(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-62890
(P2004-62890A)
(43)公開日　平成16年2月26日(2004.2.26)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	320A	5B017
G06F 17/60	G06F 12/14	310K	5J104
G09C 1/00	G06F 17/60	142	
	G09C 1/00	640E	

審査請求 未請求　請求項の数 28　ＯＬ　（全 44 頁）

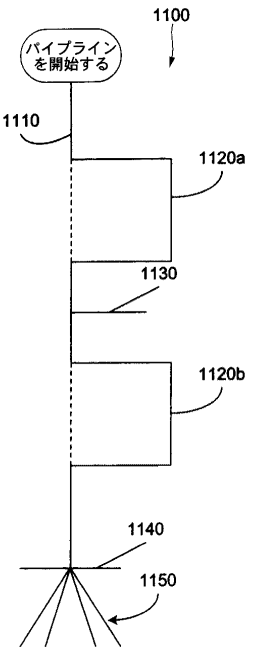
(21)出願番号　特願2003-188926(P2003-188926)
(22)出願日　平成15年6月30日(2003.6.30)
(31)優先権主張番号　10/185,906
(32)優先日　平成14年6月28日(2002.6.28)
(33)優先権主張国　米国(US)

(71)出願人　391055933
マイクロソフト　コーポレイション
ＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮ
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　（番地なし）
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　スコット　シー．コットリル
アメリカ合衆国　９８０７４　ワシントン州　サマミッシュ　ノースイースト　１４　ドライブ　２２６１８

最終頁に続く

(54)【発明の名称】デジタル権利管理サービスを提供するシステムおよび方法

(57)【要約】
【課題】サービス提供プログラム全体を変更せずに、デジタル権利管理サービスの提供範囲内の選択したタスクだけをモジュラ式に変更することができるシステムおよび方法を提供する。
【解決手段】このシステムは、権利管理デジタルコンテンツを発行し、またはライセンス交付するデジタル権利管理サービスを実行する処理フレームワークを提供するサービスプログラムを含む。デジタル権利管理サービスに関連するタスクをそれぞれ実行する複数のプラグインコンポーネントが提供される。プラグインコンポーネントは、事前定義された１組のインターフェース規則に従って、処理フレームワークに統合される。
【選択図】　図１１



【特許請求の範囲】
【請求項１】
デジタル権利管理サービスを提供するシステムであって、
デジタル権利管理サービスを実行する処理フレームワークを提供するサービスプログラムと、
前記デジタル権利管理サービスに関連するタスクをそれぞれ実行する複数のプラグインコンポーネントとを備え、
前記複数のプラグインコンポーネントはそれぞれ、事前定義されたそれぞれの１組のインターフェース規則に従って前記処理フレームワークに統合されることを特徴とするシステム。
【請求項２】
前記デジタル権利管理サービスは、発行要求を処理して権利管理デジタルコンテンツを発行することを含むことを特徴とする請求項１に記載のシステム。
【請求項３】
前記複数のプラグインコンポーネントは、権利記述、暗号化コンテンツ鍵、ならびに前記権利記述と前記暗号化コンテンツ鍵の両方に関するデジタルシグニチャを含む権利ラベルを格納するプラグインコンポーネントを含むことを特徴とする請求項２に記載のシステム。
【請求項４】
前記複数のプラグインコンポーネントは、前記権利管理デジタルコンテンツを暗号化および暗号解読することに関連して使用される秘密鍵を保護するプラグインコンポーネントを含むことを特徴とする請求項２に記載のシステム。
【請求項５】
前記複数のプラグインコンポーネントは、証明書を生成するプラグインコンポーネントを含むことを特徴とする請求項２に記載のシステム。
【請求項６】
前記複数のプラグインコンポーネントは、前記発行要求をサブミットするエンティティを認証するプラグインコンポーネントを含むことを特徴とする請求項２に記載のシステム。
【請求項７】
前記複数のプラグインコンポーネントは、前記発行要求をサブミットするエンティティが前記要求に従って前記権利管理デジタルコンテンツを発行することを許可されているかどうかを判定するプラグインコンポーネントを含むことを特徴とする請求項２に記載のシステム。
【請求項８】
前記デジタル権利管理サービスは、権利管理デジタルコンテンツをライセンス交付するライセンス要求を処理することを含むことを特徴とする請求項１に記載のシステム。
【請求項９】
前記複数のプラグインコンポーネントは、前記ライセンス要求で提供されるグループ識別子に基づいてユーザリストを取り出すグループ拡張プラグインコンポーネントを含むことを特徴とする請求項８に記載のシステム。
【請求項１０】
前記複数のプラグインコンポーネントは、権利記述、暗号化コンテンツ鍵、ならびに前記権利記述および前記暗号化コンテンツ鍵の両方に関するデジタルシグニチャを含む権利ラベルを取り出すプラグインコンポーネントを含むことを特徴とする請求項８に記載のシステム。
【請求項１１】
前記複数のプラグインコンポーネントは、証明書を取り出すプラグインコンポーネントを含むことを特徴とする請求項８に記載のシステム。
【請求項１２】
前記複数のプラグインコンポーネントは、前記ライセンス要求をサブミットするエンティ

ティを認証するプラグインコンポーネントを含むことを特徴とする請求項８に記載のシステム。
【請求項１３】
前記複数のプラグインコンポーネントは、前記ライセンス要求をサブミットするエンティティが前記要求に従って前記権利管理デジタルコンテンツを使用することを許可されているかどうかを判定するプラグインコンポーネントを含むことを特徴とする請求項８に記載のシステム。
【請求項１４】
前記複数のプラグインコンポーネントは、規定のイベントの発生に基づいてそれぞれのタスクを実行する少なくとも１つのエクステンションプラグインコンポーネントを含むことを特徴とする請求項１に記載のシステム。
【請求項１５】
前記エクステンションプラグインコンポーネントは、前記サービスプログラムの処理を停止するように適合されることを特徴とする請求項１４に記載のシステム。
【請求項１６】
前記複数のプラグインコンポーネントは、少なくとも１つの非同期コンポーネントを含むことを特徴とする請求項１に記載のシステム。
【請求項１７】
前記デジタル権利管理サービスは登録サービスを含むことを特徴とする請求項１に記載のシステム。
【請求項１８】
前記デジタル権利管理サービスは活動化サービスを含むことを特徴とする請求項１に記載のシステム。
【請求項１９】
前記デジタル権利管理サービスは認証サービスを含むことを特徴とする請求項１に記載のシステム。
【請求項２０】
前記デジタル権利管理サービスはフェデレーションサービスを含むことを特徴とする請求項１に記載のシステム。
【請求項２１】
デジタル権利管理サービスを提供する方法であって、
デジタル権利管理サービスを実行する処理フレームワークを提供するサービスプログラムを提供するステップと、
前記デジタル権利管理サービスにそれぞれ関連するタスクを実行するプラグインコンポーネントにそれぞれ関連する、複数のデジタル権利管理プラグインオプションを提供するステップと、
選択したプラグインコンポーネントを前記処理フレームワークに統合するステップであって、前記選択したプラグインコンポーネントは、前記複数のプラグインオプションから選択したプラグインオプションに対応するステップとを備えることを特徴とする方法。
【請求項２２】
前記選択したプラグインコンポーネントに対応するプラグイン選択を受け取るステップをさらに備えることを特徴とする請求項２１に記載の方法。
【請求項２３】
前記所望のプラグインコンポーネントは、事前定義された１組のインターフェース規則に従って前記処理フレームワークに統合されることを特徴とする請求項２１に記載の方法。
【請求項２４】
前記サービスプログラムは、ライセンス交付サービスを実行する処理フレームワークを提供することを特徴とする請求項２１に記載の方法。
【請求項２５】
前記サービスプログラムは、発行サービスを実行する処理フレームワークを提供すること

を特徴とする請求項２１に記載の方法。
【請求項２６】
複数のデジタル権利管理サービスを実行するコンピュータ実行可能命令が格納されたコンピュータ可読媒体を含むデジタル権利管理サーバであって、前記複数のデジタル権利管理サービスは、それぞれのパイプラインで実行され、前記それぞれのパイプラインは互いに独立であるデジタル権利管理サーバを備えることを特徴とするデジタル権利管理システム。
【請求項２７】
前記パイプラインはそれぞれ、
前記関連するデジタル権利管理サービスを実行する処理フレームワークを提供するサービスプログラムと、
前記デジタル権利管理サービスに関連するそれぞれのタスクを実行する複数のプラグインコンポーネントとを含むことを特徴とする請求項２６に記載のデジタル権利管理システム。
【請求項２８】
前記複数のプラグインコンポーネントはそれぞれ、事前定義されたそれぞれの１組のインターフェース規則に従って前記処理フレームワークに統合されることを特徴とする請求項２７に記載のデジタル権利管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はデジタル権利管理システムに関する。より詳細には、本発明は、デジタル権利管理システムにおけるパイプライン用のプラグインアーキテクチャに関する。
【０００２】
【従来の技術】
デジタル権利の管理およびエンフォースメントは、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などのデジタルコンテンツに関連して、１人または複数のユーザにそのようなデジタルコンテンツを配布すべき場合に非常に望ましい。典型的な配布方法には、磁気（フロッピー（登録商標））ディスク、磁気テープ、光（コンパクト）ディスク（ＣＤ）などの有形の装置、電子掲示板、電子ネットワーク、インターネットなどの無形の媒体が含まれる。ユーザが受け取ったとき、そのようなユーザは、パーソナルコンピュータ上のメディアプレーヤなどの適切なレンダリング装置を用いてデジタルコンテンツをレンダリングし、または再生する。
【０００３】
あるシナリオでは、作者、発行者（ｐｕｂｌｉｓｈｅｒ）、放送者などのコンテンツ所有者または権利所有者は、ライセンス料または他の何らかの対価と引換えに、そのようなデジタルコンテンツを多数のユーザまたは受信者のそれぞれに配布することを望む。このようなシナリオでは、コンテンツは曲、曲のアルバム、映画などである可能性があり、配布の目的はライセンス料を生み出すことである。このようなコンテンツ所有者は、選択肢が与えられた場合、ユーザがそのような配布されたデジタルコンテンツを用いて行えることを制限したいと望むことがあり得る。例えば、コンテンツ所有者は、少なくともコンテンツ所有者に第２のユーザからのライセンス料を与えない仕方でユーザがこのようなコンテンツをこのような第２のユーザにコピーおよび再配布するのを制限することを望む。
【０００４】
加えて、コンテンツ所有者は、様々なタイプの使用ライセンスを異なるライセンス料で購入する柔軟性をユーザに提供すると同時に、どのようなタイプのライセンスが実際に購入されたとしてもそのタイプの条件にユーザを保つことを望むことがある。例えば、コンテンツ所有者は、配布するデジタルコンテンツを限られた回数だけ再生すること、ある合計時間の間だけ再生すること、あるタイプのマシン上でのみ再生すること、あるタイプのメディアプレーヤ上でのみ再生すること、あるタイプのユーザだけが再生することなどを許

可したいと望むことがある。
【０００５】
別のシナリオでは、組織内の従業員などのコンテンツ開発者が、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、または組織外の他の人々に配布したいと望むが、その他の人にコンテンツをレンダリングさせたくない。この場合、コンテンツの配布は、ライセンス料または他の何らかの対価と引き換える広範囲の配布ではなく、秘密裏に、または限定的に組織ベースのコンテンツを共用することに近い。このようなシナリオでは、コンテンツは、オフィス環境内で交換することができるような、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、Ｅメールなどでよく、コンテンツ開発者は、コンテンツがオフィス環境内にとどまり、かつ例えば対抗者または敵対者などの許可されていない人々によってレンダリングされないことが保証されることを望むことがある。やはり、このようなコンテンツ開発者は、受信者が配布されるそのようなデジタルコンテンツを用いて行えることを制限したいと望む。例えば、コンテンツ所有者は、コンテンツをレンダリングすることを許可すべき人々の範囲外にコンテンツを公開する仕方でユーザがそのようなコンテンツを第２のユーザにコピーし、再配布することを制限したいと望む。
【０００６】
加えて、コンテンツ開発者は、様々な受信者に様々なレベルのレンダリング権利を与えることを望むことがある。例えば、コンテンツ開発者は、あるクラスの人に関しては保護されたデジタルコンテンツを閲覧可能にすることを許可するが、印刷可能にすることを許可せず、別のクラスの個人に関しては閲覧可能かつ印刷可能にすることを許可したいと望むことがある。
【０００７】
しかしいずれのシナリオでも、配布を行った後は、このようなコンテンツ所有者／開発者は、デジタルコンテンツに対する規制手段があるとしてもそれをほとんど有さない。実質上あらゆるパーソナルコンピュータが、そのようなデジタルコンテンツの厳密なデジタルコピーを作成し、そのような厳密なデジタルコピーを書込み可能な磁気ディスクや光ディスクにダウンロードし、またはインターネットなどのネットワークを介してそのような厳密なデジタルコピーを任意の宛先に送信するのに必要なソフトウェアおよびハードウェアを含むことを考えると、このことは特に問題である。
【０００８】
もちろん、コンテンツ所有者／開発者は、コンテンツを配布するトランザクションの一部として、デジタルコンテンツのユーザ／受信側に、歓迎され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ように誓約するよう要求することができる。しかし、そのような誓約は容易に作成され、容易に破られる。コンテンツ所有者／開発者は、暗号化と暗号解読を伴ういくつかの周知のセキュリティ装置のいずれかによってそのような再配布を防止しようと試みることがある。しかし、そのことによって、出来心のユーザが暗号化デジタルコンテンツを暗号解読し、そのようなデジタルコンテンツを非暗号化形式で保存し、次いでそれを再配布することが防止される可能性はほとんどない。
【０００９】
【発明が解決しようとする課題】
多くの理由により、ＤＲＭサーバ技術は動的である。すなわち、経時的に技術が発展し、またはデジタルコンテンツのセキュリティに対する新しい脅威が現れるにつれて、あるタスクを実行して特定のサービスを提供するために様々な手法が使用される傾向がある。しばしば、特定のＤＲＭサービスの提供は、タスクを分離する数の性能と関係する。しかし時として、プロバイダは１つまたはいくつかのタスクだけを異なる方式で実行したいと望むことがある。プロバイダとユーザは通常、システムが全体として中断することを可能な限り少なくすることを望む。加えて、コストやその他の制約により、そのようなＤＲＭサーバの異なるユーザは、異なる方式で実行されるシステムを望み、または必要とする。したがって、サービス提供プログラム全体を変更せずに、デジタル権利管理サービスの提供

範囲内の選択したタスクだけをモジュラ式に変更することができるシステムおよび方法が利用可能であるならば有利である。

【００１０】

さらに、典型的なＤＲＭインストールは、発行、ライセンス交付、フェデレーションサービス、登録サービスなどのいくつかのデジタル権利管理サービスを提供することができるので、インストールのプロバイダ／アドミニストレータが可能な限り効率的にシステムを維持することを可能にするようにこれらのサービスを提供することが望ましい。例えば、アドミニストレータは、ライセンス交付コンポーネントに変更が行われるたびに発行サービスを更新しなければならないことを望まないことがあり、逆も同様である。したがって、これらのサービスを互いに独立に提供するようにシステムを使用することができるならば有利である。したがって、複数のＤＲＭサービスを互いに独立に提供するモジュラ手法が当技術分野で求められている。主なビジネスロジックのコンポーネント化（ｃｏｍｐｏｎｅｎｔｉｚａｔｉｏｎ）を可能にし、それによって第３者がプラットフォームのＤＲＭ機能およびビジネスロジックを拡張および変更することができるならばこのような手法は特に有利である。

【００１１】

【課題を解決するための手段】

本発明は、デジタル権利管理システム用のセキュアサーバプラグインアーキテクチャを提供する。本発明によるデジタル権利管理サーバは、複数のデジタル権利管理サービスがそれぞれのパイプラインで実行され、それぞれのパイプラインが互いに独立であるパイプラインアーキテクチャに基づく。このようなサービスは、権利管理デジタルコンテンツを発行し、ライセンス交付することを含むことができる。各パイプラインは、デジタル権利管理サービスを実行する処理フレームワークと、デジタル権利管理サービスに関連するタスクをそれぞれ実行する複数のプラグインコンポーネントとを提供するサービスプログラムを含む。

【００１２】

ＤＲＭシステムプロバイダは、サービスプログラムと、それぞれのプラグインコンポーネントに関連する複数のデジタル権利管理プラグインオプションとを提供することができる。インストールの受信側が行った選択に基づいて、所望の各プラグインコンポーネントを、事前定義されたそれぞれの１組のインターフェース規則に従って処理フレームワーク内に統合することができる。

【００１３】

この複数のプラグインコンポーネントは、ある既定されたイベントの発生に基づいてそれぞれのタスクを実行する１つまたは複数の拡張プラグインコンポーネントを含むことができる。拡張プラグインコンポーネントは、サービスプログラムの処理を停止するように適合することができる。この複数のプラグインコンポーネントはまた、要求に対する主パイプライン処理が完了した後にそれぞれのタスクを実行する、１つまたは複数の非同期プラグインコンポーネントも含むことができる。

【００１４】

本発明の他の特徴は、添付の図面と共に行われる、本発明の実施形態の下記の詳細な説明からさらに明らかとなるであろう。

【００１５】

【発明の実施の形態】

例示的コンピュータ装置

図１と、以下の議論は、本発明を実施することができる適切なコンピュータ環境の簡潔な一般的説明を与えることを意図するものである。しかし、ハンドヘルドコンピュータ装置、ポータブルコンピューティン装置、およびすべての種類の他のコンピュータ装置も本発明と共に使用することが企図されることを理解されたい。以下では汎用コンピュータを説明するが、これは一例であり、本発明で必要とされるのは、ネットワークサーバの相互運用性および対話を有するシンクライアントだけである。したがって、クライアント資源を

ほとんど含まず、または最小のクライアント資源を含む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ブラウザまたはワールドワイドウェブへのインターフェースとして機能するネットワーク環境で本発明を実施することができる。

【００１６】

必須ではないが、開発者が使用するアプリケーションプログラミングインターフェース（ＡＰＩ）を介して本発明を実施することができ、かつ／または、クライアントワークステーション、サーバ、またはその他の装置などの１つまたは複数のコンピュータで実行されている、プログラムモジュールなどのコンピュータ実行可能命令の一般的状況で説明されるネットワークブラウジングソフトウェア内に本発明を含めることができる。一般に、プログラムモジュールは、特定のタスクを実行し、または特定の抽象データタイプを実装する、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。通常、様々な実施形態で、望む通りにプログラムモジュールの機能を組み合わせることができ、または分散させることができる。さらに、他のコンピュータシステム構成で本発明を実施できることを当業者は理解されよう。本発明と共に使用するのに適した他の周知のコンピューティングシステム、環境、および／または構成には、限定はしないがパーソナルコンピュータ（ＰＣ）、現金自動預払機、サーバコンピュータ、ハンドヘルド装置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のシステム、プログラマブル消費者向け電子機器、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、通信ネットワークまたはその他のデータ伝送媒体を介してリンクされるリモート処理装置によってタスクが実行される分散コンピューティング環境でも実施することができる。分散コンピューティング環境では、プログラムモジュールは、メモリ記憶装置を含む、ローカルコンピュータ記憶媒体とリモートコンピュータ記憶媒体のどちらにも位置することができる。

【００１７】

したがって図１は、本発明を実施することができる適切なコンピューティングシステム環境１００の一例を示しているが、上記で明らかにしたように、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に過ぎず、本発明の使用法または機能の範囲に関して何らかの制限を示唆するものではない。例示的動作環境１００に図示する構成要素のうちのいずれか１つ、あるいはそれらの組合せに関係する何らかの依存関係または要件をコンピューティング環境１００が有するものと解釈すべきでもない。

【００１８】

図１を参照すると、本発明を実施するための例示的システムは、コンピュータ１１０の形態の汎用コンピュータ装置を含む。コンピュータ１１０の構成要素は、限定はしないが、処理装置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構成要素を処理装置１２０に結合するシステムバス１２１とを含むことができる。システムバス１２１は、様々なバスアーキテクチャのうちのいずれかを用いる、メモリバスまたはメモリコントローラと、周辺バスと、ローカルバスとを含むいくつかのタイプのバス構造のうちのいずれでもよい。例えば、限定はしないが、このようなアーキテクチャには、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡ（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ）ローカルバス、およびＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ）バス（メザニンバスとも呼ばれる）が含まれる。

【００１９】

コンピュータ１１０は、一般に様々なコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータ１１０がアクセス可能である入手可能などのような媒体でもよく、それには揮発性媒体と不揮発性媒体の両方、取外し可能媒体と取外し不能媒体の両方が含まれる。例えば、限定はしないが、コンピュータ可読媒体はコンピュータ記憶媒体および通信媒体を含むことができる。コンピュータ記憶媒体は、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、または他のデータなどの情報を格納するための何らかの方法または技術で実装される、揮発性媒体と不揮発性媒体の両方、取外し可能媒体と取外し不能媒体の両方を含む。コンピュータ記憶媒体には、限定はしないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、または他のメモリ技術、ＣＤＲＯＭ、デジタル多用途ディスク（ＤＶＤ）、また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、または他の磁気記憶装置、あるいは、所望の情報を格納するのに使用することができ、コンピュータ１１０でアクセスすることができる他のどのような媒体も含まれる。通信媒体は一般に、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、または他のデータを、搬送波または他の移送機構などの被変調データ信号で実施し、通信媒体にはどのような情報送達媒体も含まれる。「被変調データ信号」という用語は、その特性集合のうちの１つまたは複数を有する信号、または情報を信号内に符号化するように変化する信号を意味する。例えば、限定はしないが、通信媒体には、有線ネットワークまたはダイレクト有線接続などの有線媒体、ならびに音響、ＲＦ、赤外線、および他の無線媒体などの無線媒体が含まれる。上記のいずれかの組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。

【００２０】

システムメモリ１３０は、読取り専用メモリ（ＲＯＭ）１３１およびランダムアクセスメモリ（ＲＡＭ）１３２などの揮発性メモリおよび／または不揮発性メモリの形態のコンピュータ記憶媒体を含む。始動中などにコンピュータ１１０内の要素間で情報を転送する助けになる基本ルーチンを含む基本入出力システム（ＢＩＯＳ）１３３が、一般にＲＯＭ１３１内に格納される。ＲＡＭ １３２は一般に、処理装置１２０に即座にアクセス可能であり、かつ／または処理装置１２０が現在操作しているデータおよび／またはプログラムモジュールを含む。例えば、限定はしないが、図１に、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。

【００２１】

コンピュータ１１０はまた、他の取外し可能／取外し不能な、揮発性／不揮発性コンピュータ記憶媒体も含むことができる。単なる一例であるが、図１に、取外し不能不揮発性磁気媒体を読み書きするハードディスクドライブ１４１と、取外し可能不揮発性磁気ディスク１５２を読み書きする磁気ディスクドライブ１５１と、ＣＤ ＲＯＭまたは他の光媒体などの取外し可能不揮発性光ディスク１５６を読み書きする光ディスクドライブ１５５とを示す。この例示的動作環境で使用することのできる他の取外し可能／取外し不能な揮発性／不揮発性コンピュータ記憶媒体には、限定はしないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、固体ＲＡＭ、および固体ＲＯＭなどが含まれる。ハードディスクドライブ１４１は一般に、インターフェース１４０などの取外し不能メモリインターフェースを介してシステムバス１２１に接続され、磁気ディスクドライブ１５１および光ディスクドライブ１５５は一般に、インターフェース１５０などの取外し可能メモリインターフェースによってシステムバス１２１に接続される。

【００２２】

上記で議論し、図１に図示するドライブと、関連するコンピュータ記憶媒体は、コンピュータ１１０に対してコンピュータ可読命令、データ構造、プログラムモジュール、および他のデータの記憶を提供する。例えば図１では、ハードディスクドライブ１４１が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を格納するものとして図示されている。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と同じでよく、または異なってい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には、少なくともこれらが相異なるコピーであることを示すために異なる符

号を付けてある。ユーザは、キーボード１６２や、マウス、トラックボール、またはタッチパッドと一般に呼ば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、コマンドおよび情報をコンピュータ１１０に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、サテライトディッシュ、スキャナなどを含めることができる。これらの入力装置や他の入力装置はしばしば、システムバス１２１に結合されるユーザ入力インターフェース１６０を介して処理装置１２０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）などの他のインターフェースおよびバス構造によって接続することもできる。

【００２３】

モニタ１９１または他のタイプのディスプレイ装置もまた、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に接続される。ノースブリッジなどのグラフィックスインターフェース１８２もシステムバス１２１に接続することができる。ノースブリッジは、ＣＰＵまたはホスト処理装置１２０と通信し、アクセラレーテッドグラフィックスポート（ＡＧＰ）通信に関する責任を引き受けるチップセットである。１つまたは複数のグラフィックス処理装置（ＧＰＵ）１８４が、グラフィッ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、ＧＰＵ　１８４は一般に、レジスタ記憶装置などのオンチップ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ＧＰＵ　１８４はコプロセッサの一例であり、したがって様々なコプロセッシング装置をコンピュータ１１０内に含めることができる。モニタ１９１または他のタイプのディスプレイ装置も、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、そのインターフェースはビデオメモリ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およびプリンタ１９６などの他の周辺出力装置も含むことができ、その周辺出力装置は、出力周辺インターフェース１９５を介して接続することができる。

【００２４】

コンピュータ１１０は、リモートコンピュータ１８０などの１つまたは複数のリモートコンピュータへの論理接続を使用して、ネットワーク環境で動作することができる。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、ピア装置、または他の共通ネットワークノードでよく、一般にコンピュータ１１０に関して上記で述べた要素のうちの多数またはすべてを含むが、図１にはメモリ記憶装置１８１だけを示してある。図１に示す論理接続は、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むことができる。このようなネットワーキング環境は、オフィス、企業全体のコンピュータネットワーク、イントラネット、およびインターネットで一般的なものである。

【００２５】

ＬＡＮネットワーキング環境で使用する際、コンピュータ１１０は、ネットワークインターフェース／アダプタ１７０を介してＬＡＮ　１７１に接続される。ＷＡＮネットワーキング環境で使用する際、コンピュータ１１０は一般に、インターネットなどのＷＡＮ　１７３を介して通信を確立するためのモデム１７２または他の手段を含む。モデム１７２は内蔵でも外付けでもよく、ユーザ入力インターフェース１６０、または他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。ネットワーク環境では、コンピュータ１１０に関して示したプログラムモジュールまたはその一部を、リモートメモリ記憶装置内に格納することができる。例えば、限定はしないが、図１に、リモートアプリケーションプログラム１８５をメモリ装置１８１上に常駐するものとして示す。図示するネットワーク接続は例示的なものであって、コンピュータ間の通信リンクを確立する他の手段も使用できることを理解されたい。

【００２６】

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なら理解することができよう。この点で、本発明は、任意の数のメモリまたは記憶装置と、任意の数の記憶装置または記憶ボリュームにわたって発生す

る任意の数のアプリケーションおよびプロセスとを有する任意のコンピュータシステムに関係する。本発明は、ネットワーク環境に配置され、リモート記憶装置またはローカル記憶装置を有する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備える環境に適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、プログラミング言語解釈機能、およびプログラミング言語実行機能を有するスタンドアロンコンピュータ装置にも適用することができる。

【００２７】

分散コンピューティングにより、コンピュータ装置／システム間の直接交換によるコンピュータ資源／サービスの共用が容易になる。これらの資源およびサービスには、情報の交換、キャッシュストレージ、およびファイルについてのディスクストレージが含まれる。分散コンピューティングはネットワーク接続性を活用し、それにより、クライアントがクライアントの集合的な能力を活用して企業全体に利益を与えることが可能となる。この点で、様々な装置が、トラステッドグラフィックスパイプラインについての本発明の認証技法を含むように対話することができるアプリケーション、オブジェクト、または資源を有することができる。

【００２８】

図２に、例示的なネットワークコンピューティング環境または分散コンピューティング環境の略図を与える。この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など、およびコンピューティングオブジェクト／装置１１０ａ、１１０ｂ、１１０ｃなどを含む。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、プログラマブルロジックなどを含むことができる。オブジェクトは、ＰＤＡ、テレビジョン、ＭＰ３プレーヤ、テレビジョン、パーソナルコンピュータなどの同じ装置または異なる装置の各部を含むことができる。各オブジェクトは、通信ネットワーク１４によって他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タ装置を含むことができる。本発明の一態様によれば、各オブジェクト１０または１１０は、トラステッドグラフィックスパイプラインについての本発明の認証技法を要求することができるアプリケーションを含むことができる。

【００２９】

１１０ｃなどのオブジェクトを別のコンピュータ装置１０または１１０上にホストできることも理解できよう。したがって、ここに示す物理的環境は、接続された装置をコンピュータとして示すことができるが、このような図示は単なる例であり、別法として、ＰＤＡ、テレビジョン、ＭＰ３プレーヤなどの様々なデジタル装置、インターフェース、ＣＯＭオブジェクトなどのソフトウェアオブジェクトを有する物理的環境を示し、または説明することもできる。

【００３０】

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、構成要素、およびネットワーク構成が存在する。例えば、コンピューティングシステムは、ワイヤラインシステムまたは無線システムによって接続することができ、ローカルネットワークまたは広域分散ネットワーク（ｗｉｄｅｌｙ ｄｉｓｔｒｉｂｕｔｅｄ ｎｅｔｗｏｒｋｓ）によって接続することができる。現在では、ネットワークの多くがインターネットに結合されている。インターネットは、広域分散コンピューティングについてのインフラストラクチャを提供し、多数の異なるネットワークを包含する。

【００３１】

ホームネットワーキング環境では、電力線、データ（無線と有線の両方）、音声（例えば電話）、およびエンターテイメントメディアなどの固有プロトコルをそれぞれサポートすることができる少なくとも４つの異なるネットワーク移送媒体が存在する。光スイッチ／電気器具などのほとんどの家庭制御装置は、接続するために電力線を使用することができる。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）として家庭に入ることができ、無線（例えば、ＨｏｍｅＲＦまたは８０２．１１ｂ）接続または

有線（例えば、ＨｏｍｅＰＮＡ、Ｃａｔ　５、さらには電力線）接続を使用して家庭内でアクセス可能である。ボイストラフィックは、有線（例えばＣａｔ　３）または無線（例えば携帯電話）として家庭に進入することができ、Ｃａｔ　３配線を使用して家庭内で配布することができる。エンターテイメントメディアは、衛星またはケーブルを介して家庭に入ることができ、一般には同軸ケーブルを使用して家庭内で配布することができる。媒体装置のクラスタのためのデジタル相互接続としてＩＥＥＥ　１３９４およびＤＶＩも出現しつつある。これらのネットワーク環境や、プロトコル標準として出現する可能性のあるその他のネットワーク環境のすべては、相互接続してイントラネットを形成することができ、イントラネットは、インターネットによって外の世界に接続することができる。簡単に言えば、データを格納および伝送するために様々な異なる供給源が存在し、したがってコンピュータ装置は、データ処理パイプラインのすべての部分でコンテンツを保護する方法を必要とすることになる。

【００３２】

インターネットは一般に、コンピュータネットワーキングの技術分野で周知である、プロトコルのＴＣＰ／ＩＰスイート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す。ＴＣＰ／ＩＰは、「Ｔｒａｎｓｐｏｒｔ　ＣｏｎｔｒｏｌＰｒｏｔｏｃｏｌ／Ｉｎｔｅｒｆａｃｅ　Ｐｒｏｇｒａｍ」の頭字語である。インターネットは、ユーザがネットワークを介して情報と対話し、情報を共用することを可能にす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、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であると説明することができる。このような広い範囲にわたって情報を共用するために、インターネットなどのリモートネットワークは、これまでのところ一般には、開発者が専用のオペレーションまたはサービスを実行するために本質的に無制限にソフトウェアアプリケーションを設計することができるオープンシステムとして発展してきた。

【００３３】

したがって、この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、ピアツーピア、また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となる。「クライアント」とは、クライアントが関係しない別のクラスまたはグループのサービスを使用するクラスまたはグループのメンバである。したがって、コンピューティングにおいて、クライアントは、別のプログラムによって提供されるサービスを要求するプロセス、すなわち大雑把に言えば１組の命令またはタスクである。クライアントプロセスは、他のプログラムまたはサービス自体についての基本的な詳細を「認識」する必要なしに、要求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、特にネットワークシステムでは、クライアントは通常、別のコンピュータ、例えばサーバによって提供される共用ネットワーク資源にアクセスするコンピュータである。図２の例では、サーバ１０ａ、１０ｂなどがデータを維持し、次いでそのデータがクライアントコンピュータ１１０ａ、１１０ｂなどに複写される場合、コンピュータ１１０ａ、１１０ｂなどをクライアントとみなすことができ、コンピュータ１０ａ、１０ｂなどをサーバとみなすことができる。

【００３４】

サーバは一般に、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でアクティブにすることができ、サーバプロセスは第２のコンピュータシステムでアクティブにすることができ、それらが通信媒体を介して互いに通信し、したがって分散機能が提供され、複数のクライアントがサーバの情報収集機能を利用することが可能となる。

【００３５】

クライアントとサーバは、プロトコル層で提供される機能を使用して互いに通信する。例えば、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ－Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）は、ワールドワイドウェブ（ＷＷＷ）と共に使用される一般的なプロトコルである。通常、ＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）またはＩＰ（Ｉｎｔｅｒｎ

ｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスなどのコンピュータネットワークアドレスを使用して、サーバコンピュータ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もできる。例えば、通信媒体を介して通信を実現することができる。具体的には、高容量通信用のＴＣＰ／ＩＰ接続を介して、クライアントとサーバを互いに結合することができる。

【００３６】

したがって、図２は、サーバがネットワーク／バスを介してクライアントコンピュータと通信している、本発明を利用することができる例示的なネットワーク環境または分散環境を示す。より詳細には、いくつかのサーバ１０ａ、１０ｂなどが、本発明に従って、通信ネットワーク／バス１４（ＬＡＮ、ＷＡＮ、イントラネット、インターネットなどでよい）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、ネットワーク機器、あるいはＶＣＲ、ＴＶ、オーブン、ライト、ヒータなどの他の装置などのいくつかのクライアントまたはリモートコンピュータ装置１１０ａ、１１０ｂ、１１０ｃ、１１０ｄなどに相互接続される。したがって、トラステッドソースからのセキュアコンテンツを処理し、格納し、またはレンダリングすることが望ましい任意のコンピュータ装置に本発明を適用できることが企図される。

【００３７】

通信ネットワーク／バス１４がインターネットであるネットワーク環境では、例えばサーバ１０は、クライアント１１０ａ、１１０ｂ、１１０ｃ、１１０ｄ、１１０ｅなどがＨＴＴＰなどのいくつかの周知プロトコルのうちのいずれかを介して通信するウェブサーバでよい。サーバ１０は、分散コンピューティング環境の特徴であるが、クライアントとして働くこともできる。通信は、適切ならば有線または無線でよい。クライアント装置１１０は、通信ネットワーク／バス１４を介して通信することも、しないこともあり、それに関連する独立な通信を有することができる。例えば、ＴＶまたはＶＣＲの場合、その制御に対してネットワーク化された性質があってもよく、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またはオブジェクト１３５を備えることができ、かつ、ファイルを格納することができ、またはファイルの一部をダウンロードまたは移送することができる、様々なタイプの記憶素子またはオブジェクトへの接続またはアクセスを備えることができる。したがって、コンピュータネットワーク／バス１４にアクセスすることができ、それと対話することができる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などと対話することができるサーバコンピュータ１０ａ、１０ｂなどと、他の装置１１１と、データベース２０とを有するコンピュータネットワーク環境で本発明を使用することができる。

【００３８】

デジタルコンテンツの発行

図３は、デジタルコンテンツを発行するための、本発明によるシステムおよび方法の好ましい実施形態の機能ブロック図である。本明細書で用いる用語「発行」は、トラステッドエンティティをそのコンテンツについて発行することができる１組の権利および条件をそのエンティティと共に確立するようにアプリケーションまたはサービスが従うプロセスを指す。本発明によれば、発行プロセスは、デジタルコンテンツを暗号化すること、およびコンテンツの作者がコンテンツのすべての可能性のあるユーザに対して意図した、永続的に実施可能な権利のリストを関連付けることを含む。コンテンツの作者が意図したのでない限り、権利のいずれかへのアクセスまたはコンテンツへのアクセスを禁止するために、保護された方式でこのプロセスを実行することができる。

【００３９】

本発明の好ましい実施形態では、具体的には次の３つのエンティティを利用してセキュアデジタルコンテンツを発行する。そのエンティティとは、クライアント３００上で実行され、発行のためにコンテンツを準備するコンテンツ準備アプリケーション３０２、やはりクライアント装置３００上に常駐するデジタル権利管理（ＤＲＭ）アプリケーションプロ

グラムインターフェース（ＡＰＩ）３０６、および通信ネットワーク３３０を介してクライアント３００に通信可能に結合されるＤＲＭサーバ３２０である。本発明の好ましい実施形態では、通信ネットワーク３３０はインターネットを含むが、通信ネットワーク３３０は、例えば独自のイントラネットなどの、どのようなローカルネットワークまたは広域ネットワークでもよいことを理解されたい。

【００４０】

コンテンツ準備アプリケーション３０２は、デジタルコンテンツを生成するどのようなアプリケーションでもよい。例えば、アプリケーション３０２はワードプロセッサでよく、またはデジタルテキストファイル、デジタル音楽、ビデオ、またはその他のそのようなコンテンツを生成する他の発行者でよい。コンテンツはまた、例えばライブイベントまたはテープ記録されたイベントのストリーミングオーディオ／ビデオなどのストリーミングコンテンツも含むことができる。本発明によれば、コンテンツ準備アプリケーションは、コンテンツ準備アプリケーションのユーザに、ユーザが提供する鍵を用いてコンテンツを暗号化するよう招待する。アプリケーション３０２は、この鍵を使用してデジタルコンテンツを暗号化し、したがって暗号化デジタルコンテンツファイル３０４を形成する。クライアントアプリケーションはまた、デジタルコンテンツファイル３０４についての権利データを提供するようユーザに招待する。権利データは、デジタルコンテンツでの権利を有する各エンティティについての識別を含む。そのようなエンティティは例えば、個人、個人のクラス、または装置でよい。そのような各エンティティについて、権利データはまた、エンティティがコンテンツで有する権利のリスト、およびそれらの権利のいずれかまたはすべてに対して課すことができる任意の条件も含む。そのような権利は、デジタルコンテンツを読み取り、編集し、コピーし、印刷するなどの権利を含むことができる。加えて、権利は包括的でよく、または排他的でよい。包括的な権利は、指定のユーザがコンテンツ内に指定の権利を有する（例えば、ユーザがデジタルコンテンツを編集することができる）ことを示す。排他的な権利は、指定のユーザが指定された権利を除いてコンテンツ内のすべての権利を有する（例えば、ユーザはデジタルコンテンツをコピーすることを除き、デジタルコンテンツを用いてどのようなことでも行うことができる）ことを示す。

【００４１】

本発明の一実施形態によれば、クライアントＡＰＩ　３０６は、暗号化デジタルコンテンツおよび権利データをＤＲＭサーバ３２０に渡すことができる。ＤＲＭサーバ３２０は、以下で詳細に説明するプロセスを使用して、ユーザが割り当てた権利を実施することができるかどうかを判定し、実施することができる場合、ＤＲＭサーバ３２０は権利データに署名し、署名済み権利ラベル（ＳＲＬ）３０８を形成する。しかし一般には、どのトラステッドエンティティも、好ましくはＤＲＭサーバ３２０が承認した鍵を使用して権利データに署名することができる。例えば、クライアントは、ＤＲＭサーバ３２０がクライアントに提供した鍵を使用して権利データに署名することができる。

【００４２】

権利ラベル３０８は、権利記述を表す権利データ、暗号化コンテンツ鍵、ならびに権利記述および暗号化コンテンツ鍵に関するデジタルシグニチャを含むことができる。ＤＲＭサーバが権利ラベルに署名している場合、ＤＲＭサーバは、クライアントＡＰＩ　３０６を介して署名済み権利ラベル３０８をクライアントに戻し、クライアントＡＰＩ　３０６は、クライアント装置３００上に署名済み権利ラベル３０８を格納する。次いでコンテンツ準備アプリケーション３０２は、署名済み権利ラベル３０８を暗号化デジタルコンテンツファイル３０４に関連付ける。例えば、ＳＲＬ　３０８を暗号化デジタルコンテンツファイルと連結して権利管理コンテンツファイル３１０を形成することができる。しかし一般には、権利データをデジタルコンテンツと組み合わせる必要はない。例えば、権利データを既知の位置に格納することができ、格納した権利データへの参照を暗号化デジタルコンテンツと組み合わせることができる。この参照は、権利データが格納されている場所（権利データを含むデータストア）を示す識別子と、その特定の格納位置のその特定の権利データに対応する（例えば、当該の特定の権利データを含むファイルを識別する）識別子と

を含むことができる。次いで、権利管理コンテンツ３１０を、誰にでも、どこにでも送達することができ、そのコンテンツを消費する権利を有するエンティティだけが、そのエンティティに割り当てられた権利に従うことによってのみ、そのコンテンツを消費することができる。

【００４３】

図４は、権利管理デジタルコンテンツを発行するための、本発明による例示的方法４００の流れ図であり、権利ラベルがＤＲＭサーバによって署名されている。しかし、この実施形態は単に例であり、一般には任意のトラステッドエンティティによって権利ラベルに署名できることを理解されたい。一般に、デジタルコンテンツを発行するための本発明による方法は、コンテンツ鍵（ＣＫ）を使用してデジタルコンテンツを暗号化すること、デジタルコンテンツに関連する権利記述を生成すること、ＤＲＭサーバについての公開鍵（ＰＵ－ＤＲＭ）に従ってコンテンツ鍵（ＣＫ）を暗号化して（ＰＵ－ＤＲＭ（ＣＫ））を得ること、および権利記述と（ＰＵ－ＤＲＭ（ＣＫ））の組合せを介して、（ＰＵ－ＤＲＭ）に対応する秘密鍵（ＰＲ－ＤＲＭ）に基づいてデジタルシグニチャを作成することを含むことができる。

【００４４】

ステップ４０２では、アプリケーション３０２が、デジタルコンテンツを暗号化するのに使用するコンテンツ鍵（ＣＫ）を生成する。好ましくはコンテンツ鍵（ＣＫ）は対称鍵であるが、一般にはデジタルコンテンツを暗号化するのにどのような鍵も使用することができる。対称鍵アルゴリズムは、「秘密鍵」アルゴリズムと呼ばれることもあり、メッセージを暗号化するのに用いたのと同じ鍵を使用してメッセージを暗号解読する。このため、（ＣＫ）を秘密に保つことが好ましい。送信側と受信側との間での（ＣＫ）の共有は、そのような（ＣＫ）が無許可に傍受されることを回避するために、非常に注意深く行うべきである。（ＣＫ）はエンクリプタとデクリプタの両方の間で共有されるので、暗号化メッセージを送信する前に（ＣＫ）を通信することが好ましい。

【００４５】

いくつかの対称鍵生成アルゴリズムが当技術分野で周知である。好ましい実施形態では、データ暗号化規格（ＤＥＳ）が利用されるが、どのような対称アルゴリズムも使用できることを理解されたい。そのような対称鍵アルゴリズムの例には、限定はしないが、Ｔｒｉｐｌｅ－ＤＥＳ、ＩＤＥＡ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ａｌｇｏｒｉｔｈｍ）、Ｃａｓｔ、Ｃａｓｔ－１２８、ＲＣ４、ＲＣ５、およびＳｋｉｐＪａｃｋが含まれる。

【００４６】

ステップ４０４では、アプリケーション３０２が、対称コンテンツ鍵（ＣＫ）を用いてデジタルコンテンツを暗号化し、暗号化デジタルコンテンツ３０４を形成する。暗号化デジタルコンテンツ３０４は、（ＣＫ（ｃｏｎｔｅｎｔ））という表記を用いて書くことができる。アプリケーション３０２を使用する作者はまた、デジタルコンテンツに関連する権利データも生成することができる。権利データは、コンテンツを消費する資格を有することになるエンティティのリスト、ならびに各エンティティがコンテンツに関して所有する特定の権利およびその権利に課すことができる何らかの条件を含むことができる。このような権利は、例えば、コンテンツの閲覧、コンテンツの印刷などを含むことができる。アプリケーション３０２は、権利データをＡＰＩ ３０６に提供する。ＸＭＬ／ＸｒＭＬフォーマットの権利データの一例を、付録１として本明細書に添付する。

【００４７】

ステップ４０６では、ＡＰＩ ３０６が、コンテンツ鍵（ＣＫ）を暗号化するのに使用する第２の暗号鍵（ＤＥＳ１）を生成する。好ましくは、（ＤＥＳ１）も対称鍵である。ステップ４０８では、ＡＰＩ ３０６が（ＤＥＳ１）を用いて（ＣＫ）を暗号化し、（ＤＥＳ１（ＣＫ））を得る。ステップ４１０では、ＡＰＩ ３０６が（ＣＫ）を廃棄し、今や（ＤＥＳ１（ＣＫ））を暗号解読することによってのみ（ＣＫ）を得ることができるという結果になる。（ＣＫ（ｃｏｎｔｅｎｔ））を中央ＤＲＭサーバ３２０に対して確実に保

護し、かつコンテンツに対するすべての「ライセンス要求」を権利データに従って中央で行うことを保証するために、ＡＰＩ　３０６は、ステップ４１２で、提供されるＤＲＭサーバ３２０と連絡し、その公開鍵（ＰＵ－ＤＲＭ）を取り出す。ステップ４１４では、ＡＰＩ　３０６が（ＰＵ－ＤＲＭ）を用いて（ＤＥＳ１）を暗号化し、（ＰＵ－ＤＲＭ（ＤＥＳ１））を得る。したがって、（ＰＵ－ＤＲＭ））に対して（ＣＫ）を保護して、ＤＲＭサーバ３２０が、（ＣＫ）へのアクセスを得ることができることになる唯一のエンティティであることを保証することができ、（ＣＫ（ｃｏｎｔｅｎｔ））を暗号解読するように要求される場合も同様である。ステップ４１６では、ＡＰＩ　３０６が、（ＤＥＳ１）を用いて権利データ（すなわち、許可されたエンティティのリストと、リスト中の許可された各エンティティに関連するそれぞれの権利および条件）を暗号化し、（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））が得られる。

【００４８】

代替実施形態では、（ＣＫ）を使用して権利データを直接暗号化し、（ＣＫ（ｒｉｇｈｔｓｄａｔａ））を得ることができ、それによって（ＤＥＳ１）の使用に完全に先行する。しかし、（ＤＥＳ１）を使用して権利データを暗号化することにより、そのような（ＤＥＳ１）を、ＤＲＭサーバにとって扱いやすい任意の特定のアルゴリズムに適合させることが可能となり、一方（ＣＫ）はＤＲＭサーバとは無関係にエンティティによって指定することができ、ＤＲＭサーバにとって扱いやすくない可能性がある。

【００４９】

ステップ４１８では、コンテンツ保護アプリケーション３０２が、（ＰＵ－ＤＲＭ（ＤＥＳ１））および（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を署名のための権利ラベルとしてＤＲＭサーバ３２０にサブミットすることができる。あるいは、クライアント自体が権利データに署名することができる。権利データを署名のためにサーバにサブミットしている場合、ステップ４２０では、ＤＲＭサーバ３２０が権利データにアクセスし、サブミットした権利ラベル内の権利および条件をＤＲＭサーバ３２０が実施できることを検証する。ＤＲＭサーバ３２０が権利データを実施できることを検証するため、ＤＲＭサーバ３２０は（ＰＲ－ＤＲＭ）を（ＰＵ－ＤＲＭ（ＤＥＳ１））に適用して（ＤＥＳ１）を得、次いで（ＤＥＳ１）を（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））に適用して、疑いのない権利データを得る。次いでサーバ３２０は、権利データ内で指定されたユーザ、権利、および条件がサーバ３２０で実施される任意のポリシー内にあることを検証するために、任意のポリシーチェックを行うことができる。サーバ３２０は、（ＰＵ－ＤＲＭ（ＤＥＳ１））および（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を含む、最初にサブミットされた権利ラベルに署名して、署名済み権利ラベル（ＳＲＬ）３０８を得（ただし、シグニチャはＤＲＭサーバ３２０の秘密鍵（ＰＲ－ＤＲＭ）に基づく）、ＳＲＬ　３０８をＡＰＩ　３０６に返す。次いでＡＰＩ　３０６は、返されたＳＲＬ　３０８をクライアントアプリケーション３０２に提示する。

【００５０】

ＳＲＬ　３０８は、デジタル署名された文書であり、それによりＳＲＬ　３０８が改ざんに対して強くなる。加えてＳＲＬ　３０８は、コンテンツを暗号化するのに使用する実際の鍵タイプおよびアルゴリズムとは無関係であるが、保護しているコンテンツと強い１対１の関係を維持する。次に図４Ａを参照すると、本発明の一実施形態では、ＳＲＬ　３０８はとりわけ、恐らくコンテンツのＩＤを含むＳＲＬ　３０８の基礎であるコンテンツについての情報、（ＰＵ－ＤＲＭ（ＤＥＳ１））と、ネットワーク上にＤＲＭサーバを配置するためのＵＲＬなどの参照情報と、およびＵＲＬが役に立たない場合のフォールバック情報とを含む、ＳＲＬ　３０８に署名するＤＲＭサーバについての情報、ＳＲＬ　３０８自体を記述する情報、（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））：（ＤＥＳ１（ＣＫ））、ならびにＳ（ＰＲＤＲＭ）を含むことができる。ＸＭＬ／ＸｒＭＬの形のサンプルＳＲＬ　３０８を、付録２として添付する。

【００５１】

トラステッドエンティティが権利データに署名して署名済み権利ラベル３０８を作成する

ことを保証することにより、ＤＲＭサーバは、権利ラベル３０８の権利データ内に記述される、発行者によって記述された条件に従ってコンテンツに関するライセンスを発行することを表明している。理解すべきであるが、特にライセンスがコンテンツ鍵（ＣＫ）を含む限り、ユーザは、コンテンツをレンダリングするのにライセンスを得る必要がある。ユーザが暗号化コンテンツに関するライセンスを得たいとき、ユーザは、そのコンテンツについてのＳＲＬ　３０８と、ＤＲＭサーバ３２０または他のライセンス発行エンティティに対するユーザのクリデンシャルを検証する証明書とを含むライセンス要求を提示することができる。次いでライセンス発行エンティティは、（ＰＵ－ＤＲＭ（ＤＥＳ１））および（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を暗号解読して権利データを生成し、作者が存在するならば作者からライセンス要求側エンティティに付与される権利すべてをリストし、その特定の権利だけを用いてライセンスを構築することができる。

【００５２】

好ましくは、アプリケーション３０２がＳＲＬ　３０８を受け取る際、そのようなアプリケーション３０２が、署名済み権利ラベル３０８を、対応する（ＣＫ（ｃｏｎｔｅｎｔ））３０４と連結し、権利管理デジタルコンテンツを形成する。あるいは、暗号化デジタルコンテンツを備える既知の位置を参照して、権利データをその位置に格納することもできる。したがって、ＤＲＭが使用可能なレンダリングアプリケーションは、レンダリングアプリケーションがレンダリングしようと試みているコンテンツを介して、署名済み権利ラベル３０８を発見することができる。この発見により、レンダリングアプリケーションがＤＲＭライセンス交付サーバ３２０に対してライセンス要求を開始する。発行側アプリケーション３０２は、例えばＤＲＭライセンス交付サーバ３２０に対するＵＲＬを格納することができ、またはＤＲＭライセンス交付サーバ３２０は、権利ラベルにデジタルに署名する前に、それ自体のＵＲＬを１つのメタデータとして権利ラベルに組み込むことができ、その結果、レンダリングアプリケーションによって呼び出されるＤＲＭクライアントＡＰＩ　３０６は、正しいＤＲＭライセンス交付サーバ３２０を識別することができる。好ましくは、例えばＧＵＩＤ（ｇｌｏｂａｌｌｙ　ｕｎｉｑｕｅ　ｉｄｅｎｔｉｆｉｅｒ）などの固有識別子が、権利ラベルが署名される前に権利ラベルに入れられる。

【００５３】

本発明の好ましい実施形態では、コンテンツ保護アプリケーション３０２またはレンダリングアプリケーションとＤＲＭサーバ３２０との間の通信のためにＳＯＡＰ（ｓｉｍｐｌｅ　ｏｂｊｅｃｔ　ａｃｃｅｓｓ　ｐｒｏｔｏｃｏｌ）を使用することができる。加えて、ＡＰＩ　３０６などのＡＰＩライブラリを提供することができ、その結果、アプリケーション３０２などのアプリケーションがＤＲＭプロトコルのクライアント側を実施する必要がなく、むしろ単にローカルＡＰＩ呼出しを行うことができる。好ましくは、デジタルコンテンツについての権利記述、ライセンス、および権利ラベルを記述するためにＸｒＭＬ、およびＸＭＬ言語が使用されるが、権利記述およびその他のデータに関してどのような適切なフォーマットも使用できることを理解されたい。

【００５４】

発行済みコンテンツについてのライセンスの取得

図５は、権利管理デジタルコンテンツをライセンス交付するための、本発明によるシステムおよび方法の好ましい実施形態の機能ブロック図である。本明細書で使用する「ライセンス交付」という用語は、アプリケーションまたはサービスが、ライセンスで指定されたエンティティがライセンスで指定された条件に従ってコンテンツを消費することを可能にするライセンスを要求し、受け取るように追従するプロセスを指す。ライセンス交付プロセスへの入力は、ライセンスが要求されているコンテンツに関連する署名済み権利ラベル（ＳＲＬ）３０８と、ライセンスが要求されているエンティティの公開鍵証明書とを含むことができる。ライセンスを要求するエンティティは、必ずしもライセンスの要求を受けているエンティティである必要はないことに留意されたい。通常、ライセンスは、ＳＲＬ　３０８からの権利記述、暗号化コンテンツを暗号解読することができる暗号化鍵、権利記述および暗号化鍵に関するデジタルシグニチャを含む。デジタルシグニチャは、エンテ

ィティおよび指定される権利が本物であることを表明する。

【００５５】

アプリケーション３０２が権利管理コンテンツ３１０を消費するための１つの方法は、クライアントＡＰＩ　３０６が通信ネットワーク３３０を介して権利管理コンテンツ３１０の署名済み権利ラベル３０８をＤＲＭサーバ３２０に転送することである。ＤＲＭサーバ３２０の位置は、例えばＳＲＬ　３０８中の参照情報内で見つけることができる。このような実施形態では、ＤＲＭライセンス交付サーバ３２０は、以下で詳細に説明するプロセスを介して、権利ラベル中の権利記述を使用し、ライセンスを発行することができるかどうかを判定し、発行することができる場合、権利記述を導出してライセンスと共に含むことができる。前述のように、権利ラベル３０８は、ＤＲＭサーバ３２０の公開鍵（ＰＵ－ＤＲＭ）に従って暗号化されたコンテンツ鍵（ＣＫ）（すなわち（ＰＵ－ＤＲＭ（ＣＫ））を含む。ライセンスを発行するプロセスでは、ＤＲＭサーバ３２０はこの値を安全に暗号解読して（ＣＫ）を得る。次いでＤＲＭサーバ３２０は、ライセンス要求で渡される公開鍵証明書中の公開鍵（ＰＵ－ＥＮＴＩＴＹ）を使用して、（ＣＫ）を再暗号化する（すなわち（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））。新たに暗号化された（ＰＵ－ＥＮＴＩＴＩＹ（ＣＫ））は、サーバ３２０がライセンス内に配置するものである。したがって、関連する秘密鍵（ＰＲ－ＥＮＴＩＴＹ）の保持者だけが（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））から（ＣＫ）を復元することができるので、（ＣＫ）を公開する危険を伴わずにライセンスを呼出し元に返すことができる。次いでクライアントＡＰＩ　３０６は（ＣＫ）を使用して暗号化コンテンツを暗号解読し、暗号解読デジタルコンテンツ３１２を形成する。次いでクライアントアプリケーション３０２は、ライセンスで提供される権利に従って暗号解読デジタルコンテンツ３１２を使用することができる。

【００５６】

あるいは、例えば発行側クライアントなどのクライアントは、それ自体のライセンスを発行してコンテンツを消費することができる。そのような実施形態では、適切な環境の下でデジタルコンテンツを暗号解読するのに必要な鍵をクライアントに提供するクライアントコンピュータ上で、保護プロセスを実行することができる。

【００５７】

図６Ａおよび６Ｂに、権利管理デジタルコンテンツをライセンス交付するための、本発明による方法６００の好ましい実施形態の流れ図を与える。本発明によれば、要求側エンティティが、１つまたは複数の潜在的なライセンスの代わりにライセンス要求をサブミットすることができる。要求側エンティティは、潜在的なライセンス所有者のうちの１つでよく、そうでなくてもよい。潜在的ライセンス所有者は、個人、グループ、装置、またはコンテンツを何らかの方式で消費することができるその他の任意のエンティティでよい。これから、ＤＲＭサーバがライセンス要求を処理する実施形態を参照しながら方法６００を説明するが、クライアント上でライセンス要求処理を実行し、クライアントがライセンスを直接発行することもできることを理解されたい。

【００５８】

ステップ６０２では、例えばＤＲＭサーバなどのライセンス発行エンティティが、ライセンス要求を受け取る。好ましくは、ライセンス要求は、要求した１つまたは複数のライセンス所有者それぞれについての公開鍵証明書または識別を含む。ライセンス要求の好ましい実施形態についてのＳＯＡＰプロトコルは、以下の通りである。

【００５９】

```
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Body>
  <AcquireLicense xmlns="http://xxxx.com/PublishingService">

   <RequestParams>
    <AcquireLicenseParams>
     <LicenseeCerts>
      <String>string</String>
      <String>string</String>
      </LicenseeCerts>
      <RightsSpecification>string</RightsSpecification>

      <RightsOfferID>string</RightsOfferID>
      <ApplicationData>string</ApplicationData>
    </AcquireLicenseParams>
    <AcquireLicenseParams>
          ...
    </AcquireLicenseParams>
   </RequestParams>
  </AcquireLicense>
 </soap:Body>
</soap:Envelope>
```

【００６０】
ステップ６０４では、要求側エンティティ（すなわち、ライセンス要求を行うエンティティ）を認証する。本発明の一実施形態によれば、ライセンス発行エンティティは、プロトコル（例えばチャレンジ－応答）認証を使用して要求側エンティティの識別を決定するように構成することができ、または要求側エンティティの認証を要求しないように構成することができる（「匿名認証を可能にする」とも呼ばれる）。認証が必要である場合、どのようなタイプの認証方式も使用することができる（例えば、前述のチャレンジ－応答方式、ＭＩＣＲＯＳＯＦＴ．ＮＥＴ、ＰＡＳＳＰＯＲＴ、ＷＩＮＤＯＷＳ（登録商標）許可などのユーザｉｄ／パスワード方式、ｘ５０９など）。好ましくは、匿名認証が可能であり、かつ統合情報システムがサポートする任意のプロトコル認証方式をサポートする。認証ステップの結果は、例えば「匿名」識別（匿名認証の場合）、または個人のアカウント識別などの識別となる。ライセンス要求を何らかの理由で許可することができない場合、エラーを返し、ライセンスを付与しない。

【００６１】
ステップ６０６では、認証したエンティティを許可する。すなわち、ステップ６０８で認証したエンティティが（そのエンティティ自体のために、または別のエンティティの代わりに）ライセンスを要求することが可能であるかどうかを判定する。好ましくは、ライセンス発行エンティティが、ライセンスを要求することが可能な（または可能でない）エンティティのリストを格納する。好ましい実施形態では、この識別のリスト中の識別が、ライセンスを要求されているエンティティの識別ではなく、要求を作成するエンティティの識別である。しかし、そのどちらでもよい。例えば、個人のアカウント識別はライセンス要求を直接行うことが可能でないことがあるが、トラステッドサーバプロセスがそのようなエンティティの代わりにライセンス要求を行うことができる。

【００６２】
本発明によれば、ライセンス要求は、潜在的な各ライセンス所有者についての公開鍵証明書または識別を含むことができる。１つのライセンス所有者だけに対してライセンスが要求された場合、１つの証明書または識別だけが指定される。複数のライセンス所有者に対してライセンスが要求された場合、潜在的な各ライセンス所有者について証明書または識別を指定することができる。

【００６３】
好ましくは、ライセンス発行エンティティは、有効な各ライセンス所有者についての公開鍵証明書を有する。しかし、アプリケーション３０２が、所与のユーザに対するライセンスを生成したいことがあるが、アプリケーション３０２は、そのユーザについての公開鍵証明書へのアクセスを有さない可能性がある。そのような状況では、アプリケーション３０２は、ライセンス要求内のユーザの識別を指定することができ、その結果、ライセンス発行エンティティは、ディレクトリサービス内のルックアップを実行し、適切なユーザの公開鍵証明書を返す登録済み証明書プラグインコンポーネントを起動することができる。

【００６４】
ステップ６０８で、公開鍵証明書がライセンス要求内に含まれていないと発行エンティティが判定した場合、発行エンティティは指定の識別を使用して、適切な公開鍵証明書を求めてディレクトリサービスまたはデータベース内のルックアップを実行する。ステップ６１０で、証明書がディレクトリ内にあると発行エンティティが判定した場合、ステップ６１２で証明書を取り出す。好ましい実施形態では、証明書プラグインを使用して、ディレクトリアクセスプロトコルによってディレクトリサービスから公開鍵証明書を取り出す。所与の潜在的なライセンス所有者について、要求内またはディレクトリ内で証明書を見つけることができなかった場合、ライセンスサーバはその潜在的なライセンス所有者についてライセンスを生成せず、ステップ６１４でエラーを要求側エンティティに返す。

【００６５】
ライセンス発行エンティティが少なくとも１つの潜在的なライセンス所有者についての公開鍵証明書を有すると仮定すると、ステップ６１６で、発行エンティティは、ライセンス所有者証明書の信頼性を妥当性検査する。好ましくは、発行エンティティは、１組のトラステッド証明書発行者証明書で構成され、ライセンス所有者の証明書の発行者がトラステッド発行者のリスト中にあるかどうかを判定する。ステップ６１６で、ライセンス所有者の証明書の発行者がトラステッド発行者のリスト中にないと発行エンティティが判定した場合、そのライセンス所有者について要求は失敗し、ステップ６１４でエラーを生成する。したがって、その証明書がトラステッド発行者によって発行されていない潜在的なライセンス所有者は、ライセンスを受け取らない。

【００６６】
加えて、発行エンティティが、トラステッド発行者証明書から個々のライセンス所有者公開鍵証明書までの証明書の連鎖中のすべてのエンティティに対して、デジタルシグニチャの妥当性検査を実行することが好ましい。連鎖中のデジタルシグニチャを妥当性検査するプロセスは、周知のアルゴリズムである。所与の潜在的なライセンス所有者についての公開鍵証明書が妥当性検査されない場合、または連鎖中の証明書が妥当性検査されない場合

、潜在的なライセンス所有者は承認されず、したがってその潜在的なライセンス所有者に対してライセンスは発行されない。そうでない場合、ステップ６１８でライセンスを発行することができる。ステップ６２０で、このプロセスは、ライセンスが要求されたすべてのエンティティを処理するまで反復する。

【００６７】

図６Ｂに示すように、ライセンス発行エンティティは、ライセンス要求で受け取った署名済み権利ラベル３０８の妥当性検査を続行する。好ましい実施形態では、発行エンティティは、権利ラベルプラグインおよびバックエンドデータベースを使用して、発行エンティティによって署名されたあらゆる権利ラベルのマスタコピーをサーバ上に格納することができる。権利ラベルは、発行時に権利ラベル内に配置されたＧＵＩＤによって識別される。ライセンス時（ステップ６２２）に、発行エンティティは、ライセンス要求内の権利ラベル入力を解析し、そのＧＵＩＤを取り出す。次いで発行エンティティは、このＧＵＩＤを権利ラベルプラグインに渡し、権利ラベルプラグインはデータベースに対して照会を発行して、マスタ権利ラベルのコピーを取り出す。マスタ権利ラベルは、ライセンス要求で送られた権利ラベルのコピーよりも新しい可能性があり、下記のステップでの要求で使用する権利ラベルとなる。ＧＵＩＤに基づいてデータベース内に権利ラベルが見つからない場合、発行エンティティは、ステップ６２４でそのポリシーをチェックして、要求内の権利ラベルに基づいてライセンスを発行することが依然として許可されているかどうかを判定する。ポリシーがこのことを許可していない場合、ライセンス要求はステップ６２６で失敗し、ステップ６２８でＡＰＩ
３０６にエラーを返す。

【００６８】

ステップ６３０で、ライセンス発行エンティティは権利ラベル３０８を妥当性検査する。権利ラベル上のデジタルシグニチャを妥当性検査し、ライセンス発行エンティティが権利ラベルの発行者（権利ラベルに署名したエンティティ）でない場合、権利ラベルの発行者が別のトラステッドエンティティ（例えば、ライセンス発行エンティティが主な材料を共用することが可能なエンティティ）であるかどうかをライセンス発行エンティティは判定する。権利ラベルを妥当性検査しない場合、または権利ラベルがトラステッドエンティティによって発行されていない場合、ライセンス要求はステップ６２６で失敗し、ステップ６２８でＡＰＩ
３０６にエラーを返す。

【００６９】

すべての妥当性検査を行った後、ライセンス発行エンティティは、権利ラベル３０８を、承認された各ライセンス所有者についてのライセンスに変換する。ステップ６３２では、ライセンス発行エンティティは、各ライセンス所有者に対して発行すべきライセンスについてのそれぞれの権利記述を生成する。各ライセンス所有者について、発行エンティティは、そのライセンス所有者の公開鍵証明書で指定される識別を、権利ラベル中の権利記述で指定される識別に照らして評価する。権利記述は、あらゆる権利または権利のセットに、ライセンス中のその権利または権利のセットを行使することができる１組の識別を割り当てる。このライセンス所有者の識別が関連するあらゆる権利または権利のセットについて、その権利または権利のセットが、ライセンスについての新しいデータ構造にコピーされる。得られるデータ構造は、特定のライセンス所有者についてのライセンス中の権利記述である。このプロセスの一部として、ライセンス発行エンティティは、権利ラベルの権利記述内の権利または権利のセットのいずれかに関連する可能性のある任意の前提条件を評価する。例えば、権利は、指定の時間の後にライセンス発行エンティティがライセンスを発行することを制限する、その権利に関連する時間前提条件を有する可能性がある。この場合、発行エンティティは現在時間をチェックする必要があり、前提条件で指定された時間を過ぎている場合、発行エンティティは、ライセンス所有者の識別がその権利に関連する場合であっても、そのライセンス所有者にその権利を発行することができなくなる。

【００７０】

ステップ６３６では、発行エンティティは権利ラベル３０８から（ＰＵ－ＤＲＭ（ＤＥＳ１））および（ＤＥＳ１（ＣＫ））を取り、（ＰＲ－ＤＲＭ）を適用して（ＣＫ）を得る。次いで発行エンティティは、ライセンス所有者の公開鍵証明書である（ＰＵ－ＥＮＴＩＴＹ）を使用して（ＣＫ）を再暗号化し、（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））を得る。ステップ６３８では、発行エンティティは、生成した権利記述を（ＰＵ－ＥＮＴＩＴＹ（ＣＫ））と連結し、得られるデータ構造を（ＰＲ－ＤＲＭ）を使用してデジタルに署名する。この署名したデータ構造は、この特定のライセンス所有者についてのライセンスである。

【００７１】

ステップ６４０で、特定の要求について生成するライセンスが存在しないと発行エンティティが判定したとき、０個以上のライセンスを生成したことになる。ステップ６４２で、生成したライセンスを、そのライセンスに関連する証明書の連鎖（例えば、サーバ自体の公開鍵証明書、およびその証明書を発行した証明書など）と共に要求側エンティティに返す。

【００７２】

ライセンス応答の好ましい実施形態についてのＳＯＡＰプロトコルは下記の通りである。

【００７３】

```
〈soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"〉
 〈soap:Body〉
  〈AcquireLicenseResponse xmlns="http://xxxx.com/LicensingService"〉

   〈AcquireLicenseResult〉
    〈AcquireLicenseResponse〉
     〈CertificateChain〉
      〈String〉string〈/String〉
      〈String〉string〈/String〉
     〈/CertificateChain〉
    〈/AcquireLicenseResponse〉
    〈AcquireLicenseResponse〉
         ...
    〈/AcquireLicenseResponse〉
         ...
   〈/AcquireLicenseResult〉
  〈/AcquireLicenseResponse〉
 〈/soap:Body〉
〈/soap:Envelope〉
```

【００７４】

本発明によるシステムの好ましい実施形態では、複数のライセンス交付者鍵を使用することができる。このような実施形態では、権利ラベル３０８を介してライセンス内に暗号化

されるコンテンツ鍵（ＣＫ）は、実際には任意のデータでよい。特に有用な一変形形態は、権利記述内の異なる権利または異なる原理にそれぞれ関連する複数の別々の暗号化コンテンツ鍵（ＣＫ）を使用することである。例えば、アルバムについての各曲のデジタルバージョンを異なる鍵（ＣＫ）を用いてすべて暗号化することができる。これらの鍵（ＣＫ）は、同じ権利ラベル内に含まれることになるが、１つの原理は、曲のうち１つを再生する権利を有することができ（例えばその人は、自分のライセンスで１つの鍵だけを取得する権利を有することができる）、一方第２の原理は、すべての曲を再生する権利を有することができる（その人は、自分のライセンス内にすべての鍵を取得する権利を有することになる）。

【００７５】

好ましくは、本発明によるシステムにより、権利ラベル３０８内のライセンス所有者の名前グループまたは名前クラスにアプリケーション／ユーザを発行することが可能となる。このような実施形態では、ライセンス発行エンティティは、権利ラベルで指定される任意のグループ／クラスを評価して、現ライセンス所有者の識別がそのグループ／クラスのメンバであるかどうかを判定することになる。指定されるグループ／クラスのメンバであることが判明した場合、発行エンティティはグループ／クラスに関連する権利または権利のセットを、ライセンスに関して使用する権利記述データ構造に追加することができる。

【００７６】

本発明の好ましい実施形態では、ＤＲＭサーバ中の発行／ライセンスプロトコルインターフェースは、呼出し側のアプリケーションまたはユーザの認証および許可をサポートし、ＤＲＭサーバについての管理コンソールにより、インターフェースをライセンス交付し、かつ発行するためのアクセス制御リストをアドミニストレータが生成することが可能となる。これにより、ユーザ／アプリケーションが発行し、ライセンス交付し、またはその両方を行うことを許可されるポリシーをサーバの顧客が適用することが可能となる。

【００７７】

署名済み権利ラベル３０８の変更または再発行

本発明の一実施形態では、コンテンツのユーザがＳＲＬ　３０８を「再発行」するための十分な許可を付与されている場合、それを行うことができる。すなわち、可能なら、ユーザはＳＲＬ　３０８内の権利データを変更することができる。特に、権利データを変更する許可は、限定的かつ慎重に付与すべきである。特に、権利データを変更する権限を有するユーザは、関連するコンテンツに関して、実質的に広範な権利をユーザ自体に付与することができるからである。恐らく、そのようなユーザは、世界に対してコンテンツを公開し、それを転送する権利をユーザ自体に付与することさえすることができる。

【００７８】

この場合、変更する許可は、特定のユーザまたはユーザのクラスが実際に権利データおよび権利ラベル３０８を変更または「再発行」することができるという表示をＳＲＬ　３０８内の権利データ内に含めることによって示される。ＤＲＭサーバ３２０がライセンスを求める要求に関連するそのような許可と共にＳＲＬ３０８を受け取ったとき、ＤＲＭサーバ３２０は、ユーザについての要求されたライセンス内にユーザの公開鍵（すなわちＰＵ－ＥＮＴＩＴＹ）に従って暗号化された対称鍵（ＤＥＳ１）を含め、（ＰＵ－ＥＮＴＩＴＹ（ＤＥＳ１））を得る。

【００７９】

したがって、ＳＲＬ　３０８内の権利データを編集する目的で、ここで図７を参照すると、ユーザは、ライセンスから（ＰＵ－ＥＮＴＩＴＹ（ＤＥＳ１））を取り出し（ステップ７０１）、それに（ＰＲ－ＥＮＴＩＴＹ）を適用して（ＤＥＳ１）を得（ステップ７０３）、ＳＲＬ　３０８から（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を取り出して（ステップ７０５）、それに（ＤＥＳ１）を適用し、権利データを得る（ステップ７０７）。その後で、ユーザは、権利データを望みの通りに変更し（ステップ７０９）、変更した権利データを、図４に関連して説明した方式でＤＲＭサーバ３２０にサブミットし、署名済み権利ラベル３０８を得る（ステップ７１１）。もちろんこの場合、署名済み権利ラベル３０８

は実際には再発行されたＳＲＬ　３０８であり、したがってＳＲＬ　３０８を受け取った後（ステップ７１３）、ユーザは、関連するコンテンツに連結された元のＳＲＬ　３０８を除去し（ステップ７１５）、次いで再発行されたＳＲＬ　３０８をそのようなコンテンツに連結する（ステップ７１７）。

【００８０】

したがって、理解するであろうが、ＳＲＬ　３０８を再発行することにより、権利、条件、およびユーザを含むＳＲＬ　３０８内の権利データを、関連するコンテンツを変更することなくユーザが更新することが可能となる。具体的には、再発行により、関連するコンテンツを新しい（ＣＫ）で再暗号化する必要がない。さらに、特に元のＳＲＬ　３０８は新しいＳＲＬ　３０８にコピーすることのできる多くの項目を有するので、再発行により、スクラッチから新しいＳＲＬを生成する必要がない。

【００８１】

署名済み権利ラベル３０８の自己発行（Ｓｅｌｆ－Ｐｕｂｌｉｓｈｉｎｇ）

本発明の一実施形態では、要求側ユーザ自身でＳＲＬ　３０８に署名することができる。したがって、ユーザはＤＲＭサーバ３２０に接触して、関連するコンテンツについてのＳＲＬ　３０８を得る必要がない。その結果、自己発行はオフライン発行とも呼ぶことができる。このような実施形態では、ＤＲＭサーバ３２０に接触し、そのような自己発行ＳＲＬ　３０８に基づいてライセンスを要求するようにユーザに要求することができる。発行エンティティがそれ自体のライセンスを発行できるようにすることができることも理解されたい。

【００８２】

具体的には、ここで図８を参照すると、この実施形態では、ユーザがまず、公開鍵（ＰＵ－ＣＥＲＴ）と、（ＰＵ－ＥＮＴＩＴＹ（ＰＲ－ＣＥＲＴ））を得るようにユーザの公開鍵（ＰＵ－ＥＮＴＩＴＹ）に従って暗号化された対応する秘密鍵（ＰＲ－ＣＥＲＴ）とを含むＤＲＭ証明書８１０をＤＲＭサーバ３２０から受け取ることによって自己発行するように準備される。以下でより詳細に論じるように、証明書は、ＤＲＭサーバ３２０が検証することができるように、ＤＲＭサーバ３２０の秘密鍵（ＰＲ－ＤＲＭ）で署名すべきである。理解するであろうが、ＤＲＭ証明書８１０は、ユーザが自己発行することを許可する。やはり理解するであろうが、鍵の組（ＰＵ－ＣＥＲＴ、ＰＲ－ＣＥＲＴ）は、（ＰＵ－ＥＮＴＩＴＹ、ＰＲ－ＥＮＴＩＴＹ）と別のものであり、特に自己発行のために使用される。ＤＲＭ証明書８１０がユーザの公開鍵（ＰＵ－ＥＮＴＩＴＹ）だけを含み、かつＤＲＭサーバ３２０の秘密鍵（ＰＲ－ＤＲＭ）によって署名され、その結果そのようなＤＲＭサーバ３２０がＤＲＭ証明書８１０を検証することができる場合には、鍵の組（ＰＵ－ＣＥＲＴ、ＰＲ－ＣＥＲＴ）を不要にすることができることに留意されたい。

【００８３】

自己発行は、ＤＲＭサーバ３２０によって実行されるステップに関して、本質的にＤＲＭサーバ３２０の場所をユーザが取るという点で、図４に示す発行とは異なる。重要なことであるが、ユーザは、ＤＲＭ証明書８１０（すなわちＳ（ＰＲ－ＣＥＲＴ））から得た（ＰＲ－ＣＥＲＴ）を用いて、（ＰＵ－ＤＲＭ（ＤＥＳ１））および（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を含む、サブミットされた権利ラベルに署名し、署名済み権利ラベル（ＳＲＬ）３０８を得る。理解すべきことであるが、ユーザは、ＤＲＭ証明書８１０から（ＰＵ－ＥＮＴＩＴＹ（ＰＲ－ＣＥＲＴ））を得て、それに（ＰＲＥ－ＥＮＴＩＴＹ）に適用することにより、そのようなＤＲＭ証明書８１０から（ＰＲ－ＣＥＲＴ）を得る。しかし、特にユーザが（ＰＵ－ＤＲＭ（ＤＥＳ１））に適用するための（ＰＲ－ＤＲＭ）を有さないので、サブミットされた権利ラベル内の権利をＤＲＭサーバ３２０が実施できることをユーザは検証できないことに留意されたい。したがって、自己発行されたＳＲＬ　３０８に基づいてライセンスが要求されたときにＤＲＭサーバ３２０自体が検証を実行すべきである。

【００８４】

ユーザがＳＲＬ　３０８を自己発行した後、ユーザはそのような自己発行したＳＲＬ　３

０８と、ＳＲＬ　３０８を生成するのに使用したＤＲＭ証明書８１０をコンテンツに連結し、ＳＲＬ　３０８およびＤＲＭ証明書８１０を有するそのようなコンテンツが別のユーザに配布される。その後で、他のユーザが、図６Ａおよび６Ｂに示すのとほぼ同じ方式で、コンテンツについてのライセンスをＤＲＭサーバ３２０に要求してそれを得る。しかしこの場合、ライセンスを要求するユーザは、自己発行したＳＲＬ　３０８およびＤＲＭ証明書８１０を、どちらもコンテンツに連結されたものとしてＤＲＭサーバ３２０にサブミットする。次いでＤＲＭサーバ３２０は、対応する（ＰＵ－ＤＲＭ）に基づいてＤＲＭ証明書８１０内のＳ（ＰＲ－ＤＲＭ）を検証し、ＤＲＭ証明書８１０から（ＰＵ－ＣＥＲＴ）を得る。次いでＤＲＭサーバ３２０は、得られた（ＰＵ－ＣＥＲＴ）に基づいてＳＲＬ　３０８内のＳ（ＰＲ－ＣＥＲＴ）を検証し、前と同様に続行する。しかし、ＤＲＭサーバ３２０がＳＲＬ　３０８内の権利を実施できることをユーザは検証しなかったので、前述のように、ＤＲＭサーバ３２０自体がこの時に検証を実行すべきであることに留意されたい。

【００８５】

権利テンプレート

前述のように、ユーザまたはユーザのクラスを定義し、定義したユーザまたはユーザのクラスごとの権利を定義し、次いで使用条件を定義することにより、ほぼどのような様々な権利データ、またはほぼどのような種類の権利データも権利ラベル内に作成する自由がユーザに与えられる。しかし、重要なことであるが、複数の権利ラベルについての権利データを繰り返し定義することは、同じユーザまたはユーザのクラス、権利、および条件が様々なコンテンツについて繰り返し定義されるときは特に厄介であり、反復的であることがある。そのような状況は例えば、特定の定義されたユーザのチームと共用すべき様々なコンテンツをユーザが繰り返し発行する、企業またはオフィスの環境で生じる可能性がある。このような状況において、本発明の一実施形態では、権利ラベルを作成することに関連してユーザが繰り返し使用することができ、ユーザまたはユーザのクラスの定義済みのセット、定義されたユーザまたはユーザのクラスごとの定義済みの権利、および定義済みの使用条件を既に含んでいる権利テンプレートが作成される。

【００８６】

本発明の一実施形態では、ここで図９を参照すると、権利テンプレート９００が、権利ラベル内に存在することになるのとほぼ同じ権利データを有する。しかし、コンテンツが発行されるまで（ＤＥＳ１）は知られていないので、権利ラベルと同様に、そのような（ＤＥＳ１）に従って権利データを暗号化することができない。本発明の一実施形態では、非暗号化権利データを有する権利テンプレート９００が、図４のステップ４１６で権利データを（ＤＥＳ１）で暗号化して（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を生成する間にサブミットされる。もちろん、権利データは、そのように暗号化されるよりも前に、サブミットされる権利テンプレート９００から取り出される。

【００８７】

権利テンプレートを構築する時に、ＤＲＭサーバ３２０とその公開鍵（ＰＵ－ＤＲＭ）が知られていることもあり、知られていないこともある。さらに、知られている場合であっても、それぞれの（ＰＵ－ＤＲＭ）を有する複数のＤＲＭサーバ３２０が存在することもあり、存在しないこともある。それでも、権利テンプレートを構築する時にＤＲＭサーバ３２０とその公開鍵（ＰＵ－ＤＲＭ）が知られており、使用するＤＲＭサーバ３２０が１つだけであるか、または権利テンプレート９００に関連して１つのＤＲＭサーバ３２０だけを使用すべきである場合、そのような権利テンプレートは、権利ラベルの公開鍵（ＰＵ－ＤＲＭ）を含む、権利テンプレート９００から得られる権利ラベルに署名すべきＤＲＭサーバ上の情報も含むことができる。そのような（ＰＵ－ＤＲＭ）は、（ＤＥＳ１）を暗号化して（ＰＵ－ＤＲＭ（ＤＥＳ１））を得るときにＳＲＬ　３０８内に現れるが、コンテンツが発行されるまで（ＤＥＳ１）は知られておらず、したがって権利ラベルと同様に、権利テンプレート９００内の（ＰＵ－ＤＲＭ）はそのような（ＤＥＳ１）を暗号化できないことを再度理解されたい。次いで本発明の一実施形態では、非暗号化（ＰＵ－ＤＲＭ

）を有する権利テンプレート９００が、図４のステップ４１４で（ＤＥＳ１）を（ＰＵ－ＤＲＭ）で暗号化して（ＰＵ－ＤＲＭ（ＤＥＳ１））を生成する間にサブミットされる。もちろん、（ＰＵ－ＤＲＭ）は、サブミットされる権利テンプレート９００から、使用される前に取り出される。

【００８８】

さらに前述の場合には、権利テンプレート内に含めることができるＤＲＭサーバ上の他の情報も、ＤＲＭサーバをネットワーク上に配置するためのＵＲＬ、ＵＲＬが役に立たない場合のフォールバック情報などの参照情報を含むことができる。いずれにしても、権利テンプレートは、とりわけ権利テンプレート９００自体を記述する情報も含むことができる。権利テンプレート９００が、コンテンツに関連する権利ラベル内に現れる情報、および／または暗号化鍵（ＣＫ）および（ＤＥＳ１）などの、発行すべきコンテンツに関連する情報のためのスペースも提供できるが、権利テンプレートのインスタンス化が実際に権利ラベルに変換されない場合にはそのようなスペースは不要であることに留意されたい。

【００８９】

これまでのところで開示した権利テンプレート９００は主に、ユーザの便宜のためのものであるが、ある状況では、権利ラベル内の権利データを定義する無制限の自由をユーザが有するべきではなく、作成することができる権利ラベルの範囲またはタイプを限定するために権利テンプレート９００を使用できることも理解されたい。例えば、特に企業またはオフィスの環境では、特定のユーザは常に特定のクラスのユーザに対するコンテンツだけを発行すべきであること、またはユーザが特定のクラスのユーザに対してコンテンツを決して発行すべきでないことをポリシーとして事前定義することができる。いずれにしても、本発明の一実施形態では、そのようなポリシーは１つまたは複数の権利テンプレート９００内の定義済み権利データとして実施され、コンテンツを発行するときにユーザがそのような権利テンプレートを使用して権利ラベルを作成することを制限することができる。特に、ユーザについての発行ポリシーを指定するのにユーザが利用できる権利テンプレートまたは権利テンプレートのグループは、本発明の精神および範囲から逸脱することなく、任意の特定のタイプの発行ポリシーを指定することができる。

【００９０】

制限されたユーザなどについて権利テンプレート９００を指定するために、ここで図１０を参照すると、アドミニストレータなどは実際には、定義済み権利データを定義し（ステップ１００１）、特定のＤＲＭサーバ３２０に関連する情報など、必要かつ適切な任意の他のデータを定義することにより（ステップ１００３）、権利テンプレート９００を構築する。重要なことであるが、制限されたユーザなどが使用するための権利テンプレートを実現するためには権利テンプレート９００を公式なものとしなければならない。すなわち、権利テンプレート９００は、制限されたユーザなどが利用することができる権利テンプレートとして認識可能でなければならない。したがって、本発明の一実施形態では、アドミニストレータなどによって構築された権利テンプレートは、ＤＲＭサーバ３２０によって署名するためにＤＲＭサーバ３２０にサブミットされ、そのような署名により、権利テンプレートが公式なものとされる（ステップ１００５）。

【００９１】

署名するＤＲＭサーバ３２０は、ＤＲＭサーバ３２０の情報が実際に権利テンプレート９００内に存在する場合、権利テンプレート９００内にその情報があるＤＲＭサーバ３２０であることに留意されたい。さらに、ＤＲＭサーバ３２０が権利テンプレート９００に署名することができるのは、必要なチェックを行うとき、または全くチェックを行わずに署名できるときだけであることにも留意されたい。最後に、ＤＲＭサーバからのテンプレートシグニチャＳ（ＰＲ－ＤＲＭ－Ｔ）（ただし、ＴはシグニチャがＯＲＴ　９００についてのものであることを表す）は、権利テンプレート９００内の定義済み権利データに少なくとも基づくが、本発明の精神および範囲から逸脱することなく、他の情報に基づくこともできることに留意されたい。以下で説明するように、シグニチャＳ（ＰＲ－ＤＲＭ－Ｔ）は権利ラベルに組み込まれ、それに関連して検証され、したがって、シグニチャが何に

基づくとしても、それを不変の形で権利ラベルに組み込むべきである。

【００９２】

ＤＲＭサーバ３２０が権利テンプレート９００に署名し、それをアドミニストレータなどに返すとき、アドミニストレータは、署名され、今や公式である権利テンプレート９００をＳ（ＰＲ－ＤＲＭ－Ｔ）と共に受け取り（ステップ１００７）、公式な権利テンプレート（ＯＲＴ）９００を、１人または複数のユーザが使用する目的でそのユーザに転送する（ステップ１００９）。したがって、ユーザがＯＲＴ　９００に基づいてコンテンツを発行する場合、ユーザはＯＲＴ　９００を検索し（ステップ１０１１）、コンテンツについての情報、適切な鍵情報、（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を得るために（ＤＥＳ１）によって暗号化されたＯＲＴ　９００からの権利データ、およびＯＲＴ　９００からのその他の任意の情報など必要な任意の情報を提供することにより、ＯＲＴ　９００に基づいて権利ラベルを構築する（ステップ１０１３）。重要なことであるが、ユーザはまた、権利ラベルと共に、ＯＲＴ　９００からのシグニチャＳ（ＰＲ－ＤＲＭ－Ｔ）も含むことができる。

【００９３】

その後で、前と同様に、ユーザは、権利ラベルを署名のためにＤＲＭサーバ３２０にサブミットする（ステップ１０１５）。しかしこの場合、ＤＲＭサーバ３２０は、権利ラベル内のＳ（ＰＲ－ＤＲＭ－Ｔ）が検証されない限り、サブミットされた権利ラベルに署名しない。すなわち、ＤＲＭサーバ３２０は、サブミットされる権利ラベルがＯＲＴ　９００からのシグニチャＳ（ＰＲ－ＤＲＭ－Ｔ）を含まない限り、そのようにサブミットされる権利ラベルに署名することを拒否することによって、ユーザがサブミットされる権利ラベルをＯＲＴ　９００に基づかせなければならないことを実施する。具体的には、ＤＲＭサーバ３２０は、そのようなシグニチャがどのような情報に基づくとしても、サブミットされる権利ラベルからそのようなＳ（ＰＲ－ＤＲＭ－Ｔ）を取り出し、次いで（ＰＵ－ＤＲＭ）に基づいてそのようなシグニチャを検証する。サブミットされる権利ラベル内の権利データが（ＤＥＳ１）に従って暗号化されることに留意されたい（すなわち（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））。したがって、図７に関連して上記で述べたように、サブミットされる権利ラベル内の権利データに基づいてシグニチャを検証することができるように、ＤＲＭサーバ３２０はまず（ＤＥＳ１）を取得し、それを用いて（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））を暗号解読しなければならない。

【００９４】

検証した後、前と同様に、ＤＲＭサーバ３２０は、Ｓ（ＰＲ－ＤＲＭ－Ｌ）を用いて、サブミットされる権利ラベルに署名し、ＳＲＬ　３０８を生成する（ただし、－Ｌは、シグニチャがＳＲＬ　３０８についてのものであることを表す）。この場合、Ｓ（ＰＲ－ＤＲＭ－Ｌ）はＳ（ＰＲ－ＤＲＭ－Ｔ）を置換することができ、またはそのようなＳ（ＰＲ－ＤＲＭ－Ｔ）に追加することもできる。追加する場合、Ｓ（ＰＲ－ＤＲＭ－Ｌ）は、部分的にＳ（ＰＲ－ＤＲＭ－Ｔ）に基づくことができる。（ＰＲ－ＤＲＭ）を使用してＳ（ＰＲ－ＤＲＭ－Ｔ）とＳ（ＰＲ－ＤＲＭ－Ｌ）を共に生成することができ、またはＳ（ＰＲ－ＤＲＭ－Ｔ）とＳ（ＰＲ－ＤＲＭ－Ｌ）それぞれについて相異なる（ＰＲ－ＤＲＭ）を使用できることに留意されたい。ＤＲＭサーバ３２０が権利ラベルに署名して、ＳＲＬ３０８をユーザに返すとき、ユーザはＳ（ＰＲ－ＤＲＭ－Ｌ）と共にＳＲＬ　３０８を受け取り（ステップ１０１７）、前と同様にそれを、発行されるコンテンツに連結することを続行する。

【００９５】

ＯＲＴ　９００のシグニチャＳ（ＰＲ－ＤＲＭ－Ｔ）が少なくとも部分的にＯＲＴ　９００内の定義済み権利データに基づく場合、（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ）内の）ＳＲＬ　３０８内に現れるそのような権利データを修正または変更することはできない。そうでない場合、Ｓ（ＰＲ－ＤＲＭ－Ｔ）は検証されない。それでも本発明の一実施形態では、ＯＲＴ　９００内の権利データは、ＯＲＴ　９００と共にやはり含まれる、規定された規則内で変化することができる。例えば、この規則は、権利データの２つの組の一方を

ＳＲＬ　３０８内に含めるように指定することができ、または１組の選択肢の中から選択することを可能にすることができる。理解するであろうが、この規則は、本発明の精神および範囲から逸脱することなく、任意の適切な構文で記述された特定のどのような規則でもよい。この場合、規則は、権利ラベルが作成されたときに、ユーザのための適切な規則インタプリタによって解釈される。権利データは変化することができるが、規則は同様には変化せず、したがって、ＯＲＴ　９００についてのテンプレートシグニチャＳ（ＰＲ－ＤＲＭ－Ｔ）は、少なくとも部分的に規則に基づき、権利データ自体には基づかない。その結果、ＯＲＴ　９００と共に含まれる規則もまた、ＳＲＬ　３０８と共に含めなければならない。

【００９６】

本発明の一実施形態では、ＯＲＴ　９００内の定義済み権利データは、一部は固定されて不変であり、一部は可変で、前述のように規則により導出される。この場合、ＯＲＴ　９００についてのテンプレートシグニチャＳ（ＰＲ－ＤＲＭ－Ｔ）は、少なくとも部分的に、規則の固定部分に基づき、権利データの可変部分についての規則に基づく。

【００９７】

理解するであろうが、ユーザが所有するＯＲＴ　９００は、旧式となり、または陳腐化する可能性がある。すなわち、ＯＲＴ　９００は、その中の権利データを通じて、旧式となり、関連がなくなり、または単にもはや適用できなくなったポリシーを反映する可能性がある。例えば、ＯＲＴ　９００の権利データ内の１人または複数のユーザまたはユーザのクラスが、もはやポリシー環境内に存在していない可能性があり、あるいはＯＲＴ　９００の権利データ内で指定される特定のユーザまたはユーザのクラスが、もはやポリシー環境内に同じ権利を有さない可能性がある。そのような場合、アドミニストレータが更新後のＯＲＴ　９００を発行した可能性があるが、ユーザは依然として、ＯＲＴ　９００の以前の陳腐化したバージョンを使用している可能性がある。

【００９８】

そのような状況において、本発明の一実施形態では、サブミットされた権利テンプレート９００に署名してＯＲＴ　９００を作成する際のＤＲＭサーバ３２０は、ＯＲＴ　９００のコピーを保持し、各ＯＲＴ　９００は、固有の識別印（ｉｄｅｎｔｉｆｙｉｎｇ　ｉｎｄｉｃｉａ）を有し、ＯＲＴ　９００に基づいて構築された各権利ラベルは、そのようなＯＲＴ　９００の識別印を含む。したがって、図１０に関連するような、サブミットされた権利ラベルを受け取る際、ＤＲＭサーバ３２０は、権利ラベル内のＯＲＴ　９００の識別印を見つけ、見つけた識別印に基づいて、そのようなＯＲＴ　９００の最新のコピーを検索し、サブミットされた権利ラベルから権利データを削除し、検索したＯＲＴ　９００からの権利データを挿入し、次いで、少なくとも部分的に、挿入した権利データに基づいて、権利ラベルに署名する。もちろん、ＤＲＭサーバはまた、（ＤＥＳ１（ｒｉｇｈｔｓｄａｔａ））の暗号解読および再暗号化を含む、プロセス中で必要でありかつ義務である、前述の必要な任意の暗号化／暗号解読ステップを実行する。ＤＲＭサーバがサブミットされた権利ラベル内に権利データを配置するように適合される場合、そのような権利ラベルと、そのような権利ラベルの構築元のＯＲＴ　９００は、必ずしも権利データを含まないことに留意されたい。その代わり、必要なのは、権利データがＤＲＭサーバ３２０に常駐することだけである。しかし、権利ラベルと、そのような権利ラベルの構築元のＯＲＴ　９００とに権利データを含めることは、ユーザにとっては有用である可能性があり、したがってある状況では有用である可能性がある。

【００９９】

ＤＲＭパイプライン用のプラグインアーキテクチャ

本発明による典型的なＤＲＭサーバ／サービスプラットフォームは、ライセンス交付、発行、登録、活動化、認証、フェデレーションなどの１つまたは複数の高レベルＤＲＭサービスを含むことができる。本発明によれば、これらの各サービスを提供するそれぞれのソフトウェアシステムを、どのような組合せでも個々にインストールすることができ、管理することができ、使用可能または使用不能にすることができ、認証または非認証にするこ

と等ができるようにモジュラ式に設計された「パイプライン」として提供することができる。スタートから、途中で様々な処理の段階を経て終了する方式で要求を処理するために、各ＤＲＭサービスをパイプラインと呼ぶことができる。

【０１００】

各パイプラインは協働して豊富なＤＲＭプラットフォームを提供し、それぞれ個々に、重要なＤＲＭサービスを提供する。加えて、ビジネスロジックをカプセル化するＤＲＭプラットフォームの特定のコンポーネント（これは、ＤＲＭサーバ／サービスを首尾よく実装するのに重要となる可能性がある）が、ＤＲＭスイート間で共用され、それは第３者によって「プラグ可能（ｐｌｕｇｇａｂｌｅ）」である。そのような実装により柔軟性がもたらされ、サービスソリューションを迅速に開発し、かつソフトウェアを顧客のＤＲＭのニーズに合わせる方法が提供される。

【０１０１】

好ましくは、サービスを書くのにＭｉｃｒｏｓｏｆｔ Ｉｎｔｅｒｎｅｔ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｒｖｅｒ（「ＩＩＳ」）およびＡＳＰ．ｎｅｔモデルを使用する。ＩＩＳは、企業イントラネットとインターネットのためのセキュリティを提供するように設計されている。加えて、ＩＩＳは、セキュア通信用のＳｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ（ＳＳＬ）プロトコル、Ｘ．５０９証明書を用いた認証、ＲＳＡ公開鍵暗号、および多数の追加のセキュリティ機能の実装を実現する。ＡＳＰ．ｎｅｔは、強力なウェブアプリケーション／サービスを迅速に開発することを可能にするプログラミングフレームワークである。ＡＳＰ．ｎｅｔは、Ｍｉｃｒｏｓｏｆｔ ．ＮＥＴプラットフォームの一部であり、任意のブラウザまたは装置をターゲットとすることができるウェブアプリケーションを構築し、配置し、実行する、容易でスケーラブルな方法を提供する。

【０１０２】

本発明の好ましい実施形態では、強く型付けされたＨＴＴＰ要求がＩＩＳ、ＡＳＰ．ｎｅｔ、および１つまたは複数のＤＲＭサービスを実行中のウェブサーバに送られる。次いでＨＴＴＰ要求は、ＩＩＳおよびＡＳＰ．ｎｅｔによって前処理され、適切なＤＲＭサービスに向けて送られる。要求がＤＲＭサービスコードに届いた後、要求は処理パイプラインのうちの１つに入る。各パイプラインは、サービスの入口点と、その入口点への要求を処理するコードとをそれ自体記述するＡＳＰ．ｎｅｔファイル（ＡＳＭＸファイル）によって最高レベルで定義される。各パイプラインについて、ＤＲＭサービスコードは入口点の後ろであり、ＡＳＭＸファイルと、その後ろのコードの組合せによってパイプラインが構成される。

【０１０３】

入口点の後ろのコードはモジュラであり、他のパイプラインとコードを共用することができる。モジュラは、１）データの必要な任意の正規化を実行し、共通のパイプライン要求スタートアップオペレーションを実行する、要求パラメータを前処理する要求に特有のスタートアップコード、２）要求の処理に特有の（かつパイプラインに特有の）アクションを実行するコード、３）共用内部コンポーネントを起動するコード（パイプライン間で共用され、ＤＲＭプラットフォームだけにアクセス可能である）および共用パブリックコンポーネント（パイプライン間で共用され、第３者によってプラグ可能である）、ならびに４）パイプラインによって生成された結果を取り、その要求に対して適切な応答を構築する要求完了コードを含むことができる。

【０１０４】

このパイプライン設計の結果として、任意の順列でＤＲＭサービスを容易に配置することができる。例えば、ライセンス交付サービスおよびフェデレーションサービスを特定のインストールでインストールすることができ、発行サーバおよび情報サービスを使用不能にすることができる。別の例では、インストールすることができるのはライセンス交付のみであり、または発行サービスを入口点ＡＳＭＸファイルに適用することによって発行サービスに対して厳格な認証要件を実施する発行サービスのみである。このようなパイプライン設計により、既存のＤＲＭサービスに影響を及ぼさずに既存のインフラストラクチャを

活用して、例えば登録サービスや署名／シグニチャ妥当性検査サービスなど、将来新しいサービスを効率的に導入することも可能となる。

【０１０５】

各パイプライン内では、いくつかのパイプラインステージが実行され、その一部は内部専用ＤＲＭコンポーネントであり、一部はパブリックなプラグ可能ＤＲＭコンポーネント（「プラグイン」）を起動する。このＤＲＭプラグイン設計の結果として、第３者が、１つの全ＤＲＭパイプラインプロセスを実行するカスタムコンポーネントを書き込み、またはそれを得ることができる。好ましくは、そのような第３者のプラグインをパイプラインフレームワークに統合する前に、そのような任意の第３者が承認された第３者であることを保証する目的で測定が行われる。．ＮＥＴフレームワークによって提供される標準のパブリックな技法を使用して、第３者プラグインが承認されていることを保証することができる。第３者プラグインは動的にインストールすることができる。例えばＤＲＭシステムの構成データ内で、このような第３者プラグインを識別し、実行時にロードすることができる。このような設計により、ＤＲＭシステムを使用し、管理することが容易になる。

【０１０６】

一般に、プラグインは、ストレージから権利ラベルを取り出し、構成データに基づいて配布点ＸＭＬノードを生成し、カスタム暗号化／暗号解読ハードウェアを使用して秘密鍵オペレーションを実行するなどの別個のタスクを実行する。本明細書ではある専用プラグインを「エクステンション」と呼ぶ。エクステンションは、要求を許可するとき、ライセンスが生成されたときなど、一般のイベントが発生したときに起動される。プラグインはパイプライン処理でよりアクティブであり、必須の必要なタスクをパイプラインで実行する。エクステンションはより受動的であり、イベントに応答し、場合によっては作業を実行し、場合によっては何も行わない。

【０１０７】

図１１に、本発明による汎用パイプライン１１００を示す。パイプライン１１００は、発行、ライセンス交付などのデジタル権利管理サービスを実行する処理フレームワークを提供するサービスプログラム１１０２を含む。パイプライン１１００は、複数のプラグインコンポーネント１１２０ａ、１１２０ｂを含む。各プラグインコンポーネント１１２０ａ、１１２０ｂは、デジタル権利管理サービスに関連するそれぞれのタスクを実行する。プラグインコンポーネントがデジタル権利管理パイプラインで実行することができるタスクのタイプが、本明細書全体で詳細に説明される。複数のプラグインコンポーネント１１２０ａ、１１２０ｂはそれぞれ、事前定義されたそれぞれの１組のインターフェース規則に従って処理フレームワーク１１０２に統合される。通常、これらのインターフェース規則はサービスプログラム処理フレームワークのプロバイダとプラグインのプロバイダとの間で交渉される（前述のように、これらは同じエンティティでも、そうでなくともよい）。パイプライン１１００はまた、１つまたは複数のエクステンション１１３０も含むことができる。

【０１０８】

パイプラインのある点１１４０では、サービスを実行する（例えば、要求を処理する）のに必要なすべてのタスクが完了している。その点１１４０の後、非同期コンポーネントを処理フレームワーク１１１０に統合することができる。主に、非同期コンポーネントは、サービスを実行するのに必要ではないタスクのために使用することができる。したがって、非同期コンポーネントは、パイプラインの処理中に実行する必要のないタスクに対してバンド外拡張モデル（ｏｕｔ　ｏｆ　ｂａｎｄ　ｅｘｔｅｎｓｉｂｉｌｉｔｙ　ｍｏｄｅｌ）を提供する。非同期コンポーネントは必要なサービスタスクが完了した後に処理されるので、非同期コンポーネントは要求の処理を妨げない。好ましくは、非同期コンポーネントは拒否権を有さない。任意の数の非同期コンポーネントを並列に処理することができる。

【０１０９】

このオープンなプラットフォームのために、測定を行ってデータおよびインターフェース

を保護することが好ましい。例えば、パイプラインの環境内で動作するプラグインが承認されていることを必要とすることができる。このことはいくつかの方式で実行することができる。例えば、サービスプログラムとそのプラグインコンポーネントの間の強い命名（ｓｔｒｏｎｇ　ｎａｍｉｎｇ）および証拠ベースのセキュリティ管理コード技法を使用して、コンポーネントを妥当性検査し、サービスプログラムがプラグインを承認すること、およびプラグインがサービスプログラムを承認することを確実にすることができる。さらに、サービスプログラムがプラグインに提供するデータ、およびサービスプログラムがプラグインから受諾するデータを注意深く制御することができる。例えば、好ましい実施形態では、プラグインがサービスプログラムのデータ構造にアクセスすることが拒絶される。むしろ、プラグイン内のデータ、およびプラグイン外のデータが複製される。

【０１１０】

図１２に、本発明による、発行パイプライン１２００の好ましい実施形態を示す。図示するように、発行パイプライン１２００は、例えば、要求を処理する処理フレームワークを提供して権利管理デジタルコンテンツを発行する発行要求プログラムなどのサービスプログラムを含むことができる。発行パイプライン１２００は、発行要求を処理することに関連するタスクをそれぞれ実行する複数のプラグインコンポーネントも含むことができる。複数のプラグインコンポーネントはそれぞれ、事前定義されたそれぞれの１組のインターフェース規則に従って処理フレームワークに統合される。次に、例示的な各プラグインコンポーネントを詳細に説明する。

【０１１１】

「認証」プラグイン１２２０ａを提供して、ライセンスを要求するエンティティの識別を判定することができる。したがって、認証プラグイン１３２０ａのプロバイダは、認証が必要かどうかを制御することができ、認証が必要である場合、プロバイダは、認証のタイプ、認証方式、匿名認証を許可するかどうか、および何らかの理由のために要求を認証することができない場合にレポートするエラーのタイプを制御することができる。

【０１１２】

「許可」プラグイン１２２０ｂを提供して、認証された識別を許可することができる。一般に、許可プラグインを使用して、要求側エンティティが要求したものが何であってもそれを要求側エンティティが行うことを許可されているかどうかを判定することができる。例えば、パイプラインを発行する際、許可プラグインを使用して、ＤＲＭシステムを使用して権利管理コンテンツを発行することを、認証された識別が許可されているかどうかを判定することができる。したがって、許可プラグインのプロバイダは、どのエンティティがどのアクションを要求することができるか、エンティティの何のリストを格納するか、そのようなリストをどのように、どこに格納するか、許可されたエンティティをどのようにリストに載せ、リストから除去するかを制御することができる。

【０１１３】

「権利ラベル格納」プラグイン１２２０ｃを使用して、本発明に従って生成したマスタ権利ラベルを格納することができる。上記で詳細に説明したように、マスタ権利ラベルは、ＧＵＩＤなどの識別子に関連付けることができる。ライセンス時に、サーバは、ＧＵＩＤに基づいて、ストレージからマスタ権利ラベルのコピーを取り出す。権利ラベル格納プラグイン１２２０ｃのプロバイダは、マスタ権利ラベルを格納すべき位置、および権利ラベルを格納するために使用する格納技法を定義することができる。

【０１１４】

「秘密鍵」プラグイン１２２０ｄを使用して、ルート秘密鍵を保護することができる。したがって、秘密鍵プラグイン１２２０ｄのプロバイダは、システムが使用する秘密鍵保護アルゴリズムを指定することができる。本発明によるＤＲＭシステムで使用するのに適したいくつかの秘密鍵保護アルゴリズムが、例えば、米国特許出願（整理番号ＭＳＦＴ－１３３４）に記載されている。

【０１１５】

完了点１２４０では、図１２に図示するように、発行要求処理が完了し、非同期コンポー

ネント１２５０がそれぞれのタスクを実行する。図示するように発行パイプライン１２００はまた、「プロパティバッグ」コンポーネント１２５０ａ、「ロギング」アプリケーション１２５０ｂ、および証明書エンジンプラグイン１２５０ｃも含むことができる。しかし、本発明による発行パイプラインは、任意の数のエクステンションまたは非同期コンポーネントを含む、任意の数のプラグインを含むことができることを理解されたい。

【０１１６】

「プロパティバッグ」１２５０ａは、実行時にプラグインが利用できる、要求コンテキスト情報を提示する資源である。したがってプロパティバッグのプロバイダは、何のデータをプロパティバッグに入れるか、何がプロパティバッグを使用できるようにされるか、どのような状況でプロパティバッグを利用できるかを制御することができる。

【０１１７】

「ロギング」アプリケーション１２５０ｂは、発行要求に関係するデータを保存するのに使用することができる。したがってロギングコンポーネントのプロバイダは、どのデータを保存するか、どこにデータを保存するか、どのフォーマットでデータを保存するかを制御することができる。

【０１１８】

「証明書エンジン」プラグイン１２５０ｃは、証明書（例えばライセンス証明書）を書き込む非同期プラグインである。証明書エンジンは、使用されている権利言語（例えばＸｒＭＬ）の文法を処理する方法を理解している。したがって証明書エンジンプラグインのプロバイダは、証明書のフォーマットおよびコンテンツ、使用されている権利言語などを制御することができる。

【０１１９】

図１３に、本発明によるライセンス交付パイプライン１３００の好ましい実施形態を示す。図示するように、ライセンス交付パイプライン１３００は、例えば、ライセンス要求を処理する処理フレームワークを提供するライセンス交付要求プログラムなどのサービスプログラムを含むことができる。ライセンス交付パイプライン１３００はまた、ライセンス要求の処理に関連するタスクをそれぞれ実行する複数のプラグインコンポーネントも含むことができる。複数のプラグインコンポーネントはそれぞれ、事前定義されたそれぞれの１組のインターフェース規則に従って、ライセンス交付要求プログラムの処理フレームワークに統合される。次に、例示的な各プラグインコンポーネントを詳細に説明する。本発明によるＤＲＭシステムの好ましい実施形態では、様々なパイプライン／ウェブサービス間でプラグインを共用することができ、ライセンス交付パイプラインに含めることができるプラグインのうちの多くは、前述の発行パイプラインに含まれるプラグインと同一でよいことに留意されたい。

【０１２０】

発行パイプラインに関連して上記で説明したような「認証」プラグイン１３２０ａを提供して、ライセンスを要求するエンティティの識別を決定することができる。

【０１２１】

発行パイプラインに関連して上記で説明したような「許可」プラグイン１３２０ｂを提供して、認証された識別を許可することができる。ライセンス交付パイプラインでは、許可プラグインを使用して、要求側エンティティがライセンスを要求することを許可されているかどうかを判定することができる。したがって、許可プラグインのプロバイダは、個人のアカウント識別がライセンス要求を直接作成することを許可されているかどうか、トラステッドサーバプロセスが、そのようなエンティティの代わりにライセンス要求を作成することができるかどうかなどを制御することができる。

【０１２２】

「グループ拡張」プラグイン１３２０ｃを使用して、グループ識別子から個々のユーザリストを取り出すことができる。一般に、事前定義グループ内のメンバシップは、時間の経過につれて変化することが予想される。したがって、本発明によるＤＲＭシステムは、グループの各メンバについてのユーザリストを含むグループリポジトリを含むことができる

。各グループは、関連するグループ識別子を有する。したがって、デジタル権利管理サービス（例えば発行）の処理中にグループｉｄをいつ受け取ったとしても、グループ拡張プラグインを呼び出して、受け取ったグループｉｄに対応する現グループリストを取り出すことができる。

【０１２３】

「権利ラベル検索」プラグイン１３２０ｄを使用して、受け取った識別子に対応する権利ラベルを取り出すことができる。上記で詳細に説明したように、サーバは、ライセンス要求内の権利ラベル入力を解析し、そのＧＵＩＤを取り出す。次いでサーバは、このＧＵＩＤを権利ラベル検索プラグイン１３２０ｄに渡し、権利ラベル検索プラグイン１３２０ｄは、データベースに対して照会を発行してマスタ権利ラベルのコピーを取り出す。

【０１２４】

「証明書検索」プラグインを使用して、証明書が格納されているサーバからそのような証明書を取り出すことができる。例えば、要求側エンティティはいつかの潜在的なライセンス所有者の事前ライセンス交付を要求している可能性があるが、要求側エンティティは、潜在的なライセンス所有者についての証明書を有さない。しかしライセンスを発行するには証明書が必要であり、したがって証明書検索プラグインを使用して、証明書が格納されているサーバから証明書を取り出すことができる。

【０１２５】

「ストレージ」プラグインを使用して、どのようなストレージアクセスが提供されてもそれをカプセル化することができる。したがって、ストレージプラグインのプロバイダは、データを格納することができるストア、またはデータを取り出すことができるストア、ならびにパイプラインがデータストアを通信するのに必要な「言語」を指定することができる。例えば、パイプラインは、ＳＱＬを介して特定のデータストアにアクセスすることが必要である可能性がある。

【０１２６】

参照ＵＲＬの超流通（ｓｕｐｅｒｄｉｓｔｒｉｂｕｔｉｏｎ）に関連して、「配布点」プラグイン１３２０ｇを使用することができる。配布点プラグイン１３２０ｇは、格納位置から参照ＵＲＬを読み取り、要求されたときにそれをＸｒＭＬ文書に組み込む。このプラグインからの出力は、クライアントが接触してライセンス交付、権利獲得などのＤＲＭオペレーションを形成することができる参照ＵＲＬを定義する明確な１つのＸＭＬである。

【０１２７】

発行パイプラインに関連して上記で説明したような「秘密鍵」プラグイン１３２０ｈを使用して、ルート秘密鍵を保護することができる。

【０１２８】

完了点１３４０では、図１３に示すように、ライセンス要求処理が完了し、非同期プラグイン１３５０が、それぞれのタスクの実行を開始する。図示するように、ライセンス交付パイプライン１３００はまた、発行パイプラインに関連して上記で説明したような、「プロパティバッグ」コンポーネント１３５０ａ、「ロギング」アプリケーション１３５０ｂ、および証明書エンジンプラグイン１３５０ｃも含むことができる。しかし、本発明によるライセンス交付パイプラインは、任意の数のエクステンションまたは非同期コンポーネントを含む、任意の数のプラグインを含むことができることを理解されたい。

【０１２９】

図１４に、デジタル権利管理システム用のセキュアサーバプラグインアーキテクチャを提供するための、本発明による方法１４００の好ましい実施形態の流れ図を与える。ステップ１４０２では、システムプロバイダが、発行、ライセンス交付などのデジタル権利管理サービスを実行するための処理フレームワークを提供するサービスを提供する。好ましい実施形態では、サービスプログラムは、関連するＤＲＭサービスを実行するためのコードを含む。

【０１３０】

ステップ１４０４では、システムプロバイダが、デジタル権利管理サービスに関連するタ

スクを実行するプラグインコンポーネントにそれぞれ関連する、複数のＤＲＭプラグインオプションを提供する。次いでインストーラ、購入者、システムアドミニストレータ、またはシステムの他のユーザは、そのインストールについてのそのパイプラインに対して消費者が望む特定の機能を提供するプラグインを選択するために、複数のプラグインオプションの中から選択することができる。

【０１３１】

ステップ１４０６では、システムプロバイダがプラグイン選択を受け取り、ステップ１４０８で、選択したプラグインオプションに対応するプラグインコンポーネントを処理フレームワークに統合する。したがって、本発明によるＤＲＭシステムのユーザは、ユーザのニーズまたは要望にシステムを合わせることができ、プラグインを変更することにより、経済的に、容易に、かつ効率的にシステムを更新することができる。

【０１３２】

結論

本発明に関連して実行されるプロセスを達成するのに必要なプログラミングは、比較的単純であり、関連するプログラミング業界の人々には明らかであろう。したがって、そのようなプログラミングは本明細書に添付されない。さらに、本発明を達成するのに、本発明の精神および範囲から逸脱することなく、任意の特定のプログラミングを使用することができる。

【０１３３】

したがって、デジタル権利管理システム用のセキュアサーバプラグインアーキテクチャを説明した。本発明の好ましい実施形態に多数の変更および修正を行えること、および本発明の精神から逸脱することなく、そのような変更および修正を行えることを当業者は理解されよう。例えば、パイプラインを発行し、ライセンス交付することに関連して本発明を詳細に説明したが、登録、活動化、認証、フェデレーションなどの他のデジタル権利管理サービスを実行する他のデジタル権利管理パイプラインで本発明を使用できることを理解されたい。したがって、頭記の特許請求の範囲は、本発明の精神および範囲内にある、すべてのそのような同等な変形形態を包含するものとする。

【０１３４】

付録１

サンプル権利データ

```
〈?xml version="1.0" ?〉
〈XrML version="1.2"〉
  〈BODY type="Rights Template"〉
    〈DESCRIPTOR〉
      〈OBJECT〉
        〈ID type="GUID"〉c43...〈/ID〉
        〈NAME〉$$411$411name$411desc〈/NAME〉
      〈/OBJECT〉
    〈/DESCRIPTOR〉
    〈WORK〉
     〈OBJECT〉
      〈ID /〉
     〈/OBJECT〉
     〈RIGHTSGROUP name="MAIN RIGHTS"〉
       〈RIGHTSLIST〉
         〈VIEW〉
           〈CONDITIONLIST〉
             〈ACCESS〉
              〈PRINCIPAL〉
                 〈OBJECT〉
                  〈ID /〉
                  〈NAME〉test@company.com〈/NAME〉
                 〈/OBJECT〉
              〈/PRINCIPAL〉
             〈/ACCESS〉
           〈/CONDITIONLIST〉
         〈/VIEW〉
```

```
        〈RIGHT name="generic"〉
          〈CONDITIONLIST〉
            〈ACCESS〉
              〈PRINCIPAL〉
                〈OBJECT〉
                  〈ID /〉
                  〈NAME〉test@company.com〈/NAME〉
                〈/OBJECT〉
              〈/PRINCIPAL〉
            〈/ACCESS〉
          〈/CONDITIONLIST〉
        〈/RIGHT〉
      〈/RIGHTSLIST〉
    〈/RIGHTSGROUP〉
  〈/WORK〉
〈/BODY〉
〈SIGNATURE〉
  〈ALGORITHM〉RSA PKCS#1-V1.5〈/ALGORITHM〉
  〈DIGEST〉
    〈ALGORITHM〉SHA1〈/ALGORITHM〉
    〈PARAMETER name="codingtype"〉
      〈VALUE encoding="string"〉surface-coding〈/VALUE〉
    〈/PARAMETER〉
    〈VALUE encoding="base64" size="160"〉MwI...=〈/VALUE〉
  〈/DIGEST〉
  〈VALUE encoding="base64" size="1024"〉Msi...=〈/VALUE〉
〈/SIGNATURE〉
〈/XrML〉
```

【０１３５】

付録２

サンプル署名権利ラベル（ＳＲＬ）３０８

```
〈?xml version="1.0" ?〉
〈XrML version=" 1.2"〉
  〈BODY type="Rights Label" version="3.0"〉
    〈ISSUEDTIME〉2002-01-01_12:00:00〈/ISSUEDTIME〉
    〈DESCRIPTOR〉
       〈OBJECT〉
        〈ID /〉
        〈NAME〉$$409$...〈/NAME〉
       〈/OBJECT〉
    〈/DESCRIPTOR〉
    〈ISSUER〉
      〈OBJECT type="DRM-Server"〉
        〈ID type="GUID"〉{d81... }〈/ID〉
        〈NAME〉Test DRM Server〈/NAME〉
        〈ADDRESS type="URL"〉http://licensing.dev.com〈/ADDRESS〉
    〈/OBJECT〉
    〈PUBLICKEY〉
                  〈ALGORITHM〉RSA〈/ALGORITHM〉
      〈PARAMETER name="public-exponent"〉
        〈VALUE encoding="integer32"〉65537〈/VALUE〉
      〈/PARAMETER〉
      〈PARAMETER name="modulus"〉
        〈VALUE encoding="base64" size="1024"〉Nc0...=〈/VALUE〉
      〈/PARAMETER〉
    〈/PUBLICKEY〉
    〈ENABLINGBITS type="sealed-key"〉
      〈VALUE encoding="base64" size="1024"〉tFg...=〈/VALUE〉
```

```
    〈/ENABLINGBITS〉
    〈SECURITYLEVEL name="Server-Version" value="2.0" /〉
    〈SECURITYLEVEL name="Server-SKU" value="22222-3333" /〉
  〈/ISSUER〉
  〈DISTRIBUTIONPOINT〉
    〈OBJECT type="LICENSE ACQUISITION URL"〉
      〈ID type="GUID"〉{0F4... }〈/ID〉
      〈NAME〉DRM Server Cluster〈/NAME〉
      〈ADDRESS type="URL"〉http://localhost/Licensing〈/ADDRESS〉
    〈/OBJECT〉
    〈/DISTRIBUTIONPOINT〉
    〈WORK〉
      〈OBJECT type="TEST-FORMAT"〉
        〈ID type="MYID"〉FDB-1〈/ID〉
      〈/OBJECT〉
    〈METADATA〉
      〈SKU type="PIDTYPE"〉P1D〈/SKU〉
    〈/METADATA〉
    〈PRECONDITIONLIST〉
      〈TIME /〉
    〈/PRECONDITIONLIST〉
  〈/WORK〉
  〈AUTHDATA name="Encrypted Rights data"〉PAB... 〈/AUTHDATA〉
〈/BODY〉
〈SIGNATURE〉
  〈ALGORITHM〉RSA PKCS#1-V1.5〈/ALGORITHM〉
  〈DIGEST〉
    〈ALGORITHM〉SHA1〈/ALGORITHM〉
    〈PARAMETER name="codingtype"〉
```

```
      〈VALUE encoding="string"〉surface-coding〈/VALUE〉
    〈/PARAMETER〉
    〈VALUE encoding="base64" size="160"〉Prc...=〈/VALUE〉
  〈/DIGEST〉
    〈VALUE encoding="base64" size="1024"〉EHd...=〈/VALUE〉
  〈/SIGNATURE〉
〈/XrML〉
```

【図面の簡単な説明】

【図１】本発明を実施することができる例示的な非限定的コンピューティング環境を表すブロック図である。

【図２】本発明を実施することができる様々なコンピュータ装置を有する例示的ネットワーク環境を表すブロック図である。

【図３】デジタルコンテンツを発行するための、本発明によるシステムおよび方法の好ましい実施形態の機能ブロック図である。

【図４】権利管理デジタルコンテンツを発行するための、本発明による方法の好ましい実施形態の流れ図である。

【図４Ａ】図４の方法によって生成される署名済み権利ラベルの構造を示すブロック図である。

【図５】権利管理デジタルコンテンツにライセンス交付するための、本発明によるシステムおよび方法の好ましい実施形態の機能ブロック図である。

【図６Ａ】権利管理デジタルコンテンツにライセンス交付するための、本発明による方法の好ましい実施形態の流れ図である。

【図６Ｂ】権利管理デジタルコンテンツにライセンス交付するための、本発明による方法の好ましい実施形態の流れ図である。

【図７】本発明の一実施形態に従って権利ラベルを再発行する際に実行される主なステップを示す流れ図である。

【図８】本発明の一実施形態に従ってユーザがオフライン発行を実行することを可能にする、ＤＲＭサーバによってユーザに発行される証明書を示すブロック図である。

【図９】本発明の一実施形態に従って権利ラベルに組み込むべき情報を指定する権利テンプレートを示すブロック図である。

【図１０】本発明の一実施形態に従って、図９の権利テンプレートを作成し、権利テンプレートに基づいて図４Ａの署名済み権利ラベルを作成する際に実行される主なステップを示す流れ図である。

【図１１】本発明による汎用パイプラインアーキテクチャを示す図である。

【図１２】本発明による、パイプラインを発行する好ましい実施形態を示す図である。

【図１３】本発明による、パイプラインにライセンス交付する好ましい実施形態を示す図である。

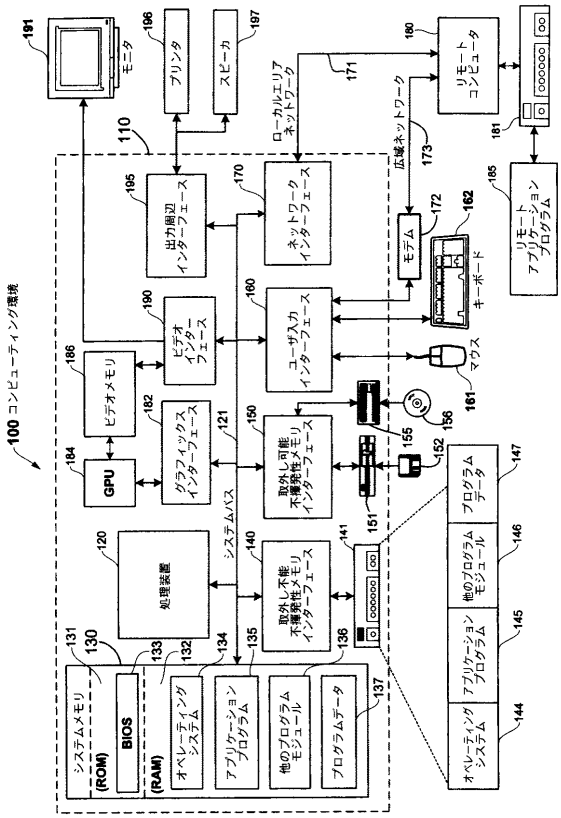
【図１４】デジタル権利管理システム用のセキュアサーバプラグインアーキテクチャを提供する、本発明による方法の好ましい実施形態の流れ図である。

【符号の説明】

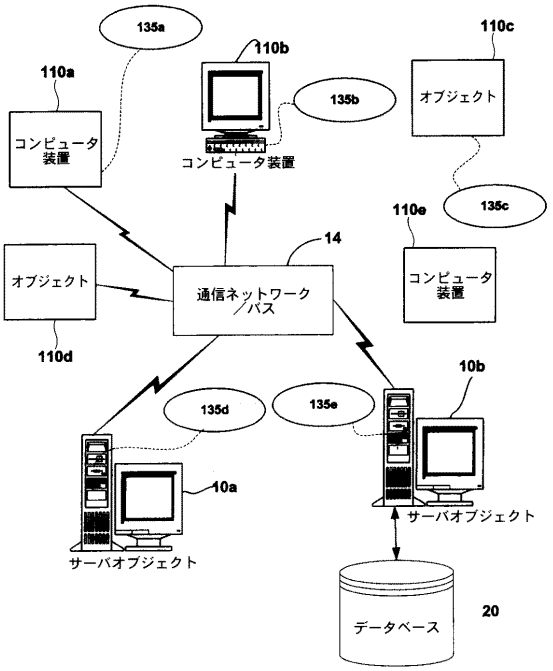
１０ａ、１０ｂ　コンピューティングオブジェクト
１４　通信ネットワーク／バス
２０　データベース
１００　コンピューティングシステム環境
１１０　コンピュータ

１１０ａ、１１０ｂ　コンピューティングオブジェクト／装置
１１１　他の装置
１２０　処理装置
１２１　システムバス
１３０　システムメモリ
１３１　読取り専用メモリ（ＲＯＭ）
１３２　ランダムアクセスメモリ（ＲＡＭ）
１３３　基本入出力システム（ＢＩＯＳ）
１３４、１４４　オペレーティングシステム
１３５、１４５　アプリケーションプログラム
１３６、１４６　他のプログラムモジュール
１３７、１４７　プログラムデータ
１４０、１５０　インターフェース
１４１　ハードディスクドライブ
１５１　磁気ディスクドライブ
１５２　取外し可能不揮発性磁気ディスク
１５５　光ディスクドライブ
１６０　ユーザ入力インターフェース
１６１　ポインティングデバイス
１６２　キーボード
１７０　ネットワークインターフェース／アダプタ
１７１　ローカルエリアネットワーク（ＬＡＮ）
１７２　モデム
１７３　広域ネットワーク（ＷＡＮ）
１８０　リモートコンピュータ
１８２　グラフィックスインターフェース
１８４　グラフィックス処理装置（ＧＰＵ）
１８５　リモートアプリケーションプログラム
１８６　ビデオメモリ
１９０　ビデオインターフェース
１９１　モニタ
１９５　出力周辺インターフェース
１９６　プリンタ
１９７　スピーカ
３０２　コンテンツ準備アプリケーション
３０４　暗号化デジタルコンテンツファイル
３０６　デジタル権利管理（ＤＲＭ）アプリケーションプログラムインターフェース（ＡＰＩ）
３０８　署名済み権利ラベル（ＳＲＬ）
３１０　権利管理コンテンツファイル
３２０　ＤＲＭサーバ
３３０　通信ネットワーク

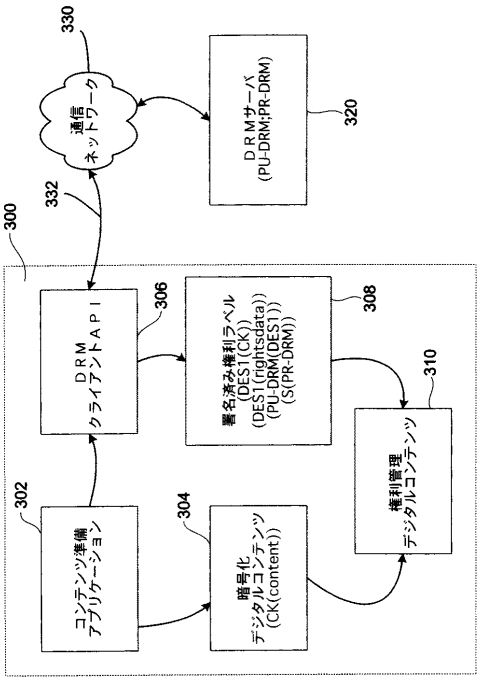
【図１】


100 コンピューティング環境
110
191 モニタ
196 プリンタ
197 スピーカ
171 ローカルエリアネットワーク
173 広域ネットワーク
180 リモートコンピュータ
181
185 リモートアプリケーションプログラム
195 出力周辺インターフェース
170 ネットワークインターフェース
172 モデム
162 キーボード
190 ビデオインターフェース
160 ユーザ入力インターフェース
161 マウス
186 ビデオメモリ
182 グラフィックスインターフェース
121 システムバス
150 取外し可能不揮発性メモリインターフェース
156
155
152
151
147 プログラムデータ
146 他のプログラムモジュール
145 アプリケーションプログラム
144 オペレーティングシステム
184 GPU
120 処理装置
140 取外し不能不揮発性メモリインターフェース
141
136
137 プログラムデータ
135 他のプログラムモジュール
134 アプリケーションプログラム
133 オペレーティングシステム
132 (RAM)
131 システムメモリ
130 (ROM)
BIOS

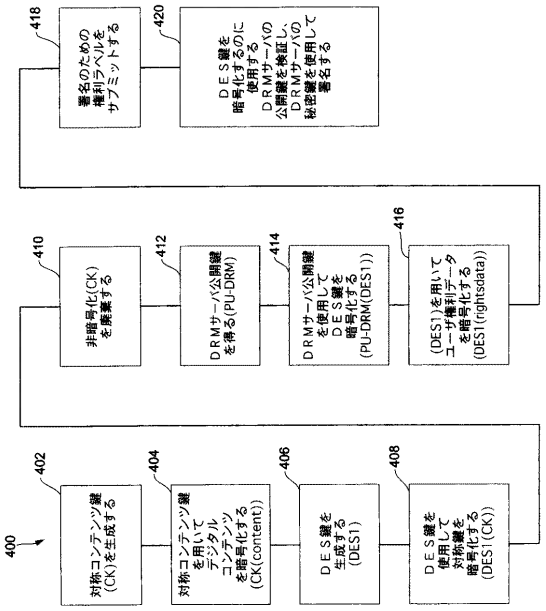
【図２】


135a
110a
コンピュータ装置
110b
コンピュータ装置
135b
110c
オブジェクト
135c
110e
コンピュータ装置
14
通信ネットワーク/パス
オブジェクト
110d
135d
135e
10b
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

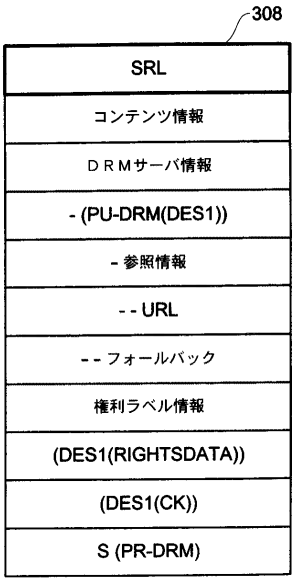
【図３】


330
通信ネットワーク
DRMサーバ (PU-DRM;PR-DRM)
320
332
300
DRM クライアントAPI
306
署名済み権利ラベル (DES1(CK)) (DES1(rightsdata)) (PU-DRM(DES1)) (S(PR-DRM))
308
310
権利管理デジタルコンテンツ
302
コンテンツ準備アプリケーション
304
暗号化デジタルコンテンツ (CK(content))

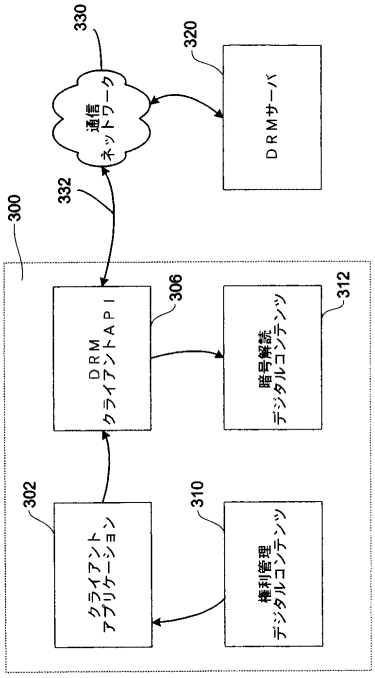
【図４】


400
402 対称コンテンツ鍵(CK)を生成する
404 対称コンテンツ鍵を用いてデジタルコンテンツを暗号化する (CK(content))
406 DES鍵を生成する (DES1)
408 DES鍵を使用して対称鍵を暗号化する (DES1(CK))
410 非暗号化(CK)を準備する
412 DRMサーバ公開鍵を得る(PU-DRM)
414 DRMサーバ公開鍵を使用してDES鍵を暗号化する (PU-DRM(DES1))
416 (DES1)を用いてユーザ権利データを暗号化する (DES1(rightsdata))
418 署名のための権利ラベルをサブミットする
420 DES鍵を暗号化するのに使用するDRMサーバの公開鍵を検証し、DRMサーバの秘密鍵を使用して署名する

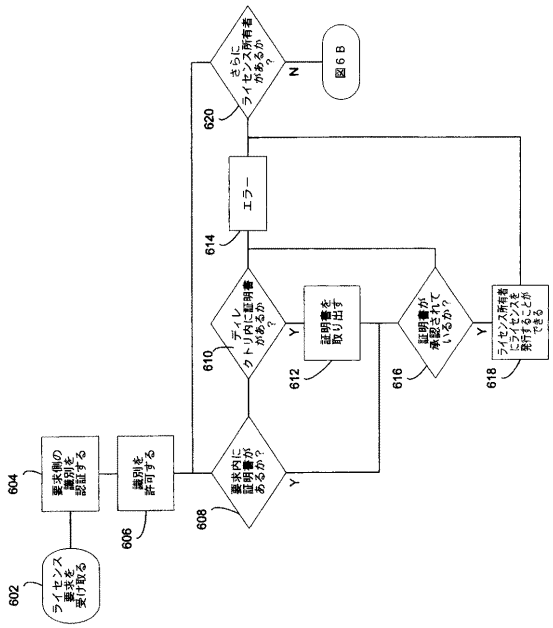
【図４Ａ】



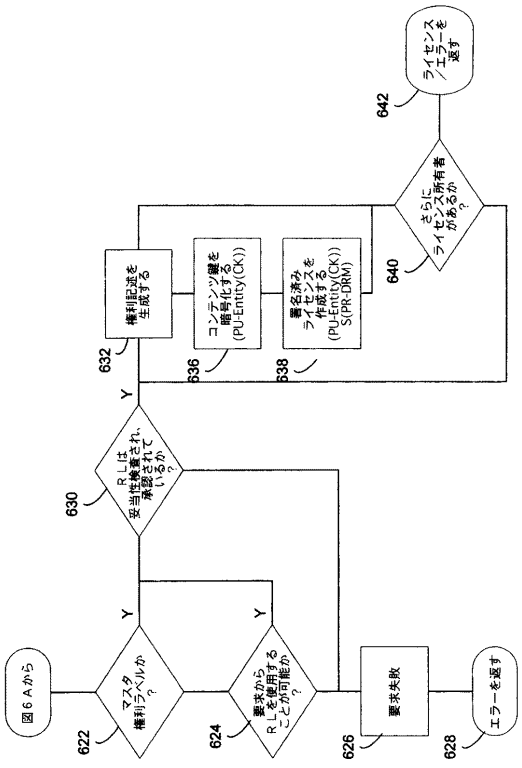
【図５】



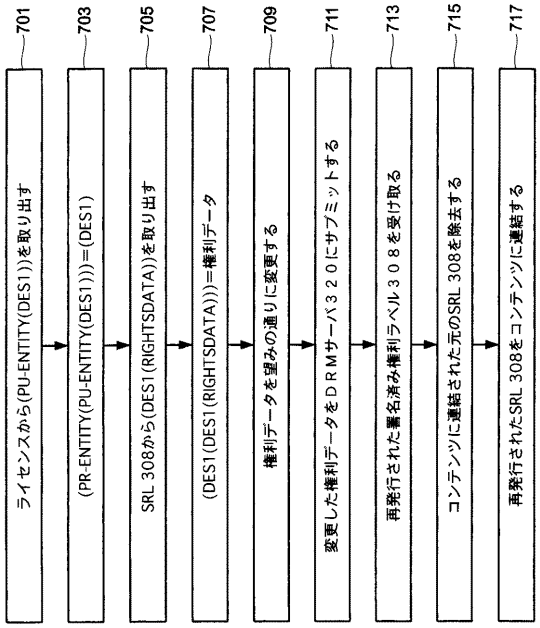
【図６Ａ】



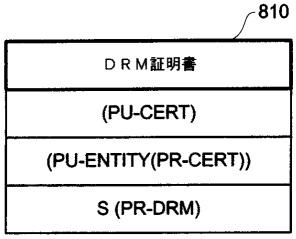
【図６Ｂ】



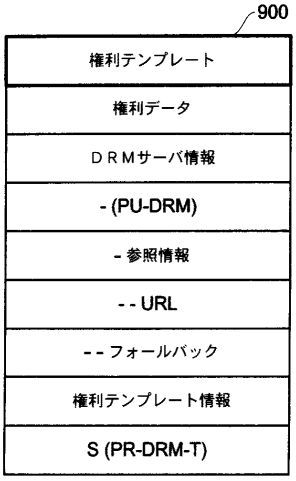
【図７】



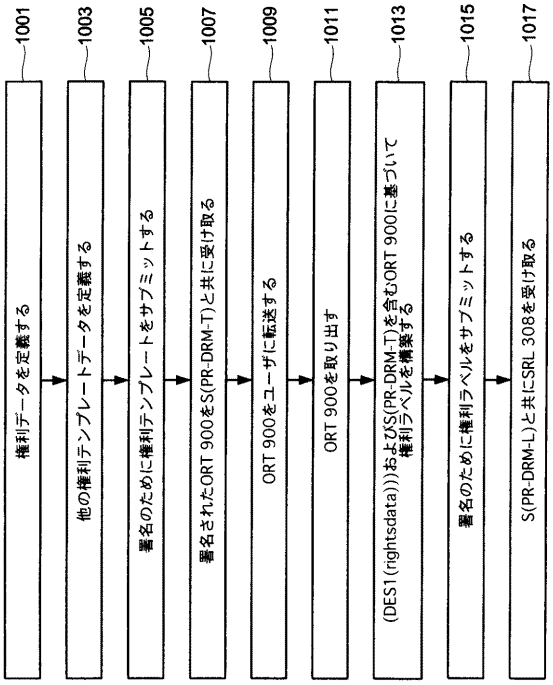
【図８】



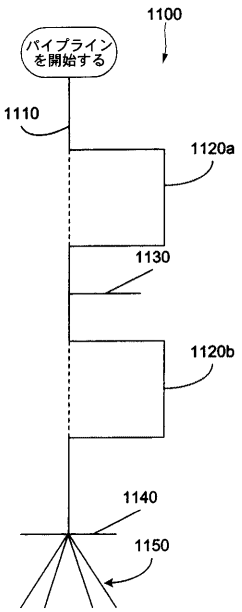
【図９】



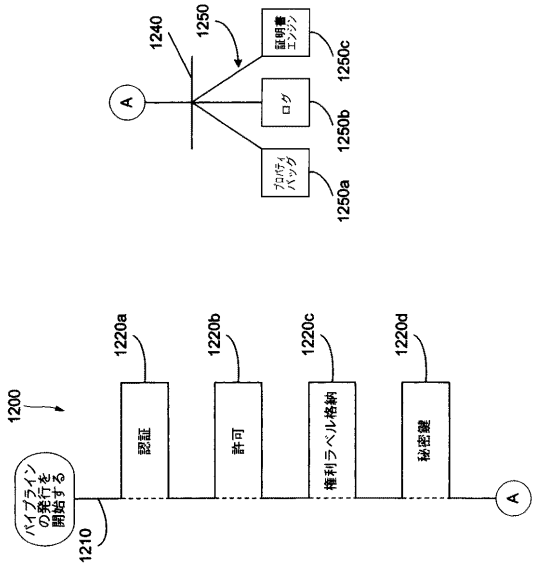
【図１０】



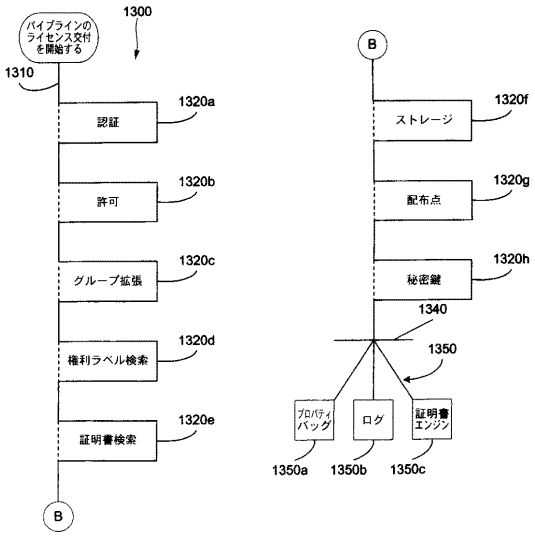
【図１１】



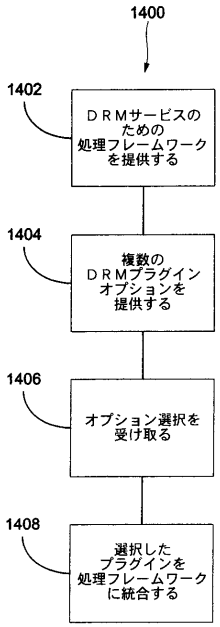
【図１２】


1240
1250
証明書エンジン
ログ
プロパティバッグ
1250c
1250b
1250a
A
1200
1220a
1220b
1220c
1220d
認証
許可
権利ラベル格納
秘密鍵
パイプラインの発行を開始する
1210
A

【図１３】


パイプラインのライセンス交付を開始する
1300
1310
認証
1320a
許可
1320b
グループ拡張
1320c
権利ラベル検索
1320d
証明書検索
1320e
B
B
ストレージ
1320f
配布点
1320g
秘密鍵
1320h
1340
1350
プロパティバッグ
ログ
証明書エンジン
1350a
1350b
1350c

【図１４】


1400
1402
DRMサービスのための処理フレームワークを提供する
1404
複数のDRMプラグインオプションを提供する
1406
オプション選択を受け取る
1408
選択したプラグインを処理フレームワークに統合する

フロントページの続き

(72)発明者 ピーター デビッド ワックスマン
アメリカ合衆国 ９８００４ ワシントン州 ベルビュー ノースイースト ２８ プレイス １０００８
(72)発明者 ビナイ クリシュナスワミー
アメリカ合衆国 ９８０７２ ワシントン州 ウッディンビル ノースイースト １４２ プレイス ２３３１９
(72)発明者 チャンドラモウリ ベンカテシュ
アメリカ合衆国 ９８０７４ ワシントン州 サマミッシュ ２１３ プレイス サウスイースト ４１４
(72)発明者 アチッラ ナリン
アメリカ合衆国 ９８０１１ ワシントン州 ボセル ノースイースト １４４ コート ８７４１
(72)発明者 グレゴリー コスタル
アメリカ合衆国 ９８０３３ ワシントン州 カークランド １０ アベニュー ４２５
(72)発明者 プラシャント マリク
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド １５６ アベニュー ノースイースト ４８５０ ナンバー３１３
(72)発明者 ウラジミール ヤーモレンコ
アメリカ合衆国 ９８１０９ ワシントン州 ドボル ノースイースト １５５ プレイス ２７４３０
(72)発明者 フランク バイラム
アメリカ合衆国 ９８１０１ ワシントン州 シアトル ウエスタン アベニュー １２００ ナンバー１２１０
(72)発明者 トーマス ケー．リンデマン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ノースイースト １３３ プレイス １７２２５

Ｆターム(参考) 5B017 AA06 BA07 CA15 CA16
5J104 AA07 KA01 KA05 KA06 LA03 LA06 MA01 NA02 NA05 NA27
NA37 NA38 NA41 PA07 PA10