

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4982031号
(P4982031)

(45) 発行日 平成24年7月25日 (2012. 7. 25)

(24) 登録日 平成24年4月27日 (2012. 4. 27)

(51) Int. Cl.

F I

G 0 6 F 12/14 (2006. 01)
 G 0 6 Q 50/10 (2012. 01)
 G 0 6 Q 30/06 (2012. 01)
 G 0 9 C 1/00 (2006. 01)
 H 0 4 L 9/08 (2006. 01)

G 0 6 F 12/14 3 2 0 E
 G 0 6 F 17/60 1 4 2
 G 0 6 F 17/60 3 0 2 E
 G 0 9 C 1/00 6 4 0 E
 H 0 4 L 9/00 6 0 1 B

請求項の数 10 (全 21 頁) 最終頁に続く

(21) 出願番号 特願2004-8621 (P2004-8621)
 (22) 出願日 平成16年1月16日 (2004. 1. 16)
 (65) 公開番号 特開2005-204093 (P2005-204093A)
 (43) 公開日 平成17年7月28日 (2005. 7. 28)
 審査請求日 平成18年10月6日 (2006. 10. 6)
 審判番号 不服2011-1118 (P2011-1118/J1)
 審判請求日 平成23年1月18日 (2011. 1. 18)

(73) 特許権者 000005108
 株式会社日立製作所
 東京都千代田区丸の内一丁目6番6号
 (74) 代理人 100100310
 弁理士 井上 学
 (72) 発明者 田中 真愉子
 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デジタルメディア開発
 本部内
 (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デジタルメディア開発
 本部内

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およびコンテンツ送信方法、コンテンツ受信方法

(57) 【特許請求の範囲】

【請求項 1】

コンテンツ送信装置であって、
 ネットワークを介して接続されたコンテンツ受信装置との間で認証を実行し、認証鍵情
 報を共有する認証手段と、

前記コンテンツ受信装置との間で交換鍵情報を共有し、前記交換鍵情報に基づいて生成
 された共通鍵情報により前記コンテンツ受信装置に送信する前記コンテンツの暗号化処理
 を行う暗号化手段と、

前記コンテンツ受信装置への所定のコマンド要求の送信から、前記コマンド要求の送信
 に対応して前記コンテンツ受信装置から送信される前記認証鍵情報に基づいて生成された
 認証情報を伴う応答の到達までの時間を計測するタイマー手段とを有し、

前記認証手段が前記認証情報を伴う応答が正しくないと判定した場合、もしくは前記タ
 イマー手段での計測結果が所定の値を超えた場合には、前記コンテンツ受信装置との間の
 前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ送信装置。

【請求項 2】

請求項 1 に記載のコンテンツ送信装置であって、

前記タイマー手段により、前記コマンド要求の送信から、前記応答の到達までの時間の
 計測を少なくとも 2 回以上実施し、計測された複数の時間に対する平均値が所定の値を超
 えた場合には、前記コンテンツ受信装置との間の前記交換鍵情報の共有を行わない

10

20

ことを特徴とするコンテンツ送信装置。

【請求項 3】

コンテンツ受信装置であって、

ネットワークを介して接続されたコンテンツ送信装置が送信するコンテンツを受信するコンテンツ受信処理手段と、

前記コンテンツ送信装置との間で認証を実行し、認証鍵情報を共有する認証手段と、

前記コンテンツ送信装置との間で交換鍵情報を共有し、前記交換鍵情報に基づいて生成された共通鍵情報により前記コンテンツ送信装置から送信されたコンテンツの復号化処理を行う復号化手段と、

前記コンテンツ送信装置へ所定のコマンド要求の送信から、前記コマンド要求の送信に対応して前記コンテンツ送信装置から送信される前記認証鍵情報に基づいて生成された認証情報を伴う応答の到達までの時間を計測するタイマー手段とを有し、

認証手段が前記認証情報を伴う応答が正しくないと判定した場合、もしくは前記タイマー手段での計測結果が所定の値を超えた場合には、前記コンテンツ送信装置との間の前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ受信装置。

【請求項 4】

請求項 3 に記載のコンテンツ受信装置であって、

前記タイマー手段により、前記コマンド要求の送信から、前記応答の到達までの時間の計測を少なくとも 2 回以上実施し、計測された複数の時間に対する平均値が所定の値を超えた場合には、前記コンテンツ送信装置との間の前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ受信装置。

【請求項 5】

コンテンツ送信装置とコンテンツ受信装置との間のコンテンツ伝送システムであって、前記コンテンツ送信装置は、

前記コンテンツ受信装置との間で認証し、認証鍵情報を共有を実行する認証手段と、

前記コンテンツ受信装置との間で交換鍵情報を共有し、前記交換鍵情報に基づいて生成された共有鍵情報により前記コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、

前記コンテンツ受信装置への所定のコマンド要求の送信から、前記コマンド要求の送信に対応して前記コンテンツ受信装置から送信される前記認証鍵情報に基づいて生成された認証情報を伴う応答の到達までの時間を計測するタイマー手段と、を有し、

前記コンテンツ受信装置は、

コンテンツ送信装置から受信するコンテンツを受け取るコンテンツ受信処理手段と、

前記コンテンツ送信装置との間で認証を実行する第 2 の認証手段と、

前記コンテンツ送信装置との間で共有された前記交換鍵情報に基づいて生成された共有鍵情報により前記コンテンツ送信装置から受信したコンテンツの復号化処理を行う復号化手段と、を有し、

前記コンテンツ送信装置の有する前記タイマー手段での計測結果が所定の値を超えた場合には、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前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ伝送システム。

【請求項 6】

コンテンツ送信装置とコンテンツ受信装置との間のコンテンツ伝送システムであって、

前記コンテンツ送信装置は、

前記コンテンツ受信装置との間で認証を実行し、認証鍵情報を共有する認証手段と、

前記コンテンツ受信装置との間で交換鍵情報を共有し、前記交換鍵情報に基づいて生成された共有鍵情報により前記コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、

前記コンテンツ受信装置へ所定のコマンド要求の送信から、前記コマンド要求の送信に

10

20

30

40

50

対応して前記コンテンツ受信装置から送信される前記認証鍵情報に基づいて生成された認証情報を伴う応答の到達までの時間を計測するタイマー手段と、を有し、

前記コンテンツ受信装置は

前記コンテンツ送信装置から受信するコンテンツを受け取るコンテンツ受信処理手段と

、

前記コンテンツ送信装置との間で認証を実行する第2の認証手段と、

前記コンテンツ送信装置との間で共有された前記交換鍵情報に基づいて生成された共有鍵情報により前記コンテンツ送信装置から受信したコンテンツの復号化処理を行う復号化手段と、

前記コンテンツ送信装置への所定の第2のコマンド要求の送信から、前記第2のコマンド要求の送信に対応して前記コンテンツ送信装置から送信される前記認証鍵情報に基づいて生成された第2の認証情報を伴う応答の到達までの時間を計測する第2のタイマー手段と、を有し、

前記コンテンツ送信装置の有するタイマー手段での計測結果が所定の値を超えた場合、あるいは前記コンテンツ送信装置の有する前記認証手段が前記認証情報を伴う応答を正しくないと判定した場合は、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前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ伝送システム。

【請求項7】

コンテンツ送信方法であって、

ネットワークを介して接続されたコンテンツ受信装置との間で認証を実行し、認証鍵情報を共有し、

前記コンテンツ受信装置への所定のコマンド要求の送信から、前記コマンド要求の送信に対応して前記コンテンツ受信装置から送信される前記認証鍵情報に基づいて生成された認証情報を伴う応答の到達までの時間を計測し、

前記コンテンツ受信装置との間で交換鍵情報を共有し、前記交換鍵情報に基づいて生成された共通鍵情報により前記コンテンツ受信装置に送信する前記コンテンツの暗号化処理を行い、

前記認証情報を伴う応答が正しくないと判定した場合、もしくは計測された前記時間が所定の値を超えた場合には、前記コンテンツ受信装置との間の前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ送信方法。

【請求項8】

請求項7に記載のコンテンツ送信方法であって、

前記コマンド要求の送信から、前記応答の到達までの時間の計測を少なくとも2回以上実施し、計測された複数の時間に対する平均値が所定の値を超えた場合には、前記コンテンツ受信装置との間の前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ送信方法。

【請求項9】

コンテンツ受信方法であって、

コンテンツ送信装置との間で認証を実行し、認証鍵情報を共有し、

前記コンテンツ送信装置へ所定のコマンド要求の送信から、前記コマンド要求の送信に対応して前記コンテンツ送信装置から送信される前記認証鍵情報に基づいて生成された認証情報を伴う応答の到達までの時間を計測し、

前記コンテンツ送信装置との間で交換鍵情報を共有し、前記交換鍵情報に基づいて生成された共通鍵情報により前記コンテンツ送信装置から送信されたコンテンツの復号化処理を行い、

前記認証情報を伴う応答が正しくないと判定した場合、もしくは計測された前記時間が所定の値を超えた場合には、前記コンテンツ送信装置との間の前記交換鍵情報の共有を行わない

10

20

30

40

50

ことを特徴とするコンテンツ受信方法。

【請求項10】

請求項9に記載のコンテンツ受信方法であって、

前記コマンド要求の送信から、前記応答の到達までの時間の計測を少なくとも2回以上実施し、計測された複数の時間に対する平均値が所定の値を超えた場合には、前記コンテンツ送信装置との間の前記交換鍵情報の共有を行わない

ことを特徴とするコンテンツ受信方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は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と記す）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と記す）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。

またその一方では大容量HDDの低価格化により、家庭用の録画装置としてもHDDを内蔵してこれに映像音声情報をデジタル記録するようなHDD録画装置が登場してきており、ディスクを録画媒体として使うことに拠る使い勝手の良さが着目されている。

上記したようなHDDを利用した録画装置やPCなどでは映像音声情報は装置内に固定されたHDDに録画されているため、家の中の、他の部屋で録画した番組を視聴しようとするような場合には装置自体を持ち運ぶしかなく、VTRなど取替え可能な媒体を利用する録画再生装置を複数備えて行えるような、媒体レベルでの映像音声情報の持ち運びは実現が難しかった。

【0003】

そこで、このような録画装置に有線あるいは無線LAN（Local Area Network）のインターフェースを搭載して、ネットワークを介して他のPCあるいは受信装置に送信することにより、宅内のどこでも録画された映像音声情報を視聴できるようにすることが考えられている。

一方コンテンツ等の情報の著作権保護のため、デジタルAV機器に取り入れられているコピープロテクトの方法の一例として例えば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（非特許文献1に記載）。

そして、装置間、あるいはネットワーク間での著作権保護のためのコピープロテクトを実現するための技術がいくつか開示されている。例えば特許文献1、特許文献2に開示されている。

【0004】

【特許文献1】特開2000-287192号公報

【0005】

【特許文献2】特開2001-358706号公報

【非特許文献1】Hitachi, Ltd. 他、5C Digital Transmission Content Protection White Paper

【発明の開示】

【発明が解決しようとする課題】

【0006】

上記した従来技術で、家庭用の録画装置に有線あるいは無線LAN（Local A

10

20

30

40

50

rea Network) のインターフェースを搭載して、コンテンツをネットワークを介して他の PC あるいは受信装置に送信して、宅内のどこでも録画された映像音声情報を視聴できるようにする場合従来は、著作権を保護すべき映像音声情報（以下コンテンツとして説明する）の著作権保護については配慮がされておらず、HDD に録画されている映像音声情報は、LAN を介して受信した他の PC において更に HDD に保存することが可能であり、扱える映像音声情報はコピーが自由に行える「コピー制限なし」のコンテンツでなければならなかった。

【0007】

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映像および音声データ（以下コンテンツと呼ぶ）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。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。

【0008】

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、例えば非特許文献 1 に記載されている D T C P 方式がある。D T C P 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。

【0009】

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、D T C P 方式と同様な考え方により、著作権保護のためのコピープロテクトを実現するための技術がいくつか開示されている。例えば特許文献 1 は、ネットワーク上のデジタルコンテンツ流通のためのコピープロテクトの方式に D T C P と同様の手法を適用するための技術が開示されており、特許文献 2 にも同様にコンテンツを著作権保護のために暗号化して通信する装置間を構成するための技術が開示されている。

そして、これらはコンテンツを有線あるいは無線 LAN を介して伝送する際には、送信側と受信側が同じ家の中に有るかどうかは考慮していない。むしろ、配信サーバからダウンロードを行うような場合には、送信側はプロバイダのサイトに有り、受信側は一般家庭などに有ることが普通である。

【0010】

したがって PC の HDD や HDD を内蔵した録画装置でコンテンツを録画して、ここから宅内の他の装置に LAN を介した伝送を行おうとする場合に上記の技術を適用したとしても、宅内の LAN がインターネットに接続されているとインターネットを介して接続される他の宅内に置かれている受信装置でコンテンツを受信して表示することができ、しかもその範囲はインターネットに接続されていれば世界中のあらゆる場所に広がることになる。

このような状況では、例え上記したような技術でコピープロテクトを行おうとしても、録画装置の使用者がこの録画装置をインターネットからアクセス可能な状態にすることによって、上記のコピープロテクトを備えた受信装置であれば自由にコンテンツを受信して表示することができ、本来の著作権保護の目的である個人的利用の範囲を大きく逸脱することになってしまう。

【0011】

本発明の目的は、宅内の有線または無線のLANを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成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或いは情報送信装置、受信装置およびコンテンツ伝送方法を提供することにある。

【課題を解決するための手段】

【0012】

前記目的は、その一例として特許請求の範囲に記載の構成により達成できる。

【発明の効果】

【0016】

本発明によれば、宅内の有線または無線のLANを利用したコンテンツ送信装置、受信装置およびコンテンツ伝送の信頼性向上を図ることができる。

【発明を実施するための最良の形態】

【0017】

以下本発明の実施の形態について図面を用いて説明する。

【実施例1】

【0018】

以下本発明の実施例1について説明する。

図1は実施例1に係るコンテンツ送信装置100およびコンテンツ受信装置200の構成を示したものであり、コンテンツ送信装置100とコンテンツ受信装置200とは互いにLANを介して接続されている。

コンテンツ送信装置100はLANを介してコンテンツ受信装置200に送信するコンテンツを送り出すコンテンツ送信回路101、コンテンツ送信回路101の出力するコンテンツを暗号化する暗号化回路102、暗号化回路102の出力および認証回路104の入出力を、LANを介して他の装置とやり取りするネットワーク通信処理回路103、LAN上に接続される他の装置との間で情報をやり取りして装置間の相互認証を行う認証回路104、認証回路104での処理に必要な情報を蓄える不揮発メモリ105、認証回路104の出力する情報に基づき暗号化回路102でのコンテンツ暗号化のために必要な鍵情報を生成する鍵生成回路106、認証回路104で相互認証に成功した回数を計測して保持するカウンタ回路107、認証回路104が発生する認証応答要求などの情報を他の装置に送信してから該情報に対する応答情報が到達するまでの時間を測定するタイマー回路108から成る。コンテンツ送信回路101の送信するコンテンツは特定の種類の物に限定されることはなく、例えばTV放送から受信している番組の映像および音声データや、HDDやDVDなどのディスクまたはテープなどの記録媒体から再生している映像および音声データなどが適用できる。図1においては放送受信のためのチューナや録画再生のための手段およびネットワークでの伝送に先立ち必要となるデータ圧縮処理回路などについては図面上では省略している。送信しようとするコンテンツの種類に応じてこれらの手段を適宜構成に加えればよい。コンテンツ送信回路101から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」の識別コードを付してコンテンツ受信装置に送信される。

【0019】

コンテンツ受信装置200はLANを介して送られてきたコンテンツを受信するコンテンツ受信回路201、コンテンツ送信装置100の暗号化回路102で暗号化されたコンテンツをネットワーク通信処理回路203から受け取り復号化してコンテンツ受信回路201に出力する復号化回路202、他の装置との間でネットワークを介して復号化回路202への入力および認証回路204の入出力をやりとりするネットワーク通信処理回路203、他の装置との間で情報をやり取りして装置間の相互認証を行う認証回路204、認証回路204での処理に必要な情報を蓄える不揮発メモリ205、認証回路204の出力する情報に基づき復号化回路202でのコンテンツ復号化のために必要な鍵を生成する鍵生成回路206から成る。コンテンツ受信回路201の出力である映像および音声データはディスプレイ装置によって表示されたりディスクやテープなどの記録媒体に記録された

りその利用形態は様々であり、本発明はその形態が特定の物に限定されることはない。図1ではディスプレイや録画の手段や受信したデータ圧縮処理済みコンテンツの伸張復元手段は省略しているが、受信したコンテンツの利用形態に応じ適宜構成に加えればよい。なお、受信したコンテンツは該コンテンツと共に送信される「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」の識別コードに従って処理され、「コピー制限なし」「一回限りコピー可」のコンテンツ記録媒体への記録が可能であり、「一回限りコピー可」のコンテンツを記録した場合にはそれ以後該コンテンツは「コピー不可」として取り扱う。

【0020】

図2はコンテンツ送信装置100およびコンテンツ受信装置200を含むLANの構成例を示したものである。1台のコンテンツ送信装置100と2台のコンテンツ受信装置200a、200bは有線LANのケーブルによりネットワークハブ装置400にそれぞれ接続され、ネットワークハブ装置400はさらにルータ300に接続される。ルータ300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。図2中の点線はコンテンツが送受信される装置とその方向を示している。

【0021】

図2のLANの構成は一例を示したに過ぎず、コンテンツ受信装置200は3台以上接続されていてもよい。またコンテンツ送信装置も2台以上接続されていてもよく、その場合にはそれぞれのコンテンツ送信装置から同時に異なるコンテンツをコンテンツ受信装置に対して、LANの帯域の許す限り送信することが可能である。なお、本発明における必要最低限の構成はコンテンツ送信装置およびコンテンツ受信装置各1台がLANに接続された状態である。

【0022】

図2に示す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) 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があるが、本発明はそのどちらかに限定される物ではない。

【0023】

コンテンツ送信装置100、およびコンテンツ受信装置200a、200b、ルータ300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300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。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300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】

図3はコンテンツ送信装置100とコンテンツ受信装置200によるコンテンツ送受信の際の、手順の一例を示したものである。左側がコンテンツ送信装置100を、右側がコ

コンテンツ受信装置 200 をそれぞれ表しており、両者の間の、情報の送受信のタイミングと方向を矢印により示している。

コンテンツの送信に先立ちコンテンツ送信装置 100 とコンテンツ受信装置 200 との間で互いに相手方の装置の認証を行い、相手方の装置が著作権保護の規則に則って正しく製造された装置であることを確認してからコンテンツの伝送を行うようにする。認証のための情報の送受信には通信プロトコルとして 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 3 においては TCP によるコネクション確立および廃棄のためのデータの送受信については省略してある。

10

始めにコンテンツ受信装置 200 の側から認証要求を作成する。認証要求には特定の認証機関により生成されコンテンツ受信装置 200 の不揮発メモリ 205 に保持される装置固有の公開鍵と該公開鍵に対する証書を付してコンテンツ送信装置 100 に送る。

公開鍵および証書は不揮発メモリ 205 にコンテンツ受信装置 200 の製造時に予め記憶させておく。コンテンツ送信装置 100 は、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 200 に送ると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認証機関が発行したコンテンツ送信装置 100 の固有の公開鍵とその証書を付してコンテンツ受信装置側 200 に送る。

【0025】

その一方でコンテンツ送信装置 100 は所定の公開鍵署名アルゴリズムに基づきコンテンツ受信装置 200 の認証を行う。公開鍵署名アルゴリズムでコンテンツ受信装置 200 の正当性を確認したらプレ認証応答要求をコンテンツ受信装置 200 に送信し、それに対応するプレ認証応答が送信されるのを待つ。

20

コンテンツ受信装置 200 の側でもコンテンツ送信装置 100 からの認証要求を受け取り、公開鍵署名アルゴリズムに基づきコンテンツ送信装置 100 の認証を行い、平行してプレ認証応答要求がコンテンツ送信装置 100 から送信されるのを待つ。プレ認証応答要求を受けたコンテンツ受信装置 200 はコンテンツ送信装置 100 の正当性を確認処理が終了し、認証応答を発行できる状態になるとプレ認証応答をコンテンツ送信装置 100 に送る。

【0026】

30

コンテンツ送信装置 100 はプレ認証応答を受けるとコンテンツ受信装置 200 へ認証応答要求を送り、タイマー回路 108 をスタートさせる。そして、認証応答要求に応じてコンテンツ受信装置 200 から送信される認証応答が受信されるまでの時間 T1 を測定する。測定値 T1 が所定の値を超えている場合には認証を不成功と判定する。時間 T1 はネットワークの状態の影響が大きく、ネットワーク負荷が大きい場合等は測定時間 T1 が一時的に所定の値を超えてしまう場合も考えられる。それを考慮し、時間測定の処理 P1 を複数回実行し、例えば、最大値、最小値を排除した平均値のような統計的な処理により T1 を算出し認証の成功を判断してもよい。

さらに、カウンタ 107 の数値をチェックし、現在値が所定の値を超えている場合には認証は不成功とし、認証に成功した場合にはカウンタ 107 の値を 1 だけ増加させる。認証が成功した場合には認証応答を発行してコンテンツ受信装置 200 に送信する。

40

以上のようにして相互に認証に成功すると互いに共通の認証鍵が生成されて共有化される。認証鍵の生成には Diffie-Hellman など周知の鍵交換アルゴリズムを利用すれば良い。

【0027】

認証鍵の共有が完了するとコンテンツ送信装置 100 は交換鍵と乱数を生成し、交換鍵と乱数をそれぞれ認証鍵により暗号化してコンテンツ受信装置 200 に送る。なお、図 3 では交換鍵と乱数を別々にコンテンツ送信装置 100 からコンテンツ受信装置 200 に送信しているがこれらをまとめて送るようにしてもよい。コンテンツ受信装置 200 では認証鍵を用いてコンテンツ送信装置 100 から送信された交換鍵を復号し、同様に受信して

50

復号した乱数と共に保有する。続いてコンテンツ送信装置100およびコンテンツ受信装置200各々の側で交換鍵と乱数を用いて予め定められた計算アルゴリズムに従い共通鍵を生成する。このようにして得た共通鍵によってコンテンツ送信装置100からコンテンツを暗号化して送信し、コンテンツ受信装置200では復号化されたコンテンツを受信することができるようになる。

【0028】

実際にコンテンツの送信を始めるにあたっては例えば図3に示すようにコンテンツ受信装置200からコンテンツ送信要求を送り、これをきっかけとしてコンテンツの送信を行うようにする。コンテンツの送信が完了したらコンテンツ送信装置100より送信完了を知らせても良いし、逆にコンテンツ受信装置200側から送信終了を要求するようにしても良い。また、予め送信するコンテンツのデータ量がわかっている場合には特にどちらかの側から送信完了を知らせたり要求したりする必要は無い。必要なコンテンツの送信がすべて完了した後は、コンテンツ送信装置100は認証鍵、交換鍵、乱数、共通鍵を破棄する。コンテンツ受信装置200においてもコンテンツの受信が完了したら認証鍵、交換鍵、乱数、共通鍵を破棄するようにし、再度コンテンツの受信を行おうとする際には新たに認証要求から行えば良いが、コンテンツ送信装置100が他のコンテンツ受信装置にコンテンツを送信していて以前の鍵が再度利用できる場合には、コンテンツ受信装置200からコンテンツ送信装置100に現在の鍵の情報を問い合わせた上で以前の鍵を再利用してもよい。

【0029】

コンテンツ送信装置100からコンテンツ受信装置200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、先にも記した通りRTP、HTTP、ftp (File Transfer Protocol) 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AES (Advanced Encryption Standard) などを利用できる。

【0030】

以上のようにして、図1に示したコンテンツ送信装置100とコンテンツ受信装置200との間で共通の暗号化用の鍵を用いて暗号化したコンテンツを送受信するので、LAN上の他の装置によってコンテンツが受信されたとしても正しく復号化することができず、コンテンツが使用者のもとで不正に複製されるのを防止することができる。

図2に示すように一度に2台以上のコンテンツ受信装置によりコンテンツを受信することも可能である。この場合には各々のコンテンツ受信装置とコンテンツ送信装置との間で図3に示す手順に従い相互に認証を行った後にコンテンツの伝送を行えばよい。このときに1台のコンテンツ送信装置が認証をおこなったコンテンツ受信装置の数はカウンタ107でカウントされるので、コンテンツ送信装置の側でコンテンツ受信装置の認証を行う際に台数の上限を定めることによって、コンテンツ受信装置を同時に複数台用いて作成できるコンテンツの複製の数を制限することが可能になる。コンテンツ受信装置の台数の上限に関しては例えばIEEE1394を用いて一度に接続可能なコンテンツ受信装置の上限である62台かあるいはそれよりも小さな値とすればよい。

【0031】

また、コンテンツ受信装置200がインターネットを介して使用者の家とは異なる他の家に置かれているような場合は、図3の時間測定の処理P1で測定した時間T1の測定結果にて制限を設ける。広域ネットワークおよびルータ300を介して送受信されるため、宅内における送受信よりも応答が帰るまでの所要時間が増加する。そこで、認証を成功と判断するための上限値を適当な値、一例として10ミリ秒など、に定めてやれば、コンテンツの伝送可能な範囲を使用者の宅内にとどめることが可能になる。

【0032】

また、T1の測定は通信プロトコルとして使用するTCPの送信データとその受信確

10

20

30

40

50

認（アクノレッジ）が返信されるまでの応答時間ではなく、認証の手続きの一環としての処理 P 1 の時間を計測ことで、他の装置がコンテンツ受信装置 200 への成りすましを抑制する。さらに、前に時間を計測処理 P 1 の事前準備としてプレコマンドを送信する手順を追加している。この手順により計算時間が時間測定結果に影響しない。よって装置の計算性能に依存しない時間計測を実現できる。

【実施例 2】

【0033】

以下本発明の実施例 2 について説明する。

実施例 2 において、コンテンツ送信装置 100 とコンテンツ受信装置 200 の構成は図 1 と同じである。

図 4 はコンテンツ送信装置 100 とコンテンツ受信装置 200 によるコンテンツ送受信の際の、手順の一例を示したものである。図 3 と同様に左側がコンテンツ送信装置 100 を、右側がコンテンツ受信装置 200 をそれぞれ表しており、両者の間の、情報の送受信のタイミングと方向を矢印により示している。基本的な処理手順は実施例 1 の図 3 と同じであるが、図 4 の例では装置相互の認証処理の結果として認証鍵を共有化した後、その認証鍵を用いてセキュアに伝送範囲確認プロセスを実施する点が異なる。

始めに認証処理プロセスを実施する。

【0034】

コンテンツ受信装置 200 の側から図 3 と同様の手順で認証要求を作成し、装置固有の公開鍵と該公開鍵に対する証書を付してコンテンツ送信装置 100 に送る。

コンテンツ送信装置 100 は、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 200 に送ると自分の側からの認証要求を作成し、装置固有の公開鍵とその証書を付してコンテンツ受信装置側 200 に送る。

その一方でコンテンツ送信装置 100 は所定の公開鍵署名アルゴリズムに基づきコンテンツ受信装置 200 の認証を行う。認証が成功した場合には認証応答を発行してコンテンツ受信装置 200 に送信する。

同様にしてコンテンツ受信装置 200 の側でもコンテンツ送信装置 100 からの認証要求を受け取った後認証を行い、成功した場合には認証応答を発行してコンテンツ送信装置 100 に送信する。

以上のようにして、相互に認証に成功すると互いに共通の認証鍵が生成されて共有化される。

【0035】

相互認証プロセスが成功すると伝送範囲確認プロセスを開始する。

まず、コンテンツ送信装置 100 側から伝送範囲確認要求を作成する。コンテンツ送信装置 100 は内部処理により生成した任意の値 N を付加しコンテンツ受信装置 200 に送信し、伝送範囲確認のためにタイマー回路 108 をスタートさせ、コンテンツ受信装置 200 からの伝送範囲確認応答を受信するまでの時間 T 3 の測定を開始する。

伝送範囲確認要求を受信したコンテンツ受信装置 200 は先の相互認証プロセスで共有化した認証鍵 K A U T H を用い、伝送範囲確認プロセスで合意されている暗号化アルゴリズム f を用いて伝送範囲確認応答データ R を $R = f(K A U T H, N)$ のように生成し、伝送範囲確認応答にデータ R を付加しコンテンツ送信装置 100 に送信する。

【0036】

一方、コンテンツ送信装置 100 においても同様の手順によりデータ R' を計算する。コンテンツ送信装置 100 は、応答データ R が自身で計算したデータ R' と比較し等しければ伝送範囲確認応答が相互認証したコンテンツ受信装置 200 から送信されたものであると判断する。更に、コンテンツ受信装置 200 からの伝送範囲確認応答を受信するまでの時間 T 3 が所定の値 T n を超えているか否かで、コンテンツ受信装置 200 が伝送可能の範囲にあるかを判断する。すなわち $R = R'$ と $T 3 < T n$ を同時に満たすとき伝送範囲確認プロセスは成功となる。

【0037】

なお、本処理手順では装置の計算能力の差の測定結果への影響を最小限に抑えるため、SHA-1 (Secure Hash Algorithm, revision 1) や AES (Advanced Encryption Standard) など計算負荷の低い暗号化アルゴリズムを用いることとする。また、SHA-1 や AES は D T C P 対応装置では実装されているため追加実装が必要ない点でも好適である。

また、実施例 1 と同様にカウンタ 1 0 7 の数値をチェックし、現在値が所定の値を超えている場合においても、伝送可能範囲の確認プロセスを不成功とし、伝送可能範囲の確認プロセスが成功した場合にはカウンタ 1 0 7 の値を 1 だけ増加させる。伝送可能範囲の確認プロセス完了後はコンテンツ送信のための鍵交換処理も実施例 1 と同じ処理なのでここでは記載を省略する。

10

以上のように、実施例 2 においても実施例 1 と同様の効果を得ることができる。さらに、伝送範囲確認応答の送信元を確認できるため、実施例 1 よりもセキュアに伝送範囲確認プロセスを実施でき、他の装置がコンテンツ受信装置 2 0 0 への成りすましを排除できる。

【実施例 3】

【0 0 3 8】

以下本発明の実施例 3 について説明する。

図 5 は実施例 3 に係るコンテンツ送信装置 5 0 0 およびコンテンツ受信装置 6 0 0 の構成を示したものである。図 5 に示すコンテンツ送信装置 5 0 0 およびコンテンツ受信装置 6 0 0 において図 1 のコンテンツ送信装置 1 0 0 およびコンテンツ受信装置 2 0 0 と異なる点は、コンテンツ受信装置 6 0 0 にも認証回路 6 0 4 が発生する認証要求などの情報を他の装置に送信してから該情報に対する応答情報が到達するまでの時間を測定するタイマー回路 6 0 8 を備える点である。

20

【0 0 3 9】

図 6 はコンテンツ送信装置 5 0 0 とコンテンツ受信装置 6 0 0 によるコンテンツ送受信の際の、手順の一例を示したものである。図 3 と同様に左側がコンテンツ送信装置 5 0 0 を、右側がコンテンツ受信装置 6 0 0 をそれぞれ表しており、両者の間の、情報の送受信のタイミングと方向を矢印により示している。基本的な処理手順は実施例 2 の図 4 と同じであるが、図 6 の例では伝送範囲確認のための時間測定をコンテンツ送信装置 5 0 0 とコンテンツ受信装置 6 0 0 の双方で、認証プロセスの手順の中で実施する点と双方で実施した時間測定結果を基に伝送範囲確認プロセスの成功を判定する点が異なる。

30

【0 0 4 0】

始めに認証処理プロセスを実施する。

コンテンツ受信装置 6 0 0 の側から図 3 と同様の手順で認証要求を作成し、装置固有の公開鍵と該公開鍵に対する証書を付してコンテンツ送信装置 5 0 0 に送る。コンテンツ送信装置 5 0 0 は、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 6 0 0 に送ると自分の側からの認証要求を作成し、装置固有の公開鍵とその証書を付してコンテンツ受信装置側 2 0 0 に送り、タイマー回路 5 0 8 をスタートさせ、コンテンツ受信装置 6 0 0 からの認証応答を受信するまでの時間 T 5 の測定を開始する。その一方でコンテンツ送信装置 5 0 0 は所定の公開鍵署名アルゴリズムに基づきコンテンツ受信装置 6 0 0 の認証を行う。認証が成功した場合には認証応答を発行してコンテンツ受信装置 6 0 0 に送信する。

40

【0 0 4 1】

コンテンツ受信装置 6 0 0 はコンテンツ送信装置 5 0 0 からの認証要求を受け取るとタイマー回路 6 0 8 をスタートさせ、コンテンツ送信装置 5 0 0 の認証処理を行い、成功した場合は認証応答を生成して送信するまでの時間 T 6 の測定を開始する。以上のようにして、相互に認証に成功すると互いに共通の認証鍵が生成されて共有化される。更に、コンテンツ送信装置 5 0 0 においては認証要求を送信してからコンテンツ受信装置 6 0 0 からの認証応答を受信するまでの時間 T 5、コンテンツ受信装置 6 0 0 においては、コンテンツ送信装置 5 0 0 からの認証要求を受信してからコンテンツ送信装置 5 0 0

50

へ認証応答を送信するまでの時間 T_6 の測定結果を得ている。
相互認証プロセスが成功すると伝送範囲確認プロセスを開始する。

【0042】

まず、コンテンツ送信装置 500 は伝送範囲確認要求を作成し、相互認証プロセスで測定した測定低時間 T_5 を付加しコンテンツ受信装置 600 に送信する。

また、コンテンツ受信装置 600 も伝送範囲確認要求を作成し、測定低時間 T_6 を付加しコンテンツ送信装置 500 に送信し、相互に測定低時間を交換する。

次に互いに、実伝送時間として $\Delta T = T_5 - T_6$ ($\Delta T' = T_5 - T_6$) を計算し、相互に認証鍵で暗号化し、伝送範囲確認応答として交換する。

そしてコンテンツ送信装置 500 側では自身で計算した実伝送時間 $\Delta T'$ とコンテンツ受信装置 600 から取得した ΔT を比較し、等しければそれがコンテンツ受信装置 600 から送信されたものであると判断する。更に、実伝送時間 $\Delta T'$ が所定の値 T_n を超えているか否かで、コンテンツ受信装置 600 が伝送可能な範囲にあるかを判断する。すなわち $\Delta T = \Delta T'$ と $\Delta T' < T_n$ を同時に満たすとき、コンテンツ送信装置 500 側での伝送範囲確認プロセスは成功となる。

【0043】

コンテンツ受信装置 600 側においても同様の処理を行い、コンテンツ送信装置 500 より取得した $\Delta T'$ が自身で計算した ΔT と等しく、かつ、 $\Delta T' < T_n$ を満たすとき伝送範囲確認プロセスは成功となる。

コンテンツ送信装置 500 によるカウンタ 507 の数値をチェック処理および、伝送可能範囲の確認プロセス完了後の鍵交換処理も実施例 1 と同じ処理なのでここでは記載を省略する。

以上のように、実施例 3 においても実施例 1 と同様の効果を得ることができる。さらに、伝送範囲確認応答の送信元をコンテンツ送信側、コンテンツ受信側双方で確認できるため、実施例 2 よりもセキュアに伝送範囲確認プロセスを実施できる。コンテンツ受信装置 600 でも伝送範囲確認プロセスを実施するため、伝送可能な範囲を超えたコンテンツの受信は拒絶することができる。

【実施例 4】

【0044】

以下本発明の実施例 4 について説明する。

図 7 は実施例 4 に係るコンテンツ送信装置 700 およびコンテンツ受信装置 800 の構成を示している。図 7 に示すコンテンツ送信装置 700 およびコンテンツ受信装置 800 において第 5 図のコンテンツ送信装置 500 およびコンテンツ受信装置 600 と異なる点は無線 LAN を使ってコンテンツの伝送を行う点にあり、LAN との接続に無線ネットワーク通信処理回路 703 および 803 を用い、WEP (Wired Equivalent Privacy) 暗号処理回路 709 および 809 を備えている点にある。WEP は無線 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周知の暗号化方式であり、送信装置と受信装置の間でセキュリティ保護がなされた通信をユーザの管理下で実現することができる。

【0045】

図 8 は図 7 に示したコンテンツ送信装置 700 とコンテンツ受信装置 800 を用いた宅内のネットワークの構成の一例を示している。図 8 においてデータ送信装置 700 と 2 台のデータ受信装置 800 a、800 b が無線アクセスポイント 900 により無線 LAN で接続される。無線 LAN アクセスポイント 900 はさらにルータ 300 に接続され、ルータ 300 は図 2 に示したルータ 300 と同様にしてインターネットに接続される。

【0046】

図 7 に示すコンテンツ送信装置 700 とコンテンツ受信装置 800 との間で相互認証とそれに続くコンテンツの伝送を行おうとする場合には、認証回路 704 および 804 により WEP 暗号処理回路 709 および 809 において WEP 処理が施されているかどうかをチェックする。そして WEP 処理が使われていなければ、相互認証とそれに続くコンテン

ツの伝送を行わないようにするか、もしくは使用者にW E P処理を起動させるように促す表示を行うなどの必要な処理をおこなうようにする。以上のようにして、無線L A Nを用いてコンテンツの伝送を行う際には必ずW E P処理が施された状態となるようにする。この結果、コンテンツ送信装置700およびコンテンツ受信装置800の使用者が意識しないところで無線L A Nを介して他のデータ受信装置が接続されてコンテンツの不正なコピーが行われてしまうのを防止する。

【0047】

上記した以外の点に関しては図5から図7までに示された本発明の実施例3のコンテンツ送信装置およびコンテンツ受信装置により実施されるコンテンツの伝送方法と全く同様にして、コンテンツの不正な複製の作成を抑止して著作権の保護を行うことができ、その際に個人の利用範囲を逸脱したコンテンツの伝送が行なわれないようにすることができる。なお、ここでは実施例3と同じ方法にて説明したが、無線L A Nに係る構成以外を実施例1および実施例2と同じ回路構成に認証手順を使えば、実施例1および実施例2と同等の効果を得られる。

【0048】

以上で説明した本発明の実施の形態では有線L A Nを用いる場合と無線L A Nを用いる場合とを別々に説明したが、これらを同時に使用して家庭内のL A Nを構築することも可能であり、その際にも本発明を適用することが可能である。図9は有線と無線を両方用いて構成したL A Nにおいて本発明の実施形態であるコンテンツ送信装置とコンテンツ受信装置を使用する場合の構成を示した物である。

【0049】

図9においてコンテンツ送信装置500、コンテンツ受信装置600a、600bはネットワークハブ装置400を介して互いに接続され、更に無線アクセスポイント900もネットワークハブ装置400に接続される。無線アクセスポイント900にはコンテンツ送信装置700、コンテンツ受信装置800a、bが無線L A Nによって接続されている。またネットワークハブ装置400はルータ300に接続されており、これにより宅内のL A Nはインターネットに接続される。

【0050】

図9の中で細い矢印の点線で示したのはコンテンツの伝送方向であり、各々のコンテンツ送信装置およびコンテンツ受信装置は相手方が有線L A Nで接続されているのか無線L A Nで接続されているのかを意識することなく、互いの間でコンテンツの伝送を行うことができる。その際の伝送手順は図6を用いて説明したのと全く同様でよい。また、無線L A Nを用いるコンテンツ送信装置700およびコンテンツ受信装置800a、bにおいては先に説明したのと同様にW E Pの稼動をチェックしてから相互の認証およびコンテンツの伝送を行うようにすればよい。この場合でも有線あるいは無線のL A Nを単独で構成した場合と同様にコンテンツ伝送の際の不正な複製の作成を防止することができ、しかもコンテンツ伝送を個人的利用の範囲にとどめることができる。

【0051】

以上の説明ではネットワークを介して伝送する対象を映像情報等のコンテンツとし、コンテンツを送受信するコンテンツ送信装置、受信装置として説明したが、映像情報等以外の種類の情報についても同様であり、これらの情報を入力する情報処理装置についても、本発明を実施できる。

【0052】

以上説明した本発明の実施の形態における、認証回路、鍵生成回路、暗号化回路、復号化回路、カウンタ回路、タイマー回路等はハードウェアによる実現に限定される物ではなく、これらのうちの全部ないしは全てをマイクロプロセッサとその上で実行されるソフトウェア処置によって実現しても良く、その際でも本発明の効果を発揮する上での違いはない。

【0053】

なおここまでの説明の都合上、コンテンツ送信装置とコンテンツ受信装置を別々の物と

しているが、コンテンツをディスクあるいはテープなどの記録媒体上に記録再生を行う装置においては、コンテンツ送信装置とコンテンツ受信装置の両方を兼ね備えるようにして構成してもよく、その際には認証回路や不揮発メモリなどを共用化することができる。

上記の課題を解決するため本発明では、ネットワークを介してコンテンツの送信を行うコンテンツ送信装置において、データの送受信を行うネットワーク通信処理手段と、ネットワークを介して接続されるコンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、該コンテンツ受信装置への所定のコマンド要求の送信から、該コマンド要求の送信に対応して該コンテンツ受信装置から送信される応答の到達までの時間を計測するタイマー手段(時間計測手段)とを有し、該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないようにする。

10

また、上記したコンテンツ送信装置における所定のコマンド要求を、所定の認証情報を伴うコマンド要求として、認証手段が前記所定の認証情報を伴う応答の認証の判定を行い認証されなかった場合、もしくはタイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないようにする。

また、上記したコンテンツ送信装置において、コンテンツ受信装置からの応答の到達までの時間の計測を少なくとも2回以上実施し、所定の統計的処理を行った結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないようにする。

20

更に、上記の課題を解決するため本発明では、ネットワークを介してコンテンツを受信するコンテンツ受信装置において、該コンテンツ送信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ送信装置に対して自身の認証要求を発行する認証手段と、該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ送信装置が送信するコンテンツの暗号復号化処理を行う復号化手段と、該コンテンツ送信装置への所定のコマンド要求の送信から、該コマンド要求の送信に対応して該コンテンツ送信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置から送出されるコンテンツの受信を行わないようにする。

30

すなわち、本発明では、コンテンツ送信装置とコンテンツ受信装置はコンテンツの伝送を行うのに先立ち、所定の認証情報を伴うコマンド要求の中の認証情報の判定、もしくは所定の認証情報を伴うコマンド要求に対応した応答の到達までの時間による認証の判定を行い、認証されなかった場合にはコンテンツ受信装置へのコンテンツ送出を行わないようにする。

これにより、宅内の有線または無線のLANを利用したコンテンツの伝送の際に、コンテンツの不正な複製を防止するコピープロテクションを実施することができ、しかもコンテンツの正当な視聴や複製の作成を個人的利用の範囲に制限することができる。

なお、上述の実施例は少なくとも下記を開示している。

40

(1)

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、

該ネットワークを介して接続されるコンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、

該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、

該コンテンツ受信装置への所定のコマンド要求の送信から、該コマンド要求の送信に対応して該コンテンツ受信装置から送信される応答の到達までの時間を計測するタイマー手

50

段とを有し、

該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置。

(2)

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続されるコンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、

該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、

該コンテンツ受信装置への所定の認証情報を伴うコマンド要求の送信から、該認証情報を伴うコマンド要求の送信に対応して該コンテンツ受信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

該認証手段が前記所定の認証情報を伴う応答の認証の判定を行い認証されなかった場合、もしくは該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置。

(3)

前記タイマー手段により、前記コンテンツ受信装置への所定のコマンド要求もしくは所定の認証情報を伴うコマンド要求の送信から、前記コンテンツ受信装置からの応答の到達までの時間の計測を少なくとも2回以上実施し、所定の統計的処理を行った結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とする(1)または(2)のいずれかに記載のコンテンツ送信装置。

(4)

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続されるコンテンツ送信装置が送信するコンテンツを該ネットワーク通信手段を介して受信するコンテンツ受信処理手段と、

該コンテンツ送信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ送信装置に対して自身の認証要求を発行する認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ送信装置が送信するコンテンツの暗号復号化処理を行う復号化手段と、

該コンテンツ送信装置への所定のコマンド要求の送信から、該コマンド要求の送信に対応して該コンテンツ送信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置から送出されるコンテンツの受信を行わないことを特徴とするコンテンツ受信装置。

(5)

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、
該ネットワークを介して接続されるコンテンツ送信装置が送信するコンテンツを該ネットワーク通信手段を介して受信するコンテンツ受信処理手段と、

該コンテンツ送信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ送信装置に対して自身の認証要求を発行する認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ送信装置が送信するコンテンツの暗号復号化処理を行う復号化手段と、

該コンテンツ送信装置への所定の認証情報を伴うコマンド要求の送信から、該認証情報を伴うコマンド要求の送信に対応して該コンテンツ送信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

認証手段が前記所定の認証情報を伴う応答の認証の判定を行い認証されなかった場合、もしくは該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置から送出されるコンテンツの受信を行わないことを特徴とするコンテンツ受信装置。

10

20

30

40

50

(6)

前記タイマー手段により、前記コンテンツ送信装置への所定のコマンド要求もしくは所定の認証情報を伴うコマンド要求の送信から、前記コンテンツ送信装置からの応答の到達までの時間の計測を少なくとも2回以上実施し、所定の統計的処理を行った結果が所定の値を超えた場合には、該コンテンツ送信装置から送出されるコンテンツの受信を行わないことを特徴とする(4)または(5)のいずれかに記載のコンテンツ受信装置。

(7)

ネットワークを介して接続されるコンテンツ受信装置にコンテンツを送信する際に、該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、

10

該コンテンツ受信装置への所定のコマンド要求の送信から、該コマンド要求の送信に対応して該コンテンツ受信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ送信装置。

(8)

ネットワークを介して接続されるコンテンツ送信装置が送信するコンテンツを受信する際に、該コンテンツ送信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ送信装置に対して自身の認証要求を発行する認証手段と、

20

該コンテンツ送信装置への所定のコマンド要求の送信から、該コマンド要求の送信に対応して該コンテンツ送信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置から送出されるコンテンツの受信を行わないことを特徴とするコンテンツ受信装置。

(9)

ネットワークを介して接続されるコンテンツ送信装置とコンテンツ受信装置との間のコンテンツ伝送方法であって、

該コンテンツ送信装置は、

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、

該コンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、

30

該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、

該コンテンツ受信装置への所定のコマンド要求の送信から、該コマンド要求の送信に対応して該コンテンツ受信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

該コンテンツ受信装置は

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、

40

該コンテンツ送信装置から受信するコンテンツを該ネットワーク通信手段から受け取るコンテンツ受信処理手段と、

該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置から受信した認証要求に対する認証の判定を行う認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの暗号復号化処理を行う復号化手段とを有し、

該コンテンツ送信装置の有する該タイマー手段での計測結果が所定の値を超えた場合には、該コンテンツ送信装置から該コンテンツ受信装置へのコンテンツ送出を行わないことを特徴とするコンテンツ伝送方法。

50

(10)

ネットワークを介して接続されるコンテンツ送信装置とコンテンツ受信装置との間のコンテンツ伝送方法であって、

該コンテンツ送信装置は、

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、

該コンテンツ受信装置に送信するコンテンツを該ネットワーク通信手段に供給する送信コンテンツ生成手段と、

該コンテンツ受信装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該コンテンツ受信装置に対して自身の認証要求を発行する認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、

該コンテンツ受信装置への所定の認証情報を伴うコマンド要求の送信から、該認証情報を伴うコマンド要求の送信に対応して該コンテンツ受信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

該コンテンツ受信装置は

ネットワークを介してデータの送受信を行うネットワーク通信処理手段と、

該コンテンツ送信装置から受信するコンテンツを該ネットワーク通信手段から受け取るコンテンツ受信処理手段と、

該コンテンツ送信装置に認証要求を発行して送るとともに、該コンテンツ送信装置から受信した認証要求に対する認証の判定を行う認証手段と、

該認証手段で認証処理を実行して得られる情報を元に鍵情報を生成し、該鍵情報により該コンテンツ送信装置から受信したコンテンツの暗号復号化処理を行う復号化手段と、

該コンテンツ送信装置への所定の認証情報を伴うコマンド要求の送信から、該認証情報を伴うコマンド要求の送信に対応して該コンテンツ送信装置から送信される応答の到達までの時間を計測するタイマー手段とを有し、

該コンテンツ送信装置の有するタイマー手段での計測結果が所定の値を超えた場合、あるいは該コンテンツ送信装置の有する認証手段が所定の認証情報を伴う応答の認証の判定を行い認証されなかった場合は、該コンテンツ送信装置から該コンテンツ受信装置へのコンテンツ送出手行わないことを特徴とするコンテンツ伝送方法。

(11)

ネットワークを介して接続される他の情報処理装置に情報を出力する際に、該他の情報処理装置からの認証要求を受け取って該認証要求に対する認証の判定を行うとともに、該他の情報処理装置に対して自身の認証要求を発行する認証手段と、

該他の情報処理装置への所定のコマンド要求の出力から、該コマンド要求の出力に対応して該他の情報処理装置から出力される応答の到達までの時間を計測する時間計測手段とを有し、

該時間計測手段での計測結果が所定の値を超えた場合には、該他の情報処理装置への情報出力を行わないことを特徴とする情報処理装置。

【産業上の利用可能性】

【0054】

本発明は著作権保護されたコンテンツを有線または無線のLANを利用して配信、あるいは受信するようなシステムにおいて、配信の範囲が宅内などに制限されるシステムに有効である。

【図面の簡単な説明】

【0055】

【図1】実施例1に係るコンテンツ送信装置およびコンテンツ受信装置の構成を示すブロック図。

【図2】実施例1に係るコンテンツ送信装置およびコンテンツ受信装置により構成されるLANのブロック図。

【図3】実施例1に係るコンテンツ送信装置とコンテンツ受信装置の間でコンテンツを伝

10

20

30

40

50

送する際の手続きのシーケンス図。

【図4】実施例2に係るコンテンツ送信装置とコンテンツ受信装置の間でコンテンツを送る際の手続きのシーケンス図。

【図5】実施例3に係るコンテンツ送信装置およびコンテンツ受信装置により構成されるLANのブロック図。

【図6】実施例3に係るコンテンツ送信装置とコンテンツ受信装置の間でコンテンツを送る際の手続きのシーケンス図。

【図7】実施例4に係るコンテンツ送信装置およびコンテンツ受信装置により構成されるLANのブロック図。

【図8】実施例4に係るコンテンツ送信装置およびコンテンツ受信装置により構成されるLANのブロック図。 10

【図9】実施例3、実施例4に係るコンテンツ送信装置およびコンテンツ受信装置により構成されるLANのブロック図。

【符号の説明】

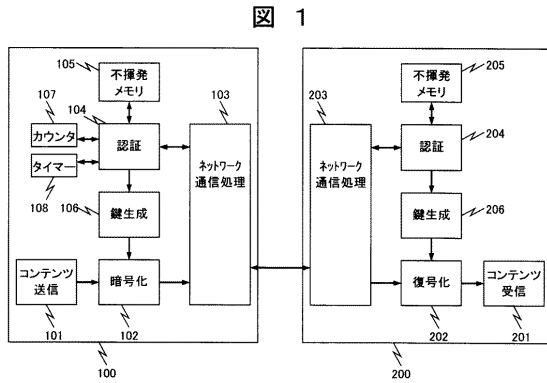
【0056】

- 100、500 …コンテンツ送信装置
- 101、501 …コンテンツ送信回路
- 102、502 …暗号化回路
- 103、503 …ネットワーク通信処理回路
- 104、504 …認証回路
- 105、505 …不揮発メモリ
- 106、506 …鍵生成回路
- 107、507 …カウンタ回路
- 108、508 …タイマー回路
- 200、600 …コンテンツ受信装置
- 201、601 …コンテンツ受信回路
- 202、602 …復号化回路
- 203、603 …ネットワーク通信処理回路
- 204、604 …認証回路
- 205、605 …不揮発メモリ
- 206、606 …鍵生成回路

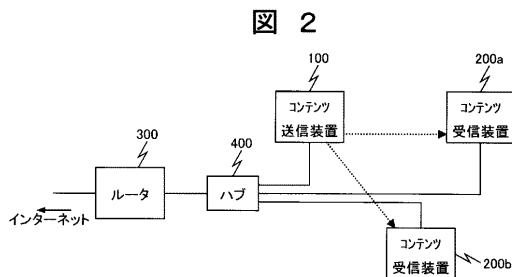
20

30

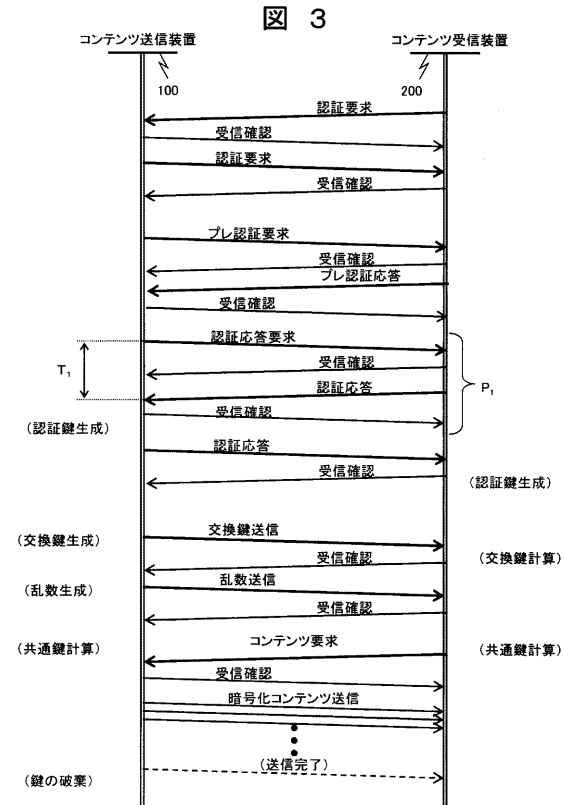
【図 1】



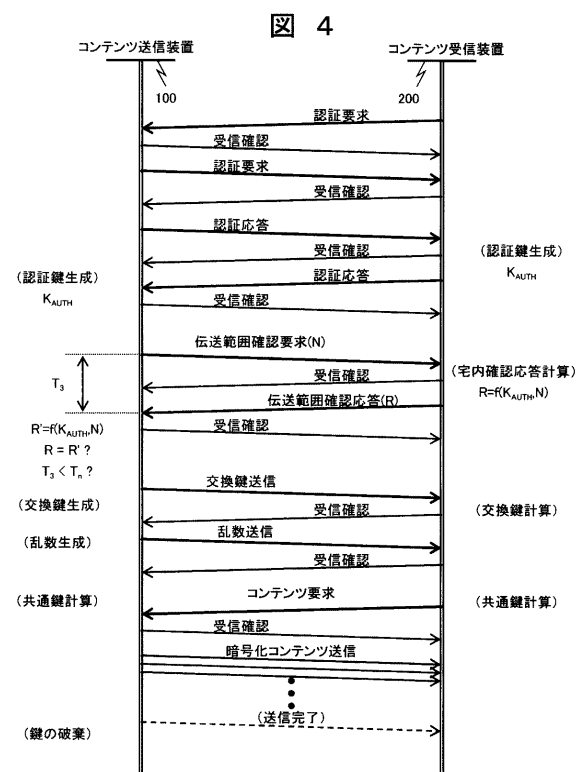
【図 2】



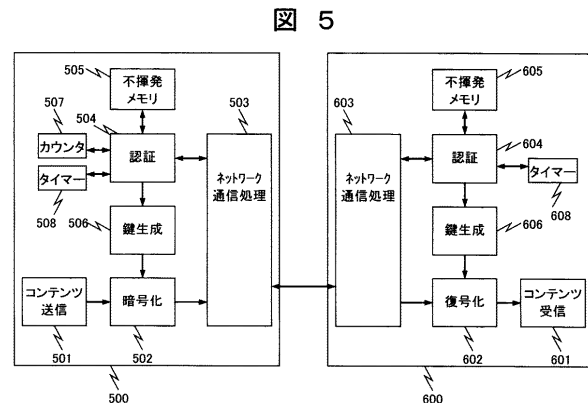
【図 3】



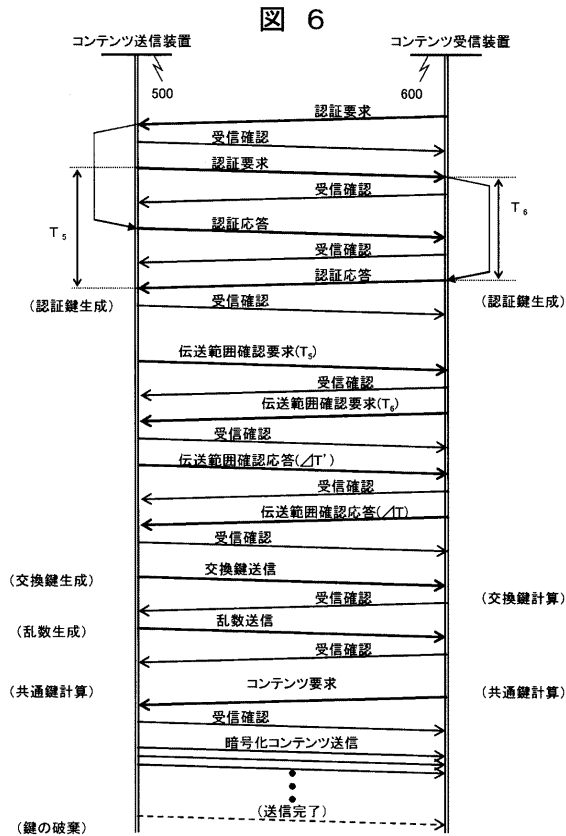
【図 4】



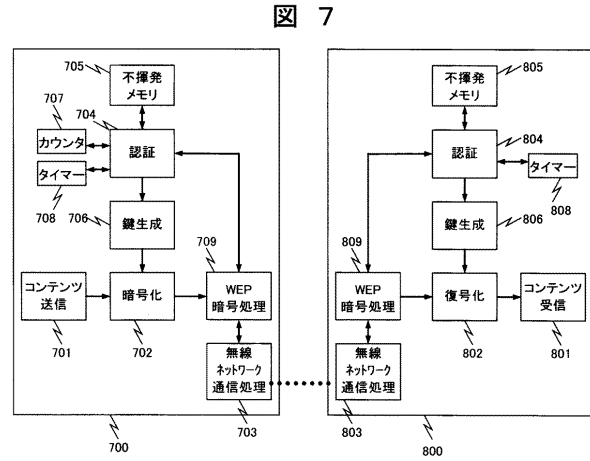
【図 5】



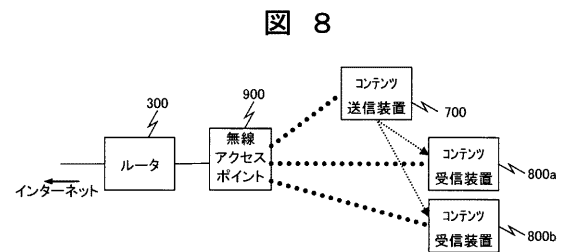
【図 6】



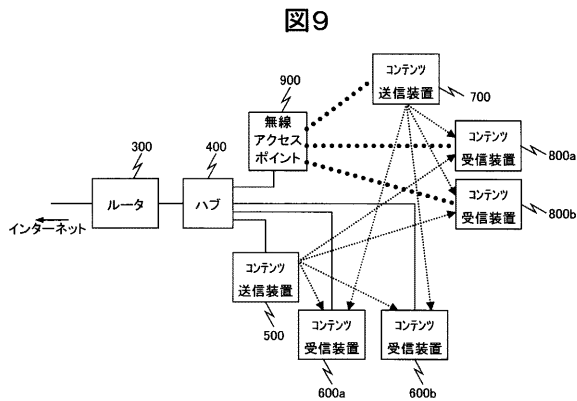
【図 7】



【図 8】



【図 9】



フロントページの続き

(51)Int.Cl. F I
H 0 4 L 9/32 (2006.01) H 0 4 L 9/00 6 7 5 Z

(72)発明者 工藤 善道
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デジタルメディア事業部内

合議体
審判長 酒井 伸芳
審判官 田中 秀人
審判官 殿川 雅也

(56)参考文献 国際公開第01/93434号
国際公開第2005/010770号
特開2004-56776号公報

(58)調査した分野(Int.Cl., DB名)
H04L9/00
G09C1/00