(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4075078号
(P4075078)
(45)発行日　平成20年4月16日(2008.4.16)　(24)登録日　平成20年2月8日(2008.2.8)

(51)Int.Cl.　　F I
G11B 7/007 (2006.01)　　G11B 7/007
G11B 20/10 (2006.01)　　G11B 20/10　H
G11B 20/10　301Z

請求項の数 4　(全 24 頁)

(21)出願番号　特願平9-511086
(86)(22)出願日　平成8年10月8日(1996.10.8)
(86)国際出願番号　PCT/JP1996/002924
(87)国際公開番号　WO1997/014144
(87)国際公開日　平成9年4月17日(1997.4.17)
審査請求日　平成15年1月10日(2003.1.10)
(31)優先権主張番号　特願平7-261247
(32)優先日　平成7年10月9日(1995.10.9)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願平8-8910
(32)優先日　平成8年1月23日(1996.1.23)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願平8-211304
(32)優先日　平成8年8月9日(1996.8.9)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100097445
弁理士　岩橋　文雄
(74)代理人　100109667
弁理士　内藤　浩樹
(74)代理人　100109151
弁理士　永野　大介
(72)発明者　大嶋　光昭
京都府京都市西京区桂南巽町１１５－３
(72)発明者　後藤　芳稔
大阪府大阪市城東区東中浜４－９－１７－２０１

最終頁に続く

(54)【発明の名称】光ディスク

(57)【特許請求の範囲】
【請求項１】
暗号化された主情報が第１変調方式で変調され、微小な凹凸であるピットによって記録された光ディスクの第１記録領域内の内周側所定部分において、反射膜を半径方向に長い形状でかつ複数個、部分的に除去することにより前記第１の変調方式と異なる第２変調方式でバーコード状の副情報が記録されている第２記録領域を有し、前記副情報は個々の光ディスクを識別するための第１識別情報を含み、
前記第１識別情報は、前記暗号化された主情報を復号するための復号鍵を生成するために用いられるものであり、
前記バーコード状の副情報は、前記第１記録領域内の内周側所定部分のピット領域に記録されていることを特徴とする光ディスク。
【請求項２】
前記バーコード状の副情報が記録されていることを示す副情報識別子が前記第１記録領域内のコントロールデータ領域に記録されていることを特徴とする請求項１記載の光ディスク。
【請求項３】
副情報に個々の光ディスクを識別するための第１識別情報に加えて、暗号の暗号鍵、暗号の復号鍵のいずれかが記録されている請求項１または２記載の光ディスク。
【請求項４】
第１変調方式として８－１６変調方式を用い、第２変調方式としてフェーズエンコーディ

ング変調方式を用いたことを特徴とする請求項１から３のいずれか１項に記載の光ディスク。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は光ディスクに関するものである。

【０００２】

【従来の技術】

近年、インターネット等のネットワークと光ＲＯＭディスクの普及に伴い、光ＲＯＭディスクを用いたネットワークソフト流通が始まりつつある。また電子商取引の検討が進んでいる。

【０００３】

従来技術として、ＣＤ－ＲＯＭをメディアとして用いたソフト電子流通システムが実用化されている。この場合パスワードを与えて、ＣＤ－ＲＯＭに予め記録され暗号化されたソフトの暗号を解くといった方法が一般的である。

【０００４】

【発明が解決しようとする課題】

しかし、ＣＤ－ＲＯＭの場合、ディスク上に追記記録できないため各ディスクのＩＤは個別に設定できない。従って単純に用いれば、１つのパスワードが同一原盤から製造された全てのディスクの暗号を解除してしまう。このため、ＣＤ－ＲＯＭを用いた場合、各々のディスク個有のＩＤをパソコン側のハードディスク上に作成したり、センターで作成したＩＤを郵便によりユーザーに送ったりするという作業が必要であった。

【０００５】

従来の光ディスクや光ディスクシステムを用いた電子流通システムにおいては、光ディスクもしくはシステムにＩＤや暗号鍵を簡便に供給することが求められている。本発明はＲＯＭディスクを用いた電子流通システムにＩＤと暗号鍵の簡便な供給を実現することを目的とする。

【０００６】

【課題を解決するための手段】

この課題を解決するために、光ディスクのピット部にバーコードを重ね書きした追記領域（以下ＢＣＡと略す）を設け光ディスク製造時に、ＢＣＡ領域にディスク毎に異なるＩＤと必要に応じて通信用の暗号鍵、受信用の復号鍵暗号文の復号鍵を個別に記録しておくことにより、ディスクをユーザーに配布した時点で、ユーザーにはユーザーＩＤ番号と通信用の送信用の暗号鍵、受信用の復号鍵の３つが自動的に配布されていることになり、従来のシステムを複雑にしていたいくつかの手順が省略できる。こうして、暗号通信とコンテンツの入ったディスクの識別が同時に実現する。

【０００７】

【発明の実施の形態】

実施例に基づき、本発明を説明する。なお、本文ではＢＣＡ方式を用いた追記領域をＢＣＡ領域、ＢＣＡにより記録されたデータをＢＣＡデータと呼ぶ。また第１識別情報はＩＤ、もしくはディスクＩＤとも呼ぶ。

【０００８】

図１はＢＣＡ付ディスクの代表的な製造工程を示す。まず、公開鍵等の第１暗号鍵８０２を用いて暗号エンコーダ８０３でコンテンツ７７７が暗号化された第１暗号８０５がマスタリング装置等の８－１６変調器９１７により変調され、この変調信号がレーザーにより原盤８００の第１記録領域９１９に凹凸のピットとして記録される。この原盤８００を用いて成形機８０８ａでディスク状の透明基板を成形し、反射膜作成機８０８ｂでＡｌ反射膜を形成し０．６ミリ厚の片面ディスク８０９ａ、８０９ｂを作成し、貼り合わせ機８０８ｃで貼り合わせた完成ディスク８０９の第２記録領域９２０にトリミング装置８０７で、ディスクＩＤ９２１もしくは第１暗号の復号鍵９２２もしくはインターネット通信用の

第２暗号鍵９２３をＰＥ変調とＲＺ変調を組み合わせたＰＥ－ＲＺ変調器８０７ａで変調し、パルスレーザーを用いた記録手段８０７ｂでＢＣＡトリミングして、ＢＣＡ付ディスク８０１を製造する。貼り合わせディスクを用いているので、中に入ったＢＣＡは改ざん出来ず、セキュリティ用途に用いることが出来る。

【０００９】

説明に入る前に、ＢＣＡについて、簡単に説明する。

【００１０】

図２の（１）に示すようにＢＣＡでは２層ディスク１８００にパルスレーザー１８０８で、アルミ反射膜１８０９をトリミングし、ストライプ状の低反射部８１０ａをＰＥ変調信号に基づいて記録する。図２（２）に示すようにＢＣＡのストライプがディスク上に形成され、このストライプを通常の光ヘッドで再生するとＢＣＡ部は反射信号がなくなるため図２（３）に示すように変調信号が間欠的に欠落した欠落部１８１０ａ、１８１０ｂ、１８１０ｃが発生する。変調信号は第１スライスレベル９１５でスライスされる。一方欠落部１８１０ａ等は信号レベルが低いので、第２スライスレベル９１６で容易にスライスできる。図３の記録再生波形図に示す様に、形成されたバーコード９２３ａ、９２３ｂは、図３（５）に示すように通常の光ピックで第２スライスレベル９１６でレベルスライスすることにより再生可能で図３（６）に示すようにＬＰＦフィルタで波形成形されＰＥ－ＲＺ復調され、（７）に示すようにデジタル信号が出力される。図４を用いて復調動作を説明する。まず、ＢＣＡ付ディスク８０１は透明基板が２枚、記録層８０１ａが中にくるように貼り合わせてあり、記録層が記録層８０１ａの１層の場合と記録層８０１ａ、８０１ｂの２層の場合がある。２層の場合は光ヘッド６に近い第１層の記録層８０１ａのコントロールデータにＢＣＡが記録されているかどうかを示すＢＣＡフラグが記録されている。ＢＣＡは第２記録層８０１ｂに記録されているので、まず第１層記録層８０１ａに焦点を合わせ第１記録領域９１９の最内周にあるコントロールデータの半径位置へ光ヘッド６を移動させる。コントロールデータは主情報なのでＥＦＭ又は８－１５又は８－１６変調されている。このコントロールデータの中のＢＣＡフラグが‘１’の時のみ、１層、２層部切換部８２７ｂで、焦点を第２記録層８０１ｂに合わせてＢＣＡを再生する。第１レベルスライサ５９０で図２（３）に示すような、一般的な第１スライスレベル９１５でスライスするとデジタル信号に変換される。この信号を第１復調部においてＥＦＭ９２５復調部又は８－１５変調　復調部９２６又は８－１６変調　復調部９２７の復調器で復調し、ＥＣＣデコーダ３６でエラー訂正し主情報が出力される。この主情報の中のコントロールデータを再生し、ＢＣＡフラグが１の場合のみＢＣＡを読みにいく。ＢＣＡフラグが１の時、ＣＰＵ９２３は１層、２層部切換部８２７ｂに指示を出し、焦点駆動部８２８を駆動して、第１層の記録層８０１ａから第２層の記録層８０１ｂへ焦点を切り替える。同時に第２記録領域９２０の半径位置、すなわちＤＶＤ規格の場合はコントロールルデータの内周側の２２．３ｍｍから２３．５ｍｍの聞にＢＣＡが記録されており、光ヘッド６を移動させ、前記ＢＣＡをよみとる。ＢＣＡ領域では図２（３）に示すようなエンベロープが部分的に欠落した信号が再生される。第２レベルスライサ９２９において第１スライスレベル９１５より低い光量の第２スライスレベル９１６を設定することにより、ＢＣＡの反射部欠落部は検出でき、デジタル信号が出力される。この信号を第２復調部９３０においてＰＥ－ＲＺ復調し、ＥＣＣデコーダ９３０ｄにおいてＥＣＣデコードすることにより副情報であるＢＣＡデータが出力される。このようにして、８－１６変調　復調部９２７等の第１復調部９２８で主情報をＰＥ－ＲＺ変調の第２復調部９３０で副情報つまりＢＣＡデータを復調再生する。

【００１１】

図５（ａ）にフィルタ（ＬＰＦ９４３）通過前の再生信号波形、（ｂ）に低反射部８１０ａのスリットの加工寸法精度を示す。スリットの巾は５～１５μｍ以下にすることは難しい。また、２３．５ｍｍより内周に記録しないと記録データを破壊してしまう。このことからＤＶＤの場合最短の記録周期＝３０μｍ、最大半径＝２３．５ｍｍの制限からフォーマット後の最大容量は１８８ｂｙｔｅｓ以下に限定される。

【００１２】
変調信号は、８－１６変調方式を用いてピットで記録されており、図５（ａ）の高周波信号部９３３のような高周波信号が得られる。一方、ＢＣＡ信号は低周波信号部９３２のような低周波信号となる。このように、主情報がＤＶＤ規格の場合、最高約４．５ＭＨｚの高周波信号９３３であり、図５（ａ）に示すように、副情報が周期８．９２μｓつまり約１００ＫＨｚの低周波信号９３２であるため、ＬＰＦ９４３を用いて副情報を周波数分離することが容易である。図４に示すようなＬＰＦ９４３を含む周波数分離手段９３４で、２つの信号を容易に分離することが出来る。この場合、ＬＰＦ９４３は簡単な構成でよいという効果がある。
【００１３】
以上がＢＣＡの概略である。
【００１４】
では、図６を用いて、暗号ソフト解錠システムの全体システムをパスワード発行と暗号通信と発注者の認証の動作に絞り説明する。まず、プレス工場のステップは、図１の場合とほぼ同じ手順で製造されるので、原盤８００と完成ディスク８０９の図は省略する。
【００１５】
プレス工場８１１において、第１～ｎ番目のコンテンツの平文８１０は暗号エンコーダ８１２により、各々第１～ｎ番目の暗号鍵８１３でデータの暗号化又は映像信号のスクランブルがなされ、光ディスクの原盤８００に記録される。この原盤８００から、プレスされて製造されたディスク状の基板に反射膜が形成された後に、２枚のディスク状の基板を貼り合わせた後、完成ディスク８０９が作られる。この完成ディスク８０９に、ディスク毎に異なるＩＤ８１５もしくは／かつ第１暗号鍵８１６（公開鍵）もしくは／かつ、第２暗号鍵８１７（公開鍵）、第２コンピュータの接続アドレス８１８がＢＣＡ領域８１４に記録されたＢＣＡ付ディスク８０１が、ユーザーに配布される。
【００１６】
このディスクのコンテンツは暗号化されているので、再生するには代金等の代価を払ってパスワード発行センターつまり電子商店もしくは、モールからパスワードをもらう必要がある。この手順を述べる。
【００１７】
ユーザーの第１コンピュータ９０９では配布されたＢＣＡ付ディスク８０１を再生装置８１９で再生すると、ＰＥ－ＲＺ復調部を含むＢＣＡ再生部８２０により、ＩＤ８１５、第１暗号鍵８１６、第２暗号鍵８１７、接続アドレス８１８のデータが再生される。パスワードをもらうためには、パスワード発行センター８２１のサーバーである第２コンピュータ８２１ａの接続アドレス８１８へ通信部８２２を介してインターネット等のネットワーク８２３経由で接続し第２コンピュータ８２１ａへＩＤを送信する。
【００１８】
ここで、暗号通信の手順について述べる。第２コンピュータ８２１ａはユーザーの再生装置８１９からのＩＤ８１５を受信する。“モール”や“電子商店”とよばれるパスワード発行センター８２１の第２コンピュータすなわちサーバー８２１ａは暗号鍵ＤＢ８２４を持っている。このデータベースにはこのディスク個有のＩＤもしくはＩＤの第１暗号鍵８１６に対応する復号鍵である秘密鍵、つまり第１復号鍵８２５とＩＤの表が収容されている。従ってサーバーは受信したＩＤをもとに第１復号鍵８２５を検索することができる。こうして第１コンピュータから第２コンピュータ８２１ａへの暗号通信が成立する。この場合、第１暗号鍵と第１復号鍵は公開鍵暗号ではなく、共通鍵暗号の共通鍵ならば同じ鍵となる。
【００１９】
利用者はＢＣＡ付ディスク８０１の中に、例えば、１０００本収納されている暗号化されたコンテンツの１部、例えばコンテンツ番号８２６がｎのコンテンツを利用したい場合、コンテンツ番号８２６つまりｎを第１暗号鍵８１６である公開鍵を用いて、公開鍵暗号関数から構成される第１暗号エンコーダ８２７で、暗号化した暗号を第２コンピュータ８２

１ａに送信する。第２コンピュータ８２１ａ側では前述のようにこの暗号を復号するための第１復号鍵８２５を検索し知っている。従ってこの暗号を確実に平文化できる。こうしてユーザーの発注情報のプライバシーは暗号により守られるという効果がある。

【００２０】

この場合第１暗号鍵８１６として公開鍵暗号の秘密鍵を用いて署名してもよい。この方法は“デジタル署名”と呼ばれる。詳しい動作の説明は、暗号の専門書例えば、“Ｅ－Ｍａｉｌ Ｓｅｃｕｒｉｔｙ ｂｙ Ｂｒｕｃｅ Ｓｃｈｎｅｉｅｒ １９９５”の“Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ”の項目等を参照されたい。

【００２１】

暗号通信にもどるとこの暗号は通信部８２２とネットワーク８２３を介して、パスワード発行センター８２１の第１暗号デコーダ８２７ａに送られる。こうして、第１暗号鍵８１６と対になっている第１復号鍵８２５を用いて第１暗号デコーダ８２７ａでは、暗号が復号される。

【００２２】

この場合、公開鍵は特定の１枚のディスクしかもっていないため、第３者のディスクからの不正な注文は排除できる。つまり、１枚のディスクの認証ができるためこのディスクの持ち主のユーザー個人の認証ができる。こうしてこのコンテンツ番号ｎは特定の個人の注文であることが証明されるため、第３者の不正な注文は排除できる。

【００２３】

この時第１暗号鍵８１６を秘密にしておけば、この手法でクレジットカード番号等の高いセキュリティが要求される課金情報の送信にも技術的には用いることができる。しかし、通常“モール”と呼ばれる店では、セキュリティの保証がないため、電子決済ではユーザーの課金情報は扱わない。クレジットカード系と銀行系の課金センター８２８のみが、ユーザーの金融情報を取り扱うことができる。現在、ＳＥＴ等のセキュリティ規格の統一化が進められており、ＲＳＡ１０２４ｂｉｔの公開鍵暗号が使われ金融情報の暗号化が実現する可能性が高い。

【００２４】

次に本発明の場合の課金情報の暗号通信手順を示す。まず、ＢＣＡ再生部８２０で再生された公開鍵暗号の第２暗号鍵８１７を用いて、個人のクレジットカード番号等の課金情報８３０は第２暗号エンコーダ８３１により、ＲＳＡ等の公開鍵系暗号により、暗号化され、通信部８２２より第２コンピュータ８２１ａを介して第３コンピュータ８２８の第２暗号デコーダ８３２に送られる。この場合デジタル署名をする場合は第２暗号鍵８１７は秘密鍵８２９を用いる。

【００２５】

パスワード発行センター８２１の第２コンピュータ８２１ａの暗号鍵の場合の手順と同様にして暗号鍵ＤＢ８２４ａよりＩＤもしくは第２暗号鍵８１７に対応する第２復号鍵８２９ａを検索し、これを用いて第２暗号デコーダ８３２において暗号化された課金情報を復号することができる。

【００２６】

なお第２暗号エンコーダ８３１で秘密鍵８２９を用いてデジタル署名すれば、第２暗号デコーダ８３２ではユーザーの署名を確認できる。こうして課金センター８２８は、ユーザーのクレジットカード番号や銀行カード番号や銀行パスワード等の課金情報をインターネットを使っても安全に入手することができる。インターネットのようなオープンなネットワークではセキュリティが問題となるが、このシステムでは、暗号通信用の暗号鍵（公開鍵）もしくはかつデジタル署名の秘密鍵がＢＣＡに記録されているので、暗号通信もしくは認証が確実に行える。このため不正な第３者による不正課金と不正注文を防げるという効果がある。またディスク毎つまりユーザー毎に異なる公開鍵を用いることができるので通信の秘密性が向上し、ユーザーの課金情報が第３者に漏洩する可能性が減少する。

【００２７】

ここで、図６に戻り、パスワードの発行手順とパスワードによる解錠手順を説明する。パ

スワード発行センター８２１では、ＩＤとユーザーが解鍵したいコンテンツ番号とユーザーの使用許可期間を示す時間情報の３つの情報に基づき、公開鍵暗号等の演算式を用いたパスワード生成部８３４でパスワードを生成し、第１コンピュータ９０９へ送信する。最も簡単な構成例を述べると、第２コンピュータでは復号鍵ディスクＩＤと時間情報を混合したｎ番目のコンテンツの暗号を解除する情報を公開鍵暗号の公開鍵で暗号化し、これを解く秘密鍵を混合したｎ番目のパスワード８３４ａをパスワード生成部８３４で作成し、第１コンピュータ９０９へ送信する。第１コンピュータは上述のｎ番目のパスワードを受信し、秘密鍵でディスクＩＤと時間情報とｎ番目のコンテンツの復号鍵を復号する。ここで、ディスクより再生したＢＣＡのＩＤ８３５ａと現在の第２時間情報８３５ｂと許可されたＩＤ８３３ａと第１時間情報８３３を照合して一致するかをパスワード演算部８３６は演算する。もし一致すれば、許可し、ｎ番目の復号鍵８３６ａを暗号デコーダ８３７へ出力し、暗号化されたｎ番目のコンテンツ８３７ａが復号され、ｎ番目のコンテンツの平文１８３８ｂが出力される。出力される期間は第１時間情報８３３と第２時間情報８３５ｂが一致している間だけに制限される。第１コンピュータ９０９側では、ＩＤとｎ番目のパスワード８３５と現在の時間を示す時計８３６ｂからの時間情報の３つの情報をパスワード演算部８３６で演算し、ＩＤと時間情報が正しければ、正しい復号鍵が演算結果として出力されるので、ｎ番目の暗号が暗号デコーダ８３７で復号もしくは、デスクランブルされ、ｎ番目のコンテンツの平文１８３８ｂの平文データもしくは、デスクランブルされた映像信号もしくはオーディオ信号が出力される。

【００２８】

この場合、時計８３６ｂの第２時間情報８３５ｂがパスワードの第１時間情報８３３と一致しないと暗号が正しく復号されないので再生はされない。時間情報を用いると、レンタル利用の際に３日間だけ映画を再生できるといった時間限定型のレンタルシステムに応用することが可能となる。

【００２９】

図６ではブロック図を用いて手順を説明したが、この手順のフローチャートは図１６～図２１を用いて後で説明する。

【００３０】

次に暗号鍵の容量についての工夫を述べる。こうして図６、図７（ａ）に示すようにＢＣＡに第１暗号鍵８１６と第２暗号鍵８１７の双方を入れることにより、“モール”との商品取引と、“課金センター”との間の代金決済の２つのセキュリティが保たれるという効果が得られる。

【００３１】

この場合、課金センターとのセキュリティに関してはＳＥＴ等の規格統一が予定されており、ＲＳＡ１０２４つまり、１２８ｂｙｔｅｓの暗号鍵が、第２暗号鍵領域８１７ａに収容されることになる。すると、ＢＣＡは１８８ｂｙｔｅｓしかないため、“モール”との取引の暗号鍵用には６０ｂｙｔｅｓしか残らない。２０バイトの大きさでＲＳＡ１０２４の１２８バイトと同程度のセキュリティをもつ暗号関数として楕円関数系公開鍵暗号が知られている。

【００３２】

本実施例では、第１暗号鍵８１６に楕円関数を用いている。楕円関数はＲＳＡ１０２４と同等のセキュリティが２０バイトで得られる。このため、楕円関数を用いることにより１８８バイトのＢＣＡ領域に、第１暗号鍵８１６と第２暗号鍵８１７の双方が収容できるという効果がある。

【００３３】

以上述べたように、ＢＣＡを光ＲＯＭディスクに適用することにより、ディスク固有のＩＤ番号、第１と第２暗号鍵、接続のアドレスが記録できる。この場合インターネットを利用した場合に、自動的にモールに接続され、コンテンツの暗号解除による商品流通と、商品購入の認証と秘密保持、代金決済時の認証と機密性の保持等のセキュリティがＢＣＡに暗号鍵が記録されたディスクを配布するだけで、実現する。このため本発明の暗号通信の

方法により、従来のようなＩＤや、暗号鍵をユーザーへ配布するためにＩＣカードやフロッピィや手紙を用いるという作業がセキュリティを落とすことなしに省略でき合理化できるという大きな効果がある。またインターネットの接続アドレスであるＵＲＬは固定ではなく、変更される。原盤にはＵＲＬが記録されており、このＵＲＬに接続すればよいが、変更された時原盤を変更するのは、時間的コスト的に効率が悪い。ＢＣＡに変更されたＵＲＬを記録しておき、ＢＣＡより接続アドレス８１８が再生された場合のみ原盤の接続アドレスよりＢＣＡ接続アドレス８１８を優先して接続すれば、原盤を新規に作成することなく、変更された接続アドレス８１８に接続されるという効果がある。

【００３４】

図６ではＢＣＡに公開鍵の第１暗号鍵と公開鍵の第２暗号鍵を記録した場合を示した。

【００３５】

図８では、ＢＣＡに公開鍵の第１暗号鍵８１６と秘密鍵の第３復号鍵８３９ｂの２つを記録した場合と暗号鍵を発生させて暗号通信する場合の２種類の実施例を示す。図６と同様の手順であるため、違う点のみを述べる。まず、プレス工場では、第１暗号鍵８１６と第３復号鍵８３９ｂがＢＣＡに記録される。第３復号鍵８３９ｂは課金センターからの公開鍵で暗号化された暗号の受信に用いる。この場合、受信のセキュリティが向上するという効果がある。

【００３６】

まず、図８を用いて暗号鍵を生成するより具体的な暗号通信の例を説明する。第１暗号鍵８１６は公開鍵なので、受信用の第３復号鍵８３９ｂをＢＣＡに記録する必要がある。一方ＢＣＡは容量が少ない。又公開鍵は処理時間を要する。そこで、図８では第１コンピュータ８３６において乱数発生器等により暗号鍵生成部１８３８ａで公開鍵の暗号鍵／復号鍵の対、又は共通鍵を生成する。共通鍵の例を述べる。共通鍵Ｋ８３８を第１暗号鍵８１６と第１暗号エンコーダ８４２で暗号化し、第２コンピュータ８２１ａへ送る。第２コンピュータでは主復号鍵８４４を用いて、主暗号デコーダ８４３で、この暗号を平文化して平文化共通鍵Ｋ８３８ａを得る。双方が共通鍵Ｋをもつので、第２暗号エンコーダ８４２ａと第２暗号デコーダ８４７に共通鍵Ｋを渡すことにより、店からユーザー、つまり第２コンピュータ８２１ａから第１コンピュータ８３６への暗号通信ができる。当然共通鍵Ｋを第２暗号エンコーダ８２７ｃと第２暗号デコーダ８４５ａに渡すことにより、ユーザーから店つまり第１コンピュータ８３６から第２コンピュータ８２１ａへの暗号通信も可能となる。公開鍵である第１暗号鍵をＢＣＡに記録し、暗号鍵を生成する方式の効果を述べる。まず、第１暗号鍵の記録だけでよく復号鍵の記録が省略できる。従ってＢＣＡの少ない容量を減らすことがない。

【００３７】

また、演算時間が短いため、処理時間が少なくて済むという効果がある。この場合暗号鍵生成部１８３８ａが共通鍵ではなく、公開鍵暗号の暗号鍵と復号鍵の一対を生成した場合暗号鍵を第２コンピュータ８２１ａへ暗号送信し、第２暗号エンコーダ８４２ａの暗号鍵として用い、復号鍵を第２暗号デコーダ８４７の復号鍵として用いれば処理時間は長くなるが共通鍵に比べてよりセキュリティを高めることができる。処理するＣＰＵの性能が高い場合は公開鍵を使う方が望ましい。公開鍵を新たに生成する場合は、ＢＣＡには第１暗号鍵の公開鍵しか記録されないため、セキュリティの問題は発生しない。ＢＣＡの容量も消費されない。また暗号鍵を変更する必要がないためメンテナンスも容易となる。

【００３８】

今度はパスワード発行センター８２１の第２コンピュータ８２１ａで平文化共通鍵Ｋ８３８ａを定義した場合、共通鍵を第３暗号鍵８３９ｂを用いて第３暗号エンコーダ８４０で暗号化し、第１コンピュータ８３６へ送信する。第１コンピュータ８３６側ではＢＣＡより再生した秘密鍵である第３復号鍵８３９ｂを用いて、第３暗号デコーダ８４１で平文化することにより、第２平文化共通鍵Ｋ８３８ｂを得る。この場合、秘密鍵である第３復号鍵８３９ｂはこのユーザーしかもっていないので、センターからユーザーへの通信の内容が第３者に漏洩することが防止されるという効果がある。この場合のフォーマットを図７

（ｂ）に示す。第３復号鍵８３９ｂは楕円関数を用いると２０バイトでよいためＢＣＡに収容できる。

【００３９】

次に図９を用いて、暗号化ディスクにＢＣＡを用いて原盤作成費用を削減する実施例を説明する。

【００４０】

ｎ個例えば、１０００本の平文のコンテンツ８５０があると、各々１～ｍ番目の暗号鍵８５１を用いて暗号エンコーダ８５２で暗号化する。この暗号化された第１～ｍ番目のコンテンツ８５３と１～ｍ番のコンテンツの復号プログラム８５４ａと第２暗号を復号するプログラムである第２暗号デコーダ８６１ａは、原盤に凹凸のピットとして記録された後、１枚の基板に成形され反射膜を形成した後、２枚の基板が貼り合わせられて、ＢＣＡ付ディスク８０１が完成する。この時、ディスク１枚目に異なるディスク固有の識別情報、いいかえるとＩＤ８５５とｎ番目、例えば１番目のコンテンツを解錠するパスワードや復号鍵等の復号プログラムを第２暗号エンコーダ８６０で暗号化した第２暗号を予めＢＣＡに記録する。すると、再生装置ではＢＣＡ再生部８２０より第２暗号が再生される。ＢＣＡ以外の通常の記録データが再生されるデータ再生部８６５より第１暗号が再生されるので、第２暗号デコーダ８６１では、第１暗号を用いて第２暗号を復号し、ＩＤ８５５ａと第ｎ番目のパスワード８５４ｂが再生される。暗号デコーダ８５５ｂでは、データ再生部８６５より再生した第ｎ番目のコンテンツの復号プログラム８５３ａを用いて、ＩＤ８５５ａと第ｎ番目のパスワード８５４ｂを用いて第１暗号を復号し、ｎ番目のコンテンツの平文８５５ｃと識別情報であるＩＤ８５５ａを得る。パソコンの場合はハードディスク８６３にコンテンツとＩＤは記録される。このＩＤ８５５ａは、プログラム起動時にネットワーク上に同じＩＤがないかをチェックし、ネットワークプロテクションを動作させるので、ソフトの不正インストールが防止できるという副次的効果がある。つまり、原盤１枚に暗号化した１千本のコンテンツを入れ、特定のソフトに対応するパスワード等の復号情報を記録しておけば、実質的に特定の１本のコンテンツの光ＲＯＭディスクを作成したのと等価となる。１枚の原盤で１０００種類のソフトの原盤をカッティングしたのと同じ効果が得られ、原盤作成費用と手間が削減できるという効果がある。

【００４１】

図１０ではＲＡＭディスクに、コンテンツを記録する際にＢＣＡを用いて暗号化する手順を述べる。まず、ＲＡＭディスク８５６よりＢＣＡ再生部８２０により、ＢＣＡのデータを再生し、ＩＤ８５７を出力し、インターフェース８５８ａ，８５８ｂとネットワークを介して、暗号化部８５９に送る。暗号化部８５９ではコンテンツ１８６０をＩＤ８５７を含む鍵で暗号エンコーダ１８６１において暗号化もしくは映像音声信号のスクランブルを行う。暗号化されたコンテンツは記録再生装置に送られ記録回路８６２によりＲＡＭディスク８５６に記録される。

【００４２】

次に、この信号を再生する時は、データ再生部８６５により、主データの復調を行い、暗号化された信号を再生し、暗号デコーダ１８６３において、復号が行なわれる。この時、ＲＡＭディスク８５６のＢＣＡ領域から、ＢＣＡ再生部８２０により、ＩＤ８５７を含む情報が再生され、暗号デコーダ１８６３に鍵の一部として送られる。この時、正規にコピーされた場合はＲＡＭディスクに記録された暗号の鍵は正規のデイスタＩＤであり、ＲＡＭディスクのＩＤも正規のディスクＩＤであるため、暗号の復号もしくはデスクランブルが行なわれ、前述の方法で記録された第ｎ番目のコンテンツの平文８６４が出力される。映像情報の場合はＭＰＥＧ信号が伸長されて、映像信号が得られる。

【００４３】

この場合、暗号化はディスクＩＤを鍵としている。ディスクＩＤは世の中に１枚しか存在しないため、１枚のＲＡＭディスクにしかコピーできないという効果が得られる。

【００４４】

ここで、もしこの正規のＲＡＭディスクから、別のＲＡＭディスクにコピーした場合、最

初の正規デイスクＩＤであるＩＤ１と、別の不正のＲＡＭディスクのディスクＩＤであるＩＤ２とは異なる。不正のＲＡＭディスクのＢＣＡを再生するとＩＤ２が再生される。しかし、コンテンツはＩＤ１で暗号化されているので、暗号デコーダ１８６３においてＩＤ２で解鍵しようとしても、鍵が異なるため、暗号は復号されない。こうして、不正コピーのＲＡＭディスクの信号が出力されず、著作権が保護されるという効果がある。本発明はＤｉｓｋ　ＩＤ方式なので正規に１回だけコピーされた正規のＲＡＭディスクはどのドライブで再生しても、暗号が解錠されるという効果がある。ただし、暗号化部８５９はセンターのかわりに暗号エンコーダを搭載したＩＣカードでもよい。

【００４５】

図１１のブロック図と図１２のフローチャートを用いて、コピー防止方法を述べる。ステップ８７７ａでインストールプログラムを動作させる。ステップ８７７ｂで貼り合わせた光ディスク８０１より、ＢＣＡ再生部８２０より副情報のＩＤが出力される。ステップ８７７ｄでデータ再生部８６５により主情報からコンテンツとネットワークチェックソフト８７０が再生される。コンテンツとＩＤ８５７はＨＤＤ８７２に記録される。ステップ８７７ｃで不正に改ざんされないようＩＤ８５７は特定の秘密の暗号演算を行い、ＨＤＤ８７２にソフトＩＤとして記録される。こうして、パソコン８７６のＨＤＤ８７２にはコンテンツとともにソフトＩＤ８７３が記録される。ここで図１２のステップ８７７ｉでプログラムを起動する場合を述べる。プログラムを起動する時は、ステップ８７７ｇにおいて、ＨＤＤ８７２のソフトＩＤ８７３を再生し、インターフェース８７５を介して、ネットワークの上の別のパソコン８７６ａのＨＤＤ８７２ａの中のソフトＩＤ８７３ａをチェックする。ステップ８７７ｈで他のパソコンのソフトＩＤ８７３ａと自分のソフトＩＤ８７３が同一番号であるかをチェックし、同一番号である場合は、ステップ８７７ｊへ進み、パソコン８７６のプログラムの起動を中止するか画面上に警告メッセージを表示する。

【００４６】

他のパソコンのソフトＩＤ８７３ａが同一番号でなかった場合は、少なくともネットワーク上にはコンテンツを複数台にインストールした形跡はないため不正コピーはないと判断し、ステップ８７７ｋへ進み、プログラムの起動を許可する。この場合、他のパソコンへネットワークを介してソフトＩＤ８７３を送信してもよい。このパソコンでは各パソコンのソフトＩＤの重複をチェックすれば不正インストールが検出できる。不正があれば、該当するパソコンに警告メッセージを送る。

【００４７】

こうして、ＢＣＡにＩＤを記録し、ネットワークチェックプログラムをピット記録領域に記録することにより、同一ネットワーク上の同一ＩＤのソフトの複数インストールを防止できる。こうして簡便な不正コピープロテクトが実現する。

【００４８】

図１３のように白色の材料からなる書き込み可能な書き込み層１８５０を塗布することにより設けることにより、文字を印刷したりペンでパスワード等を書き入れたりすることができるだけでなく、書き込み層１８５０が厚くなるため光ディスクの基板の損傷を防ぐという効果も得られる。この書き込み層１８５０の上のＢＣＡ領域８０１ａにトリミングで記録されたＢＣＡデータ１８４９の一部であるディスクＩＤ８１５を平文化し英数字に変換した文字１８５１と一般バーコード１８５２を印字することにより、販売店やユーザーがＢＣＡを再生装置でよみとることなく、ＰＯＳのバーコードリーダーや視認でＩＤの確認や照合ができる。視認できるＩＤはユーザーがパソコン経由でＩＤをセンターに通知する場合は不要である。しかしユーザーが電話でＩＤをセンターに口頭で伝える場合は、ＢＣＡのＩＤと同じＩＤがディスク上に視認できる形式で印刷することにより、ユーザーがＩＤを目でよみとれるのでパソコンにディスクを挿入することなしにＩＤをセンターに伝えることができる。図１３のフローチャートで光ディスクの製造ステップを説明する。ステップ１８５３ｄで、原盤よりディスクの成形を行い、ピットの記録された基板を作成する。ステップ１８５３ｅでアルミ反射膜を作成する。ステップ１８５３ｆで２枚のディスク基板を接着剤で貼り合わせ、ＤＶＤディスク等を完成させる。ステップ１８５３ｇでス

クリーン印刷のラベル印刷をディスクの片面に行う。この時バーコードで原盤に個有の識別情報を記録する。ステップ１８５３ｈでＰＯＳ用バーコードのフォーマットでディスク１枚ごとに異なるＩＤ等の識別情報をインクジェットバーコード印刷機や熱転写型バーコード印刷機で印刷する。ステップ１８５３ｉで、このバーコードをバーコードリーダーでよみ出し、ステップ１８５３ｊで識別情報に対応したＢＣＡデータをディスクの第２記録領域に記録する。この製造方法であると、ＢＣＡを除くＰＯＳバーコードを含む全工程を終えた後にディスク識別情報を確認した上で、ＢＣＡデータを記録する。ＢＣＡはディスクを再生しないと読めないが、ＰＯＳバーコードは密度が低いので市販のバーコードリーダーでよみとれる。工場の中のあらゆる工程で、ディスクＩＤが識別できる。ＢＣＡトリミングの前にＰＯＳバーコードでディスクＩＤを記録しておくことにより、ＢＣＡとＰＯＳバーコードの誤記録がほぼ完全に防止できる。

【００４９】

このＢＣＡ方式で二次、三次記録もできるＢＣＡの利用方法について述べる。図１５に示すようにソフト会社では、工程２で示すように海賊版防止コードと照合暗号を二次記録もできる。工程２ではディスク１枚ごとに異なるＩＤ番号やユーザーとの秘密通信用の暗号鍵を記録したディスク９４４ｂを作成しても良い。この方法によるセル販売店におけるディスク９４４ｃ、ユーザにおけるディスク９４４ｄはパスワードを入力しなくても再生できる。

【００５０】

別の応用として工程３では、暗号化やスクランブルしたＭＰＥＧ映像信号等の情報をディスク９４４ｅに記録する。ＭＰＥＧスクランブルの詳しい動作は説明を省略する。ソフト会社では工程４においてＩＤ番号とスクランブル解除情報を復号するためのサブ公開鍵をＢＣＡで二次記録したディスク９４４ｆを作成する。このディスクは単独では再生はできない。工程５では、販売店でディスクの代金を受け取った後にサブ公開鍵とペアになっているサブ秘密鍵でパスワードを作成し、ディスクに三次記録する。もしくはパスワードの印刷されたレシートをユーザーに渡す。このあと、ディスク９４４ｇはパスワードが記録されているためユーザーが再生可能となる。この方式を用いると、代金の支払われていないディスクを万引きしても映像のスクランブルが解除されないため正常に再生されないため、万引きが無意味になり減るという効果がある。

【００５１】

レンタルビデオ等の店では恒久的にパスワードをＢＣＡ記録すると万引きされた場合、使用されてしまう。この場合は工程５、６に示すように店でＢＣＡをＰＯＳバーコードリーダーでよみとりスクランブル解除のためのパスワードをステップ９５１ｇで発行し、ステップ９５１ｉでレシートに印刷し、ステップ９５１ｊで客に手渡す。客の方は、自宅においてステップ９５１ｋでレシートのパスワードをプレーヤにテンキーで入力する。ステップ９５１ｐで所定の日の間だけ再生される。ディスクの一部のソフトのパスワードのみを与えてレンタルした場合に、他のソフトをみたい時は、電話で、そのソフトのパスワードをステップ９５１ｕで通知しステップ９５１ｋで入力することにより、ディスクの他のソフトを再生することができる。レンタルビデオ店の例を示したがパソコンソフト店で、暗号化したパソコンソフトを売った時に、ＰＯＳ端末でパスワードを印刷して渡しても良い。

【００５２】

図１５の工程５、６のセル販売店、レンタル店における動作を図１４を用いてより具体的に説明する。セル販売店ではソフト会社から暗号やスクランブルがかかったディスク９４４ｆを受け取り、ユーザーからの入金を確認するとバーコード記録装置９４５よりディスク９４４ｆのＩＤ番号、サブ公開鍵のデータをＰＯＳ端末９４６経由でパスワード発行センターに送信する。小規模なシステムの場合パスワード発行センター、つまりサブ公開鍵のサブ秘密鍵を含むシステムはＰＯＳ端末の中にあっても良い。パスワード発行センターはステップ９５１ｑでディスクＩＤ番号とステップ９５１ｒで時間情報を入力し、ステップ９５１ｓで演算を行い、ステップ９５１ｔで、サブ秘密鍵を用いて暗号化し、ステップ

９５１ｇでパスワードを発行しネットワーク９４８とＰＯＳ端末９４６を介してバーコード記録装置９４５にパスワードを送り、記録されたディスク９４４ｇが客に渡される。このディスク９４４ｇは、そのまま再生できる。

【００５３】

次にレンタル店やパソコンソフト店の場合、まず暗号やスクランブルの解除されていないＲＯＭディスク９４４ｆを店頭に陳列する。客が特定のＲＯＭディスク９４４ｆを指定した場合、うずまき型にスキャンする回転型の光学ヘッド９５３を内蔵した円形バーコードリーダ９５０を手に持ち透明ケース入りのディスク９４４ｆの中心におしつけることにより、ディスク９４４ｆの無反射部による反射層のバーコードを読み取り、ディスクＩＤ番号を読み取る。ディスクＩＤの商品バーコードを図１３の１８５２のように印刷することにより通常のＰＯＳ端末のバーコードリーダーで読み取ることが出来る。原盤に予め記録されプレスされた円形バーコードから読み取っても良い。これらのディスクＩＤを含む情報はＰＯＳ端末９４６により処理され、料金がクレジットカードから決済されるとともに、前述のようにＩＤ番号に対応したパスワードがステップ９５１ｇにおいてパスワード発行センターから発行される。レンタル用途の場合、視聴可能な日数を制限するためステップ９５１ｒで用いたように時間情報を加えて、ディスクＩＤ番号を暗号化しパスワードを作成する。このパスワードの場合、特定の日付しか作動しないため、例えば３日間の貸し出し期間をパスワードの中に設定できるという効果がある。

【００５４】

さて、こうして発行されたデスクランブルのためのパスワードはステップ９５１ｉにおいて、貸出日、返却日、レンタルのタイトル料金とともにレシート９４９に印刷され客にディスクとともに渡される。客はディスク９４４ｊとレシート９４９を持ち帰り、ステップ９５１ｋでパスワードを図６の第１コンピュータ９０９のテンキー入力部９５４に入力することによりｎ番目のパスワード８３５はＩＤ８３５ａと演算されて暗号デコーダ８３７に入力され、復号鍵を用いて平文化される。正しいパスワードである場合のみ暗号デコーダ８３７でプログラムのデータをデスクランブルし、映像出力を出力させる。

【００５５】

この場合、パスワードに時間情報が含まれている場合、時計部８３６ｂの日付データと照合し、一致した日付の期間、デスクランブルをする。なお、この入力したパスワードは対応するＩＤ番号とともにメモリ７５５の不揮発メモリ７５５ａにストアされ、ユーザーは一度パスワードを入力すると２度と入力することなしにデスクランブルされる。こうして流通において電子的にディスクの鍵の開閉ができるという効果がある。

【００５６】

図１６を用いてソフトが暗号データとして記録されたディスクのソフトの復号方法を詳しく説明する。

【００５７】

ステップ８６５は暗号データと個別ＩＤのユーザーへの配布の全体フローを示す。まず、ステップ８６５ａでは、１枚の原盤のＲＯＭ領域に、秘密の第１暗号鍵で暗号化されたｍヶのデータと、暗号化されたｍヶのデータを復号するプログラムを記録する。ステップ８６５ｂでは、原盤より基板を成形し、反射膜を付加した２枚の基板を貼り合わせて完成ＲＯＭディスクを複数枚、作成する。ステップ８６５ｃでは、完成ディスクの書換できない副記録領域（ＢＣＡとよぶ）に、暗号化データの復号に必要な復号情報（プレスしたディスク毎に異なるディスク識別情報　ａｎｄ／ｏｒ　暗号データの復号鍵）をＲＯＭ領域と異なる変調方法で記録する。ステップ８６５ｄでは、ユーザーは配布されたディスクを再生し、希望する暗号化データｎを選択し、復号処理を始める。ステップ８６５ｅで、ユーザーの第１コンピュータで、ＲＯＭ領域から暗号化データと復号プログラムを再生し、副記録領域（ＢＣＡ）から、復号情報を読み出す。ステップ８６５ｆで、オンラインで第２復号情報を得ない場合は第１７図のステップ８７１ａで、ＩＤ等の復号の補助情報を画面上に表示する。ステップ８７１ｂで、ユーザーはＩＤに対応するパスワード等の第２復号情報を入手し、第１コンピュータに入力する。ステップ８７１ｃで、ディスク識別情報と

第２復号情報と暗号化データｎを用いて公開鍵系暗号関数の特定の演算を行う。ステップ８７１ｄで結果が正しければ、ステップ８７１ｆでｎ番目のデータが平文化され、ユーザーはデータｎのソフトを動作させることができる。

【００５８】

次に図１８のフローチャートを用いて、ＢＣＡを用いたインターネット等で必須な暗号通信の方法を述べる。ステップ８６８は、ユーザーへ通信プログラムと通信暗号鍵を配布する方法のルーチンである。まず、ステップ８６８ａで、１枚の原盤のＲＯＭ領域に少なくとも通信プログラムや接続情報を記録する。ステップ８６８ｂで、原盤より基板を成形し、２枚の基板を貼り合わせて完成ＲＯＭディスクを複数枚作成する。ステップ８６８ｃで、完成ディスクの書換できない副記録領域（ＢＣＡ）に、プレスしたディスク毎に異なるディスク識別情報と暗号通信用暗号鍵を記録する。場合により第２コンピュータの接続アドレス、もしくは暗号通信用復号鍵をＲＯＭ領域と異なる変調方法で記録する。ステップ８６８ｄで、ユーザーの第１コンピュータで、ＲＯＭ領域から通信プログラムと暗号化プログラムを再生し、副記録領域から、ディスク識別情報と通信用暗号鍵を読み出す。図１９に進みステップ８６７ａで、ＢＣＡ領域に接続アドレスがある場合は、ステップ８６７ｂで、ＢＣＡ領域のＵＲＬ等の接続アドレスに基づき第２コンピュータに接続し、接続アドレスがない場合はステップ８６７ｃのＲＯＭ領域の接続アドレスのコンピュータに接続する。ステップ８６７ｄで、送信データが入力され、ステップ８６７ｅで、ＢＣＡ領域に暗号通信用暗号鍵がある場合はステップ８６７ｇでＢＣＡ領域の暗号通信用暗号鍵を用いて、送信データを暗号化し、第３暗号を作成する。また、ない場合はステップ８６７ｆでＲＯＭ領域又はＨＤＤの暗号通信用の暗号鍵を用いてデータを暗号化し、第３暗号を作成する。

【００５９】

次に図２０では第２コンピュータ８２１ａから受信した暗号の復号鍵の生成ルーチンをステップ８６９で述べる。まず、第１コンピュータではステップ８６９ａで、通信復号鍵が必要な場合は、ステップ８６９ｂへ進み、ＢＣＡに通信用復号鍵があるかどうかをチェックし、復号鍵がない場合は、ステップ８６９ｃでＲＯＭ領域から再生した暗号鍵／復号鍵の生成プログラムを用いてユーザーのキー入力もしくは乱数発生器のデータをＲＯＭ領域から再生した第２暗号鍵により一対の第２通信暗号鍵／第２通信復号鍵を新たに生成する。ステップ８６９ｄで、“第２通信暗号鍵もしくはユーザーデータ”をＢＣＡに記録された通信暗号鍵とＲＯＭ領域から再生して得た暗号化ソフトを用いて暗号化した第４暗号を作成する。ステップ８６９ｅで、第４暗号と、ディスク識別情報もしくはユーザーアドレスを、ディスクから再生して得た接続アドレスの第２コンピュータに送信する。第２コンピュータの処理としては、ステップ８６９ｆで、第４暗号とディスク識別情報とユーザーアドレスを受信する。ステップ８６９ｇでは、復号鍵データベースから、ディスク識別情報と対になった通信復号鍵を選択し、これを用いて第４暗号を復号し、第２通信暗号鍵の平文を得る。ステップ８６９ｈで、第２通信暗号鍵を用いて、ユーザーデータの一部を含むサーバーのデータを暗号化した第５暗号を第１コンピュータへインターネット９０８で送信する。ステップ８６９ｉで、第５暗号（とディスク識別情報）を受信し前述の第２通信復号鍵とＲＯＭ領域に記録された復号関数を用いて復号し、前述のサーバーデータの平文を得る。こうして、図２０のステップ８６９の方式で、第１、第２コンピュータ間で双方向の暗号通信が実現する。

【００６０】

図２１のステップ８７０では課金情報の受信ルーチンについて説明する。ステップ８７０ａで、課金情報を入力する場合は、課金通信用の公開鍵暗号の第３暗号鍵を第２コンピュータへ要求する。ステップ８７０ｂでは、第２コンピュータが、第３コンピュータへ第３暗号鍵を要求する。やりとりのステップは省略するが、第３コンピュータ８２８はＩＤと第３暗号鍵を第２コンピュータ８２１ａへ送信する。ステップ８７０ｃで、第２コンピュータはＩＤと第３暗号鍵を受信し、ステップ８７０ｅで、第３暗号鍵を第２通信暗号鍵等を用いて暗号化した第７暗号を第１コンピュータへ送信する。第１コンピュータではステ

ップ８７０ｆで、第７暗号を受信し、ステップ８７０ｇで、前述の第２通信復号鍵を用いて、受信した第７暗号を復号し、第３暗号鍵（公開鍵関数の公開鍵）を得る。ステップ８７０ｈでは、必要に応じて第３暗号鍵をＨＤＤに記録する。これは次回の送信時に利用する。ステップ８７０ｉで、クレジットカード番号や決済用パスワード等の機密値が高い課金情報を入力する場合は、ステップ８７０ｊで第３暗号鍵を用いて、上記課金情報を暗号化した第８暗号を第２コンピュータ経由で第３コンピュータへ送る。第２コンピュータは、ステップ８７０ｋで第８暗号を受信し、第３コンピュータへ再転送する。第３暗号の復号鍵は金融機関である第３コンピュータ８２８しか持っていないため、第２コンピュータの電子商店では解読できない。第３コンピュータではステップ８７０ｍで、暗号鍵データベースからディスク等の識別情報を用いて第３暗号鍵に対応した第３復号鍵を探しだし、公開鍵暗号の秘密鍵である第３復号鍵で第８暗号を復号し、課金情報の平文を得る。ステップ８７０ｎでは、ユーザーの信用情報や預金残高等の金融情報から、代金が回収できるかをチェックし、ステップ８７０ｐでは、調査結果を第２コンピュータへ通知する。第２コンピュータいわゆる電子商店はステップ８７０ｑで代金の回収可能かどうかを判定して、不能と判断すれば、ステップ８７０ｒで、商品の発送や暗号データを復号する鍵の送付をしない。代金回収可能と判断した場合、図１６のような鍵提供システムの場合、ステップ８７０ｓへ進み、暗号データの復号鍵つまり商品をインターネット９０８で、ユーザーの第１コンピュータに送信する。第１コンピュータでは、ステップ８７０ｔで、暗号データの復号情報を受信して、ステップ８７０ｕでｎ番目の暗号化データの暗号を解除して、ステップ８７０ｗで、データの平文を得る。こうして、コンテンツの鍵提供システムが実現する。

【００６１】

この図２１のステップ８７０の方式は課金情報という高いセキュリティが要求される第３暗号鍵の公開鍵を第３コンピュータつまり、金融機関に、必要に応じて要求し発行させる。ＢＣＡに予め記録しておかなくてもよい。従って第３暗号鍵にＲＳＡ２０４８の２５６バイトのさらに強力なＲＳＡ系の暗号鍵をＢＣＡの容量を消費することなしに用いることができるという効果がある。さらに全てのディスクのＢＣＡに予め記録する必要がないので、第３暗号鍵の発行総数が少なくなり、第３暗号鍵の演算に要するコンピュータのＣＰＵタイムが減る。また、第３暗号がＢＣＡにないため、公開されないため、セキュリティが若干向上する。この場合のＢＣＡの役割は、図１９、２０のように、ＲＳＡ１０２４グレードの暗号鍵による秘密通信ディスクの識別情報の記録である。ＢＣＡディスク１枚あれば、第２コンピュータとの暗号通信が実現するため効果は高い。

【００６２】

次に図２２を用いて、図１０で説明したＢＣＡを用いたＲＡＭディスク記録再生装置に関して更に詳しく述べる。１つの実施例としていわゆるＰａｙ　ｐｅｒ　Ｖｉｅｗシステムにおけるディスクへの記録手順を述べる。まず、ＣＡＴＶ会社等のソフト会社は番組送信器８８３において、映画ソフト等のコンテンツ８８０を第１暗号鍵８８２を用いて第１暗号器において暗号化し、第１暗号９００を生成し、各ユーザーのＣＡＴＶデコーダの如きデコーダ８８６に送信する。デコーダ８８６側ではネットワークを介して鍵発行センター８８４へ特定の番組の要求を送ると、鍵発行センター８８４は、特定のソフトでかつ特定のデコーダのシステムＩＤ８８８かつ特定の時間制限情報９０３に対するスクランブル解除キーの如き第１復号情報でかつ、ＲＡＭディスクへの記録許可コード９０１が含まれている第１復号情報８８５ａをデコーダ８８６の第１復号部８８７へ送信する。第１復号部８８７はシステムＩＤ８８８と第１復号情報８８５ａより、第１暗号９００を復号し、映像信号の場合は、一旦デスクランブルされた信号がさらに別の暗号でコピー防止用のスクランブルされた信号が第３暗号出力部８８９から出力され、一般ＴＶ８９９で、元のＴＶ信号がコピーガードされているが視聴できる。ここで、記録許可コード９０１がＮＯの場合は、ＲＡＭディスク８９４に記録できない。しかし、ＯＫの場合はＲＡＭディスク８９４の１枚に限り記録できる。この方法を説明する。

【００６３】

デコーダ８８６では、ＩＣカード９０２ａが挿入され、ＲＡＭ記録装置のＲＡＭディスク８９４のＢＣＡをＢＣＡ再生部８９５が読み取りディスクＩＤ９０５がＩＣカード９０２ａに送られる。ＩＣカード９０２ａはディスクＩＤ９０５とデコーダ８８６の時間情報管理部９０４から得た現在の時間情報と記録許可コードａをチェックし、第３暗号出力部８８９と双方向でシェイクハンド方式のコピーチェック９０７を行い、記録許可コードとコピーチェックがＯＫならＩＣカード９０２ａの中の第２副暗号器８９１は第２暗号鍵９０６を発行する。第２暗号演算器８９０において、第３暗号は再暗号化されて特定の１枚のディスクのディスクＩＤでコンテンツ８８０が暗号化された第２暗号９１２が生成され、ＲＡＭ記録装置８９２に送られ記録手段８９３において８－１５変調や８－１６変調を用い、第１変調部により変調され、レーザーにより、ＲＡＭディスク８９４の第１記録領域８９４ａに第２暗号９１２が記録される。こうしてＲＡＭディスク８９４のデータは特定のディスクＩＤの番号で暗号化される。

【００６４】

次にこのディスクを通常の再生手段８９６で再生信号を８－１６変調の第１復調部８９６ａで復調するとコンテンツの第２暗号が出力される。第２復号器８９７は複数の第２復号鍵８９８ａ、８９８ｂ、８９８ｃをもつ。これは各ＣＡＴＶ局等の番組供給会社毎に異なる各々のＩＣカードの暗号鍵に対応した復号鍵をもつことになる。この場合、デコーダ８８６もしくはＩＣカード９０２ａの復号鍵識別情報は記録時に第１記録領域８９４ａに記録されている。再生装置では、第１記録領域８９４ａから復号鍵識別情報９１３をよみ出し、復号鍵選別手段９１４により復号鍵８９８ａ～８９８ｚを元に各々の暗号鍵に対応した、第２復号鍵８９８ａを自動的に選択し、ディスクＩＤ９０５を一つの鍵として、第２暗号は第２復号器８９７において復号される。特定の復号鍵の入ったＩＣカードを用いてもよい。映像の場合ＴＶ８９９ａにてデスクランブルされた正常な映像が得られる。

【００６５】

図２２のシステムでは、各ユーザーの自宅のデコーダに挿入したＩＣカードにディスクＩＤ９０５を送り、画像データ等を暗号化するので、ソフト会社８８３は各ユーザーに配信するコンテンツの暗号を個別に変える必要がない。従って、衛星放送やＣＡＴＶのように大量の視聴者にペイパービューのスクランブル映像を放送する場合に、ユーザー毎にＲＡＭディスク１枚だけに記録することを許可することができるという効果がある。

【００６６】

図２２のシステムで１枚のディスクに記録すると同時に、２枚目つまり他のディスクＩＤのＲＡＭディスクに不正にコピーつまり記録しようとするとＢＣＡの場合２層ディスクを用いているのでディスクＩＤを改ざんすることができないため、同時間に２枚目のディスクへの不正コピーは防止される。次に別の時間帯に擬似的な記録許可コード９０１や第３暗号をデコーダやＩＣカードに送信し、特定のディスクＩＤでデータが暗号化されているものを、別のディスクＩＤのＲＡＭディスクに記録することが考えられる。こうした不正行為にも、ＩＣカードの中の時間情報管理部９０４が鍵発行センター８８４の時間制限情報９０３やコンテンツの時間情報の時間とデコーダの中の時間情報部９０４ａの現在の時間とを比較して、時間が一致しているかどうかをチェックし、ＯＫならＩＣカード９０２ａは第２暗号演算器８９０の暗号化を許可する。

【００６７】

この場合、第２暗号演算器８９０と第１復号部８８７が双方向でチェックデータを交信するシェイクハンド方式の時間チェック方式でもよい。

【００６８】

シェイクハンド方式の場合、ＩＣカードを含む第２暗号演算器８９０と、第１復号部８８７と第３暗号出力部８８９は双方向で、暗号データを確認しあう。このためコンテンツの送信時間と同一でない別の時間帯の不正コピーは防止される。

【００６９】

こうして各ユーザーのもつデコーダ８８６においては世の中に１枚しか存在しない特定のディスクＩＤのＲＡＭディスク８９４の１枚のみに、ソフト会社のコンテンツが記録され

る。そして、このディスクはどのＲＡＭディスク再生機でも再生できる。図２２の方式でＲＡＭディスクに記録する場合でもソフト会社の著作権が守られるという効果がある。

【００７０】

なお本文の図の説明では、暗号エンコーダで暗号化、暗号デコーダで復号化を説明したが、実際はＣＰＵの中のプログラムである暗号アルゴリズム及び復号アルゴリズムを用いる。

【００７１】

【発明の効果】

このように、光ディスクのＢＣＡ領域にＩＤや暗号の暗号鍵や復号鍵を予め記録しておくことにより、暗号化されたコンテンツの暗号解除がより簡単な手順で実現する。また通信の機密性が従来の登録手続きなしで実現する。ネットワークチェックプログラムをコンテンツに収納しておくことにより、同一ネットワーク上の同一ＩＤソフトの複数インストールを防止できる。このようにセキュリティ向上の様々な効果がある。

【図面の簡単な説明】

【図１】本発明の実施例の光ディスクの製造工程図

【図２】本発明の実施例のパルスレーザーによるトリミングの断面図

【図３】本発明の実施例のトリミング部の信号再生波形図

【図４】本発明の実施例の再生装置のブロック図

【図５】（ａ）本発明のＢＣＡ部の再生信号波形図

（ｂ）本発明のＢＣＡ部の寸法関係図

【図６】本発明の実施例の暗号通信の方法とパスワードによる暗号解鍵の方法を示した図

【図７】本発明のＢＣＡのフォーマット図

【図８】本発明の実施例の暗号通信の方法とパスワードによる暗号解鍵の方法を示した図

【図９】本発明の実施例のコンテンツ部分を使用許可したディスクの動作手順図

【図１０】本発明の実施例のＲＡＭディスクにＢＣＡを記録した場合のブロック図

【図１１】本発明の実施例の不正コピー防止方式のブロック図

【図１２】本発明の実施例の不正コピー防止のフローチャート

【図１３】本発明の実施例のＢＣＡに商品バーコードを印刷した光ディスクの上面図と断面図

【図１４】本発明の実施例のＢＣＡ付ＲＯＭディスクとＰＯＳ端末を用いたＰＯＳ決済システムのブロック図

【図１５】本発明の実施例のプレス工場とソフト会社と販売店の暗号解除の流れ図

【図１６】本発明の実施例のディスクＩＤ等を用いた暗号データの暗号化復号化ステップのフローチャート

【図１７】本発明の実施例のディスクＩＤ等を用いた暗号データの暗号化復号化ステップのフローチャート

【図１８】本発明の実施例のＢＣＡを用いた通信暗号鍵の配布と暗号通信のフローチャート

【図１９】本発明の実施例のＢＣＡを用いた通信暗号鍵の配布と暗号通信のフローチャート

【図２０】本発明の実施例のＢＣＡを用いた通信暗号鍵の配布と暗号通信のフローチャート

【図２１】本発明の実施例のＢＣＡを用いた電子決済システムのフローチャート

【図２２】本発明の実施例のＢＣＡを用いた１枚のＲＡＭディスクに記録制限する記録再生方法のブロック図

【符号の説明】

８０１　ＢＣＡ付デイスク

８０２　第１暗号鍵

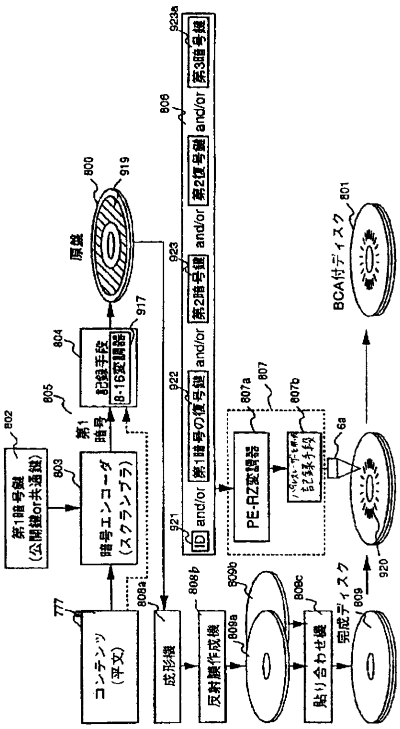
８０３　暗号エンコーダ

８０４　記録手段

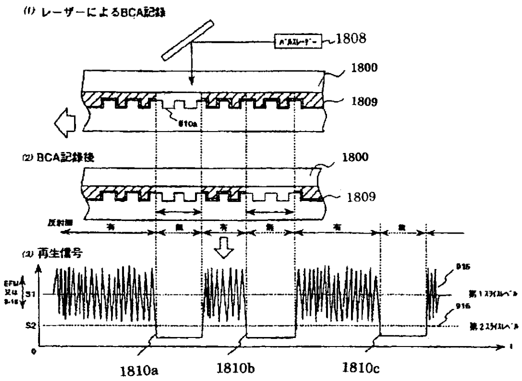
８０７　トリミング装置
８０８ａ　成形機
８０８ｂ　反射膜作成機
８０８ｃ　貼り合わせ機
８０９　完成ディスク
８０９ａ　片面デイスク
８０９ｂ　片面デイスク
８１０ａ　低反射部
８１１　プレス工場
８１６　第１暗号鍵
８１７　第２暗号鍵
８１８　接続アドレス
８１９　再生装置
８２０　ＢＣＡ再生部
８２１　パスワード発行センター
８２２　通信部
８２３　ネットワーク
８２４　暗号鍵ＤＢ
８２５　第１復号鍵
８２６　コンテンツ番号
８２７　第１暗号エンコーダ
８２７ａ　第１暗号デコーダ
８２７ｂ　第１層・第２層切換部
８２７ｃ　第２暗号エンコーダ
８２８　第３コンピュータ（課金センター）
８２９　第２暗号鍵（秘密鍵）
８３０　課金情報
８３１　第２暗号エンコーダ
８３２　第２暗号デコーダ
８３３　第１時間情報
８３４　パスワード生成部
８３５　ｎ番目のパスワード
８３７　暗号デコーダ
８３８　共通鍵Ｋ
８３８ａ　平文化共通鍵Ｋ
８３８ｂ　第２平文化共通鍵Ｋ
８３９　第３暗号鍵
８３９ｂ　第３復号鍵
８４０　第３暗号エンコーダ
８４１　第３暗号デコーダ
８４２　第１暗号エンコーダ
８４３　主暗号デコーダ
８４４　主復号鍵
８４５ａ　第２暗号デコーダ
８４７　第２暗号デコーダ
８５１　１～ｍ番目の暗号鍵
８５３　暗号化された第１～ｍ番目のコンテンツ
８６０　第２暗号エンコーダ
８６１　第２暗号デコーダ
８６２　記録回路

８６３　ＨＤＤ
８６４　第ｎ番目のコンテンツの平文
８６５　データ再生部
８９０　第２暗号演算器
８９４ａ　第１記録領域
９１５　第１スライスレベル
９１６　第２スライスレベル
９１９　第１記録領域
９２０　第２記録領域
９２３　ＣＰＵ
９２５　ＥＦＭ復調部
９２６　８－１５変調　復調部
９２７　８－１６変調　復調部
９２８　第１復調部
９３０　第２復調部
１８００　２層ディスク
１８０９　アルミ反射膜
１８３８ａ　暗号鍵生成部
１８３８ｂ　ｎ番目のコンテンツの平文
１８４９　ＢＣＡデータ
１８５０　書き込み層ＢＣＡ
１８５１　文字
１８５２　一般バーコード
１８６０　コンテンツ
１８６１　暗号エンコーダ
１８６３　暗号デコーダ

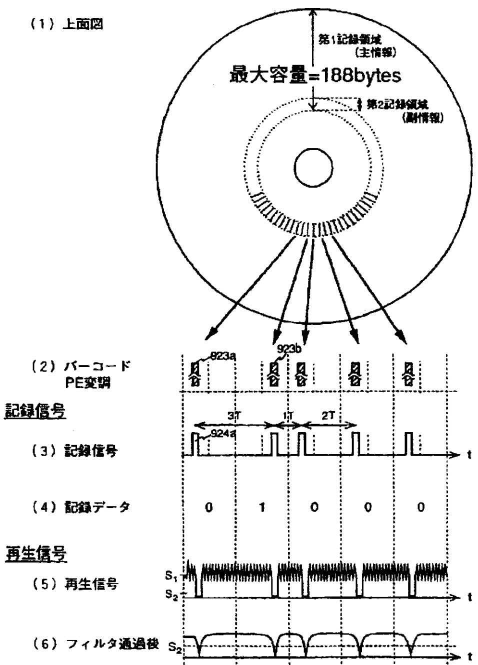
【図１】



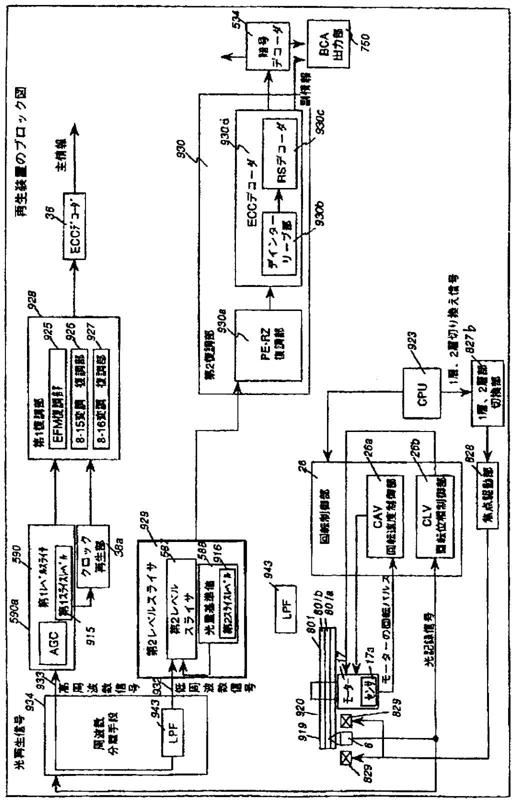
【図２】


(1) レーザーによるBCA記録
1808
1800
1809
(2) BCA記録後
1800
1809
(3) 再生信号
1810a
1810b
1810c

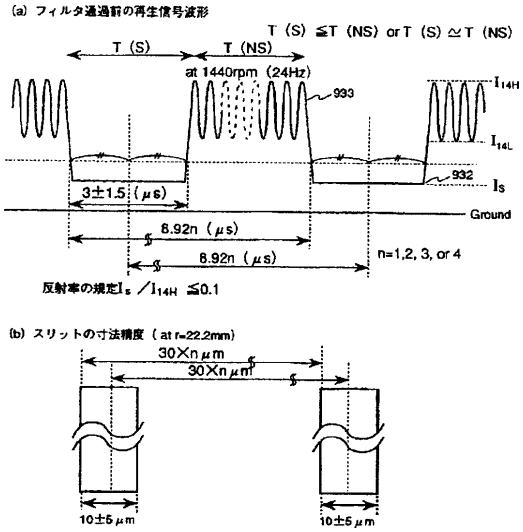
【図３】


(1) 上面図
第1記録領域
(主情報)
最大容量=188bytes
第2記録領域
(副情報)
(2) バーコード
PE変調
記録信号
(3) 記録信号
(4) 記録データ
再生信号
(5) 再生信号
(6) フィルタ通過後
(7) 再生データ

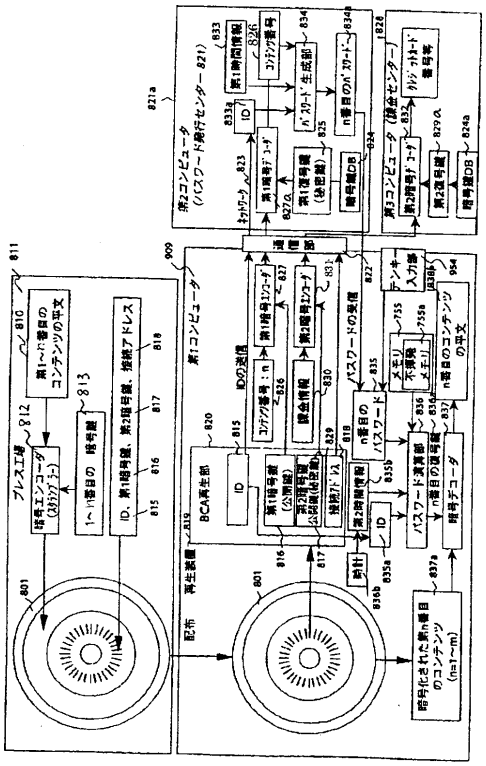
【図４】



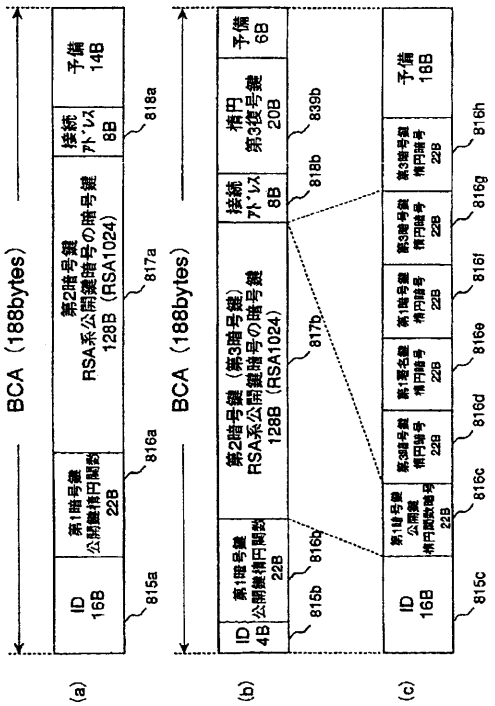
【図５】


(a) フィルタ通過前の再生信号波形
T (S) ≦T (NS) or T (S) ≒T (NS)
T (S)
T (NS)
at 1440rpm (24Hz)
933
932
I14H
I14L
Is
3±1.5 (μs)
8.92n (μs)
8.92n (μs)
n=1,2, 3, or 4
Ground
反射率の規定Is /I14H ≦0.1
(b) スリットの寸法精度 (at r=22.2mm)
30×n μm
30×n μm
10±5 μm
10±5 μm

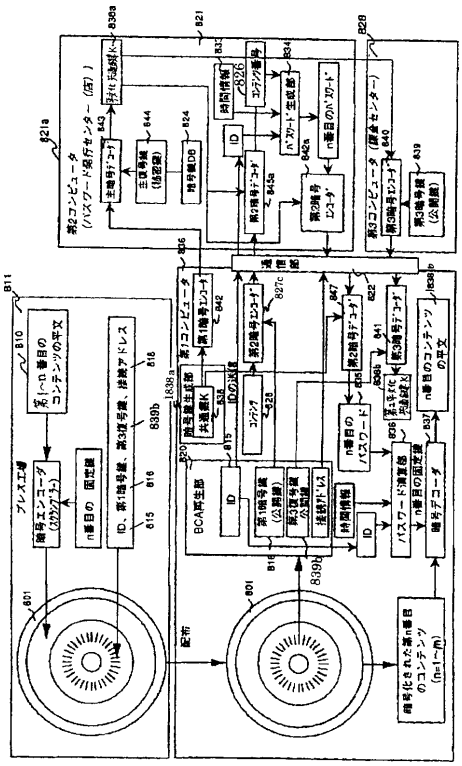
【図６】



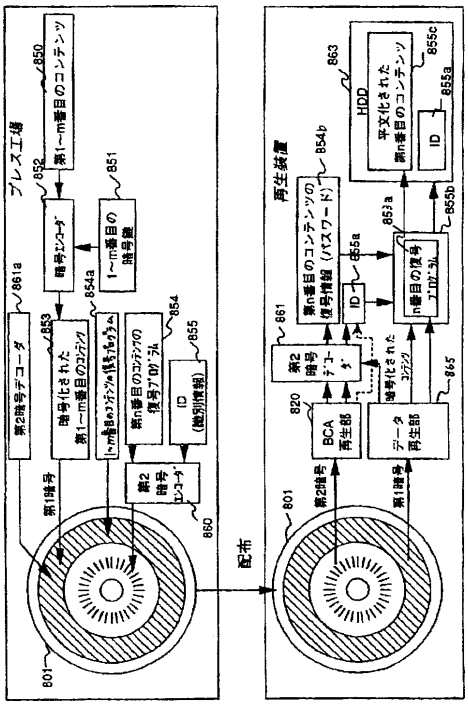
【図７】


BCA (188bytes)
ID 16B
第1暗号鍵 公開鍵楕円関数 22B
第2暗号鍵 RSA系公開鍵暗号の暗号鍵 128B (RSA1024)
接続 アドレス 8B
予備 14B
(a)
BCA (188bytes)
ID 4B
第1暗号鍵 公開鍵楕円関数 22B
第2暗号鍵 (第3暗号鍵) RSA系公開鍵暗号の暗号鍵 128B (RSA1024)
接続 アドレス 8B
楕円 第3復号鍵 20B
予備 6B
(b)
ID 16B
第1暗号鍵 公開鍵 楕円関数暗号 22B
第3暗号鍵 楕円暗号 22B
第1暗号鍵 楕円暗号 22B
第1署名鍵 楕円暗号 22B
第3暗号鍵 楕円暗号 22B
第3暗号鍵 楕円暗号 22B
予備 18B
(c)
815a
816a
817a
818a
815b
816b
817b
818b
839b
815c
816c
816d
816e
816f
816g
816h

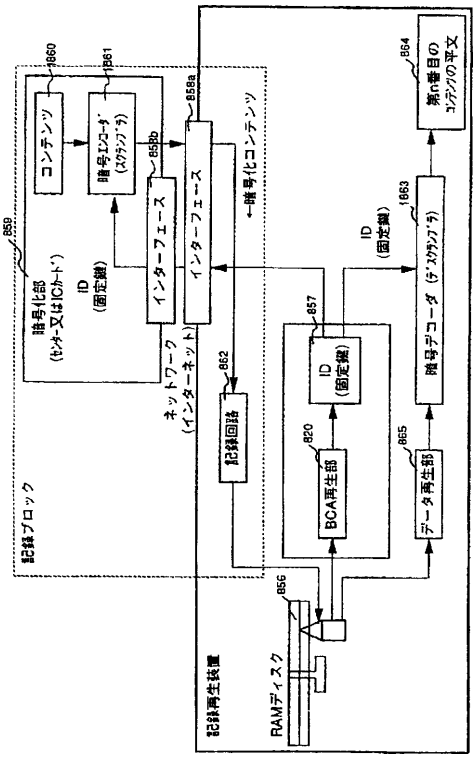
【図８】



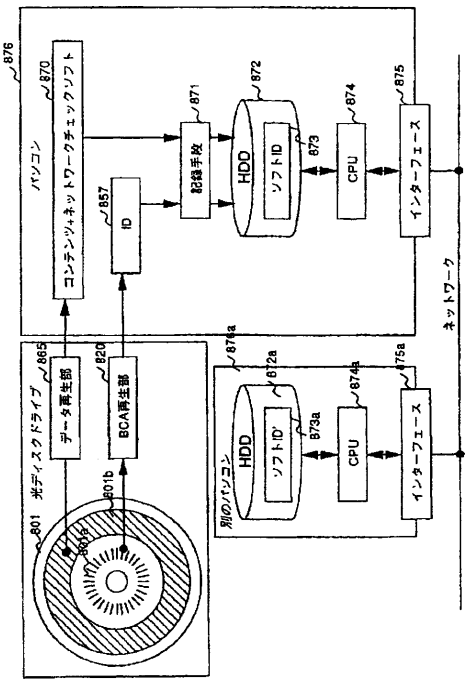
【図９】



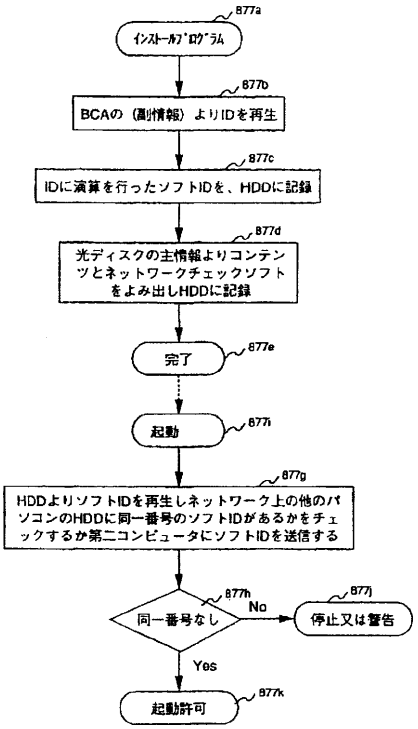
【図１０】



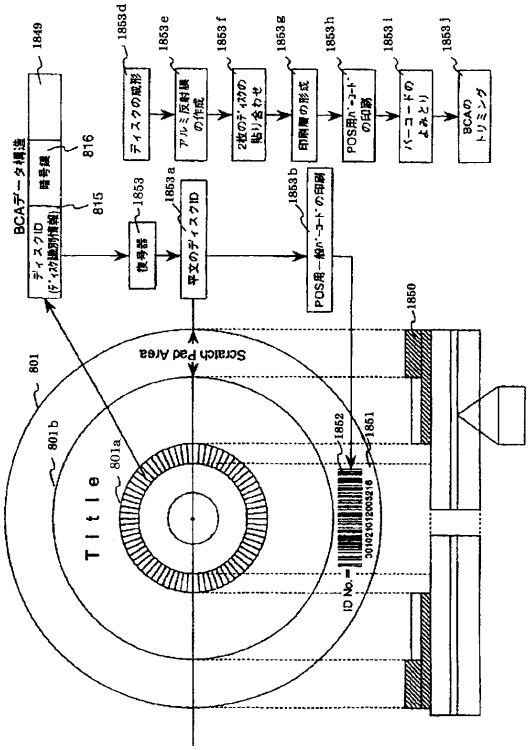
【図１１】



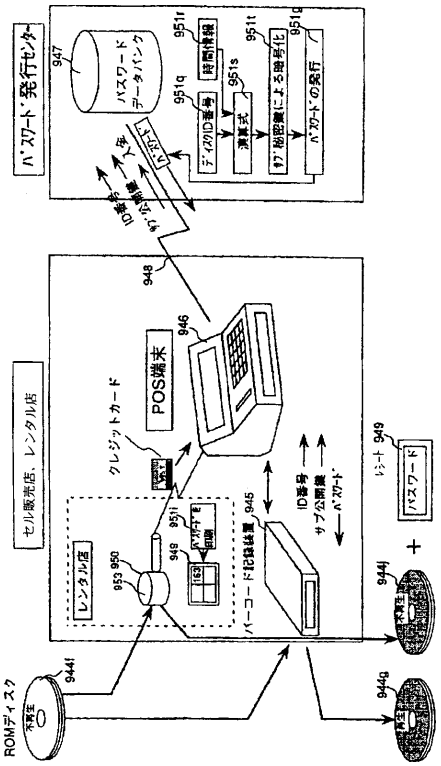
【図１２】



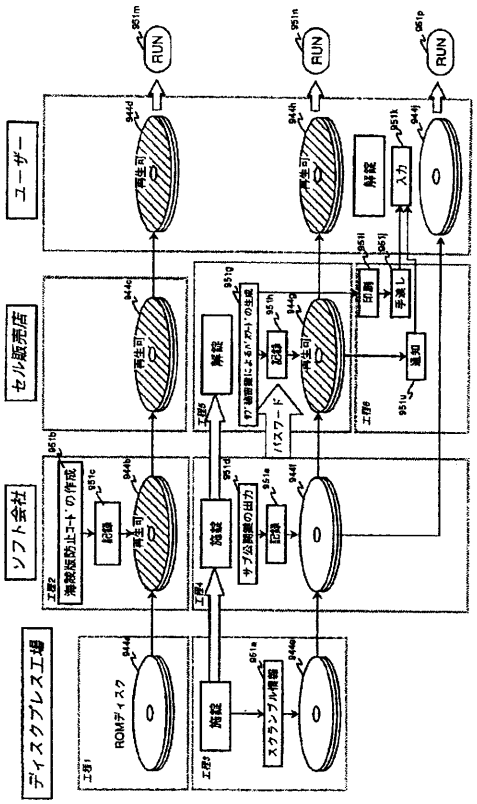
【図１３】



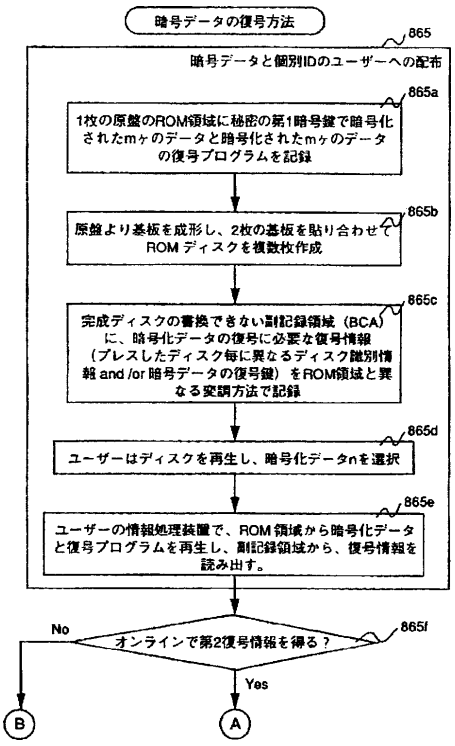
【図１４】



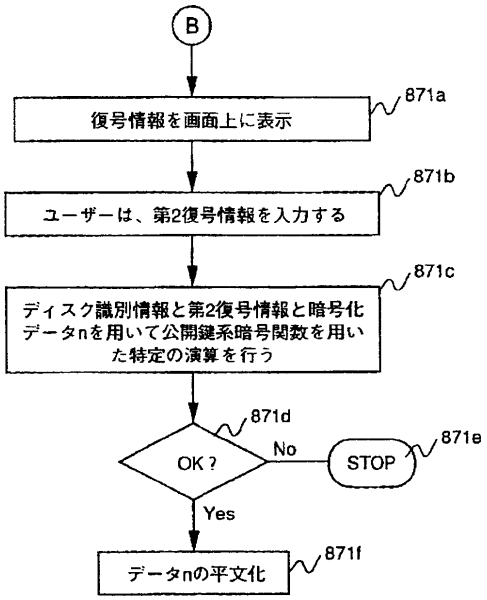
【図１５】



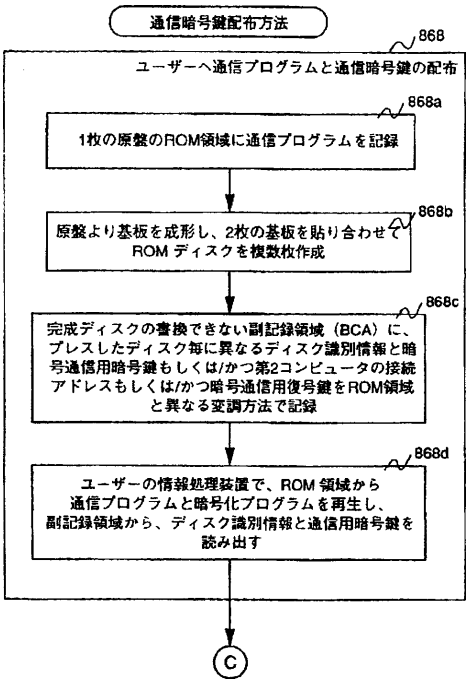
【図１６】



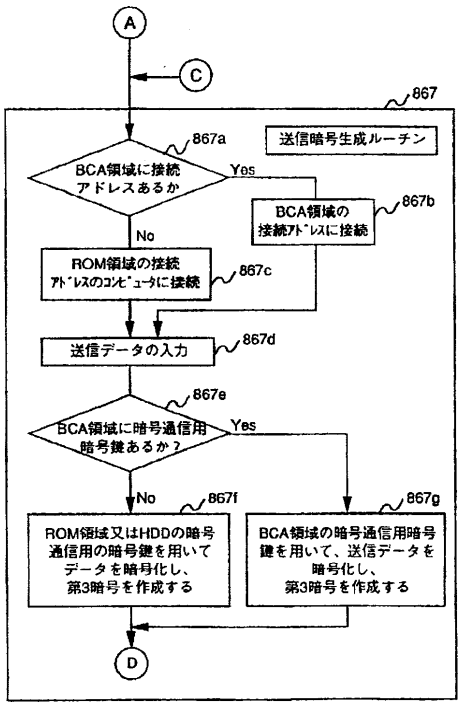
【図１７】



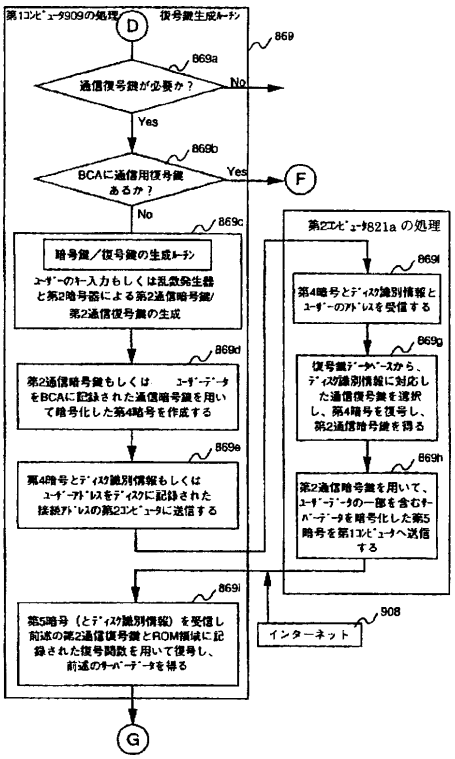
【図１８】



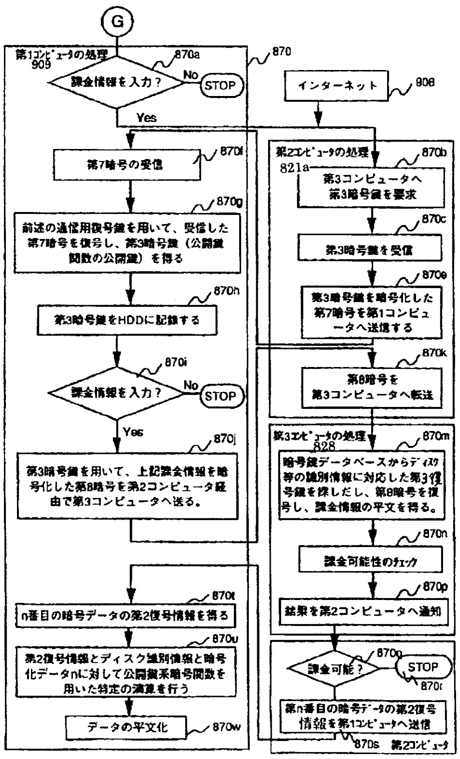
【図１９】



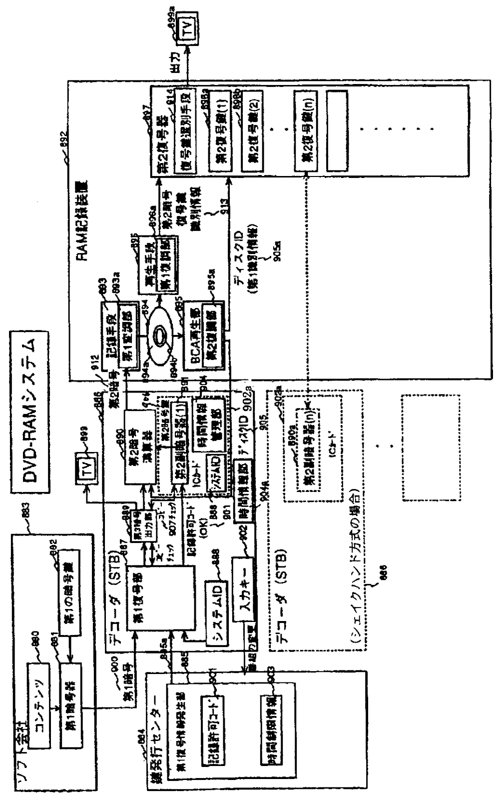
【図２０】



【図２１】


第1コンピュータの処理
課金情報を入力？
STOP
第7暗号の受信
前述の通信用復号鍵を用いて、受信した第7暗号を復号し、第3暗号鍵（公開鍵関数の公開鍵）を得る
第3暗号鍵をHDDに記録する
課金情報を入力？
第3暗号鍵を用いて、上記課金情報を暗号化した第8暗号を第2コンピュータ経由で第3コンピュータへ送る。
n番目の暗号データの第2復号情報を得る
第2復号情報とディスク識別情報と暗号化データnに対して公開鍵系暗号関数を用いた特定の演算を行う
データの平文化
インターネット
第2コンピュータの処理
第3コンピュータへ第3暗号鍵を要求
第3暗号鍵を受信
第3暗号鍵を暗号化した第7暗号を第1コンピュータへ送信する
第8暗号を第3コンピュータへ転送
第3コンピュータの処理
暗号鍵データベースからディスク等の識別情報に対応した第3復号鍵を探しだし、第8暗号を復号し、課金情報の平文を得る。
課金可能性のチェック
結果を第2コンピュータへ通知
課金可能？
第n番目の暗号データの第2復号情報を第1コンピュータへ送信
第2コンピュータ

【図２２】


DVD-RAMシステム
RAM記録装置
ソフト会社
コンテンツ
鍵発行センター
デコーダ（STB）
第1復号部
システムID
TV

フロントページの続き

(72)発明者　田中　伸一
京都府綴喜郡田辺町山手東１－４２－１４
(72)発明者　小石　健二
兵庫県三田市けやき台３－５６－８
(72)発明者　守屋　充郎
奈良県生駒市ひかりが丘３丁目１番２９号
(72)発明者　竹村　佳也
大阪府摂津市別府２－８－１１

審査官　石丸　昌平

(56)参考文献　特開平０７－２４９２２７（ＪＰ，Ａ）
特開平０５－２５７８１６（ＪＰ，Ａ）
特開昭５８－０８３３３６（ＪＰ，Ａ）
特開平０２－０５６７５０（ＪＰ，Ａ）
特開平０５－３２５１９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G11B 7/007
G11B 20/10