(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4889637号
(P4889637)
(45)発行日　平成24年3月7日(2012.3.7)　(24)登録日　平成23年12月22日(2011.12.22)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 520F
H04L 9/14 (2006.01)　　G06F 12/14 520P
　　H04L 9/00 641

請求項の数 8　(全 34 頁)

(21)出願番号　特願2007-524664 (P2007-524664)
(86)(22)出願日　平成18年7月11日 (2006.7.11)
(86)国際出願番号　PCT/JP2006/313789
(87)国際公開番号　WO2007/007764
(87)国際公開日　平成19年1月18日 (2007.1.18)
審査請求日　平成21年4月8日 (2009.4.8)
(31)優先権主張番号　特願2005-206124 (P2005-206124)
(32)優先日　平成17年7月14日 (2005.7.14)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109210
弁理士　新居　広守
(72)発明者　岡本　隆一
日本国大阪府門真市大字門真１００６番地
松下電器産業株式会社内
(72)発明者　平本　琢士
日本国大阪府門真市大字門真１００６番地
松下電器産業株式会社内
(72)発明者　櫻井　厚典
日本国大阪府門真市大字門真１００６番地
松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】ライセンス管理装置及び方法

(57)【特許請求の範囲】
【請求項１】
コンテンツを一定の利用条件の下で利用する権利を示す情報であるライセンスを管理するライセンス管理装置であって、
ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定手段と、
前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積手段と、
各ライセンス管理装置に固有な固有鍵を保持する固有鍵保持手段と、
あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段とを備え、
前記ライセンス蓄積手段は、さらに、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記固有鍵保持手段が保持する固有鍵を用いて前記ライセンスを暗号化し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵保持手段が保持するドメイン鍵を用いて、前記ライセンスを暗号化する暗号化部を備える
ことを特徴とするライセンス管理装置。
【請求項２】
前記ライセンス管理装置は、さらに、
前記ライセンスに含まれる利用条件に従ってコンテンツを利用する利用手段と、

前記利用手段によるコンテンツの利用によって、前記ライセンス種別判定手段によって判定された前記ライセンスの種別が変化したか否かを判定するライセンス種別変更判定手段とを備え、

前記暗号化部は、前記ライセンスの種別が変化したと判定された場合、変化前の種別に応じた鍵で前記ライセンスを復号した後、変化後の種別に応じた鍵で前記ライセンスを暗号化する

ことを特徴とする請求項１記載のライセンス管理装置。

【請求項３】

コンテンツを一定の利用条件の下で利用する権利を示す情報であるライセンスを管理するライセンス管理装置であって、

ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定手段と、

前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積手段と、

前記ライセンス蓄積手段に蓄積された前記ライセンスの改竄防止用の情報をセキュアに記録するための記憶領域を有するセキュア管理手段とを備え、

前記ライセンス蓄積手段は、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合には、前記セキュア管理手段に前記改竄防止情報を記録し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合には、前記セキュア管理手段に改竄防止情報を記録しない

ことを特徴とするライセンス管理装置。

【請求項４】

前記ライセンス管理装置は、さらに、

前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、コンテンツの利用の都度、前記ライセンスに含まれる利用条件を更新する更新手段と、

前記更新手段によってコンテンツの利用の都度、更新する必要のある利用条件が更新される都度、前記ライセンスの更新回数を示す更新回数情報を生成する更新回数情報生成手段とを備え、

前記改竄防止用の情報は、更新回数情報である

ことを特徴とする請求項３記載のライセンス管理装置。

【請求項５】

コンテンツを一定の利用条件の下で利用する権利を示す情報であるライセンスを管理するライセンス管理装置であって、

ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定手段と、

前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積手段と、

他のライセンス管理装置との間にセキュアな通信路を確立して前記ライセンス蓄積手段に蓄積されているライセンスの送受信を行うセキュア送受信手段と、

他のライセンス管理装置との間で、通常の通信路を介して、前記ライセンス蓄積手段に蓄積されているライセンスの送受信を行う送受信手段と、

あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段と、

他のライセンス管理装置との間の前記ライセンスの送受信制御を行う送受信制御手段とを備え、

前記ライセンス蓄積手段は、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵を用いて前記ライセンスを暗号化した上で蓄積し、

前記送受信制御手段は、前記ライセンスがコンテンツの利用の都度、更新する必要のあ

る利用条件を含んでいる場合、前記セキュア送受信手段を用いて前記ライセンスの送受信を行い、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵で暗号化された前記ライセンスを前記送受信手段を用いて送受信する

ことを特徴とするライセンス管理装置。

【請求項６】

コンテンツを一定の利用条件の下で利用する権利を示す情報であるライセンスを管理するライセンス管理装置が行うライセンス管理方法であって、

前記ライセンス管理装置は、

各ライセンス管理装置に固有な固有鍵を保持する固有鍵保持手段と、

あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段とを備え、

前記ライセンス管理方法は、

前記ライセンス管理装置が、ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定ステップと、

前記ライセンス管理装置が、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積ステップとを含み、

前記ライセンス蓄積ステップは、さらに、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記固有鍵保持手段から固有鍵を読み出して前記ライセンスを暗号化し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵保持手段からドメイン鍵を読み出して前記ライセンスを暗号化する暗号化ステップを含む

ことを特徴とするライセンス管理方法。

【請求項７】

コンテンツを一定の利用条件の下で利用する権利を示す情報であるライセンスを管理するライセンス管理装置が行うライセンス管理方法であって、

前記ライセンス管理装置は、

あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段を備え、

前記ライセンス管理方法は、

前記ライセンス管理装置が、ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定ステップと、

前記ライセンス管理装置が、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積ステップと、

前記ライセンス管理装置が、他のライセンス管理装置との間にセキュアな通信路を確立して前記ライセンス蓄積ステップで蓄積されたライセンスの送受信を行うセキュア送受信ステップと、

前記ライセンス管理装置が、他のライセンス管理装置との間で、通常の通信路を介して、前記ライセンス蓄積ステップで蓄積されたライセンスの送受信を行う送受信ステップと、

前記ライセンス管理装置が、他のライセンス管理装置との間の前記ライセンスの送受信制御を行う送受信制御ステップとを含み、

前記ライセンス蓄積ステップでは、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵保持手段からドメイン鍵を読み出して前記ライセンスを暗号化した上で蓄積し、

前記送受信制御ステップでは、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記セキュア送受信ステップにより前記ライセンスの送受信を行い、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条

件を含んでいない場合、前記ドメイン鍵で暗号化された前記ライセンスを前記送受信ステップにより送受信する
ことを特徴とするライセンス管理方法。
【請求項８】
コンテンツを一定の利用条件の下で利用する権利を示す情報であるライセンスを管理するライセンス管理装置のためのプログラムであって、
前記ライセンス管理装置は、
各ライセンス管理装置に固有な固有鍵を保持する固有鍵保持手段と、
あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段とを備え、
前記プログラムは、
ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定ステップと、
前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積ステップとをコンピュータに実行させ、
前記ライセンス蓄積ステップでは、さらに、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記固有鍵保持手段が保持する固有鍵を用いて前記ライセンスを暗号化し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵保持手段が保持するドメイン鍵を用いて、前記ライセンスを暗号化する暗号化ステップをコンピュータに実行させる
ことを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、著作権保護されているコンテンツを再生する為のライセンスを管理する装置及び方法に関する。
【背景技術】
【０００２】
近年、音楽や映像、ゲーム等のデジタル著作物であるコンテンツを、インターネットやデジタル放送等で配信するシステムが開発され、その一部は、実用化の段階を迎えている。また、これらのコンテンツの配信に当たり、著作権保護等の観点から、配信したコンテンツの再生期限や回数等を制限するコンテンツの利用制御方法が併せて検討されている。
【０００３】
従来では、サーバが、コンテンツを利用するために必要な利用条件やコンテンツ鍵等を含む情報（以下、「ライセンス」と呼ぶ）を配信し、家庭内のネットワークシステム（ホームネットワーク）上の複数の端末が、サーバから配信されたライセンスを用いてコンテンツを利用し、再生等を行うようにモデル化されている。
【０００４】
また、サーバから配信されたライセンスは、個々の端末に保有され、端末は、自らが保有するライセンスを用いてコンテンツを利用する。端末は、ライセンスを蓄積する際には、端末固有の固有鍵を用いてライセンスを暗号化して蓄積する。これにより、蓄積されているライセンスを他の端末に複製することができたとしても、復号することができないので、このライセンスを用いてコンテンツを利用することはできない。これによって著作権を安全に保護することができる。また、そうしたライセンスを複数の端末間において移動を行う際には、コンテンツの権利保護の観点、および、端末所有者のプライバシー保護の観点から、無制限な範囲での移動は許されず、ある一定範囲内での移動のみが許されるのが一般的である。一般的には同一ユーザが所有する複数の端末間においてのみ移動が許されると考えられている。

【０００５】
これを実現する従来手法として、同一ユーザが所有する複数の端末に対して一つのドメインを設定し、ドメイン毎に、ドメイン鍵を生成して各端末に配信することが考えられている。端末は、ライセンスを外部に出力する際には、固有鍵で暗号化されて蓄積されているライセンスの暗号を復号した上で、それをドメイン鍵で暗号化して出力する。この結果、同一ドメインに属する端末においては、このライセンスの復号が可能であるが、同一ドメインに属さない端末においては、このライセンスの復号ができないということになる。このようにして、二つの端末が同一のドメインに属している場合には、その端末間でのライセンスの移動を許可するが、それ以外の場合には、ライセンスの移動を許可しないということを実現している（例えば、特許文献１参照）。

【０００６】
上記従来の手法によれば、端末間でライセンスを移動する際、移動元端末においては、ライセンスをドメイン鍵で暗号化した上で出力し、移動先端末においては、ドメイン鍵で暗号化されたライセンスを入力として受け取り、それをドメイン鍵で復号して利用する。ここで、移動元端末において、ライセンスをドメイン鍵で暗号化して移動する場合、暗号化される前のライセンスは暗号化時に端末内で自動的に削除される。

【特許文献１】特開２０００－１８１８０３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】
しかしながら、ドメイン鍵で暗号化された後のライセンスは、ユーザがこれを何回でも複製することが可能である。しかも、通信路に関しても、安全な認証チャネル（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ、以降、「ＳＡＣ」と呼ぶ）を確立した上で移動先の端末に送信されるわけではない為、複製された暗号化ライセンスを何回でも、同じ移動先端末に送信することが可能である。

【０００８】
このような場合、ライセンスに含まれる利用条件として、更新する必要のない利用条件（例えば、再生期限等。以降、このような利用条件を「ステートレスな利用条件」と呼ぶ）が設定されている場合には問題は発生しないが、ライセンスに含まれる利用条件として、更新する必要のある利用条件（例えば、再生回数等。以降、このような利用条件を「ステートフルな利用条件」と呼ぶ）が設定されている場合、本来許可されている範囲を超えて再生を許可してしまうという問題が発生する。

【０００９】
例えば、利用条件として「３回再生可能」と設定されているライセンスを、ドメイン鍵で暗号化した上で出力し、それを他の端末に移動したとする。移動先の端末で、このライセンスを利用してコンテンツを３回再生した後、先程ドメイン鍵で暗号化され出力されたライセンスを、再度移動先端末に対し入力したとすると、移動先端末で、更にコンテンツを３回再生可能となってしまうといったことが考えられる。

【００１０】
一方、これに対し、ドメイン内でライセンスを移動先の端末に送信する場合、ＳＡＣなどにより安全な認証チャネルを確立した上で、再送制御を行いライセンスを送信するようにすれば、同じライセンスが何度も同じ移動先端末に送信されることを防止することができる。しかし、この場合、ライセンスの移動の都度、固有鍵で暗号化されたライセンスを復号した上、ＳＡＣを確立して送信するという処理は、端末の処理負荷が大きくなってしまうという問題がある。

【００１１】
本発明は、上記従来の課題を解決するものであり、ライセンスの種別に応じて、著作権保護のためのセキュリティの高さを切り替え、本来許可された範囲内でのみコンテンツの利用を許可しつつ、且つ、不必要なＳＡＣ確立等の処理負荷を低減することが可能なライセンス管理装置及び方法を提供することを目的とする。

【課題を解決するための手段】
【００１２】
上記従来の課題を解決するために、本発明のライセンス管理装置は、コンテンツを一定の利用条件の下で利用する権利を示す情報であるライセンスを管理するライセンス管理装置であって、ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定手段と、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積手段とを備えることを特徴とする。
【００１３】
また、前記ライセンス管理装置は、さらに、前記各ライセンス管理装置に固有な固有鍵を保持する固有鍵保持手段と、あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段とを備え、前記ライセンス蓄積手段は、さらに、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記固有鍵保持手段が保持する固有鍵を用いて前記ライセンスを暗号化し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵保持手段が保持するドメイン鍵を用いて、前記ライセンスを暗号化する暗号化部を備えるとしてもよい。
【００１４】
前記ライセンス管理装置は、さらに、前記ライセンスに含まれる利用条件に従ってコンテンツを利用する利用手段と、前記利用手段によるコンテンツの利用によって、前記ライセンス種別判定手段によって判定された前記ライセンスの種別が変化したか否かを判定するライセンス種別変更判定手段とを備え、前記暗号化部は、前記ライセンスの種別が変化したと判定された場合、変化前の種別に応じた鍵で前記ライセンスを復号した後、変化後の種別に応じた鍵で前記ライセンスを暗号化するとしてもよい。
【００１５】
また、前記ライセンス管理装置は、さらに、前記ライセンス蓄積手段に蓄積された前記ライセンスの改竄防止用の情報をセキュアに記録するための記憶領域を有するセキュア管理手段を備え、前記ライセンス蓄積手段は、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合には、前記セキュア管理手段に前記改竄防止情報を記録し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合には、前記セキュア管理手段に改竄防止情報を記録しないとしてもよい。
【００１６】
前記ライセンス管理装置は、さらに、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、コンテンツの利用の都度、前記ライセンスに含まれる利用条件を更新する更新手段と、前記更新手段によってコンテンツの利用の都度、更新する必要のある利用条件が更新される都度、前記ライセンスの更新回数を示す更新回数情報を生成する更新回数情報生成手段とを備え、前記改竄防止用の情報は、更新回数情報であるとしてもよい。
【００１７】
また、前記ライセンス管理装置は、さらに、他のライセンス管理装置との間にセキュアな通信路を確立して前記ライセンス蓄積手段に蓄積されているライセンスの送受信を行うセキュア送受信手段と、他のライセンス管理装置との間で、通常の通信路を介して、前記ライセンス蓄積手段に蓄積されているライセンスの送受信を行う送受信手段と、あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段と、他のライセンス管理装置との間の前記ライセンスの送受信制御を行う送受信制御手段とを備え、前記ライセンス蓄積手段は、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵を用いて前記ライセンスを暗号化

した上で蓄積し、前記送受信制御手段は、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記セキュア送受信手段を用いて前記ライセンスの送受信を行い、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵で暗号化された前記ライセンスを前記送受信手段を用いて送受信するとしてもよい。

【発明の効果】

【００１８】

以上のように、本発明によれば、ライセンス蓄積手段は、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行う。すなわち、コンテンツの利用の都度更新する必要のある利用条件を含んでいるライセンスについては、高い安全性を要求されるので、ライセンス蓄積手段は、処理負荷は大きいけれどもセキュリティが高い蓄積処理を行ってライセンスを蓄積する。一方、コンテンツの利用の都度更新する必要のある利用条件を含んでいないライセンスでは、コンテンツの利用の都度更新する必要のある利用条件を含んでいるライセンスほど高い安全性は要求されないので、不必要なレベルの安全性の確保を省略して、処理負荷がより小さくなる蓄積処理を行ってライセンスを蓄積することができる。従って、本発明のライセンス管理装置では、ライセンスの種別に応じた蓄積処理を用いてライセンスを蓄積処理することにより、ライセンスのセキュリティを確保し、かつ、不要な処理負荷を削減するライセンス管理を実現することが可能となるという効果がある。

【００１９】

また、本発明のライセンス蓄積手段は、さらに、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記固有鍵保持手段が保持する固有鍵を用いて前記ライセンスを暗号化し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵保持手段が保持するドメイン鍵を用いて、前記ライセンスを暗号化する暗号化部を備える。従って、コンテンツの利用の都度更新する必要のある利用条件を含んでいないライセンスをドメイン内で移動するときには、ドメイン鍵で暗号化されているライセンスをライセンス蓄積手段から読み出して、そのまま移動することができる。従って、従来であれば、固有鍵で暗号化されて蓄積されているライセンスを、一旦復号した後、改めてドメイン鍵で暗号化し直して移動する必要があったものを、これらの処理を省略することができる。これによって、ライセンス管理装置の処理負荷を低減できるという効果がある。

【００２０】

さらに、本発明のライセンス蓄積手段は、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合には、前記セキュア管理手段に前記改竄防止情報を記録し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合には、前記セキュア管理手段に改竄防止情報を記録しない。このため、より高いセキュリティを要求されるライセンスに対しては、前記セキュア管理手段に改竄防止情報を記録し、それほど高いセキュリティを要求されないライセンスについては改竄防止情報を記録しない。これにより、本発明のライセンス管理装置は、貴重なセキュア管理手段の記憶領域を有効に利用して、ライセンスの改竄をチェックすることができる。また、この改竄防止情報をライセンスのハッシュ値とせずに更新回数情報とすることで、セキュア管理手段に記録される各改竄防止情報のデータ量を１６バイトのレベルから１バイトのレベルまで低減し、貴重なセキュア管理手段の記憶領域を有効に利用することができるという効果がある。

【００２１】

また、本発明の前記送受信制御手段は、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記セキュア送受信手段を用いて前記ライセンスの送受信を行い、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵で暗号化された前記ライセンスを前記送受信手段を用いて送受信する。従って、より高いセキュリティを要求されるライセンスに対

しては、処理負荷は大きいが安全性の高いセキュアな通信路を用いて移動し、それほど高いセキュリティを要求されないライセンスについてはドメイン鍵で暗号化されたライセンスを、通常の通信路を用いて移動を行う。この結果、ライセンスを移動する際のライセンス管理装置の処理負荷を効率よく低減することができるという効果がある。

【発明を実施するための最良の形態】

【００２２】

本発明の実施の形態におけるライセンス管理装置１００について説明を行う。

【００２３】

図１は、本発明の実施の形態におけるライセンス管理装置１００の全体構成を示す図である。図１において、ライセンス管理装置１００は、ライセンス取り込み部１０１と、ライセンス蓄積制御部１０２と、ライセンス転送制御部１０３と、ライセンス転送部（転送方式Ａ）１０４と、ライセンス転送部（転送方式Ｂ）１０５と、コンテンツ取り込み部１０６と、コンテンツ蓄積部１１３と、固有情報管理部１０７と、ドメイン情報管理部１０８と、ライセンス管理情報管理部１０９と、ライセンス蓄積部１１０と、コンテンツ再生制御部１１１と、コンテンツ復号・再生部１１２とを備えている。以下ライセンス管理装置１００の各構成要素について説明を行う。

【００２４】

ここで、ライセンス蓄積制御部１０２およびライセンス転送制御部１０３の一部の機能は、「ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいるかいないかの種別を判定するライセンス種別判定手段と、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合と含んでいない場合とで、異なる蓄積処理を行うライセンス蓄積手段」とに相当する。

【００２５】

また、固有情報管理部１０７は「前記各ライセンス管理装置に固有な固有鍵を保持する固有鍵保持手段」に相当し、ドメイン情報管理部１０８は「あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段」に相当し、ライセンス蓄積部１１０は「前記暗号化手段によって暗号化された前記ライセンスを蓄積するライセンス蓄積手段」に相当し、ライセンス蓄積制御部１０２は「さらに、前記蓄積処理として、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記固有鍵保持手段が保持する固有鍵を用いて前記ライセンスを暗号化し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵保持手段が保持するドメイン鍵を用いて、前記ライセンスを暗号化する暗号化部」に相当する。

【００２６】

さらに、コンテンツ復号・再生部１１２は「前記ライセンスに含まれる利用条件に従ってコンテンツを利用する利用手段」に相当し、コンテンツ再生制御部１１１は「前記利用手段によるコンテンツの利用によって、前記ライセンス種別判定手段によって判定された前記ライセンスの種別が変化したか否かを判定するライセンス種別変更判定手段と前記ライセンスの種別が変化したと判定された場合、変化前の種別に応じた鍵で前記ライセンスを復号した後、変化後の種別に応じた鍵で前記ライセンスを暗号化する前記暗号化部」に相当する。

【００２７】

また、ライセンス管理情報管理部１０９は「前記ライセンス蓄積手段に蓄積された前記ライセンスの改竄防止用の情報をセキュアに記録するための記憶領域を有するセキュア管理手段」に相当し、ライセンス蓄積制御部１０２は「前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合には、前記セキュア管理手段に前記改竄防止情報を記録し、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合には、前記セキュア管理手段に改竄防止情報を記録しない前記ライセンス蓄積手段」に相当する。

【００２８】

さらに、コンテンツ再生制御部１１１は「前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、コンテンツの利用の都度、前記ライセンスに含まれる利用条件を更新する更新手段と、前記更新手段によってコンテンツの利用の都度、更新する必要のある利用条件が更新される都度、前記ライセンスの更新回数を示す更新回数情報を生成する更新回数情報生成手段」に相当し、ライセンス管理情報３００は「前記改竄防止用の情報である更新回数情報」に相当する。

【００２９】

また、ライセンス転送部（転送方式Ａ）１０４は「他のライセンス管理装置との間にセキュアな通信路を確立して前記ライセンス蓄積手段に蓄積されているライセンスの送受信を行うセキュア送受信手段」に相当し、ライセンス転送部（転送方式Ｂ）１０５は「他のライセンス管理装置との間で、通常の通信路を介して、前記ライセンス蓄積手段に蓄積されているライセンスの送受信を行う送受信手段」に相当し、ドメイン情報管理部１０８は「あらかじめ定められた複数のライセンス管理装置から構成されるドメイン内で他のライセンス管理装置と共有されるドメイン鍵を保持するドメイン鍵保持手段」に相当し、ライセンス蓄積部１１０及びライセンス蓄積制御部１０２は「前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記ドメイン鍵を用いて前記ライセンスを暗号化した上で蓄積する前記ライセンス蓄積手段」に相当し、ライセンス転送制御部１０３は「他のライセンス管理装置との間の前記ライセンスの送受信制御を行い、これにおいて、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいる場合、前記セキュア送受信手段を用いて前記ライセンスの送受信を行い、前記ライセンスがコンテンツの利用の都度、更新する必要のある利用条件を含んでいない場合、前記暗号化手段によって暗号化された前記ライセンスを前記送受信手段を用いて送受信する前記送受信制御手段」に相当する。

【００３０】

ライセンス取り込み部１０１は、ライセンス２００（図２に図示する）を、ライセンス配信サーバ１２０から受信し、ライセンス管理装置１００に取り込む手段である。ライセンス２００は、ライセンス配信サーバ１２０から、インターネットや、ＣＡＴＶ（Ｃａｂｌｅ　Ｔｅｌｅｖｉｓｉｏｎ）、放送波等の有線伝送路または無線伝送路を介して送信され、暗号化されているものとする。ライセンス取り込み部１０１は、ライセンス２００をライセンス管理装置１００に取り込む際に復号するものとし、ライセンス２００の復号に使用する復号鍵、もしくは、復号鍵の生成に必要な情報を、ライセンス配信サーバ１２０から取得し保持しているものとする。

【００３１】

図２に図示する通り、ライセンス２００は、少なくともライセンスＩＤ２０１と、コンテンツＩＤ２０２と、ドメインＩＤ２０３と、利用条件種別２０４と、利用条件２０５と、コンテンツ鍵２０６とを含む情報のことであり、ライセンス管理装置１００は、ライセンス２００を用いてコンテンツの再生を行うものとする。ライセンスＩＤ２０１には、ライセンス２００を一意に特定するＩＤが記述される。コンテンツＩＤ２０２には、ライセンス２００を使用して再生するコンテンツのＩＤが記述される。ドメインＩＤ２０３には、ライセンス２００を転送可能なドメインのＩＤが記述される。ドメインとは、ライセンス２００の転送が許可されるライセンス管理装置１００の集合のことであり、各々のドメインには、それを一意に特定するドメインＩＤ２０３とドメイン固有の鍵であるドメイン鍵とが付与されるものとする。利用条件種別２０４には、利用条件２０５の種別を示す情報が記述される。本実施の形態においては、利用条件２０５が、更新する必要のある利用条件（例えば、再生回数等。以降、このような利用条件を「ステートフルな利用条件」と呼ぶ）であるか、更新する必要のない利用条件（例えば、再生期限等。以降、このような利用条件を「ステートレスな利用条件」と呼ぶ）であるかを示す情報が記述されるものとする。利用条件２０５には、再生可能回数や、再生期限およびライセンスの移動の可否等、コンテンツの利用を許可する条件が記述される。コンテンツ鍵２０６には、コンテンツを復号する復号鍵が記述される。

【００３２】
図１に戻り、ライセンス蓄積制御部１０２は、ライセンス取り込み部１０１が取り込んだライセンス２００を、コンテンツ鍵２０６の部分を暗号化した上でライセンス蓄積部１１０に蓄積する手段である。ライセンス蓄積制御部１０２は、利用条件種別２０４が「ステートフルな利用条件」であるライセンス２００については、コンテンツ鍵２０６を固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いて暗号化した上で蓄積するものとする。また、その際には、ライセンス管理情報管理部１０９によって管理されているライセンス管理情報３００（図３に図示する）に、蓄積したライセンス２００に関する情報を記録するものとする。図３は、ライセンス管理情報３００のデータ構成の一例を示す図である。図３において、更新回数３０１は、ライセンス２００の利用条件２０５を更新した回数を示す情報である。図３では、例えば、ライセンスＩＤ２０１が「１１１１１１」であるライセンス２００は、その利用条件２０５を一度も更新しておらず、ライセンスＩＤ２０１が「２２２２２２」であるライセンス２００は、その利用条件２０５を「２回」、ライセンスＩＤ２０１が「２２２２２３」であるライセンス２００は、その利用条件２０５を「３回」更新していることを表している。また、ライセンス蓄積制御部１０２は、利用条件種別２０４が「ステートレスな利用条件」であるライセンス２００については、コンテンツ鍵２０６をドメイン情報管理部１０８が保持するドメイン鍵を用いて暗号化した上で蓄積するものとする。なお、暗号化に使用するドメイン鍵は、ライセンス２００のドメインＩＤ２０３で特定されるドメインのドメイン鍵を選択して使用するものとする。

【００３３】
図４は、ライセンス２００がライセンス蓄積部１１０に格納された状態を示す図である。更に、ライセンス蓄積制御部１０２は、ライセンス蓄積部１１０にライセンス２００を蓄積する際、図４に図示する通り、改竄防止情報４０１を付加して蓄積するものとする。改竄防止情報４０１は、次のように計算される。利用条件種別２０４が「ステートフルな利用条件」であるライセンス２００の場合、改竄防止情報４０１は、ライセンス管理装置固有鍵を用いてコンテンツ鍵２０６部分を暗号化されたライセンス２００に、更新回数３０１とライセンス管理装置固有鍵とを連結したデータに対するハッシュ値として計算される。利用条件種別２０４が「ステートレスな利用条件」であるライセンス２００の場合、改竄防止情報４０１は、ドメイン鍵を用いてコンテンツ鍵２０６部分を暗号化されたライセンス２００に、そのドメイン鍵を連結したデータに対するハッシュ値として計算される。なお、ハッシュ値は、本実施の形態においては、ＳＨＡ－２５６（Ｓｅｃｕｒｅ　Ｈａｓｈｉｎｇ　Ａｌｇｏｒｉｔｈｍ　２５６）アルゴリズムに基づいて計算されるものとする。

【００３４】
図１に戻り、ライセンス転送制御部１０３は、自装置と他のライセンス管理装置１００との間でのライセンス２００の転送を制御する手段である。具体的には、ライセンス転送制御部１０３は、ライセンス管理装置１００が管理しているライセンス２００のリストであるライセンスリスト５００（図５に図示する）の送受信や、ライセンス２００の転送の際、ライセンス転送部（転送方式Ａ）１０４、もしくは、ライセンス転送部（転送方式Ｂ）１０５のいずれの手段を用いて転送を行うかを決定する。図５は、ライセンスリスト５００のデータ構成の一例を示す図である。なお、図５では、このライセンスリスト５００を送信したライセンス管理装置１００では、ライセンスＩＤ２０１が「０００００１１」で、ドメインＩＤ２０３が「ＡＡＡＡＡＡ」、利用条件種別２０４が「ステートレスな利用条件」であるライセンス２００と、ライセンスＩＤ２０１が「０００００１２」で、ドメインＩＤ２０３が「ＢＢＢＢＢＢ」、利用条件種別２０４が「ステートフルな利用条件」であるライセンス２００との２つのライセンスを管理していることを表している。

【００３５】
ライセンス転送部（転送方式Ａ）１０４は、利用条件種別２０４が「ステートフルな利用条件」であるライセンス２００の転送を行う手段である。ライセンス２００の受信側及

び送信側のライセンス転送部（転送方式Ａ）１０４は、相互に連絡を取り合い、ＳＡＣ（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ）を確立した後、ライセンス２００を転送するものとする。

【００３６】

ライセンス転送部（転送方式Ｂ）１０５は、利用条件種別２０４が「ステートレスな利用条件」であるライセンス２００の転送を行う手段である。転送元及び転送先のライセンス転送部（転送方式Ｂ）１０５は、相互に連絡を取り合い、コンテンツ鍵２０６部分がドメイン鍵で暗号化されているライセンス２００を転送するものとする。

【００３７】

コンテンツ取り込み部１０６は、コンテンツ配信サーバ１３０から、コンテンツを取得し、コンテンツ蓄積部１１３に蓄積する手段である。コンテンツは、コンテンツ配信サーバ１３０から、インターネットや、ＣＡＴＶ（Ｃａｂｌｅ　Ｔｅｌｅｖｉｓｉｏｎ）、放送波等の有線伝送路または無線伝送路を介して送信されるものとし、ライセンス２００に含まれるコンテンツ鍵２０６によって復号可能なように暗号化されているものとする。なお、コンテンツには、コンテンツＩＤ２０２が付加されているものとする。

【００３８】

コンテンツ蓄積部１１３は、コンテンツを蓄積する手段である。

【００３９】

固有情報管理部１０７は、ライセンス管理装置１００固有の情報を管理する手段であり、ライセンス管理装置１００を一意に特定するライセンス管理装置ＩＤと、ライセンス管理装置１００固有のライセンス管理装置固有鍵とを保持する。

【００４０】

ドメイン情報管理部１０８は、ライセンス管理装置１００が属するドメインに関する情報を管理する手段であり、ライセンス管理装置１００が属するドメインのドメインＩＤ２０３とドメイン鍵との組を保持する。本実施の形態においては、同一のドメインに属するライセンス管理装置１００は、同一のドメインＩＤ２０３とドメイン鍵との組を共有しているものとする。また、ライセンス管理装置１００が複数のドメインに属する場合、ドメイン情報管理部１０８は、ドメインＩＤ２０３とドメイン鍵との組を複数保持するものとする。

【００４１】

ライセンス管理情報管理部１０９は、図３を用いて説明を行ったライセンス管理情報３００を管理する手段である。ライセンス管理情報管理部１０９は、ライセンス管理情報３００を、ユーザがアクセスすることのできない耐タンパ化された領域に管理するものとする。

【００４２】

ライセンス蓄積部１１０は、ライセンス２００を蓄積する手段である。

【００４３】

コンテンツ再生制御部１１１は、コンテンツの再生を制御する手段である。具体的には、ライセンス２００の利用条件２０５を参照して、コンテンツの再生可否を判定し、再生可の場合には、コンテンツ鍵２０６を復号した上で、コンテンツ復号・再生部１１２に送信する処理を行う。なお、コンテンツ再生制御部１１１から、コンテンツ復号・再生部１１２へのコンテンツ鍵２０６の送信は、ＳＡＣを確立した上で行われることが望ましい。

【００４４】

コンテンツ復号・再生部１１２は、コンテンツ再生制御部１１１から受信したコンテンツ鍵２０６を用いて、コンテンツ蓄積部１１３に蓄積されているコンテンツを復号し、再生する手段である。

【００４５】

以上で、本実施の形態におけるライセンス管理装置１００の構成についての説明を終わる。

【００４６】

次にフローチャートを用いて、本実施の形態におけるライセンス管理装置１００の動作について説明を行う。

【００４７】

図６は、図１に示したライセンス取り込み部１０１およびライセンス蓄積制御部１０２によるライセンス蓄積処理の動作を示すフローチャートである。まず、図６に示すフローチャートを参照して、本実施の形態におけるライセンス管理装置１００において、ライセンス２００をライセンス配信サーバ１２０から受信し、その後、ライセンス管理装置１００内に取り込んで蓄積する、ライセンス蓄積処理の動作について説明する。

【００４８】

Ｓ６０１：ライセンス取り込み部１０１は、ライセンス配信サーバ１２０から受信したライセンスをライセンス管理装置１００内に取り込み、取り込んだライセンス２００を復号する。なお、ライセンス取り込み部１０１は、ライセンス２００の復号に使用する復号鍵、もしくは、復号鍵の生成に必要な情報を、ライセンス配信サーバ１２０から予め取得し保持しているものとする。

【００４９】

Ｓ６０２：ライセンス蓄積制御部１０２は、ライセンス取り込み部１０１が復号したライセンス２００の利用条件種別２０４を確認する。利用条件種別２０４が「ステートフルな利用条件」の場合には、Ｓ６０３の処理に進む。利用条件種別２０４が「ステートレスな利用条件」の場合には、Ｓ６０６の処理に進む。

【００５０】

Ｓ６０３：ライセンス蓄積制御部１０２は、固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いて、ライセンス２００のコンテンツ鍵２０６を暗号化する。

【００５１】

Ｓ６０４：ライセンス蓄積制御部１０２は、ライセンス管理情報管理部１０９によって管理されているライセンス管理情報３００に、ライセンス２００に関する情報を記録する。

【００５２】

Ｓ６０５：ライセンス蓄積制御部１０２は、Ｓ６０３でコンテンツ鍵２０６部分を暗号化したライセンス２００に、Ｓ６０４で記録したライセンス管理情報３００の更新回数３０１とライセンス管理装置固有鍵とを連結したデータに対するハッシュ値を計算し、その値を改竄防止情報４０１として、ライセンス２００に付加する。

【００５３】

Ｓ６０６：ライセンス蓄積制御部１０２は、ドメイン情報管理部１０８が保持するドメイン鍵の中から、ライセンス２００のドメインＩＤ２０３と組になって記憶されているドメイン鍵を選択し、それを用いて、ライセンス２００のコンテンツ鍵２０６を暗号化する。

【００５４】

Ｓ６０７：ライセンス蓄積制御部１０２は、Ｓ６０６でコンテンツ鍵２０６部分を暗号化したライセンス２００に、ドメイン鍵を連結したデータに対するハッシュ値を計算し、その値を改竄防止情報４０１として、ライセンス２００に付加する。

【００５５】

Ｓ６０８：ライセンス蓄積制御部１０２は、ライセンス蓄積部１１０に、改竄防止情報４０１が付加されたライセンス２００を蓄積する。

【００５６】

以上で、本実施の形態におけるライセンス蓄積処理の動作についての説明を終わる。

【００５７】

図７は、図１に示したコンテンツ再生制御部１１１およびコンテンツ復号・再生部１１２によるコンテンツ再生処理の動作を示すフローチャートである。次に、図７のフローチャートを参照して、本実施の形態におけるライセンス管理装置１００において、ライセンス２００を用いてコンテンツを再生する、コンテンツ再生処理の動作について説明する。

【００５８】
Ｓ７０１：コンテンツ再生制御部１１１は、コンテンツの再生に使用するライセンス２００をライセンス蓄積部１１０から取り出す。
【００５９】
Ｓ７０２：コンテンツ再生制御部１１１は、Ｓ７０１で取り出したライセンス２００の利用条件種別２０４を確認する。利用条件種別２０４が「ステートフルな利用条件」の場合には、Ｓ７０３の処理に進む。利用条件種別２０４が「ステートレスな利用条件」の場合には、Ｓ７０４の処理に進む。
【００６０】
Ｓ７０３：図８を参照して後述する、ステートフルライセンス再生可否判定処理を実行し、コンテンツの再生可否を判定する。
【００６１】
Ｓ７０４：図９を参照して後述する、ステートレスライセンス再生可否判定処理を実行し、コンテンツの再生可否を判定する。
【００６２】
Ｓ７０５：Ｓ７０３、もしくは、Ｓ７０４での再生可否判定結果が、「再生可」の場合、Ｓ７０６の処理に進む。Ｓ７０３、もしくは、Ｓ７０４での再生可否判定結果が、「再生不可」の場合には、図示しないディスプレイなどの提示手段を介して、ユーザにコンテンツ再生不可である旨を通知し、処理を終了する。
【００６３】
Ｓ７０６：コンテンツ再生制御部１１１は、コンテンツ鍵２０６をコンテンツ復号・再生部１１２に送信する。なお、このコンテンツ鍵２０６の送信は、コンテンツ再生制御部１１１とコンテンツ復号・再生部１１２との間でＳＡＣなどの方法で保護されることが好ましい。
【００６４】
Ｓ７０７：コンテンツ復号・再生部１１２は、コンテンツ再生制御部１１１から受信したコンテンツ鍵２０６を用いて、コンテンツ蓄積部１１３に蓄積されているコンテンツを復号し、再生する。
【００６５】
Ｓ７０８：コンテンツ復号・再生部１１２は、コンテンツ終端迄再生を完了した場合や、ユーザから再生停止の指示があった場合等、コンテンツの再生を終了する。
【００６６】
Ｓ７０９：図１０を参照して後述する、コンテンツ再生停止後処理を実行する。
【００６７】
以上で、本実施の形態におけるコンテンツ再生処理の動作についての説明を終わる。
【００６８】
図８は、図１に示したコンテンツ再生制御部１１１によるステートフルライセンス再生可否判定処理の動作を示すフローチャートである。次に、図８のフローチャートを参照して、図７におけるＳ７０３の、ステートフルライセンス再生可否判定処理の動作について説明を行う。
【００６９】
Ｓ８０１：コンテンツ再生制御部１１１は、ライセンス管理情報管理部１０９が管理するライセンス管理情報３００を参照し、コンテンツ再生に利用しようとしているライセンス２００に関する情報が記述されているかどうかを確認する。記述が有る場合、Ｓ８０２の処理に進む。記述が無い場合には、Ｓ８０６の処理に進む。
【００７０】
Ｓ８０２：コンテンツ再生制御部１１１は、ライセンス２００の改竄の有無を確認する。具体的には、コンテンツ再生制御部１１１は、ライセンス２００にライセンス管理情報３００の更新回数３０１とライセンス管理装置固有鍵とを連結したデータに対するハッシュ値を計算し、その値と、ライセンス２００に付加されている改竄防止情報４０１の値と

を比較する。コンテンツ再生制御部１１１は、比較の結果、値が一致する場合にはライセンスの改竄は無かったと判定し、値が一致しない場合にはライセンスの改竄が有ったと判定するものとする。判定の結果、ライセンスの改竄が無かった場合、Ｓ８０３の処理に進む。ライセンスの改竄が有った場合、Ｓ８０６の処理に進む。

【００７１】

Ｓ８０３：コンテンツ再生制御部１１１は、ライセンス２００の利用条件２０５を参照し、コンテンツの再生が許可されているかどうかを判定する。コンテンツ再生が許可されている場合、Ｓ８０４の処理に進む。コンテンツ再生が許可されていない場合には、Ｓ８０６の処理に進む。

【００７２】

Ｓ８０４：コンテンツ再生制御部１１１は、コンテンツ再生可と判定する。

【００７３】

Ｓ８０５：コンテンツ再生制御部１１１は、ライセンス２００からコンテンツ鍵２０６を取り出し、それを固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いて復号する。

【００７４】

Ｓ８０６：コンテンツ再生制御部１１１は、コンテンツ再生不可と判定する。

【００７５】

以上で、本実施の形態におけるステートフルライセンス再生可否判定処理の動作についての説明を終わる。

【００７６】

図９は、図１に示したコンテンツ再生制御部１１１によるステートレスライセンス再生可否判定処理の動作を示すフローチャートである。次に、図９のフローチャートを参照して、図７におけるＳ７０４の、ステートレスライセンス再生可否判定処理の動作について説明を行う。

【００７７】

Ｓ９０１：コンテンツ再生制御部１１１は、ライセンス２００の改竄の有無を確認する。具体的には、コンテンツ再生制御部１１１は、ライセンス２００にドメイン鍵を連結したデータに対するハッシュ値を計算し、その値と、ライセンス２００に付加されている改竄防止情報４０１の値とを比較することによって行う。ここで、連結するドメイン鍵は、ドメイン情報管理部１０８が保持するドメイン鍵の中から、ライセンス２００のドメインＩＤ２０３と組になって記憶されているドメイン鍵を選択するものとする。コンテンツ再生制御部１１１は、比較の結果、値が一致する場合にはライセンスの改竄は無かったと判定し、値が一致しない場合にはライセンスの改竄が有ったと判定する。ライセンスの改竄が無かった場合、Ｓ９０２の処理に進む。ライセンスの改竄が有った場合、Ｓ９０５の処理に進む。

【００７８】

Ｓ９０２：コンテンツ再生制御部１１１は、ライセンス２００の利用条件２０５を参照し、コンテンツの再生が許可されているかどうかを判定する。コンテンツ再生が許可されている場合、Ｓ９０３の処理に進む。コンテンツ再生が許可されていない場合には、Ｓ９０５の処理に進む。

【００７９】

Ｓ９０３：コンテンツ再生制御部１１１は、コンテンツ再生可と判定する。

【００８０】

Ｓ９０４：コンテンツ再生制御部１１１は、ライセンス２００からコンテンツ鍵２０６を取り出し、それをドメイン情報管理部１０８が保持するドメイン鍵を用いて復号する。なお、復号に使用するドメイン鍵は、ドメイン情報管理部１０８が保持するドメイン鍵の中から、ライセンス２００のドメインＩＤ２０３と組になって記憶されているドメイン鍵を選択するものとする。

【００８１】

Ｓ９０５：コンテンツ再生制御部１１１は、コンテンツ再生不可と判定する。

【００８２】

以上で、本実施の形態におけるステートレスライセンス再生可否判定処理の動作についての説明を終わる。

【００８３】

図１０は、図１に示したコンテンツ再生制御部１１１およびコンテンツ復号・再生部１１２によるコンテンツ再生停止後処理の動作を示すフローチャートである。次に、図１０のフローチャートを参照して、図７におけるＳ７０９の、コンテンツ再生停止後処理の動作について説明を行う。

【００８４】

Ｓ１００１：コンテンツ復号・再生部１１２は、自らが保持するコンテンツ鍵２０６を削除し、コンテンツ再生制御部１１１にコンテンツ再生終了を通知する。

【００８５】

Ｓ１００２：コンテンツ再生制御部１１１は、コンテンツ再生終了通知を受信すると、コンテンツ再生に使用したライセンス２００の利用条件種別２０４を確認する。利用条件種別２０４が「ステートフルな利用条件」である場合、Ｓ１００３の処理に進む。利用条件種別２０４が「ステートレスな利用条件」である場合、そのまま処理を終了する。

【００８６】

Ｓ１００３：コンテンツ再生制御部１１１は、コンテンツを再生した分、ライセンス２００の利用条件２０５を更新する。例えば、利用条件２０５が「５回再生可」となっていた場合には、これを「４回再生可」に書きかえる処理を行う。また、例えば、利用条件２０５が「初回再生日時から１日間有効」となっていた場合で、かつ、今回が初回である場合には、現在日時から１日後の日時を算出し、その日時迄再生可能と書きかえる処理を行う。

【００８７】

Ｓ１００４：コンテンツ再生制御部１１１は、Ｓ１００３で更新した利用条件２０５を参照し、それが「ステートレスな利用条件」に変更になっていないかどうかを確認する。「ステートレスな利用条件」に変更になっている場合、コンテンツ再生制御部１１１は、ライセンス２００の利用条件種別２０４を「ステートレスな利用条件」に変更し、Ｓ１００７の処理に進む。「ステートレスな利用条件」に変更になっていない場合、Ｓ１００５の処理に進む。利用条件２０５が、「ステートレスな利用条件」に変更になる例としては、例えば、「初回再生日時から１日間有効」となっていた利用条件２０５を、「ＹＹＹＹ年ＭＭ月ＤＤ日迄再生可能」と更新した場合等が考えられる。

【００８８】

Ｓ１００５：コンテンツ再生制御部１１１は、ライセンス管理情報管理部１０９が管理しているライセンス管理情報３００を更新する。具体的には、ライセンス管理情報３００の更新回数３０１を１加算する処理を行う。

【００８９】

Ｓ１００６：コンテンツ再生制御部１１１は、ライセンス２００に、Ｓ１００５で更新した更新回数３０１とライセンス管理装置固有鍵とを連結したデータに対するハッシュ値を計算する。コンテンツ再生制御部１１１は、計算した値を新たな改竄防止情報４０１として、既存の改竄防止情報４０１と置きかえる。

【００９０】

Ｓ１００７：コンテンツ再生制御部１１１は、ライセンス管理情報管理部１０９が管理しているライセンス管理情報３００から、コンテンツ再生に使用したライセンス２００の情報を削除する。

【００９１】

Ｓ１００８：コンテンツ再生制御部１１１は、ライセンス２００のコンテンツ鍵２０６を、固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いて復号する。

【００９２】

Ｓ１００９：コンテンツ再生制御部１１１は、ドメイン情報管理部１０８が保持するドメイン鍵の中から、ライセンス２００のドメインＩＤ２０３と組になって記憶されているドメイン鍵を選択し、それを用いて、ライセンス２００のコンテンツ鍵２０６を暗号化する。

【００９３】

Ｓ１０１０：コンテンツ再生制御部１１１は、Ｓ１００９でコンテンツ鍵２０６部分を暗号化したライセンス２００に、ドメイン鍵を連結したデータに対するハッシュ値を計算する。コンテンツ再生制御部１１１は、計算した値を新たな改竄防止情報４０１として、既存の改竄防止情報４０１と置きかえる。

【００９４】

以上で、本実施の形態におけるコンテンツ再生停止後処理の動作についての説明を終わる。

【００９５】

図１１は、図１に示したライセンス転送制御部１０３によるライセンス転送処理の動作を示すフローチャートである。次に、図１１のフローチャートを参照して、ライセンス管理装置１００間で、ライセンス２００の転送を行う、ライセンス転送処理の動作について説明を行う。

【００９６】

Ｓ１１０１：ライセンス受信側のライセンス管理装置１００内のライセンス転送制御部１０３（以降、「受信側ライセンス転送制御部１０３」と呼ぶ）は、ライセンスリスト５００の送信要求を、ライセンス送信側のライセンス管理装置１００内のライセンス転送制御部１０３（以降、「送信側ライセンス転送制御部１０３」と呼ぶ）に対して送信する。

【００９７】

Ｓ１１０２：送信側ライセンス転送制御部１０３は、ライセンスリスト５００の送信要求を受信する。

【００９８】

Ｓ１１０３：送信側ライセンス転送制御部１０３は、ライセンスリスト５００を生成し、生成したライセンスリスト５００を、受信側ライセンス転送制御部１０３に対して送信する。

【００９９】

Ｓ１１０４：受信側ライセンス転送制御部１０３は、ライセンスリスト５００を受信する。

【０１００】

Ｓ１１０５：受信側ライセンス転送制御部１０３は、Ｓ１１０４で受信したライセンスリスト５００を参照し、送信を要求するライセンス２００の利用条件種別２０４を確認する。送信を要求するライセンス２００の利用条件種別２０４が「ステートフルな利用条件」である場合、Ｓ１１０６の処理に進む。送信を要求するライセンス２００の利用条件種別２０４が「ステートレスな利用条件」である場合、Ｓ１１０７の処理に進む。

【０１０１】

Ｓ１１０６：図１２及び図１３を参照して後述する、ステートフルライセンス転送処理を実行する。

【０１０２】

Ｓ１１０７：図１７を参照して後述する、ステートレスライセンス転送処理を実行する。

【０１０３】

以上で、本実施の形態におけるライセンス転送処理の動作についての説明を終わる。

【０１０４】

図１２および図１３は、図１に示したライセンス転送部（転送方式Ａ）１０４によるステートフルライセンス転送処理の動作を示すフローチャートである。図１４は、ステートフルライセンス送信要求１４００のデータ構成の一例を示す図である。図１５は、ステー

トフルライセンス送信要求レスポンス１５００のデータ構成の一例を示す図である。次に、図１２及び図１３のフローチャートを参照して、図１１におけるＳ１１０６の、ステートフルライセンス転送処理の動作について説明を行う。

【０１０５】

Ｓ１２０１：ライセンス受信側のライセンス管理装置１００内のライセンス転送部（転送方式Ａ）１０４（以降、「受信側ライセンス転送部（転送方式Ａ）１０４」と呼ぶ）は、ライセンス送信側のライセンス管理装置１００内のライセンス転送部（転送方式Ａ）１０４（以降、「送信側ライセンス転送部（転送方式Ａ）１０４」と呼ぶ）と相互に通信し合い、ＳＡＣを確立する。本ステップ以降の、受信側ライセンス転送部（転送方式Ａ）１０４と送信側ライセンス転送部（転送方式Ａ）１０４との通信は、全てこのＳＡＣ上で行われることとする。なお、ＳＡＣ確立手法に関しては、従来手法を用いることとする。

【０１０６】

Ｓ１２０２：受信側ライセンス転送部（転送方式Ａ）１０４は、図１４に図示するステートフルライセンス送信要求１４００を生成し、それを送信側ライセンス転送部（転送方式Ａ）１０４に対し送信する。受信側ライセンス転送部（転送方式Ａ）１０４は、ステートフルライセンス送信要求１４００を生成する際、ステートフルライセンス送信要求識別子１４０１には、このデータがステートフルライセンス送信要求１４００であることを示す情報を記述する。また、ライセンスＩＤ２０１には、送信を要求するライセンスのライセンスＩＤ２０１を記述する。また、ドメイン固有情報１４０２には、ドメイン情報管理部１０８が保持するドメイン鍵の中から、送信を要求するライセンス２００のドメインＩＤ２０３と組となって記憶されているドメイン鍵を選択し、そのハッシュ値を記述するものとする。

【０１０７】

Ｓ１２０３：送信側ライセンス転送部（転送方式Ａ）１０４は、ステートフルライセンス送信要求１４００を受信する。

【０１０８】

Ｓ１２０４：図１６を参照して後述する、ステートフルライセンス送信要求レスポンス生成処理を実行し、ステートフルライセンス送信要求レスポンス１５００（図１５に図示する）を生成する。図１５において、ステートフルライセンス送信要求レスポンス識別子１５０１には、このデータがステートフルライセンス送信要求レスポンス１５００であることを示す情報が記述される。ステータスコード１５０２には、ライセンスの送信が可であるか不可であるかを示す情報が記述される。ライセンスの送信が可である場合、ライセンス２００には、送信を要求されたライセンス２００が記述される。

【０１０９】

Ｓ１２０５：送信側ライセンス転送部（転送方式Ａ）１０４は、Ｓ１２０４で生成したステートフルライセンス送信要求レスポンス１５００を、受信側ライセンス転送部（転送方式Ａ）１０４に対し送信する。

【０１１０】

Ｓ１２０６：受信側ライセンス転送部（転送方式Ａ）１０４は、ステートフルライセンス送信要求レスポンス１５００を受信する。

【０１１１】

以降のステップより、図１３を参照して説明を行う。

【０１１２】

Ｓ１３０１：受信側ライセンス転送部（転送方式Ａ）１０４は、Ｓ１２０６で受信したステートフルライセンス送信要求レスポンス１５００のステータスコード１５０２を確認して、送信を要求したライセンス２００を受信できたかどうかを確認する。ライセンス２００を受信できた場合、Ｓ１３０２の処理に進む。ライセンス２００を受信できなかった場合、受信側ライセンス転送部（転送方式Ａ）１０４は、図示しないディスプレイなどの提示手段を介して、ユーザにライセンス２００を受信できなかった旨を通知し、処理を終了する。

【０１１３】
Ｓ１３０２：受信側ライセンス転送部（転送方式Ａ）１０４は、固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いて、ライセンス２００のコンテンツ鍵２０６を暗号化する。
【０１１４】
Ｓ１３０３：受信側ライセンス転送部（転送方式Ａ）１０４は、ライセンス管理情報管理部１０９によって管理されているライセンス管理情報３００に、受信したライセンス２００に関する情報を記録する。
【０１１５】
Ｓ１３０４：受信側ライセンス転送部（転送方式Ａ）１０４は、Ｓ１３０２でコンテンツ鍵２０６部分を暗号化したライセンス２００に、Ｓ１３０３で記録したライセンス管理情報３００の更新回数３０１とライセンス管理装置固有鍵とを連結したデータに対するハッシュ値を計算し、その値を改竄防止情報４０１として、ライセンス２００に付加する。
【０１１６】
Ｓ１３０５：受信側ライセンス転送部（転送方式Ａ）１０４は、ライセンス蓄積部１１０に、改竄防止情報４０１が付加されたライセンス２００を蓄積する。
【０１１７】
Ｓ１３０６：受信側ライセンス転送部（転送方式Ａ）１０４は、送信側ライセンス転送部（転送方式Ａ）１０４に対し、ライセンス２００の受信確認通知を送信する。
【０１１８】
Ｓ１３０７：送信側ライセンス転送部（転送方式Ａ）１０４は、ライセンス２００の受信確認通知を受信する。
【０１１９】
Ｓ１３０８：送信側ライセンス転送部（転送方式Ａ）１０４は、送信したライセンス２００を、ライセンス蓄積部１１０から削除し、ライセンス管理情報管理部１０９によって管理されているライセンス管理情報３００から、そのライセンス２００の情報を削除する。
【０１２０】
以上で、本実施の形態におけるステートフルライセンス転送処理の動作についての説明を終わる。
【０１２１】
図１６は、図１に示したライセンス転送部（転送方式Ａ）１０４によるステートフルライセンス送信要求レスポンス生成処理の動作を示すフローチャートである。次に、図１６のフローチャートを参照して、図１２におけるＳ１２０４の、ステートフルライセンス送信要求レスポンス生成処理の動作について説明を行う。
【０１２２】
Ｓ１６０１：送信側ライセンス転送部（転送方式Ａ）１０４は、Ｓ１２０３で受信したステートフルライセンス送信要求１４００に含まれるドメイン固有情報１４０２が正当なものかどうかを確認する。具体的には、送信側ライセンス転送部（転送方式Ａ）１０４は、ドメイン情報管理部１０８が保持するドメイン鍵の中から、送信を要求されているライセンス２００のドメインＩＤ２０３と組となって記憶されているドメイン鍵を選択し、そのハッシュ値を計算する。その後、計算した値と、ステートフルライセンス送信要求１４００に含まれるドメイン固有情報１４０２に記述されている値とを比較し、値が一致する場合には「正当」、値が不一致の場合には「不正当」と判定するものとする。ドメイン固有情報１４０２が正当である場合には、Ｓ１６０２の処理に進む。ドメイン固有情報１４０２が正当でない場合には、Ｓ１６０８の処理に進む。
【０１２３】
Ｓ１６０２：送信側ライセンス転送部（転送方式Ａ）１０４は、ライセンス管理情報管理部１０９が管理するライセンス管理情報３００を参照し、送信を要求されているライセンス２００に関する情報が記述されているかどうかを確認する。記述が有る場合、Ｓ１６

０３の処理に進む。記述が無い場合には、Ｓ１６０８の処理に進む。

【０１２４】

Ｓ１６０３：送信側ライセンス転送部（転送方式Ａ）１０４は、送信が要求されているライセンス２００の改竄の有無を確認する。具体的には、送信側ライセンス転送部（転送方式Ａ）１０４は、ライセンス２００にライセンス管理情報３００の更新回数３０１とライセンス管理装置固有鍵とを連結したデータに対するハッシュ値を計算し、その値と、ライセンス２００に付加されている改竄防止情報４０１の値とを比較する。コンテンツ再生制御部１１１は、比較の結果、値が一致する場合にはライセンスの改竄は無かったと判定し、値が一致しない場合にはライセンスの改竄が有ったと判定するものとする。判定の結果、ライセンスの改竄が無かった場合、Ｓ１６０４の処理に進む。ライセンスの改竄が有った場合、Ｓ１６０８の処理に進む。

【０１２５】

Ｓ１６０４：送信側ライセンス転送部（転送方式Ａ）１０４は、ライセンス２００の利用条件２０５を参照し、移動が許可されているかどうかを判定する。移動が許可されている場合、Ｓ１６０５の処理に進む。移動が許可されていない場合には、Ｓ１６０８の処理に進む。

【０１２６】

Ｓ１６０５：送信側ライセンス転送部（転送方式Ａ）１０４は、ステートフルライセンス送信要求レスポンス１５００のステートフルライセンス送信要求レスポンス識別子１５０１に、このデータがステートフルライセンス送信要求レスポンス１５００であることを示す情報を記述し、ステータスコード１５０２に、「ライセンスの送信可」と記述する。

【０１２７】

Ｓ１６０６：送信側ライセンス転送部（転送方式Ａ）１０４は、固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いてコンテンツ鍵２０６を復号する。

【０１２８】

Ｓ１６０７：送信側ライセンス転送部（転送方式Ａ）１０４は、ステートフルライセンス送信要求レスポンス１５００のライセンス２００に、Ｓ１６０６でコンテンツ鍵２０６が復号されたライセンス２００を記述する。

【０１２９】

Ｓ１６０８：送信側ライセンス転送部（転送方式Ａ）１０４は、ステートフルライセンス送信要求レスポンス１５００のステートフルライセンス送信要求レスポンス識別子１５０１に、このデータがステートフルライセンス送信要求レスポンス１５００であることを示す情報を記述し、ステータスコード１５０２に、「ライセンスの送信不可」と記述する。

【０１３０】

以上で、本実施の形態におけるステートフルライセンス送信要求レスポンス生成処理の動作についての説明を終わる。

【０１３１】

図１７は、図１に示したライセンス転送部（転送方式Ｂ）１０５によるステートレスライセンス転送処理の動作を示すフローチャートである。図１８は、ステートレスライセンス送信要求１８００のデータ構成の一例を示す図である。図１９は、ステートレスライセンス送信要求レスポンス１９００のデータ構成の一例を示す図である。次に、図１７のフローチャートを参照して、図１１におけるＳ１１０７の、ステートレスライセンス転送処理の動作について説明を行う。

【０１３２】

Ｓ１７０１：ライセンス受信側のライセンス管理装置１００内のライセンス転送部（転送方式Ｂ）１０５（以降、「受信側ライセンス転送部（転送方式Ｂ）１０５」と呼ぶ）は、図１８に図示するステートレスライセンス送信要求１８００を生成し、それを、ライセンス送信側のライセンス管理装置１００内のライセンス転送部（転送方式Ｂ）１０５（以降、「送信側ライセンス転送部（転送方式Ｂ）１０５」と呼ぶ）に対し送信する。受信側

ライセンス転送部（転送方式Ｂ）１０５は、ステートレスライセンス送信要求１８００を生成する際、ステートレスライセンス送信要求識別子１８０１には、このデータがステートレスライセンス送信要求１８００であることを示す情報を記述し、ライセンスＩＤ２０１には、送信を要求するライセンスのライセンスＩＤ２０１を記述するものとする。

【０１３３】

Ｓ１７０２：送信側ライセンス転送部（転送方式Ｂ）１０５は、ステートレスライセンス送信要求１８００を受信する。

【０１３４】

Ｓ１７０３：図２０を参照して後述する、ステートレスライセンス送信要求レスポンス生成処理を実行し、ステートレスライセンス送信要求レスポンス１９００（図１９に図示する）を生成する。図１９において、ステートレスライセンス送信要求レスポンス識別子１９０１には、このデータがステートレスライセンス送信要求レスポンス１９００であることを示す情報が記述される。ステータスコード１５０２には、ライセンスの送信が可であるか不可であるかを示す情報が記述される。ライセンス２００には、送信を要求されたライセンス２００が記述される。改竄防止情報４０１には、送信を要求されたライセンス２００に付加されていた改竄防止情報４０１が記述される。

【０１３５】

Ｓ１７０４：送信側ライセンス転送部（転送方式Ｂ）１０５は、Ｓ１７０３で生成したステートレスライセンス送信要求レスポンス１９００を、受信側ライセンス転送部（転送方式Ｂ）１０５に対し送信する。

【０１３６】

Ｓ１７０５：受信側ライセンス転送部（転送方式Ｂ）１０５は、ステートレスライセンス送信要求レスポンス１９００を受信する。

【０１３７】

Ｓ１７０６：受信側ライセンス転送部（転送方式Ｂ）１０５は、Ｓ１７０５で受信したステートレスライセンス送信要求レスポンス１９００のステータスコード１５０２を確認して、送信を要求したライセンス２００を受信できたかどうかを確認する。ライセンス２００を受信できた場合、Ｓ１７０７の処理に進む。ライセンス２００を受信できなかった場合、受信側ライセンス転送部（転送方式Ｂ）１０５は、図示しないディスプレイなどの提示手段を介して、ユーザにライセンス２００を受信できなかった旨を通知し、処理を終了する。

【０１３８】

Ｓ１７０７：受信側ライセンス転送部（転送方式Ｂ）１０５は、Ｓ１７０５で受信したステートレスライセンス送信要求レスポンス１９００に含まれるライセンス２００と改竄防止情報４０１とを連結して、ライセンス蓄積部１１０に蓄積する。

【０１３９】

以上で、本実施の形態におけるステートレスライセンス転送処理の動作についての説明を終わる。

【０１４０】

図２０は、図１に示したライセンス転送部（転送方式Ｂ）１０５によるステートレスライセンス送信要求レスポンス生成処理の動作を示すフローチャートである。次に、図２０のフローチャートを参照して、図１７におけるＳ１７０３の、ステートレスライセンス送信要求レスポンス生成処理の動作について説明を行う。

【０１４１】

Ｓ２００１：送信側ライセンス転送部（転送方式Ｂ）１０５は、送信を要求されているライセンス２００がライセンス蓄積部１１０に蓄積されているかどうかを確認する。確認の結果、ライセンス２００が蓄積されている場合には、Ｓ２００２の処理に進む。ライセンス２００が蓄積されていない場合には、Ｓ２００４の処理に進む。

【０１４２】

Ｓ２００２：送信側ライセンス転送部（転送方式Ｂ）１０５は、ステートレスライセン

ス送信要求レスポンス１９００のステートレスライセンス送信要求レスポンス識別子１９０１に、このデータがステートレスライセンス送信要求レスポンス１９００であることを示す情報を記述し、ステータスコード１５０２に、「ライセンスの送信可」と記述する。

【０１４３】

Ｓ２００３：送信側ライセンス転送部（転送方式Ｂ）１０５は、ステートレスライセンス送信要求レスポンス１９００のライセンス２００に、送信が要求されているライセンス２００のコンテンツ鍵をドメイン鍵で暗号化したライセンス２００を記述する。また、ステートレスライセンス送信要求レスポンス１９００の改竄防止情報４０１に、ライセンス２００に付加されていた改竄防止情報４０１を記述する。

【０１４４】

Ｓ２００４：送信側ライセンス転送部（転送方式Ｂ）１０５は、ステートレスライセンス送信要求レスポンス１９００のステートレスライセンス送信要求レスポンス識別子１９０１に、このデータがステートレスライセンス送信要求レスポンス１９００であることを示す情報を記述し、ステータスコード１５０２に、「ライセンスの送信不可」と記述する。

【０１４５】

以上で、本実施の形態におけるステートレスライセンス送信要求レスポンス生成処理の動作についての説明を終わる。

【０１４６】

以上で、本実施の形態におけるライセンス管理装置１００の動作についての説明を終わる。

【０１４７】

なお、少なくとも、ライセンス取り込み部１０１と、ライセンス蓄積制御部１０２と、ライセンス転送部（転送方式Ａ）１０４と、固有情報管理部１０７と、ドメイン情報管理部１０８と、ライセンス管理情報管理部１０９と、コンテンツ再生制御部１１１と、コンテンツ復号・再生部１１２は、耐タンパ化されて実装されることが望ましい。

【０１４８】

また、本実施の形態においては、ライセンス管理装置１００の構成要素は、一つの筐体内に実装されるものとして説明を行ったが、それに限らず、複数の筐体やＩＣカード等に分かれて実装されたりしてもよいものとする。例えば、ライセンス取り込み部１０１と、ライセンス蓄積制御部１０２と、ライセンス転送部（転送方式Ａ）１０４と、固有情報管理部１０７と、ドメイン情報管理部１０８と、コンテンツ再生制御部１１１とは、ＩＣカード内に実装され、その他の手段は、ＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）内に実装されるという構成が考えられる。

【０１４９】

なお、本実施の形態においては、ライセンス２００をライセンス蓄積部１１０に蓄積する際、コンテンツ鍵２０６のみを暗号化するとして説明を行ったが、それに限るわけではなく、コンテンツ鍵２０６を含む一部のみ、もしくは、ライセンス２００全体を暗号化するとしてもよいものとする。

【０１５０】

なお、本実施の形態においては、改竄防止情報４０１の計算の際、ライセンス２００に対し、ライセンス管理装置固有鍵、もしくは、ドメイン鍵を連結して、ハッシュ値計算対象データとするとして説明を行ったが、それに限るわけではなく、ライセンス管理装置固有鍵の替わりにライセンス管理装置ＩＤを、ドメイン鍵の替わりにドメインＩＤ２０３を連結してもよいものとする。

【０１５１】

なお、本実施の形態においては、改竄防止情報４０１の計算の際、ライセンス２００のコンテンツ鍵２０６部分を暗号化したデータに対し、各種データを連結して、ハッシュ値計算対象データとするとして説明を行ったが、それに限るわけではなく、コンテンツ鍵２０６部分の暗号化を行う前に、各種データを連結し、ハッシュ値計算対象としてもよいも

のとする。

【０１５２】

なお、本実施の形態においては、ライセンス２００にドメインＩＤ２０３を含めるとしたが、それに限るわけではなく、ドメインＩＤ２０３を特定できるその他の情報を含むとしてもよいものとする。

【０１５３】

なお、本実施の形態において、ライセンス２００に利用条件種別２０４を含め、その利用条件種別２０４をもとにどのような処理を行うか判定するとして説明を行ったが、それに限るわけではなく、ライセンス２００に利用条件種別２０４を含めずに、利用条件２０５の内容から、利用条件の種別を導き出し、導き出した情報をもとにどのような処理を行うか判定するとしてもよいものとする。

【０１５４】

なお、図１０のコンテンツ再生停止後処理において、コンテンツ復号・再生部１１２は、必ず、コンテンツ再生制御部１１１にコンテンツ再生終了を通知する（Ｓ１００１の処理）として説明を行ったが、それに限るわけではなく、コンテンツ再生に使用したライセンス２００の利用条件種別２０４が「ステートレスな利用条件」である場合については、コンテンツ再生終了を通知しないとしてもよいものとする。この場合、図７のコンテンツ再生処理において、コンテンツ再生制御部１１１が、コンテンツ鍵２０６をコンテンツ復号・再生部１１２に送信する（Ｓ７０６の処理）際、利用条件種別２０４も同時に送信するものとし、コンテンツ復号・再生部１１２は、この情報にもとづいて、コンテンツ再生終了を通知するか否かを判定するものとする。

【０１５５】

なお、本実施の形態において、ライセンスリスト５００には、利用条件種別２０４を含めるとしたが、それに限るわけではなく、利用条件種別２０４の替わりに利用条件２０５を含めてもいいものとする。この場合、利用条件２０５の内容から、利用条件の種別を導き出すものとする。

【０１５６】

なお、図１２及び図１３のステートフルライセンス転送処理において、ステートフルライセンス送信要求１４００の中に、ドメイン固有情報１４０２としてドメイン鍵のハッシュ値を含めて送信する（Ｓ１２０２の処理）として説明を行ったが、これに限るわけではなく、ドメインに属しているライセンス管理装置１００のみが生成可能なドメインに固有の情報であればどのような情報でも良いものとする。また、ドメイン固有情報１４０２の送信は、改竄や成りすましを防ぐ方法であれば、どのような方法であってもよいものとする。例えば、ＳＡＣ確立時の処理（Ｓ１２０１の処理）の中で、ドメイン固有情報１４０２を送信し、ドメインＩＤ２０３が一致しない場合にはＳＡＣ確立に失敗するようにすること等が考えられる。

【０１５７】

なお、本実施の形態においては、ライセンス２００の利用条件種別２０４に応じて、処理の内容を切り替えるよう説明を行ったが、ライセンス２００に処理の切り替えを指定する情報を設けて、それに従って処理を切り替えても良いものとする。例えば、ライセンスの移動可否や、コンテンツの内容や、コンテンツの価格等に従ってその情報を設定し、処理を切り替えるといったこと等が考えられる。

【０１５８】

なお、図７のコンテンツ再生処理において、コンテンツの再生に利用したライセンス２００の利用条件２０５の更新及びそれに伴う各種処理（図１０のＳ１００３～Ｓ１０１０の処理）は、コンテンツ再生停止後に行うとして説明を行ったが、それに限るわけではなく、コンテンツ再生開始前（図８のＳ８０４もしくはＳ８０５の後）に行われてもよいものとする。

【０１５９】

なお、図１７のステートレスライセンス転送処理において、受信側ライセンス転送部（

転送方式Ｂ）１０５は、受信したライセンス２００と改竄防止情報４０１とを、改竄有無の確認なくライセンス蓄積部１１０に蓄積する（Ｓ１７０７の処理）として説明を行ったが、蓄積前に改竄有無の確認を行ってもよいものとする。

【０１６０】

なお、図６のライセンス蓄積処理において、利用条件種別２０４が「ステートフルな利用条件」であるライセンス２００を蓄積する際には、ライセンス管理情報３００にそのライセンス２００の情報を記録する（Ｓ６０４の処理）として説明を行ったが、ライセンス管理情報３００のサイズ削減の為に、ライセンス２００の受信時には、Ｓ６０３～Ｓ６０５の処理は行わず、ライセンス利用の前（Ｓ７０１の前）にこれらの処理を行ってもよいものとする。ライセンス２００の受信時に、Ｓ６０３～Ｓ６０５の処理を行わなかった場合、ライセンス２００の蓄積時に付加する改竄防止情報４０１は、ライセンス２００に対するハッシュ値として計算され、更に改竄防止情報４０１はライセンス２００に付加された後、まとめてライセンス管理装置固有鍵で暗号化されるものとする。

【０１６１】

以上で、本実施の形態におけるライセンス管理装置１００の説明を終わる。

【０１６２】

なお、上記実施の形態では、ライセンスの移動が可能である場合を前提に説明したが、本発明は、これに限定されず、ライセンスの移動の可否が利用条件で設定されている場合にでも適用することができる。

【０１６３】

この場合、ライセンス２００の移動の可否は、図２に示す利用条件２０５に記述される。ライセンス２００が利用条件２０５で移動不可とされている場合には、ライセンス管理装置１００は、ライセンス２００の利用条件種別２０４が「ステートレスな利用条件」である場合であっても、ライセンス２００をライセンス管理装置固有鍵で暗号化してライセンス蓄積部１１０に格納する。この場合、ライセンス２００がライセンス管理装置固有鍵で暗号化されているか、ドメイン鍵で暗号化されているかは、利用条件種別２０４が「ステートレスな利用条件」かまたは「ステートフルな利用条件」かの区別だけでは判断できない。図２１は、ライセンス２００の移動の可否が利用条件で設定されている場合における蓄積時のライセンス２００のデータ構造を示す図である。このため、同図に示すように、ライセンス２００がライセンス蓄積部１１０に蓄積されるときには、ライセンス２００に、暗号鍵情報２１０１および改竄防止情報４０１が付加される。暗号鍵情報２１０１は、ライセンス２００がライセンス管理装置固有鍵およびドメイン鍵のいずれで暗号化されたかを示す情報である。改竄防止情報４０１は、利用条件種別２０４が「ステートフルな利用条件」であるライセンス２００、および利用条件２０５で「移動可」と設定されており、かつ、利用条件種別２０４が「ステートレスな利用条件」であるライセンス２００の場合、上記実施の形態と同じである。

【０１６４】

改竄防止情報４０１の計算方法が上記実施の形態と異なるものは、利用条件２０５で「移動不可」と設定されており、かつ、利用条件種別２０４が「ステートレスな利用条件」であるライセンス２００の場合である。この場合、ライセンス２００はライセンス管理装置固有鍵で暗号化される。しかし、利用条件種別２０４が「ステートフルな利用条件」ではないため、利用条件２０５はコンテンツが利用されても更新されず、このライセンス２００にはライセンス管理情報３００が生成されない。このため、ライセンス蓄積制御部１０２は、改竄防止情報４０１として、ライセンス２００にライセンス管理装置固有鍵を連結したデータに対するハッシュ値を計算する。

【０１６５】

図２２は、ライセンスの移動の可否が利用条件で設定されている場合のライセンス蓄積処理におけるライセンス管理装置１００の動作を示すフローチャートである。ライセンス蓄積処理におけるライセンス管理装置１００の動作は、利用条件種別２０４が「ステートフルな利用条件」であるライセンス２００の場合、図６に示した上記実施の形態と同じで

ある。従って、図２２と図６とで異なる処理は、図６のＳ６０２で、ライセンス蓄積制御部１０２が利用条件種別２０４を確認した結果、利用条件種別２０４が「ステートレスな利用条件」であった場合の後の処理（Ｓ２２０１、Ｓ２２０２およびＳ２２０３）である。

【０１６６】

具体的には、ライセンス蓄積制御部１０２は、Ｓ６０２で利用条件種別２０４が「ステートレスな利用条件」であった場合には、Ｓ２２０１の処理に進む。

【０１６７】

Ｓ２２０１：ライセンス蓄積制御部１０２は、ライセンス２００の利用条件２０５を確認する。利用条件２０５が「移動可」の場合には、Ｓ６０６の処理に進む。利用条件２０５が「移動不可」の場合には、Ｓ２２０２の処理に進む。

【０１６８】

Ｓ２２０２：ライセンス蓄積制御部１０２は、固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いて、ライセンス２００のコンテンツ鍵２０６を暗号化する。

【０１６９】

Ｓ２２０３：ライセンス蓄積制御部１０２は、Ｓ２２０２でコンテンツ鍵２０６部分を暗号化したライセンス２００に、ライセンス管理装置固有鍵を連結したデータに対するハッシュ値を計算し、その値を改竄防止情報４０１として、ライセンス２００に付加する。

【０１７０】

さらに、ライセンスの移動の可否が利用条件で設定されている場合、コンテンツ再生制御部１１１によるステートレスライセンス再生可否判定処理の動作が図９に示したフローチャートと一部異なる。異なる点は、Ｓ９０１の前段、Ｓ９０１およびＳ９０４の処理である。まず、コンテンツ再生制御部１１１は、ステップＳ９０１でライセンス２００の改竄の有無を確認する前に、図２１に示した暗号鍵情報２１０１を参照して、ライセンス２００にライセンス管理装置固有鍵またはドメイン鍵のいずれを連結してハッシュ値を計算するか確認する。

【０１７１】

Ｓ９０１：ライセンス２００がドメイン鍵を連結してハッシュ値を計算する場合には、図９に示したＳ９０１の通りである。異なる点は、ライセンス２００にライセンス管理装置固有鍵を連結してハッシュ値を計算する場合である。この場合には、コンテンツ再生制御部１１１は、固有情報管理部１０７からライセンス管理装置固有鍵を読み出し、ライセンス２００に連結する。そして、コンテンツ再生制御部１１１は、ライセンス管理装置固有鍵をライセンス２００に連結したデータに対するハッシュ値を計算し、その値と、ライセンス２００に付加されている改竄防止情報４０１の値とを比較する。比較の結果、値が一致する場合にはライセンスの改竄は無かったと判定し、値が一致しない場合にはライセンスの改竄が有ったと判定する。以下、Ｓ９０３までの処理の内容は、図９で説明した各ステップと同じである。

【０１７２】

Ｓ９０４：ライセンス２００がドメイン鍵で暗号化されている場合には、図９に示したＳ９０４の通りである。ライセンス２００がライセンス管理装置固有鍵で暗号化されている場合には、コンテンツ再生制御部１１１は、ライセンス２００からコンテンツ鍵２０６を取り出し、それを固有情報管理部１０７が保持するライセンス管理装置固有鍵を用いて復号する。

【０１７３】

図２３は、ライセンスの移動の可否が利用条件で設定されている場合のコンテンツ再生停止後処理の動作を示すフローチャートである。コンテンツ再生停止後処理におけるライセンス管理装置１００の動作で、図２３と図１０とで異なる処理は、図２３のＳ２３０１およびＳ１０１０の処理である。すなわち、図１０のＳ１００７で、コンテンツ再生制御部１１１が、ライセンス管理情報管理部１０９が管理しているライセンス管理情報３００から、コンテンツ再生に使用したライセンス２００の情報を削除した後の処理である。コ

ンテンツ再生制御部１１１は、Ｓ１００８の処理の前に、Ｓ２３０１の処理を行う。

【０１７４】

Ｓ２３０１：コンテンツ再生制御部１１１は、ライセンス２００の利用条件２０５を確認する。利用条件２０５が「移動可」の場合には、Ｓ１００８の処理に進む。利用条件２０５が「移動不可」の場合には、Ｓ１０１０の処理に進む。

【０１７５】

Ｓ１０１０：コンテンツ再生制御部１１１は、Ｓ１００９でコンテンツ鍵２０６部分を暗号化したライセンス２００に対しては、図１０のＳ１０１０で説明した通りの処理を行う。コンテンツ再生制御部１１１は、Ｓ２３０１で利用条件２０５が「移動不可」であることが確認されたライセンス２００に対しては、ライセンス２００にライセンス管理装置固有鍵だけを連結したデータに対するハッシュ値を計算する。コンテンツ再生制御部１１１は、計算した値を新たな改竄防止情報４０１として、既存の改竄防止情報４０１と置きかえる。

【０１７６】

図２４は、ライセンスの移動の可否が利用条件で設定されている場合のステートレスライセンス送信要求レスポンス生成処理の動作を示すフローチャートである。ステートレスライセンス送信要求レスポンス生成処理におけるライセンス管理装置１００の動作で、図２４と図２０とで異なる処理は、図２４のＳ２４０１およびＳ２４０２の処理である。すなわち、図２０のＳ２００１で、送信側ライセンス転送部（転送方式Ｂ）１０５が、送信を要求されているライセンス２００がライセンス蓄積部１１０に蓄積されているかどうかを確認し、確認の結果、ライセンス２００が蓄積されている場合の後の処理である。送信側ライセンス転送部（転送方式Ｂ）１０５は、Ｓ２００２の処理の前に、Ｓ２４０１およびＳ２４０２の処理を行う。

【０１７７】

Ｓ２４０１：送信側ライセンス転送部（転送方式Ｂ）１０５は、送信が要求されているライセンス２００の改竄の有無を確認する。具体的には、送信側ライセンス転送部（転送方式Ｂ）１０５は、ライセンス蓄積部１１０に蓄積されているライセンス２００のコンテンツ鍵２０６がライセンス管理装置固有鍵で暗号化されている場合には、ライセンス２００にライセンス管理装置固有鍵を連結したデータに対するハッシュ値を計算し、その値と、ライセンス２００に付加されている改竄防止情報４０１の値とを比較する。ライセンス蓄積部１１０に蓄積されているライセンス２００のコンテンツ鍵２０６がドメイン鍵で暗号化されている場合には、ドメイン情報管理部１０８が保持するドメイン鍵の中から、送信を要求されているライセンス２００のドメインＩＤ２０３と組となって記憶されているドメイン鍵を選択する。さらに、ライセンス２００に選択したドメイン鍵を連結し、そのデータに対するハッシュ値を計算し、その値と、ライセンス２００に付加されている改竄防止情報４０１の値とを比較する。送信側ライセンス転送部（転送方式Ｂ）１０５は、比較の結果、値が一致する場合にはライセンスの改竄は無かったと判定し、値が一致しない場合にはライセンスの改竄が有ったと判定するものとする。判定の結果、ライセンスの改竄が無かった場合、Ｓ２４０２の処理に進む。ライセンスの改竄が有った場合、Ｓ２００４の処理に進む。

【０１７８】

Ｓ２４０２：送信側ライセンス転送部（転送方式Ｂ）１０５は、ライセンス２００の利用条件２０５を参照し、移動が許可されているかどうかを判定する。移動が許可されている場合、Ｓ２００２の処理に進む。移動が許可されていない場合には、Ｓ２００４の処理に進む。

【０１７９】

（その他変形例）

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【０１８０】

（１）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭまたはハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

【０１８１】

（２）上記の各装置を構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。

【０１８２】

（３）上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。前記ＩＣカードまたは前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカードまたは前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカードまたは前記モジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

【０１８３】

（４）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０１８４】

また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

【０１８５】

また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

【０１８６】

また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

【０１８７】

また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０１８８】

（５）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【０１８９】

本発明にかかるライセンス管理装置及び方法は、デジタル放送、ＣＡＴＶ、インターネ

ット等によるコンテンツ配信サービス受信端末や、ＤＶＤ等のパッケージメディアによるコンテンツ配信サービス受信端末等として有用である。

【図面の簡単な説明】

【０１９０】

【図１】図１は、ライセンス管理装置１００の構成を示すブロック図である。

【図２】図２は、ライセンス２００の一例を示す図である。

【図３】図３は、ライセンス管理情報３００の一例を示す図である。

【図４】図４は、ライセンス２００がライセンス蓄積部１１０に格納された状態を示す図である。

【図５】図５は、ライセンスリスト５００の一例を示す図である。

【図６】図６は、ライセンス蓄積処理の動作を示すフローチャートである。

【図７】図７は、コンテンツ再生処理の動作を示すフローチャートである。

【図８】図８は、ステートフルライセンス再生可否判定処理の動作を示すフローチャートである。

【図９】図９は、ステートレスライセンス再生可否判定処理の動作を示すフローチャートである。

【図１０】図１０は、コンテンツ再生停止後処理の動作を示すフローチャートである。

【図１１】図１１は、ライセンス転送処理の動作を示すフローチャートである。

【図１２】図１２は、ステートフルライセンス転送処理の動作の動作を示すフローチャートである。

【図１３】図１３は、ステートフルライセンス転送処理の動作の動作を示すフローチャートである。

【図１４】図１４は、ステートフルライセンス送信要求１４００の一例を示す図である。

【図１５】図１５は、ステートフルライセンス送信要求レスポンス１５００の一例を示す図である。

【図１６】図１６は、ステートフルライセンス送信要求レスポンス生成処理の動作を示すフローチャートである。

【図１７】図１７は、ステートレスライセンス転送処理の動作を示すフローチャートである。

【図１８】図１８は、ステートレスライセンス送信要求１８００の一例を示す図である。

【図１９】図１９は、ステートレスライセンス送信要求レスポンス１９００の一例を示す図である。

【図２０】図２０は、ステートレスライセンス送信要求レスポンス生成処理の動作を示すフローチャートである。

【図２１】図２１は、ライセンスの移動の可否が利用条件で設定されている場合における蓄積時のライセンスのデータ構造を示す図である。

【図２２】図２２は、ライセンスの移動の可否が利用条件で設定されている場合のライセンス蓄積処理におけるライセンス管理装置の動作を示すフローチャートである。

【図２３】図２３は、ライセンスの移動の可否が利用条件で設定されている場合のコンテンツ再生停止後処理の動作を示すフローチャートである。

【図２４】図２４は、ライセンスの移動の可否が利用条件で設定されている場合のステートレスライセンス送信要求レスポンス生成処理の動作を示すフローチャートである。

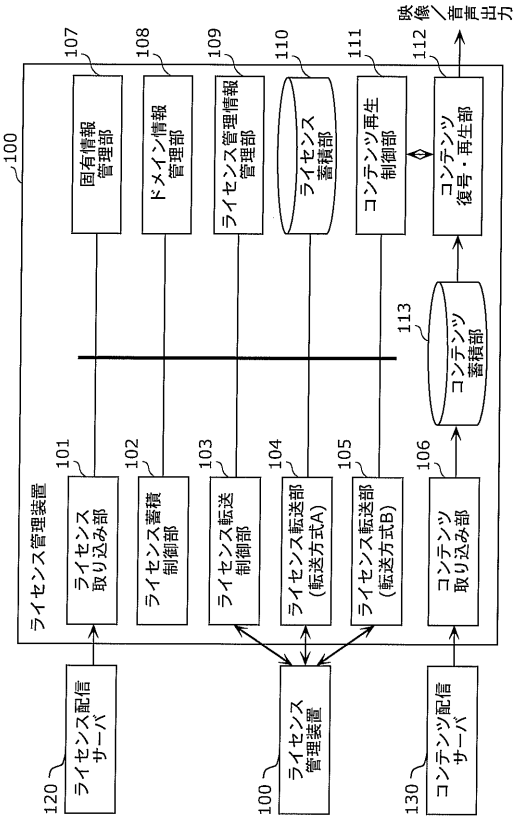
【符号の説明】

【０１９１】

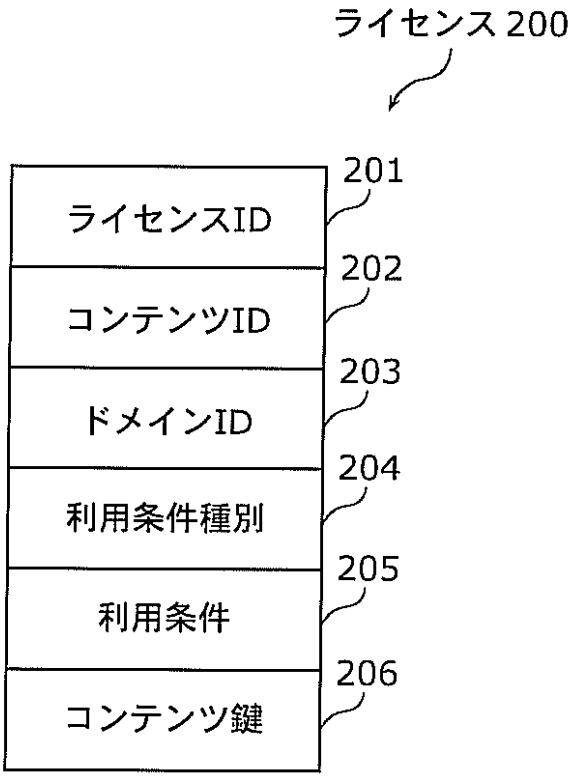
１００　ライセンス管理装置
１０１　ライセンス取り込み部
１０２　ライセンス蓄積制御部
１０３　ライセンス転送制御部
１０４　ライセンス転送部（転送方式Ａ）
１０５　ライセンス転送部（転送方式Ｂ）

１０６　コンテンツ取り込み部
１０７　固有情報管理部
１０８　ドメイン情報管理部
１０９　ライセンス管理情報管理部
１１０　ライセンス蓄積部
１１１　コンテンツ再生制御部
１１２　コンテンツ復号・再生部
１１３　コンテンツ蓄積部
１２０　ライセンス配信サーバ
１３０　コンテンツ配信サーバ
２００　ライセンス
２０１　ライセンスＩＤ
２０２　コンテンツＩＤ
２０３　ドメインＩＤ
２０４　利用条件種別
２０５　利用条件
２０６　コンテンツ鍵
３００　ライセンス管理情報
３０１　更新回数
４０１　改竄防止情報
５００　ライセンスリスト
１４００　ステートフルライセンス送信要求
１４０１　ステートフルライセンス送信要求識別子
１４０２　ドメイン固有情報
１５００　ステートフルライセンス送信要求レスポンス
１５０１　ステートフルライセンス送信要求レスポンス識別子
１５０２　ステータスコード
１８００　ステートレスライセンス送信要求
１８０１　ステートレスライセンス送信要求識別子
１９００　ステートレスライセンス送信要求レスポンス
１９０１　ステートレスライセンス送信要求レスポンス識別子

【図１】



【図２】

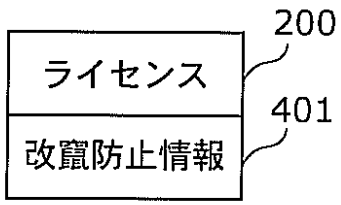


【図３】

ライセンス管理情報 300

201 ライセンスID	301 更新回数
111111	0回
222222	2回
222223	3回
・・・	・・・

【図４】

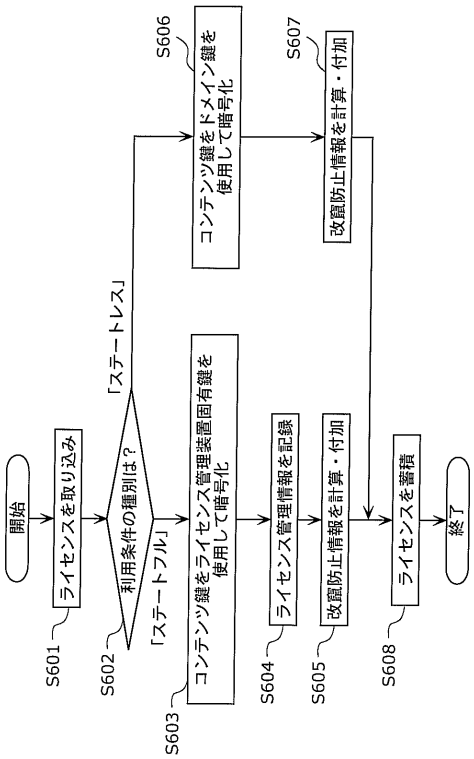


【図５】

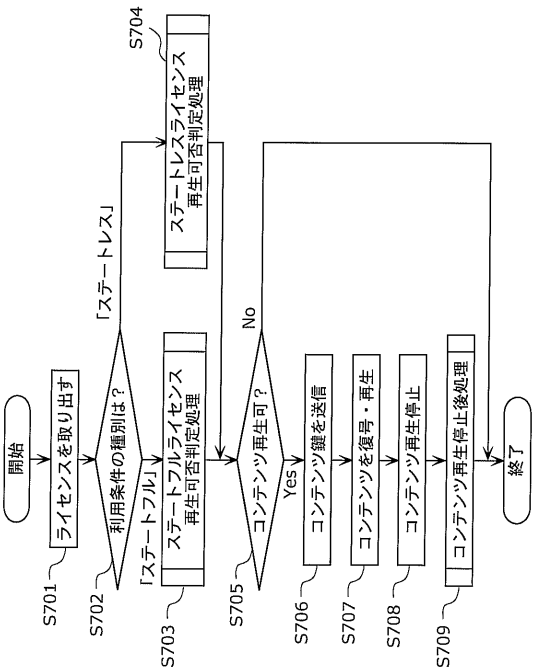
ライセンスリスト 500

201 ライセンスID	203 ドメインID	204 利用条件種別
000011	AAAAAA	ステートレス
000012	BBBBBB	ステートフル

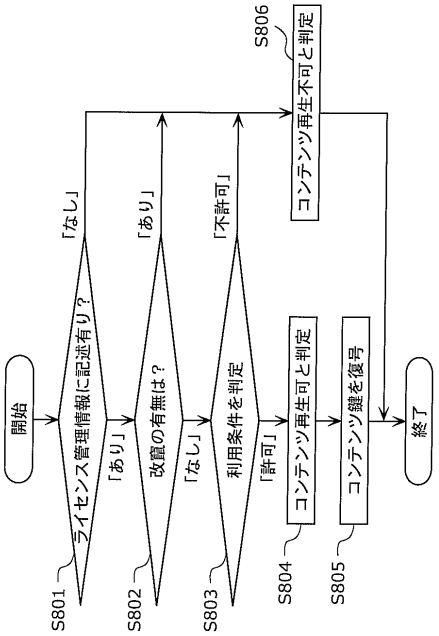
【図６】



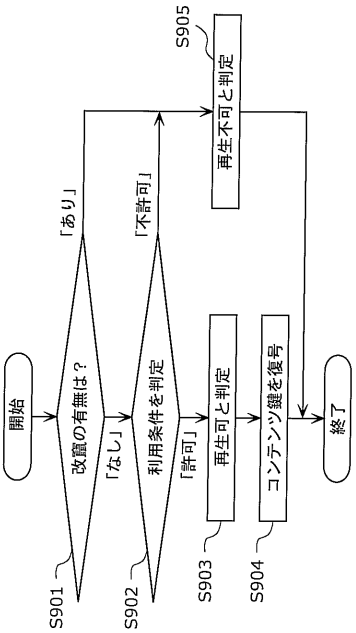
【図７】


開始
ライセンスを取り出す
S701
利用条件の種別は？
S702
「ステートフル」
「ステートレス」
S704
ステートレスライセンス
再生可否判定処理
ステートフルライセンス
再生可否判定処理
S703
コンテンツ再生可？
S705
No
Yes
コンテンツ鍵を送信
S706
コンテンツを復号・再生
S707
コンテンツ再生停止
S708
コンテンツ再生停止後処理
S709
終了

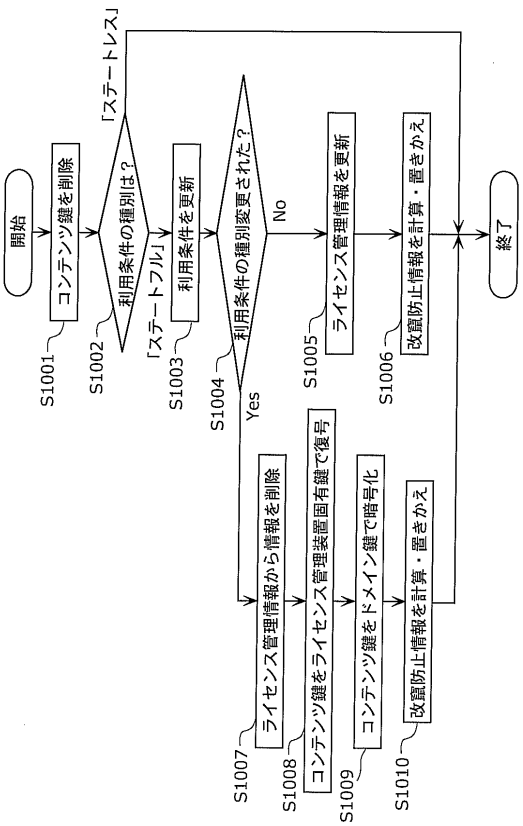
【図８】


開始
ライセンス管理情報に記述有り？
S801
「なし」
「あり」
改竄の有無は？
S802
「なし」
「あり」
利用条件を判定
S803
「不許可」
「許可」
S806
コンテンツ再生不可と判定
コンテンツ再生可と判定
S804
コンテンツ鍵を復号
S805
終了

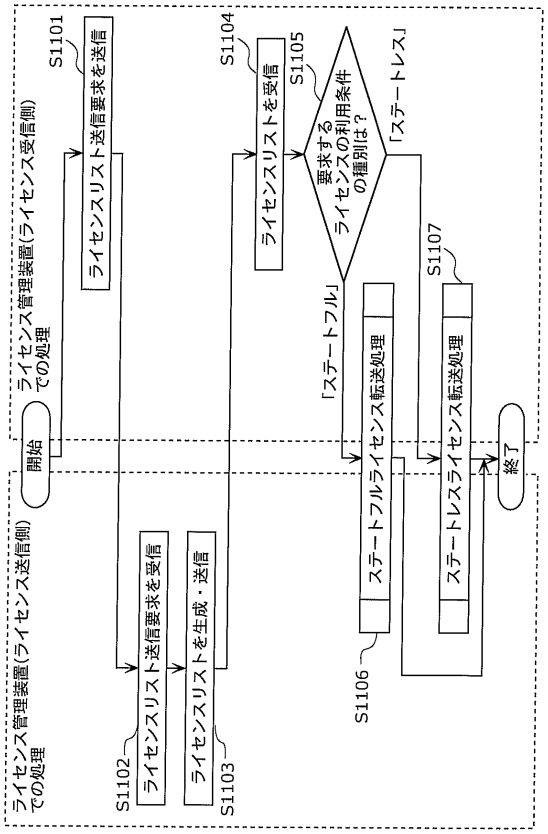
【図９】


開始
改竄の有無は？
S901
「なし」
「あり」
利用条件を判定
S902
「許可」
「不許可」
S905
再生不可と判定
再生可と判定
S903
コンテンツ鍵を復号
S904
終了

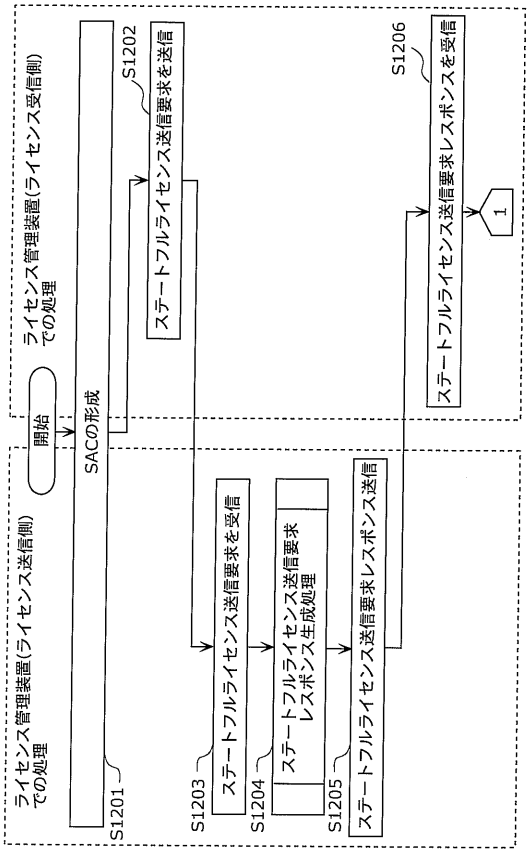
【図１０】


開始
コンテンツ鍵を削除
S1001
利用条件の種別は？
S1002
「ステートレス」
「ステートフル」
利用条件を更新
S1003
利用条件の種別変更された？
S1004
No
Yes
ライセンス管理情報を更新
S1005
改竄防止情報を計算・置きかえ
S1006
終了
ライセンス管理情報から情報を削除
S1007
コンテンツ鍵をライセンス管理装置固有鍵で復号
S1008
コンテンツ鍵をドメイン鍵で暗号化
S1009
改竄防止情報を計算・置きかえ
S1010

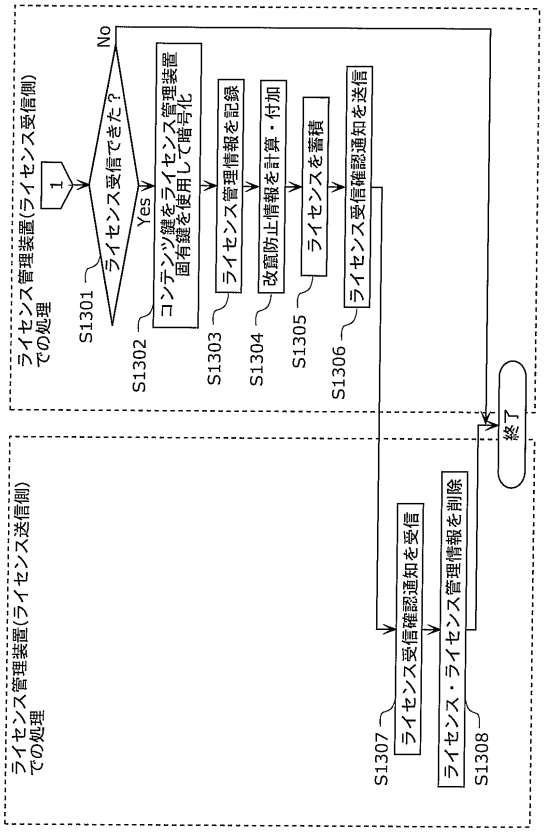
【図１１】



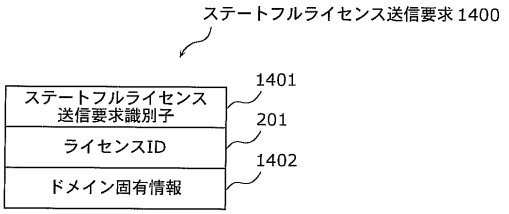
【図１２】



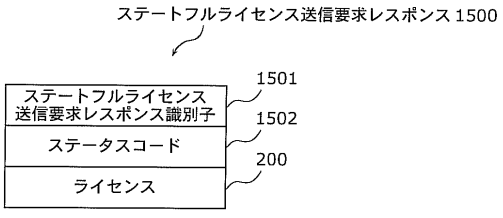
【図１３】



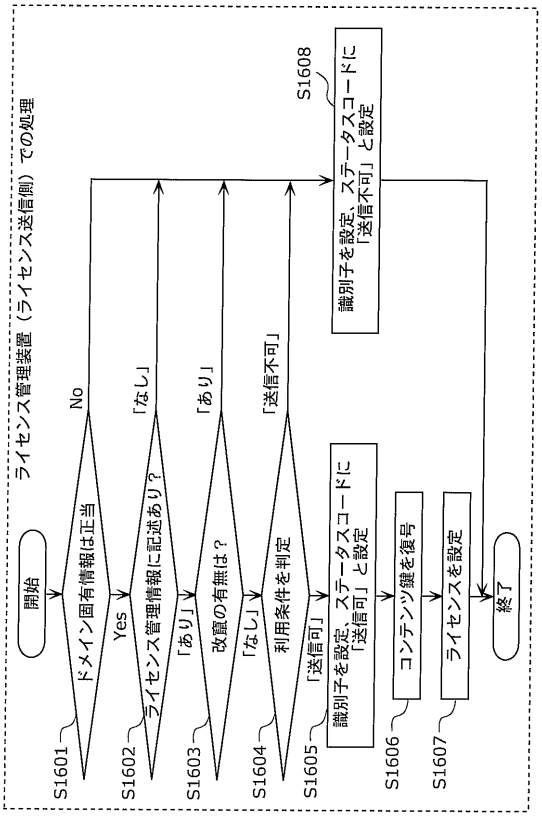
【図１４】



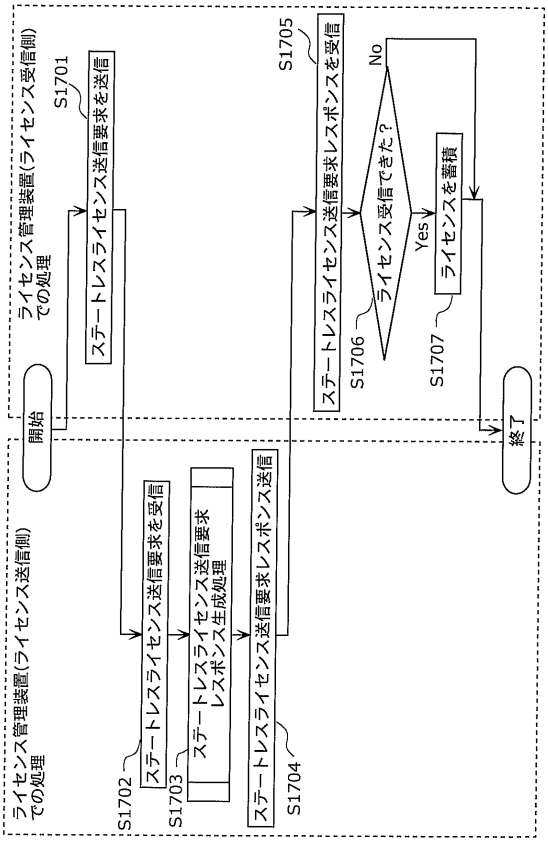
【図１５】



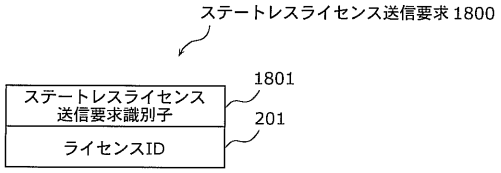
【図１６】



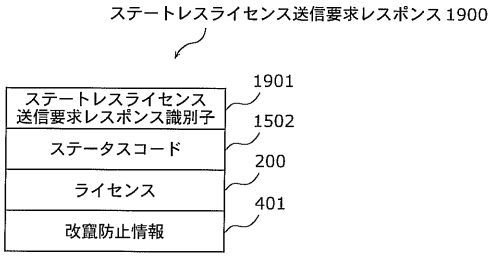
【図１７】



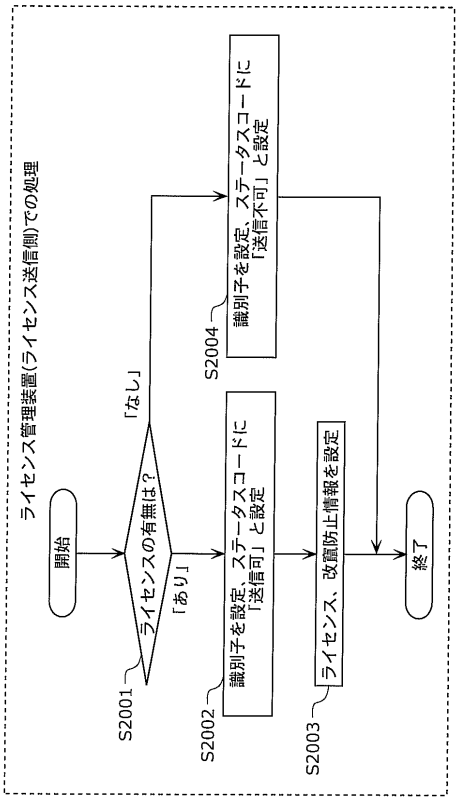
【図１８】



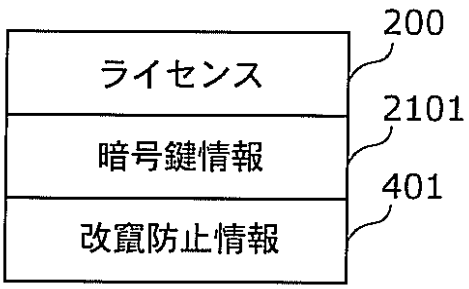
【図１９】



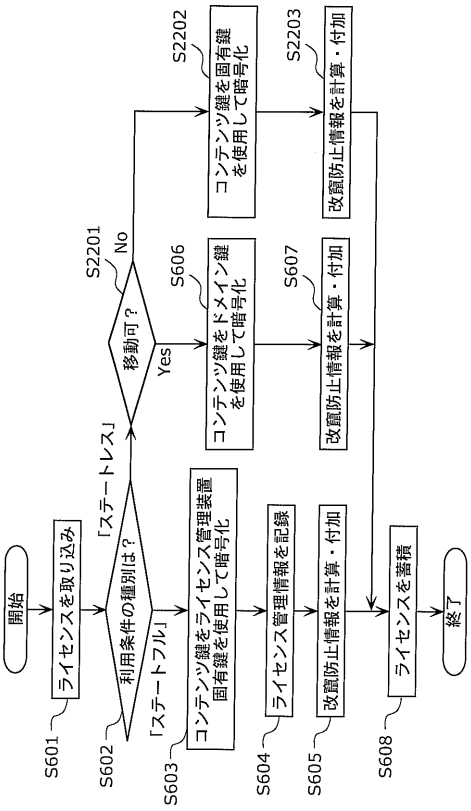
【図２０】



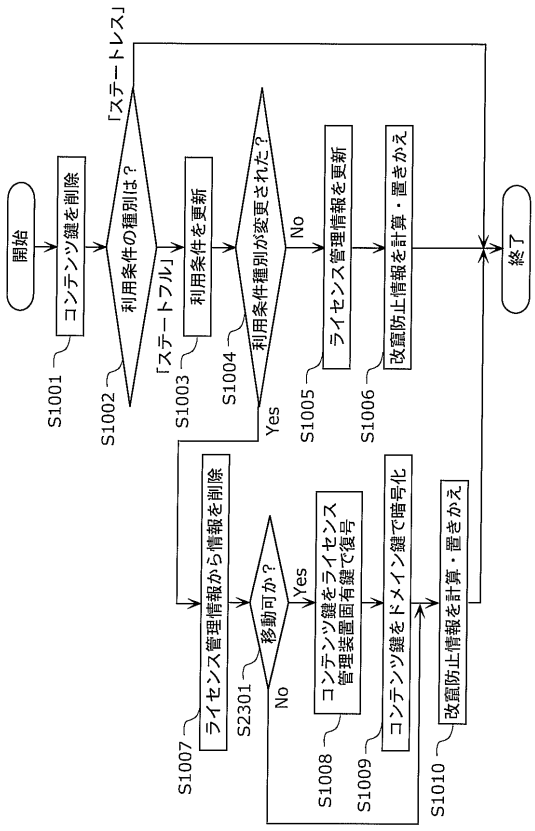
【図２１】



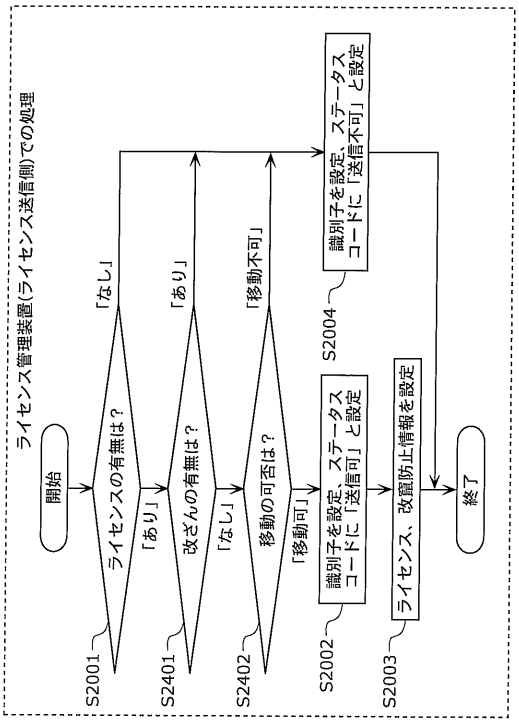
【図２２】



【図２３】



【図２４】



フロントページの続き

審査官　宮司　卓佳

(56)参考文献　国際公開第２００３／０８１４９９（WO，Ａ１）
国際公開第２００４／１０９９７２（WO，Ａ１）
国際公開第２００３／０８３７４６（WO，Ａ１）
国際公開第２００３／０９８９３１（WO，Ａ１）
特開２００４－３４８２８６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/24
H04L　9/14