(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6109445号
(P6109445)
(45)発行日　平成29年4月5日(2017.4.5)　(24)登録日　平成29年3月17日(2017.3.17)

(51)Int.Cl.		F I		
H04W 12/04	(2009.01)	H04W	12/04	
H04W 92/08	(2009.01)	H04W	92/08	１１０
H04W 12/06	(2009.01)	H04W	12/06	
H04W 88/02	(2009.01)	H04W	88/02	１５１
H04L 9/08	(2006.01)	H04L	9/00	６０１Ｃ

請求項の数 9　(全 17 頁)　最終頁に続く

(21)出願番号　特願2016-560844 (P2016-560844)
(86)(22)出願日　平成28年4月27日(2016.4.27)
(86)国際出願番号　PCT/JP2016/063243
審査請求日　平成28年10月3日(2016.10.3)

早期審査対象出願

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100152881
弁理士　山地　博人
(72)発明者　菅原　健
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　齋藤　浩兵

最終頁に続く

(54)【発明の名称】無線通信装置、論理値選択方法及び論理値選択プログラム

(57)【特許請求の範囲】
【請求項１】
情報処理装置からの受信電波の電波強度を計測する、入出力インタフェースを有しない無線通信装置であって、
前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせる第１の動作及び前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせない第２の動作のうちのいずれかを行うよう依頼するメッセージを前記無線通信装置のユーザに提示するよう前記情報処理装置に要求する要求部と、
前記要求部が前記メッセージの提示を前記情報処理装置に要求してから任意の制限時間の間に前記受信電波の電波強度に変化が生じているか否かを検出し、前記制限時間の間に前記受信電波の電波強度に変化が生じている場合に論理値のうちの一方の値を選択し、前記制限時間の間に前記受信電波の電波強度に変化が生じていない場合に前記論理値のうちの他方の値を選択する選択部とを有し、
前記要求部は、
前記第１の動作及び前記第２の動作のうち、前記情報処理装置により生成された鍵交換のための秘密情報に対して前記情報処理装置において一方向性関数を用いて行われた演算により得られた論理値に対応する動作を行うように依頼するメッセージを前記無線通信装置のユーザに提示するよう前記情報処理装置に要求する無線通信装置。
【請求項２】
前記要求部は、

前記第１の動作として前記無線通信装置を握る動作を依頼し、前記第２の動作として前記無線通信装置を握らない動作を依頼するメッセージを前記ユーザに提示するよう前記情報処理装置に要求する請求項１に記載の無線通信装置。

【請求項３】

前記無線通信装置は、

前記ユーザの口の中に配置されており、

前記要求部は、

前記第１の動作として前記口を閉じる動作を依頼し、前記第２の動作として前記口を開ける動作を依頼するメッセージを前記ユーザに提示するよう前記情報処理装置に要求する請求項１に記載の無線通信装置。

【請求項４】

前記無線通信装置は、更に、

前記受信電波を受信するためのアンテナを有し、

前記要求部は、

前記第１の動作として前記アンテナに触れる動作を依頼し、前記第２の動作として前記アンテナに触れない動作を依頼するメッセージを前記ユーザに提示するよう前記情報処理装置に要求する請求項１に記載の無線通信装置。

【請求項５】

前記情報処理装置は、

前記無線通信装置への電波を送信するためのアンテナを有し、

前記要求部は、

前記第１の動作として前記アンテナに触れる動作を依頼し、前記第２の動作として前記アンテナに触れない動作を依頼するメッセージを前記ユーザに提示するよう前記情報処理装置に要求する請求項１に記載の無線通信装置。

【請求項６】

前記選択部は、

前記ユーザにより前記第１の動作が行われた場合に計測される前記受信電波の電波強度と前記ユーザにより前記第２の動作が行われた場合に計測される前記受信電波の電波強度との差と、計測した前記受信電波の電波強度とに基づき、前記制限時間の間に前記受信電波の電波強度に変化が生じているか否かを検出する請求項１に記載の無線通信装置。

【請求項７】

前記無線通信装置は、更に、

前記無線通信装置により生成された鍵交換のための秘密情報に対して、前記情報処理装置において行われる演算と同じ演算を行って論理値を取得し、

取得した論理値と、前記選択部により選択された論理値とを照合する検証部を有する請求項１に記載の無線通信装置。

【請求項８】

情報処理装置からの受信電波の電波強度を計測する、入出力インタフェースを有しないコンピュータである無線通信装置が、前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせる第１の動作及び前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせない第２の動作のうちのいずれかを行うよう依頼するメッセージを前記無線通信装置のユーザに提示するよう前記情報処理装置に要求する要求処理と、

前記無線通信装置が、前記要求処理において前記メッセージの提示を前記情報処理装置に要求してから任意の制限時間の間に前記受信電波の電波強度に変化が生じているか否かを検出し、前記制限時間の間に前記受信電波の電波強度に変化が生じている場合に論理値のうちの一方の値を選択し、前記制限時間の間に前記受信電波の電波強度に変化が生じていない場合に前記論理値のうちの他方の値を選択する選択処理とを有し、

前記要求処理において、

前記無線通信装置が、

前記第１の動作及び前記第２の動作のうち、前記情報処理装置により生成された鍵交換

のための秘密情報に対して前記情報処理装置において一方向性関数を用いて行われた演算により得られた論理値に対応する動作を行うように依頼するメッセージを前記無線通信装置のユーザに提示するよう前記情報処理装置に要求する論理値選択方法。

【請求項９】

情報処理装置からの受信電波の電波強度を計測する、入出力インタフェースを有しないコンピュータである無線通信装置に、

前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせる第１の動作及び前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせない第２の動作のうちのいずれかを行うよう依頼するメッセージを前記無線通信装置のユーザに提示するよう前記情報処理装置に要求する要求処理と、

前記要求処理において前記メッセージの提示を前記情報処理装置に要求してから任意の制限時間の間に前記受信電波の電波強度に変化が生じているか否かを検出し、前記制限時間の間に前記受信電波の電波強度に変化が生じている場合に論理値のうちの一方の値を選択し、前記制限時間の間に前記受信電波の電波強度に変化が生じていない場合に前記論理値のうちの他方の値を選択する選択処理とを実行させ、

前記要求処理において、

前記無線通信装置に、

前記第１の動作及び前記第２の動作のうち、前記情報処理装置により生成された鍵交換のための秘密情報に対して前記情報処理装置において一方向性関数を用いて行われた演算により得られた論理値に対応する動作を行うように依頼するメッセージを前記無線通信装置のユーザに提示するよう前記情報処理装置に要求させる論理値選択プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、無線通信装置、論理値選択方法及び論理値選択プログラムに関する。

【背景技術】

【０００２】

パーソナルコンピュータ又はスマートフォンに、無線を介してマウス、キーボードなどの周辺機器を接続することがある。無線通信では、機器間の接続状況を目視確認できないため、なりすましや盗聴の脅威がある。そのため、無線通信においては、暗号技術で通信路を保護することがある。

【０００３】

暗号技術を利用して通信路を保護する方法の多くでは、機器間で、事前に秘密情報を交換する必要がある。このような機器間で事前に秘密情報を交換する行為を、以下ではペアリングと呼ぶ。一度ペアリングをすれば、以降は、機器間で共通の秘密情報を元にした安全な通信を行うことができる。

【０００４】

ペアリングを行う１つの方法は、機器の製造時に秘密情報を機器に埋め込んでから機器を出荷することである。しかし、このような方法を用いることができない機器も存在する。例えばパーソナルコンピュータやマウスなどの市販品は、不特定多数の消費者に販売される。このため、ペアリング対象の機器を製造時に決めることができない。

【０００５】

製造時にペアリングができない機器に対しては、機器の出荷後にエンドユーザがペアリングを実施することがある。例えば、エンドユーザは、無線通信規格であるＢｌｕｅｔｏｏｔｈ（登録商標）を用いて出荷後のペアリングを行うことができる。

【０００６】

非特許文献１には、Ｂｌｕｅｔｏｏｔｈ（登録商標）を利用したペアリング方法が開示されている。以下では、Ｂｌｕｅｔｏｏｔｈ（登録商標）を利用したペアリング方法の１つである「Ｐａｓｓｋｅｙ　Ｅｎｔｒｙ」について説明する。この方法では、キーボード状の入力機構を備えた周辺機器のペアリングを行うことができる。一例として、パーソナ

ルコンピュータとキーボードをペアリングする場合を説明する。
ユーザがペアリングを試みると、パーソナルコンピュータの画面に数字が表示される。ユーザは、画面から読み取った数字を、ペアリングしようとしているキーボードに打鍵する。このようにすることで、パーソナルコンピュータとキーボードが、ユーザの操作を介して関連付けられることになる。
【先行技術文献】
【非特許文献】
【０００７】
【非特許文献１】Ｂｌｕｅｔｏｏｔｈ コア仕様 ４．２，ｈｔｔｐｓ：／／ｗｗｗ．ｂｌｕｅｔｏｏｔｈ．ｏｒｇ／ｊａ－ｊｐ／ｓｐｅｃｉｆｉｃａｔｉｏｎ／ａｄｏｐｔｅｄ－ｓｐｅｃｉｆｉｃａｔｉｏｎｓ
【発明の概要】
【発明が解決しようとする課題】
【０００８】
無線通信装置の種類は年々増加している。また、入出力インタフェースを持たない無線通信装置も増えている。このような入出力インタフェースを持たない無線通信装置の一例は生体センサ（活動量計、心拍計など）である。これら生体センサは、生体の信号を絶えずモニタし、モニタした信号を無線で送信する。生体センサはユーザによる操作が不要であるため、入出力インタフェースが省略されることがある。また、生体センサによっては、体内に埋め込むため、入出力インタフェースの搭載が困難な場合もある。
【０００９】
入出力インタフェースを持たない無線通信装置では、安全にペアリングを行うことが困難であるという課題がある。例えば前述の「Ｐａｓｓｋｅｙ Ｅｎｔｒｙ」は、入出力インタフェースを持たない無線通信装置では使うことができない。
【００１０】
本発明は、上記の課題を解決することを主な目的とする。すなわち、本発明は、入出力インタフェースを有しない無線通信装置を、安全にペアリングすることを主な目的とする。
【課題を解決するための手段】
【００１１】
本発明に係る無線通信装置は、
情報処理装置からの受信電波の電波強度を計測する、入出力インタフェースを有しない無線通信装置であって、
前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせる第１の動作及び前記無線通信装置で計測される前記受信電波の電波強度に変化を生じさせない第２の動作のうちのいずれかを行うよう依頼するメッセージを前記無線通信装置のユーザに提示するよう前記情報処理装置に要求する要求部と、
前記要求部が前記メッセージの提示を前記情報処理装置に要求してから任意の制限時間の間に前記受信電波の電波強度に変化が生じているか否かを検出し、前記制限時間の間に前記受信電波の電波強度に変化が生じている場合に論理値のうちの一方の値を選択し、前記制限時間の間に前記受信電波の電波強度に変化が生じていない場合に前記論理値のうちの他方の値を選択する選択部とを有する。
【発明の効果】
【００１２】
本発明では、無線通信装置は、ユーザに第１の動作又は第２の動作を行わせ、ユーザの動作に起因する受信電波の電波強度の変化の有無に応じて論理値を選択する。このため、無線通信装置は、入出力インタフェースを有していなくても、ペアリングに用いる論理値を取得することができる。従って、本発明によれば、入出力インタフェースを有しない無線通信装置を、安全にペアリングすることができる。
【図面の簡単な説明】

【００１３】
【図１】実施の形態１に係る無線通信システムの構成例を示す図。
【図２】実施の形態１に係る第１の機器の構成例を示す図。
【図３】実施の形態１に係る第２の機器の構成例を示す図。
【図４】実施の形態１に係る第１の動作及び第２の動作の例を示す図。
【図５】実施の形態１に係る論理値の入力例を示すシーケンス図。
【図６】実施の形態１に係る第１の機器の動作例を示すフローチャート図。
【図７】実施の形態１に係る論理値の通知例を示すシーケンス図。
【図８】実施の形態１に係る補助通信路を利用したペアリングの例を示すシーケンス図。
【図９】実施の形態１に係る第１の機器の動作例を示すフローチャート図。
【図１０】実施の形態１に係る第１の動作及び第２の動作の別の例を示す図。
【図１１】実施の形態１に係る第１の機器の構成例を示す図。
【発明を実施するための形態】
【００１４】
実施の形態１．
＊＊＊構成の説明＊＊＊
図１は、本実施の形態に係る無線通信システムの構成例を示す。
本実施の形態に係る無線通信システムは、第１の機器１０１と第２の機器１０２で構成される。
第１の機器１０１は、入出力インタフェースを有していない。
また、第１の機器１０１のユーザは、第１の機器１０１に触れることができる。
第２の機器１０２には、表示器１０３が備えられている。
第１の機器１０１と第２の機器１０２は、無線通信回線１０５を介した無線通信を行うことができる。
なお、第１の機器１０１は無線通信装置に相当する。また、第２の機器１０２は情報処理装置に相当する。また、第１の機器１０１が行う動作は、論理値選択方法に相当する。
【００１５】
図２は、第１の機器１０１の構成例を示す。
第１の機器１０１はコンピュータである。
第１の機器１０１は、ハードウェアとして、プロセッサ２０１、メモリ２０２、無線インタフェース２０３を備える。
また、第１の機器１０１は、機能構成として、計測部１１１、要求部１１２及び選択部１１３を備える。
計測部１１１、要求部１１２及び選択部１１３の機能は、プログラムとして実現される。メモリ２０２には、計測部１１１、要求部１１２及び選択部１１３の機能を実現するプログラムが記憶されている。そして、プロセッサ２０１が、計測部１１１、要求部１１２及び選択部１１３の機能を実現するプログラムを実行する。
図２では、プロセッサ２０１が、計測部１１１、要求部１１２及び選択部１１３の機能を実現するプログラムを実行している状態を模式的に表している。なお、計測部１１１、要求部１１２及び選択部１１３の詳細は後述する。なお、要求部１１２及び選択部１１３の機能を実現するプログラムは、論理値選択プログラムに相当する。また、要求部１１２の動作は要求処理に相当する。また、選択部１１３の動作は選択処理に相当する。
無線インタフェース２０７は、第２の機器１０２と無線通信を行う。
【００１６】
図３は、第２の機器１０２の構成例を示す。
第２の機器１０２は、コンピュータである。
第２の機器１０２は、ハードウェアとして、プロセッサ２０４、メモリ２０５、表示器インタフェース２０６、無線インタフェース２０７を備える。
また、第２の機器１０２は、表示器１０３に接続されている。
プロセッサ２０４及びメモリ２０５は、第２の機器１０２における計算処理に用いられ

る。
表示器インタフェース２０６は、表示器１０３を制御する。
無線インタフェース２０７は、第１の機器１０１と無線通信を行う。
【００１７】
＊＊＊動作の説明＊＊＊
図４は、本実施の形態に係る第１の機器１０１と第２の機器１０２の動作の概要を示す。
第１の機器１０１は、常時、第２の機器１０２からの受信電波の電波強度を計測している。
第１の機器１０１は、第２の機器１０２に対してメッセージの表示を要求する。
第２の機器１０２は、第１の機器１０１のユーザ１０４に対して動作を依頼するメッセージを表示器１０３に表示する。
ユーザ１０４は、第２の機器１０２の表示器１０３に表示されるメッセージに従って、第１の機器１０１を握る動作又は第１の機器１０１を握らない動作（ユーザ１０４が第１の機器１０１を握らない状態を継続する動作）を行う。
ユーザ１０４が第１の機器１０１を握る動作を行うと、第１の機器１０１が計測する受信電波の電波強度が変化する。具体的には、ユーザ１０４が第１の機器１０１を握ると、第１の機器１０１が計測する受信電波の電波強度が弱くなる。一方、ユーザ１０４が第１の機器１０１を握らない動作を行った場合は、第１の機器１０１が計測する受信電波の電波強度は変化しない。
第１の機器１０１は、第２の機器１０２に対してメッセージの表示を要求してから任意の制限時間の間に受信電波の電波強度が変化した場合は、論理値０を選択する。一方、制限時間の間に受信電波の電波強度が変化しない場合は、第１の機器１０１は論理値１を選択する。
なお、第１の機器１０１は、図４と異なり、受信電波の電波強度が変化した場合に論理値１を選択し、受信電波の電波強度が変化しない場合に論理値０を選択するようにしてもよい。
このように、第１の機器１０１は、ユーザの動作に起因する受信電波の電波強度の変化の有無に応じて論理値を選択する。
【００１８】
次に、図２に示した計測部１１１、要求部１１２及び選択部１１３の動作を説明する。
【００１９】
計測部１１１は、第２の機器１０２からの受信電波の電波強度を計測する。
【００２０】
要求部１１２は、計測される受信電波の電波強度に変化を生じさせる第１の動作及び計測される受信電波の電波強度に変化を生じさせない第２の動作のうちのいずれかを行うよう依頼するメッセージをユーザ１０４に提示するよう第２の機器１０２に要求する。
具体的には、要求部１１２は、メッセージの提示を要求する開始要求を無線インタフェース２０３及び無線通信回線１０５を介して第２の機器１０２に送信する。
第１の動作は、例えば、図４に示したユーザ１０４が第１の機器１０１を握る動作である。また、第２の動作は、例えば、図４に示したユーザ１０４が第１の機器１０１を握らない動作である。
【００２１】
選択部１１３は、要求部１１２がメッセージの提示を第２の機器１０２に要求してから任意の制限時間の間に受信電波の電波強度に変化が生じているか否かを検出する。更に、選択部１１３は、制限時間の間に受信電波の電波強度に変化が生じている場合に論理値のうちの一方の値を選択する。一方、制御時間の間に受信電波の電波強度に変化が生じていない場合は、選択部１１３は、論理値のうちの他方の値を選択する。
図２に示すメモリ２０２には、参照情報が記憶されている。この参照情報は、ユーザ１０４により第１の動作が行われた場合に計測される受信電波の電波強度とユーザ１０４に

より第２の動作が行われた場合に計測される受信電波の電波強度との差が示される。
選択部１１３は、メモリ２０２から参照情報を取得する。そして、選択部１１３は、参照情報に示される受信電波の電波強度の差と、計測した受信電波の電波強度とに基づき、制限時間の間に受信電波の電波強度に変化が生じているか否かを検出する。
【００２２】
図５は、図４に示す動作原理を応用した論理値の入力例を示すシーケンス図である。
図５において、縦線は、第１の機器１０１、第２の機器１０２、表示器１０３、およびユーザ１０４を表す。
【００２３】
まず、第１の機器１０１では、要求部１１２が、開始要求を無線インタフェース２０３及び無線通信回線１０５を介して第２の機器１０２に送信する。
開始要求を受信した第２の機器１０２は、表示器１０３を介して、ユーザ１０４にメッセージを表示する。図５の例では、第２の機器１０２は、表示器１０３に「開始してください」というメッセージを表示する。
ユーザ１０４は、表示器１０３上のメッセージに従って、第１の機器１０１を握る動作（第１の動作）又は第１の機器１０１を握らない動作（第２の動作）を行う。ユーザ１０４は、第１の機器１０１に論理値０を入力しようとする場合は、第１の機器１０１を握る。一方、第１の機器１０１に論理値１を入力しようとする場合は、ユーザ１０４は第１の機器１０１を握らない動作を行う。
第１の機器１０１では、選択部１１３が、制御時間内に電波強度が変化したか否かを検出する。
制御時間内に電波強度の変化があれば、選択部１１３は、ユーザ１０４による論理値０の入力と判定し、論理値０を選択する。
一方、制御時間内に電波強度の変化が無ければ、選択部１１３は、ユーザ１０４による論理値１の入力と判定し、論理値１を選択する。
【００２４】
このように、図５の方法によれば、ユーザ１０４は、第１の機器１０１を握る動作又は第１の機器１０１を握らない動作を行うことにより、第１の機器１０１に入力する論理値を指定することができる。
【００２５】
次に、第１の機器１０１の動作例を図６のフローチャートを用いて説明する。
【００２６】
ステップＳ４０１において、要求部１１２が、無線インタフェース２０７を介して、第２の機器１０２に開始要求を送信する。
次に、ステップ４０２において、選択部１１３が、計測部１１１による受信電波の電波強度の計測値を監視する。
そして、制限時間内に電波強度の計測値に変化があった場合（ステップＳ４０３でＹＥＳ）は、選択部１１３は、論理値０を選択する（ステップＳ４０４）。
一方で、制限時間内に電波強度の計測値に変化がなかった場合（ステップＳ４０３でＮＯ）は、選択部１１３は、論理値１を選択する（ステップＳ４０５）。
【００２７】
以上のようにすることで、ユーザ１０４の意図を、第１の機器１０１へ入力することができる。また、電波強度の強弱を用いるため、ボタンやスイッチ等のハードウェアを追加することなく、第１の機器１０１への入力を実現できる。
【００２８】
また、図６の手順により、第１の機器１０１と第２の機器１０２が近傍に存在することが確認できる。そのため、Ｗｅｂログインなどの多要素認証の安全性を高めることができる。
【００２９】
図７は、図４に示す動作原理を応用した論理値の通知例を示すシーケンス図である。

図７において、縦線は、第１の機器１０１、第２の機器１０２、表示器１０３、およびユーザ１０４を表す。

【００３０】

図５の例では、表示器１０３に「開始してください」とのメッセージが表示され、ユーザ１０４は、第１の機器１０１を握る動作及び第１の機器１０１を握らない動作のいずれかを任意に選択している。図７の例では、表示器１０３に「手を閉じてください」とのメッセージ又は「手を開けてください」とのメッセージが表示される。ユーザ１０４は、表示器１０３に「手を閉じてください」とのメッセージが表示された場合は、メッセージに従って、手を閉じる動作、すなわち第１の機器１０１を握る動作を行う。一方、表示器１０３に「手を開けてください」とのメッセージが表示された場合は、メッセージに従って、手を開ける動作、すなわち第１の機器１０１を握らない動作を行う。

このように、図７の例では、第２の機器１０２が、ユーザの動作を介して、第１の機器１０１に論理値を通知している。

【００３１】

まず、第１の機器１０１では、要求部１１２が、開始要求を無線インタフェース２０３及び無線通信回線１０５を介して第２の機器１０２に送信する。

開始要求を受信した第２の機器１０２は、表示器１０３を介して、ユーザ１０４にメッセージを表示する。第２の機器１０２は、第１の機器１０１に論理値０を通知する場合は、表示器１０３に「手を閉じてください」というメッセージを表示する。一方、第１の機器１０１に論理値１を通知する場合は、第２の機器１０２は、表示器１０３に「手を開けてください」とのメッセージを表示する。

ユーザ１０４は、表示器１０３上のメッセージに従って、第１の機器１０１を握る動作（第１の動作）又は第１の機器１０１を握らない動作（第２の動作）を行う。

第１の機器１０１では、選択部１１３が、制御時間内に電波強度が変化したか否かを検出する。

制御時間内に電波強度の変化があれば、選択部１１３は、ユーザ１０４による論理値０の入力と判定し、論理値０を選択する。

一方、制御時間内に電波強度の変化が無ければ、選択部１１３は、ユーザ１０４による論理値１の入力と判定し、論理値１を選択する。

【００３２】

以上により、第２の機器１０２が有する情報を、ユーザの動作、および電波強度の変化を介して第１の機器１０１に通知することができる。図７の方法では、第２の機器１０２は、１度の試行で第１の機器１０１に１ビットの情報を通知することができる。第２の機器１０２が同じ試行をＮ回くり返すと、第２の機器１０２はＮビットの情報を第１の機器１０１に通知することができる。このように、図７の方法により、通常の通信路と同じように第２の機器１０２から第１の機器１０１へデータ伝送を行うことができる。

【００３３】

以下、第２の機器１０２の無線インタフェース２０７、無線通信回線１０５、第１の機器１０１の無線インタフェース２０３を経る経路を主通信路という。

一方、図７に示した、表示器１０３のメッセージ表示、ユーザ１０４による動作、第１の機器１０１の選択部１１３による電波強度の変化有無に応じた論理値の選択を経る経路を補助通信路という。

第１の機器１０１と第２の機器１０２は、主通信路にてデータ通信を行うことができるが、補助通信路を用いて第２の機器１０２から第１の機器１０１に論理値を通知することには以下のような利点がある。

補助通信路では、ユーザ１０４自身が第１の機器１０１を目視で識別して手の開閉などの動作を行う。このため、無線通信回線１０５が目視できないことを利用したなりすまし攻撃に対して安全性が向上する。また、表示器１０３上のメッセージと電波強度の強弱を利用するため、たとえ主通信路の無線通信回線１０５の盗聴又は無線通信回線１０５上のデータの改ざんができる攻撃者であっても、補助通信路で通知される論理値の盗聴及び改

ざんはできない。このため、補助通信路を用いて第２の機器１０２から第１の機器１０１に論理値を通知することで安全性が向上する。

【００３４】

なお、図７に示すシーケンスに加えて、第２の機器１０２が、第１の機器１０１から到来する電波強度を計測してもよい。

このようにすることで、第２の機器１０２は、メッセージで指示した内容と、電波強度の変化状況が対応しているかどうかを確認することができる。もし、メッセージで指示した内容と電波強度の変化状況が一致しない場合は、第２の機器１０２は、攻撃が行われていることを検知することができる。このような手順によって、通信の安全性がさらに向上する。

【００３５】

前述した補助通信路は、中間者攻撃に耐性を持つ鍵交換に応用できる。

以下では、補助通信路を利用した、中間者攻撃に耐性を持つペアリングを説明する。

図８は、補助通信路を利用したペアリングの例を示すシーケンス図である。

図８において、縦線は、第１の機器１０１と、第２の機器１０２を表す。前述の通り、第１の機器１０１と第２の機器１０２は、主通信路を用いて通信ができる。また、第１の機器１０１と第２の機器１０２は、前述した補助通信路を用いて通信ができる。

図８に示すペアリングでは、第１の機器１０１と第２の機器１０２は、秘密情報を交換する。

【００３６】

図８に示すシーケンスは、段階６０１、段階６０２、段階６０３及び段階６０４で構成される。

段階６０１では、暗号学的な方法を用いて第１の機器１０１と第２の機器１０２が秘密情報Ｘを共有する。段階６０２では、第１の機器１０１と第２の機器１０２が、それぞれ秘密情報Ｘから情報Ｙを計算する。段階６０３では、第２の機器１０２が補助通信路を用いて情報Ｙを第１の機器１０１に通知する。段階６０４では、第１の機器１０１が、補助通信路を用いて通知された情報Ｙの検証を行う。

【００３７】

段階６０１では、第１の機器１０１と第２の機器１０２は、主通信路を介して秘密情報を共有する。この秘密情報は主通信路を盗聴する攻撃者に漏えいしてはいけない。

このような秘密情報の共有法の一例として、参考文献に開示されるディッフィー・ヘルマン鍵交換がある。

参考文献：W. Diffie and M. E. Hellman,“New Directions in Cryptography”, IEEE Transactions on Information Theory, Vol. IT－22, No. 6, 1976.

【００３８】

段階６０１を実行することで、第１の機器１０１は秘密情報Ｘ１を得る。また、第２の機器１０２は秘密情報Ｘ２を得る。攻撃の無い状態ならば、秘密情報Ｘ１と秘密情報Ｘ２は一致することが期待される。しかし、ディッフィー・ヘルマン鍵交換などの方法では、中間者攻撃を受けた場合には、秘密情報Ｘ１と秘密情報Ｘ２が一致しなくなる可能性がある。中間者攻撃を検出するために、秘密情報Ｘ１と秘密情報Ｘ２が一致するか否かを検証する必要がある。

しかし、主通信路は攻撃者が盗聴している可能性があるため、主通信路を用いて秘密情報Ｘ１と秘密情報Ｘ２が一致するか否かを検証することはできない。

本実施の形態では、第１の機器１０１と第２の機器１０２は、秘密情報Ｘ１と秘密情報Ｘ２が一致するか否かを、補助通信路を用いて検証する。

【００３９】

段階６０２では、第１の機器１０１及び第２の機器１０２は、共有した秘密情報Ｘ１と秘密情報Ｘ２を、公開してもよい情報Ｙ１と情報Ｙ２に変換する。

具体的には、第１の機器１０１は、秘密情報Ｘ１に関数Ｈを適用して情報Ｙ１を得る。また、第２の機器１０２は、秘密情報Ｘ２に関数Ｈを適用して情報Ｙ２を得る。

秘密情報の変換に用いられる関数Ｈは、具体的には、ハッシュ関数などの一方向性関数である。

【００４０】

段階６０３では、第２の機器１０２が情報Ｙ２を、補助通信路を介して、第１の機器１０１に通知する。

つまり、情報Ｙ２の１ビットごとに、図７に示すシーケンスが行われる。情報Ｙ２の全てのビットに対して図７のシーケンスが行われると、第１の機器１０１は情報Ｙ２を取得することができる。

【００４１】

段階６０４では、第１の機器１０１が、補助通信路を介して取得した情報Ｙ２と、段階６０２で算出した情報Ｙ１を比較する。情報Ｙ１と情報Ｙ２が一致すれば、高い確率で秘密情報Ｘ１と秘密情報Ｘ２が一致していると推定できる。一方、情報Ｙ１と情報Ｙ２が一致しない場合は、高い確率で秘密情報Ｘ１と秘密情報Ｘ２が一致しないと推定できる。つまり、情報Ｙ１と情報Ｙ２が一致しない場合は、中間者攻撃が行われたと推定できる。

このように、図８に示すシーケンスにより、中間者攻撃が行われていたとしても、中間者攻撃を検知することができるので、中間者攻撃による被害を防ぐことができる。また、このように中間者攻撃を防止することで、入出力インタフェースを有しない無線通信装置のペアリングにおける安全性を向上させることができる。

【００４２】

なお、図８に示すシーケンスに加えて、第２の機器１０２が、第１の機器１０１から到来する電波強度を計測してもよい。

このようにすることで、第２の機器１０２は、メッセージで指示した内容と、電波強度の変化状況が対応しているかどうかを確認することができる。もし、メッセージで指示した内容と電波強度の変化状況が一致しない場合は、第２の機器１０２は、攻撃が行われていることを検知することができる。このような手順によって、通信の安全性がさらに向上する。

【００４３】

図８に示すシーケンスにおける第１の機器１０１の動作例を図９のフローチャートを用いて説明する。

【００４４】

ステップＳ７０１において、第１の機器１０１は、主通信路を用いて、ディッフィー・ヘルマン鍵交換等により秘密情報の共有を行う。この結果、第１の機器１０１は秘密情報Ｘ１を得る。

なお、ステップＳ７０１は、例えば、プロセッサ２０１が、図１に図示していない秘密情報共有プログラムを実行することにより行われる。

【００４５】

次に、ステップＳ７０２において、第１の機器１０１は、関数Ｈを用いて、秘密情報Ｘ１を情報Ｙ１に変換する。

なお、ステップＳ７０２は、例えば、プロセッサ２０１が、図１に図示していない変換プログラムを実行することにより行われる。

【００４６】

次に、ステップＳ７０３において、第１の機器１０１は、補助通信路を用いて、第２の機器１０２から情報Ｙ２を取得する。

ステップＳ７０３では、図７に示すシーケンスが行われる。

つまり、ステップＳ７０３では、要求部１１２は、第１の動作及び第２の動作のうち、第１の機器１０１と第２の機器１０２とが共有している秘密情報Ｘ２に対して第２の機器１０２において行われた演算により得られた情報Ｙ２に対応する動作を行うように依頼するメッセージを第１の機器１０１のユーザに提示するよう第２の機器１０２に要求する。

選択部１１３は、ユーザの動作に従って論理値（情報Ｙ２）を選択する。

【００４７】

次に、ステップ７０４において、第１の機器１０１は、補助通信路から取得した情報Ｙ２と、ステップＳ７０２で計算した情報Ｙ１を比較する。

情報Ｙ１と情報Ｙ２が一致している場合（ステップＳ７０４でＹＥＳ）は、第１の機器１０１は、秘密情報Ｘ１を共有に成功した秘密情報と認識する（ステップＳ７０５）。

一方、情報Ｙ１と情報Ｙ２が一致しない場合（ステップＳ７０４でＮＯ）は、第１の機器１０１は、秘密情報の共有に失敗したと認識する（ステップＳ７０６）。

【００４８】

図８に示すシーケンスを実現する第１の機器１０１の機能構成例を図１１に示す。

図１１では、図２の構成と比較して、検証部１１４が追加されている。

検証部１１４は、秘密情報Ｘ１に対して、第２の機器１０２において行われる演算と同じ演算を行って情報Ｙ１を取得する。そして、検証部１１４は、取得した情報Ｙ１と、選択部１１３により選択された情報Ｙ２とを照合する。

つまり、検証部１１４は、図９のステップＳ７０２、ステップＳ７０４、Ｓ７０５、Ｓ７０６を行う。

【００４９】

なお、以上では、第１の動作の例としてユーザ１０４が第１の機器１０１を握る動作を説明し、第２の動作の例としてユーザ１０４が第１の機器１０１を握らない動作を説明した。

ユーザ１０４が第１の機器１０１を握る動作は、ある周波数の電波が、ユーザ１０４の肉体によって吸収されるという性質を利用する動作である。

第１の動作は、ユーザ１０４の身体の少なくとも一部を用いる、受信電波の電波強度に変化を生じさせる動作であれば、どのような動作でもよい。同様に、第２の動作は、ユーザの身体の少なくとも一部を用いる、受信電波の電波強度に変化を生じさせない動作であれば、どのような動作でもよい。

例えば、第１の機器１０１がユーザ１０４の口の中に配置されている場合に、図１０の（ａ）に例示するように、ユーザ１０４が口を閉じる動作を第１の動作とすることができる。そして、図１０の（ｂ）に例示するように、ユーザ１０４が口を開ける動作を第２の動作とすることができる。

この場合は、要求部１１２は、第１の動作として口を閉じる動作を依頼し、第２の動作として口を開ける動作を依頼するメッセージをユーザ１０４に提示するよう第２の機器１０２に要求する。この結果、図１０の（ａ）に示す「口を閉じてください」というメッセージ又は図１０の（ｂ）に示す「口を開けてください」というメッセージが表示器１０３に表示される。

【００５０】

また、ある周波数帯では、人体が触れることによってアンテナの特性が大きく変わり、結果として電波強度が変化する。

このため、第１の機器１０１に装備されている、第２の機器１０２からの受信電波を受信するためのアンテナをユーザ１０４が触れる動作を第１の動作とすることができる。また、当該アンテナをユーザ１０４が触れない動作（ユーザ１０４がアンテナに触れていない状態を維持する動作）を第２の動作とすることができる。

この場合は、要求部１１２は、第１の動作として第１の機器１０１のアンテナに触れる動作を依頼し、第２の動作として第１の機器１０１のアンテナに触れない動作を依頼するメッセージをユーザ１０４に提示するよう第２の機器１０２に要求する。

また、第２の機器１０２に装備されている、第１の機器１０１への電波を送信するためのアンテナをユーザ１０４が触れる動作を第１の動作とすることができる。また、当該アンテナをユーザ１０４が触れない動作（ユーザ１０４がアンテナに触れていない状態を維持する動作）を第２の動作とすることができる。

この場合は、要求部１１２は、第１の動作として第２の機器１０２のアンテナに触れる

動作を依頼し、第２の動作として第２の機器１０２のアンテナに触れない動作を依頼するメッセージをユーザ１０４に提示するよう第２の機器１０２に要求する。

【００５１】

以上では、メッセージを表示器１０３に表示する例を説明したが、他の方法によりメッセージをユーザ１０４に提示してもよい。例えば、スピーカー等を用いて音声によるメッセージをユーザ１０４に提示してもよいし、バイブレータ等を用いて振動によるメッセージをユーザ１０４に提示してもよい。

【００５２】

＊＊＊実施の形態の効果の説明＊＊＊

このように、本実施の形態では、第１の機器１０１は、ユーザ１０４に第１の動作又は第２の動作を行わせ、ユーザ１０４の動作に起因する受信電波の電波強度の変化の有無に応じて論理値を選択する。このため、第１の機器１０１は、入出力インタフェースを有していなくても、ペアリングに用いる論理値を取得することができる。従って、本実施の形態によれば、入出力インタフェースを有しない無線通信装置を、安全にペアリングすることができる。

＊＊＊ハードウェア構成の説明＊＊＊

最後に、第１の機器１０１のハードウェア構成の補足説明を行う。

プロセッサ２０１は、プロセッシングを行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）である。

プロセッサ２０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ）等である。

メモリ２０２は、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、フラッシュメモリ、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）等である。

無線インタフェース２０３は、データを受信するレシーバー及びデータを送信するトランスミッターを含む。

無線インタフェース２０３は、例えば、通信チップ又はＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）である。

【００５３】

また、メモリ２０２には、ＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）も記憶されている。

そして、ＯＳの少なくとも一部がプロセッサ２０１により実行される。

プロセッサ２０１はＯＳの少なくとも一部を実行しながら、計測部１１１、要求部１１２及び選択部１１３の機能を実現するプログラムを実行する。

プロセッサ９０１がＯＳを実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、計測部１１１、要求部１１２及び選択部１１３の処理の結果を示す情報やデータや信号値や変数値が、メモリ２０２、プロセッサ２０１内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、計測部１１１、要求部１１２及び選択部１１３の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、ＤＶＤ等の可搬記憶媒体に記憶されてもよい。

【００５４】

また、計測部１１１、要求部１１２及び選択部１１３の「部」を、「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。

また、第１の機器１０１は、ロジックＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、ＧＡ（Ｇａｔｅ Ａｒｒａｙ）、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）といった電子回路により実現されてもよい。

なお、プロセッサ及び上記の電子回路を総称してプロセッシングサーキットリーともい

う。

【符号の説明】

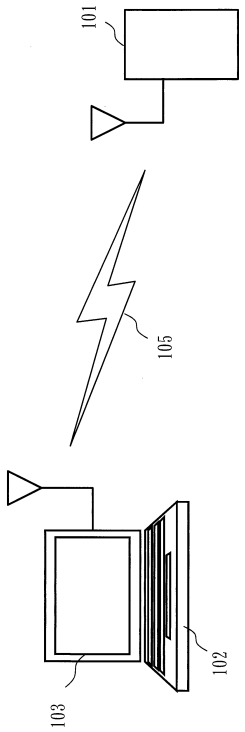
【００５５】

１０１　第１の機器、１０２　第２の機器、１０３　表示器、１０４　ユーザ、１０５　無線通信回線、１１１　計測部、１１２　要求部、１１３　選択部、１１４　検証部、２０１　プロセッサ、２０２　メモリ、２０３　無線インタフェース、２０４　プロセッサ、２０５　メモリ、２０６　表示器インタフェース、２０７　無線インタフェース。

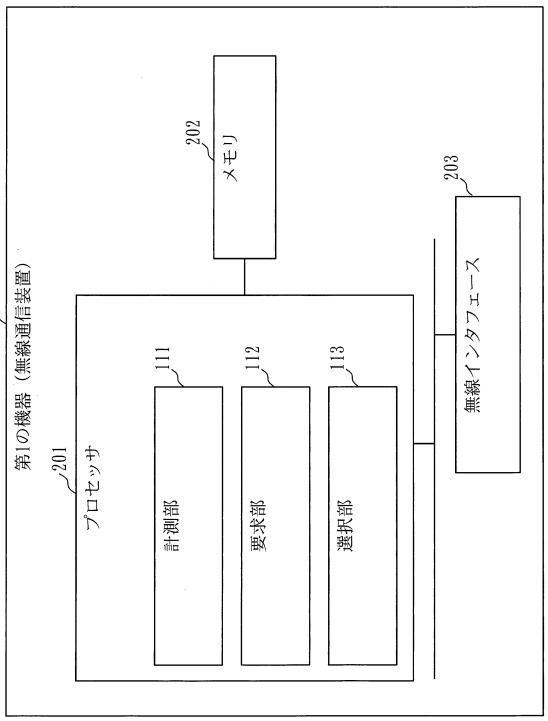
【要約】

計測部（１１１）は、第２の機器（１０２）からの受信電波の電波強度を計測する。要求部（１１２）は、計測される受信電波の電波強度に変化を生じさせる第１の動作及び計測される前記受信電波の電波強度に変化を生じさせない第２の動作のうちのいずれかを行うよう依頼するメッセージをユーザ（１０４）に提示するよう第２の機器（１０２）に要求する。選択部（１１３）は、要求部（１１２）がメッセージの提示を第２の機器（１０２）に要求してから任意の制限時間の間に受信電波の電波強度に変化が生じているか否かを検出し、制限時間の間に受信電波の電波強度に変化が生じている場合に論理値のうちの一方の値を選択し、制限時間の間に受信電波の電波強度に変化が生じていない場合に論理値のうちの他方の値を選択する。

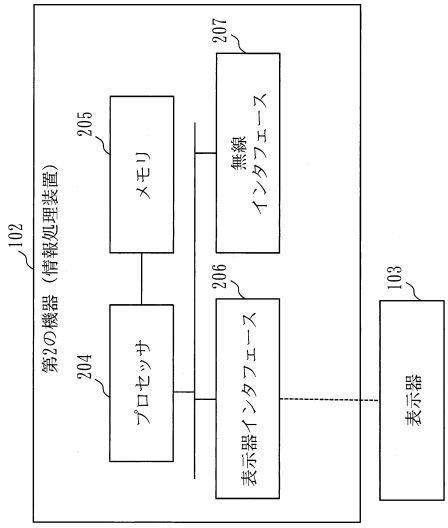
【図１】



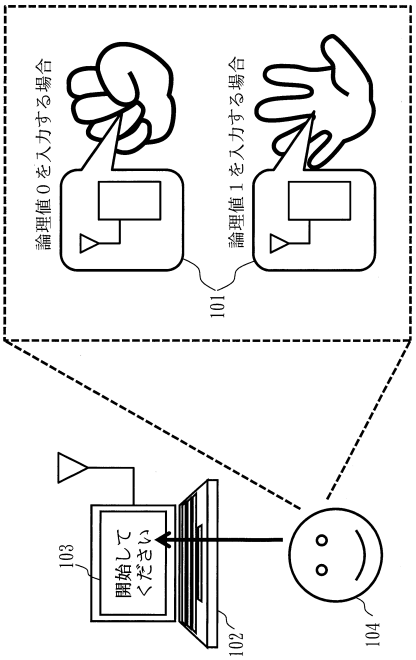
【図２】



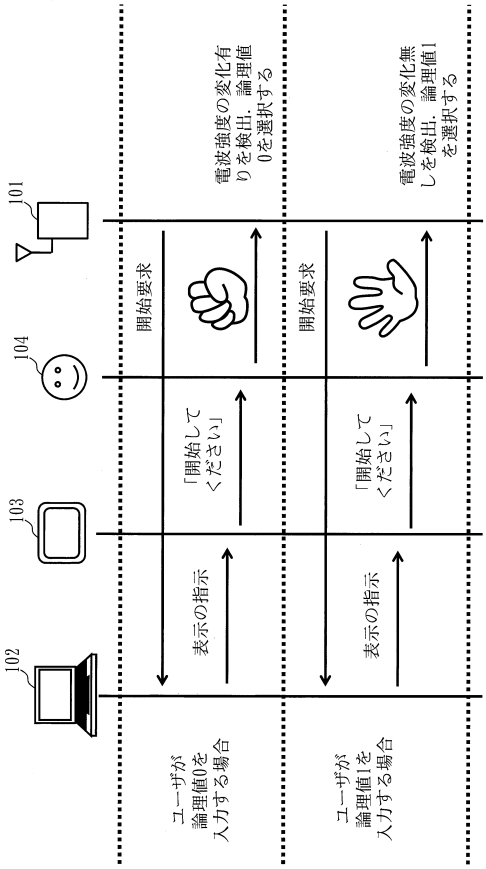
【図３】


102
第2の機器（情報処理装置）
204
プロセッサ
205
メモリ
206
表示器インタフェース
207
無線
インタフェース
103
表示器

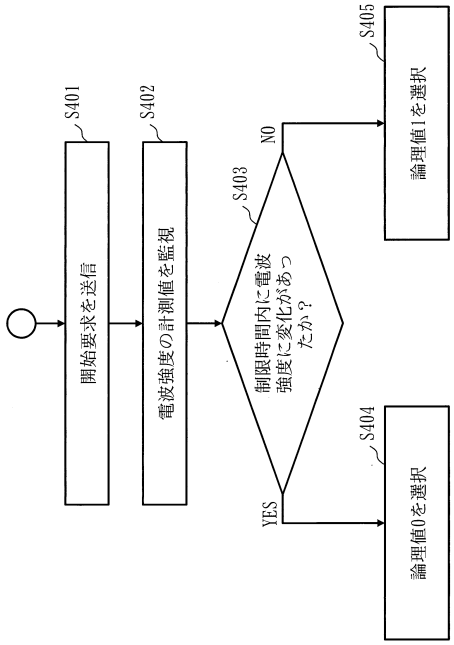
【図４】


論理値０を入力する場合
論理値１を入力する場合
101
103
開始して
ください
102
104

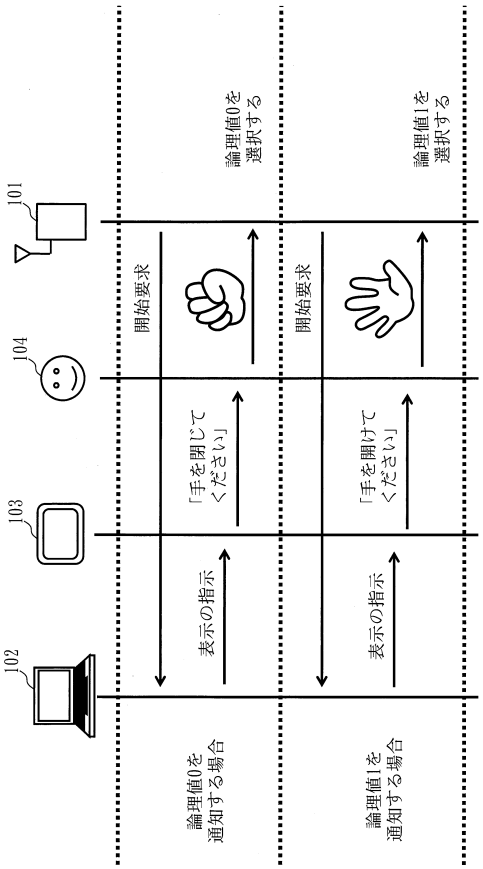
【図５】


101
104
103
102
開始要求
表示の指示
「開始して
ください」
電波強度の変化有
りを検出，論理値
０を選択する
開始要求
表示の指示
「開始して
ください」
電波強度の変化無
しを検出，論理値１
を選択する
ユーザが
論理値０を
入力する場合
ユーザが
論理値１を
入力する場合

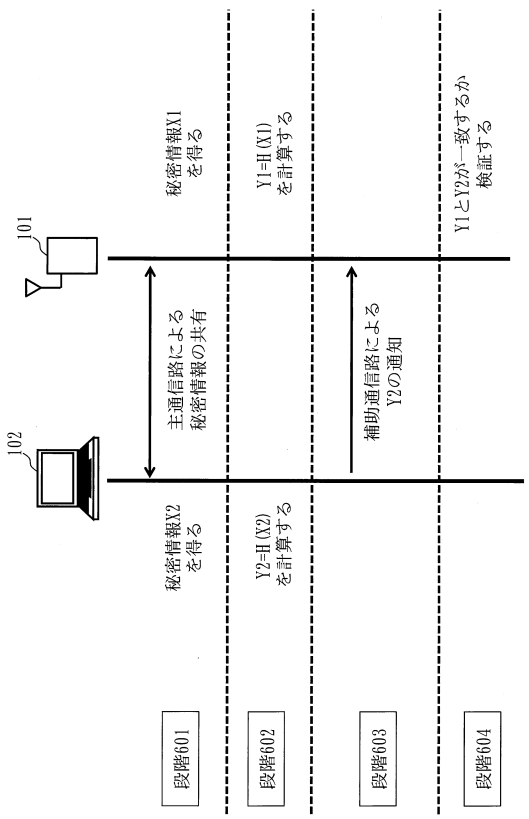
【図６】


S401
開始要求を送信
S402
電波強度の計測値を監視
S403
制限時間内に電波
強度に変化があっ
たか？
NO
YES
S405
論理値１を選択
S404
論理値０を選択

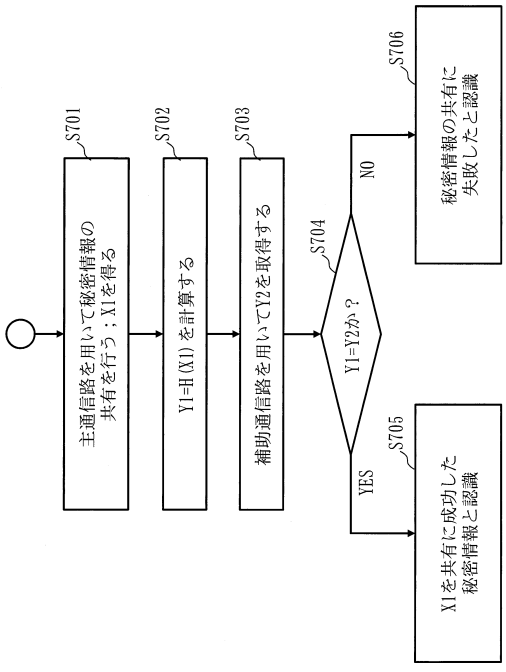
【図７】


101
104
103
102
開始要求
表示の指示
「手を閉じて
ください」
論理値0を
選択する
開始要求
表示の指示
「手を開けて
ください」
論理値1を
選択する
論理値0を
通知する場合
論理値1を
通知する場合

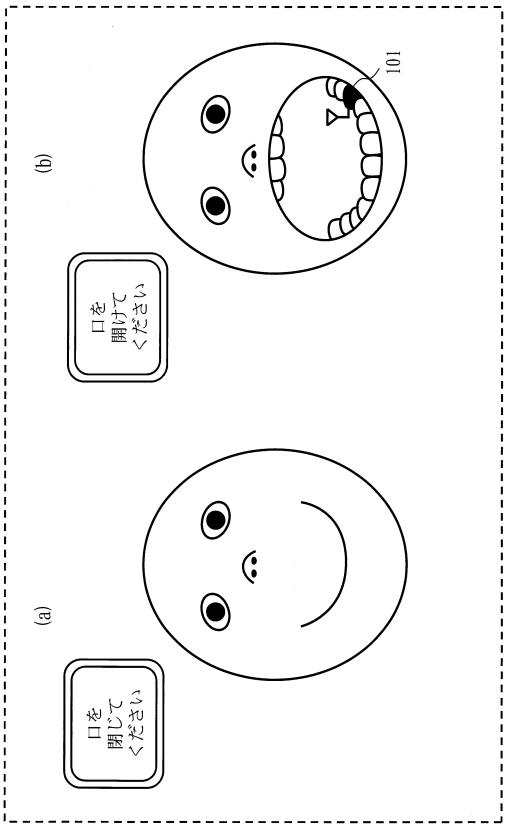
【図８】


101
102
主通信路による
秘密情報の共有
補助通信路による
Y2の通知
秘密情報X1
を得る
Y1=H(X1)
を計算する
Y1とY2が一致するか
検証する
秘密情報X2
を得る
Y2=H(X2)
を計算する
段階601
段階602
段階603
段階604

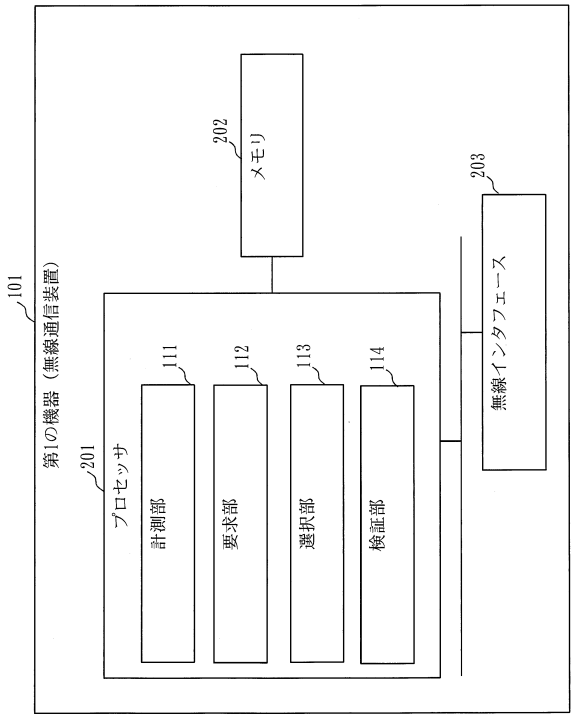
【図９】


主通信路を用いて秘密情報の
共有を行う；X1を得る
S701
Y1=H(X1)を計算する
S702
補助通信路を用いてY2を取得する
S703
Y1=Y2か？
S704
YES
NO
X1を共有に成功した
秘密情報と認識
S705
秘密情報の共有に
失敗したと認識
S706

【図１０】


(a)
口を
閉じて
ください
(b)
口を
開けて
ください
101

【図１１】


101
第1の機器（無線通信装置）
201
プロセッサ
111
計測部
112
要求部
113
選択部
114
検証部
202
メモリ
203
無線インタフェース

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 601E

(56)参考文献 米国特許出願公開第２０１５／０２２３０１１（ＵＳ，Ａ１）
特開２０１６－０１２９１８（ＪＰ，Ａ）
欧州特許出願公開第１５９６５３８（ＥＰ，Ａ１）
米国特許出願公開第２０１２／０２３１７４０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ ７／２４－７／２６
Ｈ０４Ｗ ４／００－９９／００
Ｈ０４Ｌ ９／０８