

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4564318号
(P4564318)

(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
HO 4 N 7/167 (2006.01)	HO 4 N 7/167 Z
HO 4 L 9/00 (2006.01)	HO 4 L 9/00 6 O 1 B
	HO 4 L 9/00 6 O 1 E

請求項の数 10 (全 13 頁)

(21) 出願番号	特願2004-280473 (P2004-280473)	(73) 特許権者	000003078
(22) 出願日	平成16年9月27日 (2004.9.27)		株式会社東芝
(65) 公開番号	特開2006-94405 (P2006-94405A)		東京都港区芝浦一丁目1番1号
(43) 公開日	平成18年4月6日 (2006.4.6)	(74) 代理人	100091351
審査請求日	平成19年9月19日 (2007.9.19)		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暗号化暗号鍵と共に前記通
 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の記憶装置に、それぞれ前記暗

10

20

号化暗号鍵が重複して記録されているかどうかを確認し、一方に記録されていなければ、記録されている方の前記暗号化暗号鍵を読み出して、記録されていない方に記録するべく制御する鍵重複管理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第 1 の記憶装置を登録する登録部と、

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 の記憶装置に、それぞれ前記暗号化暗号鍵が重複して記録されているかどうかを確認し、一方に記録されていなければ、記録されている方の前記暗号化暗号鍵を読み出して、記録されていない方に記録するべく制御する鍵重複管理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。

10

【請求項 4】

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べく、前記メモリ部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 5】

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。

20

【請求項 6】

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 7】

前記復調部が出力した前記映像音声信号を M P E G 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 6 記載の通信装置。

【請求項 8】

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 の記憶装置を提供する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。

30

【請求項 9】

前記通信部は、L A N、U S B 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 10】

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、

40

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前記暗号化暗号鍵と共に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、前記通信装置と前記第 1 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、

50

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路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、鍵情報管理の確実な暗号復号機能を用いることで、コンテンツ情報を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($K_c \cdot C$)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(K_1)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(K_1)とで暗号化して暗号化暗号鍵($k \cdot K_1 \cdot K_c$)を出力し、前記暗号化暗号鍵($k \cdot K_1 \cdot K_c$)を前記通信部を介してネットワーク上の第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($K_c \cdot C$)を前記暗号化暗号鍵($k \cdot K_1 \cdot K_c$)と共に前記通信部を介してネットワーク上の第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($k \cdot K$

10

20

30

40

50

1・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DVD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】

なお、本発明の一実施形態においては、暗号化暗号鍵を、例えばネットワーク上のハードディスク等の一箇所に記憶させるだけではなく、少なくとも暗号化コンテンツ情報が保存される例えばDVDレコーダ装置やPC等にも重複して記録するものである。これにより、暗号化暗号鍵の保存先であるハードディスクレコーダが故障により読取不能となっても、暗号システムが動作不能となることがない。

【0010】

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。

【0011】

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。

【0012】

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～K_n)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(28)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。

【0013】

10

20

30

40

50

又、更に、本発明の一実施形態においては、暗号化暗号鍵（ $k \cdot K_1 \cdot K_c$ ）が複数の領域に確実に存在しているかを所定タイミングで確認し、一方が読取不能となっていれば、これを自動的に復旧するものである。これにより、暗号化システムの鍵管理を確実に行うことができ、暗号復号システムを確実に動作させることができる。

【発明を実施するための最良の形態】

【0014】

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。

【0015】

<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。

【0016】

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あ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。

【0017】

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。

【0018】

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。

【0019】

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。

【0020】

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。

【0021】

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。

【0022】

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。

【0023】

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

10

20

30

40

50

を介して P C 3 3 や携帯電話 3 4 等と情報伝送を行なうために使用される。

【 0 0 2 4 】

又、上記 U S B 端子 2 3 は、一般的な U S B 対応ポートとして使用されるもので、例えばハブ 3 5 を介して、携帯電話 3 6、デジタルカメラ 3 7、メモリカードに対するカードリーダー/ライター 3 8、H D D 3 9、キーボード 4 0 等の U S B 機器を接続し、これらの U S B 機器と情報伝送を行なうために使用される。

【 0 0 2 5 】

更に、上記 i . Link 端子 2 4 は、例えば A V - H D D 4 1、D (Digital) - V H S (Video Home System) 4 2 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。

10

【 0 0 2 6 】

図 2 は、上記したデジタルテレビジョン通信装置 1 1 の主要な信号処理系を示している。すなわち、B S / C S デジタル放送受信用のアンテナ 4 3 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 4 4 を介して衛星デジタル放送用のチューナ 4 5 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。

【 0 0 2 7 】

そして、このチューナ 4 5 で選局された放送信号は、P S K (Phase Shift Keying) 復調器 4 6 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 4 7 に出力される。

【 0 0 2 8 】

20

又、地上波放送受信用のアンテナ 4 8 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 4 9 を介して地上デジタル放送用のチューナ 5 0 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。

【 0 0 2 9 】

そして、このチューナ 5 0 で選局された放送信号は、O F D M (Orthogonal Frequency Division Multiplexing) 復調器 5 1 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 4 7 に出力される。

【 0 0 3 0 】

又、上記地上波放送受信用のアンテナ 4 8 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 4 9 を介して地上アナログ放送用のチューナ 5 2 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 5 2 で選局された放送信号は、アナログ復調器 5 3 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 4 7 に出力される。

30

【 0 0 3 1 】

ここで、上記信号処理部 4 7 は、P S K 復調器 4 6 及び O F D M 復調器 5 1 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、M P E G 2 のデコード処理を施し、グラフィック処理部 5 4 及び音声処理部 5 5 に出力している。

【 0 0 3 2 】

更に、グラフィック処理部 5 4 は、信号処理部 4 7 から供給されるデジタルの映像信号に、O S D (On Screen Display) 信号生成部 5 7 で生成される O S D 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 5 4 は、信号処理部 4 7 の出力映像信号と、O S D 信号生成部 5 7 の出力 O S D 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。

40

【 0 0 3 3 】

そして、グラフィック処理部 5 4 から出力されたデジタルの映像信号は、映像処理部 5 8 に供給される。この映像処理部 5 8 は、入力されたデジタルの映像信号を、上記映像表示器 1 4 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 1 4 に出力して映像表示させるとともに、出力端子 5 9 を介して外部に導出させる。

【 0 0 3 4 】

50

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。

【0035】

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。

【0036】

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。

【0037】

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/F 65 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。

【0038】

又、上記制御部 61 は、通信 I/F 69 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 HDD 25 と、通信 I/F 69 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 HDD 25 に IP (Internet Protocol) アドレスを割り当てて制御している。

【0039】

更に、上記制御部 61 は、通信 I/F 70 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/F 70 を介して情報伝送を行なうことができる。

【0040】

又、上記制御部 61 は、USB I/F 71 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/F 71 を介して情報伝送を行なうことができる。

【0041】

更に、上記制御部 61 は、i.Link I/F 72 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/F 72 を介して情報伝送を行なうことができる。

【0042】

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。

【0043】

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べく、暗号化暗号鍵を重複して複数の領域に記録すべく管理する鍵重複管理部 73 と、鍵管理システ

10

20

30

40

50

ムに用いる静的デバイス鍵 k , 動的デバイス鍵 K_1 乃至 K_n 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。

【0044】

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。

10

【0045】

(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。

20

【0046】

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 $K_c \cdot C$ 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。

【0047】

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 $K_1 \sim$ の二つにより暗号化され、暗号化暗号鍵 $k \cdot K_1 \cdot K_c$ 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。

30

【0048】

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。

【0049】

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 ($k \cdot K_1 \cdot K_c$) と暗号化コンテンツ情報 ($K_c \cdot C$) 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 ($K_1 \sim$) 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 ($K_c \cdot C$) を復元した上で、再生処理に供するものである。

40

【0050】

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 ($K_1 \sim K_n$) 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 K_1 から K_2 、 K_2 から K_3 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なく、上述したネットワーク上の所定領域28における暗号化暗号鍵 ($k \cdot K_1 \cdot K_c \dots$) の履歴についても更新され

50

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。

【 0 0 5 1 】

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 1 1 において、制御部 6 1 及び鍵重複管理部 7 3 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 (S 1)、コンテンツ情報 C 1 をコンテンツ情報 C 1 の暗号鍵 K_{C1} で暗号化する (S 2)。この時、コンテンツ情報は、チューナ部 4 5 , 5 0 , 5 2 等により選局された放送信号を、各復調部 4 6 , 5 1 , 5 3 等により復調され、更に、信号処理部 4 7 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 6 9 乃至 7 2 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 C 1 をコンテンツ情報 C 1 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。

10

【 0 0 5 2 】

次に、暗号鍵 K_{C1} で暗号化された暗号化コンテンツ $K_{C1} \cdot C1$ を、登録部 8 0 で登録されたネットワーク上の例えば HDD 2 5 へと記録する (S 3)。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 $k \cdot K1 \cdot K_{C1}$ として、登録部 8 0 で登録されたネットワーク上の例えばハードディスクドライバ 2 8 へと通信 I / F 部 6 9 を介して転送され保存される (S 3)。ただし、通信部である通信 I / F 部 6 9 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。

20

【 0 0 5 3 】

この時、本実施形態では、先の暗号化暗号鍵 $k \cdot K1 \cdot K_{C1}$ を、登録部 8 0 で登録されたネットワーク上の例えば PC 2 8 だけではなく、暗号化コンテンツ $K_{C1} \cdot C1$ 等が記録された記録先である例えば HDD 2 5 等にも、重複して記録するものである。このように暗号化暗号鍵 $k \cdot K1 \cdot K_{C1}$ を、複数箇所に記録しておくことにより、例えば、PC 2 8 に故障が発生した場合でも、他方の HDD 2 5 等で暗号化暗号鍵 $k \cdot K1 \cdot K_{C1}$ を確保することが可能となるため、暗号化システムの動作安定性を得ることができる。又、記録先は 2 つに限定する必要はなく、それ以上の領域に重複的に記録することで、システムの確実性を向上させることができる。

30

【 0 0 5 4 】

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 $K_{C1} \cdot C1$ を再生する場合は (S 4)、登録部 8 0 で登録された記録領域である例えば PC 2 8 から、暗号化暗号鍵 $k \cdot K1 \cdot K_{C1}$ を取得し、不揮発性メモリ 7 4 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 (S 5)。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 / F 部 6 9 を介して HDD 2 5 等から取得した暗号化コンテンツ情報 $K_{C1} \cdot C1$ を復号して再生するものである (S 6)。

40

【 0 0 5 5 】

なお、鍵更新部である鍵重複管理部 7 3 は、コンテンツ信号 (例えば、C 2) 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、C 2) を復号不能とすることで再生不能とすべく、記憶領域 7 4 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 2 5 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、C 1 , C 3 , C 4) に応じた暗号化暗号鍵 ($k \cdot K2 \cdot K_{C1}$ 、 $k \cdot K2 \cdot K_{C3}$ 、 $k \cdot K2 \cdot K_{C4}$) 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 C 2 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。

50

【 0 0 5 6 】

(暗号化暗号鍵の確認動作)

次に、上述した暗号化暗号鍵 $k \cdot K_1 \cdot K_{C_1}$ 等の確認動作及び復旧動作について、図 6 のフローチャートを用いて詳細に説明する。暗号化暗号鍵 $k \cdot K_1 \cdot K_{C_1}$ はネットワーク上の複数箇所に保存されているが、装置の故障や誤って削除してしまう等により読取不可能となる場合がある。ここでは、所定のタイミングで暗号化暗号鍵 $k \cdot K_1 \cdot K_{C_1}$ が存在することを確認し、読取不能となっていればこれを自動的に復旧するものである。

【 0 0 5 7 】

すなわち、図 6 のフローチャートにおいて、初めに、暗号化暗号鍵 $k \cdot K_1 \cdot K_{C_1}$ を格納する機器のフォルダ、及び、コンテンツを格納する機器のフォルダを予め設定されたデフォルトの機器のフォルダとするか、又は、ユーザの入力に従って登録部 80 で登録された機器の所定フォルダとする (S 1 1)。そして、ユーザからの記録処理の命令があるか、又は、コンテンツの削除や移動に伴い、鍵情報の更新のタイミングか、又は、予めユーザ等に設定されたかデフォルトで設定されている所定のタイミング、例えば、日時に応じて、一日 1 回、一週間に 1 回等の所定のタイミングとなったかどうか判断される (S 1 2)。

【 0 0 5 8 】

所望のタイミングとなったことが確認できれば、登録部 80 等により指定されている機器の所望のフォルダに暗号化暗号鍵 $k \cdot K_1 \cdot K_{C_1}$ 等が確実に読取可能に記録されているかどうか確認される (S 1 3)。読取可能に存在しない場合、一方の機器のフォルダ内の暗号化暗号鍵 $k \cdot K_1 \cdot K_{C_1}$ 等を、読取が確認できなかった方の機器のフォルダ内に記録することで復旧する (S 1 4)。このようにして、暗号化暗号鍵 $k \cdot K_1 \cdot K_{C_1}$ 等を所定タイミングで確認し、適宜復旧しておくことで、暗号化システムの動作を確実なものとして、ネットワークを介したコンテンツ情報の送受信を高いセキュリティを保ちながら実行することが可能となるものである。

【 0 0 5 9 】

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 】

【 0 0 6 0 】

【 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 】

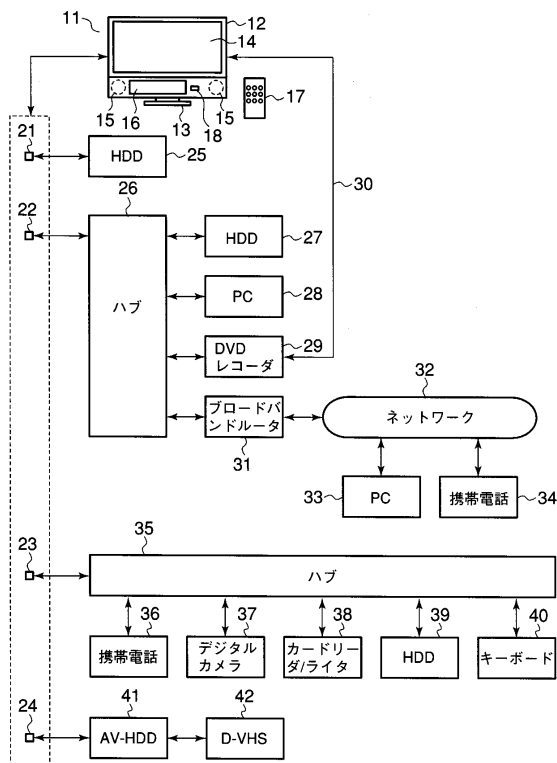
【 0 0 6 1 】

1 1 ... デジタルテレビジョン通信装置、 1 2 ... キャビネット、 1 3 ... 支持台、 1 4 ... 映像表示器、 1 5 ... スピーカ、 1 6 ... 操作部、 1 7 ... リモートコントローラ、 1 8 ... 受光部、 1 9 ... メモリカード、 2 1 ... 第 1 の LAN 端子、 2 2 ... 第 2 の LAN 端子、 2 3 ... US

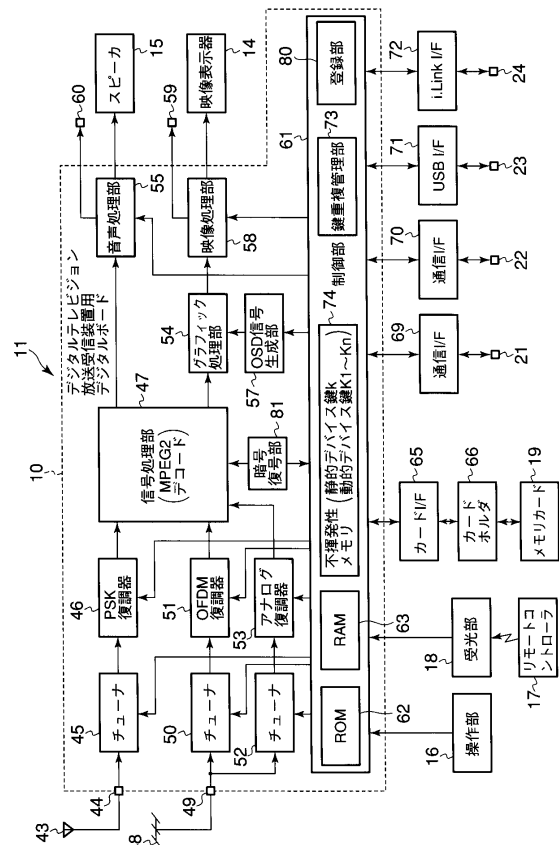
B端子、24...i.Link端子、25...HDD、26...ハブ、27...HDD、28...PC、29...DVDレコーダ、30...アナログ伝送路、31...ブロードバンドルータ、32...ネットワーク、33...PC、34...携帯電話、35...ハブ、36...携帯電話、37...デジタルカメラ、38...カードリーダー/ライター、39...HDD、40...キーボード、41...AV-HDD、42...D-VHS、43...アンテナ、44...入力端子、45...チューナ、46...PSK復調器、47...信号処理部、48...アンテナ、49...入力端子、50...チューナ、51...OFDM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...鍵重複管理部、74...不揮発性メモリ、80...登録部、81...暗号復号部。

10

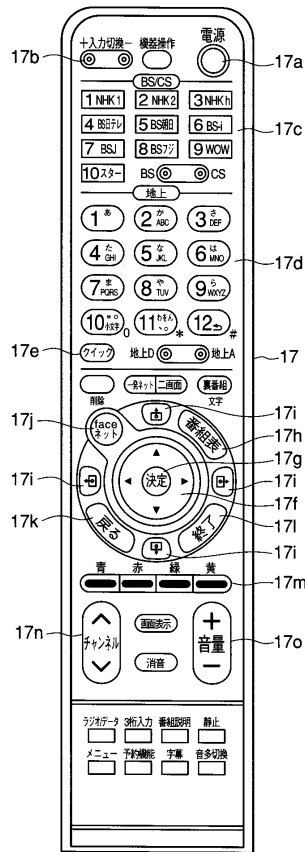
【図1】



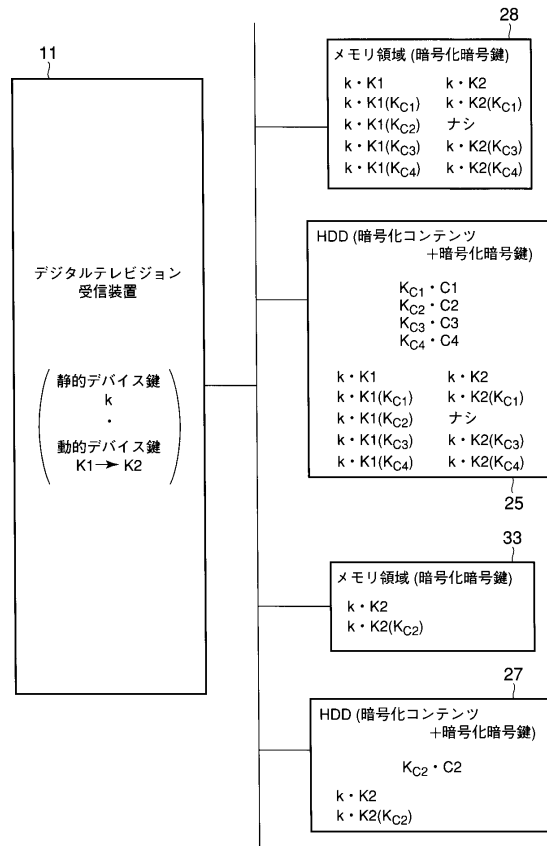
【図2】



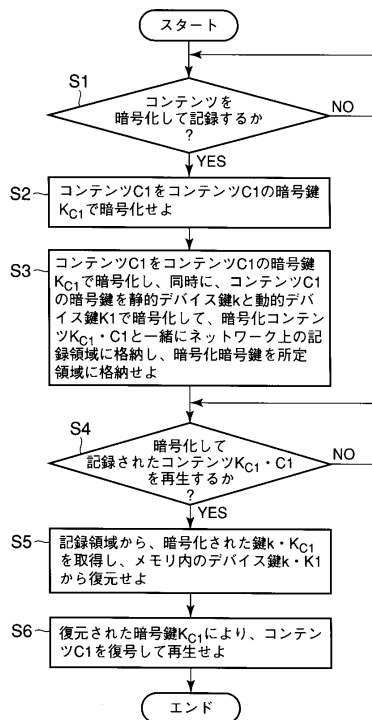
【図 3】



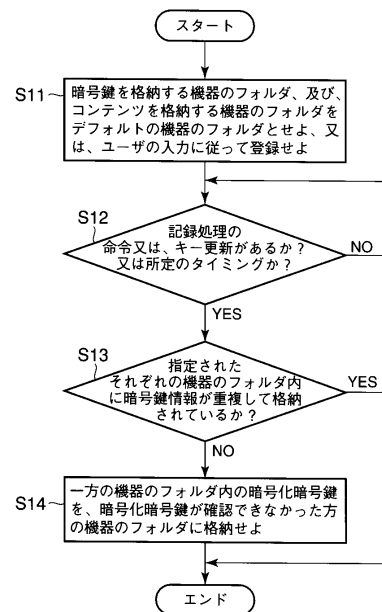
【図 4】



【図 5】



【図 6】



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

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 13/00, 15/00, 21/00 - 24

H04L 9/00 - 36