(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-108639
(P2012-108639A)
(43)公開日　平成24年6月7日(2012.6.7)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	530C	5B017
H04N 7/167	(2011.01)	H04N	7/167	Z	5B276
H04L 9/08	(2006.01)	H04L	9/00	601B	5C164
G06F 21/22	(2006.01)	H04L	9/00	601E	5J104
H04L 9/32	(2006.01)	G06F	12/14	550B	

審査請求 未請求　請求項の数 10　ＯＬ　（全 27 頁）　最終頁に続く

(21)出願番号　特願2010-255719 (P2010-255719)
(22)出願日　平成22年11月16日 (2010.11.16)

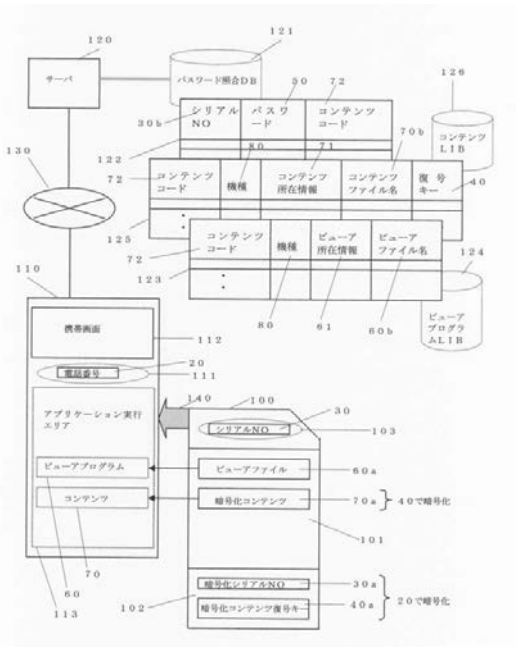
（特許庁注：以下のものは登録商標）
１．ＱＲコード

(71)出願人　507170103
牧田　恵美子
東京都千代田区１番町２０番地１３　ホーマットカヤ４０２号
(72)発明者　牧田　恵美子
東京都千代田区１番町２０番地１３ホーマットカヤ４０２号

Ｆターム(参考)　5B017 AA03 AA07 BA05 BA06 BB09 CA14 CA16
5B276 FB06
5C164 MA02S MA07S MB33P UA12P YA16
5J104 AA07 AA16 EA03 EA04 EA15 EA16 EA22 JA03 KA02 KA04 NA02 NA05 NA27 NA35 NA37 NA38 PA14

(54)【発明の名称】リムーバブル記憶メディアの閲覧・視聴システム

(57)【要約】　（修正有）
【課題】特定のコンテンツを予め購入する予約が設定されたメディアを購入すると視聴端末に合わせた視聴用プログラムとコンテンツをダウンロードでき、以後は、正当な装置以外の利用を制限し、コンテンツのコピーの防止ができるリムーバブル記憶メディアの閲覧・視聴システムを提供する。
【解決手段】正当なメディア１００に予めパスワードを付与し、本来付加されていたメディア１００固有の情報と組で登録し、この組の一致性を正当な所有者と確認する認証に使用し、認証されればコンテンツ格納を許可する。以後、指定の視聴端末１１０の固有情報で当該メディア１００の固有情報を暗号化し、使用時、復号操作により、先の視聴端末１１０の固有情報を復元できれば正当な組み合わせとして認証し、同様に復号した復号コードでコンテンツを復号し視聴を可能にする。従って、他メディアへのコピーや他端末との使用では視聴不可となる。
【選択図】図１



【特許請求の範囲】
【請求項１】
メディア固有情報及び暗号化されたコンテンツが格納されたリムーバブル記憶メディアと、
このリムーバブル記憶メディアを装着して、前記暗号化コンテンツをコンテンツ復号キーにより復号化して閲覧・視聴させる閲覧・視聴端末装置と、
正当メディアとしてリムーバブル記憶メディア毎に予めユニークに付けたパスワードと、このパスワードに紐付けたユニークな前記メディア固有情報と、前記リムーバブル記憶メディア毎に予め格納が予約された前記暗号化コンテンツについての識別情報であるコンテンツコードと、を相互に関連付けて登録した構造化情報ブロックと、
前記メディア固有情報と前記パスワードが入力されたときに、前記パスワードと前記メディア固有情報の対をキーとするレコードが前記構造化情報ブロック存在すれば、この入力パスワードに関連付けたリムーバブル記憶メディアを正当と認証するメディア認証手段と、
このメディア認証手段により正当性が認証されたリムーバブル記憶メディアの前記メディア固有情報を、このリムーバブル記憶メディアを装着した前記閲覧・視聴端末装置にユニークな装置固有情報をキーとして暗号化した暗号化メディア固有情報と、前記コンテンツコードに基づいて前記構造化情報ブロックから読み出したこの暗号化コンテンツの復号キーを、前記装置固有情報をキーとして暗号化した暗号化コンテンツ復号キーとを、このリムーバブル記憶メディアに格納する認証情報格納手段と、 このリムーバブル記憶メディアに格納指定された前記暗号化コンテンツをそのコンテンツコードに基づいて前記構造化情報ブロックから所在を参照し、このリムーバブル記憶メディアにダウンロードする暗号化コンテンツ格納手段と、
前記リムーバブル記憶メディアを前記閲覧・視聴端末装置に装着したときに、この暗号化メディア固有情報を、この装置固有情報で復号化したものが、このリムーバブル記憶メディアに格納された前記メディア固有情報と一致したときに、このリムーバブル記憶メディアとこの閲覧・視聴端末装置との組合せを正当と認証する組合せ認証手段と、
前記組合せの正当性が認証されたリムーバブル記憶メディアに格納した前記暗号化コンテンツ復号キーを、この閲覧・視聴端末装置の装置固有情報で復号化して得た前記コンテンツ復号キーにより、このリムーバブル記憶メディアに格納された暗号化コンテンツを復号化して閲覧・視聴させる閲覧・視聴手段と、
を具備していることを特徴とするリムーバブル記憶メディアの閲覧・視聴システム。
【請求項２】
前記閲覧・視聴手段は、前記メディア認証手段により正当性が認証されたリムーバブル記憶メディアに、前記コンテンツコードに基づいて前記構造化情報ブロックからこの閲覧・視聴端末装置の機種に適合した閲覧・視聴用のビューアプログラムが所在するライブラリをアクセスし、ダウンロードするビューアプログラム格納手段と、
このビューアプログラムを前記閲覧・視聴端末装置にロードし、このリムーバブル記憶メディアに格納した前記暗号化コンテンツを閲覧・視聴処理するビューアプログラム実行手段と、
を具備していることを特徴とする請求項１記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項３】
前記暗号化コンテンツ格納手段は、前記メディア認証手段により正当性が認証される限り、前記コンテンツコードで関連付けた暗号化コンテンツの更新のためのダウンロードを含むことを特徴とする請求項１または２に記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項４】
前記認証情報格納手段は、前記メディア固有情報と前記暗号化コンテンツ復号キーの暗号化処理の１過程として、被対象データへの加工処理を含むことを特徴とする請求項１～

３のいずれか１項記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項５】
前記メディア固有情報と前記暗号化コンテンツ復号キーは、前記リムーバブル記憶メディアのプロテクトエリアに格納され、前記プロテクトエリアは、データアクセス手段が秘匿されていることを特徴とする請求項１乃至４のいずれか１項に記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項６】
前記メディア固有情報は、前記リムーバブル記憶メディアの製造時に設定されたメディア固有の製造情報又はこのメディアを一意に識別する生成情報のいずれか一方であることを特徴とする請求項１乃至５のいずれか１項に記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項７】
前記閲覧・視聴端末装置は、携帯電話、携帯情報端末、タブレット端末、パーソナルコンピュータ、教育用情報機器、カーナビゲーション装置又は情報家電のいずれか一つであることを特徴とする請求項１乃至６のいずれか１項に記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項８】
前記装置固有情報は、前記閲覧・視聴端末装置の製造時に設定された機器固有の製造情報、電話番号、メールアドレス、装置を一意に識別できる装置付属物の情報又はこの装置を一意に識別する生成情報のいずれか一つであることを特徴とする請求項１乃至７のいずれか１項に記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項９】
前記パスワードの入力方法は、手入力、バーコード読みとり、２次元バーコード読みとりのいずれか一つであることを特徴とする請求項１乃至８のいずれか１項に記載のリムーバブル記憶メディアの閲覧・視聴システム。
【請求項１０】
前記構造化情報ブロックは、データベース、表計算ワークシート、インデックス付きライブラリ、インデックス付き検索ファイル又はディレクトリ型フォルダ・ファイルのいずれか一つであることを特徴とする請求項１乃至８のいずれか１項に記載のリムーバブル記憶メディアの閲覧・視聴システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、著作権保護を必要とする特定のコンテンツを予め決められたリムーバブル記憶メディアにネットワークを介してダウンロードさせる保証を行い、更に、特定のコンテンツ閲覧・視聴装置とを組み合わせることにより、両方のユニークな情報をそれぞれ認証、暗号化に使用することで、不法なコピーを無効にして、コンテンツを保護することができる技術に関する。
【背景技術】
【０００２】
メモリカードはリムーバブルメディアという利便性により、情報の一時記憶や保存に利用されてきた。近年、メモリカードの大容量化技術の進展に伴い、映画、音楽等の視聴情報、小説、画像情報や音声を含む教材情報等、大容量を必要とするコンテンツの永久保存用メディアとして注目されるようになり、これらのコンテンツの市販用メディアも出回るようになった。
【０００３】
メモリカードは不揮発性の記憶メディアであり、かつ書き換えが可能である。ネットワークを介してコンテンツをメモリカードにダウンロードして保存できる。メモリカードに格納したコンテンツを何度も閲覧・視聴したり、編集できる。このような特徴により、コンテンツの受け渡しを可能にするブリッジメディアとしての利便性が高く評価されている

。更に、大容量化が進み、適切なコストダウンが図れれば、今まで、ＤＶＤに格納して市販されていた映画等のコンテンツもメモリカードに格納して販売されるようになると推測される。

【０００４】

しかし、メモリカードの利便性は著作権のあるコンテンツの保護には却って障害となる。メモリカードの内容のコピーやデータ改ざんが簡単なため、コンテンツの保護にはコピーガードは最も必要な保護機能であり、コピーしても暗号化されているため利用できない等の技術的工夫が必要になる。その一例としては、ＣＰＲＭ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａの略、登録商標）がある。ＣＰＲＭは、著作権保護されたデジタル放送用映像コンテンツのコピー制御技術であるが、ＳＤメモリカードにも適用されている。ＣＰＲＭを採用すると、コンテンツは暗号化されるなどの利点を得られる。

【０００５】

ただし、メモリカード等のリムーバブルなメディアの厄介な点は、正当な認証を受けたコンテンツの授受であっても、一度メモリカードに格納された後は、当該メモリカードを熟知した専門家であるならば、比較的楽に、コピーガードを破り、コンテンツを利用可能な形態に不正コピーできることである。この問題に対して、特許文献１は、ネットワーク等からメモリカード等に受けたコンテンツについて、端末にユニークなシリアル番号や端末のみに秘匿して内蔵した認証コードで暗号化することにより、当該コンテンツの利用は当該メモリカードを装着した端末のみしか利用できない方式を提案している。

【０００６】

特許文献２は、次の認証方式により正当性を照合している。

１）予め暗号化されたコンテンツを格納したメモリカードそのものを現物販売することにより、課金処理を排除する。

２）製造番号のようなメモリカード固有なコードと当該メモリカードに付与したパスワード（商品番号でもよい）をデータベースに組で登録する。

３）利用の最初に、当該メモリカード固有なコードと入力されたパスワードの組を前記データベースで照合し、組が一致した場合に正当な購入者による利用と認証する。

４）認証された場合に、視聴用機器の機種に合わせたビューアプログラムを転送し、装着した前記正当なメモリカードに格納する。

５）また、当該メモリカードを装着した視聴機器のみを以後視聴可能な機器に認定し、当該機器に固有なコード（例えば携帯電話ならば電話番号）で前記メモリカードに固有なコードを暗号化して当該メモリカードに記録する。

６）２回目の利用以後は、前記暗号化されたメモリカードに固有なコードを前記機器に固有なコードで復号し、メモリカードに固有なコードを再現した場合に正当な組み合わせと認証する。

このようにして、視聴機器に合ったビューアプログラムのダウンロードと簡単・確実な認証により利用の便宜を図り、かつ、コピープロテクトを確実にしている。

【０００７】

本発明は、特許文献２の発明である認証方式を利用した発明である。

【０００８】

特許文献３は、コンテンツをダウンロードして利用させる発明であるが、コンテンツをダウンロードする際、ユーザの銀行口座やクレジットカード番号が漏洩することなく、また、料金の支払いと回収を安全に行うため、前払い済課金データを記録媒体に記録し、ダウンロードの度に料金を減額する方式を採用している。この方式により、大事な情報が漏洩せず、課金の手間を省くことを可能にした。

【先行技術文献】

【特許文献】

【０００９】

【特許文献１】特開２００８－６０７０３号公報

【特許文献２】特願２００９－１２０９９１号公報
【特許文献１】特開２００１－６０２８６号公報
【発明の概要】
【発明が解決しようとする課題】
【００１０】
しかしながら、特許文献１の方式では、メモリカードにダウンロードまたはカタログした時点では、暗号化はされておらず、初期作業において端末側で自己の端末シリアル番号等をキーにコンテンツの暗号化がなされて始めて当該端末だけで使用できるコンテンツが生成される。この暗号化前であれば、不正の目的をもった人物によって、不正なコピーコンテンツを製作できる。
【００１１】
このようにメモリカードをコピーガードされた状態にする前に無防備な状態がある。また、暗号化されていないコンテンツを伝送し、伝送後に暗号化するのは、暗号化の処理時間を考慮すると小規模なコンテンツに限られる。
【００１２】
そこで特許文献２のように暗号化されたコンテンツを予め製作し、メモリカード等のメディアに格納しておく方法が考えられる。市販されるコンテンツを格納したメモリカードの製作では、メモリカード独自にコンテンツの暗号化をすることは生産環境、時間、コスト面の制約から現実的ではない。通常、オリジナル・コンテンツと同じコードのコンテンツが一括で大量にコピー製作される。
【００１３】
保護すべきコンテンツを格納したメモリカードの利用が特定の端末のみに限定する方式は、メモリカードの盗難防止や不正使用の阻止を可能にする点において有用である。また、端末が携帯電話のような移動体通信機であったり、メディアがリムーバブルに装着できる小型の外部記憶装置であったりした場合には、利用をその組み合わせに限定する機能は強力な保護機能となる。これは、端末にユニークなコードによりメモリカードの情報を暗号化するなどの処置により実現する。即ち、論理的に相手側に紐付ける（関連付ける）方法であり、両者が切り離されると、相手側を関連付ける情報は一切存在せず、適正でない組み合わせの場合には、復号化した情報が意味をもたない。この方式は特許文献２が採用した発明のポイントである。
【００１４】
また、特許文献１には、端末側のシリアル番号を暗号キーとして、ＳＤメモリカードの認証情報とアプリケーションプログラムを暗号化することが記載されている。この場合、端末とＳＤメモリカードとの組み合わせが適正でなくとも実行し、不適正な場合は、意味のないアクセスや処理がなされる。この方法は推奨できるものではなく、使用前に適正かどうか判定する方が好ましい。さらに、認証情報の保護は重要な発明上のポイントであるが、特許文献１には詳細な説明が記載されていないため、推測であるが、おそらく、端末側に持った認証情報をＳＤメモリカードに転送しておき、照合に利用するものと考えられる。この場合には、分離後に相手側情報が残るため、暗号解読やコピーガードの仕組みなどが、ＳＤメモリカードから解明される恐れが生じる。また、その組み合わせを変更する場合には、認証情報やプログラムを端末側のコードで暗号化しているため、その解除と変更が大変な手間になり、情報の安全にも支障をきたすことになる。
【００１５】
コンテンツを含む市販されたメモリカードはコンテンツ故に価値がある。コンテンツを格納したメディアがリムーバブルであるならば、当然、コンテンツを格納したメディアとして、所有権が発生し、所有権を他人に譲渡できる機能が必要になる。また、同じ購入者（所有者）が端末の故障や買い替えなどで、組み合わせを変更することもある。このとき、組み合わせの変更ができないとか、変更に手間が掛かり、安全性が損なわれる事態が発生してはメディアの流通が阻害される。即ち、暗号化や認証情報の設定において、一方の情報を他方の情報と密接に関連させる場合には、その関連の変更に対応できることが必要

である。
【００１６】
この点において、特許文献２は、暗号化されたコンテンツが予め格納されており、当該メモリカードの所有者の変更にも簡便性がある。また、視聴用のプログラムも機種に合わせて、入れ替えも可能である。しかし、当該コンテンツを使用する機種が変更されてもコンテンツを入れ替えることができないことは問題である。機種が変わり、視聴用のプログラムが入れ替わった場合、コンテンツの構成に変更が必要でないという保証はない。また、コンテンツも更新され、近年の携帯端末の発展により、大画面を持つ機器も出現した。この場合に、コンテンツの変更もあり得る。
【００１７】
従って、コンテンツをダウンロードする方式が考えうるが、課金及び決済に伴うセキュリティ維持の問題が浮上する。この点、特許文献３では、予め、前払いしておき、コンテンツをダウンロードする度に料金を減額する方式であり、課金の確実性が保証されることと、決済時、クレジットカード等の重要な情報を取り扱うことがない点で安全である。しかし、残金の管理はコンテンツ提供側も購入側にも必要なことや、前払い金の納入時には、決済並みのセキュリティ維持が必要な点で依然として、問題の解決はできない。また、購入したコンテンツを譲渡することが困難であり、譲渡できる財産としてコンテンツを取り扱うことができない。
【００１８】
本発明は、以上の問題を解決するためになされたものであり、リムーバブル記憶メディアに格納されたコンテンツのコピーの防止を図り、その再生手段である閲覧・視聴端末装置との組み合わせが正当な場合のみに利用を制御できることに加え、特定のコンテンツを予め購入する予約がなされたリムーバブル記憶メディアを現物購入することにより、銀行口座やクレジットカード番号等の情報を扱うことなく、課金や決済の処理と無縁であることと、閲覧・視聴端末装置に合わせた視聴用プログラムとコンテンツをダウンロードできることと、リムーバブル記憶メディアを簡単な操作で安全に譲渡できることを兼ね備えたリムーバブル記憶メディアの閲覧・視聴システムを提供することを目的とする。
【課題を解決するための手段】
【００１９】
本発明に係るリムーバブル記憶メディアの閲覧・視聴システムはメディア固有情報及び暗号化されたコンテンツが格納されたリムーバブル記憶メディアと、このリムーバブル記憶メディアを装着して、前記暗号化コンテンツをコンテンツ復号キーにより復号化して閲覧・視聴させる閲覧・視聴端末装置と、正当メディアとしてリムーバブル記憶メディア毎に予めユニークに付けたパスワードと、このパスワードに紐付けたユニークな前記メディア固有情報と、前記リムーバブル記憶メディア毎に予め格納が予約された前記暗号化コンテンツについての識別情報であるコンテンツコードと、を相互に関連付けて登録した構造化情報ブロックと、前記メディア固有情報と前記パスワードが入力されたときに、前記パスワードと前記メディア固有情報の対をキーとするレコードが前記構造化情報ブロック存在すれば、この入力パスワードに関連付けたリムーバブル記憶メディアを正当と認証するメディア認証手段と、このメディア認証手段により正当性が認証されたリムーバブル記憶メディアの前記メディア固有情報を、このリムーバブル記憶メディアを装着した前記閲覧・視聴端末装置にユニークな装置固有情報をキーとして暗号化した暗号化メディア固有情報と、前記コンテンツコードに基づいて前記構造化情報ブロックから読み出したこの暗号化コンテンツの復号キーを、前記装置固有情報をキーとして暗号化した暗号化コンテンツ復号キーとを、このリムーバブル記憶メディアに格納する認証情報格納手段と、このリムーバブル記憶メディアに格納指定された前記暗号化コンテンツをそのコンテンツコードに基づいて前記構造化情報ブロックから所在を参照し、このリムーバブル記憶メディアにダウンロードする暗号化コンテンツ格納手段と、前記リムーバブル記憶メディアを前記閲覧・視聴端末装置に装着したときに、この暗号化メディア固有情報を、この装置固有情報で復号化したものが、このリムーバブル記憶メディアに格納された前記メディア固有情報と

一致したときに、このリムーバブル記憶メディアとこの閲覧・視聴端末装置との組合せを正当と認証する組合せ認証手段と、前記組合せの正当性が認証されたリムーバブル記憶メディアに格納した前記暗号化コンテンツ復号キーを、この閲覧・視聴端末装置の装置固有情報で復号化して得た前記コンテンツ復号キーにより、このリムーバブル記憶メディアに格納された暗号化コンテンツを復号化して閲覧・視聴させる閲覧・視聴手段と、を具備していることを特徴とする。

【００２０】

また、上記発明において、前記閲覧・視聴手段は、前記メディア認証手段により正当性が認証されたリムーバブル記憶メディアに、前記コンテンツコードに基づいて前記構造化情報ブロックからこの閲覧・視聴端末装置の機種に適合した閲覧・視聴用のビューアプログラムが所在するライブラリをアクセスし、ダウンロードするビューアプログラム格納手段と、このビューアプログラムを前記閲覧・視聴端末装置にロードし、このリムーバブル記憶メディアに格納した前記暗号化コンテンツを閲覧・視聴処理するビューアプログラム実行手段と、を具備していることを特徴とする。

【００２１】

さらに、上記発明において、前記暗号化コンテンツ格納手段は、前記メディア認証手段により正当性が認証される限り、前記コンテンツコードで関連付けた暗号化コンテンツの更新のためのダウンロードを含むことが望ましい。

【００２２】

この時のコンテンツのダウンロードは、同じコンテンツの再送であってもよいし、内容が更新されたコンテンツであってもよい。このように、電子週刊誌や電子新聞のような定期的に出版物を送付するアプリケーションにも本発明のコンテンツの再送・更新機能を利用できる。また、メディアの譲渡時やレンタル時にも次の利用者の端末装置に合わせて、認証情報、ビューアプログラムを再送し、格納するが、同様にコンテンツも再送される。

【００２３】

本発明は、１種類のコンテンツをダウンロードによる予約格納する形態を採るが、コンテンツグループ又はコンテンツメニューから選択できるアプリケーション構築又はサービス形態をとることができる。購入者が一つのコンテンツを選んだ後は、同じ認証機能と閲覧・視聴機能を発揮できる。

【００２４】

また、上記発明において、前記認証情報格納手段は、前記メディア固有情報と前記暗号化コンテンツ復号キーの暗号化処理の１過程として、被対象データへの加工処理を含んでいることが望ましい。

【００２５】

秘密鍵方式の暗号化と復号化は同じキーを使用するため、暗号化前の原データと暗号化後のデータを比較することにより、復号キーを解読されやすくなる。特に本発明においては、認証情報がメディアにあるので、暗号アルゴリズム解読の危険性が高い。これを防御するためには、暗号化の前に又は暗号処理の後で、あるいは、その両方でビット演算やビットずらしの加工処理を加えることにより、暗号化と復号化の間が非可逆的になり、解読が困難になる。ビットずらしは有効な解読防御手段であるが、キー情報を利用すると更に解読が困難になる。本発明で言えば、装置固有情報の最終バイトの値をビットずらしに利用すると、ずらし情報がキーにあるので、完全に隠蔽される。これを解読するためには、全数チェックがあるが、キーを長くとることにより解読を諦めさせることができる。

【００２６】

暗号化コンテンツについては、暗号化する前にコンテンツを圧縮処理することが好ましい。更に、暗号／復号キーは２５６バイト又は５１２バイトの長いもので、かつ、乱数のような出処に根拠がないものが全数チェックに対して強い安全性を与えるため、好ましい。

【００２７】

さらに、上記発明において、前記メディア固有情報と前記暗号化コンテンツ復号キーは

、前記リムーバブル記憶メディアのプロテクトエリアに格納され、前記プロテクトエリアは、データアクセス手段が秘匿されることが望ましい。

【００２８】

ＳＤメモリカードのような格納データの入出力を制御するコントローラを内蔵しているリムーバブル記憶メディアには、プロテクトエリアを設け、ここに認証情報のような秘匿すべき情報を格納し、特殊なコマンドを使用することによりアクセスできるというものがある。このようなメディアを利用できれば好ましい。プロテクトエリアが無くても暗号化により認証情報を隠蔽できるので、本発明はプロテクトエリアの有り、無しの両方を含む。

【００２９】

また、上記発明において、前記メディア固有情報は、前記リムーバブル記憶メディアの製造時に設定されたメディア固有の製造情報又はこのメディアを一意に識別する生成情報のいずれか一方であることが望ましい。

【００３０】

ＳＤメモリカードのようなリムーバブル記憶メディアには、製造時、製造情報がメディアに格納されることが多い。製造情報には一意に設定された製造番号があり、これをメディア固有の情報とすることができる。また、この製造情報は、製造情報の出力を制御するコントローラを具備しており、この製造情報をアクセスする特殊なコマンドが用意されている。また、この情報は更新や破壊ができない利点がある。しかし、このような仕組みを持たないメディアである場合には、メディアの製造時又は販売前の商品形成時にメディア毎にユニークな情報を生成し、格納する必要がある。この場合のメディア固有情報の生成方法は、「年・月・日・時・分・秒＋乱数」が好ましい。

【００３１】

また、上記発明において、前記閲覧・視聴端末装置は、携帯電話、携帯情報端末、タブレット端末、パーソナルコンピュータ、教育用情報機器、カーナビゲーション装置又は情報家電のいずれか一つであることが望ましい。

【００３２】

本発明に適合する機器は、ＳＤメモリカードのようなリムーバブル記憶メディアを装着でき、インターネット等の通信が可能な、視聴覚装置を備えた
ものであり、その候補が上記である。携帯電話の他、スマートフォンのような携帯情報端末、ｉＰｈｏｎｅ（登録商標）やｉＰａｄ（登録商標）のようなタブレット端末が代表的な機器である。また、パーソナルコンピュータ、教育用情報機器、カーナビゲーション装置又は情報家電には、備え付けが多いが、本発明の実施が可能である。

【００３３】

さらに、上記発明において、前記装置固有情報は、前記閲覧・視聴端末装置の製造時に設定された機器固有の製造情報、電話番号、メールアドレス、装置を一意に識別できる装置付属物の情報又はこの装置を一意に識別する生成情報のいずれか一つであることが望ましい。

【００３４】

本発明においては、装置固有情報は認証情報の暗号キーになる重要な情報であり、閲覧・視聴端末装置に一意でなければならない。また、ビューアプログラムから自動的にアクセスできる情報が好ましい。その意味から、電話番号やメールアドレスは適している。また、機器の製造情報や通信諸元もアクセス可能な場合には有用である。もし、これらが利用できない場合には、生成して記憶装置に格納しなければならない。一意性が要求されるので、この装置固有情報の生成方法は、「年・月・日・時・分・秒＋乱数」が好ましい。

【００３５】

さらに、上記発明において、前記パスワードの入力方法は、手入力、バーコード読みとり、２次元バーコード読みとりのいずれか一つであることが望ましい。

【００３６】

本発明のパスワードはメディア製造元又は販売者が設定する形態である。いわば商品番

号に相当する。従って、購入者が記憶することは難しく、メディアを梱包した内部にこのパスワードを記載した用紙などで提供される。原則、１回だけの使用なので、これで済むが、レンタル利用のように何度も使用される場合には不便である。このような利用形態では、バーコードや２次元バーコード（ＱＲコード等）の利用が好ましい。ただし、バーコードの場合には外部に無防備になるので、更に、２枚目のリムーバブル記憶メディアを一緒に販売し、２枚目にはパスワードを記録しておく。メディアがＳＤメモリカードならば、パスワードの使用時には２枚目のＳＤメモリカードをプログラムが読みとり、自動でサーバ等に送信する。２枚目のＳＤメモリカードには、パスワードの他、コンテンツ復号キー等の認証情報も格納でき、安全に認証情報を保護する認証用カードになりうる。また、パスワードを自動生成するならば、「年・月・日・時・分・秒＋乱数」や乱数生成後一意性チェックの手法が使える。

【００３７】

また、上記発明において、前記構造化情報ブロックは、データベース、表計算ワークシート、インデックス付きライブラリ、インデックス付き検索ファイル又はディレクトリ型フォルダ・ファイルのいずれか一つであることが望ましい。

【００３８】

パスワード／メディア固有情報の照合、コンテンツコードの取得、及びコンテンツコードに関連付けられたプログラムやコンテンツ取得には、情報の格納・登録機能と、検索機能に供することのできる構造化情報を有する媒体が必要になる。データベースが最も好ましく、また、ワークシートやインデックス付きライブラリも使える。また、ディレクトリ／ディクショナリを有する情報形態も適している。

【発明の効果】

【００３９】

本発明によれば、正当なホストデバイスとそのデバイスでのみしか閲覧・視聴できないメモリカードを提供する。即ち、コンテンツをコピーしたメモリカードでのアプリケーションの実行を不可能にし、又はコピーされたコンテンツ等を正常に閲覧できなくする効果を奏する。

【００４０】

また、セキュリティ確保を安全に保ちながら、市販されたコンテンツを簡便に譲渡できる仕組みを提供する。即ち、所有者決定時のみ、メモリカードの正当性を認証し、認証が正当ならば、ホストデバイスとメモリカードのコンビのみの利用を認める認証の設定を行い、以後は、ホストデバイスとメモリカードのコンビである認証のみで、暗号化の方式により安全にコンテンツを閲覧できる効果を奏する。

【００４１】

更に、販売時のメモリカードには、コンテンツと閲覧・視聴プログラムが格納されていないが、格納できるコンテンツが予約されており、購入後、所有者が自己のホストデバイスに適合したコンテンツと閲覧・視聴プログラムをネットワーク経由でダウンロードできる仕組みを提供する。ホストデバイスの機種を替える場合や、他人に譲渡する場合にも、機種に合ったコンテンツとプログラムに交換できる効果を奏する。

【図面の簡単な説明】

【００４２】

【図１】本発明の一実施形態に係るリムーバブル記憶メディアの閲覧・視聴システムの全体構成を示す模式図である。

【図２】本発明の一実施形態に係るリムーバブル記憶メディアの閲覧・視聴システムにおいて特定コンテンツとそのビューアのダウンロード予約を実現するリソース関連図である。

【図３】図１で示すリムーバブル記憶メディアを初期設定するとき、または譲渡あるいはレンタルするときの閲覧・視聴端末装置の処理フローを示すフローチャートである。

【図４】本発明におけるリムーバブル記憶メディアのコンテンツを閲覧・視聴端末装置により閲覧・視聴するときの閲覧・視聴端末装置の処理フローを示すフローチャートである

。
【図５】図１で示すリムーバブル記憶メディアと閲覧・視聴端末装置の電気的構成、及びネットワークに接続されたセットアップ情報供給装置を主に示すブロック図である。
【図６】図２で示した特定コンテンツとそのビューアの所在をより具体的に説明した模式図である。
【発明を実施するための形態】
【００４３】
以下、本発明の実施形態を図面に基づいて説明する。なお、これら複数の図面中、同一または相当部分には同一符号を付している。
【００４４】
本発明の実施形態に係るリムーバブル記憶メディアの閲覧・視聴システムは、閲覧・視聴端末装置としてパーソナルコンピュータ（ＰＣ）や、携帯電話を始めとする携帯端末を使用する。なお、通信機能及びコンピュータ機能を有する情報家電も本発明の閲覧・視聴端末装置に含めることができる。また、リムーバブル記憶メディアとしてＳＤメモリカードやＵＳＢフラッシュメモリを想定している。また、セットアップ情報供給装置としてデータベースを有するサーバシステムを用いている。ただし、データベースに限定されず、表計算ワークシートのようなデータが論理的に整列され、必要な情報のアクセスやデータ更新に伴う情報の再構成が即座にできる情報構造を有するものであればよい。
【００４５】
閲覧・視聴システムの典型的な構成は、携帯電話にＳＤメモリカードを装着する形態であり、小説や英会話等各種教材の閲覧や、映画、音楽のコンテンツの視聴には最適である。ＳＤメモリカードは大容量のコンテンツをコンパクトに保管でき、取り替え自由（着脱可能）なメモリメディアとして、好適である。
【００４６】
携帯電話では、電話番号という携帯電話にユニーク、すなわち、固有なアドレス情報を使用できる。また、携帯電話は閲覧・視聴用のアプリケーションプログラム（ビューア）をサーバからもＳＤメモリカードからも呼び込むことができ、アプリケーションプログラムは電話番号を呼び込むこともできる。
【００４７】
また、ＳＤメモリカードの製造時にメディアに付加される製造情報の一つである製造連続番号（シリアルＮＯ（ナンバー：番号））は、メディアにユニーク、すなわち、固有な番号であるため、ＳＤメモリカードを識別する情報として用いることができる。
【００４８】
一方、ＳＤメモリカードは、一般ユーザにはアクセスできないプロテクトエリアを設定することができる。このプロテクトエリアは認証情報等の制御情報を安全に格納するエリアとして使用できる。もっとも、本発明の認証情報は暗号等で保護されているので、プロテクトエリアの使用が必須というわけではない。より安全な保護が要求される場合にはこの機能を利用して二重の安全機構を提供することができる。
【００４９】
閲覧・視聴端末装置は、リムーバブル記憶メディアを装着する機能とセットアップ情報供給装置とコミュニケーションする機能を備えている。本実施形態を説明する前提として、閲覧・視聴端末装置のハードウェア構成と機能をまず説明する。
【００５０】
図５は、本実施形態における閲覧・視聴端末装置２のハードウェアの構成を示す構成図である。閲覧・視聴端末装置２は、基本的にはＲＯＭ５、ＲＡＭ６、ＣＰＵ７を具備し、さらに、内蔵不揮発メモリ８、操作部９、メモリカードインターフェイス４、ネットワークインターフェイス１０、付属デバイスインターフェイス１１、表示部１２を具備している。メモリカードインターフェイス４にはリムーバブル記憶メディア１が着脱可能に装着され、そのリムーバブル記憶メディア１にはプログラムやコンテンツが格納され、あるいはリムーバブル記憶メディア１の利用条件に関する制御情報を内蔵している。

【００５１】
閲覧・視聴端末装置２はバス１３により、上記ＣＰＵ７等のハードウェアの各機能要素４～１２同士を接続している。ＣＰＵ７は閲覧・視聴端末装置２の全体を制御するものであり、ＲＯＭ５に記憶された制御プログラムをＲＯＭ５からＲＡＭ６に呼び込んで実行する。内蔵不揮発メモリ８は閲覧・視聴端末装置２に備えられた固定の記憶装置であり、データや一時情報、プログラム等を格納している。操作部９は、キーボードであり、各種ボタンやキーを有し、利用者がＣＰＵ７に命令を与える機能を有する。表示部１２は液晶（ＬＣＤ）等のディスプレイであり、提供するサービスのメニューやデータ、画像等を表示する。付属デバイスインターフェイス１１は閲覧・視聴端末装置２が備えるスピーカ、カメラ、その他の機能部品の情報を出し入れするインターフェイスであり、図示しないが複数のインターフェイスがある。これらのＩ／Ｏデータや指令はバス１３を介して交換されており、その授受をＣＰＵ７が制御している。
【００５２】
セットアップ情報供給装置３は、ネットワークインターフェイス１０により、インターネット等の各種ネットワークを介して閲覧・視聴端末装置２と情報の授受を行う。セットアップ情報供給装置３は、例えば図１で示すサーバ１２０であり、パスワード照合ＤＢ１２１を備える。また図５では、セットアップ情報供給装置３は、ビューアプログラムライブラリ１２４及びコンテンツライブラリ１２６を備える。ビューアプログラムライブラリ１２４にはコンテンツ種別毎の視聴用のビューアプログラム群のライブラリである。コンテンツライブラリ１２６は、映画、音楽、芸能、文学、教育等に供されるコンテンツ群を格納したライブラリである。
【００５３】
ビューアプログラムライブラリ１２４及びコンテンツライブラリ１２６は、図５ではパスワード照合ＤＢ１２１と共にセットアップ情報供給装置３に連結されているが、他のサーバに接続されたビューアプログラムライブラリ又はコンテンツライブラリを利用することもできる。例えば、後述する図６のサーバ１２０ａ、サーバ１２０ｂ、サーバ１２０ｃのように分離して置かれてもよい。パスワード照合ＤＢ１２１のレコードには、当該コンテンツとそのビューアプログラムに関するコンテンツ情報がレコードとして登録されている。このレコードの項目に、ビューアプログラムとコンテンツのカタログ場所（サーバ／フォルダ／ファイル等の所在情報）が登録されている。
【００５４】
パスワード照合ＤＢ１２１は、パスワードを提示した者が正当なリムーバブル記憶メディアの所有者であるかどうかを照合するデータベースである。本発明では、リムーバブル記憶メディアの正当な所有者、または正当な利用者であるか否かを認証するために、リムーバブル記憶メディアにユニークな情報（例えば、ＳＤメモリカードのシリアルＮＯ．）と予め関連付けられたパスワードを組み合わせ、その両方を同時に提示できれば、正当であると認証する方法を利用している。そこで、前述のパスワードと対で登録したデータベースを用意し、当該製造情報とパスワードのユニークな情報の対をデータベースに登録した。正当性を確認するときは、同時に提示された２つのデータがデータベースの情報と一致性を照合すればよい。
【００５５】
リムーバブル記憶メディアにユニークな情報は製造されたメディアに自動的に付番される連番（例えば、ＳＤメモリカードのシリアルＮＯ．）が好ましい。ただし、自動的に付かない場合や全く固有化しないメディアもありうる。この場合には、メディア製造時、パッケージ製作時又はデータベース登録時に、生成してもよい。例えば、「年月日＋時分秒＋乱数」を当該番号にすると、絶対では無いが、実用的なユニークな番号が生成される。これを当該リムーバブル記憶メディアのユニークな情報とし、前述のパスワードと組にしてパスワード照合ＤＢ１２１に登録する。このＤＢ登録により、ユニークに識別可能なリムーバブル記憶メディアとなる。
【００５６】

なお、パスワードは、当該メディアに固有なコードであり、人為的に設けられたものである。これは、商品番号でもよいが、必ずユニークでなければならない。当該メディアへの関連付けの時期は、製造番号を持たないメディアの場合と同じであり、同様に、「年月日＋時分秒＋乱数」のような番号生成により付与することができる。

【００５７】

更に、パスワード照合ＤＢ１２１には、正当性の照合が成立したときに、コンテンツとそのコンテンツを視聴するビューアプログラムを閲覧・視聴端末装置２に転送するための情報が格納されている。セットアップ情報供給装置３は、閲覧・視聴端末装置２の機種に対応した再生用のアプリケーションプログラムであるビューア等を格納したビューアプログラムライブラリ１２４の所在を確認すると、コンテンツを閲覧・視聴するためのビューア等のアプリケーションプログラムを閲覧・視聴端末装置２に、電気通信回線の一例であるネットワーク１３０を介して送信する。なお、セットアップ情報供給装置３自体に当該プログラムファイルを所有していない場合には、コンテンツ情報提供ネットワーク１３１を介して、プログラムを所有するサーバからプログラムを取り寄せて転送する。あるいは、プログラムを所有するサーバから直接、閲覧・視聴端末装置２に転送させることもできるが、実施例では図示していない。また、同様に、コンテンツについても、正当性確認後、閲覧・視聴端末装置２の機種に対応したコンテンツの所在情報から、必要なコンテンツを取り出し、ネットワーク１３０経由で送信する。なお、コンテンツは暗号化されており、暗号化コンテンツと共にその復号キーも暗号化して、閲覧・視聴端末装置２に送信する。セットアップ情報供給装置３自体に当該コンテンツファイルを所有していない場合には、コンテンツ情報提供ネットワーク１３１を介して、コンテンツを所有するサーバからコンテンツを取り寄せる。このコンテンツが暗号化されていない場合には、暗号化する必要があるので、セットアップ情報供給装置３において暗号化処理して閲覧・視聴端末装置２に送信する。なお、暗号化されたコンテンツはリムーバブル記憶メディア１に格納される。

【００５８】

次に、本実施形態に、携帯電話、ＳＤメモリカード、サーバを用いて、コピーガードされたコンテンツの提供という目的を達成するリムーバブル記憶メディアの閲覧・視聴システムを説明する。

【００５９】

図１は、本実施形態の閲覧・視聴端末装置２に装着されたリムーバブル記憶メディア１がコピーガードを実現する仕組みを図解した模式図である。まず全体を概観すると、リムーバブル記憶メディア１としてＳＤメモリカード１００を用いる。閲覧・視聴端末装置２としては携帯電話１１０を使用する。また、携帯電話１１０は、ネットワーク１３０を介してセットアップ情報供給装置３としてのサーバ１２０と通信可能である。

【００６０】

ＳＤメモリカード１００には、製造情報１０３としてシリアルＮＯ（ナンバー：番号）３０が製造時より設定されている。シリアルＮＯ３０は、ＳＤメモリカード１００の製造時にメディア毎に、１つずつ連続して付与されるユニークな一意のコードであり、アプリケーションプログラムがＳＤメモリカード１００のコントローラにコマンドを発行したときに、カード識別レジスタＣＩＤに格納した製造情報１０３を授与する。本実施例では、この製造情報内にあるシーケンス番号をシリアルＮＯ３０としてＳＤメモリカード１００を識別する情報として用いる。なお、このＣＩＤレジスタに格納された製造情報１０３は破壊できない。

【００６１】

ＳＤメモリカード１００の認証情報エリア１０２には携帯電話１１０のアドレス情報としての電話番号２０で暗号化された暗号化シリアルＮＯ３０ａと同じく電話番号２０により暗号化された暗号化コンテンツ復号キー４０ａが格納されているが、この２つの情報は市販された当初は存在せず、初期設定時に暗号化されて格納される。認証情報エリア１０２の情報の安全性を確保することが最も重要なところから、この暗号化方式としては、公

開鍵方式が推奨されるが、共通鍵方式でも十分に目的は達成できる。本実施例では共通鍵（秘密鍵）方式を用いる。暗号アルゴリズムは公知のどのような方式でもよいが共通鍵（秘密鍵）方式を採用する場合には、暗号キーは復号キーにもなるので、暗号アルゴリズムが解読されやすい。そこで、暗号解読を不可にするため、暗号化する前に暗号化対象情報をビットずらしやビット計算のような加工を１クッション加えておくと直ちに復号できない。このような非可逆的な処置を施しておくことが望ましい。

【００６２】

例えば、暗号化には暗号化対象データをＸＯＲする方法が簡単であり、かつ、キーデータ長を大きくとれば全数検索に強くなる。その上で、ゼロ値が連続すると元の値が残り、復号方法がわかる場合があるので、バイト毎２５５をマイナスしてゼロ値を隠す処理や、８バイトを１ビットずつずらす処理を繰り返した後、ＸＯＲをかける方法を兼用することが望ましい。このようにすることにより、暗号と復号との間に非可逆の関係が生じる。ただし、この手段はプログラムから解読される恐れがある。従って、最も望ましいのは、ＳＤメモリカードのコントローラに上記の機能を導入することである。

【００６３】

また、認証情報エリア１０２をＳＤメモリカードのセキュリティ保護機能として提供されているプロテクトエリアに設定することが好ましい。プロテクトエリアは特定のコマンドを発行しなければアクセスできず、一般ユーザから隠蔽、保護されているからである。本実施例では、プロテクトエリアを採用しない形態を提供する。

【００６４】

特許文献２では、ＳＤメモリカード１００に既に暗号化された暗号化コンテンツ７０ａが格納されているものとして扱われた。本発明は、ＳＤメモリカード１００のユーザエリア１０１は市販時には空であり、利用者が当該ＳＤメモリカード購入後、セットアップ時にネットワーク１３０を経由して、特別に設定された暗号キーで暗号化された暗号化コンテンツ７０ａを受けるという方法を採る。ビューアファイル６０ａも同様である。ユーザエリア１０１は一般ユーザプログラムで自由にアクセスし、あるいは参照されるエリアである。従って、利用者は、このエリアに本実施形態とは無関係なプログラムやデータファイルを格納し、利用できる。当然、暗号化コンテンツ７０ａをコピーして他のメディアに記録できるが、暗号化されているので、所定の復号キーにより復号化しなければ閲覧・視聴はできない。

【００６５】

携帯電話１１０は表示部１２の一部としての携帯画面１１２を備える。また、プログラムやデータ処理に使用するアプリケーション実行エリア１１３を備える。アプリケーション実行エリア１１３にＳＤメモリカード１００に格納したビューアファイル６０ａからビューアプログラム６０を呼び込み、ビューアプログラム６０が暗号化コンテンツ７０ａを読み出し、コンテンツ復号キー４０でコンテンツ７０に復号化して、携帯画面１１２に表示する。コンテンツ復号キー４０は、ビューアプログラム６０がＳＤメモリカード１００の認証情報エリア１０２から暗号化コンテンツ復号キー４０ａを呼び込み、電話番号２０で復号化したものである。

【００６６】

携帯電話１１０の電話番号２０は閲覧・視聴端末装置２のユニークなアドレス情報に相当する。この情報は閲覧・視聴端末装置２にユニークな情報でなければならない。本実施形態では、携帯電話１１０の電話番号を採用した。このユニークなアドレス情報として、メールアドレスや機器にユニークな製造番号であってもよい。ただし、ビューアプログラム６０がプログラムにより取得できる情報である必要がある。電話番号２０は携帯電話１１０の内蔵不揮発メモリ８に格納され、ビューアプログラム６０がアクセスできる情報である。なお、電話番号等既知の情報を使用せずに、独自に生成したユニーク番号を利用してもよい。この内蔵不揮発メモリ８に独自に生成したユニーク番号を格納しておく。ユニーク番号は乱数であってもよいし、よりユニークさを維持するために、ＳＤメモリカードとの組み合わせが成立したときの「年月日＋時分秒＋乱数」を利用してもよい。

【００６７】
ＳＤメモリカード１００の暗号化シリアルＮＯ３０ａと暗号化コンテンツ復号キー４０ａは電話番号２０で暗号化されているので、ＳＤメモリカード１００を携帯電話１１０に装着したとき、復号キーになる電話番号２０が得られる。しかし、その組合せ（コンビネーション）が正当でなければ正しい復号キーにはならない。この組合せが正しければ、暗号化シリアルＮＯ３０ａを復号化したシリアルＮＯ３０は、製造情報１０３にあるシリアルＮＯ３０と一致し、正しい組み合わせとわかる。従って、暗号化コンテンツ復号キー４０ａを電話番号２０で復号化すれば、コンテンツ復号キー４０が得られ、暗号化コンテンツ７０ａをこのコンテンツ復号キー４０で復号化すればコンテンツ７０として利用できる。すなわち、携帯電話１１０にはＳＤメモリカード１００の認証となるシリアルＮＯ３０が存在しないこと、同様にＳＤメモリカード１００には携帯電話１１０の認証となる電話番号２０が存在しない点に特徴がある。どちらか一方のみでは解読は困難である。
【００６８】
携帯電話は通信キャリアによりＯＳの仕様が異なる。従って、このＯＳ下で稼働するビューア等のプログラムの仕様も当該ＯＳに準拠しなくてはならないことを意味する。更に、ビューアプログラムの仕様や機能とコンテンツの仕様が視聴可能なように対応しなくてはならない。また、ＳＤメモリカード１００は利用された後、自由に譲渡され、譲渡時には相手の機種に応じたビューアプログラムとコンテンツに入れ替えできることが望ましい。従って、ＳＤメモリカード１００の購入時や譲渡時に、コンテンツと閲覧・視聴するビューアプログラムは、当該利用機種のＯＳに対応したリソースをダウンロード等の操作を経て提供されねばならない。
【００６９】
ＳＤメモリカード１００は購入時、空でありコンテンツ、ビューアプログラムは格納されていない。勿論、認証情報エリア１０２も空の状態である。パッケージに当該ＳＤメモリカードは、特定のコンテンツを格納して視聴できる由が記載されている。コンテンツはビューアの仕様、視聴機器、また、　日本語・英語等の言語等に応じて、バリエーションが存在する。ビューアプログラムを含めて、これらの好みのバリエーションに応じて、ＳＤメモリカードへダウンロードできれば合理的である。また、一度、コンテンツ及びビューアプログラムが格納されれば、そのまま永続利用されることが好ましい。ただし、他のＳＤメモリカードにコンテンツをコピーされて利用されないように防御する機能が必要になる。また、このダウンロードを受ける権利の無い者に不法にダウンロードされないような仕組みが必要である。本実施形態では次のような技術的工夫を施した。
【００７０】
ＳＤメモリカード毎に固有のパスワードを、このＳＤメモリカード１００の製造時または販売時設定する。このパスワードは購入者、すなわち、ＳＤメモリカード１００の所有者しか知りえないものとして管理される必要がある。ただし、当該パスワードの使用は、購入後の１回であり、その後の利用には要求されない。同様に、譲渡時に１回だけ使うと、その後の利用には要求されない。即ち、利用時は前述のように、ＳＤメモリカード１００と携帯電話１１０との組合せの認証は人間の手を介さず実行されるからである。このようにして利用の都度、パスワードを入力する手間を無くし、パスワードの忘却や漏洩を防止できる。図１に示すように正当なＳＤメモリカード１００（リムーバブル記憶メディア１）のパスワード５０は、パスワード照合データベース１２１に格納されてサーバ１２０により管理される。このサーバ１２０は例えばＳＤメモリカード１００の管理者により管理される。
【００７１】
パスワード照合データベース１２１には、それぞれパスワード５０が付与された、販売予定のＳＤメモリカード１００の全数について、パスワード５０と、ＳＤメモリカード１００の製造連続番号（ユニーク番号）であるシリアルＮＯ３０ｂの２つの項目をキーとするシリアルＮＯ情報レコード１２２が格納されている。これらシリアルＮＯ情報レコード１２２には、対象のＳＤメモリカード１００に予め格納が予約されたコンテンツのコード、

即ちコンテンツコード７２の項目が含まれる。更に、コンテンツコード７２をキー項目としたビューア情報レコード１２３とコンテンツ情報レコード１２５が格納される。

【００７２】

ビューア情報レコード１２３は、コンテンツコード７２、機種８０、ビューア所在情報６１、ビューアファイル名６０ｂの情報を相互に関連付けて格納している。機種８０は携帯電話１１０の機種であり、メーカや製品の種別、及び当該携帯電話１１０のＯＳによりビューアプログラム６０が異なることを想定している。更に、コンテンツ７０によってもビューアプログラム６０の種類が用意されているかもしれない。そして、求めるビューアプログラム６０を格納するファイル名がビューアファイル名６０ｂである。多くのビューアプログラムの内、求めるビューアプログラム６０がどのビューアプログラムＬＩＢにあるかを示すのがビューア所在情報６１である。ビューア所在情報６１はアドレス情報の形式で表現される。本実施形態では、サーバ／ライブラリ名であるが、国や組織又はサイト等、様々な環境に対して実際の所在がコンピュータ処理できる情報形式であればよい。

【００７３】

同様に、コンテンツ情報レコード１２５はコンテンツコード７２、機種８０、コンテンツ所在情報７１、コンテンツファイル名７０ｂ、コンテンツ復号キー４０の情報を相互に関連付けて格納している。コンテンツコード７２、機種８０、コンテンツ所在情報７１、コンテンツファイル名７０ｂまでは、ビューアプログラムとコンテンツが置き換わったと同様の意義を持つ。コンテンツ７０は、暗号化されて、暗号化コンテンツ７０ａとしてＳＤメモリカード１００に格納されている。コンテンツ復号キー４０はＳＤメモリカード１００に格納した暗号化コンテンツ７０ａを復号化するための復号キーである。コンテンツの暗号化は、コンテンツＬＩＢ１２６内に既に暗号化されていても、あるいは、サーバ１２０からＳＤメモリカード１００にダウンロードする直前に暗号化してもよい。

【００７４】

まず、ＳＤメモリカード１００の利用の初期または譲渡時に、利用者が、携帯電話１１０にＳＤメモリカード１００を装着した後、ネットワーク１３０を介して、サーバ１２０に対して、セットアップを要求する。ロードされたセットアッププログラムが取得したシリアルＮＯと入力パスワード、及び携帯電話１１０の電話番号２０と機種８０とをサーバ１２０に送信する。パスワード照合ＤＢ１２１における当該ＳＤメモリカード１００のシリアルＮＯ情報レコード１２２のシリアルＮＯ３０ｂ（キー項目）とパスワード５０（キー項目）が送信されたパスワード等と一致した場合は、正当なメディアであると認証する。同時にこのＳＤメモリカード１００に関連付けられているコンテンツとそのビューアプログラムを得るために、シリアルＮＯ情報レコード１２２のコンテンツコード７２（キー項目）からビューア情報レコード１２３とコンテンツ情報レコード１２５をアクセスし、送信された機種８０に適合したビューアプログラムとコンテンツを検索する。サーバ１２０は、ビューア所在情報６１及びコンテンツ所在情報７１を参照して、該当したビューアプログラムライブラリ１２４に格納してあるビューアファイル名６０ｂとコンテンツライブラリ１２６に格納してあるコンテンツファイル名７０ｂをアクセスする。コンテンツが暗号化されていない場合には、サーバ１２０は、コンテンツ情報レコード１２５のコンテンツ復号キー４０により、コンテンツを暗号化する。サーバ１２０は、このビューアファイル６０ａと暗号化コンテンツ７０ａを携帯電話１１０に送り、携帯電話１１０で作動中のセットアッププログラムが、ビューアファイル６０ａと暗号化コンテンツ７０ａをＳＤメモリカード１００のユーザエリア１０１に格納する。

【００７５】

次に、サーバ１２０は、コンテンツ復号キー４０とシリアルＮＯ３０を電話番号２０で暗号化し、携帯電話１１０に送付する。携帯電話１１０で作動中のセットアッププログラムは、暗号化された暗号化シリアルＮＯ３０ａと暗号化された暗号化コンテンツ復号キー４０ａを認証情報エリア１０２に格納する。この処理によりＳＤメモリカード１００はコピーガードされたコンテンツ７０を格納したものになる。

【００７６】

なお、コンテンツ復号キー４０とシリアルＮＯ３０に対する、電話番号２０を暗号キーとして暗号化する処理は、携帯電話１１０に送信されたセットアッププログラムが実行してもよい。暗号化をサーバ１２０側または携帯電話１１０側のどちらで実行しても本実施形態に含まれることは言うまでもない。

【００７７】

また、パスワード５０を本実施形態では利用者の手入力で行っているが、別のＳＤメモリカードに格納したパスワードを送信するとか、携帯電話１１０内に保護されて格納したパスワードをセットアッププログラムが自動送信する方法であってもよい。

【００７８】

さらに、図示していないが、リムーバブル記憶メディア１のレンタルでは、譲渡と同様にＳＤメモリカード１００をセットアップし直すが、このとき、レンタル期間を設定するように構成してもよい。

【００７９】

また、パスワード５０を所有者が自己の携帯電話１１０から送信し、レンタル側の携帯電話の番号をサーバ１２０に知らせると、ＳＤメモリカード１００を自己の携帯電話に装着したレンタル者にセットアッププログラムをサーバ１２０から送信する方法でもよい。このセットアッププログラムはパスワードの入力を要求せず、装着したＳＤメモリカード１００のシリアルＮＯ３０の照合を行うことで足りる。この方法であれば、レンタル者にパスワードを知られる虞は解消する。

【００８０】

更に、譲渡時は、新たな正当な所有者（利用者）がパスワードを変更してもよい。旧パスワードと変更後のパスワードの一致が確認されたときに、旧パスワード５０を変更すれば済むだけである。

【００８１】

図２は、コンテンツとそのビューアプログラムのダウンロード予約を実現するリソース関連図である。本発明は、認証機能を付加したＳＤメモリカードをコンテンツが空のままで販売することに主要な特徴を置いている。消費者は、店頭に並べられたパッケージを見てコンテンツを知る。コンテンツに興味を持てば購入する。この時点で最終の需要者が店への支払い行為を実行する。店や、卸等を介して製作元との決済は簡便化される。更に、視聴するコンテンツとビューアは購入者の機種に合わせなくてはならない。すべてのバリエーションを揃える製作者にとっても店にとっても負担が掛かる。この点、ダウンロード機能により、購入後、購入者が機種に合わせてバリエーションを選ぶというビジネスの方法は販売側の負担軽減になる。また、購入側にも選択の幅が拡がるという可用性向上のメリットを与えることができ、両者に便利である。なお、本実施例ではバリエーションを携帯電話の機種に応じたバリエーションを例としているが、言語やビューア機能別のバリエーションもあり得る。この場合には、コンテンツとビューアプログラムの選択肢となる別の情報も必要になる。本発明は図示していないが、これらのバリエーションも包含している。

【００８２】

図２に基づいて、このコンテンツ／ビューアが予約された市販用のコピーガード付きＳＤメモリカードの製造と販売管理方法、及び、購入後コンテンツ／ビューアのダウンロード方法を説明する。

【００８３】

まず、手順の最初は、コピーガードされたコンテンツを格納するＳＤメモリカード１００について、その製造シリアルＮＯ３０に対応するＳＤメモリカード１００毎にユニークなパスワード５０を対応づけたパスワード照合データベース１２１を設計する。また、配給するコンテンツに結びつくコンテンツコード７２及び当該コンテンツの暗号化／復号化に関する設計も含める。コンテンツコード７２は、パスワード照合データベース１２１に格納したコンテンツに関するコンテンツ情報レコード１２５と当該コンテンツを視聴するビューアプログラムに関するビューアプログラム情報レコード１２３を関連付けている。

【００８４】
コンテンツ情報レコード１２５には、当該コンテンツがどこにあるかを示すコンテンツ所在情報７１の項目がある。携帯電話の機種別にコンテンツが異なる場合や、本実施例には含めていないが英語版や日本語版等のバリエーションもあるので、複数の所在があり得る。その所在は、遠隔地点に設置されたサーバであってもよい。また、提携したビジネスパートナーである場合もある。これらの所在をコンテンツ所在情報７１で示し、更に機種８０とコンテンツファイル名７０ｂでバリエーションを設定している。コンテンツは暗号化されて格納されていることが安全なので、コンテンツの復号化のためのコンテンツ復号キー４０の項目も設定する。
【００８５】
同様に、ビューアプログラム情報レコード１２３には、当該ビューアプログラムがどこにあるかを示すビューア所在情報６１の項目がある。コンテンツのバリエーションに合わせて、機種８０、ビューアファイル名６０ｂが存在することは、コンテンツ情報レコード１２５と同じである。
【００８６】
コンテンツとそのビューアがバリエーションを持ち、その製作場所も様々なケースが想定される。従って、サーバ等のコンピュータシステムにコンテンツとビューアプログラムのライブラリに接続し、コンテンツ等を伝送して配給する。図２では、サーバ１２０ａにコンテンツライブラリ１２５ａと１２５ｂを接続し、サーバ１２０ｂにビューアプログラムライブラリ１２４ａと１２４ｂを接続し、サーバ１２０ｃにコンテンツライブラリ１２５ｃとビューアプログラムライブラリ１２４ｃを接続した、それぞれ分散した配置のも模式図を載せている。具体的には、図６に示すように、コンテンツ情報提供ネットワーク１３１にサーバ１２０、１２０ａ、サーバ１２０ｂ、サーバ１２０ｃを接続し、所望のコンテンツとビューアプログラムを一度サーバ１２０に集め、暗号化等の処理を実施し、サーバ１２０から、ネットワーク１３０を経由して携帯電話１１０にダウンロードする方法を図示している。コンテンツ所在情報７１及びビューア所在情報６１には、所在を表すディレクトリがコード化されるが、その表現は、インターネットのＵＲＬ型でもパソコンＯＳの型でもよい。「サーバ名／ライブラリ名／フォルダ名／・・／フォルダ名／ファイル名」のように階層で表現してもよい。
【００８７】
本発明の本実施例では、コンテンツの暗号化は共通鍵方式を使用する。従って、暗号キーは復号キーと同一である。コンテンツファイル名７０ｂにファイリングされたコンテンツ７０は、ＳＤメモリカードに暗号化され、コンテンツ７０ａとして格納されている。暗号化する時点は、コンテンツライブラリ内でも、サーバ１２０から携帯電話１１０へ送信するときに暗号化してもよい。
【００８８】
次に、コンテンツの格納を予約した表記がされたＳＤメモリカードの製作手順を説明する。製造されたＳＤメモリカード１００には、製造時、製造情報としてシリアルＮＯ３０がＳＤメモリカード１１０に格納される。この自動設定がなされない場合には、図２には図示していないが、前述したように、ユニークなコードを当該ＳＤメモリカードに格納しなければならない。このシリアルＮＯ３０に対して、パスワード５０（商品番号でもよい）を付与する。このパスワード５０もＳＤメモリカード１１０毎にユニークなコードである。即ち、ＳＤメモリカード１１０は固有のシリアルＮＯ３０と固有のパスワード５０が関連付けられる。認証時、両方のコードが組みで示され、両方が一致していなければ認証されたことにならない。
【００８９】
更に、ＳＤメモリカード１００毎に、パスワード設定書５０ａを印刷（またはカード化）して、各ＳＤメモリカード１００にそれぞれ添付して販売する。これにより、パスワード設定書５０ａとＳＤメモリカード１００をセットにした販売用のＳＤメモリカード１００が完成する。パスワード設定書５０ａの中には、携帯電話１１０に購入したＳＤメモリ

カード１００を装着してから、当該パスワード５０をサーバ１２０に知らせることにより、コンテンツ格納が実現する説明が記載されている。また、パスワード５０の使用は、コンテンツ格納時の１回であり、譲渡時には、パスワード設定書５０ａと共にＳＤメモリカード１００を共に譲渡し、同様の操作により、譲渡者もコンテンツを視聴できる旨が説明されている。なお、パスワード５０のサーバ１２０への知らせ方は、本実施例では、携帯電話１１０の画面１１２から入力操作を行うが、バーコードやＱＲコードをパスワード設定書５０ａに添付して、これを携帯電話１１０のリーダにより読み取り、送信する手段もあり、これも本発明に含まれることは言うまでもない。

【００９０】

図３は、リムーバブル記憶メディア１を初期設定し、または譲渡、あるいはレンタルするときの閲覧・視聴端末装置２の処理フローである。すなわち、利用者が販売用のＳＤメモリカード１００を購入し、自己の携帯電話１１０に装着し、サーバ１２０にセットアップを要求する処理フローである。なお、ＳＤメモリカード１００の譲渡時も同様の操作を新たな所有者（利用者）が行う。また、レンタル時は、所有者がレンタル者の携帯電話１１０にＳＤメモリカード１００を装着して設定をし直し、その後レンタルする形式であるが、もっと好適なレンタル方法については、図１にて説明してある。

【００９１】

図３に示すようにまず、利用者が携帯電話１１０からサーバ１２０にＳＤメモリカード１００のセットアップを要求する（Ｓ３００）。すると、次のＳ３０１では、サーバ１２０がセットアップ画面を含むセットアッププログラムをネットワーク１３０経由で当該携帯電話１１０に送信する。携帯電話１１０は受信したセットアッププログラムを実行する（Ｓ３０２）。このセットアッププログラムを携帯電話１１０のＣＰＵ７により実行することにより、携帯電話１１０は、メディア認証手段として機能する。なお、メディア製造情報暗号化手段、復号キー暗号化手段についても携帯電話１１０側で実行可能であるが、本発明ではサーバ１２０で実行する形態をとる。セットアッププログラムはＳＤメモリカード１００のコントローラにカード識別情報を格納するＣＩＤレジスタの製造情報を要求するコマンドを発行し、ＳＤメモリカード１００のシリアルＮＯ３０を取得する（Ｓ３０４）。Ｓ３０５でＳＤメモリカード１００のコントローラがシリアルＮＯ３０を授与する。なお、シリアルＮＯ３０をコントローラが管理していない場合は、前述のように、ＳＤメモリカード製造時にこれに替わるＳＤメモリカード１００に固有のコードを生成して、シリアルＮＯ３０としてＳＤメモリカード１００内に格納する。

【００９２】

セットアッププログラムはＳ３０６で携帯電話１１０の電話番号２０を携帯電話１１０の内蔵不揮発メモリ８からアクセスする。

【００９３】

利用者は、Ｓ３０３において、パスワード設定書５０ａを参照してパスワード５０と、自己の携帯電話１１０の機種とを画面入力する。すると、セットアッププログラムは、Ｓ３０４で得たシリアルＮＯ３０とＳ３０６で得た電話番号２０と、画面上のパスワード５０と機種８０をセットアップ確認情報としてサーバ１２０に伝送する（Ｓ３０７）。また、機種８０以外にもコンテンツとビューアプログラムの選択肢がある場合には、その判別のための情報も画面入力情報に必要であることは言うまでもない。

【００９４】

Ｓ３０８でサーバ１２０は、シリアルＮＯ３０、電話番号２０、パスワード５０、機種８０を受信し、シリアルＮＯ３０をキーにパスワード照合ＤＢ１２１をアクセス（Ｓ３０９）する。受信したシリアルＮＯ３０は、読み込んだデータベース上のシリアルＮＯ情報レコード１２２のシリアルＮＯ３０ｂ（キー項目）と照合され、これらが一致したとき、すなわち、当該レコード項目の複数のパスワード５０の中に、受信したパスワード５０と同一のパスワード５０がある場合は、正当な利用者がセットアップを要求したことになる。この照合をＳ３１０で行う。一致したパスワードが無い場合は、Ｓ３１１でエラー（例えばＳＤメモリカードが正しくない等）のメッセージが携帯電話１１０へ返信され、終了

する（図示していないが再入力を促してもよい。）。すなわち、メディア認証手段により、このＳＤメモリカード１００の所有者が正当な購入者、転得者等正当な権利者であるか否かが認証される。なお、照合には、パスワード５０をキーに行ってもよく、または、シリアルＮＯ３０とパスワード５０の両方をキーにレコードの存在可否を照合に使ってもよい。

【００９５】

この認証が正当であったときは、パスワード照合ＤＢ１２１の当該シリアルＮＯ情報レコード１２２から、この一致したパスワード５０に関連付けられているコンテンツコード７２を取り出す。コンテンツコード７２をキーにビューア情報レコード１２３をアクセスし、機種８０に適合したビューア情報レコード１２３上のビューアファイル名６０ｂに基づき、ビューア所在情報６１を求める。このビューア所在情報６１を基にビューアプログラムライブラリ１２４を検索するが、ライブラリが他のサーバにある場合には、コンテンツ情報提供ネットワーク１３１を介して当該サーバに接続されたビューアプログラムライブラリ１２４をアクセスする。この結果、ビューアプログラムライブラリ１２４よりビューアファイル６０ａをアクセスし、サーバ１２０に取り込み（Ｓ３１２）、携帯電話１１０へダウンロードする（Ｓ３１１）。前述のコンテンツ復号キー４０と共に携帯電話１１０へダウンロードする（Ｓ３１３）。ビューアファイル６０ａにあるビューアプログラム６０は、携帯電話１１０のＣＰＵ７により実行されることにより、閲覧・視聴手段として機能する。

【００９６】

携帯電話１１０のセットアッププログラムは、Ｓ３１３において、ビューアプログラム６０をカタログするビューアファイル６０ａをＳＤメモリカード１００に書き込む。ＳＤメモリカード１００のコントローラがビューアファイル６０ａをユーザエリア１０１に格納する（Ｓ３１４）。

【００９７】

次に、サーバ１２０は、コンテンツコード７２をキーにコンテンツ情報レコード１２５をアクセスし、機種８０に適合したコンテンツ情報レコード１２５上のコンテンツファイル名７０ｂに基づき、コンテンツ所在情報７１を求める。このコンテンツ所在情報７１を基にコンテンツライブラリ１２６を検索するが、ライブラリが他のサーバにある場合には、コンテンツ情報提供ネットワーク１３１を介して当該サーバに接続されたコンテンツライブラリ１２６をアクセスする。この結果、コンテンツライブラリ１２６よりコンテンツファイル名７０ｂの指すファイルをアクセスし、サーバ１２０に取り込む（Ｓ３１５）。このとき、本実施例では、コンテンツファイル名７０ｂの指すファイルに格納されているコンテンツ７０は暗号化されていないものとして扱っているので、コンテンツ情報レコードにあるコンテンツ復号キー４０で暗号化する（Ｓ３１６）。ただし、すでに暗号化されている場合には暗号化処理は行わない。なお、本実施例では、コンテンツの暗号キーと復号キーは同一であるが、公開キー方式の場合には、暗号キーは別途情報として用意しておく必要がある。暗号化されたコンテンツ７０は、携帯電話１１０へダウンロードされ（Ｓ３１７）、セットアッププログラムがＳＤメモリカード１００に格納する（Ｓ３１８）。

【００９８】

次に、サーバ１２０はメディア製造情報暗号化手段と復号キー復号化手段として、セットアッププログラムから送信された電話番号２０を暗号キーに、受信したＳＤメモリカード１００のシリアルＮＯ３０とコンテンツ情報レコード１２５のコンテンツ復号キー４０を電話番号２０で暗号化し、それぞれ暗号化シリアルＮＯ３０ａと暗号化コンテンツ復号キー４０ａを生成（Ｓ３１９）し、認証情報として携帯電話１１０へ送信する（Ｓ３２０）。セットアッププログラムは、コントローラに認証情報エリア１０２へ暗号化シリアルＮＯ３０ａと暗号化コンテンツ復号キー４０ａの格納する（Ｓ３２１）。なお、認証情報エリア１０２がプロテクトエリアの場合には、コントローラへプロテクトエリアへの格納コマンドにより実行を命じなければならない。セットアッププログラムは、Ｓ３２２において、正常にセットアップが完了したことを利用者に画面上で知らせる。この後、セット

アッププログラムは、携帯電話１１０より消滅する。なお、Ｓ３１９のシリアルＮＯ３０とコンテンツ復号キー４０の暗号化、即ち、メディア製造情報暗号化手段と復号キー復号化手段は携帯電話１００で行ってもよいことは前述したとおりである。

【００９９】

図４は、本発明におけるリムーバブル記憶メディア１を閲覧・視聴に利用するときの閲覧・視聴端末装置２の処理フローである。利用者がＳＤメモリカード１００を自己の携帯電話１１０に装着し、コンテンツ７０を閲覧・視聴する処理フローである。

【０１００】

Ｓ４００において、まず、利用者が携帯電話１１０にコンテンツ７０の閲覧等をメニューから選択する。携帯電話１１０は、Ｓ４０１でＳＤメモリカード１００のユーザエリア１０１にあるビューアファイル６０ａからビューアプログラム６０をロードし（Ｓ４０２）、実行する。ビューアプログラム６０は、Ｓ４０３で自己の電話番号２０を取得する。次に、ＣＩＤレジスタの製造情報をアクセスするコマンドを発行して要求し（Ｓ４０４）、ＳＤメモリカード１００のコントローラは製造情報のシリアルＮＯ３０を授与する（Ｓ４０５）。なお、製造情報のシリアルＮＯ３０が製造時予め生成されない場合には、ＳＤメモリカード１００固有のコードを作成し、ＳＤメモリカードのユーザエリア等に格納することは前述した。本実施例では製造時に生成され、コントローラへのコマンドによりアクセスする方式で説明してある。次に、ビューアプログラム６０は、認証情報エリア１０２に格納した暗号化シリアルＮＯ３０ａを取得する（Ｓ４０６）。Ｓ４０７で、コントローラから暗号化シリアルＮＯ３０ａを取り出す。この暗号化シリアルＮＯ３０ａは正当な組合せが認証された携帯電話１１０の電話番号２０で暗号化されている。そこで、まず、電話番号２０を復号キーとして、暗号化シリアルＮＯ３０ａを復号化し、シリアルＮＯ３０に復号化する（Ｓ４０８）。

【０１０１】

暗号化シリアルＮＯ３０ａのシリアルＮＯは認証された正当なＳＤメモリカード１００のシリアルＮＯである。現在装着しているＳＤメモリカード１００の製造情報にあるシリアルＮＯと比較して、両方のシリアルＮＯ３０が一致すれば正当な利用になる。Ｓ４０９で、両方のシリアルＮＯ３０を比較する。不一致ならば、正当な組合せではないので、画面にエラー表示をする（Ｓ４１０）。一致すれば正当なＳＤメモリカード１００と携帯電話１１０の組み合せと認証される。すなわち、組合せ認証手段により、リムーバブル記憶メディア１と携帯電話１１０との組合せの正当性が認証される。Ｓ４１１では、次にコンテンツをアクセスするために、認証情報エリア１０２に格納した暗号化コンテンツ復号キー４０ａを取得する。認証情報エリア１０２から暗号化コンテンツ復号キー４０ａを読出す（Ｓ４１２）。ビューアプログラム６０は電話番号２０で暗号化コンテンツ復号キー４０ａを復号化し、コンテンツ復号キー４０を得る（Ｓ４１３）。なお、認証情報エリア１０２がプロテクトエリア仕様であった場合には、コントローラへアクセスコマンドを発行してプロテクトされた情報を授与してもらわねばならないことも前述してある。本実施例では、認証情報エリア１０２をプロテクトエリアに設定しない方式で説明している。認証情報は暗号により隠蔽されているので、この実施例の方法でもよい。

【０１０２】

ＳＤメモリカード１００のユーザエリア１０１に格納した暗号化コンテンツ７０ａはコンテンツ復号キー４０で暗号化されている。従って、Ｓ４１２で生成したコンテンツ復号キー４０でこの暗号化コンテンツ７０ａを復号化すれば閲覧・視聴できるコンテンツ７０が得られる。この後は、この復号化処理が繰り返されるが、Ｓ４１４でユーザエリア１０１から暗号化コンテンツ７０ａの１ブロックを読み込み（Ｓ４１５）、Ｓ４１６で当該ブロックをコンテンツ復号キー４０で復号化する。これを繰り返し、ビューアプログラム６０が処理できる情報を形成できる。すなわち、視聴閲覧手段により、暗号化コンテンツ復号キーが形態電話１１０の電話番号により復号され、この復号キーにより暗号化コンテンツが復号化され、携帯電話１１０で再生されてユーザにより閲覧・視聴される。この後は、ビューアプログラム６０とコンテンツ７０によるアプリケーション処理になる（Ｓ４１

７）。この処理は、ビューアアプリケーションに引き継がれる。

【０１０３】

なお、上記実施形態では、コンテンツを、予め、リムーバブル記憶メディア１（ＳＤメモリカード１００）に格納していたが、セットアップ時に、ビューアと一緒に供給することもできる。ただし、ネットワークを介すれば、ダウンロードに長時間を要することを覚悟しなければならない。

【０１０４】

また、リムーバブル記憶メディア１がＳＤメモリカード１００など、コントローラを内蔵するメディアであれば、認証情報の暗号化及び復号化をコントローラが実行できるように機能を設定する。このようにすると認証方法のアルゴリズムが完全に隠蔽できる。また、ＳＤメモリカードであれば、コントローラに内蔵するＲＣＡレジスタを通じて、ビューアプログラムとコントローラがお互いの秘密コードを交換する方式を実施すれば、お互いの正当性を確認でき、利用プログラムの自体の正当性を認証できるので、より優れたコピー操作のプロテクトが実現する。

【０１０５】

なお、暗号アルゴリズムについは、本実施形態は共通鍵方式（秘密鍵方式）を想定しているが、既存の手法を使用することができる。例えば、全数探索で解読される虞があるため、特に、コンテンツの暗号化については、シリアルＮＯの特定３ビットの数分（１～７ビット）のビットずらしの方法、ゼロ値が連続すると元の値が残る場合を避けるためバイト毎に２５５をマイナスする方法、及び、コンテンツキーを１ブロック長として、ＸＯＲビット計算するなどの付加処理を取り入れることが好ましい。１ブロックが５１２バイトであれば、４０９６ビットのキーとなり、前述の各方式を組み合わせることにより、全数探索による解読は事実上不可能である。本実施形態は共通鍵方式で説明したが、前述のような方法を用いれば解読の不可能な非可逆効果を奏することができる。また、公開鍵方式のような非対称キーの採用は元々非可逆的な方式であるため、本発明には好ましい。

【０１０６】

以上説明したように本実施形態によれば、その市販用メモリカードにユニークなコードと当該コードに固有なパスワードを組で管理しているため、著作権保護を必要とするコンテンツの格納を予約し、ダウンロードにより、視聴可能にするので、課金処理が不要になる利点を有する。また、その後の利用において、移動体機器向けに販売する場合であっても、市販用メモリカードと視聴用端末の組み合わせで正当性を認証でき、かつ、前記市販用メモリカードにコンテンツの暗号化とコピーガード機能を付加することにより、著作権を保護しつつ、販売後の譲渡に対して安全に流通させることができる。

【０１０７】

なお、上記実施形態では、リムーバブル記憶メディア１の正当性をメディア認証手段により認証し、かつこの正当なリムーバブル記憶メディア１と、閲覧・視聴端末装置２との組合せの正当性を組合せ認証手段により認証した場合に、リムーバブル記憶メディア１の暗号化コンテンツを復号化して閲覧・視聴できる場合について説明したが、本発明はこれに限定されるものではなく、例えばメディア認証手段によりリムーバブル記憶メディア１の正当性が認証されたときに、この正当なパスワードに関連付けられている複合キーとビューアを、サーバ１２０によりパスワード照合データベース１２１から読み出して閲覧・視聴端末装置２へ送信し、閲覧・視聴させるように構成してもよい。この場合は、リムーバブル記憶メディア１の正当性が認証のみで、閲覧・視聴端末装置２の正当性は認証されない。ただし、利用の都度、パスワードを入力して認証を確認することが必要である。

【０１０８】

また、コンテンツコードの欄をコンテンツグループにし、ダウンロード可能なコンテンツカテゴリを選択できる方式も可能になる。ただし、図示していないが、確定したコンテンツコードの記録項目やメニュー選択情報等の仕様が必要になる。更に、コンテンツの更新も可能とする技術を網羅すると、常に新鮮な情報やコンテンツ（日刊、週刊、月間等）の入手が可能になる。この技術は、地図情報、交通機関の最適経路選択サービス、カーナ

ビ情報の更新等に許可されたユーザのみに更新サービスを可能にする技術に拡張できる。

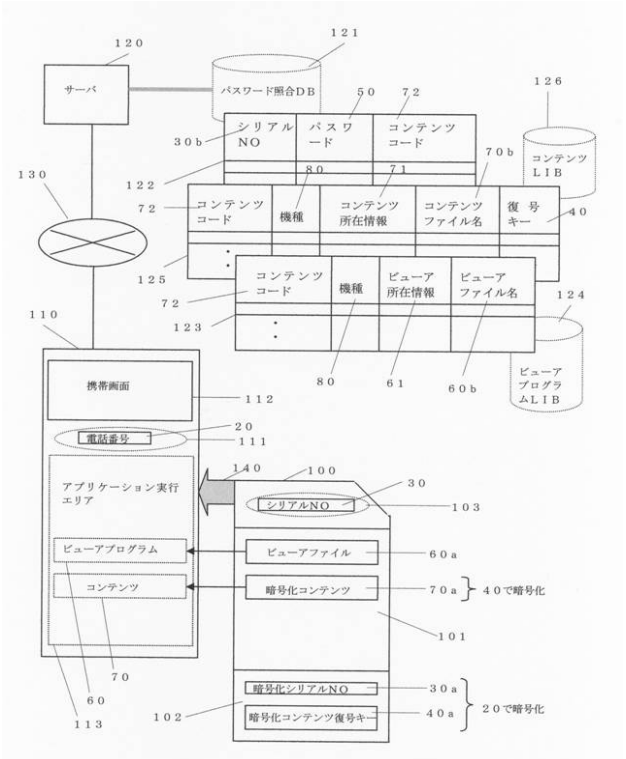
【符号の説明】

【０１０９】

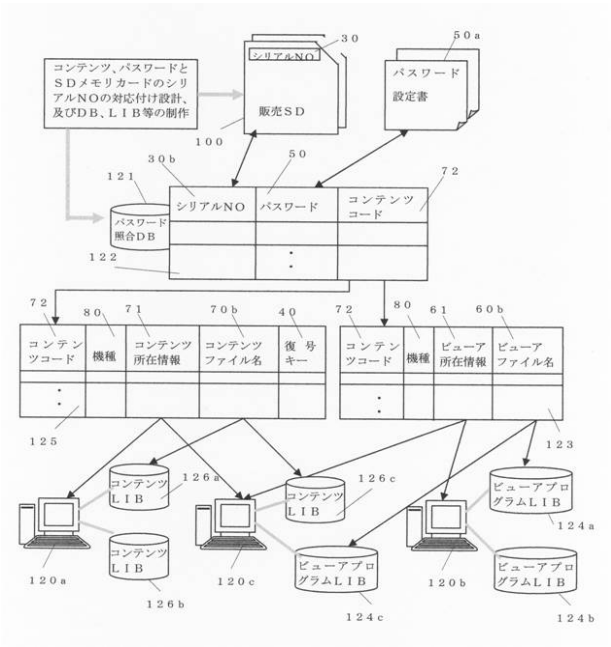
１　リムーバブル記憶メディア
２　閲覧・視聴端末装置
３　セットアップ情報供給装置
４　メモリカードインターフェイス
５　ＲＯＭ
６　ＲＡＭ
７　ＣＰＵ
８　内蔵不揮発メモリ
９　操作部
１０　ネットワークインターフェイス
１１　付属デバイスインターフェイス
１２　表示部
１３　バス
２０　電話番号
３０　シリアルＮＯ
３０ａ　暗号化シリアルＮＯ
３０ｂ　シリアルＮＯ
４０　コンテンツ復号キー
４０ａ　暗号化コンテンツ復号キー
５０　パスワード
５０ａ　パスワード設定書
６０　ビューアプログラム
６０ａ　ビューアファイル
６０ｂ　ビューアファイル名
６１　ビューア所在情報
７０　コンテンツ
７０ａ　暗号化コンテンツ
７０ｂ　コンテンツファイル名
７１　コンテンツ所在情報
７２　コンテンツコード
８０　機種
１００　ＳＤメモリカード
１０１　ユーザエリア
１０２　認証情報エリア
１０３　製造情報
１１０　携帯電話
１１１　アドレス情報
１１２　携帯画面
１１３　アプリケーション実行エリア
１２０　サーバ
１２０ａ、１２０ｂ、１２０ｃ　サーバ
１２１　パスワード照合ＤＢ
１２２　シリアルＮＯ情報レコード
１２３　ビューア情報レコード
１２４　ビューアプログラムライブラリ
１２４ａ、１２４ｂ、１２４ｃ　ビューアプログラムライブラリ
１２５　コンテンツ情報レコード

１２６　コンテンツライブラリ
１２６ａ、１２６ｂ、１２６ｃ　コンテンツライブラリ
１３０　ネットワーク
１３１　コンテンツ情報提供ネットワーク

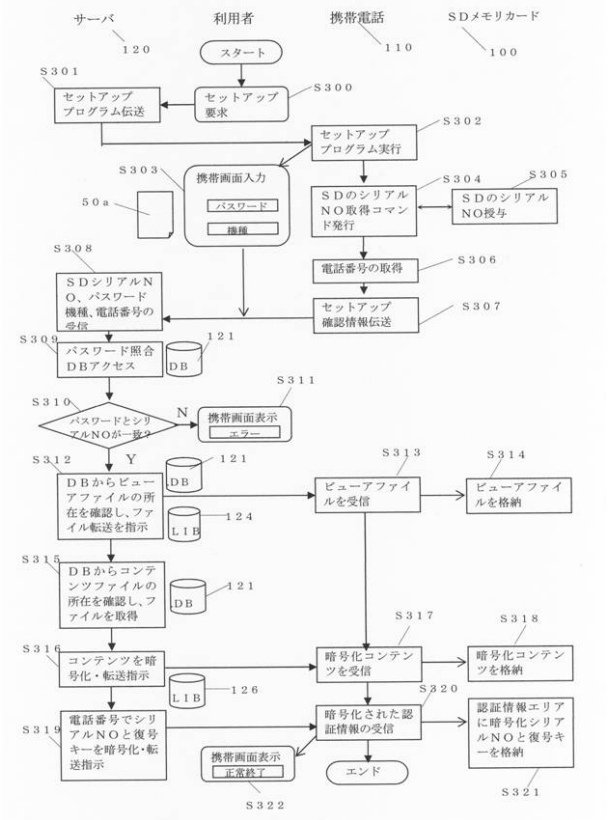
【図１】



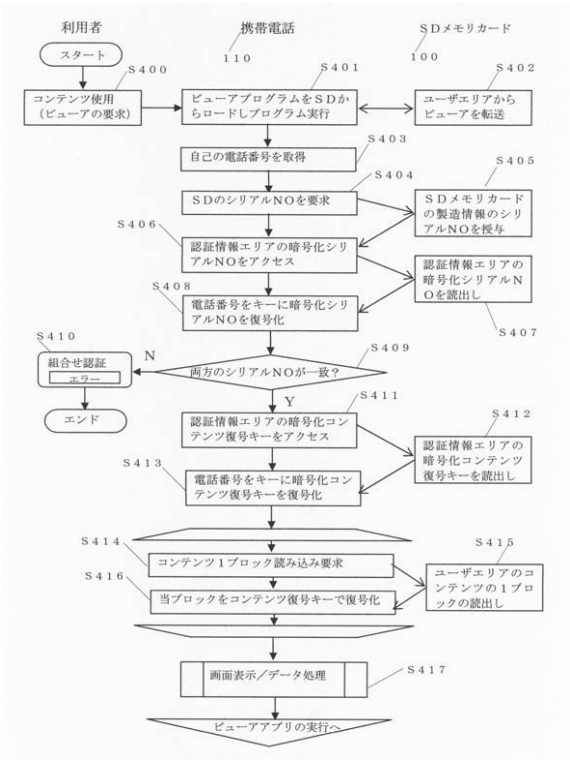
【図２】


コンテンツ、パスワードとSDメモリカードのシリアルNOの対応付け設計、及びDB、LIB等の制作
シリアルNO
販売SD
パスワード設定書
100
30
50a
30b
50
72
121
シリアルNO
パスワード
コンテンツコード
パスワード照合DB
122
コンテンツコード
機種
コンテンツ所在情報
コンテンツファイル名
復号キー
ビューア所在情報
ビューアファイル名
71
70b
40
61
60b
80
125
123
コンテンツLIB
126a
126c
ビューアプログラムLIB
124a
126b
124c
124b
120a
120c
120b

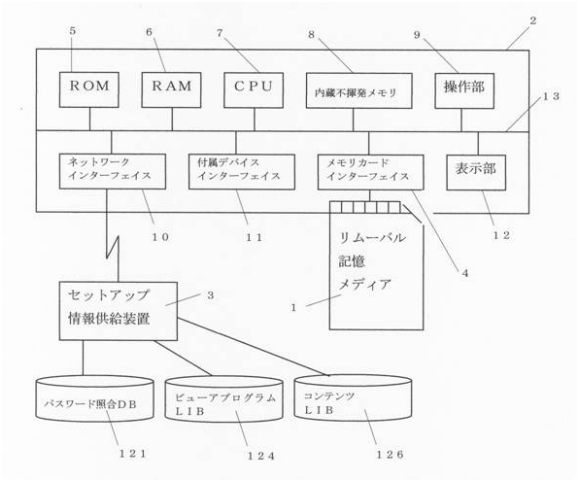
【図３】


サーバ
利用者
携帯電話
SDメモリカード
120
110
100
スタート
S301
セットアッププログラム伝送
セットアップ要求
S300
S302
セットアッププログラム実行
S303
携帯画面入力
パスワード
機種
50a
S304
SDのシリアルNO取得コマンド発行
S305
SDのシリアルNO授与
S306
電話番号の取得
S307
セットアップ確認情報伝送
S308
SDシリアルNO、パスワード機種、電話番号の受信
S309
パスワード照合DBアクセス
DB
121
S310
パスワードとシリアルNOが一致?
N
Y
S311
携帯画面表示
エラー
S312
DBからビューアファイルの所在を確認し、ファイル転送を指示
LIB
124
S313
ビューアファイルを受信
S314
ビューアファイルを格納
S315
DBからコンテンツファイルの所在を確認し、ファイルを取得
S316
コンテンツを暗号化・転送指示
126
S317
暗号化コンテンツを受信
S318
暗号化コンテンツを格納
S319
電話番号でシリアルNOと復号キーを暗号化・転送指示
S320
暗号化された認証情報の受信
認証情報エリアに暗号化シリアルNOと復号キーを格納
S321
携帯画面表示
正常終了
S322
エンド

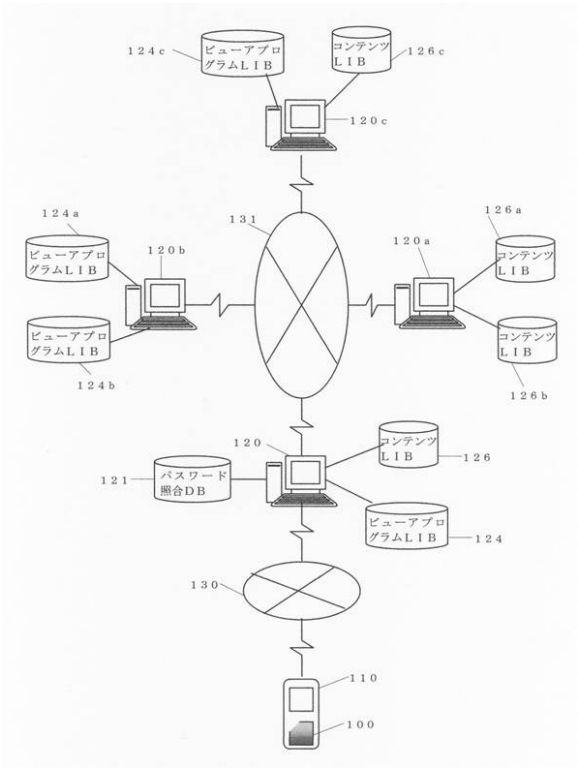
【図４】


利用者
携帯電話
SDメモリカード
スタート
110
100
S400
S401
S402
コンテンツ使用（ビューアの要求）
ビューアプログラムをSDからロードしプログラム実行
ユーザエリアからビューアを転送
S403
自己の電話番号を取得
S404
S405
SDのシリアルNOを要求
SDメモリカードの製造情報のシリアルNOを授与
S406
認証情報エリアの暗号化シリアルNOをアクセス
認証情報エリアの暗号化シリアルNOを読出し
S408
電話番号をキーに暗号化シリアルNOを復号化
S407
S410
N
S409
組合せ認証エラー
両方のシリアルNOが一致？
エンド
Y
S411
S412
認証情報エリアの暗号化コンテンツ復号キーをアクセス
認証情報エリアの暗号化コンテンツ復号キーを読出し
S413
電話番号をキーに暗号化コンテンツ復号キーを復号化
S414
S415
コンテンツ1ブロック読み込み要求
ユーザエリアのコンテンツの1ブロックの読出し
S416
当ブロックをコンテンツ復号キーで復号化
画面表示／データ処理
S417
ビューアアプリの実行へ

【図５】


5
6
7
8
9
2
ROM
RAM
CPU
内蔵不揮発メモリ
操作部
13
ネットワークインターフェイス
付属デバイスインターフェイス
メモリカードインターフェイス
表示部
10
11
12
リムーバル記憶メディア
4
1
セットアップ情報供給装置
3
パスワード照合DB
ビューアプログラムLIB
コンテンツLIB
121
124
126

【図６】


１２４ｃ
ビューアプログラムＬＩＢ
コンテンツＬＩＢ
１２６ｃ
１２０ｃ
１２４ａ
ビューアプログラムＬＩＢ
１２０ｂ
１３１
１２０ａ
１２６ａ
コンテンツＬＩＢ
ビューアプログラムＬＩＢ
１２４ｂ
コンテンツＬＩＢ
１２６ｂ
１２０
コンテンツＬＩＢ
１２６
１２１
パスワード照合ＤＢ
ビューアプログラムＬＩＢ
１２４
１３０
１１０
１００

フロントページの続き

(51)Int.Cl.	FI		テーマコード（参考）
	Ｇ０６Ｆ 9/06	６６０Ｆ	
	Ｈ０４Ｌ 9/00	６７３Ａ	