(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-104264
(P2009-104264A)
(43)公開日　平成21年5月14日(2009.5.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330C	5B285
H04L 9/32	(2006.01)	H04L	9/00	675D	5J104

審査請求 未請求　請求項の数 7　ＯＬ　（全 21 頁）

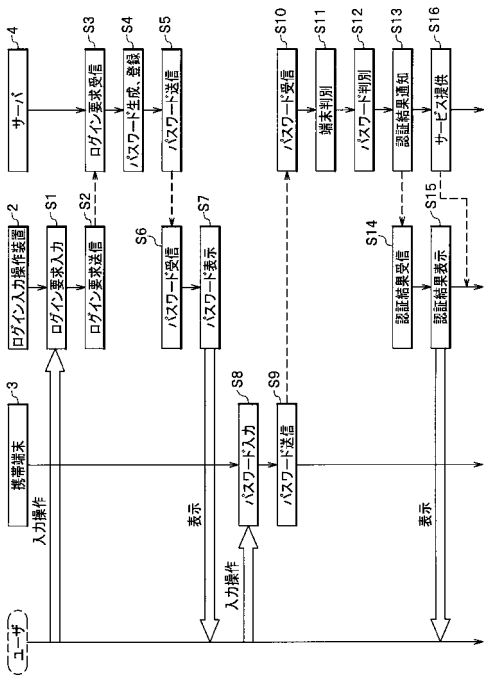
(21)出願番号　特願2007-273282 (P2007-273282)
(22)出願日　平成19年10月22日 (2007.10.22)

(71)出願人　000000295
沖電気工業株式会社
東京都港区西新橋三丁目１６番１１号
(74)代理人　100064414
弁理士　磯野　道造
(74)代理人　100132001
弁理士　伊藤　政幸
(72)発明者　森下　朋樹
東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
(72)発明者　長谷部　忍
東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内

最終頁に続く

(54)【発明の名称】ログイン認証方法、ログイン認証サーバおよびログイン認証プログラム

(57)【要約】
【課題】入力操作の手間を低減して迅速にログインできるログイン認証方式を提供する。
【解決手段】ログイン認証方式は、サーバ４において、ログイン入力操作装置２からログイン要求と共に受信したログイン入力操作装置２固有の装置情報に基づいて装置情報に対応付けてパスワードを生成し（Ｓ４）、パスワードをログイン入力操作装置２に送信し（Ｓ５）、携帯端末３からパスワードを当該携帯端末３の端末情報と共に受信し（Ｓ１０）、受信した端末情報が予め登録された端末情報と一致するか否かを判別し（Ｓ１１）、受信したパスワードが生成されたパスワードと一致するか否かを判別し（Ｓ１２）、受信したパスワードが生成されたパスワードと一致する場合に、生成されたパスワードに対応付けられた装置情報で特定されるログイン入力操作装置２に対して認証成功を示す認証結果を通知する（Ｓ１３）。
【選択図】図３



【特許請求の範囲】
【請求項１】
携帯端末固有の端末情報を記憶する端末情報記憶手段を有したログイン認証サーバと、前記ログイン認証サーバにログイン要求を送信するログイン入力操作装置と、前記端末情報記憶手段に固有の端末情報が登録済みであって前記ログイン要求に引き続いて前記ログイン認証サーバにパスワードを送信する携帯端末とを備えた認証システムにおけるログイン認証方法であって、
前記ログイン認証サーバは、
前記ログイン入力操作装置から前記ログイン要求と共に受信した前記ログイン入力操作装置固有の装置情報に基づいて前記装置情報に対応付けてパスワードを生成するパスワード生成ステップと、
前記パスワードを前記ログイン入力操作装置に送信するパスワード送信ステップと、
前記携帯端末からパスワードを当該携帯端末の端末情報と共に受信するパスワード受信ステップと、
前記受信した端末情報がログイン認証サーバ端末情報と一致するか否かを判別する端末判別ステップと、
前記受信したパスワードが前記生成されたパスワードと一致するか否かを判別するパスワード判別ステップと、
前記受信したパスワードが前記生成されたパスワードと一致する場合に、前記生成されたパスワードに対応付けられた装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する認証結果通知ステップとを実行することを特徴とするログイン認証方法。
【請求項２】
前記ログイン入力操作装置は、
前記ログイン認証サーバから受信したパスワードを表示するパスワード表示ステップを実行し、
前記携帯端末は、
パスワードを入力するパスワード入力ステップと、
前記入力されたパスワードを当該携帯端末の端末情報と共に前記ログイン認証サーバに送信するパスワード送信ステップとを実行することを特徴とする請求項１に記載のログイン認証方法。
【請求項３】
前記ログイン入力操作装置は、
前記ログイン認証サーバから受信したパスワードを前記携帯端末に送信するパスワード送信ステップを実行し、
前記携帯端末は、
前記ログイン入力操作装置からパスワードを受信するパスワード受信ステップと、
前記受信したパスワードを当該携帯端末の端末情報と共に前記ログイン認証サーバに送信するパスワード送信ステップとを実行することを特徴とする請求項１に記載のログイン認証方法。
【請求項４】
前記ログイン認証サーバは、
前記ログイン入力操作装置から、パスワードの予め定められた通知方式またはユーザ権限の少なくとも１つに関する設定情報を、前記ログイン要求および前記ログイン入力操作装置固有の装置情報と共に受信するログイン要求受信ステップと、
前記受信した設定情報が、予め登録された設定情報のうちのいずれであるかを判別する設定情報判別ステップとをさらに実行し、
前記パスワード生成ステップは、
前記受信した設定情報で指定されるパスワードを生成し、
前記パスワード送信ステップは、前記生成したパスワードを前記受信した設定情報と共

に前記ログイン入力操作装置に送信し、
前記ログイン入力操作装置は、
前記ログイン認証サーバから受信した設定情報に応じて、前記ログイン認証サーバから受信したパスワードを表示するパスワード表示ステップ、または、前記受信したパスワードを前記携帯端末に送信するパスワード送信ステップのいずれかを実行し、
前記携帯端末は、
前記パスワード表示ステップに対応してパスワードを入力するパスワード入力ステップと、前記パスワード送信ステップに対応して前記ログイン入力操作装置からパスワードを受信するパスワード受信ステップとのいずれかを実行し、
前記入力されたパスワードまたは前記受信したパスワードを当該携帯端末の端末情報と共に前記ログイン認証サーバに送信するパスワード送信ステップをさらに実行することを特徴とする請求項１に記載のログイン認証方法。
【請求項５】
携帯端末固有の端末情報を記憶する端末情報記憶手段を有したログイン認証サーバと、前記ログイン認証サーバにログイン要求を送信するログイン入力操作装置と、前記端末情報記憶手段に固有の端末情報が登録済みであって前記ログイン要求に引き続いて前記ログイン認証サーバにパスワードを送信する携帯端末とを有した認証システムにおける前記ログイン認証サーバであって、
前記ログイン入力操作装置から前記ログイン要求と共に受信した前記ログイン入力操作装置固有の装置情報に基づいてパスワードを生成するパスワード生成手段と、
前記パスワードを前記装置情報と共に記憶するパスワード記憶手段と、
前記パスワードを前記ログイン入力操作装置に送信するパスワード送信手段と、
前記携帯端末からパスワードを当該携帯端末の端末情報と共に受信するパスワード受信手段と、
前記受信した端末情報が前記端末情報記憶手段に登録された端末情報と一致するか否かを判別する端末判別手段と、
前記受信したパスワードが前記パスワード記憶手段に登録されたパスワードと一致するか否かを判別するパスワード判別手段と、
前記受信したパスワードが前記パスワード記憶手段に登録済みである場合に、前記登録済みのパスワードと共に記憶された装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する認証結果通知手段とを備えることを特徴とするログイン認証サーバ。
【請求項６】
前記ログイン入力操作装置から、パスワードの予め定められた通知方式またはユーザ権限の少なくとも１つに関する設定情報を、前記ログイン要求および前記ログイン入力操作装置固有の装置情報と共に受信するログイン要求受信手段と、
前記受信した設定情報が、予め登録された設定情報のうちのいずれであるかを判別する設定情報判別手段とをさらに備え、
前記パスワード生成手段は、
前記受信した設定情報で指定されるパスワードを生成し、
前記パスワード送信手段は、前記生成したパスワードを前記パスワードの種類を示す情報と共に前記ログイン入力操作装置に送信することを特徴とする請求項５に記載のログイン認証サーバ。
【請求項７】
携帯端末固有の端末情報を記憶する端末情報記憶手段を有したログイン認証サーバと、前記ログイン認証サーバにログイン要求を送信するログイン入力操作装置と、前記端末情報記憶手段に固有の端末情報が登録済みであって前記ログイン要求に引き続いて前記ログイン認証サーバにパスワードを送信する携帯端末とを備えた認証システムにおける前記ログイン認証サーバを実現するために、コンピュータを、
前記ログイン入力操作装置から前記ログイン要求と共に受信した前記ログイン入力操作

装置固有の装置情報に基づいてパスワードを生成するパスワード生成手段、
前記パスワードを前記ログイン入力操作装置に送信するパスワード送信手段、
前記携帯端末からパスワードを当該携帯端末の端末情報と共に受信するパスワード受信手段、
前記受信した端末情報が端末情報記憶手段に予め登録された端末情報と一致するか否かを判別する端末判別手段、
前記受信したパスワードが前記生成されたパスワードと一致するか否かを判別するパスワード判別手段、
前記受信したパスワードが前記生成されたパスワードと一致する場合に、前記生成されたパスワードに対応付けられた装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する認証結果通知手段、
として機能させることを特徴とするログイン認証プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ログイン認証方法、ログイン認証サーバおよびログイン認証プログラムに係り、特に、携帯端末をパスワードの入力装置として利用するログイン認証方法、ログイン認証サーバおよびログイン認証プログラムに関するものである。

【背景技術】

【０００２】

従来、携帯端末をパスワードの入力装置として使用するログイン認証方法が知られている（例えば、特許文献１参照）。特許文献１に記載の技術では、認証サーバは、ワンタイムパスワード（以下、単にパスワードという）を生成し、生成したパスワードを、この認証サーバに予めアドレス等を登録済である各携帯端末へ送信する。そして、ユーザは、各携帯端末から情報利用装置へ送信されたパスワードを、情報利用装置において表示されるログイン画面から入力することで、パスワードを認証サーバに送信する。認証サーバは、受信したパスワードと、生成したパスワードとを比較してそれらが一致した場合に認証成功とする。なお、認証に一度使用されたパスワードは認証サーバから消去される。

【特許文献１】特開２００４－３４８２３６号公報（段落００２３～段落００３９、図１）

【発明の開示】

【発明が解決しようとする課題】

【０００３】

しかしながら、従来の技術には、以下の不都合がある。すなわち、認証サーバは、生成したパスワードの送信先として、携帯端末ごとに異なる複数の宛先に関する情報を保有し、生成したパスワードを各携帯端末に送信する。これを実現させるために、各携帯端末のユーザは、認証サーバにログイン要求をする際に、各自に対するパスワードの受け取り先を指定する情報として、例えば、自らの携帯端末を識別する携帯端末識別情報やメールアドレス等を、認証サーバへ予め送信しておく必要がある。このようにパスワードの受け取り先を指定する情報（メールアドレス等）を携帯端末に入力する操作には手間がかかる。最初の入力操作を前提とするならば、携帯端末にパスワードの受け取り先を指定する情報を一度入力した後に、それを携帯端末のメモリに記憶させておくことも考えられる。この場合には、同じ携帯端末からの再度のログインにおいて、記憶させた情報を用いることも可能であるが、ユーザが携帯端末を変更してしまった場合には、パスワードの送信先を指定する情報を新たに入力しなければならない。

【０００４】

そこで、本発明では、前記した問題を解決し、入力操作の手間を低減して迅速にログインすることができるログイン認証方法、ログイン認証サーバおよびログイン認証プログラムを提供することを目的とする。

【課題を解決するための手段】

【０００５】
本発明は、前記目的を達成するために創案されたものであり、本発明のうち請求項１に記載のログイン認証方法は、携帯端末固有の端末情報を記憶する端末情報記憶手段を有したログイン認証サーバと、前記ログイン認証サーバにログイン要求を送信するログイン入力操作装置と、前記端末情報記憶手段に固有の端末情報が登録済みであって前記ログイン要求に引き続いて前記ログイン認証サーバにパスワードを送信する携帯端末とを備えた認証システムにおけるログイン認証方法であって、前記ログイン認証サーバが、前記ログイン入力操作装置から前記ログイン要求と共に受信した前記ログイン入力操作装置固有の装置情報に基づいて前記装置情報に対応付けてパスワードを生成するパスワード生成ステップと、前記パスワードを前記ログイン入力操作装置に送信するパスワード送信ステップと、前記携帯端末からパスワードを当該携帯端末の端末情報と共に受信するパスワード受信ステップと、前記受信した端末情報が端末情報記憶手段に予め登録された端末情報と一致するか否かを判別する端末判別ステップと、前記受信したパスワードが前記生成されたパスワードと一致するか否かを判別するパスワード判別ステップと、前記受信したパスワードが前記生成されたパスワードと一致する場合に、前記生成されたパスワードに対応付けられた装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する認証結果通知ステップとを実行することを特徴とする。
【０００６】
かかる手順によれば、ログイン認証サーバは、ログイン要求を送信したログイン入力操作装置固有の装置情報に基づいて装置情報に対応付けてパスワードを生成し、ログイン入力操作装置に送信する。ここで、パスワードは例えばワンタイムパスワードである。そして、ログイン認証サーバは、受信したパスワードが事前に生成したパスワードと一致する場合に、事前に生成したパスワードに対応付けられた装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する。したがって、ユーザは、パスワードの受け取り先を指定する情報をログイン認証サーバへ送信する必要がないので、入力操作の手間を低減して迅速にログインすることができる。
【０００７】
また、請求項２に記載のログイン認証方法は、請求項１に記載のログイン認証方法において、前記ログイン入力操作装置が、前記ログイン認証サーバから受信したパスワードを表示するパスワード表示ステップを実行し、前記携帯端末が、パスワードを入力するパスワード入力ステップと、前記入力されたパスワードを当該携帯端末の端末情報と共に前記ログイン認証サーバに送信するパスワード送信ステップとを実行することを特徴とする。
【０００８】
かかる手順によれば、ログイン入力操作装置は、受信したパスワードを表示する。そして、携帯端末は、ログイン入力操作装置に表示されたパスワードをなんらかの方法で取得し、パスワードを入力する。続いて、携帯端末は、入力されたパスワードを当該携帯端末の端末情報と共にログイン認証サーバに送信する。ここで、パスワードの取得方法は、任意である。例えば、ログイン入力操作装置に表示されたパスワードが文字や記号からなる場合には、それを見たユーザがそのパスワードをボタン操作で携帯端末に直接入力することで取得する方法が挙げられる。また、例えば、表示されたパスワードが画像やバーコードからなる場合には、ユーザがそれをカメラ付の携帯端末で取り込む操作を行うことで取得する方法が挙げられる。
【０００９】
また、請求項３に記載のログイン認証方法は、請求項１に記載のログイン認証方法において、前記ログイン入力操作装置が、前記ログイン認証サーバから受信したパスワードを前記携帯端末に送信するパスワード送信ステップを実行し、前記携帯端末が、前記ログイン入力操作装置からパスワードを受信するパスワード受信ステップと、前記受信したパスワードを当該携帯端末の端末情報と共に前記ログイン認証サーバに送信するパスワード送信ステップとを実行することを特徴とする。
【００１０】

かかる手順によれば、ログイン入力操作装置は、受信したパスワードを携帯端末に送信する。続いて、携帯端末は、受信したパスワードを当該携帯端末の端末情報と共にログイン認証サーバに送信する。ここで、パスワードを送信する方法は、任意である。例えば、ログイン入力操作装置に携帯端末を有線接続して送信することができる。また、例えば、赤外線通信やＩＣチップ間通信等の無線通信を利用することもできる。

【００１１】

また、請求項４に記載のログイン認証方法は、請求項１に記載のログイン認証方法において、前記ログイン認証サーバが、前記ログイン入力操作装置から、パスワードの予め定められた通知方式またはユーザ権限の少なくとも１つに関する設定情報を、前記ログイン要求および前記ログイン入力操作装置固有の装置情報と共に受信するログイン要求受信ステップと、前記受信した設定情報が、予め登録された設定情報のうちのいずれであるかを判別する設定情報判別ステップとをさらに実行し、前記パスワード生成ステップが、前記受信した設定情報で指定されるパスワードを生成し、前記パスワード送信ステップが、前記生成したパスワードを前記受信した設定情報と共に前記ログイン入力操作装置に送信し、前記ログイン入力操作装置が、前記ログイン認証サーバから受信した設定情報に応じて、前記ログイン認証サーバから受信したパスワードを表示するパスワード表示ステップ、または、前記受信したパスワードを前記携帯端末に送信するパスワード送信ステップのいずれかを実行し、前記携帯端末が、前記パスワード表示ステップに対応してパスワードを入力するパスワード入力ステップと、前記パスワード送信ステップに対応して前記ログイン入力操作装置からパスワードを受信するパスワード受信ステップとのいずれかを実行し、前記入力されたパスワードまたは前記受信したパスワードを当該携帯端末の端末情報と共に前記ログイン認証サーバに送信するパスワード送信ステップをさらに実行することを特徴とする。

【００１２】

かかる手順によれば、ログイン認証サーバは、ログイン入力操作装置から、ログイン要求だけではなく、パスワードの通知方式やユーザ権限に関する設定情報を受信し、受信した設定情報が、予め登録された設定情報のうちのいずれであるかを判別し、生成したパスワードと共に設定情報を送り返す。ここで、通知方式に関する設定情報は、例えば、セキュリティレベルの高低やパスワードを表示させる装置に対応して定めることができる。続いて、ログイン入力操作装置は、受信した設定情報に応じて、受信したパスワードを表示するか、または、携帯端末に送信する。受信したパスワードを表示する場合、携帯端末は、なんらかの方法でパスワードを入力する。また、ログイン入力操作装置が、受信したパスワードを携帯端末に送信する場合、携帯端末は、そのパスワードを受信する。続いて、携帯端末は、入力されたパスワードまたは受信したパスワードを当該携帯端末の端末情報と共にログイン認証サーバに送信する。したがって、ユーザは、ログイン入力操作装置によって、ログイン要求だけではなく、パスワードの通知方式やユーザ権限に関する設定情報を設定することができる。

【００１３】

また、前記課題を解決するために、請求項５に記載のログイン認証サーバは、携帯端末固有の端末情報を記憶する端末情報記憶手段を有したログイン認証サーバと、前記ログイン認証サーバにログイン要求を送信するログイン入力操作装置と、前記端末情報記憶手段に固有の端末情報が登録済みであって前記ログイン要求に引き続いて前記認証サーバにパスワードを送信する携帯端末とを備えた認証システムにおける前記ログイン認証サーバであって、前記携帯端末を識別する端末情報を記憶する端末情報記憶手段と、前記ログイン入力操作装置から前記ログイン要求と共に受信した前記ログイン入力操作装置固有の装置情報に基づいてパスワードを生成するパスワード生成手段と、前記パスワードを前記装置情報と共に記憶するパスワード記憶手段と、前記パスワードを前記ログイン入力操作装置に送信するパスワード送信手段と、前記携帯端末からパスワードを当該携帯端末の端末情報と共に受信するパスワード受信手段と、前記受信した端末情報が前記端末情報記憶手段に登録された端末情報と一致するか否かを判別する端末判別手段と、前記受信したパスワ

ードが前記パスワード記憶手段に登録されたパスワードと一致するか否かを判別するパスワード判別手段と、前記受信したパスワードが前記パスワード記憶手段に登録済みである場合に、前記登録済みのパスワードと共に記憶された装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する認証結果通知手段とを備えることを特徴とする。

【００１４】

かかる構成によれば、ログイン認証サーバは、携帯端末を識別する端末情報を予め登録しておき、ログイン要求を送信したログイン入力操作装置固有の装置情報に基づいてパスワードを生成し、生成したパスワードを装置情報と共に登録すると共にログイン入力操作装置に送信する。そして、ログイン認証サーバは、受信したパスワードが登録済みのパスワードと一致する場合に、登録済みのパスワードに対応付けられた装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する。したがって、ユーザは、パスワードの受け取り先を指定する情報をログイン認証サーバへ送信する必要がないので、入力操作の手間を低減して迅速にログインすることができる。

【００１５】

また、請求項６に記載のログイン認証サーバは、請求項５に記載のログイン認証サーバにおいて、前記ログイン入力操作装置から、パスワードの予め定められた通知方式またはユーザ権限の少なくとも１つに関する設定情報を、前記ログイン要求および前記ログイン入力操作装置固有の装置情報と共に受信するログイン要求受信手段と、前記受信した設定情報が、予め登録された設定情報のうちのいずれであるかを判別する設定情報判別手段とをさらに備え、前記パスワード生成手段が、前記受信した設定情報で指定されるパスワードを生成し、前記パスワード送信手段が、前記生成したパスワードを前記パスワードの種類を示す情報と共に前記ログイン入力操作装置に送信することを特徴とする。

【００１６】

かかる構成によれば、ログイン認証サーバは、ログイン入力操作装置から、ログイン要求だけではなく、パスワードの通知方式やユーザ権限に関する設定情報を受信し、受信した設定情報が、予め登録された設定情報のうちのいずれであるかを判別し、生成したパスワードと共に設定情報を送り返す。これにより、ログイン入力操作装置は、受信した設定情報に応じて、受信したパスワードを表示したり、携帯端末に送信したりすることが可能となる。したがって、例えば、セキュリティレベルの高低やパスワードを表示させる装置に対応して設定情報を定めることで、ログイン入力操作装置や携帯端末を操作するユーザの利便性を向上させることができる。

【００１７】

また、請求項７に記載のログイン認証プログラムは、携帯端末固有の端末情報を記憶する端末情報記憶手段を有したログイン認証サーバと、前記ログイン認証サーバにログイン要求を送信するログイン入力操作装置と、前記端末情報記憶手段に固有の端末情報が登録済みであって前記ログイン要求に引き続いて前記ログイン認証サーバにパスワードを送信する携帯端末とを備えた認証システムにおける前記ログイン認証サーバを実現するために、コンピュータを、前記ログイン入力操作装置から前記ログイン要求と共に受信した前記ログイン入力操作装置固有の装置情報に基づいてパスワードを生成するパスワード生成手段、前記パスワードを前記ログイン入力操作装置に送信するパスワード送信手段、前記携帯端末からパスワードを当該携帯端末の端末情報と共に受信するパスワード受信手段、前記受信した端末情報が端末情報記憶手段に予め登録された端末情報と一致するか否かを判別する端末判別手段、前記受信したパスワードが前記生成されたパスワードと一致するか否かを判別するパスワード判別手段、前記受信したパスワードが前記生成されたパスワードと一致する場合に、前記生成されたパスワードに対応付けられた装置情報で特定されるログイン入力操作装置に対して認証成功を示す認証結果を通知する認証結果通知手段として機能させることを特徴とする。

このように構成されることにより、このプログラムをインストールされたコンピュータは、このプログラムに基づいた各機能を実現することができる。

【発明の効果】
【００１８】
本発明によれば、ユーザは、パスワードの受け取り先を指定する情報をログイン認証サーバへ送信する必要がないので、入力操作の手間を低減して迅速にログインすることができる。また、ログイン入力操作装置をログイン認証サーバに事前登録する必要もない。したがって、ユーザは、事前登録されていないログイン入力操作装置からでもログインを要求しユーザ認証を受けることができる。また、ログイン入力操作装置は、ユーザ個人を特定する固有情報をログイン認証サーバに送信することはないので、ログイン時における個人情報の漏洩を防止することができる。したがって、ユーザは、ログイン要求操作装置と携帯端末とを利用すれば、いつでもどこからでもセキュアなログイン認証を受けることが可能となる。
【発明を実施するための最良の形態】
【００１９】
以下、図面を参照して本発明のログイン認証方法およびログイン認証サーバを実施するための最良の形態（以下「実施形態」という）について詳細に説明する。
【００２０】
［認証システムの構成］
図１は、本発明の第１実施形態に係るサーバを含む認証システムの構成を模式的に示す図である。認証システム１は、ログイン入力操作装置２と、携帯端末３と、携帯端末３固有の端末情報を記憶する端末情報記憶手段３１を有したサーバ（ログイン認証サーバ）４とを備えている。なお、図１では、ログイン入力操作装置２と、携帯端末３と、サーバ４とを１台ずつ示したが、これらの台数は任意である。
【００２１】
［ログイン入力操作装置］
ログイン入力操作装置２は、サーバ４にログイン要求を送信するものであり、例えば、ＣＰＵ（Central Processing Unit）、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）、通信を行うためのＮＩＣ（Network Interface Card）等を備えている。このログイン入力操作装置２は、例えば、パーソナルコンピュータ（以下、単にＰＣと表記する）や入退室管理用のミニパネル等から構成される。以下では、ログイン入力操作装置２が、ＰＣであるものとして説明する。このログイン入力操作装置２は、例えば、インターネットやＬＡＮ（Local Area Network）等のネットワークＮに接続されており、図１に示すように、入力手段１０と、通信手段１１と、記憶手段１２と、表示手段１３と、出力手段１４と、制御手段１５とを備えている。
【００２２】
入力手段１０は、サーバ４に対してログインを要求するための入力操作を行うものであり、例えば、キーボード、マウス、タッチパネル等の一般的な入力装置から構成される。
通信手段１１は、制御手段１５の制御の下、ネットワークＮを介してサーバ４との間で各種情報をやりとりするものであり、例えば、ＮＩＣから構成される。
記憶手段１２は、例えば、所定のプログラム等を記憶するＲＯＭや、制御手段１５による演算処理等に利用されるＲＡＭ、ハードディスク等により構成されている。本実施形態では、記憶手段３０のメモリに、ログイン入力操作装置２の装置情報が予め格納されている。装置情報は、例えば、製品番号やＭＡＣアドレスといった、ログイン入力操作装置２の固有の情報である。
【００２３】
表示手段１３は、制御手段１５の制御の下、入力手段１０により入力された情報や、通信手段１１を介してサーバ４から取得した情報（画面表示情報、パスワード、認証結果）を画面表示するものである。この表示手段１３は、例えば、液晶ディスプレイ（ＬＣＤ：Liquid Crystal Display）、ＣＲＴ（Cathode Ray Tube）、ＰＤＰ（Plasma Display Panel）等から構成される。
【００２４】

ここで、ログイン画面の一例を説明する。図２は、図１に示したログイン入力操作装置の表示手段に表示されるログイン画面の一例を示す図である。ログイン画面２００は、図２に示すように、サーバ名入力欄２１０と、送信ボタン２２０と、リターンボタン２３０とを備えている。ユーザは、ログイン画面２００が表示されているときに、ログイン認証を行うサーバ４をサーバ名入力欄２１０に入力し、送信ボタン２２０を押下する。ユーザが送信ボタン２２０を押下すると、ログイン入力操作装置２は、ログイン要求送信手段１６（図１参照）によって、ログイン要求をサーバ４へ送信する。

【００２５】

図１に戻って、ログイン入力操作装置２の構成の説明を続ける。

出力手段１４は、制御手段１５の制御の下、受信したパスワードを携帯端末３へ出力するものである。本実施形態では、出力手段１４と携帯端末３との通信は無線通信であるものとする。ここで、無線通信として採用可能な通信方式は、例えば、赤外線通信、ＦｅｌｉＣａ（登録商標）等のＩＣチップ間通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）等が挙げられる。出力手段１４には、採用された通信方式に対応した構成を適宜採用することができる。なお、携帯端末３との通信を有線通信とする場合には、出力手段１４は、携帯端末３と接続されるケーブル等が装着可能なコネクタを備えることができる。

【００２６】

制御手段１５は、例えばＣＰＵから構成され、ログイン要求送信手段１６と、パスワード受信手段１７と、認証結果受信手段１８と、パスワード送信手段１９とを備えている。

ログイン要求送信手段１６は、通信手段１１を介してログイン要求を装置情報と共にサーバ４へ送信するものである。

【００２７】

パスワード受信手段１７は、通信手段１１を介してサーバ４からワンタイムパスワード（以下、単にパスワードという）を受信するものである。以下では、一例として、パスワード受信手段１７は、受信したパスワードをそのまま表示手段１３へ表示させるものとして説明し、受信したパスワードを出力手段１４を介して携帯端末３へ送信する例については、変形例として後記することとする。この変形例において、パスワード送信手段１９は、サーバ４から受信したパスワードを携帯端末３に送信する。

【００２８】

認証結果受信手段１８は、通信手段１１を介してサーバ４から認証結果を受信するものである。この認証結果受信手段１８は、受信した認証結果を表示手段１３へ表示させる。なお、ログイン要求送信手段１６、パスワード受信手段１７、認証結果受信手段１８およびパスワード送信手段１９は、ＣＰＵがハードディスク等に格納された所定のプログラムをＲＡＭに展開して実行することによりその機能が実現されるものである。

【００２９】

［携帯端末］

携帯端末３は、サーバ４の端末情報記憶手段３１に固有の端末情報が登録済みであってログイン入力操作装置２からのログイン要求に引き続いてサーバ４にパスワードを送信するものであり、例えば、携帯電話、ＰＨＳ、情報携帯端末（ＰＤＡ：Personal Digital Assistants）等から構成される。本実施形態では、携帯端末３は、ユーザの入力操作に基づいて、パスワードを入力し、ユーザの送信操作に基づいて、入力されたパスワードを当該携帯端末３の端末情報と共にサーバ４へネットワークＮを介して送信する。なお、変形例では、携帯端末３は、ログイン入力操作装置２からパスワードを受信し、受信したパスワードを当該携帯端末３の端末情報と共にサーバ４へネットワークＮを介して送信する。

【００３０】

携帯端末３のユーザは、ログイン認証の利用に先立ち、携帯端末３をサーバ４に登録する（携帯端末登録）。この携帯端末登録時において登録する情報は、携帯端末３に固有の製品番号や契約者番号といった情報（以下、これらの情報を端末情報という）である。したがって、従来必要であった、メールアドレス等の送信先情報を登録することはしない。この点が従来のログイン方式とは大きく異なる点である。本実施形態では、サーバ４で生

成されたパスワードは、携帯端末３に送信されることはない。

【００３１】

［サーバ］

サーバ（ログイン認証サーバ）４は、ログイン認証を行うものであり、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ、ＨＤＤ（Hard Disk Drive）、ＮＩＣ等から構成され、通信手段２０と、記憶手段３０と、制御手段４０とを備えている。本実施形態では、サーバ４は、ログイン認証後に、ログイン入力操作装置２にサービス情報（例えば、ニュース等のテキストや、画像、映像、音楽等のコンテンツ等）を提供（配信）するものとする。また、サーバ４は、検索サービスや、サーバ４に蓄積したデータへの書き込みや管理等のサービスを提供することもできる。なお、サーバ４によるサービスは、ログイン入力操作装置２に各種情報を提供することに限定されるものではない。例えば、ログイン入力操作装置２が入退室管理用ミニパネルである場合には、該当する部屋の施錠または解除（入退室の許可）がサービスであり、施錠または解除を行う装置への動作指令の出力がサービスの提供となる。

【００３２】

通信手段２０は、ＮＩＣ等から構成され、ネットワークＮを介してログイン入力操作装置２との間で各種情報（ログイン要求、パスワード等）を送受信したり、ネットワークＮを介して携帯端末３からパスワードを受信したりするものである。

【００３３】

記憶手段３０は、例えば、所定のプログラム等を記憶するＲＯＭや、制御手段４０による演算処理等に利用されたり通信手段２０を介して取得した情報等を記憶したりするＲＡＭ等を備える。また、記憶手段３０は、端末情報記憶手段３１と、パスワード記憶手段３２と、サービス情報記憶手段３３とを備えている。

【００３４】

端末情報記憶手段３１は、携帯端末３を識別する端末情報を記憶するものであり、一般的なメモリやハードディスク等から構成される。

パスワード記憶手段３２は、サーバ４で生成するパスワードを、ログイン入力操作装置２の装置情報（製品番号やＭＡＣアドレス等）と共に記憶して各種ログイン情報を管理するためのものであり、一般的なハードディスク等から構成される。

サービス情報記憶手段３３は、サービス情報（例えば、ニュース等のテキストや、画像、映像、音楽等のコンテンツ等）を記憶するものであり、一般的なハードディスク等から構成される。

【００３５】

制御手段４０は、例えば、ＣＰＵ等から構成され、ログイン要求受信手段４１と、パスワード生成手段４２と、パスワード送信手段４３と、パスワード受信手段４４と、端末判別手段４５と、パスワード判別手段４６と、認証結果通知手段４７と、サービス提供手段４８とを備えている。

【００３６】

ログイン要求受信手段４１は、通信手段２０を介してログイン入力操作装置２から、ログイン要求をログイン入力操作装置２固有の装置情報と共に受信するものである。

パスワード生成手段４２は、ログイン要求受信手段４１で受信した装置情報に基づいてパスワードを生成するものである。このパスワード生成手段４２は、生成したパスワードを当該装置情報と共にパスワード記憶手段３２に登録する。ここで、パスワードの生成方法は特に限定されるものではなく、公知技術を用いることができる。例えば、数字や記号からなるパスワードを生成する場合には、装置情報としての製品番号と、乱数とに基づいて計算から求めることができる。

【００３７】

パスワード送信手段４３は、パスワード生成手段４２で生成したパスワードを通信手段２０を介して、ログイン要求を送信したログイン入力操作装置２へ送り返すものである。

パスワード受信手段４４は、通信手段２０を介して携帯端末３からパスワードを当該携

帯端末３の端末情報（例えば製品番号や契約者番号）と共に受信するものである。

【００３８】

端末判別手段４５は、受信した端末情報が端末情報記憶手段３１に登録された端末情報と一致するか否かを判別するものである。本実施形態では、この判別結果は、パスワード判別手段４６に出力される。

パスワード判別手段４６は、受信したパスワードと一致するパスワードがパスワード記憶手段３２に登録されているか否かを判別するものである。この判別結果は認証結果通知手段４７に出力される。本実施形態では、パスワード判別手段４６は、端末判別手段４５から取得した判別結果に基づいて、受信した端末情報が既に登録されていると判別された場合に、受信したパスワードと一致するパスワードがパスワード記憶手段３２に登録されているか否かを判別し、受信した端末情報が未登録であると判別された場合には、パスワードのチェックを行わずに、認証が失敗したことを示す情報を認証結果通知手段４７に出力することとする。

【００３９】

認証結果通知手段４７は、受信したパスワードがパスワード記憶手段３２に登録済みである場合に、通信手段２０を介して登録済みのパスワードと共に記憶された装置情報で特定されるログイン入力操作装置２に対して認証成功を示す認証結果を通知するものである。具体的には、認証結果通知手段４７は、パスワード判別手段４６でパスワードが既に登録されていると判別された場合に、認証成功を示す予め定められた画面表示データを認証結果として通知する。ここで、認証成功を示す画面表示データは、例えば、サービスの利用許可を示す画面表示データである。また、認証結果通知手段４７は、パスワード判別手段４６でパスワードが未登録であると判別された場合に、認証失敗を示す予め定められた画面表示データを認証結果として通知する。さらに、認証結果通知手段４７は、パスワード判別手段４６から、認証が失敗したことを示す情報を取得した場合に、認証失敗を示す画面表示データを認証結果として通知する。

【００４０】

サービス提供手段４８は、ログイン認証後に、ユーザのサービス要求にしたがって、ユーザの所望するサービス情報をサービス情報記憶手段３３から読み出して通信手段２０を介して提供するものである。なお、前記したログイン要求受信手段４１、パスワード生成手段４２、パスワード送信手段４３、パスワード受信手段４４、端末判別手段４５、パスワード判別手段４６、認証結果通知手段４７およびサービス提供手段４８手段は、ＣＰＵがハードディスク等に格納された所定のプログラムをＲＡＭに展開して実行することによりその機能が実現されるものである。

【００４１】

ここで、パスワードの種類に応じた運用例を説明する。

［パスワードを文字や記号で表示する運用例］

まず、パスワードを文字や記号で表示する場合には、ユーザは、読み取った文字や記号を携帯端末３に入力する操作を行う。この場合には、以下に示すように複数のユーザによる運用に利便性がある。

複数のユーザによる運用の第１の例として、ログイン入力操作装置２を利用する２人のユーザ（ユーザＡ、ユーザＢ）のうち、ユーザＡだけが携帯端末３を所持している場合には、ユーザＢが表示手段１３に表示されたパスワードを読み取ってユーザＡに容易に教えることができる。この２人のペアの間柄は、例えば、親子、介護者と被介護者等さまざまな関係とすることができる。

【００４２】

また、複数のユーザによる運用の第２の例として、オフィス内に２人のユーザ（ユーザＣ、ユーザＤ）がいて、ユーザＣがログイン入力操作装置２（例えば、ＰＣ）を管理し、登録済みの携帯端末３を所持していて、ユーザＤがユーザＣの不在時にログイン入力操作装置２を利用しようとする場合を想定する。このとき、ユーザＤがログイン入力操作装置２（例えば、ＰＣ）にログイン要求をしたときに表示手段１３に表示されたパスワードを

読み取って携帯電話を使ってユーザＣに口頭で教え、離れた場所にいるユーザＣが教わったパスワードを携帯端末３に入力することで、ユーザＤがログインすることができる（代理ログインを行うことができる）。

【００４３】

［パスワードを画像やバーコードで表示する運用例］

次に、携帯端末３が例えばカメラ付携帯電話である場合には、パスワードを画像やバーコードで表示する運用が可能である。この場合には、例えば、パスワードをＱＲコード（登録商標）で表示し、ユーザが携帯端末３のカメラでパスワードとしてのＱＲコード（登録商標）を取り込むことができる。その結果、パスワードを入力する操作を行う手間を省くことができる。

【００４４】

［認証システムの動作］

図１に示した認証システムの動作について図３を参照（適宜図１および図２参照）して説明する。図３は、図１に示した認証システムの動作の一例を示すシーケンス図である。予め、ユーザは、携帯端末３をサーバ４に登録しておく。すなわち、サーバ４は、携帯端末３の端末情報を端末情報記憶手段３１にユーザ名と共に記憶しておく。はじめに、ユーザがログイン入力操作装置２を用いてログインを要求するための入力操作および送信操作を行う。すなわち、ログイン入力操作装置２は、入力手段１０によって、ログイン要求を入力し（ステップＳ１）、ログイン要求送信手段１６によって、通信手段１１を介してログイン要求を装置情報と共にサーバ４へ送信する（ステップＳ２）。

【００４５】

次いで、サーバ４は、ログイン要求受信手段４１によって、通信手段２０を介してログイン要求を装置情報と共に受信する（ステップＳ３）。そして、サーバ４は、パスワード生成手段４２によって、受信した装置情報に基づいてパスワードを生成し、パスワードを当該装置情報と共にパスワード記憶手段３２に登録し（ステップＳ４：パスワード生成ステップ）、パスワード送信手段４３によって、パスワードを通信手段２０を介してログイン入力操作装置２へ送信する（ステップＳ５：パスワード送信ステップ）。

【００４６】

次いで、ログイン入力操作装置２は、パスワード受信手段１７によって、通信手段１１を介してパスワードを受信し（ステップＳ６）、受信したパスワードを表示手段１３に画面表示する（ステップＳ７：パスワード表示ステップ）。ログイン入力操作装置２を操作したユーザは、画面表示されたパスワードを確かめて携帯端末３に入力する操作および送信する操作を行う。すなわち、携帯端末３は、ユーザの入力操作に基づいて、パスワードを入力し（ステップＳ８：パスワード入力ステップ）、入力されたパスワードを当該携帯端末３の端末情報と共にサーバ４へネットワークＮを介して送信する（ステップＳ９：パスワード送信ステップ）。

【００４７】

次いで、サーバ４は、パスワード受信手段４４によって、通信手段２０を介してパスワードを携帯端末３の端末情報と共に受信し（ステップＳ１０：パスワード受信ステップ）、端末判別手段４５によって、受信した端末情報と一致する端末情報が端末情報記憶手段３１に登録されているか否かを判別する（ステップＳ１１：端末判別ステップ）。受信した端末情報が既に登録されている場合（ステップＳ１１：Ｙｅｓ）、サーバ４は、パスワード判別手段４６によって、受信したパスワードと一致するパスワードがパスワード記憶手段３２に登録されているかを判別する（ステップＳ１２：パスワード判別ステップ）。そして、サーバ４は、認証結果通知手段４７によって、通信手段２０を介して認証結果をログイン入力操作装置２へ通知する（ステップＳ１３：パスワード判別ステップ）。これにより、ログイン入力操作装置２は、認証結果受信手段１８によって、通信手段１１を介して認証結果を受信し（ステップＳ１４）、受信した認証結果を表示手段１３に画面表示する（ステップＳ１５）。

【００４８】

ここで、ステップＳ１２において、サーバ４が受信したパスワードが既に登録されている場合（ステップＳ１２：Ｙｅｓ）、認証成功なので、ステップＳ１３において、サーバ４は、認証成功を示す画面表示データを認証結果として通知する。これにより、ログイン入力操作装置２には、認証成功を示す画面が表示される。引き続いて、サーバ４は、サービス提供手段４８によって、ユーザのサービス要求にしたがって、ユーザの所望するサービス情報をサービス情報記憶手段３３から読み出して提供する（ステップＳ１６）。

【００４９】

一方、ステップＳ１２において、サーバ４が受信したパスワードが未登録である場合（ステップＳ１２：Ｎｏ）、認証失敗なので、ステップＳ１３において、サーバ４は、認証失敗を示す画面表示データを認証結果として通知する。これにより、ログイン入力操作装置２には、認証失敗を示す画面が表示される。また、ステップＳ１１において、サーバ４が受信した端末情報が未登録である場合（ステップＳ１１：Ｎｏ）、認証失敗なので、サーバ４は、ステップＳ１２をスキップしてステップＳ１３において、認証失敗を示す画面表示データを認証結果として通知する。

【００５０】

本実施形態によれば、認証システム１では、ユーザは、従来のようにパスワードの受け取り先を指定する情報をログイン認証サーバへ送信する必要がないので、入力操作の手間を低減して迅速にログインすることができる。また、認証システム１では、サーバ４にログイン入力操作装置２を事前登録する必要がなく、ユーザは、事前登録されていないログイン入力操作装置２からでもログインを要求しユーザ認証を受けることができる。また、ログイン入力操作装置２は、ユーザがサーバ４に事前登録した固有情報（携帯端末３の端末情報）をサーバ４に送信することはない。つまり、ユーザは、個人を特定することのできる固有情報をログイン入力操作装置２に入力する必要がない。そのため、ログイン時における個人情報の漏洩を防止することができる。したがって、ユーザは、ログイン入力操作装置２と携帯端末３とを利用すれば、いつでもどこからでもセキュアなログイン認証を受けることが可能となる。また、認証システム１では、ユーザは、携帯端末３を用いてパスワードをサーバ４へ入力する際に、ログイン入力操作装置２と携帯端末３との両方を活用するので、一方の装置しか利用しない場合に比べてセキュリティを高めることができる。

【００５１】

（変形例）

以上の説明では、第１実施形態の一例として、ログイン入力操作装置２のパスワード受信手段１７は、受信したパスワードをそのまま表示手段１３へ表示させるものとして説明したが、受信したパスワードを出力手段１４を介して携帯端末３へ送信することもできる。この例を変形例として説明する。この場合、認証システム１の各装置の構成は、図１に示したものと同様なので説明を省略する。

【００５２】

次に、変形例の認証システムの動作について図４を参照（適宜図１および図２参照）して説明する。図４は、図１に示した認証システムの動作の他の例を示すシーケンス図である。図４に示すステップＳ２１～ステップＳ２６およびステップＳ３０～ステップＳ３６は、図３に示したステップＳ１～ステップＳ６およびステップＳ１０～ステップＳ１６と同様なので説明を省略する。ステップＳ２６に続いて、ログイン入力操作装置２は、パスワード送信手段１９によって、サーバ４から受信したパスワードを携帯端末３に送信する（ステップＳ２７：パスワード送信ステップ）。携帯端末３は、ログイン入力操作装置２からパスワードを受信し（ステップＳ２８：パスワード受信ステップ）、受信したパスワードを当該携帯端末３の端末情報と共にサーバ４に送信する（ステップＳ２９：パスワード送信ステップ）。

【００５３】

この変形例は、パスワードをログイン入力操作装置２と携帯端末３との直接通信で受け渡し、携帯端末３からパスワードをサーバ４に送信するので、従来のログイン認証方法と

比べて以下のような優れた効果を奏する。（１）他のユーザによるパスワードの盗み見を困難にさせることができる。（２）ユーザがパスワードを入力する手間を低減できる。例えば、パスワードが数字や記号による長いコードである場合や、数字や記号が時々刻々変化するコードである場合に、特に有効である。（３）キーロガー等のスパイウェアやウイルスに対する耐性が強い。

【００５４】

（第２実施形態）

［認証システムの構成］

図５は、本発明の第２実施形態に係るサーバを含む認証システムの構成を模式的に示す図である。図５に示す認証システム１Ａは、パスワード通知選択型ログイン認証を可能とするものである。このパスワード通知選択型ログイン認証は、ログイン入力操作装置２から携帯端末３へのパスワードの通知方式（以下、単に通知方式という）が複数あることを前提としたログイン認証である。

【００５５】

従来技術では、パスワードの入力方式がパスワードを入力する装置ごとに固定的に決められている。また、従来技術では、ユーザが、ログイン後のサービス利用権限（以下、ユーザ権限という）を設定しようとする場合には、管理者権限を持つユーザ（システム管理者）がログインした後でなければ設定することができない。第２実施形態では、管理者権限のないユーザであっても、ログイン認証を行うログイン入力操作装置２によって自由にユーザ権限を設定することができる。ただし、管理者が決めた権限以上は設定できないこととする。

【００５６】

図５に示す認証システム１Ａは、サーバ４Ａの制御手段４０に設定情報判別手段５０を備え、その他の構成は図１に示した認証システム１と同様なので、同一の構成には同一の符号を付して説明を適宜省略する。また、本実施形態では、ユーザは、ログイン入力操作装置２からログイン要求をする際に、通知方式およびユーザ権限に関する設定情報を選択してサーバ４Ａへ通知することが特徴である。

【００５７】

ここで、ログイン入力操作装置２のログイン画面の一例について図６を参照して説明する。図６は、図５に示したログイン入力操作装置の表示手段に表示されるログイン画面の一例を示す図である。ログイン画面６００は、図６に示すように、サーバ名入力欄６１０と、通知方式選択欄６２０と、ユーザ権限選択欄６３０と、送信ボタン６４０と、リターンボタン６５０とを備えている。ユーザは、ログイン画面６００が表示されているときに、ログイン認証を行うサーバ４Ａをサーバ名入力欄６１０に入力するだけではなく、必要に応じて、通知方式選択欄６２０で通知方式を選択したり、ユーザ権限選択欄６３０でユーザ権限を選択したりすることができる。ユーザが、ログイン画面６００の送信ボタン６４０を押下することで、ログイン入力操作装置２は、ログイン要求送信手段１６（図５参照）によって、ログイン要求と、通知方式およびユーザ権限に関する設定情報とをサーバ４Ａへ送信する。なお、本実施形態では、ユーザ権限ごとにセキュリティレベルを設定するように構成したが、ユーザ権限ごとにパスワード通知方式を設定するように構成することもできる。

【００５８】

図５に戻って、サーバ４Ａの構成を説明する。

本実施形態では、サーバ４Ａにおいて、ログイン要求受信手段４１は、ログイン入力操作装置２から、パスワードの予め定められた通知方式およびユーザ権限に関する設定情報を、ログイン要求および装置情報と共に受信する。なお、設定情報は、必ずしも通知方式とユーザ権限との両方に関する必要はなくいずれか一方に関するものであってもよい。

【００５９】

サーバ４Ａは、記憶手段３０のメモリに設定情報が予め登録されている。

設定情報判別手段５０は、受信した設定情報が、予め登録された設定情報のうちのいず

れであるかを判別するものである。判別結果は、パスワード生成手段４２に出力される。
パスワード生成手段４２は、受信した設定情報で指定されるパスワードを生成する。なお、設定情報と、パスワードの種類とは予め対応付けられている。
パスワード送信手段４３は、生成したパスワードを、受信した設定情報と共にログイン入力操作装置２に送信する。本実施形態では、ログイン入力操作装置２は、受信した設定情報に応じて、受信したパスワードを携帯端末３に通知する方式を切り替えることができるように構成されている。

【００６０】

［設定情報とパスワードとの対応付け］

パスワードの通知方式は、低セキュリティな通知方式と高セキュリティな通知方式とに大別できる。低セキュリティな通知方式で通知されるパスワードとは、パスワードの表現を見た人間がパスワードを容易に理解できるような記号や文字、または単純な図形等の画像等である。言い換えると、低セキュリティな通知方式は、パスワードを他のユーザに容易に教えられる方式のことを指す。この低セキュリティな通知方式の例としては、パスワードをログイン入力操作装置２の表示部１３に単純に画面表示するような方式である。

【００６１】

一方、高セキュリティな通知方式で通知されるパスワードとは、パスワードの表現を見た人間がパスワードを容易には理解できないような複雑な図形等の画像やバーコードである。言い換えると、高セキュリティな通知方式は、パスワードの盗み見が難しい方式のことを指す。この高セキュリティな通知方式の例としては、パスワードをログイン入力操作装置２から携帯端末３に対して有線接続やＩＣチップ間通信等の無線通信により伝達する方式である。

【００６２】

一般に、セキュリティレベルの高低と、ユーザ権限の高低とは、連動していることが多い。すなわち、ユーザ権限が高いほど、セキュリティレベルの高い情報にアクセス可能であり、情報漏洩した場合の被害が大きくなるので、セキュリティレベルの高い通知方式を必要とする。したがって、本実施形態では、ユーザ権限を、セキュリティレベルの高低で表現することとした（図６参照）。なお、対象とする情報やユーザ権限の設定の仕方によっては必ずしも対応するものではないので、この例に限定されるものではない。

【００６３】

［認証システムの動作］

次に、第２実施形態に係る認証システムの動作について図７を参照（適宜図５および図６参照）して説明する。図７は、図５に示した認証システムの動作の一例を示すシーケンス図である。以下では、図３を参照して説明した動作と同様な動作については、詳細な説明を適宜省略する。

【００６４】

事前に、サーバ４Ａに、通知方式およびユーザ権限に関する設定情報を登録しておく。ユーザは、ログイン要求の入力時に、ユーザ権限とパスワードの通知方式とを選択する。すなわち、ログイン入力操作装置２は、入力手段１０によって、ログイン要求および設定情報を入力し（ステップＳ４１）、ログイン要求送信手段１６によって、ログイン要求および設定情報を装置情報と共にサーバ４Ａへ送信する（ステップＳ４２）。

【００６５】

次いで、サーバ４Ａは、ログイン要求受信手段４１によって、ログイン要求および設定情報を装置情報と共に受信し（ステップＳ４３：ログイン要求受信ステップ）、設定情報判別手段５０によって、受信した設定情報が、予め登録された設定情報のうちのいずれであるかを判別する（ステップＳ４４：設定情報判別ステップ）。そして、サーバ４Ａは、パスワード生成手段４２によって、受信した装置情報および設定情報に基づいてパスワードを生成し、パスワードを当該装置情報と共にパスワード記憶手段３２に登録し（ステップＳ４５：パスワード生成ステップ）、パスワード送信手段４３によって、パスワードおよび設定情報をログイン入力操作装置２へ送信する（ステップＳ４６：パスワード送信ス

テップ）。

【００６６】

次いで、ログイン入力操作装置２は、パスワード受信手段１７によって、パスワードおよび設定情報を受信し（ステップＳ４７）、受信した設定情報に応じて、受信したパスワードを携帯端末３に通知する方式を切り替える。例えば、設定情報が低セキュリティに対応している場合には、ログイン入力操作装置２は、サーバ４Ａから受信したパスワードを表示し（ステップＳ４８ａ：パスワード表示ステップ）、ユーザの入力操作に基づいて、携帯端末３は、パスワードを入力し（ステップＳ４９ａ：パスワード入力ステップ）、入力されたパスワードを当該携帯端末３の端末情報と共にサーバ４Ａに送信する（ステップＳ５０：パスワード送信ステップ）。

【００６７】

また、例えば、設定情報が高セキュリティに対応している場合には、ログイン入力操作装置２は、パスワード送信手段１９によって、サーバ４Ａから受信したパスワードを携帯端末３に送信し（ステップＳ４８ｂ：パスワード送信ステップ）、携帯端末３は、ログイン入力操作装置２からパスワードを受信し（ステップＳ４９ｂ：パスワード受信ステップ）、受信したパスワードを当該携帯端末３の端末情報と共にサーバ４Ａに送信する（ステップＳ５０：パスワード送信ステップ）。その後、図７に示すステップＳ５１～ステップＳ５７は、図３に示したステップＳ１０～ステップＳ１６と同一なので説明を省略する。

【００６８】

本実施形態によれば、ユーザは以下に示すように場面に応じてユーザ権限やパスワードの通知方式を設定変更することができる。例えば、ログイン入力操作装置２の設置場所が、大勢の人々が出入りできる共有スペース（例えば、複数のＰＣが配置された場所）である場合には、ユーザ権限を制限する（ユーザ権限を高セキュリティに設定する）。または、パスワードをログイン入力操作装置２から携帯端末に通信により通知し、携帯端末３の画面にパスワードを表示させる。また、例えば、ログイン入力操作装置２の設置場所が、人の出入りが制限された制限スペース（例えば、単独のＰＣが配置された社内や家庭の個室）である場合には、ユーザ権限を制限しない（ユーザ権限を低セキュリティに設定する）。または、パスワードをログイン入力操作装置２に表示させ、ユーザが、表示されたパスワードを携帯端末に簡易に入力する。

【００６９】

以上、本発明の好ましい実施形態について説明したが、本発明は前記した各実施形態に限定されるものではない。例えば、サーバ４（またはサーバ４Ａ）は、一般的なコンピュータを、前記した各手段として機能させるプログラム（認証管理プログラム）により動作させることで実現することができる。このプログラムは、通信回線を介して配布することも可能であるし、ＣＤ－ＲＯＭ等の記録媒体に書き込んで配布することも可能である。このプログラムをインストールされたコンピュータは、ＣＰＵが、ＲＯＭ等に格納されたこのプログラムをＲＡＭに展開することにより、サーバ４（またはサーバ４Ａ）と同等の効果を奏することができる。

【００７０】

また、各実施形態では、ログイン入力操作装置２がＰＣであるものとして説明したが、これに限定されるものでなく、入退室管理用のミニパネルとしてもよい。この場合に、ユーザは、所定の施設のミニパネルが設置された部屋の入退場や列車の車両の入退場において、携帯端末３を入場券や乗車券として使用する運用が可能となる。また、各実施形態では、サーバ４（またはサーバ４Ａ）に事前登録する情報は、携帯端末３の端末情報（製品番号や契約者番号）であるものとしたが、それ以外に、ユーザの課金情報等を登録するようにしてもよい。この場合に、ログイン入力操作装置２が入退室管理用のミニパネルとするならば、ユーザは、携帯端末３を入場券や乗車券として使用するときに、携帯端末３をプリペイド（場料や乗車料が支払い済であること）のステータス（身分証）代わりに利用することも可能となる。

【００７１】

また、第２実施形態では、ログイン入力操作装置２からサーバ４Ａへログイン要求を送る際に、パスワードの通知方式とユーザ権限とを選択できるものとして説明したが、ユーザ権限の変更のみに限定すれば携帯端末３から設定することも可能である。この場合には、携帯端末３は、パスワードをサーバ４Ａに送信する際に、ユーザ権限の変更に関する情報を共に送信するように構成することができる。このように携帯端末３からユーザ権限の変更を適宜行えるようにした場合には、以下のような運用が可能である。例えば、ログイン入力操作装置２を入退室管理用のミニパネルとする。そして、工場や実験室等の所定の施設（建物、敷地内）の随所に複数のミニパネルを設置し、この施設内を通行する通行者、例えば管理者、作業者、運送業者、見学者等に対応したユーザ権限（セキュリティレベル）を予め設定する。セキュリティレベルとして、例えば、管理者は、レベル１～４で可変とする。同様に、作業者は、レベル２～４で可変、運送業者はレベル３～４で可変、見学者はレベル４で固定のように定めることができる。各通行者は、入館許可証を受け取ったときに、所有するそれぞれの携帯端末３をサーバ４Ａに事前登録しておく。そして、各通行者は、ユーザ権限の初期値をレベル４に設定して施設内の所望の場所に移動し、管理者がユーザ権限をレベル１に変更したときにだけ、管理者室に入出できるようにすることもできる。つまり、入館許可証で通行できるエリアをより細かく設定できるようになる。さらに、この場合には、従来技術と異なり、制限エリアごとに別々の入館許可証を用意する必要もなくなる。

【図面の簡単な説明】

【００７２】

【図１】本発明の第１実施形態に係るサーバを含む認証システムの構成を模式的に示す図である。

【図２】図１に示したログイン入力操作装置の表示手段に表示されるログイン画面の一例を示す図である。

【図３】図１に示した認証システムの動作の一例を示すシーケンス図である。

【図４】図１に示した認証システムの動作の他の例を示すシーケンス図である。

【図５】本発明の第２実施形態に係るサーバを含む認証システムの構成を模式的に示す図である。

【図６】図５に示したログイン入力操作装置の表示手段に表示されるログイン画面の一例を示す図である。

【図７】図５に示した認証システムの動作の一例を示すシーケンス図である。

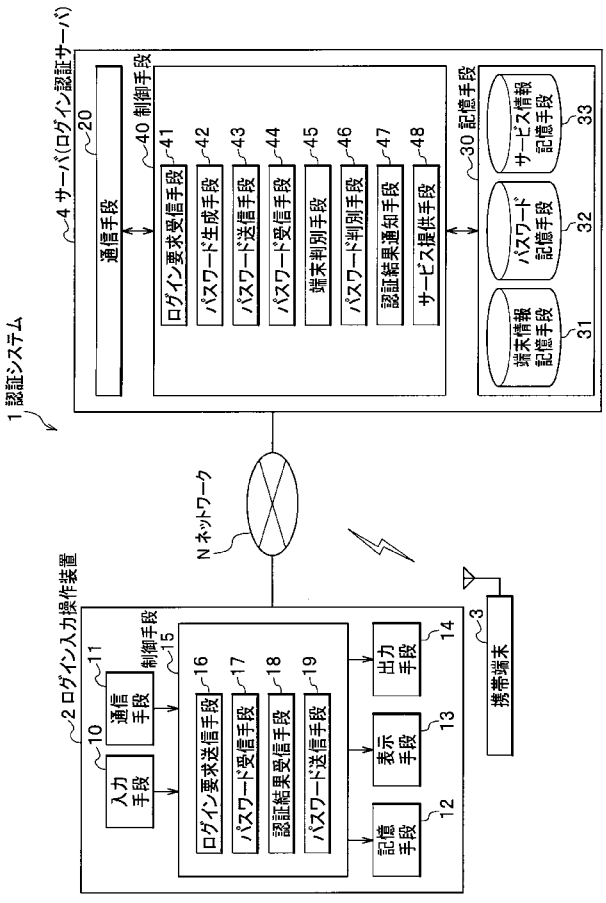
【符号の説明】

【００７３】

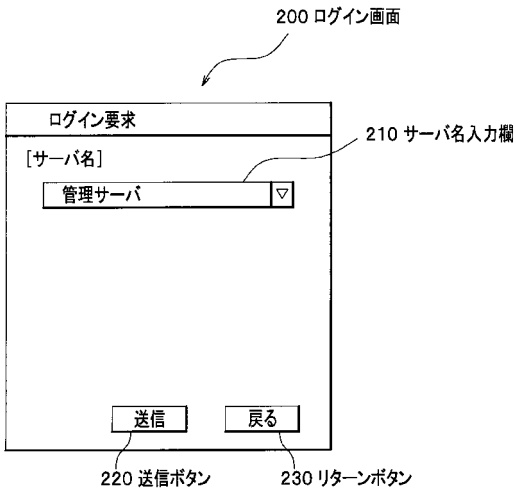
１，１Ａ　認証システム
２　　ログイン入力操作装置
３　　携帯端末
４，４Ａ　サーバ（ログイン認証サーバ）
１０　　入力手段
１１　　通信手段
１２　　記憶手段
１３　　表示手段
１４　　出力手段
１５　　制御手段
１６　　ログイン要求送信手段
１７　　パスワード受信手段
１８　　認証結果受信手段
１９　　パスワード送信手段
２０　　通信手段
３０　　記憶手段
３１　　端末情報記憶手段

３２　パスワード記憶手段
３３　サービス情報記憶手段
４０　制御手段
４１　ログイン要求受信手段
４２　パスワード生成手段
４３　パスワード送信手段
４４　パスワード受信手段
４５　端末判別手段
４６　パスワード判別手段
４７　認証結果通知手段
４８　サービス提供手段
５０　設定情報判別手段
Ｎ　ネットワーク

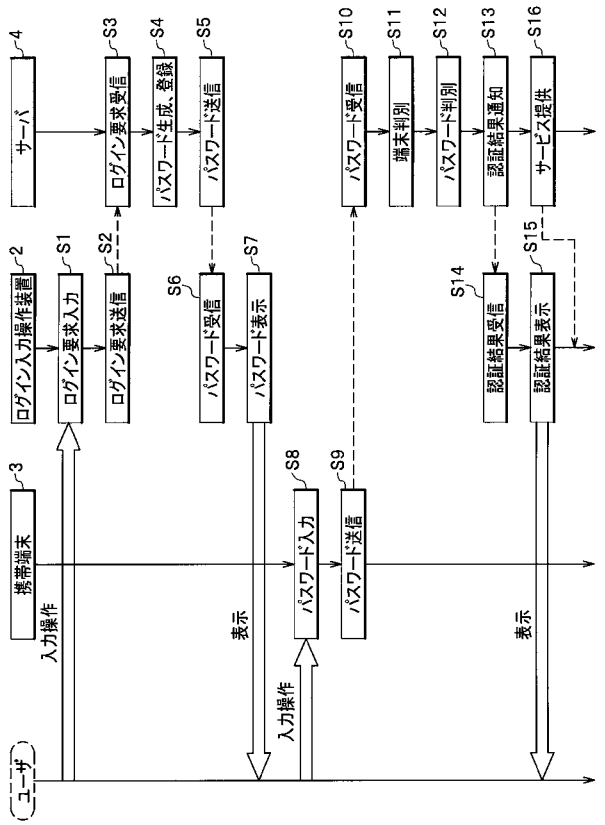
【図１】



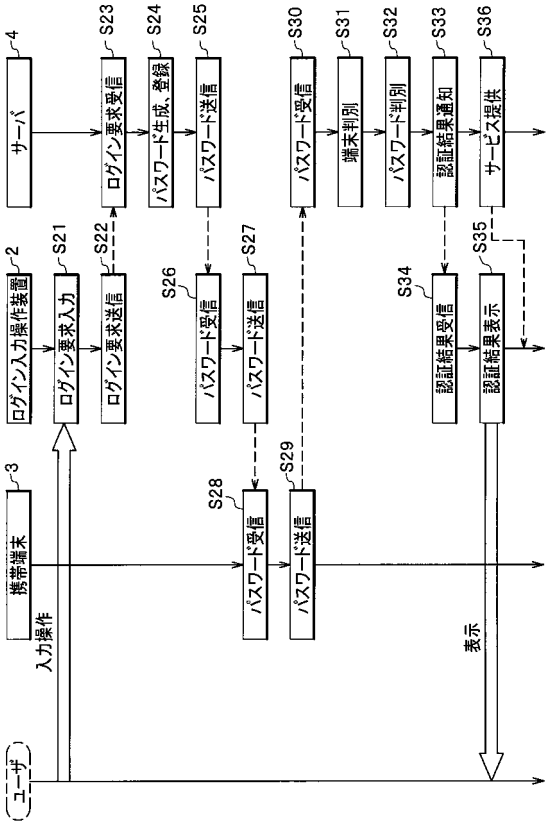
【図２】



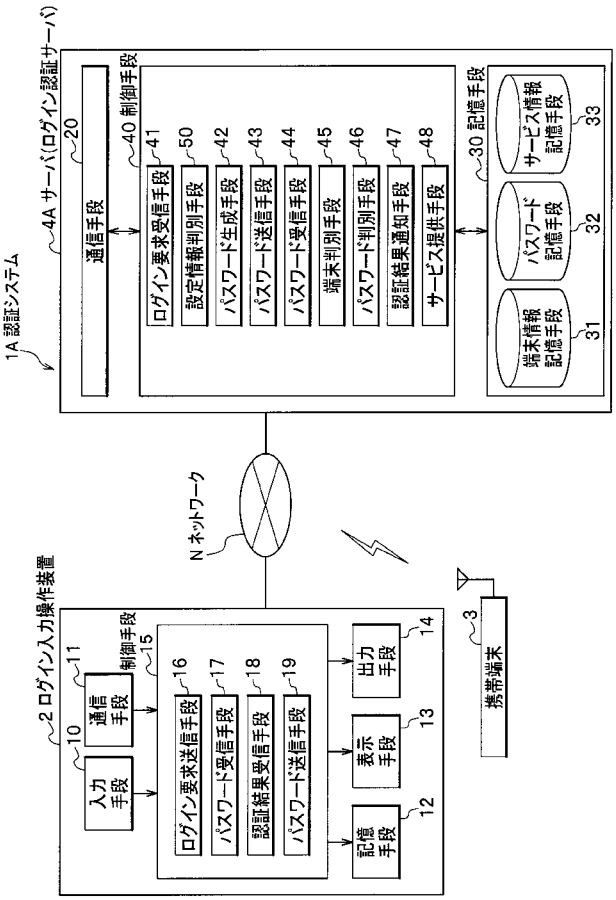
【図３】


サーバ
ログイン入力操作装置
携帯端末
ユーザ
ログイン要求受信
パスワード生成、登録
パスワード送信
パスワード受信
パスワード表示
パスワード入力
パスワード送信
パスワード受信
端末判別
パスワード判別
認証結果通知
サービス提供
ログイン要求入力
ログイン要求送信
パスワード受信
認証結果受信
認証結果表示
入力操作
表示
入力操作
表示
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
S13
S14
S15
S16

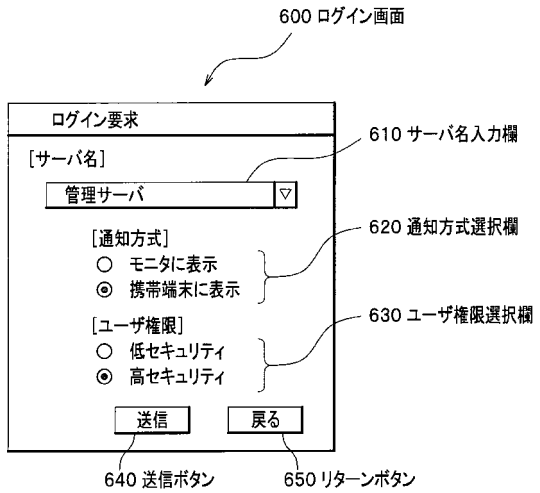
【図４】


サーバ
ログイン入力操作装置
携帯端末
ユーザ
ログイン要求受信
パスワード生成、登録
パスワード送信
パスワード受信
端末判別
パスワード判別
認証結果通知
サービス提供
ログイン要求入力
ログイン要求送信
パスワード受信
パスワード送信
パスワード受信
パスワード送信
認証結果受信
認証結果表示
入力操作
表示
S21
S22
S23
S24
S25
S26
S27
S28
S29
S30
S31
S32
S33
S34
S35
S36

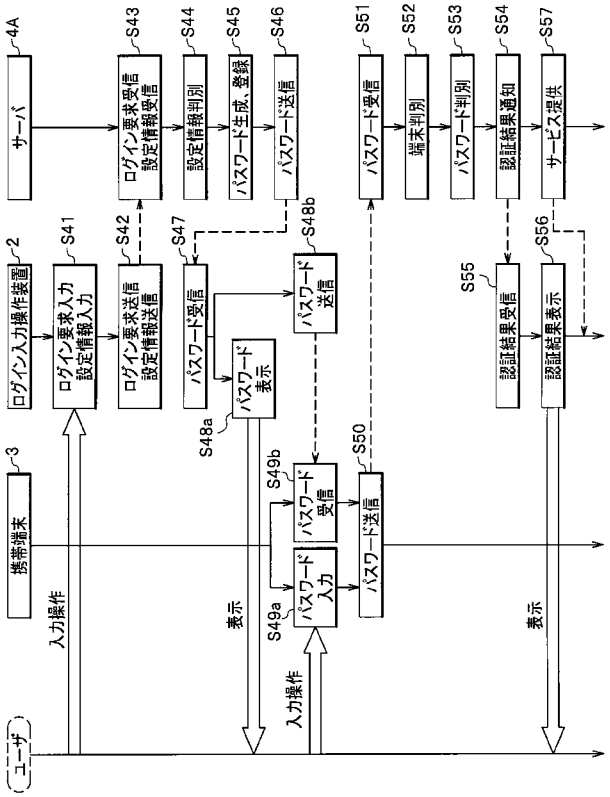
【図５】


1A 認証システム
4A サーバ(ログイン認証サーバ)
20
通信手段
40 制御手段
41
ログイン要求受信手段
50
設定情報判別手段
42
パスワード生成手段
43
パスワード送信手段
44
パスワード受信手段
45
端末判別手段
46
パスワード判別手段
47
認証結果通知手段
48
サービス提供手段
30 記憶手段
サービス情報記憶手段
33
パスワード記憶手段
32
端末情報記憶手段
31
N ネットワーク
2 ログイン入力操作装置
10
入力手段
11
通信手段
制御手段
15
16
ログイン要求送信手段
17
パスワード受信手段
18
認証結果受信手段
19
パスワード送信手段
記憶手段
12
表示手段
13
出力手段
14
3
携帯端末

【図６】


600 ログイン画面
ログイン要求
[サーバ名]
管理サーバ
610 サーバ名入力欄
[通知方式]
モニタに表示
携帯端末に表示
620 通知方式選択欄
[ユーザ権限]
低セキュリティ
高セキュリティ
630 ユーザ権限選択欄
送信
戻る
640 送信ボタン
650 リターンボタン

【図７】


4A
サーバ
S43
ログイン要求受信
設定情報受信
S44
設定情報判別
S45
パスワード生成、登録
S46
パスワード送信
S51
パスワード受信
S52
端末判別
S53
パスワード判別
S54
認証結果通知
S57
サービス提供
2
ログイン入力操作装置
S41
ログイン要求入力
設定情報入力
S42
ログイン要求送信
設定情報送信
S47
パスワード受信
S48b
パスワード
送信
S55
認証結果受信
S56
認証結果表示
S48a
パスワード
表示
3
携帯端末
S49b
パスワード
受信
S50
パスワード送信
入力操作
表示
S49a
パスワード
入力
入力操作
表示
ユーザ

フロントページの続き

Ｆターム(参考) 5B285 AA01 BA01 BA03 BA07 BA09 CA02 CB02 CB42 CB43 CB53
CB55 CB62 CB73 CB85 CB95 DA04 DA05 DA06 DA10
5J104 AA07 KA01 KA06 MA01 PA07