(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3925742号
(P3925742)
(45)発行日　平成19年6月6日(2007.6.6)　(24)登録日　平成19年3月9日(2007.3.9)

(51)Int.Cl.　F I
H04N 7/173 (2006.01)　H04N 7/173 640A
H04N 7/173 630

請求項の数 6　(全 20 頁)

(21)出願番号　特願平8-163284
(22)出願日　平成8年6月24日(1996.6.24)
(65)公開番号　特開平10-13808
(43)公開日　平成10年1月16日(1998.1.16)
審査請求日　平成15年3月10日(2003.3.10)

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100098291
弁理士　小笠原　史朗
(72)発明者　大森　基司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　松崎　なつめ
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　舘林　誠
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】情報提供システム

(57)【特許請求の範囲】
【請求項１】
１以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払う情報提供システムであって、
前記１以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、
前記契約者側には、情報サーバおよびオフライン端末が設けられ、
前記情報サーバは、
前記１以上の情報提供者が提供する情報を受信する受信手段と、
前記受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、
前記課金手段が算定して得られた利用料金を記録するデータ記録手段と、
前記オフライン端末に伝達する前記情報を、書き込み／読み出し可能な第１の携帯型記録媒体に記録し、かつ、前記オフライン端末に伝達する前記実行権データを、第２の携帯型記録媒体に記録する記録手段とを備え、
前記オフライン端末は、前記第２の携帯型記録媒体を介して前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第１の携帯型記録媒体を介して前記情報サーバから伝達された情報の利用を許可することを特徴とする情報提供システム。

【請求項２】
前記１以上の情報提供者が提供する情報は、それぞれ暗号化されており、
前記情報サーバは、前記受信手段が受信した情報を復号する第１の復号手段をさらに備えることを特徴とする、請求項１に記載の情報提供システム。
【請求項３】
前記情報サーバは、前記第１の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、
前記オフライン端末は、前記第１の携帯型記録媒体を介して前記情報サーバから伝達された、再暗号化された情報を、前記第２の携帯型記録媒体を介して前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第２の復号手段を備えることを特徴とする、請求項２に記載の情報提供システム。
【請求項４】
前記情報サーバは、
乱数を発生する乱数発生手段と、
前記第１の復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、
前記記録手段はさらに、前記オフライン端末に伝達する前記乱数を、前記第２の携帯型記録媒体に記録し、
前記オフライン端末は、前記第１の携帯型記録媒体を介して前記情報サーバから伝達された、再暗号化された情報を、前記第２の携帯型記録媒体を介して前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第２の携帯型記録媒体を介して前記情報サーバから伝達された乱数で復号する第２の復号手段を備えることを特徴とする、請求項２に記載の情報提供システム。
【請求項５】
１以上の情報提供者から提供される、利用料金を算定するための課金基準データが付加された情報を、利用料金を支払ってオフライン端末に利用させる、契約者側に設けられる情報サーバであって、
前記１以上の情報提供者が提供する情報を受信する受信手段と、
前記受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、
前記課金手段が算定して得られた利用料金を記録するデータ記録手段と、
前記オフライン端末に伝達する前記情報を、書き込み／読み出し可能な第１の携帯型記録媒体に記録し、かつ、前記オフライン端末に伝達する前記実行権データを、第２の携帯型記録媒体に記録する手段とを備える情報サーバ。
【請求項６】
１以上の情報提供者から配信される情報を契約者に提供するために、前記契約者側に設けられる情報サーバおよびオフライン端末を含む情報提供システムによって実行される情報提供方法であって、
前記１以上の情報提供者から配信される情報には、当該情報の利用料金を算定するための課金基準データが付加されており、
前記情報サーバが、前記１以上の情報提供者が提供する情報を受信し、
前記情報サーバが、受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、
前記情報サーバが、作成した実行権データおよび受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、
前記情報サーバが、算定して得た利用料金を記録し、
前記情報サーバが、前記オフライン端末に伝達する前記情報を、書き込み／読み出し可能な第１の携帯型記録媒体に記録し、かつ、前記オフライン端末に伝達する実行権データを、第２の携帯型記録媒体に記録し、

前記オフライン端末が、前記第２の携帯型記録媒体を介して前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第１の携帯型記録媒体を介して前記情報サーバから伝達された情報の利用を許可することを特徴とする、前記情報提供システムによる情報提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報提供システムに関し、より特定的には、情報提供者が契約者に情報を提供して、利用度合に応じて課金する情報提供システムに関する。

【０００２】

【従来の技術】

近年、ＢＳ放送、ＣＳ放送、ディジタルＣＡＴＶなど、有料情報提供サービスが広く行なわれるようになった。こうしたサービスでは、通常、ユーザは、情報提供者に、毎月、一定の金額の利用料金を支払うことにより、情報提供者が提供する情報を、自由に利用することができる。このため、提供される情報を、ＶＴＲ等により記録して繰り返し利用したり、さらには、記録した情報を、他のユーザに貸与あるいは譲渡するような行為が少なからず行われ、情報提供者の利益が守られないという不都合が生じている。

【０００３】

そこで、上記のような行為を制限することができる情報提供システムの開発が行われている。以下には、こうしたシステムの一例として、特開平７－１６２８３２号公報に記載されている映像情報伝送装置について説明する。この装置は、映像情報をスクランブルされたままで記録することができ、従って、記録された情報の再生に一定の制限を加えることができる。

【０００４】

図６は、上記従来の映像情報伝送装置の構成を示すブロック図である。図６の装置は、送信装置９０１、受信装置９０６および伝送路９０５で構成されている。送信装置９０１は、スクランブル装置９０２、再生限定情報生成装置９０３、多重装置９０４を備えている。受信装置９０６は、分離装置９０７、変換装置９０８、ＩＣカードＩ／Ｆ９０９、ＩＣカード９１０、ＶＴＲ９１１およびデスクランブル装置９１２を備えている。

【０００５】

図６のスクランブル装置９０２は、映像情報をスクランブルする。再生限定情報生成装置９０３は、受信装置９０６での再生を限定するための再生限定情報を生成する。多重装置９０４は、映像情報と再生限定情報とを多重化する。分離装置９０７は、多重化された情報を、映像情報と再生限定情報とに分離する。変換装置９０８は、映像情報のフォーマットを変換する。ＶＴＲ９１１は、映像情報を記録する。ＩＣカードＩ／Ｆ９０９は、ＩＣカード９１０に再生限定情報を記録する。ＩＣカード９１０は、再生限定情報を格納する。デスクランブル装置９１２は、再生限定情報に基づいて、スクランブルされた映像信号をデスクランブルする。

【０００６】

以下には、図６の映像情報伝送装置の動作について説明する。

送信装置９０１において、スクランブル装置９０２が映像情報をスクランブルする一方、再生限定情報生成装置９０３は、制御情報に従って、再生限定情報を生成して暗号化するとともに、スクランブル装置９０２に対してスクランブル情報を与える。多重装置９０４は、スクランブル装置９０２が出力する映像情報と、再生限定情報生成装置９０３が与える再生限定情報とを多重化して、伝送路９０５を介して受信装置９０６へ送信する。

【０００７】

送信された情報は、受信装置９０６の分離装置９０７により、映像情報と再生限定情報とに分離される。分離して得られた映像情報は、変換装置９０８において、伝送用のフォーマットから記録用のフォーマットに変換された後、ＶＴＲ９１１により、磁気テープに記録される。一方、分離して得られた再生限定情報は、ＩＣカードＩ／Ｆ９０９においてＩ

Ｃカード９１０に記録される。
ユーザがＩＣカード９１０をデスクランブル装置９１２に接続すると、デスクランブル装置９１２は、ＩＣカード９１０から読み出した再生限定情報が許可する範囲内で、ＶＴＲ９１１に記録された映像情報をデスクランブルする。
【０００８】
【発明が解決しようとする課題】
上記のように、図６の装置は、映像情報が録画されて、無制限に再生されるのを防ぐことができる。
しかし、情報提供者にとって、ユーザとの間で、毎月の利用料金を予め一定の金額に決めておき、一方で、上記装置等を用いて、情報の利用を、予め定めた利用度合の上限以下に制限するような方法は、必ずしも有益なものとはいえない。ユーザが情報を記録して繰り返し利用したいと希望するのであれば、記録して好きな回数だけ利用してもらい、利用度合に応じて、利用料金を徴収する方がより望ましい。同様に、ユーザが記録した情報を他のユーザに貸与あるいは譲渡したいと望む場合にも、一定の条件の下で、貸与あるいは譲渡してもらい、利用度合に応じて、いずれかのユーザから利用料金を徴収するのが望ましい。
【０００９】
また、ユーザにとっても、情報を記録して利用できなかったり、他のユーザが記録した情報を利用できないのは不便であり、また、利用料金を予め一定の金額に決めておくと、情報を利用する頻度によっては、利益にならない場合がある。
【００１０】
従って、本発明の目的は、情報提供者からユーザに情報を提供して、利用度合に応じて課金することができるような情報提供システムを提供することである。
【００１１】
また、情報が正規のユーザ以外の者によって利用されたり、課金に関するデータが不正に操作されるようなことがあると、利用度合に応じた課金を正しく行うことができない。
【００１２】
従って、本発明の他の目的は、上記システムにおいて、情報や課金に関するデータを、より安全に伝達できるようにすることである。
【００１３】
【課題を解決するための手段および発明の効果】
第１の発明は、１以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払う情報提供システムであって、
１以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、
契約者側には、情報サーバおよびオフライン端末が設けられ、
情報サーバは、
１以上の情報提供者が提供する情報を受信する受信手段と、
受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、
課金手段が算定して得られた利用料金を記録するデータ記録手段と、
オフライン端末に伝達する情報を、書き込み／読み出し可能な第１の携帯型記録媒体に記録し、かつ、オフライン端末に伝達する実行権データを、第２の携帯型記録媒体に記録する記録手段とを備え、
オフライン端末は、第２の携帯型記録媒体を介して情報サーバから伝達された実行権データが所定の条件を満たす場合に、第１の携帯型記録媒体を介して情報サーバから伝達された情報の利用を許可することを特徴としている。
【００２４】

上記のように、第１の発明では、１以上の情報提供者側に設けられた配信手段はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側には、情報サーバおよびオフライン端末が設けられ、情報サーバの受信手段は、１以上の情報提供者が提供する情報を受信する。課金手段は、受信手段が受信した情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。受信手段が受信した情報および課金手段が作成した実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。情報は、書き込み／読み出し可能な第１の携帯型記録媒体を介して、オフライン端末に伝達され、かつ、実行権データは、第２の携帯型記録媒体を介して、オフライン端末に伝達される。

【００２５】

このように、情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、契約者がオフライン端末において情報を利用する場合、利用度合に応じた課金ができる。

【００２６】

第２の発明は、第１の発明において、１以上の情報提供者が提供する情報は、それぞれ暗号化されており、

情報サーバは、受信手段が受信した情報を復号する第１の復号手段をさらに備えることを特徴としている。

【００２７】

これにより、１以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、当該情報を復号できる。

【００２８】

第３の発明は、第２の発明において、情報サーバは、第１の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、

オフライン端末は、第１の携帯型記録媒体を介して情報サーバから伝達された、再暗号化された情報を、第２の携帯型記録媒体を介して情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第２の復号手段を備えることを特徴としている。

【００２９】

これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【００３０】

第４の発明は、第２の発明において、情報サーバは、

乱数を発生する乱数発生手段と、

第１の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、

記録手段はさらに、オフライン端末に伝達する乱数を、第２の携帯型記録媒体に記録し、

オフライン端末は、第１の携帯型記録媒体を介して情報サーバから伝達された、再暗号化された情報を、第２の携帯型記録媒体を介して情報サーバから伝達された実行権データが所定の条件を満たす場合に、第２の携帯型記録媒体を介して情報サーバから伝達された乱数で復号する第２の復号手段を備えることを特徴としている。

【００３１】

上記のように、第４の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、第１の復号手段が復号して得られた情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データがオフライン端末に伝達されると、第２の復号手段は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【００６９】

第５の発明は、１以上の情報提供者から提供される、利用料金を算定するための課金基準データが付加された情報を、利用料金を支払ってオフライン端末に利用させる、契約者側に設けられる情報サーバであって、

１以上の情報提供者が提供する情報を受信する受信手段と、

受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、

課金手段が算定して得られた利用料金を記録するデータ記録手段と、

オフライン端末に伝達する情報を、書き込み／読み出し可能な第１の携帯型記録媒体に記録し、かつ、オフライン端末に伝達する実行権データを、第２の携帯型記録媒体に記録する手段とを備えている。

【００７０】

上記のように、第５の発明では、１以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。受信手段は、１以上の情報提供者が提供する情報を受信する。課金手段は、受信手段が受信した情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。受信手段が受信した情報および課金手段が作成した実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。情報は、書き込み／読み出し可能な第１の携帯型記録媒体を介して、オフライン端末に伝達され、かつ、実行権データは、第２の携帯型記録媒体を介して、オフライン端末に伝達される。

【００７１】

このように、情報サーバは、情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、情報を利用するのを許可する。これにより、契約者がオフライン端末において情報を利用する場合、利用度合に応じた課金ができる。

【００８９】

このように、情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。これにより、契約者がオフライン端末で情報を利用する場合、利用度合に応じて課金できる。

【００９８】

第６の発明は、１以上の情報提供者から配信される情報を契約者に提供するために、契約者側に設けられる情報サーバおよびオフライン端末を含む情報提供システムによって実行される情報提供方法であって、

１以上の情報提供者から配信される情報には、当該情報の利用料金を算定するための課金基準データが付加されており、

情報サーバが、１以上の情報提供者が提供する情報を受信し、
情報サーバが、受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、
情報サーバが、作成した実行権データおよび受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、
情報サーバが、算定して得た利用料金を記録し、
情報サーバが、オフライン端末に伝達する情報を、書き込み／読み出し可能な第１の携帯型記録媒体に記録し、かつ、オフライン端末に伝達する実行権データを、第２の携帯型記録媒体に記録し、
オフライン端末が、第２の携帯型記録媒体を介して情報サーバから伝達された実行権データが所定の条件を満たす場合に、第１の携帯型記録媒体を介して情報サーバから伝達された情報の利用を許可することを特徴としている。

【００９９】

上記のように、第６の発明では、１以上の情報提供者は、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側には情報サーバおよびオフライン端末が設けられており、情報サーバは、提供される情報を受信すると、当該情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成する。次に、情報サーバは、作成した実行権データ、および受信した情報に付加された課金基準データに基づいて、当該情報の利用料金を算定して記録する。なお、記録された利用料金は所定の方法で情報提供者に通知され、契約者は当該料金を支払うことになる。受信された情報および作成された実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。情報は、書き込み／読み出し可能な第１の携帯型記録媒体を介して、オフライン端末に伝達され、かつ、実行権データは、第２の携帯型記録媒体を介して、オフライン端末に伝達される。

【０１００】

このように、情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、契約者がオフライン端末において情報を利用する場合、利用度合に応じて課金できる。

【０１０６】

【発明の実施の形態】

図１は、本発明の一実施形態に係る情報提供システムの構成を示すブロック図である。図１のシステムは、情報提供者Ｘ１、情報提供者Ｙ２および情報提供者Ｚ３ならびに契約者Ａ４および契約者Ｂ５で構成されている。なお、契約者とは、１以上のユーザからなる、一つの世帯を意味する。

契約者Ａ４と契約者Ｂ５とは、通信回線／ＣＡＴＶ網を介して、または、携帯型の記録媒体を介して、双方向に情報のやりとりを行うことができる。ただし、以下では、携帯型の記録媒体を介して情報のやりとりを行う場合に限定して説明する。

【０１０７】

情報提供者Ｘ１、情報提供者Ｙ２および情報提供者Ｚ３はそれぞれ、契約者Ａ４および契約者Ｂ５に、衛星放送、地上波放送、ディジタルＣＡＴＶ網などを介して、映像情報、文字情報などの情報を提供する。その際、各情報提供者（１～３）は、それぞれが定めた配信方式、暗号方式および課金方式を用いることができる。

【０１０８】

契約者Ａ４および契約者Ｂ５はそれぞれ、各情報提供者（１～３）が提供する情報を利用して、各情報提供者（１～３）に、定期的に利用料金を支払う。ただし、利用料金は、契約者（４、５）毎に、情報を利用した度合に応じて算定される。なお、算定された利用料

金は、電話回線、パソコン通信網、ディジタルＣＡＴＶ網などを通じて、各情報提供者（１～３）に通知される。

【０１０９】

各情報提供者（１～３）は、提供しようとする情報を暗号化したうえ、情報識別子、課金基準データおよび記録許可フラグを付加して提供する。

ここで、情報識別子は、その情報を他の情報と区別するためのものであって、どの情報提供者（１～３）から提供された情報であるかを示すデータも含まれる。課金基準データは、その情報の利用料金を算定するためのデータであって、リアルタイムに利用する場合の利用料金、記録して利用する場合の利用料金などのデータを含んでいる。記録許可フラグは、その情報を契約者（４、５）側で記録できるか否かを示すフラグであって、その情報が、記録できるものであれば１、記録できないものであれば０と定められている。

【０１１０】

図１の契約者Ａ４は、情報サーバ１０ａ、１以上のユーザ端末２０ａ、移動ディスク３０ａ、ＩＣカード４０ａおよびオフライン端末５０ａを備えている。

移動ディスク３０ａは、書き込み／読み出しが可能な携帯型の記録媒体であり、ＩＣカード４０ａは、記録されたデータの不正な解析／変更が困難な携帯型の記録媒体である。情報サーバ１０ａは、受信した情報をユーザ端末２０ａに送信し、かつ、移動ディスク３０ａおよびＩＣカード４０ａに、それぞれ、情報、データ類を記録する。ユーザ端末２０ａは、情報サーバ１０ａから送信された情報を受信し、かつ、移動ディスク３０ａおよびＩＣカード４０ａにそれぞれ記録された、情報、データ類を読み出す。ユーザ端末２０ａはまた、ユーザが入力する命令等を情報サーバ１０ａに伝達することができる。オフライン端末５０ａは、移動ディスク３０ａおよびＩＣカード４０ａにそれぞれ記録された、情報、データ類を読み出す。

【０１１１】

図１の情報サーバ１０ａは、Ｘの受信部１０１ａ、Ｘの復号部１０２ａ、Ｘの課金部１０３ａ、Ｙの受信部１０４ａ、Ｙの復号部１０５ａ、Ｙの課金部１０６ａ、Ｚの受信部１０７ａ、Ｚの復号部１０８ａ、Ｚの課金部１０９ａ、情報記録部１１０ａ、共通暗号化部１１１ａ、データ記録部１１２ａおよび乱数発生部１１３ａを備えている。

【０１１２】

Ｘの受信部１０１ａは、情報提供者Ｘ１が配信する情報を受信する。Ｘの復号部１０２ａは、Ｘの受信部１０１ａが受信した情報、および情報記録部１１０ａに記録された情報のうち情報提供者Ｘ１が提供した情報を復号する。Ｘの課金部１０３ａは、Ｘの復号部１０２ａが復号する情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する。Ｘの課金部１０３ａはまた、必要に応じて、実行権データを作成する。

Ｙの受信部１０４ａは、情報提供者Ｙ２が配信する情報を受信する。Ｙの復号部１０５ａは、Ｙの受信部１０４ａが受信した情報、および情報記録部１１０ａに記録された情報のうち情報提供者Ｙ２が提供した情報を復号する。Ｙの課金部１０６ａは、Ｙの復号部１０５ａが復号する情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する。Ｙの課金部１０６ａはまた、必要に応じて、実行権データを作成する。

Ｚの受信部１０７ａは、情報提供者Ｚ３が配信する情報を受信する。Ｚの復号部１０８ａは、Ｚの受信部１０７ａが受信した情報、および情報記録部１１０ａに記録された情報のうち情報提供者Ｚ３が提供した情報を復号する。Ｚの課金部１０９ａは、Ｚの復号部１０８ａが復号する情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する。Ｚの課金部１０９ａはまた、必要に応じて、実行権データを作成する。

【０１１３】

ここで、実行権データとは、オフライン端末５０ａで情報を利用する場合や、契約者Ａ４が受信した情報を契約者Ｂ５に再提供して、契約者Ｂ５のユーザがユーザ端末２０ｂで情報を利用する場合に、その情報の利用度合およびその情報を利用可能な端末を制限するためのものであって、利用可能回数、記録モードおよび課金モードを含む。

【０１１４】

利用可能回数は、その情報を利用することができる回数であり、利用にともなって更新される。記録モードは、その情報を利用可能な端末を限定するためのものであって、オフライン端末５０ａで利用する場合は１、契約者Ｂ５のユーザ端末２０ｂで利用する場合には２と定められている。課金モードは、その情報が課金済みの情報であるか否かを示すものであって、課金済みであれば１、未課金であれば２と定められている。

【０１１５】

情報記録部１１０ａは、各受信部（１０１ａ、１０４ａ、１０７ａ）が受信した情報を記録する。ただし、情報記録部１１０ａは、記録しようとする情報に付加された記録許可フラグが１であるか否かを判定する機能を有し、記録許可フラグが１でない情報は記録しない。データ記録部１１２ａは、各課金部（１０３ａ、１０６ａ、１０９ａ）が算定して得られた利用料金を記録する。データ記録部１１２ａはまた、ユーザ端末２０ａ毎の秘密鍵を記憶している。乱数発生部１１３ａは、乱数を発生する。

【０１１６】

共通暗号化部１１１ａは、本システムに共通の暗号化アルゴリズムを保有しており、当該アルゴリズムに従って、各復号部（１０２ａ、１０５ａ、１０８ａ）が復号して得られた情報を、乱数発生部１１３ａが発生した乱数で再暗号化する。共通暗号化部１１１ａはまた、秘密鍵暗号化アルゴリズムを保有しており、再暗号化して得た情報がユーザ端末２０ａに伝達される場合、乱数発生部１１３ａが発生した乱数を、当該アルゴリズムに従って、データ記録部１１２ａが記憶している、ユーザ端末２０ａ毎の秘密鍵で暗号化する。なお、各課金部（１０３ａ、１０６ａ、１０９ａ）およびデータ記録部１１２ａは、解析、変造ないしは複製ができないような領域に配置されている。

【０１１７】

ユーザ端末２０ａは、共通復号部２０１ａを備えている。共通復号部２０１ａは、ユーザ端末２０ａに固有の秘密鍵、および秘密鍵復号アルゴリズムを保有しており、情報サーバ１０ａから伝達される、暗号化された乱数を、当該アルゴリズムに従って、この秘密鍵で復号する。共通復号部２０１ａはまた、本システムに共通の復号アルゴリズムを保有しており、当該アルゴリズムに従って、情報サーバ１０ａから伝達される、再暗号化された情報を、復号して得た乱数で復号し、かつ、情報サーバ１０ｂから伝達される、再暗号化された情報を、情報サーバ１０ｂから伝達される乱数で復号する。ただし、共通復号部２０１ａは、情報サーバ１０ｂから伝達される実行権データが所定の条件を満足するか否かを判定する機能を有しており、満足しない場合には、情報サーバ１０ｂから伝達される、再暗号化された情報を、情報サーバ１０ｂから伝達される乱数で復号する動作を行わない。

【０１１８】

オフライン端末５０ａは、共通復号部５０１ａを備えている。共通復号部５０１ａは、本システムに共通の復号アルゴリズムを保有しており、情報サーバ１０ａから伝達される、再暗号化された情報を、当該アルゴリズムに従って、情報サーバ１０ａから伝達される乱数で復号する。ただし、共通復号部５０１ａは、情報サーバ１０ａから伝達される実行権データが所定の条件を満足するか否かを判定する機能を有しており、満足しない場合には、再暗号化された情報を乱数で復号する動作を行わない。

【０１１９】

なお、契約者Ｂ５についても、オフライン端末５０ａを含まない点を除いて、上記と同様である。ただし、図１において、契約者Ｂ５の各構成要素の参照番号は、情報サーバ１０ｂ、Ｘの復号部１０２ｂなどのように、契約者Ａ４のものと区別されている。

【０１２０】

以下には、情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して、リアルタイムに利用する場合、記録して利用する場合、オフライン端末５０ａで利用する場合、および契約者Ａ４が受信して、契約者Ｂ５が利用する場合について、それぞれ本システムの動作を説明する。

（１）リアルタイムに利用する場合

図２は、情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して、リアルタイムに利用

する場合の、図１のシステムの動作を示すフローチャートである。
以下には、図２を用いて、図１の契約者Ａ４が情報提供者Ｘ１から提供される情報を受信し、契約者Ａ４のユーザが、その情報をユーザ端末２０ａでリアルタイムに利用する場合について説明する。
ユーザが、情報提供者Ｘ１が提供している、ある情報を利用したい意を、ユーザ端末２０ａに入力すると、ユーザ端末２０ａは、その意を情報サーバ１０ａに通知する。
【０１２１】
通知を受けると、情報サーバ１０ａのＸの復号部１０２ａは、Ｘの受信部１０１ａが受信した、暗号化された情報を復号する（ステップＳ１０１）。Ｘの課金部１０３ａは、その情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する（ステップＳ１０２）。ただし、利用料金は、リアルタイムに情報を利用する場合の基準に基づいて算定される。Ｘの課金部１０３ａが算定して得られた利用料金は、データ記録部１１２ａが、情報提供者（１～３）毎に記録する（ステップＳ１０３）。なお、データ記録部１１２ａが記録した利用料金は、電話回線、パソコン通信網、ディジタルＣＡＴＶ網などを通じて、定期的に各情報提供者（１～３）に通知され、契約者Ａ４は、その料金を支払うことになる。
【０１２２】
次に、乱数発生部１１３ａが乱数ｒを発生し、共通暗号化部１１１ａは、Ｘの復号部１０２ａが復号して得られた情報（ＣＯＮＴ）を、本システムに共通の暗号化アルゴリズム（ＣＯＭ）に従って、乱数ｒで再暗号化する（ステップＳ１０４）。共通暗号化部１１１ａは、さらに、秘密鍵暗号化アルゴリズム（Ｅ）に従って、データ記録部１１２ａが記憶している、ユーザ端末２０ａ毎の秘密鍵ｓｉで、乱数ｒを暗号化する（ステップＳ１０５）。情報サーバ１０ａは、共通暗号化部１１１ａが再暗号化して得られた情報ＣＯＭ（ｒ，ＣＯＮＴ）および暗号化して得られた乱数Ｅ（ｓｉ，ｒ）を、ユーザ端末２０ａに送信する（ステップＳ１０６）。ここで、ａ（ｂ，ｃ）は、アルゴリズムａに従って、鍵ｂでデータｃを暗号化することを意味する。
【０１２３】
ユーザ端末２０ａが、再暗号化された情報ＣＯＭ（ｒ，ＣＯＮＴ）および暗号化された乱数Ｅ（ｓｉ，ｒ）を受信すると（ステップＳ１０７）、ユーザ端末２０ａの共通復号部２０１ａは、最初、秘密鍵復号アルゴリズムに従って、記憶している秘密鍵ｓｉで、暗号化された乱数Ｅ（ｓｉ，ｒ）を復号して、乱数ｒを取り出し（ステップＳ１０８）、次に、再暗号化された情報ＣＯＭ（ｒ，ＣＯＮＴ）を、本システムに共通の復号アルゴリズムに従って、取り出した乱数ｒで復号して、情報（ＣＯＮＴ）をさらに取り出す（ステップＳ１０９）。ユーザ端末２０ａは、共通復号部２０１ａが復号して得られた情報（ＣＯＮＴ）を表示する。こうして、ユーザは、情報（ＣＯＮＴ）を利用することができる（ステップＳ１１０）。
【０１２４】
このように、情報提供者Ｘ１は、提供しようとする情報を暗号化したうえ、その情報の利用料金を算定するための課金基準データを付加して提供する。契約者Ａ４には、情報サーバ１０ａおよび１以上のユーザ端末２０ａが設けられ、情報サーバ１０ａのＸの受信部１０１ａは、情報提供者Ｘ１が提供する情報を受信する。Ｘの課金部１０３ａは、Ｘの復号部１０２ａが復号して得られた情報が、ユーザ端末２０ａに伝達される際に、その情報に付加された課金基準データに基づいて、その情報の利用料金を算定する。データ記録部１１２ａは、Ｘの課金部１０３ａが算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で情報提供者Ｘ１に通知され、契約者Ａ４は、その料金を支払うことになる。これにより、契約者Ａ４が情報をリアルタイムに利用する場合、利用度合に応じた課金ができる。
【０１２５】
また、乱数発生部１１３ａが乱数を発生し、共通暗号化部１１１ａは、Ｘの復号部１０１ａが復号して得られた情報を、その乱数で再暗号化し、さらに、その乱数を、データ記録

部１１２ａが記憶しているユーザ端末２０ａ毎の秘密鍵で暗号化する。再暗号化された情報および暗号化された乱数がユーザ端末２０ａに伝達されると、共通復号部２０１ａは、伝達された、暗号化された乱数を自己の秘密鍵で復号し、さらに、復号して得た乱数で、伝達された、再暗号化された情報を復号する。これにより、情報サーバ１０ａからユーザ端末２０ａに、安全に情報を伝達できる。

【０１２６】

なお、共通暗号化部１１１ａは、Ｘの復号部１０１ａが復号して得られた情報を、データ記録部１１２ａが記憶しているユーザ端末２０ａ毎の秘密鍵で再暗号化し、共通復号部２０１ａは、伝達された、再暗号化された情報を、自己の秘密鍵で復号するようにしてもよい。ただし、この場合、情報は、毎回、同一の鍵で暗号化されるため、乱数で暗号化する場合に比べると、伝達時の安全性は低くなる。

【０１２７】

（２）記録して利用する場合

図３は、情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して記録し、記録した情報を利用する場合の、図１のシステムの動作を示すフローチャートである。

以下には、図３を用いて、図１の契約者Ａ４が情報提供者Ｘ１から提供される情報を受信して記録し、記録した情報を、契約者Ａ４のユーザが利用する場合について説明する。

ユーザが、情報提供者Ｘ１が提供している、ある情報を記録したい意を、ユーザ端末２０ａに入力すると、ユーザ端末２０ａは、その意を情報サーバ１０ａに通知する。

【０１２８】

通知を受けると、情報サーバ１０ａの情報記録部１１０ａは、Ｘの受信部１０１ａが受信した情報に付加されている記録許可フラグが１であるか否か、すなわち、その情報が記録を許可されたものであるか否かを判定する（ステップＳ２０１）。

付加された記録許可フラグが１である場合、すなわち、記録を許可された情報である場合、情報記録部１１０ａは、その情報を記録する（ステップＳ２０２）。

付加された記録許可フラグが１でない場合、すなわち、記録を許可されない情報である場合には、情報記録部１１０ａは、その情報を記録せず、ユーザ端末２０ａが、エラーを表示する（ステップＳ２０３）。

【０１２９】

ユーザが、上記のようにして情報記録部１１０ａに記録された、ある情報を利用したい意を、ユーザ端末２０ａに入力すると（ステップＳ２０４）、情報サーバ１０ａは、付加された情報識別子を参照して、情報記録部１１０ａに記録された情報のうち、ユーザが求める情報を見出す。そして、情報サーバ１０ａは、その情報が情報提供者Ｘ１から提供されたものであることを認識し、その情報をＸの復号部１０２ａに入力する。Ｘの復号部１０２ａは、入力された情報を復号する（ステップＳ２０５）。

【０１３０】

次に、Ｘの課金部１０３ａは、その情報に付加された課金基準データに基づいて、その情報の利用料金を算定する（ステップＳ２０６）。ただし、利用料金は、情報を記録して利用する場合の基準に基づいて算定される。そして、データ記録部１１２ａは、Ｘの課金部１０３ａが算定して得られた利用料金を記録する（ステップＳ２０７）。

以降、上記リアルタイムに利用する場合と同様にして、情報サーバ１０ａがその情報を再暗号化してユーザ端末２０ａに送信し、ユーザ端末２０ａは、情報サーバ１０ａから送信された、再暗号化された情報を受信して復号する（ステップＳ２０８～ステップＳ２１３）。こうして、ユーザは、情報記録部１１０ａに記録された情報を利用することができる（ステップＳ２１４）。

【０１３１】

このように、情報提供者Ｘ１は、提供しようとする情報に、さらに、記録許可フラグを付加して提供する。情報記録部１１０ａは、Ｘの受信部１０１ａが受信した情報に付加されている記録許可フラグが、記録を許可することを示す１である場合に、その情報を記録することができる。Ｘの課金部１０３ａは、情報記録部１１０ａが記録した情報が、ユーザ

端末２０ａに送信される毎に、その情報に付加された課金基準データに基づいて、その情報の利用料金を算定する。これにより、契約者Ａ４が情報を記録するのを制限することができ、かつ、契約者Ａ４が情報を記録して繰り返し利用する場合、利用度合に応じた課金ができる。

【０１３２】

また、情報記録部１１０ａは、Ｘの受信部１０１ａが受信した情報を、暗号化されたままで記録し、記録された情報がユーザ端末２０ａに伝達される際に、Ｘの復号部１０２ａが、その情報を復号する。これにより、契約者Ａ４が記録した情報が不正に利用されるのを防ぐことができる。

【０１３３】

（３）オフライン端末５０ａで利用する場合

図４は、情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して、オフライン端末５０ａで利用する場合の、図１のシステムの動作を示すフローチャートである。

以下には、図４を用いて、図１の契約者Ａ４が情報提供者Ｘ１から提供される情報を受信し、契約者Ａ４のユーザが、その情報をオフライン端末５０ａで利用する場合について説明する。なお、情報提供者Ｘ１から提供された情報は、図３のステップＳ２０１～ステップＳ２０３と同様にして、情報記録部１１０ａに記録されているものとする。

【０１３４】

ユーザが、ユーザ端末２０ａに、情報記録部１１０ａに記録された、ある情報を、オフライン端末５０ａで利用したい意を入力すると、ユーザ端末２０ａは、その意を情報サーバ１０ａに通知する。

通知を受けると、情報サーバ１０ａは、付加された情報識別子を参照して、情報記録部１１０ａに記録された情報のうち、ユーザが求める情報を見出す。そして、情報サーバ１０ａは、その情報が情報提供者Ｘ１から提供されたものであることを認識し、その情報をＸの復号部１０２ａに入力する。Ｘの復号部１０２ａは、入力された情報を復号する（ステップＳ３０１）。

【０１３５】

次に、Ｘの課金部１０３ａは、実行権データを作成する。実行権データには、利用可能回数、記録モードおよび課金モードが含まれ、この場合、利用可能回数は、ユーザが申告した、その情報を利用する回数であり、記録モードは、オフライン端末５０ａで利用されるべき情報であることを示す１、課金モードは、契約者Ａ４に対して課金済みであることを示す１である。同時に、Ｘの課金部１０３ａは、Ｘの復号部１０２ａが復号して得られた情報に付加されている課金基準データに基づいて、作成した実行権に応じた利用料金、すなわち、その情報を、オフライン端末５０ａで、利用可能回数に等しい回数だけ利用する場合の利用料金を算定する（ステップＳ３０２）。そして、データ記録部１１２ａは、Ｘの課金部１０３ａが算定して得られた利用料金を記録する（ステップＳ３０３）。

【０１３６】

Ｘの復号部１０２ａが復号して得られた情報は、上記リアルタイムに利用する場合と同様にして再暗号化されたうえで、移動ディスク３０ａに記録される（ステップＳ３０４、ステップＳ３０５）。乱数発生部１１３ａが発生した乱数ｒは、Ｘの課金部１０３ａが作成した実行権データとともに、ＩＣカード４０ａに記録される（ステップＳ３０６）。

【０１３７】

次に、ユーザは、暗号化された情報が記録された移動ディスク３０ａと、乱数ｒおよび実行権データが記録されたＩＣカード４０ａとを、オフライン端末５０ａに接続する（ステップＳ３０７）。オフライン端末５０ａの共通復号部５０１ａは、最初、ＩＣカード４０ａに記録された実行権データに含まれている記録モードが１であるか否かを判定する（ステップＳ３０８）。

記録モードが１である場合、共通復号部５０１ａは、実行権データに含まれる利用可能回数が１以上であるか否かを、さらに判定する（ステップＳ３０９）。

【０１３８】

利用可能回数が１以上であれば、共通復号部５０１ａは、ＩＣカード４０ａに記録された乱数ｒで、移動ディスク３０ａに記録された情報を、上記リアルタイムに利用する場合と同様にして復号する（ステップＳ３１０）。そして、オフライン端末５０ａは、ＩＣカード４０ａに記録されている利用可能回数を更新し（ステップＳ３１１）、次いで、共通復号部５０１ａが復号して得られた情報を表示する。こうして、ユーザは、オフライン端末５０ａで、情報を利用することができる（ステップＳ３１２）。

【０１３９】

ステップＳ３０８で、記録モードが１でない場合、もしくは、ステップＳ３０９で、利用可能回数が０である場合には、共通復号部５０１ａは、暗号化された情報を乱数ｒで復号する動作を行わず、オフライン端末５０ａが、ユーザに対してエラーを通知する（ステップＳ３１３）。

【０１４０】

このように、Ｘの課金部１０３ａは、情報の利用度合およびその情報を利用可能な端末を制限するための実行権データを作成し、同時に、その情報に付加された課金基準データをに基づいて、作成した実行権データに応じた利用料金を算定する。その情報およびＸの課金部１０３ａが作成した実行権データがオフライン端末５０ａに伝達されると、オフライン端末５０ａは、伝達された実行権データが所定の条件を満たす場合に、伝達された情報をユーザに表示する。これにより、契約者Ａ４のユーザがオフライン端末５０ａで情報を利用する場合、利用度合に応じた課金ができる。

【０１４１】

また、乱数発生部１１３ａが乱数を発生し、共通暗号化部１１１ａは、Ｘの復号部１０２ａが復号して得られた情報を、その乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データがオフライン端末５０ａに伝達されると、共通復号部５０１ａは、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、オフライン端末５０ａにおいて、実行権データが所定の条件を満たす場合にのみ、情報が表示されるようにすることができる。

【０１４２】

なお、共通暗号化部１１１ａは、Ｘの復号部１０１ａが復号して得られた情報を、データ記録部１１２ａが記憶しているユーザ端末２０ａ毎の秘密鍵で再暗号化し、共通復号部２０１ａは、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、自己の秘密鍵で復号するようにしても、実行権データが所定の条件を満たす場合にのみ、情報が表示されるようにすることができる。

【０１４３】

また、共通暗号化部１１１ａが再暗号化して得られた情報は、移動ディスク３０ａのような、書き込み／読み出し可能な携帯型記録媒体を介して、乱数発生部１１３ａが発生した乱数およびＸの課金部１０３ａが作成した実行権データは、ＩＣカード４０ａのような、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれオフライン端末５０ａに伝達することにより、情報サーバ１０ａからオフライン端末５０ａに、安全に情報を伝達できる。

【０１４４】

（４）契約者Ａ４が受信して、契約者Ｂ５が利用する場合

図５は、情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して契約者Ｂ５に再提供し、契約者Ｂ５が再提供された情報を利用する場合の、図１のシステムの動作を示すフローチャートである。

以下には、図５を用いて、情報提供者Ｘ１から提供される情報を、契約者Ａ４が受信して契約者Ｂ５に再提供し、契約者Ｂ５のユーザが再提供された情報を利用する場合について説明する。なお、情報提供者Ｘ１から提供された情報は、図３のステップＳ２０１～ステップＳ２０３と同様にして、情報記録部１１０ａに記録されているものとする。

【０１４５】

契約者Ａ４のユーザが、情報記録部１１０ａに記録された、ある情報を、契約者Ｂ５に再提供したい意、および、再提供された情報を契約者Ｂが利用した場合、契約者Ａに課金されるようにするのか、契約者Ｂに課金されるようにするのかを、ユーザ端末２０ａに入力すると、ユーザ端末２０ａは、それらの意を情報サーバ１０ａに通知する。
ユーザ端末２０ａからの通知を受けると、情報サーバ１０ａは、付加された情報識別子を参照して、情報記録部１１０ａに記録された情報のうち、ユーザが求める情報を見出す。そして、情報サーバ１０ａは、その情報が情報提供者Ｘ１から提供されたものであることを認識し、その情報をＸの復号部１０２ａに入力する。Ｘの復号部１０２ａは、入力された情報を復号する（ステップＳ４０１）。次に、Ｘの課金部１０３ａは、ユーザ端末２０ａからの通知に基づいて、契約者Ａ４に課金するか否かを判定する（ステップＳ４０２）。

【０１４６】
契約者Ａ４に課金する場合、Ｘの課金部１０３ａは、上記オフライン端末５０ａで利用する場合と同様にして、実行権データを作成するとともに、作成した実行権データに応じた利用料金を算定する（ステップＳ４０３）。そして、データ記録部１１２ａは、Ｘの課金部１０３ａが算定して得られた利用料金を記録する（ステップＳ４０４）。ただし、この場合、作成された実行権データに含まれる利用可能回数は、契約者Ａ４のユーザが申告した、その情報を契約者Ｂ５に利用させる回数であり、記録モードは、契約者Ｂ５のユーザ端末２０ｂで利用されることを示す２、課金モードは、契約者Ａ４に課金済みであることを示す１である。また、算定された利用料金は、契約者Ｂ５のユーザが、ユーザ端末２０ｂで、その情報を利用可能回数に等しい回数だけ利用した場合の料金である。

【０１４７】
契約者Ｂ５に課金する場合には、Ｘの課金部１０３ａは、実行権データを作成する（ステップＳ４０５）。ただし、この場合、作成された実行権データに含まれる利用可能回数は、予め定められた十分大きな値であり、記録モードは、契約者Ｂ５のユーザ端末２０ｂで利用されることを示す２、課金モードは、未課金であることを示す２である。

【０１４８】
次に、共通暗号化部１１１ａは、Ｘの復号部１０２ａが復号して得られた情報を、上記リアルタイムに利用する場合と同様にして、乱数発生部１１３ａが発生した乱数ｒで再暗号化する（ステップＳ４０６）。そして、情報サーバ１０ａは、共通暗号化部１１１ａが再暗号化して得られた情報を移動ディスク３０ａに記録し（ステップＳ４０７）、乱数発生部１１３ａが発生した乱数ｒおよびＸの課金部１０３ａが作成した実行権データをＩＣカード４０ａに記録する（ステップＳ４０８）。

【０１４９】
契約者Ｂ５のユーザは、再暗号化された情報が記録された移動ディスク３０ａと乱数ｒおよび実行権データが記録されたＩＣカード４０ａとを取得すると、取得した移動ディスク３０ａおよびＩＣカード４０ａを、ユーザ端末２０ｂに接続し（ステップＳ４０９）、次いで、移動ディスク３０ａに記録された情報を利用する意を、ユーザ端末２０ｂに入力する。

【０１５０】
ユーザ端末２０ｂの共通復号部２０１ｂは、最初、ＩＣカード４０ａに記録された実行権データに含まれる課金モードが１であるか否か、すなわち契約者Ａ４に課金済みであるか否かを判定する（ステップＳ４１０）。
課金モードが１である場合、共通復号部２０１ｂは、実行権データに含まれる記録モードが２であるか否か、すなわち、その情報が契約者Ｂ５のユーザ端末２０ｂで利用されるべきものであるか否かを、さらに判定する（ステップＳ４１１）。
記録モードが２である場合、共通復号部２０１ｂは、実行権データに含まれる利用可能回数が１以上であるか否かを、さらに判定する（ステップＳ４１２）。

【０１５１】
利用可能回数が１以上である場合、共通復号部２０１ｂは、移動ディスク３０ａに記録さ

れた、再暗号化された情報を、上記リアルタイムに利用する場合と同様にして、ＩＣカード４０ａに記録された乱数ｒで復号する（ステップＳ４１３）。次に、ユーザ端末２０ｂは、実行権データに含まれている利用可能回数を更新し（ステップＳ４１４）、共通復号部２０１ｂが復号して得られた情報を表示する。こうして、契約者Ｂ５のユーザは、契約者Ａ４から再提供された情報を利用することができる（ステップＳ４１５）。

【０１５２】

ステップＳ４１１で、記録モードが２でない場合、もしくは、ステップＳ４１２で、利用可能回数が０である場合には、共通復号部２０１ｂは、再暗号化された情報を乱数ｒで復号する動作を行わず、ユーザ端末２０ｂがユーザに対して、その情報を利用できない意を通知する（ステップＳ４１６）。

【０１５３】

ステップＳ４１０で、課金モードが１でない場合、すなわち、未課金である場合には、ユーザ端末２０ｂは、情報サーバ１０ｂに、移動ディスク３０ａに記録された、再暗号化された情報に付加された課金基準データを通知する。情報サーバ１０ｂのＸの課金部１０３ｂは、通知された課金基準データに基づいて、その情報の利用料金を算定し（ステップＳ４１７）、データ記録部１１２ｂは、Ｘの課金部１０３ｂが算定して得られた利用料金を記録する（ステップＳ４１８）。その後、ステップＳ４１１の処理に進む。

【０１５４】

このように、契約者Ａ４に課金する場合、情報サーバ１０ａのＸの課金部１０３ａは、情報の利用度合およびその情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データに応じた利用料金を、その情報に付加された課金基準データに基づいて算定する。その情報および作成された実行権データが契約者Ｂ５に伝達されると、ユーザ端末２０ｂは、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を表示する。これにより、契約者Ａ４が受信した情報を契約者Ｂ５が利用する場合、利用度合に応じて、契約者Ａ４に課金することができる。

【０１５５】

なお、契約者Ａ４が受信した情報を契約者Ｂ５が利用して、契約者Ａ４に課金するという提供形態は、情報をプレゼントするという、情報提供の新たな形態である。

【０１５６】

契約者Ｂ５に課金する場合には、情報サーバ１０ａのＸの課金部１０３ａは、情報を利用できる端末を制限するための実行権データを作成する。その情報および作成された実行権データが契約者Ｂ５に伝達されると、情報サーバ１０ｂのＸの課金部１０３ｂは、伝達された情報に付加された課金基準データに基づいて、その情報の利用料金を算定する。一方、ユーザ端末２０ｂは、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を表示する。これにより、契約者Ａ４が受信した情報を契約者Ｂ５が利用する場合、利用度合に応じて、契約者Ｂ５に課金することができる。

【０１５７】

以上は、契約者Ａ４から契約者Ｂ５に、移動ディスク３０ａおよびＩＣカード４０ａを介して、それぞれ、情報、データ類を伝達する場合について説明しているが、以下には、ＣＡＴＶ網を介して、情報およびデータ類を伝達する場合について、図１および５を用いて説明する。

本システムの動作が、図５に示すものと異なるのは、以下に示す点である。すなわち、ステップＳ４０６～Ｓ４０８において、契約者Ａ４および契約者Ｂ５はそれぞれ、共有鍵ＫＡＢを保有しており、共通暗号化部１１１ａは、Ｘの復号部１０２ａが復号して得られた情報を、乱数発生部１１３ａが発生した乱数ｒで再暗号化し、さらに、この乱数ｒおよびＸの課金部１０３ａが作成した実行権データを、共有鍵ＫＡＢで暗号化する。そして、情報サーバ１０ａは、共通暗号化部１１１ａが再暗号化して得られた情報ならびに暗号化して得られた乱数および実行権データを、ＣＡＴＶ網を通じて、契約者Ｂ５に送信する。

【０１５８】

また、ステップＳ４０９において、ユーザ端末２０ｂが、ＣＡＴＶ網を通じて送信された

、再暗号化された情報ならびに暗号化された乱数および実行権データを受信すると、共通復号部２０１ｂは、暗号化された乱数および実行権データを、共有鍵ＫＡＢで復号する。

【０１５９】

このように、ＣＡＴＶ網のような、伝送速度が比較的大きな伝送路を通じて、情報、乱数および実行権データを伝送する場合には、情報を乱数で再暗号化し、さらに、乱数および実行権データを共有鍵ＫＡＢで暗号化することにより、契約者Ａ４から契約者Ｂ５に、安全に情報を伝達できる。

【０１６０】

なお、共有鍵ＫＡＢで乱数および実行権データを暗号化する代わりに、公開暗号方式で暗号化することもできる。また、ＣＡＴＶ網に代えて、Ｂ－ＩＳＤＮを通じて、契約者Ａから契約者Ｂに、再暗号化された情報ならびに暗号化された乱数および実行権データを伝送してもよい。

【０１６１】

次に、契約者Ａ４から契約者Ｂ５に、移動ディスク３０ａを介して情報を、通信回線を介してデータ類を、それぞれ伝達する場合について、図１および５を用いて説明する。

本システムの動作が、図５に示すものと異なるのは、以下に示す点である。すなわち、ステップＳ４０６～Ｓ４０８において、契約者Ａ４および契約者Ｂ５はそれぞれ、共有鍵ＫＡＢを保有しており、共通暗号化部１１１ａは、Ｘの復号部１０２ａが復号して得られた情報を、乱数発生部１１３ａが発生した乱数ｒで再暗号化し、さらに、この乱数ｒおよびＸの課金部１０３ａが作成した実行権データを、共有鍵ＫＡＢで暗号化する。そして、情報サーバ１０ａは、共通暗号化部１１１ａが再暗号化して得られた情報を、移動ディスク３０ａに記録し、共通暗号化部１１１ａが暗号化して得られた乱数および実行権データを、通信回線を通じて、契約者Ｂ５に送信する。

【０１６２】

また、ステップＳ４０９において、契約者Ｂ５のユーザは、再暗号化された情報が記録された移動ディスク３０ａを取得すると、取得した移動ディスク３０ａを、ユーザ端末２０ｂに接続する。また、ユーザ端末２０ｂが、通信回線を通じて送信された、暗号化された乱数および実行権データを受信すると、共通復号部２０１ｂは、暗号化された乱数および実行権データを、共有鍵ＫＡＢで復号する。

【０１６３】

このように、乱数および実行権データを、通信回線のような、伝送速度が比較的小さい伝送路を通じて伝送し、情報を、移動ディスク３０ａに記録して移動させる場合には、情報を乱数で再暗号化し、さらに、乱数および実行権データを共有鍵ＫＡＢで暗号化することにより、契約者Ａ４から契約者Ｂ５に、安全に情報を伝達できる。なお、共有鍵ＫＡＢで乱数および実行権データを暗号化する代わりに、公開暗号方式で暗号化することもできる。

【０１６４】

なお、本実施形態では、実行権データに利用可能回数が含まれるとしたが、利用可能期限が含まれるとしてもよい。

【０１６５】

また、本実施形態では、ユーザがオフライン端末５０ａで情報を利用する場合、Ｘの課金部１０３ａは、実行権データを作成すると同時に、作成した実行権に応じた利用料金を算定しているが、オフライン端末５０ａでの利用度合をＩＣカード４０ａに記録しておき、利用後に、ユーザがＩＣカード４０ａを情報サーバ１０ａに接続して、その際、Ｘの課金部１０３ａが利用料金を算定してもよい。

【０１６６】

また、本実施形態では、契約者単位で課金しているが、利用料金を端末毎に記録することにより、ユーザ単位で課金することもできる。

【０１６７】

また、ユーザにパスワードを発行し、ユーザが端末を利用する際に、認証を行うようにす

ることで、不正使用に対する安全性を、より高めることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る情報提供システムの構成を示すブロック図である。

【図２】情報提供者Ｘ１が提供する情報を、契約者Ａが受信して、リアルタイムに利用する場合の、図１のシステムの動作を示すフローチャートである。

【図３】情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して記録し、記録した情報を利用する場合の、図１のシステムの動作を示すフローチャートである。

【図４】情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して、オフライン端末５０ａで利用する場合の、図１のシステムの動作を示すフローチャートである。

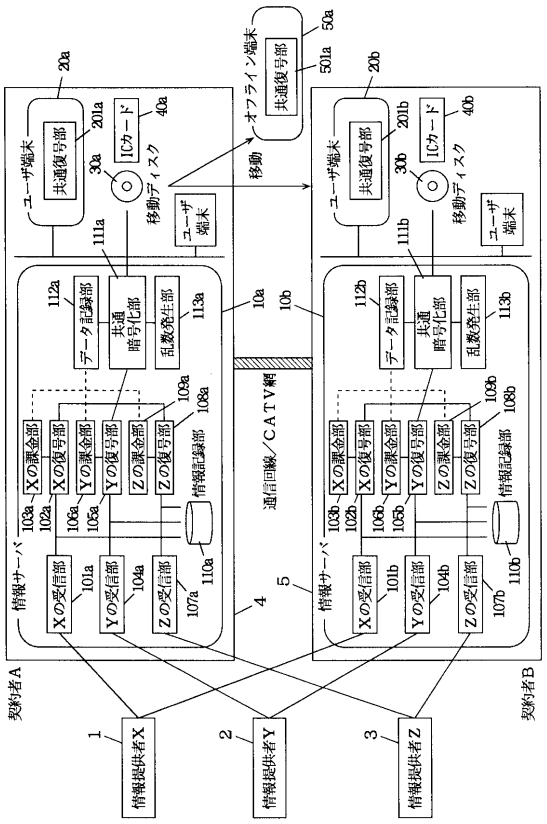
【図５】情報提供者Ｘ１が提供する情報を、契約者Ａ４が受信して契約者Ｂ５に再提供し、契約者Ｂ５が再提供された情報を利用する場合の、図１のシステムの動作を示すフローチャートである。

【図６】従来の映像情報伝送装置の構成を示すブロック図である。

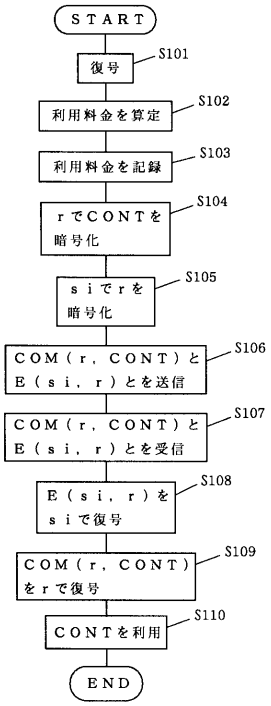
【符号の説明】

１　情報提供者Ｘ
２　情報提供者Ｙ
３　情報提供者Ｚ
４　契約者Ａ
５　契約者Ｂ
１０ａ、１０ｂ　情報サーバ
２０ａ、２０ｂ　ユーザ端末
３０ａ、３０ｂ　移動ディスク
４０ａ、４０ｂ　ＩＣカード
５０ａ　オフライン端末
１０１ａ、１０１ｂ　Ｘの受信部
１０２ａ、１０２ｂ　Ｘの復号部
１０３ａ、１０３ｂ　Ｘの課金部
１０４ａ、１０４ｂ　Ｙの受信部
１０５ａ、１０５ｂ　Ｙの復号部
１０６ａ、１０６ｂ　Ｙの課金部
１０７ａ、１０７ｂ　Ｚの受信部
１０８ａ、１０８ｂ　Ｚの復号部
１０９ａ、１０９ｂ　Ｚの課金部
１１０ａ、１１０ｂ　情報記録部
１１１ａ、１１１ｂ　共通暗号化部
１１２ａ、１１２ｂ　データ記録部
１１３ａ、１１３ｂ　乱数発生部
２０１ａ、２０１ｂ、５０１ａ　共通復号部

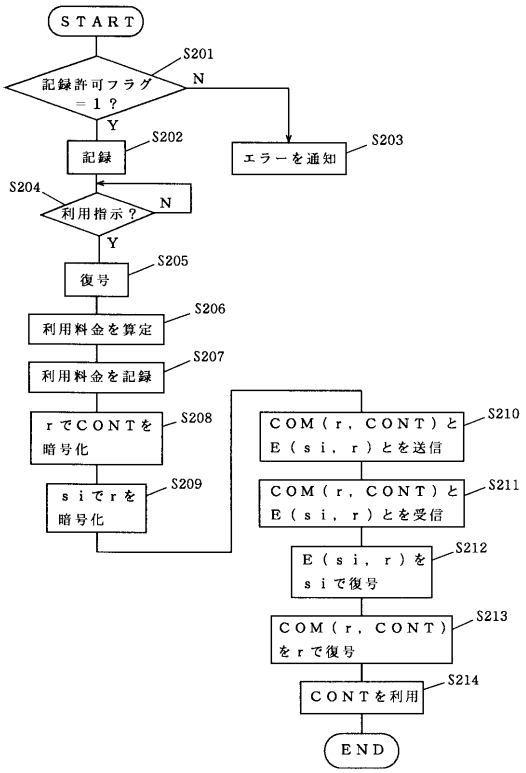
【図１】


オフライン端末
共通復号部
ユーザ端末
共通復号部
ICカード
移動ディスク
ユーザ端末
移動
データ記録部
共通暗号化部
乱数発生部
通信回線／CATV網
Xの課金部
Xの復号部
Yの課金部
Yの復号部
Zの課金部
Zの復号部
情報記録部
情報サーバ
Xの受信部
Yの受信部
Zの受信部
契約者A
契約者B
情報提供者X
情報提供者Y
情報提供者Z

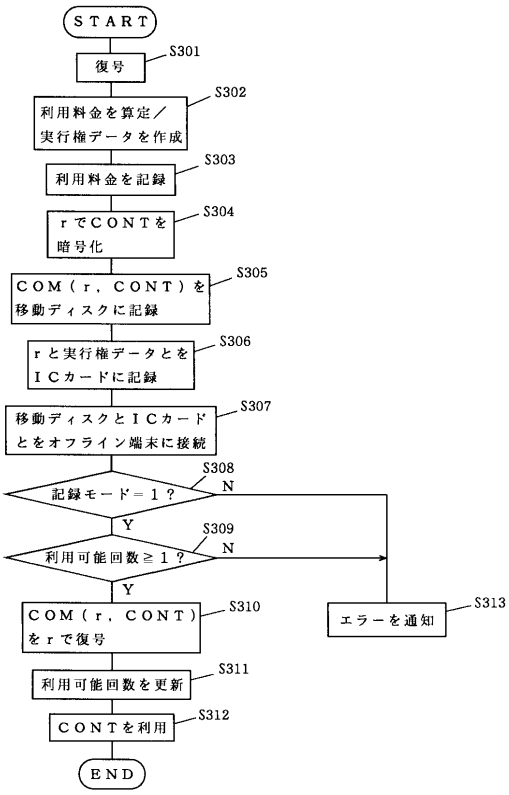
【図２】


START
復号
S101
利用料金を算定
S102
利用料金を記録
S103
ｒでＣＯＮＴを暗号化
S104
ｓｉでｒを暗号化
S105
ＣＯＭ（ｒ，ＣＯＮＴ）とＥ（ｓｉ，ｒ）とを送信
S106
ＣＯＭ（ｒ，ＣＯＮＴ）とＥ（ｓｉ，ｒ）とを受信
S107
Ｅ（ｓｉ，ｒ）をｓｉで復号
S108
ＣＯＭ（ｒ，ＣＯＮＴ）をｒで復号
S109
ＣＯＮＴを利用
S110
END

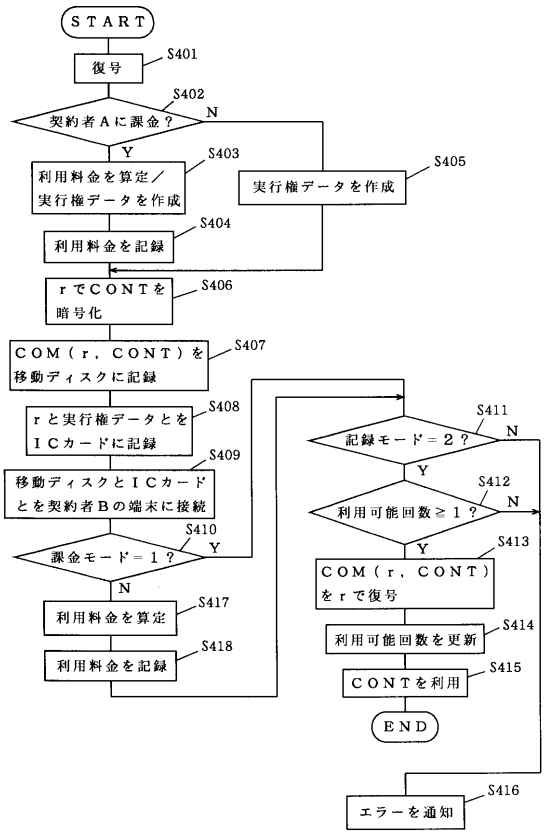
【図３】


START
記録許可フラグ＝１？
S201
N
Y
エラーを通知
S203
記録
S202
利用指示？
S204
N
Y
復号
S205
利用料金を算定
S206
利用料金を記録
S207
ｒでＣＯＮＴを暗号化
S208
ｓｉでｒを暗号化
S209
ＣＯＭ（ｒ，ＣＯＮＴ）とＥ（ｓｉ，ｒ）とを送信
S210
ＣＯＭ（ｒ，ＣＯＮＴ）とＥ（ｓｉ，ｒ）とを受信
S211
Ｅ（ｓｉ，ｒ）をｓｉで復号
S212
ＣＯＭ（ｒ，ＣＯＮＴ）をｒで復号
S213
ＣＯＮＴを利用
S214
END

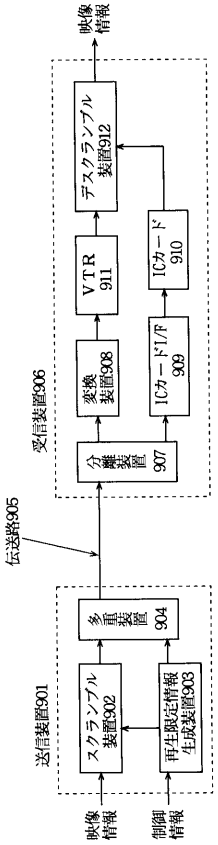
【図４】


START
復号
S301
利用料金を算定／実行権データを作成
S302
利用料金を記録
S303
ｒでＣＯＮＴを暗号化
S304
ＣＯＭ（ｒ，ＣＯＮＴ）を移動ディスクに記録
S305
ｒと実行権データとをＩＣカードに記録
S306
移動ディスクとＩＣカードとをオフライン端末に接続
S307
記録モード＝１？
S308
N
Y
利用可能回数≧１？
S309
N
Y
ＣＯＭ（ｒ，ＣＯＮＴ）をｒで復号
S310
エラーを通知
S313
利用可能回数を更新
S311
ＣＯＮＴを利用
S312
END

【図５】


ＳＴＡＲＴ
復号
S401
契約者Ａに課金？
S402
N
Y
利用料金を算定／実行権データを作成
S403
実行権データを作成
S405
利用料金を記録
S404
ｒでＣＯＮＴを暗号化
S406
ＣＯＭ（ｒ，ＣＯＮＴ）を移動ディスクに記録
S407
ｒと実行権データとをＩＣカードに記録
S408
移動ディスクとＩＣカードとを契約者Ｂの端末に接続
S409
課金モード＝１？
S410
Y
N
利用料金を算定
S417
利用料金を記録
S418
記録モード＝２？
S411
N
Y
利用可能回数≧１？
S412
N
Y
ＣＯＭ（ｒ，ＣＯＮＴ）をｒで復号
S413
利用可能回数を更新
S414
ＣＯＮＴを利用
S415
ＥＮＤ
エラーを通知
S416

【図６】


映像情報
デスクランブル装置912
VTR 911
ICカード 910
変換装置908
ICカードI/F 909
分離装置 907
受信装置906
伝送路905
多重装置 904
スクランブル装置902
再生限定情報生成装置903
送信装置901
映像情報
制御情報

フロントページの続き

審査官　川崎　優

(56)参考文献　国際公開第９４／０１４２８０（WO，Ａ１）
特開平０８－１２５６５１（ＪＰ，Ａ）
特開平０５－２８４４９６（ＪＰ，Ａ）
特開平０８－０７７２６３（ＪＰ，Ａ）
ビデオオンデマンド　ＶＯＤのサービスと要求条件，画像情報工学と放送技術，社団法人テレビジョン学会，１９９５年　5月２０日，第４９巻、第５号，P.599-604

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 7/16-173