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

特許第4314336号
(P4314336)

(45)発行日　平成21年8月12日(2009.8.12)　(24)登録日　平成21年5月29日(2009.5.29)

(51)Int.Cl.		F I		
G06F 9/46	(2006.01)	G06F	9/46	420B
G06Q 50/00	(2006.01)	G06F	17/60	132
G06Q 30/00	(2006.01)	G06F	17/60	314
G06Q 10/00	(2006.01)	G06F	17/60	512

請求項の数 6　(全 48 頁)

(21)出願番号　特願2007-239904 (P2007-239904)
(22)出願日　平成19年9月14日 (2007.9.14)
(62)分割の表示　特願平10-102933の分割
　原出願日　平成10年4月14日 (1998.4.14)
(65)公開番号　特開2008-27462 (P2008-27462A)
(43)公開日　平成20年2月7日 (2008.2.7)
　審査請求日　平成19年9月14日 (2007.9.14)

(73)特許権者　502178126
石井　美恵子
岡山県倉敷市羽島２２１番地の４
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100109162
弁理士　酒井　將行
(74)代理人　100111246
弁理士　荒川　伸夫

最終頁に続く

(54)【発明の名称】コンテンツ提供システム

(57)【特許請求の範囲】
【請求項１】
自律的なソフトウェアモジュールとしてのエージェントがユーザにマッチするコンテンツであるか否かを判断し、マッチするコンテンツを該ユーザに提供するコンテンツ提供システムであって、
ユーザと該ユーザの要求に応えてコンテンツを提供する複数のコンテンツ提供業者とからなる当事者の双方に対し中立性を有する第三者エージェントであって、前記複数のコンテンツ提供業者が提供するコンテンツがユーザにマッチするコンテンツであるか否かを判断するための第三者エージェントを格納している第三者機関コンピュータを備え、
前記第三者機関コンピュータは、
前記ユーザにマッチするコンテンツか否かを前記第三者エージェントが判断するのに必要となる当該ユーザのプロフィール情報であって前記第三者機関コンピュータへ送信されてきたプロフィール情報を、受付けるプロフィール情報受付手段と、
前記コンテンツ提供業者によって提供されるコンテンツであって前記第三者機関コンピュータへ送信されてきたコンテンツを、受付けるコンテンツ受付手段とを含み、
前記第三者エージェントは、前記プロフィール情報受付手段により受付けられたユーザのプロフィール情報に基づいて、前記コンテンツ受付手段により受付けられたコンテンツがユーザにマッチするコンテンツであるか否かの判断を前記第三者機関コンピュータ内で行ない、該判断結果を通知する通知機能を有することを特徴とする、コンテンツ提供システム。

【請求項２】
前記第三者機関コンピュータは、前記ユーザ側のために働くユーザ側エージェントが、ネットワーク上を移動して動作するときのワーキングエリアとして機能し、秘密の漏洩が防止できる秘密保持用ワーキングエリアを含み、
前記ユーザ側エージェントは、秘密にしたいプロフィール情報を秘密性が保持できる態様で知識として保有しており、該ユーザ側エージェントがホームとなるコンピュータから出て移動して仕事を行なう際に、前記秘密のプロフィール情報を使用する必要が生じた場合に、前記ユーザ側エージェントは、前記秘密保持用ワーキングエリアに移動し、該秘密保持用ワーキングエリア内で前記秘密のプロフィール情報の秘密性を解除して仕事の実行を可能にすることを特徴とする、請求項１に記載のコンテンツ提供システム。
【請求項３】
前記ユーザ側エージェントは、前記秘密のプロフィール情報を暗号化して保有しており、前記秘密保持用ワーキングエリアに移動した後前記暗号化された秘密のプロフィール情報の復号を可能にすることを特徴とする、請求項２に記載のコンテンツ提供システム。
【請求項４】
前記ユーザ側エージェントは、前記秘密のプロフィール情報の復号に用いられる復号鍵を保有しておらず、前記秘密保持用ワーキングエリアに移動した後前記秘密保持用ワーキングエリア内に取り寄せた前記復号鍵を用いた前記秘密のプロフィール情報の復号を可能にすることを特徴とする、請求項３に記載のコンテンツ提供システム。
【請求項５】
前記秘密のプロフィール情報は、前記ユーザの本人認証のための秘密鍵を含んでいることを特徴とする、請求項２～請求項４のいずれかに記載のコンテンツ提供システム。
【請求項６】
前記ユーザのプロフィール情報は、該プロフィール情報に基づいての前記第三者エージェントによる判断の結果に対するユーザの反応に基づいて更新されることを特徴とする、請求項１～請求項５のいずれかに記載のコンテンツ提供システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、たとえば、ユーザの仕事を代行するエージェントと呼ばれる自律的なソフトウェアモジュールが動作するエージェントシステムに関する。
【背景技術】
【０００２】
この種のエージェントシステムにおいて、従来から知られているものに、たとえば、特許文献１，特許文献２，特許文献３，特許文献４，特許文献５等に示すようなエージェント同士が協調して動作するマルチエージェントシステムがあった。
【０００３】
これらの従来のマルチエージェントシステムでは、それぞれに独立の知識を持ったエージェント同士が協調して仕事を行ない、ある問題を効率的に解決できるように構成されていた。
【特許文献１】特開平９－１７９９１０号公報
【特許文献２】特開平５－２３３５７４号公報
【特許文献３】特開平５－２３３５９６号公報
【特許文献４】特開平５－３４６９１０号公報
【特許文献５】特開平５－１５１１７８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ところが、たとえば、ユーザのために働くユーザ側エージェントとそのユーザの要求に応えて所定のサービスを提供するサービス業者側エージェントとが協調してある仕事をす

る場合に、ユーザ側エージェントと業者側エージェントとからなる当事者エージェントのみでは解決できない問題が生ずる場合がある。

【０００５】

たとえば、コンテンツ提供業者等のサービス業者が有料コンテンツを提供する業者であって、ユーザ側エージェントが業者側エージェントと協調して有料コンテンツを検索して希望するコンテンツが見つかればそのコンテンツを購入する仕事を想定してみる。ユーザ側エージェントがネットワーク上を移動してサービス業者側のプレースにまで行き、そのプレース上で業者側エージェントと打合せ（meeting）を行ない、有料コンテンツの検索の許可をもらう。そしてユーザ側エージェントが有料コンテンツのデータベースにアクセスして複数の有料コンテンツを検索してその中身を吟味し、希望するコンテンツがあるか否かを判断する。そしてもし希望するコンテンツがあれば、ユーザ側エージェントは所定の金額の料金を支払うための購入手続を行なった後希望するコンテンツをユーザ側に持ち帰る。

【０００６】

ところが、ユーザ側エージェントは、ユーザのために開発されユーザの利益となるように動作して仕事を行なうものであり、ユーザの命令に服従する性質のものである。その結果、ユーザがユーザ側エージェントに対し不正を働くように指令した場合やユーザ側エージェントを不正改造して不正を働くエージェントにするおそれが考えられる。そのようなユーザ側エージェントが前述した有料コンテンツを検索した場合に、希望するコンテンツが見つかったとしても業者側エージェントに対しては何ら希望するコンテンツがなかった旨の報告を行なって所定の料金を支払うための購入手続を何ら行なうことなく希望する有料コンテンツをこっそりユーザ側に持ち帰るという不正が発生するおそれがある。

【０００７】

そこで、このような不都合を防止するために、ユーザ側エージェントが直接コンテンツのデータベースにはアクセスできないようにし、ユーザ側エージェントに代わって業者側エージェントに有料コンテンツの検索を行なってもらうようにすることが考えられる。具体的には、たとえば、サービス業者側のプレース上でユーザ側エージェントと業者側エージェントとがmeetingして、ユーザの嗜好情報等のプロフィール情報や購入希望価格情報をユーザ側エージェントが業者側エージェントに通知し、それを知識として業者側エージェントがコンテンツのデータベースにアクセスして有料コンテンツを検索吟味し、ユーザが好むと思われるコンテンツを探し出してユーザ側エージェントにその結果を通知するようにすることが考えられる。

【０００８】

ところが、業者側のエージェントは、サービス業者側の利益のみを考慮して開発されて働くものであるために、サービス業者側の命令に服従する性質を有するものであり、その結果、コンテンツの検索結果ユーザが好むと思われるコンテンツがたとえなかったとしてもユーザ好みのコンテンツが多数あるという嘘の報告をユーザ側エージェントに通知する不都合が生ずるおそれがある。

【０００９】

つまり、ユーザ側エージェントや業者側エージェント等からなる当事者エージェントの場合には、互いの当事者の利益のためにのみ働く傾向があるために、自己の立場の方に有利となる利己的動作を行なうおそれがあり、当事者双方にとって中立性を要する特定の仕事が生じた場合にその特定の仕事を中立性を守りながら実行することができにくいという欠点が生ずる。

【００１０】

しかも、ユーザ側エージェントが知識として保有しているユーザのプロフィール情報は、たとえばユーザの種々の好みの情報からなる嗜好情報やユーザの年齢や職業あるいは年収等のような、ユーザが秘密にしたがる秘密情報を含んでいるのであり、サービス業者側のプレース上でユーザ側エージェントがそのような秘密情報を含んでいるプロフィール情報を業者側エージェントに通知した場合には、ユーザのプライバシーが損なわれるおそれ

が生じる。つまり、秘密情報を知得した業者側エージェントがその知得した知識に基づいて仕事を行なってその知得した知識が不要になれば、その段階でユーザ側エージェントが知得した知識を破棄して消去するようにすれば、ユーザのプライバシーも保護されるのであるが、前述したように業者側エージェントは、サービス業者側の利益のために働くエージェントであるために、ユーザのプロフィール情報を知得すればそのようなプロフィール情報を後々までも記憶しておき、顧客管理やマーケティングに有効利用してサービス業者の利益のために活用する可能性が十分ある。なお、ユーザのプライバシーの問題は、秘密情報を知識として保有するユーザ側エージェントがサービス業者側のプレースに移動しただけでも脅かされるおそれがある。

【００１１】

本発明は、かかる実情に鑑み考え出されたものであり、その目的は、自律的なソフトウェアモジュールとしてのエージェントがユーザにマッチするコンテンツであるか否かを判断してマッチするコンテンツを該ユーザに提供する際に、コンテンツ提供業者側による虚偽報告やユーザのプロフィール情報の盗用等の不正を防止できるようにすることである。

【課題を解決するための手段】

【００１２】

請求項１に記載の本発明は、自律的なソフトウェアモジュールとしてのエージェントがユーザにマッチするコンテンツであるか否かを判断し、マッチするコンテンツを該ユーザに提供するコンテンツ提供システムであって、

ユーザと該ユーザの要求に応えてコンテンツを提供する複数のコンテンツ提供業者とからなる当事者の双方に対し中立性を有する第三者エージェントであって、前記複数のコンテンツ提供業者が提供するコンテンツがユーザにマッチするコンテンツであるか否かを判断するための第三者エージェントを格納している第三者機関コンピュータを備え、

前記第三者機関コンピュータは、

前記ユーザにマッチするコンテンツか否かを前記第三者エージェントが判断するのに必要となる当該ユーザのプロフィール情報であって前記第三者機関コンピュータへ送信されてきたプロフィール情報を、受付けるプロフィール情報受付手段と、

前記コンテンツ提供業者によって提供されるコンテンツであって前記第三者機関コンピュータへ送信されてきたコンテンツを、受付けるコンテンツ受付手段とを含み、

前記第三者エージェントは、前記プロフィール情報受付手段により受付けられたユーザのプロフィール情報に基づいて、前記コンテンツ受付手段により受付けられたコンテンツがユーザにマッチするコンテンツであるか否かの判断を前記第三者機関コンピュータ内で行ない、該判断結果を通知する通知機能を有することを特徴とする。

【００１３】

請求項２に記載の本発明は、請求項１に記載の発明の構成に加えて、前記第三者機関コンピュータは、前記ユーザ側のために働くユーザ側エージェントが、ネットワーク上を移動して動作するときのワーキングエリアとして機能し、秘密の漏洩が防止できる秘密保持用ワーキングエリアを含み、

前記ユーザ側エージェントは、秘密にしたいプロフィール情報を秘密性が保持できる態様で知識として保有しており、該ユーザ側エージェントがホームとなるコンピュータから出て移動して仕事を行なう際に、前記秘密のプロフィール情報を使用する必要が生じた場合に、前記ユーザ側エージェントは、前記秘密保持用ワーキングエリアに移動し、該秘密保持用ワーキングエリア内で前記秘密のプロフィール情報の秘密性を解除して仕事の実行を可能にすることを特徴とする。

【００１４】

請求項３に記載の本発明は、請求項２に記載の発明の構成に加えて、前記ユーザ側エージェントは、前記秘密のプロフィール情報を暗号化して保有しており、前記秘密保持用ワーキングエリアに移動した後前記暗号化された秘密のプロフィール情報の復号を可能にすることを特徴とする。

【００１５】

請求項４に記載の本発明は、請求項３に記載の発明の構成に加えて、前記ユーザ側エージェントは、前記秘密のプロフィール情報の復号に用いられる復号鍵を保有しておらず、前記秘密保持用ワーキングエリアに移動した後前記秘密保持用ワーキングエリア内に取り寄せた前記復号鍵を用いた前記秘密のプロフィール情報の復号を可能にすることを特徴とする。

【００１６】

請求項５に記載の本発明は、請求項２～請求項４のいずれかに記載の発明の構成に加えて、前記秘密のプロフィール情報は、前記ユーザの本人認証のための秘密鍵を含んでいることを特徴とする。

【００１７】

請求項６に記載の本発明は、請求項１～請求項５のいずれかに記載の発明の構成に加えて、前記ユーザのプロフィール情報は、該プロフィール情報に基づいての前記第三者エージェントによる判断の結果に対するユーザの反応に基づいて更新されることを特徴とする。

【発明を実施するための最良の形態】

【００２４】

次に、本発明の実施の形態を図面に基づいて詳細に説明する。

図１は、情報の検索および配信システムの全体の概略を説明するための図である。図１を参照して、有線系メディアの一例としてのインターネット１３に対し、ユーザ宅１７のパーソナルコンピュータ（以下単にパソコンという）１４とコンテンツ提供業者７と第三者機関８と会員管理センター１２と番組関連データ制作者１１とコマーシャルメッセージ（以下単にＣＭという）制作者１０と番組制作者９と放送局２とが接続可能に構成されている。

【００２５】

コンテンツ提供業者７は、たとえば書籍情報や映画情報あるいは音楽情報，ニュース情報等の提供可能な情報を格納したデータベースを有しており、そのデータベース内の格納情報やその要約（アブストラクト）とを、インターネット１３を経由してまたは無線系メディアの一例としての放送局２からの衛星放送によりユーザ宅１７のパソコン１４に提供する。コンテンツ提供業者７が提供可能なコンテンツの種類としては、その他に、たとえば課金のために暗号化された暗号化コンテンツデータやいわゆるネット家電を制御するための制御用プログラムデータ等が考えられる。

【００２６】

ユーザのパソコン１４は、放送局２からたとえば衛星１を介して送信されてくる前述したアブストラクトデータを受信し、後述するユーザのエージェントによりそのアブストラクトを検索して取捨選択し、選択したアブストラクトデータをユーザに表示してユーザの選択指示を待つ。あるいは、ユーザにアブストラクト情報を表示する前に、そのアブストラクト情報の送信元であるコンテンツ提供業者７にまで出向いて実際のコンテンツ情報にアクセスして内容を吟味し、本当にユーザが好むコンテンツであるか否かを確認し、確認後のアブストラクトをユーザに表示するようにしてもよい。

【００２７】

ユーザの指示またはユーザのエージェント独自の判断により、コンテンツを入手したい要望が発生すれば、コンテンツ提供業者７は、その選択されたコンテンツ情報を放送局２に送信して所定の日時に放送してもらう。その放送予定日時と放送のチャンネル情報を放送局２から通知を受けたコンテンツ提供業者７は、その放送日時とチャンネル情報をインターネット１３を経由してユーザのパソコン１４に送信する。

【００２８】

コンテンツ提供業者７が提供するコンテンツ内に有料コンテンツが含まれている場合において、その有料コンテンツを販売する際には会員であるユーザのＩＤの確認が必要となる場合がある。その場合には、コンテンツ提供業者７は、ユーザのＩＤ情報を要求し、そのＩＤ情報を会員管理センター１２に送信し、ＩＤの確認を行なってもらい、確認済のユ

ーザのみに有料コンテンツの販売を行なう。

【００２９】

放送局２は、番組制作者９が制作した番組を入手し、その番組をアンテナ５，衛星１，アンテナ６を経由してユーザ宅１７に向けて放送する。その放送される番組のためのＣＭがＣＭ制作者１０により制作され、そのＣＭデータがインターネット１３を経由して放送局２にまで提供され、番組の合間にＣＭが挿入されて放送される。

【００３０】

放送局２から放送される番組を受信したユーザは、その番組を直接ＴＶ（テレビジョン）１６により放映したり、パソコン１４のＣＲＴにより直接映し出して閲覧する場合もあるが、一旦ＶＴＲ（ビデオテープレコーダ）１５により録画し、後日その録画情報を再生して閲覧する場合がある。ＴＶ１６は、このＶＴＲ１５やパソコン１４と連係して、ユーザが見たい場面だけを飛ばし飛ばし見るというイントロ再生機能や、複数のカメラ・アングルで撮影・放送された番組の場面切換をスムーズに実行できるようにする機能を有する。その機能実現のために、高速なランダム・アクセスが可能なハード・ディスク装置や半導体メモリなどが内蔵されている。また放送局２側では、映像番組に関するインデックス情報を加えて放送する。ユーザ側では、受信した番組データをＶＴＲ１５に記録させ、受信したインデックス情報をハード・ディスク装置などに蓄積する。このハード・ディスクは、ＶＴＲ１５から読出した映像データを一時的に蓄えるためにも使う。一般的に、ＶＴＲに蓄積した映像データは、検索から読出までに時間がかかる。しかし、ＶＴＲ１５から読出した映像データを一時的にハード・ディスクに蓄えれば、映像を再生している間にＶＴＲの早送りを実行することができ、ユーザから見た必要な映像を取出すまでの待ち時間が短くなる。

【００３１】

このようにして、前述したいわゆるイントロ再生がスムーズに実行することができる。その結果、受信した番組内にＣＭが挿入されている場合には、ユーザにしてみれば、その贅肉に相当するＣＭのみをカットして番組だけを閲覧したがる傾向にあり、前述したイントロ再生機能によりそのＣＭカット閲覧が容易に実行可能となる。

【００３２】

そこで、このようなＣＭカット閲覧を防止する方法として、番組関連データをＣＭに重合させて放送局２から放送する方法が考えられる。そのための番組関連データが番組関連データ制作者１１により制作されて放送局２に転送される。この番組関連データとしては、番組の意見交換用のホームページのアドレスや、番組に出てくる専門用語の解説等が考えられる。

【００３３】

ＣＭ制作者１０は、番組の合間に挿入されて放送局２から放送される一般的なＣＭばかりでなく、ユーザ（消費者）を多数の階層に分類してそれぞれの階層のみをターゲットにしたＣＭも作成する。この階層分けは、たとえば、性別，年齢別，学歴別，職業別，購買動向別等が考えられる。このようなターゲットを絞った多数のＣＭをＣＭ制作者１０が制作してデータベースに蓄積しておく。そして、ユーザのエージェントがそのＣＭ制作者にまで出向いてデータベースを検索し、ユーザが好むと思われるＣＭ情報を検索し、検索されたＣＭ情報をインターネット１３を経由してまたは放送局２からの放送により受信する。このようなユーザのエージェントによって検索されたＣＭ情報も、番組関連データ制作者１１が制作した番組関連データが重合された状態でユーザに届けられるように構成されている。

【００３４】

図２は、マルチエージェントシステムの構成を示す説明図である。本実施の形態においては、ゼネラルマジック（General Magic）社が開発した通信用言語であるテレスクリプトによる自律ソフトウェアとしてのエージェントを採用している。ユーザエージェント２６は、モバイルエージェントで構成されている。モバイルエージェントとは、分散コンピューティング環境における移動性を備えたエージェントのことであり、ネットワークを介

してエージェントがサーバーに転送・処理されること（リモート・プログラミング）が特徴となっている。モバイルエージェントが、テレスクリプト・エンジンによって提供される共通動作環境であるプレースに移動して、そのプレース上で他のエージェントと協調して相互に動作して仕事を行ない問題を解決する。

【００３５】

ユーザのパソコン１４内で動作しているユーザエージェントが、自己の判断でまたはユーザの操作指令に応じてコンテンツを検索する場合には、図２（ａ）で示すように、コンテンツ提供業者７のテレスクリプト・エンジン１８のプレース２４に移動する。プレース２４上に移動したユーザエージェント２６は、プレース２４に常駐している移動先エージェント２７と打合せ（meeting）して、データベース１９内のコンテンツを検索して希望するコンテンツを見つけ出してパソコン１４にまで持ち帰る（送信する）。

【００３６】

なお、５２はＣＲＴ，５３はキーボード，５０はＩＣカード挿入口，５１はフロッピー（登録商標）ディスク（ＦＤ）挿入口，２０はWWWサーバー，３は通信装置である。

【００３７】

一方、第三者機関８のテレスクリプト・エンジン２２のプレース２５には、第三者機関常駐エージェント２８が常駐している。データベース２３内には、複数種類の第三者機関エージェントが機能別に分類されて格納されている。この第三者機関８は、当事者（たとえばユーザとそのユーザの要求に応えてサービスを提供するサービス業者）のみでは解決困難なまたは解決不可能な中立性を要する仕事が発生した場合に、そのような特定の仕事を当事者に代わって代理実行して解決するために設立された機関であり、官庁等の公な機関あるいは半公共的な機関によって構成するのが望ましい。なお、図中２２ａは、第三者機関８が運用管理するコンピュータである。

【００３８】

第三者機関８のデータベース２３に格納されている各種第三者機関エージェントは、この第三者機関８によって運用管理されるものであり、前述した中立性を要する特定の仕事を中立性を守りながら実行して解決するために開発された専用のエージェントである。そして、ユーザエージェント２６には、たとえば、オンラインショッピングするためのショッピングエージェント，ニュースソースからニュース記事を検索して必要なもののみを選び出すニュースフィルタリングエージェント，必要な電子メールのみを選び出す電子メールエージェント，ユーザの嗜好に合致した音楽情報や映画情報を検索するファイアフライ等の情報収集エージェントなど、種々の種類が存在する。そこでそのようなユーザエージェント２６の仕事を代理実行する第三者エージェントの方も、ユーザエージェント２６の種類に合せて機能別に複数種類用意しておく必要がある。

【００３９】

コンテンツ提供業者７のプレース２４に移動したユーザエージェント２６が移動先エージェント２７と協調してデータベース１９内のコンテンツを検索する際に、データベース１９内の有料コンテンツを検索したい場合には、第三者機関常駐エージェント２８と連絡をとり、データベース２３から適した第三者機関エージェントを探し出してもらい、その第三者機関エージェントにコンテンツ提供業者７のプレース２４にまで出向してもらう。

【００４０】

その状態が図２の（ｂ）に示されている。出向してきた第三者機関エージェント２９は、ユーザエージェント２６とmeetingして、ユーザの好み等のプロフィール情報をユーザエージェント２６から聞き出す。そして、コンテンツの検索に必要な知識を取得した状態で第三者機関エージェント２９がデータベース１９にアクセスして、ユーザエージェント２６に代わってコンテンツの検索を行ないその検索結果をユーザエージェント２６に知らせる。

【００４１】

第三者機関エージェント２９がコンテンツを検索するためには、ユーザのプライバシーにかかわるような秘密情報（たとえばユーザの年収，学歴，貯蓄額等）をユーザコンテン

ツ２６から教えてもらわなければならない場合は、コンテンツ提供業者７のプレース２４上でその秘密情報をユーザエージェント２６が第三者機関エージェント２９に通知すれば、その秘密情報がコンテンツ提供業者７に漏れてしまうおそれがある。本実施の形態では、ユーザエージェント２６は、前述したような秘密情報ＳＩ（図１４参照）を暗号化して暗号化データとして保有しているために、ユーザエージェント２６はコンテンツ提供業者７のプレース２４に移動しただけでは、その秘密情報ＳＩがコンテンツ提供業者７に知られてしまうことはない。しかし、コンテンツ提供業者７のプレース２４上において、第三者機関エージェント２９が解読できるように暗号化秘密情報ＳＩを復号化して平文の形で第三者機関エージェント２９に教えた場合には、その平文の秘密情報ＳＩがコンテンツ提供業者７に知られる可能性が生ずる。

【００４２】

そこで、このような秘密情報ＳＩを用いなければコンテンツが検索できない場合には、図２（ｃ）に示すように、ユーザエージェント２６が第三者機関８のテレスクリプト・エンジン２２のプレース２５にまで移動し、そこに常駐している第三者機関常駐エージェント２８とmeetingして、最適な第三者機関エージェントを検索してもらい、その検索された第三者機関エージェント２９とユーザエージェント２６とがmeetingして、検索に必要となる秘密情報ＳＩを通知する（図２（ｄ）参照）。

【００４３】

その後、ユーザエージェント２６がコンテンツ提供業者７のプレース２４に復帰し、常駐エージェント２７とmeetingして有料コンテンツを暗号化した形で第三者機関８のプレース２５に転送してもらう。そして転送されてきた有料コンテンツを復号化して第三者機関エージェント２９がユーザエージェント２６に代わってその有料コンテンツを検索して評価する。その評価結果をプレース２４上のユーザエージェント２６に通知する。このようにすれば、ユーザエージェント２６が知識として保有している秘密情報ＳＩがコンテンツ提供業者７等に漏洩することが防止できる。なお、第三者機関８のプレース２５上では、エージェント同士がいくらmeetingしても情報が外部に漏洩することが防止できるように構成されている。

【００４４】

図３は、ユーザのパソコン１４の制御動作を示すフローチャートである。このユーザのパソコン１４の制御回路は、図１２に基づいて後述する。

【００４５】

図３を参照して、まずステップＳ（以下単にＳという）１により、インターネット上のサイトを紹介する情報を受信したか否かの判断がなされる。この情報は、放送局２から衛星放送により放送されてユーザのパソコン１４が受信したり、またはインターネット１３経由で受信する。サイト紹介情報を受信していない場合にはＳ２に進み、記録対象コンテンツの放送日時になったか否かの判断がなされる。記録対象コンテンツとは、ユーザの入力指示によりＶＴＲ１５等に記録する予定となっている番組等の放送局２から送られてくるコンテンツや、ユーザエージェントが独自の判断で記録予定にしている放送局２から送られてくるコンテンツのことである。記録対象コンテンツの放送日時になっていない場合にはＳ３に進み、放送番組のアブストラクトを受信したか否かの判断がなされる。前述したように、放送局２は、放送する番組の内容の要約（アブストラクト）を事前にユーザに向けて放送し、ユーザは、そのアブストラクト放送を受信してユーザエージェントに番組を録画記録させるかどうかを判断させる。放送番組のアブストラクトを受信していない場合にはＳ４に進み、ユーザからエージェントへの指示があったか否かの判断がなされる。

【００４６】

ユーザからエージェントへの指示がない場合には、Ｓ５に進み、コンテンツの再生指示があったか否かの判断がなされる。ない場合にはＳ６に進み、鍵ＳＫ１の送信要求があったか否かの判断がなされる。この鍵ＳＫ１は、前述した暗号化されている秘密情報ＳＩを復号化するために用いられる鍵であり、後述するように第三者機関常駐エージェント２８が必要に応じてユーザのパソコン１４に対し送信要求を出すものである。ＳＫ１の要求が

ない場合にはＳ７に進み、ユーザエージェントから放送コンテンツの記録指示があったか否かの判断がなされる。ユーザのパソコン１４内で動作しているユーザエージェントは、後述するように自己の判断に基づいて放送番組等の放送コンテンツを自動的に記録する指示をパソコン１４に出す場合がある。

【００４７】

ユーザエージェントから放送コンテンツの記録指示がない場合にはＳ８に進み、放送日時とチャンネルを受信したか否かの判断がなされる。ユーザエージェントは、図９に基づいて後述するように、ＣＭ作成者１０のプレース２５に移動してＣＭを検索し、希望するＣＭが見つかれば、その希望するＣＭが放送局２から放送される日時とチャンネルをユーザのパソコン１４に送信してくる。そのユーザエージェントからの放送日時とチャンネルが送信されてきたか否かがこのＳ８により判断される。放送日時とチャンネルを受信していない場合にはＳ９に進み、その他の処理がなされてＳ１に戻る。

【００４８】

放送局２から放送されたサイト紹介情報あるいはインターネット１３を経由して送信されてきたサイト紹介情報を受信すれば、Ｓ１によりＹＥＳの判断がなされてＳ１０に進み、ユーザのパソコン１４内で動作しているユーザエージェントにそのサイト紹介情報を知らせる処理がなされる。

【００４９】

Ｓ２により、記録対象コンテンツの放送日時になったと判断された場合にはＳ１１に進み、放送されるチャンネル周波数にチューニングし、Ｓ１２により、放送コンテンツを受信してＶＴＲ１５に記録する処理がなされる。次にＳ１３に進み、記録したコンテンツがＣＭを含むか否かの判断がなされる。含まない場合にはＳ１に戻るが、含む場合にはＳ１４に進み、編集時間があるか否かの判断がなされる。この編集時間とは、ユーザエージェントがＣＭ制作者１０のプレース５８に移動して検索して見つけ出したＣＭと放送局２が放送してＶＴＲ１５等に記録させた番組の合間に挿入されているＣＭとを差替える編集を行なうのに必要な時間のことである。

【００５０】

編集時間がある場合にはＳ１５に進み、対応する番組コンテンツのＣＭ部分を検索したＣＭに取替える編集を行なった後Ｓ１に戻る。編集時間がない場合にはＳ１６に進み、番組放映中にＣＭ放送時間が来た瞬間ユーザエージェントが検索したＣＭに切換えて放映する制御を行なってＳ１に戻る。

【００５１】

放送番組のアブストラクトが放送局２から放送されてそれを受信すればＳ３によりＹＥＳの判断がなされてＳ１７に進み、ユーザエージェントにその受信したアブストラクトを知らせる処理がなされる。

【００５２】

ユーザがキーボード５３やマウス等を操作してエージェントへの何らかの指示を行なえば、Ｓ１８に進み、パソコン１４内で活動しているユーザエージェントにその指示を知らせる処理がなされる。

【００５３】

ユーザがキーボード５３やマウス等を操作してコンテンツの再生指示を行なえばＳ５によりＹＥＳの判断がなされてＳ１９に進み、再生の対象となるコンテンツが暗号化されたコンテンツであるか否かの判断がなされる。暗号化コンテンツの場合にはＳ２０によるコンテンツ再生処理を行なった後、Ｓ２１によるコンテンツの出力処理がなされてＣＲＴ５２やＴＶ１６により放映される。一方、暗号化コンテンツでない場合にはＳ２０の処理を行なうことなく直接Ｓ２１に進み、コンテンツ出力処理がなされる。Ｓ２６のコンテンツ再生処理の詳細は、図１７に基づいて後述する。

【００５４】

鍵ＳＫ１の送信要求があった場合にはＳ６によりＹＥＳの判断がなされてＳ２２に進み、チャレンジデータＣＨを第三者機関常駐エージェント２８へ送信する処理がなされる。

このチャレンジデータＣＨは、パソコン１４が生成した乱数等により構成される。第三者機関常駐エージェント２８は、このチャレンジデータＣＨを受取り第三者機関８の秘密鍵ＳＫ３でそれを暗号化する処理すなわちE_{SK3}（ＣＨ）を算出してレスポンスデータＲＥＳとして返信する（ＳＢ１２，ＳＢ２３ｂ参照）。

【００５５】

このレスポンスデータＲＥＳを受信したパソコン１４は、Ｓ２２ａによりＹＥＳの判断がなされてＳ２２ｂに進み、受信したレスポンスデータＲＥＳを第三者機関８の公開鍵で復号化する処理すなわちD_{PK3}（ＲＥＳ）を演算し、その演算結果とＳ２２により送信したチャレンジデータＣＨとが一致するか否かの判断が行なわれる。正規の第三者機関８の第三者機関常駐エージェント２８からＳＫ１の要求があったのであれば、ＣＨ＝D_{PK3}（ＲＥＳ）となるはずであるために、その場合にはＳ２２ｃに進み、鍵ＳＫ１を第三者機関８の公開鍵ＰＫ３を用いて暗号化する演算すなわちE_{PK3}（ＳＫ１）を算出して第三者機関常駐エージェント２８へ送信する処理がなされる。一方、Ｓ２２ｂより一致しないと判断された場合にはＳ２２ｃの送信処理を行なうことなくＳ１に戻る。

【００５６】

ユーザエージェントから放送コンテンツの記録指示があった場合にはＳ２３に進み、その指示のあった記録対象コンテンツの放送日時，チャンネルを記憶する処理がなされる。

【００５７】

ユーザエージェントから放送日時とチャンネルが送信されてくればＳ８によりＹＥＳの判断がなされてＳ２４へ進み、その送信されてきた放送日時とチャンネルすなわち記録対象コンテンツの放送日時とチャンネルを記憶する処理がなされる。

【００５８】

図４～図６，図１０は、ユーザエージェントの動作を示すフローチャートである。ＳＡ１により、インターネット上のサイトの紹介情報を受取ったか否かの判断がなされ、受取っていない場合にはＳＡ２に進み、番組のアブストラクト情報を受取ったか否かの判断がなされ、受取っていない場合にはＳＡ３に進み、ユーザからの指示を受取ったか否かの判断がなされ、受取っていない場合にはＳＡ４に進み、ユーザエージェントが移動する時刻が来たか否かの判断がなされ、来ていない場合にはＳＡ５に進み、その他の処理を行なった後ＳＡ１に戻る。

【００５９】

放送局２から放送されたサイト紹介情報を受信した場合やインターネット１３経由で送信されてきたサイト紹介情報を受取った場合には、ＳＡ６に進み、その情報内にコンテンツのアブストラクトが含まれているか否かの判断がなされる。コンテンツのアブストラクトが含まれている場合にはＳＡ７に進み、そのアブストラクトとサイト紹介情報とでユーザエージェントが評価を行なう。この評価は、このユーザエージェントの持主であるユーザが好むサイトであるか否かあるいはユーザが好むコンテンツであるか否かを判断することである。ユーザエージェントは、たとえば後述する図１４に示すようなユーザの嗜好情報等を含むプロフィール情報９６を知識として保有しており、このプロフィール情報を活用して評価を行なう。

【００６０】

一方、コンテンツのアブストラクトが含まれていない場合にはＳＡ８に進み、サイト紹介情報のみで評価を行なう。次にＳＡ９に進み、評価が所定値以上であるか否かの判断がなされ、所定値以上でない場合にはＳＡ１に戻る。一方所定値以上である場合にはＳＡ１０に進み、そのサイトのアドレスを移動先予定として登録した後ＳＡ１に戻る。

【００６１】

ユーザのパソコン１４が放送番組のアブストラクトを受信してＳ１７によりユーザエージェントに知らせた場合には、ＳＡ２によりＹＥＳの判断がなされてＳＡ１１に進み、その番組アブストラクトに基づいて番組の評価を行なう。この評価は、前述したように、ユーザのプロフィール情報９６に基づいてユーザがどの程度好むかを判断して行なう。そして、ＳＡ１２により、その評価が所定値以上であるか否かの判断がなされ、所定値以上で

ない場合にはＳＡ１に戻るが、所定値以上の場合にはＳＡ１３に進み、推薦番組リストに登録する処理がなされる。この推薦番組リストに登録された番組がユーザに推薦番組として表示され、後述するようにユーザの指示を仰ぐ。ユーザがこの推薦番組の放送を受信して閲覧またはＶＴＲ１５に録画する旨の指示を出せば、その指示された推薦番組が推薦番組リストから消去されることとなる。

【００６２】

ＳＡ１４に進み、推薦番組リストに登録されている番組で放送日時が来るものがあるか否かの判断がなされ、ない場合にはＳＡ１に戻る。この推薦番組リストに登録されているということは、前述したようにユーザに推薦する番組でありながら未だにユーザが閲覧するか破棄するかの指示を出していないものであり、そのようなユーザの指示がまだ出されていない推薦番組の放送日時が来てしまった場合には、ＳＡ１５により、その推薦番組をユーザエージェントの自己判断で自動的に記録するか否かの判別を行なう。自動記録しないと判断された場合にはＳＡ１６により、推薦番組リストからその日時が来た番組を消去した後ＳＡ１に戻る。一方、自動記録すると判断された場合にはＳＡ１７に進み、その推薦番組リストに登録されている推薦番組を自動記録番組リストの方に移し替えて登録する処理がなされる。

【００６３】

次にＳＡ１８に進み、パソコン１４に対しコンテンツの記録指示を出す。その結果、前述したように、Ｓ７により、ＹＥＳの判断がなされてＳ２３により指示のあった記録対象コンテンツの放送日時，チャンネルが記録される。その結果、放送日時が現時点となるために、Ｓ２により即座にＹＥＳの判断がなされて、その放送日時が来た推薦番組を受信して記録する処理がＳ１７以降で行なわれる。

【００６４】

次にＳＡ１９に進み、指示を出した番組コンテンツにＣＭがあるか否かの判断がなされる。ない場合にはＳＡ１６に進み、推薦番組リストから日時が来たものを消去する処理がなされる。つまり、推薦番組リストに登録されている推薦番組を受信して記録することとなったために、それ以降推薦番組リストに登録しておく必要がなくなるために、その記録することとなった推薦番組を推薦番組リストから消去するのである。

【００６５】

一方、ＳＡ１９により、指示を出した番組コンテンツにＣＭがあると判断された場合にはＳＡ２０に進み、番組スポンサーに対応するＣＭを検索する処理がなされた後ＳＡ１６に進む。このＳＡ２０のスポンサーに対応するＣＭ検索処理は、後述する図１０に基づいて説明する。

【００６６】

ユーザがユーザエージェントに対し指示を出した場合にはＳ１８によりその指示がユーザエージェントに知らされ、その結果ＳＡ３によりＹＥＳの判断がなされてＳＡ２１に進む。ＳＡ２１では、そのユーザからの指示が推薦番組リストの閲覧指示であるか否かの判断がなされ、閲覧指示の場合にはＳＡ２２に進み、推薦番組リストをＣＲＴ５２またはＴＶ１６により表示する制御がなされる。一方、推薦番組リストの閲覧指示でなかった場合にはＳＡ２３に進み、自動記録番組リストの閲覧指示であるか否かの判断がなされる。ＳＡ２３よりＹＥＳの判断がなされた場合にはＳＡ２４に進み、自動記録番組リストをＣＲＴ５２またはＴＶ１６により表示させる制御がなされる。

【００６７】

自動記録番組リストの閲覧指示でなかった場合にはＳＡ２５に進み、コンテンツ検索結果の閲覧指示であるか否かの判断がなされる。ユーザエージェントがコンテンツを検索した場合には後述するようにその検索結果をパソコン１４に送信するのであり、その検索結果の閲覧指示であった場合にはＳＡ２６により、コンテンツ検索結果をＣＲＴ５２またはＴＶ１６により表示させる制御がなされる。

【００６８】

コンテンツ検索結果の閲覧指示でなかった場合にはＳＡ２７に進み、推薦番組の記録指

示であるか否かの判断がなされる。ＳＡ２２により表示された推薦番組を閲覧したユーザがその推薦番組の中から記録して閲覧したいものがあった場合にはその記録希望の推薦番組の記録指示を出す。その結果ＳＡ２７によりＹＥＳの判断がなされてＳＡ２９に進み、その指示された推薦番組コンテンツの記録指示をパソコン１４に出す処理がなされる。その結果、パソコン１４では、Ｓ７によりＹＥＳの判断が行なわれてＳ２３により、その指示された記録対象コンテンツの放送日時，チャンネルを記録する処理がなされ、その結果、Ｓ２により、その記憶した記録対象コンテンツの放送日時になった場合にＳ１１以降のコンテンツの記録処理が実行されることとなる。

【００６９】

次にＳＡ３０に進み、指示を出した番組を推薦番組リストから消去する処理がなされた後ＳＡ１９に進む。

【００７０】

推薦番組記録指示でなかった場合にはＳＡ２８に進み、ユーザエージェントがその他の処理を実行してＳＡ１に戻る。

【００７１】

ＳＡ３によりＮＯの判断がなされた場合にはＳＡ４に進み、移動時刻が来たか否かの判断がなされる。この移動時刻とは、ユーザエージェントがネットワークを介してインターネット上のサイトに移動し、コンテンツ等の検索を実行する時刻のことであり、予め設定されている時刻である。未だに移動時刻が来ていない場合にはＳＡ５に進み、その他の処理を実行した後ＳＡ１に戻る。一方、移動時刻が来た場合にはＳＡ５ａに進み、エージェント移動処理を実行した後ＳＡ１に戻る。このエージェント移動処理は、図５，図６に示されている。

【００７２】

次に、図５，図６に基づいて、エージェント移動処理のフローチャートを説明する。ＳＡ３１により、ユーザエージェントを移動させる処理を行なう。このユーザエージェントの移動先は、前述したＳＡ１０により移動先予定として登録されたアドレスにより特定される。このユーザエージェントの移動は、実際には、ユーザのパソコン１４内のユーザエージェントと全く同じユーザエージェント（クローン）を複製してそれを移動先に転送する処理である。

【００７３】

次にＳＡ３２に進み、移動先のプレースに常駐している移動先エージェント２７とmeeting（打合せ）して、種々の必要な情報交換を行なう。次にＳＡ３３に進み、そのmeetingの結果に基づいて、データベース１９内に無料コンテンツがあるか否かの判断を行ない、無料コンテンツがある場合にはＳＡ３４に進み、その無料コンテンツを検索する処理を行ない、ＳＡ３５によりその検索が完了したか否かの判断を行ない、完了するまで無料コンテンツの検索処理を続行する。そして完了した段階でＳＡ３６に進む。一方、無料コンテンツがないと判断された場合には直接ＳＡ３６に進む。

【００７４】

ＳＡ３６では、データベース１９内に有料コンテンツがあるか否かの判断がなされ、ない場合にはＳＡ３８に進み、移動先エージェント２７とmeetingして、選択したコンテンツのパソコン１４への送信指令を出してもらう。次にＳＡ３９に進み、検索結果をパソコン１４に送信する処理を行ない、ＳＡ４０に進み、移動が終了したか否かの判断がなされる。ＳＡ１０により登録された移動先予定をすべて移動した場合には移動終了と判断されてＳＡ４０ａに進み、自分自身を消去して終了する。一方、ＳＡ４０により移動終了でないと判断された場合には再びＳＡ３１に進み、次の移動予定のアドレスにユーザエージェントが移動して前述と同様の処理を行なう。

【００７５】

一方、ＳＡ３６により有料コンテンツがあると判断された場合にはＳＡ３７に進み、その有料コンテンツをコンテンツのアブストラクトにより検索する処理を行なう。そしてＳＡ４１によりその検索が完了するまでその検索を続行する。検索が完了した段階でＳＡ４

２に進み、有料コンテンツ内に、所定料金を超える高額有料コンテンツがあるか否かの判断がなされ、ない場合にはＳＡ３９に進み、有料コンテンツのアブストラクトによる検索結果をパソコン１４へ送信する。高額有料コンテンツがある場合にはＳＡ４３に進み、その高額有料コンテンツ内に入手したいものがあるか否かの判断が行なわれる。この判断は、高額有料コンテンツの前述したアブストラクトにより判断する。入手したいものがない場合にはＳＡ３９に進むが、入手したいものがある場合にはＳＡ４４に進む。

【００７６】

以上の説明のように、高額有料コンテンツでない低額有料コンテンツに対しては、そのコンテンツのアブストラクトのみを検索してその検索結果をパソコン１４へ送信し、ユーザの指示を仰ぐ。一方、高額有料コンテンツ内に入手したいものがある場合には、ＳＡ４４により、その入手希望高額コンテンツの検索に秘密情報（ＳＩ）が必要であるか否かの判断がなされる。必要でない場合にはＳＡ４５に進み、移動先エージェント２７に自己のエージェントの種類を知らせて最寄りの第三者機関エージェントに出向依頼を行なう処理がなされる。移動先エージェント２７は、この依頼を受けて、最寄りの第三者機関８の第三者機関常駐エージェント２８と交信し、ユーザエージェント２６の種類に応じた最適な種類の第三者機関エージェントの出向（派遣）を依頼する。その依頼を受けて、第三者機関エージェントが移動先であるたとえばコンテンツ提供業者７のプレース２４に出向してくれば、ＳＡ４６により、ＹＥＳの判断がなされてＳＡ６４へ進む。

【００７７】

ＳＡ６４では、出向してきた第三者機関エージェント２９とmeeting（打合せ）して入手希望高額コンテンツの検索の代理を行なってもらうよう依頼する（図２（ｂ）参照）。すると、後述するように、第三者機関エージェント２９は、必要なプロフィール情報９６をユーザエージェント２６から聞き出してそれに基づいてデータベース１９にアクセスして入手希望高額コンテンツの検索を行ない、ユーザエージェント２６の持主であるユーザが好むであろうと予想される高額コンテンツを検索してその評価を行なう。次にＳＡ６６により、ユーザエージェント２６が第三者機関エージェント２９に対し検索結果の評価を知らせてもらう。

【００７８】

次にＳＡ６７に進み、検索された有料コンテンツを購入するか否かの判断をユーザエージェント２６が行なう。購入しない場合にはＳＡ３９に進むが、購入する場合にはＳＡ６８に進み、移動先エージェント２７とmeetingして、オーダ情報ＯＩと支払い指示ＰＩとの暗号化情報E_{PK3}（ＯＩ），E_{PK3}（ＰＩ）を受取る。このオーダ情報ＯＩは、購入を希望する有料コンテンツの種類を特定するコンテンツＮＯと購入するという意思表示情報等である。また支払い指示ＰＩとは、たとえばクレジットかあるいは電子キャッシュか等の支払い方法とその支払い金額情報である。それらの情報ＯＩとＰＩとを第三者機関８の公開鍵ＰＫ３で暗号化した情報を移動先エージェント２７からユーザエージェント２６が受取る。

【００７９】

次にＳＡ６９に進み、その受取った情報とともに第三者機関８のプレース２５へ移動する。次にＳＡ７０により、第三者機関常駐エージェント２８とmeetingして（図２（ｃ）参照）、ユーザの秘密鍵ＳＫＵをユーザの鍵ＳＫ１で暗号化した暗号化秘密鍵E_{SK1}（ＳＫＵ）と、前述したE_{PK3}（ＯＩ），E_{PK3}（ＰＩ）とを第三者機関常駐エージェント２８に知らせるとともに、秘密情報ＳＩの復号鍵ＳＫ１をユーザのパソコン１４から取り寄せてもらう依頼を行なう。

【００８０】

第三者機関常駐エージェント２８は、ユーザのパソコン１４からＳＫ１を受取ってその鍵を用いて復号化処理を行ない、ＳＫＵ，ＯＩ，ＰＩを再生し、ＯＩ，ＰＩについてハッシュ化してオーダ情報ダイジェストＯＩ′と支払い指示ダイジェストＰ′を生成し、その両ダイジェストを合せた状態でユーザの秘密鍵ＳＫＵで暗号化し、そのE_{SKU}（ＯＩ′，ＰＩ′）を生成する。ＳＡ７１では、ユーザエージェント２６は、そのE_{SKU}（ＯＩ′，

ＰＩ′）を受取り移動先であるコンテンツ提供業者７のプレース２４に復帰する。次にＳＡ７２により、移動先エージェント２７とmeetingして、E_{SKU}（ＯＩ′，ＰＩ′）を通知するとともに、選択したコンテンツのパソコン１４への送信指令を出してもらう依頼を行なう。そしてその後ＳＡ３９へ進む。

【００８１】

前述したユーザの秘密鍵ＳＫＵは、たとえばＲＳＡ公開鍵暗号方式に用いられる秘密鍵のことであり、このユーザの秘密鍵が、エレクトリックコマースにおける本人認証用のデジタル署名等に用いられる。なお、ＳＫＵの秘密鍵やそれに対応する公開鍵を用いた暗号化や復号化のアルゴリズムは、ＲＳＡ公開鍵暗号方式のアルゴリズムの代わりに、いわゆる楕円曲線暗号のアルゴリズムを用いてもよい。

【００８２】

次に、前述したＳＡ４４により、入手希望高額コンテンツの検索に秘密情報ＳＩが必要であると判断された場合にはＳＡ４７に進み、ユーザ認証が必要であるか否かの判断がなされる。コンテンツ提供業者の中には、高額コンテンツの検索を希望するユーザエージェントに対し、本人認証を要求する場合がある。すなわち、検索対象となるコンテンツの料金が高額であるために、閲覧希望を出したユーザエージェントとその持主であるユーザが本当に本人自身であるか否かを確かめ、他人によるなりすましを防止したいと希望するコンテンツ提供業者が存在する。そのような場合には、ＳＡ４７により、ユーザ認証が必要であると判断され、ＳＡ４８に進み、認証対象メッセージＮＭを暗号化した暗号化認証対象メッセージE_{PK3}（ＮＭ）をユーザエージェント２６が移動先エージェント２７から受取る。

【００８３】

このＰＫ３は、前述したように、第三者機関８の公開鍵である。そしてＳＡ４９に進み、最寄りの第三者機関８へユーザエージェント２６が移動し、第三者機関常駐エージェント２８とmeetingして最適な第三者機関エージェントを検索してもらうとともに、秘密情報の復号鍵ＳＫ１をパソコン１４から取り寄せてもらう依頼を行なう。次にＳＡ５１に進み、検索された第三者機関エージェントとmeetingし、必要な暗号化秘密情報E_{SK1}（ＳＩ）をその第三者機関エージェント２９に通知する。次にＳＡ５２に進み、ユーザ認証が必要であったか否かの判断がなされ、必要であった場合にはＳＡ５３に進み、第三者機関エージェントからE_{SKU}（ＮＭ）を受取った後ＳＡ５４へ進む。

【００８４】

第三者機関エージェント２９は、後述するように、E_{PK3}（ＮＭ）を第三者機関の秘密鍵ＳＫ３で復号化して再生されたＮＭをユーザの秘密鍵ＳＫＵで暗号化した情報すなわちE_{SKU}（ＮＭ）を生成する。ユーザエージェント２６は、第三者機関エージェント２９とmeetingして、そのE_{SKU}（ＮＭ）を受取るのである。なおこの認証対象メッセージＮＭは、たとえば、移動先エージェント２７が生成した乱数等である。

【００８５】

次にＳＡ５４では、たとえばコンテンツ提供業者７のプレース２４等の移動先へ復帰する処理がなされ、ＳＡ５５に進み、移動先エージェント２７とmeetingして、暗号化された入手希望高額コンテンツE_{PK3}（ＫＣ）を第三者機関８に転送してもらう依頼を行なう。

【００８６】

第三者機関エージェント２９は、E_{PK3}（ＫＣ）を復号化して再生された入手希望高額コンテンツＫＣを検索して評価を行ない、その検索結果の評価を第三者機関８の秘密鍵であるＳＫ３により暗号化し、その暗号化データであるE_{SK3}（ＨＫ）を移動先のプレース２４上のユーザエージェント２６へ転送する。すると、ＳＡ５６によりＹＥＳの判断がなされてＳＡ５７に進み、その受取ったデータを第三者機関の公開鍵ＰＫ３で復号化する処理すなわち$D_{PK3}\{E_{SK3}$（ＨＫ）$\}$を演算して、評価ＨＫを再生する処理を行なう。

【００８７】

次にＳＡ５８へ進み、再生された評価ＨＫに基づいて有料コンテンツを購入するか否か

の判断がな行なわれ、購入しない場合にはＳＡ５９により処理完了した旨を第三者機関８へ通知した後ＳＡ３９へ進む。一方、購入する場合にはＳＡ６０へ進み、移動先エージェント２７とmeetingして、オーダ情報ＯＩと支払い指示ＰＩとの暗号情報E_{PK3}（ＯＩ），E_{PK3}（ＰＩ）を第三者機関８へ転送してもらう依頼を行なう。第三者機関常駐エージェント２８は、前述と同様に、E_{SKU}（ＯＩ′，ＰＩ′）を生成し、それを移動先のユーザエージェント２６へ送信する。その結果、ＳＡ６１によりＹＥＳの判断がなされてＳＡ６２へ進み、移動先エージェント２７とmeetingして、選択したコンテンツの送信指令を行なってもらうよう依頼する。次にＳＡ６３に進み、処理完了した旨を第三者機関８へ通知した後、ＳＡ３９へ進む。

【００８８】

前述したE_{SKU}（ＯＩ′，ＰＩ′）が、いわゆるＳＥＴ（Secure Electronic Transaction）で規定されているオ―ダ情報と支払い指示とに対するユーザの二重署名である。

【００８９】

図７は、第三者機関常駐エージェント２８の動作を示すフローチャートである。ＳＢ１により、出向依頼（派遣依頼）があったか否かの判断がなされ、ない場合にはＳＢ２に進み、ユーザエージェント２６が第三者機関８のプレース２５に来たか否かの判断がなされ、来ていない場合にはＳＢ３に進み、ユーザエージェント２６から処理完了の旨の通知があったか否かの判断がなされ、ない場合にはＳＢ４へ進み、移動先エージェント２７からE_{PK3}（ＯＩ），E_{PK3}（ＰＩ）が送信されてきたか否かの判断がなされ、送信されてきていない場合にはＳＢ１へ戻る。

【００９０】

ユーザエージェント２６が第三者機関エージェントの出向依頼を移動先エージェント２７に対し行ない移動先エージェント２７が出向依頼があった旨と出向依頼をしたユーザエージェント２６の種類（たとえばオーソリティ情報）を第三者機関常駐エージェント２８に通知すれば、ＳＢ５に進み、第三者機関常駐エージェント２８は、通知されたエージェントの種類に基づいてデータベース２３にアクセスして第三者機関エージェントを検索する処理を行なう。そして、ユーザエージェント２６の種類に合致する最適な第三者機関エージェント２９を検索してＳＢ６により、その検索された第三者機関エージェント２９に出向指令を出す処理がなされて、ＳＢ１に戻る。

【００９１】

前述したＳＡ４９またはＳＡ６９により、ユーザエージェント２６が第三者機関８のプレース２５に来た場合には、ＳＢ２によりＹＥＳの判断がなされてＳＢ７に進み、ユーザエージェント２６とmeetingする。そして必要な種々の情報交換を行ない、ＳＢ８に進み、ユーザエージェント２９が来た目的が、第三者機関エージェント２９への仕事依頼のためなのか否かの判断が行なわれる。ユーザエージェント２６がＳＡ４９に基づいて第三者機関８のプレース２５に来たのであれば、ＳＢ８によりＹＥＳの判断がなされてＳＢ９に進み、第三者機関エージェント２９を検索する処理がなされる。

【００９２】

次にＳＢ１０に進み、ユーザエージェント２６の出所すなわちパソコン１４を呼出し、秘密情報ＳＩの暗号化データを復号化するための鍵ＳＫ１を要求する処理がなされる。この要求を受けたパソコンは、前述したように、ＳＫ１を要求してきた第三者機関８が本当に正規の第三者機関であるか否かの認証を行なうために、乱数を発生させてその乱数をチャレンジデータＣＨとして返信する。そのチャレンジデータＣＨを受信した第三者機関常駐エージェントは、ＳＢ１１によりＹＥＳの判断がなされてＳＢ１２に進み、E_{SK3}（ＣＨ）をレスポンスデータＲＥＳとしてパソコン１４へ送信する。

【００９３】

パソコン１４側では、前述したように、その送信されてきたレスポンスデータＲＥＳを第三者機関の公開鍵ＰＫ３で復号化して先ほどのチャレンジデータＣＨと一致するか否かの判断が行なわれ、一致する場合にのみ鍵ＳＫ１を第三者機関の公開鍵ＰＫ３で暗号化したE_{PK3}（ＳＫ１）を送信する。それを受信した第三者機関常駐エージェントでは、ＳＢ

１４によりＹＥＳの判断がなされ、ＳＢ１５に進み、その受信データを第三者機関８の秘密鍵で復号化する処理すなわち$D_{SK3}\{E_{PK3}$（ＳＫ１）$\}$を演算してＳＫ１を再生する。次にＳＢ１６に進み、検索された第三者機関エージェント２９にそのＳＫ１を通知する処理がなされてＳＢ１７へ進む。

【００９４】

ＳＢ１７では、ユーザエージェント２６が移動先すなわちコンテンツ提供業者７のプレース２４へ復帰したか否かの判断が行なわれ、復帰するまで待機する処理が行なわれる。第三者機関８のプレース２５に移動してきたユーザエージェント２６は、前述したＳＡ５０～ＳＡ５３の処理を行なった後、移動先へ復帰するのであり（ＳＡ５４参照）、移動先であるコンテンツ提供業者７のプレース２４へユーザエージェント２６が復帰した段階でＳＢ１８へ進み、ユーザエージェント２６のクローンを消去する処理がなされる。これにより、仕事が終了したユーザエージェント２６は、第三者機関エージェント２８のプレース２５上には存在しない状態となる。次にＳＢ１９に進み、第三者機関常駐エージェント２８は、第三者機関エージェント２９とmeetingして、ユーザの秘密鍵であるＳＫＵを聞き出す処理を行なった後、制御がＳＢ１へ戻る。

【００９５】

ユーザエージェント２６が前述したＳＡ６９に基づいて第三者機関エージェント８のプレース２５に来た場合には、ＳＢ８によりＮＯの判断がなされてＳＢ２０以降の処理がなされる。つまり、ユーザエージェント２６がＳＡ６９に従って第三者機関８に来るということは、有料コンテンツの購入手続を行なうために必要な処理を秘密情報の漏洩を防止しながら行なうためである。そのような場合には、第三者機関常駐エージェント２８は、まずＳＢ２０により、やってきたユーザエージェント２６から、E_{SK1}（ＳＫＵ），E_{PK3}（ＯＩ），E_{PK3}（ＰＩ）を受取る。次にＳＢ２１により、オーダ情報ＯＩと支払い指示ＰＩを再生する処理、すなわち、$D_{SK3}\{E_{PK3}$（ＯＩ）$\}$，$D_{SK3}\{E_{PK3}$（ＰＩ）$\}$を演算する。

【００９６】

次にＳＢ２２に進み、ＯＩとＰＩとをハッシュ化して両者のダイジェストＯＩ′，ＰＩ′を算出する処理がなされる。次にＳＢ２３へ進み、ユーザエージェント２６の出所すなわちパソコン１４に対し、ＳＫ１を要求する処理が行なわれる。

【００９７】

ユーザのパソコン１４が前述と同様にチャレンジデータＣＨを送信してくれば、ＳＢ２３ａによりＹＥＳの判断がなされてＳＢ２３ｂに進み、受信したチャレンジデータＣＨを第三者機関８の秘密鍵ＳＫ３で暗号化したE_{SK3}（ＣＨ）をレスポンスデータＲＥＳとしてパソコン１４へ送信する処理がなされる。パソコン１４では、前述したようにE_{SK3}（ＣＨ）に基づいて第三者機関８の認証を行ない、認証結果正しいと判断された場合にはE_{PK3}（ＳＫ１）を送信する。第三者機関常駐エージェント２８がそれを受信すれば、ＳＢ２５へ進み、$D_{SK3}\{E_{PK3}$（ＳＫ１）$\}$が演算され、ＳＫ１が再生される。

【００９８】

次にＳＢ２６へ進み、$D_{sk1}\{E_{SK1}$（ＳＫＵ）$\}$を演算してユーザの秘密鍵ＳＫＵを再生する処理が行なわれる。次にＳＢ２７へ進み、E_{SKU}（ＯＩ′，ＰＩ′）を演算してユーザエージェント２６に通知する処理が行なわれる。このE_{SKU}（ＯＩ′，ＰＩ′）がオーダ情報と支払い指示に対するユーザの二重署名となる。

３次にＳＢ２７ａに進み、ユーザエージェントが復帰したか否かの判断がなされる。ユーザエージェント２６は、前述したように、ＳＡ７０の処理を行なった後移動先であるコンテンツ提供業者７のプレース２４に復帰するのであり（ＳＡ７１参照）、ユーザエージェント２６が復帰した段階でＳＢ２７ｂに進み、ユーザエージェントのクローンを消去する処理がなされた後ＳＢ１へ戻る。

【００９９】

図８は、第三者機関エージェント２９の動作を示すフローチャートである。ＳＣ１により出向指令があったか否かの判断がなされ、ない場合にはＳＣ２に進み、E_{SK1}（ＳＩ）

を通知されたか否かの判断がなされ、通知されていない場合にはＳＣ１へ戻る。

【０１００】

このＳＣ１，ＳＣ２のループの巡回途中で、第三者機関常駐エージェント２８から出向指令を任命されれば（ＳＢ６参照）、ＳＣ１によりＹＥＳの判断がなされてＳＣ３へ進み、たとえばコンテンツ提供業者７のプレース２４等の移動先に移動する処理が行なわれる。この移動処理は、具体的には、第三者機関エージェント２９をデータベース２３内に残したままその第三者機関エージェント２９のクローンを移動先のプレース２４へ転送する処理である。次にＳＣ４に進み、移動先のプレース２４上において、ユーザエージェント２６とmeetingして、入手希望高額コンテンツを通知してもらうとともに、必要なユーザのプロフィール情報９６（図１４参照）を教えてもらう処理が行なわれる（ＳＡ６４参照）。このユーザエージェント２６から教えてもらうユーザのプロフィール情報９６は、公表可能情報ＮＳＩ（図１３参照）に限定される。これは、秘密情報の漏洩が防止可能な第三者機関８のプレース２５上でのユーザプロフィール情報のやり取りではなく、情報提供業者７のプレース２４上でのユーザプロフィール情報のやり取りであるために、秘密性が保持できず、そのために秘密性を保持する必要のない公表可能情報ＮＳＩに限定されるのである。

【０１０１】

次にＳＣ５に進み、入手希望高額コンテンツの評価を行なう処理がなされる。この評価は、教えてもらったユーザプロフィール情報９６に基づいて、ユーザが好むであろうと推測される度合いを数値化して行なう。次にＳＣ６に進み、入手希望高額コンテンツは違法なコンテンツであるか否かの判断がなされる。違法なコンテンツとは、たとえば、麻薬の密輸ルートに関するコンテンツや拳銃の入手経路のに関するコンテンツ等の刑法に違反するようなコンテンツである。また、風俗営業法に違反するようなコンテンツも違法コンテンツに含めてもよい。

【０１０２】

違法なコンテンツでないと判断された場合にはＳＣ１０へ進み、第三者機関エージェント２９が自分自身を消去して終了する。一方、違法なコンテンツであると判断された場合にはＳＣ７へ進み、違法のため購入できない旨の評価をユーザエージェント２６に知らせ、ＳＣ８により、違法である旨の通報を警察に行なう。次にＳＣ９へ進み、違法コンテンツを第三者機関８に持ち帰り証拠として保管する処理を行なった後ＳＣ１０へ進む。

【０１０３】

ＳＣ１，ＳＣ２のループの巡回途中で、ユーザエージェント２６により、ユーザのプロフィール情報のうちの秘密情報ＳＩを暗号化した情報であるE_{sk1}（ＳＩ）が通知された場合（ＳＡ５１参照）には、ＳＣ２によりＹＥＳの判断がなされてＳＣ１１に進み、第三者機関常駐エージェント２８とmeetingして、復号化するための鍵ＳＫ１を教えてもらう処理がなされる。次にＳＣ１２へ進み、D_{SK1}｛E_{sK1}（ＳＩ）｝を演算して秘密情報ＳＩを再生して記憶する処理がなされる。

【０１０４】

次にＳＣ１８へ進み、ユーザ認証が必要であるか否かの判断がなされ、必要でない場合にはＳＣ１５へ直接進むが、必要な場合にはＳＣ１４へ進む。ＳＣ１４では、E_{SKU}（ＮＭ）を演算してユーザエージェント２６へ知らせる処理がなされる。このＮＭは、移動先エージェント２７からユーザエージェント２６が受取った認証対象メッセージであり、第三者機関の公開鍵で暗号化された暗号化情報として受取る（ＳＡ４８参照）。そしてこの暗号化認証対象メッセージがユーザエージェント２６より第三者機関８のプレース２５に持込まれ、第三者機関常駐エージェント２８により復号化されて再生された認証対象メッセージＮＭが第三者機関エージェント２９に知らされる。第三者機関エージェント２９は、その通知されたＮＭとＳＣ１２により再生されたＳＩの中に含まれているユーザの秘密鍵ＳＫＵ（図１４参照）に基づいて、E_{SKU}（ＮＭ）を演算してユーザに知らせる。このE_{SKU}（ＮＭ）が、ユーザの本人認証用のデータとなり、ユーザエージェント２６はそれを受取り（ＳＡ５３参照）、移動先のプレース２４へ復帰して（ＳＡ５４参照）、そのプ

レース２４上の移動先エージェント２７にE_{SKU}（ＮＭ）を知らせる。

【０１０５】

次にＳＣ１５へ進み、E_{PK3}（ＫＣ）を受信したか否かの判断がなされ、受信するまで待機する。E_{SKU}（ＮＭ）を移動先のプレース２４へ持ち帰ったユーザエージェント２６は、移動先エージェント２７に対し入手希望高額コンテンツＫＣを暗号化したE_{PK3}（ＫＣ）を転送してもらう依頼を行なう（ＳＡ５５参照）。これを受けた移動先エージェント２７は、E_{PK3}（ＫＣ）を第三者機関８の第三者機関エージェント２８へ送信する。その送信されてきたE_{PK3}（ＫＣ）を受信すればＳＣ１６へ進み、$D_{PK3}\{E_{PK3}$（ＫＣ）$\}$を演算してＫＣを再生する処理が行なわれる。次にＳＣ１７へ進み、その入手希望高額コンテンツＫＣの評価を行なう処理がなされる。

【０１０６】

次にＳＣ１８へ進み、入手希望コンテンツは違法なコンテンツであるか否かの判断がなされる。この判断は、前述したＳＣ６と同様に行なわれる。そして違法なコンテンツである場合にはＳＣ７へ進むが、違法なコンテンツでない場合にはＳＣ１９へ進み、入手希望高額コンテンツＫＣの評価ＨＫに対し第三者機関８の秘密鍵ＳＫ３で暗号化したデータすなわちE_{SK3}（ＨＫ）を演算し、ＳＣ２０により、その演算結果を移動先のプレース２４上にいるユーザエージェント２６に送信する処理がなされた後ＳＣ１０へ進む。

【０１０７】

図９は、ＣＭ制作者１０におけるエージェントの動作を説明するための説明図である。ＣＭ制作者１０のテレスクリプト・エンジン５７内のＣＭプレース５８には、常駐エージェント５９が存在する。図中、５６はＣＭ制作者１０が制作した多数のＣＭを格納しているデータベース、５４はＷＷＷサーバー、５５は情報処理コンピュータである。

【０１０８】

ユーザのパソコン１４内で動作しているユーザエージェントは、必要に応じてインターネット１３を経由してＣＭ制作者１０のＣＭプレース５８に移動する。そのＣＭプレース５８上において、ユーザエージェント２６と常駐エージェント５９とがmeetingし、両者協調してユーザが好むと思われるＣＭを検索する。

【０１０９】

図１０は、図４のＳＡ２０に示したスポンサーに対応するＣＭ検索の具体的な動作を示すユーザエージェントのフローチャートである。ＳＡ７３により、ユーザエージェントがパソコン１４からＣＭプレース５８へ移動する。この移動は、パソコン１４内のユーザエージェント２６を複製してクローンを作成し、そのクローンをユーザエージェント２６としてＣＭプレース５８へ派遣することにより行なわれる。次にＳＡ７４へ進み、自分のクローンが既にＣＭプレース５８に駐在しているか否かの判断がなされ、既に駐在している場合にはＳＡ７３に戻り、次のＣＭ制作者１０のＣＭプレース５８へ移動する。

【０１１０】

このＳＡ７３，ＳＡ７４により、ユーザエージェント２６は、自分のクローンが駐在していないＣＭプレース５８を見つけ出してそこに移動することとなる。自分のクローンが駐在していないＣＭプレースを見つけ出した場合には、ＳＡ７５に進み、データベース５６にアクセスしてＣＭを検索する処理が行なわれる。次にＳＡ７６へ進み、希望するＣＭがあったか否かの判断がなされ、ない場合にはＳＡ８１へ進むが、あった場合にはＳＡ７７に進む。ＳＡ７７では、希望するＣＭを電波メディア（無線系メディア）を利用してユーザ宅１７にまで送信するかまたはインターネット等の有線系メディアを利用して送信するかの判断が行なわれる。電波メディアを利用しないと判断された場合にはＳＡ７８へ進み、希望するＣＭをインターネット１３経由でパソコン１４に送信する処理がなされる。

【０１１１】

一方、電波メディアを利用する場合にはＳＡ７９へ進み、常駐エージェント５９とmeetingして、希望するＣＭの放送日時とチャンネルを教えてもらう処理がなされる。次にＳＡ８０へ進み、放送日時とチャンネルと記録指示をインターネット１３を経由してパソコン１４へ送信する処理がなされる。

【０１１２】
次にＳＡ８１へ進み、ユーザエージェント２６がこのＣＭプレース５８に駐在するか否かの判断がなされる。駐在しない場合にはＳＡ８６へ進み、移動が終了したか否かの判断がなされ、移動予定となっているＣＭ作成者の中にまだ移動していないところがある場合にはＳＡ７３に戻り、次の移動先へ移動する。一方、移動予定となっているすべてのＣＭ作成者１０を移動し終わった場合にはＳＡ７８へ進み、ユーザエージェント２６がユーザのパソコン１４へ復帰する処理がなされて制御が終了する。
【０１１３】
一方、ユーザエージェント２６がこのＣＭプレース５８に駐在すると判断した場合にはＳＡ８２へ進み、自分のクローンを作りそれを移動先予定となっている他のＣＭ作成者１０のＣＭプレースに移動させる処理がなされる。次にＳＡ８３へ進み、ＣＭプレース５８に駐在することとなったユーザエージェント２６が、常駐エージェント５９とmeetingして、新たなＣＭ作成があったか否かの判断がなされる。ＣＭ制作者１０が新たなＣＭを制作してデータベース５６に記憶させれば新たなＣＭが制作された旨を常駐エージェント５９がＣＭプレース５８に駐在しているユーザエージェント２６に知らせるのであり、その知らせがあれば、ＳＡ８３によりＹＥＳの判断がなされてＳＡ８８へ進む。
【０１１４】
ＳＡ８８では、ＣＭプレース５８に駐在しているユーザエージェント２６がその新たなＣＭを検索して評価する処理がなされる。次にＳＡ８９へ進み、評価の結果その新たなＣＭの入手を希望するか否かの判断がなされ、希望しない場合にはＳＡ８３へ進むが、希望する場合にはＳＡ９０へ進み、希望するＣＭのユーザ宅１７への送信方法として、電波メディア（無線系メディア）を利用するか否かの判断がなされる。利用しない場合には、ＳＡ９３により、希望するＣＭをインターネット１３経由でパソコン１４へ送信する処理がなされた後ＳＡ８３へ進む。一方、電波メディアを利用する場合にはＳＡ９１へ進み、常駐エージェント５９とmeetingして、入手希望のＣＭの放送日時とチャンネルを教えてもらい、ＳＡ９２により、その放送日時とチャンネルと記録指示とをインターネット１３経由でパソコン１４へ送信する処理がなされた後ＳＡ８３へ進む。
【０１１５】
ＳＡ８３により、新たなＣＭ作成がないと判断された場合にはＳＡ８４へ進み、駐在を終了させるか否かの判断がなされ、ユーザエージェント２６の駐在をまだ続行させる場合にはＳＡ８３へ進むが、駐在を終了させる場合にはＳＡ８５へ進み、駐在しているユーザエージェント２６自身を消去する処理がなされて制御が終了する。
【０１１６】
図１１（ａ）はＣＭプレース５８上の常駐エージェント５９の動作を示すフローチャートであり、図１１（ｂ）は、ＣＭ制作者１０の情報処理コンピュータ５５の制御動作を示すフローチャートである。
【０１１７】
まずＣＭプレース５８に常駐している常駐エージェント５９の動作を説明する。
ＳＤ１により、新たなＣＭが制作されたか否かの判断がなされ、制作されていない場合にはＳＤ３に進むが、制作されている場合にはＳＤ２に進む。ＳＤ２では、ＣＭプレース５８に駐在しているユーザエージェント２６とmeetingして、新たなＣＭが制作された旨を知らせる処理がなされる。次にＳＤ３に進み、ＣＭ放送日時とチャンネルの通知依頼があったか否かの判断がなされ、なかった場合にはＳＤ１に戻る。一方、前述したＳＡ７９またはＳＡ９３に基づいてユーザエージェント２６がＣＭ放送日時とチャンネルの通知依頼を行なった場合には、ＳＤ３によりＹＥＳの判断がなされてＳＤ４に進む。
【０１１８】
ＳＤ４では、通知依頼のあったＣＭが既に放送が予定されているものであるか否かの判断がなされる。既に放送が予定されているものの場合には、放送予定日時とチャンネルが既に決まっているために、ＳＤ５に進み、その放送予定日時とチャンネルをＣＭプレース５８にいるユーザエージェント２６に通知する処理がなされた後ＳＤ１に戻る。

【０１１９】
一方、放送が予定されていない場合にはＳＤ６に進み、放送局２にＣＭを送信して放送依頼を行なう処理がなされる。次にＳＤ７に進み、放送日時とチャンネルの返信があったか否かの判断がなされ、返信があるまで待機する。放送依頼を受けた放送局２は、その依頼されたＣＭをいつ放送するかの予定を立て、決まれば放送日時とチャンネルとをＣＭ制作者１０のＣＭプレース５８の常駐エージェント５９のにその旨を送信する。すると、ＳＤ７によりＹＥＳの判断がななされてＳＤ８に進み、ＣＭ番号毎に分類して返信されてきた放送日時とチャンネルとを記憶する処理がなされる。次にＳＤ９に進み、放送日時とチャンネルをＣＭプレース５８上のユーザエージェント２６に通知する処理がなされた後ＳＤ１に戻る。

【０１２０】
次に情報処理コンピュータ５５の動作を説明する。ＳＥ１により、番組関連データを受信したか否かの判断がなされ、受信していない場合にはＳＥ４へ進む。図１で説明したように、番組関連データ制作者１１からＣＭ制作者１０に番組関連データが送信されて来れば、ＳＥ１によりＹＥＳの判断がなされてＳＥ２に進み、対応する番組のＣＭをデータベース５６から検索してそのＣＭと受信したデータである番組関連データとを重合させる処理を行なう。その結果、データベース５６内のＣＭは、番組関連データが重合されたＣＭデータとなる。また同じＣＭでも、どの番組に対し放映されるＣＭかによって番組関連データが異なるため、同じＣＭでも、対象となる番組毎に異なった番組関連データが重合された複数のＣＭデータがデータベース５６に格納されることとなる。その結果、前述したＣＤ６に従って放送局に送信されるＣＭは、そのＣＭに対応する番組の番組関連データが重合されたＣＭデータとなる。また、ユーザエージェント２６が常駐エージェント５９に対しＣＭ放送日時とチャンネルの通知依頼を行なう場合には、どの番組に挿入して放映するＣＭであるかを通知する。常駐エージェント５９は、その対象となる番組に対応した番組関連データが重合されたＣＭデータをデータベース５６から検索して放送局２へ送信する。なお、データベース５６を２分割して、ＣＭのみが格納されたＣＭ専用データベースと番組関連データ制作者１１から送信されてきた番組関連データのみを格納した番組関連データ専用データベースとで構成し、ユーザエージェント２６からのＣＭ放送日時とチャンネルの通知依頼を受けたときに、そのＣＭの挿入放映の対象となる番組に関する番組関連データを常駐エージェント５９が検索し、ユーザエージェント２６により検索されたＣＭデータと常駐エージェント５９が検索した番組関連データとを重合させて放送局２へ送信するようにしてもよい。次にＳＥ３に進み、重合したＣＭのうち番組とともに放送するＣＭを放送局２へ送信する処理がなされる。つまり、番組の合間に挿入されて放送されるＣＭがこのＳＥ３により放送局に送信され、放送局２から番組の放送とともに番組関連データが重合されたＣＭが放送される。

【０１２１】
次にＳＥ４に進み、新たに制作されたＣＭのデータベース５６への入力があったか否かの判断がなされ、ない場合にはＳＥ１に戻る。一方、入力があった場合にはＳＥ５に進み、その新たなＣＭをデータベース５６に記録する処理がなされ、次にＳＥ６に進み、その新たなＣＭが制作された旨を常駐エージェント５９に通知する処理がなされた後ＳＥ１に戻る。

【０１２２】
図１２は、前述したＳＥ２により番組関連データが重合されたＣＭを受信してユーザ宅１７のパソコン１４のＣＲＴ５２またはＴＶ１６によりそのＣＭを放映した画面図である。この図１２では、パソコン１４のＣＲＴ５２によりＣＭを放映した画面図が示されている。この図１２の場合には、コロンボ警部という主人公が登場するサスペンス番組の合間に挿入されるスーツのＣＭの場合である。そして、パソコン１４のユーザが、来年大学を卒業して社会人一年生となる者であり、来年卒業する情報がユーザのプロフィール情報としてユーザエージェント２６が知識として保有している。

【０１２３】

ゆえに、ユーザエージェント２６は、その来年卒業という知識に基づいて図１２に示すようなＣＭを検索した。そして、番組関連データとして、この番組の意見交換用のホームページのアドレスを表示させたり（図１２（ａ）参照）、このＣＭの放映の次に放映される番組部分で内容上注目すべき箇所、たとえば「殺人現場でのコロンボ警部の右手に注目下さい」のメッセージ表示を行なったりする（図１２（ｂ）参照）。また、図１２（ｃ）に示すように、番組に出てくる専門用語の説明、たとえば「サブリミナル効果：人間が意識できない一瞬だけ映像を挿入して潜在意識に訴える」の文字表示等を行なってもよい。このように、ＳＥ２による重合とは、図１２に示すように、ＣＭの映像と文字情報等の重合である。

【０１２４】

図１３は、図２に示したコンテンツ提供業者７の通信装置３とユーザのパソコン１４との制御回路を示すブロック図である。通信装置３は、可変長データ生成部３１、乱数取得部３２、暗号処理部３３、論理回路３４、通信制御部３５、認証処理部３６、およびマスタキー暗号処理部３７を備えている。

【０１２５】

可変長データ生成部３１は、移動先エージェント２７による選択コンテンツの送信指令（ＳＡ３８参照）に基づいてテレスクリプト・エンジン１８から伝送されてくるコンテンツの通信容量に応じたサイズの可変長データを生成する。たとえば静止画像の場合は画像１枚毎、動画像の場合は１表示画面毎に可変長データを生成する。この可変長データは任意のビット列からなるデジタルデータである。乱数取得部３２は、コンテンツを発振する度に乱数発生装置４から自然乱数を取得する。暗号処理部３３は、可変長データおよび自然乱数に基づいて可変長乱数列を生成する。暗号化に際してはＳＸＡＬ／ＭＢＡＬ（後述する）を使用する。

【０１２６】

論理回路３４は、テレスクリプト・エンジン１８から伝送されてきたコンテンツの個々のビットと暗号処理部３３により生成された可変長乱数列との排他的論理和（イクスクルーシブオア）を判定することで当該コンテンツをストリーム暗号化するものである。このストリーム暗号化された情報を伝送情報とする。通信制御部３５は、各ユーザのパソコン１４に対して通信設定して前記伝送情報や後述の通知情報を送信するとともに、各ユーザのパソコン１４から送られる情報を受信するものである。

【０１２７】

認証処理部３６は、ユーザのアクセス制御等に際してのユーザ認証を行なうための処理部である。マスタキー暗号処理部３７は、認証処理部３６および会員管理センター１２の管理サーバー６９による認証の結果が正統の場合に暗号処理部３３において使用された可変長データと自然乱数（複数の場合にはその使用順の情報を含む）を伝送マスタキーとし、これを当該ユーザに固有の鍵に基づいて暗号化するとともに、その暗号化により得られた情報を通知情報として通信制御部３５から当該ユーザのパソコン１４に対して送信するものである。暗号化にはＳＸＡＬ／ＭＢＡＬ（後述する）を用いる。

【０１２８】

会員管理センター１２には、会員となっているユーザのＩＤやユーザ認証のための種々の会員情報がユーザ毎に分類して格納されているデータベース７０が設置されている。管理サーバー６９は、このデータベース７０にアクセスして格納情報を検索してユーザ認証を行ない、その結果をインターネット１３を経由して通信制御部３０を介して認証処理部３６へ送信する。

【０１２９】

ユーザのパソコン１４には、制御中枢としてのＣＰＵ６０，プログラムが格納されているＲＯＭ６１，ＣＰＵ６０のワーキングエリアとしてのＲＡＭ６２、ならびに電気的に記憶データの消去が可能なＥＥＰＲＯＭ６３が設けられている。さらに、外部との信号の整合性をとるための入出力インターフェイス６４が設けられている。なお、クロック発生回路，アドレスデコード回路，パワーオンリセット回路等は図示を省略している。

【０１３０】
入出力インターフェイス６４には、カードリーダライタ６６が接続されており、ユーザのＩＣカード６５との信号のやり取りがこのカードリーダライタ６６，入出力インターフェイス６４を介してＣＰＵ６０との間で行なわれる。入出力インターフェイス６４にはフロッピー（登録商標）ディスクリーダライタ６７が接続されており、フロッピー（登録商標）ディスクに対する情報の読取および書込が可能となる。
【０１３１】
入出力インターフェイス６４にはハードディスクリーダライタ６８が接続されており、ハードディスクに対する情報の読取および書込が可能となる。入出力インターフェイス６４にはキーボード５３が接続されており、ユーザがキーボード５３を操作することによりその操作信号が入出力インターフェイス６４を介してＣＰＵ６０へ入力される。入出力インターフェイス６４にはＣＲＴ５２が接続されており、ＣＲＴ表示用制御信号がＣＰＵ６０から入出力インターフェイス６４を介してこのＣＲＴ５２へ与えられる。入出力インターフェイス６４にはＣＤ－ＲＯＭリーダ６８ａが接続されており、ＣＤ－ＲＯＭ６８ｂの記録情報が読取可能となる。このＣＤ－ＲＯＭ６８ｂには、前述したユーザエージェント２６が記録されている。ユーザエージェント２６は、このＣＤ－ＲＯＭ６８ｂに記録された状態でエージェント製造業者からユーザに販売される。なお、ユーザエージェント２６の販売は、ＣＤ－ＲＯＭ６８ｂに記録させた形での販売に代えて、エージェント製造業者がインターネット１３を経由してオンラインによりユーザエージェント２６を配信して販売してもよい。
【０１３２】
図１４は、ユーザが所有するＩＣカード６５の制御回路および記憶データを示す図である。ＩＣカード６５には、制御中枢としてのＣＰＵ９１と、制御用のプログラムを記憶しているＲＯＭ９２と、ＣＰＵ９１のワーキングエリアとしてのＲＡＭ９３と、電気的に記憶データの消去が可能なＥＥＰＲＯＭ９４と、外部との信号の入出力を行なうためのＩ／Ｏポート９０とが設けられている。ＲＯＭ９２には、ＩＣカード６５のためのＯＳ（オペレーティングシステム）が記憶されている。このＯＳは、事実上の世界標準であるたとえばＭＵＬＴＯＳ（マルチ・アプリケーションＩＣカードの汎用オペレーティング・システム）等のＩＣカード汎用ＯＳを用いるのが望ましい。
【０１３３】
そして、たとえばＥＥＰＲＯＭ９４には、必要に応じて各種のアプリケーションソフト９５が記憶される。アプリケーションソフトとしては、たとえば、クレジット，デビット（預金自動引き落し），モンデックス，アクセス制御等の各種ソフトや、電子認証書，エージェント用知識データ，電子カルテ等の各種データが考えられる。これら各種アプリケーションソフトは、必要に応じて他の種類のアプリケーションソフトに書換えられるように構成されている。
【０１３４】
エージェント用知識データ９６としては、秘密性を要しない公表可能情報ＮＳＩと、秘密性を要する秘密情報ＳＩとに分類されて記憶されている。公表可能情報ＮＳＩとしては、たとえば、ユーザの職業，趣味，住所，音楽の好み，映画の好み，…ユーザの公開鍵ＰＫＵ等である。秘密情報ＳＩとしては、たとえば、ユーザの年収，電話番号，異性の好み，学歴，貯蓄額，財産，…ユーザの秘密鍵ＳＫＵ等が考えられる。この秘密情報ＳＩは、ユーザ固有の秘密鍵であるＳＫ１により暗号化された状態で記憶されている。
【０１３５】
ユーザは、自己のユーザエージェント２６を利用する場合には、たとえばＣＤ－ＲＯＭ６８ｂに記録されているユーザエージェントをＣＤ－ＲＯＭリーダ６８ａで読取らせ、さらに自己が所有しているＩＣカード６５をパソコン１４のＩＣカード挿入口５０に挿入して、エージェント用知識データ９６を読取らせ、ユーザエージェント９６にエージェント用知識データ９６を保有させた状態で、ユーザエージェント２６を動作させる。このユーザのプロフィール情報９６は、転職や引っ越し等があればユーザが職業や住所等を書換え

て更新する操作を行なう。また、ユーザエージェント２６は、ユーザのために仕事を行ないその結果をユーザに提供するのであり、その提供された結果に対するユーザの反応（満足するかまたは不満に思うか等）を観察し、必要があればユーザエージェント２６自身がユーザのプロフィール情報９６を更新したり補充したりする。その結果、ユーザエージェント２６をユーザが活用すればするほどユーザのプロフィール情報９６がユーザに適した内容のものとなり、ユーザエージェント２６を活用すればするほどユーザの満足のいく仕事を行なうものとなる。

【０１３６】

さらに、ユーザエージェント２６が、仕事の結果を提供したユーザの反応（満足するかまたは不満に思うか等）を観察し、ユーザのプロフィール情報９６ばかりでなく、ユーザエージェント２６自身のプログラムを改良するといういわゆる機械学習を応用したものである場合には、ユーザエージェント２６を、ＥＥＰＲＯＭ６３等の情報の書換えが可能な記憶媒体に記憶させておく必要がある。

【０１３７】

また、図１４に示したユーザのプロフィール情報９６は、どのアドレスにどの種類のプロフィール情報が記憶されているかあるいはどのようなデータ構造で記憶させるか等が、世界的規模で統一化されたフォーマットに従っている。

【０１３８】

図１５は、前述したＳＸＡＬ／ＭＢＡＬの概要を示す説明図である。

図示の例では、平文データである２０バイトの可変長データを８バイト（６４ビット）の暗号鍵Ｋを用いて暗号化して２０バイトの可変長暗号列を求める。図中、Ｐ，Ｅ，Ｆ，Ｇ，Ｈ，Ｉ，Ｃは各変換過程におけるデータであり、その添字はバイト数を表わしている。また、ｆｍは暗号関数である。

【０１３９】

図１５を参照して、まず、可変長データＰの左端の８バイトと拡大鍵ＫＯとの排他的論理和（イクスクルーシブオア）を判定し、判定結果を関数ｆｍによりデータ変換する。次に両端の各４バイトを合せてＳＸＡＬによりデータ変換し、残りはそのままとする。続いてデータの順番を逆にし、暗号関数ｆｍによりデータ変換した後、データの順番を逆にする。これを暗号関数ｆｍによりデータ変換し、変換後のデータの左端の８バイトと拡大鍵ＫＩとの排他的論理和（イクスクルーシブオア）を判定し、暗号化された可変長暗号列Ｃを求める。

【０１４０】

本実施の形態では、前記暗号アルゴリズムが、１６バイト以上のデータまたはファイルを１単位として暗号化するためメガバイト級の大容量毎の暗号化が可能な点、前述のように双方向のデータ入換えを複数回実施して暗号化するから解読が著しく困難となる点、および情報伝達形態において１ビット程度のビット化けやデータ改ざんに遭遇した場合にすべての情報の正常復号が不可能となる点に着目して、これを大容量情報の高速伝達を行なう場合のセキュリティ確保に用いるようにしたものである。特に、１ビット程度のビット化けやデータ改ざんに遭遇した場合、ＤＥＳ型の暗号アルゴリズムでは、復号の際にビット化けや改ざん部分の近辺またはその部分以外のみが正常に復号されないため、受信側での異常感知が著しく困難となる。これに対し、ＳＸＡＬ／ＭＢＡＬでは、すべての部分が異常情報に変わるためその感知が極めて容易であり、通信中の場合は再送要求、ファイルの場合は保管中のバックアップファイルを使用するなど、迅速な対応が可能となる。

【０１４１】

図１６は、図１３に示した送信装置３の動作を示すフローチャートである。ＳＦ１により、コンテンツの送信指令があったか否かの判断がなされ、ない場合にはＳＦ１４に進み、ユーザ認証処理を行なった後ＳＦ１へ戻る。このＳＦ１，ＳＦ１４のループの巡回途中で、前述したようにテレスクリプト・エンジン１８からコンテンツの送信指令があった場合には、ＳＦ２に進み、その指令されたコンテンツが既に放送予定となっているコンテンツであるか否かの判断がなされる。既に放送予定となっているコンテンツの場合には、放

送日時とチャンネルが放送局２からコンテンツ提供業者７へ送信されてきているために、その放送日時とチャンネルをユーザのパソコン１４へ送信した後ＳＦ１へ戻る。

【０１４２】

一方、送信指令を受けたコンテンツが未だに放送予定となっていない新たなコンテンツである場合にはＳＦ４へ進み、その選択されたコンテンツの送信単位、たとえば１フレームＦｓに対応する可変長データ（＇＇１１１…１＇＇）を生成する。次にＳＦ５へ進み、乱数発生装置４からたとえば２つの自然乱数（Ｒ１，Ｒ２）を取得して、暗号処理を行なう。具体的には可変長データを最初の自然乱数Ｒ１を鍵（暗号鍵）として前述したＳＸＡＬ／ＭＢＡＬにより暗号化し、初期乱数列ｋｄ０（図１５の下段の可変長暗号列Ｃに相当）を生成する。次に、ＳＦ７へ進み、初期乱数列ｋｄ０の該当バイトと基準論理値０１ｈとの排他的論理和（イクスクルーシブオア）判定により乱数列ＫＳ（＝ｋｄ１，ｋｄ２，…ｋｄｉ）を生成する。

【０１４３】

ここでｋｄ１はｋｄ０の１バイト目と０１ｈとの排他的論理和（イクスクルーシブオア）の判定結果、ｋｄ２はｋｄ０の２バイト目と０１ｈとの排他的論理和判定結果、…である。さらに乱数列ＫＳを次の自然乱数Ｒ２を鍵（暗号鍵）としてＳＸＡＬ／ＭＢＡＬにより暗号化し、新たな乱数列ＲＳ（＝ｒｄ１，ｒｄ２，…ｒｄｎ：可変長暗号列）を生成する（ＳＦ８）。ここでｒｄ１はｋｄ１の暗号処理結果、ｒｄ２はｋｄ２の暗号処理結果、ｒｄｎはデータ量調整されたデータｋｄｉの暗号結果、…である。

【０１４４】

次にＳＦ９へ進み、前述のようにして生成された乱数列ＲＳと送信単位Ｆｓとの排他的論理和条件を判定して伝送情報ＲＤｎを生成し、ＳＦ１０へ進み、生成された伝送情報ＲＤｎを放送局２へ送信する。放送局２では、伝送情報ＲＤｎを受信して、それをいつどのチャンネルで放送するかを決定し、その決定された放送日時とチャンネルをコンテンツ提供業者７へ返信してくる。その返信があればＳＦ１１によりＹＥＳの判断がなされてＳＦ１２へ進み、コンテンツＮＯ．毎に分類して放送日時，チャンネルを記憶する処理がなされる。次にＳＦ１３に進み、その放送日時とチャンネルをユーザのパソコン１４へ送信する処理がなされた後ＳＦ１へ戻る。

【０１４５】

図１７は、ユーザのパソコン１４によるコンテンツ再生処理動作を示すフローチャートであり、図３に示したＳ２０の具体的なフローチャートである。Ｓ２５により、可変長データと乱数（Ｒ１，Ｒ２）の記憶があるか否かの判断がなされる。この両データは、ユーザのパソコン１４を使用してユーザ認証が行なわれた結果適正である旨の判定がなされたことを条件として後述するようにコンテンツ提供業者７からユーザのパソコン１４へ送られてくるものである。この両データの記憶がない場合にはＳ２６へ進み、まずユーザ認証処理（図１８に基づいて後述する）を行なった後、Ｓ２７へ進む。

【０１４６】

Ｓ２７では、可変長データを最初の自然乱数Ｒ１によりＳＸＡＬ／ＭＢＡＬにより暗号化し、初期乱数列ｋｄ０を生成する。次に、Ｓ２８へ進み、初期乱数列ｋｄ０の該当バイトと基準論理値０１ｈとの排他的論理和（イクスクルーシブオア）判定により乱数列ＫＳ（＝ｋｄ１，ｋｄ２，…ｋｄｉ）を生成する。次にＳ２９へ進み、乱数列ＫＳを次の自然乱数Ｒ２を鍵としてＳＸＡＬ／ＭＢＡＬにより暗号化し、新たな乱数列ＲＳ（＝ｒｄ１，ｒｄ２，…ｒｄｎ）を生成する。前記初期乱数列ｋｄ０、乱数列ｋｓ，ｒｓは、それぞれ図１６に基づいて説明したものと同一のものである。

【０１４７】

このようにして生成された乱数列ＲＳと受信した伝送情報ＲＤｎとの排他的論理和条件を判定して送信単位Ｆｓを生成し（Ｓ３０）、コンテンツを再生する（Ｓ３１）。

【０１４８】

図１８は、ユーザ認証処理を示すフローチャートであり、前述したＳＦ１４，Ｓ２６の具体的な動作を示すフローチャートである。このフローチャートは、ユーザのパソコン１

４とコンテンツ提供業者７の通信装置３と会員管理センター１２の管理サーバー６９それぞれのフローチャートである。

【０１４９】

ユーザは、まず自己のＩＣカード６５をパソコン１４のＩＣカード挿入口５０へ挿入する。その状態で、ユーザが暗証番号等を入力してカード認証を行ない、そのカード認証の結果適正である旨の判定がなされたことを条件としてＳ３２の処理がなされる。Ｓ３２では、ＩＣカード６５に記憶されている会員ＩＤを読出し、その読出した会員ＩＤと選択されたコンテンツＮＯ．とをコンテンツ提供業者７の通信装置３へ送信する処理がなされる。通信装置３では、ＳＦ１５により、送信されてきたそれら情報を会員管理センター１２の管理サーバー６９へ中継して送信する処理が行なわれる。管理サーバー６９では、ＳＨ１により、データベース７０に格納されている会員管理用の情報を参照して送られてきた会員ＩＤを確認し、適正である旨の確認が行なわれたことを条件として乱数を生成してチャレンジコードＣＣとして送信する処理がなされる。

【０１５０】

コンテンツ提供業者７の通信装置３では、ＳＦ１６により、そのチャレンジコードＣＣを中継してユーザのパソコン１４へ送信する。ユーザのパソコン１４では、Ｓ３３により、ＩＣカード６５内に記憶されているユーザのネットキーＳＫを呼出し、それを鍵を使用してレスポンスコードＲＣを生成して返信する処理がなされる。この処理は、$RC=E_{SK}(CC)$を演算し、その演算結果を返信する処理である。

【０１５１】

コンテンツ提供業者７の通信装置３では、そのレスポンスコードＲＣをＳＦ１７により中継して会員管理センター１２の管理サーバー６９に伝送する処理がなされる。

【０１５２】

管理サーバー６９では、ＳＨ２により、その送信されてきたレスポンスコードＲＣに基づいてユーザの本人認証を行なって確認し、適正である旨の確認ができればその旨をコンテンツ提供業者７の通信装置３へ返信する処理がなされる。このＳＨ２の処理は、具体的には、$RC=D_{SK}(CC)$が成立するか否かに基づいて行なう。なお、ネットキーＳＫは、会員管理センター１２のデータベース７０に会員のＩＤ毎に分類して格納されており、管理サーバー６９が会員ＩＤに相当するＳＫを検索してそれを用いてユーザ認証を行なう。

【０１５３】

ユーザ認証の確認情報を受取ったコンテンツ提供業者７の通信装置３では、ＳＦ１８により、ユーザが希望するコンテンツに対応する可変長データＫＨと乱数（Ｒ１，Ｒ２）をユーザのネットキーＳＫで暗号化して秘匿した形態でユーザのパソコン１４へ転送する処理がなされる。ユーザのパソコン１４では、Ｓ３４により、その転送されてきた情報をネットキーＳＫにより復号化し、可変長データＫ１と乱数（Ｒ１，Ｒ２）とを再生して記憶する処理がなされる。このＫ１と乱数（Ｒ１，Ｒ２）とが前述した図１７に示したＳ２７以降の処理に利用される。

【０１５４】

図１９は、たとえば有料コンテンツを購入したユーザが、他のユーザにそのコンテンツを複製して配布するという不正コピーを防止するための制御回路である。この制御回路は、たとえばユーザのパソコン１４に内蔵されている。コンテンツ提供業者７が提供する有料コンテンツあるいは放送局２が放送する有料番組をユーザのパソコン１４が受信してそのコンテンツをハードディスク８１等に記録させる。前述したように、有料コンテンツの場合には、一般的に暗号化されたデータとして転送されてくるために、その転送データをそのまま暗号化された状態でパソコン１４がハードディスク８１に記録する。このハードディスク８１から読出された情報は、図１７で説明したように、所定の復号化手段８１ａにより復号化され、コンテンツが再生される。

【０１５５】

この復号化された後のコンテンツには、いわゆる電子透かし技術により、制御信号ＣＣ

Ｓ（Copy Control Signal）を透かし情報として埋込んでいる。一般的に、透かし情報は、ＭＥＰＧ２による復号化を行なうことにより読出すことができる。この復号手段８１ａにより復号化されたコンテンツデータがＭＰＥＧ２復号化器８２に入力され、復号化された情報を電子透かし検出器８３に入力することにより、透かし情報である制御信号ＣＣＳを検出することができる。そしてその電子透かし検出器８３により検出されたＣＣＳがＡＰＳ８６に入力される。このＡＰＳは、たとえば米Macrovision Corp. が開発したAnalog Protection Systemであり、複製防止処理を行なうものである。

【０１５６】

電子透かし検出器８３からグラフィックス・モジュール８４に、透かし情報を含むコンテンツデータが与えられ、グラフィックス・モジュール８４からコンテンツデータがＮＴＳＣ（National Tetevison System Committee）符号化器８５に与えられ、ＮＴＳＣ信号に変換される。そしてＮＴＳＣ信号がパソコン１４のＣＲＴ５２，ＴＶ１６，ＶＴＲ１５等に供給される。

【０１５７】

ＡＰＳ８６に与えられるＣＣＳは、たとえば、「コピー禁止」や「１度だけコピー可能」などのコピー制御信号であり、この信号に従ってＡＰＳ８６が動作してＣＣＳのデータ内容どおりのコピー禁止等の制御を行なう。

【０１５８】

図２０は、コンテンツ提供業者７と第三者機関８あるいは放送局２と番組関連データ制作者１１との間での情報のやり取りを無線系メディアを用いて行なう例を示す説明図である。この図２０は、いわゆるワイヤレス・ローカル網ＷＬＬ（Wireless Local Loop）を利用したものを示している。コンテンツ提供業者７，第三者機関８，放送局２，番組関連データ制作者１１には、それぞれ、無線装置７１，７２，７４，７５が設けられている。そして、前述したように、第三者機関８とコンテンツ提供業者７との間での、ユーザエージェント２６，有料コンテンツ，第三者機関エージェント２９等の伝送を、このＷＬＬを利用して行なう。図中７６，７７，７８，７９，８０はＷＬＬ用のアンテナである。

【０１５９】

また、放送局２と番組関連データ制作者１１との間での、番組関連データの伝送等も、ＷＬＬを利用して行なう。なお、１は衛星、５は衛星用のアンテナである。

【０１６０】

第三者機関８とコンテンツ提供業者７との間での情報のやり取りは、多数のユーザエージェントや多数の第三者機関エージェントや多数のコンテンツが比較的大量に集まって送受信されるために、そのような大量のデータをこのＷＬＬを利用して送受信することにより、効率的に送受信できる利点がある。

【０１６１】

図２１は、不正コピー防止のための他の例を示す制御回路図である。この制御回路も、たとえばユーザのパソコン１４に内蔵されている。ユーザのパソコン１４で受信した暗号化されたコンテンツデータは前述したようにハードディスク８１に記録される。この暗号化コンテンツデータ内には、その暗号化コンテンツを復号化するための前述した可変長データＫ１，乱数Ｒ１，Ｒ２が前述したユーザのネットキーＳＫで暗号化された状態で、透かし情報として組込まれている。

【０１６２】

ハードディスク８１に記録されているこのような暗号化コンテンツデータがＭＰＥＧ２復号化器８２に入力され、そこで復号化されて透かし情報が検出可能な状態に変換され、そのデータが電子透かし検出器８３に入力され、透かし情報であるE_{SK}（Ｋ１，Ｒ１，Ｒ２）が検出されてパソコン１４のＣＲＴ５２，ＴＶ１６に入力される。一方、電子透かし検出器８３からの暗号化コンテンツデータがグラフィックス・モジュール８４を経由してＮＴＳＣ符号化器８５に入力され、ＮＴＳＣ信号としてＣＲＴ５２，ＴＶ１６，ＶＴＲ１５に与えられる。このＮＴＳＣ信号は、暗号化されたコンテンツデータのＮＴＳＣ信号であるために、このＮＴＳＣ信号に基づいてそのままＣＲＴ５２，ＴＶ１６等により放映し

たとしても、暗号化されたデータに従った映像しか放映されず、ユーザが何ら認識できない映像となる。

【０１６３】

そこで、たとえばユーザのパソコン１４のＩＣカード挿入口５０にユーザのＩＣカード６５を挿入することにより、そのＩＣカード６５に記憶されているユーザのネットキーＳＫがパソコン１４により読取られ、パソコン１４に入力されたE_{SK}（Ｋ１，Ｒ１，Ｒ２）をユーザのネットキーＳＫより符号化してＫ１，Ｒ１，Ｒ２を再生し、それらデータを用いてＮＴＳＣ信号を復号化して通常のコンテンツデータに対するＮＴＳＣ信号に変換し、それに基づいてＣＲＴ５２により映像を表示するように制御する。

【０１６４】

ＴＶ１６にもＩＣカード挿入口を形成し、そこにＩＣカード６５を挿入することにより、前述と同様にＴＶ１６によりＮＴＳＣ信号を復号化して通常のコンテンツデータに対するＮＴＳＣ信号に変換して放映する。

【０１６５】

このように構成することにより、有料コンテンツを正規に購入したユーザのＩＣカード６５を、パソコン１４あるいはＴＶ１６に挿入しない限り、有料コンテンツを再生して放映することができない。なお、ＶＴＲ１５には、ＩＣカード挿入口が形成されていないため、ＶＴＲ１５に記録されるデータは暗号化されたコンテンツに対するＮＴＳＣ信号となる。そしてこのＶＴＲ１５に記録されている暗号化されたコンテンツに対するＮＴＳＣ信号をＣＲＴ５２あるいはＴＶ１６により再生する際には、ＩＣカード６０を挿入して前述したように復号化して再生閲覧する。

【０１６６】

この図２１に示す別実施の形態により、ＴＶ１６でコンテンツを再生する場合には、ＴＶ１６に図１７に示したコンテンツ再生処理の機能が内蔵されることとなる。また、ＣＲＴ５２によりコンテンツを再生する場合には、パソコン１４のＩＣカード挿入口５０にＩＣカード６５を挿入して再生するのであるが、図２１に示すように、ＮＴＳＣ符号化器８５からＣＲＴ５２に供給されたＮＴＳＣ信号に対し復号化を行なうようにし、パソコン１４内でＮＴＳＣ信号が復号化されてその復号化されたＮＴＳＣ信号がたとえばＴＶ１６やＶＴＲ１５に出力できないように構成されている。

【０１６７】

また、この図２１に示す別実施の形態では、図１８に示したユーザ認証処理を行なって適正なユーザである旨の認証が行なわれた後、可変長データＫ１と乱数（Ｒ１，Ｒ２）とをユーザのネットキーＳＫで暗合化したデータを暗号化コンテンツデータに透かし情報として組込んでその情報を放送局２等を経由してユーザのパソコン１４に転送するようにする。

【０１６８】

図２２～図２４は、図１６～図１８に示した制御動作の他の例を示す図である。

図２２は、コンテンツ提供業者７の通信装置３の動作を示すフローチャートであり、図１６と対応している。ＳＦ１９により、コンテンツの送信指令があったか否かの判断がなされ、ない場合にはＳＦ１９ａに進み、ユーザ認証処理を行なった後ＳＦ１９へ戻る。

【０１６９】

テレスクリプト・エンジン８１からコンテンツの送信指令があった場合にはＳＦ２０へ進み、既に放送予定となっているコンテンツであるか否かの判断がなされ、放送予定となっているコンテンツである場合にはＳＦ２１へ進み、放送日時とチャンネルをパソコン１４へ送信してＳＦ１９へ戻る。一方、未だに放送予定となっていない新しいコンテンツについて送信指令があった場合にはＳＦ２２へ進み、ユーザの秘密鍵ＳＫＵと同じビット数の乱数ＲＮを生成する処理がなされる。一般的にＲＳＡ等の公開鍵暗号方式で用いられる秘密鍵のビット数は、１０２４ビットであるために、このＳＦ２２で生成される乱数ＲＮも１０２４ビットになる可能性が高い。

【０１７０】

次にＳＦ２３へ進み、選択されたコンテンツをユーザの秘密鍵ＳＫＵと同じビット数（たとえば１０２４ビット）ずつに分割して分割コンテンツＡ（＝Ａ１，Ａ２，…Ａｎ）を生成する処理がなされる。ＳＫＵと同じビット数に分割した場合には、コンテンツに端数が生ずるのが一般的である。その場合には、最後の分割コンテンツＡｎがＳＫＵのビット数よりも少ないビット数のデータとなる。次にＳＦ２４へ進み、分割コンテンツＡとＳＦ２２により生成された乱数ＲＮとの排他的論理和（イクスクルーシブオア）を演算する。図２２～図２４ではイクスクルーシブオアとして○の中に＋が描かれた記号を用いているが、明細書では（＋）の記号を用いる。ＳＦ２４の具体的演算内容は、分割コンテンツＡ１，Ａ２，…Ａｎのそれぞれと乱数ＲＮとのイクスクルーシブオアを計算するものである。次にＳＦ２５へ進み、ＳＦ２４による演算結果Ａ（＋）ＲＮを放送局２へ送信する処理がなされる。これを受けた放送局２は、Ａ（＋）ＲＮを放送する日時とチャンネルを決定し、その決定された放送日時とチャンネルをコンテンツ提供業者７に返信する。その返信があれば、ＳＦ２６によりＹＥＳの判断がなされてＳＦ２７へ進み、コンテンツＮＯ．毎に分類して放送日時とチャンネルを記憶する処理がなされ、ＳＦ２８に進み、その放送日時とチャンネルをパソコン１４へ送信する処理がなされた後ＳＦ１９へ戻る。

【０１７１】

なお、ＳＦ２４の最後のＡｎ（＋）ＲＮは、分割コンテンツデータＡｎが端数の関係上ＳＫＵよりも少ないビット数の分割コンテンツである場合には、乱数ＲＮの先頭から分割コンテンツＡｎのビット数だけのデータを取出し、そのデータとＡｎのイクスクルーシブオアを演算する。

【０１７２】

図２３は、ＳＦ１９ａおよび後述するＳ３６に示されたユーザ認証処理の具体的動作を示すフローチャートであり、図１８と対応している。

【０１７３】

まずユーザが自己のＩＣカード６５をパソコン１４のＩＣカード挿入口５０に挿入して前述と同様にカード認証を行ない、適正である旨の認証が行なわれたことを条件としてＳ３８により、挿入されたＩＣカード６５に記憶されているユーザのＩＤが読取られてその会員ＩＤと選択されたコンテンツＮＯ．とがコンテンツ提供業者７の通信装置３へ送信される。通信装置３では、その送信されてきた情報をＳＦ１９により中継して会員管理センター１２の管理サーバー６９に伝送する。管理サーバー６９では、ＳＨ３により、データベース７０にアクセスして送られてきた会員ＩＤを確認して適正であるか否かの判断を行ない、適正である旨の確認をした後乱数を生成してチャレンジコードＣＣを通信装置３へ送信する。

【０１７４】

通信装置３では、その送信されてきたチャレンジコードＣＣをＳＦ２０により中継してユーザのパソコン１４へ送信する。ユーザのパソコン１４では、Ｓ３９により、ＩＣカード内のネットキーＳＫを読出し、そのＳＫを鍵としてレスポンスコードＲＣを生成して返信する処理がなされる。つまり、$RC = E_{SK}(CC)$を演算して返信する。通信装置３では、その返信されてきたＲＣをＳＦ２１により中継して管理サーバー６９に送信する処理が行なわれる。管理サーバー６９では、ＳＨ４により、その送信されてきたレスポンスコードＲＣに基づいてユーザの本人認証を行ない適正である旨の認証が行なわれたことを確認した場合にその旨を返信する処理がなされる。つまり、ＳＨ４では、$CC = D_{SK}(RC)$が成立するか否かを判断してユーザの本人認証が行なわれる。

【０１７５】

通信装置３では、ユーザの本人認証の確認情報を受取れば、選択されたコンテンツをＳＦ２３同様に分割し、分割コンテンツＡ（＝Ａ１，Ａ２，…Ａｎ）を管理サーバー６９へ送信する処理がなされる。管理サーバー６９では、ＳＨ５により、

ＳＫＵ（＋）｛Ｉ１（＋）（Ａ１（＋）ＲＮ）｝＝Ａ１

ＳＫＵ（＋）｛Ｉ２（＋）（Ａ２（＋）ＲＮ）｝＝Ａ２

ＳＫＵ（＋）｛Ｉｎ（＋）（Ａｎ（＋）ＲＮ）｝＝Ａｎ

を満たすＩ（＝Ｉ１，Ｉ２，…Ｉｎ）を演算して、E_{SK}（Ｉ）を通信装置３へ送信する処理がなされる。

【０１７６】

ここで、Ｉ１，Ｉ２，…Ｉｎは、それぞれ、Ａ１，Ａ２，…Ａｎの分割コンテンツのビット数と同じビット数（たとえば１０２４ビット）のデータである。なお、端数の関係上Ａｎが通常より少ないビット数であった場合には、ＩｎもＡｎに合せた少ないビット数となる。このＩ１，Ｉ２，…Ｉｎの算出は、比較的簡単に行なえ得る。たとえば、ＳＫＵとＡ１とＲＮとの最上位ビットがともに「１」であった場合には、

１（＋）｛Ｉ１の最上位ビット（＋）（１（＋）１）｝＝１

となり、Ｉ１の最上位ビットは自ずと「０」となる。また、ＳＫＵの最上位ビットの次のビットが０で、Ａ１とＲＮとの最上位ビットの次のビットがともに１であった場合には、

０（＋）｛Ｉ１の最上位ビットの次のビット（＋）（１（＋）１）｝＝１

となり、Ｉ１の最上位ビットの次のビットは自ずと「１」となる。

【０１７７】

通信装置３では、E_{SK}（Ｉ）を受けてＳＦ２３により中継してユーザのパソコン１４へ送信する処理がなされる。ユーザのパソコン１４では、Ｓ４０により、受信した情報を鍵ＳＫにより復号化する処理、すなわち、T_{SK}｛E_{SK}（Ｉ）｝を演算してＩを再生して記憶する処理がなされる。なお、この別実施の形態では、会員管理センター１２のデータベース７０に、会員のＩＤごとに分類して会員（ユーザ）の秘密鍵ＳＫＵが格納されている。この秘密鍵ＳＫＵは、秘密性が保持可能な状態でデータベース７０に格納されており、会員管理センター１２のある限られたオペレータのみが管理サーバー６９によりＳＫＵにアクセスできるように構成されている。

【０１７８】

図２４は、ユーザのパソコン１４の動作を示すフローチャートであり、図１７に示したフローチャートに対応したものである。まずＳ３５により、Ｉ（＝Ｉ１，Ｉ２，…Ｉｎ）を記憶しているか否かの判断がなされる。図２３に示したユーザ認証が終了した段階ではＩがユーザのパソコン１４により記憶されているために（Ｓ４０参照）、Ｓ３５によりＹＥＳの判断がなされてＳ３７に進むが、まだＩが記憶されていない場合にはＳ３６に進み、図２３に示したユーザ認証処理が行なわれた後Ｓ３７へ進む、

Ｓ３７では、

Ａ＝ＳＫＵ（＋）｛Ｉ１（＋）（Ａ１（＋）ＲＮ｝
＋ＳＫＵ（＋）｛Ｉ２（＋）（Ａ２（＋）ＲＮ｝
＋ＳＫＵ（＋）｛Ｉ３（＋）（Ａ３（＋）ＲＮ｝
：
＋ＳＫＵ（＋）｛ＩＮ（＋）（ＡＮ（＋）ＲＮ｝

を演算して、コンテンツを再生する処理がなされる。

【０１７９】

この別実施の形態では、Ｓ３７で示したように、コンテンツＡを再生するには、当該ユーザの秘密鍵であるＳＫＵが必要となる。つまりこのユーザの秘密鍵ＳＫＵを用いて暗号化コンテンツを復号化する処理がコンテンツＡを再生するのに必須の処理となっている。その結果、暗号化コンテンツを正規に購入したユーザ以外のユーザが暗号化コンテンツを復号化してコンテンツＡを再生するためには、当該暗号化コンテンツを購入した正規のユーザの秘密鍵ＳＫＵを用いて暗号化コンテンツを復号化せざるを得ず、正規のユーザからＩＣカード６５を入手しなければコンテンツＡを得ることはできない。ゆえに、セキュリティが向上する。

【０１８０】

この図２２～図２４の別実施例を別の表現で簡単に説明すれば、以下のようなものとなる。

【０１８１】

コンテンツ提供業者７が作成したコンテンツをＡとし、コンテンツ提供業者７は、その有料コンテンツＡを乱数等からなる鍵ＲＮにより暗号化してE_{RN}（Ａ）を演算してそれを放送局２から放送してもらう。またコンテンツ提供業者７は、D_{SKU}［D_I｛E_{RN}（Ａ）｝］＝Ａを満たす鍵Ｉを生成し、それを鍵ＳＫで暗号化してインターネット１３等を経由してユーザのパソコン１４へ送信する。

【０１８２】

ユーザは、放送局２から受信したE_{RN}（Ａ）をコンテンツ提供業者７から受信して再生した鍵Ｉで復号化し、さらにそれを自分の秘密鍵ＳＫＵで復号化する。その結果、コンテンツＡを得ることができる。

【０１８３】

なお、このようなＲＮやＩやＳＫＵ等の鍵を用いて暗号化，復号化するアルゴリズムを、ＲＳＡ公開鍵暗号方式やいわゆる楕円曲線暗号のアルゴリズムを用いれば、D_I｛E_{RN}（Ａ）｝＝E_{PKU}（Ａ）が成立する。ゆえに、この式を満たすＩをコンテンツ提供業者７が算出してそれをユーザのパソコン１４に送信すれば事足りることとなり、Ｉを生成するのにユーザの公開鍵ＰＫＵで事足りユーザの秘密鍵ＳＫＵを必要としないこととなる。

【０１８４】

次に、以上説明した実施の形態の変形例や特徴点等を以下に列挙する。

（１）　前述した実施の形態では、ＣＭ制作者１０が制作したＣＭに対し番組関連データ制作者１１が制作した番組関連データを重合させて放送し、番組の合間に挿入されているＣＭをユーザがカットして番組の部分のみを閲覧する不都合を防止するためのＣＭカット閲覧防止システムの発明が開示されている。

【０１８５】

この発明は、ユーザに閲覧を希望させるためのコンテンツの合間にコマーシャルメッセージを挿入して宣伝を行なう宣伝システム（宣伝方法）を発明の属する技術分野とする。

【０１８６】

従来から一般的に知られている宣伝システム（宣伝方法）は、テレビ番組等の合間にコマーシャルメッセージ（ＣＭ）を挿入して放送局から放送し、ユーザがその放送を受信してＴＶ（テレビジョン）で放映してＣＭを閲覧することにより、ＣＭのスポンサーの宣伝やスンポンサーの商品の宣伝を行なうものがあった。

【０１８７】

一方、近年、ユーザの家庭にはＶＴＲ（ビデオテープレコーダ）が普及しており、放送局が放送したＣＭを含む番組を一旦このＶＴＲ等に記録させ、後日それを再生してＴＶやパソコン等で閲覧するという記録再生閲覧が増えてきた。

【０１８８】

その結果、番組の合間に挿入されているＣＭはユーザにしてみれば贅肉に相当する部分であるために、そのＣＭ部分のみをカットして番組部分のみを再生して閲覧するというＣＭカット閲覧が増えることが予想される。

【０１８９】

このようなＣＭカット閲覧が増えた場合には、民放番組のスポンサーがＣＭによる利益を見込めなくなり、スンポンサーによって成り立っている民放が崩壊するおそれがある。

【０１９０】

つまり、従来の宣伝システム（宣伝方法）においては、ユーザに閲覧を希望させるためのコンテンツの合間に挿入されたコマーシャルメッセージのみをユーザがカットしてコンテンツのみを閲覧するために、コマーシャルメッセージの挿入による利益が見込めなくなるという欠点があった。

【０１９１】

この宣伝システムの発明は、かかる実情に鑑み考え出されたものであり、その目的は、ユーザによる前述したＣＭカット閲覧を極力防止することである。

【０１９２】

この目的を達成するための手段として、この宣伝システムの発明は、

ユーザに閲覧を希望させるためのコンテンツの合間にコマーシャルメッセージを挿入して宣伝を行なう宣伝システムであって、
前記コマーシャルメッセージが挿入される対象となる前記コンテンツに関連するコンテンツ関連情報を制作する制作者によって制作されたコンテンツ関連情報を前記コマーシャルメッセージと同時に放映する同時放映手段を含むことを特徴とする。

【０１９３】

このような手段を採用した結果、コマーシャルメッセージと同時にそのコマーシャルメッセージが挿入されたコンテンツに関連するコンテンツ関連情報が放映される。コンテンツに興味のあるユーザはそのコンテンツ関連情報をも閲覧を希望するために、コンテンツ関連情報を閲覧すれば同時にコマーシャルメッセージも閲覧する結果となる。ゆえに、コマーシャルメッセージをカットしてコンテンツのみを閲覧することが極力防止できる。

【０１９４】

前記同時放映手段は、前記コマーシャルメッセージが挿入される対象となる前記コンテンツ（番組）に関連するコンテンツ関連情報（番組の意見交換用のホームページや番組の重要なポイントに注意を促すメッセージや番組内に登場する専門用語の解説等）を制作する制作者（番組関連データ制作者１１）によって制作されたコンテンツ関連情報を前記コマーシャルメッセージと重合させる重合手段（ＳＥ１，ＳＥ２）と、該重合手段により前記コンテンツ関連情報が重合されたコマーシャルメッセージを前記コンテンツの合間に放映する放映手段（ＳＥ３，ＳＤ３～ＤＳ９，放送局２，パソコン１４あるいはＴＶ１６）とを含んでいる。

【０１９５】

前記重合手段は、たとえばテレビ番組の放映中に地震等が発生した旨の臨時ニュースのメッセージを文字情報として表示させるという従来から周知の文字作成装置等の重合手段を用いればよい。なお、前記重合手段は、前述した本実施の形態では、ＣＭ制作者１０の所に設けられたものを示したが、その代わりに、放送局２に設けてもよい。その場合には、番組関連データ制作者１１が制作した番組関連データをインターネット１３を経由して放送局２に送信し、放送局２において放送するコマーシャルメッセージにその番組関連データを重合させて放送する。

【０１９６】

また、前述したコマーシャルメッセージカット閲覧を防止する目的を達成する発明として、次のような手段を有するものであってもよい。

【０１９７】

ユーザに閲覧を希望させるためのコンテンツの合間にコマーシャルメッセージを挿入して宣伝を行なう宣伝方法であって、
前記コマーシャルメッセージが挿入される対象となる前記コンテンツに関連するコンテンツ関連情報を生成するコンテンツ関連情報生成ステップと、
該コンテンツ関連情報生成ステップにより生成された前記コンテンツ関連情報と前記コマーシャルメッセージとを重合させる重合ステップと、
該重合ステップにより前記コンテンツ関連情報が重合した前記コマーシャルメッセージを前記コンテンツの合間に放映する放映ステップとを含むことを特徴とする、宣伝方法。

【０１９８】

前述した番組関連データ制作者１１が図１２に示すような番組関連データを制作する説明部分により、前記コンテンツ関連情報生成ステップが構成されている。前記ＳＥ２により、前記重合ステップが構成される。前記ＳＥ３，ＳＤ３～ＳＤ９，放送局２，前記Ｓ１３～Ｓ１６により、前記放映ステップが構成される。

【０１９９】

（２）　前述した本実施の形態では、ユーザが好むと思われるコマーシャルメッセージを検索してそのユーザに放映閲覧させるという発明が開示されている。この発明は、コマーシャルメッセージによりユーザに対し宣伝を行なう宣伝システム（宣伝方法）を発明の属する技術分野とする。

【０２００】
この種の宣伝システム（宣伝方法）において、従来から一般的に知られてるものに、たとえば、民放の番組に対するスポンサーのためのコマーシャルメッセージをＣＭ制作者が制作し、その制作されたコマーシャルメッセージが放送局に提供されて番組の合間に挿入された状態で放送される。ユーザは、放送番組の中から閲覧を希望する放送を受信してＴＶやパソコン等により閲覧をし、その閲覧途中で挿入されたコマーシャルメッセージが放映されることにより、ユーザに対しスポンサーの宣伝を行なっていた。
【０２０１】
しかし、この種の従来の宣伝システム（宣伝方法）では、ＣＭ制作者が一方的にスポンサーのＣＭを作成してユーザが好むと好まざるとにかかわらず一方的に制作されたＣＭを放送局から放送していた。その結果、ユーザにしてみれば、全く興味のない商品のＣＭや自分にほとんど無関係なＣＭを閲覧する状態となる。たとえば、アルコールを受けつけないユーザに対しビールの宣伝をしたところでユーザにとって全く無駄であるばかりでなくスポンサー側にとっても全く効果のないＣＭとなってしまう。このように、従来の宣伝システム（宣伝方法）は、ユーザ側およびスポンサー側双方にとって無駄の多い利益の少ないものとなってしまうという欠点があった。
【０２０２】
本発明は、かかる実情に鑑み考え出されたものであり、その目的は、宣伝者側およびユーザ側の双方における無駄を極力防止することである。
【０２０３】
この目的を達成する手段として、この発明は、コマーシャルメッセージによりユーザに対し宣伝を行なう宣伝システムであって、
ユーザを複数種類の属性毎に分類し、その分類毎に当該分類に属するユーザのみをターゲットにして制作されたコマーシャルメッセージを格納するコマーシャルメッセージ格納手段と、
ユーザのプロフィール情報を知識として保有し、当該ユーザのために働くユーザエージェントに前記コマーシャルメッセージ格納手段に格納されているコマーシャルメッセージを検索させる検索手段と、
該検索手段により検索されたコマーシャルメッセージを前記ユーザエージェントの持主であるユーザに提供するコマーシャルメッセージ提供手段とを含むことを特徴とする。
【０２０４】
このような手段を採用した結果、複数種類の属性に分類されたユーザ毎に当該分類に属するユーザのみをターゲットにしてコマーシャルメッセージが制作され、ユーザエージェントによりそのような複数のコマーシャルメッセージの中からユーザが好むと思われるコマーシャルメッセージが検索されて選択され、ユーザに提供される。その結果、ユーザに適したきめ細かなコマーシャルメッセージがユーザ毎に提供可能となり、ユーザにとって不必要なコマーシャルメッセージがユーザに提供されてしまうという無駄を極力防止することができる。
【０２０５】
前記データベース５６により、ユーザを複数種類の属性毎に分類し、その分類毎に当該分類に属するユーザのみをターゲットにして制作されたコマーシャルメッセージを格納するコマーシャルメッセージ格納手段が構成されている。前記テレスクリプト・エンジン５７により、ユーザのプロフィール情報を知識として保有し、当該ユーザのために働くユーザエージェント２６に前記コマーシャルメッセージ格納手段に格納されているコマーシャルメッセージを検索させる検索手段が構成されている。前記ＳＡ７６～ＳＡ８０，ＳＡ８９～ＳＡ９３，インターネット１３，放送局２，Ｓ２，Ｓ１１～Ｓ１６により、前記検索手段により検索されたコマーシャルメッセージを前記ユーザエージェントの持主であるユーザに提供するコマーシャルメッセージ提供手段が構成されている。
【０２０６】
前記ユーザを複数種類の属性に分類する具体例としては、たとえば、ユーザを、年齢別

，性別，学識レベル別，職業別，ユーザの消費動向別，ユーザの各種好みの嗜好別等に分類することが考えられる。番組等のコンテンツの合間に挿入されるコマーシャルメッセージの放映時間としては、たとえば、２０秒，４０秒，６０秒，８０秒，１００秒等のように、複数種類の放映時間を予め規格化しておき、前記コマーシャルメッセージ格納手段に格納される複数のコマーシャルメッセージも、１つのメッセージまたは複数のメッセージを組合せて放映することにより前記規格化された時間にちょうど収まるような長さに制作しておく。

【０２０７】

一方、放送局２からコマーシャルメッセージを含む番組を放送する場合には、番組放送からコマーシャル放送に切換える直前にコマーシャルメッセージの放映時間を特定するデータを放送する。ユーザ側においては、パソコン１４等により、そのコマーシャルメッセージの放映時間を特定する情報を受信してその情報に基づいて特定されるコマーシャルメッセージ放映時間だけユーザエージェントが検索したコマーシャルメッセージに切換えて放映する。

【０２０８】

一方、ユーザエージェントが予め選択して予約した番組以外の番組をユーザが見る場合もあり、その場合に対応する方法としては、当日放送される番組のスポンサーすべてについてコマーシャルメッセージを予めユーザエージェントが検索してユーザのパソコン１４のハードディスク等に記憶しておくことが考えられる。

【０２０９】

コマーシャルメッセージの記憶は、１つのスポンサーに対し複数種類検索して記憶しておき、その複数種類のコマーシャルメッセージを入れ代わり立ち代わり放映してユーザが飽きないようにすることが望ましい。

【０２１０】

一方、ユーザが全く不要とするコマーシャルメッセージたとえばアルコールを全く受けつけないユーザに対しビールやウイスキー等のコマーシャルメッセージは、当然ユーザエージェントが検索しない。その結果、そのようなユーザに対しては、ユーザが見ている番組のスポンサーになっているにもかかわらずそのユーザには当該スンポンサーのコマーシャルメッセージが全く放映されないという不公平な事態が生ずる。そこで、たとえば一定の地域内等において、スポンサー同士コマーシャルメッセージの放映回数が平等となるように調整する調整手段を設置するのが望ましい。

【０２１１】

図１に示した衛星放送を利用してコマーシャルメッセージを放映する方法として、たとえば、コマーシャルメッセージばかりを次々と放映する衛星放送を１チャンネルまたは多数チャンネルにわたって開設し、ユーザエージェントが前記コマーシャルメッセージ格納手段にアクセスして検索選択したコマーシャルメッセージが衛星放送によって放送される日時とチャンネルを特定できるデータをユーザのパソコンに送信する。ユーザのパソコン１４では、送信されてきた日時が来れば送信されたチャンネルにチューニングして放送電波をキャッチしてその放送内容であるコマーシャルメッセージをハードディスク等に記憶させる。

【０２１２】

ほぼすべてのスポンサーについてコマーシャルメッセージをユーザエージェントが検索してユーザのパソコン１４のハードディスク等に記憶した段階では、その後においては、あるスポンサーについて新たなコマーシャルメッセージが制作された場合に限り、その新たなコマーシャルメッセージについてユーザエージェントが検索し必要と判断すればこのコマーシャルメッセージをユーザのパソコン１４のハードディスク等に記憶させる。またあるスポンサーについて古くなって消去されたコマーシャルメッセージも、そのコマーシャルメッセージがパソコン１４のハードディスクに記憶されておればそのハードディスクから消去する。

【０２１３】

その場合、前記コマーシャルメッセージ格納手段において、新たに作成されて新たに格納されたコマーシャルメッセージあるいは古くて消去されたコマーシャルメッセージが生ずるごとに、たとえばプッシュ技術を利用してユーザのパソコン１４にまでその旨を伝送する。ユーザのパソコン１４では、その伝送されてきた情報に基づいてハードディスクの記憶内容を更新する。

【０２１４】

さらに、ユーザエージェント２６が検索したコマーシャルメッセージについてより詳細なデータを入手したい場合には、インターフェイス１３経由で所定のＷＷＷサーバーへアクセスして入手できるようにするべく、そのコマーシャルメッセージについてのＷＷＷサーバーのアドレスをユーザのパソコン１４に伝送するのが望ましい。そのＷＷＷサーバーのアドレスデータの送信は、たとえば衛星データ配信・放送を利用したり、テレビ放送用の地上波を利用したデータ多重放送により配信する。

【０２１５】

（３） 前述した本実施の形態では、図２２～図２４に示したように、有料コンテンツ等の情報のセキュリティを確保するシステム（または方法）が開示されている。

【０２１６】

この発明は、情報提供者側が情報要求者側に提供する情報に対するセキュリティシステム（またはセキュリティを確保する方法）を発明の属する技術分野とする。

【０２１７】

この種のセキュリティを確保する技術として、従来から一般的に知られているものに、たとえば、あるユーザによって有料コンテンツが購入されれば、その有料コンテンツを暗号化してたとえば放送局からその暗号化コンテンツを放送してもらう。その暗号化コンテンツを購入したユーザに対しては、その暗号化コンテンツの放送日時とチャンネルとを事前に通知しておき、ユーザがその暗号化コンテンツの放送を受信して暗号化コンテンツをＶＴＲ等に記録する。そして、有料コンテンツの提供業者が前記暗号化コンテンツを復号化して再生するための鍵を当該有料コンテンツを購入した正規のユーザに対し配信する。その正規のユーザは、その配信されてきた鍵を用いてＶＴＲ等に記録してある暗号化コンテンツを復号化して再生して閲覧する。

【０２１８】

このような従来の技術の場合には、暗号化コンテンツが電波メディア（無線系メディア）により広域にわたって放送されるために、有料コンテンツに対する料金を支払った正規のユーザ以外のその他多数のユーザが暗号化された有料コンテンツを受信可能となる。このような正規のユーザ以外のその他多数のユーザが前述した暗号化された有料コンテンツを受信して記録した場合には、後はコンテンツ提供業者から配信される暗号化コンテンツを復号化するための鍵（以下単に復号化鍵という）をなんらかの方法で入手するだけで、暗号化コンテンツを復号化して再生閲覧することが可能となる。その結果、有料コンテンツに対し料金を支払っていない多数のユーザが有料コンテンツを再生閲覧可能となってしまうという不都合が生ずる。

【０２１９】

そこで、前記復号化鍵ＦＫを、料金を支払った正規のユーザの公開鍵ＰＫＵにより暗号化してE_{PKU}（ＦＫ）の形で前記正規のユーザにインターネット等を経由して配信することが考えられる。そのようにすれば、他の多数のユーザがこのE_{PKU}（ＦＫ）を傍受したとしても、料金を支払った正規のユーザの秘密鍵ＳＫＵをもっていない限り復号化して復号化鍵ＦＫを再生することができず、一応セキュリティは保たれるように思われる。

【０２２０】

しかし、あるグループの構成員全員が暗号化コンテンツデータの放送を受信し、その構成員の一人が代表として料金を支払ってE_{PKU}（ＦＫ）を受信し、その代表者の秘密鍵で復号化して$D_{SKU}\{E_{PKU}$（ＦＫ）$\}$を演算してＦＫを再生し、そのＦＫをグループの他の構成員全員に配信した場合には、一人分の料金しか払わないにもかかわらず大勢の人間が暗号化コンテンツデータを閲覧することが可能となる。

【０２２１】
この発明は、かかる実情に鑑み考え出されたものであり、その目的は、有料コンテンツ等の情報を利用する権限を有する正規のもの以外のものが不正に情報利用することを極力防止することである。
【０２２２】
このような目的を達成するべく、この発明は、次のような手段を採用している。
情報提供者側が情報要求者側に提供する情報に対するセキュリティを確保する方法であって、
前記情報提供者側において第１の鍵を用いてあるアルゴリズムに従って前記情報を変換する変換ステップと、
該変換ステップにより変換された変換情報を前記情報要求者側に提供する変換情報提供ステップと、
前記情報提供者側において、第２の鍵を生成する第２の鍵生成ステップと、
該第２の鍵生成ステップにより生成された前記第２の鍵を前記情報要求者側へ提供する第２の鍵提供ステップとを含み、
前記第２の鍵生成ステップは、前記変換情報に対し、前記第２の鍵を用いてのあるアルゴリズムに従った変換処理と前記情報要求者側の秘密鍵を用いてのあるアルゴリズムに従った変換処理とを施すことを条件として前記情報を再生できるように定められた前記第２の鍵を生成することを特徴とする、情報に対するセキュリティを確保する方法。
【０２２３】
また、前述した目的を達成する他の手段として、本発明は以下の構成を採用してもよい。
【０２２４】
情報提供者側が情報要求者側に提供する情報に対するセキュリティシステムであって、
前記情報提供者側において第１の鍵を用いてるあるアルゴリズムに従って前記情報を変換する変換手段と、
該変換手段により変換された変換情報を前記情報要求者側に提供する変換情報提供手段と、
前記情報提供者側において、第２の鍵を生成する第２の鍵生成手段と、
該第２の鍵生成手段により生成された前記第２の鍵を前記情報要求者側へ提供する第２の鍵提供手段とを含み、
前記第２の鍵生成手段は、前記変換情報に対し、前記第２の鍵を用いてのあるアルゴリズムに従った変換処理と前記情報要求者側の秘密鍵を用いてのあるアルゴリズムに従った変換処理とを施すことを条件として前記情報を再生できるように定められた前記第２の鍵を生成することを特徴とする、情報に対するセキュリティシステム。
【０２２５】
本発明がこのような手段を採用した結果、暗号化情報を復号化して再生する際に、情報提供者側が前記情報を提供する相手である正規の情報要求者側の秘密鍵を用いての変換処理が必須となる。その結果、暗号化情報を復号化して再生するには、前記正規の情報要求者側の秘密鍵を入手しなければならない。しかし、秘密鍵というものは秘密性を保持しなければならない性質のものであり、他人にみだりに貸し与えて使用させることがあまり考えられないものである。ゆえに、前記正規の情報要求者以外の他の者が正規の情報要求者から秘密鍵を入手することは一般的にあまり考えられず、正規の情報要求者以外のものが前記暗号化情報を復号化して再生することが極力防止できる。
【０２２６】
前記第２の鍵生成ステップ（第２の鍵生成手段）は、前記変換情報に対し、前記第２の鍵を用いてのあるアルゴリズムに従った変換処理が実行された後前記情報要求者側の秘密鍵を用いてのあるアルゴリズムに従った変換処理を施すことを条件として前記情報を再生できるように定められた前記第２の鍵を生成するものであることが望ましい。
【０２２７】

前記ＳＦ２２～ＳＦ２４により、前記情報提供者（コンテンツ提供業者７）側において第１の鍵（乱数ＲＮ）を用いてあるアルゴリズム（イクスクルーシブオア）に従って前記情報を変換する変換ステップ（変換手段）が構成されている。前記ＳＦ２５～ＳＦ２８，放送局２，Ｓ７，Ｓ２３，Ｓ８，Ｓ２４，Ｓ２，Ｓ１１～Ｓ１６により、前記変換ステップ（変換手段）より変換された変換情報（Ａ（＋）ＲＮ）を前記情報要求者（ユーザ）側に提供する変換情報提供ステップ（変換情報提供手段）が構成されている。

【０２２８】

前記ＳＨ５により、前記情報提供者側において、第２の鍵を生成する第２の鍵生成ステップ（第２の鍵生成手段）が構成されている。ＳＨ５，ＳＦ２３により、前記第２の鍵生成ステップ（第２の鍵生成手段）により生成された前記第２の鍵を前記情報要求者側へ提供する第２の鍵提供ステップ（第２の鍵提供手段）が構成されている。

【０２２９】

前記第２の鍵生成ステップ（第２の鍵生成手段）は、前記変換情報（Ａ（＋）ＲＮ）に対し、前記第２の鍵（Ｉ１，Ｉ２，…Ｉｎ）を用いてのあるアルゴリズム（イクスクルーシブオア）に従った変換処理と前記情報要求者側の秘密鍵（ＳＫＵ）を用いてのあるアルゴリズム（イクスクルーシブオア）に従った変換処理とを施すことを条件として前記情報（コンテンツＡ）を再生できるように定められた前記第２の鍵（Ｉ１，Ｉ２，…Ｉｎ）を生成する。

【０２３０】

（４）　前述した本実施の形態では、図２１に基づいて説明したように、情報の不正コピーを防止する発明が開示されている。

【０２３１】

この発明は、不正コピーを防止することを目的とし、その目的達成のために、次のような手段を採用した。

【０２３２】

暗号化された暗号情報内に、当該暗号情報を復号化するための鍵情報が埋込まれており、該鍵情報を読出す鍵読出手段（ＭＰＥＧ２，復号化器８２，電子透かし検出器８３）と、

該鍵読出手段より読出された鍵を用いて前記暗号情報を復号化して情報を再生する復号化手段（ＩＣカード６５，ＴＶ１６，パソコン１４）とを含み、

前記復号化手段は、前記再生された情報をユーザが認識できるように出力する出力装置（ＴＶ１６，ＣＲＴ５２を有するパソコン１４）に内蔵されている。

【０２３３】

（５）　ＩＣカード６５に、エージェント用知識データばかりでなくユーザエージェント２６のプログラム自体も記憶させてもよい。そのように構成した場合には、エージェント用知識データとユーザエージェントのプログラム自体とがユーザに常に携帯されるＩＣカードに記録されることとなるために、エージェント用知識データが他人に覗き見されるおそれが少なくなるとともに、ユーザエージェントを他人に使用される不都合も極力防止することができる。しかも、ユーザが勤務先のオフィス等に設置されているパソコンを利用して自分自身のユーザエージェントを活用したい場合には、携帯しているＩＣカード６５をそのパソコンに挿入することにより可能となり、わざわざ自宅のパソコン１４からユーザエージェントのプログラムとエージェント用知識データとを送信してもらう必要がなくなる。ＩＣカード６５のＥＥＰＲＯＭ９４により、エージェント用知識データを格納するエージェント用知識データ格納手段が構成されている。またＩＣカード６５のＥＥＰＲＯＭ９４により、エージェントプログラムを格納するエージェントプログラム格納手段が構成されている。このエージェントプログラム格納手段に格納されているエージェントプログラムは、前記ＩＣカードの所有者のために働くエージェントである。

【０２３４】

図１５に示したＳＸＡＬ／ＭＢＡＬの代わりに、ＲＳＡ公開鍵暗号方式や楕円曲線暗号方式を用いてもよい。

【０２３５】
無線装置７１，７２，アンテナ７６，７７により、コンテンツ提供業者と第三者機関との間で情報の交信を無線系メディアを利用して行なうための無線系メディア利用型情報交信手段が構成されている。
【０２３６】
前記Ｓ２２，Ｓ２２ａ，Ｓ２２ｂにより、アクセスしてきたものが、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事を処理するために設立された第三者機関本人であるか否かを認証するための第三者機関認証手段が構成されている。前記Ｓ１５により、番組の合間に挿入されて放送されてきたコマーシャルメッセージをユーザエージェントが検索したコマーシャルメッセージに取換えて編集するコマーシャルメッセージ編集手段が構成されている。前記Ｓ１６により、番組の合間に挿入されて放送されてきたコマーシャルメッセージをユーザエージェントが検索したコマーシャルメッセージに切換えて放映する切換放映手段が構成されている。
【０２３７】
前記ＳＡ１０により、ユーザエージェントの移動先予定を登録しておく移動先予定登録手段が構成されている。前記ＳＡ４５により、第三者エージェントに出向依頼を行なうための処理を行なう出向依頼処理手段が構成されている。ＳＡ４９により、ユーザエージェントが前記第三者機関へ移動するための第三者機関移動手段が構成されている。
【０２３８】
ＳＡ６８～ＳＡ７２により、ユーザエージェントによる購入手続を行なうための購入手続手段が構成されている。この購入手続手段は、購入手続に対するユーザのデジタル署名を行なうためのデジタル署名手段（ＳＡ７０，ＳＡ７１，ＳＡ７２）を含んでいる。このデジタル署名手段は、購入対象を特定可能なオーダ情報と支払方法を特定可能な支払指示との二重署名を行なう機能を有する。ＳＢ２０～ＳＢ２７，ＳＢ４～ＳＢ３１により、前記ユーザのデジタル署名を生成するためのデジタル署名生成手段が構成されている。このデジタル署名生成手段は、前記二重署名を生成する機能を有する。
【０２３９】
前記ＳＡ７３，ＳＡ７４により、ユーザエージェントのクローンが既に在駐しているところを避け在駐していないところを探し出してユーザエージェントが移動する移動先選択移動手段が構成されている。ＳＡ８１～ＳＡ８３，ＳＡ８８～ＳＡ９２により、ユーザエージェントを駐在させて新たなコマーシャルメッセージが制作された場合に当該コマーシャルメッセージに対する評価を行なうユーザエージェント駐在評価手段が構成されている。
【０２４０】
ユーザエージェント等が外国のサイト等に移動する場合には、そのサイトでは、どこの国のエージェントが移動してきたのかをチェックする必要が生ずる場合がある。人間の場合には外国に行くときにビザ（入国許可書）が必要になるのと同様に、エージェントの場合には、ビザ（入国許可書）に相当するものをチェックして、そのエージェントの侵入を許可するか否かを判断するのが望ましい。
【０２４１】
そこで、アクセスしてきたエージェントがどこの国のユーザまたは業者のために働くエージェントであるかをチェックするための国籍証明データを当該エージェントに持たせておく。この国籍証明データは、前述した第三者機関等からなる国籍証明書発行機関が外国に行こうとするエージェントに発行する。国籍証明書発行機関には、当該エージェントの公開鍵や必要に応じて秘密鍵が登録されており、国籍証明書発行機関は、これら公開鍵あるいは秘密鍵を利用して当該エージェントの本人確認を行なった上で、当該エージェントに対し国籍証明書を発行する。そして、当該エージェントが外国のサイトにアクセスしてそのサイトに移動しようとした際に、当該サイト側では、当該エージェントの公開鍵や秘密鍵を利用して当該エージェントの本人確認を行なった上で、当該エージェントが保有している国籍証明書を確認してアクセスを許してよいか否かを判断する。

【０２４２】
一方、国籍証明書の発行の代わりに、当該エージェントが移動しようとする外国に当該エージェントが入国してもよいという入国許可証を当該エージェントに発行してもよい。その場合には、前述と同様に、第三者機関等からなる入国証明書発行機関が、登録されている公開鍵や秘密鍵等を利用して当該エージェントの本人確認を行なった上で、当該エージェントに対し入国証明書を発行する。
【０２４３】
前述したように、ユーザエージェント２６等が知識として記憶している公開鍵や秘密鍵を、そのユーザエージェント２６のユーザと同じ公開鍵および秘密鍵にした実施の形態を示したが、その代わりに、ユーザの公開鍵や秘密鍵と異なった公開鍵や秘密鍵をユーザエージェント２６等に記憶させておいてもよい。そのようにすれば、ユーザエージェント２６はデジタル署名等を行なった場合に、後々、ユーザ自身がデジタル署名を行なったのかまたはユーザエージェントがデジタル署名を行なったのかを判別することが可能となる。このように、ユーザとそのエージェントとの鍵を異ならせる場合には、公開鍵あるいは秘密鍵を登録しておく鍵登録機関に、ユーザの公開鍵あるいは秘密鍵とそのエージェントの公開鍵あるいは秘密鍵とを対応づけて登録しておくのが望ましい。
【０２４４】
前述した実施の形態では、第三者エージェントが、依頼された仕事の実行として当事者の一方または双方に違法性あるか否かを監視するものを示したが違法性の有無の関し専門の第三者エージェントがネットワーク上を巡回してパトロールするようにし、その監視用第三者エージェントが訪れたプレース上において、ユーザエージェントや業者側エージェント等をその監視用第三者エージェントが尋問して違法性の有無の監視を行なうようにしてもよい。
【０２４５】
ユーザエージェント等が過去にどこのサイトを訪れてどのような仕事を誰のために実行したか等の、エージェントの過去の仕事履歴データを当該エージェントに記憶させておいてもよい。そのようにすれば、いわゆる契約ネット（contrac net）を利用したタスクの分配に際し、マネージャー側がその仕事履歴データに基づいてどの規約者（エージェント）がタスクの実行に適しているか否かを突き止めることができ、その適している規約者（エージェント）に対して指名落札（directed-award）を行なうことが可能となる。なお、契約ネットとは、多数の処理モードの交渉を通じて問題を分割し、各モードに副問題（これをタスクと呼ぶ）を割当てるためのモデルのことである。
【０２４６】
[課題を解決するための手段の具体例]
コンテンツ提供業者７とユーザ、または、ＣＭ制作者１０とユーザにより、当事者が構成されている。前記ＳＡ４４，ＳＡ４７により、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事が発生したことを判定する特定仕事判定手段が構成されている。第三者機関エージェント２９，第三者機関常駐エージェント２８により、前記当事者双方に対し中立性を有する第三者エージェントが構成されている。この第三者エージェントは、第三者機関８によって運用管理するエージェントに限定されるものではなく、たとえば前記当事者のエージェントが仕事をするテレスクリプト・エンジン内のプレースと同じプレース上で仕事をしている他のエージェントによりこの第三者エージェントを構成してもよい。
【０２４７】
前記ＳＡ４５，ＳＡ６４またはＳＡ４９～ＳＡ５３またはＳＡ６０またはＳＡ６９，ＳＡ７０により、前記特定仕事判定手段の判定結果に従って、前記当事者双方に対し中立性を有する第三者エージェントに前記特定の仕事を依頼する仕事依頼手段が構成されている。この仕事依頼手段により依頼された仕事を前記第三者エージェントが代理して実行する（図７，図８に示したフローチャート）。前記第三者機関８により、前記特定の仕事を処理するために設立された第三者機関が構成されている。そして前記第三者エージェント（

第三者機関エージェント２９，第三者機関常駐エージェント２８）は、その第三者機関により運用管理され、前記特定の仕事を行なうために開発されたエージェントである。

【０２４８】

前記ユーザエージェント２６と移動先エージェント２７とにより、前記当事者のそれぞれの側のために働く当事者エージェントが構成されている。前記特定仕事判定手段は、前記当事者エージェント同士が協調して動作しているときに、当該当事者エージェントでは自己の立場の方に有利となる利己的動作（たとえば有料コンテンツの不法持ち帰りや有料コンテンツに対する虚偽の評価）を行なうおそれのある場合に前記特定の仕事が発生した旨の判定を行なう。

【０２４９】

前記データベース１９により、有料コンテンツを格納しているコンテンツ格納手段が構成されている。コンテンツ提供業者７により、前記コンテンツ格納手段内の格納コンテンツを提供するコンテンツ提供者が構成されている。ユーザ宅１７に居住しているユーザにより、前記コンテンツ提供者が提供するコンテンツ内に入手したいコンテンツがあるか否かの検索を希望するユーザが構成されている。そして、前記特定仕事判定手段は、前記当事者エージェントのうちのユーザ側エージェント（ユーザエージェント２６）が前記コンテンツ格納手段に格納されている前記有料コンテンツの検索を希望した場合（ＳＡ４３によるＹＥＳの判断がなされた場合）に前記特定の仕事が生じたことを判定する。

【０２５０】

さらに、前記第三者エージェントは、依頼された仕事の実行を通して前記当事者の一方または双方に違法性があるか否かを監視する監視機能（ＳＣ６，ＳＣ１８）を有する。

【０２５１】

前記ＳＡ４３，ＳＡ４４，ＳＡ６７，ＳＡ５８により、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事が発生したことを判定する特定仕事判定ステップが構成されている。前記ＳＡ４５，ＳＢ１，ＳＢ５，ＳＢ６，ＳＡ４９，ＳＡ５０，ＳＢ７～ＳＢ９により、前記当事者の双方に対し中立性を有する第三者エージェントを調達する第三者エージェント調達ステップが構成されている。前記ＳＡ４５，ＳＡ４６，ＳＡ６４，ＳＡ４９～ＳＡ５３，ＳＡ６９，ＳＡ７０，ＳＡ６０により、前記特定仕事判定ステップにより前記特定の仕事が生じた旨の判定がなされた場合に、前記第三者エージェント調達ステップで調達された第三者エージェントに前記特定の仕事の依頼を行なう仕事依頼ステップが構成されている。そしてその仕事依頼ステップにより依頼された第三者エージェントが依頼された前記特定の仕事を実行する（図７，図８に示したフローチャート）。

【０２５２】

前記テレスクリプト・エンジン２２とデータベース２３とにより、第三者エージェントを提供するためのエージェント提供装置が構成されている。前記データベース２３により、複数種類の第三者エージェントを格納しているエージェント格納手段が構成されている。テレスクリプト・エンジン２２により、仕事を当事者エージェントに代わって第三者エージェントにより代理実行してもらいたい旨の依頼があった場合に、代理の対象となる前記当事者エージェントに応じた種類の第三者エージェントを前記エージェント格納手段が格納している前記第三者エージェントの中から検索して提供するエージェント検索提供手段が構成されている。

【０２５３】

ユーザエージェント２６によりユーザ側のために働くエージェントであって、ネットワーク上を移動して動作するモバイルエージェントで構成されたユーザ側エージェントが構成されている。コンテンツ提供業者７により、前記ユーザの要求に応えるサービス業者が構成されている。移動先エージェント２７により、前記サービス業者側のために働く業者側エージェントが構成されている。第三者機関８のプレース２５を有するコンピュータ２２ａにより、前記ユーザ側エージェントのワーキングエリアとして機能し、秘密の漏洩が防止できる秘密保持用ワーキングエリアが構成されている。

【０２５４】
そして、前記ユーザ側エージェントは、秘密にしたい秘密データ（秘密情報ＳＩ）を秘密性が保持できる態様（暗号化した態様）で前記知識として記憶しており、該ユーザ側エージェントが移動して仕事を行なう際に、前記秘密データを使用する必要が生じた場合に（ＳＡ４４によりＹＥＳの判断がなされた場合に）、前記ユーザ側エージェントは、前記秘密保持用ワーキングエリアに移動し（ＳＡ４９）、該秘密保持用ワーキングエリア内で前記秘密データの秘密性を解除（ＳＡ５０，ＳＡ５１）して前記仕事の実行を可能にする。

【０２５５】
前記ユーザ側エージェントは、前記秘密データを暗号化して保有している（図１４参照）。そして、ユーザ側エージェントが前記秘密保持用ワーキングエリアに移動した後前記暗号化された秘密データの復号化再生を可能にする（ＳＡ５０，ＳＡ５１）。

【０２５６】
また、前記ユーザ側エージェントは、前記秘密データの復号に用いられる復号鍵（ＳＫ１）を保有しておらず、前記秘密保持用ワーキングエリアに移動した後、該秘密保持用ワーキングエリア内に取り寄せた前記復号鍵を用いた前記秘密データの復号を可能にする（ＳＡ５０，ＳＡ５１，ＳＣ２，ＳＣ１１，ＳＣ１２）。

【０２５７】
前記秘密データは、前記ユーザの本人認証のための秘密鍵（ＳＫＵ）を含んでいる（図１４参照）。

【０２５８】
前記ＣＤ－ＲＯＭ６８ｂまたはＩＣカード６５により、それぞれに独立の知識を持つエージェント同士が協調的に動作するマルチエージェントシステムに使用され、当事者の一方の側のために働くエージェントプログラムを記録している記録媒体が構成されている。この記録媒体に記録されているプログラムは、コンピュータに、当事者の他方のエージェントと打合せする第１の打合せ手段（ＳＡ３２，ＳＡ４５，ＳＡ５５，ＳＡ６０，ＳＡ６２，ＳＡ６８，ＳＡ７２）と、前記当事者の双方が行なうには不向きな中立性を要する特定の仕事が生じた場合に、前記当事者双方に対し中立性を有する第三者エージェント（第三者機関常駐エージェント２８，第三者機関エージェント２９）と打合せする第２の打合せ手段（ＳＡ５０，ＳＡ５１，ＳＡ６４，ＳＡ７０）と、前記特定の仕事を前記第三者エージェントに代理実行してもらうのに必要な情報（ユーザのプロフィール情報９６等）を当該第三者エージェントに通知する必要情報通知手段（ＳＡ６４，ＳＡ７０，ＳＡ５１）として機能させるためのものである。

【０２５９】
前述した当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事の他の例としては、当事者エージェント同士が対立するというトラブルが発生した場合の仲裁やどちらのエージェントが正しいかの判定、当事者エージェントの一方または双方が本当に正しい当事者のエージェントであるかを立証するための第三者による証明等が考えられる。つまり、この特定の仕事とは、当事者だけでは解決が困難または不可能な中立性を要する仕事すべてを対象とする。

【課題を解決するための手段の具体例の効果】

【０２６０】
請求項１に関しては、ユーザと複数のコンテンツ提供業者とからなる当事者の双方に対し中立性を有する第三者エージェントが、ユーザにマッチするコンテンツであるか否かを判断してくれるために、中立性を保ちながらユーザにマッチするコンテンツの提供が可能となる。そのプロフィール情報に基づいた第三者エージェントによる判断が、第三者機関コンピュータ内で行なわれるため、プロフィール情報がコンテンツ提供業者に漏洩する不都合も極力防止できる。

【０２６１】
請求項２に関しては、請求項１に関する効果に加えて、ユーザ側エージェントがホーム

となるコンピュータから出て移動して仕事を行なう際に、秘密のプロフィール情報を使用する必要が生じた場合に、ユーザ側エージェントは、秘密保持用ワーキングエリアに移動し、該秘密保持用ワーキングエリア内で秘密のプロフィール情報の秘密性を解除して仕事の実行を可能にするために、秘密のプロフィール情報の漏洩を防止できながらその秘密のプロフィール情報を使用しての仕事の実行が可能となる。

【０２６２】

請求項３に関しては、請求項２に関する効果に加えて、ユーザ側エージェントが秘密のプロフィール情報を暗号化して保有しているために、ユーザ側エージェントがネットワーク上を移動して動作したとしてもその秘密のプロフィール情報が他人に漏洩されることを極力防止することができる。

【０２６３】

請求項４に関しては、請求項３に関する効果に加えて、秘密のプロフィール情報の復号に用いられる復号鍵をユーザ側エージェントが保有していないために、ユーザ側エージェントがネット上を移動して動作した際に暗号化された秘密のプロフィール情報が他人に知られたとしても、それを復号するための復号鍵までは他人に知られることが防止できるために、秘密のプロフィール情報の漏洩をより確実に防止することができる。

【０２６４】

請求項５に関しては、請求項２～請求項４のいずれかの効果に加えて、ユーザ側エージェントが保有している秘密のプロフィール情報は、ユーザの本人認証のための秘密鍵を含んでいるために、秘密保持用ワーキングエリア内に移動することによりその秘密鍵を用いてのユーザの本人認証を行なうことが可能となり、ユーザ側エージェントにより一層高度なユーザの代理仕事を行なわせることが可能となる。

【０２６５】

請求項６に関しては、ユーザのプロフィール情報は、該プロフィール情報に基づいての前記第三者エージェントによる判断の結果に対するユーザの反応に基づいて更新されるされるために、活用すればするほどユーザのプロフィール情報がユーザに適した内容のものとなり、ユーザの満足のいく仕事が行なえるものとなる。

【図面の簡単な説明】

【０２７２】

【図１】情報の検索および配信を説明するための説明図である。

【図２】各種エージェントの動作を説明するための説明図である。

【図３】パソコンの制御動作を示すフローチャートである。

【図４】ユーザエージェントの動作を示すフローチャートである。

【図５】ユーザエージェントの動作を示すフローチャートである。

【図６】ユーザエージェントの動作を示すフローチャートである。

【図７】第三者機関常駐エージェントの動作を示すフローチャートである。

【図８】第三者機関エージェントの動作を示すフローチャートである。

【図９】ＣＭの検索を行なうためのエージェントの動作を説明するための説明図である。

【図１０】ユーザエージェントの動作を示すフローチャートである。

【図１１】（ａ）はＣＭプレース常駐エージェントの動作を示すフローチャートであり、（ｂ）はＣＭ制作者の情報処理コンピュータの制御動作を示すフローチャートである。

【図１２】ユーザのパソコンのＣＲＴにより表示されたコマーシャルメッセージの表示画面図である。

【図１３】コンテンツ提供業者の通信装置とユーザのパソコンとの制御回路を示すブロック図である。

【図１４】ユーザのＩＣカードの制御回路および記録情報を示すブロック図である。

【図１５】暗号方式ＳＸＡＬ／ＭＢＡＬの概要説明図である。

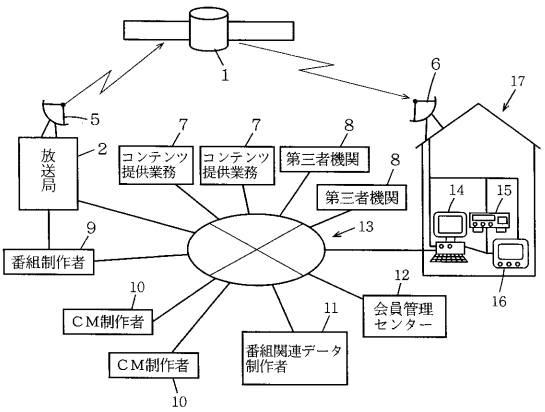
【図１６】コンテンツ提供業者の通信装置の制御動作を示すフローチャートである。

【図１７】ユーザのパソコンの制御動作を示すフローチャートである。

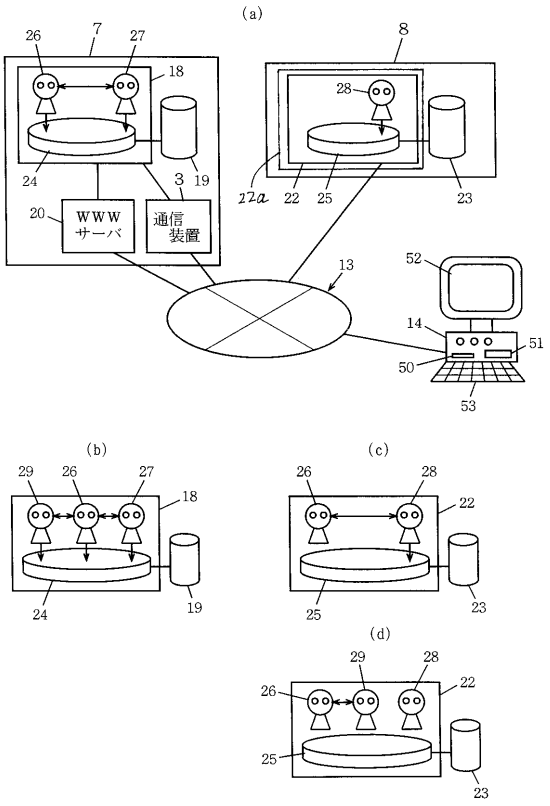
【図１８】ユーザ認証処理の制御動作を示すフローチャートである。

【図１９】コンテンツの不正コピーを防止するための制御回路を示すブロック図である。
【図２０】情報の検索および配信の他の例を示す説明図である。
【図２１】コンテンツの不正コピーを防止するための他の例を示すブロック図である。
【図２２】通信装置の制御動作の他の例を示すフローチャートである。
【図２３】ユーザ認証処理の他の例を示すフローチャートである。
【図２４】ユーザのパソコンの制御動作の他の例を示すフローチャートである。
【符号の説明】
【０２７３】
１　衛星、２　放送局、１０　ＣＭ制作者、１１　番組関連データ制作者、７　コンテンツ提供業者、８　第三者機関、１４　パソコン、１６　ＴＶ、１５　ＶＴＲ、１３　インターネット、２６　ユーザエージェント、２７　移動先エージェント、２８　第三者機関常駐エージェント、２９　第三者機関エージェント、１９，２３，５６，７０　データベース、５２　ＣＲＴ、５０　ＩＣカード挿入口、１８，２２，５７　テレスクリプト・エンジン、２４，２５，５８　プレース、３　通信装置、５９　常駐エージェント、６９　管理サーバー、６８ｂ　ＣＤ－ＲＯＭ、６５　ＩＣカード、９６　プロフィール情報、８２　ＭＰＥＧ２復号化器、８３　電子透かし検出器、８６　ＡＰＳ。

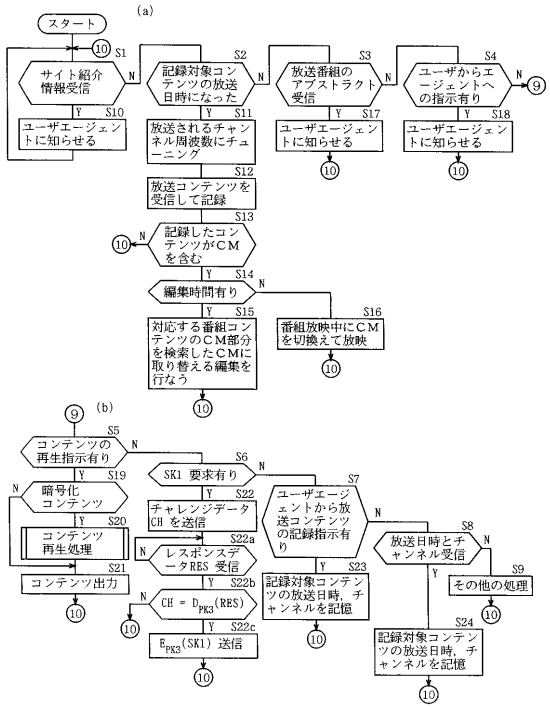
【図１】



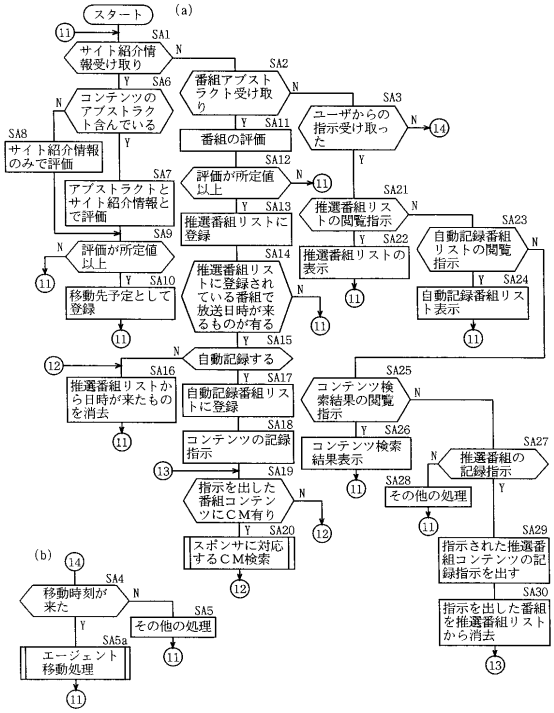
【図２】



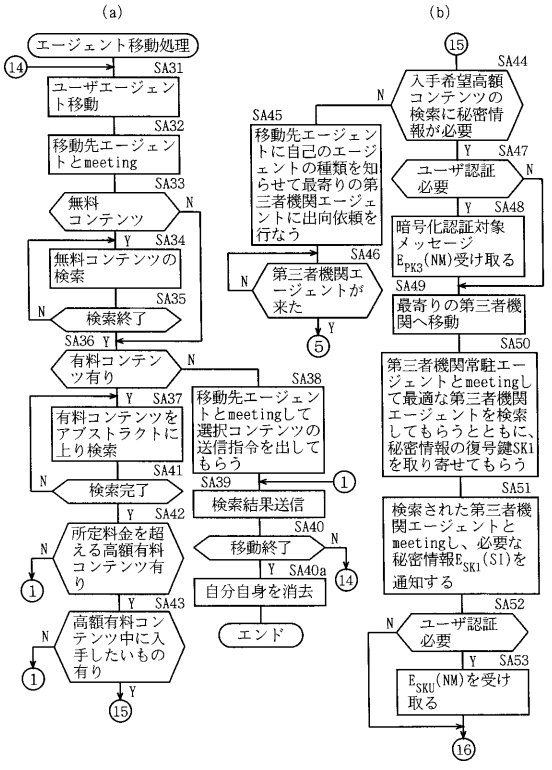
【図３】


(a)
スタート
S1 サイト紹介情報受信
S2 記録対象コンテンツの放送日時になった
S3 放送番組のアブストラクト受信
S4 ユーザからエージェントへの指示有り
S10 ユーザエージェントに知らせる
S11 放送されるチャンネル周波数にチューニング
S17 ユーザエージェントに知らせる
S18 ユーザエージェントに知らせる
S12 放送コンテンツを受信して記録
S13 記録したコンテンツがCMを含む
S14 編集時間有り
S15 対応する番組コンテンツのCM部分を検索したCMに取り替える編集を行なう
S16 番組放映中にCMを切換えて放映
(b)
S5 コンテンツの再生指示有り
S19 暗号化コンテンツ
S20 コンテンツ再生処理
S21 コンテンツ出力
S6 SK1 要求有り
S22 チャレンジデータCH を送信
S22a レスポンスデータRES 受信
S22b CH = D_PK3(RES)
S22c E_PK3(SK1) 送信
S7 ユーザエージェントから放送コンテンツの記録指示有り
S23 記録対象コンテンツの放送日時，チャンネルを記憶
S8 放送日時とチャンネル受信
S24 記録対象コンテンツの放送日時，チャンネルを記憶
S9 その他の処理

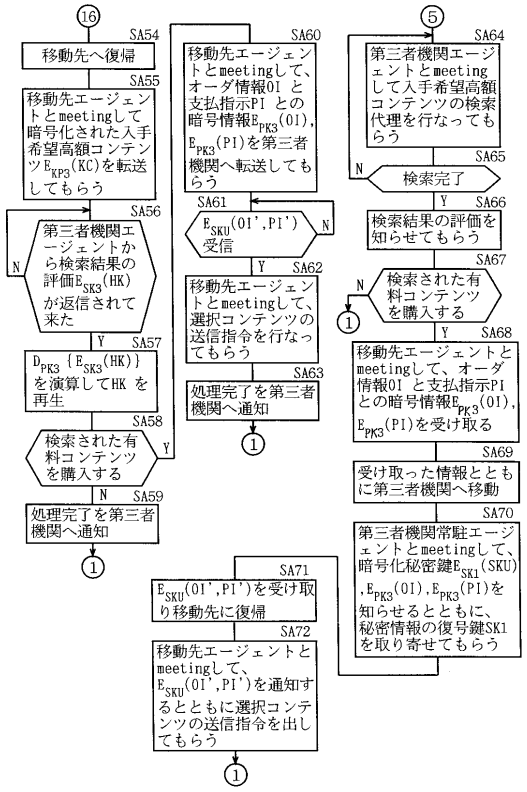
【図４】


スタート
(a)
SA1 サイト紹介情報受け取り
SA6 コンテンツのアブストラクト含んでいる
SA8 サイト紹介情報のみで評価
SA7 アブストラクトとサイト紹介情報とで評価
SA9 評価が所定値以上
SA10 移動先予定として登録
SA2 番組アブストラクト受け取り
SA11 番組の評価
SA12 評価が所定値以上
SA13 推選番組リストに登録
SA14 推選番組リストに登録されている番組で放送日時が来るものが有る
SA15 自動記録する
SA16 推選番組リストから日時が来たものを消去
SA17 自動記録番組リストに登録
SA18 コンテンツの記録指示
SA19 指示を出した番組コンテンツにCM有り
SA20 スポンサに対応するCM検索
SA3 ユーザからの指示受け取った
SA21 推選番組リストの閲覧指示
SA22 推選番組リストの表示
SA23 自動記録番組リストの閲覧指示
SA24 自動記録番組リスト表示
SA25 コンテンツ検索結果の閲覧指示
SA26 コンテンツ検索結果表示
SA27 推選番組の記録指示
SA28 その他の処理
SA29 指示された推選番組コンテンツの記録指示を出す
SA30 指示を出した番組を推選番組リストから消去
(b)
SA4 移動時刻が来た
SA5 その他の処理
SA5a エージェント移動処理

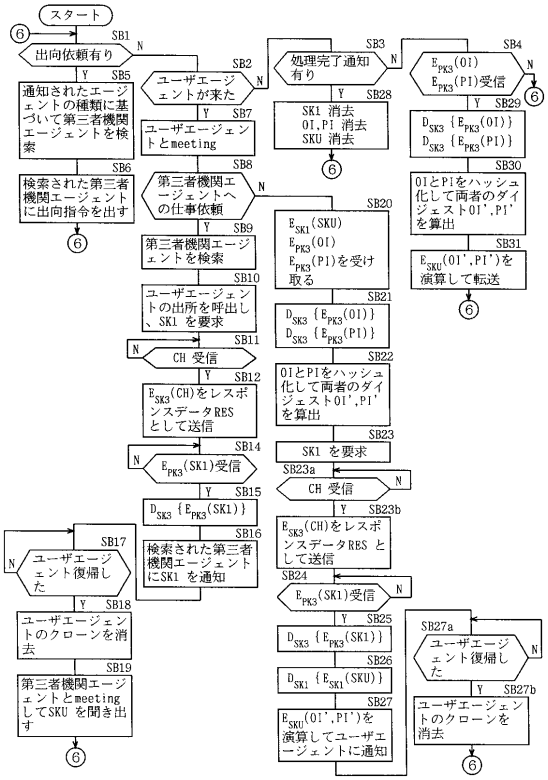
【図５】


(a)
エージェント移動処理
SA31 ユーザエージェント移動
SA32 移動先エージェントとmeeting
SA33 無料コンテンツ
SA34 無料コンテンツの検索
SA35 検索終了
SA36 有料コンテンツ有り
SA37 有料コンテンツをアブストラクトに上り検索
SA41 検索完了
SA42 所定料金を超える高額有料コンテンツ有り
SA43 高額有料コンテンツ中に入手したいもの有り
SA38 移動先エージェントとmeetingして選択コンテンツの送信指令を出してもらう
SA39 検索結果送信
SA40 移動終了
SA40a 自分自身を消去
エンド
(b)
SA44 入手希望高額コンテンツの検索に秘密情報が必要
SA45 移動先エージェントに自己のエージェントの種類を知らせて最寄りの第三者機関エージェントに出向依頼を行なう
SA46 第三者機関エージェントが来た
SA47 ユーザ認証必要
SA48 暗号化認証対象メッセージ E_PK3(NM)受け取る
SA49 最寄りの第三者機関へ移動
SA50 第三者機関常駐エージェントとmeetingして最適な第三者機関エージェントを検索してもらうとともに，秘密情報の復号鍵SK1を取り寄せてもらう
SA51 検索された第三者機関エージェントとmeetingし，必要な秘密情報E_SK1(SI)を通知する
SA52 ユーザ認証必要
SA53 E_SKU(NM)を受け取る

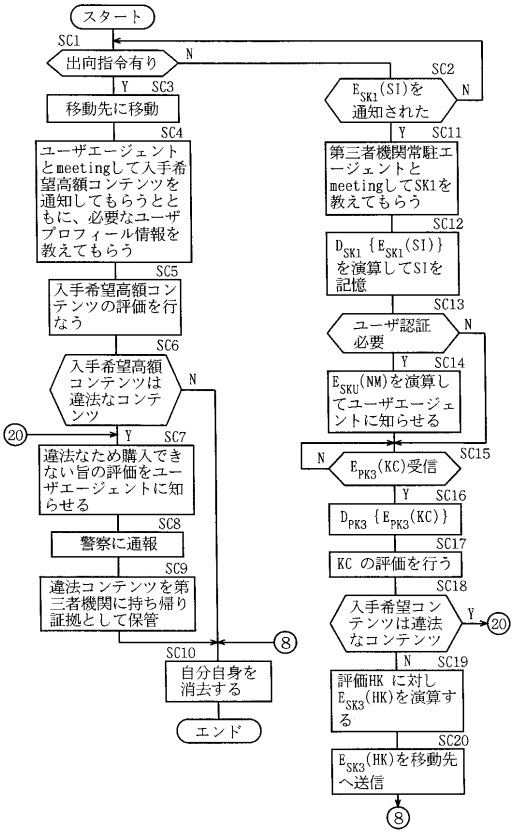
【図６】


SA54 移動先へ復帰
SA55 移動先エージェントとmeetingして暗号化された入手希望高額コンテンツE_KP3(KC)を転送してもらう
SA56 第三者機関エージェントから検索結果の評価E_SK3(HK)が返信されて来た
SA57 D_PK3{E_SK3(HK)}を演算してHK を再生
SA58 検索された有料コンテンツを購入する
SA59 処理完了を第三者機関へ通知
SA60 移動先エージェントとmeetingして，オーダ情報OI と支払指示PI との暗号情報E_PK3(OI)，E_PK3(PI)を第三者機関へ転送してもらう
SA61 E_SKU(OI',PI') 受信
SA62 移動先エージェントとmeetingして，選択コンテンツの送信指令を行なってもらう
SA63 処理完了を第三者機関へ通知
SA64 第三者機関エージェントとmeetingして入手希望高額コンテンツの検索代理を行なってもらう
SA65 検索完了
SA66 検索結果の評価を知らせてもらう
SA67 検索された有料コンテンツを購入する
SA68 移動先エージェントとmeetingして，オーダ情報OI と支払指示PI との暗号情報E_PK3(OI)，E_PK3(PI)を受け取る
SA69 受け取った情報とともに第三者機関へ移動
SA70 第三者機関常駐エージェントとmeetingして，暗号化秘密鍵E_SK1(SKU)，E_PK3(OI)，E_PK3(PI)を知らせるとともに，秘密情報の復号鍵SK1を取り寄せてもらう
SA71 E_SKU(OI',PI')を受け取り移動先に復帰
SA72 移動先エージェントとmeetingして，E_SKU(OI',PI')を通知するとともに選択コンテンツの送信指令を出してもらう

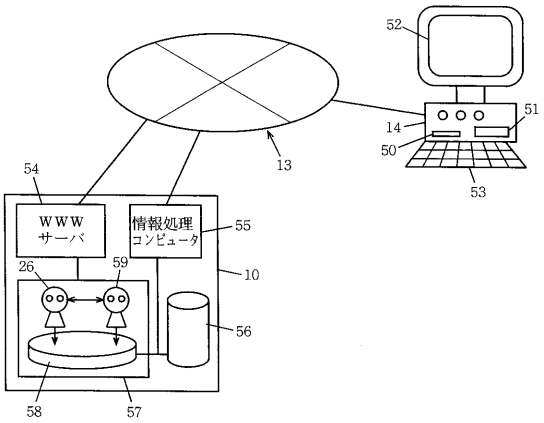
【図７】


スタート
出向依頼有り
通知されたエージェントの種類に基づいて第三者機関エージェントを検索
検索された第三者機関エージェントに出向指令を出す
ユーザエージェントが来た
ユーザエージェントとmeeting
第三者機関エージェントへの仕事依頼
第三者機関エージェントを検索
ユーザエージェントの出所を呼出し、SK1 を要求
CH 受信
E_{SK3}(CH)をレスポンスデータRESとして送信
E_{PK3}(SK1)受信
$D_{SK3}\{E_{PK3}(SK1)\}$
検索された第三者機関エージェントにSK1 を通知
ユーザエージェント復帰した
ユーザエージェントのクローンを消去
第三者機関エージェントとmeetingしてSKU を聞き出す
処理完了通知有り
SK1 消去
OI,PI 消去
SKU 消去
E_{PK3}(OI)
E_{PK3}(PI)受信
$D_{SK3}\{E_{PK3}(OI)\}$
$D_{SK3}\{E_{PK3}(PI)\}$
OIとPIをハッシュ化して両者のダイジェストOI',PI'を算出
E_{SKU}(OI',PI')を演算して転送
E_{SK1}(SKU)
E_{PK3}(OI)
E_{PK3}(PI)を受け取る
$D_{SK3}\{E_{PK3}(OI)\}$
$D_{SK3}\{E_{PK3}(PI)\}$
OIとPIをハッシュ化して両者のダイジェストOI',PI'を算出
SK1 を要求
CH 受信
E_{SK3}(CH)をレスポンスデータRES として送信
E_{PK3}(SK1)受信
$D_{SK3}\{E_{PK3}(SK1)\}$
$D_{SK1}\{E_{SK1}(SKU)\}$
E_{SKU}(OI',PI')を演算してユーザエージェントに通知
ユーザエージェント復帰した
ユーザエージェントのクローンを消去

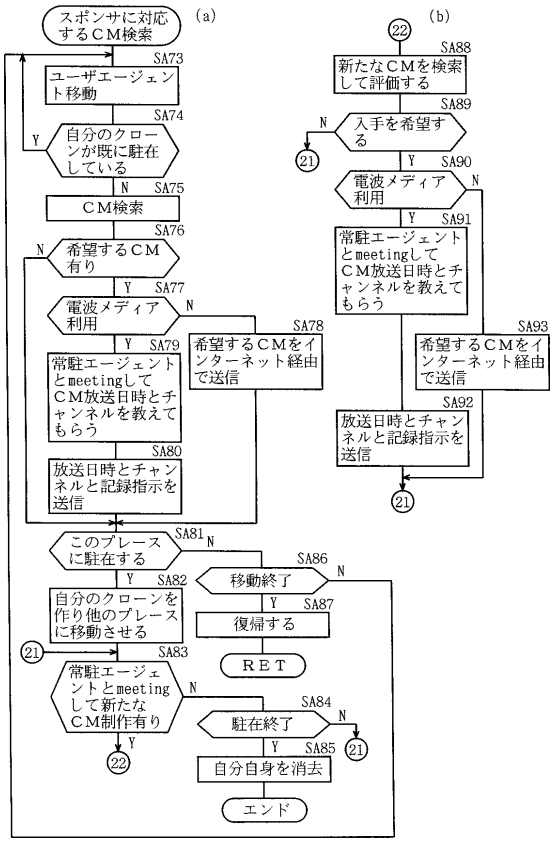
【図８】


スタート
出向指令有り
移動先に移動
ユーザエージェントとmeetingして入手希望高額コンテンツを通知してもらうとともに、必要なユーザプロフィール情報を教えてもらう
入手希望高額コンテンツの評価を行なう
入手希望高額コンテンツは違法なコンテンツ
違法なため購入できない旨の評価をユーザエージェントに知らせる
警察に通報
違法コンテンツを第三者機関に持ち帰り証拠として保管
自分自身を消去する
エンド
E_{SK1}(SI)を通知された
第三者機関常駐エージェントとmeetingしてSK1を教えてもらう
$D_{SK1}\{E_{SK1}(SI)\}$を演算してSIを記憶
ユーザ認証必要
E_{SKU}(NM)を演算してユーザエージェントに知らせる
E_{PK3}(KC)受信
$D_{PK3}\{E_{PK3}(KC)\}$
KC の評価を行う
入手希望コンテンツは違法なコンテンツ
評価HK に対しE_{SK3}(HK)を演算する
E_{SK3}(HK)を移動先へ送信

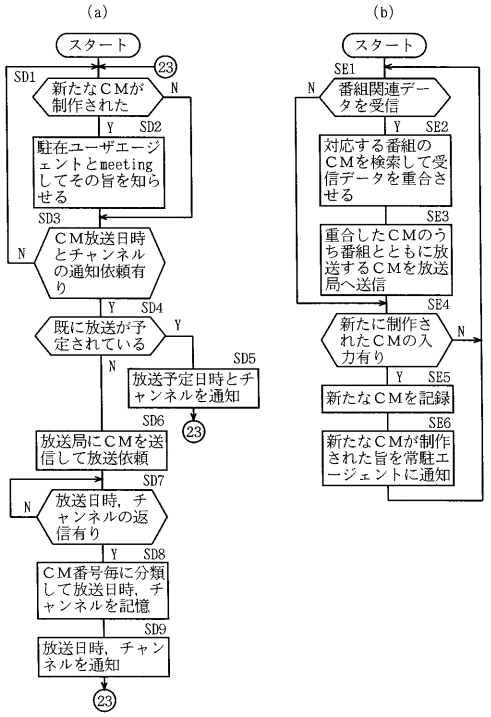
【図９】


52
51
14
50
53
13
54
WWW サーバ
情報処理コンピュータ
55
10
26
59
56
58
57

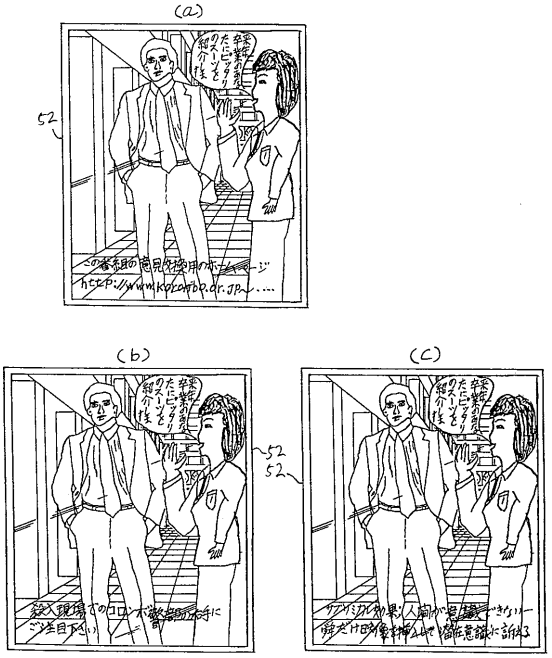
【図１０】


スポンサに対応するCM検索
(a)
ユーザエージェント移動
自分のクローンが既に駐在している
CM検索
希望するCM有り
電波メディア利用
常駐エージェントとmeetingしてCM放送日時とチャンネルを教えてもらう
希望するCMをインターネット経由で送信
放送日時とチャンネルと記録指示を送信
このプレースに駐在する
自分のクローンを作り他のプレースに移動させる
常駐エージェントとmeetingして新たなCM制作有り
移動終了
復帰する
RET
駐在終了
自分自身を消去
エンド
(b)
新たなCMを検索して評価する
入手を希望する
電波メディア利用
常駐エージェントとmeetingしてCM放送日時とチャンネルを教えてもらう
希望するCMをインターネット経由で送信
放送日時とチャンネルと記録指示を送信

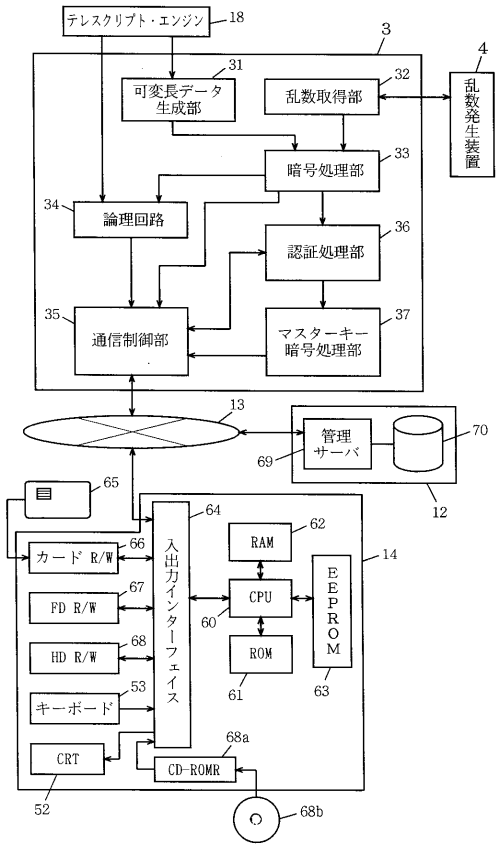
【図１１】



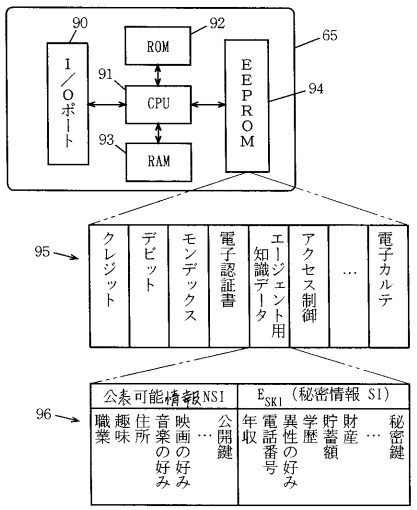
【図１２】



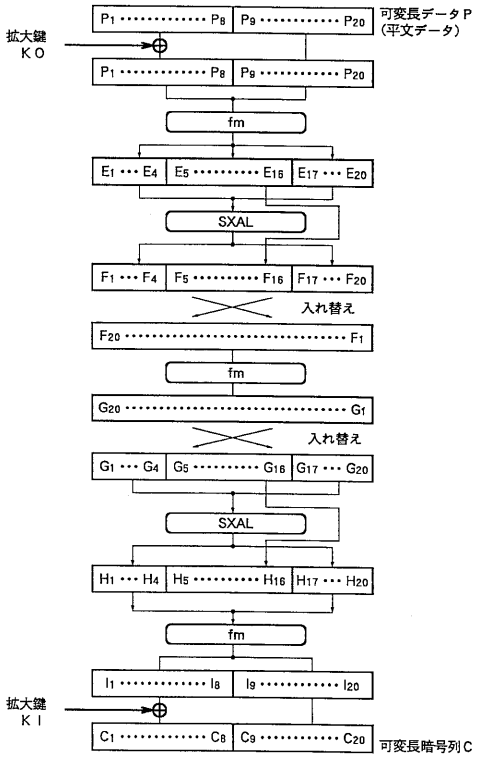
【図１３】



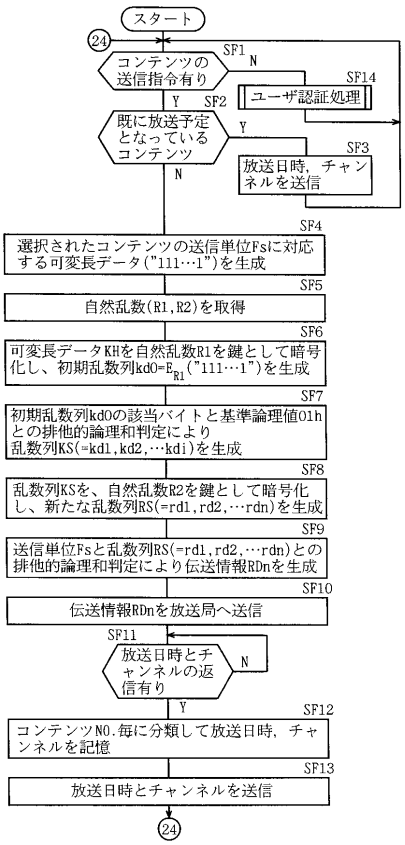
【図１４】



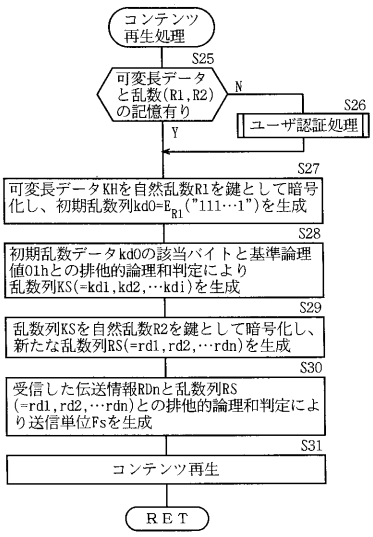
【図１５】



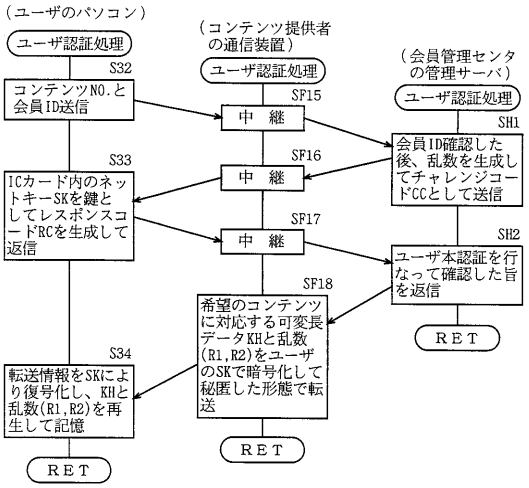
【図１６】



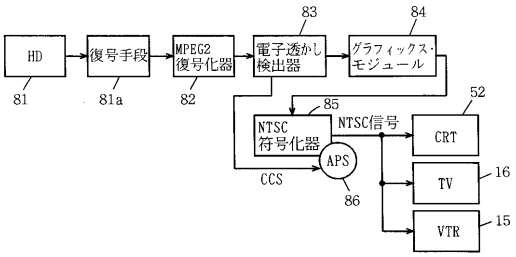
【図１７】



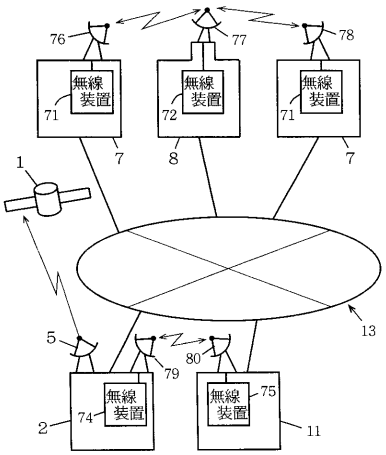
【図１８】



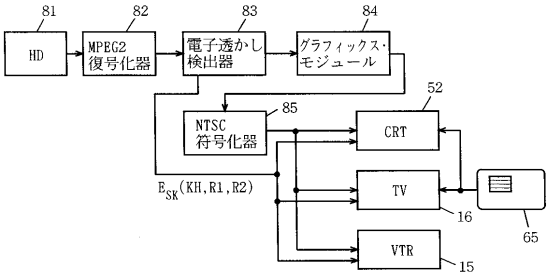
【図１９】



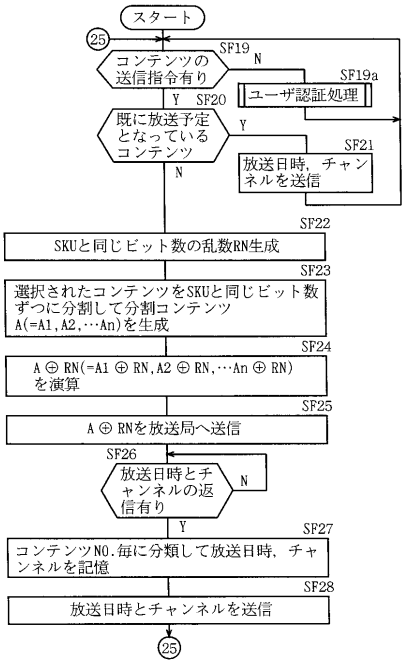
【図２０】



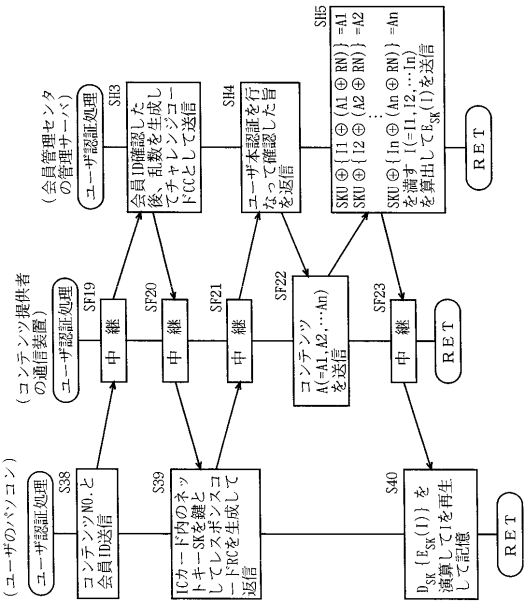
【図２１】



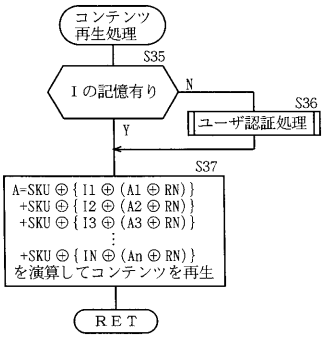
【図２２】



【図２３】



【図２４】



フロントページの続き

(74)代理人 100124523
弁理士 佐々木 眞人
(72)発明者 鳥飼 將迪
神奈川県横浜市青葉区美しが丘５丁目３５番地の２ 株式会社ローレルインテリジェントシステムズ内
(72)発明者 藤井 幹雄
神奈川県横浜市青葉区美しが丘５丁目３５番地の２ 株式会社ローレルインテリジェントシステムズ内
(72)発明者 塚本 豊
神奈川県横浜市青葉区美しが丘５丁目３５番地の２ 株式会社ローレルインテリジェントシステムズ内

審査官 殿川 雅也

(56)参考文献 FARMER, W., M., et al., Security for Mobile Agents: Issues and Requirements, Proceedings 19th National Information System Security Conference, １９９６年１０月, pp. 591 - 597
PEINE, H., et al., The Architecture of the Ara Platform for Mobile Agents, Lecture Notes in Computer Scinence, ドイツ, Springer Berlin, Mobile Agents, １９９７年, Vol. 1219/1997, pp. 50 - 61
PHAM, V. A., et al., Mobile Software Agents: An Overview, IEEE Communication Magazine, IEEE, １９９８年 7月, Vol 36, Issue 7, pp. 26 - 37

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ９／４６ － ９／５４
Ｇ０６Ｑ １０／００
Ｇ０６Ｑ ３０／００
Ｇ０６Ｑ ５０／００