打鍵データに基づく個人認証システムの評価と改良†

粕川正充†† 森 裕子†† 小松賢嗣††
赤池英夫†† 角田博保††

計算機ネットワークの普及などで，個人認証システムを改善する必要性が増してきている．Joyce と Gupta は打鍵間時間の個人差を用いる新しい認証システムを提案している．この方式は，{ユーザ名，パスワード，姓，名} を入力させ，あらかじめ登録された打鍵間時間パターンに合致するかどうかを検査するものである．しかし，このシステムをタイピング速度が低い被験者群（例えば一般の日本人）にそのまま用いると，特徴的なパターンが現れにくいなどの問題が出てきた．本研究では，この方式に改良を加え，タイピングの未熟な被験者群に対しても個人差を抽出可能な新しい認証システムを提案し，有効性を実証する．

1. はじめに

打鍵データに基づいた個人認証方式について，従来よりも認証率のよい方式を考案し実験によって検証した．

情報の重要性が高まったため，情報保護の面からより安全でかつ効率的な方法を用いる個人認証システムが要求されている．文献1）では個人の認証方法を次に示すように分類している．

個人を証明する物：鍵，ID カード，パスポート
知識　　：パスワード
動作　　：署名，行動パターン
身体的特徴　　：指紋，声色，網膜パターン

複数の人が資源やデータを共有するワークステーションのように，使用の際に前もって登録した本人かどうかの確認を必要とする計算機上では，一般には使用開始時にユーザ名とパスワードを入力し，その文字列があらかじめ登録してあるものと一致するかによって本人かどうかを判定する．この方法は，上記の「知識」というカテゴリーに分類される．

一方，欧米社会では個人認証に手書きによる署名が広く用いられている．手書きによる署名は書くという「動作」によって個人を特徴づけるものである．

この2つの認証システムを比較すると，「知識」によって認証を行うキャッシュカードの暗証番号に誕生日や電話番号など他人も容易に知りうる情報を用いている例があり，「知識」だけを用いた個人認証方法は，安全面でより劣っている．

そこで本人を特定するためのシステムとして暗証番号などのような記憶に頼る方法だけでなく，手書きによる署名のように動作の癖や特徴を利用する方法（上記の「動作」のカテゴリーを用いた方法）を併用することによってシステムの安全度を向上させることが期待できる．計算機上で収集できる利用者の動作に，打鍵パターンがある．打鍵パターンは，個人特有のものであり知識に比べて情報を得て偽造することが難しいといわれている[1]．

一般に認証システムを使用する時に起こる状況の組合せは以下の4通りである．

1. 正規の利用者が本人であると認証される．
2. 正規の利用者が本人であると認証されない．
3. 不法な利用者が正規の利用者であると認証される．
4. 不法な利用者が正規の利用者であると認証されない．

認証システムを使用する目的は，計算機内の資源やデータが正規の利用者だけによって操作され，他人によって情報が外に洩れたり壊されたりしないように保護することである．そのため認証システムでは，上記の1と4に比べて2と3が十分に起こりにくいことが望まれる．

打鍵パターンを考慮した個人認証システムの研究は今までも行われている[1),2)]．ここで述べる打鍵パターンとは，キーの種類と打鍵間時間（ある打鍵から直後の打鍵までの時間）の組の並びである．

打鍵パターンに基づく認証手法とは，利用者の打鍵パターン（検査データ）をあらかじめ登録された打鍵パターン（参照データ）と比較して本人かどうかを判定するものである．参照データと検査データの打鍵数

† An Evaluation and Improvement of User Authentication System Based on Keystroke Timing Data by MASAATSU KASUKAWA, YUKO MORI, KENZI KOMATSU, HIDEO AKAIKE and HIROYASU KAKUDA (Department of Computer Science, Faculty of Electro-Communications, The University of Electro-Communications).

†† 電気通信大学電気通信学部情報工学科

をかなり多く（100 語位）すれば，個人の認証を柔軟かつ確実に行うことができることが知られているが[2]，登録時に利用者にかかる負担は重くなる．そこで，個人が普段から慣れ親しんでおり，打鍵パターンも個人の特徴が現れやすいパターンを利用するという観点からユーザ名，パスワードに姓と名を加えたものを署名列として個人認証に用いる方法が考えられている．R. Joyce と G. Gupta はこの方法を基とし適当な距離尺度を定義して，参照データと検査データの距離が許容範囲ならば本人と判定する手法を考案した[1]．以下これを「Joyce-Gupta 手法」と呼ぶことにする．

筆者らは上記の手法を用い追実験を行って同手法の有効性を検討してみたところ，被験者の打鍵パターンのばらつきを十分に吸収することができず満足できる結果を得ることができなかった．そこで参照データと検査データとの比較方法に対して新たな手法を考案し実験を行い検定してみたところ，より良好な結果を得ることができた．

本論文では，Joyce-Gupta 手法および改良手法について説明し，行った認証実験について示す．また実験結果を検討し改良手法の有用性を示す．

2. JOYCE-GUPTA 手法

文献 1) で提案された認証手法について述べる．

[署名列]

Joyce-Gupta 手法では署名として使う打鍵列として，以下の 4 項目を用いる．

{ユーザ名，パスワード，姓，名}

以下これを「署名列」と呼ぶ．

被験者はプロンプトに従ってそれぞれの項目を打鍵する．その一連の打鍵列において，復帰改行キーを打ってから次の文字列の 1 文字目を打つまでの打鍵間時間は，その時々でかなりばらつくことが多いので個人の特徴を示す署名としては利用しない．1 文字目と 2 文字目の打鍵間から，各項目の文字列の最後の文字と復帰改行キーの打鍵間までの打鍵間時間列をもとにして認証を行う．このもととなる打鍵間時間列のことを「署名打鍵間時間列」と呼ぶ．

Joyce-Gupta 手法では，まず各利用者に自分の署名列を何度か入力させ，そこで得られた複数の署名打鍵間時間列から本人を特定するための特徴となるパターンを取り出す．このパターンを以下「参照署名」と呼ぶ．

参照署名とどの程度似ているかを示す距離尺度を定義し，本人と見なせる範囲を設定する．この許容範囲を以下「認証閾値」と呼ぶ．実際に利用者Xが利用者Aとしてログインしようとしたときの判定は，利用者Xが利用者Aの署名列を入力した時に得られる署名打鍵間時間列から利用者Aの参照署名までの距離が本人であるとみなせる認証閾値内にあるかどうか比較することによって行う．この検査を受けるために入力した署名列の署名打鍵間時間列を以下「検査署名」と呼ぶ．

[参照署名，認証閾値の算出方法]

次に参照署名と，参照署名から認証閾値を計算する方法を示す．

1) $n+1$ 文字からなる入力を 8 回行い，K_1 から K_8 の 8 個の署名打鍵間時間列を得る．

ここで，$K_i=(k_{i1}, k_{i2}, \cdots, k_{ij}, \cdots, k_{in})$, $(1 \leqq i \leqq 8)$ 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．また署名打鍵間数は n である．

2) 以下のようにして平均打鍵間時間列 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 $(k_{1j}, k_{2j}, \cdots, k_{ij}, \cdots, k_{8j})$

s_j＝標準偏差 $(k_{1j}, k_{2j}, \cdots, k_{ij}, \cdots, k_{8j})$

3) 8 個の署名打鍵間時間列 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

$$k_{ij} \leqq m_j + 3 * s_j \qquad (1)$$

が満たされるかどうかを調べる．これを満たさない k_{ij} を含む署名打鍵間時間列 K_i は稀なデータとして除去する．こうした条件のことを本論文ではデータ除去基準と呼ぶ．条件にかなう署名打鍵間時間列からなる集合を $KS=\{K_{i1}, K_{i2}, \cdots, K_{ir}\}$, $(1 \leqq r \leqq 8)$ 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．これを参照署名 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 に属する署名打鍵間時間列 K_i について，参照署名 R からのノルム $\mathrm{norm}(K_i, R)$ を計算する．ただし，$i \in \{i_1, i_2, \cdots, i_r\}$, $(1 \leqq r \leqq 8)$

$$\mathrm{norm}(K_i, R)=\sum_{j=1}^{n} |k_{ij}-r_j| \qquad (2)$$

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．ただし $i \in \{i_1, i_2, \cdots, i_r\}$, $(1 \leqq r \leqq 8)$

N_{mean}＝平均 $(\mathrm{norm}(K_i, R))$

N_{sd}＝標準偏差 (norm (K_i, R))

5) 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．

$$I = N_{mean} + 1.5 * N_{sd} \quad (3)$$

N_{sd} の係数（ここでは 1.5）のことを本論文では「スケール」と呼ぶ．

[検査署名の判定方法]

検査署名 $T=(t_1, t_2, \cdots, t_j, \cdots, t_n)$ について，参照署名 R からのノルム norm (T, R) を計算する．

$$\mathrm{norm}(T, R) = \sum_{j=1}^{n} |t_j - r_j| \quad (4)$$

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」と呼ぶことにする．

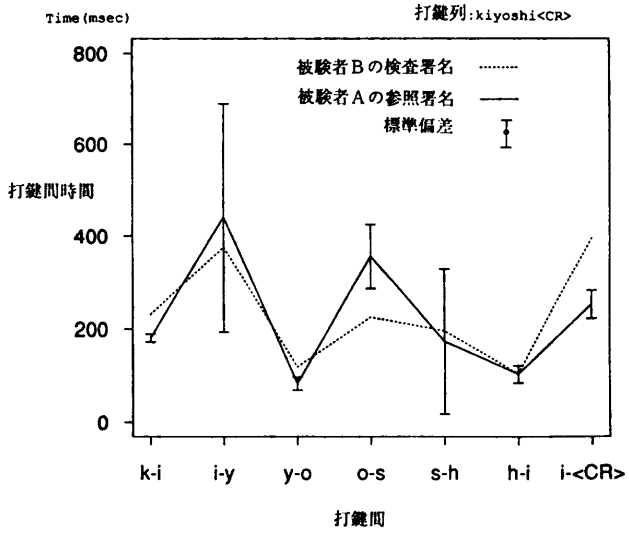

図 1 誤認が起こった例

Fig. 1 Example of invalid authentication (Accept other person).

3. 改良手法

3.1 予備実験

Joyce-Gupta 手法の有効性を見るために，ワークステーションやパソコンなどを日常的に使いキーボードを打ち慣れている大学生，大学院生および教官あわせて 6 人のボランティアを対象に，文献 1) の追実験として予備実験を行った．被験者の 6 人は各々の参照元となる署名列の時間データを登録した後，本人としての認証試行を 12 回，システム破りを試みる他人としての認証試行を他の被験者に対して 1 人について 12 回ずつ行い全体で計 432 回の試行を行った．参照署名の算出方法や認証閾値の設定は文献 1) に従った．この結果と文献 1) で示されている結果を表 1 に示す．文献 1) の結果と比べて大きな差があることがわかる．

この差がなぜ生じたかを調べるために，得られたデータを検討した．誤認が起こった例を図 1 に示す．この図は被験者Bが被験者Aに対してシステム破りを試み，成功した場合の署名列の一部を取り出したものである．

表 1 文献 1) と予備実験の比較

Table 1 Original Joyce-Gupta's result and our preexperiment's result.

	認識失敗率 (%)	誤認率 (%)
文献 1)	16.67	0.25
予備実験	45.83	2.92

図中，実線で被験者Aの参照署名を示した．単位はミリ秒である．併せて標準偏差をバー付の縦棒で示した．また，点線で被験者Bの検査署名を示した．入力された打鍵は "kiyoshi 〈CR〉" である．

この図から，被験者Aには *k-i* 間，*y-o* 間のように打鍵間時間の標準偏差が小さく打鍵のばらつきの小さい区間と，*i-y* 間，*s-h* 間のように標準偏差が大きく打鍵のばらつきの大きい区間があることがわかる．Joyce-Gupta 手法では，こうした打鍵間のばらつきの情報を個別に適用せず，ノルムとしてまとめて利用するため，打鍵間時間のばらつきの大きな打鍵間がばらつきの小さなものを覆い隠してしまう．

この例では被験者Bの打鍵は *k-i* 間，*y-o* 間，*o-s* 間，*i*-〈CR〉 間が被験者Aの標準偏差の範囲から離れている．しかし，被験者Aの *i-y* 間や *s-h* 間の標準偏差が大きいため，単純にノルムを取ると，この部分が影響して認証閾値が大きくなり，*k-i* 間などの標準偏差が小さい区間で明らかに本人とは違う打鍵間時間で打たれている部分が特徴として利用されず，誤認されてしまう．

この予備実験で明らかとなった Joyce-Gupta 手法の問題点として，

- ばらつきの大きい打鍵間がばらつきの小さい打鍵間での微妙な差を覆い隠してしまうこと，
- 参照署名登録時の打鍵間のばらつきに制限を与えないと，参照署名の許容範囲が広過ぎる場合が起

り，打鍵パターンが似ていなくても本人として認証されてしまうこと，

が挙げられる．

こうした問題点は，キーボードをさほど打ち慣れていない一般の利用者に対してより大きく影響を与えると考えられる．また，名前等をローマ字綴りで入力する場合，ひと息に打たれる打鍵の長さがローマ字の単位で切れる傾向がある．この場合には，切れ目で打鍵のばらつきが起こりやすいために，英単語を入力する場合よりいっそうこうした現象の影響を受けやすいと考えられる．

3.2 Joyce-Gupta 手法の改良

前節で得られた結果を考慮すると，打鍵間時間のばらつきが大きい人の個人認証の判定率を向上させるよう Joyce-Gupta 手法を改良するためには，打鍵間ごとの揺れの大小を強調する必要がある．そこでノルムの算出方法を以下のように変更した．

[ノルムの算出方法]

図2に被験者Cの署名打鍵間時間列（点線）とそこから計算した参照署名（実線）を部分的に取り出して示す．入力された打鍵は "komats-k〈CR〉" である．打鍵の揺れが大きい打鍵間と小さい打鍵間があり，この例では s-'-' 間が他の部分より大きく揺れていることがわかる．このログイン名を入力した者が被験者Cかどうかを判定する場合には，s-'-' 間の判定基準を緩く，他の部分の基準を厳しく検査すれば，より本人の特徴に沿った判定ができる．

そこで，採集したデータの中で打鍵の揺れが大きい打鍵間と揺れが小さい打鍵間を区別するために，式(4)で検査署名Tと参照署名Rの差の絶対値 $|t_i-r_i|$ そのものを使うのではなく，r_i に対する標準偏差で割った値を使う方法を考案した．この値を以下「新ノルム」と呼ぶ．新ノルムを用いることによって，打鍵間の揺らぎが大きい（標準偏差が大きい）区間はノルムに寄与する割合が小さくなり，揺らぎが小さい（標準偏差が小さい）区間は寄与する割合が大きくなる．揺らぎがない場合，標準偏差は0となるが，その場合は測定可能な最小単位の揺らぎがあったとして計算する．

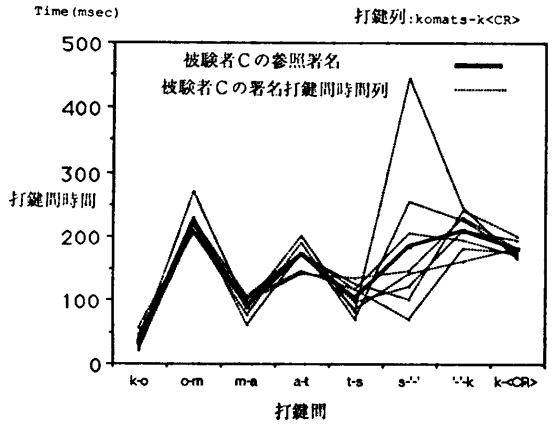

図2 打鍵のばらつきの例
Fig. 2 Example of variaties between keystroke intervals.

[新ノルムの算出方法]

KS を基にして打鍵間時間標準偏差列 $ns=(ns_1, ns_2, \cdots, ns_n)$ を計算する．ここで ns_j は j 番目の打鍵間時間の標準偏差にあたる．

ns_j＝標準偏差 $(k_{i_1,j}, k_{i_2,j}, \cdots, k_{i_r,j})$

KS に属する署名打鍵間時間列 K_i について，参照署名Rからの新ノルム newnorm(K_i, R) を ns を用いて計算する．ただし，$i \in \{i_1, i_2, \cdots, i_r\}$，$(1 \leqq r \leqq 8)$.

$$\text{newnorm}(K_i, R)=\sum_{j=1}^{n}\frac{|k_{ij}-r_j|}{ns_j} \qquad (5)$$

norm の代りに newnorm を使うことで新ノルムに対応する認証閾値 I_{new} が同様に定義できる．

[検査署名の判定方法]

検査署名の判定方法も norm を newnorm に変えるだけで同様に定義できる．

なお，この新ノルムを用いて図1の例を判定してみたところ誤認とはならなかった．

4. 実　　験

3章で提案した手法の有効性を Joyce-Gupta 手法と比較，検証するため，被験者を集めて実験を行った．

4.1 実験システム

NEC 製パーソナルコンピュータ PC-9801 RA 21 上に個人認証実験システムを作成した．C言語で約2,000 行程のプログラムで，精度5ミリ秒で被験者の打鍵を記録することができる．本システムでは UNIX システムへのログイン時の対話状況と同様に，被験者は画面に出るプロンプトに従って，ユーザ名，パスワード，姓，および，名を入力するように促される．被験者が検査署名を入力すると，試行ごとに認証判定結果（ログインできたかできないか）が画面に表示される．また，文字列を誤って打った場合には署名の最初から再入力を要求し，正しく入力されるまで繰り返させられる．

4.2 実験概要

[被験者]

被験者数は 32 人で，大学生・大学院学生および教官で日常的にキーボードを使っている人をボランティアとして募った（予備実験の6人も含まれる）．被験者は実験の目的の説明を受け，普段通りの打鍵を求められた．

[実験手順]

1) 署名打鍵間時間列の登録

被験者は自分の署名列を 12 回入力した．各打鍵間時間列は記録されており，測定した打鍵から署名打鍵間時間列を取り出した．

2) 参照署名の算出

収集した打鍵について，初めと終りの試行は慣れや心理的要因によって個人特有の打鍵パターンから大きく外れている可能性があるので，12 回の入力中初め2回と終り2回を除いた，中間8回分の署名打鍵間時間列を用いて参照署名を算出した．

3) 検査署名による認証実験

被験者の打鍵速度をあらかじめ測定しておき，打鍵速度が均等に散らばるよう 16 人の対象者を層別抽出した．各被験者は自分および他人4名に対してログインしようと試みた．この4名は 16 人の対象者から均一に散らばるように選んだ．誰が誰に対して試みるかは

表 2 実験結果
Table 2 Result of experiment.

文字/分		1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
342	1	1																															
327	2		5																														
301	3			0			0	0	0			0							0	0	0				0								
288	4				1																												
286	5	0				1								0	0		0	0							0			0		0			
272	6		0	0		0	3															0	0					0		0	0		
251	7				1			3		0	0		0			0								0			0						0
243	8								0																								
243	9			0	0	0				1			0										0				0		0		0		
242	a										2																						
235	b					0	0	0				6	0						0											0		0	
221	c	0							0				3				0						0		0	0			0			0	
220	d		0							0	0	0		2	0	0						0							0				
219	e														4																		
211	f															0																	
202	g			0	0									0			1			0	0			0								
189	h																	0															
181	i																		0														
179	j																			0													
174	k	0									0	0					0		0		2	0		0				0					
165	l		0						0	0								0		1		6			0			0					0
146	m																						1										
145	n						0	0						0	0	0					0			1	0								
143	o																								2								
122	p																									0							
118	q							0						0					0				0	0	0		1				0	0	
112	r	0				0	0				0	0								0	0							1		0			
112	s																												6				
100	t		0						0								0	0			0				0		0	0	2				
95	u																														0		
83	v			0	1								0		0	1										0	0				3	0	
83	w																																1

打鍵速度を層別化した以外は無作為に抽出してある．各々ログインしようとする相手(対象者)の署名列を8回ずつ入力し，合計で 1,280 回の認証試行を行った．

対象者それぞれに対して，他人が8人ずつ認証試行を行うことになる．対象者の署名列の文字列はあらかじめ被験者に示した．他人に対する予備的な情報（誰は打鍵が速いなどといった情報）は与えなかった．

試行ごとに検査署名と参照署名を比較し，ログインできたかどうかフィードバックを与えた．このフィードバックの計算は予備実験の結果からスケールを設定し新ノルムで算出される認証閾値を用いて判定し，成功不成功を表示した．

4.3 実験結果と考察

実験結果を**表2**に示す．これは，被験者 32 人それぞれが自分と他4人（縦軸）に対して認証試行を行った結果を示している．表中の値は最上列に並ぶ被験者がログインの目標となる人（左の縦軸に並んだ被験者）に対して行った8回の試行中にその人と認証された回数である．実験を行っていない組合せは空白にしてある．例えば被験者1は被験者1，5，c，k，r に対してログインを試みた結果，自分に対しては1回ログインでき，他の被験者に対してはログインできなかったことを示している．実験結果をみるとほとんどログインできてない．ログインできたかどうかのフィードバックを与えたことは結果にほとんど影響しなかったと考えられる．

実験で得たデータをもとにして，認証閾値計算式のスケールをさまざまに変化させて得られた認証失敗率と誤認率の関係を**表3**に示す．またノルムの計算をJoyce-Gupta 手法を用いて認証した結果も併せて示す．スケールを大きくすることは，判定の基準を緩めることであるため，認証失敗率は下がり，誤認率は上がる．個人認証システムにおいてはシステムの安全性を守るためには，認証失敗よりも誤認を起こさないことを優先する必要がある．

表3 新ノルムと Joyce-Gupta 手法のスケールによる比較
Table 3 New-norm and Joyce-Gupta way's result.

ノルム	スケール	認証失敗率(%)	誤認率(%)
新ノルム	0.5	91.4	0.0
新ノルム	1.0	85.9	0.1
新ノルム	1.5	77.0	0.4
新ノルム	2.0	68.4	1.2
新ノルム	2.5	60.5	1.6
新ノルム	3.0	54.3	2.1
新ノルム	3.5	46.5	2.7
新ノルム	4.0	40.6	3.8
新ノルム	4.5	32.4	5.1
新ノルム	5.0	24.6	6.0
Joyce-Gupta	0.5	55.9	4.3
Joyce-Gupta	1.0	34.8	9.0
Joyce-Gupta	1.5	22.7	13.8
Joyce-Gupta	2.0	16.4	20.2
Joyce-Gupta	2.5	11.3	25.5
Joyce-Gupta	3.0	7.0	29.9
Joyce-Gupta	3.5	3.1	34.3
Joyce-Gupta	4.0	2.3	40.0
Joyce-Gupta	4.5	1.2	43.2
Joyce-Gupta	5.0	0.8	47.4

新ノルムを用いた場合にはスケールを動かすことによって認証失敗率と誤認率が比較的緩やかに変化するが，Joyce-Gupta 手法をそのまま用いた場合には変動が急激である．また，Joyce-Gupta 手法ではスケールが 0.5 の場合でも誤認率が 4.3% となり，文献 1) で用いているスケール 1.5 では誤認率が 13.8% となる．これに比べて新ノルムを用いた場合には，誤認率が 0.1% から 6.0% 程度の範囲で収まっている．ざっとみてもずいぶん改善されていることがわかる．なお，予備実験での Joyce-Gupta 法との結果のずれは被験者群の違いによると考えられる．

4.4 データ除去基準の吟味

さらに結果を改善するためには，より本人らしさが現れていると考えられる揺らぎの少ない打鍵を参照署名として登録すればよい．

そこで，参照署名を登録する際に，文献 1) で行っているように打鍵間に対し式(1)で平均値から標準偏差の3倍以上離れているデータ系列を除くのではなく，中央値の2倍以上離れているデータを含む項目の打鍵間時間系列を除くことを考えた．

これは，データ件数が少ない場合，平均値よりも中央値の方がデータの変動による揺らぎの少ない代表値となることが知られているためである．本来は順序統計量に基づいて一定の信頼区間を設けるべきであるが，実地に即して参照署名を収集する場合には，文献 1) のように8件程度の少ないデータでは揺らぎがどの程度の区間にあるかを統計的に示すことは難しく，また参照署名の算出に多件数のデータを要求することは利用開始の際の登録に大きな手間が必要になるという問題がある．

そこでデータ除去基準として中央値を用いることとし，除去基準の簡便法として一般的な打鍵間時間は中央値を中心として左右対称であると考え，中央値の2倍以上の時間間隔を持つ打鍵を例外として除くことを考えた．また，これに基づいてデータ除去基準を変えることによって認証失敗率，誤認率を下げることがで

きるかどうかを調べた．

この新たなデータ除去基準に従って参照署名を計算し直したところ，標準偏差の3倍よりも厳しい基準であるため，除去されてしまう入力データが以前よりも増えた．そのため，参照署名の算出には 12 回の入力すべてを用いるものとし，最後に3件以上が残ればよいという基準を採用した．実験において，この基準を満たした被験者は 32 人中 27 人であった．以下の解析結果はこの被験者群についてのものである．新基準に従っての解析結果を表4に示す．表4は

1) ノルムに新ノルムを使うか
2) データ除去基準に中央値の2倍を用いるか標準偏差の3倍を用いるか
3) 閾値計算（式(3)）のスケールの変化

以上3点に対応した認証失敗率と誤認率を示したものである．Joyce-Gupta の場合の値が表3と違うのは中央値の2倍の除去基準によって除かれた5人を同様に除いて計算しているからである．表3と表4の結果を比較したところ，最も有効な方法は以下のようになった．

- 新ノルムを用いる．
- 中央値の2倍を基準にデータを除去する．
- 認証閾値 I の導出（式(3)）に用いるスケールを 6.5 とする．

この手法を「新 JG 手法」と呼ぶ．新 JG 手法と文献1) の手法を Wilcoxon 検定[5] を用いて比較した．個々の被験者のデータ対同士を組み合わせて順位付けを行い，比較してみたところ認証失敗率が5%水準で有意，誤認率が1%水準で有意という結果が得られた．

表 4 データ除去基準を変えた場合の比較
Table 4 New-norm, 2* median data removal and Joyce-Gupta way's result.

ノルム	データ除去基準	スケール	認証失敗率(%)	誤認率(%)
新ノルム	中央値の2倍	0.5	99.5	0.0
新ノルム	中央値の2倍	1.0	98.0	0.0
新ノルム	中央値の2倍	1.5	96.0	0.0
新ノルム	中央値の2倍	2.0	91.5	0.0
新ノルム	中央値の2倍	2.5	87.5	0.0
新ノルム	中央値の2倍	3.0	83.5	0.0
新ノルム	中央値の2倍	3.5	76.5	0.0
新ノルム	中央値の2倍	4.0	74.0	0.0
新ノルム	中央値の2倍	4.5	69.5	0.0
新ノルム	中央値の2倍	5.0	64.5	0.0
新ノルム	中央値の2倍	5.5	60.0	0.0
新ノルム	中央値の2倍	6.0	53.5	0.0
新ノルム	中央値の2倍	6.5	48.5	0.1
新ノルム	中央値の2倍	7.0	45.0	0.5
新ノルム	中央値の2倍	7.5	42.5	0.7
新ノルム	中央値の2倍	8.0	41.0	0.8
新ノルム	中央値の2倍	8.5	39.0	1.0
新ノルム	中央値の2倍	9.0	38.5	1.0
新ノルム	中央値の2倍	9.5	35.0	1.1
新ノルム	中央値の2倍	10.0	31.5	1.5
新ノルム	中央値の2倍	10.5	29.0	2.0
新ノルム	中央値の2倍	11.0	28.0	2.3
新ノルム	中央値の2倍	11.5	24.0	2.7
新ノルム	中央値の2倍	12.0	23.5	3.1
新ノルム	中央値の2倍	12.5	22.5	3.1
新ノルム	中央値の2倍	13.0	21.5	3.7
新ノルム	中央値の2倍	13.5	19.0	4.3
Joyce-Gupta	標準偏差の3倍	0.5	57.5	1.4
Joyce-Gupta	標準偏差の3倍	1.0	33.0	5.8
Joyce-Gupta	標準偏差の3倍	1.5	22.0	11.0
Joyce-Gupta	標準偏差の3倍	2.0	16.5	18.6
Joyce-Gupta	標準偏差の3倍	2.5	11.5	24.6
Joyce-Gupta	標準偏差の3倍	3.0	7.0	28.5
Joyce-Gupta	標準偏差の3倍	3.5	3.0	32.1
Joyce-Gupta	標準偏差の3倍	4.0	2.0	37.8
Joyce-Gupta	標準偏差の3倍	4.5	1.5	40.5
Joyce-Gupta	標準偏差の3倍	5.0	1.0	44.2

5. 考　　察

文献1) で行われた実験では，認証失敗率 16.67% 誤認率 0.25% と認証失敗率・誤認率共にかなり低く，望ましい結果となっているが，筆者らの行った実験ではそれほどよい結果が得られなかった．その理由として考えられるのは，文献1) の被験者群は，打鍵速度が，分速 43 語（分速約 215 文字）以上であったことである．今回筆者らが行った実験の被験者群は分速 83～342 文字の打鍵速度であった．打鍵速度だけでは被験者群の性質を規定できないが，一般に打鍵速度の速い利用者は打鍵間時間も安定しているので，文献1) での被験者は安定していたのではないかと推測される．

また，新たなデータ除去基準は参照署名を計算するためのデータ数を増加させる傾向があり，少ないデータを元にして参照署名を算出しようとする文献1) の方向とはそぐわないが，より本人らしい参照署名を求めるために，多少のデータ入力量の増加は止むをえないものと考えている．

6. おわりに

本研究で筆者らは打鍵を用いた認証方式として，文献1) の手法と同程度のデータと計算量でより良い結果の得られる認証方式を考案し検証することができた．本研究

の結果を実際の認証システムなどに応用する際には，現在用いられているパスワードと異なり，打鍵パターンの登録が問題になると考えられる．パスワードの重要性が少なくなる代わりに，アカウントを持つ本人の特徴的な打鍵パターンを多少の打鍵の揺らぎに対応して登録，判定できる方法が必要である．

セキュリティが問題になるようなアプリケーションにおいて，認証システムの頑健性を追及しすぎると，本人であっても正しく認証されない，あるいは認証されにくい，ということが起る．本研究の場合には，指先にけがをしただけでも打鍵パターンが変って認証されない，ということが起ると予測される．しかし，これに代る方法を容易に追加することは肝心のセキュリティを甘くすることになるため問題がある．こうした二律排反を解消するために，段階的な認証や曖昧さを認める OS といったような，OS の再構築を併せて考えていく必要がある．このような欠点はあるものの，打鍵間時間を用いた認証システムは実現の手軽さという点から実用性は高いと思われる．また，日本語ワープロの辞書にみられるような学習機能を持たせることによって，認証精度を向上させることが期待できる．

今回の実験では，署名列の打鍵間時間の値だけに着目した認証方法を検討したが，個人の特徴量を表すには，打鍵間時間以外にもキーを押す圧力や指使いの形など様々な要因が考えられる．しかし，打鍵間時間は現在のシステムで手軽に測定でき，これを利用したシステムは，パスワードなど記憶に頼るシステムに比べていっそう効果的な方法であることが判明した．今後，さらに効果的に個人の特徴を抽出する方法を検討する予定である．

参考文献

1) Joyce, R. and Gupta, G.: Identity Authentication Based on Keystroke Latencies, *Comm. ACM*, Vol. 33, No. 2, pp. 168-176 (1990).
2) Umphress, D. and Williams, G.: Identity Verification through Keyboard Characteristics, *Int. J. Man-Mach. Stud.*, Vol. 23, No. 3, pp. 263-273 (1985).
3) Card, S. K., Moran, T. P. and Newell, A.: *The Psychology of Human-Computer Interaction*, Lawrence Erlblaum Associates, Inc. (1983).
4) Gilb, T. and Weinberg, G. M.: *Humanized Input*, Winthrop Publishers, Inc. (1977).
5) Snedecor, G. W. and Cochran, W. G.: *Statistical Methods*, seventh ed., The Iowa State University Press (1980).

(平成3年9月12日受付)
(平成4年2月14日採録)

粕川 正充（正会員）

1960 年生．1983 年東北大学理学部数学科卒業．東京工業大学工学研究科情報科学専攻に進学．1985年理学修士．1990年同博士課程単位取得退学，同所において研究に従事，1991 年電気通信大学研究生として現在に至る．コンピュータと人間の間の界面の問題に興味を持つ．

森 裕子

平成3年電気通信大学計算機科学科卒業．4年次在学中ヒューマン・インタフェースに関する研究に従事．現在，住友銀行に勤務．

小松 賢嗣

平成3年電気通信大学計算機科学科卒業．4年次在学中ヒューマン・インタフェースに関する研究に従事．現在，セイコーエプソン(株)に勤務．

赤池 英夫（正会員）

昭和 62 年電気通信大学計算機科学科卒業．平成元年同大学大学院情報工学専攻博士課程前期修了．現在，同博士課程後期在学中．ウィンドウシステム，オペレーティングシステム，プログラミング言語に興味を持つ．

角田 博保（正会員）

昭和 25 年生．同 49 年東京工業大学理学部情報科学科卒業．同 51 年同大学院修士課程修了．同 57 年同大学院博士課程修了．同年電気通信大学計算機科学科助手，平成2年同大学情報工学科講師．理学博士．文字列処理，プログラミング方法論，ヒューマンインタフェース等に興味を持つ．ACM，日本ソフトウェア科学会各会員．