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

特許第4760101号
(P4760101)

(45)発行日　平成23年8月31日(2011.8.31)　(24)登録日　平成23年6月17日(2011.6.17)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
G06F 21/24 (2006.01)　H04L 9/00 601E
H04L 9/00 601F
G06F 12/14 520F
G06F 12/14 540A

請求項の数 10　(全 43 頁)　最終頁に続く

(21)出願番号　特願2005-111279 (P2005-111279)
(22)出願日　平成17年4月7日 (2005.4.7)
(65)公開番号　特開2006-295405 (P2006-295405A)
(43)公開日　平成18年10月26日 (2006.10.26)
審査請求日　平成20年2月15日 (2008.2.15)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(72)発明者　長尾　豊
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　西田　聡子

最終頁に続く

(54)【発明の名称】コンテンツ提供システム，コンテンツ再生装置，プログラム，およびコンテンツ再生方法

(57)【特許請求の範囲】
【請求項１】
コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置を２以上備えるコンテンツ提供システムであって：
コンテンツ提供元のコンテンツ再生装置であるコンテンツ提供元装置は，
前記コンテンツ提供元装置に固有のデバイス鍵と，コンテンツの提供先であるコンテンツ再生装置による該デバイス鍵の利用を制限するための利用制限情報と，を含むリンク情報を前記コンテンツの提供先であるコンテンツ再生装置に提供するリンク情報発行部を備え，
前記コンテンツ提供先であるコンテンツ再生装置は，
前記コンテンツ提供元装置に固有のデバイス鍵で暗号化されたコンテンツ鍵を取得するコンテンツ鍵取得部と；
前記コンテンツ提供元装置から前記リンク情報を取得するリンク情報取得部と；
前記リンク情報に含まれる前記デバイス鍵で前記コンテンツ鍵を復号するコンテンツ鍵復号部と；
前記リンク情報に含まれる前記利用制限情報に基づいて，前記デバイス鍵の利用を制限する利用制御部と；
を備えることを特徴とするコンテンツ提供システム。
【請求項２】
コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置に

おいて：
コンテンツの提供元に固有の鍵で暗号化された前記コンテンツ鍵を取得するコンテンツ鍵取得部と；
前記コンテンツ提供元に固有の鍵と，該鍵の利用を制限する利用制限情報と，を記憶するリンク情報記憶部と；
前記リンク情報記憶部に記憶されている前記鍵で前記コンテンツ鍵を復号するコンテンツ鍵復号部と；
前記リンク情報記憶部に記憶されている前記利用制限情報に基づいて，前記鍵の利用を制限する利用制御部と；
を備えることを特徴とするコンテンツ再生装置。
【請求項３】
前記リンク情報記憶部に記憶されている前記コンテンツ提供元に固有の鍵は暗号化されており；
自装置に固有のデバイス鍵を用いて前記コンテンツ提供元に固有の鍵を復号する鍵処理部を備え；
前記鍵処理部は，前記自装置を識別する識別情報と前記コンテンツ提供元を識別する識別情報とが関連付けられて前記リンク情報記憶部に記憶されている場合に，前記鍵の復号化に成功することを特徴とする，請求項２に記載のコンテンツ再生装置。
【請求項４】
前記リンク情報記憶部は，少なくとも１つのリンク情報を蓄積し，前記蓄積されたリンク情報に従って，起点が前記識別情報により識別される自装置であり，到達点が前記識別情報により識別されるコンテンツ提供元である経路が生成されることによって，前記自装置の識別情報と前記コンテンツ提供元の識別情報との関連付けを実現しており；
前記リンク情報には，一方がリンク元であり，他方がリンク先である一対の識別情報が含まれ，該識別情報は，前記コンテンツ提供元，自装置または他のコンテンツ再生装置の識別情報であることを特徴とする，請求項３に記載のコンテンツ再生装置。
【請求項５】
前記利用制限情報には，前記リンク情報記憶部に記憶されている前記コンテンツ提供元に固有の鍵による前記コンテンツ鍵の復号を制限する復号制限情報が含まれることを特徴とする，請求項２に記載のコンテンツ再生装置。
【請求項６】
前記利用制限情報には，前記リンク情報記憶部に記憶されている前記コンテンツ提供元に固有の鍵を他のコンテンツ再生装置に転送することを制限する転送制限情報が含まれることを特徴とする，請求項２に記載のコンテンツ再生装置。
【請求項７】
他のコンテンツ再生装置に前記リンク情報を発行するリンク情報発行部と；
前記他のコンテンツ再生装置に固有のデバイス鍵で自装置に固有のデバイス鍵を暗号化するデバイス鍵暗号部と；を備え，
前記リンク情報発行部は，
前記リンク情報記憶部に記憶されており，起点が前記識別情報により識別される自装置であり，到達点が前記識別情報により識別されるコンテンツ提供元である経路を生成する１又は２以上の前記リンク情報と；
前記デバイス鍵暗号部により暗号化した前記自装置に固有のデバイス鍵と；
前記リンク情報記憶部に記憶されている前記利用制限情報と；
を前記他のコンテンツ再生装置に提供することを特徴とする，請求項４に記載のコンテンツ再生装置。
【請求項８】
前記リンク情報記憶部に記憶されている利用制限情報に基づいて第２の利用制限情報を生成する制限情報生成部を備え，
前記リンク情報発行部は，前記第２の利用制限情報を前記他のコンテンツ再生装置に提

供することを特徴とする，請求項７に記載のコンテンツ再生装置。
【請求項９】
コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置に用いることが可能なプログラムであって：
コンピュータに，
コンテンツの提供元に固有の鍵で暗号化された前記コンテンツ鍵を取得するコンテンツ鍵取得ステップ；
前記コンテンツ提供元に固有の鍵と，該鍵の利用を制限する利用制限情報と，を記憶手段に記憶するリンク情報記憶ステップ；
前記記憶手段に記憶されている前記鍵で前記コンテンツ鍵を復号するコンテンツ鍵復号ステップ；
前記記憶手段に記憶されている前記利用制限情報に基づいて，前記鍵の利用を制限する利用制御ステップ；
を実行させるためのプログラム。
【請求項１０】
コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置におけるコンテンツ再生方法であって：
コンテンツの提供元に固有の鍵で暗号化された前記コンテンツ鍵を取得するコンテンツ鍵取得ステップと；
前記コンテンツ提供元に固有の鍵と，該鍵の利用を制限する利用制限情報と，を含むリンク情報を取得するリンク情報取得ステップと；
取得した前記リンク情報に含まれる前記利用制限情報に基づいて，前記鍵の利用の可否を判断する利用制御ステップと；
前記利用制御ステップにおいて前記鍵の利用が可能であると判断された場合に，前記取得したリンク情報に含まれる前記鍵で前記コンテンツ鍵を復号するコンテンツ鍵復号ステップと；
を含むことを特徴とする，コンテンツ再生方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は，コンテンツ提供システムに関し，特に，コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置に，コンテンツ鍵を提供するシステムに関する。
【背景技術】
【０００２】
近年，音楽コンテンツ等のデジタルコンテンツは，インターネットの普及やＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）等の高速・大容量化に伴って，著作権の許諾を得ない違法なコンテンツの配布・交換などが増加している。そこで，これらの違法行為を防止するため，コンテンツの流通・利用に制限を加える著作権保護技術が普及しつつある。
【０００３】
例えば，特許文献１には，コンテンツを利用許可するために必要なライセンスをユーザが所有する機器に提供して，コンテンツの再生を制限したり，コンテンツを共有したりする著作権保護技術が開示されている。この著作権保護技術により，コンテンツの著作権を保護しつつ，コンテンツを購入したユーザが所有する機器間で，ある程度自由にコンテンツを共有することが可能となる。また，ライセンスに，そのコンテンツの使用期限やコピー可能回数，チェックアウト回数などを設定して，そのライセンスに対応するコンテンツの利用条件を定めている。
【０００４】
【特許文献１】特開２００２－３５９６１６号公報
【発明の開示】

【発明が解決しようとする課題】
【０００５】
しかし，上記文献に記載された著作権保護技術を利用したコンテンツの提供システムでは，コンテンツを利用する機器ごとに，複数のコンテンツに対する利用条件を定めることはできなかった。
【０００６】
そこで，本発明は，このような問題に鑑みてなされたもので，その目的とするところは，コンテンツを利用する機器ごとに，複数のコンテンツに対する利用条件を定めることが可能なコンテンツ提供システム，コンテンツ再生装置，コンテンツ再生方法およびコンピュータプログラムを提供することにある。
【課題を解決するための手段】
【０００７】
上記課題を解決するために，本発明のある観点によれば，コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置を２以上備えるコンテンツ提供システムが提供される。本コンテンツ提供システムにおいて，コンテンツ提供元のコンテンツ再生装置であるコンテンツ提供元装置は，コンテンツ提供元装置に固有のデバイス鍵と，コンテンツの提供先であるコンテンツ再生装置による該デバイス鍵の利用を制限するための利用制限情報と，を含むリンク情報をコンテンツの提供先であるコンテンツ再生装置に提供するリンク情報発行部を備える。コンテンツ提供先であるコンテンツ再生装置は，コンテンツ提供元装置に固有のデバイス鍵で暗号化されたコンテンツ鍵を取得するコンテンツ鍵取得部と；コンテンツ提供元装置からリンク情報を取得するリンク情報取得部と；リンク情報に含まれるデバイス鍵でコンテンツ鍵を復号するコンテンツ鍵復号部と；リンク情報に含まれる利用制限情報に基づいて，デバイス鍵の利用を制限する利用制限部と；を備える。
【０００８】
上記発明によれば，コンテンツ再生装置は，コンテンツ提供元装置から，そのコンテンツ提供元装置に固有のデバイス鍵と，そのデバイス鍵の利用制限情報を取得する。また，コンテンツ再生装置は，コンテンツ提供元装置に固有のデバイス鍵により暗号化されたコンテンツ鍵を取得する。そこで，コンテンツ再生装置は，取得したデバイス鍵によりコンテンツ鍵を復号することにより，そのコンテンツ鍵に対応するコンテンツを復号して再生することができる。しかし，コンテンツ再生装置は，利用制限情報に基づいて，デバイス鍵の利用を制限される。そこで，コンテンツ提供元装置が利用制限情報をデバイス鍵とともにコンテンツ再生装置に提供することにより，コンテンツ提供先であるコンテンツ再生装置におけるコンテンツの再生を制限できる。
【０００９】
上記課題を解決するために，本発明の別の観点によれば，コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置が提供される。本コンテンツ提供装置は，コンテンツの提供元に固有の鍵で暗号化されたコンテンツ鍵を取得するコンテンツ鍵取得部と；コンテンツ提供元に固有の鍵と，該鍵の利用を制限する利用制限情報と，を記憶するリンク情報記憶部と；リンク情報記憶部に記憶されている鍵でコンテンツ鍵を復号するコンテンツ鍵復号部と；リンク情報記憶部に記憶されている利用制限情報に基づいて，鍵の利用を制限する利用制御部と；を備える。
【００１０】
コンテンツの提供元とは，著作権管理上，正当にコンテンツの提供を受けた人またはコンピュータを示す。具体的には，著作権管理サーバからライセンスの発行を受けたユーザ，またはそのユーザが使用するコンピュータである。従って，コンテンツの提供元に固有の鍵とは，著作権管理サーバからライセンスの発行を受けたユーザに固有のユーザ鍵，または，そのユーザが使用するコンピュータに固有のデバイス鍵である。
【００１１】
暗号化とは，デジタル情報を暗号鍵を用いて組み替えることである。コンテンツ鍵，ユ

ーザ鍵およびデバイス鍵は，暗号鍵である。暗号鍵は，デジタル情報の組み替えに用いる，所定の規則である。暗号化の方式として，暗号化と復号化で異なる鍵を用いる公開鍵暗号方式と，暗号化と復号化で同一の鍵を用いる秘密鍵暗号方式を例示できるが，本発明は双方の方式を適用可能である。なお，本明細書では，コンテンツを暗号化する鍵，およびコンテンツを復号する鍵の双方を，コンテンツ鍵と称する。また，ユーザ鍵は，コンテンツ提供システムを利用するユーザに与えられる鍵であり，暗号化のための鍵と，復号化のための鍵の双方を含む。デバイス鍵は，コンテンツ再生装置に与えられる鍵であり，暗号化のための鍵と，復号化のための鍵の双方を含む。

【００１２】

上記発明によれば，コンテンツ再生装置は，コンテンツ提供元に固有の鍵（上述のユーザ鍵またはデバイス鍵）と，その鍵の利用制限情報を取得する。また，コンテンツ再生装置は，コンテンツ提供元に固有の鍵により暗号化されたコンテンツ鍵を取得する。そこで，コンテンツ再生装置は，取得した鍵によりコンテンツ鍵を復号することにより，そのコンテンツ鍵に対応するコンテンツを復号して再生することができる。その際に，コンテンツ再生装置は，利用制限情報に基づいて，デバイス鍵の利用を制限する。つまり，コンテンツ再生装置は，コンテンツ提供元に固有の鍵により，その鍵で暗号化されたコンテンツ鍵を全て復号して各コンテンツ鍵に対応するコンテンツを再生することができる一方で，利用制限情報により鍵の利用を制限されることで，その鍵を利用して再生できる全てのコンテンツに対する利用を制限される。

【００１３】

上記リンク情報記憶部に記憶されているコンテンツ提供元に固有の鍵は暗号化されていてもよく，その場合，上記コンテンツ再生装置は，自装置に固有のデバイス鍵を用いてコンテンツ提供元に固有の鍵を復号する鍵処理部を備え，鍵処理部は，自装置を識別する識別情報とコンテンツ提供元を識別する識別情報とが関連付けられてリンク情報記憶部に記憶されている場合に，鍵の復号化に成功するようにしてもよい。かかる構成によれば，コンテンツ提供元に固有の鍵は暗号化されているため，その鍵が外部のコンピュータに流出した場合でも，その外部のコンピュータによって，コンテンツ提供元に固有の鍵によって暗号化されたコンテンツ鍵を復号されることを防止できる。また，コンテンツ再生装置においても，自装置を識別する識別情報とコンテンツ提供元を識別する識別情報とが関連付けられてリンク情報記憶部に記憶されている場合にのみ，コンテンツ提供元に固有の鍵の復号に成功する。そのため，上記の関連付けをリンク情報記憶部から削除されると，コンテンツ再生装置はコンテンツ提供元に固有の鍵を利用できなくなる。従って，コンテンツ提供元に固有の鍵を変更しなくても，コンテンツ再生装置による鍵の利用を防止できる。

【００１４】

上記リンク情報記憶部は，少なくとも１つのリンク情報を蓄積し，蓄積されたリンク情報に従って，起点が識別情報により識別される自装置であり，到達点が識別情報により識別されるコンテンツ提供元である経路が生成されることによって，自装置の識別情報とコンテンツ提供元の識別情報との関連付けを実現しており；リンク情報には，一方がリンク元であり，他方がリンク先である一対の識別情報が含まれ，該識別情報は，コンテンツ提供元，自装置または他のコンテンツ再生装置の識別情報であってもよい。

【００１５】

上記利用制限情報には，リンク情報記憶部に記憶されているコンテンツ提供元に固有の鍵によるコンテンツ鍵の復号を制限する復号制限情報が含まれていてもよい。

【００１６】

上記利用制限情報には，リンク情報記憶部に記憶されているコンテンツ提供元に固有の鍵を他のコンテンツ再生装置に転送することを制限する転送制限情報が含まれていてもよい。

【００１７】

上記コンテンツ再生装置は，他のコンテンツ再生装置にリンク情報を発行するリンク情報発行部と；他のコンテンツ再生装置に固有のデバイス鍵で自装置に固有のデバイス鍵を

暗号化するデバイス鍵暗号部と；を備えていてもよい。その場合，上記リンク情報発行部は，リンク情報記憶部に記憶されており，起点が識別情報により識別される自装置であり，到達点が識別情報により識別されるコンテンツ提供元である経路を生成する１又は２以上のリンク情報と；デバイス鍵暗号部により暗号化した自装置に固有のデバイス鍵と；リンク情報記憶部に記憶されている利用制限情報と；を他のコンテンツ再生装置に提供する。かかる構成によれば，コンテンツ再生装置は，コンテンツ提供元に固有の鍵で暗号化されたコンテンツ鍵を，リンク情報を発行した他のコンテンツ再生装置に利用させることができる。リンク情報を発行する際に，自装置に固有のデバイス鍵を発行先のコンテンツ再生装置に固有の鍵で暗号化することにより，安全に自装置に鍵を発行先のコンテンツ再生装置に提供できる。また，利用制限情報を提供することで，発行先のコンテンツ再生装置によるコンテンツ鍵の利用を制限することができる。

【００１８】

上記コンテンツ再生装置は，リンク情報記憶部に記憶されている利用制限情報に基づいて第２の利用制限情報を生成する制限情報生成部を備えてもよく，上記リンク情報発行部は，第２の利用制限情報を他のコンテンツ再生装置に提供してもよい。

【００１９】

上記課題を解決するために，本発明の別の観点によれば，コンピュータをして，上記コンテンツ再生装置として機能せしめるコンピュータプログラムが提供される。また，上記コンピュータプログラムを記録した，コンピュータで読み取り可能な記録媒体も提供される。

【００２０】

上記課題を解決するために，本発明の別の観点によれば，コンテンツ再生方法が提供される。

【発明の効果】

【００２１】

以上説明したように本発明によれば，コンテンツを利用する機器ごとに，複数のコンテンツに対する利用条件を定めることができる。

【発明を実施するための最良の形態】

【００２２】

以下に添付図面を参照しながら，本発明の好適な実施の形態について詳細に説明する。なお，本明細書及び図面において，実質的に同一の機能構成を有する構成要素については，同一の符号を付することにより重複説明を省略する。

【００２３】

本実施形態では，本発明にかかるコンテンツ提供システムを，コンテンツを再生する機器ごとに，コンテンツの再生期間や他の機器へのコンテンツの転送可否などを含む利用条件を設定することが可能なコンテンツ提供システム５００に適用して説明する。

【００２４】

まず，本実施形態にかかるコンテンツ提供システム５００の概要について説明する。コンテンツ提供システム５００は，有料コンテンツの提供を行うサービス事業者が管理するコンテンツ提供サーバから課金処理を行うなどして正当にコンテンツを取得した取得者が，取得したコンテンツを他の利用者と共有することを可能にするものである。しかし，正当にコンテンツを取得した取得者が，自己が取得したコンテンツを自由にあらゆる利用者に提供できてしまうと，そのコンテンツの新たな販売の機会をサービス事業者から奪うとともに，コンテンツの著作権保護の観点から問題である。そこで，コンテンツ提供システム５００では，コンテンツの著作権を保護しながら，取得者と利用者との間でのコンテンツの共有を実現するために，以下に説明するリンク方式による著作権管理を行う。

【００２５】

＜１．リンク方式による著作権管理の概要＞

まず，本実施形態にかかるリンク方式による著作権管理に対応したコンテンツ提供システムの概要について説明する。

【００２６】
本実施形態にかかるコンテンツ提供システムは，映像，音声等のデジタルコンテンツを暗号処理した著作権管理コンテンツ（以下，「コンテンツ」という）の利用者および利用状態を管理するシステムである。このコンテンツ提供システムは，インターネット等を通じたコンテンツ大量配布行為等といったコンテンツの違法利用を確実に防止するべく，コンテンツを購入したユーザ以外のユーザに対してコンテンツの利用を制限する。
【００２７】
コンテンツを購入したユーザが暗号化されたコンテンツを再生等するためには，コンテンツを暗号化したコンテンツ暗号処理鍵（以下，「コンテンツ鍵」という。）でコンテンツを復号化する必要がある。コンテンツがインターネット等により違法に配布されたとしても，このコンテンツ鍵がなければコンテンツを再生することができない。したがって，本実施形態にかかるコンテンツ提供システムにおいては，コンテンツ鍵を安全に配布し，かつ正しいユーザに使用させなければならない。
【００２８】
一方，コンテンツを購入したユーザが所有する機器間においては，ある程度自由にコンテンツを再生可能にする必要がある。さもなければ，コンテンツを購入したユーザは，コンテンツを購入したものの，自身の所有する機器でコンテンツを再生できなかったり，コンテンツを購入した機器でのみしか再生できなかったりしてしまう。
【００２９】
このように，本実施形態にかかるコンテンツ提供システムでは，著作権管理を行いつつも，私的利用の範囲内ではコンテンツの共有を認め，同一ユーザが所有する複数の機器におけるコンテンツ共有の利便性，自由度を高めることが可能な著作権管理方式を採用している。この著作権管理方式を実現させるため，本実施形態においては，リンク方式による著作権管理スキームを採用している。
【００３０】
リンク方式による著作権管理では，機器同士を関連付けることにより機器間でコンテンツを共有することが可能となる。本実施形態においては，機器同士を関連付けることを機器同士をリンクするという。例えば，ユーザが所有する機器１にユーザが所有する機器２をリンクすることにより，機器１で再生可能であるコンテンツが機器２においても再生可能となる。リンク方式については後で詳しく説明するが，コンテンツを再生できる機器１にリンクされている機器ではコンテンツを再生することができ，リンクされていない機器ではコンテンツを再生することができないため，著作権管理を行いつつも，ユーザ所有の機器においてはある程度自由にコンテンツを再生することが可能となる。
【００３１】
なお，コンテンツは，例えば，音楽，公演，ラジオ番組等の音声（Ａｕｄｉｏ）コンテンツや，映画，テレビジョン番組，ビデオプログラム，写真，絵画，図表等を構成する静止画若しくは動画からなる映像（Ｖｉｄｅｏ）コンテンツ，電子図書（Ｅ－ｂｏｏｋ），ゲーム，ソフトウェアなど，任意のコンテンツであってもよい。以下では，コンテンツとして，音楽コンテンツ，特に，配信サーバから配信された，或いは音楽ＣＤからリッピングされた音楽コンテンツの例を挙げて説明するが，本発明はかかる例に限定されない。
【００３２】
次に，図１に基づいて，上記のようなリンク方式の著作権管理を行うための，本実施形態にかかるコンテンツ提供システムにおけるリンク方式の概要について説明する。なお，図１は，本実施形態にかかるコンテンツ提供システムのリンク方式の概要を示す説明図である。
【００３３】
図１に示したように，ユーザＡはユーザ機器１０ａと１０ｂと１０ｄとを所有していたとする。例えば，ユーザＡは，ユーザ機器１０ａを介してコンテンツ提供サービスに加入して，コンテンツを購入する。ユーザＡは，自身が所有する機器であるユーザ機器１０ａでコンテンツを再生したいとすれば，ユーザ機器１０ａをユーザＡにリンクする。上述し

たように，ユーザ機器１０ａをユーザＡにリンクさせると，ユーザＡが購入したコンテンツをユーザ機器１０ａで再生することが可能となる。

【００３４】

ここで，ユーザ機器１０ａをユーザＡにリンクするとは，ユーザ機器１０ａがユーザＡの秘密情報を取得することをいう。ユーザＡの秘密情報とは，本来ユーザＡしか知ることのできない情報であって，例えば，ユーザＡの秘密鍵の情報などである。例えば，コンテンツ鍵を安全にユーザＡに配布するために，コンテンツ鍵はユーザＡの公開鍵または秘密鍵で暗号化されてユーザＡに配布される。

【００３５】

ユーザＡはユーザ機器１０ａでコンテンツを再生しようとするが，ユーザ機器１０ａがユーザＡの秘密鍵の情報を知らなければ，ユーザ機器１０ａにおいてコンテンツ鍵を復号化することができず，コンテンツを再生することができない。そこで，ユーザ機器１０ａをユーザＡにリンクする，つまりユーザ機器１０ａがユーザＡの秘密鍵の情報を取得することができれば，ユーザ機器１０ａにおいてユーザＡが購入したコンテンツを再生することが可能となる。

【００３６】

同様に，ユーザ機器１０ｂをユーザＡにリンクする。ユーザ機器１０ｂがユーザＡの秘密鍵の情報を知ることができれば，ユーザ機器１０ｂにおいてもユーザＡが購入したコンテンツを再生することが可能となる。

【００３７】

ユーザＡの秘密鍵がユーザ機器１０ａに安全に配布されるためには，ユーザＡの秘密鍵がユーザ機器１０ａの公開鍵または秘密鍵で暗号化されてユーザ機器１０ａに配布される必要がある。ユーザＡの秘密鍵はユーザ機器１０ａにより復号され，復号されたユーザＡの秘密鍵でコンテンツ鍵を復号することとなる。さらに，ユーザ機器１０ｄでもコンテンツを再生したい場合には，ユーザ機器１０ｄをユーザ機器１０ａにリンクすればよい。ユーザ機器１０ｄはユーザ機器１０ａの秘密鍵の情報を取得することができ，さらにユーザ機器１０ａの秘密鍵でユーザＡの秘密鍵の情報も取得することができる。そして，ユーザＡの秘密鍵でユーザＡが購入したコンテンツを再生することが可能となる。

【００３８】

このように，自身がリンクされた先をたどってリンク先の秘密情報を取得することにより，リンク先において購入したコンテンツを自身の機器で再生することが可能となる。例えば，ユーザＡの家族であるユーザＢにユーザ機器１０ａをリンクすれば，ユーザＢが購入したコンテンツもユーザ機器１０ａにおいて再生することが可能となる。さらにユーザＡとユーザＢをファミリーにリンクすれば，例えば，ファミリーがコンテンツ提供サービスの会員となりコンテンツを購入した場合に，ユーザＡもユーザＢもそのコンテンツを再生することが可能となる。そして，上述したように，ユーザＡおよびユーザＢにリンクされているユーザ機器があれば，そのユーザ機器でファミリーが購入したコンテンツを再生することが可能となる。

【００３９】

また，ユーザとそのユーザの所有するユーザ機器，またはユーザ所有のユーザ機器同士がリンクされていれば，コンテンツ鍵をユーザに対して安全に配布するだけで，コンテンツを利用するユーザを制限し，かつ，ユーザ所有の機器間においてはある程度自由にコンテンツを共有することが可能となる。

【００４０】

以上，リンク方式による著作権管理の概要について説明した。次に，リンク方式による著作権管理を実現する具体的な一例として，コンテンツ提供システム１００について説明する。

【００４１】

＜２．コンテンツ提供システムの全体構成＞

図２は，本実施形態にかかるコンテンツ提供システム１００の全体構成図である。図２

に示したように，コンテンツ提供システム１００は，ユーザ機器１０と，著作権管理サーバ２０ａと，コンテンツ提供サーバ２０ｂなどを備える。ユーザ機器１０は，図２に示したように，複数のユーザ機器１０ａ，１０ｂ，１０ｃ，１０ｄ・・を含んでもよい。また，著作権管理サーバ２０ａとコンテンツ提供サーバ２０ｂは別のサーバとして構成されているが，１のサーバとして構成されていてもよい。

【００４２】

ユーザ機器１０は，コンテンツを利用するための各種の情報処理装置である。図２には，ユーザ機器１０の例として，ノート型若しくはデスクトップ型のパーソナルコンピュータ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ；以下「ＰＣ」という。）１０ａ，オーディオ機器１０ｂ，１０ｃ，携帯型のコンテンツ再生装置であるポータブルデバイス（Ｐｏｒｔａｂｌｅ　Ｄｅｖｉｃｅ；以下「ＰＤ」という。）１０ｄなどを例示することができる。

【００４３】

かかるユーザ機器１０は，例えばコンテンツの利用機能（例えばコンテンツの再生，保存，移動，結合，分割，変換，複製，貸出，返却機能等），上述したリンクによるコンテンツ再生制御機能，コンテンツの管理機能（例えば，コンテンツＩＤに基づくコンテンツ，コンテンツ鍵等の検索または削除機能など），リッピング，セルフレコーディング等によるコンテンツ作成機能などを有する。

【００４４】

このユーザ機器１０のうち，ネットワーク３０を介した通信機能を有する装置（例えば，ＰＣ１０ａ）は，著作権管理サーバ２０ａおよびコンテンツ提供サーバ２０ｂとの間で通信接続可能である。このようなユーザ機器１０は，例えば，コンテンツ提供サーバ２０ｂから，コンテンツ配信サービス用のソフトウェアや，著作権管理用ソフトウェアをダウンロードして，インストール可能である。これにより，ユーザ機器１０は，コンテンツ提供サーバ２０ｂから，暗号処理されたコンテンツの配信を受けたり，著作権管理サーバ２０ａからコンテンツのコンテンツ鍵やコンテンツの利用条件などを含むライセンスの配信を受けたり，これらのデータをストレージ装置やリムーバブル記憶媒体などの記憶手段に記録することができる。

【００４５】

また，ユーザ機器１０は，例えば，セルフレコーディング（自己録音，録画等）やリッピングなどによって，新規にコンテンツを作成して，ストレージ装置やリムーバル記憶媒体に記録することができる。なお，セルフレコーディングとは，ユーザ機器１０自身が有する撮像装置／集音装置によって撮像／集音した音声等を，映像／音声のデジタルデータとして記憶することをいう。また，リッピングとは，音楽ＣＤ，ビデオＤＶＤ，ソフトウェア用ＣＤ－ＲＯＭ等の記憶媒体に記録されているデジタルコンテンツ（音声データや映像データ等）を抽出し，コンピュータで処理可能なファイル形式に変換して，ストレージ装置やリムーバル記憶媒体に記録することをいう。

【００４６】

上述したように，ユーザ機器１０ｂ，１０ｃ，１０ｄがＰＣ１０ａにリンクされていれば，ＰＣ１０ａにおいてダウンロードされ，ＰＣ１０ａにおいて再生可能なコンテンツは，リンクされたユーザ機器においても再生することができる。ユーザ機器１０においてコンテンツを再生する際には，コンテンツを暗号化したコンテンツ鍵が必要となる。このコンテンツ鍵は，さらに暗号化されており，ユーザ機器１０は，コンテンツ鍵を暗号化している鍵を取得することによりコンテンツ鍵を復号して，そのコンテンツ鍵でコンテンツを復号してコンテンツを自身の機器で再生することができる。

【００４７】

著作権管理サーバ２０ａは，コンテンツ鍵を安全にユーザに送信し，コンテンツの再生を制限しつつ，ユーザが所有する機器間においてコンテンツを共有させるためのリンク処理を行う情報処理装置である。具体的には，著作権管理サーバ２０ａは，ユーザおよびユーザが所有するユーザ機器１０の登録処理を行ったり，ユーザとユーザ機器のリンクやユーザ機器同士のリンクを行ったり，コンテンツ鍵を暗号化してユーザ機器１０に送信した

りする。
【００４８】
コンテンツ提供サーバ２０ｂは，コンテンツを提供するサーバであって，ユーザにコンテンツ提供サービスを提供するサーバである。コンテンツ提供サーバ２０ｂは，ユーザ機器１０からの要求に応じて，当該ユーザ機器１０にネットワーク３０を介してコンテンツを配信する。
【００４９】
例えば，音楽コンテンツを配信する場合には，この配信サーバ２０ｂは，電子音楽配信（ＥＭＤ；Ｅｌｅｃｔｒｏｎｉｃ Ｍｕｓｉｃ Ｄｉｓｔｒｉｂｕｔｉｏｎ）サービスを提供するサーバとして構成される。この場合，配信サーバ２０ｂは，配信対照の音楽コンテンツを，例えば，ＡＴＲＡＣ３（Ａｄｖａｎｃｅｄ Ｔｒａｎｓｆｏｒｍ Ａｃｏｕｓｔｉｇ Ｃｏｄｉｎｇ）方式，またはＭＰ３（ＭＰＥＧ Ａｕｄｉｏ Ｌａｙｅｒ－３）方式などの圧縮符号化方式で圧縮符号化し，ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）などの暗号化方式で暗号化した上で，ユーザ機器１０に配信する。また，コンテンツ提供サーバ２０ｂは，このように暗号化されたコンテンツとともに，当該コンテンツを復号化するためのコンテンツ鍵を暗号化してユーザ機器１０に送信してもよい。また，当該コンテンツ鍵を著作権管理サーバ２０ａに提供して，著作権管理サーバ２０ａにおいてコンテンツ鍵を暗号化してユーザ機器１０に送信するようにしてもよい。
【００５０】
また，コンテンツ提供サーバ２０ｂは，ユーザ機器１０が例えばリッピング，セルフレコーディング等により自ら作成したコンテンツの利用を管理する作成コンテンツ利用サービスを提供するサーバとしても構成できる。この場合，コンテンツ提供サーバ２０ｂは，ユーザ機器１０に対し，コンテンツの暗号化を解除するコンテンツ鍵を配信する。これによって，ユーザ機器１０は，コンテンツ提供サーバ２０ｂから取得したコンテンツ鍵に基づいて，上記リッピング等により自ら作成したコンテンツを再生することができるようになる。
【００５１】
ネットワーク３０は，上記ユーザ機器１０と著作権管理サーバ２０ａとコンテンツ提供サーバ２０ｂとを通信可能に接続する通信回線網である。このネットワーク３０は，例えば，インターネット，電話回線網，衛星通信網等の公衆回線網や，ＷＡＮ，ＬＡＮ，ＩＰ－ＶＰＮ等の専用回線網などで構成されており，有線・無線を問わない。
【００５２】
上記コンテンツ提供システム１００においては，コンテンツを利用制限する著作権管理機能を担保しつつ，各種のユーザ機器１０間におけるコンテンツのポータビリティを向上させ，ユーザの利便性，コンテンツ利用の自由度を向上させることができるものである。
【００５３】
＜３．ユーザ機器のハードウェア構成＞
次に，本実施形態にかかるユーザ機器１０のハードウェア構成について説明する。以下では，ユーザ機器１０の代表例として，ＰＣ１０ａとＰＤ１０ｄのハードウェア構成例について説明する。なお，ユーザ機器１０であるＰＣ１０ａとＰＤ１０ｂは，本発明のコンテンツ処理装置の一具現例として構成されている。
【００５４】
まず，図３に基づいて，本実施形態にかかるＰＣ１０ａのハードウェア構成について説明する。なお，図３は，本実施形態にかかるＰＣ１０ａのハードウェア構成例を概略的に示すブロック図である。
【００５５】
図３に示すように，ＰＣ１０ａは，例えばＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１０１と，ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１０２と，ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１０３と，ホストバス１０４と，ブリッジ１０５と，外部バス１０６と，インタフェース１０７と，入力装置１０８と，出力

装置１１０と，ストレージ装置（ＨＤＤ）１１１と，ドライブ１１２と，接続ポート１１４と，通信装置１１５とを備える。

【００５６】

ＣＰＵ１０１は，演算処理装置および制御装置として機能し，ＲＯＭ１０２またはＨＤＤ１１１に格納された各種プログラムに従って動作し，ＰＣ１０ａ内の各部を制御する。具体的な処理としては，例えば，コンテンツの暗号化および復号化処理，データ改ざん防止およびデータ検証のためのデジタル署名（ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）等）の生成および検証処理，接続された他のユーザ機器１０との間で実行するコンテンツ当の入出力時の認証およびセッションキー共有処理，コンテンツ，ライセンスおよびコンテンツ鍵等の入出力処理制御，さらに，ライセンス評価等の著作権管理処理などを実行する。

【００５７】

ＲＯＭ１０２は，ＣＰＵ１０１が使用するプログラムや，演算パラメータ等を記憶する。また，このＲＯＭ１０２は，コンテンツ，ライセンスおよびコンテンツ鍵など保存する記憶手段として利用することもできる。ＲＡＭ１０３は，ＣＰＵ１０１の実行において使用するプログラムや，その実行において適宜変化するパラメータ等を一時記憶する。これらはＣＰＵバスなどから構成されるホストバス１０４により相互に接続されている。

【００５８】

ホストバス１０４は，ブリッジ１０５を介して，ＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ／ｉｎｔｅｒｆａｃｅ）バスなどの外部バス１０６に接続されている。

【００５９】

入力装置１０８は，例えば，マウス，キーボード，タッチパネル，ボタン，スイッチ，レバー等の操作手段と，入力信号を生成してＣＰＵ１０１に出力する入力制御回路などから構成されている。ＰＣ１０ａのユーザは，この入力装置１０８を操作することにより，ＰＣ１０ａに対して各種のデータを入力したり処理動作を指示したりすることができる。

【００６０】

出力装置１１０は，例えばＣＲＴ（Ｃａｔｈｏｄｅ Ｒａｙ Ｔｕｂｅ）ディスプレイ装置，液晶ディスプレイ（ＬＣＤ）装置，ランプ等の表示装置と，スピーカ等の音声出力装置などで構成される。この出力装置１１０は，例えば再生されたコンテンツを出力する。具体的には，表示装置は再生された映像コンテンツをテキストまたはイメージで動画若しくは静止画で表示する。一方，音声出力装置は，再生された音声コンテンツを発音する。

【００６１】

ＨＤＤ１１１は，本実施形態にかかるＰＣ１０ａの記憶手段の一例として構成されたデータ格納用の装置である。このＨＤＤ１１１は，ＣＰＵ１０１が実行するプログラムや各種データをハードディスクに格納する。また，このＨＤＤ１１１には，例えば，コンテンツ，ライセンス，コンテンツ鍵などの各種データが格納される。

【００６２】

ドライブ１１２は，記憶媒体用リーダ／ライタであり，ＰＣ１０ａに内蔵，或いは外付けされる。このドライブ１１２は，ＰＣ１０ａにローディングされた磁気ディスク（ＨＤ等），光ディスク（ＣＤ，ＤＶＤ等）光磁気ディスク（ＭＯ等），または半導体メモリ等のリムーバブル記憶媒体４０に対してコンテンツ，ライセンス，コンテンツ鍵などの各種データを記録／再生する。

【００６３】

具体的には，ドライブ１１２は，リムーバル記憶媒体４０に記憶されているデータを読み出して，インタフェース１０７，外部バス１０６，ブリッジ１０５，およびホストバス１０４を介して接続されているＲＡＭ１０３に供給する。ＣＰＵ１０１は，必要に応じて，これらのデータをＲＯＭ１０２またはＨＤＤ１１１などに格納する。一方ドライブ１１２は，ＲＯＭ１０２またはＨＤＤ１１１などに格納されているデータや，新たに生成した

データ，外部装置から取得したデータをＣＰＵ１０１から受け取り，リムーバブル記憶媒体４０に書き込む。

【００６４】

接続ポート１１４は，例えば，ＰＣ１０ａと他のユーザ機器１０などの外部周辺機器とを接続するポートであり，ＵＳＢ，ＩＥＥＥ１３９４等の接続端子を有する。接続ポート１１４は，インタフェース１０７，および外部バス１０６，ブリッジ１０５，ホストバス１０４等を介してＣＰＵ１０１等に接続されている。かかる接続ポート１１４によって，ＰＣ１０ａｈａ，ＰＤ１０ｂ等に対してローカルライン３０ｂを介して接続され，各種のデータを通信可能となる。

【００６５】

通信装置１１５は，例えば，ネットワーク３０（ネットワーク３０ａを含む。）に接続するための通信デバイス等で構成された通信インタフェースである。この通信装置１１５は，他のユーザ機器１０や，著作権管理サーバ２０ａや，コンテンツ提供サーバ２０ｂ等の外部機器との間で，ネットワーク３０を介してコンテンツ，コンテンツ鍵などの各種データを送受信する。

【００６６】

次に，図４に基づいて，本実施形態にかかるＰＤ１０ｄのハードウェア構成について説明する。なお，図４は，本実施形態にかかるＰＤ１０ｄのハードウェア構成例を概略的に示すブロック図である。

【００６７】

図４に示すように，ＰＤ１０ｄは，例えば，制御装置２０１と，フラッシュメモリ２０２と，ＲＡＭ２０３と，バス２０６と，入力装置２０８と，表示装置２１０と，ＨＤＤ２１１と，ドライブ２１２と，デコーダ２１３と，通信装置２１５と，オーディオ出力回路２１６と，リモートコントローラ２１８と，ヘッドフォン２１９とを備える。

【００６８】

制御装置２０１は，例えば，フラッシュメモリ２０２またはＨＤＤ２１１に格納された各種プログラムに従って動作し，ＰＤ１０ｄの各部を制御する。フラッシュメモリ２０２は，例えば，制御装置２０１の動作を規定したプログラムや，各種のデータを記憶する。このＲＯＭ１０２は，コンテンツ，ライセンスおよびコンテンツ鍵などを保存する記憶手段として利用することもできる。また，ＲＡＭ２０３は，例えばＳＤＲＡＭ（Ｓｙｎｃｈｒｏｎｏｕｓ　ＤＲＡＭ）で構成され，制御装置２０１の処理に関する各種データを一時記憶する。

【００６９】

バス２０６は，制御装置２０１，フラッシュメモリ２０２，ＲＡＭ２０３，データ処理装置２０４，入力装置２０８，表示装置２１０，ＨＤＤ２１１，ドライブ２１２，デコーダ２１３，通信装置２１５およびオーディオ出力回路２１６などを接続するデータ線である。

【００７０】

入力装置２０８とリモートコントローラ２１８は，例えば，タッチパネル，ボタンキー，レバー，ダイヤル等の操作手段と，ユーザによる操作手段に対する操作に応じて入力信号を生成して制御装置２０１に出力する入力制御回路などから構成されている。コンテンツ処理装置１０のユーザは，この入力装置２０８や，後述のリモートコントローラ２１８を操作することにより，コンテンツ処理装置１０に対して各種のデータを入力したり処理動作を指示したりすることができる。

【００７１】

表示装置２１０は，例えばＬＣＤパネルおよびＬＣＤ制御回路などで構成される。この表示装置２１０は，制御装置２０１の制御に応じて，各種情報をテキストまたはイメージで表示する。

【００７２】

ＨＤＤ２１１は，本実施形態にかかるＰＤ１０ｄの記憶手段の一例として構成されたデ

ータ格納用の装置である。このＨＤＤ２１１は，例えば数十ＧＢの記憶容量を有するハードディスクドライブ（ＨＤＤ）で構成され，コンテンツ，ライセンス，コンテンツ鍵や，制御装置２０１のプログラム，各種のデータを格納する。かかるＨＤＤ２１１を備えたＰＤ１０ｄは，コンテンツを記録および再生可能なコンテンツ記録再生装置として構成される。これによって，ＰＣ１０ａからリムーバブル記憶媒体４０を介して提供されたコンテンツのみならず，ＰＣａ等からローカルラインを介して受信したコンテンツをＨＤＤ２１１に格納して，再生することができるようになる。しかし，かかる例に限定されず，例えば，ＰＤ１０ｄはＨＤＤ２１１を具備せず，コンテンツの再生専用装置として構成されてもよい。この場合には，ＰＤ１０ａは，例えば，リムーバブル記憶媒体４０に保存されているコンテンツを読み出して再生のみ実行可能（記録は不可能）となる。

【００７３】

ドライブ２１２は，記憶媒体用リーダ／ライタであり，ＰＣ１０ａに内蔵される。このドライブ２１２は，ＰＤ１０ｂにローディングされた上記各種のリムーバブル記憶媒体４０に対して，コンテンツ，ライセンス，コンテンツ鍵などの各種データを，記録／再生する。デコーダ２１３は，暗号化されているコンテンツのデコート処理，サラウンド処理，ＰＣＭデータへの変換処理などを行う。

【００７４】

通信装置２１５は，例えば，ＵＳＢコントローラおよびＵＳＢ端子などで構成され，ＵＳＢケーブル等のローカルライン３０ｂを介して接続されたＰＣ１０ａ等のユーザ機器１０との間で，コンテンツ，ライセンス，コンテンツ鍵，制御信号などの各種データを送受信する。

【００７５】

オーディオ出力回路２１６は，デコーダ２１３によりデコードされ，制御装置２０１によってＤＡ変換されたアナログ音声データを増幅してリモートコントローラ２１８に出力する。このアナログ音声データは，リモートコントローラ２１８からヘッドフォン２１９に出力され，ヘッドフォン２１９に内蔵されたスピーカ（図示せず）から音声出力される。

【００７６】

以上のように，図３および図４では，ユーザ機器１０の一例であるＰＣ１０ａおよびＰＣ１０ｄのハードウェア構成例を説明した。しかし，コンテンツを利用するユーザ機器１０は，上記ＰＣ１０ａおよびＰＣ１０ｄの例に限定されず，図２に示したように，据え置き型の音声プレーや１０ｆや，その他テレビジョン装置，携帯電話等さまざまな電子機器，情報処理装置によって構成することが可能である。したがって，ユーザ機器１０は，それぞれの機器固有のハードウェア構成に応じた処理を実行する。

【００７７】

＜４．著作権管理サーバの機能構成＞

次に，図５に基づいて，著作権管理サーバ２０ａの機能構成について説明する。図５に示したように，著作権管理サーバ２０ａは，受信部３０２，送信部３０４，登録部３０６，リンク発行部３０８，ライセンス発行部３１０，ユーザ情報記憶部３１２，コンテンツ鍵記憶部３１４などを含んで構成される。

【００７８】

受信部３０２は，例えば，通信回線，通信回路，通信デバイス等で構成された通信インタフェースであり，ネットワーク３０を介して接続されたユーザ端末１０の属性情報を受信したり，ユーザ端末１０において入力された情報を受信したりする。

【００７９】

登録部３０６は，コンテンツ提供サービス及び／または著作権管理サービスの利用を希望する新規ユーザの登録処理，登録変更処理，登録解除処理およびユーザアカウント情報（ユーザＩＤ，クレジット番号，パスワード等）の管理などを行う。サービス登録されたユーザに対しては，ユーザ単位で固有の鍵が付与される。ここで付与される鍵は，公開鍵暗号で使用される対となる公開鍵と秘密鍵でもよいし，秘密鍵暗号で使用される共通鍵で

もよい。また，この鍵情報はユーザＩＤとともにユーザ情報記憶部３１２に記憶される。

【００８０】

また，登録部３０６は，ユーザが所有するユーザ機器の管理を行う。登録部３０６は，受信部３０２を介してユーザ機器の特定情報（機器のタイプ，モデル，バージョン等）を取得して，デバイスＩＤとユーザ機器固有の鍵を付与する。ここで，デバイスＩＤは，そのユーザ機器を一意に特定することのできる識別情報である。デバイスＩＤは，あらかじめユーザ機器に設定されているデバイスＩＤを取得して，そのデバイスＩＤによりユーザ機器を管理するようにしてもよい。

【００８１】

このように，登録部３０６において付与された鍵情報は，ユーザＩＤまたはデバイスＩＤと関連付けられてユーザ情報記憶部３１２に記憶され，ユーザＩＤまたはデバイスＩＤと鍵情報とをノード情報として生成し，送信部３０４を介して各ユーザまたは各ユーザ機器に送信する。ノード情報を受信したユーザＩＤまたはユーザ機器は，著作権管理サーバ２０ａにおいて一意に識別されるＩＤを取得することとなる。

【００８２】

登録部３０６により付与された鍵は，サーバによりコンテンツ鍵を暗号化するために使用されたり，ユーザ機器により暗号化されたコンテンツ鍵を復号化するために使用されたりする。例えば，サーバにおいて，コンテンツ鍵をユーザの公開鍵で暗号化した場合には，そのコンテンツ鍵を受け取ったユーザは，ユーザの秘密鍵でコンテンツ鍵を復号化する必要がある。したがって，この場合には，ユーザの秘密鍵をユーザに送信しておく必要がある。

【００８３】

リンク発行部３０８は，ユーザにユーザ所有のユーザ機器を関連付けたり，ユーザが所有するユーザ機器同士を関連付けたりする機能を有する。具体的には，ユーザ機器からの入力に応じて，ユーザ機器をユーザにリンクするリンク情報を生成して，そのリンク情報を，ユーザ機器に送信し，ユーザ情報記憶部３１２にも記憶する。例えば，著作権管理サービスに登録したユーザは，ユーザ所有のユーザ機器３台で購入したコンテンツを自由に再生したいとする。ユーザは，自身の所有するユーザ機器３台のリンク要求を著作権管理サーバ２０ａに送信する。リンク要求を受けた著作権管理サーバ２０ａのリンク発行部は，ユーザが所有するユーザ機器３台とユーザをリンクする。

【００８４】

ここで，ユーザ機器３台とユーザをリンクするとは，ユーザ情報記憶部３１２に記憶されているユーザの秘密鍵を各ユーザ機器の公開鍵で暗号化することをいう。ユーザが購入したコンテンツを復号するコンテンツ鍵がユーザの秘密鍵で暗号化されている場合，暗号化されたコンテンツ鍵はユーザの秘密鍵でなければ復号することができない。しかし，ユーザ所有のユーザ機器がユーザにリンクされていれば，ユーザ所有のユーザ機器においてユーザの秘密鍵を取得して，コンテンツ鍵を復号することができ，さらにそのコンテンツ鍵で暗号化されているコンテンツを復号して再生することが可能となる。

【００８５】

ユーザ情報記憶部３１２は，ユーザＩＤやデバイスＩＤと，鍵情報およびリンク情報が関連付けられて記憶されている。著作権管理サーバ２０ａは，ユーザＩＤやデバイスＩＤを取得することにより，ユーザ情報記憶部３１２に記憶されている各ユーザやユーザ機器に対応する鍵情報を取得することができる。

【００８６】

図６に基づいて，ユーザ情報記憶部３１２に記憶されているユーザ情報について説明する。図６に示すように，ユーザ情報記憶部３１２には，ユーザＩＤ３１２１，クレジットカード番号３１２２，ユーザ鍵３１２３，デバイスＩＤ３１２４，デバイス鍵３１２５，リンク３１２６などの情報が格納されている。

【００８７】

ユーザＩＤ３１２１およびクレジット番号３１２２は，コンテンツ提供サービスおよび

著作権管理サービスの提供を受けるユーザのユーザアカウント情報であって，ユーザを一意に特定することができる識別情報である。ユーザ鍵３１２３は，１のユーザＩＤ３１２１に対して割り当てられる鍵情報である。

【００８８】

デバイスＩＤ３１２４は，ユーザにリンクされたユーザ機器のＩＤであって，ユーザが所有するユーザ機器のＩＤが格納されている。デバイス鍵３１２５は，コンテンツ提供システム１００において一意に識別される番号であって，工場出荷時等にあらかじめユーザ機器に設定された識別番号でもよいし，著作権管理サーバ２０ａの登録部３０６により設定された識別番号でもよい。

【００８９】

デバイス鍵３１２５は，各ユーザ機器に割り当てられた鍵情報が格納されている。デバイス鍵３１２５についても，予めユーザ機器に設定されているデバイス鍵を格納してもよいし，登録部３０６により割り当てられた鍵情報を格納するようにしてもよい。

【００９０】

リンク３１２６は，ユーザ機器ごとに設定されたリンク情報が格納されている。例えば，ユーザ機器１が「Ｙａｍａｄａ　Ｔａｒｏ」にリンクされている場合には，「リンクＡ」には，デバイスＩＤとユーザＩＤと関連付けの方向と，ユーザ鍵Ａ（秘密鍵）をデバイス鍵１（公開鍵）で暗号化した情報が含まれている。リンク３１２６は，各ユーザ機器に送信され，ユーザ機器の記憶部に記憶されてもよいし，ユーザ機器がサーバにアクセスすることにより，自身のリンク情報を取得するようにしてもよい。以上ユーザ情報記憶部３１２の格納情報について説明した。

【００９１】

図５に戻り，ライセンス発行部３０８は，コンテンツを購入したユーザに対してコンテンツ鍵を含むライセンスを発行する。この際，ライセンス発行部３１０は，ライセンスに含まれるコンテンツ鍵をユーザの秘密鍵で暗号化することにより，ユーザに安全にコンテンツ鍵を配布することができる。またライセンスには，コンテンツの利用条件等を含むようにしてもよい。コンテンツ鍵およびコンテンツの利用条件は，コンテンツ提供サーバ２０ｂにより提供されるようにしてもよい。

【００９２】

ライセンス発行部３１０において発行されたライセンスは，送信部３０４を介してユーザ機器１０に送信される。また，このライセンスは，ユーザ情報記憶部３１２に記憶してもよい。

【００９３】

ライセンスには，コンテンツを識別するコンテンツＩＤ等が含まれている。ユーザは，コンテンツを購入した後に著作権管理サーバ２０ａよりライセンスを取得してもよいし，コンテンツを購入する前にあらかじめライセンスを取得して，その後にコンテンツを購入してもよい。

【００９４】

また，コンテンツ鍵が格納されているコンテンツ鍵記憶部３１２と，ライセンス発行部３１０をコンテンツ提供サーバ２０ｂに備えるようにしてもよい。その場合，コンテンツ提供サーバ２０ｂは，コンテンツ鍵を暗号化するユーザ鍵等の情報を著作権管理サーバ２０ａから取得して，コンテンツ鍵を暗号化しライセンスを生成するようにしてもよい。コンテンツ提供サーバ２０ｂにおいて生成されたライセンスは，コンテンツとともにユーザ所有のユーザ機器に送信されてもよい。

【００９５】

送信部３０４は，例えば，通信回線，通信回路，通信デバイス等で構成された通信インタフェースであり，登録部３０６において登録処理が行われ発行されたノード情報や，リンク発行部３０８により発行されたリンク情報や，ライセンス発行部３１０により発行されたライセンスをネットワークを介してユーザ機器１０に送信する機能を有する。

【００９６】

コンテンツ鍵記憶部３１４には，コンテンツ鍵が格納されており，コンテンツ提供サーバ２０ｂで生成されたコンテンツ鍵を受信して記憶してもよいし，著作権管理サーバ２０ａにおいてコンテンツ鍵を生成して記憶してもよい。例えば，著作権管理サーバ２０ａにおいてコンテンツ鍵を生成して，そのコンテンツ鍵をユーザ機器に送信し，さらにコンテンツ提供サーバ２０ｂに送信してもよい。コンテンツ鍵を受信したコンテンツ提供サーバ２０ｂは，ユーザが購入したコンテンツをそのコンテンツ鍵で暗号化して，暗号化したコンテンツをユーザ機器１０に送信してもよい。

【００９７】

以上，著作権管理サーバ２０ａの機能構成について説明した。次に，コンテンツ提供システム１００を利用したリンク方式によるコンテンツ提供方法について説明する。図７～１１は，本実施形態にかかるリンク方式によるコンテンツ提供方法の基本的なフローを示すタイミングチャートである。コンテンツ提供システム１００に含まれるユーザ機器（ＰＣ）１０と著作権管理サーバ２０ａは，ネットワーク３０を介して安全に通信接続される。

【００９８】

＜５．ユーザ機器およびユーザ登録方法＞

図７は，ユーザ機器のうち，ネットワークに接続しているユーザ機器（ＰＣ）１０ａの登録方法を説明するタイミングチャートである。まず，ユーザ機器（ＰＣ）１０ａの特定情報を著作権管理サーバに送信する（Ｓ１０２）。ここで，ユーザ機器の特定情報とは，ユーザ機器の機器タイプ，モデル，バージョン等ユーザ機器を特定することができる情報である。このユーザ機器の特定情報は，ユーザ入力によりユーザ機器（ＰＣ）１０ａから送信されてもよいし，特定情報が予めユーザ機器（ＰＣ）１０ａに設定されている場合には，ユーザ機器（ＰＣ）１０ａと著作権管理サーバ２０ａの通信接続が確立された後，特定情報が著作権管理サーバ２０ａに送信されるようにしてもよい。

【００９９】

ステップＳ１０２において，ユーザ機器（ＰＣ）１０ａの特定情報を受信した著作権管理サーバ２０ａは，その特定情報を著作権管理サーバ２０ａに備わるユーザ情報記憶部に記憶する（Ｓ１０４）。また，送信されたユーザ機器（ＰＣ）１０ａの特定情報より，著作権管理サーバ２０ａにおいて一意に特定することができるデバイスＩＤを付与する。さらに，ユーザ機器毎にデバイス鍵を発行する。発行されたデバイスＩＤとデバイス鍵は，ユーザ機器（ＰＣ）１０ａの特定情報と関連付けられて，ユーザ情報記憶部に記憶される。デバイス鍵は，機器毎に発行される鍵であって，公開鍵暗号で使用される対となる公開鍵と秘密鍵でもよいし，秘密鍵暗号で使用される共通鍵でもよい。

【０１００】

ステップＳ１０４においてユーザ機器（ＰＣ）１０ａの登録が行われた後，ステップＳ１０４で発行されたデバイスＩＤとデバイス鍵を含むノードを発行する（Ｓ１０６）。ステップＳ１０６において発行されるノードは，著作権管理サーバ２０ａが各ユーザ機器を一意に特定することができる情報であって，少なくともデバイスＩＤが含まれるが，デバイス鍵やユーザ機器（ＰＣ）１０ａの特定情報などを含んでもよい。ステップＳ１０６において発行されたノードはユーザ機器（ＰＣ）１０ａに送信される（Ｓ１０８）。

【０１０１】

ユーザ機器（ＰＣ）１０ａは，著作権管理サーバ２０ａに送信されたノード情報をユーザ機器（ＰＣ）１０ａに備わるメモリに格納する。

【０１０２】

以上，ネットワークに接続しているユーザ機器（ＰＣ）１０ａの登録方法について説明した。次に，図８に基づいて，ネットワークに接続されていないユーザ機器，例えばＰＤ１０ｄの登録方法について説明する。

【０１０３】

図８は，ネットワークに接続されていないユーザ機器（ＰＤ）１０ｄの登録方法について説明するタイミングチャートである。まず，ユーザ機器（ＰＤ）１０ｄの特定情報がユ

ーザ機器（ＰＣ）１０ａに提供される（Ｓ１１０）。例えば，ユーザ機器（ＰＤ）１０ｄがユーザ機器（ＰＣ）１０ａに接続された後，ユーザ機器（ＰＤ）１０ｄの機器タイプ，モデル，バージョン等がユーザ機器（ＰＣ）１０ａに送信されるようにしてもよいし，ユーザの入力に応じてユーザ機器（ＰＤ）１０ｄの特定情報がユーザ機器（ＰＣ）１０ａに送信されるようにしてもよい。

【０１０４】

ステップＳ１１０において，ユーザ機器（ＰＤ）１０ｄの特定情報を取得したユーザ機器（ＰＣ）１０ａは，著作権管理サーバ２０ａにユーザ機器（ＰＤ）１０ｄの特定情報を送信する（Ｓ１１２）。ステップＳ１１２においてユーザ機器（ＰＤ）１０ｄの特定情報を受信した著作権管理サーバ２０ａは，ユーザ機器（ＰＤ）１０ｄの登録を行う（Ｓ１１４）。著作権管理サーバ２０ａは，ステップＳ１１４において，ユーザ機器（ＰＤ）１０ｄの特定情報をユーザ情報記憶部に記憶し，ユーザ機器（ＰＤ）１０ｄのデバイスＩＤとデバイス鍵を発行して，ユーザ機器（ＰＤ）１０ｄの特定情報と関連付けてユーザ情報記憶部に記憶する。

【０１０５】

ステップＳ１１４においてユーザ機器（ＰＤ）１０ｄの登録処理を行った後，著作権管理サーバ２０ａは，ユーザ機器（ＰＤ）１０ｄのノードを発行する（Ｓ１１６）。上述したように，ステップＳ１１６において発行されるノードには，著作権管理サーバ２０ａがユーザ機器（ＰＤ）１０ｄの識別情報や，デバイス鍵などが含まれている。ステップＳ１１６において発行されたユーザ機器（ＰＤ）１０ｄのノードは，ユーザ機器（ＰＣ）１０ａに送信される（Ｓ１１８）

ステップＳ１１８において著作権管理サーバ２０ａよりユーザ機器（ＰＤ）１０ｄのノード情報を送信されたユーザ機器（ＰＣ）は，ユーザ機器（ＰＤ）１０ｄのノード情報をユーザ機器（ＰＤ）１０ｄに提供する（Ｓ１２０）。ステップＳ１２０においてノード情報を提供されたユーザ機器（ＰＤ）１０ｄは，メモリ等の記憶部にノード情報を格納する。ユーザ機器（ＰＤ）１０ｄのノード情報は，ユーザ機器（ＰＣ）１０ａのメモリに格納するようにしてもよい。

【０１０６】

ユーザ機器（ＰＤ）１０ｄは，コンテンツやコンテンツを復号するためのコンテンツ鍵を取得するためには，ユーザ機器（ＰＣ）１０ａに接続する必要がある。したがって，ユーザ機器（ＰＣ）１０ａにおいてユーザ機器（ＰＤ）１０ｄの情報を記憶していれば，送信されたコンテンツをユーザ機器（ＰＤ）１０ｄで再生できるか否かをユーザ機器（ＰＣ）１０ａが判断することができる。

【０１０７】

以上，ネットワークに接続されていないユーザ機器（ＰＤ）１０ｄの登録方法について説明した。次に，図９に基づいて，ユーザ機器を使用するユーザの登録方法について説明する。

【０１０８】

図９は，ユーザの登録方法について説明するタイミングチャートである。ユーザＡの登録処理は，ネットワークに接続されているユーザ機器（ＰＣ）１０ａを介して行われる。まず，ユーザＡの特定情報が著作権管理サーバ２０ａに送信される（Ｓ１２２）。ここで，ユーザＡの特定情報は，ユーザＡのユーザＩＤとユーザＡが所持するクレジットカード番号等である。このユーザＩＤは著作権管理サーバ２０ａにおいて一意に特定することができる識別情報であり，ユーザＡが指定する識別情報でもよいし，著作権管理サーバ２０ａにおいて付与されてもよい。

【０１０９】

ステップＳ１２２においてユーザＡの特定情報を送信された著作権管理サーバ２０ａは，ユーザＡの登録処理を行う（Ｓ１２４）。ステップＳ１２４において，著作権管理サーバ２０ａは，ユーザＡのユーザＩＤとクレジットカード番号等をユーザ情報記憶部に記憶する。また，ユーザＡのユーザ鍵を発行して，ユーザＩＤ等と関連付けてユーザ情報記憶

部に記憶する。

【０１１０】

そして，著作権管理サーバ２０ａは，ユーザ情報記憶部に記憶されたユーザＩＤとユーザ鍵とを含むユーザＡのノードを発行する（Ｓ１２６）。著作権管理サーバ２０ａは，ステップＳ１２６において発行されたノード情報をユーザ機器（ＰＣ）１０ａに送信する。

【０１１１】

上述したように，ユーザ機器を所有するユーザは，ネットワークを介して著作権管理サーバ２０ａに自身の所有するユーザ機器を登録する。また，コンテンツ提供サービスや，著作権管理サービスを利用するユーザのユーザ登録を行う。これにより，著作権管理サービスを提供する著作権管理サーバ２０ａは，著作権管理サービスを利用したいユーザの情報や，そのユーザが所有するユーザ機器の情報をユーザ情報記憶部に記憶して管理することができる。また，各ユーザや，各ユーザ機器に対して発行された鍵情報も，ユーザやユーザ機器に関連付けてユーザ情報記憶部に記憶して管理することができる。

【０１１２】

著作権管理サーバ２０ａは，ネットワークに接続されたユーザ機器を介してユーザＡのユーザＩＤを取得して，そのユーザが所有しているユーザ機器や，そのユーザの鍵情報を知ることができる。例えば，コンテンツを暗号化したコンテンツ鍵を安全にユーザに配布するために，コンテンツ鍵をさらにユーザＡのユーザ鍵で暗号化してもよい。著作権管理サーバ２０ａは，取得したユーザＡのユーザＩＤを基に，ユーザ情報記憶部に記憶されたユーザＡの暗号鍵を取得して，コンテンツ鍵をユーザＡのユーザ鍵で暗号化する。ユーザＡの公開鍵で暗号化されたコンテンツ鍵は，ユーザＡの秘密鍵を用いなければ復号することができないため，著作権管理サーバ２０ａはコンテンツ鍵を安全にユーザに送信することが可能となる。さらに，コンテンツを購入したユーザＡのみしかコンテンツ鍵を復号することができないため，コンテンツ鍵を復号可能なユーザを制限することも可能となる。

【０１１３】

しかし，ユーザＡの暗号鍵によりコンテンツ鍵が復号できたとしても，ユーザＡの所有するユーザ機器でコンテンツが再生できなければ，ユーザＡはコンテンツを聴くことができない。本実施形態においては，ユーザ機器をユーザに関連付けることにより，ユーザＡが購入したコンテンツをユーザ機器において再生することが可能となる。次に，ユーザＡとユーザ機器の関連付けについて説明する。

【０１１４】

＜６．ユーザＡとユーザ機器の関連付け＞

図１０および１１は，ユーザＡとユーザ機器との関連付けを説明するタイミングチャートである。まず，ネットワークに接続されたユーザ機器（ＰＣ）１０ａと，ユーザＡとの関連付けについて説明する。ユーザ機器（ＰＣ）１０ａとユーザＡとを関連付ける場合には，上述の登録処理により発行されたユーザ機器（ＰＣ）１０ａのノードと，ユーザＡのノードを著作権管理サーバ２０ａに送信する（Ｓ１３０）。

【０１１５】

ステップＳ１３０において，ユーザ機器（ＰＣ）１０ａのノード情報と，ユーザＡのノード情報を取得した著作権管理サーバ２０ａは，ユーザ機器（ＰＣ）１０ａとユーザＡを関連づけるリンクを生成する（Ｓ１３２）。ステップＳ１３２において生成されるリンクには，例えば，ユーザ機器（ＰＣ）１０ａのノード情報と，ユーザＡのノード情報と，関連付けの方向とが含まれている。リンク情報に含まれるノード情報は，ユーザ機器やユーザを一意に識別できる情報であればよく，ユーザ機器のデバイスＩＤやユーザのユーザＩＤでもよい。関連付けの方向とは，どのノードがどのノードに関連付けられているかを表す情報である。ユーザ機器（ＰＣ）１０ａがユーザＡに関連付けられている場合，関連付けの方向は，リンク元となるユーザ機器（ＰＣ）１０ａからリンク先となるユーザＡへの方向を表す情報となる。

【０１１６】

ここで，図１１に基づいてステップＳ１３２において生成されるリンクについて詳細に

説明する。上述したように，ユーザ機器（ＰＣ）１０ａやユーザＡは，著作権管理サーバ２０ａにおいて，デバイスＩＤやユーザＩＤによりノードとして管理される。このノード情報４００，４０２が著作権管理サーバ２０ａに送信されると，著作権管理サーバ２０ａは，リンク４０４に含まれる「Ｆｒｏｍ」４０６と，「Ｔｏ」４０８の情報を設定する。ユーザ機器（ＰＣ）１０ａをユーザＡに関連付ける場合には，「Ｆｒｏｍ」にリンク元となるユーザ機器（ＰＣ）１０ａのノードＩＤを設定し，「Ｔｏ」にリンク先となるユーザＡのノードＩＤを設定する。ここでノードＩＤとは，ユーザ機器（ＰＣ）１０ａやユーザＡなどのノードを識別する識別情報であって，ユーザ機器（ＰＣ）１０ａのデバイスＩＤやユーザＡのユーザＩＤでもよい。

【０１１７】

また，リンク４０４には，リンク先となるユーザＡの秘密情報をリンク元となるユーザ機器（ＰＣ）１０ａの公開鍵で暗号化した鍵情報を含んでもよい。ユーザＡの秘密情報とは，本来ユーザＡしか知ることのできない情報であって，ユーザＡの秘密鍵の情報などである。

【０１１８】

図１０に戻り，ステップＳ１３２により生成されたリンク情報は，リンク元であるユーザ機器（ＰＣ）１０ａのデバイスＩＤと関連付けられて，ユーザ情報記憶部に記憶される（Ｓ１３４）。これにより，著作権管理サーバ２０ａは，ユーザ情報記憶部に記憶されているユーザ機器がどのユーザと関連付けられているかを管理することができる。そして，ユーザ機器のデバイスＩＤとユーザのユーザＩＤと関連付けの方向を含むリンク情報を発行して（Ｓ１３６），ユーザ機器（ＰＣ）１０ａに送信する（Ｓ１３８）。上述したように，ユーザ機器（ＰＣ）１０ａに送信されるリンク情報には，ユーザＡの秘密情報をユーザ機器（ＰＣ）１０ａの公開鍵で暗号化された鍵情報を含んでもよい。

【０１１９】

ステップＳ１３８においてリンク情報を受信したユーザ機器（ＰＣ）１０ａは，受信したリンク情報により，自身がどのユーザと関連付けられているかを知ることができる。また，ユーザ機器（ＰＣ）１０ａがユーザＡに関連付けられている場合には，リンクに含まれている鍵情報によって，ユーザＡの秘密情報を知ることができる。例えばユーザＡがコンテンツ提供サービスに登録し，コンテンツを購入した場合，そのコンテンツは暗号化されたユーザＡに送信される。コンテンツを暗号化したコンテンツ鍵は，ユーザＡの秘密鍵で暗号化されてユーザＡが所有するユーザ機器（ＰＣ）１０ａに送信される。このとき，ユーザ機器（ＰＣ）１０ａがユーザＡに関連付けられていれば，ユーザ機器（ＰＣ）１０ａは，著作権管理サーバ２０ａより送信されたリンク情報に含まれるユーザＡの秘密情報を取得して，暗号化されたコンテンツ鍵を復号することができる。

【０１２０】

以上，ネットワークに接続されたユーザ機器（ＰＣ）１０ａとユーザＡとの関連付けについて説明した。次に，図１２に基づいて，ネットワークに接続されていないユーザ機器（ＰＤ）１０ｄとユーザ機器（ＰＣ）１０ａとの関連付けについて説明する。

【０１２１】

まず，ユーザ機器（ＰＣ）１０ａは，ユーザ機器（ＰＣ）１０ａに接続されたユーザ機器（ＰＤ）１０ｄのノード情報を取得する（Ｓ１４０）。ステップＳ１４０においてユーザ機器（ＰＤ）１０ｄのノード情報を取得したユーザ機器（ＰＣ）１０ａは，ユーザ機器（ＰＤ）のノード情報と，自身のノード情報を著作権管理サーバ２０ａに送信する（Ｓ１４２）。ステップＳ１４２において，２のノード情報とともに，関連付けの方向も送信するようにしてもよい。

【０１２２】

ステップＳ１４２において，ユーザ機器のノードと関連付けの方向の情報を受信した著作権管理サーバ２０ａは，受信した情報を基に，リンクを生成する（Ｓ１４４）。上述したように，ステップＳ１４４において生成されるリンク情報は，ユーザ機器（ＰＤ）１０ｄのノード情報と，ユーザ機器（ＰＣ）１０ａのノード情報と，関連付けの方向の情報と

が含まれている。

【０１２３】

ステップＳ１４４において生成されたリンク情報は，ユーザ情報記憶部にユーザ機器（ＰＤ）１０ｄのデバイスＩＤと関連付けられて記録される（Ｓ１４６）。そして，ユーザ機器（ＰＤ）１０ｄのノード情報と，ユーザ機器（ＰＣ）１０ａのノード情報と，関連付けの方向の情報とが含まれているリンク情報が発行され（Ｓ１４８），ユーザ機器（ＰＣ）１０ａに送信される（Ｓ１５０）。

【０１２４】

ステップＳ１５０において著作権管理サーバ２０ａよりリンク情報を受信したユーザ機器（ＰＣ）１０ａは，そのリンク情報をユーザ機器（ＰＤ）１０ｄに提供する（Ｓ１５２）。上述したように，リンク情報には，ユーザ機器（ＰＤ）１０ｄがユーザ機器（ＰＣ）１０に関連付けられているという情報が含まれている。つまり，リンクの「Ｆｒｏｍ」にユーザ機器（ＰＤ）１０ｄのノード情報が設定され，「Ｔｏ」にユーザ機器（ＰＣ）１０ａのノード情報が設定されている。

【０１２５】

また，リンクには，ユーザ情報記憶部に記憶されているユーザ機器（ＰＣ）１０ａの秘密鍵が，ユーザ機器（ＰＤ）１０ｄの公開鍵等により暗号化された鍵情報も含まれている。ユーザ機器（ＰＤ）１０ｄは，リンク情報を取得することにより，ユーザ機器（ＰＣ）１０ａの秘密鍵の情報を取得することが可能となる。

【０１２６】

さらに，ステップＳ１４８のリンク発行の際に，ユーザ機器（ＰＤ）１０ｄのリンク先となるユーザ機器（ＰＣ）１０ｃのリンク情報を送信するようにしてもよい。ユーザ機器（ＰＣ）１０ａがユーザＡと関連付けられている場合，ユーザ機器（ＰＤ）１０ｄには，ユーザ機器（ＰＣ）１０ａとユーザＡとを関連付けるリンク情報も送信される。これにより，ユーザ機器（ＰＤ）１０ｄは，ユーザ機器（ＰＣ）１０ａの秘密鍵の情報を取得した後，ユーザ機器（ＰＣ）１０ａの秘密鍵の情報を用いてユーザＡの秘密鍵の情報も取得することが可能となる。

【０１２７】

図１３に基づいて，リンクに含まれる鍵情報について説明する。図１３は，リンクに含まれる鍵情報を説明する説明図である。

【０１２８】

図１３に示したように，ノードＡ，ノードＢ，ノードＣの３つのノードが著作権管理サーバ２０ａのユーザ情報記憶部に記憶されていたとする。上述したように，ユーザ機器やユーザに対してそれぞれ識別情報と鍵情報などを含むノード情報が割り当てられる。各ユーザやユーザ機器に対して，それぞれ，秘密鍵，公開鍵，共通鍵等が発行される。

【０１２９】

各ノードに含まれる鍵情報について説明すると，ノードＡには，ノードＡの公開鍵（Ｋｐｕｂ[Ａ]）４１０１と，秘密鍵（Ｋｐｒｉｖ[Ａ]）４１０２と，共通鍵（Ｋｓ[Ａ]）４１０３が含まれる。公開鍵暗号方式により暗号化が行われる場合には，公開鍵４１０１を用いて暗号化を行い，公開鍵４１０１と対となる秘密鍵４１０２を用いて復号化が行われる。また，共通鍵暗号方式により暗号化が行われる場合には，暗号化と復号化に同一の鍵が使用され，共通鍵４１０３を用いて暗号化を行い，共通鍵４１０３を用いて復号化が行われる。

【０１３０】

上記公開鍵暗号方式は，暗号化用の鍵は公開され，復号化用の鍵を秘密に保つ方法である。例えば，ノードＡの公開鍵４１０１はネットワーク上の公開鍵ファイルに格納され，誰でも自由に参照することができる。一方公開鍵４１０１と対となる秘密鍵４１０２は，鍵の所有者以外の者が取得することができないように，秘密に管理されるべきものである。

【０１３１】

また，上記共通鍵暗号方式は，送信側と受信側が共通鍵を共有し，秘密にする方法である。例えば，ノードＡの共通鍵４１０３は，著作権管理サーバ２０ａとノードＡ以外のものが取得することができないように，秘密に管理されるべきものである。

【０１３２】

同様に，ノードＢ４１２には，ノードＢの公開鍵（Ｋｐｕｂ[Ｂ]）４１２１と，秘密鍵（Ｋｐｒｉｖ[Ｂ]）４１２２と，共通鍵（Ｋｓ[Ｂ]）４１２３が含まれる。ノードＣ４１４には，ノードＣの公開鍵（Ｋｐｕｂ[Ｃ]）４１４１と，秘密鍵（Ｋｐｒｉｖ[Ａ]）４１４２と，共通鍵（Ｋｓ[Ａ]）４１４３が含まれる。

【０１３３】

図１３に示したように，ノードＡをノードＢに関連付ける場合には，リンク４１６が発行される。リンク４１６には，ノードＡのノードＩＤと，ノードＢのノードＩＤとノードＡとノードＢの関連付けの方向の情報が含まれている。上述したように，ノードＡがノードＢに関連付けられている場合には，リンク元がノードＡとなり，リンク先がノードＢとなる。さらに，リンク４１６には，ノードＢの秘密情報となる秘密鍵４１２２と共通鍵４１２３が，ノードＡの公開鍵４１０１または共通鍵４１０３で暗号化された鍵情報が含まれる。

【０１３４】

リンク４１６を取得したノードＡは，自身がどのノードに関連付けられているかを知るとともに，関連付けられたリンク先の秘密情報を取得することができる。リンク４１６に含まれるノードＢの秘密情報は，ノードＡの公開鍵４１０１または共通鍵４１０３で暗号化されているため，ノードＡにより秘密に管理されているノードＡの秘密鍵４１０２または共通鍵４１０３でなければ復号することができない。つまり，リンク４１６に含まれる鍵情報は，ノードＡ以外のものが取得しても復号することができない。

【０１３５】

同様に，リンク４１８には，ノードＢのノードＩＤと，ノードＣのノードＩＤと，ノードＢとノードＣとの関連付けの方向の情報が含まれている。リンク４１８に含まれる関連付けの方向は，ノードＢからノードＣに向かう方向となり，リンク元がノードＢとなり，リンク先がノードＣとなる。また，リンク４１８には，ノードＣの秘密情報が，ノードＢの公開鍵４１２２または共通鍵４１２３により暗号化された情報も含まれている。ノードＢは，リンク４１８により，ノードＣの秘密鍵４１４２または共通鍵４１４３を取得することが可能となる。

【０１３６】

例えば，ノードＣがコンテンツを購入するユーザに割り当てられた情報であったとする。コンテンツを購入したユーザは，ノードＣを著作権管理サーバ２０ａに送信する。ユーザのノードであるノードＣを受信した著作権管理サーバ２０ａは，ユーザが購入したコンテンツを暗号化したコンテンツ鍵（ＫＣ）をユーザの公開鍵であるノードＣの公開鍵（Ｋｐｕｂ[Ｃ]）で暗号化する。ノードＣの公開鍵４１４１で暗号化されたコンテンツ鍵４２０は，ユーザの所有しているユーザ機器（ＰＣ）に送信される。

【０１３７】

ユーザの所有するユーザ機器（ＰＣ）にノードＢが割り当てられた場合，ノードＣの公開鍵で暗号化されたコンテンツ鍵をノードＢの秘密鍵で復号化できなければ，コンテンツ鍵で暗号化されたコンテンツをユーザ機器（ＰＣ）で再生することができない。しかし，ノードＢにリンク４１８が発行されていれば，ノードＢは，リンク４１８の情報を基に，ノードＣの秘密情報を取得することができる。ノードＢを割り振られたユーザ機器（ＰＣ）がノードＣを割り振られたユーザの秘密情報を取得することができれば，その秘密情報に含まれるユーザの秘密鍵を用いて，コンテンツ鍵４２０を復号することができ，コンテンツ鍵４２０で暗号化されたコンテンツを復号化することができる。

【０１３８】

同様の方法で，ユーザ機器（ＰＣ）に接続されたユーザ機器（ＰＤ）にノードＡが割り振られた場合，ユーザ機器（ＰＤ）は，自身の鍵で暗号化されているノードＢの秘密情報

を復号化することができる。さらに，リンク４１６に含まれたノードＢの秘密鍵で，リンク４１８に含まれているノードＣの秘密情報を復号化することができる。ノードＣの秘密鍵を取得したノードＡを割り振られたユーザ機器（ＰＤ）は，ノードＣの公開鍵で暗号化されているコンテンツ鍵４２０を復号化し，コンテンツ鍵４２０で暗号化されたコンテンツを復号化することができる。

【０１３９】

図１３では，ノードＡがノードＢに関連付けられており，ノードＢがノードＣに関連付けられているが，ノードＡを直接ノードＣに関連付けてもよい。その場合，ノードＡに対して発行されるリンク情報には，リンク元にノードＡのノードＩＤが設定され，リンク先にノードＣのノードＩＤが設定される。また，ノードＣの秘密情報がノードＡの公開鍵により暗号化された鍵情報が含まれる。

【０１４０】

コンテンツを購入したユーザが，そのコンテンツをユーザが所有するユーザ機器で再生するには，ユーザ機器がコンテンツ鍵を暗号化したユーザ鍵の情報を取得している必要がある。各ユーザ機器は，自身に発行されたリンク情報を基に，コンテンツ鍵が暗号化されているユーザ鍵を取得して，コンテンツ鍵を復号する。

【０１４１】

このように，コンテンツを暗号化したコンテンツ鍵をユーザの公開鍵で暗号化して，ユーザが所有するユーザ機器に送信すれば，ユーザに関連付けられたユーザ機器において，暗号化されたコンテンツを復号化して再生することが可能となる。コンテンツを暗号化するコンテンツ鍵は，再生するユーザ機器毎に固有の鍵で暗号化されていなくても，リンク情報を基にコンテンツ鍵が暗号化されている鍵情報を取得してコンテンツ鍵を復号化することができる。ユーザ機器は，リンク情報により自身がどのユーザに関連付けられているかを知ることができる。つまり，リンク情報により，ユーザ機器はどのユーザの秘密情報を取得することができるかを知ることが可能となる。

【０１４２】

以上，リンクに含まれる鍵情報について説明した。次に図１４に基づいて，著作権管理サーバ２０ａにおいて発行されるライセンスについて説明する。

【０１４３】

＜７．ライセンスについて＞

図１４は，著作権管理サーバ２０ａにおけるライセンスの発行について説明するタイミングチャートである。著作権管理サーバ２０ａにおいて発行されるライセンスには，ユーザが購入したコンテンツを再生するために必要な，コンテンツを復号化するコンテンツ鍵等の情報が含まれている。ライセンスに含まれるコンテンツ鍵はさらにユーザ鍵等によって暗号化されており，ライセンスを取得したユーザ機器等は，ライセンスに含まれた各情報により，コンテンツ鍵がどのユーザ鍵で暗号化されているかを知ることができる。ラインセンスを取得したユーザ機器等は，上述したリンク情報等を基に，コンテンツ鍵を復号化することができれば，そのコンテンツ鍵で暗号化されたコンテンツを再生することが可能となる。

【０１４４】

ユーザ機器（ＰＣ）１０ａは，コンテンツを再生するために必要なライセンスを取得するために，コンテンツを一意に識別するコンテンツＩＤと，ユーザＡのノード情報とを著作権管理サーバ２０ａに送信する（Ｓ１６０）。上述したように，ユーザＡが所有するユーザ機器がユーザＡに関連付けられていれば，ユーザＡに対して発行されたライセンスを，ユーザＡに関連付けられたユーザ機器も使用することが可能となる。

【０１４５】

ステップＳ１６０において，コンテンツＩＤとユーザＡのノード情報を受信した著作権管理サーバ２０ａは，コンテンツを暗号化したコンテンツ鍵をユーザＡの公開鍵で暗号化する（Ｓ１６２）。そして，著作権管理サーバ２０ａは，ステップＳ１６２において暗号化したコンテンツ鍵を含むライセンスを生成する（Ｓ１６４）。

【０１４６】
図１５に基づいて，ステップＳ１６４において生成されるライセンスについて説明する。図１５に示したように，ライセンス４４０は，コンテンツ鍵４４１と，コントロール４４４と，プロテクタ４４７と，コントローラ４５０などを含む。また，コンテンツ４３０は，ライセンスに含まれるコンテンツ鍵により暗号化されており，コンテンツ提供サーバ２０ｂより送信される。
【０１４７】
ライセンス４４０に含まれるコンテンツ鍵４４１は，ユーザ機器（ＰＣ）１０ａにより送信されたノード情報に含まれる鍵で暗号化されている。例えば，ユーザＡのノード情報がユーザ機器（ＰＣ）より送信された場合には，ユーザＡの公開鍵でコンテンツ鍵が暗号化される。プロテクタ４４７には，コンテンツの識別情報であるコンテンツＩＤと，コンテンツ鍵の識別情報であるコンテンツ鍵ＩＤが含まれる。プロテクタ４４７に含まれる情報によって，ライセンス４４０が，どのコンテンツを再生する際に使用されるライセンスなのかがわかる。
【０１４８】
コントロール４４４には，コンテンツの利用条件等であるコントロールコード４４６が含まれる。コントロールコード４４６には，ユーザが購入したコンテンツの再生期限などが含まれ，コントロールコードに記述された利用条件の範囲内において，ユーザはコンテンツを利用することとなる。またコントロールコード４４６には，ライセンス４４０がどのノードに対して発行されたライセンスなのかがわかる情報が含まれていてもよい。
【０１４９】
ライセンス４４０を取得したユーザ機器は，コントロール４４４を参照して，ライセンス４４０がどのノードに対して発行されたものかを判別する。判別の結果，ユーザ機器に関連付けられたユーザに対して発行されたライセンスであれば，ユーザ機器はそのライセンスを利用して，コンテンツを再生することができる。
【０１５０】
コントローラ４５０は，コンテンツ鍵４４１とコントロール４４４とを関連付ける情報であって，コンテンツ鍵４４１の識別情報と，コントロール４４４の識別情報が含まれている。また，コンテンツ鍵４４１およびコントロール４４４の改ざんを判別するため，コンテンツ鍵４４１のハッシュ値４５３と，コントロール４４４のハッシュ値４５４を含んでもよい。例えば，著作権管理サーバ２０ａからユーザ機器等に送信される際に，ライセンス４４０に含まれるコンテンツ鍵４４１が改ざんされた場合には，コンテンツ鍵４４１より求められるハッシュ値と，コントローラに含まれるハッシュ値とが異なる値となり，コンテンツ鍵４４１が改ざんされたか否かを判定することができる。コントロール４４４についても，コントロールハッシュ値４５４により改ざんの判別をすることができ，ライセンスを送信する際に，コンテンツの利用条件等の書き換えを発見することが可能となる。以上，ライセンスについて説明した。
【０１５１】
図１４に戻り，ステップＳ１６４において生成されたライセンスは，ユーザ機器（ＰＣ）１０ａに対して発行され（Ｓ１１６），ユーザ機器（ＰＣ）１０ａに送信される（Ｓ１６８）。
【０１５２】
ステップＳ１６８によりライセンスを受信したユーザ機器（ＰＣ）１０ａは，ユーザ機器（ＰＣ）１０ａを所有するユーザのユーザ鍵で暗号化されたコンテンツ鍵を，リンクに含まれる鍵情報を用いて復号する。そして，ユーザ機器（ＰＣ）１０ａにおいて，コンテンツ鍵で暗号化されたコンテンツを，復号化したコンテンツ鍵で復号して再生することが可能となる。
【０１５３】
以上，ライセンスの発行について説明した。
【０１５４】

次に，図１６に基づいて，ユーザ機器が持つ鍵束の概念について説明する。各ユーザ機器はコンテンツ鍵を復号化するために必要な鍵束を持ち，その鍵束を用いて暗号化されたコンテンツ鍵を復号化する。

【０１５５】

図１６は，本実施形態にかかる鍵管理の概念図である。４６０に示されるように，本実施形態においては木構造の概念が採用されている。すなわちＫｒｏｏｔ鍵４６１を頂点として、各ノードにはＫ０鍵４６２，Ｋ１鍵４６３，Ｋ１０鍵４６４，Ｋ１１鍵４６５・・・というようにノード鍵が割り当てられている。また最下段にはＫＩ鍵４６８，ＫＪ鍵４６９・・・というように，各ユーザ機器であるＩ，Ｊが固有に保有するユーザ鍵が割り当てられる。ここで各ノード鍵は，木構造上の直下のノード鍵によって暗号化されているものとする。例えばＫ１鍵４６３は，Ｋ１０鍵４６４またはＫ１１鍵４６５によって暗号化されている。

一方で，ｐｕｂ（ｏｒ　Ｓｅｃ）Ｋｅｙ４７１はＫｒｏｏｔ鍵４６１に相当する。つまり，コンテンツ鍵４７２はＫｒｏｏｔ鍵４６１によって暗号化されている。図１３においては，コンテンツ鍵はノードＣの公開鍵によって暗号化されたが，より詳細にはコンテンツ鍵はＫｒｏｏｔ鍵４６１によって暗号化される。

ここで例えばユーザ機器Ｉが，コンテンツを復号化するコンテンツ鍵４７２を取得するためには，ＫＩ鍵，Ｅ（ＫＩ鍵，Ｋ１００鍵），Ｅ（Ｋ１００鍵，Ｋ１０鍵），Ｅ（Ｋ１０鍵，Ｋ１鍵），Ｅ（Ｋ１鍵，Ｋｒｏｏｔ鍵），Ｅ（ｐｕｂ（ｏｒ　Ｓｅｃ）Ｋｅｙ，ＣＫ）から構成される鍵束が必要になる。当該鍵束はコンテンツ本体に含まれる。

【０１５６】

このように，ユーザが所有するユーザ機器は，それぞれが持っている鍵束を用いて，Ｋｒｏｏｔ鍵４６１を取得して，コンテンツ鍵４７２を復号化することができる。

【０１５７】

以上，コンテンツ提供システム５００において採用される著作権管理方式について説明した。次に，図１７に基づいて，コンテンツ提供システム５００の全体構成について説明する。

【０１５８】

＜８．コンテンツ提供システム５００の全体構成＞

図１７に示すように，本実施形態にかかるコンテンツ提供システム５００は，コンテンツの提供元となるコンテンツ再生装置５０ａ（ＰＣ１）と，コンテンツ再生装置５０ａが保有するコンテンツを利用するコンテンツ再生装置５０ｂ（ＰＣ２），５０ｃ（ＰＣ３）を含んで構成される。なお，本実施形態において，コンテンツ提供元はコンテンツ再生装置５０ａを使用するユーザであり，コンテンツ再生装置５０ａには，コンテンツ再生装置５０ａの識別情報とユーザとを関連付けるリンク情報（リンク１）が著作権管理サーバ（図示せず）より発行されている。従って，コンテンツ発行元はユーザであるが，説明の便宜上，以後ではコンテンツ再生装置５０ａをコンテンツ提供元装置とも称する。

【０１５９】

コンテンツ再生装置５０ａ，５０ｂ，５０ｃは，コンテンツ鍵により暗号化されたコンテンツを復号し，再生するコンピュータである。コンテンツ再生装置５０ａ，５０ｂ，５０ｃとしては，パーソナルコンピュータ，ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ），携帯型のコンテンツ再生装置であるポータブルデバイス（ＰＤ）などを例示できる。ＰＤとは，より具体的には，例えば数十ＧＢの記憶容量を有するハードディスクドライブ（ＨＤＤ）を備えた携帯型オーディオプレーヤなどである。また，携帯型映像／音声プレーヤ，携帯電話，ＰＨＳなど，各種の携帯可能な装置であってもよい。

【０１６０】

コンテンツ再生装置５０ａは，上述のリンク方式の著作権管理方法において説明した著作権管理サーバ２０ａから，コンテンツ再生装置５０ａを使用するユーザ１（Ｕｓｅｒ１）のユーザＩＤと関連付けられたリンク情報であるリンク１を発行されており，ユーザ１

に対して発行されたライセンスに対応するコンテンツを再生することができる。また，コンテンツ再生装置５０ａは，コンテンツ再生装置５０ａが再生できるコンテンツをコンテンツ再生装置５０ｂと共有するために，コンテンツ再生装置５０ｂとコンテンツ再生装置５０ａとを関連付けるリンク情報であるリンク２を生成し，リンク１とリンク２をコンテンツ再生装置５０ｂに発行することができる。同様に，コンテンツ再生装置５０ａは，コンテンツ再生装置５０ａが再生できるコンテンツをコンテンツ再生装置５０ｃと共有するために，コンテンツ再生装置５０ｃとコンテンツ再生装置５０ａとを関連付けるリンク情報であるリンク３を生成し，リンク１とリンク３をコンテンツ再生装置５０ｂに発行することができる。コンテンツ再生装置５０ｂおよびコンテンツ再生装置５０ｃは，コンテンツ再生装置５０ａから発行されたリンク情報を辿ることにより，ユーザ１に発行されたライセンスに対応するコンテンツを再生することができる。

【０１６１】

リンク情報には，上述のように，ノード情報と，ノード間の関連付けの方向と，関連付けの方向においてリンク先（Ｔｏ）に設定されているノードに固有の鍵（秘密鍵）をリンク元（Ｆｏｒｍ）に設定されているノードに固有の鍵（公開鍵）で暗号化したものが含まれる。さらにコンテンツ提供システム５００では，リンク情報の利用を制限するための利用制限情報が含まれる。コンテンツ提供システム５００におけるリンク情報の利用には，コンテンツの再生のためにリンク情報を辿ってコンテンツ鍵を暗号化しているユーザ鍵を取得することと，自装置と他のコンテンツ再生装置とを関連付けるリンク情報を生成して，生成したリンク情報とともにユーザ鍵の取得に必要なリンク情報を他のコンテンツ再生装置に発行することと，を含む。利用制限情報について図１７に示した例を参照して具体的に説明する。

【０１６２】

本実施形態におけるリンク情報５００２には，利用制限情報の一例として，有効期間情報５００６，ホップカウント情報５００８およびリンク発行可能回数５０１０が含まれる。有効期間情報５００６は，リンク情報５００２を利用できる期間を制限するための情報である。有効期間情報５００６は，復号制限情報の一例でもあり，転送制限情報の一例でもある。コンテンツ再生装置は，リンク情報を利用する際に，この有効期間情報５００６を参照する。有効期間内であればコンテンツ再生装置はリンク情報を辿ることによりユーザ鍵を取得し，そのユーザ鍵を用いてコンテンツ鍵を復号し，コンテンツの再生を行うことができる。一方，有効期間外であれば，コンテンツ再生装置はもはやリンク情報を利用することはできないため，ユーザ鍵やその間に介在するデバイス鍵を利用することはできず，コンテンツの再生を行うことはできない。また，コンテンツ再生装置は，後述のホップカウント情報５００８およびリンク発行可能回数５０１０によりリンク情報の発行を制限されるが，有効期間情報５００６によってもリンク情報の発行を制限される。ホップカウント情報５００８やリンク発行可能回数５０１０によってリンク情報の発行が許可されている場合でも，有効期間外である場合にはコンテンツ再生装置は他のコンテンツ再生装置にリンク情報を発行することができない。コンテンツ再生装置は，発行するリンク情報に有効期間情報５００６を含ませるが，その設定値は，自己が利用しているリンク情報に含まれる値と同じであってもよいし，違う値であってもよい。

【０１６３】

具体的には，例えば図示のようにコンテンツ再生装置５０ａに発行されたリンク情報であるリンク１において，有効期間情報５００６に「２００５／１２／３１」が設定されている。コンテンツ再生装置５０ａは，２００５年１２月３１日まで，リンク１を利用してコンテンツの再生やリンク情報の発行をすることができる。コンテンツ再生装置５０ａが発行したリンク情報であるリンク２またはリンク３にも，同様に有効期間情報５００６が設定されており，設定値は図示の例ではリンク１と同様に「２００５／１２／３１」である。つまり，コンテンツ再生装置５０ｂまたはコンテンツ再生装置５０ｃは，２００５年１２月３１日までリンク２またはリンク３を利用してコンテンツの再生やリンク情報の発行を行うことができる。

【０１６４】
なお，リンク２やリンク３の有効期間情報５００６の設定値を，例えば「２００５／１１／３０」のようにリンク１の設定値と異なる値にすることもできる。リンク２またはリンク３の発行元であるコンテンツ再生装置５０ａが設定値を自由に決めることができてもよいし，設定値についての規則がリンク情報に含まれており，コンテンツ再生装置５０ａはその規則に基づいて値を設定してもよい。例えば，発行するリンク情報には，元となるリンク情報に含まれる有効期間よりも１ヶ月短い期間を有効期間として設定する，という規則がリンク情報に含まれており，コンテンツ再生装置５０ａはリンク情報の発行時にその規則に基づいて有効期間を計算し，値を設定してもよい。
【０１６５】
ホップカウント情報５００８およびリンク発行可能回数５０１０は，転送制限情報の一例であり，リンク情報の発行を制限する情報の例である。リンク情報の発行を制限することで，ユーザ鍵やデバイス鍵の転送を制限する。ホップカウント情報５００８は，何世代までリンク情報の発行を許可するかを制限する情報である。具体的には，例えば図示のようにコンテンツ再生装置５０ａに発行されたリンク情報であるリンク１において，ホップカウント情報５００８に「１」が設定されている。そうすると，コンテンツ再生装置５０ａは１世代までリンク情報の発行が可能であり，コンテンツ再生装置５０ａはコンテンツ再生装置５０ｂまたはコンテンツ再生装置５０ｃにリンク情報を発行することができる。リンク情報の発行の際にコンテンツ再生装置５０ａは，発行するリンク情報に利用制限情報を含ませる。コンテンツ再生装置５０ａが発行するリンク情報（リンク２またはリンク３）に含まれるホップカウント情報５００８には，「０」が設定される。コンテンツ再生装置５０ａは上述のようにリンク１によって１世代までしかリンク情報の発行を許可されていないため，発行先であるコンテンツ再生装置５０ｂまたはコンテンツ再生装置５０ｃにリンク情報の発行を許可することはできない。リンク２またはリンク３のホップカウント情報に「０」が設定されていれば，リンク２またはリンク３を利用するコンテンツ再生装置５０ｂまたはコンテンツ再生装置５０ｃは他のコンテンツ再生装置にリンク情報を発行することはできない。
【０１６６】
もし，リンク１のホップカウント情報に「２」が設定されていれば，リンク２またはリンク３のホップカウント情報には「１」が設定され，リンク２またはリンク３を発行されたコンテンツ再生装置５０ｂまたはコンテンツ再生装置５０ｃは，さらに他のコンテンツ再生装置にリンク情報を発行することができる。その場合にコンテンツ再生装置５０ｂまたはコンテンツ再生装置５０ｃが他のコンテンツ再生装置に発行するリンク情報のホップカウント情報には「０」が設定される。このように，リンク情報を発行されたコンテンツ再生装置は，リンク情報に含まれる利用制限情報に基づいてリンク情報の発行を制限される。また，コンテンツ再生装置は自己が利用するリンク情報の利用制限情報に基づいて新たな利用制限情報を生成し，生成した利用制限情報を発行するリンク情報に含ませることができる。
【０１６７】
利用制限情報にホップカウント情報を含ませることにより，サービス事業者からコンテンツを取得した取得者が，取得したコンテンツを他の利用者（例えば，友達）に提供してコンテンツを共有することができる一方で，そのコンテンツがさらに他の利用者（例えば，コンテンツを提供された友達の友達など）にまで流出してしまうことを防止することができる。従って，サービス事業者は，正当にコンテンツを取得した取得者に対して，所定の範囲内でそのコンテンツを流通させて他の利用者と共有させることを認めながらも，コンテンツの新たな販売の機会を逸することはなく，またコンテンツの著作権を保護できる。
【０１６８】
リンク情報の発行を制限する情報の他の例であるリンク発行可能回数５０１０は，リンク情報を発行する回数を制限するための情報である。コンテンツ再生装置は，リンク発行

発行可能回数５０１０に設定されている回数だけ，リンク情報を他のコンテンツ再生装置に発行することができる。具体的には，例えば図示のようにコンテンツ再生装置５０ａに発行されたリンク情報であるリンク１において，リンク発行可能回数５０１０に「２」が設定されている。そうすると，コンテンツ再生装置５０ａは２回までリンク情報の発行が可能であり，コンテンツ再生装置５０ａはまずコンテンツ再生装置５０ｂにリンク２を発行する。コンテンツ再生装置５０ａはリンク情報を発行するたびに，自己が利用しているリンク情報であるリンク１のリンク発行可能回数５０１０に設定されている数値をデクリメントする。そうすると，リンク２の発行後は，リンク１のリンク発行可能回数５０１０には「１」が設定され，コンテンツ再生装置５０ａは，あと１回リンク情報を発行することができる。その後，コンテンツ再生装置５０ａがコンテンツ再生装置５０ｃにリンク情報を発行すると，リンク１のリンク発行可能回数５０１０は「０」に設定され，コンテンツ再生装置５０ａはそれ以上リンク情報を発行することができない。一方，リンク２およびリンク３では，ホップカウント情報５００８に「０」が設定されているため，リンク発行可能回数５０１０も「０」に設定される。なお，リンク２またはリンク３においてホップカウント情報５００８に「０」以外が設定される場合には，リンク発行可能回数５０１０は，リンク２またはリンク３の発行元であるコンテンツ再生装置５０ａが任意の値を設定できるようにしてもよいし，リンク２またはリンク３の元となるリンク１と同じ値（図示の例では「２」）が設定されてもよい。また，有効期間情報５００６と同様に，設定値についての規則がリンク情報に含まれており，コンテンツ再生装置５０ａはその規則に基づいて値を設定してもよい。

【０１６９】

リンク情報にリンク発行可能回数５０１０を含ませることにより，サービス事業者からコンテンツを取得した取得者が，取得したコンテンツを提供できる他の利用者の数を定めることができる。従って，サービス事業者は，正当にコンテンツを取得した取得者に対して，所定の範囲内でそのコンテンツを流通させて他の利用者と共有させることを認めながらも，コンテンツの新たな販売の機会を逸することはなく，またコンテンツの著作権を保護できる。

【０１７０】

上述のように，本実施形態にかかるコンテンツ提供システム５００におけるコンテンツ再生装置（５０ａ）は，自己が保有するリンク情報に基づいて新たにリンク情報を生成し，他のコンテンツ再生装置に提供することができる。また，その際に，自己が保有するリンク情報に含まれる利用制限情報に基づいて，新たに利用制限情報を生成し，発行するリンク情報に含ませることができる。一方で，コンテンツ再生装置（５０ｂ，５０ｃ）は，コンテンツの提供元であるコンテンツ再生装置からリンク情報を取得し，そのリンク情報に基づいてコンテンツを再生することができる。本実施形態にかかるコンテンツ再生装置は，コンテンツ再生装置５０ａの機能のみを備えていてもよいし，コンテンツ５０ｂ，５０ｃの機能のみを備えていても良い。また，双方の機能を備えていても良い。以後では，双方の機能を備えるコンテンツ再生装置として，コンテンツ再生装置５０について説明する。

【０１７１】

以上，コンテンツ提供システム５００の全体構成について説明した。次に，図１８に基づいて，本実施形態にかかるコンテンツ再生装置５０の機能構成について説明する。

【０１７２】

＜９．コンテンツ再生装置の機能構成＞

図１８に示すように，コンテンツ再生装置５０は，リンク情報取得部５０２と，コンテンツ情報取得部５０４と，コンテンツ情報記憶部５０６と，リンク情報記憶部５０８と，判断部５１０と，利用制御部５１２と，鍵処理部５１４と，コンテンツ鍵復号部５１６と，コンテンツ再生部５１８と，コンテンツ記憶部５２０と，コンテンツ取得部５２２と，リンク情報発行部５２４と，デバイス鍵暗号部５２６と，制限情報生成部５２８と，発行先情報取得部５３０と，発行要求受付部５３２などを含んで構成される。リンク情報取得

部５０２，コンテンツ情報取得部５０４，コンテンツ情報記憶部５０６，判断部５１０，鍵処理部５１４，コンテンツ鍵復号部５１６，コンテンツ再生部５１８，コンテンツ記憶部５２０，およびコンテンツ取得部５２２は，主にリンク情報を利用したコンテンツの再生に関連する機能をもつ。リンク情報発行部５２４，デバイス鍵暗号部５２６，制限情報生成部５２８，発行先情報取得部５３０，および発行要求受付部５３２は，主にリンク情報の発行に関連する機能をもつ。リンク情報記憶部５０８および利用制御部５１２は，コンテンツの再生とリンク情報の発行の双方に関連する機能をもつ。

【０１７３】

まず，コンテンツの再生に関連する機能について説明する。リンク情報取得部５０２は，リンク情報を取得する。著作権管理サーバからリンク情報を受信してもよいし，コンテンツ提供元装置，さらに，そのコンテンツ提供元装置からリンク情報の発行を受けた他のコンテンツ再生装置からリンク情報を受信してもよい。また，フレキシブルディスクやＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ）などの外部記録装置に記録されているリンク情報を読み取ることにより，取得してもよい。リンク情報は，上述の通りである。つまり，リンク情報には，一方がリンク元であり，他方がリンク先である一対の識別情報が含まれている。その識別情報は，著作権管理サーバにおいてユーザを一意に識別する識別情報（ユーザＩＤ）またはコンテンツ再生装置を一意に識別する識別情報（デバイスＩＤ）である。リンク情報にはまた，リンク先に設定されている識別情報によって特定されるユーザまたはコンテンツ再生装置に固有の鍵（ユーザ鍵またはデバイス鍵）を，リンク元に設定されている識別情報によって特定されるユーザまたはコンテンツ再生装置に固有の鍵で暗号化した情報が含まれている。また，リンク情報の利用制限情報も含まれる。

【０１７４】

リンク情報記憶部５０８は，リンク情報取得部５０２が取得したリンク情報を記憶する。リンク情報記憶部５０８は，リンク情報を記憶することにより，リンク情報記憶部５０８が所属しているコンテンツ再生装置５０６（以後，自装置と称する。）のデバイスＩＤと，コンテンツ提供元装置を使用するユーザのユーザＩＤとの関連付けを行っている。より具体的には，リンク情報記憶部５０８は，記憶しているリンク情報に従って，起点が自装置であり，到達点がコンテンツ提供元（具体的には，コンテンツ提供元装置を使用するユーザ）である経路が生成されることによって，自装置と，コンテンツ提供元との関連付けを実現している。この経路が生成されていれば，コンテンツ再生装置５０は，リンク情報を辿ることにより，自装置に固有のデバイス鍵を用いた，コンテンツ提供元装置と関連づけられているユーザのユーザ鍵の復号に成功する。なお，著作権管理サーバが，コンテンツ提供元装置にコンテンツ鍵を提供する際に，コンテンツ提供元装置を使用するユーザのユーザ鍵ではなくコンテンツ提供元装置のデバイス鍵で暗号化する場合もある。その場合には，コンテンツ再生装置５０のリンク情報記憶部５０８において自装置のデバイスＩＤと関連付けられているのはコンテンツ提供元装置のデバイスＩＤであり，リンク情報を辿った経路の到達点はコンテンツ提供元装置を使用するユーザではなく，コンテンツ提供元装置である。

【０１７５】

コンテンツ情報取得部５０４は，コンテンツ鍵取得部の一例であり，著作権管理サーバ，コンテンツ提供元装置または他のコンテンツ再生装置からコンテンツ情報を受信する。具体的には，コンテンツ情報取得部５０４は，コンテンツＩＤ，暗号化されたコンテンツ鍵，コンテンツ提供元装置を使用するユーザのユーザＩＤ，およびコンテンツに含まれる音楽の楽曲名等のコンテンツのメタ情報が含まれるコンテンツ情報を，通信網を介して受信する。また，フレキシブルディスクやＣＤなどの外部記録装置に記録されているコンテンツ情報を読み取ることにより，取得してもよい。コンテンツ情報取得部５０４は，取得したコンテンツ情報を，コンテンツ情報記憶部５０６に格納する。

【０１７６】

コンテンツ情報記憶部５０６は，コンテンツ情報を記憶している。コンテンツ情報記憶部５０６は，ＲＡＭやＨＤＤにより構成される。

【０１７７】
コンテンツ選択部５０９は，コンテンツ情報記憶部５０６に記憶されているコンテンツ情報を選択する。具体的には，コンテンツ選択部５０９は，コンテンツ情報記憶部５０６に記憶されているコンテンツ情報に含まれるコンテンツのメタ情報を表示するディスプレイ等の表示手段と，ユーザにより所望のメタ情報を選択されるマウスやキーボード等の入力手段を含む。コンテンツ選択部５０９は，ユーザにより選択されたメタ情報と関連付けられているコンテンツのコンテンツＩＤを判断部５１０に提供する。
【０１７８】
判断部５１０は，コンテンツ情報に含まれるユーザＩＤと，リンク情報記憶部５０８において自装置と関連付けられているコンテンツ提供元装置を使用するユーザのユーザＩＤとに基づいて，コンテンツ鍵復号部にコンテンツ鍵の復号を許可するか否かを判断する。具体的には，判断部５１０は，コンテンツ選択部５０９から取得したコンテンツＩＤが含まれるコンテンツ情報を，コンテンツ情報記憶部５０６から取得する。そして，判断部５１０は，取得したコンテンツ情報に含まれるユーザＩＤと，リンク情報記憶部５０８に記憶されているユーザＩＤとを比較し，２つのユーザＩＤが対応する場合には，コンテンツ鍵復号部５１６によるコンテンツ鍵の復号処理を許可する。復号処理を許可する場合には，判断部５１０は，利用制御部５１２に処理を開始させることにより，コンテンツ再生装置５０の後続の処理を続行させる。一方，２つのユーザＩＤが対応しない場合には「このコンテンツを再生する権利がありません。」等のエラー表示を行い，コンテンツ鍵復号部５１６によるコンテンツ鍵の復号処理を不許可とし，以後の処理には進まない。２つのユーザＩＤが対応するとは，一方のユーザＩＤから，所定の法則によって他方のユーザＩＤを導き出せることであり，２つのユーザＩＤが一致する場合を含む。
【０１７９】
判断部５１０が行う処理の具体例を，図２０を参照して説明する。まず，判断部５１０は，取得したコンテンツ情報に含まれるユーザＩＤが，リンク情報記憶部５０８に記憶されているかを調べる。記憶されている場合には，判断部５１０は，リンク情報記憶部５０８において，自装置を起点とし，そのユーザＩＤを到達点とする経路が生成されているかを，リンク情報に基づいて調べる。つまり，まず，判断部５１０は，コンテンツ情報に含まれるユーザＩＤがリンク先に設定されているリンク情報（例えば，リンクＡ）を，リンク情報記憶部５０８から検索する（Ｓ２００）。
【０１８０】
該当リンク情報がある場合には（Ｓ２０２），リンクＡのリンク元に設定されている識別情報が，自装置のデバイスＩＤであるかを判断する（Ｓ２０４）。リンクＡのリンク元が，自装置のデバイスＩＤである場合には，自装置を起点とし，ユーザＩＤを到達点とする経路が生成されていると判断し，コンテンツ鍵復号部５１６によるコンテンツ鍵の復号処理を許可する（Ｓ２０８）。
【０１８１】
ステップＳ２０４で，リンクＡのリンク元が，自装置のデバイスＩＤでない場合には，判断部５１０は，リンクＡのリンク元の識別情報がリンク先として設定されている他のリンク情報（例えば，リンクＢ）を検索する（Ｓ２０６）。該当するリンク情報が無い場合には，判断部５１０は，自装置を起点とし，ユーザＩＤを到達点とする経路が生成されていないと判断し，コンテンツ鍵復号部５１６によるコンテンツ鍵の復号処理を許可しない（Ｓ２１０）。一方，ステップＳ２０６で，該当するリンク情報が有る場合には，リンクＢのリンク元に設定されている識別情報が自装置のデバイスＩＤであるかを判断する（Ｓ２０４）。
【０１８２】
上記処理を繰り返してリンク情報を辿り，リンク元に自装置のデバイスＩＤが設定されているリンク情報がリンク情報記憶部５０８に記憶されていれば，判断部５１０は，コンテンツ鍵復号部５１６によるコンテンツ鍵の復号処理を許可する。
【０１８３】

判断部５１０は，コンテンツ鍵の復号処理を許可する場合には，上記処理において特定された，自装置からユーザＩＤへの経路を生成するリンク情報（例えば，リンクＡ，リンクＢおよびリンクＣ）と，コンテンツ情報記憶部５０６から取得したコンテンツ情報を利用制御部５１２に提供する。

【０１８４】

利用制御部５１２は，リンク情報記憶部５０８に記憶されている利用制限情報に基づいて，リンク情報の利用を制限する。具体的には，利用制部５１２は，自装置からコンテンツ提供元装置を使用するユーザのユーザＩＤへの経路を生成するリンク情報（例えば，リンクＡ，リンクＢおよびリンクＣ）と，コンテンツ情報を判断部５１０から取得する。そして，リンク元に自装置のデバイスＩＤが設定されているリンク情報（リンクＣ）に含まれる利用制限情報を参照し，そのリンク情報の利用が可能であるか否かを判断する。より詳細には，利用制限情報に含まれる有効期間情報を参照し，現在の日時と有効期間に設定されている日時とを比較して有効期間内であるか否かを判断する。有効期間内であれば，利用制御部５１２は，判断部５１０から取得したリンク情報（リンクＡ，リンクＢおよりリンクＣ）とコンテンツ情報を鍵処理部５１４に提供し，コンテンツ再生装置５０に後続の処理を続行させる。一方，有効期間外である場合には，利用制御部５１２は，「有効期間を過ぎています。このコンテンツを再生できません。」等のエラー表示を行い，以後の処理には進まない。

【０１８５】

鍵処理部５１４は，リンク情報記憶部５０８に記憶されているリンク情報に基づいて，コンテンツ提供元装置を使用するユーザのユーザ鍵を復号する。具体的には，鍵処理部５１４は，利用制御部５１２からリンク情報を取得し，まず，リンク元が自装置であるリンク情報（例えば，リンクＣ）に含まれている暗号化された情報（鍵）を，自装置に固有のデバイス鍵により復号する。次に，鍵処理部５１４は，リンクＣにおいてリンク先に設定されている識別情報がリンク元に設定されているリンク情報（例えば，リンクＢ）に含まれている暗号化された情報（鍵）を，直前に復号した鍵によって復号する。鍵処理部５１４は，この処理を繰り返して，リンク先にユーザＩＤが設定されているリンク情報（例えば，リンクＡ）に含まれている暗号化された情報（すなわち，リンクＡのリンク元の鍵で暗号化されたユーザ鍵）を復号する。その後，鍵処理部５１４は，復号したユーザ鍵と，利用制御部５１２から取得したコンテンツ情報をコンテンツ鍵復号部５１６に提供する。

【０１８６】

コンテンツ鍵復号部５１６は，鍵処理部５１４からコンテンツ情報とユーザ鍵を取得し，取得したコンテンツ情報に含まれるコンテンツ鍵を，取得したユーザ鍵で復号する。コンテンツ鍵復号部５１６は，コンテンツ情報に含まれるコンテンツＩＤと，復号したコンテンツ鍵をコンテンツ再生部５１８に提供する。

【０１８７】

コンテンツ再生部５１８は，コンテンツ鍵復号部５１６から，コンテンツＩＤとコンテンツ鍵を取得し，取得したコンテンツＩＤによって特定されるコンテンツをコンテンツ記憶部５２０から取得し，そのコンテンツをコンテンツ鍵により復号して再生する。

【０１８８】

コンテンツ取得部５２２は，コンテンツ提供サーバや，コンテンツ提供元装置，他のコンテンツ再生装置などからコンテンツを取得し，コンテンツ記憶部５２０に格納する。また，フレキシブルディスクやＣＤなどの外部記録装置に記録されているコンテンツを読み取ることにより，取得してもよい。

【０１８９】

次いで，図１９に基づいて，コンテンツの再生に関わる各処理部が，どの情報を使用して各処理を行うかを簡潔に説明する。

【０１９０】

コンテンツ再生装置５０において，コンテンツの再生に関わる情報は，コンテンツ情報記憶部５０６とリンク情報記憶部５０８に記憶されている。コンテンツ情報記憶部５０６

には，少なくとも，ユーザＩＤ５０６０，コンテンツ鍵５０６２，およびコンテンツＩＤ（図示なし）を１セットとするコンテンツ情報が，１つまたは複数記憶されている。

【０１９１】

リンク情報記憶部５０８には上述の通りリンク情報が記憶されているが，具体的には，少なくとも１つのデバイスＩＤ５０６４，ユーザＩＤ５０６６，関連付けの方向５０６８，ユーザ鍵５０７０，および少なくとも１つのデバイス鍵５０７２が，各々リンク情報として関連付けられて記憶されている。なお，関連付けの方向５０６８は，各リンク情報に含まれるリンク元，リンク先を示す。また，リンク情報記憶部５０８には，利用制限情報５０７４も記憶されている。各リンク情報に利用制限情報が含まれるため，リンク情報が複数記憶されている場合には，リンク情報記憶部５０８には複数の利用制限情報が記憶されている。利用制御部５１２がリンク情報の利用制御のために参照する利用制限情報は，自装置のデバイスＩＤがリンク元として設定されているリンク情報に含まれている利用制限情報である。

【０１９２】

判断部５１０は，コンテンツ情報記憶部５０６に記憶されているユーザＩＤ５０６０と，リンク情報記憶部５０８に記憶されているデバイスＩＤ５０６４，ユーザＩＤ５０６６，関連付けの方向５０６８とを使用して，上述の判断処理を行う。

【０１９３】

鍵処理部５１４は，リンク情報記憶部５０８に記憶されているユーザ鍵５０７０と，デバイス鍵５０７２とを使用して上述のユーザ鍵の復号処理を行う。

【０１９４】

コンテンツ鍵復号部５１６は，コンテンツ情報記憶部５０６に記憶されているコンテンツ鍵５０６２と，リンク情報記憶部５０８に記憶されているユーザ鍵５０７０とを使用して，上述の，コンテンツ鍵の復号処理を行う。

【０１９５】

利用制御部５１２は，リンク情報記憶部５０８に含まれるデバイスＩＤ５０６４と，利用制限情報５０７４とを使用して，上述の利用制御処理を行う。

【０１９６】

以上，コンテンツの再生に関連する機能について説明した。次に，リンク情報の発行に関連する機能について説明する。発行要求受付部５３２は，他のコンテンツ再生装置からリンク情報の発行の要求を受けて，リンク情報の発行の可否を利用制御部５１２に問い合わせる。利用制御部５１２に問い合わせた結果，リンク情報の発行が可能であれば，発行先情報取得部５３０に通知する。一方，リンク情報の発行が不可能であれば，その旨を要求元である他のコンテンツ再生装置に通知し，処理を終了する。

【０１９７】

発行先情報取得部５３０は，リンク情報の発行の要求元である他のコンテンツ再生装置からそのコンテンツ再生装置に固有のデバイス鍵と，デバイスＩＤを取得する。なお，他のコンテンツ再生装置からリンク情報の発行要求を受けるのではなく，コンテンツ再生装置５０が主体となり他のコンテンツ再生装置にリンク情報を発行する場合には，リンク情報の発行先であるコンテンツ再生装置からデバイス鍵とデバイスＩＤの提供を受ける。発行先情報取得部５３０は，デバイス鍵を取得すると，制限情報生成部５２８に通知し，デバイス鍵暗号部５３０に取得したデバイス鍵とデバイスＩＤを提供する。

【０１９８】

制限情報生成部５２８は，リンク情報記憶部５０８に記憶されている利用制限情報に基づいて第２の利用制限情報を生成する。具体的には，制限情報生成部５２８は，利用制御部５１２から，自装置がリンク元に設定されているリンク情報に含まれる利用制限情報を取得し，その利用制限情報に基づいて，新たに利用制限情報を生成する。例えば，制限情報生成部５２８は，利用制限情報に含まれる有効期間情報，ホップカウント情報，リンク発行可能回数をリンク情報に含まれる規則に基づいて設定する。制限情報生成部５２８は，生成した利用制限情報をデバイス鍵暗号部５２６に提供する。

【０１９９】
デバイス鍵暗号部５２６は，発行先情報取得部５３０から取得した，リンク情報発行先のコンテンツ再生装置のデバイス鍵で，自装置のデバイス鍵を暗号化する。そして，暗号化した自装置のデバイス鍵と，発行先情報取得部５３０から取得したデバイスＩＤ，制限情報生成部５２８から取得した利用制限情報をリンク情報発行部５２４に提供する。
【０２００】
リンク情報発行部５２４は，デバイス鍵暗号部５２６から取得したデバイスＩＤ，自装置のデバイス鍵および利用制限情報に基づいて，リンク元がリンク情報発行先のコンテンツ再生装置であり，リンク先が自装置となる，利用制限情報および自装置のデバイス鍵を含むリンク情報を生成する。そして，自装置からコンテンツ提供元装置を使用するユーザのユーザＩＤまでの経路を生成するリンク情報をリンク情報記憶部５０８から取得し，新たに生成したリンク情報とともに，リンク情報発行先のコンテンツ再生装置に提供する。
【０２０１】
利用制御部５１２は，発行要求受付部５３２からリンク情報の発行可否の問い合わせを受けると，自装置がリンク元に設定されているリンク情報をリンク情報記憶部５０８から取得し，そのリンク情報に含まれる利用制限情報に基づいて，リンク情報の発行が可能か否かを判断する。具体的には，そのリンク情報に含まれる有効期間情報の設定値を参照して，有効期間内であるか否かを判断する。また，ホップカウント情報やリンク発行可能回数を参照して，リンク情報の発行が可能である（設定値が０以外である）か否かを判断する。また，制限情報生成部５２８からの要求を受けて，自装置がリンク元に設定されているリンク情報に含まれる利用制限情報をリンク情報記憶部５０８から取得して制限情報生成部５２８に提供する。以上，リンク情報の発行に関連する機能について説明した。
【０２０２】
以上，コンテンツ再生装置５０の機能構成について説明した。なお，上述の全ての機能がひとつのコンピュータに備えられてコンテンツ再生装置５０が構成されていてもよいが，各機能が複数のコンピュータに分散されており，全体としてひとつのコンテンツ再生装置５０として機能するように構成されていても構わない。次に，図２１に基づいて，コンテンツ再生装置５０が行うコンテンツ再生処理の流れについて説明する。
【０２０３】
＜１０．コンテンツ再生処理の流れ＞
まず，コンテンツ再生装置５０は，再生するコンテンツを選択する（Ｓ３００）。より詳細には，ユーザによる入力処理を受けて，コンテンツ選択部５０９が，再生するコンテンツのコンテンツＩＤを指定する。
【０２０４】
次に，コンテンツ再生装置５０は，コンテンツ情報に含まれるユーザＩＤと経路の到達点を比較する（Ｓ３０２）。より詳細には，判断部５１０が，Ｓ３０２で特定されたコンテンツ情報に含まれるユーザＩＤと，リンク情報記憶部５０８において自装置と関連付けられているユーザＩＤとを比較する。
【０２０５】
次に，コンテンツ再生装置５０は，コンテンツ鍵の復号を許可するか否かを判断する（Ｓ３０４）。より詳細には，判断部５１０が，Ｓ３０２において比較した２つのユーザＩＤが対応する場合には，コンテンツ鍵の復号を許可し，Ｓ３０６に進む。一方，２つのユーザＩＤが対応しない場合には，コンテンツ鍵の復号を許可せず，コンテンツ再生装置５０は，コンテンツの再生は行わずに処理を終了する。
【０２０６】
次に，コンテンツ再生装置５０は，リンク情報に含まれる利用制限情報を取得する（Ｓ３０６）。より詳細には，利用制御部５１２が，自装置がリンク元に設定されているリンク情報に含まれる利用制限情報を取得する。
【０２０７】
次に，コンテンツ再生装置５０は，リンク情報が有効期間内であるかを判断する（Ｓ３

０８）。より詳細には，利用制御部５１２が，Ｓ３０６で取得した利用制限情報に含まれる有効期間情報に基づいて，有効期間内かを判断し（Ｓ３０８），有効期間内である場合には，Ｓ３１０に進む。一方，有効期間外である場合には，コンテンツ再生装置５０は，コンテンツの再生を行わずに処理を終了する。

【０２０８】

次に，コンテンツ再生装置５０は，ユーザ鍵を復号する（Ｓ３１０）。より詳細には，鍵処理部５１４が，リンク情報記憶部５０８に記憶されている，暗号化されたユーザ鍵を，自装置のデバイス鍵を用いて復号する。なお，鍵処理部５１４は，ユーザ鍵の復号に，リンク情報記憶部５０８に記憶されている自装置以外のコンテンツ再生装置５０６（コンテンツ提供元装置を含む）のデバイス鍵を，必要に応じて使用する。

【０２０９】

次に，コンテンツ再生装置５０は，コンテンツ鍵を復号する（Ｓ３１２）。より詳細には，コンテンツ鍵復号部５１６が，コンテンツ情報に含まれている暗号化されたコンテンツ鍵を，Ｓ３１０で復号されたユーザ鍵を用いて，復号する。

【０２１０】

次に，コンテンツ再生装置５０は，再生するコンテンツを復号する（Ｓ３１４）。より詳細には，コンテンツ再生部５１８が，暗号化されているコンテンツを，Ｓ３１２で復号されたコンテンツ鍵を用いて，復号する。

【０２１１】

次に，コンテンツ再生装置５０は，コンテンツを再生する（Ｓ３１６）。より詳細には，コンテンツ再生部５１８が，Ｓ３１４で復号されたコンテンツを再生する。

【０２１２】

以上，コンテンツ再生装置５０が行うコンテンツ再生処理の流れについて説明した。次に，図２２に基づいて，コンテンツ再生装置５０が行うリンク情報発行処理の流れについて説明する。

【０２１３】

＜１１．リンク情報発行処理の流れ＞

まず，コンテンツ再生装置５０は，他のコンテンツ再生装置からリンク情報の発行要求を受け付ける（Ｓ４００）。より詳細には，発行要求受付部５３２が，他のコンテンツ再生装置からリンク情報の発行を要求するメッセージを通信網を介す等して受け付ける。

【０２１４】

次に，コンテンツ再生装置５０は，リンク情報に含まれる利用制限情報を取得する（Ｓ４０２）。より詳細には，利用制御部５１２が，自装置のデバイスＩＤがリンク元に設定されているリンク情報をリンク情報記憶部５０８から検索し，そのリンク情報に含まれる利用制限情報を取得する。

【０２１５】

次に，コンテンツ再生装置５０は，リンク情報を発行できるかを判断する（Ｓ４０４）。より詳細には，利用制御部５１２が，Ｓ４０２で取得した利用制限情報に基づいて，リンク情報の発行が可能かを判断する。Ｓ４０４において利用制御部５１２が行う処理の詳細な流れを図２３に示した。図２３に示すように，利用制御部５１２は，まず，利用制限情報に含まれる有効期間情報を参照する（Ｓ５００）。そして，現在日時と有効期間とを比較して，有効期間内であるかを判断する（Ｓ５０２）。有効期間内であれば，利用制御部５１２は次にホップカウント情報を参照する（Ｓ５０４）。そして，ホップカウント情報に設定されている値が１以上であるかを判断する（Ｓ５０６）。ホップカウント情報の設定値が１以上であれば，利用制御部５１２は次にリンク発行可能回数を参照する（Ｓ５０８）。そして，リンク発行可能回数が１以上であるかを判断する（Ｓ５１０）。１以上であれば，利用制御部５１２は，リンク情報の発行が許可されており，リンク情報の発行が可能であると判断する。それ以外の場合には，リンク情報の発行が許可されておらず，リンク情報の発行が不可能であると判断する。図２２に戻る。

【０２１６】

次に，コンテンツ再生装置５０は，リンク情報の発行先であるコンテンツ再生装置のデバイスＩＤとデバイス鍵を取得する（Ｓ４０６）。より詳細には発行先情報取得部５３０が，リンク情報の発行要求元であるコンテンツ再生装置から，そのコンテンツ再生装置に固有のデバイスＩＤとデバイス鍵（公開鍵）を取得する。

【０２１７】

次に，コンテンツ再生装置５０は，発行するリンク情報に含ませる利用制限情報を生成する（Ｓ４０８）。より詳細には，制限情報生成部５２８が，利用制御部５１２を介してリンク情報記憶部５０８から，自装置のデバイスＩＤがリンク元に設定されているリンク情報に含まれる利用制限情報を取得し，その利用制限情報に基づいて新たに利用制限情報を生成する。

【０２１８】

次に，コンテンツ再生装置５０は，リンク情報の発行先のコンテンツ再生装置のデバイス鍵で，自装置のデバイス鍵を暗号化する（Ｓ４１０）。より詳細には，デバイス鍵暗号部５２６が，Ｓ４０６で発行先情報取得部５３０により取得されたリンク情報の発行要求元のコンテンツ再生装置のデバイス鍵（公開鍵）によって自装置のデバイス鍵（秘密鍵）を暗号化する。

【０２１９】

次に，コンテンツ再生装置５０は，自装置のデバイスＩＤから，コンテンツ提供元装置のユーザのユーザＩＤまでの経路を生成するリンク情報を取得する（Ｓ４１２）。より詳細には，リンク情報発行部５２４が，リンク元が自装置のデバイスＩＤであるリンク情報と，リンク先がコンテンツ提供元装置のユーザのユーザＩＤであるリンク情報と，その間に介在している１または複数のリンク情報をリンク情報記憶部５０８から取得する。

【０２２０】

最後に，コンテンツ再生装置５０は，リンク情報を発行する（Ｓ４１４）。より詳細には，リンク情報発行部５２４が，Ｓ４０８で生成された利用制限情報とＳ４１０で暗号化された自装置のデバイス鍵とを含む，リンク情報発行先のコンテンツ再生装置から自装置への経路を生成するリンク情報を新たに生成し，生成したリンク情報と，Ｓ４１２で取得したリンク情報とを，リンク情報発行先のコンテンツ再生装置に提供する。以上，コンテンツ再生装置が行うリンク情報発行処理の流れについて説明した。

【０２２１】

本実施形態にかかるコンテンツ提供システム５００によれば，コンテンツを正当に取得した取得者に，そのコンテンツを他の利用者と共有することを認めながら，リンク情報により共有できる利用者の数や範囲，利用できる期間を定めることにより，そのコンテンツの新たな販売の機会をサービス事業者から奪うことを防止できる。また，コンテンツごとに利用制限を設定するのではなく，リンク情報に利用制限を設定することにより，複数のコンテンツ（例えば，一人の取得者が保有するコンテンツ）に対して一括して利用制限をかけることができる。また，リンク情報の発行の際に利用制限情報が新たに生成されることにより，コンテンツ再生装置ごとに異なる利用制限をかけることができる。

【０２２２】

なお，著作権や販売機会をより効果的に保護するために，コンテンツ再生装置は，著作権管理サーバ以外からのリンク情報の発行を受ける回数を制限されてもよい。その場合，コンテンツ再生装置は，どのコンテンツ再生装置からリンク情報の発行を受けるかを選択できてもよい。

【０２２３】

以上，添付図面を参照しながら本発明の好適な実施形態について説明したが，本発明は係る例に限定されないことは言うまでもない。当業者であれば，特許請求の範囲に記載された範疇内において，各種の変更例または修正例に想到し得ることは明らかであり，それらについても当然に本発明の技術的範囲に属するものと了解される。

【産業上の利用可能性】

【０２２４】

本発明は，コンテンツ提供システムに適用可能であり，特に，コンテンツ鍵により暗号化されたコンテンツを復号して再生するコンテンツ再生装置に，コンテンツ鍵を提供するシステムに適用可能である。

【図面の簡単な説明】

【０２２５】

【図１】本実施形態において採用されるリンク方式の著作権管理を説明するための，コンテンツ提供システムのリンク方式の概要を示す説明図である。

【図２】同実施の形態におけるコンテンツ提供システムの全体構成図である。

【図３】同実施の形態におけるＰＣのハードウェア構成例を概略的に示すブロック図である。

【図４】同実施の形態におけるＰＤのハードウェア構成例を概略的に示すブロック図である。

【図５】同実施の形態における著作権管理サーバの機能構成図である。

【図６】同実施の形態におけるユーザ情報記憶部の記憶内容を示す説明図である。

【図７】同実施の形態におけるＰＣの登録処理を示すタイミングチャートである。

【図８】同実施の形態におけるＰＤの登録処理を示すタイミングチャートである。

【図９】同実施の形態におけるユーザの登録処理を示すタイミングチャートである。

【図１０】同実施の形態におけるリンク処理を示すタイミングチャートである。

【図１１】同実施の形態におけるリンク情報の内容を示す説明図である。

【図１２】同実施の形態におけるリンク処理を示すタイミングチャートである。

【図１３】同実施の形態におけるリンクに含まれる鍵情報を示す説明図である。

【図１４】同実施の形態におけるライセンス発行処理を示すタイミングチャートである。

【図１５】同実施の形態におけるライセンス情報の内容を示す説明図である。

【図１６】同実施の形態における鍵情報の概念図を示す説明図である。

【図１７】本発明の実施形態にかかるコンテンツ提供システムの全体構成を示すブロック図である。

【図１８】同実施の形態におけるコンテンツ再生装置の機能構成を示すブロック図である。

【図１９】同実施の形態におけるコンテンツ再生装置の詳細な機能構成を示すブロック図である。

【図２０】同実施の形態におけるコンテンツ再生装置によるコンテンツ鍵復号可否判断処理を示すフローチャートである。

【図２１】同実施の形態におけるコンテンツ再生装置によるコンテンツ再生処理を示すフローチャートである。

【図２２】同実施の形態におけるコンテンツ再生装置のリンク情報発行処理を示すフローチャートである。

【図２３】同実施の形態におけるコンテンツ再生装置によるリンク情報発行可否判断処理を示すフローチャートである。

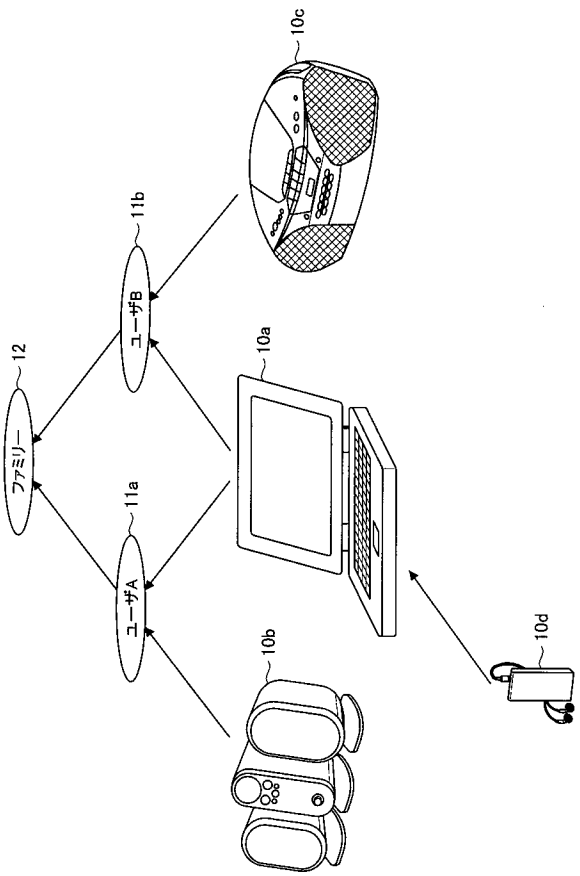
【符号の説明】

【０２２６】

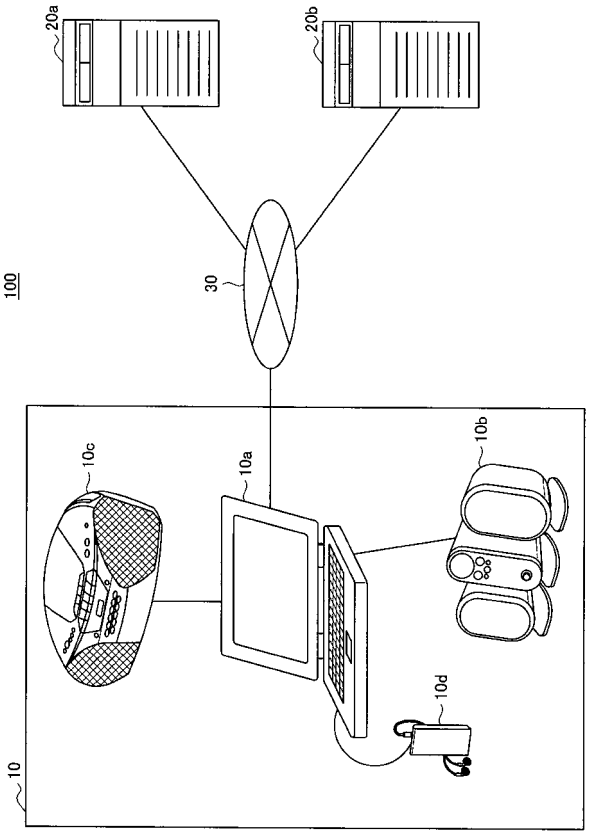
５００　　コンテンツ情報提供システム
５０ａ，５０ｂ，５０ｃ　　コンテンツ再生装置
５０２　　リンク情報取得部
５０４　　コンテンツ情報取得部
５０６　　コンテンツ情報記憶部
５０８　　リンク情報記憶部
５０９　　コンテンツ選択部
５１０　　判断部
５１２　　利用制御部
５１４　　鍵処理部

５１６　　コンテンツ鍵復号部
５１８　　コンテンツ再生部
５２０　　コンテンツ記憶部
５２２　　コンテンツ取得部
５２４　　リンク情報発行部
５２６　　デバイス鍵暗号部
５２８　　制限情報生成取得部
５３０　　発行先情報取得部
５３２　　発行要求受付部

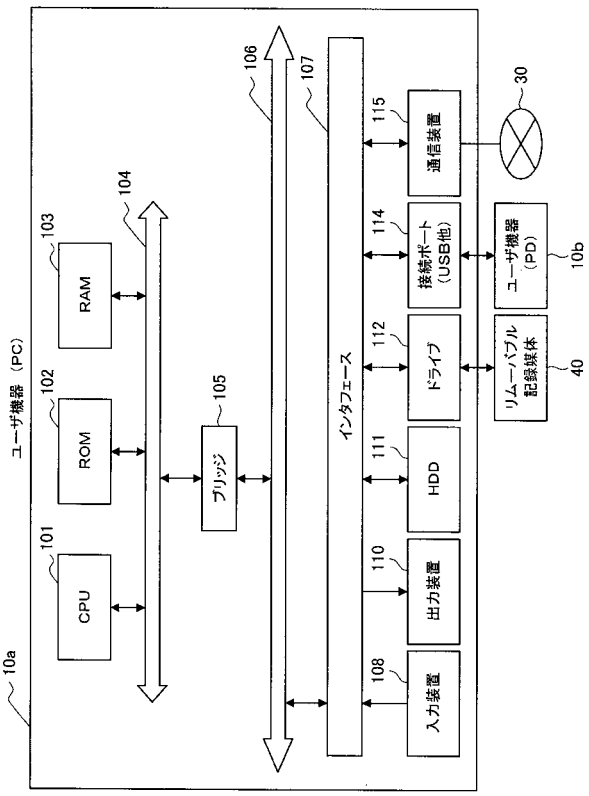
【図１】



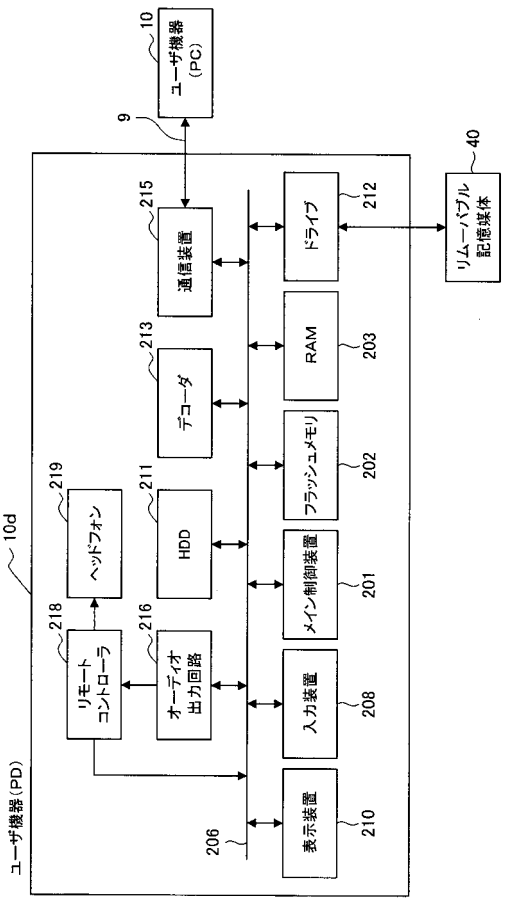
【図２】



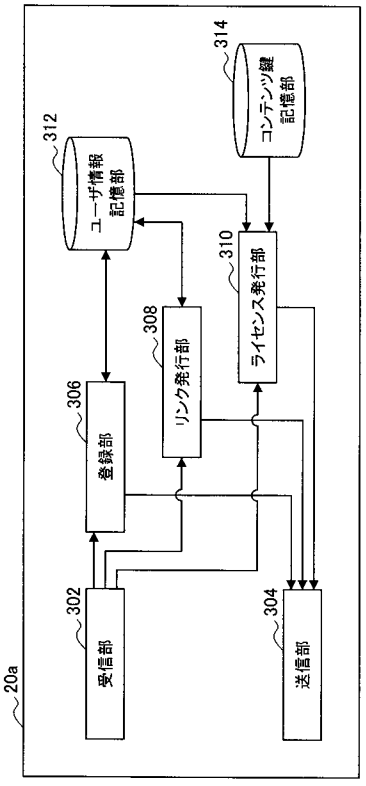
【図３】



【図４】



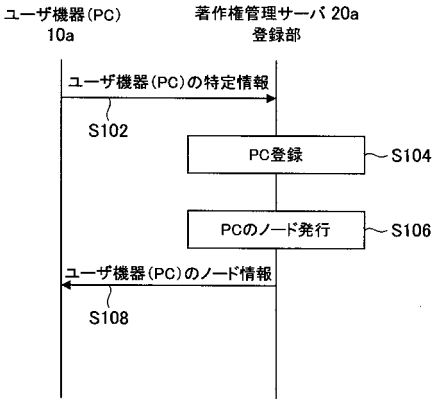
【図５】



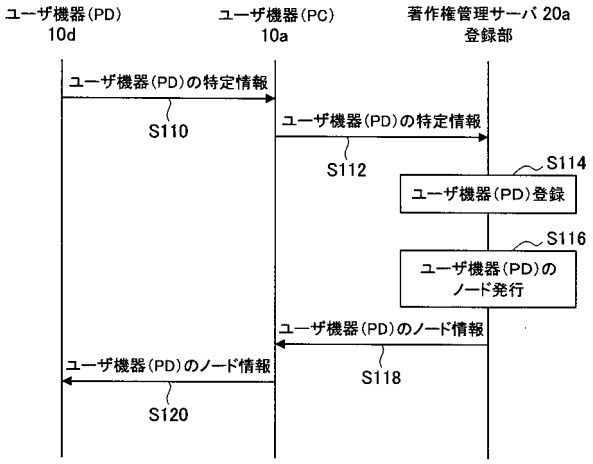
【図６】

3121 ユーザID	3122 クレジットカード番号	3123 ユーザ鍵	3124 デバイスID	3125 デバイス鍵	3126 リンク
Yamada Taro	×××-×××××	ユーザ鍵A	デバイスID 1	デバイス鍵 1	リンク A
			デバイスID 2	デバイス鍵 2	リンク B, リンク C
			デバイスID 3	デバイス鍵 3	リンク D
			デバイスID 4	デバイス鍵 4	リンク E
Suzuki Jiro	×××-×××××	ユーザ鍵B	デバイスID 5	デバイス鍵 5	リンク F
			デバイスID 6	デバイス鍵 6	リンク G
			デバイスID 7	デバイス鍵 7	リンク H
・・・	・・・	・・・	・・・	・・・	・・・

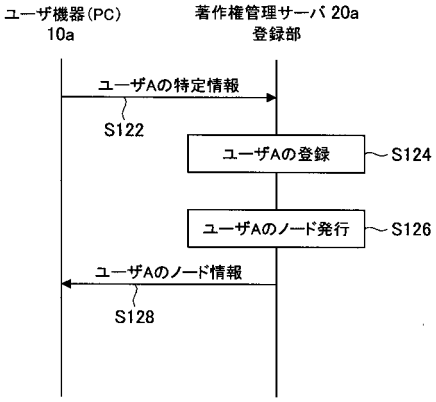
【図７】


ユーザ機器(PC)
10a
著作権管理サーバ 20a
登録部
ユーザ機器(PC)の特定情報
S102
PC登録
S104
PCのノード発行
S106
ユーザ機器(PC)のノード情報
S108

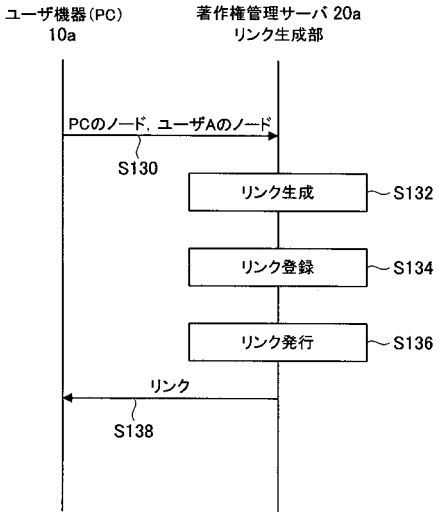
【図８】


ユーザ機器(PD)
10d
ユーザ機器(PC)
10a
著作権管理サーバ 20a
登録部
ユーザ機器(PD)の特定情報
S110
ユーザ機器(PD)の特定情報
S112
S114
ユーザ機器(PD)登録
S116
ユーザ機器(PD)の
ノード発行
ユーザ機器(PD)のノード情報
S118
ユーザ機器(PD)のノード情報
S120

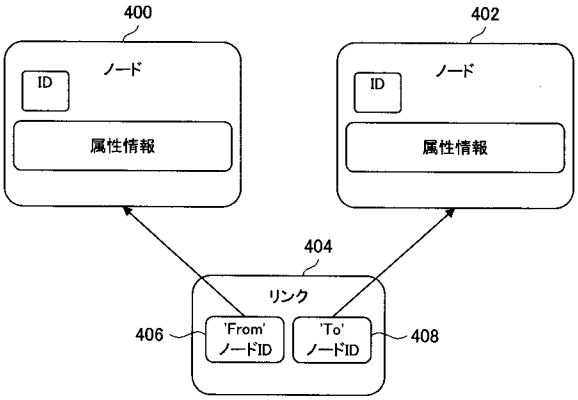
【図９】


ユーザ機器(PC)
10a
著作権管理サーバ 20a
登録部
ユーザAの特定情報
S122
ユーザAの登録
S124
ユーザAのノード発行
S126
ユーザAのノード情報
S128

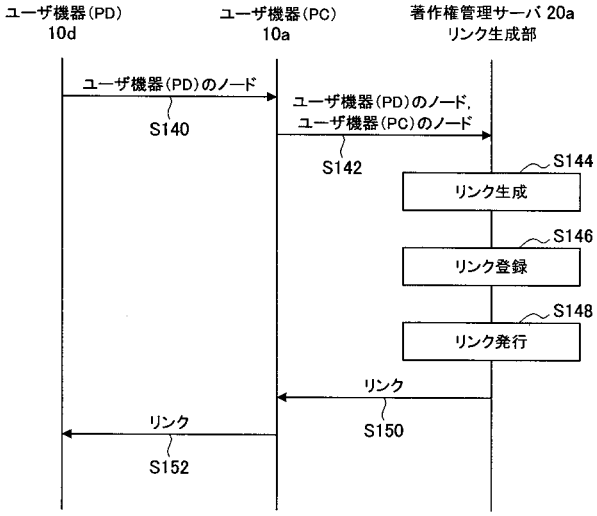
【図１０】


ユーザ機器(PC)
10a
著作権管理サーバ 20a
リンク生成部
PCのノード, ユーザAのノード
S130
リンク生成
S132
リンク登録
S134
リンク発行
S136
リンク
S138

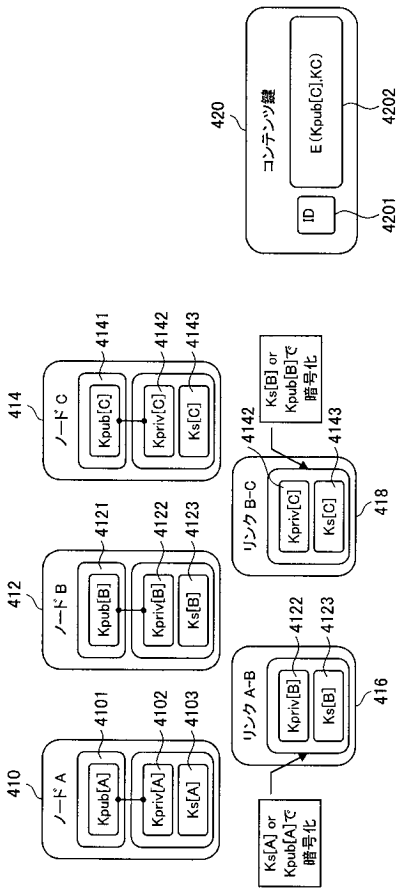
【図１１】



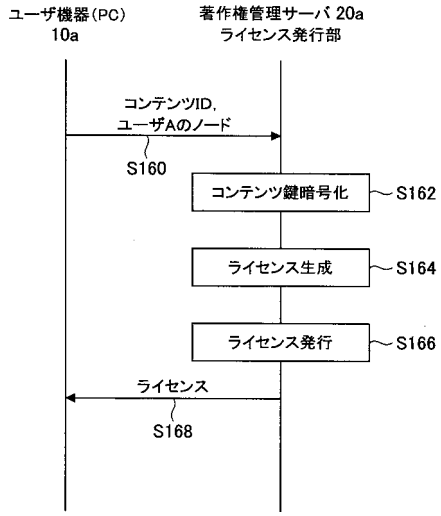
【図１２】



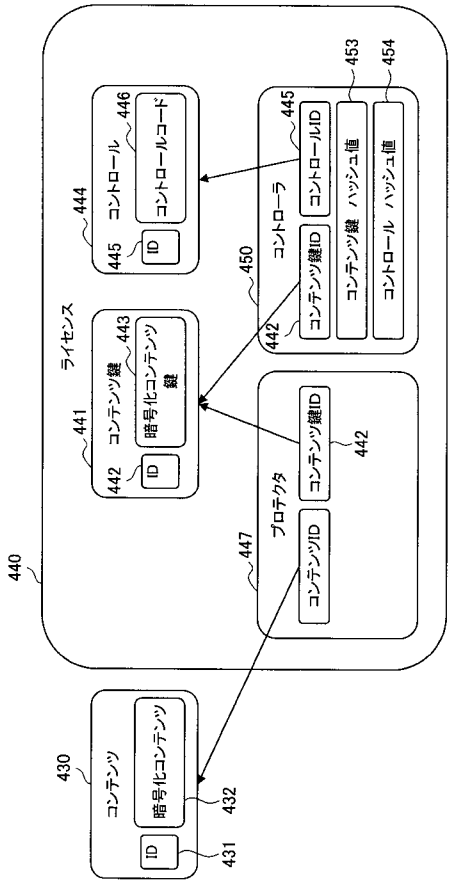
【図１３】



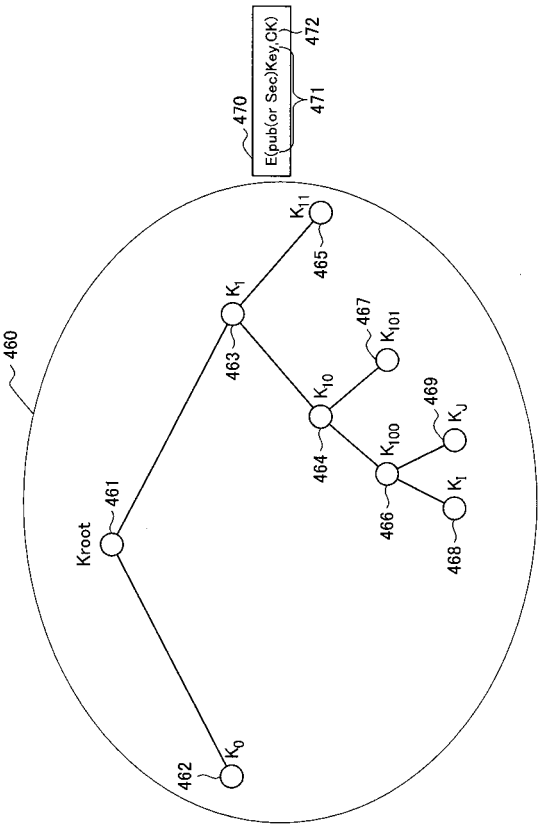
【図１４】



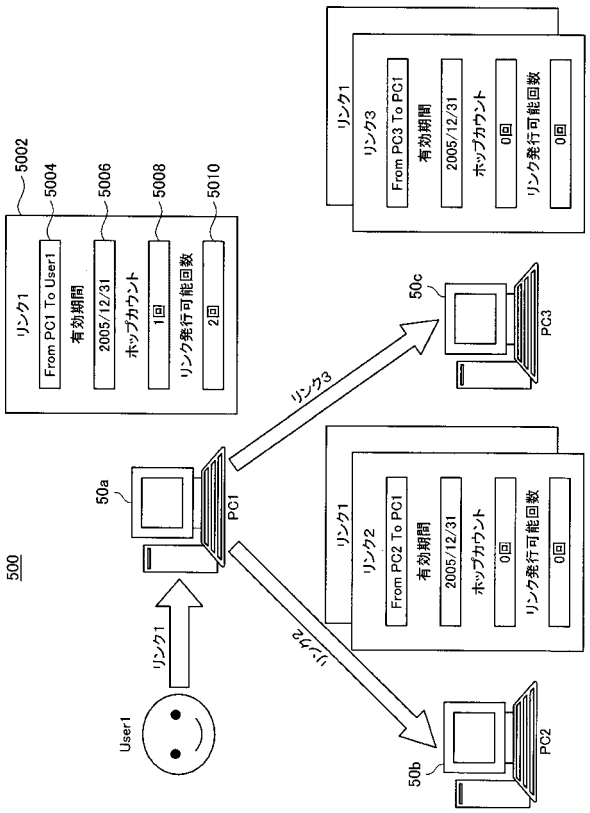
【図１５】



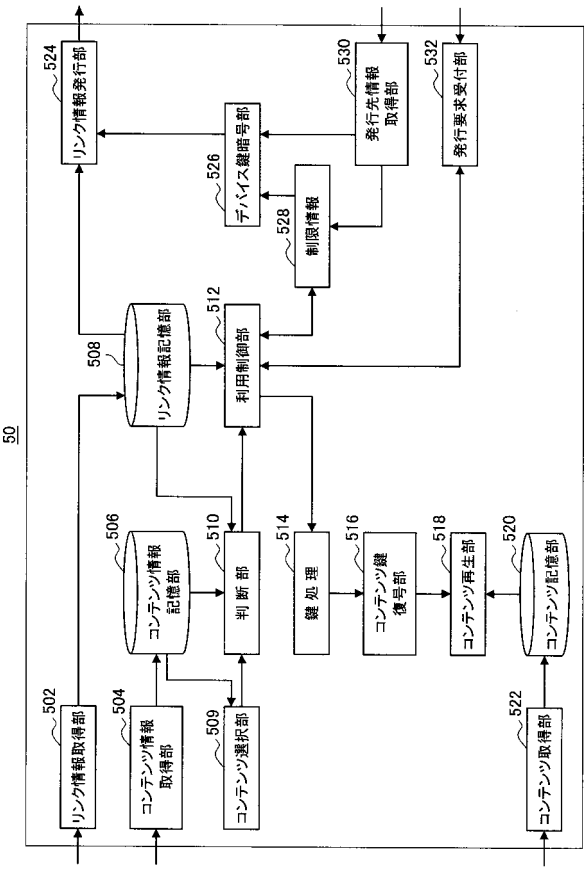
【図１６】



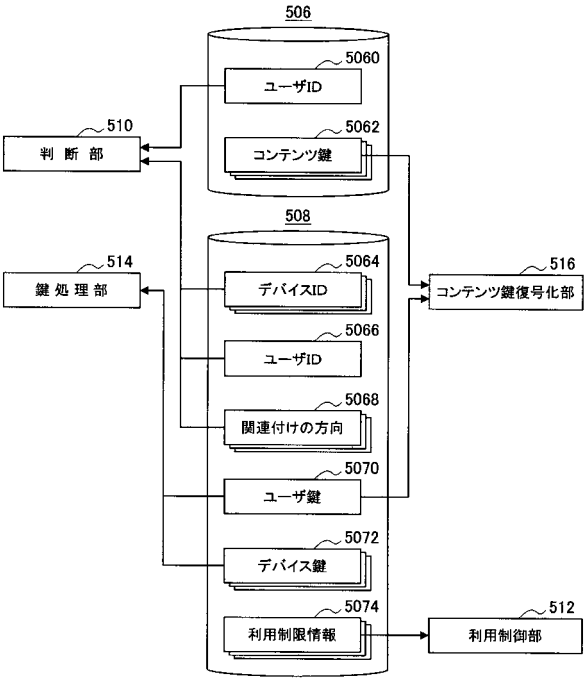
【図１７】



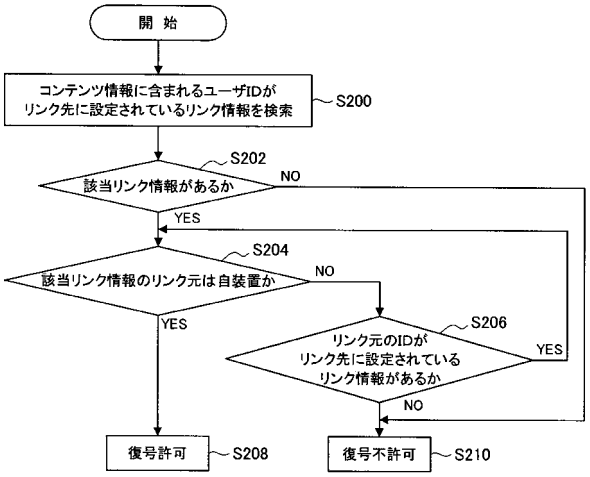
【図１８】



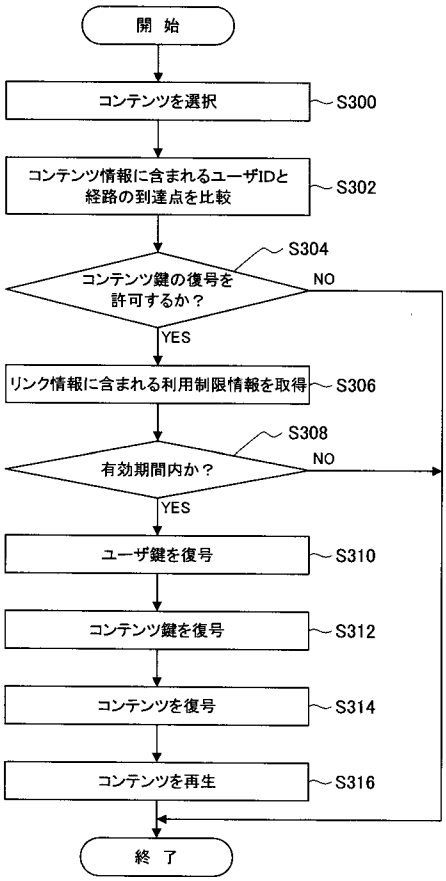
【図１９】



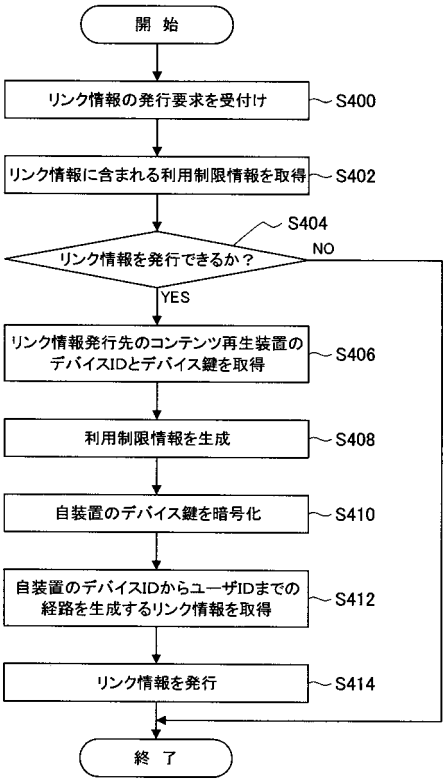
【図２０】



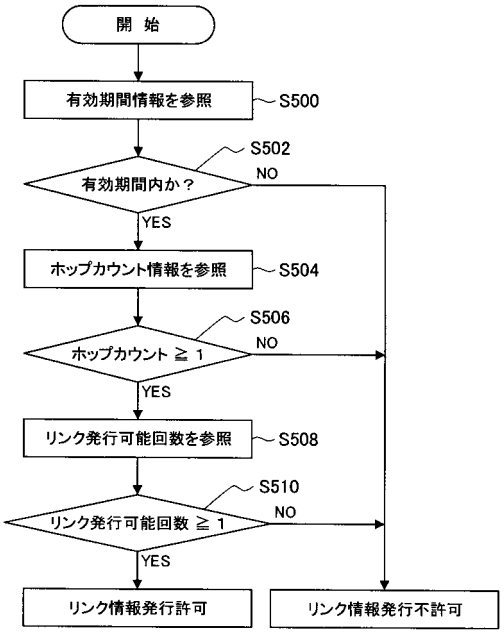
【図２１】



【図２２】



【図２３】


開 始
有効期間情報を参照
S500
S502
有効期間内か？
NO
YES
ホップカウント情報を参照
S504
S506
ホップカウント ≧ 1
NO
YES
リンク発行可能回数を参照
S508
S510
リンク発行可能回数 ≧ 1
NO
YES
リンク情報発行許可
リンク情報発行不許可

フロントページの続き

(51)Int.Cl. FI
G06F 12/14 540C
G06F 12/14 540P

(56)参考文献 特開２００１－０７８２６６（ＪＰ，Ａ）
特開２００４－２２７２８３（ＪＰ，Ａ）
特開２００５－０５６２３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｇ０６Ｆ ２１／２４