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

特許第4271863号
(P4271863)

(45)発行日　平成21年6月3日(2009.6.3)　(24)登録日　平成21年3月6日(2009.3.6)

(51)Int.Cl.		F I		
G11B 20/10	(2006.01)	G11B	20/10	H
G06F 21/24	(2006.01)	G11B	20/10	D
G09C 1/00	(2006.01)	G06F	12/14	550A
H04N 5/44	(2006.01)	G09C	1/00	660G
H04N 5/91	(2006.01)	H04N	5/44	Z

請求項の数 13　(全 13 頁)　最終頁に続く

(21)出願番号　特願2000-571104 (P2000-571104)
(86)(22)出願日　平成11年8月31日 (1999.8.31)
(65)公表番号　特表2002-525779 (P2002-525779A)
(43)公表日　平成14年8月13日 (2002.8.13)
(86)国際出願番号　PCT/US1999/019700
(87)国際公開番号　WO2000/013412
(87)国際公開日　平成12年3月9日 (2000.3.9)
審査請求日　平成18年8月16日 (2006.8.16)
(31)優先権主張番号　60/098,501
(32)優先日　平成10年8月31日 (1998.8.31)
(33)優先権主張国　米国(US)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　エフ－９２１００　ブローニュ　ビヤンクール，　ケ　アルフォンス　ル　ガロ，　４６番地
４６　Ｑｕａｉ　Ａ．　Ｌｅ　Ｇａｌｌｏ，　Ｆ－９２１００　Ｂｏｕｌｏｇｎｅ－Ｂｉｌｌａｎｃｏｕｒｔ，　Ｆｒａｎｃｅ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫

最終頁に続く

(54)【発明の名称】ホームネットワーク用のコピー保護システム

(57)【特許請求の範囲】

【請求項１】

スクランブルされたプログラムコンテンツ構成要素と暗号化された制御構成要素とを有するプログラムをコピーするための方法であって、

（ａ）記録装置内で前記プログラムを受け取るステップと、

（ｂ）前記暗号化された制御構成要素に、前記プログラムがコピーされたものであることを示すデータ項目を取り付けるステップと、

（ｃ）ネストされた制御構成要素を生成するように、前記暗号化された制御構成要素および前記データ項目を暗号化するステップと、

（ｄ）前記プログラムコンテンツ構成要素および前記ネストされた制御構成要素を記録するステップとを含んでいることを特徴とする方法。

【請求項２】

前記受け取るステップ、前記取り付けるステップ、および前記暗号化するステップが、前記記録装置に結合されたスマートカード中で実行されることを特徴とする、請求項１に記載の方法。

【請求項３】

前記暗号化された制御構成要素が、コピー制御情報と、前記スクランブルされたプログラムコンテンツ構成要素に関連付けられたスクランブル解除鍵とを含んでいることを特徴とする、請求項２に記載の方法。

【請求項４】

前記コピー制御情報が、コピー禁止（ｎｅｖｅｒ－ｃｏｐｙ）状態およびコピーワンス（ｃｏｐｙ－ｏｎｃｅ）状態のうちの１つを示すものであることを特徴とする、請求項３に記載の方法。

【請求項５】

前記暗号化された制御構成要素が、グローバル公開鍵を使用して暗号化されることを特徴とする、請求項４に記載の方法。

【請求項６】

前記ネストされた制御構成要素が、前記グローバル公開鍵を使用して暗号化されることを特徴とする、請求項５に記載の方法。

【請求項７】

前記グローバル公開鍵が、前記スマートカードに関連付けられるものであり、前記スマートカードがその中に格納された対応するプライベート鍵を有することを特徴とする、請求項６に記載の方法。

【請求項８】

前記暗号化された制御構成要素が、チャネル識別データ、イベント一致データ、日付および時刻スタンプデータ、ならびに価格データを含んでいる購入情報をさらに含んでいることを特徴とする、請求項７に記載の方法。

【請求項９】

制限されたプログラムのコピーへのアクセスを管理するための方法であって、前記方法が、

（ａ）処理装置内で前記制限されたプログラムを受け取るステップであって、前記制限されたプログラムが、スクランブルされたプログラムコンテンツ構成要素およびネストされた制御構成要素を有し、前記ネストされた制御構成要素が暗号化されるステップと、

（ｂ）暗号化された制御構成要素およびデータ項目を取得するために前記ネストされた制御構成要素を復号するステップであって、前記データ項目が、前記制限されたプログラムがコピーされたものであることを示すステップと、

（ｃ）スクランブル解除鍵およびコピー制御情報を取得するように前記暗号化された制御構成要素を復号するステップと、

（ｄ）前記コピーが有効であるかどうかを判定するように前記コピー制御情報と前記データ項目を比較するステップと、

（ｅ）前記コピーが有効であるという判定に応答して前記スクランブル解除鍵を使用し、前記プログラムコンテンツ構成要素をスクランブル解除するステップとを含んでいることを特徴とする方法。

【請求項１０】

前記暗号化された制御構成要素および前記ネストされた制御構成要素が、グローバル公開鍵を使用して暗号化されることを特徴とする、請求項９に記載の方法。

【請求項１１】

前記受け取るステップ、前記復号するステップ、前記比較するステップ、および前記スクランブル解除するステップが、前記処理装置に結合されたスマートカード中で実行され、前記復号ステップが、前記スマートカード中に格納され前記グローバル公開鍵に関連付けられたプライベート鍵を使用することを特徴とする、請求項１０に記載の方法。

【請求項１２】

前記暗号化された制御構成要素が、チャネル識別データ、イベント一致データ、日付および時刻スタンプデータ、および価格データを含んでいる購入情報をさらに含んでいることを特徴とする、請求項１１に記載の方法。

【請求項１３】

前記購入情報が前記プログラムの費用を含んでおり、前記方法がさらに、

（ａ）計算済みの現金準備額を決定するように、前記プログラムの費用を前記スマートカードに格納された現金準備額から差し引くステップと、

（ｂ）前記スマートカード中で、プラスの計算済み現金準備額を有することに応答して

、前記スクランブル解除鍵を使用して前記スクランブルされたプログラムコンテンツ構成要素をスクランブル解除するステップと、
（ｃ）前記スクランブル解除された伝送済みイベントを前記ビデオ処理装置に渡すステップとを含んでいることを特徴とする、請求項１２に記載の方法。
【発明の詳細な説明】
【０００１】
（発明の分野）
本発明は、プログラムやイベントなど、スクランブルされたデジタルストリームのコピーへのアクセスを管理するのに使用することができるシステムに関する。スクランブルされたデジタルストリームは、プログラムのコピーが合法的であると判定されるまで、スクランブル解除されない。
【０００２】
（発明の背景）
今日のＮＴＳＣテレビジョンは、様々なサービスプロバイダからの放送サービスを受信する。テレビジョン受像機の中には、放送、衛星、およびケーブルネットワークから、スクランブルされていない情報またはプログラムを受信できるものがある。従来から、スクランブルされたプログラムまたは暗号化されたプログラムを提供するケーブルネットワークまたはデジタル衛星システムには、通常、プログラムのスクランブルを解除するかまたは復号するために、別の独立型デバイス（例えばセットトップボックス）が必要であるとされている。これらのセットトップボックスは、必要な復号アルゴリズムおよび復号鍵を含んでいる取外し可能なスマートカードを利用することができる。
【０００３】
近い将来、デジタルテレビジョン（ＤＴＶ）およびデジタルセットトップボックス（ＳＴＢ）は、デジタルによる放送、ケーブル、および衛星のサービスを受信できるようになるであろう。したがって、デジタルビデオおよびオーディオコンテンツの保護は、情報技術（ＩＴ）産業、家庭用電子機器（ＣＥ）産業、および動画像（ＭＰ）産業にとって、重要な問題の１つとなっている。アナログサービスは、信号歪曲メカニズムを使用すればかなり保護することができる。しかし同じ解決方法がデジタルコンテンツには使用できないため、違法な複製に対する適切な保護策を備えた、デジタルオーディオおよびビデオコンテンツを送達するための新しい方法が必要である。
【０００４】
（発明の概要）
本発明は、一部は前述の問題を理解すること、および一部はこの問題の解決策を提供することである。デジタルコンテンツ（映画など）の無許可コピーの使用を防止する方法について説明する。ＭＰＥＧ－２トランスポートストリーム形式で提示されるコンテンツは、公開前に共通アルゴリズムを使用してスクランブルされる。スクランブル鍵および他のデータが、再生可能（ｒｅｎｅｗａｂｌｅ）セキュリティデバイス（例えば取外し可能なスマートカード）の公開鍵で暗号化することのできる、資格付与制御メッセージ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）（ＥＣＭ）に含まれる。他のデータは、コンテンツ（またはプログラム）の価格および（放送または事前記録済み）ソース、ならびにコピー制御情報（ＣＣＩ）を含んでいる。ホームネットワークに接続された記録デバイスは、プログラムを記録する前に、プログラムがスクランブルされているかどうかを第１にチェックする。スクランブルされたコンテンツが検出されると、レコーダは新しいコピーの各ＥＣＭに「コピーマーク」または「データ項目」を付け、これを公開鍵で暗号化する。データ項目とは、制限付きプログラム（実際にはオーディオ／ビデオ構成要素）がコピーされたことを示すものである。一般に、スクランブルされたコンテンツがコピーされるたびに、そのＥＣＭは再度暗号化される。このプロセスはＥＣＭネスティングと呼ばれ、表示ユニット（例えばデジタルＴＶ）に結合された再生可能セキュリティデバイスが、合法コピーと違法コピーとを見分けられるようにするものである。
【０００５】

本明細書で記載されるイベントまたはプログラムは、（１）映画、週１回の「テレビ」ショー、またはドキュメンタリーなどのオーディオ／ビジュアルデータ、（２）電子週刊誌、新聞、または天気予報などの文字データ、（３）コンピュータソフトウェア、（４）画像などのバイナリデータ、あるいは（５）ＨＴＭＬデータ（例えばＷｅｂページ）のうちの１つを含んでいる。サービスプロバイダは、例えば、従来の放送テレビジョンネットワーク、ケーブルネットワーク、デジタル衛星ネットワークなどのイベントまたはプログラムのプロバイダ、電子プログラムガイドプロバイダなどのイベント電子リストのプロバイダ、ならびに場合によってはインターネットサービスプロバイダを含んでいることができる。

【０００６】

本発明に従ったシステムは、公開鍵技術を利用することができる。典型的には、このようなシステムはすべてのサービスプロバイダに対して１つの（スマートカードに対応する）公開鍵を利用する。それぞれのスマートカードの中には、公開鍵によって暗号化されたメッセージを復号することができる、秘密のプライベート鍵が格納されている。サービスプロバイダは、公開鍵によって暗号化されたビットストリームで、サービスプロバイダ名、ならびにプログラムの名前、時間、および費用を含んでいることができる、条件付きアクセス（ＣＡ）資格付与メッセージ（すなわち資格付与制御メッセージまたはＥＣＭ）を送信する。このメッセージがスマートカードによって復号され、適切な情報がその中に格納される。一実施形態では、スマートカードは、銀行によって実行可能であった、またはサービスプロバイダからの一定額の購入クレジットを有することができる。ユーザは、制限額を超えない限り、サービスを購入することができる。何らかの適切な事前にプログラムされた時間に達すると、スマートカードはデバイス（例えばセットトップボックス）に自動的にＣＡセンターへの電話をかけさせる。銀行と提携したＣＡセンターは、保護チャネルを使用してスマートカードからの課金情報を受け取り、追加のクレジットを提供する。銀行はこの情報を転送し、適切なサービスプロバイダの貸方に記入する。

【０００７】

一般に、本発明は制限付き（またはスクランブルされた）放送または伝送プログラムのコピーへのアクセスを管理するための方法を定義する。本発明の一態様によれば、スクランブルされたプログラムコンテンツ構成要素を有するプログラム（例えばオーディオ／ビデオプログラム）および暗号化された制御構成要素を有するプログラム（例えばＥＣＭ）をコピーするための方法が定義される。この方法は、記録装置内でプログラムを受け取ること、および暗号化された制御構成要素にデータ項目を取り付けることを含んでいる。データ項目は、プログラムがコピーされたものであることを示すのに使用される。最後に、ネストされた制御構成要素を生成するために、暗号化された制御構成要素およびデータ項目が共に暗号化される。

【０００８】

本発明の他の態様によれば、制限されたプログラムのコピーへのアクセスを管理するための方法が、処理装置内で制限されたプログラムを受け取ることを含んでいる。暗号化された制御構成要素およびデータ項目を取得するために、ネストされた制御構成要素が復号される。次いで、スクランブル解除鍵およびコピー制御情報を得るために、暗号化された制御構成要素が復号される。コピーが許可されたもの（すなわち有効）であるかどうか、また許可されたものである場合はプログラムコンテンツ構成要素がスクランブル解除鍵を使用してスクランブル解除されるかどうかを判定するために、データ項目とコピー制御情報とが比較される。

【０００９】

本発明の他の態様によれば、制限されたプログラムの記録済みコピーへのアクセスを管理するための方法が、ビデオ処理装置に結合されたスマートカードを使用する。具体的に言えば、この方法は、現金準備額および資格付与をスマートカードに転送すること、制限されたプログラムの記録済みコピーをスマートカード中で受け取ること、スクランブル解除鍵、コピー制御情報、および購入情報を取得すること、前記コピーが許可されたものであ

るかどうかを判別するためにコピー制御情報とデータ項目とを比較すること、ならびに制限されたプログラムの費用が格納された現金準備額（ｃａｓｈ　ｒｅｓｅｒｖｅ）よりも少ないことを検証することを含んでいる。次に、格納された現金準備額から制限されたプログラムの費用が差し引かれ、オーディオ／ビデオ構成要素がスクランブル解除鍵を使用してスクランブル解除される。「費用モデル」の代わりに「時間モデル」を使用すること、すなわちプログラムを閲覧することが許可される時間を制御できることは、本発明の範囲内である。

【００１０】

本発明の上記態様および他の態様について、添付の図面に示された本発明の好ましい実施形態を参照しながら説明する。

【００１１】

（図面の詳細な説明）

本発明は、制限されたプログラム、例えばスクランブル（または暗号化）されたプログラムのコピーへのアクセスを管理するのに使用できる、条件付きアクセスシステムを提供する。条件付きアクセスシステムは、米国再生可能セキュリティ標準（Ｎａｔｉｏｎａｌ　Ｒｅｎｅｗａｂｌｅ　Ｓｅｃｕｒｉｔｙ　Ｓｔａｎｄａｒｄ）（ＮＲＳＳ）、ＥＩＡ－６７９、パートＡまたはパートＢに準拠したスマートカードなどの、再生可能セキュリティデバイスに組み込むことができる。条件付きアクセスシステムは、デジタルテレビジョン（ＤＴＶ）、セットトップボックス（ＳＴＢ）などで実施されると、ユーザがスクランブルされたプログラムの合法コピーのみを表示できるようにするものである。スマートカードの機能を、ＤＴＶまたはＳＴＢに埋め込むことができる。

【００１２】

認証局（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）（図示せず）は、以下で説明するように使用される、デジタル認証ならびに公開鍵とプライベート鍵のペアを発行する。認証局の役割がサービスプロバイダとデバイスの製造業者が共同で実行できるものであることは、本発明の範囲内である。課金センターを利用してユーザの勘定を管理することが可能であり、ユーザが追加のサービスを購入する準備を行った場合、およびこれらのサービスが消費または使用された場合、更新された情報が提供される。

【００１３】

放送業者は、（１）サービス、および（２）これらのサービスをユーザが購入できるようにする資格付与メッセージ（資格付与制御メッセージ）を送達する責任を負う。放送チャネルは、サービスおよびこれらのサービスへのアクセス情報を送達するためにのみ使用される。残りのすべてのトランザクションは、戻りチャネル（すなわちモデムおよび電話接続またはケーブルモデム）を使用して実行される。本条件付きアクセスシステムは、電子キャッシュカードローディングに基づくものとすることができる。ユーザは自分のカードに一定額の現金を（借方勘定または貸方勘定から）事前にローディングし、その後このカードを使用して以下のようにサービスを購入する。

【００１４】

戻りチャネル接続を使用してＣＡサーバと通信できない場合、カードに現金をローディングするには、ユーザがバックチャネルサポートを使用してデバイスにアクセスするか、または特定の場所（銀行、ＡＴＭ、ベンダの地域事務所）へ出向いてカードをローディングする必要がある。ＣＡオペレータはカード保有者の銀行またはユーザの銀行と同じ働きをし、課金センターは小売業者の銀行と同様の働きをする。ここで、再生可能セキュリティデバイス、例えば取外し可能スマートカードまたは条件付きアクセスモジュールなどにローディングされる固定額の「現金」を使用して、放送業者によって提供されるサービスまたは記録済みプログラムの表示に対する支払いを行うことができる。どちらの現金振替メカニズムが使用される場合でも、ユーザは貸方勘定または借方勘定からＣＡカードへの特定金額の振替を要求する。

【００１５】

ひとたびカードに現金がローディングされると、ユーザは放送業者が提供するサービスを

いくつでも購入することができるか、またはおそらく記録済みのプログラムの「閲覧権」を購入するのに使用することができる。サービスを購入するごとに、カードの使用可能金額からそのサービス価格分が差し引かれる。放送業者によって提供されるサービスは、ＰＰＶイベントおよびパッケージという２つのカテゴリに分類することができる。イベントとはプログラムガイド内にスロットが割り振られたＴＶプログラムのことであり、パッケージとは単なるイベントの集合体のことである。パッケージの例としては、（１）所与のシーズン中に行われるサッカーの全試合、（２）１つまたは複数のＡＴＳＣ仮想チャネルでの日曜深夜映画、（３）ＨＢＯなど特定の仮想チャネルへの加入が挙げられる。通常、すべてのイベントが、共通または共用の対称鍵アルゴリズムを使用してスクランブルされた、１つまたは複数のオーディオビジュアルストリームを有する。

【００１６】

イベントまたはパッケージを購入すると、スマートカードにレコードが格納され、その後これがＣＡベンダに転送される。格納された購入情報がひとたびＣＡデータベースに送られると、ＣＡベンダは提供されたサービスに対して放送業者に支払うことができる。

【００１７】

システムのセキュリティは、標準で幅広く受け入れられる公開鍵アルゴリズムおよび対称鍵アルゴリズムに基づくものとすることができる。例えば、好適なアルゴリズムには、公開鍵暗号化用のＲＳＡ、ならびに対称鍵スクランブル用のトリプルＤＥＳおよび／またはシングルＤＥＳが含まれる。これらのアルゴリズムを利用するシステム例には、システム全体用のグローバルＲＳＡの公開鍵／プライベート鍵のペア、Ｋｐｕｂ／Ｋｐｒｉがある。公開鍵はすべての放送業者によって共用され、対応するプライベート鍵は、ＣＡプロバイダによって消費者に配布される不正変更防止型ＮＲＳＳベースのスマートカード中に配置される。この公開鍵は、ヘッドエンド（ｈｅａｄ－ｅｎｄ）で生成されたＥＣＭを保護するのに使用される。スクランブルアルゴリズムがＤＥＳ以外の暗号であってもよいことは、本発明の範囲内である。

【００１８】

対称鍵暗号には、暗号化および復号の両方に同じ鍵を使用することが含まれる。公開鍵暗号の基礎は、公開鍵およびプライベート鍵という２つの関連する鍵を使用することにある。プライベート鍵は秘密鍵であり、公衆が使用可能な公開鍵からプライベート鍵を割り出すことは計算上不可能である。公開鍵を有する者はだれでもメッセージを暗号化できるが、これを復号できるのは、関連付けられた所定のプライベート鍵を有する人物またはデバイスのみである。

【００１９】

図１に示されるように、デジタルホームネットワーク１０とは、セットトップボックス１２、ＴＶ　１４、ＶＣＲ　１６、ＤＶＤプレーヤ１８、およびパーソナルコンピュータなどの汎用コンピュータデバイス（図示せず）を含んでいる、デジタルオーディオ／ビジュアル（Ａ／Ｖ）デバイスのクラスタのことである。いくつかのデジタルインターフェースを、ホームネットワーク内のデバイス相互接続に使用することができる。例えば、ＥＩＡ－７７５　ＤＴＶ　１３９４インターフェース仕様は、高性能シリアルバス向けＩＥＥＥ　１３９４標準に基づく、ＤＴＶへのベースバンドデジタルインターフェース向け仕様を定義する。ＩＥＥＥ　１３９４シリアルバスは、テレビジョン、ＶＣＲ、ＤＶＤプレーヤ、およびセットトップボックスなどのデジタルデバイスが、相互に通信できるようにするものである。「保証送達」用の非同期移送および「保証タイミング」用の任意選択等時性移送という、２種類の移送を提供する。（マルチメディアに適用するには等時性チャネルが必要である。）ＥＡＩ－７６１　拡張ＯＳＤ機能を備えたＤＴＶリモデュレータ仕様（ＤＴＶ　Ｒｅｍｏｄｕｌａｔｏｒ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　ｗｉｔｈ　Ｅｎｈａｎｃｅｄ　ＯＳＤ　Ｃａｐａｂｉｌｉｔｙ）およびＥＩＡ－７６２　ＤＴＶリモデュレータ仕様が、ＡＴＳＣ標準Ａ／５３　補遺Ｄに準拠した８　ＶＳＢおよび１６　ＶＳＢのリモデュレータをそれぞれ利用する一方向データパス用の最低限の仕様を定義する。

【００２０】

本発明は、デジタルホームネットワーク内でのコピー保護に関する新しい範例を定義する。この範例は、放送または事前記録のいずれかの可能性がある、デジタルコンテンツのコピーを可能にするものである。コピーは合法であるかどうかを確認してから表示される。

【００２１】

さらに、図１に示されるように、著作権で保護されているオリジナルコンテンツが、いくつかのソースからホームネットワーク１０に送達される。これは、衛星２０、地上２２、またはケーブル２４のシステムを介して伝送するか、またはデジタルテープ２６またはＤＶＤ２８に記録することができる。伝送されるかまたは媒体上に記録されたコンテンツは、「コピー禁止（ｎｅｖｅｒ－ｃｏｐｙ）」、「コピー１回（ｃｏｐｙ－ｏｎｃｅ）」、および「コピー自由（ｆｒｅｅ－ｃｏｐｙ）」として識別することができる。これら３つの状態は、コピー生成管理システム（ＣＧＭＳ）ビットを使用して表される。（ＣＧＭＳビットはＣＣＩの一部である。）クラスタ内のすべてのＡ／Ｖデバイスは、以下にまとめられた「再生制御（ｐｌａｙｂａｃｋ　ｃｏｎｔｒｏｌ）」、「レコード制御（ｒｅｃｏｒｄ　ｃｏｎｔｒｏｌ）」、および「１回生成制御（ｏｎｅ－ｇｅｎｅｒａｔｉｏｎ　ｃｏｎｔｒｏｌ）」の各規則に従うものとする。

【００２２】

【表１】

デバイスタイプ／コンテンツタイプ	コピー禁止	コピー１回	以後コピー禁止	コピー自由
プレーヤ	再生	再生	再生	再生
レコーダ	記録せず	記録後、新規コピー内でコンテンツタイプを「以後コピー禁止」に変更	記録せず	記録

【００２３】

コピー保護システムは、Ａ／Ｖデバイス間でのオーディオ／ビデオコンテンツの伝送を保護し、オーディオ／ビデオコンテンツの格納を保護しなければならない。本発明は、「コンテンツが表示されるまでそのスクランブルされた状態を維持する」ことにより、これら両方の問題の解決策を定義する。これにより、スクランブルされたコンテンツを記録することは可能であるが、コンテンツが合法でない場合（すなわちオリジナルまたは１回生成コピーでない場合）は閲覧を禁止する。これは、上記の表に定義された記録規則とは対照的である。

【００２４】

具体的に言えば、図１は、本発明が使用可能な、デジタルコンテンツ（例えば映画）を受け取ることができる様々なデジタルオーディオ／ビデオデバイスからなる、典型的なホームネットワークを示す図である。デジタルコンテンツは、ＭＰＥＧ－２トランスポートストリーム（ＴＳ）形式で符号化され、資格付与制御メッセージ（ＥＣＭ）と共に放送される。ＥＣＭ（図２ａを参照）は、制御語（すなわちスクランブル解除鍵）およびアクセス条件の暗号である。

【００２５】

ＳＴＢまたはＤＴＶは、スクランブルされたＡ／Ｖストリームをソース（放送のヘッドエンドまたはプレーヤ）から受け取り、これを直接スマートカードに伝送する。スマートカード（ＳＣ）３０がスマートカードリーダ（図示せず）に挿入または結合され、内部バスがＳＴＢまたはＤＴＶとスマートカードとを相互接続して、それらの間のデータ転送を可能にする。このようなスマートカードには、例えば米国再生可能セキュリティ標準（ＮＲＳＳ）パートＡに準拠したＩＳＯ７８１６カード、またはＮＲＳＳパートＢに準拠したＰＣＭＣＩＡカードが含まれる。上記で述べたように、本発明の概念は、本質的にスマートカードに限定されたものではなく、どんな再生可能セキュリティデバイスでも使用するこ

とができる。概念上は、スマートカードがスマートカードリーダに結合されると、スマートカードの機能はデジタルテレビジョンの機能の一部とみなされるため、スマートカードの物理的なカード本体によって作り出される「境界」は除去される。

【００２６】

スマートカードは、コンテンツが合法であるかどうかをチェックし、ＤＥＳ鍵を回復し、資格付与をチェックした後ストリームのスクランブルを解除する。（映画が開始される直前に、画面表示メッセージ（ＯＳＤ）が消費者に対して購入申し込みを開始するように指示する。）加入資格付与はカード中に格納されるが、イベント資格付与はイベントと共に伝送され、購入申し込みを生成するのに使用される。）

【００２７】

オリジナルとコピーを区別する方法と、ユーザがコピーを閲覧できるようにする前にコピーが合法であるかどうかを検証する方法という、固有であるが関連する２つの方法について以下に定義する。どちらの方法でも、スクランブルされたプログラムが記録される場合、記録デバイス（例えばＤＶＣＲまたはＤＶＤレコーダ）が第１に実行することは、プログラムがスクランブルされているかどうかを検証することである。これは、パケットヘッダ内のパケット識別（ＰＩＤ）によって識別される、ＥＣＭのチェックによって達成することができる。一代替方法は、移送パケットヘッダ内の移送スクランブル制御（Ｔｒａｎｓｐｏｒｔ　Ｓｃｒａｍｂｌｉｎｇ　Ｃｏｎｔｒｏｌ）（ＴＳＣ）ビットをチェックすることであろう。他の方法は、プログラムが以下に記載するようにスクランブルされているかどうかを確かめることであろう。ＭＰＥＧビデオ構文には、ビットストリーム内の同期化ポイントを示す、「開始コード」と呼ばれるバイト位置合わせされた３２ビットのフィールドが含まれる。例えば、ＭＰＥＧビデオビットストリーム内の各フレームの最初には、「ピクチャ開始コード」（０×００　００　０１　００）がある。これらのフレームは、毎秒６０、５０、３０、または２４フレーム（ｆｐｓ）を発生させることができる。したがって、ビットストリーム内のピクチャ開始コードを調べるのは単純なテストであろう。ピクチャ開始コードの１秒当たりの速さが、可能な速度のうちの１つに近い場合、そのビットストリームは暗号化されていないと想定するのが妥当である。

【００２８】

本発明の一実施形態では、コンテンツがスクランブルされていると、レコーダはグローバル公開鍵を使用してＥＣＭを暗号化する。暗号化を実行する前に、レコーダは各ＥＣＭにコピーを示すものとしてマーク（またはデータ項目）を取り付ける（図２ｂを参照）。一般に、スクランブルされた映画がコピーされるたびにそのＥＣＭは再度暗号化され、このプロセスが「ネスティング」と呼ばれる。これによりスマートカードは、オリジナルの映画が何回コピーされたものであるかを判定することができる。以下の例（ここで、ＧＰＫはグローバル公開鍵、Ｅは暗号化プロセス、ＣＷは制御語（スクランブル解除用の鍵）であり、ＥＣＭはＣＷ、ＣＣＩ、コンテンツのソース、および他のデータを含んでいる）では、違法コピーを検出してその表示を防止する。

【００２９】

映画のＥＣＭが、E_{GPK}（ＣＷ，ｎｅｖｅｒ－ｃｏｐｙ）の形式を有すると想定してみる。レコーダはこのＥＣＭを受け取ると、E_{GPK}［E_{GPK}（ＣＷ，ｎｅｖｅｒ－ｃｏｐｙ），ｃｏｐｙ－ｍａｒｋ）］の形式に変換する。このネストされたＥＣＭの付いた映画が、記録プロセスの出力となる。ユーザがこれを閲覧しようとすると、スマートカードはこれが「ｎｅｖｅｒ－ｃｏｐｙ（コピー禁止）」コンテンツのコピーであることを検出し、表示を禁止する。この映画が「ｃｏｐｙ－ｏｎｃｅ（コピー１回）」コンテンツである場合、ＥＣＭはコピー内でE_{GPK}［E_{GPK}（ＣＷ，ｃｏｐｙ－ｏｎｃｅ），ｃｏｐｙ－ｍａｒｋ）］の形式となる。これは合法コピーを示すものであり、スマートカードは閲覧を許可する。ただし、コピーのコピーが作成されると、ＥＣＭは例えば［E_{GPK}{E_{GPK}［E_{GPK}（ＣＷ，ｃｏｐｙ－ｏｎｃｅ），ｃｏｐｙ－ｍａｒｋ）］，ｃｏｐｙ－ｍａｒｋ}］という２層のネスティングを有することとなり、コピーは違法であることが検出される。

【００３０】
コピー保護システムのセキュリティを上げるための一方法は、記録目的のローカル公開鍵を使用することである。これには、固有の公開鍵／プライベート鍵のペアを備えたスマートカードが必要である。映画をコピーするために、スマートカードがＶＣＲに結合され公開鍵を提供する。次いで公開鍵は、対応する固有のプライベート鍵でのみ再生できるコピーを作成するために、ＥＣＭの暗号化に使用される。
【００３１】
システムのセキュリティを上げる他のオプションは、ＥＣＭのネスティングプロセス中に、ｃｏｐｙ－ｍａｒｋ（マークをコピー）と共に固有のレコーダＩＤを取り付けることである。この追加情報がコピーとレコーダとの間の結合を作成する。さらに、レコーダおよびスマートカードの双方が、同じレコーダＩＤを有する。したがって、コピーが閲覧できるのは、レコーダＩＤを有するスマートカードを使用した場合のみとなる。
【００３２】
著作権で保護された（および暗号化された）あらゆるデジタルコンテンツは、どんなレコーダにもコピーできるものとする。作成されたコピーが合法であれば、確立された支払いシステムの規則に従って閲覧することができる。例えば、ＤＴＶがネストされたＥＣＭのないスクランブルされたプログラムを受け取ると、次いでＤＴＶはこのプログラムを、スクランブルされたオリジナルのプログラムでありコピーでないものとして取り扱う。すなわち、ＤＴＶはプログラムを閲覧可能にするのである。ただし、ユーザが「オリジナルプログラム」のコピーを作成したい場合は、次いでＥＣＭおよびデータ項目が本発明に従って共に暗号化される。
【００３３】
本発明の代替実施形態では、ＣＧＭＳビットおよびアクセス権ならびに制御語を含んでいるようにＥＣＭが拡張される。この拡張ＥＣＭ（ＸＥＣＭ）は、著作権が保護されたコンテンツ（例えば映画）が記録されるたびに、コピーとオリジナルを区別するために一方向の非可逆変換（例えばハッシング）を介して修正される。セットＸからセットＹまでの関数ｆは一方向関数と呼ばれ、本質的にすべてｙ∈Ｉｍ（ｆ）の場合を除き、すべてｘ∈Ｘの場合にｆ（ｘ）が簡単に計算できるのであれば、計算上はｆ（ｘ）＝ｙであるようなどんなｘ∈Ｘも見つけることができない。
【００３４】
スマートカードはＸＥＣＭを受け取ると、システムのタイプに応じてこれを処理する。条件付きアクセス（ＣＡ）システムおよびコピー保護（ＣＰ）システムという、機能的に異なる２つのシステムをこのアーキテクチャに入れることができる。
【００３５】
（ｉ）ＣＡシステム：スマートカードは、ＣＡシステムの構成要素である。閲覧が許可される前に、スマートカードはＸＥＣＭが何回修正されるかをチェックして、ＣＡシステムの事前定義された規則に従って応答する。
【００３６】
（ｉｉ）ＣＰシステム：スマートカードは、ＣＰシステムの構成要素である。スマートカードの機能は制限されている。コンテンツの合法性をチェックし、違法コピーの閲覧を防止する。
【００３７】
ＸＥＣＭの処理について、以下の例を使用し図２ｃおよび３を参照しながら説明する。映画がＤＶＣＲでコピーされるものと想定してみる。このＸＥＣＭ構文は、$ＸＥＣＭ＝Ｅ_{Ｋ}$（ＣＷ，Ｄ／Ｔ，ｃｏｎｔｅｎｔ　ｔｙｐｅ，$ｘ_{0}$），$ｘ_{ｉ}$となるように定義され、この式で$ｘ_{0}＝ｘ_{1}$、ｉ＞０の場合$ｘ_{ｉ＋１}＝ｆ（ｘ_{ｉ}）$、Ｅは暗号化プロセス、Ｋは暗号化鍵、ＣＷは制御語、Ｄ／Ｔは日付および時刻スタンプ、$ｘ_{0}$は乱数、ならびにｆは一方向関数である。
【００３８】
（ａ）コンテンツタイプが「ｎｅｖｅｒ－ｃｏｐｙ」の場合、

レコーダ入力： E_K（ＣＷ，Ｄ／Ｔ，″ｎｅｖｅｒ－ｃｏｐｙ″，x_0），x_1
レコーダ出力： E_K（ＣＷ，Ｄ／Ｔ，″ｎｅｖｅｒ－ｃｏｐｙ″，x_0），x_2である。

【００３９】
ユーザがコピーを閲覧しようとすると、カードはＸＥＣＭを復号した後、x_0とx_2を比較する。これらが等しくないと表示することはできない。

【００４０】
（ｂ）コンテンツタイプが「ｃｏｐｙ－ｏｎｃｅ」の場合、
レコーダ入力： E_K（ＣＷ，Ｄ／Ｔ，″ｃｏｐｙ－ｏｎｃｅ″，x_0），x_1
レコーダ出力： E_K（ＣＷ，Ｄ／Ｔ，″ｃｏｐｙ－ｏｎｃｅ″，x_0），x_2
である。

【００４１】
このとき、x_0とx_2の比較によって、コピーが合法であることが明らかになる。ただし、第１回生成コピーがレコーダへの入力である場合、$f(f(x_0))=x_3$であることから、出力は違法である。ＸＥＣＭが、すでに実行された修正の回数を考慮せずに修正されることに留意されたい。

【００４２】
ＣＡシステムでは、Ｄ／Ｔスタンプフィールドが、著作権を侵害されたレコーダによって作成されたコピーを検出することができる。カードは修正されたことのない「古い」ＸＥＣＭを検出すると、これを著作権侵害コピーであるものとみなす。ＣＰシステムでは、Ｄ／Ｔスタンプを使用して、事前記録された媒体およびこれから作成された許可コピーに、制限付きの寿命を割り当てることができる。

【００４３】
「ＸＥＣＭ修正」スキームの非常に重要な特徴は、コンテンツ分配者（放送業者および出版業者）に対し、ＸＥＣＭを作成するために自分たちの暗号化アルゴリズムを選択することにおける完全な自由を与えることである。したがって、コピー保護システムはＣＡシステムの延長として構築される一方で、「減結合」される。唯一の要件は、ＸＥＣＭに共通構造を使用することである。

【００４４】
以下で説明するように、コンテンツソースから発信されるＸＥＣＭにはプライベートおよび必須という２つのセクションがある。プライベートセクションには、ＣＡシステムおよびＣＰシステムのオペレータによって個人的に定義されるフィールドが含まれる。必須セクションには、すべてのＸＥＣＭに含まれなければならない３つのフィールドが含まれる。

【００４５】
ＸＥＣＭのプライベートセクションにあるフィールドは、ＸＥＣＭ＿ｉｄ（拡張資格付与制御メッセージの固有識別子）、ＸＥＣＭ＿ｌｅｎｇｔｈ（ＸＥＣＭ内のバイト数を指定する８ビットフィールド）、ｆｏｒｍａｔ＿ｉｄｅｎｔｉｆｉｅｒ（ｐｒｏｖｉｄｅｒ＿ｉｎｄｅｘフィールドに値を割り当てる登録権限を識別する３２ビットフィールド）、ｐｒｏｖｉｄｅｒ＿ｉｎｄｅｘ（コンテンツプロバイダを識別する１６ビットフィールド）、ｐｒｏｇｒａｍ＿ｅｖｅｎｔ＿ｉｄ（特定のＴＶプログラムまたはイベントを識別する２４ビットフィールド）、ｔｒａｎｓｐｏｒｔ＿ｓｔｒｅａｍ＿ｉｄ（イベントが搬送されているトランスポートストリームを識別する１６ビットフィールド）、ｓｏｕｒｃｅ＿ｉｄ（イベントが伝送されている特定サービスを一意に識別する１６ビットフィールド）、ｅｖｅｎｔ＿ｉｄ（このトランスポートストリームの所与のサービス内で特定イベントを一意に識別する１４ビットフィールド）、ｓｔａｒｔ＿ｔｉｍｅ（イベント開始時間を示す３２ビットフィールド）、ｌｅｎｇｔｈ＿ｉｎ＿ｓｅｃｏｎｄｓ（イベントの長さを示す２０ビットフィールド）、ｔｉｔｌｅ＿ｓｅｇｍｅｎｔ（このメッセージが記述するイベントに関する英語タイトルの最初の１０文字）、ｅｖｅｎｔ＿ｐｒｉｃｅ（イベントの費用を示すＢＣＤフィールド）、ｓｃｒａｍｂｌｉｎｇ＿ｋｅｙ（考察中のイベントに

関するビデオ信号およびオーディオ信号をスクランブル解除するのに必要な６４ビット鍵）、ｄｅｓｃｒｉｐｔｏｒｓ＿ｌｅｎｇｔｈ（記述子に続く記述子リストの全長）を含んでいる。ＸＥＣＭの必須セクションは、ＣＣＩ－コピー制御情報（ＣＧＭＳビット、ＡＰＳトリガビット、およびデジタルソースビット）、ｃｏｐｙ＿ｉｎｄｉｃａｔｏｒ＿ｉｎｉｔｉａｌ＿ｖａｌｕｅ（ランダムビットシーケンス）、およびｃｏｐｙ＿ｉｎｄｉｃａｔｏｒ（ｃｏｐｙ＿ｉｎｄｉｃａｔｏｒ＿ｉｎｉｔｉａｌ＿ｖａｌｕｅに等しいビットシーケンス）を含んでいる。

【００４６】

ＤＴＶ　１４は、閲覧用デジタルコンテンツ４０の最終宛先である。スクランブルされたＡ／Ｖストリームをソース（放送／ケーブルのヘッドエンド、衛星、ケーブルＳＴＢ、ＤＢＳ　ＳＴＢまたは再生デバイス）から受け取り、これを直接スマートカード３０に伝送する。スマートカード３０は、コンテンツが合法であるかどうかをチェックする。例えば、放送ＰＰＶ映画を受け取ると、ＯＳＤは映画が開始される前に購入申し込みを開始するように消費者に指示する。映画が購入されると、カード中にレコードが格納される。次いでカードはスクランブル鍵を回復し、ストリームをスクランブル解除する。ＸＥＣＭ内に含まれるイベント（価格、開始時間、長さなど）に関する情報は、購入申し込みを生成するのに使用される。最後にＤＴＶ　１４は、受け取ったものと同じストリームを出力する。

【００４７】

映画が記録される予定であれば、ＤＶＣＲはＸＥＣＭを検出および修正する。さらに、移送パケットヘッダ内の移送スクランブル制御（ＴＳＣ）ビットをチェックして、コンテンツがスクランブルされているかどうかを調べることができる。コンテンツがスクランブルされていない場合は、現状のままコピーされる。一般に、スクランブルされた映画がコピーされるごとに、そのＸＥＣＭが再度修正される。これにより、スマートカードは、オリジナルの映画がこれまでに何回コピーされたかを判別することができる。任意選択で、レコーダに挿入されたスマートカードにＸＥＣＭ修正機能を割り当てることができる。この場合、レコーダはスマートカードリーダを備えている必要がある。

【００４８】

以上、本発明について、その様々な実施形態に関して詳細に説明してきたが、前述の内容を読んで理解すれば、説明した実施形態に様々な変更が生じること、ならびにこのような変更が添付の特許請求の範囲内に含まれるように意図されるものであることが、当業者であれば明らかとなろう。

【図面の簡単な説明】

【図１】　スクランブルされたコンテンツを複数のソースから受け取ることができる様々なデジタルデバイスからなる、ホームネットワークを示す構成図である。

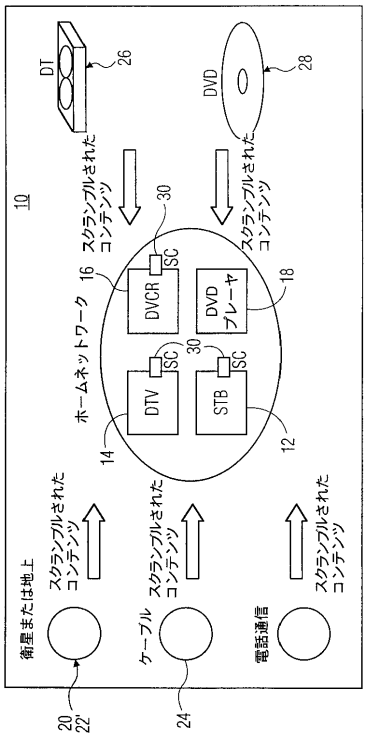
【図２ａ】　典型的な資格付与制御メッセージ（ＥＣＭ）を定義する図である。

【図２ｂ】　本発明の一実施形態によるネストされたＥＣＭを定義する図である。

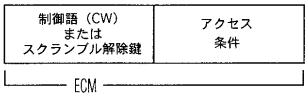
【図２ｃ】　本発明の他の実施形態による拡張ＥＣＭを定義する図である。

【図３】　本発明を使用する典型的なホームネットワークを示す構成図である。

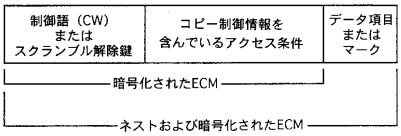
【図１】



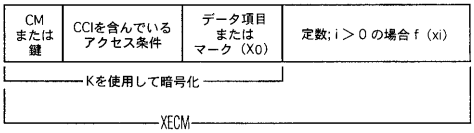
【図２ａ】



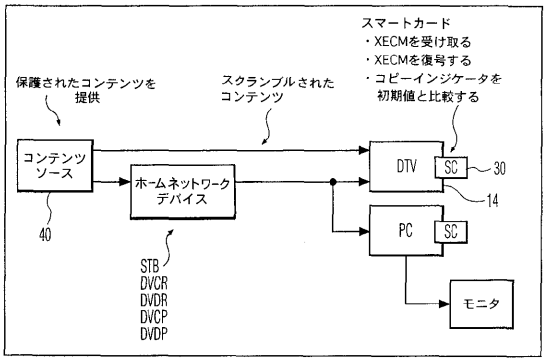
【図２ｂ】



【図２ｃ】



【図３】



フロントページの続き

(51)Int.Cl.			FI		
H04N	***5/92***	***(2006.01)***	H04N	5/91	P
H04N	***7/167***	***(2006.01)***	H04N	5/92	H
			H04N	7/167	Z

(72)発明者　アーメット　マーシット　エスキシオグル
アメリカ合衆国　４６２５０　インディアナ州　インディアナポリス　レイクショアー　トレイル　８２３５　アパートメント　１２５
(72)発明者　ウィリアム　ウェズリィ　ビヤーズ　ジュニア
アメリカ合衆国　４６０３３－９０４６　インディアナ州　カーメル　アロー　ウッド　ドライブ　１０７５

審査官　高野　美帆子

(56)参考文献　特開平０９－０９３５６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)

G11B 20/10
G06F 21/24
G09C 1/00
H04N 5/44
H04N 5/91
H04N 5/92
H04N 7/167