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

特許第3746146号

(P3746146)

(45)発行日　平成18年2月15日(2006.2.15)　(24)登録日　平成17年12月2日(2005.12.2)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	540C
G06K 17/00	(2006.01)	G06F	12/14	550A
G09C 1/00	(2006.01)	G06K	17/00	E
G11B 20/10	(2006.01)	G09C	1/00	630B
G06K 19/10	(2006.01)	G09C	1/00	630E

請求項の数 4　(全 25 頁)　最終頁に続く

(21)出願番号　特願平10-23284
(22)出願日　平成10年2月4日(1998.2.4)
(65)公開番号　特開平10-283268
(43)公開日　平成10年10月23日(1998.10.23)
審査請求日　平成12年12月13日(2000.12.13)
(31)優先権主張番号　特願平9-25303
(32)優先日　平成9年2月7日(1997.2.7)
(33)優先権主張国　日本国(JP)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100068814
弁理士　坪井　淳
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】暗号情報の生成及び復号方法及び伝送及び受信装置

(57)【特許請求の範囲】

【請求項１】

暗号化側では、

サービス情報を格納するサービス情報格納手段と、前記サービス情報を暗号化するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記サービス情報を暗号化するサービス情報暗号化手段とを具備する装置において実行され、前記鍵情報生成手段と、前記記憶手段と、前記サービス情報暗号化手段とを制御するステップであって、

前記サービス情報に対するコピー可否情報に基づいて、サービス情報を暗号化するための前記鍵情報を生成するステップと、

前記サービス情報暗号化手段を制御し、前記鍵情報に基づいて前記サービス情報を暗号化するステップとを有し、

復号化側では、

暗号化サービス情報を格納する暗号化サービス情報格納手段と、前記暗号化サービス情報を復号するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記暗号化サービス情報を復号するサービス情報復号化手段とを具備する装置において実行され、前記鍵情報生成手段と前記サービス情報復号化手段とを制御するステップであって、

前記サービス情報に対するコピー可否情報に基づいて前記鍵情報を生成するステップと、

前記サービス情報復号化手段を制御し、前記鍵情報に基づいて前記サービス情報を復号し、復号されたサービス情報を生成するステップと
を有することを特徴とする暗号化サービス情報の生成及び復号方法。
【請求項２】
暗号化側では、
サービス情報を格納するサービス情報格納手段と、前記サービス情報を暗号化するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記サービス情報を暗号化するサービス情報暗号化手段と、を具備する装置において実行され、前記鍵情報生成手段と、前記記憶手段と、前記サービス情報暗号化手段を制御することにより、暗号化サービス情報を生成する暗号化サービス情報生成方法において、前記前記鍵情報生成手段と、前記記憶手段と、前記サービス情報暗号化手段を制御するステップであって、
前記サービス情報に対するコピー可否情報を使用して第1の情報を生成するステップと、前記第1の情報を使用して、前記鍵情報としての第２の情報を生成するステップと、
前記サービス情報暗号化手段を制御し、前記第２の情報に基づいて前記サービス情報を暗号化するステップとを有し、
復号化側では、
暗号化サービス情報を格納する暗号化サービス情報格納手段と、前記暗号化サービス情報を復号するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記暗号化サービス情報を復号するサービス情報復号化手段とを具備する装置において実行され、前記鍵情報生成手段と前記サービス情報復号化手段とを制御ステップであって、
前記サービス情報に対するコピー可否情報に基づいて第1の情報を生成するステップと、
前記第1の情報を使用して、前記サービス情報を復号するための前記鍵情報としての第2の情報を生成するステップと、
前記サービス情報復号化手段を制御し、前記鍵情報に基づいて前記サービス情報を復号するステップと
を有することを特徴とする暗号化サービス情報の生成及び復号方法。
【請求項３】
サービス情報を暗号化した暗号化情報を伝送する装置においては、
前記サービス情報のコピー可否を示すコピー可否情報を含む制御情報を生成する第１の手段と、
前記制御情報に基づいて、暗号化鍵情報を生成する第２の手段と、
前記暗号化鍵情報に基づいて前記サービス情報を暗号化する第３の手段と、
前記サービス情報を暗号化したサービス情報暗号化情報を伝送する伝送手段とを具備し、
サービス情報暗号化情報を受信する受信装置においては、
元のサービス情報のコピー可否を示すコピー可否情報を含む制御情報があり、この制御情報に基づいて暗号化鍵情報を生成する手段と、
生成した前記暗号化鍵情報を用いて、受信した前記サービス情報暗号化情報をデコードするデコード手段
を有したことを特徴とする暗号情報伝送及び受信装置。
【請求項４】
前記デコード手段は、前記コピー可否情報がコピー許可を示す場合には、デコード処理を行うが、コピー不許可を示す場合には、さらに予め設定されている所定の条件情報を判定したのちに、デコードするか否かを決定する手段を含むことを特徴とする請求項３記載の暗号情報伝送及び受信装置。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】
この発明は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録される情報記録媒体、この情報記録媒体の記録装置、情報記録媒体からの情報を他の機器へ伝送して復号化する情報伝送システム、暗号化情報を暗号化鍵情報により元の情報に解読する暗号解読装置に関する。
【０００２】
【従来の技術】
現在、インターネットを用いて世界中の情報入手が可能となっている。最近では特定ドメイン（領域、地域）内での情報サービスに対する課金システムも一部実施段階に入っている。そのインターネット普及とともに不正防止を目的としたセキュリティー確保も急務となっている。
【０００３】
確保すべきセキュリティーの対象として、
Ａ）サービスを受けるユーザーを特定し、第３者が情報伝達経路の途中に入り込みサービス情報の横取りする事を防止する場合（情報横取りの防止）と、
Ｂ）著作権を侵害してサービスプロバイダー以外の第３者が元のサービス情報を他の商業目的に利用するのを防止する場合（情報複製の防止）が有る。
【０００４】
特に（Ｂ）に上げた情報複製防止に関する要請が今後急速に増加されることが予想される。これは、現在、ネットワークコンピュータの開発が精力的に進められているためである。
【０００５】
現在開発中のネットワークコンピュータは、ＨＤＤを内蔵せず、ＯＳさえも起動時に無線でホストサーバから呼び出し、作業に必要なアプリケーションソフトを必要な時、必要な機能プログラムを無線でインストールしながら作業を行う物である。
【０００６】
従って、従来はユーザが種々のアプリケーションパッケージソフトを購入し、ＨＤＤにインストールして使っている。
しかし、ネットワークコンピュータを利用した場合には、事前の購入は不要となり、必要な時、必要な機能プログラムを呼び出して使うとともに、機能プログラムを呼び出す毎に課金されるシステムとなる。この機能プログラムは、パッケージプログラムのような大規模なプログラムでは無くＪＡＶＡなどで記述された機能限定された非常に小規模なプログラムである。
【０００７】
したがって、ネットワークコンピュータを用いた場合には課金方法の特殊性から、ユーザによる機能プログラムの複製・再利用を禁止する必要が有る。
上記セキュリティー確保の方法として、アシンメトリック（対象暗号系）な暗号化技術を用いる、以下の３つの方法がある。
１．ユーザ側で公開鍵と秘密鍵を発行し、情報サービスプロバイダに対して情報サービス請求とともに公開鍵を通信する。
２．情報サービスプロバイダがユーザから送ってもらった公開鍵に基付きサービス情報を暗号化してユーザに送る。
３．ユーザ側で自分の発行した秘密鍵を用いて暗号化情報を復号化して利用する。
【０００８】
しかし、これらの方法を用いた場合には、情報サービスプロバイダはユーザからの要求がある度に暗号化する必要が生じ、サービスコストが大幅にかかってしまう。
【０００９】
それを回避する方法として、暗号化と復号化時に共通な共通鍵を用いたシンメトリック（非対象暗号系）方式を採用し、暗号化されたサービス情報と同時に暗号化した共通鍵をユーザに送り、共通鍵を知っているユーザのみが解読できるシステムを採用する方法も有る

。
【００１０】
しかし、この方法を用いた場合には、以下の問題が生じる。
ａ〕ユーザにサービス情報をＨＤＤや光ディスクに複製されてしまい、ネットワークコンピュータのように、情報サービス毎に課金出来ない。
ｂ〕共通鍵を一致させる限り、情報サービスプロバイダ以外の第３者が暗号化されたままの情報を不正に商業用に転用する事が容易となる。
【００１１】
以上の説明においてコンピュータネットワークを用いた情報サービスについて主に説明をしてきたが、同様に衛星放送を用いたサービスも存在する。放送を用いた場合にはアシンメトリック方式（公開鍵・秘密鍵を用いた方法）は使えず公開鍵を用いたシンメトリック方式を採用して、公開鍵を知っている特定ユーザーのみがサービスを受けられるように出来る。
【００１２】
しかしこの場合にも上記の〔ａ〕〔ｂ〕の問題が共通に発生する。
また、以上の問題点を暗号化技術の観点から明示する。
従来知られているように送付元と受信先が同じ鍵を使用する共通鍵（シンメトリック）方式では、以下の３つの欠点がある。
１）鍵の転送中に第３者による不正コピーされる危険性がある。
２）鍵の管理が複雑である。
３）受信先で暗号データー自体の改ざんが容易に出来る。すなわち、受信先で暗号データーを共通鍵で復号化後、改竄した後、再度共通鍵で暗号化することが用意にできる。
【００１３】
これに対して、公開鍵と秘密鍵を用いたアシンメトリック方式では上記の問題点は改善されるが、以下のような欠点がある。
イ〕暗号化／復号化の処理に膨大な時間がかかる。
ロ〕情報サービスプロバイダがユーザに情報を送る毎にＣＡセンタ（認証局）にユーザ毎の公開鍵を問い合わせる必要がある。
【００１４】
という情報サービスプロバイダ側の負担が増大する。
さらに、
ハ〕秘密鍵の保管に関してユーザに多大な負担を掛ける。
【００１５】
たとえば、秘密鍵を盗まれただけで、セキュリティー確保は不可能となる。またユーザ側で、秘密鍵の入っているＦＤやＩＣカードを容易に複製できるので、複製された秘密鍵情報が悪用される危険性がある。
【００１６】
と言う問題も有る。
上記問題を改良する方法として、データそのものを共通鍵で暗号化し、この共通鍵のみを公開鍵で再度暗号化するというハイブリッド方式が提案されている。この方式を用いれば、“［イ］暗号化／復号化の処理時間の肥大化”は、緩和されるが、［ロ］と［ハ］の煩雑さは軽減されない。
【００１７】
また、情報を暗号化して伝送または記録するシステムにおいて、情報の暗号化に用いた鍵をも伝送または記録する場合には、鍵を秘匿するために暗号化に用いた鍵をそのまま伝送または記録することはせずに、鍵を情報の暗号化手段とは別の暗号化手段により別途暗号化した鍵情報として伝送または記録する。情報再生側では、まず鍵情報を鍵の復号化手段で復号化して得られた鍵を用いて、暗号化情報を情報の復号化手段により復号化する。
【００１８】
このことを利用し、暗号化前の鍵の中に再生制御情報を含ませるようにして、再生制御情

報の改ざんを防ぐ方法が考えられる。
しかしながら、この方法だと情報再生側において、再生制御情報を知るために鍵情報を復号化しなければならず、そのことが次のような情報再生システムの場合に大きな問題となる。
【００１９】
例えば、鍵情報の復号化手段も暗号化情報の復号化手段も持たず、単に記録されたデータを読み取るだけのディスクドライブ装置に再生禁止情報を判定させ、復号化手段を持つ情報再生装置へのデータ転送を制御させるようにした情報再生システムについて説明する。
【００２０】
この場合、ディスクドライブ装置にも鍵情報の復号化手段を持たせなければならず、ディスクドライブ装置のコスト増加を招くことはもちろん、ディスクドライブ装置には不必要な鍵情報を復号化する復号化手段を持たせることによる、システム全体のセキュリティの低下を招くという深刻な問題を引き起こすからである。
【００２１】
【発明が解決しようとする課題】
この発明の目的は、コピー許可、非許可情報の改ざんを極めて効果的に防止することができるようにした暗号情報の生成及び復号方法及び伝送及び受信装置を得るものである。
【００２８】
【課題を解決するための手段】
この発明は、暗号化側では、サービス情報を格納するサービス情報格納手段と、前記サービス情報を暗号化するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記サービス情報を暗号化するサービス情報暗号化手段とを具備する装置において実行され、前記鍵情報生成手段と、前記記憶手段と、前記サービス情報暗号化手段とを制御するステップであって、
前記サービス情報に対するコピー可否情報に基づいて、サービス情報を暗号化するための前記鍵情報を生成するステップと、前記サービス情報暗号化手段を制御し、前記鍵情報に基づいて前記サービス情報を暗号化するステップとを有し、
復号化側では、暗号化サービス情報を格納する暗号化サービス情報格納手段と、前記暗号化サービス情報を復号するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記暗号化サービス情報を復号するサービス情報復号化手段とを具備する装置において実行され、前記鍵情報生成手段と前記サービス情報復号化手段とを制御するステップであって、
前記サービス情報に対するコピー可否情報に基づいて前記鍵情報を生成するステップと、前記サービス情報復号化手段を制御し、前記鍵情報に基づいて前記サービス情報を復号し、復号されたサービス情報を生成するステップとを有するものである。
又この発明では、
暗号化側では、サービス情報を格納するサービス情報格納手段と、前記サービス情報を暗号化するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記サービス情報を暗号化するサービス情報暗号化手段と、を具備する装置において実行され、前記鍵情報生成手段と、前記記憶手段と、前記サービス情報暗号化手段を制御することにより、暗号化サービス情報を生成する暗号化サービス情報生成方法において、前記前記鍵情報生成手段と、前記記憶手段と、前記サービス情報暗号化手段を制御するステップであって、前記サービス情報に対するコピー可否情報を使用して第1の情報を生成するステップと、前記第1の情報を使用して、前記鍵情報としての第２の情報を生成するステップと、前記サービス情報暗号化手段を制御し、前記第２の情報に基づいて前記サービス情報を暗号化するステップとを有し、
復号化側では、暗号化サービス情報を格納する暗号化サービス情報格納手段と、前記暗号化サービス情報を復号するための鍵情報を生成する鍵情報生成手段と、前記鍵情報を記憶する記憶手段と、前記鍵情報を用いて前記暗号化サービス情報を復号するサービス情報復号化手段とを具備する装置において実行され、前記鍵情報生成手段と前記サービス情報

復号化手段とを制御ステップであって、前記サービス情報に対するコピー可否情報に基づいて第1の情報を生成するステップと、前記第1の情報を使用して、前記サービス情報を復号するための前記鍵情報としての第2の情報を生成するステップと、前記サービス情報復号化手段を制御し、前記鍵情報に基づいて前記サービス情報を復号するステップとを有するものである。

【００３４】

【発明の実施の形態】

以下、図面を参照してこの発明の実施例に係る光ディスク再生装置を説明する。

以下、この発明の第１の実施の形態について図面を参照して説明する。

【００３５】

図１は、この発明の情報伝送システムを示すものである。この情報伝送システムは、クライアントマシン１と、このクライアントマシン１と通信回線２を介して接続されるホストサーバ３と、クライアントマシン１に装填あるいは内蔵される暗号解読部としてのＩＣカード４により構成されている。

【００３６】

すなわち、クライアントマシン１からの所定のデータとしてたとえばワープロソフト等のプログラムの転送要求がホストサーバ３へ送信される。この送信に応じて、ホストサーバ３がその転送要求に応じて、後述する記録部としてのハードディスク装置（ＨＤＤ）２９に記録されている暗号化されているワープロソフト等のプログラム（暗号化情報）をその暗号化情報に対応する暗号化鍵情報（復号化するための情報で暗号化されている）とともに、転送要求のあったクライアントマシン１に返送される。この返送に応じて、クライアントマシン１はＩＣカード４を用いて暗号化情報を暗号化鍵情報により復号化（解読）し、この復号化されたワープロソフト等のプログラムを用いて処理が行えるようになっている。

【００３７】

上記ハードディスク装置（ＨＤＤ）２９には、ユーザに提供するサービス情報毎に記録されている。このサービス情報としては、単なる特定データだけでなく、例えばプログラミング（ｊａｖａ）言語などで記述されたアプリケーション用の小単位の機能プログラムを含む。

【００３８】

上記ハードディスク装置（ＨＤＤ）２９に記録されている１つのサービス情報の構造例を、図２を用いて説明する。

すなわち、暗号化情報としての暗号化されているワープロソフト等のプログラム（ユーザが使用する情報）４０とこの暗号化情報４０を復号化（解読）する鍵情報が暗号化されている暗号化鍵情報４１とからなる情報が記録されている。

【００３９】

暗号化鍵情報４１内には、その一部に非暗号化された形で（直接読める形で）制御情報４２が含まれている。制御情報４２は、対応する暗号化情報４０を復号化（解読）する際の条件情報である。

【００４０】

制御情報４２は、図３に示すように、１ビットのコピー許可コード４３、４ビットのドライブコード４４、３２ビットのアドレスコード４５、３ビットのリージョンコード４６、１６ビットの情報作成日情報４７、７ビットの情報作成後のコピー禁止期間情報４８、２４ビットの特定パスワード情報４９、３２ビットの特定ユーザ／組織情報５０からなる１１９ビット構成となっている。

【００４１】

ドライブコード４４、アドレスコード４５は、機器情報５１と呼んでいる。リージョンコード４６は、領域情報と呼んでいる。情報作成日情報４７、コピー禁止期間情報４８は、時間的情報５２と呼んでいる。特定パスワード情報４９、特定ユーザ／組織情報５０は、ユーザ限定情報５３と呼んでいる。

【００４２】
コピー許可コード４３は、コピーの許可、不許可を示すものであり、“１”の時はコピー許可を示し、“０”の時はコピー不許可を示している。
ドライブコード４４は、情報伝送経路や使用ドライブを示している。
【００４３】
“１Ｈ（ヘキサ：１６進法）”の時、情報伝送経路がＩＳＤＮ（ＬＡＮネットワーク）１０ＭＨｚ対応を示している。
“２Ｈ”の時、情報伝達経路がＩＳＤＮ（ＬＡＮネットワーク）１００ＭＨｚ対応を示している。
【００４４】
“３Ｈ”の時、情報伝達経路がＩＳＤＮ（ＬＡＮネットワーク）５００ＭＨｚ対応を示している。
“４Ｈ”の時、情報伝達経路が一般有線電話線（モデム利用）を示している。
【００４５】
“５Ｈ”の時、情報伝達経路が地上波（多重ＴＶチャネル）を示している。
“６Ｈ”の時、情報伝達経路が衛星放送を示している。
“７Ｈ”の時、情報伝達経路が無線通信（ＰＨＳ、携帯電話ネットワーク）を示している。
【００４６】
“８Ｈ”の時、情報伝達経路が局所無線通信（家庭内通信、事業所内通信）を示している。
“９Ｈ”の時、情報伝達経路がケーブルネットワーク、“ＡＨ”の時、情報伝達経路（使用ドライブ）がＦＤＤを示している。
【００４７】
“ＣＨ”の時、情報伝達経路（使用ドライブ）が（起動時のオペレーションシステムが記録されている）ブートＨＤＤを示している。
“ＤＨ”の時、情報伝達経路（使用ドライブ）がＭＯ、ＰＤなど光ディスクを示している。
【００４８】
“ＥＨ”の時、情報伝達経路（使用ドライブ）がＣＤ－ＲＯＭ、ＣＤ－Ｒを示している。
“ＦＨ”の時、情報伝達経路（使用ドライブ）がＤＶＤVideo 、ＤＶＤ－ＲＯＭを示している。
【００４９】
“０Ｈ”の時、情報伝達経路（使用ドライブ）がＤＶＤ－ＲＡＭあるはＤＶＤ－Ｒを示している。
アドレスコード４５は、送信先や送信元を識別するためのアドレスデータ（ＩＰアドレス）を示し、たとえばネットワークアドレスとホストアドレスから構成されている。このアドレスコード４５は、情報伝達がＩＳＤＮ（ＬＡＮネットワーク）の場合に付与されている。
【００５０】
リージョンコード４６は、地球上の地域を８地域に分け、各地域毎に１６進法で１Ｈから８Ｈの番号を付与したものである。リージョンコード４６は、領域情報に対応している。
【００５１】
情報作成日情報４７は、情報作成日を示すものであり、７ビットの年情報、４ビットの月情報、５ビットの日情報で記述されている。
コピー禁止期間情報４８は、コピー禁止期間つまりコピー不許可期限を示すものであり、コピー許可コードが“０”のコピー不許可の場合に、付与されるものである。このコピー禁止期間情報４８は、最高１０年７か月＝１２７ヶ月まで記述でき、“００００００００”の場合には永久にコピー禁止を示している。
【００５２】

特定パスワード情報４９は、アルファベットと数字の４文字分で示される特定のパスワードを示すものであり、１文字分ずつに３６種類の文字が選択できるようになっている。この場合、１文字ずつが６ビットのコードで記述されている。

【００５３】

特定ユーザ／組織情報５０は、特定ユーザや組織を示すものである。

上記制御情報４２の内容は、情報伝送システムで取り扱う情報内容（コンテンツ）により簡素化するようにしても良い。たとえば、もっとも簡易的なシステムとしては、制御情報４２が１ビットのコピー許可コード４３のみから構成されるものであっても良い。

【００５４】

上記した図３に示す構造を有する制御情報４２が、そのまま図２に示す暗号化鍵情報４１内に嵌め込まれる。この暗号化鍵情報４１のサイズは、制御情報４２のサイズより大きいものであり、ハッカーによる暗号化鍵情報４１の解読を防止するためには、最低でも暗号化鍵情報４１のサイズは、制御情報４２の２倍は必要で、実際には３倍以上が望ましい。

【００５５】

したがって、上記した制御情報４２が１１９ビット構成の場合、暗号化鍵情報４１は最低でも２３８ビット、通常でも３５７ビット以上は必要となる。

また、１ビットのコピー許可コード４３のみから制御情報４２が構成されている場合、暗号化鍵情報４１は最低でも２ビット、通常でも３ビット以上は必要となる。

【００５６】

ＩＣカード４は、図４に示すように、後述するＩＣカードリーダ・ライタ１３に接続されるコネクト部としての電極部５と、ユーザパスワード入力端子用穴６と、マスター鍵入力端子用穴７とを有している。ユーザパスワード入力端子用穴６内にユーザパスワード入力端子６ａがあり、マスター鍵入力端子用穴７内にマスター鍵入力端子７ａがある。

【００５７】

ユーザパスワード入力端子用穴６と、マスター鍵入力端子用穴７とは、ＩＣカード４の発行装置により発行される際に、ユーザパスワード（第１の特定情報）とマスター鍵情報（共通鍵情報）の入力によりユーザ対応鍵情報（第２の特定情報）が生成されて、後述するＥＥＰＲＯＭ３４に記録された後、樹脂封入等で埋めこまれるようになっている。これにより、後からユーザ対応鍵情報が変更できない、つまり不正改ざんできないようにしている。

【００５８】

すなわち、ユーザ、つまりＩＣカード４の発行者であるプロバイダーにより入力される、第２の特定情報としてのユーザパスワードとマスター鍵の入力により、第１の特定情報としてのユーザ対応鍵情報を形成した後、改ざん防止のため、その入力部（入力端子）への外部からの入力経路を遮断している。

【００５９】

また、ユーザパスワード入力端子用穴６、マスター鍵入力端子用穴７が埋められる代りに、ユーザパスワード入力端子６ａ、マスター鍵入力端子７ａ自体を取り外したり、あるいはそれらの電極部分を取り外したりすることにより、後からユーザ対応鍵情報が変更できないようにしても良い。この場合、入力端子の代りにリード線を用い、発行時にリード線を引抜くことにより、取り外すようにしても良い。

【００６０】

クライアントマシン１は、パソコン等の情報処理機器であり、図５に示すように、クライアントマシン１の全体を制御するＣＰＵ１０、制御プログラムが記録されているＲＯＭ１１、データ記録用のＲＡＭ１２、上記ＩＣカード４との間でデータのやり取りを行うＩＣカードリーダ・ライタ１３、表示部１４、入力部としてのキーボード１５、記録部（情報記録媒体）としてのハードディスク装置（ＨＤＤ）１６、光ディスク１７ａが装填される記録部としての光ディスク装置１７、および上記通信回線２を介してホストサーバ３と接続される通信インターフェース１８により構成されている。

【００６１】

ハードディスク装置（ＨＤＤ）１６、光ディスク装置１７は、オプションにて後から接続できるものである。
ホストサーバ３は、図６に示すように、ホストサーバ３の全体を制御するＣＰＵ２０、制御プログラムが記録されているＲＯＭ２１、データ記録用のＲＡＭ２２、あらかじめマスター鍵情報が記録されているＥＥＰＲＯＭ２３、生情報を鍵情報により暗号化情報４０への暗号化を行う暗号器２４、暗号化鍵情報４１をマスター鍵情報により鍵情報への復号化を行う復号器２５、暗号化鍵情報４１を生成する鍵情報合成器２６、表示部としてのＣＲＴディスプレイ２７、ユーザパスワードをユーザが入力する入力部としてのキーボード２８、暗号化されているワープロソフト等のプログラム（暗号化情報）とこの暗号化情報に対応する暗号化鍵情報とからなる情報が記録されている記録部（情報記録媒体）としてのハードディスク装置（ＨＤＤ）２９、上記通信回線２を介してクライアントマシン１と接続される通信インターフェース３０により構成されている。

【００６２】
上記ハードディスク装置（ＨＤＤ）２９の代りに光ディスク装置を用いても良い。さらに、大容量の記録部とする場合には、ＲＡＩＤ（redundant arrays inexpensive disk ）等のディスクアレイにより構成されるようにしても良い。

【００６３】
上記鍵情報合成器２６は、暫定的に暗号化鍵としての暗号化鍵原案情報と制御情報４２との合成を行い、合成結果として暗号化鍵情報４１を生成するものであり、例えば図７に示すように２つのシフトレジスタ２６ａ、２６ｂにより構成されている。

【００６４】
これにより、シフトレジスタ２６ａ、２６ｂは、供給される暗号化鍵原案情報を順次出力し、ＣＰＵ２０からのロード信号が供給された際に、制御情報４１をロードすることにより、その暗号化鍵原案情報に制御情報４１を嵌め込んで出力するようになっている。この際、ＣＰＵ２０はＲＡＭ２２から読出す暗号化鍵原案情報のアドレスに基づいてロード信号が出力されるようになっている。

【００６５】
上記暗号器２４、復号器２５は、それぞれ図８に示すように、７個のシフトレジスタ６０ａ～６０ｇと３個の排他的論理和演算を行う演算器６１ａ～６１ｃにより構成されている。

【００６６】
暗号器２４の場合には、たとえば、乱数としての鍵情報「１０１００１０００１０１１」がシフトレジスタ６０ａ～６０ｇに供給され、生情報「１１１０００１１１０００１」が演算器６１ｃに供給された場合、暗号化結果として、演算器６１ｃから暗号化情報「１０１１１０００００１０１」が出力される。

【００６７】
復号器２５の場合には、たとえば、乱数としてのマスター鍵情報「１１０１０００００１１０」がシフトレジスタ６０ａ～６０ｇに供給され、暗号化鍵情報　「１００００１１１００１０１」が演算器６１ｃに供給された場合、復号化結果として、演算器６１ｃから復号化情報としての鍵情報「１０１００１０００１０１１」が出力される。

【００６８】
なお、ユーザパスワードを入力する入力部としてキーボード２８を用いているが、ユーザパスワードの代わりに声紋を用い、入力部としてマイクと声紋特徴検出器とを用いるようにしても良い。また、ユーザパスワードの代わりに顔情報を用い、入力部としてＣＣＤ等からなる顔画像読取部と顔情報特徴抽出器とを用いるようにしても良い。また、ユーザパスワードのキー入力の代わりにパスワードの音声認識を用い、入力部としてマイクと音声認識装置とを用いるようにしても良い。また、ユーザパスワードの代わりに指紋を用い、入力部としてＣＣＤ等からなる指紋読取部と画像特徴抽出器とを用いるようにしても良い。また、ユーザパスワードの代わりに指情報を用い、入力部として電極アレイによる各点での指表面抵抗値測定装置と指情報特徴抽出装置とを用いるようにしても良い。

【００６９】
上記ＩＣカード４は、図９に示すように、ＩＣカード４の全体を制御するＣＰＵ３１、制御プログラムが記録されているＲＯＭ３２、データ記録用のＲＡＭ３３、ユーザ対応鍵情報、ユーザパスワード、ユーザＩＤ等が記録されるＥＥＰＲＯＭ３４、ユーザ対応鍵情報を生成するユーザ対応鍵情報生成器３５、マスター鍵情報を生成するマスター鍵生成器３６、暗号化鍵情報４１をマスター鍵情報により鍵情報への復号化を行う復号器３７、暗号化情報４０を鍵情報により生情報への復号化を行う復号器３８、インターフェース３９、コネクト部５、ユーザパスワードが入力されるユーザパスワード入力端子６ａ、マスター鍵情報が入力されるマスター鍵入力端子７ａにより構成されている。
【００７０】
上記ＩＣカード４は、セキュリティの確保のためユーザ個々人に認証用ＩＣカード２０を持たせており、このＩＣカード２０内に全ての復号化回路が内蔵されている。この方式ではマスター鍵情報６や鍵情報３がＩＣの外に出ることは無く、ハッカーによる不正を防止している。従って図１に示した情報伝送システムでは復号化回路が内蔵されているＩＣカード２０が暗号解読装置であり、情報伝送システム全体から見ると暗号解読部に相当する。
【００７１】
ユーザ対応鍵情報生成器３５は、排他的論理和演算を行う演算器で構成され、ユーザパスワード入力端子６ａから入力されるユーザパスワードとマスター鍵入力端子７ａから入力されるマスター鍵情報の排他的論理和演算を行うことにより、演算結果としてユーザ対応鍵情報を生成するものである。
【００７２】
たとえば、ユーザパスワード「１１００」とマスター鍵情報「１０１０」の演算により、ユーザ対応鍵情報「１００１」を生成する。
マスター鍵生成器３６は、排他的論理和演算を行う演算器で構成され、ＥＥＰＲＯＭ３４から読出されたユーザ対応鍵情報と外部から供給されるユーザパスワードの排他的論理和演算を行うことにより、演算結果としてマスター鍵情報を生成するものである。
【００７３】
たとえば、ユーザ対応鍵情報「１００１」とユーザパスワード「１１００」の演算により、マスター鍵情報「１０１０」を生成する。
上記復号器３７、３８は、それぞれ図８に示すように、７個のシフトレジスタ６０ａ～６０ｇと３個の排他的論理和演算を行う演算器６１ａ～６１ｃからなる乱数発生器により構成されている。これにより、シフトレジスタ６０ａ～６０ｇにロードされた情報に対して、演算器６１ｃに逐次供給される情報により演算を行うようになっている。
【００７４】
復号器３７の場合には、たとえば、乱数としてのマスター鍵情報「１１０１０００００１１０」がシフトレジスタ６０ａ～６０ｇに供給され、暗号化鍵情報　「１００００１１１００１０１」が演算器６１ｃに供給された場合、復号化結果として、演算器６１ｃから復号化情報としての鍵情報「１０１００１０００１０１１」が出力される。
【００７５】
復号器３８の場合には、たとえば、乱数としての鍵情報「１０１００１０００１０１１」がシフトレジスタ６０ａ～６０ｇに供給され、暗号化情報「１０１１１００００００１０１」が演算器６１ｃに供給された場合、復号化結果として、演算器６１ｃから復号化情報としての生情報「１１１０００１１１００００１」が出力される。
【００７６】
次に、ホストサーバ３によるハードディスク装置（ＨＤＤ）２９への上述した（ユーザに提供する）サービス情報の記録方法について、図１０に示すフローチャートと、図１１の暗号化鍵情報４１と暗号化情報４０の生成過程を示す図を参照しつつ説明する。
【００７７】
たとえば今、ホストサーバ３のプロバイダ（ユーザに対するサービス情報を提供する）が

ＣＲＴディスプレイ２７とキーボード２８からなるユーザインターフェースを用いて、例えばプログラミング（ｊａｖａ）言語などで記述されたアプリケーション用小単位の機能プログラムとしての生情報を入力する（ＳＴ１）。この生情報は、ＣＰＵ２０によりＲＡＭ２２に記録される（ＳＴ２）。

【００７８】

さらに、ホストサーバ３のプロバイダは、ユーザインターフェースを用いて、上述した図７に示すようなコード許可コード４３等からなる制御情報４２の内容を入力する（ＳＴ３）。この制御情報４２は、ＣＰＵ２０によりＲＡＭ２２に記録される（ＳＴ４）。

【００７９】

さらに、ホストサーバ３のプロバイダは、ユーザインターフェースを用いて、暫定的に暗号化鍵としての暗号化原案情報を入力する（ＳＴ５）。この暗号化原案情報は、ＣＰＵ２０によりＲＡＭ２２に記録される（ＳＴ６）。

【００８０】

そして、ＣＰＵ２０はＲＡＭ２２に記録されている暗号化原案情報と制御情報４２とを読出し、鍵情報合成器２６に出力することにより、鍵情報合成器２６で暗号化原案情報と制御情報４２との合成処理を行わせ、暗号化鍵情報４１を生成する（ＳＴ７）。ついで、ＣＰＵ２０はこの生成された暗号化鍵情報４１をＲＡＭ２２に記録するとともに、ハードディスク装置（ＨＤＤ）２９へ記録する（ＳＴ８）。

【００８１】

ついで、ＣＰＵ２０はＲＡＭ２２に記録されている上記生成された暗号化鍵情報４１とＥＥＰＲＯＭ２３に記録されているマスター鍵情報とを読出し、復号器２５に出力することにより、復号器２５で暗号化鍵情報４１をマスター鍵情報により復号化（解読）する処理を行わせ、鍵情報を生成する（ＳＴ９）。ついで、ＣＰＵ２０はこの生成された鍵情報をＲＡＭ２２に記録する（ＳＴ１０）。

【００８２】

ついで、ＣＰＵ２０はＲＡＭ２２に記録されている生情報と上記生成された鍵情報とを読出し、暗号器２４に出力することにより、暗号器２４で生情報を鍵情報により暗号化する処理を行わせ、暗号化情報４０を生成する（ＳＴ１１）。ついで、ＣＰＵ２０はこの生成された暗号化情報４０を上記暗号化鍵情報４１に対応させてハードディスク装置（ＨＤＤ）２９へ記録する（ＳＴ１２）。

【００８３】

この場合、始めに暗号化鍵情報４１を先に作り、そのあと復号器を通して初めて鍵情報を生成し、この生成した鍵情報を用いて暗号器でユーザに供給するサービス情報である暗号化情報４０を生成し、この生成された暗号化情報４０を上記暗号化鍵情報４０とともにＨＤＤ２９に記録されるようにしたものである。

【００８４】

次に、情報サービスプロバイダによる上記ＩＣカード４の発行処理、つまりユーザ対応鍵情報のＩＣカード４内への登録方法について、図１２に示すフローチャートを参照しつつ説明する。基本的にはＩＣカード４がユーザの手元に届く前に情報サービスプロバイダが設定を行う。

【００８５】

このＩＣカード４を発行する発行機は、上記ＩＣカード４のコネクト部５とデータのやり取りが行えるとともに、ユーザパスワード入力端子６ａとマスター鍵入力端子７ａを介して入力が行えるカードリーダ・ライタと、表示部と入力部からなるユーザインターフェースと、発行処理を制御する制御部から構成されている。

【００８６】

すなわち、情報サービスプロバイダは何も記録がなされていないＩＣカード４を上記発行機に挿入する（ＳＴ２１）。これにより、発行機のカードリーダ・ライタとＩＣカード４のコネクト部５、ユーザパスワード入力端子６ａ、マスター鍵入力端子７ａとが接続される（ＳＴ２２）。

【００８７】
さらに、情報サービスプロバイダはユーザインターフェースによりＩＣカードの発行を指示するとともに、ユーザとの契約時に情報サービスプロバイダが決めたユーザパスワードと情報サービスプロバイダーのみが知っているマスター鍵情報とを入力する（ＳＴ２３）。これにより、ＩＣカードリーダ・ライタ１３およびユーザパスワード入力端子６ａとマスター鍵入力端子７ａを介して、ユーザパスワードとマスター鍵情報とがユーザ対応鍵情報生成器３５に供給される（ＳＴ２４）。すると、ユーザ対応鍵情報生成器３５はそれらの情報のビット単位の排他的論理和演算を行うことによりユーザ対応鍵情報を生成し、ＥＥＰＲＯＭ３４に出力する（ＳＴ２５）。これにより、ＥＥＰＲＯＭ３４にユーザ対応鍵情報が記録される（ＳＴ２６）。

【００８８】
また、ユーザ対応鍵情報が記録された後、情報サービスプロバイダはユーザとの契約時に決められたユーザパスワードとユーザＩＤとを入力する。これにより、ＣＰＵ１０は、ユーザパスワードとユーザＩＤとをＩＣカードリーダ・ライタ１３、コネクト部５、およびインターフェース３９を介してＣＰＵ３１に出力する。ＣＰＵ３１は、供給されるユーザパスワードとユーザＩＤとをＥＥＰＲＯＭ３４に記録する。

【００８９】
上記ユーザ対応鍵情報等が記録された後、上記発行機からＩＣカード４が発行される。この発行されたＩＣカード４に対して、ユーザパスワード入力端子用穴６とマスター鍵入力端子用穴７が、プロバイダにより樹脂封入等で埋めこまれる。これにより、ユーザ対応鍵情報生成器３５への外部からの入力経路を遮断することができ、後からユーザ対応鍵情報が変更できない、つまり不正改ざんを防止できる。

【００９０】
次に、クライアントマシン１における立上げ処理により、ホストサーバ３に対してワープロソフト等のプログラムの転送要求を行い、この要求に応じて得られる暗号化されている情報をＩＣカード４により解読して、機能プログラムとして設定する処理について、図１３に示すフローチャートを参照しつつ説明する。

【００９１】
まず、クライアントマシン１の図示しない電源をオンし、クライアントマシン１を立上げる（ＳＴ３１）。すると、クライアントマシン１は、ホストサーバ３とのやり取りにより、特定のグループ（課金システム等）に欲しいデータがあるかを確認する（ＳＴ３２）。たとえば、情報サービスとしてのワープロソフト等のプログラムのリクエストを行う。この確認（リクエスト）が指示された際、ＣＰＵ１０は上記データの呼び出しが可能な（解読が行える）ＩＣカード４の挿入を表示部１４により案内する（ＳＴ３３）。この案内に応じて、ユーザは対応するＩＣカード４を挿入する（ＳＴ３４）。

【００９２】
ついで、ＣＰＵ１０はユーザＩＤとユーザパスワードの入力を表示部１４により案内する（ＳＴ３５）。この案内に応じて、ユーザはユーザＩＤとユーザパスワードを入力する（ＳＴ３６）。

【００９３】
この入力されたユーザＩＤとユーザパスワードは、ＣＰＵ１０によりＩＣカードリーダ・ライタ１３、コネクト部５、インターフェース３９を介してＩＣカード４内のＣＰＵ３１に供給される（ＳＴ３７）。これにより、ＣＰＵ３１は供給されたユーザＩＤとユーザパスワードとＥＥＰＲＯＭ２３に事前に記録されているユーザＩＤとユーザパスワードとをそれぞれ比較し、一致するか否かを判断し（ＳＴ３８）、一致時、ユーザＩＤをクライアントマシン１に通知し（ＳＴ３９）、不一致時、不正と見なし動作を停止し、ＮＧ信号をクライアントマシン１に通知する（ＳＴ４０）。

【００９４】
上記ステップ３８による判断結果の一致時に、ステップ３９の処理と並行して、ＣＰＵ３１は上記ユーザパスワードとＥＥＰＲＯＭ３４に事前に記録されているユーザ対応鍵情報

とをマスター鍵生成器３６により排他的論理和演算を行い、演算結果としてマスター鍵情報を生成し、ＲＡＭ３３に記録しておく（ＳＴ４１）。

【００９５】

上記ステップ３９によりユーザＩＤが通知されたクライアントマシン１は、上述したユーザによる情報サービスとしてのワープロソフト等のプログラムのリクエストに基づいた情報サービス要求とＩＣカード４から得られたユーザＩＤとにクライアントマシン１のＩＰアドレスを付与してホストサーバ３に送信する（ＳＴ４２）。このホストサーバ３はその転送要求に応じて、ユーザＩＤを認証後、ハードディスク装置（ＨＤＤ）２９に暗号化されて記録されている情報サービスとしてのワープロソフト等のプログラム（暗号化情報４０）とその暗号化情報に対応する暗号化鍵情報４１（復号化するための情報で暗号化されている）とに送信元と送信先のアドレスが入っているＩＰアドレスを付与した通信パケットに入れて、転送要求のあったクライアントマシン１に返送する（ＳＴ４３）。この際、情報サービスの送信として、上記ユーザＩＤのユーザに対する課金の内容が図示しない記録部に記録される。

【００９６】

上記返送に応じて、クライアントマシン１はＩＣカード４を用いて暗号化情報４０を暗号化鍵情報４１とこの暗号化鍵情報４１内の制御情報４２により復号化（解読）し（ＳＴ４４）、この復号化されたワープロソフト等のプログラムを用いて処理が行えるようになる（ＳＴ４５）。

【００９７】

上記暗号化情報４０の復号化処理について、図１４に示すフローチャートを参照しつつ説明する。

すなわち、クライアントマシン１のＣＰＵ１０は、受信した通信パケット内のＩＰアドレスによりホストサーバ３が設置されている地域のリージョンコードを判断し、その送信元のＩＰアドレスと判断したリージョンコードとからなり、もし通信回線２が１０ＭＨｚのＬＡＮネットワークの場合には上述したようにドライブコード４４の値である「１Ｈ」も付加したクライアントマシン生成情報を作成し、ＩＣカード４へ送る（ＳＴ５１）。

【００９８】

これにより、ＩＣカード４のＣＰＵ３１は供給されるクライアントマシン生成情報をＲＡＭ３３に記録する（ＳＴ５２）。

また、その情報の供給と並行して、ＣＰＵ３１は上記一致が判定されているユーザパスワードとＥＥＰＲＯＭ３４に事前に記録されているユーザ対応鍵情報とをマスター鍵生成器３６により排他的論理和演算を行うことにより、演算結果としてマスター鍵情報を生成し、ＲＡＭ３３に記録する（ＳＴ５３）。

【００９９】

以上の準備が整った段階で、ＩＣカード４のＣＰＵ３１はコピー許可コード４３の送信要求をクライアントマシン１のＣＰＵ１０へ送信する（ＳＴ５４）。この送信要求に応じて、クライアントマシン１のＣＰＵ１０は、暗号化鍵情報４１内に埋め込まれている制御情報４２の中からコピー許可コード４３を取出し、ＩＣカード４のＣＰＵ３１へ送信する（ＳＴ５５）。

【０１００】

これにより、ＩＣカード４のＣＰＵ３１はコピー許可コード４３が“１”か“０”かで、コピー許可かコピー不許可を判断する（ＳＴ５６）。

この判断の結果、コピー許可が判断された場合、ＣＰＵ３１は暗号化情報４０等の出所がＨＤＤ１６や光ディスク装置１７のディスクに複製されたものだとしても無条件に受付け、後段のステップ６１の復号化作業へと進む。

【０１０１】

上記ステップ５６の判断の結果、コピー不許可が判断された場合、暗号化情報４０等の出所を確認する必要があるため、ＣＰＵ３１はドライブコード４４、アドレスコード４５、リージョンコード４６の送信要求をクライアントマシン１のＣＰＵ１０へ送信する（ＳＴ

５７）。この送信要求に応じて、クライアントマシン１のＣＰＵ１０は、暗号化鍵情報４１内に埋め込まれている制御情報４２の中からドライブコード４４、アドレスコード４５、リージョンコード４６を取出し、ＩＣカード４のＣＰＵ３１へ送信する（ＳＴ５８）。

【０１０２】

これにより、ＩＣカード４のＣＰＵ３１はクライアントマシン１から供給されるドライブコード４４、アドレスコード４５、リージョンコード４６と、ＲＡＭ３３に記録されているクライアントマシン生成情報との一致を確認する（ＳＴ５９）。

【０１０３】

すなわち、暗号化情報等の出所が１０ＭＨｚのＩＳＤＮであればクライアントマシン生成情報内のドライブコードは“１Ｈ”となり、制御情報４２のドライブコード４４の“１Ｈ”と一致し、暗号化情報等の出所が正しいものと判断される。

【０１０４】

また、暗号化情報等の出所がＨＤＤ１６から再生されている場合にはクライアントマシン生成情報内のドライブコードは“ＣＨ”となり、制御情報４２のドライブコード４４の“１Ｈ”と一致しないため、暗号化情報等の出所が正しくない、つまり不正コピーした情報と判断される。

【０１０５】

また、クライアントマシン生成情報内の送信元のＩＰアドレスと制御情報４２のアドレスコード４５とが一致しているか否かにより、暗号化情報等がオリジナルなものか海賊版として不正に商業用にコピーしたものなのかが判断される。

【０１０６】

上記ステップ５９により、不一致が判断された際、ＣＰＵ３１は、不正と見なし動作を停止し、ＮＧ信号をクライアントマシン１に通知する（ＳＴ６０）。

上記ステップ５９により、一致が判断された際（暗号化情報等がオリジナルなものと判断された際）、あるいは上記ステップ５６によりコピー許可が判断された際、ＣＰＵ３１は、復号化の許可を判断し、復号化作業を開始を判断し、暗号化鍵情報４１の送信要求をクライアントマシン１のＣＰＵ１０へ送信する（ＳＴ６１）。この送信要求に応じて、クライアントマシン１のＣＰＵ１０は、暗号化鍵情報４１をＩＣカード４へ送信する（ＳＴ６２）。

【０１０７】

これにより、ＩＣカード４のＣＰＵ３１は復号器３７によりクライアントマシン１から供給される暗号化鍵情報４１をＲＡＭ３３に記録されているマスター鍵情報により復号化（解読）する処理を行わせ、鍵情報を生成し、ＲＡＭ３３に記録する（ＳＴ６３）。

【０１０８】

ついで、ＣＰＵ３１は暗号化情報４０の送信要求をクライアントマシン１のＣＰＵ１０へ送信する（ＳＴ６４）。この送信要求に応じて、クライアントマシン１のＣＰＵ１０は、暗号化情報４０をＩＣカード４へ送信する（ＳＴ６５）。

【０１０９】

これにより、ＩＣカード４のＣＰＵ３１は復号器３８によりクライアントマシン１から供給される暗号化情報４２をＲＡＭ３３に記録されている鍵情報により復号化（解読）する処理を行わせ、生情報を生成し、クライアントマシン１へ送信する（ＳＴ６６）。

【０１１０】

この生情報の送信に応じて、クライアントマシン１のＣＰＵ１０は、送信されてきた生情報としてのワープロソフト等のプログラムをＲＡＭ２２に記録する　（ＳＴ６７）。この結果、クライアントマシン１においてＲＡＭ２２に記録されているワープロソフト等のプログラムを用いて処理を行うことができる。

【０１１１】

上記のように、ユーザパスワードを用いてＩＣカード４内でマスター鍵生成器により共通鍵であるマスター鍵情報をユーザには見えない場所で生成することができる。

【０１１２】

また、ユーザ対応鍵情報をＥＥＰＲＯＭにあらかじめ記録しておき、このユーザ対応鍵情報とユーザにより入力されるユーザパスワードとからマスター鍵生成器により共通鍵であるマスター鍵情報を生成し、この生成されたマスター鍵情報を用いて復号器により暗号化された情報を復号化するようになっている。

【０１１３】

上記したように、ホストサーバのユーザ要求毎の暗号化処理が不要となるため、低コストで情報配送が可能となる。

また、非常に容易に情報の不正コピーを発見することができ、セキュリティーを大幅に向上させる事ができる。

【０１１４】

暗号化を技術的に見ると、データそのものを共通鍵で暗号化し、この共通鍵のみを公開鍵で再度暗号化するという従来のハイブリッド方式に比べ、２重に共通鍵を発行し、一方の共通鍵は暗号化して暗号化されたデータと一緒に情報伝達（暗号化された共通鍵の転送）し、他方の共通鍵はユーザからの特定情報を用いてＩＣカード４内で復号化するものである。このため、伝達経路途中およびユーザ自身のどちらにも共通鍵が見えることがない。

【０１１５】

したがって、共通鍵方式の欠点に対して、

１．鍵の転送中の第３者による不正コピーされる危険性が少ない。

２．鍵の管理が容易（ユーザはＩＣカードを１枚持てば良い）。

３．受信先での暗号データの改ざんが難しい。

と大幅に改善されているだけで無く、

アシンメトリック方式に比べて

４．情報サービスプロバイダ側／ユーザ側とも、暗号化／復号化処理が相対的に容易で短時間で処理できる。

５．情報サービスプロバイダ側はマスター鍵のみ設定すれば良く、ユーザ毎の管理センタへの公開鍵の問い合わせを行う必要がないので、ユーザへの情報提供作業が大幅に効率化できる。

６．情報サービスプロバイダ側は、事前に暗号化された情報をＩＣカード側に記録しておき、それをそのまま配送できる。このため、ユーザの要求毎に暗号化して情報配送する従来の暗号化方式と比べると、情報サービスプロバイダ側の負担は大幅に改善される。

７．ＩＣカードを用いた、個人認証用にユーザパスワードを入力するという、従来の認証手続だけで、復号化の準備が完了する。従って、セキュリティー確保のため、新たにユーザに負担を強いることなく、暗号化技術を採用することができる。

８．暗号化鍵情報の制御情報内にドライブコードやアドレスコードが含まれているため、ユーザ側で暗号化された情報をそのままＨＤＤや光ディスクにコピーし、不正使用をすることを防止できる。

【０１１６】

この結果、従来の暗号化技術の欠点をすべて改善し、情報送付元・受信先ともに処理を大幅に簡素化し、セキュリティ機能を強化することができる。

次に、第２の実施態様として、ＤＶＤ－ＲＯＭ等の光ディスク１７ａに第１の実施形態のホストサーバ３の記録部（ＨＤＤ２９）に記録したような暗号化情報４０と制御情報４２が嵌め込まれる暗号化鍵情報４１からなる情報（図２参照）が記録され、このＤＶＤ－ＲＯＭ１７ａを第１の実施形態のクライアントマシン１の光ディスク装置（ＲＯＭドライブ）１７に装填して再生する場合について説明する。

【０１１７】

この場合、制御情報内のドライブコードとしてＤＶＤ－ＲＯＭを示す「ＦＨ」が記述され、時間情報として光ディスクの原盤が作成された時期を表す製造年月日が記述されている。

【０１１８】

すなわち、第１の実施形態のようにホストサーバから暗号化情報４０と制御情報４２が嵌

め込まれる暗号化鍵情報４１とＩＰアドレスからなる通信パケットが送信される代わりに、光ディスク装置１７に装填されたＤＶＤ－ＲＯＭ１７ａから暗号化情報４０と制御情報４２が嵌め込まれる暗号化鍵情報４１とが再生される。以降の動作は、図１３、図１４に示すフローチャートの場合とほぼ同様に処理される。ただし、クライアントマシン生成情報内のドライブコードは“ＦＨ”となり、制御情報４２のドライブコード４４の“ＦＨ”と一致した際に、暗号化情報等の出所が正しいものと判断される。

【０１１９】

また、光ディスク（ＤＶＤ－ＲＯＭ）１７ａに記録される暗号化情報としては、プログラム等の他にビデオデータ等他の情報であっても良い。

また、図１３、図１４に示す動作の内、ユーザパスワードに関係した部分の処理（ステップ５３）を行わないようにしても良い。この場合、ＩＣカード４にはユーザ対応鍵情報の代りにマスター鍵情報があらかじめＥＥＰＲＯＭ３４に記録されている。

【０１２０】

また、以下に示す光ディスク（ＤＶＤ－ＲＯＭ）１７ａの製造時に用いられ原盤７０に、第１の実施例の図１０～図１２を用いて説明した暗号化情報４０と制御情報４２が嵌め込まれる暗号化鍵情報４１のＨＤＤ２９への記録と同様にして、それらの情報が記録されることにより、光ディスク（ＤＶＤ－ＲＯＭ）１７ａが作成されるようになっている。

【０１２１】

図１５の（ａ）～（ｅ）、図１６の（ｆ）から（ｋ）を用いて上記光ディスク（ＤＶＤ－ＲＯＭ）１７ａの製造方法について説明する。

表面精度を保証するため厚み０．５～３０ｍｍの強化ガラスで作られたガラス板７１をスピンドルモータ７２の上に乗せ（図１５の（ａ））特定の回転数で回転させる。その上から有機溶媒に溶かされたフォトレジスト液をふりかけ、ガラス板７１の回転による遠心力を利用してフォトレジスト液を均一に広げる。この塗布法をスピナーコーティング法と一般には呼ばれている。その後ガラス板７１ごと６０～３００°Ｃに高温放置して有機溶媒を蒸発させ、均一な厚みｄｒのフォトレジスト層７３を形成する（図１５の（ｂ））。

【０１２２】

後述する図１６の（ｆ）～図１６の（ｉ）の工程で転写効率が低下するが、仮に全行程での転写効率が１００％だった場合にはこのフォトレジスト層７３の厚みｄｒが最終的な情報記録媒体の記録膜８４上でのピット深さまたはプリグルーブ深さになる。

【０１２３】

その後、後述する原盤記録装置によりレーザ光７５を対物レンズ７６により集光させてフォトレジスト層７３を断続的に露光し、露光部７４を作成する（図１５の（ｃ））。全周に渡る露光が完了するとガラス板７１ごと原盤記録装置から外し、図１５の（ｄ）に示すようにガラス板７１を回転させながら現像液７７を特定時間ふりかける。

【０１２４】

すると図１５の（ｅ）のように露光部７４が融けて欠落し、段差ｄｒの微小凹凸が出来上がる。このようにして出来上がったガラス板７１とフォトレジスト層７３を光ディスクの原盤７０と呼んでいる。このようにして作成した原盤７０をスピンドルモータ７２からはずし、Ｎｉによる無電解メッキ、電解メッキ（電鋳メッキ）により原盤７０の凹凸形状のレプリカを取る。図１６の（ｆ）に示すようにこのようにして形成したレプリカをマスター板７８と呼んでいる。マスター板７８作成が完了するとアセトンなどの有機溶剤中に付けてフォトレジスト層７３を溶かしてマスター板７８を原盤７０から剥離する。その後マスター板７８を元に電解メッキ（電鋳メッキ）によりマザー板７９を作成した後（図１６の（ｇ））、マザー板７９をマスター板７８から剥離する。再度マザー板７９を元にして電解メッキ（電鋳メッキ）によりスタンパ８０を作成する（図１６の（ｈ））。

【０１２５】

一般に情報記録媒体の透明プラスチック基板８３は“射出成形”と言う方法を用いて作成する。すなわち図１６の（ｉ）の用に金型Ａ８１、金型Ｂ８２を配置し、その間の隙間に高温でどろどろに溶かした樹脂材（一般に使用材料としてポリカーボネート、ＰＭＭＡや

ＡＢＳを用いる場合が多い）を押し込む。上記の工程で作成したスタンパ８０は金型Ａ８１に取り付けて有るので、樹脂材が押し込まれた段階でスタンパ８０の微小な凹凸形状が樹脂材に転写される。その後、数分放置して金型Ａ８１、金型Ｂ８２ごと樹脂材を常温まで冷やし、樹脂材が冷えて固まった頃金型Ａ８１、金型Ｂ８２の間を広げてプラスチック基板８３（上記の冷えて固まり・凹凸形状が転写された樹脂材をプラスチック基板８３と呼んでいる）を取り出す。

【０１２６】

このようにして得たプラスチック基板８３を真空中に配置し、スパッタ蒸着や真空蒸着やイオンプレーティングなどの蒸着により記録膜８４をプラスチック基板８３上に形成し、図１６の（ｊ）のような構造を作る。このようにして作成した物を２枚記録膜８４、８６が内側になるように配置し、その間を記録膜８４で充填して図１６の（ｋ）のような情報記録媒体を完成させる。

【０１２７】

図１５の（ｃ）で示したフォトレジスト層７３を局所的に露光させる原盤記録装置の構造を図１７に示す。前述したようにガラス板７１はスピンドルモータ７２上で特定の回転数で回転する。レーザ光７５は折り返しミラー８８で反射後対物レンズ７６によりフォトレジスト層７３上に集光する。折り返しミラー８８と対物レンズ７６は可動部８９として一体になってガラス板７１の半径方向に移動する。この可動部８９は送りモータ９０と送りギヤ９１により移動する。図示していないがガラス板７６上の集光スポット位置を光学的にモニタするモニタ部分を持ち、このモニタ出力に応じてスピンドルモータ７２の回転数が変化し、ガラス板７１上での相対的集光スポットの移動速度（線速）が常に一定になるように原盤記録制御部５０がコントロールしている。

【０１２８】

レーザ光源９７から出たレーザ光７５はＥ．Ｏ．変調器９４とＡ．Ｏ．変調器９３を通過後折り返しミラー８８へ到達する。微小な凹凸ピット形状であるプリピット信号はプリピット信号発生器９９の信号に応じて高速スイッチ９６をオン／オフして可変電圧発生器９５の電圧をＥ．Ｏ．変調器９４に対して印加したり、解放する。このＥ．Ｏ．変調器９４に対する印加電圧を変えるとＥ．Ｏ．変調器９４を通過するレーザ光量が変化する。このようにしてフォトレジスト層７３へ到達するレーザ光量を変化させてフォトレジスト層７３上の露光部７４、非露光部を作る。

【０１２９】

特定周波数発振器９２により特定周波数の電圧をＡ．Ｏ．変調器９３に加えることによりＡ．Ｏ．変調器９３内の特定の距離的周期を持った定在波（Ａ．Ｏ．変調器９３素子内の分子間の粗密波）が発生する。この定在波によりレーザ光７５がブラック（Ｂｒａｇｇ）反射を受け、特定の方向に曲げられる。従ってこの定在波の距離的周期が変わることによりブラック（Ｂｒａｇｇ）条件が変わり、レーザ光７５の曲がる角度も変化する。つまり特定周波数発振器９２の出力周波数を変えることによりレーザ光７５の進行方向が変化し、その結果フォトレジスト層７３上で集光点位置が半径方向に移動する。

【０１３０】

プリグルーブが特定周期蛇行する構造を有する情報記録媒体の場合にはウォーブル・グルーブ発生器／グルーブ・ピット切替器９８の出力に応じて特定の周期で周波数発振器９２の周波数が変化しでいる。またウォーブルピットの場合にはトラックピッチ（ランド・グルーブ間のピッチ）の半分だけ集光スポットがフォトレジスト層７３上で半径方向にずれるように特定周波数発振器９２の周波数を変化させる。

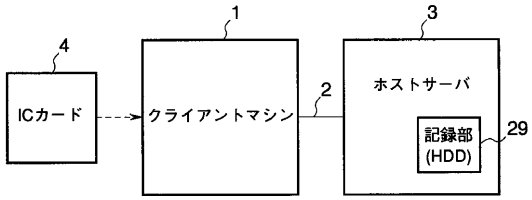
【０１３１】

上記したように、暗号化情報を復号化するための一切の復号化手段を持たないＲＯＭドライブ１７（クライアントマシン１）が単独に情報再生が可能か禁止かを判断できる。これにより、情報再生の禁止を検出した場合に、それ以降の復号化処理・再生処理を行うパソコン等の装置へ再生ならびに転送が禁止された情報を転送しないようにすることができる。

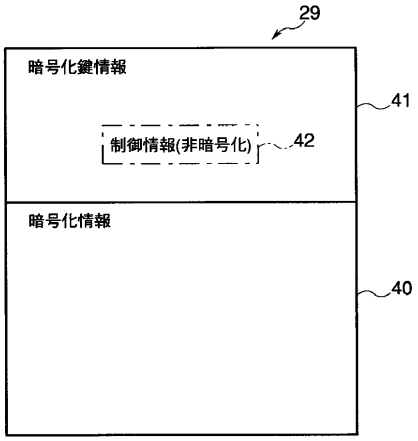
【０１３２】
また、従来のものは、復号化後の鍵に制御情報を含ませた場合には、ＲＯＭドライブ内に鍵情報を復号化する復号化手段を持たせなければならなり、コストも増加するし、従来のＲＯＭドライブとの互換性も取れなくなってしまういう欠点があるが、上記第２の実施態様では、そのような欠点を回避することができる。
【０１３３】
また、他の実施態様として、図１８に示すように、ホストサーバ１０１とユーザ用サーバ１０２とがそれぞれネットワーク１０３、１０４を介してネットワークコンピュータ１０５と接続されているネットワークシステムの場合について説明する。
【０１３４】
たとえば、ホストサーバ１０１は、第１の実施形態のホストサーバ３と同じ構成であり、暗号化情報としての暗号化されているワープロソフト等のプログラム（ユーザが使用する情報）４０と非暗号化された形で制御情報４２が嵌め込まれその暗号化情報４０を復号化（解読）する鍵情報が暗号化されている暗号化鍵情報４１とからなる情報が記録されているＨＤＤ２９を有している。
【０１３５】
ネットワークコンピュータ１０５は、ネットワークコンピュータ１０５の全体を制御する制御部１０６、ホストサーバ１０１からの暗号化情報等を受信する受信部１０７、受信受信部１０７で受信した暗号化情報等の暗号を解読する暗号解読部１０８、暗号解読部１０８により解読された情報を記録するＲＡＭメモリ１０９、制御部１０６による処理結果を暗号化する暗号器１１０、暗号器１１０により暗号化された処理結果をユーザ用サーバ１０２に情報を発信する発信部１１１により構成されている。上記暗号解読部１０８は、第１の実施形態のＩＣカード４と同じ構成と機能を有しており、暗号器１１０も第１の実施形態の暗号器２４と同じ構成と機能を有している。
【０１３６】
これにより、ホストサーバ１０１からネットワーク１０２を経由して送られてきたＪＡＶＡなどで記述された小規模機能プログラムの暗号化情報等は受信部１０７で電気信号に変換され、そのまま暗号解読部１０８に入力され、復号化後の機能プログラムはＲＡＭメモリ１０９に入力される。制御部１０６ではＲＡＭメモリ１０９から機能プログラムを読み出しながら演算処理を実施する。処理後の結果は暗号器１１０で暗号化された後、発信部１１１からネットワーク１０３を経由してユーザ用サーバ１０２に送られる。
【０１３７】
ネットワークコンピュータ１０５内の受信部１０７と発信部１１１を除く全回路はワンチップ化されているため復号化後の生信号は直接外に取り出せない構造になっており、いっそうセキュリティが強化されている。
【０１３８】
また、他の実施態様として、放送衛星を利用した例を図１９を用いて説明する。
すなわち、キー局１２１から放送衛星１２２を経由して、第１の実施形態の図２に示すような暗号化情報等が送られてくる。情報再生装置１２３内の受信部１２４で電気信号に変換後、第１の実施形態のＩＣカードにより形成される暗号解読部１２５で生信号に復号化され、表示部１２６で表示される。
上述した各実施態様によれば、セキュリティー確保が必要であるかまたは著作権確保が必要な情報に関する不正な複製の防止を行うことができる。
【０１３９】
【発明の効果】
以上説明したようにこの発明によれば、コピー許可、非許可情報の改ざんを極めて効果的に防止することができるようにした暗号情報の生成及び復号方法及び伝送及び受信装置を得ることができる。
【図面の簡単な説明】
【図１】図１は、この発明の実施の形態を説明するための情報伝送システムの概略構成を

示す図。
【図２】図２は、サービス情報の構造例を示す図。
【図３】図３は、制御情報の構成例を示す図。
【図４】図４は、図１のＩＣカードの構成を示す斜視図。
【図５】図５は、図１のクライアントマシンの概略構成を示すブロック図。
【図６】図６は、図１のホストサーバの概略構成を示すブロック図。
【図７】図７は、図６の鍵情報合成器の概略構成を示すブロック図。
【図８】図８は、図６の暗号器、復号器の概略構成を示すブロック図。
【図９】図９は、図１のＩＣカードの概略構成を示すブロック図。
【図１０】図１０は、サービス情報の記録方法を説明するためのフローチャート。
【図１１】図１１は、暗号化鍵情報と暗号化情報の生成過程を示す図。
【図１２】図１２は、ユーザ対応鍵情報のＩＣカード内への登録方法を説明するためのフローチャート。
【図１３】図１３は、要求に応じて得られる暗号化されている情報をＩＣカードにより解読して、機能プログラムとして設定する処理を説明するためのフローチャート。
【図１４】図１４は、暗号化情報の復号化処理を説明するためのフローチャート。
【図１５】図１５は、ＤＶＤ－ＲＯＭの製造方法を説明するための図。
【図１６】図１６は、ＤＶＤ－ＲＯＭの製造方法を説明するための図。
【図１７】図１７は、原盤記録装置の概略構成を説明するための図。
【図１８】図１８は、他の実施態様を説明するためのネットワークシステムの概略構成を示す図。
【図１９】図１９は、他の実施態様を説明するための放送衛星を利用した例を示す図。
【符号の説明】
１…クライアントマシン
２…通信回線
３…ホストサーバ
４…ＩＣカード
２９…記録部（ＨＤＤ）
４０…暗号化情報
４１…暗号化鍵情報
４２…制御情報

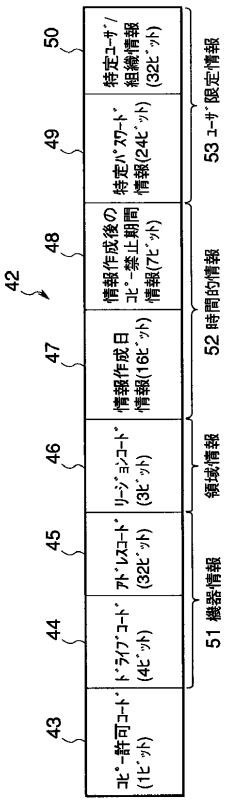
【図１】


1
3
4
ICカード
クライアントマシン
2
ホストサーバ
記録部
(HDD)
29

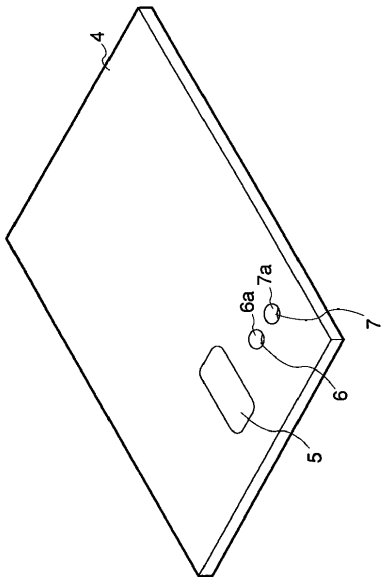
【図２】


29
暗号化鍵情報
41
制御情報(非暗号化)
42
暗号化情報
40

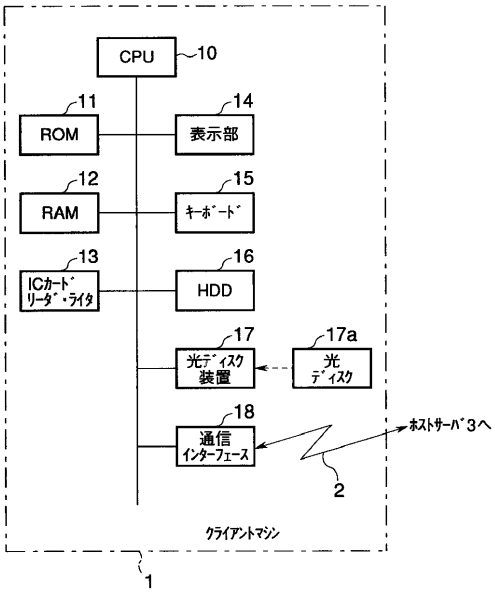
【図３】


42
50
49
48
47
46
45
44
43
特定ユーザ/組織情報(32ビット)
特定パスワード情報(24ビット)
情報作成後のコピー禁止期間情報(7ビット)
情報作成日情報(16ビット)
リージョンコード(3ビット)
アドレスコード(32ビット)
ドライブコード(4ビット)
コピー許可コード(1ビット)
53 ユーザ限定情報
52 時間的情報
領域情報
51 機器情報

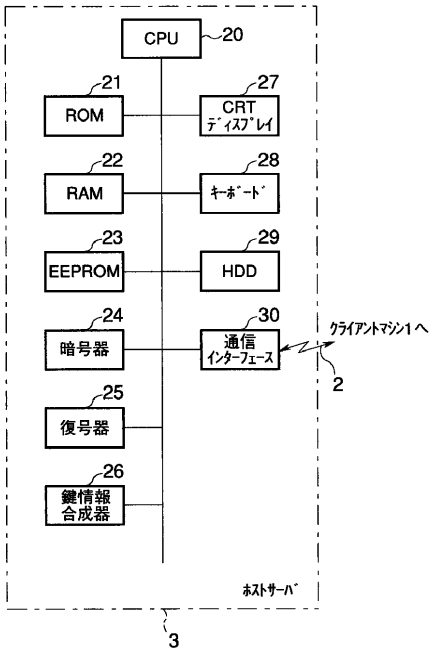
【図４】


4
6a
7a
7
6
5

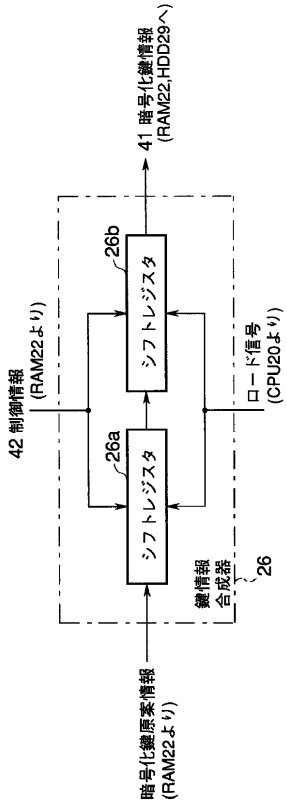
【図５】


CPU
10
ROM
11
表示部
14
RAM
12
ｷｰﾎﾞｰﾄﾞ
15
ICカード
リーダ・ライタ
13
HDD
16
光ディスク
装置
17
光
ディスク
17a
通信
インターフェース
18
ホストサーバ3へ
2
クライアントマシン
1

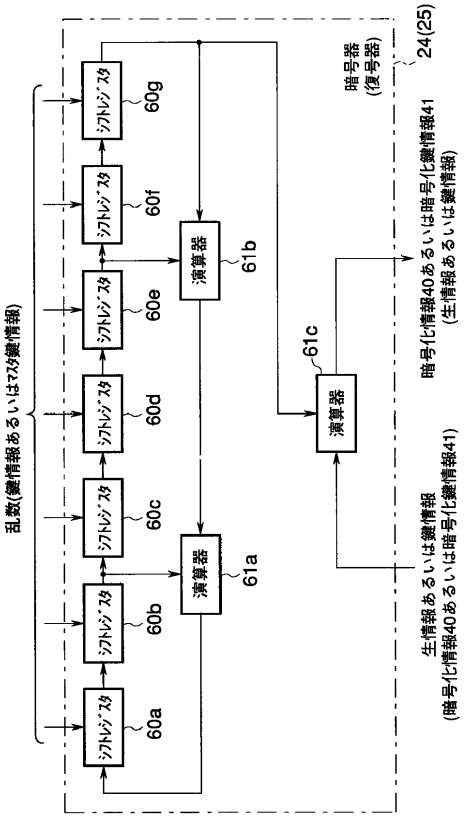
【図６】


CPU
20
ROM
21
CRT
ディスプレイ
27
RAM
22
ｷｰﾎﾞｰﾄﾞ
28
EEPROM
23
HDD
29
暗号器
24
通信
インターフェース
30
クライアントマシン1へ
2
復号器
25
鍵情報
合成器
26
ホストサーバ
3

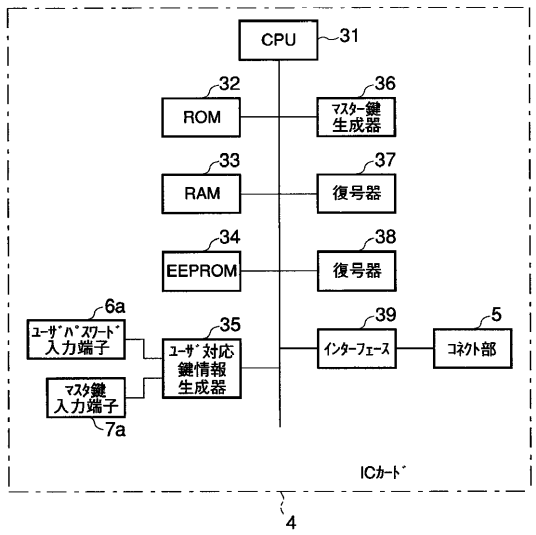
【図７】


41 暗号化鍵情報
(RAM22,HDD29へ)
26b
シフトレジスタ
42 制御情報
(RAM22より)
ロード信号
(CPU20より)
26a
シフトレジスタ
鍵情報
合成器
26
暗号化鍵原素情報
(RAM22より)

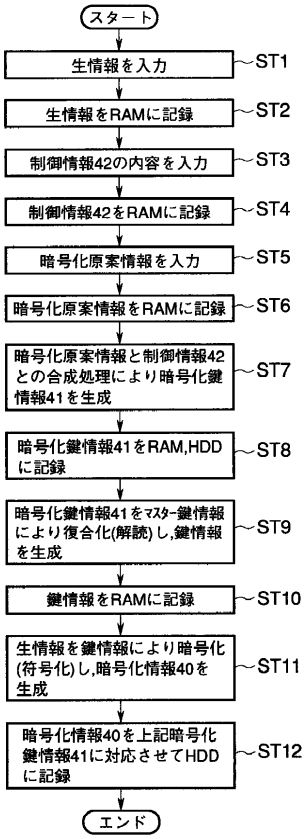
【図８】


乱数(鍵情報あるいはマスク鍵情報)
シフトレジスタ
60a
60b
60c
60d
60e
60f
60g
演算器
61a
61b
61c
暗号器
(復号器)
24(25)
暗号化情報40あるいは暗号化鍵情報41
(生情報あるいは鍵情報)
生情報あるいは鍵情報
(暗号化情報40あるいは暗号化鍵情報41)

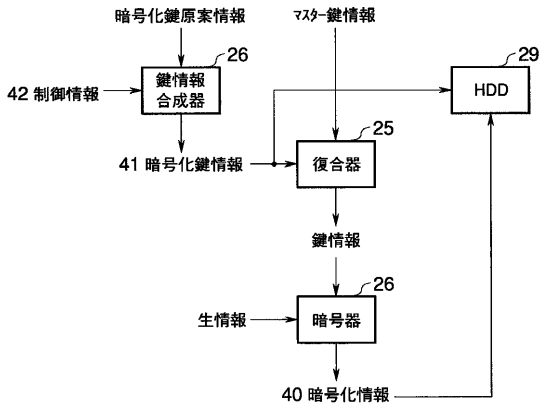
【図９】



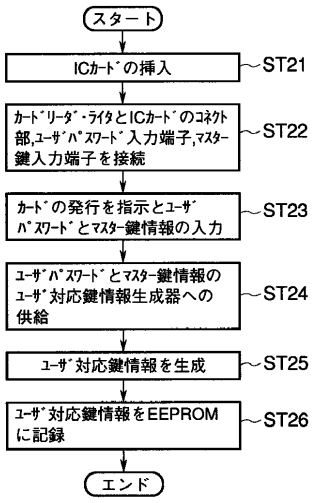
【図１０】



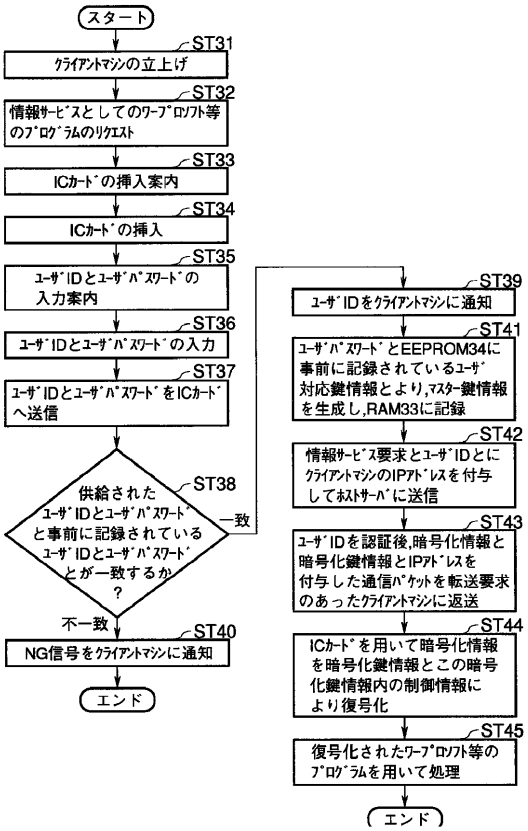
【図１１】



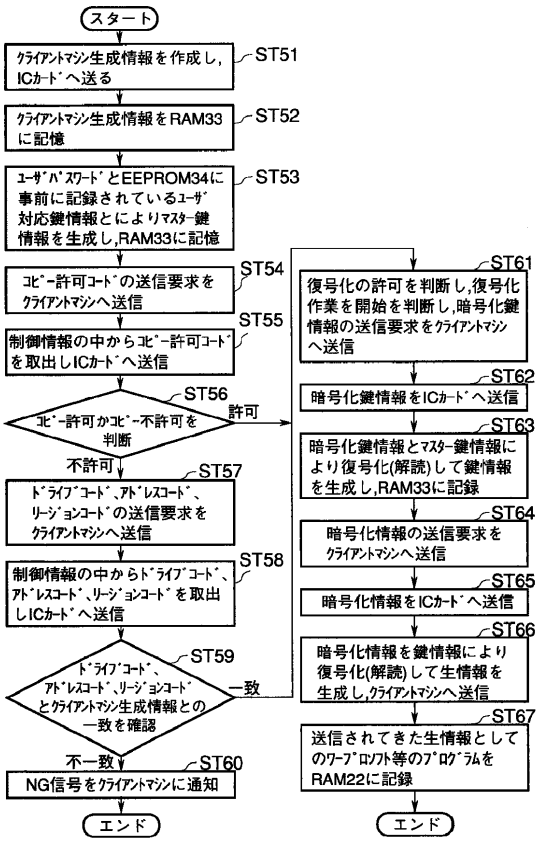
【図１２】



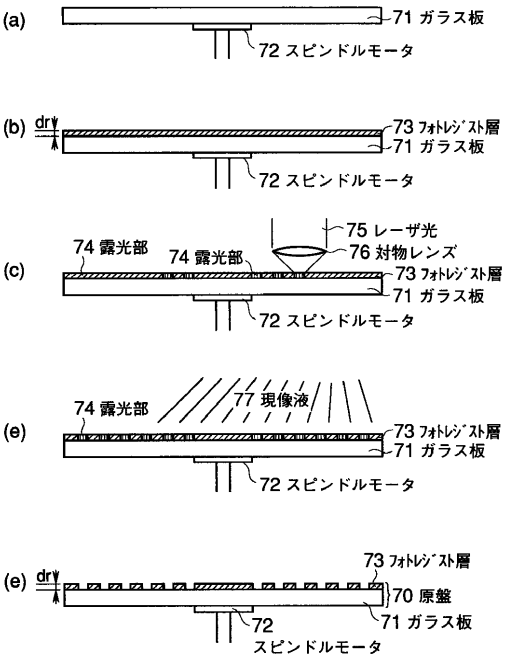
【図１３】



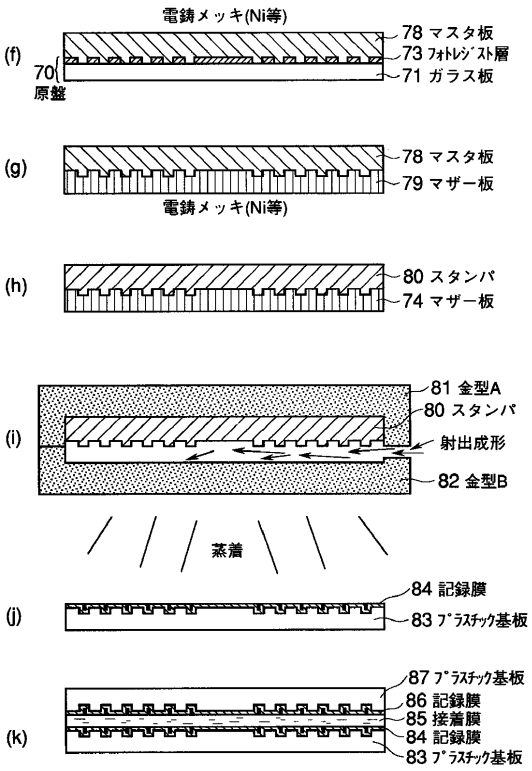
【図１４】



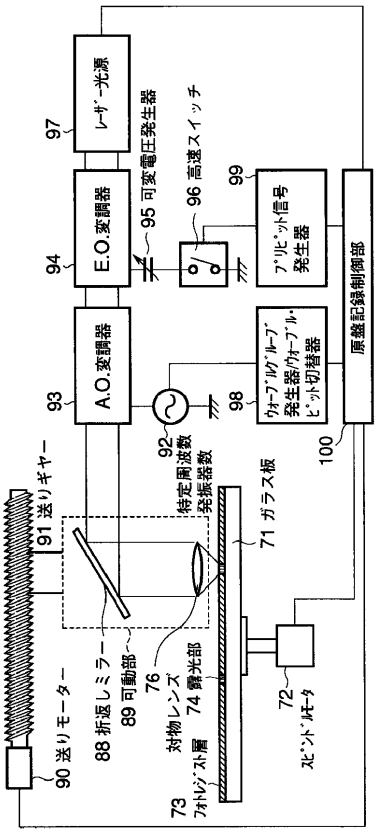
【図１５】



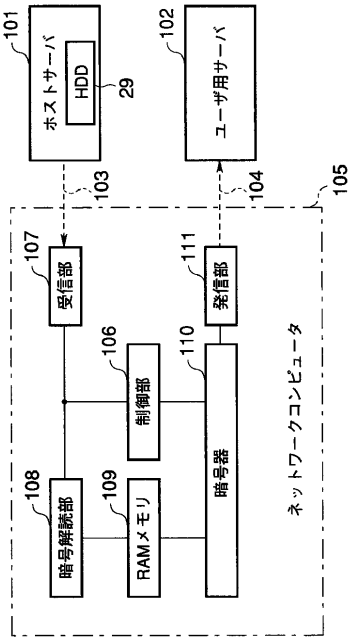
【図１６】



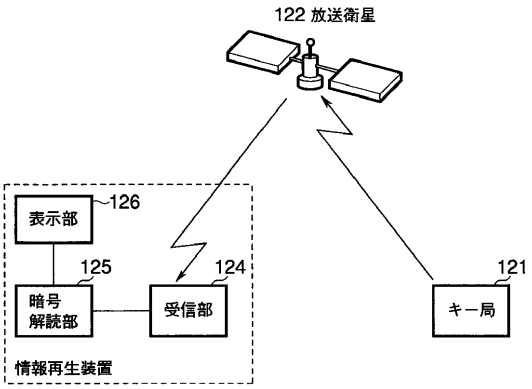
【図１７】


97 レーザー光源
94 E.O.変調器
95 可変電圧発生器
96 高速スイッチ
99 プリビット信号発生器
93 A.O.変調器
98 ウォブルグルーブ発生器/ウォブルグルーブ・ビット切替器
100 原盤記録制御部
92 特定周波数発振器
91 送りギャー
71 ガラス板
88 折返しミラー
89 可動部
76 対物レンズ
74 露光部
72 スピンドルモータ
90 送りモーター
73 フォトレジスト層

【図１８】


101 ホストサーバ
HDD
29
102 ユーザ用サーバ
103
104
105
107 受信部
111 発信部
106 制御部
110 暗号器
108 暗号解読部
109 RAMメモリ
ネットワークコンピュータ

【図１９】


122 放送衛星
126
表示部
125
暗号解読部
124
受信部
121
キー局
情報再生装置

フロントページの続き

(51)Int.Cl.			FI		
H04L 9/32	***(2006.01)***		Ｇ１１Ｂ	20/10	Ｈ
			Ｇ０６Ｋ	19/00	Ｒ
			Ｈ０４Ｌ	9/00	６７１

(74)代理人　100070437
弁理士　河井　将次
(72)発明者　山田　尚志
神奈川県川崎市幸区柳町７０番地　株式会社東芝柳町工場内
(72)発明者　安東　秀夫
神奈川県川崎市幸区柳町７０番地　株式会社東芝柳町工場内

審査官　高橋　克

(56)参考文献　特開平０６－０９５８７１（ＪＰ，Ａ）
特開平０８－１８０１０８（ＪＰ，Ａ）
特開平０７－０５６５０７（ＪＰ，Ａ）
特開２００３－０１５９６０（ＪＰ，Ａ）
特開平１１－２１９２９０（ＪＰ，Ａ）
特開平１０－２８３２７０（ＪＰ，Ａ）
特開平１１－２１９２９１（ＪＰ，Ａ）
特開昭６２－１３４６７９（ＪＰ，Ａ）
特開昭６１－２６９７３３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 12/14
G06K 17/00
G06K 19/10
G09C 1/00
G11B 20/10
H04L 9/32