(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4581955号
(P4581955)
(45)発行日　平成22年11月17日(2010.11.17)　(24)登録日　平成22年9月10日(2010.9.10)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
H04L 9/36 (2006.01)　　H04L 9/00 685

請求項の数 23　(全 44 頁)

(21)出願番号　特願2005-290753 (P2005-290753)
(22)出願日　平成17年10月4日 (2005.10.4)
(65)公開番号　特開2007-104236 (P2007-104236A)
(43)公開日　平成19年4月19日 (2007.4.19)
審査請求日　平成19年1月19日 (2007.1.19)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　鈴木　博之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　中野　雄彦
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】コンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラム

(57)【特許請求の範囲】
【請求項１】
コピー制御がなされたコンテンツを伝送するコンテンツ伝送装置であって、
コンテンツ伝送先の機器との間で認証手続きを行なう認証手段と、
コンテンツに関するコピー制御情報を記述した第１のコピー制御情報を処理する第１のコピー制御情報処理手段と、
コンテンツに関する前記第１のコピー制御情報以外の情報を含んだ第２のコピー制御情報を処理する第２のコピー制御情報処理手段と、
前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダと、コンテンツを所定のコンテンツ鍵で暗号化したペイロードからなるパケットを生成して、コンテンツ伝送先の機器に伝送するコンテンツ伝送手段と、
を具備し、
所定ビット長のノンスを用いて生成されたコンテンツ鍵で伝送コンテンツの暗号化を行ない、且つ、ヘッダ内に前記ノンスを伝送するためのフィールドを設ける伝送システム環境下で、前記コンテンツ伝送手段は、前記ノンスを伝送するためのフィールド内に前記第２のコピー制御情報を埋め込んで、パケットを伝送する、
ことを特徴とするコンテンツ伝送装置。
【請求項２】
前記第１のコピー制御情報処理手段は、コンテンツのコピーの可否を規定するコピー制御情報と、コピー可否に応じた暗号モードに関する情報を含む前記第１のコピー制御情報

を処理する、
ことを特徴とする請求項１に記載のコンテンツ伝送装置。
【請求項３】
前記第２のコピー制御情報処理手段は、コンテンツの出力制御に関する情報を含む前記第２のコピー制御情報を処理する、
ことを特徴とする請求項１に記載のコンテンツ伝送装置。
【請求項４】
ヘッダに前記第１のコピー制御情報を書き込むフィールドを設けたヘッダと、コンテンツ埋め込み型のコピー制御情報を埋め込んだコンテンツからなるペイロードで構成された形式のパケットを用いてコンテンツ伝送が行なわれる伝送システム環境下において動作し、
前記第２のコピー制御情報処理手段は、ヘッダ部に埋め込まれた第２の制御情報の有効性を示すモード情報と、第１のコピー制御情報に関するコンテンツ埋め込み型のコピー制御情報の代用可能性を示す代用性情報を含んだ前記第２のコピー制御情報を処理する、
ことを特徴とする請求項１に記載のコンテンツ伝送装置。
【請求項５】
前記伝送システム環境下では、コンテンツのフォーマットの認識可能性に応じたコンテンツのコピー制御を実施するｃｏｇｎｉｚａｎｔ機能が提供されており、
前記第２のコピー制御情報処理手段は、ヘッダに前記第２のコピー制御情報として含まれるモード情報と、ペイロード中におけるコンテンツ埋め込み型のコピー制御情報の存在の有無の組み合わせに応じてｃｏｇｎｉｚａｎｔ機能を実現する、
ことを特徴とする請求項４に記載のコンテンツ伝送装置。
【請求項６】
前記の所定ビット長よりも前記第２のコピー制御情報のビット数分だけ短い擬似ノンスを生成する擬似ノンス生成手段をさらに備え、
前記コンテンツ伝送手段は、前記第２のコピー制御情報と擬似ノンスをビット連結してなるノンスを用いて生成されるコンテンツ鍵で伝送コンテンツを暗号化する、
ことを特徴とする請求項１に記載のコンテンツ伝送装置。
【請求項７】
コンテンツ伝送先の機器からの要求に応じて、パケットのヘッダに含めたノンスの検証を行なうコンテンツ鍵確認手段をさらに備え、
前記第２のコピー制御情報を埋め込んだノンスをヘッダに含めてパケットを伝送したときには、前記コンテンツ鍵確認手段は、コンテンツ伝送先の機器からノンスの検証要求に応じて、該要求されているノンスと前記第２のコピー制御情報を埋め込んだノンスとを比較して検証する、
ことを特徴とする請求項１に記載のコンテンツ伝送装置。
【請求項８】
前記コンテンツ伝送手段が前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送するとき、前記認証手段は、コンテンツ伝送先の機器に送信する認証用コマンド内において、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送することを示す情報を記載する、
ことを特徴とする請求項１に記載のコンテンツ伝送装置。
【請求項９】
前記認証手段は、チャレンジ・アンド・レスポンス認証手続におけるチャレンジ用コマンドに含める機器証明書内に、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送することを示すフラグをセットする、
ことを特徴とする請求項８に記載のコンテンツ伝送装置。
【請求項１０】
前記認証手段は、チャレンジ・アンド・レスポンス認証手続におけるレスポンス用コマンドに含めるメッセージ内に、前記第１のコピー制御情報及び前記第２のコピー制御情報

を含んだヘッダを付けてパケットを伝送することを示すフラグをセットする、
ことを特徴とする請求項８に記載のコンテンツ伝送装置。
【請求項１１】
前記認証手段は、コンテンツ伝送先の機器からの、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送する能力があることの確認を要求するコマンドに応答して、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送することを示す情報の記載したレスポンスを返す、
ことを特徴とする請求項８に記載のコンテンツ伝送装置。
【請求項１２】
コピー制御がなされたコンテンツを伝送するコンテンツ伝送方法であって、
コンテンツ伝送先の機器との間で認証手続きを行なう認証ステップと、
コンテンツに関するコピー制御情報を記述した第１のコピー制御情報を設定する第１のコピー制御情報設定ステップと、
コンテンツに関する前記第１のコピー制御情報以外の情報を含んだ第２のコピー制御情報を設定する第２のコピー制御情報設定ステップと、
前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダと、コンテンツを所定のコンテンツ鍵で暗号化したペイロードからなるパケットを生成して、コンテンツ伝送先の機器に伝送するコンテンツ伝送ステップと、
を有し、
所定ビット長のノンスを用いて生成されたコンテンツ鍵で伝送コンテンツの暗号化を行ない、且つ、ヘッダ内に前記ノンスを伝送するためのフィールドを設ける伝送システム環境下で、前記コンテンツ伝送ステップでは、前記ノンスを伝送するためのフィールド内に前記第２のコピー制御情報を埋め込んで、パケットを伝送する、
ことを特徴とするコンテンツ伝送方法。
【請求項１３】
前記第１のコピー制御情報設定ステップでは、コンテンツのコピーの可否を規定するコピー制御情報と、コピー可否に応じた暗号モードに関する情報を含む前記第１のコピー制御情報を設定する、
ことを特徴とする請求項１２に記載のコンテンツ伝送方法。
【請求項１４】
前記第２のコピー制御情報設定ステップでは、コンテンツの出力制御に関する情報を含む前記第２のコピー制御情報を設定する、
ことを特徴とする請求項１２に記載のコンテンツ伝送方法。
【請求項１５】
ヘッダに前記第１のコピー制御情報を書き込むフィールドを設けたヘッダと、コンテンツ埋め込み型のコピー制御情報を埋め込んだコンテンツからなるペイロードで構成された形式のパケットを用いてコンテンツ伝送が行なわれる伝送システム環境下において、
前記第２のコピー制御情報設定ステップでは、ヘッダ部に埋め込まれた前記第２の制御情報の有効性を示すモード情報と、前記第１のコピー制御情報に関するコンテンツ埋め込み型のコピー制御情報の代用可能性を示す代用性情報を含んだ前記第２のコピー制御情報を設定する、
ことを特徴とする請求項１２に記載のコンテンツ伝送方法。
【請求項１６】
前記伝送システム環境下では、コンテンツのフォーマットの認識可能性に応じたコンテンツのコピー制御を実施するｃｏｇｎｉｚａｎｔ機能が提供されており、
前記第２のコピー制御情報設定ステップでは、ヘッダに前記第２のコピー制御情報として含まれるモード情報と、ペイロード中におけるコンテンツ埋め込み型のコピー制御情報の存在の有無の組み合わせに応じてｃｏｇｎｉｚａｎｔ機能を実現する、
ことを特徴とする請求項１２に記載のコンテンツ伝送方法。

【請求項１７】
前記の所定ビット長よりも前記第２のコピー制御情報のビット数分だけ短い擬似ノンスを生成する擬似ノンス生成ステップをさらに有し、
前記コンテンツ伝送ステップでは、前記第２のコピー制御情報と擬似ノンスをビット連結してなるノンスを用いて生成されるコンテンツ鍵で伝送コンテンツを暗号化する、
ことを特徴とする請求項１２に記載のコンテンツ伝送方法。
【請求項１８】
コンテンツ伝送先の機器からの要求に応じて、パケットのヘッダに含めたノンスの検証を行なうコンテンツ鍵確認ステップをさらに有し、
前記第２のコピー制御情報を埋め込んだノンスをヘッダに含めてパケットを伝送したときには、前記コンテンツ鍵確認ステップでは、コンテンツ伝送先の機器からノンスの検証要求に応じて、該要求されているノンスと第２のコピー制御情報を埋め込んだノンスとを比較して検証する、
ことを特徴とする請求項１２に記載のコンテンツ伝送方法。
【請求項１９】
前記コンテンツ伝送ステップにおいて前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送するとき、前記認証ステップでは、コンテンツ伝送先の機器に送信する認証用コマンド内において、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送することを示す情報を記載する、
ことを特徴とする請求項１２に記載のコンテンツ伝送方法。
【請求項２０】
前記認証ステップでは、チャレンジ・アンド・レスポンス認証手続におけるチャレンジ用コマンドに含める機器証明書内に、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送することを示すフラグをセットする、
ことを特徴とする請求項１９に記載のコンテンツ伝送方法。
【請求項２１】
前記認証ステップでは、チャレンジ・アンド・レスポンス認証手続におけるレスポンス用コマンドに含めるメッセージ内に、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送することを示すフラグをセットする、
ことを特徴とする請求項１９に記載のコンテンツ伝送方法。
【請求項２２】
前記認証ステップでは、コンテンツ伝送先の機器からの、前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダを付けてパケットを伝送する能力があることの確認を要求するコマンドに応答して、当該情報の記載を行なう、
ことを特徴とする請求項１９に記載のコンテンツ伝送方法。
【請求項２３】
コピー制御がなされたコンテンツを伝送するための処理をコンピュータ上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、前記コンピュータを、
コンテンツ伝送先の機器との間で認証手続きを行なう認証手段、
コンテンツに関するコピー制御情報を記述した第１のコピー制御情報を処理する第１のコピー制御情報処理手段、
コンテンツに関する前記第１のコピー制御情報以外の情報を含んだ第２のコピー制御情報を処理する第２のコピー制御情報処理手段、
前記第１のコピー制御情報及び前記第２のコピー制御情報を含んだヘッダと、コンテンツを所定のコンテンツ鍵で暗号化したペイロードからなるパケットを生成して、コンテンツ伝送先の機器に伝送するコンテンツ伝送手段、
として機能させ、
所定ビット長のノンスを用いて生成されたコンテンツ鍵で伝送コンテンツの暗号化を行

ない、且つ、ヘッダ内に前記ノンスを伝送するためのフィールドを設ける伝送システム環境下で、前記コンテンツ伝送手段は、前記ノンスを伝送するためのフィールド内に前記第２のコピー制御情報を埋め込んで、パケットを伝送する、
ことを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、著作権保護若しくはその他の目的で暗号化された伝送コンテンツを伝送処理するコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムに係り、特に、ＤＴＣＰに準拠した情報機器同士で暗号化コンテンツの伝送手続きを実行するコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムに関する。

【０００２】

さらに詳しくは、本発明は、伝送するコンテンツに関する属性情報並びにコピー制御情報をパケット内に挿入して伝送するコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムに係り、特に、コンテンツのフォーマットに依存しない形式で属性情報並びにコピー制御情報をパケット内に挿入して伝送するコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムに関する。

【背景技術】

【０００３】

情報技術の普及に伴い、ＡＶコンテンツのほとんどがデジタル化されており、ＣＤやＤＶＤなどのデジタル・コンテンツを記録再生するメディアが広く利用されている。また、最近では、ＨＤＤレコーダやＨＤＤ搭載ＤＶＤレコーダなど、コンテンツをデジタル記録する機器が家庭内にも浸透してきている。さらには、ネットワークを経由した映像や音楽などのコンテンツの流通・配信サービスが盛んとなり、ＣＤやＤＶＤなどのメディアの移動なしに、ネットワークを経由して遠隔端末間でコンテンツ配信が行なわれている。

【０００４】

勿論、これらＡＶコンテンツは、著作物の１つとして、著作権法の下で無断の複製や改竄などの不正使用から保護を受けることができる。著作権法では、同法第３０条において、個人的に又は家庭内などを使用目的とした場合の使用者本人の複製を許容する一方、同法第４９条第１項においては、私的使用以外での複製物の使用を禁止している。

【０００５】

しかしながら、デジタル化されたコンテンツはコピーや改竄などの不正な操作が比較的容易であることから、法的な整備だけでなく技術的な側面からも、個人的又は家庭的なコンテンツの使用を許容しながら不正使用に対する防御が必要である。とりわけ、国内では２０１１年の地上アナログ放送停波に向けてアナログ放送受信機からデジタル放送受信機への置き換えが急速に進んでおり、家庭内のＡＶコンテンツのデジタル化に対してコンテンツの保護を技術的に実現することが必須と考えられている。

【０００６】

デジタル・コンテンツの著作権保護を目的とした多くの技術が開発されている。例えば、デジタル伝送コンテンツの保護に関する業界標準として、ＤＴＬＡ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｌｉｃｅｎｓｉｎｇ Ａｄｍｉｎｉｓｔｒａｔｏｒ）が開発したＤＴＣＰ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ）が挙げられ、著作権が保護された形でコンテンツを伝送させるための仕組みについて規定されている（例えば、非特許文献１を参照のこと）。

【０００７】

ＤＴＣＰでは、コンテンツ伝送時における機器間の認証プロトコルと、暗号化コンテンツの伝送プロトコルについて取り決められている。その規定は、要約すれば、ＤＴＣＰ準拠機器はＭＰＥＧ（Ｍｏｖｉｎｇ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）など取り扱いが容易な圧縮コンテンツを非暗号の状態で機器外に送出しないことと、暗号化コ

ンテンツを復号するために必要となる鍵交換を所定の相互認証及び鍵交換（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ：ＡＫＥ）アルゴリズムに従って行なうこと、並びにＡＫＥコマンドにより鍵交換を行なう機器の範囲を制限することなどを取り決めている。

【０００８】

コンテンツ提供元であるサーバ（ＤＴＣＰ＿Ｓｏｕｒｃｅ）とコンテンツ提供先であるクライアント（ＤＴＣＰ＿Ｓｉｎｋ）は、ＡＫＥコマンドの送受信により、認証手続きを経て鍵を共有化し、その鍵を用いて伝送路を暗号化してコンテンツの伝送を行なう。したがって、不正なクライアントは、サーバとの認証に成功しないと暗号鍵を取得できないから、コンテンツを享受することはできない。また、ＡＫＥコマンドを送受信する機器の台数や範囲を制限することによって、コンテンツが使用される範囲を著作権法で言うところの個人的又は家庭の範囲内に抑えることができる。

【０００９】

ＤＴＣＰは、原初的には、ＩＥＥＥ１３９４などを伝送路に用いたホーム・ネットワーク上におけるデジタル・コンテンツの伝送について規定したものである。しかしながら、最近では、ＤＬＮＡ（Ｄｉｇｉｔａｌ Ｌｉｖｉｎｇ Ｎｅｔｗｏｒｋ Ａｌｌｉａｎｃｅ）に代表されるように、デジタル化されたＡＶコンテンツをＩＰネットワークを用いて家庭内で流通させようという動きが本格的になっていることから、ＩＰネットワークに対応したＤＴＣＰ技術、すなわちＤＴＣＰ－ＩＰ（ＤＴＣＰ ｍａｐｐｉｎｇ ｔｏ ＩＰ）の開発が進められている。ホーム・ネットワークの多くはルータなどを経由してインターネットなどの外部のＩＰネットワークに接続されると、コンテンツの不正コピーや改竄の危惧が指摘されている。ＤＴＣＰ－ＩＰ技術の確立により、デジタル・コンテンツを保護しながらＩＰネットワークを利用した柔軟で効率的なコンテンツの利用が図ることが急務である。

【００１０】

ＤＴＣＰ－ＩＰは、基本的にはＤＴＣＰ規格に含まれ、ＤＴＣＰ技術をＩＰネットワークに移植した同様の技術であるが、伝送路にＩＰネットワークを使用すること、暗号化されたコンテンツの伝送にＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）やＲＴＰ（Ｒｅａｌ Ｔｉｍｅ Ｐｒｏｔｏｃｏｌ）などのプロトコルを使用するという点で、ＩＥＥＥ１３９４ベースで規定された本来のＤＴＣＰとは相違する。また、ＩＰネットワーク上にはＰＣを主としたさまざまな機器が接続され、データの盗聴、改竄が簡単に行なわれてしまう危険が高いことから、ＤＴＣＰ－ＩＰは、コンテンツを保護しながらネットワーク伝送するためのさらなる方法を規定している（例えば、非特許文献２を参照のこと）。

【００１１】

ここで、ＤＴＣＰ－ＩＰに準拠したコンテンツ伝送について説明する。ＤＴＣＰ－ＩＰに準拠したＳｏｕｒｃｅ機器及びＳｉｎｋ機器間でＨＴＴＰプロトコルを利用したコンテンツ伝送を実施する場合、ＴＣＰストリームのような長大なバイト・ストリームを伝送の途中でコンテンツ鍵を変更しながら暗号化通信が行なわれ、且つ、暗号化コンテンツの復号処理その他のコンテンツ処理を実施する際にコンテンツ鍵の確認手続きが行なわれる。また、相互認証及び鍵交換（ＡＫＥ）、コンテンツ伝送、並びにコンテンツ鍵確認の手続き毎にＴＣＰコネクションが確立される。

【００１２】

具体的には、ＡＫＥ手続きが成功すると、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器とＤＴＣＰ＿Ｓｉｎｋ機器は、認証鍵K_{auth}を共有することができる。ＤＴＣＰ＿Ｓｏｕｒｃｅ機器はコンテンツ鍵の種となる種鍵K_xを生成し、認証鍵K_{auth}で暗号化してＤＴＣＰ＿Ｓｉｎｋ機器に送る。ＤＴＣＰ＿Ｓｏｕｒｃｅ機器は、乱数を用いてノンス（Ｎｏｎｃｅ）N_cを生成して、K_xとN_cと暗号モードを表すＥ－ＥＭＩを基にコンテンツ鍵K_cを生成する。そして、ＤＴＣＰ＿Ｓｉｎｋ機器から要求されているコンテンツを、コンテンツ鍵K_cを用いて暗号化し、暗号化コンテンツとノンスN_cとＥ－ＥＭＩをヘッダに含んだパケット

をＴＣＰストリーム上に乗せてＳｉｎｋ機器に送信する。一方、ＤＴＣＰ＿Ｓｉｎｋ機器側では、ＴＣＰストリームからノンスN_cとＥ－ＥＭＩを取り出すと、これらと鍵K_xを用いて同様にコンテンツ鍵K_cを算出し、暗号化コンテンツを復号することができる。

【００１３】

このように、ＤＴＣＰ－ＩＰは、ＤＴＣＰに準拠した機器同士で認証を行ない、ＤＴＣＰ認証が完了した機器同士で鍵を共有し、コンテンツを伝送する際に暗号化及び復号をすることにより、伝送路の途中におけるコンテンツの盗聴、改竄を防ぐという、ＩＰネットワーク上においても安全なコンテンツ伝送手法を提供することができる。

【００１４】

例えば、ＨＴＴＰの手続きに従ってコンテンツを要求する場合、ＤＴＣＰ＿ＳｏｕｒｃｅがＨＴＴＰサーバとなり、ＤＴＣＰ＿ＳｉｎｋがＨＴＴＰクライアントとなって、ＨＴＴＰのためのＴＣＰ／ＩＰコネクションが作成され、コンテンツの伝送を開始する。ＨＴＴＰクライアントは、通常のＨＴＴＰと全く同様の動作手順によりＨＴＴＰサーバ上のコンテンツを要求する。これに対し、ＨＴＴＰサーバは、要求通りのコンテンツをＨＴＴＰレスポンスとして返す。ＤＴＣＰ＿Ｓｏｕｒｃｅは、ＤＴＣＰ＿Ｓｉｎｋから要求されているコンテンツを、コンテンツ鍵K_cを用いて暗号化し、暗号化コンテンツからなるペイロードとノンスN_cとＥ－ＥＭＩ含んだヘッダからなるパケット（ＰＣＰ：Ｐｒｏｔｅｃｔｅｄ　Ｃｏｎｔｅｎｔ　Ｐａｃｋｅｔ）をＴＣＰストリーム上に乗せて送信する。

【００１５】

また、長大なＴＣＰストリーム全体に渡り同じ暗号鍵を使用し続けると、鍵が解読される危険は高くなる。このため、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器は１２８ＭＢのコンテンツ毎にノンスN_cを１ずつ増加させてコンテンツ鍵K_cを更新する。そして、バイト・ストリームの途中でノンスN_cが大幅に変更されることから、コンテンツ鍵の確認手続きが必要となり、ＤＴＣＰ＿Ｓｉｎｋ機器は、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器に対しノンスN_cの確認のための手続きを行なう。

【００１６】

また、著作権保護に対応したコンテンツ伝送システムでは、コンテンツ保護に関するコンテンツ属性を指定する必要がある。ＤＴＣＰ－ＩＰでは、ＰＣＰヘッダ部に記述するＥ－ＥＭＩ（Ｅｎｃｒｙｐｔｉｏｎ　Ｍｏｄｅ　Ｉｎｄｉｃａｔｏｒ）と、Ｅｍｂｅｄｅｄ　ＣＣＩ（Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）という２つのメカニズムにより、コンテンツに付随したコピー制御情報の伝送を実現している。

【００１７】

Ｅｍｂｅｄｄｅｄ　ＣＣＩは、暗号化するコンテンツ・ストリームの一部として（すなわちＰＣＰペイロードに埋め込んで）伝送されるコピー制御情報である。多くのコンテンツ・フォーマットはストリームに付随してＣＣＩを伝送するために割り当てられたフィールドを備えているが、ＣＣＩの定義やフォーマットはコンテンツ・フォーマット毎に特殊である。Ｅｍｂｅｄｄｅｄ　ＣＣＩは、“Ｃｏｐｙ　Ｎｅｖｅｒ”、“Ｃｏｐｙ　Ｏｎｅ　Ｇｅｎｅｒａｔｉｏｎ”、“Ｎｏ　Ｍｏｒｅ　Ｃｏｐｉｅｓ”、“Ｃｏｐｙ　Ｆｒｅｅ”などとして解釈される。コンテンツ・ストリームをタンパリングすると誤った暗号解読を行なうことになるので、Ｅｍｂｅｄｄｅｄ　ＣＣＩの完全性を保証することができる。

【００１８】

一方のＥ－ＥＭＩは、ＰＣＰヘッダでコンテンツ・ストリームに関するコピー制御情報を示すことにより、容易にアクセスできると同時にセキュリティを実現する。平文状態のＰＣＰヘッダの特定のビット位置というアクセス容易な場所にＥ－ＥＭＩを配置することにより、機器は、コンテンツ・ストリームのＣＣＩを即座に判断することができ、コンテンツ伝送フォーマットを復号してＥｍｂｅｄｄｅｄ　ＣＣＩを抽出する必要がない。Ｅ－ＥＭＩは、デジタルＶＣＲのように特殊なコンテンツ・フォーマットを認識したりデコードしたりすることができないビット・ストリーム記憶機器を実現する際に重要である。

【００１９】

ＤＴＣＰ－ＩＰに準拠する適正なＳｏｕｒｃｅ機器は、コンテンツ・ストリームの特性

に従って正しい暗号モードを選択し、これに基づいてＥ－ＥＭＩを設定する。また、適正なＳｉｎｋ機器は、ＰＣＰヘッダ中のＥ－ＥＭＩで指定される正しい暗号解読モードを選択する。Ｅ－ＥＭＩをコンテンツ鍵K_cの生成に使用しているので、Ｅ－ＥＭＩがタンパリングされると、暗号化時と復号時のコンテンツ鍵K_cが一致しないことから、コンテンツの暗号解読を誤るので、セキュリティが保たれる。

【００２０】

図３１には、ＰＣＰヘッダの内部構造を図解している（例えば、非特許文献３を参照のこと）。このうち、Ｅ－ＥＭＩ（Ｅｘｔｅｎｄｅｄ　ＥＭＩ）は、暗号モードを記述する４ビットのフィールドである。Ｅ－ＥＭＩの値はコピー制御情報の種類に対応する。ビット値定義を下表に示しておく（例えば、非特許文献４を参照のこと）。但し、同表で未使用となっている９つのＥ－ＥＭＩ値は将来の拡張用に予備となっている。

【００２１】

【表１】

E-EMI 値	暗号モード	コピー制御情報
1100	A0	Copy never(CN)
1010	B1	Copy-one-generation(COG)(Cognizant 機器のみ記録可)
1000	B0	Copy-one-generation(COG)(Non-Cognizant 記録可)
0110	C1	Move mode(Audiovisual)⇔Audio 用は未定義
0100	C0	No-more-copies(NMC)
0010	D0	Copy-free with EPN asserted(CF/EPN)
0000	N.A.	Copy-free(CF)

【００２２】

上述したように、ＰＣＰヘッダにコンテンツの暗号モード及びコピー制御情報を指定するＥ－ＥＭＩが記述されるが、コンテンツの保護を目的としたコピー制御情報としてはこれらのパラメータでは十分でない（すなわち４ビット長のＥ－ＥＭＩフィールドに必要なコピー制御情報を書ききれない）場合がある。例えば、コンテンツのアナログ出力制御に関するパラメータ（ＡＰＳ：ＡｎａｌｏｇＰｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）や、出力時の画サイズに関するパラメータ（ＩＣＴ：Ｉｍａｇｅ　Ｃｏｎｓｓｔｒａｉｎｔ　Ｔｏｋｅｎ）などの出力制御情報は、ＤＴＣＰではコピー制御情報の構成要素（付加的若しくは拡張的なコピー制御情報であり、本明細書では「超拡張コピー制御情報」とも呼ぶ）として扱われる。これらは、Ｅ－ＥＭＩに書き込めないため、Ｅｍｂｅｄｄｅｄ　ＣＣＩの一部としてＰＣＰペイロード中に埋め込むより他ない。

【００２３】

また、ＤＴＣＰにおけるコピー制御機能の１つとして、単純にＥ－ＥＭＩに従ってコピーの可否を制御するのではなく、機器がコンテンツのフォーマットとＥｍｂｅｄｄｅｄ　ＣＣＩを正しく認識できた場合（すなわち“ｃｏｇｎｉｚａｎｔ”である場合）、Ｅｍｂｅｄｄｅｄ　ＣＣＩに従ってコンテンツの処理方法を制御するという“Ｃｏｇｎｉｚａｎｔ　Ｆｕｎｃｔｉｏｎ”（Ｃｏｇｎｉｚａｎｔ機能）を提供している。ＰＣＰヘッダ部から取り出したＥ－ＥＭＩと、このＣｏｇｎｉｚａｎｔ機能を用いてＰＣＰペイロードから取り出したＥｍｂｅｄｄｅｄ　ＣＣＩを照合する必要がある。Ｅｍｂｅｄｄｅｄ　ＣＣＩとＥＭＩの関係を下表に示しておく。

【００２４】

【表２】

E-EMI	Embedded-CCI					
	CF	CF/EPN	NMC	COG-AV	COG-Audio	CN
A0	Allowed	Allowed	Allowed	Allowed	Allowed	Allowed
B1	Allowed	Allowed	Prohibited	Allowed	Allowed	Prohibited
B0	Allowed	Allowed	Prohibited	Allowed	Prohibited	Prohibited
C1	Prohibited	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
C0	Allowed	Allowed	Allowed	Allowed	Allowed	Prohibited
D0	Allowed	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
N.A.	Allowed	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited

【００２５】
しかしながら、ＤＴＣＰ－ＩＰでは、コンテンツ・ストリームの一部としてＥｍｂｅｄｄｅｄ　ＣＣＩを伝送するとしか規定していない。現在のＤＴＣＰ－ＩＰでは、ＭＰＥＧトランスポート・ストリームに関してＥｍｂｅｄｄｅｄ　ＣＣＩに相当するＤＴＣＰディスクリプタを挿入するという規定（例えば、非特許文献５を参照のこと）の他には、Ｅｍｂｅｄｄｅｄ　ＣＣＩの構成方法に関する規定は存在しない。ＭＰＥＧを含む多くのコンテンツ・フォーマットにおいて、ストリームに付随してＣＣＩを伝送するためのフィールドが割り当てられているが、ＣＣＩの定義やフォーマットはコンテンツ・フォーマット毎に特殊すなわち区々になっているのが現状である。
【００２６】
ＰＣＰペイロードにコピー制御情報を埋め込むことは、コンテンツ内にコピー制御情報を挿入することであるから、必然的にその記述方法はコンテンツ・フォーマットに依存し、フォーマット毎に区々になる。したがって、ＤＴＣＰ－ＩＰに準拠してＡＶコンテンツを暗号化伝送するときには、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器側ではフォーマット毎にコピー制御情報の記述方法を変えて伝送し、ＤＴＣＰ＿Ｓｉｎｋ機器側ではフォーマット毎にコピー制御情報を解析するためのソフトウェア又はハードウェアを用意する必要があり、機器コストの増大を招来する。また、暗号化したＰＣＰペイロードにコピー制御情報を埋め込むと、受信側では復号後でないとこれを取り出すことができないという問題もある。
【００２７】
【非特許文献１】Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｖｏｌｕｍｅ　１　（Ｉｎｆｏｒｍａｔｉｏｎａｌ　Ｖｅｒｓｉｏｎ），Ｒｅｖｉｓｉｏｎ　１．４（ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／）
【非特許文献２】ＤＴＣＰ　Ｖｏｌｕｍｅ　１　Ｓｕｐｐｌｅｍｅｎｔ　Ｅ　Ｍａｐｐｉｎｇ　ＤＴＣＰ　ｔｏ　ＩＰ（Ｉｎｆｏｒｍａｔｉｏｎａｌ　Ｖｅｒｓｉｏｎ），Ｒｅｖｉｓｉｏｎ　１．１　（ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／）
【非特許文献３】ＤＴＣＰ　Ｖｏｌｕｍｅ１　Ｓｕｐｐｌｅｍｅｎｔ　Ｅ　Ｍａｐｐｉｎｇ　ＤＴＣＰ　ｔｏ　ＩＰ（Ｉｎｆｏｒｍａｔｉｏｎａｌ　Ｖｅｒｓｉｏｎ），Ｒｅｖｉｓｉｏｎ　１．１，　Ｖ１ＳＥ．４．２２　Ｍｏｄｉｆｉｃａｔｉｏｎ　ｔｏ　６．６．３　Ｃｏｎｔｅｎｔ　Ｅｎｃｒｙｐｔｉｏｎ　Ｆｏｒｍａｔｓ
【非特許文献４】ＤＴＣＰ　Ｖｏｌｕｍｅ１　Ｓｕｐｐｌｅｍｅｎｔ　Ｅ　Ｍａｐｐｉｎｇ　ＤＴＣＰ　ｔｏ　ＩＰ（Ｉｎｆｏｒｍａｔｉｏｎａｌ　Ｖｅｒｓｉｏｎ），Ｒｅｖｉｓｉｏｎ１．１，　Ｖ１ＳＥ．４．７　Ｍｏｄｉｆｉｃａｔｉｏｎｓ　ｔｏ　６．４．２　Ｅｎｃｒｙｐｔｉｏｎ　Ｍｏｄｅ　Ｉｎｄｉｃａｔｏｒ（ＥＭＩ）
【非特許文献５】Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏ

tection Specification Volume1（Informational Version）, Revision1.4 Appendix B DTCP_Descriptor for MPEG Transport Streams

【発明の開示】

【発明が解決しようとする課題】

【００２８】

本発明の目的は、ＤＴＣＰに準拠した情報機器同士で暗号化コンテンツの伝送手続きを好適に実行することができる、優れたコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムを提供することにある。

【００２９】

本発明のさらなる目的は、伝送するコンテンツに関する属性情報並びにコピー制御情報をパケット内に挿入して好適に伝送することができる、優れたコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムを提供することにある。

【００３０】

本発明のさらなる目的は、コンテンツのフォーマットに依存しない共通の形式で属性情報並びにコピー制御情報をパケット内に挿入し、且つこれらの情報をセキュアに使用することができる、優れたコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムを提供することにある。

【課題を解決するための手段】

【００３１】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、コピー制御がなされたコンテンツを伝送するコンテンツ伝送装置であって、

コンテンツ伝送先の機器との間で認証手続きを行なう認証手段と、

コンテンツに関するコピー制御情報を記述した第１のコピー制御情報を処理する第１のコピー制御情報処理手段と、

コンテンツに関する第１のコピー制御情報以外の情報を含んだ第２のコピー制御情報を処理する第２のコピー制御情報処理手段と、

第１のコピー制御情報及び第２のコピー制御情報を含んだヘッダ部と、コンテンツを所定のコンテンツ鍵で暗号化したペイロードからなるパケットを生成して、コンテンツ伝送先の機器に伝送するコンテンツ伝送手段と、

を具備することを特徴とするコンテンツ伝送装置である。

【００３２】

本発明は、ＩＰネットワーク上で著作権保護が必要となる情報コンテンツを伝送する情報通信システムに関するものであり、特に、具体的には、ＤＴＣＰ－ＩＰに準拠した情報通信機器の間で、相互認証及び鍵交換を経て共有した鍵を用いて暗号化コンテンツ伝送を安全に行なうコンテンツ伝送装置に関する。

【００３３】

著作権の保護に対応したコンテンツ伝送システムにおいては、コンテンツを暗号化伝送する際に、コンテンツ保護に関するコンテンツ属性を指定する必要がある。例えばＤＴＣＰ－ＩＰでは、ＰＣＰヘッダ部に記述するＥ－ＥＭＩ（Ｅｎｃｒｙｐｔｉｏｎ Ｍｏｄｅ Ｉｎｄｉｃａｔｏｒ）と、ＰＣＰペイロード部すなわちコンテンツ・ストリーム内に埋め込むＥｍｂｅｄｅｄ ＣＣＩ（Ｃｏｐｙ Ｃｏｎｔｒｏｌ Ｉｎｆｏｒｍａｔｉｏｎ）という２つのメカニズムにより、コンテンツに付随したコピー制御情報の伝送を実現している。

【００３４】

ところが、一部のコピー制御情報をペイロード部すなわちコンテンツ・ストリームに記載するという暗号化伝送方式では、記載方法がコンテンツのフォーマットに依存するため、コピー制御情報を作成並びに解読するソフトウェア又はハードウェアのモジュールをフォーマット毎に用意しなければならず、機器コストが増大するという問題がある。

【００３５】

そこで、本発明では、一部のコピー制御情報をパケットのヘッダ部に記載し、それ以外のコピー制御情報をペイロード部に記載してコンテンツを暗号化伝送するという旧来のシステム環境下において、旧来通りのＳｏｕｒｃｅ機器及びＳｉｎｋ機器との互換性を保ちながら、（ＤＴＣＰ－ＩＰで）要求されるコピー制御を実現するために必要となるコピー制御情報をすべてヘッダ部に記載するコンテンツ伝送方式を提案する。

【００３６】

そして、コンテンツに関するコピー制御情報として第１のコピー制御情報と第２のコピー制御情報を定義する。そして、第１のコピー制御情報及び第２のコピー制御情報を含んだヘッダ部と、コンテンツを所定のコンテンツ鍵で暗号化したペイロードからなるパケットを生成して、コンテンツ伝送先の機器に伝送するようにする。

【００３７】

ペイロード部に（一部の）コピー制御情報を埋め込む場合とは相違し、ヘッダ部にコピー制御情報を埋め込む場合には、コンテンツのフォーマットに依存せず、すべてのフォーマットに共通の形式でコピー制御情報を挿入することができる。したがって、Ｓｏｕｒｃｅ機器側においてコピー制御情報を作成し、Ｓｉｎｋ機器側においてコピー制御情報を解析するためのソフトウェア又はハードウェアのモジュールをすべてのフォーマットで共通化することができ、機器コストを削減することができる。

【００３８】

第１のコピー制御情報は、例えば、コンテンツのコピーの可否を規定するコピー制御情報に対応した暗号モードを含んでいる。また、第２のコピー制御情報は、例えばコンテンツの出力制御に関する情報を含んでいる。

【００３９】

例えば、ＤＴＣＰでは、アナログ出力制御に関するパラメータ（ＡＰＳ）や、出力時の画サイズに関するパラメータ（ＩＣＴ）といった出力制御情報がコピー制御情報の構成要素となっている。本発明に係るコンテンツ伝送方式では、これらのビット長の短いＥ－ＥＭＩには書ききれない情報を、第２のコピー制御情報、すなわち超拡張コピー制御情報としてヘッダ部に記述する方法を規定する。

【００４０】

また、ヘッダに第１のコピー制御情報を書き込むフィールドを設けたヘッダと、コンテンツ埋め込み型のコピー制御情報を埋め込んだコンテンツからなるペイロードで構成された形式のパケットを用いてコンテンツ伝送が行なわれるコンテンツ伝送システムに適用する場合には、第２のコピー制御情報に、ヘッダ部に埋め込まれた第２のコピー制御情報の有効性を示すモード情報と、コンテンツ埋め込み型のコピー制御情報の代わりに第１のコピー制御情報を代用可能であることを示す代用性情報を含めるようにしてもよい。

【００４１】

また、コンテンツのフォーマットの認識可能性に応じたコンテンツのコピー制御を実施するｃｏｇｎｉｚａｎｔ機能が提供されている伝送システムに適用した場合、前記第２のコピー制御情報処理手段は、ヘッダに第２のコピー制御情報として含まれるモード情報と、ペイロード中におけるコンテンツ埋め込み型のコピー制御情報の存在の有無の組み合わせに応じてｃｏｇｎｉｚａｎｔ機能を実現することができる。

【００４２】

すなわち、ヘッダ部内の所定位置に挿入された第２のコピー制御情報フィールドの有効性に関して記述したモード情報や、本来はペイロード部に埋め込まれるコピー制御情報の代わりにヘッダ部に書き込まれるコピー制御情報で代用できることを示すＳＥ（Ｓｕｂｓｔｉｔｕｔｅ ｆｏｒ Ｅｍｂｅｄｄｅｄ ＣＣＩ）情報も、超拡張コピー制御情報としてヘッダ部に記述する。このような第２のコピー制御情報をヘッダ部の一部として構成することにより、コンテンツのフォーマットに依存せずすべてのフォーマットに共通の形式でコピー制御情報を伝送することが可能になる。すなわち、暗号化ペイロードからＥｍｂｅｄｄｅｄ ＣＣＩを取り出してＥ－ＥＭＩと照合することなく、従来はＥｍｂｅｄｄｅｄ ＣＣＩとＥ－ＥＭＩの組み合わせにより指定していたコピー制御機能や、ｃｏｇｎｉ

ｚａｎｔ機能を実現することが可能である。

【００４３】

また、伝送システムの規格により、ノンスを用いて生成されたコンテンツ鍵で伝送コンテンツの暗号化が行なわれ、且つヘッダには所定ビット長のノンスを伝送するためのフィールドが設けられている場合、ノンスを伝送するためのフィールド内に第２のコピー制御情報を埋め込んで、パケットを伝送することができる。

【００４４】

具体的には、前記の所定ビット長よりも第２のコピー制御情報のビット数分だけ短い擬似ノンスを生成し、第２のコピー制御情報とこの擬似ノンスをビット連結してなるノンスを用いて生成されるコンテンツ鍵で伝送コンテンツを暗号化することができる。

【００４５】

図３１に示したように、ＰＣＰヘッダには、Ｅ－ＥＭＩとともにノンス情報フィールドが設けられている。Ｅ－ＥＭＩは４ビットしかないので、もはや第２のコピー制御情報を記載する余裕はない。他方、ノンスN_cは、コンテンツを暗号化するコンテンツ鍵K_cを生成する基となる情報であり６４ビットが割り当てられている。本発明の１つの実装形態として、旧来のＰＣＰヘッダ内のノンス情報フィールドの上位８ビットを用いて超拡張コピー制御情報を記述し、残りの下位５６ビットに通常通りに生成されるノンスN_c’の値を書き込むようにすることができる。コンテンツ中でＥ－ＥＭＩが変わる度、また定期的にノンスN_cは更新する。通常、更新する機会毎に擬似的ノンスN_c’の値を単調に増大させるが（１ずつインクリメントしていく）、５６ビットしか使用しなくても、桁あふれは実用上は１度しか起こらないので桁あふれビットを１ビット用意することで対応できる。

【００４６】

このような場合、本発明に係るコンテンツ伝送方式に対応したＳｏｕｒｃｅ機器及びＳｉｎｋ機器は、旧来の６４ビットのノンス情報フィールド中の上位８ビットを第２のコピー制御情報フィールドとして利用するとともに、第２のコピー制御情報が書き込まれた上位８ビットと、５６ビット長の擬似的なノンスN_c’のビット連結からなる６４ビット全体をノンスN_cとして用いてコンテンツ鍵K_cの生成を行なう。不正コピー目的で第２のコピー制御情報を改竄しても、ノンスN_cを改竄することとなり、結局はコンテンツを復号できなくなるので、セキュリティも維持される。

【００４７】

一方、旧来通りのＳｉｎｋ機器も、旧来の６４ビットのノンス情報フィールド全体に書き込まれた値をノンスN_cとして解釈する。この場合、上位８ビットにＰＣＰ－ＣＣＩが書き込まれることから、ノンスN_cの値を変更した際に本来満たされるべき規則性が失われることから、本発明に係る伝送方式に対応していないＳｉｎｋ機器がノンスN_cの規則性を期待していた場合、いわゆるＬｅｇａｃｙ問題が発生する。

【００４８】

Ｓｏｕｒｃｅ機器側で旧来の６４ビットのノンス情報フィールドを８ビットの第２のコピー制御情報フィールドと５６ビットの擬似的なノンス情報フィールドがビット連結として使用した場合、第２のコピー制御情報が変化する度にＬｅｇａｃｙのＳｉｎｋ機器にとってはノンスN_cの連続性が失われる。これに応答して、ＬｅｇａｃｙのＳｉｎｋ機器はコンテンツ鍵確認手続を起動することになる。このような場合、Ｓｏｕｒｃｅ機器側では、コンテンツ鍵確認要求に対し、５６ビットの擬似的なノンスで検証するのではなく、該確認要求されているノンスを第２のコピー制御情報を埋め込んで構成される６４ビットのノンスと比較して検証するようにする。そして、ノンスN_cに異常がないことを示すレスポンス（ＡＣＣＥＰＴＥＤ）を返すことによって、ＬｅｇａｃｙのＳｉｎｋ機器は以降も障害なくコンテンツ受信処理を継続することができる。

【００４９】

また、本発明に係る伝送方式に対応したＳｉｎｋ機器においても、コンテンツ伝送元であるＳｏｕｒｃｅ機器が本方式を適用しているかどうか、すなわち上位８ビットに第２のコピー制御情報が記載されているかどうかを特定しなければならず、Ｌｅｇａｃｙ　Ｓｏ

ｕｒｃｅ機器に対するＬｅｇａｃｙ問題が発生する。

【００５０】

そこで、本発明では、前記コンテンツ伝送手段が第１のコピー制御情報及び第２のコピー制御情報を含んだヘッダを付けてパケットを伝送するとき、前記認証手段は、コンテンツ伝送先の機器に送信するコマンド内にその旨を示す情報を記載して、伝送先の機器に通知するようにしている。すなわち、コンテンツ送信元となるＳｏｕｒｃｅ機器が本発明に係るコンテンツ伝送方式に対応している場合、ＰＣＰヘッダ部に超拡張コピー制御情報を埋め込むことを示すフラグを相互認証手続（ＡＫＥ）で交換する機器証明書の中に含めることによって、Ｓｉｎｋ機器はＳｏｕｒｃｅ機器がＬｅｇａｃｙ機器でないことを認識することができる。あるいは、能力確認用のコマンドを使用するようにしてもよい。

【００５１】

また、本発明の第２の側面は、コピー制御がなされたコンテンツを伝送するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、前記コンピュータ・システムに対し、

コンテンツ伝送先の機器との間で認証手続きを行なう認証手順と、

コンテンツに関するコピー制御情報を記述した第１のコピー制御情報を設定する第１のコピー制御情報設定手順と、

コンテンツに関する第１のコピー制御情報以外の情報を含んだ第２のコピー制御情報を設定する第２のコピー制御情報設定手順と、

第１のコピー制御情報及び第２のコピー制御情報を含んだヘッダと、コンテンツを所定のコンテンツ鍵で暗号化したペイロードからなるパケットを生成して、コンテンツ伝送先の機器に伝送するコンテンツ伝送手順と、

を実行させることを特徴とするコンピュータ・プログラムである。

【００５２】

本発明の第２の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第２の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係るコンテンツ伝送装置と同様の作用効果を得ることができる。

【発明の効果】

【００５３】

本発明によれば、ＤＴＣＰに準拠した情報機器同士で暗号化コンテンツの伝送手続きを好適に実行することができる、優れたコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムを提供することができる。

【００５４】

また、本発明によれば、伝送するコンテンツに関する属性情報並びにコピー制御情報をパケット内に挿入して好適に伝送することができる、優れたコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムを提供することができる。

【００５５】

また、本発明によれば、コンテンツのフォーマットに依存しない共通の形式で属性情報並びにコピー制御情報をパケット内に挿入し、且つこれらの情報をセキュアに使用することができる、優れたコンテンツ伝送装置及びコンテンツ伝送方法、並びにコンピュータ・プログラムを提供することができる。

【００５６】

本発明によれば、ＤＴＣＰ－ＩＰに準拠した暗号化コンテンツの伝送を行なう際に、Ｓｉｎｋ機器側で必要となるすべてのコピー制御情報をＰＣＰヘッダ中に記載することができる。言い換えれば、コンテンツのフォーマットに依存せずに（すなわちすべてのフォーマットに共通の形式で）、コピー制御情報をコンテンツに付けて伝送することができる。そして、Ｓｏｕｒｃｅ機器側においてコピー制御情報を作成し、Ｓｉｎｋ機器側において

コピー制御情報を解析するためのソフトウェア又はハードウェアのモジュールをすべてのフォーマットで共通化することにより、機器コストを削減することができる。

【００５７】

また、必要となるすべてのコピー制御情報をＰＣＰヘッダ中に記載することで、コンテンツのフォーマットに依存することなくコピー制御情報を伝送することができるので、ＤＴＣＰ－ＩＰにおいて既に規定されているＭＰＥＧトランスポート・ストリームにおいても同様に適用することが可能である。

【００５８】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【発明を実施するための最良の形態】

【００５９】

本発明は、ＴＣＰ／ＩＰなどのネットワーク上やファイル・システムからバイト・ストリームとして暗号データを受理して復号する情報通信システムに関するものであり、特に、ＴＣＰストリームのような長大なバイト・ストリームを途中で復号鍵を変更しながら暗号化通信を行なう情報通信システムに関する。かかるシステムの具体例は、ＤＴＣＰ機器の間で行なわれるＨＴＴＰプロトコルを利用したコンテンツ伝送である。以下、図面を参照しながら本発明の実施形態について詳解する。

【００６０】

Ａ．システム構成

ＤＴＣＰ－ＩＰに従ったコンテンツ伝送は、コンテンツの要求を受理してコンテンツを送信するサーバとしてのＳｏｕｒｃｅ機器と、コンテンツを要求し、コンテンツを受信し、再生若しくは記録するクライアントとしてのＳｉｎｋ機器で構成される。図１には、本発明の一実施形態に係る情報通信システムの構成例を模式的に示している。

【００６１】

図示の例では、Ｓｏｕｒｃｅ機器とＳｉｎｋ機器の各エンティティにより、ＤＴＣＰ－ＩＰ　ＡＫＥシステムが構築されている。

【００６２】

ＤＴＣＰ－ＩＰ に準拠した認証サーバであるＳｏｕｒｃｅ機器とＤＴＣＰ－ＩＰに準拠した認証クライアントであるＳｉｎｋ機器はネットワークを経由して接続されている。

【００６３】

ここで言うネットワークには、Ｅｔｈｅｒｎｅｔ（登録商標）や、インターネット、その他のＩＰネットワークが含まれる。

【００６４】

図２及び図３には、図１に示した情報通信システムにおいて、クライアント（すなわち、Ｓｉｎｋ機器）及びサーバ（すなわち、Ｓｏｕｒｃｅ機器）として動作するコンテンツ伝送装置の、特に認証及びコンテンツ伝送に着目した機能構成をそれぞれ模式的に示している。Ｓｉｎｋ機器とＳｏｕｒｃｅ機器は、インターネットなどのＴＣＰ／ＩＰネットワーク上でコネクションを確立することができ、このコネクションを利用して、認証手続きやコンテンツ伝送手続きを実行することができる。

【００６５】

図２に示すＳｉｎｋ機器は、ＤＴＣＰ－ＩＰ規格に準拠しており、ＤＴＣＰ＿Ｓｉｎｋとして動作する。図示のクライアント機器は、機能ブロックとして、ＤＴＣＰ－ＩＰ認証ブロックと、ＤＴＣＰ－ＩＰコンテンツ受信ブロックと、コンテンツ再生／記録ブロックを備えている。

【００６６】

ＤＴＣＰ－ＩＰ認証ブロックは、ＡＫＥブロックと、メッセージ・ダイジェスト生成ブロックと、コンテンツ復号ブロックを備えている。

【００６７】

ＡＫＥブロックは、ＤＴＣＰ－ＩＰにおけるＡＫＥ機構（ＤＴＣＰ＿Ｓｉｎｋ側）を実

現するブロックでる。このＡＫＥブロックは後述のメッセージ・ダイジェスト生成ブロックから要求されたパラメータを渡す機能も備えている。

【００６８】

メッセージ・ダイジェスト生成ブロックは、指定されたアルゴリズムに従い、パラメータのメッセージ・ダイジェストを生成するブロックである。メッセージ・ダイジェストを生成するアルゴリズムはあらかじめ用意されたアルゴリズムを指定することができる。あらかじめ用意されたアルゴリズムとして、例えばＭＤ５やＳＨＡ－１といった一方向性ハッシュ関数に関するアルゴリズムが挙げることができる（ＳＨＡ－１は、ＭＤ５と同様、ＭＤ４を改良したものに相当するが、１６０ビットのハッシュ値を生成するので、強度はＭＤシリーズを上回る）。

【００６９】

メッセージ・ダイジェスト生成ブロックは、ＤＴＣＰ－ＩＰ認証ブロックの外に公開してはならないＡＫＥブロックが保持するパラメータのメッセージ・ダイジェストを生成できるようにＡＫＥブロックと密に配置され、ＡＫＥブロックへパラメータを要求して取得することが可能であり、そのパラメータ若しくは外部から与えられたパラメータのメッセージ・ダイジェストを作成することができる。

【００７０】

コンテンツ復号ブロックは、サーバから受信した暗号化されたコンテンツ・データをＡＫＥで交換した鍵K_xを用いてコンテンツの復号鍵K_cを算出し、暗号コンテンツを復号するブロックである。ここで復号されたコンテンツは、コンテンツ再生／記録ブロックへ渡される。

【００７１】

コンテンツ再生／記録ブロックは、渡されたコンテンツを、再生モードの場合は再生を行ない、記録モードの場合は保存する。但し、コンテンツの記録動作は、コンテンツ伝送用のパケットＰＣＰ内に挿入されているコピー制御情報の規定に従う。

【００７２】

ＤＴＣＰ－ＩＰコンテンツ受信ブロックは、ＡＫＥを実施した後にＳｏｕｒｃｅ機器とのコンテンツ伝送手続きを実行する処理モジュールである。図示の例では、ＤＴＣＰ－ＩＰコンテンツ受信ブロックはＨＴＴＰクライアント・ブロックを持ち、ＨＴＴＰクライアントとしてＨＴＴＰサーバへコンテンツを要求し、応答されたコンテンツをＨＴＴＰサーバから受信する。

【００７３】

ＨＴＴＰクライアント・ブロックは、ＨＴＴＰリクエスト管理ブロックとＨＴＴＰレスポンス管理ブロックに分かれる。さらに、ＨＴＴＰリクエスト管理ブロックは、ＨＴＴＰリクエスト送信ブロックとＨＴＴＰリクエスト生成ブロックに分かれる。

【００７４】

ＨＴＴＰリクエスト生成ブロックは、送信するコンテンツ伝送要求（ＨＴＴＰリクエスト）を生成する。ここで生成されたＨＴＴＰリクエストは、ＨＴＴＰリクエスト送信ブロックによりサーバへ送信される。

【００７５】

ＨＴＴＰレスポンス管理ブロックは、ＨＴＴＰレスポンス受信ブロックとＨＴＴＰレスポンス解釈ブロックに分かれる。サーバから返信されるＨＴＴＰレスポンスと暗号化されたコンテンツは、ＨＴＴＰ受信ブロックで受信される。ここで受信したＨＴＴＰレスポンスは、ＨＴＴＰレスポンス解釈ブロックでチェックされる。ここでのチェックがＯＫの場合は受信した暗号化コンテンツをＤＴＣＰ認証ブロック内のコンテンツ復号ブロックへ送る。また、このチェックがＮＧの場合は、エラー・レスポンスとしての処理を行なう。Ｓｏｕｒｃｅ機器からのＨＴＴＰレスポンスは１つ以上のＰＣＰからなる。

【００７６】

ＤＴＣＰ－ＩＰ認証ブロックとＤＴＣＰ－ＩＰコンテンツ受信ブロックは、サーバ機器との間で個別のＴＣＰ／ＩＰコネクションを確立して、それぞれ認証手続き及びコンテン

ツ伝送手続きを互いに独立して実行する。

【００７７】

また、図３に示すＳｏｕｒｃｅ機器は、ＤＴＣＰ－ＩＰ規格に準拠しており、ＤＴＣＰ＿Ｓｏｕｒｃｅとして動作する。サーバ機器は、機能ブロックとして、ＤＴＣＰ－ＩＰ認証ブロックと、ＤＴＣＰ－ＩＰコンテンツ送信ブロックと、コンテンツ管理ブロックを備えている。

【００７８】

ＤＴＣＰ－ＩＰ認証ブロックは、認証手続き実行手段に相当し、ＡＫＥブロックと、メッセージ・ダイジェスト生成ブロックと、コンテンツ暗号化ブロックを備えている。

【００７９】

ＡＫＥブロックは、ＤＴＣＰ－ＩＰにおけるＡＫＥ機構（ＤＴＣＰ＿Ｓｏｕｒｃｅ側）を実現するブロックである。このブロックは、後述のメッセージ・ダイジェスト生成ブロックから要求されたパラメータを渡す機能も備えている。ＡＫＥブロックは認証したＤＴＣＰ＿Ｓｉｎｋ機器に関する情報を認証した機器の数だけ保持し、それをクライアントからコンテンツが要求された際に認証済みのクライアントかどうかを判別するのに使用する。

【００８０】

メッセージ・ダイジェスト生成ブロックは指定されたアルゴリズムに従い、パラメータのメッセージ・ダイジェストを生成するブロックである。メッセージ・ダイジェストを生成するアルゴリズムはあらかじめ用意されたアルゴリズムを指定できる。あらかじめ用意されたアルゴリズムとは、例えばＭＤ５やＳＨＡ－１といった一方向性ハッシュ関数に関するアルゴリズムが挙げられる（同上）。

【００８１】

メッセージ・ダイジェスト生成ブロックは、ＤＴＣＰ－ＩＰ認証ブロックの外に公開してはならないＡＫＥブロックが保持するパラメータのメッセージ・ダイジェストを生成できるようにＡＫＥブロックと密に配置され、ＡＫＥブロックへパラメータを要求して取得することが可能で、そのパラメータ若しくは外部から与えられたパラメータのメッセージ・ダイジェストを作成することができる。

【００８２】

コンテンツ暗号化ブロックは、ＤＴＣＰ－ＩＰコンテンツ送信ブロックの要求に応じてコンテンツ管理ブロックより読み出したコンテンツ・データを、ＡＫＥで交換した鍵K_xから生成したコンテンツ鍵K_cを用いて暗号化するブロックである。ここで復号されたコンテンツは、クライアントへ送信するために、ＤＴＣＰ－ＩＰコンテンツ送信ブロックへ渡される。

【００８３】

コンテンツ管理ブロックは、ＤＴＣＰ－ＩＰの機構を用いて保護されるべきコンテンツを管理するブロックである。コンテンツ暗号化ブロックの読み出しに応じて、コンテンツのデータを渡す。

【００８４】

ＤＴＣＰ－ＩＰコンテンツ送信ブロックは、ＨＴＴＰサーバ・ブロックを持ち、ＨＴＴＰサーバとしてクライアントからのリクエストを受理し、要求に応じた処理を実行する。

【００８５】

ＨＴＴＰサーバ・ブロックは、ＨＴＴＰリクエスト管理ブロックとＨＴＴＰレスポンス管理ブロックに分かれる。さらに、ＨＴＴＰリクエスト管理ブロックは、ＨＴＴＰリクエスト受信ブロックと、ＨＴＴＰリクエスト解釈ブロックに分かれる。

【００８６】

ＨＴＴＰリクエスト受信ブロックは、クライアントからのＨＴＴＰリクエストを受信する。受信したＨＴＴＰリクエストはＨＴＴＰリクエスト解釈ブロックに送られ、チェックされる。ＨＴＴＰリクエスト解釈ブロックにおけるチェックがＯＫの場合、ＨＴＴＰリクエストの情報をＤＴＣＰ－ＩＰ認証ブロックへ通知する。

【００８７】
ＨＴＴＰレスポンス管理ブロックは、ＨＴＴＰレスポンス生成ブロックとＨＴＴＰレスポンス送信ブロックに分かれる。
【００８８】
ＨＴＴＰレスポンス生成ブロックは、ＨＴＴＰリクエスト解釈ブロックでのチェックがＯＫの場合、暗号化されたコンテンツを返すためのＨＴＴＰレスポンスを作成する。ＨＴＴＰレスポンスは１つ以上のＰＣＰからなる。一方、ＨＴＴＰリクエスト解釈ブロックでのチェックがＮＧの場合、エラーを返すためのＨＴＴＰレスポンスを作成する。
【００８９】
ＨＴＴＰレスポンス送信ブロックは、作成されたＨＴＴＰレスポンスを、要求元のクライアントへＨＴＴＰレスポンスを送信する。また、ＨＴＴＰリクエスト解釈ブロックでのチェックがＯＫの場合には、ＨＴＴＰレスポンス・ヘッダに続けて、ＤＴＣＰ－ＩＰ認証ブロック内のコンテンツ暗号化ブロックで暗号化したコンテンツを送信する。
【００９０】
ＤＴＣＰ－ＩＰ認証ブロックとＤＴＣＰ－ＩＰコンテンツ送信ブロックは、Ｓｉｎｋ機器との間で個別のＴＣＰ／ＩＰコネクションを確立して、それぞれ認証手続き及びコンテンツ伝送手続きを互いに独立して実行する。
【００９１】
なお、ＤＴＣＰ－Ｓｉｎｋ機器及びＤＴＣＰ－Ｓｏｕｒｃｅ機器のいずれもがＤＴＣＰ－ＩＰ認証ブロック内に持つメッセージ・ダイジェスト生成ブロックは、ＤＴＣＰ－ＩＰ自体で規定される機能モジュールではなく、また本発明の要旨には直接関連しない。
【００９２】
Ｂ．ＨＴＴＰを利用したコンテンツ伝送
この項では、ＤＴＣＰ－ＩＰに従ったコンテンツの伝送手順について説明する。図４には、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器とＤＴＣＰ＿Ｓｉｎｋ機器の間でＡＫＥに基づく鍵交換手続き、及び鍵交換により共有した鍵を利用した暗号化コンテンツ伝送を行なう仕組みを図解している。
【００９３】
ＤＴＣＰ＿ＳｏｕｒｃｅとＤＴＣＰ＿Ｓｉｎｋは、まず１つのＴＣＰ／ＩＰコネクションを確立し、機器同士の認証を行なう。この認証を、ＤＴＣＰ認証若しくはＡＫＥ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎａｎｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ）と言う。ＤＴＣＰ準拠機器には、ＤＴＬＡ（前述）により発行された機器証明書が埋め込まれている。ＤＴＣＰ認証手続きでは、互いが正規のＤＴＣＰ準拠機器であることを確かめた後、認証鍵K_{auth}をＤＴＣＰ＿Ｓｏｕｒｃｅ機器とＤＴＣＰ＿Ｓｏｕｒｃｅ機器で共有することができる。
【００９４】
ＡＫＥ手続きが成功すると、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器はコンテンツ鍵K_cの種となる種鍵K_xを生成し、認証鍵K_{auth}で暗号化してＤＴＣＰ＿Ｓｉｎｋ機器に送る。種鍵K_xは、コンテンツ伝送時にコンテンツを暗号化するためのコンテンツ鍵K_cを生成するために使用される。そして、ＤＴＣＰ準拠の機器間でＡＫＥによる認証及び鍵交換手続きが済んだ後、ＤＴＣＰ＿Ｓｉｎｋ機器はＤＴＣＰ＿Ｓｏｕｒｃｅ機器上のコンテンツを要求する。ＤＴＣＰ＿Ｓｏｕｒｃｅ機器は、ＣＤＳ（ＣｏｎｔｅｎｔＤｉｒｅｃｔｏｒｙ Ｓｅｒｖｉｃｅ）などを通じてＤＴＣＰ＿Ｓｉｎｋ機器にＤＴＣＰ＿Ｓｏｕｒｃｅ機器上のコンテンツへのアクセス先を示すコンテンツ場所をあらかじめ伝えることができる。ＤＴＣＰ＿Ｓｉｎｋがコンテンツを要求するとき、ＨＴＴＰやＲＴＰなどのプロトコルを利用することができる。
【００９５】
図４に示すようにＨＴＴＰの手続きに従ってコンテンツを要求する場合、ＤＴＣＰ＿ＳｏｕｒｃｅがＨＴＴＰサーバとなり、ＤＴＣＰ＿ＳｉｎｋがＨＴＴＰクライアントとなって、コンテンツの伝送を開始する。ちなみに、ＲＴＰによる伝送を要求するとき、ＤＴＣＰ＿ＳｏｕｒｃｅがＲＴＰＳｅｎｄｅｒとなり、ＤＴＣＰ＿ＳｉｎｋがＲＴＰ Ｒｅｃｅ

ｉｖｅｒとなってコンテンツの伝送を開始する。ＨＴＴＰでコンテンツ伝送を行なう際、ＤＴＣＰ認証のためのＴＣＰ／ＩＰコネクションとは別に、ＨＴＴＰのためのＴＣＰ／ＩＰコネクションがＨＴＴＰクライアントより作成される（すなわち、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器とＤＴＣＰ＿Ｓｉｎｋ機器はそれぞれ、ＡＫＥ手続き用とコンテンツ伝送用に個別のソケット（ＩＰアドレスとポート番号の組み合わせ）を持つ）。そして、ＨＴＴＰクライアントは、通常のＨＴＴＰと全く同様の動作手順によりＨＴＴＰサーバ上のコンテンツを要求する。これに対し、ＨＴＴＰサーバは、要求通りのコンテンツをＨＴＴＰレスポンスとして返す。

【００９６】

ＨＴＴＰレスポンスとして伝送されるデータは、ＨＴＴＰサーバすなわちＤＴＣＰ＿Ｓｏｕｒｃｅ機器がＡＫＥ認証をした後に共有した鍵を用いてコンテンツを暗号化したデータとなっている。具体的には、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器は、乱数を用いてノンスN_cを生成して、種鍵K_xとノンスN_cと暗号モードを表すＥ－ＥＭＩを基にコンテンツ鍵K_cを生成する。そして、ＤＴＣＰ＿Ｓｉｎｋ機器から要求されているコンテンツを、コンテンツ鍵K_cを用いて暗号化し、暗号化コンテンツからなるペイロードとノンスN_cとＥ－ＥＭＩを含んだヘッダからなるパケットであるＰＣＰ（Ｐｒｏｔｅｃｔｅｄ Ｃｏｎｔｅｎｔ Ｐａｃｋｅｔ）をＴＣＰストリーム上に乗せて送信する。そして、ＩＰプロトコルは、ＴＣＰストリームを所定の単位となるパケットの大きさに分割し、さらにヘッダ部を付加したＩＰパケットにし、指定されたＩＰアドレス宛てに届ける。

【００９７】

ＤＴＣＰ＿Ｓｉｎｋ機器側では、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器からの各ＩＰパケットを受信すると、これをＴＣＰストリームに組み立てて、送信されたＰＣＰを取り出す。そして、ストリームからノンスN_cとＥ－ＥＭＩを取り出すと、これらと種鍵K_xを用いて同様にコンテンツ鍵K_cを算出し、暗号化コンテンツを復号することができる。そして、復号化した後の平文のコンテンツに対し再生若しくは記録などの処理を実施することができる。そして、ＨＴＴＰプロトコルを利用したコンテンツ伝送が終了すると、例えばＤＴＣＰ－Ｓｉｎｋ機器側から、使用したＴＣＰコネクションを適宜切断する。

【００９８】

また、長大なＴＣＰストリーム全体に渡り同じ暗号鍵を使用し続けると、鍵が解読される危険は高くなる。このため、ＤＴＣＰ－ＩＰでは、Ｓｏｕｒｃｅ機器は１２８ＭＢ毎にノンスN_cすなわちコンテンツ鍵K_cを更新する（１ずつインクリメントする）よう取り決められている。バイト・ストリーム中で、同じノンスN_cから生成されたコンテンツ鍵K_cを用いて暗号化されたデータの範囲は、同じ鍵を用いて復号することができる復号化単位となる。

【００９９】

ＤＴＣＰ－ＩＰではさらにコンテンツ鍵の確認手続きが必要となる。すなわち、ＤＴＣＰ＿Ｓｉｎｋ機器は、コンテンツ伝送用のＴＣＰコネクションとは別に、コンテンツ鍵の確認用のＴＣＰコネクションをさらに確立し、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器に対しコンテンツ鍵確認のための手続きを行なう。ＤＴＣＰ＿Ｓｉｎｋ機器は、コンテンツ鍵の確認が必要になると、適宜このＴＣＰコネクションを確立する。例えば、ＤＴＣＰ－ＩＰ Ｖｏｌｕｍｅ １ Ｓｕｐｐｌｅｍｅｎｔ Ｅ．８．６には、コンテンツ鍵の確認手続きとして“Ｃｏｎｔｅｎｔ Ｋｅｙ Ｃｏｎｆｉｒｍａｔｉｏｎ”を規定している。これによれば、Ｓｉｎｋ機器は、ＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦ ｓｕｂｆｕｎｃｔｉｏｎを用いて、現在のノンスN_cに関連付けられたコンテンツ鍵の確認を行なう。

【０１００】

既に述べたように、ＤＴＣＰ－ＩＰでは、ノンスN_cを含んだヘッダと、暗号化コンテンツからなるペイロードで構成される、ＰＣＰというパケット形式でコンテンツ伝送が行なわれる。

【０１０１】

図５には、ＰＣＰのデータ構造を模式的に示している。ＰＣＰヘッダは平文であり、ノ

ンスN_cが含まれている。また、ＰＣＰペイロードはノンスN_cで決まるコンテンツ鍵K_cで暗号化されたコンテンツ（但し、コピー制御情報として“ｃｏｐｙ－ｆｒｅｅ”が指定されているコンテンツは暗号化不要）で構成される。ここで、ＰＣＰペイロードは、常に１６バイトの倍数になるように、必要に応じて暗号化前にｐａｄｄｉｎｇが行なわれる。また、コンテンツの安全のため、定期的にノンスN_cすなわちコンテンツ鍵K_cを更新するが、その時点でもＰＣＰは仕切られる（コンテンツ鍵K_cを更新しなくても複数のＰＣＰに仕切ることは可能）。また、ｐｒｏｔｅｃｔｅｄ＿ｃｏｎｔｅｎｔ＿ｌｅｎｇｔｈの値が１６の整数倍でないときは、コンテンツに１～１５バイトのパディングが付く。ノンスN_cの更新に伴い、コンテンツ鍵確認手続を起動するのは上述した通りである。ちなみに、ＨＴＴＰレスポンスは１つ以上のＰＣＰからなり、ＲＴＰペイロードは１つのＰＣＰからなる。図６には、ＰＣＰをパディングする様子を示している。

【０１０２】

Ｃ．コピー制御情報の伝送

ＤＴＣＰ－ＩＰのように著作権の保護を目的としたコンテンツ伝送システムにおいては、コンテンツを暗号化伝送する際に、コンテンツ保護に関するコンテンツ属性を指定する必要がある。

【０１０３】

ＤＴＣＰ－ＩＰでは、ＰＣＰヘッダにＰＣＰペイロードの暗号モード及びコピー情報を指定する４ビットのＥ－ＥＭＩフィールドを設けることと、ＰＣＰペイロードすなわちコンテンツ・ストリームの一部としてコピー制御情報Ｅｍｂｅｄｄｅｄ　ＣＣＩを伝送することが規定されている。しかしながら、Ｅｍｂｅｄｄｅｄ　ＣＣＩに関しては、ＭＰＥＧトランスポート・ストリームについてのみＤＴＣＰディスクリプタとして記述することが規定されているのみで、Ｅｍｂｅｄｄｅｄ　ＣＣＩの定義やフォーマットはコンテンツ・フォーマット毎に区々になっているのが現状である。このため、Ｅｍｂｅｄｄｅｄ　ＣＣＩの記述方法がコンテンツ・フォーマットに依存することとなり、コピー制御情報を作成並びに解読するソフトウェア又はハードウェアのモジュールをフォーマット毎に用意しなければならず、機器コストが増大するという問題がある。

【０１０４】

そこで、本実施形態では、Ｅ－ＥＭＩをＰＣＰヘッダに記載するとともに、ヘッダには書ききれないコピー制御情報をＥｍｂｅｄｄｅｄ　ＣＣＩとしてＰＣＰペイロード埋め込んでコンテンツを暗号化伝送するという旧来のＤＴＣＰ－ＩＰシステムにおいて、旧来通り（すなわちＬｅｇａｃｙ）のＳｏｕｒｃｅ機器及びＳｉｎｋ機器との互換性を保ちながら、必要となるコピー制御情報をすべてＰＣＰヘッダに記載するコンテンツ伝送方式を採用している。

【０１０５】

ＰＣＰヘッダ部にコピー制御情報を埋め込む場合、コンテンツのフォーマットに依存しないことから、すべてのコンテンツ・フォーマットに共通の形式でコピー制御情報を伝送することが可能になる。この結果、Ｓｏｕｒｃｅ機器側においてコピー制御情報を作成し、Ｓｉｎｋ機器側においてコピー制御情報を解析するためのソフトウェア又はハードウェアのモジュールをすべてのフォーマットで共通化することにより、機器コストを削減することができる。

【０１０６】

図３１を参照しながら既に説明したように、ＰＣＰヘッダには、Ｅ－ＥＭＩとともにノンス情報フィールドが設けられている。Ｅ－ＥＭＩは４ビットしかないので、もはやそれ以外のコピー制御情報（すなわち超拡張コピー制御情報）を記載する余裕はない。他方、ノンスN_cは、コンテンツを暗号化するコンテンツ鍵K_cを生成する基となる情報であり６４ビット長のフィールドがヘッダ内で割り当てられている。コンテンツ中でＥ－ＥＭＩが変わる度、また定期的にノンスN_cは更新する。通常、更新する機会毎にノンスN_cの値を単調に増大させる（１ずつインクリメントしていく）ため、６４ビットを必要としない。そこで、本実装形態では、旧来のＰＣＰヘッダ内のノンス情報フィールドの一部の領域を

用いて超拡張コピー制御情報を伝送するようにしている。

【０１０７】

本明細書では、Ｅ－ＥＭＩ以外にＰＣＰヘッダに挿入される超拡張コピー制御情報のことを“ＰＣＰ－ＣＣＩ”と呼ぶことにする。図７には、本実施形態で採用するＰＣＰヘッダのデータ構造を示している。同図の例では、旧来のＰＣＰヘッダ内のノンス情報フィールドの上位８ビットを用いてＰＣＰ－ＣＣＩを記述し、残りの下位５６ビットに通常通り生成するノンスN_c’の値を書き込むようにしている。６４ビットのノンス情報N_cフィールドの上位８ビットにＰＣＰ－ＣＣＩを埋め込んでも、コンテンツ鍵K_cの安全性は残りの５６ビットで実用に耐えられる。

【０１０８】

図７からも分るように、ＰＣＰヘッダ部の基本的な構造やサイズは旧来のものと変更されない。この場合、本実施形態に係るコンテンツ伝送方式に対応したＳｏｕｒｃｅ機器及びＳｉｎｋ機器は、旧来の６４ビットのノンス情報フィールド中のうち上位８ビットをＰＣＰ－ＣＣＩフィールドとして利用するとともに、ＰＣＰ－ＣＣＩ情報が書き込まれた上位８ビットと擬似的なノンスN_c’の値が書き込まれた５６ビットのビット連結からなる６４ビット全体をノンスN_cとして用いてコンテンツ鍵K_cの生成を行なう。この場合、不正コピー目的でＰＣＰ－ＣＣＩを改竄しても、ノンスN_cを改竄することとなり、結局はコンテンツを復号できなくなるので、セキュリティも維持される。

【０１０９】

一方、旧来通りの機器も、旧来の６４ビットのノンス情報フィールド全体に書き込まれた値をノンスN_cとして解釈する。この場合、上位８ビットにＰＣＰ－ＣＣＩが書き込まれることからＰＣＰ－ＣＣＩがストリームの途中で変化した場合にはノンスN_cの値の連続性が失われ、本発明に係る伝送方式に対応していないＳｉｎｋ機器にとって、いわゆるＬｅｇａｃｙ問題が発生する。また、本発明に係る伝送方式に対応したＳｉｎｋ機器においても、ＰＣＰすなわちコンテンツ伝送元であるＳｏｕｒｃｅ機器が本方式を適用しているかどうか、すなわち上位８ビットにＰＣＰ－ＣＣＩが記載されているかどうかを特定しなければならず、同様にＬｅｇａｃｙ問題が発生する。但し、この問題の解決方法については後述に譲る。

【０１１０】

図８には、ＰＣＰ－ＣＣＩフィールドのフォーマット構成例を示している。

【０１１１】

ＤＴＣＰでは、アナログ出力制御に関する２ビットのパラメータ（ＡＰＳ）や、出力時の画サイズに関する１ビットの情報フラグ（ＩＣＴ）といった出力制御情報がコピー制御情報の構成要素となっている。これらＥ－ＥＭＩには書ききれない情報がＰＣＰ－ＣＣＩ内に割り当てられている。また、Ｉｇｎｏｒｅビットは、下位５６ビットの擬似的なＮｃ’がカウントアップした結果、値が繰り上がってもＰＣＰ－ＣＣＩの他のフィールドに影響が出ないようにするためのフィールドである。Ｓｏｕｒｃｅ機器は、Ｉｇｎｏｒｅビットの初期値として“０”を設定し、擬似的なノンスN_c’がカウントアップした結果、値が繰り上がった場合に“１”となる。

【０１１２】

また、ＰＣＰ－ＣＣＩフィールドの有効性を記述した２ビットの情報フィールド“Ｍｏｄｅ”や、Ｅ－ＥＭＩと本来のＥｍｂｅｄｄｅｄ　ＣＣＩの代用可能性に関する１ビットの情報フラグ“ＳＥ（Ｓｕｂｓｔｉｔｕｔｅ　ｆｏｒ　Ｅｍｂｅｄｄｅｄ　ＣＣＩ）”も、ＰＣＰ－ＣＣＩ内に割り当てられている。このようなＰＣＰ－ＣＣＩをヘッダ部の一部として構成することにより、コンテンツのフォーマットに依存せずすべてのフォーマットに共通の形式でコピー制御情報を伝送することが可能になる。そして、暗号化ペイロードにＥｍｂｅｄｄｅｄ　ＣＣＩが含まれていない場合でも、従来はＥｍｂｅｄｄｅｄ　ＣＣＩとＥＭＩの組み合わせにより指定していたコピー制御機能、つまりにｃｏｇｎｉｚａｎｔ機能を実現することが可能である。

【０１１３】

Ｍｏｄｅビット・フィールドはＰＣＰ－ＣＣＩフィールドの意味若しくは有効性を表す。Ｍｏｄｅ＝００ｂのときはＰＣＰ－ＣＣＩフィールドが情報を持たないことを表す。また、Ｍｏｄｅ＝０１ｂのときはペイロードがＡｕｄｉｏ／Ｖｉｓｕａｌコンテンツであることを表し、Ｍｏｄｅ＝１０ｂのときはペイロードがＴｙｐｅ１ Ａｕｄｉｏコンテンツであることを表す（例えば、ＤＴＣＰ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｖｏｌｕｍｅ １（Ｉｎｆｏｒｍａｔｉｏｎａｌ Ｖｅｒｓｉｏｎ）, Ｒｅｖｉｓｉｏｎ１．４ Ａｐｐｅｎｄｉｘ Ａ Ａｄｄｉｔｉｏｎａｌ Ｒｕｌｅｓ ｆｏｒ Ａｕｄｉｏ Ａｐｐｌｉｃａｔｉｏｎｓを参照のこと）。Ｍｏｄｅ＝１１ｂはＲｅｓｅｒｖｅｄとする。また、Ｍｏｄｅ＝０１ｂ又はＭｏｄｅ＝１０ｂのときはＡＰＳ、ＩＣＴビットの意味を持ち、そのビットの意味はＤＴＣＰの規定（非特許文献５を参照のこと）に準ずる。

【０１１４】

図９には、Ｓｉｎｋ機器がＭｏｄｅビット・フィールドに基づいてＰＣＰ－ＣＣＩフィールドの意味を識別するための処理手順をフローチャートの形式で示している。

【０１１５】

Ｍｏｄｅ＝００ｂ、すなわちＰＣＰ－ＣＣＩフィールドが情報を持たない場合には（ステップＳ１のＹｅｓ）、さらに復号したコンテンツを検査する。そこで、Ｓｉｎｋ機器が識別可能なＥｍｂｅｄｄｅｄ ＣＣＩを検出できなければ（ステップＳ４のＮｏ）、Ｎｏｎ Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ１１）。一方、Ｅｍｂｅｄｄｅｄ ＣＣＩが検出できた場合には（ステップＳ４のＹｅｓ）、検出されたＥｍｂｅｄｄｅｄ ＣＣＩがＡｕｄｉｏ／Ｖｉｓｕａｌ用のＣＣＩかどうかを判別する（ステップＳ５）。そして、Ａｕｄｉｏ／Ｖｉｓｕａｌ用であれば、Ａｕｄｉｏ／Ｖｉｓｕａｌ Ｃｏｇｎｉｚａｎｔとして処理し（ステップＳ１０）、それ以外であればＡｕｄｉｏ Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ９）。

【０１１６】

また、Ｍｏｄｅ＝０１ｂすなわちＰＣＰ－ＣＣＩフィールドがＡｕｄｉｏ／Ｖｉｓｕａｌの情報であれば（ステップＳ２のＹｅｓ）、さらに復号したコンテンツを検査する。そこで、Ｓｉｎｋ機器が識別可能なＥｍｂｅｄｄｅｄ ＣＣＩを検出できなければ（ステップＳ６のＮｏ）、Ｎｏｎ Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ１１）。一方、Ｅｍｂｅｄｄｅｄ ＣＣＩを検出できた場合には、Ａｕｄｉｏ／Ｖｉｓｕａｌ Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ１０）。

【０１１７】

また、Ｍｏｄｅ＝１０ｂすなわちＰＣＰ－ＣＣＩフィールドがＡｕｄｉｏ Ｔｙｐｅ１の情報であれば（ステップＳ３のＹｅｓ）、さらに復号したコンテンツを検査する。Ｓｉｎｋ機器が識別可能なＥｍｂｅｄｄｅｄ ＣＣＩを検出できなければ（ステップＳ７のＮｏ）、Ｎｏｎ Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ１１）。一方、Ｅｍｂｅｄｄｅｄ ＣＣＩを検出できた場合には、Ａｕｄｉｏ Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ９）。

【０１１８】

また、Ｍｏｄｅが上記以外の値すなわち１１ｂのときは、Ｒｅｓｅｒｖｅｄとする（ステップＳ８）。

【０１１９】

図９には、Ｍｏｄｅビット・フィールドに基づいてＰＣＰ－ＣＣＩフィールドの意味を識別するための処理手順を示したが、その変形例として、Ｍｏｄｅビット・フィールドとＳＥビット・フラグの組み合わせに基づいてＰＣＰ－ＣＣＩフィールドの意味を識別することができる。図１０にはこの場合の処理手順をフローチャートの形式で示している。

【０１２０】

Ｍｏｄｅ＝００ｂ、すなわちＰＣＰ－ＣＣＩフィールドが情報を持たない場合には（ステップＳ２１のＹｅｓ）、さらに復号したコンテンツを検査する。そこで、Ｓｉｎｋ機器が識別可能なＥｍｂｅｄｄｅｄ ＣＣＩを検出できなければ（ステップＳ２４のＮｏ）、Ｎｏｎ Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ３１）。一方、Ｅｍｂｅｄｄｅ

ｄ　ＣＣＩが検出できた場合には（ステップＳ２４のＹｅｓ）、検出されたＥｍｂｅｄｄｅｄ　ＣＣＩがＡｕｄｉｏ／Ｖｉｓｕａｌ用のＣＣＩかどうかを判別する（ステップＳ２５）。そして、Ａｕｄｉｏ／Ｖｉｓｕａｌ用であれば、Ａｕｄｉｏ／Ｖｉｓｕａｌ　Ｃｏｇｎｉｚａｎｔとして処理し（ステップＳ３０）、それ以外であればＡｕｄｉｏ　Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ２９）。

【０１２１】

また、Ｍｏｄｅ＝０１ｂすなわちＰＣＰ－ＣＣＩフィールドがＡｕｄｉｏ／Ｖｉｓｕａｌの情報であれば（ステップＳ２２のＹｅｓ）、さらにＳＥビット・フラグをチェックする。ここで、ＳＥ＝１ｂであれば（ステップＳ３２のＹｅｓ）、Ａｕｄｉｏ／Ｖｉｓｕａｌ　Ｃｏｇｎｉｚａｎｔで処理するとともに、Ｅ－ＥＭＩでＥｍｂｅｄｄｅｄ　ＣＣＩを代用する（ステップＳ３４）。

【０１２２】

また、Ｍｏｄｅ＝０１ｂで（ステップＳ２２のＹｅｓ）、且つＳＥ＝１ｂでなければ（ステップＳ３２のＮｏ）、さらに復号したコンテンツを検査する。そこで、Ｓｉｎｋ機器が識別可能なＥｍｂｅｄｄｅｄ　ＣＣＩを検出できなければ（ステップＳ２６のＮｏ）、Ｎｏｎ　Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ３１）。一方、Ｅｍｂｅｄｄｅｄ　ＣＣＩを検出できた場合には、Ａｕｄｉｏ／Ｖｉｓｕａｌ　Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ３０）。

【０１２３】

また、Ｍｏｄｅ＝１０ｂすなわちＰＣＰ－ＣＣＩフィールドがＡｕｄｉｏ　Ｔｙｐｅ１の情報であれば（ステップＳ２３のＹｅｓ）、さらにＳＥビット・フラグをチェックする。ここで、ＳＥ＝１ｂであれば（ステップＳ３３のＹｅｓ）、Ａｕｄｉｏ　Ｃｏｇｎｉｚａｎｔで処理するとともに、Ｅ－ＥＭＩでＥｍｂｅｄｄｅｄ　ＣＣＩを代用する（ステップＳ３５）。

また、Ｍｏｄｅ＝１０ｂで（ステップＳ２３のＹｅｓ）、且つＳＥ＝１ｂでなければ（ステップＳ３３のＮｏ）、さらに復号したコンテンツを検査する。そして、Ｓｉｎｋ機器が識別可能なＥｍｂｅｄｄｅｄ　ＣＣＩを検出できなければ（ステップＳ２７のＮｏ）、Ｎｏｎ　Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ３１）。一方、Ｅｍｂｅｄｄｅｄ　ＣＣＩを検出できた場合には、Ａｕｄｉｏ　Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ２９）。

【０１２４】

また、Ｍｏｄｅ＝１０ｂで（ステップＳ２３のＹｅｓ）、且つＳＥ＝１ｂでなければ（ステップＳ３３のＮｏ）、さらに復号したコンテンツを検査する。そして、Ｓｉｎｋ機器が識別可能なＥｍｂｅｄｄｅｄ　ＣＣＩを検出できなければ（ステップＳ２７のＮｏ）、Ｎｏｎ　Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ３１）。一方、Ｅｍｂｅｄｄｅｄ　ＣＣＩを検出できた場合には、Ａｕｄｉｏ　Ｃｏｇｎｉｚａｎｔとして処理する（ステップＳ２９）。

【０１２５】

また、Ｍｏｄｅが上記以外の値すなわち１１ｂのときは、Ｒｅｓｅｒｖｅｄとする（ステップＳ２８）。

【０１２６】

また、ＳＥ＝１ｂのときはコンテンツにＥｍｂｅｄｄｅｄ　ＣＣＩが含まれておらず、Ｅ－ＥＭＩフィールドでＥｍｂｅｄｄｅｄ　ＣＣＩを代用することを表す。図１１には、Ｍｏｄｅビット・フィールド及びＳＥビット・フラグの値の組み合わせに基づいてＥ－ＥＭＩをＥｍｂｅｄｄｅｄ　ＣＣＩとして代用することが可能かどうかを判別するための処理手順をフローチャートの形式で示している。

【０１２７】

Ｍｏｄｅ＝００ｂであれば、ＰＣＰ－ＣＣＩフィールドが情報を持たず（ステップＳ４１のＹｅｓ）、Ｅ－ＥＭＩをＥｍｂｅｄｄｅｄ　ＣＣＩとして代用することができない（ステップＳ４６）。

【０１２８】
Ｍｏｄｅ＝０１ｂすなわちＰＣＰ－ＣＣＩフィールドがＡｕｄｉｏ／Ｖｉｓｕａｌ情報である場合（ステップＳ４２）、並びに、Ｍｏｄｅ＝１０ｂすなわちＰＣＰ－ＣＣＩフィールドがＡｕｄｉｏ情報である場合には（ステップＳ４３）、さらにＳＥビットのフラグ値を確認する（ステップＳ４４）。
【０１２９】
ここで、ＳＥフラグがセットされていれば、Ｅ－ＥＭＩをＥｍｂｅｄｄｅｄ　ＣＣＩとして代用できると判断する（ステップＳ４５）。また、ＳＥフラグがセットされていなければ、Ｅ－ＥＭＩをＥｍｂｅｄｄｅｄ　ＣＣＩとして代用できないと判断する（ステップＳ４６）。
【０１３０】
また、Ｍｏｄｅが上記以外の値すなわち１１ｂのときは、Ｒｅｓｅｒｖｅｄとする（ステップＳ４６）。
【０１３１】
Ｄ．Ｌｅｇａｃｙ問題の解決
上述した実施形態では、コピー制御情報をパケットのヘッダ部とペイロード部（すなわちコンテンツ・ストリーム）に分けて記載する方法が採用されている暗号化伝送方式において、ＰＣＰヘッダ内のノンス情報フィールドの上位８ビットを用いてＰＣＰ－ＣＣＩを記述し、残りの下位５６ビットに擬似的なノンスN_c’を書き込むようにすることで、（ＤＴＣＰ－ＩＰで）要求されるコピー制御を実現するために必要となるコピー制御情報をすべてヘッダ部に記載するようにした。この場合、ヘッダ部にはコンテンツのフォーマットに依存せず、すべてのフォーマットに共通の形式でコピー制御情報を挿入することができるので、コピー制御情報を作成し解析するためのソフトウェア又はハードウェアのモジュールをすべてのフォーマットで共通化することができ、機器コストを削減することができる。
【０１３２】
ところが、ＬｅｇａｃｙのＳｉｎｋ機器の場合、６４ビットのノンス情報フィールド全体に書き込まれた値をノンスN_cとして解釈することから、上位８ビットにＰＣＰ－ＣＣＩが書き込まれると、ＰＣＰ－ＣＣＩが変更されたときにノンスN_cの値の連続性が失われることになり、コンテンツ鍵確認手続を起動する、というＬｅｇａｃｙ問題が発生する。また、本発明に係る伝送方式に対応したＳｉｎｋ機器においても、コンテンツ伝送元であるＳｏｕｒｃｅ機器が本方式を適用しているかどうか、すなわちＰＣＰヘッダ中にＰＣＰ－ＣＣＩが記載されているかどうかを特定しなければならず、同様にＬｅｇａｃｙ問題が発生する。この項ではこれらのＬｅｇａｃｙ問題の解決方法について説明する。
【０１３３】
図１２には、ＬｅｇａｃｙのＳｏｕｒｃｅ機器とＳｉｎｋ機器間でＰＣＰを伝送する仕組みを図解している。
【０１３４】
Ｓｏｕｒｃｅ機器側では種鍵K_xを生成すると、ＡＫＥ手続を経てＳｉｎｋ機器との間で種鍵K_xを共有する。
【０１３５】
また、Ｓｏｕｒｃｅ機器は、上位層アプリケーションから伝送用のコンテンツが供給されると、Ｅ－ＥＭＩ設定部は、コンテンツ・ストリームに関連付けられたコピー制御情報に従って正しい暗号モードを選択し、これに基づいてＥ－ＥＭＩを設定する。また、常に１６バイトの倍数となるようにパディングを行ない、ＰＣＰデータ・バッファに一時格納する。
【０１３６】
コンテンツ鍵生成部は、種鍵K_xとＥ－ＥＭＩと、ノンス生成部が乱数生成などにより生成した６４ビット長のノンスN_cに所定の演算処理を施してコンテンツ鍵K_cを生成する。ノンス生成部は、定期的にノンスN_cを１ずつインクリメントするので、これに応じて

コンテンツ鍵K_cも定期的に更新されることになる。

【０１３７】

ＡＥＳ－ＣＢＣ（Ａｄｖａｎｃｅｓ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ－Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｎｇ）暗号化部は、ＰＣＰデータ・バッファからパディングされたＰＣＰペイロードを順次取り出し、現在のコンテンツ鍵K_cで暗号化処理を施す。

【０１３８】

ＰＣＰヘッダ付加部は、Ｅ－ＥＭＩ設定部で設定されたＥ－ＥＭＩを含んだＰＣＰヘッダを生成し、これを暗号化されたＰＣＰペイロードの先頭に取り付けてＰＣＰを完成する。このときのＰＣＰヘッダのデータ・フォーマットは図３１に示した通りである。そして、コンテンツ要求元としてのＳｉｎｋ機器から要求されるＨＴＴＰ又はＲＴＰなどのプロトコルに従ってＰＣＰを送出する。

【０１３９】

一方、Ｓｉｎｋ機器側では、Ｓｏｕｒｃｅ機器とのＡＫＥ手続を経て種鍵K_xを共有する。

【０１４０】

また、ＨＴＴＰ又はＲＴＰなどのプロトコルに従ってＳｏｕｒｃｅ機器からＰＣＰを受信すると、まずＰＣＰヘッダ抽出部がＰＣＰヘッダとＰＣＰペイロードに分離する。そして、ＰＣＰヘッダからはノンスN_cやＥ－ＥＭＩが取り出される。

【０１４１】

コンテンツ鍵生成部は、種鍵K_xとＰＣＰヘッダから取り出されたＥ－ＥＭＩとノンスN_cに所定の演算処理を施してコンテンツ鍵K_cを生成する。コンテンツ鍵確認部はノンスN_cの連続性を検査し、不連続を検出した場合はコンテンツ鍵確認手続を起動する。

【０１４２】

ＡＥＳ－ＣＢＣ暗号解読部は、ＰＣＰペイロードに対し、現在のコンテンツ鍵K_cで暗号解読処理を施す。解読後のＰＣＰペイロードはＰＣＰデータ・バッファに一時格納され、パディングされたデータを取り除いて、元のコンテンツが再現される。Ｅｍｂｅｄｄｅｄ ＣＣＩ検出部は、再現されたコンテンツを検査し、Ｅｍｂｅｄｄｅｄ ＣＣＩを検出する。

【０１４３】

また、図１３には、ＰＣＰ－ＣＣＩをＰＣＰヘッダに埋め込む伝送方式を適用したＳｏｕｒｃｅ機器とＳｉｎｋ機器間でＰＣＰを伝送する仕組みを図解している。

【０１４４】

Ｓｏｕｒｃｅ機器側では種鍵K_xを生成すると、ＡＫＥ手続を経てＳｉｎｋ機器との間で種鍵K_xを共有する。

【０１４５】

また、Ｓｏｕｒｃｅ機器は、上位層アプリケーションから伝送用のコンテンツが供給されると、Ｅ－ＥＭＩ／ＰＣＰ－ＣＣＩ設定部は、コンテンツ・ストリームに関連付けられたコピー制御情報に従って正しい暗号モードを選択し、これに基づいてＥ－ＥＭＩを設定し、さらにＰＣＰ－ＣＣＩを設定する（ＰＣＰ－ＣＣＩ中のＭｏｄｅビット・フィールド並びにＳＥビット・フラグの設定方法については非特許文献５を参照されたい）。ＰＣＰ－ＣＣＩは８ビット長であり、そのデータ・フォーマットは図８に示した通りである。また、常に１６バイトの倍数となるようにパディングを行ない、ＰＣＰデータ・バッファに一時格納する。

【０１４６】

擬似ノンスN_c’生成部は、乱数生成などにより５６ビット長の擬似的なノンスN_c’を生成する。ノンスN_c生成部は、擬似ノンスN_c’の上位にＰＣＰ－ＣＣＩをビット連結して、６４ビット長のノンスN_cを作成する。

【０１４７】

コンテンツ鍵生成部は、種鍵K_xとＥ－ＥＭＩと、ノンス生成部が作成した６４ビット

長のノンスN_cに所定の演算処理を施してコンテンツ鍵K_cを生成する。ノンスN_c生成部は、定期的にノンスN_cを１ずつインクリメントするので、これに応じてコンテンツ鍵K_cも定期的に更新されることになる。但し、ＰＣＰ－ＣＣＩ情報が変化すると、擬似的なノンスN_c’部分は連続的であっても、６４ビット全体で扱われるノンスN_cの連続性は失われる。

【０１４８】

ＡＥＳ－ＣＢＣ暗号化部は、ＰＣＰデータ・バッファからパディングされたＰＣＰペイロードを順次取り出し、現在のコンテンツ鍵K_cで暗号化処理を施す。

【０１４９】

ＰＣＰヘッダ付加部は、Ｅ－ＥＭＩ設定部で設定されたＥ－ＥＭＩを含んだＰＣＰヘッダを生成し、これを暗号化されたＰＣＰペイロードの先頭に取り付けてＰＣＰを完成する。このときのＰＣＰヘッダのデータ・フォーマットは図７に示した通りである。そして、コンテンツ要求元としてのＳｉｎｋ機器から要求されるＨＴＴＰ又はＲＴＰなどのプロトコルに従ってＰＣＰを送出する。

【０１５０】

一方、Ｓｉｎｋ機器側では、Ｓｏｕｒｃｅ機器とのＡＫＥ手続を経て種鍵K_xを共有する。

【０１５１】

また、ＨＴＴＰ又はＲＴＰなどのプロトコルに従ってＳｏｕｒｃｅ機器からＰＣＰを受信すると、まずＰＣＰヘッダ抽出部がＰＣＰヘッダとＰＣＰペイロードに分離する。そして、ＰＣＰヘッダからはノンスN_cやＥ－ＥＭＩ及びＰＣＰ－ＣＣＩが取り出される。

【０１５２】

ノンスN_c取得部は、ＰＣＰヘッダ中の６４ビット長のノンス情報を取得する。コンテンツ鍵確認部は、ノンスN_cの下位５６ビットの連続性を検査し、不連続を検出した場合はコンテンツ鍵確認手続を起動する。

【０１５３】

コンテンツ鍵生成部は、種鍵K_xとＰＣＰヘッダから取り出された６４ビット長のノンスN_cに所定の演算処理を施してコンテンツ鍵K_cを生成する。

【０１５４】

また、ＰＣＰ－ＣＣＩ取得部は、ノンスN_c取得部から６４ビット長のノンス情報フィールドのうち上位８ビットをＰＣＰ－ＣＣＩとして取得する。そして、ＰＣＰ－ＣＣＩ中のＭｏｄｅビット・フィールド並びにＳＥビット・フラグのビット値及びＥｍｂｅｄｄｅｄ　ＣＣＩ検出部の検出結果に基づいて、図１０に示した手順に従い、コンテンツ・フォーマットの認識（Ｃｏｇｎｉｚａｎｔ）並びにＥ－ＥＭＩのＥｍｂｅｄｄｅｄ　ＣＣＩ代用性を決定する。

【０１５５】

ＡＥＳ－ＣＢＣ暗号解読部は、ＰＣＰペイロードに対し、現在のコンテンツ鍵K_cで暗号解読処理を施す。解読後のＰＣＰペイロードはＰＣＰデータ・バッファに一時格納され、パディングされたデータを取り除いて、元のコンテンツが再現される。Ｅｍｂｅｄｄｅｄ　ＣＣＩ検出部は、再現されたコンテンツを検査し、Ｅｍｂｅｄｄｅｄ　ＣＣＩを検出する。

【０１５６】

ここで、ＰＣＰ－ＣＣＩは平文の状態でＰＣＰヘッダに記述されることから、ＰＣＰペイロードに埋め込んで暗号化する場合に比べると改竄が容易になる。しかしながら、ＰＣＰ－ＣＣＩはノンスN_cの上位８ビットを構成することから、これを改竄することは、ノンスN_cすなわちコンテンツ鍵K_cをも改竄することとなり、結局はコンテンツを復号できなくなるので、セキュリティも維持される。

【０１５７】

図１４には、図１２に示したＬｅｇａｃｙのＳｏｕｒｃｅ及びＳｉｎｋ機器と、図１３に示した新方式のＳｏｕｒｃｅ及びＳｉｎｋ機器が混在するコンテンツ伝送環境下におい

てＬｅｇａｃｙ問題が発生する様子を模式的に示している。

【０１５８】

図１２に示したＳｏｕｒｃｅ及びＳｉｎｋ機器間でのＰＣＰの伝送、並びに図１３に示したＳｏｕｒｃｅ及びＳｉｎｋ機器間でのＰＣＰの伝送は問題なく処理されることは上述した通りである。

【０１５９】

これに対し、新方式のＳｏｕｒｃｅ機器が送出するＰＣＰヘッダにＰＣＰ－ＣＣＩを埋め込んだＰＣＰ（Ｎｅｗ　ＰＣＰ　ｗｉｔｈ　ＰＣＰ－ＣＣＩ）をＬｅｇａｃｙのＳｉｎｋ機器が受信したとき、上位８ビットにＰＣＰ－ＣＣＩが書き込まれることによりノンスＮｃの値の連続性が失われるので（例えばＰＣＰ－ＣＣＩ情報が変化したとき）、コンテンツ鍵確認手続を起動する、という第１のＬｅｇａｃｙ問題が発生する。

【０１６０】

また、ＰＣＰヘッダにＰＣＰ－ＣＣＩを埋め込んだＰＣＰ（Ｎｅｗ　ＰＣＰ　ｗｉｔｈ　ＰＣＰ－ＣＣＩ）に対応したＳｉｎｋ機器の場合、コンテンツの要求先であるＳｏｕｒｃｅ機器がＬｅｇａｃｙ又は新方式のいずれであるかを正しく識別しなければならないという第２のＬｅｇａｃｙ問題が発生する。識別を誤ると、ＰＣＰヘッダに埋め込まれているＰＣＰ－ＣＣＩを読み取ることができない、あるいは６４ビットのノンス情報フィールドの上位８ビットを誤ってＰＣＰ－ＣＣＩと認識してしまうことになる。

【０１６１】

第１のＬｅｇａｃｙ問題に関しては、コンテンツ鍵確認手続は起動されるが、Ｓｏｕｒｃｅ機器側では、コンテンツ鍵確認要求に対し、ノンスN_cに異常がないことを示すレスポンス（ＡＣＣＥＰＴＥＤコマンド）を返すので、ＬｅｇａｃｙのＳｉｎｋ機器は以降も障害なくコンテンツ受信処理を継続することができ、実用上の問題は発生しない。

【０１６２】

ＤＴＣＰ－ＩＰ　Ｖｏｌｕｍｅ　１　Ｓｕｐｐｌｅｍｅｎｔ　ＳｅｃｔｉｏｎＶ１ＳＥ．８．６には、Ｃｏｎｔｅｎｔ　Ｋｅｙ　Ｃｏｎｆｉｒｍａｔｉｏｎについて規定している。これによれば、Ｓｉｎｋ機器は、コンテンツ・ストリーム毎に、最も新しく受信したＰＣＰのノンスN_cの値を確認し、さらに動的に変更される後続のノンスについても２分間隔で再確認しなければならない（但し、Ｓｉｎｋ機器がノンスを初期確認した後に後続のノンスN_cの値が単調に増大する連続的な数値であることを監視し確認する場合には、周期的なコンテンツ鍵確認の手続きを省略することができる）。Ｓｉｎｋ機器は、ＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦ　ｓｕｂｆｕｎｃｔｉｏｎを用いて、現在のノンスN_cに関連付けられたコンテンツ鍵の確認を行なうことができる。

【０１６３】

各コンテンツ・ストリームにおいて、Ｓｉｎｋ機器は、未確認の初期ノンスを取得すると、当該コンテンツ・ストリームに関して暗号化コンテンツの復号を終了しなければならなくなる前に、コンテンツ鍵の確認を再試行する猶予期間が１分間だけ与えられる。そして、Ｓｉｎｋ機器は、この猶予期間を利用してノンスN_cの確認に成功すると、暗号化コンテンツの復号動作を終了することなく継続することができる。

【０１６４】

図１５には、コンテンツ鍵確認のためのＳｉｎｋ機器とＳｏｕｒｃｅ機器間の手続きを示している。但し、Ｒは６４ビット値で、初期は乱数であるが、後続の試行では$1 \mod 2^{64}$でインクリメントするとともに、以下の通りとする。

【０１６５】

$MX = SHA1(K_x || K_x)$

$MAC3A = MAC3B = [SHA1(MX + N_c T + R)]msb80$

$MAC4A = MAC4B = [SHA1(MX + N^c T + R)]lsb80$

（上式で、“＋”は$\mod 2^{160}$の加算を意味するために使用される。）

【０１６６】

図示のコンテンツ確認手続きでは、Ｓｉｎｋ機器は、ＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦコマ

ンドにおいて、検査用のノンスN_cTをＳｏｕｒｃｅ機器に送る。

【０１６７】

Ｓｏｕｒｃｅ機器側では、ＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦコマンドを受信すると、検査用のノンスN_cTを取り出して、現在のノンスN_cと比較する。そして、現在のノンスN_cがN_cTとN_cＴ＋５の範囲にあるときには検査用のノンスN_cTが有効であることを確認する。検査用のノンスN_cTが有効であることを確認できたときには、さらにＭＡＣ３ＡとＭＡＣ３Ｂが等しいかどうかに基づいてコンテンツ鍵の確認を行なう。そして、コンテンツ鍵が正しかったことを示すＡＣＣＥＰＴＥＤレスポンス、又は正しくなかったことを示すＲＥＪＥＣＴＥＤレスポンスのいずれかをＳｉｎｋ機器に返す。

【０１６８】

Ｓｉｎｋ機器側では、Ｓｏｕｒｃｅ機器からＡＣＣＥＰＴＥＤレスポンスが返されたときには、さらにＭＡＣ４ＡとＭＡＣ４Ｂが等しいかどうかに基づいてコンテンツ鍵の確認を行なう。そして、Ｓｉｎｋ機器自身でコンテンツ鍵が正しいことを確認できた場合にはＳｉｎｋ機器はｃｏｎｆｉｒｍｅｄ状態になる。

【０１６９】

一方、Ｓｏｕｒｃｅ機器からＡＣＣＥＰＴＥＤレスポンスが返されたがＳｉｎｋ機器自身でのコンテンツ鍵確認に失敗した場合や、Ｓｏｕｒｃｅ機器からＲＥＪＥＣＴＥＤレスポンスが返されたときには、Ｓｉｎｋ機器はｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎ状態になる。

【０１７０】

ここで、ｃｏｎｆｉｒｍｅｄはＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦによりコンテンツ鍵が正しいことが確認された状態、ｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎはＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦによりコンテンツ鍵が不正であることが確認された状態であり、いずれもＤＴＣＰ Ｖｏｌｕｍｅ １ Ｓｕｐｐｌｅｍｅｎｔ Ｅ ＳｅｃｔｉｏｎＶ１ＳＥ８．６に規定されている。

【０１７１】

ｃｏｎｆｉｒｍｅｄ状態では、Ｓｉｎｋ機器は受信コンテンツの復号処理を継続して行なうことができる。他方、ｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎ状態では、Ｓｉｎｋ機器は復号処理を継続できない。

【０１７２】

図１６には、ＰＣＰ－ＣＣＩに対応したＳｏｕｒｃｅ機器がＬｅｇａｃｙのＳｉｎｋ機器との間でコンテンツ鍵確認手続きを行なうための処理手順をフローチャートの形式で示している。

【０１７３】

Ｓｏｕｒｃｅ機器は、コンテンツ伝送先となるＳｉｎｋ機器からコンテンツ確認を要求するＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦコマンドを受信すると（ステップＳ５１）、コンテンツ鍵の確認を行なう（ステップＳ５２）。具体的には、当該コマンドから検査用のノンスN_cTを取り出して、現在のノンスN_c、すなわち８ビット長のＰＣＰ－ＣＣＩと５６ビット長の擬似的なノンスN_c’をビット連結した値と比較する。そして、現在のノンスN_cがN_cTとN_cＴ＋５の範囲にあるときには検査用のノンスN_cTが有効であることを確認する。

【０１７４】

そして、Ｓｏｕｒｃｅ機器は、コンテンツ鍵が正しいことを確認した場合には その旨を示すＡＣＣＥＰＴＥＤレスポンスをＳｉｎｋ機器に返信するが（ステップＳ５３）、コンテンツ鍵が不正であることを確認した場合にはその旨を示すＲＥＪＥＣＴＥＤレスポンスを返信する（ステップＳ５４）。

【０１７５】

なお、ＡＣＣＥＰＴＥＤ並びにＲＥＪＥＣＴＥＤはともにＤＴＣＰ Ｖｏｌｕｍｅ １ Ｓｕｐｐｌｅｍｅｎｔ Ｅ ＳｅｃｔｉｏｎＶ１ＳＥ８．６に規定されている、コマンドに対するレスポンスである。

【０１７６】
また、図１７には、ＬｅｇａｃｙのＳｉｎｋ機器がＰＣＰ－ＣＣＩに対応したＳｏｕｒｃｅ機器との間でコンテンツ鍵確認手続きを行なうための処理手順をフローチャートの形式で示している。
【０１７７】
Ｓｉｎｋ機器は、コンテンツ要求先となるＳｏｕｒｃｅ機器に対しＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦコマンドを送信した後（ステップＳ６１）、当該Ｓｏｕｒｃｅ機器からのレスポンス受信を待機する（ステップＳ６２）。
【０１７８】
ここで、Ｓｏｕｒｃｅ機器からＡＣＣＥＰＴＥＤレスポンスを受信したときには（ステップＳ６３）、コンテンツ鍵を確認する（ステップＳ６４）。このとき、コンテンツ鍵が正しい場合にはｃｏｎｆｉｒｍｅｄ（ステップＳ６５）、コンテンツ鍵が不正である場合にはｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎである（ステップＳ６７）。また、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器からＲＥＪＥＣＴＥＤレスポンスを受信したときには（ステップＳ６６）、ｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎである（ステップＳ６７）。
【０１７９】
ここで、ｃｏｎｆｉｒｍｅｄはＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦによりコンテンツ鍵が正しいことが確認された状態、ｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎはＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦによりコンテンツ鍵が不正であることが確認された状態であり、いずれもＤＴＣＰ Ｖｏｌｕｍｅ １ Ｓｕｐｐｌｅｍｅｎｔ Ｅ ＳｅｃｔｉｏｎＶ１ＳＥ８．６に規定されている。
【０１８０】
ｃｏｎｆｉｒｍｅｄでは、Ｓｉｎｋ機器は受信コンテンツの復号処理を継続して行なうことができる。本実施形態では、Ｓｏｕｒｃｅ機器は、検査用のノンスN_cＴを、８ビット長のＰＣＰ－ＣＣＩと５６ビット長の擬似的なノンスN_c’をビット連結した現在のノンスN_cと比較するので、Ｓｉｎｋ機器から見るとノンスの変化が不自然であっても、ｃｏｎｆｉｒｍｅｄである限り、コンテンツの受信及びその暗号解読を継続することができる。他方、ｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎでは、Ｓｉｎｋ機器は復号処理を継続できない。
【０１８１】
また、Ｓｉｎｋ機器は、最初のｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎとなってから１分間は復号処理を継続しながらコンテンツ鍵確認手続きを繰り返すことができるので（ステップＳ６８）、ステップＳ４１に戻り（ステップＳ７０）、ＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦコマンドを再発行する。

【０１８２】
コンテンツ鍵確認手続きを再試行して、１分以内にｃｏｎｆｉｒｍｅｄとなれば（ステップＳ６５）、受信コンテンツの復号処理を継続することができる。しかし、１分間ｎｏｎ－ｃｏｎｆｉｒｍａｔｉｏｎが継続した場合には（ステップＳ６８）、受信コンテンツの復号処理を停止しなければならない（ステップＳ６９）。
【０１８３】
図１８には、ＰＣＰ－ＣＣＩに対応したＳｏｕｒｃｅ機器（Ｎｅｗ Ｓｏｕｒｃｅ）とＬｅｇａｃｙ Ｓｉｎｋの間で行なわれるコンテンツ鍵確認手続の動作シーケンスをまとめている。
【０１８４】
Ｎｅｗ Ｓｏｕｒｃｅ側で、コンテンツの伝送中にＰＣＰ－ＣＣＩを変更すると、これに伴ってＰＣＰヘッダに書き込まれるノンスN_cの連続性が失われる。Ｌｅｇａｃｙ ＳｉｎｋはこのようなノンスN_cのＪｕｍｐを認識すると、コンテンツ鍵確認用のＴＣＰコネクションを確立し、Ｎｅｗ Ｓｏｕｒｃｅに対しＣＯＮＴ＿ＫＥＹ＿ＣＯＮＦコマンドを発行する。

【０１８５】
New Source側では、CONT_KEY_CONFコマンドからノンスN_cTを取り出すと、更新後のＰＣＰ－ＣＣＩと現在の擬似的なノンスN_c'をビット連結したノンスN_cと比較する。そして、ノンスN_cの改竄でないことを確認すると、Ｌｅｇａｃｙ Ｓｉｎｋに対しＡＣＣＥＰＴＥＤレスポンスを返すとともに、継続してコンテンツを伝送する。これによって、Ｌｅｇａｃｙ Ｓｉｎｋは、コンテンツを継続して受信し解読処理を行なうことができる。
【０１８６】
また、第２のＬｅｇａｃｙ問題に関しては、相互認証手続（ＡＫＥ）で交換する機器証明書の中にＰＣＰヘッダ部に超拡張コピー制御情報を埋め込むことを示すＣＣＩフラグを含めることによって、Ｓｉｎｋ機器はＳｏｕｒｃｅ機器がＬｅｇａｃｙ機器でないことを認識することができる。あるいは、このようなＣＣＩフラグを応答する能力確認用のコマンドを使用するようにしてもよい。
【０１８７】
ＰＣＰ－ＣＣＩに対応した新規のＤＴＣＰ機器は、例えばＣＣＩフラグを１に設定された機器証明書を使用する。このＣＣＩフラグは機器証明書内の予備（ｒｅｓｅｒｖｅｄ）領域を使用することができる。Ｓｉｎｋ機器は、ＡＫＥ手続きなどにおいて、Ｓｏｕｒｃｅ機器の機器証明書をチェックして、ＰＣＰ－ＣＣＩフィールドがＰＣＰヘッダに存在するかどうかを安全に確認することができる。
【０１８８】
この場合、ＰＣＰ－ＣＣＩに対応したＳｏｕｒｃｅ機器は、ＰＣＰヘッダにＰＣＰ－ＣＣＩフィールドを埋め込んだ新しいフォーマットで、ＰＣＰパケットを常に送ることができる。一方、ＰＣＰ－ＣＣＩに対応したＳｉｎｋ機器は、新規のＳｏｕｒｃｅ機器からコンテンツ・ストリームが到来したときには、そのＰＣＰヘッダに含まれるＰＣＰ－ＣＣＩフィールドを使用することができる。
【０１８９】
図１９には、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器のＣＣＩフラグをチェックしてＰＣＰヘッダ部のコピー制御情報を処理するための手順をフローチャートの形式で示している。
【０１９０】
Ｓｉｎｋ機器は、Ｓｏｕｒｃｅ機器との間でコンテンツ伝送手続きの開始前にコンテンツ鍵交換及び認証手続（ＡＫＥ）を行なう際に、当該Ｓｏｕｒｃｅ機器はＰＣＰ－ＣＣＩをヘッダ部に埋め込んで送るかどうかを示す、ＣＣＩフラグの確認処理を実行する（Ｓ７１）。同確認処理を実施する方法として数通りが考えられるが、詳細は後述に譲る。
【０１９１】
そして、ＣＣＩフラグを確認できたかどうかをチェックする（ステップＳ７２）。確認できた場合には、コンテンツ伝送手続を開始し、Ｓｏｕｒｃｅ機器からコンテンツ・ストリームをＰＣＰとして受け取ったときに、ＰＣＰヘッダ中の６４ビット長のノンス情報フィールドのうち上位８ビットをＰＣＰ－ＣＣＩとして参照する（ステップＳ７３）。また、確認できなかった場合は、ノンス情報フィールドの上位８ビットをＰＣＰ－ＣＣＩとして参照しない（ステップＳ７４）。
【０１９２】
ステップＳ７１において確認処理を行なう方法、すなわちＳｏｕｒｃｅ機器がＰＣＰヘッダにＰＣＰ－ＣＣＩを埋め込んでいることを識別する具体的な１つの方法として、機器証明書の中にＣＣＩフラグを含めることが挙げられる。
【０１９３】
この機器証明書は、例えばＤＴＬＡのように信頼のおけるライセンス・オーソリティによる電子署名が付加されているものとする。また、証明書の中にはその送信装置の公開鍵が含まれることで、チャレンジ・アンド・レスポンス型の認証手続きにおいて、送信側が自身の署名を付加したレスポンス（受信側からのチャレンジ・データを含む）を受信側に送り、受信側に対して自身の証明書が正当なものであることを示すことができる。

【０１９４】
図２０には、機器証明書内にＣＣＩフラグを埋め込むことによって、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示している。
【０１９５】
まず、コンテンツ要求元であるＳｉｎｋ機器から、Ｒｘ乱数とＲｘ証明書を含んだＲｘチャレンジが送信される。これに対し、Ｓｏｕｒｃｅ機器からは、Ｔｘ乱数及びＴｘ証明書を含んだＴｘチャレンジが返信される。このＴｘ証明書には、例えば予備領域の１ビットを使用して、ＣＣＩフラグがセットされている。Ｓｉｎｋ機器は、このＣＣＩフラグをチェックして、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩに対応していることを確認する。
【０１９６】
以降、Ｓｏｕｒｃｅ機器から、Ｒｘ乱数、Ｔｘメッセージ、Ｔｘ署名を含んだＲｘレスポンスが送信されるとともに、Ｓｉｎｋ機器からはＴｘ乱数、Ｒｘメッセージ、Ｒｘ署名を含んだＴｘレスポンスが送信され、通常のチャレンジ・アンド・レスポンス認証手続きが続く。
【０１９７】
図２１には、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器から受信したＴｘチャレンジに含まれる機器証明書からＣＣＩフラグを検証するための処理手順をフローチャートの形式で示している。
【０１９８】
Ｓｉｎｋ機器は、Ｓｏｕｒｃｅ機器からＴｘチャレンジを受信すると（ステップＳ８１）、これに含まれている機器証明書の署名を検証する（ステップＳ８２）。そして、検証に成功したときには（ステップＳ８３）、当該証明書中のＣＣＩフラグの値を参照する（ステップＳ８４）。また、検証に失敗したときには、フラグ値のチェックを行なうことなく、認証エラーを返す（ステップＳ８５）。
【０１９９】
また、ステップＳ７１において、Ｓｏｕｒｃｅ機器がＰＣＰヘッダにＰＣＰ－ＣＣＩを埋め込んでいることを識別する他の方法として、Ｓｏｕｒｃｅ機器が自身の署名を付加して送るレスポンスの中にＣＣＩフラグを埋め込むことが挙げられる。
【０２００】
図２２には、機器が自身の署名を付加して送るレスポンスの中にＣＣＩフラグを埋め込むことによって、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示している。
【０２０１】
まず、コンテンツ要求元であるＳｉｎｋ機器から、Ｒｘ乱数とＲｘ証明書を含んだＲｘチャレンジが送信される。これに対し、Ｓｏｕｒｃｅ機器からは、Ｔｘ乱数及びＴｘ証明書を含んだＴｘチャレンジが返信される。
【０２０２】
続いて、Ｓｏｕｒｃｅ機器から、Ｒｘ乱数、Ｔｘメッセージ、Ｔｘ署名を含んだＲｘレスポンスが送信される。ここで、Ｔｘメッセージには、ＣＣＩフラグが含まれている。Ｓｉｎｋ機器は、このＣＣＩフラグをチェックして、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩに対応していることを確認する。そして、Ｓｉｎｋ機器からはＴｘ乱数、Ｒｘメッセージ、Ｒｘ署名を含んだＴｘレスポンスが送信され、通常のチャレンジ・アンド・レスポンス認証手続きが続く。
【０２０３】
図２３には、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器から受信したＲｘレスポンスに含まれるＴｘメッセージからＣＣＩフラグを検証するための処理手順をフローチャートの形式で示している。
【０２０４】
Ｓｉｎｋ機器は、Ｓｏｕｒｃｅ機器からＲｘレスポンスを受信すると（ステップＳ９１

）、Ｒｘ乱数とＴｘメッセージ対するＴｘ署名を検証する（ステップＳ９２）。そして、検証に成功したときには（ステップＳ９３）、当該Ｔｘメッセージ中のＣＣＩフラグの値を参照する（ステップＳ９４）。また、検証に失敗したときには、フラグ値のチェックを行なうことなく、認証エラーを返す（ステップＳ９５）。

【０２０５】

例えば、Ｔｘメッセージ中の予備領域の１ビットを使用して、ＣＣＩフラグを埋め込むことができる。但し、Ｒｘレスポンス中にＣＣＩフラグを挿入する場所がもはや残されていない場合には、新規のＲｘレスポンス用のコマンドを定義すればよい。

【０２０６】

また、ＬｅｇａｃｙのＳｉｎｋ機器は新規のＲｘレスポンス用のコマンドに対応することができないという問題がある。このため、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し新規のＲｘレスポンスを求めるための、新規のＲｘチャレンジ用のコマンドをさらに定義するようにしてもよい。

【０２０７】

図２４には、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し新規のＲｘチャレンジを送信し、これに対しＳｏｕｒｃｅ機器がＣＣＩフラグを埋め込んだ新規のＲｘレスポンスを返し、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示している。

【０２０８】

まず、コンテンツ要求元であるＳｉｎｋ機器から、Ｓｏｕｒｃｅ機器に対し新規のＲｘレスポンスを求めるための、新規のＲｘチャレンジ用コマンドが送信される。このＲｘチャレンジ用のコマンドには、Ｒｘ乱数とＲｘ証明書が含まれている（同上）。これに対し、Ｓｏｕｒｃｅ機器からは、Ｔｘ乱数及びＴｘ証明書を含んだＴｘチャレンジが返信される。

【０２０９】

続いて、Ｓｏｕｒｃｅ機器から、Ｒｘ乱数、Ｔｘメッセージ、Ｔｘ署名を含んだ新規のＲｘレスポンス用コマンドが送信される。ここで、Ｔｘメッセージには、ＣＣＩフラグが含まれている。Ｓｉｎｋ機器は、このＣＣＩフラグをチェックして、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩに対応していることを確認する。そして、Ｓｉｎｋ機器からはＴｘ乱数、Ｒｘメッセージ、Ｒｘ署名を含んだＴｘレスポンスが送信され、通常のチャレンジ・アンド・レスポンス認証手続きが続く。

【０２１０】

図２５は、Ｓｏｕｒｃｅ機器が、図２４に示した動作に対応したチャレンジ・アンド・レスポンス動作を行なうための処理手順をフローチャートの形式で示している。

【０２１１】

Ｓｏｕｒｃｅ機器は、Ｓｉｎｋ機器からＲｘチャレンジを受信すると（ステップＳ１０１）、これが従来通りのＲｘチャレンジ、又はＣＣＩフラグを埋め込んだ新規のＲｘレスポンスを求める新規のＲｘチャレンジのいずれであるかを判別する（ステップＳ１０２）。

【０２１２】

そして、従来通りのＲｘチャレンジを受信したときには、以降は従来通りの認証手順を実施するが（ステップＳ１０３）、新規のＲｘチャレンジを受信したときには、図２４に示した認証手順を実施して（ステップＳ１０４）、Ｓｉｎｋ機器に対し自己がＰＣＰ－ＣＣＩに対応していることを示す。

【０２１３】

また、図２６には、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器から受信した新規のＲｘレスポンスに含まれるＴｘメッセージからＣＣＩフラグを検証するための処理手順をフローチャートの形式で示している。

【０２１４】

Ｓｉｎｋ機器は、Ｓｏｕｒｃｅ機器から新規のＲｘレスポンスを受信すると（ステップ

Ｓ１１１）、Ｒｘ乱数とＴｘメッセージ対するＴｘ署名を検証する（ステップ１１９２）。そして、検証に成功したときには（ステップＳ１１３）、当該Ｔｘメッセージ中のＣＣＩフラグの値を参照する（ステップＳ１１４）。また、検証に失敗したときには、フラグ値のチェックを行なうことなく、認証エラーを返す（ステップＳ１１５）。

【０２１５】

また、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し新規のＲｘレスポンスを求める他の方法として、能力確認用のコマンドを新たに定義することが挙げられる。

【０２１６】

図２７には、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し能力確認コマンドを送信し、これに対しＳｏｕｒｃｅ機器がＣＣＩフラグを埋め込んだ能力確認レスポンスを返し、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示している。

【０２１７】

まず、コンテンツ要求元であるＳｉｎｋ機器から、Ｓｏｕｒｃｅ機器に対し能力確認コマンドが送信される。これに対し、Ｓｏｕｒｃｅ機器からは、能力確認レスポンスが返信される。このレスポンスには、ＣＣＩフラグがセットされている。

【０２１８】

続いて、コンテンツ要求元であるＳｉｎｋ機器から、Ｓｏｕｒｃｅ機器に対し新規のＲｘレスポンスを求めるための、新規のＲｘチャレンジ用コマンドが送信される。このＲｘチャレンジ用のコマンドには、Ｒｘ乱数とＲｘ証明書が含まれている（同上）。これに対し、Ｓｏｕｒｃｅ機器からは、Ｔｘ乱数及びＴｘ証明書を含んだＴｘチャレンジが返信される。

【０２１９】

続いて、Ｓｏｕｒｃｅ機器から、Ｒｘ乱数、Ｔｘメッセージ、Ｔｘ署名を含んだ新規のＲｘレスポンス用コマンドが送信される。ここで、Ｔｘメッセージには、ＣＣＩフラグがセットされている。Ｓｉｎｋ機器は、このＣＣＩフラグをチェックして、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩに対応していることを確認する。そして、Ｓｉｎｋ機器からはＴｘ乱数、Ｒｘメッセージ、Ｒｘ署名を含んだＴｘレスポンスが送信され、通常のチャレンジ・アンド・レスポンス認証手続きが続く。

【０２２０】

図２８は、Ｓｉｎｋ機器が、図２７に示した動作に対応したチャレンジ・アンド・レスポンス動作を行なうための処理手順をフローチャートの形式で示している。

【０２２１】

Ｓｉｎｋ機器は、Ｓｏｕｒｃｅ機器に対してＣＣＩフラグを埋め込んだ新規のＲｘレスポンスを要求する際には、まず能力確認コマンドを送信する（ステップＳ１２１）。

【０２２２】

そして、Ｓｏｕｒｃｅ機器から能力確認レスポンスが返されると、その中にＣＣＩフラグがセットされているかどうかをチェックする（ステップＳ１２２）。

【０２２３】

そして、ＣＣＩフラグが設定されていないときには、以降は従来通りの認証手順を実施するが（ステップＳ１２３）、ＣＣＩフラグが設定されているときには、図２７に示した認証手順を実施して（ステップＳ１２４）、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩに対応していることを確認する。新規の認証手続きは図２６に示した処理手順に従うので、ここでは説明を省略する。

【０２２４】

なお、Ｓｉｎｋ機器から能力確認コマンドを送信したのに対し、Ｓｏｕｒｃｅ機器が当該コマンドに対応していない場合には、“ｎｏｔ　ｉｍｐｌｅｍｅｎｔｅｄ”コマンドが返されるので、Ｓｉｎｋ機器はＳｏｕｒｃｅ機器がＬｅｇａｃｙであることを識別できる。

【０２２５】

また、能力確認用のコマンドを新たに定義して新規のＲｘレスポンスを求める場合の変形例として、最初の能力確認コマンドとその応答にチャレンジ・アンド・レスポンス処理を組み込み、その動作シーケンス中にＣＣＩフラグをセキュアに送ることも考えられる。この場合、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し能力確認コマンドを送信し、これに対しＳｏｕｒｃｅ機器がＣＣＩフラグを埋め込んだ署名付きの能力確認レスポンスを返し、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示すことができる。そして、引き続く認証処理は常に従来通りの手順となる。

【０２２６】

図２９には、最初の能力確認コマンドとその応答にチャレンジ・アンド・レスポンス処理を組み込んだ場合に、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示している。

【０２２７】

まず、コンテンツ要求元であるＳｉｎｋ機器から、Ｓｏｕｒｃｅ機器に対し能力確認コマンドが送信される。この能力確認コマンドには、チャレンジ・アンド・レスポンス用のＲｘ乱数２が含まれている。これに対し、Ｓｏｕｒｃｅ機器からは、能力確認レスポンスが返信される。この能力確認レスポンスには、Ｒｘ乱数２と、Ｔｘメッセージ２と、Ｔｘ署名２が含まれている。そして、Ｔｘメッセージ２にはＣＣＩフラグがセットされている。Ｓｉｎｋ機器は、このＣＣＩフラグをチェックして、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩに対応していることを確認する。

【０２２８】

続いて、Ｓｉｎｋ機器から、Ｒｘ乱数とＲｘ証明書を含んだＲｘチャレンジが送信される。これに対し、Ｓｏｕｒｃｅ機器からは、Ｔｘ乱数及びＴｘ証明書を含んだＴｘチャレンジが返信される。

【０２２９】

続いて、Ｓｏｕｒｃｅ機器から、Ｒｘ乱数、Ｔｘメッセージ、Ｔｘ署名を含んだＲｘレスポンスが送信される。そして、Ｓｉｎｋ機器からはＴｘ乱数、Ｒｘメッセージ、Ｒｘ署名を含んだＴｘレスポンスが送信され、通常のチャレンジ・アンド・レスポンス認証手続きが続く。

【０２３０】

図３０は、Ｓｉｎｋ機器が、図２９に示した動作に対応したチャレンジ・アンド・レスポンス動作を行なうための処理手順をフローチャートの形式で示している。ここでは、Ｔｘ署名２の検証を行なうにはＴｘ証明書に含まれるＳｏｕｒｃｅ機器の公開鍵が必要であるため、この検証処理はＴｘチャレンジの受信以降に行なうことになる。

【０２３１】

Ｓｉｎｋ機器は、チャレンジ・アンド・レスポンス用のＲｘ乱数２を含んだ能力確認コマンドを送信する（ステップＳ１３１）。

【０２３２】

ここで、Ｓｏｕｒｃｅ機器から応答を受信し（ステップＳ１３２）、且つこの応答がＡＣＣＥＰＴＥＤである場合には（ステップＳ１３３のＹｅｓ）、続いて、Ｒｘチャレンジの送信とＴｘチャレンジの受信を行なう（ステップＳ１３４）。そして、Ｒｘ乱数２とＴｘメッセージに対するＴｘ署名２を検証する（ステップＳ１３５）。

【０２３３】

Ｓｉｎｋ機器は、Ｔｘ署名２の検証に成功した場合には（ステップＳ１３６のＹｅｓ）、Ｔｘメッセージ２に含まれるＣＣＩフラグを参照し、セットされているかどうかを確認する（ステップＳ１３７）。そして、ＣＣＩフラグがセットされていることを確認したら、ＰＣＰ－ＣＣＩを参照可とする。続いて、Ｒｘ乱数とＲｘ証明書を含んだＲｘチャレンジが送信するとともに、Ｓｏｕｒｃｅ機器からＴｘ乱数及びＴｘ証明書を含んだＴｘチャレンジを受信する（ステップＳ１３８）。

【０２３４】

また、ステップＳ１３３において能力確認コマンドに対するＡＣＣＥＰＴＥＤ応答を受

信できなかったときには、Ｓｉｎｋ機器は、Ｒｘ乱数とＲｘ証明書を含んだＲｘチャレンジが送信するとともに、Ｓｏｕｒｃｅ機器からＴｘ乱数及びＴｘ証明書を含んだＴｘチャレンジを受信するが（ステップＳ１４０）、ＣＣＩフラグを確認することができないので（ステップＳ１４１）、ＰＣＰ－ＣＣＩは参照付加とする。

【０２３５】

また、ステップＳ１３７においてＴｘ署名２の検証に失敗したときも、ＣＣＩフラグを確認することができないので（ステップＳ１４１）、ＰＣＰ－ＣＣＩは参照付加とする。

【産業上の利用可能性】

【０２３６】

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

【０２３７】

本発明の適用例として、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器とＤＴＣＰ＿Ｓｉｎｋ機器の間で行なわれるＨＴＴＰプロトコルを利用したコンテンツ伝送を挙げることができるが、本発明の要旨はこれに限定されない。コピー制御情報とともに暗号化コンテンツを伝送するその他のさまざまなタイプの情報通信システムに対しても、同様に本発明を適用することができる。

【０２３８】

要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、特許請求の範囲を参酌すべきである。

【図面の簡単な説明】

【０２３９】

【図１】図１は、本発明の一実施形態に係る情報通信システムの構成例を模式的に示した図である。

【図２】図２は、図１に示した情報通信システムにおいて、クライアント（すなわち、Ｓｉｎｋ機器）として動作する情報通信装置の機能構成を示した図である。

【図３】図３は、図１に示した情報通信システムにおいて、サーバ（すなわち、Ｓｏｕｒｃｅ機器）として動作する情報通信装置の機能構成を示した図である。

【図４】図４は、ＤＴＣＰ＿Ｓｏｕｒｃｅ機器とＤＴＣＰ＿Ｓｉｎｋ機器の間でＡＫＥに基づく鍵交換手続き、及び鍵交換により共有した鍵を利用した暗号化コンテンツ伝送を行なう仕組みを説明するための図である

【図５】図５は、ＰＣＰのデータ構造を模式的に示した図である。

【図６】図６は、ＰＣＰペイロードにパディングする様子を示した図である。

【図７】図７は、本発明の実施形態に係るＰＣＰヘッダのデータ構造を示した図である。

【図８】図８は、ＰＣＰ－ＣＣＩフィールドのフォーマット構成例を示した図である。

【図９】図９は、Ｍｏｄｅビット・フィールドに基づいてＰＣＰ　ＣＣＩフィールドの意味を識別するための処理手順を示したフローチャートである。

【図１０】図１０は、Ｍｏｄｅビット・フィールドとＳＥビット・フラグの値の組み合わせに基づいてＰＣＰ　ＣＣＩフィールドの意味を識別するための処理手順を示したフローチャートである。

【図１１】図１１は、Ｍｏｄｅビット・フィールド及びＳＥビット・フラグの値の組み合わせに基づいてＥ－ＥＭＩでＥｍｂｅｄｄｅｄ　ＣＣＩを代用することが可能かどうかを判別するための処理手順を示したフローチャートである。

【図１２】図１２は、ＬｅｇａｃｙのＳｏｕｒｃｅ機器とＳｉｎｋ機器間でＰＣＰを伝送する仕組みを説明するための図である。

【図１３】図１３は、ＰＣＰ－ＣＣＩをＰＣＰヘッダに埋め込む伝送方式を適用したＳｏｕｒｃｅ機器とＳｉｎｋ機器間でＰＣＰを伝送する仕組みを説明するための図である。

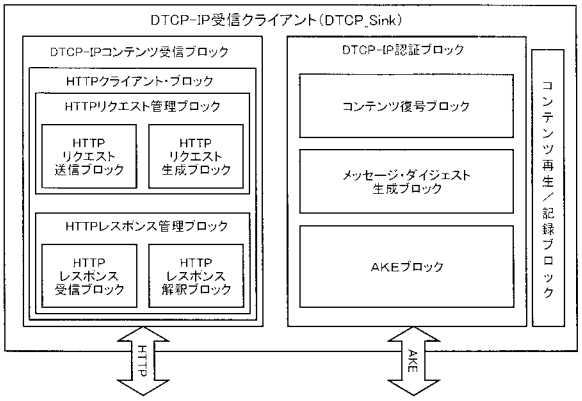
【図１４】図１４は、図１２に示したＬｅｇａｃｙのＳｏｕｒｃｅ及びＳｉｎｋ機器と、

図１３に示した新方式のＳｏｕｒｃｅ及びＳｉｎｋ機器が混在するコンテンツ伝送環境下においてＬｅｇａｃｙ問題が発生する様子を示した図である。
【図１５】図１５は、コンテンツ鍵確認のためのＳｉｎｋ機器とＳｏｕｒｃｅ機器間の手続きを示した図である。
【図１６】図１６は、ＰＣＰ－ＣＣＩに対応したＳｏｕｒｃｅ機器がＬｅｇａｃｙのＳｉｎｋ機器との間でコンテンツ鍵確認手続きを行なうための処理手順を示したフローチャートである。
【図１７】図１７は、ＬｅｇａｃｙのＳｉｎｋ機器がＰＣＰ－ＣＣＩに対応したＳｏｕｒｃｅ機器との間でコンテンツ鍵確認手続きを行なうための処理手順を示したフローチャートである。
【図１８】図１８は、ＰＣＰ－ＣＣＩに対応したＳｏｕｒｃｅ機器（Ｎｅｗ　Ｓｏｕｒｃｅ）とＬｅｇａｃｙ　Ｓｉｎｋの間で行なわれるコンテンツ鍵確認手続の動作シーケンスを示した図である。
【図１９】図１９は、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器のＣＣＩフラグをチェックしてＰＣＰヘッダ部のＰＣＰ－ＣＣＩ情報を処理するための手順を示したフローチャートである。
【図２０】図２０は、機器証明書内にＣＣＩフラグを埋め込むことによって、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示した図である。
【図２１】図２１は、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器から受信したＴｘチャレンジに含まれる機器証明書からＣＣＩフラグを検証するための処理手順を示したフローチャートである。
【図２２】図２２は、機器が自身の署名を付加して送るレスポンスの中にＣＣＩフラグを埋め込むことによって、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示した図である。
【図２３】図２３は、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器から受信したＲｘレスポンスに含まれるＴｘメッセージからＣＣＩフラグを検証するための処理手順を示したフローチャートである。
【図２４】図２４は、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し新規のＲｘチャレンジを送信し、これに対しＳｏｕｒｃｅ機器がＣＣＩフラグを埋め込んだ新規のＲｘレスポンスを返し、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示した図である。
【図２５】図２５は、Ｓｏｕｒｃｅ機器が、図２４に示した動作に対応したチャレンジ・アンド・レスポンス動作を行なうための処理手順を示したフローチャートである。
【図２６】図２６は、Ｓｉｎｋ機器がＳｏｕｒｃｅ機器から受信した新規のＲｘレスポンスに含まれるＴｘメッセージからＣＣＩフラグを検証するための処理手順を示したフローチャートである。
【図２７】図２７は、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し能力確認コマンドを送信し、これに対しＳｏｕｒｃｅ機器がＣＣＩフラグを埋め込んだ能力確認レスポンスを返し、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示した図である。
【図２８】図２８は、Ｓｉｎｋ機器が、図２７に示した動作に対応したチャレンジ・アンド・レスポンス動作を行なうための処理手順を示したフローチャートである。
【図２９】図２９は、Ｓｉｎｋ機器からＳｏｕｒｃｅ機器に対し能力確認コマンドを送信し、これに対しＳｏｕｒｃｅ機器がＣＣＩフラグを埋め込んだ署名付きの能力確認レスポンスを返し、Ｓｏｕｒｃｅ機器がＰＣＰ－ＣＣＩ対応であることをＳｉｎｋ機器に示す送受信シーケンス例を示した図である。
【図３０】図３０は、Ｓｉｎｋ機器が図２９に示した動作に対応したチャレンジ・アンド・レスポンス動作を行なうための処理手順を示したフローチャートである。
【図３１】図３１は、ＰＣＰヘッダの内部構造を示した図である。

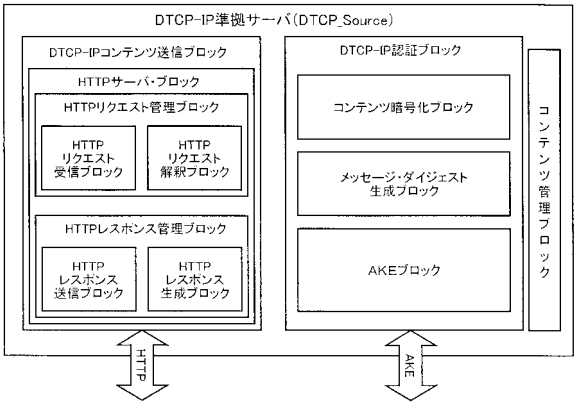
【図１】


Source機器
Sink機器

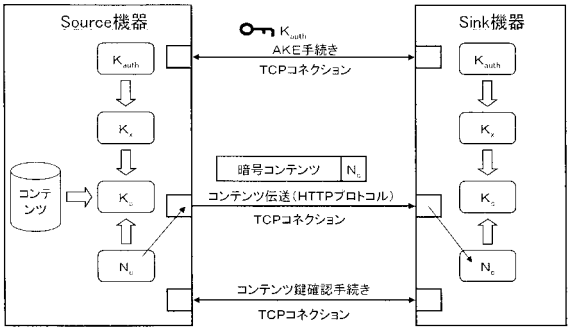
【図２】


DTCP-IP受信クライアント(DTCP_Sink)
DTCP-IPコンテンツ受信ブロック
HTTPクライアント・ブロック
HTTPリクエスト管理ブロック
HTTP リクエスト 送信ブロック
HTTP リクエスト 生成ブロック
HTTPレスポンス管理ブロック
HTTP レスポンス 受信ブロック
HTTP レスポンス 解釈ブロック
DTCP-IP認証ブロック
コンテンツ復号ブロック
メッセージ・ダイジェスト 生成ブロック
AKEブロック
コンテンツ再生／記録ブロック
HTTP
AKE

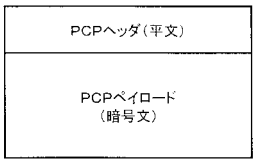
【図３】


DTCP-IP準拠サーバ(DTCP_Source)
DTCP-IPコンテンツ送信ブロック
HTTPサーバ・ブロック
HTTPリクエスト管理ブロック
HTTP リクエスト 受信ブロック
HTTP リクエスト 解釈ブロック
HTTPレスポンス管理ブロック
HTTP レスポンス 送信ブロック
HTTP レスポンス 生成ブロック
DTCP-IP認証ブロック
コンテンツ暗号化ブロック
メッセージ・ダイジェスト 生成ブロック
AKEブロック
コンテンツ管理ブロック
HTTP
AKE

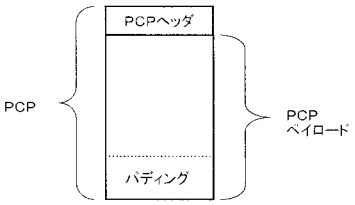
【図４】


Source機器
Sink機器
K_{auth}
AKE手続き
TCPコネクション
K_{auth}
K_x
暗号コンテンツ
N_c
コンテンツ
K_c
コンテンツ伝送(HTTPプロトコル)
TCPコネクション
N_c
コンテンツ鍵確認手続き
TCPコネクション

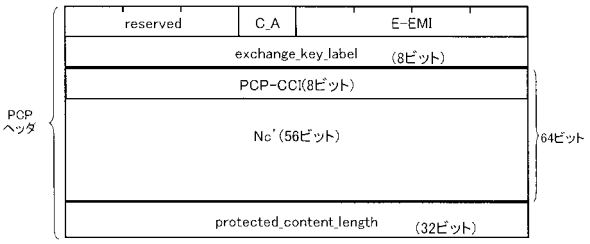
【図５】


PCPヘッダ(平文)
PCPペイロード
(暗号文)

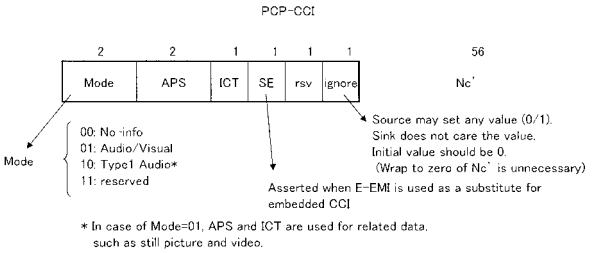
【図６】



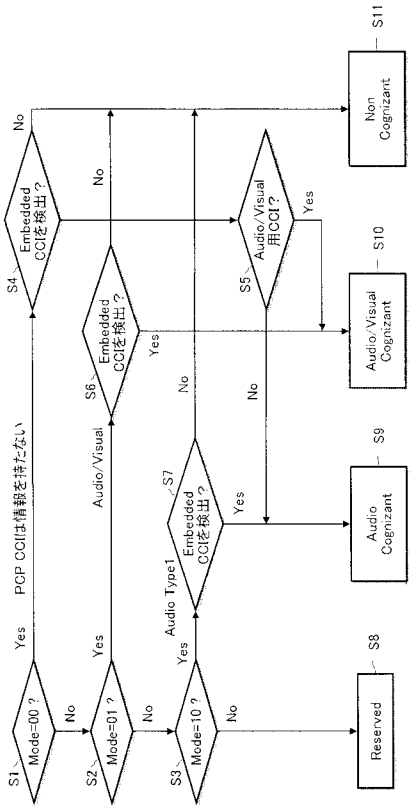
【図７】



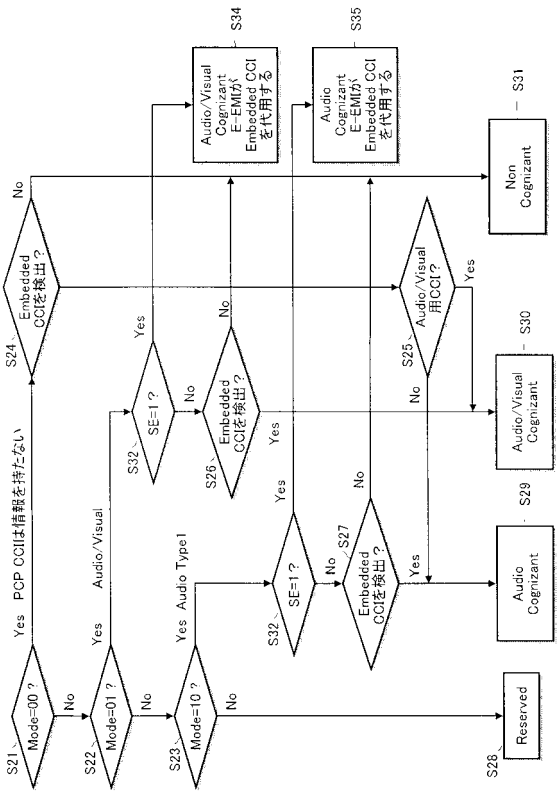
【図８】



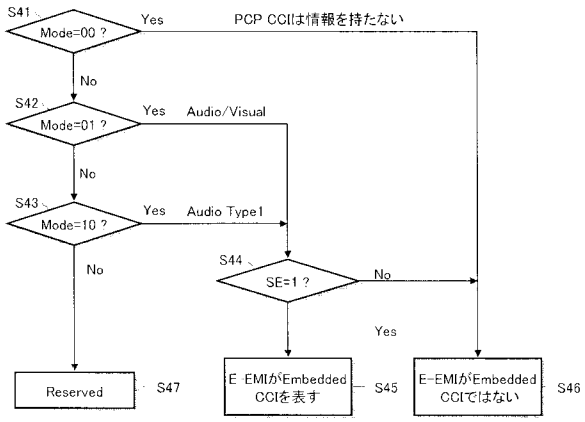
【図９】



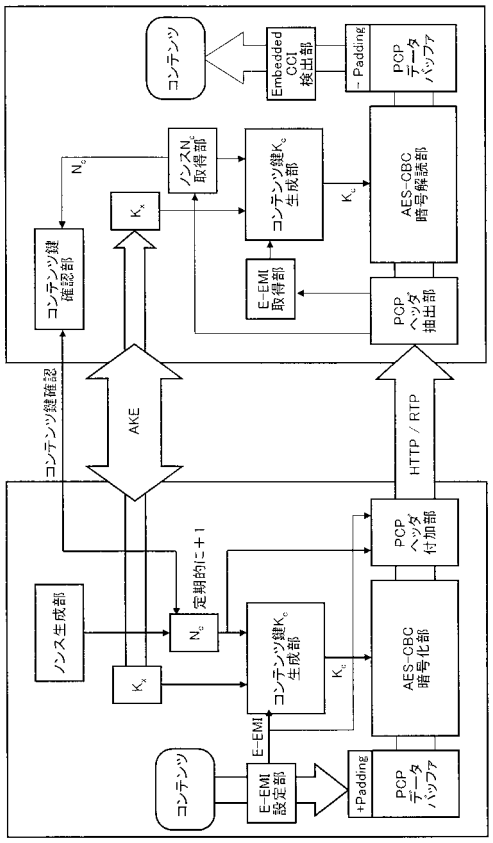
【図１０】



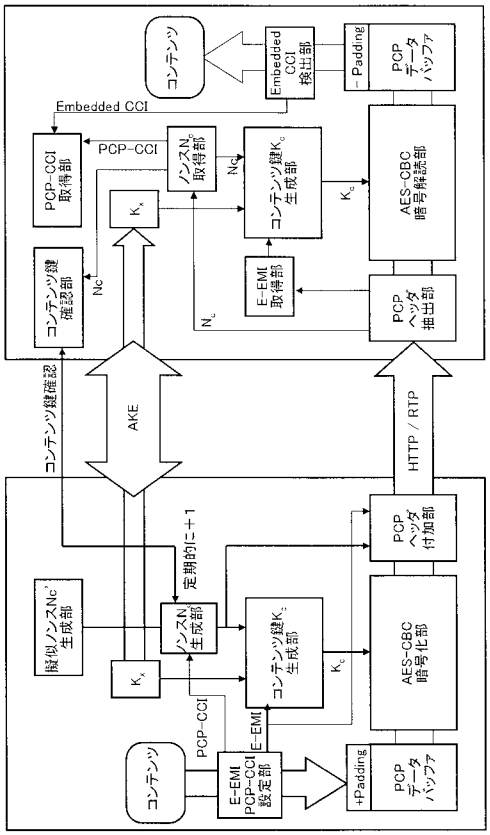
【図１１】



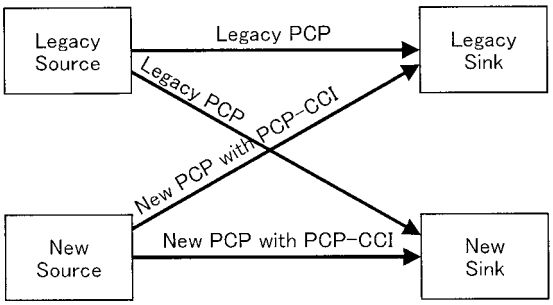
【図１２】



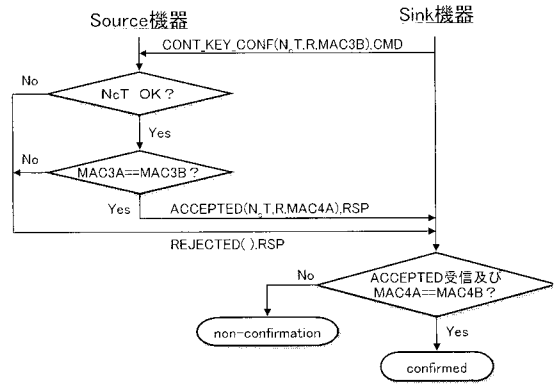
【図１３】



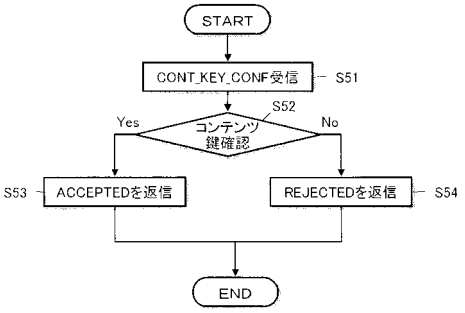
【図１４】



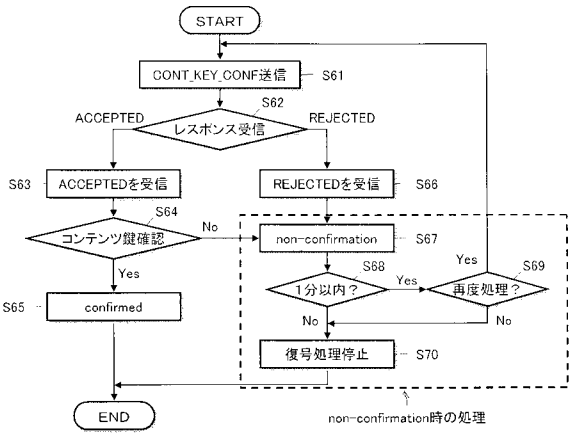
【図１５】



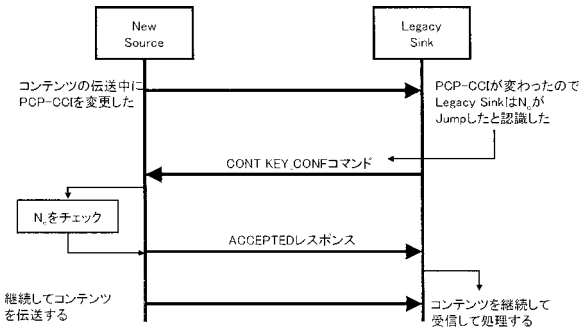
【図１６】



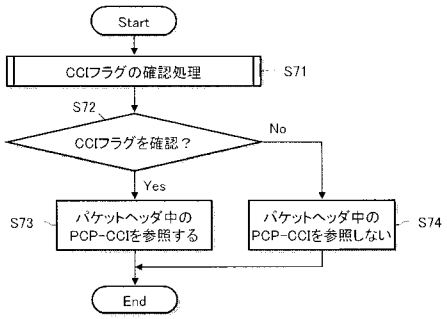
【図１７】



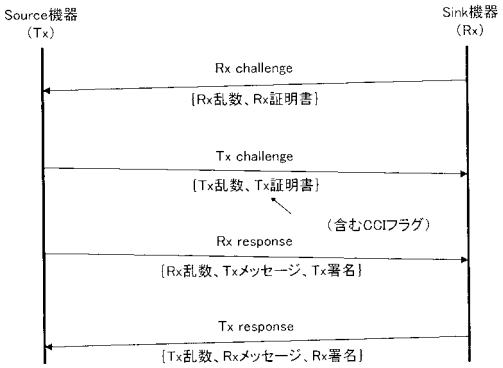
【図１８】



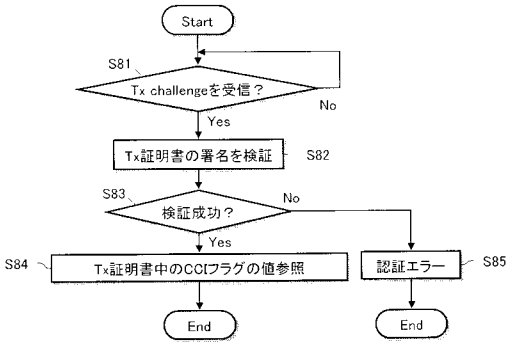
【図１９】



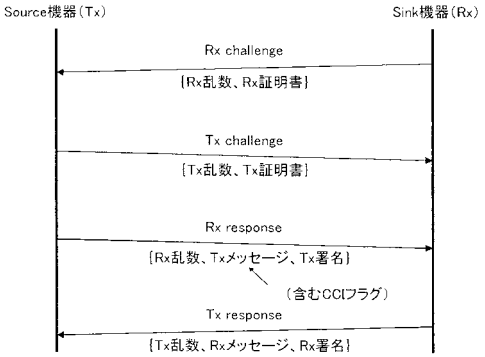
【図２０】



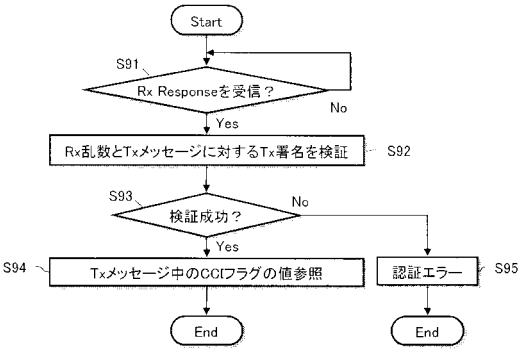
【図２１】



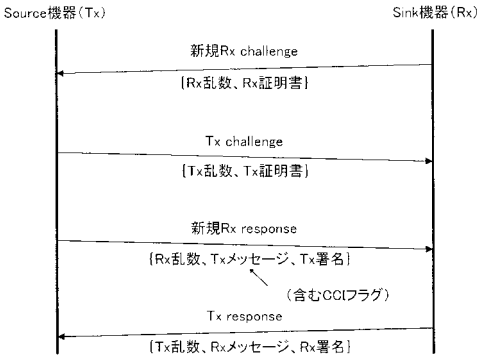
【図２２】



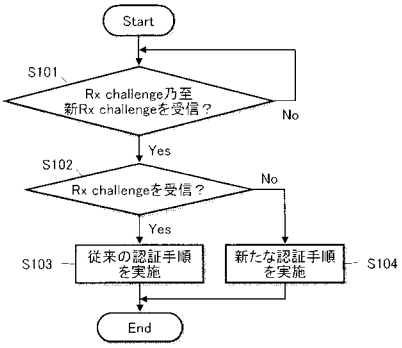
【図２３】



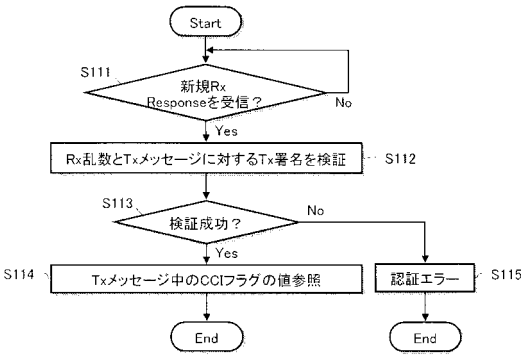
【図２４】



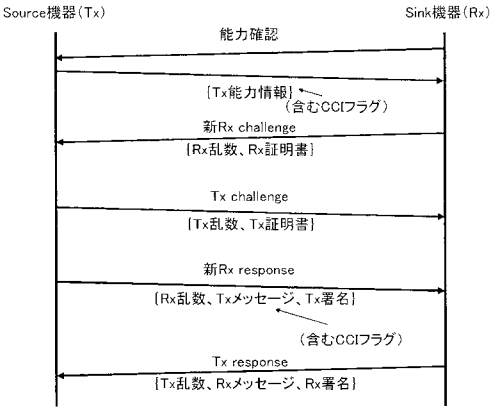
【図２５】



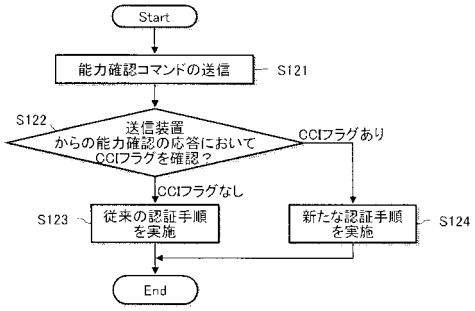
【図２６】



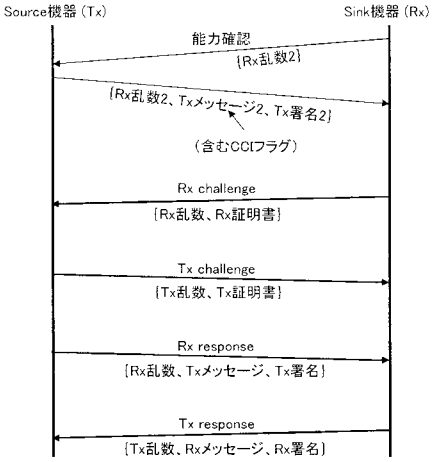
【図２７】



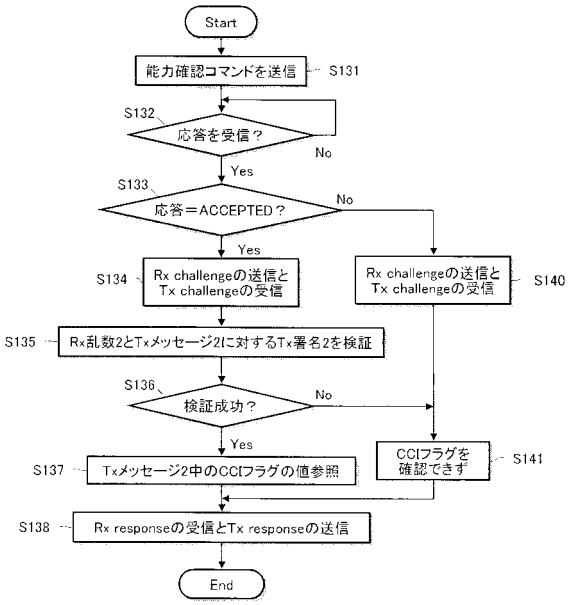
【図２８】



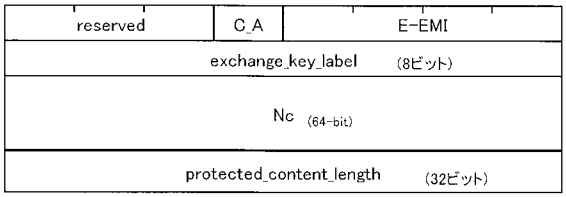
【図２９】



【図３０】



【図３１】


reserved
C_A
E-EMI
exchange_key_label (8ビット)
Nc (64-bit)
protected_content_length (32ビット)

フロントページの続き

(72)発明者　嶋　久登
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　石田　信行

(56)参考文献　特開平１０－３０２３９１（ＪＰ，Ａ）
特開２０００－０４０２９４（ＪＰ，Ａ）
国際公開第２００５／０５７８６５（WO，Ａ１）
特開２００２－０８３４６５（ＪＰ，Ａ）
特開２０００－２９５２４０（ＪＰ，Ａ）
特開２０００－０４０２９８（ＪＰ，Ａ）
特開平１１－０８６４３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　　９／３６
Ｇ０６Ｆ　２１／２４
Ｇ１１Ｂ　２０／１０