

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4099461号  
(P4099461)

(45) 発行日 平成20年6月11日 (2008. 6. 11)

(24) 登録日 平成20年3月21日 (2008. 3. 21)

(51) Int. Cl.

F I

G O 6 F 21/24 (2006. 01)

G O 6 F 12/14 5 6 O B

G O 6 F 12/00 (2006. 01)

G O 6 F 12/14 5 2 O D

H O 4 L 9/10 (2006. 01)

G O 6 F 12/14 5 4 O B

G O 6 F 21/00 (2006. 01)

G O 6 F 12/14 5 5 O A

G O 6 F 12/00 5 3 7 H

請求項の数 2 (全 33 頁) 最終頁に続く

(21) 出願番号 特願2004-149423 (P2004-149423)  
 (22) 出願日 平成16年5月19日 (2004. 5. 19)  
 (62) 分割の表示 特願平7-280984の分割  
 原出願日 平成7年10月27日 (1995. 10. 27)  
 (65) 公開番号 特開2004-303265 (P2004-303265A)  
 (43) 公開日 平成16年10月28日 (2004. 10. 28)  
 審査請求日 平成16年6月9日 (2004. 6. 9)  
 (31) 優先権主張番号 特願平6-264200  
 (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6-299835  
 (32) 優先日 平成6年12月2日 (1994. 12. 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, 8 9 1 1 9 ネバダ州,  
 ラスベガス, スイート 5, ルネサンス  
 ドライブ 2 2 1 5 - 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 杉木 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】 データ著作権管理装置

(57) 【特許請求の範囲】

【請求項 1】

データを利用する端末装置、受信装置、記録装置、またはコンピュータ装置の内部に接  
 続されたデータ著作権管理装置であって、

前記端末装置、受信装置、記録装置、またはコンピュータ装置に提供されるデータの著  
 作権を管理する著作権管理システムから、第1秘密鍵、第2秘密鍵および暗号化データ  
 を、前記端末装置、受信装置、記録装置、またはコンピュータ装置に提供することに使用され  
 るデータ著作権管理装置であって、

前記データ著作権管理装置は、

前記第1秘密鍵及び第2秘密鍵を保存する手段と、

前記端末装置、受信装置、記録装置、またはコンピュータ装置から前記暗号化データの  
 供給を受ける手段と、

前記暗号化データが前記端末装置、受信装置、記録装置、またはコンピュータ装置で加  
 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再暗号化  
 手段と、

データの加工が実行されたときに前記端末装置、受信装置、記録装置、またはコンピ  
 ュータ装置の1次ユーザ情報を格納する手段と、

前記再暗号化データがコピーあるいは転送されるときに、前記第1秘密鍵及び第2秘密  
 鍵を廃棄する手段と、を備えており、

前記端末装置、受信装置、記録装置、またはコンピュータ装置に含まれる、前記第2秘密鍵の再転送を申し込む手段が、前記端末装置、受信装置、記録装置、またはコンピュータ装置の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を利用するための前記第2秘密鍵の再転送を申し込み、前記第2秘密鍵が、前記著作権管理システムから前記データ著作権管理装置を介して前記端末装置、受信装置、記録装置、またはコンピュータ装置に再転送されると、前記データ著作権管理装置は、前記再暗号化データのコピー又は転送が前記著作権管理システムに登録されるようにする、データ著作権管理装置。

#### 【請求項2】

請求項1に記載のデータ著作権管理装置において、IC、ICカード、拡張ボード、あるいはPCカードにより構成されているデータ著作権管理装置。

10

#### 【発明の詳細な説明】

#### 【技術分野】

#### 【0001】

本発明はデジタルデータの表示、保存、複写、加工、転送においてデータを利用する装置に係るものであり、デジタルデータの著作権を保護することを目的とする。

#### 【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。

20

#### 【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。

30

#### 【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た。

40

#### 【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】

50

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、複製、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、複製、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。なお、広告付きソフトあるいはフリーウェアと呼ばれるデータは利用において原則として使用料を必要としないが、著作権は存在しており、利用の仕方によっては著作権上の制限を受ける場合がある。本発明者らは特開平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（特許文献1）及び特願平6-237673号において、デジタルデータの著作権を管理するシステムについて提案した。これらのシステム及び装置において、暗号化された番組の視聴を希望する者は通信装置を使用し通信回線を経由して管理センタに視聴申し込みを行い、管理センタはこの視聴申し込みに対して許可鍵を送信するとともに課金処理を行い料金を徴収する。許可鍵を受信した視聴希望者はオンラインあるいはオフライン手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって暗号化された番組の暗号を解除する。

#### 【0009】

特願平6-64889号に記載されたシステムは、デ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ジタルデータの表示（音声化を含む）、保存、複製、加工、転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。この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。また、この特願平6-64889号には、データが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときに復号化され、保存、コピー、転送は再び暗号化された状態で行なわれるようにすることが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

#### 【0010】

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(encryption)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。

#### 【0011】

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(cryptogram)  $C$ 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  $K_s$  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(publickey)  $K_b$  が使用され、暗号文の復号化に専用鍵(private-key)  $K_v$  が使用される公開鍵方式(public-key system) が採用される。

#### 【0012】

図1に示されたのは、本願発明に係るデータ著作権管理装置が使用される先願である特願平6-237673号に示されたデータ著作権管理システムの構成である。このシステムでは、暗号化データが1次ユーザ4からの要求に応じて双方向的に供給される。また、暗号鍵方式として秘密鍵方式及び公開鍵方式が採用される。なお、このシステム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。

10

#### 【0013】

このシステムにおいて、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、3は著作権管理センタ、8、9及び10は著作権管理センタ3に保管されている2次著作権データ、3次著作権データ・・・ $n$ 次著作権データ、2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。

20

#### 【0014】

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、著作権管理センタ3は通信ネットワーク2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からあるいは著作権管理センタ内でデータから次位のデータ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。

30

#### 【0015】

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2を経由してデータベース1にアクセスする。

#### 【0016】

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3に転送する。

40

#### 【0017】

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。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3に転送される。

#### 【0018】

これらの転送が行われた結果著作権管理センタ3には1次利用形態に対応する許可鍵  $Kp$ 、1次ユーザ情報  $Iu1$ 、原著作権情報  $Ic0$ 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  $Ic0$ は著作権使用料金分配に用いられる。

50

## 【0019】

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。

## 【0020】

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の著作権情報Ic0が著作権管理センタ3に転送される。また、1次ユーザは視聴・保存・複写・加工・転送である利用形態に対応した許可鍵の中から希望する利用形態に対応した許可鍵Kp1を選択する。この許可鍵Kp1も著作権管理センタ3に転送される。

10

## 【0021】

なお、1次ユーザが行う利用形態として視聴・保存は最低限必要であるから、これらの利用形態は最小限の利用形態として選択の対象から外し、複写・加工・転送のみを選択の対象とすることもできる。

## 【0022】

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著作権者情報Ic0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。

20

$Cks1kb1 = E(Kb1, Ks1)$

$Cks2kb2 = E(Kb2, Ks2)$

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2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。

30

## 【0023】

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。

40

$P = D(Ks2, Cpks2)$

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者がデータMを入手したとしても暗号化データMを復号化して利用することは不可能である。

## 【0024】

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

50

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Ic0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。

10

#### 【0025】

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2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。

20

#### 【0026】

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2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Ic0、1次ユーザの著作権情報Ic1が付加される。

#### 【0027】

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。

30

#### 【0028】

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2を経由して著作権管理センタ3に対してデータ名あるいは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Ic0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。

#### 【0029】

2次ユーザからの2次利用申込を受けた著作権管理センタ3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次著作権データ9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次著作権情報Ic1を2次著作権データ8に照会・確認し、確認された2次的著作権情報Ic1は3次著作権データ9に転送される。

40

#### 【0030】

2次ユーザは視聴・蓄積・複写・加工・転送の利用形態に対応した許可鍵Kp2を選択する。選択された利用形態に対応した許可鍵Kp2は3次著作権データベース9に転送される。なお、2次ユーザの利用形態として視聴・蓄積は最低限必要であるから、これらの利用形態は最小限の利用形態として選択の対象から外し、複写・加工・転送のみを選択の対象としてもよい。

50

## 【0031】

2次著作権データベース8は、第3の秘密鍵Ks3を用意する。用意された第3の秘密鍵Ks3は3次著作権データ9に転送され格納される。

## 【0032】

これらの転送が行われた結果、3次著作権データ9には許可鍵Kp2、1次ユーザ著作権情報Ic1、1次ユーザ情報Iu1、原著作権情報Ic0、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、許可鍵Kp2と1次ユーザ著作権情報Ic1及び1次ユーザ情報Iu1は、著作権使用料金分配に用いられる。

## 【0033】

以下同様にして、n次著作権データ10にはn次利用形態に対応した許可鍵Kpn、(n-1)次ユーザの2次的著作権情報Icn-1、1次ユーザ情報Iu1、原著作権情報Ic0、n次ユーザ情報Iun及び第nの秘密鍵Ksnが格納される。

10

## 【0034】

2次著作権データ8から許可鍵Kp2、1次ユーザ情報Iu1、原著作権情報Ic0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Ic0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。

$C_{ks2kb3} = E(Kb3, Ks2)$

$C_{ks3kb4} = E(Kb4, Ks3)$

また、著作権管理プログラムPは第3の秘密鍵Ks3を用いて暗号化される。

20

$C_{pks3} = E(Ks3, P)$

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2を経由して2次ユーザ端末装置5に転送される。このときに必要ならば課金が行われる。

## 【0035】

2次著作権データ8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Cks3 Kb4を復号する。

$Ks2 = D(Kv3, C_{ks2kb3})$

30

$Ks3 = D(Kv4, C_{ks3kb4})$

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。

$P = D(Ks3, C_{pks3})$

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。

$M = D(Ks2, C_{mks2})$

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。

40

## 【0036】

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、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。

## 【0037】

50

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。

#### 【００３８】

先願である特願平６－２３７６７３号で本発明者らが提案したデータ著作権管理装置を図２により説明する。このデータ著作権管理装置１５は、マイクロプロセッサ（ＣＰＵ）１６、ＣＰＵ１６のローカルバス１７、ローカルバス１７に接続された読み出し専用メモリ（ＲＯＭ）１８及び書き込み・読み出しメモリ（ＲＡＭ）１９を有するコンピュータシステムとして構成されており、ローカルバス１７がユーザ端末装置２０のマイクロプロセッサ２１のシステムバス２２に接続される。

10

#### 【００３９】

また、ユーザ端末装置２０のシステムバス２２には装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置（ＣＯＭＭ）２３、ＣＤ－ＲＯＭで供給されるデータを読み込むＣＤ－ＲＯＭドライブ（ＣＤＲＤ）２４、受け取ったデータあるいは加工したデータを外部へ供給するためにフレキシブルディスクドライブに複写するフレキシブルディスクドライブ（ＦＤＤ）２５及びデータを保存するハードディスクドライブ（ＨＤＤ）２６が接続される。なお、ユーザ端末装置のシステムバス２２には当然のこととしてＲＯＭ、ＲＡＭ等が接続されているが、この図においては記載が省略されている。

20

#### 【００４０】

データ著作権管理装置１５のＲＯＭ１８には、データベースを利用するための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ている。ＲＡＭ１９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た暗号鍵及び著作権管理プログラムが格納される。復号化あるいは再暗号化の作業はデータ著作権管理装置１５が行い、処理結果だけがローカルバス１７及びユーザ端末装置のシステムバス２１を経由してユーザ端末装置２０に転送される。このデータ著作権管理装置１５は、モノリシックＩＣ、ハイブリッドＩＣ、拡張ボード、ＩＣカードあるいはＰＣカードとして実現される。

#### 【特許文献１】特開平７－２７１８６５号公報

30

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【００４１】

本件出願においては、先願である特願平６－２３７６７３号で提案されたユーザ端末装置に付属して用いるデータ著作権管理装置をさらに具体的にしたデータ著作権管理装置を提案する。本発明のデータ著作権管理装置は、ユーザ端末装置に付属して用いられ、中央処理装置、中央処理装置バス、読み出し専用半導体メモリ、電氣的消去可能プログラマブルメモリ及び読み出し・書き込みメモリを備えている。中央処理装置バスには中央処理装置、読み出し専用半導体メモリ、電氣的消去可能プログラマブルメモリ及び読み出し・書き込みメモリが接続されるとともにデータを利用する装置のシステムバスが接続可能とされ、読み出し専用半導体メモリにはデータ著作権管理システムプログラム、暗号アルゴリズム及びユーザ情報が格納され、電氣的消去可能プログラマブルメモリには第２の専用鍵、利用許可鍵、第２の秘密鍵及び著作権情報が格納され、装置動作時には読み出し・書き込みメモリに第１の公開鍵、第１の専用鍵、第２の公開鍵及び第１の秘密鍵が転送される。著作権管理プログラムは外部から供給される場合にはＥＥＰＲＯＭに格納されるが、そうでない場合にはＲＯＭに格納される。データ著作権管理装置の形態としてはモノリシックＩＣ、ハイブリッドＩＣ、専用の端子を有する薄型のＩＣカード、ＰＣカード及び挿入用ボードが可能である。

40

#### 【００４２】

これまでに先願発明として説明したデータ著作権管理システムにおいては、入手した暗

50



号化データを表示・加工する場合には復号化して利用するが、入手あるいは加工したデータを保存・複製・転送する場合には再暗号化することによって、データの不正規な使用ができないようにしている。したがって、本発明が対象とするデータ著作権管理システムで使用される装置においては、データの復号化だけでなく、データの再暗号化も同時に行われる必要があるが、これらの先願に記載されたデータ著作権管理装置はデータの復号化あるいは再暗号化の作業のうち一方のみしか実行することができない。

#### 【0043】

そこで、本願においては著作権を管理するために暗号化されて供給されるデータを復号化と再暗号化を同時に行うことができるデータ著作権管理装置の発明を提案する。そのために、ユーザ端末装置においてユーザ端末装置全体を制御するマイクロプロセッサに加えて少なくとも1個のマイクロプロセッサ、理想的には2個のマイクロプロセッサ、を付加させることにより暗号化されて供給されたデータの復号化及び再暗号化を行う。1個のマイクロプロセッサが付加される場合は、ユーザ端末装置のマイクロプロセッサと付加されたマイクロプロセッサの中一方がデータの復号化を行い、他方が再暗号化を行う。2個のマイクロプロセッサが付加される場合は、付加されたマイクロプロセッサの中一方がデータの復号化を行い、他方のマイクロプロセッサが再暗号化を行い、ユーザ端末装置20のマイクロプロセッサは全体の動作を制御する。

#### 【0044】

付加されるマイクロプロセッサはユーザ端末装置のマイクロプロセッサのシステムバスに接続してもよいが、この構成ではマイクロプロセッサを並行して動作させるマルチプロセッサ構成を実現することはできない。そこで、本願においてはS C S IバスあるいはP C Iバスを利用してマルチプロセッサ構成としたデータ著作権管理装置を提案する。

#### 【0045】

デジタルデータには、文字データの他にグラフィックデータ、コンピュータプログラム、デジタル音声データ、J P E G等の方式による静止画データ、さらにはM P E G等による動画データがある。これらのデータからなるデータ著作物は種々の装置を用いて利用されるが、これらの装置にもデータ著作権管理機能を具えておく必要がある。そこで、本願においてはこれらのデータ著作権管理装置及び先願に記載されたデータ著作権管理装置の使用形態として種々の装置に内蔵することを提案する。

#### 【課題を解決するための手段】

#### 【0046】

本発明の第1の態様は、データを利用する端末装置、受信装置、記録装置、またはコンピュータ装置の内部に接続して用いられるデータ著作権管理装置であって、前記端末装置、受信装置、記録装置、またはコンピュータ装置に提供されるデータの著作権を管理する著作権管理システムから第1秘密鍵、第2秘密鍵および暗号化データが前記端末装置、受信装置、記録装置、またはコンピュータ装置に提供され、

前記第1秘密鍵及び第2秘密鍵を保存する手段と、前記端末装置、受信装置、記録装置、またはコンピュータ装置から前記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前記端末装置、受信装置、記録装置、またはコンピュータ装置で加工される場合に、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再暗号化手段と、データの加工が実行されたときに前記端末装置、受信装置、記録装置、またはコンピュータ装置の1次ユーザ情報を格納する手段と、前記再暗号化データがコピーあるいは転送されるときに、前記第1秘密鍵及び第2秘密鍵を廃棄する手段と、前記第2秘密鍵が再転送されるように、前記端末装置、受信装置、記録装置、またはコンピュータ装置の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を利用するための前記第2秘密鍵の再転送を申し込む手段とを備え、

前記第2秘密鍵が再転送された事により、前記再暗号化データのコピー又は転送を前記著作権管理システムに登録させるものである。

#### 【0047】

また、第２の態様は、データを利用する端末装置、受信装置、記録装置、またはコンピュータ装置の内部に接続して用いられるデータ著作権管理装置であり、

マイクロプロセッサと、前記マイクロプロセッサに接続されるローカルバスと、

前記ローカルバスに接続される読み出し専用半導体メモリ及び読み出し・書き込みメモリとを備え、

前記端末装置、受信装置、記録装置、またはコンピュータ装置のマイクロプロセッサと前記データ著作権管理装置のマイクロプロセッサのうち一方が復号化処理を行い他方が再暗号化処理を行うものでもよい。

#### 【００４８】

また、第３の態様は、データを利用する端末装置、受信装置、記録装置、またはコンピュータ装置の内部に接続して用いられ、

第１及び第２のマイクロプロセッサと、前記第１のマイクロプロセッサに接続される第１のローカルバスと、前記第１のローカルバスに接続される第１の読み出し専用半導体メモリおよび第１の読み出し・書き込みメモリと、前記第２のマイクロプロセッサに接続される第２のローカルバスと、前記第２のローカルバスに接続される第２の読み出し専用半導体メモリおよび第２の読み出し・書き込みメモリとを備え、

前記第１のマイクロプロセッサが暗号化されたデータの復号化処理を行い、前記第２のマイクロプロセッサが復号化されたデータの再暗号化処理を行うものでもよい。

#### 【発明の効果】

#### 【００４９】

本願においては著作権を管理するために暗号化されて供給されるデータを復号化と再暗号化を同時に行うことができる。

#### 【発明を実施するための最良の形態】

#### 【００５０】

以下、本願発明の実施例を図面を用いて説明する。図３に示されたのは、実施例１である本願発明に係るデータ著作権管理装置の構成を示すブロック図である。このデータ著作権管理装置３０は、先願である特願平６－２３７６７３号に記載されたデータ著作権管理装置１５の構成要素に加えて電氣的消去可能プログラマブルメモリ（ＥＥＰＲＯＭ）３１を備えている。このデータ著作権管理装置３０は、ＣＰＵ１６、ＣＰＵ１６のローカルバス１７、ローカルバス１７に接続されたＲＯＭ１８、ＲＡＭ１９及びＥＥＰＲＯＭ３１を有するコンピュータシステムであり、ローカルバス１７がユーザ端末装置２０のマイクロプロセッサ２１のシステムバス２２に接続される。また、ユーザ端末装置２０のシステムバス２２には装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置（ＣＯＭＭ）２３、ＣＤ－ＲＯＭで供給されるデータを読み込むＣＤ－ＲＯＭドライブ（ＣＤＲＤ）２４、受け取ったデータあるいは加工したデータを外部へ供給するためにフレキシブルディスクドライブに複写するフレキシブルディスクドライブ（ＦＤＤ）２５及びデータを保存するハードディスクドライブ（ＨＤＤ）２６が接続される。なお、ユーザ端末装置のシステムバス２２には当然のこととしてＲＯＭ、ＲＡＭ等が接続されているが、この図においては記載が省略されている。

#### 【００５１】

ＲＯＭ１８には、データ著作権管理プログラム、暗号アルゴリズムに基づく暗号プログラム及びユーザデータ等の固定した情報が格納されている。ＥＥＰＲＯＭ３１には暗号鍵及び著作権情報が格納される。なお、データ著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはＲＯＭ１８ではなく、ＥＥＰＲＯＭ３１に格納される。復号化あるいは再暗号化の作業はデータ著作権管理装置３０が行い、処理結果だけがローカルバス１７及びシステムバス２２を経由してユーザ端末装置２０に転送される。

#### 【００５２】

このデータ著作権管理装置３０は、モノリシックＩＣ、ハイブリッドＩＣ、拡張ボード、ＩＣカードあるいはＰＣカードとして実現される。

## 【0053】

実施例1のデータ著作権管理装置30のROM18には、データ著作権管理プログラム、暗号アルゴリズムに基づく暗号プログラム及びユーザデータ等の固定した情報が格納されている。なお、このROM18には秘密ではない秘密鍵アルゴリズムに基づく秘密鍵生成プログラム、復号化プログラム及び再暗号化プログラムを格納することができる。EEPROM31には暗号鍵及び著作権情報が格納される。なお、著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはROM18ではなく、EEPROM31に格納される。なお、このEEPROMは必ずしも必要なものではなく、省略することも可能である。RAM19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暗号鍵あるいは第2暗号鍵の一方及びデータ著作権管理システムプログラムが格納される。

10

## 【0054】

一方、ユーザ端末装置20のMPU46が必要とするソフトウェア及びユーザデータ等の情報はソフトウェアによりユーザ端末装置20に供給され、ユーザ端末装置20のRAMに格納されている。また、ユーザ端末装置20のRAM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暗号鍵あるいは第2暗号鍵の一方及び著作権管理システムプログラムが格納される。復号化及び再暗号化の作業はユーザ端末装置20本体のMPU46とデータ著作権管理装置30のCPU16が分担して、一方が復号化を他方が再暗号化を行い、データ著作権管理装置30の処理結果だけがユーザ端末装置に転送される。

## 【0055】

20

図4により、図3に示されたデータ著作権管理装置30の具体的な内部構成を示す。データ著作権管理装置30には、マイクロコンピュータ(CPU)16、読み出し専用メモリ(ROM)18、書き込み・読み出しメモリ(RAM)19及び電氣的消去可能プログラマブルメモリ(EEPROM)31が封入され、これらがマイクロコンピュータ16のマイクロコンピュータバス17に接続されており、さらにこのマイクロコンピュータバス17はユーザ端末装置20本体のシステムバス22に接続されている。

## 【0056】

読み出し専用半導体メモリ18にはデータ著作権管理システムプログラム、暗号アルゴリズム及びユーザ情報が格納されている。電氣的消去可能プログラマブルメモリ31の内部は3つのエリアに区分される。第1エリア35には第1公開鍵Kb1、第1専用鍵Kv1、第2公開鍵Kb2及び第2専用鍵Kv2が格納される。第2エリア36には著作権管理プログラムP、視聴許可・蓄積許可・複写許可・加工許可・転送許可等の1次利用における許可鍵となる第1秘密鍵Ks1及び視聴許可・蓄積許可・複写許可・加工許可・転送許可等の2次利用における許可鍵となる第2秘密鍵Ks2が格納される。なお、著作権管理プログラムが外部から供給されるのではなく、ユーザ側に予め置かれることがあるが、その場合著作権管理プログラムは電氣的消去可能プログラマブルメモリ31の第2のエリア36ではなく、読み出し専用メモリ18に格納される。第3エリア37には原著作権情報、2次著作権情報等の著作権情報及びアクセスコントロールキーが格納される。

30

## 【0057】

電氣的消去可能プログラマブルメモリ31と同様に、書き込み・読み出しメモリ19の内部も3つのエリアに区分される。第1エリア32には動作時に第1公開鍵Kb1、第1専用鍵Kv1及び第2公開鍵Kb2が格納される。第2エリア33には動作時に視聴許可・蓄積許可・複写許可・加工許可・転送許可等の1次利用における許可鍵となる第1秘密鍵Ks1が格納される。第3エリア34には動作時にアクセスコントロールキーが格納される。

40

## 【0058】

このデータ著作権管理装置を付属させたユーザ端末装置はデータを利用するためのすべての作業を本発明に係るデータ著作権管理装置内で行い、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ので、安全性が高い。

## 【0059】

情報量が多い画像データを送・受信する場合には、通信データ量を減少させるために原

50

データを圧縮してから送信し、被圧縮データを受信後に伸張して利用するが、この場合にもデータを暗号化することにより著作権管理を行うことが可能である。図5に示されたのは、暗号化されるデータがJ P E G規格あるいはM P E G規格で圧縮されたデジタル画像である場合のデータ著作権管理フローの例であり、このフローは伝送線路を挟んで送信側フローと受信側フローに分けられ、さらに受信側フローは表示フローと保存フローに分けられる。

#### 【0060】

送信側における信号処理はデジタル画像を用意する過程と用意されたデジタル画像を処理する過程から構成されている。この過程において原画像がデジタル画像41である場合にはそのまま次の処理が行われるが、原画像がアナログ画像40である場合にはデジタル

10

#### 【0061】

このような送信側信号処理が行われた画像データは、衛星放送電波、地上波放送電波、C A T V電波あるいは公衆回線・I S D N回線等の伝送線路45を経由して伝送される。なお、この伝送線路としてデジタルビデオテープ、デジタルビデオディスクあるいはC D - R O M等の記録媒体を使用する場合もある。

#### 【0062】

このようにして受信側に伝送された画像データは初めに第1秘密鍵を用いて復号化46され、次に圧縮された画像データの伸張47が行われ、表示49される。表示装置がデジタルデータ表示装置である場合にはそのまま表示されるが、アナログデータ表示装置である場合にはアナログ化48が行われる。

20

#### 【0063】

データがハードディスク、フレキシブルディスク、光磁気ディスク、追記型ビデオディスク等に保存される場合には第2秘密鍵を用いて再暗号化50された上で、保存される。再暗号化されて保存された画像データを再度表示する場合には、第2秘密鍵を用いて再復号化52され、表示49される。表示装置がデジタルデータ表示装置である場合にはそのまま表示されるが、アナログデータ表示装置である場合にはアナログ化48が行われる。なお、データが画像以外のデータである場合のデータ圧縮／伸張手段及び伝送経路はそのデータに適合した適宜なものが使用される。

30

#### 【0064】

図6に示されたのは、先願である特願平6-237673号に示されたデータベース著作権管理システムの例であり、このシステムにおいては暗号鍵方式として秘密鍵方式が採用される。この図に示すシステムにおいて、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、14は通信・放送衛星等の人工衛星、15'はC D - R O Mあるいはフレキシブルディスク等のデータ記録媒体、2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C A T V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

40

#### 【0065】

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C D - R O M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。

#### 【0066】

50

これらのうちデータベース1、鍵管理センタ16、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2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。

10

**【0067】**

データベース1あるいはデータ記録媒体15'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、デジタル音声データ、デ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2、人工衛星14あるいは記憶媒体15'を経由して1次ユーザ端末装置4に一方的に供給されるが、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。

**【0068】**

20

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。

**【0069】**

このシステムでは、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16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2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16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16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2を経由し1次ユーザ端末装置4に転送する。

30

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。

**【0070】**

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2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。

40

50

## 【0071】

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 secondary 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。

10

## 【0072】

この著作権の問題に対処するため、このシステムにおいてはデータ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。

20

## 【0073】

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16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2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16から著作権管理センタ17に登録され、以後の2次利用が可能になる。

## 【0074】

30

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2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2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。

## 【0075】

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2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。

40

## 【0076】

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2を経由して著作権管理センタ17に対してデータ名あるいは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17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2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

50

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。

#### 【0077】

このシステムにおいては、1次利用申込は鍵管理センタ16が処理し、2次利用申込は著作権管理センタ17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16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16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。

#### 【0078】

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。

#### 【0079】

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2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3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2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17に登録され、以後の利用が可能になる。

#### 【0080】

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2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2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。

#### 【0081】

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2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。この各ユーザ情報のデータへの付加には、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。

#### 【0082】

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2を経由して著作権管理

センタ 17 に対してデータ名あるいはデータ番号を指定するとともに 3 次ユーザ情報 I u3 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 I u2 も提示する。著作権管理センタ 17 は、提示された 2 次ユーザ情報 I u2 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 K s3 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 K s3、暗号化／復号化鍵である第 4 秘密鍵 K s4 を通信ネットワーク 2 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 K s3、第 4 秘密鍵 K s4 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 K s3 を用いて暗号化データ Cmks3 が復号化され  $M = D(K s3, Cmks3)$  表示あるいは加工の 3 次利用が行われる。

10

**【0083】**

このシステムにおいては、1 次ユーザが供給されるデータ M は第 1 秘密鍵 K s1 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 K s2 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 K s3 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 16 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 K s1 が、暗号化／復号化鍵として第 2 秘密鍵 K s2 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 K s1 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 17 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 K s2 が、暗号化／復号化鍵として第 3 秘密鍵 K s3 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 K s2 を用いて暗号化データ 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。

20

**【0084】**

以上説明したシステムにおけるデータベース 1、鍵管理センタ 16、著作権管理センタ 17 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 次ユーザからの第 2 秘密鍵再交付申込は鍵管理センタ 16 に対して行うのではなく著作権管理センタ 17 に対して行うようにしてもよい。□ 図 7 に示されたのは、デジタルビデオあるいはデジタルオーディオ等におけるデータの加工方法における信号処理フローであり、(a) に示されたのは、一般的に行われている加工フロー、(b) に示されたのは、信号の劣化を避けることができる加工処理フローである。(a) に示された加工フローにおいて、デジタル信号 (61) として供給された信号は初めにアナログ化 (62) され、次いでアナログ化された信号に対して表示 64 を行いながら加工 (63) が行われ、加工が終了したアナログ信号は再デジタル化 (65) されて保存、複写、転送 (66) される。この過程は簡略ではあるが、信号の加工がアナログ状態で行われ、加工終了後再びデジタル化されるため、信号の劣化を避けることができない。

30

**【0085】**

(b) に示された加工フローにおいて、デジタル信号 (61) は加工のためにアナログ化 (62) されて表示される。アナログ化 (62) された信号は加工 (63) において使用されるが、このアナログ化された信号は表示 (64) に用いられるのみであって、保存、複写、転送には用いられない。保存、複写、転写用の信号は、アナログ化されて表示されている信号と対応してデジタル信号 (61) の状態で、加工 (67) され、保存、複写、転送 (66) が行われる。この加工フローの場合には、保存、複写、転送されるデジタル信号がアナログ化されることはないから劣化は生じない。

40

**【0086】**

図 8 に示されたのは、図 6 に示されたデジタルビデオあるいはデジタルオーディオ等におけるデータの加工方法における信号処理を暗号化されたデータを加工する場合に応用したフローの例であり、(a) に示されたのは、簡略化された信号処理フロー、(b) に示

50



されたのは、著作権の管理を十分に行うことができる信号処理フローの例である。(a)に示された信号処理フローにおいて第1秘密鍵Ks1を用いて暗号化されて供給された原データCm0ks1 71は初めに第1秘密鍵Ks1を用いて復号化72され、 $M0 = D(Ks1, Cm0ks1)$

次いで復号化されたデータM0に対して表示(74)を行いながら加工(73)が行われる。加工が終了したデータM1は第2秘密鍵Ks2を用いて再暗号化(75)されてCm1ks2 = E(Ks2, M1)

保存、複写、転送(76)が行われる。この過程は簡略ではあるが、データの加工が復号化された状態で行われるため、復号化されたデータが保存、複写、転送されるおそれがあり、著作権の管理が十分に行われるとはいえない。

10

#### 【0087】

これに対して、(b)に示された信号処理フローにおいて、第1秘密鍵Ks1を用いて暗号化された原データCm0ks1 (71)は第1秘密鍵Ks1を用いて復号化(72)され、 $M0 = D(Ks1, Cm0ks1)$

復号化されたデータM0が表示(74)される。一方、加工(73)は復号化データM0を手がかりにして暗号化データCm0ks1に対して行われ、保存用の原データM0あるいは加工された加工データM1は第2秘密鍵を用いて再暗号化され $Cm0ks2 = E(Ks2, M0)$

$Cm1ks2 = E(Ks2, M1)$

暗号化データCm0ks2あるいはCm1ks2が保存、複写、転送(76)が行われる。復号化され表示されているデータと対応して復号化されることなく暗号化された状態で加工(77)され、その加工プログラムデータと暗号化されたままのデータが、保存、複写、転送(76)に用いられる。この信号処理フローの場合には、保存、複写、転送用のデータは暗号化されたままであるから、復号化されたデータが保存、複写、転送されることはない。

20

#### 【0088】

本願発明のデータ著作権管理装置が使用されるデータ著作権管理システムにおいては、入手した暗号化データを表示・加工する場合には復号化して利用するが、入手あるいは加工したデータを保存・複写・転送する場合には再暗号化することによって、データ著作権の管理を行う。しかし、図2に示された先願発明のデータ著作権管理装置15及び図3に記載された本発明のデータ著作権管理装置30は暗号化データの復号化あるいは復号化データの暗号化のいずれか一方しか行うことができない。そのため、復号化あるいは加工されたデータを保存・複写・転送する場合には一旦ユーザ端末装置あるいはデータ著作権管理装置のRAMに蓄積しておき、その後蓄積されたデータを再暗号化する必要がある。したがって、処理することができるデータに量的な制限が発生するばかりでなく、事故あるいは操作ミス等により復号化あるいは加工されたデータが失われるおそれがある。

30

#### 【0089】

一部の高級なMPUを除き、パーソナルコンピュータ等で使用される一般的なMPUは複数のマイクロコンピュータを同時に動作させるマルチプロセッサ構成について考慮されていない。したがって、パーソナルコンピュータのシステムバスに付属装置を接続しても複数の作業を同時に行うことはできない。したがって、図2に示されたデータ著作権管理装置15あるいは図3に示されたデータ著作権管理装置30をユーザ端末装置20のシステムバス22に接続してもMPU21あるいは46とCPU16が並列して動作させることが可能なマルチプロセッサ構成とはならず、暗号化されたデータの復号化及び復号化されたデータの再暗号化の作業は同時に行われるのではなく、交互に行われる。そのため、復号化及び暗号化を行うことができるデータの大きさはRAMの容量に制限され、大きなデータを処理することはできない。また、大きなデータではない場合でも、処理速度を高くすることができない。

40

#### 【0090】

一方、先願発明として説明したデータ著作権管理システムにおいては、入手した暗号化

50

データを表示・加工する場合には復号化して利用するが、入手あるいは加工したデータを保存・複製・転送する場合には再暗号化することによって、データの不正規な使用ができないようにしている。したがって、本発明が対象とするデータ著作権管理システムで利用される装置においては、データの復号化だけでなく、データの再暗号化も同時に行われることが望ましい。

#### 【0091】

一般的なパーソナルコンピュータにおいてマルチプロセッサ構成を実現する手段として、最近注目されているものにP C I (Peripheral Component Interconnect) バスがある。このP C I バスは、コンピュータのシステムバスにP C I ブリッジを介して接続される外部接続用のバスであり、P C I バスを使用することでマルチプロセッサ構成を実現する

10

#### 【0092】

図9に示されたのは、本発明実施例2である、P C I バスを使用するデータ著作権管理装置の構成であり、図3に示されたデータ著作権管理装置15と同じ構成すなわち、C P U 16、C P U 16のローカルバス17、ローカルバス17に接続されたR O M 18、R A M 19及びE E P R O M 31を有するコンピュータシステムの構成を有している。一方、ユーザ端末装置20のマイクロプロセッサ21のシステムバス22にはP C I ブリッジ82によって接続されるP C I バス81が接続されており、データ著作権管理装置80のC P U 16のローカルバス17がこのP C I バス81に接続されている。ユーザ端末装置20のシステムバス22にはさらに、装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置(C O M M) 23、C D - R O Mで供給されるデータを読み込むC D - R O Mドライブ(C D R D) 24、受け取ったデータあるいは加工したデータを外部へ供給するためにフレキシブルディスクドライブに複製するフレキシブルディスクドライブ(F D D) 25及びデータを保存するハードディスクドライブ(H D D) 26が接続される。なお、C O M M 23、C D R D 24、F D D 25及びH D D 26はP C I バス81に接続することも可能である。また、ユーザ端末装置のシステムバス22には当然のこととしてR O M、R A M等が接続されているが、この図においては記載が省略されている。

20

#### 【0093】

その他の部分の構成及び動作は図3に示された実施例1の場合と同様なのでさらなる説明は省略する。復号化及び再暗号化の作業はユーザ端末装置20のM P U 21とデータ著作権管理装置80のC P U 16が分担して、一方が復号化を他方が再暗号化を同時に行う。この実施例におけるM P U 21とC P U 16はP C I バスによる並列動作を行うマルチプロセッサ構成であるため、高い処理速度を得ることができる。

30

#### 【0094】

ところで、パーソナルコンピュータ本体に外部装置を取り付けて使用するための代表的な手段として、この他にハードディスク装置あるいはC D - R O Mドライブ等の外部記憶装置が接続されるS C S I (Small Computer System Interface) インターフェースがある。このS C S I インターフェースには、S C S I インターフェースが接続されるパーソナルコンピュータ本体も含めて最大8台の装置を接続することができ、8台の装置として複数のコンピュータを使用することができる。これら複数のコンピュータはどれも同等の役割を果たすことができ、言い換えれば、S C S I インターフェースは単なるインターフェースではなくマルチプロセッサバスとしての機能も有している。実施例3はこのS C S I インターフェースのマルチプロセッサバスとしての機能に着目し、実施例2のP C I バス81に代えてS C S I インターフェース86(以下、理解の便のため「S C S I インターフェース」を「S C S I バス」という。)を介してデータ著作権管理装置85をユーザ端末装置20のシステムバス22に接続する。

40

#### 【0095】

図10に示されたのは、S C S I バスを用いた本発明実施例3のデータ著作権管理装置の構成ブロック図である。この実施例3のデータ著作権管理装置85は、図3に示された

50

データ著作権管理装置と同じ構成すなわち、CPU16、CPU16のローカルバス17、ローカルバス17に接続されたROM18、RAM19及びEEPROM31を有するコンピュータシステムの構成を有している。

#### 【0096】

一方、ユーザ端末装置20のマイクロプロセッサ21のシステムバス22にはSCSIコントローラ(SCSICONT)87によって制御されるSCSIバス86が接続されており、データ著作権管理装置85のCPU16のローカルバス17がこのSCSIバス86に接続されている。また、ユーザ端末装置20のシステムバス22にはさらに、装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置(COMM)23、CD-ROMで供給されるデータを読み込むCD-ROMドライブ(CDRD)24、受け取ったデータあるいは加工したデータを外部へ供給するためにフレキシブルディスクドライブに複写するフレキシブルディスクドライブ(FDD)25及びデータを保存するハードディスクドライブ(HDD)26が接続される。なお、COMM23、CDRD24、FDD25及びHDD26はSCSIバス86に接続することも可能である。また、ユーザ端末装置のシステムバス22には当然のこととしてROM、RAM等が接続されているが、この図においては記載が省略されている。

10

#### 【0097】

その他の部分の構成及び動作は図3に示された実施例1の場合と同様なのでさらなる説明は省略する。復号化及び再暗号化の作業はユーザ端末装置20本体のMPU21とデータ著作権管理装置85のCPU16が分担して、一方が復号化を他方が再暗号化を同時に行い、MPU21とCPU16はSCSIバス86による並列動作を行うマルチプロセッサ構成であるため、高い処理速度を得ることができる。

20

#### 【0098】

なお、この他にマルチプロセッサ構成を実現するための手段としてSCI(Scalable Coherent Interface)等も利用可能であり、さらに可能ならばバスを介することなくマイクロプロセッサ同士を接続してもよい。

#### 【0099】

本願発明のデータ著作権管理装置が管理しようとするデータには、文字データの他にグラフィックデータ、コンピュータプログラム、デジタル音声データ、JPEG等の方式による静止画データ、さらにはMPEG等による動画データがある。これまでに説明した実施例2のデータ著作権管理装置80あるいは実施例3のデータ著作権管理装置85はPCIバスあるいはSCSIバスによってユーザ端末装置20のマイクロプロセッサ21のシステムバス22に接続されることによりマルチプロセッサを構成している。このようなマルチプロセッサ構成の場合、ユーザ端末装置20のMPU21はシステム全体を制御する役割も果たす必要がある。データが文字データ、グラフィックスデータ等比較的低速・小容量のデータである場合にはMPU21とCPU16によるマルチプロセッサ構成でも復号化及び再暗号化によるデータ著作権管理は可能であるが、データがJPEG静止画による動画、MPEG1あるいはMPEG2による動画である場合には、データが高速・大容量であるためこのような構成によるデータ著作権管理は著しく困難である。

30

#### 【0100】

図11に示された第4実施例においては、このような事態に対処するためにPCIバス81に第1のデータ著作権管理装置80及び第2のデータ著作権管理装置90を接続することにより、マルチプロセッサシステムを構成している。第2のデータ著作権管理装置90は第1のデータ著作権管理装置80と同じ構成すなわち、CPU91、CPU91のローカルバス94、ローカルバス94に接続されたROM92、RAM93及びEEPROM95を有している。なお、この実施例において第1のデータ著作権管理装置80は暗号化されたデータの復号化を行い、第2のデータ著作権管理装置90は復号化されたデータの再暗号化を行う。

40

#### 【0101】

暗号化されたデータの復号化を行う第1のデータ著作権管理装置80のROM18には

50

、データベースを利用するための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る。RAM 19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復号化用の第1暗号鍵及びデータ著作権管理システムプログラムが格納される。同様に復号化されたデータの再暗号化を行う第2のデータ著作権管理装置90のROM 92には、データベースを利用するための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、RAM 93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再暗号化用の第2暗号鍵及びデータ著作権管理システムプログラムが格納される。なお、このマルチプロセッサ構成にはSCSIあるいはSCI等も利用可能であり、さらに可能ならばバスを介することなくマイクロプロセッサ同士を接続してもよい。

#### 【0102】

図2に示された先願発明及び図3を用いて説明した本発明の実施例1において、暗号化されたデータが供給される通信装置(COMM)23及びCD-ROMドライブ(CDRD)24はユーザ端末装置20のシステムバスに接続されている。そのため、暗号化されたデータを復号化するためには、暗号化されたデータをユーザ端末装置20のシステムバスとデータ著作権管理装置のローカルバスを経由させなければならず、処理速度の低下を招くおそれがある。これは、これらの付属装置をPCIバスあるいはSCSIバスに接続した場合でも同様である。図12に示された実施例5においては、処理速度の低下を防止するために暗号化されたデータが供給される通信装置23及びCD-ROMドライブ24は復号化用データ著作権管理装置97のローカルバス17に接続される。

#### 【0103】

図12に示された実施例5のデータ著作権管理装置97は復号化用のデータ著作権管理装置であり、図3に示された実施例1のデータ著作権管理装置30と基本的には同じ構成すなわち、CPU16、CPU16のローカルバス17、ローカルバス17に接続されたROM18、RAM19及びEEPROM31を有するコンピュータシステムとして構成され、通信装置COMM23及びCD-ROMドライブCDRD24はローカルバス17に接続される。ROM18には、著作権管理プログラム、暗号アルゴリズムに基づく暗号プログラム及びユーザデータ等の固定した情報が格納されている。EEPROM31には著作権情報が格納される。なお、著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはROM18ではなく、EEPROM31に格納される。RAM19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復号化用暗号鍵及びデータ著作権管理システムプログラムが格納される。COMM23あるいはCDRD24から供給された暗号化データはデータ著作権管理装置97で復号化され、ユーザ端末装置95に転送される。

#### 【0104】

以上説明した実施例4のデータ著作権管理装置80及び90は別体に構成されたものとして記載されているが、これらを一体に構成することが可能であることは言うまでもないことである。

#### 【0105】

実施例5のデータ著作権管理装置100をさらに発展させた実施例6のデータ著作権管理装置を図13に示す。図2に示された先願発明及び図3を用いて説明した本発明の実施例1において、再暗号化されたデータを保存するHDD26等の保存装置はユーザ端末装置20のシステムバス22に接続されている。したがって、再暗号化されたデータを保存するためには、ユーザ端末装置20のシステムバス22とデータ著作権管理装置15あるいはデータ著作権管理装置30のローカルバス17を経由させなければならず、処理速度の低下を招くおそれがある。これはこれらの付属装置をPCIバスあるいはSCSIバスに接続した場合でも同様である。図13に示された実施例6のデータ著作権管理装置100においては、図12に示された実施例5の通信装置COMM23及びCD-ROMドライブCDRD24がローカルバス17に接続された復号化用データ著作権管理装置97に加えて再暗号化されたデータを保存するHDD26等の保存装置を再暗号化用データ著作権管理装置101のローカルバス94に接続する。

## 【0106】

この実施例6に示された再暗号化用のデータ著作権管理装置101は、図3に示されたデータ著作権管理装置30と基本的には同じ構成すなわち、CPU91、CPU91のローカルバス94、ローカルバス94に接続されたROM92、RAM93及びEEPROM95を有するコンピュータシステムとして構成され、ローカルバス94にHDD26が接続される。

## 【0107】

ROM92には、著作権管理プログラム、暗号アルゴリズムに基づく暗号プログラム及びユーザデータ等の固定した情報が格納されている。EEPROM95には著作権情報が格納される。なお、著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはROM92ではなく、EEPROM95に格納される。RAM93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再暗号化用暗号鍵及びデータ著作権管理システムプログラムが格納される。再暗号化用の著作権管理装置101で再暗号化されたデータはHDD26に保存される。

## 【0108】

以上説明した実施例6のデータ著作権管理装置100及び101は別体に構成されたものとして記載されているが、これらを一体に構成することが可能であることは言うまでもないことである。

## 【0109】

デジタルデータには、文字データの他にグラフィックデータ、コンピュータプログラム、デジタル音声データ、JPEG等の方式による静止画データ、さらにはMPEG等による動画データがある。データ著作物を利用するユーザ端末装置として代表的なものはパーソナルコンピュータ等のコンピュータ装置であるが、その他にテレビジョン受像器等の受信装置、これらの受信装置に付属して使用されるセットトップボックス、デジタル信号を保存するデジタルビデオテープレコーダ、デジタルビデオディスクレコーダ、デジタルオーディオテープ(DAT)等のデジタル記録装置あるいは携帯型端末装置(Personal Digital Assistants = PDA)がある。

## 【0110】

拡張ボード、ICカードあるいはPCカードとして構成された先願である特願平6-237673号に記載された図2のデータ著作権管理装置または図6のデータ著作権管理装置をコンピュータ装置、受信装置、セットトップボックス、デジタル記録装置あるいは携帯型端末装置であるユーザ端末装置に付加して使用することも可能であるが、付加時の手間及び障害の発生を考慮するとデータ著作権管理装置はユーザ端末装置に内蔵されていることが望ましい。

## 【0111】

そのためには、本発明の各実施例においてはデータ著作権管理装置の形態としてモノリシックIC、ハイブリッドICあるいは内蔵サブボードの形態を採用して、パーソナルコンピュータ等のコンピュータ装置、テレビジョン受像器等の受信装置、これらの受信装置に付属して使用されるセットトップボックス、デジタル信号を保存するデジタルビデオテープレコーダ、デジタルビデオディスクレコーダ、デジタルオーディオテープ(DAT)等のデジタル記録装置あるいは携帯型端末装置(PDA)等のユーザ端末装置に内蔵させる。

## 【0112】

さらに、以上説明したデータ著作権管理装置はデータの利用だけではなくデジタルキャッシュの流通及びテレビジョン会議システム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ジタルキャッシュシステムは秘密鍵方式で暗号化デ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

10

20

30

40

50

所、例えば家庭等、では使用不可能である。

#### 【0113】

ところで、デ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、PHS(Personal Handyphone System)等ノ携帯電話器、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。

#### 【0114】

このような端末装置をデ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を顧客側銀行に、1次ユーザ端末装置を顧客に、2次ユーザ端末装置を小売店に、著作権管理センタを小売店側銀行に、3次ユーザ端末装置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。

#### 【0115】

デ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使用例を図14を用いて説明する。この使用例は図1に示されたデータ著作権管理システムの構成を利用したものであり、この図において、111は顧客、112は顧客111の取引銀行、113は小売店、114は小売店113の取引銀行、115はメーカ、116はメーカ115の取引銀行、2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111、顧客の取引銀行112、小売店113、小売店の取引銀行114、メーカ115及びメーカの取引銀行116は通信ネットワーク2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111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、117及び118はデ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。

#### 【0116】

この使用例では暗号鍵として顧客側銀行112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。この使用例では顧客側銀行112、小売り店側銀行114、メーカ側銀行116を別個のものとして説明するが、これらを一括して金融システムとして考えてもよい。

#### 【0117】

デジタルキャッシュデータを暗号化／復号化するデジタルキャッシュ管理プログラムPは顧客111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のが望ましい。顧客111はユーザ端末装置を利用して通信ネットワーク2を経由して金額を指定することにより、顧客側銀行112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111の顧客情報Icを提示する。

#### 【0118】

顧客111から預金引出の申込を受けた顧客側銀行112は、第1秘密鍵Ks1を選択あるいは作成し、引出金額のデ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111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

10

20

30

40

50

密鍵  $Ks1$  は顧客側銀行 112 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 111 に固有のものとすることができるばかりでなく、顧客 111 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 112 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。

#### 【0119】

暗号化デ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 111 は、デ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 111 はデジタルキャッシュ管理プログラム  $P$  により暗号化デ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。

#### 【0120】

小売店 113 から物品の購入を希望する顧客 111 は、デ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ジタルキャッシュデータ  $M1$  をデ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 2 を介して暗号化デジタルキャッシュデータ  $Cm1ks2$  を小売店 113 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 113 のユーザ端末装置に転送される。また、残額デジタルキャッシュデータ  $M2$  はデ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 111 のユーザ端末装置内に保存される。

#### 【0121】

暗号化デ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 113 は、転送された暗号化デ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 2 を経由して小売店側銀行 114 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 113 から第 2 秘密鍵  $Ks2$  の転送依頼を受けた小売店側銀行 114 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 112 に転送する。小売店側銀行 114 から第 2 秘密鍵  $Ks2$  の転送依頼を転送された顧客側銀行 112 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 114 に転送する。顧客側銀行 112 から第 2 秘密鍵  $Ks2$  を転送された小売店側銀行 114 は、通信ネットワーク 2 を経由して第 2 秘密鍵  $Ks2$  を小売店 113 に転送する。

#### 【0122】

第 2 秘密鍵  $Ks2$  を転送された小売店 113 は、デジタルキャッシュ管理プログラム  $P$  により第 2 秘密鍵  $Ks2$  を用いて暗号化デジタルキャッシュデータ  $Cm1ks2$  を復号化し、

$M1=D(Ks2, Cmlks2)$

金額を確認の上、商品を顧客111に発送する。なお、この場合小売店111が小売店側銀行114ではなく顧客側銀行112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。

【0123】

小売店113が収受したデジタルキャッシュを小売店側銀行114の口座に入金する場合には、通信ネットワーク2を経由して小売店側銀行114に暗号化デジタルキャッシュデータ $Cmlks2$ とともに顧客情報 $Ic$ を転送する。暗号化デジタルキャッシュデータ $Cmlks2$ と顧客情報 $Ic$ を転送された小売店側銀行114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112に対して依頼する。小売店側銀行114から第2秘密鍵 $Ks2$ の転送を依頼された顧客側銀行112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114に転送する。顧客側銀行112から第2秘密鍵 $Ks2$ を転送された小売店側銀行114は、デジタルキャッシュ管理プログラムPにより第2秘密鍵 $Ks2$ を用いて暗号化デジタルキャッシュデータ $Cmlks2$ を復号化し、 $M1=D(Ks2, Cmlks2)$ 復号化デジタルキャッシュデータ $M1$ を小売店114の銀行口座に入金する。

【0124】

一般的な取引システムにおいては、小売店113はメーカ115あるいはメーカ115と小売店113の間に介在する卸売り店から商品を仕入れ、顧客111に販売する。そのため、顧客111と小売店113との間に存在するのと同様の取引形態が小売店113とメーカ115との間にも存在する。この小売店113とメーカ115との間で行われるデジタルキャッシュの取り扱いは、顧客111と小売店113との間で行われるデ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。

【0125】

このデジタルキャッシュシステムにおける、デ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、デジタルキャッシュの安全性を高めるためにデジタルキャッシュデータにデジタル署名を付けることが望ましい。この使用例において、デ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各種決済システム、例えば信用状(Letter of Credit:L/C)、(Bill of Lading:B/L), Payment of Settlement of Import/ Export にも拡張として応用することができる。

【0126】

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、最近で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二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。

#### 【0127】

この使用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二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確保を行うものである。

10

#### 【0128】

このテレビジョン会議データ管理システムは、例えば図1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をテレビジョン会議第1参加者に、1次ユーザ端末装置をテレビジョン会議第2参加者に、2次ユーザ端末装置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。この使用例を図15を用いて説明する。この図において、121はテレビジョン会議第1参加者、122はテレビジョン会議第2参加者、123はテレビジョン会議第3非参加者、124はテレビジョン会議第4非参加者、2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121とテレビジョン会議第2参加者122は通信ネットワーク2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122とテレビジョン会議第3非参加者123、テレビジョン会議第3非参加者123とテレビジョン会議第4非参加者124は通信ネットワーク2で接続可能とされている。また、125及び126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123及びテレビジョン会議第4非参加者124からテレビジョン会議第1参加者121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121からテレビジョン会議第2参加者122、テレビジョン会議第3非参加者123及びテレビジョン会議第4非参加者124へ暗号鍵が転送される経路である。なお、この使用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121のプライバシー及びデータセキュリティ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122のプライバシー及びデータセキュリティの確保も行うことが可能であることはいうまでもない。

20

30

#### 【0129】

映像及び音声を含むテレビジョン会議第1参加者121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122、テレビジョン会議第3非参加者123及びテレビジョン会議第4非参加者124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、この使用例では暗号鍵としてテレビジョン会議第1参加者121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122が生成する第2秘密鍵、テレビジョン会議第3非参加者123が生成する第3秘密鍵・・・が用いられる。

40

#### 【0130】

テレビジョン会議第1参加者121とテレビジョン会議第2参加者122は、各端末装置を利用し、通信ネットワーク2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121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122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

50

第2参加者122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を端末装置内に保存しておく。

【0131】

テレビジョン会議第1参加者121は、通信ネットワーク2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122に転送する。

【0132】

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122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。

$Ks2 = P(Ks1)$

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122の端末装置内に保存される場合、データ記録媒体125に複写される場合、通信ネットワーク2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。

$Cmks2 = E(Ks2, M)$

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125に複写され、あるいは、通信ネットワーク2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。

【0133】

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123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121に申し込む。

【0134】

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121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123に供給する。

【0135】

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123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123の端末装置内に保存される場合、記録媒体126に複写される場合、通信ネットワーク2を経由してテレビジョン会議第4非参加者124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。

$Cmks2 = E(Ks2, M)$

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。

$Cmks3 = E(Ks3, M)$

(その他)

10

20

30

40

50

本実施の形態は、以下の発明（以下、付記という）を開示する。

（付記１） デジタルデータを利用するユーザ端末装置に付属して用いられるデータ著作権管理装置であって、前記データ著作権管理装置は中央処理装置、中央処理装置バス、読み出し専用半導体メモリ、電氣的消去可能プログラマブルメモリ及び読み出し・書き込みメモリを備え、前記中央処理装置バスには前記中央処理装置、前記読み出し専用半導体メモリ、前記電氣電氣的消去可能プログラマブルメモリ及び前記読み出し・書き込みメモリが接続されるとともに前記ユーザ端末装置のシステムバスが接続可能とされ、前記読み出し専用半導体メモリにはデータ著作権管理システムプログラム、暗号アルゴリズム及びユーザ情報が格納され、前記電氣的消去可能プログラマブルメモリには第２の専用鍵、利用許可鍵、第２の秘密鍵、著作権管理プログラム及び著作権情報が格納され、前記読み出し・書き込みメモリには動作時に第１の公開鍵、第１の専用鍵、第２の公開鍵及び第１の暗号鍵が転送されるデータ著作権管理装置。

10

（付記２） デジタルデータを利用するユーザ端末装置に付属して用いられるデータ著作権管理装置であって、前記データ著作権管理装置は中央処理装置、中央処理装置バス、読み出し専用半導体メモリ、電氣的消去可能プログラマブルメモリ及び読み出し・書き込みメモリを備え、前記中央処理装置バスには前記中央処理装置、前記読み出し専用半導体メモリ、前記電氣電氣的消去可能プログラマブルメモリ及び前記読み出し・書き込みメモリが接続されるとともに前記ユーザ端末装置のシステムバスが接続可能とされ、前記読み出し専用半導体メモリにはデータ著作権管理システムプログラム、著作権管理プログラム、暗号アルゴリズム及びユーザ情報が格納され、前記電氣的消去可能プログラマブルメモリには第２の専用鍵、利用許可鍵、第２の秘密鍵及び著作権情報が格納され、前記読み出し・書き込みメモリには動作時に第１の公開鍵、第１の専用鍵、第２の公開鍵及び第１の暗号鍵が転送されるデータ著作権管理装置。

20

（付記３） ＩＣに構成された付記１または付記２記載のデータ著作権管理装置。

（付記４） ＩＣカードに構成された付記１または付記２記載のデータ著作権管理装置。

（付記５） ＰＣカードに構成された付記１または付記２記載のデータ著作権管理装置。

（付記６） 挿入ボードに構成された付記１または付記２記載のデータ著作権管理装置。

（付記７） 暗号化されたデジタルデータを復号化処理して表示・加工し、復号化されたデータを再暗号化処理して保存・複写・転送を行うユーザ端末装置で用いるデータ著作権管理装置であって、前記データ著作権管理装置はマイクロプロセッサ、前記マイクロプロセッサに接続されるローカルバス、前記ローカルバスに接続される読み出し専用半導体メモリ及び読み出し・書き込みメモリを備えるコンピュータが構成され、前記ユーザ端末装置のマイクロプロセッサと前記データ著作権管理装置のマイクロプロセッサのうち一方が復号化処理を行い他方が再暗号化処理を行うデータ著作権管理装置。

30

（付記８） 暗号化されたデジタルデータを復号化処理して表示・加工し、復号化されたデータを再暗号化処理して保存・複写・転送を行うユーザ端末装置で用いるデータ著作権管理装置であって、前記データ著作権管理装置は第１及び第２のマイクロプロセッサを備え、前記第１のマイクロプロセッサに接続される第１のローカルバス、前記第１のローカルバスに接続される第１の読み出し専用半導体メモリ及び第１の読み出し・書き込みメモリを備える第１のコンピュータ、前記第２のマイクロプロセッサに接続される第２のローカルバス、前記第２のローカルバスに接続される第２の読み出し専用半導体メモリ及び第２の読み出し・書き込みメモリを備える第２のコンピュータが構成され、前記第１のマイクロプロセッサが暗号化されたデータの復号化処理を行い、前記第２のマイクロプロセッサが復号化されたデータの再暗号化処理を行うデータ著作権管理装置。

40

【図面の簡単な説明】

【０１３６】

【図１】 先願発明のデータ著作権管理システムの構成図。

【図２】 先願発明のデータ著作権管理装置の構成図。

【図３】 本発明実施例１のデータ著作権管理装置の構成図。

【図４】 本発明実施例１のデータ著作権管理装置の具体的な構成図。

50

【図 5】本発明に係るデータ著作権管理システムの処理フロー図。

【図 6】先願発明のデータ著作権管理システムの構成図。

【図 7】デジタルデータの一般的な加工処理フロー図。

【図 8】本発明による暗号化データの加工処理フロー図。

【図 9】本発明実施例 2 のデータ著作権管理装置の構成図。

【図 10】本発明実施例 3 のデータ著作権管理装置の構成図。

【図 11】本発明実施例 4 のデータ著作権管理装置の構成図。

【図 12】本発明実施例 5 のデータ著作権管理装置の構成図。

【図 13】本発明実施例 6 のデータ著作権管理装置の構成図。

【図 14】本発明の使用例であるデジタルキャッシュシステムの構成図。

10

【図 15】本発明の使用例であるテレビジョン会議システム構成図。

【符号の説明】

【0137】

1 データベース

2 通信ネットワーク

3, 10, 17 著作権管理センタ

4, 5, 6, 7 ユーザ端末装置

11, 12, 13 記録媒体

14 放送・通信衛星

15' CD-ROM

20

16 鍵管理センタ

17, 22 マイクロコンピュータバス

18 読み出し専用メモリ

19 書き込み・読み出しメモリ

20 ユーザ端末装置

21, 16 マイクロコンピュータ

22 ユーザ端末装置のシステムバス

23 通信装置

24 CD-ROMドライブ

25 フレキシブルディスクドライブ

30

26 ハードディスクドライブ

30, 80, 85, 90, 97, 100, 101 データ著作権管理装置

31 電気電氣的消去可能プログラマブルメモリ

111 顧客

113 小売店

115 メーカ

112 顧客側銀行

114 小売店側銀行

116 メーカ側銀行

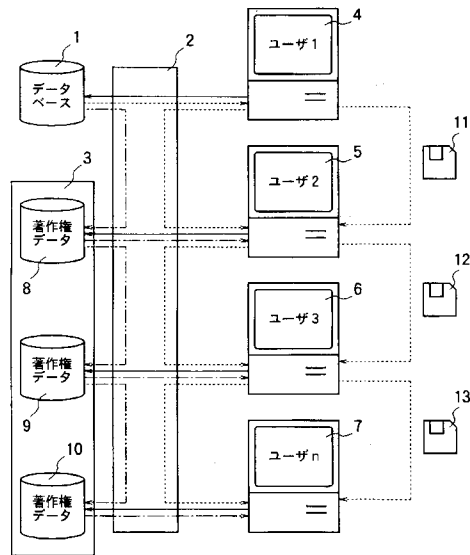
117, 118 ICカード

40

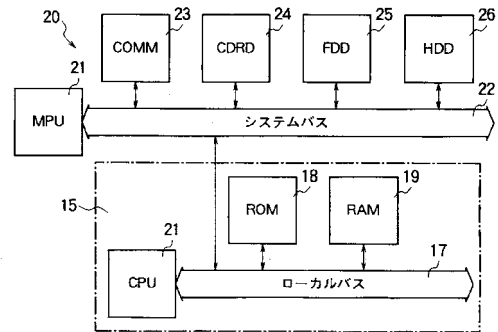
121, 122 テレビジョン会議参加者

123, 124 テレビジョン会議非参加者

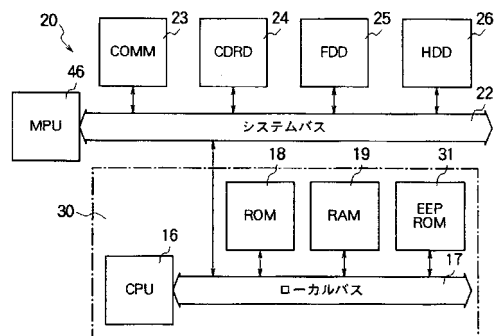
【図 1】



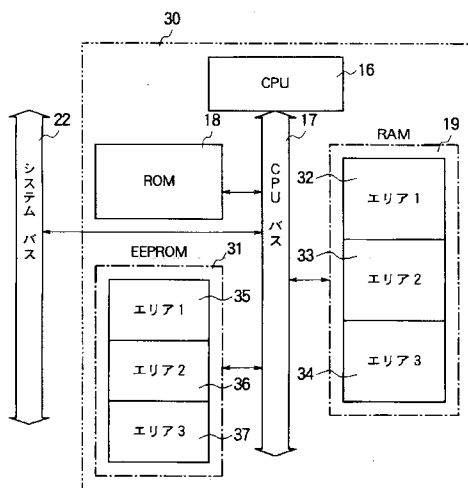
【図 2】



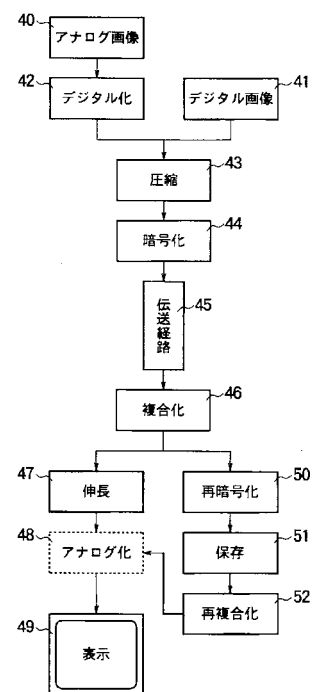
【図 3】



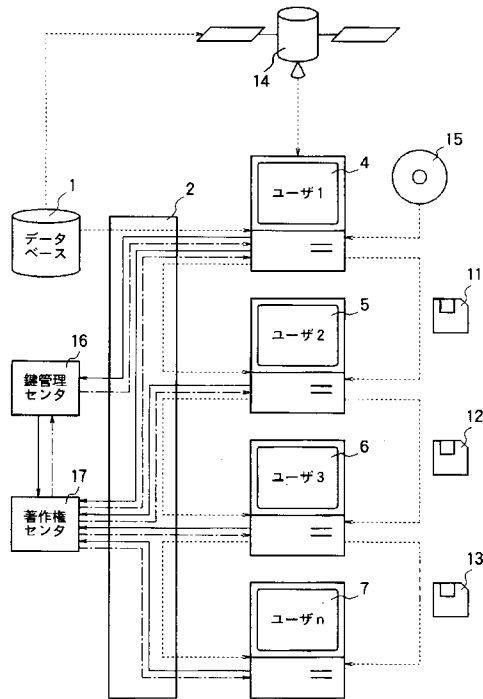
【図 4】



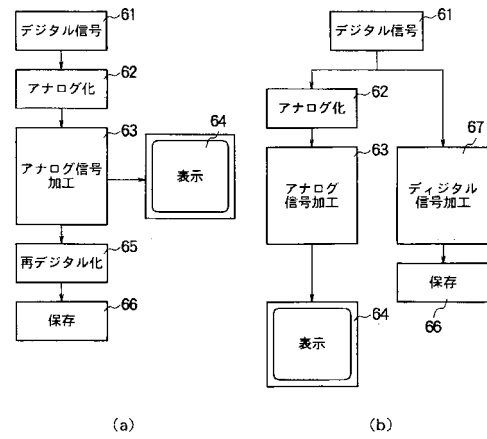
【図 5】



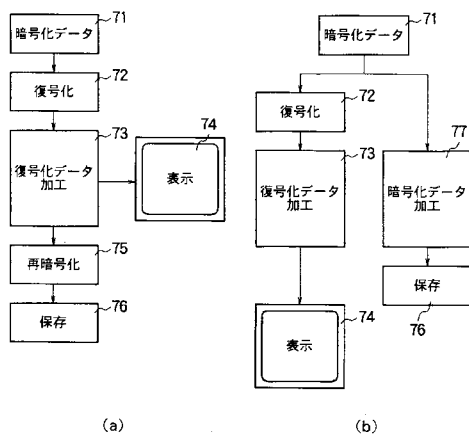
【図 6】



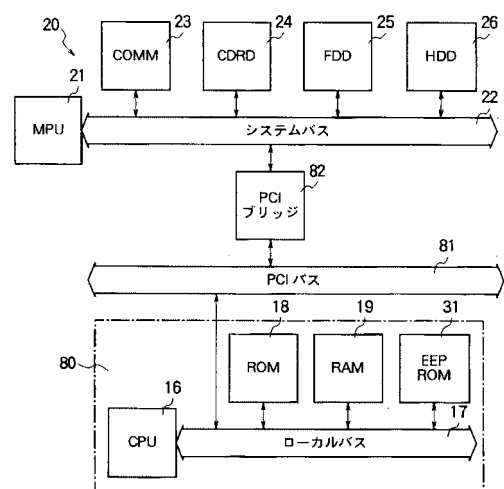
【図 7】



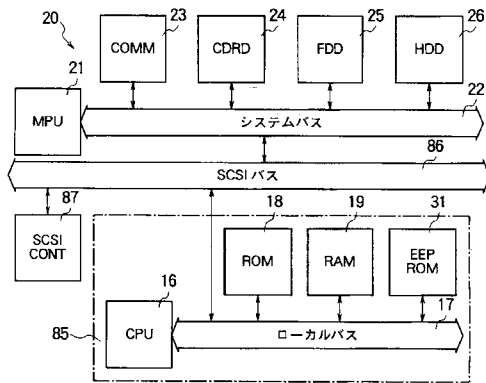
【図 8】



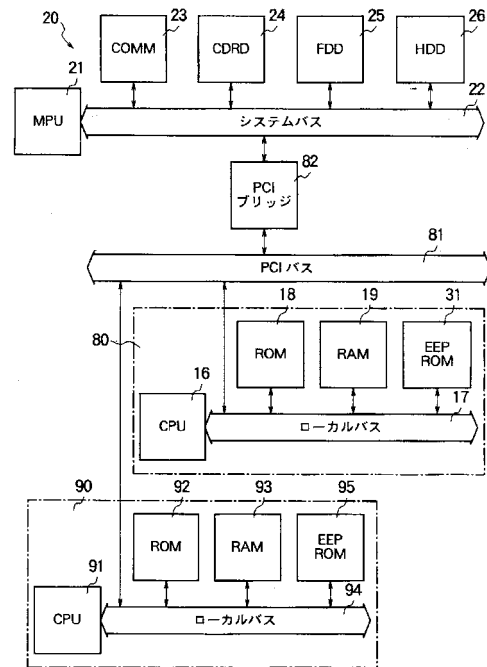
【図 9】



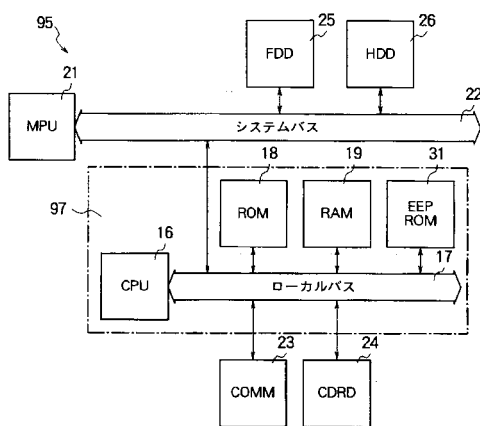
【図 10】



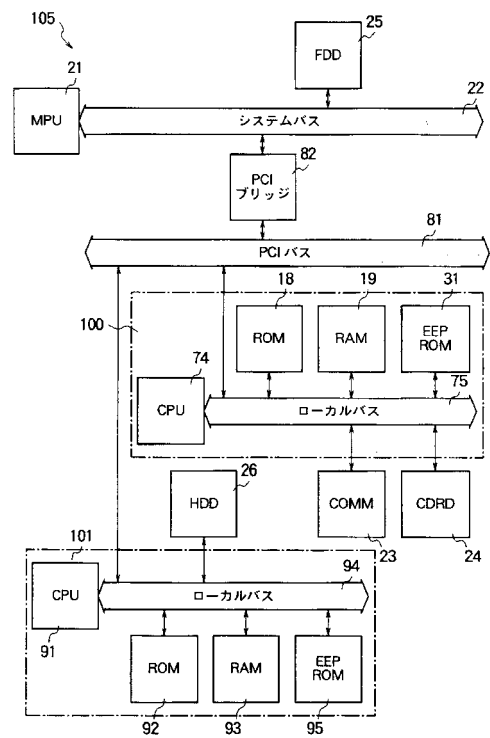
【図 11】



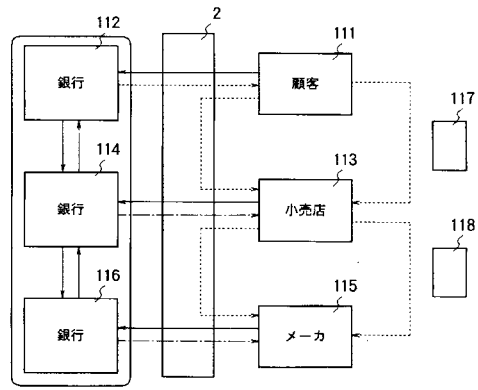
【図 12】



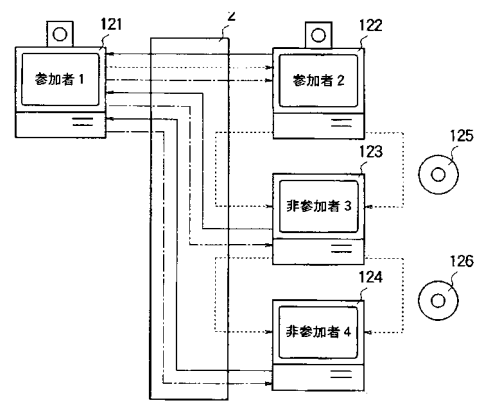
【図 13】



【図 14】



【図 15】





---

フロントページの続き

(51)Int.Cl. F I  
H 0 4 L 9/00 6 2 1 A  
G 0 6 F 15/00 3 3 0 Z

審査官 宮司 卓佳

(56)参考文献 特開平08-287014 (JP, A)  
特開平04-181282 (JP, A)  
特開昭59-169000 (JP, A)

(58)調査した分野(Int.Cl., DB名)  
G 0 6 F 2 1 / 2 4  
G 0 6 F 1 2 / 0 0  
H 0 4 L 9 / 1 0  
G 0 6 F 2 1 / 0 0