(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3698968号
(P3698968)
(45)発行日　平成17年9月21日(2005.9.21)　(24)登録日　平成17年7月15日(2005.7.15)

(51)Int.Cl.[7]　F I
H04L 9/08　H04L 9/00　601B
G06F 15/00　G06F 15/00　330Z

請求項の数 6　(全 20 頁)

(21)出願番号　特願2000-238864(P2000-238864)
(22)出願日　平成12年8月2日(2000.8.2)
(65)公開番号　特開2002-51037(P2002-51037A)
(43)公開日　平成14年2月15日(2002.2.15)
審査請求日　平成15年5月27日(2003.5.27)

(73)特許権者　503121103
株式会社ルネサステクノロジ
東京都千代田区丸の内二丁目４番１号
(74)代理人　100080001
弁理士　筒井　大和
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　丸山　純一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　常広　隆司
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】著作権保護機能つきハブ装置

(57)【特許請求の範囲】
【請求項１】
１つ以上の記憶装置やコンテンツ再生装置などの情報処理装置を接続することができるハブ装置であって、
暗号化されたコンテンツデータを復号化するための鍵を格納する、計算機機能つき鍵格納手段を有し、
前記計算機機能つき鍵格納装置は、通信相手を認証する認証手段を有し、
前記認証手段によりコンテンツデータの再生装置が通信相手として認証された場合に、暗号通信を利用して、当該再生装置に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、
前記認証手段により他の記憶装置が通信相手として認証された場合に、暗号通信を利用して、当該他の記憶装置へ送信すべき鍵を読み出して当該他の記憶装置へ送信するとともに、送信した鍵を記憶内容から消去することを特徴とする鍵格納手段つきハブ装置。
【請求項２】
請求項１記載のハブ装置であって、
前記計算機機能つき鍵格納手段は、本ハブ装置に装着自在に構成されていることを特徴とするハブ装置。
【請求項３】
請求項１あるいは２記載のハブ装置を制御する制御装置であって、
前記ハブ装置に接続された各種装置の装置情報の取得手段を有し、

コンテンツを再生する場合には、前記装置情報を利用し、前記ハブ装置に接続された各種装置の中から、
当該コンテンツの再生に使用するコンテンツ再生装置を選択し、
当該コンテンツの暗号化されたコンテンツデータを格納しているコンテンツ格納装置を検索し、
当該コンテンツデータを復号するための鍵を格納している鍵格納装置を検索し、
前記手段によって決定されたコンテンツ再生装置に当該コンテンツの再生指示を送信し、
鍵格納装置間で鍵を移動する場合には、前記装置情報を利用し、前記ハブ装置に接続された各種装置の中から、
当該コンテンツデータを復号するための鍵を格納している鍵格納装置を検索し、当該鍵格納装置に鍵移動指示を送信することを特徴とする制御装置。

【請求項４】
請求項１あるいは２記載のハブ装置であって、
請求項３記載の制御装置を内蔵していることを特徴とするハブ装置。

【請求項５】
暗号化されたコンテンツデータと当該データを復号するための鍵を扱うコンテンツ再生システムであって、
請求項１あるいは２記載のハブ装置によって接続され、
請求項３記載の制御装置によって統括された、
１つ以上の鍵格納装置、１つ以上のコンテンツ格納装置、１つ以上のコンテンツ再生装置を用いてシステムを構成するための手段を有することを特徴とするコンテンツ再生システム。

【請求項６】
請求項５記載のコンテンツ再生システムにおいて、
暗号化されたコンテンツデータと、当該データを復号するための鍵と、を管理するための管理手段であって、
コンテンツを再生もしくは移動する際は、当該処理の対象コンテンツを指定すると、別個の記憶装置に格納された、暗号化されたコンテンツデータと、該コンテンツデータを復号するための鍵を、それぞれシステム上から検索し、再生もしくは移動する機能を有することを特徴とするコンテンツ管理手段。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ライセンスを利用してコンテンツの著作権を保護する技術に関し、特に、著作権保護機能を有していない情報処理システムに対して、ライセンスによる著作権保護機能を提供し、かつ該システムに接続された不特定多数の装置に格納されているライセンスおよびコンテンツの管理を行う手段およびシステムに関するものである。

【０００２】
【従来の技術】
インターネットや衛星放送などの通信手段によって、映画や音楽といったコンテンツを配信するサービスが提案されている。このようなシステムで扱われるデータはデジタル化されており、複製が容易であるため、コンテンツの著作権を保護することが重要である。そのための手段のひとつとして、例えば特開２０００－１３８６６４号公報に記載されているように、コンテンツを暗号化して配信する方法が提案されている。これは例えば公開鍵暗号方式などにより、コンテンツを暗号化し、それと同時に暗号化されたコンテンツを復号するための鍵を作成する。暗号化されたコンテンツは対応する鍵がなければ再生できないため、この鍵をライセンスとして管理することでコンテンツの不正使用を防ぎ、コンテンツ著作者らの権利を保護できる。

【０００３】
上記のような著作権保護技術に基づいたコンテンツ配信サービスにおいては、コンテンツ

のライセンスを安全に配布する方法が重要となる。

【０００４】

１つ以上の端末によって構成された情報処理システムにおいて、各端末にライセンスの使用を許可する技術については、例えば特開平１１－２０３２４９号公報に記載されているように、ライセンス付与装置に接続された通信端末に、該装置に接続されている間だけ、ライセンスを付与する方法が提案されている。

【０００５】

【発明が解決しようとする課題】

暗号化されたコンテンツデータと、該データを復号するための鍵（以下、ライセンス鍵と称する）を使用して著作権を保護する方式によって行われるコンテンツ配信サービスにおいて、販売もしくは譲渡などの手段により、ライセンス鍵が端末間で移動することを前提としたサービスを行う場合、コンテンツが不正使用されることを防ぐためには、コンテンツを復号するためのライセンス鍵が正当な所有者以外に知られてはならず、そのためにはライセンス鍵を安全に保管する鍵格納装置がなければならない。該鍵格納装置には物理的、電気的な攻撃に対しての耐性が必要である。また、該鍵格納装置は、他の鍵格納装置やコンテンツ再生装置などと安全な通信を行うため、鍵を利用する資格を認められた正当な装置以外とは通信を行わないように、通信相手の検証をする機能や、相手との通信を暗号化して行う機能などを備えなければならない。

【０００６】

ところで、現在一般に普及している例えばＰＣ等の端末や、ＨＤＤのような記憶装置は、上記のような機能を備えていないため、ライセンス鍵を利用したコンテンツ配信サービスを受けるためには、上記のような著作権保護機能がついた記憶装置を新たに用意する必要がある。しかし、既存の情報処理システムのＰＣや記憶装置を、こうした著作権保護機能つきのものに交換するのは経済的負担が大きい。

【０００７】

ここで、著作権保護機能を持たない端末にライセンス使用を許可する手法には、例えば前出の特開平１１－２０３２４９号公報に記載されているライセンス付与手法があるが、該手法においては、ライセンス付与装置は、該装置に接続されている間に限り、通信端末にコンテンツ使用の許可を与えるのであり、実際にライセンスの移動をするわけではないので、例えばライセンス付与装置から携帯端末にライセンスをダウンロードし、ライセンス付与装置から取り外した後に、該携帯端末上でコンテンツの再生を行ったり、もしくはあるライセンスを保持している端末から、他の端末へ該ライセンスを移動する、といった使用法は実現できない。

【０００８】

また、上記のような、ライセンス鍵による著作権保護機能を備えたシステムにおいては、暗号化されたコンテンツデータと、それに対応するライセンス鍵を別々に流通および格納することができる。つまり、例えば所有するコンテンツデータが複数の装置に分散して格納されており、それらに対応するライセンス鍵もまた、複数の記憶装置に分散して格納されているような運用形態もありうる。しかし、そのような運用形態においては、暗号化されたコンテンツデータとライセンス鍵を別々に管理する必要が生じ、例えばコンテンツの再生を行う場合、複数の装置の中から、ライセンス鍵とコンテンツデータの組をそろえて探し出す必要があるなど、データの管理が非常に複雑になるため、ユーザーの利便性が高いとはいえない。

【０００９】

本発明の目的は、著作権保護機能を備えていない既存の情報処理システムに、記憶装置の交換などの大きな変更を加えることなく、容易に、著作権保護機能を提供する装置と、該装置を利用した著作権保護機能つきコンテンツ再生システムと、該システムにおいて、著作権保護機能を備えたことにより処理が複雑になることをユーザに意識させずに、データ管理を行うための装置並びに方式を提案することである。

【００１０】

【課題を解決するための手段】
上記の課題を解決するため、本発明では、暗号化されたコンテンツデータを復号するためのライセンス鍵を安全に保管するための鍵格納装置において、該格納装置に格納さている鍵を不正アクセスから守るために、外部からの攻撃に対する耐性を備えたセキュアな記憶領域と、該記憶領域が、該記憶領域外部の通信相手を認証するための認証手段と、該通信を安全に行うための暗号通信手段と、を設けた。
【００１１】
また該格納装置を既存の情報処理システムに接続するためのインターフェースと、該インターフェースを使用し、該格納装置に同時に１つ以上のコンテンツ格納装置、鍵格納装置、コンテンツ再生装置、その他情報処理用機器などを接続するためのハブ装置と、を設けた。
【００１２】
加えて、著作権保護機能つきハブ装置の制御装置が、該ハブ装置に接続されたコンテンツ格納装置、鍵格納装置、コンテンツ再生装置等の各種装置の、例えば装置名、種別、製造者名、アクセス方法、装置状態等といった情報を取得するための手段と、該手段によって得られた情報等を元に、該機器群に格納されたコンテンツデータ、鍵データなどを管理するための手段と、を設け、該ハブ装置に接続された各種装置が、該格納装置に格納されたライセインス鍵を利用して、著作権保護機能を使用できるようにするための手段を設けた。
【００１３】
さらに、該手段は、管理の複雑さによるユーザーの負担を軽減し、利便性を高めるものとした。
【００１４】
【発明の実施の形態】
以下、本発明の一実施例について説明する。
【００１５】
図１は、本発明で提案する著作権保護機能つきハブ装置（以下ライセンスハブと称する）を使用した著作権保護機能つきコンテンツ再生システムを示している。
【００１６】
該コンテンツ再生システムは、暗号化されたコンテンツデータと、該データを復号するためのライセンス鍵を一組にして、コンテンツ再生装置に送信し、該コンテンツ再生装置は、該ライセンス鍵を用いて該コンテンツデータを復号、再生する。
【００１７】
ライセンスハブ装置１０１は、著作権保護機能を備えたハブ装置であり、例えばＵＳＢなどのインターフェースを使用して、既存の情報処理システムに接続し、該ライセンスハブ１０１が接続された情報処理システムに、該ライセンスハブ１０１が有する著作権保護機能を提供する。該ライセンスハブ１０１は暗号化されたコンテンツを復号するためのライセンス鍵を安全に格納するための鍵格納装置と、例えばＵＳＢなどのインターフェースを利用して、１つ以上の情報処理装置を接続するためのハブ装置と、を有する。他のハブ装置を他段接続する機能を有していても良い。また、ライセンスハブ１０１は、例えば該ライセンスハブ１０１に接続された装置ごとに、著作権保護機能を提供するか否かを設定可能にし、著作権保護機能を提供する範囲を制限する機能を設けても良い。
【００１８】
鍵格納装置１０２は、ライセンス鍵を格納するための装置であり、ライセンスハブ１０１に設けられている鍵格納装置と同様の機能を有する。鍵格納装置１０２は、例えばいくつかのライセンス鍵を記憶した状態で販売されるライセンス鍵配布用の媒体として利用したり、ライセンスハブ１０１に内蔵された鍵格納装置の記憶容量が満杯になったときなどに、ライセンスハブの増設用外部記憶装置として使用したりするなどといった用途に利用できる。
【００１９】

制御装置１０３は、ライセンスハブに直接もしくは間接に接続された装置群と、それら装置を相互に接続するためのインターフェースと（これらの装置およびインターフェースの集合を以下ライセンスネットワークと称する）、該ライセンスネットワーク上に存在するデータと、を統括制御する。制御装置１０３は、例えばＰＣなどにその機能を持たせても良いし、組み込み用マイコンとしてライセンスハブに内蔵するなどしても良い。また該制御装置１０３は、例えばＵＳＢなどの、ホストオリエンテッドなインターフェースでは、該インターフェースのホストがその役目を果たしても良いし、例えばＩＥＥＥ１３９４などのピアツーピアなインターフェースでは、該インターフェースに接続された各デバイスに内蔵された制御装置が、その機能を有しても良い。さらに、１つの制御装置による中央集中制御方式でなく、１つ以上のデバイス上に設けられた制御装置による分散制御方式としても良い。

【００２０】

コンテンツ格納装置１０４は、例えば暗号化されたコンテンツデータや、暗号化する必要のない平文のデータなどが格納される装置であり、例えばＨＤＤ、ＤＶＤ、ＣＤ－ＲＯＭなどの記憶装置をこれに充てることができる。

【００２１】

コンテンツ再生装置１０５は、暗号化されたコンテンツデータを、ライセンス鍵を用いて復号化し、再生するための装置である。鍵格納装置１０２から認証をうけるための認証手段と、該鍵格納装置１０２から鍵を受け取るための暗号通信手段と、受け取った鍵を用いて暗号化されたコンテンツデータを復号化するための暗号処理手段と、を有する。

【００２２】

該コンテンツ再生装置は、例えば据え置き型や携帯型の再生専用装置といった形態や、携帯電話やＰＤＡなどの装置に組み込むためのチップ型などの形態が可能である。

【００２３】

入力装置１０６は、例えば各種ボタンやタッチパネルで構成され、ユーザからの、データの再生、移動、削除、等の各種指示を受け付ける。制御装置１０３への入力手段であっても良いし、その他ライセンスネットワーク上の各種装置への入力装置であっても良い。制御装置１０３が、ＰＣなどの、入力装置を別に備えたものである場合は、その入力装置をこれに替えることもできる。

【００２４】

通信装置１０７は、例えば携帯電話機や据え置き型の電話機、ＬＡＮのアダプタなどに接続し、オンラインシステムやインターネットなどのネットワークを介して、例えば暗号化されたコンテンツデータやライセンス鍵を配信するコンテンツ配信センタ（不図示）にアクセスし、暗号化されたコンテンツデータやライセンス鍵を入手するのに用いられる。また該通信装置を介して、他のライセンスネットワークとライセンス鍵やコンテンツデータをやりとりすることもできる。

【００２５】

カード読取装置１０８は、例えばメモリカード１０９などの着脱可能な記憶媒体に記録されたデータを読み書きするための装置である。該メモリカードはコンテンツ格納装置１０４として利用できるほか、該メモリカードが鍵格納装置１０２と同様の著作権保護機能を有していれば、鍵格納装置１０２として利用することもできる。

【００２６】

ハブ１１０は、集線装置として１つ以上の機器を接続する機能を有し、ネットワークの拡張性を増すための装置である。他段接続を可能にして更なる拡張性を設けても良い。該ハブ１１０は必ずしもライセンスハブ１０１と同様の機能をもつ必要はなく、著作権保護機能をもたない、通常のハブ装置であってかまわない。その場合、ライセンスハブ１０１は、著作権保護機能を持たないハブ１１０を経由して、間接的にライセンスハブ１０１に接続された装置に対しても、直接ライセンスハブ１０１に接続された装置と同様に著作権保護機能を提供できるようにしても良い。そうすることで、既存の情報処理システムの一端にライセンスハブを接続することで、該システム全体に著作権保護機能を追加するという

機能を実現できる。
【００２７】
次に図１で示した各装置の構造などについてより詳細に説明する。
【００２８】
図２は本発明の一実施例が適用されたライセンスハブ１０１の構造を示す図である。該ライセンスハブ装置１０１は、ハブ装置２０１と、鍵格納装置１０２と、インターフェース用コネクタ２０２、２０３、２０４、２０５、２０６と、を有する。ハブ装置１０１は、鍵格納装置１０２と、例えば図１に示したようなコンテンツ格納装置１０４やコンテンツ再生装置１０５などの１つ以上の装置を接続する機能を有する。鍵格納装置１０２はライセンス鍵を格納するために使用され、該鍵格納装置１０２に格納されたライセンス鍵を利用することで、ライセンスハブ１０１は、自身に接続されたシステムに著作権保護機能を提供する。該鍵格納装置１０２の替わりに、あるいはそれに加えて、同様の著作権保護機能を持つ、例えばメモリカードの読み取り装置を設け、該メモリカードを着脱可能な鍵格納装置としても良い。こうすることで、鍵格納装置の記憶領域の拡張や故障時の交換などが容易に行える。また該メモリカードをコンテンツ格納装置として使用することもできる。インターフェース用コネクタ２０２、２０３、２０４、２０５、２０６はそれぞれ該ハブ装置に外部装置を接続するために使用される。この図において、コネクタ数は５つであるが、もっと少なくてもよいし、多くてもよい。加えて、ライセンスハブ装置１０１は鍵格納装置１０２のほかに、コンテンツ格納装置１０４と同様の機能を持つ装置を備えても良い。こうすることで、ライセンスハブ１０１一台でライセンス鍵および暗号化されたコンテンツデータの双方を保管することが可能になり、利便性が増す。またライセンスハブ装置１０１は制御装置１０３を内蔵することもできる。こうすることで、ライセンスハブ装置１０１一台を接続するだけで、情報処理システムに著作権保護機能を提供することができる。またその場合は、操作性向上のために、システム制御のための入力装置や表示装置を内蔵しても良い。
【００２９】
図３は、鍵格納装置１０２の構成の一例である。
【００３０】
鍵格納装置１０２は、鍵を格納するためのタンパレジスタントモジュール３０１と、ＣＰＵ３０２と、メモリ３０３と、Ｉ/Ｏ回路３０４と、を有する。
【００３１】
タンパレジスタントモジュール３０１は、セキュリティを強固にするために、外部からの攻撃に対して耐性を備え、その内部に、ＣＰＵ３０５と、メモリ３０６と、不揮発メモリ３０７と、Ｉ/Ｏ回路３０８と、を有する。ＣＰＵ３０５はタンパレジスタントモジュール３０１内の各部を統括的に制御する。また、ＣＰＵ３０５は認証機能と暗復号化機能を有している。メモリ３０６はＲＯＭおよびＲＡＭから構成される。ＲＯＭには、ＣＰＵ３０５がタンパレジスタントモジュール３０１の各部を統括的に制御するためのプログラムと、認証機能および暗復号化機能を実現するためのプログラムが格納されている。ＲＡＭは、ＣＰＵ３０５のワークエリアとして機能する。不揮発メモリ３０７には、ライセンス鍵が格納されている。Ｉ/Ｏ回路３０８はタンパレジスタントモジュール３０１内の各部が外部との通信を行うためのインターフェースである。タンパレジスタントモジュールは複数のチップによって構成してもよいし、１チップにつくりこんでも良い。その場合はチップ間の通信に用いられる信号を解析される危険が減り、セキュリティが向上される。またタンパレジスタントモジュールは同様の機能を持つ、例えば著作権保護機能つきメモリカードなどに置き換えることができる。また、その場合は該メモリカードを取り外せないようにしてもよいし、着脱可能な機構を設けても良い。
【００３２】
ＣＰＵ３０２はタンパレジスタントモジュール３０１と外部装置との通信を制御する。ＣＰＵ３０２はタンパレジスタントモジュール内のデータにアクセスするためのコマンドと、Ｉ/Ｏ回路３０４に接続されたインターフェース用のコマンドを、相互に変換する機能

を有する。メモリ３０３はＲＯＭおよびＲＡＭから構成され、ＲＯＭにはＣＰＵ３０２がコマンドを変換するためのプログラムが格納されており、ＲＡＭはＣＰＵ３０２のワークエリアとして使用される。

【００３３】

タンパレジスタントモジュール３０１、ＣＰＵ３０２、メモリ３０３、Ｉ/Ｏ回路３０４は複数チップによって構成してもよいし、１チップにつくりこんでも良い。その場合はチップ間の通信に用いられる信号を解析される危険が減り、セキュリティが向上される。

【００３４】

図４に、暗号化されたコンテンツを再生するための再生装置１０５の構成例を示す。再生装置１０５はＩ/Ｏ回路４０１と、暗復号化回路４０２と、デコーダ回路４０３と、から構成される。Ｉ/Ｏ回路４０１は、例えばＵＳＢなどのインターフェースを用いて外部装置と通信をする。暗復号化回路４０２は鍵格納装置１０２と暗号通信を行う。またライセンス鍵を使って暗号化されたコンテンツを復号する。デコーダ回路４０３は復号されたコンテンツデータを再生する機能と、コンテンツを出力するためのモニタやスピーカーとの接続機能を持つ。モニタやスピーカーは再生装置に内蔵されていても良いし、外部の機器に接続してもよい。また、コンテンツ再生装置は複数チップによって構成されても良いし、１チップ上につくりこんでも良い。その場合はチップ間の通信に用いられる信号を解析される危険が減り、セキュリティが向上される。

【００３５】

図５に上記のライセンスハブ１０１を使用して構成した著作権保護機能つきコンテンツ再生システムの一例を示す。

【００３６】

ライセンスハブ１０１に、例えばＰＣ５０１、コンテンツ格納装置５０２、携帯電話５０３、携帯型再生装置５０４、メモリカード読取装置５０５、コンテンツ再生装置５０６などを接続し、コンテンツ再生システムを構成する。

【００３７】

メモリカード５１０には、コンテンツデータを格納できる。加えて該メモリカード５１０が著作権保護機能を有しているときは、ライセンス鍵を格納することもできる。また、このメモリカードを他のコンテンツネットワークや各種再生装置に取り付けてコンテンツの移動や再生を行うこともできる。

【００３８】

ＰＣ５０１は、例えばライセンスハブの制御装置としての機能、ライセンス鍵の発行を受けるため、鍵格納装置がコンテンツ配信センターと行う通信を、インターネットを使用して中継する機能、インターネットからコンテンツデータをダウンロードして、内蔵のＨＤＤに格納する機能、などを有する。

【００３９】

コンテンツ格納装置５０２は、例えばＨＤＤ、ＤＶＤ、ＣＤ－ＲＯＭなどの記憶装置であり、暗号化されたコンテンツデータなどを格納するのに用いる。また内蔵用コンテンツ格納装置５０９としてライセンスハブに内蔵することもできる。

【００４０】

携帯電話５０３は、例えばライセンスネットワークや、コンテンツ配信センタ（不図示）からライセンス鍵やコンテンツデータをダウンロードする機能や、内蔵する記憶装置に格納した、コンテンツの再生をする機能などを有する。内蔵する記憶装置は例えば着脱可能なメモリカード５１０のようなものでも良い。

【００４１】

携帯型再生装置５０４は、例えばライセンスネットワークからライセンス鍵およびコンテンツデータを内蔵記憶装置にダウンロードして、コンテンツの再生を行う。例えばメモリカード５１０などを着脱可能な記憶装置として利用することもできる。

【００４２】

コンテンツ再生装置５０６は、ライセンス鍵を用いて、暗号化されたコンテンツを復号し

、モニタ５０７やステレオ５０８などに出力する。
【００４３】
図５において各装置はケーブルによって接続されているが、これは例えばBlueToothのような、無線による通信形態であっても良い。
【００４４】
図６、７にライセンスハブ装置１０１の実施形態例を示す。
【００４５】
図６において、ライセンスカード６０１は例えばカード型のライセンスハブ装置であり、例えばＰＣカード、コンパクトフラッシュ、ＵＳＢなどのインタフェース用コネクタを有し、ノートパソコン６０２やＰＤＡ（不図示）等に直接接続できる。また該インターフェースとは別に、例えばＵＳＢやＩＥＥＥ１３９４のような各種インターフェース用のコネクタを１つ以上有し、該インターフェースに接続される各種装置に著作権保護機能を提供する。またはそれらコネクタの替わりに例えばBlueToothのような無線通信インターフェースを内蔵しても良い。また、前述のコンテンツ再生チップを内蔵しても良い。こうすることで、ライセンスカード６０１を取り付けるだけでコンテンツ再生が行える。記憶容量拡張等のために、メモリカード型鍵格納装置の着脱機構を設けることもできる。
【００４６】
図７に示すライセンスボード７０１は、ＰＣＩボード型のライセンスハブ装置であり、該ボードは例えばＵＳＢのような各種インターフェース用のコネクタを１つ以上有し、ＰＣのＰＣＩバス７０２に接続することでライセンスハブ機能を実現する。ＰＣＩバス以外に例えばＩＳＡなどのバスを利用しても良い。コンテンツを再生する場合は、セキュリティの関係上、ＰＣＩバス上に復号化されたコンテンツデータを流さないようにするため、グラフィックボード７０３やサウンドボード７０４には、例えば図４に示したような、コンテンツ再生用のチップを搭載する。
【００４７】
以上、著作権保護機能つきコンテンツ再生システムおよび、該システム上のライセンスネットワークの構成例について説明した。次に、該システムにおける、コンテンツ再生およびライセンス移動の手順と、それを実現するソフトウェアについて説明する。
【００４８】
図８にライセンスハブ装置１０１を使用した、ライセンスネットワーク構成例の概略を示す。ライセンスハブ１０１には１つ以上の鍵格納装置と、１つ以上のコンテンツ格納装置と、１つ以上のコンテンツ再生装置と、を接続できる。これらの装置はライセンスネットワーク上のどこにあっても良く、ライセンスハブはこれらの装置間で行われる、例えばライセンス鍵、暗号化されたコンテンツデータ、暗号化する必要のない平文のデータなどの通信を中継する。
【００４９】
同図では、鍵格納装置８０１、８０２、コンテンツ格納装置８０３、８０４、再生装置８０５、８０６はそれぞれ２台づつ接続されているが、これらはそれぞれもっと少なくても良いし、多くても良い。コンテンツの再生に関しては、ライセンスハブ１０１に内蔵される装置も含めてそれぞれの装置が１台以上ライセンスネットワークに接続されていれば良い。
【００５０】
制御用装置１０３は例えばライセンスハブに接続されたＰＣなどを用いることができるし、ライセンスネットワークを管理する機能を持つ、例えば組み込み型マイコンなどの装置をライセンスハブに内蔵しても良い。
【００５１】
制御装置１０３は、ライセンスハブ１０１もしくは該ハブ装置が所属するライセンスネットワークに接続された各種装置の、例えば、装置名、種別、製造者、アクセス方法、装置状態のリストといった情報を管理している。装置状態については、例えば各鍵格納装置に格納されているライセンス鍵のリスト、各コンテンツ格納装置に格納されているコンテン

ツデータのリスト、各再生装置の再生可能コンテンツのリスト、などが挙げられる。

【００５２】

該制御装置１０３は、上記のような情報を利用して、ユーザーからのコンテンツの再生やライセンス鍵の移動指示を受けた場合には、接続されている１つ以上の鍵格納装置、コンテンツ格納装置、コンテンツ再生装置の中から、当該指示の処理を実行するのに適当な装置を決定し、それらの装置にコンテンツの再生あるいはライセンス鍵の移動などの指示を行う。鍵格納装置とコンテンツ再生装置は、それぞれライセンス鍵の通信を安全に行うための、相手装置の認証手段と暗号通信手段を有しているので、制御装置から指示が出された後は、指示を受けた機器同士で、コンテンツの再生あるいはライセンス鍵の移動などの処理を行う。暗号化されたコンテンツの移動やコピーの場合は、特にセキュリティを考慮する必要はないため、コンテンツ格納装置は独自の通信手段を有する必要はないので、それらの処理においては、制御装置が処理手順の管理、制御を行う。

【００５３】

図９はコンテンツを再生する際に使用されるアプリケーションのユーザーインターフェースの一例である。このアプリケーションは、例えばライセンスネットワークに接続された制御装置上で動作し、コンテンツの再生、ライセンス鍵の移動などの手順を制御する。ユーザーインターフェースは例えばディスプレイパネル９０１、操作パネル９０２、再生可能コンテンツリスト９０３、ライセンスネットワーク接続装置リスト９０６などからなる。

【００５４】

ディスプレイパネル９０１は、現在のアプリケーションの動作状況や、コンテンツの名前、記録時間、作者名、配布者名、ライセンス所持者名、といった属性情報などを表示する。

【００５５】

操作パネル９０２は、再生、停止、まき戻し、早送りといった操作を行うためのボタン類を配置する。

【００５６】

再生可能コンテンツリスト９０３には、現在ライセンスネットワークにおいて再生することが可能なコンテンツの一覧を表示する。コンテンツリスト９０３には各コンテンツの名前や記録時間などの属性情報９０４、９０５などを表示する。またコンテンツデータはあるがライセンス鍵がないコンテンツや、ライセンス鍵はあるのにコンテンツデータがないというような再生不可能なコンテンツについては、コンテンツ自体を表示をしない、色を変えて表示する、アイコンによって目印をつける、などの表示方法により再生可能なコンテンツと区別し、ユーザの利便性を高める。このような表示方法をすることで、ユーザーはコンテンツ鍵とコンテンツデータが別々に管理されているというシステムの複雑さを意識せずにすむ。

【００５７】

ライセンスネットワーク接続装置リスト９０６には、ライセンスネットワークに接続され、認識されている各種装置のリストを表示する。該リスト９０６には、例えばコンテンツ再生装置９０７、鍵格納装置９０８、コンテンツ再生装置９０９などを示すアイコンを表示し、該アイコンなどにより、コンテンツの再生や、移動の際に使用する装置を指定できるようにする。

【００５８】

また、コンテンツの移動に際しては、コンテンツ名と移動先を指定するだけで、該コンテンツの暗号化されたコンテンツデータと、該データを復号するためのライセンス鍵の所在を検索し、コンテンツデータの移動もしくはコピーと、ライセンス鍵の移動と、を一度に行う機能を設ける。このようにすることで、ユーザーは移動対象コンテンツデータや対象ライセンス鍵を格納した装置を別々に探し出し、それぞれについて格納場所を指定する必要がなくなり利便性が増す。また、ユーザーが移動を指示するために必要な動作が減るため、操作性も向上する。

【００５９】
また、ユーザーが希望するライセンス鍵もしくはコンテンツデータをライセンスネットワーク上の装置群から検索する機能を設ける。またこの検索処理の結果をそれぞれライセンス鍵リストもしくはコンテンツデータリストとして、該データの名称などの属性情報とともに表示する機能を設ける。
【００６０】
以上、ライセンスハブ装置１０１を用いた著作権保護機能つきコンテンツ再生システムの動作について述べた。次に、該コンテンツ再生システム上でのコンテンツ再生や、ライセンス鍵の移動の各手順をより詳しく説明する。
【００６１】
既に述べたように、ライセンスハブに接続された制御装置は、ライセンスネットワークに接続され、コンテンツ再生に際し使用可能な再生装置の装置情報を保持しているが、それらの情報は、ライセンスネットワークの状態の変化に応じて更新をする必要がある。更新の方法には、例えば制御装置に、ライセンスネットワークに接続されている再生装置のリストを持たせ、定期的にネットワーク上の全ての機器をスキャンし、ネットワーク上に新たな再生装置が発見されたり、ネットワークから見失った機器があった場合に、再生装置リストを更新するという方法がある。あるいは、ネットワークに再生装置が接続（もしくは取り外し）された時に、ネットワーク上に再生装置の新規接続（もしくは取り外し）を示す信号を流し、その信号をトリガにして更新処理を行っても良いし、もしくは各装置が定期的に自身の存在を示す信号をネットワーク上に発信し、該信号を制御装置が集計することで、リストを更新することにしても良い。
【００６２】
図１０は、制御装置が定期的にライセンスネットワークをスキャンする方式による再生装置認識処理のフローチャートの例である。ホストは定期的にライセンスネットワーク上に接続された装置をスキャンし（Ｓ１００１）、新規に接続された再生装置を探す（Ｓ１００２）。ライセンスネットワーク上に新しい再生装置が接続された場合は、該再生装置に装置情報を要求し（Ｓ１００３）、それを受けた再生装置は制御装置に装置情報を送信する（Ｓ１００４）。装置情報を受け取った制御装置は保持している再生装置リストに該再生装置を追加する（Ｓ１００５）。ライセンスネットワークのスキャン時に（Ｓ２００１）、取り外され見失った再生装置がある場合は（Ｓ２００２）、見失った再生装置を再生装置リストから削除する。
【００６３】
また、制御装置はライセンスネットワークに接続された鍵格納装置の情報や、コンテンツ格納装置の情報を保持していなければならない。この場合も、再生装置認識の場合と同様に、制御装置にそれぞれの装置の装置情報リストを持たせておき、定期的に更新する、という方法が可能である。この方式を利用した鍵格納方式の認識法のフローチャートを図１１に、コンテンツ格納装置の認識法のフローチャートを図１２にそれぞれ示す。どちらにおいても、新しく装置を発見した時（Ｓ３００１、Ｓ５００１）あるいは見失った時（Ｓ４００１、Ｓ６００１）に装置情報リストを更新する。これらの処理は、コンテンツ再生装置の認識方法で既に述べたように、ネットワークに送信される装置の接続信号をトリガにして行っても良い。また、ネットワーク上に各装置が自身の存在を示す信号を定期的に発信することにしても良い。
【００６４】
図１３はコンテンツ再生時に使用する装置を決定する手順を説明する図である。
【００６５】
ライセンスネットワークに２つ以上の再生装置が存在している場合は、コンテンツの再生に際し、制御装置はどのコンテンツ再生装置を使用するのか決定しなければならない（Ｓ７００１）。該コンテンツを再生可能なコンテンツ再生装置がネットワーク上に存在する場合は、該コンテンツ再生装置を使用する（Ｓ７００３）。また同時に複数の再生装置が該コンテンツの再生をサポートしている場合は、それらの中から１つあるいは複数の再生

装置を使用することにする。複数の利用可能再生装置から使用する再生装置を決定する際には、再生装置の装置情報を利用し、たとえばもっとも再生性能が良いものを自動的に選択するような機能を設けても良いし、ユーザーが自身で選択可能なようにしても良い。また該コンテンツを再生可能なコンテンツ再生装置が存在しないときにはエラーとして処理する（Ｓ７０１０）。次に再生対象のコンテンツに対応したライセンス鍵を探さなければならない。ライセンスネットワーク上に１つ以上の鍵格納装置が接続されている場合は、制御装置は鍵格納装置リスト上の各鍵格納装置に格納されたライセンス鍵を検索し、該ライセンス鍵がライセンスネットワーク上に存在するか確認する（Ｓ７００４）。該ライセンス鍵が発見された場合は、該ライセンス鍵を格納している鍵格納装置を鍵格納装置として登録する（Ｓ７００６）。該ライセンス鍵が発見されなかったときは、コンテンツの再生が不可能であるので、エラーとして処理を終了する（Ｓ７０１０）。最後に再生対象コンテンツの、暗号化されたコンテンツデータを探す（Ｓ７００７）。ライセンスネットワーク上に１つ以上のコンテンツ格納装置が接続されている場合、制御装置はライセンスネットワークに接続された各コンテンツ格納装置上のコンテンツデータを検索する。再生対象コンテンツデータが発見された場合は、該コンテンツデータを格納しているコンテンツ格納装置をコンテンツ再生に際して使用する（Ｓ７００９）。目的のコンテンツデータが発見されなかったときは、コンテンツの再生が不可能であるので、エラーとして処理する（Ｓ７０１０）。

【００６６】

図１４はライセンス鍵を鍵格納装置間で移動する時に使用する装置を決定する手順を図示している。ライセンスネットワークに２つ以上の鍵格納装置が接続されている場合に、ある鍵格納装置に任意のライセンス鍵を移動させる場合、対象とするライセンス鍵を保持している鍵格納装置を検索する必要がある。制御装置は鍵格納装置リストに記載された鍵格納装置に格納されているライセンス鍵を検索し（Ｓ８００１）、対象とするライセンス鍵が発見された場合は、該ライセンス鍵を格納している鍵格納装置を移動元鍵格納装置として登録する（Ｓ８００３）。該ライセンス鍵を格納している鍵格納装置が発見されない場合は、エラーとして処理する（Ｓ８００４）。

【００６７】

図１５はコンテンツを再生する際に行われる処理のフローチャートであり、ライセンス鍵と暗号化されたコンテンツデータをもとにコンテンツを再生する手順を示す。コンテンツの再生に際しては、再生に使用する再生装置、鍵を格納している鍵格納装置、暗号化されたコンテンツデータを格納しているコンテンツ格納装置をそれぞれ特定する必要がある。各装置を特定する処理は図１３において例示したように、あらかじめ行っておく。

【００６８】

再生処理は、例えばユーザーからコンテンツ再生指示が与えられた時などに開始され、まず制御装置から再生装置にコンテンツの再生指示が与えられる（Ｓ９００１）。次に該再生装置はライセンス鍵を格納している鍵格納装置に、ライセンス鍵の送信を要求する（Ｓ９００２）。その要求を受けた鍵格納装置は、要求元の再生装置が正当なものであるかを認証し（Ｓ９００３）、正しく認証された場合は格納しているライセンス鍵を検索し、対象とするライセンス鍵が存在しているかを確認する（Ｓ９００５）。対象とするライセンス鍵を有している場合は、暗号通信を利用して該ライセンス鍵を再生装置に送信し（Ｓ９００７）、再生装置は復号する対象となるコンテンツデータをコンテンツ格納装置から読み出した後に（Ｓ９００８）、該コンテンツデータを復号・再生する（Ｓ９００９）。Ｓ９００５において該ライセンス鍵が発見されない場合は、再生が不可能であるのでエラーとなる（Ｓ９０１０）。

【００６９】

図１６はコンテンツ再生時に鍵格納装置とコンテンツ再生装置との間で行われる通信手順の一例である。

【００７０】

コンテンツ再生装置の暗復号化回路は、図のＴ１００１において、自身の認証データと、

再生対象の暗号化されたコンテンツデータの識別情報と、予め保持しているメディアクラス秘密鍵ＫＰＭＣと対のメディアクラス公開鍵ＫＯＭＣとを含んだライセンス鍵送信指示を作成し、これをコンテンツ格納装置の鍵格納装置に送信する。

【００７１】

これを受けて鍵格納装置のＣＰＵは、図のＴ１００２において、コンテンツ再生装置の認証、および、不揮発メモリに要求されたライセンス鍵が格納されていることの確認を行う。それから、ＣＰＵは、セッション鍵ＫＳ１を生成し（Ｔ１００３）、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵ＫＯＭＣで暗号化して、当該指示の送信元であるコンテンツ再生装置に送信する（Ｔ１００４）。

【００７２】

これを受けて、コンテンツ再生装置の暗復号化回路は、暗号化されたセッション鍵ＫＳ１を予め保持しているメディアクラス秘密鍵ＫＰＭＣで復号し、セッション鍵ＫＳ１を得る（Ｔ１００５）。それから、セッション鍵ＫＳ２を生成し（Ｔ１００６）、これと、予め保持しているメディア固有秘密鍵ＫＰＭと対のメディア固有公開鍵ＫＯＭとを、セッション鍵ＫＳ１で暗号化して、コンテンツ格納装置の鍵格納装置に送信する（Ｔ１００７）。

【００７３】

これを受けて、鍵格納装置のＣＰＵは、暗号化されたセッション鍵ＫＳ２とメディア固有公開鍵ＫＯＭを、セッション鍵ＫＳ１で復号し、セッション鍵ＫＳ２とメディア固有公開鍵ＫＯＭを得る（Ｔ１００８）。そして、送信を要求されているライセンス鍵ＫＣをメディア固有公開鍵ＫＯＭＣで暗号化し、さらにこれをセッション鍵ＫＳ２で暗号化して、ライセンス鍵送信指示の送信元であるコンテンツ再生装置に送信する（Ｔ１００９）。

【００７４】

これを受けて、コンテンツ再生装置の暗復号化回路は、暗号化されたライセンス鍵ＫＣをセッション鍵ＫＳ２とメディア固有秘密鍵ＫＰＭを用いて復号し、ライセンス鍵ＫＣを得る（Ｔ１０１０）。

【００７５】

以上、コンテンツデータを再生する場合の動作の一例について説明した。

【００７６】

図１７はライセンス鍵移動処理のフローチャートであり、２つの鍵格納装置間で鍵を移動する際の手順を示す。ここでは既に対象とするライセンス鍵を保持している移動元鍵格納装置１０２’があらかじめ特定されている必要がある。

【００７７】

各装置を特定する処理は例えば図１３におけるＳ７００４～Ｓ７００６の手順によって行うことができる。

【００７８】

ライセンス鍵移動処理は、例えばユーザーからライセンス鍵移動指示が与えられた時などに開始され、まず制御装置１０３から移動先鍵格納装置装置１０２にライセンス鍵の移動指示が与えられる（ＳＡ００１）。次に該移動先鍵格納装置１０２はライセンス鍵を格納している移動元鍵格納装置１０２’に、ライセンス鍵の送信を要求する（ＳＡ００２）。その要求を受けた移動元鍵格納装置は、要求元の移動先鍵格納装置が正当なものであるかを認証し（ＳＡ００３）、正しく認証された場合は格納しているライセンス鍵を検索し、対象とするライセンス鍵が存在しているかを確認する（ＳＡ００５）。対象とするライセンス鍵を有している場合は、暗号通信を利用して該ライセンス鍵を移動先鍵格納装置に送信し（ＳＡ００７）、移動元鍵格納装置は該ライセンス鍵を記憶領域から削除する（ＳＡ００８）。その後移動先鍵格納装置は受け取ったライセンス鍵を記憶領域に格納する（ＳＡ００９）。ＳＡ００５において該ライセンス鍵が発見されない場合は、再生が不可能であるのでエラーとなる。

【００７９】

図１８はライセンス鍵を２つの鍵格納装置間で移動する際に、移動元の鍵格納装置と移動先の鍵格納装置との間でおこなわれる通信手順を示す。

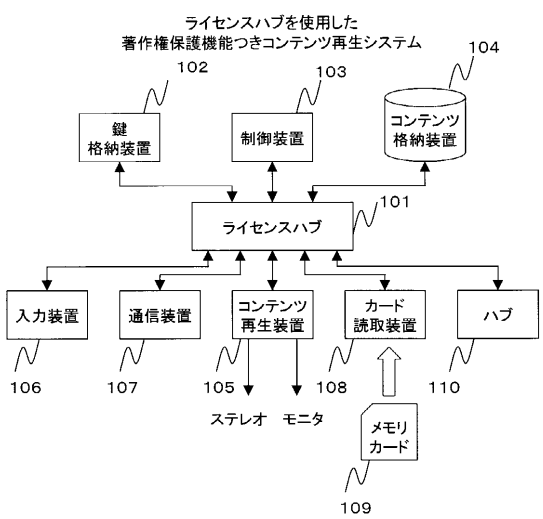
【００８０】
移動先鍵格納装置の暗復号化回路は、図のＴ２００１において、自身の認証データと、再生対象の暗号化されたコンテンツデータの識別情報と、予め保持しているメディアクラス秘密鍵Ｋ'ＰＭＣと対のメディアクラス公開鍵Ｋ'ＯＭＣとを含んだライセンス鍵送信指示を作成し、これを移動元の鍵格納装置に送信する。
【００８１】
これを受けて移動元の鍵格納装置のＣＰＵは、図のＴ２００２において、移動先鍵格納装置の認証、および、不揮発メモリに要求されたライセンス鍵が格納されていることの確認を行う。それから、ＣＰＵは、セッション鍵ＫＳ１を生成し（Ｔ２００３）、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵Ｋ'ＯＭＣで暗号化して、当該指示の送信元である移動先鍵格納装置に送信する（Ｔ２００４）。
【００８２】
これを受けて、移動先鍵格納装置の暗復号化回路は、暗号化されたセッション鍵Ｋ'Ｓ１を予め保持しているメディアクラス秘密鍵Ｋ'ＰＭＣで復号し、セッション鍵Ｋ'Ｓ１を得る（Ｔ２００５）。それから、セッション鍵Ｋ'Ｓ２を生成し（Ｔ２００６）、これと、予め保持しているメディア固有秘密鍵Ｋ'ＰＭと対のメディア固有公開鍵Ｋ'ＯＭとを、セッション鍵Ｋ'Ｓ１で暗号化して、移動元鍵格納装置の鍵格納装置に送信する（Ｔ２００７）。
【００８３】
これを受けて、移動元鍵格納装置のＣＰＵは、暗号化されたセッション鍵Ｋ'Ｓ２とメディア固有公開鍵Ｋ'ＯＭを、セッション鍵Ｋ'Ｓ１で復号し、セッション鍵Ｋ'Ｓ２とメディア固有公開鍵Ｋ'ＯＭを得る（Ｔ２００８）。そして、送信を要求されているライセンス鍵Ｋ'Ｃをメディア固有公開鍵Ｋ'ＯＭＣで暗号化し、さらにこれをセッション鍵Ｋ'２で暗号化して、ライセンス鍵送信指示の送信元である移動先鍵格納装置に送信する（Ｔ２００９）。
【００８４】
これを受けて、移動先鍵格納装置の暗復号化回路は、暗号化されたライセンス鍵Ｋ'Ｃをセッション鍵Ｋ'Ｓ２とメディア固有秘密鍵Ｋ'ＰＭを用いて復号し、ライセンス鍵Ｋ'Ｃを得る（Ｔ２０１０）。
【００８５】
以上、本発明の１実施形態について説明した。
【００８６】
【発明の効果】
以上、本発明によれば、コンテンツ配信サービス用のシステムなどの、著作権保護を必要とするシステムにおいて、著作権保護機能を備えていない既存の情報処理システムに、記憶装置の交換などの大きな変更を加えることなく、容易に、著作権保護機能を提供することができる。また、ユーザーはシステムが著作権保護機能を備えたことによるデータ構造の複雑化を意識せずに、コンテンツおよびライセンス鍵の管理を行うことができる。
【図面の簡単な説明】
【図１】本発明の一実施形態が適用された著作権保護機能つきコンテンツ再生システムの概略構成を示す図である。
【図２】図１に示すライセンスハブ１０１の概略構成を示す図である。
【図３】図１に示す鍵格納装置１０２の概略構成を示す図である。
【図４】図１に示すコンテンツ再生装置１０５の概略構成を示す図である。
【図５】本発明の一実施形態が適用されたコンテンツ再生システムの概観の一例を示す図である。
【図６】図５で示したライセンスハブ装置１０１の適用形態の一例を示す図である。
【図７】図５で示したライセンスハブ装置１０１の適用形態の一例を示す図である。
【図８】図５で例示したコンテンツ再生システムにおけるライセンスネットワーク内部での処理を説明するための図である。

【図９】コンテンツ再生システムにおいて、コンテンツを再生する際に使用されるアプリケーションのユーザーインターフェースの一例を示す図である。
【図１０】本発明の一実施形態が適用された制御装置の、再生装置認識動作を説明するフロー図である。
【図１１】本発明の一実施形態が適用された制御装置の、鍵格納装置認識動作を説明するフロー図である。
【図１２】本発明の一実施形態が適用された制御装置の、コンテンツ格納装置認識動作を説明するフロー図である。
【図１３】本発明の一実施形態が適用された制御装置が、コンテンツ再生動作時に使用する装置を決定する動作を説明するフロー図である。
【図１４】本発明の一実施形態が適用された制御装置が、ライセンス鍵移動時に使用する装置を決定する動作を説明するフロー図である。
【図１５】本発明の一実施形態が適用されたコンテンツ再生システムにおける、コンテンツ再生動作を説明するフロー図である。
【図１６】図１５に示すフロー図におけるコンテンツ再生装置と鍵格納装置間のデータのやり取りの一例を説明するためのシーケンス図である。
【図１７】本発明の一実施形態が適用されたコンテンツ再生システムにおける、鍵格納装置間のライセンス鍵移動動作を説明するフロー図である。
【図１８】図１７に示すフロー図における移動元鍵格納装置と移動先鍵格納装置間のデータのやり取りの一例を説明するためのシーケンス図である。
【符号の説明】
１０１…ライセンスハブ
１０２、８０１、８０２…鍵格納装置
１０３…制御装置
１０４、５０２、５０９、８０３、８０４…コンテンツ格納装置
１０５、５０６、８０５、８０６…コンテンツ再生装置
１０６…入力装置
１０７…通信装置
１０８、５０５…カード読取装置
１０９、５１０…メモリカード
１１０…ハブ
２０１…ハブ装置
２０２、２０３、２０４、２０５、２０６…インターフェース用コネクタ
３０１…タンパレジスタントモジュール
３０２、３０５…ＣＰＵ
３０３、３０６…メモリ
３０４、３０８、４０１…Ｉ/Ｏ回路
３０７…不揮発メモリ
４０２…暗復号化回路
４０３…デコーダ回路
５０１…ＰＣ
５０３…携帯電話
５０４…携帯型コンテンツ再生装置
５０７…モニタ
５０８…ステレオ
６０１…ライセンスカード
６０２…ノートＰＣ
７０１…ライセンスボード
７０２…ＰＣＩバス
７０３…グラフィックボード

７０４…サウンドボード
８０７、８０８、８０９、８１０…ライセンス鍵
８１１、８１２、８１３、８１４…暗号化されたコンテンツ
９０１…ディスプレイパネル
９０２…操作パネル
９０３…再生可能コンテンツリスト
９０４、９０５…コンテンツ属性情報アイコン
９０６…ライセンスネットワーク接続装置リスト
９０７、９０８、９０９…接続装置情報アイコン

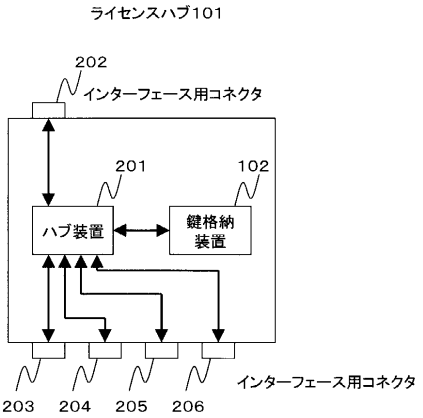
【図１】

図1



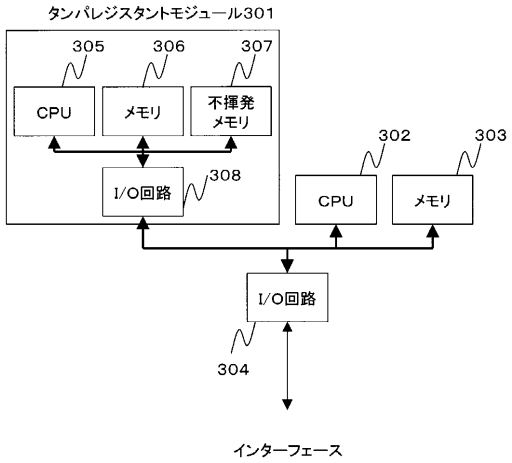
【図２】

図2



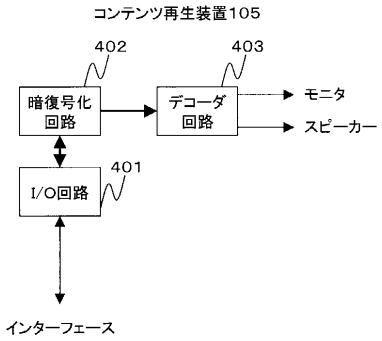
【図３】

図3



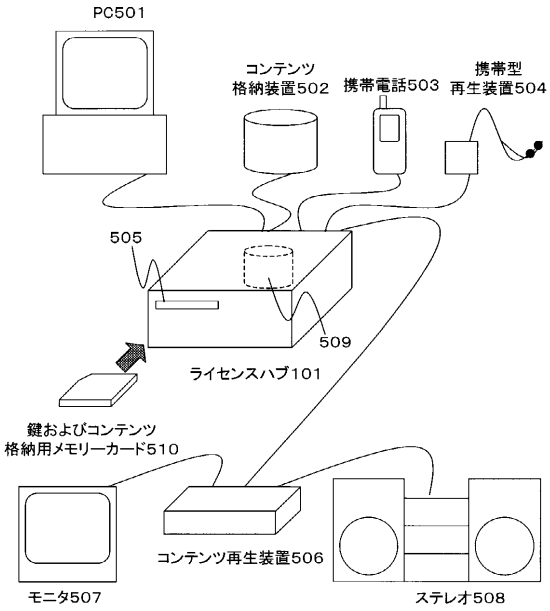
【図４】

図4



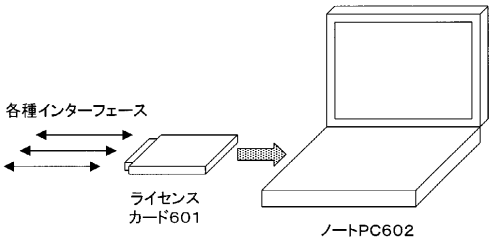
【図５】

図5



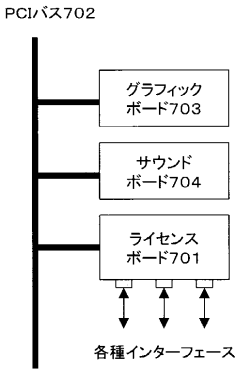
【図６】

図6



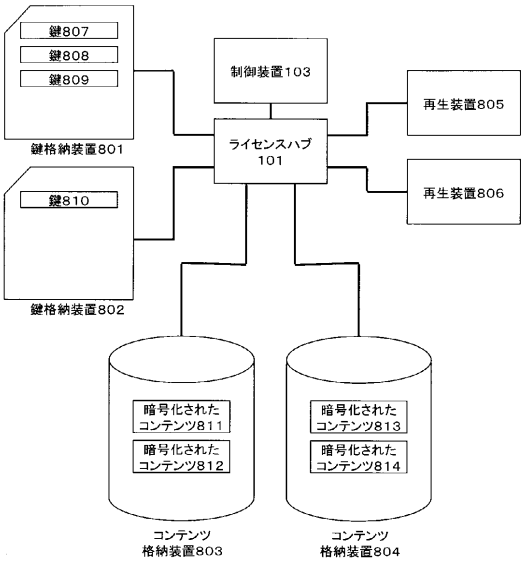
【図７】

図7



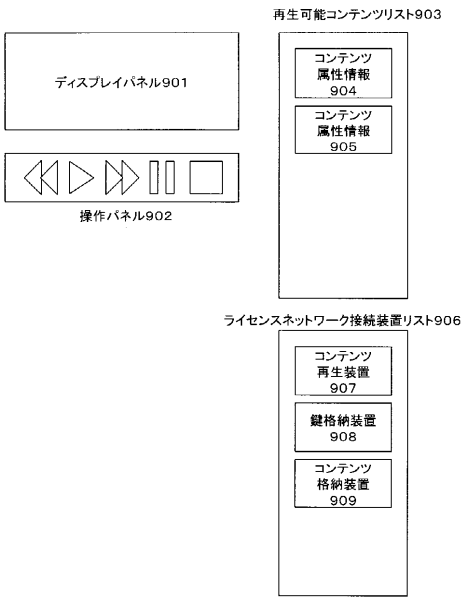
【図８】

図8



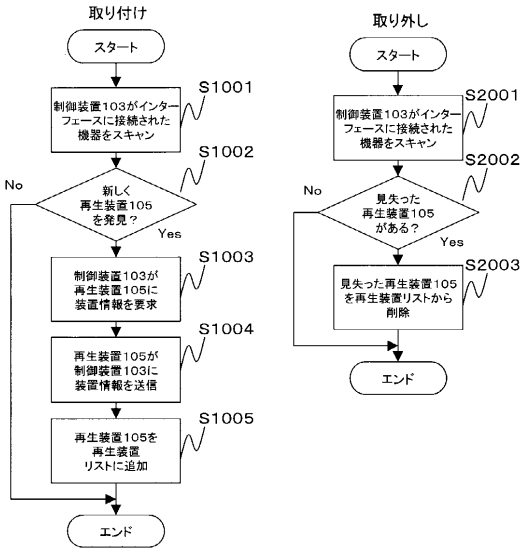
【図９】

図9



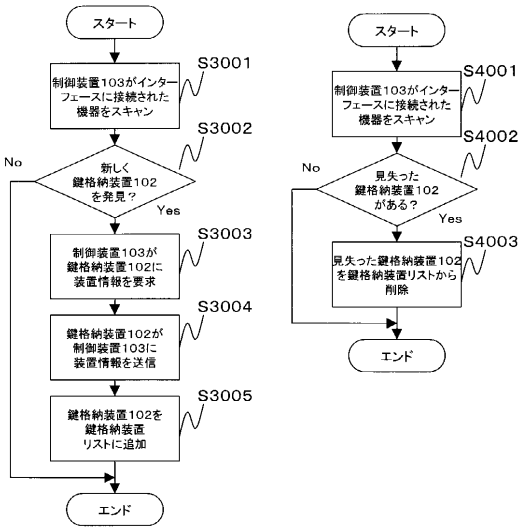
【図１０】

図10



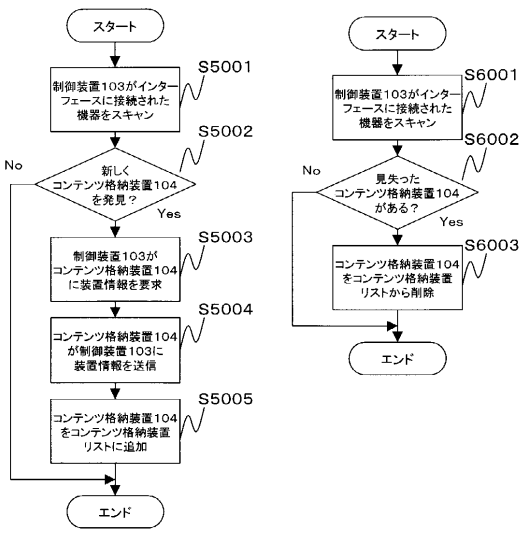
【図１１】

図11



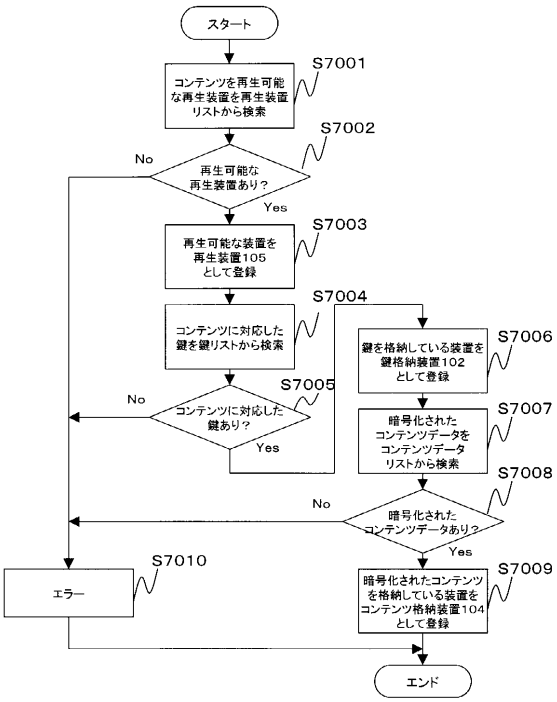
【図１２】

図12



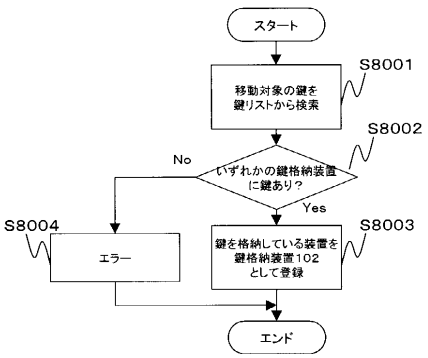
【図１３】

図13



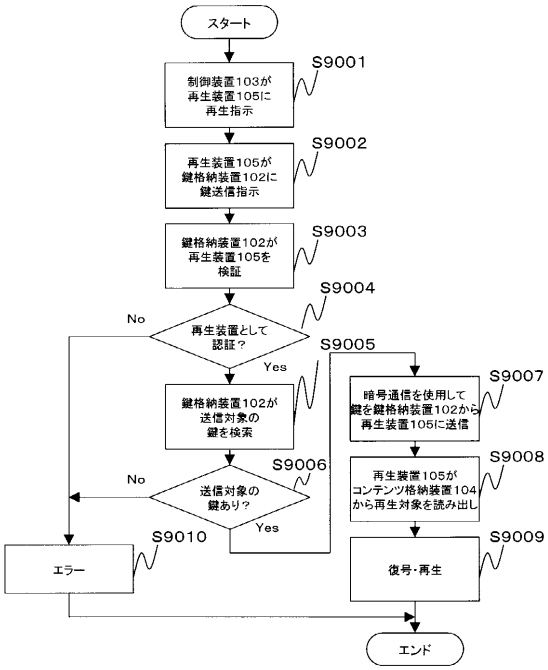
【図１４】

図14



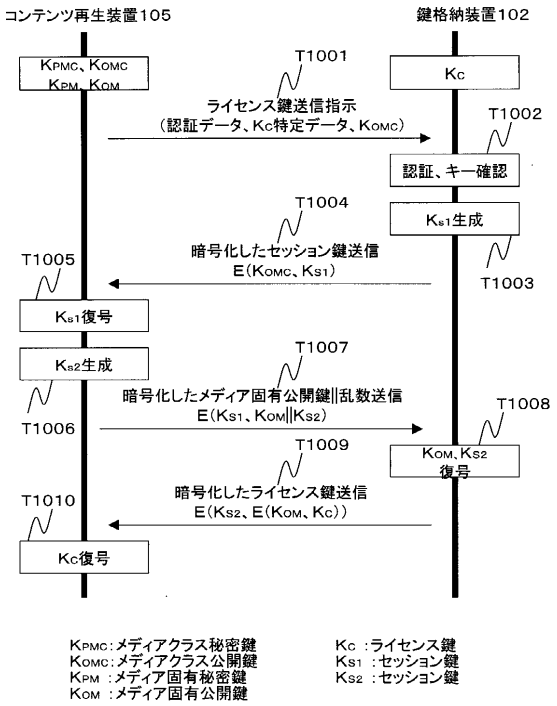
【図１５】

図15



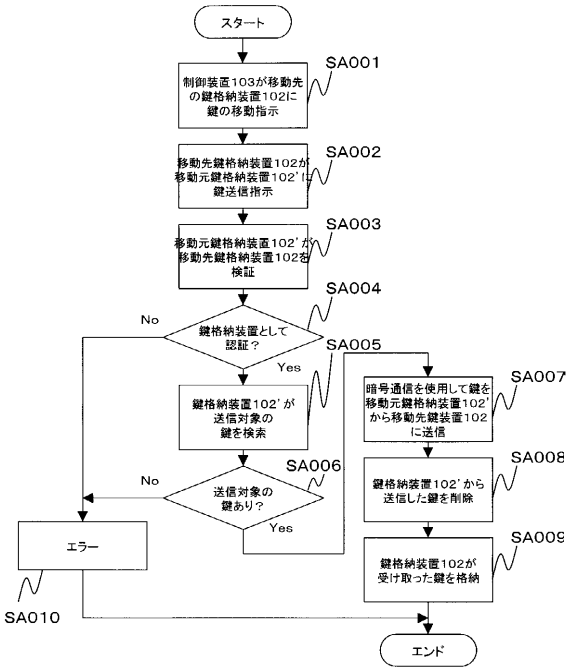
【図１６】

図16



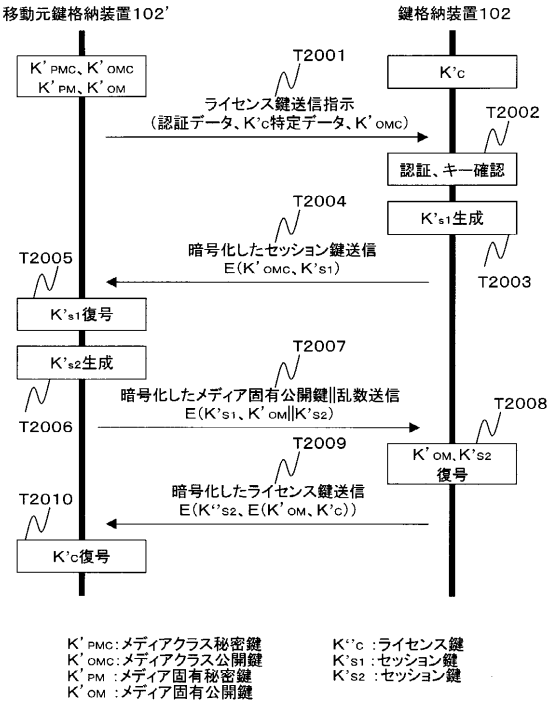
【図１７】

図17



【図１８】

図18



フロントページの続き

(72)発明者 片山 国弘
東京都小平市上水本町五丁目２０番１号 株式会社日立製作所 半導体グループ内
(72)発明者 戸塚 隆
東京都小平市上水本町五丁目２０番１号 株式会社日立製作所 半導体グループ内
(72)発明者 角田 元泰
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内
(72)発明者 井口 慎也
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内
(72)発明者 水島 永雅
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内

審査官 中里 裕正

(56)参考文献 特開平９－１２１３３５（ＪＰ，Ａ）
特開２０００－３２２８２６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 9/08
H04N 7/16
G06F 15/00 330
JICSTファイル(JOIS)