

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4559639号
(P4559639)

(45) 発行日 平成22年10月13日 (2010. 10. 13)

(24) 登録日 平成22年7月30日 (2010. 7. 30)

(51) Int. Cl.	F I
G06Q 30/00 (2006.01)	G06F 17/60 302E
G06F 21/00 (2006.01)	G06F 15/00 330Z

請求項の数 11 (全 45 頁)

(21) 出願番号	特願2000-608539 (P2000-608539)	(73) 特許権者	500046438
(86) (22) 出願日	平成12年2月25日 (2000. 2. 25)		マイクロソフト コーポレーション
(65) 公表番号	特表2003-536119 (P2003-536119A)		アメリカ合衆国 ワシントン州 9805
(43) 公表日	平成15年12月2日 (2003. 12. 2)		2-6399 レッドモンド ワン マイ
(86) 国際出願番号	PCT/US2000/004947		クロソフト ウェイ
(87) 国際公開番号	W02000/059150	(74) 代理人	100140109
(87) 国際公開日	平成12年10月5日 (2000. 10. 5)		弁理士 小野 新次郎
審査請求日	平成19年2月22日 (2007. 2. 22)	(74) 代理人	100089705
(31) 優先権主張番号	60/126, 614		弁理士 社本 一夫
(32) 優先日	平成11年3月27日 (1999. 3. 27)	(74) 代理人	100075270
(33) 優先権主張国	米国 (US)		弁理士 小林 泰
(31) 優先権主張番号	09/290, 363	(74) 代理人	100080137
(32) 優先日	平成11年4月12日 (1999. 4. 12)		弁理士 千葉 昭男
(33) 優先権主張国	米国 (US)	(74) 代理人	100096013
前置審査			弁理士 富田 博行

最終頁に続く

(54) 【発明の名称】 デジタルデジタル権利管理の実施アーキテクチャおよび方法

(57) 【特許請求の範囲】

【請求項 1】

コンピュータ装置上でデジタル権利管理 (DRM) システムを動作させるコンピュータ実行可能な命令を格納するコンピュータ読取可能媒体であって、前記コンピュータ装置は暗号解読及び暗号化手段を有し、前記暗号解読及び暗号化手段は公開／秘密鍵対を含み、前記命令は、実行されると、コンピュータ装置に、

ライセンス格納部に1つ以上のデジタル・ライセンスを格納するステップであって、前記デジタル・ライセンスは前記コンピュータ装置からのライセンス要求に応答してライセンス・サーバにより発行され、前記ライセンス・サーバは前記デジタル・ライセンスの発行に先立って前記暗号解読及び暗号化手段の認証を行う、ステップと、

前記ライセンス格納部内の前記1つ以上のデジタル・ライセンスの各々に関して行われたレンダリングの状態に関する状態情報を状態格納部に保持するステップであって、前記1つ以上のデジタル・ライセンスのうち少なくとも1つに対応するレンダリングの状態に関する状態情報を保持するステップを含む、ステップと、

保護されるデジタル・コンテンツを前記コンピュータ装置上で特定の態様でレンダリングする要求をユーザから受信するステップと、

前記ライセンス格納部に格納されている前記1つ以上のデジタル・ライセンスのうち少なくとも1つが前記保護されるデジタル・コンテンツに対応するか否かを決定するステップであって、前記ライセンス格納部に格納されている前記1つ以上のデジタル・ライセンスのいずれもが前記保護されるデジタル・コンテンツに対応しない場合には、対応するデ

10

20

ジタル・ライセンスを取得するステップと、

前記ライセンス格納部に格納されている前記1つ以上のデジタル・ライセンスのうち少なくとも1つが前記保護されるデジタル・コンテンツに対応する場合には、暗号解読機能を実行することにより少なくとも部分的に前記対応するデジタル・ライセンスを評価するステップと

を実行させ、前記対応するデジタル・ライセンスの評価は、前記コンピュータ装置が、

前記対応するデジタル・ライセンスが有効か否かを決定するステップと、

前記対応するデジタル・ライセンスにおけるライセンス規則を確認するステップであって、前記ライセンス規則は前記対応するデジタル・ライセンスにより許可されるレンダリングの種類を指定する、ステップと、

10

前記ライセンス規則により許可されるレンダリングの種類及び前記状態格納部に保持される前記状態情報において示されるレンダリングの状態に基づいて、要求を行っているユーザが要求される特定の態様で前記保護されるデジタル・コンテンツをレンダリングすることを許可されるか否かを決定するステップであって、前記状態格納部に保持される前記状態情報はデジタル・ライセンスの各評価により更新される、ステップとを実行することを含み、前記命令はさらに、前記コンピュータ装置に、

前記要求を行っているユーザが前記要求される特定の態様で前記保護されるデジタル・コンテンツのレンダリングを許可される場合、前記対応するデジタル・ライセンスから解読鍵を取得し、前記解読鍵を使用して前記保護されるデジタル・コンテンツを暗号解読するステップ

20

を実行させることを含む、コンピュータ読取可能媒体。

【請求項2】

前記ライセンス格納部は、前記1つ以上のデジタル・ライセンスに対するアクセスを提供し、前記保護されるデジタル・コンテンツに対するアクセスを提供しない請求項1に記載のコンピュータ読取可能媒体。

【請求項3】

コンピュータ装置上でデジタル権利管理(DRM)システムを動作させる方法であって、前記コンピュータ装置は暗号解読及び暗号化手段を有し、前記暗号解読及び暗号化手段は公開／秘密鍵対を含み、

前記コンピュータ装置内のライセンス格納部が1つ以上のデジタル・ライセンスを格納するステップであって、前記デジタル・ライセンスは前記コンピュータ装置からのライセンス要求に応答してライセンス・サーバにより発行され、前記ライセンス・サーバは前記デジタル・ライセンスの発行に先立って前記暗号解読及び暗号化手段の認証を行う、ステップと、

30

前記ライセンス格納部内の前記1つ以上のデジタル・ライセンスの各々に関して行われたレンダリングの状態に関する状態情報を前記コンピュータ装置内の状態格納部が保持するステップであって、前記1つ以上のデジタル・ライセンスのうち少なくとも1つに対応するレンダリングの状態に関する状態情報を保持するステップを含む、ステップと、

保護されるデジタル・コンテンツを前記コンピュータ装置上で特定の態様でレンダリングする要求を、前記コンピュータ装置がユーザから受信するステップと、

40

前記ライセンス格納部に格納されている前記1つ以上のデジタル・ライセンスのうち少なくとも1つが前記保護されるデジタル・コンテンツに対応するか否かを前記コンピュータ装置が決定するステップであって、前記ライセンス格納部に格納されている前記1つ以上のデジタル・ライセンスのいずれもが前記保護されるデジタル・コンテンツに対応しない場合には、前記コンピュータ装置が対応するデジタル・ライセンスを取得するステップと、

前記ライセンス格納部に格納されている前記1つ以上のデジタル・ライセンスのうち少なくとも1つが前記保護されるデジタル・コンテンツに対応する場合には、前記コンピュータ装置が、暗号解読機能を実行することにより少なくとも部分的に前記対応するデジタル・ライセンスを評価するステップと

50

を含み、前記対応するデジタル・ライセンスの評価は、前記コンピュータ装置が、

前記対応するデジタル・ライセンスが有効か否かを決定するステップと、

前記対応するデジタル・ライセンスにおけるライセンス規則を確認するステップであって、前記ライセンス規則は前記対応するデジタル・ライセンスにより許可されるレンダリングの種類を指定する、ステップと、

前記ライセンス規則により許可されるレンダリングの種類及び前記状態格納部に保持される前記状態情報において示されるレンダリングの状態に基づいて、要求を行っているユーザが要求される特定の態様で前記保護されるデジタル・コンテンツをレンダリングすることを許可されるか否かを決定するステップであって、前記状態格納部に保持される前記状態情報はデジタル・ライセンスの各評価により更新される、ステップとを実行することを含み、前記方法はさらに、前記コンピュータ装置が、

前記要求を行っているユーザが前記要求される特定の態様で前記保護されるデジタル・コンテンツをレンダリングすることを許可される場合、前記対応するデジタル・ライセンスから解読鍵を取得し、前記解読鍵を使用して前記保護されるデジタル・コンテンツを暗号解読するステップを含む方法。

【請求項 4】

前記ライセンス格納部は、前記 1 つ以上のデジタル・ライセンスに対するアクセスを提供し、前記保護されるデジタル・コンテンツに対するアクセスを提供しない請求項 3 に記載の方法。

【請求項 5】

対応するデジタル・ライセンスを取得する前記ステップは、前記コンピュータ装置が、前記保護されるデジタル・コンテンツからライセンス取得情報を取得するステップをさらに含む請求項 3 に記載の方法。

【請求項 6】

前記ライセンス取得情報はライセンス・サーバ位置を含み、対応するデジタル・ライセンスを取得する前記ステップは、前記ライセンス・サーバ位置におけるライセンス・サーバから前記コンピュータ装置が前記対応するデジタル・ライセンスを取得するステップを更に含む請求項 5 に記載の方法。

【請求項 7】

公開／秘密鍵対を含む暗号解読及び暗号化手段を有する、デジタル権利管理（DRM）システムを動作させるコンピュータ装置であって、

1 つ以上のデジタル・ライセンスを格納するライセンス格納部であって、前記デジタル・ライセンスは前記コンピュータ装置からのライセンス要求に応答してライセンス・サーバにより発行され、前記ライセンス・サーバは前記デジタル・ライセンスの発行に先立って前記暗号解読及び暗号化手段の認証を行う、ライセンス格納部と、

前記 1 つ以上のデジタル・ライセンスのうち少なくとも 1 つに対応するレンダリングの状態に関する状態情報の保持を含む、前記ライセンス格納部内の前記 1 つ以上のデジタル・ライセンスの各々に関して行われたレンダリングの状態に関する状態情報を保持する状態格納部と、

保護されるデジタル・コンテンツをコンピュータ装置上で特定の態様でレンダリングする要求をユーザから受信する手段と、

前記ライセンス格納部に格納されている前記 1 つ以上のデジタル・ライセンスのうち少なくとも 1 つが前記保護されるデジタル・コンテンツに対応するか否かを決定する手段であって、対応する場合に、対応するデジタル・ライセンスを出力し、前記ライセンス格納部に格納されている前記 1 つ以上のデジタル・ライセンスのいずれもが前記保護されるデジタル・コンテンツに対応しない場合には、対応するデジタル・ライセンスを取得する手段と、

暗号解読機能を実行することにより少なくとも部分的に前記対応するデジタル・ライセンスを評価する手段と

10

20

30

40

50

を含み、前記評価する手段は、

前記対応するデジタル・ライセンスが有効か否かを決定する手段と、

前記対応するデジタル・ライセンスにおけるライセンス規則を確認する手段であって、前記ライセンス規則は前記対応するデジタル・ライセンスにより許可されるレンダリングの種類を指定する、手段と、

前記ライセンス規則により許可されるレンダリングの種類及び前記状態格納部に保持される前記状態情報において示されるレンダリングの状態に基づいて、要求を行っているユーザが要求される特定の態様で前記保護されるデジタル・コンテンツをレンダリングすることを許可されるか否かを決定する手段であって、許可される場合に、前記対応するデジタル・ライセンスから解読鍵を出力し、前記状態格納部に保持される前記状態情報はデジタル・ライセンスの各評価により更新される、手段とを含み、前記DRMシステムはさらに、

10

前記解読鍵を使用して前記保護されるデジタル・コンテンツを暗号解読する手段を含む、コンピュータ装置。

【請求項8】

前記ライセンス格納部は、前記1つ以上のデジタル・ライセンスに対するアクセスを提供し、前記保護されるデジタル・コンテンツに対するアクセスを提供しない請求項7に記載のコンピュータ装置。

【請求項9】

前記対応するデジタル・ライセンスはデジタル署名を含み、前記対応するデジタル・ライセンスが有効か否かを決定する前記手段は、前記デジタル署名を評価する手段をさらに含む請求項7に記載のコンピュータ装置。

20

【請求項10】

前記デジタル署名は前記保護されるデジタル・コンテンツに基づいている請求項9に記載のコンピュータ装置。

【請求項11】

前記解読鍵を使用して前記保護されるデジタル・コンテンツを暗号解読する前記手段は、レンダリング・アプリケーションから前記保護されるデジタル・コンテンツを受信し、前記解読鍵を使用して前記保護されるデジタル・コンテンツを暗号解読し、前記暗号解読された保護されるデジタル・コンテンツを前記レンダリング・アプリケーションに返す手段をさらに含む請求項10に記載のコンピュータ装置。

30

【発明の詳細な説明】

【0001】

(関連出願に対する引用)

本願は、"ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT" (デジタル権利管理実施アーキテクチャおよび方法) と題し、弁理士整理番号MSFT-0063の下で1999年3月27日に出願した米国仮出願第60/126,614号の優先権を主張する。

【0002】

(発明の分野)

本発明は、デジタル・コンテンツにおける権利実施アーキテクチャに関する。更に特定すれば、本発明は、デジタル・コンテンツのユーザが取得した実施権 (licence right) によって指定されるパラメータのみに応じて暗号化デジタル・コンテンツに対するアクセスを許可するようにした、実施アーキテクチャに関する。

40

【0003】

(発明の背景)

デジタル権利の管理および実施は、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・マルチメディア等のようなデジタル・コンテンツに関して、このようなデジタル・コンテンツをユーザに配付する場合に非常に望ましい。典型的な配付方式は、磁気 (フロッピー) ディスク、磁気テープ、光 (コンパクト) ディスク (CD) 等のような有形デバイスや、電子掲示板、電子ネットワーク、インターネ

50

ット等のような無形媒体を含む。ユーザが受信すると、ユーザはメディア・プレーヤ、パーソナル・コンピュータのような適当なレンダリング・デバイスの助けによって、デジタル・コンテンツのレンダリング（rendering）即ち「再生」を行なう。

【0004】

典型的に、コンテンツ所有者即ち著作者、出版社、放送会社等（以下「コンテンツ所有者」）のような権利保有者は、このようなデジタル・コンテンツをライセンス料またはその他の何らかの対価との交換によってユーザ即ち受取人に販売したい。このようなコンテンツ所有者は、選択が認められれば、ユーザがこのように販売したデジタル・コンテンツを用いて行なえることを制限したいことも多いであろう。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したり、第2のユーザに再配付することを、少なくともこのような第2のユーザがコンテンツ所有者にライセンス料を拒否するような態様では、制約したいであろう。

10

【0005】

加えて、コンテンツ所有者は、異なるライセンス料で異なる種類の使用許諾を購入する柔軟性をユーザに提供しつつ、同時に実際にいかなるライセンスの種類を購入しようがユーザにその条件を維持させたいこともある。例えば、コンテンツ所有者は、販売したデジタル・コンテンツの再生を限定回数のみ、ある合計時間だけ、ある種の機械においてのみ、ある種のメディア・プレーヤにおいてのみ、ある種のユーザにのみ再生することを許可したい場合もある。

【0006】

20

しかしながら、販売を行なった後、このようなコンテンツ所有者は、デジタル・コンテンツの管理を行なうにしても、極僅かである。これは、特に、実際にあらゆる新製品または最新のパーソナル・コンピュータが、このようなデジタル・コンテンツの正確なデジタル・コピーを作成するため、ならびにこのような正確なデジタル・コピーを書き込み可能な磁気または光ディスクにダウンロードするため、またはこのような正確なコピーをあらゆる宛先にインターネットのようなネットワークを通じて送るために必要なソフトウェアおよびハードウェアを含んでいるという事実を考慮すると、問題である。

【0007】

勿論、ライセンス料が得られた場合法的処置の一部として、コンテンツ所有者はデジタル・コンテンツのユーザに、このようなデジタル・コンテンツの再配付をしないことを約束するように求めることはできる。しかしながら、このような約束は容易に行われ、容易に破られる。コンテンツ所有者は、大抵の場合暗号化および解読を伴う、いくつかの公知のセキュリティ・デバイスのいずれかによってこのような再配付を防止しようとすることもできる。しかしながら、決意の弱いユーザ（mildly determined user）に、暗号化デジタル・コンテンツを解読し、このようなデジタル・コンテンツを無暗号化形態で保存し、次いでこれを再配付する、ということを禁止できない場合が多い。

30

【0008】

したがって、デジタル・コンテンツの任意の形態のレンダリング即ち再生を管理可能にする実施アーキテクチャおよび方法を提供する必要性がある。この場合、管理は柔軟性があり、このようなデジタル・コンテンツのコンテンツ所有者によって定義可能とする。また、パーソナル・コンピュータのような計算機上においてレンダリング環境を管理する必要性もある。この場合、レンダリング環境は、このような実施アーキテクチャの少なくとも一部を含む。このようなレンダリング環境の管理によって、デジタル・コンテンツはコンテンツ所有者の制御下にはない計算機上でレンダリングされるものの、コンテンツ所有者が指定するようにのみデジタル・コンテンツをレンダリングすることが可能になる。

40

【0009】

更に、計算機上において信頼コンポーネント（trusted component）を走らせ、このような計算機のユーザがコンテンツ所有者が許可しない方法でこのようなデジタル・コンテンツにアクセスしようとしても、信頼コンポーネントがコンテンツ所有者の権利を、1片のデジタル・コンテンツに関してこのような計算機上で実施することも必要とされている。

50

単なる一例として、このような信頼ソフトウェア・コンポーネントは、計算機のユーザが、コンテンツ所有者が許可する場合を除いて、このようなデジタル・コンテンツのコピーを作成することを防止する。

(発明の概要)

前述の必要性は、少なくとも部分的にデジタル権利管理実施アーキテクチャおよび方法によって満たされる。このアーキテクチャおよび方法は、インターネット、光ディスク等において利用可能な保護(保証)デジタル・コンテンツにおいて権利を実施する。コンテンツを利用可能にするために、アーキテクチャは、コンテンツ・サーバを含み、ここからインターネット等を通じて暗号化した形態でデジタル・コンテンツにアクセス可能である。コンテンツ・サーバは、暗号化デジタル・コンテンツを供給し、光ディスク等に記録することも可能であり、暗号化デジタル・コンテンツは光ディスク自体で配付することもできる。コンテンツ・サーバでは、デジタル・コンテンツを暗号化鍵を用いて暗号化し、公開／秘密鍵技術を用いて、ユーザの計算機またはクライアント・マシン上でデジタル・コンテンツをデジタル・ライセンスと結び付ける。

10

【0010】

ユーザがデジタル・コンテンツを計算機上でレンダリングしようとする、レンダリング・アプリケーションが、このようなユーザの計算機上でデジタル権利管理(DRM)システムを呼び出す。ユーザが最初にデジタル・コンテンツをレンダリングしようとしている場合、DRMシステムはユーザをライセンス・サーバに差し向け、このようなデジタル・コンテンツをレンダリングするライセンスを、求められた態様で取得させるか、あるいはユーザ側では何の行為も必要とせずに、このようなライセンス・サーバからこのようなライセンスを透過的に取得する。ライセンスは以下を含む。

20

【0011】

ー暗号化デジタル・コンテンツを解読する解読鍵(KD)
ーライセンスおよび関連条件(開始日、終了日、再生回数等)によって与えられる権利(再生、コピー等)の記述。このような記述はデジタル的に読み取り可能な形態である。

【0012】

ーライセンスの保全を確保するデジタル署名
ユーザは、このようなライセンスをライセンス・サーバから取得しなければ、暗号化デジタル・コンテンツの解読やレンダリングを行なうことができない。取得したライセンスは、ユーザの計算機においてライセンス・ストアに格納される。

30

【0013】

重要なことは、ライセンス・サーバは「信頼」された(即ち、それ自体で認証可能な)DRMシステムにライセンスを発行するだけであるということである。「信頼」を築くために、DRMシステムには「ブラック・ボックス」が装備されており、これがこのようなDRMシステムのために解読および暗号化機能を実行する。ブラック・ボックスは、公開／秘密鍵対、バージョン番号、および一意の署名を含み、これらは全て承認された証明機関によって供給される。公開鍵は、発行されたライセンスの一部を暗号化する目的でライセンス・サーバに使用可能とされ、これによってこのようなライセンスをこのようなブラック・ボックスに結び付ける。秘密鍵は、対応する公開鍵で暗号化した情報を解読する目的のために、ブラック・ボックスにのみ使用可能であり、ユーザやその他の誰にも使用できない。最初に、DRMシステムには公開／秘密鍵対を有するブラック・ボックスが供給され、ユーザが最初にライセンスを要求するときに、更新した保証ブラック・ボックスをブラック・ボックス・サーバからダウンロードするようにユーザに促す。ブラック・ボックス・サーバは、一意の公開／秘密鍵対と共に、更新ブラック・ボックスを供給する。このような更新ブラック・ボックスは、一意の実行可能コードで書かれており、ユーザの計算機上でのみ走り、定期的に再更新される。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、そしてこのようなライセンス・サーバは、バージョン番号が現行であり署名が有効な場合、ライセンスを発行する。また、ライセンス要求は、ライセンスを要求する

40

50

デジタル・コンテンツの識別、および要求したデジタル・コンテンツに関連する解読鍵を識別する鍵 I D も含む。ライセンス・サーバは、ブラック・ボックス公開鍵を用いて解読鍵を暗号化し、解読鍵を用いてライセンス条件を暗号化し、次いで暗号化した解読鍵および暗号化したライセンス条件を、ライセンス署名と共に、ユーザの計算機にダウンロードする。

【0014】

一旦ダウンロードしたライセンスを D R M システムのライセンス・ストアに格納したなら、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おいて指定された権利にしたがって、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ると、ブラック・ボックスに解読鍵およびライセンス条件を解読させ、D R M システムのライセンス評価部がこのようなライセンス条件を評価する。ブラック・ボックスは、ライセンスの評価の結果、要求元にこのようなコンテンツを再生することを許可すると判断した場合にのみ、暗号化デジタル・コンテンツを解読する。解読したコンテンツは、レンダリング・アプリケーションに供給され、レンダリングが行われる。

(図面の簡単な説明)

前述の概要、および以下の本発明の実施形態の更に詳細な説明は、添付図面と関連付けて読むことにより、一層理解が深まるであろう。本発明を例示する目的のために、現在好適な実施形態を図面に示す。しかしながら、当然理解されるであろうが、本発明は図示する構成や手段そのものに限定される訳ではない。

(発明の詳細な説明)

図面を詳細に参照すると、全体を通じて同様のエレメントを示すために同様の番号が用いられている。図 1 には、本発明の一実施形態による実施アーキテクチャ 10 を示す。概略的に、実施アーキテクチャ 10 は、デジタル・コンテンツ 12 の所有者にライセンス規則を指定させ、このライセンス規則を満たさなければ、ユーザの計算機 14 上でこのようなデジタル・コンテンツ 12 をレンダリングすることが許可されない。このようなライセンス規則は、デジタル・ライセンス 16 に具体化され、ユーザ／ユーザの計算機 14 (以後、このような用語は、特に状況が必要としない限り、相互交換可能とする) は、コンテンツ所有者またはその代理人から取得しなければならない。デジタル・コンテンツ 12 は、暗号化した形態で配付され、自由に広く配付することもできる。好ましくは、デジタル・コンテンツ 12 を解読するための解読鍵 (K D) をライセンス 16 と共に含ませる。

計算機環境

図 1 2 および以下の論述は、本発明を実現するのに適した計算機環境の端的な一般的な説明を行なうことを意図している。必ずしもその必要はないが、本発明の説明は、少なくとも部分的には、プログラム・モジュールのような、クライアント・ワークステーションまたはサーバのようなコンピュータが実行する一般的なコンピュータ実行可能命令に関連して行なう。一般に、プログラム・モジュールは、ルーチン・プログラム、オブジェクト、コンポーネント、データ構造等を含み、特定のタスクを実行したり、あるいは特定の抽象的データ・タイプを実装する。更に、本発明およびその一部は、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系電子機器またはプログラマブル消費者電子機器、ネットワーク P C、ミニコンピュータ、メインフレーム・コンピュータ等を含む、別のコンピュータ・システム構成でも実施可能であることも認めよう。また、本発明は、分散型計算機環境においても実施可能であり、この場合、通信ネットワークを通じてリンクされたりリモート処理デバイスによってタスクを実行する。分散型計算機環境では、プログラム・モジュールは、ローカルおよびリモート・メモリ記憶装置双方に位置することができる。

【0015】

図 1 2 に示すように、本発明を実現する汎用計算機システムの一例は、従来のパーソナル・コンピュータ 120 等を含む。このパーソナル・コンピュータ 120 は、演算装置 121、システム・メモリ 122、およびシステム・メモリから演算装置 121 までを含む

種々のシステム・コンポーネントを結合するシステム・バス123を含む。システム・バス123は、数種類のバス構造のいずれでもよく、メモリ・バスまたはメモリ・コントローラ、周辺バス、および種々のバス構造のいずれかをを用いてローカル・バスが含まれる。システム・メモリは、リード・オンリ・メモリ（ROM）124およびランダム・アクセス・メモリ（RAM）125を含む。基本入出力システム126（BIOS）は、起動中のように、パーソナル・コンピュータ120内のエレメント間におけるデータ転送を補助する基本的なルーティンを含み、ROM124内に格納されている。

【0016】

更に、パーソナル・コンピュータ120は、図示しないハード・ディスクの読み書きを行なうハード・ディスク・ドライブ127、リムーバブル磁気ディスク129の読み書きを行なう磁気ディスク・ドライブ128、CD-ROMまたはその他の光媒体のようなリムーバブル光ディスク131の読み書きを行なう光ディスク・ドライブ130のような種々の周辺ハードウェア・デバイスも含む。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を介して、システム・バス123に接続されている。ドライブおよびそれに関連するコンピュータ読取可能媒体は、コンピュータ読取可能命令、データ構造、プログラム・モジュールおよびパーソナル・コンピュータ20のその他のデータの不揮発性格納を行なう。

【0017】

ここに記載する環境の一例は、ハード・ディスク、リムーバブル磁気ディスク129およびリムーバブル光ディスク131を採用するが、コンピュータによるアクセスが可能なデータを格納することができる、別の形式のコンピュータ読取可能媒体も、動作環境例では使用可能であることは、当業者には認められよう。このような他の形式の媒体は、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）、リード・オンリ・メモリ（ROM）等を含む。

【0018】

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上には、多数のプログラム・モジュールを格納可能であり、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、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を含む。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のような入力デバイスによって、コマンドおよび情報をパーソナル・コンピュータ20に入力することができる。他の入力デバイス（図示せず）は、マイクロフォン、ジョイスティック、ゲーム・パッド、衛星ディッシュ、スキャナ等を含むことができる。これらおよびその他の入力デバイスは、多くの場合、システム・バスに結合するシリアル・ポート・インターフェース146を介して、演算装置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（USB）のようなその他のインターフェースによって接続することも可能である。また、ビデオ・アダプタ148のような周辺ハードウェア・インターフェース・デバイスを介して、モニタ147またはその他の種類のディスプレイ装置もシステム・バス123に接続してある。モニタ147に加えて、パーソナル・コンピュータは、典型的に、スピーカおよびプリンタのような、その他の周辺出力デバイス（図示せず）を含む。図12のシステム例は、ホスト・アダプタ155、小型コンピュータ・システム・インターフェース（SCSI）バス156、およびSCSIバス156に接続されている外部記憶装置162も含む。

【0019】

パーソナル・コンピュータ120は、リモート・コンピュータ149のような1つ以上のリモート・コンピュータへの論理接続を用いれば、ネットワーク環境においても動作可能である。リモート・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

10

20

30

40

50

ータ、ネットワーク P C、ピア・デバイス、またはその他の共通ネットワーク・ノードとすることができ、典型的に、パーソナル・コンピュータ 1 2 0 に関して先に述べたエレメントの多くまたは全てを含むが、図 1 2 にはメモリ記憶装置 1 5 0 のみを図示している。図 1 2 に示す論理接続は、ローカル・エリア・ネットワーク (LAN) 1 5 1 およびワイド・エリア・ネットワーク (WAN) 1 5 2 を含む。このようなネットワーク環境は、会社全域に及ぶコンピュータ・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である。

【0 0 2 0】

LAN ネットワーク環境で用いる場合、パーソナル・コンピュータ 1 2 0 は、ネットワーク・インターフェースまたはアダプタ 1 5 3 を介してローカル・ネットワーク 1 5 1 に接続する。WAN ネットワーク環境で用いる場合、パーソナル・コンピュータ 1 2 0 は、典型的に、モデム 1 5 4、またはインターネットのようなワイド・エリア・ネットワーク 5 2 を通じて通信を確立する、その他の手段を含む。モデム 1 5 4 は、内蔵型でも外付けでもよく、シリアル・ポート・インターフェース 1 4 6 を介してシステム・バス 1 2 3 に接続する。ネットワーク環境では、パーソナル・コンピュータ 1 2 0 に関して図示したプログラム・モジュールまたはその一部は、ローカルまたはリモートメモリ記憶装置に格納することもできる。尚、図示のネットワーク接続は一例であり、コンピュータ間に通信リンクを確立する別の手段も使用可能であることは認められよう。

アーキテクチャ

再度図 1 を参照すると、本発明の一実施形態において、アーキテクチャ 1 0 は、前述のユーザの計算機 1 4 だけでなく、オーサリング・ツール 1 8、コンテンツ鍵データベース 2 0、コンテンツ・サーバ 2 2、ライセンス・サーバ 2 4、およびブラック・ボックス・サーバ 2 5 を含む。

アーキテクチャ・オーサリング・ツール 1 8

オーサリング・ツール 1 8 は、コンテンツ所有者が 1 片のデジタル・コンテンツ 1 2 を、本発明のアーキテクチャ 1 0 と共に使用可能な形態にパッケージ化するために用いられる。即ち、コンテンツ所有者は、オーサリング・ツール 1 8 に、デジタル・コンテンツ 1 2、ならびに当該デジタル・コンテンツ 1 2 に付随する命令および／または規則、ならびにデジタル・コンテンツ 1 2 をどのようにパッケージ化するかに関する命令および／または規則を供給する。すると、オーサリング・ツール 1 8 は、暗号化／解読鍵にしたがって暗号化したデジタル・コンテンツ 1 2、およびデジタル・コンテンツ 1 2 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 1 2 p を生成する。

【0 0 2 1】

本発明の一実施形態では、オーサリング・ツール 1 8 は、いくつかの異なるデジタル・コンテンツ 1 2 のパッケージ 1 2 p を連続して生成するように命令され、その各々が、異なる暗号化／解読鍵にしたがって暗号化された同じデジタル・コンテンツを有する。当然理解されようが、デジタル・コンテンツ 1 2 が同じである数個の異なるパッケージ 1 2 p を有することは、このようなパッケージ 1 2 p／コンテンツ 1 2 (以後、特に状況が必要としない限り、単に「デジタル・コンテンツ 1 2」) の配付を追跡する際に有用となり得る。このような配付追跡は、通常は必要でないが、デジタル・コンテンツ 1 2 が不法に販売または放送された場合には、調査機関が用いることができる。

【0 0 2 2】

本発明の一実施形態では、デジタル・コンテンツ 1 2 を暗号化する暗号化／解読鍵は、対称鍵であり、暗号化鍵が解読鍵 (K D) にもなる。以下で更に詳しく論ずるが、このような解読鍵 (K D) は、このようなデジタル・コンテンツ 1 2 のライセンス 1 6 の一部として、隠された形態でユーザの計算機 1 4 に配信される。好ましくは、各デジタル・コンテンツ 1 2 片には、コンテンツ I D が備えられており (または、各パッケージ 1 2 p にはパッケージ I D が備えられており)、各解読鍵 (K D) は鍵 I D を有し、オーサリング・ツール 1 8 によって、各デジタル・コンテンツ 1 2 片毎に (または各パッケージ 1 2 p 毎に) 解読鍵 (k D)、鍵 I D、およびコンテンツ I D (またはパッケージ I D) を鍵コンテ

ンツ・データベース 20 に格納する。加えて、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 の種類、ならびにライセンス 16 の各種類に対する条件 (terms and conditions) に関するライセンス・データも、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) に格納することができる。好ましくは、ライセンス・データは、後に、状況およびマーケット条件の要求に応じて、コンテンツ所有者によって変更することができる。

【0023】

使用においては、オーサリング・ツール 18 には、とりわけ、次の項目を含む情報が供給される。

ーパッケージ化するデジタル・コンテンツ 12

10

ー必要であれば、用いる透かしおよび／または指紋の形式およびパラメータ、

ー必要であれば、用いるデータ圧縮の形式およびパラメータ、

ー用いる暗号化の形式およびパラメータ、

ー必要であれば、用いるシリアル化の形式およびパラメータ、および

ーデジタル・コンテンツ 12 に伴う命令および／または規則。

【0024】

公知のように、透かしとは、隠されたコンピュータ読み取り可能信号であり、識別子としてデジタル・コンテンツ 12 に追加される。指紋とは、各インスタンス毎に異なる透かしのことである。当然理解されようが、インスタンスとは、一意であるデジタル・コンテンツ 12 のバージョンである。いずれのインスタンスでも、そのコピーを多数作成することができ、いずれのコピーも特定のインスタンスを有する。デジタル・コンテンツ 12 の特定のインスタンスが不法に販売または放送された場合、調査機関は、このようなデジタル・コンテンツ 12 に付加されている透かし／指紋にしたがって十中八九容疑者を特定することができる。

20

【0025】

データ圧縮は、本発明の精神および範囲から逸脱することなく、適切な圧縮アルゴリズムであればそのいずれにしたがって実施することも可能である。例えば、. mp3 または、wav 圧縮アルゴリズムを用いることができる。勿論、デジタル・コンテンツ 12 は、既に圧縮状態であってもよく、この場合追加の圧縮は不要である。

【0026】

30

デジタル・コンテンツ 12 に伴うべき命令／および規則は、實際上、本発明の精神および範囲から逸脱することなく、適切であればあらゆる命令、規則、またはその他の情報を含むことができる。以下で論ずるが、このような付随する命令／規則／情報は、主にユーザおよびユーザの計算機 14 によって、ライセンス 16 を取得し、デジタル・コンテンツ 12 をレンダリングするために用いられる。したがって、このような付随命令／規則／情報は、適切にフォーマットされたライセンス取得スクリプト等を含むことができる。これについては、以下で更に詳しく説明する。加えて、または代わりに、このような付随命令／規則／情報は、デジタル・コンテンツ 12 のプレビューをユーザに与えるように設計した、「プレビュー」情報を含むこともできる。

【0027】

40

次に、供給された情報を用いて、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 つ以上のパッケージ 12 p を生成する。各パッケージ 12 p は、次に、コンテンツ・サーバ 2 に格納され、世界中に配付される。

【0028】

本発明の一実施形態において、図 2 をここで参照すると、オーサリング・ツール 18 は、ダイナミック・オーサリング・ツール 18 であり、入力パラメータを受け取る。これらは、オーサリング・ツール 18 上で指定し、動作させることができる。したがって、このようなオーサリング・ツール 18 は、多数片のデジタル・コンテンツ 12 に対して、パッケージ 12 p の多数の変形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、図示のように、辞書 28 の形態で具体化する。ここで、辞書 28 は、以下のようなパラ

50

メータを含む。

【0029】

ーデジタル・コンテンツ12を有する入力ファイル29aの名称、
ー行われるエンコードの形式、
ー用いる暗号化／解読鍵(KD)、
ーパッケージ12p内にデジタル・コンテンツ12と共にパッケージ化する付随命令／規則／情報(「ヘッダ情報」)、
ー行なわれる多重化(muxing)の形式、および
ーデジタル・コンテンツ12に基づくパッケージ12pを書き込む出力ファイル29bの名称。

10

【0030】

当然理解されようが、このような辞書28は、オーサリング・ツール18のオペレータ(人間または機械)によって容易にかつ素早く変更可能であり、しがって、オーサリング・ツール18によって実行するオーサリングの形式も、容易にかつ素早く、動的に変更可能である。本発明の一実施形態では、オーサリング・ツール18は、コンピュータ画面上において人のオペレータに閲覧可能なオペレータ・インターフェース(図示せず)を含む。したがって、このようなオペレータは、インターフェースを通じて辞書28を変更することができ、更にインターフェースによる辞書28の変更を適切に補助したり、あるいは規制することも可能である。

20

【0031】

オーサリング・ツール18では、図2に見られるように、ソース・ファイル18aは、辞書28からデジタル・コンテンツ12を有する入力ファイル29aの名称を検索し、RAMのようなメモリ29cにデジタル・コンテンツ12を置く。エンコード・フィルタ18bは、次に、メモリ29c内のデジタル・コンテンツ12に対してエンコードを行い、入力フォーマットから、辞書28において指定されているエンコード形式に応じた出力フォーマット(即ち、.wavから.asp、.mp3から.asp.等)にファイルを転送し、エンコードしたデジタル・コンテンツ12をメモリ29c内に置く。図示のように、パッケージ化するデジタル・コンテンツ12(例えば、音楽)は、.wavまたは.mp3フォーマットのような圧縮フォーマットで受け取られ、.asp(アクティブ・ストリーミング・プロトコル)フォーマットのようなフォーマットに変換される。勿論、その他の入力および出力フォーマットも採用でき、本発明の精神および範囲から逸脱する訳ではない。

30

【0032】

その後、暗号化フィルタ18cがメモリ29c内のエンコード・デジタル・コンテンツ12を、辞書28において指定されている暗号化／解読鍵(KD)にしたがって暗号化し、暗号化したデジタル・コンテンツ12をメモリ29c内に置く。次に、ヘッダ・フィルタ18dが、辞書28において指定されているヘッダ情報を、メモリ29c内の暗号化デジタル・コンテンツ12に追加する。

【0033】

当然理解されようが、状況に応じて、パッケージ12pは、時間的に整合したデジタル・コンテンツ12の多数のストリームを含む場合もある(1つのストリームを図2に示す)。このような多数のストリームは多重化されている(即ち「muxed」)。したがって、多重化フィルタ18eは、辞書28において指定されている多重化形式にしたがって、メモリ29c内のヘッダ情報および暗号化デジタル・コンテンツ12の多重化を行い、その結果をメモリ29cに置く。次に、ファイル書き込みフィルタ18fが、メモリ29cからこの結果を検索し、このような結果を、パッケージ12pとして辞書28に指定されている出力ファイル29bに書き込む。

40

【0034】

尚、ある状況においては、実行するエンコードの形式は通常では変更しないことを注記しておく。多重化形式は典型的にエンコード形式に基づくので、多重化形式も通常では同様

50

に変更しない。実際にそういう場合には、辞書 28 は、エンコード形式および多重化形式に関するパラメータを含む必要はない。代わりに、エンコード形式をエンコード・フィルタに「ハードワイヤ」し、あるいは多重化形式を多重化フィルタに「ハードワイヤ」するだけでよい。勿論、状況が要求する場合には、オーサリング・ツール 18 は前述のフィルタ全てを含まなくてもよく、あるいは他のフィルタを含んでもよく、含んだフィルタは、ハードワイヤにしても、辞書 28 内で指定されているパラメータにしたがってその機能を実行してもよく、全て本発明の精神および範囲から逸脱することはない。

【0035】

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によって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような計算機およびこの

10

アーキテクチャーコンテンツ・サーバ 22

再度図 1 を参照すると、本発明の一実施形態において、コンテンツ・サーバ 22 は、オーサリングツール 18 が生成したパッケージを配布するか、またはその他の方法で検索できるようにする。このようなパッケージ 12 p は、適切な配布チャネルのいずれかを通じて、コンテンツ・サーバ 22 の要求に応じて配布することができ、本発明の精神および範囲から逸脱することはない。例えば、このような配布チャネルは、インターネットまたはその他のネットワーク、電子掲示板、電子メール等とすることもできる。加えて、コンテンツ・サーバ 22 を用いて、パッケージ 12 p を磁気または光ディスクあるいはその他の記憶装置にコピーすることもでき、このような記憶装置を配付してもよい。

20

【0036】

尚、コンテンツ・サーバ 22 は、いずれの信頼またはセキュリティ問題にも関係なく、パッケージを配布することは認められよう。以下で論ずるが、このような問題は、ライセンス・サーバ 24 およびこのようなライセンス・サーバ 24 とユーザの計算機 14 との間の関係と関連付けて扱われる。本発明の一実施形態では、コンテンツ・サーバ 22 は自由に、デジタル・コンテンツ 12 を有するパッケージ 12 p を、これを要求するあらゆる配布先にリリースし、配布する。しかしながら、コンテンツ・サーバ 22 は、このようなパッケージ 12 p のリリースおよび配布に制約を設けることもでき、本発明の精神および範囲から逸脱する訳ではない。例えば、コンテンツ・サーバ 22 は、配布前に、所定の配布料の

30

支払を最初に要求することもでき、あるいは配布先にそれ自体を同定することを要求することもでき、あるいは配布先の識別に基づいて配布を行なうか否か実際に判断することもできる。

【0037】

加えて、コンテンツ・サーバ 22 を用いて、オーサリング・ツール 18 を制御することによって在庫管理を行い、予めある数の異なるパッケージ 12 p を生成し、予測される需要を満たすようにすることもできる。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 12 p を生成し、各パッケージ 12 p を 10 回送達することもできる。パッケージ 12 p の供給が例えば、20 に減少すると、コンテンツ・サーバ 22 はオーサリング・ツール 18 に、例えば、80 個の追加パッケージ 12 p を再度生成するように指令することもできる。

40

【0038】

好ましくは、アーキテクチャ 10 内のコンテンツ・サーバ 22 は、一意の公開／秘密鍵対 (P U - C S, P R - C S) を有し、これをライセンス 16 を評価し、対応するデジタル・コンテンツ 12 を解読するための解読鍵 (K D) を取得するプロセスの一部として採用する。これについては、以下で更に詳しく説明する。公知のように、公開／秘密鍵対は非対称鍵であり、鍵対における鍵の一方で暗号化されるものは、鍵対における鍵の他方を用いなければ解読することができない。公開／秘密鍵対暗号化システムでは、公開鍵は世界中に知らせることができるが、秘密鍵は、このような秘密鍵の所有者によって常に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 (P

50

R-C S) でデータを暗号化する場合、解読の目的のためにその公開鍵 (P U-C S) と共に、暗号化したデータを世界に送ることができる。対応して、外部デバイスがデータをコンテンツ・サーバ 2 2 に送り、このようなコンテンツ・サーバ 2 2 のみがこのようなデータを解読するようにしたい場合、このような外部デバイスは最初にコンテンツ・サーバ 2 2 の公開鍵 (P U-C S) を取得し、次いでこのような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、コンテンツ・サーバ 2 2 (そして、コンテンツ・サーバ 2 2 のみ) がその秘密鍵 (P R-C S) を用いて、このような暗号化データを解読することができる。

【0039】

オーサリング・ツール 1 8 の場合と同様、コンテンツ・サーバ 2 2 は、適切なソフトウェアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウェアの構造および動作は、ここの開示に基づいて明らかであるので、本開示では詳細な説明は全く必要ない。更に、本発明の一実施形態では、オーサリング・ツール 1 8 およびコンテンツ・サーバ 2 2 は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。更に、コンテンツ・サーバ 2 2 は、ある状況によっては、オーサリング・ツール 1 8 を含み、先に論じたように、オーサリング・ツール 1 8 の機能を実行する場合もあることは認められよう。

デジタル・コンテンツ・パッケージ 1 2 p の構造

次に図 3 を参照すると、本発明の一実施形態において、コンテンツ・サーバ 2 2 によって配布されるデジタル・コンテンツ・パッケージ 1 2 p は次を含む。

【0040】

- 先に論じたように暗号化／解読鍵 (K D) を用いて暗号化されたデジタル・コンテンツ (即ち、(K D (C O N T E N T)))、
- このようなデジタル・コンテンツ 1 2 (またはパッケージ 1 2 p) のコンテンツ I D (またはパッケージ I D)、
- 解読鍵 (K D) の鍵 I D、
- 好ましくは無暗号化形態のライセンス取得情報、および
- コンテンツ・サーバ 2 2 の秘密鍵 (P R-C S) によって署名された、コンテンツ・サーバ 2 2 の公開鍵 (P U-C S) を暗号化する鍵 K D (即ち、(K D (P U-C S) S (P R-C S)))。

【0041】

(K D (P U-C S) S (P R-C S)) に関して、このような項目は、デジタル・コンテンツ 1 2 および／またはパッケージ 1 2 p の妥当性検査に関係して用いられることは理解されよう。これについては以下で説明する。デジタル署名を有する認証 (以下を参照のこと) とは異なり、鍵 (P U-C S) は (K D (P U-C S)) を取得するには必要ではない。代わりに、鍵 (P U-C S) は、単に解読鍵 (K D) を適用するだけで取得される。一旦こうして取得すれば、このような鍵 (P U-C S) は、署名 (S (P R-C S)) の有効性を検査するために用いることができる。

【0042】

また、このようにオーサリング・ツール 1 8 によって構築されるパッケージ 1 2 p に対して、このようなオーサリング・ツール 1 8 は、恐らくは辞書 2 8 から供給されるヘッダ情報として、既にライセンス取得情報および (K D (P U-C S) S (P R-C S)) を所持していなければならない。更に、オーサリング・ツール 1 8 およびコンテンツ・サーバ 2 2 は、恐らくは (K D (P U-C S) S (P R-C S)) を構築するために相互作用を行わなければならない。このような相互作用は、例えば、次のステップを含む。

【0043】

- コンテンツ・サーバ 2 2 が (P U-C S) をオーサリング・ツール 1 8 に送る。
- オーサリング・ツール 1 8 が (K D) を用いて (P U-C S) を暗号化し、(K D (P U-C S)) を生成する。

【0044】

ーオーサリング・ツール18が(KD(PU-CS))をコンテンツ・サーバ22に送る。
ーコンテンツ・サーバ22が(PR-CS)を用いて(KD(PU-CS))に署名し、(KD(PU-CS)S(PR-CS))を生成する。

【0045】

ーコンテンツ・サーバ22が(KD(PU-CS)S(PR-CS))をオーサリング・ツール18に送る。

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において、ライセンス・サーバ24は、1片のデジタル・コンテンツ12に関して、ユーザの計算機14からライセンス16の要求を受信し、ユーザの計算機14が、発行するライセンス16を授かることについて信用できるか否か判定を行い、このようなライセンス16を交渉し、このようなライセンス16を作成し、このようなライセンス16をユーザの計算機14に送る機能を実行する。好ましくは、このように送信されるライセンス16は、デジタル・コンテンツ12を解読するための解読鍵(KD)を含む。このようなライセンス・サーバ24およびこのような機能については、以下で更に詳しく説明する。好ましくは、そしてコンテンツ・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、一意の公開／秘密鍵対(PU-LS, PR-LS)を有し、ライセンス16を評価するプロセスの一部としてこれを用い、対応するデジタル・コンテンツ12を解読するための解読鍵(KD)を取得する。これについては、以下で更に詳しく説明する。

【0046】

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、ライセンス・サーバ24は、適切なソフトウェアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウェアの構造および動作は、ここの開示に基づいて明らかなはずであり、本開示においては詳細な論述は全く不要である。更に、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は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。

【0047】

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およびコンテンツ・サーバ22は、代理契約等を行い、ライセンス・サーバ24が実際に、コンテンツ・サーバ22が配布するデジタル・コンテンツ12の少なくとも一部について、ライセンス付与機関(licensing authority)であることに同意する。当然理解されようが、1つのコンテンツ・サーバ22は、数個のライセンス・サーバ24と代理契約を結ぶことができ、あるいは1つのライセンス・サーバ24が数個のコンテンツ・サーバ22と代理契約を結ぶこともでき、いずれも本発明の精神および範囲から逸脱する訳ではない。

【0048】

好ましくは、ライセンス・サーバ24は、実際にそれがコンテンツ・サーバ22によって配布するデジタル・コンテンツ12のライセンス16を発行する代理権を有することを世界に示すことができる。こうすることによって、ライセンス・サーバ24は、コンテンツ・サーバ22に、ライセンス・サーバ24の公開鍵(PU-LS)を送り、そしてコンテンツ・サーバ22はライセンス・サーバ24に、コンテンツ・サーバ22の秘密鍵(CERT(PU-LS)S(PR-CS))によって署名したコンテンツとして、PU-LSを含むデジタル認証を送ることが好ましい。当然理解されようが、このような認証におけるコンテンツ(PU-LS)は、コンテンツ・サーバ22の公開鍵(PR-CS)を用いなければ、アクセスすることはできない。当然理解されようが、一般には、基礎となるデータのデジタル署名は、このようなデータの暗号化形態であり、このようなデータが偽造されていたり、あるいはその他の方法で変更されている場合、解読の際にこのようなデー

タと一致しない。

【0049】

1 片のデジタル・コンテンツ 1 2 に関連するライセンス代理権として、そしてライセンス付与機能の一部として、ライセンス・サーバ 2 4 は、このようなデジタル・コンテンツ 1 2 のための解読鍵 (K D) にアクセスできなければならない。したがって、ライセンス・サーバ 2 4 は、このようなデジタル・コンテンツ 1 2 (またはパッケージ 1 2 p) に対する解読鍵 (K D)、鍵 I D、およびコンテンツ I D (またはパッケージ I D) を有するコンテンツ鍵データベース 2 0 にアクセスできることが好ましい。

アーキテクチャブラック・ボックス・サーバ 2 6

更に図 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 2 6 は、ユーザの計算機 1 4 において、新たなブラック・ボックス 3 0 をインストールし、アップデートする機能を実行する。以下で更に詳しく説明するが、ブラック・ボックス 3 0 は、ユーザの計算機 1 4 のために、暗号化および解読機能を実行する。また、以下で更に詳しく説明するが、ブラック・ボックス 3 0 は、安全であり攻撃から保護されることを想定している。このような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 3 0 を、必要に応じてブラック・ボックス・サーバ 2 6 によって新たなバージョンにアップグレードすることによって得られる。これについては、以下で更に詳しく説明する。

【0050】

オーサリング・ツール 1 8、コンテンツ・サーバ 2 2、およびライセンス・サーバ 2 4 の場合と同様、ブラック・ボックス・サーバ 2 6 は、適切なソフトウェアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウェアの構造および動作は、ここの開示に基づいて明らかではなく、したがって本開示では詳細な論述は不要である。更に、本発明の一実施形態では、ライセンス・サーバ 2 4、オーサリング・ツール 1 8、および／またはコンテンツ・サーバ 2 2 は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。しかし、セキュリティの目的上、ブラック・ボックス・サーバ 2 6 を別個の機械に有する方が賢明であることを注記しておく。

アーキテクチャユーザの計算機 1 4

次に図 4 を参照すると、本発明の一実施形態では、ユーザの計算機 1 4 は、パーソナル・コンピュータ等であり、キーボード、マウス、画面、プロセッサ、RAM、ROM、ハード・ドライブ、フロッピー・ドライブ、CD プレーヤ等のようなエレメントを有する。しかしながら、ユーザの計算機 1 4 は、とりわけ、テレビジョンまたはモニタのような専用閲覧デバイス、ステレオまたはその他の音楽プレーヤのような専用オーディオ・デバイス、専用プリンタ等でもよく、本発明の精神および範囲から逸脱することはない。

【0051】

1 片のデジタル・コンテンツ 1 2 のコンテンツ所有者は、ユーザの計算機 1 4 が、このようなコンテンツ所有者が指定した規則を固守すること、即ち、求められた態様でレンダリングを許可するライセンス 1 6 をユーザが取得しなければ、デジタル・コンテンツ 1 2 をレンダリングしないことを信用しなければならない。好ましくは、ユーザの計算機 1 4 は、このような計算機 1 4 が、デジタル・コンテンツ 1 2 に関連しユーザによって取得されたライセンス 1 6 に具体化されているライセンス規則にしたがってでなければ、デジタル・コンテンツ 1 2 をレンダリングしないことを、コンテンツ所有者に対して履行することができる、信頼 (trusted) コンポーネントまたは機構 3 2 を備えなければならない。

【0052】

ここで、信頼機構 3 2 は、デジタル権利管理 (DRM) システム 3 2 であり、ユーザが 1 片のデジタル・コンテンツ 1 2 をレンダリングすることを要求したときにイネーブルされ、ユーザが、求められた態様でデジタル・コンテンツ 1 2 をレンダリングするライセンス 1 6 を有するか否かを判定を行い、必要であれば、このようなライセンス 1 6 の取得を実施し、ライセンス 1 6 にしたがってユーザがデジタル・コンテンツ 1 2 を再生する権利を有するか否かを判定を行い、実際にユーザがこのようなライセンス 1 6 に応じてこのような権

利を有する場合、レンダリングの目的で、デジタル・コンテンツ 12 を解読する。ユーザの計算機 14 上での DRM システム 32 の内容および機能、およびアーキテクチャ 10 との関係について、以下に説明する。

DRM システム 32

DRM システム 32 は、ここに開示するアーキテクチャ 10 と共に 4 つの主要な機能を実行する。(1) コンテンツの取得、(2) ライセンスの取得、(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／更新である。好ましくは、これらの機能のいずれもいつの時点でも実行することができるが、これらの機能の一部は、デジタル・コンテンツ 12 が既に取得されていることを要件とすることは認められよう。

10

DRM システム 32 - コンテンツ取得

ユーザおよび／またはユーザの計算機 14 によるデジタル・コンテンツ 12 の取得は、典型的に、比較的単純であり、概略的には、暗号化デジタル・コンテンツ 12 を有するファイルを、ユーザの計算機 14 上に置くことから成る。勿論、ここに開示するアーキテクチャ 10 および DRM システム 32 と共に動作するためには、暗号化デジタル・コンテンツ 12 が、デジタル・パッケージ 12 p のように、このようなアーキテクチャ 10 および DRM システム 32 に適した形態であることが必要である。これについては以下で説明する。

【0053】

当然理解されようが、デジタル・コンテンツ 12 は、コンテンツ・サーバ 22 から直接的にまたは間接的に、いずれの方法でも取得可能であり、本発明の精神および範囲から逸脱することはない。例えば、このようなデジタル・コンテンツ 12 は、インターネットのようなネットワークからダウンロードしたり、取得した光または磁気ディスク等に配したり、電子メール・メッセージ等の一部として受信したり、あるいは電子掲示板等からダウンロードすることができる。

20

【0054】

このようなデジタル・コンテンツ 12 は、一旦取得すると、計算機 14 上で走るレンダリング・アプリケーション 34 (以下で説明する)、および DRM システム 32 によって、取得したデジタル・コンテンツ 12 がアクセス可能となるように、格納することが好ましい。例えば、デジタル・コンテンツ 12 は、ユーザの計算機 14 のハード・ドライブ (図示せず) 上、または計算機 14 に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置くこともできる。デジタル・コンテンツ 12 を光または磁気ディスク等に取得する場合、このようなディスクを、ユーザの計算機 14 に結合されている適切なドライブ (図示せず) に装填するだけでよい。

30

【0055】

本発明では、直接配布源としてのコンテンツ・サーバ 22 からでも、また間接配布源としてのなんらかの仲介物からでも、デジタル・コンテンツ 12 を取得するために特殊なツールを全く必要としないことを想定している。即ち、デジタル・コンテンツ 12 は、他のあらゆるデータ・ファイルと同様に容易に取得することが好ましい。しかしながら、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 を取得するのを助けるように設計したインターフェース (図示せず) を含むこともできる。例えば、インターフェースは、デジタル・コンテンツ 12 を探索するように特別に設計したウェブ・ブラウザを含むことができ、デジタル・コンテンツ 12 のソースであることがわかっている既定のインターネット・ウェブ・サイト等にリンクする。

40

DRM システム 32 - コンテンツ・レンダリング、第 1 部

図 5 A を参照すると、本発明の一実施形態では、暗号化デジタル・コンテンツ 12 が配布され、ユーザによって受信され、ユーザによって格納ファイルの形態で計算機 14 上に置かれていると仮定し、ユーザは、レンダリング・コマンド上である変形 (variation) を実行することによって、デジタル・コンテンツ 12 をレンダリングしようとする (ステッ

50

プ501)。例えば、こ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」または「開く」要求として具体化することができる。計算機環境によっては、例えば、ワシントン州RedmondのMICROSOFT Corporationが販売する"MICROSOFT WINDOWS（登録商標）"オペレーティング・システムのように、このような再生またはオープン・コマンドは、デジタル・コンテンツ12を表わすアイコン上で「クリック」することと同じ位簡単にすることができる。勿論、このようなレンダリング・コマンドのその他の実施形態も採用可能であり、本発明の精神および範囲から逸脱する訳ではない。一般に、このようなレンダリング・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か、走らせるか、実行する等を指令するときにはいつでも実行するように考慮することができる。

10

【0056】

重要なことは、そして付加的に、こ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、印刷形態、視覚形態、聴覚形態等のような別の形態にコピーする要求として具体化できることにある。当然理解されようが、同じデジタル・コンテンツ12を、コンピュータ画面上におけるように、1つの形態でレンダリングし、次いで印刷文書のように別の形態でレンダリングすることもできる。本発明では、各レンダリング形式は、ユーザがそうする権利を有する場合にのみ実行される。これについては以下で説明する。

【0057】

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・ファイルの形態であり、計算機14は、このような拡張子に基づいて、特定の種類のレンダリング・アプリケーション34を実行することを決定することができる。例えば、ファイル名拡張子が、デジタル・コンテンツ12はテキスト・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RedmondのMICROSOFT Corporationが販売する"MICROSOFT WORD"のようなワード・プロセッサの何らかの形態となる。同様に、ファイル名拡張子が、デジタル・コンテンツ12はオーディオ、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す場合、レンダリング・アプリケーション34は、同様にワシントン州RedmondのMICROSOFT Corporationが販売する"MICROSOFT MEDIA PLAYER"のような、マルチメディア・プレーヤの何らかの形態となる。

20

【0058】

勿論、レンダリング・アプリケーションを決定する他の方法も採用することができ、本発明の精神および範囲から逸脱する訳ではない。一例としてに過ぎないが、デジタル・コンテンツ12は、無暗号化形態のメタデータ（前述のヘッダ情報）を含むこともでき、この場合、メタデータは、このようなデジタル・コンテンツ12をレンダリングするために必要なレンダリング・アプリケーション34の形式に関する情報を含む。

30

【0059】

好ましくは、このようなレンダリング・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を試験し、このようなデジタル・コンテンツ12が権利保護形態で暗号化されているか否か判定を行なう（ステップ503、505）。保護されていない場合、これ以上の面倒なく、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、暗号化デジタル・コンテンツ12から、このようなデジタル・コンテンツ12を再生するためにDRMシステム32が必要か否か判定を行なう。これに応じて、このようなレンダリング・アプリケーション34は、ユーザの計算機14に、DRMシステム32をその上で走らせるように指令する（ステップ509）。次に、このようなレンダリング・アプリケーション34はこのようなDRMシステム32をコールし、デジタル・コンテンツ12を解読する（ステップ511）。以下で更に詳しく論ずるが、DRMシステム32は、実際には、ユーザがこのようなデジタル・コンテンツ12に対する有効なライセンス16、および有効なライセンス16におけるライセンス規則にしたがってデジタル・コンテンツ12を再生する権利を有する場合にのみ、デジタル・コンテンツ12を解読する。好ましくは、一旦DRMシステム32がレンダリング・アプリケーション34によってコールさ

40

50

れた場合、このようなDRMシステム32は、少なくとも、ユーザがこのようなデジタル・コンテンツ12を再生する権利を有するか否か判定を行なう目的で、レンダリング・アプリケーション34から制御を引き受ける（ステップ513）。

DRMシステム32のコンポーネント

ライセンス評価部36は、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を突き止め、このようなライセンス16が有効であるか否か判定を行い、このような有効なライセンス16におけるライセンス規則を見直し、見直したライセンス規則に基づいて、要求元のユーザが、とりわけ、求められた態様で、要求したデジタル・コンテンツ12をレンダリングする権利を有するか否か判定を行なう。当然理解されようが、ライセンス評価部36は、DRMシステム32における信頼コンポーネント（trusted component）である。この開示では、「信頼」とは、信頼エレメントが、ライセンス16における権利の記述にしたがってデジタル・コンテンツ12の所有者の望みを遂行することをライセンス・サーバ24（またはその他のあらゆる信頼する側のエレメント（trusting element））に納得させること、およびユーザがいずれの邪悪なまたはその他の目的のためにもこのような信頼エレメントを容易に変更できないことを意味する。

10

【0060】

ライセンス評価部36が実際にライセンス16を適性に評価することを保証するため、そしてこのようなライセンス評価部36が、ライセンス16の実際の評価を迂回する目的でユーザが偽造またはそれ以外に変更されていないことを保証するために、このようなライセンス評価部36は信頼されなければならない。したがって、ライセンス評価部36は、保護または隠蔽された環境で走り、このようなライセンス評価部36へのユーザのアクセスが拒否されるようにする。勿論、その他の保護対策も、ライセンス評価部36に関して採用することができ、本発明の精神および範囲から逸脱することはない。

20

DRMシステム32のコンポーネント—ブラック・ボックス30

主に、そして先に論じたように、ブラック・ボックス30は、DRMシステム32において暗号化および解読機能を実行する。即ち、ブラック・ボックス30は、ライセンス評価部36と共に動作し、ある情報をライセンス評価機能の一部として解読および暗号化する。加えて、一旦ライセンス評価部36が、実際にユーザが求められた態様で要求デジタル・コンテンツ12をレンダリングする権利を有すると判定したなら、ブラック・ボックス30には、このようなデジタル・コンテンツ12のために解読鍵（KD）が与えられ、このような解読鍵（KD）に基づいて、このようなデジタル・コンテンツ12を解読する機能を実行する。

30

【0061】

また、ブラック・ボックス30もDRMシステム32における信頼コンポーネントである。即ち、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におけるライセンス規則にしたがってのみ解読機能を実行することを信用しなければならず、更にライセンス16の実際の評価を迂回するという邪悪な目的でユーザによって偽造またはそれ以外に変更された場合には、このようなブラック・ボックス30は動作しないことも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も保護即ち隠蔽された環境で走り、ユーザはこのようなブラック・ボックス30へのアクセスを拒否される。この場合も、ブラック・ボックス30に関して他の保護対策を採用することもでき、本発明の精神および範囲から逸脱することはない。好ましくは、そしてコンテンツ・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、一意の公開／秘密鍵対（PU—BB，PR—BB）を有し、ライセンス16を評価し、デジタル・コンテンツ12を解読するための解読鍵（KD）を取得するプロセスの一部として用いられる。これについては、以下で更に詳しく説明する。

40

DRMシステム32のコンポーネント—ライセンス・ストア38

ライセンス・ストア38は、DRMシステム32が対応するデジタル・コンテンツ12に対して受領したライセンス16を格納する。ライセンス・ストア38自体は、信頼される必要はない。何故なら、ライセンス・ストア38は単にライセンス16を格納するだけに

50

過ぎず、その各々は既に信頼コンポーネントとして組み込まれているからである。これについては以下で説明する。本発明の一実施形態では、ライセンス・ストア 38 は、単に、ハード・ディスク・ドライブまたはネットワーク・ドライブのようなドライブのサブディレクトリである。しかしながら、ライセンス・ストア 38 は、DRM システム 32 に比較的好都合な場所においてライセンス 16 を格納する機能を実行する限りにおいて、本発明の精神および範囲から逸脱することなく、他のあらゆる形態で具体化することも可能である。

DRM システム 32 のコンポーネントー状態ストア 40

状態ストア 40 は、現在または以前ライセンス・ストア 38 にあったライセンス 38 に対応する状態情報を維持する機能を実行する。このような状態情報は、DRM システム 32 が作成し、必要に応じて状態ストア 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 片のデジタル・コンテンツ 12 の所定回数のレンダリングのみを許可する場合、状態ストア 40 は、このようなライセンス 16 に関して実際にレンダリングが何回行われたかに関する状態情報を維持する。状態ストア 40 は、もはやライセンス・ストア 38 にはないライセンス 16 に関する状態情報を維持し続け、状態ストア 40 から対応する状態ストア情報を削除する試みにおいて、ライセンス・ストア 38 からライセンス 16 を削除し、次いで同じライセンス 16 を取得することが有利となるような状況を回避する。

【0062】

また、状態ストア 40 も、内部に格納されている情報が、ユーザに一層好ましい状態にはリセットされないことを保証するために、信頼されなければならない。したがって、状態ストア 40 も同様に保護即ち隠蔽された環境で走り、このような状態ストア 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、状態ストア 40 に関して他の保護対策を勿論採用することができ、本発明の精神および範囲から逸脱することはない。例えば、状態ストア 40 は、DRM システム 32 によって、暗号化形態で計算機 14 上に格納してもよい。

DRM システム 32ーコンテンツ・レンダリング、第 2 部

再度図 5 A を参照し、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度論ずる。一旦 DRM システム 32 が、コール元のレンダリング・アプリケーション 34 から制御を引き受けたなら、このような DRM システム 32 は、ユーザが求められた態様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有するか否か判定を行なうプロセスを開始する。即ち、DRM システム 32 は、ライセンス・ストアにおいて有効な授權ライセンス 16 を突き止めるか（ステップ 515, 517）、あるいはライセンス・サーバ 24 から有効な授權ライセンス (enabling license) 16 を取得しようとする（即ち、以下で論じ図 7 に示すライセンス取得機能を実行する）。

【0063】

第 1 ステップとして、そしてここで図 6 を参照して、このような DRM システム 32 のライセンス評価部 36 は、ライセンス 38 をチェックして、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 を受信しているか否か確認する（ステップ 601）。典型的に、ライセンス 16 は、以下で論ずるように、デジタル・ファイルの形態となっているが、本発明の精神および範囲から逸脱することなくライセンス 16 は他の形態でもよいことは認められよう。典型的に、ユーザは、このようなライセンス 16 がなくてもデジタル・コンテンツ 12 を受信するが、本発明の精神および範囲から逸脱することなく、対応するライセンス 16 と共に、デジタル・コンテンツ 12 を受信するようにしてもよいことも同様に認められよう。

【0064】

図 3 に関連付けて先に論じたように、デジタル・コンテンツ 12 の各片は、パッケージ 12 p 内にあり、コンテンツ ID（またはパッケージ ID）がこのようなデジタル・コンテンツ 12（またはパッケージ 12 p）を識別し、鍵 ID が、暗号化デジタル・コンテンツ 12 を解読する解読鍵（KD）を識別する。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、無暗号化形態である。したがって、そして具体的には、デジ

タル・コンテンツ 12 のコンテンツ ID に基づいて、ライセンス評価部 36 は、このようなコンテンツ ID の適用可能性の識別を収容するライセンス・ストア 8 において、あらゆるライセンス 16 を探す。尚、特にデジタル・コンテンツ 12 の所有者がこのようなデジタル・コンテンツ 12 に対して数種類の異なるライセンス 16 を有し、ユーザがこのようなライセンス 16 を多数個取得している場合、このようなライセンス 16 が多数見つかる場合もあることを注記しておく。実際に、ライセンス評価部 36 がライセンス・ストア 38 において、要求されたデジタル・コンテンツ 12 に対応するライセンス 16 を全く発見できない場合、DRM システム 32 は、以下で説明するライセンス取得機能を実行する（図 5 のステップ 519）。

【0065】

ここで、DRM システム 32 が、1 片のデジタル・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、対応する 1 つ以上のライセンス 16 がライセンス・ストア 38 内にあると仮定する。本発明の一実施形態では、ここで、DRM システム 32 のライセンス評価部 36 は続いて、このようなライセンス 16 の各々について、このようなライセンス 16 自体が有効か否か判定する（図 6 のステップ 603 および 605）。好ましくは、そして具体的に、各ライセンス 116 は、当該ライセンス 16 の内容 28 に基づいたデジタル署名 26 を含む。当然理解されようが、デジタル署名 26 は、コンテンツ 28 が偽造またはそれ以外に変更されている場合、ライセンス 16 とは一致しない。したがって、ライセンス評価部 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 から受け取った形態になっているか（即ち、有効か）否か、判定を行なうことができる。ライセンス・ストア 38 において有効なライセンス 16 が見つからない場合、DRM システム 32 は、以下で説明するライセンス取得機能を実行し、このような有効なライセンス 16 を取得することができる。

【0066】

1 つ以上の有効なライセンス 16 が見つかったと仮定すると、有効なライセンス 16 各々について、DRM システム 32 のライセンス評価部 36 は、次に、このような有効なライセンス 16 が、望ましい態様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ユーザに与えるか（即ち、授權するか）否か判定を行なう。即ち、ライセンス評価部 36 は、要求元のユーザが要求したデジタル・コンテンツ 12 を再生する権利を有するか否か、各ライセンス 16 における権利の記述に基づいて、更にユーザがデジタル・コンテンツ 12 で何をしようとしているのかに基づいて判定を行なう。例えば、このような権利の記述は、ユーザに、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は許可するが、解読してデジタル・コピーにレンダリングすることは許可しない。

【0067】

当然理解されようが、各ライセンス 16 における権利の記述は、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否か指定する。要因には、ユーザが誰であるか、ユーザがどこにいるか、どの種類の計算機 114 をユーザが用いているか、どのレンダリング・アプリケーション 34 が DRM システム 32 をコールしているのか、日付、時間等が含まれる。加えて、権利の記述は、例えば、所定回数の再生、所定の再生時間にライセンス 16 を限定することもできる。このような場合、DRM システム 32 は、ライセンス 16 に関するあらゆる状態情報を参照しなければならない（即ち、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総時間量等）。このような状態情報は、ユーザの計算機 14 の DRM システム 32 の状態ストア 40 に格納されている。

【0068】

したがって、DRM システム 32 のライセンス評価部 36 は、有効な各ライセンス 16 の権利の記述を検討し、このような有効なライセンス 16 が、ユーザに求められた権利を授与するか否か判定を行なう。これを行なう際、ライセンス評価部 36 は、ユーザの計算機 14 内部の別のデータを参照して、ユーザが求めた権利を有するか否かの判定を実行しなければならない場合もある。図 4 に見られるように、このようなデータは、ユーザの計算

機（機械）１４の識別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等を含むことができる。ユーザに求められた態様でデジタル・コンテンツ１２をレンダリングする権利を与える有効なライセンス１６が見つからない場合、ＤＲＭシステム３２は、次に、以下で説明するライセンス取得機能を実行し、実際にこのようなライセンス１６が取得可能であれば、このようなライセンス１６を取得する。

【００６９】

勿論、場合によっては、ユーザは要求した態様でデジタル・コンテンツ１２をレンダリングする権利を取得できないこともある。何故なら、このようなデジタル・コンテンツ１２のコンテンツ所有者は、ユーザにテキスト文書を印刷したり、マルチメディア表現を無暗号化形態にコピーすることを許可するライセンス１６を付与しないことを指令している場合もあるからである。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の購入時にどんな権利が利用可能かに関するデータ、および利用可能なライセンス１６の種類を含む。しかしながら、１片のデジタル・コンテンツ１２のコンテンツ所有者は、いずれの時点においても、このようなデジタル・コンテンツ１２に対して得られるライセンス１６を変更することによって、このようなデジタル・コンテンツ１２に現在利用可能な権利を変更する可能性があることは認められよう。

ＤＲＭシステム３２－ライセンス取得

ここで図７を参照すると、実際にライセンス評価部３６がライセンス・ストア３８において、要求されたデジタル・コンテンツ１２に対応する有効な授権ライセンス１６を全く見つけられない場合、ＤＲＭシステム３２は、ライセンス取得機能を実行する。図３に示すように、デジタル・コンテンツ１２の各片は、このようなデジタル・コンテンツ１２をレンダリングするためのライセンス１６を取得するにはどうすればよいかに関する無暗号化形態の情報（即ち、ライセンス取得情報）と共にパッケージ化されている。

【００７０】

本発明の一実施形態では、このようなライセンス取得情報は、利用可能なライセンス１６の種類、および１つ以上の適切なライセンス・サーバ２４にアクセスすることができる１つ以上のインターネット・ウェブ・サイトまたはその他のサイト情報を（とりわけ）含むことができる。ここで、各ライセンス・サーバ２４は実際にデジタル・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、ライセンスは、他の態様で取得することもでき、本発明の精神および範囲から逸脱する訳ではない。例えば、ライセンス１６は、電子掲示板においてライセンス・サーバ２４から取得したり、あるいは自分自身でまたは磁気または光ディスク等のファイルという形態で正規のメールによって取得することもできる。

【００７１】

ライセンス１６を取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であると仮定すると、ライセンス評価部３６は、ウェブ・サイトまたはその他のサイト情報に基づいてこのようなライセンス・サーバ２４に対してネットワーク接続を確立し、次いでこのように接続したライセンス・サーバ２４からライセンス１６の要求を送る（ステップ７０１、７０３）。即ち、一旦ＤＲＭシステム３２がライセンス・サーバ２４とコンタクトしたなら、このようなＤＲＭシステム３２は適切なライセンス要求情報３７をこのようなライセンス・サーバ２４に送信する。本発明の一実施形態では、このようなライセンス１６の要求情報３６は、とりわけ、次を含むことができる。

【００７２】

－ＤＲＭシステム３２のブラック・ボックス３０の公開鍵（ＰＵＢＢ）、
－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を認証した証明機関からのデジタル署名を含む認証書（認証書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もできる）、
－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 I D)、
ーデジタル・コンテンツ 1 2 を解読するための解読鍵 (K D) を識別する鍵 I D、
ー要求されたライセンス 1 6 の種類 (実際に多数の種類が使用可能な場合)、
ーデジタル・コンテンツ 1 2 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 3 4 の種類等。

【0073】

勿論、これらよりも多い量または少ない量のライセンス 1 6 の要求情報 3 6 を、D R M システム 3 2 によって、ライセンス・サーバ 2 4 に送信することもでき、本発明の精神および範囲から逸脱することはない。例えば、レンダリング・アプリケーション 3 4 の種類に関する情報が必要ではない場合もあり、一方ユーザおよび／またはユーザの計算機 1 4 に

10

【0074】

一旦ライセンス・サーバ 2 4 が D R M システム 3 2 からライセンス 1 6 の要求情報 3 6 を受信したなら、ライセンス・サーバ 2 4 は、信頼／認証およびその他の目的のために、いくつかのチェックを行なうとよい。本発明の一実施形態では、このようなライセンス・サーバ 2 4 は、証明機関のデジタル署名を含む認証書をチェックし、これが偽造またはそれ以外に変更されていないか否か判定を行なう (ステップ 7 0 5、7 0 7)。されている場合、ライセンス・サーバ 2 4 は、要求情報 3 6 に基づいてあらゆるライセンス 1 6 を付与することを拒否する。また、ライセンス・サーバ 2 4 は、判明した「悪い」ユーザおよび／またはユーザの計算機 1 4 のリストを保持することもでき、更にリスト上にあるこのよ

20

【0075】

受信した要求およびそれに付随する情報に基づいて、特にライセンス要求情報におけるコンテンツ I D (またはパッケージ I D) に基づいて、ライセンス・サーバ 2 4 はコンテンツ鍵データベース 2 0 (図 1) に問い合わせ、要求の基準であるデジタル・コンテンツ 1 2 (またはパッケージ 1 2 p) に対応するレコードを突き止める。先に論じたように、このようなレコードは、このようなデジタル・コンテンツ 1 2 に対する解読鍵 (K D)、鍵 I D、およびコンテンツ I D を含む。加えて、このようなレコードは、デジタル・コンテンツ 1 2 に発行するライセンス 1 6 の種類、ならびにライセンス 1 6 の各種類毎の条件に関するライセンス・データを収容することができる。あるいは、このようなレコードは、このような追加情報を有する場所へのポインタ、リンク、または参照を含むこともできる。

30

【0076】

前述のように、多数の種類 of ライセンス 1 6 を得ることができる。例えば、比較的小額のライセンス料では、限られた回数のレンダリングを許可するライセンス 1 6 を得ることができる。比較的大きな額のライセンス料では、満期日まで無制限のレンダリングを許可するライセンス 1 6 を得ることができる。更に高額 of ライセンス料では、満期日なしで無制限のレンダリングを許可するライセンスを得ることができる。実際には、あらゆる種類のライセンス条件を有するあらゆる種類のライセンス 1 6 でも、ライセンス・サーバ 2 4 によって考案し発行することもでき、本発明の精神および範囲から逸脱することはない。

40

【0077】

本発明の一実施形態では、ライセンス 1 6 の要求は、ライセンス・サーバ 2 4 からユーザの計算機 1 4 まで送信する際に、ウェブ・ページ等の助けによって行われる。好ましくは、このようなウェブ・ページは、ライセンス 1 6 の要求の基準であるデジタル・コンテンツ 1 2 に対してライセンス・サーバ 2 4 から得られるあらゆる種類のライセンス 1 6 に関する情報を含む。

【0078】

50

本発明の一実施形態では、ライセンス 16 を発行するのに先立って、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チェックし、このようなブラック・ボックス 30 が比較的新しいか否か判定を行なう（ステップ 709、711）。当然理解されようが、ブラック・ボックス 30 は、安全であり、邪悪な目的（即ち、ライセンス 16 なく不適正にデジタル・コンテンツ 12 をレンダリングしたり、対応するライセンス 16 の条件に外れている）のユーザからの攻撃から保護することを目的とする。しかしながら、実際にはこのような攻撃から完全に安全なシステムもソフトウェアもないことは認められよう。

【0079】

当然理解されようが、ブラック・ボックス 30 が比較的新しい場合、即ち、比較的最近取得または更新された場合、このようなブラック・ボックス 30 がこのような邪悪なユーザによる攻撃を受けて成功する可能性は少ない。好ましくは、そして信頼問題として、ライセンス・サーバ 24 が、比較的新しくないブラック・ボックス 30 のバージョン番号を含む要求情報を有するライセンス要求を受信した場合、このようなライセンス・サーバ 24 は、対応するブラック・ボックス 30 が現行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 を発行することを拒否する。これについては以下で説明する。単純に言えば、ライセンス・サーバ 24 は、このようなブラック・ボックス 30 が比較的新しくなければ、このようなブラック・ボックス 30 を信頼しない。

【0080】

本発明のブラック・ボックス 30 に関連して、「新しい」または「比較的新しい」という用語は、ブラック・ボックス 30 の使用年数および利用度に基づいてブラック・ボックス 30 に信頼を与える機能と一貫して、適切な意味を有することができ、本発明の精神および範囲から逸脱することはない。例えば、「新しい」は、年数にしたがって定義することができる（即ち、1 か月未満）。別の例として、「新しい」は、ブラックボックス 30 がデジタル・コンテンツを解読した回数に基づいて定義することもできる（即ち、解読が 200 回未満）。更に、「新しい」は、各ライセンス・サーバ 24 が設定する理念に基づくこともでき、この場合 1 つのライセンス・サーバ 24 は別のライセンス・サーバとは異なる定義を「新しい」に対してすることもでき、更に、とりわけ、ライセンス 16 が要求されるデジタル・コンテンツ 12 に応じて、または要求されたライセンス 16 の種類に応じて、ライセンス・サーバ 24 は「新しい」を別個に定義することもできる。

【0081】

ブラック・ボックス 30 のバージョン番号またはこのようなブラック・ボックス 30 のその他の指標が新しいことに、ライセンス・サーバ 24 が納得したと仮定すると、ライセンス・サーバ 24 は次にユーザとライセンス 16 の条件を交渉する。あるいは、ライセンス・サーバ 24 はユーザとライセンス 16 の交渉を行い、このようなブラック・ボックス 30 が新しいことを示すブラック・ボックス 30 のバージョン番号にそれ自体が納得する（ステップ 713、次いで 711 を実行する）。勿論、交渉の量は、発行するライセンス 16 の種類、およびその他の要因によって異なる。例えば、ライセンス・サーバ 24 が単に一括払い無制限使用ライセンス 16 を発行する場合、殆ど交渉を行なう必要はない。一方、ライセンス 16 が、変動する価値、スライド制、区切り点、およびその他の詳細のような項目に基づく場合、このような項目および詳細は、ライセンス・サーバ 24 およびユーザ間で、ライセンス 16 を発行可能となる前に案出しなければならない場合もある。

【0082】

当然理解されようが、状況によっては、ライセンスの交渉は、ユーザが更にライセンス・サーバ 24 に情報を提供しなければならないこともあり得る（例えば、ユーザ、ユーザの計算機 14 等に関する情報）。重要なことは、ライセンスの交渉は、とりわけ、ユーザおよびライセンス・サーバ 24 が相互に受諾可能な支払手段（クレジット・アカウント、デビット・アカウント、郵送による小切手等）および／または支払方法（即時一括払い、ある時間期間の分割）を決定しなければならないことである。

【0083】

一旦ライセンス１６の全ての条件について交渉を行い、ライセンス・サーバ２４およびユーザ双方が同意したなら（ステップ７１５）、ライセンス・サーバ２２４がデジタル・ライセンス１６を生成する（ステップ７１９）。このように生成するライセンス１６は、少なくとも部分的に、ライセンス要求、ブラック・ボックス３０の公開鍵（ＰＵ－ＢＢ）、およびコンテンツ鍵データベース２０から取得した要求の基準となるデジタル・コンテンツ１２に対する解読鍵（ＫＤ）に基づいている。本発明の一実施形態では、そして図８に見られるように、生成したライセンス１６は次を含む。

【００８４】

－ライセンス１６を適用するデジタル・コンテンツ１２のコンテンツＩＤ、
－恐らくは解読鍵（ＫＤ）（即ち、ＫＤ（ＤＲＬ））で暗号化されている、デジタル権利
ライセンス（ＤＲＬ）４８（即ち、ライセンス評価部３６が問い合わせることができる所
定の書式で書かれたライセンス１６の権利の記述即ち実際の条件）、
－ライセンス要求において受信したブラック・ボックス３０の公開鍵（ＰＵ－ＢＢ）で暗
号化したデジタル・コンテンツ１２に対する解読鍵（ＫＤ）（即ち（ＰＵ－ＢＢ（ＫＤ）
））。

10

【００８５】

－（ＫＤ（ＤＲＬ））および（ＰＵ－ＢＢ（ＫＤ））に基づき、ライセンス・サーバ２４
の秘密鍵（即ち、（Ｓ（ＰＲ－ＬＳ）））を用いて暗号化した、ライセンス・サーバ２４
からのデジタル署名（認証書の添付なし）、および
－ライセンス・サーバ２４がコンテンツ・サーバ２２から以前に取得した認証書。このよ
うな認証書は、ライセンス・サーバ２４がコンテンツ・サーバ２２からのライセンス１６
を発行する権限を有することを示す（即ち、（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ）
））。

20

【００８６】

当然理解されようが、前述のエレメントおよび恐らくその他のエレメントも、デジタル・
ファイルまたはその他の何らかの適切な形態にパッケージ化される。同様に当然理解され
ようが、ＤＲＬ４８またはライセンス１６における（ＰＵ－ＢＢ（ＫＤ））が偽造または
それ以外に変更されている場合、ライセンス１６におけるデジタル署名（Ｓ（ＰＲ－ＬＳ）
）は一致せず、したがって、このようなライセンス１６は有効性が認められない。この
理由のため、ＤＲＬは必ずしも前述のような暗号化形態（即ち、（ＫＤ（ＤＲＬ））であ
る必要はないが、場合によってはこのような暗号化形態が望ましい場合もあり、したが
って、本発明の精神および範囲から逸脱することなく、採用してもよい。

30

【００８７】

一旦デジタル・ライセンス１６の準備が終了すると、次にこのようなライセンス１６を要
求元（即ち、ユーザの計算機１４上のＤＲＭシステム３２）（図７のステップ７１９）。
好ましくは、ライセンス１６は、その要求が行われたのと同じ経路（即ち、インターネッ
トまたはその他のネットワーク）を通じて送信するとよいが、他の経路を用いてもよく、
本発明の精神および範囲から逸脱することはない。受信時に、要求元ＤＲＭ３２は、自動
的に受信したデジタル・ライセンス１６をライセンス・ストア３８に置くことが好ましい
（ステップ７２１）。

40

【００８８】

尚、ユーザの計算機１４は、場合によっては誤動作する場合もあり、このようなユーザの
計算機１４上のＤＲＭシステム３２のライセンス・ストア３８に格納されているライセン
ス１６が検索不能となり、失われる場合もあり得ることは理解されよう。したがって、ラ
イセンス・サーバ２４は、発行したライセンス１６のデータベース５０（図１）を保持し
、ユーザに実際に再発行を受ける権利がある場合、このようなライセンス・サーバ２５が
、ユーザに発行したライセンス１６のコピーを与えるかまたは再発行を行なう（以後、「
再発行」）ようにすることが好ましい。ライセンス１６が検索不能となり失われるという
前述の場合では、状態ストア４０に格納されており、このようなライセンス１６に対応す
る状態情報も失われる可能性もある。このように失われた状態情報は、ライセンス１６を

50

再発行する際に考慮に入れなければならない。例えば、比較的短い時間期間の後に一定の割合に応じた形態で固定数のレンダリング・ライセンス 16 を合法的に再発行し、比較的長い時間期間の後には全く再発行しないことも可能である。DRMシステム 32—ブラック・ボックス 30 のインストール／更新

先に論じたように、ライセンス 16 を取得する機能の一部として、ライセンス・サーバ 24 は、ユーザの計算機 14 の DRMシステム 32 が、比較的新しくないブラック・ボックス 30、即ち、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 の要求を拒否することができる。このような場合、このような DRMシステム 32 のブラック・ボックス 30 を更新し、ライセンス取得機能が進行できるようにすることが好ましい。勿論、ブラック・ボックス 30 は他の時点でも更新可能であり、本発明の精神および範囲から逸脱することはない。

10

【0089】

好ましくは、ユーザの計算機 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、ブラック・ボックス 30 の一意でない「ライト」(lite)バージョンを用意する。このような「ライト」ブラック・ボックス 30 は、1 片のデジタル・コンテンツ 12 をレンダリングする前に、一意の正規バージョンにアップグレードする。当然理解されようが、各 DRMシステム 32 における各ブラック・ボックス 30 が一意であれば、1 つのブラック・ボックス 30 へのセキュリティ侵害は、他のいずれのブラック・ボックス 30 に対しても容易に繰り返すことはできない。

【0090】

20

次に図 9 を参照すると、DRMシステム 32 は、ブラック・ボックス・サーバ等から要求することによって、一意のブラック・ボックス 30 を取得する（先に論じ、図 1 に示した通りである）（ステップ 901）。典型的に、このような要求を行なうにはインターネットを用いるが、他のアクセス手段も採用でき、本発明の精神および範囲から逸脱することはない。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のいずれでも、直接接続とすることができる。1 つの一意の非ライト・ブラック・ボックス 30 から別の一意の非ライト・ブラック・ボックス 30 へのアップグレードも、いずれの時点においても、例えば、ライセンス・サーバ 24 がブラック・ボックス 30 を新しく見なしたときのように、DRMシステム 32 によって要求することができる。これは、先に論じた通りである。

30

【0091】

その後、ブラック・ボックス・サーバ 26 は、新たな一意のブラック・ボックス 30 を生成する（ステップ 903）。図 3 に見られるように、新たなブラック・ボックス 30 の各々には、バージョン番号、および証明機関からのデジタル署名を有する認証書が備えられている。ライセンス取得機能との関連で先に論じたように、ブラック・ボックス 30 のバージョン番号は、その相対的な使用期間 (age) および／または使用を示す。同様にライセンス取得機能との関連で先に論じた、証明機関からのデジタル署名を有する認証書は、ライセンス・サーバ 24 がブラック・ボックス 30 を信頼するという、証明機関からの申し出即ち証拠機構である。勿論、ライセンス・サーバ 24 は、証明機関がこのような認証書を、実際に信頼のおけるブラック・ボックス 30 に発行することを信用する。実際には、ライセンス・サーバ 24 が特定の証明機関を信頼せず、このような証明機関が発行するいずれの認証書も有効と認めることを拒絶する場合もあり得る。例えば、特定の証明機関が不正に認証書を発行しているパターンに関与していることが発覚した場合、信頼を得ることはできない。

40

【0092】

好ましくは、そして先に論じたように、ブラック・ボックス・サーバ 26 は、新たに生成した一意のブラック・ボックス 30 を有する新たな一意の公開／秘密鍵対 (PU-BB, PR-BB) を含む。好ましくは、ブラック・ボックス 30 の秘密鍵 (PU-BB) は、このようなブラック・ボックス 30 のみからアクセス可能であり、このようなブラック・ボックス 30 を含む DRMシステム 32 を有する計算機 14 およびそのユーザを含めて、

50

世界のその他からは隠されており、アクセスすることはできない。

【0093】

あらゆる秘匿方式は、実際にこのような秘匿方式が世界から秘密鍵（PU-BB）を隠す機能を実行する限り、その殆どを用いることができ、本発明の精神および範囲から逸脱することはない。一例としてに過ぎないが、秘密鍵（PU-BB）をいくつかのサブコンポーネントに分割し、各サブコンポーネントを一意に暗号化し、異なる場所に格納してもよい。このような状況では、このようなサブアセンブリを完全に組み立てて完全な秘密鍵（PU-BB）を決して生成しないことが好ましい。

【0094】

本発明の一実施形態では、このような秘密鍵（PU-BB）を暗号化するには、コードを用いる暗号化技術に従う。即ち、このような実施形態では、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（複数の暗号化鍵）として用いられる。したがって、例えば、邪悪な目的でユーザによってブラック・ボックス30のコード（またはその他のソフトウェア・コード）が偽造されたり、あるいは他の方法で変更された場合、このような秘密鍵（PU-BB）を解読することはできない。

【0095】

新たなブラック・ボックス30の各々は、新たな公開／秘密鍵対（PU-BB，PR-BB）と共に配信されるが、このような新たなブラック・ボックス30には、ユーザの計算機14上のDRMシステム32に以前に配信した古いブラック・ボックス30からの古い公開／秘密鍵対へのアクセスも与えることが好ましい（ステップ905）。したがって、アップグレードしたブラック・ボックス30は、古い鍵対を用いて、古いデジタル・コンテンツ12およびこのような古い鍵対にしたがって生成した、対応する古いライセンス16にもアクセスすることができる。これについては、以下で更に詳しく論ずる。

【0096】

好ましくは、ブラック・ボックス・サーバ26が配信するアップグレードしたブラック・ボックス30は、ユーザの計算機14に密接に連結即ち関連付けられる。したがって、アップグレードしたブラック・ボックス30は、邪悪な目的およびその他のために、多数の計算機間で動作可能に転送することはできない。本発明の一実施形態では、ブラック・ボックス30の要求（ステップ901）の一部として、DRMシステム32は、このようなDRMシステム32に一意の、および／またはユーザの計算機14に一意の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、部分的にこのような提供されたハードウェア情報に基づいて、DRMシステム32にブラック・ボックス30を生成する。このように生成されたアップグレード・ブラック・ボックス30は、次にユーザの計算機14に配信され、DRMシステム32にインストールされる（ステップ907、909）。アップグレードしたブラック・ボックス30が何らかの方法で別の計算機14に転送された場合、転送されたブラック・ボックス30は、このような他の計算機14を対象とするのではないことを認識し、このようなその他の計算機14上でレンダリングを進める要求を全て許可しない。

【0097】

一旦新たなブラック・ボックス30がDRMシステム32にインストールされると、このようなDRMシステム32は、ライセンス取得機能またはその他のいずれかの機能を実行することができる。

DRMシステム32－コンテンツ・レンダリング、第3部

次に図5Bを参照し、ここでライセンス評価部36が少なくとも1つの有効なライセンス16を発見し、このような有効なライセンス16の少なくとも1つが、求められた態様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必要な権利（即ち、授權）をユーザに与えることがわかったと仮定すると、ライセンス評価部36は、更に用いるためにこのようなライセンス16の1つを選択する（ステップ519）。即ち、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、ライセンス評価部36およびブラ

ック・ボックス 30 は、一体となってこのようなライセンス 16 から解読鍵 (KD) を取得し、ブラック・ボックス 30 はこのような解読鍵 (KD) を用いて、デジタル・コンテンツ 12 を解読する。本発明の一実施形態では、そして先に論じたように、ライセンス 16 から取得した解読鍵 (KD) は、ブラック・ボックス 30 の公開鍵 (PU-BB (KD)) で暗号化されており、ブラック・ボックス 30 は、その秘密鍵 (PU-BB) を用いて、このように暗号化されている解読鍵を解読し、解読鍵 (KD) を生成する (ステップ 521、523)。しかしながら、デジタル・コンテンツ 12 の解読鍵 (KD) を取得するその他の方法を用いてもよく、本発明の精神および範囲から逸脱することはない。

【0098】

一旦ブラック・ボックス 30 がデジタル・コンテンツ 12 の解読鍵 (KD) を有し、ライセンス評価部 36 からデジタル・コンテンツ 12 をレンダリングする許可を得たなら、制御をレンダリング・アプリケーション 34 に戻すことができる (ステップ 525、527)。本発明の一実施形態では、レンダリング・アプリケーション 34 は次に DRM システム 32 / ブラック・ボックス 30 をコールし、暗号化デジタル・コンテンツ 12 の少なくとも一部をブラック・ボックス 30 に送出し、解読鍵 (KD) にしたがって解読する (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 の解読鍵 (KD) に基づいてデジタル・コンテンツ 12 を解読し、次いでブラック・ボックス 30 は、解読したデジタル・コンテンツ 12 を実際にレンダリングするために、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、暗号化デジタル・コンテンツ 12 の一部またはデジタル・コンテンツ 12 全体をブラック・ボックス 30 に送り、本発明の精神および範囲から逸脱することなく、このようなデジタル・コンテンツ 12 の解読鍵 (KD) に基づいて解読することができる。

【0099】

好ましくは、レンダリング・アプリケーション 34 がデジタル・コンテンツ 12 をブラック・ボックス 30 に送り解読する場合、ブラック・ボックス 30 および / または DRM システム 32 はこのようなレンダリング・アプリケーション 34 の認証を行い、これが実際に DRM システム 32 に最初に走らせるように要求したのと同じレンダリング・アプリケーションであることを確認する (ステップ 531)。あるいは、レンダリングの承認が、ある種のレンダリング・アプリケーション 34 に対するレンダリング要求に基づき、実際に他の種類のレンダリング・アプリケーション 34 でレンダリングすることによって、不正に取得されたという可能性もあり得る。認証に成功し、デジタル・コンテンツ 12 がブラック・ボックス 30 によって解読されたと仮定すると、レンダリング・アプリケーション 34 は解読されたデジタル・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)。

鍵トランザクション・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・シーケンスを実行して、要求された 1 片のデジタル・コンテンツ 12 に対する解読鍵 (KD) を取得し、ライセンス 16 を評価する (即ち、図 5 A および図 5 B のステップ 515 ないし 523 を実行する)。このシーケンスでは、主に DRM システム 32 はライセンス 16 から解読鍵 (KD) を取得し、ライセンス 16 およびデジタル・コンテンツ 12 から得た情報を用いて、双方の有効性を認証即ち確認し、次いでライセンス 16 が実際に求められた態様でデジタル・コンテンツ 12 をレンダリングする権利を与えるか否か判定を行なう。与える場合、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。

【0100】

図 8 に示すように、デジタル・コンテンツ 12 の各ライセンス 16 が次を含むことを念頭に入れ、

- ーライセンス 16 を適用するデジタル・コンテンツ 12 のコンテンツ ID、
- ー恐らく解読鍵 (KD) で暗号化されているデジタル権利ライセンス (DRL) 48 (即ち、KD (DRK))。

【0101】

ーブラック・ボックス30の公開鍵(PU-BB)で暗号化されているデジタル・コンテンツ12の解読鍵(KD)(即ち、(PU-BB(KD))、
 ー(KD(DRK))および(PU-BB(KD))に基づいて、そしてライセンス・サーバ24の秘密鍵で暗号化されている、ライセンス・サーバ24からのデジタル署名(即ち、(S(PR-LS)))、および
 ーライセンス・サーバ24が以前にコンテンツ・サーバ22から取得した認証書(即ち、(CERT(PU-LS)S(PR-CS)))、
 更に、図3に示すように、デジタル・コンテンツ12を有するパッケージ12pが次を含むことも念頭に入れ、
 ーこのようなデジタル・コンテンツ12のコンテンツID、
 KDによって暗号化されているデジタル・コンテンツ12(即ち、(KD(CONTENT)))、
 ー暗号化されていないライセンス取得スクリプト、および
 ーコンテンツ・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、
 本発明の一実施形態では、鍵トランザクションの特定のシーケンスを、デジタル・コンテンツ12のライセンス16の特定の1つに関して実行する。このシーケンスは次の通りである。

【0102】

1. ライセンス16からの(PU-BB(KD))に基づいて、ユーザの計算機14上のDRMシステム32のブラック・ボックス30はその秘密鍵(PR-BB)を適用し、(KD)を取得する(ステップ1001)。(PR-BB(PU-BB(PU-BB(KD)))=(KD))。尚、重要なことは、ブラック・ボックス30は、これ以上の面倒なく、KDを用いてデジタル・コンテンツ12を解読しようとすることも可能であることを注記しておく。このような信頼は、このようなライセンス・サーバ24が、このようなブラック・ボックス30の信ぴょう性を保証する、証明機関からの認証書に基づいて、ライセンス16を発行したときに確立されている。したがって、最終ステップではなく最初のステップとしてブラック・ボックス30が解読鍵(KD)を取得しても、DRMシステム32は、以下に説明するように、全てのライセンス16の妥当性検査および評価機能を実行し続ける。

【0103】

2. デジタル・コンテンツ12からの(KD(PU-CS)S(PR-CS))に基づいて、ブラック・ボックス30は新たに取得した解読鍵(KD)を適用して(PU-CS)を取得する(ステップ1003)。(KD(KD(PU-CS)=(PU-CS))。加えて、ブラック・ボックス30は、署名(S(PR-CS))に対して(PU-CS)を適用し、このような署名およびこのようなデジタル・コンテンツ12／パッケージ12pが有効であることを納得する(ステップ1005)。有効でない場合、プロセスを中断し、デジタル・コンテンツ12へのアクセスを拒否する。

【0104】

3. ライセンス16からの(CERT(PU-LS)S(PR-CS))に基づいて、ブラック・ボックス30は、新たに取得したコンテンツ・サーバ22の公開鍵(PU-CS)を適用し、認証書が有効であることを納得する(ステップ1007)。これは、ライセンス16を発行したライセンス・サーバ24がコンテンツ・サーバ22からの機関(authority)にそうさせ、次いで認証書の内容を検査して(PU-LS)を取得することを意味する(ステップ1009)。有効でない場合、プロセスを中止し、ライセンス16に基づくデジタル・コンテンツ12へのアクセスを拒否する。

【0105】

4. ライセンス16からの(S(PR-LS))に基づいて、ブラック・ボックス30は、新たに取得したライセンス・サーバ24の公開鍵(PR-LS)を適用して、ライセンス16が有効であることを納得する(ステップ1011)。有効でない場合、プロセスを

10

20

30

40

50

中止し、ライセンス 16 に基づくデジタル・コンテンツ 12 へのアクセスを拒否する。

【0106】

5. 全ての妥当性検査ステップが成功し、ライセンス 16 内の DRL 48 が実際に解読鍵 (KD) で暗号化されていると仮定すると、ライセンス評価部 36 は、既に取得してある解読鍵 (KD) を、ライセンス 16 から取得した (KD (DRL)) に適用し、ライセンス 16 からライセンス条件を得る (即ち DRL 48) (ステップ 1013)。勿論、ライセンス 16 における DRL 48 が実際に解読鍵 (KD) で暗号化されていない場合、ステップ 1013 を省略してもよい。次に、ライセンス評価部 36 は、DRL 48 を評価し、問い合わせを行い、ユーザの計算機 14 がライセンス 16 内の DRL 48 に基づいて、求められた態様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否か (即ち、DRL 48 が授権付与しているか否か) 判定を行なう (ステップ 1015)。ライセンス評価部 36 が、このような権利が存在しないと判定した場合、プロセスを中止し、ライセンス 16 に基づくデジタル・コンテンツ 12 へのアクセスを拒否する。

10

【0107】

6. 最後に、ライセンス 16 の評価の結果、ユーザの計算機 14 は DRL 48 の条件に基づいて、求められた態様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断が得られたと仮定すると、ライセンス評価部 36 は、ブラック・ボックス 30 が解読鍵 (KD) にしたが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ことを、このようなブラック・ボックス 30 に通知する。その後、ブラック・ボックス 30 は解読鍵 (KD) を適用し、パッケージ 12 p からのデジタル・コンテンツ 12 を解読する (即ち、(KD (KD (CONTENT))) = (CONTENT)) (ステップ 1017)。

20

【0108】

先に具体化した一連のステップは、ライセンス 16 およびデジタル・コンテンツ 12 間の交互動作即ち「ピンポン動作」を表わすことを注記するのは重要である。このようなピンポン動作によって、デジタル・コンテンツ 12 を緊密にライセンス 16 に結び付けることを保証し、デジタル・コンテンツ 12 およびライセンス 16 双方が適性に発行され有効な形態で存在する場合にのみ、妥当性検査および評価プロセスを行なうことができることを保証する。加えて、ライセンス 16 からのコンテンツ・サーバ 22 の公開鍵 (PU-CS)、および解読した形態でパッケージ 12 p からデジタル・コンテンツ 12 を得るには (そして、恐らく、解読した形態でライセンス 16 からライセンス条件 (DRL 48) を得るためにも) 同じ解読鍵 (KD) が必要であるので、このような項目も緊密に結び付けられる。また、署名の妥当性検査によっても、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 から発行された同じ形態であることを保証する。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 を解読することは、不可能ではないにしても困難であり、デジタル・コンテンツ 12 またはライセンス 16 を変更しそして解読することも、不可能ではないにしても困難である。

30

【0109】

本発明の一実施形態では、署名の妥当性検査、特にライセンス 16 の署名の妥当性検査は、代わりに次のように行われる。図 8 に示すように、ライセンス・サーバ 16 の秘密鍵 (PR-LS) によって署名を暗号化するのではなく、各ライセンス 16 の署名を、秘密ルート鍵 (PR-R) (図示せず) によって暗号化する。この場合、各 DRM システム 32 のブラック・ボックス 30 は、秘密ルート鍵 (PR-R) に対応する公開ルート鍵 (PU-P) (これも図示せず) を含む。秘密ルート鍵 (PR-R) は、ルート・エンティティだけがわかっており、ライセンス・サーバ 24 は、このようなライセンス・サーバ 24 がルート・エンティティを用いてライセンス 16 を発行するように調整した場合にのみ、ライセンス 16 を発行することができる。

40

【0110】

即ち、このような実施形態では、

50

1. ライセンス・サーバ24がその公開鍵(P R-L S)をルート・エンティティに供給する。

【0111】

2. ルート・エンティティはこのようなライセンス・サーバ24に、秘密ルート鍵(P R-R)によって暗号化されたライセンス・サーバ公開鍵(P U-L S)を戻す(即ち、(C E R T (P U-L S) S (P R-R)))。

【0112】

3. 次に、ライセンス・サーバ24は、ライセンス・サーバの公開鍵(S (P R-L S))によって暗号化された署名を有するライセンス16を発行し、更に、ルート・エンティティからの認証書をライセンスに添付する(C E R T (P U-L S) S (P R-R))。 10

【0113】

DRMシステム18がこのように発行されたライセンス17の妥当性を検査するために、DRMシステム18は、

1. 公開ルート鍵(P U-R)を、添付した認証書(C E R T (P U-L S) S (P R-R))に適用し、ライセンス・サーバ公開鍵(P U-L S)を取得し、

2. 取得したライセンス・サーバ公開鍵(P U-L S)をライセンス16の署名(P R-L S)に適用する。

【0114】

重要なこととして、ルート・エンティティが認証書(C E R T (P U-L S) S (P R-R))をライセンス・サーバ24に供給することによって、このようなライセンス・サーバ24にライセンス16を発行する許可を与えるのと丁度同じように、このようなライセンス・サーバ24は同様に認証書を第2のライセンス・サーバ24に供給し(即ち、(C E R T (P U-L S 2) S (P R-L S 1)))、これによって第2のライセンス・サーバにもライセンス16を発行させることができることも認められてしかるべきである。今や明白であろうが、第2ライセンス・サーバが発行するライセンス16は、第1認証書(C E R T (P U-L S 1) S (P R-R))および第2認証書(C E R T (P U-L S 2) S (P R-L S 1))を含む。同様に、このようなライセンス16は、第1および第2認証書のチェーンに従うことによって、有効性を認められる。勿論、チェーンの中に追加のリンクを加え、これらを通過するようにしてもよい。 20

【0115】

前述の署名妥当性検査プロセスの利点の1つとして、ルート・エンティティが定期的に秘密ルート鍵(R P-R)を変更することによって、同様に定期的に各ライセンス・サーバ24に新たな認証書(C E R T (P U-L S) S (P R-R))を取得させることができる点にある。重要なことは、このような新たな認証書を取得する要件として、各ライセンス・サーバがそれ自体をアップグレードする必要があるということである。ブラック・ボックス30の場合と同様、ライセンス・サーバ24が比較的新しい場合、即ち、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を攻撃して成功する可能性は低くなる。したがって、信頼の問題として、各ライセンス・サーバ24は、署名妥当性検査プロセスのような適切なアップグレード推進機構を通じて定期的にアップグレードしなければならないようにすることが好ましい。勿論、他のアップグレード機構を採用することもでき、本発明の精神および範囲から逸脱することにはならない。 30

【0116】

勿論、秘密ルート鍵(P R-R)を変更する場合、各DRMシステム18における公開ルート鍵(P U-R)も変更しなければならない。このような変更は、例えば、通常のブラック・ボックス30のアップグレードの間に行なえばよく、あるいは実際にはブラック・ボックス30のアップグレードを行なうことが必要となる場合もある。変更した公開ルート鍵(P U-R)は潜在的に、古い秘密ルート鍵(P R-R)に基づいて発行した古いライセンス16に対する署名の妥当性検査と干渉する可能性もあるが、このような干渉は、アップグレードしたブラック・ボックス30が古い公開ルート鍵(P U-R)全てを記憶しておくことを要求することによって、最少に抑えることができる。あるいは、このよう 40 50

な干渉を最少に抑えるには、ライセンス16に対する署名の検証を1回だけ行なえばよいようにしてもよい。例えば、DRMシステム18のライセンス評価部36によって、最初にこのようなライセンス16を評価する。このような場合、署名の検証が行われたか否かに関する状態情報をコンパイルし、このような状態情報をDRMシステム18の状態ストア40に格納するべきであろう。

デジタル権利ライセンス48

本発明では、ライセンス評価部36は、ライセンス16の権利記述即ち条件としてデジタル権利ライセンス(DRL)48を評価し、このようなDRL48が、求められた態様でデジタル・コンテンツ12の対応する1片のレンダリングを許可するか否か判定を行なう。本発明の一実施形態では、いずれかのDRL言語によって、ライセンサ(即ち、コンテンツ所有者)がDRL48を書くことができる。

10

【0117】

当然理解されようが、DRL48を指定するには多くの方法がある。したがって、いずれのDRL言語においても、高い柔軟性を許容しなければならない。しかしながら、特定のライセンス言語でDRL48の全ての面を指定することは非実用的であり、このような言語の著者が、個々のデジタル・ライセンサが望むライセンスの可能な態様全てを確認できるようにすることは可能性が非常に低い。更に、非常に洗練されたライセンス言語は不要の場合もあり、比較的単純なDRL48を与えるライセンサにとっては障害となる場合もある。しかしながら、DRL48をどのように指定するかについてライセンサを不必要に制約してはならない。同時に、ライセンス評価部36は、常に多数の具体的なライセンスに関する問題に対して、DRL48から回答を得ることができなければならない。

20

【0118】

ここで図11を参照すると、本発明では、DRL48はいずれのライセンス言語でも指定することができるが、言語識別子即ちタグ54を含む。ライセンス評価部36は、ライセンス16を評価し、次いで言語タグ54を調べる暫定ステップを実行し、このような言語を識別し、次いで適切なライセンス言語エンジン52を選択し、このように識別した言語のライセンス16にアクセスする。当然理解されようが、このようなライセンス言語エンジン52が存在し、ライセンス評価部36にアクセス可能でなければならない。存在しない場合、言語タグ54および/またはDRL48は、このような言語エンジン52を取得する場所56(典型的にウェブ・サイト)を含むことが好ましい。

30

【0119】

典型的に、言語エンジン52は、ハード・ドライブのような、ユーザの計算機14のメモリに常駐する、実行可能ファイルまたは1組のファイルという形態を取る。言語エンジン52は、ライセンス評価部36がDRL48に直接問い合わせを行なう際に補助し、ライセンス評価部36は、仲介役として作用する言語エンジン48等を介して間接的にDRL48に問い合わせを行なう。言語エンジン52を実行すると、RAMのような、ユーザの計算機14のメモリのワーク・スペースにおいて走る。しかしながら、言語エンジン52はその他のいずれの形態でも用いることができ、本発明の精神および範囲から逸脱することはない。

【0120】

40

好ましくは、いずれの言語エンジン52およびいずれのDRL言語も、ライセンス評価部36が、DRL48によって回答されることを期待する、少なくともある数の具体的なライセンスに関する質問に対応するようにする。したがって、ライセンス評価部36は、いずれの特定のDRL言語にも結び付けられていない。DRL48はいずれの適切なDRL言語でも書くことができ、新たなライセンス言語で指定されたDRL48は、既存のライセンス評価部36に、対応する新たな言語エンジン52を取得させることによって、このようなライセンス評価部36が採用することができる。

DRL言語

DRL言語の例を2つ、それぞれのDRL48に具体化した場合について、以下に示す。最初の「簡単な」DRL48は、ライセンス属性を指定するDRL言語で書かれており、

50

一方 2 番目の「スクリプト」DRL 48 は、DRL 48 に指定されているスクリプトにしたがって機能を実行することができる DRL 言語で書かれている。DRL 言語で書かれている場合、各コード行の意味は、その言語規則 (linguistics) および／または以下に続く属性の記述チャートに基づいて明らかにはずである。

単純な DRL 48

【0121】

【表 1】

Simple DRL 48:

<LICENSE>

10

<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>

20

```

<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>
    <PRINCIPAL>
      <TYPE>Person</TYPE>
      <ID>39299482010</ID>
      <NAME>Arnold Blinn</NAME>
      <AUTHTYPE>Authenticate user</AUTHTYPE>
      <AUTHDATA>\\redmond\arnoldb</AUTHDATA>
    </PRINCIPAL>
  </PRINCIPAL>

```

10

20

30

40

```

<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>aaaabbbbccccddddd</ENABLINGBITS>
</DATA>
<SIGNATURE>
<SIGNERNAME>Universal</SIGNERNAME>
  <SIGNERID>9382ABK3939DKD</SIGNERID>
  <HASHALGORITHMID>MD5</HASHALGORITHMID>
  <SIGNALGORITHMID>RSA 128</SIGNALGORITHMID>
  <SIGNATURE>xxxxxxxxxxxxxxxx</SIGNATURE>
  <SIGNERPUBKEY></SIGNERPUBKEY>
  <CONTENTSSIGNEDSIGNERPUBKEY></CONTENTSSIGNEDSIGNERPUBKEY>
</SIGNATURE>
</LICENSE>
【 0 1 2 2 】
【 表 2 】

```

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</TYPE>
    </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>
    <SIGNERPUBKEY></SIGNERPUBKEY>
    <HASHID>MD5</HASHID>
    <SIGNID>RSA 128</SIGNID>
    <SIGNATURE>xxxxxxxxxxxxxxxx</SIGNATURE>
    <CONTENTSSIGNEDSIGNERPUBKEY></CONTENTSSIGNEDSI
    GNERPUBKEY>
</SIGNATURE>
</LICENSE>

```

以上に指定した2つのDRLにおいて、掲示した属性は、以下の記述およびデータ・タイプを有する。

【0123】

【表3】

属性	説明	データ・タイプ
I d	ライセンスの I D	G U I D
名称	ライセンスの名称	ストリング
コンテンツ I d	コンテンツの I D	G U I D
コンテンツ鍵 I d	コンテンツの暗号化鍵の I D	G U I D
コンテンツ名	コンテンツの名称	ストリング
コンテンツ・タイプ	コンテンツのタイプ	ストリング
所有者 I d	コンテンツの所有者の I D	G U I D
所有者名	コンテンツの所有者の名前	ストリング
所有者公開鍵	コンテンツ所有者の公開鍵。これは、コンテンツ所有者のベース－64エンコード公開鍵である	ストリング
ライセンシ I d	ライセンスを得る人の I d。ヌルでもよい。	G U I D
ライセンシ名	ライセンスを得る人の名前。ヌルでもよい。	ストリング
ライセンシ公開鍵	ライセンシの公開鍵これは、ライセンシのベース－64エンコード公開鍵である。ヌルでもよい。	ストリング
説明	人が読める単純なランセンスの説明	ストリング
条件	ライセンスの法的条件。これは法的文書（prose）を含むページへのポインタとすることもできる。	ストリング
有効性終了	ライセンス有効期間終了	日付
有効性発生	ライセンスの有効期間開始	日付
発行日	ライセンスを発行した日付	日付
D R L タイプ	D R L の タイプ 。 例は、"SIMPLE"または"SCRIPT"を含む。	ストリング
D R L データ	D R L に特定なデータ	ストリング
許可ビット	これらのビットは、実際のコンテンツへのアクセスを許可するビットである。これらのビットの解釈は、アプリケーションに委ねられるが、典型的に、これはコンテンツ解読のための秘密鍵である。このデータはベース－64エンコードされて	ストリング

10

20

30

40

	いる。これらのビットは、個々の機械の公開鍵を用いて暗号化されていることを注記しておく。		
署名者 I d	ライセンスに署名した人の I D	GUID	
署名者名	ライセンスに署名した人の名前	ストリング	
署名者公開鍵	ライセンスに署名した人の公開鍵。これは、署名者のベース－64エンコード公開鍵である。	ストリング	10
コンテンツ署名署名者公開鍵	コンテンツ・サーバの秘密鍵によって署名されたライセンスに署名した人の公開鍵。この署名を検証する公開鍵は、コンテンツに暗号化されている。これは、ベース－64エンコードされている。	ストリング	20
ハッシュ A l g I d	ハッシュを生成するために用いるアルゴリズム。これは、"MD5"のようなストリングである。	ストリング	
署名 A l g I d	署名を生成するために用いるアルゴリズム。これは、"RSA128"のようなストリングである。	ストリング	
署名	データの署名。これはベース－64エンコード・データである。	ストリング	30

メソッド

先に論じたように、言語エンジン52およびいずれのDRL言語も、DRL48が回答することをデジタル・ライセンス評価部36が期待する、少なくともある数の特定のライセンスに関する質問に対応することが好ましい。このような対応する質問を認識することは、本発明の精神および範囲から逸脱することなく、あらゆる質問を含むことができ、先にあげた2つのDRL48の例において用いられる用語と一致し、本発明の一実施形態では、このような対応する質問または、以下のような、「メソッド」は「アクセス・メソッド」

40

アクセス・メソッド

アクセス・メソッドは、最上位の属性に対してDRL48に問い合わせるために用いるVARIANT QuarryAttribute (BST R鍵)

有効な鍵は、各々BSTRバリエーションを戻す、Licence.Name, License.Id, Content.Name, Content.Id, Content.Type, Ower.Name, Owner.Id, Owner.PublicKye, Licensee.Name, Licensee.Id, Licensee.PublicKey, Description, およびTerms、ならびに、各々Dateバリエーションを戻すValidity.StartおよびValidity.Endを戻す。

DRLメソッド

以下のDRLメソッドの実装は、各DRL48毎に異なる。DRLメソッドの多くは、'd

50

ata' と称するバリエント・パラメータを含み、D R L 4 8 と一層進んだ情報を交信することを目的とする。これは主に今後の拡張性のためにある。

Boolean IsActivated (バリエント・データ)

このメソッドは、D R L 4 8 / ライセンス 1 6 が活性化しているか否かを示すブール変数を返す。活性化したライセンス 1 6 の一例は、限定動作ライセンス 1 6 であり、最初の再生のときに 4 8 時間だけアクティブとなる。

Activate (バリエント・データ)

このメソッドは、ライセンス 1 6 を活性化するために用いられる。一旦ライセンス 1 6 が活性化されると、不活性化することはできない。

Variant QueryDRL (バリエント・データ)

このメソッドは、一層進んだ D R L 4 8 と通信するために用いられる。これは、主に D R L 4 8 の特徴集合の今後の拡張性に関する。

Variant GetExpires (B S T R アクション、バリエント・データ)

このメソッドは、投入したアクションに関するライセンス 1 6 の満期日を返す。戻り値が N U L L の場合、ライセンスは無期限であると思なされるか、または未だ活性化されていない等のために、未だ満期日を有していない。

Variant GetCount (B S T R アクション、バリエント・データ)

このメソッドは、投入されたアクションの残り動作回数を返す。N U L L が戻された場合、動作は無限回数実行することができる。

Boolean IsEnabled (B S T R アクション、バリエント・データ)

このメソッドは、ライセンス 1 6 が、現時点において要求されているアクションに対応するか否かについて示す。

Boolean IsSunk (B S T R アクション、バリエント・データ)

このメソッドは、ライセンス 1 6 に対して支払が行われたか否かについて示す。前金で支払が済んでいるライセンス 1 6 は T R U E を返し、一方使用時に料金を徴収するライセンス 1 6 のように、前金で支払が済んでいないライセンス 1 6 は、F A L S E を返す。

【0124】

使用許可メソッド

これらのメソッドは、コンテンツを解読する際に用いるライセンス 1 6 を許可するために用いられる。

Boolean Validate (B S T R 鍵)

このメソッドはライセンス 1 6 の妥当性を検査するために用いられる。終了した鍵は、ライセンス 1 6 の署名の妥当性検査に用いる、対応のデジタル・コンテンツ 1 2 の解読鍵 (K D) (即ち、(K D (P U - B B))) によって暗号化された、ブラック・ボックス 3 0 の公開鍵 (P U - B B) である。戻り値が T R U E である場合、ライセンス 1 6 が有効であることを示す。戻り値が F A L S E である場合無効を示す。

int OpenLicense 16 (B S T R アクション、B S T R 鍵、バリエント・データ)

このメソッドは、解読した許可ビットにアクセスする準備のために用いられる。終了した鍵は、前述のように、(K D (P U - B B)) である。戻り値が 0 の場合、成功を示す。他の戻り値を定義することができる。

BSTR GetDecryptedEnablingBits (B S T R アクション、バリエント・データ) Variant GetDecryptedEnablingBitsAsBinary (B S T R アクション、バリエント・データ)

これらのメソッドは、解読した形態の許可ビットにアクセスするために用いられる。これが多数の理由のいずれかのために成功しなかった場合、ヌル・ストリングまたはヌル・バリエントが戻される。

void CloseLicense 16 (B S T R アクション、バリエント・データ)

このメソッドは、終了したアクションを実行するために、許可ビットへのアクセスを解除するために用いられる。これが多数の理由のいずれかのために成功しなかった場合、ヌル・ストリングが戻される。

発見法

10

20

30

40

50

先に論じたように、同じ1片のデジタル・コンテンツ12に対して多数のライセンス16が存在する場合、ライセンス16の1つを選択して用いなければならない。前述のメソッドを用いると、以下の発見法を実施してこのような選択を行なうことができる。即ち、1片のデジタル・コンテンツ12に対してあるアクション（例えば、「再生」）を実行するためには、以下のステップを実行することができる。

【0125】

1. 特定の1片のデジタル・コンテンツ12に適用するライセンス16全てを得る。
2. このようなライセンス16に対してIsEnabled関数をコールすることによってアクションをイネーブルしない各ライセンス16を削除する。

【0126】

3. このようなライセンス16に対してIsActivatedをコールすることによってアクティブでない各ライセンス16を削除する。
4. このようなライセンス16に対してIsSunkをコールすることによって、前金で支払が済んでいない各ライセンスを削除する。

【0127】

5. いずれかのライセンス16が残されている場合、これを用いる。再生回数制限ライセンス16を用いる前に、特に再生回数無制限ライセンス16に満期日がある場合、再生回数無制限ライセンスを用いる。いずれの時点においても、ユーザは、例え選択が価格効率的でないとしても、既に取得してある特定のライセンス16を選択することが許されて当然である。したがって、ユーザは、恐らくDRMシステム32には明白でない判断基準に基づいて、ライセンス16を選択することができる。

【0128】

6. 放置されているライセンス16がある場合、それを示すステータスを戻す。すると、ユーザには、
使用可能であれば、前金で支払が済んでいないライセンス16を用いる、
使用可能であれば、ライセンス16を活性化する、および／または
ライセンス・サーバ24からライセンス取得を実行する、
という選択肢が与えられる。

結論

本発明に関連して実行するプロセスを達成するために必要なプログラミングは、比較的単純であり、関連のあるプログラミング分野の人々には明白であるはずである。したがって、このようなプログラミングをここには添付しない。つまり、本発明を達成するためには、本発明の精神および範囲から逸脱することはなく、いずれの特定のプログラミングでも用いることができる。

【0129】

前述の説明では、本発明は、新規でかつ有用な実施アーキテクチャ10から成り、デジタル・コンテンツ12を制御し任意の形態でレンダリングまたは再生することを可能とし、このような制御は柔軟性があり、このようなデジタル・コンテンツ12のコンテンツ所有者によって定義可能であることがわかる。また、本発明は、デジタル・コンテンツ12が、たとえコンテンツ所有者の制御の下にない計算機14上でレンダリングするにしても、コンテンツ所有者による指定通りにしかデジタル・コンテンツ12をレンダリングしない、新規で有用なレンダリング環境の制御から成る。更に、本発明は、コンテンツ所有者が許可しない方法で、このような計算機14のユーザが1片のデジタル・コンテンツ12にアクセスしようとする試みに対してでさえ、このようなデジタル・コンテンツ12に関して、このような計算機14上でコンテンツ所有者の権利を実施する信頼コンポーネントから成る。

【0130】

尚、本発明の概念から逸脱することなく、上述の実施形態には変更も可能であることは認められよう。したがって、本発明は、開示した特定の実施形態に限定されるのではなく、添付した特許請求の範囲によって規定される本発明の精神および範囲内の変更も包含する

10

20

30

40

50

ことを意図することは理解されよう。

【図面の簡単な説明】

【図 1】 本発明の一実施形態による実施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・ツールのブロック図である。

【図 3】 本発明の一実施形態による図 1 のアーキテクチャと共に用いるデジタル・コンテンツを有するデジタル・コンテンツ・パッケージのブロック図である。

【図 4】 本発明の一実施形態による図 1 のユーザの計算機のブロック図である。

【図 5】 図 5 A は本発明の一実施形態にしたがってコンテンツをレンダリングするための、図 4 の計算機のデジタル権利管理 (D R M) システムと共に実行するステップを示すフロー図である。

10

図 5 B は本発明の一実施形態にしたがってコンテンツをレンダリングするための、図 4 の計算機のデジタル権利管理 (D R M) システムと共に実行するステップを示すフロー図である。

【図 6】 本発明の一実施形態にしたがって、何らかの有効な権限付与ライセンスがあるか否か判定するために、図 4 の D R M システムと共に実行するステップを示すフロー図である。

【図 7】 本発明の一実施形態にしたがってライセンスを取得するために、図 4 の D R M システムと共に実行するステップを示すフロー図である。

【図 8】 本発明の一実施形態にしたがって図 1 のアーキテクチャと共に用いるデジタル使用許諾のブロック図である。

20

【図 9】 本発明の一実施形態にしたがって新たなブラック・ボックスを取得するために、図 4 の D R M システムと共に実行するステップを示すフロー図である。

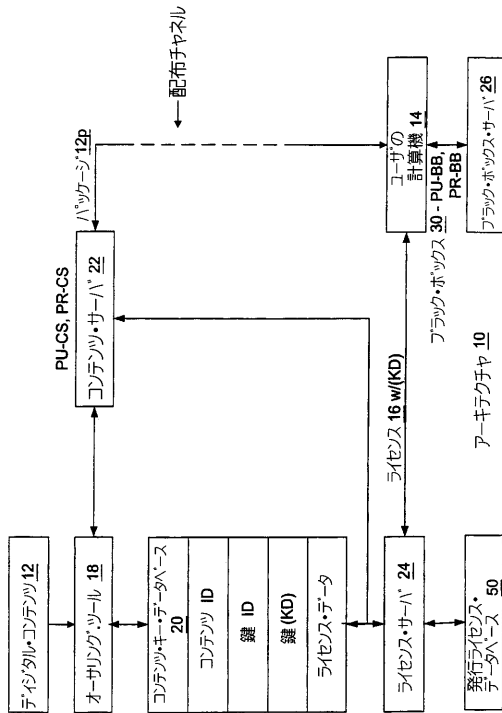
【図 1 0】 本発明の一実施形態にしたがってライセンスおよび 1 片のデジタル・コンテンツの妥当性を検査し、コンテンツをレンダリングするために、図 4 の D R M システムと共に実行する鍵トランザクション・ステップを示すフロー図である。

【図 1 1】 本発明の一実施形態による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 M を解釈する言語エンジンと共に、図 4 のライセンス評価部を示すブロック図である。

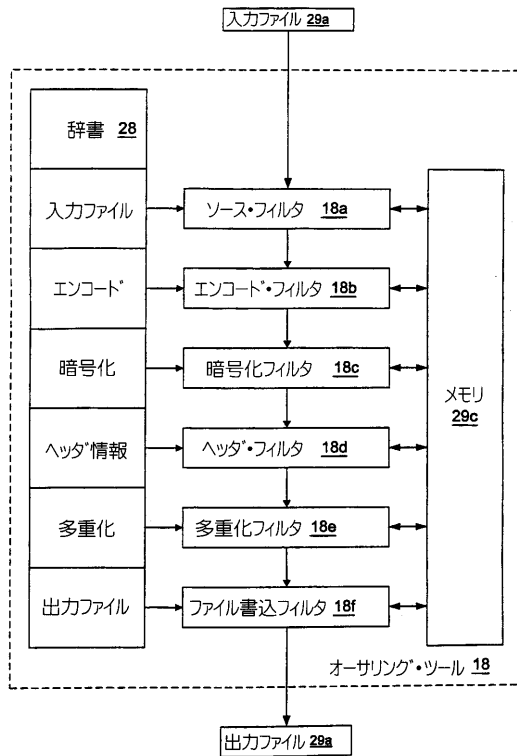
【図 1 2】 本発明の態様および／またはその一部を組み込むことができる汎用コンピュータ・システムを表わすブロック図である。

30

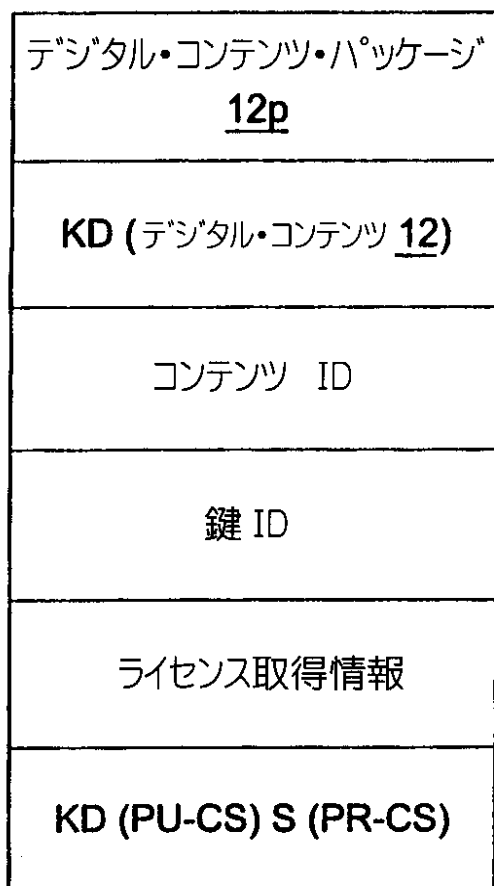
【図 1】



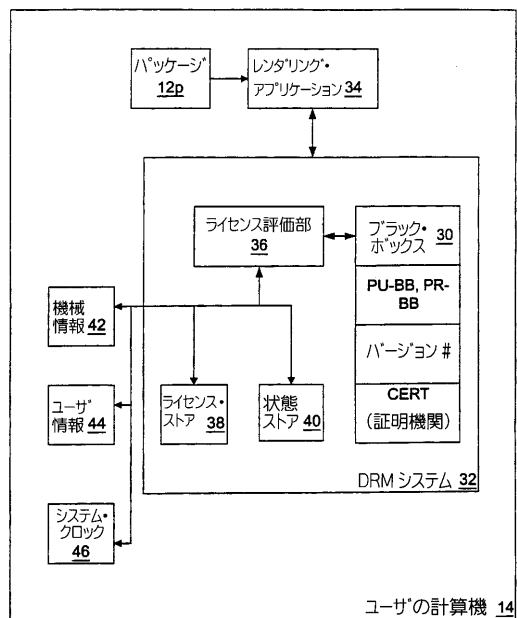
【図 2】



【図 3】



【図 4】



【図 5】

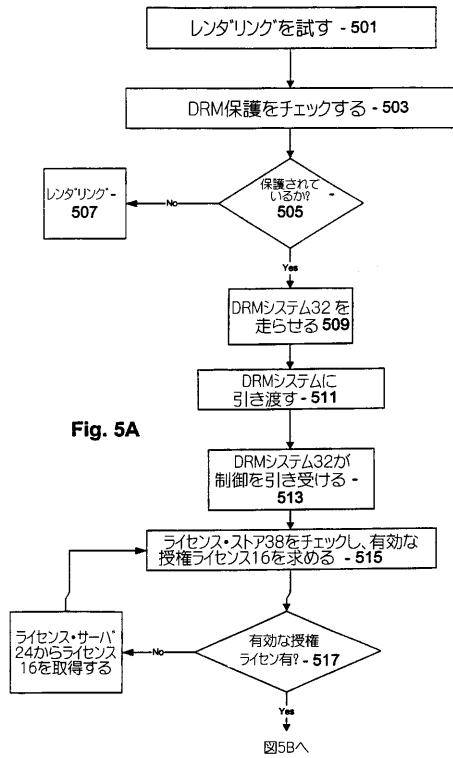
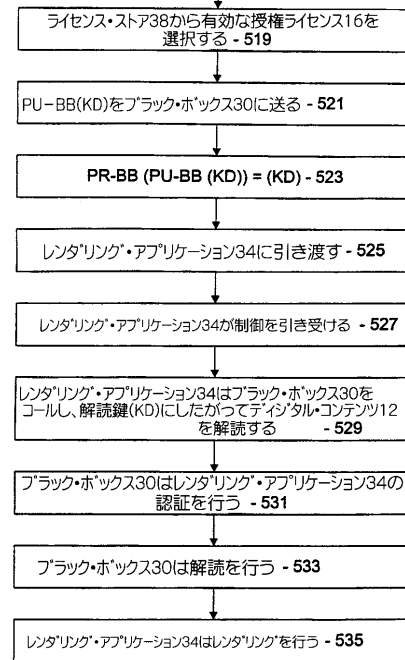
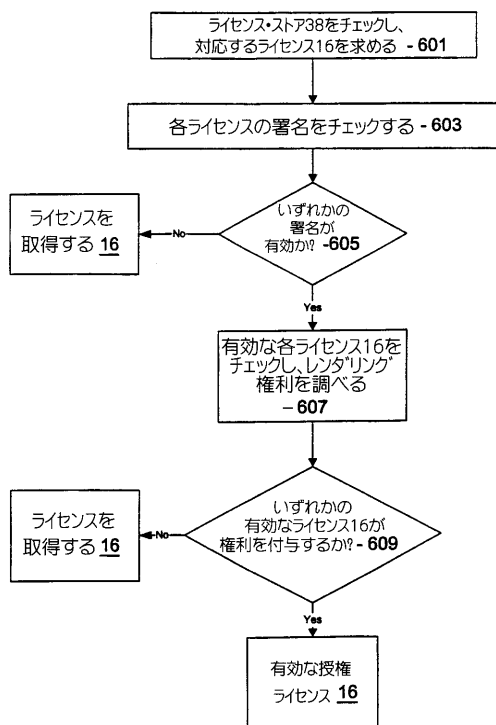


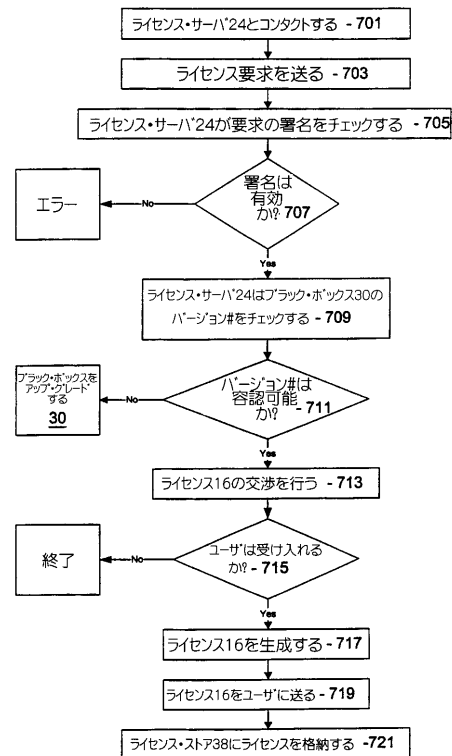
図5Aより



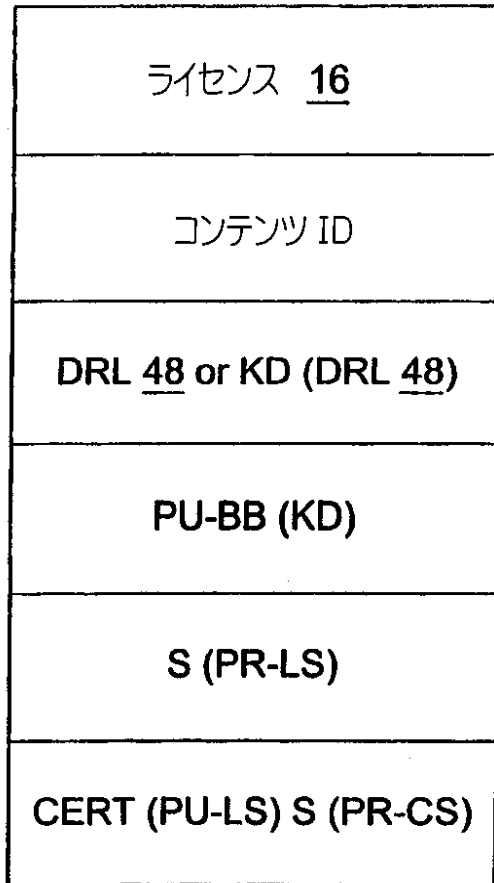
【図 6】



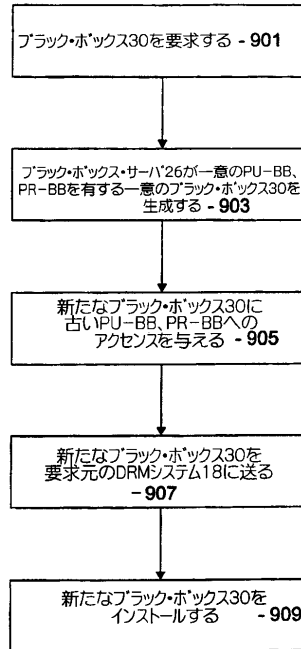
【図 7】



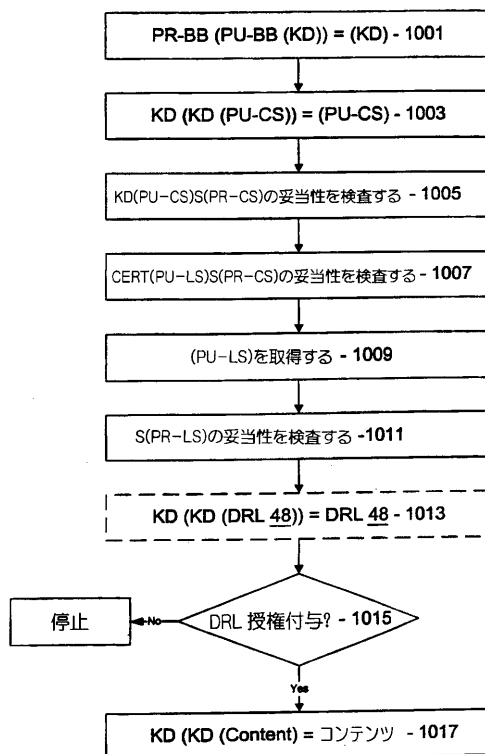
【図 8】



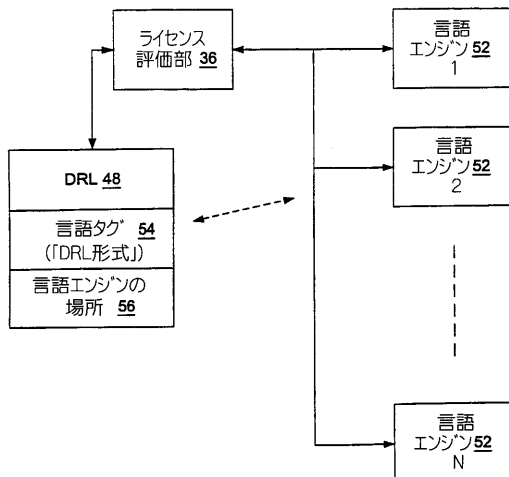
【図 9】



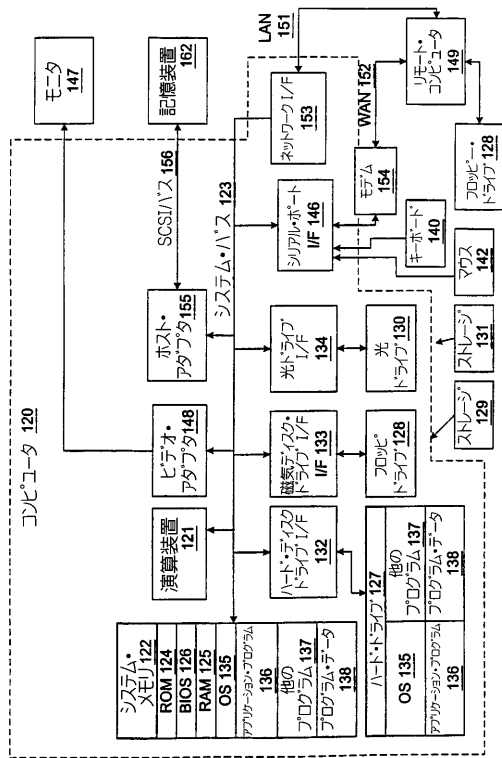
【図 10】



【図 11】



【図 12】



フロントページの続き

- (74)代理人 100147991
弁理士 鳥居 健一
- (72)発明者 ペイナド, マーカス
アメリカ合衆国ワシントン州98007, ベルビュー, ワンハンドレッドフォーティエイトス・ア
ベニュー・ノースイースト 5007, ナンバー イー207
- (72)発明者 アブブリ, ラジャセクハー
アメリカ合衆国ワシントン州98039, メディナ, ノースイースト・テンス・ストリート 78
44
- (72)発明者 ブリン, アーノルド・エヌ
アメリカ合衆国ワシントン州98004, ベルビュー, ノースイースト・トゥエンティセヴンス・
ストリート 9401
- (72)発明者 ジョーンズ, トーマス・シー
アメリカ合衆国ワシントン州98053-3618, レッドモンド, ノースイースト・シックス
・ストリート 23617
- (72)発明者 マンファーデリ, ジョン・エル
アメリカ合衆国ワシントン州98053, レッドモンド, トゥハンドレッドアンドフォーティフィ
フス・ウェイ・ノースイースト 7921
- (72)発明者 ベル, ジェフリー・アール・シー
アメリカ合衆国ワシントン州98013, シアトル, ノース・シックスティセヴンス・ストリート
107
- (72)発明者 ヴェンカテサン, ラマランナム
アメリカ合衆国ワシントン州98052, レッドモンド, ノースイースト・トゥエンティセカンド
・コート 17208
- (72)発明者 イングランド, ポール
アメリカ合衆国ワシントン州98008, ベルビュー, ノースアップ・ウェイ 16659
- (72)発明者 ジャクボウスキ, マリウス・エイチ
アメリカ合衆国ワシントン州98007, ベルビュー, ノースイースト・シックスティーン・プレ
イス 15212, ナンバー 28
- (72)発明者 ユ, ハイ・イン・ヴィンセント
アメリカ合衆国ワシントン州98007, ベルビュー, ワンハンドレッドフォーティフォース・ア
ベニュー・ノースイースト 809, ナンバー シー4

審査官 青柳 光代

- (56)参考文献 特開平10-215242 (JP, A)
特開平10-161937 (JP, A)
特開平10-063364 (JP, A)
特開平08-185444 (JP, A)
特開平09-138827 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
G06Q10/00-50/00