

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4583285号  
(P4583285)

(45) 発行日 平成22年11月17日(2010.11.17)

(24) 登録日 平成22年9月10日(2010.9.10)

(51) Int.Cl. F I  
**HO4N 7/173 (2006.01)** HO4N 7/173 610Z  
**GO6F 9/46 (2006.01)** GO6F 9/46 420B

請求項の数 9 (全 49 頁)

(21) 出願番号	特願2005-300427 (P2005-300427)	(73) 特許権者	502178126
(22) 出願日	平成17年10月14日(2005.10.14)		石井 美恵子
(62) 分割の表示	特願2004-29384 (P2004-29384) の分割		岡山県倉敷市羽島221番地の4
原出願日	平成10年4月14日(1998.4.14)	(74) 代理人	100064746
(65) 公開番号	特開2006-67619 (P2006-67619A)		弁理士 深見 久郎
(43) 公開日	平成18年3月9日(2006.3.9)	(74) 代理人	100085132
審査請求日	平成17年10月14日(2005.10.14)		弁理士 森田 俊雄
		(74) 代理人	100109162
			弁理士 酒井 将行
		(72) 発明者	塚本 豊
			京都府京都市下京区松原通東洞院東入本燈 籠町11番地 デリード烏丸東504号室
		審査官	長谷川 素直

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じ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に代わって仕事を実行するための第三者機関によって運用される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け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け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、

前記プロフィール情報は、当該プロフィール情報に対応するユーザ自身によって更新されることを特徴とする、コンテンツ提供システム。

**【請求項 2】**

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じてコンテンツを提供する複数のコンテンツ提供者とからなる当事者に代わって仕事を実行するための第三者機関によって運用される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け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け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、

前記プロフィール情報は、ユーザエージェントがユーザのために仕事を行なったその結果に対するユーザの反応に基づいて更新または補充されることを特徴とする、コンテンツ提供システム。

**【請求項 3】**

前記ユーザエージェントは、機械学習機能を有してい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】**

前記ユーザエージェントは、ユーザが携帯する格納手段に格納された状態で当該ユーザによって携帯されることを特徴とする、請求項 2 または請求項 3 に記載のコンテンツ提供システム。

**【請求項 5】**

前記第三者機関コンピュータは、モバイルエージェントで構成されたユーザエージェントが、前記ユーザのために働くために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状態で知識として保有しており、該ユーザ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性が生じた場合に、前記ユーザエージェントは、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 ~ 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 5 に記載のコンテンツ提供システム。

**【請求項 7】**

前記ユーザエージェントは、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

10

20

30

40

50

することを特徴とする、請求項 6 に記載のコンテンツ提供システム。

【請求項 8】

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 5 ～ 請求項 7 のいずれかに記載のコンテンツ提供システム。

【請求項 9】

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 8 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】

10

【0001】

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に関する。

【背景技術】

【0002】

従来において、たとえば、中立的なネゴシエータを設けて、イニシエータとレスポンドの間の交渉の仲立ちをして提案及び提示を行う、交渉システムがあった（非特許文献 1）。

【非特許文献 1】移動エージェントによる交渉システムの設計，情報処理学会ワークショップ論文集，日本，社団法人情報処理学会，1997年 7月，Vol. 97, No. 2, pp. 557 - 562

20

【発明の開示】

【発明が解決しようとする課題】

【0008】

このシステムの発明の目的は、改良されたコンテンツ提供システムを提供することである。

【課題を解決するための手段】

【0009】

上記の課題を解決するために本発明は以下の手段を採用する。

30

【0010】

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じ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に代わって仕事を実行するための第三者機関によって運用され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、

40

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け取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け取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、

前記プロフィール情報は、当該プロフィール情報に対応するユーザ自身によって更新さ

50

れることを特徴とする。

【0011】

請求項2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じてコンテンツを提供する複数のコンテンツ提供者とからなる当事者に代わって仕事を実行するための第三者機関によって運用され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け取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け取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、

前記プロフィール情報は、ユーザエージェントがユーザのために仕事を行なったその結果に対するユーザの反応に基づいて更新または補充されることを特徴とする。

【0012】

請求項3に記載の本発明は、前記ユーザエージェントは、機械学習機能を有していることを特徴とする。

【0013】

請求項4に記載の本発明は、請求項2または請求項3に記載の発明の構成に加えて、前記ユーザエージェントは、ユーザが携帯する格納手段に格納された状態で当該ユーザによって携帯されることを特徴とする。

【0015】

請求項5に記載の本発明は、請求項1～請求項4のいずれか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、モバイルエージェントで構成されたユーザエージェントが、前記ユーザのために働くために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状態で知識として保有しており、該ユーザ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。

【0016】

請求項6に記載の本発明は、請求項5に記載の発明の構成に加えて、前記ユーザエージェントは、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。

【0017】

請求項7に記載の本発明は、請求項6に記載の発明の構成に加えて、前記ユーザエージェントは、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

10

20

30

40

50

る。

【 0 0 1 8 】

請求項 8 に記載の本発明は、請求項 5 ~ 請求項 7 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。

請求項 9 に記載の本発明は、請求項 1 ~ 請求項 8 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。

。

【 発明の効果 】

10

【 0 0 1 9 】

上記の課題を解決するための手段を採用した結果、ユーザと複数のコンテンツ提供者とからなる当事者に代わって仕事を実行するための第三者機関によって運用され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、第三者機関としての中立性を有する第三者エージェントにより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者に漏洩する不都合も極力防止できる。

【 発明を実施するための最良の形態 】

【 0 0 2 1 】

20

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 1 3 に対し、ユーザ宅 1 7 のパーソナルコンピュータ（以下単にパソコンという）1 4 とコンテンツ提供者 7 と第三者機関 8 と会員管理センター 1 2 と番組関連データ制作者 1 1 とコマーシャルメッセージ（以下単に CM という）制作者 1 0 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。

【 0 0 2 2 】

コンテンツ提供者 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 1 3 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 1 7 のパソコン 1 4 に提供する。コンテンツ提供者 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。

30

【 0 0 2 3 】

ユーザのパソコン 1 4 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。

40

【 0 0 2 4 】

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 1 3 を経由してユーザのパソコン 1 4 に送信する。

【 0 0 2 5 】

50

コンテンツ提供者 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。

【 0 0 2 6 】

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。

10

【 0 0 2 7 】

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。TV 16 は、この VTR 15 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った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替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 VTR 15 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、VTR 15 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、VTR 15 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。

20

【 0 0 2 8 】

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。

30

【 0 0 2 9 】

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。

【 0 0 3 0 】

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。

40

【 0 0 3 1 】

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

50

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。

【0032】

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、コンテンツ提供者 7 のテレクリプト・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)。

【0033】

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。

【0034】

一方、第三者機関 8 のテレクリプト・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じ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。

【0035】

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 の種類に合わせて機能別に複数種類用意しておく必要がある。

【0036】

コンテンツ提供者 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者 7 のプレース 24 にまで出向してもらう。

【0037】

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

10

20

30

40

50

せる。

【 0 0 3 8 】

第三者機関エージェント 2 9 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 2 6 から教えてもらわなければならない場合は、コンテンツ提供者 7 のプレース 2 4 上でその秘密情報をユーザエージェント 2 6 が第三者機関エージェント 2 9 に通知すれば、その秘密情報がコンテンツ提供者 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 2 6 は、前述したような秘密情報 S I（図 1 4 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 2 6 はコンテンツ提供者 7 のプレース 2 4 に移動しただけでは、その秘密情報 S I がコンテンツ提供者 7 に知ら 10  
れてしまうことはない。しかし、コンテンツ提供者 7 のプレース 2 4 上において、第三者機関エージェント 2 9 が解読できるように暗号化秘密情報 S I を復号化して平文の形で第三者機関エージェント 2 9 に教えた場合には、その平文の秘密情報 S I がコンテンツ提供者 7 に知られる可能性が生ずる。

【 0 0 3 9 】

そこで、このような秘密情報 S I 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 2 6 が第三者機関 8 のテレスク립ト・エンジン 2 2 のプレース 2 5 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 2 8 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 20  
第三者機関エージェント 2 9 とユーザエージェント 2 6 とが meeting して、検索に必要な秘密情報 S I を通知する（図 2（d）参照）。

【 0 0 4 0 】

その後、ユーザエージェント 2 6 がコンテンツ提供者 7 のプレース 2 4 に復帰し、常駐エージェント 2 7 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 2 5 に転送してもらい、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 30  
エージェント 2 9 がユーザエージェント 2 6 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 2 4 上のユーザエージェント 2 6 に通知する。このようにすれば、ユーザエージェント 2 6 が知識として保有している秘密情報 S I がコンテンツ提供者 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 2 5 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。

【 0 0 4 1 】

図 3 は、ユーザのパソコン 1 4 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 1 4 の制御回路は、図 1 2 に基づいて後述する。

【 0 0 4 2 】

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 1 4 が受信したり、またはインターネット 1 3 40  
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 S 2 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 V T R 1 5 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 S 3 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 S 4 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。

【 0 0 4 3 】

ユーザからエージェントへの指示がない場合には、S 5 に進み、コンテンツの再生指示 50



があったか否かの判断がなされる。ない場合にはS 6に進み、鍵S K 1の送信要求があったか否かの判断がなされる。この鍵S K 1は、前述した暗号化されている秘密情報S I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2 8が必要に応じてユーザのパソコン1 4に対し送信要求を出すものである。S K 1の要求がない場合にはS 7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1 4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1 4に出す場合がある。

**【 0 0 4 4 】**

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S 8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1 0のプレイス2 5に移動してCMを検索し、希望するCMが見つければ、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1 4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S 8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S 9に進み、その他の処理がなされてS 1に戻る。

**【 0 0 4 5 】**

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1 3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、S 1によりYESの判断がなされてS 10に進み、ユーザのパソコン1 4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。

**【 0 0 4 6 】**

S 2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S 11に進み、放送されるチャンネル周波数にチューニングし、S 12により、放送コンテンツを受信してV T R 1 5に記録する処理がなされる。次にS 13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S 1に戻るが、含む場合にはS 14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1 0のプレイス5 8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V T R 1 5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。

**【 0 0 4 7 】**

編集時間がある場合にはS 15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S 1に戻る。編集時間がない場合にはS 16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に切替えて放映する制御を行なってS 1に戻る。

**【 0 0 4 8 】**

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S 3によりYESの判断がなされてS 17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。

**【 0 0 4 9 】**

ユーザがキーボード5 3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、S 18に進み、パソコン1 4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。

**【 0 0 5 0 】**

ユーザがキーボード5 3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S 5によりYESの判断がなされてS 19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S 20によるコンテンツ再生処理を行なった後、S 21によるコンテンツの出力処理がなされてC R T 5 2やT V 1 6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S 20の処理を行なうことなく直接S 21に進み、コンテンツ出力処理がなされる。S 26のコンテンツ

10

20

30

40

50

再生処理の詳細は、図 17 に基づいて後述する。

【 0 0 5 1 】

鍵  $SK_1$  の送信要求があった場合には  $S_6$  により  $YES$  の判断がなされて  $S_{22}$  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  $SK_3$  でそれを暗号化する処理すなわち  $E_{SK_3}(CH)$  を算出してレスポンスデータ  $RES$  として返信する ( $SB_{12}$ ,  $SB_{23b}$  参照)。

【 0 0 5 2 】

このレスポンスデータ  $RES$  を受信したパソコン 14 は、 $S_{22a}$  により  $YES$  の判断がなされて  $S_{22b}$  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  $D_{PK_3}(RES)$  を演算し、その演算結果と  $S_{22}$  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  $SK_1$  の要求があったのであれば、 $CH = D_{PK_3}(RES)$  となるはずであるために、その場合には  $S_{22c}$  に進み、鍵  $SK_1$  を第三者機関 8 の公開鍵  $PK_3$  を用いて暗号化する演算すなわち  $E_{PK_3}(SK_1)$  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、 $S_{22b}$  より一致しないと判断された場合には  $S_{22c}$  の送信処理を行なうことなく  $S_1$  に戻る。

10

【 0 0 5 3 】

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  $S_{23}$  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。

20

【 0 0 5 4 】

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  $S_8$  により  $YES$  の判断がなされて  $S_{24}$  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。

【 0 0 5 5 】

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。 $SA_1$  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  $SA_2$  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  $SA_3$  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  $SA_4$  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  $SA_5$  に進み、その他の処理を行なった後  $SA_1$  に戻る。

30

【 0 0 5 6 】

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、 $SA_6$  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  $SA_7$  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利用して評価を行なう。

40

【 0 0 5 7 】

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  $SA_8$  に進み、サイト紹介情報のみで評価を行なう。次に  $SA_9$  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  $SA_1$  に戻る。一方所定値以上である場合には  $SA_{10}$  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  $SA_1$  に戻る。

【 0 0 5 8 】

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  $S_{17}$  によりユーザエー

50

ジェントに知らせた場合には、S A 2 により Y E S の判断がなされて S A 1 1 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 9 6 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、S A 1 2 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 S A 1 に戻るが、所定値以上の場合には S A 1 3 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 V T R 1 5 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。

**【 0 0 5 9 】**

S A 1 4 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 S A 1 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を示す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、S A 1 5 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断を行なう。自動記録しないと判断された場合には S A 1 6 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 S A 1 に戻る。一方、自動記録すると判断された場合には S A 1 7 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。

**【 0 0 6 0 】**

次に S A 1 8 に進み、パソコン 1 4 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、S 7 により、Y E S の判断がなされて S 2 3 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、S 2 により即座に Y E S 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 S 1 7 以降で行なわれる。

**【 0 0 6 1 】**

次に S A 1 9 に進み、指示を出した番組コンテンツに C M があるか否かの判断がなされる。ない場合には S A 1 6 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。

**【 0 0 6 2 】**

一方、S A 1 9 により、指示を出した番組コンテンツに C M があると判断された場合には S A 2 0 に進み、番組スポンサーに対応する C M を検索する処理がなされた後 S A 1 6 に進む。この S A 2 0 のスポンサーに対応する C M 検索処理は、後述する図 1 0 に基づいて説明する。

**【 0 0 6 3 】**

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 S 1 8 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 S A 3 により Y E S の判断がなされて S A 2 1 に進む。S A 2 1 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 S A 2 2 に進み、推薦番組リストを C R T 5 2 または T V 1 6 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 S A 2 3 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。S A 2 3 より Y E S の判断がなされた場合には S A 2 4 に進み、自動記録番組リストを C R T 5 2 または T V 1 6 により表示させる制御がなされる。

**【 0 0 6 4 】**

自動記録番組リストの閲覧指示でなかった場合には S A 2 5 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 1 4 に送信するのであり、その検索結

10

20

30

40

50

果の閲覧指示であった場合にはS A 2 6により、コンテンツ検索結果をC R T 5 2またはT V 1 6により表示させる制御がなされる。

【 0 0 6 5 】

コンテンツ検索結果の閲覧指示でなかった場合にはS A 2 7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。S A 2 2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S A 2 7によりY E Sの判断がなされてS A 2 9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1 4に出す処理がなされる。その結果、パソコン1 4では、S 7によりY E Sの判断が行なわれてS 2 3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、S 2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S 1 1以降のコンテンツの記録処理が実行されることとなる。

10

【 0 0 6 6 】

次にS A 3 0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S A 1 9に進む。

【 0 0 6 7 】

推薦番組記録指示でなかった場合にはS A 2 8に進み、ユーザエージェントがその他の処理を実行してS A 1に戻る。

【 0 0 6 8 】

S A 3によりN Oの判断がなされた場合にはS A 4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S A 5に進み、その他の処理を実行した後S A 1に戻る。一方、移動時刻が来た場合にはS A 5 aに進み、エージェント移動処理を実行した後S A 1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。

20

【 0 0 6 9 】

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。S A 3 1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S A 1 0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1 4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。

30

【 0 0 7 0 】

次にS A 3 2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2 7とmeeting(打合せ)して、種々の必要な情報交換を行なう。次にS A 3 3に進み、そのmeetingの結果に基づいて、データベース1 9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S A 3 4に進み、その無料コンテンツを検索する処理を行ない、S A 3 5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S A 3 6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S A 3 6に進む。

40

【 0 0 7 1 】

S A 3 6では、データベース1 9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S A 3 8に進み、移動先エージェント2 7とmeetingして、選択したコンテンツのパソコン1 4への送信指令を出してもらう。次にS A 3 9に進み、検索結果をパソコン1 4に送信する処理を行ない、S A 4 0に進み、移動が終了したか否かの判断がなされる。S A 1 0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S A 4 0 aに進み、自分自身を消去して終了する。一方、S A 4 0により移動終了でないと判断された場合には再びS A 3 1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。

50

## 【 0 0 7 2 】

一方、S A 3 6 により有料コンテンツがあると判断された場合にはS A 3 7 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S A 4 1 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S A 4 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S A 3 9 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1 4 へ送信する。高額有料コンテンツがある場合にはS A 4 3 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S A 3 9 に進むが、入手したいものがある場合にはS A 4 4 に進む。

10

## 【 0 0 7 3 】

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1 4 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、S A 4 4 により、その入手希望高額コンテンツの検索に秘密情報(S I)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S A 4 5 に進み、移動先エージェント2 7 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2 7 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2 8 と交信し、ユーザエージェント2 6 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者7 のブレース2 4 に出向してくれば、S A 4 6 により、Y E S の判断がなされてS A 6 4 へ進む。

20

## 【 0 0 7 4 】

S A 6 4 では、出向してきた第三者機関エージェント2 9 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2 9 は、必要なプロフィール情報9 6 をユーザエージェント2 6 から聞き出してそれに基づいてデータベース1 9 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2 6 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S A 6 6 により、ユーザエージェント2 6 が第三者機関エージェント2 9 に対し検索結果の評価を知らせてもらう。

30

## 【 0 0 7 5 】

次にS A 6 7 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2 6 が行なう。購入しない場合にはS A 3 9 に進むが、購入する場合にはS A 6 8 に進み、移動先エージェント2 7 とmeeting して、オーダ情報O I と支払い指示P I との暗号化情報 $E_{PK3}(OI)$ 、 $E_{PK3}(PI)$ を受取る。このオーダ情報O I 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P I とは、たとえばクレジットが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O I とP I とを第三者機関8 の公開鍵P K 3 で暗号化した情報を移動先エージェント2 7 からユーザエージェント2 6 が受取る。

40

## 【 0 0 7 6 】

次にS A 6 9 に進み、その受取った情報とともに第三者機関8 のブレース2 5 へ移動する。次にS A 7 0 により、第三者機関常駐エージェント2 8 とmeeting して(図2 (c)参照)、ユーザの秘密鍵S K U をユーザの鍵S K 1 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2 8 に知らせるとともに、秘密情報S I の復号鍵S K 1 をユーザのパソコン1 4 から取り寄せてもらう依頼を行なう。

## 【 0 0 7 7 】

第三者機関常駐エージェント2 8 は、ユーザのパソコン1 4 からS K 1 を受取ってその

50

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。

**【0078】**

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。

**【0079】**

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認、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。

**【0080】**

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。

**【0081】**

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。

**【0082】**

次にSA54では、たとえばコンテンツ提供者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。

**【0083】**

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

10

20

30

40

50

されて S A 5 7 に進み、その受取ったデータを第三者機関の公開鍵 P K 3 で復号化する処理すなわち  $D_{PK3} \{ E_{SK3} (HK) \}$  を演算して、評価 H K を再生する処理を行なう。

【 0 0 8 4 】

次に S A 5 8 へ進み、再生された評価 H K に基づいて有料コンテンツを購入するか否かの判断が行なわれ、購入しない場合には S A 5 9 により処理完了した旨を第三者機関 8 へ通知した後 S A 3 9 へ進む。一方、購入する場合には S A 6 0 へ進み、移動先エージェント 2 7 と meeting して、オーダ情報 O I と支払い指示 P I との暗号情報  $E_{PK3} (O I)$  ,  $E_{PK3} (P I)$  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 2 8 は、前述と同様に、 $E_{SKU} (O I, P I)$  を生成し、それを移動先のユーザエージェント 2 6 へ送信する。その結果、S A 6 1 により Y E S の判断がなされて S A 6 2 へ進み、移動先エージェント 2 7 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 S A 6 3 に進み、処理完了した旨を第三者機関 8 へ通知した後、S A 3 9 へ進む。

【 0 0 8 5 】

前述した  $E_{SKU} (O I, P I)$  が、いわゆる S E T (Secure Electronic Transaction) で規定されているオー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。

【 0 0 8 6 】

図 7 は、第三者機関常駐エージェント 2 8 の動作を示すフローチャートである。S B 1 により、出向依頼 (派遣依頼) があつたか否かの判断がなされ、ない場合には S B 2 に進み、ユーザエージェント 2 6 が第三者機関 8 のプレース 2 5 に来たか否かの判断がなされ、来ていない場合には S B 3 に進み、ユーザエージェント 2 6 から処理完了の旨の通知があつたか否かの判断がなされ、ない場合には S B 4 へ進み、移動先エージェント 2 7 から  $E_{PK3} (O I)$  ,  $E_{PK3} (P I)$  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 S B 1 へ戻る。

【 0 0 8 7 】

ユーザエージェント 2 6 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 2 7 に対し行ない移動先エージェント 2 7 が出向依頼があつた旨と出向依頼をしたユーザエージェント 2 6 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 2 8 に通知すれば、S B 5 に進み、第三者機関常駐エージェント 2 8 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 2 3 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 2 6 の種類に合致する最適な第三者機関エージェント 2 9 を検索して S B 6 により、その検索された第三者機関エージェント 2 9 に出向指令を出す処理がなされて、S B 1 に戻る。

【 0 0 8 8 】

前述した S A 4 9 または S A 6 9 により、ユーザエージェント 2 6 が第三者機関 8 のプレース 2 5 に来た場合には、S B 2 により Y E S の判断がなされて S B 7 に進み、ユーザエージェント 2 6 と meeting する。そして必要な種々の情報交換を行ない、S B 8 に進み、ユーザエージェント 2 9 が来た目的が、第三者機関エージェント 2 9 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 2 6 が S A 4 9 に基づいて第三者機関 8 のプレース 2 5 に来たのであれば、S B 8 により Y E S の判断がなされて S B 9 に進み、第三者機関エージェント 2 9 を検索する処理がなされる。

【 0 0 8 9 】

次に S B 1 0 に進み、ユーザエージェント 2 6 の出所すなわちパソコン 1 4 を呼出し、秘密情報 S I の暗号化データを復号化するための鍵 S K 1 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、S K 1 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 C H として返信する。そのチャレンジデータ C H を受信した第三者機関常駐エージェントは、S B 1 1 により Y E S の判断がなされて S B 1 2 に進み、 $E_{SK3} (C H)$  をレスポンスデータ R E S としてパソコン 1 4 へ送信する。

【 0 0 9 0 】

10

20

30

40

50

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、SB14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。

【0091】

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。

【0092】

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、オーダー情報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。

【0093】

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。

【0094】

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。

【0095】

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 $E_{SKU}(OI', PI')$ がオーダー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

10

20

30

40

50



処理がなされた後 S B 1 へ戻る。

【 0 0 9 6 】

図 8 は、第三者機関エージェント 2 9 の動作を示すフローチャートである。S C 1 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 S C 2 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 S C 1 へ戻る。

【 0 0 9 7 】

この S C 1 , S C 2 のループの巡回途中で、第三者機関常駐エージェント 2 8 から出向指令を任命されれば ( S B 6 参照 )、S C 1 により Y E S の判断がなされて S C 3 へ進み、たとえばコンテンツ提供者 7 のプレース 2 4 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 2 9 をデータベース 2 3 内に残したままその第三者機関エージェント 2 9 のクローンを移動先のプレース 2 4 へ転送する処理である。次に S C 4 に進み、移動先のプレース 2 4 上において、ユーザエージェント 2 6 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 9 6 ( 図 1 4 参照 ) を教えてもらう処理が行なわれる ( S A 6 4 参照 )。このユーザエージェント 2 6 から教えてもらうユーザのプロフィール情報 9 6 は、公表可能情報 N S I ( 図 1 3 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 2 5 上でのユーザプロフィール情報のやり取りではなく、情報提供者 7 のプレース 2 4 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 N S I に限定されるのである。

【 0 0 9 8 】

次に S C 5 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 9 6 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 S C 6 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。

【 0 0 9 9 】

違法なコンテンツでないと判断された場合には S C 1 0 へ進み、第三者機関エージェント 2 9 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 S C 7 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 2 6 に知らせ、S C 8 により、違法である旨の通報を警察に行なう。次に S C 9 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 S C 1 0 へ進む。

【 0 1 0 0 】

S C 1 , S C 2 のループの巡回途中で、ユーザエージェント 2 6 により、ユーザのプロフィール情報のうちの秘密情報 S I を暗号化した情報である  $E_{SK1}(SI)$  が通知された場合 ( S A 5 1 参照 ) には、S C 2 により Y E S の判断がなされて S C 1 1 に進み、第三者機関常駐エージェント 2 8 と meeting して、復号化するための鍵 S K 1 を教えてもらう処理がなされる。次に S C 1 2 へ進み、 $D_{SK1}\{E_{SK1}(SI)\}$  を演算して秘密情報 S I を再生して記憶する処理がなされる。

【 0 1 0 1 】

次に S C 1 3 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 S C 1 5 へ直接進むが、必要な場合には S C 1 4 へ進む。S C 1 4 では、 $E_{SKU}(NM)$  を演算してユーザエージェント 2 6 へ知らせる処理がなされる。この N M は、移動先エージェント 2 7 からユーザエージェント 2 6 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 ( S A 4 8 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 2 6 より第三者機関 8 のプレース 2 5 に持込まれ、第三者機関常駐エージェント 2 8 により復号化されて再生された認証対象メッセージ N M が第三者機関エージェント 2 9 に知らされる。第三者機関エージェント 2 9 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。

【0102】

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。

10

【0103】

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

20

【0104】

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。

【0105】

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。

30

【0106】

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。

【0107】

40

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。

【0108】

50

一方、電波メディアを利用する場合にはS A 7 9へ進み、常駐エージェント5 9とmeetingして、希望するC M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S A 8 0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1 3を経由してパソコン1 4へ送信する処理がなされる。

【0 1 0 9】

次にS A 8 1へ進み、ユーザエージェント2 6がこのC Mスペース5 8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S A 8 6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C M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S A 7 3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C M作成者1 0を移動し終わった場合にはS A 8 7へ進み、ユーザエージェント2 6がユーザのパソコン1 4へ復帰する処理がなされて制御が終了する。

10

【0 1 1 0】

一方、ユーザエージェント2 6がこのC Mスペース5 8に駐在すると判断した場合にはS A 8 2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C M作成者1 0のC Mスペースに移動させる処理がなされる。次にS A 8 3へ進み、C Mスペース5 8に駐在することとなったユーザエージェント2 6が、常駐エージェント5 9とmeetingして、新たなC M作成があったか否かの判断がなされる。C M制作者1 0が新たなC Mを制作してデータベース5 6に記憶させれば新たなC Mが制作された旨を常駐エージェント5 9がC Mスペース5 8に駐在しているユーザエージェント2 6に知らせるのであり、その知らせがあれば、S A 8 3によりY E Sの判断がなされてS A 8 8へ進む。

20

【0 1 1 1】

S A 8 8では、C Mスペース5 8に駐在しているユーザエージェント2 6がその新たなC Mを検索して評価する処理がなされる。次にS A 8 9へ進み、評価の結果その新たなC M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S A 8 3へ進むが、希望する場合にはS A 9 0へ進み、希望するC Mのユーザ宅1 7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、S A 9 3により、希望するC Mをインターネット1 3経由でパソコン1 4へ送信する処理がなされた後S A 8 3へ進む。一方、電波メディアを利用する場合にはS A 9 1へ進み、常駐エージェント5 9とmeetingして、入手希望のC Mの放送日時とチャンネルを教えてもらい、S A 9 2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1 3経由でパソコン1 4へ送信する処理がなされた後S A 8 3へ進む。

30

【0 1 1 2】

S A 8 3により、新たなC M作成がないと判断された場合にはS A 8 4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2 6の駐在をまだ続行させる場合にはS A 8 3へ進むが、駐在を終了させる場合にはS A 8 5へ進み、駐在しているユーザエージェント2 6自身を消去する処理がなされて制御が終了する。

【0 1 1 3】

図1 1 ( a )はC Mスペース5 8上の常駐エージェント5 9の動作を示すフローチャートであり、図1 1 ( b )は、C M制作者1 0の情報処理コンピュータ5 5の制御動作を示すフローチャートである。

40

【0 1 1 4】

まずC Mスペース5 8に常駐している常駐エージェント5 9の動作を説明する。

S D 1により、新たなC M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S D 3に進むが、制作されている場合にはS D 2に進む。S D 2では、C Mスペース5 8に駐在しているユーザエージェント2 6とmeetingして、新たなC Mが制作された旨を知らせる処理がなされる。次にS D 3に進み、C M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S D 1に戻る。一方、前述したS A 7 9またはS A 9 1に基づいてユーザエージェント2 6がC M放送日時とチャンネルの通知依頼を行なった場合には、S D 3によりY E Sの判断がなされてS D 4に進む。

【0 1 1 5】

50

S D 4では、通知依頼のあったC M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、S D 5に進み、その放送予定日時とチャンネルをC Mスペース5 8にいるユーザエージェント2 6に通知する処理がなされた後S D 1に戻る。

【0 1 1 6】

一方、放送が予定されていない場合にはS D 6に進み、放送局2にC Mを送信して放送依頼を行なう処理がなされる。次にS D 7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C M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C M制作者1 0のC Mスペース5 8の常駐エージェント5 9にその旨を送信する。すると、S D 7によりY E Sの判断がなされてS D 8に進み、C M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S D 9に進み、放送日時とチャンネルをC Mスペース5 8上のユーザエージェント2 6に通知する処理がなされた後S D 1に戻る。

【0 1 1 7】

次に情報処理コンピュータ5 5の動作を説明する。S E 1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S E 4へ進む。図1で説明したように、番組関連データ制作者1 1からC M制作者1 0に番組関連データが送信されて来れば、S E 1によりY E Sの判断がなされてS E 2に進み、対応する番組のC Mをデータベース5 6から検索してそのC M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5 6内のC Mは、番組関連データが重合されたC Mデータとなる。また同じC Mでも、どの番組に対し放映されるC Mかによって番組関連データが異なるため、同じC M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C Mデータがデータベース5 6に格納されることとなる。その結果、前述したS D 6に従って放送局に送信されるC Mは、そのC Mに対応する番組の番組関連データが重合されたC Mデータとなる。また、ユーザエージェント2 6が常駐エージェント5 9に対しC M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C Mであるかを通知する。常駐エージェント5 9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C Mデータをデータベース5 6から検索して放送局2へ送信する。なお、データベース5 6を2分割して、C Mのみが格納されたC M専用データベースと番組関連データ制作者1 1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2 6からのC M放送日時とチャンネルの通知依頼を受けたときに、そのC M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5 9が検索し、ユーザエージェント2 6により検索されたC Mデータと常駐エージェント5 9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S E 3に進み、重合したC Mのうち番組とともに放送するC M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C MがこのS E 3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C Mが放送される。

【0 1 1 8】

次にS E 4に進み、新たに制作されたC Mのデータベース5 6への入力があったか否かの判断がなされ、ない場合にはS E 1に戻る。一方、入力があった場合にはS E 5に進み、その新たなC Mをデータベース5 6に記録する処理がなされ、次にS E 6に進み、その新たなC Mが制作された旨を常駐エージェント5 9に通知する処理がなされた後S E 1に戻る。

【0 1 1 9】

図1 2は、前述したS E 2により番組関連データが重合されたC Mを受信してユーザ宅1 7のパソコン1 4のC R T 5 2またはT V 1 6によりそのC Mを放映した画面図である。この図1 2では、パソコン1 4のC R T 5 2によりC Mを放映した画面図が示されている。この図1 2の場合には、コロ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。

【0120】

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 coronab 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。

10

【0121】

図13は、図2に示したコンテンツ提供者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、およびマスターキー暗号処理部37を備えている。

【0122】

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。

20

【0123】

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(イクスクループオア)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。

30

【0124】

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。マスターキー暗号処理部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。

40

【0125】

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。

【0126】

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

50

るROM 61, CPU 60のワーキングエリアとしてのRAM 62、ならびに電氣的に記憶データの消去が可能なEEPROM 63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。

【0127】

入出力インターフェイス64には、カードリーダーライタ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ーライタ66, 入出力インターフェイス64を介してCPU 60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)ディスクリーダーライタ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。

10

【0128】

入出力インターフェイス64にはハードディスクリーダーライタ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CPU 60へ入力される。入出力インターフェイス64にはCRT 52が接続されており、CRT表示用制御信号がCPU 60から入出力インターフェイス64を介してこのCRT 52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-ROM 68bの記録情報が読取可能となる。このCD-ROM 68b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-ROM 68b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-ROM 68b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。

20

【0129】

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CPU 91と、制御用のプログラムを記憶しているROM 92と、CPU 91のワーキングエリアとしてのRAM 93と、電氣的に記憶データの消去が可能なEEPROM 94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。ROM 92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。

30

【0130】

そして、たとえばEEPROM 94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(預金自動引き落とし), 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。

40

【0131】

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。

【0132】

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-ROM 68bに記録されているユーザエージェント26をCD-ROMリーダ68aで読取らせ、さ

50

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。

10

## 【0133】

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。

## 【0134】

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。

20

## 【0135】

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。

## 【0136】

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。

30

## 【0137】

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。

40

## 【0138】

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

50

、ユーザ認証処理を行なった後 S F 1 へ戻る。この S F 1 , S F 1 4 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 1 8 からコンテンツの送信指令があった場合には、S F 2 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 1 4 へ送信した後 S F 1 へ戻る。

【 0 1 3 9 】

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 S F 4 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  $F_s$  に対応する可変長データ ( 1 1 1 ... 1 ) を生成する。次に S F 5 へ進み、乱数発生装置 4 からたとえば 2 つの自然乱数 (  $R_1$  ,  $R_2$  ) 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  $R_1$  を鍵 ( 暗号鍵 ) として前述した S X A L / M B A L により暗号化し、初期乱数列  $k d_0$  ( 図 1 5 の下段の可変長暗号列 C に相当 ) を生成する。次に、S F 7 へ進み、初期乱数列  $k d_0$  の該当バイトと基準論理値  $0 1 h$  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  $K S$  ( =  $k d_1$  ,  $k d_2$  , ...  $k d_i$  ) を生成する。

【 0 1 4 0 】

ここで  $k d_1$  は  $k d_0$  の 1 バイト目と  $0 1 h$  との排他的論理和 ( イクスクルーシブオア ) の判定結果、 $k d_2$  は  $k d_0$  の 2 バイト目と  $0 1 h$  との排他的論理和判定結果、... である。さらに乱数列  $K S$  を次の自然乱数  $R_2$  を鍵 ( 暗号鍵 ) として S X A L / M B A L により暗号化し、新たな乱数列  $R S$  ( =  $r d_1$  ,  $r d_2$  , ...  $r d_n$  : 可変長暗号列 ) を生成する ( S F 8 ) 。ここで  $r d_1$  は  $k d_1$  の暗号処理結果、 $r d_2$  は  $k d_2$  の暗号処理結果、 $r d_n$  はデータ量調整されたデータ  $k d_i$  の暗号結果、... である。

【 0 1 4 1 】

次に S F 9 へ進み、前述のようにして生成された乱数列  $R S$  と送信単位  $F_s$  との排他的論理和条件を判定して伝送情報  $R D n$  を生成し、S F 1 0 へ進み、生成された伝送情報  $R D n$  を放送局 2 へ送信する。放送局 2 では、伝送情報  $R D n$  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者 7 へ返信してくる。その返信があれば S F 1 1 により Y E S の判断がなされて S F 1 2 へ進み、コンテンツ N O . 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 S F 1 3 に進み、その放送日時とチャンネルをユーザのパソコン 1 4 へ送信する処理がなされた後 S F 1 へ戻る。

【 0 1 4 2 】

図 1 7 は、ユーザのパソコン 1 4 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 S 2 0 の具体的なフローチャートである。S 2 5 により、可変長データと乱数 (  $R_1$  ,  $R_2$  ) 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 1 4 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者 7 からユーザのパソコン 1 4 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 S 2 6 へ進み、まずユーザ認証処理 ( 図 1 8 に基づいて後述する ) を行なった後、S 2 7 へ進む。

【 0 1 4 3 】

S 2 7 では、可変長データを最初の自然乱数  $R_1$  により S X A L / M B A L により暗号化し、初期乱数列  $k d_0$  を生成する。次に、S 2 8 へ進み、初期乱数列  $k d_0$  の該当バイトと基準論理値  $0 1 h$  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  $K S$  ( =  $k d_1$  ,  $k d_2$  , ...  $k d_i$  ) を生成する。次に S 2 9 へ進み、乱数列  $K S$  を次の自然乱数  $R_2$  を鍵として S X A L / M B A L により暗号化し、新たな乱数列  $R S$  ( =  $r d_1$  ,  $r d_2$  , ...  $r d_n$  ) を生成する。前記初期乱数列  $k d_0$ 、乱数列  $k s$  ,  $r s$  は、それぞれ図 1 6 に基づいて説明したものと同一のものである。

【 0 1 4 4 】

このようにして生成された乱数列  $R S$  と受信した伝送情報  $R D n$  との排他的論理和条件

10

20

30

40

50



を判定して送信単位  $F_s$  を生成し ( S 3 0 )、コンテンツを再生する ( S 3 1 )。

【 0 1 4 5 】

図 1 8 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 S F 1 4 , S 2 6 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 とコンテンツ提供者 7 の通信装置 3 と会員管理センター 1 2 の管理サーバー 6 9 それぞれのフローチャートである。

【 0 1 4 6 】

ユーザは、まず自己の IC カード 6 5 をパソコン 1 4 の IC カード挿入口 5 0 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 S 3 2 の処理がなされる。S 3 2 では、IC カード 6 5 に記憶されている会員 ID を読み出し、その読み出した会員 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、S F 1 5 により、送信されてきたそれら情報を会員管理センター 1 2 の管理サーバー 6 9 へ中継して送信する処理が行なわれる。管理サーバー 6 9 では、S H 1 により、データベース 7 0 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。

【 0 1 4 7 】

コンテンツ提供者 7 の通信装置 3 では、S F 1 6 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 1 4 へ送信する。ユーザのパソコン 1 4 では、S 3 3 により、IC カード 6 5 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。

【 0 1 4 8 】

コンテンツ提供者 7 の通信装置 3 では、そのレスポンスコード RC を S F 1 7 により中継して会員管理センター 1 2 の管理サーバー 6 9 に伝送する処理がなされる。

【 0 1 4 9 】

管理サーバー 6 9 では、S H 2 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者 7 の通信装置 3 へ返信する処理がなされる。この S H 2 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 1 2 のデータベース 7 0 に会員の ID 毎に分類して格納されており、管理サーバー 6 9 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。

【 0 1 5 0 】

ユーザ認証の確認情報を受取ったコンテンツ提供者 7 の通信装置 3 では、S F 1 8 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 ( R 1 , R 2 ) 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 1 4 へ転送する処理がなされる。ユーザのパソコン 1 4 では、S 3 4 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 K 1 と乱数 ( R 1 , R 2 ) とを再生して記憶する処理がなされる。この K 1 と乱数 ( R 1 , R 2 ) とが前述した図 1 7 に示した S 2 7 以降の処理に利用される。

【 0 1 5 1 】

図 1 9 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 1 4 に内蔵されている。コンテンツ提供者 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 1 4 が受信してそのコンテンツをハードディスク 8 1 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 1 4 がハードディスク 8 1 に記録する。このハード

10

20

30

40

50

ディスク 8 1 から読出された情報は、図 1 7 で説明したように、所定の復号化手段 8 1 a により復号化され、コンテンツが再生される。

【 0 1 5 2 】

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 C C 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、M P E G 2 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 8 1 a により復号化されたコンテンツデータが M P E G 2 復号化器 8 2 に入力され、復号化された情報を電子透かし検出器 8 3 に入力することにより、透かし情報である制御信号 C C S を検出することができる。そしてその電子透かし検出器 8 3 により検出された C C S が A P S 8 6 に入力される。この A P S 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。

10

【 0 1 5 3 】

電子透かし検出器 8 3 からグラフィックス・モジュール 8 4 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 8 4 からコンテンツデータが N T S C ( National Television System Committee ) 符号化器 8 5 に与えられ、N T S C 信号に変換される。そして N T S C 信号がパソコン 1 4 の C R T 5 2 , T V 1 6 , V T R 1 5 等に供給される。

【 0 1 5 4 】

A P S 8 6 に与えられる C C S 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 A P S 8 6 が動作して C C S のデータ内容どおりのコピー禁止等の制御を行なう。

20

【 0 1 5 5 】

図 2 0 は、コンテンツ提供者 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 1 1 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 2 0 は、いわゆるワイヤレス・ローカル網 W L L ( Wireless Local Loop ) を利用したものを示している。コンテンツ提供者 7 , 第三者機関 8 , 放送局 2 , 番組関連データ制作者 1 1 には、それぞれ、無線装置 7 1 , 7 2 , 7 4 , 7 5 が設けられている。そして、前述したように、第三者機関 8 とコンテンツ提供者 7 との間での、ユーザエージェント 2 6 , 有料コンテンツ, 第三者機関エージェント 2 9 等の伝送を、この W L L を利用して行なう。図中 7 6 , 7 7 , 7 8 , 7 9 , 8 0 は W L L 用のアンテナである。

30

【 0 1 5 6 】

また、放送局 2 と番組関連データ制作者 1 1 との間での、番組関連データの伝送等も、W L L 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。

【 0 1 5 7 】

第三者機関 8 とコンテンツ提供者 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 W L L 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。

【 0 1 5 8 】

図 2 1 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 1 4 に内蔵されている。ユーザのパソコン 1 4 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 8 1 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 K 1 , 乱数 R 1 , R 2 が前述したユーザのネットキー S K 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。

40

【 0 1 5 9 】

ハードディスク 8 1 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 M P E G 2 復号化器 8 2 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 8 3 に入力され、透かし情報である E<sub>SK</sub> ( K 1 , R 1 , R 2 ) が検出されてパソコン 1 4 の C R T 5 2 , T V 1 6 に入力される。一方、電子透かし

50

検出器 8 3 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 8 4 を経由して N T S C 符号化器 8 5 に入力され、N T S C 信号として C R T 5 2 , T V 1 6 , V T R 1 5 に与えられる。この N T S C 信号は、暗号化されたコンテンツデータの N T S C 信号であるために、この N T S C 信号に基づいてそのまま C R T 5 2 , T V 1 6 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。

**【 0 1 6 0 】**

そこで、たとえばユーザのパソコン 1 4 の I C カード挿入口 5 0 にユーザの I C カード 6 5 を挿入することにより、その I C カード 6 5 に記憶されているユーザのネットキー S K がパソコン 1 4 により読取られ、パソコン 1 4 に入力された  $E_{SK}(K1, R1, R2)$  をユーザのネットキー S K より符号化して K 1 , R 1 , R 2 を再生し、それらデータを用いて N T S C 信号を復号化して通常のコンテンツデータに対する N T S C 信号に変換し、それに基づいて C R T 5 2 により映像を表示するように制御する。

10

**【 0 1 6 1 】**

T V 1 6 にも I C カード挿入口を形成し、そこに I C カード 6 5 を挿入することにより、前述と同様に T V 1 6 により N T S C 信号を復号化して通常のコンテンツデータに対する N T S C 信号に変換して放映する。

**【 0 1 6 2 】**

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 I C カード 6 5 を、パソコン 1 4 あるいは T V 1 6 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、V T R 1 5 には、I C カード挿入口が形成されていないため、V T R 1 5 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 N T S C 信号となる。そしてこの V T R 1 5 に記録されている暗号化されたコンテンツに対する N T S C 信号を C R T 5 2 あるいは T V 1 6 により再生する際には、I C カード 6 0 を挿入して前述したように復号化して再生閲覧する。

20

**【 0 1 6 3 】**

この図 2 1 に示す別実施の形態により、T V 1 6 でコンテンツを再生する場合には、T V 1 6 に図 1 7 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、C R T 5 2 によりコンテンツを再生する場合には、パソコン 1 4 の I C カード挿入口 5 0 に I C カード 6 5 を挿入して再生するのであるが、図 2 1 に示すように、N T S C 符号化器 8 5 から C R T 5 2 に供給された N T S C 信号に対し復号化を行なうようにし、パソコン 1 4 内で N T S C 信号が復号化されてその復号化された N T S C 信号がたとえば T V 1 6 や V T R 1 5 に出力できないように構成されている。

30

**【 0 1 6 4 】**

また、この図 2 1 に示す別実施の形態では、図 1 8 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 K 1 と乱数 ( R 1 , R 2 ) とをユーザのネットキー S K で暗号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 1 4 に転送するようにする。

**【 0 1 6 5 】**

図 2 2 ~ 図 2 4 は、図 1 6 ~ 図 1 8 に示した制御動作の他の例を示す図である。

40

図 2 2 は、コンテンツ提供者 7 の通信装置 3 の動作を示すフローチャートであり、図 1 6 と対応している。S F 1 9 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 S F 1 9 a に進み、ユーザ認証処理を行なった後 S F 1 9 へ戻る。

**【 0 1 6 6 】**

テレスクリプト・エンジン 8 1 からコンテンツの送信指令があった場合には S F 2 0 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 S F 2 1 へ進み、放送日時とチャンネルをパソコン 1 4 へ送信して S F 1 9 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 S F 2 2 へ進み、ユーザの秘密鍵 S K U と同じビット数

50

の乱数  $R_N$  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  $R_N$  も  $1024$  ビットになる可能性が高い。

【0167】

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  $A (= A_1, A_2, \dots, A_n)$  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  $A_n$  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  $R_N$  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  $\oplus$  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  $A_1, A_2, \dots, A_n$  のそれぞれと乱数  $R_N$  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  $A(+)$   $R_N$  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、 $A(+)$   $R_N$  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。

【0168】

なお、 $SF24$  の最後の  $A_n(+)$   $R_N$  は、分割コンテンツデータ  $A_n$  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  $R_N$  の先頭から分割コンテンツ  $A_n$  のビット数だけのデータを取り出し、そのデータと  $A_n$  のイクスクルーシブオアを演算する。

【0169】

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。

【0170】

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。

【0171】

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。

【0172】

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  $A (= A_1, A_2, \dots, A_n)$  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、

$$S K U ( + ) \{ I 1 ( + ) ( A 1 ( + ) R N ) \} = A 1$$

$$S K U ( + ) \{ I 2 ( + ) ( A 2 ( + ) R N ) \} = A 2$$

.

$$S K U ( + ) \{ I n ( + ) ( A n ( + ) R N ) \} = A n$$

を満たす  $I (= I 1, I 2, \dots, I n)$  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。

【0173】

ここで、 $I 1, I 2, \dots, I n$  は、それぞれ、 $A 1, A 2, \dots, A n$  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  $A n$  が通常より少ないビット数であった場合には、 $I n$  も  $A n$  に合せた少ないビット数となる。この  $I 1, I 2, \dots, I n$  の算出は、比較的簡単に行なえ得る。たとえば、 $S K U$  と  $A 1$  と  $R N$  との最上位ビットがともに「1」であった場合には、

$$1 ( + ) \{ I 1 \text{ の最上位ビット } ( + ) ( 1 ( + ) 1 ) \} = 1$$

となり、 $I 1$  の最上位ビットは自ずと「0」となる。また、 $S K U$  の最上位ビットの次のビットが 0 で、 $A 1$  と  $R N$  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、

$$0 ( + ) \{ I 1 \text{ の最上位ビットの次のビット } ( + ) ( 1 ( + ) 1 ) \} = 1$$

となり、 $I 1$  の最上位ビットの次のビットは自ずと「1」となる。

【0174】

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  $S K$  により復号化する処理、すなわち、 $D_{SK}\{E_{SK}(I)\}$  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  $S K U$  が格納されている。この秘密鍵  $S K U$  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  $S K U$  にアクセスできるように構成されている。

【0175】

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、 $I (= I 1, I 2, \dots, I n)$  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  $Y E S$  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、

$$A = S K U ( + ) \{ I 1 ( + ) ( A 1 ( + ) R N ) \}$$

$$+ S K U ( + ) \{ I 2 ( + ) ( A 2 ( + ) R N ) \}$$

$$+ S K U ( + ) \{ I 3 ( + ) ( A 3 ( + ) R N ) \}$$

:

$$+ S K U ( + ) \{ I n ( + ) ( A n ( + ) R N ) \}$$

を演算して、コンテンツを再生する処理がなされる。

【0176】

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  $S K U$  が必要となる。つまりこのユーザの秘密鍵  $S K U$  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  $S K U$  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。

10

20

30

40

50

## 【 0 1 7 7 】

この図 2 2 ~ 図 2 4 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。

## 【 0 1 7 8 】

コンテンツ提供者 7 が作成したコンテンツを A とし、コンテンツ提供者 7 は、その有料コンテンツ A を乱数等からなる鍵  $R_N$  により暗号化して  $E_{R_N}(A)$  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者 7 は、 $D_{SKU}[D_I\{E_{R_N}(A)\}] = A$  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 1 3 等を経由してユーザのパソコン 1 4 へ送信する。

## 【 0 1 7 9 】

ユーザは、放送局 2 から受信した  $E_{R_N}(A)$  をコンテンツ提供者 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。

## 【 0 1 8 0 】

なお、このような  $R_N$  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、 $D_I\{E_{R_N}(A)\} = E_{PKU}(A)$  が成立する。ゆえに、この式を満たす I をコンテンツ提供者 7 が算出してそれをユーザのパソコン 1 4 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。

## 【 0 1 8 1 】

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 1 0 が制作した CM に対し番組関連データ制作者 1 1 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。

## 【 0 1 8 2 】

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。

## 【 0 1 8 3 】

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ポンサーの商品の宣伝を行なうものがあつた。

## 【 0 1 8 4 】

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。

## 【 0 1 8 5 】

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。

## 【 0 1 8 6 】

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。

## 【 0 1 8 7 】

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つた。

## 【 0 1 8 8 】

10

20

30

40

50

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。

【0189】

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ス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、

前記コマース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ス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。

【0190】

このような手段を採用した結果、コマースシャルメッセージと同時にそのコマース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スシャルメッセージも閲覧する結果となる。ゆえに、コマース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。

【0191】

前記同時放映手段は、前記コマース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ス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ス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。

【0192】

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ス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。

【0193】

また、前述したコマース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。

【0194】

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ス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、

前記コマース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ス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ス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。

【0195】

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。

【0196】

10

20

30

40

50

(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ス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、コマース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。

【0197】

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ス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ス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ス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。

10

【0198】

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になってしまうという欠点があった。

20

【0199】

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。

【0200】

この目的を達成する手段として、この発明は、コマース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スシャルメッセージを格納するコマース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スシャルメッセージ格納手段に格納されているコマースシャルメッセージを検索させる検索手段と、

30

該検索手段により検索されたコマース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スシャルメッセージ提供手段とを含むことを特徴とする。

【0201】

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ス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ス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ス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ス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ス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。

40

【0202】

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スシャルメッセージを格納するコマース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に前記コマースシャルメッセージ格納手段に格納されているコマース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

50



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。

【0203】

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。

10

【0204】

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り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り換えて放映する。

【0205】

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。

20

【0206】

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。

【0207】

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。

30

【0208】

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。

40

【0209】

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

50

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。

【0210】

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。

【0211】

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。

【0212】

(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。

【0213】

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。

【0214】

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。

【0215】

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ふという不都合が生ずる。

【0216】

そこで、前記復号化鍵 F K を、料金を支払った正規のユーザの公開鍵 P K U 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 S K U をもっていない限り復号化して復号化鍵 F K 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。

【0217】

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

10

20

30

40

50

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。

【0218】

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。

【0219】

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。

【0220】

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。

【0221】

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。

【0222】

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。

【0223】

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。

【0224】

前記SF22～SF24により、前記情報提供者（コンテンツ提供者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。

10

【0225】

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。

【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（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。

20

【0227】

（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。

【0228】

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。

【0229】

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

30

、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。

【0230】

（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

40

50

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。

【0231】

図15に示したS X A L / M B A Lの代わりに、R S A公開鍵暗号方式や楕円曲線暗号方式を用いてもよい。

【0232】

無線装置71, 72, アンテナ76, 77により、コンテンツ提供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。

【0233】

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mercialメッセージをユーザエージェントが検索したコマmercialメッセージに取換えて編集するコマmercial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mercialメッセージをユーザエージェントが検索したコマmercial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。

10

【0234】

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。

20

【0235】

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。

30

【0236】

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mercialメッセージが制作された場合に当該コマmercial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。

【0237】

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ある場合がある。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。

40

【0238】

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確認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

50

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。

【0239】

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。

10

【0240】

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。

20

【0241】

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。

【0242】

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（contract 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）を割当てするためのモデルのことである。

30

【0243】

以下、実施例の内容をまとめて列挙する。

コンテンツ提供者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。

40

【0244】

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

50

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、前記特定の仕事をこなうために開発されたエージェントである。

【0245】

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。

10

【0246】

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。

20

【0247】

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。

【0248】

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執行する（図7，図8に示したフローチャート）。

30

【0249】

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。

40

【0250】

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。コンテンツ提供者7により、前記ユーザの要求に応えるサービス業者が

50

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。

【0251】

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性が生じた場合に(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。

10

【0252】

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)。

【0253】

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)。

20

【0254】

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)。

【0255】

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動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。

30

【0256】

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。

40

【0257】

次に、実施例の効果を列挙する。

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代理して実行してくれるために、中立性を保ちながら特定の仕事の実行が可能となる。

【0258】

50



前記第三者エージェントが、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により運用管理され、前記特定の仕事をこなすために開発されたエージェントであるために、当事者にとってより一層中立性のあるエージェントによりより一層中立性のある代理実行が期待できる。

【0259】

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が行なわれ、第三者エージェントによる代理実行が行なわれるために、当事者エージェントによる利己的な動作による不都合を極力防止することができる。

【0260】

ユーザ側エージェントがコンテンツ格納手段に格納されている有料コンテンツの検索を希望した場合に、特定の仕事が生じたと判定されて第三者エージェントがその特定の仕事を代理実行してくれるために、ユーザ側エージェントが有料コンテンツを検索してその有料コンテンツに対する料金を支払うことなく有料コンテンツを盗んでしまう不都合が極力防止できる。

【0261】

第三者エージェントが、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を有するために、当事者の一方または双方に違法性があった場合にはそれが監視可能となる。

【0262】

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が検索されて提供されるために、当事者エージェントに代わって仕事を代理実行する第三者エージェントとしてその当事者エージェントに似ている適したエージェントを選任することができる。

【0263】

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生じた場合に、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にその特定の仕事を代理実行してもらうことのできるプログラムが記録された記録媒体を提供することができる。

【0264】

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生じた場合に、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調達されてその第三者エージェントに前記特定の仕事を代理実行してもらうことができる。

【0265】

モバイルエージェントで構成されているユーザ側エージェントがネットワーク上を移動して仕事をこなすに際し、ユーザ側エージェントが秘密データを使用する必要がある場合には、ユーザ側エージェントが秘密保持用ワーキングエリアに移動してそこで秘密データの秘密性を解除して前記仕事の実行が可能となり、秘密データの漏洩を防止できながらその秘密データを使用しての仕事の実行が可能となる。

【0266】

ユーザ側エージェントが前記秘密データ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データが他人に漏洩されることを極力防止することができる。

【0267】

前記秘密データ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前記暗号化された秘密データ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、前記秘密データの漏洩をより確実に防止することができる。

【0268】

ユーザ側エージェントが保有している秘密データは、前記ユーザの本人認証のための秘

10

20

30

40

50

密鍵を含んでいるために、前記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。

【図面の簡単な説明】

【0269】

【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ス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S X A L / M B A L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】

【0270】

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립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。

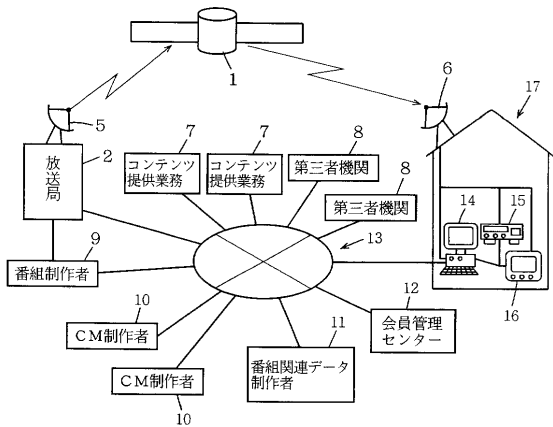
10

20

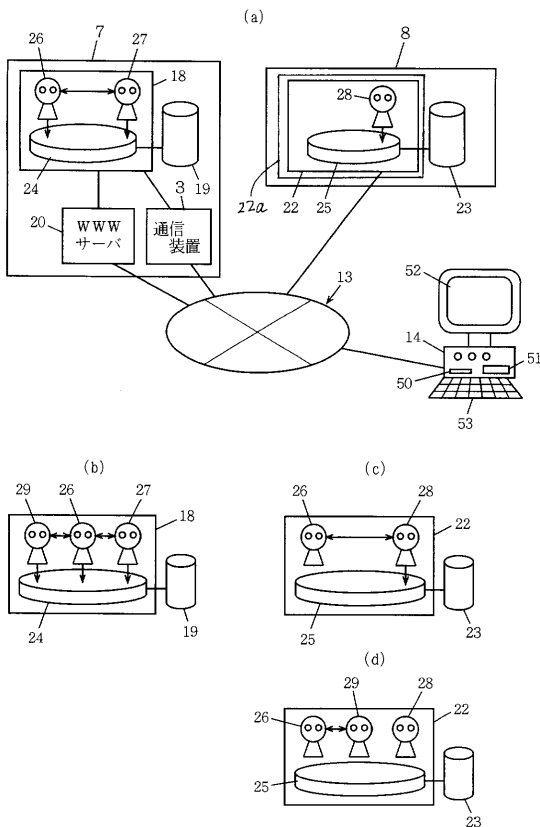
30

40

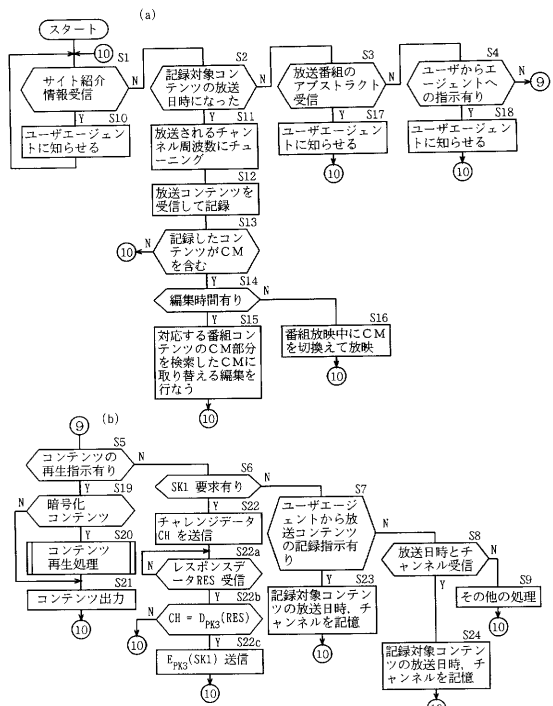
【図1】



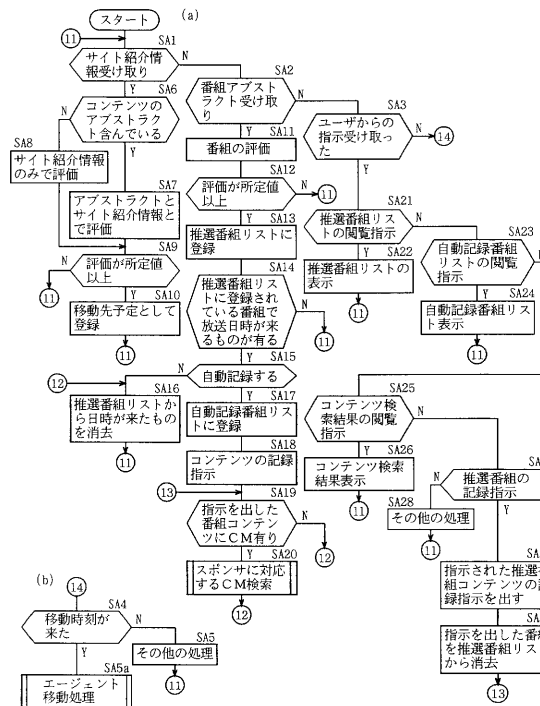
【図2】



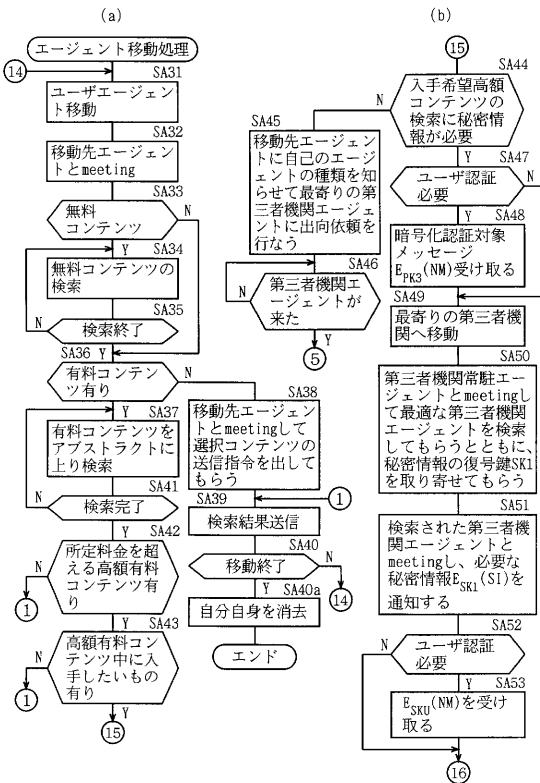
【図3】



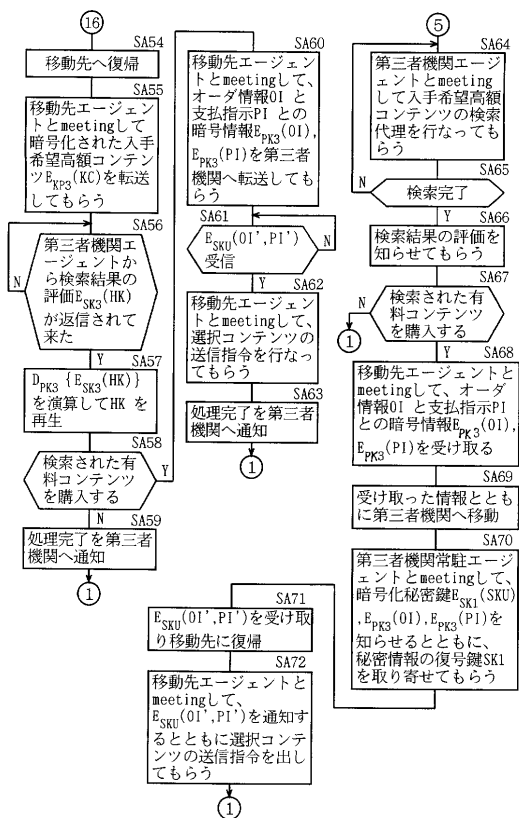
【図4】



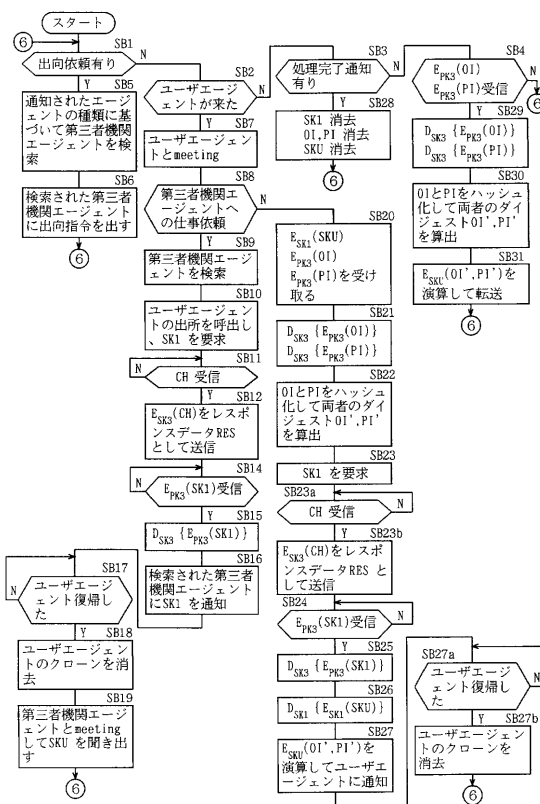
【図5】



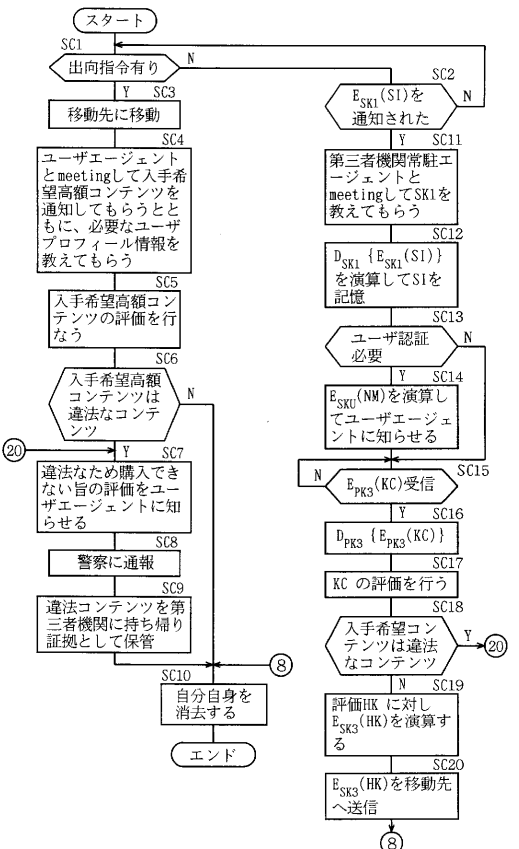
【図6】



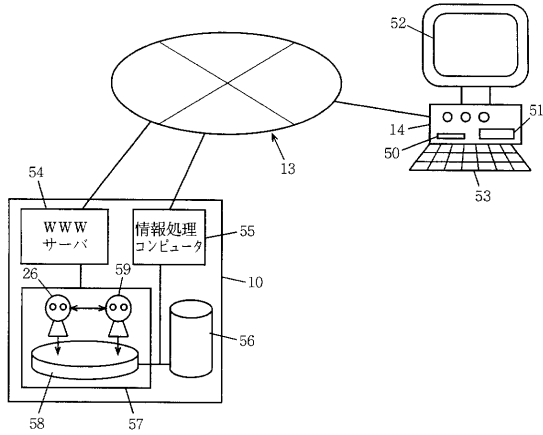
【図7】



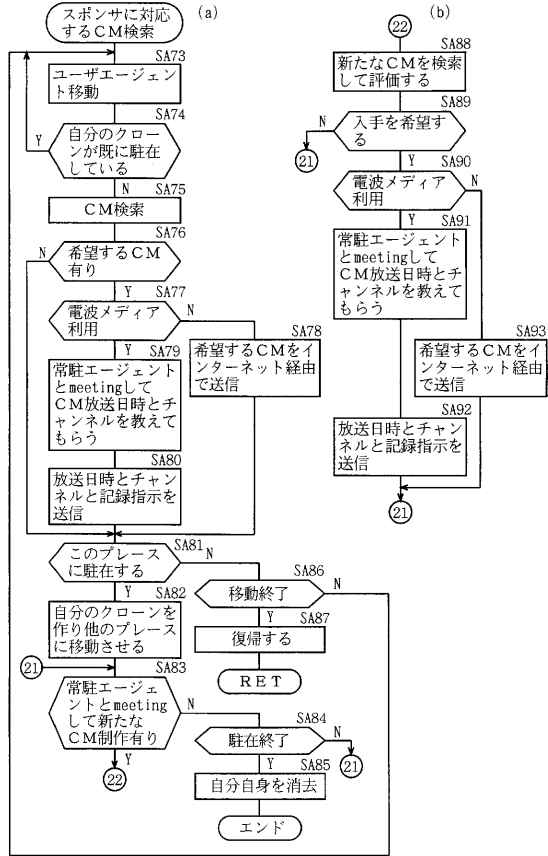
【図8】



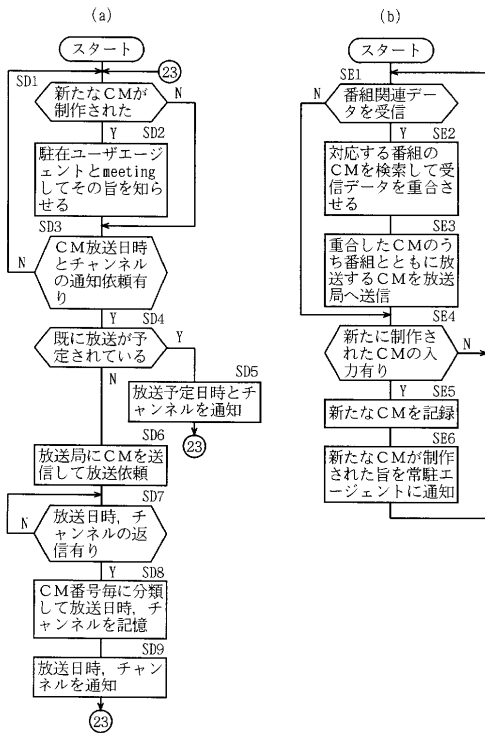
【図9】



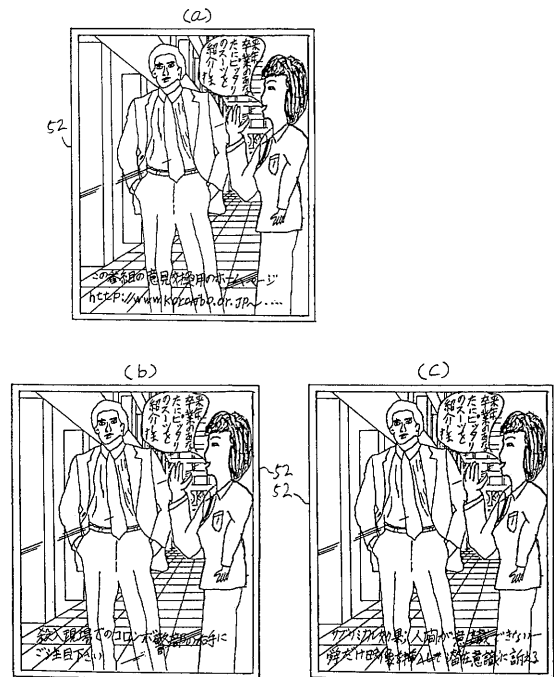
【図10】



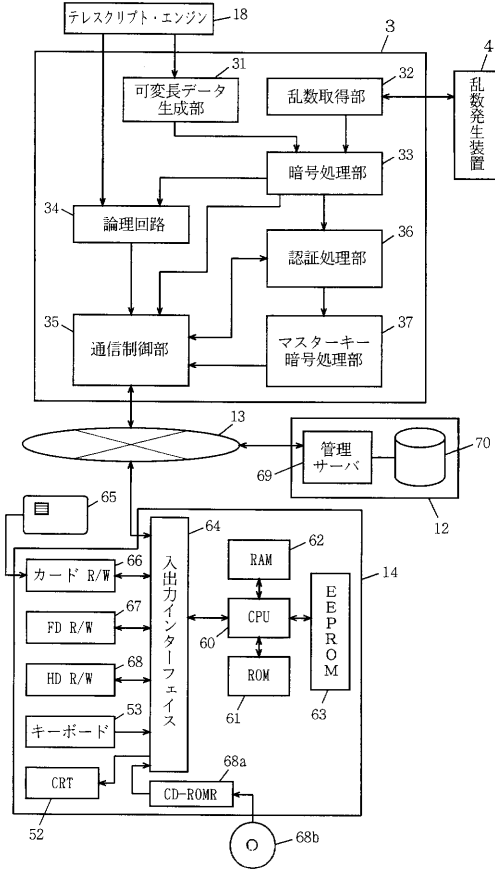
【図11】



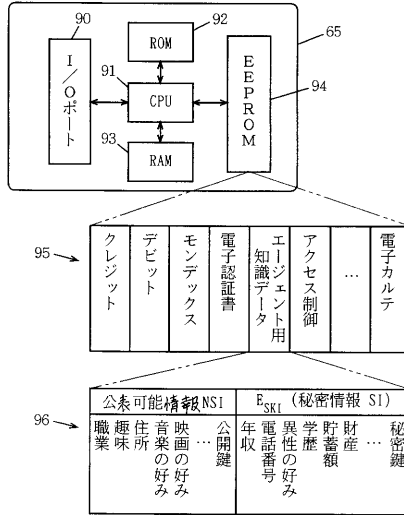
【図12】



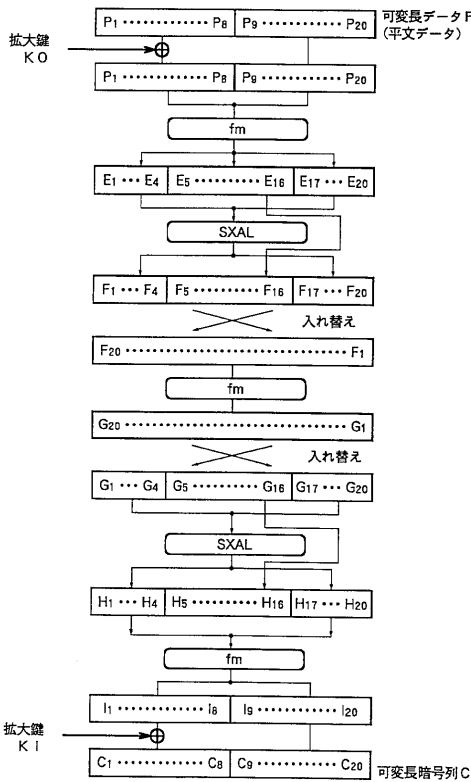
【図13】



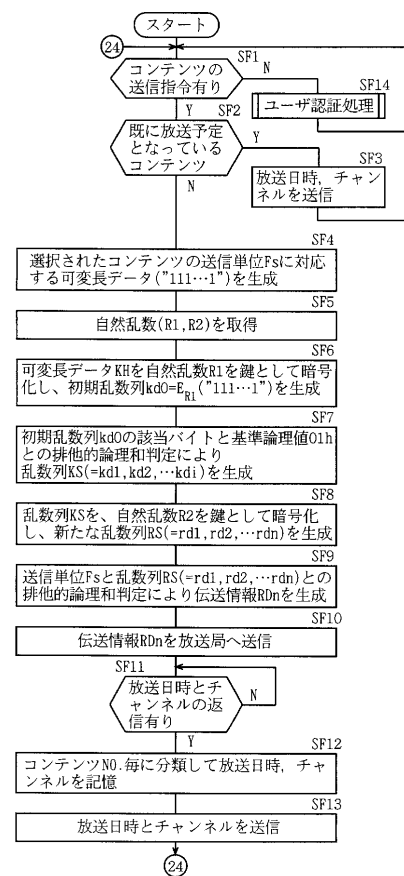
【図14】



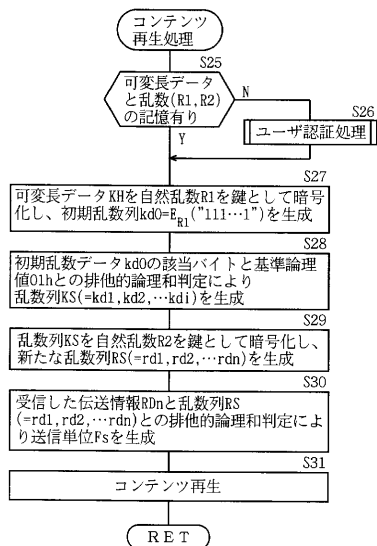
【図15】



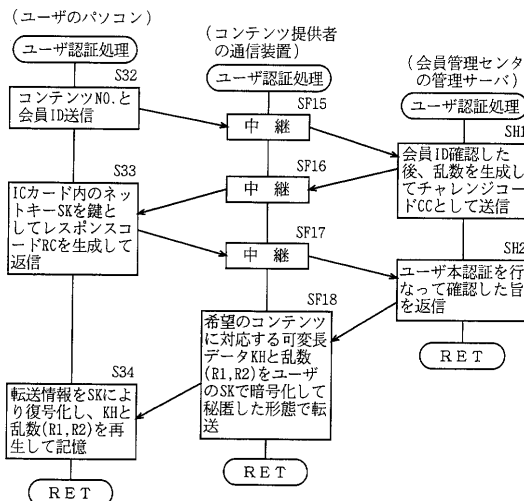
【図16】



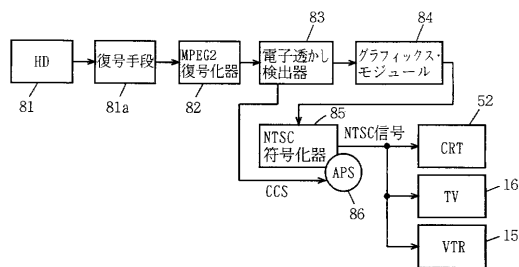
【図17】



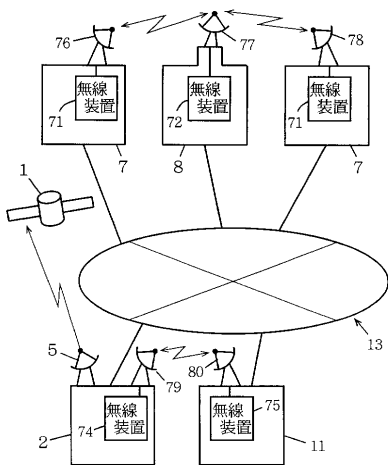
【図18】



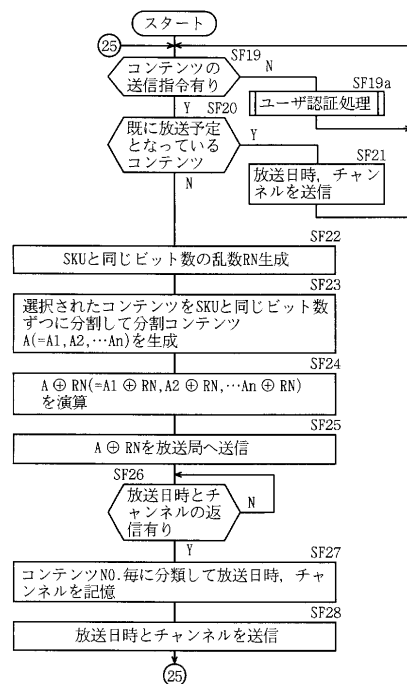
【図19】



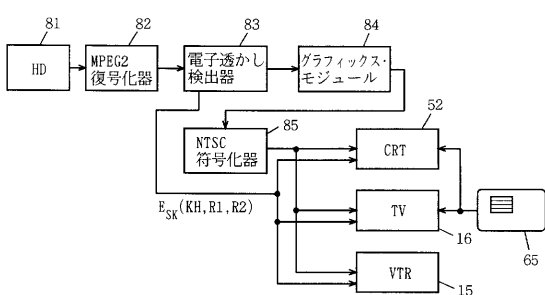
【図20】



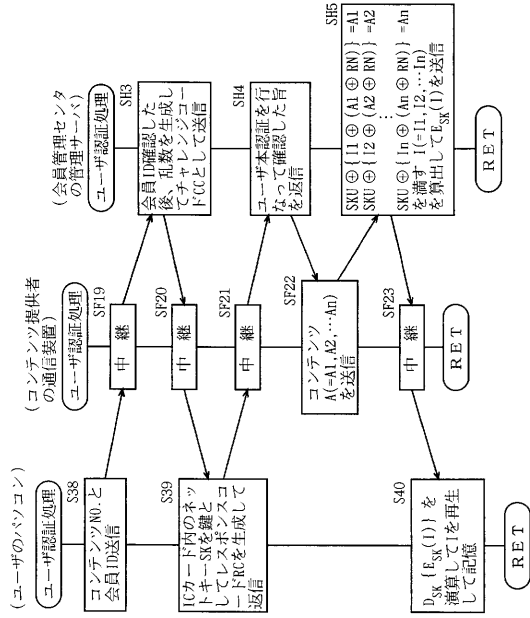
【図22】



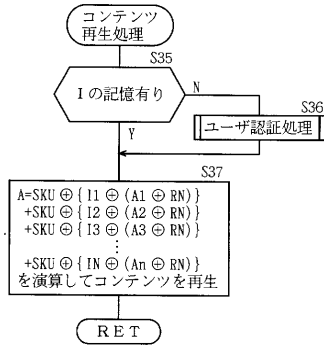
【図21】



【図23】



【図24】





## フロントページの続き

- (56)参考文献 特開平10-079711(JP,A)  
特開平09-051522(JP,A)  
特開平09-083955(JP,A)  
特開平10-032797(JP,A)  
特開平06-124309(JP,A)  
特開平09-327011(JP,A)  
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 Science, ドイツ, Springer Berlin, Mobile Agents, 1997年, Vol. 1219/1997, pp. 50 - 61  
中川智尋、外3名, モバイルエージェント間の通信のためのTracking AgentのJavaによる実装, 電子情報通信学会大会講演論文集, 日本, 社団法人電子情報通信学会, 1998年 3月, 1998総合 3, p. 167

## (58)調査した分野(Int.Cl., DB名)

H04N 7/16 - 7/173,  
G06F 9/46