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

特許第4414321号
(P4414321)

(45)発行日　平成22年2月10日(2010.2.10)　(24)登録日　平成21年11月27日(2009.11.27)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520D
G06F 21/00	(2006.01)	G06F	12/14	550A
G06Q 50/00	(2006.01)	G06F	15/00	330Z
G09C 1/00	(2006.01)	G06F	17/60	142
		G09C	1/00	640E

請求項の数 26　(全 16 頁)

(21)出願番号	特願2004-307452 (P2004-307452)
(22)出願日	平成16年10月21日 (2004.10.21)
(65)公開番号	特開2005-129058 (P2005-129058A)
(43)公開日	平成17年5月19日 (2005.5.19)
審査請求日	平成16年10月21日 (2004.10.21)
(31)優先権主張番号	60/512,927
(32)優先日	平成15年10月22日 (2003.10.22)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	2003-074000
(32)優先日	平成15年10月22日 (2003.10.22)
(33)優先権主張国	韓国 (KR)
(31)優先権主張番号	2004-055647
(32)優先日	平成16年7月16日 (2004.7.16)
(33)優先権主張国	韓国 (KR)

前置審査

(73)特許権者　390019839
三星電子株式会社
ＳＡＭＳＵＮＧ　ＥＬＥＣＴＲＯＮＩＣＳ　ＣＯ．，ＬＴＤ．
大韓民国京畿道水原市靈通区梅灘洞４１６
４１６，Ｍａｅｔａｎ－ｄｏｎｇ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ　４４２－７４２
（ＫＲ）
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆

最終頁に続く

(54)【発明の名称】携帯用保存装置を用いたデジタル著作権の管理方法及び装置

(57)【特許請求の範囲】

【請求項１】

デバイスがライセンス提供者と第１認証を行って第１結合する段階と、

携帯用保存装置と第２認証を行って第２結合する段階と、

前記ライセンス提供者からライセンスを受信する段階と、

前記ライセンスを前記携帯用保存装置に送信する段階と、を含み、

前記携帯用保存装置は、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達する携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項２】

前記ライセンス受信段階は、

前記ライセンスを前記第１認証を通じて生成された暗号キーで復号化する段階をさらに含む請求項１に記載の携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項３】

前記第２結合段階は、

ランダム数を選択して前記数をパラメータとして前記携帯用保存装置に認証を要請する段階と、

前記携帯用保存装置から前記認証要請に対する応答を受信する段階と、

前記応答に含まれた情報で構成された暗号キーを獲得する段階と、をさらに含む請求項１に記載の携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項４】
前記応答に含まれた情報は前記選択したランダム数と、前記携帯用保存装置からランダムに生成した数を含む請求項３に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項５】
前記ライセンスを送信する段階以前に、
前記第２認証を通じて生成された暗号キーで前記ライセンスを暗号化する段階をさらに含む請求項１に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項６】
携帯用保存装置がデバイスと認証を行って結合する段階と、
前記デバイスがライセンス提供者から伝達されたライセンスを前記携帯用保存装置が前記デバイスから受信する段階と、を含み、
前記携帯用保存装置は、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達する携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項７】
前記ライセンスを受信する段階以後に、前記ライセンスを前記認証を行った結果として生成された暗号キーで復号化する段階をさらに含む請求項６に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項８】
前記認証は、ランダムに選択した数をパラメータとして前記デバイスに前記数を送信する段階と、
前記デバイスから前記パラメータの送信に対する応答に含まれた情報より構成された暗号キーを獲得する段階と、を含む請求項６に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項９】
前記応答に含まれた情報は前記ランダム数と、前記デバイスで生成した数を含む請求項８に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項１０】
デバイスがドメインを管理するサーバーに前記デバイスの識別情報を登録する段階と、
前記ドメインに登録された携帯用保存装置に保存されたライセンスを用いてコンテンツを用いる段階と、を含み、
前記携帯用保存装置は、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達する携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項１１】
前記デバイスは前記デバイスの識別情報を登録する段階以後に、登録された携帯用保存装置にライセンスを送信する段階を含む請求項１０に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項１２】
前記ドメインを管理するサーバーは前記ドメインにライセンスを提供するライセンス提供者である請求項１０に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項１３】
前記携帯用保存装置は前記ドメインに登録されたデバイスを通じて前記ドメインに登録した請求項１０に記載の携帯用保存装置を用いたデジタル著作権の管理方法。
【請求項１４】
携帯用保存装置がドメインを管理するサーバーに前記携帯用保存装置の識別情報を登録する段階と、
前記ドメインに登録された第１デバイスに前記携帯用保存装置に保存されたライセンスの利用を提供する段階と、を含み、

前記携帯用保存装置は、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達する携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項１５】

前記利用を提供する段階以前に、

前記ドメインに登録された第２デバイスからライセンスを受信する段階を含む請求項１４に記載の携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項１６】

携帯用保存装置が第１デバイスからライセンスを受信する段階と、

前記第１デバイスの情報と前記ライセンスの情報とを保存する段階と、

前記情報を検索する段階と、を含み、

前記携帯用保存装置は、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達する携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項１７】

前記保存された情報を用いて、前記第１デバイスまたは前記保存された情報で指す第２デバイスに前記ライセンスを移動させる段階をさらに含む請求項１６に記載の携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項１８】

前記受信したライセンスを第２デバイスに送信する段階を含み、

前記第２デバイスは前記ドメインに登録されたデバイスである請求項１６に記載の携帯用保存装置を用いたデジタル著作権の管理方法。

【請求項１９】

携帯用保存装置とライセンスを送受信する送受信部と、

前記携帯用保存装置と認証を行う認証部と、

前記携帯用保存装置のライセンスを受信して保存する保存部と、を含み、

前記認証部は暗号化と復号化とを行い、

前記携帯用保存装置は、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達する携帯用保存装置を用いたデジタル著作権の管理装置。

【請求項２０】

前記暗号化及び復号化は前記認証部で携帯用保存装置と認証を行って生成された暗号キーを使用し、

前記暗号化及び復号化は 共通鍵方式(対称鍵)を使用する請求項１９に記載の携帯用保存装置を用いたデジタル著作権の管理装置。

【請求項２１】

前記送受信部はライセンス提供者からライセンスを受信し、

前記保存部は前記受信したライセンスを保存する請求項１９に記載の携帯用保存装置を用いたデジタル著作権の管理装置。

【請求項２２】

デバイスとライセンスを送受信する送受信部と、

前記デバイスと認証を行う認証部と、

前記デバイスから受信したライセンスを保存する保存部と、を含み、

前記認証部は暗号化と復号化とを行い、

前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達するデジタル著作権を管理する携帯用保存装置。

【請求項２３】

前記暗号化及び復号化は前記認証部でデバイスと認証を行って生成された暗号キーを使用し、

前記暗号化及び復号化は 共通鍵方式(対称鍵)を使用する請求項２２に記載のデジタル著作権を管理する携帯用保存装置。

【請求項２４】

メモリカードはモバイルデバイスとの認証を行える認証書及び暗号キーを予め有しており、前記モバイルデバイスとの認証を行えるプロトコルモジュールを有することを前提とし、

メモリカードがモバイルデバイスとの認証過程を行う段階と、前記認証過程を行った後に前記モバイルデバイスがライセンスプロバイより獲得したライセンスを受け取る段階とを含み、

前記メモリカードは、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達することを特徴とするモバイルＤＲＭサービスにおける保安方法。

【請求項２５】

メモリカードはモバイルＤＲＭサービスでＬＰと行えるライセンス獲得プロトコルモジュールを予め内部に有し、前記モバイルＤＲＭサービスでＬＰと認証プロトコルを行う時に使われる認証書及びそれによる暗号キーを内部に有することを前提とし、

メモリカードがモバイルＤＲＭサービスで定めた認証方式によってモバイルデバイスを通じてライセンスプロバイダと認証プロトコルを行う段階と、前記認証が成功すれば、ライセンスプロバイダよりライセンスを獲得する段階とを含み、

前記メモリカードは、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達することを特徴とするモバイルＤＲＭサービスにおけるライセンス獲得方法。

【請求項２６】

メモリカードがドメインを管理するＤＲＭサーバーに登録する段階と、

前記メモリカードがドメインに属する他のデバイスからライセンスを伝達される段階と、

前記ドメインに属する他のデバイスがメモリカードを用いて再生をしたり、ライセンスを受け取る段階と、を含み、

前記メモリカードは、前記ライセンスと該ライセンスを伝達したデバイスとの情報を書いたテーブルを内部に保存し、前記テーブルを使用して前記デバイスにライセンスを再び伝達することを特徴とするドメインでのコンテンツ共有時の保安性あるメモリカードの使用方法。

【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に係り、特にモバイルＤＲＭサービスを保安性ある保安マルチメディアカードとの作動に適用する方法に関する。

【背景技術】

【０００２】

最近、デジタル著作権管理（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ；以下、“ＤＲＭ”と称する）に関する研究が活発に進行しつつあり、ＤＲＭを適用した商用サービスが導入されたか、導入中にある。ＤＲＭが導入されねばならない理由はデジタルコンテンツが有する多様な特性から導出されうる。デジタルコンテンツはアナログデータとは違って損失がなく、複製可能であるという特性と、再使用及び加工、配布が容易な一方、その製作に多くのコストと努力及び時間を必要とするという特性を有する。したがって、デジタルコンテンツの無断複製及び配布が容認される場合に、これはデジタルコンテンツ製作者の利益を侵害し、デジタルコンテンツ製作者の創作意欲を殺がれ、これはデジタルコンテンツ産業の活性化に大きな阻害要素となる。

【０００３】

デジタルコンテンツを保護しようとする努力は過去にもあったが、過去には主にデジタ

ルコンテンツ無断接近防止に重点をおいてデジタルコンテンツに対するアクセス（ａｃｃｅｓｓ）は料金を支払った一部の人にだけ許容された。しかし、代価を支払った人が故意的にデジタルコンテンツを第３者に配布する場合に、第３者は代価を支払わなくてもデジタルコンテンツを使用できるようになる。このような問題点を解決するためにＤＲＭという概念が導入された。ＤＲＭは何れか暗号化されたデジタルコンテンツに対する接近が誰にも無制限に許容されるが、暗号化されたデジタルコンテンツを復号化して実行させようとするならば、権利客体というライセンスがなければならない。したがって、ＤＲＭを適用すればデジタルコンテンツを既存とは違って効率よく保護できるようになる。

【０００４】

携帯型保存装置は携帯電話、コンピュータ、デジタルカメラなど複数のデジタル機器の資料を保存し、移動可能にする着脱自在の装置であって、データを保存する保存空間と演算及び制御を担当する部分で構成される。このような携帯型保存装置の１つであるマルチメディアカードと呼ばれるＭＭＣ（Ｍｕｌｔｉ Ｍｅｄｉａ Ｃａｒｄ）は従来のハードディスクやコンパクトディスクが有する限界を超え、多様な種類のデジタル機器で使用できるようにマルチメディアデータを保存する役割をしている。また、このカードは既存の保存媒体にはない演算部を有しており、単純なデータ保存でない、制御などが可能になって大容量の、多様なマルチメディアデータの収容に適している。最近、このマルチメディアカードに保安性の機能を追加してデジタルコンテンツの保存及び送受信における保安と著作権の保護とが可能な保安用マルチメディアカード（Ｓｅｃｕｒｅ ＭＭＣ）が開発されつつ、デジタルコンテンツに関する著作権管理が保存装置とデジタル機器とで可能になった。以下、デジタルカメラ、携帯電話、コンピュータ、デジタルカムコーダなどのデジタル機器をデバイスと通称する。

【０００５】

図１は、従来の技術によるＳＤ Ｃａｒｄとデバイス間のライセンス転送を示す概念図である。代表的な保安性メモリカードであるＳＤ Ｃａｒｄ２１０の場合、モバイルＤＲＭサービスを基盤しておらず、ＣＰＲＭ互換デバイスとＳＤ Ｃａｒｄ間での動作だけ定義している。したがって、ライセンス獲得過程（Ｌｉｃｅｎｓｅ Ａｃｑｕｉｓｉｔｉｏｎ）はモデルに含まれていない。ＳＤ Ｃａｒｄ２１０の動作は、図１のようにデバイス１００とメモリカード間でのみ定義されており、ライセンス提供者との連関性は定義されていない。メモリカードはデバイスとの認証を通じて保安結合を結んでおり、デバイスはメモリカードを利用できる。

【０００６】

図２は、従来のＣＰ Ｓｅｃｕｒｅ ＭＭＣがライセンス提供者からライセンスを獲得するための連結関係を示す概念図である。保安性メモリカードであるコンテンツ保護保安マルチメディアカード（“Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｓｅｃｕｒｅ ＭＭＣ”）の場合、メモリカードに基いたＤＲＭ方式を記述している。したがって、モバイルデバイスを基盤としているモバイルＤＲＭサービスに適用し難い。図２で保安メモリカード２５０はライセンス提供者５００から直接ライセンスを獲得する。但し、保安メモリカード２５０がライセンス提供者５００と通信するための装置を備えていないために、ターミナル３００を通じてライセンス提供者５００からライセンスを獲得する。したがって、ターミナルは一種の通信プロキシだけを行い、ライセンス提供者５００とターミナル３００間、あるいはターミナル３００と保安メモリカード２５０間には何なる保安結合も存在しない。

【０００７】

このモデルは、単にメモリカード２５０が直接ライセンス提供者５００に連結されてライセンスを獲得してメモリカード２５０にライセンスが保存されうる。ＣＰ Ｓｅｃｕｒｅ ＭＭＣの動作はメモリカードだけがライセンス提供者との連関性を有しうる。メモリカード２５０はターミナル３００を通じてライセンス提供者５００と連結し、メモリカードはライセンス提供者からライセンスを受けて保存する。

【０００８】

このようなＳＤ　Ｃａｒｄ及びＣＰ　Ｓｅｃｕｒｅ　ＭＭＣのような既存のメモリカードの問題点はモバイルＤＲＭサービスとの連動を考慮していないために、今後のサービス予定のＯＭＡ　ＤＲＭのようなモバイルＤＲＭサービスとの作動が不可能である。したがって、モバイルＤＲＭと連動できる保安性メモリカードとの作動モデル及び方法が必要である。

【０００９】

これと関連して、モバイルＤＲＭ環境で保安性メモリカードの作動モデル及び方法、モバイルＤＲＭサービスでメモリカードがライセンス提供者と直接的に連動可能な方法及びモバイルＤＲＭサービスでメモリカードがドメインの１デバイスとして連動できる方法を講ずる必要がある。

【００１０】

特許文献１は、情報端末装置を開示している。携帯電話機のユーザは、新たにアーティストの曲を購入したいとき、そのアーティストの検索結果を配信サーバから受信する。携帯電話機は配信サーバから受信した検索結果に含まれる暗号化コンテンツデータがどのメモリカードに格納されているかをデータベースに基づいて検索する。そして、携帯電話機は、暗号化コンテンツデータがメモリカードに格納されているとき携帯電話機から暗号化コンテンツデータをコピーし、ライセンスを配信サーバから受信する。

【特許文献１】特開２００２－２８８４５３号

【発明の開示】

【発明が解決しようとする課題】

【００１１】

本発明が解決しようとする技術的課題は、携帯用保存装置を用いてデジタル著作権を管理することにある。

本発明が解決しようとする他の技術的課題は、携帯用保存装置に保存されたライセンスを通じてコンテンツを用いることにある。

【課題を解決するための手段】

【００１２】

本発明は、携帯用保存装置を用いたデジタル著作権の管理装置及び方法に関する。

本発明の一実施例に係る携帯用保存装置を用いたデジタル著作権の管理方法は、デバイスがライセンス提供者と第１認証を行って第１結合する段階、携帯用保存装置と第２認証を行って第２結合する段階、前記ライセンス提供者からライセンスを受信する段階及び前記ライセンスを前記携帯用保存装置に送信する段階を含む。

【００１３】

本発明に使われる主要用語を説明すれば次の通りである。

－ユーザとコンテンツ提供者、ライセンス提供者

ユーザはＤＲＭ機能があるデバイスを所有する者を意味し、コンテンツ提供者はコンテンツを分配する機関を意味する。そして、ライセンス提供者（ＬＰ）はコンテンツに該当するライセンスを販売して伝達する機関を意味する。

【００１４】

－ライセンス

コンテンツを再生できる権利を明細している客体（権利客体、ｒｉｇｈｔ　ｏｂｊｅｃｔ）を意味する。

－携帯型保存装置

携帯型保存装置は、携帯電話、コンピュータ、デジタルカメラなど多様なデジタル機器の資料を保存し、移動可能にする着脱自在の装置であって、データを保存する保存空間と演算及び制御を担当する部分とで構成されたものである。このような携帯型保存装置の１つであるマルチメディアカードと呼ばれるＭＭＣ（Ｍｕｌｔｉ　Ｍｅｄｉａ　Ｃａｒｄ）は従来のハードディスクやコンパクトディスクが有する限界を超え、多様な種類のデジタル機器で使用できるようにマルチメディアデータを保存する役割をしている。また、このカードは既存の保存媒体にはない演算部を有しており、単純なデータ保存でない、制御な

どが可能になって大容量の、多様なマルチメディアデータの収容に適している。最近、このマルチメディアカードに保安性の機能を追加してデジタルコンテンツの保存及び送受信における保安と著作権保護が可能な保安マルチメディアカード（Ｓｅｃｕｒｅ　ＭＭＣ）が開発されることによって、デジタルコンテンツに対する著作権管理が保存装置とデジタル機器とで可能になった。本明細書では、保安マルチメディアカードを中心に説明するが、これは保安マルチメディアカードに限定されるものではなく、携帯型保存装置に関するものである。

【００１５】

－モバイルデバイス

携帯電話、コンピュータ、デジタルカメラなど多様なデジタル機器を言う。最近、デバイスの移動性に対する要求が高まりつつ携帯性と移動性とを有するデジタル機器に対する開発が活発に進行しつつある。以下、デジタルカメラ、携帯電話、コンピュータ、デジタルカムコーダなどのデジタル機器をモバイルデバイスと通称する。

一方、携帯型保存装置は必ずしもモバイルデバイスでだけ使用できるものではない。マルチメディアコンテンツを再生、移動及びコピー、プリントなどを行えるコンピュータ機能を有するデバイスでは何れも使用可能な保存装置である。よって、本明細書で用いているデバイスあるいはモバイルデバイスは保安マルチメディアカードのような携帯型保存装置のコンテンツを使用し、携帯型保存装置を通じてコンテンツを移動またはコピーしうる。

【００１６】

－暗号化と復号化

携帯型保存装置とデバイス間に送受信されるライセンス及び情報は暗号化して送受信されねばならない。これは中間に不法で何れのデータを流出させるか、データを操作する可能性を防止するために必要である。本発明の一実施例では暗号キーを使用して暗号化と復号化とを行う。Ｋというキーによりデータを暗号化して送受信し、このキーを有しているデバイスと携帯型保存装置は各々受信されたデータを復号化してそれぞれの保存部にライセンスあるいはデータを保存し、データが要請する機能を行う。

【００１７】

－対称キーアルゴリズム(共通鍵方式)

秘密鍵、対称鍵（Symmetric Key）とも言う。対称キーアルゴリズムは１つのキーで暗号化と復号化とがなされることを意味する。前記１つのキーは暗号化と復号化とを行う両側であらかじめ約束されたり、定義されねばならない。

【００１８】

本実施例で使われる“部”、“モジュール”という用語はソフトウェアまたはＦＰＧＡまたはＡＳＩＣのようなハードウェア構成要素を意味し、モジュールは所定の役割を行う。しかし、モジュールはソフトウェアまたはハードウェアに限定されるものではない。モジュールはアドレッシングできる保存媒体に位置すべく構成されても良く、１つまたはそれ以上のプロセッサーを再生させるように構成されても良い。したがって、一例としてモジュールはソフトウェア構成要素、客体向けソフトウェア構成要素、クラス構成要素及びタスク構成要素のような構成要素と、プロセス、関数、属性、プロシージャー、サブルーチン、プログラムコードのセグメント、ドライバー、ファームウェア、マイクロコード、回路、データ、データベース、データ構造、テーブル、アレイ及び変数を含む。構成要素とモジュール内で提供される機能はより少数の構成要素及びモジュールに結合されるか、追加的な構成要素とモジュールにさらに分離されうる。のみならず、構成要素及びモジュールはデバイスまたは保安マルチメディアカード内の１つまたはそれ以上のＣＰＵを再生させるように具現されることもある。

【発明の効果】

【００１９】

本発明を具現することによって、携帯用保存装置を使用してデジタル著作権を管理しうる。

本発明を具現することによって、１つのドメインに存在する多様なデバイスが携帯用保存装置を通じてコンテンツを利用できる。

【発明を実施するための最良の形態】

【００２０】

以下、添付した図面に基づいて本発明の望ましい一実施例を詳細に説明する。

図３は、本発明の一実施例に係るモバイルデバイスがライセンス提供者からライセンスを獲得して保安マルチメディアカードに送信する構成を示す概念図である。認証段階でデバイス１００と保安マルチメディアカード２００とは互いに身元を把握する。図３で保安結合（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ；ＳＡ）は２つが存在する。ＳＡ１は、ライセンス提供者５００とモバイルデバイス１００間に存在し、ＳＡ２はモバイルデバイス１００と保安マルチメディアカード２００間に存在する。これは既存の”コンテンツ保護保安マルチメディアカード”が保安マルチメディアカード２００とライセンスサービス間に保安結合が１つだけ存在する場合と差がある。このように、図３は、モバイルＤＲＭ環境で保安マルチメディアカード２００がライセンスを得られるモデルを提示したことである。モバイルＤＲＭサービスを通じて伝達されたライセンスは保安マルチメディアカード２００に移され、デバイス１００は保安マルチメディアカード２００を用いて再生、移動、コピーなどの機能を活用しうる。

【００２１】

保安結合ＳＡ１は、ライセンス提供者から（モバイル）デバイス１００がライセンスを取得する過程である。この過程を経るためにはデバイス１００を通じて所定の認証と課金などを必要とする。そして、ライセンスは有無線通信を通じて可能である。これは最近活発に研究及び商用化が進んでいる無線通信の場合にも適用可能であることを意味する。ライセンス取得モジュールは前記認証または課金機能を含むモジュールになりうる。

【００２２】

トラスト管理モジュールは前記ＳＡ１過程を通じて習得したライセンスを他のデバイスあるいは携帯用保存装置に移動させるために必要な前処理作業を行う。通常、ライセンスはファイルの形に存在するので、携帯用保存装置のファイル構造に適した形に切替えられる。

【００２３】

ライセンスは前述したようにコンテンツに対するユーザの権限情報を有する客体である。ＤＲＭではコンテンツとライセンスとが独自に流通可能である。したがって、コンテンツは暗号化されて他の経路を通じて流通でき、このコンテンツに関する権利客体であるライセンスはコンテンツと異なる経路を通じて移動されうる。したがって、ライセンスの移動またはコピーは権限を有するユーザによってのみ流通または使用されるべきである。このために、ライセンスの移動またはコピー時、相互認証と認証書の保持有無などを検討する過程が必要である。また、無制限の移動及びコピーを防止するために、ライセンスの移動とコピー時にライセンスを修正可能にする。

【００２４】

したがって、トラスト転換時には上記の移動、コピー時にライセンスの情報を修正する作業を前提としうる。その他、再生の権限に制限をおいた場合、再生時にライセンスの情報を修正する作業を必要としうる。ライセンスを用いるための所定の処理段階を含むことがトラスト転換である。

【００２５】

さらに他の保安結合としては保安マルチメディアカード２００とデバイス１００間の保安結合であるＳＡ２が存在する。この過程は保安マルチメディアカード２００との情報交換時に発生可能なデータの流失または操作を防止し、保安マルチメディアカード２００が認証を受けた携帯用保存装置であるか否かを検証する過程を含む。保安マルチメディアカードとの認証過程は図４で詳述する。

【００２６】

図３の構成によってＤＲＭサービスを実行するためには、保安マルチメディアカードは

モバイルデバイスとの認証を予め行える認証書及び暗号キーを有さねばならない。この過程はＳＡ２で行われる。保安マルチメディアカードはモバイルデバイスとの認証を予め行えるプロトコルモジュールを有さねばならない。このような前提条件下で、本実施例の動作を説明すれば、保安マルチメディアカード２００はモバイルデバイス１００との認証過程を行う。保安マルチメディアカード２００はモバイルデバイス１００との認証後にモバイルデバイス１００がライセンス提供者５００から獲得したライセンスを受け取れる。モバイルデバイス１００と携帯用保存装置２００間の認証過程を説明すれば次のようである。

【００２７】

認証はデバイス１００と保安マルチメディアカード２００との結合時になされ、結合が解除されるか、または既存の認証が取消された場合に新たに認証を必要とする。認証の結果で生成されたキーをデバイスと保安マルチメディアカードとが共有し、この共有されたキーを持ってアプリケーションを行う。認証過程は相互認証でなされるが、デバイス側で保安マルチメディアカードの適否を検討し、適していない場合には結合を解除する。そして、保安マルチメディアカードでもデバイスが適した認証を通過したデバイスでなければデータの要請を拒否する。

【００２８】

図４は、本発明の一実施例に係るデバイスがライセンス提供者のライセンスを受信して携帯用保存装置に送信する過程を示す順序図である。デバイスはライセンス提供者と携帯用保存装置とを結合し、ライセンスを携帯用保存装置に送信する。まずライセンス提供者と認証段階を経て結合する（Ｓ４０２）。前記認証は、ライセンス提供者とデバイス間の保安結合を通じてデータを安全に送受信することためである。この結合が成功すれば（Ｓ４０４で「Ｙｅｓ」）、引き続き携帯用保存装置と認証を行った後に結合する（Ｓ４０６）。これもまた携帯用保存装置とデータを流失または変調なしに送受信するために認証過程時に暗号キーを相互交換しうる。認証過程を経て結合が成功すれば（Ｓ４０８で「Ｙｅｓ」）、デバイスはライセンス提供者からライセンスを受信する（Ｓ４１０）。デバイスは前記受信したライセンスを、トラスト転換過程を経て携帯用保存装置が収容可能な形に転換する（Ｓ４１２）。このように転換されたライセンスは携帯用保存装置に送信し（Ｓ４１４）、携帯用保存装置に保存されたライセンスは前記デバイスのコンテンツ利用時に使用でき、また認証過程を経た他のデバイスもコンテンツ利用時に前記ライセンスを利用できる。一方、図４のＳ４０２とＳ４０６との順序は逆転されうる。既に携帯用保存装置と認証及び結合が済んだデバイスがライセンス提供者と認証を行って結合しても良い。これはそれぞれの場合によって変わる。

【００２９】

図５は、本発明の一実施例に係るデバイスと保安マルチメディアカードとの認証過程を示す順序図である。認証はデバイスの要請によりなされ、認証過程で共通のキーを有する。この過程は次のようである。

デバイス１００でランダム数ＲＮ１を生成する（Ｓ１０２）。この数は乱数発生を通じて得られ、既定のランダム数リストから抽出しても良い。前記過程を通じて得られたランダム数は保安要請命令語ＳＥＴ＿ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ＿ＲＥＱＵＥＳＴのパラメータとして保安マルチメディアカード２００に送信する（Ｓ１０４）。これを受けた保安マルチメディアカード２００もランダム数ＲＮ２を生成し（Ｓ１０６）、ＲＮ１とＲＮ２とを結合したキーと認証書を転送する（Ｓ１０８）。デバイス１００はこのキーを受信して認証過程が完了したことを保安マルチメディアカード２００に送信し（Ｓ１１０）、以後前記ＲＮ１とＲＮ２とを結合したキーを暗号キーとしてアプリケーションを行う。

【００３０】

図６は、本発明の一実施例に係る保安マルチメディアカードがライセンス提供者からライセンスを獲得する過程を示す順序図である。

ライセンス提供者５００と保安マルチメディアカード２００とは通信を通じて保安結合ＳＡを形成しうる。保安マルチメディアカード２００は通信を行える機能がないためにデ

バイスまたはモバイルデバイスを一種のプロキシとして用いてモバイルデバイスが提供する通信線路を利用する。本実施例ではモバイルＤＲＭサービスに保安マルチメディアカード２００が連動されることを仮定しているために、保安マルチメディアカード２００とライセンス提供者５００間の認証プロトコルはモバイルＤＲＭで提供するプロトコルによる。例えば、ＯＭＡ　ＤＲＭサービスで作動する保安マルチメディアカード２００の場合はＯＭＡ　ＤＲＭで定義したライセンス獲得プロトコルをモバイルデバイス１００を通じてライセンス提供者５００と共に行える。したがって、ＣＰ　ＳｅｃｕｒｅＭＭＣとの主な違いはモバイルＤＲＭシステムで保安マルチメディアカード２００が、第１に、モバイルデバイスのようなライセンス獲得モジュールを有しており、第２に、モバイルＤＲＭサービスで定義されたライセンス獲得プロトコルを行ってライセンスを獲得できるということである。

【００３１】

図６の構成によってＤＲＭサービスを提供するためには、保安マルチメディアカード２００はモバイルＤＲＭサービスでライセンス提供者５００と行えるライセンス獲得プロトコルモジュールを予め内部に有する。そして、保安マルチメディアカード２００はモバイルＤＲＭサービスでライセンス提供者と認証プロトコルを行う時に使われる認証書及びそれによる暗号キーを内部に有さねばならない。これは図４の順序図に示された過程を通じてなされる。このような前提条件下で、本実施例の動作を見れば、保安マルチメディアカード２００はモバイルＤＲＭサービスで定めた認証方式によってモバイルデバイス１００を通じてライセンス提供者５００と認証プロトコルを行う。これにより、保安マルチメディアカード２００はライセンス提供者５００との認証が成功すれば、ライセンス提供者５００からライセンスを獲得する。

【００３２】

ライセンス獲得プロトコルは前記認証過程を通じて生成された暗号キーなどを有し、デバイス１００に保存されたライセンスを、暗号化などを通じて保安がなされた状態で送受信する。ライセンス獲得モジュールを保安マルチメディアカード２００が有している時、ライセンスは保安マルチメディアカード２００を通じてデバイス１００間に送受信が柔軟になされうる。ライセンスは権利客体であって、権利情報を有する１つのファイルで有り得るが、単純なファイルとは違ってライセンスの移動時にはライセンスの多様な情報を修正できる。

【００３３】

ライセンスはコンテンツと独自に移動可能である。したがって、携帯用保存装置に保存されたライセンスはデバイス１００に保存されたコンテンツを使用させる役割を行う。デバイス１００はライセンスを有していない状態で、保安マルチメディアカード２００と結合して保安マルチメディアカード２００内のライセンス情報を読んでコンテンツを再生するか、使用しうる。

【００３４】

一方、ライセンス提供者５００からライセンスを保存しているモバイルデバイス１００が一定時間後に保安マルチメディアカードにライセンスを移動させることもある。ライセンスはコンテンツと独立して移動するので、暗号化されたコンテンツだけが流通される状況で、このコンテンツを使用するライセンスを後で取得しうる。

【００３５】

図７は、本発明の一実施例に係るドメイン内のデバイスが保安マルチメディアカードを用いてコンテンツを共有する方式を示す概念図である。ＤＲＭでコンテンツを共有させる１つの方法としてドメインに属するデバイス１００同士でコンテンツを共有させうる。これは保安性ある保安マルチメディアカード２００がＤＲＭサービス内に存在するデバイス１００に対してのみコンテンツを共有するようにライセンスを提供する方式である。ドメインとは、デバイスの集合であるが、特定個人が所有したデバイスであるか、または特定家族が所有したデバイスであると見られる。ホームネットワーク(Home Network)よりなる家電機器または個人が所有するコンピュータと携帯電話などである場合、コンテンツとラ

イセンスの流れを防止することはコンテンツの使用に不便さを与えうる。該当コンテンツとライセンスの利用者が限定されるか、同一人で有り得るからである。したがって、ドメイン内に存在するデバイス間にはコンテンツとライセンスとを共有することが必要である。

【００３６】

これらドメインの管理は特定デバイスが行うか、またはドメイン管理者を独自に置いて、該当ドメイン内のライセンスを管理しうる。デバイス１００は保安マルチメディアカード２００にライセンスを移すことができ、保安マルチメディアカードからデバイスにライセンスが移されうる。本実施例に係る動作を説明すれば、保安マルチメディアカードもデバイスのようにドメインを管理するＤＲＭサーバーに登録される。この登録は保安マルチメディアカードが自身の識別情報をＤＲＭサーバーに転送することによってなされうる。これは通常のデバイスのうち１つがＤＲＭサーバーの役割を行う場合、デバイスとの結合を通じてＤＲＭサーバーに登録できるからである。一方、デバイスが、自身に結合された保安マルチメディアカードの識別情報をＤＲＭサーバーに転送することによってもなされうる。デバイスとは別途の装置、あるいはライセンス提供者がＤＲＭサーバーの役割を行う場合、保安マルチメディアカードがこれらと直接通信できない場合が発生するので、この時にはこれら保安マルチメディアカードが結合されたデバイスが前記保安マルチメディアカードの識別情報を前記ＤＲＭサーバーに転送することによって登録がなされる。

【００３７】

このような登録過程を経た後、保安マルチメディアカードが同じドメインに属する他のデバイスからライセンスを伝達され、ドメインに属する他のデバイスが保安マルチメディアカードを用いて再生するか、ライセンスを受け取る。

【００３８】

図８は、本発明の一実施例に係るデバイスがドメイン内の携帯用保存装置のライセンスを用いる過程を示す順序図である。

この順序図はデバイスの形成されたドメインに登録を試みる過程から示す。デバイスはドメインを管理するサーバーに識別情報を登録する（Ｓ５０２）。ドメインを管理するサーバーはＤＲＭサービスを用いるデバイスであって、ドメイン管理だけを専担するサーバーでありうる。またライセンス提供者がドメイン管理の機能を行うこともある。前記ドメインに登録されたデバイスは、以後前記ドメイン内の携帯用保存装置に保存されたライセンスを使用しうる。したがって、ライセンスを使用するための認証と結合過程がＳ５０４段階で行われる。認証時にはデバイスと携帯用保存装置がデータを安全に送受信するための暗号キーを生成できる。結合がなされれば、デバイスは携帯用保存装置と共にＤＲＭサービスを用いられる。まず、デバイスがコンテンツを利用しようとする場合（Ｓ５１０で「Ｙｅｓ」）、デバイスは前記コンテンツのライセンスを携帯用保存装置に要請する。この要請によりデバイスは前記コンテンツを利用できる（Ｓ５１２）。

【００３９】

一方、特定コンテンツの利用とは別にライセンスを送受信できる（Ｓ５２０）。ライセンスを送信してデバイスがライセンス提供者から受信したライセンスをドメイン内の他のデバイスが利用可能にする（Ｓ５２２）。さらに他のデバイスがライセンス提供者から受信したライセンスを利用するために携帯用保存装置のライセンスを受信しうる（Ｓ５３２）。

【００４０】

図９は、本発明の一実施例に係る保安マルチメディアカード内の情報保存テーブルを示す概念図である。デバイス１００と保安マルチメディアカード２００間にはライセンスが移動またはコピーされうる。保安マルチメディアカード２００内のライセンスは前記デバイスまたは他のデバイスに移動あるいはコピーされるか、コンテンツの再生に必要な情報を提供する。したがって、保安マルチメディアカード２００はライセンスとそのライセンスを伝達したデバイス１００との情報を書いたテーブルを内部に保存しておく。このテーブルの情報を通じて保安マルチメディアカード２００は自身が有しているライセンスがど

のデバイス１００から伝達されたのかが分かる。保安マルチメディアカード２００は自身にライセンスを伝達したデバイス１００を把握し、前記デバイス１００に再びライセンスを転送するか、ライセンスと関連した演算の再生、移動、コピーなどを行える。もちろん、前記デバイスではない他のデバイスに対してもライセンスを転送するか、再生、移動を行える。但し、前記テーブルを通じてライセンスを伝達したデバイスに関する情報を維持することによって、今後の認証過程でも暗号化過程を省略できる。

【００４１】

図１０は、本発明の一実施例に係るデバイスの構造を示すブロック図である。

携帯用保存装置と情報を交換する送受信部１２１が存在する。送受信部１２１は携帯用保存装置ではない他の装置との情報も交換しうる。デバイスは認証を行う認証部１２２が必要である。認証部では暗号化と復号化とを行い、共有する暗号キーを生成しうる。前記送受信部を通じて受信されたデータを復号化し、特定権利客体の携帯用保存装置への送信時に暗号化を行う。保存部１２３はライセンス提供者または携帯用保存装置から受信した権利客体を保存する。このように保存された権利客体はさらに他の携帯用保存装置に送信しうる。出力処理部１２４はデバイスが権利客体を用いて再生または出力などを行うコンテンツの出力を行う。スピーカー、モニターなどがこれに該当する。

前記送受信部と認証部 及び出力処理部のデータの流れと演算及び制御は制御部１２５で行う。また制御部は、図３で説明したトラスト転換過程を行う。

【００４２】

図１１は、本発明の一実施例に係る携帯用保存装置の構造を示すブロック図である。デバイスと情報を交換する送受信部２２１が存在する。送受信部はデバイスから命令語と権利客体とを受信し、保存された権利客体を送信する通路となる。またデバイスと認証を行う認証部２２２が存在する。認証部では暗号化と復号化とを行い、共有する暗号キーを生成しうる。認証部２２２では前記送受信部２２１を通じて受信されたデータを復号化し、特定権利客体の携帯用保存装置への送信時に暗号化を行う。

【００４３】

変換部２２３では前記送受信部２２１を通じて受信された権利客体を認証部２２２で復号化した後、携帯用保存装置が支援する形式のファイルフォーマットに変換する作業を行う。変換部２２３で行う変換作業時に再び権利客体を携帯用保存装置だけの暗号化技法で暗号化しうる。もちろん、この権利客体をデバイスに送信するためには、再び復号化する過程をさらに含みうる。

【００４４】

保存部２２４は前記変換部を通じて適するように変換された権利客体を保存する。制御部２２５は前記各部のデータ交換と制御及び演算を行う。またデバイスから受信した命令語を処理し、これによる作業を行うように各部に制御信号を発生させうる。

【００４５】

以上、添付した図面に基づいて本発明の実施例を説明したが、当業者ならば本発明がその技術的思想や必須な特徴を変更せずとも、他の具体的な形に実施可能であるという点を理解できるであろう。したがって、前述した実施例はあらゆる面で例示的なものに過ぎず、限定的でないものと理解せねばならない。本発明の範囲は前記発明の詳細な説明よりは特許請求の範囲によって示され、特許請求の範囲の意味及び範囲、そしてその均等概念から導出されるあらゆる変更または変形された形が本発明の範囲に含まれると解釈されねばならない。

【産業上の利用可能性】

【００４６】

本発明は、携帯用保存装置を用いてデジタル著作権を管理し、かつ携帯用保存装置に保存されたライセンスを通じてコンテンツを利用できる。

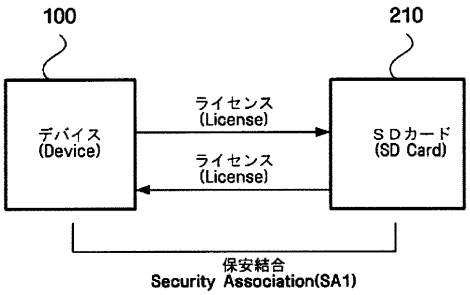
【図面の簡単な説明】

【００４７】

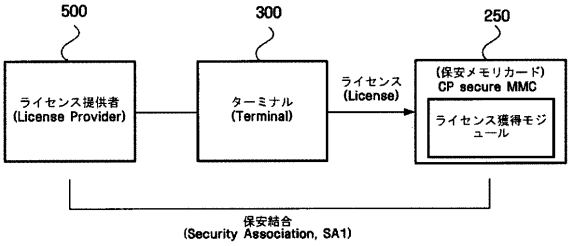
【図１】従来の技術によるＳＤ　Ｃａｒｄとデバイス間のライセンス転送を示す概念図で

ある。
【図２】従来のＣＰ　ＳｅｃｕｒｅＭＭＣがライセンス提供者からライセンスを獲得するための連結関係を示す概念図である。
【図３】本発明の一実施例に係るモバイルデバイスがライセンス提供者からライセンスを獲得して保安マルチメディアカードに送信する構成を示す概念図である。
【図４】本発明の一実施例に係るデバイスがライセンス提供者のライセンスを受信して携帯用保存装置に送信する過程を示す順序図である。
【図５】本発明の一実施例に係るデバイスと保安マルチメディアカードとの認証過程を示す順序図である。
【図６】本発明の一実施例に係る保安マルチメディアカードがライセンス提供者からライセンスを獲得する過程を示す順序図である。
【図７】本発明の一実施例に係るドメイン内のデバイスが保安マルチメディアカードを用いてコンテンツを共有する方式を示す概念図である。
【図８】本発明の一実施例に係るデバイスがドメイン内の携帯用保存装置のライセンスを用いる過程を示す順序図である。
【図９】本発明の一実施例に係る保安マルチメディアカード内の情報保存テーブルを示す概念図である。
【図１０】本発明の一実施例に係るデバイスの構造を示すブロック図である。
【図１１】本発明の一実施例に係る携帯用保存装置の構造を示すブロック図である。
【符号の説明】
【００４８】
１００　　デバイス
２００　　保安マルチメディアカード
５００　　ライセンス提供者（ＬＰ）
８００　　ドメイン

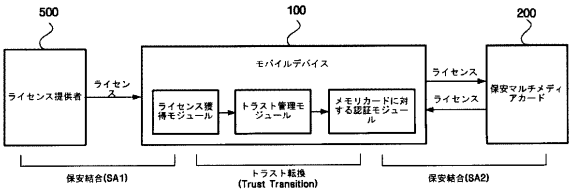
【図１】



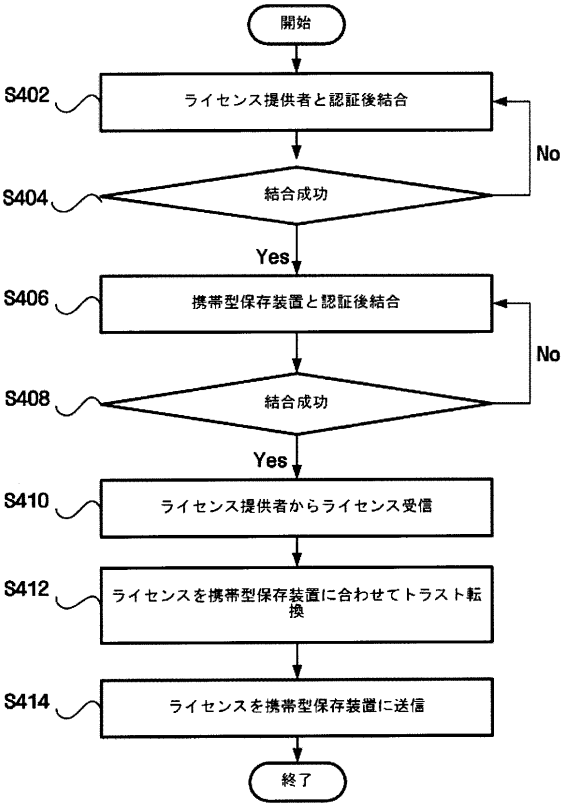
【図２】



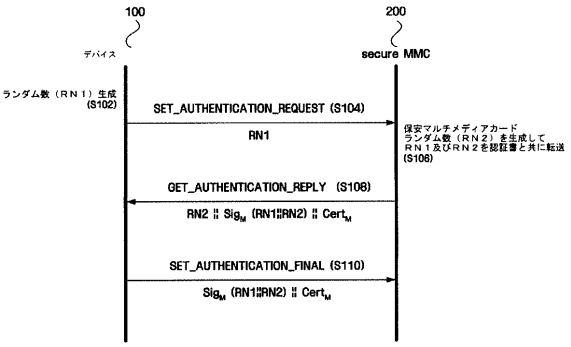
【図３】



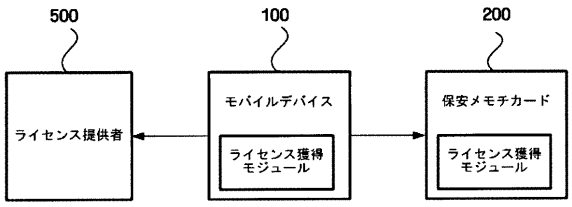
【図４】



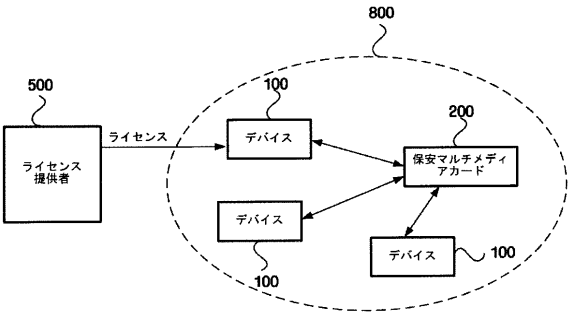
【図５】



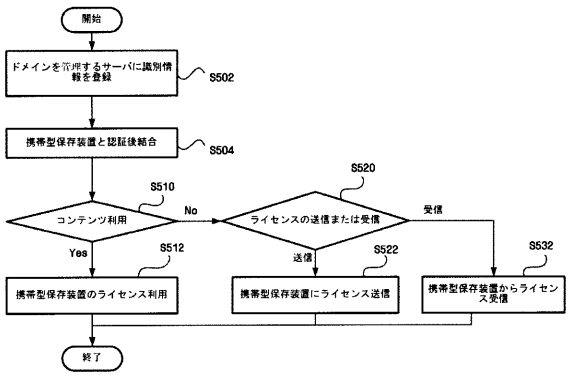
【図６】



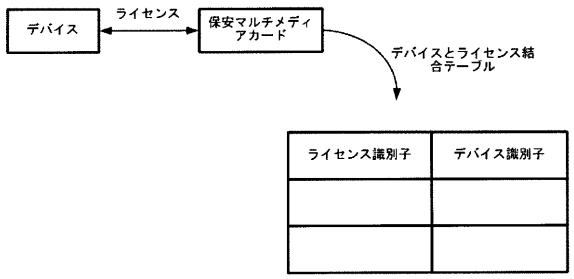
【図７】



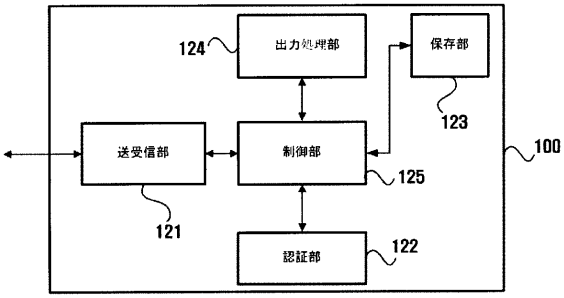
【図８】



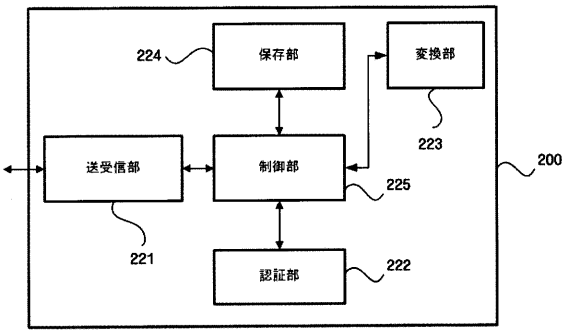
【図９】


デバイス
ライセンス
保安マルチメディアカード
デバイスとライセンス結合テーブル
ライセンス識別子
デバイス識別子

【図１０】


124
出力処理部
保存部
123
送受信部
制御部
125
100
121
認証部
122

【図１１】


224
保存部
変換部
223
送受信部
制御部
225
200
221
認証部
222

フロントページの続き

(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　李　炳來
大韓民国京畿道龍仁市水枝邑上▲ヒュン▼里（番地なし）　満▲ヒュン▼マウル盛源サンテヴィル３０６棟１０４號
(72)発明者　尹　重▲チュル▼
大韓民国ソウル特別市江北區水踰２洞３７２－９番地
(72)発明者　鄭　勍任
大韓民国京畿道城南市盆唐區亭子洞８８番地　住公３團地３１０棟２４０２號

審査官　平井　誠

(56)参考文献　特開２００２－３４２５１８（ＪＰ，Ａ）
特開２００１－２３７８１８（ＪＰ，Ａ）
特開２００２－３７３２１６（ＪＰ，Ａ）
国際公開第０１／０４１１０４（WO，Ａ１）
米国特許出願公開第２００３／００１８４９１（ＵＳ，Ａ１）
国際公開第０３／０２６２０７（WO，Ａ１）
特開２００１－３５８７０６（ＪＰ，Ａ）
特開平０９－１０７３５０（ＪＰ，Ａ）
特開２００１－２５６１１５（ＪＰ，Ａ）
特開２００１－００６２７９（ＪＰ，Ａ）
特開平１０－４０６３９（ＪＰ，Ａ）
特開２００３－２７１７６６（ＪＰ，Ａ）
特開平０４－４９４２３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　２１／００