

明 細 書

発明の名称：

ユーザ認証システム、ユーザ認証サーバ、およびユーザ認証方法

技術分野

[0001] 本発明はユーザ認証システムに関し、より詳しくは、所定パターンに配列した複数のパターン要素を認証を受けるユーザに提示パターンとして提示し、当該提示パターンに含まれる特定の位置のパターン要素に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールを当該ユーザのパスワードとするユーザ認証システムに関する。

背景技術

[0002] 従来のチャレンジ・レスポンス方式の問題を改善したユーザ認証方式として、いわゆるマトリクス認証（登録商標）方式のユーザ認証システムが使用されるようになってきた（例えば、特許文献1参照）。マトリクス認証においては、乱数を所定パターンに配列したマトリクス形状の提示パターンを認証を受けようとするユーザに提示し、当該提示パターンに含まれるパターン要素（それぞれの乱数の数字）に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールが当該ユーザのパスワードとされる。そして、サーバとクライアントで同じ提示パターンを共有し、クライアントにおいてパスワードであるワンタイムパスワード導出ルールを提示パターンに適用した結果であるワンタイムパスワードと、サーバにおいてパスワードであるワンタイムパスワード導出ルールを提示パターンに適用した結果である検証コードとを比較することによって、パスワードを直接比較することなく、ユーザ認証が実施される。マトリクス認証においては、パスワードであるワンタイムパスワード導出ルールは、マトリクス上で選択されるパターン要素の位置と順番であって、イメージとして記憶しやすいものであり、また、パスワード入力時に盗み見されてもパスワードを特定することはできないという特徴がある。

- [0003] 図3は、従来の代表的なマトリクス認証を使用したユーザ認証システム200のブロック図である（特許文献1）。ユーザ認証システム200は、大きく、ユーザの認証を行う認証サーバ201と、ユーザが認証を要求する端末である認証要求クライアント251とから構成される。認証サーバ201は、ワンタイムパスワード導出ルール記憶部202と、ユーザID受信手段203と、パターン発生手段204と、パターン送信手段205と、検証コード生成手段206と、ワンタイムパスワード受信手段207と、ユーザ認証手段208とから構成される。
- [0004] 認証要求クライアント251は、ユーザID入力手段252と、ユーザID送信手段253と、パターン受信手段254と、パターン表示手段255と、ワンタイムパスワード入力手段256と、ワンタイムパスワード送信手段257とから構成される。
- [0005] 認証サーバ201において、ワンタイムパスワード導出ルール記憶部202は、ユーザID202aおよびワンタイムパスワード導出ルール202bをお互いに関連付けてあらかじめ記憶している。ユーザID受信手段203は、認証を受けようとするユーザのユーザID281を認証要求クライアント251から受信し、パターン発生手段204は、マトリクス形状の提示パターン291に含まれるパターン要素の配列であるパターン要素列290を擬似乱数などの所定の発生規則により発生させ、パターン送信手段205は、発生させられたパターン要素列290を認証要求クライアント251に送信するものである。
- [0006] 認証に当たっては、まず、認証を受けようとするユーザが、認証要求クライアント251において、キーボードなどのユーザID入力手段252から自己のユーザID281を入力する。ユーザID送信手段253が入力されたユーザID281を認証サーバ201に送信する。認証サーバ201において、ユーザID受信手段203がユーザID281を受信する。パターン発生手段204が、マトリクス形状の提示パターン291を構成する乱数を所定の発生規則により発生する。パターン送信手段205は、発生させられ

たパターン要素列 290 を認証要求クライアント 251 に送信する。認証要求クライアント 251 において、パターン受信手段 254 がパターン要素列 290 を受信する。パターン表示手段 255 が、受信したパターン要素列 290 を所定パターン 291 p に配列して提示パターン 291 を生成し、それを画面に表示させる。

[0007] 図 7 は、マトリクス認証方式におけるワンタイムパスワード入力方法の概念図である。ユーザは、提示パターン 291 に対してワンタイムパスワード導出ルール 202 b を適用することによって、マトリクス上の所定の位置に表示された数字を順番に抽出し、ワンタイムパスワード入力手段 256 から入力する。また、提示パターン 291 に無関係な数字を入力することも可能である。すなわち、固定パスワードをワンタイムパスワードに含めることもできる。それらの数字の入力は、典型的にはタッチパネルなどのポインティングデバイスやキーボード 296 などで行われる。図 7 において破線で示した矢印と丸は、提示パターン 291 に基づくワンタイムパスワードをキーボード 296 から入力することを表わしている。ワンタイムパスワード送信手段 257 は、入力されたワンタイムパスワード 292 を認証サーバ 201 に送信する。認証サーバ 201 において、ワンタイムパスワード受信手段 207 がワンタイムパスワード 292 を受信する。検証コード生成手段 206 が、受信したユーザ ID 281 に関連付けられたワンタイムパスワード導出ルール 202 b を、送信したパターン要素列 290 に適用した結果である検証コード 293 を生成する。ユーザ認証手段 208 が、受信したワンタイムパスワード 292 と、検証コード 293 とを比較し、それらが等しい場合に当該ユーザの認証を成功させる。

先行技術文献

特許文献

[0008] 特許文献 1：特開 2007-264839 号公報

発明の概要

発明が解決しようとする課題

[0009] 従来のマトリクス認証システムにおいては、まず、認証要求クライアントにおいてユーザIDの入力画面でユーザIDを入力して認証サーバに伝達した後に、認証サーバから認証要求クライアントに、マトリクス形状の提示パターンを構成するパターン要素などが送信される。そしてユーザは、提示パターンが表示されてから、その提示パターンに対するレスポンスであるワンタイムパスワードを入力する。すなわち、ユーザIDを入力した後、別の画面でワンタイムパスワードを入力する必要がある。このような、認証のために2画面を切り替えて表示させなければならない従来の認証方法は、ユーザの操作性が必ずしもいいとは言えない。これを改善するような、ユーザID入力ステップを不要とし、ワンタイムパスワード入力の1ステップのみでユーザIDの識別と認証の両方を同時に行なうシステムの必要性が存在していた。

課題を解決するための手段

[0010] 本発明は上記の課題に鑑みてなされたものであり、以下のような特徴を有している。すなわち本発明は、所定パターンに配列した複数のパターン要素を認証を受けるユーザに提示パターンとして提示したときの特定の位置のパターン要素に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールを前記ユーザのパスワードとし、前記ワンタイムパスワード内の所定の埋込位置にユーザIDを埋め込んだ認証用文字列に基づいて前記ユーザの認証を行う、認証サーバと認証要求クライアントとを含むユーザ認証システムにおいて、

前記認証サーバは、

それぞれの前記ユーザID毎に、前記ユーザのユーザID 102 a と、前記ユーザのワンタイムパスワード導出ルール 102 b と、前記ユーザIDを前記ワンタイムパスワード内に埋め込む埋込位置を識別するユーザID埋込位置 102 c をお互いに関連付けてあらかじめ記憶するパスワード記憶部 102 と、

前記提示パターンを決定する提示パターン決定情報を所定の発生規則により発生する提示パターン決定情報発生手段 111 と、

それぞれの前記ユーザID毎に、前記提示パターン決定情報に基づいて決定される前記提示パターンを構成する前記パターン要素に前記ユーザIDに関連付けられた前記ワнтаイムパスワード導出ルールを適用した結果に対して、前記ユーザIDを前記ユーザID埋込位置に基づいて埋め込んだ検証コードを生成する検証コード生成手段 106 と、

発生させられた前記提示パターン決定情報を、前記認証を受けるユーザの前記認証要求クライアントに送信する提示パターン決定情報送信手段 112 と、

を有し、

前記認証要求クライアントは、

前記認証サーバから送信された前記提示パターン決定情報を受信する提示パターン決定情報受信手段 161 と、

前記提示パターン決定情報に基づいて前記提示パターンを構成するパターン要素を決定するパターン要素決定手段 162 と、

決定されたそれぞれの前記パターン要素を前記所定パターンに配列して提示パターンを生成し、それを画面に表示させるパターン表示手段 155 と、

前記提示パターンに含まれる前記パターン要素に前記ワнтаイムパスワード導出ルールを適用した結果であるワнтаイムパスワードに対して、前記ユーザIDを前記ユーザID埋込位置に埋め込んだ認証用文字列の入力を前記認証を受けるユーザから受け付ける認証用文字列入力手段 156 と、

入力された前記認証用文字列を前記認証サーバに送信する認証用文字列送信手段 157 と、

を有し、

前記認証サーバは、

前記認証用文字列を前記認証要求クライアントから受信する認証用文字列受信手段 107 と、

受信した前記認証用文字列と前記ユーザID毎に生成された前記検証コードとを比較し、受信した前記認証用文字列に等しい前記検証コードが存在する場合に、その検証コードに対応する前記ユーザIDの認証を成功させるユーザ認証手段108と、
をさらに有することを特徴とする。

[0011] 本発明においては、前記提示パターン決定情報は、前記提示パターンを構成する前記パターン要素とすることができる。また本発明においては、前記提示パターン決定情報は、所定のパターン要素列生成規則に適用することにより前記提示パターンを構成する前記パターン要素を発生するパターンシード値とすることができる。また本発明においては、前記検証コード生成手段は、いずれかの2つ以上の前記ユーザIDに対して等しい前記検証コードが存在する場合は、等しい前記検証コードが存在しなくなるまで、前記提示パターン決定情報発生手段によって新しい前記提示パターン決定情報を発生させ、それに基づいてそれぞれの前記ユーザIDに対して前記検証コードを生成することを反復する、ように構成できる。また本発明においては、前記認証用文字列送信手段は、入力された前記認証用文字列を記憶するとともに、ハッシュ関数でハッシュ化して前記認証サーバに送信するものであり、

前記ユーザ認証手段は、受信したハッシュ化された前記認証用文字列と、前記ユーザID毎に生成された前記検証コードを前記ハッシュ関数でハッシュ化したものとを比較し、受信したハッシュ化された前記認証用文字列に等しいハッシュ化された前記検証コードが存在する場合に、その検証コードに対応する前記ユーザID埋込位置及び前記ユーザIDの文字列の長さを前記認証要求クライアントに送信して前記認証用文字列の中の前記ユーザIDの問い合わせを行い、前記問い合わせで得られた前記ユーザIDと前記検証コードに対応する前記ユーザIDが等しい場合に前記ユーザIDの認証を成功させるものであるようにすることもできる。

[0012] 本発明は、上記のユーザ認証システムを使用したユーザ認証方法や、そのようなユーザ認証システムを実現するための認証サーバや、そのような認証

サーバで実行されるユーザ認証方法としても成立する。

- [0013] 上記あるいは特許請求の範囲に記載の発明において、サーバ、クライアントなどの用語は、装置の具体的形態や具体的呼称を限定するものではなく、その一般的な機能を備えた装置を表わすためのものである。1つの構成要素が有する機能が2つ以上の物理的構成によって実現されてもよく、2つ以上の構成要素が有する機能が1つの物理的構成によって実現されてもよい。システムの発明は、それぞれの構成要素の有する機能が逐次的に実行される方法の発明として把握することもできるし、その逆も成り立つ。方法の発明においては、各ステップは記載された順序に実行されるものに限定されるものではなく、全体としての機能が矛盾なく実行され得る限りにおいて、自由な順序でそれを実行することができる。これらの発明は、所定のハードウェアと協働して所定の機能を実現させるプログラムとしても成立し、それを記録した記録媒体としても成立する。

発明の効果

- [0014] 本発明は、所定パターンに配列した複数のパターン要素を認証を受けるユーザに提示パターンとして提示したときの特定の位置のパターン要素に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールを前記ユーザのパスワードとし、ワンタイムパスワード内の所定の埋込位置にユーザIDを埋め込んだ認証用文字列に基づいてユーザの認証を行い、その際に、すべてのユーザIDに対して、提示している提示パターンに対する正しい認証用文字列を生成して検証コードとし、ユーザから入力された認証用文字列と等しい検証コードが存在する場合、その検証コードに対応するユーザIDのユーザ認証を成功させるという構成を採用したことにより、認証の開始時にユーザIDを認証システムに入力してユーザを特定する必要がなく、認証時に単一の認証用文字列を入力することにより、ユーザの特定とユーザの真正性の確認の両方を行うことができ、認証の際にパスワードの入力の前にユーザIDを入力する必要がなく、認証のために2画面を切り替えて表示させる必要がないという効果を有する。すなわち、

本発明は、ユーザID入力ステップが不要となり、ワンタイムパスワードを含む文字列の入力の1ステップのみでユーザIDの識別と認証の両方を同時に行なうことができるという効果を有するものである。

図面の簡単な説明

[0015] [図1]本発明の一実施形態に係るユーザ認証システム100のハードウェア構成図である。

[図2]本発明の一実施形態に係るユーザ認証システム100の機能ブロック図である。

[図3]従来のマトリクス認証方式のユーザ認証システム200のブロック図である。

[図4]本発明の一実施形態に係るユーザ認証システム100の動作フロー図である。

[図5]本発明の一実施形態に係るユーザ認証システム100の動作フロー図であり、図4に示した動作フローの続きである。

[図6]マトリクス認証方式におけるワンタイムパスワード導出ルールの概念図である。

[図7]マトリクス認証方式におけるワンタイムパスワード入力方法の概念図である。

[図8]認証用文字列の構造の説明図である。

[図9]ユーザ認証システム100におけるログオン認証画面のイメージ図である。

発明を実施するための形態

[0016] [本発明に係るユーザ認証方法]

これから図面を参照して本発明の実施形態に係るユーザ認証システム100の説明を行う。図面においては、従来のユーザ認証システム200と本発明に係るユーザ認証システム100との間に対応する構成要素に関しては、付している参照番号の下2桁は同じ番号としている。図1はハードウェア構成図、図2はブロック図、図4および5は動作フロー図である。まず、本発

明に係るユーザ認証方法の概要について説明する。本発明に係るユーザ認証方法は、上述したような、チャレンジ・レスポンス方式の認証方法の一種であるマトリクス認証である。本発明に係るユーザ認証方法では、所定パターンに配列した複数のパターン要素を認証要求クライアント 151 において認証を受けるユーザに提示パターン 191 として提示し、当該提示パターン 191 に含まれる特定の位置のパターン要素 190 に対してユーザが適用することによりワンタイムパスワード 192 を生成するためのワンタイムパスワード導出ルール 102b を当該ユーザのパスワードとするものである。認証要求クライアント 151 においてユーザに提示される提示パターン 191 を生成する際に使用される情報である提示パターン決定情報 183 は、認証サーバ 101 において生成され、認証要求クライアント 151 に送信される。提示パターン決定情報 183 は、提示パターン 191 を一意的に定める情報であり、パターン要素 190 そのものでもよく、また、所定の演算を行なうことによりパターン要素 190 を一意的に定めるパターンシード値であってもよい。

[0017] ユーザは、自分のユーザ ID 102a に対応付けられたワンタイムパスワード導出ルール 102b を提示パターン 191 に適用することによってワンタイムパスワード 192 を生成するが、それを認証要求クライアント 151 に入力する際に、ワンタイムパスワード 192 内の所定の埋込位置にユーザ ID 102a を埋め込んだ認証用文字列 192A として入力する。ユーザは、その所定の位置をあらかじめ決めており、ユーザ ID 埋込位置 102c としてユーザ ID 102a と対応付けて認証サーバ 101 に記憶させておく。ユーザ ID 102a は、ユーザを一意的に特定することができる情報であり、一般的には、ユーザが自分で設定する文字列である。ユーザ ID 102a としては、ユーザが設定した文字列以外に、マイナンバー、銀行口座番号、社員番号、会員番号、メールアドレスなどのユーザに固有の任意の情報を使用することができる。

[0018] 認証要求クライアント 151 においてユーザから入力された認証用文字列

192Aは、認証要求クライアント151から認証サーバ101に送信される。認証サーバ101は、すべてのユーザID102aに対して、認証要求クライアント151に表示させている提示パターン191にユーザID102aに対応付けられたワンタイムパスワード導出ルール102bを適用することによって正しいワンタイムパスワード192を生成し、ユーザID埋込位置102cの埋込位置にユーザID102aを埋め込むことによって検証コード193を生成しておく。そして認証サーバ101は、認証要求クライアント151から送信された認証用文字列192Aを検証コード193と比較し、それらが等しければ当該ユーザに対する認証を成功させる。

[0019] [提示パターンとパターン要素]

提示パターン191とは、パターン要素190を所定パターン191pに配列したものである。所定パターン191pとしては、縦m個×横n個のそれぞれの位置に全体が方形を形成するように配置したマトリクス、そのようなマトリクスを複数並べたもの、などが典型的であるが、その他に任意の図形の形状とすることができる。本明細書では、そのような典型的なマトリクス形状以外の形状の提示パターンを使用した場合も、マトリクス認証方式と呼ぶことにする。所定パターン191pとしては、規則的な形状や印象的な形状が、ユーザの記憶に残りやすく、従ってユーザがパスワードであるワンタイムパスワード導出ルール102bを記憶しやすいために好適である。

[0020] パターン要素190とは、提示パターン191内において所定パターン191pを構成するように所定位置に配置される要素であり、好適には0から9までの1桁の数字であるが、他に、アルファベット、記号、などの任意のキャラクターとすることができる。なお、記号としては、PCの標準のキーボードに割り当てられている「+」、「-」、「*」、「=」、「_」、「!」、「?」、「#」、「\$」、「&」などの記号が特に好適である。キャラクターとして、図形、イラスト、写真などの図柄を使用することもできる。好適には、同じパターン要素190は、提示パターン191内において、複数個表示される。このようにすると、パスワードであるワンタイムパスワ

ード導出ルール102bと、ワнтаイムパスワード導出ルール102bを提示パターン191に適用した結果であるワнтаイムパスワード192とは多対1の対応となり、ワнтаイムパスワード192の入力時に自動的に一方方向化がなされることになる。すなわち、ワнтаイムパスワード192の入力時に、自動的にハッシュ関数演算と同様の処理がなされることになり、そのため、1つのワнтаイムパスワード192だけからは、ワнтаイムパスワード導出ルール102bを特定することはできない。

[0021] 本実施例では、図7などに示すような、0から9までの1桁の数字でパターン要素190が構成されるものとし、それぞれのパターン要素190を4つの4×4のマトリクスからなる所定パターン191pに配列したものを提示パターン191とする。なお、携帯電話機などのように画面の面積が小さい場合は、4×4のマトリクスの数を3つなどに減少させた提示パターン191を使用すると好適である。

[0022] [提示パターン決定情報]

提示パターン決定情報183は、提示パターン191を生成するために所定パターン191pに配置するパターン要素190を一意的に定めることができる情報である。提示パターン決定情報183は、パターン要素190そのものを順番に並べたデータでもよく、また、所定の演算を行なうことによりパターン要素190を一意的に発生させることができるパターンシード値であってもよい。所定の演算としては、ハッシュ関数演算、加算、減算、排他的論理和、桁数調整などのあらゆる演算を使用することができる。パターンシード値は、典型的には、所定の発生規則により所定の範囲内において発生させられた定数である。

[0023] [ワнтаイムパスワード導出ルール]

ワнтаイムパスワード導出ルール102bは、提示パターン191に含まれる特定の位置のパターン要素190に対して適用することによりワнтаイムパスワード192を生成するためのルールであり、ユーザのパスワードとして機能するデータである。パターン要素190に対して適用するルールと

は、典型的には、どの位置のパターン要素 190 をどの順番で選択するのかということである。この場合、ワンタイムパスワード導出ルール 102 b は、提示パターン 191 に含まれる選択されるパターン要素 190 のそれぞれの位置と、当該それぞれのパターン要素 190 が選択される順番との組み合わせの情報である。またワンタイムパスワード導出ルール 102 b は、提示パターン 191 と無関係に入力される数字などのキャラクターの情報を固定パスワードとして含んでいてもよく、この場合、ワンタイムパスワード導出ルール 102 b は、提示パターン 191 に含まれる選択されるパターン要素 190 のそれぞれの位置および当該提示パターン 191 に無関係な固定パスワードのキャラクターのそれぞれと、当該それぞれのパターン要素 190 の位置および当該それぞれのキャラクターが選択あるいは入力される順番との組み合わせの情報である。

[0024] 図 6 に典型的なワンタイムパスワード導出ルール 102 b の構造を示す。本実施例では、0 から 9 までの 1 桁の数字でパターン要素 190 が構成されるものとし、それぞれのパターン要素 190 を 4 つの 4×4 のマトリクスからなる所定パターン 191 p のそれぞれの要素の位置に配置した提示パターン 191 に対するワンタイムパスワード導出ルール 102 b が例示されている。図 6 においては、所定パターン 191 p のそれぞれの要素の位置は、01 から 64 までの数字で区別されて表示されている。提示パターン 191 が認証を受けようとするユーザに対して表示されるときには、所定パターン 191 p のそれぞれの要素の位置には 0 から 9 までの 1 桁の数字が表示される。

[0025] ワンタイムパスワード 192 は、好適には、提示パターン 191 に基づく数字と、それとは無関係に入力される数字とを使用するものである。提示パターン 191 に含まれるパターン要素の数は 64 個であるため、提示パターン 191 に含まれるパターン要素のそれぞれの位置が選択されたことは、それぞれの位置に割り当てられた 01 から 64 までの 2 桁の数字によって表わされる。そして、提示パターン 191 とは無関係に入力される数字について

は、最初にそのような数字であることを示す「9」の数字が割り当てられ、次に入力される1桁の数字が割り当てられた、2桁の数字によって表わされる。図6の例では、ワнтаイムパスワード192の最初の4つの数字は、提示パターン191の特定の位置のパターン要素を選択することによって入力されるものである。ワнтаイムパスワード導出ルール102bのそれらに対応する部分として、それらの位置を表わす数字である「01」、「16」、「29」、「20」がその順番に配置される。選択されたパターン要素190は、キーボード196や、タッチパネルなどのポインティングデバイスによって入力される。ワнтаイムパスワード192のその次の2つの数字は、提示パターン191とは無関係に、キーボード196などから入力されるものである。ワнтаイムパスワード導出ルール102bのそれらに対応する部分として、直接入力を表わす「9」の数字の後に、入力される数字である「2」および「9」がそれぞれ付加された「92」、「99」が続いてその順番に配置される。ワнтаイムパスワード192のその次の1つの最後の数字は、提示パターン191の特定の位置のパターン要素を選択することによって入力されるものである。ワнтаイムパスワード導出ルール102bのそれらに対応する部分として、その位置を表わす数字である「33」が続いて配置され、ワнтаイムパスワード導出ルール102bはここで終了する。ワнтаイムパスワード導出ルール102bには、その終了点を一意的に特定するエンドマーク、例えば「00」などの数字をその最後にさらに付加してもよいし、あるいは、ワнтаイムパスワード導出ルール102bの全体の長さを示す数値をそれに関連付けていてもよい。

[0026] [ワнтаイムパスワード]

ワнтаイムパスワード192は、認証を受けようとするユーザが提示パターン191に対して自己のワнтаイムパスワード導出ルール102bを適用することによって生成・入力される使い捨てのパスワードである。図7は、マトリクス認証方式におけるワнтаイムパスワード入力方法の概念図である。図7において使用されているワнтаイムパスワード導出ルール102bは

、図6において示したものと同一である。ユーザは、自己のワンタイムパスワード導出ルール102bに従って、提示パターン191に含まれる所定の位置のパターン要素190の選択、および提示パターン191とは無関係な所定の数字の入力を所定の順番で実施することによって、ワンタイムパスワード192として「2504290」を生成する。

[0027] [ユーザID埋込位置と認証用文字列]

図8は、認証用文字列192Aの構造の説明図である。ワンタイムパスワード192内の所定の埋込位置にユーザID102aを埋め込むことによって認証用文字列192Aを構成するが、ユーザID埋込位置102cは、その際の埋込位置を特定する情報である。図8の例では、「2504290」というワンタイムパスワード192に対して埋込が可能な位置に0から7の数字を割り当てており、ユーザID埋込位置102cは、ワンタイムパスワード192の「5」と「0」の間の「2」（破線の三角形のシンボルで囲んだもの）で示された埋込位置である。ユーザは自分のユーザID埋込位置102cをあらかじめ決めておき、パスワード記憶部102に記憶させておく。ユーザID埋込位置102cは、ユーザが設定する情報であるため、パスワードの一部として機能することにもなる。図8の例では、ワンタイムパスワード192である「2504290」において「2」のユーザID埋込位置102cに、「USER1」というユーザID102aを埋め込むことによって、「25USER104290」という認証用文字列192Aが構成されている。このように、認証用文字列192Aは、ユーザを特定するユーザID102aの情報と、パスワードであるワンタイムパスワード導出ルール102bに従って生成されたユーザの真正性を確認するためのワンタイムパスワード192の両方の情報を単一の文字列に統合したものである。すなわち、認証用文字列192Aという単一の文字列が正当なものであることを検証することによって、どのユーザID102aのユーザが認証を受けているか、及びそのユーザの真正性が確認されることとなり、そのユーザに対する本人認証が成功したかを確認することができる。

[0028] [ユーザ認証システム100のハードウェア構成]

次に、ユーザ認証システム100の構成の説明をする。図1は、本発明の一実施形態に係るユーザ認証システム100のハードウェア構成図である。図1を参照すると、ユーザ認証システム100は、大きく、認証サーバ101と認証要求クライアント151とから構成される。認証サーバ101は、CPU101a、RAM101b、記憶装置101c、ユーザインターフェース(I/F)101d、ネットワークインターフェース(I/F)101eから構成される。記憶装置101cは、その記憶領域にOS101c1、ユーザ認証アプリケーション101c2を記憶し、またその記憶領域にパスワード記憶部102を含む。パスワード記憶部102は、ユーザID102a、ワンタイムパスワード導出ルール102b、ユーザID埋込位置102cを記憶する。認証要求クライアント151は、CPU151a、RAM151b、記憶装置151c、ユーザインターフェース(I/F)151d、ネットワークインターフェース(I/F)151eから構成される。記憶装置151cは、その記憶領域にOS151c1、ブラウザアプリケーション151c2、パターン要素生成モジュール151c3を記憶する。

[0029] 認証サーバ101は、ユーザ認証システム100において、認証要求クライアント151からのユーザ認証要求に応答して、ユーザの認証を行う構成要素である。認証サーバ101は、OS101c1、ユーザ認証アプリケーション101c2などがインストールされた、サーバとしてのコンピュータなどの形態である。また、認証サーバ101は、SSL-VPNゲートウェイのようなインターネット上に仮想専用線ネットワークを提供するためのゲートウェイ装置などにおけるユーザ認証を提供するハードウェアの形態とすることもできる。CPU101aは、ユーザ認証アプリケーション101c2などをOS101c1上で実行してユーザ認証に関する情報処理を行うプロセッサである。RAM101bは、記憶装置101cに記憶されたソフトウェアがその上に読み込まれるメモリ空間と、読み込まれたソフトウェアがCPU101aによって実行される際に必要となるワークエリア等を提供す

るメモリである。記憶装置101cは、ソフトウェアやデータなどの情報を記憶・管理する構成要素であり、典型的にはハードディスクドライブなどの形態である。記憶装置101cは、好適には、OS101c1、ユーザ認証アプリケーション101c2のプログラムのファイルを記憶しており、それらのプログラムはRAM101b上に読み出されて実行される。ユーザI/F101dは、ユーザとの間でデータの入出力を行うための構成要素であり、典型的にはキーボード196、マウスなどのポインティングデバイスからなる入力手段と、画面に情報を表示するディスプレイなどの出力手段と、それらとの間のハードウェアI/Fとから構成される。

[0030] 認証サーバ101と認証要求クライアント151とはネットワークで接続される。ネットワークは、好適には、TCP/IPベースのプロトコルで動作するインターネットあるいはイントラネットである。イントラネットにおいて、認証要求クライアント151がクライアント用Windows（登録商標。以下、同じ）OSで動作している場合には、ネットワークはTCP/IPベースのプロトコルで動作するWindowsのドメインネットワークとすることができる。なお、本明細書ではOSとしてWindowsを例示して説明しているが、他のOS、例えば、Mac OS（登録商標）、Linux（登録商標）、Unix（登録商標）などを使用することも可能である。

[0031] 本発明に係る認証方法は、少なくとも以下の2つの利用形態で実施することが可能である。1つの利用形態は、認証要求クライアント151をネットワーク上のWebサービスに接続した状態で、WebブラウザなどによってWeb上のコンテンツ、SSL-VPNサービス、アプリケーションを使用する際の、当該ユーザに対する使用許可のための認証の形態である。この場合、認証サーバ101は、典型的には、インターネットまたはイントラネットなどのネットワーク上に配置され、当該ネットワークを通じてアクセスしてきた認証要求クライアント151に対してユーザ認証のためのWebページを提供し、それを通じてユーザ認証のためのデータの送受信を行うような

Webサーバの形態や、RADIUSサーバと連携して認証・アカウント管理を実施する、SSL-VPNゲートウェイのようなインターネット上に仮想専用線ネットワークを提供する装置の形態である。

[0032] もう1つの利用形態は、ユーザが認証要求クライアント151を使用して、認証サーバ101と同じWindowsのドメインネットワークに適正なネットワークユーザとして接続する際の、当該ユーザのそのネットワークへのログオン認証の形態である。この場合、認証サーバ101は、典型的には、認証のためのリソースをネットワーク上に提供しており、それによって、ユーザからの認証要求クライアント151を使用したWindowsのドメインネットワークへのログオン認証要求に応答してユーザ認証を実行し、その認証結果を当該Windowsのドメインネットワークのネットワークユーザの権限を管理するドメインコントローラに伝達する。

[0033] OS101c1は、認証サーバ101のハードウェアに密接な基本的な情報処理を行うオペレーティングシステムである。ユーザ認証アプリケーション101c2は、OS101c1上で動作するユーザ認証のためのアプリケーションソフトウェアである。認証サーバ101がWebサーバの形態である場合、ユーザ認証アプリケーション101c2は、典型的には、CGIで呼び出される形態かサブリットの形態の認証プログラムを備えた、認証のためのWebページまたはリソースをインターネットまたはイントラネットのWeb上に提供するWebサーバプログラムである。パスワード記憶部102は、典型的にはハードディスクドライブなどの記憶装置の一領域であり、好適にはデータは暗号化ファイルとしてパスワード記憶部102に記憶される。ユーザID102aは、ユーザを一意的に識別するための文字列のデータである。ワンタイムパスワード導出ルール102bは、上述したように、提示パターン191に含まれる特定の位置のパターン要素190に対して適用することによりワンタイムパスワード192を生成するためのルールであり、ユーザのパスワードとして機能するデータである。ユーザID埋込位置102cは、ワンタイムパスワード192内にユーザID102を埋め込

むことによって認証用文字列 192A を構成するための埋込位置である。

[0034] 認証要求クライアント 151 は、ユーザ認証システム 100 において、ユーザが認証サーバ 101 に対して認証を要求する構成要素であり、OS 151c1、ブラウザアプリケーション 151c2、パターン要素生成モジュール 151c3 などがインストールされた情報端末であり、具体的には、PC、スマートフォン、携帯電話機などの形態である。CPU 151a は、ブラウザアプリケーション 151c2、パターン要素生成モジュール 151c3 などを OS 151c1 上で実行して、ユーザ認証要求に関する情報処理を行うプロセッサである。RAM 151b は、記憶装置 151c に記憶されたソフトウェアがその上に読み込まれるメモリ空間と、読み込まれたソフトウェアが CPU 151a によって実行される際に必要となるワークエリア等を提供するメモリである。記憶装置 151c は、ソフトウェアやデータなどの情報を記憶・管理する構成要素であり、典型的にはハードディスクドライブなどの形態である。記憶装置 151c は、好適には、OS 151c1、ブラウザアプリケーション 151c2、パターン要素生成モジュール 151c3 のプログラムのファイルを記憶しており、それらのプログラムは RAM 151b 上に読み出されて実行される。なお、記憶装置 151c は、OS 151c1、ブラウザアプリケーション 151c2、パターン要素生成モジュール 151c3 に関しては、そのプログラムを ROM に記憶した形態であってもよい。この場合、そのような ROM は CPU 151a などのプログラム実行要素とともにファームウェアを構成することになる。ユーザ I/F 151d は、ユーザとの間でデータの入出力を行うための構成要素であり、典型的には、図示していないが、キーボード 196 や、タッチパネルなどのポインティングデバイスからなる入力手段と、画面に情報を表示するディスプレイなどの出力手段と、それらとの間のハードウェア I/F とから構成される。ネットワーク I/F 151e は、ネットワークに接続して情報の入出力を行うための I/F である。

[0035] OS 151c1、ブラウザアプリケーション 151c2、パターン要素生

成モジュール151c3は、それらの一部または全部が組み合わされて形式的には一体のプログラムの形態となってもよい。例えば、ブラウザアプリケーション151c2がパターン要素生成モジュール151c3の機能を包含していてもよく、OS151c1がブラウザアプリケーション151c2およびパターン要素生成モジュール151c3の機能を包含していてもよい。また、それらが他のアプリケーションに組み込まれていてもよい。また、それらがそれぞれ複数のプログラムに分割されていてもよい。

[0036] OS151c1は、認証要求クライアント151のハードウェアに密接な基本的な情報処理を行うオペレーティングシステムであり、認証要求クライアント151のハードウェアに応じた基本プログラムである。OS151c1は、プラットフォームに準じたアーキテクチャのファームウェアの形態であってもよい。ブラウザアプリケーション151c2は、OS151c1上で動作する、ネットワーク上に提供されている情報にアクセスして表示させ、さらにユーザからのデータの入力を受け付けるためのブラウザの機能を実現させるソフトウェアであり、典型的には、インターネットまたはイントラネット上のWebページにアクセスするためのWebブラウザアプリケーションの形態である。なお、ブラウザアプリケーション151c2は、Webブラウザアプリケーションに限られることはなく、サーバがネットワーク上に提供するユーザ認証用の画面にアクセスすることができるアプリケーションであれば、どのようなアプリケーションであってもよい。ブラウザアプリケーション151c2は、他のアプリケーションが認証を実施する際の画面表示のためのAPIを提供するプラットフォームに準じたアーキテクチャのファームウェアの形態であってもよい。パターン要素生成モジュール151c3は、ブラウザアプリケーション151c2に組み込まれて実行される、提示パターン191を生成してブラウザに表示させるためのプログラムであり、認証要求クライアント151がPCの場合、典型的には、Java（登録商標）アプレット、ActiveX（登録商標）、Flash（登録商標）などの形態である。パターン要素生成モジュール151c3は、他のアプ

リケーションが認証を実施するためのAPIを提供するプラットフォームに準じたアーキテクチャのファームウェアの形態であってもよい。

[0037] 認証サーバ101がWindowsのドメインネットワークへのログオン認証を実施する場合には、認証のためのブラウザアプリケーション151c2およびパターン要素生成モジュール151c3は、クライアント用Windows OSとしてのOS151c1に組み込まれており、認証要求クライアント151のWindowsのドメインネットワークへのログオン認証画面に提示パターン191を表示させ、本願発明に係る認証方法に基づいた認証手順をユーザに提供する。

[0038] 図9は、ユーザ認証システム100におけるログオン認証画面197のイメージ図である。これは、Windowsのドメインネットワークへのログオンしようとする時の認証画面であってもよいし、ブラウザアプリケーション151c2によるWebサービスへログオンしようとする時の認証画面であってもよい。ログオン認証画面197には、提示パターン191、パスワード入力フィールドが表示される。キーボード196やタッチパネルなどのポインティングデバイスによって認証用文字列192Aとして数字などのキャラクターがパスワード入力フィールドに入力されると、それに応答して当該キャラクターあるいは「*」のような記号が1つずつ表示される。Windowsのドメインネットワークへのログオンの場合は、認証用文字列192Aの入力が完了すると、当該認証モジュールは、認証サーバ101に認証用文字列192Aを伝達してユーザ認証を実行させ、その認証結果をドメインコントローラに伝達する。ブラウザアプリケーション151c2によるWebベースのログオンの場合は、認証サーバ101は、使用しようとしているWebサービスに認証結果を伝達する。

[0039] [ユーザ認証システム100の機能ブロック構成]

図2は、本発明の一実施形態に係るユーザ認証システム100の機能ブロック図である。図2は、図1に示したハードウェア構成のユーザ認証システム100を、ソフトウェアとハードウェア資源とが協働して実施される情報

処理の観点から表現した図であり、当該情報処理を機能ブロックの単位で表わした図である。図2において、認証サーバ101は、パスワード記憶部102、検証コード生成手段106、認証用文字列受信手段107、ユーザ認証手段108、提示パターン決定情報発生手段111、提示パターン決定情報送信手段112から構成される。これらの機能ブロックは、ユーザ認証アプリケーション101c2がOS101c1とともに記憶装置101cからRAM101b上に読み込まれ、それらのソフトウェアがCPU101aによって実行されることによって、RAM101b、記憶装置101c、ユーザI/F101d、ネットワークI/F101eなどのハードウェア要素とも適宜協働して実現されるものである。

[0040] パスワード記憶部102は、それぞれのユーザに関して、ユーザID102aと、当該ユーザのパスワードであるワンタイムパスワード導出ルール102bと、ユーザID埋込位置102cとをお互いに関連付けてあらかじめ記憶しておくための記憶装置であり、CPU101a、RAM101b、記憶装置101cなどがソフトウェアと協働することによって実現される機能ブロックである。検証コード生成手段106は、認証を受けようとしているユーザのパスワードであるワンタイムパスワード導出ルール102bを、認証要求クライアント151に表示されている提示パターン191に適用した結果にユーザID102aをユーザID埋込位置102cで示される位置に埋め込んだものである検証コード193を生成する構成要素であり、CPU101a、RAM101bなどがソフトウェアと協働することによって実現される機能ブロックである。ここで、検証コード193は、正しいワンタイムパスワード導出ルール102bが正しい提示パターンに適用された結果である正しいワンタイムパスワード192にユーザID102aを正しいユーザID埋込位置102cで示される位置に埋め込んだ場合の認証用文字列192Aと同じ値である。認証用文字列受信手段107は、認証要求クライアント151から、そこで入力された認証用文字列192Aを受信する構成要素であり、CPU101a、RAM101b、ネットワークI/F101

eなどがソフトウェアと協働することによって実現される機能ブロックである。ユーザ認証手段108は、認証用文字列192Aと検証コード193とを比較して、それらが等しいときにユーザ認証を成功させる構成要素であり、CPU101a、RAM101bなどがソフトウェアと協働することによって実現される機能ブロックである。提示パターン決定情報発生手段111は、提示パターンを規定する情報である提示パターン決定情報183を所定の発生規則により発生する構成要素であり、CPU101a、RAM101bなどがソフトウェアと協働することによって実現される機能ブロックである。提示パターン決定情報送信手段112は、提示パターン決定情報発生手段111によって発生させられた提示パターン決定情報183を認証要求クライアント151に送信する構成要素であり、CPU101a、RAM101b、ネットワークI/F101eなどがソフトウェアと協働することによって実現される機能ブロックである。

[0041] 認証要求クライアント151は、パターン表示手段155、認証用文字列入力手段156、認証用文字列送信手段157、提示パターン決定情報受信手段161、パターン要素決定手段162から構成される。これらの機能ブロックは、ブラウザアプリケーション151c2の必要部分、パターン要素生成モジュール151c3がOS151c1の必要部分とともに記憶装置151cからRAM151b上に読み込まれ、それらのソフトウェアがCPU151aによって実行されることによって、RAM151b、記憶装置151c、ユーザI/F151d、ネットワークI/F151eなどのハードウェア要素とも適宜協働して実現されるものである。

[0042] パターン表示手段155は、後述のパターン要素決定手段162によって決定されたパターン要素190を所定パターン191pに配列して提示パターン191を生成し、それを画面に表示させる構成要素であり、CPU151a、RAM151b、ユーザI/F151dなどがソフトウェアと協働することによって実現される機能ブロックである。認証用文字列入力手段156は、画面に表示させた提示パターン191などを通じて認証用文字列19

2 Aのユーザからの入力を受け付ける構成要素であり、CPU 151 a、RAM 151 b、ユーザ I/F 151 dなどがソフトウェアと協働することによって実現される機能ブロックである。認証用文字列送信手段 157 は、入力された認証用文字列 192 Aを認証サーバ 101に送信する構成要素であり、CPU 151 a、RAM 151 b、ネットワーク I/F 151 eなどがソフトウェアと協働することによって実現される機能ブロックである。提示パターン決定情報受信手段 161 は、認証サーバ 101から、提示パターン決定情報 183を受信する構成要素であり、CPU 151 a、RAM 151 b、ネットワーク I/F 151 eなどがソフトウェアと協働することによって実現される機能ブロックである。パターン要素決定手段 162 は、認証サーバ 101から受信した提示パターン決定情報 183に基づいて、パターン要素 190を決定する構成要素であり、CPU 151 a、RAM 151 bなどがソフトウェアと協働することによって実現される機能ブロックである。

[0043] [ユーザ認証システム 100の動作]

これから、ユーザ認証システム 100の動作について説明する。図4および図5は、ユーザ認証システム 100の動作フロー図である。まず、ユーザ認証システム 100で認証を受けることになるユーザは、そのユーザ ID 102 aと、パスワードであるワンタイムパスワード導出ルール 102 bと、ユーザ ID埋込位置 102 cとをあらかじめ認証サーバ 101に入力して登録しておく。パスワード記憶部 102 は、そのユーザのユーザ ID 102 aとワンタイムパスワード導出ルール 102 bとユーザ ID埋込位置 102 cとをお互いに関連付けてユーザの認証に先立ってあらかじめ記憶する（ステップ S101）。

[0044] 次に、認証を受けようとするユーザは、認証要求クライアント 151において、WindowsへのログオンやWebサービスへログオンのために、ログオン認証画面 197を表示させる。この際には、認証要求クライアント 151から認証要求が認証サーバ 101に送られ（ステップ S102）、認証サーバ 101が認証要求を受信して（ステップ S103）、認証のための

プロセスを開始する。認証サーバ101は、まず、提示パターン決定情報発生手段111によって、提示パターン決定情報183を発生し、それによって提示パターン191を構成するパターン要素190を発生する（ステップS104）。すなわち、認証サーバ101は、パターン要素190そのもの、あるいは、所定の演算を行なうことによりパターン要素190を一意的に決定するパターンシード値を乱数などで発生させ、パターン要素190、及びそれを所定パターン191pに配列した提示パターン191を発生させる。

[0045] 認証サーバ101は、検証コード生成手段106によって、すべての登録されているユーザID102aのそれぞれに対して、発生させた提示パターン決定情報183に基づいて生成される提示パターン191に、そのユーザID102aに関連付けられたワンタイムパスワード導出ルール102bを適用した結果（正しいワンタイムパスワード192に相当する）に、そのユーザID102aに関連付けられたユーザID埋込位置102cにユーザID102aを埋め込むことによって検証コード193（正しい認証用文字列192Aに相当する）を生成する（ステップS105）。この検証コード193と比較することによって、認証の際に正しい認証用文字列192Aが認証要求クライアント151から送られてきたかどうかを確認することができる。

[0046] ここで、認証用文字列192A内に埋め込まれるユーザID102aの内容やその埋込位置によっては、ある提示パターン191に対する正しい認証用文字列192Aが等しいようなユーザID102aが複数存在するような衝突が発生する可能性がある。この場合、認証用文字列192Aが正当なものであること、すなわち、認証用文字列192Aと同じ検証コード193が存在することが確認できても、それらのユーザID102aを区別することはできず、ユーザを一意的に特定することができない。

[0047] 上述のような不都合を防止するために、好適には、認証サーバ101は、検証コード生成手段106によって、異なるユーザID102aに対して等

しい検証コード193が存在するかどうかを確認する（ステップS106）。そして、いずれかの2つ以上のユーザID102aに対して等しい検証コード193が存在する場合は、衝突が発生していると判断し、ステップS104にプロセスを戻して新しい提示パターン決定情報183（すなわち、新しいパターン要素190で構成される新しい提示パターン191）を発生させ、次のステップS105で新しい検証コード193を生成させ、次のステップS106でその検証コード193を有するユーザID102aが複数存在するかどうかを確認する。このような確認を、異なるユーザID102aに対して等しい検証コード193が存在しなくなるまで実行する。これを実行することにより、すべてのユーザID102aに対して異なる検証コード193が存在することが保証されることとなり、検証コード193による認証用文字列192Aの確認により、ユーザの特定と、そのユーザの真正性の確認とを同時に行うことができるようになる。

[0048] なお、別の方法により、すべてのユーザID102aに対して確実に異なる検証コード193が存在するようにしていれば、ステップS106は必ずしも必要ない。例えば、すべてのユーザに対して、ユーザID埋込位置102cを同じ位置とし、また、ユーザID102aの文字列の長さを同じにすると、認証用文字列192A内の同じ位置にユーザID102aが現れることになるため、すべてのユーザID102aに対して必ず異なる検証コード193が存在することになる。

[0049] 認証サーバ101は、提示パターン決定情報送信手段112によって、提示パターン決定情報183を認証要求クライアント151に送信する（ステップS107）。認証要求クライアント151は、提示パターン決定情報受信手段161によって、認証サーバ101から提示パターン決定情報183を受信する（ステップS108）。認証要求クライアント151は、パターン要素決定手段162によって、受信した提示パターン決定情報183に基づいて、パターン要素190を決定する（ステップS109）。すなわち、パターン要素決定手段162は、提示パターン決定情報183がパターン要素

190そのもの場合は、受信した提示パターン決定情報183をパターン要素190とし、提示パターン決定情報183がパターンシード値の場合は、それに所定の演算を行なうことによりパターン要素190を生成する。認証要求クライアント151は、パターン表示手段155によって、生成したパターン要素190を所定パターン191p（典型的には、4つの4×4のマトリクスからなるパターン）に配列して提示パターン191を構成し、それをログオン認証画面197に含めて画面に表示させる（ステップS110）。

[0050] 次に、認証を受けようとするユーザは、認証要求クライアント151の画面に表示された提示パターン191の特定の位置に表示されたパターン要素を選択したり、提示パターン191とは無関係な数字などのキャラクターを入力したりすることを順番に実施することによって、自分のワンタイムパスワード導出ルール102bを提示パターン191に適用した結果であるワンタイムパスワード192を生成し、ワンタイムパスワード192内の予め定めたユーザID埋込位置102cに自己のユーザID102aを含めることによって認証用文字列192Aを生成し、認証要求クライアント151に入力する。すなわち、認証要求クライアント151は、認証用文字列入力手段156によって、認証用文字列192Aの入力を受け付ける（ステップS111）。次に、認証要求クライアント151は、認証用文字列送信手段157によって、入力された認証用文字列192Aを認証サーバ101に送信する（ステップS112）。次に、認証サーバ101は、認証用文字列受信手段107によって、認証要求クライアント151から送信された認証用文字列192Aを受信する（ステップS113）。

[0051] 次に、認証サーバ101は、ユーザ認証手段108によって、受信した認証用文字列192Aと等しい検証コード193が存在するかを、それぞれのユーザID102aに対して生成された検証コード193と順番に比較することによって確認し、等しい検証コード193が存在していれば、その検証コード193に対応するユーザID102aのユーザが真正のユーザである

ことが確認できたことになり、ユーザ認証を成功させる（ステップS 1 1 4）。ユーザ認証が成功すると、以下のように、そのユーザID 1 0 2 aのユーザに対して、ユーザ認証の利用形態に応じたサービスを許可することになる。すなわち、Web上のコンテンツ等の使用許可のためのユーザ認証の場合は、コンテンツへのアクセスが許可されたり、アプリケーションの利用が許可されたりする。Windowsのドメインネットワークへのログオン認証の場合は、認証サーバ1 0 1は、認証結果をWindowsのドメインコントローラに伝達し、Windowsネットワークへの参加を許可させる。認証サーバ1 0 1が、SSL-VPNゲートウェイの形態であれば、当該SSL-VPNへのアクセスが許可される。

[0052] なお、本発明において送受信するデータは、適宜ハッシュ化することによって、さらにセキュリティを高めることもできる。すなわち、認証要求クライアント1 5 1は、入力された認証用文字列1 9 2 Aを一時的に記憶するとともに、それをハッシュ関数でハッシュ化したものを認証サーバ1 0 1に送信するようにできる。そして、認証サーバ1 0 1は、受信したハッシュ化された認証用文字列1 9 2 Aと、ユーザID 1 0 2 a毎に生成された検証コード1 9 3のそれぞれをハッシュ関数でハッシュ化したものとを比較する。認証サーバ1 0 1は、受信したハッシュ化された認証用文字列1 9 2 Aに等しいハッシュ化された検証コード1 9 3が存在する場合に、当該ユーザID 1 0 2 aに対するユーザ認証を成功させることができる。ただし、この場合、ハッシュ化したもの同士を比較しているため、衝突により、認証用文字列1 9 2 Aと検証コード1 9 3が異なる場合であっても、ハッシュ化されたもの同士が等しくなる可能性がゼロではない。そのような可能性をなくすために、以下のような手順を追加的に実行することもできる。すなわち、その検証コード1 9 3に対応するユーザID 1 0 2 aに関連付けられたユーザID埋込位置1 0 2 c及び前記ユーザID 1 0 2 aの文字列の長さを認証要求クライアント1 5 1に送信して、認証用文字列1 9 2 Aの中のユーザID 1 0 2 aの問い合わせを行う。認証要求クライアント1 5 1は、それらの情報を受

信し、一時的に記憶している入力された認証用文字列 1 9 2 A 内のユーザ I D 埋込位置 1 0 2 c から、送信された文字列の長さ分の文字列を抽出して、認証サーバ 1 0 1 に送る。この文字列は正しいユーザ I D 1 0 2 a に相当するはずのものである。認証サーバ 1 0 1 は、問い合わせで得られた文字列が、検証コード 1 9 3 に対応するユーザ I D 1 0 2 a に等しい場合に、そのユーザ I D 1 0 2 a の認証を成功させる。

[0053] なお、以上に説明した動作フローにおいて、あるステップにおいて、そのステップではまだ利用することができないはずのデータを利用しているなどの動作フロー上の矛盾が生じない限りにおいて、動作フローを自由に変更することができる。

[0054] 以上に説明してきた各実施形態は、本発明を説明するための例示であり、本発明はこれらの実施形態に限定されるものではない。本発明は、その要旨を逸脱しない限り、種々の形態で実施することができる。

符号の説明

- [0055] 1 0 0 : ユーザ認証システム
1 0 1 : 認証サーバ
1 0 1 a : C P U
1 0 1 b : R A M
1 0 1 c : 記憶装置
1 0 1 c 2 : ユーザ認証アプリケーション
1 0 1 d : ユーザ I / F
1 0 1 e : ネットワーク I / F
1 0 2 : パスワード記憶部
1 0 2 a : ユーザ I D
1 0 2 b : ワンタイムパスワード導出ルール
1 0 2 c : ユーザ I D 埋込位置
1 0 6 : 検証コード生成手段
1 0 7 : 認証用文字列受信手段

1 0 8	: ユーザ認証手段
1 1 1	: 提示パターン決定情報発生手段
1 1 2	: 提示パターン決定情報送信手段
1 5 1	: 認証要求クライアント
1 5 1 a	: C P U
1 5 1 b	: R A M
1 5 1 c	: 記憶装置
1 5 1 c 2	: ブラウザアプリケーション
1 5 1 c 3	: パターン要素生成モジュール
1 5 1 d	: ユーザ I / F
1 5 1 e	: ネットワーク I / F
1 5 5	: パターン表示手段
1 5 6	: 認証用文字列入力手段
1 5 7	: 認証用文字列送信手段
1 6 1	: 提示パターン決定情報受信手段
1 6 2	: パターン要素決定手段
1 8 3	: 提示パターン決定情報
1 9 0	: パターン要素
1 9 1	: 提示パターン
1 9 1 p	: 所定パターン
1 9 2	: ワンタイムパスワード
1 9 2 A	: 認証用文字列
1 9 3	: 検証コード
1 9 6	: キーボード
1 9 7	: ログオン認証画面
2 0 0	: ユーザ認証システム
2 0 1	: 認証サーバ
2 0 2	: ワンタイムパスワード導出ルール記憶部

- 2 0 2 b : ワンタイムパスワード導出ルール
- 2 0 3 : ユーザID受信手段
- 2 0 4 : パターン発生手段
- 2 0 5 : パターン送信手段
- 2 0 6 : 検証コード生成手段
- 2 0 7 : ワンタイムパスワード受信手段
- 2 0 8 : ユーザ認証手段
- 2 5 1 : 認証要求クライアント
- 2 5 2 : ユーザID入力手段
- 2 5 3 : ユーザID送信手段
- 2 5 4 : パターン受信手段
- 2 5 5 : パターン表示手段
- 2 5 6 : ワンタイムパスワード入力手段
- 2 5 7 : ワンタイムパスワード送信手段
- 2 9 0 : パターン要素列
- 2 9 1 : 提示パターン
- 2 9 1 p : 所定パターン
- 2 9 2 : ワンタイムパスワード
- 2 9 6 : キーボード