(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年4 月20 日 (20.04.2006)

PCT

(10) 国際公開番号
WO 2006/041082 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
G06F 21/00 (2006.01) *H04N 7/167* (2006.01)
G11B 20/10 (2006.01)

(21) 国際出願番号: PCT/JP2005/018777

(22) 国際出願日: 2005 年10 月12 日 (12.10.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2004-298722
2004 年10 月13 日 (13.10.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 高辻 綾子 (TAKATSUJI, Ayako). 飯塚 裕之 (IITSUKA, Hiroyuki). 臼木 直司 (USUKI, Naoshi).

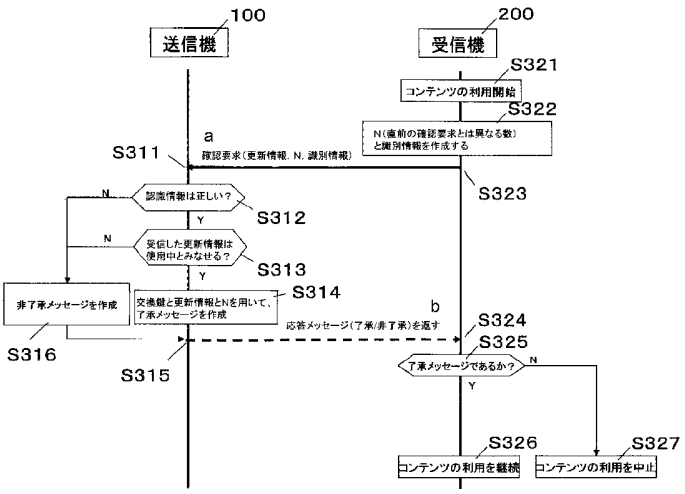
(74) 代理人: 松田 正道 (MATSUDA, Masamichi); 〒5320003 大阪府大阪市淀川区宮原５丁目１番３号 新大阪生島ビル Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: REGULAR CONTENT CHECK METHOD, CONTENT TRANSMISSION/RECEPTION SYSTEM, TRANSMITTER, AND RECEIVER

(54) 発明の名称: 正規コンテンツ確認システム



100...TRANSMITTER
200...RECEIVER
S321...CONTENT USE START
S322...CREATE N (NUMBER DIFFERENT FROM THE CHECK REQUEST IMMEDIATELY BEFORE) AND IDENTIFICATION INFORMATION
a...CHECK REQUEST (UPDATE INFORMATION, N, IDENTIFICATION INFORMATION)
S312...IDENTIFICATION INFORMATION IS CORRECT?
S313...RECEIVED UPDATE INFORMATION CAN BE CONSIDERED TO BE IN USE?
S316...CREATE NON-APPROVAL MESSAGE
S314...CREATE APPROVAL MESSAGE BY USING EXCHANGE KEY, UPDATE INFORMATION, AND N
b...RETURN RESPONSE MESSAGE (APPROVAL/NON-APPROVAL)
S325...APPROVAL MESSAGE?
S326...CONTINUE USING THE CONTENT
S327...STOP USE OF THE CONTENT

(57) Abstract: It has been impossible to detect spoofing and invalid content transmission to a receiver by using invalid device monitoring communication between a valid transmitter and a receiver. There is provided a system for transmitting update information required for creation of a content key used for encryption/decryption together with an encrypted content. The system employs a valid content check method including: a step (S323) in which the receiver (200) transmits a validity check request including update information received from the transmitter (100); an update information correlation step (S313) in which the transmitter (100) for correlating theupdate information contained in the received validity check request with predetermined update information; approval message transmission steps (S314, S315) used when the update information is matched with the predetermined information, for creating an approval message by using the update information and an exchange key shared between the transmitter (100) and the receiver (200) and transmitting the message; and a valid content judgment step (S325) in which the receiver (200) for deciding that the content is valid upon reception of the approval message.

(57) 要約: 正当な送信機と受信機の間の通信を監視した不正機器による、なりすまし・受信機への不当なコンテンツの送りつけを検出できなかった。 コンテンツの暗号化／復号に用いるコンテンツ鍵の作成に必要な更新情報を暗号化コンテンツに付随して伝送するシステムにおいて、受信機２００が、送信機１００から受信した更新情報を含む正規確認要求を送信する確認要求ステップＳ３２３と、送信機１

[続葉有]

WO 2006/041082 A1

BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

００が、受信した正規確認要求に含まれる更新情報が所定の更新情報であるか照合する更新情報照合ステップＳ３１３と、所定の更新情報に一致した場合、その更新情報と送信機１００／受信機２００間で共有の交換鍵とを用いて了承メッセージを作成し送信する了承メッセージ送信ステップＳ３１４、Ｓ３１５と、受信機２００が、了承メッセージの受信で正規のコンテンツと判断する正規コンテンツ判定ステップＳ３２５とを備えた正規コンテンツ確認方法を用いる。

明 細 書

正規コンテンツ確認システム

信機

技術分野

[0001] 本発明は、コンテンツをネットワーク経由で配信する際に、配信元(送信機)と配信先(受信機)間で正当なコンテンツを送受信するためのデータ伝送セキュリティ技術に関連した正規コンテンツ確認方法、コンテンツ送受信システム、送信機および受信機等に関する。

背景技術

[0002] 近年、インターネットへの接続環境が整い、また家電製品もネットワーク対応を進めやすい環境(ネットワーク化を行うためのデバイスのローコスト化、能力向上など)が整ってきている。また同時に、伝送されるコンテンツが、不正コピーや不正傍受、不正改竄をされないように保護するための著作権保護技術が重要視されてきている。Digital Transmission Content Protection (DTCP)は、IEEE1394シリアルバスに伝送されるAVコンテンツの著作権保護技術として開発され、拡張としてインターネットプロトコル(IP)上でも技術展開が行われている(DTCP Volume 1 Supplement E Mapping DTCP to IP (Informational Version) Revision 1.0 November 24, 2003参照)。

[0003] 図8および図9は、HTTPプロトコル(サーバとクライアント間に、コネクションを確立してから、クライアントからのリクエストに対して、サーバがレスポンスを返すという形で、データのやりとりを行う)を用いたDTCP-IPによる、従来の伝送システムにおける送信機および受信機の機能ブロック図の一例である。

[0004] 図8における送信機800は、証明書・鍵保持部801、交換鍵作成部802、認証・鍵交換部803、更新情報作成・更新部804、コピー制御情報管理部805、コンテンツ鍵算出部806、コンテンツ蓄積部807、コンテンツ暗号化部808、コンテンツパケット作成部809、コンテンツパケット送信部810、およびHTTPプロトコル部811を備える。

[0005] 証明書・鍵保持部801は、公開鍵暗号の鍵ペア(公開鍵、秘密鍵)と証明書を保持

している。

[0006] 交換鍵作成部802は、コンテンツを暗号化するためのコンテンツ鍵(Kc)を算出するために用いる交換鍵(Kx)を生成する。

[0007] 認証・鍵交換部803は、受信機からの認証要求を受け付け、当該受信機が、正当な機器であるかどうかを認証により確認する。ここで、認証としては、送信機と受信機がそれぞれ保持している公開鍵暗号の鍵ペア(公開鍵、秘密鍵)と証明書を使い、チャンレンジレスポンス型の認証を行う方法を用いる。認証の間に送信機と受信機間では認証鍵(Kauth)が共有され、認証後に、共有された認証鍵(Kauth)を用いて、交換鍵作成部802で作成された交換鍵(Kx)が受信機に渡される。これら一連の、認証から鍵取得までのプロセスを認証・鍵交換部803にて行う。

[0008] 更新情報作成・更新部804は、更新情報(Nc)を新規作成あるいは更新する。ここで、例えば、作成とは乱数発生等により新たな更新情報(Nc)の作成を行うこと、更新とは現在の値に1を加算することである。更新情報(Nc)は、TCPコネクションの確立により作成される。更新は、所定のルールにより行われる。所定のルールとしては、同一TCPコネクション上でのHTTPリクエスト・レスポンスごとに更新されるなどがあげられるが、本発明の主眼ではないため、ここでは説明を省略する。ここで、作成・更新された更新情報(Nc)は、コンテンツ保護を維持するために所定のルールでコンテンツ鍵(Kc)を算出するために用いられる。さらに、更新情報(Nc)は、コンテンツ鍵(Kc)で暗号化されたコンテンツに付随されて受信機に渡される。

[0009] コピー制御情報管理部805は、各コンテンツの管理内容(例えば、コピー禁止、一世代コピー可など)である、コンテンツに適応される暗号化モードをコピー制御情報(E_EMI)として管理する。コピー制御情報(E_EMI)は、コンテンツ鍵(Kc)の算出に用いられ、算出されたコンテンツ鍵(Kc)で暗号化されたコンテンツに付随して受信機に渡される。

[0010] コンテンツ鍵算出部806は、交換鍵作成部802で作成された交換鍵(Kx)、更新情報作成・更新部804で作成・更新された更新情報(Nc)、コピー制御情報管理部805で管理されるコピー制御情報(E_EMI)などから、一方向性関数を用いてコンテンツ鍵(Kc)を算出する。

[0011] コンテンツ蓄積部807は、配信の対象となる各種コンテンツを格納している。

[0012] コンテンツ暗号化部808は、配信するコンテンツを、コンテンツ鍵算出部806で算出されたコンテンツ鍵(Kc)を用いて暗号化する。

[0013] コンテンツパケット作成部809は、コンテンツ暗号化部808で暗号化されたコンテンツに、更新情報作成・更新部804で作成・更新された更新情報(Nc)と、コピー制御情報管理部805で管理されるコピー制御情報(E_EMI)を付加したコンテンツパケットを作成する。

[0014] コンテンツパケット送信部810は、コンテンツパケット作成部809で作成されたコンテンツパケットを送信する。

[0015] HTTPプロトコル部811は、HTTPサーバ処理を行う。HTTPリクエストを受信・解析し、HTTPレスポンスを作成して応答する。ここで、コンテンツパケット作成部809で作成されるコンテンツパケットは、送信機からのHTTP GETリクエストに対するHTTPレスポンスのボディとして送信される。

[0016] 図9における受信機900は、証明書・鍵保持部901、認証・鍵交換部902、更新情報格納部903、コピー制御情報格納部904、コンテンツ鍵算出部905、コンテンツ利用部906、コンテンツ復号部907、コンテンツパケット解析部908、コンテンツパケット受信部909、およびHTTPプロトコル部910を備える。

[0017] 証明書・鍵保持部901は、公開鍵暗号の鍵ペア(公開鍵、秘密鍵)と証明書を保持している。

[0018] 認証・鍵交換部902は、所定のタイミングで認証要求を行い、認証の間に送信機と受信機間で認証鍵(Kauth)が共有され、認証後に、送信機から、共有された認証鍵(Kauth)を用いて暗号化された交換鍵(Kx)を受け取り、復号する。

[0019] 更新情報格納部903は、送信機から受信した暗号化されたコンテンツに付随する更新情報(Nc)を格納する。

[0020] コピー制御情報格納部904は、暗号化されたコンテンツに付随するコピー制御情報(E_EMI)を格納する。

[0021] コンテンツ鍵算出部905は、認証・鍵交換部902で送信機から渡された交換鍵(Kx)と、更新情報格納部903で格納された更新情報(Nc)と、コピー制御情報格納部904

で格納されたコピー制御情報(E_EMI)などから、一方向性関数を用いてコンテンツ鍵(Kc)を算出する。

[0022] コンテンツ利用部906は、復号されたコンテンツを、コピー制御情報格納部904で格納されたコピー制御情報(E_EMI)に従って再生・記録するなどして利用する。

[0023] コンテンツ復号部907は、コンテンツ鍵算出部905で算出されたコンテンツ鍵(Kc)を用いて、暗号化されたコンテンツを復号する。

[0024] コンテンツパケット解析部908は、暗号化されたコンテンツに付随する更新情報(Nc)およびコピー制御情報(E_EMI)を分離し、それぞれ、更新情報格納部903およびコピー制御情報格納部904に渡す。

[0025] コンテンツパケット受信部909は、コンテンツパケットを受信する。

[0026] HTTPプロトコル部910は、HTTPクライアント処理を行う。HTTPリクエストを作成・送信し、HTTPレスポンスを受信・解析する。

[0027] 図10は、図8に示した送信機800および図9に示した受信機900を備えた従来の伝送システムにおける暗号通信プロトコル手順を示している。

[0028] 以下、図10を用いて、従来の暗号通信プロトコル手順について説明する。

[0029] (1001)送信機800と受信機900の間の認証プロセスを通じて、認証鍵(Kauth)が共有される。これは一回の認証毎に使い捨てられる。

[0030] (1002)送信機800は、交換鍵(Kx)を生成する。

[0031] (1003)送信機800は、認証鍵(Kauth)で交換鍵(Kx)を暗号化して(Ksx)、受信機900に送付する。

[0032] (1004)受信機900は、受け取ったKsxを認証鍵(Kauth)で復号して、交換鍵(Kx)を得る。

[0033] (1005)受信機900から送信機800に、HTTP GETリクエストによるコンテンツ要求が送信される。

[0034] (1006)送信機800は、更新情報(Nc)を生成する。

[0035] (1007)送信機800は、受信機900から要求されたコンテンツのコピー制御情報(E_EMI)を認識する。

[0036] (1008)送信機800は、交換鍵(Kx)、更新情報(Nc)、コピー制御情報(E_EMI)を入

力パラメータとして、一方向性関数により、コンテンツ鍵(Kc)を算出する。

[0037] (1009)送信機800は、受信機900から要求されたコンテンツをコンテンツ鍵(Kc)により暗号化する。

[0038] (1010)送信機800は、HTTP GETレスポンスのボディとして、暗号化したコンテンツに更新情報(Nc)、コピー制御情報(E_EMI)を付加して、受信機に送信する。

[0039] (1011)受信機900は、受信したレスポンスから、更新情報(Nc)を獲得する。

[0040] (1012)受信機900は、同様に、受信したレスポンスから、コピー制御情報(E_EMI)を獲得する。

[0041] (1013)受信機900は、交換鍵(Kx)、更新情報(Nc)、コピー制御情報(E_EMI)を入力パラメータとして、一方向性関数により、コンテンツ鍵(Kc)を算出する。

[0042] (1014)受信機900は、コンテンツ鍵(Kc)を用いて、暗号化されたコンテンツを復号する。

[0043] 上記の一連のプロトコル手順によって、送信機800と受信機900の間に、共通の交換鍵(Kx)(1080、1090)と、コンテンツに付随する、更新情報(Nc)(1081、1091)とコピー制御情報(E_EMI)(1082、1092)が共有され、正当な受信機でのみこれらを用いて、暗号化されたコンテンツを正しく復号することができる。

[0044] しかしながら、従来のシステムにおいて、交換鍵を共有している当事者間での暗号通信によるコンテンツ保護の仕組みは確立されているが、不特定多数の機器が接続するIPネットワークの特性上「誰が送ってきたのか」という認証の問題が発生する可能性がある。

[0045] すなわち、受信機がコンテンツを要求し受信したとしても、間違いなく要求先の正当な送信機からの正当なコンテンツであることを確認する手段がないため、例えば、攻撃者が、IPネットワークを監視し、流れる暗号化コンテンツを記録(キャッシュ保存)し、その後、受信機の要求に対し、正当な送信機になりすましてその記録したコンテンツで応答しても判別できない。

[0046] 図11は、従来の伝送システムのネットワーク構成における課題を説明する図を示している。以下、図11を用いて、課題とされる一事例を説明する。

[0047] 送信機800と受信機900は、それぞれ、交換鍵を共有している正当な暗号通信対

象機器である。送信機800と受信機900の間では、受信機900のコンテンツ要求(1111)に応じて、付随情報を伴った暗号化コンテンツ(1112)が伝送される。

[0048] ここで、ネットワーク上に接続した不正な機器1100は、バス上を流れるHTTPリクエスト、レスポンスを監視し、これらを記録することができる(1113)。不正な機器1100自身はコンテンツを復号し視聴するなどの利用はできないが、例えば、その後、受信機900から送信機800へのHTTPリクエストをフックし(1114)、正当な送信機800に成りすまし、以前記録したコンテンツを、本来受信機900が受け取るべきコンテンツにすり替えて送信する(1115)ことができてしまう。

[0049] このとき、受信機900は、そのすり替えて送信されてきたコンテンツが、正当な送信機800から送信されてきた正規のコンテンツなのか不正な機器1100から送信されてきたコンテンツなのかを判別できないので、そのすり替えて送信されてきたコンテンツをユーザに利用させてしまうことになる。

[0050] 本発明は、上述した従来の課題を解決するもので、受信したコンテンツが正規のコンテンツであるか否かを判別できる、正規コンテンツ確認方法、コンテンツ送受信システム、送信機および受信機等を提供することを目的とする。

発明の開示

[0051] 上述した課題を解決するために、第1の本発明は、

受信機からのコンテンツ要求に応じて、ネットワークに接続された送信機が、所定のタイミングで更新する更新情報であってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信するコンテンツ送受信システムにおける、正規コンテンツ確認方法であって、

前記受信機にて、前記送信機から受信した前記更新情報を少なくとも含む正規確認要求を送信する確認要求ステップと、

前記送信機にて、前記受信機から受信した前記正規確認要求に含まれる前記更新情報が、所定の更新情報であるかどうかを照合する更新情報照合ステップと、

前記送信機にて、前記更新情報が前記所定の更新情報であると判定した場合には、前記更新情報と、前記送信機および前記受信機の双方であらかじめ共有されている交換鍵とを用いて了承メッセージを作成し前記受信機に送信する、了承メッセー

ジ送信ステップと、

前記受信機にて、前記送信機からの前記了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツであると判断する正規コンテンツ判定ステップとを備えた、正規コンテンツ確認方法である。

[0052] また、第2の本発明は、

前記所定の更新情報は、現在使用中の更新情報または所定回数更新前の更新情報である、第1の本発明の正規コンテンツ確認方法である。

[0053] また、第3の本発明は、

前記確認要求ステップでは、前記受信機は、前記正規確認要求を送信する毎に異ならせた数も前記正規確認要求に含めて送信し、

前記了承メッセージ送信ステップでは、前記送信機は、前記正規確認要求に含まれる前記数も用いて前記了承メッセージを作成する、第1の本発明の正規コンテンツ確認方法である。

[0054] また、第4の本発明は、

前記確認要求ステップでは、前記受信機は、前記交換鍵および前記送信機から送られてきた前記更新情報を用いて作成した識別メッセージも前記正規確認要求に含めて送信し、

前記了承メッセージ送信ステップでは、前記送信機は、前記更新情報が前記所定の更新情報であると判定し、かつ、前記正規確認要求に含まれる前記識別メッセージが、前記送信機自身が前記交換鍵および前記更新情報を用いて作成した識別メッセージと一致することを確認した場合に、前記了承メッセージを前記受信機に送信する、第1の本発明の正規コンテンツ確認方法である。

[0055] また、第5の本発明は、

前記了承メッセージ送信ステップでは、前記送信機は、前記更新情報が前記所定の更新情報ではないと判定した場合には、非了承メッセージを前記受信機に送信し、

前記正規コンテンツ判定ステップでは、前記受信機にて、前記送信機からの前記非了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツでは

ないと判断し前記コンテンツを利用しない、第1の本発明の正規コンテンツ確認方法である。

[0056] また、第6の本発明は、

前記正規コンテンツ判定ステップで、前記受信機が前記了承メッセージを受信できない場合には、前記受信機にて、所定期間、前記正規確認要求を繰り返し送信する確認要求リトライ送信ステップをさらに備え、

前記正規コンテンツ判定ステップでは、前記受信機にて、前記所定期間を過ぎても前記了承メッセージを受信できない場合には、受信したコンテンツを利用しないようにする、第1の本発明の正規コンテンツ確認方法である。

[0057] また、第7の本発明は、

前記正規コンテンツ判定ステップで、前記受信機が前記了承メッセージを受信できない場合には、前記受信機にて、所定回数、前記正規確認要求を繰り返し送信する確認要求リトライ送信ステップをさらに備え、

前記正規コンテンツ判定ステップでは、前記受信機にて、前記正規確認要求を前記所定回数送信しても前記了承メッセージを受信できない場合には、受信したコンテンツを利用しないようにする、第1の本発明の正規コンテンツ確認方法である。

[0058] また、第8の本発明は、

前記正規コンテンツ判定ステップで、前記受信機にて、受信した前記コンテンツを利用しないようにした後に、所定の制限回数または所定の制限期間あるいは所定の停止条件が整うまで、前記正規確認要求を繰り返し送信する、確認要求再送信ステップをさらに備え、

前記正規コンテンツ判定ステップでは、前記受信機にて、受信した前記コンテンツを利用しないようにした後に、前記了承メッセージを受信した場合には、受信したコンテンツを利用するようにする、第5乃至第7のいずれかの本発明の正規コンテンツ確認方法である。

[0059] また、第9の本発明は、

コンテンツ要求を送信する受信機と、ネットワークにより前記受信機に接続され、前記受信機からのコンテンツ要求に応じて、所定のタイミングで更新する更新情報であ

ってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信する送信機とを備えたコンテンツ送受信システムにおいて、

前記受信機は、

前記送信機との双方であらかじめ共有されている交換鍵と、前記送信機から受信した前記更新情報とを用いて作成した正規確認要求を送信する確認要求手段と、

前記送信機からの了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツであると判断する確認結果照合手段とを有し、

前記送信機は、

前記受信機から送信されてきた前記正規確認要求を受信する確認要求受付手段と、

受信した前記正規確認要求に含まれる前記更新情報が、所定の更新情報であるかどうかを照合する更新情報確認手段と、

前記更新情報が前記所定の更新情報であると判定した場合には、前記更新情報および前記受信機との双方で共有されている前記交換鍵を用いて前記了承メッセージを作成し、前記受信機に送信する確認応答手段とを有する、コンテンツ送受信システムである。

[0060] また、第10の本発明は、

受信機からのコンテンツ要求に応じて、ネットワークに接続された送信機が、所定のタイミングで更新する更新情報であってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信するコンテンツ送受信システムに用いられる送信機であって、

前記受信機で、前記受信機との双方であらかじめ共有されている交換鍵と、前記送信機から受信した前記更新情報とを用いて作成され、前記受信機から送信されてきた正規確認要求を受信する確認要求受付手段と、

前記受信機から受信した前記正規確認要求に含まれる前記更新情報が、所定の更新情報であるかどうかを照合する更新情報確認手段と、

前記更新情報が前記所定の更新情報であると判定した場合には、前記更新情報と

前記交換鍵とを用いて、前記受信機が受信中のコンテンツが正規のコンテンツであるかどうかを判断するための了承メッセージを作成し前記受信機に送信する確認応答手段とを備えた、送信機である。

[0061] また、第11の本発明は、

受信機からのコンテンツ要求に応じて、ネットワークに接続された送信機が、所定のタイミングで更新する更新情報であってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信するコンテンツ送受信システムに用いられる受信機であって、

前記送信機との双方であらかじめ共有されている交換鍵と、前記送信機から受信した前記更新情報とを用いて作成した正規確認要求を送信する確認要求手段と、

前記送信機が、受信した前記正規確認要求に含まれる前記更新情報が所定の更新情報であると判定して、前記更新情報および前記交換鍵を用いて作成して送信してきた了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツであると判断する確認結果照合手段とを備えた、受信機である。

[0062] また、第12の本発明は、

第1の本発明の正規コンテンツ確認方法の、前記受信機にて前記正規確認要求を送信する前記確認要求ステップ、前記送信機にて前記更新情報が前記所定の更新情報であるかどうかを照合する前記更新情報照合ステップ、前記送信機にて前記了承メッセージを作成し前記受信機に送信する前記了承メッセージ送信ステップ、前記受信機にて前記送信機からの前記了承メッセージを受信した場合に前記送信機が正規の送信機であると確認する前記正規コンテンツ判定ステップ、をコンピュータに実行させるためのプログラムである。

[0063] また、第13の本発明は、

第12の本発明のプログラムを記録した記録媒体であって、コンピュータにより処理可能な記録媒体である。

[0064] 本発明により、受信したコンテンツが正規のコンテンツであるか否かを判別できる、正規コンテンツ確認方法、コンテンツ送受信システム、送信機および受信機等を提供できる。

図面の簡単な説明

[0065] [図1]本発明の実施の形態1に係るコンテンツ送受信システムで使用される送信機の機能ブロックを示す図

[図2]本発明の実施の形態1に係るコンテンツ送受信システムで使用される受信機の機能ブロックを示す図

[図3]本発明の実施の形態1に係るコンテンツ送受信システムにおける処理手順を示す図

[図4]本発明の実施の形態2に係るコンテンツ送受信システムで使用される受信機の機能ブロックを示す図

[図5]本発明の実施の形態2に係るコンテンツ送受信システムにおける処理手順を示す図

[図6]本発明の実施の形態3に係るコンテンツ送受信システムで使用される受信機の機能ブロックを示す図

[図7]本発明の実施の形態3に係るコンテンツ送受信システムにおける処理手順を示す図

[図8]従来の伝送システムにおける送信機の機能ブロックを示す図

[図9]従来の伝送システムにおける受信機の機能ブロックを示す図

[図10]従来の伝送システムにおける暗号通信プロトコル手順を示す図

[図11]従来の伝送システムのネットワーク構成における課題を説明する図

符号の説明

[0066] 100 送信機

101 確認要求受付部

102 識別情報確認部

103 更新情報確認部

104 確認応答部

105 更新情報作成・更新部

200、400、600 受信機

201 確認パラメータ生成部

202、601 確認要求部

203 確認結果照合部

204、402、602 コンテンツパケット受信部

205、403 コンテンツ利用部

401 リトライ判断部

801 証明書・鍵保持部

802 交換鍵作成部

803 認証・鍵交換部

805 コピー制御情報管理部

806 コンテンツ鍵算出部

807 コンテンツ蓄積部

808 コンテンツ暗号化部

809 コンテンツパケット作成部

810 コンテンツパケット送信部

901 証明書・鍵保持部

902 認証・鍵交換部

903 更新情報格納部

904 コピー制御情報格納部

905 コンテンツ鍵算出部

907 コンテンツ復号部

908 コンテンツパケット解析部

910 HTTPプロトコル部

発明を実施するための最良の形態

[0067] 以下、本発明の正規コンテンツ確認方法について、従来の伝送システムに適応した場合について説明する。なお、以下の各実施の形態において、上述した従来例と同一あるいはそれに相当する処理・構成については、同一符号を用いてその詳細な説明を省略する。

[0068] (実施の形態1)

図1は、本発明の実施の形態1に係るコンテンツ送受信システムで使用される送信機の機能ブロック図である。

[0069] 送信機100は、図8に示す従来の送信機800と同様、証明書・鍵保持部801、交換鍵作成部802、認証・鍵交換部803、コピー制御情報管理部805、コンテンツ鍵算出部806、コンテンツ蓄積部807、コンテンツ暗号化部808、コンテンツパケット作成部809、コンテンツパケット送信部810、およびHTTPプロトコル部811を備える。さらに、確認要求受付部101、識別情報確認部102、更新情報確認部103、確認応答部104、および更新情報作成・更新部105を備える。

[0070] なお、確認要求受付部101、更新情報確認部103、確認応答部104が、それぞれ、本発明の確認要求受付手段、更新情報確認手段、確認応答手段の一例にあたる。

[0071] 確認要求受付部101は、受信機から、更新情報(test_Nc)と任意の数(N=受信機が確認要求のたびに異なる数を指定する)と識別情報とで構成される確認要求を受信する。

[0072] 識別情報確認部102は、受信した確認要求に含まれる識別情報が、正しい受信機であることを示す情報であるかどうかを確認する。ここで、識別情報は、同じく確認要求に含まれる更新情報(Nc)と任意の数(N)、そして、受信機との間で共有されている交換鍵(Kx)を用いて算出されたものであり、同様の算出を行うことにより、送信機において正しい識別情報であるかどうかを確認できる。

[0073] ここで、例えば、識別情報は、交換鍵(Kx)を連結した数をハッシュ関数に入力し、算出されたハッシュ値と更新情報(Nc)と任意の数(N)を加算し、さらにハッシュ関数に入力して得た値(160ビット)の下位80ビットとする。ハッシュ値は擬似的な乱数のような値をとり、これをもとに原文を再現することはできないので、不当な機器がこの識別情報から交換鍵(Kx)を解読することはできない。

[0074] なお、確認要求が、本発明の正規確認要求の一例にあたり、識別情報が、本発明の識別メッセージの一例にあたる。

[0075] 更新情報作成・更新部105は、従来の送信機800の更新情報作成・更新部804と同様、更新情報(Nc)を新規作成あるいは更新すると同時に、更新前の更新情報(pre_

Nc)を保持する。

[0076] 更新情報確認部103は、受信した確認要求に含まれる更新情報(test_Nc)が、現在、送信機100がコンテンツ送信のために使用中の更新情報と一致するかどうかを確認する。ここで、使用中の更新情報としては、更新情報作成・更新部105で管理されている更新情報(Nc)あるいは直前の更新情報(pre_Nc)をさす。また、更新情報が短い期間で変更されることを考慮し、それまでに使用した複数の更新情報を直前の更新情報として保持しても良い。

[0077] ここで更新情報(test_Nc)との一致を確認するために用いる使用中の更新情報が、本発明の所定の更新情報の一例にあたる。そして、それまでに使用した複数の更新情報が、本発明の、所定回数更新前の更新情報の一例にあたる。

[0078] 確認応答部104は、識別情報確認部102及び更新情報確認部103で是と判定した場合、受信機から受け取った更新情報(test_Nc)と任意の数(N)、そして、受信機との間に共有されている交換鍵(Kx)を用いて了承メッセージを作成し、当該受信機に送信する。

[0079] ここで、例えば、了承メッセージは、下記のように算出される。交換鍵(Kx)を連結した数をハッシュ関数に入力し、ハッシュ値を算出する。算出されたハッシュ値と受信機からの更新情報(test_Nc)と任意の数(N)を加算し、さらにハッシュ関数に入力し得られた値(160ビット)の上位80ビットを了承メッセージに用いる。

[0080] 一方、識別情報確認部102あるいは更新情報確認部103で否と判定した場合、確認応答部104は、非了承メッセージを作成し、当該受信機に送信する。

[0081] 非了承メッセージは、その目的として了承メッセージと異なる値を利用すればよい。例えば、了承メッセージと同様にして得られた値の下位80ビットを用いてもよい。また、了承メッセージと同様にハッシュ値を算出する際に用いる任意の数(N)を変更(例えば1を加算)して得られた値の上位80ビットを用いてもよい。

[0082] 図2は、実施の形態1に係るコンテンツ送受信システムで使用される受信機の機能ブロック図である。

[0083] 受信機200は、図9に示した従来の受信機900と同様、証明書・鍵保持部901、認証・鍵交換部902、更新情報格納部903、コピー制御情報格納部904、コンテンツ

鍵算出部905、コンテンツ復号部907、コンテンツパケット解析部908、およびHTTPプロトコル部910を備える。さらに、確認パラメータ生成部201、確認要求部202、確認結果照合部203、コンテンツパケット受信部204、およびコンテンツ利用部205を備える。

[0084] なお、確認要求部202および確認結果照合部203が、それぞれ本発明の確認要求手段および確認結果照合手段の一例にあたる。

[0085] ここで、確認パラメータ生成部201は、確認要求のたびに異なる数(N)を生成する。そして、更新情報(Nc)と作成した任意の数(N)、および、送信機との間に共有されている交換鍵(Kx)を用いて識別情報を算出する。識別情報の算出方法は前述しているため省略する。

[0086] 確認要求部202は、更新情報格納部903に格納されている更新情報(現在受信している暗号化コンテンツに付随してきたNcであり、Test_Ncとなる)と、確認パラメータ生成部201で作成された任意の数(N)と、識別情報とで構成される確認要求を送信機へ送信する。

[0087] 確認結果照合部203は、送信機から受信した応答メッセージが、了承メッセージであるかどうかを確認する。ここで、了承メッセージかどうかを確認するために、送信した更新情報(test_Nc)と任意の数(N)、および送信機との間に共有されている交換鍵(Kx)を用いて、送信機の確認応答部104が了承メッセージを算出したのと同様の方法で了承メッセージを算出し、送信機から受信した応答メッセージと比較する。了承メッセージの算出方法は前述しているため省略する。

[0088] コンテンツパケット受信部204は、確認結果照合部203で判定された結果を受け、送信機から受信した応答メッセージが了承メッセージではないと判定された場合には、そのコンテンツを含むHTTPレスポンスの終了まで、そのボディとして受信しているコンテンツパケットを破棄する。送信機から受信した応答メッセージが了承メッセージであった、すなわち正規の送信機から送信されていると判定された場合には、正しいコンテンツを受信していると判断し、そのままコンテンツの受信を継続する。

[0089] コンテンツ利用部205は、確認結果照合部203で判定された結果を受け、送信機から受信した応答メッセージが了承メッセージではないと判定された場合には、その

コンテンツの利用を中止する。送信機から受信した応答メッセージが了承メッセージであった、すなわち正規の送信機から送信されていると判定された場合には、正しいコンテンツを受信していると判断し、そのままコンテンツの利用を継続する。

[0090] 図3は、図1の送信機100および図2の受信機200を備えた実施の形態1のコンテンツ送受信システムにおける処理手順(プロトコル)を示す図である。認証・鍵の共有やコンテンツのリクエストおよび受信の処理手順は、前述した従来例の図10での記載と同一であり省略する。

[0091] まず、図2および図3を用いて、受信機200が行う、受信コンテンツが正規であるかどうかを確認するプロトコル動作について説明する。

[0092] ステップS321:コンテンツ利用部205にて、復号コンテンツの利用を開始する。

[0093] ステップS322:確認パラメータ生成部201にて、任意の数(N)と識別情報を作成する。ここで、Nは直前に実施した確認要求で使用した数と等しくならないように作成される。

[0094] ステップS323:確認要求部202にて、コンテンツに付随していた更新情報(Nc)と任意の数(N)と識別情報とを用いた確認要求を作成し、送信する。

[0095] ステップS324:確認結果照合部203にて、送信機100より、応答メッセージを受信する。

[0096] ステップS325:確認結果照合部203にて、受信した応答メッセージが了承メッセージであるかどうかを確認する。了承メッセージであれば、ステップS326に進み、コンテンツの利用を継続する。了承メッセージでなければ、ステップS327に進み、コンテンツの利用を中止する。

[0097] ステップS326:コンテンツ利用部205にて、復号されているコンテンツの利用を継続する。

[0098] ステップS327:コンテンツ利用部205にて、コンテンツの利用を中止し、コンテンツパケット受信部204にて、受信中のコンテンツパケットを破棄する。

[0099] 次に、図1および図3を用いて、送信機100が行う、受信機が正規コンテンツを受信しているかどうかを確認するためのプロトコル動作について説明する。

[0100] ステップS311:確認要求受付部101にて、受信機より、確認要求を受信する。

[0101] ステップS312:識別情報確認部102にて、受信した確認要求に含まれる識別情報が正しいかどうかを判断する。正しければステップS313に進み、更新情報の確認を行う。正しくなければステップS316に進み、非了承メッセージを作成する。

[0102] ステップS313:更新情報確認部103にて、受信した確認要求に含まれる更新情報が使用中とみなせるかどうかを判断する。使用中であれば、ステップS314に進み、了承メッセージを作成する。使用中でなければ、ステップS316に進み、非了承メッセージを作成する。

[0103] ステップS314:確認応答部104にて、受信機200から受け取った更新情報と任意の数(N)、および受信機との間に共有されている交換鍵(Kx)を用いて了承メッセージを作成する。

[0104] ステップS316:確認応答部104にて、了承メッセージとは異なる非了承メッセージを作成する。そのままステップS315に進む。

[0105] ステップS315:確認応答部104にて、応答メッセージ(了承メッセージまたは非了承メッセージ)を送信する。

[0106] なお、ステップS323が、本発明の確認要求ステップの一例にあたり、ステップS325が、本発明の正規コンテンツ判定ステップの一例にあたる。また、ステップS313が本発明の更新情報照合ステップの一例にあたり、ステップS314とステップS315を合わせた処理が、本発明の了承メッセージ送信ステップの一例にあたる。

[0107] 更新情報は、送信機により所定のルールに従って、更新される。従って、不当な機器がコンテンツのすり替えを行った場合、すりかえられたコンテンツに付随している更新情報と、送信機がその時点で保持している更新情報は一致しない。従って、送信機は、受信機から送信されてきた確認要求に含まれる更新情報から、当該受信機が現在、正しいコンテンツを受信しているかどうかを確認できる。

[0108] また、その確認結果通知である了承メッセージが、正当な送信機と当該受信機の間であらかじめ共有された交換鍵を用いて作成されるため、受信機は、受信した了承メッセージが、正当な送信機から送られてきたものかどうかを確認できる。これにより、不当なりすまし機器からのすり替えコンテンツを判別することができる。

[0109] また、送信機における更新情報の更新は、内部処理のため、直前の更新情報が付

加されたコンテンツを受信機が受信するよりも早いタイミングで行われることが考えられるため、直前の更新情報についても了承対象とすることにより、正しいコンテンツの送受信に関して誤った確認を行う頻度を軽減するという効果が得られる。

[0110] また、確認要求の度に異ならせる数も用いることにより、例えば、不正な機器が、送信機と受信機の間で交換される更新情報と了承メッセージの組み合わせを記憶しておいて、受信機がなりすまし機器からのすり替えコンテンツ受信中に確認要求を送信したときに、不正な機器が記憶しておいたその同じ確認要求に対応する了承メッセージを送信したとしても、受信機における識別の成功を防ぐことができる。

[0111] また、確認要求にも、正当な送信機と当該受信機の間であらかじめ共有された交換鍵を用いて作成した識別情報を含めることにより、不正な機器が、現在使用中の更新情報を当該送信機に送信しても対応する了承メッセージを獲得できなくすることができるため、受信機がなりすまし機器からのすり替えコンテンツ受信中に、受信機における識別の成功を防ぐことができる。

[0112] また、受信機が、了承メッセージを受信できない場合には、すなわち、非了承メッセージを受信した場合には、受信コンテンツを利用しないことにより、不正な機器が邪魔することにより、不当なりすまし機器からのすり替えコンテンツがユーザに利用可能となるのを防ぐことができる。

[0113] なお、実施の形態1では、送信機、受信機間でHTTPプロトコルを用いて、コンテンツの送受信を行う場合について説明しているが、本発明はこれに限らず、例えば、送信機がコンテンツをリアルタイムでストリーミング配信する場合についても適応できる。

[0114] (実施の形態2)

図4は、本発明の実施の形態2に係るコンテンツ送受信システムで使用される受信機の機能ブロック図である。実施の形態2のコンテンツ送受信システムで使用される送信機の構成は、実施の形態1と同様であり、図1に示す通りである。

[0115] 実施の形態2では、実施の形態1と異なる部分について説明する。実施の形態2では、受信機から送信機に対し確認要求を最大所定回数までリトライする。

[0116] 受信機400は、図2に示す実施の形態1の受信機200と同様、証明書・鍵保持部901、認証・鍵交換部902、更新情報格納部903、コピー制御情報格納部904、コン

テンツ鍵算出部905、コンテンツ復号部907、コンテンツパケット解析部908、HTTPプロトコル部910、確認パラメータ生成部201、確認要求部202、および確認結果照合部203を備える。さらに、リトライ判断部401、コンテンツパケット受信部402、およびコンテンツ利用部403を備える。

[0117] リトライ判断部401は、確認結果照合部203で否と判定された場合に、リトライを行うかどうかを判断する。ここで、例えば、確認要求を行った回数でさらにリトライを行うかどうかを判断するとし、同じ更新情報を用いて連続して既に2回確認要求を行っている場合には、これ以上リトライを行わないと判断する。

[0118] コンテンツパケット受信部402は、リトライ判断部401を経由し、確認結果照合部203で判定された結果を受け、送信機から受信した応答メッセージが了承メッセージではないと判定された場合には、そのコンテンツを含むHTTPレスポンスの終了まで、そのボディとして受信しているコンテンツパケットを破棄する。送信機から受信した応答メッセージが了承メッセージである、すなわち正規の送信機から送信されていると判定された場合には、正しいコンテンツを受信していると判断し、そのままコンテンツの受信を継続する。

[0119] コンテンツ利用部403は、リトライ判断部401を経由し、確認結果照合部203で判定された結果を受け、送信機から受信した応答メッセージが了承メッセージではないと判定された場合には、そのコンテンツの利用を中止する。送信機から受信した応答メッセージが了承メッセージであった、すなわち正規の送信機から送信されていると判定された場合には、正しいコンテンツを受信していると判断し、そのままコンテンツの利用を継続する。

[0120] 図5は、図1の送信機100および図4の受信機400を備えた実施の形態2のコンテンツ送受信システムにおける処理手順(プロトコル)を示す図である。

[0121] 図4および図5を用いて、受信機400が行う、受信コンテンツが正規であるかどうかを確認するプロトコル動作について説明する。ステップS321～ステップS324までは、前述の実施の形態1の図3での記載と同一であり、省略する。

[0122] ステップS325:確認結果照合部203にて、受信した応答メッセージが了承メッセージであるかどうかを確認する。了承メッセージであれば、ステップS326に進み、コン

テンツの利用を継続する。了承メッセージでなければ、ステップS501に進み、リトライするかどうかを判断する。

[0123] ステップS326:コンテンツ利用部403にて、復号されているコンテンツの利用を継続する。

[0124] ステップS501:リトライ判断部401にて、確認要求のリトライを行うかどうかを判断する。リトライする場合には、ステップS322に戻り、確認要求送信のための準備をする。リトライしない場合には、S327に進む。

[0125] ここでは、「同じ更新情報を用いたリトライは2回まで」とリトライ判断部401に設定されているので、2回目の確認要求のリトライ送信後に再度ステップS501の判定が行われ場合には、ステップS322に戻らずS327に進むことになる。

[0126] なお、ステップS501が、本発明の確認要求リトライ送信ステップの一例にあたる。そして、ここでリトライ判断部401に設定されている2回というリトライの最大所定回数が、本発明の、確認要求リトライステップで正規確認要求を繰り返し送信する所定回数の一例にあたる。

[0127] ステップS327:コンテンツ利用部403にて、コンテンツ利用を中止し、コンテンツパケット受信部402にて、受信中のコンテンツパケットを破棄する。

[0128] 従って、実施の形態2の受信機400を用いることにより、リトライにより正しいコンテンツの送受信に関して誤った確認を行う頻度を軽減するという効果が得られるとともに、最大リトライ回数を設けることにより、不正な機器が邪魔することにより受信機が永遠にリトライしている間コンテンツが利用できてしまう(視聴できる)、ということも防ぐことができる。

[0129] なお、実施の形態2では、リトライの最大所定回数を2回として説明したが、使用されるコンテンツ送受信システムの使用状況や使用環境などに応じて、適切な回数を設定すればよい。

[0130] また、実施の形態2では、リトライの制限を回数としたが、期間(時間)で設けてもよく、その場合にも同様の効果が得られる。

[0131] リトライの制限として、期間をリトライ判断部401に設定した場合には、その設定した期間中にステップS501の判定が行われた場合には、ステップS322に戻り、その設

定した期間経過後にステップS501の判定が行われた場合には、ステップS322に戻らずS327に進むことになる。ここでリトライの制限としてリトライ判断部401に設定する期間が、本発明の、確認要求リトライステップで正規確認要求を繰り返し送信する所定期間の一例にあたる。

[0132] また、実施の形態2では、リトライ時に用いる更新情報は、最初の確認要求で使用する更新情報と同一固定としたが、受信コンテンツと共に変化していく更新情報と同期させてもよい。

[0133] (実施の形態3)

図6は、本発明の実施の形態3に係るコンテンツ送受信システムで使用される受信機の機能ブロック図である。実施の形態3のコンテンツ送受信システムで使用される送信機の構成は、実施の形態1と同様であり、図1に示す通りである。

[0134] 実施の形態3では、実施の形態1と異なる部分について説明する。実施の形態3では、受信機が受信コンテンツの利用を中止した後も、了承メッセージを受信できるまで、確認要求を行う。

[0135] 受信機600は、図4に示す実施の形態2の受信機400と同様、証明書・鍵保持部901、認証・鍵交換部902、更新情報格納部903、コピー制御情報格納部904、コンテンツ鍵算出部905、コンテンツ復号部907、コンテンツパケット解析部908、HTTPプロトコル部910、確認パラメータ生成部201、確認結果照合部203、リトライ判断部401、およびコンテンツ利用部403を備える。さらに、確認要求部601およびコンテンツパケット受信部602を備える。

[0136] 確認要求部601は、一旦コンテンツの利用を中止した後も、確認要求を送信機へ送信する。ここで、例えば、確認要求を送信するタイミングは、あらかじめ設定したリトライ再開時間の繰り返しとする。

[0137] コンテンツパケット受信部602は、確認要求部601からリクエストがあれば、受信中のコンテンツパケットを破棄せずに、コンテンツパケット解析部908へ渡す。これは、確認要求作成に必要な、現在受信中のコンテンツに付随する更新情報(Nc)とコピー制御情報(E_EMI)を格納するためである。

[0138] 図7は、図1の送信機100および図6の受信機600を備えた実施の形態3のコンテ

ンツ送受信システムにおける処理手順(プロトコル)を示す図である。

[0139] 図6および図7を用いて、受信機600が行う、受信コンテンツが正規であるかどうかを確認するプロトコル動作について説明する。ステップS321～ステップS327までは、前述の実施の形態2の図5での記載と同一であり、省略する。

[0140] ステップS701:確認要求部601にて、前回の確認要求を送信してからリトライ再開時間が経過しているかどうかを確認し、経過していれば、コンテンツパケット受信部602での受信コンテンツパケットの破棄を中止し、ステップS322に戻り、確認要求を送信する。なお、ステップS701が、本発明の確認要求再送信ステップの一例にあたる。

[0141] 従って、不正な機器の成りすましが終われば、直ちに受信を再開できる。

[0142] なお、確認要求部601には、リトライを無制限に行わないよう、リトライを再開させる制限回数または制限時間が設定されてもよい。ステップS701における連続した判定を、連続する回数または最初の判定からの経過時間で制限している。その制限回数または制限時間を越えた場合には、受信機600からのコンテンツ要求等が送信されるまで、確認要求のリトライ送信は中止させる。

[0143] ここで確認要求部601に設定する制限回数または制限時間が、本発明の、確認要求再送信ステップで正規確認要求を繰り返し送信する所定の制限回数または所定の制限期間の一例にあたる。

[0144] このリトライを再開させるために設定する制限回数または制限時間を、十分に多くの回数または十分に長い時間に設定することにより、不正な機器の成りすましが終わった後に、正規の送信機からの了承メッセージを確実に受信させることができる。

[0145] また、ユーザによる停止指示など、あらかじめ設定された停止条件が発生したらリトライをやめてもよい。

[0146] なお、実施の形態3では、コンテンツの利用中止後の確認要求の発行を、リトライ再開時間の繰り返しとしたが、ユーザの入力指定であってもよい。

[0147] 以上に説明したように、本発明の正規コンテンツ確認方法を用いると、送信機は、受信機から送信された更新情報から、当該受信機が現在正しいコンテンツを受信しているかどうかを確認できる。また、その確認結果通知である了承メッセージが、正当

な送信機と当該受信機の間であらかじめ共有された交換鍵を用いて作成されるため、受信機は、受信した了承メッセージが、正当な送信機から送られたものかどうかを確認できる。これにより、不当なりすまし機器からのすり替えコンテンツを判別することができる。

[0148] また、送信機における更新情報の更新は、内部処理のため、直前の更新情報が付加されたコンテンツを受信機が受信するよりも早いタイミングで行われることが考えられるため、現在使用中の更新情報だけではなく直前の更新情報についても了承対象とすることにより、正しいコンテンツの送受信に関して誤った確認を行う頻度を軽減するという効果が得られる。

[0149] また、確認要求の度に異ならせた数も用いることにより、例えば、不正な機器が、送信機と受信機の間で交換される更新情報と了承メッセージの組み合わせを記憶しておいて、受信機がなりすまし機器からのすり替えコンテンツ受信中に確認要求を送信したときに、不正な機器が記憶しておいたその同じ確認要求に対応する了承メッセージを送信したとしても、受信機における識別の成功を防ぐことができる。

[0150] また、確認要求に、正当な送信機と当該受信機の間であらかじめ共有された交換鍵を用いて作成されたメッセージを含めることにより、不正な機器が、現在使用中の更新情報を当該送信機に送信しても対応する了承メッセージを獲得できなくすることができるため、受信機がなりすまし機器からのすり替えコンテンツ受信中に、識別を成功させるのを防ぐことができる。

[0151] またここで、受信機は、了承メッセージを受信できない場合には、受信コンテンツを利用しないことにより、不当なりすまし機器からのすり替えコンテンツがユーザに利用可能となるのを防ぐことができる。

[0152] また、受信機は、了承メッセージを受信できない場合には、所定期間あるいは所定回数リトライを行った後に受信コンテンツを利用しないことにより、不正な機器が邪魔することにより、受信機が永遠にリトライしている間コンテンツが利用できてしまう(視聴できる)のを防ぐことができる。

[0153] また、受信機は、受信コンテンツの利用を中止した後も、了承メッセージを受信できるまで確認要求を行うことにより、不正な機器のなりすましが終われば、直ちに受信を

再開できるという効果が得られる。

[0154] このように、本発明の正規コンテンツ確認方法、コンテンツ送受信システム、送信機および受信機を用いることにより、不当ななりすまし機器からのすり替えコンテンツの受信を防止することができる。

[0155] なお、本発明のプログラムは、上述した本発明の正規コンテンツ確認方法の、前記受信機にて前記正規確認要求を送信する前記確認要求ステップ、前記送信機にて前記更新情報が前記所定の更新情報であるかどうかを照合する前記更新情報照合ステップ、前記送信機にて前記了承メッセージを作成し前記受信機に送信する前記了承メッセージ送信ステップ、前記受信機にて前記送信機からの前記了承メッセージを受信した場合に前記送信機が正規の送信機であると確認する前記正規コンテンツ判定ステップの、全部または一部のステップの動作をコンピュータにより実行させるためのプログラムであって、コンピュータと協働して動作するプログラムである。

[0156] また、本発明の記録媒体は、上述した本発明の正規コンテンツ確認方法の、前記受信機にて前記正規確認要求を送信する前記確認要求ステップ、前記送信機にて前記更新情報が前記所定の更新情報であるかどうかを照合する前記更新情報照合ステップ、前記送信機にて前記了承メッセージを作成し前記受信機に送信する前記了承メッセージ送信ステップ、前記受信機にて前記送信機からの前記了承メッセージを受信した場合に前記送信機が正規の送信機であると確認する前記正規コンテンツ判定ステップの、全部または一部のステップの全部または一部の動作をコンピュータにより実行させるためのプログラムを記録した記録媒体であり、コンピュータにより読み取り可能かつ、読み取られた前記プログラムが前記コンピュータと協働して利用される記録媒体である。

[0157] なお、本発明の上記「一部のステップ」とは、それらの複数のステップの内の、一つまたは幾つかのステップを意味する。

[0158] また、本発明の上記「ステップの動作」とは、前記ステップの全部または一部の動作を意味する。

[0159] また、本発明のプログラムの一利用形態は、コンピュータにより読み取り可能な記録媒体に記録され、コンピュータと協働して動作する態様であっても良い。

[0160] また、記録媒体としては、ROM等が含まれる。

[0161] また、上述した本発明のコンピュータは、CPU等の純然たるハードウェアに限らず、ファームウェアや、OS、更に周辺機器を含むものであっても良い。

[0162] なお、以上説明した様に、本発明の構成は、ソフトウェア的に実現しても良いし、ハードウェア的に実現しても良い。

産業上の利用可能性

[0163] 本発明の正規コンテンツ確認方法、コンテンツ送受信システム、送信機、および受信機等は、ネットワーク上で、不正な機器が、正当な送信機と受信機の間の通信を監視し受信機に不当なコンテンツを送りつけるといった攻撃を逃れるためのコンテンツ確認技術として有用である。

請求の範囲

[1] 受信機からのコンテンツ要求に応じて、ネットワークに接続された送信機が、所定のタイミングで更新する更新情報であってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信するコンテンツ送受信システムにおける、正規コンテンツ確認方法であって、

前記受信機にて、前記送信機から受信した前記更新情報を少なくとも含む正規確認要求を送信する確認要求ステップと、

前記送信機にて、前記受信機から受信した前記正規確認要求に含まれる前記更新情報が、所定の更新情報であるかどうかを照合する更新情報照合ステップと、

前記送信機にて、前記更新情報が前記所定の更新情報であると判定した場合には、前記更新情報と、前記送信機および前記受信機の双方であらかじめ共有されている交換鍵とを用いて了承メッセージを作成し前記受信機に送信する、了承メッセージ送信ステップと、

前記受信機にて、前記送信機からの前記了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツであると判断する正規コンテンツ判定ステップとを備えた、正規コンテンツ確認方法。

[2] 前記所定の更新情報は、現在使用中の更新情報または所定回数更新前の更新情報である、請求の範囲第1項に記載の正規コンテンツ確認方法。

[3] 前記確認要求ステップでは、前記受信機は、前記正規確認要求を送信する毎に異ならせた数も前記正規確認要求に含めて送信し、

前記了承メッセージ送信ステップでは、前記送信機は、前記正規確認要求に含まれる前記数も用いて前記了承メッセージを作成する、請求の範囲第1項に記載の正規コンテンツ確認方法。

[4] 前記確認要求ステップでは、前記受信機は、前記交換鍵および前記送信機から送られてきた前記更新情報を用いて作成した識別メッセージも前記正規確認要求に含めて送信し、

前記了承メッセージ送信ステップでは、前記送信機は、前記更新情報が前記所定の更新情報であると判定し、かつ、前記正規確認要求に含まれる前記識別メッセー

ジが、前記送信機自身が前記交換鍵および前記更新情報を用いて作成した識別メッセージと一致することを確認した場合に、前記了承メッセージを前記受信機に送信する、請求の範囲第1項に記載の正規コンテンツ確認方法。

[5] 前記了承メッセージ送信ステップでは、前記送信機は、前記更新情報が前記所定の更新情報ではないと判定した場合には、非了承メッセージを前記受信機に送信し、

前記正規コンテンツ判定ステップでは、前記受信機にて、前記送信機からの前記非了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツではないと判断し前記コンテンツを利用しない、請求の範囲第1項に記載の正規コンテンツ確認方法。

[6] 前記正規コンテンツ判定ステップで、前記受信機が前記了承メッセージを受信できない場合には、前記受信機にて、所定期間、前記正規確認要求を繰り返し送信する確認要求リトライ送信ステップをさらに備え、

前記正規コンテンツ判定ステップでは、前記受信機にて、前記所定期間を過ぎても前記了承メッセージを受信できない場合には、受信したコンテンツを利用しないようにする、請求の範囲第1項に記載の正規コンテンツ確認方法。

[7] 前記正規コンテンツ判定ステップで、前記受信機が前記了承メッセージを受信できない場合には、前記受信機にて、所定回数、前記正規確認要求を繰り返し送信する確認要求リトライ送信ステップをさらに備え、

前記正規コンテンツ判定ステップでは、前記受信機にて、前記正規確認要求を前記所定回数送信しても前記了承メッセージを受信できない場合には、受信したコンテンツを利用しないようにする、請求の範囲第1項に記載の正規コンテンツ確認方法。

[8] 前記正規コンテンツ判定ステップで、前記受信機にて、受信した前記コンテンツを利用しないようにした後に、所定の制限回数または所定の制限期間あるいは所定の停止条件が整うまで、前記正規確認要求を繰り返し送信する、確認要求再送信ステップをさらに備え、

前記正規コンテンツ判定ステップでは、前記受信機にて、受信した前記コンテンツを利用しないようにした後に、前記了承メッセージを受信した場合には、受信したコン

テンツを利用するようにする、請求の範囲第5乃至7のいずれか項に記載の正規コンテンツ確認方法。

[9] コンテンツ要求を送信する受信機と、ネットワークにより前記受信機に接続され、前記受信機からのコンテンツ要求に応じて、所定のタイミングで更新する更新情報であってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信する送信機とを備えたコンテンツ送受信システムにおいて、

前記受信機は、

前記送信機との双方であらかじめ共有されている交換鍵と、前記送信機から受信した前記更新情報とを用いて作成した正規確認要求を送信する確認要求手段と、

前記送信機からの了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツであると判断する確認結果照合手段とを有し、

前記送信機は、

前記受信機から送信されてきた前記正規確認要求を受信する確認要求受付手段と、

受信した前記正規確認要求に含まれる前記更新情報が、所定の更新情報であるかどうかを照合する更新情報確認手段と、

前記更新情報が前記所定の更新情報であると判定した場合には、前記更新情報および前記受信機との双方で共有されている前記交換鍵を用いて前記了承メッセージを作成し、前記受信機に送信する確認応答手段とを有する、コンテンツ送受信システム。

[10] 受信機からのコンテンツ要求に応じて、ネットワークに接続された送信機が、所定のタイミングで更新する更新情報であってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信するコンテンツ送受信システムに用いられる送信機であって、

前記受信機で、前記受信機との双方であらかじめ共有されている交換鍵と、前記送信機から受信した前記更新情報とを用いて作成され、前記受信機から送信されてきた正規確認要求を受信する確認要求受付手段と、

前記受信機から受信した前記正規確認要求に含まれる前記更新情報が、所定の更新情報であるかどうかを照合する更新情報確認手段と、

前記更新情報が前記所定の更新情報であると判定した場合には、前記更新情報と前記交換鍵とを用いて、前記受信機が受信中のコンテンツが正規のコンテンツであるかどうかを判断するための了承メッセージを作成し前記受信機に送信する確認応答手段とを備えた、送信機。

[11] 受信機からのコンテンツ要求に応じて、ネットワークに接続された送信機が、所定のタイミングで更新する更新情報であってコンテンツの暗号化および復号に用いるコンテンツ鍵の作成に必要な前記更新情報を、暗号化されたコンテンツに付随させて送信するコンテンツ送受信システムに用いられる受信機であって、

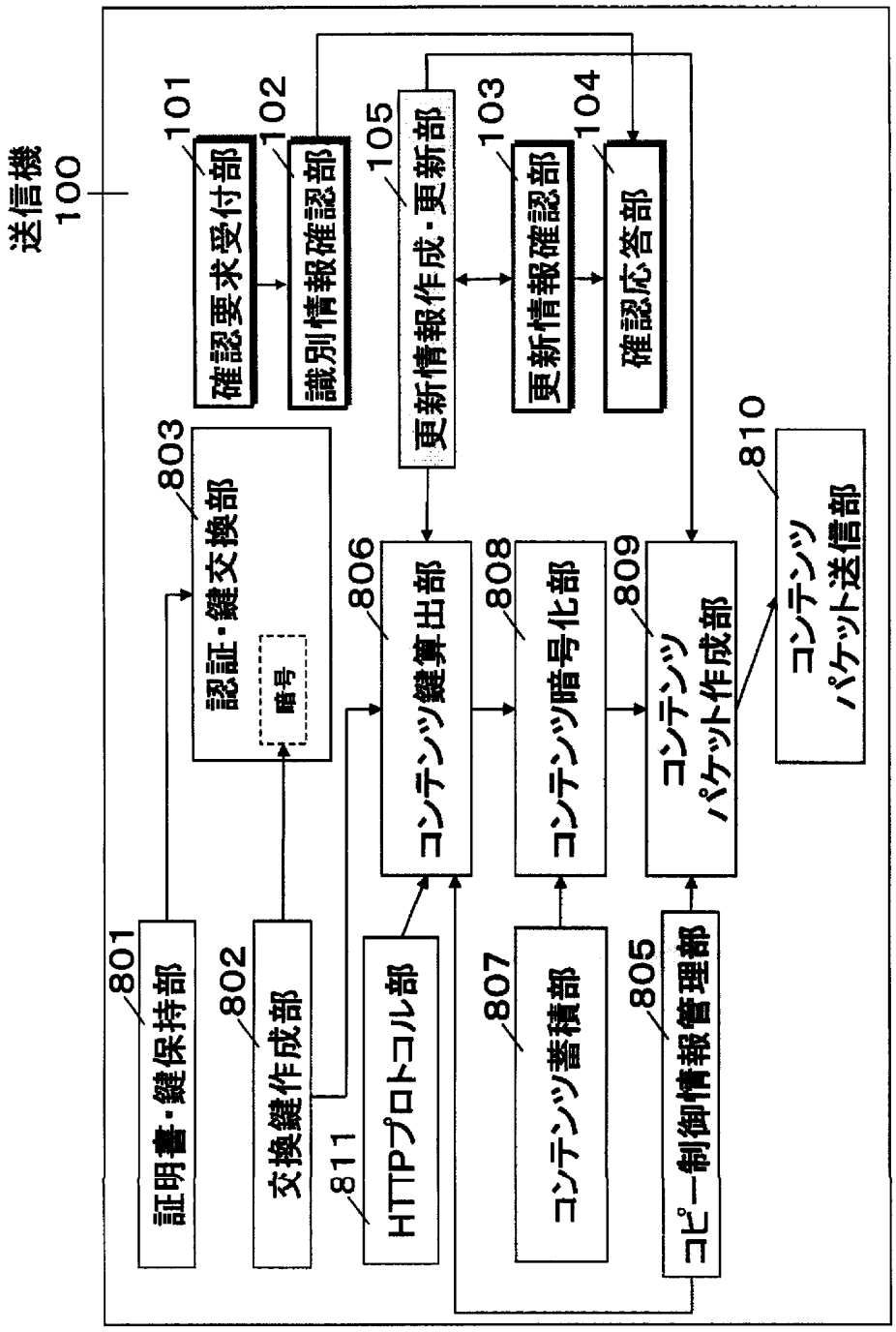
前記送信機との双方であらかじめ共有されている交換鍵と、前記送信機から受信した前記更新情報とを用いて作成した正規確認要求を送信する確認要求手段と、

前記送信機が、受信した前記正規確認要求に含まれる前記更新情報が所定の更新情報であると判定して、前記更新情報および前記交換鍵を用いて作成して送信してきた了承メッセージを受信した場合には、受信中のコンテンツが正規のコンテンツであると判断する確認結果照合手段とを備えた、受信機。

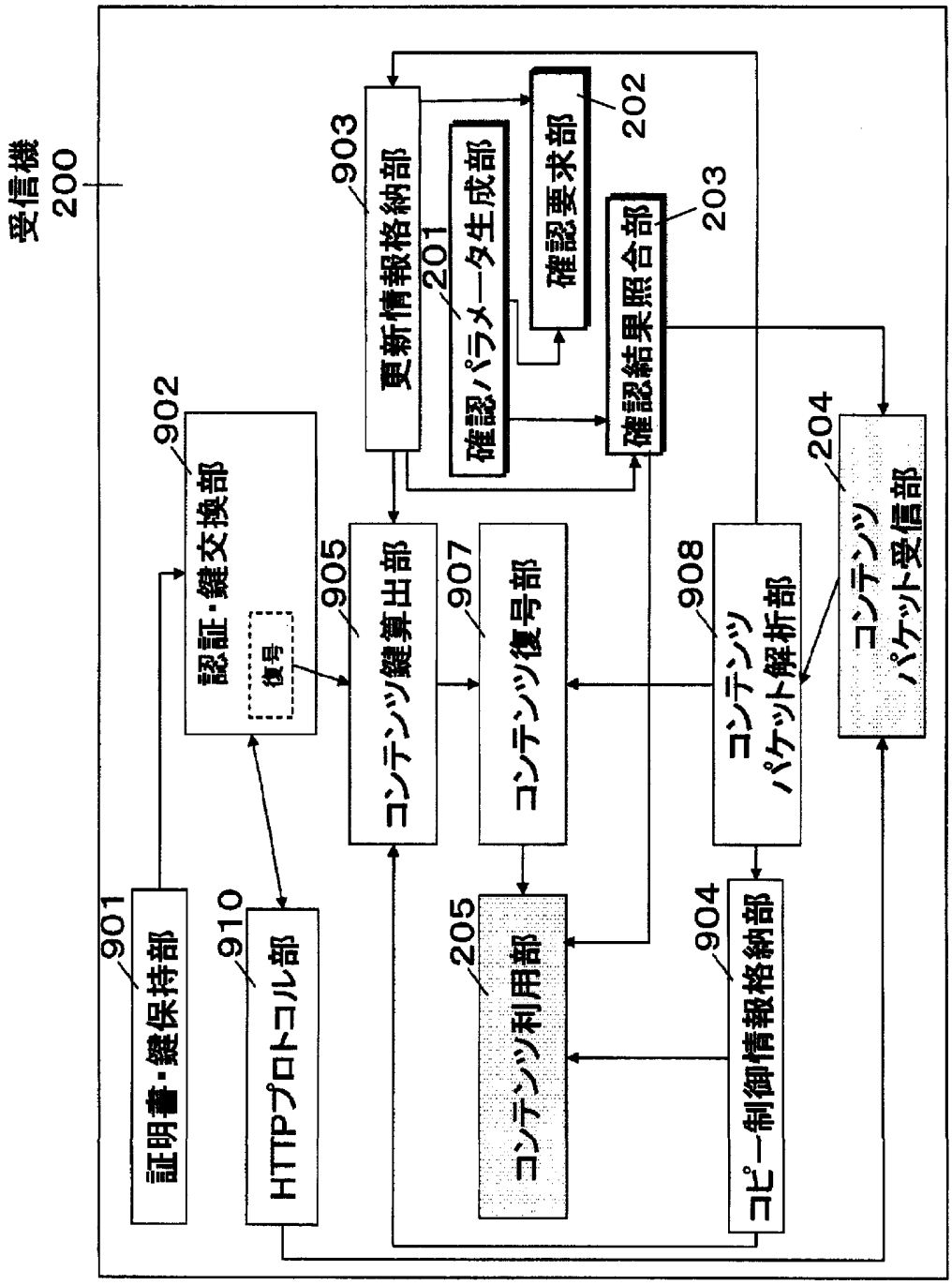
[12] 請求の範囲第1項に記載の正規コンテンツ確認方法の、前記受信機にて前記正規確認要求を送信する前記確認要求ステップ、前記送信機にて前記更新情報が前記所定の更新情報であるかどうかを照合する前記更新情報照合ステップ、前記送信機にて前記了承メッセージを作成し前記受信機に送信する前記了承メッセージ送信ステップ、前記受信機にて前記送信機からの前記了承メッセージを受信した場合に前記送信機が正規の送信機であると確認する前記正規コンテンツ判定ステップ、をコンピュータに実行させるためのプログラム。

[13] 請求の範囲第12項に記載のプログラムを記録した記録媒体であって、コンピュータにより処理可能な記録媒体。

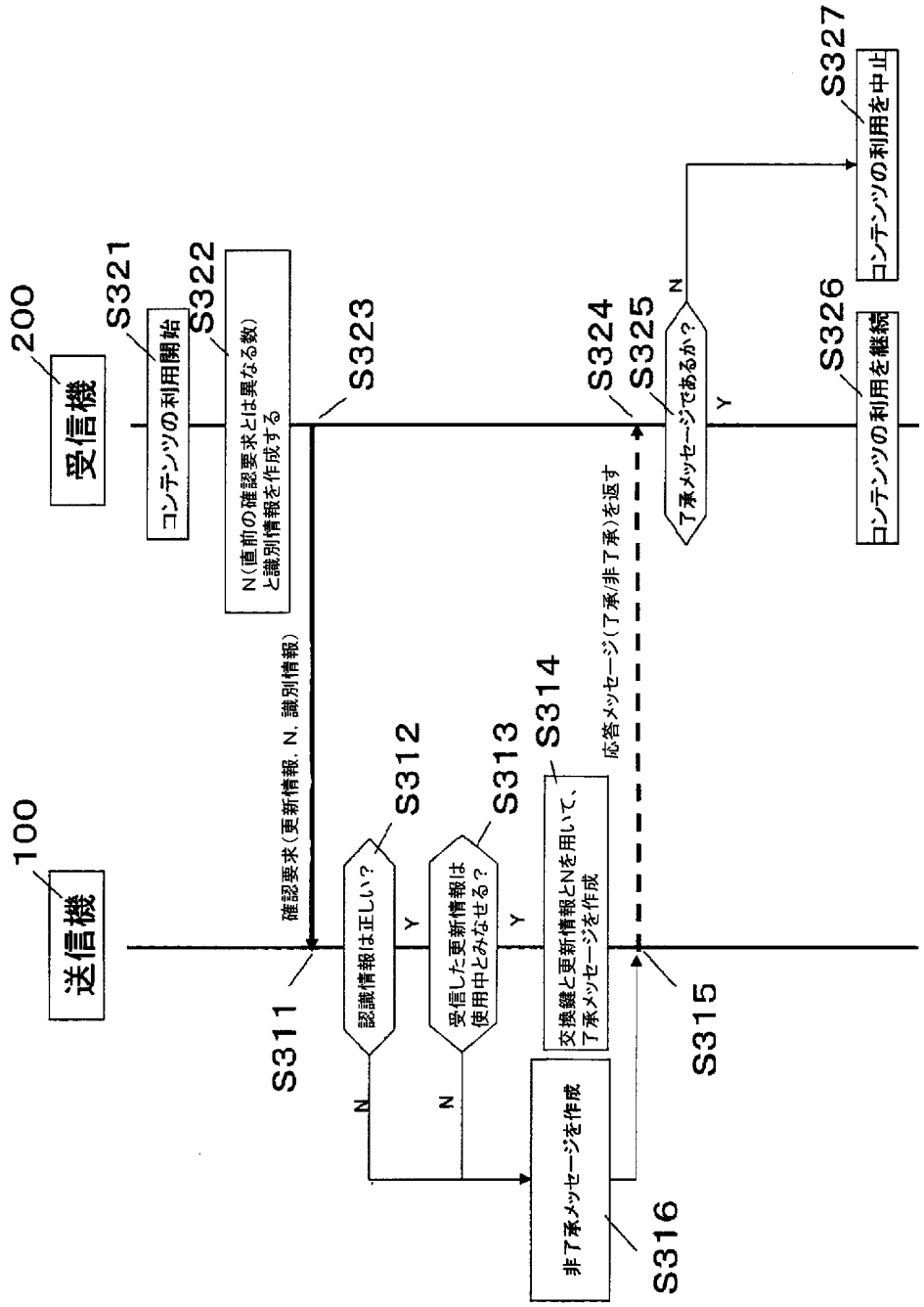
[図1]


送信機
100
101
確認要求受付部
102
識別情報確認部
105
更新情報作成・更新部
103
更新情報確認部
104
確認応答部
803
認証・鍵交換部
暗号
806
コンテンツ鍵算出部
808
コンテンツ暗号化部
809
コンテンツ
パケット作成部
810
コンテンツ
パケット送信部
801
証明書・鍵保持部
802
交換鍵作成部
811
HTTPプロトコル部
807
コンテンツ蓄積部
805
コピー制御情報管理部

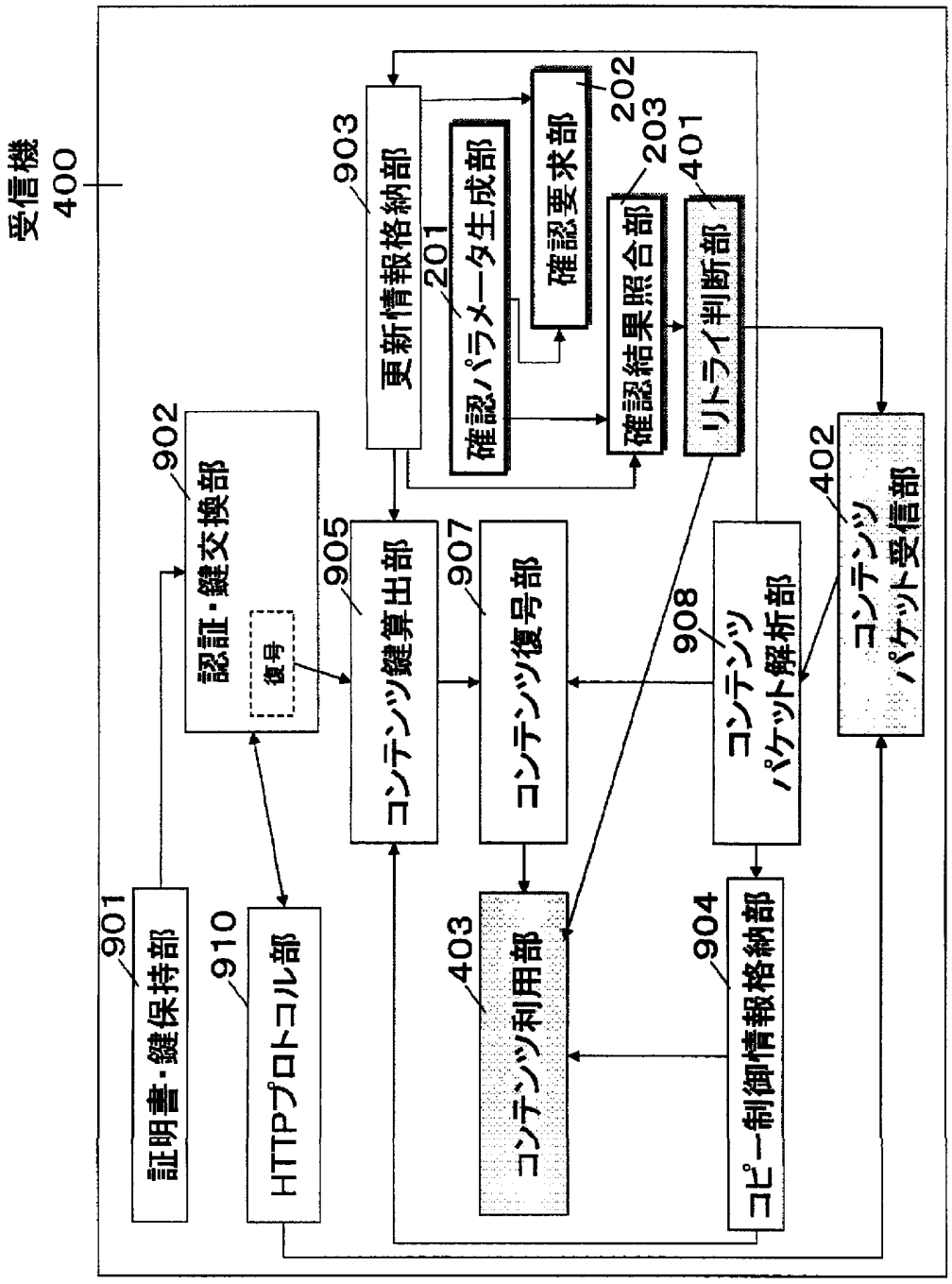
[図2]


受信機
200
証明書・鍵保持部
901
認証・鍵交換部
902
復号
更新情報格納部
903
コピー制御情報格納部
904
コンテンツ鍵算出部
905
コンテンツ
パケット解析部
908
コンテンツ復号部
907
コンテンツ利用部
205
コンテンツ
パケット受信部
204
確認パラメータ生成部
201
確認要求部
202
確認結果照合部
203
HTTPプロトコル部
910

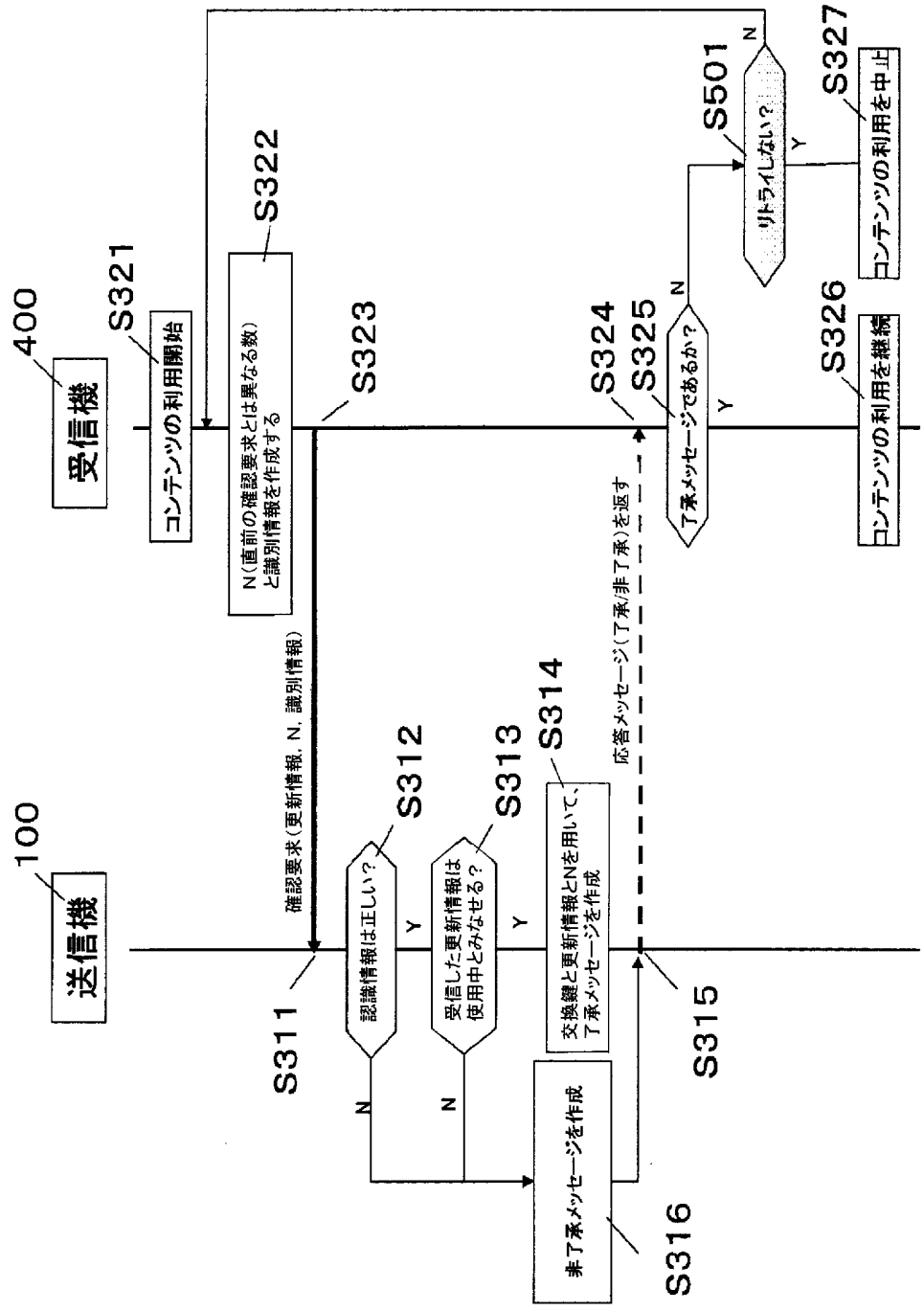
[図3]


100
送信機
200
受信機
S311
確認要求(更新情報, N, 識別情報)
S312
認識情報は正しい?
S313
受信した更新情報は使用中とみなせる?
S314
交換鍵と更新情報とNを用いて、了承メッセージを作成
S315
応答メッセージ(了承/非了承)を返す
S316
非了承メッセージを作成
S321
コンテンツの利用開始
S322
N(直前の確認要求とは異なる数)と識別情報を作成する
S323
S324
S325
了承メッセージであるか?
S326
コンテンツの利用を継続
S327
コンテンツの利用を中止
Y
N

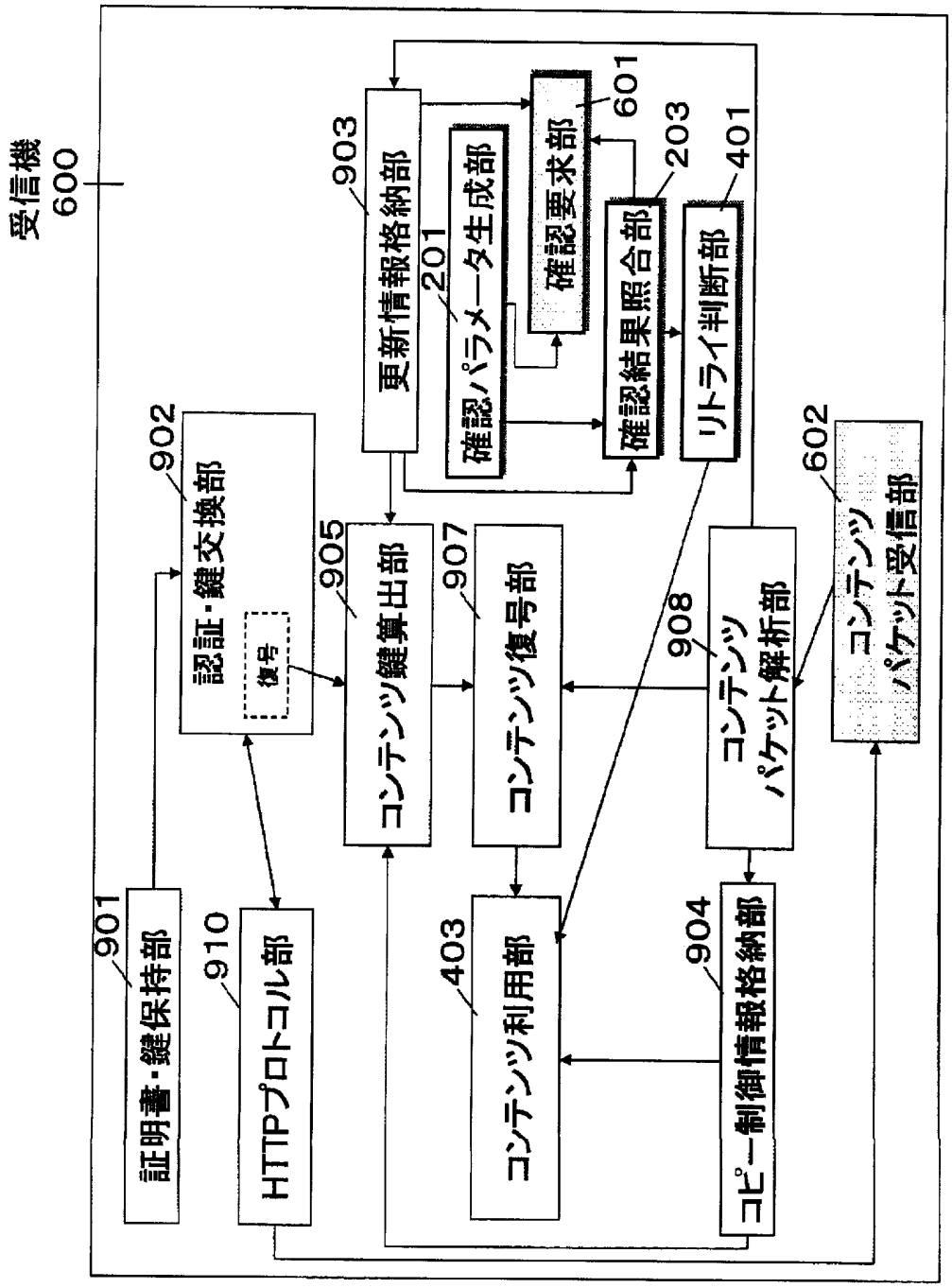
[図4]


受信機
400
903
更新情報格納部
201
確認パラメータ生成部
確認要求部
202
203
確認結果照合部
401
リトライ判断部
902
認証・鍵交換部
復号
905
コンテンツ鍵算出部
907
コンテンツ復号部
908
コンテンツ
パケット解析部
402
コンテンツ
パケット受信部
901
証明書・鍵保持部
910
HTTPプロトコル部
403
コンテンツ利用部
904
コピー制御情報格納部

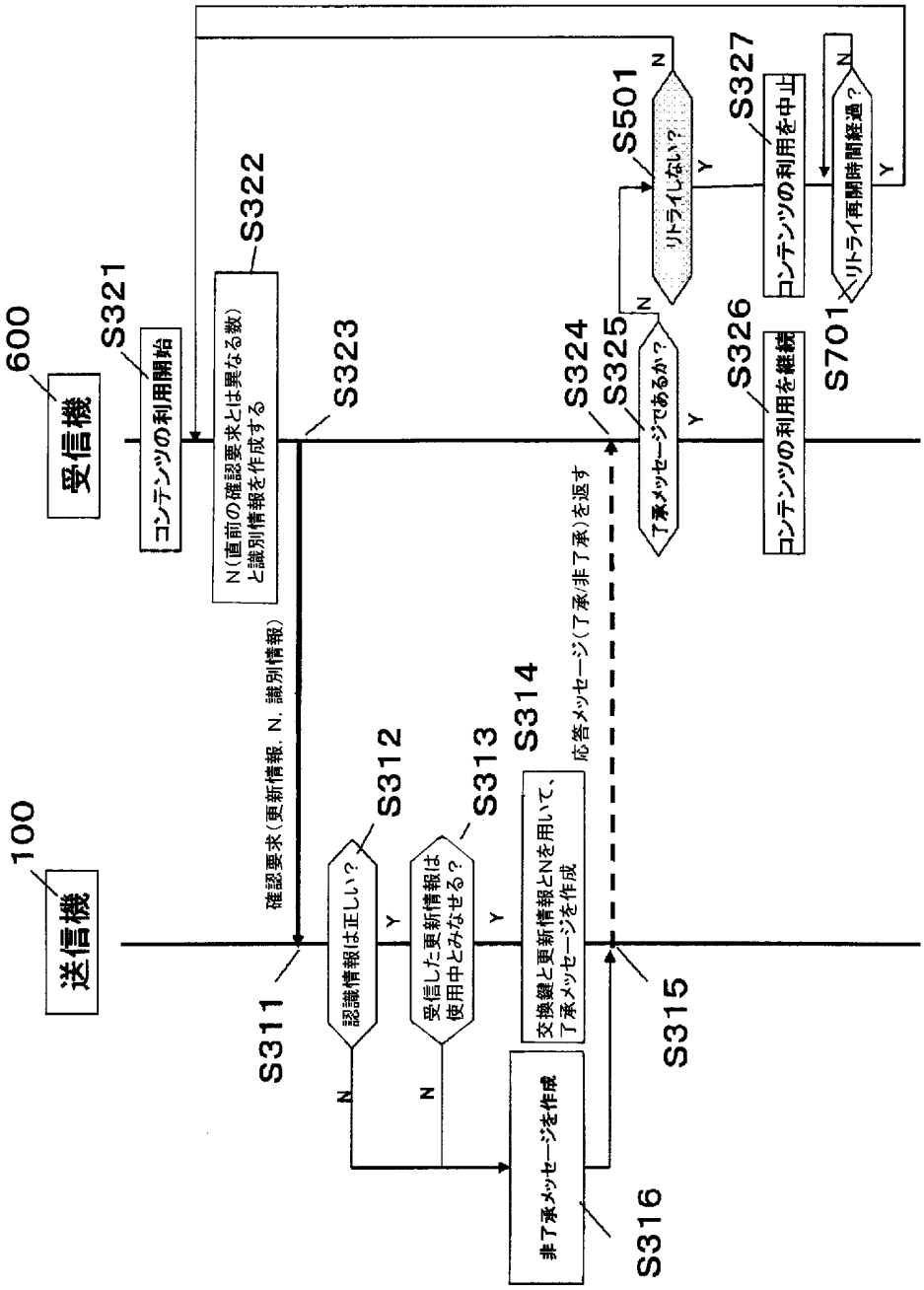
[図5]


400
受信機
100
送信機
S321
コンテンツの利用開始
S322
N(直前の確認要求とは異なる数)と識別情報を作成する
S323
確認要求(更新情報, N, 識別情報)
S311
S312
認識情報は正しい?
S313
受信した更新情報は使用中とみなせる?
S314
交換鍵と更新情報とNを用いて、了承メッセージを作成
S315
応答メッセージ(了承/非了承)を返す
S316
非了承メッセージを作成
S324
S325
了承メッセージであるか?
S326
コンテンツの利用を継続
S501
リトライしない?
S327
コンテンツの利用を中止
Y
N

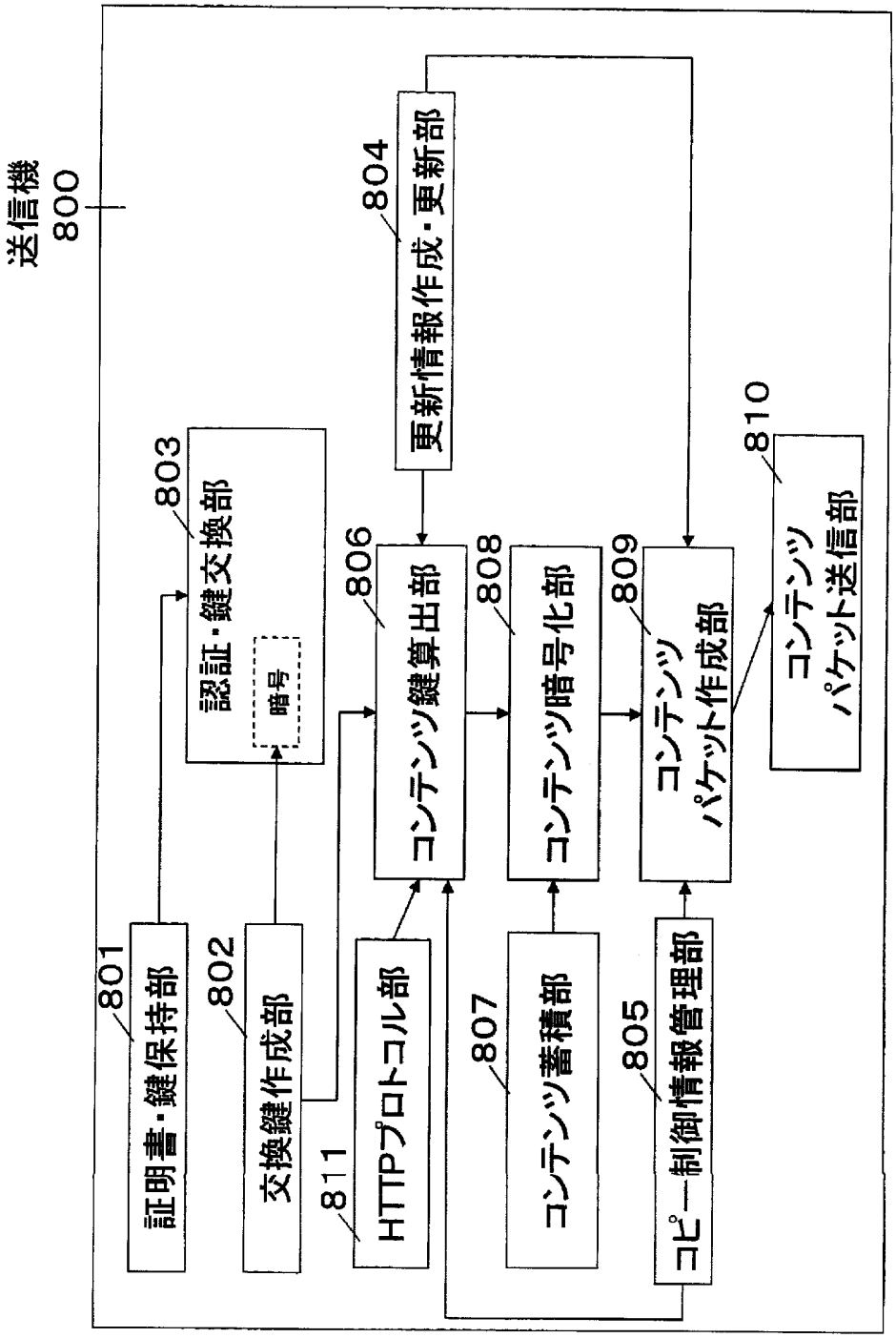
[図6]


受信機
600
証明書・鍵保持部
901
認証・鍵交換部
902
復号
更新情報格納部
903
コピー制御情報格納部
904
コンテンツ鍵算出部
905
コンテンツ復号部
907
コンテンツパケット解析部
908
HTTPプロトコル部
910
コンテンツ利用部
403
確認パラメータ生成部
201
確認要求部
601
確認結果照合部
203
リトライ判断部
401
コンテンツパケット受信部
602

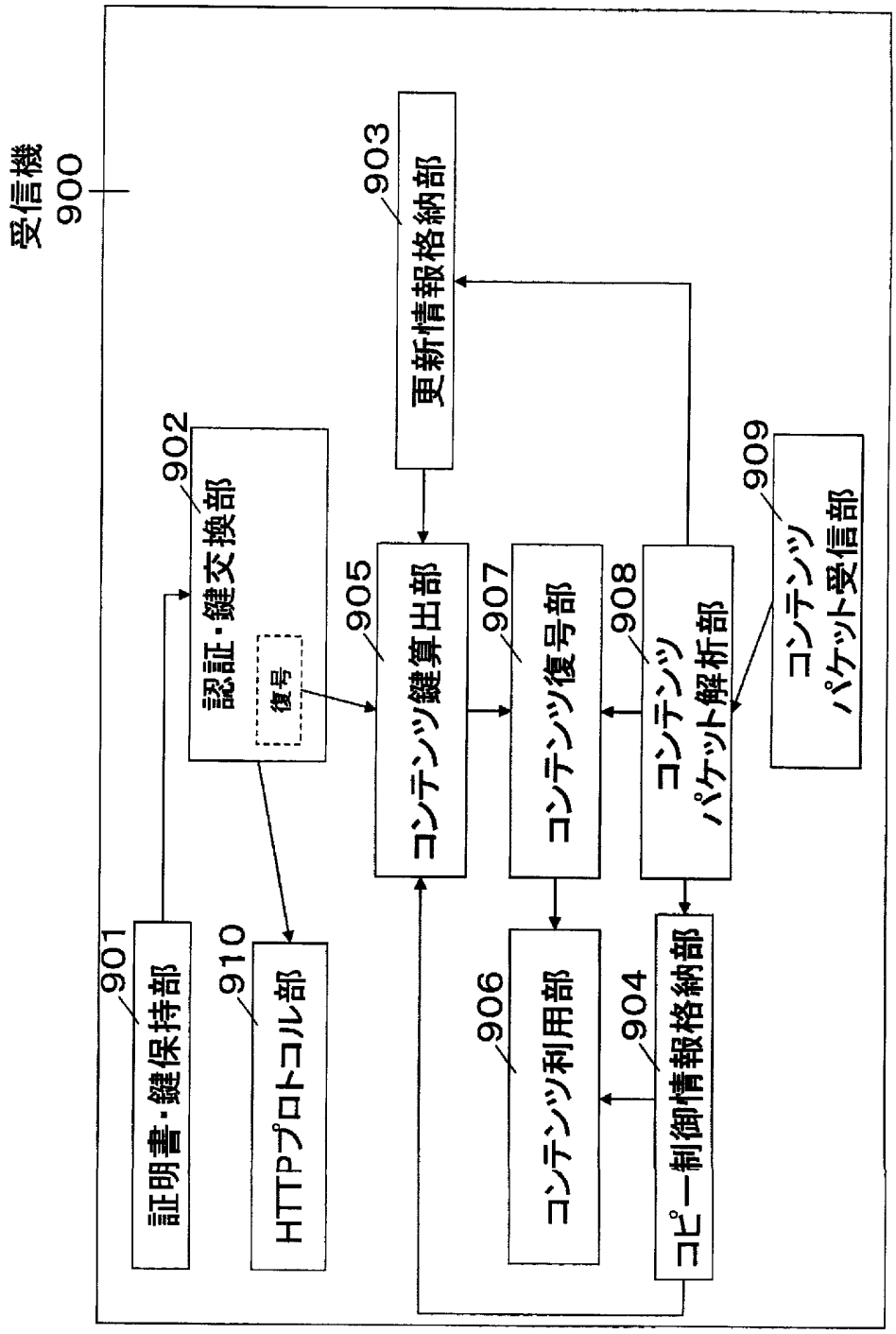
[図7]


100
送信機
600
受信機
S321
コンテンツの利用開始
S322
N(直前の確認要求とは異なる数)と識別情報を作成する
S323
確認要求(更新情報. N. 識別情報)
S311
S312
認識情報は正しい?
S313
受信した更新情報は使用中とみなせる?
S314
交換鍵と更新情報とNを用いて、了承メッセージを作成
S315
応答メッセージ(了承/非了承)を返す
S316
非了承メッセージを作成
S324
S325
了承メッセージであるか?
S326
コンテンツの利用を継続
S501
リトライしない?
S327
コンテンツの利用を中止
S701
リトライ再開時間経過?
Y
N

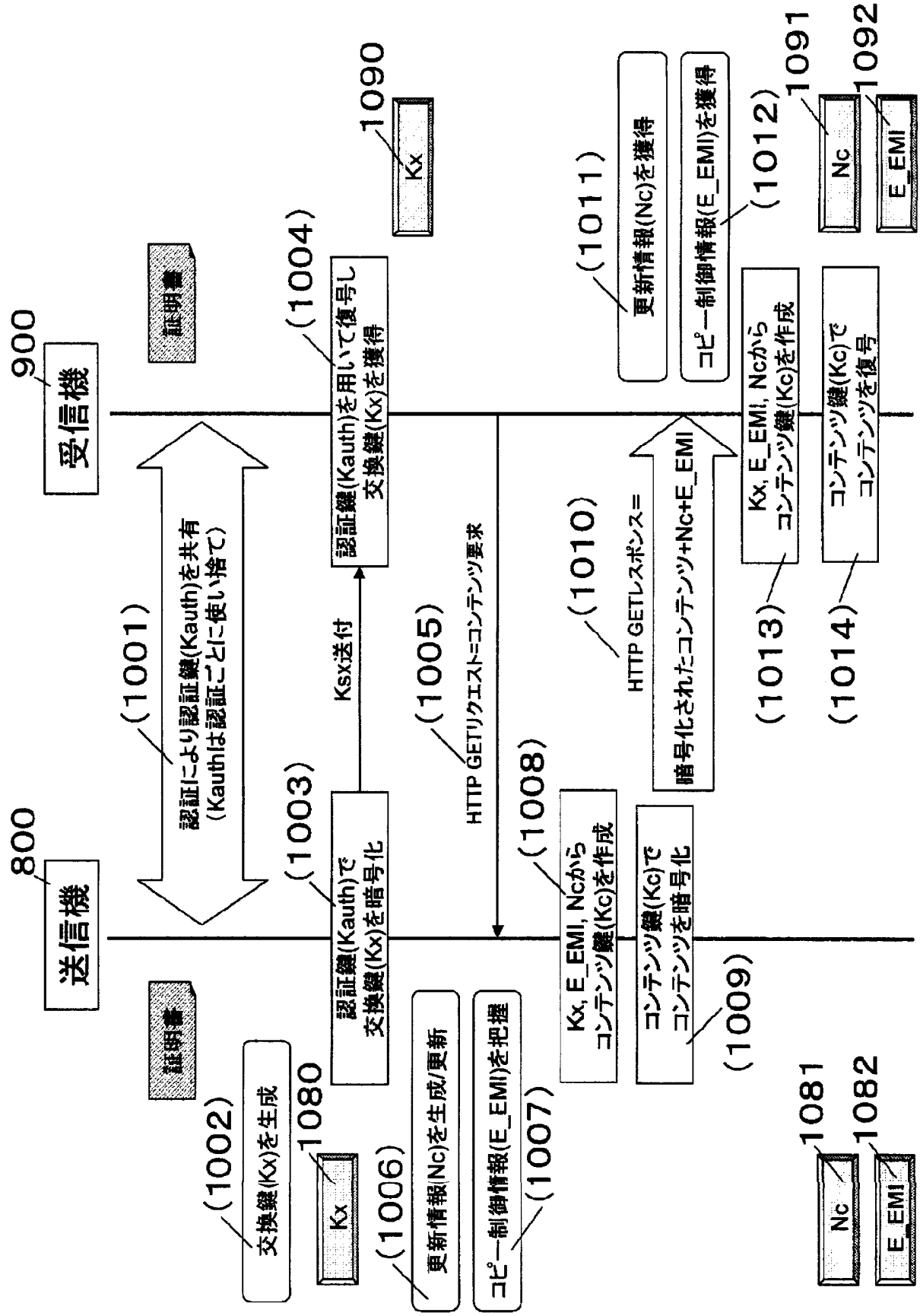
[図8]


送信機
800
801
証明書・鍵保持部
802
交換鍵作成部
803
認証・鍵交換部
暗号
804
更新情報作成・更新部
805
コピー制御情報管理部
806
コンテンツ鍵算出部
807
コンテンツ蓄積部
808
コンテンツ暗号化部
809
コンテンツ
パケット作成部
810
コンテンツ
パケット送信部
811
HTTPプロトコル部

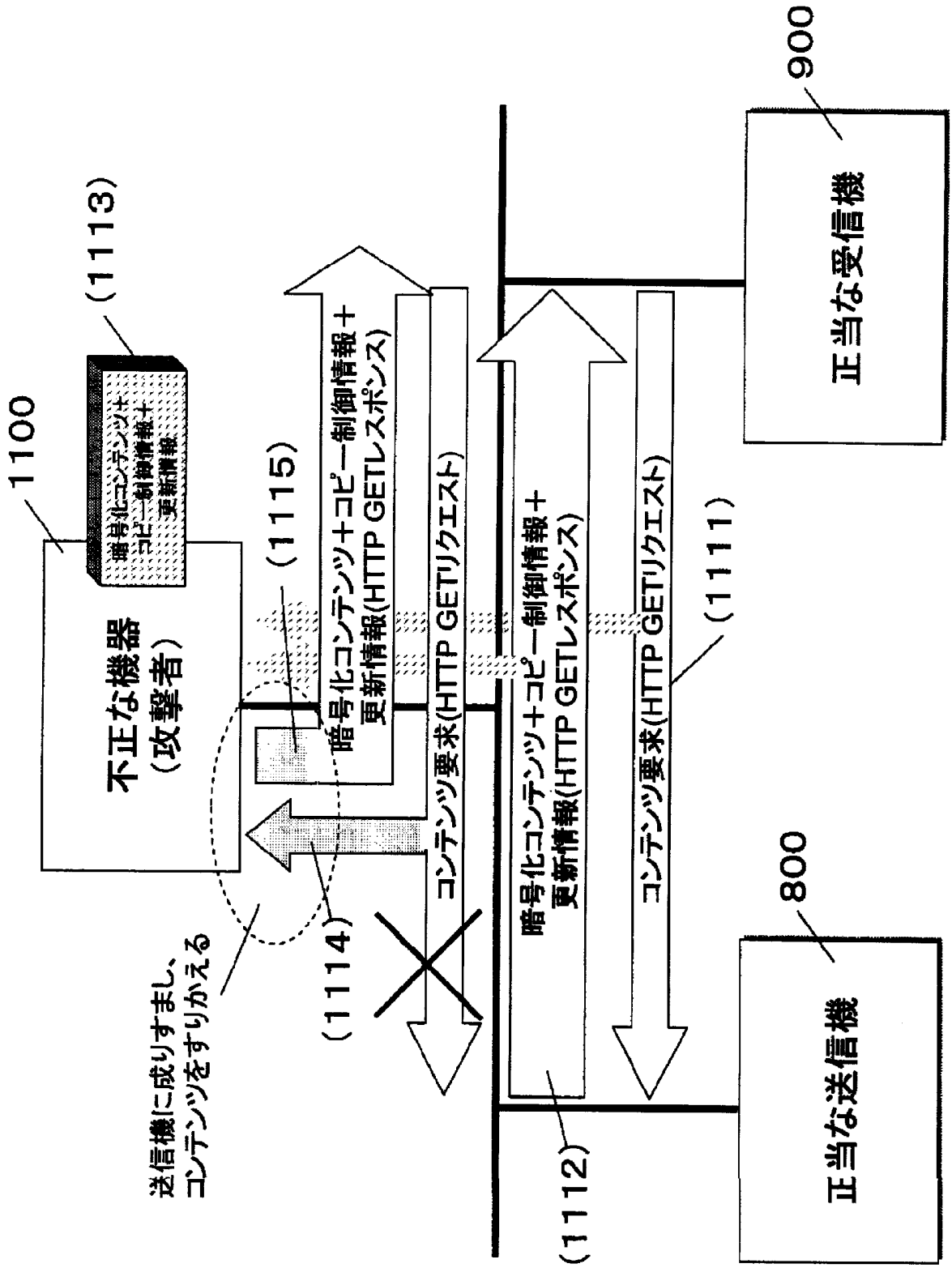
[図9]


受信機
900
903
更新情報格納部
902
認証・鍵交換部
復号
909
コンテンツ
パケット受信部
905
コンテンツ鍵算出部
907
コンテンツ復号部
908
コンテンツ
パケット解析部
901
証明書・鍵保持部
910
HTTPプロトコル部
906
コンテンツ利用部
904
コピー制御情報格納部

[図10]


800
送信機
900
受信機
証明書
証明書
(1001)
認証により認証鍵(Kauth)を共有
(Kauthは認証ごとに使い捨て)
(1002)
交換鍵(Kx)を生成
1080
Kx
(1003)
認証鍵(Kauth)で
交換鍵(Kx)を暗号化
Ksx送付
(1004)
認証鍵(Kauth)を用いて復号し
交換鍵(Kx)を獲得
1090
Kx
(1005)
HTTP GETリクエスト=コンテンツ要求
(1006)
更新情報(Nc)を生成/更新
(1007)
コピー制御情報(E_EMI)を把握
(1008)
Kx, E_EMI, Ncから
コンテンツ鍵(Kc)を作成
(1009)
コンテンツ鍵(Kc)で
コンテンツを暗号化
(1010)
HTTP GETレスポンス=
暗号化されたコンテンツ+Nc+E_EMI
(1011)
更新情報(Nc)を獲得
(1012)
コピー制御情報(E_EMI)を獲得
(1013)
Kx, E_EMI, Ncから
コンテンツ鍵(Kc)を作成
(1014)
コンテンツ鍵(Kc)で
コンテンツを復号
1081
Nc
1082
E_EMI
1091
Nc
1092
E_EMI

[図11]


900
正当な受信機
(1113)
暗号化コンテンツ+
コピー制御情報+
更新情報
1100
不正な機器
(攻撃者)
(1115)
暗号化コンテンツ+コピー制御情報+
更新情報(HTTP GETレスポンス)
コンテンツ要求(HTTP GETリクエスト)
(1111)
暗号化コンテンツ+コピー制御情報+
更新情報(HTTP GETレスポンス)
コンテンツ要求(HTTP GETリクエスト)
送信機に成りすまし、
コンテンツをすりかえる
(1114)
(1112)
800
正当な送信機

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/018777

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01), ***G06F21/00***(2006.01), ***G11B20/10***(2006.01), ***H04L9/32***(2006.01), ***H04N7/167***(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08(2006.01), ***G06F21/00***(2006.01), ***G11B20/10***(2006.01), ***H04L9/32***(2006.01), ***H04N7/167***(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-358706 A (Matsushita Electric Industrial Co., Ltd.), 26 December, 2001 (26.12.01), Full text; all drawings & US 2004/076294 A & EP 1143656 A2	1-13
Y	JP 2002-207639 A (Sony Corp.), 26 July, 2002 (26.07.02), Par. Nos. [0009] to [0012], [0045] to [0047], [0066] to [0069]; Figs. 1 to 7 (Family: none)	1-13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 January, 2006 (04.01.06)	17 January, 2006 (17.01.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０１８７７７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　*H04L9/08(2006.01), G06F21/00(2006.01), G11B20/10(2006.01), H04L9/32(2006.01), H04N7/167(2006.01)*

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　*H04L9/08(2006.01), G06F21/00(2006.01), G11B20/10(2006.01), H04L9/32(2006.01), H04N7/167(2006.01)*

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2001-358706 A（松下電器産業株式会社）2001.12.26, 全文，全図 & US 2004/076294 A & EP 1143656 A2	１－１３
Y	JP 2002-207639 A（ソニー株式会社）2002.07.26, 第【０００９】－【００１２】段落，第【００４５】－【００４７】段落，第【００６６】－【００６９】段落，図１－７　（ファミリーなし）	１－１３

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ０４．０１．２００６	国際調査報告の発送日 １７．０１．２００６
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　４２２９ 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６