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

特許第5457280号
(P5457280)

(45)発行日　平成26年4月2日(2014.4.2)　(24)登録日　平成26年1月17日(2014.1.17)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04L 9/16 | (2006.01) | H04L | 9/00 | 643 |
| G06F 21/62 | (2013.01) | G06F | 21/24 | 166E |
| G09C 1/00 | (2006.01) | G09C | 1/00 | 660D |
| G06F 21/10 | (2013.01) | G06F | 21/22 | 110F |
| H04N 7/167 | (2011.01) | G06F | 21/24 | 163J |

請求項の数 10　(全 22 頁)　最終頁に続く

(21)出願番号　特願2010-134832 (P2010-134832)
(22)出願日　平成22年6月14日 (2010.6.14)
(62)分割の表示　特願2000-584672 (P2000-584672)の分割
原出願日　平成11年11月3日 (1999.11.3)
(65)公開番号　特開2010-257475 (P2010-257475A)
(43)公開日　平成22年11月11日 (2010.11.11)
審査請求日　平成22年6月15日 (2010.6.15)
(31)優先権主張番号　60/110,017
(32)優先日　平成10年11月25日 (1998.11.25)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　09/410,681
(32)優先日　平成11年10月1日 (1999.10.1)
(33)優先権主張国　米国 (US)

前置審査

(73)特許権者　593181638
ソニー　エレクトロニクス　インク
アメリカ合衆国　ニュージャージー州　07656　パークリッジ　ソニー　ドライブ　1
(74)代理人　100092093
弁理士　辻居　幸一
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100109070
弁理士　須田　洋之
(74)代理人　100109335
弁理士　上杉　浩

最終頁に続く

(54)【発明の名称】記録されたデジタルプログラムにアクセスするための方法及び装置

(57)【特許請求の範囲】

【請求項１】

権利履歴を監視する権利履歴監視方法において、

条件付きアクセス装置に対し、スクランブルされたデータをデスクランブルするための少なくとも１つの権利であって、所定の期間において、当該データをデスクランブルしたコンテンツ又はサービスを視聴するための権利を与えるステップと、

上記条件付きアクセス装置内の権利管理メッセージにおける権利履歴フィールドに上記与えられた権利を記録し、上記スクランブルされたデータを鍵を用いてデスクランブルするとともに、デスクランブルされた上記データを上記鍵とは異なるローカル鍵を用いて再スクランブルし、再スクランブルされたデータを記録するステップと、

上記条件付きアクセス装置により、記録されているスクランブルされたデータをデスクランブルすることを要求するステップと、

上記記録されているスクランブルされたデータの権利要件と、上記権利履歴フィールド内の獲得されている権利とを比較するステップと、

上記獲得されている権利の少なくとも１つが上記記録されているスクランブルされたデータの権利要件に一致するとき、該スクランブルされたデータを上記ローカル鍵を用いてデスクランブルするステップを有する権利履歴監視方法。

【請求項２】

上記獲得されている権利のいずれもが上記記録されているスクランブルされたデータの権利要件に一致しないことを判定するステップと、

ユーザに対し、上記記録されているスクランブルされたデータをデスクランブルするための権利を獲得することを望むか否かを問い合わせるステップとを有する請求項１記載の権利履歴監視方法。

【請求項３】

上記スクランブルされたデータをデスクランブルするための権利を獲得するための１以上の条件を表示するステップを有する請求項２記載の権利履歴監視方法。

【請求項４】

上記条件の少なくとも１つは、上記スクランブルされたデータをデスクランブルする権利を獲得するための料金の支払いであることを特徴とする請求項３記載の権利履歴監視方法。

【請求項５】

権利履歴を監視する権利履歴監視装置において、

条件付きアクセス装置に対し、スクランブルされたデータをデスクランブルするための少なくとも１つの権利であって、所定の期間において、当該データをデスクランブルしたコンテンツ又はサービスを視聴するための権利を与える権利付与装置と、

上記スクランブルされたデータを鍵を用いてデスクランブルするデスクランブル装置と、

デスクランブルされた上記データを上記鍵とは異なるローカル鍵を用いて再スクランブルする再スクランブル装置と、

上記条件付きアクセス装置内の権利管理メッセージにおける権利履歴フィールドに上記与えられた権利及び再スクランブルされた上記データを記録する記録装置と、

上記条件付きアクセス装置により、記録されているスクランブルされたデータをデスクランブルすることを要求する要求装置と、

上記記録されているスクランブルされたデータの権利要件と、上記権利履歴フィールド内の獲得されている権利とを比較する比較装置と、

を備え、

上記デスクランブル装置は、上記獲得されている権利の少なくとも１つが上記記録されているスクランブルされたデータの権利要件に一致するとき、該スクランブルされたデータを上記ローカル鍵を用いてデスクランブルする、権利履歴監視装置。

【請求項６】

上記獲得されている権利のいずれもが上記記録されているスクランブルされたデータの権利要件に一致しないことを判定する判定手段と、

ユーザに対し、上記記録されているスクランブルされたデータをデスクランブルするための権利を獲得することを望むか否かを問い合わせる表示装置とを備える請求項５記載の権利履歴監視装置。

【請求項７】

上記表示装置は、上記スクランブルされたデータをデスクランブルするための権利を獲得するための１以上の条件を表示することを特徴とする請求項６記載の権利履歴監視装置。

【請求項８】

上記条件の少なくとも１つは、上記スクランブルされたデータをデスクランブルする権利を獲得するための料金の支払いであることを特徴とする請求項５記載の権利履歴監視装置。

【請求項９】

権利履歴を監視する権利履歴監視装置において、

条件付きアクセス装置に対し、スクランブルされたデータをデスクランブルするための少なくとも１つの権利であって、所定の期間において、当該データをデスクランブルしたコンテンツ又はサービスを視聴するための権利を与える権利付与手段と、

上記スクランブルされたデータを鍵を用いてデスクランブルするデスクランブル手段と、

デスクランブルされた上記データを上記鍵とは異なるローカル鍵を用いて再スクランブルする再スクランブル手段と、
上記条件付きアクセス装置内の権利管理メッセージにおける権利履歴フィールドに上記与えられた権利及び再スクランブルされた上記データを記録する記録手段と、
上記条件付きアクセス装置により、記録されているスクランブルされたデータをデスクランブルすることを要求する要求手段と、
上記記録されているスクランブルされたデータの権利要件と、上記権利履歴フィールド内の獲得されている権利とを比較する比較手段と、
を備え、
上記デスクランブル手段は、上記獲得されている権利の少なくとも１つが上記記録されているスクランブルされたデータの権利要件に一致するとき、該スクランブルされたデータを上記ローカル鍵を用いてデスクランブルする、権利履歴監視装置。
【請求項１０】
条件付きアクセス装置に対し、スクランブルされたデータをデスクランブルするための少なくとも１つの権利であって、所定の期間において、当該データをデスクランブルしたコンテンツ又はサービスを視聴するための権利を与えるステップと、
上記条件付きアクセス装置内の権利管理メッセージにおける権利履歴フィールドに上記与えられた権利を記録し、上記スクランブルされたデータを鍵を用いてデスクランブルするとともに、デスクランブルされた上記データを上記鍵とは異なるローカル鍵を用いて再スクランブルし、再スクランブルされたデータを記録するステップと、
上記条件付きアクセス装置により、記録されているスクランブルされたデータをデスクランブルすることを要求するステップと、
上記記録されているスクランブルされたデータの権利要件と、上記権利履歴フィールド内の獲得されている権利とを比較するステップと、
上記獲得されている権利の少なくとも１つが上記記録されているスクランブルされたデータの権利要件に一致するとき、該スクランブルされたデータを上記ローカル鍵を用いてデスクランブルするステップとを有する命令を含むコンピュータで読取可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、娯楽システム（entertainment systems）に用いるセットトップボックス等のプログラム視聴装置（program viewing unit）に関する。特に、本発明は、将来、鍵期間終了（key expiration）の問題を生じることなく、プログラムデータをデスクランブルして視聴できるように、プログラムデータをスクランブルする方法及び装置に関する。
【背景技術】
【０００２】
デジタル通信方式は、アナログ通信方式に代わって急速に普及しつつある。デジタルテレビジョンは、２００２年までに米国国内の全ての視聴者が利用できるようになり、２００６年までに完全に置き換えられる予定である。高精細度テレビジョン（High-definition television：ＨＤＴＶ）放送は、制限付きで多くの都市で開始されている。同様に、インターネットとワールドワイドウェブの爆発的な普及により、例えばＭＰ３フォーマットのオーディオファイルやその他のコンテンツを含むダウンロード可能なオーディオビジュアルファイルも広く普及している。
【０００３】
同時に、このようなデジタル通信方式への急速な移行に伴い、デジタル記録機器も大きく進化している。高品質の記録及びアナログ技術において知られている世代間の劣化（すなわち、コピーを繰り返すことによりデータ品質が順次劣化していくこと）を生じることなくコピーを作成するデジタル記録機器の例として、デジタルバーサタイルディスク（Digital versatile disk：以下、ＤＶＤという。）レコーダ、デジタルＶＨＳビデオテープレコーダ（以下、Ｄ－ＶＨＳ ＶＴＲという。）、ＣＤ－ＲＯＭレコーダ（例えば、ＣＤ

－Ｒ及びＣＤ－ＲＷ）、ＭＰ３記録機器、及びハードディスクを利用した記録機器等が知られている。デジタル通信方式及びデジタル記録機器の普及により、例えば映像及び音楽制作業者等のコンテンツ提供業者は、著作権等により保護されるべき素材が正当な許可なく自由にコピーされてないよう工夫する必要がある。

【０００４】

これに応じて、例えば地上波放送局、ケーブル放送局及び直接放送衛星（direct broadcast satellite：以下、ＤＢＳという。）運営業者、及びダウンロード可能なコンテンツを提供するインターネットサイトを運営する企業に何らかのコピープロテクト策を講じさせる要求が高まっている。このようなコピープロテクトの手法は、データハイディングサブグループ（Data Hiding Sub Group：以下、ＤＨＳＧという。）の５Ｃグループ（５Ｃは、ソニー、日立、東芝、松下、インテルを表す。）及びデータトランスミッションディスカッショングループ（Data Transmission Discussion Group：以下、ＤＴＤＧという。）から提案されている。これらは、コピープロテクト技術ワーキンググループ（Copy Protection Technical Working Group：ＣＰＴＷＧ という。）の製造業者委員会サブグループ（industry committee sub-groups）である。ＣＰＴＷＧは、コンテンツ提供業者と、コンピュータ及び民生用電子機器製造業者の代表団体である。

【０００５】

ＤＴＤＧのデジタル伝送コピープロテクト（Digital Transmission Copy Protection：以下、ＤＴＣＰという。）は、例えば、ＩＥＥＥ１３９４シリアルバス等のデジタル伝送媒体を介して接続されたデジタル機器間で伝送される著作権保護されたデジタルコンテンツを保護することを目的とする。この手法では、機器毎に対称鍵暗号技術（symmetric key cryptographic techniques）を用い、互換性のある機器のコンポーネントをエンコードする。これにより、デジタルコンテンツを送信する前に、全てのデジタル機器について、そのデジタル機器が互換性を有するか否かを判定するための認証処理を行うことができる。デジタルコンテンツ自身は、コンテンツが不正にコピーされた場合、そのコンテンツが理解できないようなフォーマットになるようにエンコードされた後に伝送される。

【０００６】

ＤＨＳＧが提案するコンテンツの符号化の一手法は、電子透かし技術に基づくものである。ＤＨＳＧの提案の中心は、特にＤＶＤ装置に適用されるデジタル映画及び映像コンテンツのコピープロテクトであるが、この手法は、デジタル放送又はデジタルネットワークを介して電子的に配信される如何なるデジタルコンテンツのコピープロテクトにも適用できる。ユーザが見ることのできない電子透かしは、供給されるコンテンツにマーキングされ、この電子透かしによりコンテンツがどのようにエンコードされているかを詳細に知ることができず、したがってコンテンツを損なうことなく電子透かしを除去又は変更することは極めて難しい。ＤＨＳＧでは、この技術を適用する３つの主要な検出及び制御の状況が定められている。これらは、再生、記録及びコピー生成の制御である。この電子透かし技術により、コンテンツの提供業者は、少なくとも、コンテンツを「コピー不可（copy never）」とするか、「１回のみコピー可（copy once）」とするか、「コピー自由（copy free）」とするかを特定することができる。「コピー不可」は、デジタルコンテンツのコピーが許可されていないことを示すマークを付するために使用され、「コピー自由」は、コンテンツを自由にコピーしてもよいことを示し、この情報は他の情報とともにマーキングしてもよい。これは、マーキングされていない素材とは異なるものである。「１回のみコピー可」は、デジタルコンテンツのコピーが１回だけ許可されていることを示す。コピーが作成されると、元の「１回のみコピー可」のコンテンツと、新たにコピーされたコンテンツには、「更なるコピー不可（no more copy）」のマークが付される。もちろん、例えば、特定の時間、期間、あるいは再生又は視聴の回数等、他の種類のコピー管理コマンドによりこのようなデジタルコンテンツの再生（play）又は再現（reproduction）を制限してもよい。

【０００７】

このように、現在でも、セットトップボックス、デジタルテレビジョン、デジタルオー

ディオプレイヤ、これらに類似するデジタル機器等のデジタル機器は、条件付きアクセス（conditional access：以下、ＣＡという。）、すなわち実時間視聴（real-time viewing and/or listening）のためのＣＡクリアフォーマット（CA-clear format）にコンテンツをデスクランブルするためだけの従来の機能を超えて、このようなデジタルコンテンツの記録及び再生に制約及び条件を含ませる機能を有するようになっている。現在、スクランブルされたコンテンツを後でデスクランブルして視聴するためにコピーする行為は、サービス／コンテンツ提供業者による適切な許諾又は鍵をデジタル機器に与えることにより行うことができる。

【０００８】

例えば、地上波放送局、ケーブル放送局及びＤＢＳ運営業者は、様々な鍵配信法（key delivery methods）を用いてプログラムデータをエンコードすることにより、視聴者に配信するプログラムデータを調整している。これら共通の鍵配信法では、鍵及び制御ワード（contorl word）を用いてプログラムデータ内のコンテンツをスクランブルしている。この手法では、放送の期間において周期的に変更される制御ワードを用いてプログラムデータ内のコンテンツをスクランブルしてもよい。制御ワードは、プログラムデータ内の権利制御メッセージ（entitlement control messages）に組み込まれ、このプログラムデータの権利管理メッセージ（Entitlement management messages）に挿入されている鍵を用いてスクランブルされる。コンテンツをデスクランブルするために、鍵を検索し、この鍵を用いて制御ワードをデスクランブルする必要がある。続いて、制御ワードは、コンテンツのデスクランブルに利用される。

【０００９】

視聴者に対しては、コンテンツがスクランブルされたプログラムデータを記録し、後でコンテンツをデスクランブルして表示させることが許可される。例えばセットトップボックス等のプログラム視聴装置は、記録されたプログラムデータ内のコンテンツをデスクランブルするとともに、デスクランブル処理の記録を作成し、サービス提供業者に報告するように設計してもよい。これにより、サービス提供業者は、視聴者によるプログラムデータの利用を監視し、視聴者に対しサービス利用料を請求することができる。プログラム視聴装置には、ペイパービュー（pay-per-view）、ペイパープレイ（pay-per-play）、ペイパータイム（pay-per-time）又はその他の特徴を有する特別な料金徴収方式をサポートする鍵管理機能を設けてもよい。

【００１０】

現在の鍵配信法の問題は、サービス提供業者がスクランブル制御ワードに使用する鍵を周期的に変更する点にある。このため、プログラム視聴装置は、サービス提供業者から供給される現在の鍵が、記録されているプログラムデータ内のスクランブル制御ワードに使用されている鍵と同じ場合のみしかプログラムデータ内のコンテンツをデスクランブルすることができない。記録されているプログラムデータ内の制御ワードをスクランブルするために使用された鍵の有効期間が終了した後は、プログラム視聴装置は、コンテンツをデスクランブルすることができない。

【００１１】

発明の開示

本発明の具体例においては、一方向性関数を用いて複数の鍵を所定の順序で相互に関連付ける。本発明の他の具体例においては、それぞれが所定の期間に対応するアクセス鍵を含む複数の権利制御メッセージを生成することにより将来のアクセス鍵を提供する。本発明の他の具体例においては、複数の期間に対応する複数のアクセス鍵を含む権利制御メッセージを生成することにより、将来のアクセス鍵を提供する。

【発明の概要】

【発明が解決しようとする課題】

【００１２】

本発明の他の具体例においては、過去の期間に記録されたコンテンツを視聴する権利をユーザが有しているか否かに関する情報を含む権利に関する時間的履歴フィールドを含む

権利管理メッセージを生成することにより、権利の履歴を監視する。

【００１３】

本発明の他の具体例においては、プログラムが古いものであるか否かを判定し、ユーザがその古いプログラムを視聴する権利を有しているかを判定することにより、記録されているデジタルプログラムへのアクセスを認証する。ユーザが権利を有していない場合、ユーザがその古いプログラムを視聴することを望むか否かが問い合わされ、ユーザがその古いプログラムにアクセスすることを望む場合、ユーザに対し、料金支払いに関する複数の選択肢が表示される。

【図面の簡単な説明】

【００１４】

【図１】図１は、本発明を適用した娯楽システムの構成を示すブロック図である。

【図２】図２は、本発明を適用したプログラム視聴装置の構成を示すブロック図である。

【図３】図３は、本発明を適用した条件付きアクセス器の構成を示すブロック図である。

【図４】図４は、鍵を保存するために必要な記憶容量の具体例を示す図である。

【図５Ａ】図５Ａは、現在の鍵を用いて過去の鍵を算出する方法の一具体例を説明する図である。

【図５Ｂ】図５Ｂは、現在の鍵を用いて過去の鍵を算出する手順を示すフローチャートである。

【図５Ｃ】図５Ｃは、現在の鍵を用いて過去の鍵を算出する方法の一具体例を説明する図である。

【図６Ａ】図６Ａは、権利制御メッセージの具体例であり、図６Ｂは、将来の鍵を含む権利制御メッセージの具体例を示す図である。

【図６Ｂ】図６Ｂは、権利制御メッセージの具体例であり、図６Ｂは、将来の鍵を含む権利制御メッセージの具体例を示す図である。

【図６Ｃ】図６Ｃは、将来の鍵を含む権利制御メッセージの具体例を示す図である。

【図６Ｄ】図６Ｄは、将来の鍵を含む権利制御メッセージの具体例を示す図である。

【図６Ｅ】図６Ｅは、将来の鍵を含む権利制御メッセージの具体例を示す図である。

【図６Ｆ】図６Ｆは、将来の鍵を含む権利制御メッセージの具体例を示す図である。

【図７】図７は、権利制御メッセージを生成する際に用いられるエラーメッセージの例である。

【図７Ａ】図７Ａは、将来の鍵を含む権利制御メッセージを生成する手順を示すフローチャートである。

【図７Ｂ】図７Ｂは、将来の鍵を含む権利制御メッセージを生成する手順を示すフローチャートである。

【図８Ａ】図８Ａは、権利履歴を含む権利管理メッセージの具体例を示す図である。

【図８Ｂ】図８Ｂは、権利履歴を含む権利管理メッセージの具体例を示す図である。

【図８Ｃ】図８Ｃは、権利履歴を含む権利管理メッセージの具体例を示す図である。

【図９Ａ】図９Ａは、記録されているデジタルプログラムにアクセスする権利を得るための表示を示す図である。

【図９Ｂ】図９Ｂは、記録されているデジタルプログラムにアクセスする権利を得るための表示を示す図である。

【図９Ｃ】図９Ｃは、記録されているデジタルプログラムにアクセスする権利を得るための表示を示す図である。

【図９Ｄ】図９Ｄは、記録されているデジタルプログラムにアクセスする権利を得るための表示を示す図である。

【図１０】図１０は、過去の期間に配信されたプログラムを視聴する権利をユーザが有しているか否かを判定する処理を示すフローチャートである。

【図１１】図１１は、過去の期間に配信されたプログラムのコンテンツを視聴する権利をユーザに与えるための処理を示すフローチャートである。

【発明を実施するための形態】

【００１５】
図１は、本発明に係るコピー管理方法の一具体例として示す娯楽システム（entertainment system）１００の構成を示すブロック図である。娯楽システム１００は、１以上のサービス提供業者からプログラムデータを含むビットストリームを受け取るデジタル機器１１０を備える。このようなサービス又はコンテンツ提供業者としては、地上波放送局、ケーブル放送管理事業者、直接放送衛星（ＤＢＳ）運営事業者、インターネットを介してダウンロードできるコンテンツの提供業者、及び他の同様なコンテンツ及び／又はサービス提供業者が含まれる。プログラムデータには、それぞれ後で詳細に説明するシステム情報、権利制御メッセージ、権利管理メッセージ、コンテンツ及びその他のデータが含まれる。システム情報には、プログラム名、放送時刻、ソース、検索及びデコードの方法に関する情報とともに、デジタル受信機及び他の装置に対し、プログラムデータを何時、どのように再生し、送信し、及び／又は記録するかを示す情報を提供するコピー管理コマンドが含まれている。これらコピー管理コマンドは、権利制御メッセージ（entitlement control messages：以下、ＥＣＭという。）とともに送信され、ＥＣＭは、通常、条件付きアクセス器が特定のチャンネル又はサービスへのアクセスを調整するために使用される。権利管理メッセージ（Entitlement management messages：以下、ＥＭＭという。）は、デジタル受信機１１１に対し、例えば権利及びデスクランブル鍵（descambling key）等の特権を与えるために使用される。暗号解読鍵（decryption key）は、通常、スクランブルされたデータを復元するために必要なコードであり、権利許諾の証として使用することができる。また、プログラムデータストリーム内のコンテンツは、オーディオデータ及びビデオデータを含んでいてもよく、これらはスクランブルされていてもよく、スクランブルされていなくても（clear format）よい。
【００１６】
デジタル機器１１０は、デジタル受信機１１１を備え、デジタル受信機１１１は、供給されるビットストリームを処理し、このビットストリームからプログラムデータを抽出し、プログラムデータを視聴可能なフォーマットに変換する。ここで抽出されたプログラムデータは、デコーダ１１２に供給され、コンテンツからシステム情報を分離する処理やデコード処理、伸張処理等の更なる処理が施される。デジタル受信機１１１は、さらに、娯楽システム１００内の他の構成機器によるプログラムデータへのアクセスを調整（regulate）するとともに、本発明に基づき、デスクランブルされたコンテンツ（以下、デスクランブルコンテンツという。）を有するプログラムデータと、スクランブルされたコンテンツ（以下、スクランブルコンテンツという。）を有するプログラムデータとを同時に伝送する機能をサポートする。
【００１７】
本発明の一具体例においては、デジタル機器１１０は、デジタルテレビジョンセットであり、デジタル受信機１１１は、このテレビジョンセットに一体とされたセットトップボックスであり、デコーダ１１２は、モーションピクチャエキスパートグループ（Motion Picture Experts Group：以下、ＭＰＥＧという。）デコーダである。この具体例においては、デジタルテレビジョンセットの表示装置（図示せず）は、デジタル機器１１０に一体とされている。これに代えて、デジタル機器１１０は、デジタル受信機１１１及び／又はデコーダ１１２のみを備え、表示装置をデジタル機器１１０の外部に設けてもよい。このような構成の例としては、デジタル機器１１０は、ＮＴＳＣ、ＰＡＬ又は$Y_pB_pR$信号を出力する統合型受信機／デコーダ（integrated receiver/decoder：以下、ＩＲＤという。）であってもよい。これら具体例は、全て本発明の範囲内にある。
【００１８】
デジタル機器１１０は、伝送媒体１２０を介して、娯楽システム１００内の他の構成機器に接続されていてもよい。伝送媒体１２０は、デジタル機器１１０と、娯楽システム１００内の他の構成機器との間の制御情報及びプログラムデータを含むデータの送受信に使用される。なお、図１に示す娯楽システム１００は、例示的なものであり、他のアナログ及び／又はデジタル機器を以下に説明する構成要素に加えて、又は置換して娯楽システム

を構成してもよい。

【００１９】

図１に示す娯楽システム１００は、伝送媒体１２０に接続されたオーディオ装置１３０を備える。オーディオ装置１３０は、スピーカ装置及びコンパクトディスクプレイヤ、ソニーミニディスク（登録商標）プレイヤ、又はオーディオデータを再生及び／又は記録するために使用される他の光磁気ディスク記録再生装置を備える。また、娯楽システム１００は、伝送媒体１２０を介してデジタル機器１１０及び他の構成機器に接続されたＤ－ＶＨＳビデオテープレコーダ等のデジタルビデオテープレコーダ（以下、デジタルＶＴＲという。）１４０を備える。周知のように、デジタルＶＴＲ１４０は、アナログ又はデジタルフォーマットのオーディオ及びビデオ信号を記録し、データの送受信を行う機能を有するとともに、本発明に基づき、デジタル機器１１０が受信し、伝送媒体１２０を介してデジタルＶＴＲ１４０に供給されたプログラムデータを記録するためにも使用される。

【００２０】

さらに、娯楽システム１００は、伝送媒体１２０を介してデジタル機器１１０及び他の構成機器に接続されたハードディスク記録装置１５０を備える。ハードディスク記録装置１５０は、パーソナルコンピュータシステムであってもよく、独立型のハードディスク記録装置であってもよく、その他アナログ及びデジタルフォーマットのオーディオ及びビデオ信号を記録し、データの送受信を行う機能を有するこの他のハードディスク記録装置であってもよい。本発明に基づき、ハードディスク記録装置１５０は、デジタルＶＴＲ１４０と同様、デジタル機器１１０が受信し、伝送媒体１２０を介してハードディスク記録装置１５０に供給したプログラムデータを記録するために使用される。

【００２１】

表示装置１６０は、高精細度テレビジョン表示装置であってもよく、モニタ装置であってもよく、デジタルビデオ信号を処理する能力を有する他の装置であってもよい。デジタル機器１１０が独立型のセットトップボックスである場合、表示装置１６０は、デジタルテレビジョンセットであってもよい。

【００２２】

また、伝送媒体１２０に制御装置１７０を接続してもよい。制御装置１７０は、娯楽システム１００の各構成機器の動作を調整（coordinate）及び制御するとともに、制御装置１７０にリモート接続されている他の電子機器を制御する。

【００２３】

図２は、本発明に基づくコピー管理機能を有するデジタル受信機１１１の構成例を示す図である。デジタル受信機１１１は、中央演算処理ユニット（central processing unit：以下、ＣＰＵという。）２１０を備え、ＣＰＵ２１０は、デジタル受信機１１１の全体の動作を制御するとともに、選択されたチャンネルが放送又は伝送されている周波数を決定する。この情報は、チューナ２２０に供給され、チューナ２２０は、プログラムデータを含む入力デジタルビットストリームを受信する地上波、ケーブル、衛星放送の適切な周波数又はインターネットのウェブサイトを選択する。また、ＣＰＵ２１０は、電子プログラムガイド（electronic programming guide：以下、ＥＰＧという。）等のグラフィカルユーザインターフェイス（graphical user interface：以下、ＧＵＩという。）をサポートする。ＥＰＧは、ユーザに対し、様々なチャンネル及びプログラムオプションを案内するものであり、ユーザはこれにより所望のチャンネル又はプログラムを選択し、視聴及び録画等を行うことができる。ＧＵＩは、デジタル機器１１０の表示装置（例えば、デジタル機器１１０がデジタルテレビジョンセットの場合等）に表示してもよく、表示装置１６０（例えば、デジタル機器１１０が独立型のセットトップボックスである場合）に表示してもよい。

【００２４】

チューナ２２０は、適切な周波数を選択すると、入力デジタルビットストリームを増幅し、出力ビットストリームを復調器２３０に供給する。復調器２３０は、チューナ２２０から供給されたビットストリームを復調し、伝送されてきた元のプログラムデータを再生

する。もちろん、復調器２３０が実行する復調処理の種類は、伝送処理において使用されている変調処理及び伝送の種類に基づいて決定される。例えば、ケーブルモデムを用いたインターネットのケーブル伝送の場合、復調器２３０は、直交振幅復調（quadrature amplitude demodulation：以下、ＱＡＤという。）を行い、衛星放送の場合は４相位相偏移（quadrature phase shift key：以下、ＱＰＳＫという。）復調処理が必要となる。地上波放送の場合は、残留側波帯（vestigial side band：以下、ＶＳＤという。）復調処理が必要となる場合が多い。本発明は、伝送の種類及び変調／復調の方式を限定するものではなく、上述以外の方式も本発明の範囲内にある。復調器２３０は、復調処理に加えて、受け取ったビットストリームに対するエラー訂正処理を行う。

【００２５】

復調されたビットストリームは、条件付きアクセス器２４０に供給される。（暗号化されていない復調されたビットストリームの一部は、条件付きアクセス器２４０をバイパスし、図２において破線で示すように、デマルチプレクサ２５０に直接供給してもよい。あるいは、ビットストリーム全体が暗号解読処理を必要としないこともあり、及び／又は条件付きアクセス器２４０を設けなくてもよい場合もある。）条件付きアクセス器２４０は、後述するデスクランブル処理とともに、鍵管理及び暗号解読処理を実行する。

【００２６】

通常、ＣＰＵ２１０は、デジタルビットストリーム内のプログラムデータ内のコンテンツがスクランブルされていることを判定し、このプログラムデータを条件付きアクセス器２４０に供給する。このとき、ＣＰＵ２１０は、パケット識別子（packet identifier：以下ＰＩＤという。）情報を条件付きアクセス器２４０に供給する。ＰＩＤ情報は、条件付きアクセス器２４０に対し、プログラムデータ内のどこでＥＣＭが検出されるかを知らせる。これに代えて、ＣＰＵ２１０がＥＣＭを受け取り、受け取ったＥＣＭを条件付きアクセス器２４０に供給するようにしてもよい。あるいは、条件付きアクセス器２４０にデマルチプレクス機能を設け、ビットストリーム自体からＥＣＭの位置を直接検出できるようにしてもよい。上述のように、ＥＣＭは、特定のチャンネル又はサービスへのユーザのアクセスを調整し、アクセスを許諾するためにデジタル受信機１１１が有すべきアクセス権を判定するためのメッセージである。また、ＥＣＭは、暗号解読鍵又はデスクランブル鍵を配信するために使用することもでき、あるいはスクランブルされたコンテンツをデスクランブルするために使用する鍵をどのように獲得するかを示す情報（例えば、アルゴリズム）を配信するためにも使用できる。条件付きアクセス器２４０は、このような鍵又は鍵獲得に関する情報を用いて、プログラムデータに含まれるコンテンツをデスクランブルすることができる。これに代えて、条件付きアクセス器２４０がデマルチプレクサ２５０に鍵を供給し、このデマルチプレクサ２５０によりデスクランブルを実行してもよい。

【００２７】

なお、条件付きアクセス器２４０は、一体型又は組込型として示しており、いずれの場合もデスクランブル及び暗号解読処理はデジタル受信機１１１の内部で実行されるが、条件付きアクセス器２４０を分離し、デジタル受信機１１１の外部に設けてもよい。外部に設けられる条件付きアクセス器２４０は、例えば、ナショナルリニューアブルセキュリティ方式（National Renewable Security System ：以下、ＮＲＳＳという。）のように、外部でプログラムデータコンテンツをデスクランブルし、鍵を暗号解読する。分離された条件付きアクセス器２４０においては、プログラムデータコンテンツはデジタル受信機１１１内でデスクランブルされ、鍵暗号解読処理は、例えば、スマートカード等により外部で実行される。これらいずれの方法も本発明の範囲内にある。

【００２８】

条件付きアクセス器２４０がプログラムデータコンテンツをデスクランブルすると、プログラムデータはデマルチプレクサ２５０に供給される。デマルチプレクサ２５０は、プログラムデータ内のコンテンツからシステム情報を分離する。本発明の具体例においては、デマルチプレクサ２５０は、プログラムデータを解析（parse）して、システム情報、オーディオ情報及びビデオ情報に関連付けられたＰＩＤを検出し、システム情報をＣＰＵ

２１０に供給し、オーディオ情報及びビデオ情報をデコーダ１１２に供給する。本発明の具体例においては、条件付きアクセス器２４０には、デジタルインターフェイス２６０が接続されている。後述するように、このデジタルインターフェイス２６０により、デジタル受信機１１１は、娯楽システム１００内の他のデジタル構成要素と通信を行うことができる。

【００２９】

ＣＰＵ２１０、チューナ２２０、復調器２３０、条件付きアクセス器２４０、デマルチプレクサ２５０及びデジタルインターフェイス２６０は、周知の如何なる技術及び如何なる回路を用いて実現してもよい。本発明の一具体例においては、ＣＰＵ２１０、チューナ２２０、復調器２３０、デマルチプレクサ２５０及びデジタルインターフェイス２６０は、単一の筐体内に収納され、条件付きアクセス器２４０は、（上述のように）外部ＮＲＳＳ条件付きアクセス器内に設けられる。ＮＲＳＳにおいて、条件付きアクセス器２４０は、パーソナルコンピュータメモリカードインターナショナルアソシエーション（Personal Computer Memory Card International Association：ＰＣＭＣＩＡ）規格に準拠するものであってもよく、スマートカードにより実現してもよい。

【００３０】

図３は、本発明に基づくコピー管理システムの条件付きアクセス器２４０の構成例を示すブロック図である。条件付きアクセス器２４０は、復調器２３０から復調されたプログラムデータを受け取り、プログラムデータ内のどこでＥＣＭを検出できるかを特定するＰＩＤ情報を読み出すプロセッサ３３０を備える。上述のように、このＰＩＤは、ＣＰＵ２１０から供給されてもよく、条件付きアクセス器２４０自体によりビットストリームから直接検出するようにしてもよい。

【００３１】

本発明の一具体例においては、プロセッサ３３０は、ＥＣＭを処理し、コンテンツをデスクランブルする鍵を導き出す。次に、プロセッサ３３０は、プログラムデータ及び鍵を信号線、ピン、又はピンの組３３５（以下、単に信号線３３５という。）を介してデスクランブラ３４０に供給する。デスクランブラ３４０は、信号線３３５を介して鍵及びプログラムデータを受け取り、鍵によりプログラムデータをデスクランブル又は暗号解読処理する。デスクランブラ３４０は、デスクランブルされたコンテンツを有するプログラムデータを信号線、ピン、又はピンの組３４６（以下、単に信号線３４６という。）を介して、デマルチプレクサ２５０（図２）、続いてデコーダ１１２に供給し、このプログラムデータに基づく映像が表示され、ユーザに視聴される。

【００３２】

デスクランブラ３４０は、デスクランブルされたコンテンツを有するプログラムデータを信号線、ピン、又はピンの組３４５（以下、単に信号線３４５という。）を介して再スクランブラ（re-scrambler ）３５０に供給する。再スクランブラ３５０は、プログラムデータを受け取り、そのプログラムデータのデスクランブルされているコンテンツを再びスクランブルする等の処理を実行する。この再スクランブル処理では、デスクランブル処理により用いられたアルゴリズムと同様のアルゴリズムを用いることができる。例えば、ＤＥＳをデスクランブル処理と再スクランブル処理の両方に用いることができる。

【００３３】

（なお、図３においては、説明のため、プロセッサ３３０と、デスクランブラ３４０と、再スクランブラ３５０とを個別の要素として示しているが、これらの要素は、１つの機器に統合してもよく、あるいは周知の回路又は技術により実現してもよい。）

再スクランブラ３５０は、複数の方法の内の一方法を用いてコンテンツを再スクランブルする。例えば、本発明に係るコピー管理システムの一具体例において、再スクランブラ３５０は、元のビットストリームとして送信され、デジタル受信機１１１が受信したＥＣＭを用いてコンテンツを再スクランブルしてもよい。これに代えて、元のビットストリームにおいてＥＣＭとは分離された独立した再スクランブル鍵（re-scrambling key）を伝送し、これを再スクランブラ３５０がデスクランブラ３４０から受け取ったプログラムデ

ータから抽出するようにしてもよい。本発明に係るコピー管理システムの他の具体例においては、再スクランブラ３５０は、暗号化処理又は符号化処理を行う能力を有し、デジタル受信機１１１に固有のローカル鍵（local key）を用いてコンテンツを再スクランブルしてもよい。このような鍵は、ＥＣＭを用いては伝送できないが、ＥＭＭを用いて再スクランブラ３５０に供給することができる。これに代えて、再スクランブラ３５０の製造時に作成された変更不可能な鍵を使用してもよい。

【００３４】

本発明の更なる具体例においては、鍵に加えて制御ワード（control word）を用いてもよい。このような具体例では、制御ワードは、まず、鍵を用いてスクランブルされ、続いて伝送の前に、プログラムデータのビットストリームに挿入される。この方法では、プログラムデータ内のコンテンツをデスクランブルするために、条件付きアクセス器２４０は、最初に鍵を検出し（上述のいずれかの方法を用いて）、続いて検出した鍵を用いて制御ワードをデスクランブルする。デスクランブルされた制御ワードは、コンテンツのデスクランブルに使用される。この方法により、ローカル鍵を変更する必要なく制御ワード（したがってアクセス権）を周期的に変更することができるため、特にローカル鍵が使用されている場合（すなわち、デジタル受信機１１１内に設けられている場合）、伝送における柔軟性を高め、安全性を向上させることができる。このようにして、再スクランブラ３５０は、複数の方法の内の１つを用いてコンテンツをスクランブルできる。再スクランブラ３５０は、送信されてきた元の制御ワード及び鍵を用いて制御ワードを再スクランブルしてもよい。これに代えて、再スクランブラ３５０は、デジタル受信機１１１に固有のローカル制御ワード及び鍵を使用してもよい。上述の方法は、単独でも、組み合わせても使用できることは当業者にとって明らかであり、これら及び類似の方法は、全て本発明の範囲内にある。

【００３５】

コンテンツが再スクランブルされると、この再スクランブルされたコンテンツを含むプログラムデータは、信号線、ピン、又はピンの組３５５（以下、単に信号線３５５という。）を介して出力される。本発明の一具体例においては、再スクランブルされたプログラムデータは、図２に示すように、デジタルインターフェイス２６０を介して出力される。デジタルインターフェイス２６０は、このプログラムデータが「コピー自由」であることを示すコピー管理コマンドとともにこのプログラムデータをエンコードする。デジタルインターフェイス２６０は、伝送媒体１２０に接続された構成機器（図１に示す）間のインターフェイスを司り、どの構成機器がエンコードされたプログラムデータをデコードする権利を有しているかを判定し、その権利を有する構成機器に鍵を供給し、エンコードされたプログラムデータをデコードさせる。娯楽システム１００の一具体例においては、デジタルインターフェイス２６０は、認証処理を実行し、エンコードされたプログラムデータをデコードする権利を有する機器を判定し、ＤＴＤＧのＤＴＣＰエンコード法を用い、ＩＥＥＥ１３９４伝送媒体を介して伝送されるプログラムデータをエンコードする。なお、本発明の趣旨及び範囲から逸脱することなく、他のエンコード法を用いることもできる。

【００３６】

このように、信号線３４６は、デスクランブルされたコンテンツをデマルチプレクサ２５０に供給し、デジタル機器１１０に一体とされた、又は直接接続されている表示装置にコンテンツを表示させ、一方、信号線３５５は、再スクランブルされたコンテンツを出力し、伝送媒体１２０を介して、伝送媒体１２０に接続されている１以上の構成機器に再スクランブルされたコンテンツを供給して記録させるので、この条件付きアクセス器２４０によれば、ユーザは、プログラムデータをデスクランブルして視聴できるとともに、同時にスクランブルされたプログラムデータを記録することができる。なお、この具体例においては、信号線３５５を介して出力される再スクランブルされたストリームは、視聴される前に、適切な鍵及び／又は制御ワードによりデスクランブルされなくてはならず、したがって条件付きアクセス器２４０により処理されなくてはならないため、コンテンツ提供業者は、ユーザがコンテンツをコピーできるか否か、コピーできるとすれば何時コピーで

きるか、又はコンテンツを再び視聴することができるか、できるとすれば何時視聴できるかを任意に指定することができる。

【００３７】

ユーザは、スクランブルされたデジタルコンテンツをスクランブルされたフォーマットのまま記録することができる。このような処理を行う理由は幾つかある。例えば、「コピー不可」の属性がマークされており、時間のシフトが望まれる場合、デスクランブルしたプログラムのコンテンツの記録は、提供業者によって許諾されていない。あるいは、複数のプログラムを含むデジタル伝送ストリーム全体を記録し、これらプログラムの内の１つのみをデスクランブルし、１回だけ視聴できるようにすることもできる。スクランブルされたコンテンツを再生するとき、コンテンツにおける未視聴の部分をデスクランブル及び視聴することにより、ストリームにおける未視聴の部分にアクセスすることができる。さらに、スクランブルされたコンテンツをローカルの場所に記録することにより、ペイパービュー（pay-per-view）、ペイパータイム（pay-per-time）、遅延インパルスペイパービュー（delayed impulse pay-per-view (IPPV)）、「コピー不可」の映画の再購入及び安全性を高めるための個人的なスクランブル処理等、特別な料金徴収のための鍵管理をより高度に制御することができる。

【００３８】

コンテンツをデスクランブルするために使用される情報は、鍵により提供される。この鍵情報を暗号化してもよい。鍵は、鍵の暗号解読に必要な情報とともに、ＥＭＭ又はＥＣＭにより条件付きアクセス器２４０に供給される。ＥＭＭ又はＥＣＭが変更（modify）されると、鍵情報も変更され、使用できなくなってしまう。例えば顧客の支払いサイクルに応じて１ヶ月毎等、定期的に鍵情報を変更してもよい。

【００３９】

時間により鍵を変更すると、鍵の保存に関する問題が生じる。古い期間における鍵を保存する必要があり、この鍵を保存しないと、この鍵を用いて記録されたプログラムのスクランブルされたコンテンツへのアクセスが拒否される。もちろん、古い鍵を保存することにより、古い期間に対応する鍵情報を保存することもできる。２つの異なる期間に記録されたコンテンツをデスクランブルするためには、２つの鍵を保存する必要がある場合もある。さらに、幾つかの条件付きアクセス方式は、各サービスに対して固有の鍵を設けている場合もある。各サービス毎に独立した鍵を要求する方式において、テープ状記録媒体に記録された全てのプログラムを再生することが望まれる場合には、大量の鍵を保存しなくてはならない。保存すべきデータ量は、図４に示すように、異なる期間及び異なるサービスに対応する鍵の数に応じて増加する。

【００４０】

図５Ａは、鍵を保存するために必要なデータ量を削減するために、過去の鍵を算出する方法の具体例を示す図である。鍵は一方向性関数（one way function）により関連付けられている。先行する鍵は、現在の鍵のハッシュ関数（hash）である。条件付きアクセス器２４０が現在の鍵に関する情報を有している場合、条件付きアクセス器２４０は、先行する期間に対応する先行する鍵を算出することができる。しかしながら、鍵は、一方向のみに関連付けられているため、将来の期間に対応する鍵は、現在の鍵からは算出又は導出できない。この具体例においては、鍵が関連付けられている方向は、現在の鍵から先行する鍵への方向である。これにより、条件付きアクセス器２４０は、現在の鍵に基づいて、先行する鍵をハッシュ及び算出して、以前に保存したスクランブルされたプログラムをデスクランブルすることができる。

【００４１】

この具体例では、全ての可能な鍵は、時間を遡って算出することができる。例えば、鍵が１０年間毎月変更された場合、一方向性関数を１２０回（毎年１２回×１０年）呼び出す必要がある。最初に使用された鍵は、最後に算出される。一具体例においては、このようなハッシュアルゴリズムを１０００回実行するようにし、これにより、毎月１つの鍵を使用しても最低８０年間分の鍵以上の鍵を生成することができる。

【００４２】
図５Ｂは、これらの鍵を生成及び使用する方法の一具体例を示すフローチャートである。ステップ５０５において、直前の鍵が生成される。この直前の鍵及び一方向性関数を用いて、ステップ５１０において、２つ前の鍵を生成する。２つ前の鍵は、直前の鍵及び一方向性関数から算出することができるが、直前の鍵は、２つ前の鍵からは算出することができない。この処理は、ステップ５１５において、複数回繰り返され、一連の鍵が生成される。この一連の鍵における先行する鍵は、一方向性関数により後続する鍵に関連付けられ、これにより、所定の鍵及び一方向性関数から先行する鍵を算出することができるが、所定の鍵と一方向性関数から後続する鍵を算出することはできない。ステップ５２０においては、一連の鍵の最初の鍵から最後の鍵に至る順序で、各鍵に所定の期間が割り当てられる。各鍵は割り当てられた期間に受け取ったコンテンツのデスクランブルに使用される。ステップ５２３において、所定の期間において、その期間に対応する鍵を用いて、プログラムのコンテンツはスクランブルされ、ユーザに配信される。ステップ５２５において、鍵及び一方向性関数が条件付きアクセス器２４０に供給される。ステップ５３０において、この鍵を用いてコンテンツをデスクランブルすることにより、ネットワーク上の又はストレージ装置に記録されているコンテンツにアクセスする。ステップ５３５において、鍵及び一方向性関数を用いて、先行する期間に対応する先行する鍵を算出する。ステップ５４０において、この先行する鍵を用いて、先行する期間のコンテンツをデスクランブルする。

【００４３】
鍵を生成するために使用できるハッシュアルゴリズムとしては、安全ハッシュアルゴリズム（secure hash algorithm：以下、ＳＨＡという。）及びメディアダイジェスト５（media digest 5：以下、ＭＤ５という。）等がある。また、デジタル暗号規格（digital encryption standard：以下、ＤＥＳという。）を用いて安全ハッシュ関数を生成してもよい。図５ＣにＤＥＳを用いたハッシュ関数の例を示す。

【００４４】
図６Ｂ～図６Ｅは、将来のアクセス鍵（future access keys）の記録の具体例を示す図である。図６Ａは、通常の権利制御メッセージを示す図である。コンテンツをデスクランブルするために使用される鍵は、ＥＣＭ６１０内に送られる現在のグループ又はサービス鍵（group or service key）６４０の元で暗号化される。スクランブルされたコンテンツは、記録することができる。しかしながら、鍵の有効期間は、一定期間経過すすると消滅することがある。スクランブルされ、記録されたコンテンツをユーザが後になって視聴しようとしたとき、鍵の有効期間が切れていれば条件付きアクセス器２４０は、コンテンツを再生することができない。このようにして、サービス提供業者への支払いが強制されている。

【００４５】
図６Ｂは、将来配信されるグループ又はサービス鍵を暗号化するフィールドを含むＥＣＭの具体例を示す図である。この具体例においては、コンテンツとともに複数のＥＣＭが生成され、記録される。各ＥＣＭ６６０は、所定の期間に対応する鍵６８０，６８１，６８２，６８３を有する。図６Ｂにおいて、時間Ｘは現在の鍵期間を示し、時間Ｘ－１は、次の鍵期間を示す。一年間を通してコンテンツを視聴することがユーザに認められている場合、及び鍵が毎月変更される場合、１２個の異なるＥＣＭが生成され、データストリーム内に含まれ、コンテンツとともに記録される。これにより、ユーザは、コンテンツを記録することができるとともに、コンテンツにアクセスして視聴する権利を一年間有することとなる。

【００４６】
図７Ａは、図６Ｂに示すＥＣＭを生成する方法の一具体例を示すフローチャートである。ステップ７１０において、１以上の鍵が生成される。ステップ７２０において、所定の期間が各鍵に割り当てられる。ここで、期間は、過去の期間であっても、現在の期間であっても、将来の期間であってもよい。ステップ７３０において、複数のＥＣＭが生成され

る。各ＥＣＭは、所定の期間に対応している。ステップ７４０において、所定の期間に割り当てられた鍵を所定の期間に対応するＥＣＭ内に配置する。ステップ７５０において、プログラムのコンテンツとともに、複数のＥＣＭが記録される。ステップ７６０では、所定の期間において、その期間に対応するＥＣＭから抽出された鍵を用いて、プログラムのコンテンツをデスクランブルする。

【００４７】

図６Ｃ及び図６Ｄは、ＥＣＭの他の具体例を示す図である。ここでは、１つのＥＣＭ６７４が生成され、ＥＣＭ６７４は、複数の期間に対応する複数の鍵を含む。図６Ｃでは、暗号化された各鍵６８０，６８１，６８２，６８３は、例えば、月毎の期間に対応する。図６Ｄにおいては、ＥＣＭ６７５は、複数の鍵の元で暗号化された鍵情報を有している。鍵６８４は、現在のグループ又はサービス鍵である。鍵６８５及び鍵６８６は、時間鍵（time key）である。これらは、グループ又はサービス鍵のように同じ期間に基づいて生成されてはおらず、もっとも近い期間又は複数の期間が終了した後に、保存されているコンテンツを読み出すために使用される。時間鍵はビンテージ鍵（vintage key）は、例えば２年又は３年等の特定の長さの期間が経過した後に、特定のグループ又はサービスに由来する全ての素材（material）のロックを解除するために使用される。これにより、暗号化された鍵情報のためのフィールド数を減らすことができ、したがって、ＥＣＭを短くでき、帯域幅を削減することができる。

【００４８】

図６Ｅは、ＥＣＭ６７５の他のフォーマットの具体例を示す図である。このフォーマットは、単純なカバレッジ鍵（coverage key）６８７を用いるものであり、カバレッジ鍵６８７は、安全上の問題が生じ、すなわち破られるまで変更されず、あるいは、例えば年単位といった非常に長い期間変更されない鍵である。ＥＣＭアクセス要求６３１は、プログラムを再生するために必要な全ての情報を含んでいる。このフォーマットでは、ＥＣＭ署名６５０を用いて、変更されているアクセス条件がないことを確認する。この方法は、暗号解読又は認証確認に使用される鍵がメッセージの暗号化又は署名に使用される鍵と異なる公開鍵暗号法等の場合に有効である。ある条件付きアクセス要素を完全に分析し、その有効性を失わせたとしても、必ずしも全ての条件付きアクセス要素が破られる訳ではない。公開鍵方式も同様に破られる必要がある。公開鍵による暗号化では、他のデータを含む鍵フィールドを署名により暗号化できるため、単純なカバレッジ鍵を用いなくてもよい。

【００４９】

図７Ｂは、複数の鍵により１つのＥＣＭを生成する処理の手順を示すフローチャートである。ステップ７６５において、複数の鍵が生成される。ステップ７７０において、各鍵に１以上の期間が割り当てられる。各期間は、過去の期間であっても、現在の期間であっても、将来の期間であってもよい。ステップ７８０において、複数の鍵は、権利制御メッセージ内に配置される。ステップ７８５において、プログラムのコンテンツは、権利制御メッセージとともに記録される。所定の期間において、プログラムのコンテンツはスクランブル処理される。ステップ７９０において、スクランブル処理されたコンテンツは、ＥＣＭとともに、条件付きアクセス器２４０を介してユーザに配信される。ステップ７９７において、コンテンツは、ＥＣＭから抽出された所定の期間に対応する適切な鍵を用いてデスクランブルされる。

【００５０】

本発明は、時間的な権利の監視も行う。例えば、新たになユーザが現在サービスに加入し、現在の請求期間に配信されたコンテンツを視聴する権利を得たとする。しかしながら、このユーザは、過去のサービスを視聴する権利を有していない。そこで、このユーザが所定の料金を支払わない限り、過去に記録したコンテンツを視聴できないようにすることをサービス提供業者が望む場合、サービス提供業者は、そのユーザの権利に関する履歴を監視する必要がある。加入者がサービス又はパッケージを視聴する権利を有しているか否かに関する情報は、図８Ａに示すように、他の権利情報とともに、権利管理メッセージに含ませて配信することができる。ＥＣＭ８１０は、フィールド８３０内にユーザが現在有

している権利に関する情報を格納するとともに、ユーザの権利に関する時間的履歴８４０を有している。

【００５１】

図８Ｂは、権利管理メッセージ８５０の一具体例を示す図であり、この権利管理メッセージ８５０は、ユーザの権利履歴を監視するためのフィールド８７０を備える。権利の時間的履歴は、鍵及び権利情報とともに配信することができる。権利の時間的履歴を示すフィールド８７０内の各ビットは、１以上の離散的期間において、ユーザがサービスに加入又は視聴の権利を有しているか否かを表している。例えば、図８Ｂに示す第１のビットは、２４ヶ月前に記録されたコンテンツにアクセスする権利をユーザが有しているか否かを示している。このビットが第１の状態、例えば０である場合、ユーザがこの期間に対応する鍵情報を有していたとしても、ユーザは、この期間に記録したコンテンツを視聴することができない。この方法により、権利に関する時間的履歴情報を格納するために必要なメモリの容量を削減することができる。例えば、各ビットがそれぞれ１ヶ月間を表す場合、ヘッダ８６０の他に、２年間に相当する情報は、２４ビットすなわち３バイトのみでよい。

【００５２】

図８Ｃは、変形例である権利管理メッセージ８８０を示す図である。権利の時間的履歴に関する情報８７２は、複数のフィールドを有し、各フィールドは複数の期間に対応している。例えば、第１のビット８９０は、５ヶ月間の内のいずれかの期間においてユーザがアクセス権を有していたか否かを表しており、これにより権利の履歴情報を格納するために必要なメモリの容量をさらに削減することができる。

【００５３】

図１０は、ユーザの権利に関する時間的履歴を監視する方法の具体例を示すフローチャートである。ステップ１０１０において、ユーザは１以上の期間に関する権利を獲得し、これによりユーザはこの１以上の期間に配信されたプログラムのコンテンツを視聴することができる。ステップ１０２０において、権利が獲得された期間に関する情報が記録される。ステップ１０３０において、ユーザの権利の時間的履歴フィールドを含む権利管理メッセージが生成され、このフィールドにユーザが権利を有する期間に関する情報が格納される。ステップ１０４０において、ユーザは以前の期間に配信又は送信され、記録されたプログラムを選択することができる。ステップ１０５０において、このプログラムが記録された期間と、権利管理メッセージ内の権利に関する時間的履歴情報とが比較され、この期間に配信されたプログラムを視聴する権利がユーザにあるか否かが判定される。ステップ１０６０において、ユーザがこの期間に配信されたプログラムを視聴する権利を有していると判定された場合、ユーザはこのプログラムを選択して視聴することができる。一方、ステップ１０７０において、ユーザがこの期間に配信されたプログラムを視聴する権利を有していないと判定され場合、ユーザのアクセスは拒否され、ユーザはプログラムを視聴することができない。

【００５４】

図９Ａ～図９Ｄを用いて、記録されているデジタルプログラムへのアクセスの認証手続きの具体例を説明する。ユーザは、過去に記録されたコンテンツを視聴する権利を有する場合がある。すなわち、過去のコンテンツへのアクセスがユーザに提供されるサービスとなる場合がある。例えば、サーバ又はレコーダは、一日に放送された全てのプログラムを記録する。そして、ユーザが仕事から自宅に帰ると、ユーザは、記録されているコンテンツを視聴するためにサーバにアクセスする。汎用時間（universal time）はインクリメントされ、記録されているコンテンツは、「古い（old）」コンテンツであると判定される。コンテンツが古い場合、そのコンテンツは、例えばテープ状記録媒体等の記録媒体に記録されている。続いて、二次的条件付きアクセス装置（secondary conditional access element）が記録されているコンテンツを処理する。

【００５５】

コンテンツが古い場合、図９Ａ～図９Ｃに示すように、ユーザが認証を受け、コンテン

ツを視聴するための料金を支払うことができるように、画面に案内が表示される。図９Ａは、ユーザがコンテンツを視聴する権利を有していないことを示す画面である。ユーザは、例えば質問に応答することにより、古いコンテンツを視聴する権利を獲得する。図９Ｂは、ユーザがプログラムを視聴する権利を有していないことを示し、この場合、ユーザはプログラムを視聴するための料金を支払うことにより権利を獲得する。また、ユーザは、プログラムコンテンツが視聴者に対して放送又は配信された期間に加入することで、番組を視聴する権利を得ることもできる。図９Ｃは、複数の期間の内、それぞれユーザが視聴を望むプログラムを含む期間に加入することにより、ユーザにアクセス権を与えるための画面を示す図である。

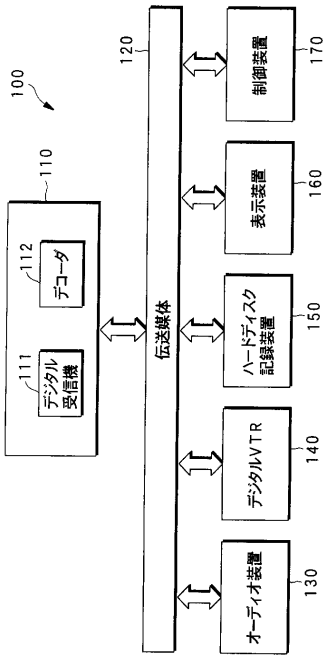
【００５６】

図９Ｄは、ユーザに対し、権利に関する履歴を表示する画面の具体例を示す図である。表９１０は、複数の期間９２０及びサービス又はコンテンツのリスト９３０を含んでいる。期間は、例えば行として表され、サービスは例えば列として表される。この表を確認することにより、ユーザは、所定の期間に放送又は配信されたコンテンツを視聴する権利を自らが有しているか否かを容易に知ることができる。例えば、表９１０における枠（box）９４０は、第１の状態にあり、ユーザは、２０００年の７月から１２月にディズニーチャンネル（Disney channel）を介して配信されたコンテンツを視聴する権利を有していない。ユーザがこの期間に配信されたこのサービスのコンテンツの視聴を望む場合、過去の権利をユーザに配信することにより、ユーザは記録されているプログラムにアクセスすることができる。すなわち、ユーザは、図９Ｄに示すフィールドを埋めるための料金を支払うことができる。このような処理により、過去に記録されたプログラムを選択的に視聴可能にすることができる。

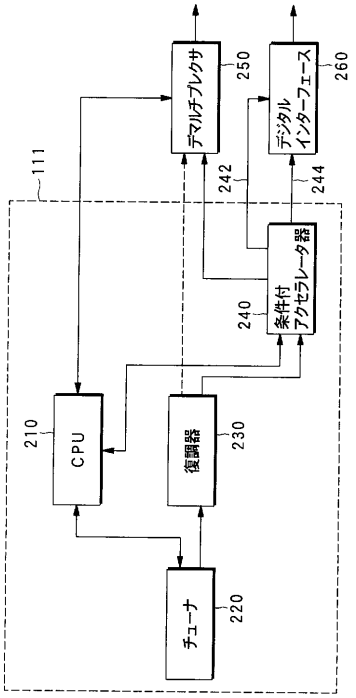
【００５７】

図１１は、過去の期間において記録又は配信されたコンテンツを視聴するための権利を得るための処理の手順を示すフローチャートである。過去の期間に記録又は配信されたプログラムを視聴する権利をユーザが有さない場合、ステップ１１１０において、そのプログラムを視聴する権利をユーザが有していないことを示すメッセージが表示される。ステップ１１２０においては、そのプログラムを視聴するための権利を獲得することをユーザが望むか否かを質問するメッセージが表示される。ステップ１１３０において、ユーザが例えばコンピュータ入力装置を用いてセットトップボックスに肯定的な応答を入力した場合、料金の支払いに関する複数の選択肢が表示される。ユーザは、この料金の支払いに関する複数の選択肢の１つを選択することにより、過去の期間に記録又は配信されたプログラムを視聴するための料金を支払い、これによりユーザはそのプログラムを視聴する権利を得る。

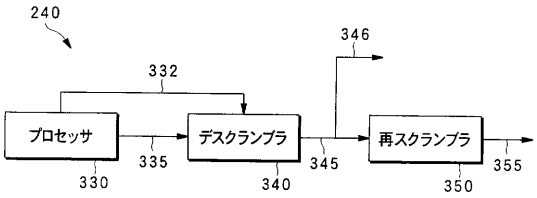
【図１】




【図２】




【図３】



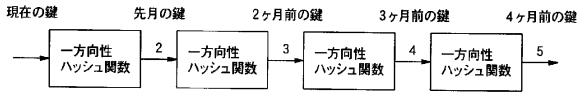

【図４】

| | 全てのサービスに対し１鍵 | 全てのサービスに対し１鍵 | 全てのサービスに対し１鍵 |
|---|---|---|---|
| 復元すべき過去の請求サイクルの数 | 7バイト (シングルDES) | 14バイト (ダブルDES) | 21バイト (トリプルDES) |
| | 7 | 14 | 21 |
| 2 | 14 | 196 | 4,116 |
| 3 | 21 | 294 | 6,174 |
| 6 | 42 | 588 | 12,348 |
| 9 | 63 | 882 | 18,522 |
| 12 | 84 | 1,176 | 24,696 |
| 18 | 126 | 1,764 | 37,044 |
| 24 | 168 | 2,352 | 49,392 |

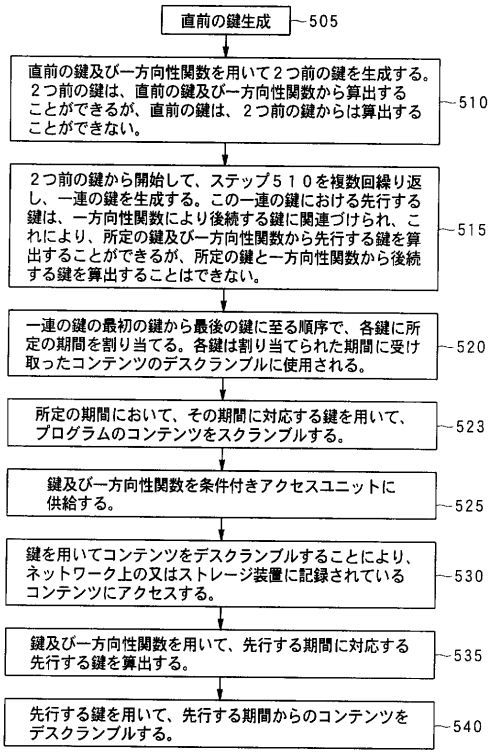
| | １０鍵 | 1パッケージ1鍵 10パッケージ可能 | |
|---|---|---|---|
| 復元すべき過去の請求サイクルの数 | 7バイト (シングルDES) | 14バイト (ダブルDES) | 21バイト (トリプルDES) |
| | 7 | 14 | 21 |
| 2 | 140 | 19,600 | 4,116,000 |
| 3 | 210 | 29,400 | 6,174,000 |
| 6 | 420 | 58,800 | 12,348,000 |
| 9 | 630 | 88,200 | 18,522,000 |
| 12 | 840 | 117,600 | 24,696,000 |
| 18 | 1,260 | 176,400 | 37,044,000 |
| 24 | 1,680 | 235,200 | 49,392,000 |

| | １００鍵 | 1サービス1鍵 100サービス可能 | |
|---|---|---|---|
| 復元すべき過去の請求サイクルの数 | 7バイト (シングルDES) | 14バイト (ダブルDES) | 21バイト (トリプルDES) |
| | 7 | 14 | 21 |
| 2 | 1,400 | 1,960,000 | 4,116,000,000 |
| 3 | 2,100 | 2,940,000 | 6,174,000,000 |
| 6 | 4,200 | 5,880,000 | 12,348,000,000 |
| 9 | 6,300 | 8,820,000 | 18,522,000,000 |
| 12 | 8,400 | 11,760,000 | 24,696,000,000 |
| 18 | 12,600 | 17,640,000 | 37,044,000,000 |
| 24 | 16,800 | 23,520,000 | 49,392,000,000 |

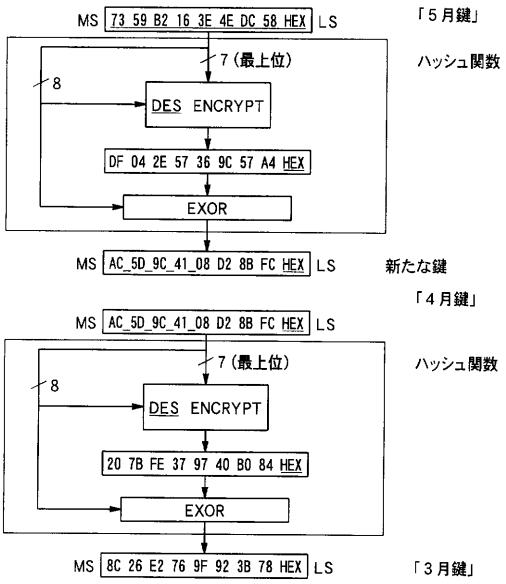
【図５Ａ】




【図５Ｂ】

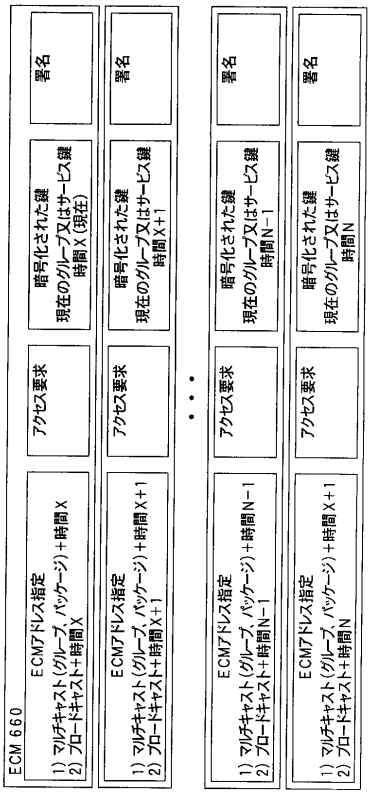



【図５Ｃ】

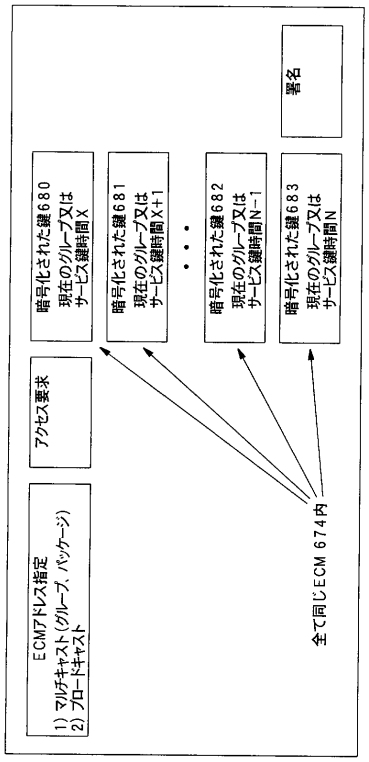



【図６Ａ】

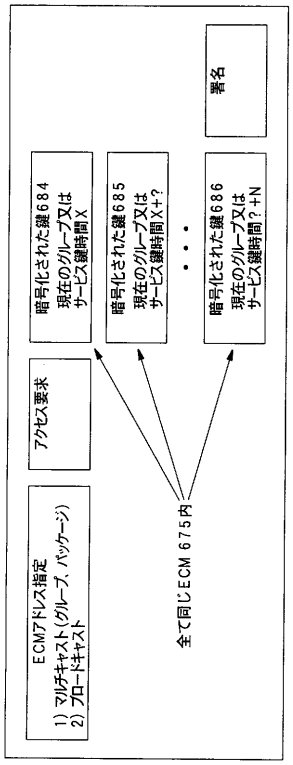

【図６Ｂ】



【図６Ｃ】

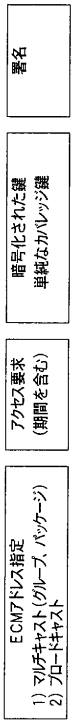



【図６Ｄ】

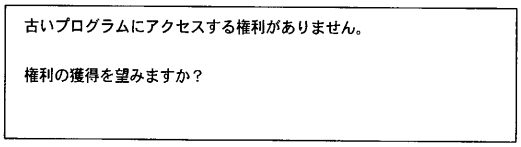



【図６Ｅ】

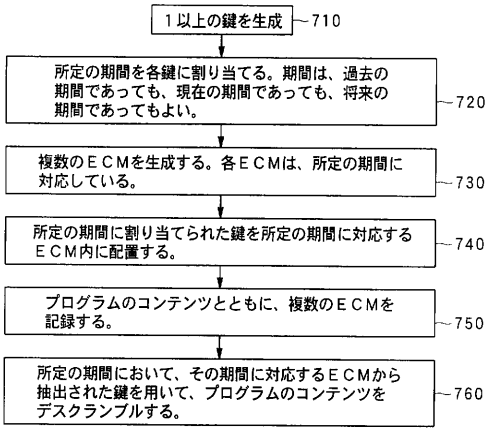

【図６Ｆ】



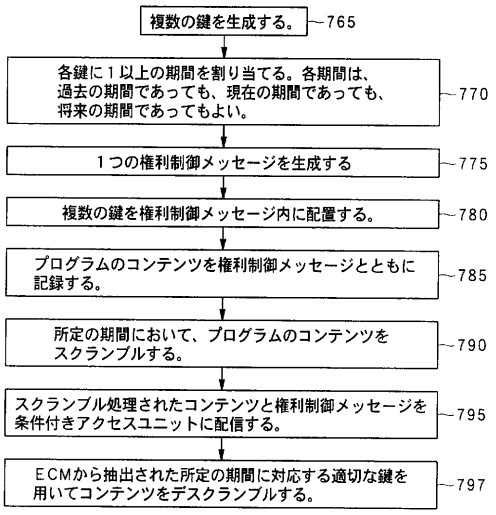
【図７】



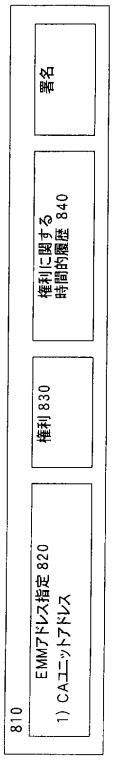

【図７Ａ】



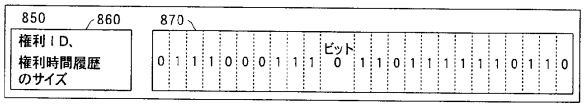

【図７Ｂ】



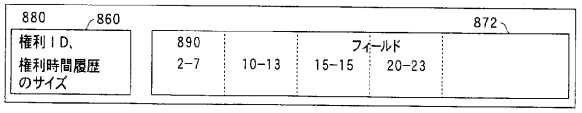

【図８Ａ】



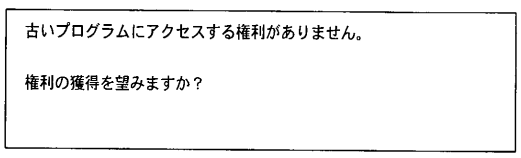

【図８Ｂ】



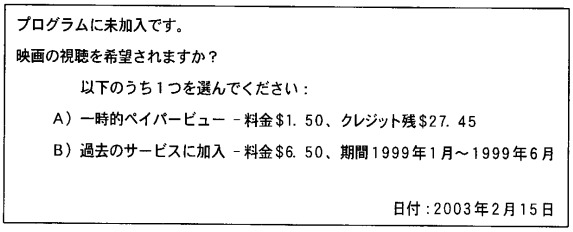

【図８Ｃ】



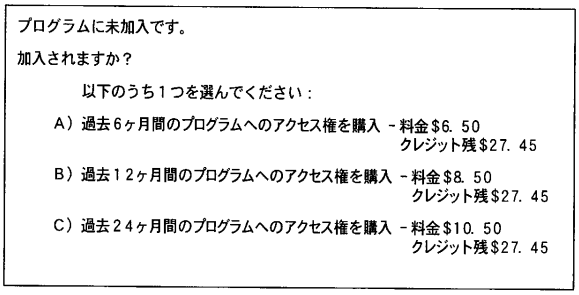

【図９Ａ】



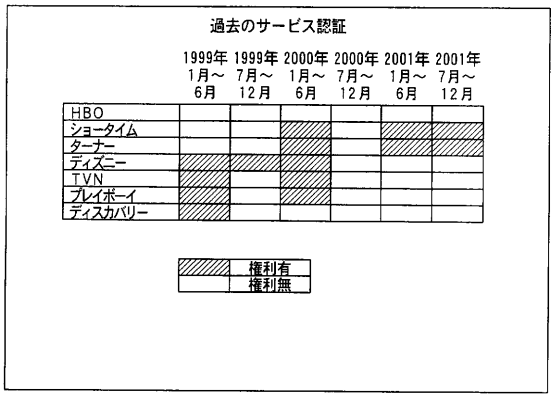

【図９Ｂ】



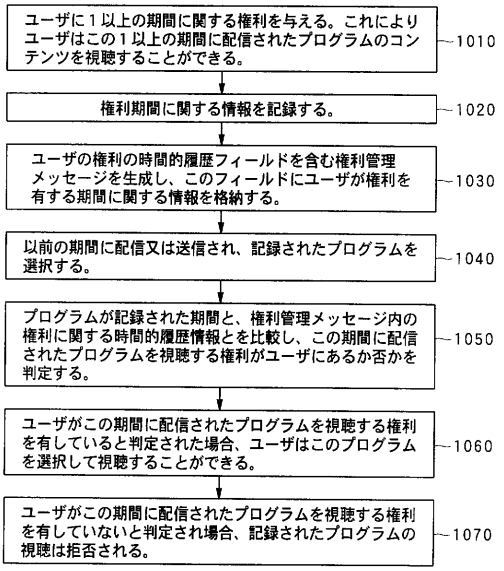
【図９Ｃ】



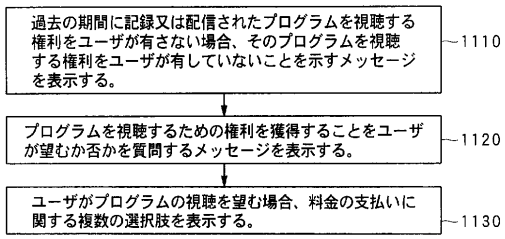

【図９Ｄ】




【図１０】




【図１１】



フロントページの続き

(51)Int.Cl. F I
*H04L 9/08 (2006.01)* H04N 7/167 Z
H04L 9/00 601B

(74)代理人 100158551
弁理士 山崎 貴明
(72)発明者 キャンデローレ, ブラント, エル
アメリカ合衆国 カリフォルニア州 92029－6502 エスコンディード クアイル グレン ウェイ 10124

審査官 青木 重徳

(56)参考文献 特開平09－034841（JP, A）
特開平07－074744（JP, A）
特開平04－150333（JP, A）
特開平03－220647（JP, A）
特開平10－191302（JP, A）
特開平09－093558（JP, A）
特開平8－125651（JP, A）
特表平10－512428（JP, A）
関一則, 榊原裕之, 岡田謙一, 松下温, “暗号を利用した新しいソフトウェア流通形態の提案”, 情報処理学会研究報告, 日本, 社団法人情報処理学会, 1993年 7月20日, Vol. 93, No. 64, p. 19－28
本池祥子, 清野正樹, “マルチメディアネットワーク技術 DVDを用いたコンテンツ流通サービス”, Matsushita Technical Journal, 日本, 松下電器産業株式会社, 1998年10月18日, 第44巻, 第5号, p. 25－33

(58)調査した分野(Int.Cl., DB名)
H04L 9／16
G06F 21／10
G06F 21／62
G09C 1／00
H04L 9／08
H04N 7／167