

明 細 書

発明の名称：二要素ユーザ認証システム、およびその方法

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のクライアント装置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し、クライアント装置のハードウェア等の識別情報を認証のためにさらに使用する二要素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において、固定パスワードより高いセキュリティを有する方式として、ユーザ認証のために1回しか使用することができない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するシステムが多く使用されるようになってきた。ワンタイムパスワードには、認証サーバと同期したワンタイムパスワード発生ルールによりワンタイムパスワードを生成するトークンを使用する方式や、認証サーバからクライアントに毎回変化するチャレンジという値が送られ、クライアントがそれに対してパスワードを所定のルールで適用したレスポンスを返すチャレンジ・レスポンス方式などがある。トークンは、それを手元の有しているユーザを確実に特定できるが、トークンを持ち歩く必要があり、またトークンの費用や、トークンを紛失した際の安全性に問題がある。一方、チャレンジ・レスポンス方式においては、トークンを使用する必要がないという簡便さはあるものの、類推されやすい固定パスワードを使用してワンタイムパスワードを発生させるので、パスワード入力時の盗み見などに弱いという問題や、クライアントにレスポンスを発生させるための専用のソフトウェアを導入する必要があるという問題などがある。

[0003] 近年、そのような従来のチャレンジ・レスポンス方式の問題を改善した方式として、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開発された。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。

[0004] さらに、マトリクス認証において、他の情報と組み合わせて提示パターンを生成するパターンシード値を用いることにより、悪意の第三者によってパターンシード値がネットワーク盗聴などされても、提示パターンを特定されることのないシステムも開発された（例えば、特許文献1）。その認証システムでは、認証サーバが提示パターンを生成するパターンシード値を生成して認証要求クライアントに送信し、認証要求クライアントはパターンシード値を使用して提示パターンを表示し、それに基づいて入力されたワンタイムパスワードを認証サーバに送って検証することによりユーザの認証を実行する。

先行技術文献

特許文献

[0005] 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

[0006] しかし、従来のマトリクス認証システムにおいては、ユーザのパスワードというユーザが知っている情報を使用した一要素の認証しか行うことができなかった。従って、ユーザのパスワードが漏洩した場合、それを用いた不正認証を防止することができず、セキュリティに限界があった。このように、よりセキュリティを高めるために、パスワード以外の情報を認証のための第2の要素とした二要素ユーザ認証（Two-factor user authentication）の必要性が高まっていた。すなわち、本人が知っている情報であるパスワード以外に、ある機器を保有していることを表わす情報や、認証を受けようとする者が本人であることを表わす情報などを、認証のための新たな要素とすることが求められていた。しかし、認証に必要な情報としてパスワード以外の情報を単に追加しただけでは、その情報がネットワーク盗聴などで漏洩する可能性があるため、セキュリティの向上は限定的である。ワンタイムパスワードトークンを使用してそのようなパスワード以外の情報を生成することとすると、ネットワーク盗聴による漏洩を防止することはできるが、専用のワンタイムパスワードトークンを導入するコストや手間がかかるし、また、認証時にワンタイムパスワードトークンを携帯していなくてはならないという不便さも生じる。

課題を解決するための手段

[0007] 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、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し、前記ユーザが使用する前記クライアントを識別する情報を前記認証のためにさらに使用する二要素ユーザ認証システムであって、認証サーバと認証要求クライアントとを有し、認証サーバは、ユーザのユーザID

Dとワンタイムパスワード導出ルールと当該ユーザが使用する認証要求クライアントを識別するクライアント識別情報とをお互いに関連付けてあらかじめ記憶し、クライアント識別情報と組み合わせられて提示パターンをユニークに決定する値であるパターンシード値を所定の発生規則により発生させて認証要求クライアントに送信し、認証要求クライアントは、認証を受けようとするユーザが使用している認証要求クライアントを識別するクライアント識別情報を取得し、取得したクライアント識別情報と受信したパターンシード値とに基づいて、所定のパターン要素列生成規則により提示パターンを生成して表示させ、ユーザから、提示パターンに含まれるパターン要素にワンタイムパスワード導出ルールを適用した結果であるワンタイムパスワードの入力を受け付けて認証サーバに送信し、認証サーバは、受信したユーザIDに関連付けられたクライアント識別情報および送信したパターンシード値に基づいて所定のパターン要素列生成規則により生成されるパターン要素列から構成される提示パターンに含まれるパターン要素に当該ユーザIDに関連付けられたワンタイムパスワード導出ルールを適用した結果である検証コードを生成し、受信したワンタイムパスワードと検証コードとを比較することによってユーザの認証を実行することを特徴とする。

[0008] 本発明は、提示パターンをパターンシード値に基づいて生成する際に、複数のクライアント識別情報に基づいてそれを生成するように構成できる。

[0009] 本発明は、提示パターンをパターンシード値に基づいて生成する際に、クライアント識別情報に加えて、ユーザのユーザIDを組み合わせるように構成できる。

[0010] 本発明は、クライアント識別情報として、認証要求クライアントのハードウェアに内蔵された識別情報を取得するように構成できる。

[0011] 本発明は、クライアント識別情報として、認証要求クライアントのインターフェースを通じて外部機器の識別情報を取得するように構成できる。

[0012] 本発明は、クライアント識別情報として、認証要求クライアントのOSのID情報を取得するように構成できる。

- [0013] 本発明は、クライアント識別情報として、認証要求クライアントに設定されたネットワークにおけるアドレス情報を取得するように構成できる。
- [0014] 本発明は、クライアント識別情報として、認証を受けようとするユーザの生体識別情報を取得するように構成できる。
- [0015] 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

- [0016] 本発明は、認証を受けるユーザに提示パターンを提示し、それに含まれる特定の位置の要素に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導出ルールをパスワードとし、ユーザが使用するクライアントを識別する情報を認証のためにさらに使用する二要素ユーザ認証システムであって、認証サーバは、ユーザが使用する認証要求クライアントを識別するクライアント識別情報と組み合わせられて提示パターンをユニークに決定する値であるパターンシード値を発生させて認証要求クライアントに送信し、認証要求クライアントは、認証を受けようとするユーザが使用している認証要求クライアントを識別するクライアント識別情報を取得し、取得したクライアント識別情報と受信したパターンシード値とに基づいて、所定のパターン要素列生成規則により提示パターンを生成して表示させ、ユーザからワンタイムパス

ワードの入力を受け付けて認証サーバに送信し、認証サーバは、提示パターンを再現して検証コードを生成し、それとワンタイムパスワードとを比較してユーザ認証を行うので、ユーザのパスワードというユーザが知っている情報に加えて、クライアント識別情報という第2の要素を認証のために使用することができるため、クライアント識別情報を出力する機器を物理的に保有していることが認証の際の追加的な検証のための条件である二要素認証を実現することができる。さらに、クライアント識別情報そのものを認証の際に検証するものではないため、認証の際のワンタイムパスワードがネットワーク盗聴されたとしても、それからクライアント識別情報が漏洩することはない。そのため、認証の際のワンタイムパスワードがネットワーク盗聴された場合でも、提示パターンやワンタイムパスワードの生成ルールの推定が不可能であり、強固なセキュリティが得られる。クライアント識別情報を出力する機器として、オフライン認証クライアント自身を含む幅広い機器を使用できるため、導入のコストや手間を最小にでき、また、クライアント識別情報を出力する機器を携帯する負担を最小にできる。

[0017] さらに本発明は、提示パターンをパターンシード値に基づいて生成する際に、複数のクライアント識別情報に基づいてそれを生成するように構成できるため、認証のための要素の数を実質的に三要素以上の多要素に拡張することができ、さらに強固なセキュリティが得られる。

[0018] さらに本発明は、提示パターンをパターンシード値に基づいて生成する際に、クライアント識別情報に加えて、ユーザのユーザIDを組み合わせるように構成できるため、パターンシード値がネットワーク盗聴された場合でも、パターンシード値から提示パターンを推定することが一層困難であり、さらに強固なセキュリティが得られる。

[0019] さらに本発明は、クライアント識別情報として、認証要求クライアントのハードウェアに内蔵された識別情報や認証要求クライアントのOSのID情報や認証要求クライアントに設定されたネットワークにおけるアドレス情報などを取得するように構成できるため、認証要求クライアントを物理的に保

有していることに基づく情報が認証の際の追加的な検証のための条件となつてセキュリティが向上する。またさらに本発明は、クライアント識別情報として、認証要求クライアントのインターフェースを通じて外部機器の識別情報を取得するように構成できるため、その外部機器を物理的に保有していることが認証の際の追加的な検証のための条件となつてセキュリティが向上する。またさらに本発明は、クライアント識別情報として、認証を受けようとするユーザの生体識別情報を取得するように構成できるため、本人であることを表わす生体情報が認証の際の追加的な検証のための条件となつてセキュリティが向上する。

図面の簡単な説明

[0020] [図1]本発明の一実施形態に係る二要素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二要素ユーザ認証システム100のブロック図である。

[図3]本発明の一実施形態に係る二要素ユーザ認証システム100の動作フロー図である。

[図4]本発明の一実施形態に係る二要素ユーザ認証システム100の動作フロー図であり、図3に示した動作フローの続きである。

[図5]本発明の一実施形態に係る二要素ユーザ認証システム100における提示パターンの生成方法の概念図である。

[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]二要素ユーザ認証システム100におけるWindows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

[0021] これから発明の実施形態の説明を行う。まず、マトリクス認証に特有の技

術についての説明をする。マトリクス認証は、所定パターンに配列した複数のパターン要素（パターン要素列 190）を認証を受けるユーザが使用するクライアント装置に提示パターン 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 102b を当該ユーザのパスワードとするものである。

[0022] [提示パターンとパターン要素]

提示パターン 191 とは、パターン要素を所定パターンに配列したものである。所定パターンとしては、縦 m 個 $\times$ 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。

[0023] パターン要素とは、提示パターン内において所定パターン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、同じパターン要素は、提示パターン内において、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、ワンタイムパスワード導出ルール 102b 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 192 とは多対 1 の対応となり、ワンタイムパスワード 192 の入力時に自動的にハッシュ化がなされることになる。すなわち、ワ

ンタイムパスワード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つのワンタイムパスワード１９２だけからは、提示パターンが特定されていたとしても、ワンタ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。

[0024] 本実施例では、図７などに示すような、０から９までの１桁の数字をパターン要素とし、それぞれのパターン要素を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を使用すると好適である。

[0025] [パターン要素列]

パターン要素列１９０は、提示パターン１９１を生成するために所定パターン１９１ｐに配置する要素の内容を表わすデータであり、典型的には、その提示パターン１９１に含まれるすべてのパターン要素を順番に並べたものである。パターン要素列１９０は、提示パターン１９１が生成される前に生成される。なお、パターン要素列１９０は、パターン要素が順番に並べられた１つの文字列でなければならないというものではなく、１つの提示パターン１９１に含まれるすべてのパターン要素の情報を含むデータを意味するものである。従って、パターン要素列１９０に含まれるそれぞれのパターン要素を提示パターン内のそれぞれの位置に対応付けられる限り、パターン要素列１９０に含まれるパターン要素の順番は自由である。またパターン要素列１９０は、複数のデータに分割されていても構わない。本発明に係るユーザ認証システム１００は、大きく、ユーザの認証を行う認証サーバ１０１と、その認証サーバとネットワークで接続された、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１５１とから構成される。ユーザ認証システム１００においては、パターン要素列１９０は、認証要求クライアント１５１の内部で生成されて、その中で提示パターン１９１の生成に使用されるが、パターン要素列１９０がそのままの形態でネットワークを通じて認証サーバ１０１に送信されることはない。

[0026] [ワンタイムパスワード導出ルール]

ワンタ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。パターン要素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 102b は、提示パターン 191 に含まれる選択されるパターン要素のそれぞれの位置と、当該それぞれのパターン要素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 102b は、提示パターン 191 に基づかないで入力される固定の数字などのキャラクターの情報を含んでもよく、この場合、ワンタイムパスワード導出ルール 102b は、提示パターン 191 に含まれる選択されるパターン要素のそれぞれの位置および当該提示パターン 191 に基づかないで入力される固定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。

[0027] 図 6 に典型的なワンタイムパスワード導出ルール 102b の構造を示す。本実施例では、0 から 9 までの 1 桁の数字をパターン要素とし、それぞれのパターン要素を 4 つの 4×4 のマトリクスからなる所定パターン 191p 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 102b が例示されている。図 6 においては、所定パターン 191p 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 191p 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。

[0028] 入力される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、それに基づかないで入力される固定の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に基づかないで入力される固定の数字については、最初にそのような固定の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、ワンタイムパスワード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。ワンタ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は、キーボード１９６などによって入力される。ワンタイムパスワード１９２のその次の２つの数字は、提示パターン１９１に基づかないで、キーボード１９６などから入力されるものである。ワンタ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。ワンタイムパスワード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。ワンタイムパスワード導出ルール１０２ｂのそれ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、ワンタイムパスワード導出ルール１０２ｂはここで終了する。ワンタイムパスワード導出ルール１０２ｂには、その終了点をユニーク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、ワンタ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。

[0029] [パターンシード値]

パターンシード値１８３は、所定の変換規則により変換されることによって、１つの提示パターン１９１に含まれるパターン要素をユニークに決定す

る値である。パターンシード値 183 そのものは、所定の発生規則により所定の範囲内において発生される。後述するが、本発明のパターンシード値 183 は、所定の変換規則を適用して 1 つの提示パターン 191 に含まれるパターン要素を生成する際に、さらに他の要素の情報と組み合わせられる点が重要な特徴である。

[0030] 認証サーバ 101 が、認証要求クライアント 151 で入力されたワンタイムパスワードが正しいかどうかを検証するためには、認証要求クライアント 151 において表示される提示パターン 191 を知る必要がある。しかし、提示パターン 191 をそのまま認証サーバ 101 から認証要求クライアント 151 に送ったのでは、それがネットワーク盗聴などにより悪意の第三者に取得されると、パスワードが推測される可能性が生じる。その一方で、提示パターン 191 を認証サーバ 101 と認証要求クライアント 151 との間で共有しなければ、認証サーバ 101 においてワンタイムパスワード 192 の検証を行うことができない。パターンシード値 183 は、このような相反する要求を解決するものであり、所定の変換規則を適用することにより提示パターン 191 をユニークに決定するが、パターン要素列 190 そのものではない情報である。認証サーバ 101 から認証要求クライアント 151 へは、パターン要素列 190 そのものは送信されず、それに代えてパターンシード値 183 が送信される。認証要求クライアント 151 は、認証サーバ 101 から受信したパターンシード値 183 に所定の変換規則を適用することにより提示パターン 191 を生成することができる。所定の変換規則とは、例えばハッシュ関数演算などが考えられる。このように、パターン要素列 190 そのものがネットワーク上を流れないため、パターンシード値 183 を使用することにより、セキュリティが向上する。

[0031] そして本発明においては、パターンシード値 183 は、所定の変換規則により 1 つの提示パターン 191 に含まれるパターン要素を生成する際に、さらに他の要素の情報と組み合わせられる。他の要素の情報としては、認証を受けようとするユーザが使用している認証要求クライアント 151 を識別する

クライアント識別情報 102c が使用される。このようにすると、クライアント識別情報 102c を出力する機器を保有していることが認証の際の追加的な検証のための条件となり、セキュリティが向上する。パターンシード値 183 は、クライアント識別情報 102c と組み合わせられて 1 つの提示パターン 191 に含まれるパターン要素をユニークに決定する。このようにすることによって、提示パターン 191 は、パターンシード値 183 だけでなく、クライアント識別情報 102c の情報も組み込んだものとなるため、ワンタイムパスワード 192 が正しいクライアント識別情報 102c が使用された提示パターン 191 に基づいて入力されたものであるかどうかを検証することが可能となる。そして、本発明においては、提示パターン 191 を、認証要求クライアント 151 を識別するクライアント識別情報 102c を使用して攪乱することによって、提示パターン 191 にはクライアント識別情報 102c の情報も組み込まれることになる。そしてワンタイムパスワード 192 は、そのようにして生成された提示パターン 191 に、ユーザに関連付けられたワンタイムパスワード導出ルール 102b を適用したものである。このように、本発明においては、ワンタイムパスワード 192 が、正しいワンタイムパスワード導出ルール 102b に基づいた正しいユーザによって入力されたものであるかどうかということと、正しいユーザが有する正しいクライアント識別情報 102c を有する認証要求クライアント 151 から入力されたものであるかどうかということという、2 つの要素に基づく認証の成否を規定する情報を含むことになる。このようにして、二要素認証を行うことができるようになるため、セキュリティが劇的に向上する。

[0032] さらに本発明においては、クライアント識別情報 102c という第 2 の要素を使用した認証を行うにもかかわらず、ユーザ認証に際してクライアント識別情報 102c そのものを検証するものではないことが大きな特徴である。すなわち、認証の際のワンタイムパスワードがネットワーク盗聴されたとしても、それからクライアント識別情報が漏洩することはない。そのため、認証の際のワンタイムパスワードがネットワーク盗聴された場合でも、提示

パターンやワンタイムパスワードの生成ルールの推定が不可能であり、強固なセキュリティが得られる。このように、第2の要素であるクライアント識別情報102cが漏洩する可能性を発生させることなく、その第2の要素を認証のために使用する要素として追加することが可能となる。

[0033] また、提示パターン191を生成する際に、複数のクライアント識別情報102cを同時に使用することも可能である。この場合は、それらの複数のクライアント識別情報102cとパターンシード値183とを組み合わせることによって提示パターン191に含まれるパターン要素を決定することになる。それらの複数のクライアント識別情報102cが異なるソースに由来するものであれば、それらが同じ認証要求クライアント151に関連付けられたものであるとしても、認証のための要素の数が実質的に三要素以上の多要素に拡張されることになり、さらに強固なセキュリティが得られる。

[0034] なお、提示パターン191を生成する際に、他の情報をさらに使用して提示パターン191をさらに攪乱することも有用である。そのような他の情報としては、例えば、ユーザID 102aを使用することが可能である。この場合、パターンシード値183は、ユーザID 102aおよびクライアント識別情報102cと組み合わせられて1つの提示パターン191に含まれるパターン要素をユニークに決定することになる。ユーザID 102aはユーザに由来する情報であるため、そのような処理は認証のための要素を増加させるものとは言えない。しかし、パターンシード値183から提示パターン191を生成するためには、さらにユーザID 102aを使用した演算が必要になるため、ワンタイムパスワード192から提示パターン191を類推することが一層困難になる。したがって、ユーザID 102aを提示パターン191の生成のためにさらに使用することによって、セキュリティをさらに向上させることができる。

[0035] パターンシード値183は、典型的には、乱数発生アルゴリズムによって発生させられた所定の範囲内の数値である。パターンシード値183は、所定の範囲内の数値であれば、乱数発生アルゴリズム以外の発生規則、例えば

、所定の初期値からの所定値ごとのカウントアップやカウントダウンで発生させられてもよい。

[0036] [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。ユーザは、提示パターン 191 に対してワ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、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てワнтаイムパスワード 192 を生成し、それを認証要求クライアント 151 に入力する。また、提示パターン 191 に基づかない固定の数字を含めて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нтаイムパスワードに含めることもできる。図 7 において破線で示した矢印と丸は、提示パターン 191 に基づくワнтаイムパスワードをキーボード 196 から入力することを表わしている。図 7 の例では、提示パターン 191 に基づいて「2504」を入力し、次に提示パターン 191 に基づかない固定の数字として「29」を入力し、次に提示パターン 191 に基づいて「0」を入力することによって、ワнтаイムパスワード 192 として「2504290」が入力されている。

[0037] [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 1 はハードウェア構成図、図 2 はブロック図、図 3 および 4 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（チャレンジコードに相当）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（レスポンスに相当）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パターンシード値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１９１は、パターンシード値１８３とクライアント識別情報１０２ｃとに基づいて生成される。認証要求クライアント１５１において、ユーザが提示パターン１９１に基づいて入力したワンタイムパスワード１９２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、当該ユーザのユーザＩＤに関連付けられたクライアント識別情報１０２ｃと受信したパターンシード値１８３とに基づいて提示パターンを再現し、それに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を適用することによって検証コード１９３を生成する。そして認証サーバ１０１は、認証要求クライアント１５１から送信されたワンタイムパスワード１９２と検証コード１９３とを比較し、それらが等しければ当該ユーザに対する認証が成功したものと判定し、認証成功時の所定の動作を開始させる。

[0038] [二要素ユーザ認証システム１００のハードウェア構成]

次に、二要素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二要素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、それらがバスを通じて接続されている。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、クライアント識別情報102cをお互いに関連付けて記憶する。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、それらがバスを通じて接続されている。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、提示パターン生成モジュール151c3、クライアント識別情報取得モジュール151c4を記憶する。

[0039] 認証サーバ101は、二要素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。記憶装置101cは、OS101c1、ユーザ認証アプリケーション101c2のプログラムに関しては、それを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 101a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 101d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、ソフトウェアキーボードなどのキー入力手段と、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。キーボード196は、テンキー、標準のフルキーボードなど、ワンタイムパスワードを構成するパターン要素の入力ができる限り、任意の形態のものを使用できる。ソフトウェアキーボードは、ディスプレイの画面上にキーボードのシンボルを表示させ、タッチパネル、マウス、トラックボールなどのポインティングデバイスを使用してキーのシンボルを選択させることによりキー入力を受け付ける。ネットワークI/F 101e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。

[0040] OS 101c1、ユーザ認証アプリケーション101c2は、それら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、OS 101c1がユーザ認証アプリケーション101c2の機能を包含していてもよい。また、ユーザ認証アプリケーション101c2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。

[0041] 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。

[0042] 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、Webサービスの提供を受ける際の認証を行うものである。例えば、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ینگ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。

[0043] もう1つの利用形態は、OSに管理されたネットワーク環境に接続する際の認証を行うものである。例えば、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。

[0044] 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ーバレ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、ユーザをユニークに識別するためのデータである。ユーザID102aは、任意の文字列を使用することができる。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。クライアント識別情報102cは、認証を受けようとするユーザが使用している認証要求クライアント151を識別するためのデータであり、提示パターンを生成する際に、パターンシード値に組み合わされて使用されるデータである。

[0045] 認証要求クライアント151は、二要素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、OS151c1、ブラウザアプリケーション151c2、提示パターン生成モジュール151c3、クライアント識別情報取得モジュール151c4などがインストールされた端末であり、具体的には、PC、携帯電話機、PDAなどの形態である。CPU151aは、ブラウザアプリケーション151c2、提示パターン生成モジュール151c3、クライアント識別情報取得モジュール151c4などをOS151c1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。RAM151b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CPU151a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、提示パターン生成モジュール151c3、クライアント識別情報取得モジュール151c4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RAM151b上に読み出されて実行される。なお、記憶装置151cは、OS151c1、ブラウザアプリケーション151c2、提示パターン生成モジュール151c3、クライアント識別情報取得モジュール151c4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CPU151a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/F151d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やソフトウェアキーボードなどのキー入力手段と、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。外部／ネットワークI/F151eは、外部通信インターフェースを搭載した外部機器や、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。外部／ネットワークI/F151eを通じて、外部通信インターフェースを搭載した外部機器からはクライアント識別情報を取得することができる。また、外部／ネットワークI/F151eを通じて、ネットワークを経由して認証サーバ101と接続することができる。外部通信インターフェースとしては、USB、Bluetooth（登録商標）、無線LAN、赤外線通信、Felica（登録商標）やRFIDの非接触通信、などの各種の通信インターフェースを使用することができ、接続される外部機器としては、USBメモリ、無線通信用データカード（USB接続、PCカード接続、Express Card接続、など）、FelicaやRFIDなどのICカード、携帯電話機、生体認証情報（指紋、虹彩、静脈など）読み取り機などを使用することができる。

[0046] なお、認証要求クライアント151は、ユーザが使用する認証要求クライアント151に関連付けられたクライアント識別情報102cを記憶したクライアント識別情報記憶部172と接続されている。なお、本発明の認証要

求クライアント１５１は、クライアント識別情報１０２ｃを取得することができればよく、クライアント識別情報記憶部１７２を備えている必要はない。クライアント識別情報記憶部１７２が認証要求クライアント１５１と同じ筐体内に存在することもあり得るが、本発明の認証要求クライアント１５１は、何らかの手段によりクライアント識別情報１０２ｃを取得できれば十分であり、そのようなクライアント識別情報記憶部１７２を必須の構成としては含まない概念である。

[0047] クライアント識別情報１０２ｃとしては、ユーザが使用する認証要求クライアント１５１のハードウェアに内蔵された情報（ハードウェア関連情報）、ユーザが使用する認証要求クライアント１５１のソフトウェアに付随する情報（ソフトウェア関連情報）、ユーザが使用する認証要求クライアント１５１に接続された外部機器から取得される情報（外部機器関連情報）、ユーザが使用する認証要求クライアント１５１に内蔵または接続された生体認証情報読み取り器から取得されるユーザの生体情報（生体認証情報）などを使用することができる。

[0048] ハードウェア関連情報については、ＣＰＵ等のハードウェア構成要素シリアル番号、ネットワークインターフェースカードのＭＡＣアドレス、ハードディスクのシリアル番号、などをクライアント識別情報１０２ｃとして使用することができる。この場合、クライアント識別情報記憶部１７２は、ＣＰＵ等のハードウェア構成要素内のシリアル番号ＩＤの記録領域、ネットワークインターフェースカードのＭＡＣアドレスの記憶領域、ハードディスクのシリアル番号の記憶領域、などとなる。ハードウェア関連情報は、そのハードウェアに対して適切な読み出し操作を行うことにより、それを記憶したハードウェアからバスを通じて取得される。

[0049] ソフトウェア関連情報については、Windows（登録商標） ＯＳのＧＵＩＤ（Ｇｌｏｂａｌｌｙ Ｕｎｉｑｕｅ ＩＤｅｎｔｉｆｉｅｒ）やプロダクトＩＤやプロダクトキー、ＴＣＰ／ＩＰネットワークのＩＰアドレス、などをクライアント識別情報１０２ｃとして使用することができる。この

場合、クライアント識別情報記憶部 172 は、Windows（登録商標）

OS の GUI D の情報を記憶したハードディスク上のファイルやメモリ上の領域、Windows OS のプロダクト ID とプロダクトキーの情報を記憶したハードディスク上のファイルやメモリ上の領域、TCP/IP ネットワークの IP アドレスの設定情報を記憶したハードディスク上のファイルやメモリ上の領域、などとなる。ソフトウェア関連情報は、OS のコマンドを使用することにより、それを記憶したハードディスク上のファイルやメモリ上の領域から取得される。

[0050] 外部機器関連情報については、USB メモリのシリアル番号、無線通信用データカードや携帯電話機のシリアル番号や契約者 ID や電話番号、Bluetooth や無線 LAN 搭載各種機器のシリアル番号、Felica や RFID などの IC カードの ID 番号（シリアル番号）、などをクライアント識別情報 102c として使用することができる。この場合、クライアント識別情報記憶部 172 は、USB メモリのシリアル番号の記憶領域、無線通信用データカードや携帯電話機のシリアル番号や契約者番号や電話番号の記憶領域、Bluetooth や無線 LAN 搭載各種機器のシリアル番号の記憶領域、Felica や RFID などの IC カードの ID 番号（シリアル番号）の記憶領域、などとなる。外部機器関連情報は、その外部機器に対して適切な読み出しコマンドを送信することにより、それを記憶した外部機器から外部／ネットワーク I/F 151e を通じて取得される。

[0051] 生体認証情報については、指紋、虹彩、静脈などの本人確認に適した所定の生体のパターンを生体認証情報読み取り機によって読み取ることによって出力される生体認証情報をクライアント識別情報 102c として使用することができる。この場合、クライアント識別情報記憶部 172 は、ユーザの所定の生体のパターンを読み取って生体認証情報を出力している際の、生体認証情報読み取り機における情報処理手段となる。すなわち、固定的なユーザの所定の生体のパターンを生体認証情報に変換することが、クライアント識別情報 102c をクライアント識別情報記憶部 172 から読み出すことに相

当する。生体認証情報は、生体認証情報読み取り機に対して適切な読み取りコマンドを送信することにより、ユーザの所定の生体のパターンを読み取っている生体認証情報読み取り機から、バス（生体認証情報読み取り機が内蔵の場合）または外部／ネットワーク I/F 151e（生体認証情報読み取り機が外部に接続されている場合）を通じて取得される。

[0052] OS 151c1、ブラウザアプリケーション151c2、提示パターン生成モジュール151c3、クライアント識別情報取得モジュール151c4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が提示パターン生成モジュール151c3やクライアント識別情報取得モジュール151c4の機能を包含していてもよく、OS 151c1がブラウザアプリケーション151c2、提示パターン生成モジュール151c3及びクライアント識別情報取得モジュール151c4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。

[0053] OS 151c1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。OS 151c1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、OS 151c1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。提示パターン生成モジュール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。認証要求クライアント151が、携帯電話機、PDAなどの場合であっても、近い将来にはブラウザアプリケーション151c2にモジュールを組み込むことが可能になると見込まれており、提示パターン生成モジュール151c3は、そのようなモジュールの形態として機能することになる。提示パターン生成モジュール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。クライアント識別情報取得モジュール151c4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、ユーザが使用している認証要求クライアント151からクライアント識別情報102cを取得するためのプログラムであり、提示パターン生成モジュール151c3と同様の形態のモジュールである。

[0054] 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および提示パターン生成モジュール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要求する。

[0055] 標準のWindowsのログオン認証画面の変更は、具体的には以下のようにして実施する。ここでは、Windows XPを例にして説明する。まず、ブラウザアプリケーション151c2、提示パターン生成モジュール

151c3、及びクライアント識別情報取得モジュール151c4の機能を実施するプログラムであるログオン認証モジュールをWindows用のDLLファイルとして作成する。ここでは、「SmxGina.dll」という名前のDLLファイルを作成する。ここで、Windowsのログオン認証画面のプログラムは、以下に示すレジストリのロケーションにおいて「GinaDLL」という名前のキーのデータとして指定されている。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

標準のログオン認証のモジュールは「msgina.dll」というDLLファイルであり、それが前述した「GinaDLL」という名前のキーのデータに設定されている。当該キーのデータを「SmxGina.dll」に書き換えると、本願発明に係る認証方法を実施するログオン認証モジュールがログオンなどの認証時に呼び出されることになる。

- [0056] 図8は、二要素ユーザ認証システム100におけるログオン認証画面197Aおよび197Bのイメージ図である。Windowsのログオン時にログオン認証モジュール「SmxGinaDLL」が起動させられることによって、まず、ログオン認証画面197Aが表示させられる。ログオン認証画面197Aには、ユーザ名入力フィールド、ログオン先入力フィールドが表示される。ログオン先にネットワーク名を入力することによってオンラインで使用するためにWindowsのドメインネットワークへのログオン認証を行わせることができる。ユーザがログオン認証画面197Aのユーザ名入力フィールドに自己のユーザIDを入力ユーザID181として入力すると、当該認証モジュールは認証サーバ101に入力ユーザID181を伝達してそれに基づいて提示パターン191を生成させる。そして、提示パターン191を含むログオン認証画面197Bが表示される。ログオン認証画面197Bにはパスワード入力フィールドがあり、キーボード196などによってワンタイムパスワードとして数字などのキャラクターが入力されると、それに応答して「*」が1つずつ表示される。ワンタイムパスワード192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にワンタイムパスワード１９２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。

[0057] [二要素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二要素ユーザ認証システム１００のブロック図である。図２は、図１に示したハードウェア構成の二要素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、認証要求受信手段１０３、検証コード生成手段１０６、ワンタイムパスワード受信手段１２１、ユーザ認証手段１２２、パターンシード値発生手段１０４、パターンシード値送信手段１０５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の必要部分がＯＳ１０１ｃ１の必要部分とともに記憶装置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。

[0058] 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、クライアント識別情報１０２ｃとをお互いに関連付けてあらかじめ記憶する構成要素であり、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。認証要求受信手段１０３は、認証要求クライアント１５１から、そこで入力された入力ユーザＩＤ１８１を含んだ認証要求を受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。パターンシード値発生手段１０４は、クライアント識別情報１０２ｃとともに

に提示パターンを規定する値であるパターンシード値 183 を所定の発生規則により発生する構成要素であり、CPU 101 a、RAM 101 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。パターンシード値送信手段 105 は、発生させられたパターンシード値 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、CPU 101 a、RAM 101 b、ネットワーク I/F 101 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。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 102 b 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 に適用した結果である検証コード 193 を生成する構成要素であり、CPU 101 a、RAM 101 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。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 102 b 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 と同じ値である。ワンタイムパスワード受信手段 121 は、認証要求クライアント 151 から、そこで入力されたワンタイムパスワード 192 を受信する構成要素であり、CPU 101 a、RAM 101 b、ネットワーク I/F 101 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 122 は、ワンタイムパスワード 192 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、CPU 101 a、RAM 101 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。

[0059] 認証要求クライアント 151 は、ユーザ ID 入力手段 152、認証要求送信手段 153、パターンシード値受信手段 154、パターン要素列生成手段 155、パターン表示手段 156、ワンタイムパスワード入力手段 157、ワンタイムパスワード送信手段 158 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 101 c 2 の必要部分、提示パターン生成モジュール 151 c 3、クライアント識別情報取得モジュール 151 c 4 な

どがOS 151 c 1の必要部分とともに記憶装置 151 cからRAM 151 b上に読み込まれ、それらのソフトウェアがCPU 151 aによって実行されることによって、RAM 151 b、記憶装置 151 c、ユーザ I/F 151 d、外部/ネットワーク I/F 151 e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。

[0060] ユーザ ID 入力手段 152 は、認証を受けようとするユーザのユーザ ID を入力ユーザ ID 181として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。認証要求送信手段 153 は、入力された入力ユーザ ID 181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、外部/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。パターンシード値受信手段 154 は、認証サーバ 101から、パターンシード値 183を受信する構成要素であり、CPU 151 a、RAM 151 b、外部/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。パターン要素列生成手段 155 は、認証要求クライアント 151で取得したクライアント識別情報 102 cおよび認証サーバ 101から受信したパターンシード値 183に基づいて、所定のパターン要素列生成規則により提示パターンに含まれるパターン要素を生成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。パターン表示手段 156 は、パターン要素列生成手段 155によって生成されたパターン要素列 190のパターン要素を所定パターン 191 p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。ワンタイムパスワード入力手段 157 は、画面に表示させた提示パターンなどを通じてワンタイムパスワード 192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。ワンタイムパスワード送信手段 158は、入力されたワンタイムパスワード 192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、外部／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。クライアント識別情報取得手段 171は、認証を受けようとするユーザが使用する認証要求クライアント 151を識別するクライアント識別情報 102 cを取得する構成要素であり、クライアント識別情報 102 cがハードウェア関連情報またはソフトウェア関連情報の場合は、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り、クライアント識別情報 102 cが外部機器関連情報の場合は、CPU 151 a、RAM 151 b、外部／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。

[0061] [二要素ユーザ認証システム 100の動作]

これから、二要素ユーザ認証システム 100の動作について説明する。図 3および 4は、二要素ユーザ認証システム 100の動作フロー図である。まず、二要素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、そのユーザが認証を受ける際に使用する認証要求クライアント 151を識別するクライアント識別情報 102 cをあらかじめ認証サーバ 101に入力して登録する。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とクライアント識別情報 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 S 101）。認証サーバ 101は、好適にはインターネットまたはイントラネットの Web 上にユーザ ID とパスワードとクライアント識別情報 102 cの登録のための初期登録 Web ページなどを提供しており、ユーザは、認証要求クライアント 151などの端末からその初期

登録Webページを通じて認証サーバ101にアクセスする。それによって、認証要求クライアント151には、ユーザID入力のための入力フィールドと、0から9までの数字を乱数的にパターン要素として配置した提示パターン191が表示される（図示せず）。ユーザは入力フィールドに自分が登録したいユーザID102aを入力する。ユーザは次に、自分が登録しようとする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に含まれるパターン要素の位置の選択または当該提示パターン191に基づかない固定の数字などのキャラクターの入力を行う。認証サーバ101は、入力されたユーザID102aをそのユーザのユーザIDとしてパスワード記憶部102に記憶させる。一方、選択または入力された数字の列は、それだけではワンタイムパスワード導出ルール102bを特定することができない。従って、認証サーバ101は、異なる提示パターン191を表示してパスワード導出ルール102bに従った2回目の数字の選択または入力を行わせ、選択または入力された数字の列を1回目のものと比較して、ワンタイムパスワード導出ルール102bを特定する。2回目の提示パターン191を、1回目の提示パターン191と大きく異なるように工夫して発生させると、通常、2回の提示パターン191の提示によってワンタイムパスワード導出ルール102bを特定することが可能である。2回の提示パターン191の提示でワンタイムパスワード導出ルール102bの特定ができなかった場合は、それが特定できるまで、提示パターン191の内容を変えてその提示を繰り返す。これによって、提示パターン191に含まれるパターン要素の中で選択されたもののそれぞれの位置および当該提示パターン191に基づかない固定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の位置および当該それぞれの固定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であるワンタイムパスワード導出ルール102bが特定される。特定されたワンタイムパスワード導出ルール102bは、当該ユーザのユーザID102aと関連付けられてパスワード記憶部102に記憶される。なお、初期登録Webページから、提示パターン生成モジュール1

51c3やクライアント識別情報取得モジュール151c4などの、認証要求クライアント151に必要なソフトウェアをダウンロードすることができるように構成すると好適である。これによって、その初期登録Webページにアクセスしてきた任意のPCの中にパターン要素列生成手段155やクライアント識別情報取得手段171を形成させ、それを認証要求クライアント151として動作できるようにすることができる。

[0062] 認証要求クライアント151が、ユーザID102aとワンタイムパスワード導出ルール102bの登録のために認証サーバ101にアクセスしたときに、クライアント識別情報取得手段171が動作することにより認証要求クライアント151が取得可能なクライアント識別情報102cを取得して、認証サーバ101に送信する。これは、ユーザID102aとワンタイムパスワード導出ルール102bの登録の前でも後でもよい。このとき、初期登録Webページが、各種のクライアント識別情報102cの取得先（CPU、MACアドレス、ハードディスク、Windows OSのGUIDやプロダクトIDやプロダクトキー、IPアドレス、USBメモリ、無線通信用データカード、携帯電話機、Bluetoothや無線LAN搭載各種機器、Felica、RFID、生体認証情報読み取り機、などのクライアント識別情報記憶部172を有するもの）を選択のために表示する。ここで、クライアント識別情報取得手段171が取得可能なクライアント識別情報102cをバスや外部／ネットワークI/Fを通じて走査して確認し、クライアント識別情報102cを取得可能な取得先だけを表示させるようにすると好適である。なお、二要素ユーザ認証システム100の管理者が、1つあるいは複数のクライアント識別情報102cの取得先をあらかじめ設定しておき、ユーザが取得先を選択しないようにも構成できる。ユーザが、表示された取得先のいずれかを選択すると、選択された取得先からクライアント識別情報102cがクライアント識別情報取得手段171によって読み出される。なお、ユーザは複数の取得先を選択することも可能である。この場合、それらの複数のクライアント識別情報102cを同時にパターンシード値18

3と組み合わせて提示パターン191を生成するようにすることもでき、認証のための要素の数を実質的に三要素以上の多要素に拡張することもできる。読み出されたクライアント識別情報102cは、認証サーバ101に送信され、認証サーバ101は、受信したクライアント識別情報102cを、ユーザID102a及びワンタイムパスワード導出ルール102bと関連付けてパスワード記憶部102に記憶することによって登録する。これらの登録の操作が完了すると、そのユーザは、二要素ユーザ認証システム100による認証を受けることができるようになる。なお、クライアント識別情報102cを登録する際に、その取得先の情報をいずれかの場所に記憶させておくことが好適である。そのようにすると、ユーザが認証を受ける際に、記憶された取得先の情報を使用して、クライアント識別情報102cの取得先を自動的に設定することが可能となるからである。取得先の情報は、認証要求クライアント151の記憶装置151c内に所定の記憶領域を設けて、そこにユーザID102aと関連付けて記憶させることができる。また、取得先の情報をクライアント識別情報102cとともに認証サーバ101に記憶させ、ユーザの認証の際に取得先の情報を認証サーバ101から認証要求クライアント151に送信するように構成することもできる。

[0063] 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、ユーザID入力手段152により自分のユーザIDを入力ユーザID181として入力する（ステップS103）。典型的には、ユーザは認証要求クライアント151上で動作しているブラウザアプリケーション151c2を使用して、認証サーバ101が提供するユーザ認証Webページにアクセスし、そこに表示されるユーザID入力のための入力フィールドに自己のユーザIDを入力する。Windowsのドメインネットワークへのログイン認証の場合は、図8に示されたログオン認証画面197Aにおいて、ユーザ一名フィールドに自己のユーザIDを入力し、ログオン先にログオンしようとするネットワーク名を入力する。次に、認証要求クライアント151は、認証要求送信手段153により、入力された入力ユーザID181を含む

認証要求を認証サーバ101に送信する（ステップS105）。典型的には、認証要求クライアント151上で動作しているブラウザアプリケーション151c2が、入力フィールドに入力された入力ユーザID181をインターネットまたはイントラネットを通じて認証サーバ101に送信する。Windowsのドメインネットワークへのログイン認証の場合は、ログオン認証モジュール「SmxGinaDLL」が入力ユーザID181を含む認証要求を認証サーバ101に送信する。次に、認証サーバ101は、認証要求受信手段103により、認証要求クライアント151から送信された入力ユーザID181を含む認証要求を受信する（ステップS107）。典型的には、認証サーバ101は、ユーザ認証アプリケーション101c2を動作させ、それによって入力ユーザID181を含む認証要求を受信する。次に、認証サーバ101は、パターンシード値発生手段104により、パターンシード値183を所定の発生規則によって発生させる（ステップS109）。所定の発生規則は、典型的には、所定の範囲内の乱数を発生させることである。図5には、パターンシード値183として、16進数で表わした「284E17・・・・39D0」が例示されている。パターンシード値183は、例えば、16バイトのような所定のビット長の数字列で表わすことができ、この場合、当該所定の範囲とは、16進数で「00000000000000000000」から「FFFFFFFFFFFFFFFFFFFFFFFF」の範囲となる。従って、当該所定の範囲の任意の数字列をパターンシード値183とすることができるため、最大で当該所定の範囲の数だけ異なる提示パターン191を生成することが可能となる。

[0064] 次に、認証サーバ101は、パターンシード値送信手段105により、発生したパターンシード値183を認証要求クライアント151に送信する（ステップS111）。典型的には、認証サーバ101は、ユーザ認証アプリケーション101c2を動作させ、それによってパターンシード値183を認証要求クライアント151に送信する。次に、認証要求クライアント151は、パターンシード値受信手段154により、認証サーバ101から送信

されたパターンシード値 183 を受信する（ステップ S 113）。典型的には、認証要求クライアント 151 上で動作しているブラウザアプリケーション 151c またはログオン認証モジュール「SmxGinaDLL」が、パターンシード値 183 を受信する。次に、認証要求クライアント 151 は、ユーザにクライアント識別情報 102c の取得先を選択させ、選択された取得先からクライアント識別情報取得手段 171 によりクライアント識別情報 102c を取得する（ステップ S 115）。なお、クライアント識別情報 102c の登録時における取得先が記憶装置 151c 内の所定領域に記憶されている場合には、その取得先の情報を使用することによって、認証要求クライアント 151 においてクライアント識別情報 102c の取得先は自動的に設定されることになる。また、クライアント識別情報 102c の登録時における取得先が認証サーバ 101 に記憶されている場合には、その取得先の情報が認証サーバ 101 から認証要求クライアント 151 に送信され、その取得先の情報を使用することによって、認証要求クライアント 151 においてクライアント識別情報 102c の取得先は自動的に設定されることになる。これらの場合、ユーザによるクライアント識別情報 102c の取得先の選択は不要である。次に、認証要求クライアント 151 は、パターン要素列生成手段 155 により、ステップ S 115 で取得したクライアント識別情報 102c と、ステップ S 113 で受信したパターンシード値 183 とに基づいて所定のパターン要素列生成規則により提示パターン 191 を構成するパターン要素列 190 を生成する（ステップ S 117）。所定のパターン要素列生成規則とは、クライアント識別情報 102c とパターンシード値 183 との組み合わせに対してユニークに決定されるパターン要素列であって、そのパターン要素列だけでは元のクライアント識別情報 102c とパターンシード値 183 とを推定することが極めて困難なものを発生させる規則であって、典型的には、以下に述べるような、クライアント識別情報 102c とパターンシード値 183 との組み合わせを一種の初期値とした暗号化演算によるものである。図 5 は、提示パターン 191 の生成方法の概念図である。ここでは、「

C 8 E 3 0 B 1 7 8 4 2 2」というクライアント識別情報 1 0 2 c と「2 8 4 E 1 7 . . . 3 9 D 0」というパターンシード値 1 8 3 とに基づいてパターン要素列 1 9 0 が生成される。そのために、まず、クライアント識別情報 1 0 2 c とパターンシード値 1 8 3 の組み合わせから、所定の数字列を一意的に生成する。図 5 の第 1 段及び第 2 段に示した例では、それぞれ 1 6 進数で表わしたクライアント識別情報 1 0 2 c とパターンシード値 1 8 3 とを結合して所定の数字列を生成している。クライアント識別情報 1 0 2 c とパターンシード値 1 8 3 との組み合わせ方としては、他には、加算、減算、排他的論理和、などのあらゆる演算を使用して組み合わせることができる。次に、その所定の数字列に対して暗号化演算を実施して、所定のビット長のビット列 1 8 4 を生成する。ここでは、所定のビット長は、6 4 の数字からなる提示パターン 1 9 1 を生成するために十分な情報量である 2 5 6 ビットである。暗号化演算としては、演算結果から元の数字列を求めることが事実上不可能なものであればよく、ハッシュ関数演算、共通鍵暗号化演算、などを使用することができる。例えば、ハッシュ関数として S H A 2 5 6 を使用して、その所定の数字列を暗号化すると、2 5 6 ビットのビット列 1 8 4 を生成することができる。また、共通鍵暗号化演算として A E S を使用して、その所定の数字列から鍵を生成し、その鍵によってあらかじめ適当に設定した 2 5 6 ビットの数字列を暗号化すると、2 5 6 ビットのビット列 1 8 4 を生成することができる。また、それらのハッシュ関数演算と共通鍵暗号化演算とを組み合わせることもできる。なお、図 5 に示したビット列 1 8 4 「0 1 1 1 0 0 1 0 1 1 0 0 1 1 0 1 . . . 1 1 0 1 0」の値は説明のための例示であり、正確な S H A 2 5 6 演算の結果を示したものではない。次に、2 5 6 ビットのビット列 1 8 4 を 7 7 桁の十進数に変換し、そこから 6 4 桁の数字を抽出してパターン要素列 1 9 0 とする。なお、図 5 に示したパターン要素列 1 9 0 「3 8 0 6 4 6 5 5 . . . 1 0 1 7」の値は説明のための例示であり、正確な変換・抽出の結果を示したものではない。6 4 桁の数字の抽出は、不要な上位ビット列の削除、不要な下位ビット列の削除、割算などのあら

ゆる演算を使用することができる。次に、認証要求クライアント151は、パターン表示手段156により、パターン要素列190のそれぞれのパターン要素を4つの4×4のマトリクスからなるパターンのそれぞれの要素の位置に配置した提示パターン191を表わす画像を生成し、それを認証要求クライアント151の画面に表示させる（ステップS119）。Windowsのドメインネットワークへのログイン認証の場合は、図8に示されるように、ログオン認証画面197Aに続いて、提示パターン191を含むログオン認証画面197Bが表示させられる。

[0065] 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（0から9のいずれかの数字）を選択したり、提示パターン191に基づかない固定の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を認証要求クライアント151に入力する。認証要求クライアント151は、ワнтаイムパスワード入力手段157により、ワнтаイムパスワード192の入力を受け付ける（ステップS121）。次に、認証要求クライアント151は、ワнтаイムパスワード送信手段158により、入力されたワнтаイムパスワード192を認証サーバ101に送信する（ステップS123）。次に、認証サーバ101は、ワнтаイムパスワード受信手段121により、認証要求クライアント151から送信されたワнтаイムパスワード192を受信する（ステップS125）。

[0066] 次に、認証サーバ101は、検証コード生成手段106により、認証要求クライアント151から受信した入力ユーザID181および認証要求クライアント151に送信したパターンシード値183に基づいて、所定のパターン要素列生成規則により生成されるパターン要素列から構成される提示パターンに、当該入力ユーザID181に対応するワнтаイムパスワード導出ルール102bを適用した結果である検証コード193を生成する（ステッ

プ S 1 2 7)。ここでの所定のパターン要素列生成規則は、認証要求クライアント 1 5 1 において、ステップ S 1 1 7 でパターン要素列生成手段 1 5 5 がパターン要素列を発生させたパターン要素列生成規則と全く同じ規則である。従って、検証コード 1 9 3 は、入力ユーザ I D 1 8 1 のユーザに関連付けられた正しいワンタイムパスワード導出ルール 1 0 2 b が、そのユーザに関連付けられた正しいクライアント識別情報 1 0 2 c と正しいパターンシード値 1 8 3 とに基づく正しい提示パターン 1 9 1 に適用された結果である正しいワンタイムパスワード 1 9 2 と同じ値となる。次に、認証サーバ 1 0 1 は、ユーザ認証手段 1 2 2 により、受信したワンタイムパスワード 1 9 2 と生成した検証コード 1 9 3 とを比較し、それらが等しければ、当該ユーザのユーザ認証が成功したものと判定する（ステップ S 1 2 9）。認証が成功すると、以下のように、ユーザ認証の利用形態に応じたサービスが許可されることになる。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認めさせる。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。

[0067] なお、認証のための要素の数を実質的に三要素以上の多要素に拡張することを目的として、複数のクライアント識別情報 1 0 2 c を同時にパターンシード値 1 8 3 と組み合わせて提示パターン 1 9 1 を生成するように構成するためには、クライアント識別情報 1 0 2 c を扱う手段やステップにおいて、複数のクライアント識別情報 1 0 2 c を使用するように本発明を構成すればいい。具体的には、パスワード記憶部 1 0 2 は、ユーザのユーザ I D と当該ユーザのワンタイムパスワード導出ルールと当該ユーザが使用する認証要求クライアントをそれぞれ識別する複数のクライアント識別情報とをお互いに関連付けてあらかじめ記憶するものであり、パターンシード値発生手段 1 0

4は、複数のクライアント識別情報と組み合わせられて提示パターンをユニークに決定する値であるパターンシード値を所定の発生規則により発生するものであり、クライアント識別情報取得手段171は、認証を受けようとするユーザが使用している認証要求クライアント151を識別する複数のクライアント識別情報102cを取得するものであり、パターン要素列生成手段155は、取得された複数のクライアント識別情報102cと受信したパターンシード値183とに基づいて、所定のパターン要素列生成規則により前記提示パターンを構成するパターン要素の集合であるパターン要素列を生成するものであり、検証コード生成手段106は、受信したユーザIDに関連付けられた複数のクライアント識別情報および送信したパターンシード値に基づいて所定のパターン要素列生成規則により生成されるパターン要素列から構成される提示パターンに含まれるパターン要素に受信したユーザIDに関連付けられたワンタイムパスワード導出ルールを適用した結果である検証コードを生成するものであるように構成するとよい。

[0068] 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。例えば、ステップS127の認証サーバ101における検証コード193の生成などは、入力ユーザID181とパターンシード値183が利用できるようになるステップS109の直後で実行されてもよい。

[0069] 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

[0070] 100 二要素ユーザ認証システム
101 認証サーバ
101a CPU
101b RAM

- 1 0 1 c 記憶装置
- 1 0 1 c 1 O S
- 1 0 1 c 2 ユーザ認証アプリケーション
- 1 0 1 d ユーザインターフェース (I / F)
- 1 0 1 e ネットワークインターフェース (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 クライアント識別情報
- 1 0 3 認証要求受信手段
- 1 0 4 パターンシード値発生手段
- 1 0 5 パターンシード値送信手段
- 1 0 6 検証コード生成手段
- 1 2 1 ワンタイムパスワード受信手段
- 1 2 2 ユーザ認証手段
- 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 1 O S
- 1 5 1 c 2 ブラウザアプリケーション
- 1 5 1 c 3 提示パターン生成モジュール
- 1 5 1 c 4 クライアント識別情報取得モジュール
- 1 5 1 d ユーザインターフェース (I / F)
- 1 5 1 e ネットワークインターフェース (I / F)
- 1 5 2 ユーザ I D 入力手段
- 1 5 3 認証要求送信手段
- 1 5 6 パターン表示手段

- 1 5 7 ワンタイムパスワード入力手段
- 1 5 8 ワンタイムパスワード送信手段
- 1 5 4 パターンシード値受信手段
- 1 5 5 パターン要素列生成手段
- 1 7 1 クライアント識別情報取得手段
- 1 7 2 クライアント識別情報記憶部
- 1 8 1 入力ユーザ I D
- 1 8 3 パターンシード値
- 1 8 4 ビット列
- 1 9 0 パターン要素列
- 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 3 検証コード
- 1 9 6 キーボード
- 1 9 7 A ログオン認証画面
- 1 9 7 B ログオン認証画面

請求の範囲

[請求項1]

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が使用するクライアント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し、前記ユーザが使用する前記クライアントを識別する情報を前記認証のためにさらに使用する二要素ユーザ認証システムであって、

前記ユーザの認証を行う認証サーバと、

前記認証サーバとネットワークで接続された、前記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と、を有し、

前記認証サーバは、

前記ユーザのユーザIDと当該ユーザのワンタイムパスワード導出ルールと当該ユーザが使用する前記認証要求クライアントを識別するクライアント識別情報と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と、

前記クライアント識別情報と組み合わせられて前記提示パターンをユニークに決定する値であるパターンシード値を所定の発生規則により発生するパターンシード値発生手段と、

認証を受けようとするユーザのユーザIDを前記認証要求クライアントから受信するユーザID受信手段と、

発生させられた前記パターンシード値を、認証を受けようとするユーザの前記認証要求クライアントに送信するパターンシード値送信手段と、

を有し、

前記認証要求クライアントは、

前記ユーザから前記ユーザIDの入力を受け付けるユーザID入力手段と、

入力された前記ユーザIDを前記認証サーバに送信するユーザID
送信手段と、

前記認証サーバから送信された前記パターンシーブ値を受信するパ
ターンシーブ値受信手段と、

認証を受けようとする前記ユーザが使用している前記認証要求ク
ラウドを識別するクラウドクラウド識別情報を取得するクラウド識別
別情報取得手段と、

取得された前記クラウドクラウド識別情報と受信した前記パターンシー
ブ値とに基づいて、所定のパターン要素列生成規則により前記提示パ
ターンを構成するパターン要素の集合であるパターン要素列を生成す
るパターン要素列生成手段と、

生成された前記パターン要素列に含まれるそれぞれのパターン要素
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と、

前記ユーザから、前記提示パターンに含まれるパターン要素に前記
クラウドの入力を受け付けるクラウドクラウド入力手段と、
入力された前記クラウドクラウドを前記認証サーバに送信する
クラウドクラウド送信手段と、

を有し、
前記認証サーバは、
前記クラウドクラウドを受信するクラウドクラウド受信手
段と、

受信した前記ユーザIDに関連付けられた前記クラウドクラウド識別情
報および送信した前記パターンシーブ値に基づいて前記所定のパター
ン要素列生成規則により生成されるパターン要素列から構成される提
示パターンに含まれるパターン要素を受信した前記ユーザIDに関連

付けられた前記クラウドクラウド導出ルールを適用した結果であ

る検証コードを生成する検証コード生成手段と、

受信した前記ワンタイムパスワードと生成された前記検証コードとを比較し、それらが等しい場合に前記ユーザIDに対応するユーザの認証を成功させるユーザ認証手段と、

をさらに有することを特徴とする二要素ユーザ認証システム。

[請求項2]

請求項1に記載の二要素ユーザ認証システムにおいて、

前記パスワード記憶部は、あらかじめ前記ユーザのユーザIDと当該ユーザのワンタイムパスワード導出ルールと当該ユーザが使用する前記認証要求クライアントをそれぞれ識別する複数のクライアント識別情報とをお互いに関連付けて記憶するものであり、

前記パターンシード値発生手段は、前記複数のクライアント識別情報と組み合わせられて前記提示パターンをユニークに決定する値であるパターンシード値を所定の発生規則により発生するものであり、

前記クライアント識別情報取得手段は、認証を受けようとする前記ユーザが使用している前記認証要求クライアントを識別する前記複数のクライアント識別情報を取得するものであり、

前記パターン要素列生成手段は、取得された前記複数のクライアント識別情報と受信した前記パターンシード値とに基づいて、所定のパターン要素列生成規則により前記提示パターンを構成するパターン要素の集合であるパターン要素列を生成するものであり、

前記検証コード生成手段は、受信した前記ユーザIDに関連付けられた前記複数のクライアント識別情報および送信した前記パターンシード値に基づいて前記所定のパターン要素列生成規則により生成されるパターン要素列から構成される提示パターンに含まれるパターン要素に受信した前記ユーザIDに関連付けられた前記ワンタイムパスワード導出ルールを適用した結果である検証コードを生成するものであることを特徴とする二要素ユーザ認証システム

[請求項3]

請求項1に記載の二要素ユーザ認証システムにおいて、

前記パターンシード値発生手段は、前記ユーザIDおよび前記クライアント識別情報と組み合わせられて前記提示パターンをユニークに決定する値であるパターンシード値を所定の発生規則により発生するものであり、

前記パターン要素列生成手段は、入力された前記ユーザIDと認証を受けようとする前記ユーザが使用している前記認証要求クライアントを識別する前記クライアント識別情報と受信した前記パターンシード値とに基づいて、所定のパターン要素列生成規則により前記提示パターンを構成するパターン要素の集合であるパターン要素列を生成するものであり、

前記検証コード生成手段は、受信した前記ユーザID、受信した前記ユーザIDに関連付けられた前記クライアント識別情報および送信した前記パターンシード値に基づいて前記所定のパターン要素列生成規則により生成されるパターン要素列から構成される提示パターンに含まれるパターン要素に受信した前記ユーザIDに対応する前記ワンタイムパスワード導出ルールを適用した結果である検証コードを生成するものである二要素ユーザ認証システム。

[請求項4] 請求項1に記載の二要素ユーザ認証システムにおいて、

前記クライアント識別情報取得手段は、前記認証要求クライアントのハードウェアに内蔵された識別情報を取得する二要素ユーザ認証システム。

[請求項5] 請求項1に記載の二要素ユーザ認証システムにおいて、

前記クライアント識別情報取得手段は、前記認証要求クライアントのOSのID情報を取得する二要素ユーザ認証システム。

[請求項6] 請求項1に記載の二要素ユーザ認証システムにおいて、

前記クライアント識別情報取得手段は、前記認証要求クライアントに設定されたネットワークにおけるアドレス情報を取得する二要素ユーザ認証システム。

[請求項7]

請求項 1 に記載の二要素ユーザ認証システムにおいて、

前記クライアント識別情報取得手段は、前記認証要求クライアントのインターフェースを通じて外部機器の識別情報を取得する二要素ユ

ーザ認証システム。

[請求項8]

請求項 1 に記載の二要素ユーザ認証システムにおいて、

前記クライアント識別情報取得手段は、認証を受けようとするユーザの生体識別情報を取得する二要素ユーザ認証システム。

[請求項9]

所定パターンに配列した複数のパターンの要素を認証を受けるユーザ

が使用するクライアント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の要素に対して適用することによりクライアントを生成するためのクライアントパースワード導出ルールを当該ユーザのパースワードとし、前記ユーザが使用する前記クライアントを識別する情報を前記認証のためにさらに使用することによって、前記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からの認証要求に応答して、当該認証要求クライアントとネットワークで接続された認証サーバが前記ユーザの認証を行う二要素ユーザ認証方法であって、

前記認証サーバが、前記ユーザの ID と当該ユーザのワタ
イムパースワード導出ルールと前記認証要求クライアントを識別するク
ライアント識別情報とをお互いに関連付けてあらかじめ記憶するス
トップと、

前記認証要求クライアントが、認証を受けようとするユーザのユー
ザ ID の入力を受け付けるストップと、

前記認証要求クライアントが、入力された前記ユーザ ID を前記認
証サーバに送信するストップと、

前記認証サーバが、前記認証要求クライアントから送信された認証
を受けようとするユーザのユーザ ID を受信するストップと、

前記認証サーバが、前記クライアント識別情報と組み合わされて前

記提示パターンをユニークに決定する値であるパターンシード値を所定の発生規則により発生するステップと、

前記認証サーバが、発生させられた前記パターンシード値を認証を受けようとするユーザの前記認証要求クライアントに送信するステップと、

前記認証要求クライアントが、前記認証サーバから送信された前記パターンシード値を受信するステップと、

前記認証要求クライアントが、認証を受けようとする前記ユーザが使用している前記認証要求クライアントを識別するクライアント識別情報を取得するステップと、

前記認証要求クライアントが、取得された前記クライアント識別情報と受信した前記パターンシード値とに基づいて、所定のパターン要素列生成規則により前記提示パターンを構成するパターン要素の集合であるパターン要素列を生成するステップと、

前記認証要求クライアントが、生成された前記パターン要素列に含まれるそれぞれの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ステップと、

前記認証要求クライアントが、前記提示パターンに含まれるパターン要素に前記ワンタイムパスワード導出ルールを適用した結果であるワンタイムパスワードの入力を前記ユーザから受け付けるステップと、

前記認証要求クライアントが、入力された前記ワンタイムパスワードを前記認証サーバに送信するステップと、

前記認証サーバが、前記ワンタイムパスワードを前記認証要求クライアントから受信するステップと、

前記認証サーバが、受信した前記ユーザIDに関連付けられた前記クライアント識別情報および送信した前記パターンシード値に基づいて前記所定のパターン要素列生成規則により生成されるパターン要素

列から構成される提示パターンに含まれるパターン要素に受信した前記ユーザIDに関連付けられた前記ワンタイムパスワード導出ルールを適用した結果である検証コードを生成するステップと、

前記認証サーバが、受信した前記ワンタイムパスワードと生成された前記検証コードとを比較し、それらが等しい場合に前記ユーザIDに対応するユーザの認証を成功させるステップと、
を有することを特徴とする二要素ユーザ認証方法。