

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3695695号

(P3695695)

(45) 発行日 平成17年9月14日(2005.9.14)

(24) 登録日 平成17年7月8日(2005.7.8)

(51) Int. Cl.⁷

F I

G 0 6 F 15/00

G 0 6 F 15/00 3 3 0 B

G 0 6 F 1/00

G 0 6 F 9/06 6 6 0 E

H 0 4 L 9/32

H 0 4 L 9/00 6 7 3 A

請求項の数 17 (全 14 頁)

(21) 出願番号	特願2000-391720 (P2000-391720)	(73) 特許権者	500506024
(22) 出願日	平成12年12月25日(2000.12.25)		株式会社カイ・コーポレーション
(65) 公開番号	特開2002-197062 (P2002-197062A)		岐阜県多治見市滝呂町九丁目152番地の
(43) 公開日	平成14年7月12日(2002.7.12)		8
審査請求日	平成16年11月8日(2004.11.8)	(74) 代理人	100091915
早期審査対象出願			弁理士 本城 雅則
		(74) 代理人	100099106
			弁理士 本城 吉子
		(72) 発明者	田口 亮
			神奈川県横浜市保土ヶ谷区帷子町1-14
		審査官	宮司 卓佳

最終頁に続く

(54) 【発明の名称】 パスワードの生成照合システムおよびその方法

(57) 【特許請求の範囲】

【請求項1】

同一のカテゴリに属する予め選択された複数のパスワード要素を格納する要素グループ記憶手段と、

カテゴリに属する前記パスワード要素とは異なる複数のスクランブル要素を格納するスクランブル要素記憶手段と、

前記要素グループ記憶手段に格納された前記複数のパスワード要素から無作為に抽出した1つの抽出パスワード要素、および、前記スクランブル要素記憶手段に格納された複数のスクランブル要素から無作為に抽出した前記抽出パスワードと同一のカテゴリに属する予め定める個数の抽出スクランブル要素、からなる混合要素グループを生成する混合要素グループ生成手段と、

前記混合要素グループから選択パスワード要素を選択する選択手段と、

前記選択パスワード要素と前記抽出パスワード要素とを照合する照合手段と、

から構成されることを特徴とするパスワードの生成照合システム。

【請求項2】

前記選択手段は、前記混合要素グループに含まれる前記抽出パスワード要素および前記複数のスクランブル要素を順序不同に表示する表示手段をさらに含むことを特徴とする請求項1記載のパスワードの生成照合システム。

【請求項3】

前記パスワード要素および前記スクランブル要素は、画像情報であることを特徴とする

10

20

請求項 1 記載のパスワードの生成照合システム。

【請求項 4】

前記混合要素グループは電気通信回線を介して前記選択手段へ送信され、かつ、前記選択パスワード要素は前記電気通信回線を介して前記照合手段へ送信されることを特徴とする請求項 1 記載のパスワードの生成照合システム。

【請求項 5】

前記選択パスワード要素と前記抽出パスワード要素との照合が複数回行われ、その照合が全て一致した場合に認証を与えることを特徴とする請求項 1 記載のパスワードの生成照合システム。

【請求項 6】

コンピュータを、
同一のカテゴリに属する予め選択された複数のパスワード要素を格納する要素グループ記憶手段、

カテゴリに属する前記パスワード要素とは異なる複数のスクランブル要素を格納するスクランブル要素記憶手段、

前記要素グループ記憶手段に格納された前記複数のパスワード要素から無作為に抽出した 1 つの抽出パスワード要素、および、前記スクランブル要素記憶手段に格納された複数のスクランブル要素から無作為に抽出した前記抽出パスワードと同一のカテゴリに属する予め定める個数の抽出スクランブル要素、からなる混合要素グループを生成する混合要素グループ生成手段、

前記混合要素グループから選択パスワードを選択する選択手段、および

前記選択パスワード要素と前記抽出パスワード要素とを照合する照合手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 7】

前記パスワード要素および前記スクランブル要素は、画像情報であることを特徴とする請求項 6 記載のコンピュータ読み取り可能な記録媒体。

【請求項 8】

前記選択パスワード要素と前記抽出パスワード要素との照合が複数回行われ、その照合が全て一致した場合に認証を与えることを特徴とする請求項 6 記載のコンピュータ読み取り可能な記録媒体。

【請求項 9】

複数の異なるカテゴリから予め選択された選択カテゴリに属する複数の要素グループを記憶する要素グループ記憶手段であって、各要素グループはそのカテゴリに属する複数のパスワード要素から構成される、前記要素グループ記憶手段と、

前記選択カテゴリに属する複数のスクランブル要素を前記カテゴリ毎に予め記憶するスクランブル要素記憶手段と、

前記選択カテゴリから特定の数の特定カテゴリを無作為に抽出するカテゴリ抽出手段と、

前記特定カテゴリ毎に前記要素グループ記憶手段から無作為に抽出した抽出パスワード要素、および、前記特定カテゴリ毎に前記スクランブル要素記憶手段から無作為に抽出した予め定める個数の前記抽出パスワード要素と異なる抽出スクランブル要素、を混合した後、前記抽出パスワード要素および前記抽出スクランブル要素を順序不同に配列した混合要素グループを前記特定カテゴリ毎に生成する混合要素グループ生成手段と、

前記混合要素グループを表示する表示手段と、

前記表示手段に表示された前記混合要素グループから前記特定カテゴリ毎に選択パスワード要素を選択する選択手段と、

前記選択パスワード要素を前記抽出パスワード要素と前記特定カテゴリ毎に照合する照合手段と、

から構成されることを特徴とするパスワードの生成照合システム。

【請求項 10】

10

20

30

40

50

前記要素グループは、前記パスワード要素を前記特定カテゴリと関連付けて前記要素グループ記憶手段に記憶されることを特徴とする請求項 9 記載のパスワードの生成照合システム。

【請求項 1 1】

前記パスワード要素は、画像情報からなることを特徴とする請求項 9 記載のパスワードの生成照合システム。

【請求項 1 2】

前記混合要素グループ生成手段は、前記表示手段および前記選択手段と電気通信回線を介して結合されることを特徴とする請求項 9 記載のパスワードの生成照合システム。

【請求項 1 3】

前記電気通信回線は、固定電話、携帯電話およびインターネットを利用するための回線を含むことを特徴とする請求項 1 2 記載のパスワードの生成照合システム。

【請求項 1 4】

前記照合手段は、前記選択パスワード要素の全てが前記抽出パスワード要素と一致する場合、一致信号を出力することを特徴とする請求項 9 記載のパスワードの生成照合システム。

【請求項 1 5】

複数の異なるカテゴリから予め選択された選択カテゴリに属する複数の要素グループ毎に複数のパスワード要素が記憶された要素グループ記憶手段と、前記選択カテゴリに属する複数のスクランブル要素を前記カテゴリ毎に予め記憶したスクランブル要素記憶手段と、

を含むメモリを具備するコンピュータ・システムにおいて、

前記複数の要素グループから要素グループを無作為に特定する段階と、

前記特定された要素グループから無作為に抽出された抽出パスワード要素、および、前記抽出パスワード要素と同一のカテゴリに属する前記抽出パスワード要素と異なる予め定める個数の抽出スクランブル要素、を混合した後、前記抽出パスワード要素および前記抽出スクランブル要素を順序不同に配列した混合要素グループを前記カテゴリ毎に生成し前記メモリの所定の位置に格納する段階と、

前記混合要素グループを前記コンピュータに結合された表示装置上に表示する段階と、

前記表示装置上に表示された前記要素グループから前記カテゴリ毎に選択パスワード要素を選択し前記メモリの所定の位置に格納する段階と、

前記選択パスワード要素および前記抽出パスワード要素を前記メモリの所定の位置からそれぞれ読み出し、同一のカテゴリ毎に前記選択パスワード要素が前記抽出パスワード要素と一致するか否かを照合する段階と、

を実行することを特徴とするパスワードの照合方法。

【請求項 1 6】

混合要素グループを前記カテゴリ毎に生成する段階は、固定電話、携帯電話およびインターネットを利用するための電気通信回線を介して電氣的に結合された表示装置上に前記混合要素グループを送出し、前記電気通信回線を介して前記選択パスワード要素を受信する段階をさらに含むことを特徴とする請求項 1 5 記載のパスワードの照合方法。

【請求項 1 7】

前記照合する段階は、前記選択パスワード要素の全てが前記抽出パスワード要素と一致する場合、一致信号を出力する段階をさらに含むことを特徴とする請求項 1 5 記載のパスワードの照合方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、パスワードの照合を行うシステムおよびパスワードの照合を行うための方法に関し、さらに詳しくは、パスワードを構成する要素毎にその要素を選択するとともにその照合を行うシステムおよびその方法に関する。

【0002】

10

20

30

40

50

【従来の技術】

コンピュータ・システムや特定のプログラムへのアクセス、電子装置の起動、ドアの開錠等において、そのセキュリティを確保するためにパスワードが使用され、それによりその権限を有する者のみが、例えば、コンピュータ・システムへのアクセスが可能となる。パスワードは、一般に、複数のアルファベットおよび数字の組み合わせから構成される。コンピュータ・システムを利用する利用者は、予め決めたパスワードをそのシステムに登録しておき、そのシステムをアクセスする度にそのパスワードを入力する。そのシステムは、登録されたパスワードと入力されたパスワードを比較し、一致すればそのシステムへのアクセスを許す。

【0003】

不正な侵入を有効に防止するために、パスワードは、アルファベットおよび数字を複雑に組み合わせた英数文字が好ましい。しかしながら、複雑な英数文字を長期にわたって正確に記憶し続けることは困難であるので、覚えやすい英数文字の組み合わせ、例えば、自分の名前、生年月日等を含むパスワードが選択される。このようなパスワードは、不正侵入者に容易く見破られ、システムへの侵入を簡単に許すことになる。

【0004】**【発明が解決しようとする課題】**

このような欠点を回避するために、意味を有する単語、例えば、普通名称、人名、地名、国名などを含むパスワードを使用しないように推奨され、また、パスワードを定期的に変更するなどして、パスワードに対する安全性を高める。このような方策は、必然的にパスワードの使い勝手を悪くする結果となり、結局覚えやすいパスワードが選択されることになる。すなわち、パスワードに対する安全性を高めると、その使い勝手が悪くなり、逆に使い勝手を良くしようとすると、その安全性が低くなる。

【0005】

さらに、社会活動が多岐にわたるにつれ、パスワードを使用する局面が増加する。たとえば、現金自動預払機(ATM)から銀行口座をアクセスする場合、コンピュータを起動する場合、インターネットで取引を行う場合など、多くの場面でパスワードが要求される。これらの複数のパスワードを記憶し、管理することは極めて困難である。その結果、パスワードの失念、記憶違いなどにより、現金が引き出せないとか、コンピュータの起動に失敗するなどして、円滑に業務を遂行できない事態に陥るおそれがある。このような煩雑さのため、パスワード使用者は、同一のパスワードを複数のシステムに対して用いたり、複数のパスワードを紙に書き留めておくなどする。このような操作は、パスワードを設定することによって生じるシステムに対する安全性を低下させる。

【0006】

また、複雑なパスワードを管理しかつ使い分けることは、高齢者に極めて大きな負担を与えると共に、現実的ではない。情報管理社会と高齢化社会がさらに進むにつれて、高齢者にとってパスワードの管理およびその入力には大きな負担となる。

【0007】

従って、本願発明は、改善されたパスワードの生成照合システムおよびその方法を提供することを目的とする。

【0008】

また、本願発明は、パスワードの管理およびその入力に簡易なパスワードの生成照合システムおよびその方法を提供することを目的とする。

【0009】**【課題を解決するための手段】**

上記目的を達成するために、本願発明においては、異なる複数のカテゴリがまず選択され、各カテゴリに属する単数または複数のパスワード要素から構成される要素グループが要素グループ記憶手段に記憶される。利用時には、まず複数のカテゴリから無作為に予め設定された特定の数のカテゴリが選択される。次に、当該各カテゴリに属する抽出パスワード要素が要素グループ記憶手段から抽出される(一つのカテゴリに複数のパスワード要素

10

20

30

40

50

が与えられている場合には、無作為に一つを抽出する)。次にこれと同じカテゴリに属するスクランブル要素がスクランブル要素記憶手段から予め定める個数だけ無作為に抽出される。抽出されたスクランブル要素は抽出された抽出パスワード要素と混合され、その後それらの要素を順序不同に配列した混合要素グループがカテゴリ毎に生成される。この混合要素グループは表示手段上に表示される。表示された表示グループから、カテゴリ毎に選択パスワード要素が選ばれ、その選択パスワード要素は照合手段でパスワード記憶手段に記憶された抽出パスワード要素とカテゴリ毎に照合される。照合の結果、選択パスワード要素の全てが各抽出パスワード要素と一致すると、一致信号が出力される。

【0010】

また、パスワードを照合する方法を提供する本願発明は、まず予め設定してある複数のカテゴリから表示するカテゴリを選択し、当該カテゴリに属する抽出パスワード要素と、同一のカテゴリに属する抽出パスワード要素と異なるスクランブル要素を無作為に選び出し、これら二つの要素を混合した後、順序不同に配列した混合要素グループをカテゴリ毎に生成する段階、その要素グループを表示する段階、表示された要素グループからカテゴリ毎に選択パスワード要素を選択する段階、および選択パスワード要素を抽出パスワード要素と同一のカテゴリ毎に照合する段階から構成されることを特徴とする。

【0011】

【実施例】

本願発明に係るパスワードの生成照合システムは、対象とするカテゴリを生成する機能、パスワードを生成する機能、およびパスワードを照合する機能を有する。本願発明の概略として、まず、カテゴリを生成する機能について説明すると、パスワード要素を分類するカテゴリは予め利用者が設定するものであり、この数が多いほど安全上は好ましい。これは、例えば、知人の名前、生誕地、出身校名(小学校、中学校、高校、大学等)、最初の会社で最初に配属された部署名、過去居住した都市名、訪問したことのある外国、趣味、等が挙げられる。これらはシステムに記憶される。

【0012】

次に、パスワードを生成する機能について説明すると、パスワードは利用の都度無作為に抽出される複数のパスワード要素によって構成され、各パスワード要素は予めパスワード使用者によってカテゴリ毎に設定される。設定されたパスワード要素は、パスワードの生成照合システムに記憶される。

【0013】

さらに、パスワードを照合する機能に関して、このシステムは、システムが選択したカテゴリ毎に任意に抽出された抽出パスワード要素(生誕地のようカテゴリが選択されれば必然的に一つに決定されるパスワード要素もあれば、知人のように複数のパスワード要素が存在する場合もある。後者の場合、システムが無作為に抽出する。)に、無作為に抽出したスクランブル要素が加えられた混合要素グループを生成する。混合要素グループは、パスワード使用者が事前に設定し、システムが前述のとおり抽出した抽出パスワード要素と、システムが抽出した複数のスクランブル要素とから構成される。パスワード使用者は、表示装置上に表示された混合要素グループからパスワード使用者が選択した選択パスワード要素を選ぶ。各要素グループから1個の選択パスワード要素が選ばれ、全ての選択パスワード要素が適切に選択されると、システムは抽出パスワード要素と選択パスワード要素とを各カテゴリ毎に照合する。その結果、システムは、全ての選択パスワード要素が抽出パスワード要素と一致すると、パスワードを入力した者が正当な権限を有すると判断する。

【0014】

パスワード要素は、一般に文字列で表されることが多いが、特定の画像情報や音情報であってもよい。例えば、画像情報の場合、所定の形式に収められた画像をパスワード要素としてシステムに記憶させる。システムはスクランブル要素として画像を与え、表示装置上からパスワード要素を選択させることが可能である。画像情報をパスワード要素として使用する場合、本人にとって馴染みのある画像は記憶が長期に維持され、パスワードの記憶

10

20

30

40

50

・管理に適する。このように様々な形式のパスワード要素が使用できるが、パスワード要素が文字列である場合について、上記本願発明の構成を図面を用いてさらに詳しく説明する。

【0015】

図1は、本願発明に係るパスワードの生成照合システム10を示し、それは要素グループ設定部11、スクランブル要素メモリ12、混合要素グループ作成部13、入出力部14、および比較部15を含むパスワード生成照合装置16と、表示装置17および入力装置18を含むパスワード設定入力端末19と、から構成される。パスワード生成照合装置16は、パスワード設定入力端末19と有線または無線の接続回線20を介して結合される。

10

【0016】

まず、要素グループがどのようにして生成されるのかについて説明する。本願発明に係るパスワードは、利用の都度無作為に設定され、カテゴリ毎に抽出される複数のパスワード要素から構成される。各パスワード要素はパスワード使用者が任意に事前に設定し、システム10の要素グループ設定部11に記憶しておく。要素グループの生成の過程を図2に示すフロー図を参照して、説明する。

【0017】

システム10は、予め様々なカテゴリ、例えば、知人の名前、生誕地、出身校名（小学校、中学校、高校、大学等）、最初の会社で最初に配属された部署名、過去居住した都市名、訪問したことのある外国、趣味、等を含むカテゴリ1, 2, 3, …, Nを用意しており、本システムを利用する利用者は、それらの中から所望するカテゴリを可能な限り多く選択する。例えば、カテゴリ1, 3, 8, 12, …, Kが選択される。これらのカテゴリを選択すると、利用者はそのカテゴリに馴染みのある名称を入力する。例えば、カテゴリ1が知人の氏名で、前川辰夫、山田太郎および小野志郎が知人である場合、これらの氏名をパスワード要素11, 12, 13に入力する。これらのパスワード要素11, 12, 13は、要素グループ23aとして、要素グループ設定11内に格納される。同様の操作をカテゴリ3, 8, 12, …, Kに対しても行うことにより、それらのカテゴリに対するパスワード要素が入力される。なお、カテゴリ8が生誕地である場合、利用者の生誕地は1つであるので、1つのパスワード要素81が与えられる。このように、利用者が選択した全てのカテゴリ1, 3, 8, 12, …, Kに対するパスワード要素が入力されると、それらは要素グループ23a, 23b, 23c, 23d, 23eとして、要素グループ設定11内に格納される。格納されたこれらのパスワード要素は、次に述べるように各カテゴリ毎に抽出パスワード要素が混合要素グループ13によって無作為に抽出される。

20

30

【0018】

次に、パスワードを照合する機能について説明する。図3は、システム10の混合要素グループ生成部13における混合要素グループを生成する手順を説明するフロー図である。上述したように、システム10を利用する利用者が生成した要素グループ23a, 23b, 23c, 23d, 23eが既に要素グループ設定11内に格納されている。利用者がシステム10にパスワードを与え、その認証を得ようとする場合、システム10は、その利用者に対しカテゴリの問いかけ数を質問する。このカテゴリの問いかけ数は、いくつのカテゴリに対してパスワード要素を利用者に質問するかを決める数である。ここでは、例えば4を与えるとすると、システム10は要素グループ23a, 23b, 23c, 23d, 23eから、例えば、要素グループ23a, 23b, 23c, 23eを無作為に特定する。これらの特定されたカテゴリに属する要素グループは、システム10に対し利用者が認証を得ようとする度に異なる。要素グループが特定されると、混合要素グループ生成部13は、各要素グループに含まれるパスワード要素から1つを無作為に抽出し、抽出パスワード要素1, 2, 3, 4を取り出す。

40

【0019】

抽出パスワード要素1, 2, 3, 4が抽出されると、スクランブル要素メモリ12に記憶されている予め定める数の抽出パスワード要素と同じカテゴリに属するスクランブル要素

50

3 1 a , 3 1 b , 3 1 c , 3 1 d がカテゴリ毎に選び出され、抽出パスワード要素 1 , 2 , 3 , 4 とそれぞれ混合される。抽出パスワード要素 1 , 2 , 3 , 4 がスクランブル要素 3 1 a , 3 1 b , 3 1 c , 3 1 d と混合されると、それらは無作為に配列し直され、表示装置 1 7 上に表示するための混合要素グループ 3 2 a , 3 2 b , 3 2 c , 3 2 d が生成される。利用者は、表示装置 1 7 上に現れた混合要素グループの中から自分に最も馴染みのある要素を選択パスワード要素として選択する。各カテゴリに対する選択パスワード要素を入力すると、システム 1 0 は、カテゴリ毎に抽出パスワード要素と照合を行う。全て一致すると、システム 1 0 は一致信号を生成し、利用者に対し認証を与える。

【 0 0 2 0 】

次に、上記プロセスを、図 1 に示す本願発明のブロック構成図 1 0 を参照しながら、さらに詳しく説明する。まず、要素グループの設定について述べる。パスワード要素は、パスワード使用者によって入力装置 1 8 から与えられる。まず、パスワード生成照合装置 1 6 からパスワード要素を入力するカテゴリの数が問い合わされ、その数に応じたカテゴリ毎のパスワード要素が入力される。あるいは、表示装置 1 7 上にシステムが用意するカテゴリを一覧表示して、利用者が選択できるようにしてもよい。また、専用の端末装置によって要素グループを設定してもよく、特にパスワードに対し高い機密性が求められる銀行等においては必要性が高い。パスワード要素は、カテゴリ別に分けて設定されるので、例えば、カテゴリの数として 7 を入力し、カテゴリとして知人の名前、生誕地、出身校名、最初の会社で最初に配属された部署名、過去居住した都市名、訪問したことがある外国、趣味を選択する。例として、知人の名前のカテゴリにおけるパスワード要素を設定する場合、知人の名前として前川辰夫、山田太郎および小野志郎を設定する。また、過去に函館、ツサン、山形およびリヨンに住んだことがあれば、過去居住した都市名として函館、ツサン、山形およびリヨンを入力する。このように、各カテゴリに対し自分にとって最も馴染みがある名称を、パスワード要素として、カテゴリ毎に入力装置 1 8 から接続回線 2 0 を経由して要素グループ設定部 1 1 に設定しておく。

【 0 0 2 1 】

本願発明に係るパスワードは、複数のパスワード要素から構成されるが、各パスワード要素は上記したように、予め設定した要素グループの中から抽出される。図 4 は、このようにして抽出されたパスワード 4 0 の構成を概念的に示すもので、抽出されたパスワード要素とその属するカテゴリ番号 4 1 , 4 2 , 4 3 , 4 4 が一対で要素グループ設定部 1 1 に格納される。カテゴリ番号は、後述するスクランブル要素の選択の際に用いられる。パスワード 4 0 を構成するパスワード要素の組み合わせは、システム 1 0 に対し利用者が認証を得ようとする度に異なる点に注意されたい。

【 0 0 2 2 】

次に、パスワードの入力および照合について説明する。システム 1 0 の混合要素グループ生成部 1 3 は、パスワードを入力する利用者に対しカテゴリの問いかけ数を質問する。例えば、カテゴリ数として 4 を入力装置 1 8 から入力すると、混合要素グループ生成部 1 3 は予め設定されている要素グループのカテゴリから 4 つのカテゴリを無作為に選ぶ。例えば、知人の氏名、生誕地、通学した小学校名、所属部署名のカテゴリを選び、さらに各カテゴリに設定されているパスワード要素から無作為に抽出パスワード要素を抽出する。混合要素グループ生成部 1 3 は、抽出パスワード要素とそのパスワード要素と同じカテゴリに属する複数のスクランブル要素をスクランブル要素メモリ 1 2 から抽出し、抽出パスワード要素と混合して順序不同に配列した混合要素グループを生成する。例えば、要素グループ作成部 1 3 は、要素グループ設定部 1 1 から抽出パスワード要素である山田太郎を取り出す。図 4 に示すように、山田太郎に対してカテゴリ番号 1 が付与されているので、要素グループ作成部 1 3 は、山田太郎が知人の氏名であることを認識すると、スクランブル要素メモリ 1 2 に格納されている氏名から所定数の氏名、例えば斎藤志郎、小川肇、市川義彦、加藤徹がスクランブル要素として無作為に選び出される。選び出されたスクランブル要素はパスワード要素と混合され、順序不同に並び替えられて、混合要素グループが作成される。このようにして、各カテゴリに対して作成された混合要素グループは、表示装

10

20

30

40

50

置 16 に送られる。

【 0023 】

図 5 (1) - (4) は、表示装置 16 上に表示した知人の氏名、生誕地、通学した小学校、所属部署名の各カテゴリ別の混合要素グループの例を示す。パスワード使用者は、表示装置 16 に表示された混合要素グループを参照して、所定のパスワード要素を選択して入力装置 17 から番号を入力する。例えば、知人の氏名のカテゴリにおいて、パスワード使用者は、予め選んだパスワード要素が山田太郎であるから、山田太郎を選択パスワード要素として番号 4 を入力装置に入力する。また、図 5 (2) に示すように、生誕地のカテゴリでは横浜を、さらに図 5 (3) の小学校では保土ヶ谷小学校を、最後に図 5 (4) における所属部署ではサプライ・マネジメント部をそれぞれ選択パスワード要素として選択する。これらの選択した選択パスワード要素は、接続回線 20 を経由して照合部 15 に送られ、要素グループ設定部 11 に格納されている抽出パスワード要素とそれぞれ比較される。比較の結果、全ての選択パスワード要素と抽出パスワード要素が一致すると、一致 / 不一致信号 21 が外部に出力される。この信号はパスワードの認証結果を利用する他の装置に送られる。

10

【 0024 】

次に、図 6 を参照すると、スクランブル要素メモリ 12 内にカテゴリ別に格納されたスクランブル要素が示される。上述したように、混合要素グループを作成する際に、所定数のスクランブル要素を無作為に抽出するために、可能な限り多くの候補となるスクランブル要素がカテゴリ別に予め準備される。すなわち、1つのスクランブル要素に対してカテゴリ番号とシリアル番号が付与され、メモリ 12 内に格納される。カテゴリは、氏名、生誕地など同じ意味を有する単語であり、シリアル番号は、スクランブル要素を無作為に選択する際に使用される連続番号である。カテゴリ 1 に属する単語はスクランブル要素 S E 1 1 ・ ・ ・ S E 1 7 ・ ・ ・ の順に配列され、カテゴリ 2 に属する単語はスクランブル要素 S E 2 1 ・ ・ ・ S E 2 7 ・ ・ ・ の順に配列される。例えば、カテゴリ 1 のスクランブル要素を抽出する場合、乱数発生により 5 が生成されると、その番号に対応するスクランブル要素 S E 1 5 が選び出される。このように選び出された所定数のスクランブル要素は要素グループ作成部 13 に送られる。カテゴリ 2 , 3 に対しても同様の処理が実行される。

20

【 0025 】

次に、パスワードの生成照合システムにおいて、パスワード使用者がパスワード要素を設定する手順を、図 7 に示すフローチャート 70 に従って説明する。パスワードの生成照合システム 10 が、パスワード要素の生成モードに入ると、まずブロック 71 において、要素グループの問いかけ数および要素グループの選択肢の数を設定する。要素グループの問いかけ数は、複数あるカテゴリの数のうち、利用時に問いかけに用いるカテゴリの数であり、上述した例では、4つであり、要素グループの選択肢の数は、図 5 に見られるように、5つである。この実施例では、ブロック 71 において要素グループ数および要素グループの選択肢数が問い合わされるが、システムがそのデフォルト値 (予め設定した値) を有していてもよい。要素グループ数および要素グループの選択肢数が設定されると、ブロック 72 において、要素グループのカテゴリが選択される。パスワード使用者は、ブロック 71 で選択した要素グループ数の範囲内で、希望するカテゴリを選択することができる。この選択は、システムが表示装置 16 上に予め用意したカテゴリを列挙し、パスワード使用者がその列挙されたカテゴリから選択できるようにしてもよい。上記例では知人の氏名、生誕地、通学した小学校および所属部署名が選択される。

30

40

【 0026 】

希望するカテゴリが設定されると、ブロック 73 に進み、各カテゴリに対するパスワード要素が入力される。例えば、知人のカテゴリに対しては山田太郎その他、複数の知人名が入力される。ブロック 74 に進むと、全てのカテゴリに対してパスワード要素が入力されたか否かが判断される。残余がある場合、処理はブロック 73 へ戻り、上述したのと同様の処理が実行される。全てのカテゴリに対するパスワード要素が入力されると、処理はブロック 75 へ進む。

50

【 0 0 2 7 】

ブロック 7 5 で、表示装置 1 6 は入力した全てのパスワード要素をカテゴリ別に表示するとともに、修正したいパスワード要素が存在する場合、ブロック 7 7 においてパスワード使用者はパスワード要素を修正する。ブロック 7 6 で表示されたパスワード要素が全て問題がなく、あるいはブロック 7 7 でパスワード要素の修正が完了すると、処理はブロック 7 8 に進み、パスワード使用者は、再度設定したパスワード要素をカテゴリ別に入力し、パスワード使用者の入力が正確であるのかどうかの確認をとる。この確認が終了すると、パスワード生成照合装置 1 5 は、パスワード要素の入力およびその設定を完了する。

【 0 0 2 8 】

次に、パスワードを照合する手順を図 8 に示すフローチャート 8 0 に従って説明する。まず、照合システム 1 5 が起動され、照合モードに入ると、ブロック 8 1 において、図 4 に示されるような要素グループが表示装置 1 6 上にカテゴリ別に示される。ブロック 8 2 へ進み、パスワード使用者は、表示装置 1 6 上に示された項目から所望する番号を入力装置 1 7 のキーパッドから入力する。例えば、知人の氏名のカテゴリでは、山田太郎がこのカテゴリの選択パスワード要素であると判断するならば、キーパッドの 4 を押す。あるいは、カーソルをスクロールして当該個所を選択する方法もある。選択パスワード要素が入力されると、ブロック 8 3 でその選択パスワード要素はメモリに記憶される。ブロック 8 4 へ進み、全ての選択パスワード要素が入力されたかどうか判断され、もしそうでない場合は、ブロック 8 1 へ進み、上記した同じ処理が実行される。

【 0 0 2 9 】

ブロック 8 4 で、全ての選択パスワード要素が入力されると、処理はブロック 8 5 へ移り、予め抽出された抽出パスワード要素と入力された選択パスワード要素とがそれぞれ照合される。全ての選択パスワード要素が抽出パスワード要素と一致する場合、ブロック 8 7 で一致信号が出力され、少なくとも 1 つの選択パスワード要素が抽出パスワード要素と一致しない場合、不一致信号が出力される。

【 0 0 3 0 】

上述したように、パスワード入力端末 1 8 から入力された選択パスワード要素は予め設定された抽出パスワード要素と比較され、全ての抽出パスワード要素に対して一致する場合に、パスワード使用者に認証を与えることが可能となる。

【 0 0 3 1 】

なお、図 7 に示す手順では、選択パスワード要素が全て入力された後に予め抽出された抽出パスワード要素との照合が開始するが、選択パスワード要素入力される度に抽出パスワード要素と比較するようにしてもよい。この場合、一致しない選択パスワード要素が入力された段階で、照合モードを終了し、選択パスワード要素を入力する者に対し、パスワードの入力エラーがあったことを表示するようにしてもよい。また、ブロック 8 8 で、不一致信号が出力されるが、特にこの処理を必要とするものではなく、ブロック 8 7 の一致信号のみを外部に出力するだけでもよい。

【 0 0 3 2 】

本願発明に係るパスワードの生成照合システムは、様々な装置またはシステムに適用することが可能で、それによりそれらの装置またはシステムの安全性を向上させることができる。図 8 は、銀行 9 1 内に設置されたコンピュータ・システム 9 2 に本願発明に係るパスワードの生成照合システム 9 3 を適用した場合のブロック構成図を示す。コンピュータ・システム 9 2 は、銀行業務を処理する装置で、一般に専用または一般回線を含む有線または無線回線 9 4 によって遠隔地に設置された端末装置 9 5 に結合される。端末装置 9 5 は、多くは現金自動預払機 (A T M) であるが、近年インターネットあるいは日本の N T T が運営する i モードの普及により固定電話または携帯電話に接続された家庭内のコンピュータ端末であってもよい。端末装置 9 5 からコンピュータ・システム 9 2 にアクセスする場合、パスワードの生成照合システム 9 3 は予め設定されたパスワードと端末装置 9 5 から送られたパスワードが一致するかどうか照合する。本願発明に従えば、コンピュータ・システム 9 2 に格納されたパスワード要素が端末装置 9 5 から送られた選択パスワード要

10

20

30

40

50

素の全てが一致するかどうか判断する。全て一致する場合、コンピュータ・システム 9 2 は端末装置 9 5 を操作する者に正当な権限を有する者としての認証を与える。この認証により端末装置 9 5 はコンピュータ・システム 9 2 に結合され、様々なランザクションを指示することが可能となる。

【 0 0 3 3 】

上記実施例は、銀行内のコンピュータ・システムに対する安全性を向上させるために本願発明を適用するが、端末装置を操作する者が正当な権限を有するかどうか認証する必要がある公的機関のコンピュータ・システムに適用することも可能である。

【 0 0 3 4 】

また、遠隔地から会社または自宅内のコンピュータに有線または無線回線を介してアクセスする場合においても、本願発明を適用してシステムの安全性の向上を図ることが可能である。特に、出張先の事務所やホテルなどから会社または自宅コンピュータに接続し、比較的低廉な費用で必要な情報を送受信することができる。

【 0 0 3 5 】

さらに、立ち入りを制限されているエリア、例えば、住居、金庫、工場、研究所、防衛施設等を管理するために、出入口の施錠および開錠を制御するコンピュータに適用することができる。

【 0 0 3 6 】

また、特定の車両、機械、装置（自動車、建設機械、農耕機械、工場機械などを含む）は、許可された者のみに操縦を許されることがある。このような場合、本人かどうかの確認のために、本願発明を装置等の稼動用鍵に適用することが可能である。

【 0 0 3 7 】

以上のように、本願発明は、基本的にパスワードによる本人確認を必要とする状況において、適用することが可能である。特に、本願発明は、複数のパスワード要素を用い、各パスワード要素は本人にとって馴染みのある数字や単語、あるいは画像情報、音情報などによって選択することができるので、従来の方法と異なり馴染みのないパスワードを常に記憶するための努力を払う必要がない。

【 0 0 3 8 】

一方、カテゴリの抽出、正しいパスワード要素の抽出、さらにはスクランブル要素はシステムが無作為に行う（ただし、パスワード要素によってはカテゴリが決まった時点で一義的に決まるものもある。例、生誕地）。これにより、無秩序度が極めて高く、よって予測可能性が極めて低い。すなわち、一定の期間パスワードが固定されている通常の静的なパスワードに較べると、極めて動的である。従って、応答時間に一定の制限を設け、それが経過して入力がない場合は検証を拒否する等の方法を用いれば、例えば設定済みのカテゴリとパスワード要素が全て他人に流出したとしても、本人並に迅速に正答することは極めて困難であり、安全性が高い。

【 図面の簡単な説明 】

【 図 1 】 本願発明に係るパスワードの生成照合システムのブロック構成図を示す。

【 図 2 】 本願発明に係る要素グループを生成する手順を説明するためのフロー図である。

【 図 3 】 本願発明に係る混合要素グループを生成する手順を説明するためのフロー図である。

【 図 4 】 本願発明に係るパスワードの概念を説明するための図である。

【 図 5 】 表示装置上に表示される要素グループの表示例を示す図である。

【 図 6 】 スクランブル要素メモリ内にカテゴリ別に格納されたスクランブル要素を示す図である。

【 図 7 】 本願発明に係るパスワード要素の生成手順を示すフローチャートを示す。

【 図 8 】 本願発明に係るパスワードの照合手順を示すフローチャートを示す。

【 図 9 】 本願発明に係るパスワードの生成照合システムを利用する一実施例を示すブロック構成図を示す。

10

20

30

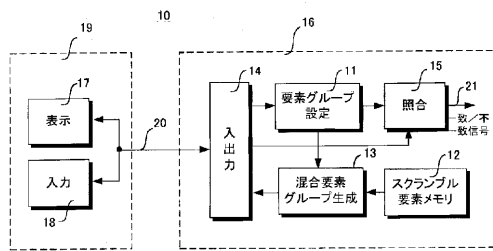
40

50

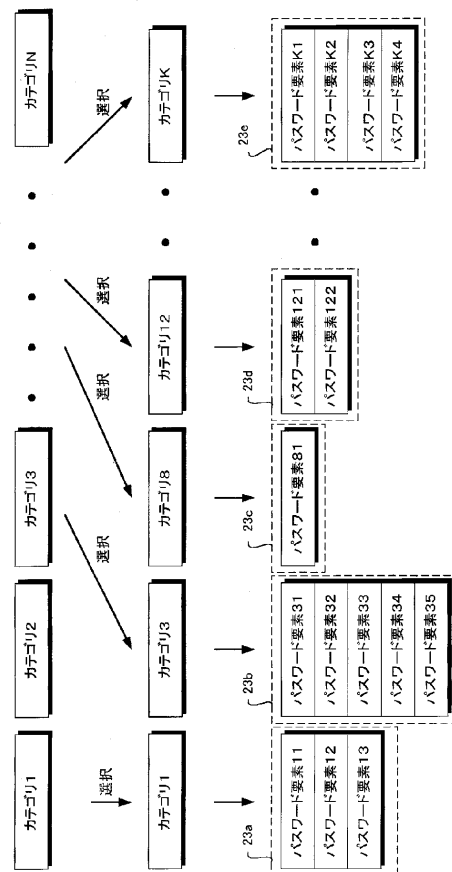
【符号の説明】

- 10：パスワードの生成照合システム
- 11：要素グループ設定部
- 12：スクランブル要素メモリ
- 13：混合要素グループ生成部
- 14：入出力部
- 15：照合部
- 16：パスワード生成照合装置
- 17：表示装置
- 18：入力装置
- 19：パスワード設定入力端末
- 20：接続回線
- 21：一致／不一致信号
- 23 a, 23 b, 23 c, 23 d, 23 e：要素グループ
- 31 a, 31 b, 31 c, 31 d：スクランブル要素
- 32 a, 32 b, 32 c, 32 d：混合要素グループ

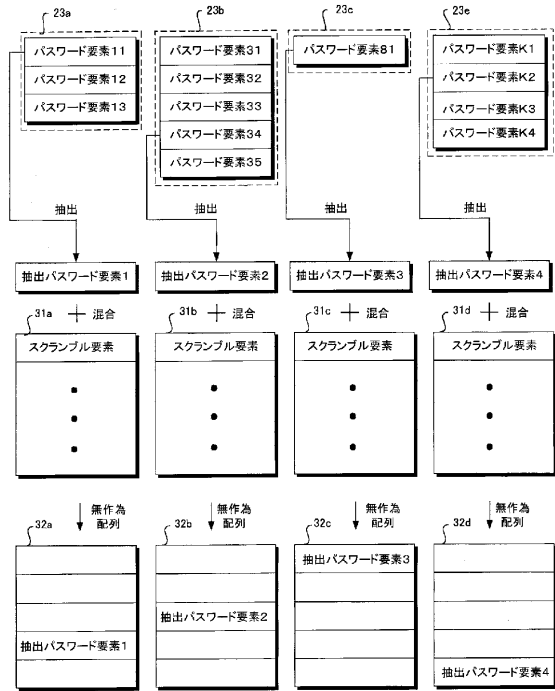
【図1】



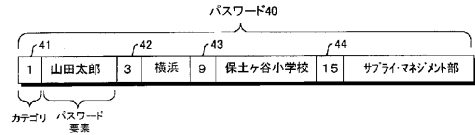
【図2】



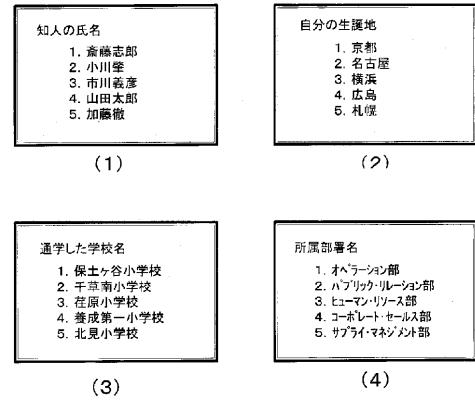
【 図 3 】



【 図 4 】



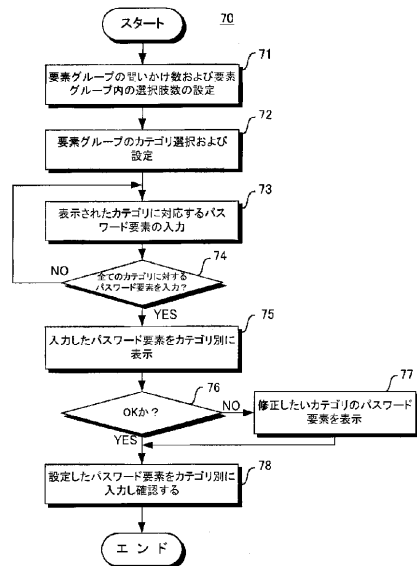
【 図 5 】



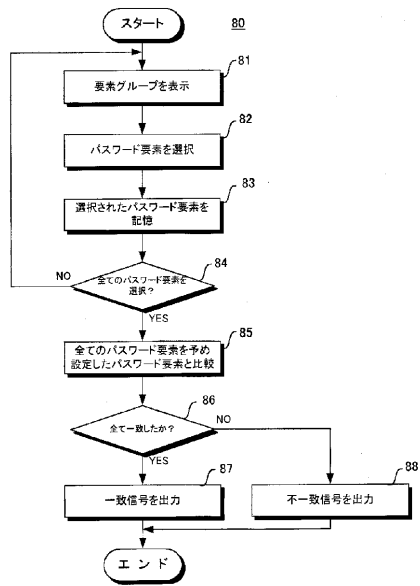
【 図 6 】

カテゴリ No.	シリアル No.	スクランブル要素	SE	カテゴリ No.	シリアル No.	スクランブル要素	SE	カテゴリ No.	シリアル No.	スクランブル要素	SE	...
1	1	SE11	2	1	SE21	3	1	SE31
1	2	SE12	2	2	SE22	3	2	SE32
1	3	SE13	2	3	SE23	3	3	SE33
1	4	SE14	2	4	SE24	3	4	SE34
1	5	SE15	2	5	SE25	3	5	SE35
1	6	SE16	2	6	SE26	3	6	SE36
1	7	SE17	2	7	SE27	3	7	SE37
*	*	...	*	*	...	*	*
*	*	...	*	*	...	*	*
*	*	...	*	*	...	*	*

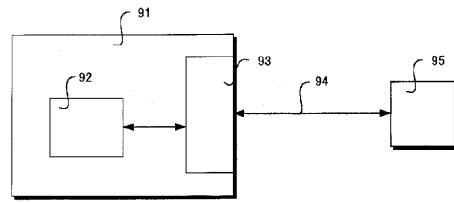
【 図 7 】



【 図 8 】



【 図 9 】



フロントページの続き

- (56)参考文献 特開平02 - 024775 (JP, A)
特開平09 - 330011 (JP, A)
特表平07 - 502351 (JP, A)
特開平04 - 326409 (JP, A)
特開平09 - 127976 (JP, A)

- (58)調査した分野(Int.Cl.⁷, DB名)
G06F15/00, G06F1/00
H04L9/00