(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6270491号
(P6270491)
(45)発行日　平成30年1月31日(2018.1.31)　(24)登録日　平成30年1月12日(2018.1.12)

(51)Int.Cl.　F I
G06F 21/44 (2013.01)　G06F 21/44 350

請求項の数 7 (全 15 頁)

(21)出願番号　特願2014-3639(P2014-3639)
(22)出願日　平成26年1月10日(2014.1.10)
(65)公開番号　特開2015-132947(P2015-132947A)
(43)公開日　平成27年7月23日(2015.7.23)
審査請求日　平成28年12月19日(2016.12.19)

(73)特許権者　000000284
大阪瓦斯株式会社
大阪府大阪市中央区平野町四丁目１番２号
(74)代理人　110001818
特許業務法人Ｒ＆Ｃ
(72)発明者　鈴木　智之
大阪府大阪市中央区平野町四丁目１番２号
大阪瓦斯株式会社内
(72)発明者　岡本　秀樹
大阪府大阪市中央区平野町四丁目１番２号
大阪瓦斯株式会社内
(72)発明者　八木　政彦
大阪府大阪市中央区平野町四丁目１番２号
大阪瓦斯株式会社内

最終頁に続く

(54)【発明の名称】認証方法及び認証システム

(57)【特許請求の範囲】
【請求項１】
認証された機器にサービスを提供するホスト機器と、当該サービスを利用するゲスト機器とが接続されたネットワークにおいて、前記ホスト機器が前記サービスの提供先として前記ゲスト機器を認証する認証方法であって、
前記ホスト機器に対しユーザーが所定の待受開始操作を行うことで、前記ホスト機器が前記ゲスト機器からの通信を待ち受ける待受状態に移行する待受開始工程と、
前記ゲスト機器に対しユーザーが所定の接続操作を行うことで、前記ゲスト機器が、自身のＩＰアドレスと前記ホスト機器を探す旨の情報とを含む探索用電文を、前記ネットワーク内にブロードキャストする探索工程と、
前記ホスト機器が前記ゲスト機器から前記探索用電文を受信したときに、前記ホスト機器が、自身のＩＰアドレスを前記ゲスト機器に通知する通知工程と、
前記ゲスト機器が前記ホスト機器のＩＰアドレスを受信したときに、前記ゲスト機器が、前記ホスト機器による認証を要求する旨の情報と前記ゲスト機器を一意に識別可能な識別子とを含む認証要求電文を前記ホスト機器に送信する認証要求工程と、
前記ホスト機器が前記認証要求電文を受信したときに、前記ホスト機器が、前記ゲスト機器を認証するか否かを、ユーザーが所定の認証操作を行うことで決定する認証決定工程と、
を順に実行する認証方法。
【請求項２】

前記待受開始操作及び前記認証操作が、前記ホスト機器に対して物理的な状態変化を伴う当該ホスト機器に特有の操作である請求項１に記載の認証方法。
【請求項３】
前記ホスト機器が、前記認証決定工程において認証済みの前記ゲスト機器の前記識別子を記憶する識別子データベースを備え、
前記ゲスト機器が前記ホスト機器の前記ＩＰアドレスに対して通信不能となった場合に、
前記探索工程、前記通知工程、前記認証要求工程を順次実行し、
前記ホスト機器が、前記認証要求電文に含まれる識別子が、前記識別子データベースに記憶されている場合に前記ゲスト機器を自動的に認証する自動認証工程を実行する請求項１または２に記載の認証方法。
【請求項４】
前記ホスト機器が、
自身のＩＰアドレスを定期的に記憶するためのアドレス記憶手段と、
自身のＩＰアドレスと、前記アドレス記憶手段に記憶されたＩＰアドレスとが同一であるかを監視するアドレス監視手段と、を備え、
前記アドレス監視手段が、ＩＰアドレスが同一でないことを検知した場合に、
前記待受状態に移行するように構成された請求項３に記載の認証方法。
【請求項５】
前記ゲスト機器が、外部表示手段を備えた携帯端末であり、
前記認証決定工程において、前記ホスト機器が前記認証要求電文を受信した旨を、前記携帯端末の外部表示手段に表示するように構成された請求項１～４の何れか一項に記載の認証方法。
【請求項６】
前記ホスト機器と同一の場所に、外部表示手段を備えたリモコンにより操作可能な熱電併給装置が設けられ、
前記認証決定工程において、前記ホスト機器が前記認証要求電文を受信した旨を、前記リモコンの外部表示手段に表示するように構成された請求項１～４の何れか一項に記載の認証方法。
【請求項７】
前記ホスト機器と前記ゲスト機器とを備えて構成され、請求項１～６のいずれか一項に記載の認証方法を実行する認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証された機器にサービスを提供するホスト機器と、当該サービスを利用するゲスト機器とが接続されたネットワークにおいて、前記ホスト機器が前記サービスの提供先として前記ゲスト機器を認証する認証方法及び認証システムに関する。
【背景技術】
【０００２】
上述のようなホスト機器におけるゲスト機器の認証方法としては、例えば非特許文献１に示すＷＰＳ(Wi-Fi Protected Setup)といった技術が一般的に知られている。ＷＰＳにおいては、ユーザーが略同時刻にゲスト機器及びホスト機器の接続開始ボタンを押すことで、ゲスト機器及びホスト機器が相互に認証し合い、自動的にネットワーク接続が完了する。具体的には、例えば特許文献１には、ホスト機器としての無線ＬＡＮ基地局（アクセスポイント）と、ゲスト機器としての無線ＬＡＮ端末（ステーション）とをＷＰＳにより接続する方法が開示されている。
【先行技術文献】
【特許文献】
【０００３】

【特許文献１】特開２０１０－１５７８８９号公報
【非特許文献】
【０００４】
【非特許文献１】Wi-Fi Alliance, “Wi-Fi Protected Setup Specification”, Version 1.0h, December, 2006
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、ＷＰＳにおいては、ホスト機器のＷＰＳ開始ボタンが押されてから、ゲスト機器の接続開始ボタンが押されるまでの間に、その他のゲスト機器からＷＰＳによる接続要求が行われると、当該その他のゲスト機器がホスト機器によって認証されるおそれがあった。すなわち、ＷＰＳによる通信を開始した直後に、ホスト機器が不正なゲスト端末を自動的に認証するおそれがあった。本願発明は、このような事情に鑑みてなされたものであり、その目的は、ホスト機器によるゲスト機器の認証を、ユーザーに必要以上に手間をかけることなく簡便、かつ、不正な端末の認証を回避できるように安全に実行できる方法を確立することにある。
【課題を解決するための手段】
【０００６】
上記目的を達成するための本願発明の特徴は、認証された機器にサービスを提供するホスト機器と、当該サービスを利用するゲスト機器とが接続されたネットワークにおいて、前記ホスト機器が前記サービスの提供先として前記ゲスト機器を認証する認証方法であって、
前記ホスト機器に対しユーザーが所定の待受開始操作を行うことで、前記ホスト機器が前記ゲスト機器からの通信を待ち受ける待受状態に移行する待受開始工程と、
前記ゲスト機器に対しユーザーが所定の接続操作を行うことで、前記ゲスト機器が、自身のＩＰアドレスと前記ホスト機器を探す旨の情報とを含む探索用電文を、前記ネットワーク内にブロードキャストする探索工程と、
前記ホスト機器が前記ゲスト機器から前記探索用電文を受信したときに、前記ホスト機器が、自身のＩＰアドレスを前記ゲスト機器に通知する通知工程と、
前記ゲスト機器が前記ホスト機器のＩＰアドレスを受信したときに、前記ゲスト機器が、前記ホスト機器による認証を要求する旨の情報と前記ゲスト機器を一意に識別可能な識別子とを含む認証要求電文を前記ホスト機器に送信する認証要求工程と、
前記ホスト機器が前記認証要求電文を受信したときに、前記ホスト機器が、前記ゲスト機器を認証するか否かを、ユーザーが所定の認証操作を行うことで決定する認証決定工程と、
を順に実行する点にある。
【０００７】
上記特徴構成により、ゲスト機器とホスト機器とが互いにＩＰアドレスを把握しておらず、通信が確立していない状況であっても、ユーザーは待受開始操作及び接続操作を行うだけで、自動的に相互に接続可能な状態とすることができる。そして、認証決定工程において、ホスト機器がゲスト機器を認証するか否かをユーザーの意思によって決定することができるため、ホスト機器が不正な端末を自動的に認証してしまうという問題を回避することができる。すなわち、ホスト機器によるゲスト機器の認証を、ユーザーに必要以上に手間をかけることなく簡便、かつ、不正な端末の認証を回避できるように安全に実行できる方法を確立することができる。
【０００８】
さらに別の特徴としては、前記待受開始操作及び前記認証操作が、前記ホスト機器に対して物理的な状態変化を伴う当該ホスト機器に特有の操作である点にある。
【０００９】
上記特徴構成によれば、ホスト機器があらかじめ備えている特有の操作に、待受開始操

作及び前記認証操作を割り当てるため、待受開始操作及び前記認証操作用に専用の操作部（例えばスイッチなど）を備えていない場合であっても、待受開始工程や認証決定工程を実行することができる。すなわち、従来型のホスト機器の筐体を流用することが可能となり、安価に本願発明の方法を実装した製品を製作することができる。また、例えば、ホスト機器としてガスコンロを用いる場合にはガスバーナーの点火、給湯器の場合には出湯、など物理的な状態変化を伴う操作とするため、電子的な不正操作によって待受開始工程や認証決定工程が実行されることを抑制することができる。

【００１０】

加えて、前記ホスト機器が、前記認証決定工程において認証済みの前記ゲスト機器の前記識別子を記憶する識別子データベースを備え、

前記ゲスト機器が前記ホスト機器の前記ＩＰアドレスに対して通信不能となった場合に、

前記探索工程、前記通知工程、前記認証要求工程を順次実行し、

前記ホスト機器が、前記認証要求電文に含まれる識別子が、前記識別子データベースに記憶されている場合に前記ゲスト機器を自動的に認証する自動認証工程を実行する構成とすると好適である。

【００１１】

上記特徴構成によれば、例えば、ルータによりホスト機器のＩＰアドレスが振り直されたときなど、ゲスト機器が以前のホスト機器のＩＰアドレスを用いて接続できなくなった場合であっても、自動的にゲスト機器からホスト機器への再接続を実現することができる。すなわち、ホスト機器によるゲスト機器の認証を、より一層ユーザーに必要以上に手間をかけることなく簡便、かつ、安全に実行できる方法を確立することができる。

【００１２】

さらに、前記ホスト機器が、

自身のＩＰアドレスを定期的に記憶するためのアドレス記憶手段と、

自身のＩＰアドレスと、前記アドレス記憶手段に記憶されたＩＰアドレスとが同一であるかを監視するアドレス監視手段と、を備え、

前記アドレス監視手段が、ＩＰアドレスが同一でないことを検知した場合に、

前記待受状態に移行するように構成すると好適である。

【００１３】

上記特徴構成によれば、ホスト機器のＩＰアドレス変更され、ゲスト機器がホスト機器と接続できなくなるおそれが生じた場合に、自動的にホスト機器が待受状態に移行するため、ユーザーが特別な操作を行うことなく、探索工程においてゲスト機器からホスト機器に通信を行うことができる。

【００１４】

さらに、前記ゲスト機器が、外部表示手段を備えた携帯端末であり、

前記認証決定工程において、前記ホスト機器が前記認証要求電文を受信した旨を、前記携帯端末の外部表示手段に表示するように構成すると好適である。

【００１５】

上記特徴構成によれば、例えば、ホスト機器が、認証操作を行う必要がある旨をユーザーに通知する手段を備えていない場合であっても、認証操作を行う必要があることを、携帯端末を介して即座に知ることができる。すなわち、ホスト機器によるゲスト機器の認証を、よりユーザーが簡便に実行できる方法を確立することができる。

【００１６】

または、前記ホスト機器と同一の場所に、外部表示手段を備えたリモコンにより操作可能な熱電併給装置が設けられ、

前記認証決定工程において、前記ホスト機器が前記認証要求電文を受信した旨を、前記リモコンの外部表示手段に表示するように構成すると好適である。

【００１７】

上記特徴構成によれば、例えば、ホスト機器が、認証操作を行う必要がある旨をユーザ

ーに通知する手段を備えていない場合であっても、認証操作を行う必要があることを、熱電併給装置のリモコンを介して即座に知ることができる。すなわち、ホスト機器によるゲスト機器の認証を、よりユーザーが簡便に実行できる方法を確立することができる。また、既に設置された熱電併給装置のリモコンを転用するため、ホスト機器にユーザーに通知する手段を備えさせる必要がなく、安価に本願発明の方法を実行可能な製品を製作することができる。

【００１８】

また、前記ホスト機器と前記ゲスト機器とを備えて構成され、上述の認証方法を実行する認証システムとすることができる。

【００１９】

上記特徴構成によれば、ホスト機器によるゲスト機器の認証を、ユーザーに必要以上に手間をかけることなく簡便、かつ、不正な端末の認証を回避できるように安全に実行できる方法を確立した認証システムを実現することができる。

【図面の簡単な説明】

【００２０】

【図１】第１実施形態に係る認証システムのブロック図

【図２】初期接続設定モードのシーケンス図

【図３】認証システムにおいて用いる電文構成を示す図

【図４】自動再接続設定モードのシーケンス図

【図５】第２実施形態に係る認証システムのブロック図

【図６】第３実施形態に係る認証システムのブロック図

【発明を実施するための形態】

【００２１】

以下では、本願発明に係る認証方法を用いた認証システムの実施形態について図を用いて説明する。

〔第１実施形態〕

（（認証システムの構成））

図１に示すように、本実施形態に係る認証方法は、認証された機器に通信手段１２を介してサービスを提供するホスト機器１と、通信手段２２を介して当該サービスを利用するゲスト機器２とが接続されたネットワークにより構成される認証システムにおいて、ホスト機器１がサービスの提供先としてゲスト機器２を認証する認証方法である。本実施形態においては、ホスト機器１としてガスコンロを、ゲスト機器２として、外部表示手段２４を備えた携帯端末を用いる場合の一例を示す。より具体的には、例えば、ゲスト機器２として、通信手段２２として無線ＬＡＮチップを備えた、いわゆるスマートフォンを用いることができる。

【００２２】

本明細書における「サービス」とは、ホスト機器１のユーザーにとって有益な情報、及びユーザーによってホスト機器１を操作可能とする手段を意味する。具体的には、ホスト機器１はサービスとして、ホスト機器１の動作状態を示す情報や、ホスト機器１のリモートコントロール機能などを提供する。これらのサービスは、ソフトウェアにより提供される。

【００２３】

本実施形態においては、ホスト機器１及びゲスト機器２がＩＰネットワークにより通信可能なように接続される。より詳しくは、ホスト機器１及びゲスト機器２は、同一のローカルネットワークに接続される。具体的には、例えば、家庭や事業所などの屋内において、（図示しない）ＤＨＣＰサーバ機能を有するルータに、ホスト機器１及びゲスト機器２が無線又は有線により接続される。このような構成により、ホスト機器１及びゲスト機器２は、図１に示すように、双方向に通信が可能となっている。通信にあたっては、互いのＩＰアドレスを用いて相互に通信を行うことや、ブロードキャストによる一方向通信が可能である。これらの通信には、例えば、ＴＣＰプロトコルやＵＤＰプロトコルを利用する

ことができる。
【００２４】
（ホスト機器の構成）
ホスト機器１は、制御手段１１、通信手段１２、記憶領域１３、識別子データベース１４、ならびに通信操作部１５及び通常操作部１６を備える。制御手段１１は、ホスト機器１に設けられた各部（制御手段１１、通信手段１２、記憶領域１３、識別子データベース１４）を制御し、所定の動作を行わせるための手段で、公知の演算処理装置を用いることができる。本実施形態においては、制御手段１１には、アドレス監視手段１１１が含まれる。アドレス監視手段１１１は、制御手段１１上で動作するソフトウェアとして構成される。
【００２５】
アドレス監視手段１１１は、現在、ホスト機器１の通信手段１２に割り当てられている自身のＩＰアドレス１２１と、記憶領域１３に記憶された直前ＩＰアドレス１３２とが同一であるかを監視する。ここで、記憶領域１３は、本願発明における「アドレス記憶手段」に相当する。
【００２６】
通信手段１２は、ゲスト機器２と通信するための手段であり、無線又は有線によりゲスト機器２を含むネットワークに接続するように構成されている。具体的には、通信手段１２としては、無線ＬＡＮチップや有線ＬＡＮチップ、もしくは近距離無線通信用のチップなどを用いることができる。通信手段１２には、図示しないＤＨＣＰサーバから、もしくはユーザーによる手動設定によりＩＰアドレス１２１が割り振られる。通信手段１２は、ＩＰアドレス１２１を用いてゲスト機器２と通信を行う。また、ホスト機器１は、当該機器を一意に識別可能な識別子１２２を記憶するように構成されている。本実施形態においては、識別子１２２として通信手段１２に備えられたＭＡＣアドレスを用いる。
【００２７】
ホスト機器１は、ゲスト機器２に対して、ネットワークを介してサービスとして、ホスト機器１の動作状態を示す情報や、ホスト機器１のリモートコントロール機能などを提供する。具体的には、例えば、ホスト機器１がガスコンロの場合、ホスト機器１は、ガスバーナの点火状態をゲスト機器２に送信するし、ゲスト機器２は受信したガスバーナの点火状態を、当該ゲスト機器２の外部表示手段２４上に表示する。ここで、ホスト機器１は、ゲスト機器２に対してサービスを提供するにあたり、あらかじめ当該ゲスト機器２に対しサービスを実行して良いかどうかを認証するための認証作業を行うように構成されている。すなわち、ホスト機器１は、あらかじめ認証したゲスト機器２にのみサービスを提供するように構成されている。
【００２８】
本実施形態においては、ホスト機器１としてのガスコンロは、ガスバーナの着火スイッチなどの加熱調理のために用いる通常操作部１６とは別に、上記認証作業に用いるための通信操作部１５を備える。通信操作部１５としては、タッチパネルや物理的なスイッチを用いることができる。より具体的には、ホスト機器１は、図２の初期接続モードＭ１１のシーケンス図に示すように、通信操作部１５として、後述する待受開始工程Ｓ１における待受開始操作＃１を行うためのスイッチ１５ａ及び、認証決定工程Ｓ５における認証操作＃３における許可または不許可を選択可能なスイッチ１５ｂを備える。
【００２９】
記憶領域１３は、任意の情報を読み書き可能に構成され、例えば、揮発性メモリもしくは不揮発性メモリを用いることができる。記憶領域１３には、ホスト機器１の種別を示す機種種別１３１や、後述するアドレス監視手段１１１により取得された直前のＩＰアドレスである直前ＩＰアドレス１３２が記憶される。具体的には、機種種別１３１は、あらかじめ機器の種別ごとに定められたコード（番号）として記憶される。
【００３０】
また、ホスト機器１は、認証作業によって今までに認証したゲスト機器２の識別子２２

２を記憶した識別子データベース１４を備える。本実施形態においては、例えば、識別子データベース１４は最大で、ゲスト機器２の１０台分に相当する識別子２２２を記憶可能に構成される。

【００３１】

（ゲスト機器の構成）

ゲスト機器２は、制御手段２１、通信手段２２、記憶領域２３、及び外部表示手段２４を備える。制御手段２１は、ゲスト機器２に設けられた各部（通信手段２２、記憶領域２３、及び外部表示手段２４）を制御し、所定の動作を行わせるための手段で、公知の演算処理装置を用いることができる。具体的には、制御手段２１は、例えば、通信手段２２を介して受信したデータに基づいて、外部表示手段２４に当該データをユーザーに表示するように構成されている。

【００３２】

通信手段２２は、ホスト機器１と通信するための手段で、ホスト機器１の通信手段１２と同様に、無線又は有線によりホスト機器１を含むネットワークに接続するように構成されている。具体的には、ゲスト機器２の通信手段２２としては、無線ＬＡＮチップや有線ＬＡＮチップ、もしくは近距離無線通信用のチップなどを用いることができる。通信手段２２には、図示しないＤＨＣＰサーバから、もしくはユーザーによる手動設定によりＩＰアドレス２２１が割り振られる。通信手段２２は、ＩＰアドレス２２１を用いてホスト機器１と通信を行う。また、ゲスト機器２は、当該機器を一意に識別可能な識別子２２２を記憶するように構成されている。本実施形態においては、識別子２２２として通信手段２２に備えられたＭＡＣアドレスを用いる。

【００３３】

記憶領域２３は、任意の情報を読み書き可能に構成され、例えば、揮発性メモリもしくは不揮発性メモリを用いることができる。記憶領域２３には、ホスト機器１の種別を示す機種種別２３１が記憶される。機種種別２３１は、ホスト機器１の機種種別１３１と同様に、あらかじめ機器の種別ごとに定められたコード（番号）として記憶される。

【００３４】

外部表示手段２４は、ゲスト機器２のユーザーに各種の情報を表示する手段で、具体的には、例えば、ディスプレイを用いることができる。本実施形態においては、ゲスト機器２の外部表示手段２４は、ユーザーによって各種の入力を行うための入力手段としても機能するように構成される。具体的には、外部表示手段２４としてタッチパネルを内蔵したディスプレイを用いる。

【００３５】

また、ゲスト機器２は、図２に示す様に、探索工程Ｓ２において、所定の接続操作＃２を実行可能に構成されている。本実施形態においては、制御手段２１により外部表示手段２４に接続操作＃２のためのユーザーインターフェースが表示され、当該ユーザーインターフェースを操作することで、ゲスト機器２からホスト機器１への接続が開始されるように構成することができる。具体的には、外部表示手段２４に接続操作＃２のためのボタンを表示し、外部表示手段２４に表示された当該ボタンをユーザーがタップしたときに、ゲスト機器２からホスト機器１への接続が開始される。

【００３６】

（（認証方法））

以下では、ホスト機器１によるゲスト機器２の認証方法について、図を用いて説明する。

【００３７】

（電文の形式）

本実施形態に係る認証方法を説明するにあたり、まず、本実施形態に係る認証システムにおいてホスト機器１とゲスト機器２との間で送受信する電文の形式について説明する。図３に電文形式の一例を示す。

【００３８】

本実施形態においては、ホスト機器１とゲスト機器２との間では、ＴＣＰ／ＩＰまたはＵＤＰ／ＩＰプロトコルに沿って通信が行われる。このため、通信に用いる電文には、ＩＰヘッダ部に図３に示すように送信元（すなわち、ホスト機器１またはゲスト機器２）のＩＰアドレス及び、送信先のＩＰアドレスが含まれる。また、ＴＣＰまたはＵＤＰヘッダ部には、送信元ポート番号及び送信先ポート番号が含まれる。

【００３９】

さらに、ＴＣＰまたはＵＤＰデータ部には、本発明に係る認証方法に用いる「送信元認証キー」及び「送信先認証キー」が含まれる。また、必要に応じて「機種種別」及び「機器コード」などが含まれる。ここで、認証キーとしては、ホスト機器１及びゲスト機器２を一意に識別可能な値を用いれば良い。具体的には、例えば、ユーザーによりあらかじめ定められた値や、各機器の製造番号などを用いることが可能である。本実施形態においては、認証キーとして、ホスト機器１の識別子１２２またはゲスト機器２の識別子２２２が用いられる。

【００４０】

（初期認証通信）

本実施形態において、ホスト機器１にゲスト機器２が初めて認証を要求する場合の通信を、「初期認証通信」と呼ぶ。図２に、初期認証通信における通信シーケンスを示す。図中では、初期認証通信を実行中のホスト機器１及びゲスト機器２の状態を、初期接続モードＭ１１及び初期接続モードＭ２１として示している。

【００４１】

本実施形態に係る認証方法においては、初期認証通信において、ホスト機器１とゲスト機器２とが協調して順に、待受開始工程Ｓ１、探索工程Ｓ２、通知工程Ｓ３、認証要求工程Ｓ４、及び認証決定工程Ｓ５を実行する。以下では、図２を用いて各工程を順に説明する。

【００４２】

１．待受開始工程Ｓ１

初期認証通信においては、まず、ユーザーが、ホスト機器１に対し所定の待受開始操作＃１を行う。ホスト機器１は、待受開始操作＃１を受付けると、ゲスト機器２からの通信を待ち受ける待受状態に移行する。より具体的には、ホスト機器１は、ゲスト機器２との初期認証通信を行うための待受状態に移行する。ここで、待受開始工程Ｓ１は、図２に示すようにホスト機器１が待受状態に移行してから、実際に初期接続モードＭ１１に移行するまで（初期認証通信を開始するまで）の間が相当する。

【００４３】

なお、本実施形態においては、ホスト機器１は、既に識別子データベース１４にあらかじめ定められた所定台数分、ゲスト機器２の識別子２２２が記憶されている場合には、待受状態に移行しないように構成されている。この場合に、識別子データベース１４が満杯である旨をユーザーに通知するように構成すると、ユーザーの利便性が向上し好適である。

【００４４】

ここで、「待受状態」とは、ホスト機器１がゲスト機器２からの通信を待ち受け可能な状態を意味する。より具体的には、例えば、ゲスト機器２を認証するためのプログラムが起動した状態、もしくはゲスト機器２を認証するためのプログラムが起動した状態で、かつ、ゲスト機器２を認証するための通信に用いる通信ポートが開放された状態を意味する。本実施形態においては、ホスト機器１は、待受状態、後述する初期接続モードＭ１１、及び自動再接続設定モードＭ１２のときに通信ポートを開放し、それ以外のときには通信ポートは閉じるように構成されている。待受状態において、ホスト機器１が、ゲスト機器２からの探索用電文ｐ１を受信すると、認証のためのプログラムが実行される。ただし、本実施形態においては、ホスト機器１は、待受状態においてあらかじめ定められた所定時間内にゲスト機器２からの探索用電文ｐ１を受信しなかった場合には、待受状態を終了するように構成されている。ここでの、所定時間としては、例えば、１日に設定することが

できる。

【００４５】

２．探索工程Ｓ２

次に、ユーザーが、ゲスト機器２に対し所定の接続操作＃２を行う。ゲスト機器２は、接続操作＃２を受付けると、自身のＩＰアドレス２２１とホスト機器１を探す旨の情報とを含む探索用電文ｐ１とを、ネットワーク内にブロードキャストする。より詳しくは、ゲスト機器２は、電文に、自身のＩＰアドレス２２１と探索用電文ｐ１とを含めてブロードキャストする。また、本実施形態においては、探索用電文ｐ１の「機種種別」に自身の機種種別２３１を設定する。ここで、探索用電文ｐ１をブロードキャストする工程が探索工程Ｓ２に相当する。

【００４６】

本実施形態において、具体的には例えば、「機種種別」にゲスト機器２の機種種別２３１である「0x80」（以下、接頭語の0xは１６進数を示す。）が入力される。また、「送信先認証キー」及び「送信元認証キー」には「0xFFFFFF」が設定される。すなわち、「送信先認証キー」及び「送信元認証キー」にはホスト機器１の識別子１２２にはなり得ない値が設定される。

【００４７】

なお、後述する通知工程Ｓ３におけるホスト機器１からの応答（応答電文ｐ２）が所定時間内に返ってこなかった場合には、ゲスト機器２は、再度、探索用電文ｐ１をブロードキャストする。それでもホスト機器１からの応答がない場合、所定回数を上限として繰り返し、探索用電文ｐ１をブロードキャストする。本実施形態においては、例えば、所定時間を５秒、上限となる所定回数を６回としている。

【００４８】

３．通知工程Ｓ３

続いて、ホスト機器１がゲスト機器２から探索用電文ｐ１を受信すると、自身のＩＰアドレス１２１を含む応答電文ｐ２をゲスト機器２に通知する。本実施形態においては、ホスト機器１は、受信した探索用電文ｐ１に含まれる「機種種別」が、適正か否かを確認し、正しくない場合には、ゲスト機器２に応答電文ｐ２を返さず、正しい場合にのみゲスト機器２に自身のＩＰアドレス１２１を含む応答電文ｐ２をゲスト機器２に通知するように構成される。ここで、適正か否かの判断については、例えば、ホスト機器１に、あらかじめ適正とみなす機種種別のリストを記憶しておき、当該リストと一致するか否かをもって判断するように構成することができる。

【００４９】

応答電文ｐ２に関してより具体的には、「送信元ＩＰアドレス」に自身のＩＰアドレス１２１が設定され、「送信先ＩＰアドレス」に、受信した探索用電文ｐ１の送信元ＩＰアドレスであるゲスト機器２のＩＰアドレス２２１を設定することで、ゲスト機器２にホスト機器１のＩＰアドレス１２１を通知する。これにより、ゲスト機器２は、ホスト機器１のＩＰアドレス１２１を把握することができ、以降では、ホスト機器１のＩＰアドレス１２１を用いて、ＴＣＰ／ＩＰ通信を行うことができる。

【００５０】

本実施形態においては、応答電文ｐ２には「機種種別」にホスト機器１の機種種別１３１が設定される。このような構成とすることにより、ネットワーク内に、複数のホスト機器１が存在する場合（例えば、ホスト機器１としてのガスコンロ及び熱電併給装置などが存在する場合）においても、ゲスト機器２は、接続対象とするホスト機器１との通信を選択的に確立することができる。

【００５１】

４．認証要求工程Ｓ４

ゲスト機器２は、ホスト機器１のＩＰアドレス１２１を受信すると、ホスト機器１による認証を要求する旨の情報とゲスト機器２を一意に識別可能な識別子２２２とを含む認証要求電文ｐ３をホスト機器１に送信する。本実施形態においては、認証要求電文ｐ３を送

信するにあたり、ゲスト機器２は、まず受信した応答電文ｐ２の「機種種別」が接続対象のものと一致するかを確認する。確認した結果、一致しない場合には、何もせず待機し、一致した場合には、認証要求電文ｐ３の「送信元認証キー」にゲスト機器２の識別子２２２を設定し、ホスト機器１に送信する。

【００５２】

５．認証決定工程Ｓ５

ホスト機器１は、認証要求電文ｐ３を受信すると、ゲスト機器２を認証するか否かを、ユーザーが所定の認証操作＃３を行うことで決定するように構成されている。具体的には、本実施形態においては、ホスト機器１が認証要求電文ｐ３を受信すると、ホスト機器１が認証要求電文ｐ３を受信した旨を、ゲスト機器２である携帯端末の外部表示手段２４に表示するように構成されている。すなわち、ホスト機器１は、認証要求電文ｐ３を受信した場合に、ゲスト機器２に対して、認証要求電文ｐ３を受信した旨を通知する。当該通知を受信したゲスト機器２は、外部表示手段２４に、その旨を表示する。このとき、当該旨の通知と合わせて、ホスト機器１において認証操作＃３を行うことを促すメッセージを表示すると良い。このような構成とすれば、ユーザーが認証操作＃３を行うタイミングを的確に把握することができ、認証操作＃３を忘れることを防止することができる。以上の工程が認証決定工程Ｓ５に相当する。

【００５３】

ここで、ユーザーにより、ホスト機器１に用意された通信操作部１５が操作されると、その結果がゲスト機器２に通知される。具体的には、通信操作部１５において許可が選択された場合には、ホスト機器１の識別子１２２が、ゲスト機器２に通知される。一方、不許可が選択された場合には、ゲスト機器２には、接続に失敗した旨が通知される。より詳しくは、許可が選択された場合には、ホスト機器１からゲスト機器２に送信される結果通知電文ｐ４の「送信元認証キー」にホスト機器１の識別子１２２が設定され、不許可の場合には、「送信元認証キー」に識別子１２２としてとり得ない値、例えば「0xFFFFFF」が設定される。以上で、ホスト機器１及びゲスト機器２による初期認証通信は終了する。

【００５４】

（自動再認証通信）

本実施形態に係る認証方法においては、ＩＰアドレスが変化するなどの要因により一度認証を行ったゲスト機器２とホスト機器１との通信が確立できなくなった場合には、再度、初期認証通信を用いることなく自動的にホスト機器１においてゲスト機器２を再認証するように構成されている。このゲスト機器２の再認証の仕組みを、ここでは「自動再認証通信」と呼ぶ。

【００５５】

以下では、図４を用いて、自動再認証通信について説明する。なお、自動再認証通信における各工程（Ｓ１～Ｓ４）の内容は、初期認証通信の各工程（Ｓ１～Ｓ４）と同一のため、以下では詳細な説明を省略する。図中では、自動再認証通信を実行中のホスト機器１及びゲスト機器２の状態を、自動再接続設定モードＭ１２及び自動再接続設定モードＭ２２として示している。

【００５６】

自動再認証通信を実行するため、上述のようにホスト機器１は、認証決定工程Ｓ５において認証済みのゲスト機器２の識別子２２２を記憶する識別子データベース１４を備える。すなわち、ホスト機器１は、認証決定工程Ｓ５において、ユーザーによる認証操作＃３によって、認証が許可された場合に、認証された識別子２２２を識別子データベース１４に記憶するように構成されている。

【００５７】

自動再認証通信は、ゲスト機器２が、初期認証通信において取得したホスト機器１のＩＰアドレス１２１に対して通信不能となった場合に開始される。具体的には、例えば、ＤＨＣＰサーバによりホスト機器１に異なるＩＰアドレスが再割当てされた場合が該当する。

【００５８】
本実施形態においては、ホスト機器１のＩＰアドレス１２１が変更されると、ホスト機器１自身が、ＩＰアドレス１２１の変更を検知するように構成されている。具体的には、ホスト機器１が、ホスト機器１自身のＩＰアドレス１２１を定期的に記憶するための記憶領域１３を備える。さらに、自身のＩＰアドレス１２１と、記憶領域１３に記憶された直前のＩＰアドレスである直前ＩＰアドレス１３２とが同一であるかを監視するアドレス監視手段１１１と、を備える。
【００５９】
アドレス監視手段１１１の動作について説明する。ホスト機器１は、アドレス監視手段１１１の動作を開始させると、まず、その時点でのホスト機器１のＩＰアドレス１２１を、記憶領域１３に直前ＩＰアドレス１３２として記憶する。続いて、その時点でのＩＰアドレス１２１を取得し、当該ＩＰアドレス１２１と記憶領域１３に記憶された直前ＩＰアドレス１３２とを比較する。ＩＰアドレス１２１と直前ＩＰアドレス１３２とが同一の場合には、この比較処理を繰り返す。ここで、比較処理を繰り返す際の間隔は、例えば、１０秒に設定すると良い。比較処理において、アドレス監視手段１１１が、ＩＰアドレス１２１と直前ＩＰアドレス１３２とが同一でないことを検知した場合には、ホスト機器１は待受状態に移行し、待受開始工程Ｓ１が実行される。その後、初期認証手順における探索工程Ｓ２、通知工程Ｓ３、及び認証要求工程Ｓ４を順次実行する。
【００６０】
自動再認証通信においては、認証要求工程Ｓ４を実行後、初期認証通信における認証決定工程Ｓ５に代えて自動認証工程Ｓ５１を実行する。自動認証工程Ｓ５１では、ホスト機器１が、受信した認証要求電文ｐ３に含まれるゲスト機器２の識別子２２２が、識別子データベース１４に記憶されている場合にゲスト機器２を自動的に認証するように構成される。
【００６１】
具体的には、自動認証工程Ｓ５１において、ゲスト機器２が、認証要求電文ｐ３において「送信元認証キー」にゲスト機器２の識別子２２２を設定し、当該認証要求電文ｐ３をホスト機器１に送信し、ホスト機器１は認証要求電文ｐ３を受信する。ホスト機器１は、認証要求電文ｐ３を受信すると、認証要求電文ｐ３の「送信元認証キー」が、識別子データベース１４に既に記憶されているか否かを確認する。ここで、認証要求電文ｐ３の「送信元認証キー」が既に記憶されている場合には、ゲスト機器２の認証を許可し、記憶されていない場合には認証を不許可とする。以上が、自動認証工程Ｓ５１に相当する。
【００６２】
ホスト機器１におけるゲスト機器２の認証の許可、不許可が決定されたのちは、初期認証通信と同様に、結果通知電文ｐ４がホスト機器１からゲスト機器２に送信される。以上で、ホスト機器１及びゲスト機器２による自動再認証通信は終了する。
【００６３】
このように本願発明に係る認証方法（初期認証通信及び自動再認証通信）を用いることで、ホスト機器１によるゲスト機器２の認証を、ユーザーに必要以上に手間をかけることなく簡便、かつ、不正な端末の認証を回避できるよう安全に実行することができる。
【００６４】
〔第２実施形態〕
本願発明の第２実施形態を、図５を用いて説明する。なお、第１実施形態と同一の構成については、以下では詳細な説明を省略する。第１実施形態においては、ホスト機器１が、通常操作部１６とは別に、認証作業に用いるための通信操作部１５を備える構成の一例を示した。第２実施形態においては、通信操作部１５を備えない場合の構成を示す。具体的には、本願発明に係るホスト機器１を、通信操作部１５を備えない従来型の機器の筐体を流用して実現する場合の構成に相当する。本実施形態においては、ホスト機器１として、ガスバーナの着火スイッチなどの加熱調理のために用いる通常操作部１６のみを備えたガスコンロを例として説明する。

【００６５】
本実施形態においては、ホスト機器１は、図５に示すように通信操作部１５を備えず、通常操作部１６のみを備える。本実施形態においては、ホスト機器１は、ホスト機器１に対して物理的な状態変化を伴う当該ホスト機器に特有の操作を行うことで、待受開始操作＃１及び認証操作＃３が実行できるように構成される。
【００６６】
より具体的には、例えば、「右コンロを点火後、左コンロを点火」することを、待受開始操作＃１としたり、認証操作＃３を行う認証決定工程Ｓ５のタイミングにおいて「右コンロを点火した場合、許可、左コンロを点火した場合は不許可」とすることができる。このような構成とすることで、通信操作部１５のない筐体を用いる場合であっても、本願発明に係るホスト機器１を実装することができる。
【００６７】
〔第３実施形態〕
本願発明の第３実施形態を、図６を用いて説明する。なお、第１実施形態と同一の構成については、以下では詳細な説明を省略する。本実施形態においては、ホスト機器１と同一の場所に、外部表示手段３１を備えたリモコン３により操作可能な熱電併給装置４が設けられている構成の一例を示す。ここで、同一の場所とは、ホスト機器１が設置された家屋内を意味する。
【００６８】
本実施形態においては、認証決定工程Ｓ５において、ホスト機器１が認証要求電文ｐ３を受信した旨を、リモコン３の外部表示手段３１に表示するように構成される。このような構成とすれば、ホスト機器１が外部表示手段を備えなくとも、本願発明に係る認証方法を円滑に実行することができる。
【００６９】
〔別実施形態〕
（１）上記実施形態においては、ホスト機器１が識別子データベース１４を備える場合の構成を示したが、ホスト機器１が識別子データベース１４を備えない構成としても構わない。この場合、ホスト機器１は、自動再認証通信を行わないように構成すると良い。
【００７０】
（２）上記実施形態においては、ホスト機器１がアドレス監視手段１１１を備える場合の構成を示したが、ホスト機器１がアドレス監視手段１１１を備えない構成としても構わない。この場合、ホスト機器１は、自動再認証通信を行うにあたり、ユーザーが通信操作部１５により＃待受開始操作＃１を行うように構成すると良い。
【００７１】
（３）上記実施形態においては、認証要求電文ｐ３を受信した旨をホスト機器１以外の外部表示手段（２４または３１）に表示する場合の構成を示したが、ホスト機器１に備えられたランプを点滅させるなどの方法で、ユーザーに認証操作＃３を促すような構成としても構わない。
【００７２】
（４）上記実施形態においては、ホスト機器１としてガスコンロを、ゲスト機器２としてスマートフォンを用いる場合の例を説明したが、これらの機器に限られない。ホスト機器１としては、図１に示す各手段（１１～１６）を備える機器であれば良く、例えば、給湯器や、冷蔵庫、洗濯機、またはスピーカーなどの電子機器を用いることが可能である。また、ゲスト機器としては、図１に示す各手段（２１～２４）を備えた機器であれば良く、例えば、ＰＣやタブレット端末を用いることが可能である。
【００７３】
（５）上記第２実施形態においては、ホスト機器１としてガスコンロを用い、ホスト機器１に対して物理的な状態変化を伴う当該ホスト機器に特有の操作として、左右のコンロを点火することで、待受開始操作＃１及び認証操作＃３を行う場合の例を説明した。物理的な状態変化を伴う当該ホスト機器に特有の操作としては、例えば、ホスト機器１として給

湯器を用いる場合にはお湯の出し入れを、冷蔵庫、洗濯機を用いる場合には、ドアの開け閉めを、またスピーカーを用いる場合には音量の上げ下げを行うこととすることが可能である。

【産業上の利用可能性】

【００７４】

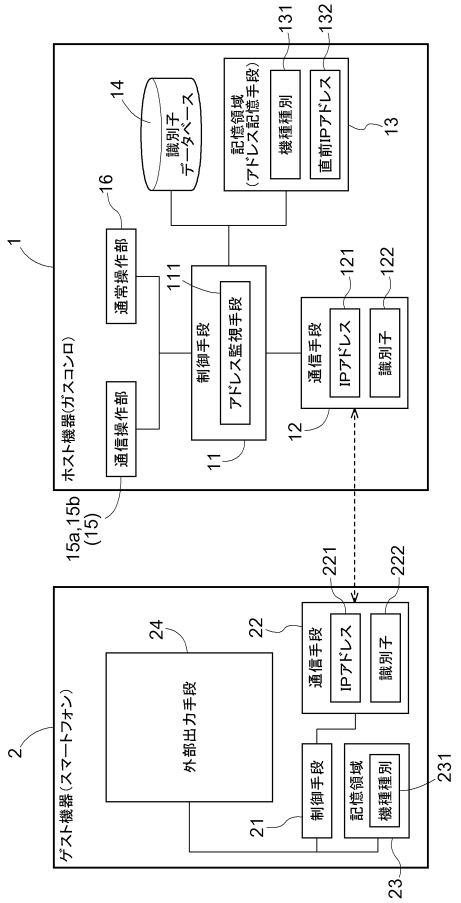
認証された機器にサービスを提供するホスト機器と、当該サービスを利用するゲスト機器とが接続されたネットワークにおいて、前記ホスト機器が前記サービスの提供先として前記ゲスト機器を認証する認証方法として利用可能である。

【符号の説明】

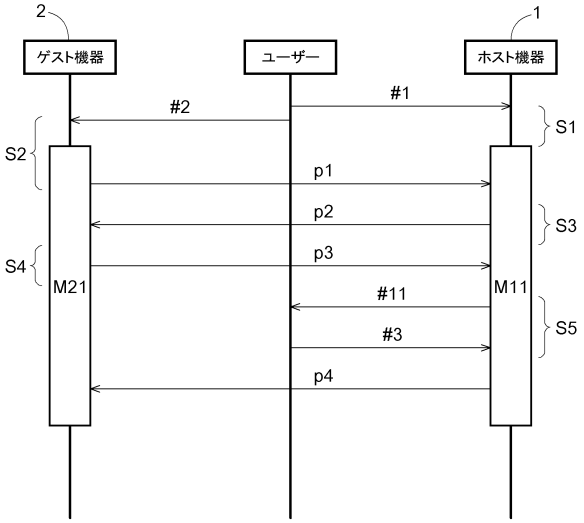
【００７５】

１　　：ホスト機器
２　　：ゲスト機器
３　　：リモコン
４　　：熱電併給装置
１３：記憶領域（アドレス記憶手段）
１４　　：識別子データベース
２４　　：外部表示手段
３１　　：外部表示手段
１１１　：アドレス監視手段
１２１　：ＩＰアドレス
１２２　：識別子
１３２　：直前ＩＰアドレス
２２１　：ＩＰアドレス
２２２　：識別子
Ｓ１　　：待受開始工程
Ｓ２　　：探索工程
Ｓ３　　：通知工程
Ｓ４　　：認証要求工程
Ｓ５　　：認証決定工程
Ｓ５１　：自動認証工程
ｐ１　　：探索用電文
ｐ３　　：認証要求電文

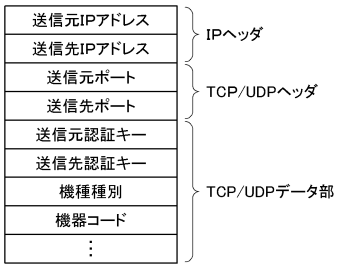
【図１】



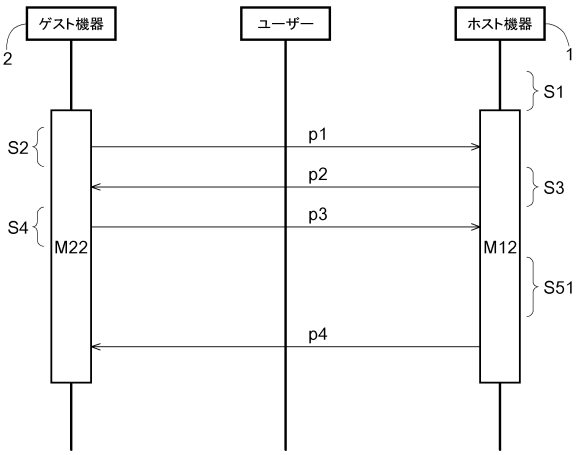
【図２】



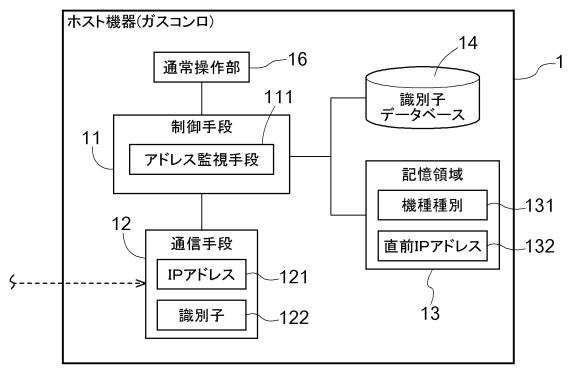
【図３】



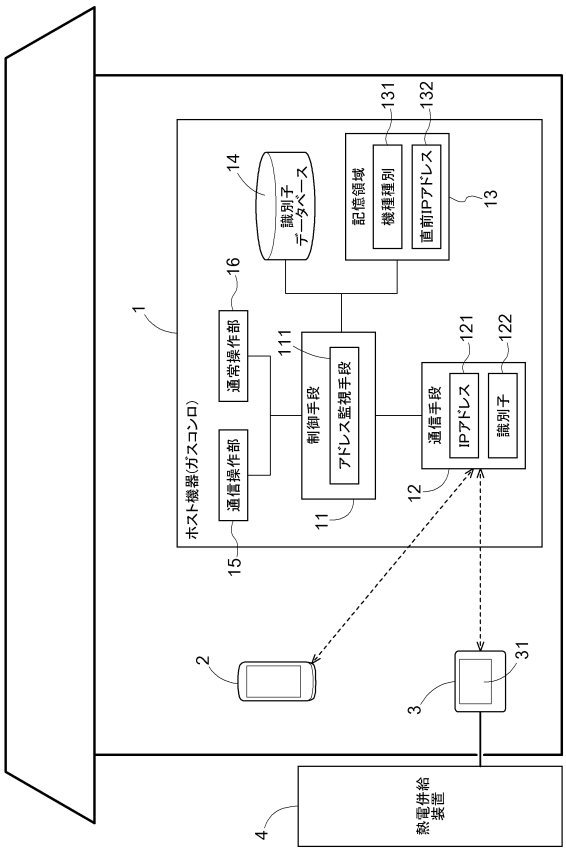
【図４】



【図５】



【図６】



フロントページの続き

(72)発明者　藤井　元
大阪府大阪市中央区平野町四丁目１番２号　大阪瓦斯株式会社内
(72)発明者　宮藤　章
大阪府大阪市中央区平野町四丁目１番２号　大阪瓦斯株式会社内
(72)発明者　石木　達也
大阪府大阪市中央区平野町四丁目１番２号　大阪瓦斯株式会社内
(72)発明者　宇野　香奈
大阪府大阪市中央区平野町四丁目１番２号　大阪瓦斯株式会社内

審査官　岸野　徹

(56)参考文献　国際公開第２００６／０４３４４６（WO，Ａ１）
特開２００９－０４３０４９（ＪＰ，Ａ）
特開２００４－１５２２４９（ＪＰ，Ａ）
米国特許出願公開第２０１２／０３２４５５４（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４