(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
2014 年 10 月 2 日(02.10.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/155844 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)

(21) 国際出願番号: PCT/JP2013/082765

(22) 国際出願日: 2013 年 12 月 6 日(06.12.2013)

(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 2013-064222 2013 年 3 月 26 日(26.03.2013) JP

(71) 出願人: ソニー株式会社(SONY CORPORATION) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 Tokyo (JP).

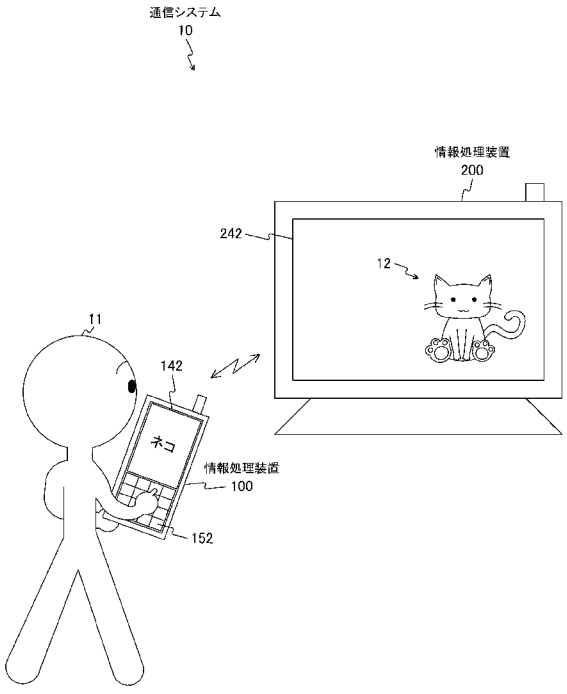
(72) 発明者: 國弘 卓志(KUNIHIRO, Takushi); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 鈴木 健斗(SUZUKI, Kento); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 佐古 曜一郎(SAKO, Yoichiro); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 竹原 充(TAKEHARA, Mitsuru); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 石田 雄仁(ISHIDA, Katsuhito); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 赤木 真(AKAGI, Makoto); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 小野 広一郎(ONO, Kouichirou); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 大沼 智也(ONUMA, Tomoya); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 丹下 明(TANGE, Akira); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 迫田 和之(SAKODA, Kazuyuki); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 小林 径宏(KOBAYASHI, Michihiro); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP).

[続葉有]

(54) **Title**: INFORMATION PROCESSING DEVICE, COMMUNICATION SYSTEM, INFORMATION PROCESSING METHOD, AND PROGRAM

(54) 発明の名称 : 情報処理装置、通信システム、情報処理方法およびプログラム

[図1]



10 Communication system
100, 200 Information processing device

(57) **Abstract**: The present invention appropriately performs connection processing when radio communication is performed between information processing devices. An information processing device is provided with a control unit. The control unit causes authentication key information for approving a radio connection to a second information processing device for a first information processing device, the radio connection transmitting data from the first information processing device to the second information processing device by using radio communication, to be outputted from the second information processing device. The control unit also determines, on the basis of the authentication key information inputted to the first information processing device and the authentication key information outputted from the second information processing device, whether to approve the radio connection for the first information processing device.

(57) 要約:

[続葉有]

WO 2014/155844 A1

(74) 代理人: 丸島　敏一(MARUSHIMA, Toshikazu); 〒1600022 東京都新宿区新宿３－３－２　京王新宿三丁目第二ビル　５Ｆ　クラフト国際特許事務所 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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

情報処理装置間で無線通信を行う場合に接続処理を適切に行う。　情報処理装置は、制御部を具備する。この制御部は、無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送信を行うための第２情報処理装置への無線接続を第１情報処理装置に許可するための認証鍵情報を第２情報処理装置から出力させる。また、その制御部は、第１情報処理装置に入力された認証鍵情報と、第２情報処理装置から出力された認証鍵情報とに基づいて、無線接続を第１情報処理装置に許可するかを決定する。

明　細　書

発明の名称 ：

情報処理装置、通信システム、情報処理方法およびプログラム

技術分野

[0001] 本技術は、情報処理装置に関する。詳しくは、無線通信を利用して情報処理装置間でデータの送受信を行う情報処理装置、通信システムおよび情報処理方法ならびに当該方法をコンピュータに実行させるプログラムに関する。

背景技術

[0002] 従来、無線通信を利用して各種データのやり取りを行う無線通信技術が存在する。例えば、無線通信を利用して周囲の情報処理装置と接続して画像データの通信を行う画像生成装置が提案されている（例えば、特許文献１参照。）。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１２－１４１５７０号公報

発明の概要

発明が解決しようとする課題

[0004] 上述の従来技術では、無線通信を利用して周囲の情報処理装置と接続することができるため、周囲の情報処理装置との間で画像データの通信を容易に行うことができる。

[0005] ここで、例えば、情報処理装置（ソースデバイス）に保持されているコンテンツを、他の情報処理装置（シンクデバイス）に無線通信を利用して送信し、シンクデバイスに表示させる場合を想定する。この場合には、そのように表示してもよいか否かの認証が必要となる。しかしながら、ソースデバイスの周囲にシンクデバイスが複数存在するような場合には、ソースデバイスが、意図しないシンクデバイスと接続されてしまうことも想定される。この場合には、意図しない相手に、ソースデバイスに保持されているコンテンツ

を見られてしまうおそれがある。

[0006] 本技術はこのような状況に鑑みて生み出されたものであり、情報処理装置間で無線通信を行う場合に接続処理を適切に行うことを目的とする。

課題を解決するための手段

[0007] 本技術は、上述の問題点を解消するためになされたものであり、その第１の側面は、無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送信を行うための上記第２情報処理装置への無線接続を上記第１情報処理装置に許可するための認証鍵情報を上記第２情報処理装置から出力させ、上記第１情報処理装置に入力された認証鍵情報と上記出力された認証鍵情報とに基づいて上記無線接続を上記第１情報処理装置に許可するかを決定する制御部を具備する情報処理装置およびその情報処理方法ならびに当該方法をコンピュータに実行させるプログラムである。これにより、認証鍵情報を第２情報処理装置から出力させ、第１情報処理装置に入力された認証鍵情報と、第２情報処理装置から出力された認証鍵情報とに基づいて、無線接続を第１情報処理装置に許可するかを決定するという作用をもたらす。

[0008] また、この第１の側面において、上記情報処理装置は、上記第２情報処理装置であり、上記第１情報処理装置から送信されたデータを出力する出力部をさらに具備し、上記制御部は、上記認証鍵情報を上記出力部から出力させ、上記無線接続を上記第１情報処理装置に許可する決定がされた後に上記第１情報処理装置から送信されたデータを上記出力部から出力させるようにしてもよい。これにより、無線接続を第１情報処理装置に許可する決定がされた後に第１情報処理装置から送信されたデータを出力させるという作用をもたらす。

[0009] また、この第１の側面において、上記出力部は、上記第１情報処理装置から送信された画像データに基づく画像を表示する表示部であり、上記制御部は、上記認証鍵情報を上記表示部に表示させ、上記無線接続を上記第１情報処理装置に許可する決定がされた後に上記第１情報処理装置から送信された画像データに基づく画像を上記表示部に表示させるようにしてもよい。これ

により、無線接続を第１情報処理装置に許可する決定がされた後に第１情報処理装置から送信された画像データに基づく画像を表示させるという作用をもたらす。

[0010] また、この第１の側面において、上記第１情報処理装置は、上記第２情報処理装置から出力された認証鍵情報を入力するための入力部から入力された認証鍵情報を上記情報処理装置に送信し、上記制御部は、上記第１情報処理装置から送信された認証鍵情報と上記出力された認証鍵情報とに基づいて上記決定を行うようにしてもよい。これにより、第１情報処理装置から送信された認証鍵情報と、第２情報処理装置から出力された認証鍵情報とに基づいて決定を行うという作用をもたらす。

[0011] また、この第１の側面において、上記入力部を、上記第２情報処理装置から出力された認証鍵情報を撮像する撮像部と、上記第２情報処理装置から出力された認証鍵情報を入力するためのユーザ操作を受け付ける操作受付部とのうちの少なくとも１つとするようにしてもよい。これにより、撮像部および操作受付部のうちの少なくとも１つを用いて認証鍵情報を入力するという作用をもたらす。

[0012] また、この第１の側面において、上記制御部は、上記第１情報処理装置に入力された認証鍵情報と上記出力された認証鍵情報とが一致すると判定された場合に上記無線接続を上記第１情報処理装置に許可すると決定するようにしてもよい。これにより、第１情報処理装置に入力された認証鍵情報と、第２情報処理装置から出力された認証鍵情報とが一致すると判定された場合に、無線接続を第１情報処理装置に許可すると決定するという作用をもたらす。

[0013] また、この第１の側面において、上記制御部は、複数の上記第２情報処理装置のうちからユーザ操作により選択された第２情報処理装置への無線接続を上記第１情報処理装置に許可するための認証鍵情報を上記選択された第２情報処理装置から出力させるようにしてもよい。これにより、複数の第２情報処理装置のうちからユーザ操作により選択された第２情報処理装置への無

線接続を第１情報処理装置に許可するための認証鍵情報を、その選択された第２情報処理装置から出力させるという作用をもたらす。

[0014] また、この第１の側面において、上記第１情報処理装置は、複数の上記第２情報処理装置に関する情報を表示させ、当該表示されている複数の第２情報処理装置のうちからユーザ操作により選択された第２情報処理装置に関する情報を上記情報処理装置に送信し、上記制御部は、上記送信された第２情報処理装置に関する情報に基づいて当該第２情報処理装置への無線接続を上記第１情報処理装置に許可するための認証鍵情報を当該第２情報処理装置から出力させるようにしてもよい。これにより、第１情報処理装置から送信された第２情報処理装置に関する情報に基づいて、その第２情報処理装置への無線接続を第１情報処理装置に許可するための認証鍵情報を、その第２情報処理装置から出力させるという作用をもたらす。

[0015] また、この第１の側面において、上記制御部は、上記無線接続を上記第１情報処理装置に許可する決定がされ、上記第１情報処理装置および上記第２情報処理装置が接続状態となっている場合に、上記認証鍵情報を上記第２情報処理装置から出力させるための要求を他の情報処理装置から受信したときには上記要求を拒否するようにしてもよい。これにより、無線接続を第１情報処理装置に許可する決定がされ、第１情報処理装置および第２情報処理装置が接続状態となっている場合に、認証鍵情報を第２情報処理装置から出力させるための要求を他の情報処理装置から受信したときにはその要求を拒否するという作用をもたらす。

[0016] また、この第１の側面において、上記制御部は、上記接続状態が開放された後に上記要求を上記他の情報処理装置から受信したときには上記要求に応じて上記認証鍵情報を上記第２情報処理装置から出力させるようにしてもよい。これにより、接続状態が開放された後に、その要求を他の情報処理装置から受信したときにはその要求に応じて認証鍵情報を第２情報処理装置から出力させるという作用をもたらす。

[0017] また、この第１の側面において、上記制御部は、上記接続状態で上記要求

を上記他の情報処理装置から受信した場合において、上記他の情報処理装置の優先度が上記第１情報処理装置の優先度よりも高い場合には上記要求を拒否せずに上記接続状態を開放するようにしてもよい。これにより、その接続状態でその要求を他の情報処理装置から受信した場合において、他の情報処理装置の優先度が第１情報処理装置の優先度よりも高い場合にはその要求を拒否せずにその接続状態を開放するという作用をもたらす。

[0018] また、この第１の側面において、上記制御部は、上記第１情報処理装置からの要求に応じて上記認証鍵情報を上記第２情報処理装置から出力させ、上記無線接続を拒否するためのユーザ操作が受け付けられた場合には、上記無線接続を上記第１情報処理装置に許可しないと決定するようにしてもよい。これにより、第１情報処理装置からの要求に応じて認証鍵情報を第２情報処理装置から出力させ、無線接続を拒否するためのユーザ操作が受け付けられた場合には、無線接続を第１情報処理装置に許可しないと決定するという作用をもたらす。

[0019] また、この第１の側面において、上記制御部は、上記第２情報処理装置へのデータ送信を行う上記第１情報処理装置が複数存在する場合には、所定規則に基づいて上記複数の第１情報処理装置のそれぞれに上記無線接続を許可するための上記第１情報処理装置毎の認証鍵情報を上記第２情報処理装置から順次出力させるようにしてもよい。これにより、第２情報処理装置へのデータ送信を行う第１情報処理装置が複数存在する場合には、所定規則に基づいて複数の第１情報処理装置のそれぞれに無線接続を許可するための第１情報処理装置毎の認証鍵情報を第２情報処理装置から順次出力させるという作用をもたらす。

[0020] また、この第１の側面において、上記制御部は、上記第１情報処理装置の数に基づいて上記第２情報処理装置へのデータ送信を行うための接続時間を決定し、上記接続時間に基づいて上記複数の第１情報処理装置のそれぞれに所定順序で上記第１情報処理装置毎の認証鍵情報を上記第２情報処理装置から順次出力させるようにしてもよい。これにより、第１情報処理装置の数に

基づいて第２情報処理装置へのデータ送信を行うための接続時間を決定し、この接続時間に基づいて複数の第１情報処理装置のそれぞれに所定順序で第１情報処理装置毎の認証鍵情報を第２情報処理装置から順次出力させるという作用をもたらす。

[0021] また、この第１の側面において、上記情報処理装置は、上記第１情報処理装置であり、上記第２情報処理装置から出力された認証鍵情報を入力するための入力部をさらに具備し、上記制御部は、上記無線通信を利用して上記第２情報処理装置に上記認証鍵情報を送信して上記第２情報処理装置から出力させ、上記入力部に入力された認証鍵情報と上記出力された認証鍵情報とに基づいて上記無線接続を許可するかを決定し、上記無線通信を利用して当該決定の結果を上記第２情報処理装置に送信するようにしてもよい。これにより、無線通信を利用して第２情報処理装置に認証鍵情報を送信して第２情報処理装置から出力させ、入力部に入力された認証鍵情報と、第２情報処理装置から出力された認証鍵情報とに基づいて無線接続を許可するかを決定し、無線通信を利用してその決定の結果を第２情報処理装置に送信するという作用をもたらす。

[0022] また、この第１の側面において、上記情報処理装置は、上記第２情報処理装置にネットワークを介して接続されるサーバであり、上記制御部は、上記ネットワークを介して上記第２情報処理装置に上記認証鍵情報を送信して上記第２情報処理装置から出力させ、上記無線接続を上記第１情報処理装置に許可する決定がされた後に上記第１情報処理装置から送信されたデータを、上記ネットワークを介して上記第２情報処理装置に送信して上記第２情報処理装置から出力させるようにしてもよい。これにより、ネットワークを介して第２情報処理装置に認証鍵情報を送信して第２情報処理装置から出力させ、無線接続を第１情報処理装置に許可する決定がされた後に第１情報処理装置から送信されたデータを、ネットワークを介して第２情報処理装置に送信して第２情報処理装置から出力させるという作用をもたらす。

[0023] また、本技術の第２の側面は、無線通信を利用して第２情報処理装置への

データ送信を行う第１情報処理装置と、上記第１情報処理装置からのデータを受信して出力する第２情報処理装置とを具備する通信システムであって、上記データ送信を行うための上記第２情報処理装置への無線接続を上記第１情報処理装置に許可するための認証鍵情報が上記第２情報処理装置から出力され、上記第１情報処理装置に入力された認証鍵情報と上記出力された認証鍵情報とに基づいて上記無線接続を上記第１情報処理装置に許可するかが決定される通信システムおよびその情報処理方法ならびに当該方法をコンピュータに実行させるプログラムである。これにより、認証鍵情報が第２情報処理装置から出力され、第１情報処理装置に入力された認証鍵情報と、第２情報処理装置から出力された認証鍵情報とに基づいて、無線接続を第１情報処理装置に許可するかが決定されるという作用をもたらす。

発明の効果

[0024] 本技術によれば、情報処理装置間で無線通信を行う場合に接続処理を適切に行うことができるという優れた効果を奏し得る。

図面の簡単な説明

[0025] [図1]本技術の第１の実施の形態における通信システム１０の構成例を示す図である。

[図2]本技術の第１の実施の形態における情報処理装置１００の内部構成例を示すブロック図である。

[図3]本技術の第１の実施の形態における情報処理装置２００の内部構成例を示すブロック図である。

[図4]本技術の第１の実施の形態における通信システム１０を構成する各装置間において通信される情報３００のフォーマット例を模式的に示す図である。

[図5]本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図6]本技術の第１の実施の形態における情報処理装置２００の表示部２４２に表示される鍵画像の表示例を示す図である。

[図7]本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図8]本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図9]本技術の第１の実施の形態における通信システム２０の構成例を示す図である。

[図10]本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図11]本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図12]本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図13]本技術の第２の実施の形態における通信システム３０の構成例を示す図である。

[図14]本技術の第２の実施の形態における通信システム３０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図15]本技術の第２の実施の形態における通信システム３０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図16]本技術の第２の実施の形態における通信システム３０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図17]本技術の第３の実施の形態における通信システム４０の構成例を示す図である。

[図18]本技術の第３の実施の形態における通信システム４０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図19]本技術の第３の実施の形態における情報処理装置２００による通信処理の処理手順の一例を示すフローチャートである。

[図20]本技術の第３の実施の形態における情報処理装置２００による通信処理の処理手順の一例を示すフローチャートである。

[図21]本技術の第３の実施の形態における情報処理装置１００による通信処理の処理手順の一例を示すフローチャートである。

[図22]本技術の第４の実施の形態における通信システム５０の構成例を示す図である。

[図23]本技術の第４の実施の形態における通信システム６０の構成例を示す図である。

[図24]本技術の第４の実施の形態における通信システム６０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図25]本技術の第４の実施の形態における通信システム６０を構成する各装置間における通信処理例を示すシーケンスチャートである。

[図26]本技術の第４の実施の形態における通信システム７０の構成例を示す図である。

[図27]本技術の第４の実施の形態における通信システム７０を構成する各装置間における通信処理例を示すシーケンスチャートである。

発明を実施するための形態

[0026] 以下、本技術を実施するための形態（以下、実施の形態と称する）について説明する。説明は以下の順序により行う。

１．第１の実施の形態（通信制御：シンクデバイスから出力された認証鍵情報と、ソースデバイスに入力された認証鍵情報とを用いて無線接続の認証を行う例）

２．第２の実施の形態（通信制御：ソースデバイスおよびシンクデバイス間において無線通信が行われている状態で他のソースデバイス接続要求がされた場合の例）

３．第３の実施の形態（通信制御：ソースデバイスの接続状態を適切なタイミングで切り替える例）

４．第４の実施の形態（通信制御：ソースデバイスおよびシンクデバイス以外の他の装置により生成された認証鍵情報を用いて認証を行う例）

[0027] ＜１．第１の実施の形態＞

［通信システムの構成例］

図１は、本技術の第１の実施の形態における通信システム１０の構成例を示す図である。図１では、２つの情報処理装置（情報処理装置１００および２００）を直接無線接続する際におけるシステム構成の一例を示す。

[0028] 通信システム１０は、情報処理装置１００および２００を備える。情報処理装置１００は、例えば、無線通信機能を備える電子機器（例えば、携帯電話、スマートフォン、タブレット端末等の無線通信装置（例えば、小型の携帯機器））である。また、情報処理装置２００は、例えば、無線通信機能を備える電子機器（例えば、画像および音声を出力する映像視聴装置（例えば、大型のテレビジョン））である。

[0029] 例えば、情報処理装置１００および２００は、ＩＥＥＥ（Institute of Electrical and Electronics Engineers）８０２．１１仕様に準拠した無線通信装置である。そして、情報処理装置１００および２００は、無線通信機能を利用して各種情報のやり取りを行うことができる。

[0030] ここで、通信システム１０に用いられる無線通信として、例えば、無線ＬＡＮ（Local Area Network）を用いることができる。この無線ＬＡＮとして、例えば、Ｗｉ－Ｆｉ（登録商標）（Wireless Fidelity） Ｄｉｒｅｃｔ、ＴＤＬＳ（Tunneled Direct Link Setup）、アドホックネットワークを用いることができる。また、通信システム１０に用いられる近距離無線ＡＶ（Audio Visual）伝送通信として、例えば、Ｗｉ－Ｆｉ ＣＥＲＴＩＦＩＥＤ Ｍｉｒａｃａｓｔを用いることができる。なお、Ｗｉ－Ｆｉ ＣＥＲＴＩＦＩＥＤ Ｍｉｒａｃａｓｔは、Ｗｉ－Ｆｉ ＤｉｒｅｃｔやＴＤＬＳの技術を利用して、一方の端末で再生される音声や表示映像を他の端末に送信し、他の端末でも同様にその音声、映像データを出力させるミラーリング技術である。

[0031] また、通信システム１０に用いられる無線通信として、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）（ＩＥＥＥ８０２．１５．１）、ＺｉｇＢｅｅ（ＩＥＥＥ８０２．１５．４）、赤外線通信等を用いることができる。また、通

信システム１０に用いられる無線通信として、例えば、公衆網（例えば、３Ｇ（3rd Generation）、ＬＴＥ（Long Term Evolution））を用いるようにしてもよい。

[0032] なお、本技術の実施の形態では、情報処理装置１００をソースデバイス（Source Device）とし、情報処理装置２００をシンクデバイス（Sink Device）とする例について説明する。ここで、ソースデバイスは、コンテンツを送信する送信側の情報処理装置を意味し、シンクデバイスは、コンテンツを受信して出力する受信側の情報処理装置を意味するものとする。例えば、ソースデバイスは、静止画、動画等のコンテンツ（ユーザコンテンツ）が格納されている情報処理装置（例えば、小型デバイス）である。また、例えば、シンクデバイスは、無線通信を利用して受信したコンテンツを出力（例えば、画像表示、音声出力）する情報処理装置（例えば、大型デバイス）である。

[0033] 情報処理装置１００は、無線通信を利用して、メモリ１３０（図２に示す）に記憶されているコンテンツ（例えば、画像データおよび音声データ）を情報処理装置２００に送信することができる。例えば、情報処理装置１００は、Ｗｉ－Ｆｉ ＣＥＲＴＩＦＩＥＤ Ｍｉｒａｃａｓｔを利用して、コンテンツを情報処理装置２００に送信することができる。なお、情報処理装置１００は、請求の範囲に記載の第１情報処理装置の一例である。

[0034] また、情報処理装置２００は、情報処理装置１００から送信されたコンテンツに基づく画像を表示部２４２に表示する。また、情報処理装置２００は、情報処理装置１００から送信されたコンテンツに基づく音声を音声出力部２７２（図３に示す）から出力する。なお、情報処理装置２００は、請求の範囲に記載の第２情報処理装置の一例である。

[0035] ここで、近年では、個人が所有する装置（例えば、スマートフォンやタブレット端末等の小型デバイス）を用いて、写真や動画を撮影して観ることができる。また、これらの写真や動画を複数人で観ることによりさらに楽しみを広げることができると考えられる。しかしながら、これらの装置（小型デバイス）の表示部（ディスプレイ）は小さいため、複数人で観ることに適し

ていないことが多い。

[0036] そのため、サイズが大きい表示部を備える装置（例えば、大型テレビジョン等の大画面ディスプレイ装置（大型デバイス））に写真や動画を表示することが想定される。例えば、無線通信（例えば、無線ＬＡＮ）を利用して、手元の小型デバイスから大型デバイスに写真や動画の情報（コンテンツ）を送信して表示させることが想定される。

[0037] ここで、無線通信を利用して情報の通信を行う場合には、一般に、ソースデバイスとシンクデバイスとをペアリングし、ソースデバイスからの情報を特定のシンクデバイスに表示してもよいという認証（Authorization）を行うことが必要になる。

[0038] 例えば、ソースデバイスとシンクデバイスの所有者が同一人物である場合には、最初に一度だけ両者に同一の鍵情報を与えることにより、ペアリングおよび認証を実現することができる。この方法は、例えば、Ｂｌｕｅｔｏｏｔｈのペアリングで実現されている。なお、同一の鍵情報は、例えば、ＰＩＮコード（Personal Identification Number Code）である。

[0039] ここで、シンクデバイスの所有者が個人ではない場合（例えば、ホテルの部屋に設置されているテレビがシンクデバイスである場合）を想定する。この場合には、シンクデバイス（例えば、テレビ）の鍵情報入力方法が装置毎に異なることが多く、鍵情報の入力が利用者にとって困難となることが想定される。

[0040] そこで、同一の鍵情報（例えば、ＰＩＮコード）を入力する代わりに、コンテンツの通信に用いる無線通信機能（例えば、無線ＬＡＮ）以外の近接無線通信機能を利用して認証を行う方法も提案されている。しかしながら、この場合には、ソースデバイスおよびシンクデバイスが複数の無線通信機能（例えば、無線ＬＡＮ、近接無線通信機能）を備える必要があるため、装置のコストが上昇するおそれがある。

[0041] そこで、単一の無線通信機能（例えば、無線ＬＡＮ）を利用して鍵情報を交換することも考えられる。ここで、ホテル等の施設では、同一施設内に複

数のシンクデバイス（例えば、ホテルの各部屋に設置されているテレビ）が設置されていることが多い。このため、例えば、ユーザが宿泊している部屋に隣接する部屋に設置されているシンクデバイスが、そのユーザが所有するソースデバイスの電波到達範囲となることも想定される。この場合には、そのユーザが宿泊している部屋に設置されているシンクデバイス以外のシンクデバイス（例えば、隣接する部屋に設置されているテレビ）との間で誤って鍵交換をしてしまうおそれがある。このように、鍵交換が誤って行われた場合には、意図しないシンクデバイスに情報を送信してしまい、他のユーザにその情報を見られてしまうおそれがある。

[0042] そこで、本技術の実施の形態では、ソースデバイスを所有するユーザが使用を所望するシンクデバイスに認証鍵情報を表示させ、この認証鍵情報を利用してソースデバイスおよびシンクデバイス間でペアリングおよび認証を行う例を示す。例えば、図１に示すように、情報処理装置１００を所有するユーザ１１が使用を所望する情報処理装置２００の表示部２４２に認証鍵情報（例えば、鍵が画像化された猫画像１２）を表示させる。この場合に、表示部２４２に表示されている認証鍵情報（猫画像１２）を利用して情報処理装置１００（ソースデバイス）および情報処理装置２００（シンクデバイス）間でペアリングおよび認証を行う。例えば、表示部２４２に表示されている認証鍵情報（猫画像１２）を見たユーザ１１に、操作受付部１５２を用いてその認証鍵情報（例えば、「ネコ」）を入力させる。これにより、情報処理装置１００および情報処理装置２００間でペアリングおよび認証を適切に行うことができる。

[0043] このように、ユーザ１１が使用を所望する情報処理装置２００（シンクデバイス）に認証鍵情報（猫画像１２）を表示させ、その認証鍵情報（猫画像１２）をユーザ１１（または、情報処理装置１００（ソースデバイス））に認識させる。これにより、ユーザ１１は、情報処理装置２００（シンクデバイス）が情報（コンテンツ）の出力先であることを確実に認識することができる。また、ユーザ１１が所有する情報処理装置１００（ソースデバイス）

から、使用を所望する情報処理装置２００（シンクデバイス）に認証鍵情報を送信し、ユーザ１１が意図するシンクデバイスとの間でペアリングおよび認証を行うことができる。

[0044] ここで、認証鍵情報として、ある範囲内（情報処理装置１００（ソースデバイス）が存在する位置を基準とする所定範囲内）で一意であることを確認することができる情報を用いることができる。例えば、ソースデバイスやシンクデバイスのデバイスアドレスを用いるようにしてもよい。

[0045] また、認証鍵情報は、ペアリングおよび認証が行われる毎に変更されることが好ましい。例えば、他の動物（例えば、犬、馬、牛、山羊）や、記号、文字等に順次変更することができる。

[0046] ［情報処理装置（ソースデバイス）の構成例］

図２は、本技術の第１の実施の形態における情報処理装置１００の内部構成例を示すブロック図である。

[0047] 情報処理装置１００は、アンテナ１１１と、通信部１１２と、制御部１２０と、メモリ１３０と、表示情報入出力部１４１と、表示部１４２とを備える。また、情報処理装置１００は、操作情報入出力部１５１と、操作受付部１５２と、撮像情報入出力部１６１と、撮像部１６２と、音声情報入出力部１７１と、音声入力部１７２と、音声出力部１７３とを備える。また、これらの各部は、バス１８０を介して接続される。

[0048] 通信部１１２は、アンテナ１１１を介して、電波の送受信を行うためのモジュール（例えば、モデム）である。例えば、通信部１１２は、無線ＬＡＮ（Local Area Network）により無線通信を行うことができる。

[0049] 例えば、通信部１１２は、制御部１２０の制御に基づいて、無線通信を利用して所定範囲内に存在する他の無線通信装置との間で、各情報（認証鍵情報、鍵画像、コンテンツ）の送受信を行う。ここで、所定範囲は、例えば、情報処理装置１００の位置を基準とする範囲であり、通信部１１２が、無線通信を利用してデータの送受信を行うことが可能な範囲を意味するものとする。また、所定範囲内に存在する他の無線通信装置は、例えば、情報処理装

置１００の近隣に存在する無線通信装置であって、無線通信を利用して情報処理装置１００との間でデータの送受信を行うことが可能な無線通信装置であるものとする。なお、上述した無線ＬＡＮ以外の他の無線通信機能を用いて無線通信を行うようにしてもよい。

[0050] 制御部１２０は、メモリ１３０に格納されている制御プログラムに基づいて情報処理装置１００の各部を制御するものである。例えば、制御部１２０は、送受信した情報の信号処理を行う。また、制御部１２０は、例えば、ＣＰＵ（Central Processing Unit）により実現される。

[0051] メモリ１３０は、各種情報を格納するメモリである。例えば、メモリ１３０には、情報処理装置１００が所望の動作を行うために必要となる各種情報（例えば、制御プログラム）が格納される。また、メモリ１３０には、再生対象となるコンテンツ（例えば、動画コンテンツ、静止画コンテンツ）等の各種コンテンツが格納される。

[0052] 例えば、無線通信を利用してデータを送信する場合には、制御部１２０は、メモリ１３０から読み出された情報や操作受付部１５２から入力された信号等を処理し、実際に送信するデータの塊（送信パケット）を生成する。続いて、制御部１２０は、その生成された送信パケットを通信部１１２に出力する。また、通信部１１２は、その送信パケットを、実際に伝送するための通信方式のフォーマット等に変換した後に、変換後の送信パケットをアンテナ１１１から外部に送信する。

[0053] また、例えば、無線通信を利用してデータを受信する場合には、通信部１１２は、アンテナ１１１を介して受信した電波信号を、通信部１１２内の受信機が行う信号処理により受信パケットを抽出する。そして、制御部１２０は、その抽出された受信パケットを解釈する。この解釈の結果、保持すべきデータであると判断された場合には、制御部１２０は、そのデータをメモリ１３０に書き込む。

[0054] 例えば、制御部１２０は、メモリ１３０に格納されている各種コンテンツを、無線通信を利用して他の無線通信装置に提供することができる。

[0055] 表示部１４２は、制御部１２０の制御に基づいて、表示情報入出力部１４１を介して供給される各種情報（例えば、図９に示す表示画面）を表示する表示部である。なお、表示部１４２として、例えば、有機ＥＬ（Electro Luminescence）パネル、ＬＣＤ（Liquid Crystal Display）パネル等の表示パネルを用いることができる。

[0056] ここで、情報処理装置１００がスマートフォンである場合には、表示部１４２のサイズ（ディスプレイサイズ）は、例えば、４インチから５インチ程度の大きさとなることが多い。また、情報処理装置１００がタブレット端末である場合には、表示部１４２のサイズ（ディスプレイサイズ）は、例えば、７インチから１０インチ程度の大きさとなることが多い。

[0057] 操作受付部１５２は、ユーザにより行われた操作入力を受け付ける操作受付部であり、受け付けられた操作入力に応じた操作情報を、操作情報入出力部１５１を介して制御部１２０に出力する。操作受付部１５２は、例えば、タッチパネル、キーボード（または、タッチパネル上のバーチャルキーボード）、マウスにより実現される。なお、操作受付部１５２および表示部１４２については、使用者がその指を表示面に接触または近接することにより操作入力を行うことが可能なタッチパネルを用いて一体で構成することができる。

[0058] 撮像部１６２は、制御部１２０の制御に基づいて、被写体を撮像して画像データ（静止画データ、動画データ）を生成するものであり、この生成された画像データを、撮像情報入出力部１６１を介して制御部１２０に出力する。また、制御部１２０は、このように生成された画像データを画像コンテンツ（静止画コンテンツ、動画コンテンツ）としてメモリ１３０に記録させる。また、撮像部１６２は、鍵画像を撮像して鍵画像を生成する。撮像部１６２は、例えば、光学系（複数のレンズ）、撮像素子、信号処理部より構成される。なお、撮像素子として、例えば、ＣＣＤ（Charge Coupled Device）やＣＭＯＳ（Complementary Metal Oxide Semiconductor）を用いることができる。なお、操作受付部１５２および撮像部１６２のうちの少なくとも１つは

、認証鍵情報を入力するための入力部として機能する。すなわち、操作受付部１５２および撮像部１６２は、請求の範囲に記載の入力部の一例である。

[0059] 音声入力部１７２は、情報処理装置１００の周囲の音を取得する音声入力部（例えば、マイクロフォン）であり、取得された音に関する情報（音声情報）を、音声情報入出力部１７１を介して制御部１２０に出力する。

[0060] 音声出力部１７３は、制御部１２０の制御に基づいて、音声情報入出力部１７１を介して供給される各種音声を出力する音声出力部（例えば、スピーカ）である。

[0061] ［情報処理装置（シンクデバイス）の構成例］

図３は、本技術の第１の実施の形態における情報処理装置２００の内部構成例を示すブロック図である。

[0062] 情報処理装置２００は、アンテナ２１１と、通信部２１２と、制御部２２０と、メモリ２３０と、表示情報入出力部２４１と、表示部２４２とを備える。また、情報処理装置２００は、操作情報入出力部２５１と、操作受付部２５２と、リモートコントローラ情報入出力部２６１と、音声情報入出力部２７１と、音声出力部２７２とを備える。また、これらの各部は、バス２８０を介して接続される。

[0063] 情報処理装置２００は、例えば、表示部２４２のサイズ（ディスプレイサイズ）が、情報処理装置１００のディスプレイサイズよりも大きい情報処理装置である。

[0064] また、アンテナ２１１、通信部２１２、表示情報入出力部２４１、表示部２４２、音声情報入出力部２７１および音声出力部２７２については、図２に示す同一名称の各部に対応する。このため、これらについては、ここでの詳細な説明を省略する。例えば、表示部２４２は、情報処理装置１００から送信された画像データに基づく画像を表示する。また、例えば、音声出力部２７２は、情報処理装置１００から送信された音声データに基づく音声を出力する。なお、表示部２４２および音声出力部２７２は、請求の範囲に記載の出力部の一例である。

[0065] 制御部２２０は、メモリ２３０に格納されている制御プログラムに基づいて情報処理装置１００の各部を制御するものである。例えば、制御部２２０は、送受信した情報の信号処理を行う。また、制御部２２０は、例えば、ＣＰＵにより実現される。

[0066] メモリ２３０は、各種情報を格納するメモリである。例えば、メモリ２３０には、情報処理装置２００が所望の動作を行うために必要となる各種情報（例えば、制御プログラム）が格納される。また、メモリ２３０には、再生対象となるコンテンツ（例えば、動画コンテンツ、静止画コンテンツ）等の各種コンテンツが格納される。

[0067] 例えば、制御部２２０は、無線通信を利用して他の無線通信装置から提供された各種コンテンツを出力（画像表示、音声出力）させることができる。

[0068] また、例えば、制御部２２０は、無線通信を利用して情報処理装置１００から情報処理装置２００へのデータ送信を行うための情報処理装置２００への無線接続を情報処理装置１００に許可するための認証鍵情報を表示部２４２に表示させる。例えば、図１に示すように、認証鍵情報として猫画像１２が表示部２４２に表示される。また、例えば、制御部２２０は、情報処理装置１００に入力された認証鍵情報と、表示部２４２に表示された認証鍵情報とに基づいて、その無線接続を情報処理装置１００に許可するかを決定する。例えば、制御部２２０は、情報処理装置１００に入力された認証鍵情報と、表示部２４２に出力された認証鍵情報とが一致すると判定された場合に、その無線接続を情報処理装置１００に許可すると決定する。また、例えば、制御部２２０は、無線接続を情報処理装置１００に許可する決定がされた後に、情報処理装置１００から送信されたコンテンツに基づく画像を表示部２４２に表示させ、そのコンテンツに基づく音声を音声出力部２７２から出力させる。

[0069] 操作受付部２５２は、ユーザにより行われた操作入力を受け付ける操作受付部であり、受け付けられた操作入力に応じた操作情報を、操作情報入出力部２５１を介して制御部２２０に出力する。操作受付部２５２は、例えば、

ボタン等の操作部材（例えば、電源ボタン、設定ボタン）により実現される。なお、操作受付部２５２および表示部２４２については、使用者がその指を表示面に接触または近接することにより操作入力を行うことが可能なタッチパネルを用いて一体で構成することができる。

[0070] リモートコントローラ２６２は、離れた場所から情報処理装置２００を遠隔操作するためのリモートコントローラであり、ユーザによる操作入力に応じた操作信号（リモートコントローラ情報）をリモートコントローラ情報入出力部２６１に送信する。例えば、リモートコントローラ２６２の出力信号として赤外線信号を用いることができる。

[0071] リモートコントローラ情報入出力部２６１は、リモートコントローラ２６２からの操作信号（リモートコントローラ情報）の入出力を行うものである。例えば、リモートコントローラ情報入出力部２６１は、リモートコントローラ２６２からの操作信号を受け付けると、受け付けられた操作信号を制御部２２０に供給する。

[0072] ［情報フォーマット例］

図４は、本技術の第１の実施の形態における通信システム１０を構成する各装置間において通信される情報３００のフォーマット例を模式的に示す図である。すなわち、図４には、ソースデバイスおよびシンクデバイス間で通信される情報３００のフォーマット例を示す。

[0073] ソースデバイスおよびシンクデバイス間で通信される情報３００には、ソースデバイスＩＤ３０１と、シンクデバイスＩＤ３０２と、情報要素識別子３０３と、データ３０４とが含まれる。

[0074] ソースデバイスＩＤ３０１は、ソースデバイスを識別するための識別情報（Identification Number）である。また、シンクデバイスＩＤ３０２は、シンクデバイスを識別するための識別情報である。これらの識別情報として、例えば、機器固有のＩＤ（例えば、ＭＡＣ（Media Access Control）アドレス）を用いることができる。

[0075] 情報要素識別子３０３は、送信対象となる情報が何であるかを識別するた

めの情報である。例えば、情報要素識別子３０３には、表示鍵情報３１０乃至拒否理由通知３１９の何れかを識別するための情報が格納される。

[0076] 表示鍵情報３１０は、データ３０４の内容が、シンクデバイスに鍵画像を表示するための鍵コードであることを示す情報である。この鍵コードは、例えば、シンクデバイスに表示すべき鍵画像を特定するための識別情報である。すなわち、この鍵コードは、シンクデバイスが、鍵を画像情報に変換するための情報である。例えば、猫の画像を特定するための鍵コードを「００１」とし、犬の画像を特定するための鍵コードを「００２」とする。この場合に、シンクデバイスに表示すべき鍵画像が、猫の画像（例えば、図１に示す猫画像１２）である場合には、猫の画像を特定するための鍵コード「００１」がデータ３０４に格納される。

[0077] 鍵画像情報３１１は、データ３０４の内容が、シンクデバイスに表示する鍵画像であることを示す情報である。すなわち、情報要素識別子３０３に鍵画像情報３１１が格納されている場合には、データ３０４に鍵画像（鍵画像データ）が格納される。

[0078] 認証鍵情報３１２は、データ３０４の内容が、ソースデバイスからシンクデバイスに送信される鍵コード（シンクデバイスに表示された鍵画像がソースデバイス側で読み取られてソースデバイスから送信される鍵コード）であることを示す情報である。すなわち、情報要素識別子３０３に認証鍵情報３１２が格納されている場合には、データ３０４に鍵コード（例えば、猫の画像を特定するための鍵コード「００１」）が格納される。

[0079] ユーザ情報３１３は、データ３０４の内容が、認証後にソースデバイスからシンクデバイスに送信されるデータ（例えば、ユーザのコンテンツ（静止画コンテンツ、動画コンテンツ））であることを示す情報である。例えば、情報要素識別子３０３にユーザ情報３１３が格納されている場合には、ユーザのコンテンツ（静止画コンテンツ、動画コンテンツ）がデータ３０４に格納される。

[0080] ここで、鍵画像情報３１１およびユーザ情報３１３は、データ３０４の内

容が、画像情報であることを示す情報であるという点では同じである。ただし、ユーザ情報３１３は、認証が完了したソースデバイスおよびシンクデバイス間でのみ、やり取りされる情報である。これに対して、鍵画像情報３１１は、認証が完了する前のソースデバイスおよびシンクデバイス間でやり取りされる情報であるという点が異なる。すなわち、シンクデバイスは、認証前の状態であっても鍵画像情報３１１に対応する画像のみは表示部に表示する必要がある。

[0081] 接続開放要求３１４は、データ３０４の内容が、ソースデバイスおよびシンクデバイス間の接続状態を開放するための要求（接続開放要求）であることを示す情報である。すなわち、情報要素識別子３０３に接続開放要求３１４が格納されている場合には、データ３０４に接続開放要求に関する情報が格納される。

[0082] 鍵情報要求３１５は、データ３０４の内容が、ソースデバイスが鍵情報提供サーバに対して認証鍵情報の送信を要求する鍵情報送信要求であることを示す情報である。すなわち、情報要素識別子３０３に鍵情報要求３１５が格納されている場合には、データ３０４に鍵情報送信要求に関する情報が格納される。なお、鍵情報提供サーバについては、本技術の第４の実施の形態で示す。

[0083] 鍵一致確認結果３１６は、データ３０４の内容が、鍵の認証（鍵一致確認）の結果（鍵一致確認結果）であることを示す情報である。すなわち、情報要素識別子３０３に鍵一致確認結果３１６が格納されている場合には、データ３０４に鍵一致確認結果（一致または不一致）が格納される。

[0084] 認証鍵生成要求３１７は、データ３０４の内容が、認証鍵の生成をシンクデバイスに要求する認証鍵生成要求であることを示す情報である。すなわち、情報要素識別子３０３に認証鍵生成要求３１７が格納されている場合には、データ３０４に認証鍵生成要求に関する情報が格納される。

[0085] 鍵情報表示通知３１８は、データ３０４の内容が、シンクデバイスに認証鍵情報が表示された旨のソースデバイスへの通知（鍵情報表示通知）である

ことを示す情報である。すなわち、情報要素識別子３０３に鍵情報表示通知３１８が格納されている場合には、データ３０４に鍵情報表示通知に関する情報が格納される。

[0086] 拒否理由通知３１９は、データ３０４の内容が、ソースデバイスからの接続要求を拒否した場合におけるその理由（シンクデバイスからソースデバイスに送信される拒否理由通知）であることを示す情報である。すなわち、情報要素識別子３０３に拒否理由通知３１９が格納されている場合には、データ３０４に拒否理由通知に関する情報が格納される。なお、接続要求は、無線通信を利用してソースデバイスからシンクデバイスへのデータ送信を行うためのシンクデバイスへの無線接続の要求である。すなわち、接続要求は、その無線接続をソースデバイスに許可するための認証鍵情報をシンクデバイスから出力させるための要求として把握することができる。

[0087] データ３０４は、情報要素識別子３０３に格納されている情報に対応するデータである。

[0088] ［通信例］

図５は、本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図５では、図１に示す状態で、ユーザ１１が認証開始指示操作を行う場合における通信処理例を示す。また、図５では、シンクデバイス（情報処理装置２００）においてユーザ１１が認証開始指示操作を行い、シンクデバイス（情報処理装置２００）側で認証鍵を生成する場合における通信処理例を示す。

[0089] 最初に、ユーザ１１は、シンク側の情報処理装置２００の操作受付部２５２またはリモートコントローラ２６２を用いて認証開始指示操作を行う（４０１）。例えば、認証開始指示操作を行うための操作部材（例えば、設定ボタン）の押下を行う（４０１）。

[0090] このように、シンク側の情報処理装置２００において認証開始指示操作が行われた場合には（４０１）、シンク側の情報処理装置２００の制御部２２０は、その認証開始指示操作をトリガとして、認証処理を行う際に用いる認

証鍵を生成する（４０２）。例えば、図１に示す例では、鍵として「ネコ（猫）」が生成される。

[0091] 続いて、シンク側の情報処理装置２００の制御部２２０は、生成された認証鍵を画像情報に変換して鍵画像を生成する（４０３）。この鍵画像は、生成された認証鍵に対応する画像であり、生成された認証鍵をユーザに視認させるための画像である。例えば、図１に示す例では、鍵画像として、鍵「ネコ（猫）」に対応する猫の画像（猫画像１２）が生成される。

[0092] 続いて、シンク側の情報処理装置２００の制御部２２０は、生成された鍵画像を表示部２４２に表示させる（４０４）。例えば、図１に示す例では、鍵画像として猫画像１２が表示部２４２に表示される。このように、表示部２４２に鍵画像が表示されることにより、ユーザ１１は、その鍵画像を視認することができる（４０５）。例えば、図１に示すように、鍵画像として猫画像１２が表示部２４２に表示されている場合には、ユーザ１１は、鍵が「ネコ（猫）」であることを把握することができる。

[0093] このように、表示部２４２に表示されている鍵画像（例えば、ネコ（猫））を視認した後に（４０５）、ユーザ１１は、鍵画像に対応する認証鍵情報を、ソース側の情報処理装置１００の操作受付部１５２において入力する（４０６）。例えば、図１に示すように、鍵画像として猫画像１２が表示部２４２に表示されている場合には、ユーザ１１は、認証鍵情報として「ネコ」を入力する。ここで、入力方法が指定されている場合（例えば、カタカナ入力が指定されている場合）には、その指定に応じた文字（例えば、カタカナ）を入力する。

[0094] また、例えば、鍵画像に対応する認証鍵情報を、音声により入力するようにしてもよい。例えば、ソース側の情報処理装置１００の音声入力部１７２を用いて、認証鍵情報の音声「ネコ」を入力し、この音声に基づいて認証鍵情報「ネコ」を取得するようにしてもよい。

[0095] 続いて、ソース側の情報処理装置１００の制御部１２０は、無線通信を利用して、入力された認証鍵情報をシンク側の情報処理装置２００に送信する

（４０７、４０８）。この場合に送信対象となる情報に含まれるソースデバイスＩＤ３０１（図４に示す）には、情報処理装置１００の識別情報が格納され、シンクデバイスＩＤ３０２（図４に示す）には、情報処理装置２００の識別情報が格納される。また、情報要素識別子３０３（図４に示す）には認証鍵情報３１２が格納され、データ３０４（図４に示す）には、入力された認証鍵情報が格納される。なお、これ以降に示す各情報についても、ソースデバイスＩＤ３０１（図４に示す）には情報処理装置１００の識別情報が格納され、シンクデバイスＩＤ３０２（図４に示す）には情報処理装置２００の識別情報が格納されるものとする。

[0096] 認証鍵情報を受信すると（４０８）、シンク側の情報処理装置２００の制御部２２０は、生成された認証鍵情報と、受信した認証鍵情報（データ３０４（図４に示す）に格納されている認証鍵情報）とが一致するか否かを確認する（４０９）。すなわち、認証開始指示操作をトリガとして生成された認証鍵情報と、この認証鍵情報に対応する鍵画像が表示部２４２に表示された後に受信した認証鍵情報とが一致するか否かが確認される（４０９）。

[0097] 続いて、シンク側の情報処理装置２００の制御部２２０は、認証鍵情報の一致確認の結果（鍵一致確認結果）をソース側の情報処理装置１００に送信する（４１０、４１１）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には鍵一致確認結果３１６が格納され、データ３０４（図４に示す）には、鍵一致確認結果（一致または不一致）が格納される。

[0098] 例えば、表示部２４２に猫画像１２（鍵画像）が表示され（４０４）、認証鍵情報として「ネコ」が入力された場合には（４０６）、２つの認証鍵情報が一致すると判断される（４０９）。この場合には、鍵が一致した旨を示す鍵一致確認結果（一致）が、シンク側の情報処理装置２００からソース側の情報処理装置１００に送信される（４１０、４１１）。すなわち、認証に成功した旨を示す情報（鍵一致確認結果）が、シンク側の情報処理装置２００からソース側の情報処理装置１００に送信される（４１０、４１１）。

[0099] このように、認証に成功した場合には、ソース側の情報処理装置１００およびシンク側の情報処理装置２００間が接続状態となる。これにより、ソース側の情報処理装置１００からシンク側の情報処理装置２００に送信したコンテンツを、シンク側の情報処理装置２００から出力させることができる（４１２、４１３）。すなわち、認証に成功した旨の鍵一致確認結果がソース側の情報処理装置１００に送信された以降は、ソース側の情報処理装置１００が送信したコンテンツを、シンク側の情報処理装置２００から出力させることができる（４１２、４１３）。

[0100] 例えば、ソース側の情報処理装置１００のメモリ１３０に格納されているコンテンツを、無線通信を利用して、ソース側の情報処理装置１００からシンク側の情報処理装置２００に送信することができる（４１２、４１３）。そして、そのコンテンツ（静止画コンテンツや動画コンテンツ）を受信すると（４１３）、シンク側の情報処理装置２００は、受信したコンテンツを表示部２４２に表示させることができる（４１３）。

[0101] また、シンク側の情報処理装置２００から出力させるコンテンツの送信が終了した場合には、ソース側の情報処理装置１００の制御部１２０は、接続開放要求をシンク側の情報処理装置２００に送信する（４１４、４１５）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には接続開放要求３１４が格納され、データ３０４（図４に示す）には、接続開放要求に関する情報が格納される。

[0102] このように、接続開放要求を送信することにより、ソース側の情報処理装置１００およびシンク側の情報処理装置２００間の接続状態を終了させることができる。

[0103] また、例えば、表示部２４２に猫画像１２（鍵画像）が表示されている場合に（４０４）、認証鍵情報として「ネコ」以外の情報（文字、記号、数字等）が入力された場合には（４０６）、２つの認証鍵情報が一致しないと判断される（４０９）。例えば、認証鍵情報として「ペンギン」が入力された場合には（４０６）、２つの認証鍵情報が一致しないと判断される（４０９

）。この場合には、鍵が一致しない旨を示す鍵一致確認結果（不一致）が、ソース側の情報処理装置１００に送信される（４１０、４１１）。すなわち、認証に失敗した旨を示す情報（鍵一致確認結果）が、シンク側の情報処理装置２００からソース側の情報処理装置１００に送信される（４１０、４１１）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には鍵一致確認結果３１６が格納され、データ３０４（図４に示す）には、鍵一致確認結果（不一致）が格納される。

[0104] このように、認証に失敗した場合には、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのコンテンツの送信を行うことができない。このため、認証に失敗した場合には、その旨をユーザに通知するようにしてもよい。例えば、ソース側の情報処理装置１００およびシンク側の情報処理装置２００のうちの少なくとも一方から、認証に失敗した旨の通知情報を出力（画像表示、音声出力）することができる。

[0105] 図５では、ユーザ１１が、シンク側の情報処理装置２００の表示部２４２に表示されている鍵画像を視認し、その鍵画像に対応する認証鍵情報を入力する例を示した。ただし、認証鍵情報をソース側の情報処理装置１００に入力させるようにしてもよい。

[0106] 例えば、ソース側の情報処理装置１００の撮像部１６２が、シンク側の情報処理装置２００の表示部２４２に表示されている鍵画像を撮像してその鍵画像を取得する。そして、ソース側の情報処理装置１００の制御部１２０は、その取得された鍵画像に基づいて認証鍵情報を取得し、この取得された認証鍵情報をシンク側の情報処理装置２００に送信することができる。

[0107] 例えば、ソース側の情報処理装置１００の制御部１２０は、撮像部１６２により取得された鍵画像を認証鍵情報とし、この認証鍵情報をシンク側の情報処理装置２００に送信することができる。この場合には、シンク側の情報処理装置２００は、生成された鍵画像と、受信した鍵画像との一致を確認する。この場合には、例えば、画像同士のマッチング処理により一致を確認することができる。

[0108] また、図５では、イメージをユーザが把握することができる鍵画像（猫画像１２）を表示する例を示したが、イメージを把握することができない鍵画像を表示するようにしてもよい。この場合には、その鍵画像を利用してユーザが認証鍵情報を取得することができるようにする。

[0109] 例えば、文字、記号、数字等を表示して、これらを認識技術により認識して、この認識結果に基づいて認証鍵情報を取得するようにしてもよい。この表示例を図６のａに示す。

[0110] また、多次元コード（例えば、１次元コード、２次元コード、３次元コード）を表示して、これらを認識技術により認識して、この認識結果に基づいて認証鍵情報を取得するようにしてもよい。この表示例を図６のｂに示す。

[0111] また、ウォーターマーク（電子透かし）を表示して、このウォーターマークを利用して認証鍵情報を取得するようにしてもよい。この表示例を図６のｃに示す。

[0112] ［鍵画像の表示例］

図６は、本技術の第１の実施の形態における情報処理装置２００の表示部２４２に表示される鍵画像の表示例を示す図である。

[0113] 図６のａには、文字、記号、数字、シンボル（絵文字）等を鍵画像として表示する例を示す。この場合には、例えば、表示部２４２に表示されている鍵画像（１７ＫＭ８０９）をユーザが視認し、この鍵画像（１７ＫＭ８０９）を情報処理装置１００の操作受付部１５２に入力することにより、情報処理装置１００は認証鍵情報を取得することができる。また、上述したように、認識技術により認証鍵情報（１７ＫＭ８０９）を認識して、この認識結果に基づいて認証鍵情報を取得するようにしてもよい。

[0114] 図６のｂには、２次元コード（例えば、ＱＲコード（登録商標）（Quick Response code））を鍵画像として表示する例を示す。

[0115] ここで、ＱＲコードは、小さな矩形（３隅に配置される「回」の字型の矩形を含む）が所定の規則に従って縦横に配置されているマトリックス型２次元コードである。また、ＱＲコードを撮像して読み取ることにより、そのＱ

Ｒコードに配置されている各矩形に応じた各種情報（付随情報）を取得することができる。

[0116] この場合には、例えば、表示部２４２に表示されている鍵画像（ＱＲコード）を撮像部１６２が撮像し、制御部１２０が、その撮像により生成された鍵画像（ＱＲコード）を解析して有効な情報（認証鍵情報）を取得する。

[0117] また、ＱＲコードの代わりに、バーコードを表示して用いるようにしてもよい。また、他の多次元コードを表示して用いるようにしてもよい。

[0118] 図６のｃには、鍵画像としてのウォーターマーク（電子透かし）が埋め込まれている画像（日の出の富士山）の表示例を示す。

[0119] ウォーターマークは、表示対象となる画像に埋め込まれている電子透かしである。また、本技術の実施の形態では、表示対象となる画像に認証鍵情報を埋め込む例を示す。ここで、ウォーターマークは、主に、知覚可能型のウォーターマーク（可視的なウォーターマーク）および知覚困難型のウォーターマーク（不可視的なウォーターマーク）の２種類が存在する。

[0120] 知覚困難型のウォーターマークの場合には、シンク側の情報処理装置２００の表示部２４２に表示されている画像をユーザが見てもわからない。このため、ウォーターマークとともに、ウォーターマークを表示している旨をユーザに通知することが好ましい。例えば、ウォーターマークを表示している旨の画像表示や、その旨の音声出力を行うことができる。この通知例については、図１５に示す。

[0121] なお、知覚困難型のウォーターマークの場合は、このウォーターマークの画像生成時に相当の演算を行う必要がある。しかしながら、シンク側の情報処理装置２００の表示部２４２に表示されている画像をユーザが視聴している場合でも、その視聴を損なわずに、認証鍵情報を通知することができる。

[0122] また、例えば、ソース側の情報処理装置１００の姿勢（例えば、振動や傾き）を利用して認証鍵情報を入力するようにしてもよい。例えば、その姿勢を検出するセンサ（例えば、ジャイロセンサ、加速度センサ）をソース側の情報処理装置１００に設ける。そして、例えば、認証鍵情報として「情報処

理装置１００を３回振る」をシンク側の情報処理装置２００の表示部２４２に表示する。この場合に、例えば、ユーザ１１が情報処理装置１００を３回振ると、センサがその３回の振動を検出する。この検出結果に基づいて、ソース側の情報処理装置１００の制御部１２０は、認証鍵情報（３回の振動）を取得することができる。

[0123] なお、図６では、説明の容易のため、認証鍵情報を比較的大きく表示した例を示すが、認証鍵情報については、表示部２４２の表示画面における隅（例えば、左下、右下）に表示することが好ましい。

[0124] また、認証鍵情報は、表示される毎に毎回変更することが好ましい。例えば、図１に示す鍵画像（認証鍵情報がイメージ化された画像）、図６のａに示す文字、図６のｂに示すＱＲコード、図６のｃに示すウォーターマークを順番に表示することができる。また、同一種類の認証鍵情報の内容を順次変更して表示するようにしてもよい。例えば、認証鍵情報がイメージ化された鍵画像を表示する場合には、動物（例えば、猫、犬、馬、ウサギ）、乗り物（例えば、車、電車、バイク）等を順次変更して表示することができる。また、ユーザの好みに応じて、認証鍵情報を変更して表示するようにしてもよい。例えば、車好きのユーザには、各種の車を認証鍵情報として表示して、表示された車の車種名を認証鍵情報として入力させるようにしてもよい。なお、ユーザの好みは、例えば、ユーザが所有する情報処理装置にユーザの好みに関するユーザ情報を格納しておき、このユーザ情報に基づいて取得することができる。また、本技術の実施の形態では、認証開始指示操作が行われる毎に、認証鍵情報（または、鍵画像）を生成する例を示す。ただし、認証鍵情報（または、鍵画像）を装置内に予め記憶させておき、認証開始指示操作が行われる毎に、その記憶されている認証鍵情報（または、鍵画像）のうちから順次選択して用いるようにしてもよい。この場合には、その記憶されている認証鍵情報（または、鍵画像）のうちから所定の順序に従って選択するようにしてもよく、ランダムに選択するようにしてもよい。

[0125] なお、図１および図６に示す認証鍵情報は一例であり、これに限定される

わけではない。すなわち、図１および図６に示す認証鍵情報以外の認証鍵情報を表示して認証鍵情報として用いるようにしてもよい。

[0126] ［ソース側の情報処理装置が認証鍵を生成する例］

図５では、シンク側の情報処理装置２００において認証開始指示操作を行う例を示したが、ソース側の情報処理装置１００において認証開始指示操作を行うようにしてもよい。そこで、この通信例を図７、図８に示す。なお、図７では、ソース側の情報処理装置が認証鍵を生成する例を示す。また、図８では、ソース側の情報処理装置が鍵画像を生成する例を示す。

[0127] 図７は、本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図７に示す通信処理例は、図５に示す通信処理の一部を変形したものであるため、図５に示す通信処理と共通する部分には、同一の符号を付して、これらの説明の一部を省略する。

[0128] 最初に、ユーザ１１は、ソース側の情報処理装置１００の操作受付部１５２において、認証開始指示操作を行う（４２１）。例えば、ユーザ１１は、認証開始指示操作を行うための操作部材（例えば、タッチパネル、キーボード）の押下操作を行う（４２１）。

[0129] このように、ソース側の情報処理装置１００において認証開始指示操作が行われた場合には（４２１）、ソース側の情報処理装置１００の制御部１２０は、その認証開始指示操作をトリガとして、認証処理を行う際に用いる認証鍵を生成する（４２２）。例えば、図１に示す例では、認証鍵として「ネコ（猫）」が生成される。

[0130] 続いて、ソース側の情報処理装置１００の制御部１２０は、生成された認証鍵を画像情報に変換するための表示鍵情報をシンク側の情報処理装置２００に送信する（４２３、４２４）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には、表示鍵情報３１０が格納され、データ３０４（図４に示す）には、生成された認証鍵に対応する表示鍵情報（鍵コード）が格納される。

[0131] 表示鍵情報を受信すると（４２４）、シンク側の情報処理装置２００の制御部２２０は、受信した表示鍵情報を画像情報に変換して鍵画像を生成する（４２５）。例えば、図１に示す例では、鍵「ネコ（猫）」に対応する猫画像１２が生成される。

[0132] 続いて、シンク側の情報処理装置２００の制御部２２０は、生成された鍵画像を表示部２４２に表示させる（４２６）。例えば、図１に示す例では、鍵画像として猫画像１２が表示部２４２に表示される。

[0133] なお、これ以降の各処理については、図５に示す通信処理と同一であるため、ここでの説明を省略する。

[0134] このように、ソースデバイス側で認証鍵を生成することにより、シンクデバイス側の処理を単純化することができ、シンクデバイス側の処理を軽減させることができる。

[0135] ［ソース側の情報処理装置が鍵画像を生成する例］

図８は、本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図８に示す通信処理例は、図５に示す通信処理の一部を変形したものであるため、図５に示す通信処理と共通する部分には、同一の符号を付して、これらの説明の一部を省略する。

[0136] 最初に、ユーザ１１は、ソース側の情報処理装置１００の操作受付部１５２において、認証開始指示操作を行う（４３１）。このように、ソース側の情報処理装置１００において認証開始指示操作が行われた場合には（４３１）、ソース側の情報処理装置１００の制御部１２０は、その認証開始指示操作をトリガとして、認証処理を行う際に用いる認証鍵を生成する（４３２）。

[0137] 続いて、ソース側の情報処理装置１００の制御部１２０は、生成された認証鍵を画像情報に変換して鍵画像を生成する（４３３）。例えば、図１に示す例では、鍵画像として、鍵「ネコ（猫）」に対応する猫画像１２が生成される。

[0138] 続いて、ソース側の情報処理装置１００の制御部１２０は、生成された鍵画像をシンク側の情報処理装置２００に送信する（４３４、４３５）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には、鍵画像情報３１１が格納され、データ３０４（図４に示す）には、生成された鍵画像（鍵画像の画像データ）が格納される。

[0139] 鍵画像を受信すると（４３５）、シンク側の情報処理装置２００の制御部２２０は、受信した鍵画像を表示部２４２に表示させる（４３６）。例えば、図１に示す例では、猫画像１２が表示部２４２に表示される。

[0140] なお、これ以降の各処理については、図５に示す通信処理と同一であるため、ここでの説明を省略する。

[0141] このように、ソースデバイス側で鍵画像まで生成することにより、シンクデバイス側の処理をさらに単純化することができ、シンクデバイス側の処理をさらに軽減させることができる。

[0142] なお、図７および図８に示す例では、ソース側の情報処理装置１００が認証鍵を生成するため、シンク側の情報処理装置２００に表示される認証鍵をソース側の情報処理装置１００が把握していることになる。そこで、このような場合には、認証鍵情報を入力する際に、例えば、ソース側の情報処理装置１００の表示部１４２に、複数の鍵画像（例えば、犬の画像、牛の画像、豚の画像）を表示させることができる。そして、表示部１４２に表示されている複数の鍵画像から、シンク側の情報処理装置２００の表示部２４２に表示されている鍵画像（例えば、猫画像１２）をユーザ操作により選択するようにする。これにより、ユーザによる選択操作のみにより、認証鍵情報の入力操作を行うことができる。

[0143] ［複数のシンクデバイスの選択例］

図９は、本技術の第１の実施の形態における通信システム２０の構成例を示す図である。

[0144] 図９では、各部屋（２１０号室乃至２１２号室）に情報処理装置２００乃至２０２（図１に示すシンク側の情報処理装置２００に相当）が設置されて

いるホテルを例にして説明する。また、図９では、このホテルの２１１号室に、情報処理装置１００を所持するユーザが宿泊する場合を例にして説明する。

[0145] 図１、図５、図７、図８等では、１つのソースデバイスおよび１つのシンクデバイス間において情報のやり取りを行う例を示した。ここで、例えば、図９に示すように、各部屋（２１０号室乃至２１２号室）に情報処理装置２００乃至２０２が設置されているホテルに、情報処理装置１００を所持するユーザが宿泊する場合を想定する。この場合に、ユーザが所持している情報処理装置１００と、このユーザが宿泊している２１１号室に設置されている情報処理装置２０１とを無線接続し、情報処理装置１００に記憶されているコンテンツを情報処理装置２０１に表示させることが可能である。

[0146] しかしながら、情報処理装置１００と、ユーザが宿泊している２１１号室以外の部屋（２１０号室、２１２号室）に設置されている情報処理装置２００、２０２との間でも無線接続が可能であることも想定される。例えば、図７、図８に示すように、ソース側の情報処理装置１００により生成された情報（表示鍵情報、鍵画像）を送信すると、情報処理装置２０１以外の情報処理装置２０１、２０２に送信されることも想定される。この場合には、情報処理装置１００に記憶されているコンテンツを情報処理装置２０１に適切に表示させることができないおそれがある。

[0147] そこで、図９では、ユーザによる選択操作により無線接続の対象となる情報処理装置を選択する例を示す。

[0148] 例えば、図９に示す例では、複数のシンクデバイスの中からどのシンクデバイスに、最初の表示鍵情報（または、鍵画像情報）を送信するかを決定する。例えば、ソース側の情報処理装置１００において検出された複数のシンクデバイス（シンク側の情報処理装置２００乃至２０２）を、ソース側の情報処理装置１００の表示部１４２に表示する。例えば、図９に示すように、各部屋（２１０号室乃至２１２号室）に設置されている情報処理装置２００乃至２０２に対応する選択ボタン３２１乃至３２３が表示される。そして、

ユーザは、選択ボタン３２１乃至３２３のうちから所望の情報処理装置２０１に対応する選択ボタン３２２の押下操作を行うことにより、認証開始指示操作（図７に示す４２１、図８に示す４３１）を行うことができる。この認証開始指示操作により認証鍵が生成され、選択された選択ボタンに対応する情報処理装置２０１に表示鍵情報（または、鍵画像情報）が送信される（図７に示す４２３（または、図８に示す４３４））。

[0149] なお、図５に示す例（シンクデバイス側で認証鍵を生成する例）では、シンクデバイスにおける認証開始指示操作により認証処理が開始される。このため、表示したいシンクデバイスにおいて認証開始指示操作を行うことにより、そのシンクデバイスに鍵画像を適切に表示させることができる。例えば、図９に示す例において、シンクデバイス側で認証鍵を生成する場合には、表示したい情報処理装置２０１において認証開始指示操作を行うことにより、情報処理装置２０１に鍵画像を適切に表示させることができる。

[0150] このように、ソース側の情報処理装置１００の制御部１２０は、複数のシンクデバイスに関する情報を表示部１４２に表示させる。そして、制御部１２０は、その表示されている複数のシンクデバイスのうちからユーザ操作により選択されたシンクデバイスに関する情報を、選択されたシンクデバイスに送信する。

[0151] また、シンク側の情報処理装置２００の制御部２２０は、選択されたシンクデバイス（シンク側の情報処理装置２０１）に関する情報に基づいて、無線接続をソース側の情報処理装置１００に許可するための認証鍵情報を表示部２４２に表示させる。すなわち、制御部２２０は、複数のシンクデバイスのうちからユーザ操作により選択されたシンクデバイス（シンク側の情報処理装置２０１）への無線接続をソース側の情報処理装置１００に許可するための認証鍵情報をシンク側の情報処理装置２０１に表示させる。

[0152] ［ソース側の情報処理装置が認証（鍵一致確認）を行う例］

図５、図７、図８では、シンク側の情報処理装置２００において認証（鍵一致確認）を行う例を示したが、ソース側の情報処理装置１００において認

証（鍵一致確認）を行うようにしてもよい。そこで、この通信例を図１０に示す。

[0153] 図１０は、本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図１０に示す通信処理例は、図８に示す通信処理の一部を変形したものであるため、図８に示す通信処理と共通する部分には、同一の符号を付して、これらの説明の一部を省略する。

[0154] シンク側の情報処理装置２００の表示部２４２に表示されている鍵画像（例えば、猫画像１２）を視認した後に（４０５）、ユーザ１１は、鍵画像に対応する認証鍵情報を、ソース側の情報処理装置１００の操作受付部１５２において入力する（４０６）。

[0155] 続いて、ソース側の情報処理装置１００の制御部１２０は、生成された認証鍵情報と、入力された認証鍵情報とが一致するか否かを確認する（４４１）。すなわち、認証開始指示操作をトリガとして生成された認証鍵情報と、この認証鍵情報に対応する鍵画像をシンク側の情報処理装置２００に送信した後に入力された認証鍵情報とが一致するか否かが確認される（４４１）。

[0156] 続いて、ソース側の情報処理装置１００の制御部１２０は、認証鍵情報の一致確認の結果（鍵一致確認結果）をシンク側の情報処理装置２００に送信する（４４２、４４３）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には鍵一致確認結果３１６が格納され、データ３０４（図４に示す）には、鍵一致確認結果（一致または不一致）が格納される。

[0157] このように、認証に成功した場合には、シンク側の情報処理装置２００は、鍵一致確認結果の受信後に送信されるコンテンツを受信して出力させる（４４４、４４５）。すなわち、ソース側の情報処理装置１００からシンク側の情報処理装置２００に送信したコンテンツを、シンク側の情報処理装置２００から出力させることができる（４４４、４４５）。

[0158] また、シンク側の情報処理装置２００から出力させるコンテンツの送信が

終了した場合には、ソース側の情報処理装置１００の制御部１２０は、接続開放要求をシンク側の情報処理装置２００に送信する（４４６、４４７）。

[0159] なお、認証に失敗した場合には、シンク側の情報処理装置２００は認証前の状態に戻る。

[0160] このように、ソース側の情報処理装置１００の制御部１２０は、シンク側の情報処理装置２００への無線接続をソース側の情報処理装置１００に許可するための認証鍵情報をシンク側の情報処理装置２００の表示部２４２から出力させるための制御を行う。また、例えば、制御部１２０は、ソース側の情報処理装置１００に入力された認証鍵情報と、シンク側の情報処理装置２００から出力された認証鍵情報とに基づいて、その無線接続をソース側の情報処理装置１００に許可するかを決定する。そして、制御部１２０は、無線通信を利用してその決定の結果（鍵一致確認結果）をシンク側の情報処理装置２００に送信する。

[0161] このように、ソースデバイス側で認証鍵の生成、認証（鍵一致確認）を行うことにより、シンクデバイス側の処理をさらに単純化することができ、シンクデバイス側の処理をさらに軽減させることができる。

[0162] ［ソース側で認証開始指示操作を行いシンク側で認証鍵を生成する例］

以上では、認証開始指示操作が行われた情報処理装置が認証鍵を生成する例を示したが、認証開始指示操作が行われた情報処理装置以外の情報処理装置に認証鍵を生成させるようにしてもよい。そこで、この通信例を図１１に示す。

[0163] 図１１は、本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図１１に示す通信処理例は、図５に示す通信処理の一部を変形したものであるため、図５に示す通信処理と共通する部分には、同一の符号を付して、これらの説明の一部を省略する。

[0164] 最初に、ユーザ１１は、ソース側の情報処理装置１００の操作受付部１５２において、認証開始指示操作を行う（４５１）。このように、認証開始指

示操作が行われた場合には（４５１）、ソース側の情報処理装置１００の制御部１２０は、その認証開始指示操作をトリガとして、認証鍵生成要求をシンク側の情報処理装置２００に送信する（４５２、４５３）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には、認証鍵生成要求３１７が格納され、データ３０４（図４に示す）には、認証鍵生成要求に関する情報が格納される。

[0165] 認証鍵生成要求を受信すると（４５３）、シンク側の情報処理装置２００の制御部２２０は、その認証鍵生成要求の受信をトリガとして、認証処理を行う際に用いる認証鍵を生成する（４０２）。

[0166] ［認証鍵情報が表示されている旨を通知する例］

ここで、シンクデバイスに認証鍵情報が表示されている状態でも、その認証鍵情報の表示をユーザが把握することができないことも想定される。例えば、鍵画像として知覚困難型のウォーターマークを利用する場合には、鍵画像が表示されている状態となっているのか、または、そのような状態になっていないのかをユーザが判断することが困難であることが想定される。そこで、ここでは、認証鍵情報が表示されている旨をユーザに通知する例を示す。

[0167] 図１２は、本技術の第１の実施の形態における通信システム１０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図１２に示す通信処理例は、図５、図７、図８、図１０、図１１に示す通信処理の一部を変形したものであるため、これらの通信処理と共通する部分については、図示およびその説明を省略する。

[0168] シンク側の情報処理装置２００の表示部２４２に鍵画像が表示された後に（４６１）、シンク側の情報処理装置２００の制御部２２０は、鍵情報表示通知をソース側の情報処理装置１００に送信する（４６２、４６３）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には、鍵情報表示通知３１８が格納され、データ３０４（図４に示す）には、鍵情報表示通知に関する情報が格納される。

[0169] 鍵情報表示通知を受信すると（４６３）、ソース側の情報処理装置１００の制御部１２０は、ユーザに対して視認開始を促すため、鍵情報表示通知を出力する（４６４）。例えば、表示部１４２への表示や、音声出力部１７３からの音声出力により、鍵情報表示通知が出力される（４６４）。例えば、認証鍵情報として数値を用いる場合には、「ＴＶに表示されている数値を入力して下さい」のメッセージを表示部１４２に表示させることができる。または、「ＴＶに表示されている数値を入力して下さい」のメッセージを音声出力部１７３から音声出力させることができる。また、例えば、撮像部１６２を用いて認証鍵情報（例えば、知覚困難型ウォーターマーク）を取得する場合には、「ＴＶにカメラを向けて下さい」のメッセージを表示部１４２に表示させる。

[0170] このように、鍵情報表示通知を出力することにより（４６４）、ユーザは、認証鍵情報を視認し（４６５）、認証鍵情報の入力を行うことができる（４６６）。なお、認証鍵情報が知覚困難型のウォーターマークである場合には、ソース側の情報処理装置１００の撮像部１６２により認証鍵情報が視認される（４６５）。

[0171] このように、鍵情報表示通知が出力されることにより、シンク側の情報処理装置２００に鍵画像が表示されている旨をユーザに通知することができる。これにより、ユーザが鍵画像を視認（または、ソース側の情報処理装置１００の撮像部１６２により撮像）することを促すことができる。

[0172] ここで、例えば、無線通信を利用してソースデバイスに保持されているコンテンツをシンクデバイスに送信して表示させる場合に、そのように表示してもよいか否かの認証が必要となる。そこで、本技術の第１の実施の形態では、その認証のための認証鍵情報をシンクデバイスから出力（例えば、表示、音声出力）させる。そして、その認証鍵情報をソースデバイスのユーザまたはソースデバイス自身が認識してソースデバイスからシンクデバイスに無線通信を利用して送信する。また、シンクデバイスは、その認証鍵情報を照合することにより、ソースデバイスおよびシンクデバイスを接続してもよい

か否かを適切に判断することができる。これにより、ユーザが意図する通りのペアリングおよび認証を容易に行うことができる。すなわち、ソースデバイスおよびシンクデバイス間で無線通信を行う場合に接続処理を適切に行うことができる。

[0173] また、本技術の第１の実施の形態によれば、無線通信を利用してユーザ情報（コンテンツ）をシンクデバイスから出力させる場合に、認証鍵情報が出力（表示、音声出力）されたシンクデバイスからの出力に限定することができる。これにより、ユーザが保持しているソースデバイス（手元の端末）のユーザ情報（コンテンツ）を、ユーザが意図した適切なシンクデバイスから出力させることができる。

[0174] また、ユーザが意図しないシンクデバイス（すなわち、ユーザから見える範囲内に存在しないシンクデバイス）から、ユーザが保持しているソースデバイス（手元の端末）のユーザ情報（コンテンツ）が間違って出力されることを防止することができる。

[0175] ＜２．第２の実施の形態＞

本技術の第１の実施の形態では、認証開始指示操作が行われてから接続開放要求があるまでの間、ソースデバイスおよびシンクデバイス間において無線通信を行う例を示した。ここで、認証開始指示操作が行われてから接続開放要求があるまでの間、他のソースデバイスにより認証開始指示操作が行われ、他のソースデバイスからシンクデバイスに接続要求がされることも想定される。

[0176] そこで、本技術の第２の実施の形態では、ソースデバイスおよびシンクデバイス間において無線通信が行われている状態で、他のソースデバイスからシンクデバイスに接続要求がされた場合の例を示す。なお、本技術の第２の実施の形態における通信システムは、図１に示す通信システム１０と略同様である。このため、通信システム１０と共通する部分については、同一の符号を付して、これらの説明の一部を省略する。

[0177] ［通信システムの構成例］

図１３は、本技術の第２の実施の形態における通信システム３０の構成例を示す図である。

[0178] 通信システム３０は、情報処理装置１００、１０１、２００を備える。なお、通信システム３０は、図１に示す通信システム１０において、ソース側の情報処理装置１０１を追加したものである。また、情報処理装置１０１の内部構成については、図１に示す情報処理装置１００と同様である。すなわち、図１３では、２つのソースデバイスおよび１つのシンクデバイスを備える通信システムの例を示す。

[0179] ［他のソースデバイスからの接続要求を拒否する例］

図１４は、本技術の第２の実施の形態における通信システム３０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図１４では、図１３に示す状態で、ユーザが認証開始指示操作を行う場合における通信処理例を示す。また、図１４では、ソースデバイス（情報処理装置１００、１０１）においてユーザが認証開始指示操作を行い、ソースデバイス（情報処理装置２００）側で認証鍵を生成する場合における通信処理例を示す。

[0180] また、図１４では、ソース側の情報処理装置１００およびシンク側の情報処理装置２００間の認証が成功した後に、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのコンテンツ送信が行われている場合を想定する。なお、処理（４１０乃至４１３）は、図７に示す処理と同一であるため、同一の符号を付してここでの説明を省略する。また、処理（４１０乃至４１３）よりも前の各処理については、図示を省略する。

[0181] このように、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのコンテンツ送信が行われている状態で（４１２、４１３）、ソース側の情報処理装置１０１の操作受付部において認証開始指示操作が行われた場合を想定する（４７１）。この場合には、図７に示す各処理（４２１乃至４２４）と同様に、ソース側の情報処理装置１０１により認証鍵が生成され（４７２）、ソース側の情報処理装置１０１からシンク側の情報処理装置

２００に表示鍵情報が送信される（４７３、４７４）。

[0182] しかしながら、シンク側の情報処理装置２００が、ソース側の情報処理装置１０１のユーザ３２が意図するシンクデバイスでないことも想定される。すなわち、ソース側の情報処理装置１０１のユーザ３２が、シンク側の情報処理装置２００以外のシンクデバイスにコンテンツを表示させるため、認証開始指示操作を行っていることも想定される。

[0183] また、シンク側の情報処理装置２００にコンテンツが表示されている場合に（４１３）、ソース側の情報処理装置１０１からの指示に基づく鍵画像をシンク側の情報処理装置２００に表示すると、表示されているコンテンツの視聴を邪魔することになる。すなわち、他のユーザ３１の視聴を毀損するような攻撃をし得るおそれがある。

[0184] そこで、本技術の第２の実施の形態では、このような攻撃を回避するため、コンテンツの無線通信が行われている状態で、他のソースデバイスから接続要求がされた場合には、その接続要求を拒否する例を示す。

[0185] 例えば、表示鍵を受信した場合には（４７４）、シンク側の情報処理装置２００は、拒否理由通知をソース側の情報処理装置１０１に送信する（４７５、４７６）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には、拒否理由通知３１９が格納され、データ３０４（図４に示す）には、拒否理由に関する情報（例えば、メッセージ、接続可能時刻）が格納される。

[0186] 拒否理由通知を受信すると（４７６）、ソース側の情報処理装置１０１は、拒否理由通知を表示する（４７７）。例えば、図１３に示すように、ソース側の情報処理装置１０１の表示部１０２に拒否理由通知（利用者に状況を知らせるための通知）が表示される。

[0187] なお、ソース側の情報処理装置１００からシンク側の情報処理装置２００に接続開放要求が送信され、これらの装置間の接続状態が解除された場合には、シンク側の情報処理装置２００は、何れのソースデバイスからも接続要求を受け付けるようにする。ここで、シンク側の情報処理装置２００がホテ

ルに設置されている場合を想定する。この場合には、例えば、シンク側の情報処理装置２００が設置されている部屋に宿泊しているユーザが、チェックアウトしたタイミングで、ソース側の情報処理装置１００およびシンク側の情報処理装置２００の接続状態を解除するようにしてもよい。

[0188] このように、シンク側の情報処理装置２００の制御部２２０は、ソース側の情報処理装置１００から送信されたデータが表示部２４２に表示されている状態で、接続要求を他のソースデバイスから受信した場合には、その接続要求を拒否する。なお、制御部２２０は、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのデータ送信が終了した後に、接続要求を他のソースデバイスから受信した場合には、その接続要求に応じて認証鍵情報を表示部２４２に出力させる。

[0189] なお、接続状態に入る前でも接続要求を拒否するようにしてもよい。この拒否例を図１５に示す。

[0190] ［他のソースデバイスからの接続要求を拒否する例］

図１５は、本技術の第２の実施の形態における通信システム３０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図１５では、シンク側の情報処理装置２００が接続状態に入る前に、ユーザによる手動操作により接続要求を拒否する通信処理例を示す。また、図１５では、ソースデバイス（情報処理装置１００、１０１）においてユーザが認証開始指示操作を行い、ソースデバイス（情報処理装置１００、１０１）側で認証鍵を生成する場合における通信処理例を示す。

[0191] ここで、シンク側の情報処理装置２００は、接続状態に入る前の状態（すなわち、接続状態に入る直前の状態も含む）であるものとする。

[0192] この状態で、ソース側の情報処理装置１０１の操作受付部において認証開始指示操作が行われた場合を想定する（４８１）。この場合には、図１４に示す各処理（４７１乃至４７４）と同様に、ソース側の情報処理装置１０１により認証鍵が生成され（４８２）、ソース側の情報処理装置１０１からシンク側の情報処理装置２００に表示鍵情報が送信される（４８３、４８４）

。そして、シンク側の情報処理装置２００は、鍵画像を生成し（４８５）、鍵画像を表示する（４８６）。例えば、図１に示すように、鍵画像が表示される。

[0193] このように、シンク側の情報処理装置２００の表示部２４２に鍵画像が表示された場合に（４８６）、この鍵画像を見たユーザ３１が、ソース側の情報処理装置１０１からの接続要求を拒否する場合を想定する。この場合には、ユーザ３１は、シンク側の情報処理装置２００の操作受付部２５２またはリモートコントローラ２６２を用いて拒否指示操作を行う（４８７）。例えば、拒否指示操作を行うための操作部材（例えば、設定ボタン）の押下を行う（４８７）。

[0194] このように、シンク側の情報処理装置２００において拒否指示操作が行われた場合には（４８７）、シンク側の情報処理装置２００は、拒否理由通知をソース側の情報処理装置１０１に送信する（４８８、４８９）。

[0195] 拒否理由通知を受信すると（４８９）、ソース側の情報処理装置１０１は、拒否理由通知を表示する（４９０）。例えば、図１３に示すように、ソース側の情報処理装置１０１の表示部１０２に拒否理由通知（利用者に状況を知らせるための通知）が表示される。この拒否理由として、図１３に示す他のユーザが利用中である旨以外に、例えば、当該端末の利用が不可（例えば、サービス停止中）である旨、その他の利用不可（例えば、通信機能が故障中）を通知することができる。なお、他のユーザが利用中である旨を通知する場合には、利用することができるようになるまでの時間を通知することが好ましい。例えば、「あと、〇分後に使用可能」を表示することができる。

[0196] また、これ以降に接続要求が送信された場合でも（４９１乃至４９４）、シンク側の情報処理装置２００は認証鍵情報を表示せずに拒否する（４９５乃至４９７）。これにより、シンク側の情報処理装置２００に、認証鍵情報が一度は表示されてしまうが、それ以降の不必要な認証鍵情報の表示を防止することができる。また、ユーザの視聴体験の毀損を最小限に抑えることができる。なお、この拒否状態は、所定条件を満たすタイミング（例えば、一

定時間のタイマのカウント）で解除することが好ましい。

[0197] なお、この例では、拒否通知をソースデバイスから出力してユーザに通知する例を示したが、拒否通知をシンクデバイスから出力してユーザに通知するようにしてもよい。また、ソースデバイスおよびシンクデバイスの双方で通知するようにしてもよい。

[0198] このように、シンク側の情報処理装置２００の制御部２２０は、無線接続を拒否するためのユーザ操作（拒否指示操作）が受け付けられた場合には、その無線接続をソース側の情報処理装置１００に許可しないと決定する。

[0199] このように、本技術の第２の実施の形態では、ユーザが保持しているソースデバイス（手元の端末）とシンクデバイスとが接続状態となった後には、他のソースデバイスからの接続要求（認証要求）を拒否する。これにより、意図しない他のソースデバイスからの接続要求を抑制することができる。すなわち、ユーザがコンテンツを視聴している状態の時に、ユーザ体験を毀損するような認証鍵情報の表示を防止することができる。

[0200] また、シンクデバイス側で接続要求（認証要求）を拒否することができるため、視聴体験を毀損するような意図しないユーザからの認証鍵情報の表示を抑制することができる。

[0201] 以上では、他のソースデバイスからの接続要求を拒否する例を示した。しかしながら、先に接続されているソースデバイスよりも、後から接続要求を送信したソースデバイスの方を優先して接続する方が好ましいことも想定される。そこで、以下では、各ソースデバイスに優先度を付して、この優先度に基づいて切り替えの要否を判断する例を示す。

[0202] ［シンクデバイスへの接続権を切り替える例］

図１６は、本技術の第２の実施の形態における通信システム３０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図１６では、ソース側の情報処理装置１０１の優先度が、ソース側の情報処理装置１００の優先度よりも高い場合における通信処理例を示す。また、図１６では、ソースデバイス（情報処理装置１００、１０１）側で認証鍵を生成

する場合における通信処理例を示す。

[0203] また、接続対象となるソースデバイス（情報処理装置１００、１０１）については、シンク側の情報処理装置２００が管理しているものとする。例えば、シンク側の情報処理装置２００におけるユーザ操作により、接続対象となるソースデバイスに関する情報を入力して管理情報として登録するようにしてもよく、接続要求を送信したソースデバイスを順次登録するようにしてもよい。

[0204] ここで、優先順位の決定方法について説明する。例えば、ソースデバイスが要求する認証の種類に応じて、ソースデバイスの優先度を決定することができる。すなわち、認証レベルを可変とすることができる。

[0205] 例えば、ユーザ操作により入力された認証鍵情報を用いる認証を要求するソースデバイスの優先度よりも、撮像部により生成された鍵画像に基づく認証鍵情報を用いる認証を要求するソースデバイスの優先度を高くすることができる。また、例えば、ウォーターマークを用いる認証の場合には、知覚困難型のウォーターマークを用いる認証を要求するソースデバイスの優先度を、知覚可能型のウォーターマークを用いる認証を要求するソースデバイスの優先度を高くすることができる。

[0206] また、例えば、ソースデバイスの機種に応じて、ソースデバイスの優先度を決定することができる。例えば、高価（高機能）なソースデバイスの優先度を、安価（単機能）なソースデバイスの優先度よりも高くすることができる。

[0207] また、例えば、コンテンツの種別に応じて、ソースデバイスの優先度を決定することができる。例えば、高品位のコンテンツを送信するソースデバイスの優先度を、低品位のコンテンツを送信するソースデバイスの優先度よりも高くすることができる。

[0208] また、例えば、シンクデバイスとの通信履歴や、シンクデバイスを管理する管理者による手動操作により、優先度をソースデバイスに予め付与しておくようにしてもよい。

[0209] また、ソースデバイスを使用するユーザに応じて優先度を付与するようにしてもよい。例えば、シンクデバイスを管理するユーザの親しい友達のソースデバイスには優先度を高く設定し、そうでもない友達のソースデバイスには優先度を低く設定する。

[0210] また、シンクデバイスがホテルに設置されている場合には、ＶＩＰのお客と一般客とを分けてサービスを提供するようにしてもよい。例えば、ＶＩＰのお客がチェックインする際に、そのお客のソースデバイス（例えば、スマートフォン）に優先度を高くするための情報を入力し、そのお客がチェックアウトする際に、そのお客のソースデバイスから、優先度に関する情報を消去するようにする。

[0211] なお、これらの優先度の決定方法は一例であり、他の決定方法を用いるようにしてもよい。

[0212] ここで、図１３に示すように、ソース側の情報処理装置１００およびシンク側の情報処理装置２００間の認証が成功した後に、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのコンテンツ送信が行われている場合を想定する。なお、処理（５０１乃至５０４）は、図５に示す処理（４１０乃至４１３）と同一であるため、ここでの説明を省略する。また、処理（５０１乃至５０４）よりも前の各処理については、図示を省略する。

[0213] このように、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのコンテンツ送信が行われている場合に（５０３、５０４）、他のソースデバイス（情報処理装置１０１）において認証開始指示操作が行われた場合を想定する（５０５）。この場合には、図１４に示す各処理（４７１乃至４７４）と同様に、ソース側の情報処理装置１０１により認証鍵が生成され（５０６）、ソース側の情報処理装置１０１からシンク側の情報処理装置２００に表示鍵情報が送信される（５０７、５０８）。

[0214] 表示鍵情報を受信すると（５０８）、シンク側の情報処理装置２００の制御部２２０は、その表示鍵情報を送信したソースデバイス（情報処理装置１０１）と、現在の接続先（情報処理装置１００）との優先度を確認する（５

０９）。上述したように、図１６では、ソース側の情報処理装置１０１の優先度が、ソース側の情報処理装置１００の優先度よりも高いものとする。このように、現在接続中のソースデバイスよりも優先度が高いソースデバイスから接続要求が送信された場合には、シンク側の情報処理装置２００の制御部２２０は、現在の接続を開放して優先度が高いソースデバイスへの接続に切り替える。

[0215] 具体的には、シンク側の情報処理装置２００の制御部２２０は、現在の接続先であるソース側の情報処理装置１００に接続開放要求を送信する（５１０、５１１）。これにより、シンク側の情報処理装置２００およびソース側の情報処理装置１００の接続が開放される。

[0216] 続いて、シンク側の情報処理装置２００の制御部２２０は、受信した表示鍵情報を画像情報に変換して鍵画像を生成する（５１２）。なお、これ以降の各処理（５１３乃至５１７）は、図７に示す処理（４２６、４０５乃至４０８）と同一であるため、ここでの説明を省略する。また、処理（４０８）以降の各処理については、図示を省略する。

[0217] なお、表示鍵情報を送信したソースデバイスと、現在の接続先のソースデバイスとの優先度を確認した結果（５０９）、表示鍵情報を送信したソースデバイスの優先度と、現在の接続先のソースデバイスとの優先度とが同位であることも想定される。また、表示鍵情報を送信したソースデバイスの優先度が、現在の接続先のソースデバイスとの優先度よりも低いことも想定される。この場合には、図１４、図１５に示す例と同様に、表示鍵情報を送信したソースデバイスに拒否理由通知を送信するようにする。

[0218] このように、ソースデバイスおよびシンクデバイスの接続状態では、原則として、他のソースデバイスからの接続要求を拒否するが、所定条件を満たすソースデバイスについてのみは、その接続要求に応じることができる。すなわち、現在の接続先のソースデバイスの優先度よりも、他のソースデバイスの優先度が高い場合には、その接続要求に応じることができる。

[0219] ＜３．第３の実施の形態＞

本技術の第２の実施の形態では、ソースデバイスおよびシンクデバイス間で無線通信が行われている状態で、他のソースデバイスからの接続要求があった場合には、拒否理由を通知して拒否する例を示した。ここで、例えば、１つのシンクデバイスに対してソースデバイスの数が多い場合を想定する。このような場合には、１つのソースデバイスが、シンクデバイスからのコンテンツの出力を継続して長時間行うことも想定される。このように、１つのソースデバイスに長時間のコンテンツの出力を許可すると、他のユーザが使用することができなくなる。このため、各ユーザがシンクデバイスからのコンテンツの出力を適切に行えるようにすることが重要である。

[0220] そこで、本技術の第３の実施の形態では、ソースデバイスの接続状態を適切なタイミングで切り替える（開放する）例を示す。なお、本技術の第３の実施の形態における通信システムは、図１に示す通信システム１０と略同様である。このため、通信システム１０と共通する部分については、同一の符号を付して、これらの説明の一部を省略する。

[0221] ［通信システムの構成例］

図１７は、本技術の第３の実施の形態における通信システム４０の構成例を示す図である。

[0222] 通信システム４０は、情報処理装置１００、１０１、１０３、２００を備える。なお、通信システム４０は、図１３に示す通信システム３０において、ソース側の情報処理装置１０３を追加したものである。また、情報処理装置１０３の内部構成については、図１に示す情報処理装置１００と同様である。すなわち、図１７では、３つのソースデバイスおよび１つのシンクデバイスを備える通信システムの例を示す。

[0223] ここで、図１７に示すように、複数のソースデバイスと、１つのシンクデバイスが存在する場合に、複数のソースデバイスのそれぞれにシンクデバイスへの接続権を順次与えることを所望することも想定される。ここで、接続権は、ソースデバイスがシンクデバイスに接続することができる権利を意味する。

[0224] 例えば、仲間内で各自の持っているスマートフォン（または、タブレット端末）の画像を大画面のディスプレイに表示して楽しみたいと所望することが想定される。この場合、各スマートフォンに所定時間だけ接続権を与え、各スマートフォンの画像を大画面のディスプレイに順次表示することが考えられる。例えば、ソースデバイスとシンクデバイスの接続状態を一定時間のタイマのカウントで解除するようにすることにより、各スマートフォンに所定時間だけ接続権を与えることができる。

[0225] このタイマの長さは、接続要求を行ったソースデバイスの数に基づいて決定することができる。例えば、接続要求を行うソースデバイスの数が多い場合には、タイマの長さを短く設定し、接続要求を行うソースデバイスの数が少ない場合には、タイマの長さを長く設定するようにする。これにより、各ソースデバイスに平等に接続権を与えることができる。

[0226] そこで、１つのシンクデバイスに接続するための接続権を、複数のソースデバイスに順次割り当てる場合にその割り当てのタイミングをタイマで切り替える場合に用いられるタイマの算出方法について説明する。

[0227] このタイマの値（ソースデバイス切替タイマ値）ｔは、次の式１により求めることができる。

ｔ＝ｍｉｎ（Ｔ，Ｘ／ｎ） … 式１

[0228] ここで、Ｔは、１つのソースデバイス（１人のユーザ）に割り当てる最大時間を示す値である。すなわち、Ｔは、１つのソースデバイス（１人のユーザ）が連続して接続を占有することができる時間（接続占有時間）を示す値である。例えば、Ｔとして５分を設定することができる。この設定は、最大５分間接続を占有することができる設定である。

[0229] また、Ｘは、次回の接続までの待ち時間を示す値である。すなわち、Ｘは、接続要求を行った複数のソースデバイス（複数のユーザ）の接続要求が一回りする時間（すなわち、各自が一回ずつ接続するために必要となる時間）である。言い換えると、Ｘは、自分の順番をどれだけ待てるかを示す時間である。例えば、Ｘとして３０分（または、３０分程度）を設定することがで

きる。

[0230] また、ｎは、接続要求を行ったソースデバイスの数を示す値である。

[0231] また、ｍｉｎ（Ｔ，Ｘ／ｎ）は、１人のユーザの接続占有時間Ｔと、接続要求が一回りする時間Ｘをソースデバイスの総数ｎで除算した値とのうちの小さい値を意味する。すなわち、ソースデバイス切替タイマ値ｔは、ＴおよびＸ／ｎのうちの小さい値である。例えば、接続ソースデバイス数が少ない場合には、１人のソースデバイスに割り当てる最大時間Ｔが選択され、接続ソースデバイス数が多い場合には、Ｘ／ｎが選択されることになる。

[0232] 例えば、図１７に示す例（ｎは３）において、Ｔとして５分を設定し、Ｘとして３０分を設定する場合を想定する。この場合には、ｔ＝ｍｉｎ（５，１０（＝３０／３））であるため、ソースデバイス切替タイマ値ｔは、５分と算出される。

[0233] なお、このタイマの算出方法は一例であり、これ以外の算出方法によりタイマを算出するようにしてもよい。例えば、シンクデバイスがオープンな空間（例えば、不特定の環境（例えば、公衆広場、ホテルのロビー））に設置されているか、閉じた空間（例えば、特定の環境（例えば、ホテルの部屋、家庭内））に設置されているかに応じてタイマを変更するようにしてもよい。例えば、シンクデバイスがオープンな空間に設置されている場合には、タイマを短くし、閉じた空間に設置されている場合には、タイマを長くすることができる。また、シンクデバイスからの出力対象となるコンテンツが動画であるか、静止画であるかに応じてタイマを変更するようにしてもよい。例えば、シンクデバイスからの出力対象となるコンテンツが動画である場合には、タイマを長くし、静止画である場合には、タイマを短くする。

[0234] また、接続権を割り当てる順序は、優先度の順序としてもよく、ランダムとしてもよい。

[0235] ［シンクデバイスへの接続権を切り替える例］

図１８は、本技術の第３の実施の形態における通信システム４０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図

１８では、図１７に示す状態で、ソース側の情報処理装置１００からソース側の情報処理装置１０１に接続権を切り替える場合における通信処理例を示す。また、図１８では、ソースデバイス（情報処理装置１００、１０１、１０３）側で認証鍵を生成する場合における通信処理例を示す。

[0236] また、接続対象となるソースデバイス（情報処理装置１００、１０１、１０３）については、シンク側の情報処理装置２００が管理しているものとする。

[0237] ここで、図１８に示すように、ソース側の情報処理装置１００およびシンク側の情報処理装置２００間の認証が成功した後には、鍵一致確認結果が送信される（５２０、５２１）。続いて、シンク側の情報処理装置２００の制御部２２０は、タイマを設定する（５２２）。このタイマの値については、上述した式１を用いて算出される。

[0238] 続いて、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのコンテンツ送信が行われる（５２４、５２５）。なお、処理（５２０）よりも前の各処理については、図示を省略する。

[0239] ここで、ソース側の情報処理装置１００からシンク側の情報処理装置２００へのコンテンツ送信が行われている場合に（５２３、５２４）、タイマが満了した場合を想定する（５２５）。この場合には、シンク側の情報処理装置２００の制御部２２０は、現在の接続先であるソース側の情報処理装置１００に接続開放要求を送信する（５２６、５２７）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には接続開放要求３１４が格納され、データ３０４（図４に示す）には、接続開放要求に関する情報が格納される。

[0240] 続いて、シンク側の情報処理装置２００の制御部２２０は、次の接続先であるソース側の情報処理装置１０１に認証鍵生成要求を送信する（５２８、５２９）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には認証鍵生成要求３１７が格納され、データ３０４（図４に示す）には、認証鍵生成要求に関する情報が格納される。

[0241] 認証鍵生成要求が送信されると（５２８、５２９）、図７に示す各処理（４２２乃至４２６）と同様に、ソース側の情報処理装置１０１により認証鍵が生成される（５３０）。そして、ソース側の情報処理装置１０１からシンク側の情報処理装置２００に表示鍵情報が送信される（５４１、５４２）。なお、処理（５４３乃至５４８）は、図７に示す処理（４２５、４２６、４０５乃至４０８）と同一であるため、ここでの説明を省略する。また、処理（４０８）以降の各処理については、図示を省略する。

[0242] また、シンク側の情報処理装置２００は、ソースデバイス切替タイマ値ｔを用いて、接続状態にあるソースデバイス以外のソースデバイスに、あと何分で利用可能となるかを通知するための情報を提供するようにしてもよい。

[0243] このように、シンク側の情報処理装置２００へのデータ送信を行うソースデバイスが複数存在する場合には、各ソースデバイスのそれぞれに接続権が順次設定される。すなわち、シンク側の情報処理装置２００の制御部２２０は、所定規則に基づいて、複数のソースデバイスのそれぞれに無線接続を許可するため、ソースデバイス毎の認証鍵情報を表示部２４２に順次表示させる。この場合に、前のソースデバイスの接続状態が開放された後に、次のソースデバイスの認証鍵情報が表示部２４２に表示される。また、所定規則は、例えば、ソースデバイス切替タイマ値ｔ単位でソースデバイスを切り替える規則である。

[0244] また、シンク側の情報処理装置２００の制御部２２０は、ソースデバイスの数に基づいて、ソースデバイスへのデータ送信を行うための接続時間（例えば、ソースデバイス切替タイマ値ｔ）を決定する。そして、制御部２２０は、その接続時間に基づいて、複数のソースデバイスのそれぞれに所定順序でソースデバイス毎の認証鍵情報を表示部２４２に順次表示させる。

[0245] ［情報処理装置（シンクデバイス）の動作例］

図１９および図２０は、本技術の第３の実施の形態における情報処理装置２００による通信処理の処理手順の一例を示すフローチャートである。

[0246] 最初に、制御部２２０は、認証開始指示操作が行われたか否かを判断する

（ステップＳ９０１）。認証開始指示操作が行われた場合には（ステップＳ９０１）、ステップＳ９０３に進む。また、認証開始指示操作が行われていない場合には（ステップＳ９０１）、制御部２２０は、認証鍵生成要求を受信したか否かを判断する（ステップＳ９０２）。そして、認証鍵生成要求を受信した場合には（ステップＳ９０２）、制御部２２０は、認証鍵を生成し（ステップＳ９０３）、鍵画像を生成し（ステップＳ９０４）、鍵画像を表示部２４２に表示させる（ステップＳ９０５）。なお、ステップＳ９０５は、請求の範囲に記載の第１手順の一例である。

[0247] 続いて、制御部２２０は、認証鍵情報を受信したか否かを判断し（ステップＳ９０９）、認証鍵情報を受信した場合には、受信した認証鍵と生成された認証鍵とが一致するか否かを判断する（ステップＳ９１０）。そして、受信した認証鍵と生成された認証鍵とが一致する場合には（ステップＳ９１０）、認証鍵情報を送信したソースデバイスに鍵一致確認結果（一致した旨を示す結果）を送信する（ステップＳ９１１）。一方、受信した認証鍵と生成された認証鍵とが一致しない場合には（ステップＳ９１０）、認証鍵情報を送信したソースデバイスに鍵一致確認結果（一致しない旨を示す結果）を送信し（ステップＳ９１２）、通信処理の動作を終了する。なお、ステップＳ９０９乃至Ｓ９１２は、請求の範囲に記載の第２手順の一例である。

[0248] 続いて、制御部２２０は、タイマを設定する（ステップＳ９１８）。このタイマの値については、上述した式１を用いて算出される。続いて、制御部２２０は、鍵一致確認結果を送信したソースデバイスからのコンテンツを受信したか否かを判断し（ステップＳ９１９）、コンテンツを受信した場合には、その受信したコンテンツを表示部２４２に表示させる（ステップＳ９２０）。

[0249] また、コンテンツを受信していない場合には（ステップＳ９１９）、制御部２２０は、接続開放要求を受信したか否かを判断する（ステップＳ９２１）。そして、接続開放要求を受信した場合には（ステップＳ９２１）、通信処理の動作を終了する。また、接続開放要求を受信していない場合には（ス

テップＳ９２１）、制御部２２０は、表示鍵情報を受信したか否かを判断する（ステップＳ９２２）。

[0250] 表示鍵情報を受信していない場合には（ステップＳ９２２）、制御部２２０は、タイマが満了になったか否かを判断する（ステップＳ９２３）。そして、タイマが満了になっていない場合には（ステップＳ９２３）、ステップＳ９１９に戻る。一方、タイマが満了になった場合には（ステップＳ９２３）、制御部２２０は、ソースデバイスに接続開放要求を送信し（ステップＳ９２４）、通信処理の動作を終了する。

[0251] また、表示鍵情報を受信した場合には（ステップＳ９２２）、制御部２２０は、その表示鍵情報を送信したソースデバイスの優先度は、接続状態のソースデバイスの優先度よりも高いか否かを判断する（ステップＳ９２５）。そして、その表示鍵情報を送信したソースデバイスの優先度が、接続状態のソースデバイスの優先度よりも高くない場合には（ステップＳ９２５）、制御部２２０は、表示鍵情報を受信したソースデバイスに拒否理由通知を送信する（ステップＳ９２６）。一方、その表示鍵情報を送信したソースデバイスの優先度が、接続状態のソースデバイスの優先度よりも高い場合には（ステップＳ９２５）、制御部２２０は、接続状態のソースデバイスに、接続開放要求を送信し（ステップＳ９２７）、ステップＳ９０４に戻る。

[0252] また、認証鍵生成要求を受信していない場合には（ステップＳ９０２）、制御部２２０は、表示鍵情報を受信したか否かを判断する（ステップＳ９０６）。表示鍵情報を受信した場合には（ステップＳ９０６）、制御部２２０は、拒否する旨がメモリ２３０に記憶されているか否かを判断する（ステップＳ９０７）。そして、拒否する旨がメモリ２３０に記憶されていない場合には（ステップＳ９０７）、ステップＳ９０４に進む。一方、拒否する旨がメモリ２３０に記憶されている場合には（ステップＳ９０７）、通信処理の動作を終了する。

[0253] また、表示鍵情報を受信していない場合には（ステップＳ９０６）、制御部２２０は、鍵画像を受信したか否かを判断する（ステップＳ９０８）。そ

して、鍵画像を受信した場合には（ステップＳ９０８）、ステップＳ９０５に進む。一方、鍵画像を受信していない場合には（ステップＳ９０８）、通信処理の動作を終了する。

[0254] また、認証鍵情報を受信していない場合には（ステップＳ９０９）、制御部２２０は、鍵一致確認結果を受信したか否かを判断する（ステップＳ９１３）。そして、鍵一致確認結果を受信した場合には（ステップＳ９１３）、制御部２２０は、受信した鍵一致確認結果が一致する旨を示すものであるか否かを判断する（ステップＳ９１４）。そして、鍵一致確認結果が一致する旨を示すものである場合には（ステップＳ９１４）、ステップＳ９１８に進む。一方、鍵一致確認結果が一致しない旨を示すものである場合には（ステップＳ９１４）、通信処理の動作を終了する。

[0255] また、鍵一致確認結果を受信していない場合には（ステップＳ９１３）、制御部２２０は、拒否指示操作が行われたか否かを判断する（ステップＳ９１５）。そして、拒否指示操作が行われた場合には（ステップＳ９１５）、制御部２２０は、他のソースデバイスからの要求に対して拒否する旨をメモリ２３０に記憶させる（ステップＳ９１６）。続いて、制御部２２０は、認証鍵生成要求を送信したソースデバイスに拒否理由通知を送信し（ステップＳ９１７）、通信処理の動作を終了する。

[0256] ［情報処理装置（ソースデバイス）の動作例］

図２１は、本技術の第３の実施の形態における情報処理装置１００による通信処理の処理手順の一例を示すフローチャートである。

[0257] 最初に、制御部１２０は、認証鍵情報入力操作が行われたか否かを判断する（ステップＳ９３１）。そして、認証鍵情報入力操作が行われていない場合には（ステップＳ９３１）、制御部１２０は、認証開始指示操作が行われたか否かを判断する（ステップＳ９３２）。

[0258] 認証開始指示操作が行われた場合には（ステップＳ９３２）、制御部１２０は、認証鍵を生成する（ステップＳ９３３）。続いて、制御部１２０は、鍵画像をソースデバイス側で生成する設定がされているか否かを判断する（

ステップＳ９３４）。

[0259] 鍵画像をソースデバイス側で生成する設定がされていない場合には（ステップＳ９３４）、制御部１２０は、生成された認証鍵を画像情報に変換するための表示鍵情報をシンクデバイスに送信する（ステップＳ９３５）。また、鍵画像をソースデバイス側で生成する設定がされている場合には（ステップＳ９３４）、制御部１２０は、生成された認証鍵を画像情報に変換して鍵画像を生成し（ステップＳ９３６）、その鍵画像をシンクデバイスに送信する（ステップＳ９３７）。

[0260] また、認証開始指示操作が行われていない場合には（ステップＳ９３２）、制御部２２０は、鍵情報表示通知を受信したか否かを判断する（ステップＳ９３８）。そして、鍵情報表示通知を受信した場合には（ステップＳ９３８）、制御部１２０は、受信した鍵情報表示通知を表示部１４２に表示させる（ステップＳ９３９）。

[0261] また、鍵情報表示通知を受信していない場合には（ステップＳ９３８）、制御部１２０は、拒否理由通知を受信したか否かを判断する（ステップＳ９４０）。そして、拒否理由通知を受信した場合には（ステップＳ９４０）、制御部１２０は、受信した拒否理由通知を表示部１４２に表示させる（ステップＳ９４１）。

[0262] また、認証鍵情報入力操作が行われた場合には（ステップＳ９３１）、制御部１２０は、鍵一致確認をソースデバイス側で実施する設定がされているか否かを判断する（ステップＳ９４２）。そして、鍵一致確認をソースデバイス側で実施する設定がされている場合には（ステップＳ９４２）、ステップＳ９４５に進む。一方、鍵一致確認をソースデバイス側で実施する設定がされていない場合には（ステップＳ９４２）、制御部１２０は、入力された認証鍵情報をシンクデバイスに送信する（ステップＳ９４３）。

[0263] 続いて、制御部１２０は、鍵一致確認結果を受信したか否かを判断し（ステップＳ９４４）、鍵一致確認結果を受信していない場合には、監視を継続して行う。一方、鍵一致確認結果を受信した場合には（ステップＳ９４４）

、制御部１２０は、受信した鍵一致確認結果が一致する旨を示すものであるか否かを判断する（ステップＳ９４５）。そして、鍵一致確認結果が一致しない旨を示すものである場合には（ステップＳ９４５）、通信処理の動作を終了する。

[0264] また、鍵一致確認結果が一致する旨を示すものである場合には（ステップＳ９４５）、制御部１２０は、メモリ１３０に記憶されているコンテンツのシンクデバイスへの送信を開始する（ステップＳ９４６）。続いて、制御部１２０は、送信対象となるコンテンツの送信が終了したか否かを判断する（ステップＳ９４７）。そして、送信対象となるコンテンツの送信が終了した場合には（ステップＳ９４７）、制御部１２０は、接続開放要求をシンクデバイスに送信する（ステップＳ９４８）。一方、送信対象となるコンテンツの送信が終了していない場合には（ステップＳ９４７）、制御部１２０は、接続開放要求を受信したか否かを判断する（ステップＳ９４９）。そして、接続開放要求を受信していない場合には（ステップＳ９４９）、ステップＳ９４６に戻る。一方、接続開放要求を受信した場合には（ステップＳ９４９）、通信処理の動作を終了する。

[0265] ＜４．第４の実施の形態＞

本技術の第１乃至第３の実施の形態では、ソースデバイスおよびシンクデバイスの何れかが認証鍵情報を生成する例を示した。ここで、例えば、ソースデバイスおよびシンクデバイス以外の他の装置により生成された認証鍵情報を、ソースデバイスおよびシンクデバイスが用いるようにしてもよい。

[0266] そこで、本技術の第４の実施の形態では、他の装置（例えば、サーバ）により生成された認証鍵情報を用いて認証処理を行う例を示す。なお、本技術の第４の実施の形態における通信システムは、図１に示す通信システム１０と略同様である。このため、通信システム１０と共通する部分については、同一の符号を付して、これらの説明の一部を省略する。

[0267] ［シンクデバイス側に鍵情報提供サーバを設ける例］

最初に、シンクデバイス側に鍵情報提供サーバを設ける例について説明す

る。

[0268] ［通信システムの構成例］

図２２は、本技術の第４の実施の形態における通信システム５０の構成例を示す図である。

[0269] 通信システム５０は、情報処理装置１００と、情報処理装置２００乃至２０２と、鍵情報提供サーバ６００と、ネットワーク６１０とを備える。

[0270] なお、情報処理装置２００乃至２０２は、図１に示す情報処理装置２００に対応する。ただし、情報処理装置２００乃至２０２は、ネットワーク６１０を介して鍵情報提供サーバ６００と接続され、鍵情報提供サーバ６００との間で鍵に関する各情報のやり取りを行う点が、情報処理装置２００とは異なる。

[0271] 通信システム５０は、例えば、各部屋にシンクデバイスが設置されている施設（例えば、ホテル）に構築されることが想定される。また、鍵情報提供サーバ６００として、例えば、ホテルの鍵管理サーバが想定される。

[0272] ネットワーク６１０は、情報処理装置２００乃至２０２と、鍵情報提供サーバ６００とを接続するネットワークである。例えば、ネットワーク６１０は、有線ネットワーク（例えば、イーサネット（登録商標））や同軸ケーブルである。

[0273] 鍵情報提供サーバ６００は、鍵に関する情報（認証鍵、鍵画像）を集中管理する情報処理装置であり、管理されている鍵に関する情報を情報処理装置２００乃至２０２に提供する。例えば、通信システム５０では、シンクデバイス（情報処理装置２００乃至２０２）の代わりに、鍵情報提供サーバ６００において認証開始指示操作を行うようにする。この認証開始指示操作が行われた場合には、鍵情報提供サーバ６００が、各シンクデバイス（情報処理装置２００乃至２０２）のそれぞれに認証鍵情報を送信する。この場合には、シンクデバイス毎に異なる認証鍵情報を送信するようにする。また、認証開始指示操作が行われた場合に、鍵情報提供サーバ６００からシンクデバイスの全てに認証鍵情報を送信するようにしてもよく、一部のシンクデバイス

にのみ認証鍵情報を送信するようにしてもよい。このように、一部のシンクデバイスにのみ認証鍵情報を送信する場合には、認証開始指示操作により送信先のシンクデバイスを指定するようにしてもよい。

[0274] また、鍵情報提供サーバ６００から各シンクデバイス（情報処理装置２００乃至２０２）に表示鍵情報のみを送信して鍵画像をシンクデバイスで生成するようにしてもよく、鍵画像そのものを送信するようにしてもよい。また、認証開始指示操作により、送信対象となる認証鍵情報を指定するようにしてもよい。

[0275] なお、図２２では、複数のシンクデバイス（情報処理装置２００乃至２０２）と、鍵情報提供サーバ６００とが接続される例を示すが、１つのシンクデバイスと１つの鍵情報提供サーバとが接続される場合についても同様に適用することができる。また、鍵情報提供サーバ６００を省略して、複数のシンクデバイス（情報処理装置２００乃至２０２）のうちの少なくとも１つに、鍵情報提供サーバ６００と同等の機能を備えるようにしてもよい。この場合には、鍵情報提供サーバ６００と同等の機能を備えるシンクデバイスが、他のシンクデバイスに鍵に関する情報を提供する。

[0276] ［ソースデバイス側に鍵情報提供サーバを設ける例］

次に、ソースデバイス側に鍵情報提供サーバを設ける例について説明する。

[0277] ［通信システムの構成例］

図２３は、本技術の第４の実施の形態における通信システム６０の構成例を示す図である。

[0278] 通信システム６０は、情報処理装置１００と、情報処理装置２００乃至２０２と、鍵情報提供サーバ６２０と、ネットワーク６３０とを備える。

[0279] なお、情報処理装置１００は、図１に示す情報処理装置１００と略同一である。ただし、情報処理装置１００は、ネットワーク６３０を介して鍵情報提供サーバ６２０と接続され、鍵情報提供サーバ６２０との間で鍵に関する各情報のやり取りを行う点が、情報処理装置１００とは異なる。また、情報

処理装置２００乃至２０２は、図１に示す情報処理装置２００に対応する。

[0280] なお、通信システム６０は、図２２に示す通信システム５０の変形例であり、鍵情報提供サーバ６００およびネットワーク６１０の代わりに、鍵情報提供サーバ６２０およびネットワーク６３０を備える点が、通信システム５０とは異なる。

[0281] なお、図２３では、ソースデバイス（情報処理装置１００）の無線接続が、シンクデバイスとの間の無線接続と、ネットワーク６３０（例えば、インターネット、ローカルネットワーク）との間の無線接続との二通り存在する例を示す。ただし、これらの無線接続が同一の無線接続となる場合についても同様に適用することができる。すなわち、情報処理装置１００がネットワーク６３０と接続する場合には、情報処理装置２００乃至２０２との接続に使用する無線通信機能を利用するようにしてもよく、他の無線通信機能を利用するようにしてもよい。例えば、３Ｇ、ＬＴＥ等の無線通信機能を情報処理装置１００に備え、この無線通信機能によりネットワーク６３０に接続するようにしてもよい。

[0282] また、鍵情報提供サーバ６２０は、インターネット上に設置するようにしてもよく、ローカルネットワーク（ＬＡＮ）上に設置するようにしてもよい。なお、鍵情報提供サーバ６２０として、例えば、インターネット上の鍵情報管理サーバ／アプリケーション等が想定される。

[0283] ネットワーク６３０は、電話網、インターネット等の公衆回線網である。また、情報処理装置１００が、３Ｇ、ＬＴＥ等の通信機能を利用してネットワーク６３０と接続する場合には、情報処理装置１００とネットワーク６３０とは、通信制御装置（図示せず）を介して接続される。

[0284] 鍵情報提供サーバ６２０は、情報処理装置１００からの鍵情報要求に応じて鍵に関する情報を提供する情報処理装置である。この鍵情報提供サーバ６２０および情報処理装置１００間における情報のやり取りについては、図２４、図２５を参照して詳細に説明する。

[0285] なお、図２３では、複数のシンクデバイスと、鍵情報提供サーバ６２０と

を備える通信システム６０の例を示すが、１つのシンクデバイスと１つの鍵情報提供サーバとを備える通信システムについても同様に適用することができる。また、鍵情報提供サーバ６２０を省略して、複数のシンクデバイス（情報処理装置２００乃至２０２）のうちの少なくとも１つに、鍵情報提供サーバ６２０と同等の機能を備えるようにしてもよい。この場合には、鍵情報提供サーバ６２０と同等の機能を備えるシンクデバイスが、ソース側の情報処理装置１００に鍵に関する情報を提供する。また、鍵情報提供サーバ６２０を省略して、複数のソースデバイスのうちの少なくとも１つに、鍵情報提供サーバ６２０と同等の機能を備えるようにしてもよい。この場合には、鍵情報提供サーバ６２０と同等の機能を備えるソースデバイスが、ソース側の情報処理装置１００に鍵に関する情報を提供する。

[0286] ［鍵情報提供サーバが鍵のみを生成する場合の通信例］

図２４は、本技術の第４の実施の形態における通信システム６０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図２４では、図２３に示す状態で、ユーザが情報処理装置１００を用いて認証開始指示操作を行う場合における通信処理例を示す。また、図２４では、ソースデバイス（情報処理装置１００）からの鍵情報要求に応じて鍵情報提供サーバ６２０が認証鍵のみを生成して提供する場合における通信処理例を示す。

[0287] 最初に、ユーザは、ソース側の情報処理装置１００の操作受付部１５２を用いて認証開始指示操作を行う（７０１）。このように、認証開始指示操作が行われた場合には（７０１）、ソース側の情報処理装置１００の制御部１２０は、鍵情報要求を鍵情報提供サーバ６２０に送信する（７０２、７０３）。この場合に送信対象となる情報に含まれる情報要素識別子３０３（図４に示す）には、鍵情報要求３１５が格納され、データ３０４（図４に示す）には、鍵情報要求に関する情報が格納される。

[0288] 鍵情報要求を受信すると（７０３）、鍵情報提供サーバ６２０は、認証処理を行う際に用いる認証鍵を生成する（７０４）。続いて、鍵情報提供サー

バ６２０は、鍵情報要求を送信した情報処理装置１００に、生成された認証鍵を画像情報に変換するための表示鍵情報を送信する（７０５、７０６）。

[0289] 鍵を受信すると（７０６）、ソース側の情報処理装置１００の制御部１２０は、シンク側の情報処理装置２００に、その受信した表示鍵情報を送信する（７０７、７０８）。続いて、シンク側の情報処理装置２００の制御部２２０は、受信した表示鍵情報を画像情報に変換して鍵画像を生成する（７０９）。

[0290] なお、これ以降の各処理については、本技術の第１乃至第３の実施の形態に示す各処理と同様であるため、ここでの図示およびその説明を省略する。

[0291] ［鍵情報提供サーバが鍵画像を生成する場合の通信例］

図２５は、本技術の第４の実施の形態における通信システム６０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図２５は、図２４の変形例であり、ソースデバイス（情報処理装置１００）からの鍵情報要求に応じて鍵情報提供サーバ６２０が鍵画像を生成して提供する点が、図２４とは異なる。このため、図２５では、これらの異なる点を中心にして説明する。

[0292] なお、認証鍵を生成するまでの各処理（７１１乃至７１４）については、図２４に示す各処理（７０１乃至７０４）と同一であるため、ここでの説明を省略する。

[0293] 鍵情報提供サーバ６２０は、生成された認証鍵を画像情報に変換して鍵画像を生成する（７１５）。続いて、鍵情報提供サーバ６２０は、鍵情報要求を送信した情報処理装置１００に、生成された鍵画像を送信する（７１６、７１７）。

[0294] 鍵画像を受信すると（７１７）、ソース側の情報処理装置１００の制御部１２０は、シンク側の情報処理装置２００に、その受信した鍵画像を送信する（７１８、７１９）。

[0295] なお、これ以降の各処理については、本技術の第１乃至第３の実施の形態に示す各処理と同様であるため、ここでの図示およびその説明を省略する。

[0296] ［サーバが鍵画像の生成および鍵一致確認を行う場合の通信例］

以上では、サーバが、鍵に関する情報（認証鍵、鍵画像）を生成して情報処理装置に提供する例を示した。ここで、サーバが鍵画像の生成および鍵一致確認を行うようにしてもよい。そこで、以下では、サーバが鍵画像の生成および鍵一致確認を行う例を示す。

[0297] ［通信システムの構成例］

図２６は、本技術の第４の実施の形態における通信システム７０の構成例を示す図である。

[0298] 通信システム７０は、情報処理装置１００と、情報処理装置２００乃至２０２と、サーバ６５０と、ネットワーク６６０と、アクセスポイント６７０とを備える。

[0299] なお、通信システム７０は、図２２に示す通信システム５０の変形例であり、鍵情報提供サーバ６００およびネットワーク６１０の代わりに、サーバ６５０、ネットワーク６６０およびアクセスポイント６７０を備える点が、通信システム５０とは異なる。

[0300] また、図２６では、各シンクデバイスが無線通信機能を備えていない場合でも本技術の第１乃至第３の実施の形態を適用することができる通信システムを示す。例えば、ホテルのような環境以外に、一般家庭のような環境でも、本技術の第１乃至第３の実施の形態を適用することができる。例えば、無線通信機能を備えていないシンクデバイスが、サーバ６５０およびアクセスポイント６７０を介してソース側の情報処理装置１００と接続するような環境でも、本技術の第１乃至第３の実施の形態を適用することができる。

[0301] アクセスポイント６７０は、情報処理装置１００およびサーバ６５０間で通信を行う際に用いられるアクセスポイント（例えば、Ｗｉ－Ｆｉアクセスポイント）である。すなわち、図２６に示す例では、ソースデバイス（情報処理装置１００）は、シンクデバイス（情報処理装置２００乃至２０２）と直接通信せずに、アクセスポイント６７０を介してサーバ６５０と通信する。また、サーバ６５０は、アクセスポイント６７０を介してソースデバイス

（情報処理装置１００）から受信した情報（例えば、コンテンツ）を、シンクデバイス（情報処理装置２００乃至２０２）にネットワーク６６０を介して送信する。

[0302] サーバ６５０は、アクセスポイント６７０を介してソースデバイス（情報処理装置１００）との間で通信を行うサーバである。また、サーバ６５０の制御部６５１は、鍵画像の生成および鍵一致確認を行う。また、サーバ６５０の制御部６５１は、ネットワーク６６０を介してシンクデバイス（情報処理装置２００乃至２０２）に画像情報（鍵画像、コンテンツ）を提供する。

[0303] ［通信例］

図２７は、本技術の第４の実施の形態における通信システム７０を構成する各装置間における通信処理例を示すシーケンスチャートである。なお、図２７では、図２６に示す状態で、ユーザが情報処理装置１００を用いて認証開始指示操作を行う場合における通信処理例を示す。

[0304] 図２７に示す例は、画像情報の通信（７２３乃至７２７、７３６乃至７３９）以外は、アクセスポイント６７０を介してソース側の情報処理装置１００およびサーバ６５０間でやり取りが行われる。また、図２７に示す各処理（７２１乃至７４０）は、画像情報の通信（７２３乃至７２７、７３６乃至７３９）以外は、図７に示す各処理（４２１乃至４１５）と同様である。このため、ここでの図示およびその説明を省略する。

[0305] このように、サーバ６５０の制御部６５１は、ネットワーク６６０を介してシンク側の情報処理装置２００に認証鍵情報（例えば、鍵画像）を送信してシンク側の情報処理装置２００から出力（例えば、鍵画像の表示）させる（７２６乃至７２８）。また、サーバ６５０の制御部６５１は、ソース側の情報処理装置１００に入力された認証鍵情報と、シンク側の情報処理装置２００出力された認証鍵情報とに基づいて、無線接続をソース側の情報処理装置１００に許可するかを決定する（７３３乃至７３５）。また、サーバ６５０の制御部６５１は、その無線接続を許可する決定がされた後に、ソース側の情報処理装置１００から送信されたデータを、ネットワーク６６０を介し

てシンク側の情報処理装置２００に送信して出力させる（７３６乃至７３９）。

[0306] このように、サーバで鍵に関する情報の生成や提供を行うことにより、ソースデバイスやシンクデバイスの処理を単純化することができ、ソースデバイスやシンクデバイスの処理を軽減させることができる。

[0307] なお、ソースデバイスとして、例えば、無線通信機能を備える他の情報処理装置（例えば、パソコン、ゲーム機、デジタルスチルカメラ、デジタルビデオカメラ（例えば、カメラ一体型レコーダ））を用いるようにしてもよい。また、シンクデバイスとして、例えば、無線通信機能を備える他の情報処理装置（例えば、プロジェクタ、パーソナルコンピュータ）や携帯型の情報処理装置（例えば、スマートフォン、タブレット端末）を用いるようにしてもよい。

[0308] なお、上述の実施の形態は本技術を具現化するための一例を示したものであり、実施の形態における事項と、請求の範囲における発明特定事項とはそれぞれ対応関係を有する。同様に、請求の範囲における発明特定事項と、これと同一名称を付した本技術の実施の形態における事項とはそれぞれ対応関係を有する。ただし、本技術は実施の形態に限定されるものではなく、その要旨を逸脱しない範囲において実施の形態に種々の変形を施すことにより具現化することができる。

[0309] また、上述の実施の形態において説明した処理手順は、これら一連の手順を有する方法として捉えてもよく、また、これら一連の手順をコンピュータに実行させるためのプログラム乃至そのプログラムを記憶する記録媒体として捉えてもよい。この記録媒体として、例えば、ＣＤ（Compact Disc）、ＭＤ（MiniDisc）、ＤＶＤ（Digital Versatile Disc）、メモリカード、ブルーレイディスク（Blu-ray（登録商標） Disc）等を用いることができる。

[0310] なお、本技術は以下のような構成もとることができる。

（１）

無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送

信を行うための前記第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を前記第２情報処理装置から出力させ、前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかを決定する制御部を具備する情報処理装置。

（２）

前記情報処理装置は、前記第２情報処理装置であり、

前記第１情報処理装置から送信されたデータを出力する出力部をさらに具備し、

前記制御部は、前記認証鍵情報を前記出力部から出力させ、前記無線接続を前記第１情報処理装置に許可する決定がされた後に前記第１情報処理装置から送信されたデータを前記出力部から出力させる

前記（１）に記載の情報処理装置。

（３）

前記出力部は、前記第１情報処理装置から送信された画像データに基づく画像を表示する表示部であり、

前記制御部は、前記認証鍵情報を前記表示部に表示させ、前記無線接続を前記第１情報処理装置に許可する決定がされた後に前記第１情報処理装置から送信された画像データに基づく画像を前記表示部に表示させる

前記（２）に記載の情報処理装置。

（４）

前記第１情報処理装置は、前記第２情報処理装置から出力された認証鍵情報を入力するための入力部から入力された認証鍵情報を前記情報処理装置に送信し、

前記制御部は、前記第１情報処理装置から送信された認証鍵情報と前記出力された認証鍵情報とに基づいて前記決定を行う

前記（１）から（３）のいずれかに記載の情報処理装置。

（５）

前記入力部は、前記第２情報処理装置から出力された認証鍵情報を撮像する撮像部と、前記第２情報処理装置から出力された認証鍵情報を入力するためのユーザ操作を受け付ける操作受付部とのうちの少なくとも１つである前記（４）に記載の情報処理装置。

（６）

前記制御部は、前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とが一致すると判定された場合に前記無線接続を前記第１情報処理装置に許可すると決定する前記（１）から（５）のいずれかに記載の情報処理装置。

（７）

前記制御部は、複数の前記第２情報処理装置のうちからユーザ操作により選択された第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を前記選択された第２情報処理装置から出力させる前記（１）から（６）のいずれかに記載の情報処理装置。

（８）

前記第１情報処理装置は、複数の前記第２情報処理装置に関する情報を表示させ、当該表示されている複数の第２情報処理装置のうちからユーザ操作により選択された第２情報処理装置に関する情報を前記情報処理装置に送信し、

前記制御部は、前記送信された第２情報処理装置に関する情報に基づいて当該第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を当該第２情報処理装置から出力させる

前記（１）から（６）のいずれかに記載の情報処理装置。

（９）

前記制御部は、前記無線接続を前記第１情報処理装置に許可する決定がされ、前記第１情報処理装置および前記第２情報処理装置が接続状態となっている場合に、前記認証鍵情報を前記第２情報処理装置から出力させるための要求を他の情報処理装置から受信したときには前記要求を拒否する前記（１

）から（６）のいずれかに記載の情報処理装置。

（１０）

前記制御部は、前記接続状態が開放された後に前記要求を前記他の情報処理装置から受信したときには前記要求に応じて前記認証鍵情報を前記第２情報処理装置から出力させる前記（９）に記載の情報処理装置。

（１１）

前記制御部は、前記接続状態で前記要求を前記他の情報処理装置から受信した場合において、前記他の情報処理装置の優先度が前記第１情報処理装置の優先度よりも高い場合には前記要求を拒否せずに前記接続状態を開放する前記（９）に記載の情報処理装置。

（１２）

前記制御部は、前記第１情報処理装置からの要求に応じて前記認証鍵情報を前記第２情報処理装置から出力させ、前記無線接続を拒否するためのユーザ操作が受け付けられた場合には、前記無線接続を前記第１情報処理装置に許可しないと決定する前記（１）から（６）のいずれかに記載の情報処理装置。

（１３）

前記制御部は、前記第２情報処理装置へのデータ送信を行う前記第１情報処理装置が複数存在する場合には、所定規則に基づいて前記複数の第１情報処理装置のそれぞれに前記無線接続を許可するための前記第１情報処理装置毎の認証鍵情報を前記第２情報処理装置から順次出力させる前記（１）から（６）のいずれかに記載の情報処理装置。

（１４）

前記制御部は、前記第１情報処理装置の数に基づいて前記第２情報処理装置へのデータ送信を行うための接続時間を決定し、前記接続時間に基づいて前記複数の第１情報処理装置のそれぞれに所定順序で前記第１情報処理装置毎の認証鍵情報を前記第２情報処理装置から順次出力させる前記（１３）に記載の情報処理装置。

（１５）

前記情報処理装置は、前記第１情報処理装置であり、

前記第２情報処理装置から出力された認証鍵情報を入力するための入力部をさらに具備し、

前記制御部は、前記無線通信を利用して前記第２情報処理装置に前記認証鍵情報を送信して前記第２情報処理装置から出力させ、前記入力部に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を許可するかを決定し、前記無線通信を利用して当該決定の結果を前記第２情報処理装置に送信する

前記（１）に記載の情報処理装置。

（１６）

前記情報処理装置は、前記第２情報処理装置にネットワークを介して接続されるサーバであり、

前記制御部は、前記ネットワークを介して前記第２情報処理装置に前記認証鍵情報を送信して前記第２情報処理装置から出力させ、前記無線接続を前記第１情報処理装置に許可する決定がされた後に前記第１情報処理装置から送信されたデータを、前記ネットワークを介して前記第２情報処理装置に送信して前記第２情報処理装置から出力させる

前記（１）に記載の情報処理装置。

（１７）

無線通信を利用して第２情報処理装置へのデータ送信を行う第１情報処理装置と、前記第１情報処理装置からのデータを受信して出力する第２情報処理装置とを具備する通信システムであって、

前記データ送信を行うための前記第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報が前記第２情報処理装置から出力され、前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかが決定される

通信システム。

（１８）

無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送信を行うための前記第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を前記第２情報処理装置から出力させる第１手順と、

前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかを決定する第２手順と

を具備する情報処理方法。

（１９）

無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送信を行うための前記第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を前記第２情報処理装置から出力させる第１手順と、

前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかを決定する第２手順と

をコンピュータに実行させるプログラム。

符号の説明

[0311] １０、２０、３０、４０、５０、６０、７０　通信システム

１００、１０１、１０３　情報処理装置

１０２　表示部

１１１、２１１　アンテナ

１１２、２１２　通信部

１２０、２２０、６５１　制御部

１３０、２３０　メモリ

１４１、２４１　表示情報入出力部

１４２、２４２　表示部

１５１、２５１　操作情報入出力部

１５２、２５２　操作受付部

１６１　撮像情報入出力部

１６２　撮像部

１７１、２７１　音声情報入出力部

１７２　音声入力部

１７３、２７２　音声出力部

１８０、２８０　バス

２００～２０２　情報処理装置

２６１　リモートコントローラ情報入出力部

２６２　リモートコントローラ

６００、６２０　鍵情報提供サーバ

６１０、６３０、６６０　ネットワーク

６５０　サーバ

６７０　アクセスポイント

請求の範囲

[請求項1] 無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送信を行うための前記第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を前記第２情報処理装置から出力させ、前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかを決定する制御部を具備する情報処理装置。

[請求項2] 前記情報処理装置は、前記第２情報処理装置であり、

前記第１情報処理装置から送信されたデータを出力する出力部をさらに具備し、

前記制御部は、前記認証鍵情報を前記出力部から出力させ、前記無線接続を前記第１情報処理装置に許可する決定がされた後に前記第１情報処理装置から送信されたデータを前記出力部から出力させる

請求項１記載の情報処理装置。

[請求項3] 前記出力部は、前記第１情報処理装置から送信された画像データに基づく画像を表示する表示部であり、

前記制御部は、前記認証鍵情報を前記表示部に表示させ、前記無線接続を前記第１情報処理装置に許可する決定がされた後に前記第１情報処理装置から送信された画像データに基づく画像を前記表示部に表示させる

請求項２記載の情報処理装置。

[請求項4] 前記第１情報処理装置は、前記第２情報処理装置から出力された認証鍵情報を入力するための入力部から入力された認証鍵情報を前記情報処理装置に送信し、

前記制御部は、前記第１情報処理装置から送信された認証鍵情報と前記出力された認証鍵情報とに基づいて前記決定を行う

請求項１記載の情報処理装置。

[請求項5] 前記入力部は、前記第２情報処理装置から出力された認証鍵情報を

撮像する撮像部と、前記第２情報処理装置から出力された認証鍵情報を入力するためのユーザ操作を受け付ける操作受付部とのうちの少なくとも１つである請求項４記載の情報処理装置。

[請求項6] 前記制御部は、前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とが一致すると判定された場合に前記無線接続を前記第１情報処理装置に許可すると決定する請求項１記載の情報処理装置。

[請求項7] 前記制御部は、複数の前記第２情報処理装置のうちからユーザ操作により選択された第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を前記選択された第２情報処理装置から出力させる請求項１記載の情報処理装置。

[請求項8] 前記第１情報処理装置は、複数の前記第２情報処理装置に関する情報を表示させ、当該表示されている複数の第２情報処理装置のうちからユーザ操作により選択された第２情報処理装置に関する情報を前記情報処理装置に送信し、

前記制御部は、前記送信された第２情報処理装置に関する情報に基づいて当該第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を当該第２情報処理装置から出力させる

請求項１記載の情報処理装置。

[請求項9] 前記制御部は、前記無線接続を前記第１情報処理装置に許可する決定がされ、前記第１情報処理装置および前記第２情報処理装置が接続状態となっている場合に、前記認証鍵情報を前記第２情報処理装置から出力させるための要求を他の情報処理装置から受信したときには前記要求を拒否する請求項１記載の情報処理装置。

[請求項10] 前記制御部は、前記接続状態が開放された後に前記要求を前記他の情報処理装置から受信したときには前記要求に応じて前記認証鍵情報を前記第２情報処理装置から出力させる請求項９記載の情報処理装置。

[請求項11] 前記制御部は、前記接続状態で前記要求を前記他の情報処理装置から受信した場合において、前記他の情報処理装置の優先度が前記第１情報処理装置の優先度よりも高い場合には前記要求を拒否せずに前記接続状態を開放する請求項９記載の情報処理装置。

[請求項12] 前記制御部は、前記第１情報処理装置からの要求に応じて前記認証鍵情報を前記第２情報処理装置から出力させ、前記無線接続を拒否するためのユーザ操作が受け付けられた場合には、前記無線接続を前記第１情報処理装置に許可しないと決定する請求項１記載の情報処理装置。

[請求項13] 前記制御部は、前記第２情報処理装置へのデータ送信を行う前記第１情報処理装置が複数存在する場合には、所定規則に基づいて前記複数の第１情報処理装置のそれぞれに前記無線接続を許可するための前記第１情報処理装置毎の認証鍵情報を前記第２情報処理装置から順次出力させる請求項１記載の情報処理装置。

[請求項14] 前記制御部は、前記第１情報処理装置の数に基づいて前記第２情報処理装置へのデータ送信を行うための接続時間を決定し、前記接続時間に基づいて前記複数の第１情報処理装置のそれぞれに所定順序で前記第１情報処理装置毎の認証鍵情報を前記第２情報処理装置から順次出力させる請求項１３記載の情報処理装置。

[請求項15] 前記情報処理装置は、前記第１情報処理装置であり、

前記第２情報処理装置から出力された認証鍵情報を入力するための入力部をさらに具備し、

前記制御部は、前記無線通信を利用して前記第２情報処理装置に前記認証鍵情報を送信して前記第２情報処理装置から出力させ、前記入力部に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を許可するかを決定し、前記無線通信を利用して当該決定の結果を前記第２情報処理装置に送信する

請求項１記載の情報処理装置。

[請求項16] 前記情報処理装置は、前記第２情報処理装置にネットワークを介して接続されるサーバであり、

前記制御部は、前記ネットワークを介して前記第２情報処理装置に前記認証鍵情報を送信して前記第２情報処理装置から出力させ、前記無線接続を前記第１情報処理装置に許可する決定がされた後に前記第１情報処理装置から送信されたデータを、前記ネットワークを介して前記第２情報処理装置に送信して前記第２情報処理装置から出力させる

請求項１記載の情報処理装置。

[請求項17] 無線通信を利用して第２情報処理装置へのデータ送信を行う第１情報処理装置と、前記第１情報処理装置からのデータを受信して出力する第２情報処理装置とを具備する通信システムであって、

前記データ送信を行うための前記第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報が前記第２情報処理装置から出力され、前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかが決定される

通信システム。

[請求項18] 無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送信を行うための前記第２情報処理装置への無線接続を前記第１情報処理装置に許可するための認証鍵情報を前記第２情報処理装置から出力させる第１手順と、

前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかを決定する第２手順と

を具備する情報処理方法。

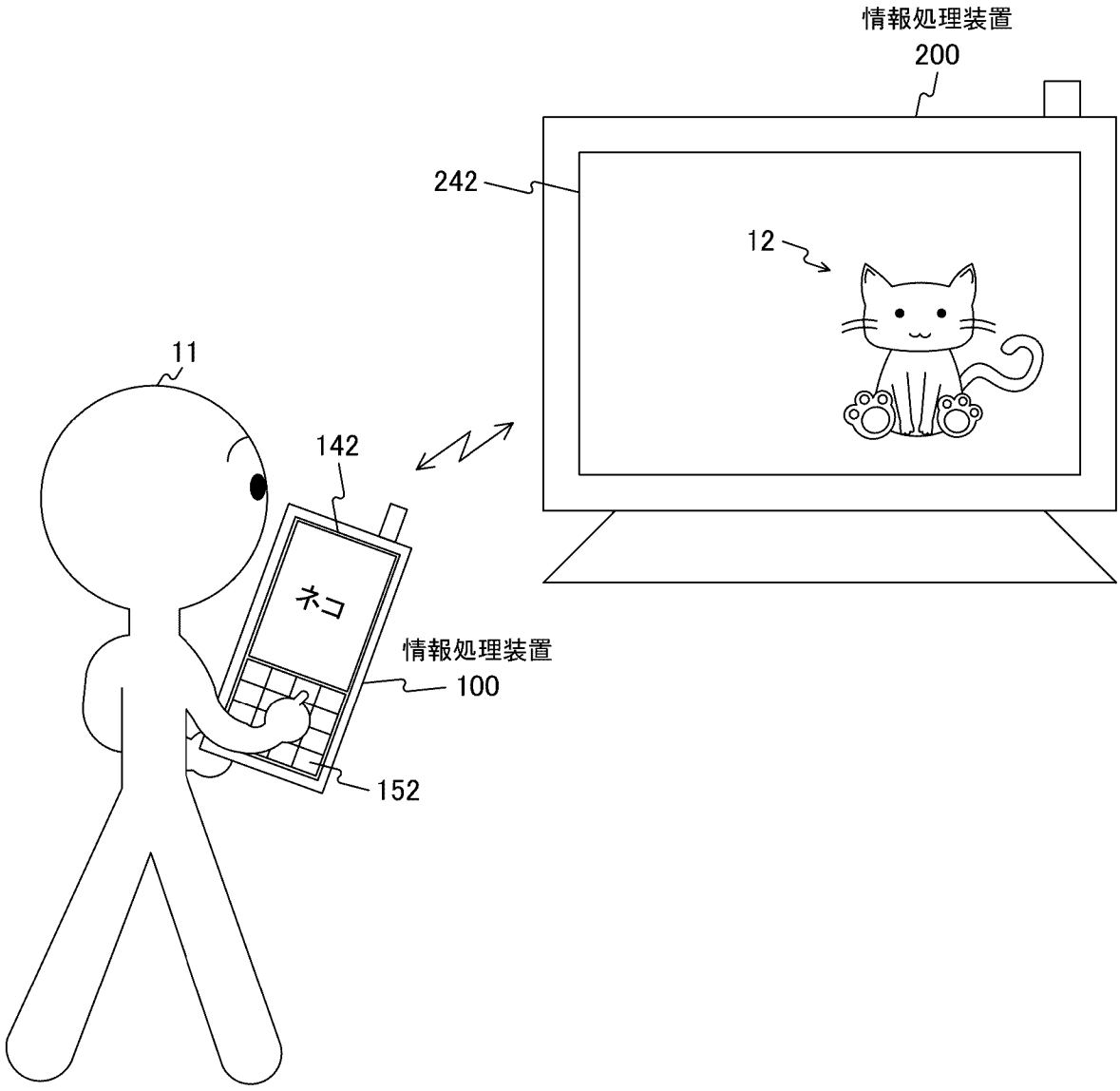
[請求項19] 無線通信を利用して第１情報処理装置から第２情報処理装置へのデータ送信を行うための前記第２情報処理装置への無線接続を前記第１

情報処理装置に許可するための認証鍵情報を前記第２情報処理装置から出力させる第１手順と、

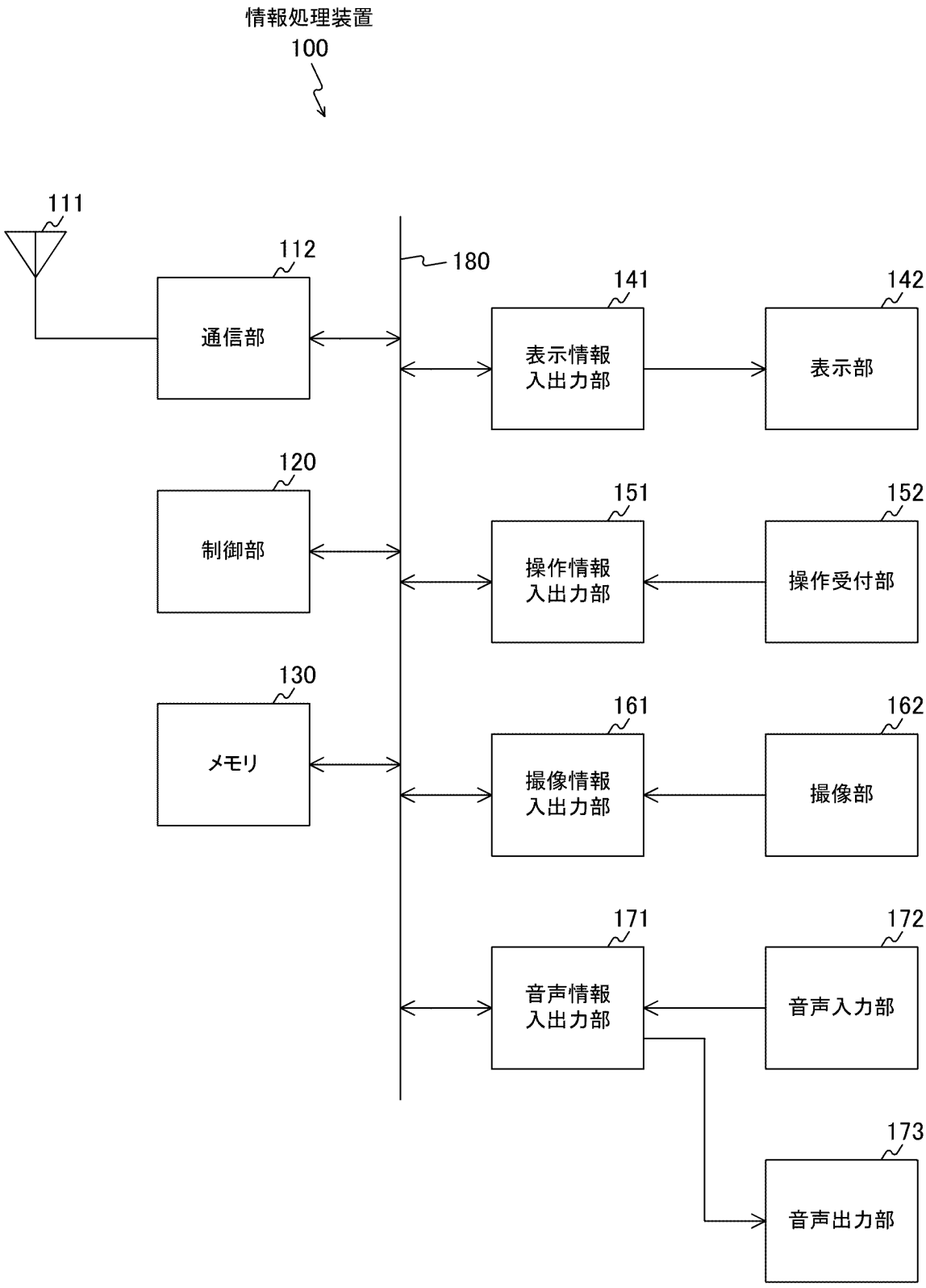
前記第１情報処理装置に入力された認証鍵情報と前記出力された認証鍵情報とに基づいて前記無線接続を前記第１情報処理装置に許可するかを決定する第２手順と

をコンピュータに実行させるプログラム。

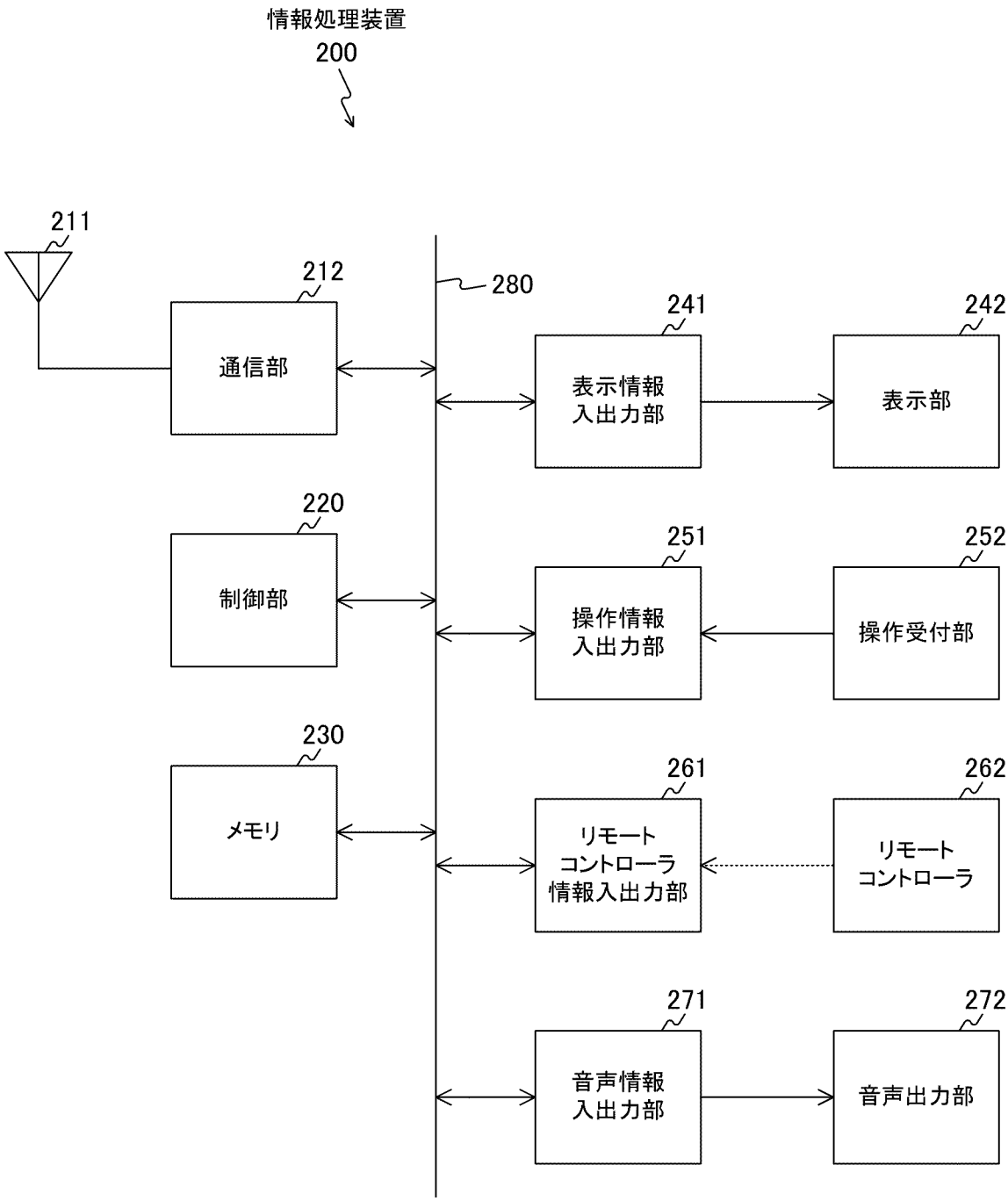
[図1]



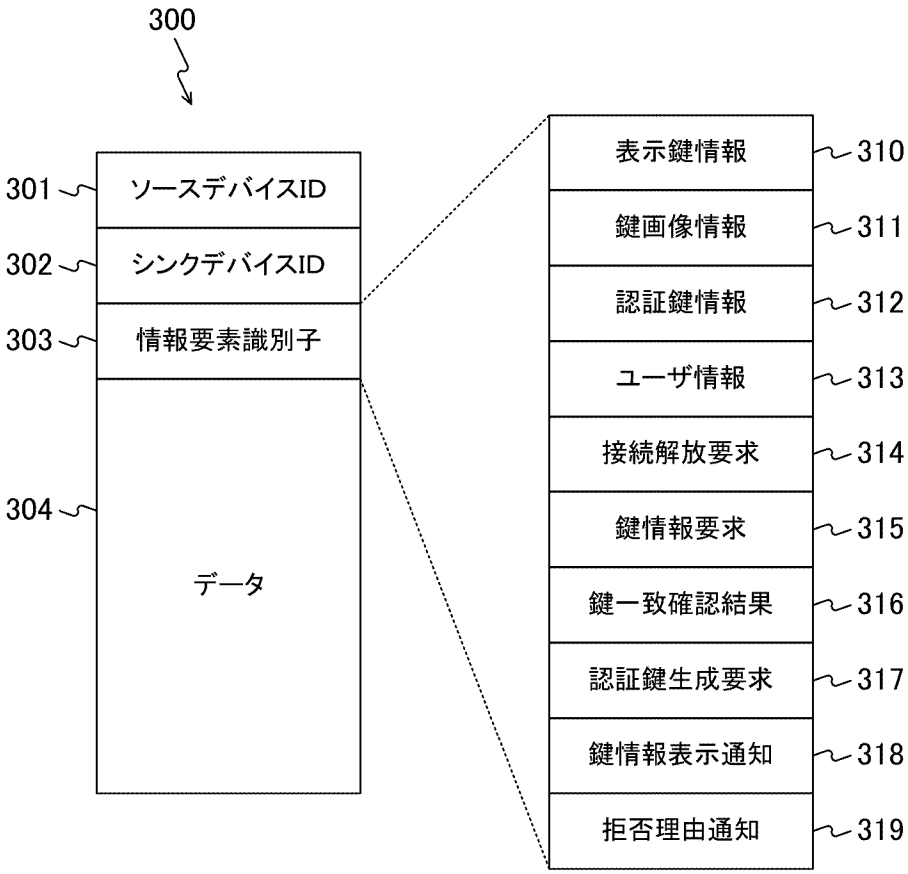
[図2]


情報処理装置
100
111
112
通信部
180
141
表示情報
入出力部
142
表示部
120
制御部
151
操作情報
入出力部
152
操作受付部
130
メモリ
161
撮像情報
入出力部
162
撮像部
171
音声情報
入出力部
172
音声入力部
173
音声出力部

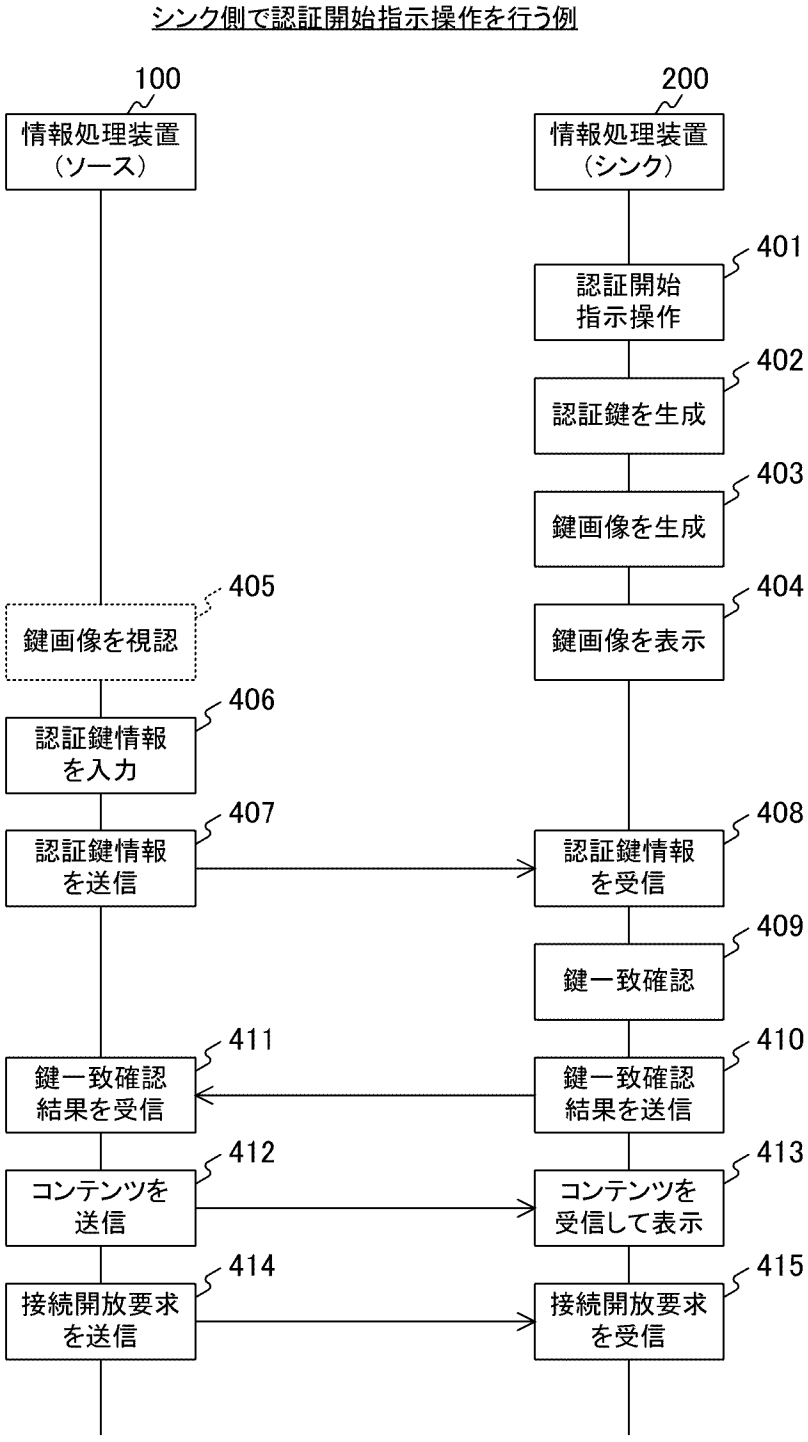
[図3]


情報処理装置
200
211
212
通信部
280
241
表示情報
入出力部
242
表示部
220
制御部
251
操作情報
入出力部
252
操作受付部
230
メモリ
261
リモート
コントローラ
情報入出力部
262
リモート
コントローラ
271
音声情報
入出力部
272
音声出力部

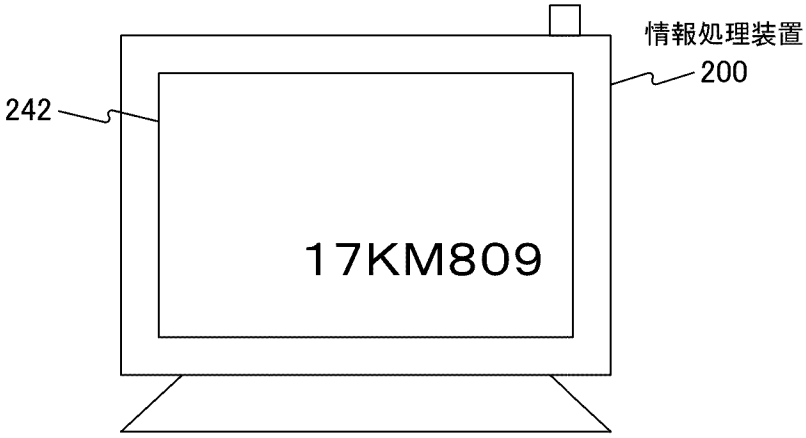
[図4]


300
301
ソースデバイスID
302
シンクデバイスID
303
情報要素識別子
304
データ
表示鍵情報
310
鍵画像情報
311
認証鍵情報
312
ユーザ情報
313
接続解放要求
314
鍵情報要求
315
鍵一致確認結果
316
認証鍵生成要求
317
鍵情報表示通知
318
拒否理由通知
319

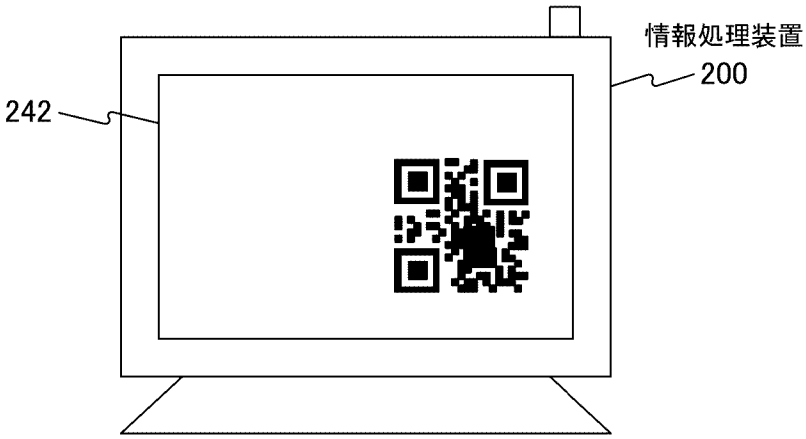
[図5]


シンク側で認証開始指示操作を行う例
100
情報処理装置
（ソース）
200
情報処理装置
（シンク）
401
認証開始
指示操作
402
認証鍵を生成
403
鍵画像を生成
404
鍵画像を表示
405
鍵画像を視認
406
認証鍵情報
を入力
407
認証鍵情報
を送信
408
認証鍵情報
を受信
409
鍵一致確認
410
鍵一致確認
結果を送信
411
鍵一致確認
結果を受信
412
コンテンツを
送信
413
コンテンツを
受信して表示
414
接続開放要求
を送信
415
接続開放要求
を受信

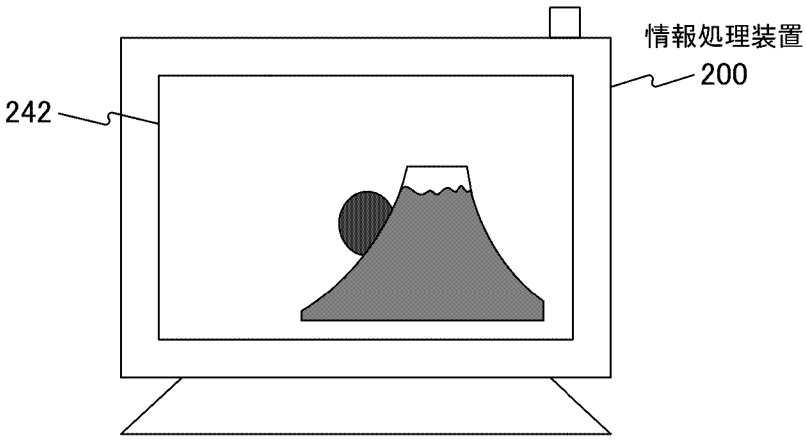
[図6]



a

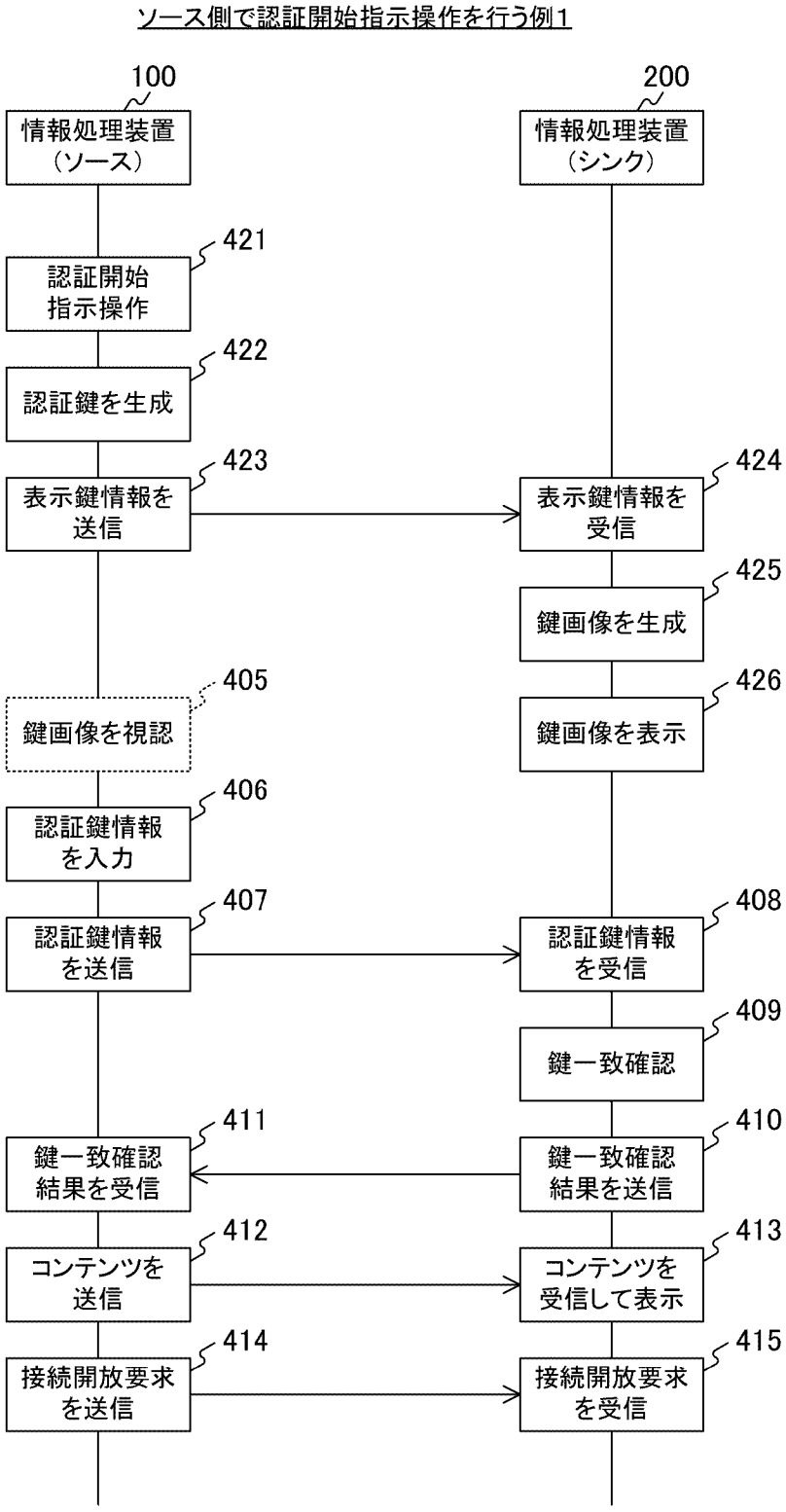


b

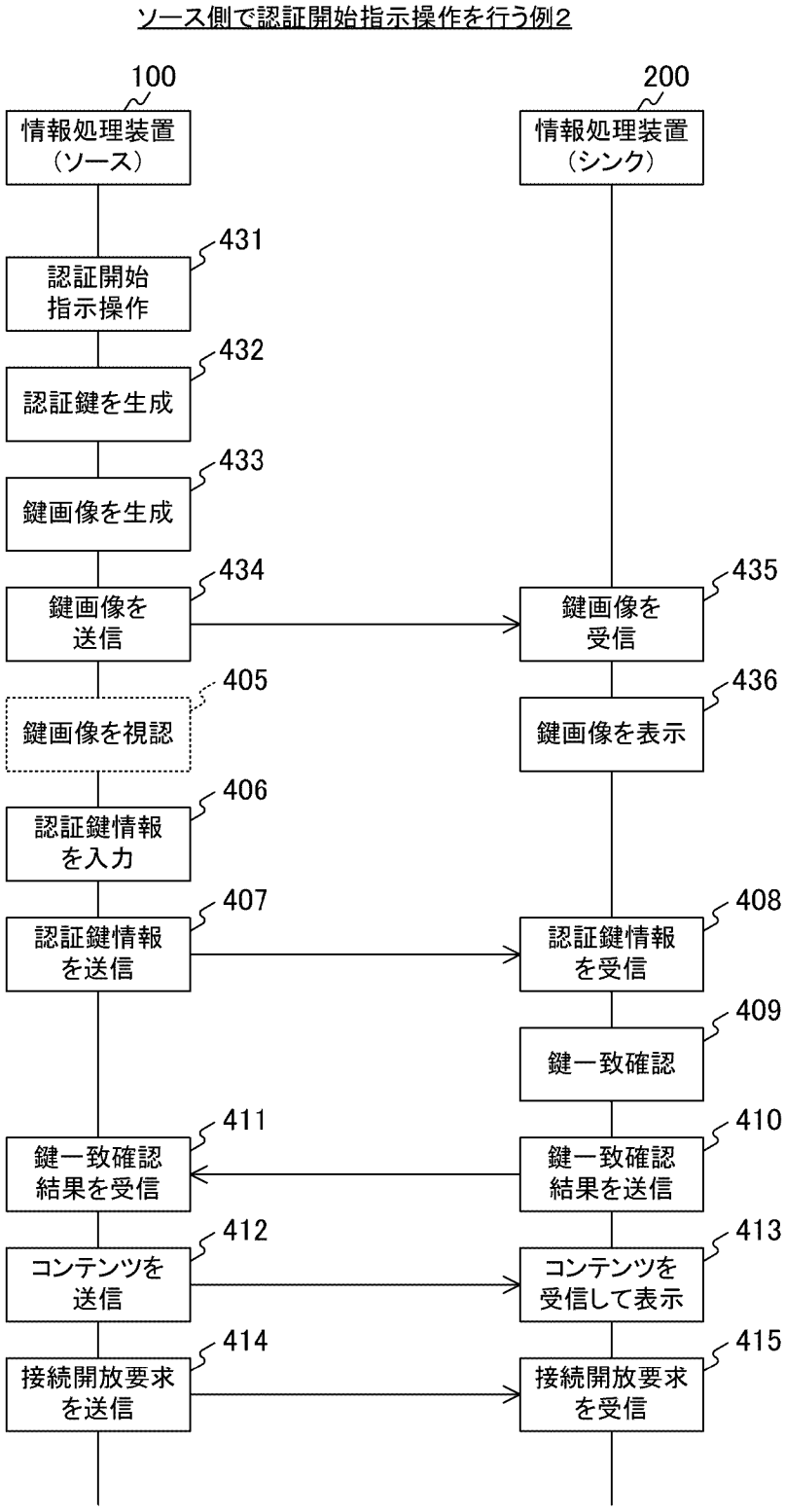


c

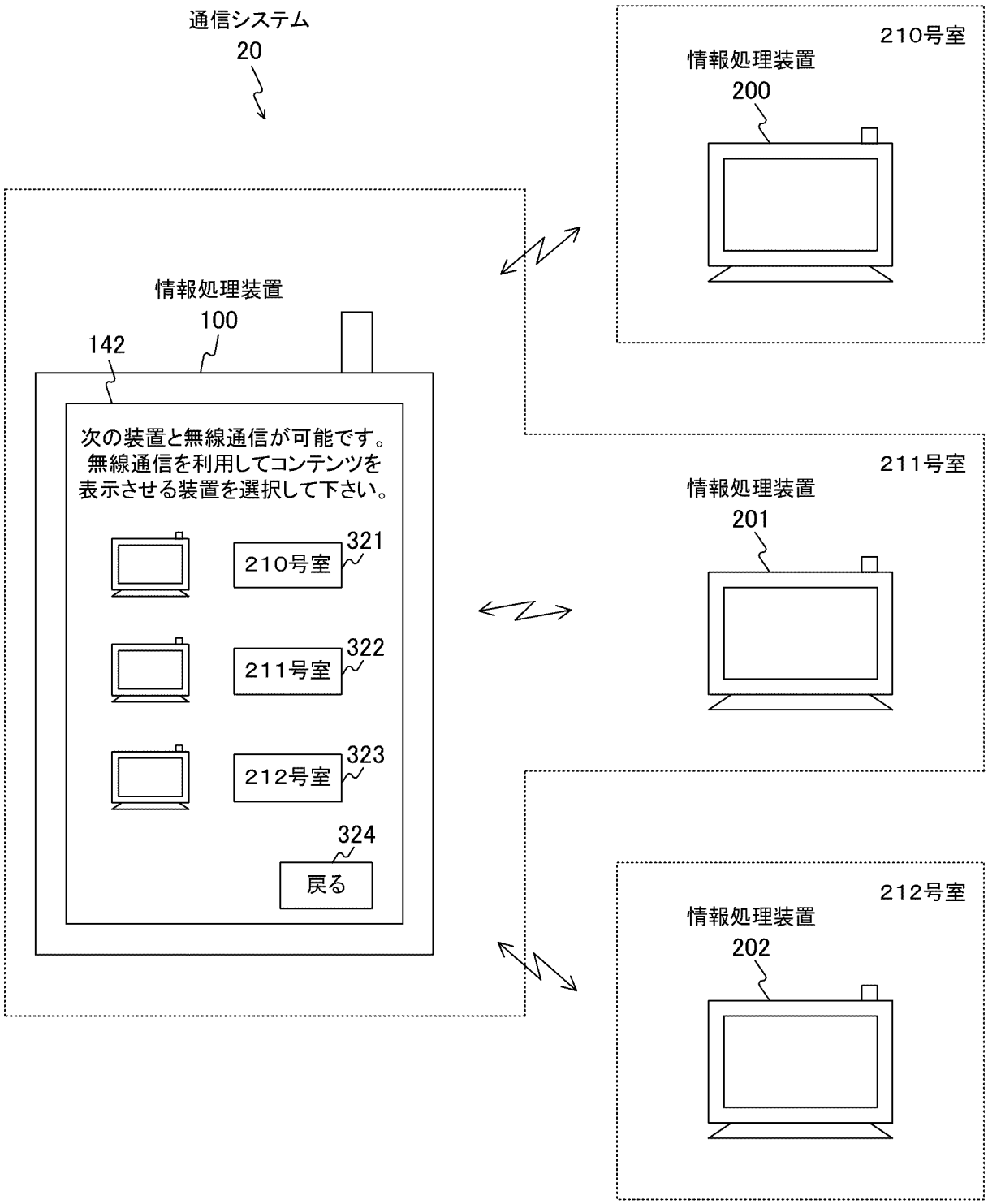
[図7]


ソース側で認証開始指示操作を行う例1
100
情報処理装置
（ソース）
200
情報処理装置
（シンク）
421
認証開始
指示操作
422
認証鍵を生成
423
表示鍵情報を
送信
424
表示鍵情報を
受信
425
鍵画像を生成
405
鍵画像を視認
426
鍵画像を表示
406
認証鍵情報
を入力
407
認証鍵情報
を送信
408
認証鍵情報
を受信
409
鍵一致確認
411
鍵一致確認
結果を受信
410
鍵一致確認
結果を送信
412
コンテンツを
送信
413
コンテンツを
受信して表示
414
接続開放要求
を送信
415
接続開放要求
を受信

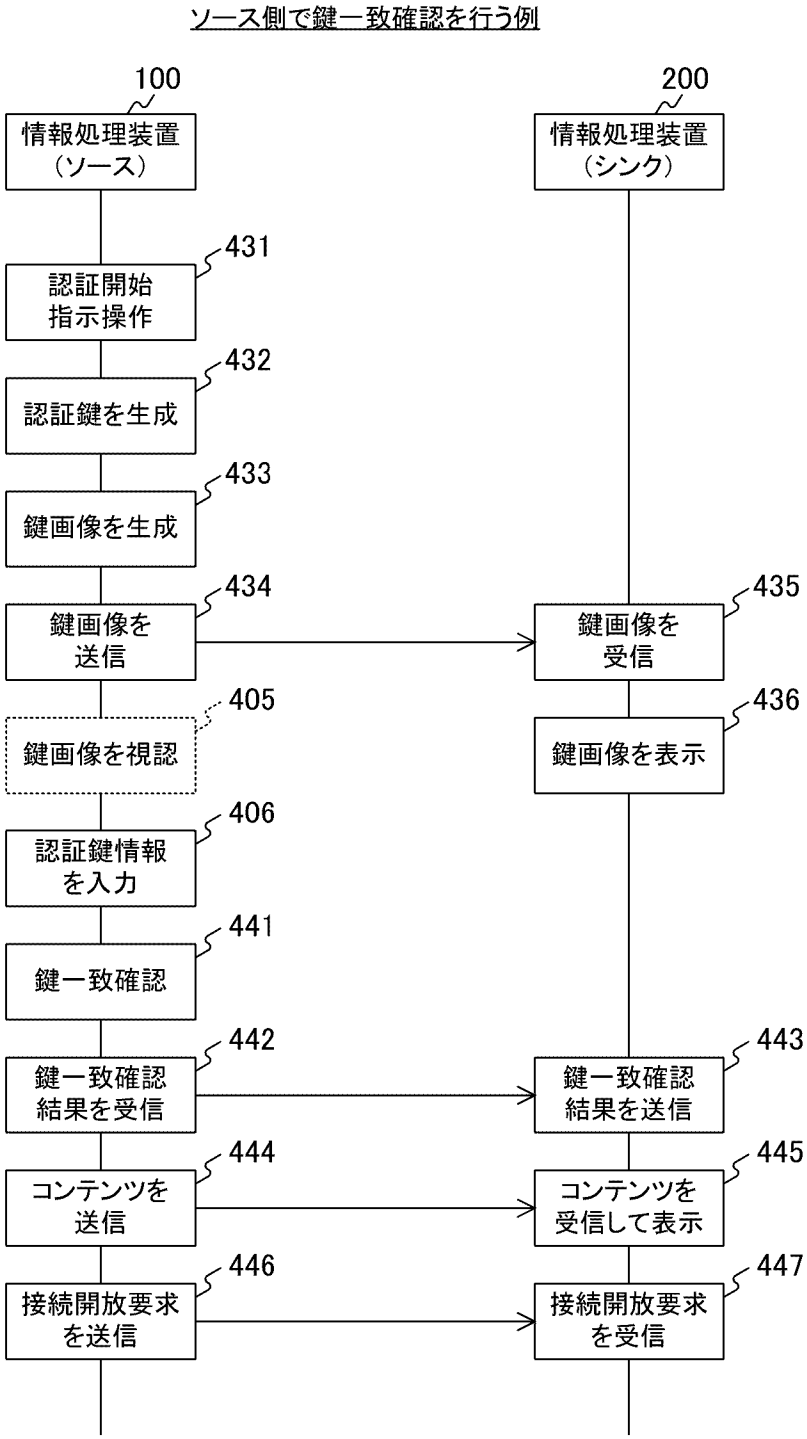
[図8]


ソース側で認証開始指示操作を行う例2
100
情報処理装置
（ソース）
200
情報処理装置
（シンク）
431
認証開始
指示操作
432
認証鍵を生成
433
鍵画像を生成
434
鍵画像を
送信
435
鍵画像を
受信
405
鍵画像を視認
436
鍵画像を表示
406
認証鍵情報
を入力
407
認証鍵情報
を送信
408
認証鍵情報
を受信
409
鍵一致確認
411
鍵一致確認
結果を受信
410
鍵一致確認
結果を送信
412
コンテンツを
送信
413
コンテンツを
受信して表示
414
接続開放要求
を送信
415
接続開放要求
を受信

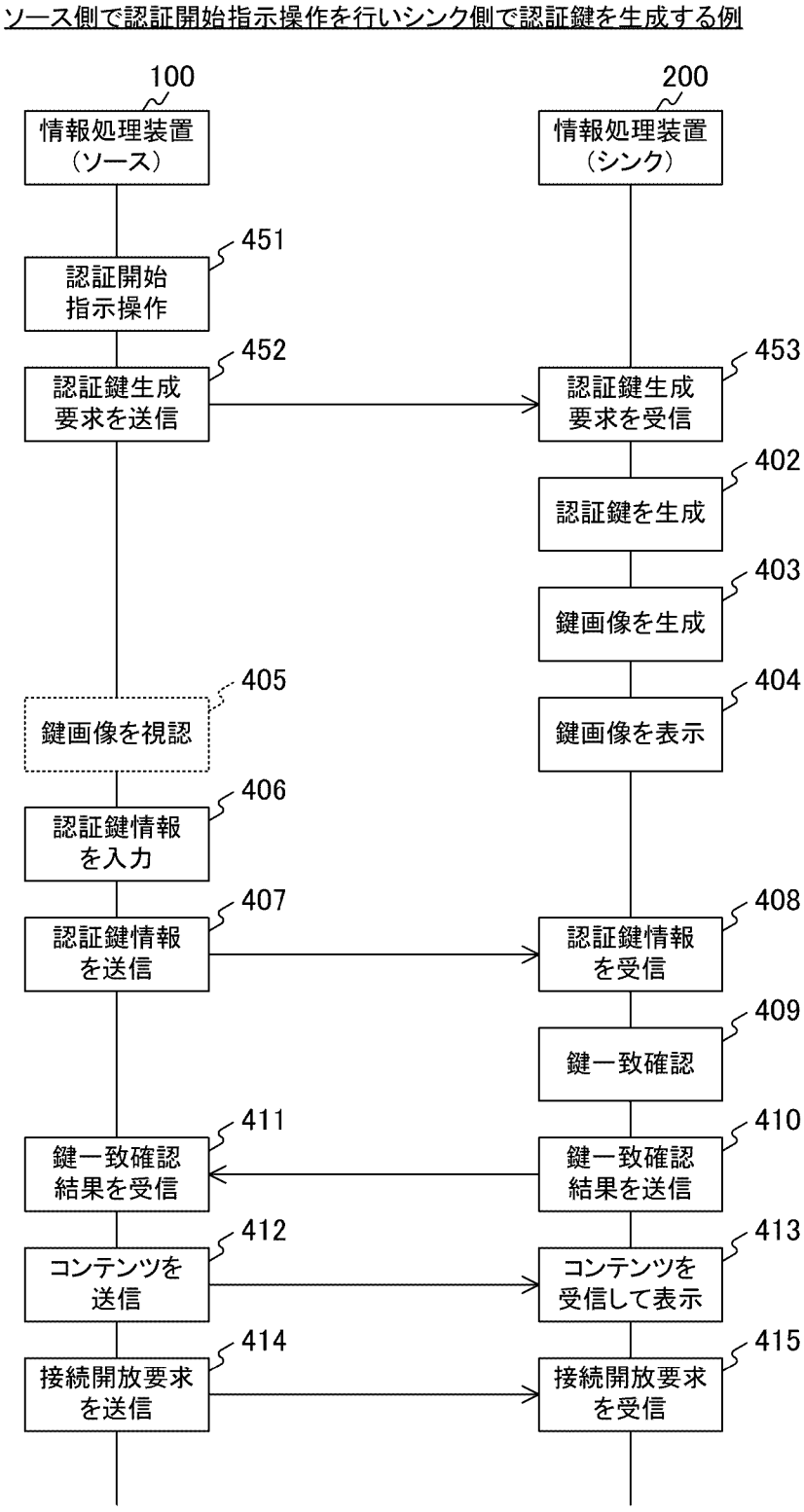
[図9]


通信システム
20
210号室
情報処理装置
200
情報処理装置
100
142
次の装置と無線通信が可能です。
無線通信を利用してコンテンツを
表示させる装置を選択して下さい。
210号室
321
211号室
322
212号室
323
324
戻る
211号室
情報処理装置
201
212号室
情報処理装置
202

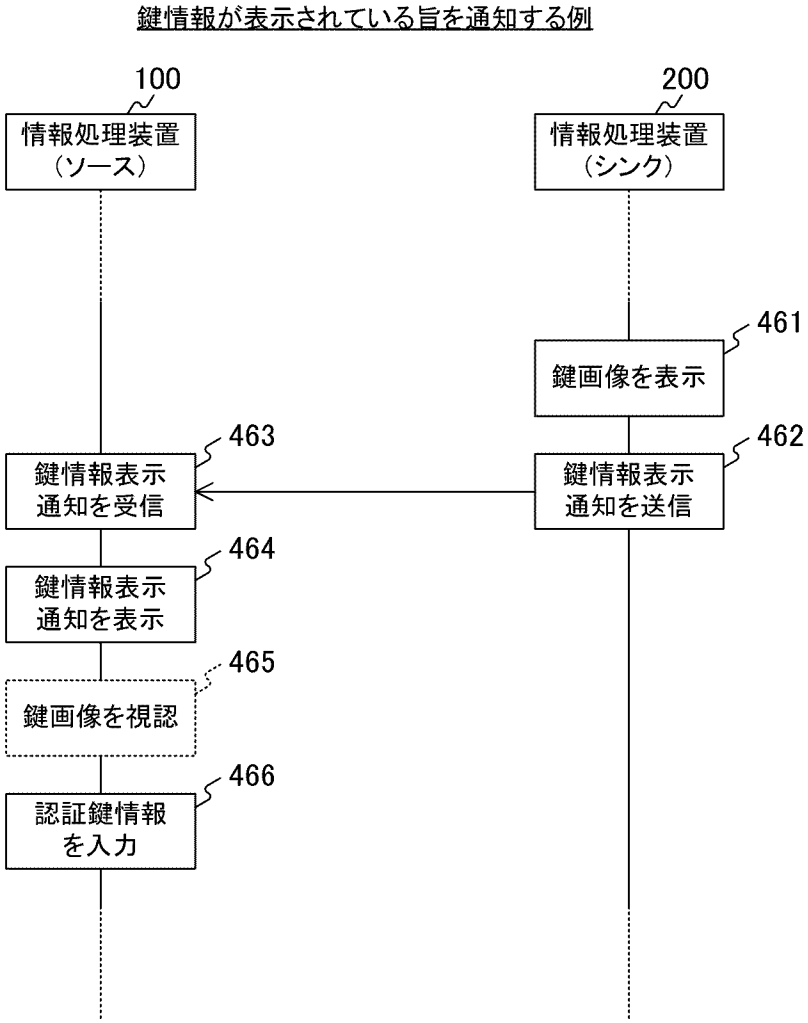
[図10]


ソース側で鍵一致確認を行う例
100
情報処理装置
（ソース）
200
情報処理装置
（シンク）
431
認証開始
指示操作
432
認証鍵を生成
433
鍵画像を生成
434
鍵画像を
送信
435
鍵画像を
受信
405
鍵画像を視認
436
鍵画像を表示
406
認証鍵情報
を入力
441
鍵一致確認
442
鍵一致確認
結果を受信
443
鍵一致確認
結果を送信
444
コンテンツを
送信
445
コンテンツを
受信して表示
446
接続開放要求
を送信
447
接続開放要求
を受信

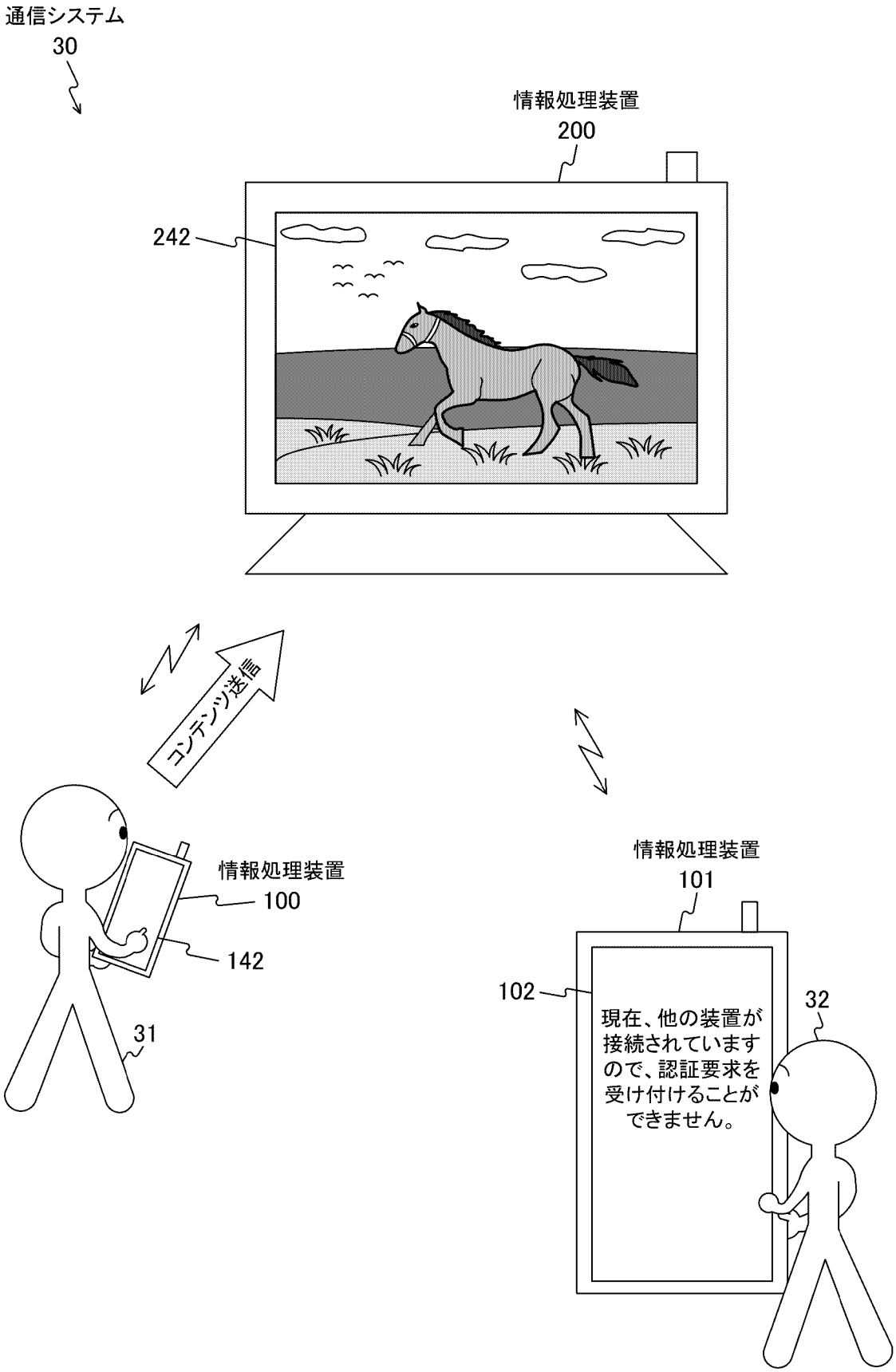
[図11]


ソース側で認証開始指示操作を行いシンク側で認証鍵を生成する例
100
情報処理装置
（ソース）
200
情報処理装置
（シンク）
451
認証開始
指示操作
452
認証鍵生成
要求を送信
453
認証鍵生成
要求を受信
402
認証鍵を生成
403
鍵画像を生成
405
鍵画像を視認
404
鍵画像を表示
406
認証鍵情報
を入力
407
認証鍵情報
を送信
408
認証鍵情報
を受信
409
鍵一致確認
411
鍵一致確認
結果を受信
410
鍵一致確認
結果を送信
412
コンテンツを
送信
413
コンテンツを
受信して表示
414
接続開放要求
を送信
415
接続開放要求
を受信

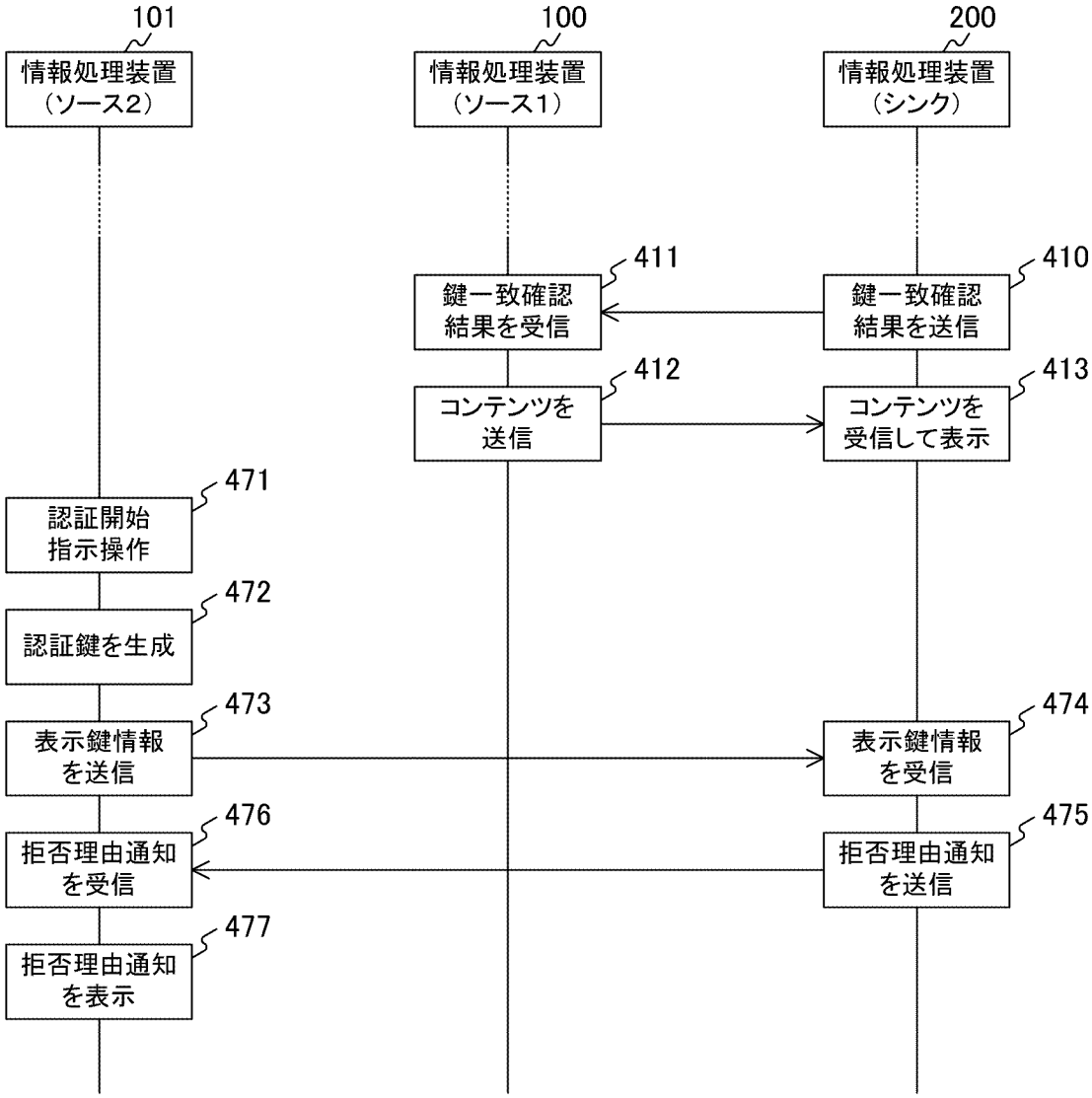
[図12]


鍵情報が表示されている旨を通知する例
100
情報処理装置
（ソース）
200
情報処理装置
（シンク）
461
鍵画像を表示
463
鍵情報表示
通知を受信
462
鍵情報表示
通知を送信
464
鍵情報表示
通知を表示
465
鍵画像を視認
466
認証鍵情報
を入力

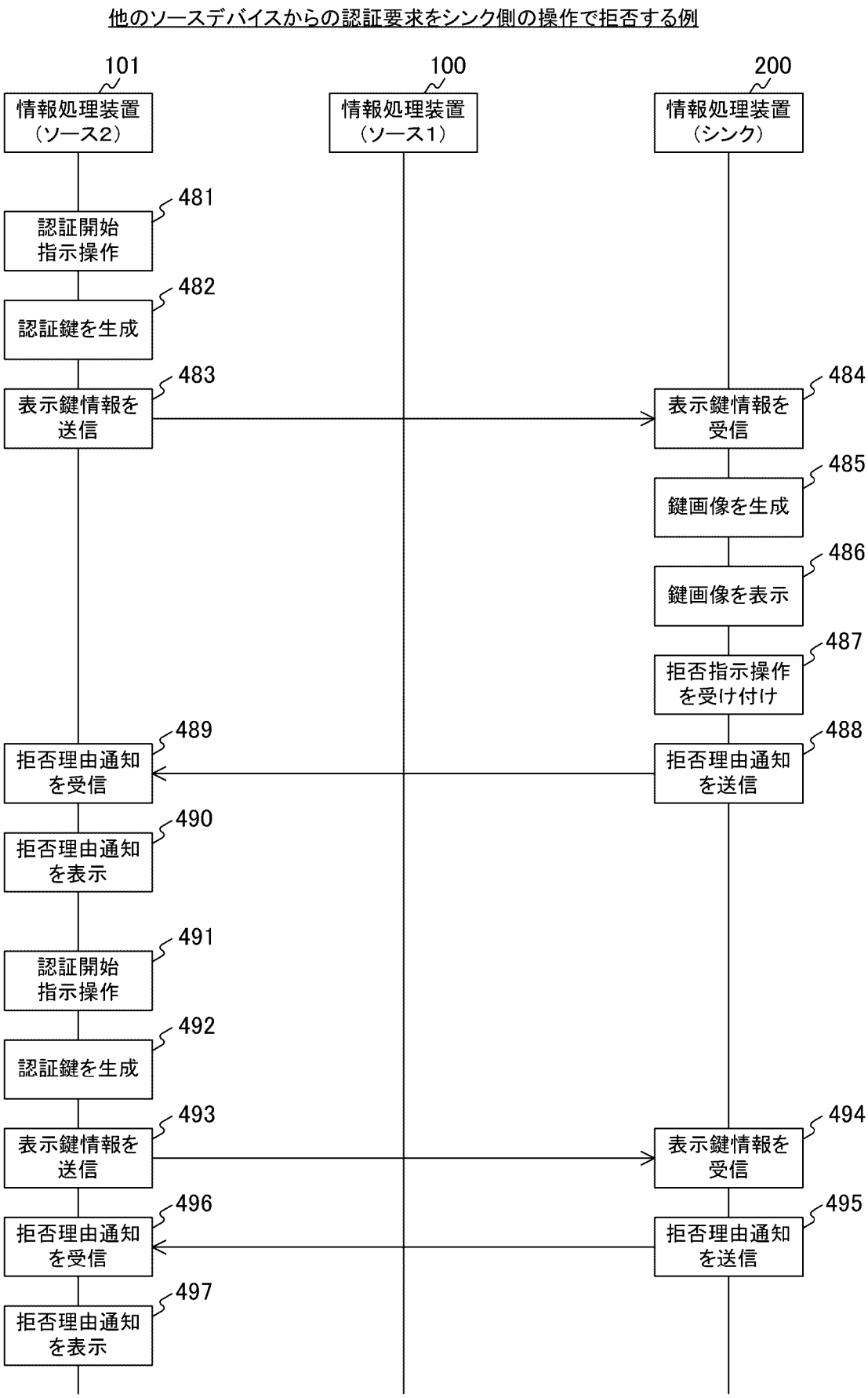
[図13]


通信システム
30
情報処理装置
200
242
コンテンツ送信
情報処理装置
100
142
31
情報処理装置
101
102
現在、他の装置が接続されていますので、認証要求を受け付けることができません。
32

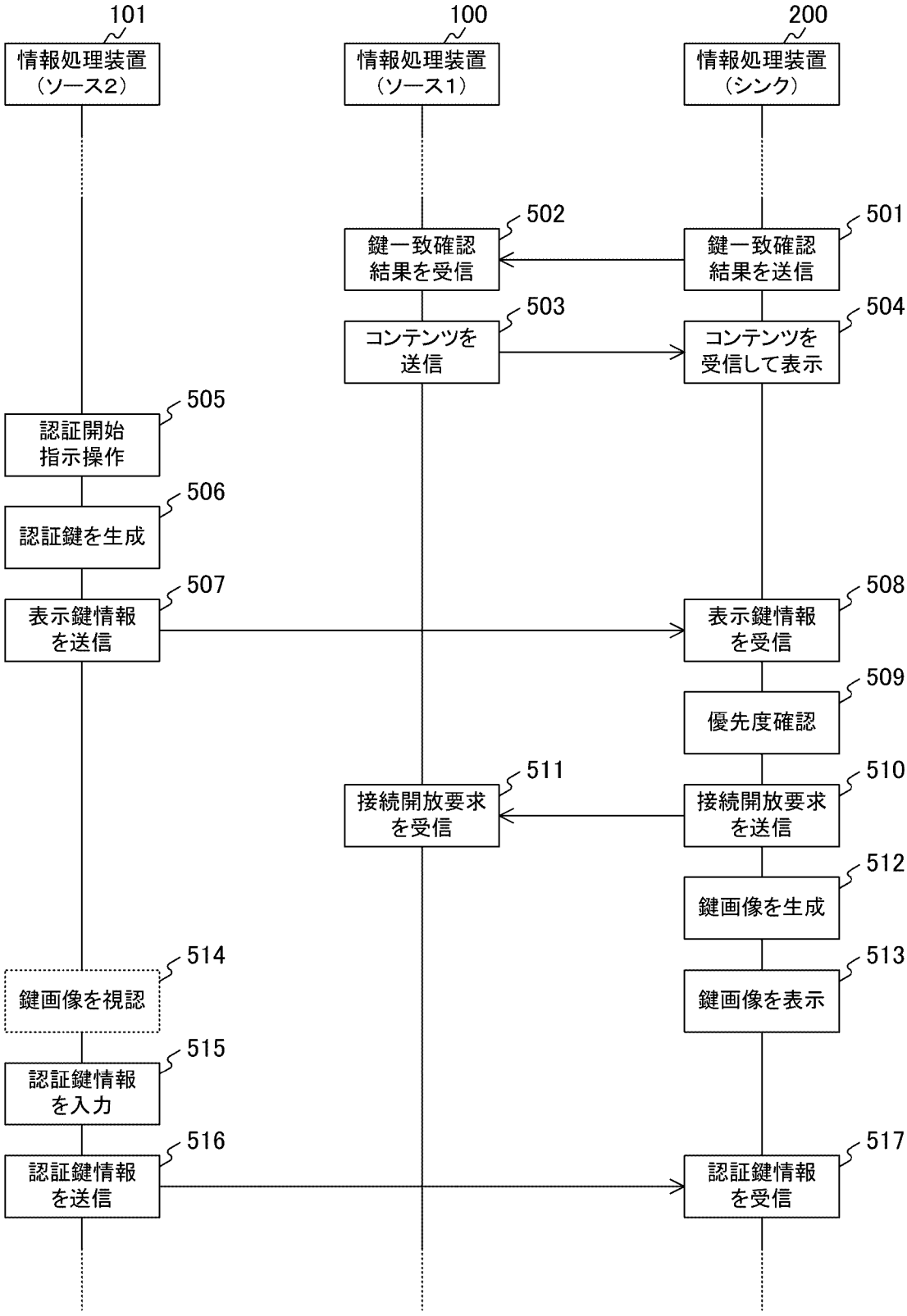
[図14]


他のソースデバイスからの認証要求を拒否する例
101
情報処理装置
（ソース2）
100
情報処理装置
（ソース1）
200
情報処理装置
（シンク）
411
鍵一致確認
結果を受信
410
鍵一致確認
結果を送信
412
コンテンツを
送信
413
コンテンツを
受信して表示
471
認証開始
指示操作
472
認証鍵を生成
473
表示鍵情報
を送信
474
表示鍵情報
を受信
476
拒否理由通知
を受信
475
拒否理由通知
を送信
477
拒否理由通知
を表示

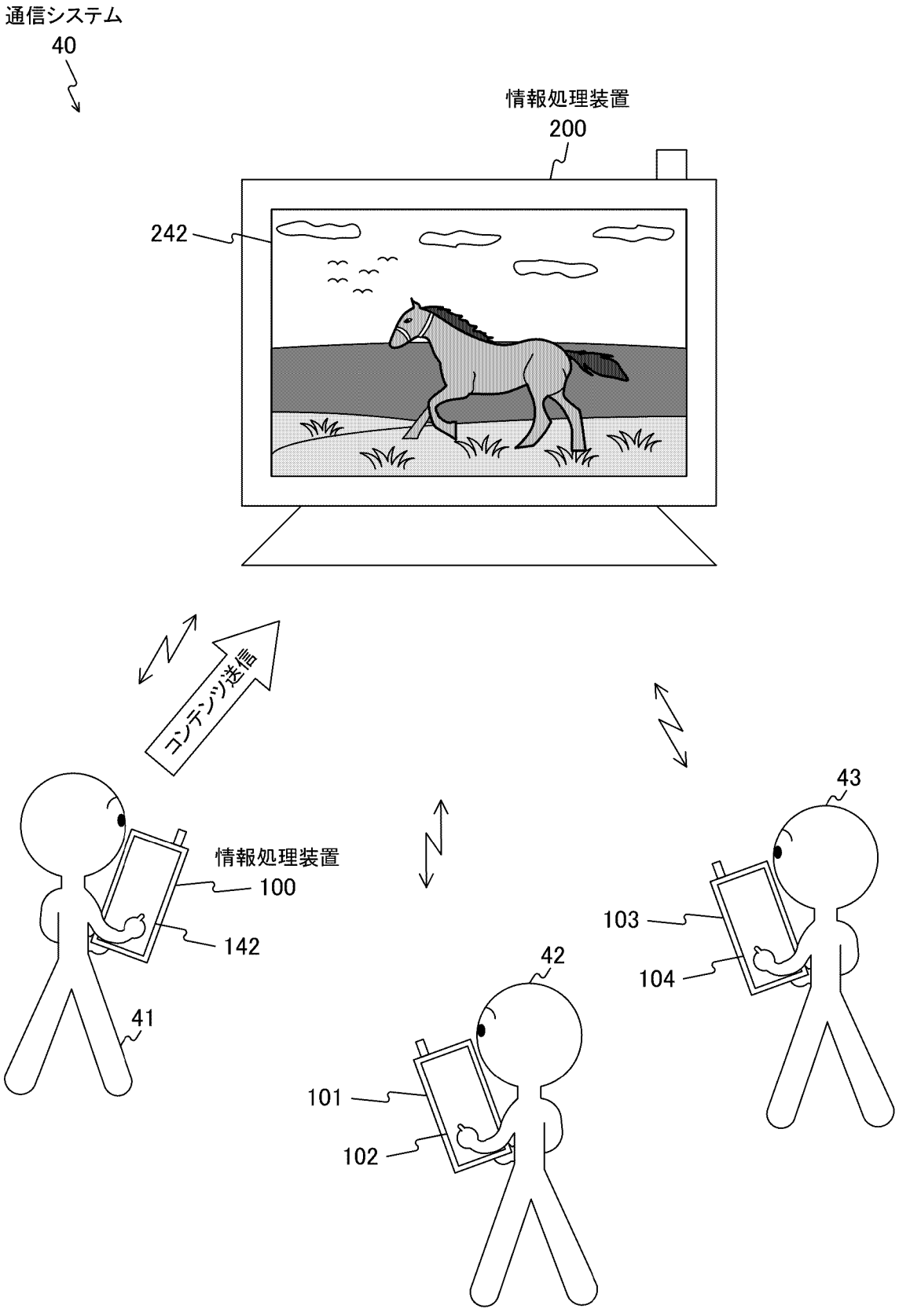
[図15]


他のソースデバイスからの認証要求をシンク側の操作で拒否する例
101
情報処理装置（ソース2）
100
情報処理装置（ソース1）
200
情報処理装置（シンク）
481
認証開始指示操作
482
認証鍵を生成
483
表示鍵情報を送信
484
表示鍵情報を受信
485
鍵画像を生成
486
鍵画像を表示
487
拒否指示操作を受け付け
488
拒否理由通知を送信
489
拒否理由通知を受信
490
拒否理由通知を表示
491
認証開始指示操作
492
認証鍵を生成
493
表示鍵情報を送信
494
表示鍵情報を受信
495
拒否理由通知を送信
496
拒否理由通知を受信
497
拒否理由通知を表示

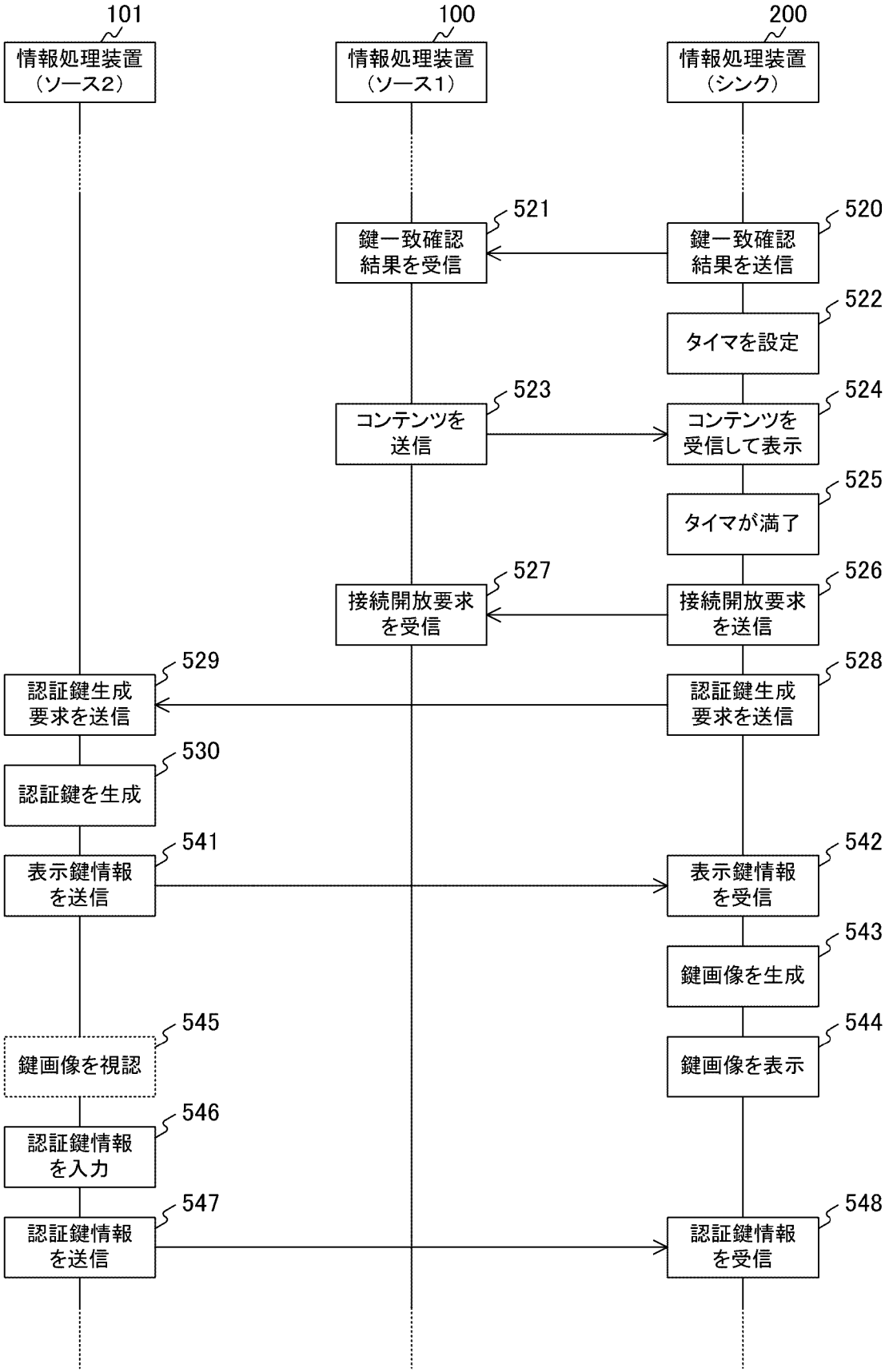
[図16]


他のソースデバイスからの認証要求の受付の要否を優先度を用いて判断する例
101
情報処理装置
（ソース2）
100
情報処理装置
（ソース1）
200
情報処理装置
（シンク）
502
鍵一致確認
結果を受信
501
鍵一致確認
結果を送信
503
コンテンツを
送信
504
コンテンツを
受信して表示
505
認証開始
指示操作
506
認証鍵を生成
507
表示鍵情報
を送信
508
表示鍵情報
を受信
509
優先度確認
511
接続開放要求
を受信
510
接続開放要求
を送信
512
鍵画像を生成
514
鍵画像を視認
513
鍵画像を表示
515
認証鍵情報
を入力
516
認証鍵情報
を送信
517
認証鍵情報
を受信

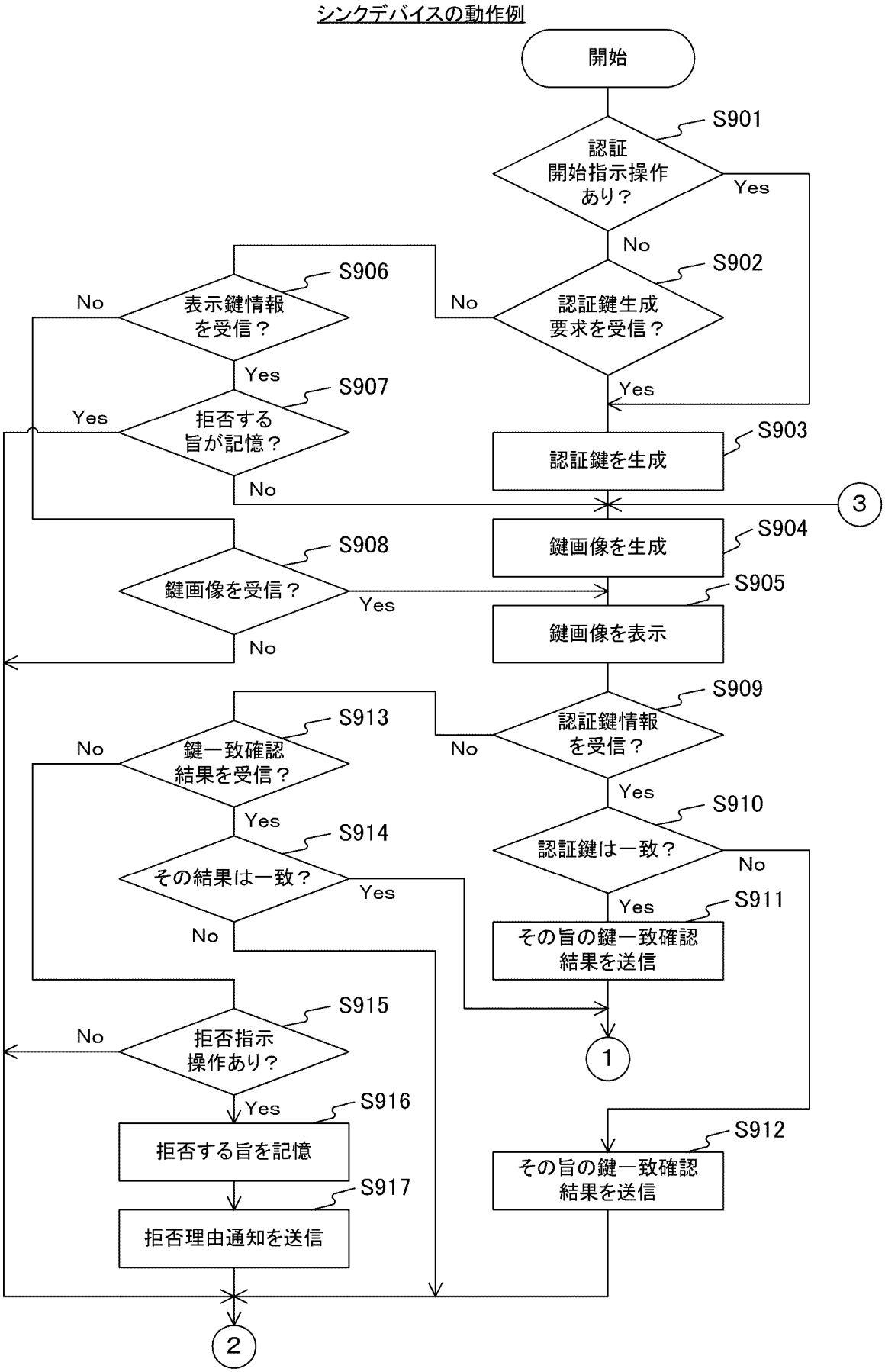
[図17]


通信システム
40
情報処理装置
200
242
コンテンツ送信
情報処理装置
100
142
41
43
103
104
42
101
102

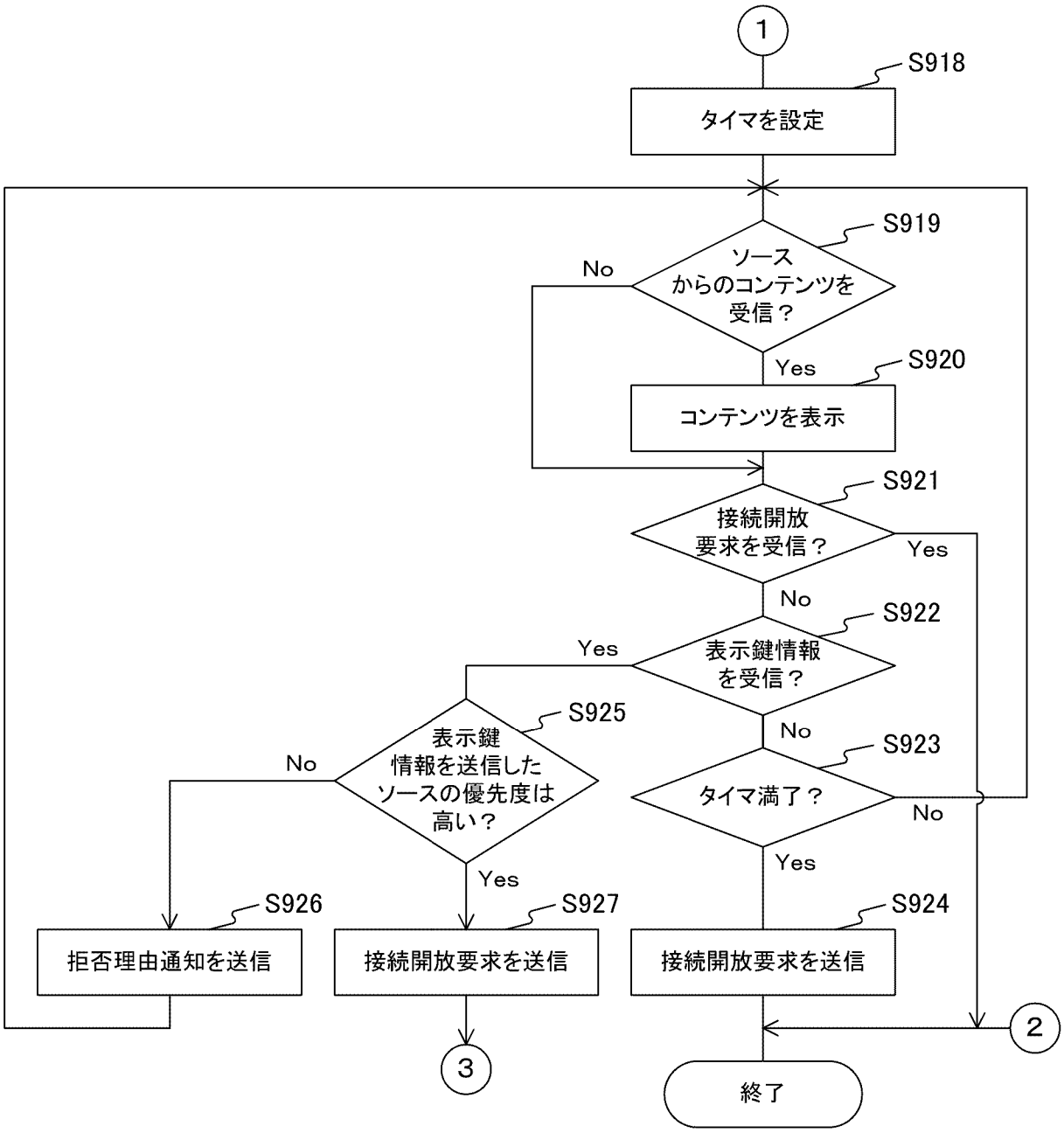
[図18]


複数のソースデバイスの接続権を所定間隔で切り替える例
101
情報処理装置
（ソース2）
100
情報処理装置
（ソース1）
200
情報処理装置
（シンク）
521
鍵一致確認
結果を受信
520
鍵一致確認
結果を送信
522
タイマを設定
523
コンテンツを
送信
524
コンテンツを
受信して表示
525
タイマが満了
527
接続開放要求
を受信
526
接続開放要求
を送信
529
認証鍵生成
要求を送信
528
認証鍵生成
要求を送信
530
認証鍵を生成
541
表示鍵情報
を送信
542
表示鍵情報
を受信
543
鍵画像を生成
545
鍵画像を視認
544
鍵画像を表示
546
認証鍵情報
を入力
547
認証鍵情報
を送信
548
認証鍵情報
を受信

[図19]

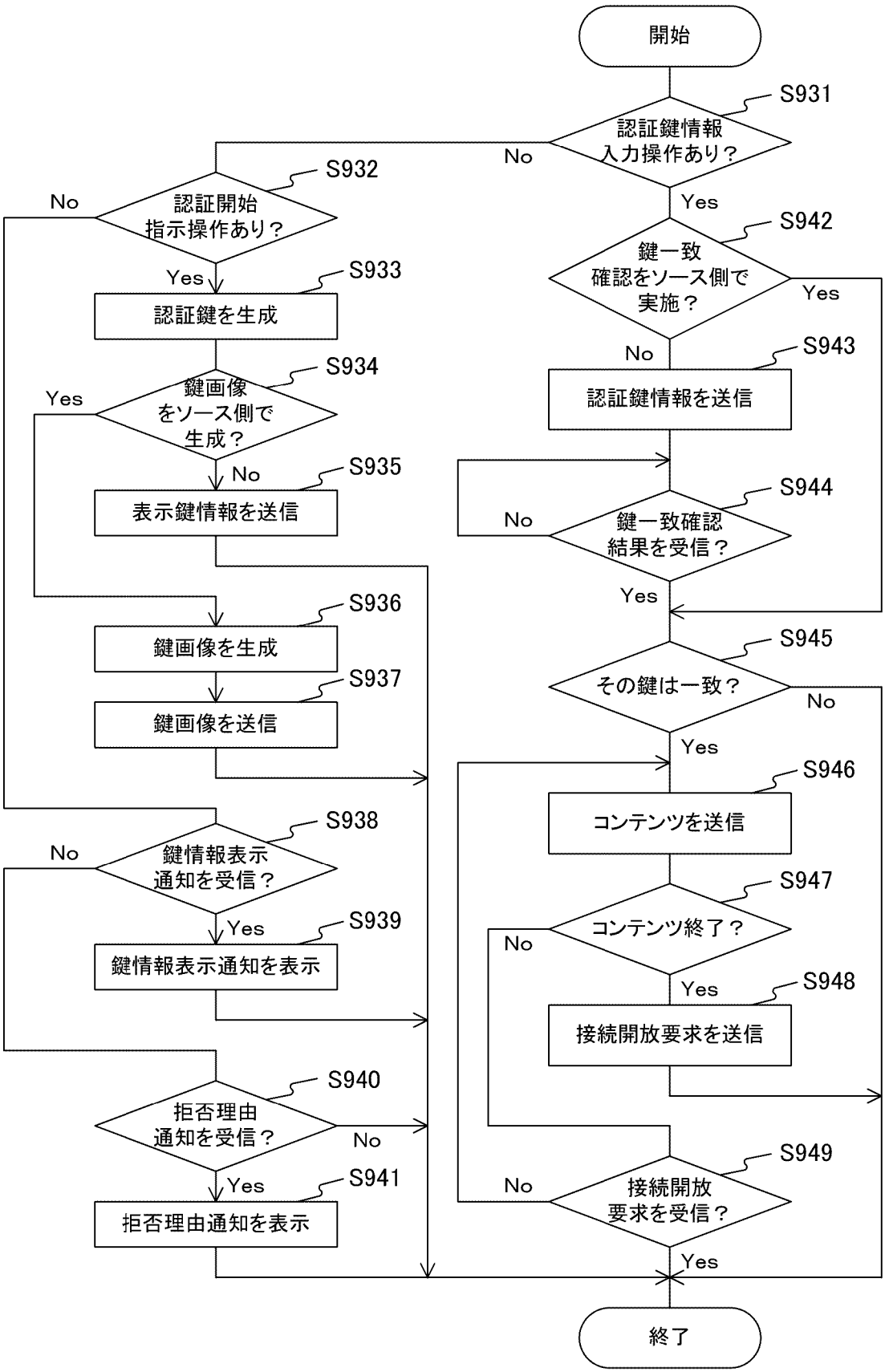

シンクデバイスの動作例
開始
S901
認証
開始指示操作
あり？
Yes
No
S902
認証鍵生成
要求を受信？
No
Yes
S903
認証鍵を生成
3
S904
鍵画像を生成
S905
鍵画像を表示
S906
表示鍵情報
を受信？
No
Yes
S907
拒否する
旨が記憶？
Yes
No
S908
鍵画像を受信？
Yes
No
S909
認証鍵情報
を受信？
No
Yes
S910
認証鍵は一致？
No
Yes
S911
その旨の鍵一致確認
結果を送信
1
S912
その旨の鍵一致確認
結果を送信
S913
鍵一致確認
結果を受信？
No
Yes
S914
その結果は一致？
Yes
No
S915
拒否指示
操作あり？
No
Yes
S916
拒否する旨を記憶
S917
拒否理由通知を送信
2

[図20]

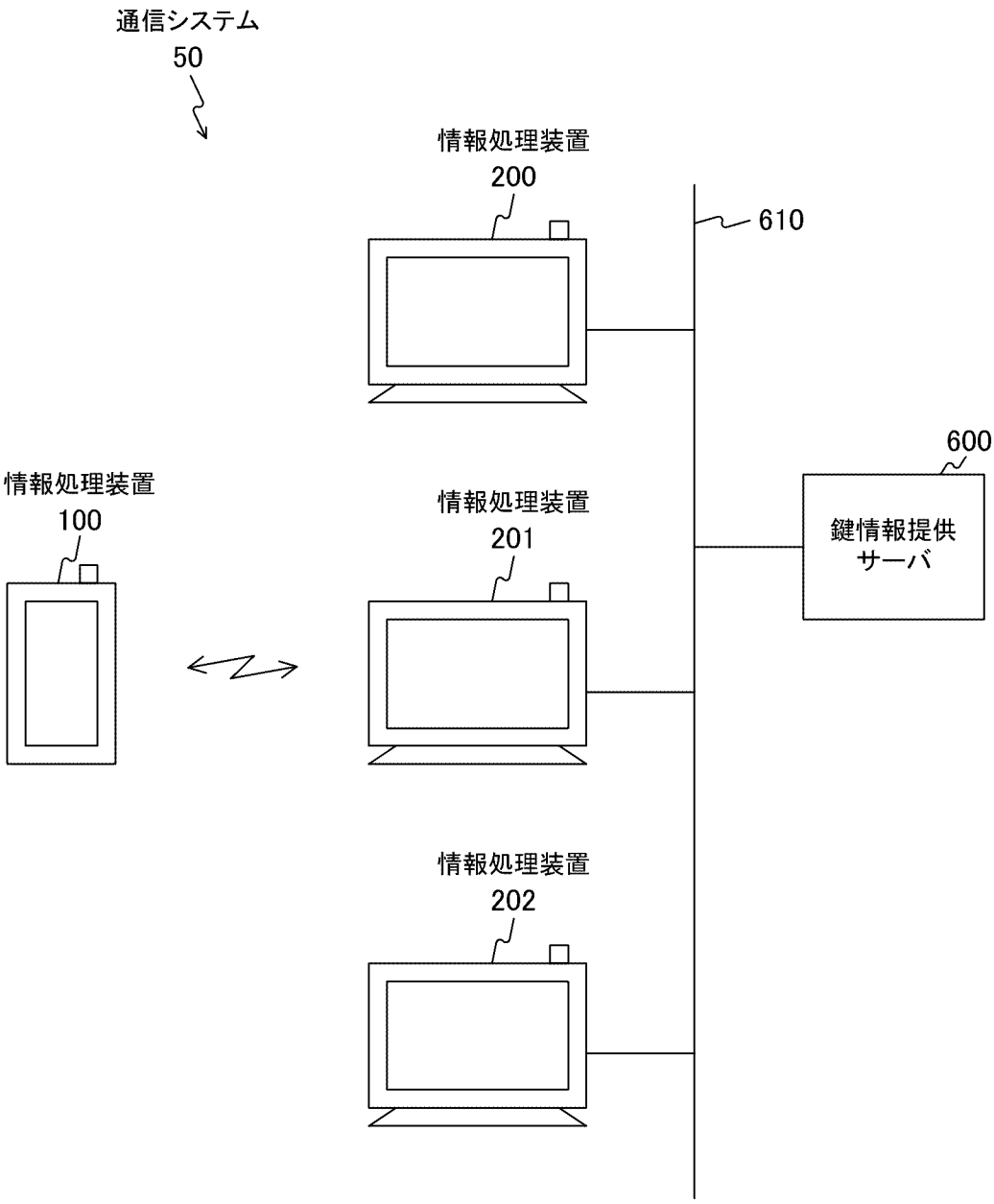

1
S918
タイマを設定
S919
ソース
からのコンテンツを
受信？
No
Yes
S920
コンテンツを表示
S921
接続開放
要求を受信？
Yes
No
S922
表示鍵情報
を受信？
Yes
No
S925
表示鍵
情報を送信した
ソースの優先度は
高い？
No
Yes
S923
タイマ満了？
No
Yes
S926
拒否理由通知を送信
S927
接続開放要求を送信
S924
接続開放要求を送信
2
3
終了

[図21]

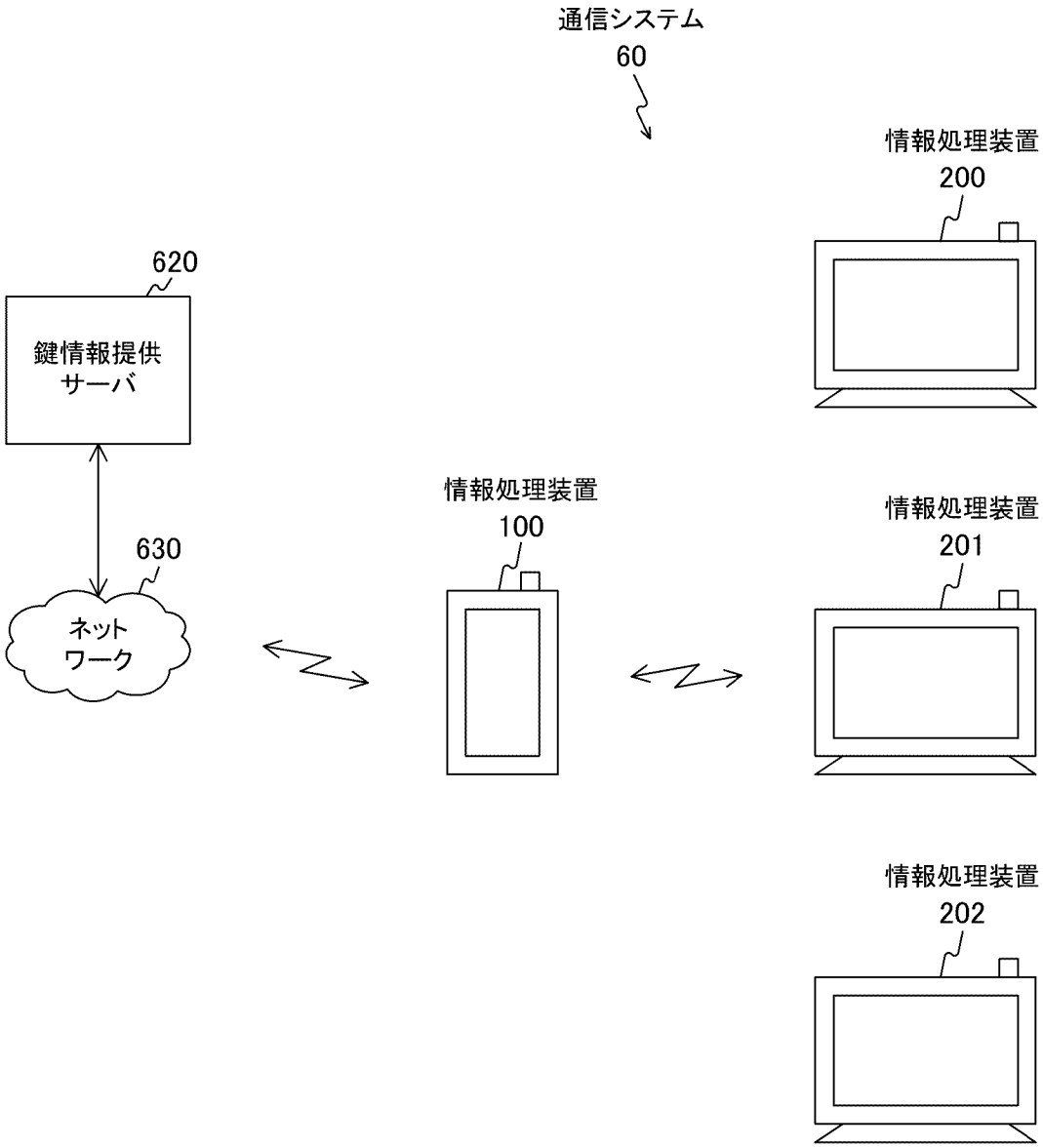
ソースデバイスの動作例



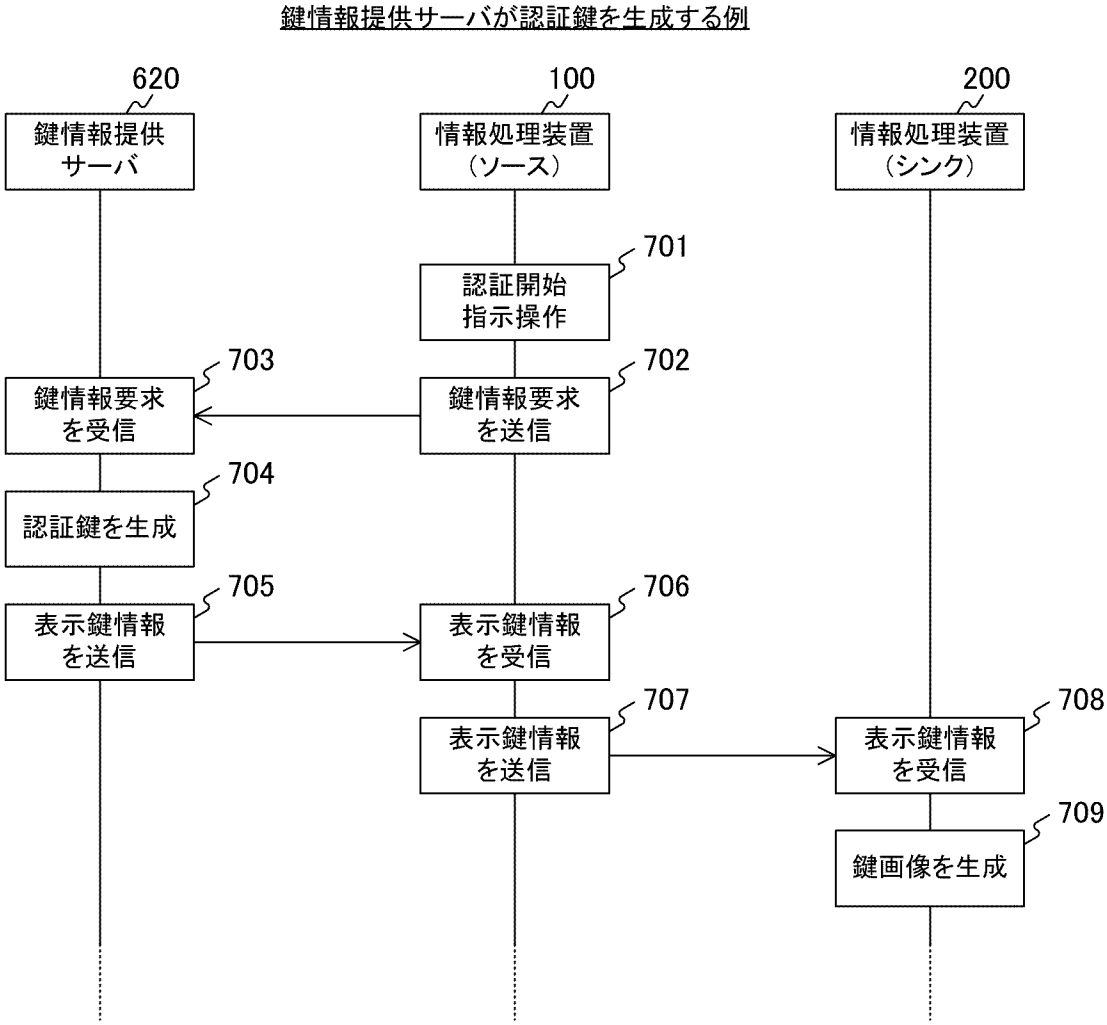
[図22]


通信システム
50
情報処理装置
200
610
600
鍵情報提供
サーバ
情報処理装置
100
情報処理装置
201
情報処理装置
202

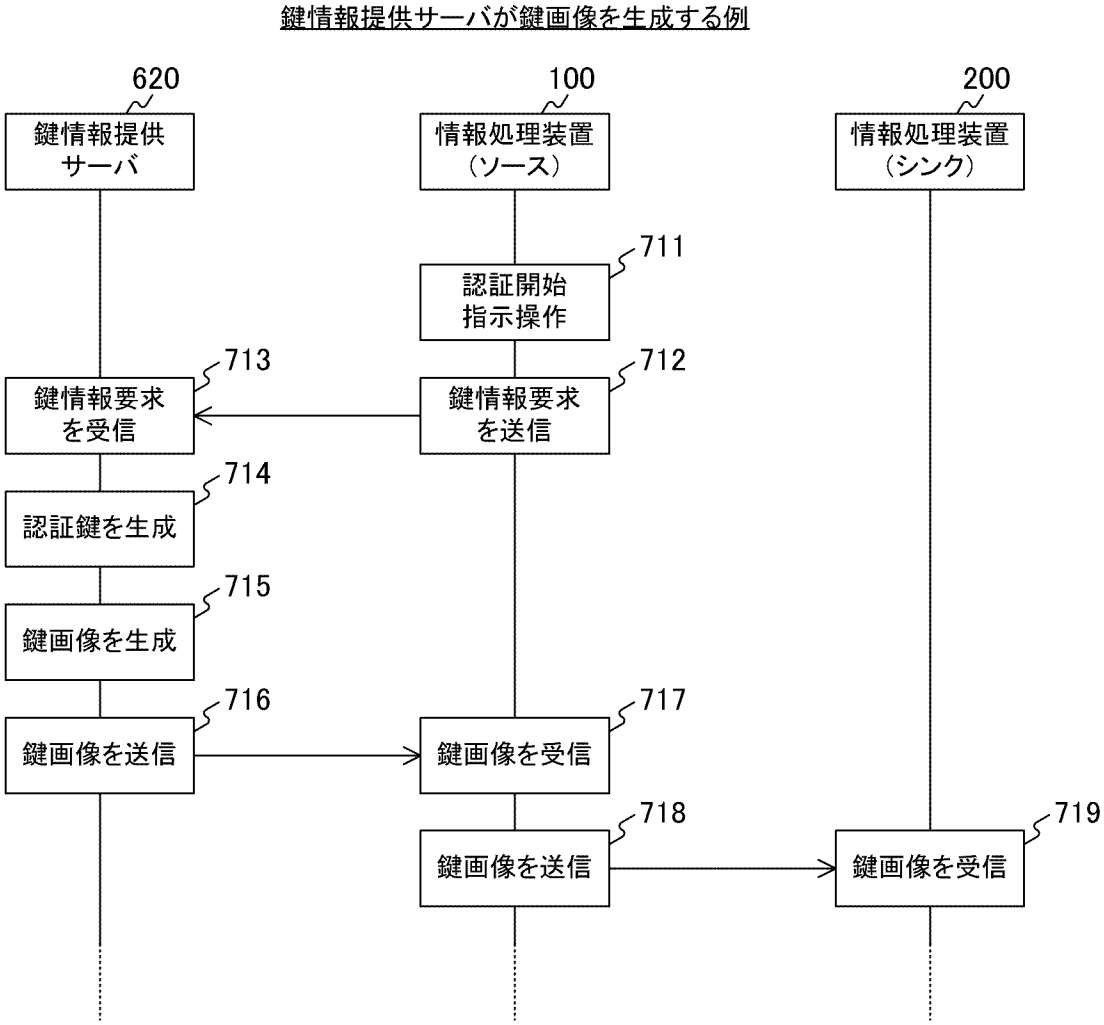
[図23]


通信システム
60
情報処理装置
200
620
鍵情報提供
サーバ
630
ネット
ワーク
情報処理装置
100
情報処理装置
201
情報処理装置
202

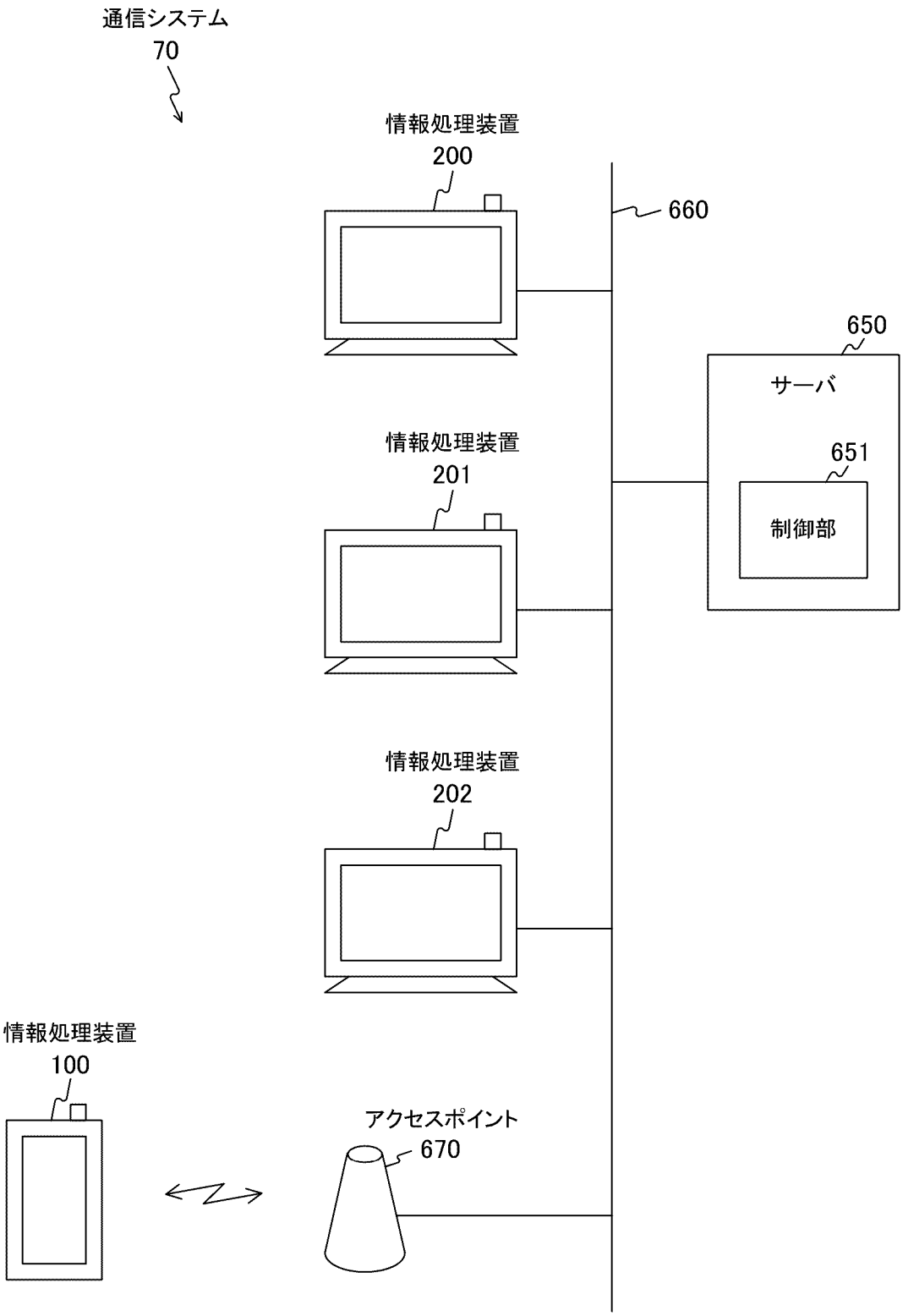
[図24]


鍵情報提供サーバが認証鍵を生成する例
620
鍵情報提供サーバ
100
情報処理装置（ソース）
200
情報処理装置（シンク）
701
認証開始指示操作
703
鍵情報要求を受信
702
鍵情報要求を送信
704
認証鍵を生成
705
表示鍵情報を送信
706
表示鍵情報を受信
707
表示鍵情報を送信
708
表示鍵情報を受信
709
鍵画像を生成

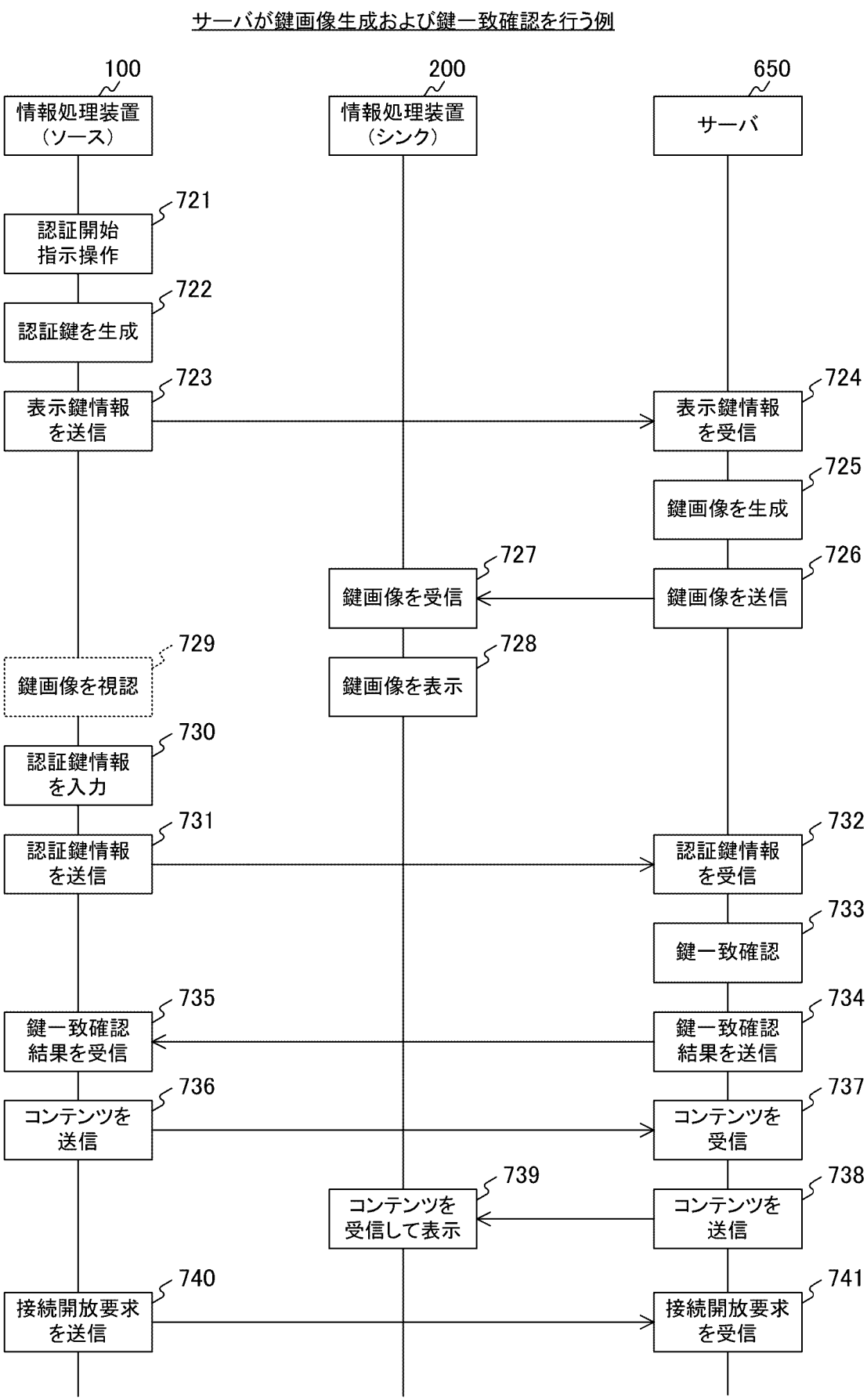
[図25]


鍵情報提供サーバが鍵画像を生成する例
620
鍵情報提供サーバ
100
情報処理装置（ソース）
200
情報処理装置（シンク）
711
認証開始指示操作
712
鍵情報要求を送信
713
鍵情報要求を受信
714
認証鍵を生成
715
鍵画像を生成
716
鍵画像を送信
717
鍵画像を受信
718
鍵画像を送信
719
鍵画像を受信

[図26]


通信システム
70
情報処理装置
200
660
650
サーバ
651
制御部
情報処理装置
201
情報処理装置
202
情報処理装置
100
アクセスポイント
670

[図27]


サーバが鍵画像生成および鍵一致確認を行う例
100
情報処理装置（ソース）
200
情報処理装置（シンク）
650
サーバ
721
認証開始指示操作
722
認証鍵を生成
723
表示鍵情報を送信
724
表示鍵情報を受信
725
鍵画像を生成
726
鍵画像を送信
727
鍵画像を受信
728
鍵画像を表示
729
鍵画像を視認
730
認証鍵情報を入力
731
認証鍵情報を送信
732
認証鍵情報を受信
733
鍵一致確認
734
鍵一致確認結果を送信
735
鍵一致確認結果を受信
736
コンテンツを送信
737
コンテンツを受信
738
コンテンツを送信
739
コンテンツを受信して表示
740
接続開放要求を送信
741
接続開放要求を受信

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/082765

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *H04W12/06*(2009.01)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)
H04L9/32, H04W12/06

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 1996-2014
Kokai Jitsuyo Shinan Koho 1971-2014 Toroku Jitsuyo Shinan Koho 1994-2014

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 A	JP 4996754 B1 (Toshiba Corp.), 08 August 2012 (08.08.2012), paragraphs [0009] to [0012], [0039] to [0052], [0056] to [0068]	1-8,17-19 9-12 13-16
X Y A	JP 5132807 B1 (Toshiba Corp.), 30 January 2013 (30.01.2013), paragraphs [0008] to [0011], [0036] to [0041], [0045] to [0050]	1-6,13,17-19 9-12 7,8,14-16
X Y	JP 2012-80482 A (Panasonic Corp.), 19 April 2012 (19.04.2012), paragraphs [0001], [0056] to [0064], [0069], [0071]	1,4-6,17-19 16

☒ 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
14 February, 2014 (14.02.14)	25 February, 2014 (25.02.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/082765

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-347956 A (Toshiba Corp.), 05 December 2003 (05.12.2003), paragraphs [0012] to [0031], [0045] to [0060]	9-11
Y	WO 2006/027725 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 16 March 2006 (16.03.2006), page 8, line 4 to page 9, line 13; page 11, lines 26 to 33	12
Y	JP 2012-105100 A (Nippon Telegraph and Telephone Corp.), 31 May 2012 (31.05.2012), paragraph [0024]	16

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2013/082765

JP 4996754 B2	2012.05.18	EP 2501160 A1	2012.09.19
JP 5132807 B2	2012.11.16	US 2013/0083922 A1	2013.04.04
JP 2012-80482 A	2012.04.19	(Family: none)	
JP 2003-347956 A	2003.12.05	US 2003/0223604 A1	2003.12.04
WO 2006/027725 A1	2006.03.16	JP 2008-512891 A	2008.04.04
		US 2008/0320587 A1	2008.12.25
		EP 1635508 A1	2006.03.15
		DE 602005019589 D	2010.04.08
		CN 101015173 A	2007.08.08
		KR 10-2007-0050057 A	2007.05.15
		AT 459158 T	2010.03.15
JP 2012-105100 A	2012.05.31	(Family: none)	

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０８２７６５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, H04W12/06(2009.01)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（ＩＰＣ））

Int.Cl.　H04L9/32, H04W12/06

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	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４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	関連する請求項の番号
X	JP 4996754 B1（株式会社東芝）2012.08.08, 9-12, 39-52, 56-68 段落	1-8, 17-19
Y		9-12
A		13-16
X	JP 5132807 B1（株式会社東芝）2013.01.30, 8-11, 36-41, 45-50 段落	1-6, 13, 17-19
Y		9-12
A		7, 8, 14-16

☑　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	国際調査報告の発送日
１４．０２．２０１４	２５．０２．２０１４

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　９３６４
中里　裕正
電話番号　０３－３５８１－１１０１　内線　３５４６

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	関連する請求項の番号
X Y	JP 2012-80482 A（パナソニック株式会社）2012.04.19, 1, 56-64, 69,71 段落	1, 4-6, 17-19 16
Y	JP 2003-347956 A（株式会社東芝）2003.12.05, 12-31, 45-60 段落	9-11
Y	WO 2006/027725 A1（KONINKLIJKE PHILIPS ELECTRONICS N.V.）2006.03.16, 8 頁 4 行-9 頁 13 行, 11 頁 26-33 行	12
Y	JP 2012-105100 A（日本電信電話株式会社）2012.05.31, 24 段落	16

JP 4996754 B2	2012.05.18	EP 2501160 A1	2012.09.19
JP 5132807 B2	2012.11.16	US 2013/0083922 A1	2013.04.04
JP 2012-80482 A	2012.04.19	ファミリーなし	
JP 2003-347956 A	2003.12.05	US 2003/0223604 A1	2003.12.04
WO 2006/027725 A1	2006.03.16	JP 2008-512891 A	2008.04.04
		US 2008/0320587 A1	2008.12.25
		EP 1635508 A1	2006.03.15
		DE 602005019589 D	2010.04.08
		CN 101015173 A	2007.08.08
		KR 10-2007-0050057 A	2007.05.15
		AT 459158 T	2010.03.15
JP 2012-105100 A	2012.05.31	ファミリーなし	