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

特許第5734367号
(P5734367)

(45)発行日　平成27年6月17日(2015.6.17)　(24)登録日　平成27年4月24日(2015.4.24)

(51)Int.Cl.		F I		
G06F 21/10	(2013.01)	G06F	21/10	350
H04L 9/14	(2006.01)	H04L	9/00	641
H04L 9/32	(2006.01)	H04L	9/00	673B
G06Q 50/10	(2012.01)	G06Q	50/10	140
G06F 21/30	(2013.01)	G06F	21/30	

請求項の数 6　(全 24 頁)　最終頁に続く

(21)出願番号　特願2013-156251 (P2013-156251)
(22)出願日　平成25年7月29日 (2013.7.29)
(62)分割の表示　特願2008-66964 (P2008-66964)の分割
原出願日　平成20年3月17日 (2008.3.17)
(65)公開番号　特開2014-2762 (P2014-2762A)
(43)公開日　平成26年1月9日 (2014.1.9)
審査請求日　平成25年7月29日 (2013.7.29)

前置審査

(73)特許権者　000005810
日立マクセル株式会社
大阪府茨木市丑寅一丁目１番８８号
(74)代理人　110000442
特許業務法人　武和国際特許事務所
(72)発明者　大野　千代
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所コンシューマエレクトロニクス研究所内
(72)発明者　岡本　宏夫
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所コンシューマエレクトロニクス研究所内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】コンテンツ送信装置、コンテンツ受信装置、コンテンツ送信方法およびコンテンツ受信方法

(57)【特許請求の範囲】
【請求項１】
第１のネットワークにルータを介さずに接続された第１の接続状態のコンテンツ受信装置、あるいは、前記第１のネットワークとルータを介して接続されている第２のネットワークに接続された第２の接続状態の前記コンテンツ受信装置に対して、受信したコンテンツを送信するコンテンツ送信装置において、
前記コンテンツを受信する受信手段と、
受信したコンテンツの暗号化を行う暗号化手段と、
前記コンテンツ受信装置からの送信要求に応じて前記暗号化手段で暗号化したコンテンツを送信する送信手段と、
前記コンテンツ送信装置と前記コンテンツ受信装置との間での接続状態確認要求の送受信結果に基づいて、前記第１の接続状態及び前記第２の接続状態のいずれの接続状態であるかを確認する接続状態確認手段と、
前記コンテンツ受信装置が前記第１の接続状態にあるときに、前記コンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報を登録するための情報登録手段と、
前記暗号化手段と前記送信手段とを制御する制御手段と、を備え、
前記制御手段の制御状態には、
前記第１の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、第１の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを前記コンテンツ受信装置に送信する第１の制御状態と、

前記第２の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、前記コンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報が予め前記情報登録手段に登録されている場合にのみ、前記第１の暗号化方法とは異なる第２の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを該第２のコンテンツ受信装置に送信する第２の制御状態と、

があることを特徴とするコンテンツ送信装置。

【請求項２】

第１のネットワークにルータを介さずに接続された第１の接続状態のコンテンツ受信装置、あるいは、前記第１のネットワークとルータを介して接続されている第２のネットワークに接続された第２の接続状態の前記コンテンツ受信装置に対して、受信したコンテンツを送信するコンテンツ送信装置におけるコンテンツ送信方法において、

前記コンテンツ送信装置と前記コンテンツ受信装置との間での接続状態確認要求の送受信結果に基づいて、前記第１の接続状態及び前記第２の接続状態のいずれの接続状態であるかを確認する接続状態確認ステップと、

前記コンテンツ受信装置が前記第１の接続状態にあるときに、前記コンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報を登録する情報登録ステップと、

前記コンテンツを受信する受信ステップと、

受信したコンテンツを暗号化する暗号化ステップと、

暗号化したコンテンツを送信する送信ステップと

を有し、

前記暗号化ステップと前記送信ステップには、

前記第１の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、第１の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを前記コンテンツ受信装置に送信する第１の制御状態と、

前記第２の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、前記コンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報が予め前記情報登録ステップにおいて登録されている場合にのみ、前記第１の暗号化方法とは異なる第２の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを該第２のコンテンツ受信装置に送信する第２の制御状態と、

があることを特徴とするコンテンツ送信方法。

【請求項３】

第１のネットワークにルータを介さずに接続された第１の接続状態のコンテンツ受信装置、あるいは、前記第１のネットワークとルータを介して接続されている第２のネットワークに接続された第２の接続状態の前記コンテンツ受信装置に対して、受信したコンテンツを送信するコンテンツ送信装置において、

前記コンテンツを受信する受信手段と、

受信したコンテンツの暗号化を行う暗号化手段と、

前記コンテンツ受信装置からの送信要求に応じて前記暗号化手段で暗号化したコンテンツを送信する送信手段と、

前記コンテンツ送信装置と前記コンテンツ受信装置との間での接続状態確認要求の送受信結果に基づいて、前記第１の接続状態及び前記第２の接続状態のいずれの接続状態であるかを確認する接続状態確認手段と、

前記コンテンツ受信装置が前記第１の接続状態にあるときに、前記コンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報を登録するための情報登録手段と、

前記暗号化手段と前記送信手段とを制御する制御手段と、を備え、

前記制御手段の制御状態には、

前記第１の接続状態にあることが確認された前記コンテンツ受信装置に、第１の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを送信する第１の制御状態と、

前記第２の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテン

ツの送信要求を受信したときに、前記のコンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報が予め前記情報登録手段に登録されている場合にのみ、前記第１の暗号化方法とは異なる第２の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを送信する第２の制御状態と、

があることを特徴とするコンテンツ送信装置。

【請求項４】

第１のネットワークにルータを介さずに接続された第１の接続状態のコンテンツ受信装置、あるいは、前記第１のネットワークとルータを介して接続されている第２のネットワークに接続された第２の接続状態の前記コンテンツ受信装置に対して、受信したコンテンツを送信するコンテンツ送信装置におけるコンテンツ送信方法において、

前記コンテンツ送信装置と前記コンテンツ受信装置との間での接続状態確認要求の送受信結果に基づいて、前記第１の接続状態及び前記第２の接続状態のいずれの接続状態であるかを確認する接続状態確認ステップと、

前記コンテンツ受信装置が前記第１の接続状態にあるときに、前記コンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報を登録する情報登録ステップと、

前記コンテンツを受信する受信ステップと、

受信したコンテンツを暗号化する暗号化ステップと、

暗号化したコンテンツを送信する送信ステップとを有し、

前記暗号化ステップと前記送信ステップには、

前記第１の接続状態にあることが確認された前記コンテンツ受信装置に、第１の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを送信する第１の制御状態と、

前記第２の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、前記コンテンツ受信装置と前記コンテンツ送信装置とを関連付ける情報が予め前記情報登録ステップにおいて登録されている場合にのみ、前記第１の暗号化方法とは異なる第２の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを送信する第２の制御状態と、

があることを特徴とするコンテンツ送信方法。

【請求項５】

第１のネットワークにルータを介さずに接続された第１の接続状態のコンテンツ受信装置、あるいは、前記第１のネットワークとルータを介して接続されている第２のネットワークに接続された第２の接続状態の前記コンテンツ受信装置に対して、受信したコンテンツを送信するコンテンツ送信装置において、

前記コンテンツを受信する受信手段と、

受信したコンテンツの暗号化を行う暗号化手段と、

前記コンテンツ受信装置からの送信要求に応じて前記暗号化手段で暗号化したコンテンツを送信する送信手段と、

前記コンテンツ送信装置と前記コンテンツ受信装置との間での接続状態確認要求の送受信結果に基づいて、前記第１の接続状態及び前記第２の接続状態のいずれの接続状態であるかを確認する接続状態確認手段と、

前記コンテンツ受信装置が前記第１の接続状態にあるときに、前記コンテンツ受信装置との間で認証を行う認証手段と、

前記暗号化手段と前記送信手段とを制御する制御手段と、を備え、

前記制御手段の制御状態には、

前記第１の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、第１の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを前記コンテンツ受信装置に送信する第１の制御状態と、

前記第２の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、前記コンテンツ受信装置が前記認証手段により認証されたものである場合にのみ、前記第１の暗号化方法とは異なる第２の暗号化方法で前記コン

テンツの暗号化を行い、暗号化を行った前記コンテンツを前記コンテンツ受信装置に送信する第２の制御状態と、
があることを特徴とするコンテンツ送信装置。
【請求項６】
第１のネットワークにルータを介さずに接続された第１の接続状態のコンテンツ受信装置、あるいは、前記第１のネットワークとルータを介して接続されている第２のネットワークに接続された第２の接続状態の前記コンテンツ受信装置に対して、受信したコンテンツを送信するコンテンツ送信装置におけるコンテンツ送信方法において、
前記コンテンツ送信装置と前記コンテンツ受信装置との間での接続状態確認要求の送受信結果に基づいて、前記第１の接続状態及び前記第２の接続状態のいずれの接続状態であるかを確認する接続状態確認ステップと、
前記コンテンツ受信装置が前記第１の接続状態にあるときに、前記コンテンツ受信装置との間で認証を行う認証ステップと、
前記コンテンツを受信する受信ステップと、
受信したコンテンツを暗号化する暗号化ステップと、
暗号化したコンテンツを送信する送信ステップと
を有し、
前記暗号化ステップと前記送信ステップには、
前記第１の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、第１の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを前記第１のコンテンツ受信装置に送信する第１の制御状態と、
前記第２の接続状態にあることが確認された前記コンテンツ受信装置から前記コンテンツの送信要求を受信したときに、前記コンテンツ受信装置が前記認証手段により認証されたものである場合にのみ、前記第１の暗号化方法とは異なる第２の暗号化方法で前記コンテンツの暗号化を行い、暗号化を行った前記コンテンツを該第２のコンテンツ受信装置に送信する第２の制御状態と、
があることを特徴とするコンテンツ送信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
映像音声等のコンテンツをネットワークを介して送受信するのに際して、伝送されるコンテンツの著作権を保護するのに好適な送信装置、受信装置およびコンテンツ伝送方法に関するものである。
【背景技術】
【０００２】
パーソナルコンピュータ（以下、ＰＣ）の演算速度や記憶容量など処理能力の発展に伴い、ＰＣに内蔵されるハードディスクドライブ（以下、ＨＤＤ）も大容量化が進んでいる。こうした状況のもとで最近では一般の家庭で利用されるようなランクのＰＣにおいてもＨＤＤを利用してＴＶ放送番組を録画し、これをＰＣのディスプレイで視聴を行うといった使い方ができるようになってきた。
【０００３】
また、近年デジタル映像信号処理技術の発展に伴い、デジタル放送を受信するデジタルチューナ内蔵テレビ（以下、ＤＴＶ）や、デジタル放送番組を録画・再生するデジタル記録装置（例えば、ＨＤＤレコーダやＤＶＤレコーダ、ＢＤレコーダ等）のデジタルＡＶ装置が次々と製品化されている。
【０００４】
さらに、ブロードバンド／インターネットの普及により、これらのデジタルＡＶ装置に有線／無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、ＩＥＥＥ１３９４、ＵＳＢなどのデジタルインタフェースを搭載し、ネットワークを介してデジタルコンテンツを

伝送することが可能である。
【０００５】
一般にデジタル録画されたコンテンツを上記のようにネットワーク等を介してある装置から他の装置へ伝送して記録を行うような場合には伝送時のデータ品質の劣化が少なく、送信側の装置にあるコンテンツと同じ品質のコピー（複製）が受信側で作成できるため、著作権を保護すべきコンテンツに対しては、個人的利用の範囲を逸脱したコンテンツの不正なコピー作成を防止できるような配慮が必要である。
【０００６】
例えばデジタルＡＶ機器の間でコンテンツを送信する際には、コンテンツ送信装置側において暗号化を行い、コンテンツ受信装置側との間で復号化のための情報の共有化を行うことによって、送信先であるコンテンツ受信装置以外の機器によってコンテンツが正しく受信されて復号されない様にして、無制限なコピーの作成を防ぐコピープロテクトが実施されている。
【０００７】
このようなコピープロテクトの方法の一例としてデジタルＡＶ機器に取り入れられているものには、例えばＩＥＥＥ１３９４バス上でのコピープロテクト方法を定めたＤｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ（ＤＴＣＰ）方式がある。ＤＴＣＰ方式ではコンテンツを「コピー制限なし」「一回限りコピー可」「コピー禁止」に分類して管理し、録画装置では「コピー制限なし」「一回限りコピー可」のコンテンツだけを記録し、「一回限りコピー可」のコンテンツは一度記録した後は「コピー不可」として取り扱い、バス上では「コピー制限なし」のコンテンツを除いて送信側で暗号化処理を施して伝送を行うことによって、無制限なコンテンツのコピーが行えないようにしている。
【０００８】
また、有線あるいは無線のＬＡＮによるコンテンツ伝送においても、ＤＴＣＰ方式をＩＰネットワーク用に拡張し、さらなるセキュリティ強化を図ったＤＴＣＰ－ＩＰ方式が規定されている。ＤＴＣＰ－ＩＰ方式では、家庭内で記録した放送番組などの著作権保護対象となるコンテンツが無制限に宅外へ配信すること無いように、家庭内ネットワークであることを判断するための技術が開示されている。
【先行技術文献】
【特許文献】
【０００９】
【特許文献１】特開２００５－５８２１号公報
【発明の概要】
【発明が解決しようとする課題】
【００１０】
上記従来の技術では、著作権保護対象のコンテンツを有線あるいは無線ＬＡＮを介して伝送する際、送信側と受信側の機器が同じ家の中にあることを確認する機能が組み込まれている。
【００１１】
しかし、ノート型ＰＣや携帯端末といったモバイル環境で使用する機器を所有しているユーザにとっては、これらの機器を用いて旅行先や通勤途中の電車の中などから家庭内のコンテンツにアクセスしたいという要求は高い。
【００１２】
そこで、有線または無線のＬＡＮを利用し、宅内の機器から宅外の機器へコンテンツを伝送する際に、コンテンツの正当な視聴が個人的利用の範囲に制限することのできるコンテンツ送信装置、受信装置およびコンテンツ伝送方法を提供することを目的とする。
【課題を解決するための手段】
【００１３】
上記目的を解決するために、例えば特許請求の範囲に記載の構成を採用する。

【発明の効果】
【００１４】
宅内で予めコンテンツ送信装置との間で通常の機器認証処理と宅外アクセス用の機器認証処理を実行し、これらの処理に成功したコンテンツ受信装置のみ、宅外から宅外専用の機器認証処理を実行すれば宅内のコンテンツを視聴可能となる。これにより、正規のユーザが個人的利用の範囲を超えることなく宅外から宅内のコンテンツを視聴することができ、ユーザの利便性が向上する。
【図面の簡単な説明】
【００１５】
【図１】システムの一構成例
【図２】ＤＴＶの一ブロック構成例
【図３】ＨＤＤレコーダの一ブロック構成例
【図４】ＰＣの一ブロック構成例
【図５】携帯電話の一ブロック構成例
【図６】機器情報管理部の一構成例
【図７】機器情報の一構成例
【図８】宅内のコンテンツ送信装置とコンテンツ受信装置の間で通常実行する機器認証シーケンスの一例。
【図９】宅内のコンテンツ送信装置とコンテンツ受信装置の間で宅外アクセス用の鍵交換を実行する機器認証シーケンスの一例。
【図１０】宅外に持ち出すコンテンツ受信装置の機器情報管理部で保持するリモートアクセス用情報テーブルの一構成例。
【図１１】宅内のコンテンツ送信装置と宅外のコンテンツ受信装置の間でコンテンツ転送を実行するシーケンスの一例。
【図１２】機器情報の一構成例
【図１３】システムの一構成例
【図１４】宅外のコンテンツ受信装置から宅内のコンテンツ送信装置へコンテンツ転送を実行するシーケンスの一例。
【図１５】携帯電話のコンテンツ送信装置一覧画面例
【図１６】携帯電話のコンテンツ一覧画面例
【図１７】携帯電話のコンテンツ再生装置一覧画面例
【図１８】機器情報の一構成例
【図１９】宅外のコンテンツ受信装置から宅内のコンテンツ送信装置へコンテンツ転送を実行するシーケンスの一例
【発明を実施するための形態】
【００１６】
以下本発明の実施の形態について説明する。
【実施例１】
【００１７】
本実施の形態の特徴は、コンテンツの個人的利用の範囲を超えることなく、不正な視聴／複製を防止しながら、宅外にあるコンテンツ受信装置で宅内のコンテンツを視聴可能にすることである。
【００１８】
図１は、システム構成を示したものであり、ユーザＡが外出先から自宅内の機器にアクセスする場合を想定している。
【００１９】
ユーザＡ宅１内には、ユーザＡの所有しているＤＴＶ１００、ＨＤＤレコーダ２００、ＰＣ３００がハブ１１を介して有線ＬＡＮでネットワーク接続されている。また、該ハブ１１はルータ１２を介してインターネット３に接続可能になっている。
【００２０】

ユーザＡの外出先（例えば、ホテルや会社等）２では、ユーザＡの携帯電話５００が無線アクセスポイント２２と通信可能であり、ルータ２１を介してインターネット３に接続可能になっている。また、ユーザＢのＰＣ４００も同様の方法でインターネット３に接続可能とする。また、外出先に設置されたＤＴＶ６００は、ルータ２１を介してインターネット３に接続可能とする。

【００２１】

ＬＡＮにおいては、ネットワークプロトコルとして標準のＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）を使用し、上位のトランスポートプロトコルにはＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）およびＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）を用いる。コンテンツの伝送には更に上位のアプリケーションプロトコル、例えばＲＴＰ（Ｒｅａｌ－ｔｉｍｅ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）やＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、ＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）等が使用される。なお、ＩＰにはバージョンの違いとしてＩＰｖ４とＩＰｖ６が有るが、そのどちらかに限定される物ではない。

【００２２】

ネットワーク接続された上記ＤＴＶ１００、ＨＤＤレコーダ２００、ＰＣ３００、４００．携帯電話５００、ルータ１２、２１は、それぞれＬＡＮ上で自身を識別するＩＰアドレスを所有する。また各々のネットワーク通信処理回路のインターフェース部には４８ビットのＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）アドレスが予め製造時に与えられている。各装置へのＩＰアドレスの設定は、従来よりネットワークにおけるアドレスの自動設定に広く採用されているＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）により、例えばルータ１２、２１をＤＨＣＰサーバとして動作させ、ここから各装置のＩＰアドレスを割り振るようにすれば良い。

【００２３】

なお、ＩＰｖ６を用いる場合にはステートレス自動設定と呼ばれる方法によりルータ１２、２１のＩＰアドレスの上位６４ｂｉｔとＭＡＣアドレスから各装置が自身のＩＰアドレスを定めることも可能である。

【００２４】

ここで、図１ではユーザ宅１内は各機器間を有線ＬＡＮで接続しているが、無線アクセスポイントを使用したＬＡＮやＩＥＥＥ１３９４、ＵＳＢ、Ｂｌｕｅｔｏｏｔｈ（登録商標）等を用いても良い。また、ハブ１１とルータ１２、あるいは無線アクセスポイント２２とルータ２１が一体型になった形態でも良い。

【００２５】

また、ルータ１２、２１は、図示しないモデムあるいは光電変換器などを介して、もしくはルータに内蔵されるモデムあるいは光電変換器によりインターネットに接続される。インターネットへの接続形態はＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ Ｄｉｇｉｔａｌ Ｓｕｂｓｃｒｉｂｅｒ ｌｉｎｅ）や光ファイバーなどの高速アクセス回線やＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅｓ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ）、アナログ電話回線、携帯電話などの移動体通信網などその種類を問わない。外出先２内のネットワーク構成も前記同様である。

【００２６】

また、外出先２からインターネット３を介してユーザ宅１内の各機器にアクセスする方法は、ルータのポートフォワード機能やＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）などの技術を利用すれば良い。

【００２７】

次に、図２を用いて、ＤＴＶ１００の一構成例について説明する。なお、ＤＴＶ６００も同様の構成とする。

【００２８】

ＤＴＶ１００は、チューナ１０１、デスクランブラ１０２、デマルチプレクサ１０３、

デコーダ１０４、表示部／スピーカ１０５、デジタル端子１０６、入力処理部１０７、機器認証処理部１０８、機器情報管理部１０９、暗号／復号処理部１１０、通信処理部１１１、デジタル入出力端子１１２、制御部１１３から構成される。

【００２９】

チューナ１０１は、放送局からアンテナ１０を介して受信した複数のチャンネルから所望のチャンネルを選局し、デジタル変調された番組を復調する部分である。

デスクランブラ１０２は、サービス事業者と契約したチャンネルのみを受信可能とするためにかけられている番組のスクランブルを解除する部分である。

デマルチプレクサ１０３は、放送番組から音声データ、映像データを抽出する部分である。

デコーダ１０４は、放送番組やデジタル入出力端子１１２から受信した圧縮された音声データや映像データを復号して、元の音声信号、映像信号に伸長する部分である。

【００３０】

表示部／スピーカ１０５は、該デコーダ１０４からの出力信号や、デジタル端子１０６から入力された信号を再生する部分である。内蔵ではなく、外付けでも良い。

デジタル端子１０６は、非圧縮のデジタルデータを入力する部分であり、例えばＨＤＭＩ（Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ Ｍｕｌｔｉｍｅｄｉａ Ｉｎｔｅｒｆａｃｅ）（登録商標）などがある。

入力処理部１０７は、リモコンやタッチパネルなどを利用してユーザがＤＴＶ１００を操作する部分である。

【００３１】

機器認証処理部１０８は、ＬＡＮを介して著作権保護対象のコンテンツを転送するために、他のＡＶ機器との間で特定の認証プロトコルに準拠してお互いに正規に認定された機器であるかを認証し、コンテンツの暗号／復号に使用する鍵を共有する部分である。該特定の認証プロトコルは、例えば前記ＤＴＣＰ方式などが挙げられる。

【００３２】

機器情報管理部１０９は、前記機器認証処理部１０８で認証が成功したＡＶ機器に関する情報を管理する部分である。

暗号／復号処理部１１０は、放送番組やＬＡＮ経由でデジタル入出力端子１１２を介して受信したコンテンツを、前記機器認証処理部１０８で共有した鍵を使用して暗号化あるいは復号化する部分である。

【００３３】

通信処理部１１１は、デジタル入出力端子１１２を介してＬＡＮで接続した他のＡＶ機器との間でコンテンツや制御コマンドを送受信する部分である。送信されるコンテンツにはその取り扱い方を示す「コピー制限なし」「一回限りコピー可」「コピー禁止」「コピー不可」などの識別コードを付して送信される。

【００３４】

デジタル入出力端子１１２は、ＬＡＮ経由でコンテンツや制御コマンドを入出力する部分である。

制御部１１３は、ＤＴＶ１００における各部の動作を統括的に制御する部分である。

【００３５】

次に、図３を用いて、ＨＤＤレコーダ２００の一構成例について説明する。

ＨＤＤレコーダ２００は、入力処理部２０１、機器認証処理部２０２、機器情報管理部２０３、記録／再生処理部２０４、ＨＤＤ２０５、暗号／復号処理部２０６、通信処理部２０７、デジタル入出力端子２０８、デコーダ２０９、デジタル端子２１０、制御部２１１から構成される。

【００３６】

記録／再生処理部２０４は、コンテンツをＨＤＤ２０５に記録するための記録制御と、該ＨＤＤ２０５に記録したコンテンツを再生するための再生制御を行う部分である。

ＨＤＤ２０５は、放送番組を記録する内蔵メモリである。その他に着脱可能なＨＤＤや

光ディスク、メモリカード、そしてこれらを組み合わせたハイブリッド形態などが考えられる。

【００３７】

デジタル端子２１０は、デコーダ２０９から出力された非圧縮のデジタルデータを外部の表示部やスピーカへ出力する部分である。

それ以外の部分については、ＤＴＶ１００と同様である。

【００３８】

次に、図４を用いて、ＰＣ３００の一構成例について説明する。

ＰＣ３００は、チューナ３０１、デスクランブラ３０２、デマルチプレクサ３０３、デコーダ３０４、表示部／スピーカ３０５、デジタル端子３０６、入力処理部３０７、機器認証処理部３０８、機器情報管理部３０９、記録／再生処理部３１０、ＨＤＤ３１１、暗号／復号処理部３１２、通信処理部３１３、デジタル入出力端子３１４、無線暗号／復号処理部３１５、無線通信処理部３１６、制御部３１７から構成される。

【００３９】

無線暗号／復号処理部３１５は、無線ＬＡＮ経由で無線通信処理部３１６を介して受信したコンテンツあるいは暗号／復号処理部３１２から出力されたコンテンツを、ＷＥＰ（Ｗｉｒｅｄ Ｅｑｕｉｖａｌｅｎｔ Ｐｒｉｖａｃｙ）などの無線ＬＡＮにおけるセキュリティ保護の目的で標準的に用いられている公知の暗号化方式を用いて暗号化／復号化する部分である。無線ＬＡＮ以外に、３ＧやＷ－ＣＤＭＡ（Ｗｉｄｅｂａｎｄ Ｃｏｄｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ）など携帯電話などで使用している無線通信方式を利用しても良い。

【００４０】

無線通信処理部３１６は、無線ＬＡＮで接続した無線アクセスポイント２２や他のＡＶ機器との間でコンテンツや制御コマンドを送受信する部分である。無線ＬＡＮだけでなく、　それ以外の部分については、ＤＴＶ１００、ＨＤＤレコーダ２００と同様である。また、ＰＣ４００も同様の構成で良い。

【００４１】

次に、図５を用いて、携帯電話５００の一構成例について説明する。

携帯電話５００は、チューナ５０１、デスクランブラ５０２、デマルチプレクサ５０３、デコーダ５０４、表示部／スピーカ５０５、デジタル端子５０６、カメラ撮像部５０７、通信処理部５０８、入力処理部５０９、機器認証処理部５１０、機器情報管理部５１１、記録／再生処理部５１２、記録メモリ５１３、暗号／復号処理部５１４、無線暗号／復号処理部５１５、無線通信処理部５１６、制御部５１７から構成される。

【００４２】

カメラ撮像部５０７は、カメラで撮影する部分である。

記録メモリ５１３は、該カメラ撮像部５０７で撮影した動画／静止画や、チューナ５０１経由で受信した番組や、個人情報やアドレス帳などの情報を格納する不揮発性のメモリである。内蔵あるいは着脱可能なメモリ形態が考えられる。

それ以外の部分については、ＤＴＶ１００、ＨＤＤレコーダ２００、ＰＣ３００と同様である。

【００４３】

次に、図６を用いて、前記各機器内の機器情報管理部１０９（２０３、３０９、５１１も同様）の一構成例について説明する。

機器情報管理部１０９は、タイマー１０８１、機器情報更新部１０８２、機器情報格納部１０８３から構成される。

【００４４】

タイマー１０８１は、前記機器認証処理部１０８（２０２、３０８、５１０も同様）で認証相手の機器が宅内に存在するか否かを確認する場合、あるいは後述の機器情報格納部１０８３に格納された登録情報の有効期限を管理する場合の時間計測に使用する部分である。

【００４５】
機器情報更新部１０８２は、後述の機器情報格納部１０８３に保持した登録情報の有効期限を管理し、必要に応じて登録／更新／削除を行う部分である。
機器情報格納部１０８３は、前記機器認証処理部１０８で機器認証が成功した場合に、認証相手の機器に関する情報を保持する部分である。
【００４６】
次に、図７を用いて、前記機器情報格納部１０８３で格納する機器情報７０の一構成例について説明する。
機器情報７０は、管理テーブル７００、機器情報テーブル７１０から構成される。
管理テーブル７００は、最機器認証最大数７０１、カウンタ最大値７０２、外部アクセス最大数７０３で構成する。
【００４７】
最機器認証最大数７０１は、前記機器認証処理部１０８を用いてコンテンツの送信装置と受信装置の間で機器認証が実行可能な最大数を示す。
カウンタ最大値７０２は、前記タイマー１０８１に設定するカウンタの最大値を示す。
外部アクセス最大数７０３は、宅外からのコンテンツアクセス要求を許可する最大数を示す。
【００４８】
一方、機器情報テーブル７１０は、ＩＤ７１１、デバイスＩＤ７１２、アドレス情報７１３、カウンタ値７１４、宅外アクセス鍵７１５、宅外アクセス鍵ラベル７１６、アクセス状況７１６で構成する。
ＩＤ７１１は、該テーブルの登録番号を示す。
【００４９】
デバイスＩＤ７１２は、各機器を一意に識別するための識別子を示す。例えば、ＩＥＥＥ１３９４で使用するユニークＩＤやＤＴＣＰで使用するデバイスＩＤなど、特定の認証機関により生成され、各機器の製造時に予め不揮発メモリに保存される機器固有の情報であり、機器毎にユニークな値を持つ。その他、公開鍵などの情報を含んでいても良い。
【００５０】
アドレス情報７１３は、ネットワーク上における各機器のＩＰアドレスやＭＡＣアドレス等を示す。
カウンタ値７１４は、前記タイマー１０８１に設定したカウンタの現在の値を示す。
宅外アクセス鍵７１５は、宅内とコンテンツ送信装置と宅外のコンテンツ受信装置との間でコンテンツ転送する際に認証／暗復号処理で用いる鍵情報を示す。
【００５１】
宅外アクセス鍵ラベル７１６は、前記宅外アクセス鍵７１５を識別するために用いる識別子を示す。
アクセス状況７１６は、コンテンツの送信装置と受信装置との間の転送状況（例えば、停止／宅内／宅外）を示す。
【００５２】
以上に記載した各機器と各情報を用いて、前記図１に示したシステム構成において、ＨＤＤレコーダ２００（コンテンツ送信装置）とＤＴＶ１００（コンテンツ受信装置）との間で実行する機器認証処理手順８００について、図８を用いて説明する。ここで、機器認証処理のための情報の送受信にはプロトコルとしてＴＣＰを用い、相手方の装置への認証要求とこれに対する認証応答等の各種情報が送信されるとこれに対する受信確認が相手方の装置から返送され、これにより伝送エラーの検知が可能な通信路が確保される。なお、図８においてはＴＣＰによるコネクションの確立および破棄のためのデータ送受信については省略してある。
【００５３】
最初に、コンテンツ受信装置１００側から認証要求を作成する。コンテンツ受信装置１００の機器認証処理部１０８は、認証要求に前記したデバイスＩＤを含む機器固有の情報

と、該情報に対する証書を付して、通信処理部１１１を介してコンテンツ送信装置２００に送る（Ｓ８０１）。

【００５４】

コンテンツ送信装置２００の機器認証処理部２０２は、通信処理部２０７を介して認証要求を受け取りその受信確認をコンテンツ受信装置１００に送ると（Ｓ８０２）、コンテンツ送信装置２００の機器認証処理部２０２は自分の側からの認証要求を作成し、コンテンツ受信装置の場合と同様にコンテンツ送信装置２００の固有情報とその証書を付してコンテンツ受信装置１００に送る（Ｓ８０３）。

【００５５】

コンテンツ受信装置１００の機器認証処理部１０８は、認証要求を受け取り、その受信確認をコンテンツ送信装置１００へ送る（Ｓ８０４）。

【００５６】

次に、コンテンツ送信装置２００の機器認証処理部２０２は、前記認証要求で受信した各情報を検証し、鍵情報の生成に必要なパラメータを付した認証応答をコンテンツ受信装置１００に送る（Ｓ８０５）。

【００５７】

コンテンツ受信装置１００の機器認証処理部１０８は、認証応答を受け取りその受信確認をコンテンツ送信装置２００に送った（Ｓ８０６）後、自分の側からの認証応答を作成し、コンテンツ送信装置の場合と同様に鍵情報の生成に必要なパラメータを付した認証応答をコンテンツ送信装置２００に送り（Ｓ８０７）、必要なパラメータを用いてコンテンツ送信装置２００と共通の認証鍵を生成する。

【００５８】

コンテンツ送信装置２００の機器認証処理部２０２は、認証応答を受け取りその受信確認をコンテンツ受信装置１００に送り（Ｓ８０８）、コンテンツ受信装置と同様に、必要なパラメータを用いてコンテンツ受信装置１００と共通の認証鍵を生成する。

【００５９】

ここまでの手順で、コンテンツ送信装置２００の機器認証処理部１０８とコンテンツ受信装置の機器認証処理部２０２は、互いに共通の認証鍵が生成されて共有される。

【００６０】

次に、コンテンツ送信装置２００は、コンテンツ受信装置１００が宅内に存在する機器であるか確認するために、宅内確認の準備を行う旨をコンテンツ受信装置１００に送る（Ｓ８０９）。

【００６１】

コンテンツ受信装置１００の機器認証処理部１０８は、宅内確認準備の通知を受け取り、その受信確認をコンテンツ送信装置２００に送ると（Ｓ８１０）、自分の側からの宅内確認準備通知を作成し、コンテンツ送信装置２００へ送る（Ｓ８１１）。

【００６２】

コンテンツ送信装置２００の機器認証処理部２０２は、宅内確認準備の通知を受け取り、その受信確認をコンテンツ受信装置１００に送ると（Ｓ８１２）、宅内確認に必要な情報を付した宅内確認設定要求をコンテンツ受信装置１００に送る（Ｓ８１３）。

【００６３】

コンテンツ受信装置１００の機器認証処理部１０８は、宅内確認設定要求を受け取り、宅内確認に必要な準備を行い、その受信確認をコンテンツ送信装置２００に送る（Ｓ８１４）。

【００６４】

受信確認を受け取ったコンテンツ送信装置２００の機器認証処理部２０２は、前記機器情報管理部２０３内のタイマー１０８１を起動した後、コンテンツ受信装置１００が宅内に存在するか確認するための宅内確認実行要求をコンテンツ受信装置１００に送る（Ｓ８１５）。

【００６５】

コンテンツ受信装置１００の機器認証処理部１０８は、宅内確認実行要求を受け取り、その受信確認をコンテンツ送信装置２００に送る（Ｓ８１６）。

【００６６】

コンテンツ送信装置２００の機器認証処理部２０２は、受信確認を受け取ると、前記タイマー１０８１を停止し、前記宅内確認実行要求を発行してから受信確認を受け取るまでの計測値（Ｔ１）が所定の値（Ｔ）を超えていないことを確認する。計測値（Ｔ１）≦所定の値（Ｔ）である場合、コンテンツ受信装置１００は宅内に存在し、個人的利用の範囲内に存在する装置であると判断し、宅内確認結果としてコンテンツ受信装置１００へ送る（Ｓ８１７）。一方、計測値（Ｔ１）＞所定の値（Ｔ）である場合は、コンテンツ受信装置１００は宅外に存在する可能性があると判断し、以降の処理を中断して機器認証処理を終了する。

【００６７】

該宅内確認結果を受け取ったコンテンツ受信装置１００の機器認証処理部１０８は、受信確認をコンテンツ送信装置２００に送ると（Ｓ８１８）、コンテンツ送信装置２００の機器認証処理部２０２はコンテンツを暗号する際に使用する交換鍵を生成し、前記認証鍵を用いて交換鍵を暗号化し、該交換鍵を識別するためのＩＤと一緒にコンテンツ受信装置１００に送る（Ｓ８１９）。

【００６８】

コンテンツ受信装置１００の機器認証処理部１０８は、前記認証鍵を用いてコンテンツ送信装置２００から送信された交換鍵を復号し、受信確認を送る（Ｓ８２０）。

【００６９】

コンテンツ送信装置２００の機器認証処理部２０２は、受信確認を受け取ると、前記機器情報管理部２０３内の前記機器情報テーブル７１０にコンテンツ受信装置１００に関する情報を登録する（Ｓ８２１）。例えば、機器情報テーブル７１０内のＩＤ７１１のレコード７２１に示すように、前記Ｓ８０１で受け取ったコンテンツ受信装置１００のデバイスＩＤをデバイスＩＤ７１２に設定し、ネットワーク上でのコンテンツ受信装置１００のＭＡＣアドレスをアドレス情報７１３に設定し、管理テーブル７００内のカウンタ最大値７０２をカウンタ値７１４に設定し、アクセス状況７１６に『停止』を設定する。

【００７０】

以上から、コンテンツ送信装置２００の機器認証処理部２０２とコンテンツ受信装置１００の機器認証処理部１０８は、互いに共通の交換鍵を共有する。該交換鍵は、コンテンツを暗号化／復号化するための共通鍵を生成するために使用する。上記認証鍵、交換鍵、共通鍵の生成には、周知の鍵生成／鍵交換アルゴリズムを利用すれば良い。また、前記Ｓ８０９とＳ８１３の処理、Ｓ８１７とＳ８１９の処理をそれぞれ纏めても良い。

【００７１】

以上の手順は、宅内でのコンテンツ転送を行う場合に、コンテンツ送信装置とコンテンツ受信装置の間で実行する機器認証処理について説明した。

【００７２】

次に、前記図１に示したシステム構成において、ＨＤＤレコーダ２００（コンテンツ送信装置）と携帯電話５００（コンテンツ受信装置）との間で実行する宅外アクセス用の機器認証処理手順について、図９を用いて説明する。

【００７３】

まず、コンテンツ送信装置２００とコンテンツ受信装置５００は、前記図８で説明した機器認証処理８００を実施する。

【００７４】

その後、コンテンツ受信装置５００の機器認証処理部５１０は、宅外アクセス用認証要求を作成し、コンテンツ送信装置２００へ送る（Ｓ９０１）。該宅外アクセス用認証要求には、所定の計算アルゴリズムを用いて生成した乱数や前記の機器固有の情報などを含んでも良い。

【００７５】

コンテンツ送信装置２００の機器認証処理部２０２は、宅外アクセス用認証要求を受け取りその受信確認をコンテンツ受信装置５００に送ると（Ｓ９０２）、コンテンツ受信装置の場合と同様に自分の側からの宅外アクセス用認証要求を作成し、コンテンツ受信装置５００に送る（Ｓ９０３）。

【００７６】

コンテンツ受信装置５００の機器認証処理部５１０は、宅外アクセス用認証要求を受け取り、その受信確認をコンテンツ送信装置１００へ送る（Ｓ９０４）。

【００７７】

次に、コンテンツ送信装置２００の機器認証処理部２０２は、宅外アクセス用認証要求で受信した各情報を検証し、鍵情報の生成に必要なパラメータを付した宅外アクセス用認証応答をコンテンツ受信装置５００に送る（Ｓ９０５）。

【００７８】

コンテンツ受信装置５００の機器認証処理部５１０は、宅外アクセス用認証応答を受け取りその受信確認をコンテンツ送信装置２００に送った（Ｓ９０６）後、自分の側からの宅外アクセス用認証応答を作成し、コンテンツ送信装置の場合と同様に鍵情報の生成に必要なパラメータを付した宅外アクセス用認証応答をコンテンツ送信装置２００に送り（Ｓ９０７）、必要なパラメータを用いてコンテンツ送信装置２００と共通の認証鍵を生成する。

【００７９】

コンテンツ送信装置２００の機器認証処理部２０２は、宅外アクセス用認証応答を受け取りその受信確認をコンテンツ受信装置５００に送り、コンテンツ受信装置と同様に、必要なパラメータを用いてコンテンツ受信装置５００と共通の認証鍵を生成する（Ｓ９０８）。そして、コンテンツ送信装置２００の機器認証処理部２０２は、宅外からコンテンツを利用する際の機器認証処理およびコンテンツ暗号に使用するためのコンテンツ受信装置５００専用の宅外アクセス鍵を生成し、Ｓ９０８で生成した前記認証鍵を用いて宅外アクセス鍵を暗号化してコンテンツ受信装置５００に送る（Ｓ９０９）。

【００８０】

コンテンツ受信装置５００の機器認証処理部５１０は、宅外アクセス用鍵を受信すると、受信確認をコンテンツ送信装置１００へ送り（Ｓ９１０）、前記認証鍵を用いて宅外アクセス鍵を復号化する。

【００８１】

コンテンツ送信装置２００の機器認証処理部２０２は、受信確認を受け取ると、前記機器情報管理部２０３内の前記機器情報テーブル７１０にコンテンツ受信装置５００に関する情報を追加する（Ｓ９１１）。例えば、機器情報テーブル７１０内のＩＤ７１１のレコード７２２に示すように、ＩＤ７１１、デバイスＩＤ７１２、アドレス情報７１３、カウンタ値７１４、アクセス状況７１６は前記の通りに設定されており、さらに追加でコンテンツ受信装置５００に送った前記宅外アクセス用鍵を宅外アクセス鍵７１５に設定する。

【００８２】

一方、コンテンツ受信装置５００の機器認証処理部５１０は、機器情報管理部５１１に格納したリモートアクセス用情報テーブル１０００を生成または更新する（Ｓ９１２）。

【００８３】

ここで、図１０を用いて、該リモートアクセス用情報テーブル１０００の一構成例について説明する。

【００８４】

機器情報管理部５１１内で保持するリモートアクセス用情報テーブル１０００は、アドレス情報１００１、登録情報１００２、外部アクセス用共通鍵１００３から構成される。

【００８５】

アドレス情報１００１は、コンテンツ受信装置５００が宅外からコンテンツ送信装置２００やルータ１２にアクセスするために必要なアドレス情報、例えばＭＡＣアドレスやＩＰアドレス、ポート番号などを登録する。

【００８６】
登録情報１００２は、コンテンツ受信装置５００が宅外からコンテンツ送信装置２００やルータ１２にログインするために必要なユーザ名やパスワードを登録する。
外部アクセス用共通鍵１００３は、前記Ｓ９１０で受信した宅外アクセス鍵を設定する。
【００８７】
以上から、コンテンツ送信装置２００とコンテンツ受信装置５００は、通常の機器認証を実行した後、コンテンツ受信装置５００からの要求に応じて、宅外からコンテンツ送信装置２００に格納したコンテンツを利用するための宅外アクセス用の共通鍵を共有する。前記コンテンツ送信装置２００が生成する宅外アクセス鍵は、前記コンテンツ受信装置５００専用の共通鍵とし、他のコンテンツ受信装置には適用できないものとする。また、該宅外アクセス鍵は、宅外からのコンテンツ配信要求時に実行する機器認証処理、また／あるいはコンテンツ暗号化するための共通鍵を生成するために使用する。上記認証鍵、交換鍵、該宅外アクセス鍵の生成には、周知の鍵生成／鍵交換アルゴリズムを利用すれば良い。
【００８８】
ここで、前記Ｓ９０３～Ｓ９０８の処理を省略し、Ｓ９０９で通常の機器認証処理８００で共有した認証鍵を用いて宅外アクセス鍵を暗号化してコンテンツ受信装置５００へ送信する方法もある。また、通常の機器認証処理８００が終了後、コンテンツ送信装置２００が前記宅外アクセス用認証要求を受付け可能な時間を設け、所定の時間内にコンテンツ受信装置５００が宅外アクセス用認証要求を発行する必要があるようにしても良い。さらに、前記Ｓ９０１～Ｓ９０２の処理を、通常の機器認証処理８００内のＳ８１９の直前に行うようにしても良く、その場合はＳ８２０の後にＳ９０９～Ｓ９１０を実行、あるいはＳ８１９とＳ９０９の処理を１つに纏めても良い。
【００８９】
次に、ユーザＡが前記携帯電話５００を宅外へ持ち出し、外出先Ｂから該携帯電話（コンテンツ受信装置）５００を用いて、ＨＤＤレコーダ（コンテンツ送信装置）２００のＨＤＤ２０５に記録したコンテンツを視聴する場合の手順について、図１１を用いて説明する。
【００９０】
まず、前記携帯電話５００の入力処理部５０９を用いてユーザＡがコンテンツ視聴を指示すると、携帯電話５００の制御部５１７は、コンテンツ送信装置一覧画面（図１５）を表示部／スピーカ５０５上に表示する。該コンテンツ送信装置一覧画面１５００には、記録メモリ５１３と、現在ネットワーク上に存在することを検出したコンテンツ送信装置（ＤＴＶ６００）と、機器情報管理部５１１で管理するリモートアクセス用情報テーブル１０００に登録されているコンテンツ送信装置２００を表示する（Ｓ１１０１）。
【００９１】
ここで、ネットワーク上に存在するコンテンツ送信装置を検出する方法としては、例えばネットワーク上の全装置に対して「コンテンツ送信機能を備えた機器の検出要求」を含んだＵＤＰパケットをマルチキャスト送信し、該機能を備えた装置のみが返信することにより、該コンテンツ送信装置を認識する方法がある。この方法は既存の技術を使用すればよく、例えばＳＳＤＰ（Ｓｉｎｐｌｅ Ｓｅｒｖｉｃｅ Ｄｉｓｃｏｖｅｒｙ Ｐｒｏｔｏｃｏｌ）やＤＬＮＡ（Ｄｉｇｉｔａｌ Ｌｉｖｉｎｇ Ｎｅｔｗｏｒｋ Ａｌｌｉａｎｃｅ）が挙げられる。
【００９２】
次に、ユーザＡが前記コンテンツ送信装置一覧画面１５００上でコンテンツ送信装置２００を選択すると、コンテンツ受信装置５００の制御部５１７は、前記リモートアクセス用情報テーブル１０００に登録されているコンテンツ受信装置５００のアドレス情報を参照し、無線通信処理部５１６から無線アクセスポイント２２とルータ２１を介してインターネット３経由でユーザＡ宅１のコンテンツ送信装置２００に対して、コンテンツ情報の

取得要求を送る（Ｓ１１０２）。
【００９３】
コンテンツ送信装置２００の制御部２１１は、通信制御部２０７を介して受信確認をコンテンツ受信装置５００へ送り（Ｓ１１０３）、ＨＤＤ２０５に格納しているコンテンツの一部あるいは全てに関する情報（例えばタイトル、日付、コピー制御情報、記録時間など）をコンテンツ受信装置５００へ送る（Ｓ１１０４）。
【００９４】
コンテンツ受信装置５００の制御部５１７は、受信確認をコンテンツ送信装置２００へ送り（Ｓ１１０５）、受信したコンテンツ情報をコンテンツ一覧画面（図１６）として表示部／スピーカ５０５上に表示する。ユーザＡは、該コンテンツ一覧画面１６００上で視聴したいコンテンツを入力処理部５０９経由で指示すると（Ｓ１１０６）、コンテンツ受信装置５００の機器認証処理部５１０は、宅外認証要求を作成する。宅外認証要求には、前記したデバイスＩＤを含む機器固有の情報と、前記宅外アクセス鍵あるいは該鍵を用いて生成した計算値と、証書を付してコンテンツ送信装置２００に送る（Ｓ１１０７）。
【００９５】
コンテンツ送信装置２００の機器認証処理部２０２は、宅外認証要求を受け取ると、前記機器情報管理部２０３内で管理している前記機器情報テーブル７１０に、コンテンツ受信装置５００のデバイスＩＤが登録されていることを確認した後、その受信確認をコンテンツ受信装置５００に送る（Ｓ１１０８）。もし前記機器情報テーブル７１０内に該コンテンツ受信装置５００のデバイスＩＤが登録されていない場合は、コンテンツ送信装置１００は以降の処理を中断する。
【００９６】
次に、コンテンツ送信装置２００の機器認証処理部２０２は、自分の側からの宅外認証要求を作成し、コンテンツ受信装置の場合と同様に、コンテンツ送信装置２００の固有情報と前記宅外アクセス鍵あるいは該鍵を用いて生成した計算値と、証書を付してコンテンツ受信装置５００に送る（Ｓ１１０９）。
【００９７】
コンテンツ受信装置５００の機器認証処理部５１０は、宅外認証要求を受け取り、その受信確認をコンテンツ送信装置２００へ送る（Ｓ１１１０）。
【００９８】
次に、コンテンツ送信装置２００の機器認証処理部２０２は、前記宅外認証要求で受信した各情報を検証し、前記宅外アクセス鍵あるいは該鍵を用いて生成した計算値と、鍵情報の生成に必要なパラメータを付した宅外認証応答をコンテンツ受信装置５００に送る（Ｓ１１１１）。
【００９９】
コンテンツ受信装置５００の機器認証処理部５１０は、前記宅外認証応答を受け取りその受信確認をコンテンツ送信装置２００に送った（Ｓ１１１２）後、自分の側からの宅外認証応答を作成し、コンテンツ送信装置の場合と同様に、鍵情報の生成に必要なパラメータを付した宅外認証応答をコンテンツ送信装置２００に送り（Ｓ１１１３）、必要なパラメータを用いてコンテンツ送信装置２００と共通の宅外認証鍵を生成する。
【０１００】
コンテンツ送信装置２００の機器認証処理部２０２は、宅外認証応答を受け取り、その受信確認をコンテンツ受信装置５００に送り、コンテンツ受信装置と同様に、必要なパラメータを用いてコンテンツ受信装置５００と共通の認証鍵を生成する（Ｓ１１１４）。そして、前記機器情報テーブル７１０内のコンテンツ受信装置５００のカウンタ値７１４が０になっていないことを確認した後（Ｓ１１１５）、コンテンツを暗号する際に使用する宅外用交換鍵を生成し、前記宅外認証鍵を用いて宅外用交換鍵を暗号化し、該宅外用交換鍵を識別するためのＩＤと一緒にコンテンツ受信装置５００に送る（Ｓ１１１６）。
【０１０１】
コンテンツ受信装置５００の機器認証処理部５１０は、前記宅外認証鍵を用いてコンテ

ンツ送信装置２００から送信された宅外用交換鍵を復号し、受信確認を送る（Ｓ１１１７）。

【０１０２】

コンテンツ送信装置２００の機器認証処理部２０２は、受信確認を受け取ると、前記機器情報管理部２０３内の前記機器情報テーブル７１０にコンテンツ受信装置５００に関する情報を更新する（Ｓ１１１８）。具体的には、アクセス状況７１６を『停止』から『宅外』に更新する。

【０１０３】

その後、コンテンツ受信装置５００の制御部５１７は、所望のコンテンツの視聴要求をコンテンツ送信装置２００に送る（Ｓ１１１９）。その際、該視聴要求には、Ｓ１１１６で受信した前記宅外用交換鍵を識別するためのＩＤを付加しても良い。

【０１０４】

コンテンツ送信装置２００の制御部２１１は、コンテンツ視聴要求に対して受信確認を送り（Ｓ１１２０）、機器認証処理部２０２は前記宅外用交換鍵の識別ＩＤが正しいかチェックし、機器情報更新部１０８２は前記機器情報管理部２０３内のタイマー１０８１を定期的に（例えば、1分間隔や１０分間隔等）通知が入るように設定し、起動する。また、機器認証処理部２０２は前記宅外用交換鍵を用いてコンテンツを暗号化するための共通鍵を生成し、暗号／復号処理部２０６に該共通鍵を設定する。

【０１０５】

そして、ＨＤＤ２０５から読み出した所望のコンテンツを暗号／復号処理部２０６で暗号化しながらコンテンツ受信装置５００に送る（Ｓ１１２１）。ここで、コンテンツ送信中に前記タイマー１０８１から通知が入る毎に、機器情報更新部１０８２は前記機器情報テーブル７１０内のカウンタ値７１４を更新する（例えば、カウンタ値をデクリメントする）。

【０１０６】

コンテンツ受信装置５００の機器認証処理部５１０は、前記宅外用交換鍵を用いてコンテンツを復号化するための共通鍵を生成し、暗号／復号処理部５１４に該共通鍵を設定する。そして、無線通信処理部５１６と無線暗号／復号処理部５１５を介して受信したコンテンツを暗号／復号処理部５１４で復号化し、デコーダ５０４でデコードしながら表示部／スピーカ５０５に出力する。

【０１０７】

以上から、予め宅内においてコンテンツ送信装置とコンテンツ受信装置との間で宅外アクセス用の機器認証処理９００を実施し、該認証処理に成功したコンテンツ受信装置を宅外へ持ち出した場合に限り、宅外専用の認証処理Ｓ１１０７～Ｓ１１１７を実行して成功すれば、宅内のコンテンツ送信装置から宅外のコンテンツ受信装置へコンテンツを転送することができる。

コンテンツ転送が終了すると、コンテンツ送信装置はタイマー１０８１を停止し、前記宅外用交換鍵を破棄し、コンテンツ受信装置が続けて別のコンテンツの視聴要求を発行しても再度宅外専用の認証処理を実行しない限り送信しないようにしても良い。

【０１０８】

また、コンテンツ送信装置は、管理テーブル７００内の外部アクセス最大数７０３を用いて、宅外から同時にアクセスできるコンテンツ受信装置の台数を制限することができる。

【０１０９】

上記Ｓ１１１９において、コンテンツ送信装置２００はコンテンツの「視聴要求」を受信しているが、宅外からそれ以外の要求、例えば「コピー要求」あるいは「ムーブ要求」を受信した場合は、コンテンツの不正利用を極力避けるため拒否するようにしても良い。

【０１１０】

ここで、コンテンツ送信装置２００からコンテンツ受信装置５００にコンテンツを送信するのに使用するプロトコルは特定のものに限定されることはなく、ＲＴＰ、ＨＴＴＰ、

ＦＴＰ等を用いることが可能である。コンテンツの伝送に際しては各転送プロトコルにおけるペイロード部分に共通鍵を用いて予め決められたアルゴリズムにより暗号化したコンテンツを収容して送信すれば良い。暗号化アルゴリズムとしては例えば周知の暗号化技術であるＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）を使用すれば良い。

【０１１１】

また、コンテンツ送信装置が定期的に更新する機器情報テーブル７１０内のカウンタ値７１４は、宅内および宅外の両方のコンテンツ送信時で共用することも可能であるが、図１２に示すように、宅内と宅外で別々のカウンタ値を使用することも可能である。その場合、それぞれのカウンタ値に設定する最大値を別々の値にしても良い（すなわち管理テーブル７００の宅内用カウンタ最大値７０２、宅外用カウンタ最大値７０４）。

【０１１２】

以上のことから、宅内の機器に宅外からアクセスするコンテンツ受信装置は、予め宅内でコンテンツ送信装置との間で通常の機器認証処理と宅外アクセス用の機器認証処理を実施し、宅外アクセス鍵を共有すると同時にコンテンツ送信装置の機器情報テーブルに該コンテンツ受信装置に関する情報を登録してもらう。これにより、前記コンテンツ受信装置はあくまでも個人所有の機器として見なすことができ、宅外に持ち出した場合でも、コンテンツの個人利用の範囲を超えることなく、安全に視聴することができる。

【実施例２】

【０１１３】

本実施の形態の特徴は、コンテンツの個人的利用の範囲を超えることなく、不正な視聴／複製を防止しながら、外出先の不特定のコンテンツ受信装置で宅内のコンテンツを視聴可能にすることである。

【０１１４】

図１３は、システム構成例を示したものであり、ユーザＡは携帯電話５００を外出先に持ち出し、該携帯電話５００と同じ外出先に設置してある大画面のＤＴＶ６００で自宅内のＨＤＤレコーダ２００のコンテンツを視聴する場合を想定している。ＤＴＶ６００は、前記ＤＴＶ１００と同様の構成とする。

【０１１５】

ユーザＡが外出先２のＤＴＶ６００で自宅内のＨＤＤレコーダ２００のコンテンツを視聴する手順について、図１４を用いて説明する。

【０１１６】

ユーザＡは、前記実施例１で説明した通り、自宅内でＨＤＤレコーダ２００（コンテンツ送信装置）と携帯電話５００との間で宅外アクセス用機器認証９００を実行し、両者間で宅外アクセス鍵を共有しておく。

【０１１７】

ユーザＡは携帯電話５００を外出先（ホテル等）に持って行き、同じ場所にあるＤＴＶ６００で宅内のコンテンツを視聴する場合、まずは前記Ｓ１１０１～Ｓ１１１８と同様の手順でコンテンツ送信装置２００と携帯電話５００との間でコンテンツ情報の取得、宅外専用の機器認証処理を実行する。

【０１１８】

前記宅外専用の機器認証処理に成功し、両者間で宅外用交換鍵と該交換鍵の識別ＩＤを共有した後、携帯電話５００（コントローラ）の制御部５１７は、例えばネットワーク上の全装置に対して「再生機能を備えた機器の検出要求」を含んだＵＤＰパケットをマルチキャスト送信し、該機能を備えた装置のみが返信するなど、前記ＤＬＮＡなどの周知技術を利用してネットワーク上に他のコンテンツ再生装置が存在するか否か検出し、存在する場合は表示部／スピーカ５０５にコンテンツ再生装置一覧画面（図１７）を表示する。

【０１１９】

ユーザＡは該一覧画面１７００上で入力処理部５０９を介してコンテンツ再生装置を選択（この場合、ＤＴＶ６００）すると、制御部５１７はＤＴＶ６００に対してコンテンツ

視聴発行要求を送る（Ｓ１４０１）。コンテンツ視聴発行要求には、視聴するコンテンツに関する情報とリモートアクセス用情報テーブル１０００に登録しているコンテンツ送信装置２００のアドレス情報１００１を含み、場合によって登録情報１００２を付しても良い。

【０１２０】

前記コンテンツ視聴発行要求を受信したＤＴＶ６００（コンテンツ受信装置）は、受信確認をコントローラ５００に送り（Ｓ１４０２）、コントローラ５００との間で通常の機器認証処理８００を実施する。この際、コントローラ５００の機器認証処理部５１０は、Ｓ８１９においてＤＴＶ６００に送付する交換鍵と識別ＩＤとして、前記Ｓ１１１６でコンテンツ送信装置２００と共有した宅外用交換鍵とその識別ＩＤを使用する。これにより、コンテンツ送信装置２００、コントローラ５００、コンテンツ受信装置６００の間で同じ宅外用交換鍵と該交換鍵の識別ＩＤが共有できたことになる。

【０１２１】

その後、ＤＴＶ６００は、コンテンツ送信装置２００に対してコンテンツ視聴要求を送る（Ｓ１４０３）。該コンテンツ視聴要求には、前記宅外用交換鍵の識別ＩＤを付加する。また、コンテンツ送信装置２００側で必要に応じてフォーマット変換あるいは画質変換を実施してコンテンツ送信してもらうために、ＤＴＶ６００で再生可能なデータ・フォーマット（例えば、ＭＰＥＧ２－ＴＳやＨ．２６４等）や画質（ＨＤやＳＤ、７６０ｐや１０８０ｉ等）の情報を該コンテンツ視聴要求に含むことも可能である。該コンテンツ視聴要求と別の要求で発行しても良い。

【０１２２】

コンテンツ送信装置２００の制御部２１１は、前記コンテンツ視聴要求を受け取ると、受信確認をＤＴＶ６００に送る（Ｓ１４０４）。そして機器認証処理部２０２は前記宅外用交換鍵の識別ＩＤが正しいことをチェックし、機器情報更新部１０８２は前記機器情報管理部２０３内のタイマー１０８１を定期的に通知が入るように設定し、起動する。

【０１２３】

また、機器認証処理部２０２は前記宅外用交換鍵を用いてコンテンツを暗号化するための共通鍵を生成し、暗号／復号処理部２０６に該共通鍵を設定する。そして、ＨＤＤ２０５から読み出した所望のコンテンツを暗号／復号処理部２０６で暗号化しながらＤＴＶ６００に送る（Ｓ１４０５）。ここで、コンテンツ送信中に前記タイマー１０８１から通知が入る毎に、機器情報更新部１０８２は前記機器情報テーブル７１０内のカウンタ値７１４を更新する。

【０１２４】

ＤＴＶ６００は、前記宅外用交換鍵を用いてコンテンツを復号化するための共通鍵を生成し、暗号／復号処理部１１０に該共通鍵を設定する。そして、ルータ２１と通信処理部１１１を介して受信したコンテンツを暗号／復号処理部１１０で復号化し、デコーダ１０４でデコードしながら表示部／スピーカ１０５に出力する。

【０１２５】

以上から、予め宅内においてコンテンツ送信装置との間で宅外アクセス鍵を共有したコントローラを宅外へ持ち出した際に、該コンテンツ送信装置と該コントローラとの間で宅外用交換鍵を共有できた場合に限り、該コントローラは通常の認証処理に成功した宅外のコンテンツ受信装置に前記宅外用交換鍵を渡すことができる。

【０１２６】

これにより、コンテンツの個人利用の範囲を超えることなく、安全に宅外のコンテンツ受信装置で宅内のコンテンツを視聴することができる。

【実施例３】

【０１２７】

前述した実施例２では、コンテンツ送信装置２００は、コントローラ５００に対してのみ、コンテンツの暗号化に必要な宅外用交換鍵を送信していた。したがって、コントローラ５００とコンテンツ受信装置６００との間の鍵交換（通常の機器認証処理８００）につ

いては関与していない。

【０１２８】

本実施の形態の特徴は、コントローラ５００がコンテンツ送信装置２００に対して、コンテンツ受信装置６００に該宅外用交換鍵を渡した旨を通知することである。

【０１２９】

図１８、図１９を用いて、本実施例の特徴を示す視聴手順について説明する。

まず図１８に示す通り、コンテンツ送信装置２００の機器情報テーブル７１０に、宅外での使用時に、デバイスＩＤ７１２が示す装置の代わりにコンテンツを受信する別の装置のデバイスＩＤを設定する代理デバイスＩＤ７１８を設ける。その他に、代理アドレス情報（ＭＡＣアドレスやＩＰアドレス等）や代理用カウンタ値を追加しても良い。

【０１３０】

次に、ユーザＡが外出先２のＤＴＶ６００で自宅内のＨＤＤレコーダ２００のコンテンツを視聴する手順について、図１９を用いて説明する。

コンテンツ送信装置２００とコントローラ５００との間のＳ１１０１～Ｓ１１８までの処理は、図１２と同様である。また、コントローラ５００とコンテンツ受信装置６００との間のＳ１４０１～Ｓ１４０２、機器認証処理８００までの処理も図１２と同様である。

【０１３１】

その後、コントローラ５００は、コンテンツ送信装置２００に対して、自装置の代わりに機器認証済みの外部装置（この場合、コンテンツ受信装置６００）を用いてコンテンツ受信するための外部機器設定要求を発行する（Ｓ１９００）。該設定要求には、コンテンツ受信装置６００に関する情報－例えば、デバイスＩＤやＭＡＣアドレスなどを含む。

【０１３２】

該外部機器設定要求を受信したコンテンツ送信装置２００は、該要求に含まれたコンテンツ受信装置６００のデバイスＩＤを、前記機器情報テーブル７１０内の代理デバイスＩＤ７１８に設定し（Ｓ１９０１）、受信確認をコントローラ５００に対して発行する（Ｓ１９０２）。

【０１３３】

その後、コンテンツ受信装置６００は、コンテンツ送信装置２００に対してコンテンツ視聴要求を発行する（Ｓ１４０３）。この際、該視聴要求には、コンテンツ受信装置６００のデバイスＩＤあるいはアドレス情報（ＭＡＣアドレスやＩＰアドレス等）を含む。

【０１３４】

該コンテンツ視聴要求を受信したコンテンツ送信装置２００は、該要求が代理デバイスＩＤ７１８から発行されたものであるか確認した後、受信確認をコンテンツ受信装置６００に発行し、前記宅外用交換鍵を用いて暗号化したコンテンツを転送する。

【０１３５】

ここで、コンテンツ送信装置２００は、該代理デバイスＩＤ７１８のコンテンツ受信装置６００に対してコンテンツ送信中に、デバイスＩＤ７１２のコントローラ５００からコンテンツ視聴要求を受信した場合、コンテンツ受信装置６００へのコンテンツ送信を中断する、あるいは該コンテンツ視聴要求を拒否し、同時に送信するデバイスは一台としても良い。

【０１３６】

以上から、コンテンツの個人利用の範囲を超えることなく、安全に宅外のコンテンツ受信装置で宅内のコンテンツを視聴することができる。

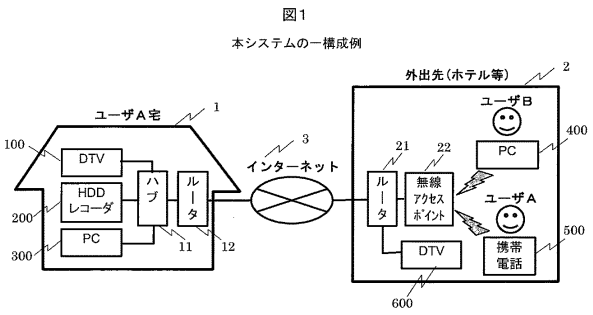
【符号の説明】

【０１３７】

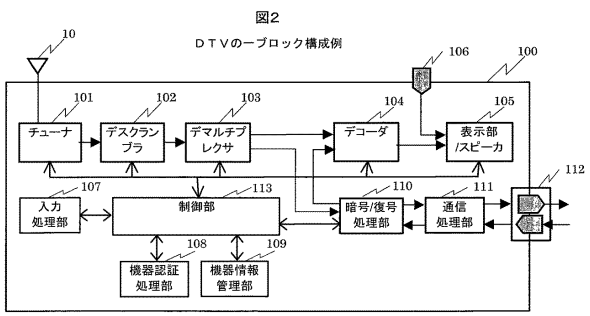
２００・・・コンテンツ送信装置
１００、５００・・・コンテンツ受信装置
１０８、２０２、５１０・・・機器認証処理部
１０９、２０３、５１１・・・機器情報管理部
１１０、２０６、５１４・・・暗号／復号処理部

２０５・・・ＨＤＤ
５１３・・・記録メモリ
１０８１・・・タイマー
１０８２・・・機器情報更新部
１０８３・・・機器情報格納部
７０・・・機器情報
７００・・・管理テーブル
７１０・・・機器情報テーブル

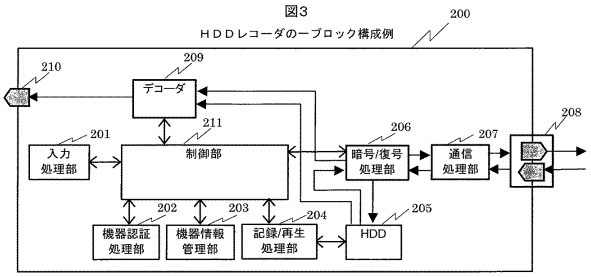
【図１】



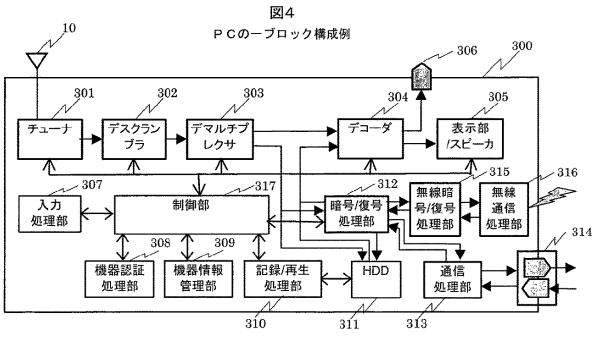
【図２】



【図３】

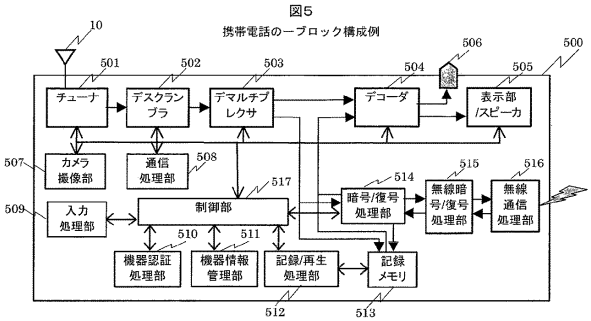


【図４】



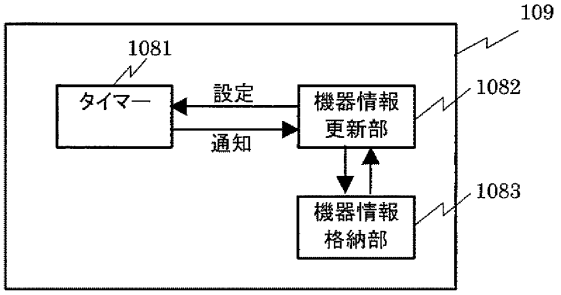
【図５】

図5
携帯電話の一ブロック構成例



【図６】

図6
機器情報管理部の構成例



【図７】

図7
機器情報の一構成例

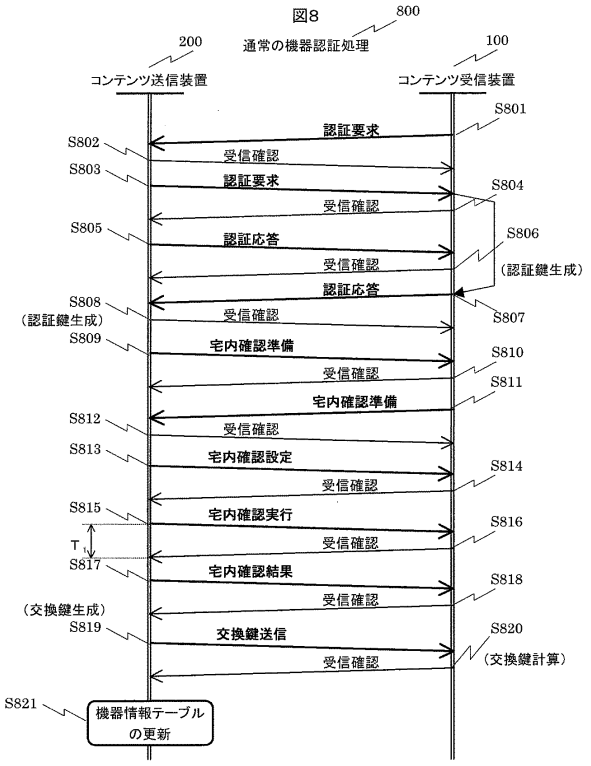
管理テーブル 700

機器認証最大数	34	701
カウンタ最大値	1000	702
外部アクセス最大数	3	703

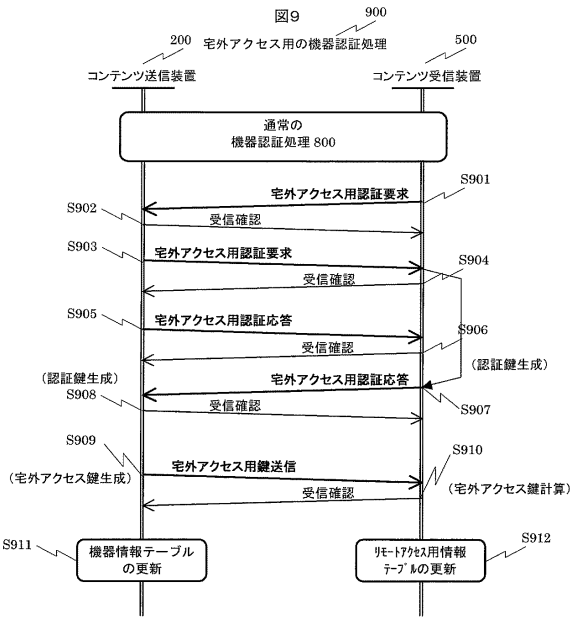
機器情報テーブル 710

ID 711	デバイス ID 712	アドレス情報（例：MACアドレス） 713	カウンタ値 714	宅外アクセス鍵 715	アクセス状況 716	
0	aabbccddee (DTV100)	AAAAA	1000	—	停止	721
1	ffgghhiijj (携帯電話 500)	BBBBB	459	*@$%**#1?	宅外	722
2	kkllmmnn (PC300)	CCCCC	173	—	宅内	723
..	...	...	...	...	...	
33	...	...	...	...	...	

【図８】



【図９】

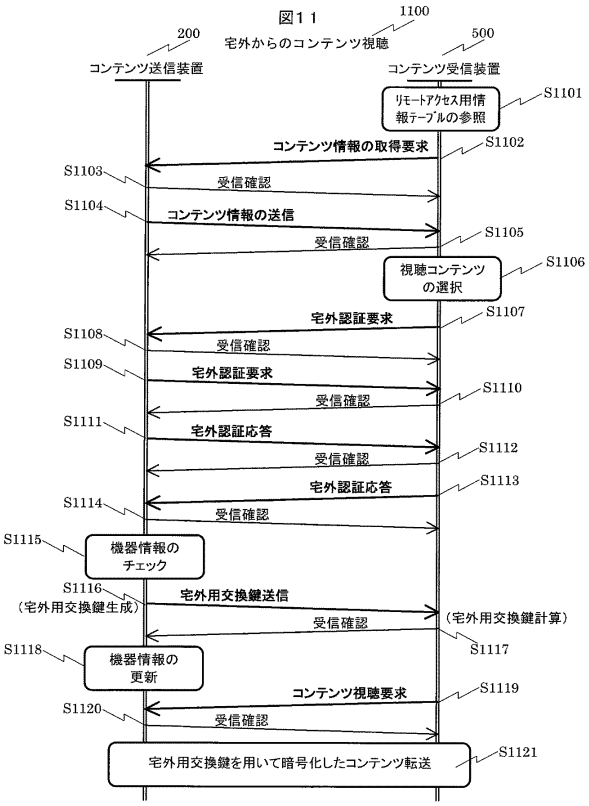


【図１０】

図10
リモートアクセス用情報テーブル 1000

ID	アドレス情報 1001		登録情報 1002		外部アクセス用共通鍵 1003
	MAC	IP	ユーザ名	パスワード	
0	DDDDD	133.144.XXX.YYY	Paul	********	*@$%**#1?
..	...	...	...	...	...

【図１１】



【図１２】

図12

機器情報の一構成例

管理テーブル 700

機器認証最大数	34
宅内用カウンタ最大値	1000
外部アクセス最大数	3
宅外用カウンタ最大値	1500

704

機器情報テーブル 710

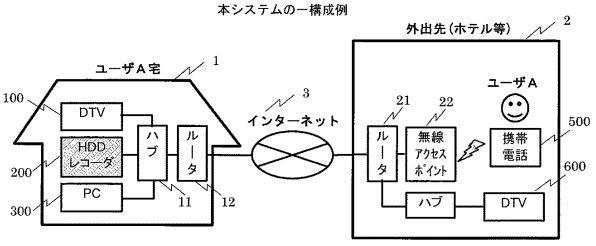
717

ID	デバイス ID	アドレス情報（例：MACアドレス）	宅内用カウンタ値	宅外アクセス鍵	アクセス状況	宅外用カウンタ値
0	aabbccddee (DTV100)	AAAAA	680	—	宅内	—
1	ffgghhiijj (携帯電話 500)	BBBBB	459	*@$%**#1?	宅外	1500
2	kkllmmnn (PC300)	CCCCC	173	—	停止	—
..	...	...	...	...	...	...
33	...	...	...	...	...	...

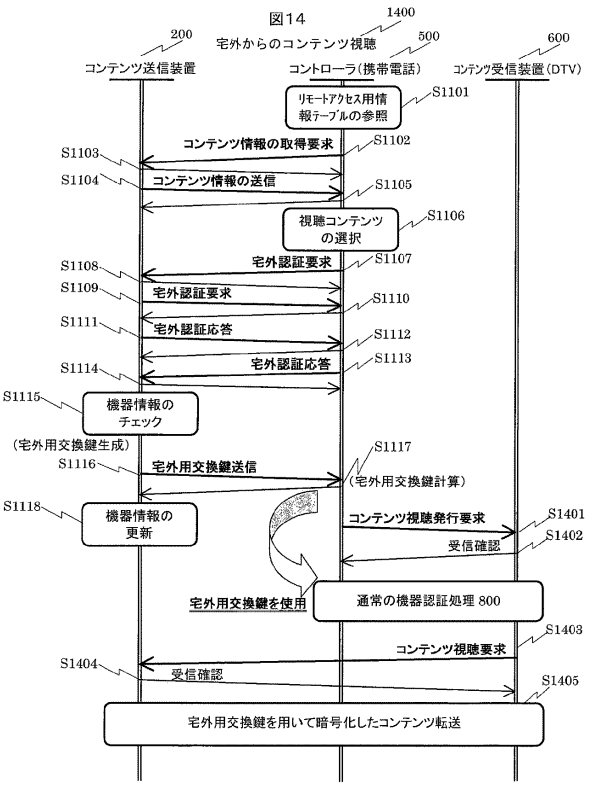
【図１３】

図13

本システムの一構成例



【図１４】

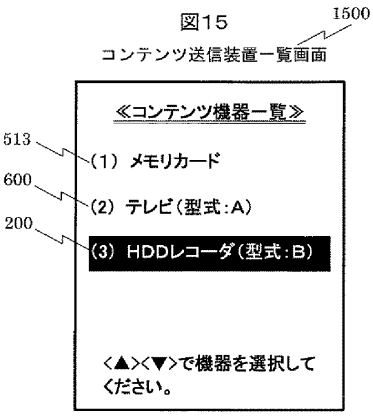


【図１５】

図15

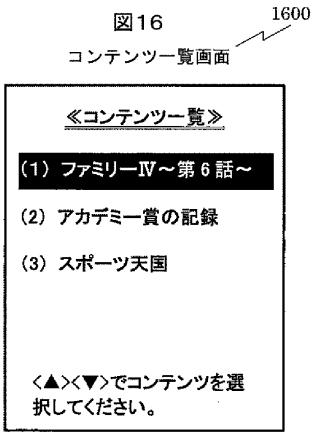
1500

コンテンツ送信装置一覧画面



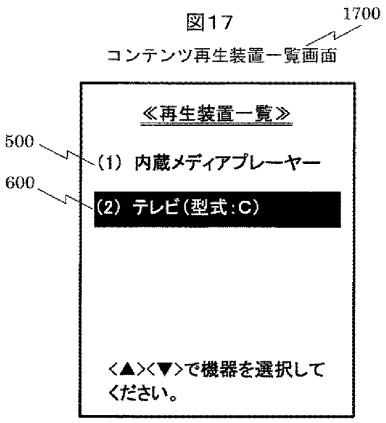
【図１６】

図16



【図１７】

図17



【図１８】

図18

機器情報の一構成例

管理テーブル 700

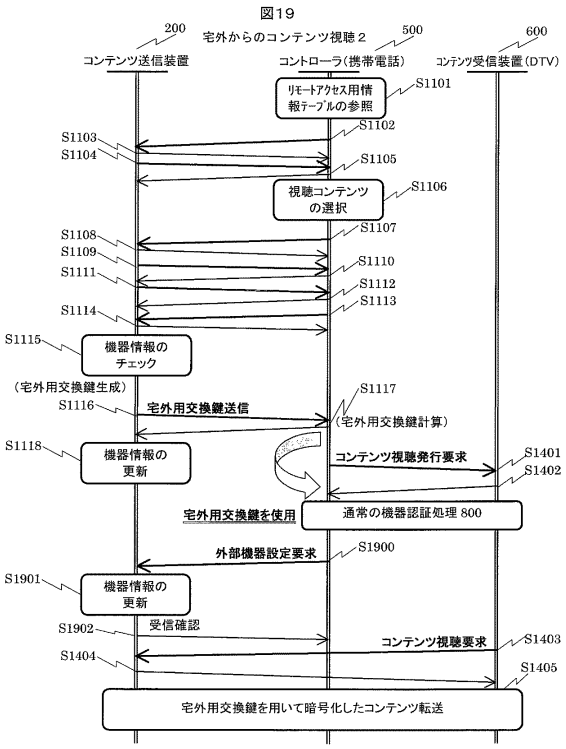
機器認証最大数	34
宅内用カウンタ最大値	1000
外部アクセス最大数	3
宅外用カウンタ最大値	1500

機器情報テーブル 710

ID	デバイス ID 712	アドレス情報 (例:MACｱﾄﾞﾚｽ)	宅内用 カウンタ値	宅外アクセス鍵	アクセス状況	宅外用 カウンタ値	代理 ﾃﾞﾊﾞｲｽID 718
0	aabbccddee (DTV100)	AAAAA	680	—	宅内	—	—
1	ffgghhiijj (携帯電話 500)	BBBBB	459	*@$%**#1?	宅外	1500	ooppqqrr (DTV 600)
2	kkllmmnn (PC300)	CCCCC	173	—	停止	—	—
..	...	...	...	...	...	...	...
33	...	...	...	...	...	...	...

【図１９】

図19



フロントページの続き

(51)Int.Cl.			FI		
G06F 21/45	***(2013.01)***		G06F	21/45	
G06F 21/60	***(2013.01)***		G06F	21/60	320

(56)参考文献 特開2003－037802（JP，A）
特開2006－339847（JP，A）
特開2005－341348（JP，A）
特開2005－352910（JP，A）
特開2004－180020（JP，A）
特開2008－054348（JP，A）
特開2005－102021（JP，A）

(58)調査した分野(Int.Cl.，DB名)
G06F 21／10
G06F 21／30
G06F 21／45
G06F 21／60
G06Q 50／10
H04L 9／14
H04L 9／32