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

特許第5036187号
(P5036187)

(45)発行日　平成24年9月26日(2012.9.26)　(24)登録日　平成24年7月13日(2012.7.13)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
G09C 1/00 (2006.01)　G09C 1/00 640D
H04L 9/00 675D

請求項の数 11　外国語出願　(全 21 頁)

(21)出願番号　特願2006-24792(P2006-24792)
(22)出願日　平成18年2月1日(2006.2.1)
(65)公開番号　特開2006-222951(P2006-222951A)
(43)公開日　平成18年8月24日(2006.8.24)
審査請求日　平成21年1月13日(2009.1.13)
(31)優先権主張番号　11/048,087
(32)優先日　平成17年2月1日(2005.2.1)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(74)復代理人　100115624
弁理士　濱中　淳宏
(74)復代理人　100145388
弁理士　藤原　弘和

最終頁に続く

(54)【発明の名称】コンテンツ権利管理システムにおける、柔軟なライセンス供与アーキテクチャ

(57)【特許請求の範囲】
【請求項１】
コンピューティング装置上のデジタルコンテンツへのアクセスを承認する方法であって、前記デジタルコンテンツは、暗号化されており、かつ、解読鍵（ＫＤ）に従って解読可能であり、
前記コンピューティング装置が、前記デジタルコンテンツに対応するデジタルライセンスを取得するステップであって、前記デジタルライセンスは承認部および解読部を有する前記コンピューティング装置に発行され、
前記承認部は、前記デジタルコンテンツに関連して許可された権利を記述し、前記許可された権利を行使するために満たすべき条件を承認し、前記解読部において特定されたルート信頼機関に戻る証明書のチェーンに基づくデジタル署名を有し、前記ルート信頼機関は、特定の公開／秘密鍵（ＰＵ－ＲＯＯＴ、ＰＲ－ＲＯＯＴ）を有し、
前記解読部は、前記デジタルライセンスが発行されたコンピューティング装置によってのみアクセス可能であり、前記解読鍵（ＫＤ）を有し、前記ルート信頼機関の識別を有し、ルート信頼機関に戻る証明書のチェーンから得られた前記ルート信頼機関の公開鍵（ＰＵ－ＲＯＯＴ）を有する、ステップと、
前記コンピューティング装置が、前記解読部にアクセスするステップと、
前記コンピューティング装置が、前記アクセスした解読部から前記解読鍵および前記公開鍵を取得するステップと、
前記コンピューティング装置が、前記公開鍵を前記デジタル署名に適用することにより

前記承認部のデジタル署名を認証するステップと、
前記コンピューティング装置が、前記承認部の承認条件に基づき前記承認部の権利の行使を許可するかを検証するステップと、
前記コンピューティング装置が、前記解読鍵が使用される前に前記デジタル署名が認証されているか検証するステップと、
前記コンピューティング装置が、前記解読鍵を使用して前記暗号化されたデジタルコンテンツを解読することによって、前記承認部の権利を行使するステップと
を有し、前記コンピューティング装置は、第２の公開／秘密鍵対（ＰＵ－ＵＳＥＲ、ＰＲ－ＵＳＥＲ）を有する前記デジタルライセンスを発行されており、前記解読部は前記第２の前記公開鍵（ＰＵ－ＵＳＥＲ）に従って少なくとも部分的に暗号化され、前記第２の秘密鍵（ＰＲ－ＵＳＥＲ）を前記解読部に適用して前記解読部を解読することにより前記解読部にアクセスするステップをさらに有することを特徴とする方法。
【請求項２】
前記解読部は、前記デジタルライセンスが発行された前記コンピューティング装置により解読可能な形式で少なくとも部分的に暗号化されており、前記コンピューティング装置が前記部分的に暗号化された解読部を解読することにより前記解読部にアクセスするステップをさらに有することを特徴とする請求項１に記載の方法。
【請求項３】
前記解読部は前記デジタルライセンスが発行された前記コンピューティング装置に知られた共有秘密に従って少なくとも部分的に暗号化されており、前記コンピューティング装置が前記部分的に暗号化された解読部を前記共有秘密に従って解読することにより前記解読部にアクセスするステップをさらに有することを特徴とする請求項２に記載の方法。
【請求項４】
前記解読部は満たされるべき条件を有し、前記コンピューティング装置が、前記解読部に記述された前記条件を検証し、前記条件が満たされているか判定するステップをさらに有することを特徴とする請求項２に記載の方法。
【請求項５】
コンピューティング装置上のデジタルコンテンツへのアクセスを承認させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記デジタルコンテンツは、暗号化されており、かつ、解読鍵（ＫＤ）に従って解読可能であり、前記コンピューティング装置に、
前記デジタルコンテンツに対応するデジタルライセンスを取得するステップであって、前記デジタルライセンスは承認部および解読部を有する前記コンピューティング装置に発行され、
前記承認部は、前記デジタルコンテンツに関連して許可された権利を記述し、前記許可された権利を行使するために満たすべき条件を承認し、前記解読部において特定されたルート信頼機関に戻る証明書のチェーンに基づくデジタル署名を有し、前記ルート信頼機関は、特定の公開／秘密鍵（ＰＵ－ＲＯＯＴ、ＰＲ－ＲＯＯＴ）を有し、
前記解読部は、前記デジタルライセンスが発行されたコンピューティング装置によってのみアクセス可能であり、前記解読鍵（ＫＤ）を有し、前記ルート信頼機関の識別を有し、ルート信頼機関に戻る証明書のチェーンから得られた前記ルート信頼機関の公開鍵（ＰＵ－ＲＯＯＴ）を有する、ステップと、
前記解読部にアクセスするステップと、
前記アクセスした解読部から前記解読鍵および前記公開鍵を取得するステップと、
前記公開鍵を前記デジタル署名に適用することにより前記承認部のデジタル署名を認証するステップと、
前記承認部の承認条件に基づき前記承認部の権利の行使を許可するかを検証するステップと、
前記解読鍵が使用される前に前記デジタル署名が認証されているか検証するステップと、

前記解読鍵を使用して前記暗号化されたデジタルコンテンツを解読することによって、前記承認部の権利を行使するステップと、

を実行させ、前記コンピューティング装置は、第２の公開／秘密鍵対（ＰＵ－ＵＳＥＲ、ＰＲ－ＵＳＥＲ）を有する前記デジタルライセンスを発行されており、前記解読部は前記第２の前記公開鍵（ＰＵ－ＵＳＥＲ）に従って少なくとも部分的に暗号化され、前記第２の秘密鍵（ＰＲ－ＵＳＥＲ）を前記解読部に適用して前記解読部を解読するためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６】

前記解読部は前記承認部から分離されていることを特徴とする請求項５に記載のコンピュータ読み取り可能な記録媒体。

【請求項７】

前記承認部は、少なくとも１つの特定のコンピューティング装置または認証部を使用できるコンピューティング装置のタイプ、および、前記特定のコンピューティング装置または前記タイプに関して許可された権利を行使するために満たすべき条件を指定することを特徴とする請求項５に記載のコンピュータ読み取り可能な記録媒体。

【請求項８】

満たされるべき条件を有する前記解読部は、前記承認部において前記デジタル署名が認証された後にのみ、前記解読部内の前記解読鍵が暗号化されたデジタルコンテンツを解読するために使用される条件を含むことを特徴とする請求項５に記載のコンピュータ読み取り可能な記録媒体。

【請求項９】

満たされるべき条件を有する前記解読部は、前記承認部に記述された条件が満たされる場合のみ、前記承認部において許可された権利を行使できる条件を含むことを特徴とする請求項５に記載のコンピュータ読み取り可能な記録媒体。

【請求項１０】

前記解読部は、前記デジタルライセンスが発行された前記コンピューティング装置により解読可能な形式で少なくとも部分的に暗号化されたことを特徴とする請求項５に記載のコンピュータ読み取り可能な記録媒体。

【請求項１１】

前記解読部は、前記デジタルライセンスが発行された前記コンピューティング装置に知られた共有秘密に従って少なくとも部分的に暗号化されたことを特徴とする請求項１０に記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンテンツ権利管理システムにおける、柔軟なライセンス供与アーキテクチャに関し、権利管理（ＲＭ）システムによりデジタルコンテンツに対するアクセスが、対応するデジタルライセンスに従ってのみ提供され、そのようなＲＭシステムに関連して利用される特定のライセンス供与アーキテクチャであって、このアーキテクチャによって各ライセンスは１つまたは複数のルート信頼機関に結び付けてもよく、各ライセンスは実際に複数のライセンス文書を備えてもよいコンテンツ権利管理システムにおける、柔軟なライセンス供与アーキテクチャ。

【背景技術】

【０００２】

権利管理および行使は、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デジタルコンテンツに関連して非常に望ましい。そのようなデジタルコンテンツは１人または複数のユーザに対して配布されうる。デジタルコンテンツは、例えばテキスト文書のように静的であることができ、またはライブイベントのストリームオーディオ／ビデオのようにストリーム化することもできる。一般的な配布モードは、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）等の有形装置、電子掲示板、電子ネットワーク、インターネット等の無形媒体を含む。ユーザが受信する際、そのユーザはデジタルコンテンツを、パーソナルコンピュータまたは他のハードウェア上のオーディオプレイヤー、テキストディスプレイヤー等の適切なレンダリングソフトウェアを用いてレンダリングする。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

ある場合では、著作者、出版者、放送者等のコンテンツオーナーまたは権利オーナーは、そのようなデジタルコンテンツを多くのユーザまたは受信者それぞれに対して、ライセンス料または他の報酬と引き換えに配布することを望む。そのような場合では、コンテンツはオーディオレコーディング、マルチメディアプレゼンテーション等であってよく、ライセンス料を生むことが配布の目的となる。そのようなコンテンツオーナーは、選択権が与えられれば、ユーザがそのような配布されたデジタルコンテンツでできることを制限したいとおそらく思うであろう。例えば、コンテンツオーナーは、少なくともコンテンツオーナーに第２ユーザからのライセンス料を与えない方法でユーザがそのコンテンツをコピーして第２ユーザに再配布することを、制限したいと思う。

【０００４】

さらに、コンテンツオーナーは、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できる柔軟性をユーザに提供し、同時に実際購入された全てのタイプのライセンス条項に関してユーザを束縛したいかもしれない。例えば、コンテンツオーナーは、配布されたデジタルコンテンツが、制限回数だけ、全体で一定の時間だけ、一定のタイプのマシン上でだけ、一定のタイプのレンダリングプラットフォーム上でだけ、一定のタイプのユーザによってのみ等で、レンダリングされるようにしたいかもしれない。

【０００５】

別の場合では、組織の従業員もしくはメンバー等のコンテンツ開発者は、そのようなデジタルコンテンツを組織内の１人または複数の他の従業員もしくはメンバー、または組織外の他の個人に配布したいが、それ以外の者はコンテンツをレンダリングできないようにしたいと思う。この場合において、コンテンツの配布は、ライセンス料または何らかの他の報酬と引き換えでの広範な配布ではなく、機密的または制限的な方法での組織規模のコンテンツ共有により似通っている。

【０００６】

そのような場合では、コンテンツは、例えば職場内で交換されるような文書プレゼンテーション、スプレッドシート、データベース、電子メール等であってよく、コンテンツ開発者は、コンテンツが組織または職場内に留まり、例えば競争相手または敵対者等の、承認していない個人がレンダリングしないことを保証したいと思うかもしれない。ここでもまた、そのようなコンテンツ開発者は受信者がそのような配布されたデジタルコンテンツでできることを制限したいと思う。例えば、コンテンツオーナーは、少なくともそのコンテンツのレンダリングが許可されるべき個人の範囲外にコンテンツを公開することによって、ユーザがそのようなコンテンツをコピーして第２ユーザに再配布することを制限したいと思う。

【０００７】

さらに、コンテンツ開発者は、異なるレベルのレンダリング権を様々な受信者に提供することを望むかもしれない。例えば、コンテンツ開発者は、保護されたデジタルコンテンツを、あるクラスの個人に関しては閲覧可能かつ印刷不可、また別のクラスの個人に関しては閲覧可能かつ印刷可能であるよう許可することを望むかもしれない。

【０００８】

しかしながら、どちらの場合においても、コンテンツが配布されてしまうと、そのようなコンテンツオーナー／開発者は、デジタルコンテンツの制御手段を、たとえ持つとしても、ほとんど持たない。これは、そ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こと、そのような正確なデジタルコピーを書き込み可能な磁気もしくは光ディ

スクにダウンロードすること、またはそのような正確なデジタルコピーをインターネット等のネットワーク上で任意の目的地へ送信することのために必要なソフトウェアおよびハードウェアを、現実的に全てのパーソナルコンピュータが含むという事実から見て特に問題である。

【０００９】

もちろん、コンテンツ配布のトランザクションの一部として、コンテンツオーナー／開発者は、デジタルコンテンツのユーザ／受信者に対し、望ましくない方法でそのようなデジタルコンテンツを再配布しないと約束するよう要求してもよい。しかしながら、そのような約束は簡単になされ、簡単に破られる。コンテンツオーナー／開発者は、通常は暗号化および解読を伴う既知のセキュリティ装置のいずれかを通して、そのような再配布を防ごうと試みてもよい。しかしながら、決心が緩いユーザが暗号化されたデジタルコンテンツを解読し、そのようなデジタルコンテンツを非暗号化形態で保存し、その後同様に再配布するといったことを防ぐことはおそらくほとんどできない。

【００１０】

従って、ＲＭおよび行使のアーキテクチャおよび方法は、任意の形態のデジタルコンテンツを制御された形でレンダリングできるよう提供されており、そのような制御は柔軟で、そのようなデジタルコンテンツのコンテンツオーナー／開発者によって定義可能である。そのようなアーキテクチャによって、上述のいずれかの場合における、制御されたレンダリングが可能になり、容易になる。

【００１１】

一般的には、デジタルライセンスは、例えばデジタル証明書チェーン経由でグローバルまたはグローバルに近いルート信頼機関に結び付けられ、従ってそのようなライセンスを認証／検証したいエンティティは皆、そのようなルート信頼機関に関する適切な情報を保有しなければならない。しかしながら、理解されるべきであるが、落ち度のないエンティティが実際にそのような適切な情報を有さず、従ってそのようにライセンスを認証／検証できないという状況が起こる場合がある。一例では、エンティティがコピーを受信後、情報に変化があったのかもしれない。別の例では、ルート信頼機関が変わったのかもしれない。

【００１２】

いずれの例においても、エンティティを任意の特定のルート信頼機関に依存させ、他のどのルート信頼機関にも関係しないようにするというのは明らかに危険である。本質的には、他のルート信頼機関が存在するようになっても、および特定のルート信頼機関が存在しなくなっても、エンティティは常に特定のルート信頼機関およびその情報に依存する。

【００１３】

従って、デジタルライセンスとその動作を定義する、より柔軟なアーキテクチャに対する必要性が存在する。詳細には、複数のルート信頼機関を可能にし、同様に認証／検証を行うことができる各ルート信頼機関を、ライセンス自体が指定できるようなアーキテクチャに対する必要性が存在する。さらに、そのようなアーキテクチャを有効にするため、複数のライセンス文書を備える新しいタイプのライセンスに対する必要性が存在する。

【課題を解決するための手段】

【００１４】

前述の必要性は、少なくともある程度本発明によって満たされる。本発明においては、コンピューティング装置上のデジタルコンテンツの対応する部分のレンダリングを、デジタルライセンスが承認する。ここでは、コンテンツは暗号化された形態にあり、解読鍵（ＫＤ）に従って解読可能である。ライセンスはユーザに対して発行され、解読部と承認部を有する。

【００１５】

解読部はライセンスを発行されたユーザによってのみアクセス可能で、解読鍵（ＫＤ）と、ルート信頼機関の識別を含む検証情報を有する。承認部は、デジタルコンテンツに関連して許可される権利と、その許可される権利を行使するために満たすべき条件を記述し

、解読部の識別されたルート信頼機関に従って検証されるデジタル署名を有する。

【００１６】

ライセンスを発行されたユーザは、解読部にアクセスし、その中の検証情報を利用して承認部のデジタル署名を検証する。そのようなユーザは、承認部内の条件が承認部の権利の行使を許可する場合にのみ、その権利を行使する。その権利は、解読部からの解読鍵（ＫＤ）を用いて暗号化されたコンテンツを解読し、解読されたコンテンツをレンダリングすることで、行使される。重要なことは、ライセンスをどの特定のルート信頼機関にも結び付ける必要がないということである。

【発明を実施するための最良の形態】

【００１７】

前述の概要は、以下の本発明の実施形態の詳細な記述と同様、添付図面と共に読むと、より良く理解されるであろう。本発明を図示するため、現段階で好ましい実施形態を図面に示している。しかしながら、理解して頂きたいのは、示したとおりの配置および手段に本発明は制限されない。

【００１８】

（コンピュータ環境）

図１および以下の議論は、本発明が実装されうる適切なコンピューティング環境の簡単な一般的記述を提供するよう意図されている。しかしながら、当然のことながらハンドヘルド、ポータブル、および他の全ての種類のコンピューティング装置の、本発明に関連した使用が考慮されている。汎用コンピュータを以下に記述するが、これは１つの例に過ぎず、本発明に必要なのはネットワークサーバ相互運用性および相互作用を有するシンクライアントのみである。従って、本発明は、非常に少ないかまたは最小限のクライアントリソースが関わるネットワークホストサービスの環境、例えば、クライアント装置が単にワールドワイドウェブに対するブラウザまたはインタフェースの役割を果たすようなネットワーク化環境において実装してもよい。

【００１９】

要求はされないが、本発明は、開発者が使用するためのアプリケーションプログラミングインタフェース（ＡＰＩ）を介して実装することができ、および／またはネットワークブラウジングソフトウェア内に含むことができる。ネットワークブラウジングソフトウェアは、クライアントワークステーション、サーバ、もしくは他の装置等の、１つまたは複数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等のコンピュータ実行可能命令の一般的なコンテキストで記述される。通常、プログラムモジュールは、特定のタスクを行うか、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造等を含む。一般的に、プログラムモジュールの機能性は、様々な実施形態において望ましいように結合または分散してもよい。さらに、本発明は他のコンピュータシステム構成でも実施してもよいことを、当業者は理解するであろう。本発明とともに使用するのに適切でありうる他の既知のコンピューティングシステム、環境、および／または構成は、これらに限らないが、パーソナルコンピュータ（ＰＣ）、現金自動預入支払機、サーバコンピュータ、ハンドヘルドまたはラップトップ装置、マルチプロセッサシステム、マイクロプロセッサベースシステム、プログラム可能家庭用電化製品、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む。本発明は、通信ネットワークまたは他のデータ伝送媒体を通してリンクされるリモートプロセッシング装置がタスクを行う、分散コンピューティング環境内で実施してもよい。分散コンピューティング環境において、プログラムモジュールは、メモリストレージ装置を含むローカルコンピュータストレージ媒体およびリモートコンピュータストレージ媒体の両方にあってもよい。

【００２０】

図１はこのように本発明が実装されうる適切なコンピューティングシステム環境の例１００を示す。しかしながら上記で明確にしたように、コンピューティングシステム環境１００は適切なコンピューティング環境の一例でしかなく、本発明の使用または機能性の範

囲に関していかなる制限をも示唆するものではない。コンピューティング環境１００は、例示的な動作環境１００内に図示されたコンポーネントのどの１つまたはどの組み合わせに関しても、いかなる依存性もいかなる要求事項も有しないと解釈すべきである。

【００２１】

図１を参照すると、本発明を実装する例示的システムは、コンピュータ１１０の形態の汎用コンピューティング装置を含む。コンピュータ１１０のコンポーネントは、これらに限らないが、処理装置１２０、システムメモリ１３０、およびシステムメモリを含む様々なシステムコンポーネントを処理装置１２０に結合するシステムバス１２１を含む。システムバス１２１は、メモリバスまたはメモリコントローラ、周辺バス、および任意の様々なバスアーキテクチャを使用するローカルバスを含む、いくつかのタイプのバス構造のいずれであってもよい。一例としては、これに限らないが、そのようなアーキテクチャは、業界標準アーキテクチャ（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（ＭＣＡ）バス、拡張ＩＳＡ（ＥＩＳＡ）バス、ビデオ電子規格協会（ＶＥＳＡ）ローカルバス、周辺コンポーネント相互接続（ＰＣＩ）バス（メザニンバスとしても知られる）を含む。

【００２２】

コンピュータ１１０は、一般的に、様々なコンピュータ読み取り可能媒体を含む。コンピュータ読み取り可能媒体はコンピュータ１１０によってアクセス可能な任意の利用可能な媒体であることができ、揮発性および不揮発性媒体、取り外し可能および固定の媒体の両方を含む。限定するためではなく、例として、コンピュータ読み取り可能媒体はコンピュータストレージ媒体および通信媒体を含んでよい。コンピュータストレージ媒体は、コンピュータ読み取り可能命令、データ構造、プログラムモジュールまたは他のデータ等の情報を格納する任意の方法または技術で実装される、揮発性および不揮発性、取り外し可能および固定の媒体の両方を含む。コンピュータストレージ媒体は、これらに限らないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤＲＯＭ、デジタル多用途ディスク（ＤＶＤ）もしくは他の光ディスクストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ストレージ装置、または所望情報を格納するために使用可能で、コンピュータ１１０によってアクセス可能な任意の他の媒体を含む。通信媒体は、一般的に、コンピュータ読み取り可能命令、データ構造、プログラムモジュールまたは他のデータを、搬送波もしくは他のトランスポート機構等の変調データ信号に具現し、任意の情報配送媒体を含む。“変調データ信号”という用語は、信号の特性の１つまたは複数を、信号内の情報を符号化する方法で設定または変えられた信号を意味する。例として、これらに限らないが、通信媒体は、有線ネットワークまたは直接有線接続等の有線媒体と、音響、ＲＦ、赤外線および他の無線媒体等の無線媒体を含む。上記の任意の組み合わせも、コンピュータ読み取り可能媒体の範囲内に含むべきである。

【００２３】

システムメモリ１３０は、コンピュータストレージ媒体を、読取専用メモリ（ＲＯＭ）１３１およびランダムアクセスメモリ（ＲＡＭ）１３２等の揮発性および／または不揮発性メモリの形態で含む。例えば起動時にコンピュータ１１０内の要素間の情報転送を補助する基本ルーチンを含む、基本入力／出力システム１３３（ＢＩＯＳ）は、一般的に、ＲＯＭ１３１に格納される。ＲＡＭ１３２は、一般的に、即座にアクセス可能な、および／または処理装置１２０によって現在動作中のデータおよび／またはプログラムモジュールを含む。例として、これらに限らないが、図１はオペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６およびプログラムデータ１３７を示す。

【００２４】

コンピュータ１１０は、他の取り外し可能／固定の、揮発性／不揮発性コンピュータストレージ媒体を含んでもよい。例としてのみ図１に示されているのは、取り外し不可能、不揮発性磁気媒体へ読み書きするハードディスクドライブ１４１、取り外し可能、不揮発性磁気ディスク１５２へ読み書きする磁気ディスクドライブ１５１、およびＣＤ－ＲＯＭ

または他の光媒体等の取り外し可能、不揮発性光ディスク１５６へ読み書きする光ディスクドライブ１５５である。例示的動作環境で使用できる他の取り外し可能／固定の、揮発性／不揮発性コンピュータストレージ媒体は、これらに限らないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、半導体ＲＡＭ、半導体ＲＯＭ等を含む。ハードディスクドライブ１４１は、インタフェース１４０等の固定のメモリインタフェースを通してシステムバス１２１に一般的に接続され、磁気ディスクドライブ１５１と光ディスクドライブ１５５は、インタフェース１５０等の取り外し可能メモリインタフェースによってシステムバス１２１に一般的に接続される。

【００２５】

上述する、図１に示されるドライブとそれに関連するコンピュータストレージ媒体は、コンピュータ１１０に対してコンピュータ読み取り可能命令、データ構造、プログラムモジュールおよび他のデータのストレージを提供する。図１において、例えば、ハードディスクドライブ１４１は、オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６およびプログラムデータ１４７を格納するとして示されている。これらのコンポーネントは、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７と同じであってもよいし、異なってもよいことに留意されたい。オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７は、最小限、それらが異なるコピーであることを図示するために、ここでは異なった番号が与えられている。ユーザは、キーボード１６２および、マウス、トラックボールまたはタッチパッドと通例呼ばれるポインティング装置１６１等の入力装置を通してコンピュータ１１０に命令および情報を入力してもよい。他の入力装置(不図示）は、マイクロフォン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナ等を含んでよい。これらおよび他の入力装置は、システムバス１２１に結合されるユーザ入力インタフェース１６０を通して処理装置１２０に接続されることが多いが、パラレルポート、ゲームポートまたはユニバーサルシリアルバス（ＵＳＢ）等の他のインタフェースおよびバス構造によって接続されてもよい。

【００２６】

モニタ１９１または他のタイプの表示装置も、ビデオインタフェース１９０等のインタフェースを介してシステムバス１２１に接続される。ノースブリッジ等のグラフィクスインタフェース１８２も、システムバス１２１に接続してもよい。ノースブリッジは、ＣＰＵまたはホスト処理装置１２０と通信するチップセットで、アクセラレイテッドグラフィクスポート（ＡＧＰ）通信を行う。１つまたは複数のグラフィクス処理装置（ＧＰＵ）１８４はグラフィクスインタフェース１８２と通信してもよい。この点について、ＧＰＵ１８４は、通常、レジスタストレージ等のオンチップメモリストレージを含み、ＧＰＵ１８４はビデオメモリ１８６と通信する。しかしながらＧＰＵ１８４は、コプロセッサの一例に過ぎず、従って様々なコプロセッシング装置をコンピュータ１１０内に含んでよい。モニタ１９１または他のタイプの表示装置も、ビデオインタフェース１９０等のインタフェースを介してシステムバス１２１に接続され、ビデオメモリ１８６と順に通信してもよい。モニタ１９１に加えて、コンピュータはスピーカ１９７およびプリンタ１９６等の他の周辺出力装置も含んでよく、それらは出力周辺インタフェース１９５を通して接続してもよい。

【００２７】

コンピュータ１１０は、リモートコンピュータ１８０等の１つまたは複数のリモートコンピュータに対する論理接続を使用して、ネットワーク化環境で動作してもよい。リモートコンピュータ１８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピア装置または他の共通ネットワークノードであってよく、図１ではメモリストレージ装置１８１のみを示しているが、コンピュータ１１０に関して上述した多くのまたは全ての要素を一般的に含む。図１に描かれている論理接続は、ローカルエリアネットワーク（ＬＡＮ）１７１および広域ネットワーク（ＷＡＮ）１７３を含むが、他のネットワークも

含んでよい。そのようなネットワーキング環境は職場、企業規模のコンピュータネットワーク、イントラネットおよびインターネットにおいて普通である。

【００２８】

ＬＡＮネットワーキング環境で使用するとき、コンピュータ１１０はＬＡＮ１７１にネットワークインタフェースまたはアダプタ１７０を通して接続される。ＷＡＮネットワーキング環境で使用するとき、コンピュータ１１０は一般的に、モデム１７２またはインターネット等のＷＡＮ１７３上の通信を確立するための他の手段を含む。モデム１７２は、内臓であっても外付けであってもよく、ユーザ入力インタフェース１６０または他の適切なメカニズムを介してシステムバス１２１に接続してもよい。ネットワーク化環境においては、コンピュータ１１０に関して描かれ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一部はリモートメモリストレージ装置に格納してもよい。限定するためではなく、例として、図１は、メモリ装置１８１上にあるとしてリモートアプリケーションプログラム１８５を示す。当然のことながら、示したネットワーク接続は例示的であり、コンピュータ間の通信リンクを確立する他の手段を使用してもよい。

【００２９】

コンピュータ１１０または他のクライアント装置をコンピュータネットワークの一部として配置できることを、当業者は理解できる。この点について、本発明は、任意の数のメモリまたはストレージユニットと、任意の数のストレージユニットまたはボリュームに渡って発生する任意の数のアプリケーションおよびプロセスを有する、任意のコンピュータシステムに関する。本発明は、ネットワーク環境に配置されたサーバコンピュータおよびクライアントコンピュータを伴う環境に適用してよく、サーバコンピュータおよびクライアントコンピュータは、リモートまたはローカルストレージを有する。本発明は、プログラミング言語の機能性、プログラミング言語を解釈および実行する能力を有する独立コンピューティング装置に適用してもよい。

【００３０】

分散コンピューティングは、コンピューティング装置およびシステム間の直接的なやりとりによって、コンピュータリソースおよびサービスの共有を容易にする。これらのリソースおよびサービスは、情報交換、キャッシュストレージ、およびファイルに対するディスクストレージを含む。分散コンピューティングは、ネットワーク接続性を活かすことにより、クライアントがその集団的能力を活用することを可能にし、企業全体に利益をもたらす。この点について、様々な装置は、信頼できるグラフィックパイプラインに対する本発明の認証技術を関与させるために相互作用できる、アプリケーション、オブジェクトまたはリソースを有してもよい。

【００３１】

図２は、例示的なネットワーク化または分散コンピューティング環境の概略図を提供する。分散コンピューティング環境は、コンピューティングオブジェクト１０ａ、１０ｂ等、およびコンピューティングオブジェクトまたは装置１１０ａ、１１０ｂ、１１０ｃ等を備える。これらのオブジェクトはプログラム、メソッド、データストア、プログラム可能ロジック等を備えてよい。これらのオブジェクトは、ＰＤＡ、テレビ、ＭＰ３プレイヤー、テレビ、パーソナルコンピュータ等の同じまたは異なる装置の一部を備えてよい。各オブジェクトは、通信ネットワーク１４を経由して別のオブジェクトと通信できる。このネットワーク自体は、図２のシステムにサービスを提供する他のコンピューティングオブジェクトおよびコンピューティング装置を備えてよい。本発明の一態様に従って、各オブジェクト１０または１１０は、信頼できるグラフィックパイプラインに対する本発明の認証技術を要求するかもしれないアプリケーションを含んでもよい。

【００３２】

当然のことながら、１１０ｃ等のオブジェクトを、別のコンピューティング装置１０または１１０上にホスティングしてもよい。従って、描かれた物理的環境はコンピュータ等の接続された装置を示すかもしれないが、そのような図示は単に例示的なものであり、その物理的環境は、それに代わって、ＰＤＡ、テレビ、ＭＰ３プレイヤー等の様々なデジタ

ル装置、インタフェース、ＣＯＭオブジェクト等のソフトウェアオブジェクトを備えるものとして描写または記述してもよい。

【００３３】

分散コンピューティング環境をサポートする様々なシステム、コンポーネント、およびネットワーク構成がある。例えば、コンピューティングシステムは、有線または無線システムによって、ローカルネットワークまたは広域分散ネットワークによってともに接続されてもよい。現在は、ネットワークの多くはインターネットに結合され、インターネットは、広域分散コンピューティングに対するインフラストラクチャを提供し、多くの異なるネットワークを包含する。

【００３４】

ホームネットワーキング環境では、少なくとも４つの異なるネットワークトランスポート媒体があり、それぞれが、電力線、データ（無線および有線両方の）、音声（例えば、電話）およびエンターテインメントメディア等の一意のプロトコルをサポートできる。ライトのスイッチおよび電気器具等の家庭用制御装置のほとんどは、接続のために電力線を使用できる。データサービスはブロードバンド（例えば、ＤＳＬまたはケーブルモデムのいずれか）として家庭内に入ることができ、無線（例えば、ホームＲＦまたは８０２．１１ｂ）または有線（例えば、ホームＰＮＡ、Ｃａｔ５、電力線）接続を使用して屋内でアクセス可能である。音声トラフィックは有線（例えば、Ｃａｔ３）または無線（例えば、携帯電話）として家庭内に入ることができ、Ｃａｔ３ワイヤリングを使用して屋内で配布することができる。エンターテインメントメディアは衛星またはケーブルを通して家庭内に入ることができ、一般的に同軸ケーブルを使用して屋内で配布される。ＩＥＥＥ１３９４およびＤＶＩも、メディア装置のクラスタに対するデジタル相互接続として現れてきている。これらのネットワーク環境の全ておよび、プロトコル標準として現れうる他のネットワーク環境は、相互接続してイントラネットを形成してもよく、イントラネットをインターネット経由で外部に接続してもよい。つまり、様々な異なるソースがデータの格納と伝送に対して存在し、その結果、さらに進むと、コンピューティング装置はデータ処理パイプラインの全ての部分でコンテンツを保護する方法を必要とするだろう。

【００３５】

“インターネット”は、通例、ＴＣＰ／ＩＰプロトコル一式を利用する、ネットワークおよびゲートウェイの集合を指し、コンピュータネットワーキング業界で良く知られている。ＴＣＰ／ＩＰは“Ｔｒａｎｓｐｏｒｔ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｆａｃｅ　Ｐｒｏｇｒａｍ”の頭字語である。インターネットは、地理的に分散したリモートコンピュータネットワークのシステムとして記述でき、そのリモートコンピュータネットワークは、ユーザがネットワーク上で情報をやり取りし共有できるネットワーキングプロトコルを実行するコンピュータによって相互接続されたものである。そのような広範囲の情報共有のために、インターネット等のリモートネットワークは、これまで通常オープンシステムに発展し、このオープンシステム用に、開発者は専門化した動作またはサービスを行うソフトウェアアプリケーションを本質的に制限なしで設計できる。

【００３６】

従って、そのネットワークインフラストラクチャによって、クライアント／サーバ、ピアツーピア、またはハイブリッドアーキテクチャ等の多数のネットワークトポロジが可能になる。“クライアント”は、あるクラスまたはグループのメンバーであり、自分に関係のない別のクラスまたはグループのサービスを使用する。従って、コンピューティングにおいて、クライアントは、プロセス即ち、大まかに言うと命令またはタスクの集合であり、別のプログラムが提供するサービスを要求する。クライアントプロセスは要求したサービスを利用し、他のプログラムまたはサービス自体についての作業の詳細を何ら“知る”必要はない。クライアント／サーバアーキテクチャ、特にネットワーク化システムにおいてクライアントは、普通、例えばサーバ等の別のコンピュータが提供する共有ネットワークリソースにアクセスするコンピュータである。図２の例において、コンピュータ１１０ａ、１１０ｂ等は、クライアントと考えることができ、コンピュータ１０ａ、１０ｂ等は

、サーバと考えることができる。サーバ１０ａ、１０ｂ等は、データを維持し、そのデータをクライアントコンピュータ１１０ａ、１１０ｂ等で複製する。

【００３７】

サーバは、一般的に、インターネット等のリモートネットワーク上でアクセス可能なリモートコンピュータシステムである。クライアントプロセスは第１コンピュータシステム内で、サーバプロセスは第２コンピュータシステム内で、それぞれアクティブであることができ、互いに通信媒体上で通信することによって、分散機能性を提供し、複数のクライアントがサーバの情報収集能力を利用できるようにする。

【００３８】

クライアントおよびサーバは、プロトコル層が提供する機能性を利用して互いに通信する。例えば、ハイパーテキスト転送プロトコル（ＨＴＴＰ）は、ワールドワイドウェブ（ＷＷＷ）と併せて使用される共通プロトコルである。一般的に、ユニバーサルリソースロケータ（ＵＲＬ）等のコンピュータネットワークアドレス、またはインターネットプロトコル（ＩＰ）アドレスを使用して、サーバまたはクライアントコンピュータを互いに識別する。ネットワークアドレスは、ユニバーサルリソースロケータアドレスと呼ぶことができる。例えば、通信は通信媒体上で提供できる。詳細には、クライアントおよびサーバは、大容量通信用のＴＣＰ／ＩＰ接続を介して、互いに結合してもよい。

【００３９】

このように、図２は、サーバがクライアントコンピュータとネットワーク／バスを介して通信する、例示的なネットワーク化または分散環境を示しており、この環境の中で本発明を利用してもよい。より詳細には、多数のサーバ１０ａ、１０ｂ等が、通信ネットワーク／バス１４を介して、ポータブルコンピュータ、ハンドヘルドコンピュータ、シンクライアント、ネットワーク化機器などの多数のクライアントまたはリモートコンピューティング装置１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ等、またはＶＣＲ、ＴＶ、オーブン、ライト、ヒータ等といった他の装置と、本発明に従って相互接続される。通信ネットワーク／バス１４は、ＬＡＮ、ＷＡＮ、イントラネット、インターネット等であってよい。このように、本発明は、任意のコンピューティング装置に適用してよく、それと共に信頼できるソースからの安全なコンテンツを処理、格納またはレンダリングすることが望ましいと考えられる。

【００４０】

通信ネットワーク／バス１４が、例えばインターネットであるネットワーク環境において、サーバ１０はウェブサーバであることができ、そのウェブサーバとクライアント１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅ等は、ＨＴＴＰ等の多数の既知のプロトコルのうち任意のものを介して通信する。サーバ１０は、分散コンピューティング環境の特徴であるように、クライアント１１０の役割も果たしてもよい。通信は、適切な場合には、有線であっても無線であってもよい。クライアント装置１１０は通信ネットワーク／バス１４を介して通信してもしなくてもよく、それに関連する独立した通信を有してもよい。例えば、ＴＶまたはＶＣＲの場合は、その制御に対してネットワーク化された態様があってもなくてもよい。各クライアントコンピュータ１１０およびサーバコンピュータ１０は、様々なアプリケーションプログラムモジュールもしくはオブジェクト１３５ａ～ｅ、および様々なタイプのストレージ要素もしくはオブジェクトに対する通信もしくはアクセスを装備してもよい。このストレージ要素もしくはオブジェクト内全体にてファイルを格納してもよく、またはファイルの一部（複数または単数）をそれらにダウンロードもしくは移動させてもよい。このように、本発明は、コンピュータネットワーク／バス１４にアクセスでき、それと相互作用できるクライアントコンピュータ１１０ａ、１１０ｂ等と、クライアントコンピュータ１１０ａ、１１０ｂ等と相互作用することのできるサーバコンピュータ１０ａ、１０ｂ等と、他の装置１１１およびデータベース２０を有するコンピュータネットワーク環境において利用することができる。

【００４１】

（権利管理（ＲＭ）の概観）

既知のように、図３を参照すると、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デジタルコンテンツ３２に関連して、そのようなデジタルコンテンツ３２がユーザに配布される場合、権利管理（ＲＭ）および行使は非常に望ましい。ユーザはデジタルコンテンツ３２を受信すると、パーソナルコンピュータ３４等のメディアプレイヤー、テキストディスプレイヤー等の適切なレンダリング装置を用いて、それをレンダリングする。

【００４２】

一般的には、そのようなデジタルコンテンツ３２を配布するコンテンツオーナーまたは開発者（以下、“オーナー”という）は、ユーザがそのような配布されたデジタルコンテンツ３２でできることを制限することを望む。例えば、コンテンツオーナーは、ユーザがそのようなコンテンツ３２をコピーして第２ユーザに再配布することを制限したいかもしれず、または配布されたデジタルコンテンツ３２のレンダリングを、例えば、制限回数だけ、全体で一定の時間だけ、一定のタイプのマシン上でだけ、一定のタイプのレンダリングプラットフォーム上でだけ、一定のタイプのユーザでだけ等の条件で、許可したいかもしれない。

【００４３】

しかしながら、配布後に、そのようなコンテンツオーナーはデジタルコンテンツ３２に対する制御手段を、ほとんど有しない。そこで、ＲＭシステム３０は、任意形態のデジタルコンテンツ３２の制御されたレンダリングを許可する。ＲＭシステム３０では、そのような制御は柔軟で、そのようなデジタルコンテンツのコンテンツオーナーによって定義可能である。一般的に、コンテンツ３２はパッケージ３３の形態で、任意の適切な配布チャネルを経由してユーザに配布される。デジタルコンテンツパッケージ３３は、対称の暗号化／解読鍵（ＫＤ）（即ち、（ＫＤ（ＣＯＮＴＥＮＴ））で暗号化されたデジタルコンテンツ３２、および、コンテンツを識別する他の情報、そのようなコンテンツに対するライセンスの獲得方法等を含むことができる。

【００４４】

信頼ベースのＲＭシステム３０により、デジタルコンテンツ３２のオーナーは、そのようなデジタルコンテンツがユーザのコンピューティング装置３４上でレンダリングを許可される前に満たすべきライセンスルールを指定することができる。そのようなライセンスルールは、前述の時間的要件を含むことができ、デジタルライセンスまたは使用ドキュメント（以下、“ライセンス”という）３６内で、具現化してもよい。ライセンス３６は、ユーザ／ユーザのコンピューティング装置３４（以下、この用語は状況が別途要求しない限り、交換可能である）がコンテンツオーナーまたはそのエージェントから取得しなければならない。そのようなライセンス３６は、おそらくユーザのコンピューティング装置３４により解読可能な鍵に従って暗号化された、デジタルコンテンツを解読するための解読鍵（ＫＤ）も含む。図３に見られるように、そのような暗号化鍵はユーザのコンピューティング装置３４の公開鍵（ＰＵ－ＢＢ）であり、ユーザのコンピューティング装置３４は、おそらく（ＰＵ－ＢＢ（ＫＤ））を解読する、対応する秘密鍵（ＰＲ－ＢＢ）を有する。

【００４５】

デジタルコンテンツ３２の一部分に対するコンテンツオーナーは、ライセンス３６内のそのようなコンテンツオーナーが指定したルールおよび要件にユーザのコンピューティング装置３４が従うこと、即ちライセンス３６内のルールおよび要件を満たさない限り、デジタルコンテンツ３２はレンダリングされないことを信じなければならない。好ましくは、ユーザのコンピューティング装置３４に、信頼できるコンポーネントまたはメカニズム３８を提供する。そのコンポーネントまたはメカニズム３８は、デジタルコンテンツ３２に関連しユーザが取得したライセンス３６内で具現化したライセンスルールに従わない限りデジタルコンテンツ３２をレンダリングしない。

【００４６】

信頼できるコンポーネント３８は、一般的にライセンス評価部４０を有し、このライセ

ンス評価部４０は、ライセンス３６が有効か否かを判定し、そのような有効なライセンス３６内のライセンスルールおよび要件を検討し、検討したライセンスルールおよび要件に基づいて、要求しているユーザが要求されたデジタルコンテンツ３２を、特に求められた方法でレンダリングする権利を有するか否かを判定する。理解されるべきであるが、ＲＭシステム３０において、ライセンス評価部４０はデジタルコンテンツ３２のオーナーの望みをライセンス３６内のルールおよび要件に従って実行すると信頼されており、ユーザは、不正であるないにかかわらず、いかなる目的のためでもそのような信頼された要素を容易に変更できるべきではない。

【００４７】

理解されるべきであるが、ライセンス３６内のルールおよび要件は、ユーザがデジタルコンテンツ３２をレンダリングする権利を有するか否かを任意のいくつかの要因に基づいて指定することができる。このような要因は、ユーザが誰か、ユーザがどこにいるか、どんなタイプのコンピューティング装置をユーザが使用しているか、どんなレンダリングアプリケーションがＲＭシステム３０を呼び出しているか、日付、時間等を含む。さらに、ライセンス３６のルールおよび要件は、ライセンス３６を、例えば所定の回数のレンダリング、または所定のレンダリング時間に限定してもよい。従って、信頼できるコンポーネント３８は、コンピューティング装置３４上のクロック４２を参照する必要があるかもしれない。

【００４８】

ルールおよび要件を、任意の適切な言語および構文に従ってライセンス３６で指定してもよい。例えば、言語は満たすべき属性および値を単純に指定してもよく（例えば、ＤＡＴＥはＸより後でなければならない、等）、指定したスクリプトに従った機能の遂行を要求してもよい（例えば、ＤＡＴＥがＸより大きければ、．．．せよ、等）。

【００４９】

ライセンス３６が有効で、かつユーザがそのライセンスのルールおよび要件を満たすとライセンス評価部４０が判定すると、デジタルコンテンツ３２はレンダリングできる。詳細には、コンテンツ３２をレンダリングするために、解読鍵（ＫＤ）をライセンス３６から取得し、その解読鍵をコンテンツパッケージ３３からの（ＫＤ（ＣＯＮＴＥＮＴ））に適用すると、実際のコンテンツ３２となり、次に、実際のコンテンツ３２をレンダリングする。

【００５０】

上述のように、（ＰＵ－ＢＢ（ＫＤ））を有するライセンス３６は、実質的に、（ＰＲ－ＢＢ）を保有するエンティティに対して、（ＫＤ）にアクセスし、それにより、そのような（ＫＤ）に従って暗号化されたコンテンツ３２にアクセスする権限を与える。もちろん、そのエンティティはライセンス３６に記述された全ての条件に従うと仮定してのことである。しかしながら、理解されるべきであるが、他のタイプのライセンス３６がＲＭシステム３０内に存在してもよい。

【００５１】

当然のことながら、例えば、ある場合ではコンテンツ３２の著作者または出版者４４は、特定のライセンサ４６にパブリッシングライセンス３６Ｐを提供することによって、対応するコンテンツ３２に対するライセンス３６を発行する権限をそのライセンサ４６に与えてもよい。理解されるように、そのようなパブリッシングライセンス３６Ｐは、この場合はライセンサの公開鍵（ＰＵ－ＢＢ）に従って暗号化されたデジタルコンテンツ３２を解読するための解読鍵（ＫＤ）をおそらく含むという点で、ライセンス３６と類似している。同様に、パブリッシングライセンス３６Ｐは、コンテンツ３２をレンダリングするためのルールおよび要件をおそらく含む。しかしながら、ここでは、そのようなルールおよび要件は、ライセンサ４６が発行するときにライセンス３６に挿入することになり、ライセンサ４６に特に適用可能というわけではない。

【００５２】

しかしながら、パブリッシングライセンス３６Ｐは、ライセンサ４６に実際に適用可能

な他のルールおよび要件を実際に含んでもよいことに留意されたい。従って、ライセンサ４６は、ユーザのコンピューティング装置３４と類似の方法で、ライセンス評価部４０を有する信頼できるコンポーネント３８を含むべきである。

【００５３】

重要なことは、ライセンス３６、３６Ｐ等の各タイプは、提供されたときに一般的に認証／検証の目的でデジタル署名を含み、各デジタル署名は、ルート信頼機関からのデジタル証明書または、そのようなルート信頼機関に戻る一連のそのようなデジタル証明書に関して検証される。とりわけ、各証明書は認証／検証の目的でデジタル署名を含み、各署名は秘密鍵に基づいて構築され、対応する公開鍵に従って検証される。

【００５４】

理解されるように、ルート信頼機関から特定のライセンス３６、３６Ｐ等に到る証明書チェーンにおいて、ルート信頼機関からのルートデジタル証明書は、ルート信頼機関からの秘密鍵に基づいて署名され、検証エンティティに対して利用可能と仮定される対応する公開鍵に基づいて検証される。チェーン内の他のデジタル証明書それぞれ、およびライセンス３６、３６Ｐ等に対し、チェーンの最後で、そのような他の証明書またはライセンス３６、３６Ｐ等は、特定の秘密鍵に基づいて署名され、ルート信頼機関に向かうチェーン内の次の証明書から取得される対応する公開鍵に基づいて検証される。

【００５５】

従って、ライセンス３６、３６Ｐ等を検証するために、ルート信頼機関に戻る対応する証明書チェーンを見つけ、そのようなルート信頼機関の対応する公開鍵を見つけ、ルート信頼機関の見つけた公開鍵を利用してルート証明書を検証する。そのような検証が成功すると仮定すると、公開鍵はルート証明書内にあり、チェーン内の次の証明書を検証するために利用される。その処理は、そこで公開鍵を見つけ、ライセンス３６、３６Ｐ等を検証するために用いられる、チェーン内の最後の証明書まで繰り返す。もちろん、何らかの検証が失敗すると、処理は終了し、ライセンス３６、３６Ｐ等は検証されない。一般的に、検証されなければ、ＲＭシステム３０はライセンス３６、３６Ｐ等を認めない。

【００５６】

（ライセンス内のルート信頼機関の定義）

現段階で理解されるべきであるが、ライセンス３６、３６Ｐ等（以下、ライセンス３６）を検証するには、信頼できるコンポーネント３８等の検証エンティティが、証明書チェーンで定義されるこのライセンス３６に対応するルート信頼機関の公開鍵を既に保有していることが必要である。しかしながら、以前指摘したように、それ自体には欠陥のないエンティティが実際はそのような公開鍵を、何らかのいくつかの理由により保有しない状況が発生しうる。もちろん、全ての証明書チェーンは単一のグローバルまたはグローバルに近いルート信頼機関に戻ることができるであろうが、そのような１つまたは少数のルート機関に依存することは、そのようなルート信頼を不必要に集中させ、集中されたルート信頼が損なわれる場合に問題であり、またはさもなければ失敗する。

【００５７】

従って本発明の一実施形態において、ライセンス３６は任意の特定のルート信頼機関を、それに対応する公開鍵をそれとともに含むことによって定義し、これにより次に公開鍵を利用して、そのようなライセンス３６に添付された証明書チェーンを検証し始める。結果として、任意の検証エンティティは任意の特定のルート信頼機関のいかなる特定の公開鍵も保有している必要は既にないが、その代わり、そのような公開鍵に基づいて最終的に検証されうる対応するライセンス３６に基づいて、そのような公開鍵を取得することができる。このように、そのような検証エンティティはどの特定のルート信頼機関にも結び付けられず、そのかわり、対応する証明書チェーンを通して任意の指定されたルート信頼機関に結び付けられた、ほとんどの任意のライセンス３６を検証できる。

【００５８】

しかしながら、本質的にそれによって検証されるべきライセンス３６を有するルート信頼機関の公開鍵を含むことにより、ライセンス３６は自己検証的となり、理解されるべき

であるが、これは普通、セキュリティ上で受け入れられないものであることに留意されたい。従って、本発明の一実施形態において、および図４に見られるように、ライセンス３６は解読部３６Ｄおよび承認部３６Ａを含む少なくとも２つの部分に分離され、それぞれはそのようなライセンス３６を利用して対応するコンテンツ３２をレンダリングしようと試みるユーザによって保有されなければならない。重要なことは、解読部３６Ｄはライセンス３６が発行されたユーザによってのみアクセス可能であるべきで、一方で承認部３６Ａは他人によってアクセス可能であるが、解読部３６Ｄ内の情報で検証される署名を有する必要がある。従って、そのような部分３６Ａ、３６Ｄがあることで、承認部３６Ａは自己検証的ではない。ライセンス３６は、本発明の精神と範囲を逸脱することなく、他の部分を有してもよいことに留意されたい。

【００５９】

本発明の一実施形態において、およびなお図４を参照して、ライセンス３６の承認部３６Ａはライセンス３６の発行者を識別し、例えば１つまたは複数の特定の方法でコンテンツ３２の一部をレンダリングするための権利、あるタイプのライセンス３６を発行するための権利といった具体的な権利許可を含み、関連コンテンツ３２の識別を含んでもよい。加えて、承認部３６Ａは、ライセンス３６の承認部３６Ａを使用できる１人または複数の特定のユーザまたはユーザタイプを指定してもよく、各指定されたユーザ／ユーザタイプに対して、ライセンス３６の使用に関連して満たすべき条件を指定してもよい。

【００６０】

重要なことは、承認部３６Ａは少なくとも前述の項目の一部に基づいたデジタル署名を含み、そこではその署名が特定の公開／秘密鍵の対（ＰＵ－ＲＯＯＴ、ＰＲ－ＲＯＯＴ）を有する特定のルート信頼機関に戻るということである。即ち、そして理解されるべきであるが、署名（Ｓ（ＰＲ－ＲＯＯＴ））はＰＲ－ＲＯＯＴに基づくか、またはＰＲ－ＲＯＯＴに基づいた署名を有する最後の証明書に戻る証明書チェーンを含んでもよい。いずれの場合も、これも理解されるべきであるが、署名（Ｓ（ＰＲ－ＲＯＯＴ））を、直接的または証明書チェーン経由のどちらかで、どちらの場合でも適切な（ＰＵ－ＲＯＯＴ）の適用に基づいて検証することができる。

【００６１】

しかしながら、承認部３６Ａは、それ自体そのような（ＰＵ－ＲＯＯＴ）を含まないことに留意されたい。そのかわり、本発明の一実施形態において解読部３６Ｄは、対応するコンテンツ３２を解読するための解読鍵（ＫＤ）と共にルート鍵（ＰＵ－ＲＯＯＴ）を含む。加えて、解読部３６Ｄは、承認部３６Ａに記述された権利と条件に加え、他の権利および条件を含んでもよい。最も重要なことは、解読部３６Ｄが、その中のルート鍵（ＰＵ－ＲＯＯＴ）を利用して対応する承認部３６Ａ上の署名を検証しない限り、その中の解読鍵（ＫＤ）は利用できないことを、権利／条件として表現すべきであるということである。

【００６２】

デジタル署名は本発明の精神と範囲を逸脱することなく提供することができるが、解読部３６Ｄはおそらくデジタル署名されていない。理解されるように、署名されているならば、そのような署名はおそらく、検証ルート鍵がユーザのコンピューティング装置３４に結び付けられるべきでないと仮定して、（ＰＵ－ＲＯＯＴ）に基づいて検証されなければならないであろう。しかしながら再び、そのような（ＰＵ－ＲＯＯＴ）に基づいて検証される解読部３６Ｄ内に（ＰＵ－ＲＯＯＴ）を含むことは、解読部３６Ｄを自己検証的にし、理解されるべきであるがこれは普通、セキュリティ上受け入れられないものである。

【００６３】

そのかわり、本発明の一実施形態において、解読部３６Ｄはその中の鍵を保護するために暗号化され、その暗号化鍵は、対応する解読鍵がユーザのコンピューティング装置３４に対して利用可能なように選択される。理解されるように、そうすることは、解読部３６Ｄがそのような解読鍵経由でユーザのコンピューティング装置３４に結び付けられうるという利点がある。さらに理解されるように、そうすることは、ユーザのコンピューティン

グ装置３４に対して利用可能である限り、解読鍵は複数ある鍵のどれでもよいという追加的な利点を有する。

【００６４】

例えば、本発明の一実施形態において解読鍵は、図４に示されるように、暗号化鍵として利用される公開鍵に対応する秘密鍵である。従って、ユーザのコンピューティング装置３４はそれ自体そのような公開／秘密鍵の対を有してもよく、またはユーザの公開／秘密鍵の対自体に対するアクセスを有してもよい。または、ユーザのコンピューティング装置３４上の信頼できるコンポーネント３８は、そのような公開／秘密鍵の対を有することができる。任意のそのような状況において公開鍵は、ライセンス３６の、特に、同様な暗号化において使用するための解読部３６Ｄのコンストラクタに提供され、一方で秘密鍵は解読部３６Ｄを解読するために秘密に保持される。

【００６５】

そのかわり、解読鍵および暗号化鍵は同じであってもよく、この場合においてそのようなコンストラクタおよびユーザのコンピューティング装置３４は、そのような対称鍵（不図示）を生成するための共有秘密を確立できる。もちろん、ユーザのコンピューティング装置はその後、将来取り出すためにそのような対称鍵を確実に格納しなければならないであろう。

【００６６】

図５に移り、このように上述した、図３、４との関連において、ユーザのコンピューティング装置３４上でのコンテンツ３２のレンダリングが以下の方法で達成される。前もって、コンテンツ３２内のなんらかの適切な識別に基づき、ユーザのコンピューティング装置３４およびその上の信頼できるコンポーネント３８は、コンテンツに対応するライセンス３６を発行できる図３のライセンサ４６のようなライセンスサーバに向けられ、要求がこのライセンス３６についてこのライセンスサーバ４６に発行される（ステップ５０１）。一般的に、そのような要求は、ユーザ、ユーザのコンピューティング装置３４、信頼できるコンポーネント３８等のいずれかを識別する証明書等を含み、その証明書はその中に公開鍵（ＰＵ－ＵＳＥＲ）を含む。その後、証明書を含む要求に基づいて、ライセンスサーバ４６はそれに応えて、ライセンス３６を発行するか否かを決定する。理解されるように、そのような決定は、本発明の精神と範囲を逸脱することなく任意の適切な要因に基づいてよい。

【００６７】

ライセンスサーバ４６が実際にライセンス３６の発行を決定する（ステップ５０３）と仮定すると、そのようなライセンスサーバは解読部３６Ｄおよび承認部３６Ａを上述の形態で構築し（ステップ５０５）、解読部３６Ｄ内のルート鍵（ＰＵ－ＲＯＯＴ）に基づいて承認部３６Ａに署名し（ステップ５０７）、要求付きの証明書の公開鍵（ＰＵ－ＵＳＥＲ）に基づいて解読部３６Ｄを暗号化する（ステップ５０９）。ステップ５０１で、各要求は異なる公開鍵（ＰＵ－ＵＳＥＲ）を含み、この（ＰＵ－ＵＳＥＲ）を利用して、要求されたライセンス３６の解読部３６Ｄを暗号化する。従って、各解読部３６Ｄは、それに対応して異なることに、ここでは留意されたい。しかしながら、承認部３６Ａは、同じルート鍵（ＰＵ－ＲＯＯＴ）に基づいて検証されるために署名されるべきであるので、解読部３６Ｄのように異なることはおそらくないであろう。従って、各要求に応じて、異なる解読部３６Ｄがステップ５０５で構築され、ステップ５０９で暗号化されるが、単一の共通承認部３６Ａのみがステップ５０５で構築され、ステップ５０７で署名され、単一の承認部３６Ａが全ての要求に対して適用可能であるという場合が実際にありうる。

【００６８】

いずれにせよ、ライセンスサーバ４６はユーザのコンピューティング装置３４からの要求に応答して、それに対して承認部３６Ａおよび解読部３６Ｄを含むライセンス３６を返す（ステップ５１１）。しかしながら、承認部３６Ａは必ずしもいずれか特定のライセンス３６に対して固有である必要はなく、従って実際、複数のライセンス３６に対して共通であってよいことに留意されたい。従って、解読部３６Ｄはステップ５０５で各要求に応

答して構築されるが、承認部３６Ａは、要求側がそのような承認部３６Ａを既に保有しない場合にのみステップ５０５で構築されるという場合が実際にありうる。それに対応して、要求側が実際に既にそのような承認部３６Ａを保有する場合、ライセンスサーバ４６はステップ５０５で同様に構築する必要はなく、ステップ５１１で同様にライセンス３６を返す必要はない。

【００６９】

図６に示すように、解読部３６Ｄと、暗号化されたコンテンツ３２に対応するライセンス３６の承認部３６Ａとを保有するユーザのコンピューティング装置３４は、そのようなコンテンツ３２を以下の方法で解読およびレンダリングする。

【００７０】

予め、コンテンツ３２に基づき、ユーザのコンピューティング装置３４は、ライセンス３６、または少なくともその解読部３６Ｄを突き止める（ステップ６０１）。従って、ユーザのコンピューティング装置３４は、そのような解読部３６Ｄを暗号化するために利用した暗号化方式が何であれ、それに準じて同様に解読する（ステップ６０３）。例えば、解読部３６Ｄまたはその一部がユーザの公開鍵（ＰＵ－ＵＳＥＲ）に基づいて暗号化される場合、ユーザのコンピューティング装置３４は対応する秘密鍵（ＰＲ－ＵＳＥＲ）を適用してそのような解読部３６Ｄまたはその一部を明らかにする。

【００７１】

さらに、ユーザのコンピューティング装置３４は解読部３６Ｄ内に記述された権利／条件を検討し、その権利が、求められ、かつその条件を満たす方法でコンテンツ３２をレンダリングすることを許可するか否かを判定する（ステップ６０５）。重要なことは、そのような判定が以下のことを保証することを含むということである。すなわち、解読部３６Ｄ内のルート鍵（ＰＵ－ＲＯＯＴ）を利用して対応する承認部３６Ａにおける署名を検証しない限り、解読部３６Ｄ内の解読鍵（ＫＤ）は、利用されないということである。権利／条件が解読部３６Ｄ内で暗号化されない場合、ステップ６０５をステップ６０３の前に行ってもよく、求められた方法でコンテンツ３２をレンダリングすることをそのような権利／条件が許可しない場合はステップ６０３を回避してもよいことに留意されたい。また、解読部３６Ｄの権利／条件または任意の他の部分が暗号化されない場合、そのような部分は少なくともデジタル署名の基礎となるべきで、そのようなデジタル署名を検証して改ざんから守るべきであることにも留意されたい。

【００７２】

解読部３６Ｄ内の権利／条件が求められた方法でコンテンツ３２をレンダリングすることを許可すると仮定する。ユーザのコンピューティング装置３４はルート鍵（ＰＵ－ＲＯＯＴ）と、対応するコンテンツ３２を解読するための解読鍵（ＫＤ）とを解読部３６Ｄから取得し（ステップ６０７）、承認部３６Ａを突き止め（ステップ６０８）、その後そのような（ＰＵ－ＲＯＯＴ）を利用して承認部３６Ａのデジタル署名（Ｓ（ＰＲ－ＲＯＯＴ））を検証する（ステップ６０９）。そのような検証は、本発明の精神と範囲を逸脱することなく、任意の適切な方法で行われてもよい。そのような検証は、関連する一般各位には既知で、または明らかであるはずなので、ここではこれ以上詳細に記述する必要はない。

【００７３】

検証が成功すると仮定すると、ユーザのコンピューティング装置３４はその後、承認部３６Ａ内に記述された権利／条件を検討し、その権利が、求められ且つその条件を満たす方法でのコンテンツ３２のレンダリングを許可するか否かを判定してもよい（ステップ６１１）。ステップ６１１をステップ６０９の前に行ってもよく、求められた方法でコンテンツ３２をレンダリングすることをそのような権利／条件が許可しない場合はステップ６０９を回避してもよいことに留意されたい。

【００７４】

承認部３６Ａ内の権利／条件が、求められた方法でコンテンツ３２をレンダリングすることを許可すると仮定すると、ユーザのコンピューティング装置３４はステップ６０７で

取得した解読鍵（ＫＤ）を利用して、暗号化されたコンテンツ３２を実際に解読し（ステップ６１３）、その後そのような解読されたコンテンツ３２をレンダリングする（ステップ６１５）。

【００７５】

結論

本発明に関連して行われるプロセスを有効にするために必要なプログラミングは、比較的簡単であり、関係する一般プログラマーには明らかなはずである。従って、そのようなプログラミングはここには添付されていない。任意の特定のプログラミングは、それゆえ、本発明の精神および範囲を逸脱することなく、本発明を有効にするために利用されてもよい。

【００７６】

本発明において、デジタルライセンス３６およびその動作を定義するために、柔軟なアーキテクチャが提供される。そのアーキテクチャによって、複数のルート信頼機関が可能となり、ライセンス３６がそれ自体、同様に認証／検証するために利用できる各ルート信頼機関を指定できる。そのようなアーキテクチャを有効にするために、ライセンス３６は、特定のユーザまたはユーザグループによってのみアクセス可能な方法で暗号化された解読部３６Ｄと、解読部３６Ｄから取得された鍵に基づいて検証されなければならない承認部３６Ａを含む。

【００７７】

当然のことながら、上述した実施形態は、本発明概念から逸脱することなく、変更できる。従って、当然のことながら、本発明は開示された特定の実施形態に制限されることはなく、添付する請求項によって定義される本発明の精神および範囲内の修正を包含するよう意図されている。

【図面の簡単な説明】

【００７８】

【図１】本発明が実装しうる例示的で非制限なコンピューティング環境を表すブロック図である。

【図２】本発明が実装しうる様々なコンピューティング装置を有する例示的なネットワーク環境を表すブロック図である。

【図３】本発明の一実施形態によるデジタルライセンスを含む、信頼ベースシステムの一例の行使アーキテクチャを示すブロック図である。

【図４】図３のライセンスをより詳細に示し、本発明の一実施形態による承認部および解読部を含むブロック図である。

【図５】本発明の一実施形態による、図３および４のライセンスを発行する時に行われる鍵ステップを示すフロー図である。

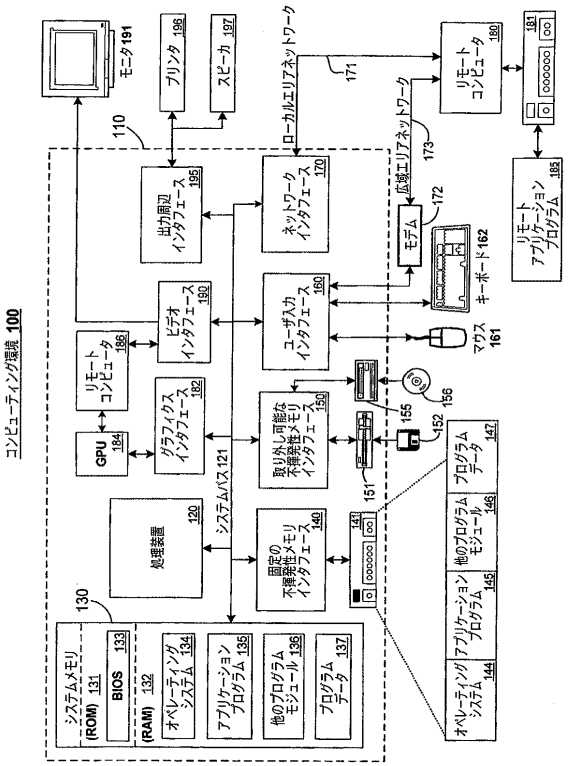
【図６】本発明の一実施形態による、図３および４のライセンスを利用してコンテンツをレンダリングするときに行われる鍵ステップを示すフロー図である。

【符号の説明】

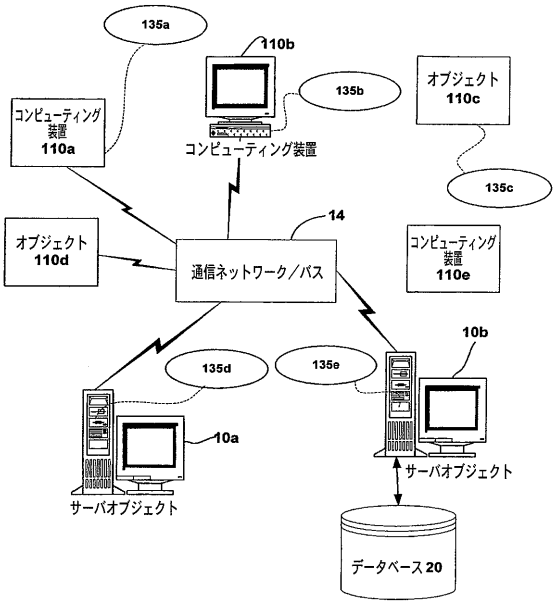
【００７９】

１３５ａ～ｅ　オブジェクト

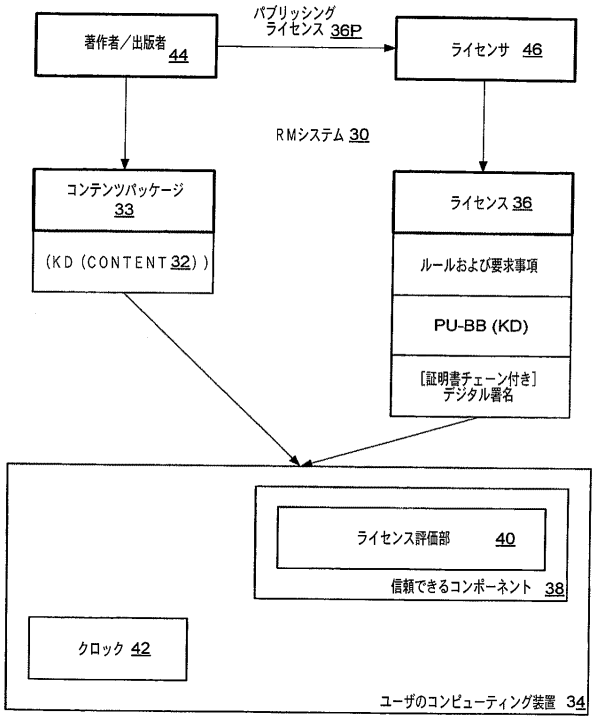
【図１】


コンピューティング環境 100
モニタ 191
プリンタ 196
スピーカ 197
ローカルエリアネットワーク
171
リモートコンピュータ 180
181
広域エリアネットワーク
173
リモートアプリケーションプログラム 185
110
出力周辺インタフェース 195
ネットワークインタフェース 170
モデム 172
キーボード 162
ビデオインタフェース 190
ユーザ入力インタフェース 160
マウス 161
リモートコンピュータ 188
GPU 184
グラフィクスインタフェース 182
取り外し可能な不揮発性メモリインタフェース 150
155
156
152
151
プログラムデータ 147
システムバス 121
処理装置 120
固定の不揮発性メモリインタフェース 140
143
他のプログラムモジュール 146
アプリケーションプログラム 145
オペレーティングシステム 144
130
システムメモリ (ROM) 131
BIOS 133
(RAM) 132
オペレーティングシステム 134
アプリケーションプログラム 135
他のプログラムモジュール 136
プログラムデータ 137

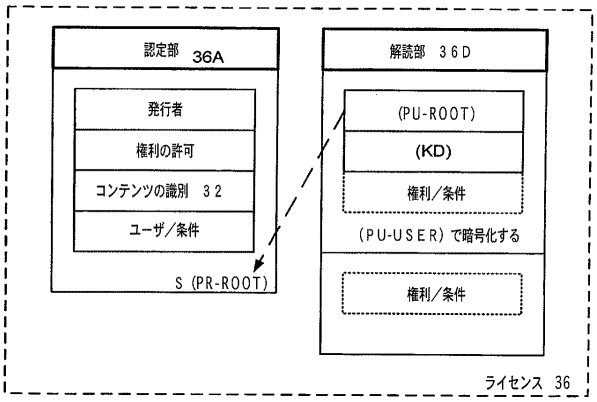
【図２】


135a
110b
135b
オブジェクト 110c
コンピューティング装置 110a
コンピューティング装置
135c
14
オブジェクト 110d
通信ネットワーク／バス
コンピューティング装置 110e
10b
135d
135e
10a
サーバオブジェクト
サーバオブジェクト
データベース 20

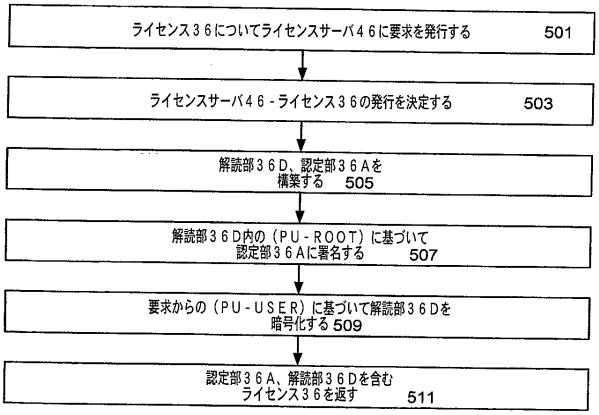
【図３】


著作者／出版者 44
パブリッシング ライセンス 36P
ライセンサ 46
RMシステム 30
コンテンツパッケージ 33
(KD (CONTENT 32))
ライセンス 36
ルールおよび要求事項
PU-BB (KD)
[証明書チェーン付き] デジタル署名
ライセンス評価部 40
信頼できるコンポーネント 38
クロック 42
ユーザのコンピューティング装置 34

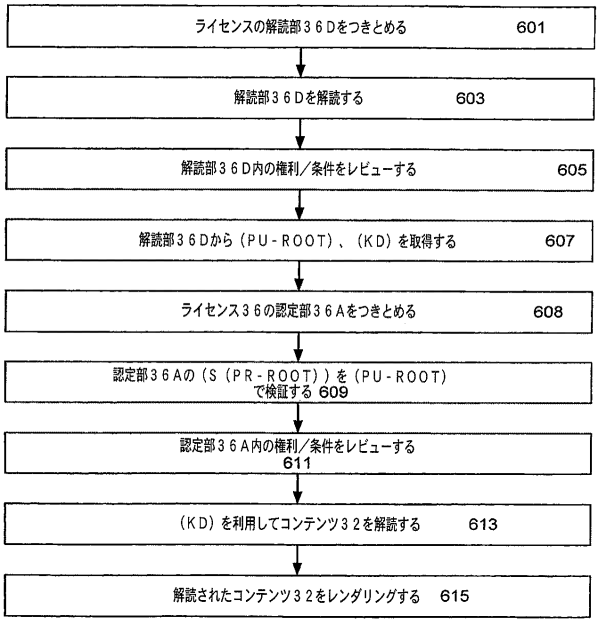
【図４】


認定部 36A
発行者
権利の許可
コンテンツの識別 32
ユーザ／条件
S (PR-ROOT)
解読部 36D
(PU-ROOT)
(KD)
権利／条件
(PU-USER) で暗号化する
権利／条件
ライセンス 36

【図５】


ライセンス３６についてライセンスサーバ４６に要求を発行する 501
ライセンスサーバ４６ - ライセンス３６の発行を決定する 503
解読部３６D、認定部３６Aを構築する 505
解読部３６D内の (PU - ROOT) に基づいて認定部３６Aに署名する 507
要求からの (PU - USER) に基づいて解読部３６Dを暗号化する 509
認定部３６A、解読部３６Dを含むライセンス３６を返す 511

【図６】


ライセンスの解読部３６Ｄをつきとめる 601
解読部３６Ｄを解読する 603
解読部３６Ｄ内の権利／条件をレビューする 605
解読部３６Ｄから（ＰＵ－ＲＯＯＴ）、（ＫＤ）を取得する 607
ライセンス３６の認定部３６Ａをつきとめる 608
認定部３６Ａの（Ｓ（ＰＲ－ＲＯＯＴ））を（ＰＵ－ＲＯＯＴ）で検証する 609
認定部３６Ａ内の権利／条件をレビューする 611
（ＫＤ）を利用してコンテンツ３２を解読する 613
解読されたコンテンツ３２をレンダリングする 615

フロントページの続き

(72)発明者 マルコ エー. デメロ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 ムトゥクリシュナン パラマシバム
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 ピーター ディー. ワックスマン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 ラビンドラ エヌ. パンドヤ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 スティーブン ボーン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 ビナイ クリシュナスワミー
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内

審査官 青木 重徳

(56)参考文献 特開２００４－２４０９５９（ＪＰ，Ａ）
特開２００３－３０９５４５（ＪＰ，Ａ）
特開２００３－２８９２９７（ＪＰ，Ａ）
特開平１０－２１５２４５（ＪＰ，Ａ）
国際公開第２００２／０８０４４６（WO，Ａ１）
米国特許出願公開第２００３／０１８７８０１（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００