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

特許第4718560号
(P4718560)

(45)発行日　平成23年7月6日(2011.7.6)　(24)登録日　平成23年4月8日(2011.4.8)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520P
H04L 9/32	(2006.01)	G06F	12/14	540A
		G06F	12/14	560C
		H04L	9/00	675A

請求項の数 8　(全 17 頁)

(21)出願番号	特願2007-550312 (P2007-550312)
(86)(22)出願日	平成18年1月13日 (2006.1.13)
(65)公表番号	特表2008-527536 (P2008-527536A)
(43)公表日	平成20年7月24日 (2008.7.24)
(86)国際出願番号	PCT/KR2006/000157
(87)国際公開番号	WO2006/075899
(87)国際公開日	平成18年7月20日 (2006.7.20)
審査請求日	平成19年7月5日 (2007.7.5)
(31)優先権主張番号	60/643,150
(32)優先日	平成17年1月13日 (2005.1.13)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10-2005-0112554
(32)優先日	平成17年11月23日 (2005.11.23)
(33)優先権主張国	韓国(KR)

(73)特許権者　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国キョンギ－ド，スウォン－シ，ヨントン－ク，マエタン－ドン　４１６
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(72)発明者　オー，ユン－サン
大韓民国　１３５－８５５　ソウル　カンナム－グ　ドゴク・２－ドン　ゲポ・ハンシン・アパート　８－７０３（番地なし）

最終頁に続く

(54)【発明の名称】デジタル著作権管理装置及び方法

(57)【特許請求の範囲】

【請求項１】

所定のメタ情報を含む権利オブジェクトおよび前記メタ情報に対する所定のハッシュ値を格納する格納モジュールであって、前記メタ情報は少なくとも前記権利オブジェクトの使用可否を表す状態情報を含み、前記状態情報は、前記権利オブジェクトの使用可能を表す有効状態、前記権利オブジェクトの使用不可を表す無効状態、及び前記権利オブジェクトの使用可否が確認できない確認不可状態の３つの状態を取ることができる、格納モジュールと、

権利オブジェクト検出要請が入力される場合、前記格納モジュールに格納されている権利オブジェクトのメタ情報を提供する制御モジュールと、

メタ情報に含まれる状態情報を変更する状態情報更新モジュールと、

前記メタ情報についての無欠性をチェックする無欠性チェックモジュールとを有し、前記無欠性チェックモジュールは前記状態情報更新モジュールによって状態情報が変更された場合、変更されたメタ情報に対するハッシュ値を計算し、前記格納モジュールに既に格納されている前記権利オブジェクトのメタ情報に対するハッシュ値を前記計算されたハッシュ値に更新するよう構成されており、

前記状態情報更新モジュールは、前記状態情報が前記確認不可状態である場合、所定の時間情報と前記制限情報との比較によって前記権利オブジェクトの使用可否を判断し、前記判断の結果、前記権利オブジェクトが使用不可の場合、前記権利オブジェクトの状態情報を無効状態に変更するよう構成されている、

デジタル著作権管理装置。
【請求項２】
前記無欠性チェックモジュールは、所定のハッシュ関数を用いて、前記制御モジュールが提供するメタ情報に対するハッシュ値を計算し、前記計算したハッシュ値が前記格納モジュールに格納されたハッシュ値と同一であるかどうかを確認することによって前記メタ情報についての無欠性をチェックする
ことを特徴とする請求項１に記載のデジタル著作権管理装置。
【請求項３】
前記メタ情報はさらに、所定のコンテンツオブジェクトを再生するための前記権利オブジェクトの消費可能限度を表す制限情報、前記権利オブジェクトを通じて使用可能な前記コンテンツオブジェクトの再生方式を表す許可情報のうち少なくとも１つを含むことを特徴とする請求項１に記載のデジタル著作権管理装置。
【請求項４】
前記状態情報更新モジュールが、前記制限情報と前記権利オブジェクトの消費程度にしたがって前記状態情報を設定及び変更するよう構成されていることを特徴とする請求項１に記載のデジタル著作権管理装置。
【請求項５】
著作権管理装置によって実行される著作権管理方法であって、
権利オブジェクト検出要請が入力される場合、制御モジュールによって、所定の格納媒体に格納されている権利オブジェクトのメタ情報を提供するステップであって、前記格納媒体は前記メタ情報に対する所定のハッシュ値を格納しており、前記メタ情報は少なくとも前記権利オブジェクトの使用可否を表す状態情報を含み、前記状態情報は、前記権利オブジェクトの使用可能を表す有効状態、前記権利オブジェクトの使用不可を表す無効状態、及び前記権利オブジェクトの使用可否が確認できない確認不可状態の３つの状態を取ることができる、ステップと、
前記提供されるメタ情報についての無欠性を無欠性チェックモジュールによってチェックするステップと、
状態情報更新モジュールによって状態情報が変更された場合、前記無欠性チェックモジュールによって、変更されたメタ情報に対するハッシュ値を計算し、前記格納モジュールに既に格納されている前記権利オブジェクトのメタ情報に対するハッシュ値を前記計算されたハッシュ値に更新するステップとを含み、当該方法がさらに、
前記状態情報が前記確認不可状態である場合、
前記状態情報更新モジュールによって、所定の時間情報と前記制限情報との比較によって前記権利オブジェクトの使用可否を判断するステップと、
前記判断の結果、前記権利オブジェクトが使用不可の場合、前記状態情報更新モジュールによって、前記権利オブジェクトの状態情報を無効状態に変更するステップと、
をさらに含むことを特徴とするデジタル著作権管理方法。
【請求項６】
前記無欠性をチェックするステップは、所定のハッシュ関数を用いて前記メタ情報に対するハッシュ値を計算し、前記計算したハッシュ値が前記格納媒体に格納されたハッシュ値と同一であるかどうかを確認することによって前記メタ情報についての無欠性をチェックするステップを含む
ことを特徴とする請求項５に記載のデジタル著作権管理方法。
【請求項７】
前記メタ情報はさらに、所定のコンテンツオブジェクトを再生するための前記権利オブジェクトの消費可能限度を表す制限情報、前記権利オブジェクトを通じて使用可能な前記コンテンツオブジェクトの再生方式を表す許可情報のうち少なくとも１つを含むことを特徴とする請求項５に記載のデジタル著作権管理方法。
【請求項８】
前記状態情報更新モジュールによって、前記制限情報と前記権利オブジェクトの消費程

度にしたがって前記状態情報を変更するステップをさらに含むことを特徴とする請求項５に記載のデジタル著作権管理方法。

【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関し、より詳しくは、権利オブジェクトの情報を効率的に管理し得るデジタル著作権管理装置及び方法に関する。

【背景技術】

【０００２】

最近、デジタル著作権管理（以下、「ＤＲＭ」という）に関する研究が活発で、ＤＲＭを適用した常用サービスが導入されたり、導入されつつある。ＤＲＭは、容易に不正コピー及び配布できるデジタルコンテンツを保護するための技術概念である。

【０００３】

デジタルコンテンツを保護しようとする努力は従来にもあったが、それは主にデジタルコンテンツに対する不正アクセスの防止に重点を置いていた。例えば、デジタルコンテンツに対するアクセスは代価を払った人だけに許容され、代価を払わないユーザはデジタルコンテンツにアクセスできなかった。しかし、デジタルデータの特性上、デジタルコンテンツは、再使用、加工、コピー及び配布が容易であるため、代価を払ってデジタルコンテンツにアクセスしたユーザがこれを不正コピーまたは配布する場合には代価を払わないユーザもデジタルコンテンツを使用することができる。

【０００４】

このような問題点を克服するために、ＤＲＭは、デジタルコンテンツを暗号化して配布し、暗号化されたデジタルコンテンツを使用するためには、権利オブジェクト（ＲＯ）というライセンスが必要である。

【０００５】

図１に示すように、デバイス１０は、デジタルコンテンツをコンテンツ供給者２０から得ることができる。このとき、コンテンツ供給者２０が供給するデジタルコンテンツは暗号化された状態であり、暗号化されたデジタルコンテンツを使用するためには、権利オブジェクトが必要である。

【０００６】

デバイス１０は、権利オブジェクト発行機関３０から、暗号化されたデジタルコンテンツを使用できる権限が含まれた権利オブジェクトを得ることができるが、このために、ユーザは一定の代価を払わなければならない。権利オブジェクトは、暗号化されたデジタルコンテンツを復号化し得るキーを含む。

【０００７】

権利オブジェクト発行機関３０は、コンテンツ供給者２０に権利オブジェクト発行内訳を報告し、場合によっては権利オブジェクト発行機関３０とコンテンツ供給者２０が同一主体であり得る。

【０００８】

権利オブジェクトを得たデバイス１０は、権利オブジェクトを消費して、暗号化されたデジタルコンテンツを使用することができる。

【０００９】

一方、暗号化されたデジタルコンテンツは、他のデバイス（図示せず）にも自由にコピー及び配布できる。しかし、権利オブジェクトには、暗号化されたデジタルコンテンツの使用可能な回数や期間、権利オブジェクトのコピー許容回数といった制限情報が含まれているため、暗号化されたデジタルコンテンツとは違って、権利オブジェクトは、その再使用やコピーに制限がある。このようなＤＲＭ技術によればデジタルコンテンツを効果的に保護することができる。

【００１０】

上記のように、ＤＲＭにおいて権利オブジェクトが重要な役割するため、権利オブジェ

クトを格納しているデバイスは、外部装置のアクセスから権利オブジェクトを安全に保護しなければならない。このために、従来技術では、デバイスが所定のセキュリティ格納領域に権利オブジェクトを格納することによって権利オブジェクトをハードウェア的に保護するだけでなく、各種の暗号アルゴリズムを用いて権利オブジェクトを暗号化した状態で格納することによって権利オブジェクトをソフトウェア的にも保護している。

【発明の開示】

【発明が解決しようとする課題】

【００１１】

ところが、暗号化方式のソフトウェア的な保護方法は、結果的にデバイスのメモリに対する読み取り及び書き込み作業の速度を低下させる原因になる。例えば、従来技術によれば、ユーザがデバイスに格納されている権利オブジェクトに関する情報を検索しようとする場合、デバイスは、暗号化された権利オブジェクトを復号化し、復号化した権利オブジェクトから既に設定されている情報を抽出した後、抽出した情報を表示するため、ユーザの要求に対する応答速度が低下するという問題点がある。特に、コンテンツオブジェクトを再生し得る一般デバイスに比べて演算能力が低い携帯用格納装置に格納されている権利オブジェクトを検索しようとする場合、前記問題はさらに深刻になる。

【課題を解決するための手段】

【００１２】

本発明の目的は、権利オブジェクトに関する情報をより効果的に検索し得ることにある。

【００１３】

本発明の目的は以上で言及した目的に制限されず、言及していないさらなる目的は下記によって当業者に明確に理解できるものである。

【００１４】

前記目的を達成するための本発明のデジタル著作権管理装置は、所定のメタ情報を含む権利オブジェクトを格納する格納モジュール、権利オブジェクト検索要請が入力される場合、前記格納モジュールに格納されている権利オブジェクトのメタ情報を提供する制御モジュール、及び前記メタ情報についての無欠性を維持させる無欠性チェックモジュールを含む。

【００１５】

前記目的を達成するための本発明のデジタル著作権管理方法は、権利オブジェクト検索要請が入力される場合、所定の格納媒体に格納されている権利オブジェクトのメタ情報を提供するステップ、及び前記提供されるメタ情報についての無欠性を維持させるステップを含む。

【発明の効果】

【００１６】

本発明のデジタル著作権管理装置及び方法によれば、権利オブジェクトに関する情報をより効果的に検索し得る。

【発明を実施するための最良の形態】

【００１７】

本発明の利点及び特徴、そしてそれらを達成する方法は、添付する図面とともに詳述する実施形態を参照すれば明確になる。しかし、本発明は以下に開示する実施形態に限定されず、相異なる多様な形態で実現できる。本実施形態は、本発明の開示を完全なものにし、本発明の属する技術分野における通常の知識を有する者に発明の範疇を知らせるために提供するものであって、本発明は請求項の範疇によってのみ定義される。また、明細書全体において同じ参照符号は同じ構成要素を示す。

【００１８】

以下、添付する図面を参照して本発明の好ましい実施形態をより詳細に説明する。

【００１９】

まず、本発明で使っている用語について概略に説明をするが、これは、本発明の理解を

助けるものであって、本発明を限定するものではない。したがって、本発明の詳細な説明で特に限定しない限り、以下で説明する用語は、本発明の技術的思想を限定するものとして使っているのではないことに注意しなければならない。

【００２０】

ホストデバイス

ホストデバイスは、携帯用格納装置と連結可能で、権利オブジェクトを消費してコンテンツオブジェクトを再生し得る装置を意味する。ホストデバイスは、携帯電話、ＰＤＡ、ＭＰ３プレーヤといった携帯用コンテンツ再生装置、及びデスクトップコンピュータ、デジタルＴＶといった固定型コンテンツ再生装置であり得る。

【００２１】

携帯用格納装置

携帯用格納装置は、フラッシュメモリのように、データを読み取り、書き込み、削除することができる機能を有する非揮発性メモリを含み、データに対する所定の演算能力を有し、ホストデバイスと容易に連結／分離できる格納装置を意味する。携帯用格納装置は、例えばスマートメディア、メモリスティック、ＣＦカード、ＸＤカード、マルチメディアカードなどがある。

【００２２】

コンテンツオブジェクト

コンテンツオブジェクトは、暗号化された状態のデジタルコンテンツである。ここで、デジタルコンテンツは、動画、停止画、オーディオ、ゲーム、テキストなどその種類に制限されない。

【００２３】

権利オブジェクト（ＲＯ）

権利オブジェクトは、コンテンツオブジェクトの使用権限を有する一種のライセンスである。権利オブジェクトは、コンテンツ暗号化キー、許可情報、制限情報、状態情報、及びコンテンツ暗号化キーで再生し得るコンテンツオブジェクトを識別し得るコンテンツオブジェクト識別子を含む。

【００２４】

コンテンツ暗号化キー

コンテンツ暗号化キーは、コンテンツオブジェクトを再生し得るキーであり、所定の２進値の形態であり得る。例えば、コンテンツ暗号化キーはコンテンツオブジェクトを復号化してオリジナルコンテンツを得るのに用いられる。

【００２５】

許可情報

許可情報は、コンテンツオブジェクトの再生方式と権利オブジェクトのコピー方式を表す情報である。

【００２６】

再生方式は、例えば再生、ディスプレイ、実行、プリントなどがある。ここで、再生は、コンテンツオブジェクトをオーディオやビデオの形態で表現する権利を意味する。例えば、コンテンツオブジェクトが動画や音楽に関するものであれば、コンテンツオブジェクトを再生するために消費する権利オブジェクトの許可情報として再生が設定できる。また、ディスプレイは、コンテンツオブジェクトを視覚装置に表示し得る権利を意味し、プリントは、コンテンツオブジェクトのハードコピーを生成し得る権利を意味する。例えば、コンテンツオブジェクトが停止画に関するものであれば、コンテンツオブジェクトを再生するために消費する権利オブジェクトの許可情報としてディスプレイとプリントのうち少なくとも１つが設定できる。そして、実行は、ゲームや他のアプリケーションプログラム形式のコンテンツオブジェクトを使用し得る権利を意味する。例えば、コンテンツオブジェクトがＪａｖａ（登録商標）ゲームの場合、コンテンツオブジェクトを再生するために消費する権利オブジェクトの許可情報として実行が設定できる。

【００２７】

一方、コピー方式としては、例えばコピーと移動がある。コピーと移動は、あるデバイスが格納していた権利オブジェクトを他のデバイスに格納し得る権限である。移動の場合、他のデバイスに権利オブジェクトを格納すると、既存のデバイスに格納されていた権利オブジェクトが非活性化されるが、コピーの場合、他のデバイスに権利オブジェクトを格納しても、既存のデバイスに格納されていた権利オブジェクトは活性化状態のままである。ここで、非活性化は、権利オブジェクトの削除を意味することもある。

【００２８】

制限情報

制限情報は、コンテンツオブジェクトの再生可能限度を表す情報であって、許可情報のために１つ以上の制限情報が設定できる。制限情報は、例えば回数制限、日時制限、期間制限、累積時間制限などがある。

【００２９】

ここで回数制限は、コンテンツオブジェクトの再生可能回数を限定する。例えば、権利オブジェクトに対する回数制限が１０に設定されていれば、ホストデバイスは、権利オブジェクトを消費してコンテンツオブジェクトを１０回再生することができる。

【００３０】

日時制限は、コンテンツオブジェクトの再生可能日時を限定し、開始要素と終了要素のうち少なくとも１つを含むことができる。ホストデバイスは、日時制限が設定された権利オブジェクトを消費する場合、日時制限の開始要素が示す日時以後にコンテンツオブジェクトを再生することができ、終了要素が示す日時以前までコンテンツオブジェクトを再生することができる。例えば、権利オブジェクトに対する日時制限が開始要素として、２００５年１２月１日０時０分０秒に設定されていれば、ホストデバイスは、２００５年１２月１日０時０分０秒以後から権利オブジェクトを消費してコンテンツオブジェクトを再生することができる。

【００３１】

期間制限は、権利オブジェクトを消費してコンテンツオブジェクトを始めて再生した時点から、これから権利オブジェクトを消費してコンテンツオブジェクトを再生し得る期間を限定する。例えば、権利オブジェクトに対する制限情報として、期間制限が１週間に設定された場合、ホストデバイスが２００５年１２月１日０時０分０秒に権利オブジェクトを始めて消費してコンテンツオブジェクトを再生したとすれば、ホストデバイスは、２００５年１２月８日０時０分０秒まで権利オブジェクトを消費してコンテンツオブジェクトを再生することができる。

【００３２】

累積時間制限は、権利オブジェクトを消費してコンテンツオブジェクトを再生し得る時間の総和を限定する。例えば、権利オブジェクトに対して累積時間制限が１０時間に設定されていれば、ホストデバイスは、権利オブジェクトを消費して総１０時間コンテンツオブジェクトを再生することができる。このとき、ホストデバイスは、権利オブジェクトを消費してコンテンツオブジェクトを再生した回数や日付に関する制限はされない。

【００３３】

状態情報

権利オブジェクトは、制限情報が許容する範囲内で消費されるが、状態情報は、その制限情報に基づいて権利オブジェクトの使用可否を表す情報である。各権利オブジェクトの状態情報は、権利オブジェクトの使用可否を表す有効状態、権利オブジェクトの使用可否を表す無効状態、及び権利オブジェクトの使用可否が確認できない確認不可状態のいずれか１つの状態を含む。ここで、確認不可状態は、時間が経過するにつれて権利オブジェクトの使用可否が変更し得る場合に設定できる状態である。例えば、権利オブジェクトの制限情報として、日時制限や期間制限が設定されている場合、制限情報だけでは権利オブジェクトの使用可否を判断することができず、状態情報を確認しようとする時点の時間情報がさらに必要である。したがって、日時制限や期間制限が設定されている権利オブジェクトの状態情報は、確認不可状態に設定できる。

【００３４】
メタ情報
メタ情報は、権利オブジェクトに対するメタデータであって、許可情報、制限情報、及び状態情報のうち少なくとも１つを含む。
【００３５】
公開キー暗号化
非対称暗号化ともいい、データを暗号化するのに用いられるキーと、データを復号化するのに用いられるキーが異なるキーで構成される。公開キー暗号化方式でキーは、公開キーと個人キーの対からなる。公開キーは、秘密に保管する必要がなく一般に容易に公開され得るが、個人キーは、特定装置にだけ公開すべきである。公開キー暗号化アルゴリズムは、例えばＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ方式、ＲＳＡ方式、ＥｌＧａｍａｌ方式、及び楕円曲線方式などがある。
【００３６】
対称キー暗号化
秘密キー暗号化ともいい、データを暗号化するのに用いられるキーと、データを復号化するのに用いられるキーが同じキーで構成される。このような対称キー暗号化は、例えばＤＥＳ方式が最も一般に用いられ、最近にはＡＥＳ方式を採用したアプリケーションが増加している。
【００３７】
乱数
任意性を有する数字列、文字列、またはこれらの組み合わせを意味する。
【００３８】
モジュール
モジュールは、ソフトウェア、及びＦＰＧＡやＡＳＩＣといったハードウェアの構成要素を意味し、ある役割を行う。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意味ではない。モジュールは、アドレス指定可能な媒体に格納することができ、１つまたはそれ以上のプロセッサを実行し得るように構成することができる。したがって、モジュールは、例えばソフトウェアの構成要素、オブジェクト指向ソフトウェアの構成要素、クラスの構成要素、タスクの構成要素といった構成要素と、プロセス、関数、属性、プロシージャ、サブルーチン、プログラムコードのセグメント、ドライバ、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、変数を含むことができる。構成要素とモジュールにより提供される機能は、さらに小さい数の構成要素及びモジュールで結合されたり、さらなる構成要素とモジュールに分離され得る。
【００３９】
以上で説明していない用語について、以下では必要な部分で別に説明する。
【００４０】
図２は、本発明の一実施形態によるデジタル著作権管理装置１００を示すブロック図である。図示のデジタル著作権管理装置１００は、格納モジュール１１０、検索〔検出〕モジュール１２０、無欠性〔完全性〕チェックモジュール１３０、状態情報更新モジュール１４０、暗号化／復号化モジュール１５０、及び制御モジュール１６０を含む。
【００４１】
格納モジュール１１０は、フラッシュメモリのような格納媒体を含み、セキュリティ格納領域と一般格納領域とに区分できる。セキュリティ格納領域には、権利オブジェクト、権利オブジェクトのメタ情報に対するハッシュ値、及び所定の暗号キーなどの外部装置（図示せず）や外部モジュール（図示せず）のアクセスから保護する必要があるセキュリティデータが格納される。反面、一般格納領域には、コンテンツオブジェクトのように外部に公開されても差し支えない非セキュリティデータが格納される。セキュリティ格納領域に格納されるデータは、外部装置や外部モジュールによるアクセスから物理的または論理的に保護される。

【００４２】
格納モジュール１１０に格納された各権利オブジェクトはメタ情報を含むことができる。メタ情報は、権利オブジェクトにおいて固定フィールド（例えば、権利オブジェクトのａ番目のビットからｎ番目のビットまではメタ情報が記録されるフィールドとして予め定められる）に含まれるのが好ましい。この場合、権利オブジェクトの種類に関係なく、各権利オブジェクトの固定フィールドにアクセスすれば、各権利オブジェクトのメタ情報を得ることができる。
【００４３】
検索モジュール１２０は、権利オブジェクト検索要請が入力される場合、格納モジュール１１０に格納されている権利オブジェクトのメタ情報を検索する。権利オブジェクト検索要請は、外部装置や外部モジュールから入力され得る。
【００４４】
無欠性チェックモジュール１３０は、メタ情報についての無欠性を維持させる。すなわち、無欠性チェックモジュール１３０は、メタ情報（例えば、外部装置や外部モジュールがアクセスするメタ情報）についての無欠性をチェックすることによって、メタ情報の変更を防止することができる。例えば、無欠性チェックモジュール１３０は、所定のハッシュ関数を用いて、外部装置や外部モジュールがアクセスするメタ情報に対するハッシュ値を計算し、計算したハッシュ値を格納モジュール１１０に格納されたハッシュ値と比較することができる。２つのハッシュ値が同一であれば、無欠性チェックモジュール１３０は、メタ情報についての無欠性が維持されていると判断する。ここで、格納モジュール１１０に格納されたハッシュ値は、権利オブジェクトが格納モジュール１１０に格納されるとき、無欠性チェックモジュール１３０が権利オブジェクトのメタ情報に対して計算しておいたものであり得る。これにより、メタ情報は外部装置や外部モジュールに公開され得るが、外部装置や外部モジュールによって変更されることはない。
【００４５】
また、無欠性チェックモジュール１３０は、状態情報更新モジュール１４０によって任意のメタ情報に含まれた状態情報が変更されれば、状態情報が変更されたメタ情報に対するハッシュ値を計算し、計算したハッシュ値を格納モジュール１１０に格納しておく。これにより、状態情報が更新されたメタ情報に対して、既に格納モジュール１１０に格納していたハッシュ値は新しく計算されたハッシュ値に更新される。
【００４６】
状態情報更新モジュール１４０は、検索モジュール１２０が検索したメタ情報に含まれた状態情報が確認不可状態に設定されている場合、メタ情報検索時点の時間情報とメタ情報に含まれた制限情報とを比べて、権利オブジェクトの使用可否を判断することができる。例えば、メタ情報に含まれた制限情報として、期間制限の終了要素が２００５年１１月１日０時０分０秒に設定されており、メタ情報検索時点の時間情報が２００５年１１月２日０時０分０秒であれば、権利オブジェクトは使用不可状態と判断される。メタ情報検索時点の時間情報は外部装置や外部モジュールから得ることができる。
【００４７】
判断結果、権利オブジェクトが使用可能であれば、状態情報更新モジュール１４０は、メタ情報に含まれた状態情報を確認不可状態に維持させる。しかし、判断結果、権利オブジェクトが使用不可であれば、状態情報更新モジュール１４０は、メタ情報に含まれた状態情報を無効状態に変更する。
【００４８】
また、状態情報更新モジュール１４０は、有効状態の権利オブジェクトが全部消費されて、それ以上権利オブジェクトを使用できない場合、該当権利オブジェクトのメタ情報に含まれた状態情報を無効状態に変更する。
【００４９】
暗号化／復号化モジュール１５０は、所定のデータに対する暗号化及び復号化を行うモジュールであって、制御モジュール１６０の要請に応じて外部装置や外部モジュールに伝

送するデータを暗号化したり、外部装置や外部モジュールから暗号化されて受信されたデータを復号化することができる。暗号化／復号化モジュール１５０は、公開キー暗号化方式だけでなく、秘密キー暗号化方式も行うことができ、２つの方式を各々行うための１つ以上の暗号化／復号化モジュールが存在することも可能である。また、暗号化／復号化モジュール１５０は、外部装置や外部モジュールとの相互認証過程時に必要な所定の乱数を生成することもできる。一方、格納モジュール１１０に格納される各権利オブジェクトは、メタ情報を除く部分が暗号化／復号化モジュール１５０によってデジタル著作権管理装置１００が有する固有の暗号キーで暗号化された状態であり得る。権利オブジェクトのうち暗号化される部分として、コンテンツ暗号化キーがある。したがって、権利オブジェクトを外部装置や外部モジュールに提供する必要がある場合、暗号化／復号化モジュール１５０は権利オブジェクトの暗号化された部分を復号化した後、権利オブジェクトの提供対象となる外部装置や外部モジュールが復号化し得る方式で権利オブジェクトをまた暗号化することができる。

【００５０】

制御モジュール１６０は、デジタル著作権管理装置を構成する各モジュール１１０ないし１５０の動作を制御する。したがって、制御モジュール１６０は、デジタル著作権管理装置のＤＲＭ作業を総括するＤＲＭエージェントとして機能し得る。また、制御モジュール１６０は、外部装置や外部モジュールとの相互認証過程を制御することができる。

【００５１】

一方、制御モジュール１６０は、検索モジュール１２０が検索したメタ情報を外部装置や外部モジュールに提供することができる。本発明において、「メタ情報を提供する」とは、権利オブジェクト検索を要請した外部装置や外部モジュールにメタ情報を能動的に伝送する意味だけでなく、権利オブジェクト検索を要請した外部装置や外部モジュールが権利オブジェクトのメタ情報にアクセスするのを許可する意味でもある。

【００５２】

以下図３を参照して、上述したデジタル著作権管理装置１００の動作過程について説明する。

【００５３】

図３は、本発明の一実施形態によるデジタル著作権管理方法を示すフローチャートである。

まず、外部装置や外部モジュールから権利オブジェクト検索要請が入力されると（Ｓ４１０）、検索モジュール１２０は格納モジュール１１０に格納されている権利オブジェクトのメタ情報を検索する（Ｓ４１５）。

【００５４】

もし、メタ情報に状態情報が含まれていれば、状態情報更新モジュール１４０は、状態情報が確認不可状態に設定されているか確認する（Ｓ４２０）。

【００５５】

確認結果、状態情報が確認不可状態でなければ（例えば、状態情報が有効状態であるか、または無効状態である場合）、制御モジュール１６０は検索されたメタ情報を外部装置や外部モジュールに提供する（Ｓ４５０）。

【００５６】

一方、過程Ｓ４２０での確認結果、状態情報が確認不可状態である場合、状態情報更新モジュール１４０は、メタ情報検索時の時間情報とメタ情報に含まれた制限情報とを比べて、メタ情報を含む権利オブジェクトの使用可否を判断する（Ｓ４２５）。

【００５７】

判断結果、権利オブジェクトが使用可能であれば、状態情報更新モジュール１４０はメタ情報に含まれた状態情報を確認不可状態に維持させ（Ｓ４４５）、制御モジュール１６０はメタ情報を提供する（Ｓ４５０）。

【００５８】

しかし、過程Ｓ４２５での判断結果、権利オブジェクトが使用不可であれば、状態情報

更新モジュール１４０は、メタ情報に含まれた状態情報を無効状態に変更する（Ｓ４３０）。このとき、無欠性チェックモジュール１３０は、所定のハッシュ関数を用いて、状態情報が変更されたメタ情報に対するハッシュ値を計算する（Ｓ４３５）。その後、無欠性チェックモジュール１３０は、計算されたハッシュ値を格納モジュール１１０に格納する（Ｓ４４０）。すなわち、無欠性チェックモジュール１３０は、格納モジュール１１０に格納されたハッシュ値のうち状態情報が変更されたメタ情報に対する既存のハッシュ値を過程Ｓ４３５で計算したハッシュ値に変える。その後、制御モジュール１６０は変更された状態情報を含むメタ情報を提供する（Ｓ４５０）。

【００５９】

もし、格納モジュール１１０に残余権利オブジェクトがあれば（Ｓ４５５）、検索モジュール１２０は残余権利オブジェクトのメタ情報を検索する（Ｓ４１５）。

【００６０】

したがって、上記過程は格納モジュール１１０に格納されている全ての権利オブジェクトのメタ情報が全部検索されるまで繰り返される。

【００６１】

一方、図３の過程中に、無欠性チェックモジュール１３０は外部装置や外部モジュールによってメタ情報が変更されないようにし、この過程を図４に示した。

【００６２】

制御モジュール１６０がメタ情報を提供し（Ｓ５１０）、外部装置や外部モジュールがメタ情報にアクセスすると（Ｓ５２０）、無欠性チェックモジュール１３０は外部装置や外部モジュールによってアクセスされるメタ情報の無欠性を維持させる（Ｓ５３０）。例えば、無欠性チェックモジュール１３０は、所定のハッシュ関数を用いて、外部装置や外部モジュールによってアクセスされるメタ情報のハッシュ値を計算し、計算したハッシュ値が格納モジュール１１０に格納されたハッシュ値と同一値を有するように強制することによって、メタ情報の不正変更を防止することができる。

【００６３】

図２ないし図４に示すデジタル著作権管理装置１００は、多様な形態のデバイスによって実現することができる。例えば、デジタル著作権管理装置１００は、ホストデバイスによって実現でき、これを図５に示した。

【００６４】

図５は、本発明の一実施形態によるホストデバイスを示すブロック図である。

図示のホストデバイス２００は上記デジタル著作権管理装置１００を含む。すなわち、ホストデバイス２００の格納モジュール２１０、検索モジュール２２０、無欠性チェックモジュール２３０、状態情報更新モジュール２４０、暗号化／復号化モジュール２５０、及び制御モジュール２６０は、各々デジタル著作権管理装置１００の格納モジュール１１０、検索モジュール１２０、無欠性チェックモジュール１３０、状態情報更新モジュール１４０、暗号化／復号化モジュール１５０、及び制御モジュール１６０と同じ機能を行うことができる。したがって、ホストデバイス２００の格納モジュール２１０、検索モジュール２２０、無欠性チェックモジュール２３０、状態情報更新モジュール２４０、暗号化／復号化モジュール２５０、及び制御モジュール２６０についての説明は省略する。

【００６５】

また、ホストデバイスは、ユーザ入力モジュール２１５、デバイスインターフェースモジュール２２５、再生モジュール２３５、ディスプレイモジュール２４５、及び時間管理モジュール２５５をさらに含む。

【００６６】

ユーザ入力モジュール２１５はユーザから所定のコマンドや要請を受信する。このために、ユーザ入力モジュール２１５は、キーパッド、タッチパッド、タッチスクリーンといった入力手段を含むことができる。したがって、ユーザはユーザ入力モジュール２１５を通じて格納モジュール２１０に格納されている権利オブジェクトの検索を要請することができ、権利オブジェクト検索要請が入力された場合、図３及び図４に示す作業が行われる

。
【００６７】
デバイスインターフェースモジュール２２５は、外部装置（例えば、携帯用格納装置）にデータを送信したり、外部装置からデータを受信する。したがって、ホストデバイス２００は、デバイスインターフェースモジュール２２５を介して外部装置と連結できる。
【００６８】
再生モジュール２３５は、権利オブジェクトを使用してコンテンツオブジェクトを再生する。例えば、再生モジュール２３５は動画デコードモジュールを含むことができ、ＭＰＥＧ形式に圧縮された動画データで構成されるコンテンツオブジェクトを再生することができる。
【００６９】
ディスプレイモジュール２４５は、再生モジュール２３５によって再生されるコンテンツオブジェクトを表示したり、制御モジュール２６０によって提供されるメタ情報を表示する。したがって、ユーザはディスプレイモジュール２４５を通じて格納モジュール２１０に格納されている権利オブジェクトのメタ情報を確認することができる。ディスプレイモジュール２４５は、ＰＤＰ、ＬＣＤ、有機ＥＬといったディスプレイパネルによって実現できる。
【００７０】
時間管理モジュール２５５は現在の時間情報を管理する。
このような構造を有するホストデバイス２００がホストデバイス２００に格納されている権利オブジェクトを検索する動作過程は、図３及び図４によって理解し得る。
【００７１】
このとき、図３の過程Ｓ４２５に示す、状態情報が確認不可状態である権利オブジェクトの使用可否を確認する作業で必要な時間情報は、時間管理モジュール２５５から提供され得る。また、図３の過程Ｓ４５０で提供されるメタ情報はディスプレイモジュール２４５を通じて表示できる。
【００７２】
本発明の他の実施形態として、ユーザはホストデバイス２００の外に、携帯用格納装置に権利オブジェクトを格納しておくことができ、ホストデバイス２００を使用して携帯用格納装置に格納されている権利オブジェクトを消費したり、携帯用格納装置に格納されている権利オブジェクトを検索することができる。このとき、図２に示したデジタル著作権管理装置１００は、携帯用格納装置によっても実現できる。図６を参照して携帯用格納装置を使用するＤＲＭシステムについて説明し、図７を参照して携帯用格納装置の構成について説明する。
【００７３】
図６は、本発明の一実施形態によるＤＲＭシステムを示す図面である。図示のＤＲＭシステムはホストデバイス２００と携帯用格納装置３００を含む。
【００７４】
ユーザは、ホストデバイス２００を通じて従来のようにコンテンツ供給者２０からコンテンツオブジェクトを得たり、一定の代価を払って権利オブジェクト発行機関３０から権利オブジェクトを購入することができる。購入した権利オブジェクトはホストデバイス２００に格納しておくことができるが、ホストデバイス２００に格納した権利オブジェクトを携帯用格納装置３００に移動またはコピーしておくこともできる。この他にも、携帯用格納装置３００はその生産時から１つ以上の権利オブジェクトを格納していることができる。
【００７５】
携帯用格納装置３００が権利オブジェクトを格納している場合、ホストデバイス２００は、携帯用格納装置３００と連結された後、携帯用格納装置３００に格納されている権利オブジェクトを消費してコンテンツオブジェクトを再生することができる。ここで、ホストデバイス２００は図５に示したような構造及び機能を行うことができる。

【００７６】
図７は、本発明の一実施形態による携帯用格納装置３００を示すブロック図である。図示の携帯用格納装置３００は、上述したデジタル著作権管理装置１００を含む。すなわち、携帯用格納装置３００の格納モジュール３１０、検索モジュール３２０、無欠性チェックモジュール３３０、状態情報更新モジュール３４０、暗号化／復号化モジュール３５０、及び制御モジュール３６０は、各々デジタル著作権管理装置１００の格納モジュール１１０、検索モジュール１２０、無欠性チェックモジュール１３０、状態情報更新モジュール１５０、暗号化／復号化モジュール１５０、及び制御モジュール１６０と同じ機能を行うことができる。したがって、携帯用格納装置３００の格納モジュール３１０、検索モジュール３２０、無欠性チェックモジュール３３０、状態情報更新モジュール３４０、暗号化／復号化モジュール３５０、及び制御モジュール３６０についての説明は省略する。また、携帯用格納装置３００はデバイスインターフェースモジュール３７０をさらに含む。

【００７７】
デバイスインターフェースモジュール３７０は、外部装置（例えば、ホストデバイス２００）にデータを送信したり、外部装置からデータを受信する。したがって、携帯用格納装置３００はデバイスインターフェースモジュール３７０を介して外部装置と連結できる。

【００７８】
このような携帯用格納装置３００に格納されている権利オブジェクトを検索するために、ホストデバイス２００と携帯用格納装置３００を連結する場合、ホストデバイス２００と携帯用格納装置３００は相互認証を行うのが好ましい。相互認証は、ホストデバイス２００と携帯用格納装置３００が各々互いが正当な装置であることを確認し、互いに交換されるデータのセキュリティを維持するための基礎過程である。これを図８を参照して説明する。

【００７９】
図８は、本発明の一実施形態による相互認証過程を示すフローチャートである。本実施形態における下添字の「Ｈ」は、ホストデバイス２００が有しているか、またはホストデバイス２００が生成したデータを意味し、下添字の「Ｓ」は、携帯用格納装置３００が有しているか、または携帯用格納装置３００が生成したデータを意味する。

【００８０】
まず、ホストデバイス２００と携帯用格納装置３００が連結されれば、ホストデバイス２００は携帯用格納装置３００に相互認証を要請する（Ｓ６１０）。このとき、ホストデバイス２００は認証機関（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）がホストデバイス２００に対して発行した認証書$_H$をともに伝送することができる。認証書$_H$はホストデバイス２００のＩＤ$_H$と公開キー$_H$を含み、認証機関によって電子署名されている。また、ホストデバイス２００が携帯用格納装置３００と連結されるということは、ホストデバイス２００と携帯用格納装置３００が有線媒体を介して電気的に接触することを意味するが、これは例示的なものに過ぎず、ホストデバイス２００と携帯用格納装置３００が接触しない状態で無線媒体を介して互いに通信できる状態にあることも意味する。

【００８１】
ホストデバイス２００の認証書$_H$を受信した携帯用格納装置２００は、認証書廃棄リスト（以下、「ＣＲＬ」という）を用いて認証書$_H$が有効なのかを確認する（Ｓ６１２）。もし、ホストデバイス２００の認証書$_H$がＣＲＬに登録されている認証書であれば、携帯用格納装置３００はホストデバイス２００との相互認証を拒否することができる。しかし、ホストデバイス２００の認証書$_H$がＣＲＬに登録されていない認証書であれば、携帯用格納装置３００は認証書$_H$を通じてホストデバイス２００の公開キー$_H$を得ることができる。

【００８２】
認証書$_H$確認によってホストデバイス２００が正当な装置であると判断されれば、携帯

用格納装置３００は乱数$_S$を生成し（Ｓ６１４）、生成した乱数$_S$をホストデバイス２００の公開キー$_H$で暗号化する（Ｓ６１６）。

【００８３】

その後、携帯用格納装置３００は相互認証応答を行う（Ｓ６２０）。相互認証応答時に携帯用格納装置３００は、認証機関が携帯用格納装置３００に対して発行した認証書$_S$及び暗号化された乱数$_S$をともに伝送する。認証書$_S$は携帯用格納装置３００のＩＤ$_S$と公開キー$_S$を含み、認証機関によって電子署名されている。

【００８４】

携帯用格納装置３００から認証書$_S$及び暗号化された乱数$_S$を受信したホストデバイス２００は、認証書$_S$を通じて携帯用格納装置３００が正当な装置であることを確認し、暗号化された乱数$_S$をホストデバイス２００の個人キー$_H$で復号化する（Ｓ６２２）。このとき、ホストデバイス２００は、携帯用格納装置３００の認証書$_S$を通じて携帯用格納装置３００の公開キー$_S$を得ることができる。また、認証書$_S$確認作業は携帯用格納装置３００と同様にＣＲＬを通じて行うことができる。

【００８５】

認証書$_S$確認によって携帯用格納装置３００が正当な装置であると判断されれば、ホストデバイス２００は乱数$_H$を生成し（Ｓ６２４）、生成された乱数$_H$を携帯用格納装置３００の公開キー$_S$で暗号化する（Ｓ６２６）。

【００８６】

その後、ホストデバイス２００は、携帯用格納装置３００に相互認証終了を要請する（Ｓ６３０）。相互認証終了の要請時にホストデバイス２００は暗号化された乱数$_H$をともに伝送する。

【００８７】

ホストデバイス２００から暗号化された乱数$_H$を受信した携帯用格納装置３００は、自身の個人キー$_S$で暗号化された乱数$_H$を復号化する（Ｓ６３２）。

【００８８】

これにより、ホストデバイス２００と携帯用格納装置３００は、互いに２つの乱数（乱数$_H$及び乱数$_S$）を共有する。

【００８９】

相互認証結果、２つの乱数（乱数$_H$及び乱数$_S$）を共有したホストデバイス２００と携帯用格納装置３００は、２つの乱数（乱数$_H$及び乱数$_S$）を用いてセッションキーを生成する（Ｓ６４０、Ｓ６４２）。このとき、ホストデバイス２００と携帯用格納装置３００がセッションキーを生成するために使用するキー生成アルゴリズムは互いに同一である。したがって、ホストデバイス２００と携帯用格納装置３００は互いに同じセッションキーを共有する。

【００９０】

ホストデバイス２００と携帯用格納装置３００は、相互認証後、互いに伝送するデータをセッションキーで暗号化し、互いから受信して暗号化したデータをセッションキーで復号化する。これにより、ホストデバイス２００と携帯用格納装置３００との間のデータ伝送にセキュリティが維持できる。以下の各実施形態で特に言及しなくても、ホストデバイス２００と携帯用格納装置３００は、互いに送信するデータを相互認証結果により生成したセッションキーで暗号化し、互いから受信して暗号化したデータをセッションキーで復号化すると理解することができる。

【００９１】

相互認証を終了すれば、ホストデバイス２００は携帯用格納装置３００に権利オブジェクトを移動またはコピーしたり、携帯用格納装置３００に格納されている権利オブジェクトを消費してコンテンツオブジェクトを再生することができる。

【００９２】

また、本発明の一実施形態によって、ホストデバイス２００は携帯用格納装置３００に格納されている権利オブジェクトに対する検索を要請することができ、これを図９を参照

して説明する。

【００９３】

図９は、本発明の一実施形態による携帯用格納装置３００に格納されている権利オブジェクトの検索過程を示すフローチャートである。

【００９４】

まず、ホストデバイス２００のユーザ入力モジュール２１５がユーザから携帯用格納装置３００に格納されている権利オブジェクトに対する検索要請を受信すれば（Ｓ７１０）、制御モジュール２６０はデバイスインターフェースモジュール２４５を通じて携帯用格納装置３００に権利オブジェクト検索を要請する（Ｓ７２０）。このとき、制御モジュール２６０は権利オブジェクト検索要請メッセージを生成し、デバイスインターフェースモジュール２４５が権利オブジェクト検索要請メッセージを携帯用格納装置３００に伝送することができる。

【００９５】

携帯用格納装置３００のデバイスインターフェースモジュール３７０がホストデバイス２００から権利オブジェクト検索要請を受信すれば、検索モジュール３２０は格納モジュール３１０に格納されている権利オブジェクトのメタ情報を検索する（Ｓ７３０）。

【００９６】

その後、制御モジュール３６０は、検索されたメタ情報をデバイスインターフェースモジュール３７０を介してホストデバイス２００に提供する（Ｓ７４０）。ここで、ホストデバイス２００にメタ情報を提供する前に、携帯用格納装置２００は図３の過程Ｓ４２０ないしＳ４４５を行うことができる。このとき、過程Ｓ４２５で必要な時間情報はホストデバイス２００から得ることができる。

【００９７】

一方、ホストデバイス２００にメタ情報を提供することは、携帯用格納装置３００がデバイスインターフェースモジュール３７０を介してホストデバイス２００にメタ情報を能動的に伝送する場合だけでなく、ホストデバイス２００がメタ情報にアクセスできるように許可する場合も含む。

【００９８】

ホストデバイス２００のデバイスインターフェースモジュール２２５が携帯用格納装置３００からメタ情報を得れば、ディスプレイモジュール２４５はメタ情報を表示する（Ｓ７５０）。

【００９９】

このとき、ユーザがユーザ入力モジュール２４０を通じて携帯用格納装置３００に格納されている権利オブジェクトのメタ情報を変更しようとすれば、携帯用格納装置３００の無欠性チェックモジュール３３０の無欠性チェック作業によってメタ情報の変更が拒否できる。

【０１００】

以上、添付する図面を参照して本発明の実施形態を説明したが、本発明の属する技術分野における通常の知識を有する者は本発明がその技術的思想や必須的な特徴を変更せずに他の具体的な形態によって実施できることを理解することができる。したがって前述した実施形態はすべての面で例示的なものであって、限定的なものではないことを理解しなければならない。

【図面の簡単な説明】

【０１０１】

【図１】従来技術によるＤＲＭ概念を示す図である。

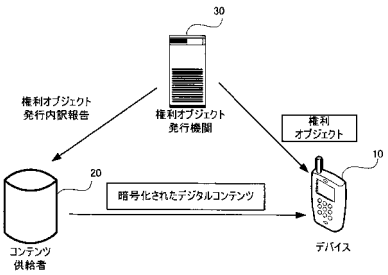
【図２】本発明の一実施形態によるデジタル著作権管理装置を示すブロック図である。

【図３】本発明の一実施形態によるデジタル著作権管理方法を示すフローチャートである。

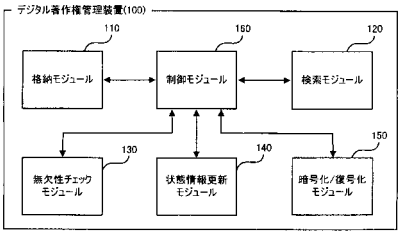
【図４】本発明の一実施形態によるメタ情報の無欠性維持過程を示すフローチャートである。

【図５】本発明の一実施形態によるホストデバイスを示すブロック図である。
【図６】本発明の一実施形態によるＤＲＭシステムを示す図である。
【図７】本発明の一実施形態による携帯用格納装置を示すブロック図である。
【図８】本発明の一実施形態による相互認証過程を示すフローチャートである。
【図９】本発明の一実施形態による携帯用格納装置に格納されている権利オブジェクトの検索過程を示すフローチャートである。

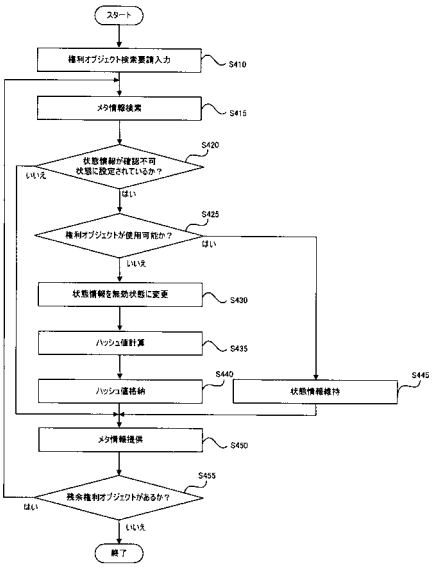
【図１】



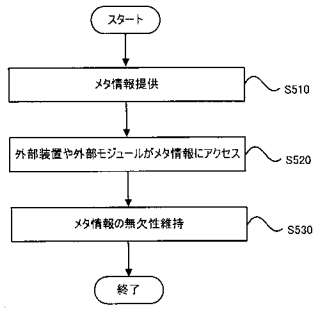
【図２】



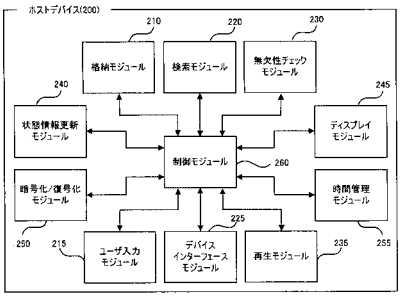
【図３】



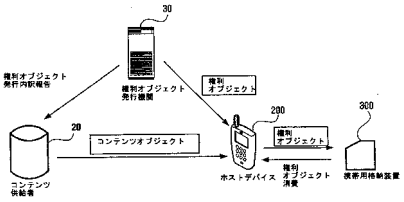
【図４】



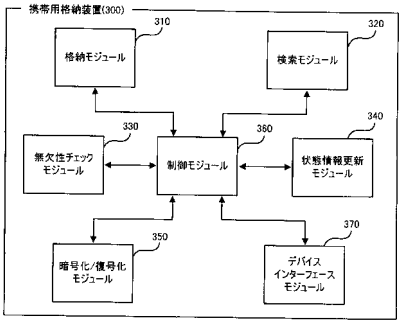
【図５】



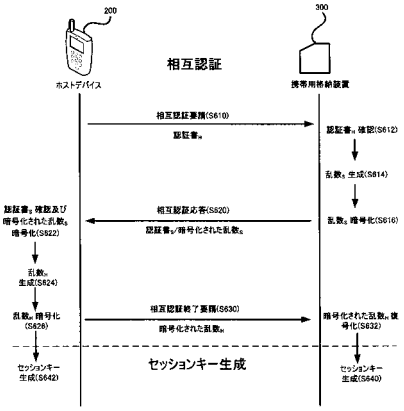
【図６】



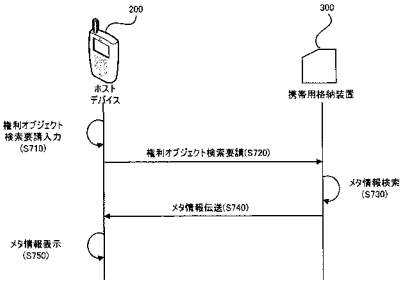
【図７】



【図８】



【図９】



フロントページの続き

(72)発明者 ジョン，ギョンーイム
大韓民国 ４６３－７２８ キョンギード ソンナムーシ ブンダンーグ スネードン パーク・タウン・ロッテ・アパート １２８－９０３（番地なし）
(72)発明者 シム，サンーギュ
大韓民国 １３５－８６０ ソウル カンナムーグ ドゴク・１－ドン ９５１－９ キャスル・ヴィラ ２０３ エー
(72)発明者 リ，ソックーボン
大韓民国 ４４３－４７０ キョンギード スウォンーシ ヨントンーグ ヨントンードン ９９２－１０ ２０５

審査官 和田 財太

(56)参考文献 特開２００３－３４５６６０（ＪＰ，Ａ）
特開２００３－３３１１３９（ＪＰ，Ａ）
特開２００３－２７２２８９（ＪＰ，Ａ）
特開２０００－３０６３２８（ＪＰ，Ａ）
特開２００１－０７５８６８（ＪＰ，Ａ）
特開２００３－３０８２４９（ＪＰ，Ａ）
特開２００２－３４２５１８（ＪＰ，Ａ）
特開２００４－３１２７１７（ＪＰ，Ａ）
米国特許出願公開第２００５／００２２０２５（ＵＳ，Ａ１）
米国特許出願公開第２００３／０００９４２３（ＵＳ，Ａ１）
特開２００５－０８５１１３（ＪＰ，Ａ）
特開２００５－３３９１７１（ＪＰ，Ａ）
特開２００５－０６３０２８（ＪＰ，Ａ）
特開２００１－１８４２６４（ＪＰ，Ａ）
特開２００５－１３５０６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
H04L 9/32