

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5315542号
(P5315542)

(45) 発行日 平成25年10月16日 (2013. 10. 16)

(24) 登録日 平成25年7月19日 (2013. 7. 19)

(51) Int. Cl.

F I

G O 6 F 21/10 (2013. 01)

G O 6 F 21/22 1 1 O K

G O 6 F 21/62 (2013. 01)

G O 6 F 21/24 1 6 6 A

H O 4 N 7/173 (2011. 01)

H O 4 N 7/173 6 3 O

G O 6 F 13/00 (2006. 01)

G O 6 F 13/00 5 4 O S

請求項の数 12 (全 20 頁)

(21) 出願番号 特願2008-257962 (P2008-257962)
 (22) 出願日 平成20年10月3日 (2008. 10. 3)
 (65) 公開番号 特開2010-86489 (P2010-86489A)
 (43) 公開日 平成22年4月15日 (2010. 4. 15)
 審査請求日 平成23年8月19日 (2011. 8. 19)

前置審査

(73) 特許権者 509189444
 日立コンシューマエレクトロニクス株式会
 社
 東京都千代田区大手町二丁目2番1号
 (74) 代理人 100100310
 弁理士 井上 学
 (72) 発明者 寺岡 秀敏
 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

最終頁に続く

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

(57) 【特許請求の範囲】

【請求項 1】

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、コンテンツとコピー制御情報とを送信するコンテンツ送信装置であって、

前記コンテンツの暗号化と、前記コンテンツの1つ以上のコンテンツパケットへのパケット化と、前記コピー制御情報のコピー制御情報パケットへのパケット化とを行うコンテンツ処理部と、

前記コンテンツパケットとコピー制御情報パケットを前記ネットワークを介して前記コンテンツ受信装置に送信する通信処理部と、

前記コンテンツパケットと前記コピー制御情報パケットを送信するために、前記コンテンツ処理部と前記通信処理部とを制御する制御部と、を有し、

前記コンテンツ処理部は、前記コピー制御情報を基に生成した暗号化鍵で前記コンテンツを暗号化し、

前記制御部は、前記コンテンツパケットを送信する前に、前記1つ以上のコンテンツパケットとは別のパケットとして、かつ、複数の異なるフォーマットのコピー制御情報を記述できるパケットとして生成した前記コピー制御情報パケットを送信するように、前記コンテンツ処理部および前記通信処理部を制御する、

ことを特徴とするコンテンツ送信装置。

【請求項 2】

前記コンテンツパケットと、前記コピー制御情報パケットは、識別子を有するヘッダ部

10

20

とペイロード部から構成されており、

前記コピー制御情報パケットは、前記コンテンツパケットとは異なる値の識別子を有するヘッダ部と前記コピー制御情報を格納するペイロード部から構成される、

ことを特徴とする請求項 1 に記載のコンテンツ送信装置。

【請求項 3】

前記制御部は、

前記コンテンツ受信装置との間で交換鍵を交換し、

前記コンテンツ受信装置と前記コンテンツ送信装置との間で交換された前記交換鍵を基に生成された暗号化鍵で前記コンテンツを暗号化し、

前記コンテンツ処理部で暗号化され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ように前記コンテンツ処理部および前記通信処理部を制御する、

ことを特徴とする請求項 1 または 2 に記載のコンテンツ送信装置。

【請求項 4】

前記制御部は、

前記送信するコンテンツの前記コピー制御情報の値が変化したときに、前記コピー制御情報をパケット化して前記コンテンツ受信装置に送信するように前記コンテンツ処理部および前記通信処理部を制御する、

ことを特徴とする請求項 1 ～ 3 のいずれか 1 項に記載のコンテンツ送信装置。

【請求項 5】

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、コンテンツとコピー制御情報と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であって、

前記コンテンツの暗号化と、前記コンテンツの 1 つ以上のコンテンツパケットへのパケット化と、前記コピー制御情報のコピー制御情報パケットへのパケット化と、を行うコンテンツ処理ステップと、

前記コンテンツパケットとコピー制御情報パケットを前記ネットワークを介して前記コンテンツ受信装置に送信する通信処理ステップと、を有し、

前記コンテンツ処理ステップでは、前記コピー制御情報を基に生成した暗号化鍵で前記コンテンツを暗号化し、

前記通信処理ステップでは、前記コンテンツパケットを送信する前に、前記 1 つ以上のコンテンツパケットとは別のパケットとして、かつ、複数の異なるフォーマットのコピー制御情報を記述できるパケットとして生成した前記コピー制御情報パケットを送信する、

ことを特徴とするコンテンツ送信方法。

【請求項 6】

前記コンテンツパケットと、前記コピー制御情報パケットは、識別子を有するヘッダ部とペイロード部から構成されており、

前記コピー制御情報パケットは、前記コンテンツパケットとは異なる値の識別子を有するヘッダ部と前記コピー制御情報を格納するペイロード部から構成される、

ことを特徴とする請求項 5 に記載のコンテンツ送信方法。

【請求項 7】

前記コンテンツ受信装置との間で交換鍵を交換し、

前記コンテンツ受信装置との間で交換された前記交換鍵を基に生成された暗号化鍵で前記コンテンツを暗号化し、

暗号化され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、

ことを特徴とする請求項 5 または 6 に記載のコンテンツ送信方法。

【請求項 8】

前記送信するコンテンツの前記コピー制御情報の値が変化したときに、前記コピー制御情報をパケット化して前記コンテンツ受信装置に送信する、

ことを特徴とする請求項 5 ～ 7 のいずれか 1 項に記載のコンテンツ送信方法。

【請求項 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から送信されたコンテンツパケットとコピー制御情報パケットとを受信するコンテンツ受信装置であって、

前記コンテンツパケットと、前記コピー制御情報パケットと、を前記ネットワークを介して受信する通信処理部と、

受信した前記コンテンツパケットと、前記コピー制御情報パケットと、を識別し、前記コンテンツパケットから暗号化されたコンテンツを抽出、復号する処理と、前記コピー制御情報パケットからコピー制御情報を抽出する処理と、を行うコンテンツ処理部と、

前記コンテンツパケットと前記コピー制御情報パケットとを受信するために、前記コンテンツ処理部と前記通信処理部とを制御する制御部と、
を有し、

10

前記制御部は、前記コンテンツパケットとは別のパケットとして、かつ、複数の異なるフォーマットのコピー制御情報を記述したパケットとして構成された前記コピー制御情報パケットを受信した場合に、前記コピー制御情報パケット以降に受信した前記コンテンツパケットを、前記コピー制御情報に基づき生成した復号化鍵で前記コンテンツを復号するように前記コンテンツ処理部及び前記通信処理部を制御する、

ことを特徴とするコンテンツ受信装置。

【請求項 10】

前記コンテンツ処理部は、

前記コンテンツ送信装置との間で交換鍵を交換し、

前記コンテンツ送信装置との間で交換された前記交換鍵を基に生成された復号化鍵で前記コンテンツを復号化する、

20

ことを特徴とする請求項 9 に記載のコンテンツ受信装置。

【請求項 11】

ネットワークを介して接続されるコンテンツ送信装置から送信されたコンテンツパケットとコピー制御情報パケットとを受信するコンテンツ受信装置におけるコンテンツ受信方法であって、

前記コンテンツパケットと、前記コピー制御情報パケットと、を前記ネットワークを介して受信する通信処理ステップと、

受信した前記コンテンツパケットと、前記コピー制御情報パケットと、を識別し、前記コンテンツパケットから暗号化されたコンテンツを抽出、復号する処理と、前記コピー制御情報パケットからコピー制御情報を抽出する処理と、を行うコンテンツ処理ステップと、
を有し、

30

前記コンテンツ処理ステップにおいて、前記コンテンツパケットとは別のパケットとして、かつ、複数の異なるフォーマットのコピー制御情報を記述したパケットとして構成された前記コピー制御情報パケットを受信した場合に、前記コピー制御情報パケット以降に受信した前記コンテンツパケットを、前記コピー制御情報に基づき生成したコンテンツ鍵でコンテンツを復号する、

ことを特徴とするコンテンツ受信方法。

【請求項 12】

前記コンテンツ送信装置との間で交換鍵を交換し、

40

前記コンテンツ送信装置との間で交換された前記交換鍵を基に生成された復号化鍵で前記コンテンツを復号化する、

ことを特徴とする請求項 11 に記載のコンテンツ受信方法。

【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】

50

【 0 0 0 2 】

デジタル A V 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。

【 0 0 0 3 】

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 A V 機器に取り入れられているものには、例えば特許文献 1 に記載の方式がある。特許文献 1 に記載の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、有線あるいは無線のネットワークによるコンテンツ伝送において、「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。また、本方式では、コピー制御情報をコンテンツ中に挿入する方法と、一部のコピー制御情報を伝送パケットのヘッダ部に記載して伝送する方法が開示されている。

【 0 0 0 4 】

【特許文献 1】特開 2 0 0 7 - 1 0 4 2 3 6 公報

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 5 】

上記従来の技術では、著作権保護対象のコンテンツについてのコピー制御情報は、コンテンツ伝送パケットのヘッダ部あるいはコンテンツ内、またはその両方に埋め込まれて送信される。

【 0 0 0 6 】

しかし、近年、以前は想定されていなかった有限回のコピーが許可されたコンテンツや、コンテンツ視聴期限が決められたコンテンツが流通し始めている。

【 0 0 0 7 】

著作権保護対象のコンテンツにこのように拡張されたコピー制御情報（以下、拡張コピー制御情報）が付属している場合、前記方式で定義されたフォーマットでは、ヘッダサイズの制限などによりすべてのコピー制御情報を伝達できないという課題がある。

【 0 0 0 8 】

本発明では、有線または無線の L A N を利用してコンテンツを送信する際に、コピー回数や視聴期限などを含むコピー制御情報を伝達できるコンテンツ送信装置、コンテンツ受信装置及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】

【 0 0 0 9 】

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】

【 0 0 1 0 】

以上により、有線または無線の L A N を利用してコンテンツを送信する際に、コピー回数や視聴期限などを含む拡張されたコピー制御情報を伝達できる。

【発明を実施するための最良の形態】

【 0 0 1 1 】

以下、本発明の実施の形態について説明する。

【実施例 1】

【 0 0 1 2 】

図 1 は、システム構成例を示したものである。ユーザ宅 1 では、コンテンツ送信装置 2 0 0 とコンテンツ受信装置 1 0 0 が有線 L A N のケーブルによりネットワークハブ装置 1

10

20

30

40

50

１にそれぞれ接続され、ネットワークハブ装置１１はルータ１２に接続される。ルータ１２はモデムや光電変換器などを介してインターネット２へ接続される。

【００１３】

ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）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。

10

【００１４】

コンテンツ送信装置２００、およびコンテンツ受信装置１００、ルータ１２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）アドレスが与えられている。各装置へのＩＰアドレスの設定は、ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）により、例えばルータ１２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。

20

【００１５】

なお、ＩＰｖ６（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ Ｖｅｒｓｉｏｎ ６）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のＩＰアドレスの上位６４ビットと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。

【００１６】

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等を用いても良い。また、ハブ１１とルータ１２が一体型になった形態でも良い。

【００１７】

図２は、コンテンツ受信装置１００の一構成例である。

30

コンテンツ受信装置１００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、記録／再生処理部１１０、ＨＤＤ１１１、暗号／復号処理部１１２、通信処理部１１３、デジタル入出力端子１１４、制御部１１５から構成される。

【００１８】

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。

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。

40

【００１９】

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。

デコーダ１０４は、放送番組やデジタル入出力端子１１４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。

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。内蔵ではなく、外付けでも良い。

【００２０】

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

50

入力処理部 107 は、ユーザによるリモコンやタッチパネルなどの利用によりコンテンツ受信装置 100 を操作する。

【0021】

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。特定の認証プロトコルは、例えば DTCP (Digital Transmission Content Protection) 方式などが挙げられる。

機器情報管理部 109 は、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。

10

【0022】

記録 / 再生処理部 110 は、コンテンツを HDD 111 に記録するための記録制御と、HDD 111 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。

HDD 111 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でもよい。

【0023】

暗号 / 復号処理部 112 は、放送番組や LAN 経由でデジタル入出力端子 114 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とともに、ネットワークに送信するパケットを生成あるいは解析する。

20

【0024】

通信処理部 113 は、デジタル入出力端子 114 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。受信す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」などの識別コードに加え、コピー回数や視聴期限などのコピー制御情報を付加されている。

【0025】

デジタル入出力端子 114 は、LAN 経由でコンテンツや制御コマンドを入出力する。

制御部 115 は、コンテンツ受信装置 100 における各部の動作を統括的に制御する。

【0026】

図 3 は、コンテンツ送信装置 200 の一構成例である。

30

コンテンツ送信装置 200 は、チューナ 201、デスクランブラ 202、デマルチプレクサ 203、デコーダ 204、表示部 / スピーカ 205、デジタル端子 206、入力処理部 207、機器認証処理部 208、機器情報管理部 209、記録 / 再生処理部 210、HDD 211、暗号 / 復号処理部 212、通信処理部 213、デジタル入出力端子 214、制御部 215 から構成される。

【0027】

チューナ 201 は、放送局からアンテナ 20 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。

デスクランブラ 202 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。

40

【0028】

デマルチプレクサ 203 は、放送番組から音声データ、映像データを抽出する。

デコーダ 204 は、放送番組やデジタル入出力端子 214 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。

表示部 / スピーカ 205 は、該デコーダ 204 からの出力信号や、デジタル端子 206 から入力された信号を再生する。内蔵ではなく、外付けでも良い。

【0029】

デジタル端子 206 は、非圧縮のデジタルデータを入力する、例えば HDMI などがある。

入力処理部 207 は、ユーザによるリモコンやタッチパネルなどの利用によりコンテン

50

ツ送信装置 200 を操作する。

【0030】

機器認証処理部 208 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ことを認証し、コンテンツの暗号 / 復号に使用する鍵を共有する。特定の認証プロトコルは、例えば D T C P 方式などが挙げられる。

機器情報管理部 209 は、機器認証処理部 208 で認証が成功した AV 機器に関する情報を管理する。

【0031】

記録 / 再生処理部 120 は、コンテンツを HDD 211 に記録するための記録制御と、HDD 211 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。

HDD 211 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でもよい。

【0032】

暗号 / 復号処理部 212 は、放送番組や LAN 経由でデジタル入出力端子 214 を介して受信したコンテンツを、機器認証処理部 208 で共有した鍵を使用して暗号化あるいは復号化するとともに、ネットワークに送信するパケットを生成あるいは解析する。

【0033】

通信処理部 213 は、デジタル入出力端子 214 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。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」などの識別コードに加え、コピー回数や視聴期限などのコピー制御情報を付して送信される。

【0034】

デジタル入出力端子 214 は、LAN 経由でコンテンツや制御コマンドを入出力する。

制御部 215 は、コンテンツ送信装置 200 における各部の動作を統括的に制御する。

【0035】

図 4 は、各機器内の機器情報管理部 109 (209 も同様) の一構成例である。

機器情報管理部 109 は、タイマー 1091、機器情報更新部 1092、機器情報格納部 1093 から構成される。

【0036】

タイマー 1091 は、機器認証処理部 108 (208 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 1093 に格納された登録情報の有効期限を管理する場合に時間計測を行う。

機器情報更新部 1092 は、後述の機器情報格納部 1093 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。

機器情報格納部 1093 は、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。

【0037】

図 5 は、機器情報格納部 1093 で格納する機器情報テーブル 50 の一構成例である。

機器情報テーブル 50 は、ID 501、機器情報 502 としてデバイス ID 5021 及びアドレス情報 5022、拡張コピー制御情報受信可否 503 で構成される。

【0038】

ID 501 は、テーブル 50 の登録番号を示す。

デバイス ID 5021 は、各機器を一意に識別するための識別子を示す。例えば、IEEE 1394 で使用するユニーク ID や D T C P 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も良い。

【0039】

10

20

30

40

50

アドレス情報 5 0 2 2 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。

拡張コピー制御情報受信可否は、対象デバイスの拡張コピー制御情報受信能力有無を示す。

【 0 0 4 0 】

図 6 は図 1 に示したシステム構成において、コンテンツ送信装置 2 0 0 とコンテンツ受信装置 1 0 0 との間で実行する機器認証処理手順 6 0 0 の例である。

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。

10

なお、図 6 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。

【 0 0 4 1 】

最初に、コンテンツ受信装置 1 0 0 側から認証要求を作成する。コンテンツ受信装置 1 0 0 の機器認証処理部 1 0 8 は、認証要求にデバイス 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 1 1 1 を介してコンテンツ送信装置 2 0 0 に送る (S 6 0 1) 。

【 0 0 4 2 】

コンテンツ送信装置 2 0 0 の機器認証処理部 2 0 8 は、通信処理部 2 0 7 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 1 0 0 に送ると (S 6 0 2)、コンテンツ送信装置 2 0 0 の機器認証処理部 2 0 8 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 2 0 0 の固有情報とその証書を付して認証要求をコンテンツ受信装置 1 0 0 に送る (S 6 0 3) 。

20

【 0 0 4 3 】

コンテンツ受信装置 1 0 0 の機器認証処理部 1 0 8 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 2 0 0 へ送る (S 6 0 4) 。

次に、コンテンツ送信装置 2 0 0 の機器認証処理部 2 0 8 は、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 1 0 0 に送る (S 6 0 5) 。

30

【 0 0 4 4 】

コンテンツ受信装置 1 0 0 の機器認証処理部 1 0 8 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 2 0 0 に送った (S 6 0 6) 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 2 0 0 に送り (S 6 0 7)、必要なパラメータを用いてコンテンツ送信装置 2 0 0 と共通の認証鍵を生成する。

【 0 0 4 5 】

コンテンツ送信装置 2 0 0 の機器認証処理部 2 0 8 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 1 0 0 に送り (S 6 0 8)、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 1 0 0 と共通の認証鍵を生成する。

40

ここまでの手順で、コンテンツ送信装置 2 0 0 の機器認証処理部 1 0 8 とコンテンツ受信装置の機器認証処理部 2 0 8 は、互いに共通の認証鍵が生成されて共有される。

【 0 0 4 6 】

次に、コンテンツ送信装置 2 0 0 は、コンテンツ受信装置 1 0 0 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 1 0 0 に送る (S 6 0 9) 。

コンテンツ受信装置 1 0 0 の機器認証処理部 1 0 8 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 2 0 0 に送ると (S 6 1 0)、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 2 0 0 へ送る (S 6 1 1) 。

【 0 0 4 7 】

50

コンテンツ送信装置 200 の機器認証処理部 208 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 (S612)、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 (S613)。

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 (S614)。

【0048】

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 208 は、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 (S615)

10

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 (S616)。

【0049】

コンテンツ送信装置 200 の機器認証処理部 208 は、受信確認を受け取ると、タイマー 1081 を停止し、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) が所定の値 (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 (S617)。

20

【0050】

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して判断し、以降の処理を中断して機器認証処理を終了する。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 (S618)、コンテンツ送信装置 200 の機器認証処理部 208 はコンテンツを暗号する際に使用する交換鍵を生成し、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 (S619)。

【0051】

コンテンツ受信装置 100 の機器認証処理部 108 は、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 (S620)。

30

コンテンツ送信装置 200 の機器認証処理部 208 は、受信確認を受け取ると、機器情報管理部 203 内の機器情報テーブル 510 にコンテンツ受信装置 100 に関する情報を登録する (S621)。

例えば、機器情報テーブル 510 内の ID 501 のレコード 512 に示すように、S601 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 ID 5021 に設定し、ネットワーク上でのコンテンツ受信装置 100 の IP アドレスをアドレス情報 5022 に設定し、拡張コピー制御情報受信可否 503 に『否』を設定する。

【0052】

以上から、コンテンツ送信装置 200 の機器認証処理部 208 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。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、S609 と S613 の処理、S617 と S619 の処理をそれぞれ纏めても良い。

40

【0053】

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 200 とコンテンツ受信装置 100 の間で実行する機器認証処理について説明した。

上記手順を実施することにより、装置間で互いを正規に認定された機器であることを確認し、コンテンツの暗号化 / 復号に使用する鍵を共有することができる。

【0054】

50

図7は、図1に示したシステム構成において、コンテンツ送信装置200とコンテンツ受信装置100との間で実行する拡張コピー制御情報対応用の機器認証処理手順の例である。

最初に、コンテンツ受信装置100の機器認証処理部108は通信処理部111を介して自機器が拡張コピー制御情報受信可能であることを示す能力通知をコンテンツ送信装置200に送る(S701)。

【0055】

コンテンツ送信装置200の機器認証処理部208は、通信処理部207を介して能力通知を受け取り、自機器が拡張コピー制御情報送信可能であることを示す受信確認をコンテンツ受信装置100に送る(S702)。

10

次に、コンテンツ送信装置200とコンテンツ受信装置100は、図6で説明した機器認証処理600を実施する。

【0056】

コンテンツ送信装置200の機器認証処理部208は、機器認証処理600が完了すると、機器情報管理部203内の機器情報テーブル510にコンテンツ受信装置100に関する情報を登録する(S703)。例えば、機器情報テーブル510内のID501のレコード511に示すように、S601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ID5021に設定し、ネットワーク上でのコンテンツ受信装置100のIPアドレスをアドレス情報5022に設定し、拡張コピー制御情報受信可否503に『可』を設定する。

20

【0057】

上記手順を実施することにより、装置間で互いを正規に認定された機器であることとともに拡張コピー制御情報の伝送に対応しているかどうかを確認しつつ、コンテンツの暗号化/復号に使用する鍵を共有することができる。

【0058】

図8は、コンテンツ伝送パケットフォーマット800の例である。

コンテンツ伝送パケットはヘッダ部801とペイロード部802から構成される。

【0059】

ヘッダ部801は、予約領域(Reserved)8011、暗号方式(C__A)8012、暗号モード(E-EMI)8013、交換鍵ラベル(Exchange__Key__Label)8014、乱数値(Nc)8015、ペイロードサイズ(Byte Length of Payload)8016から構成される。

30

【0060】

予約領域(Reserved)8011は予約領域であり、000を設定する。暗号方式(C__A)8012は、ペイロード部の暗号方式を示す。例えば、128ビットの鍵長のAESで暗号化されていることなどを明示する。

暗号モード(E-EMI)8013は、ペイロード部の暗号モードを示し、乱数値(Nc)8015と合わせてコンテンツ鍵の算出に利用する。

【0061】

交換鍵ラベル(Exchange__Key__Label)8014は、前記600の認証手順で交換した鍵を特定するラベルを設定する。

40

ペイロードサイズ(Byte Length of Content)8016は、当該パケットのペイロードサイズを設定する。

ペイロード部802は、暗号化コンテンツから構成される。

【0062】

図9は、拡張コピー制御情報対応に拡張したコンテンツ伝送パケット900のヘッダ部の例である。

拡張コピー制御情報対応に拡張したコンテンツ伝送パケット900はヘッダ部901とペイロード部902から構成される。

【0063】

50

ペイロードタイプ (P _ T) 9 0 1 7 は、ペイロードがコンテンツであるか拡張コピー制御情報であることを示す識別子であり、例えばコンテンツの場合は 0 を、拡張コピー制御情報の場合は 1 を設定する。

予約領域 (R e s e r v e d) 9 0 1 2 は予約領域であり、0 0 を設定する。
それ以外の部分については、従来のコンテンツ伝送パケットのヘッダ部と同様である。

【 0 0 6 4 】

ペイロード部 9 0 2 は、暗号化コンテンツあるいは暗号化された拡張コピー制御情報から構成される。

ペイロード部 9 0 2 が拡張コピー制御情報である場合の暗号モード (E - E M I) 8 0 1 3 は、コンテンツに設定されるものと同じでも良いし、異なる値でもよい。

10

【 0 0 6 5 】

本フォーマットを用いた場合、ペイロード部 9 0 2 の暗号化方法については、交換鍵と暗号モード (E - E M I) 8 0 1 3、乱数値 (N c) 8 0 1 5 を元に生成したコンテンツ鍵を用いて暗号化すればよい。

また、例えば拡張コピー制御情報をハッシュ化し、コンテンツパケットのヘッダ部に含まれる乱数値 (N c) 8 0 1 5 との排他的論理和をコンテンツの暗号鍵とすることなどにより、拡張コピー制御情報の値とコンテンツを暗号化するコンテンツ鍵を相関させることで、拡張コピー制御情報を暗号化せずに送信しても拡張コピー制御情報の改ざんを防止することもできる。

【 0 0 6 6 】

20

図 1 0 は、拡張コピー制御情報の一構成例である。

拡張コピー制御情報は、T y p e 1 0 0 1、L e n g t h 1 0 0 2、拡張コピー制御情報 1 0 0 3 で構成される。

T y p e 1 0 0 1 は拡張コピー制御情報の型を表す ID であり、当該パケットの拡張コピー制御情報のフォーマットを識別するために利用される。

L e n g t h 1 0 0 2 は当該パケットに含まれる拡張コピー制御情報のサイズを示す。

【 0 0 6 7 】

拡張コピー制御情報 1 0 0 3 は当該コンテンツのコピー制御情報を示し、例えば、R e t e n t i o n _ M o v e _ M o d e 1 0 0 3 1、R e t e n t i o n _ S t a t e 1 0 0 3 2、E P N 1 0 0 3 3、D T C P _ C C I 1 0 0 3 4、I m a g e _ C o n s t r a i n t _ T o k e n 1 0 0 3 5、A P S 1 0 0 3 6、C o p y _ C o u n t 1 0 0 3 7、T i m e _ S p a n 1 0 0 3 8 から構成される。

30

R e t e n t i o n _ M o v e _ M o d e 1 0 0 3 1 は一時蓄積可否を示す。

R e t e n t i o n _ S t a t e 1 0 0 3 2 は一時蓄積時間を示す。

【 0 0 6 8 】

E P N 1 0 0 3 3 は出力保護つきコピー無制限運用可否を示す。

D T C P _ C C I 1 0 0 3 4 は D T C P 方式で規定されるコピー制御情報を示す。

I m a g e _ C o n s t r a i n t _ T o k e n 1 0 0 3 5 は映像出力信号の制限有無を示す。

A P S 1 0 0 3 6 はアナログ出力コピー制御情報

40

C o p y _ C o u n t 1 0 0 3 7 はコピー回数を示す。

T i m e _ S p a n 1 0 0 3 8 は視聴期限を示す。

【 0 0 6 9 】

拡張コピー制御情報を伝送するパケットは、データの 1 ビット目を拡張コピー制御情報伝送用パケットとコンテンツ伝送用パケットを識別するための識別子として取り扱い、拡張コピー制御情報の場合は該識別子を 1 にするなどして図 8 におけるコンテンツ伝送パケットフォーマットと区別できる形であれば、コンテンツ伝送パケットフォーマットと類似の図 9 に示す形ではなく、例えばヘッダが図 1 0 の構成例における T y p e 1 0 0 1、L e n g t h 1 0 0 2 から構成され、ペイロード部が拡張コピー制御情報 1 0 0 3 のみから構成される形式でもよい。

50

【 0 0 7 0 】

以上のようなフォーマットで拡張コピー制御情報を伝送することにより、例えば現在 D T C P - I P 方式で規定されていないコピー制御情報を、コンテンツのフォーマットに依存しない形で容易に伝送することができる。また、本フォーマットによれば、パケットがコンテンツか拡張コピー制御情報かを簡単に区別できるとともに、コピー制御情報の追加、変更などが容易に行える。

【 0 0 7 1 】

図 1 1 は、図 9 に示したフォーマットを用い、H T T P プロトコルを利用してコンテンツを伝送する場合のデータ例である。ここで、トランスポート層プロトコルとして T C P を用いるが、T C P ヘッダは省略する。

10

図 9、図 1 0 で示したフォーマットを用いてコンテンツを伝送する場合の伝送データ 1 1 0 0 は、H T T P ヘッダ 1 1 0 1、拡張コピー制御情報伝送用パケット 1 1 1 0、コンテンツ伝送用パケット 1 1 2 0 から構成される。

【 0 0 7 2 】

拡張コピー制御情報伝送用パケット 1 1 1 0 は拡張コピー制御情報用ヘッダ部 1 1 1 1 とペイロード部（拡張コピー制御情報）1 1 1 2 から構成される。

コンテンツ伝送用パケット 1 1 2 0 はコンテンツ用ヘッダ部 1 1 2 1 とペイロード部（コンテンツ）1 1 2 2 から構成される。

【 0 0 7 3 】

拡張コピー制御情報用ヘッダ部 1 1 1 1 は図 9 で示したコンテンツ伝送パケットのヘッダ部においてペイロードタイプ（P _ T）9 0 1 7 を 1 に設定したヘッダ部である。

20

ペイロード部（拡張コピー制御情報）1 1 1 2 には、図 7 の拡張コピー制御情報転送用の機器認証処理 7 0 0 において交換された交換鍵と、拡張コピー制御情報用ヘッダ部 1 1 1 1 に設定された暗号モード（E - E M I）8 0 1 3 や乱数値（N c）8 0 1 5 などの情報を元に暗号化された拡張コピー制御情報を格納する。

【 0 0 7 4 】

拡張コピー制御情報には、図 1 0 に示した構成例のみでなく、複数のフォーマットの情報が同時に含まれていてもよい。

拡張コピー制御情報伝送用パケット 1 1 1 0 は、以降のコンテンツのコピー制御情報を示すものであり、少なくともコンテンツのコピー制御情報が変化する毎に、送信データに挿入する。

30

【 0 0 7 5 】

コンテンツ用ヘッダ部 1 1 2 1 は図 9 で示したコンテンツ伝送パケットのヘッダ部においてペイロードタイプ（P _ T）を 0 に設定したヘッダ部である。

ペイロード部（コンテンツ）1 1 2 2 には、図 7 の拡張コピー制御情報転送用の機器認証処理 7 0 0 において交換された交換鍵と、コンテンツ用ヘッダ部 1 1 2 1 に設定された暗号モード（E - E M I）8 0 1 3 や乱数値（N c）8 0 1 5 などの情報を元に暗号化されたコンテンツを設定する。

【 0 0 7 6 】

図 1 1 に示す形式で、同一の T C P 及び H T T P セッション上で、かつ、共通の交換鍵を元に生成した鍵で暗号化して拡張コピー制御情報とコンテンツを伝送することにより、拡張コピー制御情報の改ざんを防止するとともに、拡張コピー制御情報とコンテンツを一意に結びつけることが可能となる。

40

【 0 0 7 7 】

また、例えば R T P プロトコルを利用してコンテンツを伝送する場合も、H T T P ヘッダ 1 1 0 1 を R T P ヘッダに置き換えることで、図 1 1 と同様の構成でコンテンツの伝送が可能である。あるいは、R T P パケット毎に拡張コピー制御情報伝送用パケット 1 1 1 0 とコンテンツ伝送用パケット 1 1 2 0 の両方を格納すれば、拡張コピー制御情報を確実に伝送することができる。

【 0 0 7 8 】

50

図 1 2 は拡張コピー制御情報を利用して、コピー制御情報にコピー回数や視聴期限を含むコンテンツを転送する場合の手順の例である。

最初に、コンテンツ送信装置 2 0 0 とコンテンツ受信装置 1 0 0 の間で転送するコンテンツを決定する (S 1 2 0 1)。ここで、コンテンツ選択までの手順には、コンテンツ受信装置 1 0 0 におけるコンテンツ送信装置 2 0 0 の発見、コンテンツ送信装置 2 0 0 によるコンテンツの提示、コンテンツ受信装置 1 0 0 におけるコンテンツの選択などの手順があるが、これには、D L N A (D i g i t a l L i v i n g N e t w o r k A l l i a n c e) などの技術を使用すればよい。

【 0 0 7 9 】

次に、コンテンツ送信装置 2 0 0 とコンテンツ受信装置 1 0 0 の間で、図 7 で説明した拡張コピー制御情報転送用の機器認証処理 7 0 0 を実施する。拡張コピー制御情報転送用の機器認証処理 7 0 0 が完了すると、コンテンツ受信装置 1 0 0 の制御部 1 1 5 は、通信処理部 1 1 3 を介して、H T T P の G E T リクエスト等を用いてコンテンツ送信装置 2 0 0 にコンテンツ転送要求を発行する (S 1 2 0 2)。

【 0 0 8 0 】

コンテンツ送信装置 2 0 0 の制御部 2 1 5 は、要求されたコンテンツが転送可能な場合、コンテンツ受信装置に H T T P のレスポンスヘッダなどを用いて転送が可能であることを示す受信確認を送信する (S 1 2 0 3)。

【 0 0 8 1 】

次に、コンテンツ送信装置 2 0 0 の機器情報管理部 2 0 9 が、機器情報テーブル 5 0 内の対象となるコンテンツ受信装置 1 0 0 の拡張コピー制御情報受信可否が『可』になっていることを確認した後 (S 1 2 0 4)、暗号/復号処理部 2 1 2 が、図 9、図 1 0、図 1 1 に示すフォーマットで図 9 のペイロードタイプ 9 0 1 7 を 1 にしてパケットが拡張コピー制御情報伝送用パケットであることを示したヘッダ部と暗号化した拡張コピー制御情報を含むペイロードから構成される拡張コピー制御情報伝送用パケットを送信し (S 1 2 0 5) する。

【 0 0 8 2 】

続いて図 9、図 1 1 に示すフォーマットで図 9 のペイロードタイプ 9 0 1 7 を 0 にして該パケットがコンテンツ伝送用パケットであることを示したヘッダ部と暗号化コンテンツを含むペイロードから構成されるコンテンツ伝送用パケットを送信する (S 1 2 0 6)。

【 0 0 8 3 】

コンテンツ受信装置 1 0 0 の拡張コピー制御情報受信可否が『否』になっている場合は、コンテンツを送信しないか、あるいは従来のフォーマットでコンテンツを送信すればよい。

以上の手順でコンテンツを伝送することにより、正規に拡張コピー制御情報に対応した機器にのみ、拡張されたコピー制御情報を含むコンテンツを伝送することができる。

【 0 0 8 4 】

以上により、有線または無線の L A N を利用してコンテンツを伝送する際に、コピー回数や視聴期限などを含むコピー制御情報を伝達できる。

【 実施例 2 】

【 0 0 8 5 】

前述した本実施 1 ではコンテンツの開始直前のみコピー制御情報を送信していた。本実施例 2 は、コピー制御情報がコンテンツの途中で変化する場合にこれに追従して確実にコピー制御情報を伝達する。

【 0 0 8 6 】

図 1 3 は、コンテンツの途中でコピー制御情報が変化する場合の伝送データ例である。ここでは、アプリケーション層プロトコルとして H T T P プロトコルを、トランスポート層プロトコルとして T C P を用いるが、T C P ヘッダは省略する。

【 0 0 8 7 】

伝送データ 1 3 0 0 は、H T T P ヘッダ 1 3 0 1 と、拡張コピー制御情報 1 のコンテン

10

20

30

40

50

ツ伝送ブロック 1 3 1 0 と、拡張コピー制御情報 2 のコンテンツ伝送ブロック 1 3 2 0 から構成される。

拡張コピー制御情報のコンテンツ伝送ブロック 1 3 1 0 は、拡張コピー制御情報伝送用パケット 1 3 1 1 と、コンテンツ伝送用パケット 1 3 1 2 ~ 1 3 1 5 から構成される。ここで、コンテンツ伝送用パケット 1 3 1 2 ~ 1 3 1 5 に含まれるコンテンツのコピー制御は、拡張コピー制御情報伝送用パケット 1 3 1 1 で伝送されたコピー制御情報に従う。

【 0 0 8 8 】

拡張コピー制御情報 2 のコンテンツ伝送ブロック 1 3 2 0 は、拡張コピー制御情報伝送用パケット 1 3 2 1 と、コンテンツ伝送用パケット 1 3 2 2 ~ 1 3 2 3 から構成される。

ここで、コンテンツ伝送用パケット 1 3 2 2 ~ 1 3 2 3 に含まれるコンテンツのコピー制御は、拡張コピー制御情報伝送用パケット 1 3 2 1 で伝送されたコピー制御情報に従う。

【 0 0 8 9 】

コンテンツ内で複数回コピー制御情報が変化する場合には、以下、コピー制御情報が変化する毎に該コピー制御情報を伝送する拡張コピー制御情報伝送パケットと該コピー制御情報に従うコンテンツの部分を伝送するコンテンツ伝送用パケットから構成されるブロックを追加すればよい。

【 0 0 9 0 】

図 1 4 は、拡張コピー制御情報を利用して、コピー制御情報にコピー回数や視聴期限を含むコンテンツを転送する場合において、コンテンツの途中でコピー制御情報が変化する場合の転送手順の例である。

【 0 0 9 1 】

転送するコンテンツの選択からコンテンツの最初のコピー制御情報ブロックの転送開始までは図 1 2 の通常のコンテンツ転送処理 1 2 0 0 と同様である。コンテンツ送信装置 2 0 0 は、制御部 2 1 5 が送信するコンテンツのコピー制御情報の変化を検出すると (S 1 4 0 1)、暗号/復号処理部 2 1 2 が図 9、図 1 0、図 1 1 に示すフォーマットで図 9 のペイロードタイプ 9 0 1 7 を 1 にして該パケットが拡張コピー制御情報伝送用パケットであることを示したヘッダ部と暗号化した変化後のコピー制御情報を含むペイロードから構成される拡張コピー制御情報伝送用パケットを送信する (S 1 4 0 2)

続いて図 9、図 1 1 に示すフォーマットで図 9 のペイロードタイプ 9 0 1 7 を 0 にして該パケットがコンテンツ伝送用パケットであることを示したヘッダ部と変化後のコピー制御情報に従う暗号化コンテンツを含むペイロードから構成されるコンテンツ伝送用パケットを送信する (S 1 4 0 3)。コンテンツ内で複数回コピー制御情報が変化する場合には、以下、コピー制御情報が変化する度に前述の手順 S 1 4 0 1 から S 1 4 0 3 を繰り返す。

【 0 0 9 2 】

図 1 3 のような伝送データ形式を用いて、図 1 4 の手順でコンテンツを送信することによって、コンテンツの途中でコピー制御情報が変化する場合でも、そのコピー制御情報を確実に伝送することができ、コピー制御情報の変化に合わせたコピー制御を行うことが可能となる。

【 0 0 9 3 】

以上により、有線または無線の L A N を利用してコンテンツを伝送する際に、コンテンツの途中でコピー制御情報が変化する場合においても、コピー回数や視聴期限などを含むコピー制御情報を伝達できる。

なお、上述の実施例は少なくとも下記を開示している。

上記の課題を解決するために、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コンテンツ送信方法であって、

コピー制御情報の対象となるコンテンツを送信する前に、前記コンテンツとは別のパケットとして、同一のアプリケーション層セッション上で、前記コピー制御情報を含むパケットを送信することを特徴とするコンテンツ送信方法を提供する。

(1)

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コンテンツ送信方法であって、

コピー制御情報の対象となるコンテンツを送信する前に、前記コンテンツとは別のパケットとして、同一のアプリケーション層セッション上で、前記コピー制御情報を含むパケットを送信することを特徴とするコンテンツ送信方法。

(2)

前記コピー制御情報を含むパケットは、前記コンテンツを含むパケットと異なることを示す識別子を有するヘッダ部と前記コピー制御情報を格納するペイロード部から構成されることを特徴とする (1) に記載のコンテンツ送信方法。

10

(3)

前記コピー制御情報と前記コンテンツとは、前記コンテンツ受信装置と前記コンテンツ送信装置との間で交換された交換鍵を元に生成された鍵で暗号化されることを特徴とする (1) または (2) に記載のコンテンツ送信方法。

(4)

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コンテンツ送信装置であって、

コピー制御情報の対象となるコンテンツを送信する前に、前記コンテンツとは別のパケットとして、同一のアプリケーション層セッション上で、前記コピー制御情報を含むパケットを送信する機器認証処理部
を有することを特徴とするコンテンツ送信装置。

20

(5)

前記コピー制御情報を含むパケットは、前記コンテンツを含むパケットと異なることを示す識別子を有するヘッダ部と前記コピー制御情報を格納するペイロード部から構成されることを特徴とする (4) に記載のコンテンツ送信装置。

(6)

前記コピー制御情報と前記コンテンツとは、前記コンテンツ受信装置と前記コンテンツ送信装置との間で交換された交換鍵を元に生成された鍵で暗号化されることを特徴とする (4) または (5) に記載のコンテンツ送信装置。

【図面の簡単な説明】

30

【 0 0 9 4 】

【図 1】システムの一構成例を示した説明図である。

【図 2】コンテンツ受信装置の一構成例を示した説明図である。

【図 3】コンテンツ送信装置の一構成例を示した説明図である。

【図 4】機器情報管理部の一構成例を示した説明図である。

【図 5】機器情報テーブルの一構成例を示した説明図である。

【図 6】コンテンツ受信装置とコンテンツ送信装置の間で実施される機器認証処理シーケンスの一例を示した説明図である。

【図 7】コンテンツ受信装置とコンテンツ送信装置の間で実施される拡張コピー制御情報用の機器認証処理シーケンスの一例を示した説明図である。

40

【図 8】コンテンツ伝送時のパケットフォーマットを示した説明図である。

【図 9】拡張コピー制御情報用コンテンツ伝送時のパケットフォーマットの一例を示した説明図である。

【図 10】拡張コピー制御情報の一構成例を示した説明図である。

【図 11】拡張コピー制御情報用コンテンツ伝送時の伝送データ構成の一例を示した説明図である。

【図 12】拡張コピー制御情報用コンテンツ転送処理シーケンスの一例を示した説明図である。

【図 13】コンテンツの途中でコピー制御情報が変わる場合の拡張コピー制御情報用コンテンツ伝送時の伝送データ構成の一例を示した説明図である。

50

【図 1 4】コンテンツの途中でコピー制御情報が変わる場合の拡張コピー制御情報用コンテンツ転送処理シーケンスの一例を示した説明図である。

【符号の説明】

【 0 0 9 5 】

2 0 0 . . . コンテンツ送信装置

1 0 0 . . . コンテンツ受信装置

1 0 8、2 0 8 . . . 機器認証処理部

1 0 9、2 0 9 . . . 機器情報管理部

1 1 2、2 1 2 . . . 暗号 / 復号処理部

1 1 1、2 1 1 . . . H D D

1 0 9 1 . . . タイマー

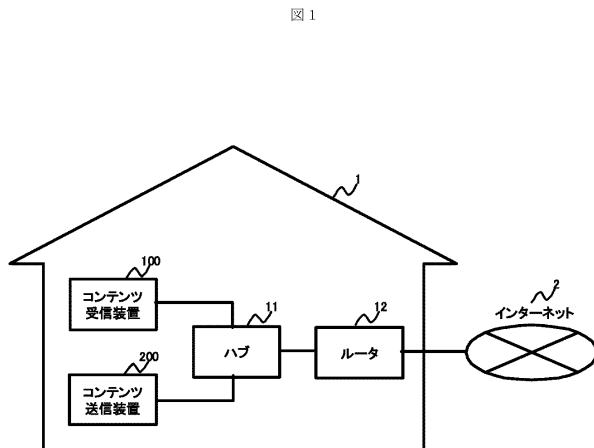
1 0 9 2 . . . 機器情報更新部

1 0 9 3 . . . 機器情報格納部

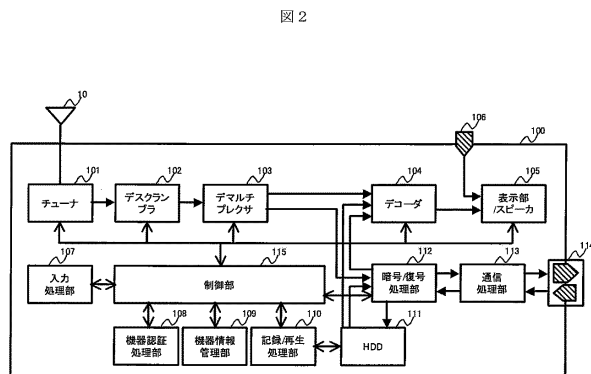
5 0 . . . 機器情報管理テーブル

10

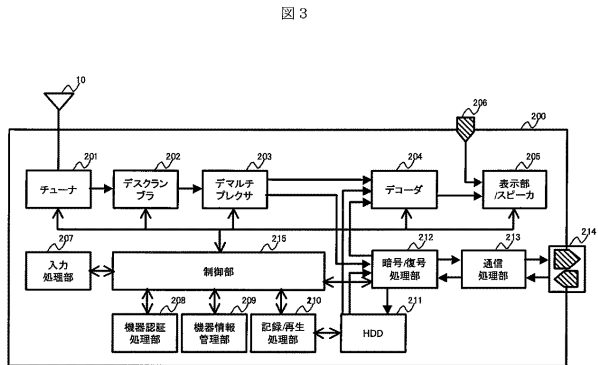
【図 1】



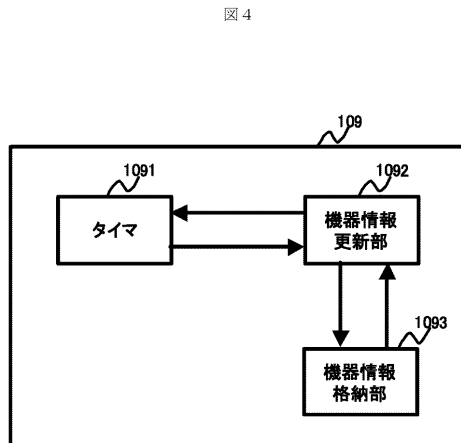
【図 2】



【図 3】



【図 4】



【図 5】

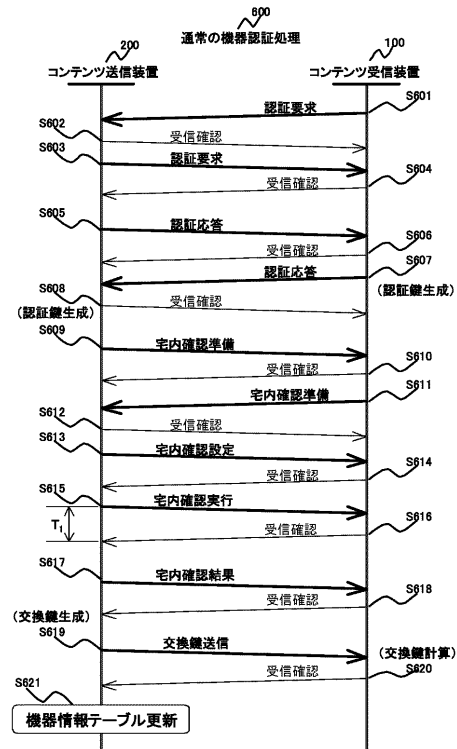
図 5

機器情報テーブル 50

ID 501	機器情報 502		拡張コピー 制御情報 受信可否 503
	デバイスID 5021	アドレス情報 (例: IPアドレス) 5022	
0	aabbccdde	192.168.23.111	可 511
1	ffgghhiij	192.168.23.232	否 512
...

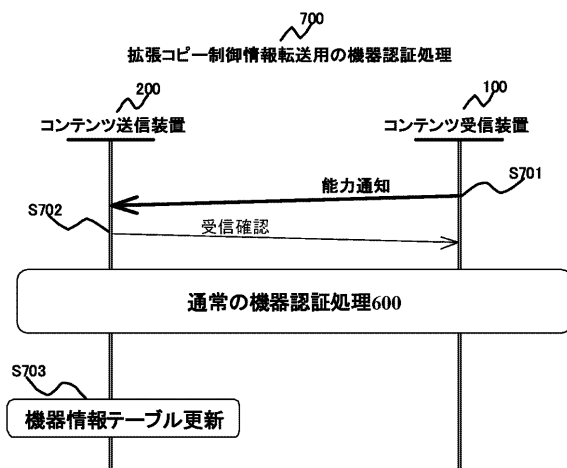
【図 6】

図 6



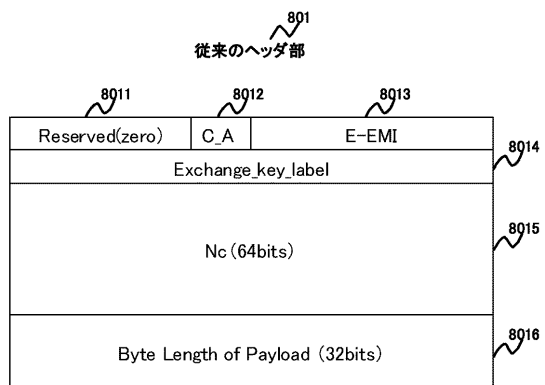
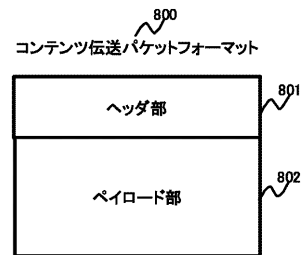
【図 7】

図 7

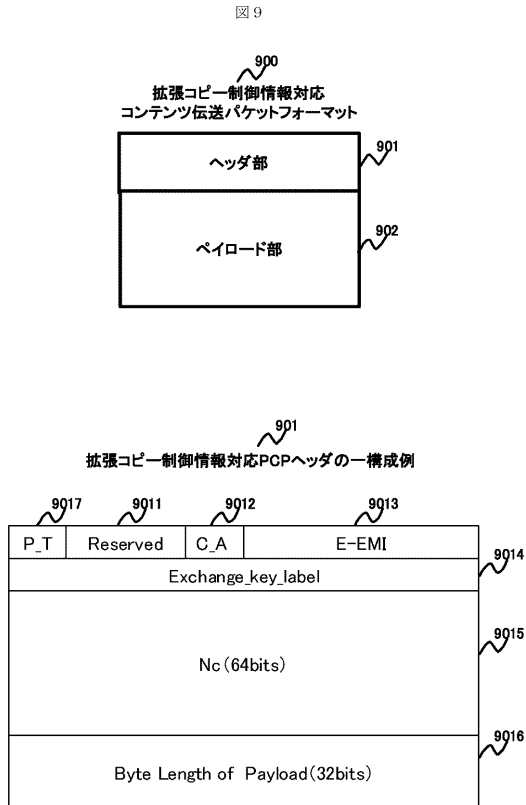


【図 8】

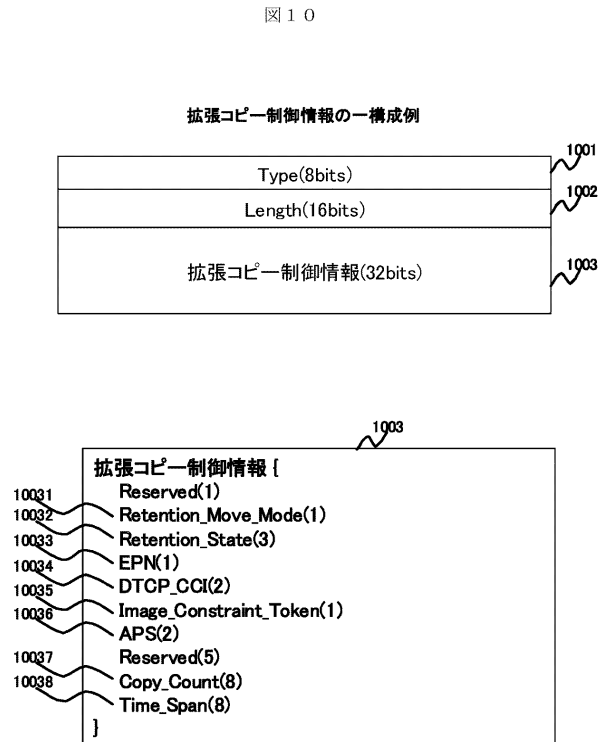
図 8



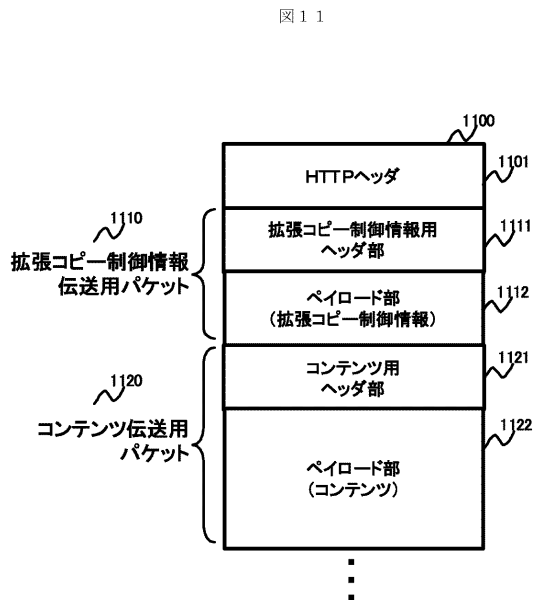
【図 9】



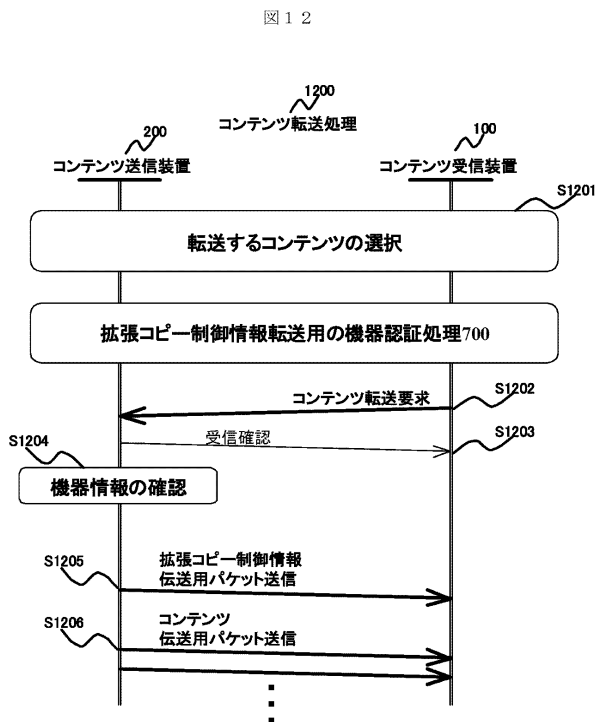
【図 10】



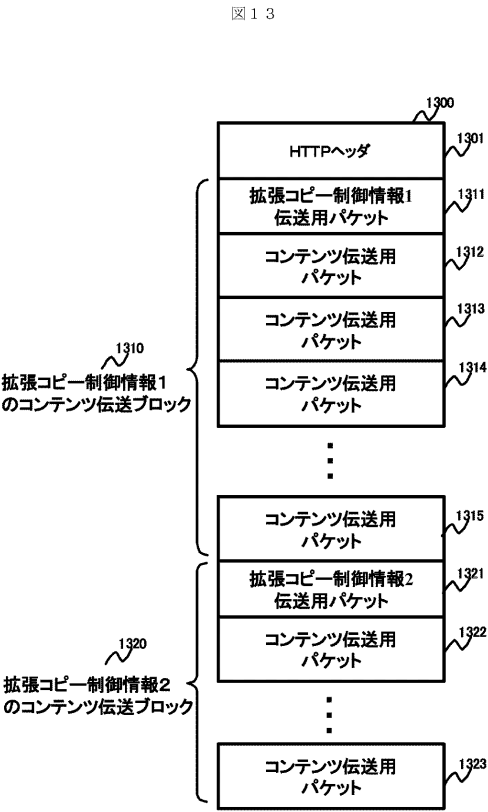
【図 11】



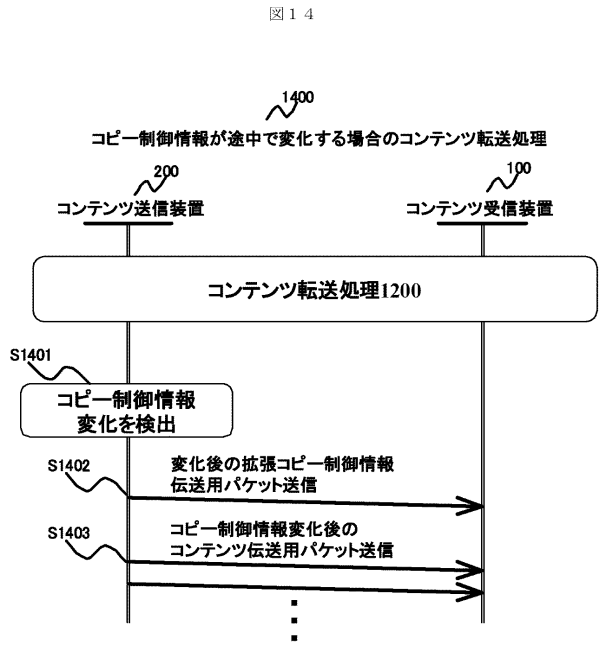
【図 12】



【図 1 3】



【図 1 4】



フロントページの続き

審査官 岸野 徹

(56)参考文献 特開 2 0 0 7 - 0 1 1 5 6 3 (J P , A)
特開 2 0 0 7 - 1 0 4 2 3 6 (J P , A)
特開 2 0 0 5 - 2 4 2 9 7 2 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)
G 0 6 F 2 1 / 1 0
G 0 6 F 1 3 / 0 0
G 0 6 F 2 1 / 6 2
H 0 4 N 7 / 1 7 3