(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3767561号
(P3767561)
(45)発行日　平成18年4月19日(2006.4.19)　(24)登録日　平成18年2月10日(2006.2.10)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 15/00 330C

請求項の数 12 (全 35 頁)

(21)出願番号　特願2003-52375(P2003-52375)
(22)出願日　平成15年2月28日(2003.2.28)
(65)公開番号　特開2004-152249(P2004-152249A)
(43)公開日　平成16年5月27日(2004.5.27)
審査請求日　平成16年4月21日(2004.4.21)
(31)優先権主張番号　特願2002-256471(P2002-256471)
(32)優先日　平成14年9月2日(2002.9.2)
(33)優先権主張国　日本国(JP)

(73)特許権者　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　吉川　典史
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　小堀　洋一
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】機器認証装置、機器認証方法、および情報処理装置、情報処理方法、並びにコンピュータ・プログラム

(57)【特許請求の範囲】

【請求項１】

クライアント／サーバシステムのクライアント側に設けられる第１の装置と、

クライアント／サーバシステムのサーバ側に設けられる第２の装置とから構成され、

前記第１の装置は、ユーザの登録要求操作に応じて、第１の装置固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求手段と、

前記第２の装置は、ユーザの第１の確認操作が為されてから所定時間内に複数回または一回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶手段と、

前記第２の装置は、ユーザの第２の確認操作に応じて、前記仮記憶手段に仮記憶されたＭＡＣアドレスを持つ第１の装置宛に登録確認を送出する登録確認手段と、

前記第１の装置は、前記登録確認を受信して前記登録要求手段に一斉送出停止を指示する一方、その登録確認を送出した第２の装置宛に登録確認応答を返送する登録確認応答手段と、

前記第２の装置は、前記登録確認応答を受信した後に為されるユーザの第３の確認操作に応じて、前記仮記憶手段に仮記憶されているＭＡＣアドレスを認証登録する認証登録手段とを具備し、

前記第２の装置は、自己に認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つ第１の装置を備えたクライアントからのアクセスを拒否し、そのクライアントに対して何等応答しないようサーバに指示することを特徴とする機器認証装置。

【請求項２】
前記第２の装置は、ＭＡＣアドレスが異なる複数の競合した登録要求を受信した場合、それら競合したＭＡＣアドレスを仮記憶させず、競合したＭＡＣアドレスを持つ第１の装置からの登録要求を無視して機器認証を中止することを特徴とする請求項１記載の機器認証装置。
【請求項３】
クライアント／サーバシステムのクライアント側に設けられる第１の装置と、
クライアント／サーバシステムのサーバ側に設けられる第２の装置とから構成され、
前記第１の装置は、ユーザの登録要求操作に応じて、第１の装置固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求手段と、
前記第２の装置は、ユーザの第１の確認操作が為されてから所定時間内に複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶手段と、
前記第２の装置は、ユーザの第２の確認操作に応じて、前記仮記憶手段に仮記憶されたＭＡＣアドレスを持つ第１の装置宛に、登録確認およびパスワード要求を送出する登録確認手段と、ユーザ宛に生成したパスワードを提示する手段と、生成したパスワードを自己に記憶しておく手段と、
前記第１の装置は、前記登録確認を受信して前記登録要求手段に一斉送出停止を指示する一方、その登録確認を送出した第２の装置宛に、ユーザ操作にて入力されたパスワードと登録確認応答とを返送する登録確認応答手段と、
前記第２の装置は、前記登録確認応答手段から受信したパスワードと、自己に記憶しておいたパスワードとを照合し、両者が一致した場合に前記仮記憶手段に仮記憶されているＭＡＣアドレスを認証登録する認証登録手段とを具備し、
前記第２の装置は、自己に認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つ第１の装置を備えたクライアントからのアクセスを拒否し、そのクライアントに対して何等応答しないようサーバに指示することを特徴とする機器認証装置。
【請求項４】
前記第２の装置は、第１の装置側から受信したパスワードと、自己に予め設定されているパスワードとの照合が所定回連続して不一致になった場合、前記仮記憶手段に仮記憶されたＭＡＣアドレスを消去して機器認証を中止することを特徴とする請求項３記載の機器認証装置。
【請求項５】
クライアントサーバシステムにおいて実行する機器認証方法であり、
前記クライアントの実行ステップであり、ユーザの登録要求操作の検出に基づいてクライアント固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求実行ステップと、
前記サーバの実行ステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に、前記登録要求実行ステップにおいて前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、
前記サーバの実行ステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号を送出する登録確認ステップと、
前記クライアントの実行ステップであり、前記サーバから前記登録確認信号を受信し、前記登録要求の一斉送出を停止し、前記登録確認信号を送出したサーバに登録確認応答を返送する登録確認応答ステップと、
前記サーバの実行ステップであり、前記クライアントから前記登録確認応答を受信した後、前記サーバに対するユーザの第３の確認操作の検出に応じて、前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、
前記サーバの実行ステップであり、前記認証登録ステップにおいてサーバに認証登録さ

れたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、
を有することを特徴とする機器認証方法。
【請求項６】
前記機器認証方法は、さらに、
前記サーバの実行ステップであり、ＭＡＣアドレスが異なる複数の競合した登録要求を受信した場合、それら競合したＭＡＣアドレスを仮記憶することなく、競合したＭＡＣアドレスを持つクライアントの機器認証を中止するステップを有することを特徴とする請求項５記載の機器認証方法。
【請求項７】
クライアントサーバシステムにおいて実行する機器認証方法であり、
前記クライアントの実行ステップであり、ユーザの登録要求操作の検出に基づいて、クライアント固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求実行ステップと、
前記サーバの実行ステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に、前記登録要求実行ステップにおいて前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、
前記サーバの実行ステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号およびパスワード要求を送出する登録確認ステップと、
前記クライアントの実行ステップであり、前記サーバから前記登録確認信号およびパスワード要求を受信し、前記登録要求の一斉送出を停止し、前記登録確認信号を送出したサーバにユーザ入力に基づくパスワードと登録確認応答を返送する登録確認応答ステップと、
前記サーバの実行ステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとを照合し、両者が一致した場合に前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、
前記サーバの実行ステップであり、前記認証登録ステップにおいてサーバに認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、
を有することを特徴とする機器認証方法。
【請求項８】
前記機器認証方法は、さらに、
前記サーバの実行ステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとの照合が所定回連続して不一致になった場合、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを消去して機器認証を中止するステップを有することを特徴とする請求項７記載の機器認証方法。
【請求項９】
クライアントの機器認証処理をサーバに実行させるコンピュータ・プログラムであり、
前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、
前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号を送出する登録確認ステップと、
前記サーバの制御部に実行させるステップであり、前記クライアントから登録確認応答

を受信した後、前記サーバに対するユーザの第３の確認操作の検出に応じて、前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、
前記サーバの制御部に実行させるステップであり、前記認証登録ステップにおいてサーバに認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、
を実行させることを特徴とするコンピュータ・プログラム。
【請求項１０】
前記コンピュータ・プログラムは、さらに、
前記サーバの制御部に実行させるステップであり、ＭＡＣアドレスが異なる複数の競合した登録要求を受信した場合、それら競合したＭＡＣアドレスを仮記憶することなく、競合したＭＡＣアドレスを持つクライアントの機器認証を中止するステップ、
を実行させることを特徴とする請求項９記載のコンピュータ・プログラム。
【請求項１１】
クライアントの機器認証処理をサーバに実行させるコンピュータ・プログラムであり、
前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、
前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号およびパスワード要求を送出する登録確認ステップと、
前記サーバの制御部に実行させるステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとを照合し、両者が一致した場合に前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、
前記サーバの制御部に実行させるステップであり、前記認証登録ステップにおいてサーバに認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、
を実行させることを特徴とするコンピュータ・プログラム。
【請求項１２】
前記コンピュータ・プログラムは、さらに、
前記サーバの制御部に実行させるステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとの照合が所定回連続して不一致になった場合、前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを消去して機器認証を中止するステップ、
を実行させることを特徴とする請求項１１記載のコンピュータ・プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ネットワーク接続された機器間での通信を実行する構成において、効率的にかつ確実にアクセス権限判定情報を生成し、生成情報に基づくアクセス制限処理を可能とした機器認証装置、機器認証方法、および情報処理装置、情報処理方法、並びにコンピュータ・プログラムに関する。特に、ネットワーク対応の家電機器やコンピュータ、その周辺機器をネットワークで接続したホームネットワークや、公衆の無線ＬＡＮ環境等で用いて好適な構成に関する技術である。
【０００２】
【従来の技術】
昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で

通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

【０００３】

このようなホームネットワークの構成に適するプロトコルとしてユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）が知られている。ユニバーサルプラグアンドプレイ（ＵＰｎＰ）は、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、困難な操作や設定を伴うことなくネットワーク接続された機器において各接続機器の提供サービスを受領可能とするものである。また、ＵＰｎＰはデバイス上のＯＳ（オペレーティングシステム）にも依存せず、容易に機器の追加ができるという利点を持つ。

【０００４】

ＵＰｎＰは、接続機器間で、ＸＭＬ（eXtensible Markup Language）に準拠した定義ファイルを交換し、機器間において相互認識を行なう。ＵＰｎＰの処理の概要は、以下の通りである。

（１）ＩＰアドレス等の自己のデバイスＩＤを取得するアドレッシング処理。

（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

【０００５】

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供および受領が可能となる。ネットワークに新たに接続される機器は、上記のアドレッシング処理によりデバイスＩＤを取得し、ディスカバリ処理によりネットワーク接続された他のデバイスの情報を取得して、取得情報に基づいて他の機器にサービスの要求が可能となる。

【０００６】

しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホームネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。

【０００７】

このようなホームネットワーク内のサーバに格納されたコンテンツは、ネットワーク接続された他の機器からアクセス可能となる。例えば、上述の簡易な機器接続構成であるＵＰｎＰ接続を実行した機器によってコンテンツを取得することが可能となる。コンテンツが映画データや音楽データの場合、ネットワーク接続機器としてＴＶ、あるいはプレーヤ等を接続すれば、映画を視聴したり、音楽を聴いたりすることが可能となる。

【０００８】

コンテンツの利用権を有するユーザの接続した機器によるアクセスは許容されてもよいが、上述のようなネットワーク構成においては、コンテンツ等の利用権を持たないユーザがネットワークに入り込むことも容易である。例えば無線ＬＡＮによって構成されたネットワークの場合には家の中にあるサーバに対して、戸外、あるいは隣家等から通信機器を利用して不正にネットワークに参入し、コンテンツの搾取を行なうような事態も発生し得る。このような不正なアクセスを許容する構成は、秘密漏洩を生じさせることにもなり、また、コンテンツ著作権の管理の観点からも重要な問題となる。

【０００９】

上述のような不正アクセスを排除するため、例えばサーバにアクセスを許容するクライアントのリストを保持させ、クライアントからサーバに対するアクセス要求の際に、サーバでリストとの照合処理を実行して不正アクセスを排除する構成が提案されている。

【００１０】

例えば、ネットワーク接続機器に固有の物理アドレスであるＭＡＣ（Ｍｅｄｉａ　Ａｃｃ

ｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを、アクセス許容機器リストとして設定するＭＡＣアドレスフィルタリングが知られている。ＭＡＣアドレスフィルタリングとは、ホームネットワーク等の内部ネットワーク（サブネット）と外部ネットワークとを隔離するルータあるいはゲートウェイに、予めアクセスを許容するＭＡＣアドレスを登録しておき、受信したパケットのＭＡＣアドレスと登録されたＭＡＣアドレスとを照合し、登録されていないＭＡＣアドレスを有する機器からのアクセスを拒否するものである。なお、この種の技術については、例えば特許文献１に開示されている。

【００１１】

しかし、アクセス制限をするためのＭＡＣアドレスの登録処理を行なうためには、ネットワークに接続される機器の全てのＭＡＣアドレスを調べることが必要であり、取得した全ての機器のＭＡＣアドレス（４８ｂｉｔ）をオペレータが入力してリストを作成するという処理が必要となる。このような処理は、例えば特定の会社、団体等、セキュアな環境を構築することが要求される場合には、所定の管理者の下に行なうことも可能であるが、例えば一般家庭に設定されるホームネットワーク環境において、一般ユーザにＭＡＣリストの生成、格納を要求することは現実的ではない。

【００１２】

ホームネットワークにおいては、新たな機器の追加処理が行われることは頻繁に発生することであり、このような機器追加処理の際に、ユーザが逐次、機器のＭＡＣアドレスを調べて登録処理をしなければならないとすると、ネットワーク構築の容易性を阻害することになる。

【００１３】

一方、一般家庭においても、ＰＣのみならず、家電機器も含んだネットワーク構成が構築され、どのような機器からでもネットワークにアクセス可能ないわゆるユビキタス環境が構築されつつあり、また、無線ＬＡＮ等の普及により、通信可能な機器が外部から無線ＬＡＮに侵入することも容易となっている。このようなネットワーク環境において、ネットワーク接続機器に対する不正アクセスもより発生しやすくなっており、不正なアクセスによる秘密情報の搾取、コンテンツの不正読み取り等が実行される可能性はますます高くなっている。このような状況において、一般ユーザに負担を強いることなく、適切なアクセス制御構成を容易に実現することが求められている。

【００１４】

【特許文献１】

特許公開平１０－２７１１５４号公報

【００１５】

【発明が解決しようとする課題】

本発明は、上述の問題点に鑑みてなされたものであり、様々な機器がネットワーク接続される構成において、ネットワーク接続機器を有するユーザに負担を強いることなく、容易にかつ的確にアクセス制御構成を構築することを可能とした機器認証装置、機器認証方法、および情報処理装置、情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００１６】

ある種のＩＳＰ（インターネット・サービス・プロバイダ）が提供する商用ネットワークでは、同一サブネットに複数のユーザを割り当てている。そうした接続サービスを受ける場合には、自宅のホームネットワークが同一サブネット内の他のユーザから不正アクセスされないようにする為、上述したＭＡＣアドレスフィルタリングを行うルータを設けなければならない、という問題がある。また、ケーブルＴＶを用いた接続サービスでは、約款でルータ接続を禁止している場合もある。そのような接続サービスでは、ＭＡＣアドレスフィルタリングを行えず、ＩＰアドレスを用いてアクセス認証するが、ＩＰアドレスは論理的に設定される為に比較的容易に詐称でき、セキュリティの高いアクセス制御は難しいという欠点がある。

【００１７】

そこで本発明は、このような事情に鑑みてなされたもので、ルータを用いることなくセキュリティの高いアクセス制御を行うことができる機器認証装置、機器認証方法および機器認証プログラムを提供することを目的としている。

【００１８】

さらに、本発明は、アクセス制御構成の構築のための認証処理すなわち機器登録処理において、クライアント機器の正規な登録処理の確実な実行を確保するための構成、具体的には登録完了の通知構成を実現する。また、機器登録処理において、サーバクライアント間で実行される登録処理メッセージが機器登録処理実行プログラムのバージョンによって異なる場合の問題を解決し、新旧様々の機器が混在するネットワーク環境においても確実な機器登録処理を実現する機器認証装置、機器認証方法、および情報処理装置、情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００１９】

【課題を解決するための手段】

本発明の第１の側面は、

クライアント／サーバシステムのクライアント側に設けられる第１の装置と、クライアント／サーバシステムのサーバ側に設けられる第２の装置とから構成され、前記第１の装置は、ユーザの登録要求操作に応じて、第１の装置固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求手段と、前記第２の装置は、ユーザの第１の確認操作が為されてから所定時間内に複数回または一回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶手段と、前記第２の装置は、ユーザの第２の確認操作に応じて、前記仮記憶手段に仮記憶されたＭＡＣアドレスを持つ第１の装置宛に登録確認を送出する登録確認手段と、前記第１の装置は、前記登録確認を受信して前記登録要求手段に一斉送出停止を指示する一方、その登録確認を送出した第２の装置宛に登録確認応答を返送する登録確認応答手段と、前記第２の装置は、前記登録確認応答を受信した後に為されるユーザの第３の確認操作に応じて、前記仮記憶手段に仮記憶されているＭＡＣアドレスを認証登録する認証登録手段とを具備し、前記第２の装置は、自己に認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つ第１の装置を備えたクライアントからのアクセスを拒否し、そのクライアントに対して何等応答しないようサーバに指示することを特徴とする。

【００２０】

さらに、本発明の機器認証装置の一実施態様において、前記第２の装置は、ＭＡＣアドレスが異なる複数の競合した登録要求を受信した場合、それら競合したＭＡＣアドレスを仮記憶させず、競合したＭＡＣアドレスを持つ第１の装置からの登録要求を無視して機器認証を中止することを特徴とする。

【００２１】

さらに、本発明の第２の側面は、

クライアント／サーバシステムのクライアント側に設けられる第１の装置と、クライアント／サーバシステムのサーバ側に設けられる第２の装置とから構成され、前記第１の装置は、ユーザの登録要求操作に応じて、第１の装置固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求手段と、前記第２の装置は、ユーザの第１の確認操作が為されてから所定時間内に複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶手段と、前記第２の装置は、ユーザの第２の確認操作に応じて、前記仮記憶手段に仮記憶されたＭＡＣアドレスを持つ第１の装置宛に、登録確認およびパスワード要求を送出する登録確認手段と、ユーザ宛に生成したパスワードを提示する手段と、生成したパスワードを自己に記憶しておく手段と、前記第１の装置は、前記登録確認を受信して前記登録要求手段に一斉送出停止を指示する一方、その登録確認を送出した第２の装置宛に、ユーザ操作にて入力されたパスワードと登録確認応答とを返送する登録確認応答手段と、前記第２の装置は、前記登録確認応答手段から受信したパスワードと、自己に記憶しておいたパスワードとを照合し、両者が一致した場合に前記仮記憶手段に仮記憶されているＭＡＣアドレスを認証登録する認証登録手段とを具備

し、前記第２の装置は、自己に認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つ第１の装置を備えたクライアントからのアクセスを拒否し、そのクライアントに対して何等応答しないようサーバに指示することを特徴とする。

【００２２】

さらに、本発明の機器認証装置の一実施態様において、前記第２の装置は、第１の装置側から受信したパスワードと、自己に予め設定されているパスワードとの照合が所定回連続して不一致になった場合、前記仮記憶手段に仮記憶されたＭＡＣアドレスを消去して機器認証を中止することを特徴とする。

【００２３】

さらに、本発明の第３の側面は、

クライアントサーバシステムにおいて実行する機器認証方法であり、

前記クライアントの実行ステップであり、ユーザの登録要求操作の検出に基づいてクライアント固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求実行ステップと、

前記サーバの実行ステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に、前記登録要求実行ステップにおいて前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、

前記サーバの実行ステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号を送出する登録確認ステップと、

前記クライアントの実行ステップであり、前記サーバから前記登録確認信号を受信し、前記登録要求の一斉送出を停止し、前記登録確認信号を送出したサーバに登録確認応答を返送する登録確認応答ステップと、

前記サーバの実行ステップであり、前記クライアントから前記登録確認応答を受信した後、前記サーバに対するユーザの第３の確認操作の検出に応じて、前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、

前記サーバの実行ステップであり、前記認証登録ステップにおいてサーバに認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、

を有することを特徴とする機器認証方法にある。

【００２４】

さらに、本発明の機器認証方法の一実施態様において、前記機器認証方法は、さらに、前記サーバの実行ステップであり、ＭＡＣアドレスが異なる複数の競合した登録要求を受信した場合、それら競合したＭＡＣアドレスを仮記憶することなく、競合したＭＡＣアドレスを持つクライアントの機器認証を中止するステップを有することを特徴とする。

【００２５】

さらに、本発明の第４の側面は、

クライアントサーバシステムにおいて実行する機器認証方法であり、

前記クライアントの実行ステップであり、ユーザの登録要求操作の検出に基づいて、クライアント固有のＭＡＣアドレスの登録要求をネットワーク上に一斉送出する登録要求実行ステップと、

前記サーバの実行ステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に、前記登録要求実行ステップにおいて前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、

前記サーバの実行ステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号およびパスワード要求を送出する登録確認ステップと、

前記クライアントの実行ステップであり、前記サーバから前記登録確認信号およびパス

ワード要求を受信し、前記登録要求の一斉送出を停止し、前記登録確認信号を送出したサーバにユーザ入力に基づくパスワードと登録確認応答を返送する登録確認応答ステップと、

前記サーバの実行ステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとを照合し、両者が一致した場合に前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、

前記サーバの実行ステップであり、前記認証登録ステップにおいてサーバに認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、

を有することを特徴とする機器認証方法にある。

【００２６】

さらに、本発明の機器認証方法の一実施態様において、前記機器認証方法は、さらに、前記サーバの実行ステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとの照合が所定回連続して不一致になった場合、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを消去して機器認証を中止するステップを有することを特徴とする。

【００２７】

さらに、本発明の第５の側面は、

クライアントの機器認証処理をサーバに実行させるコンピュータ・プログラムであり、

前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、

前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号を送出する登録確認ステップと、

前記サーバの制御部に実行させるステップであり、前記クライアントから登録確認応答を受信した後、前記サーバに対するユーザの第３の確認操作の検出に応じて、前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、

前記サーバの制御部に実行させるステップであり、前記認証登録ステップにおいてサーバに認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、

を実行させることを特徴とするコンピュータ・プログラムにある。

【００２８】

さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、前記サーバの制御部に実行させるステップであり、ＭＡＣアドレスが異なる複数の競合した登録要求を受信した場合、それら競合したＭＡＣアドレスを仮記憶することなく、競合したＭＡＣアドレスを持つクライアントの機器認証を中止するステップ、を実行させることを特徴とする。

【００２９】

さらに、本発明の第６の側面は、

クライアントの機器認証処理をサーバに実行させるコンピュータ・プログラムであり、

前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第１の確認操作の検出から所定時間内に前記クライアントから送出される複数回同一のＭＡＣアドレスを有する登録要求を受信した場合に、そのＭＡＣアドレスを仮記憶する仮記憶ステップと、

前記サーバの制御部に実行させるステップであり、前記サーバに対するユーザの第２の確認操作の検出に応じて、前記仮記憶ステップにて仮記憶されたＭＡＣアドレスを持つクライアントに対して登録確認信号およびパスワード要求を送出する登録確認ステップと、

前記サーバの制御部に実行させるステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとを照合し、両者が一致した場合に前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを認証登録する認証登録ステップと、

前記サーバの制御部に実行させるステップであり、前記認証登録ステップにおいてサーバに認証登録されたＭＡＣアドレス以外のＭＡＣアドレスを持つクライアントからのアクセスを拒否するステップと、

を実行させることを特徴とするコンピュータ・プログラムにある。

【００３０】

さらに、本発明のコンピュータ・プログラムの一実施態様において、前記コンピュータ・プログラムは、さらに、前記サーバの制御部に実行させるステップであり、前記登録確認応答ステップにおいて前記クライアントから受信したパスワードと、前記サーバ内のメモリに記憶済みのパスワードとの照合が所定回連続して不一致になった場合、前記仮記憶ステップにおいて仮記憶されたＭＡＣアドレスを消去して機器認証を中止するステップ、を実行させることを特徴とする。

【００６５】

【作用】

本発明の構成によれば、ユーザ操作によってオーソライズされた第１の装置（クライアント）のＭＡＣアドレスだけが第２の装置に認証登録され、第２の装置は認証登録されたＭＡＣアドレスを有する第１の装置（クライアント）とのアクセスだけを許容する結果、同一サブネット内の他のユーザと隔離するためのルータを設置せずとも、認証登録されていない不正な相手からのアクセスを避ける一方、不正に機器認証しようとする第１の装置（クライアント）側にサーバの存在を知られないようにする結果、セキュリティの高いアクセス制御を提供することが可能になる。

【００６６】

さらに、本発明の構成によれば、ＭＡＣ登録処理の最終ステップとして、登録完了（Ｃｏｍｐｌｅｔｅ）確認処理を実行する構成とし、サーバ（デバイス）側からＭＡＣ登録完了確認をクライアント（コントローラ）側に対して送信する構成としたので、双方の機器において登録完了メッセージに基づいて、ユーザが最終的な登録完了の確認をすることが可能となる。また、クライアント（コントローラ）側では、ＭＡＣ登録完了確認通知をサーバ（デバイス）側から受信したことを条件として、サービス検索処理としてのＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈの送信処理を実行すれば、サーバ（デバイス）側においてＭＡＣ登録が完了していることが保障されているので、サービス検索処理の応答を確実に受信することが可能となる。

【００６７】

さらに、本発明の構成によれば、登録完了（Ｃｏｍｐｌｅｔｅ）確認処理を実行する構成とすることで、ＭＡＣ登録完了確認通知をサーバ（デバイス）側から受信したことを条件としてＭ－ｓｅａｒｃｈの送信処理を自動的に実行することが可能となり、ユーザの入力処理等を介在させることなく、クライアントはサーバに対する登録処理に続いてサーバからサービス情報を受領することが可能となる。

【００６８】

さらに、本発明の構成によれば、すでにサーバのＭＡＣリストに登録されたクライアントからのＭＡＣ登録要求があった場合は、機器間において登録済みであることの確認通知処理が実行されるので、これらの通知に基づいて登録済みであることのメッセージ表示が可能となり、ユーザは、クライアント機器がすでにサーバに登録されていることを確認することが可能となる。

【００６９】

さらに、本発明の構成によれば、サーバクライアント間での機器登録処理において、双方の機器の有する処理プログラムのバージョン情報の通知を実行し、処理シーケンスを調整して機器登録処理を実行する構成としたので、様々なバージョンのプログラムを格納した

機器間においても、統一した処理シーケンスに従った機器登録処理が実行できる。
【００７０】
なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。
【００７１】
本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【００７２】
【発明の実施の形態】
以下、図面を参照して本発明の機器認証装置、機器認証方法、および情報処理装置、情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。
【００７３】
［システム概要］
まず、図１を参照して、本発明の適用可能なネットワーク構成例について説明する。図１は、様々なクライアント装置からの処理要求に応じて処理を実行するサーバ１０１と、サーバ１０１に対して処理要求を行なうクライアント装置としてのＰＣ１２１，モニター１２２，携帯電話１２３、再生機１２４、ＰＤＡ(Personal Digital Assistant)１２５がネットワーク１００を介して接続された構成、例えばホームネットワーク構成を示している。クライアント装置としては、この他にも様々な電子機器、家電機器が接続可能である。
【００７４】
サーバ１０１がクライアントからの要求に応じて実行する処理は、例えばサーバ１０１の保有するハードディスク等の記憶手段に格納されたコンテンツの提供、あるいはサーバの実行可能なアプリケーションプログラムの実行によるデータ処理サービス等である。なお、図１においては、サーバ１０１と、クライアント装置とを区別して示しているが、クライアントからの要求に対するサービスを提供する機器をサーバとして示しているものであり、いずれのクライアント装置も、自己のデータ処理サービスを他のクライアントに提供する場合には、サーバとしての機能を提供可能となる。従って、図１に示すネットワーク接続されたクライアント装置もサーバとなり得る。
【００７５】
ネットワーク１００は、有線、無線等いずれかのネットワークであり、各接続機器は、例えばイーサネット（登録商標）フレーム等の通信パケットをネットワーク１００を介して送受信する。すなわち、クライアントは、イーサネットフレームのデータ部に処理要求情報を格納したフレームをサーバ１０１に送信することにより、サーバ１０１に対するデータ処理要求を実行する。サーバ１０１は、処理要求フレームの受信に応じて、データ処理を実行し、必要に応じてデータ処理結果としての結果データを通信パケットのデータ部に格納し、各クライアントに送信する。
【００７６】
ネットワーク接続機器は、例えばユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）対応機器によって構成される。従って、ネットワークに対する接続機器の追加、削除が容易な構成である。ネットワークに新たに接続する機器は、
（１）ＩＰアドレス等の自己のデバイスＩＤを取得するアドレッシング処理。
（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。
（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサ

ービス要求処理。
上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスを受領することが可能となる。
【００７７】
図１に示すサーバおよびクライアント装置を構成する情報処理装置の一例としてＰＣのハードウェア構成例について図２を参照して説明する。
【００７８】
ＣＰＵ(Central Processing Unit)２０１は、ＲＯＭ(Read Only Memory)２０２、またはＨＤＤ(hard disk drive)２０４等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。ＲＡＭ(random access memory)２０３には、ＣＰＵ２０１が実行するプログラムやデータが適宜記憶される。ＣＰＵ２０１、ＲＯＭ２０２、およびＲＡＭ２０３、ＨＤＤ２０４は、バス２０５を介して相互に接続されている。
【００７９】
バス２０５には、入出力インタフェース２０６が接続されており、この入出力インタフェース２０６には、例えば、ユーザにより操作されるキーボード、スイッチ、ボタン、あるいはマウス等により構成される入力部２０７、ユーザに各種の情報を提示するＬＣＤ、ＣＲＴ、スピーカ等により構成される出力部２０８が接続される。さらに、データ送受信手段として機能する通信部２０９、さらに、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体２１１を装着可能で、これらのリムーバブル記録媒体２１１からのデータ読み出しあるいは書き込み処理を実行するドライブ２１０が接続される。
【００８０】
図２に示す構成は、図１に示すネットワーク接続機器の一例としてのサーバ、パーソナルコンピュータ（ＰＣ）の例であるが、ネットワーク接続機器はＰＣに限らず、図１に示すように携帯電話、ＰＤＡ等の携帯通信端末、その他、再生装置、ディスプレイ等の様々な電子機器、情報処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。
【００８１】
図３は、本発明による機器認証装置が適用されたホームネットワーク３００のサーバ３１０とクライアント３２０の最小構成例を示すブロック図である。この図に示すサーバ３１０とクライアント３２０により構成されるネットワークは、上述した所謂ＵＰｎＰ（ユニバーサルプラグアンドプレイ）環境を提供する。図３に示す例においてクライアント３２０は、サーバとの各種通信処理を実行するネットワーク対応機器３２１と、例えばサーバからの受信コンテンツを表示するテレビジョン受像機３２２により構成されているものとする。
【００８２】
サーバ３１０は、ネットワーク対応機器３２１からの要求に応じて各種アプリケーション機能やコンテンツデータを提供する。ネットワーク対応機器３２１は、ホームネットワーク３００のコントロールポイントとして機能するハードウェアであって、ユーザ操作に応じて発生するイベントに従い、サーバ３１０側に指定サービスの実行を要求したり、その要求に応じてサーバ３２１側から提供されるサービスを処理する。
【００８３】
このようなネットワーク構成において、例えばＭＰＥＧ圧縮されたビデオ素材がサーバ３１０側に格納され、ネットワーク対応機器３２１がそのビデオ素材の送出を要求した場合、サーバ３１０はネットワーク対応機器３２１からの要求に応じてビデオ素材を送出し、ネットワーク対応機器３２１では、そのＭＰＥＧ圧縮されたビデオ素材をデコード（伸長）したビデオ信号をテレビジョン受像機３２２に供給して映像再生を行う。
【００８４】

［機器認証装置の構成］
さて、上述したホームネットワークでは、同一サブネット内の他のユーザからの不正アクセスを防ぐ機器認証装置がサーバおよびネットワーク対応機器に搭載される。図４は機器認証装置の機能的構成を示すブロック図である。
【００８５】
機器認証装置３５０は、オブジェクトに対する操作を定義したメソッドと呼ばれる各種ルーチンから形成されるプログラム集合体であって、クライアント、すなわち、ネットワーク対応機器側に実装されるコントローラ３５１と、サーバ側に実装されるデバイス３５２とから構成される仮想的な装置である。
【００８６】
コントローラ３５１は、登録要求時に行われるユーザ操作、例えば登録ボタンの押下等に応じてユーザシグナルを発生する。コントローラ３５１では、ユーザ操作に応じて発生するユーザシグナルに従い、登録要求をＵＤＰ層でブロードキャストする。また、コントローラ３５１は、デバイス３５２側からＴＣＰ層でユニキャストされるメソッドを受信してレスポンスを返送したり、受信したメソッドに対応した内容を表示するためのデバイスシグナルを発生する。
【００８７】
一方、デバイス３５２は、登録確認時に行われるユーザ操作、例えば確認ボタンの押下等に応じてユーザシグナルを発生する。デバイス３５２では、コントローラ３５１側からブロードキャストされた登録要求を受信した場合、ユーザ操作に応じて発生するユーザシグナルに従い、クライアント側のＭＡＣアドレスをＭＡＣアドレステーブルに登録して機器認証すると共に、登録要求を出したコントローラ３５１側に認証登録した旨をＴＣＰ層でユニキャストする。
【００８８】
デバイス３５２は、コントローラ３５１側からＴＣＰ層でユニキャスト返送されるレスポンスを受信し、受信したレスポンスに対応した内容を表示するためのデバイスシグナルを発生する。デバイス３５２は、所定のユーザ操作に応じて、ＭＡＣアドレステーブルに登録されたＭＡＣアドレスの全てあるいは一部の消去を指示する。また、デバイス３５２では、ＭＡＣアドレステーブルに認証登録された以外のＭＡＣアドレスを有する機器からのアクセスを拒否し、何等返送しないようになっている。
【００８９】
したがって、こうしたコントローラ３５１およびデバイス３５２から構成される機器認証装置３５０を備えるホームネットワーク１００では、同一サブネット内の他のユーザと隔離するためのルータを設置せずとも、機器認証装置３５０が認証登録されていない不正な相手からのアクセスを避ける一方、不正に機器認証しようとするコントローラ３５１側にサーバ１の存在を知られないようにする為、セキュリティの高いアクセス制御が可能になっている。
【００９０】
［クライアント登録処理例－実施例１］
次に、図５～図７を参照して機器認証装置３５０によるクライアント登録処理の第１実施例について説明する。ここでは、例えば図１、図３に示したホームネットワークにおいて、コントローラ３５１を備えた新たなネットワーク対応機器が接続され、その新たなネットワーク対応機器（クライアント側）に実装されるコントローラ３５１が、サーバ側のデバイス３５２に認証登録を依頼する動作（手順）について説明する。
【００９１】
機器認証装置３５０は、パスワードを使用せずに機器認証するモードと、パスワードを用いて機器認証するモードとを備えており、以下、各モード別に動作説明する。
【００９２】
▲１▼ワンタイムパスワード無しの場合
パスワードを使用せずに機器認証するモードでは、図５に示すシーケンスで認証登録が行

われる。以下、図５に示すシーケンスを参照して説明する。まず最初にユーザがクライアント（コントローラ３５１）側に設けられた登録ボタンを押下する。すると、コントローラ３５１は登録ボタンの押下に応じて発生するユーザシグナルＡ（ＵＳＡ）に従い、ＭＡＣアドレス登録メソッドをＵＤＰ層でブロードキャストする。ブロードキャストする形態としては、例えば５分間３秒毎のブロードキャスト送信を行う。なお、コントローラ３５１が、５分間経過してデバイス３５２側からのＭＡＣ登録確認メソッドを受信できない場合には、認証に失敗したと判断して最初からやり直す。

【００９３】

ユーザは、クライアント（コントローラ３５１）側に設けられた登録ボタンを押下した後、サーバ（デバイス３５２）側に移動する。そして、サーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２は確認ボタンの押下に応じて発生するユーザシグナルＢ（ＵＳＢ）に従い、ＭＡＣアドレス登録メソッドを１０秒間受信する。

【００９４】

１０秒間に同一のＭＡＣアドレスを有する複数のＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はそのＭＡＣアドレスをＭＡＣアドレステーブルに仮記憶した後、ユーザに対して「機器を発見しました。登録しますか？」なるメッセージを表示するデバイスシグナルＡ（ＤＳＡ）を発生し、その状態で１分間待機する。なお、このデバイスシグナルＡ（ＤＳＡ）は、省略されても良い。

【００９５】

１分間待機中に、ユーザがサーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２はそれに応じて発生するユーザシグナルＣ（ＵＳＣ）に従い、ＭＡＣ登録確認メソッドをＴＣＰ層でコントローラ３５１に対してユニキャストする。

【００９６】

前項においてデバイスシグナルＡ（ＤＳＡ）が省略された場合には、１０秒間に同一のＭＡＣアドレスを有するＭＡＣアドレス登録メソッドを受信した場合、ユーザシグナルＣ（ＵＳＣ）を必要とせず、ただちにデバイス３５２はＭＡＣ登録確認メソッドをＴＣＰ層でコントローラ３５１に対してユニキャストする。ＭＡＣ登録確認メソッドには、登録を行ったデバイス名ｄｅｖ－ｎａｍｅが付加される。

【００９７】

コントローラ３５１は、ＭＡＣ登録確認メソッドを受信すると、ＭＡＣアドレス登録メソッドの送信を停止すると共に、受信したＭＡＣ登録確認メソッドに含まれるデバイス名ｄｅｖ－ｎａｍｅに基づき、ユーザに対して「デバイス“ＸＸＸＸ”に登録されました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生する。そして、自己の名前ｃｐ－ｎａｍｅを付加したＭＡＣ登録確認レスポンスをデバイス３５２へユニキャスト返信する。

【００９８】

デバイス３５２では、コントローラ３５１からのＭＡＣ登録確認レスポンスを受信すると、ＭＡＣ登録確認レスポンスに含まれるコントローラ名ｃｐ－ｎａｍｅに基づき、ユーザに対して「コントローラ“ＹＹＹＹ”を登録できます。本当に登録してよろしいですか？」なるメッセージを表示するデバイスシグナルＤ（ＤＳＤ）を発生する。

【００９９】

ここで、ユーザがサーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２はそれに応じて発生するユーザシグナルＤ（ＵＳＤ）に従い、ユーザに対して「コントローラ“ＹＹＹＹ”を登録しました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して認証登録を終える。

【０１００】

上述の認証登録が済むと、デバイス３５２は、コントローラ３５１からのサービス検索処理として実行されるＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合、ＭＡＣリストを参照し、登録済みデバイス３５２からの要求であることを確認し、サービス検索に対する応答を行う。

【０１０１】
なお、デバイス３５２では、ユーザシグナルＤ（ＵＳＤ）を受ける以前、すなわち、完全に認証登録し終える以前に、コントローラ３５１からＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合、デバイス３５２は応答しないようになっている。
【０１０２】
▲２▼ワンタイムパスワード有りの場合
次に、図６に示すシーケンスを参照し、パスワードを用いて機器認証するモード下で行われる認証登録の動作について説明する。まず最初にユーザがクライアント（コントローラ３５１）側に設けられた登録ボタンを押下する。すると、コントローラ３５１は登録ボタンの押下に応じて発生するユーザシグナルＡ（ＵＳＡ）に従い、ＭＡＣアドレス登録メソッドをＵＤＰ層でブロードキャストする。ブロードキャストする形態としては、例えば５分間３秒毎に行う。なお、５分間経過してデバイス３５２側からのＭＡＣ登録確認を受信できない場合には、認証に失敗したと判断して最初からやり直す。
【０１０３】
クライアント（コントローラ３５１）側に設けられた登録ボタンを押下した後、ユーザはサーバ（デバイス３５２）側に移動する。そして、サーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２は確認ボタンの押下に応じて発生するユーザシグナルＢ（ＵＳＢ）に従い、ＭＡＣアドレス登録メソッドを１０秒間受信する。
【０１０４】
１０秒間に同一のＭＡＣアドレスのみからＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はそのＭＡＣアドレスをＭＡＣアドレステーブルに仮記憶した後、ユーザに対して「機器を発見しました。登録しますか？」なるメッセージを表示するデバイスシグナルＡ（ＤＳＡ）を発生し、その状態で１分間待機する。
【０１０５】
なお、既に認証登録済みのコントローラ３５１からのＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はＭＡＣ登録完了を意味するＭＡＣ登録確認メソッドを送信して直ちに認証登録を終了する。
【０１０６】
さて、デバイスシグナルＡ（ＤＳＡ）を発生した状態で１分間待機している間に、ユーザがサーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２は確認ボタンの押下に応じて発生するユーザシグナルＣ（ＵＳＣ）に従い、ＭＡＣ登録確認メソッドをＴＣＰ層でユニキャストする。ＭＡＣ登録確認メソッドには、パスワード要求フラグが付加される。
【０１０７】
コントローラ３５１は、パスワード要求フラグが付加されたＭＡＣ登録確認メソッドを受信すると、ＭＡＣアドレス登録メソッドの送信を停止すると共に、デバイス３５２へＭＡＣ登録確認レスポンスをユニキャストで返信する。
【０１０８】
デバイス３５２は、このＭＡＣ登録確認レスポンスを受信すると、ユーザに対して「コントローラ“ＹＹＹＹ”のためのワンタイムパスワードは”○○○○”です。」なるメッセージを表示するデバイスシグナルＣ（ＤＳＣ）を発生し、ワンタイムパスワードを提示した状態で５分間待機する。
【０１０９】
一方、コントローラ３５１は、受信したＭＡＣ登録確認メソッドに含まれるパスワード要求フラグに基づき、ユーザに対して「デバイス“ＸＸＸＸ”のパスワードを入力してください。」なるメッセージを表示するデバイスシグナルＢ（ＤＳＢ）を発生し、ワンタイムパスワードの入力を５分間待機する。
【０１１０】
この待機中にユーザがサーバ側からクライアント（コントローラ３５１）側に移動する。

そして、クライアント（コントローラ３５１）側に移動してきたユーザは、パスワードを入力する。すると、コントローラ３５１は入力されたパスワードを付加したパスワードメソッドをデバイス３５２にＴＣＰ層でユニキャストして１０秒間待機する。

【０１１１】

デバイス３５２では、ワンタイムパスワードを提示する５分間の待機状態でコントローラ３５１からのパスワードメソッドを受信すると、自己に予め設定されているワンタイムパスワードと照合する。以下、パスワード照合ＯＫの場合とパスワード照合ＮＧの場合とに分けて動作説明する。

【０１１２】

（ａ）パスワード照合ＯＫの場合

コントローラ３５１から送られてきたワンタイムパスワードが適正であると、デバイス３５２はＭＡＣアドレステーブルに仮記憶されたＭＡＣアドレスを正式に認証登録した後、コントローラ３５１に照合ＯＫを付加したパスワードレスポンスをユニキャストで返信する。そして、ユーザに対して「コントローラ“ＹＹＹＹ”を登録しました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して認証登録を終える。

【０１１３】

一方、コントローラ３５１では、パスワードメソッドをデバイス３５２にＴＣＰ層でユニキャストして１０秒間待機中に、デバイス３５２から照合ＯＫが付加されたパスワードレスポンスを受信すると、ＭＡＣアドレスが認証登録されたとして、ユーザに対して「デバイス“ＸＸＸＸ”に登録されました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して機器認証を終える。

【０１１４】

上述の認証登録が済むと、デバイス３５２は、コントローラ３５１からのサービス検索処理として実行されるＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合、ＭＡＣリストを参照し、登録済みデバイス３５２からの要求であることを確認し、サービス検索に対する応答を行う。

【０１１５】

なお、デバイス３５２では、デバイスシグナルＺ（ＤＳＺ）を発行する以前、すなわち、完全に認証登録し終える以前に、コントローラ３５１からＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合、デバイス３５２は応答しないようになっている。

【０１１６】

（ｂ）パスワード照合ＮＧの場合

コントローラ３５１から送られてきたワンタイムパスワードが不正であると、デバイス３５２はコントローラ３５１に照合ＮＧを付加したパスワードレスポンスをユニキャストで返信し、コントローラ３５１から再度パスワード入力されるのを５分間待機する。

【０１１７】

そして、この待機期間中にパスワード照合ＮＧが３回連続すると、デバイス３５２はパスワード入力の再試行を中止させ、ユーザに対して「コントローラ“ＹＹＹＹ”を登録できません。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して機器認証を終える。この場合、デバイス３５２では、ＭＡＣアドレステーブルに仮記憶されたＭＡＣアドレスを消去する。

【０１１８】

一方、コントローラ３５１では、デバイス３５２から再試行中止のリザルトコードが付加されたパスワードレスポンスを受信すると、ユーザに対して「デバイス“ＸＸＸＸ”には登録できません。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して機器認証を終了する。

【０１１９】

▲３▼異なるコントローラを検出した場合

次に、デバイス３５２がＭＡＣアドレス登録メソッドを１０秒間受信する最中に、ＭＡＣ

アドレス登録メソッドをブロードキャストしたコントローラ３５１とは異なる他のコントローラを検出した場合の動作について図７を参照して説明する。

【０１２０】

ユーザがクライアント（コントローラ３５１）側に設けられた登録ボタンを押下し、これに応じて発生するユーザシグナルＡ（ＵＳＡ）に従い、コントローラ３５１がＭＡＣアドレス登録メソッドをＵＤＰ層でブロードキャストする。この後、ユーザがサーバ（デバイス３５２）側に移動してサーバ側に設けられた確認ボタンを押下すると、デバイス３５２は確認ボタンの押下に応じて発生するユーザシグナルＢ（ＵＳＢ）に従い、ＭＡＣアドレス登録メソッドを１０秒間受信する。

【０１２１】

この１０秒間中に異なるＭＡＣアドレスからのＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はユーザに対して「複数のコントローラを発見しました。登録を行いません。」なるメッセージを表示するデバイスシグナルＸ（ＤＳＸ）を発生して機器認証を中止する。

【０１２２】

こうして、デバイス３５２側が一方的に機器認証を終了すると、コントローラ３５１はＭＡＣ登録確認メソッドを受信できず、ＭＡＣアドレス登録メソッドをブロードキャストする５分間のタイムリミットが経過して時点で、ユーザに対して「登録に失敗しました。」なるメッセージを表示するデバイスシグナルＸ（ＤＳＸ）を発生して機器認証を中止する。

【０１２３】

また、ＭＡＣアドレス登録メソッドを１０秒間受信する期間に、デバイス３５２が２秒以内に同じＭＡＣアドレスから複数のＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はユーザに対して「不正なコントローラを発見しました。登録を行いません。」なるメッセージを表示するデバイスシグナルＸ（ＤＳＸ）を発生して機器認証を終了する。

【０１２４】

そして、この場合もコントローラ３５１ではＭＡＣ登録確認メソッドを受信できず、ＭＡＣアドレス登録メソッドをブロードキャストする５分間のタイムリミットが経過して時点で、ユーザに対して「登録に失敗しました。」なるメッセージを表示するデバイスシグナルＸ（ＤＳＸ）を発生して機器認証を中止する。

【０１２５】

このように、コントローラ３５１からのＭＡＣアドレス登録メソッドが競合した場合には、デバイス３５２は機器認証は行わず、競合したＭＡＣアドレスを有するコントローラ３５１のいずれにも応答しないようにして不正アクセスを防ぐと共に、不正に機器認証しようとするコントローラ３５１側に自身の存在を知られないようにしている。

【０１２６】

また、本手順のコントローラ３５１からＭＡＣアドレス登録メソッドをＵＤＰ層でブロードキャストしている段階において、ユーザがコントローラ３５１に備えられた登録作業キャンセル処理を行った場合、コントローラ３５１はただちにＭＡＣアドレス登録メソッドの送信を停止し、代わりに数回ＭＡＣアドレス登録中止メソッドをブロードキャストし、処理を終える。１０秒間のＭＡＣアドレス受信中のデバイスがこのＭＡＣアドレス登録中止メソッドを受信した場合は、ただちに処理を止めて、「機器の登録がキャンセルされました」等のメッセージをユーザに提示する。

【０１２７】

以上説明したように、本実施の形態によれば、ユーザがクライアント（コントローラ３５１）側の登録ボタンを押下すると、コントローラ３５１がＭＡＣアドレス登録メソッドをネットワーク上に一定時間一定周期でブロードキャストする。ユーザがサーバ側の確認ボタンを押下すると、デバイス３５２は一定時間内に同一のＭＡＣアドレスを有するＭＡＣアドレス登録メソッドを受信した場合、そのＭＡＣアドレスをＭＡＣアドレステーブルに

仮記憶する。ユーザがサーバ側の確認ボタンを押下すると、デバイス３５２はＭＡＣ登録確認メソッドをコントローラ３５１にユニキャストし、それを受信したコントローラ３５１は、ＭＡＣ登録確認レスポンスをデバイス３５２へユニキャスト返信する。そしてデバイス３５２がＭＡＣ登録確認レスポンスを受信してユーザに認証登録するか促し、これに応じてユーザがサーバ側に設けられた確認ボタンを押下すると、ＭＡＣアドレステーブルに仮記憶されたＭＡＣアドレスが認証登録される。

【０１２８】

こうして、ユーザがオーソライズしたコントローラ３５１（クライアント）のＭＡＣアドレスだけがデバイス３５２のＭＡＣアドレステーブルに認証登録され、デバイス３５２はＭＡＣアドレステーブルに認証登録されたＭＡＣアドレスのコントローラ３５１（クライアント）とのアクセスを許容するＭＡＣアドレスフィルタリングを実行する結果、ルータを設置して同一サブネット内の他のユーザと隔離せずとも、機器認証装置３５０は認証登録されていない不正な相手からのアクセスを避ける一方、不正に機器認証しようとするコントローラ３５１側にサーバ１の存在を知られないようにするので、セキュリティの高いアクセス制御を提供することが可能になっている。

【０１２９】

なお、本発明による機器認証装置３５０は、上述したアクセス制御を用いて著作権保護する機能も具現できる。すなわち、機器認証するには、上述した通り、ユーザがサーバ側に設けられた確認ボタンとクライアント（コントローラ３５１）側に設けられた登録ボタンとをそれぞれ操作しなければならない。

【０１３０】

この為、同一サブネット内の他のユーザのコントローラ３５１（クライアント）を、ホームネットワーク１００側で機器認証することは出来ず、これ故、ホームネットワーク１００のサーバ１が不正アクセスされ、サーバ１に格納されるコンテンツの著作権が侵害されるような事態に陥ることはない。

【０１３１】

また、上述した実施の一形態では、説明の簡略化を図る為、１対のサーバ／クライアントに配備される機器認証装置３５０を一例に挙げて説明したが、本発明の要旨はこれに限定されず、複数のサーバおよび複数のクライアントを備えるネットワークであっても勿論適用可能である。すなわち、サーバ（デバイス３５２）が複数存在する場合には、ユーザが機器認証しようとするサーバにおいて確認ボタンを押下すれば、そのサーバが必然的に認証元になるからである。

【０１３２】

［クライアント登録処理例－実施例２］

次に、図８および図９を参照してクライアント登録処理の第２実施例について説明する。第２実施例においては、ＭＡＣ登録処理の最終ステップとして、登録完了（Ｃｏｍｐｌｅｔｅ）確認処理を実行する。

【０１３３】

本実施例においても、パスワードを使用せずに機器認証するモードと、パスワードを用いて機器認証するモードとを備えており、以下、各モード別に動作説明する。

【０１３４】

▲１▼ワンタイムパスワード無しの場合

パスワードを使用せずに機器認証するモードでは、図８に示すシーケンスで認証登録が行われる。以下、図８に示すシーケンスを参照して説明する。まず最初にユーザがクライアント（コントローラ３５１）側に設けられた登録ボタンを押下する。すると、コントローラ３５１は登録ボタンの押下に応じて発生するユーザシグナルＡ（ＵＳＡ）に従い、ＭＡＣアドレス登録メソッドをＵＤＰ層でブロードキャストする。ブロードキャストする形態としては、例えば５分間３秒毎のブロードキャスト送信を行う。なお、コントローラ３５１が、５分間経過してデバイス３５２側からのＭＡＣ登録確認メソッドを受信できない場合には、認証に失敗したと判断して最初からやり直す。

【０１３５】
ユーザは、クライアント（コントローラ３５１）側に設けられた登録ボタンを押下した後、サーバ（デバイス３５２）側に移動する。そして、サーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２は確認ボタンの押下に応じて発生するユーザシグナルＢ（ＵＳＢ）に従い、ＭＡＣアドレス登録メソッドを１０秒間受信する。
【０１３６】
１０秒間に同一のＭＡＣアドレスを有する複数のＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はそのＭＡＣアドレスをＭＡＣアドレステーブルに仮記憶した後、ＭＡＣ登録確認メソッドをＴＣＰ層でコントローラ３５１に対してユニキャストする。ＭＡＣ登録確認メソッドには、登録を行ったデバイス名ｄｅｖ－ｎａｍｅが付加される。
【０１３７】
なお、１０秒間に同一のＭＡＣアドレスを有する複数のＭＡＣアドレス登録メソッドを受信しなかった場合、デバイス３５２は「機器を発見できませんでした」なるメッセージを表示するデバイスシグナルＡ（ＤＳＡ）を発生して機器認証を終了する。
【０１３８】
コントローラ３５１は、ＭＡＣ登録確認メソッドを受信すると、ＭＡＣアドレス登録メソッドの送信を停止すると共に、自己の名前ｃｐ－ｎａｍｅを付加したＭＡＣ登録確認レスポンスをデバイス３５２へユニキャスト返信する。その後、コントローラ３５１は、ＭＡＣ登録完了確認メソッドの受信待機状態に移行する。
【０１３９】
デバイス３５２では、コントローラ３５１からのＭＡＣ登録確認レスポンスを受信すると、ＭＡＣ登録確認レスポンスに含まれるコントローラ名ｃｐ－ｎａｍｅに基づき、ユーザに対して「コントローラ“ＹＹＹＹ”を登録できます。本当に登録してよろしいですか？」なるメッセージを表示するデバイスシグナルＣ（ＤＳＣ）を発生する。
【０１４０】
ここで、ユーザがサーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２はそれに応じて発生するユーザシグナルＣ（ＵＳＣ）に従い、登録処理を実行するとともに、ＭＡＣ登録完了確認メソッドをＴＣＰ層でコントローラ３５１に対してユニキャストする。ＭＡＣ登録完了確認メソッドには、登録完了したデバイス名ｄｅｖ－ｎａｍｅが付加される。
【０１４１】
コントローラ３５１は、ＭＡＣ登録完了確認メソッドを受信すると、ＭＡＣ登録完了確認レスポンスをデバイス３５２へユニキャスト返信する。さらに、受信したＭＡＣ登録完了確認メソッドに含まれるデバイス名ｄｅｖ－ｎａｍｅに基づき、ユーザに対して「デバイス“ＸＸＸＸ”に登録されました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生する。
【０１４２】
デバイス３５２は、ＭＡＣ登録完了確認メソッド送信から所定時間、例えば１０秒間待機し、ＭＡＣ登録完了確認レスポンスをコントローラ３５１から受信すると、ユーザに対して「コントローラ“ＹＹＹＹ”を登録しました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して認証登録を終える。
【０１４３】
なお、デバイス３５２が、ＭＡＣ登録完了確認メソッド送信から所定時間、例えば１０秒間待機し、ＭＡＣ登録完了確認レスポンスをコントローラ３５１から受信しない場合には、２つの設定が可能である。１つは、ＭＡＣ登録完了確認レスポンスの受信の有無にかかわらず登録を有効にし、ユーザに対して「コントローラ“ＹＹＹＹ”を登録しました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して認証登録を終える処理態様である。
【０１４４】
もう１つの処理態様は、デバイス３５２がコントローラ３５１からＭＡＣ登録完了確認レ

スポンスを所定時間内に受信しなかった場合、登録を無効にし、デバイス３５２側でユーザに対して「コントローラ“ＹＹＹＹ”の登録をキャンセルしました。」なるメッセージを表示して処理を終える態様である。なおこの登録無効化処理を実行する場合は、デバイス３５２はコントローラ３５１に対して登録キャンセル通知を送信し、コントローラ３５１においてユーザに対して「デバイス“ＸＸＸＸ”への登録はキャンセルされました。」とのメッセージを表示する構成とすることが好ましい。

【０１４５】

デバイス３５２がコントローラ３５１からのＭＡＣ登録完了確認レスポンスを所定時間受信しなかった場合の処理としては上記２つの処理態様の設定が可能である。

【０１４６】

コントローラ３５１がデバイス３５２のＭＡＣリストに登録され、認証登録が済むと、その後、デバイス３５２はコントローラ３５１からのサービス検索処理として実行されるＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合、ＭＡＣリストを参照し、登録済みデバイス３５２からの要求であることを確認し、サービス検索に対する応答を行う。

【０１４７】

なお、デバイス３５２は、完全に認証登録し終える以前に、コントローラ３５１からＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合には、ＭＡＣリストに未登録であるので、デバイス３５２は応答しない。

【０１４８】

▲２▼ワンタイムパスワード有りの場合

次に、図９に示すシーケンスを参照し、パスワードを用いて機器認証するモード下で行われる認証登録の動作について説明する。まず最初にユーザがクライアント（コントローラ３５１）側に設けられた登録ボタンを押下する。すると、コントローラ３５１は登録ボタンの押下に応じて発生するユーザシグナルＡ（ＵＳＡ）に従い、ＭＡＣアドレス登録メソッドをＵＤＰ層でブロードキャストする。ブロードキャストする形態としては、例えば5分間3秒毎のブロードキャスト送信を行う。なお、コントローラ３５１が、５分間経過してデバイス３５２側からのＭＡＣ登録確認メソッドを受信できない場合には、認証に失敗したと判断して最初からやり直す。

【０１４９】

ユーザは、クライアント（コントローラ３５１）側に設けられた登録ボタンを押下した後、サーバ（デバイス３５２）側に移動する。そして、サーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２は確認ボタンの押下に応じて発生するユーザシグナルＢ（ＵＳＢ）に従い、ＭＡＣアドレス登録メソッドを１０秒間受信する。

【０１５０】

１０秒間に同一のＭＡＣアドレスを有する複数のＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はそのＭＡＣアドレスをＭＡＣアドレステーブルに仮記憶し、ユーザに対して「機器を発見しました」なるメッセージを表示するデバイスシグナルＡ（ＤＳＡ）を発生し、ＭＡＣ登録確認メソッドをＴＣＰ層でユニキャストする。ＭＡＣ登録確認メソッドには、パスワード要求フラグが付加される。

【０１５１】

なお、１０秒間に同一のＭＡＣアドレスを有する複数のＭＡＣアドレス登録メソッドを受信しなかった場合、デバイス３５２は「機器を発見できませんでした」なるメッセージを表示するデバイスシグナルＡ（ＤＳＡ）を発生して機器認証を終了する。

【０１５２】

コントローラ３５１は、パスワード要求フラグが付加されたＭＡＣ登録確認メソッドを受信すると、ＭＡＣアドレス登録メソッドの送信を停止すると共に、デバイス３５２へＭＡＣ登録確認レスポンスをユニキャストで返信する。

【０１５３】

デバイス３５２は、このＭＡＣ登録確認レスポンスを受信すると、ユーザに対して「コン

トローラ“ＹＹＹＹ”のためのワンタイムパスワードは”○○○○”です。」なるメッセージを表示するデバイスシグナルＣ（ＤＳＣ）を発生し、ワンタイムパスワードを提示した状態で５分間待機する。図９においては、パスワードとして［１３３４］を例示している。このパスワードは、デバイス３５２が例えば乱数発生処理により生成する。

【０１５４】

一方、コントローラ３５１は、受信したＭＡＣ登録確認メソッドに含まれるパスワード要求フラグに基づき、ユーザに対して「デバイス“ＸＸＸＸ”のパスワードを入力してください。」なるメッセージを表示するデバイスシグナルＢ（ＤＳＢ）を発生し、ワンタイムパスワードの入力を５分間待機する。

【０１５５】

この待機中にユーザがサーバ側からクライアント（コントローラ３５１）側に移動する。そして、クライアント（コントローラ３５１）側に移動してきたユーザは、デバイス３５２側で表示されたパスワードをクライアント（コントローラ３５１）側の入力手段から入力する。すると、コントローラ３５１は入力されたパスワードを付加したパスワードメソッドをデバイス３５２にＴＣＰ層でユニキャストして１０秒間待機する。

【０１５６】

デバイス３５２では、ワンタイムパスワード提示後の５分間の待機状態中にコントローラ３５１からのパスワードメソッドを受信すると、自己に予め設定されているワンタイムパスワードと照合する。以下、パスワード照合ＯＫの場合とパスワード照合ＮＧの場合とに分けて動作説明する。

【０１５７】

（ａ）パスワード照合ＯＫの場合

コントローラ３５１から送られてきたワンタイムパスワードが適正、すなわちデバイスが設定したワンタイムパスワードと一致した場合は、デバイス３５２はＭＡＣアドレステーブルに仮記憶されたＭＡＣアドレスを正式に認証登録した後、コントローラ３５１に照合ＯＫを付加したパスワードレスポンスをユニキャストで返信する。

【０１５８】

コントローラ３５１は、パスワードメソッドをデバイス３５２にＴＣＰ層でユニキャストして１０秒間待機中に、デバイス３５２から照合ＯＫが付加されたパスワードレスポンスを受信すると、ＭＡＣ登録完了確認メソッドの受信待機状態に移行する。

【０１５９】

さらに、デバイス３５２は、コントローラ名ｃｐ－ｎａｍｅに基づき、ユーザに対して「コントローラ“ＹＹＹＹ”を登録できます。本当に登録してよろしいですか？」なるメッセージを表示するデバイスシグナルＣ（ＤＳＣ）を発生する。

【０１６０】

ここで、ユーザがサーバ側に設けられた確認ボタンを押下する。すると、デバイス３５２はそれに応じて発生するユーザシグナルＣ（ＵＳＣ）に従い、登録処理を実行するとともに、ＭＡＣ登録完了確認メソッドをＴＣＰ層でコントローラ３５１に対してユニキャストする。ＭＡＣ登録完了確認メソッドには、登録完了したデバイス名ｄｅｖ－ｎａｍｅが付加される。

【０１６１】

コントローラ３５１は、ＭＡＣ登録完了確認メソッドを受信すると、ＭＡＣ登録完了確認レスポンスをデバイス３５２へユニキャスト返信する。さらに、受信したＭＡＣ登録完了確認メソッドに含まれるデバイス名ｄｅｖ－ｎａｍｅに基づき、ユーザに対して「デバイス“ＸＸＸＸ”に登録されました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生する。

【０１６２】

デバイス３５２は、ＭＡＣ登録完了確認メソッド送信から所定時間、例えば１０秒間待機し、ＭＡＣ登録完了確認レスポンスをコントローラ３５１から受信すると、ユーザに対して「コントローラ“ＹＹＹＹ”を登録しました。」なるメッセージを表示するデバイスシ

グナルＺ（ＤＳＺ）を発生して認証登録を終える。
【０１６３】
なお、デバイス３５２が、ＭＡＣ登録完了確認メソッド送信から所定時間、例えば１０秒間待機し、ＭＡＣ登録完了確認レスポンスをコントローラ３５１から受信しない場合には、２つの設定が可能である。１つは、ＭＡＣ登録完了確認レスポンスの受信の有無にかかわらず登録を有効にし、ユーザに対して「コントローラ“ＹＹＹＹ”を登録しました。」なるメッセージを表示するデバイスシグナルＺ（ＤＳＺ）を発生して認証登録を終える処理態様である。
【０１６４】
もう１つの処理態様は、デバイス３５２がコントローラ３５１からＭＡＣ登録完了確認レスポンスを所定時間内に受信しなかった場合、登録を無効にし、デバイス３５２側でユーザに対して「コントローラ“ＹＹＹＹ”の登録をキャンセルしました。」なるメッセージを表示して処理を終える態様である。なおこの登録無効化処理を実行する場合は、デバイス３５２はコントローラ３５１に対して登録キャンセル通知を送信し、コントローラ３５１においてユーザに対して「デバイス“ＸＸＸＸ”への登録はキャンセルされました。」とのメッセージを表示する構成とすることが好ましい。
【０１６５】
デバイス３５２がコントローラ３５１からのＭＡＣ登録完了確認レスポンスを所定時間受信しなかった場合の処理としては上記２つの処理態様の設定が可能である。
【０１６６】
コントローラ３５１がデバイス３５２のＭＡＣリストに登録され、認証登録が済むと、その後、デバイス３５２はコントローラ３５１からのサービス検索処理として実行されるＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合、ＭＡＣリストを参照し、登録済みデバイス３５２からの要求であることを確認し、サービス検索に対する応答を行う。
【０１６７】
なお、デバイス３５２は、完全に認証登録し終える以前に、コントローラ３５１からＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈを受信した場合には、ＭＡＣリストに未登録であるので、デバイス３５２は応答しない。
【０１６８】
（ｂ）パスワード照合ＮＧの場合
コントローラ３５１から送られてきたワンタイムパスワードが不正、すなわち、デバイスが設定したワンタイムパスワードと一致しなかった場合は、デバイス３５２はコントローラ３５１に照合ＮＧを付加したパスワードレスポンスをユニキャストで返信し、コントローラ３５１から再度パスワード入力されるのを５分間待機する。
【０１６９】
そして、この待機期間中にパスワード照合ＮＧが３回連続すると、デバイス３５２はパスワード入力の再試行を中止させ、ユーザに対して「コントローラ“ＹＹＹＹ”を登録できません。」なるメッセージを表示するデバイスシグナルＥ（ＤＳＥ）を発生して機器認証を終える。この場合、デバイス３５２では、ＭＡＣアドレステーブルに仮記憶されたＭＡＣアドレスを消去する。
【０１７０】
一方、コントローラ３５１では、デバイス３５２から再試行中止のリザルトコードが付加されたパスワードレスポンスを受信すると、ユーザに対して「デバイス“ＸＸＸＸ”には登録できません。」なるメッセージを表示するデバイスシグナルＥ（ＤＳＥ）を発生して機器認証を終了する。
【０１７１】
なお、本実施例２において、デバイス３５２がＭＡＣアドレス登録メソッドを１０秒間受信する最中に、ＭＡＣアドレス登録メソッドをブロードキャストしたコントローラ３５１とは異なる他のコントローラを検出した場合の動作についは、実施例１と同様の処理（図

７参照）となり、デバイス３５２はユーザに対して「複数のコントローラを発見しました。登録を行いません。」なるメッセージを表示して機器認証を中止する。

【０１７２】

こうして、デバイス３５２側が一方的に機器認証を終了すると、コントローラ３５１はＭＡＣ登録確認メソッドを受信できず、ＭＡＣアドレス登録メソッドをブロードキャストする５分間のタイムリミットが経過して時点で、ユーザに対して「登録に失敗しました。」なるメッセージを表示して機器認証を中止する。

【０１７３】

また、ＭＡＣアドレス登録メソッドを１０秒間受信する期間に、デバイス３５２が２秒以内に同じＭＡＣアドレスから複数のＭＡＣアドレス登録メソッドを受信した場合、デバイス３５２はユーザに対して「不正なコントローラを発見しました。登録を行いません。」なるメッセージを表示して機器認証を終了する。

【０１７４】

そして、この場合もコントローラ３５１ではＭＡＣ登録確認メソッドを受信できず、ＭＡＣアドレス登録メソッドをブロードキャストする５分間のタイムリミットが経過して時点で、ユーザに対して「登録に失敗しました。」なるメッセージを表示して機器認証を中止する。

【０１７５】

このように、コントローラ３５１からのＭＡＣアドレス登録メソッドが競合した場合には、デバイス３５２は機器認証を行わず、競合したＭＡＣアドレスを有するコントローラ３５１のいずれにも応答しないようにして不正アクセスを防ぐと共に、不正に機器認証しようとするコントローラ３５１側に自身の存在を知られないようにしている。

【０１７６】

以上説明したように、本実施例２の処理構成によれば、ＭＡＣ登録処理の最終ステップとして、登録完了（Ｃｏｍｐｌｅｔｅ）確認処理を実行する構成とし、サーバ（デバイス）側からＭＡＣ登録完了確認をクライアント（コントローラ）側に対して送信する構成としたので、双方の機器において登録完了メッセージに基づいて、ユーザが最終的な登録完了の確認をすることが可能となる。

【０１７７】

また、クライアント（コントローラ）側では、ＭＡＣ登録完了確認通知をサーバ（デバイス）側から受信したことを条件として、サービス検索処理としてのＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈの送信処理を実行すれば、サーバ（デバイス）側においてＭＡＣ登録が完了していることが保障されているので、サービス検索処理の応答を確実に受信することが可能となる。

【０１７８】

なお、この処理シーケンスは、ユーザによる明示的なＭ－ｓｅａｒｃｈの送信処理開始命令を実行することなく、クライアント（コントローラ）側の機器のプログラムに基づいて自動実行する構成としてもよい。すなわち、ＭＡＣ登録完了確認通知をサーバ（デバイス）側から受信したことを条件としてＭ－ｓｅａｒｃｈの送信処理を自動的に実行する。このような自動実行処理シーケンスを設定することで、ユーザの入力処理等を介在させることなく、クライアントはサーバに対する登録処理に続いてサーバからサービス情報を受領することが可能となる。

【０１７９】

［登録済みコントローラからの登録要求］

次に、すでにサーバ（デバイス）側のＭＡＣリストに対する登録がなされているクライアント（コントローラ）からのＭＡＣアドレス登録要求が発生した場合の処理について、図１０のフローチャートを参照して説明する。

【０１８０】

通常の登録処理においては、上述したようにサーバ（デバイス）は、クライアント（コントローラ）からのＭＡＣアドレス登録要求を受信すると、ＭＡＣ登録確認をクライアント

に対して送信する。しかし、登録要求に含まれるＭＡＣアドレスが、サーバの有するＭＡＣリストに登録されたものと同一であった場合には、サーバ（デバイス）は、クライアント（コントローラ）に対して、すでに登録済みであることを示す登録済み通知を送信する。図１０に示すフローの各ステップについて説明する。

【０１８１】

まず、クライアント側のコントローラ３５１は、ステップＳ１１１において、ユーザ指示に基づいてＭＡＣアドレス登録メソッドをＵＤＰ層でブロードキャストする。サーバ側のデバイス３５２は、ステップＳ２１１において、コントローラからのＭＡＣ登録要求に含まれるＭＡＣアドレスがＭＡＣリストに登録済みか否かを判定し、リストに含まれていない場合は、ステップＳ２２１において、通常のＭＡＣ登録処理シーケンスを実行する。上述した各処理例に従った処理である。

【０１８２】

一方、ステップＳ２１１において、デバイス３５２が、コントローラからのＭＡＣ登録要求に含まれるＭＡＣアドレスがＭＡＣリストに登録済みであると判定した場合は、ステップＳ２１２において、登録済みであることを明示した登録済み通知をＭＡＣ登録確認としてクライアント側のコントローラ３５１に送信する。

【０１８３】

クライアント側のコントローラ３５１は、ステップＳ１１１のＭＡＣ登録要求送信後、登録確認を待機し、待機時間内に登録確認を受信しなかった場合（ステップＳ１１２：Ｎｏ、ステップＳ１２１：Ｙｅｓ）は、ステップＳ１２２において上位のアプリケーションプログラムへタイムアウト通知を実行し、上位のアプリケーションプログラムにより、登録確認受信の失敗を示すメッセージ表示処理等が実行される。

【０１８４】

規定時間内に登録確認を受信した場合は、ステップＳ１１３に進み、登録済み通知であるか否かが判定される。登録済み通知でない場合は、ステップＳ１２３に進み、通常のＭＡＣ登録処理シーケンスを実行する。上述した各処理例に従った処理である。登録済み通知である場合は、ステップＳ１１４に進み、登録済み通知に対する了解応答メッセージとしての登録確認応答をサーバ（デバイス）側に送信する。

【０１８５】

サーバ（デバイス３５２）は、ステップＳ２１２の登録済み通知を送信後、登録確認応答を待機し、待機時間内に登録確認応答を受信しなかった場合（ステップＳ２１３：Ｎｏ、ステップＳ２２２：Ｙｅｓ）は、ステップＳ２２３において上位のアプリケーションプログラムへタイムアウト通知を実行し、上位のアプリケーションプログラムにより、登録確認応答受信の失敗を示すメッセージ表示処理等を実行し処理を終了する。

【０１８６】

待機時間内に登録確認応答を受信した場合（ステップＳ２１３：Ｙｅｓ）は、ステップＳ２１４において、上位のアプリケーションプログラムへ登録済み通知を実行する。上位のアプリケーションプログラムは、例えば、登録済みであることを示すメッセージ表示処理等を実行し処理を終了する。

【０１８７】

一方、ステップＳ１１４において、登録済み通知に対する了解応答メッセージとしての登録確認応答をサーバ（デバイス）側に送信したクライアント（コントローラ３５１）は、ステップＳ１１５において、上位のアプリケーションプログラムへ登録済み通知を実行する。上位のアプリケーションプログラムは、例えば、登録済みであることを示すメッセージ表示処理等を実行し処理を終了する。

【０１８８】

このように、すでにサーバのＭＡＣリストに登録されたクライアントからのＭＡＣ登録要求があった場合は、機器間において登録済みであることの確認通知処理が実行されるので、これらの通知に基づいて登録済みであることのメッセージ表示が可能となり、ユーザは、クライアント機器がすでにサーバに登録されていることを確認することが可能となる。

【０１８９】
［登録要求処理におけるバージョン管理］
前述のクライアント登録処理例の実施例１および実施例２において説明したように、サーバクライアント間で実行される機器登録処理シーケンスは、異なるシーケンスに従って実行される場合がある。これは、クライアントあるいはサーバに格納されている機器認証プログラムのバージョンによって処理シーケンスが異なることになる。例えば上述のクライアント登録処理例の実施例１をバージョン１．０、実施例２をバージョン１．１のプログラムのように、異なるバージョンとして定義される。
【０１９０】
サーバおよびクライアントの双方に格納された機器認証処理プログラムが同一のバージョンである場合には、双方が一致した処理シーケンスに従って処理が実行されることになるが、双方の機器に異なるバージョンの処理プログラムが格納されている場合に、それぞれが異なる処理シーケンスで処理を行ってしまうと、結果として正常な機器登録処理が実行されないことになる。
【０１９１】
そこで、本発明の構成においては、サーバクライアント間において、処理プログラムのバージョン情報を通知し、処理シーケンスを一致させて機器登録を実行する。
【０１９２】
なお、処理プログラムのバージョンは、古いものから新しいものに従って、順次、［１．０］、［１．１］、［１．２］．．、［２．０］、［２．１］．．のように設定される。［ｘ．ｙ］の２つの数値は、それぞれｘ＝メジャーバージョン、ｙ＝マイナーバージョンと定義される。
【０１９３】
ここで、メジャーバージョンが等しいものについては、より新しいバージョンは古いバージョンの処理シーケンスをサポートする。すなわち、バージョン［１．２］は、［１．０］、［１．１］をサポートする。バージョン［２．１］は、［２．０］をサポートする。機器登録処理シーケンスにおけるバージョン情報の通知に基づく処理について、図１１、図１２を参照して説明する。
【０１９４】
図１１は、サーバ（デバイス）側において、クライアント（コントローラ）側からのバージョン通知に基づく処理シーケンスの設定手順を説明するフローチャートである。サーバは、ステップＳ５０１において、クライアントからのＭＡＣ登録要求を受信する。これは、上述のクライアント登録処理例の実施例１、実施例２において説明したＭＡＣアドレス登録メソッドであり、ＵＤＰ層で例えば５分間３秒毎のブロードキャストデータである。
【０１９５】
クライアントは、クライアントからのＭＡＣ登録要求に自己の実行するＭＡＣ登録処理シーケンスの実行プログラムのバージョン情報、例えば［１．０］、［１．１］などを格納し、サーバに送信する。
【０１９６】
サーバは、ステップＳ５０１において、クライアントからのＭＡＣ登録要求（Ｒｅｇｉｓｔｅｒ）を受信すると、ステップＳ５０２において、クライアントからのＭＡＣ登録要求に含まれるバージョン情報中のメジャーバージョンと、自己の実行可能な処理プログラムのバージョン情報のメジャーバージョンの比較に基づいて処理可能性の判定を行う。
【０１９７】
前述したように、同一のメジャーバージョンであれば、処理可能であるので、クライアントからのＭＡＣ登録要求に含まれるバージョン情報中のメジャーバージョンと、自己の実行可能な処理プログラムのバージョン情報のメジャーバージョンが一致する場合はステップＳ５０３に進む。一致しない場合は、処理不可と判定し、そのまま処理を終了する。なお、この場合、サーバは処理不可であることをクライアントに通知する処理を実行する構成としてもよい。

【０１９８】
ステップＳ５０３では、クライアントからのＭＡＣ登録要求に含まれるバージョン情報中のマイナーバージョンと、自己の実行可能な処理プログラムのバージョン情報のマイナーバージョンとを比較する。クライアントのＭＡＣ登録要求に含まれるマイナーバージョンが自己の実行可能な処理プログラムのマイナーバージョンより小であれば、ステップＳ５０５に進み、クライアントからのＭＡＣ登録要求に含まれるバージョン情報に合わせた処理シーケンスでの処理を実行する。
【０１９９】
一方、クライアントのＭＡＣ登録要求に含まれるマイナーバージョンが自己の実行可能な処理プログラムのマイナーバージョンより小でなければ、ステップＳ５０４に進み、自己の保有する処理プログラムのバージョンに合わせた処理シーケンスでの処理を実行する。
【０２００】
次に、図１２を参照してクライアント（コントローラ）側において、サーバ（デバイス）側からのバージョン通知に基づいて処理シーケンスを設定する手順について説明する。クライアントは、ステップＳ７０１において、サーバからのＭＡＣ登録確認要求（Ｃｏｎｆｉｒｍ）を受信する。これは、上述のクライアント登録処理例の実施例１、実施例２において説明したクライアントから送信するＭＡＣアドレス登録メソッドに対するサーバからの応答であり、ＴＣＰ層でのユニキャストデータである。
【０２０１】
サーバは、サーバから送信するＭＡＣ登録確認に自己の実行するＭＡＣ登録処理シーケンスの実行プログラムのバージョン情報、例えば［１．０］、［１．１］などを格納し、クライアントに送信する。
【０２０２】
クライアントは、ステップＳ７０１において、サーバからのＭＡＣ登録確認を受信すると、ステップＳ７０２において、サーバからのＭＡＣ登録確認に含まれるバージョン情報中のメジャーバージョンと、自己の実行可能な処理プログラムのバージョン情報のメジャーバージョンの比較に基づいて処理可能性の判定を行う。
【０２０３】
同一のメジャーバージョンであれば、処理可能であるので、サーバからのＭＡＣ登録確認に含まれるバージョン情報中のメジャーバージョンと、自己の実行可能な処理プログラムのバージョン情報のメジャーバージョンが一致する場合はステップＳ７０３に進む。一致しない場合は、処理不可と判定し、そのまま処理を終了する。なお、この場合、クライアントは処理不可であることをサーバに通知する処理を実行する構成としてもよい。
【０２０４】
ステップＳ７０３では、サーバからのＭＡＣ登録確認に含まれるバージョン情報中のマイナーバージョンと、自己の実行可能な処理プログラムのバージョン情報のマイナーバージョンとを比較する。サーバのＭＡＣ登録確認に含まれるマイナーバージョンが自己の実行可能な処理プログラムのマイナーバージョンより小であれば、ステップＳ７０５に進み、サーバからのＭＡＣ登録確認に含まれるバージョン情報に合わせた処理シーケンスでの処理を実行する。
【０２０５】
一方、サーバのＭＡＣ登録確認に含まれるマイナーバージョンが自己の実行可能な処理プログラムのマイナーバージョンより小でなければ、ステップＳ７０４に進み、自己の保有する処理プログラムのバージョンに合わせた処理シーケンスでの処理を実行する。
【０２０６】
このように、本発明の構成においては、サーバクライアント間での機器登録処理において、双方の機器の有する処理プログラムのバージョン情報の通知を実行し、処理シーケンスを調整して機器登録処理を実行する構成としたので、様々なバージョンのプログラムを格納した機器間においても、統一した処理シーケンスに従った機器登録処理が実行できる。
【０２０７】

［サーバおよびクライアントの機能構成］
サーバおよびクライアント装置のハードウェア構成については、先に図２を参照して説明した通りであり、上述した各種の処理は、サーバクライアントそれぞれの記憶部に格納されたプログラムに従って制御部としてのＣＰＵが実行する。
【０２０８】
ＣＰＵによって実行される処理は、例えばサーバ側では、クライアントからの要求を入力し、入力情報の解析、解析結果に基づくＭＡＣリスト、すなわちアクセス制御情報へ登録する処理、クライアントと送受信するパケット生成、解析処理、さらに、登録処理における各種メッセージ出力、ユーザ入力情報の解析処理等である。クライアント側の処理としては、サーバから受信する情報解析処理、サーバと送受信するパケット生成、解析処理、さらに、登録処理における各種メッセージ出力、ユーザ入力情報の解析処理等である
【０２０９】
基本的にこれらの処理は、サーバ、クライアント装置の制御部としてのＣＰＵの制御の下に予め格納された処理プログラムに従って実行される。制御部としてのＣＰＵが実行する処理および記憶部の格納データ等について、図１３および図１４を参照して説明する。図１３は、サーバの主要機能構成を説明するブロック図であり、図１４は、クライアントの主要機能構成を説明するブロック図である。
【０２１０】
まず、図１３のサーバの機能構成を示すブロック図を参照してサーバの機能構成について説明する。データ送受信部５０１は、クライアントに対するパケット、クライアントからのパケットを受信する。データ送受信部５０１は、送信パケットの生成処理、受信パケットの解析処理を行う。パケットのアドレス設定、アドレス認識、データ部に対するデータ格納、データ部からのデータ取得処理などである。
【０２１１】
登録処理部５０２は、クライアントからの登録要求に基づく一連の処理シーケンスを実行する。上述した各シーケンス図、フローに対応する処理を記憶部５０５に格納された機器認証プログラム５２１に従って実行する。登録処理部５０２は、パスワードの生成処理および照合処理を実行するパスワード生成判定部５１１と、図１１のフローを参照して説明したプログラムバージョンを参照し、処理シーケンスを決定するバージョン判定部５１２を有する。
【０２１２】
データ入力部５０３は、登録処理部５０２に対するユーザシグナルを入力するキーボード等の入力部である。データ出力部５０４は、登録処理部５０２が出力するデバイスシグナルに基づくメッセージデータ等を表示するディスプレイ等の出力部である。
【０２１３】
記憶部５０５には、登録処理シーケンスを実行するための機器認証プログラム５２１が格納される。この処理プログラムにはメジャーバージョンとマイナーバージョンからなるバージョン情報が付加されている。記憶部５０５には、さらにクライアントのアクセス制御情報としてクライアントＭＡＣアドレスを格納したＭＡＣリスト５２２が格納される。
【０２１４】
次に、クライアント装置の機能構成について、図１４を参照して説明する。データ送受信部５０１は、クライアントに対するパケット、クライアントからのパケットを受信する。データ送受信部６０１は、送信パケットの生成処理、受信パケットの解析処理を行う。パケットのアドレス設定、アドレス認識、データ部に対するデータ格納、データ部からのデータ取得処理などである。
【０２１５】
登録要求処理部６０２は、サーバに対するクライアント登録要求処理の一連の処理シーケンスを実行する。上述した各シーケンス図、フローに対応する処理を記憶部６０５に格納された機器認証プログラム６２１に従って実行する。登録要求処理部６０２は、図１２のフローを参照して説明したプログラムバージョンを参照し、処理シーケンスを決定するバ

ージョン判定部６１１を有する。
【０２１６】
データ入力部６０３は、登録要求処理部６０２に対するユーザシグナルを入力するキーボード等の入力部である。データ出力部６０４は、登録要求処理部６０２が出力するデバイスシグナルに基づくメッセージデータ等を表示するディスプレイ等の出力部である。
【０２１７】
記憶部６０５には、登録処理シーケンスを実行するための機器認証プログラム６２１が格納される。この処理プログラムにはメジャーバージョンとマイナーバージョンからなるバージョン情報が付加されている。記憶部６０５には、さらにクライアントのＭＡＣアドレス６２２が格納される。
【０２１８】
サーバ、およびクライアントは、機能的には図１３、図１４に示す各機能を有し、上述した各処理を実行する。ただし、図１３、図１４に示すブロック図は、機能を説明するブロック図であり、実際には、図２に示すＰＣ等のハードウェア構成におけるＣＰＵの制御の下に各種の処理プログラムが実行される。
【０２１９】
以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。
【０２２０】
なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。
【０２２１】
例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。
【０２２２】
なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。
【０２２３】
なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【０２２４】
【発明の効果】
以上、説明したように、本発明によれば、ユーザ操作によってオーソライズされたクライアントのＭＡＣアドレスだけがサーバ側に認証登録され、サーバは認証登録されたＭＡＣアドレスを有するクライアントとのアクセスだけを許容する結果、同一サブネット内の他

のユーザと隔離するためのルータを設置せずとも、認証登録されていない不正な相手からのアクセスを避ける一方、不正に機器認証しようとするクライアント（コントローラ３５１）側にサーバの存在を知られないようにすることができる。

【０２２５】

さらに、本発明の構成によれば、ＭＡＣアドレスが異なる複数の競合した登録要求を受信した場合、それら競合したＭＡＣアドレスを仮記憶させず、競合したＭＡＣアドレスを持つクライアント（コントローラ３５１）側からの登録要求を無視して機器認証を中止するので、不正アクセスを防ぐと共に、不正に機器認証しようとするクライアント（コントローラ３５１）側に自身の存在を知られないようにすることができる。

【０２２６】

さらに、本発明の構成によれば、パスワード照合して一致した場合にのみオーソライズされたクライアントのＭＡＣアドレスだけがサーバ側に認証登録され、サーバは認証登録されたＭＡＣアドレスを有するクライアントとのアクセスだけを許容する結果、同一サブネット内の他のユーザと隔離するためのルータを設置せずとも、認証登録されていない不正な相手からのアクセスを避ける一方、不正に機器認証しようとするクライアント（コントローラ３５１）側にサーバの存在を知られないようにする、セキュリティの高いアクセス制御を提供することができる。

【０２２７】

さらに、本発明の構成によれば、入力されるパスワードと自己に予め設定されているパスワードとの照合が所定回連続して不一致になった場合、仮記憶しておいたＭＡＣアドレスを消去して機器認証を中止するので、パスワード詐称による不正アクセスを防ぐことができる。

【０２２８】

さらに、本発明の構成によれば、ＭＡＣ登録処理の最終ステップとして、登録完了（Ｃｏｍｐｌｅｔｅ）確認処理を実行する構成とし、サーバ（デバイス）側からＭＡＣ登録完了確認をクライアント（コントローラ）側に対して送信する構成としたので、双方の機器において登録完了メッセージに基づいて、ユーザが最終的な登録完了の確認をすることが可能となる。また、クライアント（コントローラ）側では、ＭＡＣ登録完了確認通知をサーバ（デバイス）側から受信したことを条件として、サービス検索処理としてのＳＳＤＰ（シンプルサービス検出プロトコル）のＭ－ｓｅａｒｃｈの送信処理を実行すれば、サーバ（デバイス）側においてＭＡＣ登録が完了していることが保障されているので、サービス検索処理の応答を確実に受信することが可能となる。

【０２２９】

ＭＡＣ登録処理の最終ステップとして、登録完了（Ｃｏｍｐｌｅｔｅ）確認処理を実行する構成とすることで、ＭＡＣ登録完了確認通知をサーバ（デバイス）側から受信したことを条件としてＭ－ｓｅａｒｃｈの送信処理を自動的に実行することが可能となり、ユーザの入力処理等を介在させることなく、クライアントはサーバに対する登録処理に続いてサーバからサービス情報を受領することが可能となる。

【０２３０】

さらに、本発明の構成によれば、すでにサーバのＭＡＣリストに登録されたクライアントからのＭＡＣ登録要求があった場合は、機器間において登録済みであることの確認通知処理が実行されるので、これらの通知に基づいて登録済みであることのメッセージ表示が可能となり、ユーザは、クライアント機器がすでにサーバに登録されていることを確認することが可能となる。

【０２３１】

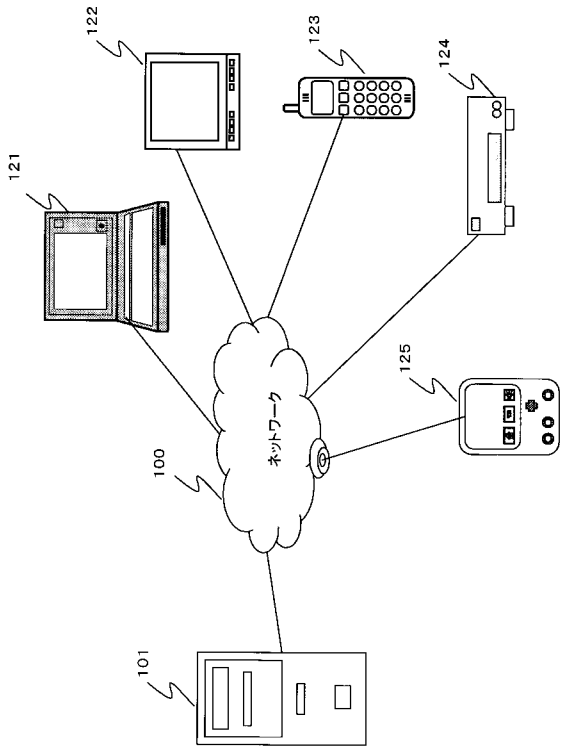
さらに、本発明の構成によれば、サーバクライアント間での機器登録処理において、双方の機器の有する処理プログラムのバージョン情報の通知を実行し、処理シーケンスを調整して機器登録処理を実行する構成としたので、様々なバージョンのプログラムを格納した機器間においても、統一した処理シーケンスに従った機器登録処理が実行できる。

【図面の簡単な説明】

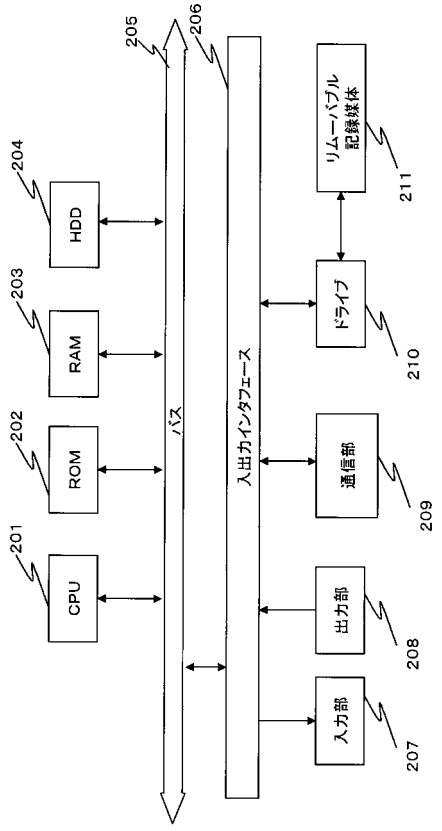
【図１】本発明の適用可能なネットワーク構成例を示す図である。
【図２】ネットワーク接続機器の構成例について説明する図である。
【図３】本発明の実施の一形態によるホームネットワークの構成を示すブロック図である。
【図４】機器認証装置の機能的構成を示すブロック図である。
【図５】クライアント登録処理例の実施例１において、パスワードを使用せずに機器認証する場合の動作を示すシーケンス図である。
【図６】クライアント登録処理例の実施例１において、パスワードを使用して機器認証する場合の動作を示すシーケンス図である。
【図７】ＭＡＣアドレス登録メソッドが競合した場合の動作を示すシーケンス図である。
【図８】クライアント登録処理例の実施例２において、パスワードを使用せずに機器認証する場合の動作を示すシーケンス図である。
【図９】クライアント登録処理例の実施例２において、パスワードを使用して機器認証する場合の動作を示すシーケンス図である。
【図１０】クライアント登録処理において、登録済み通知処理を中心として説明するフローチャートである。
【図１１】クライアント登録処理において、サーバにおいて実行するバージョン調整処理を説明するフローチャートである。
【図１２】クライアント登録処理において、クライアントにおいて実行するバージョン調整処理を説明するフローチャートである。
【図１３】サーバの機能構成を示すブロック図である。
【図１４】クライアントの機能構成を示すブロック図である。
【符号の説明】
１００　ネットワーク
１０１　サーバ
１２１　ＰＣ
１２２　モニター
１２３　携帯電話
１２４　再生機
１２５　ＰＤＡ
２０１　ＣＰＵ
２０２　ＲＯＭ
２０３　ＲＡＭ
２０４　ＨＤＤ
２０５　バス
２０６　入出力インタフェース
２０７　入力部
２０８　出力部
２０９　通信部
２１０　ドライブ
２１１　リムーバブル記録媒体
３００　ホームネットワーク
３１０　サーバ
３２０　クライアント
３２１　ネットワーク対応機器
３２２　テレビジョン受像機
３５０　機器認証装置
３５１　コントローラ（第１の装置、第１の処理および第１のプログラム）
３５２　デバイス（第２の装置、第２の処理および第２のプログラム）
５０１　データ送受信部

５０２　登録処理部
５０３　データ入力部
５０４　データ出力部
５０５　記憶部
５１１　パスワード生成判定部
５１２　バージョン判定部
５２１　機器認証プログラム
５２２　ＭＡＣリスト
６０１　データ送受信部
６０２　登録要求処理部
６０３　データ入力部
６０４　データ出力部
６０５　記憶部
６１１　バージョン判定部
６２１　機器認証プログラム
６２２　クライアントＭＡＣアドレス

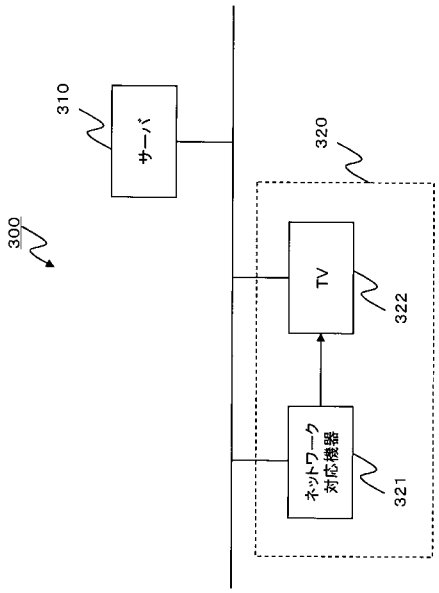
【図１】



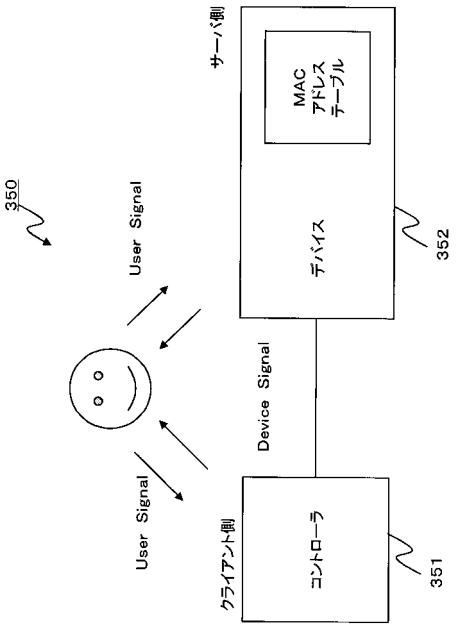
【図２】



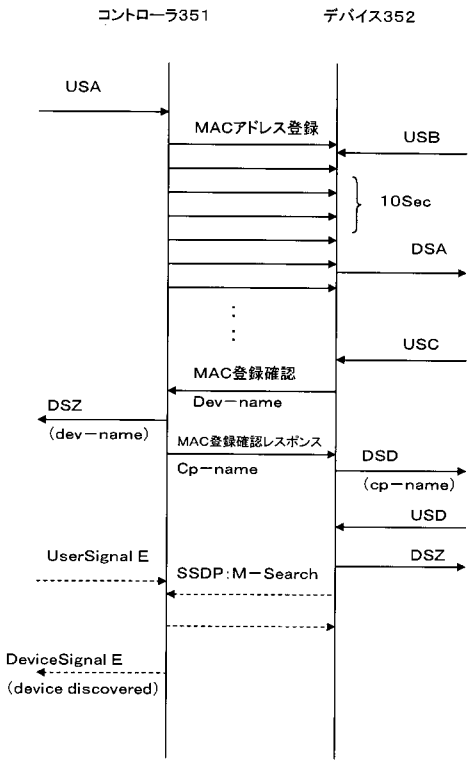
【図３】


300
310
サーバ
320
TV
322
ネットワーク対応機器
321

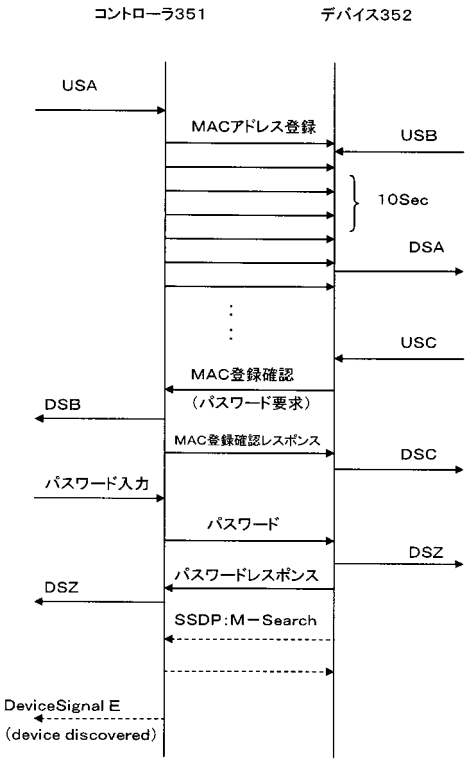
【図４】


350
User Signal
サーバ側
MAC アドレス テーブル
デバイス
352
Device Signal
User Signal
クライアント側
コントローラ
351

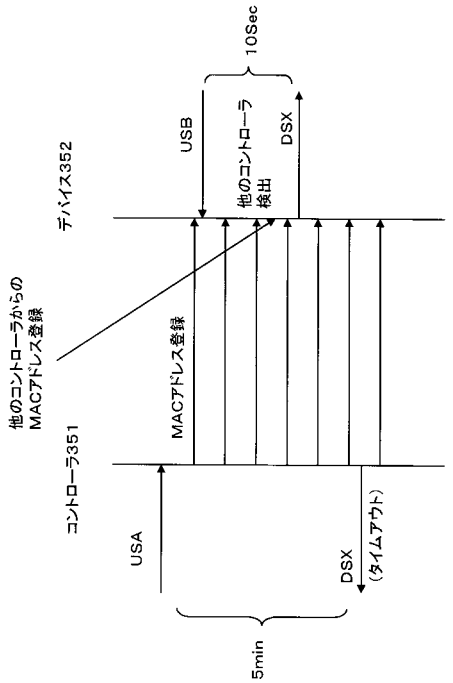
【図５】


コントローラ351
デバイス352
USA
MACアドレス登録
USB
10Sec
DSA
USC
MAC登録確認
Dev−name
DSZ
(dev−name)
MAC登録確認レスポンス
Cp−name
DSD
(cp−name)
USD
UserSignal E
SSDP:M−Search
DSZ
DeviceSignal E
(device discovered)

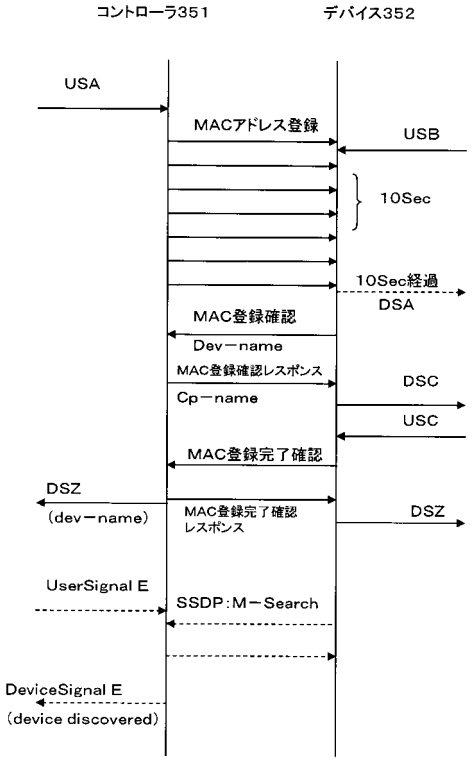
【図６】


コントローラ351
デバイス352
USA
MACアドレス登録
USB
10Sec
DSA
USC
MAC登録確認
(パスワード要求)
DSB
MAC登録確認レスポンス
DSC
パスワード入力
パスワード
DSZ
パスワードレスポンス
DSZ
SSDP:M−Search
DeviceSignal E
(device discovered)

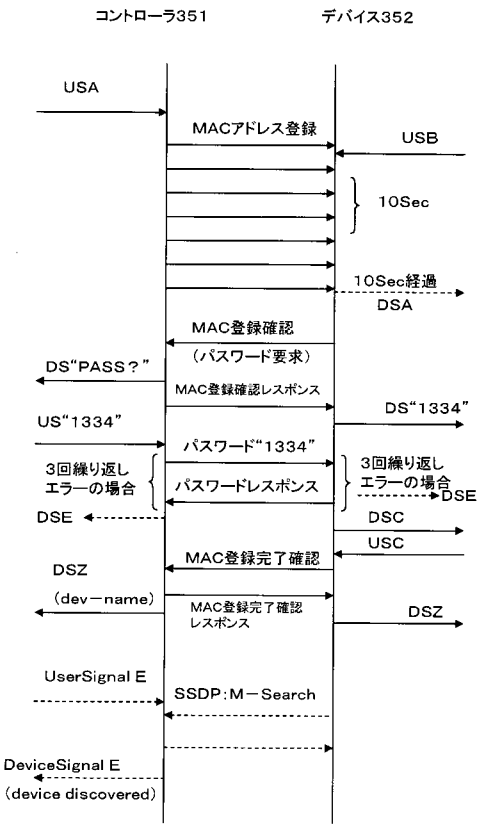
【図７】


10Sec
USB
他のコントローラ検出
DSX
デバイス352
他のコントローラからのMACアドレス登録
MACアドレス登録
コントローラ351
USA
DSX（タイムアウト）
5min

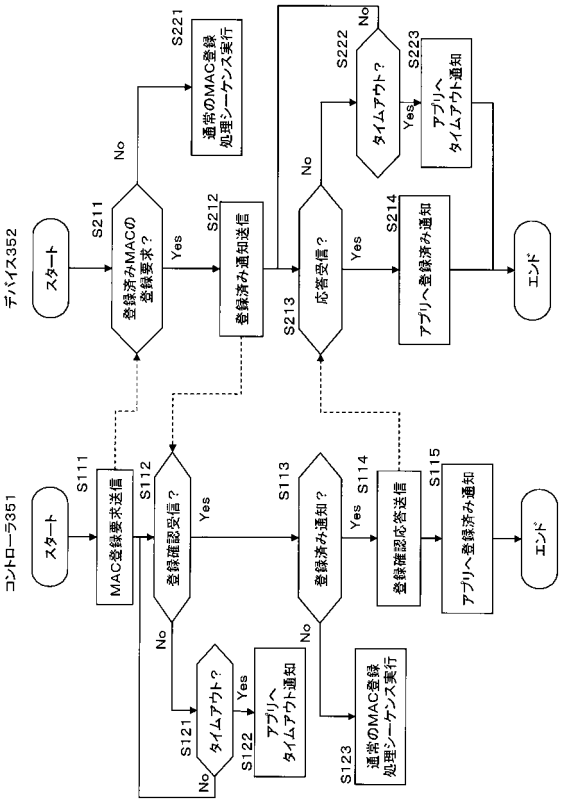
【図８】


コントローラ351
デバイス352
USA
MACアドレス登録
USB
10Sec
10Sec経過
DSA
MAC登録確認
Dev－name
MAC登録確認レスポンス
Cp－name
DSC
USC
MAC登録完了確認
DSZ
（dev－name）
MAC登録完了確認レスポンス
DSZ
UserSignal E
SSDP：M－Search
DeviceSignal E
（device discovered）

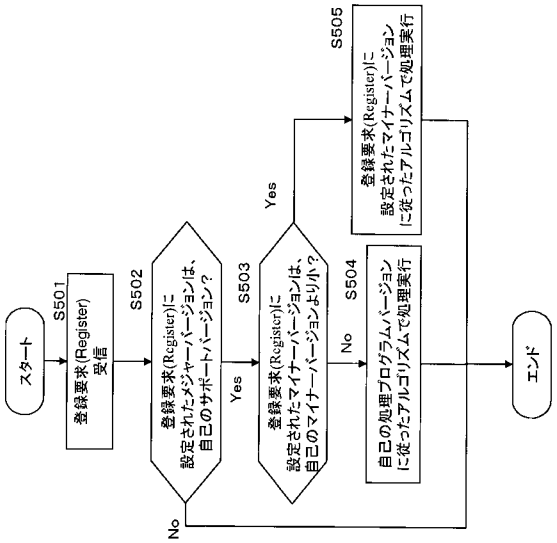
【図９】


コントローラ351
デバイス352
USA
MACアドレス登録
USB
10Sec
10Sec経過
DSA
MAC登録確認
（パスワード要求）
DS“PASS？”
MAC登録確認レスポンス
DS“1334”
US“1334”
パスワード“1334”
3回繰り返し
エラーの場合
パスワードレスポンス
3回繰り返し
エラーの場合
DSE
DSE
DSC
USC
MAC登録完了確認
DSZ
（dev－name）
MAC登録完了確認
レスポンス
DSZ
UserSignal E
SSDP：M－Search
DeviceSignal E
（device discovered）

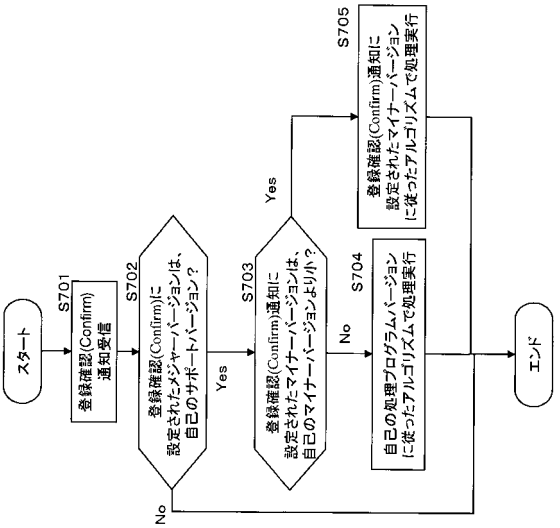
【図１０】


デバイス352
スタート
S211
登録済みMACの登録要求？
No
Yes
S221
通常のMAC登録処理シーケンス実行
S212
登録済み通知送信
S213
応答受信？
No
Yes
S222
タイムアウト？
No
Yes
S223
アプリへタイムアウト通知
S214
アプリへ登録済み通知
エンド
コントローラ351
スタート
S111
MAC登録要求送信
S112
登録確認受信？
No
Yes
S121
タイムアウト？
No
Yes
S122
アプリへタイムアウト通知
S113
登録済み通知？
No
Yes
S123
通常のMAC登録処理シーケンス実行
S114
登録確認応答送信
S115
アプリへ登録済み通知
エンド

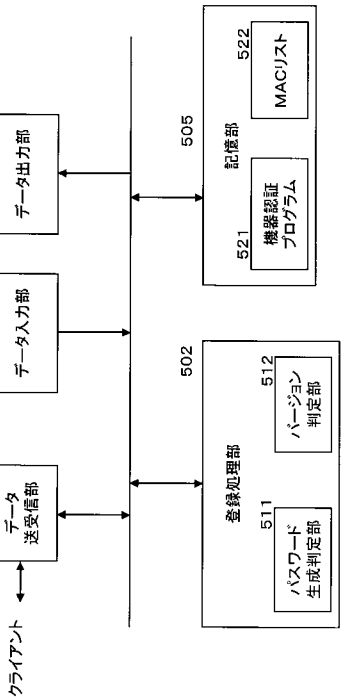
【図１１】



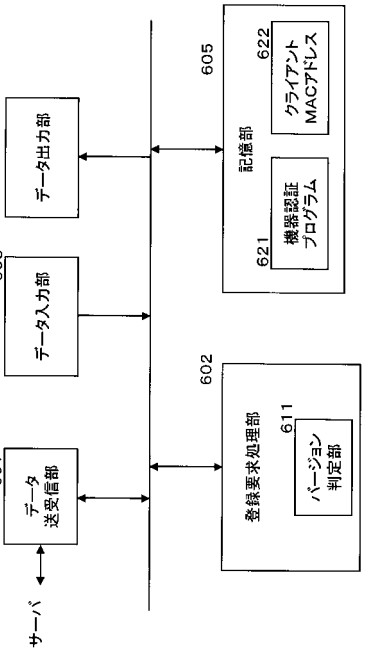
【図１２】



【図１３】



【図１４】



フロントページの続き

(72)発明者　森田　岳彦
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　高久　義之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　酒向　範幸
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　濱田　全章
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　五十嵐　卓也
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　宮司　卓佳

(56)参考文献　特開２００２－２０４２４７（ＪＰ，Ａ）
特開２００２－２２３２２７（ＪＰ，Ａ）
特開平９－１９１３１６（ＪＰ，Ａ）
特開２０００－５９３９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20,H04L12/20