打鍵データの特性を生かした個人認証システム

佐村敏治[*1]・高岡沙緒里[*2]・柴田千恵[*3]
西野順二[**]・小高知宏[**]・小倉久和[**]

Fundamental Studies of User Authentication System Based on Keystroke characteristics

Toshiharu Samura, Saori Takaoka, Chie Shibata
Junji Nishino, Tomohiro Odaka and Hisakazu Ogura

As the use of computer systems proliferates, the need for appropriate computer security grows. The implementation of safeguards for computer security is based on the ability to verify the identity of authorized computer systems users accurately. The most common form of identity verification in use today is the password, but passwords have many poor traits as an access control mechanism. To overcome the many disadvantages of simple password protection, we are proposing the use of the biometric characteristics of keyboard input as a method for verifying user identity. This paper reports on an experiment that was conducted to assess the viability of using keystroke characteristic (time between two successive keystrokes) as an identity verifier.

1.はじめに

コンピュータシステムの急増によりコンピュータセキュリティの必要性も高まってきた．現在コンピュータセキュリティにおける基本的な情報リソースの保護は通常ユーザの個人認証によって行われている．ユーザが一度ログインすると，そのユーザの権限を持ち，情報リソースにアクセスし，それらのリソースを変更することができる．従って確実な個人認証システムがコンピュータシステムに必要であることが分かる[1)]．

今日使用されている個人認証システムはパスワードである．パスワードによる認証は費用がかからなく実行することが容易である．しかし，そのパスワードが漏れると，不正なユーザによるアクセスが可能になるという危険性がある．

＊1 経営工学科　＊2＊3 経営工学科4年生　＊＊福井大学工学部情報工学科

Joyce と Gupta[2] は，個人認証システムを4つのカテゴリーに分けた．

(1) 個人の所有するもの．例えば，鍵・IDカード・パスポート等

(2) 知識を使うもの．例えば，パスワード・数字あわせ鍵・PIN数等

(3) 行動によるもの．例えば，署名・行動パターン等

(4) 生物的測定を用いるもの．例えば，物理的なふるまい・指紋・網膜・声紋等

これらの中で最近注目されているのが，身体や生物的反応を測定した(4)の方法である[1]．

これらの方法は，生まれ持った個人特有の性質を利用するため，他人の進入を受け難い．しかし，多くがコンピュータに接続される高価な装置を必要とする．

我々は，個人が入力する打鍵のリズムを利用した認証方法の研究に着目した．個人が入力する打鍵データは個人に特有のものである．もし打鍵パターンのデータを解析するアルゴリズムができれば，権限を与えられたユーザを認識し，不正なユーザを拒絶することができるかもしれない．また，高価な機器が必要でなく誰でも導入できる．そして，打鍵データのパターンを解析することは，セキュリティの研究に利用できるだけでなく，コンピュータ環境における生物学的研究においても有効となるであろう．また，マン・マシーン・インターフェース開発の研究分野においても利用できるであろう．

本稿では，打鍵データを入力文字の打鍵間時間を計測し，それを解析することで個人認証する実験を行う．次章で述べるように，打鍵間時間による個人認証方法にも，パスフレーズによる個人認証するものや長文テキストなどを入力することで個人認証するものなどがあるが，ここでは，4つの短いパスフレーズ（姓・名・fukui・よく使用するフレーズ）を入力した時の打鍵データを使って実験を行った．

今回の実験は，あまりキーボードに慣れていないものを含む 8 人の被験者を対象に行った．得られた打鍵データをもとに，解析方法として粕川達のノルムによる認証方法[3]を使い，認証検査を次の3つの方法で行った．(i)それぞれのパスフレーズごとに認証する方法，(ii) 3つないし4つのパスフレーズを合わせて，1つのパスフレーズのように解析する方法，(iii) 4つのパスフレーズの中で2つ以上本人と認証されれば，全体的に本人と見なす方法，である．(iii)については新しい試みである．本実験での解析の結果，(i)や(ii)の方法よりも認証率を上げることができた．

第2章では打鍵データによる個人認証システムの先行実験について簡単にまとめる．打鍵間時間を扱った認証実験はあまり日本では取り上げられることがないので，本稿でまとめておくことは有効であると考える．第3章では我々が行った実験方法を説明する．第4章で実験結果を述べる．第5章で結論と考察を行う．

2．打鍵データによる個人認証の概要

本稿では，打鍵データの分析法として，入力したキーの打鍵間時間を計測して解析を行う．

打鍵間時間を扱うアプローチには大きく分けると2つある．

(a) パスフレーズ（IDやパスワードなど短いフレーズ）を入力したときの打鍵データ

(b) 長文のテキスト文書を入力したときの打鍵データ

表1．打鍵データによる個人認証システムの結果（最適値のみ表示）

方　法	認証失敗率(%)	誤認率(%)	文　献
パスフレーズによる個人認証			
・統計的処理を扱った方法			
(1)Joyce-Guptaによるノルム法	16.7	0.3	2)
(2)粕川達によるノルム法	53.5	0.0	3)
・ニューラルネットワークによる方法 (Brown-Rogers による解析)	21.3	0.0	4)
長文テキスト入力による個人認証			
・スタティックな解析（文章の長さ固定）			
(1)Umphress-Williams によるフィルタ	11.7	5.8	5)
(2)Leggett-Williams によるフィルタ	5.5	5.0	6)
・ダイナミックな解析（文章入力時に自動的に判定）(Leggett-Williams-Usnisk による解析)	11.1	12.8	7)

表1は，2つのアプローチを扱った論文から認証失敗率（本人なのに他人と判断された割合）と誤認率（他人が認証して本人と判断された割合）の最適値を表にしたものである．ただし，この数値はそれぞれの筆者が独自に実験を行ったもので，打鍵データの対象者や実験環境が異なり，得られた認証率から解析方法の優劣を判断することができないことを注意しておく．例えば Brown と Rogers 達のニューラルネットワークを用いた方法[4]は，誤認率は 0.0%ではなければならないという前提でそのときの限界の認証失敗率を求めている．また粕川達によるノルムを用いた方法[3]は日本人によるキーボードの不慣れな被験者を含めた実験になっている．というように様々な異なった環境や条件で解析しているので，パスフレーズによる個人認証を比較した時，Joyce-Gupta の方法が優れているとは必ずしも言えない．

(b)については，1985 年に Umphress と Williams が参照データに 1400 字程度の文章を，検査データに 300 字程度の文章を入力したときの打鍵データを使って個人認証ができることを実証した[5]．彼らは文章の打鍵間時間を計測して，いくつかの方法でフィルタ化して，抽出されたデータを最初の文字と後の文字の行列を作り，参照データと検査データとを比較する方法を用いた．結果として，17 人の被験者を使って実験を行ったところ，認証失敗率 11.7%，誤認率 5.8%を得た．また後に Leggett と Williams[6] がフィルタの方法を変えて解析したところ，最適な結果として,認証失敗率 5.5%，誤認率 5.0%を得ている．Leggett, Williams, Usnick と Longnecker 達[7]は検査データの文章を固定させないダイナミックな解析で認証が行えることを示した．

一方(a)については，1990 年に Joyce と Gupta[2] がパスフレーズ（ユーザ ID・パスワード・姓・名）を使って打鍵データのノルムという値を計算することで個人認証するアルゴリズムを論じた．認証失敗率や誤認率は納得のいく値を得ている．そして，粕川達[3]はフィルタを再検討し,ノルムについても重みを考慮したものを発表した．また彼らは日本人などのキーボードに慣れていない被験者を対象に解析を行った．最近の打鍵データの解析方法では，Brown と Rogers[4] が行ったようにニューラルネットワークを使って打鍵データの解析を行ったものがある．

本稿では (a)についての個人認証実験を行う．

3.実験方法

本実験では，キーボードに慣れていない被験者を含む 8 名を選び（A から H と名づける），よく使用する機会があると思われる 4 つのパスフレーズ（「姓」・「名」・「fukui」・「よく使用しているフレーズ」）を１０回入力して，それを本人の”参照データ”とする．

実験に使用したコンピュータは，EPSON 製のワークステーションで，Pentium II プロセッサ 300MHz，メモリ 192MB を搭載している．OS には Windows NT Workstation を利用したが，使用した言語が Java のため，将来他の OS でも実験することができる．時間の精度は 10 ミリ秒である．約 2000 行のプログラムで，GUI 環境によってナビゲーションをする設計になっている（図 1）．実験によって得られた入力文字と打鍵間時間のリズムの例を図 2 に示す．

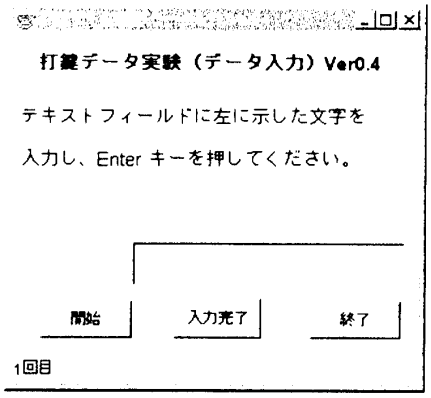

図 1. 打鍵データ実験ソフト

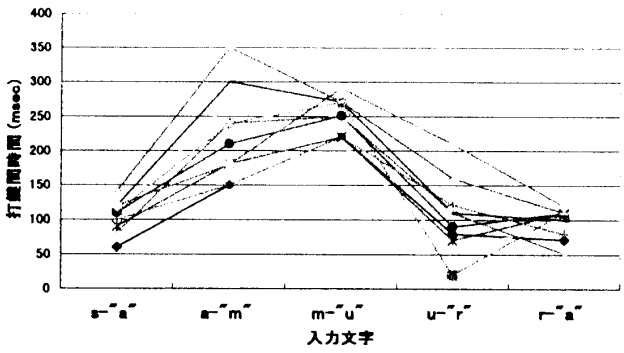

図 2. 入力文字と打鍵間時間の例
（“samura”と入力）

以下，我々は粕川達の行った方法[3]を使って解析を行なった．

【参照データ】

1. $n+1$ 文字からなる入力を 10 回行い、K_1 から K_{10} の 10 個の打鍵間時間列を得る．
   ここで，$K_i=(k_{i1}, k_{i2}, \cdots, k_{ij}, \cdots, k_{in})$，$(1 \leqq i \leqq 10)$ であり k_{ij} は i 回目の試行での j 番目の打鍵間時間である．また打鍵間数は n である．
2. 平均打鍵間時間列 m および打鍵間時間標準偏差列 s を計算する。ここで $m=(m_1, m_2, \cdots, m_j, \cdots, m_n)$，$s=(s_1, s_2, \cdots, s_j, \cdots, s_n)$ とする。ただし、m_j＝平均 $(k_{1j},k_{2j},\cdots,k_{ij},\cdots,k_{10j})$，$s_j$＝標準偏差 $(k_{1j},k_{2j},\cdots,k_{ij},\cdots,k_{10j})$ とする．
3. 10 個の打鍵間時間列 K_i それぞれについて個々の打鍵間時間を調べ、すべての j $(1 \leqq j \leqq n)$ について，平均から標準偏差の 3 倍を超えるものを希なデータとして取り除く．条件にかなう打鍵間時間列からなる集合を $KS=\{K_{i1},K_{i2},\cdots,K_{ir}\}$，$(1 \leqq r \leqq 10)$ とする。KS をもとにして再び平均打鍵間時間列を 2. に従って計算する。これを参照データ R と呼ぶことにする。$R=(r_1,r_2,\cdots,r_j,\cdots,r_n)$ で r_j は KS に属する K_i についての j 番目の打鍵間時間の平均値である。
4. KS 属する打鍵間時間列 K_i について、参照データ R からのノルム $norm\ (K_i,R)$ を計算する．
   $$norm\ (K_i,R)=\Sigma\ |\ k_{ij}-r_j\ |\ /\ ns_j. \tag{1}$$
5. 続いて、各ノルムの平均値 N_{mean} と標準偏差 N_{sd} を計算する。
   $$N_{mean}=\text{平均}\ (norm\ (K_i,R))\ ,\ N_{sd}=\text{標準偏差}\ (norm\ (K_i,R))\ . \tag{2}$$

6. 本人とみなせるノルムの境界を示す認証閾値 I を以下のように定める。

$$I = N_{mean} + scale \times N_{sd} \quad (3)$$

ここで，*scale* は 0.5～3.0 までの値をとる．

【検査データ】

検査データ $T = (t_1, t_2, \cdots, t_j, \cdots, t_n)$ について、参照データ R からのノルム $norm(T,R)$ を計算する

$$norm(T,R) = \Sigma \mid t_{ij} - r_j \mid / ns_j \quad (4)$$

【認証方法】

$norm(T,R) < I$ を満たす場合に本人であると判定する．なお、以降では利用者本人の入力した署名を誤りと判定してしまう場合を「認証失敗」，利用者以外の入力した検査署名を本人と判定してしまう場合を「誤認」と呼ぶ．

4．実験結果

本章では実験結果について述べる．

その前に 3 章の解析から得られる誤認率の傾向について触れておく．(3)式から *scale* の寄与によって認証率が異なってくることが分かる． *scale* が小さいと，認証閾値 I が小さくなるため，誤認する割合は減るが，本人に対する認証が失敗する割合が大きくなる．逆に *scale* が大きくなると，I が大きくなるため，認証失敗率が減ってくるが，同時に誤認率が大きくなる．打鍵データを認証方法として実用化するには，この閾値をどの程度に設定するかということがポイントになってくる．

本稿では，3つの認証検査方法を使って認証を行った．

4-1. 各パスフレーズごとの認証

まず，パスフレーズ（姓・名・fukui・よく使用しているフレーズ）をそれぞれ分けて解析した結果を表わす．例として，*scale* を 1.5 にした場合を表 2～5 に示す．列の被験者の「参照データ」に対して行の被験者が認証を確かめたときの結果である．本人として認証されると○，他人として認証されると×で表わす．ただし各被験者の横に示した数字は，本人のコンピュータのキーボードに対する熟達度を調べるために，同じ日本語の散文を 5 分間入力した時の 1 分あたりの平均語数を示している．本人の認証は 2 度行った．ただし 2 回目の認証実験は時間をおいて実施した．

表2.「姓」を入力した時の認証結果（*scale*=1.5）

	語/分	A	B	C	D	E	F	G	H
A	79.0	××	×	×	×	×	×	×	×
B	65.6	○	○○	×	×	×	×	×	×
C	40.6	×	×	○×	×	○	×	×	×
D	37.4	×	×	×	○○	×	×	×	×
E	30.0	×	×	×	×	○○	×	×	×
F	27.6	×	×	×	×	×	×○	×	×
G	26.2	×	×	×	×	×	×	○×	×
H	17.4	×	×	×	×	×	×	×	○○

表3.「名」を入力した時の認証結果（*scale*=1.5）

	語/分	A	B	C	D	E	F	G	H
A	79.0	×○	×	×	×	×	○	×	×
B	65.6	○	××	×	×	×	○	×	×
C	40.6	×	×	××	×	×	×	×	×
D	37.4	×	×	×	××	×	×	×	×
E	30.0	×	×	×	×	×○	×	×	×
F	27.6	×	×	×	×	×	○○	×	×
G	26.2	×	×	×	×	×	×	○×	×
H	17.4	×	×	×	×	×	×	×	××

表 4.「fukui」を入力した時の認証結果

（*scale*=1.5）

	語/分	A	B	C	D	E	F	G	H
A	79.0	○○	×	×	×	×	×	×	×
B	65.6	×	○×	×	×	×	×	×	×
C	40.6	×	×	××	×	×	×	×	×
D	37.4	×	×	×	○○	×	×	×	×
E	30.0	×	×	×	×	××	×	×	○
F	27.6	×	×	×	×	×	××	×	×
G	26.2	×	×	×	×	×	×	×○	×
H	17.4	×	×	×	×	×	×	×	××

表 5.「よく使うフレーズ」を入力した時の認証結果

（*scale*=1.5）

	語/分	A	B	C	D	E	F	G	H
A	79.0	×○	×	×	○	×	×	○	×
B	65.6	×	○○	×	○	×	×	○	×
C	40.6	×	○	○×	○	×	×	○	×
D	37.4	×	×	×	○○	×	×	○	×
E	30.0	×	×	×	×	×○	×	○	×
F	27.6	×	×	×	○	×	○×	○	×
G	26.2	×	×	×	×	×	×	○○	×
H	17.4	×	×	×	×	○	×	×	○×

表 6. scale=1.5 での認証率

	認証失敗率(%)	誤認率(%)
姓	31.25	3.57
名	68.75	5.35
fukui	62.5	1.78
1-word	31.25	21.42

個々の結果を見ると，本人であれば認証され,他人では拒否されることが全体の傾向として見られる．従って各人ごとに打鍵データにリズムを持っていることが分かる．この結果を認証失敗率と誤認率で表わした結果が表６である．そして各スケールごとに認証率を解析した結果が表 7 である．この表から分かることは，それほど良い認証率を与えていないということである．よって，打鍵データにリズム性はあるものの認証率が低いため，個人認証に利用するのは難しい．また章の最初に述べた *scale* と認証の傾向もあまり見られない．これは各フレーズの文字数が少なく，ちょっとした誤差が全体の認証に影響を与えていることが原因でないかと推測される．

表 7. scale による認証率の変化

	誤認失敗率				誤認率			
scale	姓	名	fukui	1-word	姓	名	fukui	1-word
0.5	37.5	68.8	56.3	31.3	5.4	3.6	1.8	23.2
1.0	31.3	68.8	62.5	31.3	5.4	5.4	1.8	23.2
1.5	31.3	68.8	62.5	31.3	3.6	5.4	1.8	21.4
2.0	31.3	68.8	62.5	31.3	3.6	5.4	3.6	21.4
2.5	31.3	68.8	62.5	31.3	3.6	5.4	5.4	19.6
3.0	31.3	68.8	62.5	37.5	3.6	7.1	5.4	19.6

そこで今度は各パスフレーズを組み合わせて認証を行う．本稿では２つの可能性について調べた．

まず，３つ（または４つ）のパスフレーズをひとまとめにして，３章の解析方法を使って認証を行う方法である．もう一つは、各パスフレーズを認証して，４つの中で２つ以上が本人と認証されれば，全体的に本人として認定するという方法である．

4-2. ３つ（または４つ）のフレーズをひとまとめにした認証

いままで別々にフレーズを扱ってきたが，今度は全てをまとめて解析を行った．表 8 は，（姓・名・fukui）の３つをひとまとめにして解析を行った認証結果である（ただし *scale* = 1.5 のとき）．表 9 は，各 *scale* によって認証率を解析した結果である．この表から，誤認率が非常に低いことが分かる．しかし，逆に認証失敗率が大きくなっている．少なくとも本人の認証には 2 回以上入力する必要が出てくることが分かる．

表 8. 姓・名・fukui をひとまとめにして解析した結果（*scale* = 1.5）

	語/分	A	B	C	D	E	F	G	H
A	79.0	○×	×	×	×	×	×	×	×
B	65.6	○	×○	×	×	×	×	×	×
C	40.6	×	×	××	×	×	×	×	×
D	37.4	×	×	×	○×	×	×	×	×
E	30.0	×	×	×	×	××	×	×	×
F	27.6	×	×	×	×	×	○×	×	×
G	26.2	×	×	×	×	×	×	○×	×
H	17.4	×	×	×	×	×	×	×	×○

表 9. 姓・名・fukui をひとまとめにして解析した結果の各 *scale* による認証率

スケール	認証失敗率(%)	誤認率(%)
0.5	87.5	0.00
1.0	75.0	0.00
1.5	62.5	1.79
2.0	62.5	1.79
2.5	56.3	1.79
3.0	50.0	1.79

表 10 は，（姓・名・fukui・よく使用するフレーズ）の 4 つをひとまとめにして解析を行った認証結果である（ただし *scale* = 1.5 のとき）．表 11 は，それを各 scale によって認証率を求めた結果である．

表 10. 姓・名・fukui・よく使うフレーズをひとまとめにして解析した結果（*scale* = 1.5）

	語/分	A	B	C	D	E	F	H	H
A	79.0	××	×	×	×	×	×	×	×
B	65.6	×	××	×	×	×	×	×	×
C	40.6	×	×	××	×	×	×	×	×
D	37.4	×	×	×	××	×	×	×	×
E	30.0	×	×	×	×	××	×	×	×
F	27.6	×	×	×	×	×	○×	×	×
G	26.2	×	×	×	×	×	×	○×	×
H	17.4	×	×	×	×	×	×	×	××

表 11. 姓・名・fukui・よく使うフレーズをひとまとめにして解析した認証率

スケール	認証失敗率(%)	誤認率(%)
0.5	93.8	0.00
1.0	93.8	0.00
1.5	87.5	0.00
2.0	75.0	0.00
2.5	68.8	0.00
3.0	68.8	0.00

誤認することが全く無くなったことが分かる．しかし，今度は，認証失敗率がさらに大きくなった（全体の 2 回だけしか認証を受けていない）．これだけ認証失敗率が大きくなると個人認証システムとしての実用性はなくなる．

4-3. 各フレーズの 2 つ以上認証された場合に本人として認証

表 12 に，例として *scale* が 1.5 の場合の結果を表す．これを他の *scale* に当てはめた結果の認証率が表 13 である．後で示す 3 フレーズをまとめたもの（表 8）と比べて，認証失敗率が低く,良い結果を得ていることが分かる．誤認率も満足のいくものである．今回解析した 3 つの中では一番良い認証率を得た。

表 12. 表 2 から表 5 で○が 2 つ以上で本人とした場合

	語/分	A	B	C	D	E	F	G	H
A	79.0	×○	×	×	×	×	×	×	×
B	65.6	○	○○	×	×	×	×	×	×
C	40.6	×	×	○×	×	×	×	×	×
D	37.4	×	×	×	○○	×	×	×	×
E	30.0	×	×	×	×	×○	×	×	×
F	27.6	×	×	×	×	×	○○	×	×
G	26.2	×	×	×	×	×	×	○○	×
H	17.4	×	×	×	×	×	×	×	○×

表 13. 各 *scale* での認証率

scale	認証失敗率(%)	誤認率(%)
0.5	31.3	0.0
1.0	25.0	1.8
1.5	25.0	1.8
2.0	25.0	3.8
2.5	25.0	3.8
3.0	25.0	3.8

5．結論と考察

我々は，打鍵データから個人を認証する際の解析方法について議論してきた．第2章で述べたように，打鍵データの解析にもいろいろなものがあるが，本稿では4つの短いパスフレーズ(姓·名·fukui·よく使用するフレーズ）を使ってその打鍵間時間のデータによる個人認証を行った．

今回の実験は，あまりキーボードに慣れていないものを含む 8 人の被験者を対象に行われた．認証解析方法として，粕川達のノルムによる認証方法[3]を使い，検査方法を3つに分けたが，その中で一番良い認証率を得たのが本稿で我々が提案した「4つのパスフレーズの中で2つ以上認証されれば，個人として認証」する方法であった．

この方法は，他の論文ではまだ議論されていないし，ニューラルネットワークなどの方法に比べて簡単な解析方法であることもあり，今後の新しい認証方法として期待できる．

しかし，全体を通じて云えることは，打鍵データだけを情報リソースの保護に使うには，まだ不安が残る．パスワードなどと合わせて個人認証する方がより強固な個人認証を生むものと考えられる．

今回論じた実験はまだ一部である．現在次の方法を解析・検討中である．(1)今までの打鍵間時間はすべて隣接した文字間のみである．それを拡張してすべての文字間の打鍵間時間を計って解析をする．(2)認証方法自体として，音楽的リズムを用いた認証を取りいれる．これにより，あまりキーボードに慣れていない人もマウスを使うなどして個人認証をできる可能性がある．(3)今回の解析は粕川達のノルムによる方法を使ったが，他に多変量解析のマハラノビス距離による解析を取り入れて計算する．

最後に，本稿を作成するにあたってコンピュータセキュリティおよび生物的測定に対する個人認証システムについて，経営工学科の細貝康夫先生に貴重なご意見をいただいたことに感謝する．

参考文献

1) 小畑秀文：個人識別技術の現状と展望，システム／制御／情報，Vol.35, No. 7, pp. 383 – 389 (1991).

2) Joyce, R, and Gupta, G.: Identity Authentication Based on Keystroke Latencies, Comm. ACM, Vol. 33, No.2, pp. 168 – 176 (1990).

3) 粕川正充，森裕子，小松賢嗣，赤池英夫，角田博保：打鍵データに基づく個人認証システムの評価と改良，情報処理学会論文誌，Vol. 33, No. 5, pp. 728 – 735 (1992).

4) Brown, M. and Rogers, S. J. : User Identification via keystroke characteristics of typed names using neural networks, Int. J. Man-Machine Studies, Vol. 39, pp. 999 – 1014 (1993).

5) Umphress, D. and Williams, G. : Identity verification through keyboard characteristics, Int. J. Man-Machine Studies, Vol. 23, pp. 263 – 273 (1985).

6) Leggett, J. and Williams, G. : Verifying Identity via keystroke characteristics, Int. J. Man-Machine Studies, Vol. 28, pp. 67 – 76 (1988).

7) Leggett, J., Williams, G., Usnike, M. and Longnecker, M. : Dynamic identity verification via keystroke characteristics, Int. J. Man-Machine Studies, Vol. 35, pp. 859 – 870 (1991).

（平成10年12月21日受理）