイスパラメータを用いることにより、前記トリガメッセージがＳＲＭにコンテンツに対する権利を提供するためのものであるかをチェックすることであって、前記ＳＲＭデバイスパラメータは、前記ＳＲＭを示す、ことと、
前記トリガメッセージがＳＲＭに権利を提供するためのものであると決定されると、前記端末により、前記権利発行サーバから前記ＳＲＭに対する権利を要求するための権利要求メッセージを生成することであって、前記権利は、前記ＳＲＭに結び付けられており、前記権利要求メッセージは、前記端末のＩＤではなく前記ＳＲＭを識別するためのＳＲＭＩＤを含む、ことと、
前記ＳＲＭが前記ＳＲＭに対する権利を要求したことを確認するために、前記ＳＲＭに対する権利を要求するための前記生成された権利要求メッセージを含むシグネチャ要求メッセージを前記端末から前記ＳＲＭに転送することと、
前記端末により、前記ＳＲＭのシグネチャを含むシグネチャ応答メッセージを前記ＳＲＭから受信することであって、前記シグネチャは、前記ＳＲＭが前記権利を要求すること

を確認する、ことと、
前記ＳＲＭに対して前記ＳＲＭに対する権利を要求するための前記生成された権利要求メッセージを前記端末から前記権利発行サーバに転送することであって、前記ＳＲＭの前記受信されたシグネチャは、前記生成された権利要求メッセージに挿入される、ことと、
前記端末により、権利応答メッセージおよび保護された権利を前記権利発行サーバから受信することであって、前記権利応答メッセージは、前記端末のＩＤではなく前記ＳＲＭＩＤを含み、前記権利は、前記ＳＲＭに暗号により結び付けられている、ことと、
前記端末により、前記保護された権利を、前記受信された権利に関する情報のために用いられるフォーマットに変換することと、
前記ＳＲＭにインストールされるべき前記保護された権利に関する情報を前記端末から前記ＳＲＭに転送することと
を含む、方法。
【請求項２】
前記保護された権利は、ＫＲＥＫ（Ｒｉｇｈｔｓ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ）およびＫＭＡＣ（ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）Ａｌｇｏｒｉｔｈｍ　Ｋｅｙ）を含み、
前記権利応答メッセージ中の前記保護された権利のＫＭＡＣ、ＫＲＥＫおよびＳＲＭＩＤのうちの少なくとも１つは、前記ＳＲＭのパブリックキーによって暗号化される、請求項１に記載の方法。
【請求項３】
前記トリガメッセージは、ＲＯＡＰトリガメッセージである、請求項１に記載の方法。
【請求項４】
前記トリガメッセージ中の前記ＳＲＭデバイスパラメータがチェックされたか否かを決定することをさらに含む、請求項１に記載の方法。
【請求項５】
前記権利応答メッセージは第２のシグネチャを含み、
前記方法は、前記第２のシグネチャを検証することをさらに含む、請求項１に記載の方法。
【請求項６】
前記変換するステップは、前記保護された権利に関する情報が前記ＳＲＭにインストール可能であるように、前記保護された権利に関する情報をフォーマットすることを含む、請求項１に記載の方法。
【請求項７】
ＳＲＭ（Ｓｅｃｕｒｅ　Ｒｅｍｏｖａｂｌｅ　Ｍｅｄｉａ）の権利を管理する端末であって、
前記端末は、権利を管理するためのＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ）エージェントを有するプロセッサを備え、
前記ＤＲＭエージェントは、
前記端末により、権利発行サーバからトリガメッセージを受信するステップと、
前記トリガメッセージに含まれるＳＲＭデバイスパラメータを用いることにより、前記トリガメッセージがＳＲＭにコンテンツに対する権利を提供するためのものであるかをチェックするステップであって、前記ＳＲＭデバイスパラメータは、前記ＳＲＭを示す、ステップと、
前記トリガメッセージがＳＲＭに権利を提供するためのものであると決定されると、前記権利発行サーバから前記ＳＲＭに対する権利を要求するための権利要求メッセージを生成するステップであって、前記権利は、前記ＳＲＭに結び付けられており、前記権利要求メッセージは、前記端末のＩＤではなく前記ＳＲＭを識別するためのＳＲＭ　ＩＤを含む、ステップと、
前記ＳＲＭが前記ＳＲＭに対する権利を要求することを確認するために、前記生成された権利要求メッセージを含むシグネチャ要求を前記端末から前記ＳＲＭに転送するステッ

プと、
前記端末により、前記ＳＲＭのシグネチャを含むシグネチャ応答を前記ＳＲＭから受信するステップであって、前記シグネチャは、前記ＳＲＭが前記権利を要求することを確認する、ステップと、
前記ＳＲＭの前記受信されたシグネチャが挿入される前記生成された権利要求メッセージを前記端末から前記権利発行サーバに転送するステップと、
前記端末により、権利応答メッセージおよび保護された権利を前記権利発行サーバから受信するステップであって、前記権利応答メッセージは、前記ＳＲＭ　ＩＤを含み、前記権利は、前記ＳＲＭに暗号により結び付けられている、ステップと、
前記端末により、前記保護された権利を、前記保護された権利に関する情報のために用いられるフォーマットに変換するステップと、
前記ＳＲＭにインストールされるべき前記保護された権利に関する情報を前記端末から前記ＳＲＭに転送するステップと
を実行する、端末。
【請求項８】
前記保護された権利は、ＫＲＥＫ（Ｒｉｇｈｔｓ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ）およびＫＭＡＣ（ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）　Ａｌｇｏｒｉｔｈｍ　Ｋｅｙ）を含み、
前記権利中のＫＭＡＣ、ＫＲＥＫおよびＳＲＭ　ＩＤのうちの少なくとも１つは、前記ＳＲＭのパブリックキーによって暗号化される、請求項７に記載の端末。
【請求項９】
前記トリガメッセージは、ＲＯＡＰトリガメッセージである、請求項７に記載の端末。
【請求項１０】
前記ＤＲＭエージェントは、さらに、前記トリガメッセージ中の前記ＳＲＭデバイスパラメータが前記ＳＲＭを示すか否かを決定することを実行する、請求項７に記載の端末。
【請求項１１】
前記権利応答メッセージはシグネチャを含み、
前記プロセッサは、さらに、前記第シグネチャを検証するように構成される、請求項７に記載の端末。
【請求項１２】
前記プロセッサは、前記保護された権利に関する情報が前記ＳＲＭにインストール可能であるように、前記保護された権利に関する情報をフォーマットするように構成される、請求項７に記載の端末。
【請求項１３】
前記トリガメッセージ中の前記ＳＲＭデバイスパラメータがチェックされるか否かを決定することをさらに含む、請求項１に記載の方法。
【請求項１４】
前記端末により、前記権利に含まれる前記暗号化されたＫＲＥＫおよびＫＭＡＣを前記ＳＲＭに転送することと、
前記端末により、復号化されたＫＭＡＣキーを前記ＳＲＭから受信することと、
前記端末により、前記復号化されたＫＭＡＣを用いて、前記保護された権利中のＭＡＣ値を検証することと
をさらに含む、請求項２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタル著作権管理（Digital Rights Management：以下、ＤＲＭという）システムに関し、特に、ＤＲＭデジタルコンテンツの使用権利（RightsObject）をＳＲＭ（secure removable media：セキュアリムーバブルメディア）に発行、ダウンロード、及び保存する方法及びシステムに関する。

【背景技術】
【０００２】
一般的に、ＤＲＭは、デジタルコンテンツの使用権利を安全に保護し、体系的に管理するための技術であり、デジタルコンテンツの違法複製、前記デジタルコンテンツの使用権利の取得、及び前記デジタルコンテンツの使用過程に関する一連の保護並びに管理システムを提供する。
【０００３】
図１は、一般的なＤＲＭシステムを示す。
【０００４】
一般的なＤＲＭシステムは、前記ユーザがユーザに与えられた使用権利（ＲＯ）分の前記デジタルコンテンツを使用できるように、コンテンツプロバイダからユーザに提供されたデジタルコンテンツを制御する。ここで、前記コンテンツプロバイダは、コンテンツ発行者（Contents Issuer：ＣＩ）及び／又は使用権利発行者（Rights Issuer：ＲＩ）に該当するエンティティである。
【０００５】
前記コンテンツ発行者は、アクセス権利を有しないユーザからＤＲＭコンテンツを保護できるように特定暗号化キーを用いて保護されたコンテンツ（以下、ＤＲＭコンテンツ（又は、デジタルコンテンツ）という）を発行し、前記ＤＲＭコンテンツを使用するために必要な使用権利を発行する。
【０００６】
ＤＲＭエージェントは、端末に搭載され、前記コンテンツ発行者及び前記使用権利発行者からＤＲＭコンテンツ及び使用権利を受信し、前記使用権利に含まれる許可権（Permission）及び／又は制約（Constraint）を解析することにより該当端末における前記ＤＲＭコンテンツの使用を制御する。
【発明の開示】
【発明が解決しようとする課題】
【０００７】
一般的に、前記使用権利は、特定端末の公開キーにより暗号化されているので、前記公開キーに対応する秘密キーを所有した端末以外の端末は、前記使用権利に関するＤＲＭコンテンツを復号化及び使用することができない。
【０００８】
従って、一般的なＤＲＭシステムにおいて、前記使用権利及びそれに関するＤＲＭコンテンツがマルチメディアカードなどの携帯用メモリカード（すなわち、ＳＲＭ）に保存された場合、前記使用権利が発行された特定端末以外の他端末は、前記メモリカード（すなわち、ＳＲＭ）から前記ＤＲＭコンテンツを読み取ることができないという問題がある。
【０００９】
また、一般的なＤＲＭシステムにおいて、前記使用権利が前記特定端末に発行されているので、前記メモリカードに前記使用権利及び該使用権利に関連するＤＲＭコンテンツが保存される場合、前記使用権利が発行されている前記特定端末のみが前記ＳＲＭから前記ＤＲＭコンテンツ及び前記使用権利を読み取ることができる。従って、前記ＳＲＭの有用性が低下するという問題が発生する。
【００１０】
さらに、一般的なＤＲＭシステムにおいて、コンテンツプロバイダが前記ＳＲＭに前記ＤＲＭコンテンツの使用権利を発行できないので、前記ＳＲＭがＳＲＭ名義の使用権利を有することができないという問題が発生する。
【課題を解決するための手段】
【００１１】
従って、本発明の目的は、メモリカードがメモリカード名義の使用権利を保有できるメモリカードのデジタル著作権管理方法及び装置を提供することにある。
【００１２】

本発明の他の目的は、メモリカードにＤＲＭコンテンツの使用権利を発行、ダウンロード、保存する方法及びシステムを提供することにある。

【００１３】

本発明のさらに他の目的は、前記ＳＲＭに接続された端末がＳＲＭ名義でコンテンツ使用権利を取得して前記ＳＲＭに伝送するＳＲＭの使用権利管理方法及び装置を提供することにある。

【００１４】

上記の目的を達成するために、本発明は、ＳＲＭ名義の使用権利をサーバから受信する端末と、前記端末を介して前記使用権利を受信するＳＲＭとを含むＳＲＭの使用権利管理システムを提供する。

【００１５】

本発明の他の態様において、本発明は、デバイスが使用権利発行者にＳＲＭ名義の使用権利を要求する過程と、前記デバイスが前記コンテンツプロバイダから前記ＳＲＭ名義の使用権利を受信する過程と、前記デバイスが前記ＳＲＭ名義の使用権利をＳＲＭに伝送する過程とを含むＳＲＭの使用権利管理方法を提供する。

【００１６】

本発明の他の態様において、本発明は、ＳＲＭ名義の使用権利が使用権利発行者から端末に発行できることを通知するためのトリガを使用権利発行者が前記端末に伝送する過程と、前記使用権利発行者が前記端末を介して前記ＳＲＭ名義の使用権利の要求を受信する過程と、前記使用権利発行者が前記端末を介して前記ＳＲＭ名義の使用権利を前記ＳＲＭに発行する過程とを含むＳＲＭの使用権利管理方法を提供する。

【００１７】

本発明の他の態様において、本発明は、ＳＲＭのデジタル著作権を管理するための端末を提供し、前記端末は、ＳＲＭ名義の使用権利を受信するＤＲＭエージェントを含む。

【００１８】

前記ＤＲＭエージェントは、前記受信された使用権利を前記ＳＲＭに伝送する。

【００１９】

本発明の他の態様において、本発明は、デジタル著作権を管理するためのＳＲＭを提供し、前記ＳＲＭは、接続された端末を介して使用権利発行者からＳＲＭ名義の使用権利を受信するＤＲＭエージェントを含む。

【００２０】

本発明の他の態様において、本発明は、ＳＲＭのための使用権利管理方法を提供し、前記方法は、端末がＳＲＭ名義の使用権利を要求するための使用権利要求メッセージを使用権利発行者に送信する過程と、前記端末が前記使用権利発行者から応答メッセージを受信する過程と、前記端末が前記応答メッセージに含まれる使用権利を検証してＳＲＭに伝送する過程と、前記ＳＲＭが前記伝送された使用権利を検証してインストールする過程とを含む。

【００２１】

本発明の他の態様において、メモリカードの使用権利管理方法は、サーバから受信された使用権利応答メッセージに含まれる使用権利を端末がメモリカードに連動して検証する過程と、前記端末が前記使用権利を前記メモリカードが解析できる特定フォーマットに変換して前記メモリカードに伝送する過程とを含む。

【００２２】

本発明の他の態様において、メモリカードの使用権利管理方法は、サーバから受信された使用権利応答メッセージに含まれる使用権利を端末がメモリカードと連動して検証可能にする過程と、前記使用権利検証が失敗した場合、前記端末が前記使用権利のインストール失敗を通知可能にする過程とを含む。

【００２３】

本発明の他の態様において、ＳＲＭ名義の使用権利管理方法は、使用権利発行者からホストデバイスにＲＯＡＰトリガを伝送する過程と、前記ホストデバイスから前記使用権利

発行者にＲＯ要求メッセージを送信し、前記要求メッセージに対する応答メッセージを前記使用権利発行者から前記ホストデバイスに受信する過程と、前記応答メッセージに含まれる使用権利を前記ホストデバイスのＤＲＭエージェントからＳＲＭのＤＲＭエージェントに伝送してインストールする過程とを含む。

【００２４】

本発明の前記及び他の目的、特徴、態様、及び長所は、後述する発明の詳細な説明及び添付図面によりさらに明確になるであろう。

【発明を実施するための最良の形態】

【００２５】

以下、添付図面を参照して本発明の好ましい実施形態を説明する。

【００２６】

本発明は、メモリカードに接続された端末を介して前記メモリカード名義の使用権利（ＲＯ）が発行される。前記端末は、メモリカード名義の使用権利（ＲＯ）がコンテンツプロバイダ、すなわち、使用権利発行者（ＲＩ）に用意され、前記メモリカード名義の使用権利が前記メモリカードにインストールされることを端末に通知するＲＯ取得トリガ（RO Acquisition trigger：ＲＯＡＰトリガ）を受信する。前記端末は、少なくとも前記メモリカードのデバイスＩＤ及び前記メモリカードのデジタル署名値（signaturevalue）を含むＲＯ要求メッセージを生成して前記使用権利発行者（ＲＩ）に送信する。前記使用権利発行者は、前記使用権利要求メッセージに含まれるメモリカードのデバイスＩＤとメモリカード名義の使用権利を少なくとも含む応答メッセージ（ＲＯ応答）を送信する。前記端末は、前記応答メッセージに含まれる使用権利を前記メモリカードに伝送し、前記メモリカードは、前記使用権利を検証してインストールする。

【００２７】

前記ＲＯＡＰトリガは、前記メモリカードのデバイスＩＤを含む。前記ＲＯ要求メッセージは、前記メモリカードのデバイスＩＤ、前記メモリカードの署名値、及び前記メモリカードの認証チェーン（certificate chain）を含む。前記応答メッセージは、前記メモリカードのデバイスＩＤと前記メモリカード名義の使用権利を含む。

【００２８】

以下、添付図面を参照して本発明の好ましい実施形態について説明する。

【００２９】

図２は、本発明によるメモリカードの使用権利管理システムを示す。

【００３０】

図２に示すように、本発明によるメモリカードのデジタル著作権管理システムは、メモリカードのＩＤを用いて使用権利を受信し、前記使用権利を前記メモリカード１０に伝送する端末２０と、前記端末２０を介して前記メモリカード１０のＩＤを用いて前記使用権利を受信する前記メモリカード１０とを含む。

【００３１】

前記デジタル著作権管理システムは、前記端末２０の要求に応じてＤＲＭコンテンツ及び／又はメモリカード名義の使用権利を発行するコンテンツプロバイダをさらに含む。前記コンテンツプロバイダは、デジタルコンテンツの使用権利を発行する使用権利発行者（ＲＩ）３０を含む。

【００３２】

前記端末２０は、メモリカード名義の使用権利を要求する使用権利要求メッセージを生成して送信し、前記使用権利発行者３０から発行されたメモリカード名義の使用権利を前記メモリカード１０に伝送するＤＲＭエージェント２１を含む。

【００３３】

前記メモリカード１０は、セキュアリムーバブルメディア（ＳＲＭ）という。前記ＳＲＭ１０は、前記端末２０と相互認証を行い、前記端末２０の要求に応じてＳＲＭのデジタル署名値を前記端末２０に伝送し、前記端末２０を介してＤＲＭコンテンツ及び／又はＳＲＭ名義の使用権利を受信するＤＲＭエージェント１１を含む。

【００３４】
前記端末２０は、前記使用権利発行者３０と通信する通信モジュール２２と、ＤＲＭコンテンツ及び／又は使用権利を受信するために、前記ＤＲＭエージェント２１の制御により、前記使用権利発行者３０にアクセスするｗｅｂ/ＷＡＰ（wireless application protocol）ブラウザ２３と、前記ＤＲＭエージェント２１の制御により、ユーザとインタフェースするユーザインタフェース２６とをさらに含む。
【００３５】
前記端末２０は、前記ＤＲＭコンテンツのメタデータ及び／又は前記使用権利のメタデータを保存するメディアライブラリー２４と、前記ＤＲＭコンテンツ、並びに前記ＤＲＭエージェント２１のアプリケーションプログラム及びデータを保存するメモリ２５とをさらに含む。
【００３６】
前記コンテンツプロバイダは、前記ＤＲＭコンテンツを発行するコンテンツ発行者及び／又は前記ＳＲＭ名義の使用権利を発行する使用権利発行者３０を含む。
【００３７】
前記ＳＲＭ１０は、簡単な計算（又は、処理）機能を実行するためにプロセッサ及びメモリを含む携帯用メモリカードでもよい。
【００３８】
前記ＳＲＭ１０は、前記端末２０を介して受信されたＤＲＭコンテンツ及び／又は使用権利を含むＳＲＭＤＲＭエージェント情報を保存するメモリ１２をさらに含む。
【００３９】
前記ＳＲＭ ＤＲＭエージェント情報は、ＤＲＭコンテンツ、前記ＤＲＭコンテンツのメタデータ、前記ＤＲＭコンテンツの使用権利、前記使用権利のメタデータ、前記使用権利発行者のＲＩコンテキスト、及び前記使用権利を受信するためのドメインのドメインコンテキストを含む。
【００４０】
前記ＳＲＭエージェント１１は、前記ＳＲＭ名義の使用権利を要求する前記使用ＲＯメッセージに含まれるＳＲＭ署名値を前記端末２０のＤＲＭエージェント２１に伝送し、前記ＤＲＭエージェント２１を介して伝送された使用権利を検証する。前記ＳＲＭエージェント１１は、前記端末２０とセキュリティリンクを設定する。前記セキュリティリンクは、セキュリティ通信チャネルを示す。
【００４１】
前記ＳＲＭ１０は、セキュアデジタル（secure digital：ＳＤ）カード、マルチメディアカード（multi-media card：ＭＭＣ）、スマートメディアカード（smartmedia card：ＳＭＣ）、ＳＩＭ（Subscriber Identification Module）カード、及びマルチメディアを保存できる各種メモリカードを含む。
【００４２】
前記ユーザインタフェース２６は、キーパッド、ジョグシャトル、スイッチ、ファンクションキー、ソフトキー、メニューの少なくとも１つを含む。
【００４３】
以下、前述したように構成された本発明によるＳＲＭのデジタル著作権管理システムの動作について添付図面を参照して説明する。
【００４４】
前記ＳＲＭ１０は通信モジュールを有していないため、前記端末２０を介して前記ＤＲＭコンテンツの使用権利を受信しようとする。
【００４５】
図３及び図４は、本発明によるＳＲＭのデジタル著作権管理方法を示す。
【００４６】
まず、本発明による前記ＳＲＭのデジタル著作権管理方法の第１実施形態について説明する。

【００４７】
前記ＳＲＭ１０が前記端末２０に挿入された後、電源が供給されると、前記端末２０は、前記ＳＲＭ１０を認識し（Ｓ１１）、前記ＳＲＭ１０のＤＲＭエージェント１１と相互認証を行う（Ｓ１２）（以下、前記ＳＲＭ１０のＤＲＭエージェント１１は、前記ＳＲＭＤＲＭエージェント１１を意味する）。ここで、前記端末ＤＲＭエージェント２１及び前記ＳＲＭ ＤＲＭエージェント１１は、端末ＩＤ（端末１０のデバイスＩＤ）とＳＲＭＩＤ（ＳＲＭ１０のデバイスＩＤ）を互いに確認する。
【００４８】
相互認証が正常に完了すると、前記端末ＤＲＭエージェント２１及び前記ＳＲＭＤＲＭエージェント１１は、セキュリティ通信チャネルを設定する。ここで、前記端末ＤＲＭエージェント２１と前記ＳＲＭ ＤＲＭエージェント１１間のセキュリティ通信チャネルが選択的に設定される（Ｓ１３）。
【００４９】
前記端末ＤＲＭエージェント２１は、ＳＲＭ１１のＤＲＭエージェント情報をＳＲＭＤＲＭエージェント１１に要求する（Ｓ１４）（以下、ＳＲＭのＤＲＭエージェント情報はＳＲＭ ＤＲＭエージェント情報を意味する）。前記ＳＲＭ ＤＲＭエージェント１１は、要求された前記ＳＲＭＤＲＭエージェント情報を前記端末ＤＲＭエージェント２１に提供する（Ｓ１５）。この段階Ｓ１４及びＳ１５は、前記セキュリティ通信チャネルで行われる。前記ＳＲＭ ＤＲＭエージェント情報は、前記ＳＲＭ１０のメモリ１２に保存される。前記ＳＲＭＤＲＭエージェント情報は、ＤＲＭコンテンツ、前記ＤＲＭコンテンツのメタデータ、前記ＤＲＭコンテンツの使用権利、前記使用権利のメタデータ、前記使用権利発行者のＲＩコンテキスト、及び前記使用権利を受信するためのドメインのドメインコンテキストを含む。
【００５０】
前記ＳＲＭ ＤＲＭエージェント情報が前記ＳＲＭ１０により提供される場合、前記端末２０は、前記ＳＲＭＤＲＭエージェント情報と前記メディアライブラリー２４に保存されている情報に基づいて、発行されるＤＲＭコンテンツ及び使用権利を確認する。
【００５１】
前記特定ＤＲＭコンテンツがＳＲＭ１０と端末２０の少なくとも１つに予め保存されている場合、前記端末２０は、前記特定ＤＲＭコンテンツをダウンロードしない。前記端末２０は、前記特定ＤＲＭコンテンツを再生するための使用権利を受信するためにコンテンツ購入要求（content purchase request）をコンテンツプロバイダのコンテンツ発行者（ＣＩ）に送信する。
【００５２】
前記特定ＤＲＭコンテンツが前記ＳＲＭ１０と端末２０のどちらにも保存されていない場合、前記端末２０は、前記ＤＲＭコンテンツと前記ＤＲＭコンテンツの再生のための使用権利を要求するためにコンテンツ購入要求をコンテンツプロバイダのコンテンツ発行者（ＣＩ）に送信する。
【００５３】
前記端末２０は、特定ＤＲＭコンテンツを要求するためにｗｅｂ／ＷＡＰブラウザ２３を介して前記コンテンツ発行者の所定ドメインにアクセスする（Ｓ１６）。前記特定ＤＲＭコンテンツを要求する場合、前記端末２０は、デバイスパラメータを前記コンテンツ発行者に伝送する。前記デバイスパラメータは、前記使用権利が属するデバイスの識別子を示す。例えば、前記使用権利は前記ＳＲＭに属し、前記デバイスパラメータはＳＲＭＩＤを示す。
【００５４】
前記特定ＤＲＭコンテンツの購入要求を受信した前記コンテンツ発行者は、前記特定ＤＲＭコンテンツに対する使用権利の生成を使用権利発行者３０に要求する（Ｓ１７）。ここで、前記コンテンツ発行者は、前記端末２０から伝送されたデバイスパラメータを前記使用権利発行者３０に伝送する。また、前記コンテンツ発行者は、前記ＤＲＭコンテンツ

のＩＤのメタデータを前記使用権利発行者３０に伝送する。

【００５５】

その後、前記使用権利発行者３０は、前記デバイスパラメータに基づいて前記ＤＲＭコンテンツの使用権利を生成する（Ｓ１８）。前記デバイスパラメータが前記ＳＲＭ１０のデバイスＩＤを示す場合、前記使用権利発行者３０は、前記ＳＲＭ１０名義の使用権利を生成する。

【００５６】

前記使用権利発行者３０は、前記ＳＲＭ１０の使用権利が生成されていることを通知するために、デバイスパラメータを含むＲＯ生成確認メッセージを前記コンテンツ発行者に送信する（Ｓ１９）。

【００５７】

前記コンテンツ発行者は、前記ＤＲＭコンテンツの使用権利を受信することを端末２０に通知するために、使用権利ダウンロードトリガ、すなわち、ＲＯ取得トリガ（ＲＯＡＰトリガ）を前記端末２０に伝送する（Ｓ２０）。前記ＲＯＡＰトリガは、前記デバイスパラメータ（すなわち、ＳＲＭＩＤ）と前記使用権利発行者３０の情報を含む。また、前記コンテンツ発行者は、前記ＲＯＡＰトリガを前記ＤＲＭコンテンツとともに端末２０に送信する。前記ＤＲＭコンテンツは、前記端末２０に保存されるか、又は前記ＳＲＭ１０に保存される。前記端末２０は、ダウンロードされた前記特定ＤＲＭコンテンツのメモリ領域をユーザが決定できるようにするインタフェース（例えば、ＧＵＩ（graphic user interface））を提供する。

【００５８】

前述した段階Ｓ１６～Ｓ１９は、行われないこともある。

【００５９】

一方、段階Ｓ１１～Ｓ１５が行われた後、前記端末２０は、使用権利を受信するために前記使用権利発行者３０からＲＯＡＰトリガを受信できる（Ｓ２０）。

【００６０】

このように、前記使用権利発行者３０からＲＯＡＰトリガを受信した端末２０は、前記ＲＯＡＰトリガに含まれるデバイスパラメータ（ＳＲＭＩＤ）を確認する（Ｓ２１）。

【００６１】

前記デバイスパラメータがＳＲＭ ＩＤを示す場合、前記端末２０は、ＳＲＭ１０のＳＲＭエージェント１１に認証チェーンを要求し（Ｓ２２）、前記認証チェーンを受信する（Ｓ２３）。前記受信されたＳＲＭ認証チェーンは、前記ＳＲＭ１０の公開キーを含む。前記端末２０がＳＲＭ１０に接続されていない場合、前記端末２０は、前記ＳＲＭ１０名義の使用権利の受信手順（すなわち、ＲＯＡＰトランザクション）を直ちに終了する。

【００６２】

前記端末２０は、前記ＳＲＭ名義の使用権利を要求するために、ＳＲＭＩＤを用いることにより、前記段階Ｓ２３で受信した前記ＳＲＭ認証チェーンを含むＲＯ要求メッセージを生成する（Ｓ２４）。

【００６３】

このように、前記ＳＲＭ１０名義の使用権利を要求するためのＲＯ要求メッセージが生成されると、前記端末２０は、前記ＳＲＭ１０のＤＲＭエージェント１１に前記ＲＯ要求メッセージを送信し、前記ＤＲＭエージェント１１にデジタル署名を要求する（Ｓ２５）。

【００６４】

前記ＳＲＭ１０のＤＲＭエージェント１１は、ＤＲＭエージェント１１の秘密キーを用いてデジタル署名を生成した後、前記端末２０のＤＲＭエージェント２１に前記生成されたデジタル署名を伝送する（Ｓ２６）。

【００６５】

前記端末２０のＤＲＭエージェント２１は、前記ＤＲＭエージェント１１から受信したＳＲＭデジタル署名を含む前記使用権利要求メッセージを使用権利発行者３０に送信する

（Ｓ２７）。
【００６６】
前記使用権利発行者３０は、ＳＲＭ ＩＤと使用権利を含むＲＯ応答メッセージを端末２０に送信する（Ｓ２８）。デジタルコンテンツと使用権利が共に伝送される複合伝送（combined delivery）の場合、前記使用権利が前記端末２０に伝送されるときに前記コンテンツも共に端末２０に伝送される。
【００６７】
前記端末２０のＤＲＭエージェント２１は、前記応答メッセージを解析し、前記応答メッセージのデジタル署名を検証する（Ｓ２９）。
【００６８】
このようにして、メッセージ検証が正常に完了すると、前記端末２０のＤＲＭエージェント２１は、前記使用権利応答メッセージに含まれている使用権利のメタデータを前記メディアライブラリー２４に登録する。前記使用権利とともにコンテンツが伝送された場合、前記端末２０は、前記コンテンツのメタデータもメディアライブラリー２４に登録する。ユーザが希望する場合、前記コンテンツを前記端末２０に保存する。
【００６９】
前記端末２０は、前記使用権利発行者３０から伝送された前記使用権利を、必要に応じてＳＲＭ１０のＤＲＭエージェント１１が解析できるフォーマットに変換できる（Ｓ３３）。前記端末２０は、前記使用権利をＳＲＭ１０のＤＲＭエージェント１１に伝送して前記使用権利のインストールを指示する（Ｓ３４）。ここで、前記使用権利とともに前記コンテンツもＳＲＭ１０に伝送される。前記ＳＲＭ１０のＤＲＭエージェント１１は、前記使用権利のインストールの結果を前記端末２０のＤＲＭエージェント２１に通知する（Ｓ３８）。
【００７０】
以下、本発明によるＳＲＭのデジタル著作権管理方法の第２実施形態について説明する。
【００７１】
第２実施形態は、図４に示す段階Ｓ３０～Ｓ３２、Ｓ３５～Ｓ３６が第１実施形態に加えられて行われる方式である。
【００７２】
第２実施形態の段階Ｓ１１～Ｓ２９は、第１実施形態の段階Ｓ１１～Ｓ２９と同一であるので、以下、段階Ｓ３０～Ｓ３６について説明する。
【００７３】
前記端末２０のＤＲＭエージェント２１がＲＯ要求メッセージに対する応答として応答メッセージを使用権利発行者（ＲＩ）３０から受信すると、前記ＤＲＭエージェント２１は、前記ＳＲＭ１０のＤＲＭエージェント１１と連動して前記応答メッセージに含まれる使用権利を検証する。すなわち、前記端末２０のＤＲＭエージェント２１は、前記応答メッセージに含まれる前記使用権利の検証のために前記ＳＲＭ１０のＤＲＭエージェント１１にＲＯ検証情報を要求する。つまり、前記端末２０のＤＲＭエージェント２１は、暗号化されたＫＲＥＫ（Rights Encryption Key；使用権利を暗号化するキー）又は暗号化されたＫＭＡＣ（使用権利の完全性を検証するためにＭＡＣアルゴリズムに使用されるキー）の復号化を要求する（Ｓ３０）。
【００７４】
前記ＳＲＭ１０のＤＲＭエージェント１１は、ＤＲＭエージェント１１が有している秘密キー又はドメインキーを用いてＫＲＥＫ又はＫＭＡＣを復号化し、前記復号化したＫＲＥＫ又はＫＭＡＣを前記端末２０のＤＲＭエージェント２１に伝送する（Ｓ３１）。
【００７５】
前記端末２０のＤＲＭエージェント２１は、前記伝送されたＫＲＥＫ又はＫＭＡＣを用いることにより、前記応答メッセージに含まれる使用権利のＭＡＣ値を検証する（Ｓ３２）。

【００７６】
前記メッセージ検証が正常に完了すると、前記端末２０のＤＲＭエージェント２１は、前記応答メッセージに含まれている使用権利のメタデータをメディアライブラリー２４に登録する。前記使用権利とともにコンテンツが伝送された場合、前記端末２０は、前記コンテンツのメタデータもメディアライブラリー２４に登録する。ユーザが希望する場合、前記端末２０は、前記コンテンツを前記端末２０に保存する。
【００７７】
前記端末２０は、前記使用権利発行者３０から伝送された前記使用権利を、必要に応じてＳＲＭ１０のＤＲＭエージェント１１が解析できるフォーマットに変換する（Ｓ３３）。前記端末２０は、使用権利をＳＲＭ１０のＤＲＭエージェントに伝送した後、インストールを要求する（Ｓ３４）。
【００７８】
前記ＳＲＭ１０のＤＲＭエージェント１１は、ＤＲＭエージェント１１が有している秘密キー又はドメインキーで復号化されたＫＭＡＣを用いることにより、前記ＤＲＭエージェント２１から伝送された前記使用権利のＭＡＣ値を検証する（Ｓ３５）。その結果、ＭＡＣ値が有効であると、前記ＳＲＭ１０のＤＲＭエージェント１１は、前記伝送された使用権利をインストールする（Ｓ３７）。前記ＭＡＣ値が有効でないと、前記ＳＲＭ１０のＤＲＭエージェント１１は、前記伝送された使用権利をインストールせずに放棄する。
【００７９】
一方、前記検証されたＭＡＣ値が前記段階Ｓ３５で有効な場合、前記ＤＲＭエージェント１１は、前記伝送された使用権利に含まれるデジタル署名値を検証する（Ｓ３６）。前記デジタル署名値が有効である場合、前記ＳＲＭ１０のＤＲＭエージェント１１は、前記伝送された使用権利をインストールする（Ｓ３７）。
【００８０】
前記ＳＲＭ１０のＤＲＭエージェント１１は、前記ＭＡＣ値又は前記デジタル署名値が有効でない場合、前記伝送された使用権利をインストールせずに放棄する。
【００８１】
前記使用権利をインストールした後、前記ＳＲＭ１０は、使用権利インストールに関する確認メッセージを前記端末２０に送信する（Ｓ３８）。
【００８２】
以下、本発明の第３実施形態によるＳＲＭのデジタル著作権取得方法について説明する。
【００８３】
まず、前記ユーザが前記使用権利発行者に接続すると、前記使用権利発行者は、前記使用権利が前記ＳＲＭにインストールされなければならないことを示すＲＯＡＰトリガを前記端末のＤＲＭエージェントに伝送する。
【００８４】
前記端末のＤＲＭエージェントは、前記ＳＲＭの前記ＤＲＭエージェントに認証書（Certificate）を要求し、前記ＳＲＭの前記ＤＲＭエージェントから前記認証書を受信する。
【００８５】
前記端末のＤＲＭエージェントは、前記ＳＲＭの認証書を含むＲＯ要求メッセージを生成し、前記生成されたＲＯ要求メッセージのデジタル署名値をＳＲＭのＤＲＭエージェントを介して取得する（ここで、前記ＳＲＭのＤＲＭエージェントは、ＤＲＭエージェントの秘密キーを用いてデジタル署名値を計算した後、前記端末に前記デジタル署名値を伝送する）。前記端末は、前記ＳＲＭのＤＲＭエージェントから取得した前記デジタル署名値を前記オリジナルＲＯ要求メッセージに添付して前記使用権利発行者に送信する。ここで、前記ＲＯ要求メッセージは、少なくともＳＲＭＩＤ、ＳＲＭ認証チェーン、及びＳＲＭ情報を含む。前記ＳＲＭ認証チェーンは、前記端末がＳＲＭに接続されていることを示し、前記端末が前記ＳＲＭに接続されていない場合、前記端末は、ＳＲＭ名義の使用権利を

受信するための後続の手順を直ちに終了する。

【００８６】

前記使用権利発行者は、前記ＳＲＭの公開キーにより暗号化されたＲＯ、ＳＲＭＩＤ、及びデジタル署名値を含むＲＯ Ｒｅｓｐｏｎｓｅメッセージ（応答メッセージ）を端末に送信する。前記デジタル署名値は、前記ＲＯ要求メッセージにより受信されたデジタル署名値と同じ値である。その後の応答メッセージの実行過程は、図４に示す段階Ｓ２９～Ｓ３８と同一である。

【００８７】

次に、本発明の他の一実施形態によるＳＲＭの使用権利取得方法を成功ケースと失敗ケースに基づいて説明する。

【００８８】

前記ＲＯ要求メッセージを送信し、使用権利発行者（使用権利発行サーバ）からＲＯ応答メッセージを受信すると、前記端末のＤＲＭエージェントは、前記ＳＲＭの認証書を要求して受信する。前記端末のＤＲＭエージェントは、前記ＳＲＭのＤＲＭエージェントと連動して前記ＲＯ応答メッセージに含まれる使用権利（ＲＯ）を検証する過程を経る。すなわち、前記端末のＤＲＭエージェントは、前記ＲＯ応答メッセージに含まれる前記ＲＯを検証するために、ＫＲＥＫとＫＭＡＣの復号化を前記ＳＲＭのＤＲＭエージェントに要求する。

【００８９】

前記ＳＲＭのＤＲＭエージェントは、ＫＭＡＣとＫＲＥＫを前記ＳＲＭの秘密キーを用いて復号化し、前記復号化したＫＭＡＣを前記端末のＤＲＭエージェントに伝送する。

【００９０】

前記端末のＤＲＭエージェントは、前記受信したＫＭＡＣを用いて前記ＲＯの完全性を確認する。

【００９１】

前記端末のＤＲＭエージェントは、前記ＲＯに含まれる一対の暗号化されたＣＥＫとコンテンツＩＤをＲＯＩＤとともに前記ＳＲＭのＤＲＭエージェントに伝送し、前記ＳＲＭのＤＲＭエージェントに前記ＣＥＫの復号化を要求する。

【００９２】

前記ＳＲＭのＤＲＭエージェントは、前記端末のＤＲＭエージェントから伝送された前記暗号化されたＣＥＫを前記復号化した前記ＫＲＥＫを用いて復号化し、各ＣＥＫをコンテンツＩＤにバインドすることにより保存し、ＣＥＫの復号化が成功したか否かを前記端末のＤＲＭエージェントに伝送する。

【００９３】

前記ＣＥＫの復号化が成功した場合、前記ＳＲＭのＤＲＭエージェントは、前記復号化の成功を前記端末のＤＲＭエージェントに通知する。その後、前記ＳＲＭのＤＲＭエージェントは、前記端末のＤＲＭエージェントの要求に応じてＲＯＩＤとコンテンツＩＤを用いてＣＥＫを探して前記端末のＤＲＭエージェントに伝送する。前記端末のＤＲＭエージェントは、ＲＯを前記ＳＲＭが認識できるフォーマット（例えば、ＳＲＭＦ（Secure Removable Media Format for Rights Object））に変換し、前記ＳＲＭのＤＲＭエージェントに前記ＲＯを伝送して前記ＲＯのインストールを命令する。前記ＳＲＭのＤＲＭエージェントは、ＲＯのインストールが成功したか否かを前記端末のＤＲＭエージェントに伝送する。

【００９４】

しかしながら、前記暗号化されたＣＥＫの復号化が失敗した場合、前記ＳＲＭのＤＲＭエージェントは、前記暗号化されたＣＥＫの復号化が失敗したことを前記端末のＤＲＭエージェントに通知する。

【００９５】

前記ＲＯのインストールが成功したか否かを示すフラグが前記使用権利発行者から受信されたＲＯＡＰトリガに設定されている場合、前記端末のＤＲＭエージェントは、ＲＯＩ

Ｄと前記ＲＯがＳＲＭに正常にインストールされているか否かを前記使用権利発行者に伝送する。前記ＲＯがＳＲＭに正常にインストールされている場合、前記端末のＤＲＭエージェントは、ＲＯＩＤとともにＳＲＭへのＲＯのインストールの成功を前記使用権利発行者に伝送する。前記ＲＯが前記ＳＲＭに正常にインストールされていない場合、前記端末のＤＲＭエージェントは、ＲＯＩＤとともに前記ＲＯのインストールの失敗を使用権利発行者に伝送する。前記端末のＤＲＭエージェントは、前記ＲＯのＳＲＭへのインストールが成功したか否かをユーザに通知する。

【００９６】

前述したように、本発明において、前記ＳＲＭは、通信モジュールを有する前記端末を介して前記ＤＲＭコンテンツ及び／又は前記使用権利を受信できる。

【００９７】

図５は、図３及び図４に示すＳＲＭの使用権利管理方法を示す。

【００９８】

図５に示すように、前記ＳＲＭ名義の使用権利は、ホストデバイスを介して前記使用権利発行者から発行される。前記ＳＲＭ名義の使用権利を受信する手順は、（Ａ）前記使用権利発行者から前記ホストデバイスにＲＯＡＰトリガを伝送する段階と、（Ｂ）前記ホストデバイスから前記使用権利発行者にＲＯ要求メッセージを送信し、前記ＲＯ要求メッセージに対するＲＯ応答メッセージを受信する段階と、（Ｃ）前記ＲＯ応答メッセージに含まれる使用権利を前記ホストデバイスのＤＲＭエージェントから前記ＳＲＭのＤＲＭエージェントに伝送し、前記使用権利をインストールする段階とを含む。

【００９９】

前記ホストデバイス（例えば、端末）は、前記ＲＯＡＰトリガを前記使用権利発行者から受信する。前記ＲＯＡＰトリガは、少なくともＳＲＭＩＤを含む。

【０１００】

前記ホストデバイスは、前記ＳＲＭ名義の使用権利を要求するためのＲＯ要求メッセージを前記使用権利発行者に送信する。前記ＲＯ要求メッセージは、少なくともＳＲＭＩＤ、ＳＲＭの認証チェーン、及びＳＲＭ情報を含む。ここで、前記ＳＲＭ ＩＤは、前記ＲＯＡＰトリガに含まれるＳＲＭ ＩＤと同じ値である。前記ＳＲＭ情報は、前記ＳＲＭのデジタル署名値を含む。前記ＳＲＭ認証チェーンにより前記ＳＲＭの公開キーが前記使用権利発行者に伝送され、前記使用権利発行者は、前記ＳＲＭの公開キーを用いて前記ＳＲＭの署名値を検証する。前記ＳＲＭが前記ホストデバイスに接続されていない場合、前記ホストデバイスは、前記ＳＲＭ名義のＲＯを受信する手順を直ちに終了する（すなわち、ＲＯＡＰトランザクションを終了する）。

【０１０１】

前記ホストデバイスは、前記ＲＯ要求メッセージに対するＲＯ応答メッセージを前記使用権利発行者から受信する。前記ＲＯ応答メッセージは、少なくとも前記ＳＲＭＩＤ、デジタル署名、及び保護された使用権利（protected RO）を含む。

【０１０２】

前記ホストデバイスは、前記ＲＯ応答メッセージに含まれる前記ＲＯをインストールすることを前記ＳＲＭに通知し、前記ＳＲＭは、前記ＲＯ応答メッセージに含まれる前記ＲＯを検証して前記ＲＯをインストールする。前記ＳＲＭは、ＳＲＭの秘密キー又はドメインキーを用いてＭＡＣキーを復号化し、前記復号化したＭＡＣキーを用いて前記ＲＯ応答メッセージに含まれるＲＯのＭＡＣ値を検証する。前記ＲＯのＭＡＣ値が有効である場合、前記ＳＲＭは、前記ＲＯをインストールする。また、前記ＳＲＭは、前記ＲＯ応答メッセージに含まれるＲＯのＭＡＣ値及び前記ＲＯ応答メッセージのデジタル署名値を検証し、前記ＭＡＣ値と前記デジタル署名値の両方が有効である場合、前記ＳＲＭは、前記ＲＯをインストールする。

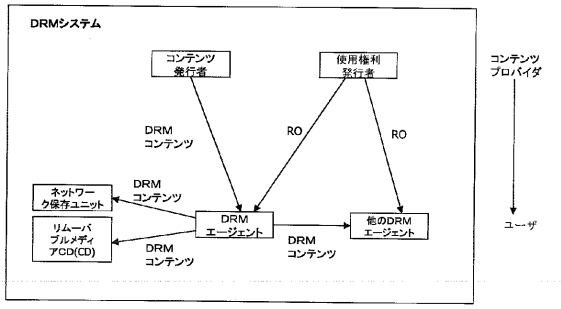
【０１０３】

前述したように、メモリカードのデジタル著作権管理方法及び装置には、次のような利点がある。

【０１０４】
前記ＳＲＭを有する端末は、前記ＳＲＭのＤＲＭエージェントと連動して前記ＳＲＭ名義の使用権利を要求するメッセージを生成し、前記ＲＯ要求メッセージを使用権利発行者に送信することにより、前記使用権利発行者により発行された前記ＳＲＭ名義の使用権利を前記ＳＲＭにインストールできる。
【０１０５】
前記ＳＲＭに接続された端末が前記ＳＲＭとの連動により前記ＳＲＭ名義の使用権利を要求するＲＯ要求メッセージを生成するので、前記使用権利発行者は、ＳＲＭ名義の使用権利を発行できる。
【０１０６】
前記ＳＲＭを有する端末と前記ＳＲＭの少なくとも１つに特定ＤＲＭコンテンツが保存されているとき、前記特定ＤＲＭコンテンツの使用権利は、前記端末を介して前記ＳＲＭに発行され、前記ＳＲＭにインストールされる。
【０１０７】
前記ＤＲＭコンテンツ及び前記ＳＲＭ名義の使用権利は、複合伝送方式又は独立伝送方式で使用権利発行者から発行される。
【０１０８】
最後に、前記ＳＲＭは、前記ＤＲＭコンテンツ及び／又は前記ＳＲＭ名義の使用権利を保存できる。
【０１０９】
本発明の精神や基本的な特性から外れない限り多様な形態で本発明を実現することができ、前述した実施形態は前述した詳細な記載内容によって限定されるのではなく、添付された請求の範囲に定義された本発明の精神や範囲内で広く解釈されるべきであり、本発明の請求の範囲内で行われるあらゆる変更及び変形、並びに請求の範囲の均等物は本発明の請求の範囲に含まれる。
【図面の簡単な説明】
【０１１０】
発明の理解を容易にするために添付され、本明細書の一部を構成する図面は、発明の多様な実施形態を示し、明細書と共に発明の原理を説明するためのものである。
【図１】一般的なＤＲＭシステムを示す図である。
【図２】本発明によるＳＲＭのデジタル著作権管理システムを示す図である。
【図３】本発明によるＳＲＭのデジタル著作権管理方法を示す図である。
【図４】本発明によるＳＲＭのデジタル著作権管理方法を示す図である。
【図５】図３及び図４に示すＳＲＭのデジタル著作権管理方法を示す図である。

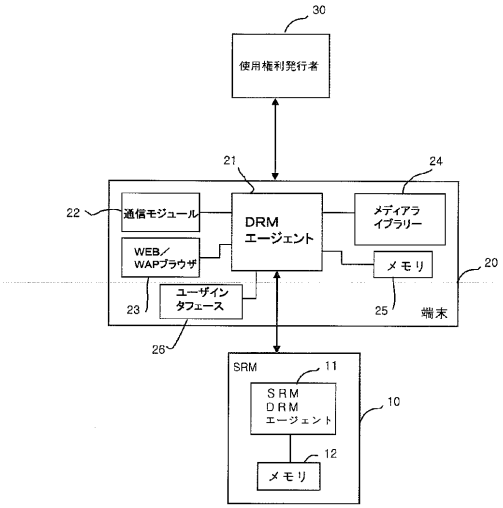
【図１】

【図１】



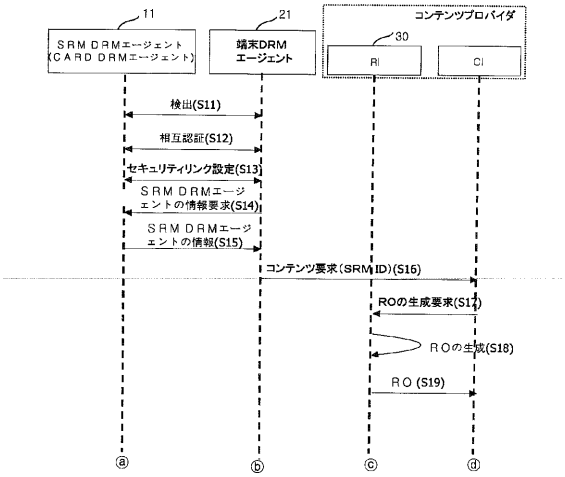
【図２】

【図2】



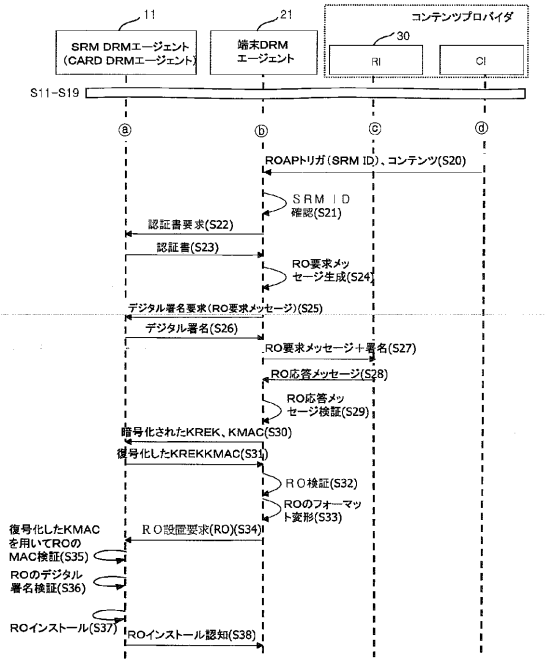
【図３】

【図3】



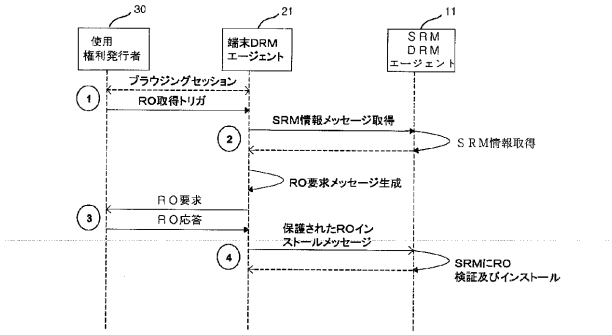
【図４】

【図4】



【図５】

【図5】


30
21
11
使用
権利発行者
端末DRM
エージェント
SRM
DRM
エージェント
ブラウジングセッション
1
RO取得トリガ
SRM情報メッセージ取得
2
ＳＲＭ情報取得
RO要求メッセージ生成
ＲＯ要求
3
ＲＯ応答
保護されたROイン
ストールメッセージ
4
SRMにRO
検証及びインストール

フロントページの続き

(51)Int.Cl.	FI	
	G06K 19/00	P
	G06K 19/00	N
	H04L 9/00	675B

(72)発明者 キム, テーヒュン
大韓民国 437－771 キョンギード, ウイワン, ポイルードン, 518, ドンーア エコービル アパートメント 102－1002
(72)発明者 リ, スン イエ
大韓民国 151－022 ソウル, クワナクーク, シリム 12－ドン, 1734, センタービル 104－703

審査官 戸島 弘詩

(56)参考文献 特開2005－129058（JP, A）
特表2002－517869（JP, A）
特開2004－326210（JP, A）
米国特許出願公開第2005／0216739（US, A1）
米国特許出願公開第2005／0209972（US, A1）
特開2005－86547（JP, A）
OMA DRM Specification V2.0, Open Mobile Alliance, 2004年 4月20日, Draft Version 2.0, p.20,22-23,40-45, [平成22年11月16日検索], URL, http://xml.coverpages.org/OMADRMv204-20040420.pdf

(58)調査した分野(Int.Cl., DB名)
G06F21/00-21/24
G09C1/00-5/00
H04K1/00
H04L9/00
G06K17/00,19/00