(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-33924
(P2008-33924A)
(43)公開日　平成20年2月14日(2008.2.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330E	5B020
G06F 3/02	(2006.01)	G06F	3/02	370A	5B285
G06F 3/023	(2006.01)	G06F	3/023	310L	5E501
H03M 11/04	(2006.01)	G06F	3/048	654A	
G06F 3/048	(2006.01)				

審査請求 未請求　請求項の数 21　ＯＬ　（全 21 頁）

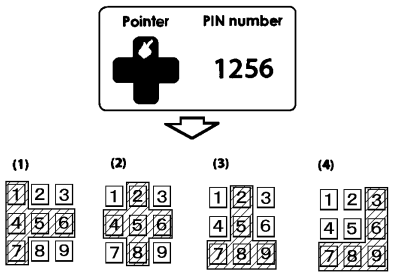
(21)出願番号　特願2007-175073 (P2007-175073)
(22)出願日　平成19年7月3日 (2007.7.3)
(31)優先権主張番号　特願2006-184996 (P2006-184996)
(32)優先日　平成18年7月4日 (2006.7.4)
(33)優先権主張国　日本国 (JP)

(71)出願人　301021533
独立行政法人産業技術総合研究所
東京都千代田区霞が関１－３－１
(72)発明者　高田　哲司
東京都千代田区霞が関１－３－１　独立行政法人産業技術総合研究所内

Ｆターム(参考)　5B020 AA01 CC12 DD02 DD30 FF17 FF53 GG15
5B285 AA01 BA02 CB02 CB04
5E501 AA09 AC42 BA08 BA20 CA04 CB02 CB05 CB09 EA10 EA11 FA03 FA04 FA23 FB28 FB43

(54)【発明の名称】フェイクポインタによる暗証番号入力装置および暗証番号入力方法

(57)【要約】
【課題】　複数の入力キーを同時に選択指示するフェイクポインタにより暗証番号の入力を行い、暗証番号の認証を行う暗証番号入力装置を提供する。
【解決手段】　複数の入力キーを同時に選択指示するフェイクポインタをキーボードに表示する表示処理手段と、フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるように入力手段による入力操作により制御されて前記ポインタの位置を制御するポインタ位置制御手段と、ポインタ位置制御手段により制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報により定められたデータを入力する入力処理手段と、入力処理手段によるデータの入力を受け付け、所定の文字数のデータを受け付けると、予め記憶された暗証番号と比較を行い、暗証番号を認証するデータ処理手段とを備える。
【選択図】　図３



【特許請求の範囲】
【請求項１】
キーボードを表示する表示手段と、前記キーボードの中の入力キーを指示して入力操作を行う入力手段と、データ処理を行うデータ処理手段とを備えた情報処理装置において、暗証番号を入力し暗証番号の認証を行う暗証番号入力装置であって、
前記キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタを当該キーボードに表示する表示処理手段と、
前記フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるように前記入力手段による入力操作により制御されて前記ポインタの位置を制御するポインタ位置制御手段と、
前記ポインタ位置制御手段により制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報により定められたデータを入力する入力処理手段と、
前記入力処理手段によるデータの入力を受け付け、所定の文字数のデータを受け付けると、予め記憶された暗証番号と比較を行い、暗証番号を認証するデータ処理手段と
を備えたことを特徴とする暗証番号入力装置。
【請求項２】
請求項１に記載の暗証番号入力装置において、
暗証番号認証の開始時に、前記表示処理手段が、前記フェイクポインタの形状を選択するための選択画面を表示し、前記入力手段の入力操作に基づいて、フェイクポインタの形状が複数の所定のパターンの中から選択される
ことを特徴とする暗証番号入力装置。
【請求項３】
請求項１に記載の暗証番号入力装置において、
前記入力処理手段は、前記ポインタ位置制御手段により制御されたポインタにより選択指示された複数の入力キーの中からポインタの形状に応じて所定の位置の入力キーのデータを入力する
ことを特徴とする暗証番号入力装置。
【請求項４】
請求項１に記載の暗証番号入力装置において、
暗証番号認証の開始時に、前記表示処理手段が、前記フェイクポインタの形状を選択するための選択画面を表示し、前記入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択し、
選択されたフェイクポインタの形状に応じた所定の位置の入力キーが、前記入力処理手段により入力される入力キーのデータとする
ことを特徴とする暗証番号入力装置。
【請求項５】
請求項２に記載の暗証番号入力装置において、
前記フェイクポインタとしてテンキーパターンが選択された場合には、前記表示処理手段が、回答選択情報を取得するための選択画面を表示し、前記入力手段の入力操作に基づいて、ユーザが取得した回答選択情報が決定され、前記入力処理手段は、前記ポインタ位置制御手段により位置移動されたフェイクポインタにより選択指示された複数の入力キーの中から前記回答選択情報に基づくデータを入力する
ことを特徴とする暗証番号入力装置。
【請求項６】
請求項５に記載の暗証番号入力装置において、
前記回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、
前記フェイクポインタの位置移動操作により、テンキーパターンの数字配置が、前記ポインタ位置制御手段により位置移動される
ことを特徴とする暗証番号入力装置。

【請求項７】
請求項５に記載の暗証番号入力装置において、
前記回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、
前記フェイクポインタの位置移動操作により、テンキーの各数字キーの背景に表示される図形が、前記ポインタ位置制御手段により位置移動される
ことを特徴とする暗証番号入力装置。
【請求項８】
キーボードを表示する表示手段と、前記キーボードの中の入力キーを指示して入力操作を行う入力手段と、データ処理を行うデータ処理手段とを備えた情報処理装置において、暗証番号を入力し暗証番号の認証を行う暗証番号入力方法であって、
表示処理手段により、前記キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタを当該キーボードに表示し、
ポインタ位置制御手段により、前記フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるように前記入力手段による入力操作により制御されて前記ポインタの位置を制御し、
入力処理手段により、前記ポインタ位置制御手段により制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報により定められたデータを入力し、
データ処理手段により、入力されたデータを受け付け、所定の文字数のデータを受け付けると、予め記憶された暗証番号と比較を行い、暗証番号を認証する
ことを特徴とする暗証番号入力方法。
【請求項９】
請求項８に記載の暗証番号入力方法において、
暗証番号認証の開始時に、表示処理手段により、前記フェイクポインタの形状を選択するための選択画面を表示し、前記入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択される
ことを特徴とする暗証番号入力方法。
【請求項１０】
請求項８に記載の暗証番号入力方法において、
入力処理手段により、ポインタ位置制御手段により制御されたポインタにより選択指示された複数の入力キーの中からポインタの形状に応じて所定の位置の入力キーのデータを入力する
ことを特徴とする暗証番号入力方法。
【請求項１１】
請求項８に記載の暗証番号入力方法において、
暗証番号認証の開始時に、表示処理手段により、前記フェイクポインタの形状を選択するための選択画面を表示し、入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択し、
選択されたフェイクポインタの形状に応じた所定の位置の入力キーが、前記入力処理手段により入力される入力キーのデータとする
ことを特徴とする暗証番号入力方法。
【請求項１２】
請求項９に記載の暗証番号入力方法において、
前記フェイクポインタとしてテンキーパターンが選択された場合には、前記表示処理手段が、回答選択情報を取得するための選択画面を表示し、前記入力手段の入力操作に基づいて、ユーザが取得した回答選択情報が決定され、前記入力処理手段は、前記ポインタ位置制御手段により位置移動されたフェイクポインタにより選択指示された複数の入力キーの中から前記回答選択情報に基づくデータを入力する
ことを特徴とする暗証番号入力方法。
【請求項１３】

請求項１２に記載の暗証番号入力方法において、
前記回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、
前記フェイクポインタの位置移動操作により、テンキーパターンの数字配置が、前記ポインタ位置制御手段により位置移動される
ことを特徴とする暗証番号入力方法。
【請求項１４】
請求項１２に記載の暗証番号入力方法において、
前記回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、
前記フェイクポインタの位置移動操作により、テンキーの各数字キーの背景に表示される図形が、前記ポインタ位置制御手段により位置移動される
ことを特徴とする暗証番号入力方法。
【請求項１５】
キーボードを表示する表示手段と、前記キーボードの中の入力キーを指示して入力操作を行う入力手段と、データ処理を行うデータ処理手段とを備えた情報処理装置において、暗証番号を入力し暗証番号の認証を行う暗証番号入力処理をコンピュータにより実行するプログラムであって、
前記キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタを当該キーボードに表示する表示処理手段と、
前記フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるように前記入力手段による入力操作により制御されて前記ポインタの位置を制御するポインタ位置制御手段と、
前記ポインタ位置制御手段により制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報により定められたデータを入力する入力処理手段と、
前記入力処理手段によるデータの入力を受け付け、所定の文字数のデータを受け付けると、予め記憶された暗証番号と比較を行い、暗証番号を認証するデータ処理手段
としてコンピュータを機能させるプログラム。
【請求項１６】
請求項１５に記載のプログラムにおいて、
暗証番号認証の開始時に、前記表示処理手段が、前記フェイクポインタの形状を選択するための選択画面を表示し、前記入力手段の入力操作に基づいて、フェイクポインタの形状が複数の所定のパターンの中から選択される
ことを特徴とするプログラム。
【請求項１７】
請求項１５に記載のプログラムにおいて、
前記入力処理手段は、前記ポインタ位置制御手段により制御されたポインタにより選択指示された複数の入力キーの中からポインタの形状に応じて所定の位置の入力キーのデータを入力する
ことを特徴とするプログラム。
【請求項１８】
請求項１５に記載のプログラムにおいて、
暗証番号認証の開始時に、前記表示処理手段が、前記フェイクポインタの形状を選択するための選択画面を表示し、前記入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択し、
選択されたフェイクポインタの形状に応じた所定の位置の入力キーが、前記入力処理手段により入力される入力キーのデータとする
ことを特徴とするプログラム。
【請求項１９】
請求項１６に記載のプログラムにおいて、
前記フェイクポインタとしてテンキーパターンが選択された場合には、前記表示処理手

段が、回答選択情報を取得するための選択画面を表示し、前記入力手段の入力操作に基づいて、ユーザが取得した回答選択情報が決定され、前記入力処理手段は、前記ポインタ位置制御手段により位置移動されたフェイクポインタにより選択指示された複数の入力キーの中から前記回答選択情報に基づくデータを入力する
ことを特徴とするプログラム。
【請求項２０】
請求項１９に記載のプログラムにおいて、
前記回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、
前記フェイクポインタの位置移動操作により、テンキーパターンの数字配置が、前記ポインタ位置制御手段により位置移動される
ことを特徴とするプログラム。
【請求項２１】
請求項１９に記載のプログラムにおいて、
前記回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、
前記フェイクポインタの位置移動操作により、テンキーの各数字キーの背景に表示される図形が、前記ポインタ位置制御手段により位置移動される
ことを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタにより暗証番号の入力を行い、暗証番号の認証を行う暗証番号入力装置および暗証番号入力方法に関するものである。
【背景技術】
【０００２】
個人認証において、覗き見攻撃に対する対策は急務である。個人認証における秘密情報の入力作業は、第三者に見られない環境で行うことが望ましいが、それは非現実的であると言わざるをえない。日本では、２００５年末から２００６年初頭にかけて銀行ＡＴＭにおける盗撮事件が発生し、この脅威は広く知れ渡ることとなった。最近では、画像を用いた認証手法（非特許文献１，非特許文献２）が提案されているが、これらにおいても覗き見対策は課題の１つとなっている。これまで、これに対する既存の対策手法は、プライバシーフィルタや遮蔽板の取り付けといった物理的な対策方法が主流である。しかし、すべての認証端末にこれらの対策を行うのは困難である。
【０００３】
従来から画像認証の分野でいくつか提案されている「覗き見攻撃」に対する対策手法を紹介すると、例えば、非特許文献３においては、画像認証で使われる画像に画像処理を施すことで、一見しただけではなんの画像かわからないようにして認証に使用する方法を提案している。正規ユーザは、原画像からその不鮮明化画像に至るまでの画像処理の過程を見ることで、その不鮮明化画像を記憶することができ、結果として認証時にはそれを正確に判別することが可能になる。ユーザ評価により、複数枚の画像群の中からパスワード画像の判別が可能であることを実証している。しかし、被験者が限定されているため、結果は普遍的とは言い難く、長期記憶や利便性の面からも疑問点が残されているといわざるを得ない。
【０００４】
非特許文献４において紹介される手法は、事前にpass-objectと呼ばれる特定のアイコンを複数個決めておき、認証時には画面に３つのpass-objectが表示されるので、そのpass-objectで構成される三角形の内部にあるアイコンを回答として選択する。これを複数回行い、すべての回答があっていれば認証成功とする手法である。
【０００５】
この手法はChallenge & Response になっており、かつ正解を直接選択しないという点

で優れているが、多数（数百～数千）のobjectが画面に表示されることが前提となるため、pass-objectの識別が容易とは言い難く、認証時間も長くなることが予測される。また、pass-objectの数やその配置にも依存するが、画面の中心を回答として選び続けることで認証に成功する可能性が高くなるという可能性もある（非特許文献５参照）。

【０００６】

また、この種の暗証番号入力装置の技術に関係する特許文献としては、特許文献１～特許文献５が参照できる。いずれも、暗証番号の入力方法を工夫して、覗き見攻撃に対する対策を提案している。

【特許文献１】特開２００１－１４７７６３号公報

【特許文献２】特開２０００－３３９０８４号公報

【特許文献３】特開平０５－３３４３３４号公報

【特許文献４】特開平０９－２９７８７５号公報

【特許文献５】特開２００２－２８７８７１号公報

【非特許文献１】Rachna Dhamijaand Adrian Perrig: Deja Vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, Aug (2003).http://www.sims.berkeley.edu/%7erachna/dejavu/site accessed at Apr 17, 2006.

【非特許文献２】高田哲司, 小池英樹: あわせ絵: 画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法, 情報処理学会論文誌, Vol.44, No.8, pp.2002{2012, (2003).

【非特許文献３】原田篤史, 漁田武雄, 水野忠則, 西垣正勝: 画像記憶のスキーマを利用したユーザ認証システム, 情報処理学会論文誌, Vol.46, No.8, pp.1997{2013, (2005).

【非特許文献４】L.Sobrado andJ.-C. Birget: Graphical passwords, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, (2002).http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htmsite accessed at Apr 17, 2006.

【非特許文献５】S. Man, D. hong and M. Mathews: A shoulder-surfingresistant graphical password scheme - WIW, in proceedings of International Conference on Security and Management, Las Vegas, NV, (2003).

【発明の開示】

【発明が解決しようとする課題】

【０００７】

従来においては、これらの特許文献１～５、非特許文献１～５などに見られるように、暗証番号の入力装置、または暗証番号認証のための入力装置に対して、これまでに「覗き見攻撃」に対する対策が様々に提案されているが、十分な対策となっていないという問題がある。

【０００８】

そこで、本発明では、例えば、画面に表示される選択肢から正解を選択するという入力操作を行う認証を対象とし、覗き見攻撃に対する安全性を改善する手法として、フェイクポインタを用いる手法を提案する。本発明のフェイクポインタを用いる手法では、ユーザが秘密情報（暗証番号）を選択する手法として正解を直接選択するのではなく、フェイクポインタと呼ぶポインタの操作により正解を選択する。フェイクポインタでは、常に複数の回答候補を選択する状態となっているので、第三者が認証行為をのぞき見たとしても、それによりユーザの秘密情報が特定されるという事態を回避することが可能となる。

【０００９】

具体的には、本発明の目的は、キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタにより暗証番号の入力を行い、暗証番号の認証を行う暗証番号入力装置および暗証番号入力方法を提供することにある。

【課題を解決するための手段】

【００１０】

上記のような目的を達成するため、本発明は、第１の態様として、本発明による暗証番

号入力装置が、キーボードを表示する表示手段と、キーボードの中の入力キーを指示して入力操作を行う入力手段と、データ処理を行うデータ処理手段とを備えた情報処理装置において、暗証番号を入力し暗証番号の認証を行う暗証番号入力装置であって、キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタを当該キーボードに表示する表示処理手段と、フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるように入力手段による入力操作により制御されてポインタの位置を制御するポインタ位置制御手段と、ポインタ位置制御手段により制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報により定められたデータを入力する入力処理手段と、入力処理手段によるデータの入力を受け付け、所定の文字数のデータを受け付けると、予め記憶された暗証番号と比較を行い、暗証番号を認証するデータ処理手段を備える構成とされる。

【００１１】

この場合に、本発明による暗証番号入力装置においては、暗証番号認証の開始時に、表示処理手段が、フェイクポインタの形状を選択するための選択画面を表示し、入力手段の入力操作に基づいて、フェイクポインタの形状が複数の所定のパターンの中から選択されるように構成される。

【００１２】

本発明による暗証番号入力装置において、入力処理手段は、ポインタ位置制御手段により制御されたポインタにより選択指示された複数の入力キーの中からポインタの形状に応じて所定の位置の入力キーのデータを入力するように構成される。

【００１３】

また、本発明による暗証番号入力装置が、暗証番号認証の開始時に、表示処理手段が、フェイクポインタの形状を選択するための選択画面を表示し、入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択し、選択されたフェイクポインタの形状に応じた所定の位置の入力キーが、入力処理手段により入力される入力キーのデータとするように構成されてもよい。

【００１４】

本発明の暗証番号入力装置において、フェイクポインタとしてテンキーパターンが選択された場合には、表示処理手段が、回答選択情報を取得するための選択画面を表示し、入力手段の入力操作に基づいて、ユーザが取得した回答選択情報が決定され、入力処理手段は、ポインタ位置制御手段により位置移動されたフェイクポインタにより選択指示された複数の入力キーの中から回答選択情報に基づくデータを入力するように構成される。

【００１５】

この場合に、回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、フェイクポインタの位置移動操作により、テンキーパターンの数字配置が、ポインタ位置制御手段により位置移動されるように構成される。

【００１６】

また、回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、フェイクポインタの位置移動操作により、テンキーの各数字キーの背景に表示される図形が、ポインタ位置制御手段により位置移動されるように構成されても良い。

【００１７】

また、本発明は、第２の態様として、本発明による暗証番号入力方法が、キーボードを表示する表示手段と、キーボードの中の入力キーを指示して入力操作を行う入力手段と、データ処理を行うデータ処理手段とを備えた情報処理装置において、暗証番号を入力し暗証番号の認証を行う暗証番号入力方法であって、表示処理手段により、キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタを当該キーボードに表示し、ポインタ位置制御手段により、フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるように入力手段による入力操作により制御されてポインタの位置を制御し、入力処理手段により、ポインタ位置制御手段により制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報

により定められたデータを入力し、データ処理手段により、入力されたデータを受け付け、所定の文字数のデータを受け付けると、予め記憶された暗証番号と比較を行い、暗証番号を認証するように構成される。

【００１８】

この場合に、本発明による暗証番号入力方法においては、暗証番号認証の開始時に、表示処理手段により、フェイクポインタの形状を選択するための選択画面を表示し、入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択される。また、入力処理手段により、ポインタ位置制御手段により制御されたポインタにより選択指示された複数の入力キーの中からポインタの形状に応じて所定の位置の入力キーのデータを入力するように構成される。

【００１９】

また、本発明による暗証番号入力方法においては、暗証番号認証の開始時に、表示処理手段により、フェイクポインタの形状を選択するための選択画面を表示し、入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択し、選択されたフェイクポインタの形状に応じた所定の位置の入力キーが、入力処理手段により入力される入力キーのデータとするように構成される。

【００２０】

本発明の暗証番号入力方法においては、フェイクポインタとしてテンキーパターンが選択された場合には、表示処理手段が、回答選択情報を取得するための選択画面を表示し、入力手段の入力操作に基づいて、ユーザが取得した回答選択情報が決定され、入力処理手段は、ポインタ位置制御手段により位置移動されたフェイクポインタにより選択指示された複数の入力キーの中から回答選択情報に基づくデータを入力するように構成される。

【００２１】

この場合に、回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、フェイクポインタの位置移動操作により、テンキーパターンの数字配置が、ポインタ位置制御手段により位置移動されるように構成される。

【００２２】

また、回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、フェイクポインタの位置移動操作により、テンキーの各数字キーの背景に表示される図形が、ポインタ位置制御手段により位置移動されるように構成されても良い。

【００２３】

また、本発明の別の態様では、本発明は、キーボードを表示する表示手段と、キーボードの中の入力キーを指示して入力操作を行う入力手段と、データ処理を行うデータ処理手段とを備えた情報処理装置において、暗証番号を入力し暗証番号の認証を行う暗証番号入力処理をコンピュータにより実行するプログラムであって、キーボードにおける複数の入力キーを同時に選択指示するフェイクポインタを当該キーボードに表示する表示処理手段と、入力操作により制御されて、フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるようにポインタの位置を制御するポインタ位置制御手段と、ポインタ位置制御手段により制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報により定められたデータを入力する入力処理手段と、入力処理手段によりデータの入力を受け付け、所定の文字数のデータを受け付けると、予め記憶された暗証番号と比較を行い、暗証番号を認証するデータ処理手段としてコンピュータを機能させるプログラムであるように構成される。

【００２４】

この場合に、暗証番号を入力し暗証番号の認証を行う暗証番号入力処理をコンピュータにより実行するプログラムにおいては、プログラム処理により、暗証番号認証の開始時に、表示処理手段により、フェイクポインタの形状を選択するための選択画面を表示し、入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択される。また、入力処理手段により、ポインタ位置制御手段により制御されたポインタにより選択指示された複数の入力キーの中からポインタの形状に応じて所定の位置の入力キ

ーのデータを入力するように構成される。

【００２５】

また、本発明による暗証番号を入力し暗証番号の認証を行う暗証番号入力処理をコンピュータにより実行するプログラムにおいては、プログラム処理により、暗証番号認証の開始時に、表示処理手段により、フェイクポインタの形状を選択するための選択画面を表示し、入力手段の入力操作により、フェイクポインタの形状を複数の所定のパターンの中から選択し、選択されたフェイクポインタの形状に応じた所定の位置の入力キーが、入力処理手段により入力される入力キーのデータとするように構成される。

【００２６】

この場合、プログラム処理により、フェイクポインタとしてテンキーパターンが選択された場合には、表示処理手段が、回答選択情報を取得するための選択画面を表示し、入力手段の入力操作に基づいて、ユーザが取得した回答選択情報が決定され、入力処理手段は、ポインタ位置制御手段により位置移動されたフェイクポインタにより選択指示された複数の入力キーの中から回答選択情報に基づくデータを入力するように構成される。

【００２７】

この場合に、回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、フェイクポインタの位置移動操作により、テンキーパターンの数字配置が、ポインタ位置制御手段により位置移動されるように構成される。

【００２８】

また、回答選択情報は、テンキーの各数字キーの背景に表示される図形情報であり、フェイクポインタの位置移動操作により、テンキーの各数字キーの背景に表示される図形が、ポインタ位置制御手段により位置移動されるように構成されても良い。

【発明の効果】

【００２９】

上記のような構成の暗証番号入力装置および暗証番号入力方法によれば、フェイクポインタを用いることにより、ユーザが秘密情報（暗証番号）を選択する場合には、正解を直接に選択するのではなく、フェイクポインタを使って正解を選択する。フェイクポインタでは、常に複数の回答候補を選択するようになっているので、第三者が暗証番号を入力する認証行為をのぞき見たとしても、それによりユーザの秘密情報が特定されるという事態が回避されることになり、これにより、覗き見攻撃に対する安全性が改善される。

【００３０】

すなわち、覗き見攻撃を可能にしている一番の原因は、認証時に正解である回答候補を直接選択させているためであるので、本発明の暗証番号入力装置および暗証番号入力方法においては、正解を直接選択させるかわりに、フェイクポインタと呼ぶ特殊な形状のポインタを用意し、それを使って認証（暗証番号）を回答させる。フェイクポインタは、常に複数の回答候補を選択するため、第三者が認証行為をのぞき見たとしても、認証者の秘密情報（暗証番号）の特定は困難になる。

【発明を実施するための最良の形態】

【００３１】

以下、本発明を実施する場合の形態について、実施例を具体的に図面を参照して説明する。具体例により説明する。図１は、本発明において用いるフェイクポインタを説明する図である。図２は、本発明において用いる正規ユーザの秘密情報の一例を説明する図である。また、図３は、フェイクポインタを用いる暗証番号入力の入力操作の一例を説明する図である。

【００３２】

まず、フェイクポインタについて説明する。図１に示す暗証番号を入力するためのキーボード画面は、銀行ＡＴＭの認証画面を想定して、暗証番号の入力画面を示したものである。図中左の図は、既存の銀行ＡＴＭの認証画面において表示される暗証番号の入力のためキーボードにおいて、暗証番号として、その中の数字の「５」を選択した例である。実際の銀行ＡＴＭの認証画面では、液晶タッチパネルにはテンキーボードだけが表示されて

おり、図に示すようなポインタによっての選択指示はなされないが、液晶タッチパネルにより、指で直接に１つの入力キーを選択することは、図示のようなポインタが存在し、このようなポインタによって指示しているとみなすことができる。

【００３３】

これに対しフェイクポインタは、複数の数字を同時に指示するポインタである。具体的には、図１の右側に示すように、例えば、十字型のポインタを使用して選択指示を行う。これにより、認証画面（暗証番号の入力画面）の数字キーの中で暗証番号の数字が選択される場合には、複数の回答候補が同時に選択された状態になる。すなわち、図１の右側に示す例では、入力する暗証番号の数字として「２」，「４」，「５」，「６」，「８」の５つの回答候補が選択されている状態となっている。これを第三者が覗き見たとしても、ユーザの選択した回答（暗証番号の数字）がそのうちのどれなのかが不明となり、覗き見攻撃に対して対抗できるものとなっている。

【００３４】

この場合、正規ユーザには、図２に示すように、フェイクポインタの形状と、当該フェイクポインタの正解選択用の位置に関する情報が、ユーザの秘密情報として、暗証番号と共に事前に知らされているものとする。このユーザの秘密情報は暗証番号入力装置の側にも登録されており、複数の入力キーの中から入力するデータを定めるための情報として利用される。したがって、正規ユーザは、予め知らされている秘密情報にしたがって、この場合には、フェイクポインタとして使用する十字型ポインタ内の上側部分の特定部位において自分の暗証番号を選択し、暗証番号の数字の回答を行うことになる。例えば、図１の右側に示すように、フェイクポインタを用いて暗証番号の数字を選択している場合には、数字「２」が選択された状態となる。

【００３５】

このようなフェイクポインタを入力操作により移動させると、その移動により、フェイクポインタの一部が、認証画面（テンキーボード）を逸脱するが、後述するように、その場合には逸脱した部分を折り返すことで対処する。

【００３６】

したがって、図２に示すような秘密情報を持つユーザが、十字型ポインタのフェイクポインタにより、暗証番号「１２５６」を入力する場合には、図３に示すように、フェイクポインタの位置を移動させて入力する。まず、暗証番号の「１」を入力する場合には、図３（１）に示すように、フェイクポインタを位置決めして入力を行い、次に、暗証番号の「２」を入力する場合には、図３（２）に示すように、フェイクポインタを位置決めして入力を行い、続いて、暗証番号の「５」を入力する場合には、図３（３）に示すように、フェイクポインタを位置決めして入力を行い、最後に、暗証番号の「６」を入力する場合には、図３（４）に示すように、フェイクポインタを位置決めして入力を行う。

【００３７】

この場合、フェイクポインタを移動させると、その移動により、フェイクポインタの一部が、認証画面（テンキーボード）から逸脱するが、逸脱した部分を折り返す処理がなされている。例えば、図３（１）に示す画面では、十字型ポインタの左部分が逸脱しており、その逸脱部分は右側に折り返されている。図３（３）に示す画面では、十字型ポインタの下部分が逸脱しており、その逸脱部分は上側に折り返されている。また、図３（４）に示す画面では、十字型ポインタの右部分および下部分が逸脱しており、その逸脱部分はそれぞれ左側および上側に折り返されている。

【００３８】

図４は、認証画面を逸脱したフェイクポインタの折り返し処理を説明する図である。図４では、Ｌ字型ポインタのフェイクポインタの折り返し処理を示している。図中の上と中の例は、ポインタの一部が画面右および上に「はみだした」例である。これらの場合、はみだした部分は折り返されて認証画面の左および下の部分を選択することになる。図中下の例は、はみだした部分の１つが右下にはみだしているが、これも同様に２回折り返し処理をすることにより左上の「１」を選択することになる。これによりフェイクポインタの

どの部分であっても全ての回答候補が選択可能になる。したがって、Ｌ字型ポインタのフェイクポインタを用いて秘密情報である暗証番号「１２５６」を入力する場合には、ユーザが認証に回答する入力操作は、図５に示すようになる。図５は、Ｌ字型ポインタのフェイクポインタを用いる暗証番号入力の入力操作の別の例を説明する図となっている。

【００３９】

図６は、本発明の一実施例の暗証番号入力装置のシステム構成を示すブロック図である。図１において、１１は入力データ記憶部、１２は表示制御部、１３はキーボートおよびフェイクポインタを表示する液晶ディスプレイで構成される表示部、１４は認証処理部、１５はデータの入力処理を行う入力制御部、１６はキー操作部およびポインタデバイスなどで構成され入力操作を受け付ける入力部、１７は暗証番号データ記憶部である。

【００４０】

入力データ記憶部１１は、入力部１６から入力制御部１５を介して入力された入力キーのデータを記憶する。表示制御部１２は、ポインタ位置制御部１２ａと、認証画面表示制御部１２ｂのサブシステムを含んでおり、表示部１３を制御して、表示画面に暗証番号の入力のためのキーボードおよびフェイクポインタなどユーザインタフェース部品を表示画面に表示する表示処理を行い、入力制御部１５による入力操作の制御動作と共にグラフィックユーザインタフェース機能を提供する。ポインタ位置制御部１２ａは、フェイクポインタをキーボードが表示されている表示画面に表示し、その際にフェイクポインタの表示位置に応じてフェイクポインタの折り返しの表示処理を行う。表示処理では、例えば、フェイクポインタを、キーボードの複数の入力キーに重ねて表示し、フェイクポインタの位置を入力操作に基づき制御して表示画面に表示する。

【００４１】

認証画面表示制御部１２ｂは、例えば、フェイクポインタの操作による入力操作により入力された入力済みのデータの文字数を“＊”により認証画面の所定のフィールドに表示する。暗証番号データ記憶部１７は、認証を行うべき暗証番号データを記憶している記憶部である。認証処理部１４は入力制御部１５の制御によってデータ入力の終了により起動され、入力データ記憶部１１に記憶された入力データと、暗証番号データ記憶部１７に記憶されている暗証番号データとを比較して、認証結果を出力する。

【００４２】

この実施例の暗証番号入力装置においては、表示部１３により表示画面に認証画面を表示して、キーボードを表示すると共に、入力部１６の入力操作により、キーボードの中の入力キーを指示する入力操作が行われる。ここでの暗証番号入力処理では、入力データ記憶部１１，表示制御部１２，認証処理部１４がデータ処理を行い、暗証番号の入力を受けて暗証番号の認証を行う。表示制御部１２においては、表示画面のキーボードにおける複数の入力キーを同時に選択指示するフェイクポインタをキーボードに表示する処理を行うが、この場合に、ポインタ位置制御部１２ａが、フェイクポインタにより選択指示された複数の入力キーの中に暗証番号として入力する入力キーが含まれるように、入力部１６による入力操作により制御されてポインタの位置を制御する。入力制御部１５では、ポインタ位置制御部１２ａにより制御されたフェイクポインタにより選択指示された複数の入力キーの中からユーザの秘密情報により定められたデータ（暗証番号）を入力し、このデータを入力データ記憶部１１に一時記憶する。認証処理部１４では、入力制御部１５から暗証番号のデータの入力を受け付け、所定の文字数のデータを受け付けると、暗証番号データ記憶部１７に予め記憶された暗証番号と比較を行い、暗証番号を認証し、その結果を出力する。

【００４３】

図７は、本発明の一実施例の暗証番号入力装置にかかる暗証番号入力処理の処理フローを示すフローチャートであり、図８は、認証画面の初期画面において表示されるフェイクポインタの選択画面を例示する図である。図７のフローチャートを参照しながら、暗証番号入力処理について説明する。まず、暗証番号を入力できるようにするため、最初に、認証画面において入力操作のためのキーボードを表示するが、フェイクポインタを用いる場

合には、図８に示すようなフェイクポインタの選択画面を表示する（Ｓ１００）。ユーザは利用するフェイクポインタのパターンを選択する指示を行う（Ｓ１０１）。ユーザがポインタのカーソルを移動し選択を行うなどの選択指示を行い、フェイクポインタを選択画面から選択すると（Ｓ１０１）、選択されたフェイクポインタにＩＤを割り当てる（Ｓ１０２）。ここで付与されたフェイクポインタのＩＤにより、同時に選択される複数の入力キーの中の１つの入力キーのデータが暗証番号入力の入力データとして選択されて入力される。

【００４４】

ユーザがフェイクポインタを、マウスまたはキー操作部のカーソルキーなどの入力操作により移動させる操作を行うと、フェイクポインタの位置が表示画面のキーボード上で移動されて、キーボードに重ねて表示される（Ｓ１０３）。そして、フェイクポインタの所定の位置がユーザが入力する暗証番号のデータの位置に位置するように移動されて、フェイクポインタの位置を決定する入力操作がなされると（Ｓ１０４）、その選択されたフェイクポインタの位置に対応した入力データを暗証番号として入力する（Ｓ１０５）。これを暗証番号データの入力終了まで繰り返す（Ｓ１０６）。入力された暗証番号データは、入力データ記憶部１１に保持される。

【００４５】

ここで、暗証番号データの入力が終了すれば（Ｓ１０６）、暗証番号が正しいかどうかを判断する認証処理（認証処理部１４）に、保持している文字情報を受け渡すなどして処理を終了する。暗証番号の入力が終了したかどうかは、例えば、入力データ数が暗証番号データの文字数と一致したかどうか、暗証番号データの入力桁数を表示するためのフィールドを表示する。

【００４６】

本発明においては、このように、フェイクポインタを用いて安全性が高い暗証番号入力装置を構成できるが、同時に選択指示する入力キーの数が多くないパターンのフェイクポインタを用いる場合には、十分な安全性を確保できない場合がある。これに対して、更に安全性を高くするための実施例について説明する。

【００４７】

これは、フェイクポインタを使用しても、覗き見により攻撃者が得られる秘密情報の数は少なく、十分な安全性を確保できない場合に対する例である。

【００４８】

ここではＬ字型ポインタのフェイクポインタを例にとる。図５により説明したように、正規ユーザが「１２５６」という暗証番号を入力した例にしたがって説明すると、攻撃者がこれを覗き見ていた場合、フェイクポインタのそれぞれの選択位置に対応する回答を読みとることで、「１２５６」，「４５８９」，および「５６９７」の３つの秘密情報候補を得ることができてしまう。回答候補が３つでは、既存の銀行ＡＴＭでも「なりすまし」に成功する可能性がかなり高い。このような場合には、覗き見攻撃に対する安全性はないことになる。またフェイクポインタが画面内のすべての回答選択肢を選択する形状だとしても、図５の認証画面では最大で９個しか攻撃者に暗証番号候補を与えることができず、１／３の確率で「なりすまし」に成功することとなる。これでは、覗き見攻撃に対する安全性を向上させたとは言えない。

【００４９】

そこで、フェイクポインタにＩＤを割り当て、かつ、そのＩＤ値を利用してユーザに「偽証」させる仕組みを導入する。詳細について説明すると、ここでは、フェイクポインタの選択可能場所数をＰｎとする。この選択可能場所数Ｐｎは、フェイクポインタとしてＬ字型ポインタを選択した場合はＰｎ＝３であり、十字型ポインタを選択した場合はＰｎ＝５である。この条件で、ポインタの各選択位置に１からＰｎ＋１までの数字をＩＤとして用意し、その中からＰｎ個のＩＤを重複することなく割り当てる。図９はその一例である。

【００５０】

図９は、フェイクポインタとしてＩＤ付きのＬ字型ポインタを使用する場合の操作例を説明する図である。Ｌ字型ポインタのそれぞれの位置にはＩＤが割り付けられているが、正規ユーザは、どのＩＤの位置で秘密情報を選択すべきかを、事前に知らされているものとする。この場合、ユーザはこのＬ字型ポインタのフェイクポインタを用いて秘密情報を入力する場合、１回の入力毎にＩＤの割付けが変更される。

【００５１】

このフェイクポインタを用いる回答方法は、その正解選択用のＩＤ値がフェイクポインタ内に存在するかによって、以下の２通りとされる。

（１）ＩＤが存在する場合、該当ＩＤの位置で秘密情報を選択する。

（２）ＩＤが存在しない場合には、どの回答候補を選択してもよい。

【００５２】

図９に示す例で説明すると、ここでは、正解回答用のＩＤを４とすると、「２ｎｄ　ｔｉｍｅ」を除く3回の回答は、フェイクポインタ内にＩＤ＝４が存在するので、Ｌ字型ポインタのフェイクポインタを位置決めし、ＩＤ＝４の位置において秘密情報を選択するようにＬ字型ポインタのフェイクポインタを位置決めして、秘密情報を入力する。

【００５３】

ただし、「２ｎｄ　ｔｉｍｅ」の場合は、正解選択位置を示すＩＤが存在しないので、ユーザは何を選択してもよく、それは正解となる。これによりユーザは、４回の回答のうち１回だけ嘘「かもしれない」回答をすることになる。これにより、認証行為を覗いていた攻撃者に与えることのできる秘密情報の候補数は増加する。覗き見ていた攻撃者が得る秘密情報の数は、

「偽証を含む回答の数」×「偽証のかわりに正解となりうる回答候補数」

となり、図９の例では４×９＝３６通りとなる。

【００５４】

これにより、覗き見攻撃に対する一定の安全性を確保しうるものとなる。しかし、これでもまだ欠陥がある。理由は、この方法の導入により、Ｂｒｕｔｅ－ｆｏｒｃｅ攻撃に対する安全性が低下するためである。具体的に説明すると、ユーザがとりうる秘密情報を、攻撃者が「しらみつぶし」に調べる場合、調査すべき秘密情報の数は、暗証番号のうち１桁分が意味をなさなくなるため、9^4個から4×9^3個に減少するからである。

【００５５】

覗き見攻撃に対する対策のために、Ｂｒｕｔｅ－ｆｏｒｃｅ攻撃に対する安全性が下がることは許されない。よって、その低下分を補う必要があるが、その方法として一番簡単な方法は、回答回数を１回増やすことであり、暗証番号ならば、暗証番号の桁数を１つ増やすこととなる。これは、安全性を向上させるためにユーザが負担しなければならないコストであると言える。

【００５６】

上述したように、本発明においては、フェイクポインタを用いて安全性が高い暗証番号入力装置を構成しているが、ここでのフェイクポインタは暗証番号を入力する度に変更するような構成とすることにより、ワンタイムパスワード化することができる。また、フェイクポインタの形状は、暗証番号の入力する際に毎回変更することも可能である。これにより、さらに安全性が高まる。

【００５７】

フェイクポインタの形状は、複数の回答候補を選択しうる形状であれば、基本的に自由なパターンとすることができる。ただし、ＩＤ割り当ての都合上、フェイクポインタは、（１回の認証における回答回数－１）以上の選択位置を持つ必要がある。

【００５８】

次に、フェイクポインタ情報の取得／通知方法であるが、これに関しては、通知方法に厳格な機密性がなくても運用は可能である。その理由は、仮にフェイクポインタに関する情報が第三者に知られることになったとしても、認証の秘密情報自体が第三者に知られない限り、それが即座に「なりすまし」につながらないからである。なぜなら、フェイクポ

インタは秘密情報の一部であり、それだけでは、認証を成功させるための十分条件ではないからである。銀行ＡＴＭを例に考えると、暗証番号が攻撃者に知られない限り、フェイクポインタに関する情報が攻撃者に知られたとしても認証の安全性は保たれるということである。この手法は、あくまで覗き見攻撃に対する安全性改善手法であり、認証における安全性は、この手法を導入する認証手法によって確保される。よって、フェイクポインタ情報の取得／通知方法に関しては、より簡単な認証や電子メールによる通知でも問題にはならない。

【００５９】

フェイクポインタ情報の取得／通知方法の機密性に関する前述の特徴を利用することにより、提示選択型認証を擬似的にワンタイムパスワード化することが可能となる。ここで「擬似的」という意味は、一度発行されたフェイクポインタが二度と使用されないことを保証しないため、厳密な意味でワンタイムパスワードではないという意味である。

【００６０】

暗証番号入力装置において、フェイクポインタの形状を複数種用意している認証システムを設けておき、この認証システムが、ユーザからのフェイクポインタ発行依頼を受け、その中からランダムに形状を選択し、ＩＤ値を割り当てて発行する。発行されたフェイクポインタは、１回の認証でのみ使用可能とする。

【００６１】

認証を行うユーザは、認証のたびにフェイクポインタの発行を受ける必要があり、フェイクポインタは、各ユーザに対して常に１つだけ発行されるものとし、以前発行されたフェイクポインタは、それが未使用であっても新たなフェイクポインタが発行された時点で無効とする。これらの規則を導入することにより、フェイクポインタが秘密情報のランダム化を果たすことになり、結果として、既存の認証を擬似的にワンタイムパスワード化することが可能になる。

【００６２】

これにより、２つの利点が得られることとなる。１つは、記憶負担の軽減である。この枠組により、ユーザはフェイクポインタに関する情報を記憶する必要がなくなる。結果として、ユーザに新たな記憶負担を課すことなく、認証における安全性を向上させることができる。もう１つは、安全性の強化である。先にＢｒｕｔｅ－ｆｏｒｃｅ攻撃に対する安全性の低下について指摘したが、ワンタイムパスワード化によりその安全性の低下を補うことができる。なぜならば、認証時にフェイクポインタの形状を選択する必要が生まれることから、回答回数が１つ増加するためである。

【００６３】

フェイクポインタの形状数が、それ以降の認証画面の回答候補数以上であれば、このフェイクポインタ選択が、偽証による回答無効分の代替となり、結果としてｂｒｕｔｅ－ｆｏｒｃｅ攻撃に対する安全性は維持されることとなる。また、この対策は、覗き見不可能な攻撃者に対して、ｂｒｕｔｅ－ｆｏｒｃｅ攻撃に対する安全性が向上させることにもなる。なぜならば、覗き見をしてない攻撃者にとっては、暗証番号も不明な上にフェイクポインタの形状も不明なためである。

【００６４】

ところで、フェイクポインタとしては、特殊な形状でなく、また、移動操作をおこなっても形状が変化しないテンキーパターンの形状を、フェイクポインタの一つのパターンとしても利用することができる。この場合には、フェイクポインタの移動操作はテンキーの数字配置の移動となる。また、後述するように、数字配置が移動されたテンキーから暗証番号を特定するために、回答選択情報を用いる。この回答選択情報は、前述の秘密情報に代わるものとしても利用できる。このようなフェイクポインタの利用の選択は、例えば、初期画面のフェイクポインタのパターンの選択の際に行う。その場合には、回答選択情報が必要となるので、これについても、初期画面において選択操作を行って利用できるように設定される。

【００６５】

次に、テンキーパターンのフェイクポインタによる認証方法について、フェイクポインタを４桁数字からなる暗証番号認証を行う銀行ＡＴＭに適用する場合について説明する。図１０は、テンキーパターンのフェイクポインタによる認証画面の一例を示す図であり、図１１は、テンキーパターンのフェイクポインタによる認証方法に用いる回答選択情報の一例を説明する図であり、図１２は、フェイクポインタの操作による数字配置の制御を説明する図である。

【００６６】

図１０に示されるように、テンキーパターンのフェイクポインタは、見た目は普通のテンキー配列であり、各数字キーの背景にさまざまな形の図形が表示された画面となっている。この画面の中の数字キーの背景に表示されている個々の情報を、“回答選択記号”と呼ぶ。テンキーパターンのフェイクポインタでは、全てのキーの背景に“回答選択記号”が描画される。また、その各キーへの回答選択記号の配置は、認証画面を生成のたびにランダムに決定される。

【００６７】

このテンキーパターンのフェイクポインタで認証を行う場合、ユーザは認証前に“回答選択情報”を取得する必要がある。この例では、図１１に示すように、回答選択情報は、暗証番号の４桁数字に対応して４つの図形としている。この回答選択情報は、ユーザの秘密情報（暗証番号）を入力するのに必要な情報である。ユーザは、図１２に示すように、フェイクポインタの操作による数字配置の制御を行う。つまり、左右キーを使用することでテンキーパターンのキー配列における数字の割り当てを変更し、暗証番号の各桁の数字を入力する操作を行う。すなわち、ユーザは、認証前に取得した回答選択情報の上に自身の暗証番号が重なるよう左右キーを用いて数字の配置を変更し、暗証番号と回答選択記号が重なった時点で確定キーを押す。これによって、１つの数字が入力される。１桁目の暗証番号を回答選択情報の１つめの記号で選択するという仕組みである。したがって、４桁の暗証番号を入力するにはこれを４回繰り返すことになる。ここでは、左右キーを用いてフェイクポインタを操作し、数字の配置を変更するようにしているが、数字の配置は固定しておき、数字に重なる回答選択情報の図形の配置が、左右キーを用いてフェイクポインタを操作して変更されるようにしても良い。

【００６８】

一方、攻撃者にとっては、正規ユーザの認証行為を覗き見たとしても、その認証における“回答選択情報”を知り得ない限り、暗証番号を知ることは困難である。仮に攻撃者が認証行為をビデオで撮影したとしても、その安全性は維持される。一方、攻撃者が回答選択情報を知り得たとしても、それは暗証番号とは全く関連のない情報であり、それだけでは正規ユーザにとって脅威にはならない。

【００６９】

暗証番号が漏洩するのは、回答選択情報が攻撃者に渡るとともに、その回答選択情報を使用した認証行為を攻撃者に覗き見られた場合のみである。

【００７０】

図１３は、テンキーパターンのフェイクポインタの操作による認証手順を示すフローチャートである。図１３に示すように、この場合の認証手順では、まず、初期画面により、ユーザがシステムからユーザの予め登録された秘密情報に基づいて提示された回答選択情報を取得する（Ｓ２０１）。次にユーザ操作により、フェイクポインタの操作によるテンキーパターンの数字配置の制御を行い、回答選択情報の対応する図形と入力する暗証番号の数字が一致するようにして暗証番号の入力操作を行い、これを回答入力が終了するまで繰り返す（Ｓ２０２，Ｓ２０３）。回答入力が終了すると予め登録された暗証番号と、回答入力として入力された番号との比較による認証処理を行い、認証結果を出力して、処理を終了する（Ｓ２０４）。

【００７１】

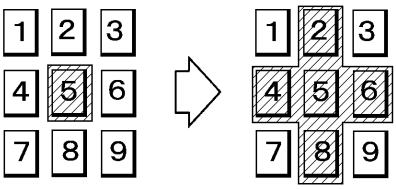
フェイクポインタでは、認証行為、すなわち秘密情報（例：暗証番号、パスワード）を入力する前に“回答選択情報”を取得しなければならない（Ｓ２０１）。回答選択情報は

、秘密情報を入力するのに必要不可欠な情報であり、以下のような特徴を持つ。
（１）使い捨てである
（２）システム側でランダムに生成される
【００７２】
ここでの“使い捨てである”という特徴は、次の２つのことを意味する。１つは、取得した回答選択情報は一回の認証でのみ使用可能とされ、ユーザは認証するたびに回答選択情報を取得しなければならないという点である。ただし、利便性を考慮すると、ある一定期間は同一の回答選択情報で認証可能にするという運用も考えられる。もう１つは、ユーザが回答選択情報を記憶し続ける必要がないという点である。
【００７３】
また、回答選択情報は、その都度ランダムに生成される。この特徴は、安全性確保のために必要不可欠である。回答選択情報が常に一定だとすると、複数の認証行為の記録から暗証番号を割り出されてしまうからである。
【００７４】
なお、回答選択情報は上記以外の制約はない。図１４は、回答選択情報の他の例を示す図である。図１４に示すように、数字、文字、記号、図形、写真などさまざまな情報を回答選択記号として利用することができる。なお、図１４に示す回答選択情報の例では、回答選択情報の記号数が秘密情報の文字数と同一の場合（図１４のアルファベットや数字）と、そうでない場合（ひらがなや図形）がある。この差は、回答入力方法に違いを生むことになる。次にその回答入力方法について述べる。
【００７５】
（回答入力方法）
次にテンキーパターンのフェイクポインタにおける回答入力方法について説明する。テンキーパターンのフェイクポインタでは、回答選択情報で秘密情報を指し示すことで回答を行う。具体的に言うと、秘密情報と回答選択情報を認証画面上で重ね合わせることで回答を指示する。各認証画面では、回答選択記号が各数字キーの背景に表示されるが、認証画面に表示される回答選択記号群の中に１つだけ回答選択情報が含まれるようになっており、その他の回答選択記号は“おとり”となっている。なお、回答選択情報の記号数は、秘密情報の文字数と同一の場合と異なる場合がある。このそれぞれの場合において、回答方法は若干異なる。以降では、そのそれぞれの場合における回答方法について説明する。図１５は、回答選択情報を使った回答方法の例を説明する図であり、図１６は、回答選択情報を使った回答方法の別の例を説明する図である。また、図１７は、位置による回答選択情報を提示する場合の回答方法の別の例を説明する図である。
【００７６】
（回答選択情報と秘密情報の記号数が同一の場合）
秘密情報の文字数と回答選択情報の記号数が同一である場合の回答方法について説明する。この場合における回答方法は、１つめの回答選択情報で１つめの秘密情報を指し示し、以降、同様に入力が終わるまで繰り返す。図１５を例にして説明すると、１桁目の暗証番号である“７”を、回答選択情報の１つめの文字であるアルファベット“ｈ”で指示し、つぎに２桁目の暗証番号である“２”を回答選択情報の２つめの文字である“ｅ”で指し示す．．．という具合である。
【００７７】
（回答選択情報と秘密情報の記号数が異なる場合）
次に、回答選択情報の記号数と秘密情報の記号数が異なる場合の回答方法について説明する。この場合には、秘密情報の文字数と回答選択情報の数が異なるため、それらを一対一で対応づけすることができない。よって、この場合、図１６に示すように、個々の秘密情報の入力のために個別の回答選択記号を割り当てるかわりに、回答選択情報内の記号のいずれかで秘密情報を指示する。この場合の認証画面は、表示される回答選択記号群の中に回答選択情報のうちの記号が１つだけ含まれるよう認証画面が生成される。よってユーザは、認証画面の中から自身の回答選択情報の含まれている記号を見つけ、その回答選択

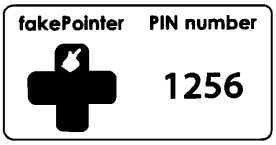
記号で秘密情報を指し示すことで回答入力を行う。
【００７８】
図１６の例では、回答選択情報が秘密情報の数よりも少ない場合を示している。この例では、１つめの回答選択情報で１桁目と４桁目の暗証番号を選択し、２つめの回答選択情報で、２および３桁目の暗証番号を指示し回答したことを示している。なお、回答選択情報と秘密情報の組み合せは、認証のたびにランダムに決定されることとなる。
【００７９】
（他のバリエーション）
回答選択情報の役割は、秘密情報（暗証番号）を指し示す”位置”を指示していると言いかえることができる。この場合の例を、図１７を参照して説明すると、回答選択情報としては、例えば、図１７の形式にすることも可能だと言える。つまり、回答選択情報を記号で与えるかわりに回答を指し示す位置と順序を直接ユーザに与えるのである。
【００８０】
図１７では、４つの記号からなる回答選択情報と、同等の回答選択情報の一例を示している。すなわち、１桁目の暗証番号を左中段の位置にて指示し、暗証番号２桁目を中央最下段の位置にて指示する．．．（以降略）という手順を繰り返すことで回答する。回答選択情報をこのように位置と順序で直接指定すると、認証画面は、図１０に示すフェイクポインタの認証画面のように、数字の背景に回答選択記号を表示する必要がなくなり、既存の銀行ＡＴＭと同様の画面にすることができる。つまり、画面表示そのものを大きく変更することなく覗き見攻撃に対する安全性向上策を導入することが可能になる。また、回答を指示する位置が明確になるため、認証時にユーザが自身の回答選択情報がどこにあるか探索する必要がなくなる。これは認証時における作業負担軽減に寄与する。
【００８１】
フェイクポインタが対象とする主たるアプリケーションは、第三者の目のある環境下で暗証番号による認証が必要となる全てのアプリケーションであり、銀行ＡＴＭや携帯電話、大画面インタフェースでの認証などが主たるアプリケーションになる。また暗証番号だけに限らず、他の認証にも適用可能である。
【産業上の利用可能性】
【００８２】
以上に説明したように、本発明によるフェイクポインタを用いる暗証番号入力装置によれば、覗き見攻撃に対する対策手法として、「見られないようにする」のではなく、「見られても一定の安全性を確保可能にする」手法により安全性が高められる。また、本発明は、提示選択型の認証であれば広く適用可能な安全性改善法であり、それは既存の銀行ＡＴＭの認証でも適用可能である。また、ワンタイムパスワード生成のために乱数表や特定のハードウェアをも持つ必要もない。
【００８３】
また、本発明では、安全性を向上させつつも、ユーザに課される負担を増やさないように配慮している。銀行ＡＴＭを例にとると、安全性向上のためにユーザに課される記憶負担の増加は、フェイクポインタに関する情報は記憶しなくても運用可能なため、数字1 桁分だけである。また、その操作性は、既存の提案手法と比較しても大きく変わるものではない。また、既存の認証手法をその枠組を大きく変化させることなくワンタイムパスワード化することも可能であり、それによりＢｒｕｔｅ－ｆｏｒｃｅ攻撃に対する安全性強化も可能となる。
【図面の簡単な説明】
【００８４】
【図１】本発明において用いるフェイクポインタを説明する図である。
【図２】本発明において用いる正規ユーザの秘密情報の一例を説明する図である。
【図３】フェイクポインタを用いる暗証番号入力の入力操作の一例を説明する図である。
【図４】認証画面を逸脱したフェイクポインタの折り返し処理を説明する図である。
【図５】Ｌ字型ポインタのフェイクポインタを用いる暗証番号入力の入力操作の別の例を

説明する図である。
【図６】本発明の一実施例の暗証番号入力装置のシステム構成を示すブロック図である。
【図７】本発明の一実施例の暗証番号入力装置にかかる暗証番号入力処理の処理フローを示すフローチャートである。
【図８】認証画面の初期画面において表示されるフェイクポインタの選択画面を例示する図である。
【図９】フェイクポインタとしてＩＤ付きのＬ字型ポインタを使用する場合の操作例を説明する図である。
【図１０】テンキーパターンのフェイクポインタによる認証画面の一例を示す図である。
【図１１】テンキーパターンのフェイクポインタによる認証方法に用いる回答選択情報の一例を説明する図である。
【図１２】フェイクポインタの操作による数字配置の制御を説明する図である。
【図１３】テンキーパターンのフェイクポインタの操作による認証手順を示すフローチャートである。
【図１４】回答選択情報の他の例を示す図である。
【図１５】回答選択情報を使った回答方法の例を説明する図である。
【図１６】回答選択情報を使った回答方法の別の例を説明する図である。
【図１７】位置による回答選択情報を提示する場合の回答方法の別の例を説明する図である。
【符号の説明】
【００８５】
１１　入力データ記憶部
１２　表示制御部
１３　表示部
１４　認証処理部
１５　入力制御部
１６　入力部
１７　暗証番号データ記憶部

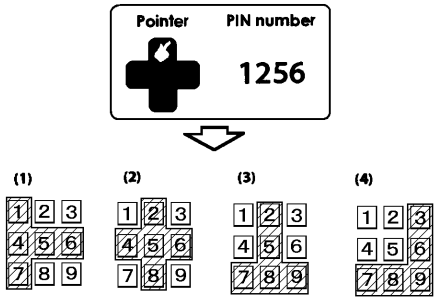
【図１】



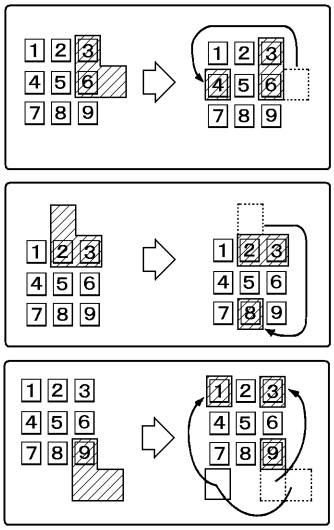
【図２】



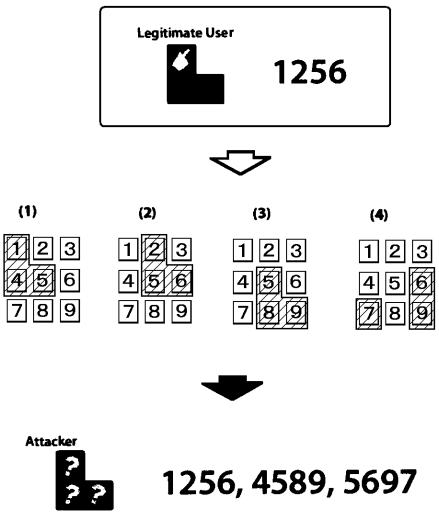
【図３】



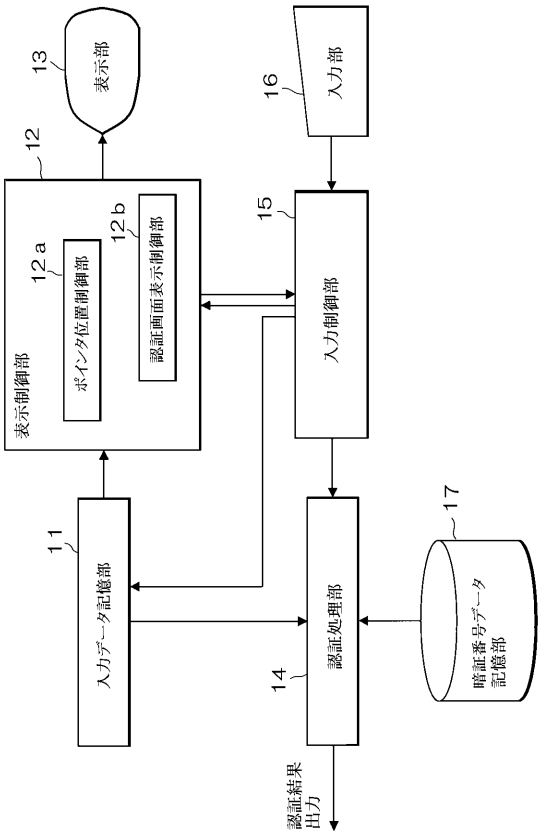
【図４】



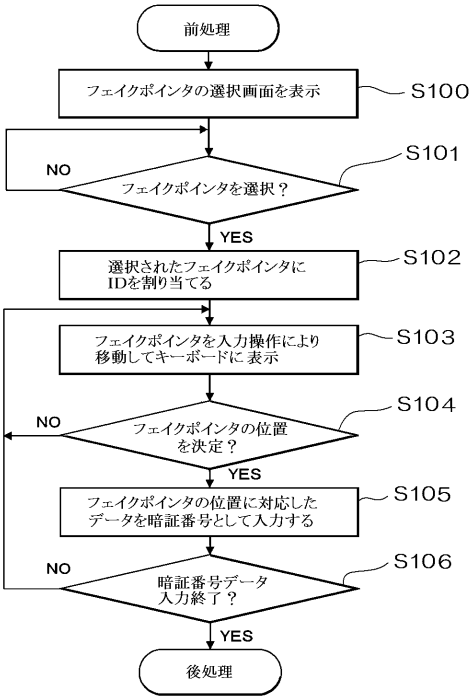
【図５】



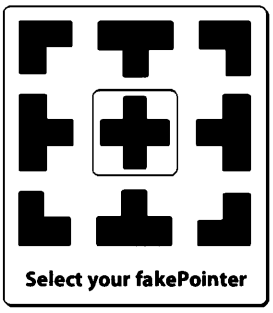
【図６】



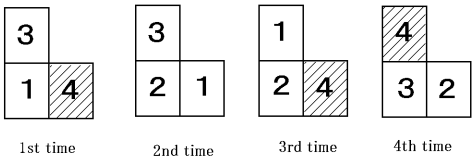
【図７】



【図８】

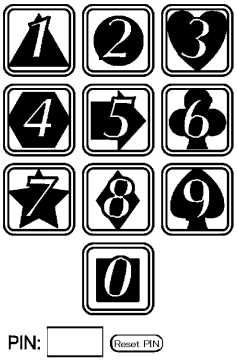


【図９】



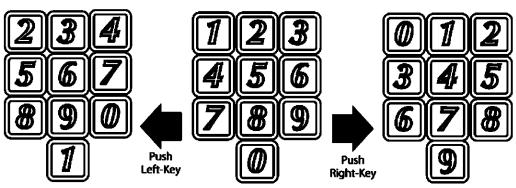
Pn=3, ID={1, 2, 3, 4}

【図１０】

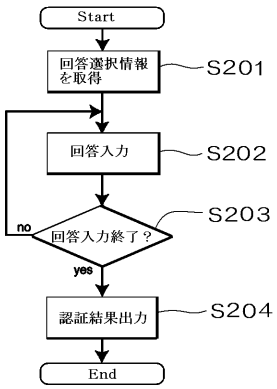


【図１１】

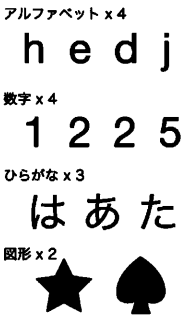
【図１２】



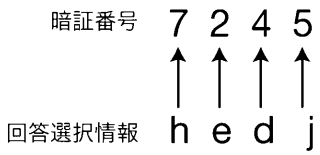
【図１３】



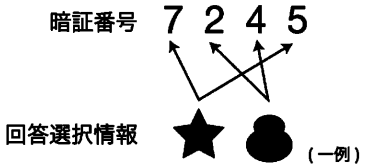
【図１４】



【図１５】



【図１６】



【図１７】