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

特許第4564319号
(P4564319)

(45)発行日　平成22年10月20日(2010.10.20)　(24)登録日　平成22年8月6日(2010.8.6)

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

請求項の数 11　(全 13 頁)

(21)出願番号　特願2004-280694(P2004-280694)
(22)出願日　平成16年9月27日(2004.9.27)
(65)公開番号　特開2006-94435(P2006-94435A)
(43)公開日　平成18年4月6日(2006.4.6)
審査請求日　平成19年9月19日(2007.9.19)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100084618
弁理士　村松　貞男

最終頁に続く

(54)【発明の名称】通信装置と通信方法

(57)【特許請求の範囲】
【請求項１】
ネットワークを介し外部の第１の記憶装置および第２の記憶装置と通信を行う通信部と、
与えられたコンテンツを暗号鍵で暗号化して暗号化コンテンツを出力する暗号部と、
予め静的デバイス鍵と動的デバイス鍵を記憶するメモリ部と、
前記暗号鍵を前記静的デバイス鍵と前記動的デバイス鍵とで暗号化して暗号化暗号鍵を生成し、前記暗号化暗号鍵を前記通信部を介してネットワーク上の前記第１の記憶装置に記録し、前記暗号部が暗号化した前記暗号化コンテンツを前記通信部を介してネットワーク上の前記第２の記憶装置に記録する鍵暗号部と、
ユーザの再生指示に応じて、前記第１の記憶装置から前記暗号化暗号鍵を前記通信部を介して読み出し、前記静的デバイス鍵及び前記動的デバイス鍵により前記暗号鍵へと復号する鍵復号部と、
前記第２の記憶装置から前記通信部を介して前記暗号化コンテンツを読み出し、前記鍵復号部が復号した前記暗号鍵により前記コンテンツへと復号する復号部と、
前記復号部が復号した前記コンテンツを再生する再生部と、
前記暗号鍵を廃止する際に、前記記憶されている動的デバイス鍵を更新する鍵更新部とを具備することを特徴とする通信装置。
【請求項２】
前記鍵暗号部及び前記鍵復号部は回路基板に設けられていることを特徴とし、

前記回路基板が新しいものに交換された際に、以前の回路基板の前記静的デバイス鍵と前記動的デバイス鍵とを、新しい回路基板に復旧させる復旧部を更に有することを特徴とする請求項１記載の通信装置。

【請求項３】

前記復旧部は前記回路基板上に設けられており、以前の回路基板の前記静的デバイス鍵については、ユーザ又はサービスマンにより入力され、以前の回路基板の前記動的デバイス鍵については、前記通信部が前記ネットワーク上の前記第１の記憶装置に格納した前記動的デバイス鍵を前記復旧部が前記通信部及び前記ネットワークを介して取得して保存することで、以前の回路基板を復旧することを特徴とする請求項２記載の通信装置。

【請求項４】

前記コンテンツを反復して記録するための前記ネットワーク上の前記第２の記憶装置を登録し、前記暗号化暗号鍵を反復して記録するための前記ネットワーク上の前記第１の記憶装置を登録する登録部を更に有しており、

前記復旧部は、前記登録部の登録に基づいて、以前の回路基板の前記動的デバイス鍵については、前記ネットワーク上の前記第１の記憶装置に格納されている以前の前記動的デバイス鍵を前記通信部及び前記ネットワークを介して取得して保存することで、以前の回路基板を復旧することを特徴とする請求項３記載の通信装置。

【請求項５】

前記鍵更新部は、前記コンテンツがその後にある機器から別の機器に移動されたか、または削除された場合に、前記ネットワーク上の前記暗号化コンテンツを復号不能とすることで再生不能とするべく、前記記憶領域の動的デバイス鍵を新たな動的デバイス鍵に変更し、更に、現時点で再生可能な全ての暗号化コンテンツに応じた暗号化暗号鍵を前記ネットワーク上の第１の記憶装置に記録することを特徴とする請求項３記載の通信装置。

【請求項６】

前記静的デバイス鍵と前記動的デバイス鍵とを記憶している前記メモリ部は、不揮発性メモリであることを特徴とする請求項１記載の通信装置。

【請求項７】

放送信号を受けて選局し選局信号を出力するチューナ部と、

前記チューナ部からの選局信号を復調して得られる映像音声信号を前記コンテンツとして、前記暗号部に供給する復調部とを更に有することを特徴とする請求項１記載の通信装置。

【請求項８】

前記復調部が出力した前記映像音声信号をＭＰＥＧデコードして得られた映像音声信号を前記コンテンツとして前記暗号部に供給する信号処理部を更に有することを特徴とする請求項７記載の通信装置。

【請求項９】

前記通信部は、前記ネットワーク上の前記第１の記憶装置及び前記第２の記憶装置と認証処理を行い、認証が成功した後に前記暗号化コンテンツ又は暗号化暗号鍵を送信することを特徴とする請求項１記載の通信装置。

【請求項１０】

前記通信部は、ＬＡＮ、ＵＳＢ端子、ｉ．Link端子の少なくとも一つを含むことを特徴とする請求項１記載の通信装置。

【請求項１１】

通信装置部において、与えられたコンテンツを暗号鍵で暗号化して暗号化コンテンツを出力し、

予め静的デバイス鍵と動的デバイス鍵とを前記通信装置部内のメモリ部に記憶しておき、

前記通信装置において、前記暗号鍵を前記静的デバイス鍵と前記動的デバイス鍵とで暗号化して暗号化暗号鍵を生成し、

前記通信装置とネットワーク上の第１の記憶装置およびネットワーク上の第２の記憶装

置との間で通信を行って、前記暗号化暗号鍵をネットワーク上の前記第１の記憶装置に記録し、前記暗号化コンテンツをネットワーク上の前記第２の記憶装置に記録し、
ユーザの再生指示に応じて、前記第１の記憶装置と前記第２の記憶装置との間で通信を行って、前記第１の記憶装置から前記暗号化暗号鍵を読み出し、前記通信装置において前記静的デバイス鍵及び前記動的デバイス鍵により前記暗号鍵へと復号し、
前記通信装置と前記第２の記憶装置との間で通信を行い、前記第２の記憶装置から前記ネットワークを介して前記暗号化コンテンツを読み出し、前記通信装置において前記復号した暗号鍵により前記コンテンツへと復号し、
前記通信装置において前記復号したコンテンツを再生し、
前記通信装置において前記暗号鍵を廃止する際に、前記記憶されている動的デバイス鍵を更新することを特徴とする通信方法。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、ネットワーク機能をもつテレビジョン装置等の通信装置に関し、特に、暗号復号機能を用いることでネットワーク経由による映像音声信号のセキュリティを向上させる通信装置及び通信方法に関する。

【背景技術】

【０００２】

周知のように、近年では、テレビジョン放送のデジタル化が推進されている。例えば、日本国内においては、ＢＳ（Broadcasting Satellite）デジタル放送及び１１０度ＣＳ（Communication Satellite）デジタル放送等の衛星デジタル放送だけでなく、地上デジタル放送も開始されている。

【０００３】

そして、このようなデジタルテレビジョン放送を受信するデジタル通信装置にあっては、映像や音声情報をデジタル信号で扱うことができるため、コンテンツ情報の記録、再生、検索、管理等の処理や電子番組情報の活用も容易に行うことが可能となっている。この例として、特許文献１には、ディジタルテレビ放送から電子番組情報を取得し活用する技術が開示されている。

【特許文献１】特開２００２－１４２１６３号公報。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

しかしながら、特許文献１においては、取得したディジタルコンテンツをネットワークを介してどのように利用するかが示されておらず、更に、ネットワークを利用する際に用いられる暗号復号方法については何ら示されていないという問題がある。

【０００５】

本発明は、コンテンツ情報を暗号復号機能を用いることでセキュリティを維持しながらネットワークを介して記録装置等に供給することができる通信装置及び通信方法を提供すること目的とする。

【課題を解決するための手段】

【０００６】

本発明の一実施形態である通信装置は、
ネットワークを介し外部の第１の記憶装置および第２の記憶装置と通信を行う通信部（６９－７２）と、
与えられたコンテンツ（Ｃ）を暗号鍵（K_C）で暗号化して暗号化コンテンツ（K_C・Ｃ）を出力する暗号部（８１）と、
予め静的デバイス鍵（ｋ）と動的デバイス鍵（Ｋ１）を記憶するメモリ（７４）部と、
前記暗号鍵（K_C）を前記静的デバイス鍵（ｋ）と前記動的デバイス鍵（Ｋ１）とで暗号化して暗号化暗号鍵（ｋ・Ｋ１・K_C）を生成し、前記暗号化暗号鍵（ｋ・Ｋ１・K_C

）を前記通信部を介してネットワーク上の前記第１記憶装置（２８）に記録し、前記暗号部が暗号化した前記暗号化コンテンツ（K_C・Ｃ）を前記通信部を介してネットワーク上の前記第２記憶装置（２５）に記録する鍵暗号部（７３）と、

ユーザの再生指示に応じて、前記第１記憶装置（２８）から前記暗号化暗号鍵（ｋ・Ｋ１・K_C）を前記通信部を介して読み出し、前記静的デバイス鍵（ｋ）及び前記動的デバイス鍵（Ｋ１）により前記暗号鍵（K_C）へと復号する鍵復号部（７３）と、

前記第２記憶装置（２５）から前記通信部を介して前記暗号化コンテンツ（K_C・Ｃ）を読み出し、前記鍵復号部が復号した前記暗号鍵（K_C）により前記コンテンツ（Ｃ）へと復号する復号部（８１）と、

前記復号部が復号した前記コンテンツ（Ｃ）を再生する再生部（４７）と、前記暗号鍵（K_C）を廃止する際に、前記記憶されている動的デバイス鍵を更新する鍵更新部（７３）とを具備することを特徴とする通信装置である。

【発明の効果】

【０００７】

上記した通信装置においては、例えば、ネットワーク機能を備えたテレビジョン装置であって、一例としてデジタル放送信号に応じたコンテンツ情報（Ｃ）をネットワーク上の例えばハードディスクレコーダ（２５）等に転送して録画する際に、このコンテンツ情報を暗号鍵（K_C）で暗号化した暗号化コンテンツ情報（K_C・Ｃ）として、ハードディスクレコーダ等に転送し記録する。

【０００８】

この際に、暗号化に供した暗号鍵（K_C）は、不揮発性メモリ７４等に保存された静的デバイス鍵（ｋ）と動的デバイス鍵（Ｋ１～）の二つにより暗号化され、暗号化暗号鍵（ｋ・Ｋ１・K_C）として、ネットワーク上のＰＣやハードディスク等の所定領域（２８）に保存される。

【０００９】

このようにコンテンツ情報の暗号鍵を暗号化してネットワーク上に保存し、コンテンツ情報も暗号化してネットワーク上の装置に記録することで、データを安全にネットワーク上に保存することができる。又、コンテンツ情報の暗号鍵（K_C）は、テレビジョン装置側では特に保存はしておらず、コンテンツ情報を復号する際は、ネットワーク上から再び取得するものである。

【００１０】

すなわちテレビジョン装置において、コンテンツ情報の再生の際には、ネットワーク上から暗号化暗号鍵（ｋ・Ｋ１・K_C）と暗号化コンテンツ情報（K_C・Ｃ）とを再び回収し、更に、不揮発性メモリ７４等に保存されている静的デバイス鍵（ｋ）と動的デバイス鍵（Ｋ１～）の二つにより、コンテンツ情報の暗号鍵（K_C）を復旧する。そして、復旧した暗号鍵（K_C）により、暗号化コンテンツ情報（K_C・Ｃ）を復元した上で、再生処理に供するものである。

【００１１】

ここで、静的デバイス鍵（ｋ）は、内容を変更することのない回路基板に応じた暗号鍵であり、一方、動的デバイス鍵（Ｋ１～Ｋｎ）は、例えば、コンテンツ情報を移動したり削除したりして、鍵を無効とするときに、その値をＫ１からＫ２、Ｋ２からＫ３と、そのつど更新されて使用されるものである。又、この動的デバイス鍵の更新情報は、テレビジョン装置の不揮発性メモリ７４において更新されるだけではなく、上述したネットワーク上の所定領域（２５）における暗号化暗号鍵（ｋ・Ｋ１・K_C…）の履歴についても更新されるものである。これにより、ネットワーク上のセキュリティや著作権を保護しながら、コピー不可のコンテンツ情報をネットワーク内に自由に移動する等の処理が可能となるものである。

【００１２】

又、更に、本発明の一実施形態においては、このような静的デバイス鍵（ｋ）や動的デバイス鍵（Ｋ１～Ｋｎ）を搭載したデジタルボードに故障が生じたりして新しいものと交

換した際に、これらの鍵を新しいデジタルボードにおいて迅速に復旧するべく、復旧機能をもっているものである。すなわち、新しいデジタルボードにおいても、以前の静的デバイス鍵（ｋ）をサービスマンが入力するとこれを保存したり、更新された現在の動的デバイス鍵（Ｋ１～Ｋｎ）をネットワーク上から回収して復旧を行い、過去の履歴を継続した状態で、ネットワーク上の適正な暗号化コンテンツだけを再生することを可能とするものである。

【発明を実施するための最良の形態】

【００１３】

以下、この発明の実施の形態について図面を参照して詳細に説明する。

【００１４】

＜本発明に係るネットワーク機能を備えたテレビジョン装置＞

初めに、本発明に係る通信装置であるネットワーク機能を備えたテレビジョン装置の一例を図面を用いて以下に説明する。図２は、本発明の一実施形態に係るデジタルテレビジョン通信装置の構成の一例を示すブロック図、図３は、本発明の一実施形態に係るデジタルテレビジョン通信装置のリモートコントローラの一例を示すブロック図である。

【００１５】

すなわち、デジタルテレビジョン通信装置１１は、主として、薄型のキャビネット１２と、このキャビネット１２を起立させて支持する支持台１３とから構成されている。そして、キャビネット１２には、例えば液晶表示パネル等でなる平面パネル型の映像表示器１４、スピーカ１５、操作部１６、リモートコントローラ１７から送信される操作情報を受ける受光部１８等が設置されている。

【００１６】

又、このデジタルテレビジョン通信装置１１には、例えばＳＤ（Secure Digital）メモリカード、ＭＭＣ（Multimedia Card）及びメモリスティック等のメモリカード、又、更に、例えば契約情報等の記録されたメモリカード（ＩＣカード）等のメモリカード１９が着脱可能となっている。これらのメモリカード１９に対して番組や写真等の情報の記録再生が行なわれたり、情報の記録再生が行なわれるようになっている。

【００１７】

又、このデジタルテレビジョン通信装置１１は、第１のＬＡＮ（Local Area Network）端子２１、第２のＬＡＮ端子２２、ＵＳＢ（Universal Serial Bus）端子２３及びｉ．Link端子２４を備えている。

【００１８】

このうち、第１のＬＡＮ端子２１は、ＬＡＮ対応ＨＤＤ専用ポートとして使用されるもので、接続されたＮＡＳ（Network Attached Storage）であるＬＡＮ対応のＨＤＤ２５に対して、イーサネット（登録商標）により情報の記録再生を行なうために使用される。

【００１９】

このように、ＬＡＮ対応ＨＤＤ専用ポートとしての第１のＬＡＮ端子２１を設けることにより、他のネットワーク環境やネットワーク使用状況等に影響されることなく、ＨＤＤ２５に対してハイビジョン画質による番組の情報記録を安定して行なうことができる。

【００２０】

又、第２のＬＡＮ端子２２は、イーサネット（登録商標）を用いた一般的なＬＡＮ対応ポートとして使用されるもので、例えばハブ２６を介して、ＬＡＮ対応のＨＤＤ２７、ＰＣ（Personal Computer）２８、ＨＤＤ内蔵のＤＶＤ（Digital Versatile Disk）レコーダ２９等の機器を接続し、これらの機器と情報伝送を行なうために使用される。

【００２１】

なお、ＤＶＤレコーダ２９については、第２のＬＡＮ端子２２を介して通信されるデジタル情報が制御系のみの情報であるため、デジタルテレビジョン通信装置１１との間でアナログの映像及び音声情報を伝送するために、専用のアナログ伝送路３０を設ける必要がある。

【００２２】

更に、この第２のＬＡＮ端子２２は、ハブ２６に接続されたブロードバンドルータ３１を介して、例えばインターネット等のネットワーク３２に接続し、そのネットワーク３２を介してＰＣ３３や携帯電話３４等と情報伝送を行なうために使用される。

【００２３】

又、上記ＵＳＢ端子２３は、一般的なＵＳＢ対応ポートとして使用されるもので、例えばハブ３５を介して、携帯電話３６、デジタルカメラ３７、メモリカードに対するカードリーダ／ライタ３８、ＨＤＤ３９、キーボード４０等のＵＳＢ機器を接続し、これらのＵＳＢ機器と情報伝送を行なうために使用される。

【００２４】

更に、上記ｉ．Link端子２４は、例えばＡＶ－ＨＤＤ４１、Ｄ（Digital）－ＶＨＳ（Video Home System）４２等をシリアル接続し、これらの機器と情報伝送を行なうために使用される。

【００２５】

図２は、上記したデジタルテレビジョン通信装置１１の主要な信号処理系を示している。すなわち、ＢＳ／ＣＳデジタル放送受信用のアンテナ４３で受信した衛星デジタルテレビジョン放送信号は、入力端子４４を介して衛星デジタル放送用のチューナ４５に供給されることにより、所望のチャンネルの放送信号が選局される。

【００２６】

そして、このチューナ４５で選局された放送信号は、ＰＳＫ（Phase Shift Keying）復調器４６に供給されて、デジタルの映像信号及び音声信号に復調された後、信号処理部４７に出力される。

【００２７】

又、地上波放送受信用のアンテナ４８で受信した地上デジタルテレビジョン放送信号は、入力端子４９を介して地上デジタル放送用のチューナ５０に供給されることにより、所望のチャンネルの放送信号が選局される。

【００２８】

そして、このチューナ５０で選局された放送信号は、ＯＦＤＭ（Orthogonal Frequency Division Multiplexing）復調器５１に供給されて、デジタルの映像信号及び音声信号に復調された後、上記信号処理部４７に出力される。

【００２９】

又、上記地上波放送受信用のアンテナ４８で受信した地上アナログテレビジョン放送信号は、入力端子４９を介して地上アナログ放送用のチューナ５２に供給されることにより、所望のチャンネルの放送信号が選局される。そして、このチューナ５２で選局された放送信号は、アナログ復調器５３に供給されてアナログの映像信号及び音声信号に復調された後、上記信号処理部４７に出力される。

【００３０】

ここで、上記信号処理部４７は、ＰＳＫ復調器４６及びＯＦＤＭ復調器５１からそれぞれ供給されたデジタルの映像信号及び音声信号に対して、選択的に所定のデジタル信号処理、例えば、ＭＰＥＧ２のデコード処理を施し、グラフィック処理部５４及び音声処理部５５に出力している。

【００３１】

更に、グラフィック処理部５４は、信号処理部４７から供給されるデジタルの映像信号に、ＯＳＤ（On Screen Display）信号生成部５７で生成されるＯＳＤ信号を重畳して出力する機能を有する。このグラフィック処理部５４は、信号処理部４７の出力映像信号と、ＯＳＤ信号生成部５７の出力ＯＳＤ信号とを選択的に出力すること、又、両出力をそれぞれ画面の半分を構成するように組み合わせて出力することができる。

【００３２】

そして、グラフィック処理部５４から出力されたデジタルの映像信号は、映像処理部５８に供給される。この映像処理部５８は、入力されたデジタルの映像信号を、上記映像表示器１４で表示可能なフォーマットのアナログ映像信号に変換した後、映像表示器１４に

出力して映像表示させるとともに、出力端子５９を介して外部に導出させる。
【００３３】
又、上記音声処理部５５は、入力されたデジタルの音声信号を、上記スピーカ１５で再生可能なフォーマットのアナログ音声信号に変換した後、スピーカ１５に出力して音声再生させるとともに、出力端子６０を介して外部に導出させる。
【００３４】
ここで、このデジタルテレビジョン通信装置１１は、上記した各種の受信動作を含むその全ての動作を制御部６１によって統括的に制御されている。この制御部６１は、ＣＰＵ（Central Processing Unit）等を内蔵しており、上記操作部１６からの操作情報を受け、又は、リモートコントローラ１７から送出された操作情報を上記受光部１８を介して受信し、その操作内容が反映されるように各部をそれぞれ制御している。
【００３５】
この場合、制御部６１は、主として、そのＣＰＵが実行する制御プログラムを格納したＲＯＭ（Read Only Memory）６２と、該ＣＰＵに作業エリアを提供するＲＡＭ（Random Access Memory）６３と、各種の設定情報及び制御情報等が格納される不揮発性メモリ６４とを利用している。
【００３６】
又、この制御部６１は、カードＩ／Ｆ（Interface）６５を介して、上記メモリカード１９が装着可能なカードホルダ６６に接続されている。これによって、制御部６１は、カードホルダ６６に装着されたメモリカード１９と、カードＩ／Ｆ６５を介して情報伝送を行なうことができる。更に、上記制御部６１は、図示しないカードＩ／Ｆとカードホルダとを介して、図示しない第２のメモリカードが装着可能に接続されている。これにより、制御部６１は、第２のメモリカードと情報伝送を行なうことができる。
【００３７】
又、上記制御部６１は、通信Ｉ／Ｆ６９を介して第１のＬＡＮ端子２１に接続されている。これにより、制御部６１は、第１のＬＡＮ端子２１に接続されたＬＡＮ対応のＨＤＤ２５と、通信Ｉ／Ｆ６９を介して情報伝送を行なうことができる。この場合、制御部６１は、ＤＨＣＰ（Dynamic Host Configuration Protocol）サーバ機能を有し、第１のＬＡＮ端子２１に接続されたＬＡＮ対応のＨＤＤ２５にＩＰ（Internet Protocol）アドレスを割り当てて制御している。
【００３８】
更に、上記制御部６１は、通信Ｉ／Ｆ７０を介して第２のＬＡＮ端子２２に接続されている。これにより、制御部６１は、第２のＬＡＮ端子２２に接続された各機器（図１参照）と、通信Ｉ／Ｆ７０を介して情報伝送を行なうことができる。
【００３９】
又、上記制御部６１は、ＵＳＢ Ｉ／Ｆ７１を介して上記ＵＳＢ端子２３に接続されている。これにより、制御部６１は、ＵＳＢ端子２３に接続された各機器（図１参照）と、ＵＳＢ Ｉ／Ｆ７１を介して情報伝送を行なうことができる。
【００４０】
更に、上記制御部６１は、ｉ．Link Ｉ／Ｆ７２を介してｉ．Link端子２４に接続されている。これにより、制御部６１は、ｉ．Link端子２４に接続された各機器（図１参照）と、ｉ．Link Ｉ／Ｆ７２を介して情報伝送を行なうことができる。
【００４１】
更に、各チューナ部４５，５０，５２、各復調器４６，５１，５３、制御部６１、信号処理部４７等が搭載されたデジタルボード１０の構成の一例が、図２に示されている。このデジタルボード１０の構成は一例であって、他の回路を含むものでもよく、又、図面中の各ブロックは、必ずしもデジタルボード１０に設けなくともよく、他の基板上で構成されることも可能である。
【００４２】
更に、上記制御部６１は、デジタルボード１０に故障が生じてこれを交換した後に、鍵

管理システムを復旧させるための復旧機能と、この鍵管理システムを管理する復旧部・鍵管理部７３と、鍵管理システムに用いる静的デバイス鍵ｋ，動的デバイス鍵Ｋ１乃至Ｋｎを格納する不揮発性メモリ７４と、テレビジョン通信装置１１からのコンテンツ情報を記録するためのネットワーク上の記録再生機器を登録する登録部８０を有している。又、暗号化処理、復号処理のために、信号処理部４７に接続されて暗号復号部８１が設けられている。

【００４３】

図３は、上記リモートコントローラ１７の外観を示している。このリモートコントローラ１７には、主として、電源キー１７ａ、入力切換キー１７ｂ、衛星デジタル放送チャンネルのダイレクト選局キー１７ｃ、地上波放送チャンネルのダイレクト選局キー１７ｄ、クイックキー１７ｅ、カーソルキー１７ｆ、決定キー１７ｇ、番組表キー１７ｈ、ページ切換キー１７ｉ、faceネット（ナビゲーション）キー１７ｊ、戻るキー１７ｋ、終了キー１７ｌ、青，赤，緑，黄のカラーキー１７ｍ、チャンネルアップダウンキー１７ｎ、音量調整キー１７ｏ、メニューキー１７ｐ等が設けられている。

【００４４】

（暗号鍵システム）

次に、上記したデジタルテレビジョン通信装置における、ネットワークに応じた、コンテンツ情報の暗号復号システムを図面を用いて詳細に説明する。図４は、本発明の一実施形態に係るデジタルテレビジョン通信装置の鍵管理方法の一例を説明するシステム図、図５は、本発明の一実施形態に係るデジタルテレビジョン通信装置の暗号復号処理の一例を説明するフローチャート、図６は、本発明の一実施形態に係るデジタルテレビジョン通信装置の暗号復号処理の一例を説明するフローチャートである。

【００４５】

すなわち、上記した通信装置においては、例えば、ネットワーク機能を備えたテレビジョン装置であって、一例としてデジタル放送信号に応じたコンテンツ情報（Ｃ）をネットワーク上の例えばＨＤＤ２５等に転送して録画する際に、暗号復号処理が施される。すなわち、このコンテンツ情報を暗号鍵（K_C）で暗号化した暗号化コンテンツ情報（K_C・Ｃ）として、ハードディスクレコーダ等に転送して記録するものである。

【００４６】

この際に、暗号化に供した暗号鍵（K_C）は、不揮発性メモリ７４等に保存された静的デバイス鍵（ｋ）と動的デバイス鍵（Ｋ１～）の二つにより暗号化され、暗号化暗号鍵（ｋ・Ｋ１・K_C）として、ネットワーク上のＰＣやハードディスク等の所定領域２５に保存される。

【００４７】

このようにコンテンツ情報の暗号鍵（K_C）を暗号化してネットワーク上に保存し、コンテンツ情報も暗号化してネットワーク上の装置に記録することで、データを安全にネットワーク上に保存することができる。又、コンテンツ情報の暗号鍵（K_C）は、テレビジョン装置側では特に保存はしておらず、コンテンツ情報を復号する際は、ネットワーク上から再び取得するものである。

【００４８】

すなわちテレビジョン装置において、又は、他のネットワーク上の機器がコンテンツ情報の再生の際には、ネットワーク上から暗号化暗号鍵（ｋ・Ｋ１・K_C）と暗号化コンテンツ情報（K_C・Ｃ）とを再び回収し、更に、不揮発性メモリ７４等に保存されている静的デバイス鍵（ｋ）と動的デバイス鍵（Ｋ１～）の二つにより、コンテンツ情報の暗号鍵（K_C）を復旧する。そして、復旧した暗号鍵（K_C）により、暗号化コンテンツ情報（K_C・Ｃ）を復元した上で、再生処理に供するものである。

【００４９】

ここで、静的デバイス鍵（ｋ）は、内容を変更することのない回路基板に応じた暗号鍵であり、一方、動的デバイス鍵（Ｋ１～Ｋｎ）は、例えば、コンテンツ情報を移動したり削除したりして、鍵を無効とするときに、その値をＫ１からＫ２、Ｋ２からＫ３と、その

つど更新されて使用されるものである。又、この動的デバイス鍵の更新情報は、テレビジョン装置の不揮発性メモリ７４において更新されるだけではなく、上述したネットワーク上の所定領域２５における暗号化暗号鍵（ｋ・Ｋ１・K_C…）の履歴についても更新されるものである。これにより、ネットワーク上のセキュリティや著作権を保護しながら、コピー不可のコンテンツ情報をネットワーク内に自由に移動する等の処理が可能となるものである。

【００５０】

次に、図４のシステムズ及び図５のフローチャートを用いて、時系列的に暗号処理、復号処理を説明する。すなわち、デジタルテレビジョン放送受信装置１１において、制御部６１及び鍵管理部７３の制御に基づき、コンテンツ情報を暗号化して記録せよとの指示信号等があれば（Ｓ１）、コンテンツ情報Ｃ１をコンテンツ情報Ｃ１の暗号鍵K_{C1}で暗号化する（Ｓ２）。この時、コンテンツ情報は、チューナ部４５，５０，５２等により選局された放送信号を、各復調部４６，５１，５３等により復調され、更に、信号処理部４７において、例えば、ＭＰＥＧ２デコード処理された出力である。又、例えば、各インタフェース６９乃至７２から与えられたものであることも好適である。次に、このコンテンツ情報Ｃ１をコンテンツ情報Ｃ１の暗号鍵K_{C1}で暗号化する。ここで、この暗号鍵K_{C1}は、図示しない鍵生成部でそのつど生成することが好適であるが、これに限定されるものではない。又、必ずしも生成した暗号鍵K_{C1}を保存する必要はなく、基本的にネットワーク上に保存するものである。

【００５１】

次に、暗号鍵K_{C1}で暗号化された暗号化コンテンツK_{C1}・Ｃ１を、登録部８０で登録されたネットワーク上の例えばＨＤＤ２５へと記録する（Ｓ３）。これと同時に、暗号鍵K_{C1}も静的デバイス鍵ｋと動的デバイス鍵Ｋ１で暗号化して、暗号化暗号鍵ｋ・Ｋ１・K_{C1}として、登録部８０で登録されたネットワーク上の例えばＰＣ２８へと通信Ｉ／Ｆ部６９を介して転送され保存される（Ｓ３）。ただし、通信部である通信Ｉ／Ｆ部６９等では、ネットワーク上の装置と認証処理を行い、認証が成功した後に暗号化コンテンツ信号や暗号化暗号鍵を送信するものである。

【００５２】

そして、次に、ユーザ等の命令により、暗号化して記録されたコンテンツ情報K_{C1}・Ｃ１を再生する場合は（Ｓ４）、登録部８０で登録された記録領域である例えばＰＣ２８から、暗号化暗号鍵ｋ・Ｋ１・K_{C1}を取得し、不揮発性メモリ７４内の静的デバイス鍵ｋ及び動的デバイス鍵Ｋ１から復元する（Ｓ５）。そして、復元された暗号鍵K_{C1}により、通信部である通信Ｉ／Ｆ７０から取得した暗号化コンテンツ情報K_{C1}・Ｃ１を復号して再生するものである（Ｓ６）。

【００５３】

なお、鍵更新部である鍵管理部７３は、コンテンツ信号（例えば．Ｃ２）がその後に移動や削除をした際に、ネットワーク上の暗号化コンテンツ信号（例えば．Ｃ２）を復号不能とすることで再生不能とするべく、記憶領域７４の動的デバイス鍵Ｋ１を新たな動的デバイス鍵Ｋ２に変更する。そして、図４に示すように、ネットワーク上のハードディスクドライバ２５における暗号化暗号鍵として、現時点で再生可能な全ての暗号化コンテンツ信号（例えば、Ｃ１，Ｃ３，Ｃ４）に応じた暗号化暗号鍵（ｋ・Ｋ２・K_{C1}、ｋ・Ｋ２・K_{C3}、ｋ・Ｋ２・K_{C4}）を記録するものである。これにより、再生不能であるべきコンテンツ情報Ｃ２以外のコンテンツ情報は、動的デバイス鍵が更新された後も再生可能となる。

【００５４】

（暗号鍵システムの復旧処理）

次に、上記の暗号鍵システムのための構成が設けられたデジタルボード１１が故障等により新しいものに交換された場合に、上記した静的デバイス鍵ｋや動的デバイス鍵Ｋ１～Ｋｎを復旧する処理について、図６のフローチャートを用いて以下に詳細に説明する。

【００５５】

すなわち、本発明の一実施形態においては、このような静的デバイス鍵ｋや動的デバイス鍵Ｋ１～Ｋｎを搭載したデジタルボードに故障が生じたりすると、他の部品と同様に、例えば、サービスマン等により新しいものと交換されることとなる。その際に、これらの鍵を新しいデジタルボードにおいて迅速に復旧する必要があり、制御部６１の復旧部７３は、この復旧処理を行うものである。つまり、新しいデジタルボードにおいても、以前の静的デバイス鍵ｋをサービスマンが入力するとこれを保存したり、更新された現在の動的デバイス鍵Ｋ１～Ｋｎをネットワーク上から回収して復旧を行い、過去の履歴を継続した状態で、ネットワーク上の適正な暗号化コンテンツ情報だけを再生することを保障して、一貫した著作権の保護を可能としている。

【００５６】

すなわち、図６のフローチャートに示すように、デジタルテレビジョン受信装置１１において、故障等によりデジタルボード１１の交換が必要となれば（Ｓ１１）、サービスマン等が、古いデジタルボードを新しいものに交換し、その際に、サービスマンの作業として、古いデジタルボードの静的デバイス鍵ｋを新しいデジタルボードに書き込む（Ｓ１２）。更に、新しいデジタルボードを通電して、復旧部７３の復旧プログラムを起動させる（Ｓ１３）。ここで、デジタルボードの各機能の動作チェックが自動的に行われ、動作チェックの結果がＯＫであれば（Ｓ１４）、復旧プログラムの働きにより、登録部８０により登録されているネットワーク上の所定領域２８から、現在の動的デバイス鍵Ｋｎ（例えば、現在はＫ２）を取得し、新しいデジタルボード１０の不揮発性メモリ７４に書き込む（Ｓ１５）。

【００５７】

このような復旧部７３の復旧動作により、以前のデジタルボードの動的デバイス鍵Ｋ１～Ｋｎが、静的デバイス鍵ｋと共に復旧し、以前のコンテンツ情報の履歴情報が反映された形でコンテンツ情報の使用管理が継続して行われるものである。

【００５８】

以上記載した様々な実施形態により、当業者は本発明を実現することができるが、更にこれらの実施形態の様々な変形例を思いつくことが当業者によって容易であり、発明的な能力をもたなくとも様々な実施形態へと適用することが可能である。従って、本発明は、開示された原理と新規な特徴に矛盾しない広範な範囲に及ぶものであり、上述した実施形態に限定されるものではない。

【図面の簡単な説明】

【００５９】

【図１】本発明の一実施形態に係るデジタルテレビジョン通信装置とこれを中心に構成されるネットワークシステムの一例を概略的に説明する説明図。

【図２】本発明の一実施形態に係るデジタルテレビジョン通信装置の構成の一例を示すブロック図。

【図３】本発明の一実施形態に係るデジタルテレビジョン通信装置のリモートコントローラの一例を示すブロック図。

【図４】本発明の一実施形態に係るデジタルテレビジョン通信装置の鍵管理方法の一例を説明するシステム図。

【図５】本発明の一実施形態に係るデジタルテレビジョン通信装置の暗号復号処理の一例を説明するフローチャート。

【図６】本発明の一実施形態に係るデジタルテレビジョン通信装置の暗号復号処理の一例を説明するフローチャート。

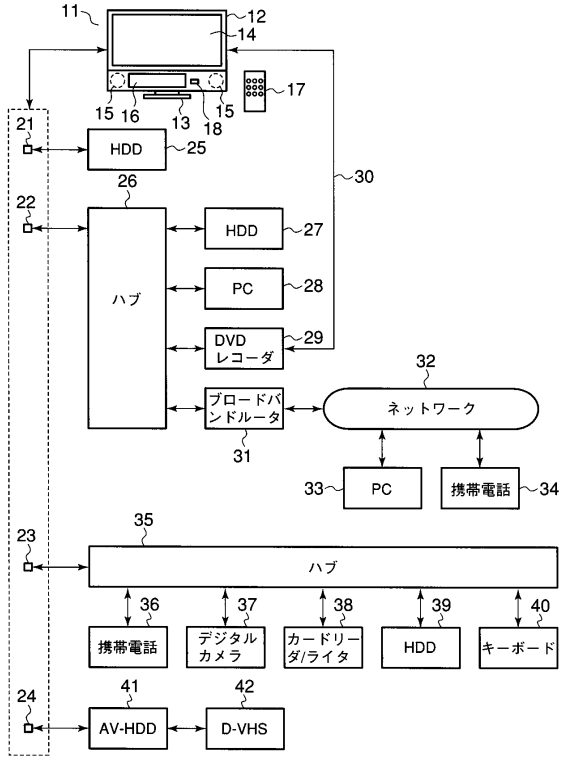
【符号の説明】

【００６０】

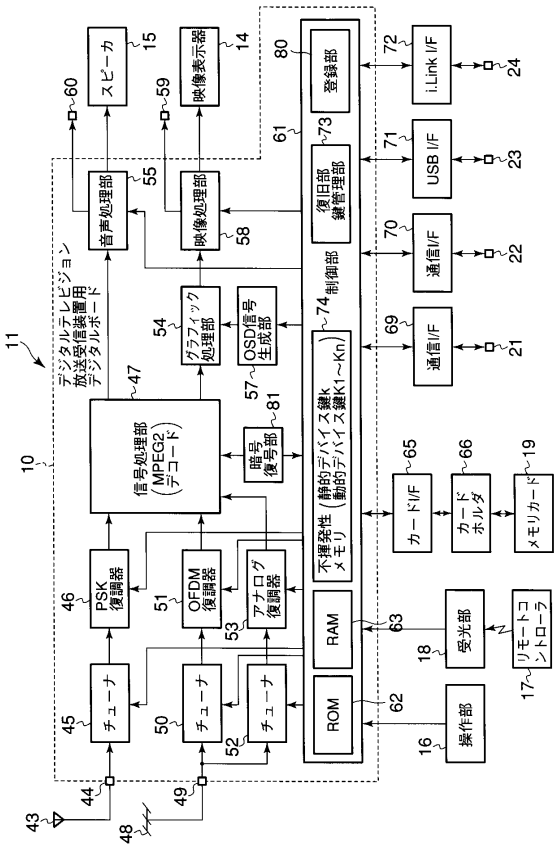
１１…デジタルテレビジョン通信装置、１２…キャビネット、１３…支持台、１４…映像表示器、１５…スピーカ、１６…操作部、１７…リモートコントローラ、１８…受光部、１９…メモリカード、２１…第１のＬＡＮ端子、２２…第２のＬＡＮ端子、２３…ＵＳＢ端子、２４…ｉ．Link端子、２５…ＨＤＤ、２６…ハブ、２７…ＨＤＤ、２８…ＰＣ、

２９…ＤＶＤレコーダ、３０…アナログ伝送路、３１…ブロードバンドルータ、３２…ネットワーク、３３…ＰＣ、３４…携帯電話、３５…ハブ、３６…携帯電話、３７…デジタルカメラ、３８…カードリーダ／ライタ、３９…ＨＤＤ、４０…キーボード、４１…ＡＶ－ＨＤＤ、４２…Ｄ－ＶＨＳ、４３…アンテナ、４４…入力端子、４５…チューナ、４６…ＰＳＫ復調器、４７…信号処理部、４８…アンテナ、４９…入力端子、５０…チューナ、５１…ＯＦＤＭ復調器、５２…チューナ、５３…アナログ復調器、５４…グラフィック処理部、５５…音声処理部、５７…ＯＳＤ信号生成部、５８…映像処理部、５９…出力端子、６０…出力端子、６１…制御部、６２…ＲＯＭ、６３…ＲＡＭ、６４…不揮発性メモリ、６５…カードＩ／Ｆ、６６…カードホルダ、６７…カードＩ／Ｆ、６８…カードホルダ、６９…通信Ｉ／Ｆ、７０…通信Ｉ／Ｆ、７１…ＵＳＢ Ｉ／Ｆ、７２…ｉ．Ｌｉｎｋ Ｉ／Ｆ、７３…復旧部鍵管理部、７４…不揮発性メモリ、８０…登録部。

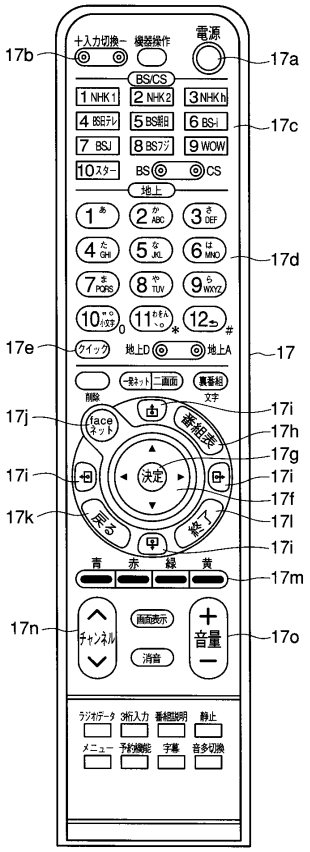
【図１】



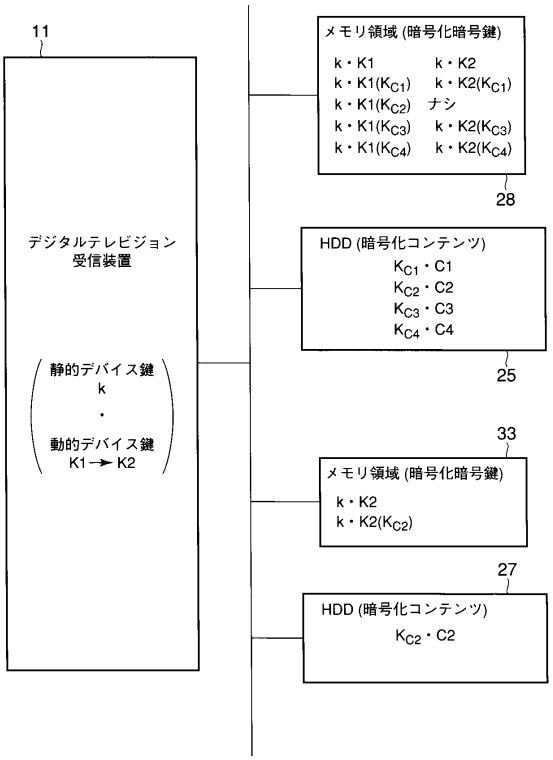
【図２】



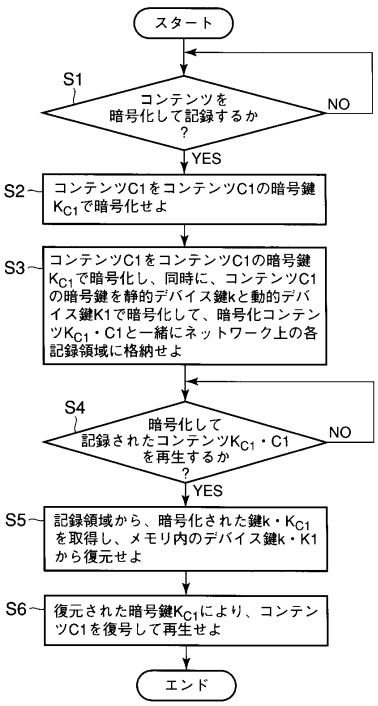
【図３】


17b
17a
17c
17d
17e
17
17i
17j
17h
17g
17i
17f
17k
17l
17i
17m
17n
17o
電源
BS/CS
地上
決定
戻る
青
赤
緑
黄
チャンネル
音量
画面表示
消音

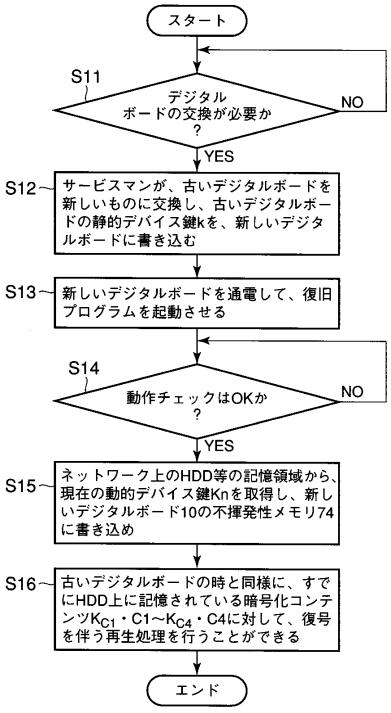
【図４】


11
デジタルテレビジョン
受信装置
静的デバイス鍵
k
・
動的デバイス鍵
K1→K2
メモリ領域 (暗号化暗号鍵)
k・K1
k・K2
k・K1(KC1)
k・K2(KC1)
k・K1(KC2)
ナシ
k・K1(KC3)
k・K2(KC3)
k・K1(KC4)
k・K2(KC4)
28
HDD (暗号化コンテンツ)
KC1・C1
KC2・C2
KC3・C3
KC4・C4
25
33
メモリ領域 (暗号化暗号鍵)
k・K2
k・K2(KC2)
27
HDD (暗号化コンテンツ)
KC2・C2

【図５】


スタート
S1
コンテンツを
暗号化して記録するか
?
NO
YES
S2
コンテンツC1をコンテンツC1の暗号鍵
KC1で暗号化せよ
S3
コンテンツC1をコンテンツC1の暗号鍵
KC1で暗号化し、同時に、コンテンツC1
の暗号鍵を静的デバイス鍵kと動的デバ
イス鍵K1で暗号化して、暗号化コンテン
ツKC1・C1と一緒にネットワーク上の各
記録領域に格納せよ
S4
暗号化して
記録されたコンテンツKC1・C1
を再生するか
?
NO
YES
S5
記録領域から、暗号化された鍵k・KC1
を取得し、メモリ内のデバイス鍵k・K1
から復元せよ
S6
復元された暗号鍵KC1により、コンテン
ツC1を復号して再生せよ
エンド

【図６】


スタート
S11
デジタル
ボードの交換が必要か
?
NO
YES
S12
サービスマンが、古いデジタルボードを
新しいものに交換し、古いデジタルボー
ドの静的デバイス鍵kを、新しいデジタ
ルボードに書き込む
S13
新しいデジタルボードを通電して、復旧
プログラムを起動させる
S14
動作チェックはOKか
?
NO
YES
S15
ネットワーク上のHDD等の記憶領域から、
現在の動的デバイス鍵Knを取得し、新し
いデジタルボード10の不揮発性メモリ74
に書き込め
S16
古いデジタルボードの時と同様に、すで
にHDD上に記憶されている暗号化コンテ
ンツKC1・C1～KC4・C4に対して、復号
を伴う再生処理を行うことができる
エンド

フロントページの続き

(74)代理人　100092196
　　弁理士　橋本　良郎
(72)発明者　木村　嘉雄
　　東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
(72)発明者　坂本　典哉
　　東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内

審査官　川崎　優

(56)参考文献　特開２００３－２３３９４８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｎ　　７／１６－１７３
　　Ｇ０６Ｆ　２１／００－２４，１３／００，１５／００
　　Ｈ０４Ｌ　　９／００－３６