(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4853870号
(P4853870)

(45)発行日　平成24年1月11日(2012.1.11)　(24)登録日　平成23年11月4日(2011.11.4)

(51)Int.Cl.		F I		
H04W 84/12	(2009.01)	H04L	12/28	300Z
H04M 9/00	(2006.01)	H04M	9/00	C
G09C 1/00	(2006.01)	G09C	1/00	640E
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 52/04	(2009.01)	H04Q	7/00	430

請求項の数 9　(全 24 頁)　最終頁に続く

(21)出願番号　特願2006-300042 (P2006-300042)
(22)出願日　平成18年11月6日 (2006.11.6)
(65)公開番号　特開2008-118419 (P2008-118419A)
(43)公開日　平成20年5月22日 (2008.5.22)
審査請求日　平成21年3月2日 (2009.3.2)

(73)特許権者　591128453
株式会社メガチップス
大阪府大阪市淀川区宮原４丁目１番６号
(74)代理人　100088672
弁理士　吉竹　英俊
(74)代理人　100088845
弁理士　有田　貴弘
(72)発明者　本岡　茂哲
大阪府大阪市淀川区宮原４丁目１番６号
株式会社メガチップスシステムソリューションズ内

審査官　田畑　利幸

最終頁に続く

(54)【発明の名称】中継器、無線通信端末、通信システム、通信方法およびプログラム

(57)【特許請求の範囲】

【請求項１】

１以上の無線通信端末との間で無線通信を行う中継器であって、

通信電波によって情報を送受信する無線通信部と、

複数ビットからなる認証情報を記憶する記憶部と、

無線通信端末から前記無線通信部が一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定部と、

前記測定部の測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１または０であると判定する判定部と、

前記判定部の判定結果と前記記憶部に記憶されている認証情報とに基づいて前記無線通信端末を認証する認証部と、

を備えることを特徴とする中継器。

【請求項２】

請求項１に記載の中継器であって、

前記認証情報は、少なくとも１つの１の状態のビットと少なくとも１つの０の状態のビットとを含む情報であり、

前記判定部は、前記測定部の測定結果に基づいて、前記閾値を決定することを特徴とする中継器。

【請求項３】

コンピュータ読み取り可能なプログラムであって、前記プログラムの前記コンピュータによる実行は、前記コンピュータに、
複数ビットからなる認証情報を記憶する記憶工程と、
通信電波によって情報を送受信する無線通信工程と、
前記無線通信工程において、無線通信端末から一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定工程と、
前記測定工程における測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１または０であると判定する判定工程と、
前記判定工程における判定結果と前記記憶工程において記憶した認証情報とに基づいて前記無線通信端末を認証する認証工程と、
を実行させることを特徴とするプログラム。
【請求項４】
中継器との間で無線通信を行う無線通信端末であって、
パスコードを受け付ける操作部と、
前記操作部が受け付けたパスコードを記憶する記憶部と、
通信電波によって前記中継器に情報を送信する無線通信部と、
前記記憶部に記憶されているパスコードに基づいて、前記中継器に送信する認証要求情報の送信回数を決定するとともに、一の認証要求情報を送信する際の通信電波の強度を前記一の認証要求情報ごとに決定して前記無線通信部を制御する通信制御部と、
を備えることを特徴とする無線通信端末。
【請求項５】
請求項４に記載の無線通信端末であって、
前記通信制御部は、前記操作部が受け付けたパスコードのビット数に応じて、前記送信回数を決定することを特徴とする無線通信端末。
【請求項６】
コンピュータ読み取り可能なプログラムであって、前記プログラムの前記コンピュータによる実行は、前記コンピュータに、
パスコードを受け付ける入力工程と、
前記入力工程において受け付けたパスコードを記憶する記憶工程と、
前記記憶工程において記憶されたパスコードに基づいて、認証要求情報の送信回数を決定する回数決定工程と、
一の認証要求情報を送信する際の通信電波の強度を、前記一の認証要求情報ごとに決定する強度決定工程と、
前記強度決定工程において決定された強度の通信電波で、前記回数決定工程において決定された送信回数だけ、認証要求情報を中継器に送信する無線通信工程と、
を実行させることを特徴とするプログラム。
【請求項７】
１以上の無線通信端末が中継器との間で無線通信を行う通信システムであって、
前記中継器が、
通信電波によって情報を送受信する無線通信部と、
複数ビットからなる認証情報を記憶する記憶部と、
無線通信端末から前記無線通信部が一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定部と、
前記測定部の測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１または０であると判定する判定部と、
前記判定部の判定結果と前記記憶部に記憶されている認証情報とに基づいて前記無線通信端末を認証する認証部と、
を備え、

無線通信端末が、
パスコードを受け付ける操作部と、
前記操作部が受け付けたパスコードを記憶する記憶部と、
通信電波によって前記中継器に情報を送信する無線通信部と、
前記記憶部に記憶されているパスコードに基づいて、前記中継器に送信する認証要求情報の送信回数を決定するとともに、一の認証要求情報を送信する際の通信電波の強度を前記一の認証要求情報ごとに決定して前記無線通信部を制御する通信制御部と、
を備えることを特徴とする通信システム。
【請求項８】
請求項７に記載の通信システムであって、
前記通信制御部は、認証要求情報に送信番号を含め、
前記測定部は、認証要求情報に含まれる送信番号と、前記認証要求情報を受信したときの通信電波の強度とを関連付けることを特徴とする通信システム。
【請求項９】
１以上の無線通信端末が中継器との間で無線通信を行う通信方法であって、
中継器に複数ビットからなる認証情報を記憶させる第１記憶工程と、
無線通信端末においてパスコードを受け付ける入力工程と、
前記入力工程において受け付けたパスコードを前記無線通信端末に記憶する第２記憶工程と、
前記第２記憶工程において記憶されたパスコードに基づいて、認証要求情報の送信回数を決定する回数決定工程と、
一の認証要求情報を送信する際の通信電波の強度を、前記一の認証要求情報ごとに決定する強度決定工程と、
前記強度決定工程において決定された強度の通信電波で、前記回数決定工程において決定された送信回数だけ、認証要求情報を前記無線通信端末から送信する無線送信工程と、
前記無線送信工程において送信された認証要求情報を受信する無線受信工程と、
前記無線受信工程において、前記無線通信端末から一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定工程と、
前記測定工程における測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１または０であると判定する判定工程と、
前記判定工程における判定結果と前記第１記憶工程において記憶した認証情報とに基づいて前記無線通信端末を認証する認証工程と、
を備えることを特徴とする通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信を安全に行う技術に関する。より詳しくは、無線通信を行う通信端末を中継器において認証する技術に関する。
【背景技術】
【０００２】
無線通信を使用する通信システムでは、外部からの不正アクセスを防止するために、アクセスを許可する無線通信端末を限定する必要がある。これを解決するために、無線通信端末にオペレータがＷＥＰキーを入力し、このＷＥＰキーで通信の内容を暗号化して無線通信を行う技術が知られている。
【０００３】
しかし、ＷＥＰキー等の情報は、無線通信を行うたびに使用されることとなるため、複雑な情報であることが要求される。一方で、オペレータにとって複雑な情報を正確に入力する作業は負担が大きい。特に、無線通信端末を増設する場合には、一般のユーザがオペレータとしてこれらの情報を入力せねばならず、さらに問題である。

【０００４】
例えば、特許文献１には、認証情報を無線通信端末から送信し、当該認証情報をある閾値以上の通信電波で受信できた場合にのみ、中継器からＷＥＰキーを送信する技術が提案されている。すなわち、比較的電波状態のよい近傍から認証情報を送信する無線通信端末は、正規の無線通信端末であると認めることにより、複雑な情報の入力を省略してオペレータの負担を軽減するのである。
【０００５】
【特許文献１】特開２００６－１００９５７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
ところが、特許文献１に記載されている技術では、たまたま１回でも認証情報を受信できれば正規の無線通信端末であると認めてしまうという問題があった。すなわち、無線通信が成立しなかった場合に、送信する通信電波の強度を上げることは無線通信端末側の一般的な解決手段であるために、特許文献１に記載されている技術では、セキュリティレベルが低下しすぎるという問題があった。
【０００７】
本発明は、上記課題に鑑みなされたものであり、オペレータの負担を抑制しつつ、無線通信におけるセキュリティを確保することを目的とする。
【課題を解決するための手段】
【０００８】
上記の課題を解決するため、請求項１の発明は、１以上の無線通信端末との間で無線通信を行う中継器であって、通信電波によって情報を送受信する無線通信部と、複数ビットからなる認証情報を記憶する記憶部と、無線通信端末から前記無線通信部が一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定部と、前記測定部の測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１または０であると判定する判定部と、前記判定部の判定結果と前記記憶部に記憶されている認証情報とに基づいて前記無線通信端末を認証する認証部とを備えることを特徴とする。
【０００９】
また、請求項２の発明は、請求項１の発明に係る中継器であって、前記認証情報は、少なくとも１つの１の状態のビットと少なくとも１つの０の状態のビットとを含む情報であり、前記判定部は、前記測定部の測定結果に基づいて、前記閾値を決定することを特徴とする。
【００１０】
また、請求項３の発明は、コンピュータ読み取り可能なプログラムであって、前記プログラムの前記コンピュータによる実行は、前記コンピュータに、複数ビットからなる認証情報を記憶する記憶工程と、通信電波によって情報を送受信する無線通信工程と、前記無線通信工程において、無線通信端末から一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定工程と、前記測定工程における測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１または０であると判定する判定工程と、前記判定工程における判定結果と前記記憶工程において記憶した認証情報とに基づいて前記無線通信端末を認証する認証工程とを実行させることを特徴とする。
【００１１】
また、請求項４の発明は、中継器との間で無線通信を行う無線通信端末であって、パスコードを受け付ける操作部と、前記操作部が受け付けたパスコードを記憶する記憶部と、通信電波によって前記中継器に情報を送信する無線通信部と、前記記憶部に記憶されてい

るパスコードに基づいて、前記中継器に送信する認証要求情報の送信回数を決定するとともに、一の認証要求情報を送信する際の通信電波の強度を前記一の認証要求情報ごとに決定して前記無線通信部を制御する通信制御部とを備えることを特徴とする。

【００１２】

また、請求項５の発明は、請求項４の発明に係る無線通信端末であって、前記通信制御部は、前記操作部が受け付けたパスコードのビット数に応じて、前記送信回数を決定することを特徴とする。

【００１３】

また、請求項６の発明は、コンピュータ読み取り可能なプログラムであって、前記プログラムの前記コンピュータによる実行は、前記コンピュータに、パスコードを受け付ける入力工程と、前記入力工程において受け付けたパスコードを記憶する記憶工程と、前記記憶工程において記憶されたパスコードに基づいて、認証要求情報の送信回数を決定する回数決定工程と、一の認証要求情報を送信する際の通信電波の強度を、前記一の認証要求情報ごとに決定する強度決定工程と、前記強度決定工程において決定された強度の通信電波で、前記回数決定工程において決定された送信回数だけ、認証要求情報を中継器に送信する無線通信工程とを実行させることを特徴とする。

【００１４】

また、請求項７の発明は、１以上の無線通信端末が中継器との間で無線通信を行う通信システムであって、前記中継器が、通信電波によって情報を送受信する無線通信部と、複数ビットからなる認証情報を記憶する記憶部と、無線通信端末から前記無線通信部が一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定部と、前記測定部の測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１または０であると判定する判定部と、前記判定部の判定結果と前記記憶部に記憶されている認証情報とに基づいて前記無線通信端末を認証する認証部とを備え、無線通信端末が、パスコードを受け付ける操作部と、前記操作部が受け付けたパスコードを記憶する記憶部と、通信電波によって前記中継器に情報を送信する無線通信部と、前記記憶部に記憶されているパスコードに基づいて、前記中継器に送信する認証要求情報の送信回数を決定するとともに、一の認証要求情報を送信する際の通信電波の強度を前記一の認証要求情報ごとに決定して前記無線通信部を制御する通信制御部とを備えることを特徴とする。

【００１５】

また、請求項８の発明は、請求項７の発明に係る通信システムであって、前記通信制御部は、認証要求情報に送信番号を含め、前記測定部は、認証要求情報に含まれる送信番号と、前記認証要求情報を受信したときの通信電波の強度とを関連付けることを特徴とする。

【００１６】

また、請求項９の発明は、１以上の無線通信端末が中継器との間で無線通信を行う通信方法であって、中継器に複数ビットからなる認証情報を記憶させる第１記憶工程と、無線通信端末においてパスコードを受け付ける入力工程と、前記入力工程において受け付けたパスコードを前記無線通信端末に記憶する第２記憶工程と、前記第２記憶工程において記憶されたパスコードに基づいて、認証要求情報の送信回数を決定する回数決定工程と、一の認証要求情報を送信する際の通信電波の強度を、前記一の認証要求情報ごとに決定する強度決定工程と、前記強度決定工程において決定された強度の通信電波で、前記回数決定工程において決定された送信回数だけ、認証要求情報を前記無線通信端末から送信する無線送信工程と、前記無線送信工程において送信された認証要求情報を受信する無線受信工程と、前記無線受信工程において、前記無線通信端末から一の認証要求情報を受信するごとに、前記一の認証要求情報を受信したときの通信電波の強度を測定する測定工程と、前記測定工程における測定結果に基づいて、前記一の認証要求情報を受信したときの通信電波の強度と閾値とを比較し、前記一の認証要求情報を受信したときの通信電波の状態を１

または０であると判定する判定工程と、前記判定工程における判定結果と前記第１記憶工程において記憶した認証情報とに基づいて前記無線通信端末を認証する認証工程とを備えることを特徴とする。

【発明の効果】

【００１７】

請求項１ないし３および７ないし９に記載の発明では、無線通信端末から一の認証要求情報を受信するごとに、一の認証要求情報を受信したときの通信電波の強度を測定して、一の認証要求情報を受信したときの通信電波の状態を１または０であると判定し、認証情報と比較して認証することにより、無線通信端末の認証を容易に、かつ、安全に行うことができる。

【００１８】

請求項２に記載の発明では、認証情報は、少なくとも１つの１の状態のビットと少なくとも１つの０の状態のビットとを含む情報であり、判定部は、測定部の測定結果に基づいて、閾値を決定することにより、認証を行うときの通信状態に応じて閾値を決定することができる。

【００１９】

請求項４ないし６に記載の発明では、パスコードに基づいて、中継器に送信する認証要求情報の送信回数を決定するとともに、一の認証要求情報を送信する際の通信電波の強度を一の認証要求情報ごとに決定することにより、複雑なパスコードを要求することなく、セキュリティを向上できる。

【００２０】

請求項８に記載の発明では、通信制御部は、認証要求情報に送信番号を含め、測定部は、認証要求情報に含まれる送信番号と、認証要求情報を受信したときの通信電波の強度とを関連付けることにより、送信された認証要求情報ごとに、当該認証要求情報を受信したか否かを容易に判定できる。したがって、認証精度が向上する。

【発明を実施するための最良の形態】

【００２１】

以下、本発明の好適な実施の形態について、添付の図面を参照しつつ、詳細に説明する。

【００２２】

＜１．　実施の形態＞

図１は、本発明における通信システムであるドアホンシステム１を示す図である。ドアホンシステム１は、室内子機２、室外子機３、屋外カメラ４および本体ユニット５を備える。ドアホンシステム１は、訪問者の有無を家人（住民）に報知する機能や、室内子機２間で内線通話等を提供する機能を有している。

【００２３】

一般にドアホンシステム１で送受信される情報は家人に限定されるべき性質のものであり、特に無線通信においては外部からの不正アクセスを防止する必要がある。また、ドアホンシステム１で使用される無線通信端末（室内子機２および屋外カメラ４）は、設置後に増設されることがあり、その場合、通常、家人によって増設された無線通信端末の登録（起動）が実行される。

【００２４】

なお、本発明における通信システムはドアホンシステム１に限定されるものではなく、例えば無線ＬＡＮを使用する一般的なシステムに適用可能である。

【００２５】

図２は、室内子機２の構成を示すブロック図である。本発明における無線通信端末である室内子機２は、ＣＰＵ２０、記憶装置２１、操作部２２、表示部２３、スピーカ２４、マイク２５および無線通信部２７を備える。

【００２６】

ＣＰＵ２０は、記憶装置２１に記憶されているプログラム２１０に従って動作すること

により、各種データの演算や制御信号の生成を行う。図２に示すように、ＣＰＵ２０は、バス配線により室内子機２の各構成と接続されており、生成した制御信号によってこれらの構成を制御する。なお、ＣＰＵ２０の動作および機能についての詳細は後述する。

【００２７】

記憶装置２１は、各種ＲＯＭや、ＲＡＭから構成されており、プログラム２１０や各種データを記憶する。

【００２８】

操作部２２は、複数のボタン類から構成される。オペレータは、操作部２２を操作することにより、室内子機２（ドアホンシステム１）に必要な指示情報を入力することができる。オペレータによって入力される指示情報としては、呼出に応答するための応答情報やパスコード等がある。

【００２９】

表示部２３は、液晶ディスプレイや、ＬＥＤ等から構成され、これらによって様々な情報を表示し、オペレータに各種状態を知らせる機能を有する。例えば、表示部２３は、本体ユニット５による認証に成功したか否かを示す情報を表示する。

【００３０】

スピーカ２４は、一般的な音声再生装置であり、電気信号に基づいて音声を再生する機能を有する。スピーカ２４によって再生される音声情報に含まれる音声としては、室外子機３または他の室内子機２から本体ユニット５を介して送信される音声（外線・内線通話における音声）、あるいは記憶装置２１に予め記憶されている呼出音等がある。

【００３１】

マイク２５は、室内子機２の周囲の音声を電気信号に変換する機能を有する。マイク２５は、主に室内子機２を使用するオペレータの肉声を音声情報に変換するために使用される。

【００３２】

無線通信部２７は、室内子機２と本体ユニット５とを無線通信によって情報のやりとりが可能な状態で接続する機能を有する。具体的には、無線通信を実現するための送信アンテナや、受信アンテナ等が該当する。

【００３３】

図３は、室内子機２の機能ブロックを情報の流れとともに示す図である。図３に示す通信制御部２００およびタイマ２０１が、主にＣＰＵ２０がプログラム２１０に従って動作することにより実現される機能ブロックである。

【００３４】

通信制御部２００は、操作部２２により受け付けたパスコード２１１を参照し、参照したパスコード２１１に基づいて認証要求情報２１２を送信する回数Ｎを決定する。また、一の認証要求情報２１２を送信するごとに、当該認証要求情報２１２を送信する通信電波の強度をそれぞれ決定する（すなわち、Ｎ回分の通信電波の強度を決定する）。

【００３５】

また、通信制御部２００は、何番目の送信に係る認証要求情報２１２かを示す送信番号（１からＮまでの数字となる）を認証要求情報２１２に含める。

【００３６】

また、通信制御部２００は、タイマ２０１から伝達される時間を、認証要求情報２１２に含める。これにより、室内子機２から送信される認証要求情報２１２には、室内子機２から送信された時間が含まれる。

【００３７】

タイマ２０１は、時間を計測しつつ、その結果を通信制御部２００に伝達する。

【００３８】

図４は、認証要求情報２１２の構造を例示する図である。図４に示すように、認証要求情報２１２には、コマンド識別子２１３、メーカ識別コード２１４、時間情報２１５および送信番号２１６が含まれている。

【００３９】
コマンド識別子２１３は、情報が認証要求情報２１２であると識別するための情報であり、主に、認証要求情報２１２を受信する本体ユニット５によって参照される情報である。コマンド識別子２１３は、予め、ドアホンシステム１において固定の情報として定められている。
【００４０】
メーカ識別コード２１４は、ドアホンシステム１の製造メーカを識別するための情報であるが、必須の情報項目ではなく、例えば、製品番号等の情報であってもよい。このように、認証要求情報２１２に任意の情報を含めることによって、さらに認証精度の向上を図ることができる。
【００４１】
時間情報２１５および送信番号２１６は、先述のように、通信制御部２００によって、送信前に含められる情報であり、Ｎ回送信される認証要求情報２１２ごとにそれぞれ異なる情報（内容）となる。
【００４２】
図１に戻って、室外子機３は、図示しない操作ボタンを備えており、主に住居を訪れた訪問者によって操作される。訪問者によって操作ボタンが操作されると、室外子機３は、操作ボタンが操作されたことを示す来訪情報を生成して本体ユニット５に送信する。すなわち、室外子機３から来訪情報を受信することにより、本体ユニット５は訪問者があったことを検出する。
【００４３】
また、室外子機３は、図１に示すように、本体ユニット５とケーブルによって接続されており、本体ユニット５との間で有線による通信を行う。このように、ドアホンシステム１は、室外子機３のように、有線通信を行う有線通信端末を備えていてもよい。
【００４４】
また、室外子機３は、図示しないスピーカ、マイクおよびカメラを備えており、本体ユニット５によって回線接続された室内子機２との間で音声通話が可能であるとともに、当該室内子機２に向けて画像情報を送信することも可能とされている。すなわち、訪問者が発した音声をマイクによって音声情報に変換して送信するとともに、訪問者をカメラによって撮像してその画像情報を送信する。また、室内子機２から受信した音声情報をスピーカによって再生する。
【００４５】
図５は、屋外カメラ４の構成を示すブロック図である。室内子機２と同様に本発明における無線通信端末である屋外カメラ４は、ＣＰＵ４０、記憶装置４１、操作部４２、表示部４３、撮像部４４および無線通信部４７を備える。
【００４６】
ＣＰＵ４０は、記憶装置４１に記憶されているプログラム４１０に従って動作することにより、各種データの演算や制御信号の生成を行う。図４に示すように、ＣＰＵ４０は、バス配線により屋外カメラ４の各構成と接続されており、生成した制御信号によってこれらの構成を制御する。なお、ＣＰＵ４０は、プログラム４１０に従って動作することにより、通信制御部２００およびタイマ２０１と同様の機能ブロックを実現する。
【００４７】
記憶装置４１は、各種ＲＯＭや、ＲＡＭから構成されており、プログラム４１０や、各種データ（パスコード２１１や認証要求情報２１２）を記憶する。
【００４８】
操作部４２は、複数のボタン類から構成される。オペレータは、操作部４２を操作することにより、屋外カメラ４に必要な指示情報を入力することができる。特に、本実施の形態における屋外カメラ４では、パスコードが操作部４２から入力される。
【００４９】
表示部４３は、ＬＥＤ等から構成され、これらの点滅によって様々な情報を表示し、オ

ペレータに各種状態を知らせる機能を有する。例えば、表示部４３は、本体ユニット５による認証に成功したか否かを示す情報を表示する。

【００５０】

撮像部４４は、一般的なデジタルカメラとしての機能を有しており、所定の撮像領域を撮像することにより画像情報を取得する。なお、本実施の形態における撮像部４４は、動画像を撮像するが、もちろん静止画像であってもよい。

【００５１】

無線通信部４７は、屋外カメラ４と本体ユニット５とを無線通信によって情報のやりとりが可能な状態で接続する機能を有する。具体的には、無線通信を実現するための送信アンテナや、受信アンテナ等が該当する。

【００５２】

このような構成により、屋外カメラ４は、無線通信部４７によって本体ユニット５と接続されており、本体ユニット５からの制御信号に基づいて、撮像部４４が撮像を行う。さらに、撮像により取得した画像情報は、無線通信部４７が本体ユニット５に送信する。

【００５３】

図６は、本体ユニット５の構成を示すブロック図である。本体ユニット５は、ＣＰＵ５０、記憶装置５１、操作部５２、表示部５３、無線通信部５７および有線通信部５８を備え、ドアホンシステム１が備える各装置間の通信を中継するルータとしての機能を有する。

【００５４】

なお、先述のように、ドアホンシステム１において、室内子機２および屋外カメラ４は、無線通信を行う無線通信端末として構成されている。したがって、室内子機２および屋外カメラ４が通信（無線通信）を行う場合、本体ユニット５は、アクセスポイント（中継器）として機能する。

【００５５】

ＣＰＵ５０は、記憶装置５１に記憶されているプログラム５１０に従って動作することにより、各種データの演算や制御信号の生成を行う。図６に示すように、ＣＰＵ５０は、バス配線により本体ユニット５の各構成と接続されており、生成した制御信号によってこれらの構成を制御する。なお、ＣＰＵ５０の動作および機能については後述する。

【００５６】

記憶装置５１は、各種ＲＯＭや、ＲＡＭ等から構成されており、プログラム５１０や各種データ（パラメータ情報等）を記憶する。

【００５７】

操作部５２は、複数のボタン類から構成される。本体ユニット５のオペレータは、操作部５２を操作することにより、本体ユニット５（ドアホンシステム１）に必要な指示情報を入力することが可能とされている。

【００５８】

表示部５３は、ＬＥＤやランプ等から構成され、これらの点滅状況によってオペレータに各種状態を知らせる機能を有する。なお、表示部５３は、各種情報を画像として表示する液晶ディスプレイ等を備えていてもよい。

【００５９】

無線通信部５７は、無線によるデータ通信を行う構成（本実施の形態では、室内子機２および屋外カメラ４）と、本体ユニット５とをデータ通信可能な状態で接続する機能を有する。具体的には、無線通信を実現するための送信アンテナや、受信アンテナ等から構成される。

【００６０】

有線通信部５８は、有線によるデータ通信を行う構成（室外子機３）と、本体ユニット５とをデータ通信可能な状態で接続する機能を有する。具体的には、通信用の各種ケーブルを接続する端子等が該当する。

【００６１】

図７は、本体ユニット５の機能ブロックを情報の流れとともに示す図である。図７に示す測定部５００、判定部５０１、タイマ５０２および認証部５０３が、主にＣＰＵ５０がプログラム５１０に従って動作することにより実現される機能ブロックである。

【００６２】

測定部５００は、無線通信部５７が情報を受信した場合における通信電波の強度を測定する。そして、受信した情報にコマンド識別子２１３が含まれているか否かに基づいて、当該情報が認証要求情報２１２であるか否かを判定する。さらに、受信した情報が認証要求情報２１２であった場合には、この認証要求情報２１２を受信したときの通信電波の強度を測定情報５１１として記憶装置５１に記憶させる。

【００６３】

すなわち、測定部５００は、一の認証要求情報２１２を送信するために使用された通信電波の強度（受信強度）を、それぞれ測定して、測定情報５１１を生成する機能を有している。

【００６４】

判定部５０１は、認証要求情報２１２とタイマ５０２を参照することにより、一の無線通信端末（室内子機２または屋外カメラ４）から受信する少なくも１以上の認証要求情報２１２をすべて受信したか否かを検出する。

【００６５】

本実施の形態におけるドアホンシステム１では、例えば、ある室内子機２を本体ユニット５に登録する場合、当該室内子機２から認証要求情報２１２を複数回（Ｎ回）送信する。したがって、本体ユニット５は、認証を行う場合、認証を要求する端末から送信されたすべての認証要求情報２１２（Ｎ回の認証要求情報２１２）を受信したか否かを検出する必要がある。なお、受信完了を検出する具体的な動作については後述する。

【００６６】

また、判定部５０１は、受信完了となった状態で、測定情報５１１を参照して、閾値情報５１２を生成する。本実施の形態における判定部５０１は、測定情報５１１に記録されている通信電波の強度の最大値Ｖを求め、閾値Ｑを３／４Ｖとして、閾値情報５１２を生成する。

【００６７】

さらに、判定部５０１は、測定情報５１１を参照して、一の認証要求情報２１２を受信したときの通信電波の強度を、それぞれ閾値情報５１２と比較する。そして、比較した通信電波の強度が閾値Ｑより大きければ当該通信電波の状態を「１」、それ以外であれば当該通信電波の状態を「０」と判定する。そして、その判定結果に基づいて、判定情報５１３を生成する。すなわち、判定情報５１３は、一連の認証要求情報２１２の受信が完了するたびに生成される。

【００６８】

タイマ５０２は、時間を計測しつつ、その結果を判定部５０１に伝達する。

【００６９】

認証部５０３は、判定情報５１３と認証情報５１４とを比較して、これが一致するか否かに基づいて、認証要求情報２１２を送信してきた無線通信端末（室内子機２および屋外カメラ４）を認証する。

【００７０】

以上が、本実施の形態におけるドアホンシステム１の構成および機能の説明である。次に、ドアホンシステム１の動作について説明する。

【００７１】

ドアホンシステム１では、無線通信の内容を他人に知られないために、アクセスポイントである本体ユニット５と正規の無線通信端末（家人が使用する室内子機２および屋外カメラ４）との間で情報を暗号化して送受信する。そして、暗号化（復号化）に必要な情報（ＷＥＰキー）は、正規の無線通信端末であると認証された無線通信端末に、本体ユニット５から送信される。したがって、室内子機２や屋外カメラ４は、予め本体ユニット５に

よって認証されなければ、ドアホンシステム１において使用することができない。

【００７２】

図８および図９は、室内子機２の動作を示す流れ図である。図８および図９は、主に、室内子機２が本体ユニット５に対して認証を要求する処理を示す。

【００７３】

本実施の形態では、本体ユニット５に予め記憶されている認証情報５１４は、個々の本体ユニット５に個別に設定された複数ビットの情報である。また、本実施の形態における認証情報５１４は、少なくとも１つのビットの状態が「１」であり、かつ、少なくとも１つのビットの状態が「０」となる任意の情報である。例えば、二進数表現において「１」の状態を含まない「０」や「００」、「０」の状態を含まない「１」や「１１」、複数ビットでない「０」や「１」等は認証情報５１４として設定することはできないが、「０１」であればよい。また、ドアホンシステム１では、認証情報５１４における「０１」と「００１」とは明確に区別される。

【００７４】

なお、室内子機２を認証させる正規のオペレータは、認証情報５１４をパスコードとして、別途、知らされているものとする。例えば、パスコードは、製品の保証書やマニュアル等に記載されていて、オペレータはそれを見ることでパスコードを知ることができる。

【００７５】

以下では、認証情報５１４が、二進数表現の「０１０１」である場合を例として説明するが、もちろん認証情報５１４の内容はこれに限定されるものではない。

【００７６】

室内子機２の電源が投入されると、室内子機２は、オペレータによってパスコードが入力されるまで待機する（ステップＳ１１）。

【００７７】

室内子機２をドアホンシステム１において使用可能とするために、オペレータは、当該室内子機２の操作部２２を操作して、予め知らされているパスコードを入力する。なお、オペレータは、室内子機２および屋外カメラ４を設置する前（各部屋や屋外等に設置する前）に、本体ユニット５の近傍で、認証作業を行うものとする。

【００７８】

操作部２２が操作され、パスコードが入力されると、室内子機２はステップＳ１１においてＹｅｓと判定し、入力されたパスコードを記憶装置２１にパスコード２１１として記憶させる。

【００７９】

次に、通信制御部２００が記憶装置２１からパスコード２１１を取得し（ステップＳ１２）、取得したパスコード２１１に基づいて、認証要求情報２１２を送信する回数Ｎを決定する（ステップＳ１３）。ここでは通信制御部２００は、パスコード２１１の最上位ビットの桁番号を「Ｎ」とする。なお、最上位ビットの内容が「０」であるか「１」であるかは問わない。なお、例えば、パスコードとして入力される「０」と「１」の数を単純に数えて回数Ｎを決定してもよい。

【００８０】

次に、通信制御部２００は、ステップＳ１２で取得したパスコード２１１に基づいて、一の認証要求情報２１２を送信するための通信電波の強度を各回ごとに決定する（ステップＳ１４）。

【００８１】

具体的には、パスコード２１１の各ビットごとに、その内容が「１」であるか「０」であるかを判定し、「１」のときは通信電波の強度を「１００」に、「０」のときは「５０」に決定する。すなわち、パスコード２１１が「０１０１」であれば、送信する通信電波の強度は、「１００，５０，１００，５０」と決定される（下位ビットから送信する）。

【００８２】

なお、ここに示す例における「１００」とは、無線通信部２７が送信可能な最大強度の

１００％を意味し、「５０」とは５０％を示す。ただし、このような値に限定されるものではない。

【００８３】

通信電波の強度が決定されると、通信制御部２００はカウンタを１にセットする（ステップＳ１５）。すなわち、カウンタを１にリセットする。なお、ここに言うカウンタとは、認証要求情報２１２の送信回数をカウントするための情報である。

【００８４】

次に、通信制御部２００は、カウンタに示されている値を送信番号２１６として認証要求情報２１２に含めるとともに（ステップＳ２１）、タイマ２０１を参照して、そのときの時間を時間情報２１５として認証要求情報２１２に含める（ステップＳ２２）。これにより、次に送信される認証要求情報２１２が準備されることとなる。

【００８５】

本実施の形態における認証要求情報２１２は、認証前に送信される情報であるから、その後の通信に比べて解読される可能性が高いと言える。また、似た内容の情報が何度も送信される場合にはさらに解読される可能性が高くなるという問題がある。しかし、このように、時間情報２１５を認証要求情報２１２に含めることにより、通信される情報のスクランブルが行われるため、認証のための通信を傍受した第三者に送信内容を解読されることを抑制できる。

【００８６】

認証要求情報２１２が準備されると、通信制御部２００は、そのときのカウンタ値に応じた通信電波の強度を無線通信部２７に伝達する。これにより、無線通信部２７は、認証要求情報２１２を送信する際の通信電波の強度をセットする（ステップＳ２３）。

【００８７】

なお、本実施の形態における通信制御部２００は、パスコード２１１の下位ビットから順に対応する認証要求情報２１２を送信するように無線通信部２７を制御する。すなわち、送信番号２１６は、入力されたパスコードのビット番号（桁番号）と一致する。

【００８８】

ここに示す例において正常にパスコードが入力されていれば、通信制御部２００は、１回目と３回目とにおいて通信電波の強度として「１００」を無線通信部２７に伝達し、２回目と４回目とにおいて通信電波の強度として「５０」を無線通信部２７に伝達する。

【００８９】

通信制御部２００から伝達された数値に基づいて通信電波の強度をセットすると、無線通信部２７は、一の認証要求情報２１２を記憶装置２１から取得して、セットした強度の通信電波で、本体ユニット５に向けて送信する（ステップＳ２４）。このとき送信された認証要求情報２１２は、本体ユニット５により受信されるが、認証要求情報２１２を受信した本体ユニット５の動作については後述する。

【００９０】

次に、通信制御部２００は、カウンタ値と回数Ｎとが等しいか否かを判定し（ステップＳ２５）、等しくない場合は、カウンタをインクリメントして（ステップＳ２６）、ステップＳ２１に戻って処理を繰り返す。このようにして、カウンタ値がＮとなるまで、ステップＳ２４が繰り返され、認証要求情報２１２がＮ回送信される。

【００９１】

一般に、無線通信端末が認証を要求する場合、認証要求情報２１２に相当する情報を１回だけ送信する。しかし、本実施の形態における無線通信端末は、ステップＳ２５によって処理を繰り返すことにより、１回の認証を受ける際に、認証要求情報２１２を複数回送信することとなる。

【００９２】

したがって、１回の無線通信によって認証する場合に比べて、正規の無線通信端末でない無線通信端末を正規の無線通信端末と誤認することを抑制できる。すなわち、オペレータの作業負担を増大させることなく、ドアホンシステム１のセキュリティレベルを向上さ

せることができる。

【００９３】

カウンタ値と回数Ｎとが等しい場合（ステップＳ２５においてＹｅｓ）、Ｎ回の送信が終了したと判定する。そして、無線通信部２７が本体ユニット５からの認証結果情報を受け取るまで待機し、受け取った認証結果情報に基づいて、当該室内子機２の認証が正常に行われたか否かを判定する（ステップＳ２７）。

【００９４】

認証に失敗した場合（ステップＳ２７においてＮｏ）、室内子機２は処理を終了する。この場合、当該室内子機２はドアホンシステム１において使用可能な状態にはならない。なお、このとき、表示部２３に認証に失敗したことを知らせるメッセージを表示してもよい。

【００９５】

一方、認証に成功した場合（ステップＳ２７においてＹｅｓ）、本体ユニット５から送信されるＷＥＰキーを取得して（ステップＳ２８）、記憶装置２１に記憶する。これにより、以後の無線通信では、当該室内子機２は、取得したＷＥＰキーに基づいて暗号化を行って、本体ユニット５との間でデータの送受信を行う。すなわち、当該室内子機２は、ドアホンシステム１において使用可能な状態となる。

【００９６】

ＷＥＰキーを取得すると、室内子機２は、通常待機の状態に移行する（ステップＳ２９）。なお、「通常待機」とは、使用可能な状態で待機していることを指す。すなわち、詳細は説明しないが、訪問者があった場合の報知処理や、複数の室内子機２間における内線通話処理等の通常処理は、ステップＳ２９の通常待機の状態において検出された後、実行される。

【００９７】

以上が、ドアホンシステム１の主に室内子機２の動作である。なお、認証を要求する際の処理は、先述のように、屋外カメラ４においても同様であるので、屋外カメラ４が認証を要求する際の動作については説明を省略する。

【００９８】

図１０および図１１は、本体ユニット５の動作を示す流れ図である。

【００９９】

電源が投入されると、本体ユニット５は所定の初期設定を実行した後、待機状態となる。この待機状態において、本体ユニット５は、様々な状態を監視している。例えば、室外子機３が操作されたか（来訪情報を受信したか）、室内子機２や屋外カメラ４から無線通信を要求されたか等である。

【０１００】

図１０では、無線通信端末の認証を行うために必要な監視ステップについてのみ図示している。具体的には、無線通信の有無（ステップＳ３１）、および認証要求情報２１２の受信を完了したか否か（ステップＳ３６）である。

【０１０１】

待機状態において、無線通信部５７が無線通信を開始すると、本体ユニット５は、ステップＳ３１においてＹｅｓと判定する。このとき、測定部５００は無線通信部２７が受信した通信電波の強度を測定し（ステップＳ３２）、無線通信部２７は受信した情報を記憶装置５１に転送する。

【０１０２】

無線通信部２７が受信した情報が記憶装置５１に転送されると、測定部５００は当該情報にコマンド識別子２１３が含まれているかを解析して、当該情報が認証要求情報２１２であるか否かを判定する（ステップＳ３３）。

【０１０３】

受信した情報が認証要求情報２１２でない場合（ステップＳ３３においてＮｏ）、本体ユニット５は再び待機状態に戻る。一方、受信した情報が認証要求情報２１２である場合

（ステップＳ３３においてＹｅｓ）、タイマ５０２がタイマをセットする（ステップＳ３４）。

【０１０４】

この処理と並行して、測定部５００は、測定情報５１１を生成し、測定した通信電波の強度を、送信番号２１６に従って格納する。このように、本体ユニット５では、一の認証要求情報２１２を受信するたびに、ステップＳ３２ないしＳ３５の処理が実行され、その認証要求情報２１２を受信したときの通信電波の強度が測定情報５１１に送信番号２１６とともに記録される。

【０１０５】

室内子機２や屋外カメラ４のような無線通信端末から送信される通信電波は、本体ユニット５に受信されるときには減衰するため、一般には送信時の強度で受信されない。しかし、正規のオペレータは、通常本体ユニット５の近傍で、認証作業を行うことが可能であるため、認証作業中において受信される通信電波の強度が極端に減衰することもない。また、認証要求情報２１２の複数回の送信は短時間で終了するため、この間に通信の状態が変化することは通常考慮しなくてよい。

【０１０６】

以下の説明では、無線通信端末から「１００」および「５０」の強度で送信された通信電波は、本体ユニット５において、それぞれ「９０」および「４５」の強度で受信されるとして説明する。

【０１０７】

なお、通信電波の強度を測定情報５１１に格納する度に、本体ユニット５は、一旦、待機状態に戻る。

【０１０８】

待機状態において、本体ユニット５は、定期的に認証要求情報２１２の受信を完了しているか否かを監視している（ステップＳ３６）。ステップＳ３６において、受信を完了していないと判定した場合、本体ユニット５は待機状態を継続する。

【０１０９】

なお、ステップＳ３６に言う「受信完了」とは、ある一つの認証要求情報２１２についての受信の完了ではなく、１回の認証に必要な、全ての認証要求情報２１２についての受信の完了である。本実施の形態におけるドアホンシステム１では、先述のように、１回の認証の際に、正常であれば、複数の認証要求情報２１２を送信する。したがって、送信された全ての認証要求情報２１２を本体ユニット５が受信してから、認証を開始するように、ステップＳ３６が設けられている。

【０１１０】

ステップＳ３６における判定の手法を以下に具体的に説明する。なお、判定部５０１は、認証情報５１４のビット数ｎ（ここに示す例ではｎ＝４）を予め取得しているものとする。

【０１１１】

ステップＳ３６が開始されると、まず、判定部５０１は、記憶装置２１に認証要求情報２１２が存在しているか否かを判定する。認証要求情報２１２が存在していない場合とは、すなわち認証要求情報２１２の受信の開始すらされていない状態であるから、この場合判定部５０１は受信を完了していないと判定する。

【０１１２】

認証要求情報２１２が存在している場合、さらに判定部５０１は、存在している認証要求情報２１２のうち最新の認証要求情報２１２に含まれる送信番号２１６（受信した最大の送信番号２１６）を最終番号Ｍとして取得して、「Ｍ」と「ｎ」とを比較し、「Ｍ」が「ｎ」以上であれば、受信完了と判定する。

【０１１３】

このように認証要求情報２１２には送信番号２１６が含まれているので、全ての認証要求情報２１２を受信したか否かを効率的に判定することができる。なお、ｎ番目の認証要

求情報２１２を受信してからも、パスコードの桁数を誤って多く入力した場合には、さらに認証要求情報２１２が送信されてくる可能性がある。

【０１１４】

したがって、詳細は図示していないが、判定部５０１は、最新の認証要求情報２１２を受信してから、ステップＳ３６の判定を行うまでに、所定の時間間隔を設けている。詳細は後述するが、これにより、必要数以上の認証要求情報２１２を送信した無線通信端末（すなわちパスコードが間違っている無線通信端末）を、正規の無線通信端末であると誤認することを抑制できる。すなわち、パスコードとして「００１０１」が入力された場合と、「０１０１」が入力された場合とを見分けることができる。

【０１１５】

一方、「Ｍ」が「ｎ」未満である場合には、さらに、ステップＳ３４においてセットしたタイマ５０２を参照する。このタイマ５０２において、タイムアウトのために設けられている所定の時間が経過していない場合は受信を完了していないと判定し、経過している場合は受信を完了したと判定する。

【０１１６】

このように、タイマ５０２によってタイムアウトを設けることにより、送信された認証要求情報２１２が足りない場合であっても、処理が停止することがない。本実施の形態においては、先述のように複数回の認証要求情報２１２が送信されるが、例えこれらの一部を受信できなかった場合であっても、一旦、認証処理を終了することができる。

【０１１７】

図１２は、測定情報５１１の例を示す図である。図８および図９に示す例では、正規の無線通信端末は、１回目から順に「１００，５０，１００，５０」の強度の通信電波で認証要求情報２１２を４回送信する。

【０１１８】

したがって、本体ユニット５の無線通信部５７がこれを正常に受信すれば、測定情報５１１ａとして示すように、受信した通信電波の強度が、昇順に「９０，４５，９０，４５，０，・・・」と記録される。

【０１１９】

しかし、例えば、送信番号２１６が「２」となる認証要求情報２１２を受信していない場合には、最大の送信番号２１６（Ｍ）は「ｎ」以上となるため、タイムアウトにはならないが、測定情報５１１ｂとして示すように、「９０，０，９０，４５，０，・・・」と記録される。また、例えば、送信番号２１６が「３」以降の認証要求情報２１２を受信できなかった場合には、タイムアウトとなり、測定情報５１１ｃとして示すように、「９０，４５，０，０，０，・・・」となる。

【０１２０】

誤ったパスコードが入力された例を説明すれば、例えば、パスコードとして「００１０１」が入力された場合は、測定情報５１１ｄとして示すように、「９０，４５，９０，４５，４５，・・・」と記録される。また、パスコードとして「１０１」が入力された場合には、測定情報５１１ｅとして示すように「９０，４５，９０，０，０，・・・」と記録される。

【０１２１】

図１０において図示を省略するが、認証に必要な認証要求情報２１２の受信を完了すると（ステップＳ３６においてＹｅｓ）、本体ユニット５は、これまでに受信した認証要求情報２１２を削除する。これにより、以後、改めて無線通信端末から認証要求情報２１２を受信しない限り、本体ユニット５が待機状態に戻っても、ステップＳ３６における判定はＮｏとなる。

【０１２２】

次に、判定部５０１は、測定情報５１１に基づいて、閾値Ｑを求め、閾値情報５１２を生成する（ステップＳ３７）。ここに示す例では、測定情報５１１に記録されている通信電波の強度の最大値Ｖは、「９０」である。したがって、判定部５０１は、Ｑ＝３／４Ｖ

＝６７．５と閾値Ｑを求める。
【０１２３】
認証要求情報２１２が受信されている限り（測定情報５１１が作成されている限り）、すべての通信電波の強度が「０」となることはあり得ないので、判定部５０１は、値が「０」より大きい閾値Ｑを必ず決定できる。
【０１２４】
このようにして閾値Ｑを決定すると、無線通信端末から「５０，５０，５０，５０」の強度の通信電波が送信された場合（入力されたパスコードが「００００」であった場合）、後述する処理において、「１１１１」と誤認する。しかし、先述のように、認証情報５１４には、必ず「０」の状態のビットが含まれるので、「００００」のパスコードが「１１１１」と誤認された場合であっても、これが認証情報５１４と一致することはない。すなわち、誤ったパスコード「００００」によって認証に成功することはない。
【０１２５】
一方、認証情報５１４には、必ず「１」の状態のビットが含まれるので、パスコード「００００」がパスコードとして「正常」であることはない。したがって、「００００」のパスコードが「１１１１」と誤認されたために、認証情報５１４と一致しない状況が生じても、認証結果に問題はない。
【０１２６】
このように、認証作業中において記録された通信電波の最大値Ｖに基づいて閾値Ｑを求めることにより、ドアホンシステム１が設置される環境の通信状態に応じて閾値Ｑを決定することができる。
【０１２７】
なお、上記のように、閾値Ｑを通信状態に応じて決定することは、通信可能な距離にある無線通信端末に、無制限に認証の機会を与えることに相当する。
【０１２８】
しかし、先述のように、認証情報５１４には、必ず「０」の状態のビットが含まれているため、ドアホンシステム１において正常に認証されるためには、送信する通信電波の強度が「５０」であっても（遠方には届きにくい）、本体ユニット５との間で無線通信が可能でなければならない。
【０１２９】
すなわち、必ず「０」の状態のビットが含まれるように認証情報５１４を設定することは、正常に認証される認証作業を行う位置を、比較的近傍の範囲に限定していることを意味し、遠方からの不正アクセスを有効に防止する効果を奏する。
【０１３０】
閾値情報５１２を生成すると、判定部５０１は、測定情報５１１から読み込む情報を指定するためのカウンタを１にセットする（ステップＳ３８）。これにより、送信番号２１６が「１」のときの通信電波の強度から順に読み込まれることとなる。
【０１３１】
次に、カウンタに示される送信番号の通信電波の強度を測定情報５１１から取得して（ステップＳ４１）、取得した通信電波の強度が「０」か否かを判定する（ステップＳ４２）。
【０１３２】
本体ユニット５の無線通信部５７によって受信された以上、そのときの通信電波の強度が「０」となることはない。すなわち、測定情報５１１において、強度が「０」と記録されていることは、該当する送信番号２１６の認証要求情報２１２を受信していないことを示している。したがって、ステップＳ４２の判定は、カウンタによって示される値の送信番号２１６が含まれていた認証要求情報２１２の受信の有無を判定することに相当する。
【０１３３】
このように判定することにより、ドアホンシステム１は、認証要求情報２１２を受信した通信電波が弱かった場合と、そもそも認証要求情報２１２を受信できなかった場合とを

区別することができる。

【０１３４】

取得した通信電波の強度が「０」でない場合（ステップＳ４２においてＮｏ）、当該認証要求情報２１２を受信したときの通信電波の強度に基づいて、そのときの通信電波の状態を判定する。具体的には、閾値情報５１２を参照しつつ、当該強度が、ステップＳ３７で求めた閾値Ｑより大きいか否かを判定する（ステップＳ４３）。

【０１３５】

そして、通信電波の強度が閾値Ｑより大きい場合（ステップＳ４３においてＹｅｓ）、カウンタに示される値に該当するビット（判定情報５１３のビット）に「１」を格納する（ステップＳ４４）。一方、通信電波の強度が閾値Ｑ以下の場合（ステップＳ４３においてＮｏ）、カウンタに示される値に該当するビット（判定情報５１３のビット）に「０」を格納する（ステップＳ４５）。すなわち、ステップＳ４４およびＳ４５によって、１ビットずつ判定情報５１３が生成される。

【０１３６】

判定情報５１３に１ビット分の情報を書き込むと（ステップＳ４４またはＳ４５を実行すると）、判定部５０１はカウンタをインクリメントして（ステップＳ４６）、測定情報５１１から次の情報を読み込むためにステップＳ４１に戻って処理を繰り返す。

【０１３７】

このようにして、ステップＳ４１で取得する通信電波の強度が「０」となるまで（ステップＳ４２においてＹｅｓと判定されるまで）、判定情報５１３の生成が行われる。

【０１３８】

図１３は、判定情報５１３を例示する図である。図１３に示す判定情報５１３ａ，５１３ｂ，５１３ｃ，５１３ｄ，５１３ｅは、それぞれ図１２に示す測定情報５１１ａ，５１１ｂ，５１１ｃ，５１１ｄ，５１１ｅに基づいて生成される判定情報５１３を示す。

【０１３９】

判定情報５１３ａを見れば明らかなように、パスコード「０１０１」が正常に受信された場合に生成される測定情報５１１ａからは、正常に「０１０１」が複合化されている。

【０１４０】

一方、判定情報５１３ｂ，５１３ｃを見れば明らかなように、送信された認証要求情報２１２を一部でも受信できなかった場合は、送信されたパスコード「０１０１」を正常に複合化できない。すなわち、本実施の形態におけるドアホンシステム１では、たまたま１度通信に成功しただけでは、認証に成功することはない。したがって、本体ユニット５の遠方（比較的通信状態が悪く、受信できない場合が発生する）から不正にアクセスしようとする第三者を効果的に排除できる。

【０１４１】

さらに、判定情報５１３ｄ，５１３ｅを見れば明らかなように、パスコードの桁数を誤って入力した場合にも、入力されたパスコードが正確に複合化されるために、結果として誤ったパスコードによって、認証に成功する事態は抑制される。

【０１４２】

ステップＳ４２においてＹｅｓと判定されると、判定部５０１は、判定情報５１３の生成を終了し、認証部５０３が判定情報５１３と認証情報５１４とが一致するか否かを判定する（ステップＳ４７）。

【０１４３】

一致しない場合（ステップＳ４７においてＮｏ）、本体ユニット５は当該室内子機２（認証を要求した無線通信端末）を正規の無線通信端末と認めず、認証結果情報として拒否通知を送信する（ステップＳ４８）。

【０１４４】

一方、一致した場合（ステップＳ４７においてＹｅｓ）、本体ユニット５は当該室内子機２（認証を要求した無線通信端末）を正規の無線通信端末と認め、認証結果情報としてＷＥＰキーを送信する（ステップＳ４９）。

【０１４５】
本体ユニット５は、ステップＳ４８またはＳ４９を実行すると、認証処理を終了して、図１０に示す待機状態に戻る。
【０１４６】
以上のように、本実施の形態におけるドアホンシステム１では、入力されたパスコードを、認証要求情報２１２の送信回数と、認証要求情報２１２を送信する際の通信電波の強度とに対応付けることによって、複雑なパスコードを要求することなく、不正な無線通信端末の誤登録を防止できる。したがって、オペレータの負担を増大させることなく、無線通信におけるセキュリティを確保できる。
【０１４７】
なお、詳細は説明を省略したが、複数の無線通信端末から認証要求情報２１２を受信する場合を想定して、端末識別情報を認証要求情報２１２に含めるようにしてもよい。このとき、複数の無線通信端末に対する認証を並行しておこなってもよいし、一台ずつ認証するようにしてもよい（遅れた端末は待機させるか、一旦拒否する）。
【０１４８】
また、例えば、２世帯住宅で、それぞれ本体ユニット５を設置した場合に、互いの認識情報５１４が共通であれば、各室内子機２が誤った本体ユニット５に登録される可能性がある。したがって、認証情報５１４（パスコード）は、個々の本体ユニット５ごとに固有であることが好ましい。
【０１４９】
一方で、個々の本体ユニット５に対して固有の認証情報５１４を付与すると、認証情報５１４のビット数が増大し、認証のための通信回数（認証要求情報２１２を送信する回数Ｎ）が増大して、登録に時間を要することとなる。
【０１５０】
これを回避するためには、予め複数種類の認証情報５１４を用意しておき、そのいずれか１つが、使用される認証情報５１４として初期設定されていてもよい。また、上記２世帯住宅の例において初期設定された認証情報５１４が重複しないように、オペレータが操作部５２を操作して、初期設定された認証情報５１４を変更できるように構成してもよい。
【０１５１】
また、本体ユニット５を設置する際に、認証情報５１４をオペレータが任意に決定し、本体ユニット５の操作部５２を操作して入力してもよい。
【０１５２】
また、ドアホンシステム１の室内子機２は、認証要求情報２１２を共通鍵（正当なメーカの装置であれば予め記憶している）で暗号化して送信する。本体ユニット５では、受信した認証要求情報２１２を共通鍵で復号化し、メーカ識別コード２１４を解読する。そして、本体ユニット５側で記憶している情報と一致するか否かを判定して、一致しない場合は、認証に失敗したと判定する。偽装端末は一般に正当なメーカの製品でない可能性が高いので、このように構成することにより、本体ユニット５は、不正に電波強度を強化した偽装端末を排除でき、セキュリティレベルを確保することができる。
【０１５３】
＜２．　変形例＞
以上、本発明の実施の形態について説明してきたが、本発明は上記実施の形態に限定されるものではなく様々な変形が可能である。
【０１５４】
例えば、上記実施の形態において通信制御部２００等の機能ブロックはプログラムによってソフトウェア的に実現されると説明したが、その一部または全部を専用の回路によってハードウェア的に実現してもよい。
【０１５５】
また、上記実施の形態に示した各工程は、あくまでも例示であって、その内容および順

序に限定されるものではない。すなわち、同様の効果が得られるのであれば、その内容および順序が適宜変更されてもよい。

【０１５６】

また、上記実施の形態では、パスコードとして認証情報５１４そのものを入力したが、これに限定されるものではない。例えば、パスコードとして、認証情報５１４のビット数と、十進数表現に変換された数字とを入力してもよい。すなわち、認証情報５１４が「０１０１」である場合に、パスコードとして「４（ビット数），９（１０１の十進数表現）」を入力してもよい。一般に二進数表現は桁数が多くなるだけでなく、人間にとって理解（記憶）しにくい数字であるが、パスコードを十進数表現にすることによってオペレータの負担が軽減される。

【０１５７】

また、認証情報５１４のビット数については、本体ユニットと無線通信端末との間で予め決定しておいてもよい。この場合、セキュリティレベルは低下するが、オペレータの負担は軽減される。すなわち、ネットワークに要求されるセキュリティレベルに応じて、決定すればよい。

【０１５８】

また、認証部５０３は必ずしも上記実施の形態に示した判定情報５１３に基づいて判定しなくてもよい。例えば、認証情報５１４が４ビットである場合に、５回目の認証要求情報２１２を受信した時点、あるいは３回の認証要求情報２１２を受信しただけでタイムアウトになった時点で認証に失敗したと判定してもよい。

【０１５９】

また、無線通信端末は、室内子機２や屋外カメラ４のような専用のハードウェアに限定されるものではなく、一般のコンピュータであってもよい。本体ユニット５についても同様である。

【０１６０】

また、上記実施の形態では、測定情報５１１に基づいて演算により求めたが、閾値Ｑは予め適切な値が固定値として定められていてもよい。この場合、認証要求情報５１４として、必ず「１」の状態を１つ以上含むように設定することが好ましい。「１」を送信した場合においても、受信側において固定の閾値Ｑを超えない範囲にある無線通信端末は、「１」が「０」と判定されるために、結果として認証に失敗する。すなわち、無線通信端末から必ず「１」を送信させることにより、認証を許可する範囲（距離）を予め限定することができ、セキュリティレベルを向上できる。

【０１６１】

また、上記実施の形態では、認証要求情報２１２を受信したにもかかわらず、このときの通信電波の強度が閾値Ｑ以下であれば、通信電波の状態が「０」であると判定した。言い換えれば、閾値Ｑ以下でかつ「０」より大きい強度で受信された認証要求情報２１２については、通信電波の状態を「０」と判定していた。しかし、通信電波の状態が「０」か否かを判定するための別の閾値を設定してもよい。

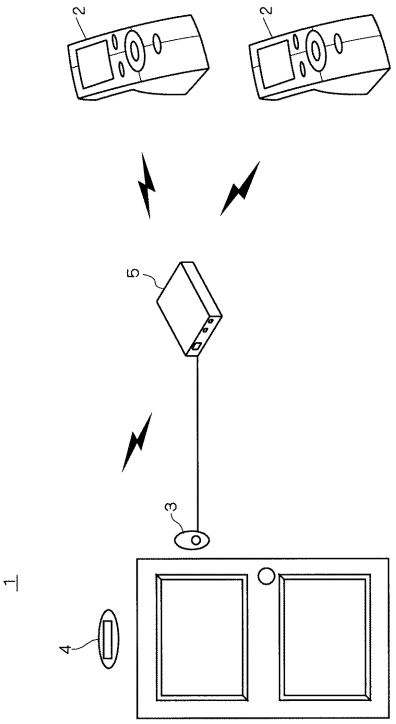
【図面の簡単な説明】

【０１６２】

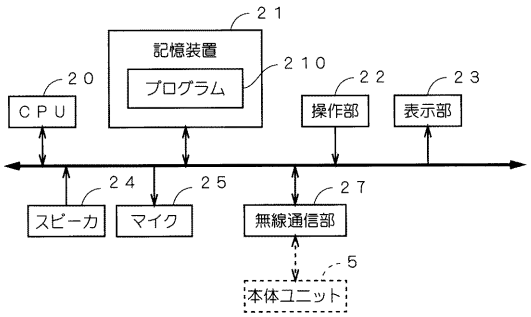
【図１】本発明における通信システムであるドアホンシステムを示す図である。
【図２】室内子機の構成を示すブロック図である。
【図３】室内子機の機能ブロックを情報の流れとともに示す図である。
【図４】認証要求情報の構造を例示する図である。
【図５】屋外カメラの構成を示すブロック図である。
【図６】本体ユニットの構成を示すブロック図である。
【図７】本体ユニットの機能ブロックを情報の流れとともに示す図である。
【図８】室内子機の動作を示す流れ図である。
【図９】室内子機の動作を示す流れ図である。
【図１０】本体ユニットの動作を示す流れ図である。

【図１１】本体ユニットの動作を示す流れ図である。
【図１２】測定情報の例を示す図である。
【図１３】判定情報を例示する図である。
【符号の説明】
【０１６３】
１　ドアホンシステム
２　室内子機
２０，４０，５０　ＣＰＵ
２００　通信制御部
２０１，５０２　タイマ
２１，４１，５１　記憶装置
２１０，４１０，５１０　プログラム
２１１　パスコード
２１２　認証要求情報
２１５　時間情報
２１６　送信番号
２２，４２，５２　操作部
２３，４３，５３　表示部
２７，４７，５７　無線通信部
３　室外子機
４　屋外カメラ
５　本体ユニット
５００　測定部
５０１　判定部
５０３　認証部
５１１，５１１ａ，５１１ｂ，５１１ｃ，５１１ｄ，５１１ｅ　測定情報
５１２　閾値情報
５１３，５１３ａ，５１３ｂ，５１３ｃ，５１３ｄ，５１３ｅ　判定情報
５１４　認証情報

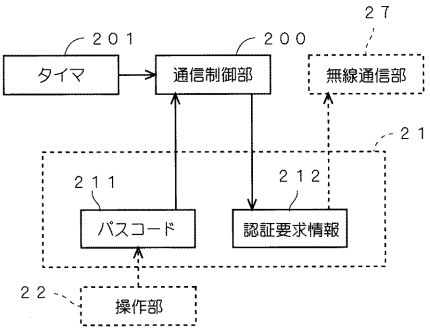
【図１】



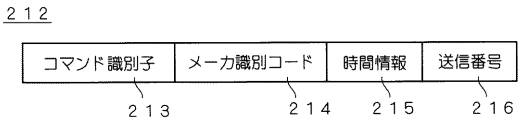
【図２】



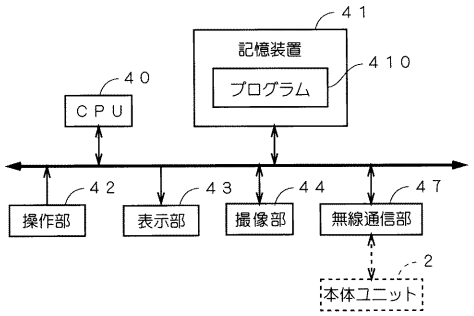
【図３】



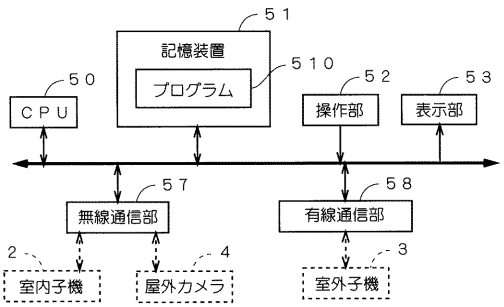
【図４】



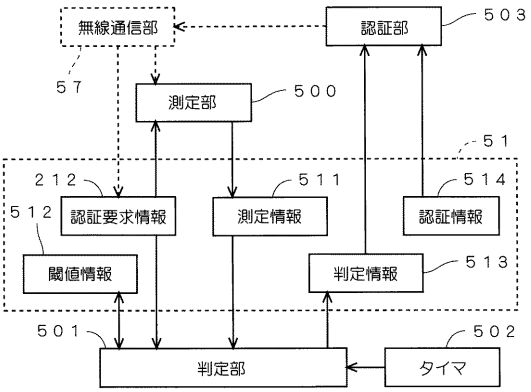
【図５】



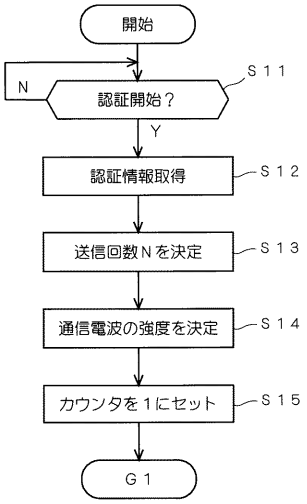
【図６】



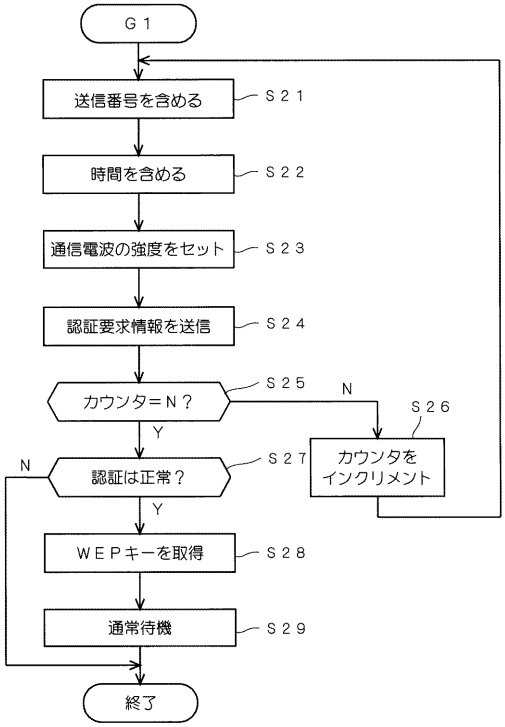
【図７】



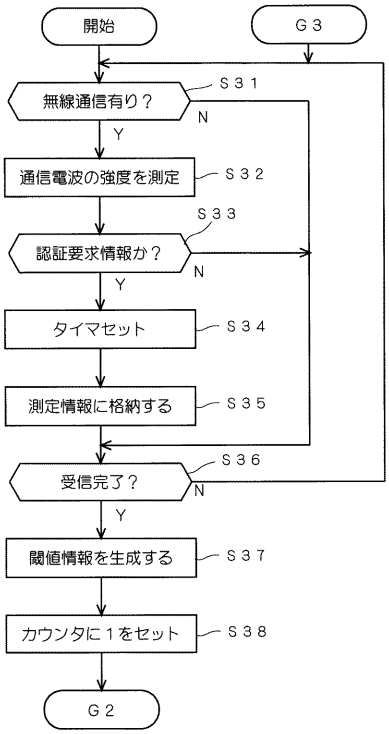
【図８】


開始
認証開始？
S11
N
Y
認証情報取得
S12
送信回数Ｎを決定
S13
通信電波の強度を決定
S14
カウンタを１にセット
S15
Ｇ１

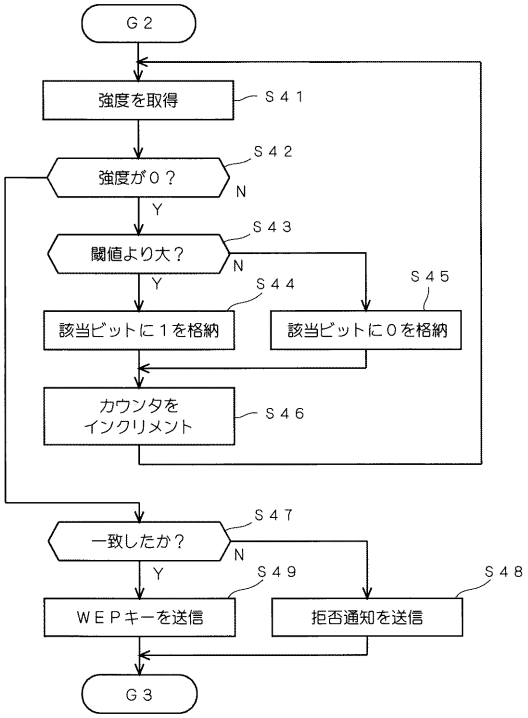
【図９】


Ｇ１
送信番号を含める
S21
時間を含める
S22
通信電波の強度をセット
S23
認証要求情報を送信
S24
カウンタ＝Ｎ？
S25
N
S26
カウンタを
インクリメント
Y
N
認証は正常？
S27
Y
ＷＥＰキーを取得
S28
通常待機
S29
終了

【図１０】


開始
Ｇ３
無線通信有り？
S31
N
Y
通信電波の強度を測定
S32
S33
認証要求情報か？
N
Y
タイマセット
S34
測定情報に格納する
S35
S36
受信完了？
N
Y
閾値情報を生成する
S37
カウンタに１をセット
S38
Ｇ２

【図１１】


Ｇ２
強度を取得
S41
S42
強度が０？
N
Y
S43
閾値より大？
N
Y
S44
S45
該当ビットに１を格納
該当ビットに０を格納
カウンタを
インクリメント
S46
S47
一致したか？
N
Y
S49
S48
ＷＥＰキーを送信
拒否通知を送信
Ｇ３

【図１２】

511a

送信番号	1	2	3	4	5	・・・
強度	90	45	90	45	0	・・・

511b

送信番号	1	2	3	4	5	・・・
強度	90	0	90	45	0	・・・

511c

送信番号	1	2	3	4	5	・・・
強度	90	45	0	0	0	・・・

511d

送信番号	1	2	3	4	5	・・・
強度	90	45	90	45	45	・・・

511e

送信番号	1	2	3	4	5	・・・
強度	90	45	90	0	0	・・・

【図１３】

513a

ビット番号	4	3	2	1
値	0	1	0	1

513b

ビット番号	1
値	1

513c

ビット番号	2	1
値	0	1

513d

ビット番号	5	4	3	2	1
値	0	0	1	0	1

513e

ビット番号	3	2	1
値	1	0	1

フロントページの続き

(51)Int.Cl. F I
H04W 84/10 (2009.01) H04Q 7/00 628

(56)参考文献 特開２００６－１２９０８３（ＪＰ，Ａ）
特開２００４－３３６５５２（ＪＰ，Ａ）
特開２００６－２９５５９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ ８４／１２
Ｇ０９Ｃ １／００
Ｈ０４Ｍ ９／００
Ｈ０４Ｗ １２／０６
Ｈ０４Ｗ ５２／０４
Ｈ０４Ｗ ８４／１０