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

特許第5045317号
(P5045317)

(45)発行日　平成24年10月10日(2012.10.10)　(24)登録日　平成24年7月27日(2012.7.27)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 21/20 136
G09C 1/00 (2006.01)　　G06F 21/20 142
　　G09C 1/00 640E

請求項の数 3　(全 13 頁)

(21)出願番号　特願2007-226901 (P2007-226901)
(22)出願日　平成19年8月31日 (2007.8.31)
(65)公開番号　特開2009-59235 (P2009-59235A)
(43)公開日　平成21年3月19日 (2009.3.19)
審査請求日　平成22年4月27日 (2010.4.27)

(73)特許権者　504155293
国立大学法人島根大学
島根県松江市西川津町１０６０
(74)代理人　100081673
弁理士　河野　誠
(74)代理人　100141483
弁理士　河野　生吾
(72)発明者　六井　淳
島根県松江市西川津町１０６０　国立大学法人島根大学内

審査官　▲吉▼田　耕一

最終頁に続く

(54)【発明の名称】ユーザ認証システム

(57)【特許請求の範囲】
【請求項１】
各成分が図柄又は文字からなるｍ行×ｎ列の認証マトリックス（Ｃ）に関するデータをユーザ毎に記憶部（７）に記憶し、該認証マトリックス（Ｃ）に基づいてユーザの認証を行うユーザ認証システムにおいて、認証要求をしたユーザの認証マトリックス（Ｃ）からランダムにｋ行ｌ列目の成分を選択する要素選択手段（２２）と、ｍ行×ｎ行のマス目からなる選択表（Ｓ）及び要素選択手段（２２）により選択した認証マトリックス（Ｃ）のｋ行ｌ列目の図柄又は文字をユーザ側の認証画面（４）に表示する表示手段（２３）と、該表示手段（２３）によって認証画面（４）に表示された図柄又は文字が認証マトリックス（Ｃ）のどの行のどの列に位置するかを認証画面（４）に表示された前記選択表（Ｓ）の対応するマス目をタッチ又はクリックすることにより回答する回答手段（２４）と、回答手段（２４）による回答が認証マトリックス（Ｃ）と照合して正しいか否かを判定する判定手段（２６）とを備え、判定手段（２６）の判定結果に基づいてユーザ認証を行うユーザ認証システム。
【請求項２】
記憶部（７）にユーザ毎に配置パターンキーを記憶し、該配置パターンキーから行列を生成するパターン生成手段（１２）を介して認証マトリックス（Ｃ）を生成する請求項１のユーザ認証システム。
【請求項３】
パターン生成手段（１２）が配置パターンキーからユーザマトリックス（Ｕ）を生成し

、該ユーザマトリックス（Ｕ）をそのまま認証マトリックス（Ｃ）として用いるか、９０度回転させて認証マトリックス（Ｃ）として用いるか、１８０度回転させて認証マトリックス（Ｃ）として用いるか、２７０度回転させて認証マトリックス（Ｃ）として用いるかをランダムに選択する方向選択手段（１９）と、該方向選択手段（１９）による選択結果によりユーザマトリックス（Ｕ）から認証マトリックス（Ｃ）を生成する認証マトリックス生成手段（２１）とを設け、表示手段（２３）が方向選択手段（１９）による選択結果を認証要求ユーザのみに分かる形態で認証画面（４）に表示する請求項１又は２のユーザ認証システム。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、ホストコンピュータにネットワークを介してユーザ端末からアクセスする際の本人確認のため、オペレーティングシステムにログインする際の本人確認のため等に用いられるユーザ認証システムに関する。

【背景技術】

【０００２】

ユーザ認証システムとしては、予め登録されたユーザＩＤ及びパスワードと入力されたユーザＩＤ及びパスワードとの照合を行うことにより本人確認を行うものが広く普及しているが、ユーザ端末からネットワークを介してホストコンピュータにユーザＩＤ及びパスワードを送る場合、ネットワークがハッキングされるとユーザＩＤ及びパスワードに関する情報が他人に盗まれてしまい、他人が本人になりすましてユーザ認証を行うことが可能になり、セキュリティの面で問題がある。くわえて、オペレーティングシステムへのログインに用いられるユーザ認証システムにおいても、キーボードの入力履歴が漏洩すること等により同様の問題が懸念される。

【０００３】

上記問題を改善するため、ｍ行×ｎ列のマトリックスからなる乱数表からランダムに複数の成分を選択し、各成分の数字をユーザに問合せ、ユーザは手元に所持しているカードに記載された上記乱数表に基づいて各成分の数字を入力することにより上記問合せに対して回答し、入力された各数字を上記乱数表と照合することにより、ユーザ認証を行う特許文献１に示すユーザ認証システムが公知となっている。このユーザ認証システムによれば、問合せに対する回答のために入力する数値は乱数表の一部であり、この情報だけでは他人が本人になりすましてユーザ認証を行うのは困難であるため、高いセキュリティが確保できる。

【０００４】

また、使い捨てパスワードであるワンタイムパスワードを使用したユーザ認証システムが公知となっている。このユーザ認証システムによれば、所定条件によりパスワードが変更されるため、高いセキュリティが確保できる。

【特許文献１】特開平８－１２３７５９号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかし、特許文献１のユーザ認証システムは、乱数表の成分内容が問い合わされる度にカードを参照して問い合わせ成分の数字を入力する作業が必要になるため、認証に手間がかかり、利便性が低いという課題がある。また、ワンタイムパスワードを使用したユーザ認証システムも、頻繁にパスワードが変更されるのでパスワードを覚えることが困難であり、利便性が低く、課題が残る。

本発明は、上記課題を解決し、セキュリティの高さと利便性の高さとを両立したユーザ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】

上記課題を解決するため本発明のユーザ認証システムは、第１に各成分が図柄又は文字からなるｍ行×ｎ列の認証マトリックスＣに関するデータをユーザ毎に記憶部７に記憶し、該認証マトリックスＣに基づいてユーザの認証を行うユーザ認証システムにおいて、認証要求をしたユーザの認証マトリックスＣからランダムにｋ行ｌ列目の成分を選択する要素選択手段２２と、ｍ行×ｎ行のマス目からなる選択表Ｓ及び要素選択手段２２により選択した認証マトリックスＣのｋ行ｌ列目の図柄又は文字をユーザ側の認証画面４に表示する表示手段２３と、該表示手段２３によって認証画面４に表示された図柄又は文字が認証マトリックスＣのどの行のどの列に位置するかを認証画面４に表示された選択表Ｓの対応するマス目をタッチ又はクリックすることにより回答する回答手段２４と、回答手段２４による回答が認証マトリックスＣと照合して正しいか否かを判定する判定手段２６とを備え、判定手段２６の判定結果に基づいてユーザ認証を行うことを特徴としている。

【０００７】

第２に、記憶部７にユーザ毎に配置パターンキーを記憶し、該配置パターンキーから行列を生成するパターン生成手段１２を介して認証マトリックスＣを生成することを特徴としている。

【０００８】

第３に、パターン生成手段１２が配置パターンキーからユーザマトリックスＵを生成し、該ユーザマトリックスＵをそのまま認証マトリックスＣとして用いるか、９０度回転させて認証マトリックスＣとして用いるか、１８０度回転させて認証マトリックスＣとして用いるか、２７０度回転させて認証マトリックスＣとして用いるかをランダムに選択する方向選択手段１９と、該方向選択手段１９による選択結果によりユーザマトリックスＵから認証マトリックスＣを生成する認証マトリックス生成手段２１とを設け、表示手段２３が方向選択手段１９による選択結果を認証要求ユーザのみに分かる形態で認証画面４に表示することを特徴としている。

【発明の効果】

【０００９】

以上のように構成される本発明のユーザ認証システムによれば、認証画面に表示される図柄又は文字に基づいて認証画面に表示された選択表の対応するマス目をクリック又はタッチすることによりユーザ認証を行うため、数字を入力する手間が省かれるとともに、感覚的な操作が可能であり、コンピュータに不馴れなユーザでも容易にユーザ認証を行うことができる。くわえて、回答手段により回答するのは認証マトリックスの一部であるため、１回のユーザ認証のためにやり取りされる情報が漏洩したのみでは他人が本人になりすましてユーザ認証を行うことは困難である。このようにして、高いセキュリティと高い利便性とを両立することが可能になる。

【００１０】

また、配置パターンキーから行列を生成するパターン生成手段を介して認証マトリックスを生成することにより、配置パターンキーがハッキング等で他人に盗まれた場合でもパターン生成手段に関するアルゴリズムが他人に知られない限り認証マトリックスを生成することができないため、高いセキュリティが確保される。

【００１１】

さらに、ユーザマトリックスに方向に関する情報を付加して認証マトリックスを生成することにより、より高いセキュリティを確保することが可能になる。

【発明を実施するための最良の形態】

【００１２】

以下図示する例に基づき、本発明の実施形態について説明する。

図１は、本発明を適用したユーザ認証システムの概略を示す説明図である。まず、ホストコンピュータ１にアクセスするためにユーザ端末２からホストコンピュータ１に認証要求を行うと、ホストコンピュータ１からユーザ端末２にパスワード認証画面３が出力表示される。なお、ユーザ端末は２、ユーザインターフェイスとして、図示しないディスプレイ、マウス及びキーボードを備えている。

【００１３】
図２に示すように、ユーザがパスワード認証画面３のユーザＩＤ欄３ａにユーザＩＤ「ｓｕｚｕｋｉ」を、パスワード欄３ｂにパスワード「＃ａｈ＠６７」を入力し、ログインボタン３ｃをクリックすると、ホストコンピュータ１にユーザＩＤ及びパスワードが送信される。受信したユーザＩＤ及びパスワードがホストコンピュータ１に予め登録されているユーザＩＤ及びパスワードと一致すると（図５参照）、パスワード認証処理が完了され、パターン認証処理に移行する。
【００１４】
パターン認証処理が開始されると、まず、ホストコンピュータ１側で認証を要求しているユーザの乱数表Ｕ（ユーザマトリックス）が生成される。この乱数表Ｕは５行×５列のマトリックスによって構成され、各成分に「１」から「２５」までの２５種類の数字が重複しないように配置されている。ホストコンピュータ１は、上記乱数表Ｕを生成するとともに、ユーザ端末２にパターン認証画面４（認証画面）を出力表示する。
【００１５】
パターン認証画面４には、図３に示すように、選択欄４ａと、方向表示欄４ｂと、要素内容表示欄４ｃとが表示される。同図の例では、選択欄４ａに後述する認証マトリックスＣと同一行×同一列（５行×５列）のマス目からなる選択表Ｓが、方向表示欄４ｂに緑色の矢印が、要素内容表示欄４ｃに「１７」の数字が表示されている。
【００１６】
ユーザは各自、認証カード６を所持している。図４に示すように、認証カード６には、上記乱数表Ｕが記載され、この乱数表Ｕの上側に上矢印A_Uが、下側に下矢印A_Dが、左側に左矢印A_Lが、右側に右矢印A_Rがそれぞれ記載されている。４つの矢印A_U，A_D，A_L，A_Rはそれぞれ異なる色の矢印である。同図の例では、上矢印A_Uの色が赤、下矢印A_Dの色が紫、左矢印A_Lの色が青、右矢印A_Rの色が緑に塗られている。なお、４つの矢印A_U，A_D，A_L，A_Rの配色パターンはユーザ毎に異なっている。
【００１７】
乱数表Ｕの各マス目には同じ数字が４つ記載されている。４つの数字中、１つは上矢印A_Uと同一色で同一方向を向いた数字であり、１つは下矢印A_Dと同一色で同一方向を向いた数字であり、１つは左矢印A_Lと同一色で同一方向を向いた数字であり、１つは右矢印A_Rと同一色で同一方向を向いた数字である。
【００１８】
ユーザは、図３に示すパターン認証画面４に緑色の矢印が表示されているので、図４（Ａ）に示す認証カード６の乱数表Ｕの右矢印A_L（緑色の矢印）が上向きになるように、認証カード６の乱数表Ｕを回転させる。すなわち乱数表Ｕを９０度回転（反時計回りに９０度回転）させる。この際、緑色の数字を各成分とするマトリックスがユーザ認証に用いる認証マトリックスＣになる。同図の例では、認証マトリックスＣが、以下の表列式で表される。
【００１９】
【数１】

$$C=\begin{pmatrix}10 & 6 & 16 & 25 & 18\\ 12 & 9 & 20 & 4 & 22\\ 3 & 21 & 2 & 17 & 13\\ 14 & 5 & 23 & 8 & 24\\ 7 & 19 & 11 & 1 & 15\end{pmatrix}$$

【００２０】
すなわち、上記４つの矢印A_U，A_D，A_L，A_Rの配色パターンは認証要求ユーザに乱数表Ｕから認証マトリックスＣを生成させるための情報を示唆するものである。認証カード６に記載された上矢印A_Uがパターン認証画面４の方向表示欄４ｂに表示されている

と乱数表Ｕがそのまま認証マトリックスＣになり、認証カード６の下矢印$Ａ_{D}$がパターン認証画面４の方向表示欄４ｂに表示されていると下矢印$Ａ_{D}$が上を向くように乱数表Ｕを反時計回りに１８０度回転させた行列が認証マトリックスＣになり、認証カード６の左矢印$Ａ_{L}$がパターン認証画面４の方向表示欄４ｂに表示されていると左矢印$Ａ_{L}$が上を向くように乱数表Ｕを反時計回りに２７０度回転させた行列が認証マトリックスＣになり、認証カード６の右矢印$Ａ_{R}$がパターン認証画面４の方向表示欄４ｂに表示されていると、右矢印$Ａ_{R}$が上を向くように乱数表Ｕを反時計回りに９０度回転させた行列が認証マトリックスＣになる。

【００２１】

ちなみに、認証要求ユーザ以外の他人は、図４（Ａ）に示す認証カード６を所持していないので、パターン認証画面４の方向表示欄４ｂに表示された緑色の矢印が上矢印$Ａ_{U}$と、下矢印$Ａ_{D}$と、左矢印$Ａ_{L}$と、右矢印$Ａ_{R}$との何れであるかの識別ができないので、乱数表Ｕが知られた場合でも、その乱数表Ｕから認証マトリックスＣを生成することができない。

【００２２】

そして、ユーザは要素内容表示欄４ｃの数字「１７」が認証マトリックスＣのどの行のどの列に配置されているかを確認する。上記例では、「１７」の数字が上記認証マトリックスＣの３行４列目に配置されているため、パターン認証画面４の選択欄４ａに表示された選択表Ｓの３行４列目のマス目$Ｓ_{3\ 4}$をマウスでクリックすると、正しい回答になる。なお、ユーザ端末２がタッチパネル方式のインターフェイスを備えている場合には、マス目$Ｓ_{3\ 4}$をタッチしてもよい。

【００２３】

上記認証処理（ホストコンピュータ１からユーザ端末２へのパターン認証画面４の出力表示→　ユーザが認証カード６から要素表示欄４ｃの数字が認証マトリックスＣのどの行のどの列に配置されているかを確認→　パターン認証画面４の選択表Ｓの対応するマス目をクリック）を８回繰り返し、全ての認証処理においてクリックした選択表Ｓのマス目が正しいことが確認されると、ホストコンピュータ１が認証成功処理を行い、パターン認証処理が終了し、これにともない認証要求ユーザに対する全てのユーザ認証処理が完了する。なお、認証成功処理がされると、ユーザ端末２からホストコンピュータ１へアクセスが許可される。

【００２４】

次に、上記ユーザ認証処理を行うためのユーザ認証システムの構成について詳述する。

図５は、本発明を適用したユーザ認証システムの構成を示すブロック図であり、図６は、パターン認証システム、パターン生成手段及び入出力部の詳細な構成を示したブロック図である。本ユーザ認証システムは、記憶部７と、パスワード認証処理を行うパスワード認証システム８と、パターン認証処理を行うパターン認証システム９と、ユーザ端末２との情報のやり取りを行う入出力部１１と、パターン生成手段１２とを備えている。

【００２５】

上記記憶部７は、ユーザに関する各種情報が登録されたユーザテーブル１３をデータベーステーブルと有している。ユーザテーブル１３は、フィールドとして、少なくとも、ユーザＩＤと、パスワードと、配置パターンキーと、示唆パターンキーとを有している。

【００２６】

上記パターン生成手段１２は、配置パターン生成１４と示唆パターン生成１６とにより構成されている。配置パターン生成１４は、認証要求ユーザの配置パターンキーに基づき、ユーザマトリックスである５行×５列の乱数表Ｕを生成する。示唆パターン生成１６は、認証要求ユーザの示唆パターンキーに基づき、前述した４つの矢印$Ａ_{U}$，$Ａ_{D}$，$Ａ_{L}$，$Ａ_{R}$の配色パターンを生成する。

【００２７】

各ユーザの乱数表Ｕは、各成分内容が「１」～「２５」までの２５種類の数字の何れかになり且つ各成分内容が重複しないように構成されている。すなわち、各乱数表Ｕに含ま

れる数字は、「１」～「２５」までの２５個の数字で、全て共通であり、この２５個の数字の配置パターンがユーザ毎に異なっている。

【００２８】

例えば、図５に示すユーザテーブル１３に登録されたユーザＩＤ「ｓｕｚｕｋｉ」の配置パターンキーから、パターン生成手段１２の配置パターン生成１４により、図４（Ａ）に示す乱数表Ｕが生成される。

【００２９】

このようにすることにより、配置パターンキー及び配置パターン生成１４のアルゴリズムをシンプルに構成することが可能になり、そのアルゴリズムの作成、変更も容易になる。このため、ホストコンピュータ１毎に配置パターン生成アルゴリズムを変更することも容易にできるようになる。

【００３０】

なお、本ユーザ認証システムでは、ユーザマトリックスＵの成分内容として、「１」～「２５」までの２５種類の数字を用いるが、ユーザマトリクスＵの要素数（本実施例では５×５で２５個の要素数）と同数種類の図柄又は文字（例えば、「@」、「＃」、「Ａ」，「Ｂ」，「Ｃ」等）を用意し、これをユーザマトリックスＵの成分内容として用いてもよい。

【００３１】

また、本ユーザ認証システムでは、ユーザマトリクスＵとして５行×５列の行列を用いるが、ｍ（２以上の自然数）行×ｎ（２以上の自然数）行の行列をユーザマトリックスＵとして用いてもよい。

【００３２】

各ユーザの矢印A_U，A_D，A_L，A_Rの配色パターンは、前述したように認証要求ユーザに乱数表Ｕから認証マトリックスＣを生成させるための情報を示唆するものであり、上記４つの矢印A_U，A_D，A_L，A_Rの色をＨＴＭＬの標準１６色（ｂｌａｃｋ，ｗｈｉｔｅ，ｇｒａｙ，ｓｉｌｖｅｒ，ｒｅｄ，ｆｕｃｈｓｉａ，ｎａｖｙ，ｂｌｕｅ，ａｑｕａ，ｔｅａｌ，ｇｒｅｅｎ，ｌｉｍｅ，ｏｌｉｖｅ，ｙｅｌｌｏｗ，ｍａｒｏｏｎ，ｐｕｒｐｌｅ）からそれぞれ重複しないように選ぶ。

【００３３】

例えば、図５に示すユーザテーブルに登録されたユーザＩＤ「ｓｕｚｕｋｉ」の示唆パターンキーから、パターン生成手段１２の示唆パターン生成１６により、図４（Ａ）に示すように上矢印A_Uが「赤」、下矢印A_Dが「紫」、左矢印A_Lが「青」、右矢印A_Rが「緑」に配色される。

【００３４】

なお、配色に用いる色は、最低４種類用意する必要があり、１６種類以上に増加させることができる。配色に用いる色を少なくすると、示唆パターンキー及び示唆パターン生成アルゴリズムをシンプルに構成することが可能になる一方で、配色に用いる色を多くすると、示唆パターンキー及び示唆パターン生成アルゴリズムは複雑になるが、セキュリティ強度が向上する。ちなみに、配色に用いる色を増やした場合でも、認証を受けるユーザ側の手間は変わらないため、ユーザ側の利便性は維持される。

【００３５】

また、本ユーザ認証システムでは、認証要求ユーザに乱数表Ｕから認証マトリックスＣを生成させるための情報を示唆する手段として、４つの矢印A_U，A_D，A_L，A_Rの配色パターンを用いたが、４つの各矢印A_U，A_D，A_L，A_Rがある位置に種類の異なる４つの図柄又は文字（例えば、「○」、「×」、「△」、「□」）等をそれぞれ配置して、認証要求ユーザに乱数表Ｕから認証マトリックスＣを生成させるための情報を示唆するようにしてもよい。この場合には、図柄又は文字のパターン情報を、示唆パターンキーに含ませるようにする。

【００３６】

上記パスワード認証システム８は、入出力部１１を介して送られてくるユーザＩＤ及び

パスワードをユーザテーブル１３に登録されたユーザＩＤ及びパスワードと照合し、両者が一致していると、パスワード認証処理を完了させ、パターン認証システム９に処理を移行させる。

【００３７】

例えば、図２に示すように、パスワード認証画面３において入力されたユーザＩＤ「ｓｕｚｕｋｉ」及びパスワード「＃ａｈ＠６７」は、ユーザテーブル１３に登録されているユーザＩＤ「ｓｕｚｕｋｉ」及びパスワード「＃ａｈ＠６７」と一致しているので、パスワード認証処理が完了され、処理がパターン認証システムに移行される。

【００３８】

上記パターン認証システム９は、パターン生成手段１２に生成させた認証要求ユーザの乱数表Ｕ及び示唆パターンを取得する取得手段１７と、データを一時的に記憶させるデータ保持手段１８と、方向選択手段１９と、方向選択手段１９の選択結果に基づいて乱数表Ｕから認証マトリックスＣを生成する認証マトリックス生成手段２１と、乱数表Ｕを構成する成分（本実施例では２５個の構成要素）からランダムに１個を選択する要素選択手段２２とを備えている。

【００３９】

方向選択手段１９によって、乱数表Ｕをそのまま認証マトリックスＣとして用いるか、９０度回転させて認証マトリックスＣとして用いるか、１８０度回転させて認証マトリックスＣとして用いるか、２７０度回転させて認証マトリックスＣとして用いるかがランダムに選択される。

【００４０】

要素選択手段２２は、１以上ｍ（認証マトリックスＣの行の数に対応し、本実施例では５）以下の自然数からランダムに１個の自然数ｋを選択するとともに、１以上ｎ（認証マトリックスＣの列の数に対応し、本実施例では５）以下の自然数からランダムに１個の自然数ｌを選択する。そして、認証マトリックスにおけるｋ行目ｌ列の成分が要素選択手段２２により選択された成分（要素）となる。

【００４１】

データ保持手段１８は、取得手段１７により取得した認証要求ユーザの乱数表Ｕ及び示唆パターンと、方向選択手段１９の選択結果と、認証マトリックス生成手段２１により生成された認証マトリックスＣと、要素選択手段２２の選択結果と、後述する回答手段による回答を一時的に記憶して保持するように構成されている。

【００４２】

上記入力出部１１は表示手段２３と回答手段２４とを備えている。表示手段２３は、データ保持手段１８に保持された認証マトリックスＣ、方向選択手段１９の選択結果及び要素選択手段２２の選択結果に関する情報に基づいて、図３に示すパターン認証画面４を認証要求ユーザ側に出力表示するように構成されている。具体的には、パターン認証画面４の選択欄４ａに認証マトリックスＣと同一行×同一列（５行×５列）のマス目からなる選択表Ｓを、要素内容表示欄４ｃに要素選択手段２２により選択した認証マトリックスＣの成分内容（ｋ行ｌ列目の成分内容）を、方向表示欄４ｂに認証要求ユーザの示唆パターン及び方向選択手段１９の選択結果に基づいた色の矢印をそれぞれ出力表示する。

【００４３】

回答手段２４は、パターン認証画面４の選択表Ｓがマウスでクリックされたかの検知と、選択表Ｓのどの列のどの行のマス目がマウスでクリックされたかの検知とを行い、この検出結果をパターン認証システム９に送る。なお、タッチパネル方向式のユーザインターフェイスを備えている場合には、選択表Ｓ内がタッチされたか否かの検知と、選択表Ｓのどの行のどの列のマス目がタッチされたかの検知も行う。

【００４４】

パターン認証システム９は回答手段２４から送られてくる上記検知結果を回答として受け取り、その回答がデータ保持手段に一時的に保持される。パターン認証システム９には、前述したものにくわえて、判定手段２６及び認証処理手段２７が設けられている。判定

手段２６は、データ保持手段によって保持された上記各回答に関する情報を読み込み、各回答についてクリック又はタッチされた選択表Ｓのマス目の行（ｉ）及び列（ｊ）を抽出する。そして、各回答について、認証マトリックスＣにおけるｉ行ｊ列目の成分と、要素選択手段２２により選択された認証マトリックスのｋ行ｌ列目の成分とが一致するか否かの判定（ｉ＝ｋ且つｊ＝ｌの判定又は$C_{ij}=C_{kl}$の判定）を行い、一致すればその回答が正しい旨の判定がされ、一致しなければその回答が誤りである旨の判定がされる。

【００４５】

認証処理手段２７は、判定手段２６による判定結果を反映させて、アクセス許可、アクセス拒否、ログイン、ログイン拒否、認証成功画面表示、認証エラー画面表示等の認証処理を行う。

【００４６】

図７は、パターン認証処理の処理フロー図である。パターン認証処理が開始されると、まずステップＳ１に進む。ステップＳ１では、取得手段１７により認証要求ユーザの乱数表Ｕの取得が行われ、ステップＳ２に進む。ステップＳ２では、整数ｐに０の値を代入し、ステップＳ３に進む。ステップＳ３では、整数ｐが８以上であるか否かの検出が行われ、ｋが８よりも小さいと、ステップＳ４に進む。

【００４７】

ステップＳ４では、方向選択手段１９によるランダム選択が行われ、ステップＳ５に進む。ステップＳ５では、方向選択手段１９の選択結果に基づいて認証マトリックス生成手段２１により認証要求ユーザの認証マトリックスＣが生成され、ステップＳ６に進む。ステップＳ６では、要素選択手段２２によるランダム選択が行われ、ステップＳ７に進む。ステップＳ７では表示手段２３によりパターン認証画面４がユーザ側に出力表示され、ステップＳ８に進む。

【００４８】

ステップＳ８では、パターン認証画面４の選択表Ｓ内がクリック又はタッチされたか否かを検知することにより、ユーザ側から回答があったか否かの検出を行う。ユーザ側からの回答がある場合にはステップＳ９に進み、ユーザ側からの回答がない場合にはステップＳ８の処理を再び繰り返す。すなわち、ユーザ側からの回答があるまで、ステップＳ８の処理が繰り返される。ステップＳ９では、整数ｐに「１」の値を加算してステップＳ３に処理を戻す。

【００４９】

そして、ステップＳ３→ステップＳ４→・・・→ステップＳ８→ステップＳ９の処理を再び繰り返す。ステップＳ３において、整数ｐの値が８以上であることが検出されると、ステップＳ１０に進む。すなわち、ユーザ側のパターン認証画面４が８回表示され、そのそれぞれに対して回答手段による回答がされ、その８回分の回答がデータ保持手段に保持される。ステップＳ１０では、データ保持手段に保持された８回分の各回答が正しいか否かを判定手段２６により判定する。そして、８回分全ての回答が正しい場合にのみステップＳ１１に進み、１回分でも誤りがあるとステップＳ１２に進む。

【００５０】

ステップＳ１１では、認証処理手段によりユーザ端末２からアクセス許可、ログイン、ユーザ側への認証成功画面の出力表示等の認証成功処理が行われ、パターン認証処理が終了する。テップＳ１２では、認証処理手段２７によりログイン拒否、ユーザ端末２からホストコンピュータ１へのアクセス拒否、ユーザ側への認証エラー画面表示の出力表示等の認証失敗処理が行われ、パターン認証処理が終了する。

【００５１】

このように、本ユーザ認証システムは、ユーザが回答手段２４によって回答する度に判定手段２６による判定結果をユーザに示唆するのではなく、回答手段２４による回答を複数個まとめてデータ保持手段１８に保持し、後でこの複数個の各回答についてまとめ正誤判断を行い、複数個の回答が全て正しい場合にのみユーザ認証成功処理を行う。このため、ユーザ認証処理が失敗した場合に、複数個の回答のどれが誤りであるかを知ることがで

きないため、セキュリティ強度が向上する。

【００５２】

なお、ステップＳ３→ステップＳ４→・・・→ステップＳ８→ステップＳ９の処理回数は、ステップ３の「８」の値を増減させることにより、変更可能である。これによって、セキュリティ強度を自由に選択できる。なお、最低限度のセキュリティを確保することを考えると、上記処理を複数回行うことが望ましい。一方、パターン認証処理時の情報漏洩の危険性を加味すると、上記処理回数の上限は乱数表Ｕの要素数の３分の１程度とすることが好ましい。

【００５３】

図８は、本ユーザ認証システムが適用されたホストコンピュータの構成を示すブロック図である。ホストコンピュータ１は、一般の汎用コンピュータ（ＰＣ／ＡＴ互換機）であり、中央電算装置２８（ＣＰＵ）と、ランダムアクセスメモリ２９（メモリ）と、ハードディスク３１と、マウスやキーボードやディスプレイ等のユーザインターフェイス３２と、ネットワークインターフェイス３３とを備えおり、メモリ２９上に展開されるオペレーティングシステム３４によって各種アプリケーションが制御される。

【００５４】

ハードディスク３１は前述の記憶部７を有し、オペレーティングシステム３４からユーザテーブル１３へのアクセスが可能になっている。ネットワークインターフェイス３３はユーザネットワーク３６に接続されており、このユーザネットワーク３６を介してユーザ端末２からホストコンピュータ１にアクセス可能になっている。

【００５５】

上記オペレーティングシステム３４によって、前述したパスワード認証システム８及びパターン認証システム９が実装されたユーザ認証アプリケーション３７と、パターン生成手段１２が実装されたパターン生成アプリケーション３８と、ユーザネットワーク３６に接続された上記ユーザ端末２に対して入出力部１１を構成するウェブサーバ３９とが制御される。

【００５６】

なお、ホストコンピュータ１のユーザインターフェイス３２によっても、ユーザ認証システム９の入出力部１１が構成され、ホストコンピュータ１のディスプレイに前述のパスワード認証画面３及びパターン認証画面４等のユーザ認証画面を出力表示することが可能である。すなわち、本ユーザ認証システムは、ネットワークを介して認証形態の他、オペレーティングシステム３４へのログイン処理やコンピュータの起動認証処理等、本人確認が必要とされる様々なシステムに適用可能である。

【００５７】

以上のように構成される本ユーザ認証システムによれば、ユーザテーブル１３が他人に盗まれた場合でも、配置パターン生成アルゴリズムや示唆パターン生成アルゴリズムが他人に漏洩しない限り、他人が本人になりすまして、ユーザ認証を受けることができないため、高いセキュリティが確保できる。

【００５８】

くわえて、配置パターン生成アルゴリズムはシンプルなものであるため、システム管理者等が容易に作成、変更が可能であり、本ユーザ認証システムを備えた各ホストコンピュータ１で異なる配置パターン生成アルゴリズムを搭載することも可能である。このため、セキュリティ強度はさらに高まる。

【００５９】

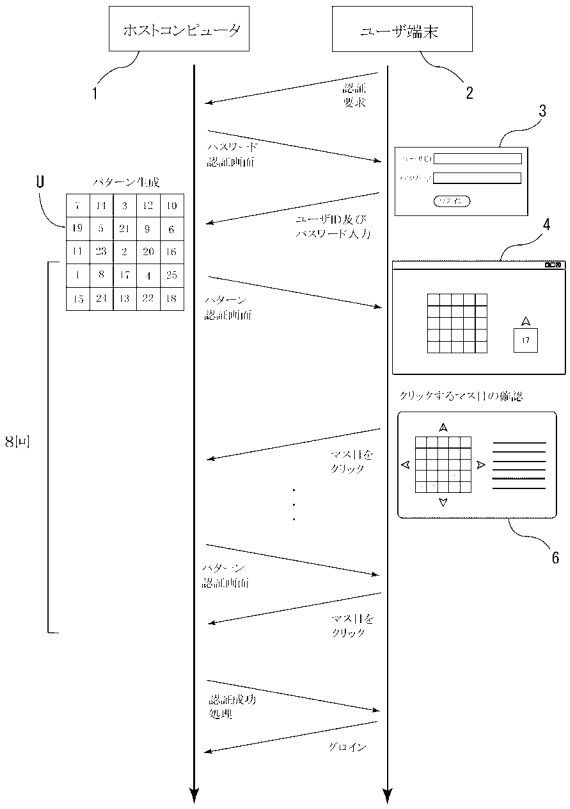
また、ユーザマトリックスＵの行数や列数を適宜変更することにより、そのシステムに適したセキュリティ強度が選択できるため、利便性も高い。

【００６０】

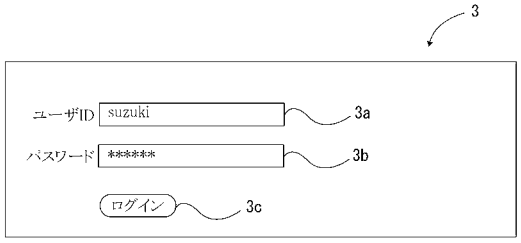
さらに、認証カード６に示される４つの矢印A_U，A_D，A_L，A_Rの配色に用いる色の種類を増減させることによってもセキュリティ強度を自由に変更できるため、メリットが大きい。

【図面の簡単な説明】
【００６１】
【図１】本発明を適用したユーザ認証システムの説明図である。
【図２】パスワード認証画面の説明図である。
【図３】パターン認証画面の説明図である。
【図４】（Ａ）は認証カードの説明図であり、（Ｂ）は認証カードに記載された乱数表の各マスの説明図である。
【図５】本発明を適用したユーザ認証システムの構成を示すブロック図である。
【図６】パターンパターン認証システム、パターン生成手段及び入出力部の詳細な構成を示したブロック図である。
【図７】パターン認証処理の処理フロー図である。
【図８】本ユーザ認証システムが適用されたホストコンピュータの構成を示すブロック図である。
【符号の説明】
【００６２】
４　パターン認証画面（認証画面）
７　記憶部
１２　パターン生成手段
１９　方向選択手段
２１　認証マトリックス生成手段
２２　要素選択手段
２３　表示手段
２４　回答手段
２６　判定手段
Ｃ　認証マトリックス
Ｓ　選択表
Ｕ　ユーザマトリックス（乱数表）

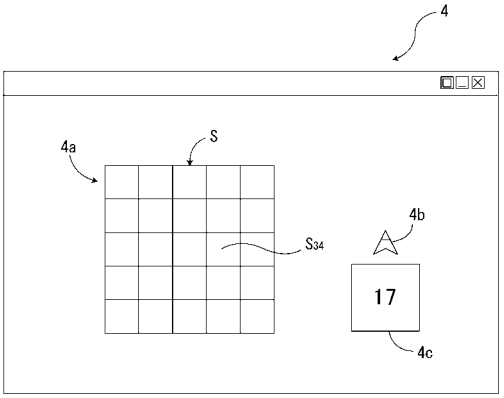
【図１】


ホストコンピュータ
ユーザ端末
1
2
認証要求
パスワード認証画面
3
ユーザID及びパスワード入力
パターン認証画面
4
パターン生成
U
7 14 3 12 10
19 5 21 9 6
11 23 2 20 16
1 8 17 4 25
15 24 13 22 18
8[回]
クリックするマス目の確認
マス目をクリック
6
パターン認証画面
マス目をクリック
認証成功処理
ログイン

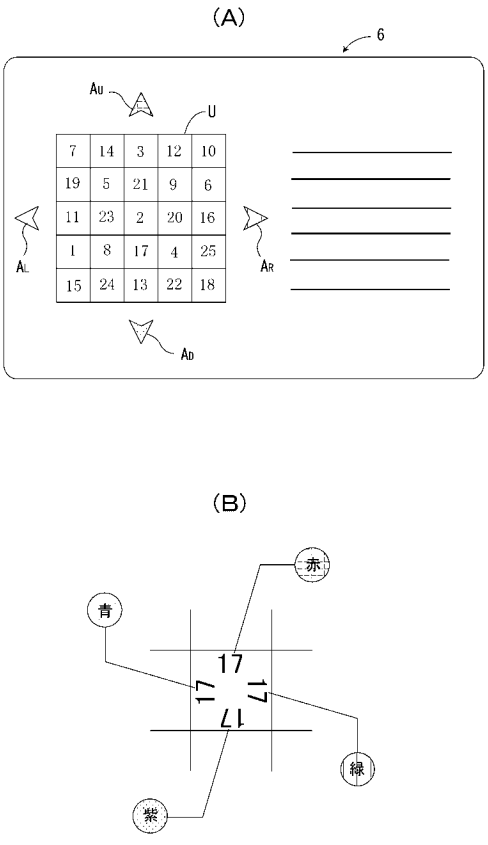
【図２】


3
ユーザID
suzuki
3a
パスワード
*****
3b
ログイン
3c

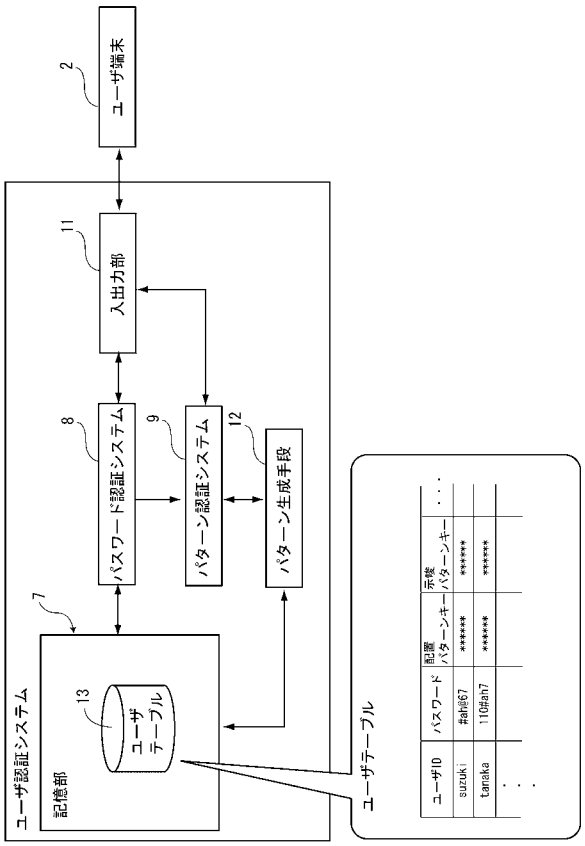
【図３】


4
4a
S
S34
4b
17
4c

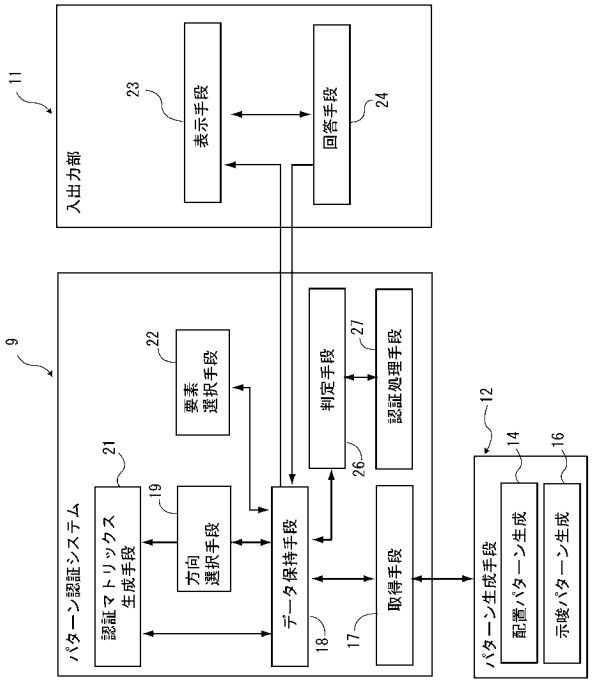
【図４】


(A)
6
AU
U
7 14 3 12 10
19 5 21 9 6
11 23 2 20 16
1 8 17 4 25
15 24 13 22 18
AL
AR
AD
(B)
赤
青
緑
紫
17
17
17
17

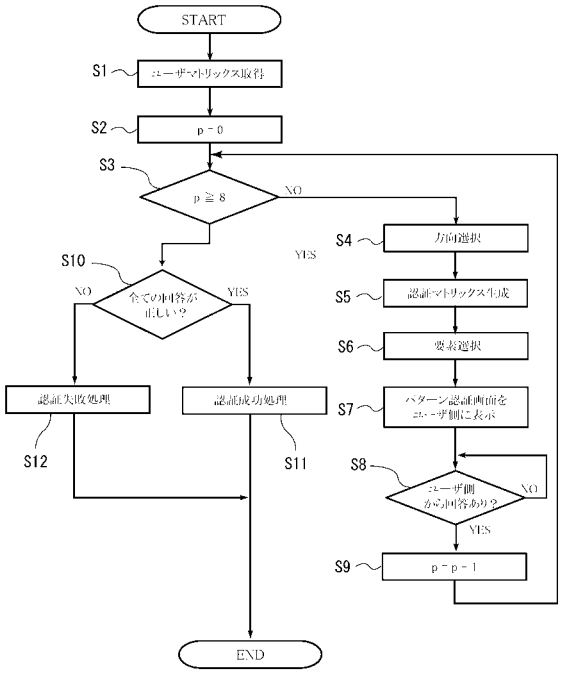
【図５】


2
ユーザ端末
11
入出力部
8
パスワード認証システム
9
パターン認証システム
12
パターン生成手段
7
ユーザ認証システム
記憶部
13
ユーザテーブル
ユーザテーブル
ユーザID
パスワード
配置パターンキー
示唆パターンキー
suzuki
#ahe67
******
******
tanaka
110@an7
******
******

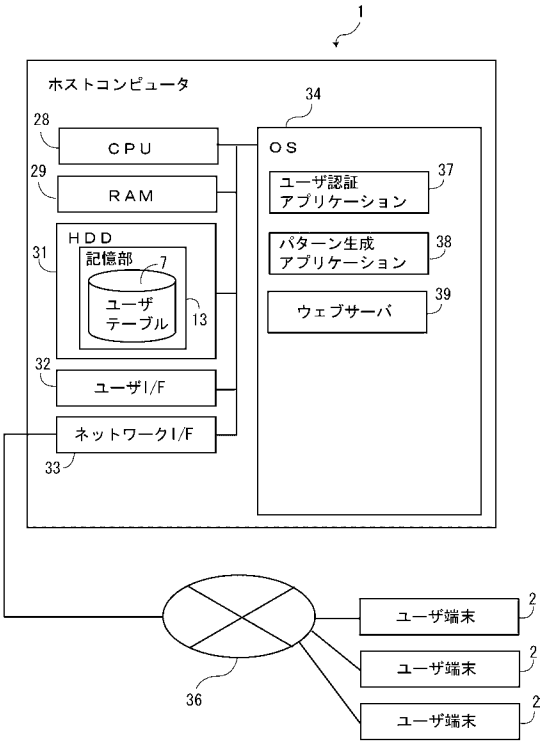
【図６】


11
入出力部
23
表示手段
24
回答手段
9
パターン認証システム
22
要素選択手段
27
判定手段
認証処理手段
12
21
19
認証マトリックス生成手段
方向選択手段
データ保持手段
26
取得手段
14
16
パターン生成手段
配置パターン生成
示唆パターン生成
18
17

【図７】


START
S1
ユーザマトリックス取得
S2
p－0
S3
p ≧ 8
NO
YES
S4
方向選択
S5
認証マトリックス生成
S6
要素選択
S7
パターン認証画面をユーザ側に表示
S8
ユーザ側から回答あり?
NO
YES
S9
p－p－1
S10
全ての回答が正しい?
NO
YES
認証失敗処理
S12
認証成功処理
S11
END

【図８】


1
ホストコンピュータ
34
28
CPU
OS
29
RAM
ユーザ認証アプリケーション
37
パターン生成アプリケーション
38
HDD
31
記憶部
7
ユーザテーブル
13
ウェブサーバ
39
32
ユーザI/F
ネットワークI/F
33
36
ユーザ端末
2
ユーザ端末
2
ユーザ端末
2

フロントページの続き

(56)参考文献 特開平０９－３０５５４１（ＪＰ，Ａ）
特開２００６－０３９６７９（ＪＰ，Ａ）
特開２００７－００４４０１（ＪＰ，Ａ）
特開２００４－００５６０５（ＪＰ，Ａ）
特開２００４－１０２４６０（ＪＰ，Ａ）
特開平０８－１２３７５９（ＪＰ，Ａ）
特開２００６－１９５７１６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２０
Ｇ０９Ｃ １／００