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

特許第6387887号
(P6387887)

(45)発行日　平成30年9月12日(2018.9.12)　(24)登録日　平成30年8月24日(2018.8.24)

(51)Int.Cl.		F I		
G06F 21/36	(2013.01)	G06F	21/36	
G06F 21/31	(2013.01)	G06F	21/31	
H04L 9/32	(2006.01)	H04L	9/00	673A
G06F 1/00	(2006.01)	G06F	1/00	370E

請求項の数 7　(全 15 頁)

(21)出願番号　特願2015-79357(P2015-79357)
(22)出願日　平成27年4月8日(2015.4.8)
(65)公開番号　特開2016-200904(P2016-200904A)
(43)公開日　平成28年12月1日(2016.12.1)
審査請求日　平成29年2月22日(2017.2.22)

(73)特許権者　000006150
京セラドキュメントソリューションズ株式会社
大阪府大阪市中央区玉造１丁目２番２８号
(74)代理人　100097113
弁理士　堀　城之
(74)代理人　100162363
弁理士　前島　幸彦
(72)発明者　中里　洋介
大阪府大阪市中央区玉造１丁目２番２８号　京セラドキュメントソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】認証装置、認証プログラム、及び認証システム

(57)【特許請求の範囲】
【請求項１】
ユーザー識別情報と、基準とする基準識別情報と、複数の識別表示の中から選択された複数の選択識別表示及び前記選択識別表示の順番からなる選択順識別表示列とをユーザー毎に登録するユーザー情報登録処理部と、
前記複数の識別表示をランダムに配列したランダム識別表示列における前記基準識別情報に対応する識別表示の位置から前記選択順識別表示列の前記選択識別表示までの位置を前記選択識別表示の前記順番に算出して決定されたパスワードと、前記ユーザー識別情報とを用いてユーザー認証を行うユーザー認証処理部と
を備え、
前記ユーザー認証処理部は、
前記複数の識別表示をランダムに配列することにより、少なくとも全ての前記選択識別表示を含むランダム識別表示列を作成し、
前記選択順識別表示列の前記選択識別表示の各々に対して、前記ランダム識別表示列内の前記各選択識別表示が前記基準識別情報から何番目の位置にあるかを示す値を算出し、
前記選択識別表示列における前記選択識別表示の前記順番に基づいて前記算出された値を配列した前記パスワードを作成する
ことを特徴とする認証装置。
【請求項２】
前記基準識別情報は、前記複数の識別表示の中から選択された１つの基準識別表示であ

ることを特徴とする請求項１に記載の認証装置。
【請求項３】
前記基準識別情報は、前記ランダム識別表示列の基準位置であることを特徴とする請求項１に記載の認証装置。
【請求項４】
表示部を備え、
前記ユーザー認証処理部は、前記ランダム識別表示列を前記表示部に表示することを特徴とする請求項１から請求項３の何れか一項に記載の認証装置。
【請求項５】
前記ユーザー認証処理部は、前記ユーザー認証がエラーとなったときにユーザー認証エラー通知を前記表示部に表示することを特徴とする請求項４に記載の認証装置。
【請求項６】
ユーザー識別情報と、基準とする基準識別情報と、複数の識別表示の中から選択された複数の選択識別表示及び前記選択識別表示の順番からなる選択順識別表示列とをユーザー毎に登録するユーザー情報登録処理部、及び
前記複数の識別表示をランダムに配列したランダム識別表示列における前記基準識別情報に対応する識別表示の位置から前記選択順識別表示列の前記選択識別表示までの位置を前記選択識別表示の前記順番に算出して決定されたパスワードと、前記ユーザー識別情報とを用いてユーザー認証を行うユーザー認証処理部として認証装置のコンピューターを機能させ、
前記ユーザー認証処理部は、
前記複数の識別表示をランダムに配列することにより、少なくとも全ての前記選択識別表示を含むランダム識別表示列を作成し、
前記選択順識別表示列の前記選択識別表示の各々に対して、前記ランダム識別表示列内の前記各選択識別表示が前記基準識別情報から何番目の位置にあるかを示す値を算出し、
前記選択識別表示列における前記選択識別表示の前記順番に基づいて前記算出された値を配列した前記パスワードを作成する
ことを特徴とする認証プログラム。
【請求項７】
ネットワークを介して接続された認証装置、画像形成装置、及び端末装置を有し、
前記認証装置は、
ユーザー識別情報と、基準とする基準識別情報と、複数の識別表示の中から選択された複数の選択識別表示及び前記選択識別表示の順番からなる選択順識別表示列とをユーザー毎に登録するユーザー情報登録処理部と、
前記複数の識別表示をランダムに配列したランダム識別表示列における前記基準識別情報に対応する識別表示の位置から前記選択順識別表示列の前記選択識別表示までの位置を前記選択識別表示の前記順番に算出して決定されたパスワードと、前記ユーザー識別情報とを用いてユーザー認証を行うユーザー認証処理部と
を備え、
前記ユーザー認証処理部は、
前記複数の識別表示をランダムに配列することにより、少なくとも全ての前記選択識別表示を含むランダム識別表示列を作成し、
前記選択順識別表示列の前記選択識別表示の各々に対して、前記ランダム識別表示列内の前記各選択識別表示が前記基準識別情報から何番目の位置にあるかを示す値を算出し、
前記選択識別表示列における前記選択識別表示の前記順番に基づいて前記算出された値を配列した前記パスワードを作成し、
前記端末装置から前記画像形成装置に操作が行われたときに、前記認証装置の前記ユーザー認証処理部は前記端末装置から入力された前記ユーザー識別情報によりユーザー認証を行うことを特徴とする認証システム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、本人であるかを認証する認証装置、認証プログラム、及び認証システムに関する。
【背景技術】
【０００２】
インターネットの普及により、インターネットを使用して買い物や現金の振り込みを行うことができる。このため、他人が本人になりすまして買い物や現金の振り込みを行うことを防止するために、本人認証を行っている。しかし、パスワードによる本人認証では、覗き見や盗聴などによりパスワードが漏洩した場合に、パスワードを入手した他人が容易に本人になりすますことができる。このため、一回だけ有効となる使い捨てパスワード（以下、「ワンタイムパスワード」という）が用いられている。例えば、特許文献１の本人認証方式では、マトリックスに毎回異なるランダムな記号を発生させ、ユーザーが自分で定義したワンタイムパスワード用パターンに従ってマトリックスの記号を順に読み取り、読み取った記号列をワンタイムパスワードとして利用することができる本人認証方式を提供している。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００６－３０１６８４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかし、特許文献１のワンタイムパスワードによる本人認証方式では、ユーザーが自分で定義したワンタイムパスワード用パターンに基づいてワンタイムパスワードが作成されるので、ユーザーは自分で定義したワンタイムパスワード用パターンを覚えなければならないという問題があった。また、同じワンタイムパスワード用パターンを長期間使用すると、複数のワンタイムパスワードが覗き見や盗聴されることで、ワンタイムパスワード用パターンが推測される恐れがある。このため、ユーザーがワンタイムパスワード用パターンを定期的に変更しなければならない。しかし、ユーザーは、ワンタイムパスワード用パターンを変更する度に、複雑なワンタイムパスワード用パターンを覚えなければならないという問題があった。また、生体認証のような認証を行うためには、新たな機器を設置しなければならないという問題があった。
【０００５】
本発明はこのような状況に鑑みてなされたものであり、上記課題を解決できる認証装置、認証プログラム、及び認証システ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】
【０００６】
本発明の認証装置は、ユーザー識別情報と、基準とする基準識別情報と、複数の識別表示の中から選択された複数の選択識別表示及び前記選択識別表示の順番からなる選択順識別表示列とをユーザー毎に登録するユーザー情報登録処理部と、前記複数の識別表示をランダムに配列したランダム識別表示列における前記基準識別情報に対応する識別表示の位置から前記選択順識別表示列の前記選択識別表示までの位置を前記選択識別表示の前記順番に算出して決定されたパスワードと、前記ユーザー識別情報とを用いてユーザー認証を行うユーザー認証処理部とを備え、前記ユーザー認証処理部は、前記複数の識別表示をランダムに配列することにより、少なくとも全ての前記選択識別表示を含むランダム識別表示列を作成し、前記選択順識別表示列の前記選択識別表示の各々に対して、前記ランダム識別表示列内の前記各選択識別表示が前記基準識別情報から何番目の位置にあるかを示す値を算出し、前記選択識別表示列における前記選択識別表示の前記順番に基づいて前記算出された値を配列した前記パスワードを作成することを特徴としている。

また、本発明の認証装置の前記基準識別情報は、前記ランダム識別表示列の基準位置であることを特徴としている。

また、本発明の認証装置は、表示部を備え、前記ユーザー認証処理部は、前記ランダム識別表示列を前記表示部に表示することを特徴としている。

また、本発明の認証装置の前記ユーザー認証処理部は、前記ユーザー認証がエラーとなったときにユーザー認証エラー通知を前記表示部に表示することを特徴としている。

本発明の認証プログラムは、ユーザー識別情報と、基準とする基準識別情報と、複数の識別表示の中から選択された複数の選択識別表示及び前記選択識別表示の順番からなる選択順識別表示列とをユーザー毎に登録するユーザー情報登録処理部、及び

前記複数の識別表示をランダムに配列したランダム識別表示列における前記基準識別情報に対応する識別表示の位置から前記選択順識別表示列の前記選択識別表示までの位置を前記選択識別表示の前記順番に算出して決定されたパスワードと、前記ユーザー識別情報とを用いてユーザー認証を行うユーザー認証処理部として認証装置のコンピューターを機能させ、前記ユーザー認証処理部は、前記複数の識別表示をランダムに配列することにより、少なくとも全ての前記選択識別表示を含むランダム識別表示列を作成し、前記選択順識別表示列の前記選択識別表示の各々に対して、前記ランダム識別表示列内の前記各選択識別表示が前記基準識別情報から何番目の位置にあるかを示す値を算出し、前記選択識別表示列における前記選択識別表示の前記順番に基づいて前記算出された値を配列した前記パスワードを作成することを特徴としている。

本発明の認証システムは、ネットワークを介して接続された認証装置、画像形成装置、及び端末装置を有し、前記認証装置は、ユーザー識別情報と、基準とする基準識別情報と、複数の識別表示の中から選択された複数の選択識別表示及び前記選択識別表示の順番からなる選択順識別表示列とをユーザー毎に登録するユーザー情報登録処理部と、前記複数の識別表示をランダムに配列したランダム識別表示列における前記基準識別情報に対応する識別表示の位置から前記選択順識別表示列の前記選択識別表示までの位置を前記選択識別表示の前記順番に算出して決定されたパスワードと、前記ユーザー識別情報とを用いてユーザー認証を行うユーザー認証処理部とを備え、前記ユーザー認証処理部は、前記複数の識別表示をランダムに配列することにより、少なくとも全ての前記選択識別表示を含むランダム識別表示列を作成し、前記選択順識別表示列の前記選択識別表示の各々に対して、前記ランダム識別表示列内の前記各選択識別表示が前記基準識別情報から何番目の位置にあるかを示す値を算出し、前記選択識別表示列における前記選択識別表示の前記順番に基づいて前記算出された値を配列した前記パスワードを作成し、前記端末装置から前記画像形成装置に操作が行われたときに、前記認証装置の前記ユーザー認証処理部は前記端末装置から入力された前記ユーザー識別情報によりユーザー認証を行うことを特徴としている。

【発明の効果】

【０００７】

本発明の認証装置、認証プログラム、及び認証システムは、新たな機器を設けることなくセキュリティを確保できるワンタイムパスワード方式を容易に実現することができ、またワンタイムパスワードの作成方法が推測されることを防止できる。

【図面の簡単な説明】

【０００８】

【図１】本発明の実施形態１に係る認証システムの構成を示す図である。

【図２】図１に示す認証装置の機能構成を示す図である。

【図３】実施形態１に係る認証システムにおけるユーザー認証手順を示す図である。

【図４】実施形態１に係るパスワード設定画面の詳細について説明する図である。

【図５】実施形態１に係る認証装置のパスワード認証処理の流れを示すフローチャートである。

【図６】実施形態２に係るパスワード設定画面の詳細について説明する図である。

【発明を実施するための形態】

【０００９】
以下、本発明を実施するための第１の実施形態（以下、「実施形態１」という）を、図面を参照して説明する。実施形態１は、携帯端末から画像形成装置に対してジョブの実行要求を行うと、認証装置がパスワードによるユーザー認証を行い、正当なユーザーであると認証されると、画像形成装置がジョブの実行を行うものである。
【００１０】
まず、本実施形態１の認証装置１００を用いる認証システム１０の構成について、図１を用いて説明する。図１に示すように、認証システム１０は、認証装置１００、画像形成装置２００、携帯端末３００、アクセスポイント４００、ネットワーク５００、ルーター６００、インターネット７００、及びアクセスポイント８００によりにより構成されている。認証装置１００、画像形成装置２００、及びアクセスポイント４００は、ネットワーク５００に接続され、ネットワーク５００はルーター６００を経由してインターネット７００に接続されている。
【００１１】
認証装置１００は、ユーザーＩＤ（ユーザー識別情報）とパスワードによりユーザー認証を行うサーバーであり、画像形成装置２００、及び携帯端末３００とデータの送受信を行うことができる。
【００１２】
画像形成装置２００は、プリンター、多機能プリンター、多機能周辺装置、又は複合機であり、認証装置１００、及び携帯端末３００とデータの送受信を行うことができる。
【００１３】
携帯端末３００は、携帯電話、スマートフォン、タブレット端末等であり、ネットワーク５００のアクセスポイント４００、又はインターネット７００のアクセスポイント８００により認証装置１００、及び画像形成装置２００とデータの送受信を行うことができる。
【００１４】
アクセスポイント４００は、ネットワーク５００に接続され、無線通信によりアクセスポイント４００に対して接続要求を行っている携帯端末３００をネットワーク５００に接続する。
【００１５】
ネットワーク５００は、ＬＡＮ（Local Area Network）などのネットワーク(イントラネット等)であり、認証装置１００、画像形成装置２００、アクセスポイント４００、及びルーター６００が接続されている。
【００１６】
ルーター６００は、ネットワーク５００に接続され、ネットワーク５００をインターネット７００に接続する。
【００１７】
インターネット７００は、インターネットやイントラネット等のＩＰネットワークであり、携帯端末３００がアクセスポイント８００を経由してインターネット７００に接続される。
【００１８】
次に、認証システム１０の認証装置１００の機能構成について、図２を用いて説明する。図２に示す認証装置１００は、制御部１１０、メモリー部１２０、操作パネル１３０、操作パネル処理部１４０、及びネットワーク通信部１５０を備え、これら各部はバスなどにより接続される構成となっている。制御部１１０には、ユーザー情報登録処理部１１０ａとユーザー認証処理部１１０ｂが設けられている。メモリー部１２０には、画面データ記憶エリア１２０ａとユーザー情報記憶エリア１２０ｂが設けられている。
【００１９】
制御部１１０は、ＲＡＭやＲＯＭ等の主記憶手段、及びＣＰＵ(Central Processing Unit)等の制御手段を備えている。また、制御部１１０は、各種Ｉ／Ｏや、ＵＳＢ（ユニバ

ーサル・シリアル・バス）等のインターフェイス、バスコントローラー等を含む総合的な認証装置１００の制御を行う。

ユーザー情報登録処理部１１０ａは、携帯端末３００から登録されるユーザーＩＤ、ユーザー自身が決定することでユーザーだけが覚えることができる１つの記号（以下、「基準記号」という）、及び複数の記号の中から選択された複数の選択記号及び選択記号の順番からなる選択記号列（以下、「選択順記号列」という）を、ユーザー毎にユーザー情報記憶エリア１２０ｂに記憶する。また、ユーザーＩＤ、基準記号及び選択順記号列は画像形成装置２００から登録可能としてもよい。

ユーザー認証処理部１１０ｂは、登録されたユーザーＩＤと基準記号、選択順記号列及びユーザーが携帯端末３００から設定するパスワードによりユーザー認証を行う。ユーザー認証処理部１１０ｂが実行するユーザー認証処理の詳細については、後述する。

【００２０】

メモリー部１２０は、フラッシュメモリー等の補助記憶装置で、制御部１１０が実行する処理のプログラムやデータを記憶する。

画面データ記憶エリア１２０ａは、操作パネル１３０に表示する画面や携帯端末３００に表示する画面のフォーマット、表示データ、及び操作データなどを記憶する。画面データ記憶エリア１２０ａには、後述するユーザーＩＤ入力画面３１１、パスワード設定画面３１２、及びユーザー認証エラー通知画面３１３の表示や操作を行うためのデータが記憶される。

ユーザー情報記憶エリア１２０ｂは、ユーザー情報登録処理部１１０ａにより登録されたユーザーＩＤ、基準記号及び選択順記号列を記憶する。

【００２１】

操作パネル１３０は、認証装置１００が備えている機能に対する操作を行うための操作画面の表示と、ユーザーによる操作受け付けを行う液晶パネルである。

【００２２】

操作パネル処理部１４０は、操作画面を操作パネル１３０に表示する処理、又は操作パネル１３０から操作を入力する処理を行う。

【００２３】

ネットワーク通信部１５０は、着脱可能なＬＡＮインターフェイスを備え、ネットワーク５００に接続する。

【００２４】

次に、認証システム１０におけるユーザー認証手順について、図３を用いて説明する。

【００２５】

まず、（１）に示すように、ユーザーが携帯端末３００から画像形成装置２００に対してジョブを実行する操作を行うと、（２）に示すように、携帯端末３００は、画像形成装置２００にジョブを格納したジョブ実行要求通知を送信する。

【００２６】

次いで、画像形成装置２００は、携帯端末３００からジョブ実行要求通知を受信すると、（３）に示すように、認証装置１００にジョブ実行要求通知の送信元である携帯端末３００のアドレスを格納したユーザー認証要求通知を送信する。

【００２７】

次いで、認証装置１００は、画像形成装置２００からユーザー認証要求通知を受信すると、（４）に示すように、ユーザー認証要求通知に格納されたアドレスの携帯端末（以下、「携帯端末」という）３００に、ユーザーＩＤ入力画面３１１の表示や操作を行うためのデータ（以下、「ユーザーＩＤ入力画面データ」という）を送信する。

【００２８】

次いで、携帯端末３００は、認証装置１００からユーザーＩＤ入力画面データを受信すると、（５）に示すように、携帯端末３００の操作パネル３１０にユーザーＩＤ入力画面３１１を表示する。ユーザーＩＤ入力画面３１１には、ユーザーＩＤを入力するユーザーＩＤ入力エリア３１１ａが設けられている。

【００２９】
次いで、（６）に示すように、ユーザーがユーザーＩＤ入力画面３１１のユーザーＩＤ入力エリア３１１ａからユーザーＩＤを入力すると、（７）に示すように、携帯端末３００は、認証装置１００にユーザーＩＤを送信する。
【００３０】
次いで、認証装置１００は、携帯端末３００からユーザーＩＤを受信すると、（８）に示すように、携帯端末３００にパスワード設定画面３１２の表示や操作を行うためのデータ（以下、「パスワード設定画面データ」という）を送信する。
【００３１】
次いで、携帯端末３００は、認証装置１００からパスワード設定画面データを受信すると、（９）に示すように、携帯端末３００の操作パネル３１０にパスワード設定画面３１２を表示する。パスワード設定画面３１２には、ランダム記号列表示エリア３１２ａとパスワード設定エリア３１２ｂが設けられている。なお、パスワード設定画面３１２のランダム記号列表示エリア３１２ａとパスワード設定エリア３１２ｂの詳細については、後述する。
【００３２】
次いで、（１０）に示すように、ユーザーがパスワード設定画面３１２のパスワード設定エリア３１２ｂからパスワードを設定すると、（１１）に示すように、携帯端末３００は、認証装置１００にパスワードを送信する。
【００３３】
次いで、（１２）に示すように、認証装置１００は、パスワードを受信すると、ユーザーＩＤとパスワードによりユーザー認証を行う。
【００３４】
次いで、認証装置１００は、ユーザーＩＤとパスワードにより正当なユーザーと認証したときには、（１３）に示すように、画像形成装置２００にユーザー認証完了通知を送信する。
【００３５】
次いで、画像形成装置２００は、認証装置１００からユーザー認証完了通知を受信すると、（１４）に示すように、携帯端末３００から送信されたジョブ実行要求通知に格納されているジョブを実行する。
【００３６】
また、認証装置１００は、ユーザーＩＤとパスワードにより正当なユーザーと認証できなかったときには、（１５）に示すように、認証装置１００は、携帯端末３００にユーザー認証エラー通知画面の表示を行うためのデータ（以下、「ユーザー認証エラー通知画面データ」という）を送信する。
【００３７】
次いで、携帯端末３００は、認証装置１００のユーザー認証処理部１１０ｂからユーザー認証エラー通知画面データを受信すると、（１６）に示すように、携帯端末３００の操作パネル３１０にユーザー認証エラー通知画面３１３を表示する。
【００３８】
次いで、（１７）に示すように、認証装置１００のユーザー認証処理部１１０ｂは、画像形成装置２００にユーザー認証エラー通知を送信する。
【００３９】
次いで、画像形成装置２００は、認証装置１００からユーザー認証エラー通知を受信すると、（１８）に示すように、携帯端末３００から送信されたジョブ実行要求通知に格納されているジョブをキャンセルする。
【００４０】
次に、パスワード設定画面３１２に設けられているランダム記号列表示エリア３１２ａとパスワード設定エリア３１２ｂについて、図４を用いて説明する。
ランダム記号列表示エリア３１２ａには、基準記号及び選択順記号列の全ての選択記号

を含む複数の記号をランダムに配列したランダムな記号列（以下、「ランダム記号列」という）が表示される。

パスワード設定エリア３１２ｂには、ユーザーだけが覚えている基準記号、並びに選択順記号列の複数の選択記号及び選択記号の順番に基づいて決定されるパスワードが設定される。図４に示すように、基準記号が「〒」であり、ランダム記号列表示エリア３１２ａに「＃」、「〒」、「♪」、「○」、「☆」、「◆」、「●」、「■」、「▼」のランダム記号列が表示され、選択順記号列の複数の選択記号及び選択記号の順番が「☆」→「●」→「♪」であるときのパスワードについて説明する。このような例では、まず、選択順記号列における最も左端の選択記号「☆」は、ランダム記号列表示エリア３１２ａのランダム記号列において基準記号「〒」から３番目の位置にあるので、パスワードの１桁目が「３」となる。次いで、選択記号「☆」の右側にある「→」が示す選択記号「●」は、基準記号「〒」から５番目の位置にあるので、パスワードの２桁目が「５」となる。次いで、選択記号「●」の右側にある「→」が示す選択記号「♪」は、基準記号「〒」から１番目の位置にあるので、パスワードの３桁目が「１」となる。従って、このように算出して決定された「３５１」がパスワードとなり、パスワード設定エリア３１２ｂに設定される。

【００４１】

次に、認証装置１００のユーザー認証処理部１１０ｂが実行するパスワード認証処理の詳細について説明する。認証装置１００のネットワーク通信部１５０が画像形成装置２００からユーザー認証要求通知を受信すると、ネットワーク通信部１５０がユーザー認証要求通知を制御部１１０に出力する。制御部１１０は、ユーザー認証要求通知を入力すると、ユーザー認証処理部１１０ｂを起動する。ユーザー認証処理部１１０ｂが起動されると、ユーザー認証処理部１１０ｂは、ユーザー認証処理を開始する。以下、ユーザー認証処理の詳細について、図５に示すフローチャートを用いてステップ順に説明する。

【００４２】

（ステップＳ１０１）

まず、ユーザー認証処理部１１０ｂは、画面データ記憶エリア１２０ａからユーザーＩＤ入力画面データを取り出し、ネットワーク通信部１５０により携帯端末３００にユーザーＩＤ入力画面データを送信する。

【００４３】

（ステップＳ１０２）

次いで、ユーザー認証処理部１１０ｂは、携帯端末３００からネットワーク通信部１５０が受信したユーザーＩＤを入力する。

【００４４】

（ステップＳ１０３）

次いで、ユーザー認証処理部１１０ｂは、画面データ記憶エリア１２０ａからパスワード設定画面データを取り出す。

【００４５】

（ステップＳ１０４）

次いで、ユーザー認証処理部１１０ｂは、ユーザー情報記憶エリア１２０ｂからユーザーＩＤに対応する基準記号と選択順記号列とを取り出し、基準記号及び選択順記号列の全ての選択記号を含むランダム記号列を作成する。このランダム記号列は、作成の度に異なる記号列となるようにする。なおランダム記号列の記号の数は予め決められており、ランダム記号列の記号の数が選択順記号列の記号の数の上限になる。

【００４６】

（ステップＳ１０５）

次いで、ユーザー認証処理部１１０ｂは、図４に示すパスワード設定画面のランダム記号列表示エリア３１２ａにランダム記号列が表示されるように、パスワード設定画面データにランダム記号列をセットする。

【００４７】

（ステップＳ１０６）
次いで、ユーザー認証処理部１１０ｂは、ネットワーク通信部１５０により携帯端末３００にパスワード設定画面データを送信する。
【００４８】
（ステップＳ１０７）
次いで、ユーザー認証処理部１１０ｂは、携帯端末３００からネットワーク通信部１５０が受信したパスワードを入力する。
【００４９】
（ステップＳ１０８）
次いで、ユーザー認証処理部１１０ｂは、基準記号、選択順記号列及びランダム記号列の記号と、選択順記号列の記号の順番からパスワードが正しく設定されているかを判断する。パスワードが正しく設定されているとき（ステップＳ１０８のＹＥＳ）は、ステップＳ１０９に進む。パスワードが正しく設定されていないとき（ステップＳ１０８のＮｏ）は、ステップＳ１１０に進む。
【００５０】
（ステップＳ１０９）
ステップＳ１０８のＹｅｓにおいて、ユーザー認証処理部１１０ｂは、画像形成装置２００にユーザー認証完了通知を送信し、ユーザー認証処理を終了する。
【００５１】
（ステップＳ１１０）
ステップＳ１０８のＮｏにおいて、ユーザー認証処理部１１０ｂは、画面データ記憶エリア１２０ａからユーザー認証エラー通知画面データを取り出し、ネットワーク通信部１５０により携帯端末３００にユーザー認証エラー通知画面データを送信する。これにより、携帯端末３００の操作パネル３１０にユーザー認証エラー通知画面３１３が表示される。
【００５２】
（ステップＳ１１１）
次いで、ユーザー認証処理部１１０ｂは、画像形成装置２００にユーザー認証エラー通知を送信し、ユーザー認証処理を終了する。
【００５３】
次に、本発明を実施するための第２の実施形態（以下、「実施形態２」という）を、図面を参照して説明する。実施形態２は、実施形態１の基準記号をランダム記号列からパスワードを決定するための基準位置（以下、「基準位置」という）に換えるものである。つまり、ユーザーは、基準記号でなく基準位置を覚える。
実施形態２の認証システムの構成は、図１に示す実施形態１の認証システム１０の構成に同じである。また、実施形態２のユーザー認証手順は、図３に示す実施形態１のユーザー認証手順に同じである。
【００５４】
次に、実施形態２の認証システム１０の認証装置１００の機能構成について、図２を用いて説明する。実施形態２の認証装置１００の機能構成は、ユーザー情報記憶エリア１２０ｂ以外は、実施形態１に同じであるので、以下、ユーザー情報記憶エリア１２０ｂについて説明する。
ユーザー情報記憶エリア１２０ｂは、ユーザー情報登録処理部１１０ａにより登録されたユーザーＩＤ、基準位置及び選択順記号列を記憶する。
【００５５】
次に、実施形態２のパスワード設定画面３１２に設けられているランダム記号列表示エリア３１２ａとパスワード設定エリア３１２ｂについて、図６を用いて説明する。
ランダム記号列表示エリア３１２ａには、選択順記号列の全ての選択記号を含む複数の記号をランダムに配列したランダム記号列が表示される。
パスワード設定エリア３１２ｂには、ユーザーだけが覚えている基準位置、並びに選択

順記号列の複数の選択記号及び選択記号の順番に基づいて決定されるパスワードが設定される。図６に示すように、基準位置が「左から３番目」であり、ランダム記号列表示エリア３１２ａに「＃」、「〒」、「♪」、「○」、「☆」、「◆」、「●」、「■」、「▼」のランダム記号列が表示され、選択順記号列の複数の選択記号及び選択記号の順番が「☆」→「●」→「♪」であるときのパスワードについて説明する。このような例では、まず、選択順記号列における最も左端の選択記号「☆」は、ランダム記号列表示エリア３１２ａのランダム記号列において「左から３番目」の基準位置にある「♪」から２番目の位置にあるので、パスワードの１桁目が「２」となる。次いで、選択記号「☆」の右側にある「→」が示す選択記号「●」は、基準位置にある「♪」から４番目の位置にあるので、パスワードの２桁目が「４」となる。次いで、選択記号「●」の右側にある「→」が示す選択記号「♪」は、基準位置の「♪」であるので、パスワードの３桁目が「０」となる。従って、このように算出して決定された「２４０」がパスワードとなり、パスワード設定エリア３１２ｂに設定される。

【００５６】

次に、実施形態２の認証装置１００のユーザー認証処理部１１０ｂが実行するパスワード認証処理の詳細について、図５に示すフローチャートを用いて説明する。実施形態２のパスワード認証処理は、ステップＳ１０４及びステップＳ１０８以外は、実施形態１に同じであるので、以下、ステップＳ１０４とステップＳ１０８について説明する。

【００５７】

（ステップＳ１０４）

次いで、ユーザー認証処理部１１０ｂは、ユーザー情報記憶エリア１２０ｂからユーザーＩＤに対応する基準位置と選択順記号列とを取り出し、基準位置の記号及び選択順記号列の全ての選択記号を含むランダム記号列を作成する。このランダム記号列は、作成の度に異なる記号列となるようにする。なおランダム記号列の記号の数は予め決められており、ランダム記号列の記号の数が選択順記号列の記号の数の上限になる。

【００５８】

（ステップＳ１０８）

次いで、ユーザー認証処理部１１０ｂは、基準位置、選択順記号列及びランダム記号列の記号と、選択順記号列の記号の順番からパスワードが正しく設定されているかを判断する。パスワードが正しく設定されているとき（ステップＳ１０８のＹＥＳ）は、ステップＳ１０９に進む。パスワードが正しく設定されていないとき（ステップＳ１０８のＮｏ）は、ステップＳ１１０に進む。

【００５９】

以上の実施形態１及び実施形態２により、表示されるランダム記号列と、ユーザーだけが覚えている基準記号又は基準位置、並びに選択順記号列の記号及びその順番とからユーザーがパスワードを決定することで、容易にワンタイムパスワード方式を実現することができる。また、このようなワンタイムパスワード方式により、パスワード設定エリア３１２ｂに設定されるワンタイムパスワードが覗き見や盗聴が行われた場合でも、このワンタイムパスワードから基準記号又は基準位置と、選択順記号列とを推測することが困難であるので、覗き見や盗聴に対して安全なワンタイムパスワードを提供できる。また、一般的なワンタイムパスワード方式においては、携帯端末３００に認証専用ソフトが必要となることがあるが、認証装置１００から携帯端末３００にユーザーＩＤ入力画面３１１、パスワード設定画面３１２、及びユーザー認証エラー通知画面３１３の画面データを送信するので、携帯端末３００に認証専用ソフトが不要となる。更に、認証装置１００と携帯端末３００との時間的な同期も不要となる。

【００６０】

なお、実施形態１及び実施形態２においては、記号を用いたが、記号に限定されず、数字、文字、画像、色又は背景色など操作パネルに表示でき、ユーザーが識別可能なあらゆる識別表示を使用することができる。例えば、ユーザーだけが覚えている基準とする識別表示（基準識別情報）を赤色、又はユーザーだけが覚えている基準位置（基準識別情報）

にある識別表示を赤色とすると、「◆」だけが赤色で、その他の識別表示が赤色以外のそれぞれが異なる色である「＃」、「〒」、「♪」、「○」、「☆」、「◆」、「●」、「■」、「▼」の複数の識別表示をランダムに配列した識別表示列（ランダム識別表示列）が表示され、複数の選択表示列及び選択表示列の順番からなる識別表示列（選択順識別表示列）が「☆」→「●」→「♪」である場合のパスワードについて説明する。このような例では、まず、選択順識別表示列における最も左端の記号「☆」は、赤色である識別表示「◆」から１番目の位置にあるので、パスワードの１桁目が「１」となる。次いで、記号「☆」の右側にある「→」が示す記号「●」は、赤色である識別表示「◆」から１番目の位置にあるので、パスワードの２桁目が「１」となる。次いで、記号「●」の右側にある「→」が示す記号「♪」は、赤色である識別表示「◆」から３番目の位置にあるので、パスワードの３桁目が「３」となる。従って、このように算出して決定された「１１３」がパスワードとなる。

【００６１】

また、実施形態１及び実施形態２においては、選択順記号列の記号の数を３文字とすることで、パスワードが３桁になる例について説明したが、これに限定されない。パスワードの桁数は、選択順記号列の記号の数と同じになり、また選択順記号列の記号の数の上限がランダム記号列の記号の数となる。従って、ランダム記号列の記号の数の範囲内でランダム記号列の記号の数を変更することで、パスワードの桁数も変更可能である。

【００６２】

また、実施形態１及び実施形態２においては、ユーザーＩＤ入力画面３１１からユーザーＩＤを入力するようにしたが、ユーザーを特定できるのであれば、ユーザーＩＤの代わりにユーザーが保持しているＩＤカードを用いることも可能である。

【００６３】

また、実施形態１及び実施形態２においては、携帯端末３００のユーザーを認証する手順について説明したが、これに限定されない。例えば、ＰＣ／ＡＴ互換機等のパソコンについても、ネットワーク５００又はインターネット７００に接続可能であれば、同様にパソコンのユーザーを認証できるので、携帯端末３００又はパソコンなどの端末（以下、「端末装置」という）のユーザーを認証できる。

【００６４】

また、実施形態１及び実施形態２においては、認証装置１００によりユーザー認証を行うが、これに限定されない。たとえば、画像形成装置２００にユーザー情報登録処理部１１０ａ、ユーザー認証処理部１１０ｂ、画面データ記憶エリア１２０ａ、及びユーザー情報記憶エリア１２０ｂを設けることで、認証装置１００を設置することなく画像形成装置２００だけでユーザー認証を行うことができる。

【００６５】

また、実施形態１及び実施形態２においては、携帯端末３００からユーザー認証が必要な操作が行われたときに、携帯端末３００の操作パネル３１０にユーザーＩＤ入力画面３１１、パスワード設定画面３１２、及びユーザー認証エラー通知画面３１３を表示するが、これに限定されない。例えば、ユーザーが認証装置１００からユーザー認証を直接行うときには、認証装置１００の操作パネル１３０にユーザーＩＤ入力画面３１１、パスワード設定画面３１２、及びユーザー認証エラー通知画面３１３を表示することも可能である。

【００６６】

このような本発明の認証装置、認証プログラム、及び認証システムは、新たな機器を設けることなくセキュリティを確保できるワンタイムパスワード方式を容易に実現することができ、またワンタイムパスワードの作成方法が推測されることを防止できる。

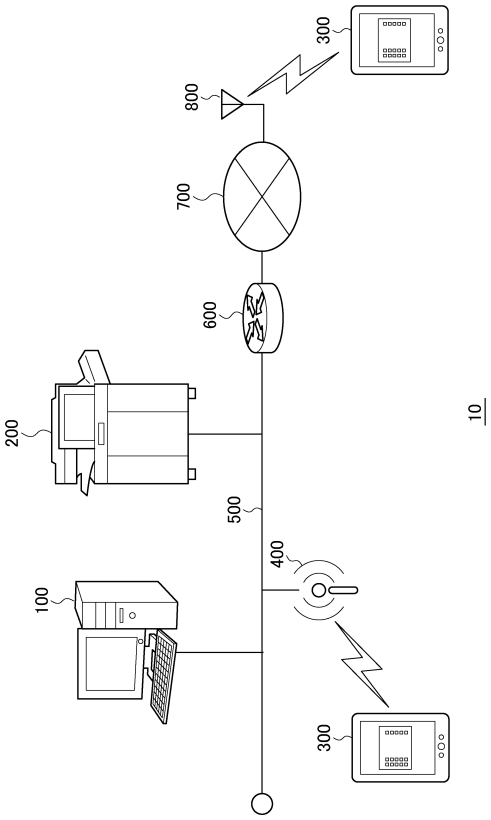
【００６７】

以上、具体的な実施の形態により本発明を説明したが、上記実施の形態は本発明の例示であり、この実施の形態に限定されないことは言うまでもない。

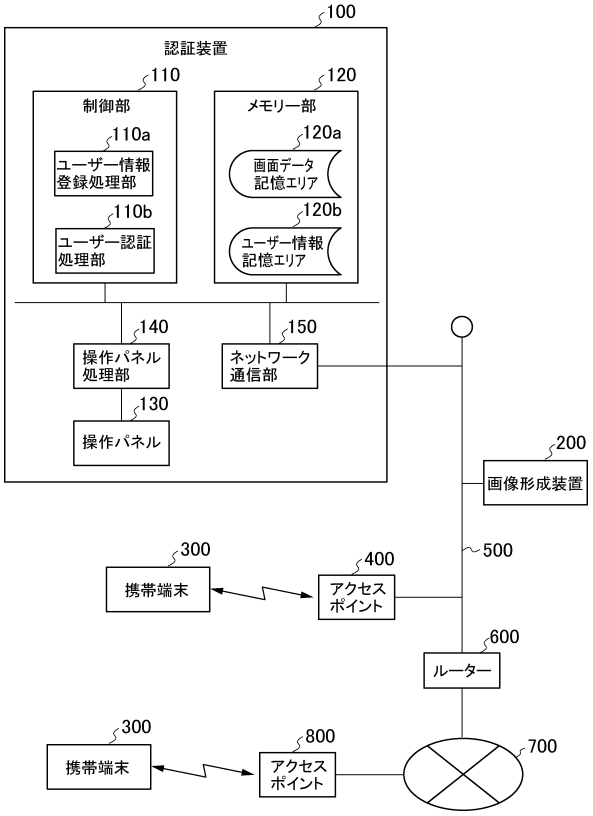
【産業上の利用可能性】

【００６８】
本発明の認証装置、認証プログラム、及び認証システムは、認証を行うあらゆる装置、認証プログラム、及び認証システムに適用できる。
【符号の説明】
【００６９】
１０・・・・・認証システム
１００・・・・・認証装置
１１０・・・・・制御部
１１０ａ・・・・ユーザー情報登録処理部
１１０ｂ・・・・ユーザー認証処理部
１２０・・・・・メモリー部
１２０ａ・・・・画面データ記憶エリア
１２０ｂ・・・・ユーザー情報記憶エリア
１３０・・・・・操作パネル
１４０・・・・・操作パネル処理部
１５０・・・・・ネットワーク通信部
２００・・・・・画像形成装置
３００・・・・・携帯端末
３１０・・・・・操作パネル
３１１・・・・・ユーザーＩＤ入力画面
３１１ａ・・・・ユーザーＩＤ入力エリア
３１２・・・・・パスワード設定画面
３１２ａ・・・・ランダム記号列表示エリア
３１２ｂ・・・・パスワード設定エリア
３１３・・・・・ユーザー認証エラー通知画面
４００・・・・・アクセスポイント
５００・・・・・ネットワーク
６００・・・・・ルーター
７００・・・・・インターネット
８００・・・・・アクセスポイント

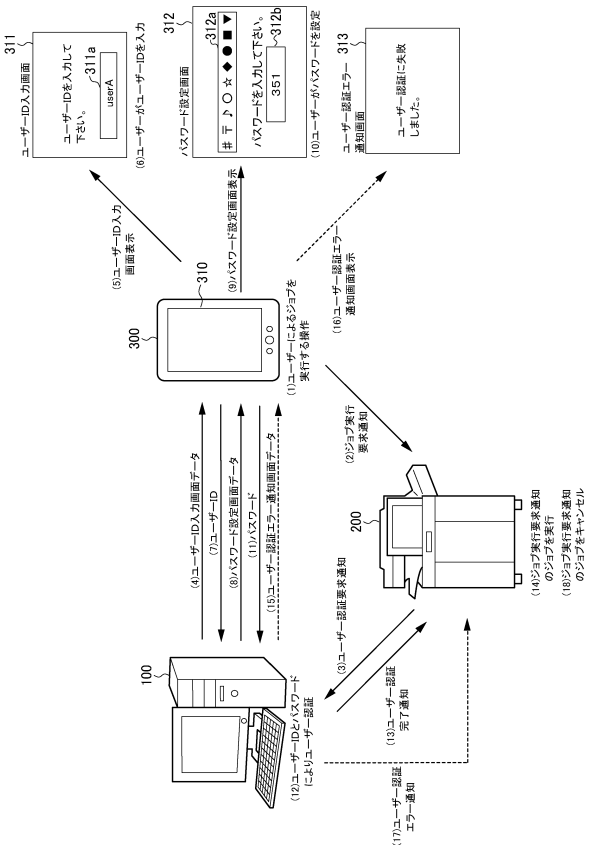
【図１】



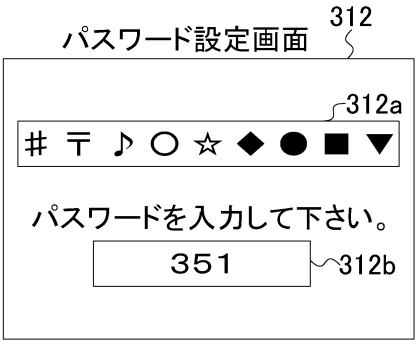
【図２】



【図３】

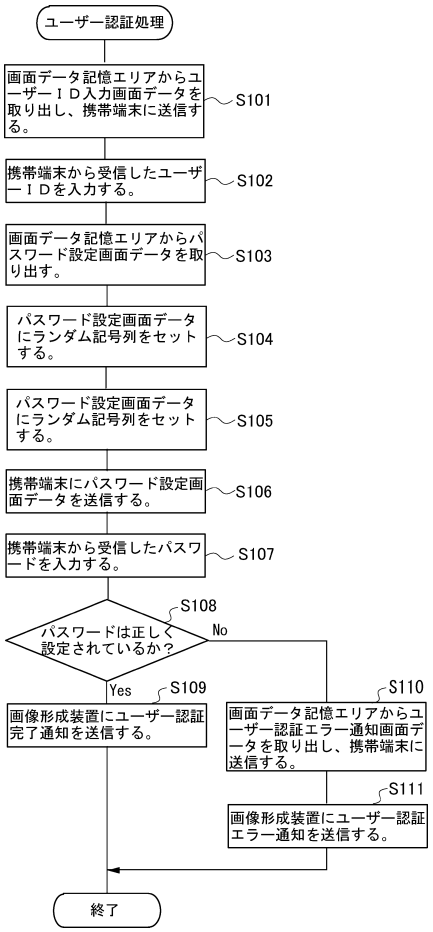


【図４】

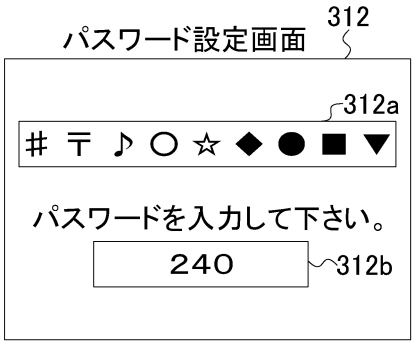


〒: 基準記号
☆ → ● → ♪:選択順記号列
☆: 基準記号から3番目の位置
●: 基準記号から5番目の位置
♪: 基準記号から1番目 の位置

【図５】



【図６】



左から3番目（♪）：基準位置
☆ → ● → ♪：選択順記号列
☆：基準位置から2番目の位置
●：基準位置から4番目の位置
♪：基準位置から0番目の位置

フロントページの続き

(72)発明者　小若　真
大阪府大阪市中央区玉造１丁目２番２８号　京セラドキュメントソリューションズ株式会社内

審査官　金木　陽一

(56)参考文献　特開２００７－１６４６５６（ＪＰ，Ａ）
特開２００９－２８９０３０（ＪＰ，Ａ）
特開２０１１－１４１４０（ＪＰ，Ａ）
特開２０１１－２０９８３５（ＪＰ，Ａ）
米国特許出願公開第２０１３／００４７２３６（ＵＳ，Ａ１）
米国特許出願公開第２０１６／００７０９０１（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３６
Ｇ０６Ｆ　　１／００
Ｇ０６Ｆ　２１／３１
Ｈ０４Ｌ　　９／３２