(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-538633
(P2008-538633A)
(43)公表日　平成20年10月30日(2008.10.30)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| G06F 21/24 | (2006.01) | G06F | 12/14 | 520D | 5B017 |
| H04L 9/08 | (2006.01) | H04L | 9/00 | 601B | 5B285 |
| G06F 21/00 | (2006.01) | G06F | 12/14 | 540P | 5J104 |
| | | H04L | 9/00 | 601E | |
| | | G06F | 15/00 | 330Z | |

審査請求 未請求　予備審査請求 未請求　（全 39 頁）

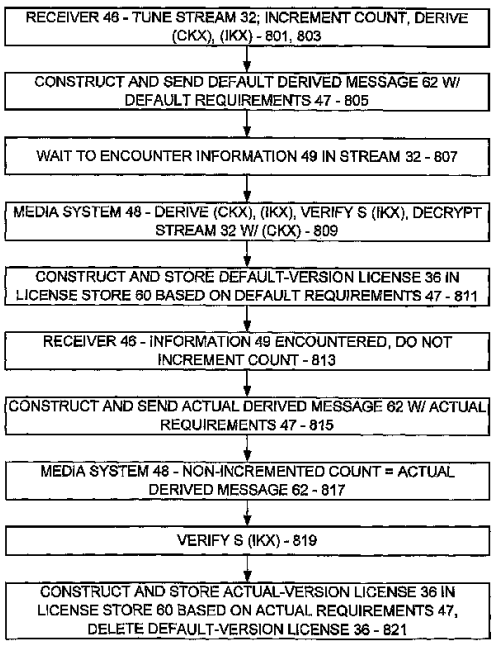
(21)出願番号　特願2008-507664 (P2008-507664)
(86)(22)出願日　平成18年3月16日 (2006.3.16)
(85)翻訳文提出日　平成19年12月18日 (2007.12.18)
(86)国際出願番号　PCT/US2006/009650
(87)国際公開番号　WO2006/115608
(87)国際公開日　平成18年11月2日 (2006.11.2)
(31)優先権主張番号　11/113,215
(32)優先日　平成17年4月22日 (2005.4.22)
(33)優先権主張国　米国(US)

(71)出願人　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　100089705
弁理士　社本　一夫
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行

最終頁に続く

(54)【発明の名称】ストリーミングされたマルチメディア・コンテンツのための権利管理システム

(57)【要約】
受信機が、コンテンツをチューニングし、対応するライセンスのための条件と関係する情報を最初は発見せず、従って、デフォルト条件を含むデフォルト・メッセージを構築し、構築されたデフォルト・メッセージをデフォルト条件と共に、コンテンツをレンダリングする計算機に送信する。この計算機は、送信されたデフォルト・メッセージを前記デフォルト条件と共に受信すると、受信されたデフォルト条件に基づいて、ライセンスのデフォルト・バージョンを構築し、ライセンスの構築されたデフォルト・バージョンを、それ自身のライセンス記憶装置に記憶し、ライセンスのデフォルト・バージョンだけに従ってコンテンツをレンダリングする。



【特許請求の範囲】
【請求項１】
デジタル・ライセンスのための条件（requirements）を、対応するデジタル・コンテンツの受信機から、前記デジタル・コンテンツがレンダリングされる計算機へ通信する方法であって、
前記受信機が前記コンテンツをチューニングするステップと、
前記受信機が、前記ライセンスのための前記条件と関係する情報を最初は発見せず、デフォルト条件を含むデフォルト・メッセージを構築し、前記構築されたデフォルト・メッセージを前記デフォルト条件と共に前記計算機へ送信するステップと、
前記計算機が、前記送信されたデフォルト・メッセージを前記デフォルト条件と共に受信し、前記受信されたデフォルト条件に基づいて、前記ライセンスのデフォルト・バージョンを構築し、前記ライセンスの前記構築されたデフォルト・バージョンを前記計算機のライセンス記憶装置に記憶し、前記ライセンスの前記デフォルト・バージョンだけに従って前記コンテンツをレンダリングするステップと、
前記受信機が、前記ライセンスのための前記条件と関係する情報を発見し、前記発見された情報からの実際の条件を用いて実際のメッセージを構築し、前記構築された実際のメッセージを前記実際の条件と共に前記計算機に送信するステップと、
前記計算機が、前記送信された実際のメッセージを前記実際の条件と共に受信し、前記受信された実際の条件に基づいて前記ライセンスの実際のバージョンを構築し、前記ライセンスの前記デフォルト・バージョンの代わりに前記ライセンスの前記構築された実際のバージョンを前記計算機のライセンス記憶装置に記憶し、前記ライセンスの前記実際のバージョンだけに従って前記コンテンツをレンダリングするステップと、
を含み、よって、前記受信機は、前記ライセンスのための前記条件と関係する前記条件が発見されるまで前記計算機による前記コンテンツのレンダリングを遅らせる必要がないことを特徴とする方法。
【請求項２】
請求項１記載の方法において、前記デジタル・コンテンツはデジタル・コンテンツのストリームであり、前記ストリームは複数の前記ストリームを有する信号からのストリームであり、この方法は、前記受信機が前記信号からの前記ストリームをチューニングするステップを含むことを特徴とする方法。
【請求項３】
請求項１記載の方法において、前記受信機が前記ライセンスのための前記条件と関係する情報を最初は発見せず、別の計算機においてレンダリングするための前記コンテンツのコピーを許さないデフォルト条件を含むデフォルト・メッセージを構築するステップを含むことを特徴とする方法。
【請求項４】
請求項１記載の方法において、前記受信機は、前記条件と関係する前記情報を、前記コンテンツの中の既知の間隔及び位置において発見することを特徴とする方法。
【請求項５】
請求項１記載の方法において、前記計算機は、前記条件のそれぞれのフィールドを所定のマッピング規則に従って前記ライセンスにマップするマッピング・アルゴリズムを用いることにより、前記受信された条件に基づいて前記ライセンスを構築することを特徴とする方法。
【請求項６】
請求項１記載の方法において、
前記受信機が、前記ライセンスのための前記条件と関係する情報を最初は発見せず、カウントｘをインクリメントして前記デフォルト条件と前記カウントｘとを含むデフォルト・メッセージを構築し、前記構築されたデフォルト・メッセージを前記デフォルト条件及びカウントｘと共に前記計算機に送信するステップと、
前記受信機が、前記ライセンスのための前記条件と関係する情報を発見し、前記カウン

トｘをインクリメントするのではなく代わりに前記実際の条件と前記カウントｘとを用いて実際のメッセージを構築し、前記構築された実際のメッセージを前記実際の条件及びカウントｘと共に前記計算機に送信するステップと、
を含み、前記計算機は、前記実際のメッセージの中のインクリメントされていないカウントｘを、前記ライセンスの前記構築された実際のバージョンが前記ライセンスの前記デフォルト・バージョンの代わりに前記ライセンス記憶装置に記憶されるべきであることを意味するものと理解することを特徴とする方法。
【請求項７】
請求項１記載の方法において、前記受信機が、前記ライセンスのための前記条件と関係する情報を最初は発見せず、性質において最も制限的なデフォルト条件を含むデフォルト・メッセージを構築し、前記構築されたデフォルト・メッセージを前記デフォルト条件と共に前記計算機に送信するステップを含むことを特徴とする方法。
【請求項８】
請求項１記載の方法において、前記ライセンスのための前記条件と関係する情報を前記コンテンツの内部において発見するステップを含むことを特徴とする方法。
【請求項９】
デジタル・ライセンスのための条件を、対応するデジタル・コンテンツの受信機から、前記デジタル・コンテンツがレンダリングされる計算機へ通信する方法を実装するコンピュータ実行可能な命令が記憶されているコンピュータ可読な媒体であって、前記方法は、
前記受信機が前記コンテンツをチューニングするステップと、
前記受信機が、前記ライセンスのための前記条件と関係する情報を最初は発見せず、デフォルト条件を含むデフォルト・メッセージを構築し、前記構築されたデフォルト・メッセージを前記デフォルト条件と共に前記計算機へ送信するステップと、
前記計算機が、前記送信されたデフォルト・メッセージを前記デフォルト条件と共に受信し、前記受信されたデフォルト条件に基づいて、前記ライセンスのデフォルト・バージョンを構築し、前記ライセンスの前記構築されたデフォルト・バージョンを前記計算機のライセンス記憶装置に記憶し、前記ライセンスの前記デフォルト・バージョンだけに従って前記コンテンツをレンダリングするステップと、
前記受信機が、前記ライセンスのための前記条件と関係する情報を発見し、前記発見された情報からの実際の条件を用いて実際のメッセージを構築し、前記構築された実際のメッセージを前記実際の条件と共に前記計算機に送信するステップと、
前記計算機が、前記送信された実際のメッセージを前記実際の条件と共に受信し、前記受信された実際の条件に基づいて前記ライセンスの実際のバージョンを構築し、前記ライセンスの前記デフォルト・バージョンの代わりに前記ライセンスの前記構築された実際のバージョンを前記計算機のライセンス記憶装置に記憶し、前記ライセンスの前記実際のバージョンだけに従って前記コンテンツをレンダリングするステップと、
を含み、よって、前記受信機は、前記ライセンスのための前記条件と関係する前記条件が発見されるまで前記計算機による前記コンテンツのレンダリングを遅らせる必要がないことを特徴とするコンピュータ可読な媒体。
【請求項１０】
請求項請求項９記載の媒体において、前記デジタル・コンテンツはデジタル・コンテンツのストリームであり、前記ストリームは複数の前記ストリームを有する信号からのストリームであり、この方法は、前記受信機が前記信号からの前記ストリームをチューニングするステップを含むことを特徴とする媒体。
【請求項１１】
請求項９記載の媒体において、前記方法は、前記受信機が前記ライセンスのための前記条件と関係する情報を最初は発見せず、別の計算機においてレンダリングするための前記コンテンツのコピーを許さないデフォルト条件を含むデフォルト・メッセージを構築するステップを含むことを特徴とする媒体。
【請求項１２】

請求項９記載の媒体において、前記受信機は、前記条件と関係する前記情報を、前記コンテンツの中の既知の間隔及び位置において発見することを特徴とする媒体。
【請求項１３】
請求項９記載の媒体において、前記計算機は、前記条件のそれぞれのフィールドを所定のマッピング規則に従って前記ライセンスにマップするマッピング・アルゴリズムを用いることにより、前記受信された条件に基づいて前記ライセンスを構築することを特徴とする媒体。
【請求項１４】
請求項９記載の媒体において、前記方法は、
前記受信機が、前記ライセンスのための前記条件と関係する情報を最初は発見せず、カウントｘをインクリメントして前記デフォルト条件と前記カウントｘとを含むデフォルト・メッセージを構築し、前記構築されたデフォルト・メッセージを前記デフォルト条件及びカウントｘと共に前記計算機に送信するステップと、
前記受信機が、前記ライセンスのための前記条件と関係する情報を発見し、前記カウントｘをインクリメントするのではなく代わりに前記実際の条件と前記カウントｘとを用いて実際のメッセージを構築し、前記構築された実際のメッセージを前記実際の条件及びカウントｘと共に前記計算機に送信するステップと、
を含み、前記計算機は、前記実際のメッセージの中のインクリメントされていないカウントｘを、前記ライセンスの前記構築された実際のバージョンが前記ライセンスの前記デフォルト・バージョンの代わりに前記ライセンス記憶装置に記憶されるべきであることを意味するものと理解することを特徴とする媒体。
【請求項１５】
請求項９記載の媒体において、前記方法は、前記受信機が、前記ライセンスのための前記条件と関係する情報を最初は発見せず、性質において最も制限的なデフォルト条件を含むデフォルト・メッセージを構築し、前記構築されたデフォルト・メッセージを前記デフォルト条件と共に前記計算機に送信するステップを含むことを特徴とする媒体。
【請求項１６】
請求項９記載の媒体において、前記方法は、前記ライセンスのための前記条件と関係する情報を前記コンテンツの内部において発見するステップを含むことを特徴とする媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、それによって流されたデジタル・コンテンツへのアクセスが対応するディジタル・ライセンスに従ってのみ提供される収益権管理（ＲＭ）システムに関する。
特に、その発明は、流された内容を扱うのにそのようなＲＭシステムによって使用されたシステムと方法に関する。
【背景技術】
【０００２】
そのようなデジタル・コンテンツが１つ以上のユーザーに配布されることになっている場合、権利管理（ＲＭ）および施行は、デジタル・オーディオ、デジタルビデオ、ディジタル・テキスト、デジタルデータ、ディジタル・マルチメディアなどのようなデジタル・コンテンツに関して高度に望ましい。デジタル・コンテンツは、テキストドキュメントのように、例えば静的になりえるか、あるいはマルチメディアプレゼンテーションの流されたオーディオおよびビデオのように、それを流すことができるかもしれない。そのようなものの分配の典型的なモードは内容を流した、光ディスクのような明確で無形の形式を含んでいる、ケーブル・アクセス材料、インターネットのような電子的ネットワークからの材料、放送中の放送などからの材料　それの適切なコンピューティング装置でユーザーによって受け取られる際、そのようなユーザーは、コンピューティング装置、適切なレンダーリング・ソフトウェア、およびスピーカー、ビデオモニターなどのような適切な出力デバイスの援助によって流されたデジタル・コンテンツを与える。

【０００３】
１つのシナリオでは、流された内容は、購読サービスの一部としてディストリビュータによって分配される、のように、例えばデジタル・テレビ・サービス、また、分配されるような流された内容は保護される、のように、暗号化により例えば、あるいは非保護である。それが流された内容が非保護の形式で確かに分配されるというその場合である場合、それは、直ちに消費され与えられ、かつどんな意味のある回復可能な形式でも格納されないために、流された内容にディストリビュータが主として用いるつもりのその場合かもしれない。例えば、流された内容は、ディジタル・ケーブル・セットトップ・ボックスによって、および直ちに受け取られることになってい、前述の適切な出力デバイスへ次に転送されることになっておりそのために与えられたことになっている、ディジタル・ケーブルテレビ信号中の内容の多くのストリームのうちの１つかもしれない。

【０００４】
しかしながら、後のレンダーリングおよび（または）他のコンピューティング装置への再分配のために流された内容を確かに格納することができるストレージシステムが、存在しかつ、または開発されていることは認識されることになっている。そのようなストレージシステムに関して、それでは、もしそのように望まれれば、流された非保護の内容のディストリビュータは、非保護の形式で、およびそのような再分配を制限する能力なしでそのような非保護の内容をむしろ格納（記憶）したくない。ディストリビュータなどは、特にそのようなものをコピーすることをユーザーに禁じたいかもしれない、別のストレージシステムあるいはその他同種のものへの内容を流した、ユーザーがコピーすることを可能にしたいかもしれないこと、一時的、または制限などを数える。流された内容の無制限の複写の禁止によって、評価されるかもしれないように、ディストリビュータは、流された内容の原始のディジタルコピーの未検査の分散を回避することができる。そこでは、そのような未検査の分散は、そのようなディストリビュータによって提示された購読サービスを予約することから先行することからの他のユーザーを激励するだろう。

【０００５】
さらに、ディストリビュータは様々なユーザーに異なる与える権利を提供したいかもしれない。例えば、より高いレベルの層が相応してより高い受信料を命じるところで、ディストリビュータはサービスの異なる層を提示してもよい。また、特別の層で予約するユーザーがアクセスに許可されるべきでない場所は、非保護の形式中のより高い層からの内容を流した。

【０００６】
ノート、しかしながら、流された内容の後のそれは分配された、ディストリビュータは全く何も持っていない、場合、流された内容に対する任意の実際のコントロール。これは、事実を考慮して特に問題である、どんなパーソナルコンピュータも含んでいる大部分、そのようなものの正確なディジタルコピーを作るのに必要なソフトウェアおよびハードウェアは、内容を流した、またｒｅにそのような正確なディジタルコピーをダウンロードすること－光ディスクのような配布媒体、あるいは任意の宛先へインターネットのようなネットワーク上のそのような正確なディジタルコピーを送ること
もちろん、流された内容が予約されるトランザクションの一部として、ディストリビュータは、好ましくないやり方で再度そのような内容を分配しないと約束することを流された内容のユーザー／受信者に要求してもよい。しかしながら、そのような約束は容易になされ容易に破られる。ディストリビュータは、いくつかの既知の機密保持用装置、通常含んでいる暗号化および解読のうちのどれによってもそのような再分配を防ぐことを試みてもよい。しかしながら、特に単純な場合そのような機密保持用装置、姿勢、暗号化コンテンツを解読したい温和に信念の固いユーザーの小さな問題は暗号化されていない形式でそのような内容を保存し、次に、再度同じを分配する。

【０００７】
ＲＭと施行のアーキテクチャおよび方法はデジタル・コンテンツを含んでいる任意の形式のコントロールされたレンダーリングに流された内容を与えるためにこのように提供さ

れた。そこでは、そのようなコントロールはそのようなデジタル・コンテンツにディストリビュータなどによって柔軟で、定義可能である。そのようなアーキテクチャは、上に述べられるようなシナリオ中のそのような抑制されたレンダーリングを許可し促進する。

【０００８】

１つの特別の協定では、流された内容は、レシーバー（受信機）に結合信号として提供されるそのような内容の多くのストリームのうちの１つである。レシーバーは、媒体システムからコマンド上のストリームの特別の１つを選び、その後の処理のために選択されたストリームｔＱにそのような媒体システムを提供する。顕著に、レシーバーに提供されるような選択されたストリームは非保護である。しかし、媒体システムに提供される前に、選択されたストリームは、特別のＲＭ暗号化システムによるレシーバーによって保護された事実にある。

【０００９】

典型的には、ＲＭ暗号化システムでは、内容は内容キー（ＣＫ）によって暗号化されることにより保護される。対称な暗号化および解読がより容易でより速く、非対称の暗号化および解読ほど高価ではないので、そのような内容キー（ＣＫ）は典型的に対称である。さらに典型的には、内容キー（ＣＫ）は、暗号化された形式中の、およびそのような内容がｄｅｃｒｙｐｔｏｒ／媒体システムによって解読され与えられることを許される前に、満たされるに違いないライセンス規則を指定する、ディジタル・ライセンスなどの一部としての媒体システムのようなｄｅｃｒｙｐｔｏｒへのレシーバーのような暗号に変える人によって提供される。

【００１０】

流された内容が媒体システムのコマンドでレシーバーによって有効に調整されるかもしれない多くのデジタルテレビジョン信号のうちの１つである状況では、恐らく一度と同じくらいのの命令で、適正にレギュラーベース上の異なるデジタル信号中で合わせるべき媒体システムから、レシーバーがコマンドを受け取ると予想することができることは認識されることになっている、１秒まで皆半分、特に媒体システムのユーザーが有効である場合、かすめて飛ぶこと、によって、あるいは「サーフィン」いくつかの信号。また、新しく調整された信号がそれぞれレシーバーに新しいライセンスを要求することを認識して、特にライセンスが詳述される場合、そのような新しいライセンスを構築しレシーバーから媒体システムまで同じを送ることが、全く厄介かもしれないことは認識されることになっている、暗号化されたエレメントを含んでいる、デジタル署名などを含んでいる。したがって、レシーバーが完全に新しいライセンスを作成することは恐らく期待されない場合がある、ごとに、媒体システムコマンド、特にそのようなコマンドの周波数が２等品の命令である場合に、異なるデジタル信号を合わせるそのようなレシーバー。

【００１１】

必要は、すべての時間完全にそのような新しいライセンスを作成する事実にレシーバーがレシーバーが間接費に行く必要はないように、そのような新しいライセンスに入る必要条件の短縮版を作成するべきシステムおよび方法のために、そのとき存在する、そのようなレシーバーは新しくデジタル信号を合わせる。必要は、特にユーザーが変更が見えていても、レシーバーが新しくデジタル信号を合わせるごとに、速く作成することができ、媒体システムに送ることができるような必要条件のそのような短縮版のために存在する、の命令で、一度、すべての２位、程度。さらに、必要は、簡潔で、にもかかわらず、スペースの必要最低限量に調整されたデジタル信号用のライセンス必要条件についてすべて記述するようなそのような必要条件の短縮版のために存在する。最後に、必要は、レシーバー以外のソースからの媒体システムに提供されるような流されたデジタル・コンテンツに関して雇うことができるような必要条件のそのような短縮版のために存在する。

【００１２】

異なる内容（コンテンツ）キー（ＣＫ）によるレシーバーによって新しく調整された信号がそれぞれ暗号化されるかもしれないことをさらに認識して、新しいライセンスに同じを置きレシーバーから媒体システムまで同じを送ることにより、そのような内容キー（Ｃ

Ｋ）の媒体システムに通知することが、同様に全く厄介かもしれないことは認識されることになっている。再び、レシーバーが新しい内容キー（ＣＫ）で完全に新しいライセンスを作成することは恐らく期待されない場合がある、ごとに、媒体システムコマンド、特にそのようなコマンドの周波数が２等品の命令である場合に、異なるデジタル信号を合わせるそのようなレシーバー。

【００１３】

必要は、システム、および個々のそのような内容キー（ＣＫ）で実際のライセンスを作成する必要なしにレシーバーと媒体システムの間で個々の新しい内容キー（ＣＫ）を共有する方法のために、そのときそこに存在する。必要は、特にレシーバーおよび媒体システムが最初の内容キーを交換することができ、次に、最初の内容キーに基づいた内容キーを回転させることができる方法のために存在する。さらに、必要は、それによってレシーバーおよび媒体システムが統合方法でキーを回転させるような方法のために存在する。

【００１４】

新しく調整された信号に対応する必要条件が信号内に周期的な方式に置かれるかもしれないが、そのような周期性が比較的時間の長期かもしれないことをさらに認識して、そのような必要条件がそのような信号内にある事実にあるまで、媒体システムウエイトを比較的時間のそのような長期にすることが不合理かもしれないことは認識されることになっている。特に恐らく一度と同じくらいのの命令で、適正にレギュラーベース上の異なるデジタル信号中でレシーバーが合わせているシチュエーションで、１秒まで皆半分、レシーバーが比較的新しく調整された信号内の必要条件を見つける時間の長期を待つことができることは恐らく期待されない場合がある。

【００１５】

実際に位置した時、必要は、レシーバーが予備方式で必要条件のデフォルト・セットを送るべきシステムおよび方法、そして次に必要条件の実際のセットのために、そのとき存在する。必要は、特にレシーバーが実需が送られるまで、媒体システムによって雇われるそのようなデフォルト必要条件を送ることができる方法のために存在する。さらに、必要は、それによって媒体システムがそのようなデフォルト必要条件とそのような対応する実需の間に基本的相違を示すことができ、デフォルト必要条件をそれの受信上の対応する実需に取り替えることができるような方法のために存在する。

【００１６】

有望な媒体システムが新しく調整された信号に対応する比較的大量のライセンスを格納するだろうということを最後に認識すること、しかしその多数、そうでなければ、ほとんどのそのようなライセンスはそれほど長く必要ではない、それは評価されることになっている、そのようなライセンス、すべきだ、大部分は一時的基礎だけ上に格納される。もう一度、シチュエーションで、レシーバーが恐らく一度と同じくらいのの命令で適正にレギュラーベース上の異なるデジタル信号中で合わせているところで、１秒まで皆半分、媒体システムによって作成され格納されるような対応するライセンスがすべて、永久の方式で利用可能になるかなるべきことは恐らく期待されない場合がある。

【００１７】

必要は、媒体システムが一時的方式上にのみ調整された信号に対応するいくつかのライセンスを少なくとも格納するべきシステムおよび方法のために、そのとき存在する。必要は、特に媒体システムが認識することができる方法のために存在する、どれが許可するかを単に一時的方式上に格納する必要がある。さらに、必要は、それによって媒体システムがそのような一時的に格納されたライセンスを削除するような方法のために存在する。

【発明の概要】

【００１８】

以上の必要性は、デジタル・ライセンスのための条件（必要条件、要件、requirements）を、対応するデジタル・コンテンツの受信機から、前記デジタル・コンテンツがレンダリングされる計算機へ通信する方法が提供される本発明によって少なくとも部分的に満足される。この方法では、前記受信機が、前記コンテンツをチューニングし、前記ライセン

スのための前記条件と関係する情報を最初は発見せず、デフォルト条件を含むデフォルト・メッセージを構築し、前記構築されたデフォルト・メッセージを前記デフォルト条件と共に前記計算機へ送信する。前記計算機は、前記送信されたデフォルト・メッセージを前記デフォルト条件と共に受信し、前記受信されたデフォルト条件に基づいて、前記ライセンスのデフォルト・バージョンを構築し、前記ライセンスの前記構築されたデフォルト・バージョンを前記計算機のライセンス記憶装置に記憶し、前記ライセンスの前記デフォルト・バージョンだけに従って前記コンテンツをレンダリングする。

【００１９】

次に、前記受信機が、前記ライセンスのための前記条件と関係する情報を発見し、前記発見された情報からの実際の条件を用いて実際のメッセージを構築し、前記構築された実際のメッセージを前記実際の条件と共に前記計算機に送信する。そして、前記計算機が、前記送信された実際のメッセージを前記実際の条件と共に受信し、前記受信された実際の条件に基づいて前記ライセンスの実際のバージョンを構築し、前記ライセンスの前記デフォルト・バージョンの代わりに前記ライセンスの前記構築された実際のバージョンを前記計算機のライセンス記憶装置に記憶し、前記ライセンスの前記実際のバージョンだけに従って前記コンテンツをレンダリングする。こうして、前記受信機は、前記ライセンスのための前記条件と関係する前記条件が発見されるまで前記計算機による前記コンテンツのレンダリングを遅らせる必要がなくなる。

【発明を実施するための最良の形態】

【００２０】

コンピュータ環境

図１及び以下の議論は、本発明を実現しうる適切なコンピューティング環境に関して簡潔で一般的な説明を提供することを意図している。しかし、本発明との関係では、あらゆる種類のハンドヘルド型、携帯型及びそれ以外の計算機の使用が想定されていることを理解すべきである。以下では、汎用コンピュータが説明されているが、これは単なる一例であって、本発明が必要とするのは、ネットワーク・サーバとの相互動作可能性及び相互作用を有する単純なクライアントだけである。従って、本発明は、クライアント側のリソースが非常に限られているようなネットワーク・ホスト・サービスの環境、例えば、クライアント装置は単にワールド・ワイド・ウェブへのブラウザ又はインターフェースとしてだけ機能するようなネットワーク環境においても実現することができる。

【００２１】

必要というわけではないが、本発明は、アプリケーション・プログラミング・インターフェース（ＡＰＩ）を介して実現することができ、これは、開発者によって使用される場合もあるし、及び／又は、クライアント・ワークステーション、サーバ又はそれ以外の装置など１又は複数のコンピュータによって実行されるプログラム・モジュールなどのコンピュータ実行可能な命令の一般的なコンテキストにおいて説明されるネットワーク・ブラウジング用ソフトウェアの中に含まれる。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、特定のタスクを実行する又は特定の抽象的なデータ・タイプを実現するものなど、を含む。典型的には、プログラム・モジュールは、様々な実施例において希望に従って組み合わせや分散が可能である。更に、当業者であれば理解するように、本発明は、他のコンピュータ・システム構成を用いても実現が可能である。本発明と共に用いるのが適切である他の広く知られたコンピューティング・システム、環境及び／又は構成（コンフィギュレーション）には、限定を意味しないが、パーソナル・コンピュータ（ＰＣ）、自動テラー・マシン、サーバ・コンピュータ、ハンドヘルド又はラップトップ型の装置、マルチプロセッサ・システム、マイクロプロセッサ・ベースのシステム、プログラマブルな家電製品、ネットワークＰＣ、ミニコンピュータ、メインフレーム・コンピュータなどが含まれる。本発明は、また、通信ネットワーク又はそれ以外のデータ伝送媒体を介してリンクされている遠隔（リモート）処理装置によってタスクが実行される分散型計算（コンピューティング）環境においても実現可能である。分散型の計算環境では、プログラム・モジュールは、メモリ記憶装置を含む

ローカル及びリモートの両方の記憶媒体に配置することができる。

【００２２】

図１は、従って、本発明を実現することが可能な適切な計算システム環境１００の一例を図解している。ただし、上述した通り、計算システム環境１００は、適切な計算環境の一例に過ぎず、本発明の使用及び機能の範囲に関するいかなる限定も意図するものではない。計算環境１００を、例示的な動作環境１００に図解されている複数の構成要素の中のいずれか又はそれらの組合せと関係する従属性又は必要条件を有するものと解釈すべきではない。

【００２３】

図１を参照すると、本発明を実現する例示的なシステムは、コンピュータ１１０の形態を有する汎用計算機を含む。コンピュータ１１０のコンポーネントには、限定は意味しないが、処理ユニット１２０と、システム・メモリ１３０と、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ユニット１２０に結合するシステム・バス１２１とを含む。システム・バス１２１は、メモリ・バス又はメモリ・コントローラを含む複数のタイプのバス構造、周辺バス、様々なバス・アーキテクチャの中のいずれかを用いるローカル・バス、の中の任意のものでありうる。例えば、限定を意味しないが、そのようなアーキテクチャには、インダストリ・スタンダード・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、エンハンストＩＳＡ（ＥＩＳＡ）バス、ビデオ・エレクトロニクス・スタンダーズ・アソシエーション（ＶＥＳＡ）ローカル・バス、ペリフェラル・コンポーネント・インターコネクト（ＰＣＩ）バス（これはまた、メザニン（Mezzanine）バスとしても知られている）などが含まれる。

【００２４】

コンピュータ１１０は、典型的には、様々なコンピュータ可読な媒体を含む。コンピュータ可読な媒体は、コンピュータ１１０によってアクセスされうる任意の入手可能な媒体でよく、揮発性及び不揮発性、取り外し可能及び取り外し可能でない媒体を含む。例えば、限定は意味しないが、コンピュータ可読な媒体は、コンピュータ記憶媒体と通信媒体とを含む。コンピュータ記憶媒体には、コンピュータ可読な命令、データ構造、プログラム・モジュール又はそれ以外のデータなど情報の記憶のための任意の方法又は技術において実現可能な揮発性及び不揮発性、取り外し可能及び取り外し可能でない媒体を含む。コンピュータ記憶媒体には、限定は意味しないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュ・メモリ又はそれ以外のメモリ技術、ＣＤＲＯＭ、デジタル・バーサタイル・ディスク（ＤＶＤ）又はそれ以外の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置又はそれ以外の磁気記憶装置、所望の情報を記憶するのに用いることができコンピュータ１１０によってアクセス可能な任意のそれ以外の媒体などが含まれる。通信媒体は、典型的には、コンピュータ可読命令、データ構造、プログラム・モジュール、搬送波やそれ以外の転送機構などの変調されたデータ信号の中のデータなどがその例であり、任意の情報搬送媒体を含む。「変調されたデータ信号」という用語は、信号の中の情報を符号化する態様でその特性の中の１又は複数が設定又は変更された信号を意味する。例えば、限定は意味しないが、通信媒体には、ワイアード・ネットワーク又は直接配線された接続などのワイアード媒体と、音響、ＲＦ、赤外線及びそれ以外のワイアレス媒体などのワイアレス媒体とが含まれる。上述したものの任意の組合せもまた、コンピュータ可読媒体の範囲に含まれる。

【００２５】

システム・メモリ１３０は、リード・オンリ・メモリ（ＲＯＭ）１３１やランダム・アクセス・メモリ（ＲＡＭ）１３２などの揮発性及び／又は不揮発性メモリの形態を有するコンピュータ記憶媒体を含む。基本入出力システム（ＢＩＯＳ）１３３は、立ち上げの際などにコンピュータ１１０の内部の要素の間で情報を転送するのを助ける基本ルーチンを含むが、典型的には、ＲＯＭ１３１の中に記憶されている。ＲＡＭ１３２は、典型的には、処理ユニット１２０によって直ちにアクセスが可能であり及び／又はその上で現に動作されるデータ及び／又はプログラム・モジュールを含む。例えば、限定は意味しないが、

図１には、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、それ以外のプログラム・モジュール１３６、プログラム・データ１３７などが図解されている。

【００２６】

コンピュータ１１０は、また、他の取り外し可能／取り外し不可能、揮発性／不揮発性のコンピュータ記憶媒体を含む。単なる例であるが、図１には、取り外し不可能な不揮発性磁気媒体からの読み出し及びそこへの書き込みをするハード・ディスク・ドライブ１４１と、取り外し可能で不揮発性の磁気ディスク１５２からの読み出し及びそこへの書き込みをする磁気ディスク・ドライブ１５１と、ＣＤやＲＯＭやそれ以外の光媒体など取り外し可能で不揮発性の光ディスク１５６からの読み出しとそこへの書き込みをする光ディスク・ドライブ１５５などが図解されている。この例示的な動作環境において用いることができる他の取り外し可能／取り外し不可能、揮発性／不揮発性のコンピュータ記憶媒体には、限定は意味しないが、磁気テープ・カセット、フラッシュ・メモリ・カード、デジタル・バーサタイル・ディスク、デジタル・ビデオ・テープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭなどが含まれる。ハード・ディスク・ドライブ１４１は、典型的には、インターフェース１４０安堵の取り外し不可能なメモリ・インターフェースを介したシステム・バス１２１と、典型的にはインターフェース１５０などの取り外し可能なメモリ・インターフェースによってシステム・バス１２１に接続されている磁気ディスク・ドライブ１５１及び光ディスク・ドライブ１５５に接続される。

【００２７】

上述した及び図１に図解されているドライブ及びそれと関連するコンピュータ記憶媒体は、コンピュータ１１０に、コンピュータ可読な命令、データ構造、プログラム・モジュール、それ以外のデータなどを提供する。図１では、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、それ以外のプログラム・モジュール１４６、プログラム・データ１４７などを記憶するものとして図解されている。注意してほしいのであるが、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、それ以外のプログラム・モジュール１３６、プログラム・データ１３７などと同じであるか異なるかのいずれかである。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、それ以外のプログラム・モジュール１４６、プログラム・データ１４７には、ここでは異なる参照番号が付与され、少なくとも、これらが異なるコピーであることを説明している。ユーザは、キーボード１６２や、通常はマウスやトラックボールやタッチ・パッドとして称されるポインティング・デバイス１６１などの入力装置を介して、コンピュータ１１０にコマンド及び情報を入力することができる。他の入力装置（図示せず）には、マイクロフォン、ジョイスティック、ゲーム・パッド、衛星ディッシュ、スキャナなどが含まれる。これらの及びそれ以外の装置は、多くの場合、システム・バス１２１に結合されているユーザ入力インターフェース１６０を介して処理ユニット１２０に接続されているが、パラレル・ポート、ゲーム・ポート、ユニバーサル・シリアル・バス（ＵＳＢ）などの異なるインターフェース及びバス構造によって接続される場合もある。

【００２８】

モニタ１９１又はそれ以外のタイプの表示装置もまた、ビデオ・インターフェース１９０などのインターフェースを介してシステム・バス１２１に接続されている。ノースブリッジ（Northbridge）などのグラフィクス・インターフェース１８２を、システム・バス１２１に接続することもできる。ノースブリッジは、ＣＰＵ又はホスト処理ユニット１２０と通信するチップセットであり、加速されたグラフィクス・ポート（ＡＧＰ）通信に対する責任を有する。１又は複数のグラフィクス処理ユニット（ＧＰＵ）１８４が、グラフィクス・インターフェース１８２と通信することができる。この点で、ＧＰＵ１８４は、一般に、レジスタ記憶装置などオンチップのメモリ記憶装置を含み、ビデオ・メモリ１８６と通信する。しかし、ＧＰＵ１８４は、単にコプロセッサの一例に過ぎず、様々なコプロセッサ（同時処理装置）がコンピュータ１１０に含まれうる。モニタ１９１又は他のタ

イプの表示装置は、また、ビデオ・インターフェース１９０などのインターフェースを介してシステム・バス１２１に接続され、ビデオ・インターフェース１９０は、ビデオ・メモリ１８６と通信することができる。モニタ１９１に加えて、コンピュータは、また、スピーカ１９７及びプリンタ１９６などの他の周辺出力装置を含むことがある。これらの周辺出力装置は、出力周辺インターフェース１９５を介して接続される。

【００２９】

コンピュータ１１０は、リモート・コンピュータ１８０など１又は複数のリモート・コンピュータへの論理接続を用いたネットワーク接続された環境で動作することもできる。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（peer）装置、それ以外の一般的なネットワーク・ノードであり、典型的には、コンピュータ１１０に関して上述した要素の多く又はすべてを含むが、図１には、メモリ記憶装置１８１だけが図解されている。図１に示されている論理接続は、ローカル・エリア・ネットワーク（ＬＡＮ）１７１とワイド・エリア・ネットワーク（ＷＡＮ）１７３とを含むが、それ以外のネットワークも含むことがある。そのようなネットワーク接続環境は、オフィス、企業単位のコンピュータ・ネットワーク、イントラネット、インターネットなどで一般的である。

【００３０】

ＬＡＮネットワーク接続環境において用いられる場合には、コンピュータ１１０は、ネットワーク・インターフェース又はアダプタ１７０を介して、ＬＡＮ１７１と接続されている。ＷＡＮネットワーク接続環境において用いられる場合には、コンピュータ１１０は、典型的には、モデム１７２や、インターネットなどのＷＡＮ１７３を介する通信を確立する他の手段を含む。モデム１７２は、内蔵の場合も外付けの場合もあるが、ユーザ入力インターフェース１６０又はそれ以外の適切な機構を介して、システム・バス１２１に接続することができる。ネットワーク接続された環境では、コンピュータ１１０との関係で上述したプログラム・モジュール又はその一部が、リモート・メモリ記憶装置に記憶されうる。例えば、限定は意味しないが、図１は、メモリ装置１８１に常駐するリモート・アプリケーション・プログラム１８５を図解している。示されているネットワーク接続は、例示であり、コンピュータの間で通信リンクを確立する他の手段を用いることもできる。

【００３１】

この技術分野の当業者であれば理解することであるが、コンピュータ１１０又はそれ以外のクライアント装置は、コンピュータ・ネットワークの一部として用いることができる。この点で、本発明は、任意の数のメモリ又は記憶ユニットと、任意の数又は容量の記憶ユニットにおいて生じる任意の数のアプリケーション及びプロセスとを有する任意のコンピュータ・システムに関するものである。本発明は、リモート又はローカルな記憶装置を有するネットワーク環境において用いられるサーバ・コンピュータとクライアント・コンピュータとを有する環境に応用することができる。本発明は、また、プログラミング言語機能と解釈及び実行能力とを有するスタンドアロンの計算機にも応用できる。

【００３２】

分散型のコンピューティングは、計算機及びシステムの間での直接の交換によって、コンピュータ・リソース及びサービスの共有を容易にする。これらのリソース及びサービスには、情報とキャッシュ記憶装置とファイルのためのディスク記憶装置との交換が含まれる。分散型のコンピューティングは、ネットワーク接続を利用して、複数のクライアントがその集合的な性能にレバレッジ（てこ）をかけて全体的な効果をねらうことを可能にする。この点で、様々な装置が、信頼のできるグラフィック・パイプラインのための本発明による認証技術を用いることができるように相互作用をするアプリケーション、オブジェクト又はリソースを有することができる。

【００３３】

図２は、ネットワーク接続されたすなわち分散型の例示的なコンピューティング環境の概略図を提供している。この分散型の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などと、コンピューティング・オブジェクト又は装置１１０

ａ、１１０ｂ、１１０ｃなどとを含む。これらのオブジェクトは、プログラム、方法（メソッド）、データ記憶、プログラマブル・ロジックなどを含む。これらのオブジェクトは、ＰＤＡ、テレビ、ＭＰ３プレイヤ、パーソナル・コンピュータなど、同一の又は異なる装置の一部を含む。それぞれのオブジェクトは、通信ネットワーク１４を介して、別のオブジェクトと通信することができる。このネットワークは、それ自体が、図２のシステムにサービスを提供することができる他のコンピューティング・オブジェクトやコンピューティング装置を含みうる。本発明のある特徴によると、それぞれのオブジェクト１０又は１１０は、信頼できるグラフィック・パイプラインのための本発明による認証技術をリクエストするアプリケーションを含む。

【００３４】

１１０ｃなどのオブジェクトは、別のコンピューティング装置１０又は１１０においてホストされる場合もありうる。従って、図面に示されている物理的な環境はコンピュータなどの接続された装置を示してはいるが、この図解は単なる例示であり、この物理的環境は、別の形態として、ＰＤＡ、テレビ、ＭＰ３プレイヤなどの様々なデジタル装置、インターフェースなどのソフトウェア・オブジェクト、ＣＯＭオブジェクトなどを含むように示す又は記述することも可能である。

【００３５】

分散型の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、コンポーネント及びネットワーク・コンフィギュレーションが存在する。例えば、コンピューティング・システムは、ワイアライン又はワイアレス・システム、ローカル・ネットワーク又は広範囲に分散されたネットワークによって相互に接続される場合もある。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ており、インターネットは、広範囲に分散されたコンピューティングのための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に広がっている。

【００３６】

家屋内のネットワーク接続環境には、電力線、データ（無線及びワイアード）、音声（例えば電話）及びエンターテイメント媒体というそれぞれが一意的なプロトコルをサポートする少なくとも４つの異なるネットワーク転送媒体が存在する。データ・サービスは、ブロードバンド（例えば、ＤＳＬ又はケーブル・モデム）として家屋に入り、ワイアレス（例えば、ホームＲＦ又は８０２．１１ｂ）又はワイアード（例えば、ホームＰＮＡ、Ｃａｔ５、更には電力線）の接続を用いて、その家屋の中でアクセス可能である。音声トラフィックは、ワイアード（例えば、Ｃａｔ５）又はワイアレス（例えば、携帯電話）として家屋に入り、Ｃａｔ３の配線を用いてその家屋の中で分散される。エンターテイメント媒体は、衛星又はケーブルを介して家屋に入り、同軸ケーブルを用いてその家屋内で分散されるのが典型的である。ＩＥＥＥ１３９４及びＤＶＩもまた、媒体装置で構成される複数のクラスタのためのデジタル相互接続として用いられはじめている。これらのネットワーク環境のすべて及びプロトコル標準として用いられるそれ以外の環境は、相互接続されて、インターネットを介して外部の世界と接続することができる。簡単に言うと、データの記憶及び伝送のために様々な異なるソースが存在しており、その結果、ますます、計算機は、データ処理パイプラインのあらゆる箇所においてコンテンツを保護する方法を必要としているのである。

【００３７】

「インターネット」という用語は、一般的に、コンピュータ・ネットワークの技術において広く知られているＴＣＰ／ＩＰプロトコルを用いているネットワーク及びゲートウェイの集合を意味する。ＴＣＰ／ＩＰとは、「トランスポート・コントロール・プロトコル／インターフェース・プログラム」の略語である。インターネットは、ユーザがネットワークを介して相互作用（インタラクト、対話）をして情報を共有することを可能にするネットワーク・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地理的に分散されたリモート・コンピュータ・ネットワークのシステムとして説明することができる。このような広範囲に広がった情報の共有により、インターネットなどのリモート・ネットワ

ークは、これまでに、開発者たちが特定の動作又はサービスを実行するソフトウェア・アプリケーションをほぼ制限なしに設計することができるオープン・システムに成長している。

【００３８】

このように、ネットワーク・インフラストラクチャにより、クライアント／サーバ、Ｐ２Ｐ又はハイブリッド・アーキテクチャなどのネットワーク・トポロジのホストが可能になる。「クライアント」とは、それ自体が関係していない別のクラス又はグループのサービスを利用するクラス又はグループのメンバーである。このように、コンピューティングにおいては、クライアントとはプロセスであり、すなわち、大まかに表現するなら、別のプログラムによって提供されるサービスをリクエストする命令又はタスクの集合である。クライアント・プロセスは、他のプログラム又は当該サービス自体に関するいかなる作業上の詳細を知ることを必要とすることなくリクエストしたサービスを利用する。クライアント／サーバ・アーキテクチャでは、特にネットワーク接続されたシステムでは、クライアントは、通常は、例えばサーバなどの別のコンピュータによって提供された共有のネットワーク・リソースにアクセスするコンピュータである。図２の例では、コンピュータ１１０ａ、１１０ｂなどはクライアントと考えることができ、コンピュータ１０ａ、１０ｂなどはサーバと考えることができる。ここで、サーバ１０ａ、１０ｂなどは、クライアント・コンピュータ１１０ａ、１１０ｂなどにおいて複製が作成されるデータを維持する。

【００３９】

サーバは、典型的には、インターネットなどのリモート・ネットワークを介して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のコンピュータ・システムにおいてアクティブであり、サーバ・プロセスは第２のコンピュータ・システムにおいてアクティブであり、相互に通信媒体を介して通信することにより、分散型の機能が提供され、複数のクライアントがサーバの情報収集能力を利用することが可能となる。

【００４０】

クライアントとサーバとは、プロトコル層によって提供される機能を用いて相互に通信する。例えば、ハイパーテキスト・トランスファ・プロトコル（ＨＴＴＰ）は、ワールド・ワイド・ウェブ（ＷＷＷ）との関係で用いられる一般的なプロトコルである。典型的には、ユニバーサル・リソース・ロケータ（ＵＲＬ）やインターネット・プロトコル（ＩＰ）アドレスなどのコンピュータ・ネットワーク・アドレスを用いて、サーバやクライアントは相互に識別する。ネットワーク・アドレスは、ＵＲＬアドレスと称することもある。例えば、通信は、通信媒体を介して提供されることもある。特に、クライアントとサーバとは、高性能通信のためにＴＣＰ／ＩＰ接続を介して相互に接合される場合がある。

【００４１】

このように、図２は、本発明を用いることができるネットワーク接続されたすなわち分散型の例示的な環境を図解しており、そこではサーバとクライアントとがネットワーク／バスを介して通信する。更に詳細には、多数のサーバ１０ａ、１０ｂなどが、ＬＡＮ、ＷＡＮ、イントラネット、インターネットなどである通信ネットワーク／バス１４を介して多数のクライアント又はリモート計算機１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅなどと相互に接続されている。クライアント又はリモート計算機の例としては、本発明によるポータブル・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（thin client）、ネットワーク接続された機器などがあり、ＶＣＲ、ＴＶ、オーブン、照明、ヒータ、などがある。本発明は、信頼できるソースからの安全なコンテンツを処理し記憶しレンダリングすることを希望する任意の計算機に応用可能である。

【００４２】

たとえば通信ネットワーク／バスがインターネットであるネットワーク環境では、サーバ１０は、クライアント１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅなどが任意の数のＨＴＴＰなどの既知のプロトコルを介して通信するウェブ・サーバでありうる。サーバ１０は、またクライアント１１０としても機能することができるのであるが、これは

分散型のコンピューティング環境の特徴である。通信は、状況に応じて適宜ワイアード又はワイアレスである。クライアント装置１１０は、通信ネットワーク／バス１４を介して通信することも通信しないこともあり、関連付けがなされた独立の通信を有する場合もある。例えば、ＴＶ又はＶＣＲの場合には、その制御に関してネットワーク接続された側面が存在する場合と存在しない場合とがある。クライアント・コンピュータ１１０とサーバ・コンピュータ１０とは、それぞれが、様々なアプリケーション・プログラム・モジュール又はオブジェクト１３５を装備していて、これらは様々なタイプの記憶素子又はオブジェクトへの接続又はアクセスを有している。様々なタイプの記憶素子又はオブジェクトには、ファイルを記憶することができ、ファイルの一部をダウンロード又は移動させることができる。このように、本発明は、コンピュータ・ネットワーク／バス１４にアクセスし相互作用可能なクライアント・コンピュータ１１０ａ、１１０ｂなどと、クライアント・コンピュータ１１０ａ、１１０ｂ及びそれ以外の装置１１１やデータベース２０との相互作用が可能なサーバ・コンピュータ１０ａ、１０ｂなどとを有するコンピュータ・ネットワーク環境において用いることができる。

権利管理（ＲＭ）の概要

知られているように、そして図３を参照すると、デジタル・コンテンツ３２がユーザに配信又は再配信されるデジタル・オーディオ、デジタル・ビデオ、デジタル・テキスト、デジタル・データ、デジタル・マルチメディアなどのデジタル・コンテンツ３２との関係で、権利の管理（rights management、ＲＭ）及び執行（engorcement、エンフォースメント）が強く望まれている。ユーザは、受信すると、パーソナル・コンピュータ３４などにおけるメディア・プレーヤ、テキスト表示装置などの適切なレンダリング装置を用いて、デジタル・コンテンツ３２をレンダリングする。

【００４３】

典型的には、コンテンツのオーナーや開発者、又は、このようなデジタル・コンテンツ３２を配信する配信者（ディストリビュータ）は、配信されたデジタル・コンテンツ３２との関係でユーザがすることが可能なことを制限することを望むし、少なくとも、希望しない態様でコンテンツが再配信されないことを望む。例えば、コンテンツ・ディストリビュータは、そのコンテンツ３２をコピーしたり第２のユーザに再配信したりしないようにユーザを制限することを望むし、あるいは、配信されたデジタル・コンテンツ３２が限定された回数だけレンダリングされる、一定の合計時間の範囲でレンダリングされる、特定のタイプのマシンにおいてのみレンダリングされる、特定のタイプのレンダリング・プラットフォームでだけレンダリングされる、特定のタイプのユーザによってのみレンダリングされる、などを望む場合がある。

【００４４】

しかし、上述したように、配信がなされてしまった後では、そのようなディストリビュータは、デジタル・コンテンツ３２に対しては、もしあるとしてもほんのわずかな制御（コントロール）しか有さない。ＲＭシステムは、そこで、任意の形式のデジタル・コンテンツ３２のレンダリングを制御することを可能にし、その場合に、そのような制御は柔軟性があり、当該デジタル・コンテンツ３２のコンテンツ・ディストリビュータによって定義可能となっている。典型的には、コンテンツ３２を保護するために、コンテンツ３２は、対称な暗号化／復号化鍵（ＫＤ）を用いて暗号化され（例えば、ＫＤ（ＣＯＮＴＥＮＴ））、３３の中に、コンテンツ３２と関連する他の情報と共にパッケージングされる。

【００４５】

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のディストリビュータは、そのようなデジタル・コンテンツ３２がユーザの計算機３４によってレンダリングされることが許可される前に充足しなければならない少なくともいくつかのライセンス規則を特定することが可能になる。このようなライセンス規則は、上述した一時的な条件を含むことがあり、ユーザ／ユーザの計算機３４（以後は、これらの用語は、状況に応じて必要な場合以外は相互交換可能である）が有していなければならないデジタル・ライセンス又はユーザ文書（以下では、「ライセンス」とする）において、具体化される。このよ

うなライセンス３６は、また、ユーザの計算機３４によって復号可能な鍵に従って暗号化されたデジタル・コンテンツ３２を復号する復号鍵（ＫＤ）を含む。図３に示されているように、このような暗号鍵は、ユーザの計算機３４の公開鍵（ＰＵ－Ｃ）であり、ユーザの計算機３４がそれによって復号が可能な（ＰＵ－Ｃ（ＫＤ））対応する秘密鍵（ＰＲ－Ｃ）を揺することが想定されている。

【００４６】

あるデジタル・コンテンツ３２のコンテンツ・ディストリビュータは、ライセンス３６においてコンテンツ・オーナー（コンテンツ権利者）によって特定された規則及び条件をユーザの計算機３４が順守することを信頼しなければならない。すなわち、ライセンス３６の中の規則及び条件が満足されなければ、デジタル・コンテンツ３２はレンダリングされないということを信頼しなければならない。ユーザの計算機３４には、当該デジタル・コンテンツ３２と関連付けがなされユーザによって取得されたライセンス３６において具体化されているライセンス規則に従う場合を除いてはデジタル・コンテンツ３２をレンダリングしないという信頼できるコンポーネント又は機構３８が備わっていることが好ましい。

【００４７】

信頼できるコンポーネント３８は、典型的には、ライセンス３６が有効であるかどうかを判断し、そのような有効なライセンス３６の中のライセンス規則及び条件を検討し、とりわけ、検討されたライセンス規則及び条件に基づいてリクエストをしているユーザがリクエストされたデジタル・コンテンツ３２を要求された態様でレンダリングする権利を有しているかどうかを判断するライセンス評価器４０を有する。理解すべきことであるが、ライセンス評価器４０は、ＲＭシステム３０において、ライセンス３６の中の規則及び条件に従ってデジタル・コンテンツ３２の権利者の希望を実行するという点で信頼され、ユーザは、どのような不正な又はそれ以外の目的であっても、そのような信頼素子を変更することができないようにすべきである。

【００４８】

理解できるであろうが、ライセンス３６の中の規則及び条件は、複数のファクタの中のいくつかに基づいて当該ユーザが当該デジタル・コンテンツ３２をレンダリングする権利を有しているかどうかを特定する。ただし、個のでの複数のファクタには、ユーザが誰であるか、ユーザがどこに位置しているか、ユーザがどのタイプの計算機を用いているか、どのレンダリング・アプリケーションがＲＭシステム３０をコールしているかなどが含まれる。更に、ライセンス３６の規則及び条件は、ライセンス３６を、例えば、所定の数のレンダリング回数や、所定のレンダリング時間に制限する場合がありうる。このように、信頼されるコンポーネント３８は、計算機３４に関してクロック４２を参照することを必要とする場合がある。そのようなクロック４２が提供される場合には、そのようなクロック４２は、ライセンス３６の一時的な制限を緩和するためにユーザが変更することができない安全なクロック４２である。

【００４９】

規則及び条件は、任意の適切な言語及びシンタクスに従って、ライセンス３６において特定することができる。例えば、言語は、単に属性と満足すべき値とを特定するか（例えば、日付はＸよりも後でなければならない）、又は、特定のスクリプト（例えば、IF DATE greater than X, THEN DO...など）。

【００５０】

ライセンス３６が有効であってユーザがその中の規則及び条件を充足しているとライセンス評価器４０が判断すると、デジタル・コンテンツ３２をレンダリングすることができる。特に、コンテンツ３２をレンダリングするには、復号鍵（ＫＤ）をライセンス３６から取得して、コンテンツ・パッケージ３３からの（ＫＤ（ＣＯＮＴＥＮＴ））に適用すると、その結果として、実際のコンテンツ（現実のコンテンツ、actual content）３２が得られ、この実際のコンテンツがレンダリングされる。上述したように、（ＰＵ－Ｃ（ＫＤ））を有するライセンスが、（ＫＤ）にアクセスするための（ＰＲ－Ｃ）を有する実体を

認証し、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。ただし、この実体は、ライセンス３６において設定されているすべての条件を順守していると仮定する。

【００５１】

典型的にはライセンス３６が認証／確認目的のためのデジタル署名を含むことに注意してください。同様に、１片のデジタル・コンテンツ３２のようなディジタル構成物の他の形式にはさらに認証／確認目的のためのそのようなデジタル署名があるかもしれない。知られているべきように、そのようなデジタル署名は、シグネチャが付けられており、次にキーを備えたハッシュを暗号化している基礎資料上である種のハッシュを行なうことにより、１ペアの非対称暗号鍵、あるいは対称な保全性キーからの最初のキーに例えば基づいて構築されるかもしれない。その後、そのシグネチャは、暗号化されたハッシュを解読し解読されたハッシュをシグネチャが付けられている基礎資料の別のハッシュと比較することにより、ペアの非対称暗号鍵から２番目のキーあるいは保全性キーを塗ることにより再び例えば確認される。ハッシュが一致する場合、それはそれと推定することができる、基礎資料、変更されていない、また、根本的なものは構築する、したがって、確証することができる。典型的には、ＲＭシステム３０は、確証されないライセンス３６などを尊敬しないだろう。受理と取り扱い用システムはマルチメディア内容３２を流した

図４、受理用のシステム４４および取り扱いマルチメディア内容３２に今変わることは示される。明白であるべきように、そのようなシステム４４は、マルチメディア内容３２の多数のストリームを含む入力信号の扱いに特に適している、のように、例えば、テレビジョン信号、から、１つの、マルチ―チャネル・ディストリビュータ。しかしながら、そのようなものはシステム４４になるだろう、さらに本発明の趣旨およびスコープから外れずに、他の入力信号を扱ってもよい。

【００５２】

システム４４では、それのディストリビュータによって提供されるような前述の入力信号は、本発明の趣旨およびスコープから外れずに、任意の適切なレシーバーかもしれない（もちろんをを、そのようなレシーバー、できる、考えて）レシーバー４６に適用される、ここに発表された機能を行なう。例えば、レシーバー４６は、ディジタル・ケーブルテレビ信号を受け取り、かつさらに内容３２のレンダーリングをそこに含むディジタル加工のために同じを進めるために開発されているような片方向ケーブル・レシーバ（ＵＤＣＲ）かもしれない。評価されるかもしれないように、複合のもののうちの１つがマルチメディアに流す、そのように命じられた調子であることの上のレシーバー４６は、その後の処理のために入力信号および前方へ同じから３２を満足させる。さらに、内容３２の調整されたストリームを進める前のレシーバー４６はしてもよい、必要ならば、そのようなストリーム３２をそのようなその後の処理に対してより法的責任のある在来のフォーマットからフォーマットに変換する。

【００５３】

構想を描かれるように、入力信号中のマルチメディア内容３２の多数のストリームの各々は暗号化されるかもしれないし、暗号化されないかもしれない。入力信号内の内容３２の特別のストリームを合わせる際、それでは、もし暗号化されれば、レシーバー４６はそのようなストリームを解読する、そして再組立、より詳細に下に述べられる方法においてより詳細に下に述べられるだろうか、もし暗号化されなければ単に再びストリームを暗号化する方法において同じ上に示唆されたように、レシーバー４６は、ストリームがＲＭ保護されることを保証する部分として内容３２のストリームを暗号化する。したがって、内容３２のストリームは非保護の形式で再分配されることが利用可能ではない。

【００５４】

さらに図４に示されるように、媒体システム４８はレシーバー４６から内容３２の暗号化されたストリームを受け取り、かつさらに同じを処理するために提供される。推測上、そのようなコマンドが本発明の趣旨およびスコープから外れずに、他のソースによって始められるかもしれないことをそれは恐らく認識したが、媒体システム４８は恐らくユーザ

ーから対応するコマンドを受け取ることで、入力信号の内部からの内容３２の特別のストリームを合わせることをレシーバー４６に命じた。とにかく、レシーバー４６から内容３２のストリームを受け取る際、媒体システム４８は、回復とレンダーリングのために適切な記憶装置５０に同じを直ちにあるいはある時間遅れで格納する。ストリーム３２のレンダーリングに際して、媒体システム４８は、前方へ１つ以上のモニター５２、スピーカー５４、他のディスプレイ５６などのような１つ以上の出力デバイスに信号を充当する。

【００５５】

格納されたストリーム３２としてのＩｎａｓｍｕｃｈはＲＭに保護された形式である、媒体システム４８は、信頼されたコンポーネント３８のようなＲＭコンポーネントを含んでいる、エバリュエーター４０および図３のクロック４２を許可する。したがって、特別のストリーム３２を検索する際、媒体システム３８は同じを与える、しかしより詳細に下に述べられるのと同じくらい対応するライセンス３６に従ってのみ。従って、暗号化されたストリーム３２は、ライセンス３６にそのようなライセンス３６がそのように許可するかどうかに、および内容キー（ＣＫ）セットでのみ前へ解読され与えられる。暗号化されたストリーム３２が（一世）媒体システム４８上に少なくとも一時的に格納されるので、理論上そのために与えるために、別の（秒）媒体システム４８にそれのユーザーが同じをコピーしてもよいことに注意してください。しかしながら、ストリームが暗号化され、ライセンス３６によってのみ解読することができるので、およびライセンス３６が最初の媒体システム４８に結び付けられるので、そのようなライセンス３６は第２の媒体システム４８によって雇われないかもしれない。

【００５６】

しかしながら、理解されるに違いないように、それは、最初の媒体システム４８がそうすることができる事実にあると考えて、最初の媒体システム４８が第２の媒体システム４８へのコピーされたストリーム３２用の再実施権３６を出すことができるというその場合かもしれない。また、ライセンス３６はそのように許可する。そうならば、第２の媒体システム４８に結び付けられるように再実施権３６は、より詳細に下に述べられるとともにストリーム３２を与える第２の媒体システム４８によって、実際雇うことができる。媒体システム４８にレシーバー４６からのライセンス必要条件を伝えること

上に述べられたように、恐らく一度と同じくらいのの命令で、適正にレギュラーベース上の入力信号からの異なるディジタルストリーム３２に合わせるべき媒体システム４８から、レシーバー４６がコマンドを受け取ると予想することができることは認識されることになっている、１秒まで皆半分、特に媒体システム４８のユーザーが有効である場合、かすめて飛ぶこと、によって、あるいは「サーフィン」いくつかのストリーム３２。しかしながら、新しく調整されたストリーム３２はそれぞれ、新しい内容キー（ＣＫ）を備えた新しい対応するライセンス３６を要求する。典型的には、そのようなライセンス３６はレシーバー４６によって構築され、レシーバー４６から媒体システム４８にちょうど調整されたストリーム３２を伝える前に送られるだろう。

【００５７】

しかしながら、特にライセンス３６が詳述される場合、そのような新しいライセンス３６を構築し媒体システム４８にレシーバー４６から同じを送ることが、全く厄介かもしれないことは認識されることになっている、暗号化されたエレメントを含んでいる、デジタル署名などを含んでいる。したがって、レシーバー４６が新しく調整されたストリーム３２の新しいライセンス３６を完全に構築することができることは恐らく期待されない場合がある、ごとに、媒体システムコマンド、そのようなレシーバー、に、事実調子中で、そのようなストリーム３２。前述のサーフィン・シチュエーションのための場合であるように、そのようなコマンドの周波数が２等品の命令である場合、これは特に真実である。さらに、レシーバー４６には迅速なやり方でそのようなライセンス３６を構築するのに必要かもしれないのと同じくらい特に重要な計算能力が提供されていなければ、これは特に真実である。とにかく新しいストリーム３２がそうであるように命じる典型的なユーザー－調整された、コマンドが出された後、高々１秒あるいは２秒でそのような新しいストリー

ム３２が与えられ示されることと予想するだろう。

【００５８】

明白に、それでは、ストリーム３２が新しく調整されるごとに、レシーバー４６は恐らく新しいライセンス３６を送ることができない。代わりに本発明の１つの実施例の中で、レシーバー４６は作成し送る、１つの、略記された、あるいは、レシーバー４６を代表してそのような新しいライセンス３６を構築するために、そのような新しいライセンス３６に入る必要条件４７の短縮版およびそのような必要条件４７を受け取ることの上の媒体システム４８に、レシーバー４６によって推測上レシーバー４６に利用可能なものより大きな計算能力の援助が任せられる。

【００５９】

推測上、レシーバー４６は、ストリーム３２内の情報４９からのストリーム３２用の必要条件４７をそれ自体決定する。ストリーム３２の情報４９からのそのような必要条件４７の決定は知られているか、適切な公に明白であるべきであり、したがって、ここに少しも詳細に述べられる必要はない。また、従って、ストリーム３２からのそのような必要条件４７を決定するどんな方法も本発明の趣旨およびスコープから外れずに雇われるかもしれない。例えば、それは、分配されるようなストリーム３２に既知の間隔および場所で情報４９が周期的に供給されるというその場合かもしれない。

【００６０】

レシーバー４６によって特別のストリーム３２のために指定されるような必要条件４７は、もちろん本発明の趣旨およびスコープから外れずに、任意の必要条件４７かもしれない。しかしながら、典型的には、必要条件４７は、最初の媒体システム４８の記憶装置５０に格納され、そのような第１の媒体システム４８に許可されるようなストリーム３２が別の媒体システム４８に実際コピーされシステムにサブ許可されるかもしれないかどうか少なくとも一部分明示する。例えば、そのようなコピー権は、コピーとして自由に（ＣＦ）述べられるかもしれない、コピー、一度（ＣＯ）、コピーする、決してない（ＣＮ）、など。

【００６１】

したがって、本発明で、レシーバー４６は間接費に行く必要はない、すべての時間そのような新しいライセンス３６を構築する事実では、そのようなレシーバー４６は新しく特別のストリーム３２を合わせて、ユーザーが変更が見えていても、レシーバーが新しくストリーム３２を合わせるごとに、そのようなライセンス３６の必要条件４７の短縮版を、速く作成することができ、媒体システム４８に送ることができる、の命令で、一度、すべての２位、程度。

【００６２】

さらに、また、必要条件４７だけを送ることにより評価されるかもしれないとともに、そしてない、ライセンス３６、それ自体、レシーバー４６は、ライセンス３６のどんな特別のフォーマットもそれ自体負わせられる必要はない。したがって、あるポイントでは、新フォーマットがライセンス３６に対して指定される場合、単にレシーバー４６ではなく媒体システム４８にそのようなフォーマットを伝える必要がある。

【００６３】

まだ図４を指して、レシーバー４６からストリーム３２を受け取ることに加えて、媒体システム４８が他のソースからさらに直接あるいは間接的にストリーム３２を受け取るかもしれないことは理解される。他のそのようなソース、だろう、例えばＮＴＳＣ入力信号、ＡＴＳＣ入力信号などを含む。見られたとともに、のために、個々、少なくともいくつかの入力信号の、直接受け取った、それは、媒体システム４８が両方へのレシーバー４６の方法で作用するハードウェアまたはソフトウェアのゲートウェイ５８を含んでいるというその場合かもしれない、受信入力信号内のストリーム３２を媒体システム４８により従順な暗号化されたフォーマットに変換する、そしてさらに作成し送ることために１つの、略記された、あるいはストリーム３２用の必要条件４７の短縮版、それは媒体システム４８によって作成されるような新しいライセンス３６に入るだろう。ここで、ゲートウェイ

５８は、ストリーム３２内の情報４９からのストリーム３２用の必要条件４７をそれ自体決定することができたか、あるいはそのようなストリーム３２からそうでなければ利用可能なデフォルト必要条件４７を構成することができた。

【００６４】

本発明の１つの実施例では、任意の特別のソースからの任意の特別のストリーム３２に提供されるような必要条件４７は、共通形式で述べられる。従って、媒体システム４８は異なるソースに対応する複数フォーマットに関係のある必要がない。本発明の１つの実施例では、媒体システム４８に、あるいはそのシステム内に速く容易に必要条件４７を送信することができるように、共通形式は比較的略した性質である。また、媒体システム４８は同様に速くそこからライセンス３６を構築することができる。

【００６５】

例えば、今、図５に変わって、本発明の１つの実施例では、共通形式が３２ビットを多くのあらかじめ定義されたフィールドに分割することは理解される（そして）。フィールドは以下のように定義される：

－　インプット・コピープロテクト方法　－　このフィールドは、対応するストリーム３２の特別の内容保護法への前もって定義したやり方で一致する、８ビットの値を指定する。

そのような内容保護法は含んでいるかもしれないが、次のものに制限されていない：

無　－　コピープロテクトはストリーム３２のために指定されない。また、ＲＭに基づいた制限は、同じに課されるべきでない。

ハードウェア・マクロビジョン　－　ストリーム３２は保護されたマクロビジョン（波形）である。

ＣＧＭＳ－Ａ　－　ストリーム３２はＩＥＣ　６１８８０あるいはＥＩＡ－６０８－Ｂによって指定されるようなＣＧＭＳ－Ａ内容プロテクションを含んでいる。

ＷＳＳ　－　ストリーム３２はＩＴＵ－Ｒ　ＢＴ　１１１９－１によって指定されるようなＷＳＳプロテクションを含んでいる。

ケーブル研究所ディジタル・ケーブル　－　ストリーム３２はケーブル研究所ＵＤＣＲレシーバー４６に配達された。

ＡＴＳＣ　－　ストリーム３２は高画質テレビシステム受託者（ＡＴＳＣ）フォーマットで伝えられた。

－　入力装置は頑強性規則に会う　－　入力装置（例えばレシーバー４６としての同調器カード）が、インプット・コピープロテクト方法によって定義されたその頑強性規則に遭遇する場合、この１ビットのフィールドは１にセットされる。

－　コピー・デフォルト　－　コピープロテクト必要条件４７がストリーム３２からまだ分からない場合、この１ビットのフィールドは１にセットされる。また、デフォルト・コピープロテクトが適用されることになっている。

－　フラグ／制限された内容を放送してください　－　この１ビットのフィールドはＡＴＳＣに特有で、ストリーム３２が再配送コントロールされる場合、１にセットされる。

－　ＣＩＴ　－　この１ビットのフィールドはケーブル研究所ディジタル・ケーブルに特有で、制約付きのイメージが起きている場合、１にセットされる。

－　ＡＰＳ　－　この２ビットのフィールドはあるマクロビジョン・フォーマットに特有のアナログ保護システム必要条件４７を表わす。

－　コピー制御価値－この２ビットのフィールドは言う、ストリーム３２は、どのように媒体システム４８から別の媒体システム４８にコピーされるかもしれないか（サブ許可された）：

コピー、自由に（ＣＦ）、コピー、一度（ＣＯ）、コピーする、決してない（ＣＮ）、など。

【００６６】

顕著に、図５に示される１つの具体化では、３２ビットのうちの１６ビットは後の使用のために取っておかれる。従って、現在のタイプのコピープロテクトの中に既にある追加

機構かもしれないとともに、新しいタイプのコピープロテクトに特有の特徴は予約のビット内にインプリメントされるかもしれない。さらに顕著に、あるタイプのコピープロテクトに関するのみ使用のために現在取っておかれる特定ビット、そしてしたがって他のタイプのコピープロテクトに役に立つように、しかしながら異なる目的のための他のそのようなタイプのコピープロテクトに関して雇われるかもしれない。

【００６７】

以上から理解できるように、特定のストリーム３２に対応するライセンス３６のための条件４７を表す一般的なフォーマットを用いることによって、そのような条件４７を、配信されたそのようなストリーム３２のどの特定のフォーマットにも限定されない一般的な態様で特定することができる。条件４７は、どの特定のソース・コンテンツ保護機構にとっても特有ではない態様で簡潔に特定され、受信機４６やゲートウェイ５８（以下では、状況により必要にならない限り、「受信機４６」と称する）などの比較的単純な装置が、任意の特定のフォーマットから条件４７を導くことができ、一般的なフォーマットに変換することができる。

【００６８】

次に、図６を参照すると、コマンドに応答して受信機４６によって特定のストリーム３２をチューニングするのに用いられる方法が示されている。理解し得るように、このようなコマンドは、典型的には、最初はユーザによって媒体システム４８に（ステップ６０１）、次に、媒体システム４８から受信機４６に（ステップ６０３）に発行される。ただし、それとは異なり、媒体システム４８は、そのようなチューニング・コマンドがユーザからの促しなしでも発行することができ、そのような場合でも本発明の範囲に含まれる。いずれにしても、チューニング・コマンドに応答して、受信機４６は、発行の時点でストリーム３２を実際にチューニングする（ステップ６０５）。そのようなチューニングは、一般的に知られており、本発明に関係する一般的な公衆にはは明らかなはずであるので、ここでは詳細は割愛する。従って、このようなチューニングは、本発明の精神及び範囲から逸脱することなく、任意の適切な態様で実行することができる。

【００６９】

いったんチューニングされると、受信機４６は、必要に応じてストリーム３２を復号し（ステップ６０７）、媒体システム４８と共有されている対称コンテンツ鍵（ＣＫ）に従って再び暗号化する（ステップ６０９）。そのようなコンテンツ鍵（ＣＫ）を媒体システム４８と共有する方法の１つが、以下で説明される。ただし、そのような方法は、本発明の精神及び範囲から逸脱することなく、用いることができる。

【００７０】

更に、復号されたストリーム３２から、受信機４６は、ストリーム３２に対応するライセンス３６のための条件４７と関係する上述した情報４９を発見する（ステップ６１１）。上述したように、条件４７を有する情報４９は、既知の間隔及び位置において、ストリーム３２の中で周期的に供給される。例えば、この既知の間隔は２０秒の１回というオーダーであり、位置は、ストリーム３２がデジタルである場合には特定の識別されたパケットであり、ストリーム３２がアナログである場合には特定のビデオ・ブランキング間隔である。後で詳述するが、受信機４６がまだストリーム３２においてそのような情報４９と遭遇しておらず、情報４９を待つのは実行可能でない場合には、受信機４６は、情報４９の何らかのデフォルトの集合に基づいて条件４７を送信することによって先に進み、実際の情報４９が受信された後の時点で、実際の条件４７を送信する。

【００７１】

いずれにしても、発見された情報４９を用いて、受信機４６は、条件４７が上述した一般的なフォーマットで表現されるストリーム３２に対応する条件４７の集合を構築し（ステップ６１３）、その条件４７を媒体システム４８に送信し（ステップ６１５）、特に、媒体システム４８の信頼されるコンポーネント３８に送信する。その後で、媒体システム４８は、条件４７に基づいてライセンス３６を構築して（ステップ６１７）、構築されたライセンス３６をそのライセンス３６記憶装置６０又は類似の場所に記憶する（ステップ

６１９）。

【００７２】

条件４７からライセンス３６を構築することは、一般的に知られている内容であり、関係者には明らかであるから、ここではその詳細は割愛する。従って、ライセンス３６の構築は、本発明の精神及び範囲から逸脱することなく、適切な態様で実行することが可能である。例えば、条件４７が上述した又は類似の３２ビットの一般的なフォーマットに従って表現されている場合には、媒体システム４８は、ビットのそれぞれのフィールドを所定のマッピング規則に従ってライセンス３６にマップするマッピング・アルゴリズムを用いることができる。

【００７３】

注意すべきであるが、ライセンス３６を構築する際には、媒体システム４８は当該ストリームのためのコンテンツ鍵（ＣＫ）を記憶していることが想定でき、（ＣＫ）は媒体システム４８の公開鍵（ＰＵ－ＭＳ）などの別の鍵に従って暗号化されたライセンス３６の中で後述する態様で取得できて、結果的に（ＰＵ－ＭＳ（ＣＫ））を得る。このようにして、その媒体システム４８だけが、（ＰＵ－ＭＳ）に対応する秘密鍵（ＰＲ－ＭＳ）の助けを借りて、ライセンス３６からの（ＰＵ－ＭＳ（ＣＫ））から（ＣＫ）にアクセスすることができる。結果的に、ライセンス３６は、媒体システム４８と結合していると言うことができ、どの他の媒体システム４８や他の装置によっても用いられない。例えば無料コピー（ＣＦ）とか１回だけコピー（ＣＯ）とか表明することによって、媒体システム４８が別の媒体システム４８がストリーム３２をレンダリングするためのサブライセンス３６を発行することをライセンス３６が認証する場合には、媒体システム４８は、サブライセンス３６を作成する際に最初に（ＰＲ－ＭＳ）を（ＰＵ－ＭＳ（ＣＫ））に適用して（ＣＫ）を明らかにし、次に、別の媒体システム４８の（ＰＵ－ＭＳ）に従って（ＣＫ）を暗号化しなければならず、その新たな（ＰＵ－ＭＳ（ＣＫ））をサブライセンス３６の中に挿入する。

【００７４】

注意すべきであるが、媒体システム４８は、特定のストリーム３２のためのコンテンツ鍵（ＣＫ）を、同じストリーム３２のための対応するライセンス３６を構築する前に、有している可能性が高く、従って、コンテンツ（ＣＫ）を用いて受信機４６から送信された暗号化されているストリームを復号し、そのようにして復号されたストリーム３２をレンダリングする（ステップ６２１）。従って、ステップ６１７及び６１９のように、媒体システムがライセンスを構築して記憶することの必要性に疑問をもつことが可能である。しかし、理解すべきであるように、記憶されたライセンス３６は、媒体システム４８がリセットなどの間に（ＣＫ）を失う場合などコンテンツ鍵（ＣＫ）を検索する必要がある場合には、媒体システム４８によって用いられる。同様に、媒体システム４８が記憶装置５０からのストリーム３２を遅れて再生している場合には、ライセンス３６は、（ＣＫ）が記憶される唯一の位置である可能性がある。また、ライセンス３６は、ストリーム３２と関連するどのような著作権を記憶し検索するのに必要であり、この点では、後で言及することが必要になるであろうストリーム３２と対応する他の条件４７も同様である。

【００７５】

どの特定のストリーム３２でも、その情報４９は、１回又は複数回変化する可能性がある。もしそうであれば、受信機４６は、ステップ６１３及び６１５のように、新たな条件４７を媒体システム４８に発行しなければならず、媒体システム４８は、ステップ６１７及び６１９のように、新たなライセンス３６を構築して記憶しなければならない。このようにして、受信機４６は、ストリーム３２の中の情報４９のそれぞれの集合について自覚しなければならず、情報３９の素養な集合がいつストリーム３２の中で変化したかを注意しなければならない。

受信機４６と媒体システム４８との間でのコンテンツ鍵の共有

上述したように、受信機４６は、異なるストリーム３２をチューニングする度に、異なるコンテンツ鍵（ＣＫ）に従って暗号化され新たにチューニングされたストリーム３２を

送信し、更に、対応する条件の集合も送信する。従って、受信機４６と媒体システム４８とは、コンテンツ鍵（ＣＫ）を共有しなければならず、特に、媒体システム４８は受信機４６が特定のストリーム３２を暗号化するのにどのコンテンツ鍵（ＣＫ）を用いたのかを知らなければならない。

【００７６】

しかし、著しいことには、受信機４６がそれぞれの特定のストリーム３２に対するそれぞれのコンテンツ鍵（ＣＫ）を例えば条件４７の一部として又は典型的なＲＭライセンス３６の中で媒体システム４８に送るということは現時点では考えられない。上述したように、受信機４６がそれぞれの新たにチューニングされたストリーム３２に対してそのような典型的なＲＭライセンス３６を構築して送信することは期待できない。というのは、そのようなライセンス３６を構築することは非常に労働集約的（面倒）であるし、新たなチューニングされたストリーム３２が毎秒１回程度の頻度で要求されるような場合がありうるからである。従って、受信機４６と媒体システム４８とは、異なる通信方法を介して、そのようなコンテンツ鍵（ＣＫ）を共有しなければならない。

【００７７】

よって、本発明のある実施例では、受信機４６と媒体システム４８とは、初期化の一部として、多かれ少なかれ典型的なＲＭライセンス３６によって最初のコンテンツ鍵（ＣＫ０）を共有し、次に、受信機４６と媒体システム４８とのそれぞれが、（ＣＫ（０））から新たなコンテンツ鍵（ＣＫｘ）を直接的に又は間接的に必要に応じて強調した態様で導く。着目すべきことであるが、初期化ＲＭライセンス３６は、別の初期化が必要となるまで１回だけ要求され、よって、そのようなＲＭライセンス３６の労働集約的な側面に、別の初期化が必要となるまで１回直面するだけである。そのような初期化は、本発明の精神及び範囲から逸脱することなく、任意の適切な間隔に従って実行される。例えば、初期化は、数時間又は数日に１回程度の頻度で実行されるか、又は、媒体システム４８が始動される又はリセットされる度に１回実行される。

【００７８】

本発明のある実施例では、次に図７を参照すると、初期化イベントのときに、媒体システム４８は、初期化リクエストを受信機４６に送る（ステップ７０１）。この初期化リクエストは、受信機４６によって信頼されている権威又は一連の権威によって媒体システム４８に発行されたマシン証明書などを含む。この送信されたマシン証明書には媒体システム４８の公開鍵（ＰＵ－ＭＳ）が含まれ、媒体システム４８は対応する秘密鍵（ＰＲ－ＭＳ）を有している。

【００７９】

次に、受信機４６は、媒体システム４８は信頼できるという送られてきたマシン証明書に基づいた確認を行い、初期化ＲＭライセンス３６を構築して（ステップ７０３）、この初期化ＲＭライセンス３６を媒体システム４８に送る（ステップ７０５）。初期化ライセンス３６は、受信機４６によって判断された最初のコンテンツ鍵（ＣＫ０）を含み、この最初のコンテンツ鍵（ＣＫ０）は、マシン証明書からの公開鍵（ＰＵ－ＭＳ）に従って暗号化され結果的に（ＰＵ－ＭＳ（ＣＫ０））を生じる。よって、媒体システム４８は、初期化ライセンス３６を受信してライセンス記憶装置６０に記憶すると、そこから（ＰＵ－ＭＳ（ＣＫ０））を検索し、それに（ＰＲ－ＭＳ）を適応して結果的に（ＣＫ０）を得て（ステップ７０７）、その（ＣＫ０）を適切で安全な位置にカウントと共に記憶する。このカウントは、ゼロに設定される（ステップ７０９）。受信機４６は、また、この（ＣＫ０）を、同じゼロ・カウントと共に、適切で安全な位置に記憶する。

【００８０】

この時点で、初期化ライセンス３６は受信機４６によって署名される場合があり、そのような場合に、受信機４６は、対称完全（symmetric integrity）鍵（ＩＫ）を用い、ＭＡＣなどの対称署名プロトコルに基づいて初期化ライセンス３６に署名をする。この場合、本発明のある実施例では、最初のコンテンツ鍵（ＣＫ０）と最初の完全鍵（ＩＫ０）である完全鍵（ＩＫ）とは、共に、マシン証明書からの公開鍵（ＰＵ－ＭＳ）に従って暗号

化され結果的に（ＰＵ－ＭＳ（ＣＫ，ＩＫ０））を生じる。ここで、媒体システム４８は、初期化ライセンス３６を受信すると、そこから（ＰＵ－ＭＳ（ＣＫ，ＩＫ０））を検索し（ＰＲ－ＭＳ）を適用して（ＣＫ０）及び（ＩＫ０）をステップ７０７で得る。そして、次に、ステップ７０９において、（ＣＫ０）及び（ＩＫ０）をゼロ・カウントと共に適切で安全な位置に記憶する。更に、媒体システム４８は、この最初の完全鍵（ＩＫ０）を用いて、初期化ライセンス３６の署名を確認する。

【００８１】

以上をまとめると、受信機４６と媒体システム４８とは、安全な位置に、最初のコンテンツ鍵（ＣＫ０）と、最初の完全鍵（ＩＫ０）と、ゼロに設定されたカウントとを記憶する。しかし、受信機４６は、何らかのコンテンツ鍵（ＣＫ）や何らかの対応する条件４７に従って暗号化されたストリーム３２を媒体システム４８にまだ送信していない。しｋし、媒体システム４８は、いずれかの時点で、そのような状況の第１の例を、図６のステップ６０３において、命じることになる。従って、受信機４６は、図６のステップに沿って進んで、第１のストリーム３２をステップ６０７において暗号化するための第１の新たな対称コンテンツ鍵（ＣＫｘ）である（ＣＫ１）を要求する時点に到達する。

【００８２】

ここで、本発明のある実施例では、受信機４６は、カウントをインクリメントし（ステップ７１１）最初のコンテンツ鍵（ＣＫ０）から（ＣＫｘ）／（ＣＫ１）を導くことによって、コンテンツ鍵（ＣＫｘ）／（ＣＫ１）を発生する（ステップ７１３）。更に、そのような（ＣＫｘ）を最初のコンテンツ鍵（ＣＫ（０））から導くときには、受信機４６は、最初の完全鍵（ＩＫ０）から対応する完全鍵（ＩＫｘ）／（ＩＫ１）を導く（ステップ７１５）。

【００８３】

本発明のある実施例では、コンテンツ鍵（ＣＫｘ）と完全鍵（ＩＫｘ）との両方が、最初の値（ＣＫ（０））又は（ＩＫ（０））を新たなカウント値と共に「値（ｘ）＝関数（値（０），カウント）」という関数に適用することによって、（ＣＫ（０））と（ＩＫ（０））とからそれぞれ導かれる。例えば、この関数は、ＳＨＡ関数などの一方向ハッシュ関数であり、必要に応じて、適切なトランケーション（切断、truncation）又は伸長（lengthening）とを備えている。従って、コンテンツ鍵（ＣＫｘ）を用いて、受信機４６は、ステップ６０９でのように、ストリーム３２を暗号化する。

【００８４】

本発明のある実施例では、受信機４６は、図６のステップ６１３及び６１５のようにストリーム３２に対応する条件４７の集合を構築して条件４７を媒体システム４８に送るとき、鍵（ＣＫｘ，ＩＫｘ）の派生物（derivation）又は回転（rotation）と新たなカウントとを媒体システム４８に通信する。特に、本発明のある実施例では、受信機４６は、ステップ６１３及び６１５を実行するときには、ステップ７０５において送られた初期化ライセンス３６の中の値に基づくその中の値を用いて、導かれたメッセージ６２を構築する。

【００８５】

特に、例えばカウント＝１と対応する第１のストリーム３２など、特定のカウントｘと対応する任意の特定のストリーム３２に対して、受信機４６は、当該ストリーム３２のための条件４７とカウントｘと完全鍵（ＩＫｘ）とを含む導かれたメッセージ６２を構築し（ステップ７１７）、構築された導かれたメッセージ６２を媒体システム４８に送信する（ステップ７１９）。署名が対称鍵に基づく限り、そのような導かれたメッセージ６２を構築することは、非対称鍵に基づく署名と比較すると、受信機４６にとってそれほど面倒ではない。

【００８６】

いずれにしても、ストリーム３２とそれに対応する導かれたメッセージ６２とを受信すると、媒体システム４８は、それ自身で、受信した導かれたメッセージ６２と（ＣＫ（０））と（ＩＫ（０））とステップ７１５で用いられた関数とに関する知識に基づいて、対

応するコンテンツ鍵（ＣＫｘ）と完全鍵（ＩＫｘ）とを導く。特に、受信機４６の場合のように、媒体システム４８は、（ＣＫ（０））と（ＩＫ（０））とのそれぞれを発見し（ステップ７２１）、受信機４６と同じ関数と現在のカウントｘとを用いることによって（ＣＫｘ）と（ＩＫｘ）とを導き（ステップ７２３）、導かれた（ＣＫｘ）と（ＩＫｘ）とを対応するカウントと共に適切に記憶する（ステップ７２５）。更に、媒体システム４８は、完全鍵（ＩＫｘ）を用いて、対応する導かれたメッセージ６２の署名を確認する（ステップ７２７）。更に、ストリーム３２に対応するコンテンツ鍵（ＣＫｘ）を用いて、対応する導かれたメッセージ６２が確認し許容することを想定すると、媒体システム４８は、レンダリング及び／又は更なる処理のためにストリーム３２を復号することができる（ステップ７２９）。

【００８７】

注意すべきであるが、媒体システム４８によって受信機４６から受信された導かれたメッセージ６２は、図６のステップ６１７及び６１９のように媒体システム４８によって構築されライセンス記憶装置６０に記憶されたライセンス３６ではない。そうではなく、導かれたメッセージ６２は、ステップ６１７及び６１９のライセンス３６を構築するのに用いられた条件を含む。

【００８８】

この出願において説明されている本発明を用いると、受信機４６は、すべての新たにチューニングされたストリーム３２について、コンテンツ鍵（ＣＫｘ）又は完全鍵（ＩＫｘ）を媒体システム４８に明確に通信することを必要としない。その代わりに、受信機４６は、単に、媒体システム４８を用いて鍵（ＣＫ０，ＩＫ０）の初期値を確立すればいいだけであり、受信機４６と媒体システム４８とはそれぞれが、（ＣＫ（０），ＩＫ（０））と導く（誘導する）ための関数とに関する先行する知識に基づいて、それぞれの新たなストリーム３２に対する新たな値（ＣＫｘ，ＩＫｘ）を独立に導くことができる。このように、受信機４６は、それぞれの新たなストリーム３２とその中で非対称的に暗号化された（ＣＫｘ）とに対して、典型的なＲＭライセンス３６を構築するという相当な負担を被る必要がない。なお、ＲＭライセンス３６は、非対称的に署名がなされている。その代わりに、受信機４６は、媒体システム４８を用いて初期化するときに典型的なＲＭライセンス３６を構築することだけを必要とし、その後で、暗号化され対称的に署名された（ＣＫｘ）なしに、それぞれの新たなストリーム３２に対してより負担の少ない導かれたメッセージ６２を構築することができる。

【００８９】

本発明の別の実施例では、（ＣＫ（０））及び（ＩＫ（０））から（ＣＫｘ）及び（ＩＫｘ）を導くのではなくて、（ＣＫｘ）及び（ＩＫｘ）は、それぞれが（ＣＫ（ｘ－１））及び（ＩＫ（ｘ－１））から導かれる。このようにすることは、（ＣＫｘ）及び（ＩＫｘ）を（ＣＫ（０））及び（ＩＫ（０））から導くこととほとんどの点で類似しているが、（ＣＫ（ｘ））及び（ＩＫ（ｘ））が記憶され（ＣＫ（ｘ＋１））及び（ＩＫ（ｘ＋１））を導くために検索する必要がある点は異なっている。

【００９０】

また、受信機４６と媒体システム４８との間でコンテンツ鍵を共有する際に、これらの要素は、例えば認証などの安全な方法を用いて相互に通信することができる。あるいは、状況が保証するのであれば、安全ではない方法を用いることも考えられる。

デフォルトの導かれたメッセージ６２

述べられかつ、または言及したとして、に、の上に、派生したメッセージ新しく調整された項目に対応する６２を構築する際に、ストリーム３２、レシーバー４６は情報４９を見つける、ストリーム３２からの派生したメッセージ６２の必要条件４７に関係のあること、として、ステップ６１１で、そのような必要条件４７を備えたそのような情報４９が既知の間隔および場所のストリーム３２内に周期的に供給されるかもしれない場合。

そのような既知の間隔はそうかもしれない、の命令で、２０秒ごとに一度、あるいはより長い、また、従って、それは非常に多くの場合ありそうである、時間の相当な長さ待つ必

要なしに、レシーバー４６がストリーム３２のそのような情報４９に遭遇しないだろうというその場合。しかしながら、特にレシーバー４６が第２の時間フレーム内のそのような情報４９に基づいた必要条件４７を備えたそのような派生したメッセージ６２を送ると予想される場合、そのような待機は実現可能ではない、程度、ストリーム３２を合わせることを命じられる後。

【００９１】

従って、レシーバー４６がその上に基づいた必要条件４７を構築するために新しく調整されたストリーム３２からの情報４９をそのうちに所有していなければ、本発明の１つの実施例中で、対応する派生したメッセージ６２およびｓｅ［イータ］ｄに同じを置く、適時の方法の派生したメッセージ６２、図７のステップ７１５および７１７では、レシーバー４６がその代りに、構築し送るとともに、デフォルトはメッセージ６２を引き出した。評価されるかもしれないように、そのようなデフォルトはメッセージ６２を引き出した、とても、本来限定的な必要条件４７を含んでいる、のように、例えば、コピー、決してない（ＣＮ）。その後、レシーバー４６が新しく調整されたストリーム３２からの情報４９を所有している事実にいる場合、その後、レシーバー４６は実際の派生したメッセージ６２を構築し送る。ここで評価されるかもしれないように、そのような実際の派生したメッセージ６２は、そのような気が狂った情報４９に基づいた事実にあり、対応するデフォルトを派生したメッセージ６２からの必要条件４７に取って代わるのが目的の必要条件４７を含んでいる。

【００９２】

項目中で、また、新しく命じられたストリーム３２（ステップ８０１）を合わせる際、今、図８に変わって、レシーバー４６は計算をインクリメントし由来する、１つの（ＣＫｘ）そして（ＩＫｘ）ステップ７０９－７１３（ステップ８０３）でのようなストリームのために。しかしながら、適時のやり方で新しく調整されたストリーム３２に必要条件４７に関係する前述の情報４９にまだ遭遇していないと考えて、レシーバー４６はデフォルトを構築し送る、とても、本来限定的なデフォルト必要条件４７を含んでいるメッセージ６２を引き出した、のように、例えば、コピー、決してない（ＣＮ）（ステップ８０５）。その後、そのような待機が続くことができるところで、新しく調整されたストリーム３２からの情報４９が遭遇した（ステップ８０７）事実にあるまで、レシーバー４６は待つ、２０秒どころかある状況での分の方法と同じくらい長い

で、ストリーム３２の情報４９に遭遇する事実では、その後、レシーバー４６は、そのような遭遇した情報４９（ステップ８１５）に基づいた事実にある実需４７を含んでいる実際の派生したメッセージ６２を構築し送る、実際の派生したメッセージ６２のそのような実需４７は、対応するデフォルトからの４７が引き出したデフォルト必要条件を交換するのが目的である、メッセージ６２．著しく、また本発明の１つの実施例中で、ステップ８１５でのような実際の派生したメッセージ６２を構築し送ることにおけるレシーバー４６は、計算（ステップ８１３）をインクリメントしない。したがって、デフォルトはメッセージ６２および対応する実際の派生したメッセージ６２を引き出した、同じ計算を持っている、そこに注意した。

【００９３】

今、デフォルトを受け取ることで評価されるかもしれないとして、メッセージ６２を引き出した、そして、として、の前に、媒体システム４８は対応する内容キー（ＣＫｘ）および保全性キー（ＩＫｘ）を引き出す、として、図７のステップ７２１および７２３で、そのようなデフォルトのシグネチャを確認するそのような保全性キー（ＩＫｘ）を使用する、メッセージ６２を引き出した、として、ステップ７２５で、また内容キーＣＫｘ）で、媒体システム４８はストリーム３２を解読することができる、として、ステップ７２７（ステップ８０９）で。著しく、そのようなデフォルトがメッセージ６２を引き出したので、大部分であるデフォルト必要条件４７を持っている－自然界において限定的、媒体システムはさらにデフォルト・バージョンを構築し格納する、ライセンスで３６を許可する、図６のステップ６１７および６１９では、それがそのようなデフォルト必要条件４７に

基づき、それが重要な尊敬（ステップ８１１）においてその結果、高度に限定的なとともに、６０を格納する。

【００９４】

しかしながら、で、後、実際の派生したメッセージ６２を受け取ること、また、本発明の１つの実施例中の媒体システム４８は、実際の派生したメッセージ６２がデフォルトからの４７が引き出したデフォルト必要条件を交換することである実需４７を含むことを不変の計算価値を意味するものと実際の派生したメッセージ６２がデフォルトの計算価値から変更していないようなものの中の計算価値がメッセージ６２を引き出したことに注目することに特に思う、メッセージ６２（ステップ８１７）．あるいは、媒体システム４８はデフォルトのうちの４７が引き出した必要条件中でコピー・デフォルト・フィールドから注意するかもしれない、そのようなメッセージ６２があるメッセージ６２、自然界における事実デフォルト、そして次に、対応する実際の派生したメッセージ６２を待つ

従って、そのような媒体システム４８はデフォルトに関して引き出されるような保全性キー（ＩＫｘ）が引き出した雇用を行うが、媒体システム４８は対応する内容キー（ＣＫｘ）および図７のステップ７２１および７２３でのような保全性キー（ＩＫｘ）を引き出す必要はない、ステップ７２５でのような実際の派生したメッセージ６２のシグネチャを確認するメッセージ６２、またデフォルトに関して引き出されるような内容キー（ＣＫｘ）を使用する、ストリーム３２を解読し続けるメッセージ６２を引き出した。

ステップ７２７（ステップ８１９）で。著しく、実際の派生したメッセージ６２に本来それ以上限定的になりえない実需４７があるので、媒体システム４８はさらに実際のバージョンを構築し格納する、ライセンスで３６を許可する、図６のステップ６１７および６１９では、それがそのような実需４７に基づき、それが対応するデフォルトを交換することであるとともに、６０を格納する―バージョン、デフォルト必要条件４７（ステップ８２１）に基づいて、３６を許可する。

【００９５】

デフォルト必要条件４７に基づいた、デフォルト・バージョン・ライセンス３６によってストリーム３２が与えることができる時の量については、ユーザーが恐らく複写の性質およびその他同種のもの中のそのようなストリーム３２を備えた何もすることができないことに注意してください。しかしながら、デフォルトがメッセージ６２を引き出した後、対応する実際の派生したメッセージ６２が数分に媒体システム４８によって高々約２０秒受け取られるべきであるので、そして実需４７に基づいて、実際のバージョンが３６を許可するような時に、デフォルト・バージョンを交換するだろう、デフォルト必要条件４７に基づいて、３６を許可する、そのようなストリーム３２が非常に限定的にコントロールされる場合、時間フレームは、些細なことのポイントに比較的小さい。

【００９６】

とにかく、実際の派生したメッセージ６２が提供されるかもしれない実需４７を見つける前に、デフォルトが媒体システム４８へのメッセージ６２を引き出したと規定することによって、レシーバー４６は、少なくともそのような媒体システム４８のユーザーが与えられたストリーム３２を速やかに不適当な量のすぐに経験することができるように、媒体システム４８が迅速なやり方で対応するストリーム３２を与えることを認める。実際の派生したメッセージ６２が媒体システム４８に結局提供される場合、その後、そのような媒体システムは実需４７に基づいた対応する実際のバージョン・ライセンス３６を構築することができ、実損のないデフォルト必要条件４７に基づいたデフォルト・バージョン・ライセンス３６を交換することができる。

一時的なライセンス記憶装置６０

典型的なＲＭアーキテクチャ中で、作成されたライセンス３６、そして１片の内容３２に対応する、内容３２が入手可能な間利用可能であるべきである。したがって、内容３２が例えば１０年間存在すると予想されるドキュメントである場合、対応するライセンス３６はさらに同じ１０年の間ライセンス店６０の中にあるに違いない。相応して、内容３２が例えばまさに短期間の間存在すると予想されるストリーム３２、次に対応するライセン

ス３６のような暫時の信号である場合、さらに同じのためのライセンス店６０の中にあるべきである、理想的にまさに短期間。

【００９７】

したがって、レシーバー４６が多くのストリーム３２を恐らく一度合わせると予想することができる場合、図４のシナリオ中で、すべての２位、程度、媒体システム４８によってライセンス店６０に格納されるような対応するライセンス３６が、使用されて、大部分はかろうじてあることは認識されることになっている、また以前使用された、再び使用することができないこと　さらに、媒体システム４８によってライセンス店６０に格納されたようなライセンス３６のシヤー・ボリュームは、速く巨大な存続期間に接近することができる。そのようなライセンス店６０に非常に多くのライセンス３６を格納することにより、さらに、探索、のために、そして比較的時間の長期に確かに必要とされるわずかのライセンス３６がそうでありうる発見、厄介で、遅い。

【００９８】

本発明の１つの実施例中で、したがって、媒体システム６０によって格納されるように３６を許可する、比較的分離される、短い、ライセンス３６を実践した、そして比較的長い、ライセンス３６を実践した。比較的短くて、そのような具体化中で、さらに、ライセンス３６を実践した、より一時的・より揮発性のライセンスに格納される、媒体システム４８のうちの、および比較的６０を格納する、長い、ライセンス３６を実践した、より永久・より不揮発性のライセンスに格納される、媒体システム４８のうちの６０を格納する。例えば、本発明の趣旨およびスコープから外れずに、他のタイプのそのような記憶は雇われるかもしれないが、永久のライセンス店６０が媒体システム４８の固定ドライブ記憶に位置しているかもしれない一方、一時許可証店６０は媒体システム４８のＲＡＭメモリに位置するかもしれない。

【００９９】

本発明の１つの実施例中で、媒体システム４８配設位置、長命のストリーム３２に相当する永久のライセンス店６０に３６を許可する、ユーザーなど、記憶装置５０に後のために保存されるために指図した、別の媒体システム４８などへのプレイバックあるいは複写。したがって、他のすべてのライセンス３６（それらは推測上略して生きられておりより多くの一時河川３２になるだろう）は、媒体システム４８によって一時許可証店６０に入れられるだろう。永久のライセンス店６０が不揮発性の場合、評価されるかもしれないように、媒体システム４８が切られるかリセットされる場合は常に、ライセンス３６はそこに削除されず、不定の方式で対応する長命のストリーム３２を与えるために従って雇うことができる。もはや必要でなかった時、パーマネント・ライセンスからライセンス３６を削除し削除するべきことは６０を格納するが注意してください。

【０１００】

しかしながら、一時許可証店６０が揮発性の場合、媒体システム４８が切られるかリセットされる場合は常に、ライセンス３６はそこに削除される。

しかしながら、そのような削除は暗にある。また、媒体システム４８が比較的時間（そのような一時許可証蓄積はその間満たされかつ／または妨げられたようになることができる）の長期のために作動する場合、さらに、削除のより明示的な方法が必要であることが認識されることになっている。

【０１０１】

したがって、本発明の１つの実施例では、そのようなライセンス３６がもはや必要ではないとそのような媒体システム４８が思う場合、媒体システム４８は、一定時間で一時許可証店６０のライセンス３６の削除を明示的に命じる。そのような一定時間は本発明の趣旨およびスコープから外れずに、任意の適切な回かもしれない。例えば、それはそうかもしれない、対応するストリーム３２がもはやレシーバー４６によって調整されない場合にライセンス３６を削除する媒体システム４８コマンド、のように、レシーバー４６が媒体システム４８によって別のストリーム３２を合わせることを命じられる場合、例えば。

【０１０２】

しかしながら、そのようなライセンス３６を非常に速く削除する事実中のそれが時期尚早かもしれないことは認識されることになっている。例えば、それは、そのような将来の削除されたライセンス３６での情報がまだ必要か、それに対応するストリーム３２が短期間に再度調整されるかもしれないということかもしれない。同様に、それは、媒体システム４８の１つのプロセスはもはやライセンス３６を要求せず、そのようなライセンス３６の削除を命じたが、別のプロセスがまだ同じを要求するかもしれないというその場合かもしれない。

【０１０３】

本発明の１つの実施例中で、従って、また、今、図９に変わって、一時許可証からライセンス３６を削除したい媒体システム４８のどんなプロセスも、６０を格納する、そうする、ない、によって、同じを削除する事実中で、だがそのようなライセンス３６にフラグなど（ステップ９０１）のような適切なマークで印をつけることによって（その代り）。評価されるかもしれないように、そのようなフラグは、ライセンス３６にそのような使用のために、および適切に取っておかれたビットによって表わされるかもしれない、セットは、一時許可証店６０などによって維持された基準テーブル中の同様のビットかもしれない。したがって、マークされるように、そのようなライセンス３６は直ちに削除されず、同じを要求する媒体システム４８の他のプロセスによって雇うことができる。

【０１０４】

後で、ライセンス３６が実際そうだった後、削除のためにそれではマークされた、そして媒体システムの他のプロセスもそのような印のあるライセンス３６の使用を要求することができた後、推測上よく、事実中の媒体システム４８は、ハウスキーピング・プロセスなど（ステップ９０３）を始動させること経由でそのような印のあるライセンス３６を削除する。項目中で、また、評価されるかもしれないように、一時許可証中で各ライセンス３６を検査するために媒体システム４８のそのようなハウスキーピング・プロセスを周期的にそのために始動するだろう、６０（ステップ９０５）を格納する、ライセンス３６が削除（ステップ９０７）のためにマークされた事実にある場合、およびそのように事実中で場合、決定する、一時許可証からそのような印のあるライセンス３６を削除する、６０（ステップ９０９）を格納する。

【０１０５】

本発明で、それでは、比較的時間の長期に必要とされないライセンス３６は本来揮発性の一時許可証店６０に格納されることにより、他のライセンス３６から分離される。さらに、一時許可証店６０があまりにも多くのそのようなライセンス３６で充満するようになるのを防ぐように、もはや必要でなかった時、そのようなライセンス３６は削除のためにマークされる。また、ハウスキーピング・プロセスは周期的に実際一時許可証店６０からそのような印のあるライセンス３６を削除する。

結論

本発明に関して行なわれたプロセスを有効にするのに必要なプログラミングは、比較的真直ぐで、適切なプログラムする公に明白であるべきである。従って、そのようなプログラミングはここに付けられない。どんな特別のプログラミングもそれでは、それの精神およびスコープから外れずに、本発明を有効にするために雇われるかもしれない。

【０１０６】

本発明では、システムと方法は、そのようなレシーバー４６が新しくストリーム３２を合わせるごとに完全にそのような新しいライセンス３６を作成する事実中でレシーバー４６が間接費に行く必要はないようにライセンス３６を構築するために雇われることになっている必要条件４７の短縮版を作成するレシーバー４６のために提供される。ユーザーが変更が見えていても、レシーバー４６が新しくストリーム３２を合わせるごとに、そのような必要条件４７の短縮版は速く作成し、媒体システム４８に送ることができる、の命令で、一度、すべての２位、程度。さらに、そのような必要条件４７の短縮版は簡潔で、にもかかわらず、スペースの必要最低限量に調整されたストリーム３２用のライセンス必要条件についてすべて記述する。そのような必要条件４７のフォーマットはレシーバー４６

以外のソースからの媒体システム４８に提供されるようなストリーム３２に関して雇うことができる。

【０１０７】

さらに、本発明では、システムと方法は、個々のそのような内容キー（ＣＫ）で実際のライセンス３６を作成する必要なしにレシーバー４６と媒体システム４８の間で個々の新しい内容キー（ＣＫ）を共有するためにそこに提供される。レシーバー４６および媒体システム４８は最初の内容キー（ＣＫＯ）を交換し、次に、統合方法で最初の内容キー（ＣＫＯ）に基づいた内容キー（ＣＫｘ）を回転させる。

【０１０８】

さらに、本発明では、実際に位置した時、システムと方法は、予備方式で必要条件のデフォルト・セットに４７を送るレシーバー４６そして次に必要条件４７の実際のセットのために提供される。実需４７が送られるまで、そのようなデフォルト必要条件４７は媒体システム４８によって雇われる。また、媒体システム４８は、そのようなデフォルト必要条件４７とそのような対応する実需４７の間に基本的相違を示すことができ、デフォルト必要条件４７をそれの受信上の対応する実需４７に取り替えることができる。

【０１０９】

最後に、本発明では、一時的方式上にのみ調整されたストリーム３２に対応するいくつかのライセンス３６を少なくとも格納するために、システムと方法は、媒体システム４８に提供される。媒体システム４８は認識することができる、ライセンス３６はそれを必要とする、一時的基礎および媒体システム上に単に格納される、もはや必要でなかった時そのような一時的に格納されたライセンスを削除する。

【０１１０】

それについて発明概念から外れずに、上に記述された具体化に変更を行なうことができるかもしれないことは認識されるべきである。したがって、この発明が示された特別の具体化に制限されていないことは理解されるに違いない。しかし、それは、アペンドされたクレームによって定義されるような本発明の趣旨およびスコープ内の変更をカバーするように意図される。

【図面の簡単な説明】

【０１１１】

上述した発明の概要及び本発明の実施例に関する詳細な説明は、以下で簡単に説明する添付の図面を参照することによって、よりよく理解できる。本発明を図解するため、図面には好適実施例が示されている。しかし、本発明は、示されている実施例には限定されない。

【図１】本発明が実現される例示的であって限定を意味しないコーティング環境を示すブロック図である。

【図２】本発明が実現される、様々な計算機を有する例示的なネットワーク環境を示すブロック図である。

【図３】本発明の様々な実施例による、対応するデジタル・コンテンツをレンダリングするためのデジタル・ライセンスを含む信頼ベースのシステムの一例の実行アーキテクチャを示すブロック図である。

【図４】図３の信頼ベースの一例を示すブロック図であり、特に、本発明の様々な実施例により、コンテンツの暗号化されたストリームをレンダリングするために媒体システムに送る受信機を示すブロック図である。

【図５】本発明の実施例により、図４の暗号化されたコンテンツと関係し、図４の受信機によって図４の媒体システムに送られる必要条件の簡略化されたバージョンを示すブロック図である。

【図６】図６から図９までは、本発明の様々な実施例により図４の受信機と媒体システムとによって実行されるキー・ステップを示す流れ図である。特に、図６は、受信機が図５の必要条件を媒体システムに送る態様を示している。

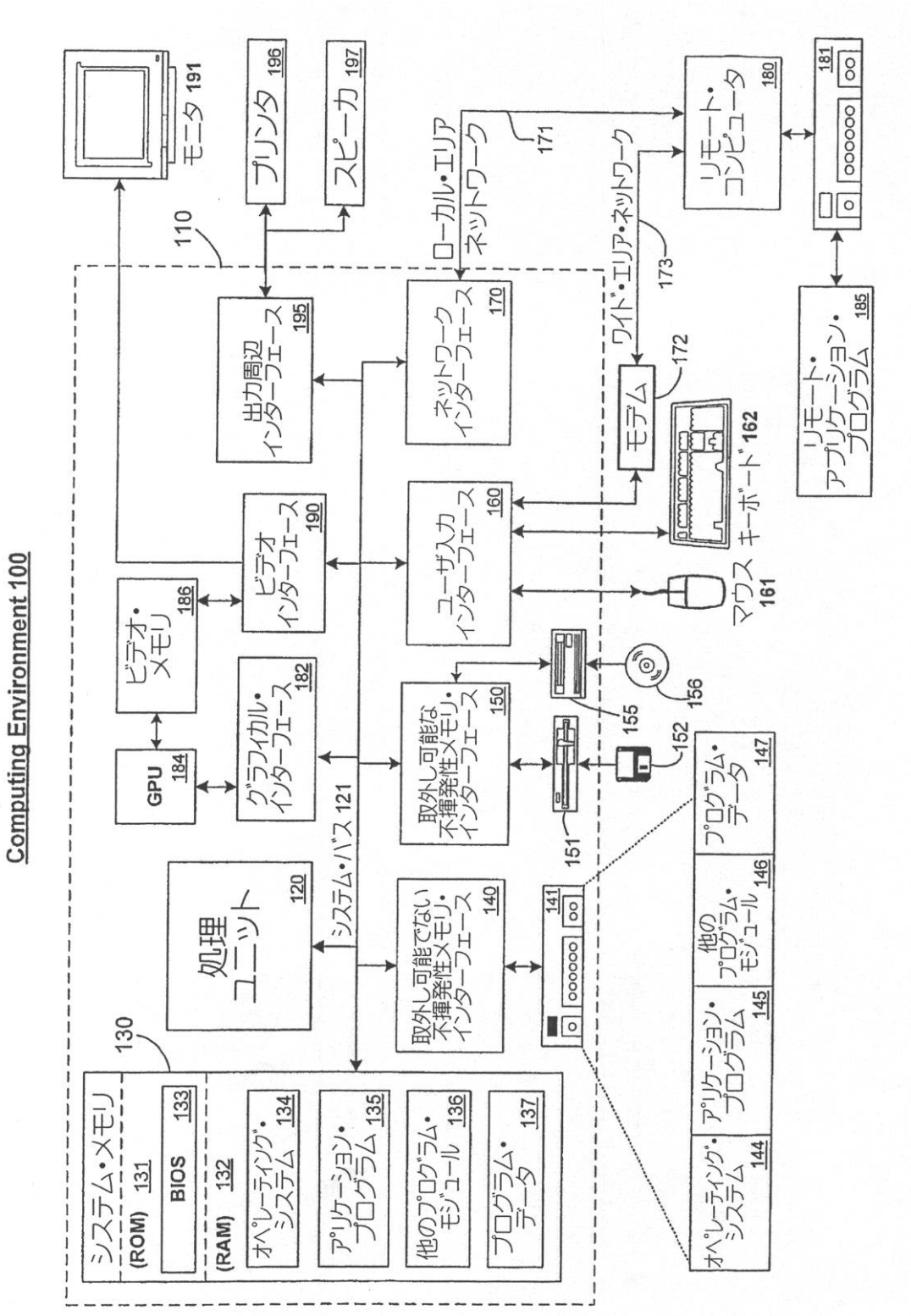
【図７】図６から図９までは、本発明の様々な実施例により図４の受信機と媒体システム

とによって実行されるキー・ステップを示す流れ図である。特に、図７は、受信機と媒体システムとが、それぞれ、新たな調整（チューニング）されるストリームのためのコンテンツ鍵（ＣＫ）を導く様子を示している。

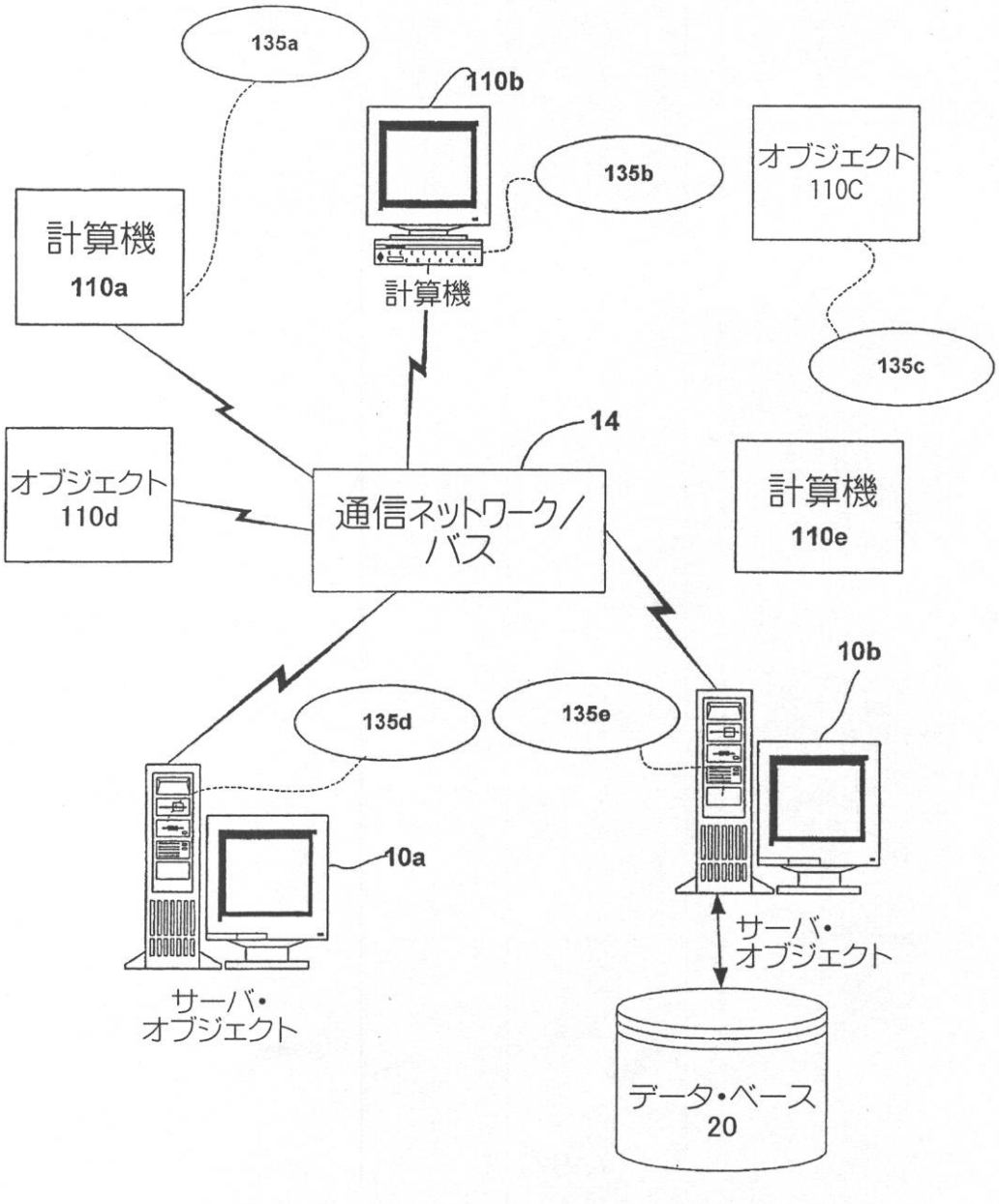
【図８】図６から図９までは、本発明の様々な実施例により図４の受信機と媒体システムとによって実行されるキー・ステップを示す流れ図である。特に、図８は、受信機が、実際の条件をそこから構築することができるストリームにおいて条件と遭遇する前に、新たにチューニングされるストリームのためにデフォルトの条件を有するデフォルトの導かれたメッセージを媒体システムに送る様子が示されている。

【図９】図６から図９までは、本発明の様々な実施例により図４の受信機と媒体システムとによって実行されるキー・ステップを示す流れ図である。特に、図９は、媒体システムが、一時的なライセンス記憶装置を用いて、ハウスキーピング機能を用いて、マークの付けられたライセンスをそこから削除する様子が示されている。

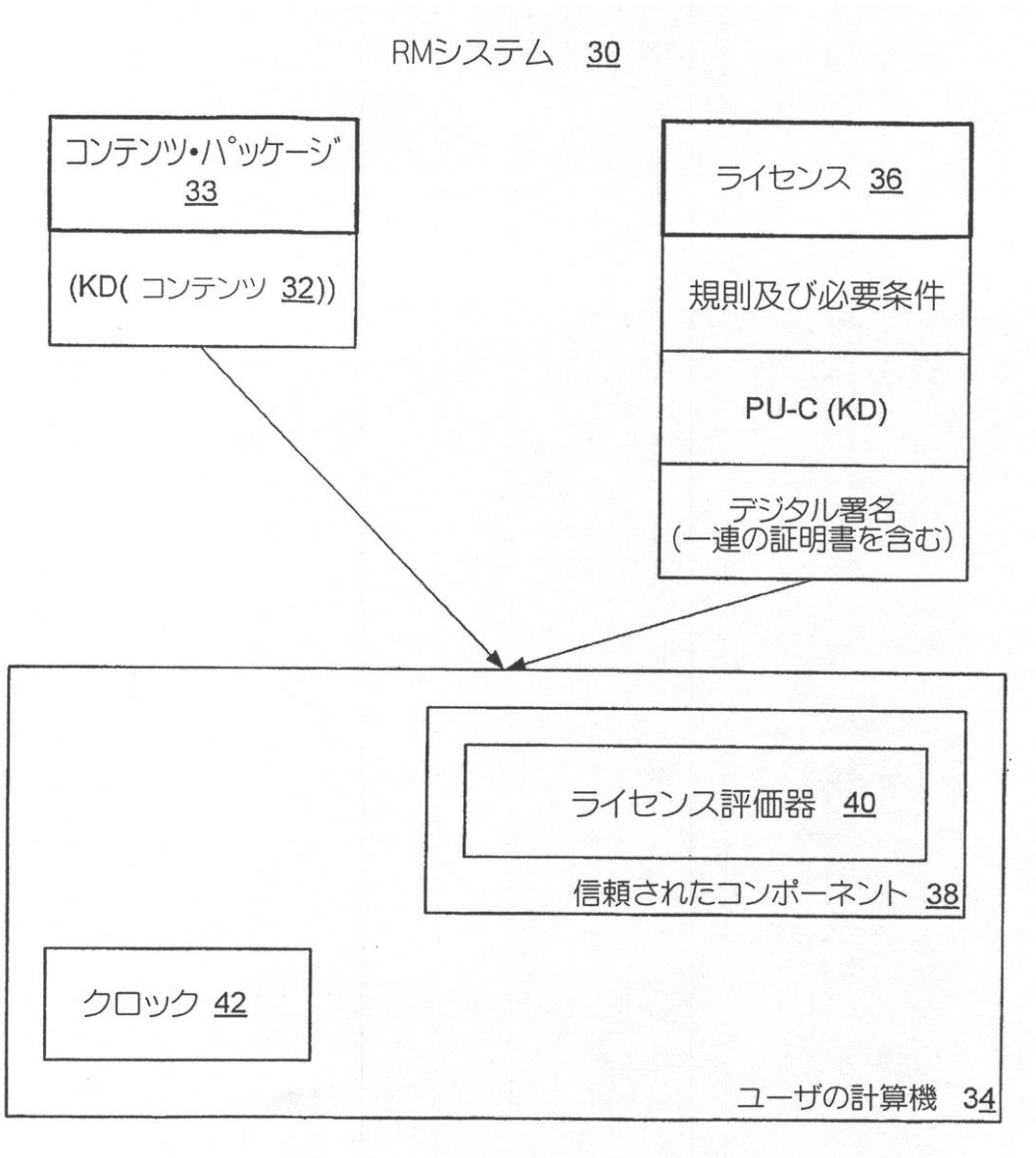
【図１】


Computing Environment 100
110
モニタ 191
プリンタ 196
スピーカ 197
出力周辺インターフェース 195
ローカル・エリア・ネットワーク 171
ネットワークインターフェース 170
ワイド・エリア・ネットワーク 173
リモート・コンピュータ 180
181
リモート・アプリケーション・プログラム 185
モデム 172
ビデオ・メモリ 186
ビデオインターフェース 190
ユーザ入力インターフェース 160
キーボード 162
マウス 161
GPU 184
グラフィカル・インターフェース 182
取外し可能な不揮発性メモリ・インターフェース 150
システム・バス 121
処理ユニット 120
取外し可能でない不揮発性メモリ・インターフェース 140
151
155
156
152
141
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
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
プログラム・データ 147

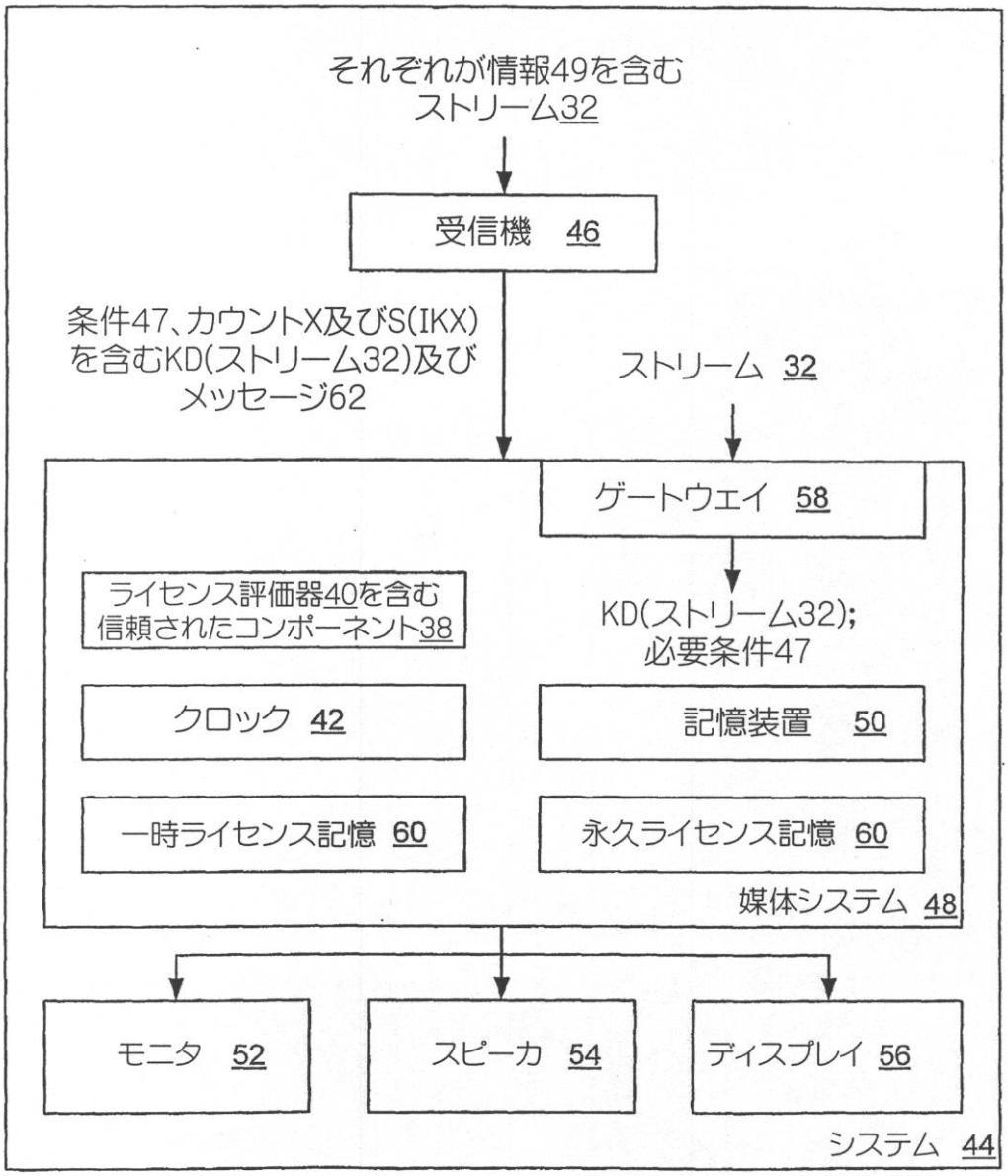
【図２】


135a
110b
135b
オブジェクト
110C
計算機
110a
計算機
135c
14
オブジェクト
110d
通信ネットワーク／
バス
計算機
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

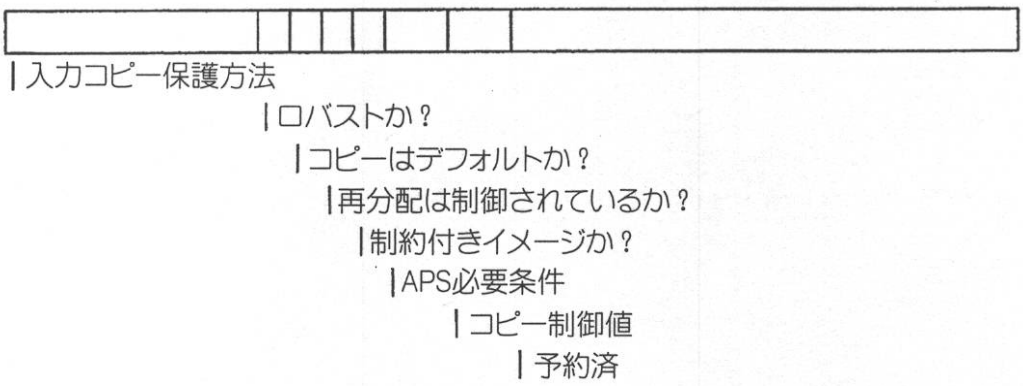
【図３】


RMシステム 30
コンテンツ・パッケージ 33
(KD( コンテンツ 32))
ライセンス 36
規則及び必要条件
PU-C (KD)
デジタル署名
(一連の証明書を含む)
ライセンス評価器 40
信頼されたコンポーネント 38
クロック 42
ユーザの計算機 34

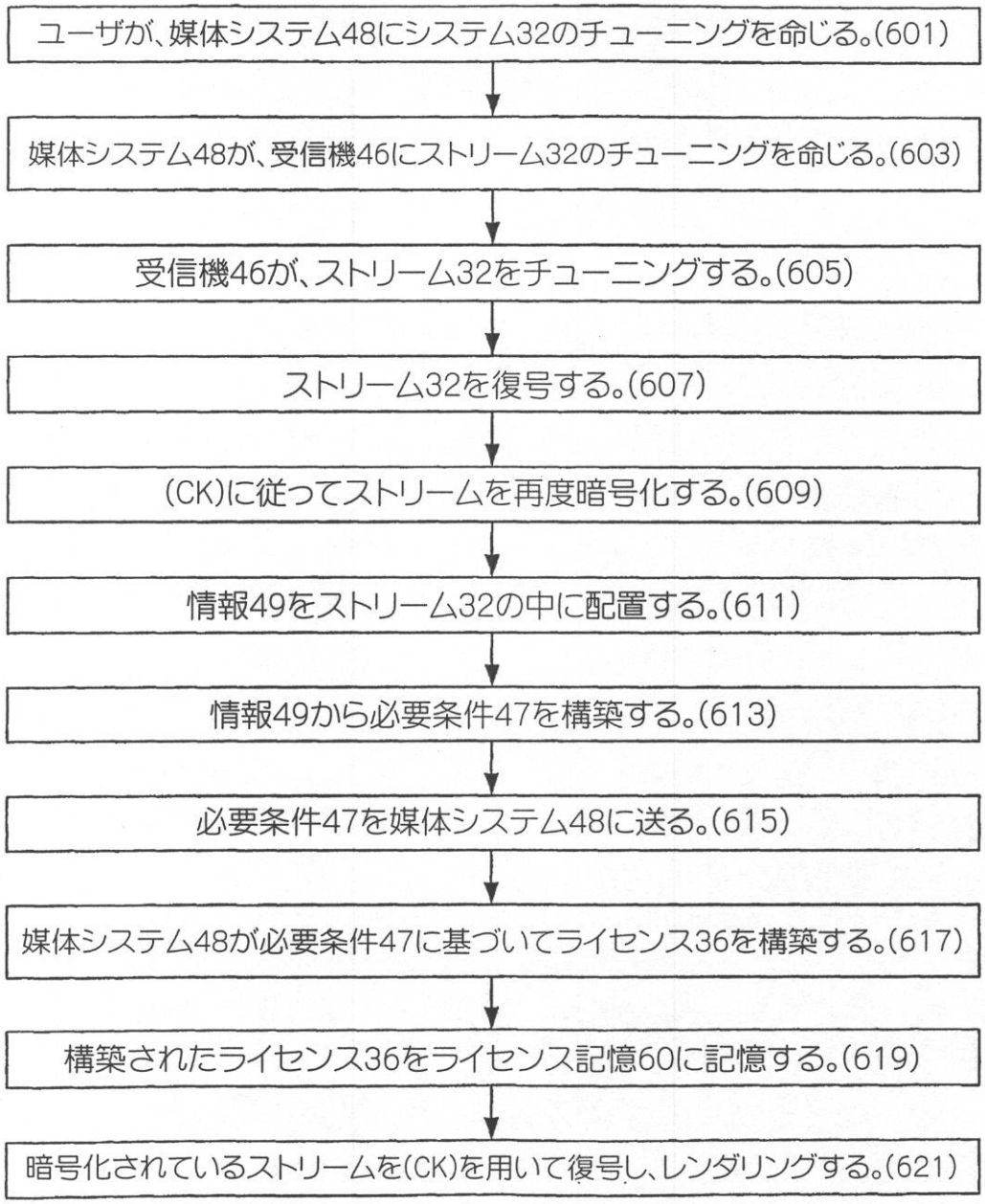
【図４】


それぞれが情報49を含む
ストリーム32
受信機 46
条件47、カウントX及びS(IKX)
を含むKD(ストリーム32)及び
メッセージ62
ストリーム 32
ゲートウェイ 58
ライセンス評価器40を含む
信頼されたコンポーネント38
KD(ストリーム32);
必要条件47
クロック 42
記憶装置 50
一時ライセンス記憶 60
永久ライセンス記憶 60
媒体システム 48
モニタ 52
スピーカ 54
ディスプレイ 56
システム 44

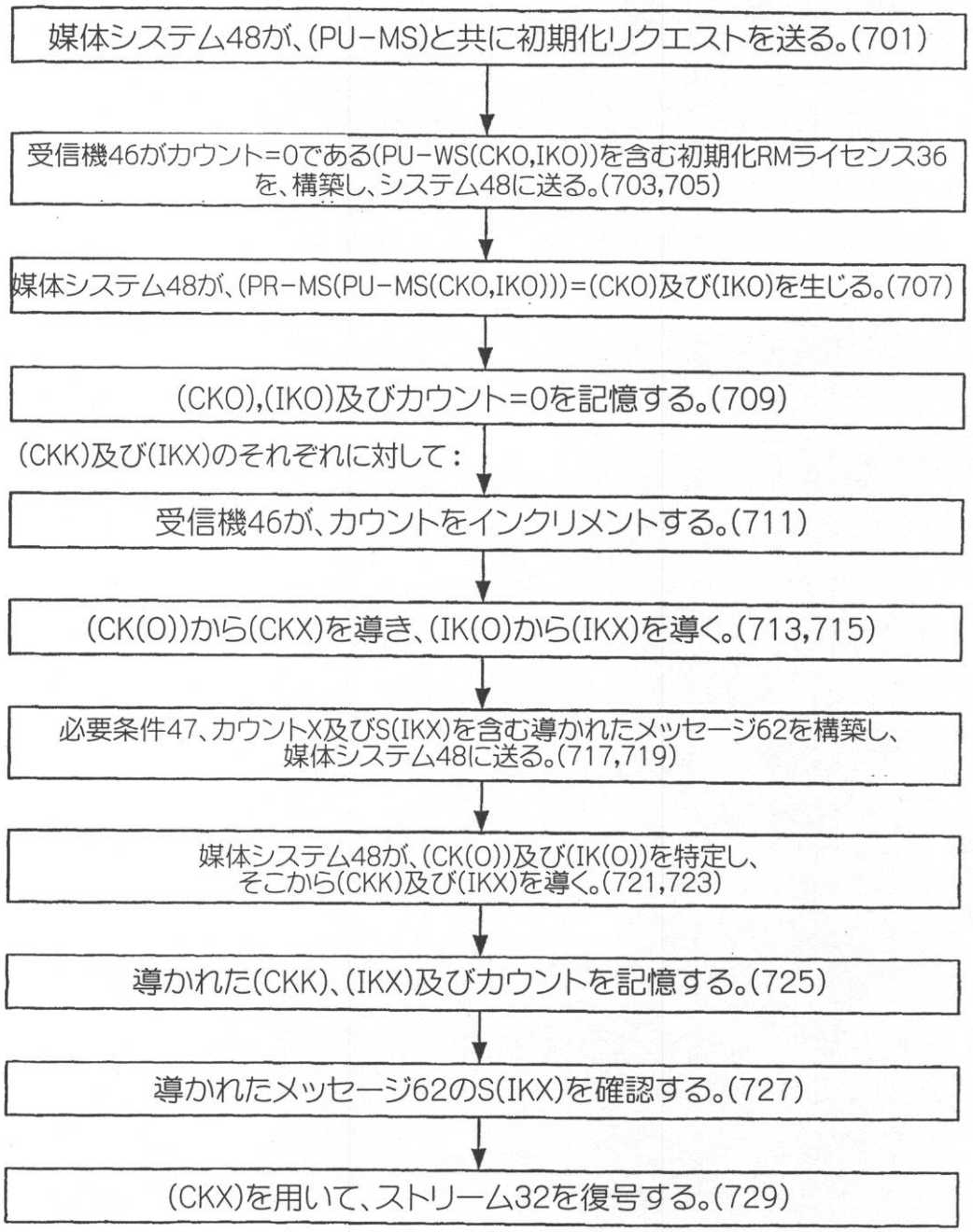
【図５】


入力コピー保護方法
ロバストか？
コピーはデフォルトか？
再分配は制御されているか？
制約付きイメージか？
APS必要条件
コピー制御値
予約済

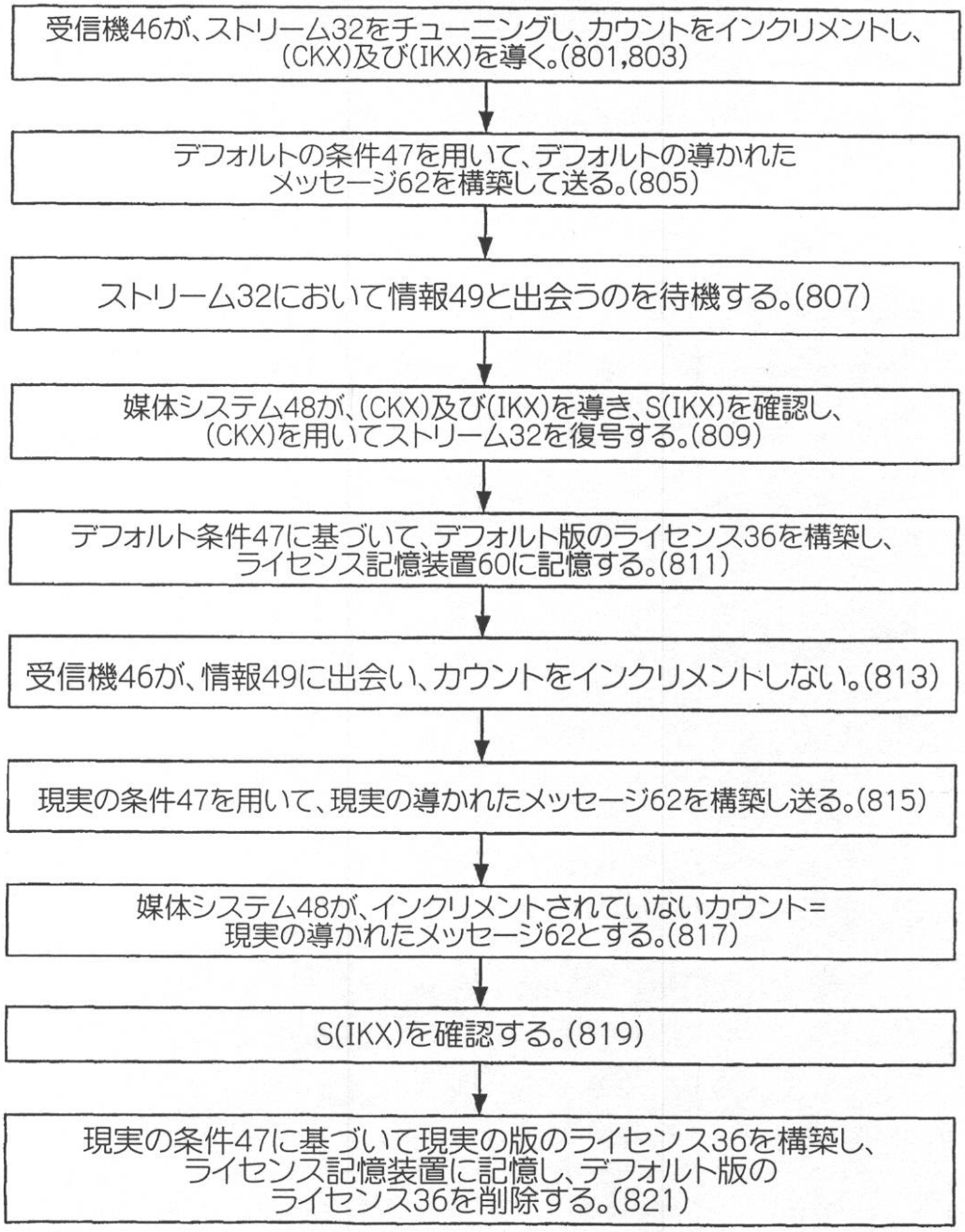
【図６】


ユーザが、媒体システム48にシステム32のチューニングを命じる。(601)
媒体システム48が、受信機46にストリーム32のチューニングを命じる。(603)
受信機46が、ストリーム32をチューニングする。(605)
ストリーム32を復号する。(607)
(CK)に従ってストリームを再度暗号化する。(609)
情報49をストリーム32の中に配置する。(611)
情報49から必要条件47を構築する。(613)
必要条件47を媒体システム48に送る。(615)
媒体システム48が必要条件47に基づいてライセンス36を構築する。(617)
構築されたライセンス36をライセンス記憶60に記憶する。(619)
暗号化されているストリームを(CK)を用いて復号し、レンダリングする。(621)

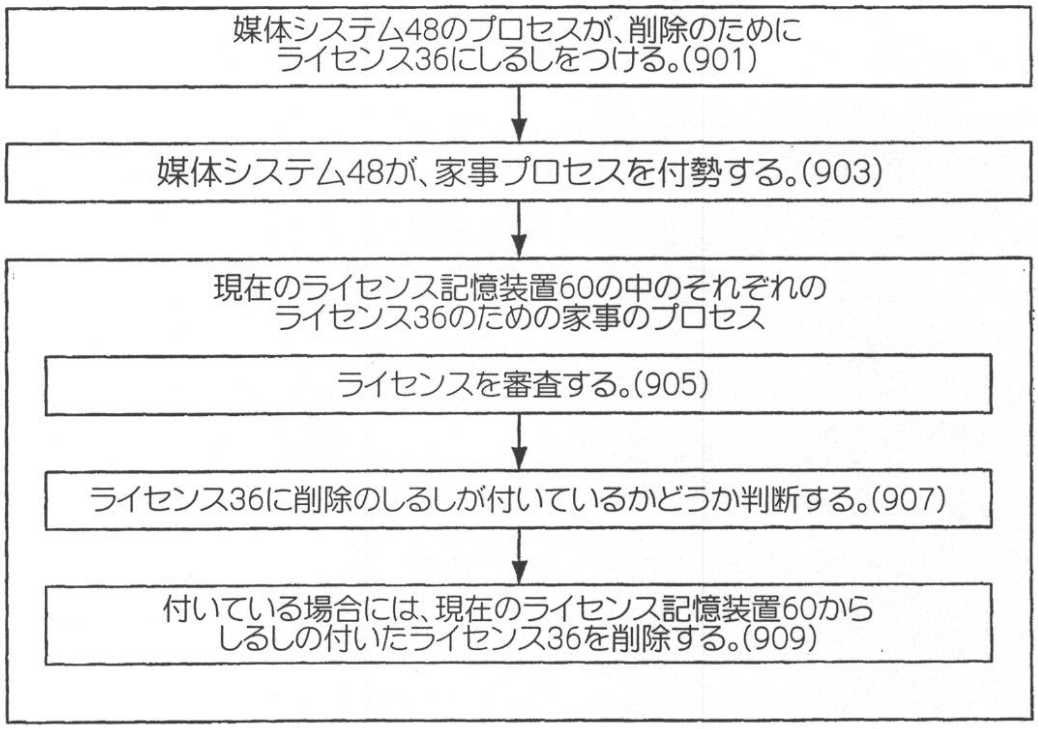
【図７】


媒体システム48が、(PU−MS)と共に初期化リクエストを送る。(701)
受信機46がカウント=0である(PU−WS(CKO,IKO))を含む初期化RMライセンス36を、構築し、システム48に送る。(703,705)
媒体システム48が、(PR−MS(PU−MS(CKO,IKO)))=(CKO)及び(IKO)を生じる。(707)
(CKO),(IKO)及びカウント=0を記憶する。(709)
(CKK)及び(IKX)のそれぞれに対して：
受信機46が、カウントをインクリメントする。(711)
(CK(O))から(CKX)を導き、(IK(O)から(IKX)を導く。(713,715)
必要条件47、カウントX及びS(IKX)を含む導かれたメッセージ62を構築し、媒体システム48に送る。(717,719)
媒体システム48が、(CK(O))及び(IK(O))を特定し、そこから(CKK)及び(IKX)を導く。(721,723)
導かれた(CKK)、(IKX)及びカウントを記憶する。(725)
導かれたメッセージ62のS(IKX)を確認する。(727)
(CKX)を用いて、ストリーム32を復号する。(729)

【図８】


受信機46が、ストリーム32をチューニングし、カウントをインクリメントし、(CKX)及び(IKX)を導く。(801,803)
デフォルトの条件47を用いて、デフォルトの導かれたメッセージ62を構築して送る。(805)
ストリーム32において情報49と出会うのを待機する。(807)
媒体システム48が、(CKX)及び(IKX)を導き、S(IKX)を確認し、(CKX)を用いてストリーム32を復号する。(809)
デフォルト条件47に基づいて、デフォルト版のライセンス36を構築し、ライセンス記憶装置60に記憶する。(811)
受信機46が、情報49に出会い、カウントをインクリメントしない。(813)
現実の条件47を用いて、現実の導かれたメッセージ62を構築し送る。(815)
媒体システム48が、インクリメントされていないカウント=現実の導かれたメッセージ62とする。(817)
S(IKX)を確認する。(819)
現実の条件47に基づいて現実の版のライセンス36を構築し、ライセンス記憶装置に記憶し、デフォルト版のライセンス36を削除する。(821)

【図９】


媒体システム48のプロセスが、削除のために
ライセンス36にしるしをつける。(901)
媒体システム48が、家事プロセスを付勢する。(903)
現在のライセンス記憶装置60の中のそれぞれの
ライセンス36のための家事のプロセス
ライセンスを審査する。(905)
ライセンス36に削除のしるしが付いているかどうか判断する。(907)
付いている場合には、現在のライセンス記憶装置60から
しるしの付いたライセンス36を削除する。(909)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100096068
弁理士 大塚 住江
(72)発明者 エバンス, ブライアン・ピー
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
(72)発明者 ストロム, クリフォード・ピー
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
(72)発明者 ローゼンステイン, ダニエル
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
(72)発明者 パカ, アナンド・ディー
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

Ｆターム(参考) 5B017 AA03 AA07 BA07 CA16
5B285 AA02 BA09
5J104 AA16 AA32 EA01 EA04 EA15 EA16 JA03 MA05 NA02 NA27
NA37 PA14