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

特許第4030486号

(P4030486)

(45)発行日　平成20年1月9日(2008.1.9)　(24)登録日　平成19年10月26日(2007.10.26)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G06F 21/24	(2006.01)	H04L	9/00	601E
G06Q 50/00	(2006.01)	G06F	12/14	540A
		G06F	12/14	550A
		G06F	17/60	142

請求項の数 3　(全 52 頁)

(21)出願番号　特願2003-322109(P2003-322109)
(22)出願日　平成15年9月12日(2003.9.12)
(62)分割の表示　特願平7-228366の分割
　原出願日　平成7年9月5日(1995.9.5)
(65)公開番号　特開2004-72792(P2004-72792A)
(43)公開日　平成16年3月4日(2004.3.4)
　審査請求日　平成15年9月17日(2003.9.17)
(31)優先権主張番号　特願平6-237673
(32)優先日　平成6年9月30日(1994.9.30)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願平6-264199
(32)優先日　平成6年10月27日(1994.10.27)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願平6-269959
(32)優先日　平成6年11月2日(1994.11.2)
(33)優先権主張国　日本国(JP)

(73)特許権者　505269423
インターシア　ソフトウェア　エルエルシー
アメリカ合衆国，８９１１９　ネバダ州，ラスベガス，スイート　５，ルネサンス　ドライヴ　２２１５－ビー
(74)代理人　100083839
弁理士　石川　泰男
(72)発明者　斉藤　誠
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内
(72)発明者　籾木　隼一
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内

最終頁に続く

(54)【発明の名称】端末装置、ディジタルキャッシュ管理システム

(57)【特許請求の範囲】

【請求項１】

データベースからユーザに暗号化データとして供給されるデータの著作権を管理する、そのような著作権管理システムと通信する端末装置であって、

前記著作権管理システムから第１秘密鍵の交付を受ける手段と、

ネットワーク、人工衛星、または記憶媒体を経由して暗号化データの供給を受ける手段と、

前記暗号化データが表示される場合に、前記第１秘密鍵を用いて暗号化データを復号データに復号する手段と、

前記著作権管理システムから供給された著作権管理プログラムにより第２秘密鍵を生成する手段と、

前記第２秘密鍵を用いてその表示されたデータを再暗号化データへ暗号化する手段とから構成される端末装置であって、

前記端末装置の１次ユーザ情報を前記著作権管理システムへ提示して前記データの利用を要求する手段と、

前記再暗号化データに前記１次ユーザ情報を付加する手段と、

を更に備える端末装置であって、

前記復号する手段または前記暗号化する手段は、著作権管理プログラムを実行するマイクロプロセッサにより構成され、

２次ユーザとして再暗号化データを利用する場合に、前記再暗号化データに付加された

前記１次ユーザ情報を提示して前記著作権管理システムに再暗号化データの利用を要求する手段と、
前記著作権管理システムから第２秘密鍵を受け取る手段と、
前記第２秘密鍵、２次ユーザ情報、前記著作権管理プログラムの使用頻度のいずれか一つあるいはいくつかに基づいて第３秘密鍵を生成する手段と、を更に備え、
前記再暗号化データが表示または加工される場合に、前記復号する手段は、前記第２秘密鍵を用いて再暗号化データを復号し、
前記表示または加工されたデータが、保存、コピーまたは転送される場合に、前記暗号化する手段は、前記表示または加工されたデータを前記第３秘密鍵を用いて再暗号化し、
前記付加する手段は、前記再暗号化されたデータに前記２次ユーザ情報を付加する端末装置。

【請求項２】
データベースからユーザに暗号化データとして供給されるデータの著作権を管理する、そのような著作権管理システムと通信する端末装置であって、
前記著作権管理システムから第１秘密鍵の交付を受ける手段と、
ネットワーク、人工衛星、または記憶媒体を経由して暗号化データの供給を受ける手段と、
前記暗号化データが加工される場合に、前記第１秘密鍵を用いて暗号化データを復号データに復号する手段と、
前記著作権管理システムから供給された著作権管理プログラムにより第２秘密鍵を生成する手段と、
前記第２秘密鍵を用いてその加工されたデータを再暗号化データへ暗号化する手段と
から構成される端末装置であって、
前記端末装置の１次ユーザ情報を前記著作権管理システムへ提示して前記データの利用を要求する手段と、
前記再暗号化データに前記１次ユーザ情報を付加する手段と、
を更に備える端末装置であって、
前記復号する手段または前記暗号化する手段は、著作権管理プログラムを実行するマイクロプロセッサにより構成され、
２次ユーザとして再暗号化データを利用する場合に、前記再暗号化データに付加された前記１次ユーザ情報を提示して前記著作権管理システムに再暗号化データの利用を要求する手段と、
前記著作権管理システムから第２秘密鍵を受け取る手段と、
前記第２秘密鍵、２次ユーザ情報、前記著作権管理プログラムの使用頻度のいずれか一つあるいはいくつかに基づいて第３秘密鍵を生成する手段と、を更に備え、
前記再暗号化データが表示または加工される場合に、前記復号する手段は、前記第２秘密鍵を用いて再暗号化データを復号し、
前記表示または加工されたデータが、保存、コピーまたは転送される場合に、前記暗号化する手段は、前記表示または加工されたデータを前記第３秘密鍵を用いて再暗号化し、
前記付加する手段は、前記再暗号化されたデータに前記２次ユーザ情報を付加する端末装置。

【請求項３】
前記第２秘密鍵を生成する手段は、前記第１秘密鍵、前記１次ユーザ情報、前記著作権管理プログラムの使用頻度のいずれか一つあるいはいくつかに基づいて生成する、請求項１乃至２のうちいずれか１項に記載の端末装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明はディジタルデータの利用，保存，複写，加工，転送において著作権を管理するシステムに係るものであり、特にマルチメディアシステムに対して用いることを考慮したも

のである。

【背景技術】

【０００２】

情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム２値データであり、自然画及び動画のような情報量が格段に多いデータを取扱うことができなかった。

【０００３】

ところで、各種電気信号のディジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた２値データ以外の画像信号もディジタル処理技術の開発が進められている。この画像信号のディジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をディジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【０００４】

画像データは、文字データ及び音声データと比較して圧倒的に情報量が多いため、そのままでは保存，転送あるいはコンピュータにおける各種の処理が困難である。そのため、これらの画像データを圧縮／伸張することが考えられ、いくつかの画像データ圧縮／伸張用の規格が作成されてきた。その中で、共通の規格としてこれまでに静止画像用のＪＰＥＧ（Joint Photographic image coding ExpertsGroup）規格，テレビジョン会議用のＨ．２６１規格，画像蓄積用のＭＰＥＧ１（Moving Picture image coding Experts Group 1）規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するＭＰＥＧ２規格が作成された。これらの技術により、ディジタル映像データのリアルタイム処理が可能となってきている。

【０００５】

従来広く普及しているアナログデータは保存，複写，加工，転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、ディジタルデータは保存，複写，加工，転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、ディジタルデータの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもディジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【０００６】

データベースの利用法は単にその内容を参照するだけでなく、通常は得たデータを保存，複写，加工することによって有効活用し、加工したデータを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオンラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログデータである音声データ及び画像データがディジタル化されてデータベースとされる。

【０００７】

このような状況において、データベース化されたデータの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写，加工，転送等の２次利用について完成された著作権管理手段はない。本発明者らは特願平６－４６４１９号及び特開平６－１４１００４号で公衆電信電話回線を通じて鍵管理センタから利用許可鍵を入手することによって著作権管理を行うシステムを、特開平６－１３２９１６号でそのための装置を提案した。

【０００８】

また、特願平６－６４８８９号において、これらの上記先願発明をさらに発展させることによって、ディジタル映像のリアルタイム送信も含むデータベースシステムにおけるディジタルデータの表示（音声化を含む），保存等の１次利用及び複写，加工，転送等の２次利用における著作権管理方法を提案した。

【０００９】

この先願のデータベース著作権管理システムは、著作権の管理を行うために、申し込まれた利用形態に対応した利用許可鍵の他に、著作権を管理するためのプログラム，著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を用いる。

【００１０】

著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【００１１】

著作権管理プログラム，著作権情報及び著作権管理メッセージは、各々利用許可鍵とともに全体が供給される場合、データとともに全体が供給される場合及び一部が利用許可鍵とともに供給され、一部がデータとともに供給される場合がある。データ，利用許可鍵，著作権管理メッセージ、著作権情報及び著作権管理プログラムには、暗号化された状態で送信されるが利用時には暗号が解かれる場合、暗号化された状態で送信され表示の際のみに暗号が解かれその他の場合は暗号化された状態である場合、全く暗号化されない場合、の三つの場合がある。

【発明の開示】

【発明が解決しようとする課題】

【００１２】

（発明の概要）本願においては先願である上記特願平６－６４８８９号において提案されたデータ著作権管理方法を、具体的にしたデータ著作権管理システムを提供する。

【課題を解決するための手段】

【００１３】

本発明においては、データ著作権管理システムを原データを保管するデータベース、暗号鍵を管理する鍵管理センタ、データ著作権を管理する著作権管理センタ及びこれらを相互に接続する通信ネットワークから構成し、データベースからユーザに供給されるデータは暗号化して配布され、ユーザは鍵管理センタあるいは著作権管理センタから入手した暗号鍵を用いて暗号化データを復号化して利用する。ユーザへのデータ供給は暗号化データを放送等により一方向的に供給する方法と、暗号化データをユーザの要求に応じて双方向的に供給する方法がある。

【００１４】

データの暗号化に用いられる暗号鍵システムには秘密鍵システム、公開鍵システムあるいは秘密鍵と公開鍵を組み合わせたシステムが採用され、さらにデータ著作権を管理する著作権管理プログラムが採用される。

【００１５】

ユーザがデータを保存、複写あるいは転送する場合には、鍵が鍵管理センタあるいは著作権管理センタから供給される場合と、著作権管理プログラムによって生成される場合がある。

【００１６】

また、本発明は単一のデータだけではなく単一のデータベースから供給された複数のデータあるいは複数のデータベースから供給された複数のデータを利用する場合のデータ著作権管理システムにも適用可能である。また、あわせてデータ著作権管理を行うためにユーザ側で使用する装置についても提案する。

【発明を実施するための最良の形態】

【００１７】

（実施例）以下、本発明について説明するが初めに暗号技術について一般的な説明をして

おく。暗号技術には、秘密鍵暗号方式（secret-key cryptosystem）と、公開鍵暗号方式（public-key cryptosystem）がある。秘密鍵暗号方式は、暗号化と復号化に同じ暗号鍵を使用する暗号方式であり、暗号化及び復号化に要する時間が短い反面、秘密鍵が発見され暗号が解読（Cryptanalize）されてしまうことがある。一方、公開鍵暗号方式は暗号化用の鍵が公開鍵（public-key）として公開されており、復号化用の鍵が公開されていない暗号鍵方式であり、暗号化用の鍵は公開鍵と呼ばれ、復号化用の鍵は専用鍵（private-key）と呼ばれる。この暗号方式を使用するには、情報を発信する側は暗号を受信する側の公開鍵で暗号化（encrption）し、情報を受信する側は公開されていない専用鍵で復号化（decryption）する暗号方式であり、暗号化及び復号化に要する時間が長い反面、専用鍵を発見することが殆ど不可能であり暗号の解読が非常に困難である。

【００１８】

暗号技術においては平文（plaintext）Ｍを暗号鍵（cryption key）Ｋを用いて暗号化し暗号文（cryptgram）Ｃを得る場合をＣ＝Ｅ（Ｋ，Ｍ）
と表現し、暗号文Ｃを暗号鍵Ｋを用いて復号し平文Ｍを得る場合をＭ＝Ｄ（Ｋ，Ｃ）
と表現する。本発明において使用される暗号方式には、暗号化と復号化に同じ秘密鍵Ｋｓが使用される秘密鍵方式（secret-key system）と、平文の暗号化に公開鍵（public key）Ｋbが使用され、暗号文の復号化に専用鍵（private-key）Ｋvが使用される公開鍵方式（public-key system）が採用される。

【００１９】

［実施例１］図１に示されたのは、本願発明に係るデータベース著作権管理システムの第１の実施例であり、この実施例１においては暗号鍵方式として秘密鍵方式が採用される。この図に示す実施例において、１はテキストデータ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ，ディジタル音声データ，ディジタル映像データが暗号化された状態で格納されたデータベースであり、２は通信・放送衛星等の人工衛星、３はＣＤ－ＲＯＭあるいはフレキシブルディスク等のデータ記録装置、８は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワーク、４は１次ユーザ端末装置である。また、９は秘密鍵を管理する鍵管理センタ、１０はデータベース著作権を管理する著作権管理センタである。

【００２０】

５，６及び７は各々２次ユーザ端末装置，３次ユーザ端末装置及びｎ次ユーザ端末装置であり、１１，１２及び１３は各々フレキシブルディスクあるいはＣＤ－ＲＯＭ等の記憶媒体である２次ディスク，３次ディスク及びｎ次ディスクである。なお、このｎは任意の整数でありｎが４よりも大きい場合には３次ユーザ端末装置６とｎ次ユーザ端末装置７の間及び３次ディスク１２とｎ次ディスク１３との間には対応するユーザ端末装置及びディスクが配置されている。

【００２１】

これらのうちデータベース１、鍵管理センタ９、著作権管理センタ１０、１次ユーザ端末装置４、２次ユーザ端末装置５、３次ユーザ端末装置６及びｎ次ユーザ端末装置７は通信ネットワーク８に接続されている。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、１点鎖線で示された経路は各データベースからの利用形態に対応した許可情報とともに秘密鍵が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録をしておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に著作権管理プログラムを動作させるためのプログラムが含まれている。

【００２２】

データベース１あるいはデータ記録装置３に格納されているテキストデータ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ，ディジタル音声データ，ディジタル映像データである原データＭ0が通信ネットワーク８、人工衛

星２あるいは記憶媒体３を経由して１次ユーザ端末装置４に一方向的に供給されるが、このときには第１秘密鍵Ｋs1を用いて暗号化される。
Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）
なお、広告付等の無料で提供されるデータの場合でも著作権保護のためには、暗号化を必要とする。

【００２３】
前に述べた先願である特願平６－６４８８９号には、データの利用形態には、最も基本的な表示の他に保存，加工，コピー，転送があり、利用許可鍵はこれらの利用形態のうちの１つあるいは複数に対応するものが用意され、その管理は著作権管理プログラムによって実行されることが示されている。また、データの表示及び加工のための表示以外の利用形態すなわちデータが保存，コピー，転送される場合には著作権管理プログラムによりデータが再暗号化されることが述べられている。いいかえれば、著作権が主張されたデータは暗号化された状態で流通し、平文化されるのは著作権処理機能を有するユーザ端末装置において、表示あるいは加工のための表示が行われるときのみである。

【００２４】
この実施例では、これら先願に記載された事項を利用する。供給された暗号化データＣm0ks1の１次利用を希望する１次ユーザは鍵管理センタ９に対して１次ユーザ端末装置４を利用し通信ネットワーク８を経由して原データ名あるいは原データ番号等を指定することにより暗号化原データＣm0ks1の１次利用申込を行うが、このときに１次ユーザに関する情報Iu1を鍵管理センタ９に提示する。１次ユーザ端末装置４を利用しての１次利用申込を受けた鍵管理センタ９は、著作権管理プログラムPとともに１次ユーザがデータベース１から入手した暗号化原データＣm0ks1を復号化するための第１秘密鍵Ｋs1及び復号された原データＭ0あるいは原データを加工して得られた加工データＭ1を再暗号化するための第２秘密鍵Ｋs2を通信ネットワーク８を経由し１次ユーザ端末装置４に転送する。

【００２５】
復号鍵である第１秘密鍵Ｋs1，暗号化／復号化鍵である第２秘密鍵Ｋs2を受け取った１次ユーザ端末装置４において、初めに著作権管理プログラムＰを利用して第１秘密鍵Ｋs1を用いて暗号化原データＣm0ks1を復号化しＭ0＝Ｄ（Ｋs1，Ｃm0ks1）
復号化された原データＭ0をそのままあるいは加工データＭ1として利用する。

【００２６】
原データＭ0あるいは加工データＭ1であるデータＭが１次ユーザ端末装置４の内部、すなわちメモリあるいは内蔵のハードディスクドライブに保存されている状態ではそのデータを利用することができるのは１次ユーザのみであるが、データＭがフレキシブルディスク等の外部記憶媒体１１にコピーされた場合、あるいは通信ネットワーク８を経て２次ユーザ端末装置５に転送された場合には、２次利用による著作権の問題が生じる。

【００２７】
また、１次ユーザが入手した原データＭ0をそのまま複写して２次ユーザに供給した場合にはその原データＭ0に何等の改変も加えられていないため、そのデータＭ0に１次ユーザの著作権は発生しない。しかし、１次ユーザが入手したデータＭ0を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータＭ1を作成した場合にはそのデータＭ1に１次ユーザの著作権（２次的著作権 secondarily exploitation right）が発生する。同様に、２次ユーザが１次ユーザから入手した原データＭ0あるいは加工データＭ1を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータＭ2を作成した場合には、同様に２次ユーザの著作権が発生する。

【００２８】
この著作権の問題に対処するため、この実施例においてはデータＭの保存、コピー、転送が行われるときには著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いてデータＭが暗号化され、以後１次ユーザ端末装置４においては第２秘密鍵Ｋs2を用いてデータＭの復号化及び暗号化が行われる。

Ｃmks2＝Ｅ（Ｋs2，Ｍ）
Ｍ＝Ｄ（Ｋs2，Ｃmks2）
なお、１次ユーザがデータの表示及び加工を行い加工データを得ることは原則として自由にできるが、その場合は著作権管理プログラムによってその回数に制限を設けることができる。

【００２９】
外部記憶媒体１１にデータＭがコピーされたとき及び通信ネットワーク８を経てデータが転送されたときには１次ユーザ端末装置４内の第１秘密鍵Ｋs1及び第２秘密鍵Ｋs2は著作権管理プログラムＰによって廃棄される。したがって、１次ユーザが再度データＭを利用する場合には鍵管理センタ９に利用申込を行い、第２秘密鍵Ｋs2の再交付を受ける必要がある。この第２秘密鍵Ｋs2の再交付を受けたことは、データＭが外部記憶媒体１１へコピーあるいは通信ネットワーク８を経由しての２次ユーザ端末装置５へ転送されることによる２次利用が行われたことを意味するから、このことが鍵管理センタ９から著作権管理センタ１０に登録され、以後の２次利用が可能になる。

【００３０】
１次ユーザ端末装置４からの２次ユーザ端末装置５へのデータＭの移動は外部記憶媒体１１によってあるいは通信ネットワーク８により行われ、外部記憶媒体１１へのコピーあるいは通信ネットワーク８を経由して移動が行われるときには、第２秘密鍵Ｋs2を用いてデータＭが暗号化される。

【００３１】
外部記憶媒体１１にデータＭがコピーされたとき及び通信ネットワーク８を経てデータＭが転送されたときに１次ユーザ端末装置４内の第１秘密鍵Ｋs1及び第２秘密鍵Ｋs2は廃棄されるが、このときに１次ユーザ端末装置４内に保存されている暗号化データＣmks2に、暗号化されていない１次ユーザ情報Ｉu1が付加され、暗号化データＣmks2を２次ユーザに転送する際に１次ユーザ情報Ｉu1も転送される。

【００３２】
１次ユーザからコピーあるいは転送された暗号化データＣmks2の２次利用を希望する２次ユーザは、２次ユーザ端末装置５を利用して通信ネットワーク８を経由して著作権管理センタ１０に対して原データ名あるいは原データ番号を指定するとともに２次ユーザ情報Ｉu2を提示して２次利用申込を行うが、そのときに１次ユーザとの関係を明確にするために暗号化データＣmks2に付加されている暗号化されていない１次ユーザ情報Ｉu1も提示する。著作権管理センタ１０は、提示された１次ユーザ情報Ｉu1に基づきその１次ユーザがそのデータを２次利用するために第２秘密鍵Ｋs2の再交付を受けていることを確認し、復号化鍵である第２秘密鍵Ｋs2，暗号化／復号化鍵である第３秘密鍵Ｋs3を通信ネットワーク８を経由して２次ユーザ端末装置５に転送する。第２秘密鍵Ｋs2，第３秘密鍵Ｋs3を受け取った２次ユーザ端末装置５において、著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化データＣmks2が復号化されＭ＝Ｄ（Ｋs2，Ｃmks2）
表示あるいは加工の２次利用が行われる。

【００３３】
この実施例においては、１次利用申込は鍵管理センタ９が処理し、２次利用申込は著作権管理センタ１０が処理する。また、１次ユーザが供給されるデータＭは第１秘密鍵Ｋs1を用いて暗号化されているが、２次ユーザが供給されるデータＭは第２秘密鍵Ｋs2を用いて暗号化されている。一方、１次ユーザに対して鍵管理センタ９からは暗号鍵として第１秘密鍵Ｋs1及び第２秘密鍵Ｋs2が転送される。そのため、２次ユーザが１次ユーザであると偽って鍵管理センタ９に対して１次利用申込を行った場合には復号化鍵として第１秘密鍵Ｋs1が，暗号化／復号化鍵として第２秘密鍵Ｋs2が転送される。しかし、復号化鍵として転送された第１秘密鍵Ｋs1を用いて暗号化データＣmks2を復号することはできない。したがって、データの利用について虚偽の申込を行うことは不可能であり、その結果データの原著作権だけでなく、データについての１次ユーザの著作権も保護される。

【００３４】

２次ユーザ端末装置５においてデータＭの表示及び加工のための表示以外の利用形態である保存，コピー，転送が行われるときには著作権管理プログラムＰによって第３秘密鍵Ｋs3を用いてデータＭの暗号化が行われ、以後第３秘密鍵Ｋs3を用いてデータの復号及び暗号化が行われる。

Ｃmks3＝Ｅ（Ｋs3，Ｍ）

Ｍ＝Ｄ（Ｋs3，Ｃmks3）

なお、２次ユーザが表示及び加工を行い加工データＭ2を得ることも原則として自由にできるが、その場合は著作権管理プログラムＰによってその回数に制限を設けることができる。

【００３５】

外部記憶媒体１２にデータＭがコピーされたとき及び通信ネットワーク８を経てデータが転送されたときには２次ユーザ端末装置５内の第２秘密鍵Ｋs2及び第３秘密鍵Ｋs3は著作権管理プログラムＰによって廃棄される。したがって、２次ユーザが再度データＭを利用する場合には著作権管理センタ１０に利用申込を行い、第３秘密鍵Ｋs3の再交付を受ける必要がある。この第３秘密鍵Ｋs3の再交付を受けたことは、データＭが外部記憶媒体１２へコピーあるいは通信ネットワーク８を経由しての３次ユーザ端末装置６へ転送されることによる２次利用が行われたことを意味するから、このことが著作権管理センタ１０に登録され、以後の利用が可能になる。

【００３６】

２次ユーザ端末装置５からの３次ユーザ端末装置６へのデータＭの移動は外部記憶媒体１２によってあるいは通信ネットワーク８により行われ、外部記憶媒体１２へのコピーあるいは通信ネットワーク８を経由して移動が行われるときには、第３秘密鍵Ｋs3を用いてデータＭが暗号化される。

【００３７】

外部記憶媒体１２にデータＭがコピーされたとき及び通信ネットワーク８を経てデータＭが３次ユーザ端末装置６に転送されたときに２次ユーザ端末装置５内の第２秘密鍵Ｋs2及び第３秘密鍵Ｋs3は廃棄されるが、このときに２次ユーザ端末装置５内に保存されている暗号化データＣmks3に、暗号化されていない２次ユーザ情報Ｉu2が付加される、暗号化データＣmks3を３次ユーザに転送する際に２次ユーザ情報Ｉu2も転送される。この場合、各ユーザ情報のデータへの付加は、全てのユーザ情報がコピーあるいは転送の度にデータに付加される場合と、その度に最新のものに書き換えられる履歴が著作権管理センタに保管される場合がある。

【００３８】

２次ユーザからコピーあるいは転送された暗号化データＣmks3の３次利用を希望する３次ユーザは、３次ユーザ端末装置６を利用して通信ネットワーク８を経由して著作権管理センタ１０に対して原データ名あるいは原データ番号を指定するとともに３次ユーザ情報Ｉu3を提示して３次利用申込を行うが、そのときに２次ユーザとの関係を明確にするために暗号化データＣmks3に付加されている暗号化されていない２次ユーザ情報Ｉu2も提示する。著作権管理センタ１０は、提示された２次ユーザ情報Ｉu2に基づきその２次ユーザがそのデータを３次利用するための準備手続き、すなわち第３秘密鍵Ｋs3の再交付を受けていることを確認し、復号化鍵である第３秘密鍵Ｋs3，暗号化／復号化鍵である第４秘密鍵Ｋs4を通信ネットワーク８を経由して３次ユーザ端末装置６に転送する。第３秘密鍵Ｋs3、第４秘密鍵Ｋs4を受け取った３次ユーザ端末装置６において、著作権管理プログラムＰにより第３秘密鍵Ｋs3を用いて暗号化データＣmks3が復号化されＭ＝Ｄ（Ｋs3，Ｃmks3）表示あるいは加工の３次利用が行われる。

【００３９】

この実施例においては、１次ユーザが供給されるデータＭは第１秘密鍵Ｋs1を用いて暗号化され、２次ユーザが供給されるデータＭは第２秘密鍵Ｋs2を用いて暗号化されているが、３次ユーザが供給されるデータＭは第３秘密鍵Ｋs3を用いて暗号化されている。そのため、３次ユーザが１次ユーザであると偽って鍵管理センタ９に対して１次利用申込を行っ

た場合には復号化鍵として第１秘密鍵Ｋs1が，暗号化／復号化鍵として第２秘密鍵Ｋs2が転送される。しかし、復号化鍵として転送された第１秘密鍵Ｋs1を用いて暗号化データＣmks3を復号化することはできない。また、３次ユーザが２次ユーザであると偽って著作権管理センタ９に対して２次利用申込を行った場合には復号化鍵として第２秘密鍵Ｋs2が，暗号化／復号化鍵として第３秘密鍵Ｋs3が転送される。しかし、復号化鍵として転送された第２秘密鍵Ｋs2を用いて暗号化Ｃmks3を復号することはできない。したがって、データの利用について虚偽の申込を行うことは不可能であり、その結果データの原著作権だけでなく、データについての１次ユーザの著作権及び２次ユーザの著作権も保護される。以下、同様の手続きが４次以降の利用にも適用される。

【００４０】

以上説明した実施例におけるデータベース１，鍵管理センタ９，著作権管理センタ１０は別個に設置されているが、これらは必ずしも別個のものである必要はなく、これらの全てあるいは適当な２つを一体に設置することも可能である。また、１次ユーザからの２次暗号鍵再交付申込は実施例のように鍵管理センタ９に対して行うのではなく著作権管理センタ１０に対して行うようにしてもよい。

【００４１】

［実施例２］次に、実施例２について説明するが、この実施例の大部分の構成は実施例１の構成と同様であるが、著作権管理プログラム、場合によってはさらに第１秘密鍵と第２秘密鍵が、暗号化されて供給される。この実施例でも第１実施例と同様に原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。なお、実施例２で用いるシステム構成は図１に示された実施例１のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【００４２】

この実施例において、データベース１に格納されている原データＭ0が人工衛星２，記憶媒体３あるいは通信ネットワーク８を経由して１次ユーザ端末装置４に一方向的に供給されるが、そのときには第１秘密鍵Ｋs1を用いて暗号化される。

Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）

【００４３】

供給された暗号化データＣm0ks1の１次利用を希望する１次ユーザは鍵管理センタ９に対して１次ユーザ端末装置４を利用し通信ネットワーク８を経由して原データ名あるいは原データ番号等を指定することにより暗号化原データＣm0ks1の１次利用申込を行うが、このときに１次ユーザ情報Ｉu1を鍵管理センタ９に提示する。

【００４４】

暗号化原データＣm0ks1の１次利用申込を受けた鍵管理センタ９は、１次ユーザ情報Ｉu1を利用して１次ユーザ専用の秘密鍵Ｋsu1を生成し著作権管理センタ１０に転送する。

【００４５】

１次ユーザ専用の秘密鍵Ｋsu1を受け取った著作権管理センタ１０は、この１次ユーザ専用秘密鍵Ｋsu1を用いて著作権管理プログラムＰを暗号化し、Ｃpksu1＝Ｅ（Ｋsu1，Ｐ）暗号化著作権管理プログラムＣpksu1を鍵管理センタ９に転送する。このようにして生成された暗号化著作権管理プログラムＣpksu1は１次ユーザに固有のものである。また、鍵管理センタ９は著作権管理センタ１０から受け取った暗号化著作権管理プログラムＣpksu1とともに復号化鍵である第１秘密鍵Ｋs1及び復号化／暗号化鍵である第２秘密鍵Ｋs2を通信ネットワーク８を経由し１次ユーザ端末装置４に転送する。

【００４６】

暗号化著作権管理プログラムＣpksu1，第１秘密鍵Ｋs1，第２秘密鍵Ｋs2を受け取った１次ユーザ端末装置４において、初めに予め配布されているデータベース組織用ソウフトウェアSが１次ユーザ情報Ｉu1に基づいて１次ユーザ専用秘密鍵Ｋsu1を生成し、Ｋsu1＝Ｓ（Ｉu1）

生成された１次ユーザ専用秘密鍵Ｋsu1を用いて暗号化著作権管理プログラムＣpsu1を復

号化し、Ｐ＝Ｄ（Ｋsu1，Ｃpsu1）
復号化された著作権管理プログラムＰを利用して第１秘密鍵Ｋs1を用いて暗号化原データＣm0ks1を復号化しＭ0＝Ｄ（Ｋs1，Ｃm0ks1）
復号化された原データＭ0をそのままあるいは加工データＭ1として利用する。
【００４７】
原データＭ0あるいは加工データＭ1であるデータＭの保存，コピー，転送が行われるときには著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いてデータＭが暗号化され、以後１次ユーザ端末装置４においては第２秘密鍵Ｋs2を用いてデータＭの復号化及び暗号化が行われる。
Ｃmks2＝Ｅ（Ｋs2，Ｍ）
Ｍ＝Ｄ（Ｋs2，Ｃmks2）
【００４８】
外部記憶媒体１１にデータＭがコピーされたとき及び通信ネットワーク８を経てデータが転送されたときには１次ユーザ端末装置４内の第１秘密鍵Ｋs1及び第２秘密鍵Ｋs2は著作権管理プログラムＰによって廃棄される。したがって、１次ユーザが再度データＭを利用する場合には鍵管理センタ９に利用申込を行い、第２秘密鍵Ｋs2の再交付を受ける必要がある。この第２秘密鍵Ｋs2の再交付を受けたことは、データＭが外部記憶媒体１１へコピーあるいは通信ネットワーク８を経由しての２次ユーザ端末装置５へ転送されることによる２次利用が行われたことを意味するから、このことが鍵管理センタ９から著作権管理センタ１０に登録され、以後の２次利用が可能になる。
【００４９】
１次ユーザ端末装置４からの２次ユーザ端末装置５へのデータＭの移動は外部記憶媒体１１によってあるいは通信ネットワーク８により行われる。データＭの外部記憶媒体１１へのコピーあるいは通信ネットワーク８を経由して転送が行われるときには、第２秘密鍵Ｋs2を用いてデータＭが暗号化される。
【００５０】
外部記憶媒体１１にデータＭがコピーされたとき及び通信ネットワーク８を経てデータＭが転送されたときに１次ユーザ端末装置４内の第１秘密鍵Ｋs1及び第２秘密鍵Ｋs2は廃棄されるが、このときに１次ユーザ端末装置４内に保存されている暗号化データＣmks2に、１次ユーザについての暗号化されていない情報Ｉu1が付加される。そのため、暗号化データＣmks2を２次ユーザに転送する際に１次ユーザ情報Ｉu1も転送される。
【００５１】
１次ユーザからコピーあるいは転送された暗号化データＣmks2の２次利用を希望する２次ユーザは、２次ユーザ端末装置５を利用して通信ネットワーク８を経由して著作権管理センタ１０に対して原データ名あるいは原データ番号を指定するとともに２次ユーザ情報Ｉu2を提示して２次利用申込を行うが、そのときに１次ユーザとの関係を明確にするために暗号化データＣmks2に付加されている暗号化されていない１次ユーザ情報Ｉu1も提示する。著作権管理センタ１０は、提示された１次ユーザ情報Ｉu1に基づきその１次ユーザがそのデータを２次利用するために第２秘密鍵Ｋs2の再交付を受けていることを確認し、提示された２次ユーザ情報Ｉu2に基づいて２次ユーザ専用の秘密鍵Ｋsu2を生成する。
【００５２】
著作権管理センタ１０はこの２次ユーザ専用秘密鍵Ｋsu2を用いて著作権管理プログラムＰを暗号化し、Ｃpksu2＝Ｅ（Ｋsu2，Ｐ）
暗号化著作権管理プログラムＣpksu2，復号化鍵である第２秘密鍵Ｋs2，暗号化／復号化鍵である第３秘密鍵Ｋs3を通信ネットワーク８を経由して２次ユーザ端末装置５に転送する。なお、この暗号化著作権管理プログラムＣpksu2に１次ユーザに関する情報Ｉu1を付加しておいてもよい。
【００５３】
第２秘密鍵Ｋs2，第３秘密鍵Ｋs3を受け取った２次ユーザ端末装置５において、データベース組織利用ソフトウェアが２次ユーザ情報Ｉu2に基づいて２次ユーザ専用秘密鍵Ｋsu2

を生成し、Ｋsu2＝Ｓ（Ｉu2）
生成された２次ユーザ専用秘密鍵Ｋsu2を用いて暗号化著作権管理プログラムＣpsu2を復号化し、Ｐ＝Ｄ（Ｋsu2，Ｃpsu2）
復号化された著作権管理プログラムＰを利用して第２秘密鍵Ｋs2を用いて暗号化原データＣmks2を復号化しＭ＝Ｄ（Ｋs2，Ｃmks2）
復号化されたデータＭをそのままあるいは加工して利用する。

【００５４】
このように、利用申込を行ったユーザのユーザ情報に基づいてユーザ専用暗号鍵を生成し、生成されたユーザ専用暗号鍵を用いて著作権管理プログラムを暗号化することにより、データ著作権管理システムの安全性が高くなる。また、このときにユーザに供給される各秘密鍵もユーザ専用暗号鍵を用いて暗号化すれば、データ著作権管理システムの安全性がより高くすることができる。

【００５５】
［実施例３］さらに、図１に示されたシステムにおいて、外部記憶媒体１１にデータＭがコピーされた場合、あるいは通信ネットワーク８を経てデータＭが転送された場合に生じる著作権の問題に対応するためのさらに別の方法として、１次ユーザ端末４の使用者が行う１次利用申込を表示許可，保存許可及び加工許可だけに限定しそれ以外の利用申込すなわちコピー許可及び転送許可を受けることはできず、コピー許可及び転送許可の申込は別に行うようにし、外部記憶媒体１１にデータＭがコピーされたとき及び通信ネットワーク８を経てデータが２次ユーザ端末装置５に転送されたときに、１次ユーザ端末装置４内の第１秘密鍵Ｋs1及び第２秘密鍵Ｋs2は廃棄されるようにすることもできる。このようにすれば、データＭのコピーあるいは転送をより確実に著作権管理センタ１０で把握することができる。

【００５６】
［実施例４］図２に示されたのは、本願発明に係るデータ著作権管理システムの実施例４の構成である。図１に示されたシステムでは、暗号化データが衛星２，記録媒体３あるいは通信ネットワーク８を経由して一方向的に供給されるが、実施例２では１次ユーザ４からの要求に応じて暗号化データが双方向的に供給される。また、この実施例においては、暗号鍵方式として公開鍵方式が採用される。なお、実施例２がデータ供給手段としてデータベース以外に広告付き等の無料の暗号化する必要の無い衛星放送，地上波放送，ＣＡＴＶ放送あるいは記録媒体を用いる場合にも適用可能なことは勿論のことである。

【００５７】
図１に示されたシステムと同様にこの図に示されたシステムにおいて、１はデータベース，４は１次ユーザ端末装置，５は２次ユーザ端末装置，６は３次ユーザ端末装置，７はｎ次ユーザ端末装置である。また、１４は２次著作権管理センタ，１５は３次著作権管理センタ，１６はｎ次著作権管理センタ，８は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワークである。

【００５８】
これらのうち、データベース１，１次ユーザ端末装置４，２次ユーザ端末装置５，３次ユーザ端末装置６，ｎ次ユーザ端末装置７，２次著作権管理センタ１４，３次著作権管理センタ１５，ｎ次著作権管理センタ１６は通信ネットワーク８に接続されており相互に接続可能である。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、１点鎖線で示された経路は各データベースからの利用形態に対応した許可情報とともに暗号鍵が転送される経路であり、２点鎖線で示された経路はデータベースあるいは各著作権管理センタデータベースから次位の著作権管理センタデータベースへ著作権情報が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録をしておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に暗号化された著作権管理プログラムを復号化するためのプログラムが含まれてい

る。
【００５９】
データベース１を利用するに当たり、１次ユーザは１次ユーザ認証データＡｕ１，第１公開鍵Ｋｂ１及び第１公開鍵Ｋb1に対応する第１専用鍵Ｋv1，第２公開鍵Ｋb2及び第２公開鍵Ｋb2に対応する第２専用鍵Ｋv2を用意し、１次ユーザ端末装置４を利用し通信ネットワーク８を経由してデータベース１にアクセスする。
【００６０】
１次ユーザから１次ユーザ認証データＡu1，第１公開鍵Ｋb1、第２公開鍵Ｋb2の転送を受けたデータベース１は、１次ユーザ認証データＡu1を確認し、確認された１次ユーザ認証データＡu1を１次ユーザ情報Ｉu1として２次著作権管理センタ１４に転送する。
【００６１】
一方、データベース１は２個の秘密鍵すなわち第１の秘密鍵Ｋs1と第２の秘密鍵Ｋs2を用意する。この２個の秘密鍵の用意は図１に示された実施例１の鍵センタ９を利用して行ってもよい。用意された第１の秘密鍵Ｋs1及び第２の秘密鍵Ｋs2中、第２の秘密鍵Ｋs2も予め著作権管理センタ１４に転送される。
【００６２】
これらの転送が行われた結果著作権管理センタ１４には１次ユーザ情報Ｉu1、原著作権情報Ｉc及び第２秘密鍵Ｋs2が格納される。なお、これらの中で原著作権情報Ｉcは著作権使用料金分配に用いられる。
【００６３】
データの利用を希望する１次ユーザは、１次ユーザ端末装置４を利用してデータベース１にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。
【００６４】
データメニューが転送されると１次ユーザはデータメニュー検索を行いデータＭを選択する。このとき、選択されたデータＭの原著作権情報Ｉcが著作権管理センタ１４に転送される。
【００６５】
１次ユーザの要求に応じてデータベース１から原データＭ0が読み出される。読み出された原データＭ0は第１秘密鍵Ｋs1で暗号化される。
Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）
この暗号化データＣm0ks1には暗号化されていない原著作権者情報Ｉcが付けられている。また、第１の秘密鍵Ｋs1を第１の公開鍵Ｋb1で、第２の秘密鍵Ｋs2を同じく第２の公開鍵Ｋb2で暗号化する。
Ｃks1kb1＝Ｅ（Ｋb1，Ｋs1）
Ｃks2kb2＝Ｅ（Ｋb2，Ｋs2）
併せて著作権管理プログラムＰも第２の秘密鍵Ｋs2で暗号化されるが、Ｃpks2＝Ｅ（Ｋs2，Ｐ）
著作権管理プログラムＰの暗号化は第２の秘密鍵Ｋs2で暗号化されなければならないものではなく、他の適当な暗号鍵を用いて暗号化することができる。暗号化原データＣm0ks1，暗号化著作権管理プログラムＣpks2及び２個の暗号化秘密鍵Ｃks1kb1，Ｃks2kb2が通信ネットワーク８を経由して１次ユーザ端末装置４に転送される。このときに必要ならば課金が行われる。なお、暗号化著作権管理プログラムＣpks2はデータベース１から供給されるのではなく、ユーザ端末装置４内の例えばＲＯＭに内蔵しておくことも可能である。
【００６６】
データベース１から暗号化原データＣm0ks1，２個の暗号化秘密鍵Ｃks1kb1，Ｃks2kb2及び暗号化著作権管理プログラムＣpks2を受け取った１次ユーザは、データベース組織利用ソフトウェアを利用して第１公開鍵Ｋb1に対応する第１専用鍵Ｋv1を用いて暗号化第１秘密鍵Ｃks1kb1を復号化し、Ｋs1＝Ｄ（Ｋv1，Ｃks1kb1）
第２公開鍵Ｋb2に対応する第２専用鍵Ｋv2を用いて暗号化第２秘密鍵Ｃks2kb2を復号化す

る。
Ｋｓ2＝Ｄ（Ｋｖ2，Ｃｋｓ2ｋｂ2）
さらに、復号化された第２秘密鍵Ｋｓ2を用いて暗号化著作権管理プログラムＣｐｋｓ2を復号化する。
Ｐ＝Ｄ（Ｋｓ2，Ｃｐｋｓ2）
【００６７】
最後に、復号化された著作権管理プログラムＰを利用して復号化された第１秘密鍵Ｋｓ1を用いて暗号化データＣｍ0ｋｓ1を復号化し、Ｍ0＝Ｄ（Ｋｓ1，Ｃｍ0ｋｓ1）
復号化された原データＭ0をそのままあるいは加工データＭ1として利用する。前に説明したように、第１専用鍵Ｋｖ1及び第２専用鍵Ｋｖ2は１次ユーザが用意し他には公開していない暗号鍵であるから、第３者が暗号化データを入手したとしてもその暗号化データを復号化して利用することは不可能である。
【００６８】
以後原データＭ0あるいは加工データＭ1であるデータＭの保存、コピーあるいは転送を行う場合には第２秘密鍵Ｋｓ2を用いて暗号化及び復号が行われる。
Ｃｍｋｓ2＝Ｅ（Ｋｓ2，Ｍ）
Ｍ＝Ｄ（Ｋｓ2，Ｃｍｋｓ2）
復号された第２の秘密鍵Ｋｓ2は以後データの保存，コピーあるいは転送を行う場合にデータの暗号化／復号化を行う際の暗号鍵として用いられる。１次ユーザ端末装置４には、これらの第１専用鍵Ｋｖ1及び第２専用鍵Ｋｖ2，第１の秘密鍵Ｋｓ1及び第２秘密鍵Ｋｓ2，データＭ，著作権管理プログラムＰとともに原著作権情報Ｉｃ及び１次ユーザがデータの加工を行った場合には１次ユーザ情報及び加工日時等である著作権情報Ｉｃ1も格納される。なお、この著作権情報Ｉｃ1は著作権情報ラベルとしてデータに付けるようにし、さらにディジタル署名付にしておけば安全である。暗号化データＣｍｋｓ2は暗号化されて流通し、復号鍵である第２秘密鍵Ｋｓ2を入手するためには、著作権情報ラベルが手がかりとなるから、暗号化データＣｍｋｓ2からこの著作権情報ラベルが取り外された場合には、第２秘密鍵Ｋｓ2を入手することができない。
【００６９】
暗号化データＣｍｋｓ2が１次ユーザ端末装置４内に保存された場合には第２の秘密鍵Ｋｓ2が装置内に保存されるが、暗号化データＣｍｋｓ2が１次ユーザ端末装置４内に保存されることなく記憶媒体１１にコピーあるいは通信ネットワーク８を経由して２次ユーザ端末装置５への転送が行なわれた場合には、１次ユーザ端末装置４における以降の利用を不可能にするために第２の秘密鍵Ｋｓ2が廃棄される。なお、この場合コピー・転送回数に制限を設けて、制限回数内のコピー・転送では第２の秘密鍵Ｋｓ2が廃棄されないようにしてもよい。
【００７０】
データＭを外部記憶媒体１１にコピーあるいは通信ネットワーク８を経由して転送しようとする１次ユーザは、コピーあるいは転送を行うにあたって第２秘密鍵Ｋｓ2を用意し、データＭを第２の秘密鍵Ｋｓ2を用いて暗号化する。
Ｃｍｋｓ2＝Ｅ（Ｋｓ2，Ｍ）
この暗号化データＣｍｋｓ2には暗号化されていない原著作権情報Ｉｃ、１次ユーザの著作権情報Ｉｃ1が付加される。
【００７１】
２次ユーザは、データベース使用前に１次ユーザと同様に２次ユーザを認証するための認証データＡｕ2，第３の公開鍵Ｋｂ3及び第３の公開鍵Ｋｂ3に対応する第３の専用鍵Ｋｖ3，第４の公開鍵Ｋｂ4及び第４の公開鍵Ｋｂ4に対応する第４の専用鍵Ｋｖ4を用意する。
【００７２】
コピーあるいは転送された暗号化データＣｍｋｓ2の２次利用を希望する２次ユーザは、２次ユーザ端末装置５を利用して通信ネットワーク８を経由して２次著作権管理センタ１４に対して原データ名あるいは原データ番号を指定して２次利用申込を行うが、そのときに、２次ユーザ認証データＡｕ2、原著作権情報Ｉｃ及び１次ユーザ著作権情報Ｉｃ1に加えて第

３の公開鍵Ｋb3と第４の公開鍵Ｋb4も転送する。

【００７３】

２次ユーザからの２次利用申込を受けた２次著作権管理センタ１４は、２次ユーザの認証データＡu2を確認し、確認された２次ユーザ認証データＡu2は２次ユーザ情報として３次著作権管理センタ１５に転送される。また、１次ユーザの２次著作権情報Ｉc1が転送された場合には２次的著作権情報Ｉc1を２次著作権管理センタ１４に照会・確認し、確認された２次的著作権情報Ｉc1は３次著作権管理センタ１５に転送される。

【００７４】

２次著作権管理センタ１４は、第３の秘密鍵Ｋs3を用意する。この第３の秘密鍵Ｋs3は実施例１に示された鍵センタ９を利用して用意してもよい。用意された第３の秘密鍵Ｋs3は３次著作権管理センタ１５に転送され格納される。

【００７５】

これらの転送が行われた結果、３次著作権管理センタ１５には１次ユーザ著作権情報Ｉc1，１次ユーザ情報Ｉ1，原著作権情報Ｉc，２次ユーザ情報Ｉu2及び第３の秘密鍵Ｋs3が格納される。これらの中、１次ユーザ著作権情報Ｉc1及び１次ユーザ情報Ｉ1は、著作権使用料金分配に用いられる。

【００７６】

以下同様にして、ｎ次著作権管理センタ１６には（ｎ－１）次ユーザの２次的著作権情報Ｉcn-1，１次ユーザ情報Ｉ1，原著作権情報Ｉc，ｎ次ユーザ情報Ｉn及び第ｎの秘密鍵Ｋsnが格納される。

【００７７】

２次著作権管理センタ１４から１次ユーザ情報Ｉ1，原著作権情報Ｉc及び第２の秘密鍵Ｋs2が読み出される。この中、原著作権情報Ｉcは著作権使用料配分のために使用される。読み出された第２の秘密鍵Ｋs2は２次ユーザの第３の公開鍵Ｋb3を用いて、第３の秘密鍵Ｋs3は同じく第４の公開鍵Ｋb4を用いて暗号化される。

Ｃks2kb3＝Ｅ（Ｋb3，Ｋs2）

Ｃks3kb4＝Ｅ（Ｋb4，Ｋs3）

また、著作権管理プログラムＰは第３の秘密鍵Ｋs3を用いて、第３の秘密鍵Ｋs3は第４の公開鍵Ｋb4を用いて暗号化される。

Ｃpks3＝Ｅ（Ｋs3，Ｐ）

Ｃks3kb4＝Ｅ（Ｋb4，Ｋs3）

暗号化著作権管理プログラムＣpks3及び暗号化第２秘密鍵Ｃks2kb3及び暗号化第３秘密鍵Ｃks3kb4が通信ネットワーク８を経由して２次ユーザ端末装置３に転送される。このときに必要ならば課金が行われる。

【００７８】

２次著作権管理センタ１４から暗号化された２個の秘密鍵Ｃks2kb3及びＣks3kb4及び暗号化された著作権管理プログラムＣpks3を受け取った２次ユーザは、データベース利用ソフトウェアを利用して第３専用鍵Ｋv3を用いて暗号化第２秘密鍵Ｃks2kb3を復号し、第４の公開鍵Ｋb4に対応する第４の専用鍵Ｋv4を用いて暗号化第３秘密鍵Ｃks3Ｋb4を復号する。

Ｋs2＝Ｄ（Ｋv3，Ｃks2kb3）

Ｋs3＝Ｄ（Ｋv4，Ｃks3kb4）

また、復号化された第３の秘密鍵Ｋs3を用いて暗号化著作権管理プログラムＣpks3が復号される。

Ｐ＝Ｄ（Ｋs3，Ｃpks3）

次に、復号化された著作権管理プログラムＰを利用して復号された第２の秘密鍵Ｋs2を用いて暗号化データＣmks2を復号化し利用する。

Ｍ＝Ｄ（Ｋs2，Ｃmks2）

【００７９】

前に説明したように、第３専用鍵Ｋv3及び第４専用鍵Ｋv4は２次ユーザが用意しただけで

他には公開していない暗号鍵であるから、第３者が暗号化データＣmks2を入手したとしても復号化して利用することは不可能である。

【００８０】

以上説明した実施例において、データベース１，２次著作権管理センタ１４，３次著作権管理センタ１５及びｎ次著作権管理センタ１６は、利用申込の輻輳を避けるために別個に設けられている。しかし、利用申込の輻輳が問題とならないならば、これらの全部あるいは一部を合体させることもできる。

【００８１】

［実施例５］図３に示されたのは、実施例５のシステム構成であり、この実施例５において、原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。この実施例において、暗号鍵方式に秘密鍵方式が採用される。

【００８２】

この図において、１はテキストデータ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ，ディジタル音声データ，ディジタル映像データが暗号化された状態で格納されたデータベースであり、２は通信・放送衛星等の人工衛星，３はＣＤ－ＲＯＭあるいはフレキシブルディスク等のデータ記録媒体，８は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワーク，４は１次ユーザ端末装置である。また、１７はデータの著作権を管理する著作権管理センタであり、５，６及び７は各々２次ユーザ端末装置，３次ユーザ端末装置及びｎ次ユーザ端末装置である。

【００８３】

これらのうちデータベース１，著作権管理センタ１７，１次ユーザ端末装置４，２次ユーザ端末装置５，３次ユーザ端末装置６及びｎ次ユーザ端末装置７は通信ネットワーク８によって相互に接続可能とされている。

【００８４】

このシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要がある。また、この登録の際にデータベース利用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアプログラムが含まれている。このデータベース組織を利用するためのソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマスクＲＯＭ，ＥＰＲＯＭ，ＥＥＰＲＯＭ等に格納することも可能である。

【００８５】

また、このシステムにおいてはユーザ側で秘密鍵を生成するため、ユーザ端末装置に秘密鍵生成アルゴリズムが格納されるが、この秘密鍵生成アルゴリズム自身は必ずしも秘密のものではないため、データベース組織に対して利用を登録するときにユーザに対して供給されるデータベース組織利用ソフトウェアに内蔵させてもよい。なお、原データが広告付等無料で供給される場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。

【００８６】

この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、１点鎖線で示された経路は著作権管理センタから暗号鍵が転送される経路である。

【００８７】

データベース１あるいはデータ記録媒体３に格納されている原データＭ0は通信ネットワーク８を経由して有線経路で、人工衛星２等経由して放送電波によりあるいは記録媒体３を経由して１次ユーザ端末装置４に供給されるがこのときに第１秘密鍵Ｋs1を用いて暗号化される。

Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）

【００８８】

実施例１～４の場合と同様に、暗号化されて供給される原データＣm0ks1の著作権を保護するために、本発明者らによる先願である特願平６－６４８８９号に示されているように、１次ユーザ端末装置４において、原データM0は、表示及び加工のための表示以外の利用形態である保存，コピー，転送が行われるときには第２秘密鍵Ｋs2を用いて暗号化され、Ｃm0ks2＝Ｅ（Ｋs2，M0）
以後の利用においては第２秘密鍵Ｋs2によって原データの暗号化／復号化が行われる。

【００８９】
暗号化原データＣm0ks1を入手した１次ユーザは１次ユーザ端末装置４を利用して、原データ名あるいは原データ番号等を指定して、暗号化原データＣm0ks1の１次利用を著作権管理センタ１７に申し込む。１次ユーザ端末装置４から暗号化原データＣm0ks1の１次利用申込を受けた著作権管理センタ１７は、第１秘密鍵Ｋs1とともに著作権管理プログラムＰを１次ユーザ端末装置４に転送する。この著作権管理プログラムＰには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムにより秘密鍵の生成及びデータの復号化／暗号化が行われる。

【００９０】
第１秘密鍵Ｋs1と著作権管理プログラムＰを受け取った１次ユーザ端末装置４は、暗号プログラムを利用して第１秘密鍵Ｋs1を用いて暗号化原データＣm0ks1を復号し、M0＝Ｄ（Ｋs1，Ｃm0ks1）
復号化された原データM0をそのままあるいは加工データM1として利用する。また、著作権管理プログラムＰにより第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2が生成される。
Ｋs2＝Ｐ（Ｋs1）

【００９１】
原データM0あるいは加工データM1であるデータMが１次ユーザ端末装置４内に保存される場合，記録媒体１１に複写される場合，２次ユーザ端末装置５に転送される場合には、著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化される。
Ｃmks2＝Ｅ（Ｋs2，M）

【００９２】
第２秘密鍵Ｋs2によって暗号化されたデータＣmks2は、原データ名あるいは原データ番号とともに、記録媒体１１に複写あるいは通信ネットワーク８を経由して２次ユーザ端末装置５に転送される。

【００９３】
暗号化されたデータＣmks2を入手した２次ユーザは２次ユーザ端末装置５を利用して、原データ名あるいは原データ番号を指定することにより暗号化データＣmks2の２次利用を著作権管理センタ１７に申し込む。

【００９４】
暗号化データＣmks2の２次利用申込を受けた著作権管理センタ１７は、原データ名あるいは原データ番号から第１秘密鍵Ｋs1を探し出し、著作権管理プログラムＰにより第１秘密鍵Ｋs1から第２秘密鍵Ｋs2を生成し、Ｋs2＝Ｐ（Ｋs1）
生成された第２秘密鍵Ｋs2を著作権管理プログラムＰとともに２次ユーザ端末装置５に供給する。

【００９５】
第２秘密鍵Ｋs2と著作権管理プログラムＰを受け取った２次ユーザ端末装置５は、第２秘密鍵Ｋs2で暗号化されたデータＣmks2を第２秘密鍵Ｋs2で復号化してＭ＝Ｄ（Ｋs2，Ｃmks2）
表示あるいは加工の利用を行う。

【００９６】
復号されたデータMが２次ユーザ端末装置５内に保存される場合，記録媒体１２に保存される場合，通信ネットワーク８を経由して３次ユーザ端末装置６に転送される場合には、そのデータMは著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化される。

【００９７】

さらに、著作権管理プログラムＰが、第２秘密鍵Ｋs2に基づいて第３秘密鍵Ｋs3を生成するようにし、Ｋs3＝Ｐ（Ｋs2）

【００９８】

データＭが２次ユーザ端末装置５内に保存される場合，記録媒体１２に複写される場合，通信ネットワーク８を経由して３次ユーザ端末装置６に転送される場合には、そのデータＭは著作権管理プログラムＰにより第３の秘密鍵Ｋs3を用いて暗号化されるようにしてもよい。

Ｃmks3＝Ｅ（Ｋs3，Ｍ）

【００９９】

［実施例６］次に、実施例６について説明するが、実施例５と同様に原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。この実施例において採用される暗号鍵方式は秘密鍵方式であり、第２秘密鍵は１次ユーザ情報と第１秘密鍵に基づいて生成される。なお、実施例６で用いるシステム構成は図３に示された実施例５のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【０１００】

実施例６において、データベース１に格納されている原データＭ0は通信ネットワーク８を経由して有線経路で，人工衛星２等経由して放送電波によりあるいは記録媒体３を経由して第１秘密鍵Ｋs1を用いて暗号化されてＣm0ks1＝Ｅ（Ｋs1，Ｍ0）
１次ユーザ端末装置４に供給される。

【０１０１】

暗号化原データＣm0ks1を入手した１次ユーザは１次ユーザ端末装置４を利用して、暗号化原データＣm0ks1の１次利用を著作権管理センタ１７に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに１次ユーザ情報Ｉu1を提示する。

【０１０２】

１次ユーザから暗号化原データＣm0ks1の１次利用申込を受けた著作権管理センタ１７は、第１秘密鍵Ｋs1と著作権管理プログラムＰを１次ユーザ端末装置４に供給する。

【０１０３】

著作権管理プログラムＰには、暗号アルゴリズムを有する暗号プログラムＰが含まれており、この暗号プログラムＰにより秘密鍵生成及び復号／暗号化が行われる。

【０１０４】

第１秘密鍵Ｋs1と著作権管理プログラムを受け取った１次ユーザ端末装置４では、暗号プログラムＰにより第１秘密鍵Ｋs1を用いて暗号化原データＭ0を復号してＭ0＝Ｄ（Ｋs1，Ｃm0ks1）
復号化された原データＭ0をそのままあるいは加工データＭ1として利用する。また、供給された著作権管理プログラムＰが、１次ユーザ情報Ｉu1あるいは１次ユーザ情報Ｉu1と第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成する。
Ｋs2＝Ｐ（Ｉu1）　又はＫs2＝Ｐ（Ｉu1＋Ｋs1）
生成された第２秘密鍵Ｋs2は１次ユーザ情報Ｉu1に基づいているため、正しい１次ユーザ情報Ｉu1を有していなければ生成することが不可能である。なお、１次ユーザ情報Ｉu1に代えて、１次ユーザ情報Ｉu1に基づいて生成された１次ユーザデータ、あるいは１次ユーザ端末装置４に付与されている装置番号を利用することもできる。

【０１０５】

原データＭ0あるいは加工データＭ1であるデータＭが１次ユーザ端末装置４内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して２次ユーザ端末装置５に供給される場合には、そのデータＭは著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化される。

Ｃmks2＝Ｅ（Ｋs2，Ｍ）

【０１０６】

第２秘密鍵Ｋs2で暗号化されたデータＣmks2は、原データ名あるいは原データ番号及び１

次ユーザ情報Ｉu1とともに、記録媒体１１に複写されあるいは、通信ネットワーク８を経由して２次ユーザ端末装置５に供給される。

【０１０７】

暗号化されたデータＣmks2を入手した２次ユーザは２次ユーザ端末装置５を利用して、データＭの２次利用を著作権管理センタ１７に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに１次ユーザ情報Ｉu1を提示する。

【０１０８】

データＭの２次利用申込を受けた著作権管理センタ１７は、原データ名あるいは原データ番号を手がかりとして第１秘密鍵Ｋs1を探し出し、１次ユーザデ情報Ｉu1，第１秘密鍵Ｋs1あるいは１次ユーザ情報Ｉu1と第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、生成された第２秘密鍵Ｋs2を著作権管理プログラムＰとともに２次ユーザ端末装置５に提供する。

【０１０９】

第２秘密鍵Ｋs2と著作権管理プログラムＰを受け取った２次ユーザは２次ユーザ端末装置５を利用して、著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化データＣmks2を復号化して利用する。

Ｍ＝Ｄ（Ｋs2，Ｃmks2）

データＭが２次ユーザ端末装置５内に保存される場合、記録媒体１１に複写される場合、通信ネットワークを経由して３次ユーザ端末装置６に供給される場合には、そのデータは第２秘密鍵Ｋs2によって暗号化される。

【０１１０】

なお、著作権管理プログラムＰにより第２秘密鍵Ｋs2に基づいて第３秘密鍵Ｋs3を生成するようにし、Ｋs3＝Ｐ（Ｋs2）

データＭが２次ユーザ端末装置５内に保存される場合，記録媒体１１に複写される場合，通信ネットワークを経由して３次ユーザ端末装置６に供給される場合には、そのデータは第３秘密鍵Ｋs3によって暗号化されるようにすることもできる。

【０１１１】

また、２次ユーザが著作権管理センタ１７に２次利用申込を行うときに、２次ユーザ情報Ｉu2を提示し、提示された２次ユーザ情報Ｉu2に基づいて第３秘密鍵Ｋs3が生成されるようにすることもできる。

【０１１２】

この実施例６において、第２秘密鍵Ｋs2を生成する著作権管理プログラムＰを全データベース組織において共通のものとしておけば、どのデータベース組織においても１次ユーザ情報Ｉu1及び第１秘密鍵Ｋs1が変更されない限り同一の原データに対しては同一の第２秘密鍵Ｋs2が生成される。

【０１１３】

［実施例７］次に、実施例７について説明するが、実施例５及び実施例６と同様に原データは単一のデータベースから暗号化されて１方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。また、この実施例において第２秘密鍵は著作権管理プログラムの使用回数と第１秘密鍵に基づいて生成される。

【０１１４】

この実施例において採用される暗号鍵方式は秘密鍵方式である。なお、実施例７で用いるシステム構成は図３に示された実施例５及び実施例６のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【０１１５】

データベース１に格納されている原データＭ0は通信ネットワーク８を経由して有線経路で，人工衛星２等を経由して放送電波によりあるいは記録媒体３を経由して第１秘密鍵Ｋs1を用いて暗号化されてＣm0ks1＝Ｅ（Ｋs1，Ｍ0）

１次ユーザ端末装置４に供給される。

【０１１６】

暗号化原データＣｍ0ks1を入手した１次ユーザは１次ユーザ端末装置４を利用して、原データ名あるいは原データ番号等を指定することにより原データM0の１次利用を著作権管理センタ１７に申し込む。

【０１１７】

原データM0の１次利用申込を受けた著作権管理センタ１７は、第１秘密鍵Ｋs1及び著作権管理プログラムＰを１次ユーザ端末装置４に転送する。

【０１１８】

この著作権管理プログラムＰには暗号アルゴリズムを有する暗号プログラムが含まれており、暗号鍵の生成及びデータの復号化／暗号化が行われる。また、著作権管理プログラムＰにはカウンタが付属しており、このカウンタがプログラムＰの使用回数Ｎを計数する。

【０１１９】

第１秘密鍵Ｋs1及び著作権管理プログラムＰを受け取った１次ユーザは、暗号化原データＣｍ0ks1を著作権管理プログラムＰを利用して第１秘密鍵Ｋs1を用いて復号化してM0＝Ｄ（Ｋs1，Ｃｍ0ks1）

復号化された原データM0をそのままあるいは加工データM1として利用する。

【０１２０】

このシステムにおいては、データの著作権を管理するために原データM0あるいは加工データM1であるデータMが１次ユーザ端末装置４内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して２次ユーザ端末装置５に転送される場合に著作権管理プログラムにＰより第２秘密鍵Ｋs1を用いて暗号化されるが、このときに用いられる第２暗号鍵Ｋs2は著作権管理プログラムの使用回数Ｎと第１秘密鍵Ｋs1に基づいて生成される。

Ｋs2＝Ｐ（Ｎ＋Ｋs1）

【０１２１】

このようにして生成される第２秘密鍵Ｋs2は著作権管理プログラムＰの使用回数Ｎと第１秘密鍵Ｋs1に基づいているため、データMは利用される度に最新の第２秘密鍵Ｋs2で暗号化される。

Ｃｍks2＝Ｅ（Ｋs2，Ｍ）

【０１２２】

最後の利用によって生成された第２秘密鍵Ｋs2によって暗号化されたデータＣｍks2は、原データ名あるいは原データ番号、カウンタデータＮ1とともに、記録媒体１１に複写あるいは、通信ネットワーク８を経由して２次ユーザ端末装置５に転送される。

【０１２３】

暗号化データＣｍks2を入手した２次ユーザは２次ユーザ端末装置５を用いて、原データ名あるいは原データ番号及びカウンタデータＮ1を提示して、暗号化データＣｍks2の２次利用を著作権管理センタ１７に申し込む。

【０１２４】

暗号化データＣｍks2の２次利用申込を受けた著作権管理センタ１７は、提示された原データ名あるいは原データ番号から第１秘密鍵Ｋs1を探し出し、カウンタデータＮ1及び第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、著作権管理プログラムＰとともに第２秘密鍵Ｋs2を通信ネットワーク８を経由して２次ユーザ端末装置５に供給する。

【０１２５】

第２秘密鍵Ｋs2と著作権管理プログラムＰを受け取った２次ユーザは、暗号化データＣｍks2を著作権管理プログラムＰを利用して第２秘密鍵Ｋs2を用いて復号化しＭ＝Ｄ（Ｋs2，Ｃｍks2）

復号化されたデータＭをそのままあるいは加工して利用する。

【０１２６】

データＭが２次ユーザ端末装置５内に保存される場合、記録媒体１１に複写される場合、通信ネットワーク８を経由して３次ユーザ端末装置６に転送される場合には、データＭは著作権管理プログラムＰにより第２秘密鍵Ｋs2によって暗号化される。

Ｃmks2＝Ｅ（Ｋs2，Ｍ）

【０１２７】

この場合、さらに著作権管理プログラムＰが、２次ユーザ端末装置５における著作権管理プログラムＰの使用回数Ｎ2と秘密鍵Ｋs2に基づいて第３秘密鍵Ｋs3を生成するようにすることもできる。

Ｋs3＝Ｐ（Ｎ2＋Ｋs2）

この場合、データＭが２次ユーザ端末装置５内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して３次ユーザ６に転送される場合には、データＭは著作権管理プログラムＰにより第３秘密鍵Ｋs3によって暗号化される。

Ｃmks3＝Ｅ（Ｋs3，Ｍ）

【０１２８】

［実施例８］図４に示されたのは、データ著作権管理システムの実施例８のシステム構成であり、この実施例８において単一のデータベースから供給される原データはユーザからの要求に応じて双方向的に供給される。この実施例において採用される暗号方式は秘密鍵方式であり、第１秘密鍵に基づいて第２秘密鍵が生成される。

【０１２９】

この図において、１はデータベース，４は１次ユーザ端末装置，５は２次ユーザ端末装置，６は３次ユーザ端末装置，７はｎ次ユーザ端末装置である。また、１８は著作権管理センタ，８は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワークである。

【０１３０】

これらのうちデータベース１，著作権管理センタ１８，１次ユーザ端末装置４，２次ユーザ端末装置５，３次ユーザ端末装置６及びｎ次ユーザ端末装置７は通信ネットワーク８によって相互に接続可能とされている。

【０１３１】

このシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要がある。また、この登録の際にデータベース組織用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアプログラムが含まれている。このデータベース組織用ソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマスクＲＯＭ，ＥＰＲＯＭ，ＥＥＰＲＯＭ等に格納することも可能である。

【０１３２】

また、このシステムにおいてはユーザ側で秘密鍵を生成するためユーザ端末装置に秘密鍵生成アルゴリズムが格納されるが、この秘密鍵生成アルゴリズム自身は必ずしも秘密のものではないため、データベース組織に利用を登録するときにユーザに対して提供されるデータベース組織用ソフトウェアに内蔵させてもよい。なお、広告付等の無料で供給される原データの場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。

【０１３３】

なお、この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、１点鎖線で示された経路は各データベースからの利用形態に対応した利用許可情報及び著作権管理プログラムとともに秘密鍵が転送される経路である。

【０１３４】

この図において、データベース１にはテキストデータ，グラフィックスデータあるいはバイナリデータ，音声データ，映像データが暗号化されていない状態で保管されている。

【０１３５】

１次ユーザは１次ユーザ端末装置４を使用して通信ネットワーク８を経由してデータベース１に対して、利用することを希望する原データ名を指定して原データＭ0の利用を申し込む。

【０１３６】
１次ユーザ端末装置４から原データＭ0の利用申し込みを受けたデータベース１は、原データＭ0を第１秘密鍵Ｋs1で暗号化し、Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）
暗号化された原データＣm0ks1及び第１秘密鍵Ｋs1とともに著作権管理プログラムＰを１次ユーザ端末装置４に供給する。この著作権管理プログラムＰには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムＰにより、秘密鍵の生成及びデータの復号化／暗号化が行われる。なお、この暗号アルゴリズムを第１秘密鍵Ｋs1に依存するものにしておけば、著作権管理プログラムＰをその原データＭ0に固有のものとすることができる。
【０１３７】
第１秘密鍵Ｋs1を用いて暗号化された原データＣm0ks1とともに第１秘密鍵Ｋs1と著作権管理プログラムＰを受け取った１次ユーザ端末装置４は、第１秘密鍵Ｋs1を用いて暗号化原データＣm0ks1を復号し、Ｍ0＝Ｄ（Ｋs1，Ｃm0ks1）
復号化された原データＭ0をそのままあるいは加工データＭ1として利用する。また、著作権管理プログラムＰにより、第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2が生成される。
Ｋs2＝Ｐ（Ｋs1）
【０１３８】
復号された原データあるいは加工されたデータであるデータＭが１次ユーザ端末装置４内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して２次ユーザ端末装置５に転送される場合には、そのデータＭは著作権管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化される。
Ｃmks2＝Ｅ（Ｋs2，Ｍ）
【０１３９】
暗号化データＣmks2は、原データ名あるいは原データ番号とともに、記録媒体１１に複写され、あるいは、通信ネットワーク８を経由して２次ユーザ端末装置５に転送される。
【０１４０】
暗号化データＣmks2を入手した２次ユーザは、２次ユーザ端末装置５を利用して、原データ名あるいは原データ番号を指定することにより原データあるいは加工データであるデータＭの２次利用を著作権管理センタ１８に申し込む。
【０１４１】
データＭの２次利用申込を受けた２次著作権管理センタ１８は、原データ名あるいは原データ番号を手がかりとして第１秘密鍵Ｋs1を探し出し、第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、Ｋs2＝Ｐ（Ｋs1）
生成された第２秘密鍵Ｋs2を著作権管理プログラムＰとともに２次ユーザ端末装置５に供給する。
【０１４２】
第２秘密鍵Ｋs2と著作権管理プログラムＰを受け取った２次ユーザ端末装置５は、暗号化データＣmks2を著作権管理プログラムＰを利用して第２秘密鍵Ｋs2を用いて復号化してＭ＝Ｄ（Ｋs2，Ｃmks2）
復号化されたＭをそのままあるいは加工して利用する。データＭが２次ユーザ端末装置５内に保存される場合，記録媒体１２に複写される場合，通信ネットワーク８を経由して３次ユーザ端末装置６に転送される場合には、
【０１４３】
著作権管理プログラムＰにより第２秘密鍵Ｋs2に基づいて第３秘密鍵Ｋs3が生成され、Ｋs3＝Ｐ（Ｋs2）
著作権管理プログラムＰによりこの生成された第３秘密鍵Ｋs3を用いてデータＭが暗号化される。
Ｃmks3＝Ｅ（Ｋs3，Ｍ）
【０１４４】
［実施例９］次に説明する実施例９は図４に示された実施例８と同様に単一のデータベー

スから供給される原データはユーザからの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式であり、第２秘密鍵の生成に実施例８で用いられた第１秘密鍵に加えてユーザデータを利用する。なお、この実施例のシステム構成は実施例８のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【０１４５】

データベース１には、原データM0が暗号化されていない状態で保管されている。１次ユーザが１次ユーザ端末装置４を利用してデータベース１にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【０１４６】

データメニューが転送されると１次ユーザはデータメニュー検索を行い原データM0を選択し、選択した原データM0の原データ名等を指定することによりデータベース１に対して、原データM0の１次利用を申し込む。

【０１４７】

１次ユーザ端末装置４から原データM0の利用申し込みを受けたデータベース１では、原データM0が読み出され、読み出された原データM0が第１秘密鍵Ｋs1で暗号化され、Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）

暗号化された原データＣm0ks1及び第１秘密鍵Ｋs1とともに著作権管理プログラムＰを１次ユーザ端末装置４に供給される。

【０１４８】

ここで使用される著作権管理プログラムＰは全てのデータベース組織において共通のものであり、さらに暗号アルゴリズムを有する暗号プログラムを含んでおり、この暗号プログラムにより暗号生成及びデータの復号化／暗号化が行われる。

【０１４９】

第１秘密鍵Ｋs1と著作権管理プログラムＰを受け取った１次ユーザ端末装置４は、著作権管理プログラムＰにより第１秘密鍵Ｋs1を用いて暗号化された原データＣm0ks1を復号化してM0＝Ｄ（Ｋs1，Ｃm0ks1）

復号化された原データM0をそのままあるいは加工データM1として利用する。また、著作権管理プログラムＰが、１次ユーザ情報Ｉu1に基づいて第２の秘密鍵Ｋs2を生成する。

Ｋs2＝Ｐ（Ｉu1）

この第２の秘密鍵Ｋs2は、１次ユーザ情報Ｉu1以外に第１秘密鍵Ｋs1あるいは１次ユーザデータＩu1と第１秘密鍵Ｋs1とに基づいて生成することもできる。

Ｋs2＝Ｐ（Ｋs1）

Ｋs2＝Ｐ（Ｋs1＋Ｉu1）

【０１５０】

原データM0あるいは加工データM1であるデータMが１次ユーザ端末装置４内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して２次ユーザ端末装置５に転送される場合には、そのデータMは著作権管理プログラムＰにより第２の秘密鍵Ｋs2によって暗号化される。

Ｃmks2＝Ｅ（Ｋs2，Ｍ）

【０１５１】

第２の秘密鍵Ｋs2によって暗号化されたデータＣmks2は、原データ名あるいは原データ番号が付されるとともに、記録媒体１１に複写されあるいは、通信ネットワーク８を経由して２次ユーザ端末装置５に転送される。

【０１５２】

第２秘密鍵Ｋs2によって暗号化されたデータＣmks2を入手した２次ユーザは、２次ユーザ端末装置５を利用してデータMの２次利用を著作権管理センタ１８に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに暗号化されていない１次ユーザ情報Ｉu1を提示する。

【０１５３】

データMの２次利用申込を受けた著作権管理センタ１８は、指定された原データ名あるい

は原データ番号により第１秘密鍵Ｋs1を探し出し、著作権管理プログラムＰにより提示された１次ユーザ情報Ｉu1，探し出された第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、著作権管理プログラムＰとともに２次ユーザ端末装置５に供給する。

【０１５４】

第２秘密鍵Ｋs2と著作権管理プログラムＰを受け取った２次ユーザは２次ユーザ端末装置５を利用して、著作権管理プログラムＰにより第２の秘密鍵Ｋs2を用いて暗号化されたデータＣmks2を復号化して、Ｍ＝Ｄ（Ｋs2，Ｃmks2）

復号化されたデータＭをそのままあるいは加工して利用する。データＭが２次ユーザ端末装置５内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して３次ユーザ端末装置６に転送される場合には、そのデータＭは著作権管理プログラムＰにより第２の秘密鍵Ｋs2によって暗号化される。

Ｃmks2＝Ｅ（Ｋs2，Ｍ）

【０１５５】

なお、この場合、著作権管理プログラムＰが、１次ユーザ情報Ｉu1，第２秘密鍵Ｋs2あるいは１次ユーザ情報Ｉu1と第２秘密鍵Ｋs2に基づいて第３の秘密鍵Ｋs3を生成するＫs3＝Ｐ（Ｉu1）

Ｋs3＝Ｐ（Ｉu1＋Ｋs1）

Ｋs3＝Ｐ（Ｋs1）

ようにすることもできる。また、２次ユーザが２次利用申込を行うときに２次ユーザ情報Ｉu2を提示し、１次ユーザ情報Ｉu1の代わりに２次ユーザ情報Ｉu2に基づいて第３秘密鍵を生成することもできる。データＭは著作権管理プログラムＰにより第３秘密鍵Ｋs3によって暗号化される。

Ｃmks3＝Ｅ（Ｋs3，Ｍ）

【０１５６】

この実施例において、第２秘密鍵Ｋs2を生成する著作権管理プログラムＰは全データベース組織において共通のものであるから、どのデータベース組織においても、１次ユーザデータＩu1及び第１秘密鍵Ｋs1が変更されない限り同一の原データに対しては同一の第２秘密鍵Ｋs2が生成される。

【０１５７】

［実施例１０］次に説明する実施例１０は図４に示された実施例８と同様に原データが単一のデータベースからユーザからの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式である。この実施例においては、第２秘密鍵の生成に実施例９で用いられたユーザ情報に代えて著作権管理プログラムの使用回数を利用する。なお、この実施例のシステム構成は実施例８のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【０１５８】

データベース１には、原データＭ0が暗号化されていない状態で保管されている。１次ユーザが１次ユーザ端末装置４を利用してデータベース１にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【０１５９】

データメニューが転送されると１次ユーザはデータメニュー検索を行い原データＭ0を選択し、１次ユーザ端末装置４を利用して、通信ネットワーク８を経由してデータベース１に対して、原データ名等を指定して１次利用を希望する原データＭ0の利用を申し込む。

【０１６０】

１次ユーザからデータ利用申し込みを受けたデータベース１は、原データＭ0を第１秘密鍵Ｋs1で暗号化し、Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）

暗号化されたデータＣm0ks1と第１秘密鍵Ｋs1とともに著作権管理プログラムＰを１次ユーザ端末装置４に供給する。

【０１６１】

この著作権管理プログラムＰには暗号アルゴリズムを有する暗号プログラムが含まれてお

り、この暗号プログラムにより暗号鍵生成及びデータの復号化／暗号化が行われる。また、著作権管理プログラムＰにはカウンタが付属しており、このカウンタがプログラムの使用回数Ｎあるいは原データの利用回数Ｎを計数する。なお、この暗号アルゴリズムを第１秘密鍵Ｋs1に依存するものにしておけば、著作権管理プログラムＰをその原データ固有のものとすることができる。

【０１６２】

第１秘密鍵Ｋs1と著作権管理プログラムＰを受け取った１次ユーザは、暗号化された原データＣm0ks1を著作権管理プログラムＰを使用して第１秘密鍵Ｋs1を用いて復号化して、

Ｍ0＝Ｄ（Ｋs1，Ｃm0ks1）

復号化された原データＭ0をそのままあるいは加工データＭ1として利用する。

【０１６３】

データの著作権を保護するため、原データＭ0あるいは加工データＭ1であるデータＭが１次ユーザ端末装置４内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して２次ユーザ端末装置５に転送される場合には、そのデータＭは著作権管理プログラムＰにより暗号化される。言い換えれば、これらの利用が行われるときには必ず著作権管理プログラムが動作する。

【０１６４】

一方、供給された著作権管理プログラムＰが使用されるとプログラム内のカウンタが計数を行い、そのカウント数Ｎと第１秘密鍵Ｋs1に基づいて著作権管理プログラムＰが第２秘密鍵Ｋs2を生成する。

Ｋs2＝Ｐ（Ｎ＋Ｋs2）

【０１６５】

この第２秘密鍵Ｋs2は著作権管理プログラムＰの使用回数Ｎにも基づいているため、データＭは利用される度に新しい第２秘密鍵Ｋs2で暗号化される。

Ｃmks2＝Ｅ（Ｋs2，Ｍ）

最後に生成された第２秘密鍵Ｋs2によって暗号化されたデータＣmks2は、原データ名あるいは原データ番号，１次ユーザ情報Ｉu1及びカウンタデータＮとともに、記録媒体１１に複写あるいは、通信ネットワーク８を経由して２次ユーザ端末装置５に転送される。

【０１６６】

第２秘密鍵Ｋs2を用いて暗号化されたデータＣmks2を入手した２次ユーザは、原データ名あるいは原データ番号，１次ユーザ情報Ｉu1及びカウンタデータＮを提示して、データＭの２次利用を著作権管理センタ１８に申し込む。

【０１６７】

暗号化されたデータＣmks2の２次利用申込を受けた著作権管理センタ１８は、そのデータの原データ名あるいは原データ番号から第１の秘密鍵Ｋs1を探し出し、第１の秘密鍵、提示された１次ユーザ情報Ｉu1及びカウンタデータＮから第２の秘密鍵Ｋs2を生成し、生成された第２の秘密鍵Ｋs2を著作権管理プログラムＰとともに２次ユーザ端末装置５に転送する。

【０１６８】

第２の秘密鍵kS2と著作権管理プログラムＰを受け取った２次ユーザ端末装置５は、著作権管理プログラムＰを利用して暗号化データＣmks2を第２の秘密鍵Ｋs2を用いて復号化し

Ｍ＝Ｄ（Ｋs2，Ｃmks2）

復号化されたデータＭをそのままあるいは加工して利用する。

【０１６９】

データが２次ユーザ端末装置５内に保存される場合，記録媒体１２に複写される場合，通信ネットワーク８を経由して３次ユーザ端末装置６に転送される場合には、そのデータは著作権管理プログラムにより第２の秘密鍵によって暗号化される。

【０１７０】

なお、さらに著作権管理プログラムが、第２の秘密鍵に基づいて第３の秘密鍵を生成することもできる。

【０１７１】
以上説明した実施例１から実施例１０はいずれもデータベースから供給された単一原データを利用する場合についてのものである。しかし、データの利用形態としての加工には単一のデータを加工する他に、同一のデータベースから入手した複数の原データを組み合わせて新しいデータを作成する場合及び複数のデータベースから入手した複数の原データを組み合わせて新しいデータを作成する場合がある。
【０１７２】
［実施例１１］次に説明する実施例１１は、１次ユーザが単一のデータベースに保存されている複数の原データを組み合わせて新しいデータを作成する実施例であり、１次ユーザはデータベースに保存されている第１，第２，第３の原データを材料にして新しいデータを作成する。
【０１７３】
この実施例においては図４に示された実施例８と同様に複数の原データが単一のデータベースからユーザの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式である。なお、この実施例のシステム構成は実施例８のシステム構成と異なる点はないので、システム構成についての説明は省略する。
【０１７４】
データベース１には、原データM01，M02，M03が暗号化されていない状態で保管されている。１次ユーザが１次ユーザ端末装置４を利用してデータベース１にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。
【０１７５】
データメニューが転送されると１次ユーザはデータメニュー検索を行い原データM01，M02，M03を選択し、１次ユーザ端末装置４を利用して、通信ネットワーク８を経由してデータベース１に対して、第１，第２，第３の原データM01，M02，M03の原データ名あるいは原データ番号を指定して各原データの供給を申し込むがこのときに１次ユーザ情報Ｉu1を提示する。
【０１７６】
１次ユーザから第１，第２，第３の原データM01，M02，M03の供給申し込みを受けたデータベース１は、供給申込を受けた第１，第２，第３の原データM01，M02，M03を各々第１，第２，第３の秘密鍵Ｋs01，Ｋs02，Ｋs03を用いて暗号化し、Ｃm01ks01＝Ｅ（Ｋs01，M01）
Ｃm02ks02＝Ｅ（Ｋs02，M02）
Ｃm03ks03＝Ｅ（Ｋs03，M03）
第１，第２，第３の秘密鍵Ｋs01，Ｋs02，Ｋs03及び全てのデータベース組織と全ての原データに共通する著作権管理プログラムＰを１次ユーザ端末装置４に供給する。この著作権管理プログラムＰには暗号アルゴリズムを有する暗号プログラムが含まれており、暗号鍵生成及び復号化／暗号化が行われる。
【０１７７】
暗号化第１原データＣm01ks01，暗号化第２原データＣm02ks02，暗号化第３原データＣm03ks03，第１秘密鍵Ｋs01，第２秘密鍵Ｋs02，第３秘密鍵Ｋs03，著作権管理プログラムＰを受け取った１次ユーザ端末装置４は、著作権管理プログラムＰを利用してこれらの秘密鍵Ｋs01，Ｋs02，Ｋs03を用いて第１，第２，第３の各暗号化原データＣm01ks01，Ｃm02ks02，Ｃm03ks03を復号化しM01＝Ｄ（Ｋs01，Ｃm01ks01）
M02＝Ｄ（Ｋs02，Ｃm02ks02）
M03＝Ｄ（Ｋs03，Ｃm03ks03）
原データM01，M02，M03を加工して新しいデータM1を作成する。
【０１７８】
また、著作権管理プログラムＰが第１秘密鍵Ｋs01，第２秘密鍵Ｋs02，第３秘密鍵Ｋs03，１次ユーザデータＩu1のうちの１つあるいはこの中のいくつかに基づいて第４秘密鍵Ｋ

s4を生成する。
Ｋs4＝Ｐ（Ｋs01／Ｋs02／Ｋs03／Ｉu1）
【０１７９】
加工データＭ1が１次ユーザ端末装置４内に保存される場合，記録媒体１１に複写される場合，通信ネットワーク８を経由して２次ユーザ５に転送される場合には、著作権管理プログラムＰにより第４秘密鍵Ｋs4によって暗号化される。
Ｃm1ks4＝Ｅ（Ｋs4，Ｍ1）
【０１８０】
暗号化加工データＣm1ks4は原データ名あるいは原データ番号及び１次ユーザデータＩu1とともに、記録媒体１１に複写あるいは通信ネットワーク８を経由して２次ユーザ端末装置５に転送される。
【０１８１】
暗号化加工データＣm1ks4を入手した２次ユーザは２次ユーザ端末装置５を利用して暗号化加工データＣm1ks4の２次利用を著作権管理センタ１８に申し込むが、このときに原データＭ01，Ｍ02，Ｍ03のデータ名あるいはデータ番号等を指定するとともに１次ユーザ情報Ｉu1を提示する。
【０１８２】
２次ユーザから暗号化加工データＣm1ks4の２次利用申込を受けた著作権管理センタ１８は、第１原データＭ01のデータ名あるいはデータ番号から第１秘密鍵Ｋs01を探し出し、第２原データＭ02のデータ名あるいはデータ番号から第２秘密鍵Ｋs02を探し出し、第３原データＭ03のデータ名あるいは原データ番号から第３秘密鍵Ｋs03を探し出し、共通の著作権管理プログラムＰにより、探し出された第１秘密鍵Ｋs01，第２秘密鍵Ｋs02，第３秘密鍵Ｋs03，１次ユーザ情報Ｉu1のうちの１つあるいはこの中のいくつかに基づいて第４秘密鍵Ｋs4を生成し、Ｋs4＝Ｐ（Ｋs01／Ｋs02／Ｋs03／Ｉu1）
共通の著作権管理プログラムＰとともに２次ユーザ５に提供する。
【０１８３】
第４の秘密鍵と共通の著作権管理プログラムを受け取った２次ユーザは、著作権管理プログラムＰにより第４秘密鍵Ｋs4を用いて加工データＭ1を復号化しＭ1＝Ｄ（Ｋs4，Ｃm1ks4）
復号化された加工データＭ1をそのままあるいは再加工データＭ2として利用する。
【０１８４】
加工データＭ1あるいは再加工データＭ2が２次ユーザ端末装置５内に保存される場合，記録媒体１２に複写される場合あるいは通信ネットワーク８を経由して３次ユーザ６に転送される場合には、著作権管理プログラムＰにより第４秘密鍵Ｋs4に基づいて第５秘密鍵Ｋs5が生成され、Ｋs5＝Ｐ（Ｋs4）
それらのデータは著作権管理プログラムＰにより第５秘密鍵Ｋs5を用いて暗号化される。
Ｃm1ks5＝Ｅ（Ｋs5，Ｃm1）
Ｃm2ks5＝Ｅ（Ｋs5，Ｃm2）
【０１８５】
なお、共通の著作権管理プログラムＰが、第４秘密鍵Ｋs4を用いて第５秘密鍵Ｋs5を生成し、生成された第５秘密鍵Ｋs5を用いて以後の暗号化／復号化を行うようにすることもできる。
【０１８６】
この実施例において、第４の秘密鍵を生成する著作権管理プログラムは全データベース組織において共通のものであるから、どのデータベース組織においても、１次ユーザデータ及び第１の秘密鍵が変更されない限り同一の原データに対しては同一の第４の秘密鍵が生成される。
【０１８７】
この実施例における、共通の著作権管理プログラムは著作権管理センタ１８から供給されるが、各ユーザ端末装置内のＲＯＭに内蔵、あるいはデータベースを利用するためのソフ

トウェアに内蔵してもよい。

【０１８８】

［実施例１２］次に説明する実施例１２では、複数のデータベースからユーザの要求に応じて供給される複数の原データを組み合わせて新しいデータを作成する実施例であり、この実施例においては暗号鍵方式として秘密鍵方式が採用される。

【０１８９】

図５において、１９，２０，２１はテキストデータ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ，音声データあるいは映像データが格納された第１，第２及び第３のデータベース，４は１次ユーザ端末装置，５は２次ユーザ端末装置，６は３次ユーザ端末装置，７はｎ次ユーザ端末装置，１０はデータ著作権を管理する著作権管理センタであり、８は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等である通信ネットワークである。

【０１９０】

これらのうち第１，第２及び第３データベース１９，２０，２１，著作権管理センタ１０，１次ユーザ端末装置４，２次ユーザ端末装置５，３次ユーザ端末装置６及びｎ次ユーザ端末装置７は通信ネットワーク８によって相互に接続可能とされている。

【０１９１】

このシステムを利用する各ユーザは予め各々のデータベース組織に登録をしておく必要がある。また、この登録の際に各データベース組織の利用ソフトウェアがユーザに対して供給される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアプログラムが含まれている。これらのデータベース組織利用ソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマスクＲＯＭ，ＥＰＲＯＭ，ＥＥＰＲＯＭ等に格納することも可能である。

【０１９２】

また、このシステムにおいてはユーザ側で秘密鍵を生成するためにユーザ端末装置に暗号鍵生成アルゴリズムが格納されるが、この暗号鍵生成アルゴリズム自身は必ずしも秘密のものではないため、各々のデータベース組織利用ソフトウェアに内蔵させてもよい。なお、広告付等の無料で供給される原データの場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置から各データベース及び著作権管理センタへ要求を行う経路であり、１点鎖線で示された経路は各データベース及び著作権管理センタから各ユーザ端末装置へ利用形態に対応する許可情報、著作権管理プログラム及び暗号鍵が転送される経路である。

【０１９３】

この実施例においては原データ毎に異なる秘密鍵及び著作権管理プログラムが使用されるが、これらは予め各データベース及び著作権管理センタに保管されている。

【０１９４】

第１データベース１９には、第１原データM1が暗号化されていない状態で保管されており、１次ユーザが１次ユーザ端末装置４を利用して第１データベース１９にアクセスすると、データメニューが転送される。

【０１９５】

データメニューが転送されると１次ユーザはデータメニュー検索を行い第１原データM1を選択し、１次ユーザ端末装置４を利用して、通信ネットワーク８を経由して第１データベース１９に対して、原データ名あるいは原データ番号を指定して第１原データM1の供給を申し込むがこのときに１次ユーザ情報Ｉu1を提示する。

【０１９６】

１次ユーザから第１原データM1の利用申し込みを受けた第１データベース１９は、利用申込を受けた第１の原データM1を第１秘密鍵Ｋs1を用いて暗号化し、Ｃm1ks1＝Ｅ（Ｋs1，M1）

１次ユーザ端末装置４に供給する。
【０１９７】
第２データベース２０には、第２原データM2が暗号化されていない状態で保管されており、１次ユーザが１次ユーザ端末装置４を利用して第２データベース２０にアクセスすると、データメニューが転送される。
【０１９８】
データメニューが転送されると１次ユーザはデータメニュー検索を行い第２原データM2を選択し、１次ユーザ端末装置４を利用して、通信ネットワーク８を経由して第２データベース２０に対して、原データ名あるいは原データ番号を指定して第２原データM2の供給を申し込むがこのときに１次ユーザ情報Ｉu1を提示する。
【０１９９】
１次ユーザから第２原データM2の利用申し込みを受けた第２データベース２０は、利用申込を受けた第２原データM2を第２秘密鍵Ｋs2を用いて暗号化し、Ｃm2ks2＝Ｅ（Ｋs2，M2）
１次ユーザ端末装置４に供給する。
【０２００】
第３データベース２１には、第２原データM3が暗号化されていない状態で保管されており、１次ユーザが１次ユーザ端末装置４を利用して第３データベース２１にアクセスすると、データメニューが転送される。
【０２０１】
データメニューが転送されると１次ユーザはデータメニュー検索を行い第３原データM3を選択し、１次ユーザ端末装置４を利用して、通信ネットワーク８を経由して第３データベース２２に対して、原データ名あるいは原データ番号を指定して第３原データM3の供給を申し込むがこのときに１次ユーザ情報Ｉu1を提示する。
【０２０２】
１次ユーザから第３原データM3の利用申し込みを受けた第３データベース２１は、利用申込を受けた第３原データM3を第３秘密鍵Ｋs3を用いて暗号化し、Ｃm3ks3＝Ｅ（Ｋs3，M3）
１次ユーザ端末装置４に供給する。
【０２０３】
暗号化第１，第２，第３原データＣm1ks1，Ｃm2ks2，Ｃm3ks3を供給された１次ユーザは、１次ユーザ端末装置４を利用して暗号化第１，第２，第３の原データＣm1ks1，Ｃm2ks2，Ｃm3ks3を１次利用するために通信ネットワーク８を経由して、原データ名あるいは原データ番号を指定して、著作権管理センタ１０に対して１次利用申込を行う。
【０２０４】
１次ユーザからの暗号化第１，第２，第３原データＣm1ks1，Ｃm2ks2，Ｃm3ks3の１次利用申し込みを受けた著作権管理センタ１０は、第１原データM1の暗号鍵である第１秘密鍵Ｋs1とともに第１著作権管理プログラムＰ1，第２原データM2の暗号鍵である第２秘密鍵Ｋs2とともに第２著作権管理プログラムＰ2、第３原データM3の暗号鍵である第３秘密鍵Ｋs3とともに第３著作権管理プログラムＰ3を１次ユーザ端末装置４に供給する。
【０２０５】
これらの著作権管理プログラムＰ1，Ｐ2，Ｐ3には暗号アルゴリズムを有する暗号プログラムが各々含まれており、これらの暗号プログラムにより新しい秘密鍵の生成及びデータの復号／暗号化が行われる。なお、これらの暗号アルゴリズムを各々第１，第２，第３秘密鍵Ｋs1，Ｋs2，Ｋs3に依存するものにしておけば、第１，第２，第３著作権管理プログラムＰ1，Ｐ2，Ｐ3を各第１，第２，第３原データM1，M2，M3に固有のものとすることができる。
【０２０６】
第１，第２，第３の秘密鍵Ｋs1，Ｋs2，Ｋs3を受け取った１次ユーザ端末装置４は、これらの秘密鍵を用いて暗号化された第１，第２，第３の各原データＣm1ks1，Ｃm2ks2，Ｃm3

ks3を復号化して、M1＝D（Ks1，Cm1ks1）
M2＝D（Ks2，Cm2ks2）
M3＝D（Ks3，Cm3ks3）
復号化された各原データM1，M2，M3をそのままあるいは加工して利用する。また、第１著作権管理プログラムP1が第１秘密鍵Ks1に基づいて第４の秘密鍵Ks4を、第２著作権管理プログラムP2が第２秘密鍵Ks2に基づいて第５秘密鍵Ks5を、第３著作権管理プログラムP3が第３の秘密鍵Ks3に基づいて第６秘密鍵Ks6を、各々生成する。
Ks4＝P1（Ks1）
Ks5＝P2（Ks2）
Ks6＝P3（Ks3）

【０２０７】
各原データM1，M2，M3あるいは加工データM4，M5，M6が１次ユーザ端末装置４内に保存される場合、記録媒体１１に複写される場合、通信ネットワーク８を経由して２次ユーザ端末装置５に転送される場合には、第１の原データM1あるいは加工データM4が第１著作権管理プログラムP1により第４秘密鍵Ks4を用いて、第２の原データM2あるいは加工データM5が第２著作権管理プログラムP2により第５秘密鍵Ks5を用いて、第３の原データM3あるいは加工データM6が第３著作権管理プログラムP3により第６秘密鍵Ks6を用いて、各々暗号化される。
Cm1ks4＝E（Ks4，M1）
Cm2ks5＝E（Ks5，M2）
Cm3ks6＝E（Ks6，M3）
Cm4ks4＝E（Ks4，M4）
Cm5ks5＝E（Ks5，M5）
Cm6ks6＝E（Ks6，M6）

【０２０８】
第４，第５，第６秘密鍵Ks4，Ks5，Ks6によって暗号化された原データCm1ks4，Cm2ks5，Cm3ks6あるいは暗号化された加工データCm4ks4，Cm5ks5，Cm6ks6は第１，第２，第３の原データ名あるいは原データ番号及び１次ユーザデータIu1とともに、記録媒体１１に複写されて、あるいは通信ネットワーク８を経由して２次ユーザ端末装置５に転送される。

【０２０９】
暗号化された第１，第２，第３の原データCm1ks4，Cm2ks5，Cm3ks6あるいは暗号化された加工データCm4ks4，Cm5ks5，Cm6ks6を供給された２次ユーザ端末装置５においては、原データ名あるいは原データ番号を指定することにより、第１，第２，第３の原データM1，M2，M3あるいは加工データMの２次利用を著作権管理センタ１０に申し込む。

【０２１０】
２次ユーザ端末装置５から第１，第２，第３の原データM1，M2，M3あるいは加工データM4，M5，M6の２次利用申込を受けた著作権管理センタ１０は、第１の原データ名から第１秘密鍵Ks1及び第１著作権管理プログラムP1を探し出し、第２の原データ名あるいは原データ番号から第２秘密鍵Ks2及び第２著作権管理プログラムP2を探し出し、第３の原データ名から第３秘密鍵Ks3及び第３著作権管理プログラムP3を探し出し、第１著作権管理プログラムP1が第１秘密鍵Ks1から第４秘密鍵Ks4を生成し、第２著作権管理プログラムP2が第２秘密鍵Ks2から第５秘密鍵Ks5を生成し、第３著作権管理プログラムP3が第３秘密鍵から第６の秘密鍵Ks6を生成し、Ks4＝P1（Ks1）
Ks5＝P2（Ks2）
Ks6＝P3（Ks3）
第１，第２，第３の著作権管理プログラムP1，P2，P3とともに２次ユーザ端末装置５に供給する。

【０２１１】
第４，第５，第６秘密鍵Ks4，Ks5，Ks6と第１，第２，第３著作権管理プログラムP1

，Ｐ2，Ｐ3を受け取った２次ユーザ端末装置５では、暗号化された第１の原データＣm1ks4あるいは加工データＣm4ks4が第１著作権管理プログラムＰ1により第４秘密鍵Ｋs4を用いて、暗号化された第２の原データＣm2ks5あるいは加工データＣm5ks5が第２著作権管理プログラムＰ2により第５秘密鍵Ｋs5を用いて、暗号化された第３の原データＣm3ks6あるいは加工データＣm6ks6が第３著作権管理プログラムＰ3により第６秘密鍵Ｋs6を用いて、各々復号化され、M4＝Ｄ（Ｋs4，Ｃm4ks4）
M5＝Ｄ（Ｋs5，Ｃm5ks5）
M6＝Ｄ（Ｋs6，Ｃm6ks6）
復号化された各データM4，M5，M6をそのままあるいは加工して利用する。

【０２１２】

第１，第２，第３の原データM1，M2，M3あるいは加工データM4，M5，M6が２次ユーザ端末装置５内に保存される場合、記録媒体１２に複写される場合、通信ネットワーク８を経由して２次ユーザ端末装置６に転送される場合には、第１の原データM1あるいは加工データM4は第１著作権管理プログラムＰ1により第４秘密鍵Ｋs4を用いて、第２の原データM2あるいは加工データM5は第２著作権管理プログラムＰ2により第５秘密鍵Ｋs5を用いて、第３の原データM3あるいは加工データM6は第３著作権管理プログラムＰ3により第６秘密鍵Ｋs6を用いて、各々暗号化される。

【０２１３】

なお、この場合第１著作権管理プログラムＰ1が第４秘密鍵Ｋs4に基づいて第７秘密鍵Ｋs7を、第２著作権管理プログラムＰ2が第５秘密鍵Ｋs5に基づいて第８秘密鍵Ｋs8を、第３著作権管理プログラムＰ3が第６秘密鍵Ｋs6に基づいて第９秘密鍵Ｋs9を各々生成するようにし、Ｋs7＝Ｐ1（Ｋs4）
Ｋs8＝Ｐ2（Ｋs5）
Ｋs9＝Ｐ3（Ｋs6）
これら第１，第２，第３の原データM1，M2，M3あるいは加工データM4，M5，M6が２次ユーザ端末装置５内に保存される場合，記録媒体１２に複写される場合，通信ネットワーク８を経由して３次ユーザ端末装置６に転送される場合には、それら第１，第２，第３の原データM1，M2，M3あるいは加工データM4，M5，M6は第１，第２，第３著作権管理プログラムＰ1，Ｐ2，Ｐ3により第７，第８，第９秘密鍵Ｋs7，Ｋs8，Ｋs9を用いて暗号化されるようにすることもできる。
Ｃm1ks7＝Ｅ（Ｋs7，M1）
Ｃm2ks8＝Ｅ（Ｋs8，M2）
Ｃm3ks9＝Ｅ（Ｋs9，M3）
Ｃm4ks7＝Ｅ（Ｋs7，M4）
Ｃm5ks8＝Ｅ（Ｋs8，M5）
Ｃm6ks9＝Ｅ（Ｋs9，M6）

【０２１４】

［実施例１３］次に説明する実施例１３は、実施例１２と同様に複数のデータベースからユーザの要求に応じて供給される複数の原データを利用して新しいデータを作成する実施例であり、この実施例においては暗号鍵方式として秘密鍵方式が採用される。また、暗号化／復号化に用いられる暗号鍵の生成に実施例７及び実施例１１の場合と同様にさらに著作権管理プログラムの使用回数が利用される。

【０２１５】

この実施例においては、著作権管理プログラムにはカウンタが付属しており、このカウンタがプログラムの使用回数あるいは原データの利用回数を計数し、そのカウンタ数Nを利用して第４，第５，第６秘密鍵Ｋs4，Ｋs5，Ｋs6が生成される。２次ユーザは各々の原データの原データ名あるいは原データ番号，１次ユーザデータとともにカウンタ数Nを提示して、データの２次利用を著作権管理センタ１０に申し込む。データの２次利用申込を受けた著作権管理センタ１０は、各々の原データ名あるいは原データ番号から第１，第２，第３秘密鍵Ｋs1，Ｋs2，Ｋs3を探し出し、第１，第２，第３著作権管理プログラムＰ1，

Ｐ2，Ｐ3により各々のデータの第１，第２，第３秘密鍵Ｋs1，Ｋs2，Ｋs3、１次ユーザＩu1及び第１，第２，第３カウンタ数Ｎ1，Ｎ2，Ｎ3から第４，第５，第６秘密鍵Ｋs4，Ｋs5，Ｋs6を生成し、第４，第５，第６著作権管理プログラムＰ1，Ｐ2，Ｐ3とともに２次ユーザに提供する。これ以外の点は、実施例１２のシステム構成と異なる点はないので具体的な説明は省略する。

【０２１６】

［実施例１４］１次ユーザが入手した原データをそのまま複写して２次ユーザに供給した場合にはそのデータに何等の価値も加えられていないため、そのデータに１次ユーザの著作権は発生しない。しかし、入手した原データから新しいデータを作成した場合、すなわち、入手した単一の原データから新しいデータを作成した場合及び入手した複数の原データから新しいデータを作成した場合には、新しいデータについて１次ユーザの２次的著作権が発生する。

【０２１７】

一方、加工に利用された原データにも原著作権者の著作権が存在しているため、加工データには原データの著作者の原著作権と加工を行った１次ユーザの２次的著作権とが存在することになる。著作権は単なる物権ではなく人格権の要素が強い権利であるため、著作者がその存在を強く主張することが多い。そのため、原データの加工が行われた場合であっても、加工データから原データあるいは著作権者を容易に特定できるようにすることが望ましい。

【０２１８】

これまでに実施例１～１３で説明したデータ著作権管理システムでは、原データあるいは加工データを暗号化することによってデータの著作権を管理しているが、このシステムではデータが原データであるのかあるいは加工データであるのか、また、加工データの中でどの部分が原データであり、どの部分が加工データであるのかが区別されることなくデータの著作権が管理されるため、加工データから原データあるいは著作権者を特定することはできない。

【０２１９】

これから説明する実施例１４ではデータを原著作権しか存在しない原データと原著作権に加えて２次的著作権も存在する加工データを区別できるとともに、原著作権と２次的著作権を明確に管理することができる。

【０２２０】

データの加工は加工用プログラムを利用して原データに改変を加えることによってなされるため、原データと加工内容（必要な場合はさらに加工用プログラム）が特定されることによって加工データが再現される。いいかえれば、原データと加工内容（必要な場合はさらに加工用プログラム）が特定されなければ加工データの再現は不可能である。実施例１４で説明する２次的著作権の管理は、原データと加工内容（必要な場合はさらに加工用プログラム）を特定し、これらを管理することによって行われる。

【０２２１】

単一の原データにより新しいデータを作成する場合には、原データＡを改変して加工データ「Ａ'」を得る場合、原データＡに１次ユーザがデータＸを付加することにより加工データ「Ａ＋Ｘ」を得る場合、原データＡを原データ要素Ａ1，Ａ2，Ａ3・・・に分割し配列をＡ3，Ａ2，Ａ1のように変更して加工データ「Ａ"」を得る場合、原データＡを原データ要素Ａ1，Ａ2，Ａ3・・・に分割し１次ユーザのデータＸをＸ1，Ｘ2，Ｘ3・・・に分割しこれらを配列して加工データ「Ａ1＋Ｘ1＋Ａ2＋Ｘ2＋Ａ3＋Ｘ3・・・」を得る場合等がある。これらの場合、原データの改変、原データの配列変更、原データと１次ユーザデータの組み合わせ、原データの分割及び１次ユーザデータとの組み合わせ、が各々２次的著作権の対象となり、これらの２次的著作権を保護する必要がある。なお、１次ユーザが付加したデータＸには１次ユーザの原著作権が存在することはいうまでもない。

【０２２２】

複数の原データを組み合わせることにより新しいデータを作成する場合には、原データＡ

，Ｂ，Ｃ・・・を単純に組み合わせて加工データ「Ａ＋Ｂ＋Ｃ・・・」を得る場合、原データＡ，Ｂ，Ｃ・・・に１次ユーザがデータＸを付加することにより加工データ「Ａ＋Ｘ」を得る場合、原データＡ，Ｂ，Ｃ・・・を原データ要素Ａ1，Ａ2，Ａ3・・・，Ｂ1，Ｂ2，Ｂ3・・・，Ｃ1，Ｃ2，Ｃ3・・・に分割し組み合わせて配列を変更し加工データ「Ａ1＋Ｂ1＋Ｃ1＋・・・＋Ａ2＋Ｂ2＋Ｃ2＋・・・＋Ａ3＋Ｂ3＋Ｃ3＋・・・」を得る場合、原データＡ，Ｂ，Ｃ・・・を原データ要素Ａ1，Ａ2，Ａ3・・・，Ｂ1，Ｂ2，Ｂ3・・・，Ｃ1，Ｃ2，Ｃ3・・・に分割し１次ユーザのデータＸ1，Ｘ2，Ｘ3・・・を組み合わせて配列を変更して加工データ「Ａ1＋Ｂ1＋Ｃ1＋Ｘ1＋・・・＋Ａ2＋Ｂ2＋Ｃ2＋Ｘ2＋・・・＋Ａ3＋Ｂ3＋Ｃ3＋Ｘ3＋・・・」を得る場合等がある。これらの場合も、複数の原データの組み合わせ、複数の原データと１次ユーザデータの組み合わせ、複数の原データの分割及び配列変更、分割された複数の原データと１次ユーザデータの組み合わせ、が各々２次的著作権の対象となり、これらの２次的著作権を保護する必要がある。また、１次ユーザが付加したデータＸ1，Ｘ2，Ｘ3・・・には１次ユーザの原著作権が存在することはいうまでもない。

【０２２３】

図６に示されたのは複数の原データＡ，Ｂ，Ｃを利用して新しいデータＤを作成する手法例である。この手法は原データＡ，Ｂ，Ｃから要素ａ，ｂ，ｃを抽出（カット）し、抽出された要素ａ，ｂ，ｃを貼り付けて（ペースト）１つのデータＤを合成するカットアンドペースト手法によってデータの加工を行うものである。

【０２２４】

ところで、原データ及び１次ユーザデータがデータであることは明白であるが、データの加工過程である原データの改変，原データの配列変更，原データと１次ユーザデータの組み合わせ，原データの分割及び１次ユーザデータとの組み合わせ，複数の原データの組み合わせ，複数の原データと１次ユーザデータの組み合わせ，複数の原データの分割及び配列変更，分割された複数の原データと１次ユーザデータの組み合わせもデータそのものである。

【０２２５】

これまでに説明した実施例１～１３では、データの著作権を原データあるいは加工データを暗号化することによってデータそのものの著作権を管理しているがこの他に、原データの配置関係及び加工手順等であるデータの加工過程もデータであることに着目すると、加工データに関する２次的著作権を原データに関する原著作者の１次著作権及び１次ユーザデータに関する１次ユーザの１次著作権に加えて加工過程データに関する１次ユーザの１次著作権を管理することによって保護することが可能となる。なお、加工過程や加工用プログラムを加工シナリオと呼ぶこともできる。

【０２２６】

すなわち、加工データを原データと１次ユーザデータと加工過程データとから構成するものとし、これらの原データ，１次ユーザデータ及び加工過程データを各々これまでに実施例１～１３で説明したデータ著作権管理システムによって管理することにより、原データとともに加工データの著作権を充分に管理することができる。なお、この場合データの加工において使用された加工用プログラムも必要ならばデータ著作権管理システムの管理対象とする。

【０２２７】

このデータの加工は原データをその原データに対応する加工プログラムを使用して加工することもできるが、原データを最近注目されているオブジェクト指向ソフトウェアとして取り扱うようにすれば、より容易な加工とよりよいデータ著作権管理を行うことができる。また、さらに進んでエージェント指向ソフトウェアを採用すれば、ユーザは労することなくデータの合成を行うことができる。

【０２２８】

エージェント指向ソフトウェアは、自律性・適応性・協調性を兼ね備えたプログラムであり、従来のソフトウェアのようにすべての作業手順を具体的に指示しなくても、ユーザの

一般的な指示のみに基づいてその自律性・適応性・協調性との特質により、ユーザの要求に応えることができる。このエージェントプログラムをデータ著作権管理システムの基本的なシステムの中に組み込み、ユーザのデータベース利用形態を監視させ、その結果得られた情報をデータベース側あるいは著作権管理センタ側で収集するように構成することにより、ユーザのデータベース利用傾向をデータベース側あるいは著作権管理センタ側が知ることができ、よりきめの細かい著作権管理を行うことができる。したがって、エージェントプログラム及びデータも著作権保護の対象となり、原データと同様に暗号化される。

【０２２９】

［実施例１５］著作物中には、著作権が存在しないものと著作権が存在するものとがあり、著作権が存在するものの中には、著作権の行使が行われるものと著作権の行使が行われないものがある。著作権が存在しない著作物としては法令によって著作権が存在しないものとされている著作物と著作権の期限が過ぎてしまったものがある。これらの著作権が存在しない著作物を除くすべての著作物には著作権が存在するが、著作権が存在する著作物には通常著作権の存在を主張する表示がなされており、この表示があることによって著作権の侵害に対する抑止効果が発揮される。このことは、著作物がデータである場合にも同様であって、著作権が存在するデータの場合には利用されるデータあるいはデータのファイルヘッダに著作権表示あるいは著作権者表示が行われることによってデータ著作権の侵害行為が抑止される。また、データに著作権が存在することを示す著作権フラグをファイルに付加し、ユーザ端末装置においてこのフラグを識別するようにすることにより、データ著作権の侵害行為を阻止することができる。

【０２３０】

しかしながら、このような著作権に関する表示がなされていたとしてもそのデータ著作物を利用するユーザが著作権の存在を無視した場合には著作権の侵害が行われる可能性がある。そのような場合に対処するために、これまで説明した実施例においてはデータを暗号化し、暗号化データを復号化するための復号鍵を管理し、復号化データが保存、複写、転送される場合には復号鍵とは異なる暗号鍵を用いて暗号化／復号化が行われる。そのような場合であっても、ユーザ端末装置の主記憶装置上にデータが存在している状態においてデータをユーザ端末装置の主記憶装置以外の記憶装置に転送することにより、復号鍵と異なる暗号鍵を用いることなくデータを保存，複写，転送する可能性を完全に否定することはできない。

【０２３１】

このような事態を防止するには、データ著作権利用ソフトウェアをユーザ端末装置の基本システムに組み込み、著作権行使の対象であるデータ著作物のファイルには著作権行使の属性を表示し、データ著作物の著作権行使属性についてユーザ端末装置の基本システムが監視し、著作権行使属性を有するデータ著作物はデータ著作権利用ソフトウェアによって管理されるようにすることが最善である。基本システムとしては、ユーザ端末装置がパーソナルコンピュータ等のコンピュータである場合にはＤＯＳ等のソフトウェアオペレーティングシステムであり、ユーザ端末装置が携帯情報端末装置あるいはＳＴＢ（セットトップボックス）である場合にはＲＯＭに内蔵されたハードウェアオペレーティングシステムである。なお、このオペレーティングシステムによるデータ著作権管理をより強固なものとするためには、データ著作権利用ソフトウェアはオペレーティングシステムのできるだけ上位のレベルに組み込むことが望ましい。

【０２３２】

ユーザ端末装置の内部における処理及びデータはすべてオペレーティングシステムの管理下におかれている。言い換えれば、オペレーティングシステムはユーザ端末装置の内部における処理及びデータをすべて把握することができる。したがって、ユーザの指示によるのではなくオペレーティングシステムが把握したデータの利用状況に応じて著作権管理プログラムが自動的にデータ著作権の管理を行うようにすることができ、このような構成によればユーザによるデータ著作権の利用が容易になるとともに、より完全なデータ著作権管理を行うことができる。また、暗号鍵，データ著作権情報あるいは著作権ラベル等を管

理する著作権管理プログラムはオペレーティングシステム自体が管理するシステム領域言い換えればユーザプログラムがアクセスすることができないシステム領域に保持されることが望ましい。

【０２３３】

しかし、この場合でもデータ著作物の一部のみが切りとられて利用されたような場合にはデータ著作権の管理が著しく困難になる。したがって、そのような状況をオペレーティングシステムが認識した場合には著作権管理プログラムにより切りとられた一部のデータに原データが有していた著作権情報及び著作権行使属性を付与するように構成することにより、切りとられた一部のデータのデータ著作権も管理する事が可能となる。また、切り取られたデータに元のデータ著作物の著作権を継承させるために、著作権管理プログラムによりその切り取られたデータと元のデータ著作物との間に親子関係のリンクを形成する。このようにしておけばユーザが複数の著作権付きデータからそれぞれ希望する部分を切り出して取り込み新しいデータを作成した場合にも、その新しいデータに元の各データ著作権物の著作権を継承させることができる。

【０２３４】

［実施例１６］著作権は財産権の一種であるから、著作権を利用する場合には当然のこととして使用料支払いの問題が発生する。また、秘密鍵の提供，著作権管理プログラムの提供等のサービスは有料で行われる必要がある。これらの料金支払の最も簡易な方法は請求書の発行と支払を組み合わせたものであるが、この方法は使用料の支払が直接に行われる反面、作業が煩雑な上、不払い等の事故の可能性もある。また、通信回線事業者が行う料金徴収代行方法もあり、この方法は料金徴収作業を通信回線事業者が行うため簡便であり、不払い等の事故の可能性が低い反面、使用料の徴収が直接に行われないため、料金徴収代行手数料の支払が必要となる。

【０２３５】

これらの問題を解決する方法として、ディジタルキャッシュを利用する方法がある。このディジタルキャッシュはディジタルデータであり、暗号化され使用される。

【０２３６】

［実施例１７］さらに、以上説明したデータ著作権管理システムの構成はデータの流通だけではなくディジタルキャッシュの流通に対しても適用可能である。これまでに種々提案されているディジタルキャッシュシステムは秘密鍵方式で暗号化ディジタルキャッシュデータを銀行預金口座あるいはクレジット会社のキャッシングサービスから転送してＩＣカードに保存しており、入出力用の端末装置を利用して支払を行う。このＩＣカードを電子財布として利用するディジタルキャッシュシステムは商店等入出力用の端末装置が設置されている場所であればどこでも使用可能である反面、入出力用の端末装置がない場所、例えば家庭等、では使用不可能である。

【０２３７】

ところで、ディジタルキャッシュは暗号化データであるからＩＣカード以外にも暗号化データを保存することができ、かつ支払先にデータを転送することができる装置であればどのようなものでもディジタルキャッシュデータを保存する電子財布として利用することができる。具体的に電子財布として利用可能なユーザ端末装置としては、パーソナルコンピュータ，インテリジェントテレビジョン装置、携帯情報端末装置（Personal Digital Assistant ＰＤＡ），ＰＨＳ（Personal Hadyphone System）等の携帯電話器，インテリジェント電話機，入出力機能を有するＰＣカード等がある。

【０２３８】

このような端末装置をディジタルキャッシュ用の電子財布として利用することによる取引は、これまでに説明したデータ著作権管理システムの構成におけるデータベース１を顧客側銀行に、１次ユーザ端末装置４を顧客に、２次ユーザ端末装置５を小売店に、著作権管理センタ１８を小売店側銀行に、３次ユーザ端末装置６を卸売またはメーカに置き換えることにより実現される。

【０２３９】

また、ディジタルキャッシュは単なるデータではなくデータと機能が結びついたオブジェクト（object）として処理されることが望ましい。ディジタルキャッシュの取り扱いにおいては共通のディジタルキャッシュフォーム，所有者固有の未記入ディジタルキャッシュフォーム，所有者固有のディジタルキャッシュフォームの書き込み欄，金額であるディジタルキャッシュデータ，ディジタルキャッシュ取り扱いの指示，金額が書き込まれた所有者固有のディジタルキャッシュフォームがある。一方、オブジェクト指向プログラミング（object-oriented programming）においては、オブジェクト，クラス（class），スロット（slot），メッセージ（message），インスタンス（instance）との概念が使用される。これらの対応関係は、共通のディジタルキャッシュフォームがオブジェクトとなり、所有者固有の未記入ディジタルキャッシュフォームがクラスとなり、所有者固有のディジタルキャッシュフォームの記入欄がスロットとなり、ディジタルキャッシュ取り扱いの指示がメッセージとなり、金額が記入された所有者固有のディジタルキャッシュフォームがインスタンスとなる。金額等からなるディジタルキャッシュデータは引数（argument）として使用され、メッセージによりインスタンス変数（instance variable）とも呼ばれるスロットに引き渡されて格納されることにより、金額等が更新されたディジタルキャッシュである新しいインスタンスが作られる。

【０２４０】

オブジェクト化されたディジタルキャッシュについて、図６を用いて具体的に説明する。この図において、２３，２５，２７は顧客端末装置に保存されている金額が書き込まれた顧客固有のディジタルキャッシュフォーム，２９は小売店端末装置に保存されている金額が記入された小売店固有のディジタルキャッシュフォーム，２４，２６，２８は各々の顧客の取引銀行にある預金口座である。

【０２４１】

顧客２３はディジタルキャッシュを使用するために、預金口座２４から必要な金額を引き出し、端末装置に保存されているディジタルキャッシュフォーム２３にディジタルキャッシュ引出金データ３１を引き渡す。この場合、ディジタルキャッシュフォーム２３にはディジタルキャッシュ残金データ３０が既に記入されているのが普通であるため、ディジタルキャッシュフォーム２３はクラスではなくインスタンスである。ディジタルキャッシュ引出金データ３１はディジタルキャッシュ残金データ３０に対して加算することを指示するメッセージによりディジタルキャッシュフォーム２３の記入欄であるスロットに引数として引き渡され、ディジタルキャッシュフォーム２３のディジタルキャッシュ残金データ３０にディジタルキャッシュ引出金データ３１が加算されてディジタルキャッシュフォーム２３の記入欄の金額が変更された新しいインスタンスが作られる。

【０２４２】

顧客が小売店に対して支払を行う場合には、支払金額に相当するディジタルキャッシュ支払金データ３２をディジタルキャッシュフォーム２３の記入欄の金額から減算することを指示するメッセージによりディジタルキャッシュフォーム記入欄であるスロットに引数として引き渡され、ディジタルキャッシュフォーム２３のディジタルキャッシュ残金データ３０及びディジタルキャッシュ引出金データ３１からディジタルキャッシュ支払金データ３２が減算されてディジタルキャッシュフォーム２３の記入欄の金額が変更された新しいインスタンスが作られる。また、ディジタルキャッシュ支払金データ３２が小売店固有のディジタルキャッシュフォーム２９に引き渡される。

【０２４３】

同様な引出処理及び支払処理が他の顧客のディジタルキャッシュフォーム２５及び２７でも行われ、ディジタルキャッシュフォーム２５からはディジタルキャッシュ支払金データ３３が、ディジタルキャッシュフォーム２７からはディジタルキャッシュ支払金データ３４が小売店固有のディジタルキャッシュフォーム２９に引き渡される。小売店固有のディジタルキャッシュフォーム２９の場合にもディジタルキャッシュ残金データ３５が既に記入されているのが普通である。ディジタルキャッシュ支払金データ３２，ディジタルキャッシュ支払金データ３３及びディジタルキャッシュ支払金データ３４はディジタルキャッ

シュ残金データ３５に対して加算することを指示するメッセージによりディジタルキャッシュフォーム２９の記入欄であるスロットに引数として引き渡され、ディジタルキャッシュ残金データ３５にディジタルキャッシュ支払金データ３２，ディジタルキャッシュ支払金データ３３及びディジタルキャッシュ支払金データ３４が加算されて、ディジタルキャッシュフォーム記入欄の金額が変更された新しいインスタンスが作られる。

【０２４４】

通常のオブジェクト指向プログラミングにおいては、引数がメッセージによりスロットに引き渡されることにより新しいインスタンスが作られ、新しく作られたインスタンス全体引き渡されることはない。しかし、ディジタルキャッシュの場合には安全上暗号技術が使用されるから、支払元においてディジタルキャッシュ支払金データが記入されたインスタンスを作り、このインスタンスを暗号化して支払先に引き渡すこともできる。

【０２４５】

ディジタルキャッシュを通信ネットワークを経由して転送することにより行われる取引システムの実施例を図７を用いて説明する。この実施例は図４に示されたシステム構成を利用したものであり、この図において、３６は顧客，３７は顧客３６の取引銀行，３８は小売店，３９は小売店３８の取引銀行，４０はメーカ，４１はメーカ４０の取引銀行，８は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワークであり、顧客３６，顧客の取引銀行３７，小売店３８，小売店の取引銀行３９，メーカ４０及びメーカの取引銀行４１は通信ネットワーク８によって相互に接続可能とされている。このシステムにおいて、顧客３６は銀行の他にキャッシングサービスを行うクレジット会社を利用することが可能であり、小売店とメーカとの間に適当な数の卸売り店を介在させることが可能である。また、４２及び４３はディジタルキャッシュデータが格納されるＩＣカードあるいはＰＣカードであり、通信ネットワークを利用しない場合に使用される。なお、この図において、破線で示されたのは暗号化されたディジタルキャッシュデータの経路であり、実線で示されたのは顧客，小売店あるいはメーカから銀行への要求の経路であり、１点鎖線で示されたのは各銀行からの秘密鍵の経路である。さらに、この実施例では暗号鍵として顧客側銀行３７が用意する第１秘密鍵及び顧客が生成する第２秘密鍵，小売店が生成する第３秘密鍵及びメーカが生成する第４秘密鍵が用いられる。この実施例では顧客側銀行３７，小売り店側銀行３９，メーカ側銀行４１を別個のものとして説明したが、これらを一括して金融システムとして考えてもよい。

【０２４６】

ディジタルキャッシュデータを暗号化／復号化するディジタルキャッシュ管理プログラムＰは顧客３６に予め配布され、ユーザ端末装置に保存されている。また、ディジタルキャッシュ管理プログラムＰは銀行との取引が行われる毎にデータとともに転送されるようにすることもできる。さらに、ディジタルキャッシュ管理プログラムＰは全銀行において共通するものとすることが望ましい。顧客３６はユーザ端末装置を利用して通信ネットワーク８を経由して金額を指定することにより、顧客側銀行３７に預金口座からの預金の引出の申込を行うがこのときに顧客３６の顧客情報Ｉcを提示する。

【０２４７】

顧客３６から預金引出の申込を受けた顧客側銀行３７は、第１秘密鍵Ｋs1を選択あるいは作成し、引出金額のディジタルキャッシュデータM0をこの第１秘密鍵Ｋs1で暗号化し、

Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）

暗号化ディジタルキャッシュデータＣm0ks1及び復号鍵である第１秘密鍵Ｋs1を顧客３６に転送するとともに、顧客情報Ｉc及び第１秘密鍵Ｋs1を保管する。この場合、第１秘密鍵Ｋs1は顧客側銀行３７が予め用意したものから選択してもよいが、顧客が引き出し時に顧客情報Ｉcを提示し、ディジタルキャッシュ管理プログラムＰにより、提示された顧客情報Ｉcに基づいて作成することもできる。

Ｋs1＝Ｐ（Ｉc）

このようにすれば、第１秘密鍵Ｋs1を顧客３６に固有のものとすることができるばかりでなく、顧客３６に対して第１秘密鍵Ｋs1を転送する必要がないため、システムの安全性が

高くなる。また、第１秘密鍵Ｋs1は顧客側銀行３７の銀行情報Ｉbsあるいは銀行情報Ｉbsと作成日時に基づいて作成することもできる。

【０２４８】

暗号化ディジタルキャッシュデータＣm0ks1及び第１秘密鍵Ｋs1を転送された顧客３６は、ディジタルキャッシュ管理プログラムＰにより、顧客情報Ｉc，第１秘密鍵Ｋs1の何れか１つあるいは双方に基づいて第２秘密鍵Ｋs2を生成し、Ｋs2＝Ｐ（Ｉc）

生成された第２秘密鍵Ｋs2がユーザ端末装置内に保存される。また、顧客３６はディジタルキャッシュ管理プログラムＰにより暗号化ディジタルキャッシュデータＣm0ks1を第１秘密鍵Ｋs1を用いて復号化してＭ0＝Ｄ（Ｋs1，Ｃm0ks1）

内容を確認するが、内容が確認された復号化ディジタルキャッシュデータＭ0が電子財布であるユーザ端末装置内に保存される場合には、生成された第２秘密鍵Ｋs2を用いてディジタルキャッシュ管理プログラムＰにより暗号化される。

Ｃm0ks2＝Ｅ（Ｋs2，Ｍ0）

また、このときに第１秘密鍵Ｋs1が廃棄される。

【０２４９】

小売店３８から物品の購入を希望する顧客３６は、ディジタルキャッシュ管理プログラムＰにより電子財布であるユーザ端末装置に保存されている暗号化ディジタルキャッシュデータＣm0ks2を第２秘密鍵Ｋs2を用いて復号化し、Ｍ0＝Ｄ（Ｋs2，Ｃm0ks2）

必要な金額に対応するディジタルキャッシュデータＭ1をディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化し、Ｃm1ks2＝Ｅ（Ｋs2，Ｍ1）

通信ネットワーク８を介して暗号化ディジタルキャッシュデータＣm1ks2を小売店３８の電子財布であるユーザ端末装置に転送することにより、支払を行う。このときに、顧客情報Ｉcも小売店３８のユーザ端末装置に転送される。また、残額ディジタルキャッシュデータＭ2はディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化され、Ｃm2ks2＝Ｅ（Ｋs2，Ｍ2）

顧客３６のユーザ端末装置内に保存される。

【０２５０】

暗号化ディジタルキャッシュデータＣm1ks2及び顧客情報Ｉcを転送された小売店３８は、転送された暗号化ディジタルキャッシュデータＣm1ks2及び顧客情報Ｉcをユーザ端末装置に保存するとともに、内容を確認するために通信ネットワーク８を経由して小売店側銀行３９に顧客情報Ｉcを提示して、復号鍵である第２秘密鍵Ｋs2の転送を依頼する。小売店３８から第２秘密鍵Ｋs2の転送依頼を受けた小売店側銀行３９は、第２秘密鍵Ｋs2の転送依頼とともに顧客情報Ｉcを顧客側銀行３７に転送する。小売店側銀行３９から第２秘密鍵Ｋs2の転送依頼を転送された顧客側銀行３７は、第２秘密鍵Ｋs2が顧客情報Ｉcのみに基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉcに基づいて第２秘密鍵Ｋs2を生成し、第２秘密鍵Ｋs2が顧客情報Ｉcと第１秘密鍵Ｋs1に基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉcと第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、生成された第２秘密鍵Ｋs2を小売店側銀行３９に転送する。顧客側銀行３７から第２秘密鍵Ｋs2を転送された小売店側銀行３９は、通信ネットワーク８を経由して第２秘密鍵Ｋs2を小売店３８に転送する。

【０２５１】

第２秘密鍵Ｋs2を転送された小売店３８は、ディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化ディジタルキャッシュデータＣm1ks2を復号化し、Ｍ1＝Ｄ（Ｋs2，Ｃm1ks2）

金額を確認の上、商品を顧客３６に発送する。なお、この場合小売店３６が小売店側銀行３９ではなく顧客側銀行３７に直接に第２秘密鍵Ｋs2の転送を依頼するようにすることもできる。

【０２５２】

小売店３８が収受したディジタルキャッシュを小売店側銀行３９の口座に入金する場合には、通信ネットワーク８を経由して小売店側銀行３９に暗号化ディジタルキャッシュデー

タＣm1ks2とともに顧客情報Ｉcを転送する。暗号化ディジタルキャッシュデータＣm1ks2と顧客情報Ｉcを転送された小売店側銀行３９は、顧客情報Ｉcを転送することにより第２秘密鍵Ｋs2の転送を顧客側銀行２４に対して依頼する。小売店側銀行３９から第２秘密鍵Ｋs2の転送を依頼された顧客側銀行３７は、第２秘密鍵Ｋs2が顧客情報Ｉcのみに基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉcに基づいて第２秘密鍵Ｋs2を生成し、第２秘密鍵Ｋs2が顧客情報Ｉcと第１秘密鍵Ｋs1に基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉcと第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、生成された第２秘密鍵Ｋs2を小売店側銀行３９に転送する。顧客側銀行３７から第２秘密鍵Ｋs2を転送された小売店側銀行３９は、ディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化ディジタルキャッシュデータＣm1ks2を復号化し、Ｍ1＝Ｄ（Ｋs2，Ｃm1ks2）

復号化ディジタルキャッシュデータＭ1を小売店３９の銀行口座に入金する。

【０２５３】

一般的な取引システムにおいては、小売店３８はメーカ４０あるいはメーカ４０と小売店３８の間に介在する卸売り店から商品を仕入れ、顧客３６に販売する。そのため、顧客３６と小売店３８との間に存在するのと同様の取引形態が小売店３８とメーカ４０との間にも存在する。この小売店３８とメーカ４０との間で行われるディジタルキャッシュの取り扱いは、顧客３６と小売店３８との間で行われるディジタルキャッシュの取り扱いと基本的な相違はないため、煩雑さをさけるため説明を省略する。

【０２５４】

このディジタルキャッシュシステムにおける、ディジタルキャッシュの取扱いはすべて銀行を介在させて行われるため、顧客側銀行にディジタルキャッシュの取扱いに関する金額，日付，秘密鍵要求者情報等の情報を保存しておくことにより、ディジタルキャッシュの残高及び使用履歴を把握することができる。また、ディジタルキャッシュデータを保存する電子財布であるユーザ端末装置が紛失あるいは破損により使用不能となった場合でも、顧客側銀行に保存されている使用残高及び使用履歴に基づきディジタルキャッシュを再発行することが可能である。なお、ディジタルキャッシュの安全性を高めるためにディジタルキャッシュデータにディジタル署名を付けることが望ましい。この実施例において、ディジタルキャッシュには顧客情報が付加されており、この顧客情報はディジタル署名付とされることがある。つまり、この実施例においてディジタルキャッシュは顧客を振り出し人とする手形決済システムとしての機能も有する。さらに、このシステムは従来紙を用いて行われている国際貿易における信用状、船積み有価証券等による各種決済システムにも応用することができる。

【０２５５】

［実施例１８］実施例１７で説明したディジタルキャッシュシステムにおけるディジタルキャッシュの取扱いはすべて銀行を介在させて行われるが、この他に銀行を介在させることなくディジタルキャッシュを取り扱うこともできるので、次に、銀行を介在させないディジタルキャッシュシステムを説明する。このディジタルキャッシュシステムにおいては、ディジタルキャッシュデータを暗号かする暗号鍵として公開鍵及び専用鍵が用いられ、実施例１７で用いられる秘密鍵Ｋs及び顧客情報Ｉcは用いられない。したがって、この実施例においてディジタルキャッシュは貨幣と同様な形態で使用される。これら以外の点は、実施例１７のシステム構成と異なる点はないので具体的な説明は省略する。

【０２５６】

このディジタルキャッシュシステムに関係する各銀行，顧客，小売店，メーカでディジタルキャッシュを受け取る側になる者は、各々公開鍵及び専用鍵を用意する。その中の公開鍵は支払予定者に予め送付しておくことも、あるいは取引を行う前に支払者に送付することもできるが、ここでは支払予定者に予め配布されているものとして説明する。顧客３６は端末装置を利用して通信ネットワーク８を経由して金額を指定することにより、顧客側銀行３７に預金口座からの預金の引出の申込を行う。顧客３６から預金引出の申込を受けた顧客側銀行３７は、引出金額のディジタルキャッシュデータＭ0を予め送付されている

顧客公開鍵Ｋbcを用いてディジタルキャッシュ管理プログラムＰにより暗号化し、Ｃm0kbc＝Ｅ（Ｋbc，Ｍ0）
暗号化ディジタルキャッシュデータＣm0kbcを顧客３６に転送する。
【０２５７】
暗号化ディジタルキャッシュデータＣm0kbcを転送された顧客３６は、ディジタルキャッシュ管理プログラムＰにより顧客公開鍵Ｋbcに対応する顧客専用鍵Ｋvcを用いて復号化し、Ｍ0＝Ｄ（Ｋvc，Ｃm0kbc）
内容を確認し、端末装置内に残金額のデータＭ1がある場合には残金額のデータをＭ2（＝Ｍ0＋Ｍ1）に変更し、金額が変更されたディジタルキャッシュデータＭ2をディジタルキャッシュ管理プログラムＰにより顧客公開鍵Ｋbcで暗号化して、Ｃm2kbc＝Ｅ（Ｋbc，Ｍ2）
端末装置内に保存する。
【０２５８】
小売店３８から物品の購入を希望する顧客３６は、端末装置に保存されている暗号化ディジタルキャッシュデータＣm2kbcをディジタルキャッシュ管理プログラムＰにより顧客専用鍵Ｋvcを用いて復号化し、Ｍ2＝Ｄ（Ｋvc，Ｃm2kbc）
必要な金額に対応するディジタルキャッシュデータＭ3を予め送付されている小売店公開鍵Ｋbsを用いてディジタルキャッシュ管理プログラムＰにより暗号化し、Ｃm3kbs＝Ｅ（Ｋbs，Ｍ3）
通信ネットワーク８を介して小売店３８の端末装置に転送することにより、支払を行う。
また、残額ディジタルキャッシュデータＭ4（＝Ｍ2－Ｍ3）はディジタルキャッシュ管理プログラムＰにより顧客公開鍵Ｋbcで暗号化されて、Ｃm4kbc＝Ｅ（Ｋbc，Ｍ4）
端末装置内に保存される。
【０２５９】
暗号化ディジタルキャッシュデータＣm3kbsを転送された小売り店３８は、ディジタルキャッシュ管理プログラムＰにより小売店公開鍵Ｋbsに対応する小売店専用鍵Ｋvsを用いて復号化し、Ｍ3＝Ｄ（Ｋvs，Ｃm3kbs）
内容を確認し、端末装置内に残金額のデータＭ5がある場合には残金額のデータをＭ6（＝Ｍ5＋Ｍ3）に変更し、金額が変更されたディジタルキャッシュデータＭ6をディジタルキャッシュ管理プログラムＰにより小売店公開鍵Ｋbsで暗号化して、Ｃm6kbs＝Ｅ（Ｋbs，Ｍ6）
端末装置内に保存する。
【０２６０】
メーカ４０に対する商品仕入代金の決済を行おうとする小売店３８も同様な方法で決済を行う。さらには、顧客３６の顧客側銀行３７への入金、小売店３６の小売店側銀行３９への入金、メーカ４０のメーカ側銀行４１への入金も同様な方法で行われる。
【０２６１】
以上説明した実施例１７及び実施例１８においては、ディジタルキャッシュシステムを実現するために図４を用いて説明されたデータ著作権管理システムの構成を応用し、さらに実施例１７においては顧客情報を利用し、用いられる秘密鍵を変化させ、実施例１８においては公開鍵及び専用鍵を用いている。しかし、ディジタルキャッシュシステムを実現させるシステムの構成として、この他の著作権管理システムの構成すなわち、図１に示されたデータ著作権管理システム、図２に示されたデータ著作権管理システム、図３に示されたデータ著作権システム、図５に示されたデータ著作権システムの何れの構成も応用可能である。また、その場合に用いられる暗号鍵方式としては、変化しない秘密鍵、公開鍵と専用鍵、秘密鍵と公開鍵と専用鍵の組み合わせ、鍵の２重化、という実施例１から実施例１３で説明した暗号鍵方式の何れもが応用可能である。
【０２６２】
［実施例１９］これまでは従来の音声電話器にテレビジョン映像を付加したものに過ぎなかったテレビジョン会議システムが、最近はコンピュータシステムに組み込まれることに

より音声あるいは映像の品質が向上したばかりでなく、コンピュータ上のデータも音声及び映像と同時に扱うことができるように進化している。このような中で、テレビジョン会議参加者以外の盗視聴による使用者のプライバシー侵害及びデータの漏洩に対するセキュリティーは秘密鍵を用いた暗号化システムによって保護されている。しかし、テレビジョン会議参加者自身が入手する会議内容は復号化されたものであるため、テレビジョン会議参加者自身が会議内容を保存し、場合によっては加工を行い、さらにはテレビジョン会議参加者以外の者に配布する２次的な利用が行われた場合には他のテレビジョン会議参加者のプライバシー及びデータのセキュリティーは全く無防備である。特に、伝送データの圧縮技術が発達する一方でデータ蓄積媒体の大容量化が進んだ結果テレビジョン会議の内容全てがデータ蓄積媒体に複写されたりあるいはネットワークを介して転送される恐れさえ現実のものとなりつつある。

【０２６３】

この実施例はこのような状況に鑑みて、これまでに説明したデータ著作権管理システムの構成をテレビジョン会議システムに応用することにより、テレビジョン会議参加者自身の２次的な利用による他のテレビジョン会議参加者のプライバシー及びデータのセキュリティー確保を行うものである。

【０２６４】

このテレビジョン会議データ管理システムは、例えば図４に示されたデータ著作権管理システムの構成におけるデータベース１をテレビジョン会議第１参加者に、１次ユーザ端末装置４をテレビジョン会議第２参加者に、２次ユーザ端末装置５をテレビジョン会議非参加者に置き換えることにより実現することができる。この実施例を図９を用いて説明する。この図において、４４はテレビジョン会議第１参加者、４５はテレビジョン会議第２参加者、４６はテレビジョン会議第３非参加者及び４７はテレビジョン会議第４非参加者、８は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡテレビジョン回線等の通信ネットワークであり、テレビジョン会議第１参加者４４とテレビジョン会議第２参加者４５は通信ネットワーク８によって相互に接続可能とされている。また、テレビジョン会議第２参加者４５とテレビジョン会議第３非参加者４６、テレビジョン会議第３非参加者４６とテレビジョン会議第４非参加者４７は通信ネットワーク８で接続可能とされている。また、４８はデータ記録媒体である。この図において、破線で示されたのは暗号化されたテレビジョン会議内容の経路であり、実線で示されたのはテレビジョン会議第３非参加者４６及びテレビジョン会議第４非参加者４７からテレビジョン会議第１参加者へ暗号鍵を要求する経路であり、１点鎖線で示されたのはテレビジョン会議第１参加者４４からテレビジョン会議第２参加者４５、テレビジョン会議第３非参加者４６及びテレビジョン会議第４非参加者４７へ暗号鍵が転送される経路である。なお、この実施例で説明するテレビジョン会議データ管理システムでは説明を簡明にするために、テレビジョン会議第１参加者４４のプライバシー及びデータセキュリティーの確保のみが行われる場合について説明するが、テレビジョン会議第２参加者４５のプライバシー及びデータセキュリティーの確保も行うことが可能であることはいうまでもない。

【０２６５】

映像及び音声を含むテレビジョン会議第１参加者４４のテレビジョン会議データを暗号化／復号化するテレビジョン会議管理プログラムＰはテレビジョン会議第２参加者４５，テレビジョン会議第３非参加者４６及びテレビジョン会議第４非参加者４７に予め配布され、各々の端末装置に内蔵されている。なお、テレビジョン会議データ管理プログラムＰは暗号鍵が転送される毎に転送されるようにすることもできる。さらに、この実施例では暗号鍵としてテレビジョン会議第１参加者４４が用意する第１秘密鍵及びテレビジョン会議第２参加者４５が生成する第２秘密鍵，テレビジョン会議第３非参加者４６が生成する第３秘密鍵・・・が用いられる。

【０２６６】

テレビジョン会議第１参加者４４とテレビジョン会議第２参加者４５は、各端末装置を利用し、通信ネットワーク８を経由して音声，映像，データ（これらを一括して「テレビジ

ョン会議データ」と呼ぶ）を相互に転送することによりテレビジョン会議を行うが、テレビジョン会議を開始する前にテレビジョン会議第１参加者４４は第１秘密鍵Ｋs1を選択あるいは生成し、第１秘密鍵Ｋs1をテレビジョン会議を開始する前にテレビジョン会議第２参加者４５に供給する。また、第１秘密鍵Ｋs1を転送されたテレビジョン会議第２参加者４５は、テレビジョン会議データ管理プログラムＰにより、第１秘密鍵Ｋs1基づいて第２秘密鍵Ｋs2を生成し、Ｋs2＝Ｐ（Ｋs1）
生成された第２秘密鍵Ｋs2を端末装置内に保存しておく。

【０２６７】

テレビジョン会議第１参加者４４は、通信ネットワーク８を経由して行われるテレビジョン会議において、テレビジョン会議データＭ0を第１秘密鍵Ｋs1で暗号化し、Ｃm0ks1＝Ｅ（Ｋs1，Ｍ0）
暗号化されたテレビジョン会議データＣm0ks1をテレビジョン会議第２参加者４５に転送する。

【０２６８】

第１秘密鍵Ｋs1を用いて暗号化されたテレビジョン会議データＣm0ks1を受け取ったテレビジョン会議第２参加者４５は、第１秘密鍵Ｋs1を用いて暗号化テレビジョン会議データＣm0ks1を復号し、Ｍ0＝Ｄ（Ｋs1，Ｃm0ks1）
復号化されたテレビジョン会議データＭ0を利用する。また、テレビジョン会議データ管理プログラムＰにより、第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2が生成される。
Ｋs2＝Ｐ（Ｋs1）

【０２６９】

復号されたテレビジョン会議データＭ0がテレビジョン会議第２参加者４５の端末装置内に保存される場合、データ記録媒体４８に複写される場合、通信ネットワーク８を経由してテレビジョン会議第３非参加者に転送される場合には、そのデータＭはテレビジョン会議データ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化される。
Ｃmks2＝Ｅ（Ｋs2，Ｍ）

【０２７０】

暗号化データＣmks2は、テレビジョン会議データ名あるいはテレビジョン会議データ番号とともに、記録媒体１１に複写され、あるいは、通信ネットワーク８を経由してテレビジョン会議第３非参加者に供給される。

【０２７１】

暗号化データＣmks2を入手したテレビジョン会議第３非参加者４６は端末装置を利用して、テレビジョン会議データ名あるいはテレビジョン会議データ番号を指定することによりテレビジョン会議データＭの２次利用をテレビジョン会議第１参加者４４に申し込む。

【０２７２】

データＭの２次利用申込を受けたテレビジョン会議第１参加者４４は、テレビジョン会議データ名あるいはテレビジョン会議データ番号を手がかりとして第１秘密鍵Ｋs1を探し出し、第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、Ｋs2＝Ｐ（Ｋs1）
生成された第２秘密鍵Ｋs2をテレビジョン会議第３非参加者４６に供給する。

【０２７３】

第２秘密鍵Ｋs2を受け取ったテレビジョン会議第３非参加者４６は、暗号化データＣmks2をテレビジョン会議データ管理プログラムＰを利用して第２秘密鍵Ｋs2を用いて復号化してＭ＝Ｄ（Ｋs2，Ｃmks2）
復号化されたテレビジョン会議データＭを利用する。テレビジョン会議データＭがテレビジョン会議第３非参加者４６の端末装置内に保存される場合，記録媒体４９に複写される場合，通信ネットワーク８を経由してテレビジョン会議第４非参加者４７に転送される場合には、そのテレビジョン会議データＭはテレビジョン会議データ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化される。
Ｃmks2＝Ｅ（Ｋs2，Ｍ）

【０２７４】

なお、さらにテレビジョン会議データ管理プログラムＰにより第２秘密鍵Ｋs2に基づいて第３秘密鍵Ｋs3が生成され、Ｋs3＝Ｐ（Ｋs2）
テレビジョン会議データ管理プログラムＰによりこの生成された第３秘密鍵Ｋs3を用いてデータＭが暗号化されるようにすることもできる。
Ｃmks3＝Ｅ（Ｋs3，Ｍ）

【０２７５】

以上説明した実施例１９においては、テレビジョン会議データ管理システムを実現するために図４を用いて説明されたデータ著作権管理システムの構成を応用し、使用される秘密鍵を変化させている。しかし、テレビジョン会議データシステムを実現させるシステムの構成として、この他のシステム構成すなわち、図１に示されたシステム構成，図２に示されたシステム構成，図１に示されたシステム構成，図３に示されたシステム構成，図５に示されたシステム構成の何れもが応用可能である。また、その場合に用いられる暗号鍵方式としては、変化しない秘密鍵，公開鍵と専用鍵，秘密鍵と公開鍵と専用鍵の組み合わせ，鍵の２重化、という実施例１から実施例１３で説明した暗号鍵方式が応用可能である。

【０２７６】

また、この説明ではテレビジョン会議第２参加者がテレビジョン会議データを保存して利用すること及び記録媒体に複写あるいは通信ネットワークを経由して転送することを前提にしているが、暗号化に使用された暗号鍵が直ちに廃棄されるようにすることにより、これらの行為を制限することもできる。

【０２７７】

［実施例２０］前に説明したように、本発明のシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要があり、また、この登録の際にデータベース用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に第１暗号鍵を用い著作権管理プログラムを復号するためのプログラムが含まれているため、その保護を図る必要がある。また、本発明においてはデータＭを利用するために第１暗号鍵Ｋ1、第２暗号鍵Ｋ2及び著作権管理プログラムＰが各ユーザに対して転送され、各ユーザはこれらを保管しておく必要がある。さらには著作権情報ラベル、ユーザ情報、公開鍵方式の公開鍵と専用鍵そして秘密鍵生成アルゴリズムを含むプログラム等が必要に応じて保管される。

【０２７８】

これらを保管しておく手段としてフレキシブルディスクを使用することが最も簡便な手段であるが、フレキシブルディスクはデータの消失あるいは改竄に対して極めて脆弱である。また、ハードディスクドライブを使用した場合にもフレキシブルディスク程ではないがデータの消失あるいは改竄に対する不安がある。ところで、最近カード形状の容器にＩＣ素子を封入したＩＣカードが普及し、特にマイクロプロセッサを封入したＰＣカードがＰＣＭＣＩＡカードあるいはＪＥＩＤＡカードとして規格化が進められている。

【０２７９】

図１０に示されたのは、このＰＣカードを用いて本発明のデータベース著作権管理システムのユーザ端末装置を構成した実施例である。この図において、５０はユーザ端末装置本体のマイクロプロセッサであり、５１はシステムバスである。また、５２は内部にＰＣカードマイクロプロセッサ５３，読み出し専用メモリ５５，書き込み・読み出しメモリ５６が封入されこれらがＰＣカードマイクロプロセッサバス５４で接続されたＰＣカードである。

【０２８０】

読み出し専用メモリ５５には、データベース用ソフトウェア及びユーザデータ等の固定した情報がデータベース組織において格納されている。また、この読み出し専用メモリ５５には鍵管理センタ９あるいは著作権管理センタから供給される第１暗号鍵，第２暗号鍵及び著作権管理プログラムも格納される。この読み出し専用メモリ５５は書き込みも行われるため、ＥＥＰＲＯＭを使用することが最も簡便である。

【０２８１】

前に説明したように、データ、第１暗号鍵Ｋ1，第２暗号鍵Ｋ2，第３暗号鍵Ｋ3・・・及び著作権管理プログラムＰ1，　Ｐ2，　Ｐ3・・・はいずれも暗号化された状態でユーザに供給され、データを利用するには第１暗号鍵Ｋ1，著作権管理プログラムＰ，データＭ及び第２暗号鍵Ｋ2を復号しなければならない。これらの作業はユーザ端末装置本体のマイクロプロセッサ５０がＰＣカード５２の読み出し専用メモリ５５に格納されているソフトウェア，第１暗号鍵Ｋ1及び著作権管理プログラムＰ1を用いて行ってもよいが、その場合にはこれらのデータがユーザ端末装置に転送されるため、不正規な使用が行われる危険性がある。この危険を避けるためにはすべての作業をＰＣカード５２内のマイクロプロセッサ５３がＣＰＵバス５４を介して書き込み・読み出しメモリ５６を利用して行い、結果だけをユーザ端末装置に転送し各種の利用を行うようにする。このＰＣカードを利用した場合には異なる装置をユーザ端末装置とすることができる。また、ＰＣカードの他にこれらの機能を有するボードあるいは外部装置を用いることもできる。

【０２８２】

また、本実施の形態は以下に付記する発明を開示する。

（付記１）　暗号化されてデータベースから利用者に供給されるデータの著作権を管理するデータ著作権管理システムであって：該データ著作権管理システムは、データベース１及び鍵管理センタ９を有し；前記暗号化データの復号鍵が前記鍵管理センタ９から前記利用者に供給され；前記利用者が前記データを表示あるいは加工を行う場合には前記復号鍵を用いて前記暗号化データが復号され；前記利用者が前記データあるいは前記加工が行われたデータを保存，複写あるいは転送する場合には前記データが再暗号化される、データ著作権管理システム。

（付記２）　前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、付記１記載のデータ著作権管理システム。

（付記３）　前記著作権管理プログラムが前記利用者が使用する装置のＲＯＭに格納されている、付記３記載のデータ著作権管理システム。

（付記４）　前記著作権管理プログラムが前記利用者が使用する装置のオペレーティングシステムが管理するシステム領域にに格納されている、付記３記載のデータ著作権管理システム。

（付記５）　さらに、前記データの著作権を管理する著作権管理プログラムが用いられる、付記１又は付記２記載のデータ著作権管理システム。

（付記６）　さらに、前記データの著作権についての暗号化されていない著作権情報が用いられる、付記１，付記２，付記３，付記４又は付記５記載のデータ著作権管理システム。

（付記７）　前記暗号化されていない著作権情報が著作権情報ラベルとして前記暗号化データに付加されており、前記データの保存，複写あるいは転送が行われた場合に前記著作権情報ラベルが前記データとともに保存，複写あるいは転送される、付記１，付記２，付記３，付記４，付記５又は付記６記載のデータ著作権管理システム。

（付記８）　前記著作権情報ラベルにディジタル署名がされている、付記７記載のデータ著作権管理システム。

（付記９）　データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース１、鍵管理センタ９及び著作権管理センタ１０から構成され；前記データ著作権管理システムでは秘密鍵、利用者情報及び著作権管理管理プログラムが利用され；前記データベース１はデータを第１秘密鍵によって暗号化して通信ネットワーク８、通信・放送衛星２、記録媒体３を介して１次ユーザ４に配布し；前記１次ユーザ４は前記鍵管理センタ９に対して１次ユーザ情報を提示して利用要求を行い；前記鍵管理センタ９は前記１次ユーザ情報を前記著作権管理センタ１０に転送し；前記鍵管理センタ９は前記第１秘密鍵及び第２秘密鍵とともに著作権管理プログラムを前記通信ネットワーク８を経由して前記１次ユーザ４に転送し；前記１次ユーザ４は前記著作権管理プログラムにより前記第１秘密鍵を用いて前記暗号化データを復号化して利用し；前記復号化データの保存、コピーあるいは転送が

行われる場合には前記著作権管理プログラムにより前記第２秘密鍵を用いて再暗号化されるとともにコピーあるいは転送される再暗号化データに暗号化されていない１次ユーザ情報が付加される、データ著作権管理システム。

（付記１０） 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第１秘密鍵及び第２秘密鍵が廃棄され；前記暗号化データを再利用する前記１次ユーザ４は前記著作権管理センタ１０に再暗号化データの再利用のために前記第２秘密鍵の再転送を申し込み；前記第２秘密鍵が再転送される、付記９記載のデータ著作権管理システム。

（付記１１） 前記第２秘密鍵が再転送されたことにより、前記著作権管理センタ１０に前記暗号化データのコピーあるいは転送が登録される、付記１０記載のデータ著作権管理システム。

（付記１２） ２次ユーザ５は前記著作権管理センタ１０に前記１次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ１０は前記１次ユーザ４に対する前記第２秘密鍵の再転送を確認した上で前記２次ユーザ５に前記第２秘密鍵及び第３秘密鍵及び前記著作権管理プログラムを転送し；前記２次ユーザ５は前記著作権管理プログラムにより前記第２秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第３秘密鍵を用いて再暗号化及び再復号化が行われる、付記１０又は付記１１記載のデータ著作権管理システム。

（付記１３） 前記第２秘密鍵が前記著作権管理プログラムにより前記第１秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか１つあるいはいくつかに基づいて生成される、付記９，付記１０，付記１１又は付記１２記載のデータ著作権管理システム。

（付記１４） データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース１、鍵管理センタ９及び著作権管理センタ１０から構成され；前記データ著作権管理システムでは秘密鍵、利用者情報及び著作権管理管理プログラムが利用され；１次ユーザ４は前記データベース１に１次ユーザ４情報を提示してデータの利用要求を行い；前記データベース１は要求された前記データを第１秘密鍵を用いて暗号化して前記第１秘密鍵、前記第２秘密鍵及び前記著作権管理プログラムとともに前記通信ネットワーク８を経由して前記１次ユーザ４に転送し；前記鍵管理センタ９は前記１次ユーザ情報を前記著作権管理センタ１０に転送し；前記鍵管理センタ９は前記第１秘密鍵及び第２秘密鍵とともに著作権管理プログラムを前記通信ネットワーク８を経由して前記１次ユーザ４に転送し；前記１次ユーザ４は前記著作権管理プログラムにより前記第１秘密鍵を用いて前記暗号化データを復号化して利用し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第２秘密鍵を用いて再暗号化されるとともにコピーあるいは転送される再暗号化データに暗号化されていない１次ユーザ情報が付加される、データ著作権管理システム。

（付記１５） 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第１秘密鍵及び第２秘密鍵が廃棄され；前記暗号化データを再利用する場合には前記１次ユーザ４は前記著作権管理センタ１０に再暗号化データの再利用のために前記第２秘密鍵の再転送を申し込み；前記第２秘密鍵が再転送される、付記１４記載のデータ著作権管理システム。

（付記１６） 前記第２秘密鍵が再転送されたことにより、前記著作権管理センタ１０に前記暗号化データのコピーあるいは転送が登録される、付記１５記載のデータ著作権管理システム。

（付記１７） 前記２次ユーザ５は前記著作権管理センタ１０に前記１次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ１０は前記１次ユーザ４への前記第２秘密鍵の再転送を確認した上で前記２次ユーザ５に前記第２秘密鍵及び第３秘密鍵及び前記著作権管理プログラムを転送し；前記２次ユーザ５は前記著作権管理プログラムにより前記

第２秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第３秘密鍵を用いて再暗号化及び再復号化が行われる、付記１５又は付記１６記載のデータ著作権管理システム。

（付記１８） 前記第２秘密鍵が前記著作権管理プログラムにより前記第１秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか１つあるいはいくつかに基づいて生成される、付記１４，付記１５，付記１６又は付記１７記載のデータ著作権管理システム。

（付記１９） データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース１、鍵管理センタ９及び著作権管理センタ１０から構成され；前記データ著作権管理システムでは秘密鍵、公開鍵及び専用鍵が利用され；１次ユーザ４は前記鍵管理センタ９に前記第１公開鍵、第２公開鍵及び１次ユーザ情報を提示して利用希望データの利用要求を行い；利用要求を受けた前記データベース１は前記データを前記第１秘密鍵を用いて暗号化し、前記第１秘密鍵を前記第１公開鍵を用いて暗号化し、前記第２秘密鍵を前記第２公開鍵を用いて暗号化し、前記暗号化データ，前記暗号化第１秘密鍵及び前記暗号化第２秘密鍵及び著作権管理プログラムを前記１次ユーザ４に転送し；前記１次ユーザ４は著作権管理プログラムにより前記暗号化第１秘密鍵を前記第１専用鍵を用いて復号化し、前記暗号化データを前記復号化第１秘密鍵を用いて復号化し、前記暗号化第２秘密鍵を前記第２専用鍵を用いて復号化し、前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第２秘密鍵を用いて暗号化及び復号化が行われる、データ著作権管理システム。

（付記２０） 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第１秘密鍵及び第２秘密鍵が廃棄され；前記暗号化データを再利用する前記１次ユーザ４は前記著作権管理センタ１０に再暗号化データの再利用のために前記第２秘密鍵の再転送を申し込み；前記第２秘密鍵が再転送される、付記１９記載のデータ著作権管理システム。

（付記２１） 前記第２秘密鍵が再転送されたことにより、前記著作権管理センタ１０に前記暗号化データのコピーあるいは転送が登録される、付記２０記載のデータ著作権管理システム。

（付記２２） 前記２次ユーザ５は前記著作権管理センタ１０に前記１次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ１０は前記１次ユーザ４に対する前記第２秘密鍵の再転送を確認した上で前記２次ユーザ５に前記第２秘密鍵及び第３秘密鍵及び前記著作権管理プログラムを転送し；前記２次ユーザ５は前記著作権管理プログラムにより前記第２秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第３秘密鍵を用いて再暗号化及び再復号化が行われる、付記２０又は付記２１記載のデータ著作権管理システム。

（付記２３） 前記第２秘密鍵が前記著作権管理プログラムにより前記第１秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか１つあるいはいくつかに基づいて生成される、付記１９，付記２０，付記２１又は付記２２記載のデータ著作権管理システム。

（付記２４） 各々異なる暗号鍵で暗号化されてデータベース１から利用者に供給される複数のデータを利用するためのデータ著作権管理システムであって：該データ著作権管理システムでは暗号鍵、利用者情報及び著作権管理プログラムが利用され；１次ユーザ４は著作権管理センタ１０から前記複数の原データ固有の複数の著作権管理プログラム及び複数の第１暗号鍵を入手し、前記複数の原データを前記複数の第１暗号鍵で復号し；前記複数の原データ固有の複数の著作権管理プログラムにより１つ又は複数の第２暗号鍵が生成され；利用された前記複数の原データあるいは複数の加工データは前記複数の原データ固有の複数の著作権管理プログラムにより前記１つ又は複数の第２暗号鍵で暗号化されて加

工過程データとともに保存・複写・転送され；前記１つ又は複数の第２の暗号鍵で暗号化された前記複数の原データあるいは前記複数の加工データは２次ユーザ５が前記著作権管理センタ１０から入手した前記複数の著作権管理プログラム及び前記１つ又は複数の第２の暗号鍵で復号化されて前記加工過程データを用いて加工されて利用される、データ著作権管理システム。

（付記２５） 前記第２秘密鍵が前記著作権管理プログラムにより前記第１秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか１つあるいはいくつかに基づいて生成される、付記２４記載のデータ著作権管理システム。

（付記２６） データベース１から利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：該データ著作権管理システムでは暗号鍵、利用者情報及び著作権管理管理プログラムが利用され；前記利用者は前記データベース１に利用者情報を提示し；前記データベース１は前記第１利用者に第１暗号鍵で暗号化された前記データを供給し；前記第１利用者は前記著作権管理プログラムを利用して前記第１暗号鍵に基づく第２暗号鍵を生成し；前記第１利用者が前記暗号化データを利用する場合には前記第１暗号鍵を用いて前記暗号化データが復号され；前記第１利用者が前記復号化データを保存、複写あるいは転送する場合には、前記復号化データが前記第２暗号鍵を用いて再暗号化される、データ著作権管理システム。

（付記２７） 前記暗号鍵が秘密鍵である、付記２６記載のデータ著作権管理システム。

（付記２８） 前記暗号鍵が公開鍵及び専用鍵である、付記２６記載のデータ著作権管理システム。

（付記２９） 暗号化されて金融機関から第１利用者に供給されるディジタルキャッシュを利用するためのディジタルキャッシュ管理システムであって：該ディジタルキャッシュ管理システムにおいては、前記暗号化ディジタルキャッシュデータの復号鍵が金融機関から前記第１利用者に供給され；前記第１利用者が前記ディジタルキャッシュデータの確認を行う場合には前記復号鍵を用いて前記暗号化ディジタルキャッシュデータが復号され；前記第１利用者が前記復号化ディジタルキャッシュデータを保存する場合、変更されたディジタルキャッシュデータを保存する場合、あるいは第２利用者にディジタルキャッシュデータを転送する場合には前記データが再暗号化される、ディジタルキャッシュ管理システム。

（付記３０） 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、付記２９のディジタルキャッシュ管理システム。

（付記３１） さらに、前記ディジタルキャッシュを管理するディジタルキャッシュ管理プログラムが用いられる、付記２９又は付記３０のディジタルキャッシュ管理システム。

（付記３２） さらに、暗号化されていない第１利用者情報が用いられる、付記２９，付記３０又は付記３１のディジタルキャッシュ管理システム。

（付記３３） 前記暗号化されていない第１利用者情報が第１利用者情報ラベルとして前記暗号化ディジタルキャッシュデータに付加されており、前記ディジタルキャッシュデータが保存される場合、変更されたディジタルキャッシュデータが保存される場合、あるいは第２利用者にディジタルキャッシュデータが転送される場合には前記ディジタルキャッシュデータとともに保存あるいは転送される、付記２９，付記３０，付記３１又は付記３２のディジタルキャッシュ管理システム。

（付記３４） 前記第１利用者情報ラベルにディジタル署名がされている、付記３３記載のデータ著作権管理システム。

（付記３５） 暗号化されて金融機関から第１利用者に供給されるディジタルキャッシュを利用するためのディジタルキャッシュ管理システムであって：該ディジタルキャッシュ管理システムでは暗号鍵、利用者情報及びディジタルキャッシュ管理プログラムが利用され；前記第１利用者は前記金融機関に第１利用者情報を提示し；前記金融機関は前記第１利用者に第１暗号鍵で暗号化された前記ディジタルキャッシュを供給し；前記第１利用者は前記ディジタルキャッシュ管理プログラムを利用して前記第１暗号鍵に基づく第２暗号鍵を生成し；前記第１利用者が前記暗号化ディジタルキャッシュデータの確認を行う場合

には前記第１暗号鍵を用いて前記暗号化ディジタルキャッシュデータが復号され；前記利用者が前記復号化ディジタルキャッシュデータを保存する場合には、前記第２暗号鍵を用いて再暗号化され；前記復号化ディジタルキャッシュデータが第２利用者に転送される時に前記第２暗号鍵を用いて再暗号化され、前記再暗号化ディジタルキャッシュデータが前記第１利用者情報とともに前記第２利用者に転送され；前記第２利用者から前記金融機関に前記第１利用者情報が提示され；前記金融機関は前記第１利用者情報に基づく前記第２暗号鍵を生成して前記第２利用者に転送し；前記第２利用者は前記転送された第２暗号鍵を用いて前記ディジタルキャッシュ管理プログラムにより前記再暗号化ディジタルキャッシュデータを復号する、ディジタルキャッシュ管理システム。

（付記３６） 前記暗号鍵が秘密鍵である、付記３５のディジタルキャッシュ管理システム。

（付記３７） 前記暗号鍵が公開鍵及び専用鍵である、付記３５のディジタルキャッシュ管理システム。

（付記３８） 暗号化されて金融機関から第１利用者に供給されるディジタルキャッシュを利用するためのディジタルキャッシュ管理システムであって：該ディジタルキャッシュ管理システムでは公開鍵及び専用鍵が利用され；前記第１利用者は前記金融機関に第１公開鍵を提示し；前記金融機関は前記第１公開鍵でディジタルキャッシュデータを暗号化して前記第１利用者に供給し；前記第１利用者は前記ディジタルキャッシュデータを第１専用鍵を用いて復号し；前記第２利用者は前記第１利用者に第２公開鍵を提示し；前記第１利用者は復号化された前記ディジタルキャッシュデータを第２公開鍵で暗号化して第２利用者に転送し；前記第２利用者は前記ディジタルキャッシュデータを第２専用鍵を用いて復号する、ディジタルキャッシュ管理システム。

（付記３９） 第１利用者から第２利用者に暗号化されて供給されるテレビジョン会議データを利用するためのテレビジョン会議データ管理システムであって：該テレビジョン会議データ管理システムにおいては、前記暗号化テレビジョン会議データの復号鍵が第１利用者から前記第２利用者に供給され；前記第２利用者が前記テレビジョン会議データを利用する場合には前記復号鍵を用いて前記暗号化テレビジョン会議データが復号され；前記第２利用者が前記復号化テレビジョン会議データを保存する場合、加工されたテレビジョン会議データを保存する場合、あるいは第３利用者にテレビジョン会議データを転送する場合には前記データが再暗号化される、テレビジョン会議データ管理システム。

（付記４０） 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、付記３９のテレビジョン会議データ管理システム。

（付記４１） さらに、前記テレビジョン会議データを管理するテレビジョン会議データ管理プログラムが用いられる、付記３９又は付記４０のテレビジョン会議データ管理システム。

（付記４２） さらに、暗号化されていない第２利用者情報が用いられる、付記３９，付記３４０は付記４１のテレビジョン会議データ管理システム。

（付記４３） 前記暗号化されていない第２利用者情報が第２利用者情報ラベルとして前記暗号化テレビジョン会議データに付加されており、前記テレビジョン会議データが保存される場合、変更されたテレビジョン会議データが保存される場合、あるいは第２利用者にテレビジョン会議データが転送される場合には前記テレビジョン会議データとともに保存あるいは転送される、付記３９，付記４０，付記４１又は付記４２のテレビジョン会議データ管理システム。

（付記４４） 前記第１利用者情報ラベルにディジタル署名がされている、付記４３のテレビジョン会議データ管理システム。

（付記４５） 第１利用者から第２利用者に暗号化されて供給されるテレビジョン会議データを利用するためのテレビジョン会議データ管理システムであって：該テレビジョン会議データ管理システムでは暗号鍵、利用者情報及びテレビジョン会議データ管理プログラムが利用され；前記第２利用者は前記第１利用者に第２利用者情報を提示し；前記第１利用者は前記第２利用者に第１暗号鍵で暗号化された前記テレビジョン会議データを供給し

；前記第２利用者は前記テレビジョン会議データ管理プログラムを利用して前記第１暗号鍵に基づく第２暗号鍵を生成し；前記第２利用者が前記暗号化テレビジョン会議データを利用する場合には前記第１暗号鍵を用いて前記暗号化テレビジョン会議データが復号され；前記第２利用者が前記復号化テレビジョン会議データを保存、複写あるいは転送する場合には、前記復号化テレビジョン会議データが前記第２暗号鍵を用いて再暗号化される、テレビジョン会議データ管理システム。

（付記４６） 前記暗号鍵が秘密鍵である、付記４５のテレビジョン会議データ管理システム。

（付記４７） 前記暗号鍵が公開鍵及び専用鍵である、付記４５のテレビジョン会議データ管理システム。

（付記４８） ユーザ端末装置のユーザ端末装置本体のシステムバスに接続して用いられ、マイクロプロセッサ、マイクロプロセッサバスに接続された読み出し専用メモリ、書き込み・読み出しメモリ及び書換可能読み出し専用メモリから構成され、前記読み出し専用メモリには、データベース組織利用ソフトウェア及びユーザデータ等の固定した情報が格納され、読み出し専用メモリには鍵管理センタあるいは著作権管理センタから供給される第１暗号鍵，第２暗号鍵及び著作権管理プログラムが格納される、データ著作権管理装置。

【図面の簡単な説明】

【０２８３】

【図１】本発明実施例１，実施例２，実施例３のデータ著作権管理システム構成図。

【図２】本発明実施例４のデータ著作権管理システム構成図。

【図３】本発明実施例５，実施例６，実施例７のデータ著作権管理システム構成図。

【図４】本発明実施例８，実施例９，実施例１０，実施例１１のデータ著作権管理システム構成図。

【図５】本発明実施例１２，実施例１３のデータ著作権管理システムの実施例。

【図６】データ加工の説明図。

【図７】ディジタルキャッシュシステムの説明図。

【図８】本発明実施例１７，実施例１８のディジタルキャッシュシステム構成図。

【図９】本発明実施例１９のテレビジョン会議システム構成図。

【図１０】本発明のデータ著作権管理システムで用いるユーザ端末装置の実施例構成図。

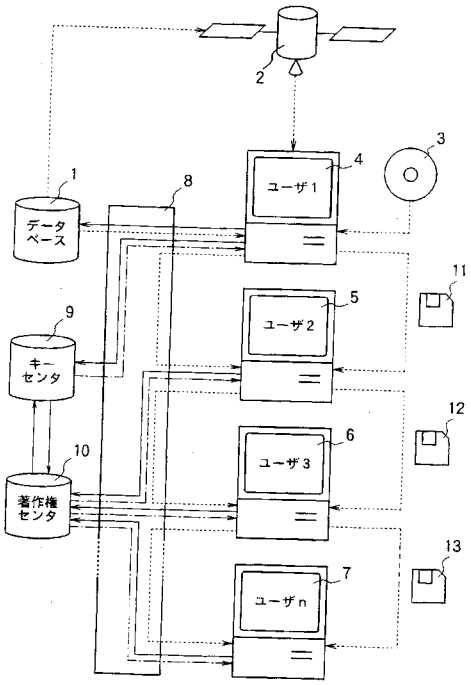
【符号の説明】

【０２８４】

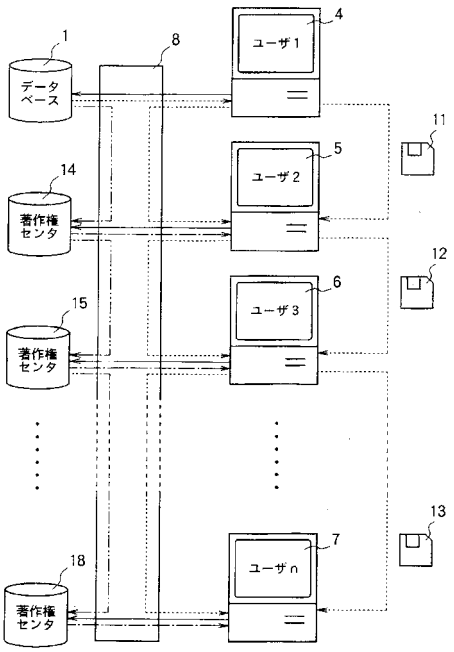
１，１９，２０，２１ データベース
２ 放送・通信衛星
３ １１，１２，１３，４８，４９ 記録媒体
４，５，６，７ ユーザ端末装置
８ 通信ネットワーク
９ 鍵管理センタ
１０，１４，１５，１７，１８ 著作権管理センタ
２３，２５，２７，２９ 電子財布
２４，２６，２８ 預金口座
３０，３５ 残金
３１ 引出金
３２，３３，３４ 支払金
３６ 顧客
３８ 小売店
４０ メーカ
３７ 顧客側銀行
３９ 小売店側銀行
４１ メーカ側銀行

４２，４３　ＩＣカード
４４，４５　テレビジョン会議参加者
４６，４７　テレビジョン会議非参加者
５０　マイクロプロセッサ
５１　システムバス
５２　ＰＣカード
５３　ＰＣカードマイクロプロセッサ
５４　ＰＣカードマイクロプロセッサバス
５５　読み出し専用メモリ
５６　書き込み・読み出しメモリ

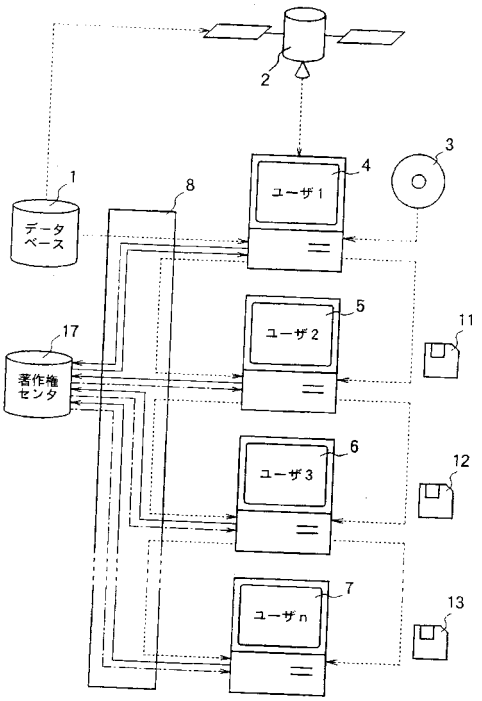
【図１】



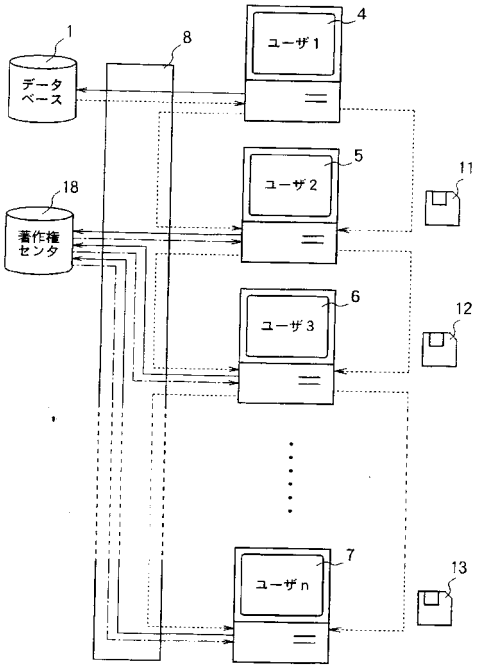
【図２】



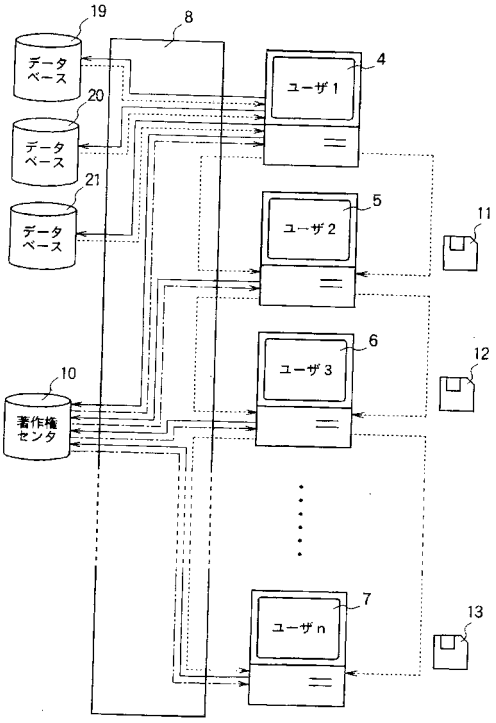
【図３】


2
3
1
8
4
ユーザ１
データベース
5
ユーザ２
11
17
著作権センタ
6
ユーザ３
12
7
ユーザｎ
13

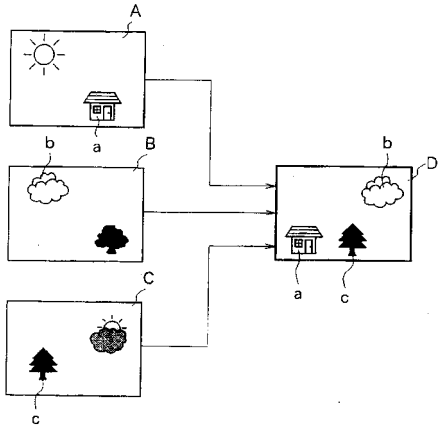
【図４】


1
8
4
ユーザ１
データベース
5
ユーザ２
11
18
著作権センタ
6
ユーザ３
12
7
ユーザｎ
13

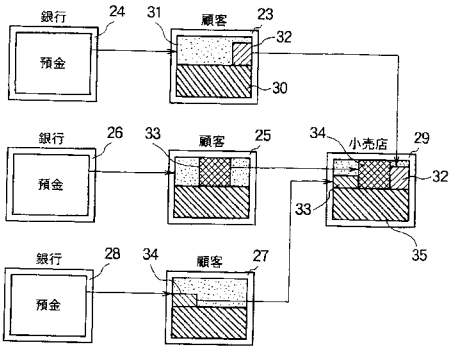
【図５】


19
8
データベース
4
ユーザ１
20
データベース
21
データベース
5
ユーザ２
11
6
ユーザ３
12
10
著作権センタ
7
ユーザｎ
13

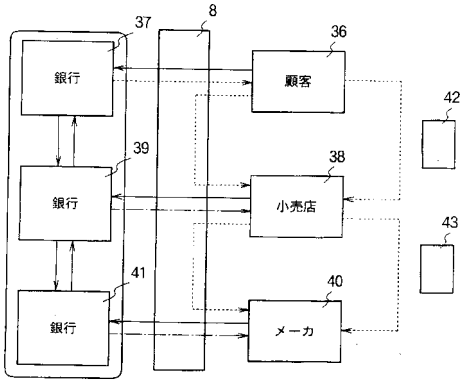
【図６】


A
a
b
B
b
D
a
c
C
c

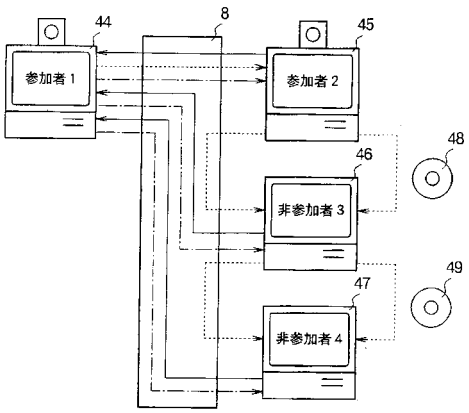
【図７】


銀行
預金
24
31
顧客
23
32
30
銀行
預金
26
33
顧客
25
34
小売店
29
32
33
35
銀行
預金
28
34
顧客
27

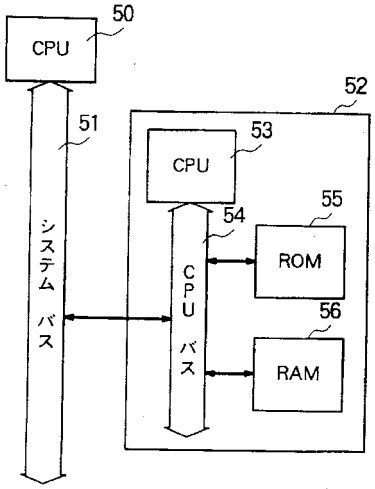
【図８】


37
8
銀行
36
顧客
42
39
銀行
38
小売店
43
41
銀行
40
メーカ

【図９】


44
8
参加者 1
45
参加者 2
48
46
非参加者 3
49
47
非参加者 4

【図１０】


50
CPU
52
51
53
CPU
システムバス
54
55
ROM
CPUバス
56
RAM

フロントページの続き

審査官　中里　裕正

(56)参考文献　特公昭６２－０４２３０４（ＪＰ，Ｂ１）
特開平０５－２９８３７３（ＪＰ，Ａ）
特開昭５８－１６９０００（ＪＰ，Ａ）
暗号を利用した新しいソフトウェア流通形態の提案，情報処理学会研究報告，１９９３年　7月２０日，，Vol.93 No.64(93-IS-45-3)，p.19-28

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｑ　５０／００