



- (51) 国際特許分類:
H04L 9/08 (2006.01) H04N 7/16 (2006.01)
H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2009/052504
- (22) 国際出願日: 2009年2月16日(16.02.2009)
- (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 2008-066964 2008年3月17日(17.03.2008) JP
- (71) 出願人(米国を除く全ての指定国について): 株式会社日立製作所(HITACHI, LTD.) [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目6番6号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 大野 千代(OHNO, Chiyo) [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所 コンシューマエレクトロニクス研究所内 Kanagawa (JP). 岡本 宏夫(OKAMOTO, Hiroo) [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町292番

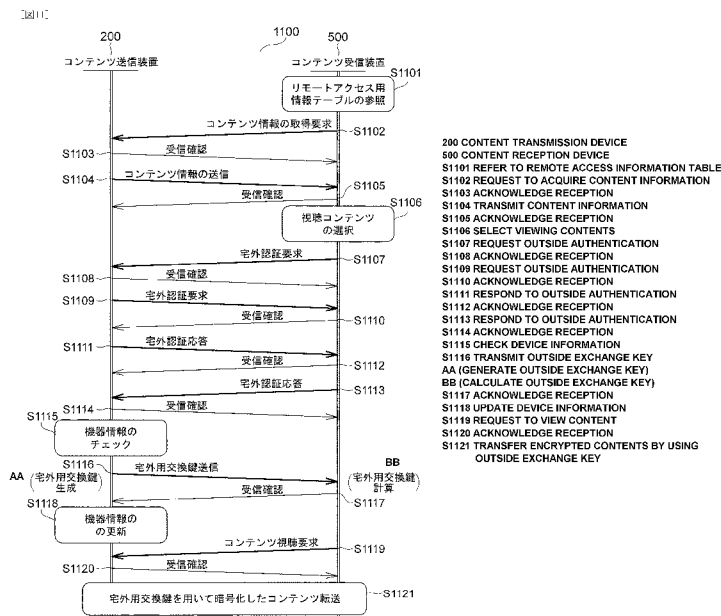
地 株式会社日立製作所 コンシューマエレクトロニクス研究所内 Kanagawa (JP).

- (74) 代理人: 特許業務法人浅村特許事務所(ASAMURA PATENT OFFICE, p.c.); 〒1000004 東京都千代田区大手町2丁目2番1号 新大手町ビル331 Tokyo (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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF,

[続葉有]

(54) Title: CONTENT TRANSMISSION DEVICE AND CONTENT RECEPTION DEVICE

(54) 発明の名称: コンテンツ送信装置、コンテンツ受信装置



(57) Abstract: A content reception device which accesses from outside to an in-house content transmission device previously performs first authentication and outside access information sharing required at the time of an access from the outside along with the content transmission device in-house and instructs the content transmission device to register information on the content reception device and the outside access information in the device information table of the content transmission device. If the content reception device carried outside accesses the in-house content transmission device, the information on the content reception device is registered in the device information table of the content transmission device. Only if second authentication using the outside access information between both devices is successful, the content transmission device can transmit contents to the content reception device.

(57) 要約: 宅内のコンテンツ送信装置に対して宅外からアクセスするコンテンツ受信装置は、予め宅内で該コンテンツ送信装置との間で第1の認証処理と宅外からのアクセス時に必要となる

宅外アクセス情報共有処理を実施し、該コンテンツ送信装置の機器情報テーブルに該コンテンツ受信装置に関する情報と該宅外アクセス情報を登録してもらう。宅外に持ち出した該コンテンツ受信装置で宅内の該コンテンツ送信装置にアクセスする場合は、該コンテンツ送信装置の該機器情報テーブルに該コンテンツ受信装置に関する情報が登録され且つ両装置間で該宅外アクセス情報を利用した第2の認証処理に成功した場合のみ、該コンテンツ送信装置は該コンテンツ受信装置に対してコンテンツを送送できる。

WO 2009/116338 A1



CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, 添付公開書類:
TG).

— 国際調査報告 (条約第 21 条(3))

明 細 書

コンテンツ送信装置、コンテンツ受信装置

参照による取り込み

- [0001] 本出願は、2008年3月17日に出願された日本特許出願第2008-066964号の優先権を主張し、その内容を参照することにより本出願に取り込む。

技術分野

- [0002] 映像音声等のコンテンツをネットワークを介して送受信するのに際して、伝送されるコンテンツの著作権を保護するのに好適な送信装置、受信装置およびコンテンツ伝送方法に関するものである。

背景技術

- [0003] パーソナルコンピュータ(以下、PC)の演算速度や記憶容量など処理能力の発展に伴い、PCに内蔵されるハードディスクドライブ(以下、HDD)も大容量化が進んでいる。こうした状況のもとで最近では一般の家庭で利用されるようなランクのPCにおいてもHDDを利用してTV放送番組を録画し、これをPCのディスプレイで視聴を行うといった使い方ができるようになってきた。
- [0004] また、近年デジタル映像信号処理技術の発展に伴い、デジタル放送を受信するデジタルチューナ内蔵テレビ(以下、DTV)や、デジタル放送番組を録画・再生するデジタル記録装置(例えば、HDDレコーダやDVDレコーダ、BDレコーダ等)のデジタルAV装置が次々と製品化されている。
- [0005] さらに、ブロードバンド／インターネットの普及により、これらのデジタルAV装置に有線／無線LAN(Local Area Network)、IEEE1394、USBなどのデジタルインタフェースを搭載し、ネットワークを介してデジタルコンテンツを伝送することが可能である。
- [0006] 一般にデジタル録画されたコンテンツを上記のようにネットワーク等を介してある装置から他の装置へ伝送して記録を行うような場合には伝送時のデータ品質の劣化が少なく、送信側の装置にあるコンテンツと同じ品質のコピー(複製)が受信側で作成できるため、著作権を保護すべきコンテンツに対しては、個人的利用の範囲を逸脱した

コンテンツの不正なコピー作成を防止できるような配慮が必要である。

[0007] 例えばデジタルAV機器の間でコンテンツを送信する際には、コンテンツ送信装置側において暗号化を行い、コンテンツ受信装置側との間で復号化のための情報の共有化を行うことによって、送信先であるコンテンツ受信装置以外の機器によってコンテンツが正しく受信されても復号されない様にして、無制限なコピーの作成を防ぐコピープロテクトが実施されている。

[0008] このようなコピープロテクトの方法の一例としてデジタルAV機器に取り入れられているものには、例えばIEEE1394バス上でのコピープロテクト方法を定めたDigital Transmission Content Protection(DTCP)方式がある。DTCP方式ではコンテンツを「コピー制限なし」「一回限りコピー可」「コピー禁止」に分類して管理し、録画装置では「コピー制限なし」「一回限りコピー可」のコンテンツだけを記録し、「一回限りコピー可」のコンテンツは一度記録した後は「コピー不可」として取り扱い、バス上では「コピー制限なし」のコンテンツを除いて送信側で暗号化処理を施して伝送を行うことによって、無制限なコンテンツのコピーが行えないようにしている。

[0009] また、有線あるいは無線のLANによるコンテンツ伝送においても、DTCP方式をIPネットワーク用に拡張し、さらなるセキュリティ強化を図ったDTCP-IP方式が規定されている。DTCP-IP方式では、家庭内で記録した放送番組などの著作権保護対象となるコンテンツが無制限に宅外へ配信すること無いように、家庭内ネットワークであることを判断するための技術が開示されている。

[0010] 特許文献1:特開2005-5821号公報

発明の開示

発明が解決しようとする課題

[0011] 上記従来技術では、著作権保護対象のコンテンツを有線あるいは無線LANを介して伝送する際、送信側と受信側の機器が同じ家の中にあることを確認する機能が組み込まれている。

[0012] しかし、ノート型PCや携帯端末といったモバイル環境で使用する機器を所有しているユーザにとっては、これらの機器を用いて旅行先や通勤途中の電車の中などから家庭内のコンテンツにアクセスしたいという要求は高い。

[0013] そこで、有線または無線のLANを利用し、宅内の機器から宅外の機器へコンテンツを送信する際に、コンテンツの正当な視聴が個人的利用の範囲に制限することのできるコンテンツ送信装置、受信装置およびコンテンツ伝送方法を提供することを目的とする。

課題を解決するための手段

[0014] 上記の課題を解決するために、コンテンツ送信装置は、

宅内のネットワークに接続されたコンテンツ受信装置との間で、第1の認証プロトコルに準拠してお互いに正規に認定された機器であることを認証し、該コンテンツ受信装置が宅内に存在することを確認する第1の認証手段と、

該コンテンツ受信装置との間で、宅外からのアクセス時に必要となる情報を共有する宅外アクセス情報共有手段と、

該第1の認証手段で認証処理に成功した該コンテンツ受信装置に関する情報と、該宅外アクセス情報共有手段で共有した情報とを保持および管理する機器情報管理手段と、

宅外のネットワークに接続されたコンテンツ受信装置との間で、前記宅外アクセス情報共有手段で共有した情報を利用する第2の認証プロトコルに準拠して、お互いに正規に認定された機器であることを認証する第2の認証手段と、

該第1の認証手段で認証処理を実行して該コンテンツ受信装置との間で共有できた第1の鍵情報、または該第2の認証手段で認証処理を実行して共有できた第2の鍵情報を用いて該コンテンツ受信装置に送信するコンテンツの暗号化処理を行う暗号化手段と、

を備え、

前記第1の認証手段を用いて前記コンテンツ受信装置との間で認証処理に成功した場合に限り、前記宅外アクセス情報共有手段を用いて宅外からのアクセス時に必要となる宅外アクセス情報を共有し、前記機器情報管理手段を用いて該コンテンツ受信装置に関する情報と該宅外アクセス情報を登録し、

前記第2の認証処理手段を用いて該コンテンツ受信装置との間で認証処理に成功した場合に限り、前記暗号化手段を用いて宅外にあるコンテンツ受信装置に対してコ

ンテンツを暗号化しながら送信する。

発明の効果

- [0015] 宅内で予めコンテンツ送信装置との間で通常の機器認証処理と宅外アクセス用の機器認証処理を実行し、これらの処理に成功したコンテンツ受信装置のみ、宅外から宅外専用の機器認証処理を実行すれば宅内のコンテンツを視聴可能となる。これにより、正規のユーザが個人的利用の範囲を超えることなく宅外から宅内のコンテンツを視聴することができ、ユーザの利便性が向上する。

本発明の他の目的、特徴及び利点は添付図面に関する以下の本発明の実施例の記載から明らかになるであろう。

図面の簡単な説明

- [0016] [図1]システムの一構成例
[図2]DTVの一ブロック構成例
[図3]HDDレコーダの一ブロック構成例
[図4]PCの一ブロック構成例
[図5]携帯電話の一ブロック構成例
[図6]機器情報管理部の一構成例
[図7]機器情報の一構成例
[図8]宅内のコンテンツ送信装置とコンテンツ受信装置の間で通常実行する機器認証シーケンスの一例。
[図9]宅内のコンテンツ送信装置とコンテンツ受信装置の間で宅外アクセス用の鍵交換を実行する機器認証シーケンスの一例。
[図10]宅外に持ち出すコンテンツ受信装置の機器情報管理部で保持するリモートアクセス用情報テーブルの一構成例。
[図11]宅内のコンテンツ送信装置と宅外のコンテンツ受信装置の間でコンテンツ転送を実行するシーケンスの一例。
[図12]機器情報の一構成例
[図13]システムの一構成例
[図14]宅外のコンテンツ受信装置から宅内のコンテンツ送信装置へコンテンツ転送を

実行するシーケンスの一例。

[図15]携帯電話のコンテンツ送信装置一覧画面例

[図16]携帯電話のコンテンツ一覧画面例

[図17]携帯電話のコンテンツ再生装置一覧画面例

[図18]機器情報の一構成例

[図19]宅外のコンテンツ受信装置から宅内のコンテンツ送信装置へコンテンツ転送を実行するシーケンスの一例

発明を実施するための最良の形態

[0017] 以下本発明の実施の形態について説明する。

実施例 1

[0018] 本実施の形態の特徴は、コンテンツの個人的利用の範囲を超えることなく、不正な視聴／複製を防止しながら、宅外にあるコンテンツ受信装置で宅内のコンテンツを視聴可能にすることである。

[0019] 図1は、システム構成を示したものであり、ユーザAが外出先から自宅内の機器にアクセスする場合を想定している。

[0020] ユーザA宅1内には、ユーザAの所有しているDTV100、HDDレコーダ200、PC300がハブ11を介して有線LANでネットワーク接続されている。また、該ハブ11はルータ12を介してインターネット3に接続可能になっている。

[0021] ユーザAの外出先(例えば、ホテルや会社等)2では、ユーザAの携帯電話500が無線アクセスポイント22と通信可能であり、ルータ21を介してインターネット3に接続可能になっている。また、ユーザBのPC400も同様の方法でインターネット3に接続可能とする。また、外出先に設置されたDTV600は、ルータ21を介してインターネット3に接続可能とする。

[0022] LANにおいては、ネットワークプロトコルとして標準のIP(Internet Protocol)を使用し、上位のトランスポートプロトコルにはTCP(Transmission Control Protocol)およびUDP(User Datagram Protocol)を用いる。コンテンツの伝送には更に上位のアプリケーションプロトコル、例えばRTP(Real-time Transport Protocol)やHTTP(Hyper Text Transfer Protocol)、FTP(File Transfer Protocol)

ol)等が使用される。なお、IPにはバージョンの違いとしてIPv4とIPv6が有るが、そのどちらかに限定される物ではない。

- [0023] ネットワーク接続された上記DTV100、HDDレコーダ200、PC300、400、携帯電話500、ルータ12、21は、それぞれLAN上で自身を識別するIPアドレスを所有する。また各々のネットワーク通信処理回路のインターフェース部には48ビットのMAC(Media Access Control)アドレスが予め製造時に与えられている。各装置へのIPアドレスの設定は、従来よりネットワークにおけるアドレスの自動設定に広く採用されているDHCP(Dynamic Host Configuration Protocol)により、例えばルータ12、21をDHCPサーバとして動作させ、ここから各装置のIPアドレスを割り振るようにすれば良い。
- [0024] なお、IPv6を用いる場合にはステートレス自動設定と呼ばれる方法によりルータ12、21のIPアドレスの上位64bitとMACアドレスから各装置が自身のIPアドレスを定めることも可能である。
- [0025] ここで、図1ではユーザ宅1内は各機器間を有線LANで接続しているが、無線アクセスポイントを使用したLANやIEEE1394、USB、Bluetooth等を用いても良い。また、ハブ11とルータ12、あるいは無線アクセスポイント22とルータ21が一体型になった形態でも良い。
- [0026] また、ルータ12、21は、図示しないモデムあるいは光電変換器などを介して、もしくはルータに内蔵されるモデムあるいは光電変換器によりインターネットに接続される。インターネットへの接続形態はADSL(Asymmetric Digital Subscriber line)や光ファイバーなどの高速アクセス回線やISDN(Integrated Services Digital Network)、アナログ電話回線、携帯電話などの移動体通信網などその種類を問わない。外出先2内のネットワーク構成も前記同様である。
- [0027] また、外出先2からインターネット3を介してユーザ宅1内の各機器にアクセスする方法は、ルータのポートフォワード機能やVPN(Virtual Private Network)などの技術を利用すれば良い。
- [0028] 次に、図2を用いて、DTV100の一構成例について説明する。なお、DTV600も同様の構成とする。

[0029] DTV100は、チューナ101、デスクランブラ102、デマルチプレクサ103、デコーダ104、表示部／スピーカ105、デジタル端子106、入力処理部107、機器認証処理部108、機器情報管理部109、暗号／復号処理部110、通信処理部111、デジタル入出力端子112、制御部113から構成される。

[0030] チューナ101は、放送局からアンテナ10を介して受信した複数のチャンネルから所望のチャンネルを選局し、デジタル変調された番組を復調する部分である。

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

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

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

[0031] 表示部／スピーカ105は、該デコーダ104からの出力信号や、デジタル端子106から入力された信号を再生する部分である。内蔵ではなく、外付けでも良い。

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

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

[0032] 機器認証処理部108は、LANを介して著作権保護対象のコンテンツを転送するために、他のAV機器との間で特定の認証プロトコルに準拠してお互いに正規に認定された機器であるかを認証し、コンテンツの暗号／復号に使用する鍵を共有する部分である。該特定の認証プロトコルは、例えば前記DTCP方式などが挙げられる。

[0033] 機器情報管理部109は、前記機器認証処理部108で認証が成功したAV機器に関する情報を管理する部分である。

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

[0034] 通信処理部111は、デジタル入出力端子112を介してLANで接続した他のAV機器との間でコンテンツや制御コマンドを送受信する部分である。送信されるコンテンツにはその取り扱い方を示す「コピー制限なし」「一回限りコピー可」「コピー禁止」「コピー不可」などの識別コードを付して送信される。

[0035] デジタル入出力端子112は、LAN経由でコンテンツや制御コマンドを入出力する部分である。

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

[0036] 次に、図3を用いて、HDDレコーダ200の一構成例について説明する。

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

[0037] 記録／再生処理部204は、コンテンツをHDD205に記録するための記録制御と、該HDD205に記録したコンテンツを再生するための再生制御を行う部分である。

HDD205は、放送番組を記録する内蔵メモリである。その他に着脱可能なHDDや光ディスク、メモリカード、そしてこれらを組み合わせたハイブリッド形態などが考えられる。

[0038] デジタル端子210は、デコーダ209から出力された非圧縮のデジタルデータを外部の表示部やスピーカへ出力する部分である。

それ以外の部分については、DTV100と同様である。

[0039] 次に、図4を用いて、PC300の一構成例について説明する。

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

[0040] 無線暗号／復号処理部315は、無線LAN経由で無線通信処理部316を介して受信したコンテンツあるいは暗号／復号処理部312から出力されたコンテンツを、WEP

(Wired Equivalent Privacy)などの無線LANにおけるセキュリティ保護の目的で標準的に用いられている公知の暗号化方式を用いて暗号化／復号化する部分である。無線LAN以外に、3GやW-CDMA(Wideband Code Division Multiple Access)など携帯電話などで使用している無線通信方式を利用しても良い。

[0041] 無線通信処理部316は、無線LANで接続した無線アクセスポイント22や他のAV機器との間でコンテンツや制御コマンドを送受信する部分である。無線LANだけでなく、

それ以外の部分については、DTV100、HDDレコーダ200と同様である。また、PC400も同様の構成で良い。

[0042] 次に、図5を用いて、携帯電話500の一構成例について説明する。

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

[0043] カメラ撮像部507は、カメラで撮影する部分である。

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

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

[0044] 次に、図6を用いて、前記各機器内の機器情報管理部109(203、309、511も同様)の一構成例について説明する。

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

[0045] タイマー1081は、前記機器認証処理部108(202、308、510も同様)で認証相手の機器が宅内に存在するか否かを確認する場合、あるいは後述の機器情報格納部1083に格納された登録情報の有効期限を管理する場合の時間計測に使用する部

分である。

- [0046] 機器情報更新部1082は、後述の機器情報格納部1083に保持した登録情報の有効期限を管理し、必要に応じて登録／更新／削除を行う部分である。

機器情報格納部1083は、前記機器認証処理部108で機器認証が成功した場合に、認証相手の機器に関する情報を保持する部分である。

- [0047] 次に、図7を用いて、前記機器情報格納部1083で格納する機器情報70の一構成例について説明する。

機器情報70は、管理テーブル700、機器情報テーブル710から構成される。

管理テーブル700は、最機器認証最大数701、カウンタ最大値702、外部アクセス最大数703で構成する。

- [0048] 最機器認証最大数701は、前記機器認証処理部108を用いてコンテンツの送信装置と受信装置の間で機器認証が実行可能な最大数を示す。

カウンタ最大値702は、前記タイマー1081に設定するカウンタの最大値を示す。

外部アクセス最大数703は、宅外からのコンテンツアクセス要求を許可する最大数を示す。

- [0049] 一方、機器情報テーブル710は、ID711、デバイスID712、アドレス情報713、カウンタ値714、宅外アクセス鍵715、宅外アクセス鍵ラベル715A、アクセス状況716で構成する。

ID711は、該テーブルの登録番号を示す。

- [0050] デバイスID712は、各機器を一意に識別するための識別子を示す。例えば、IEEE 1394で使用するユニークIDやDTCPで使用するデバイスIDなど、特定の認証機関により生成され、各機器の製造時に予め不揮発メモリに保存される機器固有の情報であり、機器毎にユニークな値を持つ。その他、公開鍵などの情報を含んでも良い。

- [0051] アドレス情報713は、ネットワーク上における各機器のIPアドレスやMACアドレス等を示す。

カウンタ値714は、前記タイマー1081に設定したカウンタの現在の値を示す。

宅外アクセス鍵715は、宅内とコンテンツ送信装置と宅外のコンテンツ受信装置と

の間でコンテンツ転送する際に認証／暗復号処理で用いる鍵情報を示す。

[0052] 宅外アクセス鍵ラベル715Aは、前記宅外アクセス鍵715を識別するために用いる識別子を示す。

アクセス状況716は、コンテンツの送信装置と受信装置との間の転送状況（例えば、停止／宅内／宅外）を示す。

[0053] 以上に記載した各機器と各情報を用いて、前記図1に示したシステム構成において、HDDレコーダ200（コンテンツ送信装置）とDTV100（コンテンツ受信装置）との間で実行する機器認証処理手順800について、図8を用いて説明する。ここで、機器認証処理のための情報の送受信にはプロトコルとしてTCPを用い、相手方の装置への認証要求とこれに対する認証応答等の各種情報が送信されるとこれに対する受信確認が相手方の装置から返送され、これにより伝送エラーの検知が可能な通信路が確保される。なお、図8においてはTCPによるコネクションの確立および破棄のためのデータ送受信については省略してある。

[0054] 最初に、コンテンツ受信装置100側から認証要求を作成する。コンテンツ受信装置100の機器認証処理部108は、認証要求に前記したデバイスIDを含む機器固有の情報と、該情報に対する証書を付して、通信処理部111を介してコンテンツ送信装置200に送る（S801）。

[0055] コンテンツ送信装置200の機器認証処理部202は、通信処理部207を介して認証要求を受け取りその受信確認をコンテンツ受信装置100に送ると（S802）、コンテンツ送信装置200の機器認証処理部202は自分の側からの認証要求を作成し、コンテンツ受信装置の場合と同様にコンテンツ送信装置200の固有情報とその証書を付してコンテンツ受信装置100に送る（S803）。

[0056] コンテンツ受信装置100の機器認証処理部108は、認証要求を受け取り、その受信確認をコンテンツ送信装置100へ送る（S804）。

[0057] 次に、コンテンツ送信装置200の機器認証処理部202は、前記認証要求で受信した各情報を検証し、鍵情報の生成に必要なパラメータを付した認証応答をコンテンツ受信装置100に送る（S805）。

[0058] コンテンツ受信装置100の機器認証処理部108は、認証応答を受け取りその受信

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

[0059] コンテンツ送信装置200の機器認証処理部202は、認証応答を受け取りその受信確認をコンテンツ受信装置100に送り(S808)、コンテンツ受信装置と同様に、必要なパラメータを用いてコンテンツ受信装置100と共通の認証鍵を生成する。

[0060] ここまでの手順で、コンテンツ送信装置200の機器認証処理部108とコンテンツ受信装置の機器認証処理部202は、互いに共通の認証鍵が生成されて共有される。

[0061] 次に、コンテンツ送信装置200は、コンテンツ受信装置100が宅内に存在する機器であるか確認するために、宅内確認の準備を行う旨をコンテンツ受信装置100に送る(S809)。

[0062] コンテンツ受信装置100の機器認証処理部108は、宅内確認準備の通知を受け取り、その受信確認をコンテンツ送信装置200に送ると(S810)、自分の側からの宅内確認準備通知を作成し、コンテンツ送信装置200へ送る(S811)。

[0063] コンテンツ送信装置200の機器認証処理部202は、宅内確認準備の通知を受け取り、その受信確認をコンテンツ受信装置100に送ると(S812)、宅内確認に必要な情報を付した宅内確認設定要求をコンテンツ受信装置100に送る(S813)。

[0064] コンテンツ受信装置100の機器認証処理部108は、宅内確認設定要求を受け取り、宅内確認に必要な準備を行い、その受信確認をコンテンツ送信装置200に送る(S814)。

[0065] 受信確認を受け取ったコンテンツ送信装置200の機器認証処理部202は、前記機器情報管理部203内のタイマー1081を起動した後、コンテンツ受信装置100が宅内に存在するか確認するための宅内確認実行要求をコンテンツ受信装置100に送る(S815)。

[0066] コンテンツ受信装置100の機器認証処理部108は、宅内確認実行要求を受け取り、その受信確認をコンテンツ送信装置200に送る(S816)。

[0067] コンテンツ送信装置200の機器認証処理部202は、受信確認を受け取ると、前記タ

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

[0068] 該宅内確認結果を受け取ったコンテンツ受信装置100の機器認証処理部108は、受信確認をコンテンツ送信装置200に送ると(S818)、コンテンツ送信装置200の機器認証処理部202はコンテンツを暗号する際に使用する交換鍵を生成し、前記認証鍵を用いて交換鍵を暗号化し、該交換鍵を識別するためのIDと一緒にコンテンツ受信装置100に送る(S819)。

[0069] コンテンツ受信装置100の機器認証処理部108は、前記認証鍵を用いてコンテンツ送信装置200から送信された交換鍵を復号し、受信確認を送る(S820)。

[0070] コンテンツ送信装置200の機器認証処理部202は、受信確認を受け取ると、前記機器情報管理部203内の前記機器情報テーブル710にコンテンツ受信装置100に関する情報を登録する(S821)。例えば、機器情報テーブル710内のID711のレコード721に示すように、前記S801で受け取ったコンテンツ受信装置100のデバイスIDをデバイスID712に設定し、ネットワーク上でのコンテンツ受信装置100のMACアドレスをアドレス情報713に設定し、管理テーブル700内のカウンタ最大値702をカウンタ値714に設定し、アクセス状況716に『停止』を設定する。

[0071] 以上から、コンテンツ送信装置200の機器認証処理部202とコンテンツ受信装置100の機器認証処理部108は、互いに共通の交換鍵を共有する。該交換鍵は、コンテンツを暗号化／復号化するための共通鍵を生成するために使用する。上記認証鍵、交換鍵、共通鍵の生成には、周知の鍵生成／鍵交換アルゴリズムを利用すれば良い。また、前記S809とS813の処理、S817とS819の処理をそれぞれ纏めても良い。

[0072] 以上の手順は、宅内でのコンテンツ転送を行う場合に、コンテンツ送信装置とコン

テンツ受信装置の間で実行する機器認証処理について説明した。

[0073] 次に、前記図1に示したシステム構成において、HDDレコーダ200(コンテンツ送信装置)と携帯電話500(コンテンツ受信装置)との間で実行する宅外アクセス用の機器認証処理手順について、図9を用いて説明する。

[0074] まず、コンテンツ送信装置200とコンテンツ受信装置500は、前記図8で説明した機器認証処理800を実施する。

[0075] その後、コンテンツ受信装置500の機器認証処理部510は、宅外アクセス用認証要求を作成し、コンテンツ送信装置200へ送る(S901)。該宅外アクセス用認証要求には、所定の計算アルゴリズムを用いて生成した乱数や前記の機器固有の情報などを含んでも良い。

[0076] コンテンツ送信装置200の機器認証処理部202は、宅外アクセス用認証要求を受け取りその受信確認をコンテンツ受信装置500に送ると(S902)、コンテンツ受信装置の場合と同様に自分の側からの宅外アクセス用認証要求を作成し、コンテンツ受信装置500に送る(S903)。

[0077] コンテンツ受信装置500の機器認証処理部510は、宅外アクセス用認証要求を受け取り、その受信確認をコンテンツ送信装置200へ送る(S904)。

[0078] 次に、コンテンツ送信装置200の機器認証処理部202は、宅外アクセス用認証要求で受信した各情報を検証し、鍵情報の生成に必要なパラメータを付した宅外アクセス用認証応答をコンテンツ受信装置500に送る(S905)。

[0079] コンテンツ受信装置500の機器認証処理部510は、宅外アクセス用認証応答を受け取りその受信確認をコンテンツ送信装置200に送った(S906)後、自分の側からの宅外アクセス用認証応答を作成し、コンテンツ送信装置の場合と同様に鍵情報の生成に必要なパラメータを付した宅外アクセス用認証応答をコンテンツ送信装置200に送り(S907)、必要なパラメータを用いてコンテンツ送信装置200と共通の認証鍵を生成する。

[0080] コンテンツ送信装置200の機器認証処理部202は、宅外アクセス用認証応答を受け取りその受信確認をコンテンツ受信装置500に送り、コンテンツ受信装置と同様に、必要なパラメータを用いてコンテンツ受信装置500と共通の認証鍵を生成する(S9

08)。そして、コンテンツ送信装置200の機器認証処理部202は、宅外からコンテンツを利用する際の機器認証処理およびコンテンツ暗号に使用するためのコンテンツ受信装置500専用の宅外アクセス鍵を生成し、S908で生成した前記認証鍵を用いて宅外アクセス鍵を暗号化してコンテンツ受信装置500に送る(S909)。

[0081] コンテンツ受信装置500の機器認証処理部510は、宅外アクセス用鍵を受信すると、受信確認をコンテンツ送信装置200へ送り(S910)、前記認証鍵を用いて宅外アクセス鍵を復号化する。

[0082] コンテンツ送信装置200の機器認証処理部202は、受信確認を受け取ると、前記機器情報管理部203内の前記機器情報テーブル710にコンテンツ受信装置500に関する情報を追加する(S911)。例えば、機器情報テーブル710内のID711のレコード722に示すように、ID711、デバイスID712、アドレス情報713、カウンタ値714、アクセス状況716は前記の通りに設定されており、さらに追加でコンテンツ受信装置500に送った前記宅外アクセス用鍵を宅外アクセス鍵715に設定する。

[0083] 一方、コンテンツ受信装置500の機器認証処理部510は、機器情報管理部511に格納したリモートアクセス用情報テーブル1000を生成または更新する(S912)。

[0084] ここで、図10を用いて、該リモートアクセス用情報テーブル1000の一構成例について説明する。

[0085] 機器情報管理部511内で保持するリモートアクセス用情報テーブル1000は、アドレス情報1001、登録情報1002、外部アクセス用共通鍵1003から構成される。

[0086] アドレス情報1001は、コンテンツ受信装置500が宅外からコンテンツ送信装置200やルータ12にアクセスするために必要なアドレス情報、例えばMACアドレスやIPアドレス、ポート番号などを登録する。

[0087] 登録情報1002は、コンテンツ受信装置500が宅外からコンテンツ送信装置200やルータ12にログインするために必要なユーザ名やパスワードを登録する。

外部アクセス用共通鍵1003は、前記S910で受信した宅外アクセス鍵を設定する。

[0088] 以上から、コンテンツ送信装置200とコンテンツ受信装置500は、通常の機器認証を実行した後、コンテンツ受信装置500からの要求に応じて、宅外からコンテンツ送

信装置200に格納したコンテンツを利用するための宅外アクセス用の共通鍵を共有する。前記コンテンツ送信装置200が生成する宅外アクセス鍵は、前記コンテンツ受信装置500専用の共通鍵とし、他のコンテンツ受信装置には適用できないものとする。また、該宅外アクセス鍵は、宅外からのコンテンツ配信要求時に実行する機器認証処理、また／あるいはコンテンツ暗号化するための共通鍵を生成するために使用する。上記認証鍵、交換鍵、該宅外アクセス鍵の生成には、周知の鍵生成／鍵交換アルゴリズムを利用すれば良い。

[0089] ここで、前記S903～S908の処理を省略し、S909で通常の機器認証処理800で共有した認証鍵を用いて宅外アクセス鍵を暗号化してコンテンツ受信装置500へ送信する方法もある。また、通常の機器認証処理800が終了後、コンテンツ送信装置200が前記宅外アクセス用認証要求を受付け可能な時間を設け、所定の時間内にコンテンツ受信装置500が宅外アクセス用認証要求を発行する必要があるようにしても良い。さらに、前記S901～S902の処理を、通常の機器認証処理800内のS819の直前に行うようにしても良く、その場合はS820の後にS909～S910を実行、あるいはS819とS909の処理を1つに纏めても良い。

[0090] 次に、ユーザAが前記携帯電話500を宅外へ持ち出し、外出先Bから該携帯電話(コンテンツ受信装置)500を用いて、HDDレコーダ(コンテンツ送信装置)200のHDD205に記録したコンテンツを視聴する場合の手順について、図11を用いて説明する。

[0091] まず、前記携帯電話500の入力処理部509を用いてユーザAがコンテンツ視聴を指示すると、携帯電話500の制御部517は、コンテンツ送信装置一覧画面(図15)を表示部／スピーカ505上に表示する。該コンテンツ送信装置一覧画面1500には、記録メモリ513と、現在ネットワーク上に存在することを検出したコンテンツ送信装置(DTV600)と、機器情報管理部511で管理するリモートアクセス用情報テーブル1000に登録されているコンテンツ送信装置200を表示する(S1101)。

[0092] ここで、ネットワーク上に存在するコンテンツ送信装置を検出する方法としては、例えばネットワーク上の全装置に対して「コンテンツ送信機能を備えた機器の検出要求」を含んだUDPパケットをマルチキャスト送信し、該機能を備えた装置のみが返信す

ることにより、該コンテンツ送信装置を認識する方法がある。この方法は既存の技術を使用すればよく、例えばSSDP(Simple Service Discovery Protocol)やDLNA(Digital Living Network Alliance)が挙げられる。

[0093] 次に、ユーザAが前記コンテンツ送信装置一覧画面1500上でコンテンツ送信装置200を選択すると、コンテンツ受信装置500の制御部517は、前記リモートアクセス用情報テーブル1000に登録されているコンテンツ受信装置500のアドレス情報を参照し、無線通信処理部516から無線アクセスポイント22とルータ21を介してインターネット3経由でユーザA宅1のコンテンツ送信装置200に対して、コンテンツ情報の取得要求を送る(S1102)。

[0094] コンテンツ送信装置200の制御部211は、通信制御部207を介して受信確認をコンテンツ受信装置500へ送り(S1103)、HDD205に格納しているコンテンツの一部あるいは全てに関する情報(例えばタイトル、日付、コピー制御情報、記録時間など)をコンテンツ受信装置500へ送る(S1104)。

[0095] コンテンツ受信装置500の制御部517は、受信確認をコンテンツ送信装置200へ送り(S1105)、受信したコンテンツ情報をコンテンツ一覧画面(図16)として表示部／スピーカ505上に表示する。ユーザAは、該コンテンツ一覧画面1600上で視聴したいコンテンツを入力処理部509経由で指示すると(S1106)、コンテンツ受信装置500の機器認証処理部510は、宅外認証要求を作成する。宅外認証要求には、前記したデバイスIDを含む機器固有の情報と、前記宅外アクセス鍵あるいは該鍵を用いて生成した計算値と、証書を付してコンテンツ送信装置200に送る(S1107)。

[0096] コンテンツ送信装置200の機器認証処理部202は、宅外認証要求を受け取ると、前記機器情報管理部203内で管理している前記機器情報テーブル710に、コンテンツ受信装置500のデバイスIDが登録されていることを確認した後、その受信確認をコンテンツ受信装置500に送る(S1108)。もし前記機器情報テーブル710内に該コンテンツ受信装置500のデバイスIDが登録されていない場合は、コンテンツ送信装置100は以降の処理を中断する。

[0097] 次に、コンテンツ送信装置200の機器認証処理部202は、自分の側からの宅外認証要求を作成し、コンテンツ受信装置の場合と同様に、コンテンツ送信装置200の固

有情報と前記宅外アクセス鍵あるいは該鍵を用いて生成した計算値と、証書を付してコンテンツ受信装置500に送る(S1109)。

[0098] コンテンツ受信装置500の機器認証処理部510は、宅外認証要求を受け取り、その受信確認をコンテンツ送信装置200へ送る(S1110)。

[0099] 次に、コンテンツ送信装置200の機器認証処理部202は、前記宅外認証要求で受信した各情報を検証し、前記宅外アクセス鍵あるいは該鍵を用いて生成した計算値と、鍵情報の生成に必要なパラメータを付した宅外認証応答をコンテンツ受信装置500に送る(S1111)。

[0100] コンテンツ受信装置500の機器認証処理部510は、前記宅外認証応答を受け取り、その受信確認をコンテンツ送信装置200に送った(S1112)後、自分の側からの宅外認証応答を作成し、コンテンツ送信装置の場合と同様に、鍵情報の生成に必要なパラメータを付した宅外認証応答をコンテンツ送信装置200に送り(S1113)、必要なパラメータを用いてコンテンツ送信装置200と共通の宅外認証鍵を生成する。

[0101] コンテンツ送信装置200の機器認証処理部202は、宅外認証応答を受け取り、その受信確認をコンテンツ受信装置500に送り、コンテンツ受信装置と同様に、必要なパラメータを用いてコンテンツ受信装置500と共通の認証鍵を生成する(S1114)。そして、前記機器情報テーブル710内のコンテンツ受信装置500のカウンタ値714が0になっていないことを確認した後(S1115)、コンテンツを暗号する際に使用する宅外用交換鍵を生成し、前記宅外認証鍵を用いて宅外用交換鍵を暗号化し、該宅外用交換鍵を識別するためのIDと一緒にコンテンツ受信装置500に送る(S1116)。

[0102] コンテンツ受信装置500の機器認証処理部510は、前記宅外認証鍵を用いてコンテンツ送信装置200から送信された宅外用交換鍵を復号し、受信確認を送る(S1117)。

[0103] コンテンツ送信装置200の機器認証処理部202は、受信確認を受け取ると、前記機器情報管理部203内の前記機器情報テーブル710にコンテンツ受信装置500に関する情報を更新する(S1118)。具体的には、アクセス状況716を『停止』から『宅外』に更新する。

- [0104] その後、コンテンツ受信装置500の制御部517は、所望のコンテンツの視聴要求をコンテンツ送信装置200に送る(S1119)。その際、該視聴要求には、S1116で受信した前記宅外用交換鍵を識別するためのIDを付加しても良い。
- [0105] コンテンツ送信装置200の制御部211は、コンテンツ視聴要求に対して受信確認を送り(S1120)、機器認証処理部202は前記宅外用交換鍵の識別IDが正しいかチェックし、機器情報更新部1082は前記機器情報管理部203内のタイマー1081を定期的に(例えば、1分間隔や10分間隔等)通知が入るように設定し、起動する。また、機器認証処理部202は前記宅外用交換鍵を用いてコンテンツを暗号化するための共通鍵を生成し、暗号／復号処理部206に該共通鍵を設定する。
- [0106] そして、HDD205から読み出した所望のコンテンツを暗号／復号処理部206で暗号化しながらコンテンツ受信装置500に送る(S1121)。ここで、コンテンツ送信中に前記タイマー1081から通知が入る毎に、機器情報更新部1082は前記機器情報テーブル710内のカウンタ値714を更新する(例えば、カウンタ値をデクリメントする)。
- [0107] コンテンツ受信装置500の機器認証処理部510は、前記宅外用交換鍵を用いてコンテンツを復号化するための共通鍵を生成し、暗号／復号処理部514に該共通鍵を設定する。そして、無線通信処理部516と無線暗号／復号処理部515を介して受信したコンテンツを暗号／復号処理部514で復号化し、デコーダ504でデコードしながら表示部／スピーカ505に出力する。
- [0108] 以上から、予め宅内においてコンテンツ送信装置とコンテンツ受信装置との間で宅外アクセス用の機器認証処理900を実施し、該認証処理に成功したコンテンツ受信装置を宅外へ持ち出した場合に限り、宅外専用の認証処理S1107～S1117を実行して成功すれば、宅内のコンテンツ送信装置から宅外のコンテンツ受信装置へコンテンツを転送することができる。
- コンテンツ転送が終了すると、コンテンツ送信装置はタイマー1081を停止し、前記宅外用交換鍵を破棄し、コンテンツ受信装置が続けて別のコンテンツの視聴要求を発行しても再度宅外専用の認証処理を実行しない限り送信しないようにしても良い。
- [0109] また、コンテンツ送信装置は、管理テーブル700内の外部アクセス最大数703を用いて、宅外から同時にアクセスできるコンテンツ受信装置の台数を制限することがで

きる。

[0110] 上記S1119において、コンテンツ送信装置200はコンテンツの「視聴要求」を受信しているが、宅外からそれ以外の要求、例えば「コピー要求」あるいは「ムーブ要求」を受信した場合は、コンテンツの不正利用を極力避けるため拒否するようにしても良い。

[0111] ここで、コンテンツ送信装置200からコンテンツ受信装置500にコンテンツを送信するのに使用するプロトコルは特定のものに限定されることはなく、RTP、HTTP、FTP等を用いることが可能である。コンテンツの伝送に際しては各転送プロトコルにおけるペイロード部分に共通鍵を用いて予め決められたアルゴリズムにより暗号化したコンテンツを収容して送信すれば良い。暗号化アルゴリズムとしては例えば周知の暗号化技術であるAES (Advanced Encryption Standard)を使用すれば良い。

[0112] また、コンテンツ送信装置が定期的に更新する機器情報テーブル710内のカウンタ値714は、宅内および宅外の両方のコンテンツ送信時で共用することも可能であるが、図12に示すように、宅内と宅外で別々のカウンタ値を使用することも可能である。その場合、それぞれのカウンタ値に設定する最大値を別々の値にしても良い(すなわち管理テーブル700の宅内用カウンタ最大値702、宅外用カウンタ最大値704)。

[0113] 以上のことから、宅内の機器に宅外からアクセスするコンテンツ受信装置は、予め宅内でコンテンツ送信装置との間で通常の機器認証処理と宅外アクセス用の機器認証処理を実施し、宅外アクセス鍵を共有すると同時にコンテンツ送信装置の機器情報テーブルに該コンテンツ受信装置に関する情報を登録してもらう。これにより、前記コンテンツ受信装置はあくまでも個人所有の機器として見なすことができ、宅外に持ち出した場合でも、コンテンツの個人利用の範囲を超えることなく、安全に視聴することができる。

実施例 2

[0114] 本実施の形態の特徴は、コンテンツの個人的利用の範囲を超えることなく、不正な視聴／複製を防止しながら、外出先の不特定のコンテンツ受信装置で宅内のコンテンツを視聴可能にすることである。

[0115] 図13は、システム構成例を示したものであり、ユーザAは携帯電話500を外出先に

持ち出し、該携帯電話500と同じ外出先に設置してある大画面のDTV600で自宅内のHDDレコーダ200のコンテンツを視聴する場合を想定している。DTV600は、前記DTV100と同様の構成とする。

[0116] ユーザAが外出先2のDTV600で自宅内のHDDレコーダ200のコンテンツを視聴する手順について、図14を用いて説明する。

[0117] ユーザAは、前記実施例1で説明した通り、自宅内でHDDレコーダ200(コンテンツ送信装置)と携帯電話500との間で宅外アクセス用機器認証900を実行し、両者間で宅外アクセス鍵を共有しておく。

[0118] ユーザAは携帯電話500を外出先(ホテル等)に持って行き、同じ場所にあるDTV600で宅内のコンテンツを視聴する場合、まずは前記図11のS1101～S1118と同様の手順でコンテンツ送信装置200と携帯電話500との間でコンテンツ情報の取得、宅外専用の機器認証処理を実行する。

[0119] 前記宅外専用の機器認証処理に成功し、両者間で宅外用交換鍵と該交換鍵の識別IDを共有した後、携帯電話500(コントローラ)の制御部517は、例えばネットワーク上の全装置に対して「再生機能を備えた機器の検出要求」を含んだUDPパケットをマルチキャスト送信し、該機能を備えた装置のみが返信するなど、前記DLNAなどの周知技術を利用してネットワーク上に他のコンテンツ再生装置が存在するか否か検出し、存在する場合は表示部／スピーカ505にコンテンツ再生装置一覧画面(図17)を表示する。

[0120] ユーザAは該一覧画面1700上で入力処理部509を介してコンテンツ再生装置を選択(この場合、DTV600)すると、制御部517はDTV600に対してコンテンツ視聴発行要求を送る(S1401)。コンテンツ視聴発行要求には、視聴するコンテンツに関する情報とリモートアクセス用情報テーブル1000に登録しているコンテンツ送信装置200のアドレス情報1001を含み、場合によって登録情報1002を付しても良い。

[0121] 前記コンテンツ視聴発行要求を受信したDTV600(コンテンツ受信装置)は、受信確認をコントローラ500に送り(S1402)、コントローラ500との間で通常の機器認証処理800を実施する。この際、コントローラ500の機器認証処理部510は、S819においてDTV600に送付する交換鍵と識別IDとして、前記S1116でコンテンツ送信

装置200と共有した宅外用交換鍵とその識別IDを使用する。これにより、コンテンツ送信装置200、コントローラ500、コンテンツ受信装置600の間で同じ宅外用交換鍵と該交換鍵の識別IDが共有できたことになる。

- [0122] その後、DTV600は、コンテンツ送信装置200に対してコンテンツ視聴要求を送る(S1403)。該コンテンツ視聴要求には、前記宅外用交換鍵の識別IDを付加する。また、コンテンツ送信装置200側で必要に応じてフォーマット変換あるいは画質変換を実施してコンテンツ送信してもらうために、DTV600で再生可能なデータ・フォーマット(例えば、MPEG2-TSやH. 264等)や画質(HDやSD、760pや1080i等)の情報を該コンテンツ視聴要求に含むことも可能である。該コンテンツ視聴要求と別の要求で発行しても良い。
- [0123] コンテンツ送信装置200の制御部211は、前記コンテンツ視聴要求を受け取ると、受信確認をDTV600に送る(S1404)。そして機器認証処理部202は前記宅外用交換鍵の識別IDが正しいことをチェックし、機器情報更新部1082は前記機器情報管理部203内のタイマー1081を定期的に通知が入るように設定し、起動する。
- [0124] また、機器認証処理部202は前記宅外用交換鍵を用いてコンテンツを暗号化するための共通鍵を生成し、暗号／復号処理部206に該共通鍵を設定する。そして、HDD205から読み出した所望のコンテンツを暗号／復号処理部206で暗号化しながらDTV600に送る(S1405)。ここで、コンテンツ送信中に前記タイマー1081から通知が入る毎に、機器情報更新部1082は前記機器情報テーブル710内のカウンタ値714を更新する。
- [0125] DTV600は、前記宅外用交換鍵を用いてコンテンツを復号化するための共通鍵を生成し、暗号／復号処理部110に該共通鍵を設定する。そして、ルータ21と通信処理部111を介して受信したコンテンツを暗号／復号処理部110で復号化し、デコーダ104でデコードしながら表示部／スピーカ105に出力する。
- [0126] 以上から、予め宅内においてコンテンツ送信装置との間で宅外アクセス鍵を共有したコントローラを宅外へ持ち出した際に、該コンテンツ送信装置と該コントローラとの間で宅外用交換鍵を共有できた場合に限り、該コントローラは通常の認証処理に成功した宅外のコンテンツ受信装置に前記宅外用交換鍵を渡すことができる。

[0127] これにより、コンテンツの個人利用の範囲を超えることなく、安全に宅外のコンテンツ受信装置で宅内のコンテンツを視聴することができる。

実施例 3

[0128] 前述した実施例2では、コンテンツ送信装置200は、コントローラ500に対してのみ、コンテンツの暗号化に必要な宅外用交換鍵を送信していた。したがって、コントローラ500とコンテンツ受信装置600との間の鍵交換(通常の機器認証処理800)については関与していない。

[0129] 本実施の形態の特徴は、コントローラ500がコンテンツ送信装置200に対して、コンテンツ受信装置600に該宅外用交換鍵を渡した旨を通知することである。

[0130] 図18、図19を用いて、本実施例の特徴を示す視聴手順について説明する。

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

[0131] 次に、ユーザAが外出先2のDTV600で自宅内のHDDレコーダ200のコンテンツを視聴する手順について、図19を用いて説明する。

コンテンツ送信装置200とコントローラ500との間のS1101～S118までの処理は、図14と同様である。また、コントローラ500とコンテンツ受信装置600との間のS1401～S1402、機器認証処理800までの処理も図14と同様である。

[0132] その後、コントローラ500は、コンテンツ送信装置200に対して、自装置の代わりに機器認証済みの外部装置(この場合、コンテンツ受信装置600)を用いてコンテンツ受信するための外部機器設定要求を発行する(S1900)。該設定要求には、コンテンツ受信装置600に関する情報—例えば、デバイスIDやMACアドレスなどを含む。

[0133] 該外部機器設定要求を受信したコンテンツ送信装置200は、該要求に含まれたコンテンツ受信装置600のデバイスIDを、前記機器情報テーブル710内の代理デバイスID718に設定し(S1901)、受信確認をコントローラ500に対して発行する(S1902)。

[0134] その後、コンテンツ受信装置600は、コンテンツ送信装置200に対してコンテンツ

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

[0135] 該コンテンツ視聴要求を受信したコンテンツ送信装置200は、該要求が代理デバイスID718から発行されたものであるか確認した後、受信確認をコンテンツ受信装置600に発行し、前記宅外用交換鍵を用いて暗号化したコンテンツを転送する。

[0136] ここで、コンテンツ送信装置200は、該代理デバイスID718のコンテンツ受信装置600に対してコンテンツ送信中に、デバイスID712のコントローラ500からコンテンツ視聴要求を受信した場合、コンテンツ受信装置600へのコンテンツ送信を中断する、あるいは該コンテンツ視聴要求を拒否し、同時に送信するデバイスは一台としても良い。

[0137] 以上から、コンテンツの個人利用の範囲を超えることなく、安全に宅外のコンテンツ受信装置で宅内のコンテンツを視聴することができる。

上記記載は実施例についてなされたが、本発明はそれに限らず、本発明の精神と添付の請求の範囲の範囲内で種々の変更および修正をすることができることは当業者に明らかである。

請求の範囲

- [1] 宅内のネットワークに接続されたコンテンツ受信装置との間で、第1の認証方法に基づいて第1の認証処理を行い、第1の鍵情報を共有する第1の認証手段と、
- 宅内のネットワークに接続された前記コンテンツ受信装置との間で、宅外からの通信時に必要となる第2の鍵情報を共有する宅外アクセス情報共有手段と、
- 前記第1の認証手段で認証された前記コンテンツ受信装置に関する情報と、前記宅外アクセス情報共有手段で共有された前記第2の鍵情報を管理する機器情報管理手段と、
- 宅外のネットワークに接続された前記コンテンツ受信装置との間で、前記宅外アクセス情報共有手段で共有された前記第2の鍵情報を用いて、第2の認証処理を行う第2の認証手段と、
- 前記第1の鍵情報を用いて宅内のコンテンツ受信装置へ送信するコンテンツの暗号化処理を行い、または前記第2の鍵情報を用いて宅外のコンテンツ受信装置へ送信するコンテンツの暗号化処理を行う暗号化手段と、
- 時間を計測するタイマー手段と、
- を備え、
- 前記第1の認証手段による前記第1の認証処理に成功した前記コンテンツ受信装置とのみ、前記第2の鍵情報を共有し、
- 前記機器情報管理手段に登録され、前記第2の認証処理による前記第2の認証処理に成功した前記コンテンツ受信装置以外の宅外のコンテンツ受信装置に対してコンテンツ送出を行わないことを特徴とするコンテンツ送信装置。
- [2] 前記タイマー手段を用いて所定の時間が経過した後、前記機器情報管理手段で管理される前記第2の鍵情報を削除することを特徴とする請求項1記載のコンテンツ送信装置。
- [3] 宅外のネットワークに接続された前記コンテンツ受信装置に対して所望のコンテンツを送信し終わると、前記第2の認証手段で共有された第2の鍵情報を破棄することを特徴とする請求項1記載のコンテンツ送信装置。
- [4] 宅外のネットワークに接続された前記コンテンツ受信装置からコピーあるいはムー

ブを目的としたコンテンツ配信要求を受信した場合、コンテンツ配信を拒否することを特徴とする請求項1記載のコンテンツ送信装置。

- [5] 宅内のネットワークに接続されたコンテンツ送信装置との間で、第1の認証方法に基づいて第1の認証処理を行い、第1の鍵情報を共有する第1の認証手段と、

宅内のネットワークに接続された前記コンテンツ送信装置との間で、宅外からの通信時に必要となる第2の鍵情報を共有する宅外アクセス情報共有手段と、

前記第1の認証手段で認証された前記コンテンツ送信装置に関する情報と、前記宅外アクセス情報共有手段で共有された前記第2の鍵情報を管理するリモートアクセス情報管理手段と、

宅外のネットワークに接続された前記コンテンツ送信装置との間で、前記宅外アクセス情報共有手段で共有された前記第2の鍵情報を用いて、第2の認証処理を行う第2の認証手段と、

前記第1の鍵情報を用いて宅内のコンテンツ送信装置から受信したコンテンツの復号化処理を行い、または前記第2の鍵情報を用いて宅外のコンテンツ送信装置から受信したコンテンツの復号化処理を行う暗号化手段と、

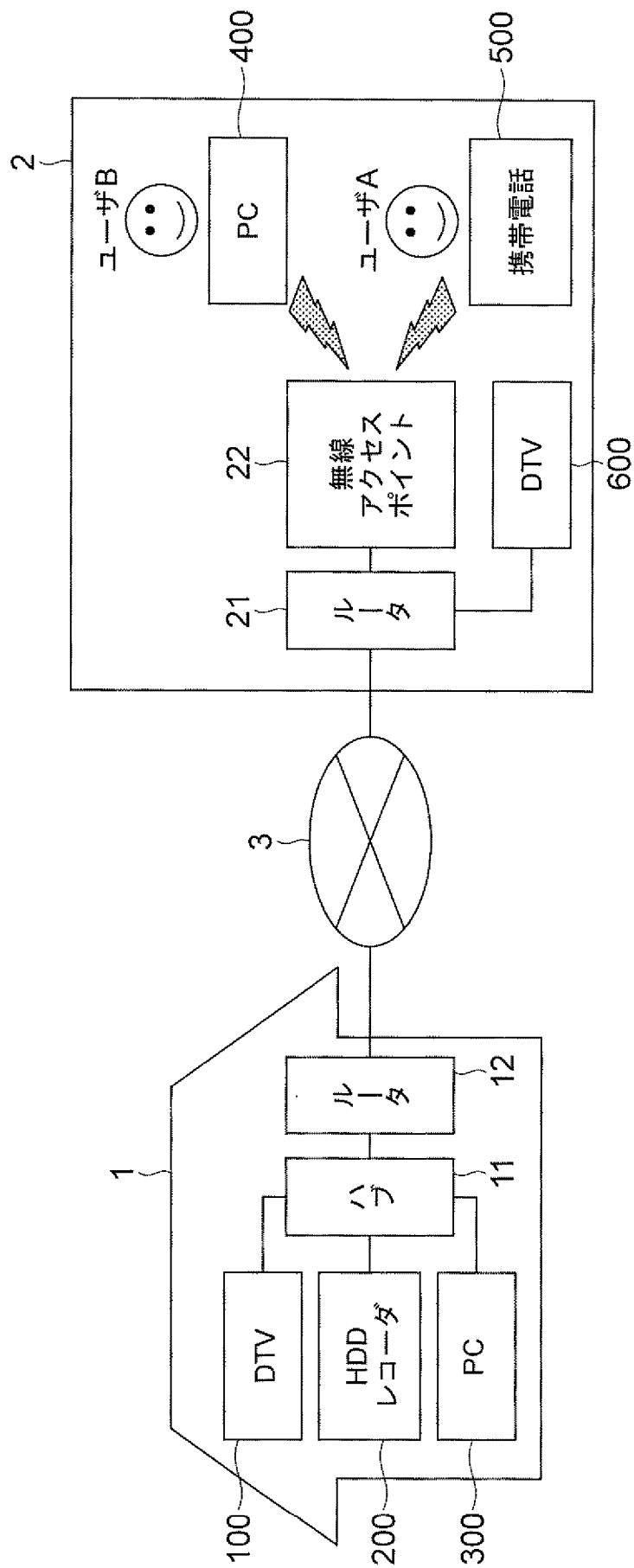
を備え、

前記第1の認証手段による前記第1の認証処理に成功した前記コンテンツ送信装置とのみ、前記第2の鍵情報を共有し、

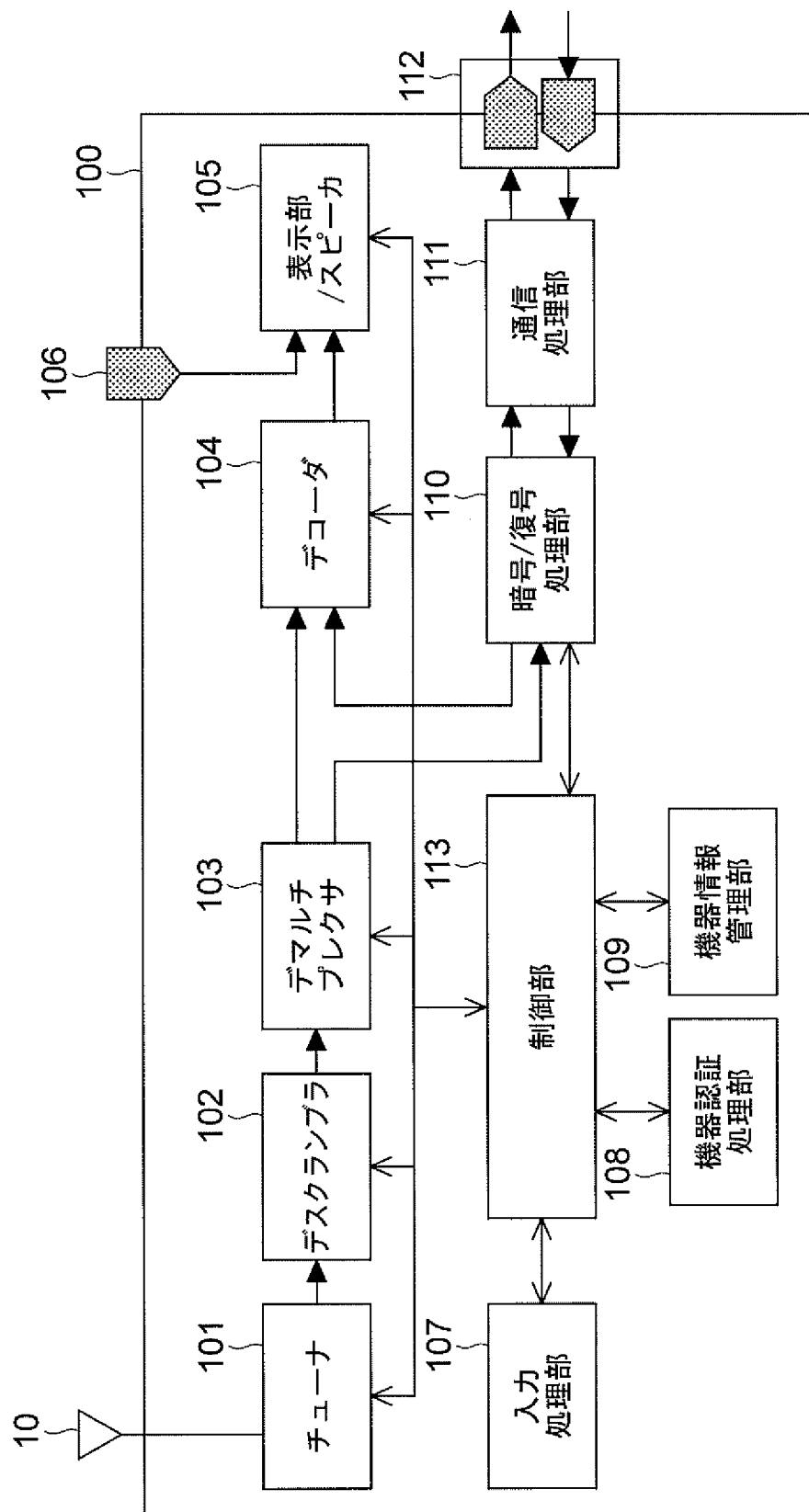
宅外に持ち出した際に前記コンテンツ送信装置からコンテンツ配信を要求する場合は、前記リモートアクセス情報管理手段に登録されたコンテンツ送信装置に対して前記第2の認証処理を用いた前記第2の認証処理を行うことを特徴とするコンテンツ受信装置。

- [6] 宅外に持ち出した際に、前記第2の認証手段を用いて宅外のネットワークに接続された前記コンテンツ送信装置と認証処理が成功した場合に限り、前記コンテンツ送信装置に関する情報と前記第2の鍵情報を宅外の他のコンテンツ受信装置に対して送信し、前記他のコンテンツ送信装置と前記コンテンツ受信装置とのコンテンツ転送を可能にすることを特徴とする請求項5記載のコンテンツ受信装置。

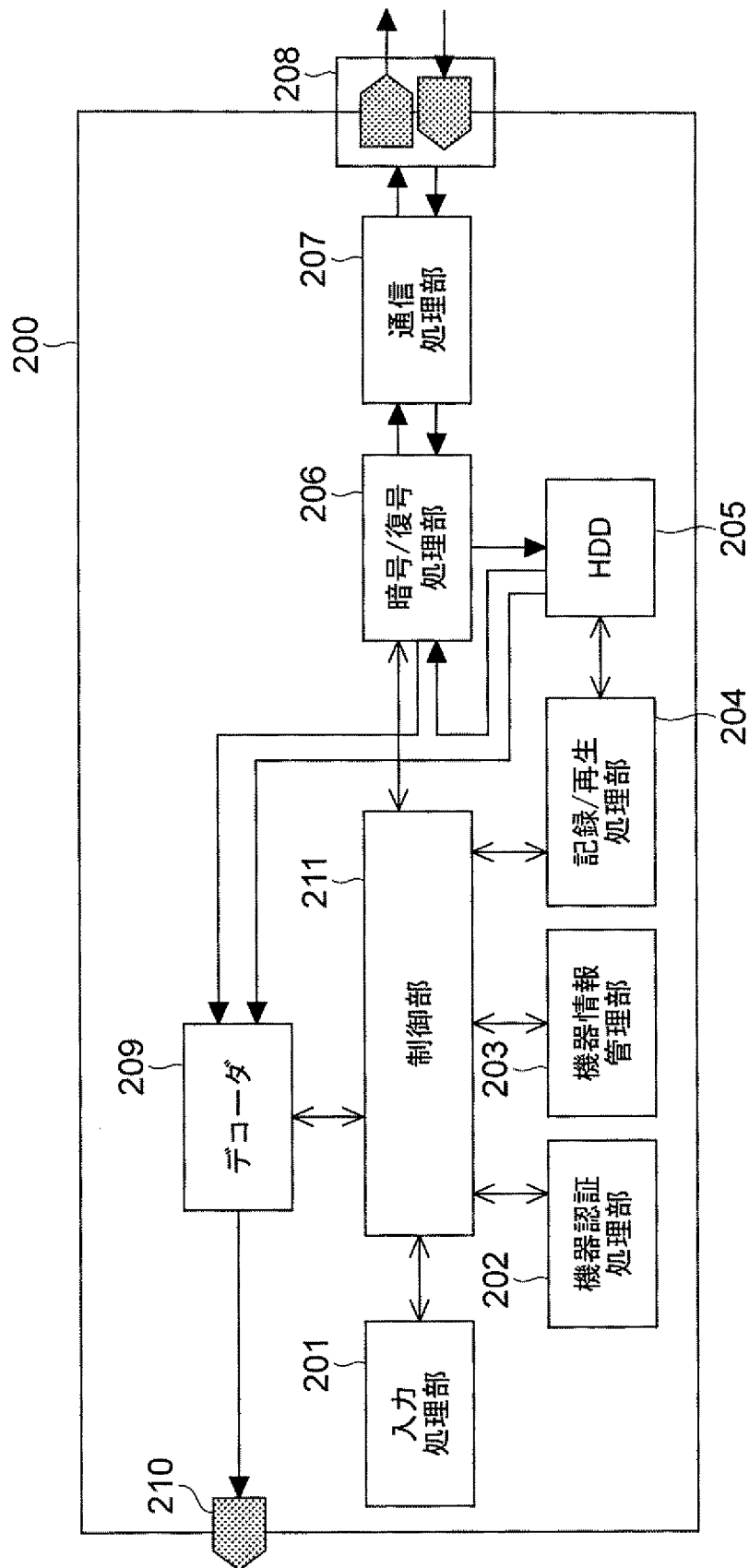
[図1]



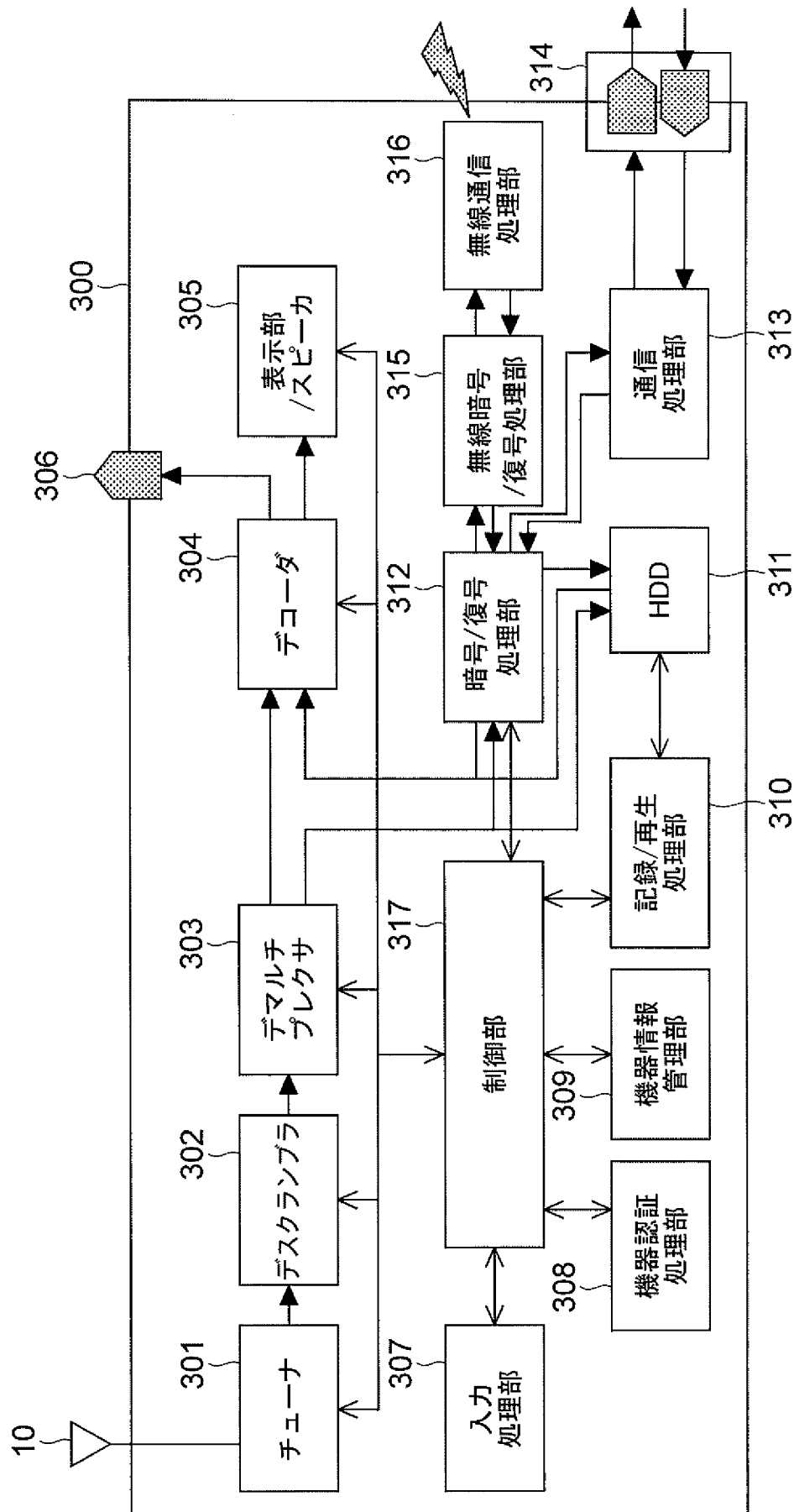
[図2]



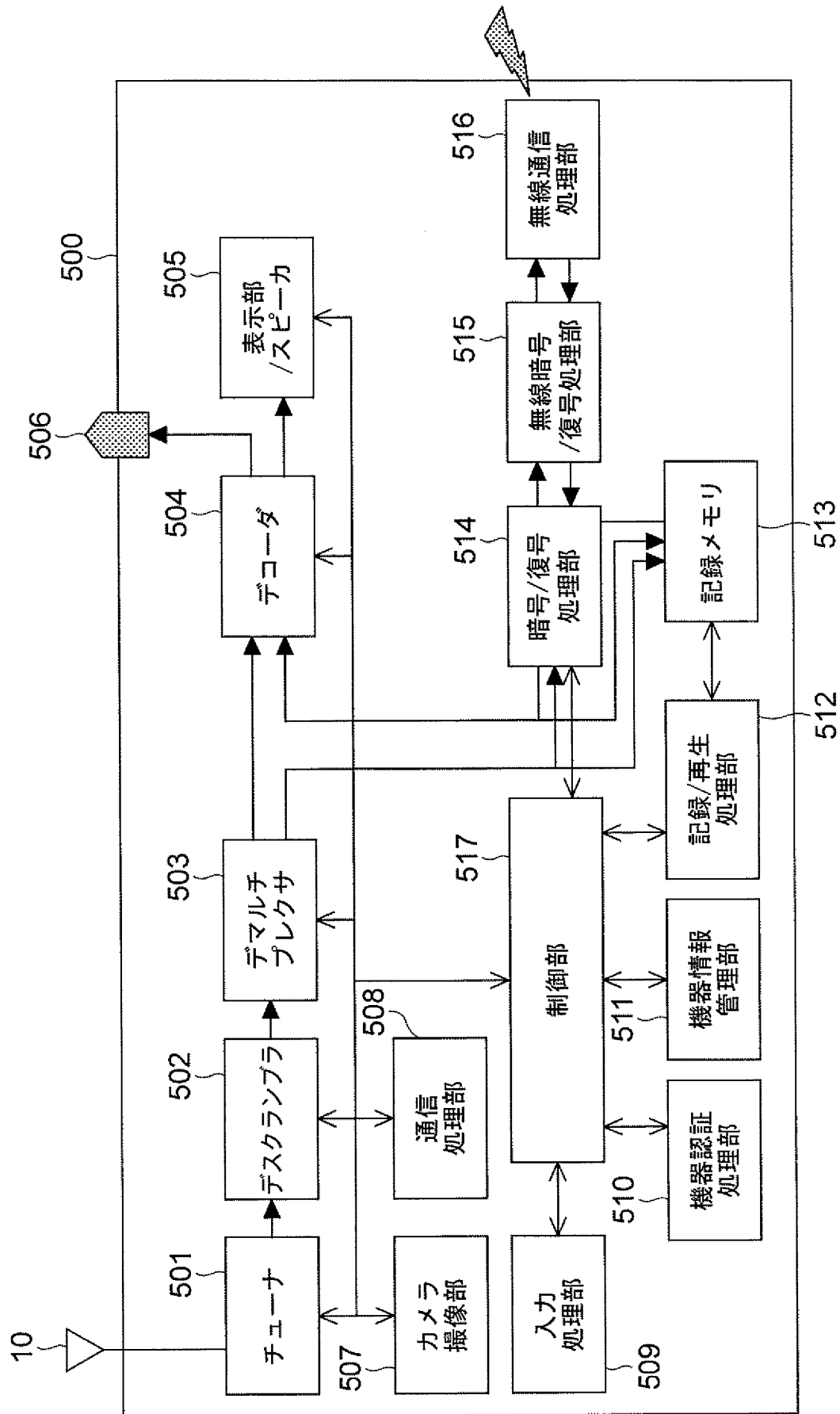
[図3]



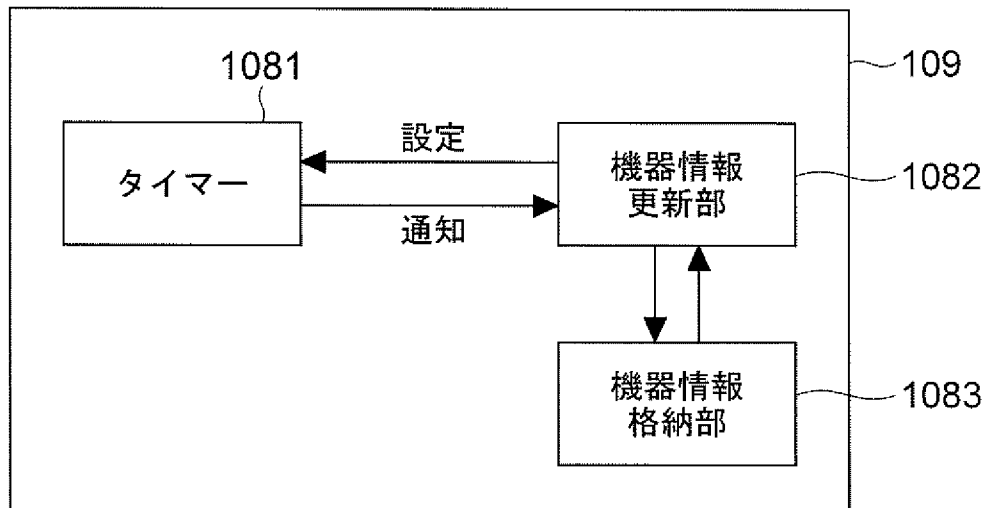
[図4]



[図5]



[図6]

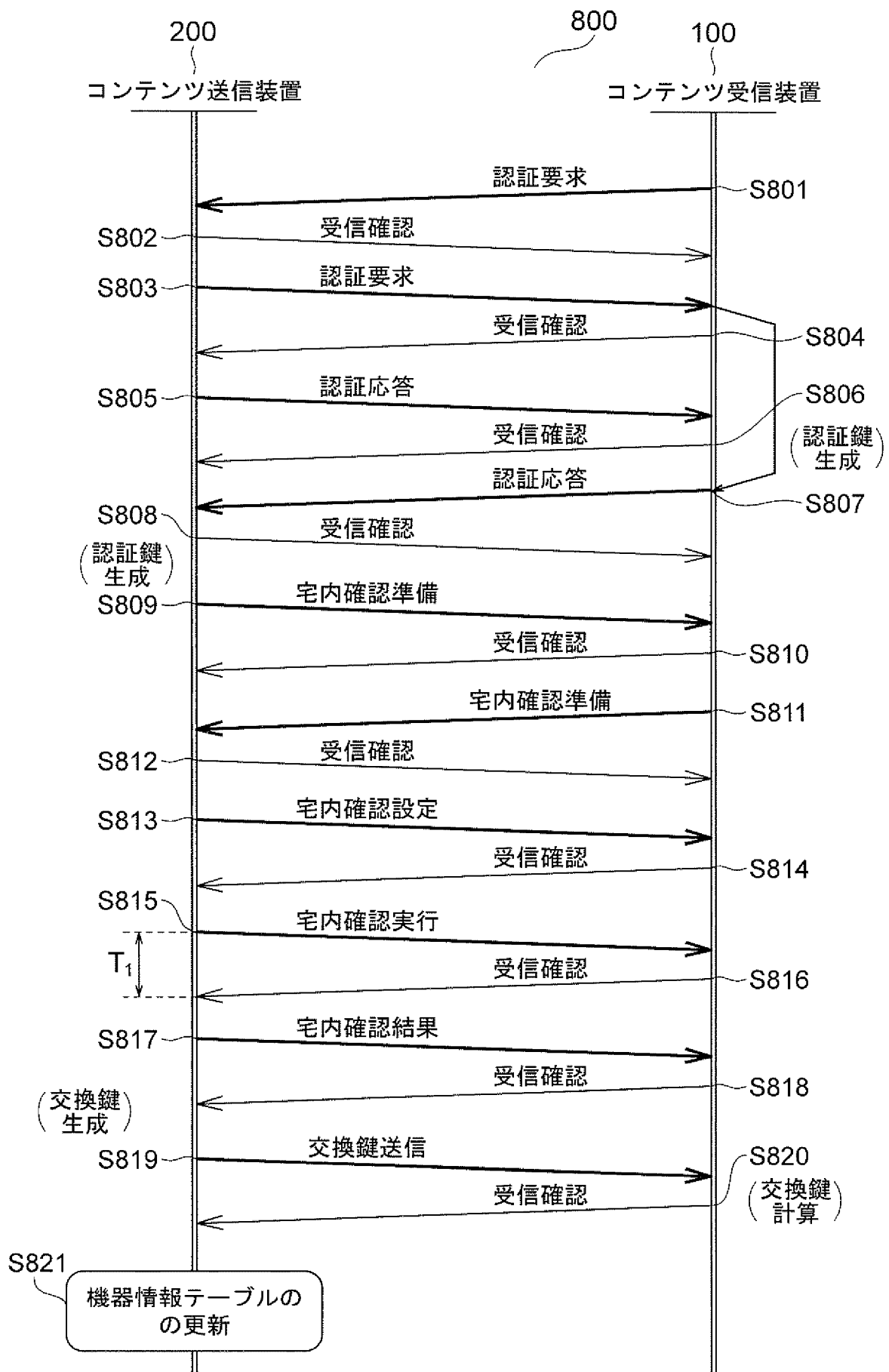


[図7]

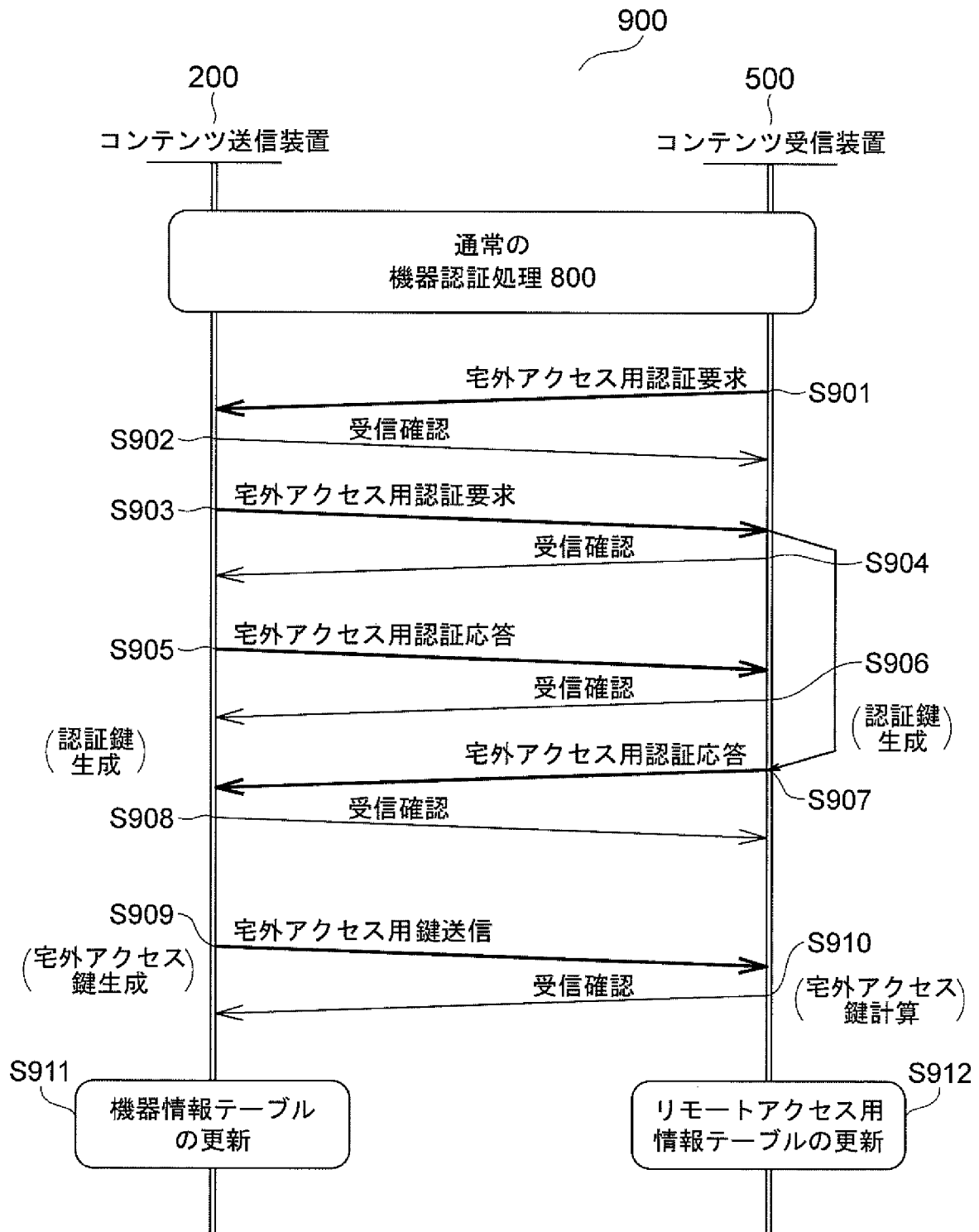
70		700		701	
				702	
				703	
機器認証最大数		34			
カウンタ最大値		1000			
外部アクセス最大数		3			

710		715		716									
		714		715A									
				721									
				722									
				723									
711	ID	712	デバイスID	713	アドレス情報 (例:MACアドレス)	714	カウンタ値	715	宅外アクセス鍵	715A	宅外アクセス 鍵ラベル	716	アクセス 状況
0		aabbcdddee (DTV100)		AAAAA		1000		—		—		停止	
1		ffgghhijj (携帯電話 500)		BBBBB		459		*@\$%**#1?		XXXXX		宅外	
2		kkllmmnn (PC300)		CCCCC		173		—		—		宅内	
..		...		...		...		...				...	
33		...		...		...		...				...	

[図8]



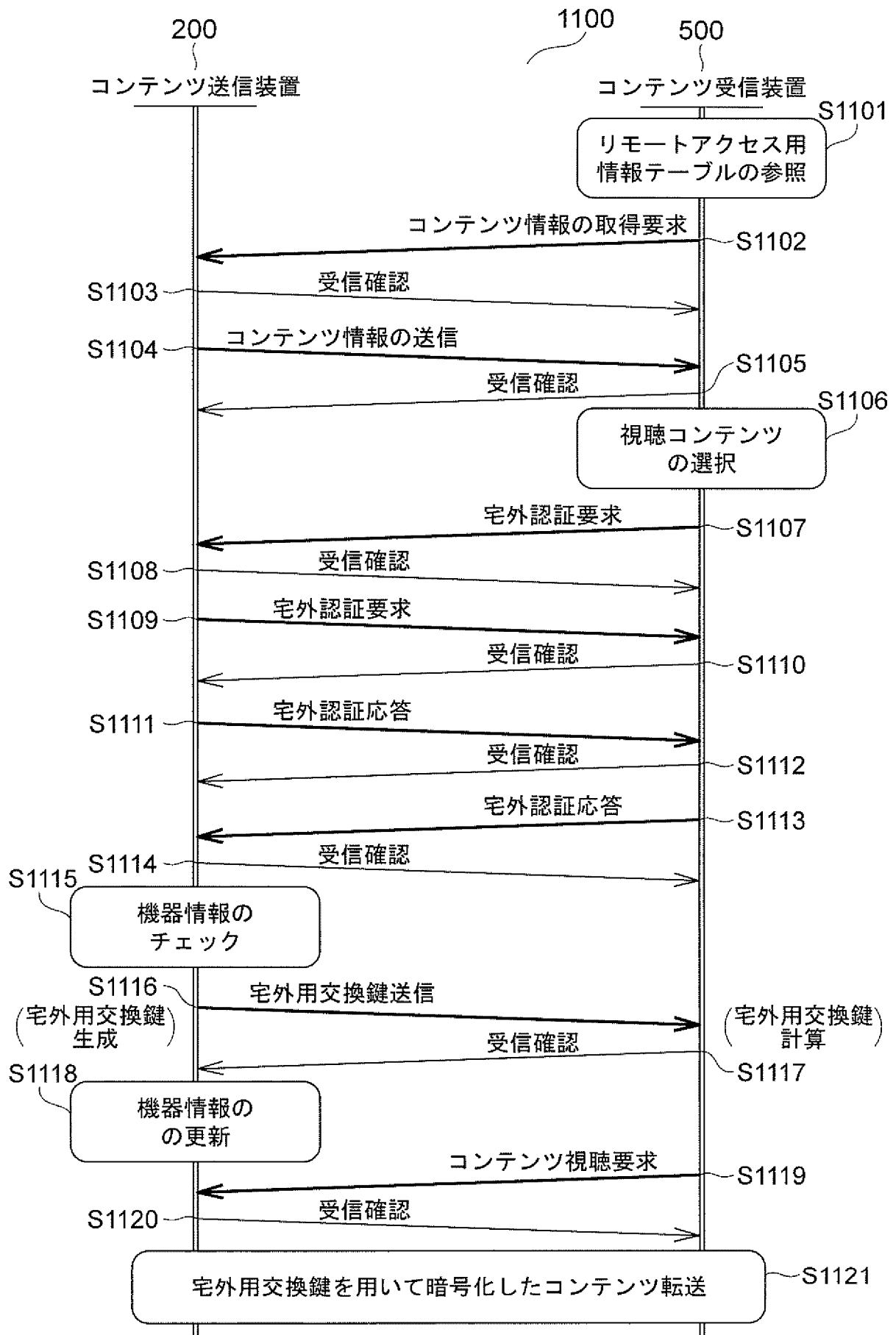
[図9]



[図10]

1000			
1001		1002	
アドレス情報		登録情報	
ID	MAC	ユーザ名	パスワード
	DDDDD	Paul	*****
	...	...	...
1003		外部アクセス用 共通鍵	
0		*@\$%***#1?	
..		...	

[図11]



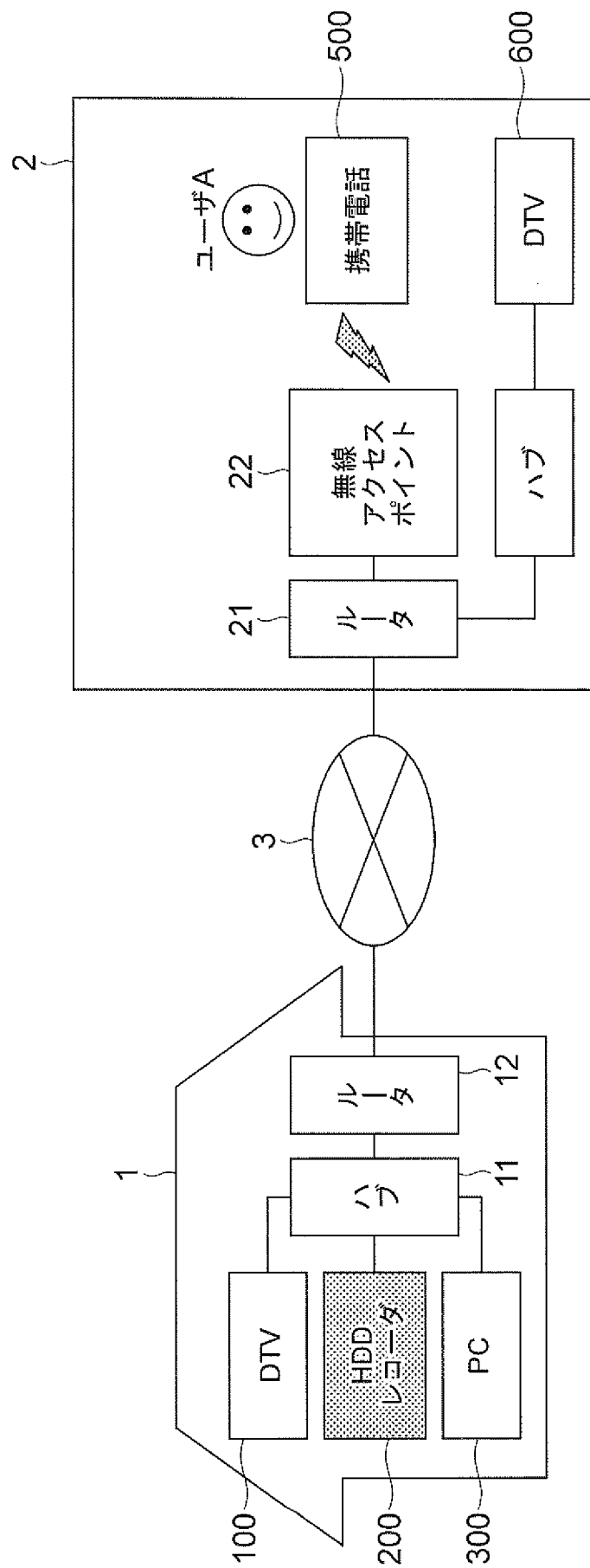
[図12]

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

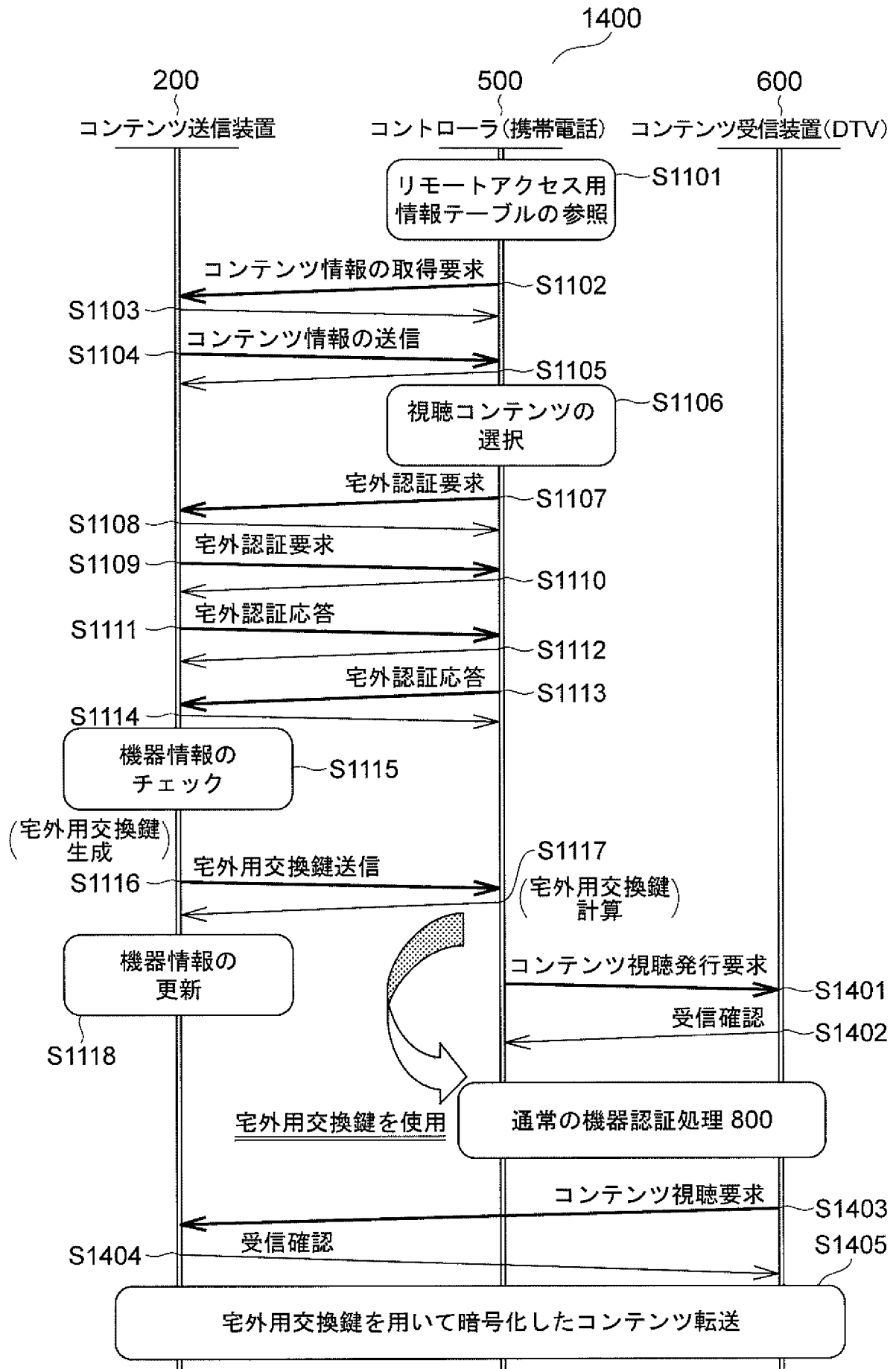
710		アドレス情報 (例:MACアドレス)	宅内用 カウンタ値	宅外アクセス 鍵ラベル	アクセス 状況	宅外用 カウンタ値
ID	デバイスID					
0	aabbccdde (DTV100)	AAAAA	680	—	宅内	—
1	ffgghhiij (携帯電話 500)	BBBBB	459	*@%***#1?	宅外	1500
2	kkllmmnn (PC300)	CCCCC	173	—	停止	—
..	...	...	...	...	...	...
33	...	...	...	...	...	...

717

[図13]



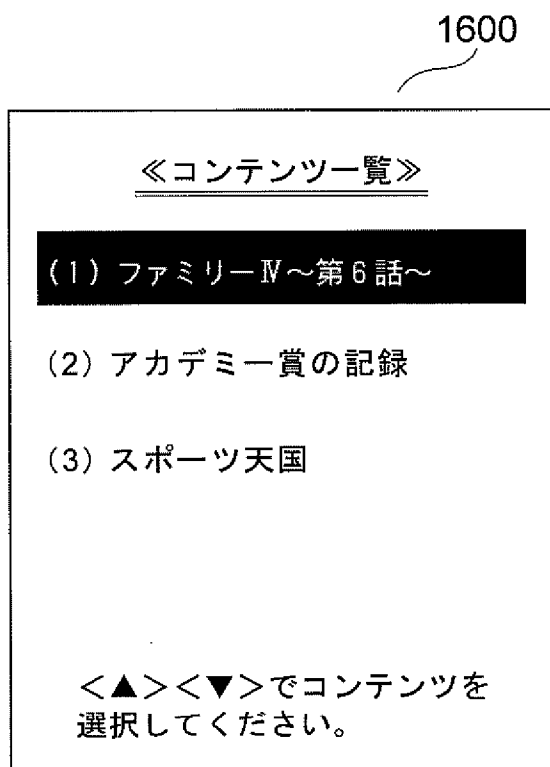
[図14]



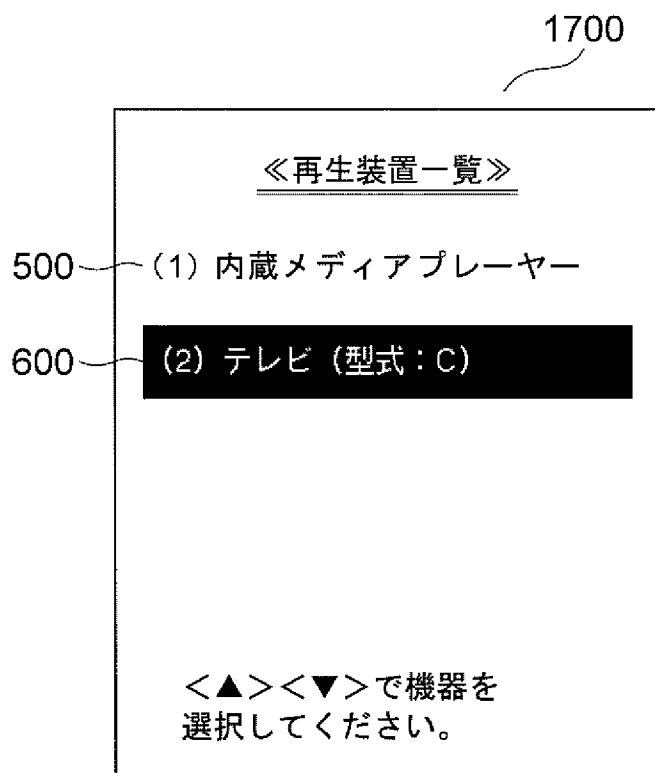
[図15]



[図16]



[図17]



[図18]

700

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

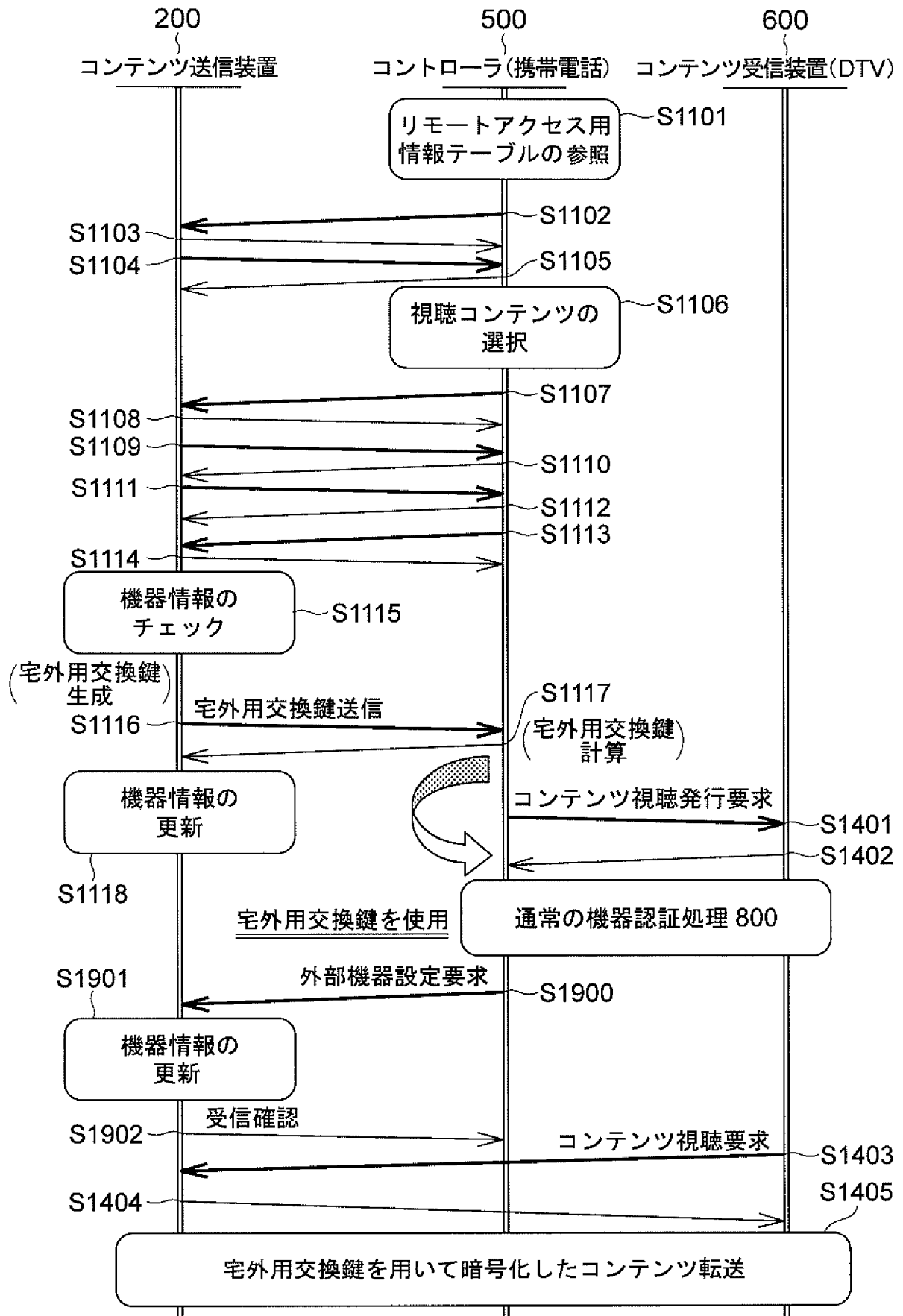
710

712

ID	デバイスID	アドレス情報 (例:MACアドレス)	宅内用 カウンタ値	宅外アクセス鍵	宅外アクセス 鍵ラベル	アクセス 状況	宅外用 カウンタ値	代理 デバイスID
0	aabbcdddee (DTV100)	AAAAA	680	—	—	宅内	—	—
1	ffgghhiiij (携帯電話 500)	BBBBB	459	*@\$%**#1?	XXXXX	宅外	1500	oopppqqrr (DTV600)
2	kkllmmnn (PC300)	CCCCC	173	—	—	停止	—	—
..	...	...	...	...	...	...	...	...
33	...	...	...	...	...	...	...	...

718

[図19]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/052504

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01) i, H04L9/32(2006.01) i, H04N7/16(2006.01) i

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, H04L9/32, H04N7/16

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	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

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.
X Y	JP 2005-269288 A (Hitachi, Ltd.), 29 September, 2005 (29.09.05), Par. Nos. [0019] to [0046] & US 2005/0210290 A1	1-3, 5 4, 6
Y	JP 2005-102021 A (Renesas Technology Corp.), 14 April, 2005 (14.04.05), Par. No. [0030] (Family: none)	4
Y	JP 2007-220095 A (Samsung Electronics Co., Ltd.), 30 August, 2007 (30.08.07), Par. Nos. [0040], [0041] & US 2007/0192837 A1	6

☒ 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
25 February, 2009 (25.02.09)

Date of mailing of the international search report
10 March, 2009 (10.03.09)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/052504

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-180020 A (Toshiba Corp.), 24 June, 2004 (24.06.04), Par. Nos. [0012] to [0085] & US 2004/0158634 A1	1-6

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/08(2006.01)i, H04L9/32(2006.01)i, H04N7/16(2006.01)i

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（I P C））

Int.Cl. H04L9/08, H04L9/32, H04N7/16

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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
X	JP 2005-269288 A（株式会社日立製作所）2005.09.29, 【0019】～ 【0046】段落 & US 2005/0210290 A1	1-3, 5
Y		4, 6
Y	JP 2005-102021 A（株式会社ルネサステクノロジ）2005.04.14, 【0030】段落（ファミリーなし）	4

☒ 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

2 5 . 0 2 . 2 0 0 9

国際調査報告の発送日

1 0 . 0 3 . 2 0 0 9

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

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）

青木 重徳

5 S

3 8 5 7

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 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 2007-220095 A (三星電子株式会社) 2007. 08. 30, 【0040】, 【0041】 段落 & US 2007/0192837 A1	6
A	JP 2004-180020 A (株式会社東芝) 2004. 06. 24, 【0012】 ~ 【0085】 段落 & US 2004/0158634 A1	1-6