

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4486321号
(P4486321)

(45) 発行日 平成22年6月23日 (2010. 6. 23)

(24) 登録日 平成22年4月2日 (2010. 4. 2)

(51) Int. Cl.

F I

G 0 6 F 21/22 (2006.01)

G 0 6 F 9/06 6 6 0 A

請求項の数 22 (全 57 頁)

(21) 出願番号	特願2003-137934 (P2003-137934)	(73) 特許権者	500046438
(22) 出願日	平成15年5月15日 (2003. 5. 15)		マイクロソフト コーポレーション
(65) 公開番号	特開2003-330560 (P2003-330560A)		アメリカ合衆国 ワシントン州 9805
(43) 公開日	平成15年11月21日 (2003. 11. 21)		2-6399 レッドモンド ワン マイ
審査請求日	平成18年5月2日 (2006. 5. 2)		クロソフト ウェイ
(31) 優先権主張番号	10/146, 236	(74) 代理人	100077481
(32) 優先日	平成14年5月15日 (2002. 5. 15)		弁理士 谷 義一
(33) 優先権主張国	米国 (US)	(74) 代理人	100088915
			弁理士 阿部 和夫
		(72) 発明者	マークス ペイナード
			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

最終頁に続く

(54) 【発明の名称】 デジタル権利管理 (DRM) システムを使用するソフトウェアアプリケーションの保護のための方法および媒体

(57) 【特許請求の範囲】

【請求項 1】

計算デバイス上で処理されるアプリケーションを保護する方法であって、

前記計算デバイスは、デジタル権利管理 (DRM) システム、アプリケーション、および前記アプリケーションに関する DRM デジタルライセンスとを有し、

前記アプリケーションは、第 1 のコードと第 2 のコードとを含み、

前記 DRM デジタルライセンスは、第 1 のデジタルライセンスと第 2 のデジタルライセンスとを含み、

前記アプリケーションが前記計算デバイス上で処理されるある時点で、前記第 1 のコードがトリガされるステップと、

ここで、前記第 1 のコードは、ある機能を行うように実行されることを目的として、前記 DRM デジタルライセンスに基づき、該アプリケーションが、前記機能を行うように実行されることが許されているかどうかを前記 DRM システムが決定することを要求するコードであり、

前記第 1 のコードにより、前記 DRM システムにおいて、前記アプリケーションが、第 1 のデジタルライセンスに基づいて前記機能を行うように実行されることが許可されていることを認証する第 1 の認証ステップと、

ここで、該第 1 のデジタルライセンスは、前記アプリケーションの使用が有効であることを証明するものであり、

前記アプリケーションが前記計算デバイス上で処理されるある時点で、前記第 2 のコー

ドがトリガされるステップと、

ここで、前記第2のコードは、該アプリケーションが、前記計算デバイス上または前記DRMシステムに関連して実行されるべきことを決定するためのコードであり、

前記第2のコードにより、前記アプリケーションにおいて、該アプリケーションが、第2のデジタルライセンスに基づいて前記DRMシステムに接続された状態で実行されることが許可されていることを認証する第2の認証ステップと、

ここで、該第2のデジタルライセンスは、前記DRMシステムと前記アプリケーションとの組み合わせが有効であることを証明するものであって、前記計算デバイス上に存在していることを示す前記アプリケーションの一意なIDと前記計算デバイス上に存在していることを示す前記DRMシステムの一意なIDとを有するものであり、

前記第1のデジタルライセンスおよび／又は第2のデジタルライセンスにより実際に、アプリケーションがある機能を行うように実行することが許されると判定した場合にだけ、DRMシステムによってアプリケーションが実行されるステップと

を具え、前記アプリケーションは、保護されていない第1のアプリケーションから前記第1のコードおよび前記第2のコードにより保護された第2のアプリケーションに変換されており、前記第2のアプリケーションは、前記第1のアプリケーションとして機能するが、該第2のアプリケーションを変更することにより、前記アプリケーションが動作しなくなるように制御されたことを特徴とする方法。

【請求項2】

前記第1の認証ステップは、

前記第1のコードにより、前記DRMシステムが自らの有効性を証明するドキュメントを前記アプリケーションに提出することを該DRMシステムに要求するステップと、

前記第1のコードは、前記提出されたドキュメントを受け取り、該提出されたドキュメントを検査するステップと、

前記第1のコードにより、前記検査されたドキュメントに基づき、前記DRMシステムが、前記DRMデジタルライセンスを行使することができるものとして信頼されるべきかどうかの有効性を判断するステップと、

前記第1のコードにより、前記アプリケーションが前記機能を行うように実行されることが前記DRMデジタルライセンスによって許されるかどうかを前記DRMシステムが決定することを要求し、前記DRMシステムは、その後、前記DRMデジタルライセンスにおけるあらゆる条項を検討して、その条項が前記アプリケーションのその実行を許すかどうかを決定するステップと、

前記DRMシステムが、前記信頼されるべきものと判断された場合で、かつ、前記DRMシステムが、前記DRMデジタルライセンスにより実際に、前記アプリケーションが前記機能を行うように実行することが許されると判定した場合にだけ、前記アプリケーションを実行するステップと

を含むことを特徴とする請求項1記載の方法。

【請求項3】

前記アプリケーションのロード中又は前記アプリケーションの実行中の所定の時点、および周期的から成るグループから選択された時点に応答して、前記第1のコードがトリガされるステップを含むことを特徴とする請求項2記載の方法。

【請求項4】

前記第1のコードにより、前記DRMシステムが、デジタル証明書を提出することによって自らの有効性を証明することを要求し、前記第1のコードにより、前記証明書が有効であるかどうかを判断するステップを含むことを特徴とする請求項2記載の方法。

【請求項5】

前記第1のコードにより、前記DRMシステムが、デジタル署名を提出することによって自らの有効性を証明することを要求し、前記第1のコードにより、前記証明書が検証されるかどうかを判断するステップを含むことを特徴とする請求項2記載の方法。

【請求項6】

前記アプリケーションは、IDを有し、前記ライセンスは、アプリケーションIDを含む識別情報を有するものであり、

前記識別情報の中の前記アプリケーションIDが、前記アプリケーションの前記IDに一致するかどうかを判定するステップと、

前記識別情報の中の前記アプリケーションIDが前記アプリケーションの前記IDに一致した場合にだけ、前記アプリケーションを実行するステップと
をさらに具えたことを特徴とする請求項2記載の方法。

【請求項7】

前記DRMシステムにより、前記識別情報の中の前記アプリケーションID、および前記アプリケーションの前記IDを獲得し、前記DRMシステムにより、前記識別情報の中の前記アプリケーションIDが、前記アプリケーションの前記IDに一致するかどうかを決定するステップを含むことを特徴とする請求項6記載の方法。

【請求項8】

前記DRMシステムにより、前記識別情報の中の前記アプリケーションIDを獲得して前記アプリケーションIDを前記第1のコードに送り、前記第1のコードにより、前記識別情報の中の前記アプリケーションIDが、前記アプリケーションの前記IDに一致するかどうかを判定するステップを含むことを特徴とする請求項6記載の方法。

【請求項9】

前記第2の認証ステップは、

前記アプリケーションは、IDを有し、前記DRMシステム又は前記計算デバイスは、IDを有し、また前記ライセンスは、アプリケーションID、およびDRMシステムID又は計算デバイスIDを有する証明書を含み、これにより当該方法は、

第2のコードにより、前記ライセンスから前記証明書を取得するステップと、

第2のコードにより、前記証明書の中から、前記アプリケーションID、および前記DRMシステムID又は前記計算デバイスIDを取得するステップと、

前記第2のコードにより、前記DRMシステム又は前記計算デバイスから、前記DRMシステム又は前記計算デバイスの前記IDを取得するステップと、

前記第2のコードにより、前記アプリケーションから、前記アプリケーションの前記IDを取得するステップと、

前記第2のコードにより、前記アプリケーションから取得された前記IDが、前記証明書からの前記アプリケーションIDに一致するかどうかを判定するステップと、

前記第2のコードにより、前記DRMシステムと前記計算デバイスのどちらから取得された前記IDが、前記証明書からの前記DRMシステム／計算デバイスIDに一致するかどうかを判定するステップと、

前記第2のコードにより、前記アプリケーションから取得された前記IDが、前記証明書からの前記アプリケーションIDに一致し、前記DRMシステムと前記計算デバイスのどちらから取得された前記IDが、前記証明書からの前記DRMシステム／計算デバイスIDに一致すると決定された場合にだけ、前記アプリケーションを実行するステップとを含むことを特徴とする請求項1記載の方法。

【請求項10】

前記アプリケーションのロード中又は前記アプリケーションの実行中の所定の時点、および周期的から成るグループから選択された時点に応答して、前記第2のコードがトリガされるステップを含むことを特徴とする請求項9記載の方法。

【請求項11】

請求項1ないし10のいずれかに記載の方法を、前記計算デバイスとしてのコンピュータに実行させることが可能な命令を有するプログラム。

【請求項12】

請求項11記載のプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項13】

計算デバイス上で処理されるアプリケーションを保護する装置であって、

10

20

30

40

50

前記計算デバイスは、デジタル権利管理（DRM）システム、アプリケーション、および前記アプリケーションに関するDRMデジタルライセンスとを有し、

前記アプリケーションは、第1のコードと第2のコードとを含み、

前記DRMデジタルライセンスは、第1のデジタルライセンスと第2のデジタルライセンスとを含み、

前記アプリケーションが前記計算デバイス上で処理されるある時点で、前記第1のコードがトリガされる手段と、

ここで、前記第1のコードは、ある機能を行うように実行されることを目的として、前記DRMデジタルライセンスに基づき、該アプリケーションが、前記機能を行うように実行されることが許されているかどうかを前記DRMシステムが決定することを要求するコードであり、

10

前記第1のコードにより、前記DRMシステムにおいて、前記アプリケーションが、第1のデジタルライセンスに基づいて前記機能を行うように実行されることが許可されていることを認証する第1の認証手段と、

ここで、該第1のデジタルライセンスは、前記アプリケーションの使用が有効であることを証明するものであり、

前記アプリケーションが前記計算デバイス上で処理されるある時点で、前記第2のコードがトリガされる手段と、

ここで、前記第2のコードは、該アプリケーションが、前記計算デバイス上または前記DRMシステムに関連して実行されるべきことを決定するためのコードであり、前記第2のコードにより、前記アプリケーションにおいて、該アプリケーションが、第2のデジタルライセンスに基づいて前記DRMシステムに接続された状態で実行されることが許可されていることを認証する第2の認証手段と、

20

ここで、該第2のデジタルライセンスは、前記DRMシステムと前記アプリケーションとの組み合わせが有効であることを証明するものであって、前記計算デバイス上に存在していることを示す前記アプリケーションの一意なIDと前記計算デバイス上に存在していることを示す前記DRMシステムの一意なIDとを有するものであり、

前記第1のデジタルライセンスおよび／又は第2のデジタルライセンスにより実際に、アプリケーションがある機能を行うように実行することが許されると判定した場合にだけ、DRMシステムによってアプリケーションが実行される手段と

30

を具え、前記アプリケーションは、保護されていない第1のアプリケーションから前記第1のコードおよび前記第2のコードにより保護された第2のアプリケーションに変換されており、前記第2のアプリケーションは、前記第1のアプリケーションとして機能するが、該第2のアプリケーションを変更することにより、前記アプリケーションが動作しなくなるように制御されたことを特徴とする装置。

【請求項14】

前記第1の認証手段は、

前記第1のコードにより、前記DRMシステムが自らの有効性を証明するドキュメントを前記アプリケーションに提出することを該DRMシステムに要求する手段と、

前記第1のコードは、前記提出されたドキュメントを受け取り、該提出されたドキュメントを検査する手段と、

40

前記第1のコードにより、前記検査されたドキュメントに基づき、前記DRMシステムが、前記DRMデジタルライセンスを行使することができるものとして信頼されるべきかどうかの有効性を判断する手段と、

前記第1のコードにより、前記アプリケーションが前記機能を行うように実行されることが前記DRMデジタルライセンスによって許されるかどうかを前記DRMシステムが決定することを要求し、前記DRMシステムは、その後、前記DRMデジタルライセンスにおけるあらゆる条項を検討して、その条項が前記アプリケーションのその実行を許すかどうかを決定する手段と、

前記DRMシステムが、前記信頼されるべきものと判断された場合で、かつ、前記DR

50

Mシステムが、前記DRMデジタルライセンスにより実際に、前記アプリケーションが前記機能を行うように実行することが許されると判定した場合にだけ、前記アプリケーションを実行する手段と

を含むことを特徴とする請求項13記載の装置。

【請求項15】

前記アプリケーションのロード中又は前記アプリケーションの実行中の所定の時点、および周期的から成るグループから選択された時点に応答して、前記第1のコードがトリガされる手段を含むことを特徴とする請求項14記載の装置。

【請求項16】

前記第1のコードにより、前記DRMシステムが、デジタル証明書を提出することによって自らの有効性を証明することを要求し、前記第1のコードにより、前記証明書が有効であるかどうかを判断する手段を含むことを特徴とする請求項14記載の装置。

10

【請求項17】

前記第1のコードにより、前記DRMシステムが、デジタル署名を提出することによって自らの有効性を証明することを要求し、前記第1のコードにより、前記証明書が検証されるかどうかを判断する手段を含むことを特徴とする請求項14記載の装置。

【請求項18】

前記アプリケーションは、IDを有し、前記ライセンスは、アプリケーションIDを含む識別情報を有するものであり、

前記識別情報の中の前記アプリケーションIDが、前記アプリケーションの前記IDに一致するかどうかを判定する手段と、

20

前記識別情報の中の前記アプリケーションIDが前記アプリケーションの前記IDに一致した場合にだけ、前記アプリケーションを実行する手段と

をさらに具えたことを特徴とする請求項14記載の装置。

【請求項19】

前記DRMシステムにより、前記識別情報の中の前記アプリケーションID、および前記アプリケーションの前記IDを獲得し、前記DRMシステムにより、前記識別情報の中の前記アプリケーションIDが、前記アプリケーションの前記IDに一致するかどうかを決定する手段を含むことを特徴とする請求項18記載の装置。

【請求項20】

30

前記DRMシステムにより、前記識別情報の中の前記アプリケーションIDを獲得して前記アプリケーションIDを前記第1のコードに送り、前記第1のコードにより、前記識別情報の中の前記アプリケーションIDが、前記アプリケーションの前記IDに一致するかどうかを判定する手段を含むことを特徴とする請求項18記載の装置。

【請求項21】

前記第2の認証手段は、

前記アプリケーションは、IDを有し、前記DRMシステム又は前記計算デバイスは、IDを有し、また前記ライセンスは、アプリケーションID、およびDRMシステムID又は計算デバイスIDを有する証明書を含み、これにより当該装置は、

第2のコードにより、前記ライセンスから前記証明書を取得する手段と、

40

第2のコードにより、前記証明書の中から、前記アプリケーションID、および前記DRMシステムID又は前記計算デバイスIDを取得する手段と、

前記第2のコードにより、前記DRMシステム又は前記計算デバイスから、前記DRMシステム又は前記計算デバイスの前記IDを取得する手段と、

前記第2のコードにより、前記アプリケーションから、前記アプリケーションの前記IDを取得する手段と、

前記第2のコードにより、前記アプリケーションから取得された前記IDが、前記証明書からの前記アプリケーションIDに一致するかどうかを判定する手段と、

前記第2のコードにより、前記DRMシステムと前記計算デバイスのどちらから取得された前記IDが、前記証明書からの前記DRMシステム／計算デバイスIDに一致する

50

かどうかを判定する手段と、

前記第2のコードにより、前記アプリケーションから取得された前記IDが、前記証明書からの前記アプリケーションIDに一致し、前記DRMシステムと前記計算デバイスのどちらから取得された前記IDが、前記証明書からの前記DRMシステム／計算デバイスIDに一致すると決定された場合にだけ、前記アプリケーションを実行する手段とを含むことを特徴とする請求項13記載の装置。

【請求項22】

前記アプリケーションのロード中又は前記アプリケーションの実行中の所定の時点、および周期的から成るグループから選択された時点に応答して、前記第2のコードがトリガされる手段を含むことを特徴とする請求項21記載の装置。

10

【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行使するためのアーキテクチャに係るアプリケーションの保護のための方法および媒体に関する。より詳細には、本発明は、デジタルコンテンツのユーザによって獲得されたライセンス権利によって指定されたパラメータに従ってのみ暗号化されたデジタルコンテンツへのアクセスを許すというような行使アーキテクチャに関する。さらに詳細には、本発明は、ソフトウェアアプリケーションを保護するのに使用されるアーキテクチャに関する。

【0002】

20

＜関連出願の相互参照＞

本出願は、参照によりそれぞれ全体が本明細書に組み込まれている

1999年4月12日に出願した「ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT」という名称の米国特許出願番号09／290,363、および1999年3月27日に出願した「ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT」という名称の米国特許仮出願番号60,126,614に関連する。

【0003】

【従来の技術】

デジタル権利の管理および行使は、デジタルコンテンツがユーザに配布される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極めて望ましい。典型的な配布の様式には、磁気（フロッピー（登録商標））ディスク、磁気テープ、光（コンパクト）ディスク（CD）などの有形のデバイス、ならびに電子掲示板、電子ネットワーク、インターネットなどの無形の媒体が含まれる。ユーザが受け取ると、ユーザは、パーソナルコンピュータ上のメディアプレーヤなどの適切なレンダリングデバイスの助けを借りてデジタルコンテンツをレンダリングする、つまり「再生」する。

30

【0004】

通常、作成者、発行者、放送業者などのコンテンツ所有者または権利所有者（以降、「コンテンツ所有者」）は、ライセンス料または何らかの他の対価と引換えにユーザまたは受け手にデジタルコンテンツを配布することを望む。コンテンツ所有者は、選択が与えられるのであれば、ユーザが、配布されたデジタルコンテンツに対して何を行うことができるかを制限することを望む可能性が高い。例えば、コンテンツ所有者は、ユーザが、少なくとも第2のユーザからのライセンス料をコンテンツ所有者に与えないような仕方

40

でコンテンツをコピーして第2のユーザに再配布することを禁止することを望む。

【0005】

さらに、コンテンツ所有者は、ユーザに実際に購入されたあらゆるタイプのライセンスの条項を守らせながら、異なるライセンス料で異なるタイプの使用ライセンスを購入する柔軟性をユーザに提供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、配布されたデジタルコンテンツが、限られた回数だけ、ある合計時間だけ、あるタイプのマシン上でだけ、あるタイプのメディアプレーヤ上でだけ、あるタイプのユーザによってだけ

50

再生されるのを許すことを望む場合がある。

【0006】

【発明が解決しようとする課題】

しかし、ユーザにデジタルコンテンツの配布が行われた後、コンテンツ所有者は、デジタルコンテンツに対してほとんど規制を有さない。このことは、実質的にすべての新しいパーソナルコンピュータまたは最新のパーソナルコンピュータが、デジタルコンテンツの正確なデジタルコピーを作成し、正確なデジタルコピーを書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、または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のに必要なソフトウェアおよびハードウェアを含むことに鑑みて特に問題である。

10

【0007】

もちろん、ライセンス料が得られた正当な取引の一環として、コンテンツ所有者は、デジタルコンテンツのユーザが、デジタルコンテンツを再配布しないことを約束することを要求することができる。しかし、そのような約束は、簡単に結ばれて簡単に破られる。コンテンツ所有者は、通常、暗号化および暗号化解除に関わるいくつかの周知のセキュリティデバイスの任意のものを介してそのような再配布を防止しようと試みることができる。

【0008】

しかし、ある程度、決心したユーザが、暗号化されたデジタルコンテンツを暗号化解除し、デジタルコンテンツを暗号化されていない形態で保存した後、そのコンテンツを再配布することを防止するものはほとんど存在しない。

20

【0009】

そこで、本発明の目的は、特にデジタルコンテンツの再配布の防止に関して規制が柔軟であり、デジタルコンテンツのコンテンツ所有者によってその規制の定義が可能であり、任意の形態のデジタルコンテンツの規制されたレンダリングまたは再生を可能にした行使アーキテクチャおよび行使方法に係るアプリケーションの保護のための方法および媒体を提供することにある。

【0010】

また、本発明の他の目的は、レンダリング環境が行使アーキテクチャの少なくとも一部分を含む、パーソナルコンピュータなどの計算デバイス上で規制されたレンダリング環境を提供することにある。レンダリング環境は、デジタルコンテンツが、コンテンツ所有者の規制下でない計算デバイス上でレンダリングされるにしても、コンテンツ所有者によって指定されたとおりにしかレンダリングされることを許さない。

30

【0011】

さらに、本発明の他の目的は、信頼される構成要素が、コンテンツ所有者によって許可されていない仕方ではデジタルコンテンツにアクセスしようとする計算デバイスのユーザによる試みにさえ抗して、あるデジタルコンテンツに関連して計算デバイス上でコンテンツ所有者の権利を行使する、計算デバイス上で実行される信頼される構成要素を提供することにある。1例として、信頼されるソフトウェア構成要素は、計算デバイスのユーザが、デジタルコンテンツのコンテンツ所有者によって許可されている形を除き、デジタルコンテンツのコピーを作成するのを防止する。

40

【0012】

最後に、本発明の他の目的は、デジタル権利管理アーキテクチャがソフトウェアアプリケーションの保護をサポートすることを可能にする方法および機構を提供することにある。より詳細には、通常のソフトウェアアプリケーションが、多数の構成ファイルからなる可能性があることに留意すると、デジタル権利管理アーキテクチャが、ソフトウェアアプリケーションが、アプリケーションの所有者によって望まれない形で使用されることを防ぐことを可能にする方法および機構の必要性が存在する。

【0013】

【課題を解決するための手段】

前述した必要性は、アーキテクチャおよび方法が、インターネット、光ディスクなどの媒

50

体上で利用可能な保護された（セキュアな）デジタルコンテンツにおける権利を行使する、デジタル権利管理のための行使アーキテクチャおよび行使方法によって少なくともある程度、満たされる。コンテンツを供与するため、このアーキテクチャは、インターネットなどを介して暗号化された形態でデジタルコンテンツがアクセス可能であるコンテンツサーバを含む。また、コンテンツサーバは、光ディスク等の上に記録するために暗号化されたデジタルコンテンツを供給することも可能であり、暗号化されたデジタルコンテンツを光ディスク自体の上で配布することができる。コンテンツサーバにおいて、デジタルコンテンツは、暗号化鍵を使用して暗号化され、デジタルコンテンツをユーザの計算デバイスまたはクライアントマシンにおいてデジタルライセンスとバインドするのに公開鍵／秘密鍵技術が使用される。

10

【0014】

ユーザが、計算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試みたとき、レンダリングアプリケーションが、ユーザの計算デバイス上でデジタル権利管理（DRM）システムを起動する。ユーザが、初めてそのデジタルコンテンツをレンダリングしようと試みている場合、DRMシステムは、求めている仕方でデジタルコンテンツをレンダリングするライセンスを獲得するようライセンスサーバにユーザを導くか、またはユーザ側でアクションを全く必要とすることなくライセンスサーバからライセンスをトランスペアレントに獲得する。ライセンスは、以下のものを含む。

- －暗号化されたデジタルコンテンツを暗号化解除する暗号化解除鍵（KD）。
- －記述がデジタル可読形態である場合、ライセンスによって与えられる権利（再生、コピー等）、および関連する条件（開始日、失効日、再生の回数等）の記述。
- －ライセンスの完全性を保証するデジタル署名。

20

【0015】

ユーザが、ライセンスサーバからそのようなライセンスを獲得すること無しに暗号化されたデジタルコンテンツを暗号化解除してレンダリングすることができてはならない。獲得されたライセンスはユーザの計算デバイス内のライセンスストアに格納される。

【0016】

重要なことには、ライセンスサーバは、「信頼される」（すなわち、自らを認証することができる）DRMシステムだけにライセンスを発行する。「信頼」を実装するため、DRMシステムは、DRMシステムのために暗号化解除機能および暗号化機能を行う「ブラックボックス」を備えている。ブラックボックスは、公開鍵／秘密鍵ペア、バージョン番号、および固有署名を含み、以上すべてが、承認された認定機関によって提供されるものである。公開鍵は、発行されるライセンスの部分を暗号化し、これにより、ライセンスをブラックボックスにバインドする目的でライセンスサーバに供与される。秘密鍵は、対応する公開鍵を使用して暗号化された情報を暗号化解除する目的で、ブラックボックスにだけ利用可能であり、ユーザまたは他の何人にも利用可能ではない。DRMシステムは、最初、公開鍵／秘密鍵ペアを有するブラックボックスを備え、ユーザは、ライセンスを最初に要求したとき、ブラックボックスサーバから更新されたセキュアなブラックボックスをダウンロードするように促される。ブラックボックスサーバは、固有の公開鍵／秘密鍵ペアとともに更新されたブラックボックスを提供する。更新されたブラックボックスは、ユーザの計算デバイス上でだけ実行される固有の実行可能コードで書かれ、定期的に再更新される。

30

40

【0017】

ユーザが、ライセンスを要求したとき、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り、ライセンスサーバは、バージョン番号が最新であり、署名が有効である場合にだけ、ライセンスを発行する。また、ライセンス要求は、行われたライセンスの要求が関係す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する暗号化解除鍵を特定する鍵IDも含む。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暗号化解除鍵を暗号化し、暗号化解除鍵を使用してライセンス条項を暗号化した後、暗号化された暗号化解除鍵および暗号

50

化されたライセンス条項をライセンス署名とともにユーザの計算デバイスにダウンロードする。

【0018】

ダウンロードされたライセンスが、DRMシステムライセンスストアの中に記憶されると、ユーザは、ライセンスによって与えられ、ライセンス条項によって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要求が行われたとき、ブラックボックスが、暗号化解除鍵およびライセンス条項を暗号化解除するようにさせられ、またDRMシステムライセンスイバリュエータ (evaluator) が、ライセンス条項を評価する。ブラックボックスは、ライセンス評価により、要求者が、コンテンツを再生することが許されているという判定がもたらされる場合にだけ暗号化されたデジタルコンテンツを暗号化解除する。暗号化解除されたコンテンツが、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。

10

【0019】

本発明の一実施形態では、デジタル権利管理 (DRM) システム、アプリケーション、およびアプリケーションに関する DRM デジタルライセンスがすべて計算デバイス上にある。アプリケーションは、ある機能を行うように実行されるものであり、ライセンスに基づいてアプリケーションがその機能を行うように実行されることが許されていることを DRM システムが判定することを要求するコードを含む。コードは、トリガされたとき、DRM システムが、ドキュメントを提出することによって有効性を証明することを要求し、提出されたドキュメントを受け取り、そのドキュメントを検査し、提出されたドキュメントに基づき、DRM システムが、有効であり、ライセンスを行使するものとして信頼されるかどうかを判断する。また、コードは、DRM システムは、ライセンスにより、アプリケーションが、機能を行うように実行することを許すかどうかを判定するように要求し、その後、DRM システムは、ライセンスの中のあらゆる条項を検査して、条項によりアプリケーションの実行が許されるかどうかを判定する。次に、DRM システムが、ライセンスによって実際にアプリケーションが機能を行うように実行することを許すと判定した場合にだけ、アプリケーションが実行される。

20

【0020】

アプリケーションは、そのアプリケーションが、計算デバイスの 1 つの上で、または DRM システムに関連して実行されることを判定するためのコードをさらに含む。コードは、トリガされたとき、証明書からアプリケーション ID、および DRM システム ID と計算デバイス ID のどちらかを獲得し、また DRM システムと計算デバイスのどちらかから ID を取得し、アプリケーションからそのアプリケーションの ID を取得する。次に、コードは、アプリケーションから取得された ID が、証明書からのアプリケーション ID に一致するかどうかを判定し、また DRM システムと計算デバイスのどちらかから取得された ID が、証明書からの DRM システム / 計算デバイス ID に一致するかどうかを判定する。次に、アプリケーションから取得された ID が、証明書からのアプリケーション ID に一致し、DRM システムと計算デバイスのどちらかから取得された ID が、証明書からの DRM システム / 計算デバイス ID に一致する場合にだけ、アプリケーションが実行される。

30

40

【0021】

以上の概要、および本発明の実施形態の以下の詳細な説明は、添付の図面と併せて読まれるとき、よりよく理解される。本発明を例示するため、図面には、現在、好ましいとされる実施形態を示している。ただし、理解されるべきこととして、本発明は、図示した構成および手段 (instrumentalities) には限定されない。

【0022】

【発明の実施の形態】

同様の符号が、すべての図面にわたって同様の要素を指すように使用される図面を詳細に参照すると、図 1 に、本発明の一実施形態による行使アーキテクチャ 10 が示されている。全体として、行使アーキテクチャ 10 により、デジタルコンテンツ 12 の所有者が、デ

50

デジタルコンテンツ１２がユーザの計算デバイス１４上でレンダリングされることが許されるには、まず満たされなければならないライセンス規則を指定することが可能になる。ライセンス規則は、ユーザ／ユーザの計算デバイス１４（以降、状況により別段、必要とされない限り、これらの用語は区別しない）が、コンテンツ所有者、またはコンテンツ所有者の代理業者から獲得しなければならないデジタルライセンス１６の中で実現される。デジタルコンテンツ１２は、暗号化された形態で配布され、無料で広汎に配布されることが可能である。好ましくは、デジタルコンテンツ１２を暗号化解除するための暗号化解除鍵（ＫＤ）が、ライセンス１６に含められる。

【００２３】

<コンピュータ環境>

図１２、および以下の考察は、本発明および／または本発明の部分を実施することができる適切な計算環境の簡単な一般的説明を提供するものとする。必須ではないが、本発明は、サーバ上のクライアントワークステーションなどの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のコンピュータ実行可能命令の一般的な文脈で説明する。一般に、プログラムモジュールには、特定のタスクを行う、または特定の抽象データタイプを実装するルーチン、プログラム、オブジェクト、構成要素、データ構造等が含まれる。さらに、本発明、および／または本発明の部分は、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の家庭用電化製品またはプログラマブル家庭用電化製品、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等を含め、他のコンピュータシステム構成で実施してもよいことを理解されたい。また、本発明は、タスクが、通信網を介してリンクされた遠隔処理デバイスによって行われる分散計算環境において実施してもよい。分散計算環境では、プログラムモジュールが、ローカルのメモリ記憶デバイスと遠隔の記憶デバイスの両方の中に配置されることが可能である。

【００２４】

図１２に示すとおり、例としての汎用計算システムには、処理ユニット１２１、システムメモリ１２２、およびシステムメモリから処理ユニット１２１までを含む様々なシステム構成要素を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等が含まれる。システムバス１２３は、様々なバスアーキテクチャの任意のものを使用するメモリバスまたはメモリコントローラ、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任意のものであることが可能である。システムメモリは、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を含む。始動中などに、パーソナルコンピュータ１２０内部の要素間で情報を転送するのを助ける基本ルーチンを含む基本入力／出力システム１２６（ＢＩＯＳ）が、ＲＯＭ１２４の中に記憶される。

【００２５】

パーソナルコンピュータ１２０は、ハードディスク（図示せず）に対して読取りおよび書込みを行うためのハードディスクドライブ１２７、取外し可能な磁気ディスク１２９に対して読取りおよび書込みを行うための磁気ディスクドライブ１２８、およびＣＤ－ＲＯＭ、または他の光媒体などの取外し可能な光ディスク１３１に対して読取りおよび書込みを行うための光ディスクドライブ１３０をさらに含むことが可能である。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でシステムバス１２３に接続される。以上のドライブ、および関連するコンピュータ可読媒体により、コンピュータ可読命令、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ストレージがパーソナルコンピュータ２０に提供される。

【００２６】

本明細書で説明する例としての実施形態は、ハードディスク、取外し可能な磁気ディスク１２９、および取外し可能な光ディスク１３１を使用するが、コンピュータがアクセスすることが可能なデータを記憶することができる他のタイプのコンピュータ可読媒体も、例

10

20

30

40

50

としての動作環境において使用できることを理解されたい。そのような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）等が含まれる。

【0027】

オペレーティングシステム135、1つまたは複数のアプリケーションプログラム136、その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を含め、いくつかのプログラムモジュールをハードディスク、磁気ディスク129、光ディスク131、ROM124、またはRAM125に記憶することができる。ユーザは、キーボード140や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、マイクロホン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナ等が含まれることが可能である。以上の入力デバイス、およびその他の入力デバイスは、しばしば、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に接続されるが、パラレルポート、ゲームポート、またはユニバーサルシリアルバス（universal serial bus）（USB）などの他のインターフェースで接続してもよい。また、モニタ147、または他のタイプの表示デバイスも、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は、通常、スピーカやプリンタなどの他の周辺出力デバイス（図示せず）も含む。また、図12の例としてのシステムは、ホストアダプタ155、スモールコンピュータシステムインターフェース（Small Computer System Interface）（SCSI）バス156、およびSCSIバス156に接続された外部記憶デバイス162も含む。

【0028】

パーソナルコンピュータ120は、遠隔コンピュータ149のような1つまたは複数の遠隔コンピュータに対する論理接続を使用するネットワーク化された環境において動作することが可能である。遠隔コンピュータ149は、別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、または他の一般的なネットワークノードであることが可能であり、通常、パーソナルコンピュータ120に関連して前述した要素の多く、またはすべてを含むが、図12では、メモリ記憶デバイス150だけを示している。図12に描いた論理接続は、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を含む。そのようなネットワーキング環境は、オフィス、企業全体のコンピュータ網、イントラネット、およびインターネットで一般的である。

【0029】

LANネットワーキング環境で使用されるとき、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、またはネットワークアダプタ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されるとき、パーソナルコンピュータ120は、通常、インターネットなどのワイドエリアネットワーク152を介して通信を確立するためのモデム154、または他の手段を含む。内部にあることも、外部にあることも可能なモデム154は、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。ネットワーク化された環境では、パーソナルコンピュータ120に関連して描いたプログラムモジュール、またはプログラムモジュールの部分が、遠隔メモリ記憶デバイスの中に記憶されることが可能である。図示したネットワーク接続は、例としてのものであり、コンピュータ間で通信リンクを確立する他の手段も使用できることが理解されよう。

【0030】

<アーキテクチャ>

図1を再び参照すると、本発明の一実施形態では、アーキテクチャ10が、オーサリングツール（authoring tool）18、コンテンツ鍵データベース20、コン

10

20

30

40

50

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、ならびに前述したユーザの計算デバイス 14を含む。

【0031】

＜アーキテクチャオーサリングツール 18＞

オーサリングツール 18は、デジタルコンテンツ 12をパッケージ化して、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態にするためにコンテンツ所有者によって使用される。詳細には、コンテンツ所有者が、デジタルコンテンツ 12、デジタルコンテンツ 12に付随すべき命令および／または規則、およびデジタルコンテンツ 12がどのようにパッケージ化されるべきかに関する命令および／または規則をオーサリングツール 18に提供する。次に、オーサリングツール 18が、暗号化／暗号化解除鍵、およびデジタルコンテンツ 12に付随する命令および／または規則に従ってデジタルコンテンツ 12が暗号化されたデジタルコンテンツパッケージ 12pを生成する。

10

【0032】

本発明の一実施形態では、オーサリングツール 18は、異なる暗号化／暗号化解除鍵に従って暗号化された同一のデジタルコンテンツ 12をそれぞれが有するいくつかの異なるデジタルコンテンツ 12パッケージ 12pを連続的に生成するように命令される。理解されるべきこととして、同一のデジタルコンテンツ 12を有するいくつかの異なるパッケージ 12pを有することは、パッケージ 12p／コンテンツ 12（以降、別段、必要とされない限り、単に「デジタルコンテンツ 12」）の配布を追跡するのに役立つ可能性がある。そのような配布追跡は、通常、必要ないが、デジタルコンテンツ 12が違法に販売された、または放送された場合、調査機関によって使用されることが可能である。

20

【0033】

本発明の一実施形態では、デジタルコンテンツ 12を暗号化する暗号化／暗号化解除鍵は、暗号化鍵が暗号化解除鍵（KD）でもあることで、対称鍵である。以下により詳細に述べるとおり、暗号化解除鍵（KD）は、デジタルコンテンツ 12に関するライセンス 16の一部として隠された形態でユーザの計算デバイス 14に送られる。好ましくは、各デジタルコンテンツ 12は、コンテンツ IDを備え（または各パッケージ 12pが、パッケージ IDを備え）、各暗号化解除鍵（KD）が、鍵 IDを有し、またオーサリングツール 18により、各デジタルコンテンツ 12（または各パッケージ 12p）に関する暗号化解除鍵（KD）、鍵 ID、およびコンテンツ ID（またはパッケージ ID）が、コンテンツデータベース 20の中に記憶させられる。さらに、デジタルコンテンツ 12に関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、および各タイプのライセンス 16に関する条項および条件が、コンテンツデータベース 20、あるいは別のデータベース（図示せず）の中に記憶されることが可能である。好ましくは、ライセンスデータは、状況、および市場の条件によって必要となるに応じて、コンテンツ所有者によって変更されることが可能である。

30

【0034】

使用時に、オーサリングツール 18には、とりわけ、以下を含む情報が供給される。

－パッケージ化されるべきデジタルコンテンツ 12。

－透かし入れ（watermarking）、および／または指紋入れ（fingerprinting）が使用される場合、透かし入れ、および／または指紋入れのタイプおよびパラメータ。

40

－データ圧縮が使用される場合、データ圧縮のタイプおよびパラメータ。

－使用される暗号化のタイプおよびパラメータ。

－シリアル化（serialization）が使用される場合、シリアル化のタイプおよびパラメータ。

－デジタルコンテンツ 12に付随すべき命令および／または規則。

【0035】

周知のとおり、透かしは、識別子としてデジタルコンテンツ 12に追加される、隠されたコンピュータ可読の信号である。指紋は、各インスタンスに関して異なる透かしである。

50

理解されるべきこととして、インスタンスは、固有である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複数のコピーを作成することができ、またあらゆるコピーは、特定のインスタンスのものである。デジタルコンテンツの特定のインスタンスが違法に販売された、または放送されたとき、調査機関が、場合により、デジタルコンテンツ 12 に追加された透かし／指紋に従って容疑者を特定することが可能である。

【0036】

データ圧縮は、本発明の趣旨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行われることが可能である。例えば、. mp3 圧縮アルゴリズム、または、wav 圧縮アルゴリズムを使用することができる。もちろん、デジタルコンテンツ 12 が、既に圧縮された状態にあることも可能であり、その場合、さらなる圧縮は必要ない。

10

【0037】

デジタルコンテンツ 12 に付随すべき命令および／または規則には、本発明の趣旨および範囲を逸脱することなく、実質的にあらゆる適切な命令、規則、または他の情報が含まれることが可能である。以下に述べるとおり、付随する命令／規則／情報は、主に、デジタルコンテンツ 12 をレンダリングするライセンス 16 を獲得するためにユーザ、およびユーザの計算デバイス 14 によって使用される。したがって、付随する命令／規則／情報には、以下により詳細に説明するとおり、適切にフォーマットされたライセンス獲得スクリプト等が含まれることが可能である。追加として、または別法として、付随する命令／規則／情報には、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」情報が含まれることが可能である。

20

【0038】

供給された情報を使用して、オーサリングツール 18 は、デジタルコンテンツ 12 に対応する 1 つまたは複数のパッケージ 12 p を生成する。次に、各パッケージ 12 p を世界に配布するためにコンテンツサーバ 22 上に記憶することができる。

【0039】

本発明の一実施形態では、図 2 を参照すると、オーサリングツール 18 は、指定し、操作することが可能な入力パラメータを受け取る動的オーサリングツール 18 である。したがって、オーサリングツール 18 は、複数のデジタルコンテンツ 12 に関して複数の変種のパッケージ 12 p を迅速に生成することができる。好ましくは、入力パラメータは、図示するとおり、情報 28 の形態で実現され、辞書 28 は、以下のようなパラメータを含む。

30

ーデジタルコンテンツ 12 を有する入力ファイル 29 a の名前。

ー行われるべき符号化のタイプ。

ー使用されるべき暗号化／暗号化解除鍵 (KD)。

ーデジタルコンテンツ 12 とともにパッケージ 12 p の中にパッケージ化されるべき付随する命令／規則／情報 (「ヘッダ情報」)。

ー行われるべき多重化 (muxing) のタイプ。

ーデジタルコンテンツ 12 に基づいてパッケージ 12 p が書き込まれるべき出力ファイル 29 b の名前。

【0040】

理解されるべきこととして、辞書 28 は、オーサリングツール 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変更可能であり、したがって、オーサリングツール 18 によって行われるオーサリングのタイプも同様に、動的な仕方で容易かつ迅速に変更可能である。本発明の一実施形態では、オーサリングツール 18 は、人間のオペレータに対してコンピュータスクリーン上で表示可能なオペレータインターフェース (図示せず) を含む。したがって、オペレータは、そのインターフェースを使用して辞書 28 を変更することができ、またさらに、そのインターフェースを使用して辞書 28 を変更する際に適切な支援および／または制限を受けることが可能である。

40

【0041】

オーサリングツール 18 内部で、図 2 に見られるとおり、ソースフィルタ 18 a が、デジタルコンテンツ 12 を有する入力ファイル 29 a を辞書 28 から受け取り、その入力ファ

50

イルからデジタルコンテンツ12を取得して、デジタルコンテンツ12をRAMなどのメモリ29cの中に入れる。次に、符号化フィルタ18bが、メモリ29cの中のデジタルコンテンツ12に対して符号化を行い、辞書28の中で指定される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に（すなわち、.wavから.aspに、.mp3から.aspになど）転換し、符号化されたデジタルコンテンツ12をメモリ29cの中に入れる。図示するとおり、パッケージ化されるべきデジタルコンテンツ（例えば、音楽）が、.wav形式または.mp3形式などの圧縮された形式で受け取られ、.asp（アクティブストリーミングプロトコル（active streaming protocol））形式などの形式に変換される。もちろん、本発明の趣旨および範囲を逸脱することなく、他の入力形式および出力形式を使用することができる。

10

【0042】

その後、暗号化フィルタ18cが、辞書28の中で指定された暗号化／暗号解除鍵（KD）に従ってメモリ29cの中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の中に入れる。次に、ヘッダフィルタ18dが、辞書28の中で指定されたヘッダ情報をメモリ29cの中の暗号化されたデジタルコンテンツ12に追加する。

【0043】

理解されるべきこととして、状況に応じて、パッケージ12pは、複数のストリームが多重化された（すなわち、「mux処理」された）時間的に揃えられたデジタルコンテンツ12の複数のストリーム（図2では、1つのストリームを示している）を含むことが可能である。したがって、多重化フィルタ（mux filter）18eが、辞書28の中で指定された多重化のタイプに従ってメモリ29cの中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に対して多重化を行い、その結果をメモリ29cの中に入れる。次に、ファイルライタフィルタ（file writer filter）18fが、その結果をメモリ29cから取得し、辞書28の中で指定された出力ファイル29bにその結果をパッケージ12pとして書き込む。

20

【0044】

ある状況では、行われるべき符号化のタイプは、通常、変化しないことに留意されたい。多重化のタイプは、通常、符号化のタイプに基づくので、同様に、多重化のタイプも、変化しないことが通例である。実際に変化しない場合、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がない。実際、符号化のタイプが、符号化フィルタの中に「配線によって組まれ（hardwired）」、かつ／または多重化のタイプが、多重化フィルタの中に「配線によって組まれる」だけでよい。もちろん、本発明の趣旨および範囲を逸脱することなく、状況によって必要とされるのに応じて、オーサリングツール18は、前述したフィルタのすべてを含むこと、または他のフィルタを含むことが可能であり、またあらゆる含まれるフィルタが、配線によって組まれる、または辞書28の中で指定されたパラメータに従って機能を行うことが可能である。

30

【0045】

好ましくは、オーサリングツール18は、適切なソフトウェアを使用して適切なコンピュータ上、プロセッサ上、または他の計算マシン上に実装される。そのようなマシン、およびそのようなソフトウェアの構造および動作は、本明細書の開示に基づいて明白であるはずであり、したがって、本開示において詳述することは必要ない。

40

【0046】

<アーキテクチャーコンテンツサーバ22>

図1を再び参照すると、本発明の一実施形態では、コンテンツサーバ22が、オーサリングツール18によって生成されたパッケージ12pを配信するか、または別の形で取得のために供与する。パッケージ12pは、本発明の趣旨および範囲を逸脱することなく、コンテンツサーバ22が要求するのに応じて任意の適切な配信チャネルを使用して配信されることが可能である。例えば、配信チャネルは、インターネットまたは別のネットワーク、電子掲示板、電子メール等であることが可能である。コンテンツサーバ22を使用して

50

パッケージ 12 p を磁気ディスク、または光ディスク、あるいはその他の記憶デバイスにコピーすることができ、次に、記憶デバイスを配布することができる。

【0047】

コンテンツサーバ 22 は、信頼問題またはセキュリティ問題を顧慮せずにパッケージ 12 p を配信することが認められよう。以下で述べるとおり、そのような問題は、ライセンスサーバ 24、およびライセンスサーバ 24 とユーザの記憶デバイス 14 の間の関係に関連して対処される。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 を要求するあらゆる配信先 (d i s t r i b u t e e) にデジタルコンテンツ 12 を有するパケット 12 p を自由にリリースし、配信する。ただし、コンテンツサーバ 22 は、配信に先立って所定の配信料の支払いをまず要求する、あるいは配信先が自らを認証することを要求する、あるいは実際に、配信先の識別に基づいて配信が行われるべきかどうかを決定することが可能である。

10

【0048】

さらに、予期されるデマンドを満たすように事前にいくつかの異なるパッケージ 12 p を生成するようにオーサリングツール 18 を制御することにより、コンテンツサーバ 22 を使用してインベントリ (i n v e n t o r y) 管理を行うことができる。例えば、サーバは、同一のデジタルコンテンツ 12 に基づいて 100 のパッケージを生成し、各パッケージ 12 p を 10 回、提供することが可能である。例えば、パッケージ 12 p の供給が、20 まで減少すると、コンテンツサーバ 22 は、やはり例として、80 のさらなるパッケージ 12 p を生成するようにオーサリングツール 18 を導くことができる。

20

【0049】

好ましくは、アーキテクチャ 10 におけるコンテンツサーバ 22 は、以下により詳細に説明するとおり、ライセンス 16 を評価し、対応するデジタルコンテンツ 12 を暗号化解除するための暗号化解除鍵 (K D) を獲得するプロセスの一環として使用される固有の公開鍵／秘密鍵ペア (P U - C S、P R - C S) を有する。周知のとおり、公開鍵／秘密鍵ペアは、鍵ペアの鍵の 1 つで暗号化されたものが、鍵ペアの鍵の他方によってだけ暗号化解除することができることで、非対称鍵である。公開鍵／秘密鍵ペア暗号化システムでは、公開鍵は、世界に知らせてもよいが、秘密鍵は、秘密鍵の所有者によって常に秘密に保たなければならない。したがって、コンテンツサーバ 22 は、秘密鍵 (P R - C S) を使用してデータを暗号化した場合、暗号化解除の目的で、公開鍵 (P U - C S) とともにその暗号化されたデータを世界に送り出すことができる。したがって、外部デバイスが、コンテンツサーバ 22 だけがデータを暗号化解除することができるようにデータをコンテンツサーバ 22 に送ることを望む場合、外部デバイスは、まず、そのコンテンツサーバ 22 の公開鍵 (P U - C S) を獲得し、次に、その公開鍵を使用してデータを暗号化しなければならない。したがって、次に、コンテンツサーバ 22 が (また、コンテンツサーバ 22 だけが)、その秘密鍵 (P R - C S) を使用して暗号化されたデータを暗号化解除することができる。

30

【0050】

オーサリングツール 18 と同様に、コンテンツサーバ 22 も、適切なソフトウェアを使用して適切なコンピュータ上、プロセッサ上、またはその他の計算マシン上で実装される。そのようなマシンおよびそのようなソフトウェアの構造および動作は、本明細書の開示に基づいて明白であるはずであり、したがって、本開示で詳述することは必要ない。本発明の一実施形態では、オーサリングツール 18、およびコンテンツサーバ 22 が、それぞれ別個の作業スペース内で、単一のコンピュータ上、単一のプロセッサ上、または単一の他の計算マシン上に常駐することが可能である。さらに、コンテンツサーバ 22 は、ある状況では、前述したとおり、オーサリングツール 18 を含むことが可能であり、かつ／またはオーサリングツール 18 の機能を行うことが可能であることを認識されたい。

40

【0051】

<デジタルコンテンツパッケージ 12 p の構造>

次に、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

50

されるデジタルコンテンツパッケージ12pが、以下のものを含む。

- ー前述したとおり、暗号化／暗号化解除鍵(KD)を使用して暗号化されたデジタルコンテンツ12(すなわち、(KD(CONTENT)))、
- ー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)、
- ー暗号化解除鍵(KD)の鍵ID。
- ー好ましくは、暗号化されていない形態のライセンス獲得情報。
- ーコンテンツサーバ22秘密鍵(PR-CS)で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)))。

10

【0052】

(KD(PU-CS)S(PR-CS))に関して、このアイテムは、以下に説明するとおり、デジタルコンテンツ12および／またはパッケージ12pを検証すること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(以下を参照)を有する証明書とは異なり、(KD(PU-CS))を得るのに鍵(PU-CS)は必要ない。代わりに、鍵(PU-CS)は、単に暗号化解除鍵を適用することによって獲得される。獲得されると、その鍵(PC-CS)を使用して署名(S(PR-CS))の有効性を試験することができる。

【0053】

また、パッケージ12pがオーサリングツール18によって構成されるには、オーサリングツール18が、想定では、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、オーサリングツール18とコンテンツサーバ22が、想定では、(KD(PU-CS)S(PR-CS))を構成するように対話しなければならない。この対話は、例えば、以下のステップを含むことが可能である。

20

- ー(PU-CS)をオーサリングツール18に送るコンテンツサーバ22。
- ー(KD)を使用して(PU-CS)を暗号化して(KD(PU-CS))を生成するオーサリングツール18。
- ー(KD(PU-CS))をコンテンツサーバ22に送るオーサリングツール18。
- ー(PR-CS)を使用して(KD(PU-CS))に署名して(KD(PU-CS)S(PR-CS))を生成するコンテンツサーバ22。
- ー(KD(PU-CS)S(PR-CS))をオーサリングツール18に送るコンテンツサーバ22。

30

【0054】

<アーキテクチャーライセンスサーバ24>

図1を再び参照すると、本発明の一実施形態では、ライセンスサーバ24が、デジタルコンテンツ12に関連してユーザの計算デバイス14からライセンス16の要求を受け取る機能、ユーザの計算デバイス14が、発行されたライセンス16を遵守するものとして信頼できるかどうかを判定する機能、ライセンス16を交渉する機能、ライセンス16を構成する機能、およびライセンス16をユーザの計算デバイス14に伝送する機能を行う。好ましくは、伝送されるライセンス16は、デジタルコンテンツ12を暗号化解除するための暗号化解除鍵(KD)を含む。このライセンスサーバ24、および以上の機能を以下により詳細に説明する。好ましくは、コンテンツサーバ22と同様に、アーキテクチャ10におけるライセンスサーバ24は、以下により詳細に説明するとおり、ライセンス16を評価し、対応するデジタルコンテンツ12を暗号化解除するための暗号化解除鍵(KD)を獲得するプロセスの一環として使用される固有の公開鍵／秘密鍵ペア(PU-LS、PR-LS)を有する。

40

【0055】

オーサリングツール18およびコンテンツサーバ22と同様に、ライセンスサーバ24は、適切なソフトウェアを使用して適切なコンピュータ上、プロセッサ上、または他の計算

50

マシン上に実装される。そのようなマシンおよびそのようなソフトウェアの構造および動作は、本明細書の開示に基づいて明白であるはずであり、したがって、本開示において詳述する必要はない。さらに、本発明の一実施形態では、オーサリングツール18および／またはコンテンツサーバ22が、ライセンスサーバ24とともに、それぞれ別個の作業スペース内で、単一のコンピュータ上、単一のプロセッサ上、または単一の他の計算マシン上に常駐することが可能である。

【0056】

本発明の一実施形態では、ライセンス16の発行に先立って、ライセンスサーバ24とコンテンツサーバ22は、ライセンスサーバ24が、実際に、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の少なくとも一部分に関してライセンス機関 (licensing authority) となることに合意する代理契約 (agency agreement) 等を結ぶ。理解されるべきこととして、本発明の趣旨および範囲を逸脱することなく、1つのコンテンツサーバ22が、いくつかのライセンスサーバ24と代理契約等を結ぶことができ、かつ／または1つのライセンスサーバ24が、いくつかのコンテンツサーバ22と代理契約等を結ぶことができる。

10

【0057】

好ましくは、ライセンスサーバ24は、実際に、自らが、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を発行する権限を有することを世界に示すことができる。これを行うため、ライセンスサーバ24が、コンテンツサーバ22にライセンスサーバ24公開鍵 (PULS) を送り、また次に、コンテンツサーバ22が、ライセンスサーバ24に、コンテンツサーバ22秘密鍵で署名されたコンテンツ (CERT (PULS) S (PRCS)) としてPULSを含むデジタル証明書を送ることが好ましい。理解されるべきこととして、証明書の中のコンテンツ (PULS) には、コンテンツサーバ22公開鍵 (PUCS) を使用してだけアクセスすることが可能である。やはり理解されるべきこととして、一般に、基底のデータのデジタル署名は、そのデータの暗号化された形態であり、そのデータが改ざんされている場合、または別の仕方で変更されている場合、そのデータにマッチしない。

20

【0058】

デジタルコンテンツ12に関連するライセンス機関として、またライセンス機能の一環として、ライセンスサーバ24は、デジタルコンテンツ12に関する暗号化解除鍵 (KD) へのアクセスを有さなければならない。したがって、ライセンスサーバ24が、デジタルコンテンツ12 (またはパッケージ12p) に関する暗号化解除鍵 (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にアクセスを有することが好ましい。

30

【0059】

<アーキテクチャブラックボックスサーバ26>

やはり図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、ユーザの計算デバイス14における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／またはアップグレードする機能を行う。以下により詳細に説明するとおり、ブラックボックス30は、ユーザの計算デバイス14のために暗号化機能、および暗号化解除機能を行う。やはり、以下により詳細に説明するとおり、ブラックボックス30は、攻撃に対してセキュアであり、保護されているものとされる。このセキュリティおよび保護は、以下により詳細に説明するとおり、少なくともある程度、ブラックボックスサーバ26を使用して、必要に応じて、ブラックボックス30を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。

40

【0060】

オーサリングツール18と同様に、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は、適切なソフトウェアを使用して適切なコンピュータ上、プロセッサ上、または他の計算マシン上に実装される。そのようなマシンおよびそのようなソフトウェアの構造および動作は、本明細書の開示に基づいて明白であるはずであり

50

、したがって、本開示において詳述することは必要ない。さらに、本発明の一実施形態では、ライセンスサーバ24、オーサリングツール18、および／またはコンテンツサーバ22が、それぞれ別個の作業スペース内で、ブラックボックスサーバ26とともに、単一のコンピュータ上、単一のプロセッサ上、または単一の他の計算マシン上に常駐することが可能である。ただし、セキュリティ上の目的で、ブラックボックスサーバ26を別個のマシン上に有することが賢明である可能性があることに留意されたい。

【0061】

次に、図4を参照すると、本発明の一実施形態では、ユーザの計算デバイス14は、キーボード、マウス、スクリーン、プロセッサ、RAM、ROM、ハードドライブ、フロッピー（登録商標）ドライブ、CDプレーヤ、および／または以上に類するものを含む要素を有するパーソナルコンピュータ等である。ただし、ユーザの計算デバイス14は、本発明の趣旨および範囲を逸脱することなく、とりわけ、テレビジョンまたはモニタなどの専用ビューイング（viewing）デバイス、ステレオプレーヤ、またはその他の音楽プレーヤなどの専用オーディオデバイス、専用プリンタ等であることも可能である。

10

【0062】

デジタルコンテンツ12のコンテンツ所有者は、ユーザの計算デバイス14が、コンテンツ所有者自身が指定した規則を遵守すること、すなわち、求める仕方でレンダリングを可能にするライセンス16をユーザが獲得しない限り、デジタルコンテンツ12がレンダリングされないことを信頼しなければならない。したがって、好ましくは、ユーザの計算デバイス14は、デジタルコンテンツ12に関連し、ユーザによって獲得されるライセンス16で実現されるライセンス規則に従ってでなければ、デジタルコンテンツ12をレンダリングしないことをコンテンツ所有者に確信させることができる信頼される構成要素、または信頼される機構32を提供しなければならない。

20

【0063】

この場合、信頼される機構32は、デジタルコンテンツ12がレンダリングされることをユーザが要求したときにイネーブルにされ、求める仕方でデジタルコンテンツ12をレンダリングするライセンス16をユーザが有するかどうかを判定し、必要な場合、そのライセンス16を獲得することを実行し、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ライセンス16に従って判定し、また、ライセンス16に従ってユーザがそのような権利を実際に有する場合、レンダリング目的でデジタルコンテンツ12を暗号化解除するデジタル権利管理（DRM）システム32である。ユーザの計算デバイス14上の、アーキテクチャ10に関連するDRMシステム32の内容および機能を以下に説明する。

30

【0064】

<DRMシステム32>

DRMシステム32は、本明細書に開示するアーキテクチャ10を使用して以下の4つの主な機能を行う。すなわち、（1）コンテンツ獲得、（2）ライセンス獲得、（3）コンテンツレンダリング、および（4）ブラックボックス30インストール／更新である。好ましくは、以上の機能の任意のものが、任意の時点で行われることが可能である。ただし、機能のいくつかは、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ことが認められる。

40

【0065】

<DRMシステム32－コンテンツ獲得>

ユーザおよび／またはユーザの計算デバイス14によるデジタルコンテンツ12の獲得は、通常、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計算デバイス14上に置くことに関わる。もちろん、本明細書で開示するアーキテクチャ10、およびDRMシステム32で機能するには、暗号化されたデジタルコンテンツ12が、以下に説明するとおり、デジタルパッケージ12pなどの、アーキテクチャ10およびDRMシステム32に適する形態になっていることが必要である。

【0066】

50

理解されるべきこととして、デジタルコンテンツ 12 は、本発明の趣旨および範囲を逸脱することなく、直接に、または間接的に、コンテンツサーバ 22 から任意の仕方で獲得することが可能である。例えば、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されること、獲得された光ディスクまたは磁気ディスク等の上に存在すること、電子メール等の一部として受信されること、または電子掲示板等からダウンロードされることが可能である。

【0067】

デジタルコンテンツ 12 は、獲得されると、好ましくは、計算デバイス 14 上で実行されるレンダリングアプリケーション 34（以下に説明する）によって、または DRM システム 32 によってアクセス可能であるように記憶される。例えば、デジタルコンテンツ 12 は、ユーザの計算デバイス 14 のハードドライブ（図示せず）上、または計算デバイス 14 がアクセス可能なネットワークサーバ（図示せず）上のファイルとして配置することが可能である。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獲得される場合、そのディスクが、ユーザの計算デバイス 14 に結合された適切なドライブ（図示せず）の中に存在するだけでよい可能性がある。

【0068】

本発明では、直接の配布ソースとしてのコンテンツサーバ 22 からも、間接の配布ソースとしての何らかの仲介役からも、デジタルコンテンツ 12 を獲得するのに特別なツールが必要であることを全く想定していない。つまり、デジタルコンテンツ 12 が、他のあらゆるデータファイルと同様に容易に獲得されることが好ましい。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 を獲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）を含むことが可能である。例えば、このインターフェースは、デジタルコンテンツ 12 を探索すること、デジタルコンテンツ 12 のソースであることが分かっている事前定義されたインターネット Web サイトにリンクすること等を行うように特に設計された Web ブラウザを含むことが可能である。

【0069】

<DRM システム 32－コンテンツレンダリング、第 1 部>

次に、図 5A 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、ユーザに配布されて受け取られ、ユーザによって記憶されたファイルの形態で計算デバイス 14 上に置かれたものと想定して、ユーザが、レンダリングコマンドの何らかの変種を実行することにより、デジタルコンテンツ 12 をレンダリングしようと試みる（ステップ 501）。例えば、そのようなレンダリングコマンドは、デジタルコンテンツ 12 を「再生する」要求、または「開く」要求として実現することができる。例えば、ワシントン州レッドモンドのマイクロソフトコーポレーションによって販売される「MICROSOFT WINDOWS（登録商標）」オペレーティングシステムなどの一部の計算環境では、この再生コマンド、または開くコマンドは、単にデジタルコンテンツ 12 を表すアイコン上で「クリックする」程度の簡単なものであることが可能である。もちろん、本発明の趣旨および範囲を逸脱することなく、レンダリングコマンドの他の実施形態も使用することができる。一般に、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 を有するファイルが開かれ、遂行され、実行され、かつ／または以上に類することが行われるように指示したときにはいつでも、実行されるものと見なすことができる。

【0070】

重要なことには、さらに、レンダリングコマンドは、デジタルコンテンツ 12 を、印刷された形態、ビジュアル形態、オーディオ形などの別の形態にコピーする要求として実現することができる。理解されるべきこととして、同一のデジタルコンテンツ 12 を、コンピュータスクリーン上などのある形態でレンダリングし、次に、印刷されたドキュメントなどの別の形態でレンダリングすることが可能である。本発明では、各タイプのレンダリングは、以下に説明するとおり、ユーザがレンダリングを行う権利を有する場合にだけ行われる。

【0071】

本発明の一実施形態では、デジタルコンテンツ12は、拡張子で終わるファイル名を有するデジタルファイルの形態になっており、計算デバイス14が、その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を開始することを決めることができる。例えば、ファイル名拡張子が、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す場合、レンダリングアプリケーション34は、ワシントン州レッドモンドのマイクロソフトコーポレーションによって販売される「MICROSOFT WORD」などの何らかの形態のワードプロセッサである。同様に、ファイル名拡張子が、デジタルコンテンツ12がオーディオファイル、ビデオファイル、および／またはマルチメディアファイルであることを示す場合、レンダリングアプリケーション34は、やはり、ワシントン州レッドモンドのマイクロソフトコーポレーションによって販売される「MICROSOFT MEDIA PLAYER」などの何らかの形態のマルチメディアプレーヤである。

10

【0072】

もちろん、本発明の趣旨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決める他の方法を使用することも可能である。単に一例として、デジタルコンテンツ12は、その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を含むメタデータを暗号化されていない形態（すなわち、前述したヘッダ情報の形態）で含むことが可能である。

【0073】

好ましくは、レンダリングアプリケーション34は、ファイル名に関連するデジタルコンテンツ12を検査し、そのデジタルコンテンツ12が、権利の保護された形態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、無造作にレンダリングすることができる（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、そのデジタルコンテンツ12を再生するのにDRMシステム32が必要であると判定する。したがって、レンダリングアプリケーション34は、ユーザの計算デバイス14が、そのデバイス14上のDRMシステム32を実行するように導く（ステップ509）。次に、レンダリングアプリケーション34は、DRMシステム32を呼び出してデジタルコンテンツ12を暗号化解除する（ステップ511）。以下により詳述するとおり、DRMシステム32は、ユーザが、デジタルコンテンツ12に関して有効なライセンス16を有し、その有効なライセンス16におけるライセンス規則に従ってデジタルコンテンツ12を再生する権利を有する場合にだけ、実際にそのデジタルコンテンツ12を暗号化解除する。好ましくは、DRMシステム32は、レンダリングアプリケーション34によって呼び出された後、少なくとも、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判定する目的で、レンダリングアプリケーション34から制御を引き継ぐ（ステップ513）。

20

30

【0074】

本発明の一実施形態では、図4を再び参照すると、DRMシステム32が、ライセンスイバリュエータ36、ブラックボックス30、ライセンスストア38、および状態ストア40を含む。

40

【0075】

<DRMシステム32構成要素—ライセンスイバリュエータ36>

ライセンスイバリュエータ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つまたは複数のライセンス16を探し出し、そのライセンス16が有効であるかどうかを判定し、有効なライセンス16におけるライセンス規則を検討し、検討したライセンス規則に基づき、要求側のユーザが、求める仕方でも要求のデジタルコンテンツ12をレンダリングする権利を有するかどうかを判定する。理解されるべきこととして、ライセンスイバリュエータ36は、DRMシステム32における信頼される構成要素である。本開示では、「信頼される」ということは、ライセンスサーバ24（または任意の他の信頼する側の要素）が、信頼される要素が、ライセンス16における権利記述に従ってデジタル

50

コンテンツ 12 の所有者の願いを実行すること、およびユーザが、不正な、または別の何らかの目的で信頼される要素を容易に変更できないことを確信させられることを意味する。

【0076】

ライセンスイバリユータ 36 は、実際にライセンス 16 を適切に評価することを確実にするため、またライセンス 16 の実際の評価を回避する目的で、ユーザによって不正改造されている、または別の仕方に変更されていることがないことを確実にするため、信頼されなければならない。したがって、ライセンスイバリユータ 36 は、保護された環境、または覆われた環境において実行して、ライセンスイバリユータ 36 に対するユーザのアクセスが拒否されるようにする。本発明の趣旨および範囲を逸脱することなく、ライセンスイバリユータ 36 に関連して他の保護手段も使用することができる。

10

【0077】

＜DRMシステム 32 構成要素－ブラックボックス 30＞

主に、前述したとおり、ブラックボックス 30 は、DRMシステム 32 において暗号化機能および暗号化解除機能を行う。詳細には、ブラックボックス 30 は、ライセンスイバリユータ 36 と連携して動作して、ある情報をライセンスイバリユータ機能の一環として暗号化解除すること、および暗号化することを行う。さらに、ライセンスイバリユータ 36 が、ユーザが、求める仕方で要求のデジタルコンテンツ 12 をレンダリングする権利を実際に有すると判定すると、ブラックボックス 30 は、デジタルコンテンツ 12 に関する暗号化解除鍵（KD）の提供を受け、暗号化解除鍵（KD）に基づいてデジタルコンテンツ 12 の暗号化解除の機能を行う。

20

【0078】

ブラックボックス 30 は、DRMシステム 32 の信頼される構成要素でもある。詳細には、ライセンスサーバ 24 が、ブラックボックス 30 が、ライセンス 16 におけるライセンス規則に従ってだけ暗号化解除機能を行うことを信頼し、またブラックボックス 30 が、ライセンス 16 の実際の評価を回避するという不正な目的で、ユーザによって不正改造された、または別の仕方に変更された場合、動作しないことを信頼しなければならない。したがって、ブラックボックス 30 も、保護された環境、または覆われた環境において実行して、ブラックボックス 30 に対するユーザのアクセスが拒否されるようにする。この場合も、本発明の趣旨および範囲を逸脱することなく、ブラックボックス 30 に関連して他の保護手段も使用することができる。好ましくは、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 におけるブラックボックス 30 は、以下により詳細に説明するとおり、ライセンス 16 を評価し、デジタルコンテンツ 12 を暗号化解除するための暗号化解除鍵（KD）を獲得するプロセスの一環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。

30

【0079】

＜DRMシステム 32 構成要素－ライセンスストア 38＞

ライセンスストア 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 を記憶する。ライセンスストア 38 自体は、信頼される必要はない。というのは、ライセンスストア 38 は、以下に説明するとおり、信頼構成要素がそれぞれ、内部に既に組み込まれていなければならないライセンス 16 を単に記憶するだけだからである。本発明の一実施形態では、ライセンスストア 38 は、ハードディスクドライブまたは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に過ぎない。ただし、ライセンスストア 38 は、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 を記憶する機能を行う限り、本発明の趣旨および範囲を逸脱することなく、任意の他の形態で実現することができる。

40

【0080】

＜DRMシステム 32 構成要素－状態ストア 40＞

状態ストア 40 は、現在、ライセンスストア 38 の中にある、または以前にライセンスストア 38 の中にあったライセンス 16 に対応する状態情報を保持する機能を行う。状態情

50

報は、DRMシステム32によって生成され、必要に応じて状態ストア40の中に記憶される。例えば、特定のライセンス16により、対応するデジタルコンテンツ12の所定回数のレンダリングだけが許される場合、状態ストア40は、ライセンス16に関連して何回のレンダリングが実際に行われたかに関する状態情報を保持する。状態ストア40は、ライセンスストア38の中にもはや存在しないライセンス16に関する状態情報を保持しつつ、そうでなければ、ライセンスストア38からライセンスを削除した後、状態ストア40から対応する状態情報を削除しようとして同一のライセンス16を獲得することが有利である状況を回避する。

【0081】

状態ストア40も、内部に記憶されている情報が、ユーザにより都合の良い状態にリセットされないことを確実にするために信頼されなければならない。したがって、状態ストア40も同様に、保護された環境、または覆われた環境において実行して、状態ストア40に対するユーザのアクセスが拒否されるようにする。この場合も、本発明の趣旨および範囲を逸脱することなく、もちろん、他の保護手段も使用することができる。例えば、状態ストア40は、DRMシステム32によって計算デバイス14上に暗号化された形態で記憶されることが可能である。

【0082】

<DRMシステム32—コンテンツレンダリング、第2部>

図5Aを再び参照し、本発明の一実施形態におけるコンテンツレンダリングについて再び述べると、DRMシステム32は、呼出し側のレンダリングアプリケーション34から制御を引き継いだ後、ユーザが、求める仕方で要求のデジタルコンテンツ12を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。詳細には、DRMシステム32は、ライセンスストアの中で有効な、使用を可能にするライセンス16を探し出すか（ステップ515、517）、またはライセンスサーバ24から、有効な、使用を可能にするライセンス16を獲得しようとする（すなわち、以下に述べ、図7に示すライセンス獲得機能を行う）。

【0083】

第1のステップとして、図6を参照すると、DRMシステム32のライセンスイバリュエータ36が、デジタルコンテンツ12に対応する1つまたは複数の受け取られたライセンス16の存在に関してライセンスストア38を検査する（ステップ601）。通常、ライセンス16は、以下に述べるとおり、デジタルファイルの形態になっている。ただし、ライセンス16は、本発明の趣旨および範囲を逸脱することなく、他の形態になっていることも可能であることが認められよう。通常、ユーザは、ライセンス16なしにデジタルコンテンツ12を受け取る。ただし、デジタルコンテンツ12は、本発明の趣旨および範囲を逸脱することなく、対応するライセンス16とともに受け取られることが可能であることも同様に認められよう。

【0084】

図3に関連して前述したとおり、各デジタルコンテンツ12は、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を暗号化解除する暗号化解除鍵（KD）を識別する鍵IDを備えたパッケージ12pの中にある。好ましくは、コンテンツID（またはパッケージID）、および鍵IDは、暗号化解除されていない形態になっている。したがって、特に、デジタルコンテンツ12のコンテンツIDに基づき、ライセンスイバリュエータ36は、そのコンテンツIDに該当する識別子を含むライセンス16をライセンスストア38の中で探す。特に、デジタルコンテンツ12の所有者が、デジタルコンテンツ12に関して複数の異なる種類のライセンス16を指定しており、ユーザが、そのライセンス16のなかの複数のライセンスを獲得している場合、複数のそのようなライセンスが見出される可能性があることに留意されたい。実際、ライセンスイバリュエータ36が、要求のデジタルコンテンツ12に対応するライセンス16をライセンスストア38の中で全く見出さなかった場合、DRMシステム32は、以下に説明するライセンス獲得の機能（図

10

20

30

40

50

5のステップ519)を行うことが可能である。

【0085】

次に、DRMシステム32に、デジタルコンテンツ12をレンダリングする要求が行われており、またデジタルコンテンツ12に対応する1つまたは複数のライセンス16が、ライセンスストア38の中に存在するものと想定する。本発明の一実施形態では、DRMシステム32のライセンスイバリユエータ36は、各ライセンス16に関して、そのライセンス16自体が有効であるかどうかを判定することに取りかかる(図6のステップ603および605)。好ましくは、詳細には、各ライセンス16が、そのライセンス16のコンテンツ28に基づくデジタル署名を含む。理解されるべきこととして、デジタル署名26は、コンテンツ28が改ざんされているか、または別の仕方に変更されている場合、ライセンス16にマッチしない。したがって、ライセンスイバリユエータ36は、デジタル署名26に基づき、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態をしている(すなわち、有効である)かどうかを判定することができる。有効なライセンス16がライセンスストア38の中で見出されなかった場合、DRMシステム32は、以下に説明するライセンス獲得機能を行って有効なライセンス16を獲得することができる。

10

【0086】

1つまたは複数の有効なライセンス16が見出されたと想定すると、それぞれの有効なライセンス16に関して、DRMシステム32のライセンスイバリユエータ36が、次に、その有効なライセンス16が、所望の仕方に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ユーザに与える(すなわち、使用を可能にするものである)かどうか判定する(ステップ607および609)。詳細には、ライセンスイバリユエータ36は、各ライセンス16における権利記述に基づき、またユーザが、デジタルコンテンツ12に何をしようとしているかに基づき、要求側のユーザが、要求の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、この権利記述により、ユーザが、デジタルコンテンツ12をサウンドにレンダリングすることが許されるが、暗号化解除されたデジタルコピーにレンダリングすることは許されない。

20

【0087】

理解されるべきこととして、各ライセンス16における権利記述は、ユーザが誰であるか、どこにユーザが所在するか、どのようなタイプの計算デバイス14をユーザが使用しているか、どのような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、時刻等を含め、いくつかのファクタの任意のものに基づき、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、例えば、所定の回数の再生に、または所定の再生時間にライセンスを制限することが可能である。そのような場合、DRMシステム32は、ライセンス16に関してあらゆる状態情報(すなわち、何回、デジタルコンテンツ12が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等)を参照しなければならず、この状態情報は、ユーザの計算デバイス14上のDRMシステム32の状態ストア40の中に記憶されている。

30

【0088】

したがって、DRMシステム32のライセンスイバリユエータ36が、それぞれ有効なライセンス16の権利記述を検討して、その有効なライセンス16により、求めている権利がユーザに与えられるかどうかを判定する。これを行う際、ライセンスイバリユエータ36は、ユーザの計算デバイス14にローカルな他のデータを参照して、ユーザが、求めている権利を有するかどうかの判定を行う。図4に見られるとおり、このデータは、ユーザの計算デバイス(マシン)14の識別42およびデバイス14の特定の態様、ユーザの識別44およびユーザの特定の態様、レンダリングアプリケーション34の識別およびアプリケーション34の特定の態様、システムクロック46等を含むことが可能である。求める仕方デジタルコンテンツ12を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が見出されない場合、DRMシステム32は、以下に説明するライセンス獲得機能を行い、そのようなライセンス16が実際に獲得可能である場合、そのライセンス1

40

50

6を獲得する。

【0089】

もちろん、一部の場合、ユーザは、要求する仕方ではデジタルコンテンツ12をレンダリングする権利を獲得することができない。というのは、デジタルコンテンツ12のコンテンツ所有者が、そのような権利が許可されるべきでないことを実際に指示しているからである。例えば、デジタルコンテンツ12のコンテンツ所有者が、ユーザがテキストドキュメントを印刷すること、または暗号化されていない形態でマルチメディアプレゼンテーションをコピーすることを許すライセンス16が交付されるべきでないことを指示していることが可能である。本発明の一実施形態では、デジタルコンテンツ12は、ライセンス16の購入時にどのような権利が入手可能かに関するデータ、および入手可能なライセンス16のタイプに関するデータを含む。ただし、デジタルコンテンツ12のコンテンツ所有者は、デジタルコンテンツ12に関して入手可能なライセンス16を変更することにより、デジタルコンテンツに関して現行で入手可能な権利を任意の時点で変更できることが認められよう。

【0090】

<DRMシステム32－ライセンス獲得>

次に、図7を参照すると、ライセンスイバリユエータ36が、実際に、要求されたデジタルコンテンツ12に対応する有効な、使用を可能にするライセンス16をライセンスストア38の中で見出さなかった場合、DRMシステム32が、ライセンス獲得の機能を行うことが可能である。図3に示すとおり、各デジタルコンテンツ12は、その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をどのように獲得するかに関する暗号化されていない形態の情報（すなわち、ライセンス獲得情報）とともにパッケージ化される。

【0091】

本発明の一実施形態では、ライセンス獲得情報は、とりわけ、入手可能なライセンス16のタイプを含み、また各ライセンスサーバ24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場合、1つまたは複数の適切なライセンスサーバ24にアクセスすることが可能な1つまたは複数のインターネットWebサイト、または他のサイト情報を含むことが可能である。もちろん、ライセンス16は、本発明の趣旨および範囲を逸脱することなく、他の仕方でも獲得することも可能である。例えば、ライセンス16は、電子掲示板において、あるいは磁気ディスクまたは光ディスク等の上のファイルの形態で直接に、または通常の郵便を介してでも獲得することが可能である。

【0092】

ライセンス16を獲得するための場所が、実際に、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、ライセンスイバリユエータ36が、Webサイト情報、または他のサイト情報に基づき、ライセンスサーバ24に対するネットワーク接続を確立し、次に、接続されたライセンスサーバ24にライセンス16の要求を送信する（ステップ701、703）。詳細には、DRMシステム32は、ライセンスサーバ24に接触すると、適切なライセンス要求情報36をそのライセンスサーバ24に伝送する。

【0093】

本発明の一実施形態では、ライセンス16は、以下に類するものを含むことが可能な情報36を要求する。すなわち、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）。

－DRMシステム32のブラックボックス30のバージョン番号。

－ブラックボックス30を認定する認定機関からのデジタル署名を伴う証明書（ただし、証明書は、ブラックボックス30の前述した公開鍵およびバージョン番号を実際に含む）。

－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）。

－デジタルコンテンツ12を暗号化解除するための暗号化解除鍵（KD）を識別する鍵I

10

20

30

40

50

D。

ー要求されたライセンス16のタイプ（実際に、複数のタイプが入手可能な場合）。
ー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。

および／または以上に類するもの。

【0094】

もちろん、本発明の趣旨および範囲を逸脱することなく、より多量の、またはより少量のライセンス16要求情報36が、DRMシステム32によってライセンスサーバ24に伝送されることが可能である。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必要でない可能性がある一方で、ユーザおよび／またはユーザの計算デバイス14に関する追加の情報が必要である可能性がある。

10

【0095】

ライセンスサーバ24は、DRMシステム32からライセンス16要求情報36を受け取ると、信頼／認証に関して、またその他の目的でいくつかの検査を行うことができる。本発明の一実施形態では、ライセンスサーバ24は、認定機関のデジタル署名に関して証明書を検査して、署名が改ざんされているかどうか、または別の仕方に変更されているかどうかを判定する（ステップ705、707）。改ざん、または変更されている場合、ライセンスサーバ24は、要求情報36に基づいてライセンス16を交付するのを拒否する。また、ライセンスサーバ24は、既知の「不良な」ユーザおよび／またはユーザの計算デバイス14のリストも保持することができ、リスト上のいずれかの不良なユーザおよび／または不良なユーザの計算デバイス14からの要求に基づいてライセンス16を交付するのを拒否することができる。本発明の趣旨および範囲を逸脱することなく、そのような「不良」リストを任意の適切な仕方編成することが可能である。

20

【0096】

受け取られた要求、およびその要求に関連する情報に基づき、また詳細には、ライセンス要求情報の中のコンテンツID（またはパッケージID）に基づき、ライセンスサーバ24は、コンテンツー鍵データベース20（図1）に問い合わせ、要求の根拠であるデジタルコンテンツ12（またはパッケージ12p）に対応するレコードを探し出すことができる。前述したとおり、このレコードは、そのデジタルコンテンツ12に関する暗号化解除鍵（KD）、鍵ID、およびコンテンツIDを含む。さらに、このレコードは、デジタルコンテンツ12に関して発行されるべきライセンス16のタイプに関するライセンスデータ、および各タイプのライセンス16に関する条項および条件を含むことが可能である。あるいは、このレコードは、そのような追加の情報を有する場所に対するポインタ、リンク、またはリファレンスを含むことが可能である。

30

【0097】

前述したとおり、複数のタイプのライセンス16が入手可能であることが可能である。例えば、比較的小額のライセンス料で、限られた回数のレンダリングを許すライセンス16が入手可能であることが可能である。より高額のライセンス料で、失効日まで無制限のレンダリングを許すライセンス16が、入手可能であることが可能である。さらに高額のライセンス料で、失効日なしの無制限のレンダリングを許すライセンス16が入手可能であることが可能である。本発明の趣旨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項を有する実質的にあらゆるタイプのライセンス16を考案することが可能であり、またライセンスサーバ24によって発行することが可能である。

40

【0098】

本発明の一実施形態では、ライセンス16の要求は、ライセンスサーバ24からユーザの計算デバイス14に伝送されるWebページ等の助けを借りて達せられる。好ましくは、このWebページは、ライセンス16要求の根拠であるデジタルコンテンツ12に関してライセンスサーバ24から入手可能なすべてのタイプのライセンス16に関する情報を含む。

【0099】

50

本発明の一実施形態では、ライセンス16を発行することに先立ち、ライセンスサーバ24は、ブラックボックス30のバージョン番号を検査して、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）。理解すべきこととして、ブラックボックス30は、不正な（すなわち、ライセンス16なしにデジタルコンテンツ12を不適切にレンダリングする、または対応するライセンス16の条項を外れてレンダリングする）目的を有するユーザからの攻撃に対してセキュアであり、保護されているものとする。ただし、そのような攻撃に対して完全にセキュアな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認識されたい。

【0100】

また、理解されるべきこととして、ブラックボックス30が比較的新しい場合、すなわち、比較的最近に獲得されるか、または更新されている場合、ブラックボックス30が、不正なユーザによって成功裏に攻撃されている可能性がより低い。好ましくは、信頼に関わることとして、ライセンスサーバ24は、比較的新しくはないブラックボックス30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った場合、以下に説明するとおり、対応するブラックボックス30が現行のバージョンに更新されるまで、要求されたライセンス16を発行するのを拒否する。簡単に言えば、ライセンスサーバ24は、ブラックボックス30が比較的新しくない限り、ブラックボックス30を信頼しない。

【0101】

本発明のブラックボックス30のコンテキストでは、「現行の」または「比較的新しい」という用語は、本発明の趣旨および範囲を逸脱することなく、ブラックボックス30の経時（age）、または使用法に基づいてブラックボックス30を信頼する機能と整合する任意の適切な意味を有することが可能である。例えば、「現行」は、経時に従って（すなわち、1カ月以内の経時）定義することができる。代替の例として、「現行」は、ブラックボックス30がデジタルコンテンツ12を暗号化解除した回数（すなわち、200回以内の暗号化解除）に基づいて定義することができる。さらに、「現行」は、ライセンスサーバ24ごとに「現行」に違った定義が行われ、ライセンスサーバ24が、さらに、とりわけ、ライセンス16が要求されたデジタルコンテンツ12に依存して、または要求されたライセンス16のタイプに依存して「現行」に違った定義を行う、各ライセンスサーバ24によって設定されたポリシーに基づくことが可能である。

【0102】

ブラックボックス30のバージョン番号、またはブラックボックス30の他の指示から、ブラックボックス30が現行のものであるとライセンスサーバ24が確信させられたと想定して、ライセンスサーバ24が、ライセンス16に関する条項および条件をユーザと交渉することに取りかかる（ステップ713）。あるいは、ライセンスサーバ24は、ユーザとライセンス16を交渉し、次に、ブラックボックス30のバージョン番号から、ブラックボックス30が現行のものであるという確信を得る（すなわち、ステップ713を行い、次にステップ711を行う）。もちろん、交渉の量は、発行されるべきライセンス16のタイプ、およびその他のファクタに応じて様々である。例えば、ライセンスサーバ24が、単に支払済みの無制限の使用ライセンス16を発行する場合、ほとんど交渉を行う必要がない。他方、ライセンス16が、変化する値、スライディングスケール（sliding scale）、ブレイクポイント（break point）、およびその他の詳細などの項目に基づく場合、そのような項目および詳細をライセンスサーバ24とユーザの間で調整してからでないと、ライセンス16を発行することができない可能性がある。

【0103】

理解されるべきこととして、状況に応じて、ライセンス交渉は、ユーザが、ライセンスサーバ24にさらなる情報（例えば、ユーザ、ユーザの計算デバイス14等に関する情報）を提供することを必要とする可能性がある。重要なことには、ライセンス交渉は、ユーザおよびライセンスサーバ24が、とりわけ、互いに受入れ可能な支払い手段（クレジット口座、デビット（debit）口座、郵送される小切手等）、および／または支払い方法

10

20

30

40

50

(即時の支払い、ある期間にわたる支払い等)を決めることも要求することが可能である。

【0104】

ライセンス16のすべての条項が交渉され、ライセンスサーバ24とユーザの両方によって合意されると(ステップ715)、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(ステップ719)、この生成されたライセンス16は、少なくともある程度、ライセンス要求、ブラックボックス30公開鍵(PUBB)、およびコンテンツ鍵データベース20から獲得される要求の根拠であるデジタルコンテンツ12に関する暗号化解除鍵(KD)に基づいている。

【0105】

本発明の一実施形態では、図8で見られるとおり、生成されたライセンス16は、以下のものを含む。すなわち、

ーライセンス16が適用されるデジタルコンテンツ12のコンテンツID。

ー暗号化解除鍵(KD)で、場合により、暗号化されたデジタル権利ライセンス(DRL)48(すなわち、ライセンスイバリュエータ36が問い合わせることができる所定の形式で書かれたライセンス16の権利記述、または実際の条項および条件)(すなわち、KD(DRL))。

ーライセンス要求の中で受け取られたブラックボックス30公開鍵(PUBB)で暗号化されたデジタルコンテンツに関する暗号化解除鍵(すなわち、(PUBB(KD)))

。

ー(KD(DRL))および(PUBB(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(付加された証明書なしの)(すなわち、(S(PR-LS)))。

ーライセンスサーバ24が、コンテンツサーバ22から以前に獲得した、ライセンスサーバ24が、ライセンス16を発行するコンテンツサーバ22からの許可を有することを示す証明書(すなわち、(CERT(PU-LS)S(PR-CS)))である。

【0106】

理解されるべきこととして、前述した要素、および、場合により、その他の要素は、デジタルファイル、または何らかの他の適切な形態にパッケージ化される。やはり、理解されるべきこととして、ライセンス16の中のDRL48、または(PUBB(KD))が改ざんされた、または別の仕方に変更された場合、ライセンス16の中のデジタル署名(S(PR-LS))は、ライセンス16にマッチせず、したがって、ライセンス16を有効にしない。この理由で、DRL48は、必ずしも暗号化された形態(すなわち、前述した(KD(DRL)))でなくてもよい。ただし、暗号化された形態は、一部の場合、望ましく、したがって、本発明の趣旨および範囲を逸脱することなく使用することができる。

【0107】

デジタルライセンス16が準備されると、このライセンス16は、要求側(すなわち、ユーザの計算デバイス14上のDRMシステム32)に対して発行される(図7のステップ719)。好ましくは、ライセンス16は、ライセンス16の要求が行われたのと同じパス(すなわち、インターネット、または別のネットワーク)を介して伝送される。ただし、本発明の趣旨および範囲を逸脱することなく、別のパスを使用することもできる。受領時に、要求側のDRMシステム32は、好ましくは、受領したデジタルライセンス16をライセンスストア38の中に配置する(ステップ721)。

【0108】

ユーザの計算デバイス14には、ときとして動作不良が生じる可能性があり、そのユーザの計算デバイス14上のDRMシステム32のライセンスストア38の中に記憶されたライセンス16が、回復不能な仕方であられる可能性があることを理解されたい。したがって、ライセンスサーバ24が、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)、またライセンスサーバ24が、発行済みライセンス16のコピーまたは再発行(

10

20

30

40

50

以降、「再発行」)をユーザに提供することを、そのユーザが、実際に、再発行を受ける資格がある場合、行うことが好ましい。ライセンス16が回復不能な仕方です失われる前述したケースでは、状態ストア40の中に記憶され、ライセンス16に対応する状態情報も失われていることになっている可能性が高い。この失われた状態情報が、ライセンス16を再発行する際、考慮に入れられなければならない。例えば、固定回数のレンダリングライセンス16は、比較的短い期間の後、応分に割振り計算した形で正当に再発行することが可能であるが、比較的長い期間の後、再発行することは可能でない。

【0109】

＜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＞

前述したとおり、ライセンス16を獲得する機能の一環として、ライセンスサーバ24は、ユーザの計算デバイス14が、比較的新しくはない、すなわち、比較的古いバージョン番号を有するブラックボックス30を備えたDRMシステム32を有する場合、ユーザからのライセンス16の要求を拒否する可能性がある。その場合、その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て、その後にライセンス獲得機能を開始できるようにすることが好ましい。もちろん、ブラックボックス30は、本発明の趣旨および範囲を逸脱することなく、任意の時点でアップグレードすることができる。

【0110】

好ましくは、ユーザの計算デバイス14上のDRMシステム32をインストールするプロセスの一環として、ブラックボックス30の固有でない「ライト(light)」バージョンが提供される。次に、この「ライト」ブラックボックス30を、デジタルコンテンツ12をレンダリングするのに先立って固有の通常のバージョンにアップグレードする。理解されるべきこととして、各DRMシステム32の中のブラックボックス30は固有であり、1つのブラックボックス30のセキュリティを破って侵入することにより、何らかの他のブラックボックス30で容易に侵入を繰り返すことはできない。

【0111】

次に、図9を参照すると、DRMシステム32が、ブラックボックスサーバ26等(前述し、図1に示した)から固有のブラックボックス30を要求することにより、ブラックボックス30を獲得する(ステップ901)。通常、この要求は、インターネットを使用して行われるが、本発明の趣旨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に対する接続は、ローカル式または遠隔式の直接接続であることが可能である。ある固有のライトでないブラックボックス30から別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も、例えば、前述したとおり、ライセンスサーバ24が、ブラックボックス30が現行のものでないと見なした時点などの任意の時点で、DRMシステム32によって要求されることが可能である。

【0112】

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に見られるとおり、それぞれの新しいブラックボックス30は、バージョン番号、および認定機関からのデジタル署名を有する証明書を備えている。ライセンス獲得機能に関連して前述したとおり、ブラックボックス30のバージョン番号は、ブラックボックス30の相対的な経時および／または使用法を示す。やはりライセンス獲得機能に関連して前述した、認定機関からのデジタル署名を備えた証明書は、ライセンスサーバ24がブラックボックス30を信頼すべきことの認定機関からの進言(proffer)機構、または保証機構である。もちろん、ライセンスサーバ24は、認定機関が、実際に信頼に値するブラックボックス30に関して証明書を発行するものと信頼しなければならない。実際には、ライセンスサーバ24が、特定の認定機関を信用せず、その認定機関によって発行されたあらゆる証明書を尊重することを拒否する可能性がある。例えば、特定の認定機関が、証明書を不適切に発行することを繰り返し行っていることが分かった場合、信頼がなされない可能性がある。

【0113】

好ましくは、前述したとおり、ブラックボックスサーバ26は、新しい固有の公開鍵／秘密鍵ペア（PU－BB、PR－BB）を新たに生成された固有のブラックボックス30に含める（図9のステップ903）。好ましくは、そのブラックボックス30に関する秘密鍵（PR－BB）には、そのブラックボックス30だけがアクセス可能であり、そのブラックボックス30を有するDRMシステム32を有する計算デバイス14、および計算デバイス14のユーザを含め、それ以外の世界には隠されており、アクセス不可能である。

【0114】

世界から秘密鍵（PR－BB）を隠す機能を実際に行う限り、本発明の趣旨および範囲を逸脱することなく、ほとんどの任意の隠蔽スキームを使用することができる。単に一例として、秘密鍵（PR－BB）は、いくつかの下位構成要素に分割することができ、各下位構成要素を固有に暗号化して、異なる場所に記憶することができる。そのような状況では、下位構成要素が決して完全に組み立てられて秘密鍵全体（PR－BB）をもたらすことができないことが好ましい。

【0115】

本発明の一実施形態では、秘密鍵（PR－BB）は、コードベースの暗号技術に従って暗号化される。詳細には、この実施形態では、ブラックボックス30の実際のソフトウェアコード（または他のソフトウェアコード）が、暗号化鍵として使用される。したがって、ブラックボックス30のコード（または他のソフトウェアコード）が、例えば、不正な目的を有するユーザによって改ざんされた、または別の仕方に変更された場合、その秘密鍵（PR－BB）を暗号化解除することができない。

【0116】

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）と共に配信されるが、新しいブラックボックス30には、好ましくは、ユーザの計算デバイス14上のDRMシステム32に以前に配信された古いブラックボックス30からの古い公開鍵／秘密鍵ペアに対するアクセスも与えられる（ステップ905）。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、それでも、以下により詳細に述べるとおり、古い鍵ペアを使用して、その古い鍵ペアに従って生成されたより古いデジタルコンテンツ12、およびより古い対応するライセンス16にアクセスすることができる。

【0117】

好ましくは、ブラックボックスサーバ26によって配信されたアップグレードされたブラックボックス30は、ユーザの計算デバイス14に緊密に結び付く、または緊密に関連する。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、またはその他の目的で、複数の計算デバイス14間で動作上、転送することができない。本発明の一実施形態では、ブラックボックス30の要求（901）の一環として、DRMシステム32が、そのDRMシステム32に固有であり、かつ／またはユーザの計算デバイス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、その提供されたハードウェア情報にある程度、基づき、そのDRMシステム32用のブラックボックス30を生成する。次に、この生成されたアップグレード済みのブラックボックス30が、ユーザの計算デバイス14上のDRMシステム32に配信されて、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、何らかの仕方別の計算デバイス14に転送された場合、転送されたブラックボックス30は、その別の計算デバイス14を宛先としていないことを認識し、要求されたレンダリングが、その別の計算デバイス14上で進められることを全く許さない。

【0118】

新しいブラックボックス30がDRMシステム32にインストールされると、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開始することができる。

【0119】

<DRMシステム32－コンテンツレンダリング、第3部>

次に、図5Bを参照すると、ライセンスイバリュエータ36が、少なくとも1つの有効なライセンス16を見出し、また有効なライセンス16の少なくとも1つが、求める仕方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、使用を可能にするものである）ものと想定すると、ライセンスイバリュエータ36が、そのライセンス16の1つをさらなる使用のために選択する（ステップ519）。詳細には、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、ライセンスイバリュエータ36とブラックボックス30が一緒に、ライセンス16から暗号化解除鍵（KD）を獲得し、ブラックボックス30が、その暗号化解除鍵（KD）を使用してデジタルコンテンツ12を暗号化解除する。本発明の一実施形態では、前述したとおり、ライセンス16から獲得された暗号化解除鍵（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、その暗号化された暗号化解除鍵を自らの秘密鍵（PR-BB）を使用して暗号化解除して、暗号化解除鍵（KD）をもたらす（ステップ521、523）。ただし、本発明の趣旨および範囲を逸脱することなく、デジタルコンテンツ12に関する暗号化解除鍵（KD）を獲得する他の方法も使用することができる。

10

【0120】

ブラックボックス30は、デジタルコンテンツ12に関する暗号化解除鍵（KD）、およびそのデジタルコンテンツ12をレンダリングするライセンスイバリュエータ36からの許可を入手すると、制御が、レンダリングアプリケーション34に戻ることが可能である（ステップ525、527）。本発明の一実施形態では、次に、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の少なくとも一部分を暗号化解除鍵（KD）に従って暗号化解除のためにブラックボックス30に向かわせる（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に関する暗号化解除鍵（KD）に基づいてデジタルコンテンツ12を暗号化解除し、次に、暗号化解除したデジタルコンテンツ12を実際のレンダリングのためにレンダリングアプリケーション34に戻す（ステップ533、535）。レンダリングアプリケーション34は、本発明の趣旨および範囲を逸脱することなく、デジタルコンテンツ12に関する暗号化解除鍵（KD）に基づき、暗号化解除のために暗号化されたデジタルコンテンツ12の一部分、またはデジタルコンテンツ12全体をブラックボックス30に送ることができる。

20

30

【0121】

好ましくは、レンダリングアプリケーション34が、暗号化解除のためにデジタルコンテンツ12をブラックボックス30に送ったとき、ブラックボックス30および／またはDRMシステム32が、そのレンダリングアプリケーション34を認証して、そのレンダリングアプリケーション34が、DRMシステム32に動作するように最初に要求を行ったのと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（ステップ531）。そうでなければ、あるタイプのレンダリングアプリケーション34上のレンダリング要求に基づくことにより、レンダリング許可が不適切に獲得され、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を使用してレンダリングが行われる可能性が存在する。認証が成功し、デジタルコンテンツ12が、ブラックボックス30によって暗号化解除されたものと想定すると、次に、レンダリングアプリケーション34が、暗号化解除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）。

40

【0122】

<鍵トランザクションのシーケンス>

次に、図10を参照すると、本発明の一実施形態では、鍵トランザクションのシーケンスが、暗号化解除鍵（KD）を獲得し、要求されたデジタルコンテンツ12に関するライセンス16を評価するように（すなわち、図5Aおよび5Bのステップ515～523を行うように）行われる。主に、このシーケンスでは、DRMシステム32が、ライセンス16から暗号化解除鍵（KD）を獲得し、ライセンス16およびデジタルコンテンツ12か

50

ら獲得された情報を使用して、ライセンス16とデジタルコンテンツ12の両方の有効性を認証し、または確実にし、次に、ライセンス16が、求められる仕方でデジタルコンテンツ12をレンダリングする権利を実際に提供するかどうかを判定する。提供する場合、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。

【0123】

図8に見られるとおり、デジタルコンテンツ12に関する各ライセンス16が、
ーライセンス16が適用されるデジタルコンテンツ12のコンテンツID。
ー暗号化解除鍵(KD)で、場合により、暗号化されたデジタル権利ライセンス(DRL)48(すなわち、KD(DRL))。
ーブラックボックス30公開鍵(PU-BB)で暗号化されたデジタルコンテンツ12に関する暗号化解除鍵(KD)(すなわち、(PU-BB(KD)))。
ー(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)))。 10

【0124】

ライセンスサーバ24が、コンテンツサーバ22から以前に獲得した証明書(すなわち、(CERT(PU-LS)S(PR-CS)))を含むことを念頭に置き、また、図3に見られるとおり、デジタルコンテンツ12を有するパッケージ12pが、
ーデジタルコンテンツ12のコンテンツID。
ーKDで暗号化されたデジタルコンテンツ12(すなわち、(KD(CONTENT))) 20

ー暗号化されていないライセンス獲得スクリプト。
ーコンテンツサーバ22秘密鍵(PR-CS)で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)))を含むことも念頭に置いて、本発明の一実施形態では、デジタルコンテンツ12に関するライセンス16の特定の1つに関する鍵トランザクションの特定のシーケンスが、以下のとおりである。

【0125】

1. ライセンス16からの(PU-BB(KD))に基づき、ユーザの計算デバイス14上のDRMシステム32のブラックボックス30が、自らの秘密鍵(PR-BB)を適用して(KD)を獲得する(ステップ1001)。(PR-BB(PU-BB(KD)))=(KD))。重要なこととして、次に、ブラックボックス30は、KDを使用して無造作にデジタルコンテンツ12を暗号化解除することを開始できることに留意されたい。ただし、やはり重要なこととして、ライセンスサーバ24は、ブラックボックス30がそうしないものと信頼する。この信頼は、ライセンスサーバ24が、ブラックボックス30が信頼に値することを保証する認定機関からの証明書に基づいてライセンス16を発行した時点で確立されている。したがって、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暗号化解除鍵(KD)を獲得するにも関わらず、DRMシステム32は、以下に説明するとおり、すべてのライセンス16検証機能および評価機能を行いつづける。 30 40

【0126】

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、新たに獲得された暗号化解除鍵(KD)を適用して(PU-CS)を獲得する(ステップ1003)。(KD(KD(PU-CS)))=(PU-CS))。さらに、ブラックボックス30は、(PU-CS)を署名(S(PR-CS))に照らして適用して、署名およびデジタルコンテンツ12/パッケージ12pが有効であることの確信を得ることができる(ステップ1005)。有効でない場合、プロセスは停止され、デジタルコンテンツ12へのアクセスが拒否される。

【0127】

3. ライセンス16からの(CERT(PU-LS)S(PR-CS))に基づき、ブラ 50

ックボックス 30 は、新たに獲得されたコンテンツサーバ 22 公開鍵 (P U - C S) を適用して、証明書が有効であることの確信を得る (ステップ 1007)。有効であることは、ライセンス 16 を発行したライセンスサーバ 24 が、そうすることの許可をコンテンツサーバ 22 から得ていることを意味する。次に、ブラックボックス 30 は、証明書コンテンツを検査して (P U - L S) を獲得する (ステップ 1009)。有効でなかった場合、プロセスは停止され、ライセンス 16 に基づくデジタルコンテンツ 12 へのアクセスは拒否される。

【0128】

4. ライセンス 16 からの (S (P R - L S)) に基づき、ブラックボックス 30 は、新たに獲得されたライセンスサーバ 24 公開鍵 (P U - L S) を適用して、ライセンス 16 が有効であることの確信を得る (ステップ 1011)。有効でなかった場合、プロセスは停止され、ライセンス 16 に基づくデジタルコンテンツ 12 へのアクセスは拒否される。

【0129】

5. すべての検証ステップが成功し、ライセンス 16 の中の D R L 48 が、暗号化解除鍵 (K D) で実際に暗号化されたものと想定すると、次に、ライセンスイバリュエータ 36 が、既に獲得済みの暗号化解除鍵 (K D) をライセンス 16 から獲得された (K D (D R L)) に適用して、ライセンス 16 からライセンス条項 (すなわち、D R L 48) を獲得する (ステップ 1013)。もちろん、ライセンス 16 の中の D R L 48 が、実際に暗号化解除鍵 (K D) で暗号化されていない場合、ステップ 1013 は、省略することができる。次に、ライセンスイバリュエータ 36 が、D R L 48 の評価/問合せを行い、ライセンス 16 の中の D R L 48 に基づき、ユーザの計算デバイス 14 が、求める仕方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有するかどうか (すなわち、D R L 48 が使用を可能にするものであるかどうか) を判定する (ステップ 1015)。ライセンスイバリュエータ 36 が、その権利が存在しないと判定した場合、プロセスは停止され、ライセンス 16 に基づくデジタルコンテンツ 12 へのアクセスは拒否される。

【0130】

6. 最後に、ライセンス 16 の評価により、D R L 48 条項に基づいてユーザの計算デバイス 14 が、求める仕方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有するという肯定的な判定がもたらされたものと想定すると、ライセンスイバリュエータ 36 は、ブラックボックス 30 が、暗号化解除鍵 (K D) に従って対応するデジタルコンテンツ 12 をレンダリングすることができることをブラックボックス 30 に知らせる。その後、ブラックボックス 30 は、暗号化解除鍵 (K D) を適用して、パッケージ 12 p からデジタルコンテンツ 12 を暗号化解除する (すなわち、(K D (K D (C O N T E N T))) = (C O N T E N T)) (ステップ 1017)。

【0131】

以上に指定した一連のステップは、ライセンス 16 とデジタルコンテンツ 12 の間の交替、または「ピンポン (p i n g - p o n g i n g)」を表すことに留意することが重要である。このピンポンにより、検証プロセスおよび評価プロセスが、デジタルコンテンツ 12 とライセンス 16 がともに適切に発行された有効な形態で存在する場合にだけ行われることが可能であるということで、デジタルコンテンツ 12 が、ライセンス 16 に緊密に結合されることが確実になる。さらに、ライセンス 16 からコンテンツサーバ 22 公開鍵 (P U - C S) を獲得するのと、パッケージ 12 p からデジタルコンテンツ 12 を暗号化解除された形態で (また、場合により、ライセンス 16 からライセンス条項 (D R L 48) を暗号化解除された形態で) 獲得するのと同じ暗号化解除鍵 (K D) が必要とされるため、以上のアイテムも緊密に結合される。また、署名検証により、デジタルコンテンツ 12 およびライセンス 16 が、コンテンツサーバ 22 およびライセンスサーバ 24 からそれぞれ発行されたのと同じ形態であることが確実になる。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 を暗号化解除することは、不可能でないにしても困難であり、また、デジタルコンテンツ 12 またはライセンス 16 を改変した後、暗号化解除することも、不可能でないにしても困難である。

【0132】

本発明の一実施形態では、署名確認、特にライセンス16の署名確認が、以下のとおり交替で行われる。図8に見られるように、ライセンスサーバ24の秘密鍵（PR-L S）で署名が暗号化されるのではなく、各ライセンス16の署名が、秘密根底鍵（private root key）（PR-R）（図示せず）で暗号化され、各DRMシステム32のブラックボックス30が、その秘密根底鍵（PR-R）に対応する公開根底鍵（public root key）（PU-R）（やはり図示せず）を含んでいる。秘密根底鍵（PR-R）は、根底エンティティにだけ知られ、ライセンスサーバ24は、ライセンス16を発行することを根底エンティティと取り決めた場合にだけ、ライセンス16を発行することができる。

10

【0133】

詳細には、この実施形態では、

1. ライセンスサーバ24が、自らの公開鍵（PU-L S）を根底エンティティに提供し、
2. 根底エンティティが、秘密根底鍵（PR-R）で暗号化されたライセンスサーバ公開鍵（PU-L S）（すなわち、（CERT（PU-L S）S（PR-R）））をライセンスサーバ24に戻し、また
3. 次に、ライセンスサーバ24が、ライセンスサーバ秘密鍵（S（PR-L S））で暗号化された署名を有するライセンス16を発行し、また根底エンティティからの証明書（CERT（PU-L S）S（PR-R））をライセンスに付加する。

20

【0134】

DRMシステム18が発行されたライセンス16を検証するには、DRMシステム18は、

1. 公開根底鍵（PU-R）を付加された証明書（CERT（PU-L S）S（PR-R））に適用してライセンスサーバ公開鍵（PU-L S）を獲得し、また
2. 獲得されたライセンスサーバ公開鍵（PU-L S）をライセンス16の署名（S（PR-L S））に適用する。

【0135】

重要なことには、根底エンティティが、ライセンスサーバ24に対して証明書（CERT（PU-L S）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ると、ライセンスサーバ24は、同様の証明書を第2のライセンスサーバ24に提供することができ（すなわち、（CERT（PU-L S2）S（PR-L S1）））、これにより、第2のライセンスサーバもライセンス16を発行することができるようになることを認識されたい。既に明白であるとおり、第2のライセンスサーバによって発行されるライセンス16は、第1の証明書（CERT（PU-L S1）S（PR-R））、および第2の証明書（CERT（PU-L S2）S（PR-L S1））を含む。同様に、このライセンス16は、第1の証明書から第2の証明書までの連鎖を辿ることによって検証される。もちろん、その連鎖にさらなるリンクを追加してトラバース（traverse）することも可能である。

30

【0136】

前述した署名確認プロセスの1つの利点は、根底エンティティが、定期的に秘密根底鍵（PR-R）を変更し、これにより、各ライセンスサーバ24が新しい証明書（CERT（PU-L S）S（PR-R））を獲得することを同様に要求することが可能なことである。重要なことには、その新しい証明書を獲得する要件として、各ライセンスサーバが、自らをアップグレードすることが必要とされる可能性がある。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、比較的新しい場合、すなわち、比較的最近、アップグレードされている場合、ライセンスサーバ24が、成功裏に攻撃を受けている可能性がより低い。したがって、信頼に関わることとして、各ライセンスサーバ24は、好ましくは、署名確認プロセスなどの適切なアップグレードトリガ機構を介して、定期的にアップグレードされることが必要とされる。もちろん、本発明の趣旨および範囲を逸脱すること

40

50

なく、他のアップグレード機構も使用することができる。

【0137】

もちろん、秘密根底鍵（P R - R）が変更された場合、各 D R M システム 1 8 における公開根底鍵（P U - R）も変更されなければならない。この変更は、例えば、通常のブラックボックス 3 0 アップグレード中に行われることが可能であり、あるいは、実際に、ブラックボックス 3 0 アップグレードが行われることを要する可能性がある。変更された公開根底鍵（P U - R）は、より古い秘密根底鍵（P R - R）に基づいて発行されたより古いライセンス 1 6 に関する署名検証の障害になる可能性があるが、この障害は、アップグレードされたブラックボックス 3 0 が、すべての古い公開根底鍵（P U - R）を憶えておくことを要求することによって最小限に抑えることができる。あるいは、ライセンス 1 6 に関する証明書確認を 1 回だけ、例えば、ライセンス 1 6 が、D R M システム 1 8 のライセンスイバリュエータ 3 6 によって最初に評価されるときにだけ要求することにより、その障害を最小限に抑えることができる。その場合、署名確認が行われたかどうかに関する状態情報がまとめられなければならない、またその状態情報は、D R M システム 1 8 の状態ストア 4 0 の中に記憶されなければならない。

10

【0138】

＜デジタル権利ライセンス 4 8＞

本発明の一実施形態では、ライセンスイバリュエータ 3 6 が、ライセンス 1 6 の権利記述または権利条項としてデジタル権利ライセンス（D R L）4 8 を評価して、D R L 4 8 により、求める仕方で対応するデジタルコンテンツ 1 2 をレンダリングすることが許されるかどうか判定される。本発明の一実施形態では、D R L 4 8 は、任意の D R L 言語でライセンサ（l i c e n s o r）（すなわち、コンテンツ所有者）が書くことが可能である。

20

【0139】

理解されるべきこととして、D R L 4 8 を指定する多数のやり方が存在する。したがって、あらゆる D R L 言語において高い度合いの柔軟性が見込まなければならない。ただし、特定のライセンス言語における D R L 4 8 のすべての態様を指定することは実際的ではなく、その言語の作成者が、特定のデジタルライセンサが所望する可能性があるすべての可能なライセンシングの態様を理解できる可能性は、極めて低い。さらに、極めて高度なライセンス言語は、不必要であり、比較的簡単な D R L 4 8 を提供するライセンサには障害とさえなる可能性がある。それでも、ライセンサは、どのように D R L 4 8 を指定すべきかを不必要に制限してはならない。同時に、ライセンスイバリュエータ 3 6 は、いくつかの特定のライセンス問題に関して常に D R L 4 8 から回答を得ることができなければならない。

30

【0140】

本発明では、図 1 1 を参照すると、D R L 4 8 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、または言語タグ 5 4 を含む。ライセンス 1 6 を評価するライセンスイバリュエータ 3 6 が、言語タグ 5 4 を検討して言語を識別する予備ステップを行い、次に、その識別された言語でライセンス 1 6 にアクセスするのに適切なライセンス言語エンジン 5 2 を選択する。理解されるべきこととして、ライセンス言語エンジン 5 2 は、存在し、ライセンスイバリュエータ 3 6 がアクセスできなければならない。存在しない場合、言語タグ 5 4 および／または D R L 4 8 は、好ましくは、言語エンジン 5 2 を獲得するための場所 5 6（通常、W e b サイト）を含む。

40

【0141】

通常、言語エンジン 5 2 は、ハードドライブなどのユーザの計算デバイス 1 4 のメモリの中に常駐する実行可能ファイル、または 1 組のファイルの形態をしている。言語エンジン 5 2 は、ライセンスイバリュエータ 3 6 を助けて、D R L 4 8 に直接に問合せを行い、ライセンスイバリュエータ 3 6 は、仲介役をする言語エンジン 5 2 等を介して D R L 4 8 に間接的に問合せを行う。実行されたとき、言語エンジン 5 2 は、R A M などの、ユーザの計算デバイス 1 4 のメモリ内部の作業空間において実行される。ただし、本発明の趣旨お

50

よび範囲を逸脱することなく、任意の他の形態の言語エンジン 5 2 も使用することができる。

【0142】

好ましくは、任意の言語エンジン 5 2、および任意の D R L 言語が、以下に述べるとおり、あらゆる D R L 4 8 によって応えられることをライセンスイバリュエータ 3 6 が予想する少なくともいくつかの特定のライセンス問題をサポートする。したがって、ライセンスイバリュエータ 3 6 は、何らかの特定の D R L 言語には結び付いておらず、D R L 4 8 は、任意の適切な D R L 言語で書くことができ、また、新しいライセンス言語で指定された D R L 4 8 が既存のライセンスイバリュエータ 3 6 によって使用されることが、対応する新しい言語エンジン 5 2 をライセンスイバリュエータ 3 6 に獲得させることによって可能になる。

10

【0143】

< D R L 言語 >

それぞれ D R L 4 8 で実現された D R L 言語の 2 つの例を以下に提示する。第 1 の「簡単な」D R L 4 8 は、ライセンス属性を指定する D R L 言語で書かれ、一方、第 2 の「スクリプト」D R L 4 8 は、D R L 4 8 の中で指定されたスクリプトに従って機能を行うことができる D R L 言語で書かれる。D R L 言語で書かれているが、コードの各行の意味は、各行の言語 (l i n g u i s t i c s)、および／または以下の属性記述チャートに基づいて明白なはずである。

Simple DRL 48:

<LICENSE>

<DATA>

<NAME>Beastie Boy's Play</NAME>

<ID>39384</ID>

<DESCRIPTION>Play the song 3 times</DESCRIPTION> <TERMS></TERMS>

<VALIDITY>

10

<NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>

<NOTAFTER>19980102 23:20:14Z</NOTAFTER>

</VALIDITY>

<ISSUEDDATE>19980102 23:20:14Z</ISSUEDDATE> <LICENSORSITE>http://www.f
oo.com</LICENSORSITE>

<CONTENT>

<NAME>Beastie Boy's</NAME>

20

<ID>392</ID>

<KEYID>39292</KEYID>

<TYPE>MS Encrypted ASF 2.0</TTYPE>

</CONTENT>

<OWNER>

<ID>939KDKD393KD</ID>

<NAME>Universal</NAME>

30

<PUBLICKEY></PUBLICKEY>

</OWNER>

<LICENSEE>

<NAME>Arnold</NAME>

<ID>939KDKD393KD</ID>

<PUBLICKEY></PUBLICKEY>

40

</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> 10
</PRINCIPAL>
<PRINCIPAL>
<TYPE>Application</TYPE>
<ID>2939495939292</ID>
<NAME>Window=s Media Player</NAME>
<AUTHTYPE>Authenticode SHA-1</AUTHTYPE>
<AUTHDATA>93939</AUTHDATA> 20
</PRINCIPAL>
</PRINCIPAL>
<PRINCIPAL>
<TYPE>Person</TYPE>
<ID>39299482010</ID>
<NAME>Arnold Blinn</NAME>
<AUTHTYPE>Authenticate user</AUTHTYPE> 30
<AUTHDATA>¥¥redmond¥arnolddb</AUTHDATA>
</PRINCIPAL>
</PRINCIPAL>
<DRLTYPE>Simple</DRLTYPE>[the language tag 54]
<DRLDATA>
<START>19980102 23:20:14Z</START>
<END>19980102 23:20:14Z</END> 40
<COUNT>3</COUNT>

```

<ACTION>PLAY</ACTION>
 </DRLDATA>
 <ENABLINGBITS>aaaabbbbccccdddd</ENABLINGBITS>
 </DATA>
 <SIGNATURE>
 <SIGNERNAME>Universal</SIGNERNAME>
 <SIGNERID>9382ABK3939DKD</SIGNERID> <HASHALGORITHMID>MD5</HASHALGORITHMID> 10
 <SIGNALGORITHMID>RSA 128</SIGNALGORITHMID> <SIGNATURE>xxxxxxxxxxxxxx
 xxyyy</SIGNATURE> <SIGNERPUBLICKKEY></SIGNERPUBLICKKEY> <CONTENTSSIGNEDSIGN
 ERPUBLICKKEY></CONTENTSSIGNEDSIGNERPUBLICKKEY>
 </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> 30
 <NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>
 <NOTAFTER>19980102 23:20:14Z</NOTAFTER>
 </VALIDITY>
 <ISSUEDDATE>19980102 23:20:14Z</ISSUEDDATE> <LICENSORSITE>http://www.f
 oo.com</LICENSORSITE>
 <CONTENT>
 <NAME>Beastie Boy's</NAME> 40
 <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> <SIGNERPU
BLICKEY></SIGNERPUBLICKEY> <HASHID>MD5</HASHID>
<SIGNID>RSA 128</SIGNID>

<SIGNATURE>xxxxxxxxxxxxxxxxxxxx</SIGNATURE>
<CONTENTSSIGNEDSIGNERPUBLICKEY></CONTENTSSIGNEDSIGNERPUBLICKEY>
</SIGNATURE>
</LICENSE>

```

以上に指定した2つのDRL 48では、リストされた属性が、以下の記述、および以下の

10

20

30

40

50

データタイプを有する。

【0144】

【表1】

属性	説明	データタイプ
Id	ライセンスのID	GUID
Name	ライセンスの名前	ストリング
Content Id	コンテンツのID	GUID
Content Key Id	コンテンツの暗号化鍵のID	GUID
Content Name	コンテンツの名前	ストリング
Content Type	コンテンツのタイプ	ストリング
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	ストリング
Owner Public Key	コンテンツの所有者に関する公開鍵。これは、コンテンツの所有者に関するbase64で符号化された公開鍵である。	ストリング
Licensee Id	ライセンスを獲得する個人のId。空である可能性がある。	GUID
Licensee Name	ライセンスを獲得する個人の名前。空である可能性がある。	ストリング
Licensee Public Key	ライセンシーの公開鍵。これは、ライセンシーのbase64で符号化された公開鍵である。空である可能性がある。	ストリング
Description	ライセンスの簡単な人間可読の記述	ストリング

10

20

30

【0145】

【表2】

Terms	ライセンスの法律条項。これは、法律文を含むWebページに対するポインタであることが可能である。	ストリング
Validity Not After	ライセンス失効の有効期間	日付
Validity Not Before	ライセンス開始の有効期間	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、「単純」または「スクリプト」が含まれる。	ストリング
DRL Data	DRLに特有のデータ	ストリング
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である。このビットの解釈は、アプリケーションに任されるが、通常、コンテンツの暗号化解除のための秘密鍵である。このデータは、base64で符号化される。このビットは、個別のマシンの公開鍵を使用して暗号化解除されることに留意されたい。	ストリング
Signer Id	ライセンスに署名する個人のID	GUID

10

20

【 0 1 4 6 】

【表 3】

30

Signer Name	ライセンスに署名する個人の名前	ストリング
Signer Public Key	ライセンスに署名する個人に関する公開鍵。これは、署名者に関するbase64符号化公開鍵である。	ストリング
Content Signed Signer Public Key	コンテンツサーバ秘密鍵で署名されたライセンスに署名する個人に関する公開鍵。この署名を確認する公開鍵が、コンテンツの中で暗号化される。これは、base64で符号化される。	ストリング
Hash Alg Id	ハッシュを生成するのに使用されるアルゴリズム。これは、「MD5」などのストリングである。	ストリング
Signature Alg Id	署名を生成するのに使用されるアルゴリズム。これは、「RSA128」などのストリングである。	ストリング
Signature	データの署名。これは、base64で符号化されたデータである。	ストリング

10

20

【0147】

<メソッド>

前述したとおり、任意の言語エンジン52および任意のDRL言語が、デジタルライセンスイバリュエータ36が、あらゆるDRL48によって応えられるものと予期する少なくともいくつかの特定のライセンス問題をサポートすることが好ましい。サポートされる問題を認識することには、本発明の趣旨および範囲を逸脱することなく、前述した2つのDRL48の例で使用した用語法と整合するあらゆる問題が含まれる可能性があり、本発明の一実施形態では、サポートされる問題、つまり「メソッド」には、以下のとおり、「アクセスメソッド」、「DRLメソッド」、および「イネーブル使用(enabling use)メソッド」が含まれる。

30

【0148】

<アクセスメソッド>

アクセスメソッドは、最上位レベルの属性に関してDRL48にクエリを行うのに使用される。

40

VARIANT QueryAttribute(BSTR key)

有効な鍵は、BSRT Variantをそれぞれが戻すLicense. Name、License. Id、Content. Name、Content. Id、Content. Type、Owner. Name、Owner. Id、Owner. PublicKey、Licensee. Name、Licensee. Id、Licensee. PublicKey、Description、およびTerms、ならびにDate Variantをそれぞれが戻すIssued、Validty. Start、およびValidty. Endを含む。

【0149】

<DRLメソッド>

50

以下のDRLメソッドの実装は、DRL48ごとに異なる。DRLメソッドの多くは、より高度な情報をDRL48に伝えることを目的とする「データ」というラベルが付けられた変種のパラメータを含む。これは、現在、主に将来の拡張性のためのものである。

Boolean IsActivated(Variant data)

このメソッドは、DRL48／ライセンス16が活動化されているかどうかを示すブーリアン（Boolean）を返す。活動化されたライセンス16の例は、初回の再生時に48時間だけアクティブである制限された動作のライセンス16である。

【0150】

Activate(Variant data)

このメソッドは、ライセンス16を活動化するのに使用される。ライセンス16は、活動化されると、非活動化することができない。

10

【0151】

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、主に、DRL48機能セットの将来の拡張性に関するものである。

【0152】

Variant GetExpires(BSTR action,Variant data)

このメソッドは、提出済みアクション（passed-in action）に関するライセンス16の失効日を返す。戻り値がNULLである場合、ライセンス16は、決して失効しないか、または活動化されていない等のために、まだ失効日を有さないものと考えられる。

20

【0153】

Variant GetCount(BSTR action,Variant data)

このメソッドは、残っている提出済みアクションの動作の回数を返す。NULLが戻された場合、その動作は、無制限の回数、行うことができる。

【0154】

Boolean IsEnabled(BSTR action,Variant data)

このメソッドは、ライセンス16が、現時点で要求されたアクションをサポートするかどうかを示す。

【0155】

30

Boolean IsSunk(BSTR action,Variant data)

このメソッドは、ライセンス16の代金が支払われているかどうかを示す。前払いで代金が支払われているライセンス16は、TRUEを返し、一方、使用されるにつれて代金を徴収するライセンス16などの、前払いで代金が支払われていないライセンス16は、FALSEを返す。

【0156】

<イネーブル使用メソッド>

このメソッドは、コンテンツを暗号化解除する際に使用するためにライセンス16をイネーブルにするのに使用される。

【0157】

40

Boolean Validate(BSTR key)

このメソッドは、ライセンス16を検証するのに使用される。提出済みの鍵は、ライセンス16の署名の検証で使用するための対応するデジタルコンテンツ12に関する暗号化解除鍵（KD）で暗号化されたブラックボックス30公開鍵（PU-BB）（すなわち、（KD（PU-BB）））である。TRUEの戻り値は、ライセンス16が有効であることを示す。FALSEの戻り値は、無効を示す。

【0158】

int OpenLicense 16(BSTR action,BSTR key,Variant data)

このメソッドは、暗号化解除されたイネーブルビット（enabling bit）にアクセスする準備をするのに使用される。提出済みの鍵は、前述したとおり、（KD（PU

50

ー B B)) である。0 の戻り値が、成功を示す。その他の戻り値は、定義することができる。

【0159】

BSTR GetDecryptedEnablingBits(BSTR action, Varinat data)

Variant GetDecryptedEnablingBitsAsBinary(BSTR action, Variant Data)

このメソッドは、暗号化解除された形態のイネーブルビットにアクセスするのに使用される。いくつかの理由のどれかのためにそれが成功しなかった場合、空のストリング、または空のバリエーションが戻される。

【0160】

void CloseLicense(BSTR action, Variant data)

10

このメソッドは、提出済みアクションを行うためにイネーブルビットへのアクセスをロック解除するのに使用される。いくつかの理由のどれかのためにこれが成功しなかった場合、空のストリングが戻される。

【0161】

<ヒューリスティック>

前述したとおり、同一のデジタルコンテンツ 12 に関して複数のライセンス 16 が存在する場合、ライセンス 16 の 1 つが、さらなる使用のために選択されなければならない。前述したメソッドを使用して、この選択を行うために以下のヒューリスティックを実施することが可能である。詳細には、デジタルコンテンツ 12 に対してアクション（例えば、「再生」）を行うため、以下のステップを行うことが可能である。

20

【0162】

1. 特定のデジタルコンテンツ 12 に適用されるすべてのライセンス 16 を獲得する。

【0163】

2. アクションを可能にしない各ライセンス 16 を、そのライセンス 16 に対して IsEnabled フังก์ションを呼び出すことによって除去する。

【0164】

3. アクティブでない各ライセンス 16 を、そのライセンス 16 に対して IsActive を呼び出すことによって除去する。

【0165】

4. 前払いで代金が支払われていない各ライセンス 16 を、そのライセンス 16 に対して IsSunk を呼び出すことによって除去する。

30

【0166】

5. 何らかのライセンス 16 が残っている場合、そのライセンス 16 を使用する。特に、無制限回数の再生のライセンス 16 が失効日を有する場合、無制限回数の再生のライセンス 16 を使用してから、制限された回数の再生のライセンス 16 を使用する。あらゆる時点で、ユーザは、既に獲得された特定のライセンス 16 を選択することが、その選択の費用対効果が大きくない場合でも、許されていなければならない。したがって、ユーザは、DRM システム 32 には、場合により、明白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。

【0167】

40

6. ライセンス 16 が全く残っていない場合、そのことを示すステータスを戻す。次に、ユーザに、以下のオプションが与えられる。すなわち、前払いで代金が支払われていないライセンス 16 が利用可能である場合、そのライセンス 16 を使用すること、あるライセンス 16 が利用可能である場合、そのライセンス 16 を活動化すること、かつ／またはライセンスサーバ 24 からのライセンス獲得を行うこと。

【0168】

<ソフトウェアアプリケーションの保護>

以上に開示したとおり、以上に提示した DRM アーキテクチャ 10 は、単一のコンピュー

50

タファイルの形態のデジタルコンテンツ12を保護する。ただし、当分野の技術者一般（*relevant public*）には理解されるべきこととして、このDRMアーキテクチャ10は、複数の構成コンピュータファイルの形態のデジタルコンテンツ12を保護するのにも使用することができる。例えば、各構成ファイルは、前述したとおり、DRMシステム32によって検査される対応するライセンス16を有することが可能である。同様に、その構成ファイルの一部だけが対応するライセンスを必要とすることが、特に、その他のファイルが、ライセンスファイルなしにはアクセス不可能であるか、使用不可能であるか、または別の形で利用不可能である場合に可能である。

【0169】

複数のファイルの形態をしているデジタルコンテンツ12の一例は、複数の構成ファイルを有するコンピュータソフトウェアアプリケーションである。詳細には、ソフトウェアアプリケーションは、通常、実行可能コードを少なくとも1つが含むファイルの集合の形態で、ソフトウェアプロバイダによって提供される。したがって、DRMアーキテクチャ10の文脈では、各ファイルが暗号化され、対応するライセンス16に伴われていることが可能である。そうではなく、1つのライセンス16が、アプリケーションのファイルのすべてのファイル、または複数のファイルに適用可能であることも可能である。

10

【0170】

あるいは、実行可能コードを有する各ファイルだけが暗号化され、対応するライセンス16に伴われていることが、特に、すべての他のファイルに、その「実行可能」ファイルを介してだけ到達可能である場合に可能である。別の代案として、実行可能ファイルの選択されたファイルだけが暗号化され、対応するライセンス16に伴われることが、特に、その選択された実行可能ファイルが決定的である、重要である、主要である等と考えられる場合に可能である。この場合も、1つのライセンス16が、アプリケーションの実行可能ファイルのなかのすべての実行可能ファイル、または複数の実行可能ファイルに適用可能であることが可能である。

20

【0171】

通常、計算デバイス14上のアプリケーションは、計算デバイス14上に常駐するオペレーティングシステムの一部であるローダ等を使用してロードされる。したがって、アプリケーションの少なくとも一部のファイルがDRM保護されている場合、ローダは、そのファイルが保護されていることを認識し、それぞれの保護されたファイルに関して、計算デバイス14上でDRMシステム32を使用して、その保護されたファイルに対してDRM認証および暗号化解除を行わなければならない。ただし、重要なことには、アプリケーションをロードすることは、特に時間を消費するタスクである可能性があり、1つまたは複数のアプリケーションファイルのDRM暗号化解除などの何らかの相当なDRM活動を追加することにより、過度であると考えられる量までロード時間が長引く可能性がある。重要なことには、複数のアプリケーションファイル、大きいアプリケーションファイル、またはこの組合せのDRM暗号化解除が必要とされる場合、過度なロード時間の可能性がより高くなる。

30

【0172】

本発明の一実施形態では、アプリケーションを保護するのにDRM暗号化は利用されない。ただし、本発明の趣旨および範囲を逸脱することなく、何らかの種類のDRM暗号化をアプリケーションに関連して使用することができる。代わりに、本発明の一実施形態では、図13を参照すると、記載したアプリケーションは、どこか内部に、DRMシステム32と協働してアプリケーションがロードされ、実行されるのを許されるべきことを確実にする第1のセットのコード60を含む。詳細には、アプリケーションが、DRMコンテンツ12として作用し、少なくとも1つの対応するDRMライセンス16を有し、アプリケーション12内部の第1のコード60により、何らかの時点で、アプリケーション12が、計算デバイス14上のDRMシステム32の認証を行うようにさせられる。

40

【0173】

特に、アプリケーション12内部の第1のコード60は、本発明の趣旨および範囲を逸脱

50

することなく、適切な時点でDRMシステム32の認証をトリガする。例えば、認証は、アプリケーション12がロードされたとき、アプリケーション12の1つまたは複数の特定の機能のそれぞれにアクセスが行われたとき、かつ／または10分ごとになど、周期的にトリガされることが可能である。さらに、前述した特定のファンクションに関して、対応するライセンス16により、各ファンクションにアクセスすることができるかどうか指定されることが可能である。さらに、それぞれの特定のファンクションが、別々の対応するライセンス16を必要とすること、または特定のファンクションの特定のもの、および／または組合せに関して複数のライセンス16が利用可能であり得ることが可能である。

【0174】

本発明の一実施形態では、第1のコード60は、アプリケーション12の開発中にアプリケーションに追加される。したがって、アプリケーション12の開発者は、アプリケーション12に第1のコード60を追加することによって認証を使用することを組み込む。

【0175】

理解されるであろうとおり、不正なエンティティが、第1のコード60の動作を迂回し、これにより、第1のコード60が、アプリケーション12のDRM認証をトリガするのを防止することを試みる可能性がある。この迂回は、例えば、第1のコード60を迂回するようにアプリケーション12を書き換えることにより、またはアプリケーション12から第1のコード60を削除するか、または別の仕方では除去することによって達することが可能である。したがって、アプリケーション12内部の第1のコード60のそのような迂回を回避するため、本発明の一実施形態では、第1のコード60を含むアプリケーション12が、開発中に、第1の保護されていない形態から第2の保護された形態に完全性プロテクタ(integrity protector)62(図13)によって変換される。

【0176】

一般に、完全性プロテクタ62は、第2の形態のアプリケーション12が、第1の形態のアプリケーション12と同じように機能するように操作する。ただし、重要なこととして、第1の形態から第2の形態へのアプリケーション12の変換中、完全性プロテクタ62は、前述した不正なエンティティによって試みられるもののような、第2の形態からのアプリケーションのあらゆる改変、改造、または変更により、アプリケーション12が動作しなくなる結果が、その結果を回避する相当な努力が行われな限り、もたらされるようにアプリケーション12を変更する。完全性プロテクタ62は、アプリケーション12の各インスタンスを固有バージョンとして生成するように使用することができ、アプリケーション12のインスタンスのグループを固有バージョンとして生成するように使用することができ、かつ／またはアプリケーション12のすべてのインスタンスを同一のバージョンとして生成するように使用することができ、ことに留意されたい。一般に、完全性プロテクタ62は、ソフトウェア構成体であり、当分野の技術者一般には周知であるか、または明白なはずである。したがって、本発明の趣旨および範囲を逸脱することなく、任意の適切なソフトウェアまたはハードウェアの完全性プロテクタ62を使用することができる。

【0177】

完全性プロテクタ62の例が、参照により本明細書に組み込まれている、2000年3月14日に出願した「BORE-Resistant Digital Goods Configuration and Distribution Methods And Arrangements」という名称(例えば、米国特許出願番号09/525,206(整理番号MS1-394US/131064.1))に提示されている。簡単に述べると、この出願では、完全性プロテクタは、コードオブティマイザ(optimizer)が、実行可能コードを受け取り、所定の最適化パラメータに基づいてそのコードを最適化するコード最適化の副産物である。要点を述べると、コードオブティマイザが、最適化パラメータに従ってコードの部分を再構成して、機能的に等価である(すなわち、同一の機能を行う)が、動作上、最適化された最適化バージョンを生成する。さらに、この最適化されたコードは、最適化後に変更された場合、通常、動作しなくなる。

【0178】

完全性プロテクタ62により、ディストリビュータ(distributor)プログラムによって配信されたアプリケーション12が、完全性の保護された形態になることが確実にすることに留意されたい。したがって、本発明の趣旨および範囲を逸脱することなく、配布のために完全性の保護された形態でアプリケーション12を生成する任意の他の方法、または機構を使用することができる。例えば、この完全性の保護された形態は、アプリケーション12を設計し、符号化する過程で実現することができる。

【0179】

本発明の一実施形態では、第1のコード60を有するアプリケーション12のライセンスが、ユーザの計算デバイス12上のDRMシステム32に従ってそのユーザに与えられる。したがって、ユーザは、上記に指定したような任意の適切な仕方でライセンスサーバ24等からDRMライセンス16を獲得する。ただし、重要なこととして、獲得されたライセンス16は、特に、アプリケーション12が暗号化される必要がない限りで、アプリケーション12を暗号化解除するコンテンツ鍵を含まない。代わりに、図13に見られるとおり、獲得されたライセンス16は、アプリケーション12を識別する識別情報64を含む。もちろん、それでも、本発明の趣旨および範囲を逸脱することなく、アプリケーション12の暗号化を使用することもできる。

10

【0180】

計算デバイス14上のアプリケーション12の実行中、第1のコード60が、DRMシステム32を検査して、獲得されたDRMライセンス16が計算デバイス上に存在することを確実にする。詳細には、本発明の一実施形態では、第1のコード60が、DRM認証の一環として、計算デバイス14上のDRMシステム32と認証プロトコルをやり取りして、ライセンス16に基づき、アプリケーション12を実行するのが許されているという証拠をDRMシステム32から獲得する。

20

【0181】

次に、図14を参照すると、第1のコード60が、次のように動作するのが分かる。準備として、理解されたとおり、第1のコード60が、アプリケーション12のロードの最初の部分としてか、アプリケーション12の動作中の何らかの所定の時点においてか、周期的にか、または別の仕方で、何らかの時点においてトリガされる(ステップ1401)。次に、第1のコード60は、計算デバイス14上のDRMシステム32が、自らが有効なDRMシステム32であることを証明するように要求する(ステップ1403)。本発明の一実施形態では、この証明は、前述した仕方で、すなわち、信頼される機関からの証明書やそれに類するもの、デジタル署名等を提示することによって行われる。特に、計算デバイス14上のDRMシステム32が、自らを第1のコード60に対して証明するようにさせることは、DRMシステム32がどのようにか破壊され、対応するライセンス16に関係なくアプリケーション12を実行するが可能になるシナリオを防止しようとする試みである。想定上、DRMシステム32は、破壊された場合、自らを第1のコード60に対して証明することができない。というのは、破壊されたDRMシステム32により、証明書が損なわれるか、提示された署名が不合格になる等のことがもたらされるからである。さらに基本的なこととして、DRMシステム32が自らを証明するようにさせることにより、アプリケーションが、実際に、DRMシステム32と通信していること自体が確実になる。簡単に述べると、アプリケーション12は、予期される要素、すなわち、DRMシステム32とだけ通信していることを必要とする。

30

40

【0182】

したがって、第1のコード60は、DRMシステム32からの提示されたアイテムを受け取り、検査して(ステップ1405)、そのアイテムを検討し(ステップ1407)、DRMシステム32が、有効なものであり、アプリケーション60の所有者の権利を行使することができるかどうかの判断を行う(ステップ1409)。この判断は、本発明の趣旨および範囲を逸脱することなく、任意の適切な仕方で行うことが可能であることに留意されたい。例えば、提示されたアイテムが署名である場合、その署名が、適切なものとして

50

確認され、また提示されたアイテムが証明書である場合、その証明書が適切なものとして検査される。

【0183】

DRMシステム32が第1のコード60によって認証される前、認証されている最中、および認証された後に、第1のコード60は、有効なDRMライセンス16により、所与の条件下でアプリケーション12が実行することが許されるかどうかをDRMシステム32が判定することを要求する(ステップ1411)。したがって、DRMシステム32は、ライセンス16の中のあらゆる条項を前述した仕方でも検討して、その条項により、要求される仕方でもアプリケーション12の実行が許されるかどうかを判定する。もちろん、実行は、条項によって許可される場合にだけ許可される。

10

【0184】

本発明の一実施形態では、計算デバイス14上に常駐するアプリケーション12は、大域的に固有であることも、固有でないことも可能なID(図13)を有し、アプリケーション12に関してライセンサによって発行され、アプリケーション12を有する計算デバイス14上に常駐するあらゆるライセンス16は、アプリケーション12の識別情報64の中にアプリケーション12のIDを含む。したがって、DRMシステム32、または第1のコード60により、ライセンス16の識別情報64の中のIDが、アプリケーション12のIDに一致するかどうかの判定が行われる(ステップ1413)。もちろん、先に進むには、一致を要する。DRMシステム32がこの判定を行う場合、DRMシステム32は、ライセンス16の識別情報64から、またアプリケーション12からIDを獲得する(ステップ1413a)ことに留意されたい。同様に、アプリケーション12の第1のコード60がこの判定を行う場合、DRMシステム32が、ライセンス16の識別情報64からIDを獲得して、そのIDを第1のコードに送る(ステップ1413b)。

20

【0185】

ライセンス16が、アプリケーション12のIDを含む識別情報64を有することで、アプリケーションが、ライセンス16に結び付けられる。同様に、ライセンス16が、前述したようなある結合情報を有することで、ライセンスは、DRMシステム32、および計算デバイス14に結び付けられる。ただし、それだけでは、アプリケーション12は、DRMシステム、または計算デバイス14に直接に結び付けられない。したがって、アプリケーション12、および対応するライセンスが、別の計算デバイス14上の別のDRMシステム32にコピーされることが可能であり、その別のDRMシステム32が、有効なライセンス16かどうか調べないが、それでも、信頼される価値があると自らを第1のコード60に対して提示することができる場合、第1のコード60が、覆される。

30

【0186】

したがって、本発明の一実施形態では、アプリケーション12が、DRMシステム32、または計算デバイス14に直接に結び付けられる。詳細には、この実施形態では、アプリケーション12に関するライセンス16をライセンサから獲得することに加えて、ユーザは、アプリケーション12のID、およびDRMシステム32または計算デバイス14のIDを含む証明書66(図13)も、ライセンサから獲得する。したがって、証明書66は、アプリケーション12をDRMシステム32、または計算デバイス14に結び付けるか、バインドするか、または結合させる。証明書66は、本発明の趣旨および範囲を逸脱することなく、獲得されたライセンス16の中にあることも、ライセンス16とは別個であることも可能であり、またライセンス16とともに獲得することも、別の時点で獲得することも可能であることに留意されたい。また、DRMシステム32のIDは、DRMシステム32の所定の固有IDであること、ブラックボックス鍵(PU-BB、PR-BB)に基づくこと、またはその他の鍵に基づくことが可能である。

40

【0187】

さらに、この実施形態では、アプリケーション12は、DRMシステム32または計算デバイス14と協働して、第2のコード68を有するアプリケーション12が、実際に、DRMシステム32または計算デバイス14に結び付いている、または結合されていること

50

を確実にする（すなわち、結合検査を行う）第2のセットのコード68を備える。詳細には、第2のコード68は、証明書66を検査し、アプリケーション12、およびDRMシステム32または計算デバイス14から適切な識別情報を獲得し、その識別情報から、DRMシステム32または計算デバイス14、およびアプリケーション12が、証明書66の中で特定されているものであるかどうかを判定する。DRMシステム32または計算デバイス14の識別情報は、DRMシステム32または計算デバイス14のIDを含むその情報からの証明書または署名であることが可能であり、またアプリケーション12の識別は、アプリケーション12の前述したIDであることが可能である。

【0188】

特に、第2のコード68は、第1のコード60が実行されるたびに毎回、実行される、または第1のコード60が実行されたとき、何らかの事前選択された時点にだけ実行されることが可能である。例えば、第2のコード68は、アプリケーション12の最初のロード時にだけ実行されることが可能である。

10

【0189】

本発明の一実施形態では、第1のコード60の場合と同様に、第2のコード68は、アプリケーション12の開発中にアプリケーション12に追加される。したがって、アプリケーション12の開発者は、第2のコード68をアプリケーション12に追加することにより、また証明書66が、ライセンシングプロセスの一環として、または別の時点でアプリケーション12のユーザに提供されることを確実にすることにより、結合検査を組み込む。

20

【0190】

第1のコード60の場合と同様に、不正なエンティティが、第2のコード68の動作を迂回し、これにより、第2のコード68が、結合検査を行うのを防止することを試みる可能性がある。この場合も、そのような迂回は、例えば、第2のコード68を迂回するようにアプリケーション12を書き換えることにより、またはアプリケーション12から第2のコード68を削除する、または別の仕方で除去することにより達することが可能である。ただし、第1のコード60および第2のコード68を含むアプリケーション12が、開発中に完全性プロテクタ62（図13）により第1の保護されていない形態から第2の保護された形態に変換されるものと想定すると、アプリケーション12の中の第2のコード68の迂回は、容易に行うことができない。

30

【0191】

次に、図15を参照すると、第2のコード68が、次のように動作するのが分かる。準備として、理解されるとおり、第2のコード68は、アプリケーション12のロードの最初の部分として、またはアプリケーション12の動作中、何らかの所定の時点で、何らかの時点でトリガされる（ステップ1501）。理解されるとおり、第2のコード68は、第1のコード60がトリガされるたびに毎回、トリガされることが可能であり、実際、第1のコード60によってトリガされることが可能であり、あるいは場合により、第1のコード60以外のコードによって他の時点でトリガされることが可能である。

【0192】

その後、第2のコード68は、アプリケーション12のID、およびDRMシステム32または計算デバイス14のIDを含む証明書66（図13）をライセンサから取得し（ステップ1503）、DRMシステム32または計算デバイス14からDRMシステム32または計算デバイス14のIDを取得し（ステップ1505）、またアプリケーション12からアプリケーション12のIDを取得する（ステップ1507）。したがって、アプリケーション12から取得されたIDが、証明書66からのアプリケーションIDに一致するかどうかの判定（ステップ1509）、およびDRMシステム32または計算デバイス14から取得されたIDが、証明書66からのDRMシステム／計算デバイスIDに一致するかどうかの判定（ステップ1511）が、第2のコード68によって行われる。もちろん、先に進むには、各判定により、一致がもたらされなければならない（ステップ1513）。そうでなく、結合検査が不合格であった場合、アプリケーション12の実行は

40

50

停止されるか、または別の仕方で切り上げられる。

【0193】

証明書66および第2のコード68を使用することの主要な態様は、アプリケーション12が、直接に、またはDRMシステム32を介して間接的に、容易に複製して配布することができない要素に結び付けられることである。通常、この要素は、元来、ソフトウェアファイルより複製して配布するのに費用がかかるハードウェアである。通常、このハードウェアは、ライセンスが、アプリケーションが実行される場所として意図する計算デバイス14である。ただし、ハードウェアは、本発明の趣旨および範囲を逸脱することなく、任意の他の適切なアイテムであることが可能である。例えば、ハードウェアは、スマートカード、または認証することが可能な任意の他の物理的なトークンであることが可能である。また、ハードウェアは、3つの計算デバイス14と5つのトークンのセットなどの、複数のアイテムとして指定されることも可能である。

10

【0194】

証明書66を使用してアプリケーション12を何らかのエンティティに結合させることができるが、本発明の趣旨および範囲を逸脱することなく、他のタイプの結合表現も使用できることにも留意されたい。例えば、結合先のエンティティ(married-to-entity)のセットを符号化してアプリケーション12の実行可能コードにすることが可能である。

【0195】

<結論>

20

本発明では、計算デバイス14上のDRMシステム32が、対応するライセンス16の条項に従って計算デバイス14上のアプリケーション12の実行を許す。重要なこととして、計算デバイス14上のDRMシステム32は、DRMシステム32が、対応するライセンス16の欠如にも関わらず、またはライセンス16の条項に基づく許可にも関わらず、アプリケーション12の実行を許すように不正なエンティティによって破壊される可能性があるものと想定されている。

【0196】

したがって、アプリケーション12は、基本的に、DRMシステム32が、自らを信頼に値するものとしてアプリケーション12に認証することを要求する第1のセットのコード60を備える。さらに、アプリケーション12は、基本的に、アプリケーション12が、DRMシステム32を有する計算デバイス14を宛先とすることを確実にする第2のセットのコード68を備える。最後に、第1のコード60および第2のコード68を有するアプリケーション12が、完全性プロテクタ62によって処理されて、第1のコード60または第2のコード68の機能を迂回しようとするあらゆる試みにより、アプリケーション12が動作しないようになることが、そうした結果を回避しようとする相当な努力がなされない限り、もたらされることを確実にする。

30

【0197】

特に、DRMシステム32が破壊される可能性があるという想定に基づき、アプリケーション12の第1のコード60および第2のコード68が、それぞれのアクションを行うことが頼りにされる。さらに、第1のコード60および第2のコード68は、アプリケーション12の一部であり、アプリケーション12とともにロードされるので、計算デバイス14上に常駐するオペレーティングシステムのローダは、第1のコード60および第2のコード68の機能を実施する際に課される特別の手続きに関与する必要がない。

40

【0198】

本発明は、1つまたは複数の構成ファイルが、計算デバイス14上のDRMシステム32によって規制される対応するライセンス16に従ってだけ実行されるアプリケーション12に関連して特に有用である。ただし、重要なこととして、本発明は、本発明の趣旨および範囲を逸脱することなく、例えば、テキスト、オーディオ、ビデオ、および／またはマルチメディアのコンテンツ12などの、計算デバイス14上のDRMシステム32によって規制される対応するライセンス16に従ってだけレンダリングされる任意の他のコンテ

50

ンツ 12 に関して実施することも可能である。

【0199】

本発明に関連して、ソフトウェアアプリケーション 12 の保護をサポートする方法および機構が、必ずしも本明細書で開示するすべての DRM 機能は必要としないことに留意することが重要である。最も重要なこととして、存在しなければならない DRM 機能には、ライセンス評価が含まれる。詳細には、各ライセンス 16 を評価し、アプリケーション 12、またはアプリケーション 12 の一部を実行することなどの特定のアクションが許可されているかどうかを判定することができるライセンスイバリユエータ 36 が存在しなければならない。ライセンスイバリユエータ 36 は、必ずしも計算デバイス 14 上の完全な DRM システム 32 に含まれる必要がない。例えば、ライセンスイバリユエータ 36 は、アプリケーション 12 内部に含まれることが可能であり、あるいは独立の要素であることが可能である。したがって、規制は、本発明の趣旨および範囲を逸脱することなく、基本的な DRM タイプの機能によって行われ、DRM システム 32 自体によっては行われないことが可能である。

10

【0200】

本発明に関連して行われるプロセスを実施するのに必要なプログラミングは、比較的簡単であり、該当のプログラミング分野の技術者一般 (relevant programming public) には明白であるはずである。したがって、そのプログラミングは、本明細書には添付しない。したがって、本発明の趣旨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施することができる。

20

【0201】

以上の説明では、DRM アーキテクチャ 10 が、ソフトウェアアプリケーション 12 が、アプリケーション 12 の所有者等によって望まれない仕方で使用されるのを防止することにより、アプリケーション 12 の保護をサポートすることを可能にする新しく有用な方法および機構を本発明が含むことを理解することができる。本発明の概念を逸脱することなく、前述した実施形態に変更を加えることができることを理解されたい。一例として、本発明の一実施形態では、DRM システム 32 が、アプリケーション 12 の第 1 のコード 60 および／または第 2 のコード 68 を無しで済ませ、単に、特定の ID、または他の識別情報、あるいはハードウェアまたはソフトウェアの存在などの計算デバイス 14 に関する条件について試験を行う。別の例として、本発明の別の実施形態では、DRM システム 32 の機能が、アプリケーション 12 内部に含まれ、したがって、DRM システム 32 が、アプリケーション 12 に対して認証される必要がない。

30

【0202】

したがって、本発明は、開示した特定の実施形態には限定されず、頭記の特許請求の範囲によって定義される本発明の趣旨および範囲に含まれる変更形態を範囲に含むものとする。

【0203】

【発明の効果】

以上説明したように、本発明によれば、ある機能を行うために実行されるアプリケーションに関する DRM デジタルライセンスがすべて計算デバイス上に存在する場合、該アプリケーションは、計算デバイスの 1 つの上で実行されるべきであることを判定するためのコード、または、ライセンスに基づき上記ある機能を行うように実行されることが許されているかどうかを判定する DRM システムに関連して実行されるべきであることを判定するためのコードを含んでいるので、例えば、デジタルコンテンツのユーザによって獲得されたライセンス権利によって指定されたパラメータに従ってのみ暗号化されたデジタルコンテンツへのアクセスを許すことができるようになり、特に、デジタルコンテンツのコンテンツ所有者によってそのデジタルコンテンツの再配布の防止に関する規制を任意に定義することができ、任意の形態のデジタルコンテンツの規制されたレンダリングまたは再生を行うことができ、これにより、デジタルコンテンツの再配布の防止に関する規制を柔軟に対応させることが可能な行使アーキテクチャおよび行使方法を作成することができる。

40

50

【図面の簡単な説明】

【図 1】本発明の一実施形態による行使アーキテクチャを示すブロック図である。

【図 2】本発明の一実施形態による図 1 のアーキテクチャのオーサリングツール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有するデジタルコンテンツパッケージを示すブロック図である。

【図 4】本発明の一実施形態による図 1 のユーザの計算デバイスを示すブロック図である。

【図 5 A】本発明の一実施形態によるコンテンツをレンダリングする図 4 の計算デバイスのデジタル権利管理（D R M）システムに関連して行われるステップを示す流れ図である。

10

【図 5 B】本発明の一実施形態によるコンテンツをレンダリングする図 4 の計算デバイスのデジタル権利管理（D R M）システムに関連して行わ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よる何らかの有効な、使用を可能にする（e n a b l i n g）ライセンスが存在するかどうかを判定する図 4 の D R M システムに関連して行わ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よるライセンスを獲得する図 4 の D R M システムに関連して行わ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よる図 1 のアーキテクチャに関連して使用されるデジタルライセンスを示すブロック図である。

20

【図 9】本発明の一実施形態による新しいブラックボックスを獲得する図 4 の D R M システムに関連して行われるステップを示す流れ図である。

【図 1 0】本発明の一実施形態によるライセンスおよびデジタルコンテンツを検証し、そのコンテンツをレンダリングする図 4 の D R M システムに関連して行わ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 1 1】本発明の一実施形態による図 4 のライセンスイバリユエータをライセンスのデジタル権利ライセンス（D R L）および D R L を解釈するための言語エンジンとともに示すブロック図である。

【図 1 2】本発明の態様、および／または態様の部分を組み込むことができる汎用コンピュータシステムを示すブロック図である。

30

【図 1 3】本発明の実施形態による D R M 機能を実行するための第 1 のコードおよび第 2 のコードを有するアプリケーションを示すブロック図である。

【図 1 4】本発明の実施形態による第 1 のコードに対して D R M システムを検証する図 1 3 の第 1 のコードに関連して行われる主要なステップを示す流れ図である。

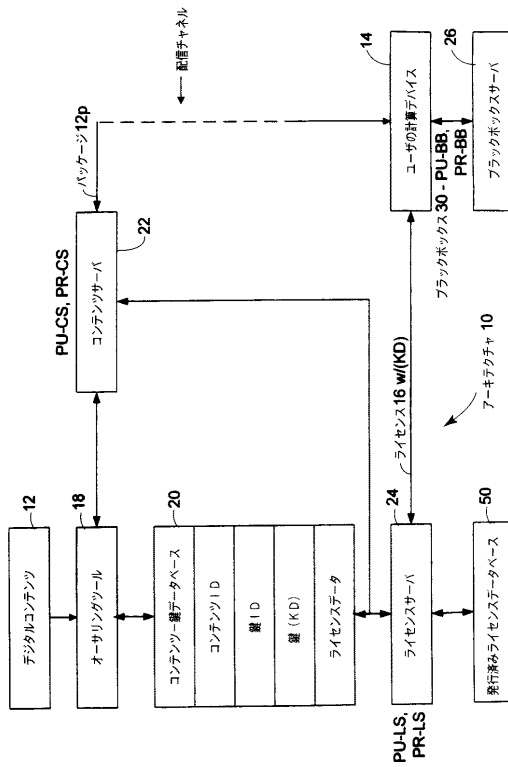
【図 1 5】本発明の実施形態による D R M システムにアプリケーションが「組み合わされる」ことを確実にする図 1 3 の第 2 のコードに関連して行われる主要なステップを示す流れ図である。

【符号の説明】

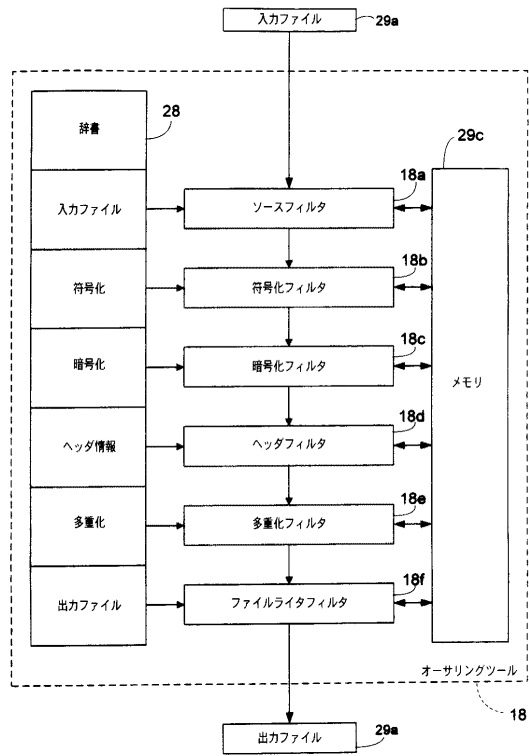
- 1 2 デジタルコンテンツ
- 1 6 デジタルライセンス
- 3 0 ブラックボックス
- 3 2 D R M システム
- 3 4 レンダリングアプリケーション
- 3 8 ライセンスストア

40

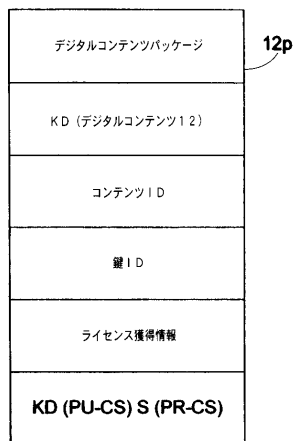
【図 1】



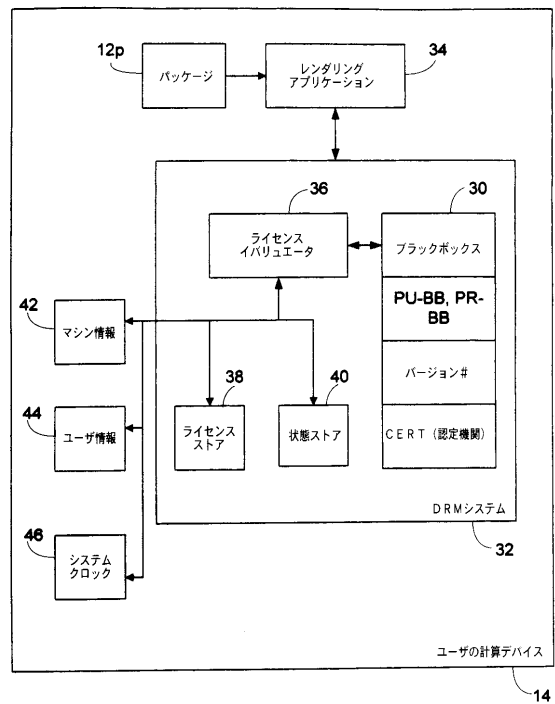
【図 2】



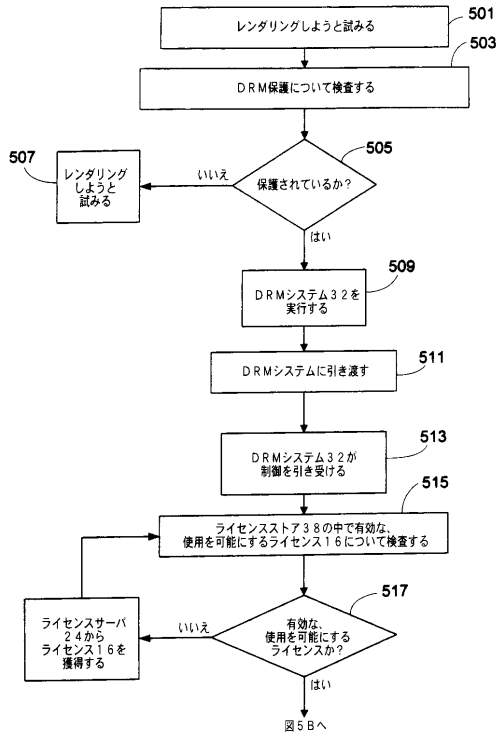
【図 3】



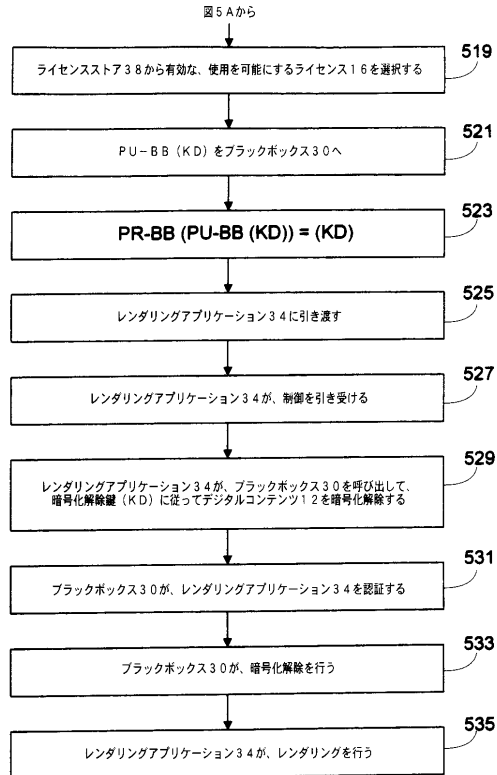
【図 4】



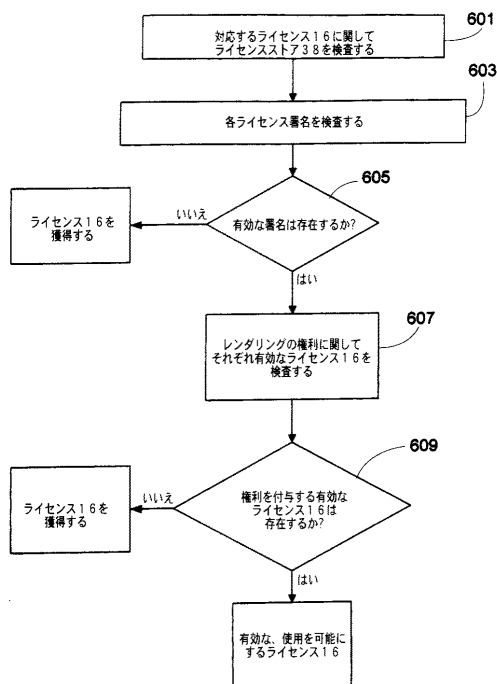
【図 5 A】



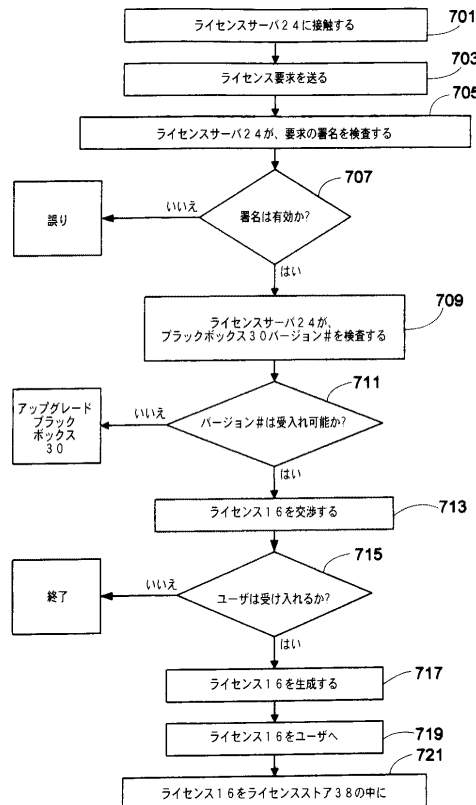
【図 5 B】



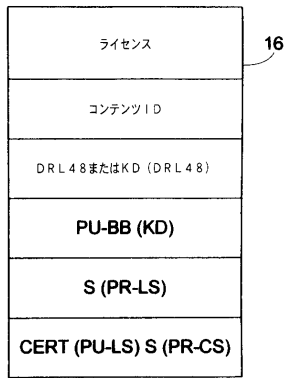
【図 6】



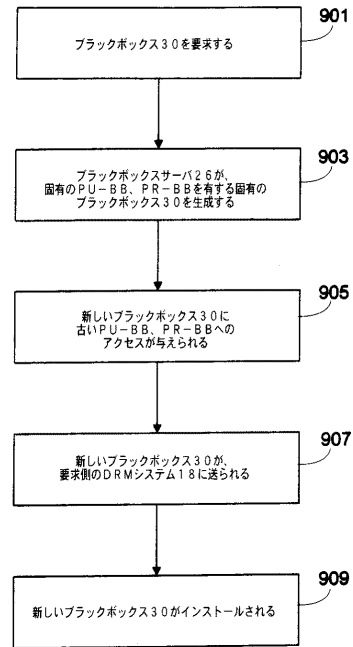
【図 7】



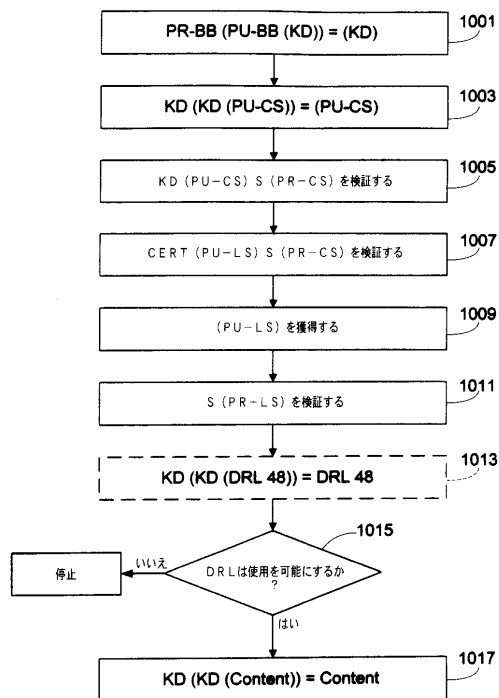
【図 8】



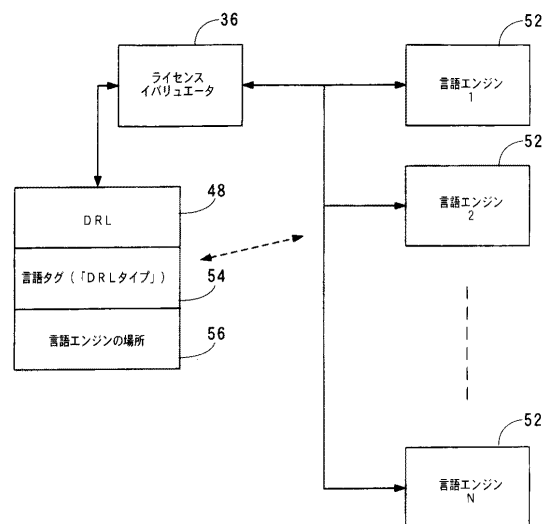
【図 9】



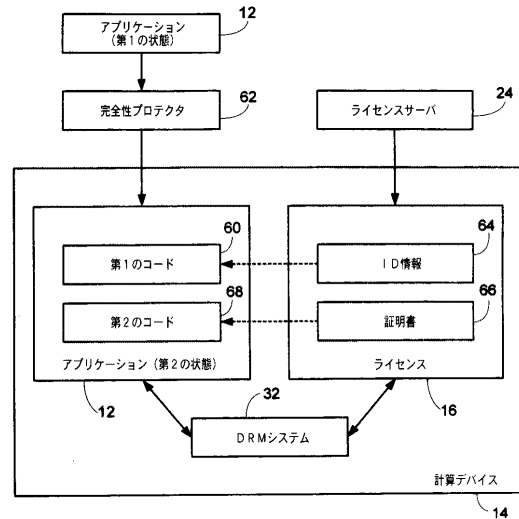
【図 10】



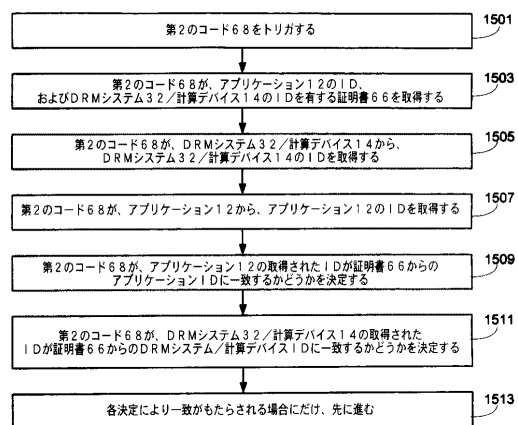
【図 11】



【图 1 3】



【図 15】



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 ノースラップ ウェイ 16659

(72)発明者 ジョン エル. マンファードリ

アメリカ合衆国 98053 ワシントン州 レッドモンド 245 ウェイ ノースイースト
7921

審査官 岩崎 志保

(56)参考文献 特開2000-330783 (JP, A)

国際公開第02/019598 (WO, A1)

特開2000-242491 (JP, A)

特開2001-051742 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/22