

【特許請求の範囲】**【請求項 1】**

デジタル放送を送出するヘッドエンド装置と、前記ヘッドエンド装置から前記デジタル放送を受信するデジタルテレビと、前記デジタルテレビとデータ通信可能に接続され、有料放送コンテンツの視聴のための課金媒体から情報を読み取る端末装置とを備え、

前記ヘッドエンド装置は、データ放送及び前記有料放送コンテンツを含むデジタル放送を前記デジタルテレビに送出し、

前記デジタルテレビ及び前記端末装置はそれぞれテレビ側視聴制限制御部及び端末側視聴制限制御部を有し、前記テレビ側視聴制限制御部は、前記ヘッドエンド装置から受信された前記データ放送に基づいて中間鍵データを生成して前記端末装置へ送信し、前記端末側視聴制限制御部は、前記端末装置により前記課金媒体から情報が読み取られた場合に前記中間鍵データから本鍵データを生成して前記デジタルテレビに送信し、前記テレビ側視聴制限制御部は、前記本鍵データの認証処理を行って認証に成功すると前記有料放送コンテンツの視聴制限を解除することを特徴とするデジタル放送視聴システム。

10

【請求項 2】

前記ヘッドエンド装置は、前記中間鍵データの生成に用いられる中間鍵生成関数及び前記本鍵データの生成に用いられる本鍵生成関数を前記データ放送に付加する関数付加部を有し、

前記テレビ側視聴制限制御部は、前記中間鍵生成関数に基づいて前記中間鍵データを生成する中間鍵生成部と、前記中間鍵データを前記本鍵生成関数で処理して前記本鍵データを生成するテレビ側本鍵生成部とを有し、

20

前記端末装置は、前記本鍵生成関数を予め記憶する端末側情報記憶部を有し、

前記端末側視聴制限制御部は、前記端末側情報記憶部に記憶された前記本鍵生成関数で前記中間鍵データを処理して前記本鍵データを生成する端末側本鍵生成部を有し、

前記テレビ側視聴制限制御部は、更に、前記端末装置から送られてくる前記本鍵データと前記テレビ側本鍵生成部により生成された前記本鍵データとを照合する鍵照合部を有することを特徴とする請求項 1 に記載のデジタル放送視聴システム。

【請求項 3】

前記関数付加部は、前記中間鍵生成関数及び前記本鍵生成関数を、前記データ放送の B M L コンテンツ内にスクリプトで埋め込み、前記テレビ側視聴制限制御部は、前記 B M L コンテンツから前記中間鍵生成関数及び前記本鍵生成関数を取得することを特徴とする請求項 2 に記載のデジタル放送視聴システム。

30

【請求項 4】

前記中間鍵生成部は、前記デジタル放送に含まれる時刻情報を前記中間鍵生成関数で処理することにより前記中間鍵データを生成することを特徴とする請求項 2 又は 3 に記載のデジタル放送視聴システム。

【請求項 5】

前記デジタルテレビは、認証 I D データを記憶するテレビ側情報記憶部を有し、

前記端末装置の前記媒体側情報記憶部は前記テレビ側情報記憶部と同じ前記認証 I D データを記憶し、

40

前記テレビ側本鍵生成部及び前記端末側本鍵生成部の各々は、前記中間鍵データ及び前記認証 I D データを前記本鍵生成関数で処理して前記本鍵データを生成することを特徴とする請求項 2 乃至 4 のいずれかに記載のデジタル放送視聴システム。

【請求項 6】

前記テレビ側情報記憶部は、更に視聴日の切替り時刻を表す日替情報を記憶し、

前記テレビ側視聴制限制御部は、前記日替情報に基づいて視聴日が切り替わったか否かの判定を行い、視聴日が変わると視聴制限を行う日替処理部を有することを特徴とする請求項 5 に記載のデジタル放送視聴システム。

【請求項 7】

前記テレビ側情報記憶部は、前記デジタルテレビの N V - R A M における自主放送用の

50

領域で構成されることを特徴とする請求項 5 又は 6 に記載のデジタル放送視聴システム。

【請求項 8】

前記ヘッドエンド装置は、前記データ放送に前記課金媒体の媒体 ID を付加する ID 付加部を有し、

前記端末側視聴制限制御部は、前記課金媒体から読み取られた前記媒体 ID を前記デジタルテレビに送信し、

前記テレビ側視聴制限制御部は、前記データ放送に含まれる前記媒体 ID と前記端末装置から受信された前記媒体 ID を照合する ID 照合部を有することを特徴とする請求項 1 乃至 7 のいずれかに記載のデジタル放送視聴システム。

【請求項 9】

デジタルテレビに組み込まれたプログラム処理部によりデジタル放送の視聴を制限するために実行される視聴制限制御プログラムであって、

データ放送及び有料放送コンテンツを含むデジタル放送が受信されたときに、前記デジタル放送に含まれるデータ放送に基づいて中間鍵データを生成し、

前記デジタルテレビに通信可能に接続され、有料放送の視聴のための課金媒体から情報を読み取る端末装置へと前記中間鍵データを提供し、

前記端末装置にて前記課金媒体から情報が読み取られた場合に前記中間鍵データから生成された本鍵データを前記端末装置から取得し、

前記本鍵データの認証処理を行って認証に成功すると有料放送コンテンツの視聴制限を解除する処理を前記デジタルテレビの前記プログラム処理部に実行させることを特徴とする視聴制限制御プログラム。

【請求項 10】

請求項 9 に記載の視聴制限制御プログラムを記憶しており、前記視聴制限制御プログラムを前記デジタルテレビへ送信すると共に、前記中間鍵データ及び前記本鍵データを生成するための鍵生成関数を含んだデータ放送を前記デジタルテレビへ供給することを特徴とするヘッドエンド装置。

【請求項 11】

デジタルテレビとデータ通信可能に接続され、有料放送の視聴のための課金媒体から情報を読み取る端末装置であって、

視聴制限処理のための中間鍵データから本鍵データを生成するための本鍵生成関数を記憶する端末側情報記憶部と、

前記デジタルテレビから前記中間鍵データを取得し、前記端末装置により前記課金媒体から情報が読み取られた場合に前記中間鍵データを前記本鍵生成関数で処理して本鍵データを生成し、前記本鍵データを前記デジタルテレビへ供給する端末側視聴制限制御部と、を有することを特徴とする端末装置。

【請求項 12】

ヘッドエンド装置からデジタルテレビへデジタル放送を送出するデジタル放送視聴システムにおいて有料放送コンテンツの視聴を制限するデジタル放送視聴方法であって、

前記ヘッドエンド装置から前記デジタルテレビへ、データ放送及び有料放送コンテンツを含むデジタル放送を送出し、

前記デジタルテレビにて、前記ヘッドエンド装置から受信された前記データ放送に基づいて中間鍵データを生成し、

前記デジタルテレビから、課金媒体から情報を読み取る端末装置へと前記中間鍵データを送信し、

前記端末装置にて、前記課金媒体から情報が読み取られた場合に前記中間鍵データから本鍵データを生成し、

前記本鍵データを前記端末装置から前記デジタルテレビに送信し、

前記デジタルテレビにて、前記本鍵データの認証処理を行って認証に成功すると前記有料放送コンテンツの視聴制限を解除することを特徴とするデジタル放送視聴方法。

【請求項 13】

デジタルテレビにおいて有料放送コンテンツの視聴を制限する視聴制限制御方法であって、

データ放送及び前記有料放送コンテンツを含むデジタル放送を受信し、

受信された前記データ放送に基づいて中間鍵データを生成し、

前記デジタルテレビに通信可能に接続され、有料放送の視聴のための課金媒体から情報を読み取る端末装置へと前記中間鍵データを提供し、

前記端末装置にて前記課金媒体から情報が読み取られた場合に前記中間鍵データから生成された本鍵データを前記端末装置から取得し、

前記本鍵データの認証処理を行って認証に成功すると有料放送コンテンツの視聴制限を解除することを特徴とする視聴制限制御方法。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、デジタル放送における有料放送コンテンツの視聴制限を行うことが可能なデジタル放送視聴システムに関する。

【背景技術】

【0002】

従来、ホテルなどには、有料放送を視聴可能な放送視聴システムが備えられている。従来の放送視聴システムでは、客室毎にテレビとカードリーダーが接続され、カードリーダーは、有料放送の視聴用の課金カードの挿入口を有している。従来の放送視聴システムはアナログ映像信号に対応しており、客室に配信された映像信号はカードリーダーに一旦取り込まれ、カードリーダーからテレビに供給される。カードリーダーは、有効な課金カードが挿入されると、視聴制限を解除し、テレビに映像信号を供給する。課金カードが挿入されていない場合、又は使用済み等の無効な課金カードが挿入されている場合、カードリーダーはテレビへの映像信号の供給を制限する。このようにして、従来は、カードリーダーによって有料放送の視聴が制限されていた（例えば特許文献1参照）。

20

【特許文献1】特開2004-48590号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

30

しかしながら、従来の放送視聴システムは、アナログ映像信号に対応しており、そのままではデジタル放送には対応できないという問題があった。従来は、カードリーダーがアナログ映像信号をテレビのアナログ映像端子（S端子）に供給するように構成されているので、デジタルテレビへの適用は不可能であった。

【0004】

また、従来のアナログ対応システムをデジタル放送用に改造することもある。しかしながら、この場合はデジタルテレビの改造が必要になってしまうという問題がある。また、有料放送のデータが複数の回路を経由することにより画質が低下するという問題もある。また、デジタル放送視聴システムで有料放送を提供しようとした場合、通信解読による不正利用を確実に防ぐことが重要になる。

40

【0005】

本発明は、従来の問題を解決するためになされたもので、その目的は、デジタルテレビを改造せずに、画質を低下させることなく、通信解読による不正利用を防ぎつつ、視聴制限付きで有料放送を提供可能にするデジタル放送視聴システムを提供することにある。

【課題を解決するための手段】

【0006】

本発明のデジタル放送視聴システムは、デジタル放送を送出するヘッドエンド装置と、前記ヘッドエンド装置から前記デジタル放送を受信するデジタルテレビと、前記デジタルテレビとデータ通信可能に接続され、有料放送コンテンツの視聴のための課金媒体から情報を読み取る端末装置とを備え、前記ヘッドエンド装置は、データ放送及び前記有料放送

50

コンテンツを含むデジタル放送を前記デジタルテレビに送出し、前記デジタルテレビ及び前記端末装置はそれぞれテレビ側視聴制限制御部及び端末側視聴制限制御部を有し、前記テレビ側視聴制限制御部は、前記ヘッドエンド装置から受信された前記データ放送に基づいて中間鍵データを生成して前記端末装置へ送信し、前記端末側視聴制限制御部は、前記端末装置により前記課金媒体から情報が読み取られた場合に前記中間鍵データから本鍵データを生成して前記デジタルテレビに送信し、前記テレビ側視聴制限制御部は、前記本鍵データの認証処理を行って認証に成功すると前記有料放送コンテンツの視聴制限を解除する。

【0007】

この構成により、ヘッドエンド装置がデータ放送及び有料放送コンテンツを含むデジタル放送をデジタルテレビに送出し、デジタルテレビのテレビ側視聴制限制御部がデータ放送に基づいて中間鍵データを生成して端末装置へ送信し、端末装置の端末側視聴制限制御部が課金媒体から情報が読み取られた場合に中間鍵データから本鍵データを生成してデジタルテレビに送信し、テレビ側視聴制限制御部が本鍵データの認証処理を行って認証に成功すると有料放送コンテンツの視聴制限を解除する。このように、本発明は、デジタル放送に含まれるデータ放送と、デジタルテレビ - 端末装置間のデータ通信とによって、デジタル放送視聴システムでの視聴制限付きの有料放送提供を実現できる。デジタルテレビには、データ放送受信機能が装備されており、また、外部とのデータ通信機能も装備されており、したがって、本発明のシステムはデジタルテレビに搭載された標準機能によって実現できる。また、デジタル放送がヘッドエンド装置からデジタルテレビに送られるので、複数の回路の通過による画質低下を避けることができる。さらに、デジタルテレビ - 端末装置間で中間鍵データ及び本鍵データが伝達されており、暗号化により不正利用を排除し、視聴を好適に制限できる。このようにして、デジタルテレビを改造せずに、画質を低下させることなく、通信解読による不正利用を防ぎつつ、視聴制限付きで有料放送を提供することができる。

【0008】

本発明のデジタル放送視聴システムにおいて、前記ヘッドエンド装置は、前記中間鍵データの生成に用いられる中間鍵生成関数及び前記本鍵データの生成に用いられる本鍵生成関数を前記データ放送に付加する関数付加部を有し、前記テレビ側視聴制限制御部は、前記中間鍵生成関数に基づいて前記中間鍵データを生成する中間鍵生成部と、前記中間鍵データを前記本鍵生成関数で処理して前記本鍵データを生成するテレビ側本鍵生成部とを有し、前記端末装置は、前記本鍵生成関数を予め記憶する端末側情報記憶部を有し、前記端末側視聴制限制御部は、前記端末側情報記憶部に記憶された前記本鍵生成関数で前記中間鍵データを処理して前記本鍵データを生成する端末側本鍵生成部を有し、前記テレビ側視聴制限制御部は、更に、前記端末装置から送られてくる前記本鍵データと前記テレビ側本鍵生成部により生成された前記本鍵データとを照合する鍵照合部を有する。

【0009】

この構成により、データ放送にて中間鍵生成関数及び本鍵生成関数がデジタルテレビへ送られる。デジタルテレビでは、中間鍵生成関数を用いて中間鍵データが生成される。中間鍵データが端末装置に送られ、端末装置は、予め記憶してある本鍵生成関数を用いて中間鍵データから本鍵データを生成する。一方、デジタルテレビでも、データ放送により取得した本鍵生成関数を用いて中間鍵データから本鍵データが生成される。これらの2つの本鍵データが照合され、両者が一致すれば、認証が成功する。このようにして、本発明によれば、中間鍵生成関数及び本鍵生成関数を用いる構成が提供され、高いセキュリティ性を確保して、デジタル放送用の視聴制限を好適に実現できる。

【0010】

本発明のデジタル放送視聴システムにおいて、前記関数付加部は、前記中間鍵生成関数及び前記本鍵生成関数を、前記データ放送のBMLコンテンツ内にスクリプトで埋め込み、前記テレビ側視聴制限制御部は、前記BMLコンテンツから前記中間鍵生成関数及び前記本鍵生成関数を取得する。

【 0 0 1 1 】

この構成により、中間鍵生成関数及び本鍵生成関数をデータ放送に付加して好適にデジタルテレビに提供できる。

【 0 0 1 2 】

本発明のデジタル放送視聴システムにおいて、前記中間鍵生成部は、前記デジタル放送に含まれる時刻情報を前記中間鍵生成関数で処理することにより前記中間鍵データを生成する。

【 0 0 1 3 】

この構成により、中間鍵データ生成の元データとして時刻情報を用いるので、中間鍵データが、元の時刻に応じて変化する。中間鍵データから生成される本鍵データも、元の時刻に応じて変化する。したがって、セキュリティ性を更に向上できる。

【 0 0 1 4 】

本発明のデジタル放送視聴システムにおいて、前記デジタルテレビは、認証IDデータを記憶するテレビ側情報記憶部を有し、前記端末装置の前記媒体側情報記憶部は前記テレビ側情報記憶部と同じ前記認証IDデータを記憶し、前記テレビ側本鍵生成部及び前記端末側本鍵生成部の各々は、前記中間鍵データ及び前記認証IDデータを前記本鍵生成関数で処理して前記本鍵データを生成する。

【 0 0 1 5 】

この構成により、中間鍵データ及び認証IDデータを本鍵生成関数で処理して本鍵データを生成する。認証IDデータを本鍵生成の元データにすることにより、更にセキュリティ性を向上できる。

【 0 0 1 6 】

本発明のデジタル放送視聴システムにおいて、前記テレビ側情報記憶部は、更に視聴日の切替り時刻を表す日替情報を記憶し、前記テレビ側視聴制限制御部は、前記日替情報に基づいて視聴日が切り替わったか否かの判定を行い、視聴日が変わると視聴制限を行う日替処理部を有する。

【 0 0 1 7 】

この構成により、日替管理も適切に行うことができ、課金媒体を使った視聴制限を好適に行うことができる。

【 0 0 1 8 】

本発明のデジタル放送視聴システムにおいて、前記テレビ側情報記憶部は、前記デジタルテレビのNV-RAMにおける自主放送用の領域で構成される。

【 0 0 1 9 】

この構成により、デジタルテレビに標準装備されたNV-RAMを利用して本発明のデジタル放送視聴システムとそれによる視聴制限を好適に実現できる。

【 0 0 2 0 】

本発明のデジタル放送視聴システムにおいて、前記ヘッドエンド装置は、前記データ放送に前記課金媒体の媒体IDを付加するID付加部を有し、前記端末側視聴制限制御部は、前記課金媒体から読み取られた前記媒体IDを前記デジタルテレビに送信し、前記テレビ側視聴制限制御部は、前記データ放送に含まれる前記媒体IDと前記端末装置から受信された前記媒体IDを照合するID照合部を有する。この構成により、媒体IDの照合も行うので、セキュリティ性を更に向上できる。

【 0 0 2 1 】

本発明の別の態様は、デジタルテレビに組み込まれたプログラム処理部によりデジタル放送の視聴を制限するために実行される視聴制限制御プログラムであって、データ放送及び有料放送コンテンツを含むデジタル放送が受信されたときに、前記デジタル放送に含まれるデータ放送に基づいて中間鍵データを生成し、前記デジタルテレビに通信可能に接続され、有料放送の視聴のための課金媒体から情報を読み取る端末装置へと前記中間鍵データを提供し、前記端末装置にて前記課金媒体から情報が読み取られた場合に前記中間鍵データから生成された本鍵データを前記端末装置から取得し、前記本鍵データの認証処理を

10

20

30

40

50

行って認証に成功すると有料放送コンテンツの視聴制限を解除する処理を前記デジタルテレビの前記プログラム処理部に実行させる。この態様によっても上述した本発明の利点を得られる。上述した各種の構成をこの態様にも適用可能である。

【0022】

本発明の別の態様はヘッドエンド装置であり、上記の視聴制限制御プログラムを記憶しており、前記視聴制限制御プログラムを前記デジタルテレビへ送信すると共に、前記中間鍵データ及び前記本鍵データを生成するための鍵生成関数を含んだデータ放送を前記デジタルテレビへ供給する。この態様によっても上述した本発明の利点を得られる。上述した各種の構成をこの態様にも適用可能である。

【0023】

本発明の別の態様は、デジタルテレビとデータ通信可能に接続され、有料放送の視聴のための課金媒体から情報を読み取る端末装置であって、視聴制限処理のための中間鍵データから本鍵データを生成するための本鍵生成関数を記憶する端末側情報記憶部と、前記デジタルテレビから前記中間鍵データを取得し、前記端末装置により前記課金媒体から情報が読み取られた場合に前記中間鍵データを前記本鍵生成関数で処理して本鍵データを生成し、前記本鍵データを前記デジタルテレビへ供給する端末側視聴制限制御部と、を有する。この態様によっても上述した本発明の利点を得られる。上述した各種の構成をこの態様にも適用可能である。

【0024】

本発明の別の態様は、ヘッドエンド装置からデジタルテレビへデジタル放送を送出するデジタル放送視聴システムにおいて有料放送コンテンツの視聴を制限するデジタル放送視聴方法であって、前記ヘッドエンド装置から前記デジタルテレビへ、データ放送及び有料放送コンテンツを含むデジタル放送を送出し、前記デジタルテレビにて、前記ヘッドエンド装置から受信された前記データ放送に基づいて中間鍵データを生成し、前記デジタルテレビから、課金媒体から情報を読み取る端末装置へと前記中間鍵データを送信し、前記端末装置にて、前記課金媒体から情報が読み取られた場合に前記中間鍵データから本鍵データを生成し、前記本鍵データを前記端末装置から前記デジタルテレビに送信し、前記デジタルテレビにて、前記本鍵データの認証処理を行って認証に成功すると前記有料放送コンテンツの視聴制限を解除する。この方法によっても上述した本発明の利点を得られる。上述した各種の構成をこの態様にも適用可能である。

【0025】

本実施の形態の別の態様は、デジタルテレビにおいて有料放送コンテンツの視聴を制限する視聴制限制御方法であって、データ放送及び前記有料放送コンテンツを含むデジタル放送を受信し、受信された前記データ放送に基づいて中間鍵データを生成し、前記デジタルテレビに通信可能に接続され、有料放送の視聴のための課金媒体から情報を読み取る端末装置へと前記中間鍵データを提供し、前記端末装置にて前記課金媒体から情報が読み取られた場合に前記中間鍵データから生成された本鍵データを前記端末装置から取得し、前記本鍵データの認証処理を行って認証に成功すると有料放送コンテンツの視聴制限を解除する。この方法によっても上述した本発明の利点を得られる。上述した各種の構成をこの態様にも適用可能である。

【発明の効果】

【0026】

本発明は、デジタル放送に含まれるデータ放送と、デジタルテレビと端末装置の間のデータ通信とによって、デジタル放送の視聴制限を実現でき、デジタルテレビを改造せずに、画質を低下させることなく、通信解読による不正利用を防ぎつつ、視聴制限付きで有料放送を提供できるという効果を有するデジタル放送視聴システムを提供することができる。

【発明を実施するための最良の形態】

【0027】

以下、本発明の実施の形態のデジタル放送視聴システムについて、図面を用いて説明す

10

20

30

40

50

る。

【 0 0 2 8 】

本発明の実施の形態のデジタル放送視聴システムを図 1 ~ 図 4 に示す。本実施の形態の例では、デジタル放送視聴システムがホテルに備えられ、ホテルの自主放送にて視聴制限付きで有料放送コンテンツが提供される。図 1 は自主放送とその視聴制限の概要を示しており、図 2 は視聴制限関連の構成を示しており、図 3 は全体構成を示し、図 4 は自主放送視聴の概要を示している。以下では、まず、図 3 及び図 4 を参照してシステム概要を説明し、それから図 1、図 2 を参照して本発明についてより詳細に説明する。

【 0 0 2 9 】

図 3 に示すように、デジタル放送視聴システム 1 は、ヘッドエンド装置 3、複数のデジタルテレビ 5 及び複数の端末装置 7 を備えている。デジタルテレビ 5 及び端末装置 7 は各客室に設置されている。ヘッドエンド装置 3 は同軸ケーブル等のホテル内放送用配線によって複数のデジタルテレビ 5 と接続されており、デジタルテレビ 5 は L A N で端末装置 7 に接続されている。

10

【 0 0 3 0 】

ヘッドエンド装置 3 はデジタル放送を送出する装置であり、デジタル放送は複数のデジタルテレビ 5 にて受信及び表示される。デジタルテレビ 5 及び端末装置 7 は後述するようにデータ通信を行って有料放送コンテンツの視聴制限を実現する。端末装置 7 はカードリーダーであり、P E T カード 9 を挿入可能である。P E T カード 9 は本発明の課金媒体の典型例である。

20

【 0 0 3 1 】

また、カード発券機 1 1 がホテルの廊下等の適当な場所に設置されており、P E T カード 9 は、カード発券機 1 1 で発券され、端末装置 7 に挿入される。

【 0 0 3 2 】

図 3 に示すように、ヘッドエンド装置 3 は、一般放送送出部 1 3、自主放送送出部 1 5 及び混合器 1 7 を備えており、これら構成により複数の客室でのデジタル放送の視聴を可能にする共聴システムを実現する。

【 0 0 3 3 】

一般放送送出部 1 3 は、地上波デジタル放送及び B S デジタル放送をホテルの無料放送として送出する。地上波デジタル放送及び B S デジタル放送は、アンテナ等により外部から受信されて一般放送送出部 1 3 に供給され、一般放送送出部 1 3 から再配信される。

30

【 0 0 3 4 】

自主放送送出部 1 5 は自主放送を送出する。自主放送はデジタル放送であって、ホテルの有料放送である。有料放送コンテンツは例えば C S チューナーから受信されて自主放送送出部 1 5 に供給される。また、有料放送コンテンツは、D V D 等のレコーダで再生されて自主放送送出部 1 5 に供給される。自主放送送出部 1 5 は、有料放送コンテンツのデータ形式を必要に応じてデジタル放送に適合するように変換する。自主放送送出部 1 5 又はその外部にリアルタイムエンコーダが設けられ、リアルタイムエンコーダにより有料放送コンテンツのデジタル放送データが生成されてよい。

【 0 0 3 5 】

一般放送送出部 1 3 及び自主放送送出部 1 5 から送出されたデジタル放送のデータは、混合器 1 7 で混合されて、全客室のデジタルテレビ 5 に配信される。デジタルテレビ 5 は、選択されたチャンネルのデジタル放送を受信する。

40

【 0 0 3 6 】

上記のうち、地上波デジタル放送及び B S デジタル放送は、ホテルにおける無料放送であり、視聴制限を受けることなく各デジタルテレビ 5 で表示される。一方、自主放送は有料放送であり、視聴制限がかけられる。本実施の形態の例では、本発明の視聴制限技術が自主放送に適用される。そこで、以下では主として自主放送用の構成について説明する。

【 0 0 3 7 】

本実施の形態では、自主放送が、A R I B 規格における「データ放送型サービス」で提

50

供され、そして、有料放送コンテンツの視聴制限を実現するためにデータ放送が利用される。データ放送は、自主放送装置 15 に備えられた多重化機能によって多重化されて提供される。A R I B 規格に規定されるデータ放送の仕組みを利用し、映像を非表示（全画面オーバーレイ）、音声をミュートとすることにより、有料放送コンテンツの視聴が制限される。このとき、多重化されたデータ放送は視聴制限用の画面として機能する。有料放送視聴のための認証が成功すると、視聴制限が解除され、有料放送コンテンツがデジタルテレビ 5 にて表示される。

【0038】

図 4 は、本実施の形態のデジタル放送視聴システム 1 における自主放送（有料放送）視聴のイメージを示す図である。図示のように、テレビの電源が入ると、まず、一般放送として地上波デジタル放送が受信される。ユーザのリモコン操作により自主放送チャンネル（例えば 11ch）が選択されると、自主放送が受信され、データ放送画面が表示される。

【0039】

次に、ユーザのリモコン操作により有料番組が選択されると、デジタルテレビは端末装置と通信を行い、未使用の P E T カードが挿入されているかを確認する。この確認の結果、視聴条件が整っていれば、視聴制限が解除され、有料番組が表示される。P E T カードが時間制限付きであってよく、この場合、端末装置との通信により視聴許可の条件としてタイマー残量が残っているかが確認されてよく、タイマー残量の確認は表示中も行われてよい。

【0040】

図 1 は、デジタル放送視聴システム 1 の視聴制限の概要を示している。図 1 に示すように、ヘッドエンド装置 3 は、データ放送と有料放送コンテンツをデジタルテレビ 5 に送出する。データ放送は、認証に使われる関数として中間鍵生成関数及び本鍵生成関数を含み、これらは、B M L コンテンツにスクリプトで埋め込まれる。また、B M L コンテンツには、システム内で提供される全 P E T カード 9 のカード I D が付加される。カード I D は本発明の媒体 I D に相当する。さらに、ヘッドエンド装置 3 からは、A R I B 規格に基づき T S 中で T O T（Time Offset Table）が送出される。T O T は現在日時の情報であり、本発明の時刻情報に相当する。

【0041】

デジタルテレビ 5 は、端末装置 7 と B M L 規格による通信を行い、上記の各種情報を用いて認証を行う。デジタルテレビ 5 はテレビ側視聴制限制御部 51 を有し、端末装置 7 は端末側視聴制限制御部 71 を有している。これら制御部は、各装置のプロセッサで実現されてよい。テレビ側視聴制限制御部 51 は、まず、中間鍵生成関数を用いて T O T を演算処理して中間鍵データを生成する。中間鍵データは、端末装置 7 に送信されると共に、デジタルテレビ 5 の内部で処理される。

【0042】

端末装置 7 では、適正な P E T カード 9 から情報が読み取られた場合に、端末側視聴制限制御部 71 が、本鍵生成関数を用いて中間鍵データと認証 I D データを演算処理することにより、本鍵データを生成する。認証 I D データ及び本鍵生成関数は予め端末装置 7 に登録されている。生成された本鍵データはデジタルテレビ 5 へと送信される。

【0043】

テレビ側視聴制限制御部 51 でも、本鍵生成関数を用いた中間鍵データと認証 I D データの演算処理により、本鍵データを生成する。本鍵生成関数はヘッドエンド装置 3 からの受信データから抽出される。認証 I D データは予めデジタルテレビ 5 に登録されており、好ましくは後述するようにデジタルテレビ 5 の N V - R A M が記憶装置として利用される。

【0044】

テレビ側視聴制限制御部 51 は、端末装置 7 から受信した本鍵データと自ら生成した本鍵データを照合し、両者が一致すれば、鍵の認証が成功する。

【0045】

10

20

30

40

50

テレビ側視聴制限制御部 51 は、さらに、カード ID を使った認証を行う。カード ID は P E T カード 9 の ID である。前述したように、データ放送の B M L コンテンツには、全 P E T カード 9 のカード ID が保持されている。また、端末装置 7 は、P E T カード 9 から読み取ったカード ID をデジタルテレビ 5 へ送信する。テレビ側視聴制限制御部 51 は、端末装置 7 から受信されたカード ID が、ヘッドエンド装置 3 から取得された全 P E T カード 9 のカード ID に含まれているかを判定する。一致するカード ID が含まれていれば、カード ID の認証が成功する。

【 0 0 4 6 】

上記の鍵の認証とカード ID の認証が成功すると、テレビ側視聴制限制御部 51 は有料放送コンテンツの視聴制限を解除する。

10

【 0 0 4 7 】

上記に説明されたように、本実施の形態では、中間鍵データが、鍵生成時の時刻 (T O T) に基づいており、したがってランダムな値になる。本鍵データも中間鍵データから作られており、ランダムな値になる。そこで、中間鍵及び本鍵は乱数鍵 (中間乱数鍵及び本乱数鍵、或いは、第 1 乱数鍵及び第 2 乱数鍵) と呼んでもよい。

【 0 0 4 8 】

以上に図 1 を参照して本実施の形態のデジタル放送視聴システム 1 における自主放送の視聴制限の概要を説明した。次に、図 2 を参照し、上記の視聴制限を実現するための構成をより詳細に説明する。

【 0 0 4 9 】

20

図 2 は、本実施の形態のデジタル放送視聴システム 1 における視聴制限関連の構成を示している。

【 0 0 5 0 】

図 2 に示すように、ヘッドエンド装置 3 において、デジタル放送送出部 15 は、データ放送提供部 31、有料放送コンテンツ提供部 33、関数付加部 35、時刻情報付加部 37 及び ID 付加部 39 を有する。

【 0 0 5 1 】

デジタル放送提供部 31 は、B M L で記述されたデータ放送を提供するための構成であり、有料放送の視聴案内 (メニュー画面) がデータ放送で提供される。有料放送コンテンツ提供部 33 は有料放送コンテンツを提供する。有料放送コンテンツは外部から取得されて、必要に応じてデジタル放送形式に変換される。関数付加部 35 は、中間鍵生成関数及び本鍵生成関数をデータ放送に付加する。これら関数は、データ放送の B M L コンテンツ内にスクリプトで埋め込まれる。時刻情報付加部 37 は時刻情報をデジタル放送に付加する。時刻情報は具体的には T O T であり、T S 中で送出される。ID 付加部 39 は、カード発券機 11 から提供される総ての P E T カード 9 のカード ID をデータ放送に付加する。カード ID 情報は、B M L コンテンツに保持されて、デジタルテレビ 5 に供給される。

30

【 0 0 5 2 】

次に、デジタルテレビ 5 及び端末装置 7 の構成を説明する。デジタルテレビ 5 は、図 1 を用いて説明されたテレビ側視聴制限制御部 51 と、ヘッドエンド装置 3 からデジタル放送を受信する放送受信部 53 と、端末装置 7 とデータ通信を行う通信部 55 と、視聴制限の処理に使われる情報を記憶するテレビ側情報記憶部 57 とを備える。

40

【 0 0 5 3 】

一方、端末装置 7 は、端末側視聴制限制御部 71 と、P E T カード 9 に対して読取及び書込を行うリーダライタ部 73 と、カードリーダライタ部 73 を制御して P E T カード 9 に関する処理を行うカード処理部 75 と、デジタルテレビ 5 とデータ通信を行う通信部 77 と、視聴制限の処理に使われる情報を記憶する端末側情報記憶部 79 とを備える。

【 0 0 5 4 】

P E T カード 9 は磁気カードであり、磁気情報の読取及び書込がリーダライタ部 73 により行われる。リーダライタ部 73 は、P E T カード 9 を挿入及び排出のために搬送するモータ、P E T カード 9 の有無を検出するセンサ及び P E T カード 9 に情報を読み書きす

50

るヘッドを備える。

【0055】

デジタルテレビ5の通信部55と端末装置7の通信部77は、LANで接続される。デジタルテレビは、標準的な機能として、BMLサーバとLANにより接続可能に構成されている。この接続機能が、上記接続に使用されている。したがって、端末装置7はBMLサーバとして機能し、デジタルテレビ5がクライアントとして機能し、両者はBML通信を行う。

【0056】

デジタルテレビ5のテレビ側情報記憶部59は、NV-RAMで構成されている。NV-RAMは、デジタルテレビに標準的に装備されており、多数のチャンネルの各々に所定サイズの記憶領域が割り当てられている。本実施の形態では、自主放送用の領域が、テレビ側情報記憶部59として利用される。

10

【0057】

テレビ側視聴制限制御部51は、デジタルテレビ5のプロセッサによって実現される。プロセッサは、テレビ側視聴制限制御部51の機能を実現するプログラムを実行する。このプログラムは、本発明の視聴制限制御プログラムに相当し、図示されないが、ヘッドエンド装置3からデジタルテレビ5に送信されてよい。端末装置7の端末側視聴制限制御部71及びカード処理部75も、端末装置7のプロセッサによって実現される。プロセッサは、これらの構成の機能を実現するプログラムを実行する。

【0058】

20

テレビ側視聴制限制御部51はテレビ側登録部511、中間鍵生成部512、テレビ側本鍵生成部513、鍵照合部514、ID照合部515及び日替処理部516を有する。端末側視聴制限制御部71は、端末側登録部711及び端末側本鍵生成部712を有する。また、カード処理部75は、カード有無判定部751及び正規カード判定部752を有する。

【0059】

テレビ側視聴制限制御部51のテレビ側登録部511は、端末側視聴制限制御部71の端末側登録部711と共に、認証に使われる情報を予め登録する。

【0060】

図5は、登録処理の例を示している。登録処理では、認証IDがデジタルテレビ5及び端末装置7に登録される。登録処理は、ユーザによる視聴に先立って、管理者により、デジタルテレビ5の初期管理画面上で行われる。図示のように、テレビリモコンが操作されて管理画面が表示され、認証IDが入力される。図の例では認証IDは4桁の数字（例えば1234）である。認証IDデータは、デジタルテレビ5のテレビ側情報記憶部57に格納される。テレビ側情報記憶部57はテレビ内NV-RAM領域であり、より詳細にはNV-RAMにて自主放送に割り当てられた領域である。

30

【0061】

また、認証IDデータは、デジタルテレビ5から端末装置7へと送信される。認証IDデータはARIB規格に基づく双方向通信機能により送信される。認証IDデータは、端末装置7の端末側登録部711に取得されて、端末側情報記憶部79に格納される。

40

【0062】

図5の管理画面では、日替設定の登録も行われる。日替設定登録では、日替情報が管理者により入力される。日替情報は、日替時刻、すなわち視聴日の切替り時刻を表す。日替情報もテレビ側登録部511によりテレビ側情報記憶部57に登録される。日替情報もNV-RAMに格納されてよい。

【0063】

また、端末装置7では、事前の登録処理として、本鍵生成関数が端末側登録部711により端末側情報記憶部79に格納される。本鍵生成関数は、ヘッドエンド装置3からデジタルテレビ5へ送信されるBMLコンテンツ内にスクリプトで埋め込まれた本鍵生成関数と同じである。本鍵生成関数は工場出荷時に格納されていてよい。本鍵生成関数は、端末

50

装置 7 に対する管理者の操作によって登録されてよい。また、本鍵生成関数がデジタルテレビ 5 の管理画面上で入力され、端末装置 7 へ送信されてもよい。

【 0 0 6 4 】

図 6 は、テレビ側視聴制限制御部 5 1 の中間鍵生成部 5 1 2 の処理を示している。中間鍵生成部 5 1 2 は、中間鍵データを生成する構成である。中間鍵生成部 5 1 2 は、受信されたデータ放送から中間鍵生成関数を取得し、TOT (時刻情報) を中間鍵生成関数で処理することにより中間鍵データを生成する。図 6 の例では、時刻が 22 : 00 であり、時刻が 4 桁の数値 “ 2 2 0 0 ” として扱われる。中間鍵生成関数は “ $\times 2$ ” であり、すなわち「 2 倍」である。したがって、中間鍵データは、4 4 0 0 (2 2 0 0 の 2 倍) である。中間鍵生成部 5 1 2 は、中間鍵データをテレビ内の処理のためにテレビ側本鍵生成部 5 1 3 に供給する。また、中間鍵生成部 5 1 2 は、中間鍵データを通信部 5 5 を介して端末装置 7 へと送信し、端末側本鍵生成部 7 1 2 へ提供する。

10

【 0 0 6 5 】

図 7 は、テレビ側本鍵生成部 5 1 3 及び端末側本鍵生成部 7 1 2 の処理を示している。テレビ側本鍵生成部 5 1 3 は、テレビ側情報記憶部 5 7 から認証 ID データを取得し、また、ヘッドエンド装置 3 から受信されたデータ放送から本鍵生成関数を取得する。テレビ側本鍵生成部 5 1 3 は、中間鍵データ及び認証 ID データを本鍵生成関数で処理して、本鍵データを生成する。図の例では、中間鍵データが「 4 4 0 0 」であり、認証 ID データが「 1 2 3 4 」である。本鍵生成関数は、「 (中間鍵 + 認証 ID) $\times 3$ の下 4 桁」である。したがって、本鍵データは「 6 9 0 2 」である。

20

【 0 0 6 6 】

また、端末側本鍵生成部 7 1 2 は、デジタルテレビ 5 から受信される中間鍵データを用いて本鍵データを生成する。本鍵生成の処理は、テレビ側と同じである。ただし、認証 ID データ及び本鍵生成関数は予め登録されており、端末側情報記憶部 7 9 から取得される。

【 0 0 6 7 】

端末側の本鍵生成は、図 2 のカード処理部 7 5 にて適正な PET カード 9 が認識されている場合にのみ行われる。カード処理部 7 5 のカード有無判定部 7 5 1 は、PET カード 9 がリーダライタ部 7 3 に装着されているか否かを判定し、正規カード判定部 7 5 2 は、装着された PET カード 9 が正規カードであるか否かを判定する。端末側本鍵生成部 7 1 2 は、カード処理部 7 5 からの情報を基に、正規の PET カード 9 が装着されている場合に、本鍵データを生成する。本鍵データは、デジタルテレビ 5 へと送信される。

30

【 0 0 6 8 】

次に、図 2 に示されるテレビ側視聴制限制御部 5 1 の鍵照合部 5 1 4、ID 照合部 5 1 5 及び日替処理部 5 1 6 について説明する。鍵照合部 5 1 4 は、テレビ側本鍵生成部 5 1 3 から本鍵データを取得し、また、端末装置 7 の端末側本鍵生成部 7 1 2 で生成された本鍵データを取得する。鍵照合部 5 1 4 は、2 つの本鍵データを照合し、両者が一致している場合、鍵の認証が成功したと判定する。

【 0 0 6 9 】

ID 照合部 5 1 5 は、カード ID の照合を行う。ID 照合部 5 1 5 は、ヘッドエンド装置 3 からデータ放送により供給された全 PET カード 9 のカード ID を取得する。また、端末装置 7 では、リーダライタ部 7 3 により PET カード 9 からカード ID が読み取られる。カード ID はリーダライタ部 7 3 からカード処理部 7 5 を介して端末側視聴制限制御部 7 1 に供給され、更に通信部 7 7 を介してデジタルテレビ 5 に送信され、ID 照合部 5 1 5 に取得される。ID 照合部 5 1 5 は、端末装置 7 から取得されたカード ID が、全 PET カード 9 のカード ID に存在する否かを判定する。一致するカード ID があれば、認証が成功する。

40

【 0 0 7 0 】

日替処理部 5 1 6 は、テレビ側情報記憶部 5 7 に記憶された日替情報、すなわち、日替時刻の情報に基づいて視聴制限を行う構成である。日替時刻は例えばホテルのチェックア

50

ウト時刻と同じでよい。日替処理部 5 1 6 は、日替時刻を超えているか否かを判定する。日替時刻を超えていなければ視聴が許可される。

【 0 0 7 1 】

テレビ側視聴制限制御部 5 1 は、上記の鍵照合部 5 1 4 及び I D 照合部 5 1 5 での認証が成功し、かつ、日替処理部 5 1 6 により視聴が許可された場合、有料放送コンテンツの視聴制限を解除する。

【 0 0 7 2 】

日替処理部 5 1 6 は、有料放送コンテンツを提供している最中も、日替判定の処理を継続する。そして、日替時刻を経過すると、視聴が制限される。

【 0 0 7 3 】

以上に、本実施の形態のデジタル放送視聴システム 1 の構成について詳細に説明した。次に、図 8 ~ 図 1 1 を参照し、デジタル放送視聴システム 1 の動作を説明する。図中には、デジタルテレビ 5 側の処理と、端末装置 7 側の処理が示されている。デジタルテレビ 5 側では、映像表示処理とデータ放送処理が行われる。データ放送処理はテレビ側視聴制限制御部 5 1 により制御される。データ放送に関しては、図示のように、画面上でのデータ放送表示と共に B M L 処理が内部で行われる。端末装置 7 では、テレビ応答処理と、カード処理が行われる。テレビ応答処理は、端末側視聴制限制御部 7 1 による行われる処理であって、デジタルテレビ 5 との通信に関連する処理である。既に説明したようにカード端末装置 7 に備えられた B M L サーバが図中のテレビ応答処理を行い、端末側視聴制限制御部 7 1 の機能を実現する。カード処理はカード処理部 7 5 により行われる。

【 0 0 7 4 】

図 8 は、初期設定の動作を示している。テレビ側では、管理画面が表示され (S 1) 、データ放送表示が「端末 I D を入力して下さい」になり、 (S 2) 、端末 I D が認証 I D として入力され、認証 I D 登録要求が発生し (S 3) 、認証 I D データが N V - R A M (テレビ側情報記憶部 5 7) に書き込まれる (S 4) 。また、認証 I D データは、端末装置 7 に送信されて登録される (S 5) 。

【 0 0 7 5 】

端末装置 7 は、端末 I D 登録完了通知をデジタルテレビ 5 に返す (S 6) 。デジタルテレビ 5 は、端末 I D 登録完了の通知を受信し (S 7) 、データ放送表示「日替設定を選択してください」により日替設定の操作を要求する (S 8) 。ここでは、日替時刻が複数の選択肢から選択される。日替設定の操作が行われると、日替設定登録が行われ (S 9) 、日替時刻が日替情報として N V - R A M に書き込まれる (S 1 0) 。そして、デジタルテレビ 5 は、データ放送表示を「初期設定が完了しました」として、初期登録を終了する。

【 0 0 7 6 】

図 9 ~ 図 1 1 は、ユーザ (ホテルの客) により自主放送チャンネルが選局されたときの動作を示している。

【 0 0 7 7 】

図 9 において、案内チャンネル (自主放送チャンネル) が選局されると (S 2 1) 、データ放送表示により、有料放送の案内画面が提示される。この画面で有料番組が選択されると (S 2 2) 、映像表示としてはお試スクイーズ視聴が行われる (S 2 3) 。また、データ放送表示は「暫くお待ちください」になり (S 2 4) 、中間鍵生成部 5 1 2 により中間鍵生成関数及び T O T (時刻情報) から中間鍵データが生成されると共に、視聴許諾要求が発生する (S 2 5) 。

【 0 0 7 8 】

視聴許諾要求と中間鍵データはデジタルテレビ 5 から送信され、端末装置 7 に受信される (S 2 6) 。視聴許諾要求が受信されると、テレビ応答処理からカード処理にカード確認が要求される。この要求は、端末側視聴制限制御部 7 1 からカード処理部 7 5 に対して行われ、そして、要求に応じてまずカード有無判定部 7 5 1 が P E T カードの有無を判別する (S 2 7) 。

【 0 0 7 9 】

10

20

30

40

50

P E Tカード9が無い場合、カード無し通知が端末装置7から送信され(S 2 8)、デジタルテレビ5に受信される(S 2 9)。そして、データ放送表示「カードを入れてください」によりカード挿入が要求され(S 3 0)、データ放送表示は案内T O P画面に戻る(S 4 7)。

【0080】

ステップS 2 7にてP E Tカード9が端末装置7に装着されていれば、カード有り通知が端末装置7から送信され(S 3 1)、デジタルテレビ5に受信される(S 3 2)。データ放送表示は、「暫くお待ちください」に維持される(S 3 3)。端末装置7では、正規カード判定部7 5 2によりP E Tカードが正規か否かが判定される(S 3 4)。この判定は、リーダライタ部7 3によりP E Tカード9からの読み取られた磁気情報に基づいて行われる。P E Tカードが非正規カード(利用済を含む)である場合、非正規カードの通知が端末装置7から送信され(S 3 5)、デジタルテレビ5に受信される(S 3 6)。データ放送表示「カードが違います」が提示されて(S 3 7)、データ放送表示は案内T O P画面に戻る(S 4 7)。

【0081】

ステップS 3 4にてP E Tカードが正規カードであると判定された場合、図10に移り、端末装置7は、本鍵データを生成し、デジタルテレビ5へ送信する(S 3 8)。本鍵データは、端末側本鍵生成部7 1 2により、中間鍵データと認証I Dデータを本鍵生成関数で処理することにより生成される。

【0082】

一方、デジタルテレビ5でも中間鍵データから本鍵データが生成される(S 3 9)。デジタルテレビ5では、テレビ側本鍵生成部5 1 3により本鍵データが生成される。そして、鍵照合部5 1 4が、ステップS 3 8、S 3 9で生成された2つの本鍵データ(端末装置7及びデジタルテレビ5で別々に生成された2つの本鍵データ)を比較し、両者が一致するか否かを判定する(S 4 0)。

【0083】

ステップS 4 0にて2つの本鍵データが一致しない場合、データ放送表示「認証できません」が提示され(S 4 1)、データ放送表示は案内T O P画面に戻る(S 4 7)。

【0084】

また、端末装置7では、カード処理部7 5が、ステップS 3 4の判定処理にてリーダライタ部7 3により読み取られたカードI Dを端末側視聴制限制御部7 1に供給する。このカードI Dの通知が端末装置7からデジタルテレビ5へ送信される(S 4 2)。デジタルテレビ5では、ステップS 4 0の判定がO Kの場合、さらにカードI Dの一致判定がI D照合部5 1 5により行われる(S 4 3)。I D照合部5 1 5は、データ放送から取得された全P E Tカード9のカードI Dの中に、端末装置7から取得されたカードI Dが存在するか否かを判定する。一致するカードI Dが存在しなければ、I D一致判定がN Gであり、データ放送表示「認証できません」が提示され(S 4 4)、データ放送表示は案内T O P画面に戻る(S 4 7)。

【0085】

ステップS 4 3の判定がO Kの場合、日替処理部5 1 6が、現在時刻が日替時刻を超えていないか判定する(S 4 5)。日替情報はN V - R A Mであるテレビ側情報記憶部5 7から取得される。現在時刻が日替時刻を超えていれば、判定結果がN Gになり、データ放送表示「認証できません」が提示され(S 4 6)、データ放送表示は案内T O P画面に戻る(S 4 7)。

【0086】

ステップS 4 5の判定にて現在時刻が日替時刻を超えていなければ、判定結果がO Kになり、視聴開始処理と認証完了通知が行われる(S 4 8)。映像表示は、全画面表示に切り替わり、音声ミュートも解除され、音声が出力される(S 4 9)。また、完了通知は、端末装置7に受信される(S 5 0)。カード完了通知が受信されると、カード利用済み処理が行われる(S 5 1)。ここでは、カード処理部7 5の指示に従い、リーダライタ部7

10

20

30

40

50

3により、利用済みの情報がP E Tカード9に書き込まれる。そして、カード処理部75は、リーダライタ部73にP E Tカード9を掃き出させる(S52)。

【0087】

図11は、視聴開始後の動作を示している。視聴開始後は、デジタルテレビ5の日替処理部516により、日替判定処理が継続的に行われる(S53)。日替判定としては、現在時刻が日替時刻を超えてるか否かが判定される(S54)。現在時刻が日替時刻を超えていなければ、現在の状態が「未超過」であり、ステップS30に戻る。現在時刻が日替時刻を超えていれば、現在の状態が「超過」である。この場合、視聴終了処理が行われ(S55)、番組視聴が終了し、データ放送表示は案内TOP画面に戻る(S56)。

【0088】

以上に本実施の形態に係るデジタル放送視聴システム1の動作を説明した。本実施の形態のデジタル放送視聴システム1は、データ放送及びB M L通信を利用する構成において高いセキュリティ性を確保するように配慮されており、ヘッドエンド装置3とデジタルテレビ5の間のセキュリティ確保、デジタルテレビ5と端末装置7のセキュリティ確保、端末装置7とカード発券機11の間のセキュリティ確保が下記のようにして達成されている。

【0089】

(1)ヘッドエンド装置 - デジタルテレビ(客室)間

この部分では、ヘッドエンド装置3から送出される放送ストリームを客室内にて記憶媒体に保存され、解析されるのを防ぐことが求められる。この要求に応えるため、本実施の形態では、P M Tのコピーコントロール記述子で「C o p y n e v e r」が設定され、D V Dレコーダ等の民生記憶装置へのコピーが制限される。また、事前初期設定にてN V - R A Mに認証I Dを設定することにより、ストリーム解析だけでは看破が不可能であり、これによりセキュリティ性が確保される。

【0090】

(2)デジタルテレビ - 端末装置間

この部分では、L A N接続を適用しているので、ハブとパーソナルコンピュータを持ち込んで通信内容を丸ごとハッキングされるのを防ぐことが求められる。この要求に関し、本実施の形態では、「中間鍵データ」が、“変数”である「時刻情報」をキーに認証の都度生成される“使い捨て鍵”であり、解読は非常に困難である。

【0091】

更に、「本鍵データ」は、「本鍵生成関数」「認証I D」という2要素をキーに「中間鍵データ」からその都度生成される。「本鍵生成関数」は端末装置及びヘッドエンド装置により共有され、「認証I D」は端末装置及びデジタルテレビにより供給される。このように「本鍵データ」は、端末装置が異なる相手(ヘッドエンド装置及びデジタルテレビ)と事前にそれぞれ共有する「本鍵生成関数」「認証I D」という2つの要素から生成されており、解読は不可能に近いと考えられる。

【0092】

(3)端末装置 - カード発券機間

この部分では、P E Tカードの改造や偽造による不正を防ぐことが求められる。本実施の形態では、端末装置の内部処理が、端末側視聴制限制御部とカード処理部に別れており、すなわち、デジタルテレビと通信するアプリケーション処理(B M L通信サーバソフト)とP E T(磁気)カード読取判定処理に切り分けられており、これにより、偽造P E Tカード対策はカード発券機とP E Tカード読取判定処理の問題に限定させることが可能である。この切分けにより、システムへの侵入等に対して、上記(2)に示したような高いセキュリティ性を確保できる。

【0093】

以上に説明したように、本実施の形態では高いセキュリティ性を得ることができる。次に本実施の形態の効果について説明する。

【0094】

10

20

30

40

50

本実施の形態によれば、ヘッドエンド装置 3 がデータ放送及び有料放送コンテンツを含むデジタル放送をデジタルテレビ 5 に送出し、デジタルテレビ 5 のテレビ側視聴制限制御部 51 はデータ放送に基づいて中間鍵データを生成して端末装置 7 へ送信し、端末装置 7 の端末側視聴制限制御部 71 は課金媒体から情報が読み取られた場合に中間鍵データから本鍵データを生成してデジタルテレビ 5 に送信し、テレビ側視聴制限制御部 51 が本鍵データの認証処理を行って認証に成功すると有料放送コンテンツの視聴制限を解除する。

【0095】

このように、本発明は、デジタル放送に含まれるデータ放送と、デジタルテレビ 5 - 端末装置 7 間のデータ通信とによって、デジタル放送視聴システム 1 での視聴制限付きの有料放送提供を実現できる。デジタルテレビ 5 には、データ放送受信機能が装備されており、また、外部とのデータ通信機能も装備されており、したがって、本発明のシステムはデジタルテレビ 5 に搭載された標準機能によって実現できる。また、デジタル放送がヘッドエンド装置 3 からデジタルテレビ 5 に送られるので、複数の回路の通過による画質低下を避けることができる。さらに、デジタルテレビ 5 - 端末装置 7 間で中間鍵データ及び本鍵データが伝達されており、暗号化により不正利用を排除し、視聴を好適に制限できる。このようにして、デジタルテレビ 5 を改造せずに、画質を低下させることなく、通信解読による不正利用を防ぎつつ、視聴制限付きで有料放送を提供することができる。

【0096】

上記に関して説明を補足すると、デジタルテレビ 5 の BML による双方向通信機能は、通常は外部のセンタ等とのインターネット接続のために用いられる。しかし、本発明では、双方向通信機能が、客室内での端末装置 7 との通信に使われている。このような双方向通信機能の活用と、上述したデータ放送の利用とにより、既存のデジタルテレビの装備の範囲で、セキュリティ性の高い視聴制限を行える有料放送提供を実現している。データ放送を使って視聴が制限されており、ヘッドエンド装置 3 からデジタルテレビ 5 へは一方通行のデジタル放送が行われればよいので、同軸ケーブル等の配線設備が利用可能であり、この点でも本発明は有利である。

【0097】

また、本実施の形態によれば、データ放送にて中間鍵生成関数及び本鍵生成関数がデジタルテレビ 5 へ送られる。デジタルテレビ 5 では、中間鍵生成関数を用いて中間鍵データが生成される。中間鍵データが端末装置 7 に送られ、端末装置 7 は、予め記憶してある本鍵生成関数を用いて中間鍵データから本鍵データを生成する。一方、デジタルテレビ 5 でも、データ放送により取得した本鍵生成関数を用いて中間鍵データから本鍵データが生成される。これらの 2 つの本鍵データが照合され、両者が一致すれば、認証が成功する。このようにして、本発明によれば、中間鍵生成関数及び本鍵生成関数を用いる構成が提供され、高いセキュリティ性を確保しつつ、デジタル放送用の視聴制限を実現できる。

【0098】

また、本実施の形態によれば、中間鍵生成関数及び本鍵生成関数が、データ放送の BML コンテンツ内にスクリプトで埋め込まれる。デジタルテレビ 5 では、BML コンテンツから中間鍵生成関数及び本鍵生成関数が取得される。中間鍵生成関数及び本鍵生成関数をデータ放送に付加して好適にデジタルテレビに提供できる。

【0099】

また、本実施の形態によれば、デジタル放送に含まれる時刻情報を中間鍵生成関数で処理することにより中間鍵データが生成される。中間鍵データ生成の元データとして時刻情報を用いるので、中間鍵データが、元の時刻に応じて変化する。中間鍵データから生成される本鍵データも、元の時刻に応じて変化する。したがって、セキュリティ性を更に向上できる。

【0100】

また、本実施の形態によれば、同じ認証 ID データがデジタルテレビ 5 と端末装置 7 に記憶される。デジタルテレビ 5 と端末装置 7 の各々において、中間鍵データ及び認証 ID データを本鍵生成関数で処理することにより、本鍵データが生成される。認証 ID データ

を本鍵生成の元データにすることにより、更にセキュリティ性を向上できる。

【0101】

また、本実施の形態によれば、デジタルテレビ5には更に視聴日の切替り時刻を表す日替情報が記憶される。日替情報に基づいて視聴日が切り替わったか否かの判定が行われ(日替判定)、視聴日が変わると視聴制限が行われる。これにより、日替管理も適切に行うことができ、課金媒体を使った視聴制限を好適に行うことができる。

【0102】

また、本実施の形態によれば、テレビ側情報記憶部が、デジタルテレビのN V - R A Mにおける自主放送用の領域で構成される。デジタルテレビに標準装備されたN V - R A Mを利用して本発明のデジタル放送視聴システムとそれによる視聴制限を好適に実現できる。

10

【0103】

また、本実施の形態によれば、データ放送に課金媒体の媒体ID(上記の例ではPETカードのカードID)が付加される。課金媒体から読み取られた媒体IDが端末装置7からデジタルテレビ5に送信される。そして、データ放送に含まれる媒体IDと端末装置から受信された媒体IDが照合される。媒体IDの照合も行うので、セキュリティ性を更に向上できる。

【0104】

以上に本発明の好適な実施の形態を説明した。しかし、本発明は上述の実施の形態に限定されず、当業者が本発明の範囲内で上述の実施の形態を変形可能なことはもちろんである。

20

【産業上の利用可能性】

【0105】

以上のように、本発明にかかるデジタル放送視聴システムは、デジタルテレビを改造せずに、画質を低下させることなく、通信解読による不正利用を防ぎつつ、視聴制限付きで有料放送を提供できるという効果を有し、ホテル用デジタル放送視聴システム等として有用である。

【図面の簡単な説明】

【0106】

【図1】本発明の実施の形態におけるデジタル放送視聴システムの構成を示す図

30

【図2】デジタル放送視聴システムの構成をより詳細に示す図

【図3】ホテルに設置される場合のデジタル放送視聴システムの全体構成を示す図

【図4】本実施の形態における有料放送視聴のイメージを示す図

【図5】デジタル放送視聴システムの初期設定処理を示す図

【図6】中間鍵データの生成処理を示す図

【図7】本鍵データの生成処理を示す図

【図8】初期設定時のデジタル放送視聴システムの動作を示す図

【図9】自主放送チャンネルが選局されたときのデジタル放送視聴システムの動作を示す図

【図10】自主放送チャンネルが選局されたときのデジタル放送視聴システムの動作を示す図

40

【図11】自主放送チャンネルが選局されたときのデジタル放送視聴システムの動作を示す図

【符号の説明】

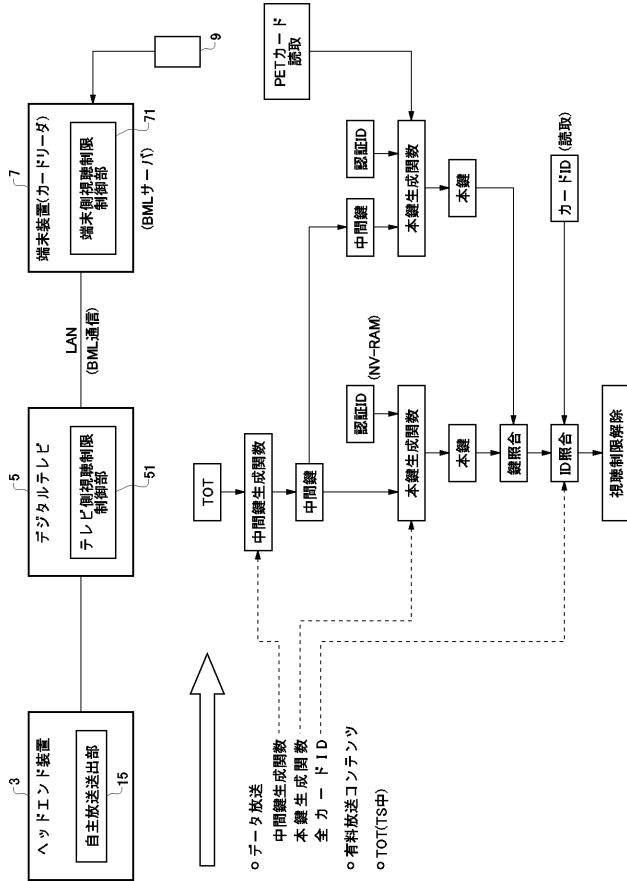
【0107】

- 1 デジタル放送視聴システム
- 3 ヘッドエンド装置
- 5 デジタルテレビ
- 7 端末装置
- 9 PETカード
- 11 カード発券機

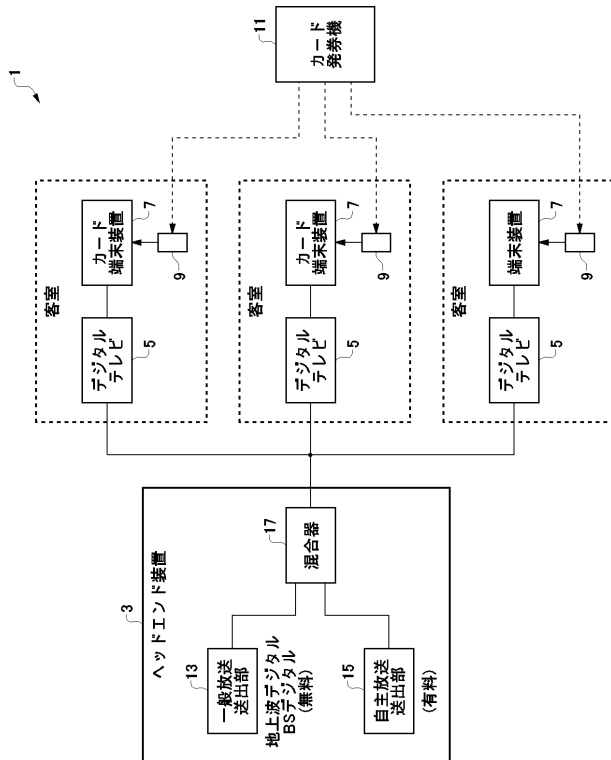
50

1 3	一般放送送出部	
1 5	自主放送送出部	
1 7	混合器	
3 1	データ放送提供部	
3 3	有料放送コンテンツ提供部	
3 5	関数付加部	
3 7	時刻情報付加部	
3 9	I D 付加部	
5 1	テレビ側視聴制限制御部	
5 3	放送受信部	10
5 5	通信部	
5 7	テレビ側情報記憶部	
7 1	端末側視聴制限制御部	
7 3	リーダライタ部	
7 5	カード処理部	
7 7	通信部	
7 9	端末側情報記憶部	
5 1 1	テレビ側登録部	
5 1 2	中間鍵生成部	
5 1 3	テレビ側本鍵生成部	20
5 1 4	鍵照合部	
5 1 5	I D 照合部	
5 1 6	日替処理部	
7 1 1	端末側登録部	
7 1 2	端末側本鍵生成部	
7 5 1	カード有無判定部	
7 5 2	正規カード判定部	

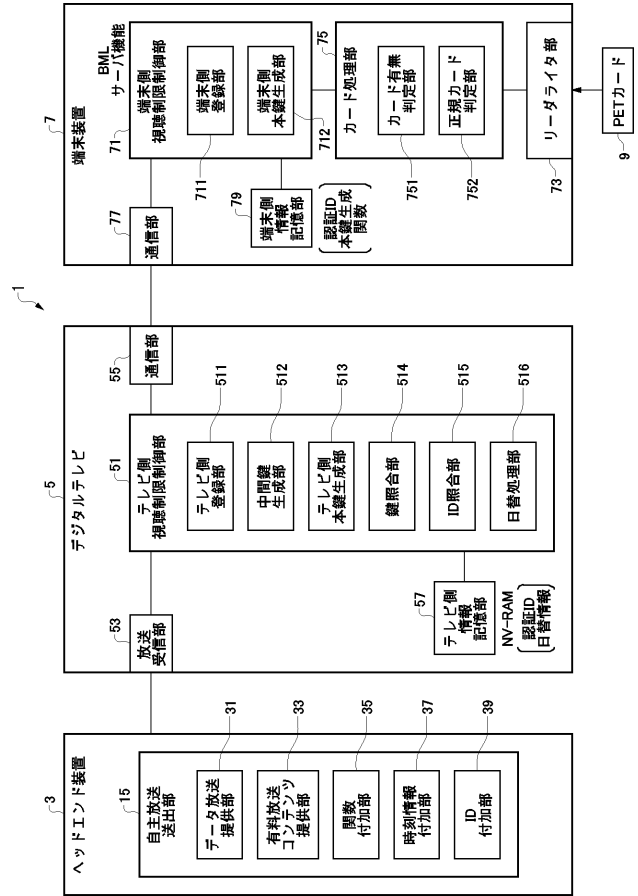
【 図 1 】



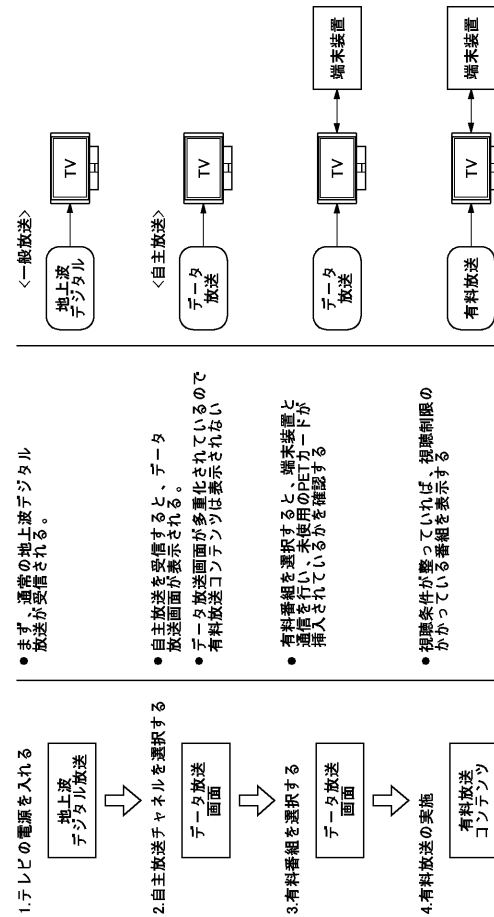
【 図 3 】



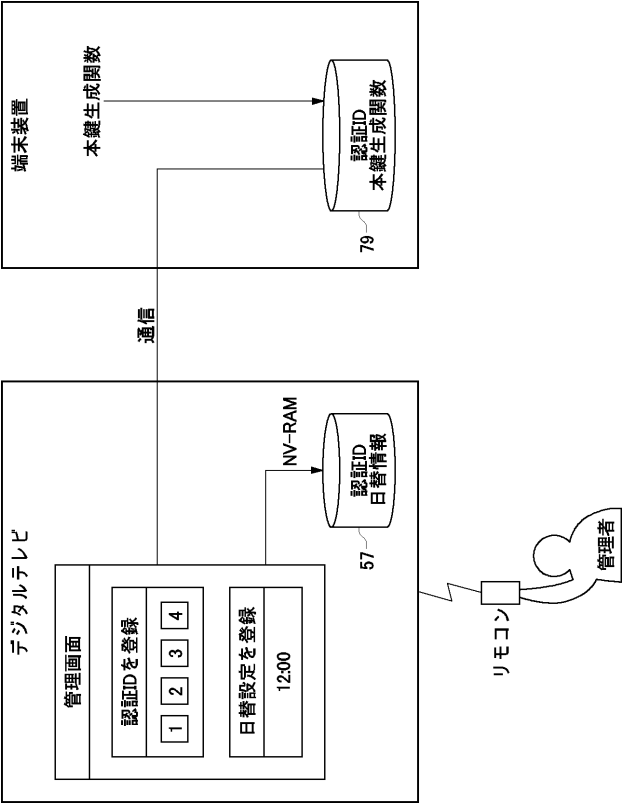
【圖 2】



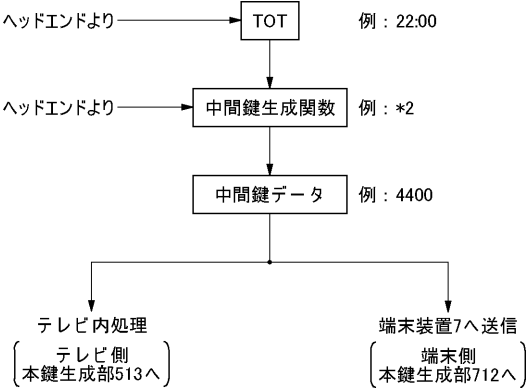
【 図 4 】



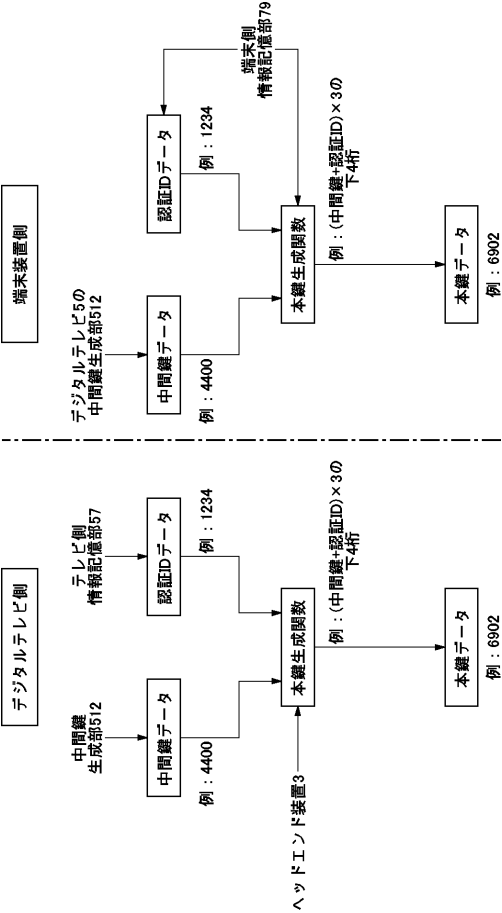
【図5】



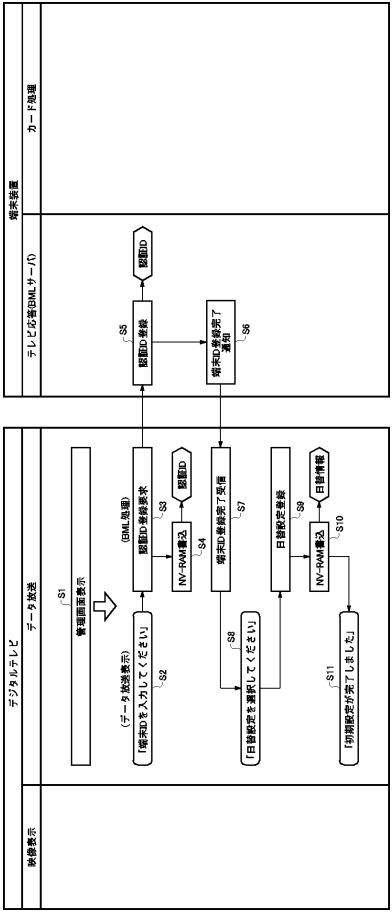
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 新井 幹秀

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

(72)発明者 柴田 真宏

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

(72)発明者 山本 俊明

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

F ターム(参考) 5C164 FA15 PA25 UA14P UB61S UC22P

5J104 AA07 AA16 AA32 BA03 EA03 EA04 EA08 EA16 EA18 JA03

KA02 MA06 NA02 NA05 NA36 NA37 PA05