(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-254193
(P2004-254193A)
(43)公開日　平成16年9月9日(2004.9.9)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/08	H04L 9/00	601B	5B017
G06F 12/14	G06F 12/14	320F	5C064
G06F 17/60	G06F 17/60	142	5J104
H04N 7/16	G06F 17/60	302E	
H04N 7/173	G06F 17/60	332	

審査請求 未請求　請求項の数 11　ＯＬ　（全 26 頁）　最終頁に続く

(21)出願番号　特願2003-44363(P2003-44363)
(22)出願日　平成15年2月21日(2003.2.21)

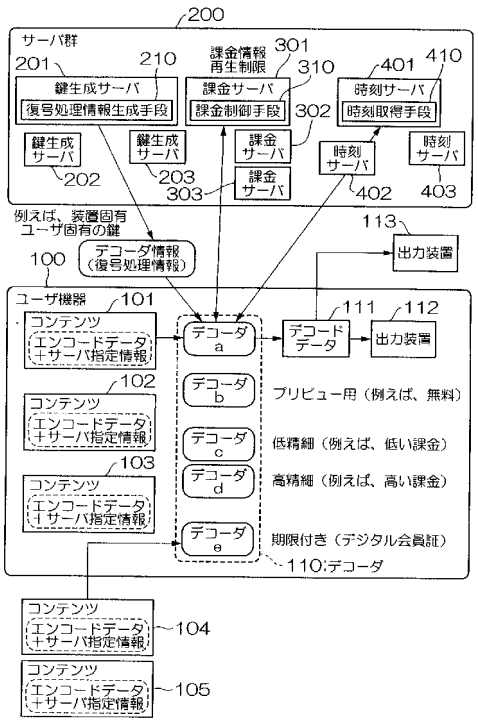
(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　100095728
弁理士　上柳　雅誉
(74)代理人　100107076
弁理士　藤綱　英吉
(74)代理人　100107261
弁理士　須澤　修
(72)発明者　稲積　満広
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

Ｆターム(参考)　5B017 AA06　AA07　BB10　CA16

最終頁に続く

(54)【発明の名称】ユーザ機器、サーバ、コンテンツ流通システム、コンテンツ流通方法、及びプログラム

(57)【要約】
【課題】本発明においては、ユーザの利便性を確保しながら、同時に、コンテンツの不正なコピー、不正な使用を防止し、また適正な課金を可能にする、ユーザ機器、サーバ、コンテンツ流通システムを提供することを目的とする。
【解決手段】ユーザ機器１００は、符号化されたコンテンツを復号するための復号処理情報を、再生条件（復号条件）を選択指定して、サーバ群２００の鍵生成サーバ２０１に要求し、鍵生成サーバ２０１から復号処理情報を受信する。そして、この復号処理情報を基に、デコーダ１１０により、符号化されたコンテンツの復号を行う。また、サーバ群２００内の鍵生成サーバ２０１は、ユーザ機器１００から、復号処理情報の送信要求を受信し、ユーザ機器１００おいて選択された再生条件を基に、復号処理情報を生成してユーザ機器１００に送信する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記ユーザ機器であって、
符号化されたコンテンツの情報を取得するための符号化データ取得手段と、
前記符号化されたコンテンツの復号処理情報を前記サーバに要求する復号処理情報要求手段と、
前記サーバから復号処理情報を受信する復号処理情報受信手段と、
前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手段と
を具備することを特徴とするユーザ機器。
【請求項２】
前記符号化されたコンテンツの復号条件を指定して、前記復号処理情報を前記サーバに要求する復号処理情報要求手段を
具備することを特徴とする請求項１に記載のユーザ機器。
【請求項３】
前記コンテンツ流通システムには、さらにユーザへの課金情報を保持する課金サーバが通信ネットワークを介して接続され、
前記復号処理情報により復号処理を実行する際には、前記課金サーバから課金情報を取得し、該課金情報に応じて復号処理の範囲を制限する手段を
さらに具備することを特徴とする請求項１または請求項２に記載のユーザ機器。
【請求項４】
前記コンテンツ流通システムには、さらにユーザへ時刻情報を提供する時刻サーバが通信ネットワークを介して接続され、
前記復号処理情報により復号処理を実行する際には、前記時刻サーバから時刻情報を取得し、該時刻情報を基に復号制限期間を判断する手段を
さらに具備することを特徴とする請求項１から３のいずれかに記載のユーザ機器。
【請求項５】
符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記サーバであって、
前記ユーザ機器から、前記復号処理情報の送信要求を受信するための復号処理情報送信要求受信手段と、
前記復号処理情報を生成するための復号処理情報生成手段と、
前記ユーザ機器に前記復号処理情報を送信するための復号処理情報送信手段と
を具備することを特徴とするサーバ。
【請求項６】
前記復号処理情報が、ユーザ機器から受信した復号条件に応じて生成されることを
特徴とする請求項５に記載のサーバ。
【請求項７】
前記コンテンツ流通システムには、さらにユーザへの課金情報を保持する課金サーバが通信ネットワークを介して接続され、
前記ユーザ機器から復号処理情報の送信要求があった場合には、前記課金サーバから課金情報を取得する手段と、
前記復号処理情報を、ユーザへの課金情報に応じて生成する手段と
を具備することを特徴とする請求項５または請求項６に記載のサーバ。
【請求項８】
符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおいて、

前記ユーザ機器には、
符号化されたコンテンツの情報を取得するための符号化データ取得手段と、
前記符号化されたコンテンツを復号するための復号処理情報を前記サーバに要求する復号処理情報要求手段と、
前記サーバから復号処理情報を受信する復号処理情報受信手段と、
前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手段と
を具備し、
前記サーバには、
前記ユーザ機器から、復号処理情報の送信要求を受信するための復号処理情報送信要求受信手段と、
前記復号処理情報を生成するための復号処理情報生成手段と、
前記ユーザ機器に前記復号処理情報を送信するための復号処理情報送信手段と
を具備することを特徴とするコンテンツ流通システム。
【請求項９】
符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおけるコンテンツ流通方法であって、
前記ユーザ機器により、
符号化されたコンテンツの情報を取得するための符号化データ取得手順と、
前記符号化されたコンテンツを復号するための復号処理情報を前記サーバに要求する復号処理情報要求手順と、
前記サーバから復号処理情報を受信する復号処理情報受信手順と、
前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手順と
が行われ、
前記サーバにより、
前記ユーザ機器から、復号処理情報の送信要求を受信するための復号処理情報送信要求受信手順と、
前記復号処理情報を生成するための復号処理情報生成手順と、
前記ユーザ機器に前記復号処理情報を送信するための復号処理情報送信手順と
が行われることを特徴とするコンテンツ流通方法。
【請求項１０】
符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記ユーザ機器内のコンピュータに、
符号化されたコンテンツの情報を取得するための符号化データ取得手順と、
前記符号化されたコンテンツの復号処理情報を前記サーバに要求する復号処理情報要求手順と、
前記サーバから復号処理情報を受信する復号処理情報受信手順と、
前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手順と
を実行させるためのプログラム。
【請求項１１】
符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記サーバ内のコンピュータに、
前記ユーザ機器から、前記復号処理情報の送信要求を受信するための復号処理情報送信要求受信手順と、
前記復号処理情報を生成するための復号処理情報生成手順と、
前記ユーザ機器に前記復号処理情報を送信するための復号処理情報送信手順と

を実行させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子情報（ディジタル情報）による種々のデータ、例えば動画データ、静止画データ、音楽データ、文字データ（本明細書では、これらのデータを単に「コンテンツ」ともいう）などの不正使用の防止および課金に係わる、ユーザ機器、サーバ、コンテンツ流通システム、及びプログラムに関し、特に、ユーザの利便性を確保しながら、同時に、コンテンツの不正なコピー、不正な使用を防止し、また適正な課金を可能にする、ユーザ機器、サーバ、コンテンツ流通システム、及びプログラムに関する。
【０００２】
【従来の技術】
ネットワーク技術の進歩により、広範囲のディジタル情報（コンテンツ）が、ネットワーク上で容易にやり取りされるようになった。これはユーザの利便性を大きく向上させるものである。その一方で、ディジタル情報であるコンテンツは複製による劣化が生じないため、不正、違法な複製物がネットワーク上に大量に公開されると言う状況もおきている。
【０００３】
このような状況は、短期的には著作権者の不利益、また、不正利用者の違法な利益になると考えられるが、これらの不正使用の防止策を必要以上に強化すれば、正当な使用者の利便性が低下し、コンテンツ利用者の減少を招くおそれもある。このような状態は、創作活動も停滞し、著作権者、利用者の双方の不利益につながるものである。
従って、使用者の利便性を確保しながら、同時に、コンテンツの不正なコピー、不正な使用を防止し、また適正な課金を可能にするシステムの提供が望まれていた。
【０００４】
このような問題を解決するための先行技術として以下に示すものがある。
例えば、特許文献１（特開平８－６７８４号公報「ソフトウェア／著作物の無断複製使用防止システムおよび無断複製使用防止処理方法」）に開示された発明は、図２４（特許文献１の図１）に示されているように、コンテンツの開錠／再利用処理手段、およびそれに与える利用鍵により、コンテンツを保護するものである。そのコンテンツの初回の使用時、また、利用鍵の使用期限が切れた場合は、外部の管理装置に対し、利用鍵の発行を要求し、新しい利用鍵を取得する。この際に課金処理が行われるものである。
【０００５】
また、特許文献２（特開平１１－８５５０４号公報「デジタルコンテンツ配布システム装置」）に開示された発明は、図２５及び図２６（特許文献２の図２及び図１１）に示すように、コンテンツを自己解凍型とすることにより、そのコンテンツを保護するものである。例えば、コンテンツの配布時においてはプリビューのみが可能なような解凍形式となっている。この制限を解除するために、ユーザは著作権代行センターへコンテンツの書き換え処理の発行を要求する。ユーザは、この発行された書き換え処理を用いて、前記コンテンツを書き換えることにより、制限を解除したコンテンツの利用が可能となる。課金は、この書き換え処理の発行の際に行われる。この従来例においては、コンテンツは常に自己解凍形式であり、鍵の紛失や、鍵とデータの対応の管理などが不要となる。また、この自己解凍形式のコンテンツは、使用時において、それ自身が単独で、その使用環境をチェックするようにすることも可能である。
【０００６】
また、特許文献３（特開２０００－９００３９号公報「音楽配信方法、送信装置および方法、ならびに、再生装置および方法」）に開示された発明は、機器が持つ固有のＩＤと公開鍵方式の暗号処理によりコンテンツを保護するものである。特許文献３の図６の処理に見られるように、機器の固有のＩＤに基づく公開鍵、秘密鍵を生成し、その公開鍵を認証サーバへ登録する。サーバにおいては、この公開鍵を用いてコンテンツを暗号化する。この暗号化されたコンテンツを解読できるのは秘密鍵を持つ機器のみであることにより、コ

ンテンツの受領者を特定することができ、それに対し課金を行う。
【０００７】
また、特許文献４（特開２０００－１８７９３５号公報「ディジタルデータ記録装置及びその方法並びにそのプログラムを記録したコンピュータ読み取り可能な記録媒体」）に開示された発明は、二次記憶媒体が持つ固有のＩＤを用いてコンテンツの保護を行うものである。特許文献４の図１に示されるように、暗号化されて配信されたコンテンツは一旦復号される。その後、コンテンツは、二次記憶媒体固有のＩＤを用いて再度暗号化され記録される。そのため、暗号化されたコンテンツが他の二次記憶媒体、つまり他のＩＤを持つ媒体へコピーされても、その暗号を解読することはできない。課金は、基本的にデータの受信時に行われる。
【０００８】
【特許文献１】
特開平８－６７８４号公報
【特許文献２】
特開平１１－８５５０４号公報
【特許文献３】
特開２０００－９００３９号公報
【特許文献４】
特開２０００－１８７９３５号公報
【０００９】
【発明が解決しようとする課題】
しかしながら、特許文献１で開示された発明では、コンテンツ利用の制限としては、再生期間の制限のみにしか対応できないものである。例えば、再生回数制限などには対応できない。
また、特許文献２で開示された発明では、デジタルコンテンツ配布システム装置は、自己解凍型の処理であるので、解凍時に何らかのチェック機能を持たせることができる。しかし、例えば再生回数制限のあるコンテンツを複製してしまえば、その複製のそれぞれが所定の回数の再生が可能となる。つまり、実質的に再生回数の制限を行うことはできない。
また、特許文献３に開示された発明では、単にコンテンツの配布先を特定する機能のみであり、再生期間の制限、再生回数の制限などを行うことはできない。また、特許文献４に開示された発明では、二次記憶媒体を特定する機能のみであり、再生期間の制限、再生回数の制限などを行うことはできない。
【００１０】
本発明はこのような問題を解決するためになされたものである。本発明においては、コンテンツの購入前に閲覧（プリビュー）を容易に可能とする。また、コンテンツの購入時においても必要に応じ、再生回数の制限、再生期間の制限、再生装置の制限、再生精度の制限を可能とする。またそれらの制限による適切な課金を可能とする。また、著作権者側へは、悪意あるユーザによる違法コピーを抑制する機能を提供し、また、正当なユーザの使用に対する適切な課金を可能とする、ユーザ機器、サーバ、コンテンツ流通システム、コンテンツ流通方法、及びプログラムを提供することを目的とする。
【００１１】
【課題を解決するための手段】
本発明は上記課題を解決するためになされたものであり、本発明のユーザ機器は、符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記ユーザ機器であって、符号化されたコンテンツの情報を取得するための符号化データ取得手段と、前記符号化されたコンテンツの復号処理情報を前記サーバに要求する復号処理情報要求手段と、前記サーバから復号処理情報を受信する復号処理情報受信手段と、前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手段とを具備することを特徴とする。

このような構成であれば、ユーザ機器おいて、符号化（暗号化）されたデータ（コンテンツ）を復号して再生する場合に、サーバに対して、復号するコンテンツの情報を指定して、復号処理情報（復号処理そのものを実行する情報）の送信を要求する。そして、サーバから復号処理情報を受信して、符号化されたデータを復号して再生する。
これにより、符号化データと対になった復号処理情報（復号処理そのものを実行する情報）を鍵として用いることができる。これにより、仮に符号化方式を不正に解読されたとしても、そのデータのみ、あるいは、同じ方式で符号化されたデータのみしか解読されない。また、今後、技術が進歩した場合、より高品質、あるいは、より解読が困難な符号化方式へ容易に移行できる。また、重要な情報はクライアント（ユーザ機器）の外部にあるため、クライアント側ではデータも復号処理もバックアップしたり、コピーしたりすることが自由である。また、コピーされたデータが外部に流出し使用された場合、その課金はコピー元に対してなされるため、ユーザ自身の不正な使用が抑制される。また、不正に持ち出そうとした場合においても、流出元が特定できることが、そのような不正行為を抑制する。

【００１２】
また、本発明のユーザ機器は、前記符号化されたコンテンツの復号条件を指定して、前記復号処理情報を前記サーバに要求する復号処理情報要求手段を具備することを特徴とする。
このような構成であれば、ユーザは、符号化されたコンテンツの復号条件を指定して、復号処理情報の生成を要求することができる。
これにより、符号化データの無制限使用、回数制限のある使用、時間制限のある使用、復号するハードウェアに制限のある使用、データ精度、データ量に制限のある使用、ユーザに制限のある使用、後処理での使用など、ユーザの都合にあわせて復号条件を指定（選択）してコンテンツを利用できる。

【００１３】
また、本発明のユーザ機器は、前記コンテンツ流通システムには、さらにユーザへの課金情報を保持する課金サーバが通信ネットワークを介して接続され、前記復号処理情報により復号処理を実行する際には、前記課金サーバから課金情報を取得し、該課金情報に応じて復号処理の範囲を制限する手段をさらに具備することを特徴とする。
このような構成であれば、復号処理情報を実行する際に、課金サーバからユーザの課金情報を取得し、ユーザの課金情報に応じて復号処理の範囲を制限する。
これにより、復号処理が起動された場合に、ユーザ機器は課金サーバと通信を行い、ユーザ自身の課金情報に応じて復号処理の範囲が制限できる。また、課金情報を偽造されることもない。

【００１４】
また、本発明のユーザ機器は、前記コンテンツ流通システムには、さらにユーザへ時刻情報を提供する時刻サーバが通信ネットワークを介して接続され、前記復号処理情報により復号処理を実行する際には、前記時刻サーバから時刻情報を取得し、該時刻情報を基に復号制限期間を判断する手段をさらに具備することを特徴とする。
このような構成であれば、例えば、コンテンツの利用に時間（期間）制限がある場合に、時刻サーバの時刻を基準として、再生制限を行う。
これにより、外部の時刻サーバから時刻情報を取得させるため、時刻情報を偽造されることもない。

【００１５】
また、本発明のサーバは、符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記サーバであって、前記ユーザ機器から、前記復号処理情報の送信要求を受信するための復号処理情報送信要求受信手段と、前記復号処理情報を生成するための復号処理情報生成手段と、前記ユーザ機器に前記復号処理情報を送信するための復号処理情報送信手段とを具

備することを特徴とする。
このような構成であれば、サーバにおいては、ユーザ機器からのコンテンツの指定情報と、復号処理情報（復号処理そのものを実行する情報）の送信要求を受信し、復号処理情報を生成し、ユーザ機器に送信する。
これにより、符号化データと対になった復号処理情報を鍵として用いることができる。これにより、仮に符号化方式を不正に解読されたとしても、そのデータのみ、あるいは、同じ方式で符号化されたデータのみしか解読されない。また、今後、技術が進歩した場合、より高品質、あるいは、より解読が困難な符号化方式へ容易に移行できる。また、重要な情報はクライアント（ユーザ機器）の外部にあるため、クライアント側ではデータも復号処理もバックアップしたり、コピーしたりすることが自由である。また、コピーされたデータが外部に流出し使用された場合、その課金はコピー元に対してなされるため、ユーザ自身の不正な使用が抑制される。また、不正に持ち出そうとした場合においても、流出元が特定できることが、そのような不正行為を抑制する。
【００１６】
また、本発明のサーバは、前記復号処理情報が、ユーザ機器から受信した復号条件に応じて生成されることを特徴とする。
このような構成であれば、サーバは、ユーザから指定された復号条件を基に、復号処理情報を生成する。
これにより、符号化データの無制限使用、回数制限のある使用、時間制限のある使用、復号するハードウェアに制限のある使用、データ精度、データ量に制限のある使用、ユーザに制限のある使用、後処理での使用など、ユーザの都合にあわせてコンテンツを利用できる。
【００１７】
また、本発明のサーバは、前記コンテンツ流通システムには、さらにユーザへの課金情報を保持する課金サーバが通信ネットワークを介して接続され、前記ユーザ機器から復号処理情報の送信要求があった場合には、前記課金サーバから課金情報を取得する手段と、前記復号処理情報を、ユーザの課金情報に応じて生成する手段とを具備することを特徴とする。
このような構成であれば、サーバで復号処理情報を生成する際に、ユーザの課金情報に応じて復号処理の範囲を制限することができる。
これにより、ユーザ自身の課金情報に応じて復号処理の範囲が決定できる。また、課金情報を偽造されることもない。
【００１８】
また、本発明のコンテンツ流通システムは、符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおいて、前記ユーザ機器には、符号化されたコンテンツの情報を取得するための符号化データ取得手段と、前記符号化されたコンテンツを復号するための復号処理情報を前記サーバに要求する復号処理情報要求手段と、前記サーバから復号処理情報を受信する復号処理情報受信手段と、前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手段とを具備し、前記サーバには、前記ユーザ機器から、復号処理情報の送信要求を受信するための復号処理情報送信要求受信手段と、前記復号処理情報を生成するための復号処理情報生成手段と、前記ユーザ機器に前記復号処理情報を送信するための復号処理情報送信手段とを具備することを特徴とする。
このような構成であれば、ユーザ機器は、符号化されたコンテンツを復号するための復号処理情報（復号処理そのものを実行する情報）をサーバに要求し、サーバから復号処理情報を受信する。そして、この復号処理情報を基に、符号化されたコンテンツの復号を行う。また、サーバは、ユーザ機器から、復号処理情報の送信要求を受信し、復号処理情報を生成してユーザ機器に送信する。
これにより、符号化データと対になった復号処理情報を鍵として用いることができる。こ

れにより、仮に符号化方式を不正に解読されたとしても、そのデータのみ、あるいは、同じ方式で符号化されたデータのみしか解読されない。同様に、今後、技術が進歩した場合、より高品質、あるいは、より解読が困難な符号化方式へ容易に移行できる。また、重要な情報はクライアント（ユーザ機器）の外部にあるため、クライアント側ではデータも復号処理もバックアップしたり、コピーしたりすることが自由である。また、コピーされたデータが外部に流出し使用された場合、その課金はコピー元に対してなされるため、ユーザ自身の不正な使用が抑制される。また、不正に持ち出そうとした場合においても、流出元が特定できることが、そのような不正行為を抑制する。

【００１９】

また、本発明のコンテンツ流通方法は、符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおけるコンテンツ流通方法であって、前記ユーザ機器により、符号化されたコンテンツの情報を取得するための符号化データ取得手順と、前記符号化されたコンテンツを復号するための復号処理情報を前記サーバに要求する復号処理情報要求手順と、前記サーバから復号処理情報を受信する復号処理情報受信手順と、前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手順とが行われ、前記サーバにより、前記ユーザ機器から、復号処理情報の送信要求を受信するための復号処理情報送信要求受信手順と、前記復号処理情報を生成するための復号処理情報生成手順と、前記ユーザ機器に前記復号処理情報を送信するための復号処理情報送信手順とが行われることを特徴とする。

このような手順であれば、ユーザ機器は、符号化されたコンテンツを復号するための復号処理情報（復号処理そのものを実行する情報）をサーバに要求し、サーバから復号処理情報を受信する。そして、この復号処理情報を基に、符号化されたコンテンツの復号を行う。また、サーバは、ユーザ機器から、復号処理情報の送信要求を受信し、復号処理情報を生成してユーザ機器に送信する。

これにより、符号化データと対になった復号処理情報を鍵として用いることができる。これにより、仮に符号化方式を不正に解読されたとしても、そのデータのみ、あるいは、同じ方式で符号化されたデータのみしか解読されない。同様に、今後、技術が進歩した場合、より高品質、あるいは、より解読が困難な符号化方式へ容易に移行できる。また、重要な情報はクライアント（ユーザ機器）の外部にあるため、クライアント側ではデータも復号処理もバックアップしたり、コピーしたりすることが自由である。また、コピーされたデータが外部に流出し使用された場合、その課金はコピー元に対してなされるため、ユーザ自身の不正な使用が抑制される。また、不正に持ち出そうとした場合においても、流出元が特定できることが、そのような不正行為を抑制する。

【００２０】

また、本発明のコンピュータプログラムは、符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記ユーザ機器内のコンピュータに、符号化されたコンテンツの情報を取得するための符号化データ取得手順と、前記符号化されたコンテンツの復号処理情報を前記サーバに要求する復号処理情報要求手順と、前記サーバから復号処理情報を受信する復号処理情報受信手順と、前記復号処理情報を基に、前記符号化されたコンテンツの復号を行う復号処理手順とを実行させるためのプログラムである。

【００２１】

また、本発明のコンピュータプログラムは、符号化されたコンテンツを復号して利用するユーザ機器と、前記符号化されたコンテンツの復号処理を実行する復号処理情報を前記ユーザ機器に通信ネットワークを介して送信するサーバとで構成されるコンテンツ流通システムにおける前記サーバ内のコンピュータに、前記ユーザ機器から、前記復号処理情報の送信要求を受信するための復号処理情報送信要求受信手順と、前記復号処理情報を生成するための復号処理情報生成手順と、前記ユーザ機器に前記復号処理情報を送信するための

復号処理情報送信手順とを実行させるためのプログラムである。
【００２２】
【発明の実施の形態】
次に本発明の実施の形態例について図面を参照して説明する。
【００２３】
［本発明の概要説明］
図１は、本発明のコンテンツ流通システムの概要を説明するための図であり、符号化（暗号化）されたコンテンツを復号して利用するユーザ機器１００と、サーバ群２００をシステムの構成要素としている。
サーバ群２００には、鍵となる「復号処理情報（復号処理そのものを実行するデコードプログラムなどの情報）」を生成するための復号処理情報生成手段２１０を有する鍵生成サーバ２０１、２０２、２０３、課金制御および再生制限情報を与えるための課金制御手段３１０を有する課金サーバ３０１、３０２、３０３、時刻情報（再生期限の判断情報）を与えるための時刻取得手段４１０を有する時刻サーバ４０１、４０２、４０３から構成される。
【００２４】
ユーザ機器１００は、パーソナルコンピュータなどであり、デコーダ１１０には、鍵生成サーバ２０１から受信したデコード情報（復号処理情報）が記録される。そして、符号化（暗号化）されたコンテンツ１０１乃至１０５を、デコーダ１１０により復号処理を行い、デコードデータ１１１を生成し、出力装置１１２又は１１３により再生する。なお、符号化（暗号化）されたコンテンツ１０１乃至１０５は、インターネットなどの通信ネットワークを介して受信したコンテンツか、または雑誌の付録により配布されるＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどに記録されたコンテンツである。このコンテンツは、「エンコードデータ（符号化されたデータ）」と、アクセスするサーバを特定する「サーバ指定情報」を含む。また、デコーダ１１０は固定的なものではなく、例えば、ソフトウェア手段により構成されるものであり、サーバ群２００から、デコード情報（復号処理情報）や、課金情報、再生制限情報、及び時刻情報を取得し、それぞれの情報に応じたデコード処理を行う。
例えば、デコーダａでは再生制限なくデコードを行い、デコーダｂではプリビュー用（無料）の再生を行い、デコーダｃでは低精細の解像度で再生を行う。また、デコーダｄでは高精細の解像度で再生を行い、デコーダｅでは、期限付きで再生を行う。
【００２５】
以上説明した、本発明のコンテンツ流通システムには以下の特徴がある。
・本発明のコンテンツ流通システムの、第１番目のポイントは、符号化（暗号化）されたコンテンツ１０１乃至１０５を通信により配布あるいは雑誌の付録などにより流通させ、それに対応する「デコード情報（復号処理情報）」は復号処理そのものを実行するプログラム（又はコード）などであり、これを符号化されたデータを使用するための鍵とし、この「復号処理情報」を課金と引き換えに生成し、配布すると言うものである。この点においては、前述した従来例２（特許文献２）に類似したものであるが、本発明においては、コンテンツと一体化した自己解凍形式を採らない。これにより、鍵（復号処理情報）とコンテンツの１対多数の対応を可能とする。これは、例えば会費制のＷＥＢサイトでのコンテンツアクセスなどを容易に可能とするものである。
【００２６】
・本発明のコンテンツ流通システムの第２番目のポイントは、その鍵たる「デコード情報（復号処理情報）」は、課金に係わる情報を外部の課金サーバ３０１との通信により取得すること、また、期限付き使用などの場合の時刻情報においても、外部の時刻サーバ４０１との通信により取得するものとすることである。これにより、ユーザサイドでのデータの偽造を防止する。またユーザ機器１００においても、コンテンツの複製、バックアップを可能とするものである。
【００２７】

・本発明のコンテンツ流通システムの第３番目のポイントは、上の２番目のポイントの例外として、ユーザの信用度に応じて、後処理課金を可能とすることである。これにより、課金サーバ３０１、時刻サーバ４０１との通信が不可能である場合に、コンテンツの使用を単純に禁止すると言うような、ユーザの利便性の低下を防ぐものである。
・また、このコンテンツ流通システムにおいては、「復号処理情報」そのものが動的に生成され、デコーダ情報（復号処理情報）が鍵として配布される。そのため、符号化（暗号化）アルゴリズムは技術の進歩により都度更新することが可能となる。また、通信プロトコル、通信先なども容易に変更が可能となる。そのため、従来例２にあるような著作権代行センターのようなものは不要である。つまり、同一の流通手段においても、コンテンツ毎にその著作権者が独自の課金制御手段を運用することが可能となる。またこのように、通信プロトコル、通信先などが複数となり得るので、悪意あるユーザによる通信データの偽造は困難になる。
・また、正当なユーザにおいては、このような通信はユーザに意識されない部分で行われるため、利便性を低下させることはない。

【００２８】
実際の運用においては、例えば、データのプリビューのみを行える鍵（「復号処理情報」）は、自由に流通させることが考えられる。この鍵は、例えば、動画データ、音楽データであれば、視聴できる範囲が限られるなどの制約を与える。静止画データなどであれば、その画像サイズ、解像度などに制約を与える。あるいは、それらにおいて、画像の主要部分にプリビューである旨の表示がなされるようにしてもよい。

【００２９】
ユーザがそのプリビューより判断し、そのデータの購入を決めた場合、鍵生成サーバ２０１内の復号処理情報生成手段２１０に対し、ユーザがそのデータを復号する環境、ユーザがそのデータを使用したい条件などを送信し、そのデータをそのユーザが使用するための、カスタマイズされた復号処理情報の生成を要求する。

【００３０】
また、鍵生成サーバ２０１内の復号処理情報生成手段２１０は、課金サーバ３０１内の課金制御手段３１０との通信により、カスタマイズされた復号処理の生成の許諾を求める。許諾が得られた場合、復号処理情報生成手段２１０は、復号処理情報を生成し、ユーザ機器１００へ送信する。一方、課金制御手段３１０には、それに対する課金情報が記録される。

【００３１】
この復号処理には、例えば以下のようなパターンが考えられる。
（１）符号化されたコンテンツのデータの無制限使用（多分最も高価）
復号処理は、起動される度に、人力されたデータを確認し、対応するデータであれば無条件に復号処理を行う。
（２）回数制限のある使用
復号処理は、起動される度に、予め自らの中にある情報により課金制御手段３１０へ通信を行い、そこから得られる許容された回数に達するまでは復号処理を行う。許容された回数を超えた場合、復号処理は、復号を拒否するか、あるいは、追加の課金を受諾するかどうかをユーザ機器へ質問する。この時、許容回数データは課金制御手段３１０の中にあるので、ユーザはこれを偽造できない。
また、通信プロトコル、通信データの符号化、通信先などは、カスタマイズされた復号処理ごとに変更が可能であるので、悪意あるユーザの通信データの偽造は困難である。
このパターンにおいては、許容された回数を超えるまでは、ユーザは、課金制御手段３１０などを意識することはない。

【００３２】
（３）時間制限のある使用
復号処理は、起動される度に、予め自らの中にある情報により課金制御手段３１０へ通信を行い、許容された制限時間を取得する。その後、同様に自らの中にある情報により時刻

取得手段４１０と通信を行い時刻情報を得る。その時刻と、課金制御手段３１０から得た制限時刻情報との比較により復号処理を行う。時刻が許可されない値である場合、復号を拒否するか、あるいは、追加の課金を受諾するかどうかをユーザ機器へ質問する。この時、制限時刻データは課金制御手段３１０の中にあり、現在の時刻は時刻取得手段４１０の中にあるので、ユーザはこれを偽造できない。
このパターンにおいては、許容された時刻を超えるまでは、ユーザは、課金制御手段３１０、時刻取得手段４１０などを意識することはない。
【００３３】
（４）復号するハードウェアに制限のある使用
復号処理は、起動される度に、予め自らの中にあるハードウェアの情報を用いて、自らが起動されたハードウェアが正当なものかどうかを判断することができる。これには、ネットワークアドレス、ネットワークハードウェアのＭＡＣアドレス、ＣＰＵのＩＤ、あるいは、その他のハードウェアの名称、ＩＤなど、さらには、それらの組み合わせを用いることができる。
逆に言うと、この制限の無い場合、正当なユーザは、この復号処理のコピー、符号化されたデータのコピーを、他の制限内において、任意のハードウェアで実行することが可能となる。
【００３４】
（５）データ精度、データ量に制限のある使用
上のハードウェア制限と類似したものであるが、例えば、ある静止画であれば、許諾された分解能、サイズまででであれは使用できるとするものである。また動画であれば、更に、再生区間の制限などが考えられる。
（６）ユーザに制限のある使用
復号処理は、起動される度に、ユーザへ何らかの認証手段の提示を求め、予め自らの中にある情報を用いて、正当なユーザであるかどうかの判断を行う。
（７）後処理での使用
上の何れの使用においても、使用が許可されない場合、例えば、ユーザ機器１００が課金制御手段３１０、時刻取得手段４１０との通信ができない場合などにおいて、その復号手段の正当な所有者の信頼度、あるいは、前払いされた課金情報などによっては、一時的な使用を許可すると言うパターンも考えられる。
【００３５】
［従来例との比較］
なお、従来例１（特許文献１）とは、コンテンツと鍵が別であると言う点は同じである。しかし、従来例１では、鍵に通信機能や復号機能はなく、極端に言えは、単に使用期限日を示すためだけのものである。そのため、再生回数の制限は不可能であり、また期日の制限も容易に偽造され得る。
従来例２（特許文献２）とは、復号処理を鍵として使用すると言う点は同じである。しかし、従来例２では、この鍵とコンテンツは一体化され、自己解凍処理として実行される。そのため、再生回数の制限は容易に破られ得るものである。また期日の制限も容易に偽造され得る。
さらに、鍵とコンテンツが一体化されていると言うことにより、例えば、あるコンテンツのグループに対し、一括した鍵を与えると言うようなことはできない。
従来例３、４（特許文献３、４）においては、コンテンツの使用に対し、細かな制限を課すことはできない。
【００３６】
［具体例の説明］
図２は、本発明のコンテンツ流通システムにおけるユーザ機器１００が有する手段の構成例を示す図であり、本発明に直接関係する手段の構成例を示したものである。なお、ユーザ機器１００にはパーソナルコンピュータなどを使用できる。
（１）符号化データ取得手段１２１

取り扱いたい種々の電子情報、例えば動画データ、静止画データ、音楽データ、文字データ（コンテンツ）などを取得する手段である。具体的には、ネットワーク経由であればネットワーク通信手段、雑誌の付録のＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどでの配布形態であれば固定記憶媒体読み出し手段、同様に、磁気記憶媒体などへバックアップされたデータ、あるいはコピーされたデータであれば、それらの読み出し手段である。また、インターネット放送などのストリーミングデータなどの時は、それらの受信手段である。

【００３７】

（２）符号化データ記憶手段１２２

複数回の復号処理（再生処理）などを想定した場合、符号化されたコンテンツのデータを記憶するための手段である。なお、ストリーミングなどの１回のみの復号処理時は、符号化データ記憶手段１２２を省略することができる。

（３）復号処理選択手段１２３

符号化されたコンテンツに対応する復号処理を、後述する「復号処理情報記憶手段１２６」の中から選択する。コンテンツデータに対応する復号処理が「復号処理情報記憶手段１２６」の中に発見された場合、それを選択する。発見できなかった場合は、「復号処理情報要求手段１２４」を起動する。

【００３８】

（４）復号処理情報要求手段１２４

上述した符号化されたコンテンツに対応する「復号処理生成要求」を、外部のサーバ群２００内の復号処理情報生成手段２１０へ送信する。この時、以下の情報の内の１つ以上が復号処理生成条件として送信データに付加される。

・クライアントであるユーザ機器１００自身の情報、例えば、ネットワークアドレス、ネットワークハードウェアのＭＡＣアドレス、などの自分自身を特定する情報

・復号したいコンテンツデータに係わる情報、例えばファイル名、あるいは、データの識別子などの情報

・復号条件の選択情報（復号処理にかかわる条件）、例えば、期限付き復号、回数制限付き復号、解像度制限、表示装置制限などのユーザによる復号条件の選択情報

・ユーザに係わる情報、例えば登録された会員のユーザＩＤなどの情報等

【００３９】

なお、「復号処理情報生成要求」のデータの送信先となる「復号処理情報生成手段２１０」は、「課金制御手段３１０」と同一のサーバ内にあってもよい。あるいは、別のサーバに設けてもよい。また、この時、復号処理情報生成手段２１０は、要求元であるクライアント（ユーザ機器１００）に対し、要求されたデータ、要求された条件での復号処理情報を生成することを許可するかしないかを「課金制御手段３１０」へ問い合わせることができる。

課金制御手段３１０が「復号処理情報」の生成を不許可とした場合、それをクライアントのユーザ機器１００へ通知する。課金制御手段３１０が「復号処理情報」の生成を許可した場合、許可された条件に対する「復号処理情報」を生成したことを「課金制御手段３１０」へ通知する。また同時に、「復号処理情報」をクライアント（ユーザ機器１００）へ送信する。この生成された「復号処理情報」には、上に述べた復号処理情報生成条件に加え、課金制御手段３１０への通信方法、時刻取得手段４１０への通信方法、などが符号化（暗号化）されて付加される。

【００４０】

（５）復号処理情報受信手段１２５

復号処理情報生成手段２１０の生成した情報を受信する。復号処理情報生成手段２１０が復号処理情報の生成を拒否した場合、その旨がユーザ機器１００へ通知される。

（６）復号処理情報記憶手段１２６

復号処理情報生成手段２１０により生成された１つ以上の「復号処理情報」を記憶する。「復号処理情報」は復号処理そのものを実行する情報（例えば、デコーダプログラムなど）であり、復号処理情報記憶手段１２６に記憶される「復号処理」は、対応する符号化デ

ータを復号する鍵となるものであり、かつ、次に掲げる機能の内、少なくとも一つ以上の機能を有する。
・復号許可条件記憶機能
復号するデータの識別子、回数制限、時刻制限、精度制限、マシン制限、ユーザ制限、通信すべき課金制御手段３１０の識別子、通信すべき時刻取得手段４１０の識別子、後処理許可の条件
・課金制御手段３１０との通信機能
・時刻取得手段４１０との通信機能
・復号履歴記憶機能
【００４１】
（７）出力手段１２７
復号処理により復号されたデータを出力する。プリンタ、プロジェクタ、ディスプレイ、オーディオ機器などである。これが、記憶装置であってはならない。この部分は、何らかの意味で出力機器のハードウェア依存となる。例えば、ビデオ信号、オーディオ信号、プリンタ制御信号などである。このレベルでの信号の盗聴、再利用については、有効な対策が少ない。しかし、このレベルの信号が出力ハードウェア依存であることが、ある程度の不正に対する抑止効果をもつ。
【００４２】
また、図３は、復号処理情報の生成要求についての、ユーザ機器１００内のデータ処理手段１３０、サーバ群２００内の復号処理情報生成手段２１０、課金制御手段３１０との相互作用を説明するための図である。説明を簡単にするために、「復号処理情報生成要求」が成功する場合のみを記載している。なお、復号処理情報生成手段２１０と、課金制御手段３１０は同一のサーバ内にあってもよい。また、それぞれが複数のサーバに設けられてもよい。
（１）ステップＳ１０１：ユーザ機器１００内のデータ処理手段１３０により、サーバ群２００内の復号処理情報生成手段２１０に対して、復号処理パラメータを送信する。この復号処理パラメータは、ユーザが選択した復号条件を基に生成されるパラメータである。
（２）ステップＳ１０２：サーバ群２００内の復号処理情報生成手段２１０では、ユーザ機器１００からの「復号処理パラメータ」を受信する。
（３）ステップＳ１０３：復号処理情報生成手段２１０から課金制御手段３１０に、「復号処理情報の生成」の許可／不許可の問い合わせを行う。
（４）ステップＳ１０４：課金制御手段３１０は、「復号処理情報の生成」の許可／不許可の判断を行う。
（５）ステップＳ１０５：課金制御手段３１０により、「復号処理情報の生成」が許可された場合は、復号処理情報生成手段２１０は、「復号処理情報」を生成し、ユーザ機器１００に送信する。
（６）ステップＳ１０６：ユーザ機器１００内のデータ処理手段１３０では、「復号処理情報」を受信し、記憶する。
（７）ステップＳ１０７：サーバ群２００内の復号処理情報生成手段２１０は、課金制御手段３１０に対して、「復号処理情報」を生成したことを通知する。
（８）ステップＳ１０８：課金制御手段３１０では、復号処理情報生成手段２１０から受信した「復号処理情報」を基に、課金情報を記録する。
【００４３】
また、図４は、復号処理において、ユーザ機器１００内のデータ処理手段１３０と、サーバ群２００内の課金制御手段３１０と、時刻取得手段４１０との相互作用を説明するための図である。説明を簡単にするために、ユーザ機器１００において「復号処理」が許可される場合のみを記載している。この時、課金制御手段３１０と、時刻取得手段４１０は同一のサーバ内にあってもよい。また、それぞれが複数のサーバに設けられてもよい。
（１）ステップＳ２０１：ユーザ機器１００内のデータ処理手段１３０により、サーバ群２００内の課金制御手段３１０に「復号処理パラメータ」を送信する。なお、この復号処

理パラメータは、ユーザが選択した復号条件を基に生成されるパラメータである。
（２）ステップＳ２０２：サーバ群２００内の課金制御手段３１０では、ユーザ機器１００からの「復号処理パラメータ」を受信する。
（３）ステップＳ２０３：課金制御手段３１０では、「復号」の許可／不許可の判断を行う。
（４）ステップＳ２０４：課金制御手段３１０は、復号の許可条件をユーザ機器１００へ送信する。
（５）ステップＳ２０５：課金制御手段３１０は、復号履歴の情報を記録する。
（６）ステップＳ２０６：ユーザ機器１００内のデータ処理手段１３０では、「許可条件」を受信する。
（７）ステップＳ２０７：ユーザ機器１００内のデータ処理手段１３０は、サーバ群２００内の時刻取得手段４１０に対して、時刻情報の送信を要求する。
（８）ステップＳ２０８：サーバ群２００内の時刻取得手段４１０は、ユーザ機器１００から「時刻情報要求」を受信する。
（９）ステップＳ２０９：時刻取得手段４１０は、「時刻情報」をユーザ機器１００に送信する。
（１０）ステップＳ２１０：ユーザ機器１００は、サーバ群２００の時刻取得手段４１０から「時刻情報」を受信する。
（１１）ステップＳ２１１：ユーザ機器１００内のデータ処理手段１３０では、「時刻情報」を基に、復号の許可／不許可を判断する。
（１２）ユーザ機器１００では、復号が許可されている場合に、復号を開始する。
【００４４】
また、図５はユーザ機器１００における復号処理の例を示すフローチャートである。
（１）ステップＳ３０１：復号処理パラメータを添えて復号処理を起動する。なお、この復号処理パラメータは、ユーザが選択した復号条件を基に生成されるパラメータである。
（２）ステップＳ３０２：「復号の許可／不許可」をサーバ群２００内の課金制御手段３１０へ問い合わせる。
（３）ステップＳ３０３：復号許可の問い合わせが成功したかどうかを判断する。
（４）ステップＳ３０４：復号許可の問い合わせが成功した場合は、復号が許可されるかどうかを判断する。
（５）ステップＳ３０５：復号許可の場合は、時刻条件があるかどうかを判断する。時刻条件のない場合は、復号処理を開始する（ステップＳ３０８）。
（６）ステップＳ３０６：時刻条件がある場合は、「時刻情報」をサーバ群２００の時刻取得手段４１０に問い合わせる。
【００４５】
（７）ステップＳ３０７：時刻条件が「ＯＫ（はい）」がどうかを判断する。
（８）ステップＳ３０８：時刻条件が「ＯＫ」の場合は、復号を開始する。
（９）ステップＳ３０９：時刻条件が「ＮＯ（いいえ）」の場合は、復号不許可通知を受信する。
（１０）ステップＳ３１０：時刻条件により復号が許可されない場合は、追加課金を了承するかどうかを判断する。
（１１）ステップＳ３１１：追加課金を了承する場合は、新しい「復号処理情報」の生成を要求する。
（１２）ステップＳ３１２：ステップＳ３０３において、復号許可の問い合わせが行えなかった場合は、後処理（例えば、料金後納）が許可されているかどうかを判断する。後処理（例えば、料金後納）が許可されている場合は、復号処理を開始する（ステップＳ３０８）。
【００４６】
また、図６はプリビュー、および解像度制限を説明するための図であり、ある花の絵を説明のために二値化したものである。

【００４７】
図７は説明のための１例として、ＪＰＥＧ２０００の処理を概説するための図である。ＪＰＥＧ２０００においては、水平方向、垂直方向のそれぞれにおいて、画像の空間周波数を高周波側、低周波側に２分する。この低周波側を更に分割することにより、再帰的に画像の周波数成分を分解して行く。その結果、図７の最も左上に低周波成分の画像、あるいは縮小画像が得られ、右下の方へ向かうにつれて、その画像の高周波成分が示される。
【００４８】
図８は、周波数領域によるデータの例を示す図である。図８（ａ）は、例として、３段階に分解された内の最も低周波側のデータを示したものである。図８（ｂ）はそれに続く中間周波数領域を、図８（ｃ）は最も高周波領域のデータを示したものである。
【００４９】
また、図９は、花の絵ではないが、この周波数成分の画像に与える影響を模式的に示した図である。図９は、例えば、最も低周波側のデータのみを用いて復号した画像である。このように、空間解像度の低い画像が得られる。あるいは、空間解像度を上げるとすると、小さな画像となる。
【００５０】
また、図１０は周波数データの全てを用いて復号した画像の例を示す図である。このように、図９に比較して、より精細な画像が復号される。このような性質を用い、図９のような画像はプリビュー画像として無償で提供し、図１０のような、より精細な画像を要求するユーザには課金を行うことを想定している。
【００５１】
また、図１１は、異なる周波数成分により画像の精細度を変化させる方法を説明するための図である。例えば、図８（ａ）、（ｂ）、（ｃ）に示したような、各周波数成分毎のデータが、同一の符号化方式で符号化されているとする。つまり、プリビューで許容されている図８（ａ）に示す画像と、それ以外のデータが同じ符号化方式で符号化されているとすると、悪意のあるユーザにより、プリビュー用の復号処理手段より、図８（ｂ）、（ｃ）を復号する処理情報を作成される可能性がある。本発明においては、ユーザへは符号化された全てのデータが配布されていると想定しているため、このような処理情報が作成されれば、「復号処理情報」がコンテンツ保護の鍵としての機能を失ってしまう。
【００５２】
このようなことを防ぐために、本発明においては、例えば、図１１に示すように、周波数成分毎に異なる符号化方式で符号化することができる。すなわち、低解像度データにはデータ符号化処理ａを施し、符号化データ０を生成する。高解像度差分データ１には、データ符号化処理ｂを施し、符号化データ１を生成する。高解像度差分データ２には、データ符号化処理ｃを施し、符号化データ２を生成する。高解像度差分データＮには、データ符号化処理Ｎを施し、符号化データＮを生成する。そして、これらのデータ符号化処理の際には、それぞれ異なる符号化方式で符号化する。この符号化処理には、異なる符号化アルゴリズム、異なる符号化パラメータを使用するなどの方法が使用できる。これにより、プリビュー画像（低解像度データ）の「復号処理情報」の中には、高周波側のデータ（高解像度の符号化データ）の復号処理に係る情報が含まれないために、コンテンツをより有効に保護することができる。
【００５３】
また、図１２は、種々の再生制限に係る情報と、その符号化について説明するための図である。最初に、いくつかの制限について説明する。
・条件Ａは、ユーザＩＤが「１２３４」であるユーザが、コンテンツの１を、無制限使用が可能な条件において買い取った場合を想定している。この時、再生回数制限や再生期限制限は、パラメータ中に「なし」と記載される。
・条件Ｂは、例えば雑誌などに広告として、コンテンツの２から８までを、再生回数制限あり、再生期限制限あり、再生量の制限もありとして、例えば、無料で配布するような場合のパラメータの例である。

・条件Ｃは、例えば、あるコンテンツを配布するサイトの、会費制会員を実現するような例である。この時、再生できるコンテンツは無制限であるが、ユーザは制限され、かつ再生期限も制限される。また、この例では、会員の信用度により、課金の後払いも許可と言うパラメータ例となっている。
これらの条件は、パラメータ符号化処理により符号化され、符号化パラメータとして、復号処理情報に組み込まれる。
【００５４】
また、図１３は、復号処理１４０に必要な機能及び要素をまとめて示した図である。本発明によるコンテンツ保護の鍵となる復号処理情報には、図１３に示す要素を含んでもよい。
（１）課金制御手段通信機能１４１
課金制御手段通信機能１４１は、課金制御手段との通信機能である。悪意あるユーザに改変されないように、この通信機能は複数用意され、あるいは、通信相手となる課金制御手段ごとに異なってもよい。
（２）時刻取得手段通信機能１４２
時刻取得手段通信機能１４２は、時刻取得手段との通信機能である。悪意あるユーザに改変されないように、この通信機能は複数用意され、あるいは、通信相手となる時刻取得手段ごとに異なっても良い。
（３）符号化パラメータ１４３
符号化パラメータ１４３は、図１２に例示したパラメータである。
（４）コンテンツ情報取得手段１４４
コンテンツ情報取得手段１４４は、符号化パラメータ１４３に記載されたデータと、実際に復号しようとしているコンテンツとの一致をみるためのものである。例えば、コンテンツの一部としての識別子の読み出し手段であるとか、あるいは、コンテンツのチェックサムを計算する計算手段などであってもよい。
【００５５】
（５）ハードウェア情報取得手段１４５
ハードウェア情報取得手段１４５は、符号化パラメータ１４３に記載されたデータと、実際に復号しようとしているハードウェアとの一致をみるためのものである。例えば、ネットワークアドレス、ネットワークハードウェアのＭＡＣアドレスの読み出し手段であるとか、あるいは、ハードウェア全体の構成を数値化する識別子計算手段などであってもよい。
（６）ユーザ情報取得手段１４６
ユーザ情報取得手段１４６は、符号化パラメータ１４３に記載されたデータと、ユーザとの一致をみるためのものである。例えば、ユーザに対してパスワードを求めるとか、あるいは、生体特徴（生体情報）を用いた個人認証手段であってもよい。
（７）データ復号化処理１４７
これは、符号化されたコンテンツを復号する処理であり、必要なもののみが含まれれば良い。例えば、プリビューのみを許可するような場合は、それ用の復号処理のみが含まれる。
【００５６】
図１４は、静止画を例としたプリビューの例を示す図である。例えば、図１４（ａ）のように、解像度の低いデータに、それがプリビューであることを示す情報「Ｐｒｅｖｉｅｗ」を付加して表示する。あるいは、図１４（ｂ）のように、課金対象となる高解像度のデータに、内容を劣化させる情報を重畳して表示することなどが考えられる。
【００５７】
また、図１５は、ユーザ機器１００がサーバと通信ができないような状況で、かつ、課金後処理が許されている場合の表示例を示す図である。
【００５８】
また、図１６から図１９は、復号しようとしている状況が、何らかの制限を越えているよ

うな場合の表示例である。
・図１６に示す画面は、コンテンツの使用期限（再生許可の期限）を過ぎた場合に表示される画面例を示す図である。追加課金されることを了承すると、コンテンツを再度再生できるようになる。
・図１７に示す画面は、コンテンツを許可されていない装置により再生しようとした場合に表示される画面例を示す図である。追加課金されることを了承すると、コンテンツを再生できるようになる。
・図１８に示す画面は、高解像度でのコンテンツの再生が許可されなかった場合の画面例を示す図である。追加課金されることを了承すると、コンテンツを高精度で再生できるようになる。
・図１９に示す画面は、コンテンツの使用回数制限を超過した場合に表示される画面例を示す図である。追加課金されることを了承すると、コンテンツを再生できるようになる。
・図２０に示す画面は、復号制限としてユーザが限定されている場合に、ユーザにパスワードの入力を求める画面例を示す図である。

【００５９】

また、図２１は、ユーザ機器１００が、通信ネットワーク１を介して、サーバ群２００と接続されることを示す模式図である。鍵生成サーバ２０１ａから鍵生成サーバ２０１ｎには、それぞれ復号処理情報生成手段１（２１０ａ）から復号処理情報生成手段Ｎ（２１０ｎ）が設けられる。課金サーバ３０１ａから課金サーバ３０１ｎには、それぞれ課金制御手段１（３１０ａ）から課金制御手段Ｎ（３１０ｎ）が設けられる。時刻サーバ４０１ａから時刻サーバ４０１ｎには、それぞれ時刻取得手段１（４１０ａ）から時刻取得手段Ｎ（４１０ｎ）が設けられる。すなわち、復号処理情報生成手段、課金制御手段、時刻取得手段のそれぞれの手段が複数の場所（サイト）に存在し得ることが本発明のコンテンツ流通システムの特徴であることを示している。

【００６０】

また、図２２は、本発明のコンテンツ流通システムにおけるユーザ機器１００の構成例を示すブロック図であり、本発明に直接関係するものを示したものである。図２２において、ユーザ機器１００には、ユーザ機器１００と通信ネットワーク１とを接続する通信用インタフェース１５１、ユーザ機器１００の全体を統括制御する制御部１５２、処理プログラム部１６０が設けられる。なお、ユーザ機器１００としてはパーソナルコンピュータを使用できる。

【００６１】

また、処理プログラム部１６０には、以下の処理部が含まれる。
・符号化データ取得処理部１６１は、取り扱いたい種々の電子情報、例えば動画データ、静止画データ、音楽データ、文字データ（コンテンツ）などを取得する処理部である。具体的には、ネットワーク経由であればネットワーク通信処理部、雑誌の付録のＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどでの配布形態であれば固定記憶媒体読み出し処理を行う。同様に、磁気記憶媒体などへバックアップされたデータ、あるいはコピーされたデータであれば、それらの読み出し処理を行う。また、放送などのストリーミングデータなどの時は、それらの受信処理を行う。

【００６２】

・符号化データ記憶処理部１６２は、複数回の復号処理（再生処理）などを想定した場合、符号化されたコンテンツのデータを記憶するための処理部である。ストリーミングなどの１回のみの復号処理時は、符号化データ記憶処理部１６２を省略することができる。
・復号処理選択処理部１６３は、符号化データされたコンテンツに対応する復号処理を、記憶部１７０内に記録された「復号処理情報」の中から選択するための処理部である。コンテンツデータに対応する復号処理が、記憶部１７０内に記録された「復号処理情報」の中から発見された場合、それを選択する。発見できなかった場合は、復号処理情報要求処理部１６４を起動する。
・復号処理情報要求処理部１６４は、符号化されたコンテンツに対応する「復号処理情報

生成要求」を、外部のサーバ群２００内の復号処理情報生成手段２１０へ送信するための処理部である。なお、この「復号処理情報生成要求」には、復号条件の選択情報（復号処理にかかわる条件）、例えば、期限付き復号、回数制限付き復号、解像度制限、表示装置制限などのユーザによる復号条件の選択情報が付加されて送信される。

【００６３】

・復号処理情報受信処理部１６５は、サーバ群２００内の復号処理情報生成手段２１０が生成した「復号処理情報」を受信するための処理部である。復号処理情報生成手段２１０が復号処理情報の生成を拒否した場合、その旨がユーザ機器１００に通知される。

・復号処理情報記憶処理部１６６は、サーバ群２００内の復号処理情報生成手段２１０により生成された１つ以上の「復号処理情報」を記憶部１７０に記憶するための処理部である。

・時刻情報要求処理部１６７は、サーバ群２００内の時刻取得手段４１０に対して、「時刻情報要求」を送信するための処理部である。

・時刻情報受信処理部１６８は、サーバ群２００内の時刻取得手段４１０から、「時刻情報」を受信するための処理部である。

・出力処理部１６９は、復号処理により復号されたデータを出力するための処理部である。復号されたデータを、プリンタ、プロジェクタ、ディスプレイ、オーディオ機器などに出力する。

【００６４】

なお、ユーザ機器１００の処理プログラム部１６０は専用のハードウェアにより実現されるものであってもよく、またこの処理プログラム部はメモリおよびＣＰＵ（中央処理装置）等の汎用の情報処理装置により構成され、この処理部の機能を実現するためのプログラム（図示せず）をメモリにロードして実行することによりその機能を実現させるものであってもよい。なお、このユーザ機器１００には、周辺機器として入力装置、表示装置等（いずれも図示せず）が接続され又は内蔵されているものとする。ここで、入力装置としては、キーボード、マウス等の入力デバイスのことをいう。表示装置とは、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）や液晶表示装置等のことをいう。

【００６５】

また、図２３は、本発明のコンテンツ流通システムにおけるサーバの構成例を示すブロック図であり、本発明に直接関係するものを示したものである。なお、図２３に示す構成例では、図２１に示す復号処理情報生成手段２１０ａ、課金制御手段３１０ａ、時刻取得手段４１０ａを一つのサーバ内に設けた例を示しているが、勿論、複数のサーバに分散して設備してもよい。図２３において、サーバ５００には、サーバ５００と通信ネットワーク１とを接続する通信用インタフェース５０１、サーバ５００の全体を統括制御する制御部５０２、処理プログラム部５１０が設けられる。また、処理プログラム部５１０は、復号処理情報生成処理部５２０と、課金制御処理部５３０と、時刻取得処理部５４０で構成される。

そして、復号処理情報生成処理部５２０には下の処理部が含まれる。

・復号処理情報要求受信処理部５２１は、ユーザ機器１００から、「復号処理情報」の送信要求を受信するための処理部である。

・復号処理情報生成処理部５２２は、符号化されたコンテンツを復号処理するための「復号処理情報」を生成するための処理部である。

・復号処理情報送信処理部５２３は、ユーザ機器に「復号処理情報」を送信するための処理部である。

【００６６】

また、課金制御処理部５３０には下の処理部が含まれる。

・復号処理パラメータ受信処理部５３１は、ユーザ機器１００または復号処理情報生成処理部５２０から、復号処理パラメータを受信するための処理部である。なお、この復号処理パラメータは、ユーザが選択した復号条件を基に生成されたパラメータである。

・復号の許可／不許可判断処理部５３２は、課金情報ＤＢ５７０内の課金情報を参照し、

該当ユーザの課金情報を基に、「復号処理情報」を生成することについての許可／不許可の判断を行うための処理部である。
・許可条件の送信処理部５３３は、復号の許可条件をユーザ機器１００の送信するための処理部である。
・復号履歴更新処理部５３４は、復号履歴の情報を課金情報ＤＢ５７０に記録するための処理部である。
【００６７】
また、時刻取得処理部５４０には下の処理部が含まれる。
・時刻情報要求受信処理部５４１は、ユーザ機器１００から「時刻情報要求」を受信するための処理部である。
・時刻情報生成処理部５４２は、ユーザ機器１００に送信する時刻情報を生成するための処理部である。
・時刻情報送信処理部５４３は、「時刻情報」をユーザ機器１００に送信するための処理部である。
なお、ユーザ情報データベース（ＤＢ）５５０には、このコンテンツ流通システムに登録した会員の個人情報と、会員識別ＩＤ、パスワードの情報などが記録される。また、復号処理情報ＤＢ５６０には、生成した復号処理情報が記録される。また、課金情報ＤＢ５７０には、ユーザへの課金情報、課金情報に応じて決定されるコンテンツの再生制限情報、ユーザ機器１００に送信した復号処理情報の履歴情報（復号履歴）の情報が記録される。
【００６８】
なお、サーバ５００の処理プログラム部５１０は専用のハードウェアにより実現されるものであってもよく、またこの処理プログラム部はメモリおよびＣＰＵ（中央処理装置）等の汎用の情報処理装置により構成され、この処理部の機能を実現するためのプログラム（図示せず）をメモリにロードして実行することによりその機能を実現させるものであってもよい。なお、このサーバ５００には、周辺機器として入力装置、表示装置等（いずれも図示せず）が接続され又は内蔵されているものとする。ここで、入力装置としては、キーボード、マウス等の入力デバイスのことをいう。表示装置とは、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）や液晶表示装置等のことをいう。
【００６９】
また、図２２に示すユーザ機器１００内の処理プログラム部１６０、および図２３に示すサーバ５００内の処理プログラム部５１０の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより、図２２に示すユーザ機器１００内の処理プログラム部１６０、および図２３に示すサーバ５００内の処理プログラム部５１０に必要な処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや、周辺機器等のハードウェアを含むものとする。
【００７０】
また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可般媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。
さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの（伝送媒体ないしは伝送波）、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。
また上記プログラムは、前述した機能の一部を実現するためのものであってもよく、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。
【００７１】
以上、本発明の実施の形態について説明したが、本発明のユーザ機器、サーバ、コンテン

ツ流通システムは、上述の図示例にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

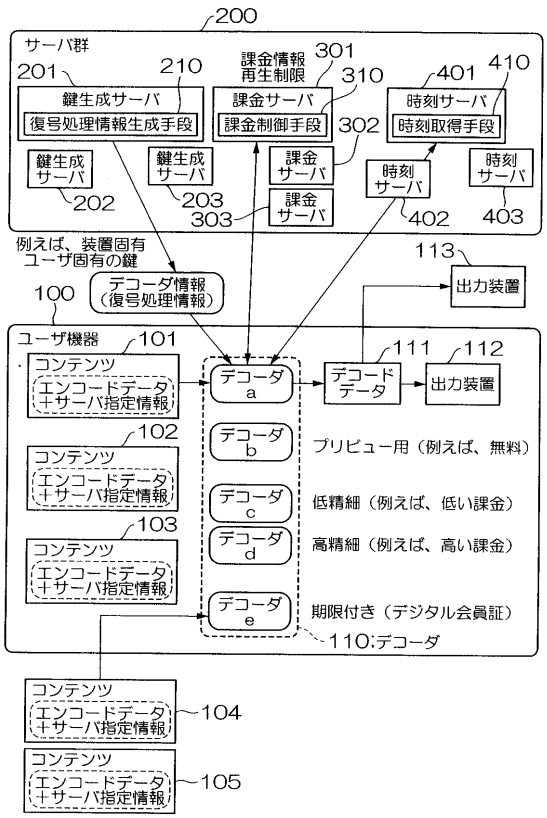
【図面の簡単な説明】

【図１】本発明のコンテンツ流通システムの概要を説明するための図。
【図２】ユーザ機器が有する手段の構成例を示す図。
【図３】ユーザ機器とサーバ群との相互作用を説明するための図その１。
【図４】ユーザ機器とサーバ群との相互作用を説明するための図その２。
【図５】ユーザ機器における復号処理を示すフローチャート。
【図６】プリビュー及び解像度制限を説明するための図。
【図７】ＪＰＥＧ２０００の処理を概説するための図。
【図８】周波数領域によるデータの例を示す図。
【図９】周波数成分の画像に与える影響を模式的に示した図。
【図１０】周波数データの全てを用いて復号した画像の例を示す図。
【図１１】異なる周波数成分により精細度を変化させる方法の説明図。
【図１２】再生制限に係る情報と符号化について説明するため図。
【図１３】復号処理に必要な機能及び要素をまとめて示した図。
【図１４】静止画を例としたプリビューの例を示す図。
【図１５】課金後処理が許されている場合の表示例を示す図。
【図１６】使用期限を過ぎた場合に表示される画面例を示す図。
【図１７】許可されない装置により再生する場合の画面例を示す図。
【図１８】高解像度での再生が許可されない場合の画面例を示す図。
【図１９】使用回数制限を超過した場合に表示される画面例を示す図。
【図２０】ユーザにパスワードを求める画面例を示す図。
【図２１】ユーザ機器とサーバ群が接続されることを示す模式図。
【図２２】ユーザ機器の構成例を示すブロック図。
【図２３】サーバの構成例を示すブロック図。
【図２４】特許文献１の図１を示す図。
【図２５】特許文献２の図２を示す図。
【図２６】特許文献２の図１１を示す図。

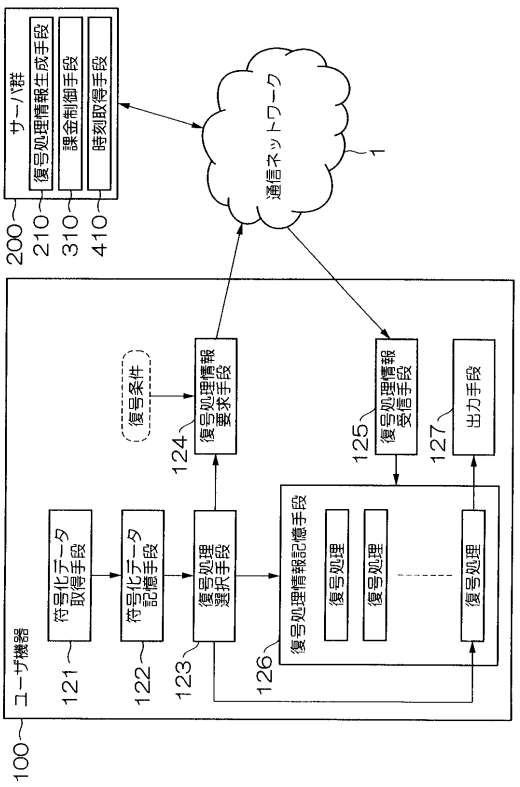
【符号の説明】

１００　ユーザ機器、１０１～１０５　符号化されたコンテンツ
１２１　符号化データ取得手段、１２２　符号化データ記憶手段
１２３　復号処理選択手段、１２４　復号処理情報要求手段
１２５　復号処理情報受信手段、１２６　復号処理情報記憶手段
１２７　出力手段、２０１　鍵生成サーバ、２１０　復号処理情報生成手段
３０１　課金サーバ、３１０　課金制御手段
４０１　時刻サーバ、４１０　時刻取得手段

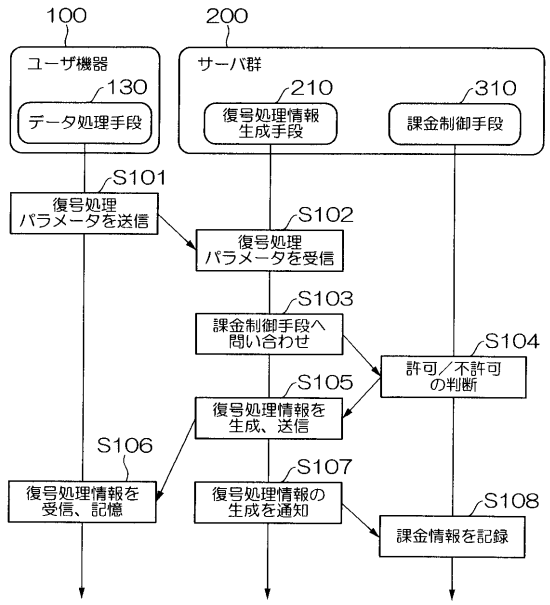
【図１】


200
サーバ群
201
210
課金情報再生制限
301
310
401
410
鍵生成サーバ
復号処理情報生成手段
課金サーバ
課金制御手段
302
時刻サーバ
時刻取得手段
鍵生成サーバ
202
鍵生成サーバ
203
課金サーバ
303
課金サーバ
時刻サーバ
402
時刻サーバ
403
例えば、装置固有ユーザ固有の鍵
113
出力装置
100
デコーダ情報（復号処理情報）
ユーザ機器
101
コンテンツ（エンコードデータ＋サーバ指定情報）
デコーダ a
デコードデータ
111
112
出力装置
102
コンテンツ（エンコードデータ＋サーバ指定情報）
デコーダ b
プリビュー用（例えば、無料）
103
コンテンツ（エンコードデータ＋サーバ指定情報）
デコーダ c
低精細（例えば、低い課金）
デコーダ d
高精細（例えば、高い課金）
デコーダ e
期限付き（デジタル会員証）
110:デコーダ
コンテンツ（エンコードデータ＋サーバ指定情報）
104
コンテンツ（エンコードデータ＋サーバ指定情報）
105

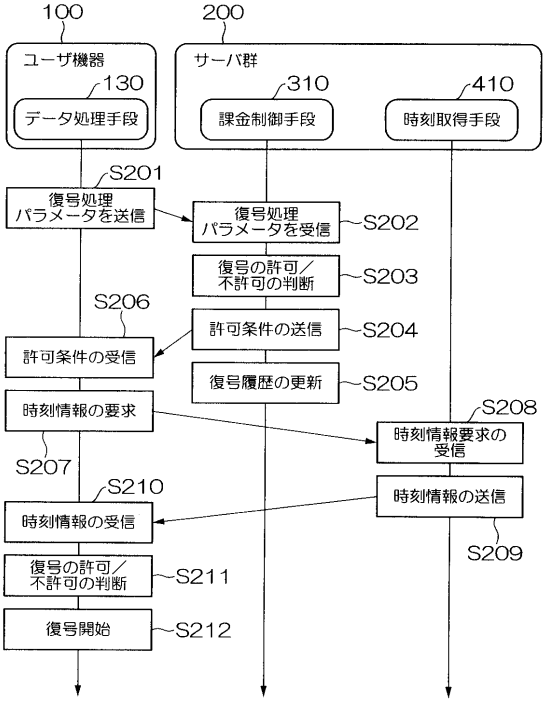
【図２】


サーバ群
復号処理情報生成手段
課金制御手段
時刻取得手段
通信ネットワーク
1
200
210
310
410
復号条件
復号処理情報要求手段
124
復号処理情報受信手段
125
出力手段
127
ユーザ機器
符号化データ取得手段
121
符号化データ記憶手段
122
復号処理選択手段
123
復号処理情報記憶手段
126
復号処理
復号処理
復号処理
100

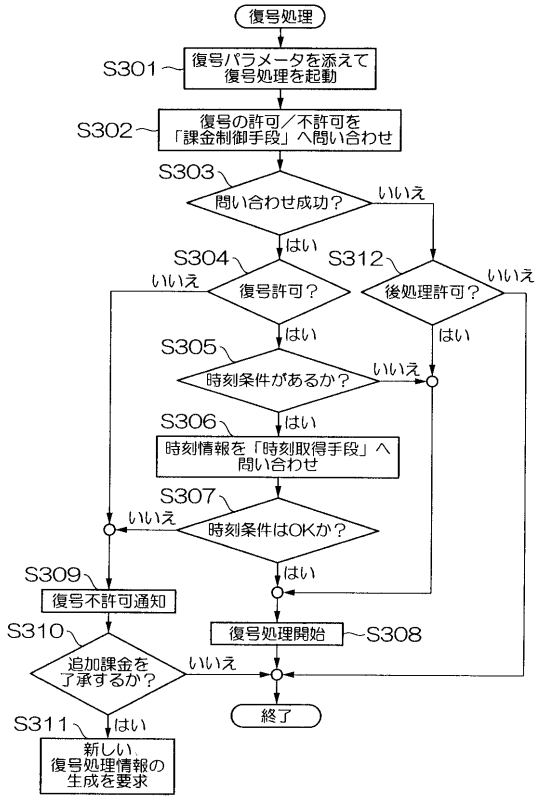
【図３】


100
200
ユーザ機器
130
データ処理手段
サーバ群
210
復号処理情報生成手段
310
課金制御手段
S101
復号処理パラメータを送信
S102
復号処理パラメータを受信
S103
課金制御手段へ問い合わせ
S104
許可／不許可の判断
S105
復号処理情報を生成、送信
S106
復号処理情報を受信、記憶
S107
復号処理情報の生成を通知
S108
課金情報を記録

【図４】

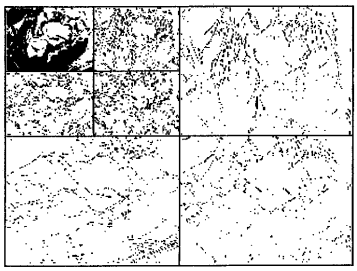

100
200
ユーザ機器
130
データ処理手段
サーバ群
310
課金制御手段
410
時刻取得手段
S201
復号処理パラメータを送信
復号処理パラメータを受信
S202
復号の許可／不許可の判断
S203
S206
許可条件の送信
S204
許可条件の受信
復号履歴の更新
S205
時刻情報の要求
S208
時刻情報要求の受信
S207
S210
時刻情報の送信
時刻情報の受信
S209
復号の許可／不許可の判断
S211
復号開始
S212

【図５】



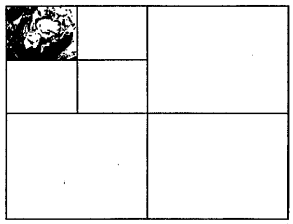
【図６】

【図７】

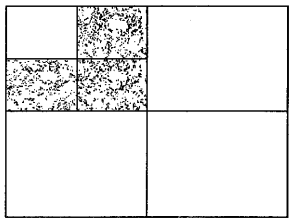


【図８】

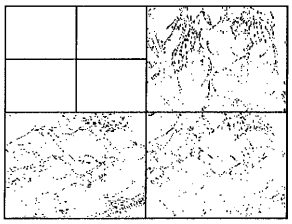
(a)



(b)



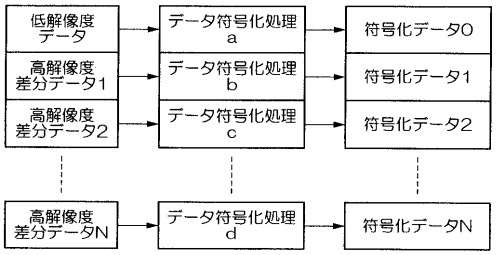
(c)



【図９】

【図１０】

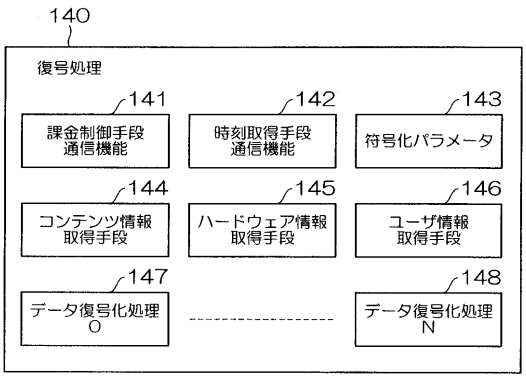
【図１１】



【図１２】

	条件A	条件B	条件C
コンテンツ制限	コンテンツ1	コンテンツ2から8	なし
ユーザ制限	UserID:1234	なし	UserID:5678
再生回数制限	なし	残り2回	なし
再生期限制限	なし	X年Y月Z日まで	X年Y月Z日まで
再生精度制限	なし	なし	なし
再生量制限	なし	先頭の1分のみ	なし
再生ハード制限	なし	なし	なし
課金後処理	許可	不許可	許可
復号処理生成手段	URI−1	URI−2	URI−3
課金処理手段	URI−4	URI−5	URI−6
時刻取得手段	なし	URI−7	URI−8
パラメータ符号化処理	X	Y	Z
符号化パラメータ	A	B	C

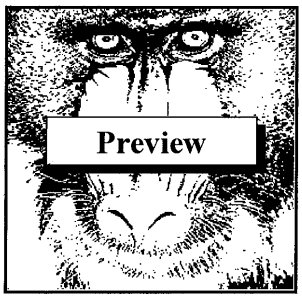
【図１３】



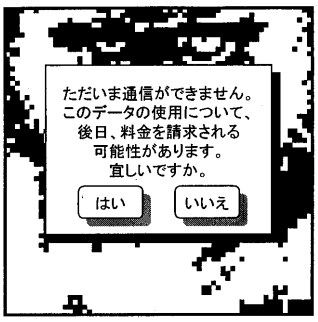
【図１４】

(a)

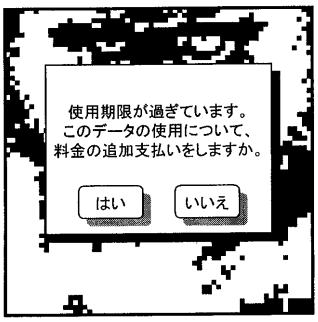
(b)



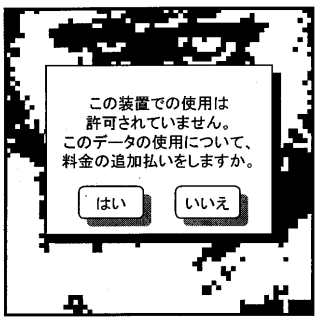
【図１５】



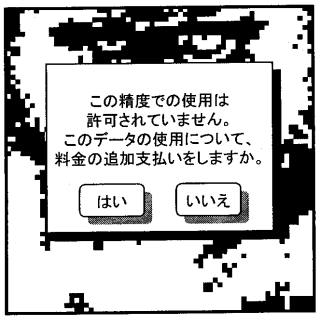
【図１６】



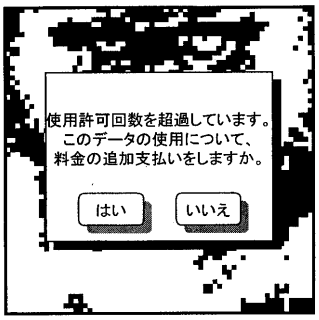
【図１７】



【図１８】

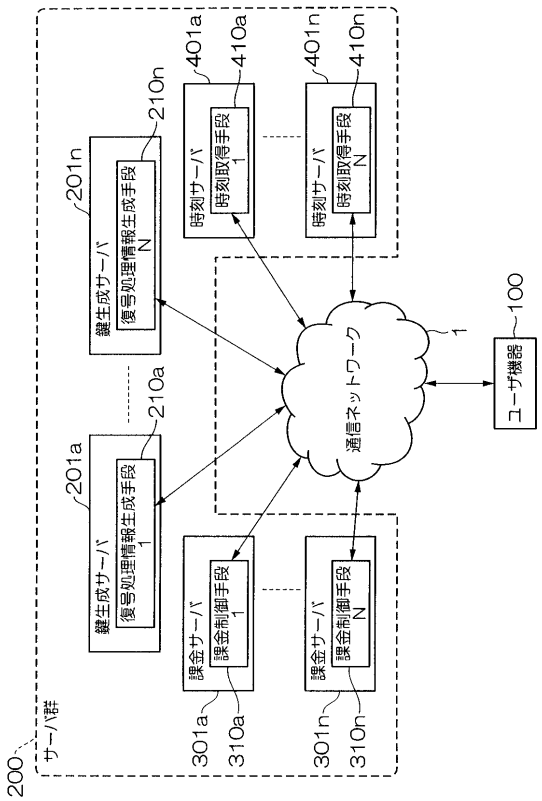


【図１９】

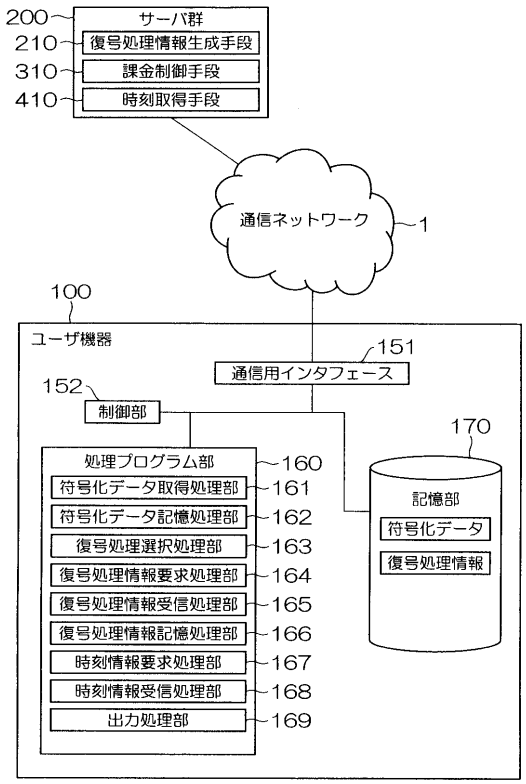


【図２０】

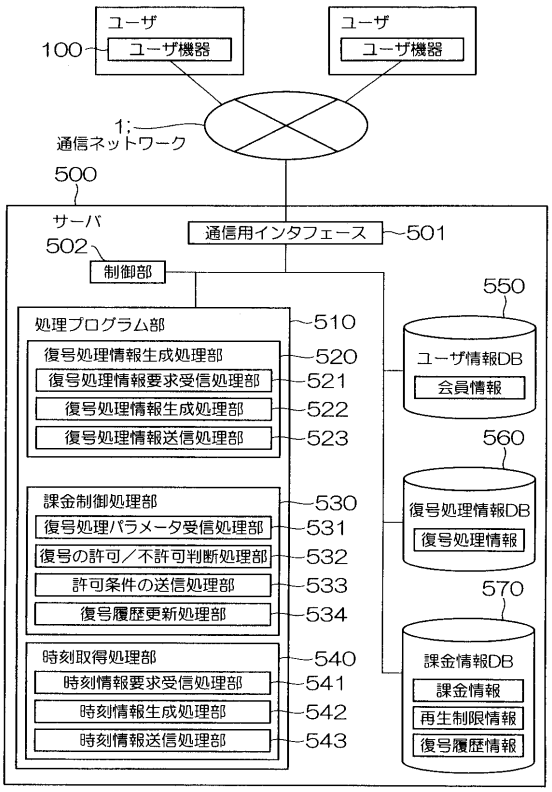
【図２１】



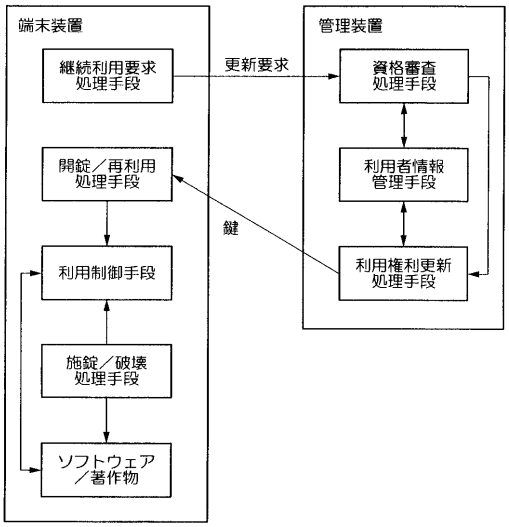
【図２２】



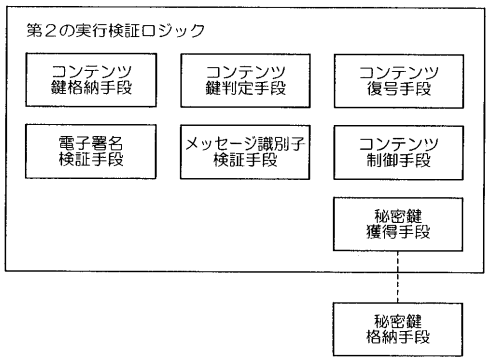
【図２３】



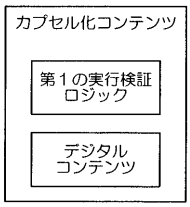
【図２４】



【図２６】



【図２５】



フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	Ｈ０４Ｎ 7/16	Ｃ	
	Ｈ０４Ｎ 7/173	６３０	
	Ｈ０４Ｌ 9/00	６０１Ｄ	

Ｆターム(参考) 5C064 BA01 BB01 BB02 BC01 BC16 BC20 BC22 BC23 BD02 BD03
BD04 BD08 BD09
5J104 AA13 AA16 EA04 EA15 MA05 NA02 PA07 PA11