(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4406190号
(P4406190)
(45)発行日　平成22年1月27日(2010.1.27)　(24)登録日　平成21年11月13日(2009.11.13)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14 560A

請求項の数 14 (全 53 頁)

(21)出願番号　特願2002-186968(P2002-186968)
(22)出願日　平成14年6月26日(2002.6.26)
(65)公開番号　特開2003-122636(P2003-122636A)
(43)公開日　平成15年4月25日(2003.4.25)
審査請求日　平成17年6月17日(2005.6.17)
(31)優先権主張番号　09/892,298
(32)優先日　平成13年6月27日(2001.6.27)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(74)復代理人　100115624
弁理士　濱中　淳宏
(74)復代理人　100156971
弁理士　稲　綾子

最終頁に続く

(54)【発明の名称】デジタル権管理（ＤＲＭ）システムを有するコンピューティングデバイスのセキュアビデオカード

(57)【特許請求の範囲】
【請求項１】
コンピューティングデバイス上で保護されたデジタルコンテンツのレンダリングを可能にするためのデジタル権管理（ＤＲＭ）システムを含むコンピューティングデバイスであって、
前記コンテンツは前記コンピューティングデバイスに結合されたモニタ上で表示されるビデオコンテンツを含み、前記コンピューティングデバイスはさらに、
前記コンテンツを受信し、当該受信したコンテンツに基づいて前記モニタに送信されるビデオ信号を生成するビデオカードであって、前記受信したコンテンツを格納するための、前記ビデオカードの外部の任意のエンティティに対して書込み専用となるように構成されたビデオメモリと、前記ビデオカードの外部の任意のエンティティに対して前記ビデオメモリが書込み専用となるように構成されていることを前記ＤＲＭシステムに対して認証する認証デバイスとを含む、ビデオカードを備え、
前記ビデオメモリは、前記ＤＲＭシステムによってレンダリングできるように、権利保護されたデジタルコンテンツのみに対して書込み専用となるように構成され、
前記認証デバイスは、前記ＤＲＭシステムに提示されるトークンであって、前記ビデオカードの製造において、当該ビデオカード内のビデオメモリを前記ビデオカードの外部の任意のエンティティに対して書込み専用となるように構成するという条件が合意された場合に当該認証デバイスに与えられるトークンを含み、
前記ＤＲＭシステムは、前記提示されたトークンに基づいて前記ビデオカードを信用す

るかどうかを決定し、信用できる場合は前記ビデオカードの前記ビデオメモリを前記ビデオカードに対して読取り可能にすることを特徴とする、コンピューティングデバイス。

【請求項２】

前記ビデオカードの外部の任意のエンティティは、前記ビデオメモリに格納された前記受信したコンテンツを読み取ることができないことを特徴とする請求項１に記載のコンピューティングデバイス。

【請求項３】

前記ビデオメモリはビデオＲＡＭであることを特徴とする請求項１に記載のコンピューティングデバイス。

【請求項４】

前記コンテンツは、前記コンテンツに対する書込み専用の構成を実装するために前記ビデオカードへの信号を伴うことを特徴とする請求項１に記載のコンピューティングデバイス。

【請求項５】

前記書込み専用の構成は、前記ビデオメモリ内に少なくとも１つの書込み専用バッファを作成することによって、前記ビデオメモリ内で実装されることを特徴とする請求項４に記載のコンピューティングデバイス。

【請求項６】

各書込み専用バッファは、１次サーフェスを介して表示されるためのビットマップされた２次ビデオサーフェスであることを特徴とする請求項５に記載のコンピューティングデバイス。

【請求項７】

前記ビデオカードは、各書込み専用バッファを解放すると同時に書込み専用バッファを消去することを特徴とする請求項５に記載のコンピューティングデバイス。

【請求項８】

前記提示されたトークンは証明であり、定期的に更新される証明リストに照らして前記ＤＲＭシステムによって再検討され、前記ＤＲＭシステムは、当該証明についての再検討に基づいて前記ビデオカードを信用するかどうかを決定し、前記証明リストは、前記ビデオカードの製造業者によって書込み専用でないビデオメモリを備えた前記ビデオカードが製造され、前記合意に反している場合、前記再検討された証明が遵守されていないことを反映するように前記ＤＲＭシステムによって更新されることを特徴とする請求項１に記載のコンピューティングデバイス。

【請求項９】

保護されたデジタルコンテンツのレンダリングを可能にするために、デジタル権管理（ＤＲＭ）システムを含むコンピューティングデバイスにおいて実行される方法であって、前記コンピューティングデバイスはビデオカードを備え、前記方法は、

前記ビデオカードが、前記コンピューティングデバイスのモニタ上で表示されるビデオコンテンツを含む前記コンテンツを受信するステップと、

前記ビデオカードが、当該ビデオカード内に含まれるビデオメモリであって、外部の任意のエンティティに対して書込み専用となるように構成されたビデオメモリに前記受信したコンテンツを格納するステップと、

前記ビデオカードに含まれる認証デバイスが、当該ビデオメモリが外部の任意のエンティティに対して書込み専用となるように構成されていることを前記ＤＲＭシステムに対して認証するステップであって、当該ビデオカード内のビデオメモリを前記ビデオカードの外部の任意のエンティティに対して書込み専用とするように構成するという条件が合意された場合に当該認証デバイスに与えられるトークンを、前記ＤＲＭシステムに提示することによって認証するステップと、

前記ＤＲＭシステムが、前記提示されたトークンに基づいて、前記ビデオカードを信用するかどうかを決定し、信用できる場合にのみ前記ビデオカードの前記ビデオメモリを前記ビデオカードに対して読取り可能にするステップと、

前記ビデオメモリが読取り可能にされた場合、前記ビデオカードが、当該ビデオメモリ内に格納された前記コンテンツに基づいてビデオ信号を生成し、生成されたビデオ信号を前記モニタに送信するステップと、

前記コンピューティングデバイスが、前記生成されたビデオ信号に基づいて前記コンテンツを前記モニタにレンダリングするステップと

を含むことを特徴とする方法。

【請求項１０】

前記ビデオメモリは、ビデオＲＡＭであることを特徴とする請求項９に記載の方法。

【請求項１１】

前記コンテンツは、前記コンテンツに対する書込み専用構成を実装するための前記ビデオカードへの信号を伴い、

前記方法は、

前記ビデオカードが、前記コンテンツから前記信号を受信して、前記ビデオメモリ内に前記コンテンツを書き込むための少なくとも１つの書込み専用バッファを作成することによって、書込み専用構成を実装するステップをさらに含むことを特徴とする請求項９に記載の方法。

【請求項１２】

前記書込み専用バッファは、１次サーフェスを介して表示するためのビットマップされた２次ビデオサーフェスであることを特徴とする請求項１１に記載の方法。

【請求項１３】

前記ビデオカードは、各書込み専用バッファを解放すると同時に書込み専用バッファを消去することを特徴とする請求項１１に記載の方法。

【請求項１４】

前記トークンは証明であり、

前記方法はさらに、

前記ＤＲＭシステムが、前記証明と、該ＤＲＭシステムに含まれ、かつ定期的に更新される証明リストとに基づいて、前記ビデオカードを信用するかどうかを決定するステップをさらに含み、

前記証明リストは、証明が与えられているビデオカードが書込み専用でないビデオメモリを備えており、前記合意に反している場合は、当該証明を受け入れ不可とするように、前記ＤＲＭシステムによって更新されることを特徴とする請求項９に記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はデジタルコンテンツにおける権利を強制するためのアーキテクチャに関する。より詳細には、本発明は、デジタルコンテンツのユーザが取得したライセンス権によって指定されるパラメータに従う場合のみ、暗号化されたデジタルコンテンツへのアクセスを可能にするような強制アーキテクチャに関する。さらに具体的に言えば、本発明は、コンピューティングデバイス内のビデオカードなどの復号化されたデジタルコンテンツを受け取るデバイスを確実に信用できるものにすることに関する。

【０００２】

【従来の技術】

本発明は、１９９９年４月１２日出願の「Ｅｎｆｏｒｃｅｍｅｎｔ Ａｒｃｈｉｔｅｃｔｕｒｅ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ」という名称の米国特許出願第０９／２９０３６３号、および１９９９年3月２７日出願の「Ｅｎｆｏｒｃｅｍｅｎｔ Ａｒｃｈｉｔｅｃｔｕｒｅ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ」という名称の米国仮出願第６０／１２６６１４号に関するものであって、各出願全体が参照により本明細書に組み込まれている。

【０００３】

デジタルオーディオ、デジタルビデオ、デジタルテキスト、デジタルデータ、デジタルマルチメディアなどのデジタルコンテンツに関連して、こうしたデジタルコンテンツがユーザに配信される場合には、デジタル権を管理および強制することが非常に望ましい。典型的な配信モードには、磁気（フロッピィ（登録商標））ディスク、磁気テープ、光（コンパクト）ディスク（ＣＤ）などの有形デバイス、および電子掲示板、電子ネットワーク、インターネットなどの無形媒体が含まれる。このようなユーザはデジタルコンテンツを受け取ると、パーソナルコンピュータのメディアプレーヤなどの適切なレンダリング（ｒｅｎｄｅｒｉｎｇ）デバイスを使用して、これをレンダリングまたは「再生」する。

【０００４】

典型的には、著者、出版者、放送者などのコンテンツの所有者または権利所有者（以下「コンテンツ所有者」と呼ぶ）は、こうしたデジタルコンテンツを、ライセンス料または何らかの他の報酬と引き換えにユーザまたは受信者に配信することを望む。こうしたコンテンツ所有者は、選べるならば、ユーザがこのような配信されたデジタルコンテンツを使ってできることを制限しようとするであろう。例えば、コンテンツ所有者は、ユーザがこのようなコンテンツをコピーすること、および少なくともコンテンツ所有者が第２のユーザからライセンス料を得られないような方法でユーザがこうした第２のユーザにコンテンツを再配信することを制限しようとするであろう。

【０００５】

さらに、コンテンツ所有者は、様々なタイプの使用ライセンスを様々なライセンス料で購入できる柔軟性をユーザに提供すると同時に、実際に購入したライセンスのタイプに応じた条件にユーザを拘束することを望む可能性がある。例えば、コンテンツ所有者は、配信されたデジタルコンテンツの再生を、限定回数のみ、一定の合計時間のみ、一定タイプのマシンでのみ、一定タイプのメディアプレーヤでのみ、一定タイプのユーザによってのみ、などと制限しようとすることができる。

【０００６】

しかし、いったん配信されてしまうと、こうしたコンテンツ所有者は殆どデジタルコンテンツを管理することができない。こうしたデジタルコンテンツの正確なデジタルコピーを作成すること、こうした正確なデジタルコピーを書き込み可能な磁気ディスクまたは光ディスクにダウンロードすること、あるいはこうした正確なデジタルコピーをインターネットなどのネットワークを介して任意の宛先に送信することなどに必要なソフトウェアおよびハードウェアが、事実上、新しいか、または最近のあらゆるパーソナルコンピュータに含まれているという事実から考えると、これは特に問題である。

【０００７】

勿論、ライセンス料が得られた場合の妥当な取引の一部として、コンテンツ所有者は、デジタルコンテンツのユーザがこうしたデジタルコンテンツを再配信しないように約束させる場合もある。ただし、こうした約束は、結ぶことも簡単であるが、破ることも簡単である。コンテンツ所有者は、通常は暗号化および復号を含む、いくつかの知られたセキュリティデバイスのいずれかを使用して、こうした再配信の防止を試みることができる。ただし、決意の甘いユーザが、暗号化されたデジタルコンテンツを復号化し、こうしたデジタルコンテンツを暗号化されていない形式で保存し、同様のものを再配信するのを防ぐのは殆ど不可能である。

【０００８】

【発明が解決しようとする課題】

そこで、任意の形式のデジタルコンテンツの制御されたレンダリングまたは再生を可能にする強制アーキテクチャおよび方法を提供すること、並びにこうしたデジタルコンテンツのコンテンツ所有者によるこうした制御が柔軟かつ設定可能であることが求められている。さらに、パーソナルコンピュータなどのコンピューティングデバイス上に制御されたレンダリング環境を提供し、このレンダリング環境には少なくともこうした強制アーキテクチャの一部が含まれることも求められている。こうした制御されたレンダリング環境では、デジタルコンテンツがコンテンツ所有者の制御下にないコンピューティングデバイス上

でレンダリングされようとした場合であっても、デジタルコンテンツは、コンテンツ所有者が指定した通りにレンダリングされるだけであるようにすることができる。

【０００９】

さらに、コンピューティングデバイス上で実行する信用される（ｔｒｕｓｔｅｄ）構成要素も求められており、信用される構成要素は、こうしたコンピューティングデバイスのユーザが、コンテンツ所有者によって許可されていない方法でこうしたデジタルコンテンツにアクセスしようとする試みに対しても、こうしたコンピューティングデバイス上で１ピースのデジタルコンテンツに関連してコンテンツ所有者の権利を強制する。さらに、コンテンツ泥棒がビデオカード上に常駐する／ビデオカード用とされたコンテンツを盗用するのを防ぐために、コンピューティングデバイスのセキュア（ｓｅｃｕｒｅ）ビデオカードも求められている。

【００１０】

【課題を解決するための手段】

前述のニーズは、デジタル権管理のための強制アーキテクチャおよび方法によって少なくとも一部が満たされ、このアーキテクチャおよび方法によって、インターネット、光ディスクなどの媒体上で使用可能な保護された（セキュア）デジタルコンテンツにおける権利が強制される。コンテンツを使用可能にするために、アーキテクチャには、インターネットなどを介して暗号化形式のデジタルコンテンツにアクセス可能なコンテンツサーバが含まれる。コンテンツサーバは、光ディスクなどにレコーディングするための暗号化されたデジタルコンテンツも供給可能であり、暗号化されたデジタルコンテンツは、光ディスクそれ自体で配布することができる。コンテンツサーバでは、デジタルコンテンツが暗号鍵を使用して暗号化され、ユーザのコンピューティングデバイスまたはクライアントマシンでは、デジタルコンテンツをデジタルライセンスで拘束するために公開／秘密鍵技法が使用される。

【００１１】

ユーザがコンピューティングデバイス上でデジタルコンテンツをレンダリングしようとすると、レンダリングアプリケーションは、こうしたユーザのコンピューティングデバイス上でデジタル権管理（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ／ＤＲＭ）システムを起動する。ユーザが初めてデジタルコンテンツをレンダリングしようとした場合、ＤＲＭシステムは、要求される方法でそのようなデジタルコンテンツをレンダリングするためのライセンスを取得するようにユーザをライセンスサーバに向けさせる、または、ユーザ側で行為を必要とすることなく、そのようなライセンスサーバからそのようなライセンスを透過的に取得する。ライセンスには、

暗号化されたデジタルコンテンツを復号する復号鍵（ＫＤ）と、

ライセンスおよび関連条件（開始日、満了日、再生回数など）が与えられた権利（再生、コピーなど）の、デジタル方式で読取り可能な形式の記述と、

ライセンスの保全性を保証するデジタル署名とが含まれる。

【００１２】

ユーザは、こうしたライセンスをライセンスサーバから取得せずに、暗号化されたデジタルコンテンツを復号およびレンダリングすることはできない。取得されたライセンスは、ユーザのコンピューティングデバイスにあるライセンス記憶域に格納される。

【００１３】

ライセンスサーバは、「信用される」（すなわちそれ自体が認証可能な）ＤＲＭシステムに限って、ライセンスを発行することが重要である。ＤＲＭシステムには「信用」を実施するために、こうしたＤＲＭシステムに対して復号および暗号化機能を実施する「ブラックボックス」が備えられている。ブラックボックスには、公開鍵／秘密鍵のペア、バージョン番号、および固有の署名が含まれており、これらはすべて承認済みの証明機関（ｃｅｒｔｉｆｙｉｎｇ　ａｕｔｈｏｒｉｔｙ）によって与えられる。ライセンスサーバは、公開鍵を使用して発行済みライセンスの一部を暗号化することが可能であり、これによって、こうしたライセンスがこうしたブラックボックスに結び付けられる。秘密鍵は、対応す

る公開鍵で暗号化された情報を復号するためにブラックボックスのみが使用できるものであり、ユーザやその他の人は使用できない。ＤＲＭシステムには、初期時には公開鍵／秘密鍵ペアを備えたブラックボックスが与えられており、ユーザが最初にライセンスを要求すると、ブラックボックスサーバから更新済みのセキュアブラックボックスをダウンロードするように指示される。ブラックボックスサーバは、更新済みのブラックボックスと共に固有の公開鍵／秘密鍵ペアを提供する。こうした更新済みのブラックボックスは、ユーザのコンピューティングデバイス上でのみ実行される固有の実行可能コードで作成されており、定期的に再更新される。

【００１４】

ユーザがライセンスを要求すると、クライアントマシンはブラックボックスの公開鍵、バージョン番号、および署名をライセンスサーバに送信し、こうしたライセンスサーバは、バージョン番号が現在のものであり、署名が有効である場合にのみ、ライセンスを発行する。ライセンス要求には、ライセンスが要求されるデジタルコンテンツの識別、および要求されたデジタルコンテンツに関連付けられた復号鍵を識別する鍵（ｋｅｙ）ＩＤも含まれている。ライセンスサーバは、ブラックボックス公開鍵を使用して復号鍵を暗号化し、復号鍵を使用してライセンス条件を暗号化したのち、暗号化された復号鍵および暗号化されたライセンス条件を、ライセンス署名と共にユーザのコンピューティングデバイスにダウンロードする。

【００１５】

ダウンロードされたライセンスがＤＲＭシステムのライセンス記憶域にいったん格納されると、ユーザは、ライセンスによって与えられライセンス条件に指定された権利に従って、デジタルコンテンツをレンダリングすることができる。デジタルコンテンツをレンダリングするように要求されると、ブラックボックスが復号鍵およびライセンス条件を復号し、ＤＲＭシステムのライセンス評価器がこうしたライセンス条件を評価する。ブラックボックスは、ライセンス評価の結果、要求者がこうしたコンテンツを再生してもよいという結論に達した場合に限って、暗号化されたデジタルコンテンツを復号する。復号されたコンテンツは、レンダリングのためにレンダリングアプリケーションに提供される。

【００１６】

本発明では、コンピューティングデバイスに、対応するデジタルライセンスに指定された権利に従う場合に限って、コンピューティングデバイス上で権利保護されたデジタルコンテンツのレンダリングが可能なデジタル権管理（ＤＲＭ）システムが含まれる。コンテンツには、コンピューティングデバイスに結合されたモニタ上で表示されるビデオコンテンツが含まれる。コンピューティングデバイスには、コンテンツを受信し、受信したコンテンツに基づいてモニタに送信されるビデオ信号を生成するためのビデオセクションも含まれる。ビデオセクションには、受信したコンテンツを格納するためのビデオメモリが含まれ、このビデオメモリは、ビデオセクションに関する以外は書込み専用となるように構成される。さらにビデオセクションには、ビデオメモリがビデオセクションに関する以外は書込み専用となるように構成されることをＤＲＭシステムに認証するための認証デバイスも含まれる。

【００１７】

したがって、コンピューティングデバイス上の他の構成要素がそのように作成されたデータを読み取れないような方法で、ビデオデータを出力デバイスにレンダリングできるセキュアコンピューティング環境が作成される。ビデオセクションは、こうしたビデオセクションにアクセスするアプリケーションまたはオペレーティングシステム構成要素に関して書込み専用のビデオバッファを提示するか、あるいはビデオセクションが、伝送およびレンダリングされたデータを効果的に隠すために、ローカル処理またはリモートエンティティとの暗号化接続を確立できるようにするかのいずれかによって、セキュア出力をサポートする。

【００１８】

データの作者は、ビデオセクションに送信したデータが、ビデオセクションに見せかけた

不当なソフトウェアではなく、真のビデオセクションに送信されたことを確認しなければならない。こうした確認は、暗号認証によって達成することができる。

【００１９】

前述の概要並びに後述の本発明の実施形態の詳細な説明は、添付の図面と共に読むと、より良く理解されよう。図面には、本発明を例示する目的で、現在の好ましい実施形態が示されている。ただし、本発明は、図面に示された精密な配置構成および手段に限定されるものでないことを理解されたい。

【００２０】

【発明の実施の形態】

図面を詳細に参照すると、全体を通じて同じ要素を示すのには同じ番号が使用されており、図１には、本発明の一実施形態に従った強制アーキテクチャ１０が示されている。全体として、強制アーキテクチャ１０は、デジタルコンテンツ１２の所有者がライセンス規則を指定できるようにするものであり、この規則を満たした後に、こうしたデジタルコンテンツ１２がユーザのコンピューティングデバイス１４上でレンダリング可能とならなければならない。こうしたライセンス規則は、ユーザ／ユーザのコンピューティングデバイス１４（以下、このような用語は、それ以外の状況が必要でない限り、交換可能である）が、コンテンツ所有者またはそのエージェントから取得しなければならないデジタルライセンス１６内で具体化される。デジタルコンテンツ１２は暗号化形式で配信され、自由かつ広範囲に配信することができる。デジタルコンテンツ１２を復号するための復号鍵（ＫＤ）は、ライセンス１６と共に含められることが好ましい。

【００２１】

コンピュータ環境

図１３および以下の考察は、本発明および／またはその一部が実施可能な好適なコンピューティング環境を簡単に概説することを意図するものである。必須ではないが、本発明は、クライアントワークステーションまたはサーバなどコンピュータによって実行される、プログラムモジュールなどコンピュータ実行可能命令の一般的なコンテキストで説明される。一般に、プログラムモジュールには、特定のタスクを実行するかまたは特定の抽象データ型を実施するルーチン、プログラム、オブジェクト、構成要素、データ構造などが含まれる。さらに、本発明および／またはその一部は、ハンドヘルドデバイス、マルチプロセッサシステム、マイクロプロセッサベースまたはプログラム可能な大衆消費電子製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータなどを含む他のコンピュータシステム構成でも実施可能であることを理解されたい。本発明は、通信ネットワークを介してリンクされたリモート処理デバイスによってタスクが実行される分散コンピューティング環境でも実施可能である。分散コンピューティング環境では、プログラムモジュールを、ローカルおよびリモートの両方のメモリストレージデバイスに配置することができる。

【００２２】

図１３に示されるように、例示的な汎用コンピューティングシステムには、処理ユニット１２１、システムメモリ１２２、並びに、システムメモリを含む様々なシステム構成要素を処理ユニット１２１に結合するシステムバス１２３を含む従来のパーソナルコンピュータ１２０などが含まれる。システムバス１２３は、様々なバスアーキテクチャのいずれかを使用するメモリバスまたはメモリ制御装置、周辺バス、およびローカルバスを含む、いくつかのタイプのバス構造のいずれかであってよい。システムメモリには、読取り専用メモリ（ＲＯＭ）１２４およびランダムアクセスメモリ（ＲＡＭ）１２５が含まれる。起動時などにパーソナルコンピュータ１２０内の要素間で情報を転送するのに役立つ基本ルーチンを含む基本入出力システム１２６（ＢＩＯＳ）がＲＯＭ１２４内に格納される。

【００２３】

さらにパーソナルコンピュータ１２０には、ハードディスク（図示せず）からの読取りおよびこれへの書込みのためのハードディスクドライブ１２７、取外し可能磁気ディスク１２９からの読取りおよびこれへの書込みのための磁気ディスクドライブ１２８、並びに、

ＣＤ－ＲＯＭまたは他の光学式媒体などの取外し可能光ディスク１３１からの読取りおよびこれへの書込みのための光ディスクドライブ１３０が含まれることがある。ハードディスクドライブ１２７、磁気ディスクドライブ１２８、および光ディスクドライブ１３０は、それぞれハードディスクドライブインターフェース１３２、磁気ディスクドライブインターフェース１３３、および光ドライブインターフェース１３４によって、システムバス１２３に接続される。ドライブおよびそれらに関連付けられたコンピュータ読取り可能媒体は、パーソナルコンピュータ２０用のコンピュータ読取り可能命令、データ構造、プログラムモジュール、および他のデータの不揮発性記憶域を提供する。

【００２４】

本明細書に記載された例示的な環境では、ハードディスク、取外し可能磁気ディスク１２９、および取外し可能光ディスク１３１を使用しているが、例示的な動作環境では、コンピュータがアクセス可能なデータを格納できる他のタイプのコンピュータ読取り可能媒体も使用できることを理解されたい。こうした他のタイプの媒体には、磁気カセット、フラッシュメモリカード、デジタルビデオディスク、ベルヌーイカートリッジ、ランダムアクセスメモリ（ＲＡＭ）、読取り専用メモリ（ＲＯＭ）などが含まれる。

【００２５】

いくつかのプログラムモジュールは、オペレーティングシステム１３５、１つ以上のアプリケーションプログラム１３６、他のプログラムモジュール１３７、およびプログラムデータ１３８を含むハードディスク、磁気ディスク１２９、光ディスク１３１、ＲＯＭ１２４、またはＲＡＭ１２５に格納することができる。ユーザは、キーボード１４０およびポインティングデバイス１４２などの入力デバイスを介して、パーソナルコンピュータ１２０にコマンドおよび情報を入力することができる。他の入力デバイス（図示せず）には、マイクロフォン、ジョイスティック、ゲームパッド、衛星放送受信アンテナ、スキャナなどが含まれる。これらおよび他の入力デバイスは、システムバスに結合されたシリアルポートインターフェース１４６を介して処理ユニット１２１に接続されることが多いが、パラレルポート、ゲームポート、またはＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）などの他のインターフェースによって接続することもできる。モニタ１４７または他のタイプのディスプレイ装置も、ビデオアダプタ１４８などのインターフェースを介してシステムバス１２３に接続される。モニタ１４７に加えて、パーソナルコンピュータには、典型的に、スピーカおよびプリンタなどの他の周辺出力デバイス（図示せず）も含まれる。図１３の例示的システムには、ホストアダプタ１５５、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍ Ｉｎｔｅｒｆａｃｅ）バス１５６、およびＳＣＳＩバス１５６に接続された外部ストレージデバイス１６２も含まれる。

【００２６】

パーソナルコンピュータ１２０は、リモートコンピュータ１４９などの１つ以上のリモートコンピュータへの論理接続を使用するネットワーク環境で動作することが可能である。リモートコンピュータ１４９は、他のパーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス、または他の共通ネットワークノードであってよく、図１３にはメモリストレージデバイス１５０だけが示されているが、典型的には、パーソナルコンピュータ１２０に関して上述した多くのまたはすべての要素が含まれる。図１３に示された論理接続には、ローカルエリアネットワーク（ＬＡＮ）１５１およびワイドエリアネットワーク（ＷＡＮ）１５２が含まれる。こうしたネットワーキング環境は、会社や企業規模のコンピュータネットワーク、イントラネット、およびインターネットでは一般的なものである。

【００２７】

ＬＡＮネットワーキング環境で使用する場合、パーソナルコンピュータ１２０はネットワークインターフェースまたはアダプタ１５３を介してＬＡＮ１５１に接続される。ＷＡＮネットワーキング環境で使用する場合、パーソナルコンピュータ１２０には典型的に、インターネットなどのワイドエリアネットワーク１５２を介した通信を確立するためのモデム１５４または他の手段が含まれる。モデム１５４は内部でも外部でもよく、シリアルポ

ートインターフェース１４６を介してシステムバス１２３に接続される。ネットワーク環境では、パーソナルコンピュータ１２０に関して示されたプログラムモジュールまたはその一部を、リモートメモリストレージデバイスに格納することができる。図示されたネットワーク接続は例示的なものであり、コンピュータ間の通信リンクを確立する他の手段が使用可能であることを理解されたい。

【００２８】

アーキテクチャ

図１を再度参照すると、本発明の一実施形態では、アーキテクチャ１０には認証ツール１８、コンテンツ鍵データベース２０、コンテンツサーバ２２、ライセンスサーバ２４、およびブラックボックスサーバ２６、並びに前述のユーザのコンピューティングデバイス１４が含まれる。

【００２９】

アーキテクチャ―認証ツール１８

認証ツール１８は、コンテンツ所有者が１ピースのデジタルコンテンツ１２を、本発明のアーキテクチャ１０に関連して使用するのに適した形式にパッケージングするために使用される。具体的に言えば、コンテンツ所有者は、認証ツール１８に、デジタルコンテンツ１２、並びにデジタルコンテンツ１２がどのようにパッケージングされるかに関する命令および／または規則に付随するデジタルコンテンツ１２、命令、および／または規則を提供する。次いで認証ツール１８は、暗号／復号鍵に従って暗号化されたデジタルコンテンツ１２、並びにデジタルコンテンツ１２に付随する命令および／または規則を有するデジタルコンテンツパッケージ１２ｐを生成する。

【００３０】

本発明の一実施形態では、認証ツール１８は、それぞれが、異なる暗号／復号鍵に従って暗号化された同じデジタルコンテンツ１２を有するいくつかの異なるデジタルコンテンツ１２のパッケージ１２ｐを順次生成するように命令される。同じデジタルコンテンツ１２を備えたいくつかの異なるパッケージ１２ｐを有することは、こうしたパッケージ１２ｐ／コンテンツ１２（以下、それ以外の状況が必要でない限り、単に「デジタルコンテンツ１２」とする）の配信を追跡するのに役立てられることを理解されたい。こうした配信追跡は、通常は不要であるが、デジタルコンテンツ１２が不法に販売またはブロードキャストされた場合は、調査機関が使用することがある。

【００３１】

本発明の一実施形態では、デジタルコンテンツ１２を暗号化する暗号／復号鍵は対称鍵であり、暗号鍵は復号鍵（ＫＤ）でもある。以下でより詳細に説明するように、こうした復号鍵（ＫＤ）は、こうしたデジタルコンテンツ１２用のライセンス１６の一部として、隠された形態で、ユーザのコンピューティングデバイス１４に送達される。デジタルコンテンツ１２の各ピースにコンテンツＩＤが提供され（または各パッケージ１２ｐにパッケージＩＤが提供され）、各復号鍵（ＫＤ）が鍵ＩＤを有し、認証ツール１８が、デジタルコンテンツ１２の各ピース（または各パッケージ１２ｐ）に関する復号鍵（ＫＤ）、鍵ＩＤ、およびコンテンツＩＤ（またはパッケージＩＤ）を、コンテンツ鍵データベース２０に格納されるようにすることが好ましい。さらに、デジタルコンテンツ１２に対して発行されるライセンス１６のタイプに関するライセンスデータ、およびライセンス１６の各タイプに関する条件を、コンテンツ鍵データベース２０またはその他のデータベース（図示せず）に格納することもできる。ライセンスデータは、状況および市場条件の要求に応じて、コンテンツ所有者が後で修正可能であることが好ましい。

【００３２】

使用の際、認証ツール１８には、とりわけ、

パッケージングされるデジタルコンテンツ１２と、

使用されるウォータマーキングおよび／またはフィンガプリンティング（あれば）のタイプおよびパラメータと、

使用されるデータ圧縮（あれば）のタイプおよびパラメータと、

使用される暗号化のタイプおよびパラメータと、
使用される逐次化（ｓｅｒｉａｌｉｚａｔｉｏｎ）（あれば）のタイプおよびパラメータと、
デジタルコンテンツ１２に付随する命令および／または規則とを含む情報が供給される。

【００３３】

周知のことながら、ウォータマークとは隠れたコンピュータ読取り可能信号であり、デジタルコンテンツ１２に識別子として追加される。フィンガプリントとは、インスタンスによって異なるウォータマークである。当然のことながら、インスタンスとは、固有のデジタルコンテンツ１２のバージョンである。任意のインスタンスのコピーを複数作成することが可能であり、いずれかのコピーが特定インスタンスのものである。デジタルコンテンツ１２の特定インスタンスが不法に販売またはブロードキャストされた場合、調査機関はおそらく、こうしたデジタルコンテンツ１２に加えられたウォータマーク／フィンガプリントに従って容疑者を識別することができる。

【００３４】

データ圧縮は、本発明の精神および範囲を逸脱することなく、任意の適切な圧縮アルゴリズムに従って実行することができる。例えば、．ｍｐ３または．ｗａｖ圧縮アルゴリズムを使用することができる。勿論、追加の圧縮が必要でない場合、デジタルコンテンツ１２は既に圧縮状態にある可能性がある。

【００３５】

デジタルコンテンツ１２に付随する命令および／または規則は、本発明の精神および範囲を逸脱することなく、実際に、任意の適切な命令、規則、または他の情報を含むことができる。以下で論じるように、こうした付随の命令／規則／情報は、主にユーザおよびユーザのコンピューティングデバイス１４が、デジタルコンテンツ１２をレンダリングするためのライセンス取得に使用される。したがって、こうした付随の命令／規則／情報には、以下でより詳細に説明するように、適切に形式化されたライセンス獲得スクリプトなどが含まれる。さらに、または別の方法として、こうした付随の命令／規則／情報は、ユーザにデジタルコンテンツ１２のプレビューを提供するように設計された「プレビュー」情報を含むことができる。

【００３６】

次いで認証ツール１８は、供給された情報を使用して、デジタルコンテンツ１２に対応する１つ以上のパッケージ１２ｐを生成する。次いで各パッケージ１２ｐを、世界に配信するためにコンテンツサーバ２２上に格納することができる。

【００３７】

本発明の一実施形態では、またここで図２を参照すると、認証ツール１８は、指定および動作可能な入力パラメータを受け取る動的な認証ツール１８である。したがって、こうした認証ツール１８は、デジタルコンテンツ１２の複数のピースに対して、パッケージ１２ｐの複数のバリエーションを即時に生成することができる。図に示されるように、入力パラメータは辞書２８の形式で具体化されることが好ましく、辞書２８には、
デジタルコンテンツ１２を有する入力ファイル２９ａの名前と、
実行される符号化のタイプと、
使用される暗号／復号鍵（ＫＤ）と、
パッケージ１２ｐ内でデジタルコンテンツ１２と共にパッケージングされる、付随する命令／規則／情報（「ヘッダ情報」）と、
発生する多重化（ｍｕｘｉｎｇ）のタイプと、
デジタルコンテンツ１２に基づいたパッケージ１２ｐが書き込まれる出力ファイル２９ｂの名前、
などのパラメータが含まれる。

【００３８】

当然のことながら、こうした辞書２８は認証ツール１８のオペレータ（人間またはマシン）によって容易かつ迅速に修正可能であるため、認証ツール１８によって実行される認証

のタイプも同様に、動的な方法で容易かつ迅速に修正可能である。本発明の一実施形態では、認証ツール１８に、人間のオペレータに対してコンピュータ画面上に表示可能なオペレータインターフェース（図示せず）が含まれる。したがって、こうしたオペレータは、インターフェースを使って辞書２８を修正することが可能であり、さらに、辞書２８の修正の際に、インターフェースによって適切に支援および／または制限されることが可能である。

【００３９】

認証ツール１８では、図２に示されるように、ソースフィルタ１８ａがデジタルコンテンツ１２を有する入力ファイル２９ａの名前を辞書２８から受け取り、こうしたデジタルコンテンツ１２をこうした入力ファイルから受け取って、このデジタルコンテンツ１２をＲＡＭなどのメモリ２９ｃ内に配置する。その後、符号化フィルタ１８ｂは、辞書２８に指定された符号化のタイプに従って、ファイルを入力形式から出力形式（すなわち、．ｗａｖから．ａｓｐ、．ｍｐ３から．ａｓｐなど）に転送（transform）するために、メモリ２９ｃ内のデジタルコンテンツ１２の符号化を実行し、符号化されたデジタルコンテンツ１２をメモリ２９ｃ内に配置する。図に示されるように、パッケージングされるデジタルコンテンツ１２（例えば音楽）は、．ｗａｖまたは．ｍｐ３形式などの圧縮形式で受け取られ、．ａｓｐ（ａｃｔｉｖｅ　ｓｔｒｅａｍｉｎｇ　ｐｒｏｔｏｃｏｌ）形式などの形式に変換される。勿論、本発明の精神および範囲を逸脱することなく、他の入力および出力形式も使用できる。

【００４０】

その後、暗号化フィルタ１８ｃが、辞書２８に指定された暗号／復号鍵（ＫＤ）に従って、メモリ２９ｃ内の符号化されたデジタルコンテンツ１２を暗号化し、暗号化されたデジタルコンテンツ１２をメモリ２９ｃ内に配置する。次いでヘッダフィルタ１８ｄが、辞書２８に指定されたヘッダ情報を、メモリ２９ｃ内の暗号化されたデジタルコンテンツ１２に追加する。

【００４１】

当然のことながら、状況に応じてパッケージ１２ｐは、一時的に位置合わせされたデジタルコンテンツ１２の複数のストリーム（１つのストリームが図２に示されている）を含むことが可能であり、こうした複数のストリームはマルチプレックス（すなわち多重化）される。したがって、多重化フィルタ１８ｅは、辞書２８に指定された多重化のタイプに従って、メモリ２９ｃ内のヘッダ情報および暗号化されたデジタルコンテンツ１２に対して多重化を実行し、その結果をメモリ２９ｃ内に配置する。その後ファイル書込みフィルタ１８ｆがメモリ２９ｃからその結果を取り出し、こうした結果を辞書２８に指定された出力ファイル２９ｂにパッケージ１２ｐとして書き込む。

【００４２】

一定の状況では、実行される符号化のタイプが通常は変化しないことに留意されたい。多重化のタイプは典型的には符号化のタイプに基づいているため、多重化のタイプも同様に、通常は変化しない。実際にこのような場合、辞書２８は、符号化のタイプおよび／または多重化のタイプに関するパラメータを含む必要はない。代わりに、符号化のタイプが符号化フィルタに「ハードワイヤードする」こと、および／または多重化のタイプが多重化フィルタに「ハードワイヤードする」ことだけが必要である。勿論、状況によって必要であれば、認証ツール１８は前述のすべてのフィルタを含まないことも、他のフィルタを含むこともでき、含まれる任意のフィルタは、ハードワイヤードすることも、辞書２８に指定されたパラメータに従ってその機能を実行することもでき、これらはすべて、本発明の精神および範囲を逸脱しない。

【００４３】

認証ツール１８は、適切なコンピュータ、処理装置、または他のコンピューティングマシン上で、適切なソフトウェアによって実施されることが好ましい。こうしたマシンおよびこうしたソフトウェアの構造および動作は、本明細書の開示内容に基づいて明らかとなるはずであるため、本開示では詳細な説明は不要である。

【００４４】
アーキテクチャ－コンテンツサーバ２２
再度図１を参照すると、本発明の一実施形態では、コンテンツサーバ２２が、認証ツール１８によって生成されたパッケージ１２ｐを配信するか、またはそうでなければこのパッケージ１２ｐの取出しに使用することができる。こうしたパッケージ１２ｐは、本発明の精神および範囲を逸脱することなく、任意の適切な配信チャネルを使用して、コンテンツサーバ２２の要求に応じて配信することが可能である。例えば、こうした配信チャネルはインターネットまたは他のネットワーク、電子掲示板、電子メールなどであってよい。さらに、コンテンツサーバ２２を使用して、パッケージ１２ｐを磁気または光ディスク、あるいは他のストレージデバイス上にコピーし、その後こうしたストレージデバイスを配布することが可能である。
【００４５】
コンテンツサーバ２２は、どんな信用またはセキュリティの問題があろうとも、パッケージ１２ｐを配信することを理解されよう。以下で論じるように、こうした問題は、ライセンスサーバ２４と共同で、こうしたライセンスサーバ２４とユーザのコンピューティングデバイス１４との間の関係で処理される。本発明の一実施形態では、コンテンツサーバ２２は、デジタルコンテンツ１２を有するパッケージ１２ｐを、書込み専用バッファを要求している任意の配信受信者（ｄｉｓｔｒｉｂｕｔｅｅ）に自由に公開および配信する。ただし、コンテンツサーバ２２は、こうしたパッケージ１２ｐを、本発明の精神および範囲を逸脱することなく、制限された方法で公開および配信することもできる。例えば、コンテンツサーバ２２は、配信に先立って第１に所定の配信料の支払いを要求するか、または配信受信者がそれ自体を識別するように要求するか、または配信が配信受信者の識別に基づいて発生するものであるかどうかを実際に決定することができる。
【００４６】
さらに、コンテンツサーバ２２を使用して、認証ツール１８がいくつかの異なるパッケージ１２ｐを生成するのを制御することによって、予想される需要を満たす前に、在庫管理を実行することができる。例えばサーバは、同じデジタルコンテンツ１２に基づいて１００個のパッケージ１２ｐを生成し、それぞれのパッケージ１２ｐを１０回処理する場合がある。パッケージ１２ｐの供給が２０個まで減少すると、例えばコンテンツサーバ２２は、その後認証ツール１８に、８０個の追加のパッケージ１２ｐを生成するように再度指示することができる。
【００４７】
アーキテクチャ１０のコンテンツサーバ２２は、以下でより詳細に説明するように、ライセンス１６を評価し、対応するデジタルコンテンツ１２を復号するための復号鍵（ＫＤ）を取得するプロセスの一部として使用される固有の公開鍵／秘密鍵ペア（ＰＵ－ＣＳ、ＰＲ－ＣＳ）を有することが好ましい。周知のように、公開鍵／秘密鍵ペアは対称鍵であるため、鍵ペアの一方の鍵で暗号化されたものは、その鍵ペアの他方の鍵を使用しなければ復号することができない。公開鍵／秘密鍵ペア暗号化システムでは、公開鍵は外部に公開しても良いが、秘密鍵はこうした秘密鍵の所有者によって常時秘密に保持されていなければならない。したがって、コンテンツサーバ２２がその秘密鍵（ＰＲ－ＣＳ）を使ってデータを暗号化した場合、その暗号化したデータを復号のために公開鍵（ＰＵ－ＣＳ）と共に外部に送信することができる。これに対して、こうしたコンテンツサーバ２２だけがこうしたデータを復号できることから、外部デバイスがコンテンツサーバ２２にデータを送信しようとする場合、こうした外部デバイスは、第１にコンテンツサーバ２２の公開鍵（ＰＵ－ＣＳ）を取得した後、こうした公開鍵でデータを暗号化しなければならない。したがって、その後コンテンツサーバ２２（そしてコンテンツサーバ２２だけ）が、その秘密鍵（ＰＲ－ＣＳ）を使用して、こうした暗号化データを復号することができる。
【００４８】
認証ツール１８の場合と同様に、コンテンツサーバ２２は、適切なコンピュータ、処理装置、または他のコンピューティングマシン上で、適切なソフトウェアによって実施される

。こうしたマシンおよびこうしたソフトウェアの構造および動作は、本明細書の開示内容に基づいて明らかとなるはずであるため、本開示では詳細な説明は不要である。さらに、本発明の一実施形態では、認証ツール１８およびコンテンツサーバ２２は、それぞれ別の作業スペース内にある単一のコンピュータ、処理装置、または他のコンピューティングマシン上に常駐することができる。さらにコンテンツサーバ２２は、前述のように、一定の状況では認証ツール１８を含み、および／または認証ツール１８の機能を実行することができることを理解されたい。

【００４９】

デジタルコンテンツパッケージ１２ｐの構造

ここで図３を参照すると、本発明の一実施形態では、コンテンツサーバ２２によって配信される場合、デジタルコンテンツパッケージ１２ｐには、

前述のように、暗号鍵／復号鍵（ＫＤ）によって暗号化されたデジタルコンテンツ１２（すなわち（ＫＤ（ＣＯＮＴＥＮＴ））と、

こうしたデジタルコンテンツ１２（またはパッケージ１２ｐ）のコンテンツＩＤ（またはパッケージＩＤ）と、

復号鍵（ＫＤ）の鍵ＩＤと、

好ましくは暗号化されていない形式のライセンス獲得情報と、

コンテンツサーバ２２の秘密鍵（ＰＲ－ＣＳ）によって署名されたコンテンツサーバ２２の公開鍵（ＰＵ－ＣＳ）を暗号化する鍵ＫＤ（すなわち（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））とが含まれる。

【００５０】

（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））に関して、こうした項目は、以下で説明するように、デジタルコンテンツ１２および／またはパッケージ１２ｐの妥当性検査に関連して使用されることを理解されたい。デジタル署名（下記を参照）による証明とは異なり、鍵（ＰＵ－ＣＳ）は（ＫＤ（ＰＵ－ＣＳ））を入手する必要がない。その代わりに鍵（ＰＵ－ＣＳ）は、単に復号鍵（ＫＤ）を適用するだけで得られる。このようにして得られると、こうした鍵（ＰＵ－ＣＳ）を使用して、署名Ｓ（ＰＲ－ＣＳ）の妥当性を検査することができる。

【００５１】

また、こうしたパッケージ１２ｐが認証ツール１８によって構築される場合、こうした認証ツール１８は、おそらく辞書２８によって供給されるヘッダ情報として、ライセンス獲得情報および（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））を既に所有していなければならない。さらに、認証ツール１８とコンテンツサーバ２２は、おそらく（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））を構築するために対話しなければならない。こうした対話には、例えば、

コンテンツサーバ２２が認証ツール１８に（ＰＵ－ＣＳ）を送信するステップと、

認証ツール１８が（ＫＤ（ＰＵ－ＣＳ））を生成するために（ＫＤ）で（ＰＵ－ＣＳ）を暗号化するステップと、

認証ツール１８が、（ＫＤ（ＰＵ－ＣＳ））をコンテンツサーバ２２に送信するステップと、

コンテンツサーバ２２が、（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））を生成するために、（ＰＲ－ＣＳ）で（ＫＤ（ＰＵ－ＣＳ））に署名するステップと、

コンテンツサーバ２２が、（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））を認証ツール１８に送信するステップとが含まれる。

【００５２】

アーキテクチャ－ライセンスサーバ２４

再度図１を参照すると、本発明の一実施形態では、ライセンスサーバ２４は、ライセンス１６についての要求を１ピースのデジタルコンテンツ１２に関連してユーザのコンピューティングデバイス１４から受け取る機能と、ユーザのコンピューティングデバイス１４が発行されたライセンス１６を受けるだけの信用に値するかどうかを判別する機能と、こう

したライセンス１６を取り決める機能と、こうしたライセンス１６を構築する機能と、こうしたライセンス１６をユーザのコンピューティングデバイス１４に伝送する機能とを実行する。このように伝送されたライセンス１６には、デジタルコンテンツ１２を復号するための復号鍵（ＫＤ）が含まれることが好ましい。こうしたライセンスサーバ２４およびこうした機能については、以下でより詳細に説明する。また、以下でより詳細に説明するように、コンテンツサーバ２２と同様、アーキテクチャ１０のライセンスサーバ２４は固有の公開鍵／秘密鍵ペア（ＰＵ－ＬＳ、ＰＲ－ＬＳ）を有し、これがライセンス１６を評価し、対応するデジタルコンテンツ１２を復号するための復号鍵（ＫＤ）を取得するプロセスの一部として使用されることが好ましい。

【００５３】

認証ツール１８およびコンテンツサーバ２２の場合と同様に、ライセンスサーバ２４は、適切なコンピュータ、処理装置、または他のコンピューティングマシン上で、適切なソフトウェアによって実施される。こうしたマシンおよびこうしたソフトウェアの構造および動作は、本明細書の開示内容に基づいて明らかとなるはずであるため、本開示では詳細な説明は不要である。さらに、本発明の一実施形態では、認証ツール１８および／またはコンテンツサーバ２２は、それぞれ別の作業スペース内にある単一のコンピュータ、処理装置、または他のコンピューティングマシン上に、ライセンスサーバ２４と共に常駐することができる。

【００５４】

本発明の一実施形態では、ライセンス１６を発行する前に、ライセンスサーバ２４とコンテンツサーバ２２が仲介契約などを結び、ライセンスサーバ２４は、コンテンツサーバ２２によって配信されるデジタルコンテンツ１２の少なくとも一部に対してライセンスを付与する機関となることを事実上認める。当然のことながら、１つのコンテンツサーバ２２は、いくつかのライセンスサーバ２４と仲介契約などを結ぶことが可能であり、および／または、１つのライセンスサーバ２４は、いくつかのコンテンツサーバ２２と仲介契約などを結ぶことが可能であるが、これらはすべて、本発明の精神および範囲を逸脱しないものとする。

【００５５】

ライセンスサーバ２４は、コンテンツサーバ２２によって配信されるデジタルコンテンツ１２に関するライセンス１６を発行する権限を実際に持っていることを、外部に示すことができることが好ましい。そのためには、ライセンスサーバ２４がライセンスサーバ２４の公開鍵（ＰＵ－ＬＳ）をコンテンツサーバ２２に送信し、その後コンテンツサーバ２２が、コンテンツサーバ２２の秘密鍵によって署名されたコンテンツとして、ＰＵ－ＬＳを含むデジタル証明（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））をライセンスサーバ２４に送信することが好ましい。当然のことながら、こうした証明のコンテンツ（ＰＵ－ＬＳ）には、コンテンツサーバ２２の公開鍵（ＰＵ－ＣＳ）を使用しなければアクセスできない。また当然のことながら、一般に、基礎となるデータのデジタル署名はこうしたデータの暗号化形式であり、こうしたデータの質が落とされた（ａｄｕｌｔｅｒａｔｅｄ）か、そうでなければ修正された場合は、復号したときにこうしたデータと一致しなくなる。

【００５６】

１ピースのデジタルコンテンツ１２に関連したライセンス機関として、およびライセンス機能の一部として、ライセンスサーバ２４は、こうしたデジタルコンテンツ１２の復号鍵（ＫＤ）へのアクセス権を有していなければならない。したがってライセンスサーバ２４は、こうしたデジタルコンテンツ１２（またはパッケージ１２ｐ）に関する復号鍵（ＫＤ）、鍵ＩＤ、およびコンテンツＩＤ（またはパッケージＩＤ）を有するコンテンツ鍵データベース２０へのアクセス権を有することが好ましい。

【００５７】

アーキテクチャ―ブラックボックスサーバ２６

さらに図１を参照すると、本発明の一実施形態では、ブラックボックスサーバ２６が、ユーザのコンピューティングデバイス１４で、新しいブラックボックス３０をインストール

する機能および／または更新する機能を実行する。以下でより詳細に説明するように、ブラックボックス３０は、ユーザのコンピューティングデバイス１４に対して暗号化および復号機能を実行する。さらに以下でより詳細に説明するように、ブラックボックス３０は安全にし、攻撃から保護されることを意図したものである。以下でより詳細に説明するように、こうしたセキュリティおよび保護は、少なくとも部分的に、ブラックボックスサーバ２６を使用して、ブラックボックス３０を必要に応じて新しいバージョンにアップグレードすることによって提供される。

【００５８】

認証ツール１８、コンテンツサーバ２２、およびライセンスサーバ２４の場合と同様に、ブラックボックスサーバ２６は、適切なコンピュータ、処理装置、または他のコンピューティングマシン上で、適切なソフトウェアによって実施される。こうしたマシンおよびこうしたソフトウェアの構造および動作は、本明細書の開示内容に基づいて明らかとなるはずであるため、本開示では詳細な説明は不要である。さらに、本発明の一実施形態では、ライセンスサーバ２４、認証ツール１８、および／またはコンテンツサーバ２２は、それぞれ別の作業スペース内にある単一のコンピュータ、処理装置、または他のコンピューティングマシン上に、ブラックボックスサーバ２６と共に常駐することができる。ただし、セキュリティの目的で、ブラックボックスサーバ２６は別のマシン上に置くほうが賢明であろう。

【００５９】

アーキテクチャ－ユーザのコンピューティングデバイス１４

ここで図４を参照すると、本発明の一実施形態では、ユーザのコンピューティングデバイス１４は、キーボード、マウス、スクリーン、処理装置、ＲＡＭ、ＲＯＭ、ハードドライブ、フロッピィ（登録商標）ドライブ、ＣＤプレーヤ、および／または同様のものを含む要素を有するパーソナルコンピュータなどである。ただし、ユーザのコンピューティングデバイス１４は、とりわけ、テレビジョンまたはモニタなどの専用ディスプレイ装置、ステレオまたは他の音楽プレーヤなどの専用オーディオデバイス、専用プリンタなどであってもよいが、これらはすべて本発明の精神および範囲を逸脱しないものとする。

【００６０】

１ピースのデジタルコンテンツ１２のコンテンツ所有者は、ユーザのコンピューティングデバイス１４が、こうしたコンテンツ所有者が指定した規則を守るものであること、すなわち、求められる方法でのレンダリングを許可するライセンス１６をユーザが取得しない限り、デジタルコンテンツ１２がレンダリングされることはないことを、信用しなければならない。その後ユーザのコンピューティングデバイス１４は、こうしたコンピューティングデバイス１４が、デジタルコンテンツ１２に関連付けられたライセンス１６で具体化され、ユーザによって取得されたライセンス規則に従う場合以外は、デジタルコンテンツ１２をレンダリングしないものであることをコンテンツ所有者に対して納得させることのできる信用される構成要素またはメカニズム３２を提供しなければならないことが好ましい。

【００６１】

ここでは、信用されるメカニズム３２はデジタル権管理（ＤＲＭ）システム３２であり、このシステムが、ユーザが１ピースのデジタルコンテンツ１２をレンダリングするように要求した場合に実行可能であり、ユーザが要求された方法でデジタルコンテンツ１２をレンダリングするためのライセンス１６を有するかどうかを判定し、必要であればこうしたライセンス１６の取得を実行し、ライセンス１６に従ってデジタルコンテンツ１２を再生する権利をユーザが有するかどうかを判定し、ユーザがこうしたライセンス１６に従ってこうした権利を実際に有する場合、レンダリングのためにデジタルコンテンツ１２を復号する。ユーザのコンピューティングデバイス１４上にあり、アーキテクチャ１０に関連したＤＲＭシステム３２のコンテンツおよび機能について、以下で説明する。

【００６２】

ＤＲＭシステム３２

ＤＲＭシステム３２は、本明細書に開示されたアーキテクチャ１０を使用して、（１）コンテンツの獲得、（２）ライセンスの獲得、（３）コンテンツのレンダリング、および（４）ブラックボックス３０のインストール／更新、という４つの主な機能を実行する。いずれの機能もいつでも実行できることが好ましいが、機能の中には、デジタルコンテンツ１２が獲得されることを既に必要とするものもあることを理解されたい。

【００６３】

ＤＲＭシステム３２―コンテンツの獲得

ユーザおよび／またはユーザのコンピューティングデバイス１４によるデジタルコンテンツ１２の獲得は、典型的には比較的簡単なことであり、一般に、暗号化されたデジタルコンテンツ１２を有するファイルをユーザのコンピューティングデバイス１４上に配置することが含まれる。勿論、本明細書に開示されたアーキテクチャ１０およびＤＲＭシステム３２を使って作業するためには、暗号化されたデジタルコンテンツ１２が、以下で説明するようなデジタルパッケージ１２ｐなどの、こうしたアーキテクチャ１０およびＤＲＭシステム３２に適した形であることが必要である。

【００６４】

当然のことながら、デジタルコンテンツ１２は、本発明の精神および範囲を逸脱することなく、コンテンツサーバ２２から直接的または間接的に、任意の方法で取得することができる。例えば、こうしたデジタルコンテンツ１２は、インターネットなどのネットワークからダウンロードするか、取得された光ディスクまたは磁気ディスクなどに配置するか、Ｅメールメッセージなどの一部として受け取るか、または電子掲示板などからダウンロードすることができる。

【００６５】

こうしたデジタルコンテンツ１２はいったん取得されると、取得されたデジタルコンテンツ１２が、コンピューティングデバイス１４上で実行中のレンダリングアプリケーション３４（以下で説明）およびＤＲＭシステム３２によってアクセスされるような方法で格納されることが好ましい。例えば、デジタルコンテンツ１２は、ユーザのコンピューティングデバイス１４のハードドライブ（図示せず）上、またはコンピューティングデバイス１４にアクセス可能なネットワークサーバ（図示せず）上に、ファイルとして配置することができる。デジタルコンテンツ１２が光ディスク上または磁気ディスク上などで取得される場合、こうしたディスクがユーザのコンピューティングデバイス１４に結合された適切なドライブ（図示せず）内に存在するだけでよい。

【００６６】

本発明では、直接配信ソースとしてのコンテンツサーバ２２から、または間接配信ソースとしての何らかの媒介から、デジタルコンテンツ１２を獲得するために何らかの特別なツールが必要であるとは考えていない。すなわち、デジタルコンテンツ１２は、任意の他のデータファイルと同様に容易に獲得できることが好ましい。ただし、ＤＲＭシステム３２および／またはレンダリングアプリケーション３４は、ユーザがデジタルコンテンツ１２を取得するのを支援するように設計されたインターフェース（図示せず）を含むことができる。例えば、インターフェースは、デジタルコンテンツ１２を検索するように特別に設計されたＷｅｂブラウザ、デジタルコンテンツ１２のソースとして知られる事前定義されたインターネットＷｅｂサイトへのリンクなどを含むことができる。

【００６７】

ＤＲＭシステム３２―コンテンツのレンダリング、パート１

ここで図５を参照すると、本発明の一実施形態では、暗号化されたデジタルコンテンツ１２がユーザに配信され、ユーザによって受け取られて、ユーザによって格納ファイルの形式でコンピューティングデバイス１４上に配置されると想定しており、ユーザは、レンダリングコマンドの何らかのバリエーションを実行することによって、デジタルコンテンツ１２のレンダリングを試みる（ステップ５０１）。例えば、こうしたレンダリングコマンドは、デジタルコンテンツ１２を「再生」または「開く」ための要求として実施することができる。例えば、ワシントン州ＲｅｄｍｏｎｄにあるＭＩＣＲＯＳＯＦＴ（登録商標）

Ｃｏｒｐｏｒａｔｉｏｎによって配布されるオペレーティングシステム「ＭＩＣＲＯＳＯＦＴ（登録商標）ＷＩＮＤＯＷＳ（登録商標）」などのコンピューティング環境では、こうした「再生」や「開く」などのコマンドは、デジタルコンテンツ１２のアイコン表示を単に「クリック」するだけでよい。勿論、本発明の精神および範囲を逸脱することなく、こうしたレンダリングコマンドの他の実施形態を使用することもできる。一般に、こうしたレンダリングコマンドは、ユーザが、デジタルコンテンツ１２を有するファイルを開く、実行するなどの命令を出した場合に必ず実行されるものとみなすことができる。

【００６８】

さらに、こうしたレンダリングコマンドは、デジタルコンテンツ１２を、印刷形式、表示形式、オーディオ形式などに関する他の形式にコピーするための要求として実施することも可能であることが重要である。当然のことながら、同じデジタルコンテンツ１２をある形式でコンピュータ画面上などにレンダリングした後、印刷文書などの他の形式でレンダリングすることができる。本発明では、以下で説明するように、ユーザが実行する権利を有している場合に限って、それぞれのレンダリングタイプが実行される。

【００６９】

本発明の一実施形態では、デジタルコンテンツ１２は、最後に拡張子が付いたファイル名を有するデジタルファイルの形式であり、コンピューティングデバイス１４は、こうした拡張子に基づいて、特定の種類のレンダリングアプリケーション３４の開始を決定することができる。例えば、ファイル名の拡張子が、デジタルコンテンツ１２がテキストファイルであることを示している場合、レンダリングアプリケーション３４は、ワシントン州ＲｅｄｍｏｎｄにあるＭＩＣＲＯＳＯＦＴ（登録商標）Ｃｏｒｐｏｒａｔｉｏｎによって配布される「ＭＩＣＲＯＳＯＦＴ（登録商標）ＷＯＲＤ（登録商標）」などの何らかのワードプロセッサ形式である。同様に、ファイル名の拡張子が、デジタルコンテンツ１２がオーディオ、ビデオ、および／またはマルチメディアファイルであることを示している場合、レンダリングアプリケーション３４は、これもワシントン州ＲｅｄｍｏｎｄにあるＭＩＣＲＯＳＯＦＴ（登録商標）Ｃｏｒｐｏｒａｔｉｏｎによって配布される「ＭＩＣＲＯＳＯＦＴ（登録商標）ＭＥＤＩＡ　ＰＬＡＹＥＲ（登録商標）」などの何らかのマルチメディアプレーヤ形式である。

【００７０】

勿論、本発明の精神および範囲を逸脱することなく、レンダリングアプリケーションを判別する他の方法も使用可能である。ただ１つの例として、デジタルコンテンツ１２は、暗号化されていない形式のメタデータ（すなわち、前述のヘッダ情報）を含むことが可能であり、このメタデータには、こうしたデジタルコンテンツ１２をレンダリングするのに必要なレンダリングアプリケーション３４のタイプに関する情報が含まれる。

【００７１】

こうしたレンダリングアプリケーション３４は、ファイル名に関連付けられたデジタルコンテンツ１２を検証し、こうしたデジタルコンテンツ１２が権利保護形式で暗号化されているかどうかを判定する（ステップ５０３、５０５）。保護されていない場合、デジタルコンテンツ１２は特別な作業の必要なくレンダリングできる（ステップ５０７）。保護されている場合、レンダリングアプリケーション３４は、暗号化されたデジタルコンテンツ１２から、ＤＲＭシステム３２がこうしたデジタルコンテンツ１２の再生に必要であるかどうかを判定する。したがって、こうしたレンダリングアプリケーション３４は、ユーザのコンピューティングデバイス１４に対して、ＤＲＭシステム３２を実行するように命令する（ステップ５０９）。次いでこうしたレンダリングアプリケーション３４は、デジタルコンテンツ１２を復号するためにこうしたＤＲＭシステム３２を呼び出す（ステップ５１１）。以下でより詳細に論じるように、ＤＲＭシステム３２は、ユーザがこうしたデジタルコンテンツ１２に関する有効なライセンス１６と、有効なライセンス１６のライセンス規則に従ってデジタルコンテンツ１２を再生する権利とを有する場合に限って、実際にデジタルコンテンツ１２を復号する。レンダリングアプリケーション３４によって、ＤＲＭシステム３２がいったん呼び出されると、こうしたＤＲＭシステム３２は、少なくとも

ユーザがこうしたデジタルコンテンツ１２を再生する権利を有するかどうかを判定する目的で、レンダリングアプリケーション３４からの制御を想定する（ステップ５１３）。

【００７２】

ＤＲＭシステム３２構成要素

本発明の一実施形態では、再度図４を参照すると、ＤＲＭシステム３２には、ライセンス評価器３６、ブラックボックス３０、ライセンス記憶域３８、および状態記憶域４０が含まれる。

【００７３】

ＤＲＭシステム３２構成要素－ライセンス評価器３６

ライセンス評価器３６は、とりわけ、要求されたデジタルコンテンツ１２に対応する１つ以上のライセンス１６を見つけ出し、こうしたライセンス１６が有効であるかどうかを判定し、こうした有効なライセンス１６のライセンス規則を再検討し、再検討したライセンス規則に基づいて、求められる方法で要求されたデジタルコンテンツ１２をレンダリングする権利を要求側ユーザが有しているかどうかを判定する。当然のことながら、ライセンス評価器３６は、ＤＲＭシステム３２内の信用される構成要素である。本開示では、「信用される」ということは、信用される要素がライセンス１６の権利記述に従ってデジタルコンテンツ１２の所有者の希望を実行すること、および不正であろうとなかろうと何らかの目的でこうした信用される要素をユーザが容易に変更できないことを、ライセンスサーバ２４（または任意の他の信用する（ｔｒｕｓｔｉｎｇ）要素）に納得させるということを意味する。

【００７４】

ライセンス評価器３６は、こうしたライセンス評価器３６が実際にライセンス１６を正しく評価することを保証するため、並びに、こうしたライセンス評価器３６が、ライセンス１６の実際の評価を省略する目的でユーザによって質が落とされるかそうでなければ修正されることがないことを保証するために、信用されるものでなければならない。したがって、ライセンス評価器３６は、ユーザがこうしたライセンス評価器３６へのアクセスを拒否されるような、保護または包囲された環境で実行される。勿論、本発明の精神および範囲を逸脱することなく、ライセンス評価器３６に関連した他の保護手段を使用することも可能である。

【００７５】

ＤＲＭシステム３２構成要素－ブラックボックス３０

第一に、また前述のように、ブラックボックス３０はＤＲＭシステム３２内で暗号化および復号機能を実行する。具体的に言えば、ブラックボックス３０は、ライセンス評価器３６と共に、ライセンス評価機能の一部として一定の情報を復号および暗号化するために動作する。さらに、ライセンス評価器３６が、ユーザが実際には要求されたデジタルコンテンツ１２を求められた方法でレンダリングする権利を有していると判定すると、ブラックボックス３０に、こうしたデジタルコンテンツ１２に関する復号鍵（ＫＤ）が与えられ、こうした復号鍵（ＫＤ）に基づいてこうしたデジタルコンテンツ１２を復号する機能を実行する。

【００７６】

ブラックボックス３０も、ＤＲＭシステム３２内の信用される構成要素である。具体的に言えば、ライセンスサーバ２４は、ブラックボックス３０がライセンス１６のライセンス規則に従っている場合にのみ復号機能を実行するものであることを信用し、こうしたブラックボックス３０が、ライセンス１６の実際の評価を省略する目的でユーザによって質が落とされるかそうでなければ修正された場合には、動作しないものであることを信用しなければならない。したがって、ブラックボックス３０も、ユーザがこうしたブラックボックス３０へのアクセスを拒否されるような、保護または包囲された環境で実行される。ここでも、本発明の精神および範囲を逸脱することなく、ブラックボックス３０に関連した他の保護手段を使用することが可能である。コンテンツサーバ２２およびライセンスサーバ２４と同様に、ＤＲＭシステム３２内のブラックボックス３０は、以下でより詳細に説

明するように、ライセンス１６を評価し、デジタルコンテンツ１２を復号するための復号鍵（ＫＤ）を取得するプロセスの一部として使用される固有の公開鍵／秘密鍵ペア（ＰＵ－ＢＢ、ＰＲ－ＢＢ）を有する。

【００７７】

ＤＲＭシステム３２構成要素－ライセンス記憶域３８

ライセンス記憶域３８は、対応するデジタルコンテンツ１２に関してＤＲＭシステム３２によって受け取られたライセンス１６を格納する。以下で説明するように、ライセンス記憶域３８それ自体は単にライセンス１６を格納するだけであり、ライセンス１６がそれぞれ既に組み込まれた信用構成要素を有しているため、信用される必要はない。本発明の一実施形態では、ライセンス記憶域３８は単に、ハードディスクドライブやネットワークドライブなどのドライブのサブディレクトリである。ただし、ライセンス記憶域３８は、こうしたライセンス記憶域３８が、ＤＲＭシステム３２にとって比較的便利な場所にライセンス１６を格納する機能を実行する限りは、本発明の精神および範囲を逸脱することなく、任意の他の形式で具体化することができる。

【００７８】

ＤＲＭシステム３２構成要素－状態記憶域４０

状態記憶域４０は、現在または以前にライセンス記憶域３８にあったライセンス１６に対応する状態情報を維持する機能を実行する。こうした状態情報は、ＤＲＭシステム３２によって作成され、必要に応じて状態記憶域４０に格納される。例えば、特定のライセンス１６が、対応する１ピースのデジタルコンテンツ１２の所定数のレンダリングのみを実行できる場合、状態記憶域４０は、こうしたライセンス１６に関連して実際に何回レンダリングが実行されたかについての状態情報を維持する。状態記憶域４０は、普通ならライセンス記憶域３８からライセンス１６を削除した後、対応する状態情報を状態記憶域４０から削除しようとする際に同じライセンス１６を取得することが有利なはずであるという状況を避けるために、ライセンス記憶域３８内にもはや存在しないライセンス１６に関する状態情報を維持し続ける。

【００７９】

状態記憶域４０も、格納された情報がユーザにとってより好ましい状態にリセットされないことを保証するために、信用されるものでなければならない。したがって、状態記憶域４０もまた同様に、ユーザがこうした状態記憶域４０へのアクセスを拒否されるような保護または包囲された環境で実行される。ここでも勿論、本発明の精神および範囲を逸脱することなく、状態記憶域４０に関連した他の保護手段を使用することが可能である。例えば、状態記憶域４０は、ＤＲＭシステム３２によってコンピューティングデバイス１４上に暗号化形式で格納することができる。

【００８０】

ＤＲＭシステム３２－コンテンツのレンダリング、パート２

図５を再度参照し、本発明の一実施形態でのコンテンツのレンダリングについて再度論じると、いったんＤＲＭシステム３２が呼び出し側のレンダリングアプリケーション３４からの制御を想定した場合、その後こうしたＤＲＭシステム３２は、ユーザが要求されたデジタルコンテンツ１２を求められる方法でレンダリングする権利を有するかどうかを判定するプロセスを開始する。具体的に言えば、ＤＲＭシステム３２は、ライセンス記憶域内で有効な実行可能化ライセンス（enabling license）１６を見つけ出す（ステップ５１５、５１７）か、またはライセンスサーバ２４から有効な実行可能なライセンス１６を獲得するよう試みる（すなわち、以下で考察し、図８に示されるように、ライセンス獲得機能を実行する）。

【００８１】

ここで図７を参照すると、第１のステップとして、こうしたＤＲＭシステム３２のライセンス評価器３６は、デジタルコンテンツ１２に対応する１つ以上の受け取られたライセンス１６の有無について、ライセンス記憶域３８をチェックする（ステップ６０１）。典型的には、以下で論じるように、ライセンス１６はデジタルファイル形式であるが、ライセ

ンス１６は、本発明の精神および範囲を逸脱することがなければ他の形式であってもよいことを理解されよう。典型的には、ユーザはこうしたライセンス１６なしにデジタルコンテンツ１２を受け取るが、デジタルコンテンツ１２は、本発明の精神および範囲を逸脱することがなければ、対応するライセンス１６と共に受け取ることができることも同様に理解されよう。

【００８２】

図３に関連して上記で論じたように、デジタルコンテンツ１２の各ピースは、こうしたデジタルコンテンツ１２（またはパッケージ１２ｐ）を識別するコンテンツＩＤ（またはパッケージＩＤ）、および暗号化されたデジタルコンテンツ１２を復号する復号鍵（ＫＤ）を識別する鍵ＩＤと共に、パッケージ１２ｐ内にある。コンテンツＩＤ（またはパッケージＩＤ）および鍵ＩＤは、暗号化されていない形式であることが好ましい。したがって、具体的に言えば、デジタルコンテンツ１２のコンテンツＩＤに基づいて、ライセンス評価器３６は、ライセンス記憶域３８内で、こうしたコンテンツＩＤへの適用性の識別を含むいずれかのライセンス１６を探す。特に、デジタルコンテンツ１２の所有者がこうしたデジタルコンテンツ１２に対していくつかの異なる種類のライセンス１６を指定した場合、およびユーザがこうしたライセンス１６のうち複数を取得した場合、複数のこうしたライセンス１６を見つけられることに留意されたい。実際に、ライセンス評価器３６がライセンス記憶域３８内で要求されたデジタルコンテンツ１２に対応するいずれかのライセンス１６を見つけられない場合、その後ＤＲＭシステム３２は、以下に記述するように、ライセンス獲得機能を実行することができる（図５のステップ５１９）。

【００８３】

ここで、ＤＲＭシステム３２が１ピースのデジタルコンテンツ１２をレンダリングするように要求されており、それに対応する１つ以上のライセンス１６がライセンス記憶域３８に存在すると想定する。本発明の一実施形態では、その後続いて、ＤＲＭシステム３２のライセンス評価器３６が、こうしたライセンス１６それぞれについて、こうしたライセンス１６それ自体が有効であるかどうかを判定する（図７のステップ６０３および６０５）。具体的に言えば、それぞれのライセンス１６には、ライセンス１６のコンテンツ２８に基づいたデジタル署名２６が含まれることが好ましい。当然のことながら、コンテンツ２８の質が落とされるかそうでなければ修正された場合、デジタル署名２６はライセンス１６と一致しない。したがって、ライセンス評価器３６は、デジタル署名２６に基づいて、コンテンツ２８がライセンスサーバ２４から受け取られた形式である（すなわち有効である）かどうかを判定することができる。ライセンス記憶域３８内に有効なライセンス１６が見つからない場合、その後ＤＲＭシステム３２はこうした有効なライセンス１６を取得するために、以下に述べるライセンス獲得機能を実行することができる。

【００８４】

それぞれの有効なライセンス１６について、１つ以上の有効なライセンス１６が見つかると想定すると、ＤＲＭシステム３２のライセンス評価器３６は、次に、こうした有効なライセンス１６がユーザに対して、所望の方法で対応するデジタルコンテンツ１２をレンダリングする権利を与える（すなわち実行可能化する）かどうかを判定する（ステップ６０７および６０９）。具体的に言えば、ライセンス評価器３６は、それぞれのライセンス１６の権利記述に基づいて、およびユーザがデジタルコンテンツ１２で何をしようとしているかに基づいて、要求側のユーザが要求されたデジタルコンテンツ１２を再生する権利を有するかどうかを判定する。例えば、こうした権利記述は、ユーザがデジタルコンテンツ１２を音声にレンダリングできるが、復号されたデジタルコピーにはレンダリングできないようにするものである。

【００８５】

当然のことながら、それぞれのライセンス１６の権利記述は、ユーザが誰であるか、ユーザがどこにいるか、ユーザがどのタイプのコンピューティングデバイス１４を使用しているか、どのレンダリングアプリケーション３４がＤＲＭシステム３２を呼び出しているか、日付、時刻などを含むいくつかの要因のいずれかに基づいて、ユーザがデジタルコンテ

ンツ１２を再生する権利を有するかどうかを指定する。さらに、権利記述はライセンス１６を所定の再生回数、または所定の再生回数時間などに限定することができる。このような場合、ＤＲＭシステム３２は、ライセンス１６に関する任意の状態情報（すなわち、デジタルコンテンツ１２が何回レンダリングされたか、デジタルコンテンツ１２がレンダリングされた合計時間など）を参照しなければならず、こうした状態情報は、ユーザのコンピューティングデバイス１４上にあるＤＲＭシステム３２の状態記憶域４０に格納される。

【００８６】

したがって、ＤＲＭシステム３２のライセンス評価器３６は、こうした有効なライセンス１６が求められる権利をユーザに与えるかどうかを判定するために、それぞれの有効なライセンス１６の権利記述を再検討する。これを実行する場合、ライセンス評価器３６はユーザが求められる権利を有するかどうかの判定を実行するために、ユーザのコンピューティングデバイス１４に対してローカルな他のデータを参照しなければならない。図４に見られるように、こうしたデータは、ユーザのコンピューティングデバイス（マシン）１４の識別（ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）４２およびその特定の態様、ユーザの識別４４およびその特定の態様、レンダリングアプリケーション３４の識別およびその特定の態様、システムクロック４６などを含むことが可能である。デジタルコンテンツ１２を求められる方法でレンダリングする権利をユーザに提供する有効なライセンス１６が見つからない場合、その後ＤＲＭシステム３２は、こうしたライセンス１６が実際に取得可能であれば、こうしたライセンス１６を取得するために、以下で説明するライセンス獲得機能を実行することができる。

【００８７】

勿論、いくつかのインスタンスでは、こうしたデジタルコンテンツ１２のコンテンツ所有者が、事実上こうした権利を認めないように指示しているため、ユーザは要求された方法でデジタルコンテンツ１２をレンダリングする権利を取得することができない。例えば、こうしたデジタルコンテンツ１２のコンテンツ所有者は、ユーザがテキスト文書を印刷できるようにするか、またはマルチメディア表示を暗号化されていない形式にコピーできるようにするためのライセンス１６を付与しないように指示することができる。本発明の一実施形態では、デジタルコンテンツ１２には、ライセンス１６を購入すると何の権利が使用できるのか、および使用可能なライセンス１６のタイプについてのデータが含まれる。ただし、１ピースのデジタルコンテンツ１２のコンテンツ所有者は、こうしたデジタルコンテンツ１２に使用可能なライセンス１６を変更することによって、こうしたデジタルコンテンツ１２に対して現在使用可能な権利を、いつでも変更可能であることを理解されよう。

【００８８】

ＤＲＭシステム３２―ライセンスの獲得

ここで図８を参照すると、実際にライセンス評価器３６がライセンス記憶域３８内に要求されるデジタルコンテンツ１２に対応する有効な実行可能化ライセンス１６を見つけなければ、その後ＤＲＭシステム３２はライセンスの獲得機能を実行することができる。図３に示されるように、デジタルコンテンツ１２の各ピースには、こうしたデジタルコンテンツ１２をレンダリングするためにライセンス１６を取得する方法に関して（すなわちライセンス獲得情報）、暗号化されていない形式で情報がパッケージングされる。

【００８９】

本発明の一実施形態では、こうしたライセンス獲得情報が、（とりわけ）使用可能なライセンス１６のタイプと、１つ以上の適切なライセンスサーバ２４にアクセス可能な１つ以上のインターネットＷｅｂサイトまたは他のサイト情報とを含むことが可能であり、こうしたライセンスサーバ２４のそれぞれが、実際にデジタルコンテンツ１２に対応するライセンス１６を発行することができる。勿論、ライセンス１６は、本発明の精神および範囲を逸脱することなく、他の方法で取得することができる。例えば、ライセンス１６は、電子掲示板でライセンスサーバ２４から取得することが可能であり、これはあるいは自分で

、または磁気ディスクまたは光ディスクなどに入れたファイル形式のものを定期的に郵送することでも取得可能である。

【００９０】

ライセンス１６を取得する場所が、実際にはネットワーク上のライセンスサーバ２４であると想定すると、その後ライセンス評価器３６はＷｅｂサイトまたは他のサイトの情報に基づいてこうしたライセンスサーバ２４へのネットワーク接続を確立し、その後こうした接続されたライセンスサーバ２４からのライセンス１６の要求を送信する（ステップ７０１、７０３）。具体的に言えば、ＤＲＭシステム３２がいったんライセンスサーバ２４にコンタクトすると、こうしたＤＲＭシステム３２は、適切なライセンス要求情報３６をこうしたライセンスサーバ２４に伝送する。本発明の一実施形態では、こうしたライセンス１６の要求情報３６は、とりわけ、

ＤＲＭシステム３２のブラックボックス３０の公開鍵（ＰＵ－ＢＢ）と、

ＤＲＭシステム３２のブラックボックス３０のバージョン番号と、

ブラックボックス３０を証明する証明機関からのデジタル署名での証明（証明には、実際に前述のブラックボックス３０の公開鍵およびバージョン番号を含むことができる）と、

デジタルコンテンツ１２（またはパッケージ１２ｐ）を識別するコンテンツＩＤ（またはパッケージＩＤ）と、

デジタルコンテンツ１２を復号するための復号鍵（ＫＤ）を識別する鍵ＩＤと、

要求されたライセンス１６のタイプ（実際に複数のタイプが使用可能な場合）と、

デジタルコンテンツ１２のレンダリングを要求したレンダリングアプリケーション３４のタイプなどを含むことができる。勿論、本発明の精神および範囲を逸脱することなく、これよりも多量または少量のライセンス１６の要求情報３６を、ＤＲＭシステム３２によって、ライセンスサーバ２４に伝送することができる。例えば、レンダリングアプリケーション３４のタイプに関する情報が不要である場合もあり、ユーザおよび／またはユーザのコンピューティングデバイス１４に関する追加情報が必要な場合もある。

【００９１】

いったんライセンスサーバ２４がＤＲＭシステム３２からライセンス１６の要求情報３６を受け取ると、その後ライセンスサーバ２４は、信用／認証および他の目的でいくつかのチェックを実行することができる。本発明の一実施形態では、こうしたライセンスサーバ２４が、証明機関のデジタル署名での証明をチェックして、これらが質を落とされたものかそうでなければ修正されたものかどうかを判定する（ステップ７０５、７０７）。そうであれば、ライセンスサーバ２４は要求情報３６に基づいて、どんなライセンス１６の付与も拒否する。ライセンスサーバ２４は、わかっている「不良」ユーザおよび／またはユーザのコンピューティングデバイス１４のリストを維持し、リストに掲載されたこうした不良ユーザおよび／または不良ユーザのコンピュータデバイス１４からの要求に基づいて、どんなライセンス１６の付与も拒否することができる。こうした「不良」リストは、本発明の精神および範囲を逸脱することなく、任意の適切な方法で編集することができる。

【００９２】

受け取った要求およびそれに関連付けられた情報に基づいて、さらに具体的にはライセンス要求情報にあるコンテンツＩＤ（パッケージＩＤ）に基づいて、ライセンスサーバ２４はコンテンツ鍵データベース２０（図１）を調査し、要求の基礎であるデジタルコンテンツ１２（またはパッケージ１２ｐ）に対応する記録を見つけることができる。前述のように、こうした記録には、こうしたデジタルコンテンツ１２の復号鍵（ＫＤ）、鍵ＩＤ、およびコンテンツＩＤが含まれる。さらにこうした記録は、デジタルコンテンツ１２について発行されるライセンス１６のタイプ、および各タイプのライセンス１６の条件に関するライセンスデータを含むことができる。あるいはこうした記録は、こうした追加情報を有する場所を示すポインタ、リンク、または参照を含むことができる。

【００９３】

前述のように、ライセンス１６は複数タイプが使用可能である。例えば、ライセンス料が比較的安い場合、レンダリング回数が限定されたライセンス１６が使用可能である。ライ

センス料が比較的高い場合、期限内に何回でもレンダリングできるライセンス１６が使用可能である。さらにライセンス料が高い場合、無期限に何回でもレンダリングできるライセンス１６が使用可能である。実際にライセンスサーバ２４は、本発明の精神および範囲を逸脱することなく、任意の種類のライセンス条件を有する任意のタイプのライセンス１６を考案および発行することができる。

【００９４】

本発明の一実施形態では、ライセンス１６の要求は、Ｗｅｂページなどを用いて、ライセンスサーバ２４からユーザのコンピューティングデバイス１４に伝送されたときに達成される。こうしたＷｅｂページには、ライセンス１６要求の基礎であるデジタルコンテンツ１２について、ライセンスサーバ２４から使用可能なすべてのタイプのライセンス１６に関する情報が含まれる。

【００９５】

本発明の一実施形態では、ライセンス１６を発行する前に、ライセンスサーバ２４がブラックボックス３０のバージョン番号をチェックして、こうしたブラックボックス３０が比較的新しいかどうかを判定する（ステップ７０９、７１１）。当然のことながら、ブラックボックス３０は、不正な目的を持った（すなわち、ライセンス１６なしにデジタルコンテンツ１２を不正にレンダリングするか、または対応するライセンス１６の条件から外れた）ユーザの攻撃から守られ、保護されることを意図するものである。ただし、実際にはこうした攻撃から完全に守られたシステムおよびソフトウェアデバイスは存在しないことを理解されよう。

【００９６】

当然のことながら、ブラックボックス３０が比較的新しい、すなわち比較的最近取得または更新されたものである場合、こうしたブラックボックス３０は、こうした不正ユーザからの攻撃をまともに受けてしまう可能性は少ない。信用の問題として、ライセンスサーバ２４がブラックボックス３０の比較的新しくないバージョン番号を含む要求情報３６を伴うライセンス要求を受け取ると、こうしたライセンスサーバ２４は、以下で説明するように、対応するブラックボックス３０が最新のバージョンにアップグレードされるまで、要求されたライセンス１６の発行を拒否することが好ましい。簡単に言えば、ライセンスサーバ２４は、こうしたブラックボックス３０が比較的新しくない限りは、こうしたブラックボックス３０を信用しないということである。

【００９７】

本発明のブラックボックス３０のコンテキストでは、「最新の」または「比較的新しい」という用語は、年数または用途に基づいてブラックボックス３０に信用を与える機能に適合する、本発明の精神および範囲を逸脱することのない任意の適切な意味を持つことが可能である。例えば、「最新の」は年数に応じて（すなわち１カ月未満）定義することができる。これに代わる例として、「最新の」は、ブラックボックス３０がデジタルコンテンツ１２を復号した回数に基づいて（すなわち復号インスタンスが２００回未満）定義することができる。さらに「最新の」は、各ライセンスサーバ２４が設定した方針に基づくものとすることが可能であり、１つのライセンスサーバ２４の「最新の」の定義が他のライセンスサーバ２４の定義と異なってもよく、さらにライセンスサーバ２４は、ライセンス１６が要求されたデジタルコンテンツ１２に応じて、あるいはとりわけ要求されたライセンス１６のタイプに応じて、「最新の」を様々に定義することもできる。

【００９８】

ライセンスサーバ２４が、ブラックボックス３０のバージョン番号またはこうしたブラックボックス３０が最新のものであることを示す他の印に納得したと想定すると、次いでライセンスサーバ２４は、そのライセンス１６の条件について、ユーザと交渉することになる（ステップ７１３）。あるいはライセンスサーバ２４は、ライセンス１６についてユーザと交渉した後、ブラックボックス３０のバージョン番号から、こうしたブラックボックスが最新であることを納得する（すなわち、ステップ７１３を実行した後、ステップ７１１を実行する）。勿論、交渉量は発行されるライセンス１６のタイプおよび他の要素に応

じて異なる。例えば、ライセンスサーバ２４が単に支払済みの使用無制限のライセンス１６を発行している場合、交渉の必要は殆どない。これに対して、ライセンス１６が、変動料金、スライド料金、ブレークポイント（ｂｒｅａｋ　ｐｏｉｎｔｓ）、およびその他詳細などの項目に基づくものである場合、こうした項目および詳細について、ライセンスサーバ２４とユーザとの間でライセンス１６を発行する前に解決しておく必要がある。

【００９９】

当然のことながら、状況に応じてライセンス交渉には、ユーザがそれ以上の情報をライセンスサーバ２４に提供する必要が生じる場合もある（例えば、ユーザ、ユーザのコンピューティングデバイス１４などに関する情報）。さらにライセンス交渉には、ユーザおよびライセンスサーバ２４が、とりわけ、相互に受け入れ可能な支払い手段（掛売り勘定、借方勘定、郵送小切手など）および／または支払い方法（即時支払い済み、一定期間に渡るなど）を決定する必要が生じる場合もある。

【０１００】

ライセンス１６のすべての条件について交渉し、ライセンスサーバ２４とユーザの両者によって合意される（ステップ７１５）と、ライセンスサーバ２４によってデジタルライセンス１６が生成されるが（ステップ７１９）、こうした生成されるライセンス１６は、少なくとも一部が、コンテンツ鍵データベース２０から取得される要求の基礎であるデジタルコンテンツ１２のライセンス要求、ブラックボックス３０公開鍵（ＰＵ－ＢＢ）、および復号鍵（ＫＤ）に基づくものである。本発明の一実施形態では、図９に示されるように、生成されるライセンス１６には、

ライセンス１６が適用されるデジタルコンテンツ１２のコンテンツＩＤと、

おそらく復号鍵（ＫＤ）によって暗号化されたデジタル権ライセンス（ＤＲＬ）４８（すなわち、ライセンス評価器３６が調べることのできる所定の形式で書かれたライセンス１６の権利記述または実際の条件）（すなわちＫＤ（ＤＲＬ））と、

ライセンス要求で受け取られるときに、ブラックボックス３０公開鍵（ＰＵ－ＢＢ）で暗号化されたデジタルコンテンツ１２の復号鍵（ＫＤ）（すなわち（ＰＵ－ＢＢ（ＫＤ））と、

（ＫＤ（ＤＲＬ））および（ＰＵ－ＢＢ（ＫＤ））に基づき、ライセンスサーバ２４秘密鍵で暗号化された、ライセンスサーバ２４からのデジタル署名（添付証明なし）（すなわち（Ｓ（ＰＲ－ＬＳ））と、

ライセンスサーバ２４が以前にコンテンツサーバ２２から取得した、ライセンスサーバ２４がライセンス１６を発行する権限をコンテンツサーバ２２から得ていることを示す証明（すなわち、（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））とが含まれる。

【０１０１】

当然のことながら、前述の要素およびおそらく他の要素は、デジタルファイルまたは何らかの他の適切な形式にパッケージングされる。さらに当然のことながら、ＤＲＬ４８またはライセンス１６の（ＰＵ－ＢＢ（ＫＤ））の質が落とされるかそうでなければ修正された場合、ライセンス１６のデジタル署名（Ｓ（ＰＲ－ＬＳ））は一致しなくなり、こうしたライセンス１６の有効性が証明されなくなる。そのため、ＤＲＬ４８は暗号化形式（すなわち、前述の（ＫＤ（ＤＲＬ））である必要はないが、こうした暗号化形式は場合によっては望ましいものであるため、本発明の精神および範囲を逸脱することなく使用することができる。

【０１０２】

デジタルライセンス１６がいったん作成されると、次にこうしたライセンス１６は要求者（すなわちユーザのコンピューティングデバイス１４にあるＤＲＭシステム３２）に対して発行される（図８のステップ７１９）。ライセンス１６は、要求が実行されたのと同じ経路（すなわちインターネットまたは他のネットワーク）を介して伝送されることが好ましいが、本発明の精神および範囲を逸脱することなく、他の経路を使用することができる。要求側ＤＲＭシステム３２は、受け取ると同時に、受け取ったデジタルライセンス１６を自動的にライセンス記憶域３８に配置することが好ましい（ステップ７２１）。

【０１０３】
ユーザのコンピューティングデバイス１４は、時に誤動作を起こす場合があり、こうしたユーザのコンピューティングデバイス１４上にあるＤＲＭシステム３２のライセンス記憶域３８に格納されたライセンス１６は、回復不可能なほどに失われる場合があることを理解されよう。したがって、ライセンスサーバ２４は発行されたライセンス１６のデータベース５０を維持し（図１）、こうしたライセンスサーバ２４は、発行されたライセンス１６のコピーまたは再発行（以下「再発行」という）をユーザに提供することが好ましいが、これはユーザが実際にこうした再発行を行う資格を与えられている場合である。前述のようにライセンス１６が回復不可能なほどに失われた場合、状態記憶域４０に格納されたこうしたライセンス１６に対応する状態情報も失われる可能性がある。こうして失われた状態情報は、ライセンス１６を再発行する際に考慮に入れなければならない。例えば、固定数のレンダリングライセンス１６は、比較的短い期間の後には、比例配分形式で正当に再発行されるが、比較的長い期間の後には再発行されない場合がある。

【０１０４】
ＤＲＭシステム３２―ブラックボックス３０のインストール／アップグレード前述のように、ライセンス１６の獲得機能の一部として、ユーザのコンピューティングデバイス１４が、比較的新しくない、すなわち比較的古いバージョン番号のブラックボックス３０を備えたＤＲＭシステム３２を有する場合、ライセンスサーバ２４は、ユーザからのライセンス１６の要求を拒否することができる。このような場合、こうしたＤＲＭシステム３２のブラックボックス３０をアップグレードした後、ライセンス獲得機能を続行できることが好ましい。勿論、ブラックボックス３０は、本発明の精神および範囲を逸脱することなく、その他のときにアップグレードしてもよい。

【０１０５】
ユーザのコンピューティングデバイス１４上にＤＲＭシステム３２をインストールするプロセスの一部として、固有でない「ライト（ｌｉｔｅ）」バージョンのブラックボックス３０が提供されることが好ましい。その後こうした「ライト」ブラックボックス３０は、１ピースのデジタルコンテンツ１２をレンダリングする前に、固有の正規バージョンにアップグレードされる。当然のことながら、各ＤＲＭシステム３２の各ブラックボックス３０が固有であれば、１つのブラックボックスに進入したセキュリティ侵害が、他のいずれかのブラックボックス３０で簡単に再現されてしまうことはない。

【０１０６】
ここで図１０を参照すると、ＤＲＭシステム３２は、（前述および図１に示されるように）ブラックボックスサーバ２６から要求するなどによって、固有のブラックボックス３０を取得する（ステップ９０１）。典型的には、こうした要求はインターネットを使用して実行されるが、本発明の精神および範囲を逸脱することなく、他のアクセス手段を使用することもできる。例えば、ブラックボックスサーバ２６への接続は、ローカルまたはリモートいずれかの直接接続であってよい。１つの固有のライトでないブラックボックス３０から、他の固有のライトでないブラックボックス３０へのアップグレードは、ＤＲＭシステム３２によっていつでも、例えばライセンスサーバ２４が、前述のようにブラックボックス３０が最新でないと考えたときなどに要求することが可能である。

【０１０７】
その後、ブラックボックスサーバ２６は、新しい固有のブラックボックス３０を生成する（ステップ９０３）。図３に示されるように、それぞれの新しいブラックボックス３０に、バージョン番号と、証明機関からのデジタル署名が付いた証明とが与えられる。ライセンス獲得機能に関連して前述したように、ブラックボックス３０のバージョン番号は、その相対的な年数および／または用途を示すものである。さらにライセンス獲得機能に関連して前述したように、証明機関からのデジタル署名が付いた証明は、ライセンスサーバ２４がブラックボックス３０を信用しているということの証明機関からの提供または証明メカニズムである。勿論、ライセンスサーバ２４は、実際に信用する価値のあるブラックボックス３０に関するこうした証明の発行について、証明機関を信用しなければならない。

実際には、ライセンスサーバ２４は特定の証明機関を信用するのではなく、こうした証明機関によって発行された証明の受け取りを拒む場合もある。例えば、特定の証明機関が、不正な証明の発行に携わっていることがわかった場合、信用することはできない。

【０１０８】

前述のように、ブラックボックスサーバ２６には、新しく生成された固有のブラックボックス３０と共に、新しい固有の公開鍵／秘密鍵ペア（ＰＵ－ＢＢ、ＰＲ－ＢＢ）が含まれることが好ましい（図１０のステップ９０３）。ブラックボックス３０の秘密鍵（ＰＲ－ＢＢ）はこうしたブラックボックス３０のみアクセス可能であり、こうしたブラックボックス３０を備えたＤＲＭシステム３２を有するコンピューティングデバイス１４およびそのユーザを含む、それ以外の世界に対しては隠されていてアクセスすることができないことが好ましい。

【０１０９】

殆どの隠し方式は、こうした隠し方式が実際に外部から秘密鍵（ＰＲ－ＢＢ）を隠す機能を実行する限りは、本発明の精神および範囲を逸脱することなく使用することができる。１つだけ例を挙げると、秘密鍵（ＰＲ－ＢＢ）をいくつかの２次構成要素に分割することが可能であり、それぞれの２次構成要素を固有に暗号化し、異なる場所に格納することができる。こうした状況では、こうした２次構成要素のすべてが組み合わせられて、秘密鍵（ＰＲ－ＢＢ）全体を作成することは決してないことが好ましい。

【０１１０】

本発明の一実施形態では、こうした秘密鍵（ＰＲ－ＢＢ）は、符号ベースの暗号化技法に従って暗号化される。具体的に言えば、こうした実施形態では、ブラックボックス３０の実際のソフトウェア符号（または他のソフトウェア符号）が暗号鍵として使用される。したがって、ブラックボックス３０の符号（または他のソフトウェア符号）の質が落とされるかそうでなければ修正された場合、例えばユーザが不正な目的でこうした秘密鍵（ＰＲ－ＢＢ）を復号することはできない。

【０１１１】

それぞれの新しいブラックボックス３０は新しい公開鍵／秘密鍵ペア（ＰＵ－ＢＢ、ＰＲ－ＢＢ）と共に送達されるが、こうした新しいブラックボックス３０には、ユーザのコンピューティングデバイス１４上にあるＤＲＭシステム３２に以前に送達された古いブラックボックス３０からの古い公開鍵／秘密鍵ペアへのアクセスも与えられることが好ましい（ステップ９０５）。したがって、以下でより詳細に論じるように、アップグレードされたブラックボックス３０は、こうした古い鍵ペアに従って生成された古いデジタルコンテンツ１２および古い対応するライセンス１６にアクセスする際に、依然として古い鍵ペアを使用することができる。

【０１１２】

ブラックボックスサーバ２６によって送達されるアップグレードされたブラックボックス３０は、ユーザのコンピューティングデバイス１４と緊密に結合または関連付けられていることが好ましい。したがって、アップグレードされたブラックボックス３０は、不正な目的のために複数のコンピューティングデバイス１４間で転送されるように動作可能ではない。本発明の一実施形態では、ブラックボックス３０の要求（ステップ９０１）の一部として、ＤＲＭシステム３２が、こうしたＤＲＭシステム３２に固有であり、および／またはユーザのコンピューティングデバイス１４に固有であるハードウェア情報を、ブラックボックスサーバ２６に提供し、ブラックボックスサーバ２６は、こうして提供されたハードウェア情報の一部に基づいて、ＤＲＭシステム３２用のブラックボックス３０を生成する。こうして生成された、アップグレードされたブラックボックス３０は、その後ユーザのコンピューティングデバイス１４上にあるＤＲＭシステム３２に送達され、インストールされる（ステップ９０７、９０９）。その後アップグレードされたブラックボックス３０が何らかの方法で他のコンピューティングデバイス１４に転送されると、転送されたブラックボックス３０は、こうした他のコンピューティングデバイス１４向けでないために、こうした他のコンピューティングデバイス１４上で要求されたどんなレンダリングも

実行できないことがわかる。
【０１１３】
新しいブラックボックス３０がＤＲＭシステム３２にいったんインストールされると、こうしたＤＲＭシステム３２は、ライセンス獲得機能または任意の他の機能を実行することができる。
【０１１４】
ＤＲＭシステム３２－コンテンツのレンダリング、パート３
ここで図６を参照し、ライセンス評価器３６が少なくとも１つの有効なライセンス１６を見つけ出し、こうした有効なライセンス１６のうち少なくとも１つが、求められる方法で対応するデジタルコンテンツ１２をレンダリングするのに必要な権利をユーザに提供する（すなわち実行可能にする）と想定すると、その後、ライセンス評価器３６はこうしたライセンス１６のうち１つを将来使用するために選択する（ステップ５１９）。具体的に言えば、要求されたデジタルコンテンツ１２をレンダリングするために、ライセンス評価器３６とブラックボックス３０が共同でこうしたライセンス１６から復号鍵（ＫＤ）を取得し、ブラックボックス３０が、デジタルコンテンツ１２を復号するためにこうした復号鍵（ＫＤ）を使用する。本発明の一実施形態では、前述のように、ライセンス１６から取得された復号鍵（ＫＤ）がブラックボックス３０公開鍵で暗号化され（ＰＵ－ＢＢ（ＫＤ））、ブラックボックス３０が、復号鍵（ＫＤ）を生成するために、こうした暗号化された復号鍵をその秘密鍵（ＰＲ－ＢＢ）で復号する（ステップ５２１、５２３）。ただし、本発明の精神および範囲を逸脱することなく、デジタルコンテンツ１２の復号鍵（ＫＤ）を取得する他の方法が使用可能である。
【０１１５】
いったんブラックボックス３０が、デジタルコンテンツ１２をレンダリングするために、デジタルコンテンツ１２の復号鍵（ＫＤ）とライセンス評価器３６からの許可を得ると、制御をレンダリングアプリケーション３４に返すことができる（ステップ５２５、５２７）。本発明の一実施形態では、その後、レンダリングアプリケーション３４がＤＲＭシステム３２／ブラックボックス３０を呼び出し、暗号化されたデジタルコンテンツ１２の少なくとも一部を、復号鍵（ＫＤ）に従って復号するためにブラックボックス３０に向けて送る（ステップ５２９）。ブラックボックス３０は、デジタルコンテンツ１２の復号鍵（ＫＤ）に基づいてデジタルコンテンツ１２を復号し、その後、ブラックボックス３０は、実際のレンダリングのために、復号されたデジタルコンテンツ１２をレンダリングアプリケーション３４に返す（ステップ５３３、５３５）。レンダリングアプリケーション３４は、本発明の精神および範囲を逸脱することなく、暗号化されたデジタルコンテンツ１２の一部またはデジタルコンテンツ１２全体のいずれかを、こうしたデジタルコンテンツ１２の復号鍵（ＫＤ）に基づいて復号するために、ブラックボックス３０に送信することができる。
【０１１６】
レンダリングアプリケーション３４が復号のためにデジタルコンテンツ１２をブラックボックス３０に送信するときに、ブラックボックス３０および／またはＤＲＭシステム３２は、最初にＤＲＭシステム３２に実行を要求したものと実際に同じレンダリングアプリケーション３４であることを確実にするために、こうしたレンダリングアプリケーション３４を認証することが好ましい（ステップ５３１）。そうでない場合は、レンダリング要求を１タイプのレンダリングアプリケーション３４に基づくものとし、実際には、別のタイプのレンダリングアプリケーション３４を使ってレンダリングすることによって、レンダリングの承認が不正に取得された可能性がある。認証が無事に実行され、ブラックボックス３０によってデジタルコンテンツ１２が復号されたと想定すると、その後レンダリングアプリケーション３４は、復号されたデジタルコンテンツ１２をレンダリングすることができる（ステップ５３３、５３５）。
【０１１７】
鍵トランザクションのシーケンス

ここで図１１を参照すると、本発明の一実施形態では、復号鍵（ＫＤ）を取得し、デジタルコンテンツ１２の要求されたピースのライセンス１６を評価するために（すなわち、図５～図６のステップ５１５～５２３を実行するために）、鍵トランザクションのシーケンスが実行される。主として、こうしたシーケンスでは、ＤＲＭシステム３２がライセンス１６から復号鍵（ＫＤ）を取得し、ライセンス１６およびデジタルコンテンツ１２から取得された情報を使用して双方の妥当性を認証または確認し、その後、実際にライセンス１６が求められる方法でデジタルコンテンツ１２をレンダリングするための権利を提供しているかどうかを判定する。提供している場合は、デジタルコンテンツ１２がレンダリング可能である。

【０１１８】

図９に示されるように、デジタルコンテンツ１２に関するそれぞれのライセンス１６が、
ライセンス１６が適用されるデジタルコンテンツ１２のコンテンツＩＤと、
おそらく復号鍵（ＫＤ）で暗号化されたデジタル権ライセンス（ＤＲＬ）４８（すなわちＫＤ（ＤＲＬ））と、
ブラックボックス３０公開鍵（ＰＵ－ＢＢ）で暗号化されたデジタルコンテンツ１２の復号鍵（ＫＤ）（すなわち（ＰＵ－ＢＢ（ＫＤ））と、
（ＫＤ（ＤＲＬ））および（ＰＵ－ＢＢ（ＫＤ））に基づき、ライセンスサーバ２４秘密鍵で暗号化された、ライセンスサーバ２４からのデジタル署名（すなわち（Ｓ（ＰＲ－ＬＳ））と、
ライセンスサーバ２４が事前にコンテンツサーバ２２から取得した証明（すなわち（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））とを含んでいることを念頭に置き、
さらに、図３に示されるように、デジタルコンテンツ１２を有するパッケージ１２ｐが、
こうしたデジタルコンテンツ１２のコンテンツＩＤと、
ＫＤによって暗号化されたデジタルコンテンツ１２（すなわち（ＫＤ（ＣＯＮＴＥＮＴ））と、
暗号化されていないライセンス獲得スクリプトと、
コンテンツサーバ２２秘密鍵（ＰＲ－ＣＳ）によって署名された、コンテンツサーバ２２公開鍵（ＰＵ－ＣＳ）を暗号化する鍵（ＫＤ）（すなわち（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））とを含んでいることも念頭に置くと、
本発明の一実施形態では、デジタルコンテンツ１２のライセンス１６のうち特定の１つに関して実行される鍵トランザクションの具体的シーケンスは、以下の通りである。

【０１１９】

１．ライセンス１６からの（ＰＵ－ＢＢ（ＫＤ））に基づき、ユーザのコンピューティングデバイス１４上にあるＤＲＭシステム３２のブラックボックス３０は、（ＫＤ）を取得するためにその秘密鍵（ＰＲ－ＢＢ）を適用する（ステップ１００１）。（ＰＲ－ＢＢ（ＰＵ－ＢＢ（ＫＤ））＝（ＫＤ））。これでブラックボックス３０は、難なくデジタルコンテンツ１２を復号するためにＫＤを使用することができるようになることが重要なので留意されたい。ただし、ライセンスサーバ２４は、ブラックボックス３０がそのように実行しないと信用していることも重要である。こうした信用は、こうしたブラックボックスの信頼性を証明するために、こうしたライセンスサーバ２４が証明機関からの証明に基づいてライセンス１６を発行したときに確立されたものである。したがって、以下で述べるように、ブラックボックス３０が最終ステップではなく初期ステップとして復号鍵（ＫＤ）を取得するのにもかかわらず、ＤＲＭシステム３２は、すべてのライセンス１６の妥当性検査および評価機能の実行を継続する。

【０１２０】

２．デジタルコンテンツ１２からの（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））に基づき、ブラックボックス３０は、（ＰＵ－ＣＳ）を取得するために新しく取得された復号鍵（ＫＤ）を適用する（ステップ１００３）。（ＫＤ（ＫＤ（ＰＵ－ＣＳ））＝（ＰＵ－ＣＳ））。さらに、ブラックボックス３０は、こうした署名およびこうしたデジタルコンテンツ１２／パッケージ１２ｐが有効であることをそれ自体が納得するために、署名（Ｓ（ＰＲ

－ＣＳ））に対するものとして（ＰＵ－ＣＳ）を適用することができる（ステップ１００５）。有効でない場合、プロセスは中止され、デジタルコンテンツ１２へのアクセスは拒否される。

【０１２１】

３．ライセンス１６からの（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））に基づき、ブラックボックス３０は、ライセンス１６を発行したライセンスサーバ２４が、そうする権限をコンテンツサーバ２２から得ていることを示す証明が有効であることをそれ自体が納得するために、新しく取得されたコンテンツサーバ２２公開鍵（ＰＵ－ＣＳ）を適用し（ステップ１００７）、その後、（ＰＵ－ＬＳ）を取得するために証明の内容を検証する（ステップ１００９）。有効でない場合、プロセスは中止され、ライセンス１６に基づいたデジタルコンテンツ１２へのアクセスは拒否される。

【０１２２】

４．ライセンス１６からの（Ｓ（ＰＲ－ＬＳ））に基づき、ブラックボックス３０は、ライセンス１６が有効であることをそれ自体が納得するために、新しく取得されたライセンスサーバ２４公開鍵（ＰＵ－ＬＳ）を適用する（ステップ１０１１）。有効でない場合、プロセスは中止され、ライセンス１６に基づいたデジタルコンテンツ１２へのアクセスは拒否される。

【０１２３】

５．すべての妥当性検査ステップが首尾よく終了し、ライセンス１６内のＤＲＬ４８が実際に復号鍵（ＫＤ）で暗号化されていると想定すると、次いでライセンス評価器３６は、ライセンス１６からライセンス条件（すなわちＤＲＬ４８）を取得するために、既に取得された復号鍵（ＫＤ）を、ライセンス１６から取得されたものとして（ＫＤ（ＤＲＬ））に適用する（ステップ１０１３）。勿論、ライセンス１６内のＤＲＬ４８が実際には復号鍵（ＫＤ）で暗号化されていない場合、ステップ１０１３は省略してもよい。次いでライセンス評価器３６はＤＲＬ４８を評価／調査し、求められる方法で対応するデジタルコンテンツ１２をレンダリングするために、ユーザのコンピューティングデバイス１４がライセンス１６内のＤＲＬ４８に基づいた権利を有しているかどうか（すなわちＤＲＬ４８がイネーブルされているかどうか）を判定する（ステップ１０１５）。ライセンス評価器３６がこのような権利が存在しないと判定すると、プロセスは中止され、ライセンス１６に基づいたデジタルコンテンツ１２へのアクセスは拒否される。

【０１２４】

６．最終的に、ライセンス１６を評価した結果、求められる方法で対応するデジタルコンテンツ１２をレンダリングするために、ユーザのコンピューティングデバイス１４がＤＲＬ４８の条件に基づいた権利を有するという肯定的な決定が下されると想定し、ライセンス評価器３６は、ブラックボックス３０が復号鍵（ＫＤ）に従って対応するデジタルコンテンツ１２をレンダリングできるということを、こうしたブラックボックス３０に通知する。その後ブラックボックス３０は、パッケージ１２ｐからデジタルコンテンツ１２を復号するために、復号鍵（ＫＤ）を適用する（すなわち（ＫＤ（ＫＤ（ＣＯＮＴＥＮＴ））＝（ＣＯＮＴＥＮＴ））（ステップ１０１７）。

【０１２５】

上記に指定された一連のステップが、ライセンス１６とデジタルコンテンツ１２との間で交互に生じるもの、すなわち「ピンポン」を表すことに留意されたい。こうしたピンポンは、デジタルコンテンツ１２がライセンス１６と緊密に結びついていることを保証するものであり、そこでは、妥当性検査および評価のプロセスは、デジタルコンテンツ１２とライセンス１６の両方が適切に発行された有効な形式で存在している場合に限って発生できるものである。さらに、ライセンス１６からコンテンツサーバ２２公開鍵（ＰＵ－ＣＳ）と、パッケージ１２ｐからデジタルコンテンツ２２を、復号された形式で（さらにおそらく、ライセンス１６からライセンス条件（ＤＲＬ４８）を復号された形式で）取得するためには、同じ復号鍵（ＫＤ）が必要であるため、これらのものも緊密に結びついている。署名の妥当性検査も、デジタルコンテンツ１２およびライセンス１６が、それぞれコンテ

ンツサーバ２２およびライセンスサーバ２４から発行されたものと同じ形式であることを保証するものである。したがって、ライセンスサーバ２４を迂回することによってデジタルコンテンツ１２を復号するのは不可能でなければ困難であり、また、デジタルコンテンツ１２またはライセンス１６を変更した後に復号するのも不可能でなければ困難である。

【０１２６】

本発明の一実施形態では、署名の妥当性検査、および特にライセンス１６の署名の妥当性検査は、以下のように別の方法で実行される。各ライセンス１６は、図９に示したように、ライセンスサーバ１６の秘密鍵（ＰＲ－ＬＳ）によって暗号化された署名ではなく、秘密ルート鍵（ＰＲ－Ｒ；Private Root Key－R）（図示せず）によって暗号化された署名を有し、各ＤＲＭシステム３２のブラックボックス３０には、秘密ルート鍵（ＰＲ－Ｒ）に対応する公開ルート鍵（ＰＵ－Ｒ）（これも図示せず）が含まれる。秘密ルート鍵（ＰＲ－Ｒ）は、ルートエンティティにしか知られておらず、ライセンスサーバ２４は、こうしたライセンスサーバ２４がライセンス１６を発行するためにルートエンティティで配置構成されている場合に限って、ライセンス１６を発行することができる。

【０１２７】

具体的に言えば、こうした実施形態では、

１．ライセンスサーバ２４がその公開鍵（ＰＵ－ＬＳ）をルートエンティティに提供し、

２．ルートエンティティが、ライセンスサーバ公開鍵（ＰＵ－ＬＳ）を、秘密ルート鍵（ＰＲ－Ｒ）で暗号化されたこうしたライセンスサーバ２４に返し（すなわち、（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））、

３．その後ライセンスサーバ２４が、ライセンスサーバ秘密鍵で暗号化された署名（Ｓ（ＰＲ－ＬＳ））を伴うライセンス１６を発行し、さらにライセンスにルートエンティティからの証明を添付する（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））。

【０１２８】

ＤＲＭシステム１８がこうして発行されたライセンス１６を妥当性検査する場合、次いでＤＲＭシステム１８は、

１．ライセンスサーバ公開鍵（ＰＵ－ＬＳ）を取得するために、添付された証明（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））に公開ルート鍵（ＰＵ－Ｒ）を適用し、

２．取得されたライセンスサーバ公開鍵（ＰＵ－ＬＳ）を、ライセンス１６の署名（Ｓ（ＰＲ－ＬＳ））に適用する。

【０１２９】

ルートエンティティが、ライセンスサーバ２４に対して、こうしたライセンスサーバ２４に証明（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））を提供することによってライセンス１６を発行する許可を与えたのと同様に、こうしたライセンスサーバ２４は、同様の証明を第２のライセンスサーバ２４に提供する（すなわち、（ＣＥＲＴ（ＰＵ－ＬＳ２）Ｓ（ＰＲ－ＬＳ１））ことが可能であり、これによって、第２のライセンスサーバもライセンス１６が発行できるようになることが重要である。ここで明らかなように、第２のライセンスサーバによって発行されたライセンス１６には、第１の証明（ＣＥＲＴ（ＰＵ－ＬＳ１）Ｓ（ＰＲ－Ｒ））と第２の証明（ＣＥＲＴ（ＰＵ－ＬＳ２）Ｓ（ＰＲ－ＬＳ１））とが含まれる。同様に、こうしたライセンス１６は、第１および第２の証明を介したチェーンに従って実行することで、妥当性が検査される。勿論、このチェーンでは他のリンクを追加し、掛け渡すことができる。

【０１３０】

前述の署名の妥当性検査プロセスの利点の１つは、ルートエンティティが定期的に秘密ルート鍵（ＰＲ－Ｒ）を変更できることであり、これによって同様に、それぞれのライセンスサーバ２４に新しい証明（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））を取得することも定期的に要求する。こうした新しい証明を得るための要件として、各ライセンスサーバはそれ自体をアップグレードすることが要求される場合がある。ブラックボックス３０の場合と同様に、ライセンスサーバ２４が比較的新しい、すなわち比較的最近アップグレードされたものであれば、ライセンスサーバ２４がまともに攻撃を受けてしまう可能性も少な

い。したがって、信用の問題として、各ライセンスサーバ２４は、署名の妥当性検査プロセスなどの適切なアップグレードトリガメカニズムを介して、定期的にアップグレードする必要があることが好ましい。勿論、本発明の精神および範囲を逸脱することなく、他のアップグレードメカニズムを使用することもできる。

【０１３１】

勿論、秘密ルート鍵（ＰＲ－Ｒ）を変更した場合は、各ＤＲＭシステム１８内の公開ルート鍵（ＰＵ－Ｒ）も変更しなければならない。こうした変更は、例えば通常のブラックボックス３０のアップグレード時に実行することが可能であり、実際には、ブラックボックス３０のアップグレードの実行が必要な場合もある。変更された公開ルート鍵（ＰＵ－Ｒ）は、潜在的に、古い秘密ルート鍵（ＰＲ－Ｒ）に基づいて発行された古いライセンス１６の署名の妥当性検査を妨害する可能性があるが、こうした妨害は、アップグレードされたブラックボックス３０に古い公開ルート鍵（ＰＵ－Ｒ）をすべて覚えておくように要求することで、最小限に抑えることができる。あるいはこうした妨害は、ライセンス１６の署名の妥当性検査を、例えばこうしたライセンス１６が、ＤＲＭシステム１８のライセンス評価器３６によって最初に評価されたときなどに１回だけ要求することで、最小限に抑えることができる。このような場合、署名の妥当性検査が実行されたかどうかに関する状態情報は編集しなければならず、こうした状態情報をＤＲＭシステム１８の状態記憶域４０に格納しなければならない。

【０１３２】

デジタル権ライセンス４８

本発明では、ライセンス評価器３６は、デジタル権ライセンス（ＤＲＬ）４８が求められた方法でデジタルコンテンツ１２の対応するピースのレンダリングを可能にするものであるかどうかを判定するために、こうしたＤＲＬ４８を、ライセンス１６の権利記述または条件として評価する。本発明の一実施形態では、ＤＲＬ４８は、ライセンサ（すなわちコンテンツ所有者）が任意のＤＲＬ言語で作成することができる。

【０１３３】

当然のことながら、ＤＲＬ４８を指定する方法は数多くある。したがって、任意のＤＲＬ言語には高度の柔軟性がなければならない。ただし、特定のライセンス言語でＤＲＬ４８のすべての側面を指定することは無理であり、こうした言語の作者が、特定のデジタルライセンサが望むすべての可能なライセンシングの側面を理解できるということも殆どあり得ない。さらに、高度なライセンス言語は不要であり、ライセンサが比較的単純なＤＲＬ４８を提供するのには邪魔になることさえある。しかし、ライセンサは、ＤＲＬ４８の指定方法を不必要に制限されるべきではない。同時にライセンス評価器３６は、いくつかの特定のライセンスに関する問題点について、ＤＲＬ４８からいつでも回答を得られるべきである。

【０１３４】

ここで図１２を参照すると、本発明では、ＤＲＬ４８は任意のライセンス言語で指定することができるが、言語識別子またはタグ５４を含んでいる。ライセンス１６を評価するライセンス評価器３６は、その後、こうした言語を識別するために言語タグ５４を再検討する予備ステップを実行し、その後、このように識別された言語でライセンス１６にアクセスするための適切なライセンス言語エンジン５２を選択する。当然のことながら、こうしたライセンス言語エンジン５２が存在し、ライセンス評価器３６にアクセス可能でなければならない。存在していない場合、言語タグ５４および／またはＤＲＬ４８には、こうした言語エンジン５２を取得するためのロケーション５６（典型的にはＷｅｂサイト）が含まれることが好ましい。

【０１３５】

典型的には、言語エンジン５２は実行可能ファイルまたはファイルセットの形式であり、ハードドライブなどのユーザのコンピューティングデバイス１４のメモリ内に常駐する。言語エンジン５２は、ＤＲＬ４８を直接調査するためにライセンス評価器３６を支援し、ライセンス評価器３６は、媒介などとして動作する言語エンジン５２を介して、間接的に

ＤＲＬ４８を調査する。実行される場合、言語エンジン５２は、ＲＡＭなどのユーザのコンピューティングデバイス１４のメモリ内にある作業スペースで動作する。ただし、本発明の精神および範囲を逸脱することなく、任意の他の形式の言語エンジン５２を使用することも可能である。

【０１３６】

任意の言語エンジン５２および任意のＤＲＬ言語は、以下で論じるように、ＤＲＬ４８が回答するであろうとライセンス評価器３６が予測している少なくともいくつかの特定の言語問題をサポートすることが好ましい。したがって、ライセンス評価器３６は任意の特定のＤＲＬ言語に結び付けられておらず、ＤＲＬ４８は任意の適切なＤＲＬ言語で作成することが可能であり、既存のライセンス評価器３６に対応する新しい言語エンジン５２を取得させることによって、既存のライセンス評価器３６は新しいライセンス言語で指定されたＤＲＬ４８を使用することができる。

【０１３７】

ＤＲＬ言語

それぞれＤＲＬ４８で具体化された２つのＤＲＬ言語の例を、以下に示す。第１に、ライセンス属性を指定する「単純な（ｓｉｍｐｌｅ）」ＤＲＬ４８が、ＤＲＬ言語で作成され、第２に、ＤＲＬ４８で指定されたスクリプトに従って機能を実施できる「スクリプト（ｓｃｒｉｐｔ）」ＤＲＬ４８が、ＤＲＬ言語で作成されている。ＤＲＬ言語で作成されているが、コードの各行の意味は、その語学上のおよび／または後に続く属性記述チャートに基づいていることは明らかであろう。

【０１３８】

Simple DRL 48:

```
〈LICENSE〉
〈DATA〉
〈NAME〉Beastie Boy′ s Play〈/NAME〉
〈ID〉39384〈/ID〉
〈DESCRIPTION〉Play the song 3 times〈/DESCRIPTION〉
〈TERMS〉〈/TERMS〉
〈VALIDITY〉
〈NOTBEFORE〉19980102 23:20:14Z〈/NOTBEFORE〉
〈NOTAFTER〉19980102 23:20:14Z〈/NOTAFTER〉
〈/VALIDITY〉
〈ISSUEDDATE〉19980102 23:20:14Z〈/ISSUEDDATE〉
〈LICENSORSITE〉http://www.foo.com〈/LICENSORSITE〉
〈CONTENT〉
〈NAME〉Beastie Boy′ s〈/NAME〉
〈ID〉392〈/ID〉
〈KEYID〉39292〈/KEYID〉
〈TYPE〉MS Encrypted ASF 2.0〈/TTYPE〉
〈/CONTENT〉
〈OWNER〉
〈ID〉939KDKD393KD〈/ID〉
〈NAME〉Universal〈/NAME〉
〈PUBLICKEY〉〈/PUBLICKEY〉
〈/OWNER〉
〈LICENSEE〉
〈NAME〉Arnold〈/NAME〉
〈ID〉939KDKD393KD〈/ID〉
〈PUBLICKEY〉〈/PUBLICKEY〉
〈/LICENSEE〉
```

〈PRINCIPAL TYPE==AND=〉
〈PRINCIPAL TYPE==OR=〉
〈PRINCIPAL〉
〈TYPE〉x86Computer〈/TYPE〉
〈ID〉3939292939d9e939〈/ID〉
〈NAME〉Personal Computer〈/NAME〉
〈AUTHTYPE〉Intel Authenticated Boot PC SHA-1 DSA512〈/AUTHTYPE〉
〈AUTHDATA〉29293939〈/AUTHDATA〉
〈/PRINCIPAL〉
〈PRINCIPAL〉
〈TYPE〉Application〈/TYPE〉
〈ID〉2939495939292〈/ID〉
〈NAME〉Window=s Media Player〈/NAME〉
〈AUTHTYPE〉Authenticode SHA-1〈/AUTHTYPE〉
〈AUTHDATA〉93939〈/AUTHDATA〉
〈/PRINCIPAL〉
〈/PRINCIPAL〉
〈PRINCIPAL〉
〈TYPE〉Person〈/TYPE〉
〈ID〉39299482010〈/ID〉
〈NAME〉Arnold Blinn〈/NAME〉
〈AUTHTYPE〉Authenticate user〈/AUTHTYPE〉
〈AUTHDATA〉¥¥redmond¥arnoldb〈/AUTHDATA〉
〈/PRINCIPAL〉
〈/PRINCIPAL〉
〈DRLTYPE〉Simple〈/DRLTYPE〉[the language tag 54]
〈DRLDATA〉
〈START〉19980102 23:20:14Z〈/START〉
〈END〉19980102 23:20:14Z〈/END〉

〈COUNT〉3〈/COUNT〉
〈ACTION〉PLAY〈/ACTION〉
〈/DRLDATA〉
〈ENABLINGBITS〉aaaabbbbccccdddd〈/ENABLINGBITS〉
〈/DATA〉
〈SIGNATURE〉
〈SIGNERNAME〉Universal〈/SIGNERNAME〉
〈SIGNERID〉9382ABK3939DKD〈/SIGNERID〉
〈HASHALGORITHMID〉MD5〈/HASHALGORITHMID〉
〈SIGNALGORITHMID〉RSA 128〈/SIGNALGORITHMID〉
〈SIGNATURE〉xxxyyyxxxyyyxxxyyy〈/SIGNATURE〉
〈SIGNERPUBLICKEY〉〈/SIGNERPUBLICKEY〉
〈CONTENTSIGNEDSIGNERPUBLICKEY〉〈/CONTENTSIGNEDSIGNERPUBLICKEY〉
〈/SIGNATURE〉
〈/LICENSE〉

Script DRL 48:

〈LICENSE〉
〈DATA〉
〈NAME〉Beastie Boy′ s Play〈/NAME〉
〈ID〉39384〈/ID〉
〈DESCRIPTION〉Play the song unlimited〈/DESCRIPTION〉
〈TERMS〉〈/TERMS〉
〈VALIDITY〉
〈NOTBEFORE〉19980102 23:20:14Z〈/NOTBEFORE〉
〈NOTAFTER〉19980102 23:20:14Z〈/NOTAFTER〉
〈/VALIDITY〉
〈ISSUEDDATE〉19980102 23:20:14Z〈/ISSUEDDATE〉
〈LICENSORSITE〉http://www.foo.com〈/LICENSORSITE〉
〈CONTENT〉

〈NAME〉Beastie Boy′ s〈/NAME〉
〈ID〉392〈/ID〉
〈KEYID〉39292〈/KEYID〉
〈TYPE〉MS Encrypted ASF 2.0〈/TTYPE〉
〈/CONTENT〉
〈OWNER〉
〈ID〉939KDKD393KD〈/ID〉
〈NAME〉Universal〈/NAME〉
〈PUBLICKEY〉〈/PUBLICKEY〉
〈/OWNER〉
〈LICENSEE〉
〈NAME〉Arnold〈/NAME〉
〈ID〉939KDKD393KD〈/ID〉
〈PUBLICKEY〉〈/PUBLICKEY〉
〈/LICENSEE〉
〈DRLTYPE〉Script〈/DRLTYPE〉[the language tag 54]
〈DRLDATA〉
function on_enable(action,args)as boolean
result=False
if action=" PLAY" then
result=True
end if
on_action=False
end function
...
〈/DRLDATA〉
〈/DATA〉
〈SIGNATURE〉
〈SIGNERNAME〉Universal〈/SIGNERNAME〉

〈SIGNERID〉9382〈/SIGNERID〉
〈SIGNERPUBLICKEY〉〈/SIGNERPUBLICKEY〉
〈HASHID〉MD5〈/HASHID〉
〈SIGNID〉RSA 128〈/SIGNID〉
〈SIGNATURE〉xxxyyyxxxyyyxxxyyy〈/SIGNATURE〉
〈CONTENTSIGNEDSIGNERPUBLICKEY〉〈/CONTENTSIGNEDSIGNERPUBLICKEY〉
〈/SIGNATURE〉
〈/LICENSE〉

【０１３９】
上記で指定した２つのＤＲＬ４８では、リストされた属性の説明およびデータタイプは次の通りである。
【０１４０】
【表１】

属　性	説　明	ﾃﾞｰﾀﾀｲﾌﾟ
Id	ライセンスのID	GUID
Name	ライセンスの名前	文字列
Content Id	コンテンツのID	GUID
Content Key Id	コンテンツの暗号鍵用のID	GUID
Content Name	コンテンツの名前	文字列
Content Type	コンテンツのタイプ	文字列
Owner Id	コンテンツの所有者のID	GUID
Owner Name	コンテンツの所有者の名前	文字列
Owner Public Key	コンテンツの所有者用の公開鍵。Base64で符号化されたコンテンツの所有者用の公開鍵。	文字列
Licensee Id	ライセンスを取得する人物のID。nullも可能。	GUID
Licensee Name	ライセンスを取得する人物の名前。nullも可能。	文字列
Licensee Public Key	ライセンシーの公開鍵。Base64で符号化されたライセンシーの公開鍵。nullも可能。	文字列
Description	人間が読み取り可能な簡単なライセンス記述。	文字列
Terms	ライセンスの法的条件。法律文が記載されたWebページを指すポインタの場合もある。	文字列
Validity Not After	ライセンスの有効期限満了日	日付
Validity Not Before	ライセンスの有効期限開始日	日付
Issued Date	ライセンスが発行された日付	日付
DRL Type	DRLのタイプ。例には「SIMPLE」または「SCRIPT」が含まれる。	文字列
DRL Data	DRL特有のデータ	文字列
Enabling Bits	実際のコンテンツへのアクセスを可能にするビット。これらのビットの解釈はアプリケーションによって異なるが、典型的にはコンテンツを復号するための秘密鍵。このデータはBase64で符号化される。これらのビットは個々のマシンの公開鍵を使用して暗号化されることに留意。	文字列
Signer Id	ライセンスに署名する人物のID	GUID
Signer Name	ライセンスに署名する人物の名前	文字列
Signer Public Key	ライセンスに署名する人物の公開鍵。 Base64で符号化された署名者用の公開鍵。	文字列
Content　Signed Singer Public Key	コンテンツサーバ秘密鍵によって署名されたライセンスに署名する人物の公開鍵。 この署名を検証するための公開鍵は、コンテンツ内で暗号化される。Base64で符号化されている。	文字列
Hash Alg Id	ハッシュの生成に使用されるアルゴリズム。「MD5」などの文字列である。	文字列
Signature Alg Id	署名の生成に使用されるアルゴリズム。 「RSA 128」などの文字列である。	文字列
Signature	データの署名。Base64で符号化されたデータ。	文字列

【０１４１】

メソッド

前述のように、任意の言語エンジン５２および任意のＤＲＬ言語は、デジタルライセンス評価器３６が、任意のＤＲＬ４８が回答してくれると予想する少なくともいくつかの特有のライセンス問題をサポートしていることが好ましい。このようにサポートされた問題には、本発明の精神および範囲を逸脱することなく、前述の２つのＤＲＬ４８の例で使用された用語に適合する任意の問題が含まれることからすると、本発明の一実施形態では、こ

のようにサポートされた問題または「メソッド」には、以下のように、「アクセスメソッド」、「ＤＲＬメソッド」、および「使用可能化メソッド」が含まれる。

【０１４２】

アクセスメソッド

アクセスメソッドは、トップレベルの属性についてＤＲＬ４８を照会する際に使用される。

【０１４３】

ＶＡＲＩＡＮＴ　ＱｕｅｒｙＡｔｔｒｉｂｕｔｅ（ＢＳＴＲ　ｋｅｙ）

有効な鍵には、それぞれＢＳＴＲ　Ｖａｒｉａｎｔを返す、Ｌｉｃｅｎｓ．Ｎａｍｅ、Ｌｉｃｅｎｓｅ．Ｉｄ、Ｃｏｎｔｅｎｔ．Ｎａｍｅ、Ｃｏｎｔｅｎｔ．Ｉｄ、Ｃｏｎｔｅｎｔ．Ｔｙｐｅ、Ｏｗｎｅｒ．Ｎａｍｅ、Ｏｗｎｅｒ．Ｉｄ、Ｏｗｎｅｒ．ＰｕｂｌｉｃＫｅｙ、Ｌｅｃｅｎｓｅｅ．Ｎａｍｅ、Ｌｉｃｅｎｓｅｅ．Ｉｄ、Ｌｉｃｅｎｓｅｅ．ＰｕｂｌｉｃＫｅｙ、Ｄｅｓｃｒｉｐｔｉｏｎ、およびＴｅｒｍｓと、それぞれＤａｔｅ　Ｖａｒｉａｎｔを返す、Ｉｓｓｕｅｄ、Ｖａｌｉｄｉｔｙ．Ｓｔａｒｔ、およびＶａｌｉｄｉｔｙ．Ｅｎｄとが含まれる。

【０１４４】

ＤＲＬメソッド

以下のＤＲＬメソッドの実施は、ＤＲＬ４８によって異なる。多くのＤＲＬメソッドには、ＤＲＬ４８でより高度な情報を通信するように意図された、「ｄａｔａ」とラベル付けされたバリアントパラメータ（a variant parameter）が含まれる。これは主に、将来の拡張性のために存在している。

【０１４５】

Ｂｏｏｌｅａｎ　ＩｓＡｃｔｉｖａｔｅｄ（Ｖａｒｉａｎｔ　ｄａｔａ）

このメソッドは、ＤＲＬ４８／ライセンス１６がアクティベートされているかどうかを示すＢｏｏｌｅａｎを返す。アクティベートされたライセンス１６の例が、初回再生時に４８時間のみアクティブな限定付き動作ライセンス１６である。

【０１４６】

Ａｃｔｉｖａｔｅ（Ｖａｒｉａｎｔ　ｄａｔａ）

このメソッドは、ライセンス１６をアクティベートするのに使用される。ライセンス１６は、いったんアクティベートされると非アクティベートすることができない。

【０１４７】

Ｖａｒｉａｎｔ　ＱｕｅｒｙＤＲＬ（Ｖａｒｉａｎｔ　ｄａｔａ）

このメソッドは、より高度なＤＲＬ４８と通信するのに使用される。これは、ＤＲＬ４８機能セットの将来の拡張性のためのものである。

【０１４８】

Ｖａｒｉａｎｔ　ＧｅｔＥｘｐｉｒｅｓ（ＢＳＴＲ　ａｔｃｉｏｎ，Ｖａｒｉａｎｔ　ｄａｔａ）

このメソッドは、パスインアクション（passed-in action）に関して、ライセンス１６の満了日を返す。返り値（ｒｅｔｕｒｎ　ｖａｌｕｅ）がＮＵＬＬの場合、ライセンス１６は決して満了しないか、またはアクティベートされていないためにまだ満了日がないなどである。

【０１４９】

Ｖａｒｉａｎｔ　ＧｅｔＣｏｕｎｔ（ＢＳＴＲ　ａｔｃｉｏｎ，Ｖａｒｉａｎｔ　ｄａｔａ）

このメソッドは、残されたパスインアクションの動作数を返す。ＮＵＬＬが返された場合、動作は何回でも無制限に実行できる。

【０１５０】

Ｂｏｏｌｅａｎ　ＩｓＥｎａｂｌｅｄ（ＢＳＴＲ　ａｃｔｉｏｎ，　Ｖａｒｉａｎｔ　ｄａｔａ）

このメソッドは、ライセンス１６が要求されたアクションを現時点でサポートしているか

どうかを示す。
【０１５１】
Ｂｏｏｌｅａｎ　ＩｓＳｕｎｋ（ＢＳＴＲ　ａｃｔｉｏｎ，　Ｖａｒｉａｎｔｄａｔａ）
このメソッドは、ライセンス１６に対する支払いが行われたかどうかを示す。前払いされたライセンス１６がＴＲＵＥを返すのに対して、使用されたときに徴収するライセンス１６などのまだ支払われていないライセンス１６は、ＦＡＬＳＥを返す。
【０１５２】
使用可能化メソッド
これらのメソッドは、復号コンテンツで使用するためにライセンス１６を使用可能にする際に使用される。
【０１５３】
Ｂｏｏｌｅａｎ　Ｖａｌｉｄａｔｅ（ＢＳＴＲ　ｋｅｙ）
このメソッドは、ライセンス１６の妥当性を検査する際に使用される。パスイン鍵は、ライセンス１６の署名の妥当性検査に使用される対応するデジタルコンテンツ１２に関して、復号鍵（ＫＤ）によって暗号化された、ブラックボックス３０公開鍵（ＰＵ－ＢＢ）である（すなわち（ＫＤ（ＰＵ＝ＢＢ））。返り値ＴＲＵＥは、ライセンス１６が有効であることを示す。返り値ＦＡＬＳＥは無効を示す。
【０１５４】
ｉｎｔ　ＯｐｅｎＬｉｃｅｎｓｅ　１６（ＢＳＴＲ　ａｃｔｉｏｎ，ＢＳＴＲｋｅｙ，Ｖａｒｉａｎｔ　ｄａｔａ）
このメソッドは、復号された使用可能化ビットへアクセスする準備を整えるのに使用される。パスイン鍵（ＫＤ（ＰＵ＝ＢＢ））は、上記の通りである。返り値０は成功したことを示す。その他の返り値も定義可能である。
【０１５５】
ＢＳＴＲ　ＧｅｔＤｅｃｒｙｐｔｅｄＥｎａｂｌｉｎｇＢｉｔｓ（ＢＳＴＲ　ａｃｔｉｏｎ，Ｖａｒｉａｎｔ　ｄａｔａ）
Ｖａｒｉａｎｔ　ＧｅｔＤｅｃｒｙｐｔｅｄＥｎａｂｌｉｎｇＢｉｔｓＡｓＢｉｎａｒｙ（ＢＳＴＲ　ａｃｔｉｏｎ，Ｖａｒｉａｎｔ　Ｄａｔａ）
これらのメソッドは、復号された形の使用可能化ビットへのアクセスに使用される。いくつかの理由のいずれかによって成功しない場合、ｎｕｌｌ文字列またはｎｕｌｌバリアントが返される。
【０１５６】
ｖｏｉｄＣｌｏｓｅＬｉｃｅｎｓｅ（ＢＳＴＲ　ａｃｔｉｏｎ，Ｖａｒｉａｎｔ　ｄａｔａ）
このメソッドは、パスインアクションを実行するために使用可能化ビットへのアクセスのロックを解除するのに使用される。いくつかの理由のいずれかによって成功しない場合、ｎｕｌｌ文字列が返される。
【０１５７】
ヒューリスティックス（heuristics）
前述のように、デジタルコンテンツ１２の同じピースについて複数のライセンス１６が存在する場合、将来の使用に備えてライセンス１６のうち１つを選択しなければならない。上記のメソッドを使用して、こうした選択を行うために以下のヒューリスティックスを実施することができる。具体的に言えば、１ピースのデジタルコンテンツ１２上でアクション（例えばＡＰＬＡＹ@）を実行するには、以下のステップを実行することができる。
【０１５８】
１．デジタルコンテンツ１２の特定のピースに適用するすべてのライセンス１６を取得する。
２．アクションを実行可能にしない各ライセンス１６でＩｓＥｎａｂｌｅｄ関数を呼び出して、こうしたライセンス１６を消去する。
３．アクティブでない各ライセンス１６でＩｓＡｃｔｉｖａｔｅｄを呼び出して、こうし

たライセンス１６を消去する。
４．前払いされていない各ライセンス１６でＩｓＳｕｎｋを呼び出して、こうしたライセンス１６を消去する。
５．いずれかのライセンス１６が残っている場合は、これを使用する。再生回数限定ライセンス１６を使用する前に、特に、再生回数無制限ライセンス１６に満了日がある場合は、再生回数無制限ライセンス１６を使用する。たとえ選択の費用効果が低い場合でも、ユーザは既に獲得された特有のライセンス１６をいつでも選択することができるはずである。したがってユーザは、おそらくＤＲＭシステム３２に対して明らかでない基準に基づいて、ライセンス１６を選択することができる。
６．ライセンス１６が残っていない場合は、その旨を示すステータスを返す。その後ユーザには、
前払いされていないライセンス１６が使用可能であれば、これを使用すること、
ライセンス１６が使用可能であれば、これをアクティベートすること、および／または
ライセンスサーバ２４からのライセンス獲得を実行すること、
というオプションが与えられることになる。
【０１５９】
コンテンツ保護技法－ビデオカード
本発明のＤＲＭアーキテクチャ１０では、権利が保護されたコンテンツ１２が暗号化形式で送達され、対応するライセンス１６に指定された権利に従う場合にのみ復号される。当然のことながら、勿論、ライセンス１６に従って実行可能でない限り、復号された形式のコンテンツ１０が取得できないことを確実にするために、多くの対策が講じられる。したがって、復号されたコンテンツ１２を受け取る各モジュールが、確実に動作することが信用できることを保証し、「コンテンツ泥棒」などの無法なエンティティに対してこうした復号されたコンテンツ１２を提供しないように、例えばパス認証が使用できる。こうしたパス認証については、２０００年3月１５日出願の「Ｒｅｌｅａｓｉｎｇ　ＤｅｃｒｙｐｔｅｄＤｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ　Ｔｏ　Ａｎ　ＡｕｔｈｅｎｔｉｃａｔｅｄＰａｔｈ」という名称で、参照によりその全体が本明細書に組み込まれた、米国特許出願第０９／５２５５１０号に、より詳細に記載されている。
【０１６０】
ただし、復号されたコンテンツ１２または少なくともその一部は、こうした復号されたコンテンツ１２をレンダリングする通常の過程において、バッファおよび他のメモリデバイスに必ず格納されることを理解されよう。より具体的に言えば、こうしたバッファ内にある復号されたコンテンツ１２は、コンテンツ泥棒がそれほど苦労をせずに取得できてしまう。
【０１６１】
特にビデオコンテンツなどのコンテンツ１２の場合、および図１４に示されるように、こうしたコンテンツ１２は、復号されると最終的にビデオカード６０に格納される。具体的に言えば、当然のことながら、ビデオデータは、復号および／または圧縮解除された後、モニタ６４などに送信されるビデオ信号を生成するためにビデオカード６０によって使用される前に、ビデオカード６０上のビデオＲＡＭ（ＶＲＡＭ）６２に書き込まれる。ビデオカードの動作は関係者に知られているかまたは明らかであるため、本明細書で詳細に論じる必要はない。ビデオカード６０のＶＲＡＭ６２であっても、ビデオデータは、こうしたＶＲＡＭ６２からのこうしたビデオデータを読み取るためのハードウェアおよび／またはソフトウェアを使用しているコンテンツ泥棒によって盗用される可能性があることが重要である。そこでこうしたＶＲＡＭ６２は、コンテンツ泥棒にとって、コアＤＲＭシステム３２の機能に関わらず品質の良いビデオデータを盗用するための手段となる。
【０１６２】
コンテンツ保護技法－ビデオカード－書込み専用ＶＲＡＭ
したがって、本発明の一実施形態では、ビデオカード６０上のＶＲＡＭ６２は、ビデオカード６０それ自体に関する以外は書込み専用であるように構成されている。コンテンツ泥

棒などのビデオカード６０のいかなる外部エンティティも、ＶＲＡＭ６２上にあるこうしたビデオデータを読み取ることはできない。こうした構成は、ＤＲＭシステム３２およびそれによって制御された保護されたコンテンツ１２に関してのみ適用可能であるか、または保護されているかまたは保護されていないすべてのコンテンツに関して適用可能である。

【０１６３】

前者の場合、保護されたコンテンツ１２は、書込み専用機能を実施するためのビデオカード６０およびＶＲＡＭ６２への適切な信号を伴うことが可能である。こうした信号は、例えばＤＲＭシステム３２またはレンダリングアプリケーション３４からのハードウェアまたはソフトウェア信号であってよく、関係者に知られているかまたは明らかであるため、本明細書で詳細に論じる必要はない。したがって、本発明の精神および範囲を逸脱することなく、任意の適切な信号を使用することができる。後者の場合、結果的には、たとえ合法的な意図を有する人物またはプログラムであっても、ビデオカード上のＶＲＡＭ６２からは一切何も読み取ることができなくなる。

【０１６４】

本発明の一実施形態では、書込み専用ＶＲＡＭ６２は、ＶＲＡＭ６２でホストされる１つ以上の書込み専用バッファを作成することによって、ビデオカード６０内で実施される。最も単純な場合、各書込み専用バッファは、１次サーフェスを介して表示されるビットマップされた２次ビデオサーフェスであってよい。ビットマップデータは各バッファに書き込むことができるが、データを読み取ると、黒塗り、カラーキー、ナンセンス、雑音などが返される。

【０１６５】

書込み専用にするために、本発明のビデオカード６０は、保護された画面領域を含むピクセルを読み取る他の方法を一切提供していない。例えば、保護された画面領域へのアクセスを提供する別のピクセル読取り動作が一切ない。あるいは、既存のメカニズムを使用してピクセルを読み取ると、黒塗り、カラーキー、ナンセンス、雑音などが返される。

【０１６６】

さらに、書込み専用ＶＲＡＭ６２は、各書込み専用バッファのコンテンツが解放されたときには消去されるかまたはゼロとなるのに必要な機能を、ビデオカード６０に与えることによって、ビデオカード６０で実施される。したがって、こうした書込み専用バッファは、解放された後で上書きされる前に、攻撃プロセスによって読み取られることはない。

【０１６７】

本方式は、本発明の精神および範囲を逸脱することなく、他のビデオ処理アーキテクチャにも等しく適用することができる。例えば、ビデオカード６０が圧縮解除アクセラレーションをサポートしている場合、同様の規則が適用される。具体的に言えば、こうしたビデオカード６０上でビデオアクセラレータと通信している各バッファは書き込み専用であり、これにレンダリングされるビデオを他の手段によって読み取ることはできない。

【０１６８】

コンテンツ保護技法－ビデオカード－認証

勿論、ＤＲＭシステム３２は、ビデオカード６０およびその上にあるＶＲＡＭ６２が、こうしたビデオカード６０上にあるこうしたＶＲＡＭ６２が本発明に従って書き込み専用であるという点で信用できるものであることを、それ自体が納得できなければならない。したがってビデオカード６０は、書込み専用ＶＲＡＭ６２を有するものとして、それ自体をこうしたＤＲＭシステム３２に対して認証できるものでなければならない。

【０１６９】

ＤＲＭシステム３２は、ＶＲＡＭ６２／ビデオバッファが実際に書き込み専用であることの確実な保証を、時折のリードバックチェックおよび他の標準的なデバッグ防止技術を介して提供できることが想定される。ただし、こうしたチェックでは、保護されたビデオデータが、例えば二重マッピングメモリ、非保護メモリへのビット転送、Ｒｅａｄ　Ｐｉｘｅｌ（ピクセル読取り）コマンドなどの何らかの他のメカニズムによって使用される可能

性は否定できない。

【０１７０】

認証に関連して発生する難点の１つが、ビデオカード製造業者がこうした認証の実施を必ずしも希望していないという点である。具体的に言えば、製造業者のビデオカードを使用して実際にコンテンツ泥棒などがビデオデータを入手できる場合、こうしたカードはさらに魅力的かつ市場性の高いものとなる。すると、本発明の方法を遵守してコンテンツ保護を実施する合法的で正直なビデオカード製造業者は市場シェアを失い、非合法非遵守のビデオカード製造業者にその地位を譲ることになる。したがって認証は、こうした難点があっても達成しなければならないものである。

【０１７１】

以下に、こうした認証を可能にするためのいくつかのメカニズムについて説明する。

【０１７２】

合法的デバイス

本発明の一実施形態では、ビデオカード６０は、１つ以上の知的所有権（特許権、著作権、商標、営業上の秘密など）によって法的に保護された１つ以上の要素６５を備えることによる、一般に受動的な方法で、ＤＲＭシステム３２に対してそれ自体を認証し、各要素６５はビデオカード６０に組み込まれるものとする。したがって、権利が保護された要素６５を備えたビデオカード６０の製造を希望する製造業者は、そのように実行するためのライセンスを取得し、とりわけ、権利が保護された要素６５を備えたビデオカード６０を製造する過程で、ある所定のライセンスタイプの規則に従わなければならず、ここで最も重要な点は、ビデオカード上のＶＲＡＭ６２が上記の方法によって書込み専用となっていることである。当然のことながら、こうした実施形態では、ＤＲＭシステム３２に、関連付けられたビデオカード６０が準拠したものであることを積極的に判定する手段がない。

【０１７３】

本発明の同様の実施形態では、ビデオカード６０は、１つ以上の前述の知的所有権（特許権、著作権、商標、営業上の秘密など）によって保護された１つ以上の前述の要素６５を組み込むことによって、より自発的な方法で、ＤＲＭシステム３２に対してそれ自体を認証するが、ここで要素６５は、要求時に提供されるか、あるいはＤＲＭシステム３２、レンダリングアプリケーション３４、および／またはコンピューティングシステム１４上にある他のエンティティに、適切なトークン６７を要求した時点で提供される。

【０１７４】

したがって、保護される対象は、デジタル信号を提供するハードウェアまたはソフトウェア、あるいはそれ自体が提供されるソフトウェア構造体であってよい。要素６５を備えたビデオカードの製造を希望する製造業者は、そのように実行するためのライセンスを取得し、とりわけ、要素６５を備えたビデオカード６０を製造する過程で、ある所定のライセンスタイプの規則に従わなければならず、ここで最も重要な点は、ビデオカード上のＶＲＡＭ６２が上記の方法によって書込み専用となっていることである。次に、製造業者はビデオカード６０に組み込むための要素６５を受け取るか、またはこうした要素６５をビデオカード６０に組み込むことを許可される。ライセンスのない製造業者も要素６５をそのビデオカード６０に組み込むことができるが、そのように実行した場合、ライセンスのない製造業者は要素６５に関する知的所有権の侵害で起訴されることになる。

【０１７５】

技術的デバイス

本発明の一実施形態では、ビデオカード６０は、暗号認証方式を使用する一般的に自発的な方法で、ＤＲＭシステム３２に対してそれ自体を認証する。ここで、ビデオカード６０はデジタル証明６６などの暗号証明を有し、ビデオカード６０が信用できるものであることを証明するために、これをＤＲＭシステム３２、レンダリングアプリケーション３４、または他の要求側エンティティに提示することができる。提示されたデジタル証明６６はその後、コンピューティングデバイス１４で、受入れ可能および／または受入れ不可の証明６６などの定期的または不定期に更新されるリスト６８に照らして、再検討することが

可能であり、少なくとも一部はそれに基づいて、ビデオカード６０が信用できるかどうかが判定される。こうした実施形態では、ビデオカード６０には、証明６６を不揮発的な方法で保持すること、および証明６６を適切な要求側エンティティの請求時に提示すること、という両方の機能が備えられていなければならない。

【０１７６】

適切な証明６６は、ビデオカード６０の製造業者が、ビデオカード６０を製造する過程で、ある所定のライセンスタイプの規則に従うことに合意した時点で、その製造業者に提供されることが好ましく、ここで最も重要な点は、ビデオカード上のＶＲＡＭ６２が上記の方法によって書込み専用になっていることである。次に、このように提供された証明６６は、製造業者によって製造される際に、ビデオカード６０に適切に組み込まれる。製造業者が、例えば読み取り可能ＶＲＡＭ６２を備えたビデオカード６０を製造するなどによって合意に反した場合、証明６６を前述の受入れ不可リスト６８に記載することができる。証明６６の組込みおよび提供、コンピューティングデバイス１４へのリスト６８の提供、並びにコンピューティングデバイス１４上のこうしたリスト６８の更新については、関係者に知られているかまたは明らかであるため、本明細書で詳細に論じる必要はない。したがって、証明６６の組込みおよび提供、並びにリスト６８の更新の任意の方法を、本発明の精神および範囲を逸脱することなく使用することができる。

【０１７７】

デジタル証明６６を使用する場合、ビデオカードは小型の暗号処理装置、あるいはそうでなければコンピューティングデバイス１４の処理装置上で実行する他の暗号化符号および一意の証明された鍵７０を必要とすることに留意されたい。ＤＲＭシステム３２、レンダリングアプリケーション３４、またはコンピューティングデバイス１４上の他のエンティティは、カード署名鍵７０が受入れ可能リスト６８に記載されている、および／または受入れ不可リスト６８に記載されていない、として適切に証明されているかどうかを確認するために、ビデオカード６０上の暗号化チャレンジ／応答などの認証を実行することができる。

【０１７８】

証明６６および鍵７０を使用しても、ライセンスを受けていない製造業者がライセンスを受けた製造業者になりすますことはできない。また、証明６６が損なわれた場合は、損なわれた証明６６を受入れ不可としてマークするために、リスト６８を更新することもできる。

【０１７９】

使用時の認証

最も単純な実施形態では、ビデオカード６０上にあるＶＲＡＭ６２の少なくとも一部が永続的に書込み専用となり、それ以外の方法で構成することはできない。この場合、ビデオカード６０は、認証時にそのタイプ（すなわち、アドレス領域Ｘに永続的な書込み専用ＶＲＡＭを備えた信用のあるビデオカード）をコンピューティングデバイス１４に対して確認するだけでよい。その後、コンピューティングデバイス１４上にある認証側のエンティティは、アドレス領域Ｘにデータを書き込むことができること、およびこうして書き込まれたデータは信用のあるビデオカード６０だけが読み取ることができることを理解する。

【０１８０】

ただし、ビデオカードがいくつかのモード（書込み専用対読取り書込みなど）の中から構成できる場合は、認証側ビデオカード６０それ自体では不十分である。信用のないエンティティによって構成が設定できる場合、攻撃者は、オリジナルデータの作者がビデオカード上で書込み専用バッファを認証および構成するまで待ち、そのバッファを読取り書込みに再構成し、次いで、ＶＲＡＭ６２に書き込まれるときデータを読み取ることができよう。この問題は、特に、プロセスの任意の集まりを同じコンピューティングデバイス１４上で並行して実行できるようにする現在のマルチタスキングオペレーティングシステムの状況に関する。この問題は、以下のような複数の方法で解決することができる。

【０１８１】

１．認証済み状態のチェック：ビデオカード６０は、制約なしで再構成することができる。ただし、こうしたカード６０は、認証済みの方法でその構成／状態を照会するためのホストコンピューティングデバイス１４上での処理を可能にする。すなわち、ビデオカード６０が最初の認証によって、タイプＸＹＺの信用されるビデオカードであること、および書込み専用バッファがアドレス領域ＡＢＣに割り振られていることを、ホストデバイス１４に確認することが可能であるのとまったく同様に、ビデオカード６０が追加の認証によって、過去Ｙ分の間、構成が変更されていないことなどを確認することができる。

【０１８２】

２．認証済み構成の変更：ビデオカード６０が、構成の変更を要求しているエンティティを認証することが必要である。原則として、この認証は、コンピューティングデバイス１４によるビデオカード６０の認証とはまったく別個にすることができる。デバイス１４からの書込み専用バッファに対する最初の要求は、だれがどの方法でバッファを再構成できるかに関する方針を記述することができる。この方針は、例えばライセンス１６などの形式を取ることができる。

【０１８３】

ビデオカード６０を認証する場合、ホストコンピューティングデバイス１４でのプロセスは、

ＧｅｔＷｒｉｔｅＯｎｌｙＢｕｆｆｅｒ（ｉｎｔ　ｂｕｆｆｅｒｓｉｚｅ）、および

ＲｅｃｏｎｆｉｇｕｒｅＢｕｆｆｅｒ（ｃｏｎｆｉｇｕｒａｔｉｏｎ　ｄｅｓｃｒｉｐｔｉｏｎ）

などの関数を呼び出すことが可能であり、公開鍵／秘密鍵暗号化を使用して、ビデオカード６０が秘密鍵を備え、信用されるエンティティからの証明中に対応する公開鍵を入れることができる。したがって、ホストデバイス１４上のコンテンツソース（ＣＳ）が公開鍵を備えた証明を使用可能にし、ＣＳが、例えばデジタル署名の検証および／または満了日または廃棄の検査によって、証明の妥当性を検査する。

【０１８４】

その後、ＶＲＡＭ６２の初期構成の一部としての（すなわち、上記のＧｅｔＷｒｉｔｅＯｎｌｙＢｕｆｆｅｒに関連する）ＣＳは、乱数Ｚ（ｎｏｎｃｅ）を生成し、結果がＰＵ（Ｚ）となるように証明からの公開鍵でＺを暗号化した後、ＰＵ（Ｚ）をビデオカード６０に送信する。ビデオカードが秘密鍵を使用してＰＵ（Ｚ）を復号するとＺとなり、その後メッセージ（Ｚ，Ｍ，Ｓ）をＣＳに送信するが、ここでＭは任意のメッセージテキストであり、Ｓは秘密鍵で作成されたＸ，Ｍを介したデジタル署名である。この例では、Ｍのテキストは「アドレスａとｂの間のメモリ領域は書込み専用として構成されている」という趣旨の可能性がある。実際にビデオカード６０はそのように構成されることが想定される。

【０１８５】

これで、再構成の認証（すなわち、上記のＲｅｃｏｎｆｉｇｕｒｅＢｕｆｆｅｒ関数に関連する）は、Ｚの知識に基づくものとなる。すなわち、ビデオカード６０にＶＲＡＭ６２の再構成を要求する呼出し側はＺの知識を実証しなければならず、そうでなければビデオカード６０がこの要求を拒否する。ＣＳだけがＺの知識を有するため、Ｚの知識のない攻撃者は失敗することが想定される。

【０１８６】

こうした認証には、例えばメッセージ（Ｍ，ｍ）をビデオカード６０に送信するＣＳを含むことが可能であり、ここでＭは「バッファａ．．．ｂを以下のように構成すること」という旨のメッセージであり、ｍはメッセージ認証コードｍ＝ＭＡＣ（Ｍ，Ｚ）のコンピューティング結果である。したがって、ビデオカード６０はＺの独自のコピーを使用してＭＡＣを検証する。具体的に言えば、ビデオカード６０は、ＭＡＣが検証された場合に限って再構成要求を受け付ける。

【０１８７】

書込み専用ＶＲＡＭ６２の使用に加えて、また別の方法として、ＣＳは、ビデオデータが

ビデオカード６０によってのみ復号されるように、ビデオデータを暗号化することができる。書込み専用のＶＲＡＭ６２の場合と同様に、これには、データが信頼のできるビデオカード６０に対してのみ暗号化されていることを、ＣＳが検証できるようにする認証が必要である。典型的には、認証メカニズムを使用すると、ＣＳおよびビデオカードが共用秘密（セッション鍵）Ｚを確立することができる。したがって、ビデオカード６０にデータを送信するために、ＣＳはＺに従ってデータを暗号化し、ビデオカードはＺに従ってデータを復号する。

【０１８８】

結論

本発明に関連して実行されるプロセスの実行に必要なプログラミングは比較的簡単であり、プログラミング関係者に明らかなものであるはずである。したがって、こうしたプログラミングは本明細書に添付されていない。本発明の精神および範囲を逸脱することなく、任意の特定のプログラミングを使用して本発明を実行することができる。

【０１８９】

前述の説明で、本発明が、任意の形式でのデジタルコンテンツ１２の制御されたレンダリングまたは再生を可能にする新しい役立つ強制アーキテクチャ１０を含むことが明らかであり、こうした制御はフレキシブルでありこうしたデジタルコンテンツ１２のコンテンツ所有者によって設定可能である。さらに本発明は、デジタルコンテンツ１２が、コンテンツ所有者の制御下にないコンピューティングデバイス１４上でレンダリングされる場合であっても、デジタルコンテンツ１２をコンテンツ所有者が指定した通りにしかレンダリングしない、新しい役立つ制御されたレンダリング環境も含む。さらに本発明は、コンテンツ泥棒がビデオカード６０に常駐するコンテンツを盗用するのを防ぐ、コンピューティングデバイス１４上にあるセキュアビデオカード６０も含む。

【０１９０】

前述の実施形態には、本発明の発明性のある概念を逸脱することなく変更が加えられることを理解されたい。原則的に、本発明は単にビデオカード６０に限定される必要のないものであることを理解されよう。その代わりに本発明は、例えばサウンドカードなどの復号されたデータを格納するためのメモリを有する任意のタイプのデバイスを含むことを意図するものである。同様に、本発明は、上記で図１～図１２に関連して開示したＤＲＭシステム３２などのＤＲＭシステムに限定されるものではない。その代わりに本発明は、セキュア環境を維持するか、またはデータが許可なく使用および／またはアクセスされるのを防ぐためのセキュリティモジュールを提供する任意のシステムを含む任意のタイプのＤＲＭシステムを含むことを意図するものである。

【０１９１】

本発明の主要な点は、メモリがデバイス以外に対しては読み取り専用であり、そのデバイスはそれ自体を信用できるものとして認証することができるという点である。これらの概念は、コンテンツフローが一定方向（すなわち、ＣＰＵ／メインメモリから、他のデバイス（例えばモニタ、スピーカなど）へのメモリを有するデバイスへの一方向）である限りは、任意の種類のコンテンツ１２およびデバイスに適用される。したがって、本発明は、開示された特定の実施形態に限定されるものではなく、特許請求の範囲によって定義される本発明の精神および範囲内であれば、修正が可能であることを意図するものである。

【図面の簡単な説明】

【図１】本発明の一実施形態に従った強制アーキテクチャを示す構成図である。

【図２】本発明の一実施形態に従った図１のアーキテクチャの認証ツールを示す構成図である。

【図３】本発明の一実施形態に従った図１のアーキテクチャに関連して使用するためのデジタルコンテンツを備えた、デジタルコンテンツパッケージを示す構成図である。

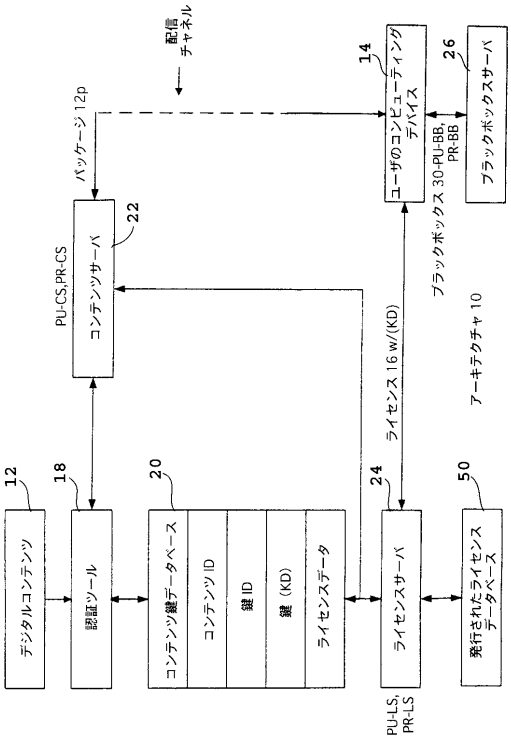
【図４】本発明の一実施形態に従った図１のユーザのコンピューティングデバイスを示す構成図である。

【図５】本発明の一実施形態に従ってコンテンツをレンダリングするために、図４のコン

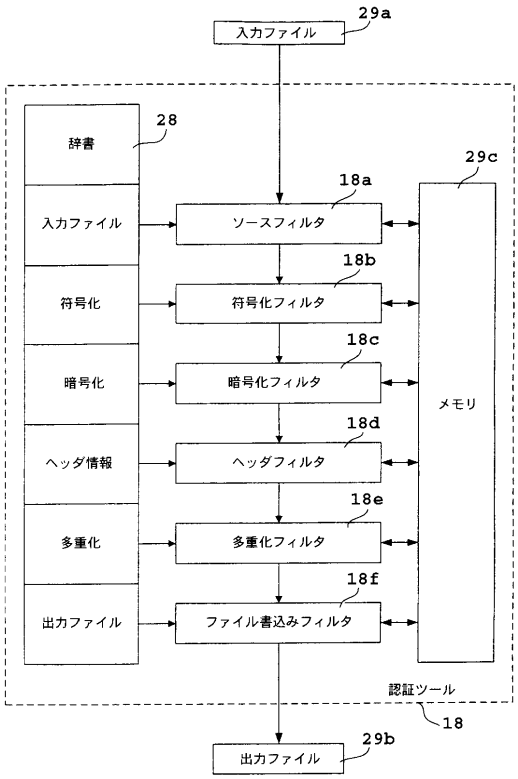
ピューティングデバイスのデジタル権管理（ＤＲＭ）システムに関連して実行されるステップを示す流れ図である。
【図６】本発明の一実施形態に従ってコンテンツをレンダリングするために、図４のコンピューティングデバイスのデジタル権管理（ＤＲＭ）システムに関連して実行されるステップを示す流れ図である。
【図７】本発明の一実施形態に従って任意の有効な実行可能化ライセンスが存在するかどうかを判定するために、図４のＤＲＭシステムに関連して実行されるステップを示す流れ図である。
【図８】本発明の一実施形態に従ってライセンスを取得するために、図４のＤＲＭシステムに関連して実行されるステップを示す流れ図である。
【図９】本発明の一実施形態に従った図１のアーキテクチャに関連して使用するためのデジタルライセンスを示す構成図である。
【図１０】本発明の一実施形態に従って新しいブラックボックスを取得するために、図４のＤＲＭシステムに関連して実行されるステップを示す流れ図である。
【図１１】本発明の一実施形態に従って、ライセンスおよびデジタルコンテンツピースの妥当性を検査し、コンテンツをレンダリングするために、図４のＤＲＭシステムに関連して実行される主要なトランザクションステップを示す流れ図である。
【図１２】本発明の一実施形態に従った、図４のライセンス評価器並びに、ライセンスのデジタル権ライセンス（ＤＲＬ）およびＤＲＬを解釈するための言語エンジンを示す構成図である。
【図１３】本発明の態様および／またはその一部を組み込むことができる汎用コンピュータシステムを表す構成図である。
【図１４】本発明の一実施形態に従った、図４のＤＲＭシステムおよびレンダリングアプリケーション並びに図１のコンピューティングデバイス上のビデオカードを示す構成図である。
【符号の説明】
１０　アーキテクチャ
１２　デジタルコンテンツ
１２ｐ　デジタルコンテンツパッケージ
１４　ユーザのコンピューティングデバイス
１８　認証ツール
１８ａ　ソースフィルタ
１８ｂ　符号化フィルタ
１８ｃ　暗号化フィルタ
１８ｄ　ヘッダフィルタ
１８ｅ　多重化フィルタ
１８ｆ　ファイル書込みフィルタ
２０　コンテンツ鍵データベース
２２　コンテンツサーバ
２４　ライセンスサーバ
２６　ブラックボックスサーバ
２８　辞書
２９ａ　入力ファイル
２９ｂ　出力ファイル
２９ｃ，１５０　メモリ
３０　ブラックボックス
３２　ＤＲＭシステム
３４　レンダリングアプリケーション
３６　ライセンス評価器
３８　ライセンス記憶域

４０　状態記憶域
５０　発行されたライセンスデータベース
６０　ビデオカード
６２　書込み専用ＶＲＡＭ
６４，１４７　モニタ
６５　保護された要素
６６　トークン／デジタル証明
６７　トークン
６８　リスト
７０　鍵
１２０　コンピュータ
１２１　処理ユニット
１２２　システムメモリ
１２３　システムバス
１２４　ＲＯＭ
１２５　ＲＡＭ
１２６　ＢＩＯＳ
１２７　ハードドライブ
１２８　フロッピィ（登録商標）ドライブ
１２９，１３１　ストレージ
１３０　光ドライブ
１３２　ハードディスクドライブインターフェース
１３３　磁気ディスクドライブインターフェース
１３４　光ドライブインターフェース
１３５　ＯＳ
１３６　アプリケーションプログラム
１３７　他のプログラム
１３８　プログラムデータ
１４０　キーボード
１４２　マウス
１４６　シリアルポートインターフェース
１４８　ビデオアダプタ
１４９　リモートコンピュータ
１５１　ＬＡＮ
１５２　ＷＡＮ
１５３　ネットワークインターフェース
１５４　モデム
１５５　ホストアダプタ
１５６　ＳＣＳＩバス
１６２　ストレージデバイス

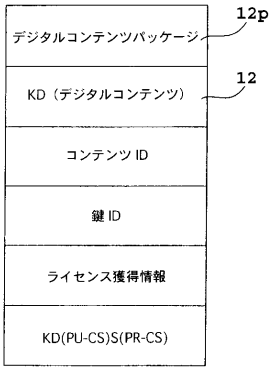
【図１】


配信チャネル
パッケージ 12p
14
ユーザのコンピューティングデバイス
26
ブラックボックスサーバ
ブラックボックス 30-PU-BB, PR-BB
PU-CS,PR-CS
コンテンツサーバ
22
ライセンス 16 w/(KD)
アーキテクチャ 10
12
デジタルコンテンツ
18
認証ツール
20
コンテンツ鍵データベース
コンテンツ ID
鍵 ID
鍵 (KD)
ライセンスデータ
24
ライセンスサーバ
50
発行されたライセンスデータベース
PU-LS, PR-LS

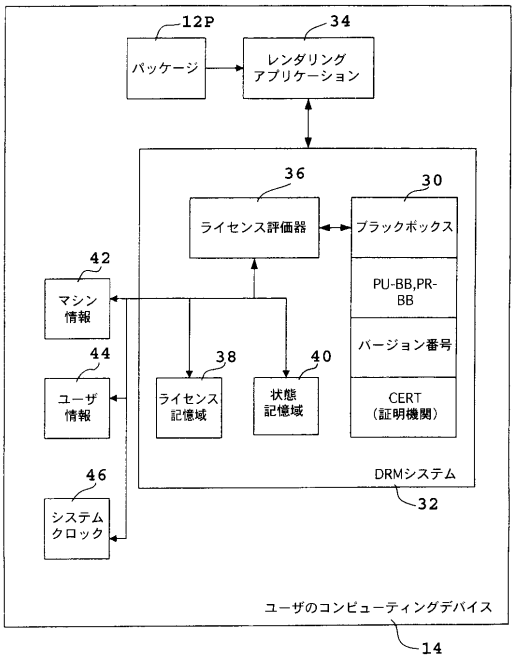
【図２】


29a
入力ファイル
辞書
28
入力ファイル
符号化
暗号化
ヘッダ情報
多重化
出力ファイル
18a
ソースフィルタ
18b
符号化フィルタ
18c
暗号化フィルタ
18d
ヘッダフィルタ
18e
多重化フィルタ
18f
ファイル書込みフィルタ
29c
メモリ
認証ツール
18
29b
出力ファイル

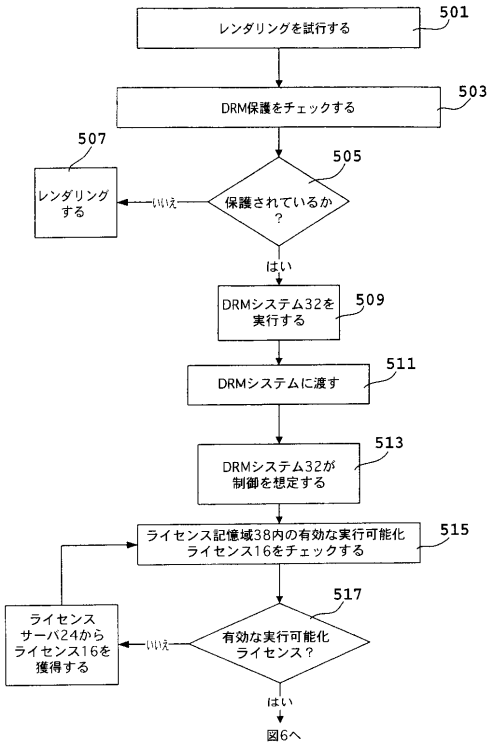
【図３】


デジタルコンテンツパッケージ
12p
KD（デジタルコンテンツ）
12
コンテンツ ID
鍵 ID
ライセンス獲得情報
KD(PU-CS)S(PR-CS)

【図４】


12P
パッケージ
34
レンダリングアプリケーション
36
ライセンス評価器
30
ブラックボックス
PU-BB,PR-BB
バージョン番号
CERT（証明機関）
42
マシン情報
44
ユーザ情報
38
ライセンス記憶域
40
状態記憶域
46
システムクロック
DRMシステム
32
ユーザのコンピューティングデバイス
14

【図５】


レンダリングを試行する
501
DRM保護をチェックする
503
保護されているか？
505
いいえ
レンダリングする
507
はい
DRMシステム32を実行する
509
DRMシステムに渡す
511
DRMシステム32が制御を想定する
513
ライセンス記憶域38内の有効な実行可能化ライセンス16をチェックする
515
有効な実行可能化ライセンス？
517
いいえ
ライセンスサーバ24からライセンス16を獲得する
はい
図6へ

【図６】

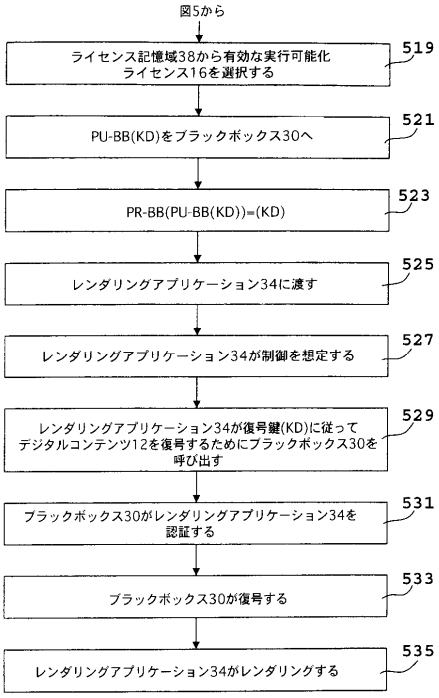
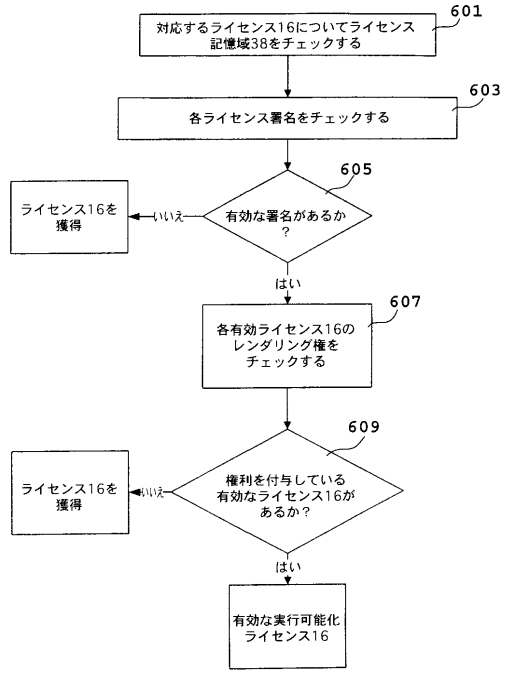
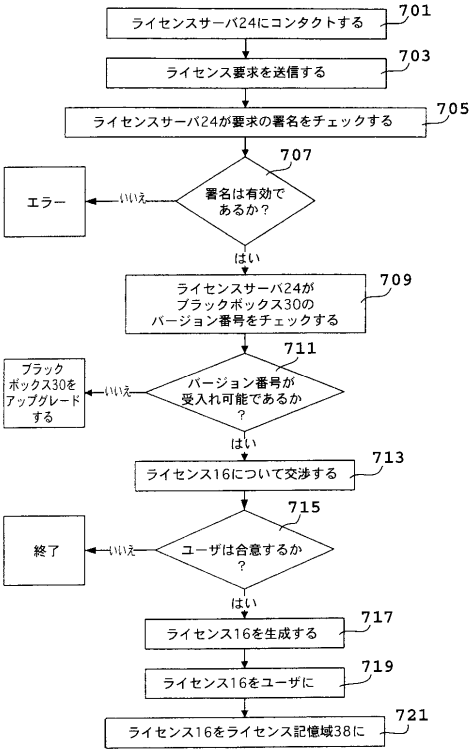


図5から
ライセンス記憶域38から有効な実行可能化ライセンス16を選択する
519
PU-BB(KD)をブラックボックス30へ
521
PR-BB(PU-BB(KD))=(KD)
523
レンダリングアプリケーション34に渡す
525
レンダリングアプリケーション34が制御を想定する
527
レンダリングアプリケーション34が復号鍵(KD)に従ってデジタルコンテンツ12を復号するためにブラックボックス30を呼び出す
529
ブラックボックス30がレンダリングアプリケーション34を認証する
531
ブラックボックス30が復号する
533
レンダリングアプリケーション34がレンダリングする
535

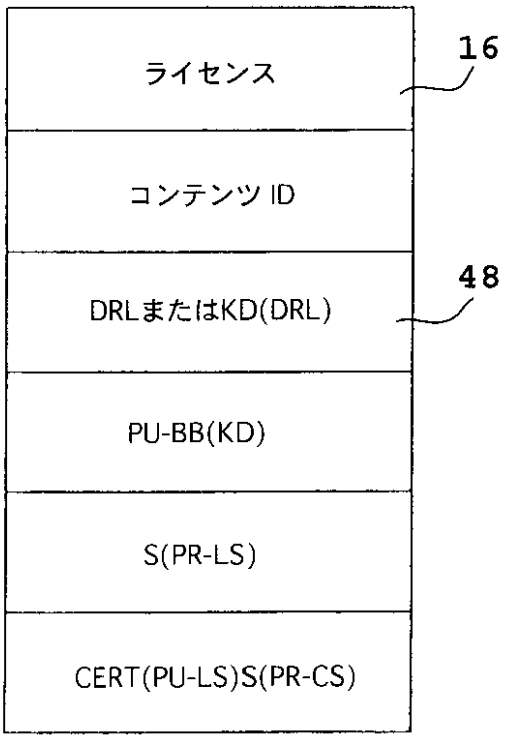
【図７】


対応するライセンス16についてライセンス記憶域38をチェックする
601
各ライセンス署名をチェックする
603
有効な署名があるか？
605
いいえ
ライセンス16を獲得
はい
各有効ライセンス16のレンダリング権をチェックする
607
権利を付与している有効なライセンス16があるか？
609
いいえ
ライセンス16を獲得
はい
有効な実行可能化ライセンス16

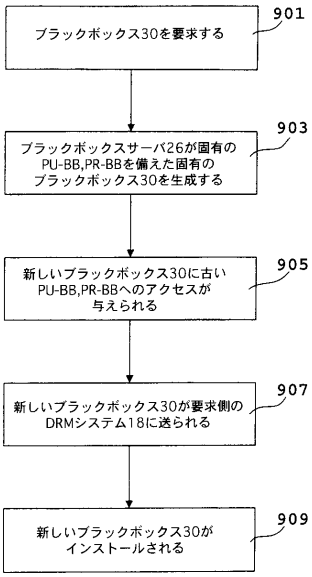
【図８】


ライセンスサーバ24にコンタクトする
701
ライセンス要求を送信する
703
ライセンスサーバ24が要求の署名をチェックする
705
署名は有効であるか？
707
いいえ
エラー
はい
ライセンスサーバ24がブラックボックス30のバージョン番号をチェックする
709
バージョン番号が受入れ可能であるか？
711
いいえ
ブラックボックス30をアップグレードする
はい
ライセンス16について交渉する
713
ユーザは合意するか？
715
いいえ
終了
はい
ライセンス16を生成する
717
ライセンス16をユーザに
719
ライセンス16をライセンス記憶域38に
721

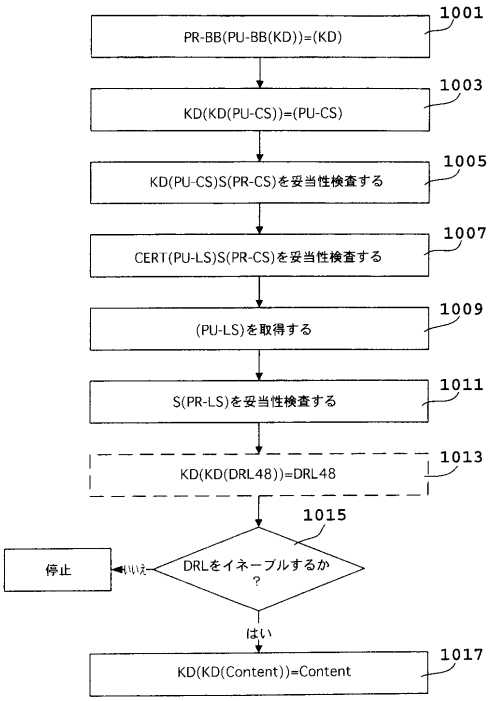
【図９】



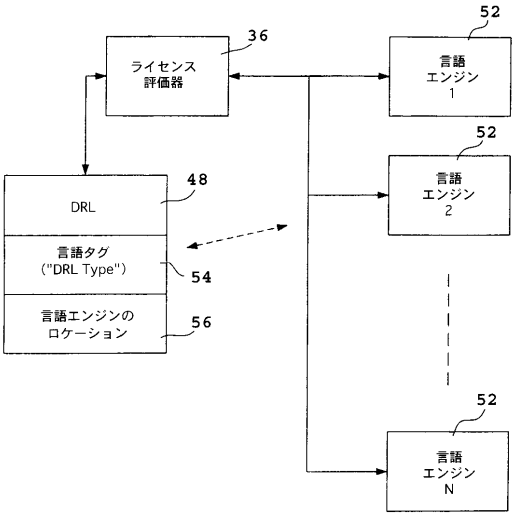
【図１０】



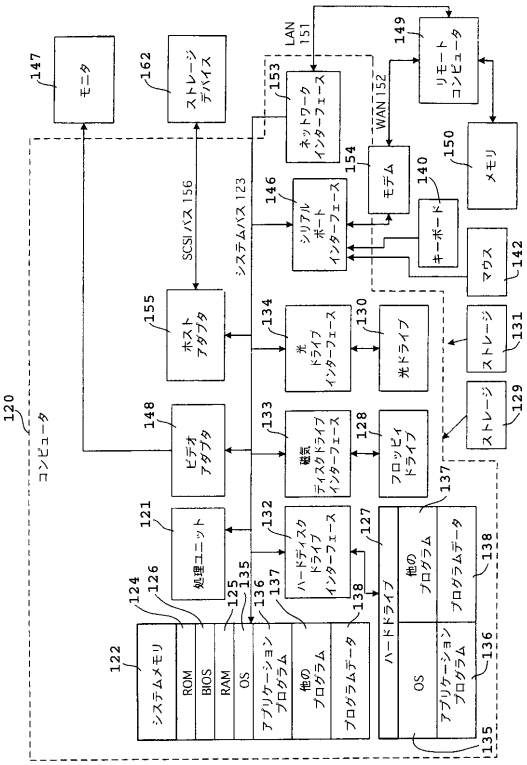
【図１１】



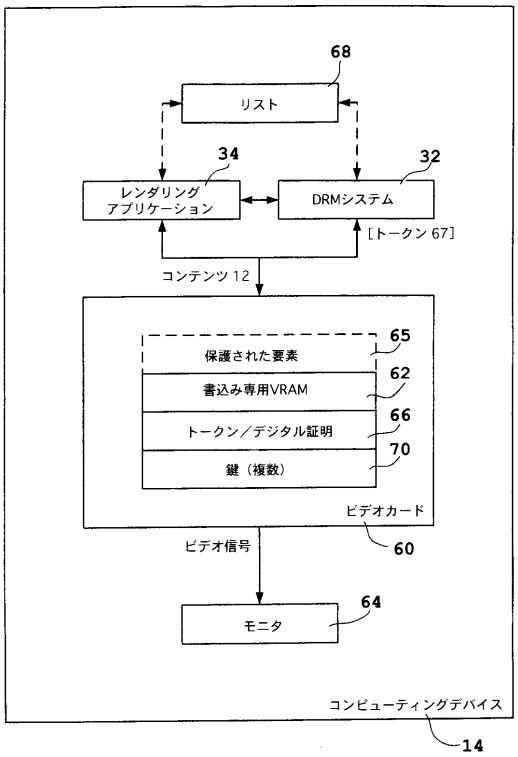
【図１２】



【図１３】


コンピュータ
120
モニタ
147
ストレージデバイス
162
LAN 151
ネットワークインターフェース
153
WAN 152
リモートコンピュータ
149
SCSIバス 156
システムバス 123
シリアルポートインターフェース
146
モデム
154
キーボード
140
メモリ
150
マウス
142
ホストアダプタ
155
光ドライブインターフェース
134
光ドライブ
130
ストレージ
131
ビデオアダプタ
148
磁気ディスクドライブインターフェース
133
フロッピィドライブ
128
ストレージ
129
処理ユニット
121
ハードディスクドライブインターフェース
132
ハードドライブ
127
他のプログラム
137
プログラムデータ
138
システムメモリ
122
ROM
124
BIOS
126
RAM
125
OS
135
アプリケーションプログラム
136
他のプログラム
137
プログラムデータ
138
OS
135
アプリケーションプログラム
136

【図１４】


68
リスト
34
レンダリングアプリケーション
32
DRMシステム
[トークン 67]
コンテンツ 12
65
保護された要素
62
書込み専用VRAM
66
トークン／デジタル証明
70
鍵（複数）
ビデオカード
60
ビデオ信号
64
モニタ
コンピューティングデバイス
14

フロントページの続き

(72)発明者 ポール イングランド
アメリカ合衆国 ９８００８ ワシントン州 ベルビュー ノースアップ ウェイ １６６５９
(72)発明者 マーカス ピーネイド
アメリカ合衆国 ９８００８ ワシントン州 ベルビュー １６８ アベニュー ノースイースト ７
(72)発明者 ムクンド サンカラナラヤン
アメリカ合衆国 ９８０２９ ワシントン州 イサコア サウスイースト ４１ ストリート ２５８４０

審査官 高橋 克

(56)参考文献 特開平１１－１１０２９５（ＪＰ，Ａ）
特開２０００－０６９４１５（ＪＰ，Ａ）
国際公開第９６／０２７１５５（WO，Ａ１）
国際公開第９８／００９２０９（WO，Ａ１）
欧州特許出願公開第００７１５２４５（ＥＰ，Ａ１）
SDMI Portable Device Specification Part 1 Version 1.0, Secure Digital Music Initiative，１９９９年 7月 8日

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21