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

特許第4520148号
(P4520148)

(45)発行日　平成22年8月4日(2010.8.4)　(24)登録日　平成22年5月28日(2010.5.28)

(51)Int.Cl.　F I
H04N 7/167 (2006.01)　H04N 7/167 Z

請求項の数 30　(全 19 頁)

(21)出願番号	特願2003-541273(P2003-541273)	(73)特許権者	591034154
(86)(22)出願日	平成14年10月24日(2002.10.24)		フランス・テレコム
(65)公表番号	特表2005-507619(P2005-507619A)		フランス・７５０１５・パリ・プラス・ダルレ・６
(43)公表日	平成17年3月17日(2005.3.17)	(74)代理人	100064908
(86)国際出願番号	PCT/FR2002/003655		弁理士　志賀　正武
(87)国際公開番号	WO2003/039153	(74)代理人	100089037
(87)国際公開日	平成15年5月8日(2003.5.8)		弁理士　渡邊　隆
審査請求日	平成16年6月15日(2004.6.15)	(74)代理人	100108453
審判番号	不服2007-18419(P2007-18419/J1)		弁理士　村山　靖彦
審判請求日	平成19年7月2日(2007.7.2)	(74)代理人	100110364
(31)優先権主張番号	01 13963		弁理士　実広　信哉
(32)優先日	平成13年10月29日(2001.10.29)		
(33)優先権主張国	フランス(FR)		

最終頁に続く

(54)【発明の名称】データ交換ネットワークにおけるスクランブルされたデジタルデータのためのアクセスコントロールを伴う送信方法およびシステム

(57)【特許請求の範囲】

【請求項１】

データ交換ネットワーク（２）に接続された少なくとも一つの端末（４）にアクセスコントロールを伴ってデジタルデータを送信する方法であって、

第１のスクランブルステップと、第２のブロードキャストステップと、第３のデスクランブルステップとを備え、

前記第１のスクランブルステップは、

コントロールワードＣＷを用いて、送信されるべきデジタルデータをスクランブルし、

前記データ交換ネットワーク（２）における少なくとも一つの端末（４）に特有なデジタルデータ及び第１のランダムデジタルデータＡＬＥＡ１の関数として計算された前記端末（４）のそれぞれについてのデジタルシーケンスＳを発生し、

前記コントロールワードＣＷおよび前記デジタルシーケンスＳの関数として前記端末（４）についての少なくとも一つの特定のデジタルキーＫを計算し、

前記対応する特定のデジタルキーＫを前記端末（４）に送信する

ことを備え、

第２のブロードキャストステップは、

スクランブルされたデジタルデータおよび前記第１のランダムデジタルデータＡＬＥＡ１を前記端末（４）に送信し、

第３のデスクランブルステップは、

前記データ交換ネットワーク（２）における少なくとも一つの端末（４）に特有なデジ

タルデータ及び前記第１のランダムデジタルデータＡＬＥＡ１を用いて前記デジタルシーケンスＳを発生し、
前記特定のデジタルキーＫおよび前記デジタルシーケンスＳから前記コントロールワードＣＷを解読し、
前記解読されたコントロールワードＣＷを用いて、前記送信されたデジタルデータをデスクランブルする
ことを備えた方法。
【請求項２】
前記データ交換ネットワーク（２）を通じて提供されるサービスへのアクセス権を既に予約している全てのユーザに予約番号を割り当てるステップと、
前記データ交換ネットワーク（２）における少なくとも一つの端末（４）に特有のデジタルデータ及び前記予約番号と引き替えに前記ユーザに前記特定のデジタルキーＫを送信するステップと
をさらに備えたことを特徴とする請求項１記載の方法。
【請求項３】
前記デジタルデータは、無線チャンネル、有線、デジタルケーブル、デジタルデータの記録媒体の何れかによって伝送されることを特徴とする請求項２記載の方法。
【請求項４】
前記データ交換ネットワーク（２）はＩＰネットワークであることを特徴とする請求項２記載の方法。
【請求項５】
前記データ交換ネットワーク（２）における少なくとも一つの端末（４）に特有のデジタルデータは、前記データ交換ネットワーク（２）における前記端末（４）のアドレスであることを特徴とする請求項４記載の方法。
【請求項６】
前記コントロールワードＣＷはランダムに発生されることを特徴とする請求項１乃至５の何れか１項記載の方法。
【請求項７】
前記データ交換ネットワーク（２）における前記端末（４）のアドレスおよび前記予約番号は、ＴＣＰ／ＩＰプロトコルを用いてプログラム供給者に端末ユーザによって送信されることを特徴とする請求項２記載の方法。
【請求項８】
前記デジタルデータはオーディオビジュアルプログラムであることを特徴とする請求項１乃至７の何れか１項記載の方法。
【請求項９】
スクランブルされたデジタルデータと共に、前記コントロールワードＣＷと組み合わせて追加的なスクランブルキーとして使用される第２のランダムデジタルデータＡＬＥＡ２を送信するステップを更に備えたことを特徴とする請求項１乃至８の何れか１項記載の方法。
【請求項１０】
前記データ交換ネットワーク（２）を通じて提供される各サービスにマルチキャストアドレスを割り当て、且つ、前記マルチキャストアドレス、前記対応する第１のランダムデジタルデータＡＬＥＡ１、および前記コントロールワードＣＷをサービステーブルに格納するステップを備えることを特徴とする請求項４記載の方法。
【請求項１１】
前記第１のランダムデジタルデータＡＬＥＡ１および前記コントロールワードＣＷのペアは、定期的に変更されることを特徴とする請求項１０記載の方法。
【請求項１２】
前記ブロードキャストステップにおいて送信されるスクランブルされたデジタルデータは、複数のエレメンタリオーディオ、ベーシックビデオ、およびエンハンスドビデオを備

えたことを特徴とする請求項１０記載の方法。
【請求項１３】
前記スクランブルステップは、サブステップとして、
ＩＰ／ＵＤＰデータグラムのヘッダーにある送信先ポート及びアドレスの関数としてスクランブルされる前記ＩＰ／ＵＤＰデータグラムをフィルタするステップと、
前記サービスに関連する前記コントロールワードを用いて、フィルタされた各ＩＰ／ＵＤＰデータグラムをスクランブルするステップと、
前記スクランブルされたＩＰ／ＵＤＰデータグラムを含むコンテンツおよびデスクランブラに与えられる送信先ポート番号、送信先アドレスとしてサービスのマルチキャストアドレスを備えるＩＰヘッダーを用いて第２のＩＰ／ＵＤＰデータグラムを構築するステップと
を備えたことを特徴とする請求項１２記載の方法。
【請求項１４】
前記ブロードキャストステップは、
前記ＩＰネットワークを通じて前記第２のＩＰ／ＵＤＰデータグラムを送信するステップからなることを特徴とする請求項１３記載の方法。
【請求項１５】
前記第２のＩＰ／ＵＤＰデータグラムは、ＵＤＰトランスポートプロトコルを使用することを特徴とする請求項１４記載の方法。
【請求項１６】
前記デスクランブルステップは、サブステップとして、
受信された全てのＩＰ／ＵＤＰデータグラムを分析し、もしあるＩＰ／ＵＤＰデータグラムが前記選択されたサービスに対応するポート及び前記マルチキャストアドレスを備えていれば、
前記コンテンツをデスクランブルするステップ
を備えたことを特徴とする請求項１３記載の方法。
【請求項１７】
前記エレメンタリオーディオ、ベーシックビデオ及びエンハンスドビデオは、異なる送信先ポートを用いることにより前記データ交換ネットワーク（２）上に別々にブロードキャストされることを特徴とする請求項１６記載の方法。
【請求項１８】
前記エレメンタリオーディオ、ベーシックビデオ及びエンハンスドビデオは、所定のポート上に一つのサービスのみを送信するために多重化されることを特徴とする請求項１６記載の方法。
【請求項１９】
前記エレメンタリオーディオ及びベーシックビデオのみスクランブルされることを特徴とする請求項１７記載の方法。
【請求項２０】
データ交換ネットワーク（２）に接続された少なくとも一つの端末（４）に対する、コントロールワードＣＷによってスクランブルされたデジタルデータのアクセスコントロールを伴う送信システムであって、
予約ゲートウェイ（１４）と、
送信されるべきデータをスクランブルするように設計されたプラットフォーム（１６）と、
スクランブルされたデータをブロードキャストするように設計されたサーバー（６）と、
を備え、
前記予約ゲートウェイ（１４）は、
前記データ交換ネットワーク（２）における少なくとも一つの端末（４）に特有のデジタルデータ及び第１のランダムデジタルデータＡＬＥＡ１の関数としてデジタルシーケン

スＳを発生する手段と、
前記コントロールワードＣＷ及び前記デジタルシーケンスＳの関数として、前記端末（４）についての特定のデジタルキーＫを計算する手段と、
を備えたことを特徴とするシステム。
【請求項２１】
前記データ交換ネットワーク（２）における少なくとも一つの端末（４）に特有なデジタルデータは、このデータ交換ネットワーク（２）における前記端末（４）のアドレスからなることを特徴とする請求項２０記載のシステム。
【請求項２２】
前記予約ゲートウェイは、
前記データ交換ネットワーク（２）を通じて提供されるサービスに対するアクセス権を予め予約した任意のユーザに予約番号を割り当てる手段と、
前記データ交換ネットワーク（２）における少なくとも一つの端末（４）に特有のデジタルデータ及び前記予約番号と引き替えにこのユーザに前記特定のデジタルキーＫを送信する手段と、
を備えたことを特徴とする請求項２１記載のシステム。
【請求項２３】
前記予約ゲートウェイ（１４）は、また、特定のデジタルキーＫにそれぞれ対応する複数の予約番号を格納するように設計されたデータベースを備えたことを特徴とする請求項２２記載のシステム。
【請求項２４】
前記データ交換ネットワーク（２）はＩＰネットワークであることを特徴とする請求項２１乃至２３の何れか１項記載のシステム。
【請求項２５】
前記予約ゲートウェイ（１４）は、前記データ交換ネットワーク（２）を通じて提供される各サービスにマルチキャストアドレスを割り当てる手段と、対応するマルチキャストアドレス、第１のランダムデジタルデータＡＬＥＡ１、および前記コントロールワードＣＷを関連づけるサービステーブルを格納するメモリとを備えたことを特徴とする請求項２４記載のシステム。
【請求項２６】
前記コントロールワードＣＷは、ランダムに発生されることを特徴とする請求項２５記載のシステム。
【請求項２７】
前記デジタルデータは、オーディオビジュアルプログラムであることを特徴とする請求項２１乃至２６の何れか１項記載のシステム。
【請求項２８】
前記スクランブルプラットフォーム（１６）は、また、
ＩＰ／ＵＤＰデータグラムのヘッダーに存在する送信先ポート及びアドレスの関数としてスクランブルされるＩＰ／ＵＤＰデータグラムをフィルタする手段と、
前記サービスに関連づけられた前記コントロールワードＣＷを用いて、フィルタされた各ＩＰ／ＵＤＰデータグラムをスクランブルする手段と、
前記スクランブルされたＩＰ／ＵＤＰデータグラムを備えるコンテンツ及びデスクランブラに与えられる送信先ポート番号、送信先アドレスとしてサービスのマルチキャストアドレスを備えるＩＰヘッダーを用いて第２のＩＰ／ＵＤＰデータグラムを構築する手段と、
を備えたことを特徴とする請求項２７記載のシステム。
【請求項２９】
受信装置を備え、該受信装置は、
受信された全てのＩＰ／ＵＤＰデータグラムを分析し、もしＩＰ／ＵＤＰデータグラムが前記選択されたサービスに対応するポート及びマルチキャストアドレスを備えていれば

、
前記コンテンツをデスクランブルする
ことを特徴とする請求項２８記載のシステム。
【請求項３０】
スクランブルされたデジタルデータのための受信装置であって、
受信された全てのＩＰ／ＵＤＰデータグラムを分析する手段と、
もしＩＰ／ＵＤＰデータグラムが、選択されたサービスに対応するポート及びマルチキャストアドレスを備えていれば、コンテンツをデスクランブルする手段と、
を備え、
前記デスクランブルする手段は、前記受信装置に特有なデジタルデータ及び受信された第１のランダムデジタルデータＡＬＥＡ１を用いてデジタルシーケンスＳを発生し、受信された特定のデジタルキーＫおよび前記デジタルシーケンスＳからコントロールワードＣＷを解読し、前記解読されたコントロールワードＣＷを用いて、前記コンテンツをデスクランブルし、
前記コンテンツおよび前記第１のランダムデジタルデータＡＬＥＡ１はブロードキャストされ、
前記特定のデジタルキーＫは、前記コントロールワードＣＷおよび前記デジタルシーケンスＳの関数として前記受信装置について計算され、前記受信装置に送信されることを特徴とする装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタルデータ、イベント、オーディオビジュアルプログラムに対するアクセスコントロールおよびブロードキャスト、並びにセキュリティプロセッサを具備しない端末に開放された環境におけるテーマ別チャンネルブロードキャストの分野に属する。
更に詳しくは、本発明は、ＩＰ型ネットワークに接続された多くの端末へのオーディオビジュアルプログラムに対するセクセスコントロールを伴うブロードキャスト方法およびシステムに関する。
【背景技術】
【０００２】
従来、ＤＶＢ(Digital Video Broadcasting)規格は、アクセスコントロールメカニズムを含み、このアクセスコントロールメカニズムでは、ＥＣＭ(Entitlement Control Message)およびＥＭＭ(Entitlement Management Message)アクセスコントロールメッセージと共に加入者にスクランブル／デスクランブル情報が送信されてメモリカードに格納される。この情報は、定期的に、例えば１０秒ごとに変わる暗号化されたコントロールワードＣＷを備える。同一のプログラムまたは新たなプログラムに対応する新たなコントロールワードは、ＥＣＭアクセスコントロールメッセージと共に加入者に送信される。
【０００３】
例えば、ＥＣＭは１０秒ごとに更新され、各ＥＣＭは３つのフィールドを備えている。第１のフィールドは、例えば親によるアクセスコントロール(parental control)またはスクランブルされたプログラム受信の地域的制限のような、スクランブルされたデータに対するアクセス条件(conditions of access)を規定するアクセスパラメータを備える。第２のフィールドは、オペレーションキーによって暗号化(encrypt)されたコントロールワードＣＷを備える。第３のフィールドは、送信された情報のための完全性チェックパラメータ(integrity checking parameter)を備える。
【０００４】
通常、ＥＭＭは３つのフィールドを備え、第１のアドレスフィールドは、ユーザまたはユーザグループに対するデコーダを選択するためのものである。第２のフィールドは、ユーザまたは複数のユーザに対するアクセス許可を備え、前もって加入者グループに分配されたグループキーによって暗号化されたオペレーションキーを備える。そして第３のフィ

ールドは、送信された情報に対する完全性チェックパラメータを備える。
【０００５】
ＥＭＭは、それらが適用可能なプログラムの前に送信され、スマートカードに格納される。
デコーダがそのグループに対応する暗号化されたオペレーションキーを備えるＥＭＭを受信すると、このキーが既に格納されているか否かをチェックする。もし、格納されていなければ、オペレーションキーは暗号化関数の逆関数により解読(decrypt)されて格納される。一般に、デコーダはセキュリティプロセッサを統合(integrate)する端末およびスマートカードから構成される。そして、スクランブルされたプログラムがブロードキャストされると、オペレーションキーは、それに関連づけられたコントロールワードＣＷを解読するために使用され、そしてそれはＥＣＭを通じて加入者に送られ、または受信機が初期化されるとすぐに書き込まれる
【０００６】
上述したシステムにおいて、加入者は、スクランブルされたプログラムをアクセスするためには、このスクランブルされたプログラムに対するアクセス権を規定するアクセスパラメータを収容するスマートカードに含まれるセキュリティプロセッサを一般に有するところの装置を備える必要がある。
【０００７】
多数の潜在的な加入者およびこれら加入者の地理的な離散のため、スマートカードリーダーをあらゆるユーザに分配することは不可能であるために、上述したアクセスコントロールシステムは、インターネットネットワークを通じたブロードキャストには適さない。
【０００８】
本発明の目的は、セキュリティプロセッサまたはスマートカードを備えない端末を用いて読み取られるスクランブルされたデータに対するアクセスをコントロールする方法を提起することである。
【０００９】
さらに詳しくは、この方法は、二つのタイプのサービス、即ちイベントコントロールされたブロードキャストおよびテレビジョンプログラムチャンネルのブロードキャストに適用可能である。
【００１０】
イベントコントロールされたブロードキャストは、各イベント（ミュージックコンサート、スポーツイベント、トレーニングなど）に対して一つのチャンネルを必要とする。
テレビジョンプログラムチャンネルのブロードキャストは、
－ テレビジョンチャンネルの再ブロードキャスト、
－ 一般加入によるチャンネルプログラムの再ブロードキャスト、
－ １又は２以上のテーマ別加入での一般加入によるチャンネルの再ブロードキャスト、
－ 加入に特有のそのコンテンツのシーケンスを含むチャンネルのブロードキャストおよび創設(creation)、
－ 個人に特有のそのコンテンツのシーケンスを含むチャンネルのブロードキャストおよび創設、
－ 加入に特有のそのコンテンツのシーケンスを含むチャンネルのブロードキャストおよび創設
に関する。
【発明の開示】
【課題を解決するための手段】
【００１１】
本発明による方法は３つのステップを備える。
－ 第１のスクランブルステップは、
・ コントロールワードＣＷを用いて送信されるデジタルデータをスクランブルし、

・ 第１のランダムデータＡＬＥＡ１の関数として且つネットワークにおける端末特有のデータの関数として計算された端末に対するデジタルシーケンスＳを発生し、
・ デジタルシーケンスＳの関数として且つコントロールワードＣＷの関数として端末に対する少なくとも一つの特定のデジタルキーＫを計算し、
・ 対応する特定のデジタルキーＫを端末に送信することにある。

【００１２】

－ 第２のブロードキャストステップは、
・ スクランブルされたデジタルデータ及び第１のランダムデジタルデータＡＬＥＡ１を端末に送信することにある。

【００１３】

－ 第３のデスクランブルステップは、
・ データ交換ネットワークにおける端末のアドレスおよびランダムデータＡＬＥＡ１を用いてデジタルシーケンスＳを再構成し、
・ シーケンスＳおよび特定のデジタルキーＫを発端としてコントロールワードＣＷを解読し、
・ スクランブルされたデジタルデータをデスクランブルすることにある。

【００１４】

本発明によれば、本方法は、また、次の基本的ステップ、即ち、
－ ネットワークを通じて提供されるサービスに対するアクセス権を既に予約した全てのユーザに予約番号を割り当てるステップと、
－ ネットワークにおける前記端末特有のデジタルデータおよび前記予約番号と引き替えに特定デジタルキーＫをこのユーザに送信するステップとを備える。

【００１５】

好ましくは、端末特有のデジタルデータは、ネットワークにおけるこの端末のアドレスである。
本発明によれば、スクランブルされたデジタルデータは、無線チャンネルまたは有線またはデジタルケーブルの何れかにより送信される。
本発明によれば、データ交換ネットワークはＩＰ型である。

【００１６】

本発明によれば、コントロールワードＣＷは、好ましくはランダム法で発生される。
本発明によれば、ネットワークにおける端末アドレスおよび予約番号は、端末ユーザによってデジタルデータサプライヤーにＴＣＰ／ＩＰプロトコルを用いて送信される。
本発明によれば、デジタルデータは、例えばオーディオビジュアルプログラムであってもよい。

【００１７】

本発明による方法は、同一のコントロールワードＣＷを用いてスクランブル／デスクランブルステップを識別するために、スクランブルされたデジタルデータと共に第２のランダムデータを送信する追加的ステップを備える。

【００１８】

本発明による方法は、ネットワークを通じて提供される各サービスにマルチキャストアドレスを割り当て、そしてこのマルチキャストアドレス、ランダムデータ（Ａｌｅａｌ）及び対応するコントロールワードＣＷをサービステーブルに格納するステップを備える。
本発明によれば、（ＡＬＥＡ１，ＣＷ）のペアは定期的に変更される。
このペアの有効期間(validity duration)は固定または可変であってもよい。

【００１９】

本発明の一つの特別な用途において、各ブロードキャストサービスは、複数のエレメンタリオーディオ(elementary audio)、ベーシックビデオ(basic video)、エンハンスドビデオ(enhanced video)スループットを備える。
この用途において、スクランブルステップは、次のサブステップ、即ち、
－ データグラムのヘッダーにある送信先ポート及びアドレスの関数としてスクランブ

ルされるように、マルチキャストアドレスデータグラムをフィルタし、
－ サービスと関連づけられたコントロールワードを用いて入力で受信された各データグラムをスクランブルし、
－ アクセスコントロールに特有のヘッダーを各データグラムに付け加え、
－ アクセスコントロールに特有のヘッダーおよびスクランブルされた入力データグラムを備える有用なコンテンツ、およびデスクランブラに与えられる送信先ポート番号、送信先アドレス、サービスのマルチキャストアドレスを備えるＩＰヘッダーを使って第２のデータグラムを構成するサブステップを備える。

【００２０】
本発明の変形に係る一実施形態によれば、ブロードキャストステップは、ＩＰネットワークを通じて第２のＩＰデータグラムを送信する。
この変形例においては、第２のＩＰデータグラムは、ＵＤＰトランスポートプロトコルを使用すると共に、デスクランブルステップは、次のサブステップ、即ち、
－ 全ての受信データグラムを分析し、そして、もし一つのデータグラムが、選択されたサービスに対応するポートとマルチキャストアドレスとを備えていれば、
・ アクセスコントロールに特有のヘッダーを削除し、
・ 有用なコンテンツをデスクランブルし、
・ アプリケーション表示モジュールによる処理のためにＩＰスタック上にデスクランブルされた有用なコンテンツを再挿入する
というサブステップを備える。

【００２１】
第１のケースでは、所定のサービスのエレメンタリオーディオ及びビデオスループットは、異なる送信先ポートを用いてネットワーク上に別々にブロードキャストされる。このケースでは、ベーシックオーディオおよびビデオデータのみがスクランブルされる。エンハンスドビデオデータはスクランブルされるかも知れず、或いはスクランブルされないかも知れない。

【００２２】
第２のケースでは、所定のサービスのエレメンタリオーディオ及びビデオスループットは、それらのみが所定ポート上に単一のサービススループットを送信するように、多重化(multiplex)される。このケースでは、サービススループットのみがスクランブルされる。

【００２３】
本発明による方法は、データ交換ネットワークに接続された少なくとも一つの端末に対するコントロールワードＣＷによってスクランブルされたデジタルデータのアクセスコントロールを伴う送信システムにおいて実施され、上記データ交換ネットワークは、
－ 予約ゲートウェイと、
－ 送信されるべきデジタルデータをスクランブルするように設計されたプラットフォームと、
－ スクランブルされたデータをブロードキャストするように設計されたサーバー
を備える。

【００２４】
本発明によれば、予約ゲートウェイは、
・ ネットワークにおける端末に特有のデータおよびランダムデータＡＬＥＡ１の関数として端末についてのデジタルシーケンスＳを発生する手段と、
・ コントロールワードＣＷおよびデジタルシーケンスＳの関数として、前記端末についての特定のデジタルキーＫを計算する手段と、
を備える。

【００２５】
本発明によれば、予約ゲートウェイは、
－ ネットワークを通じて提供されるサービスへのアクセス権を予め予約した任意のユ

ーザに予約番号を割り当てる手段と、
－ ネットワークにおける前記端末に特有のデジタルデータおよび前記予約番号と引き替えに、このユーザに特定のデジタルキーＫを送信する手段と、
を備える。
【００２６】
本発明によれば、予約ゲートウェイは、また、それぞれが特定の個別キーに対応する複数の予約番号を格納するように設計されたデータベースを備える。
本発明によれば、予約ゲートウェイは、ネットワークを通じて提供される各サービスにマルチキャストアドレスを割り当てる手段と、対応するマルチキャストアドレス、ポート、ランダムデータ（ＡＬＥＡ１）およびコントロールワードＣＷを関連づけるサービステーブルを収容するメモリを備える。好ましくは、（ＡＬＥＡ１，ＣＷ）のペアは定期的に変更される。
【００２７】
好ましくは、コントロールワードＣＷはランダムに発生される。
本発明の特別な一実施形態において、データ交換ネットワークは、ＩＰ型であり、そして、前記スクランブルプラットフォームは、また、
－ データグラムのヘッダーに存在する送信先ポート及びアドレスの関数としてスクランブルされるべきマルチキャストアドレスのＩＰデータグラムをフィルタリングする手段と、
－ サービスに関連づけられたコントロールワードを用いて、入力で受信された各データグラムをスクランブルする手段と、
－ アクセスコントロールに特有のヘッダーを各データグラムに付け加える手段と、
－ アクセスコントロールに特有のヘッダー及びスクランブルされた入力データグラムを備える有用なコンテンツ及びデスクランブラに与えられる送信先ポート番号、送信先アドレス、サービスのマルチキャストアドレスを備えるＩＰヘッダーを用いて第２のデータグラムを構成する手段とを備える。
【００２８】
本発明は、また、スクランブルされたデジタルデータの受信装置に関し、この装置は、
－ 全ての受信されたデータグラムを分析する手段を備え、もし、データグラムが、選択されたサービスに対応するポートおよびマルチキャストアドレスを備えていれば、
－ アクセスコントロールに特有のヘッダーを削除する手段と、
－ 有用なコンテンツをデスクランブルする手段と、
－ 受信されたプログラムの表示および処理のためのポートを通じてＩＰスタック上にデスクランブルされた有用なコンテンツを再挿入(reinject)する手段とを備える。
【００２９】
本発明による処理は、
・ 従来のオペレータ（ラジオ、テレビジョン）については、
－ それらの視聴者を拡大し、
－ それらの地理的なサービスエリア(coverage area)を拡大し、
－ マーケティングオファー(marketing offer)を充実させ、
－ 双方向性により個別のサービス（オンデマンドビデオ）を提供することを可能にする。
・ 新たなオペレータ（特定のコンテンツ）については、
－ テーマコンテンツを提供し、
－ テレビジョンオペレータによって売買されないライブプログラム（コンサート、スポーツなど）を提供し、
－ 企業のための内部通信媒体（従業員）または外部通信媒体（提供者）を提供することを可能にする。
【００３０】
本発明の利点と他の特徴は、添付の図面を参照して非制限的な例として与えられる以下

の説明から明らかになるであろう。

【発明を実施するための最良の形態】

【００３１】

図１は、必ずしもセキュリティプロセッサーを用いることなく、端末４にインターネットネットワーク２を通じてスクランブルされたオーディオビジュアルプログラムまたはテーマ別のチャンネルをブロードキャストするシステムを示す。

【００３２】

このシステムは、単一のデータパケットを端末４に送信するマルチキャストブロードキャスティングサーバー６を備える。このサーバー６は、ＭＰＥＧ２／ＭＰＥＧ４標準に従って送信されるオーディオビジュアルプログラムの受信用のアンテナ８に接続され、またはデータベース１０に接続され、またはピックアップカメラ１２のようなテレビジョンプログラムのソースに接続される。サーバー６は、また、オーディオビジュアルプログラム予約ゲートウェイ１４およびスクランブルプラットフォーム１６に接続される。

【００３３】

予約ゲートウェイ１４は、オーディオビジュアルプログラムのコマーシャルオファー(commercial offer)のプレゼンテーションページを管理し、これらプログラムに対するアクセス権のための予約番号を発生するために使用されるソフトウェアを備えたコンピュータである。

スクランブルプラットフォーム１６は、個別キーを計算するために使用される暗号化関数Ｇを含む暗号ソフトウェア(cryptographic software)を備えるコンピュータに接続される。

顧客端末４は、コントロールワードＣＷを再構成するために使用される暗号化関数を使用するソフトウェアを備える。

本発明による処理は、図２から６を参照して説明されるであろう。

【００３４】

本発明の好ましい一実施形態において、本発明による処理は、“ＩＰからＵＤＰへのトンネル(IP to UDP tunnel)”のソリューションに基づいており、換言すると、到来するＩＰ／ＵＤＰデータグラムがスクランブルされて、新たな出力ＩＰ／ＵＤＰデータグラムにカプセル化される。このソリューションは、フランステレコムによる“ＩＰサービスへの条件付きアクセスのための方法、システムおよび装置(METHOD, SYSTEM AND DEVICE FOR CONDITIONAL ACCESS TO IP SERVICES)”と題されたフランス特許出願において述べられており、第０１　０５３１８号として登録されている。

【００３５】

コントロールされたオーディオビジュアルサービスが創設されるとき、コンテンツ配給業者(content distributor)は、サービス入力パラメータ（マルチキャストアドレスなど）を規定する。

顧客のステーションは、この出願において述べられた方法を使用して、ネットワークを通じて受信されたＩＰ／ＵＤＰデータプログラムをデスクランブルし、サービス入力パラメータを抽出し、そしてそれらを表示するために、暗号化されていないブロードキャストプログラムをアプリケーションレベルに提示する。

【００３６】

＜アクセス権の予約＞

本発明による方法は、ブロードキャストプログラムへのアクセスをコントロールするための２つの予備的ステップを使用する。即ち、

・ 予約ゲートウェイに格納された予約番号によって表される予約チケットの販売、

・ １又は２以上の個別キーとチケットとの引き替えである。

【００３７】

これら２つのステップは独立である。予約キーを取得することは、

－ イベントのブロードキャスト日の前になされることができ、

－ 表示のために使用されるステーション以外の顧客のステーション上でなされること

ができ、
－ 広告キャンペーンに由来することができ、
－ 無料で提供されることができ、
－ 等々である。
【００３８】
各ユーザは、個別キーを顧客ステーション上で取得する。このキーは、各端末に対しユニーク(unique)であり、そして顧客端末に特有の内部データを用いて特徴付けられる。２つの上記ステップ（チケットの販売およびこれらチケットと個別キーとの引き替え）は、イベントコントロールされたオーディオビジュアルブロードキャストをアクセスするために必要であり、且つブロードキャストプログラムをデスクランブルするために必要なパラメータを取得するために必要である。
【００３９】
＜予約チケットの発生＞
ゲートウェイ１４は、ユーザがイベントを購入した後に予約チケットを分配する。チケットはゲートウェイ１４において管理（発生、分配）される。プログラムが分配される前に、チケットが発生され且つユニークであることがチェックされる。販売された全てのチケットは、進行中のイベントのため、および将来のイベントのために、予約チケットを収容するデータベースに記憶される。イベントの日の後、サービスはもはや提供されず、そして記憶されたチケットはデータベースから自動的に削除される。
【００４０】
図２は、ユーザがゲートウェイ１４にインターネットネットワーク２を通じて、１又は２以上の予約チケットを購入するための要求を送信（矢印２０）する本発明の実施形態による予約手順を示す。ゲートウェイ１４は、予約番号を発生し、そして顧客端末４に１又は２以上の予約番号を返す（矢印２２）。
【００４１】
図３は、本実施形態を用いて個別キーと予約チケットを交換するための手順を示す。
ユーザは、ゲートウェイ１４に個別キーの要求を送信する（矢印２４）。この要求は、所定のプログラムに特有の予約チケットの番号、ひいては顧客端末４のアドレス@TERMINALを備える。
【００４２】
ユーザが個別キーを獲得するために予約チケットを交換するときに、ユーザのユニークな識別子であるアドレス@TERMINALはデータベースに登録される。
ゲートウェイ１４は、１又は２以上の個別キーＫを管理し、そして、それらをユーザの端末４に送信する（矢印２６）。
【００４３】
＜個別キーの発生および分配＞
（単数または複数の）個別キーＫは、ユーザが予約チケットを交換することによりイベントを表示したいときに発生される。ユーザは、引き替え要求の間に、端末アドレス（@TERMINAL）およびチケット番号（ticket number）を提供する。個別キーはこのアドレスの関数として計算される。
【００４４】
＜個別キーの計算＞
図４は、個別キーの計算を図式的に示す機能ブロックを表す。
第１のランダムデジタルデータＡＬＥＡ１と共に（ステップ３２）、ソフトウェアモジュールはランダムにコントロールワードＣＷを発生する（ステップ３０）。ランダムデータＡＬＥＡ１は、それから、第１の関数Ｆを用いて、ユーザ端末４のアドレス（@TERMINAL 34）を暗号化するために使用される。暗号化の結果は、次の表現で与えられるデジタルシーケンスＳである
Ｓ＝Ｆ（ＡＬＥＡ１，@TERMINAL）
【００４５】

ネットワークにおける顧客端末のアドレス（@TERMINAL）は、ネットワークにおけるこの端末に特有の如何なるパラメータによって置き換えられてもよいことに留意されたい。

次のステップは、第２の関数Ｇを用いてコントロールワードＣＷのデジタルシーケンスＳによる暗号化の結果として得られる特定のデジタルキーＫ＝Ｇ（Ｓ，ＣＷ）を規定することから構成される。

【００４６】

予約チケットが１又は２以上の個別キーと引き替えられるべきであることを顧客が要求すると、この要求はスクランブルされたプログラムがブロードキャストされる前にインターネットのネットワークを通じてユニキャストで顧客端末４に送信される（矢印４２）。

顧客に購入された各イベントについて、関連する個別キーＫがこの顧客の端末に格納される。

【００４７】

＜ゲートウェイ１４／ブロードキャスタ６及びスクランブルプラットフォーム１６の間の通信＞

第１にはゲートウェイ１４、ブロードキャスタ６と、第２にはスクランブルプラットフォーム１６との間の通信は、サービスが創設されるとき又はキーが変更されるときに、データＡＬＥＡ１及びコントロールワードＣＷのランダム発生を要求するため、またはサービスに関連するパラメータを交換するため、送信ポイント装置（ゲートウェイ１４／サーバー６）とスクランブルプラットフォーム１６との間でＡＰＩ(Application Programming Interface)ユーザインターフェイスを規定することによりなされる。

【００４８】

＜サービスの管理＞

ゲートウェイ１４は、異なるブロードキャストサービスについてスクランブルプラットフォーム１６に通知する。マルチキャストアドレスが各サービスに割り当てられる。サービスは、多くのエレメンタリスループット（オーディオ、ベーシックオーディオ、エンハンスドビデオ）を備え、それらを処理することのできるハイレンジ受信機の受信品質を改善する。これらのエレメンタリスループットは異なる分配ポートを使用することによりネットワーク２上に個別にブロードキャストされるか、または所定ポート上で一つのみのスループットを送信するために多重化される。

【００４９】

第１のケースでは、オーディオおよびベーシックオーディオおよびビデオデータのみがスクランブルされる。エンハンスドデータはスクランブルされてもよく、あるいはスクランブルされなくてもよい。

第２のケースでは、サービススループットのみがスクランブルされる。

【００５０】

スクランブルプラットフォーム１６は、サービスに割り当てられたポート及びマルチキャストアドレスのためのコントロールワードＣＷ、信号でブロードキャストされるランダムデータＡＬＥＡ１、サービスを関連づけるサービステーブルにおいて、スクランブルされるべきデータを管理する。

これらのテーブルは、サービスロケーションテーブルＩ、いわゆるプロファイルテーブルＩＩ、およびアソシエーションテーブルＩＩＩから構成される。

サービステーブルの例を次に示す。

【００５１】

【表１】

テーブルＩ

サービスロケーション		
Service_Id	@MultiCast	No_Port
1	X	2
1	X	3

【００５２】
【表２】

テーブルＩＩ

プロファイルテーブル		
Profile_CA_Id	ALEA	CW
10	AA AA AA AA AA AA AA AA	BB BB BB BB BB BB BB BB
11	CC CC CC CC CC CC CC CC	DD DD DD DD DD DD DD DD
12	EE EE EE EE EE EE EE EE	AA AA AA AA AA AA AA AA
13	FF FF FF FF FF FF FF FF	CC CC CC CC CC CC CC CC
14	FF FF FF FF FF FF FF FF	CC CC CC CC CC CC CC CC

【００５３】
【表３】

テーブルＩＩＩ

アソシエーションテーブル		
@MultiCast	No_Port	Profile_CA_Id(current
X	2	10
X	3	10

【００５４】
サービスロケーションテーブルＩは、予約ゲートウェイ１４を通じて宣言された１又は２以上のサービスの基本的スループットを格納する。
プロファイルテーブルＩＩは、予約ゲートウェイ要求１４上で発生されたスクランブルパラメータ（ＡＬＥＡ＋ＣＷ）を格納する。
アソシエーションテーブルＩＩＩは、各エレメンタリスループットについて、スクランブルされている暗号化区間で使用される現在のプロファイル(current profile)についての情報を提供する。
【００５５】
＜サーバーからのＩＰ／ＵＤＰデータグラムアウトプットのスクランブル＞
データサーバー６によって供給される暗号化されていないＩＰ／ＵＤＰデータグラムは、スクランブルプラットフォーム１６に入力される。ＩＰ／ＵＤＰデータグラムのヘッダーに存在する送信先ポート及びアドレスに応じて、スクランブルプラットフォーム１６は、
・ スクランブルされるべき@MultiCastからのＩＰ／ＵＤＰデータグラムをフィルタし、これらのアドレスは上述のサービステーブルに収容され、
・ サービスに関連づけられたコントロールワードを用いて入力に受信されるＩＰ／Ｕ

ＤＰデータグラムをスクランブルし、
・ アクセスコントロール特有のヘッダーをスクランブルされたデータグラムに付け加え、
・ 第２のＩＰ／ＵＤＰデータグラムを、
－ 送信先アドレスとしてサービスのマルチキャストアドレスを備えるＩＰヘッダーと、
－ 送信先ポートとしてスクランブラに与えられるポート番号と、
－ ＩＰ／ＵＤＰスクランブルされた入力データグラム（ヘッダーを含む）を備える有用なコンテンツとを用いて構築する。

【００５６】
ランダムデータＡＬＥＡ１は、スクランブルされたデータと共にブロードキャストされ、そして予約チケットを引き替えた顧客は、引き替えに個別キーＫを受け取るであろうことを記憶に留められたい。

【００５７】
＜コントロールワードの解読＞
顧客端末４は、ランダムデータＡＬＥＡ１を受信するまではコントロールワードＣＷを計算することはできず、換言すると、受信されたデータをデスクランブルすることは、それを必要とするのと同時である。コントロールワードＣＷは、顧客端末の個別のアドレス@TERMINALおよび個別キーなしでは計算することはできない。これは、個別キーの違法コピーの源を発見する手段を提供し、それは、顧客端末に割り当てられた当該顧客端末のユニークな識別子から分離できない。もし、このようなタイプの不正行為が発見されれば、不正行為がなされた顧客端末は、後の個別キーセットのブロードキャストから自動的に除外される。

【００５８】
上述したように、コントロールワードＣＷは、アドレス@TERMINALおよびスクランブルされたプログラムと共に受信されたランダム可変(random variable)のＡＬＥＡ１の関数として計算されるデジタルシーケンスＳと、ユニキャストで受信された個別キーＫの関数として解読関数Ｇ′によって計算される。

【００５９】
スクランブルされたプログラムがブロードキャストされるとき、第２のランダムデータＡＬＥＡ２が、新たなスクランブル／デスクランブルキーを取得するためにコントロールワードＣＷと組み合わせられ、この新たなスクランブル／デスクランブルキーはランダムデータＡＬＥＡ１と同時に顧客端末４に送信される。この新たなデータＡＬＥＡ２は追加的なデスクランブルキーのように使用され、そして具体的に決定された時間、例えば新たなデータグラムを送信する時に修正され得る。

【００６０】
＜受信スクランブルデータの受信およびデスクランブル＞
顧客端末は、スクランブルされた又はスクランブルされていないデータグラムを受信する。それは、全てのそれらのフレームを解析する。もし、ＩＰ／ＵＤＰデータグラムが、選択されたサービスに対応するポート及びマルチキャストアドレスを持っていれば、それは、
・ スクランブラによって付け加えられたＩＰ／ＵＤＰヘッダーを削除し、
・ 有用なコンテンツをスクランブルし、
・ スクランブルされていない有用なコンテンツ、換言すると、受信プログラムの表示のために設けられた顧客端末のポートを通じてＩＰスタック上にデータグラムの暗号化されていないコンテンツ及びＩＰ／ＵＤＰヘッダーを再挿入する。

【００６１】
上述した方法は、イベントの分離されたブロードキャスト(isolated broadcasting oh an event)を行うときに使用されてもよい。この場合、単一の個別キーがイベントの期間に等しい寿命で発生されるであろう。しかし、この個別キーはイベントの期間中に何回も

置き換えられてもよい。

【００６２】

＜ＴＶチャンネルのブロードキャスト＞

このタイプのブロードキャストについてはイベントの寿命(the life of the event)の間、単一のキーを使用することは適切ではない。ＴＶチャンネルの受信は、より長期の加入読(subscription)、例えば、月々の加入、テーマ別の加入に依存する。この受信方法を保護するため、コントロールワードＣＷを次のように変更すること、即ち、

・ 一般的な加入の場合には定期的に、

・ テーマ別の加入の場合にはブロードキャストコンテンツによって、

変えることが必要である。

【００６３】

＜一般的な加入モード＞

コンテンツの配給者は、顧客端末上でのＴＶチャンネルの受信を提案する。その表示は、コンテンツにかかわらず、所定区間の間にプログラムをアクセスするために購入された加入(subscription)に依存する。

【００６４】

このタイプの加入については、予約チケットは、この加入の購入品のように取り扱われる。各加入の更新は、予約チケットを購入した後になされるであろう。第１の個別キーは、購入検証区間(purchased validation period)に対応するチケットの引き替え中に分配されるであろう。この加入の有効区間中、コントロールワードの変更は、権利を購入した全顧客端末上でのプログラムブロードキャストの受信を保護するために必要であろう。

【００６５】

図５および６に示された変形に係る一実施形態において、コントロールワードに対する変更は、次のステップ、即ち、

－ 加入区間を、それぞれがコントロールワードの寿命に対応する一連の暗号化区間CP_iに分解するステップと、

－ 暗号化区間CP_iに偶数値を割り当てると共に次の暗号化区間CP_{i+1}に奇数値を割り当て、または、暗号化区間CP_iに奇数値を割り当てると共に次の暗号化区間CP_{i+1}に偶数値を割り当てるステップと、

－ 各暗号化区間CP_iについて、使用される少なくとも一つの偶数のコントロールワードおよび少なくとも一つの奇数のコントロールワードを発生するステップと、

－ 使用される奇数のコントロールワードおよび偶数のコントロールワードを再構築するために既存の暗号化区間および次の暗号化区間に対応する個別キーを各端末に送信するステップと、

－ もし暗号化区間に割り当てられた値が偶数であれば顧客端末が偶数のコントロールワードを使用すると共に、もし暗号化区間に割り当てられた値が奇数であれば顧客端末が奇数のコントロールワードを使用するように、スクランブルされたプログラムと共に各端末にコントロールワード変更インジケータ(change control word indicator)を送信するステップとを備える。

【００６６】

コントロールワード変更インジケータは、暗号化区間が変えられる度にパリティを変更するデジタル値である。

好ましくは、データスループットは、ビデオ又はオーディオデータと同じマルチキャストアドレスで送信されるが、異なるポート番号で送信される。このスループットは、ＳＤＰ(Session Description Protocol)ファイルにおいて識別されるか、またはシグナリングスループット(signaling throughput)において識別される。

【００６７】

スクランブルされたプログラムが備えるパリティ変更インジケータを発端として、端末は、新たなコントロールワードＣＷが使用されるべき時間を決定する。

もし、暗号化区間CP_iに割り当てられた値が偶数であれば、顧客端末は、偶数のコン

トロールワード（ＣＷ０，ＣＷ２，など）を使用し、そして、もし暗号化区間$ＣＰ_{i}$に割り当てられた値が奇数であれば、奇数のコントロールワード（ＣＷ１，ＣＷ３，など）を使用する。

【００６８】

個別キーは、必ずしも、オーディオビジュアルプログラムを表す信号に示される暗号化区間の変化に同期してブロードキャストされるとは限らない。第２の情報は、顧客端末４が次の暗号化区間のために個別キーを読み出さなければならない時期を示すための信号に使用されるであろう。

この情報が変わる度に、顧客端末が次の暗号化区間のために個別キーを読み出さなくてはならない。

【００６９】

図６に示されるダイアグラムは、キーが変更される時点でのシステムの動作を記す。

この図において、最初の日ｄ１と最後の日ｄ２との間の加入期間Ｄは、それぞれが暗号化区間に対応する４つのフェーズ（$ｐ_{0}$，$ｐ_{1}$，$ｐ_{2}$，$ｐ_{3}$）のシーケンスに分解される。２進値０（５０参照）は偶数のペア$ｐ_{0}$および$ｐ_{2}$に割り当てられ、２進値１（５２参照）は奇数のフェーズ$ｐ_{1}$および$ｐ_{3}$に割り当てられる。加入期間Ｄの期間中、一連のコントロールワードのペア（ＣＷ０，ＣＷ１），（ＣＷ２，ＣＷ１），（ＣＷ２，ＣＷ３），（ＣＷ４，ＣＷ３）は、コントロールワードの連続的変化に対し時間ｔ１、ｔ２、ｔ３、ｔ４で一連の個別キーのペア（Ｋ０，Ｋ１），（Ｋ２，Ｋ１），（Ｋ２，Ｋ３），（Ｋ４，Ｋ３）の形式で顧客端末に送信される。端末は、個別キー（Ｋ０，Ｋ１）のなかのワードのペアを受信し、そして最初のフェーズ$ｐ_{0}$の期間中、Ｋ０を使用する。

【００７０】

端末は、奇数のフェーズ$ｐ_{1}$の間、奇数のコントロールワードＫ１を使用する。同じ手順が次のフェーズの期間中に使用される。

従って、ＴＶチャンネルへの接続がなされるときにはいつでも、換言すると、予約チケットが個別キーと引き替えられた後、顧客端末は、使用すべき“偶数および奇数”の個別キーを読み取る。

【００７１】

この読み出しに対するソリューションは予想できる。即ち、

・ 個別キーは、ＩＰ／ＵＤＰデータグラムのデスクランブルを始める前にデータスループットに読み取られる。このソリューションは、潜在的なユーザの数があまり大きくなければ可能である。

・ 個別キーは、ゲートウェイ１４と接続することにより読み出され、そして、もし顧客端末が偶数フェーズのデータグラムを識別すれば、次の変更まで偶数のコントロールワードを使用し、そして、もし奇数フェーズのデータグラムを識別すれば、次の変更まで奇数のコントロールワードを使用する。

【００７２】

＜テーマ別の加入＞

上述した処理は、この加入モードで使用できる。

しかしながら、この加入のタイプでのプログラムのブロードキャストについては、全ブロードキャストイベント及びそれらのテーマが識別されなければならない。例えば、イベント１（スポーツ）、イベント２（シネマ）、イベント３（ニュース）、等である。このブロードキャストにおける各イベントはキーの変更とリンク(link)されるであろう。

送信装置については、この情報は知られ、それをＭＰＥＧ４標準に準拠して符号化された信号で送信可能とするために適合されなければならない。

【図面の簡単な説明】

【００７３】

【図１】本発明によるブロードキャストシステムを示す図である。

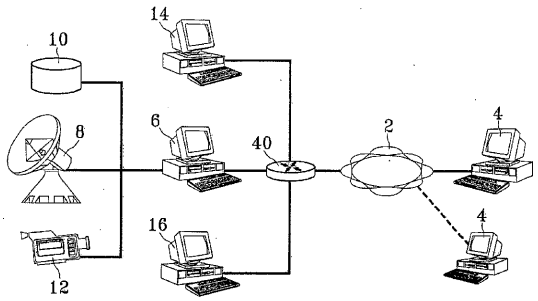
【図２】本発明による方法の初期化における二つのステップを図式的に示す図である。

【図３】本発明による方法の初期化における二つのステップを図式的に示す図である。

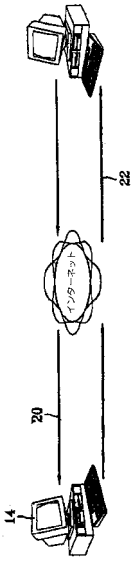
【図４】本発明による方法の好ましい実施形態を図示するブロックダイアグラムを示す図である。
【図５】本発明によるコントロールワードを変えるための処理を図式的に示す図である。
【図６】本発明によるコントロールワードを変えるための処理を図式的に示す図である。

【図１】

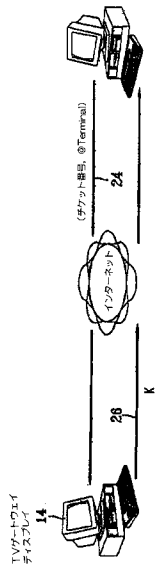
FIG. 1



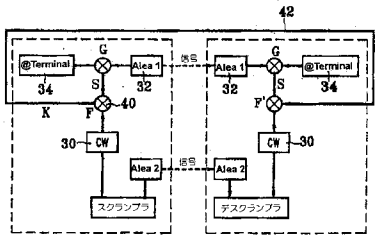
【図２】



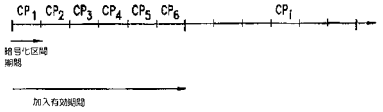
【図３】



【図４】

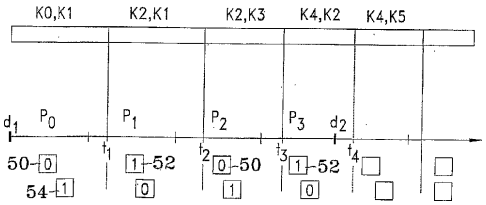


【図５】



【図６】

FIG.6



フロントページの続き

(72)発明者　アンドレ・コデ
フランス・Ｆ－３５２００・レネ・シュマン・ドゥ・トリネ・１・アパルトマン・４７５７
(72)発明者　ピエール・フェヴリエール
フランス・Ｆ－３５２５０・サン・シュルパイス・ラ・フォレ・リュ・デ・トロワ・ピグノン・３

合議体
審判長　渡邊　聡
審判官　志摩　兆一郎
審判官　乾　雅浩

(56)参考文献　特開２０００－２８７１９２（ＪＰ，Ａ）
特開平１１－１２２２３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N7/167