アルペジオ打鍵列を利用した個人認証手法の提案

粕川正充[†] 角田博保[††] 森 裕子[††]

R. Joyce と G. Gupta は個人認証を行う場合に，個人ごとの特徴をあるキーが打たれてから次のキーを打つまでの時間（以下，これを打鍵間時間と呼ぶ）に求め，その個人差を判定の基準とした個人認証手法を提案した．また筆者らはこの手法を改良し，新 JG 手法と呼ぶ別方式を提案した．さらに解析を進めて打鍵間時間の分布を調べるうちに，筆者らは連続多打鍵間の打鍵間時間の変動が，それを構成する個々の打鍵間時間の変動よりも小さくなる場合があることを見いだした．以下，この現象をアルペジオ打鍵と名付ける．このアルペジオ打鍵を利用することによって，Joyce と Gupta の提案した方法よりも効率的な個人認証手法を考案することができた．本論文では考案した手法について，JG 手法，新 JG 手法との比較のもとに説明し，実験を通じて新手法の優位性を検証する．

An Identity Authentication Method Based on Arpeggio Keystrokes

MASAATSU KASUKAWA,[†] HIROYASU KAKUDA[††] and YUKO MORI[††]

We previously reported some authentication mechanism of the workstation that worked well. For the further experiments, we found interesting phenomena. Interkeystroke timing of distance three or more keys often had a smaller variance than predicted from the sum of the timings of each keystroke. These kinds of keystrokes were named Arpeggio-keystrokes. To use these phenomena, a new authentication method (Arpeggio-Method) was developed. To compare with the older methods, we got much improved results with some experiments. This paper describes the mechanism of this method and reports the experimental result compared with previous methods.

1. はじめに

筆者らは R. Joyce と G. Gupta[1]の行った打鍵間時間を利用した個人認証実験の追試を行い，その実現における問題点を改良した新 JG 法を発表した（文献 2)．

さらに解析を進めた結果，筆者らは打鍵事象において，連続多打鍵を一単位とした打鍵動作が現れることを見出した．この現象は「本人らしさ」が普通の打鍵間時間よりもよく現れており，いっそう個人について特徴的である．この連続多打鍵列をアルペジオ打鍵列と呼ぶ．アルペジオ打鍵列を個人認証方式に応用することによって，より効率的な打鍵認証システムを構築できると考え，アルペジオ手法を考案した．さらに，その有効性を実験的に検証した．

なお，ここで論じる個人認証方式はタイピング速度の安定した熟練者を対象としたものであり，タイピング速度の揺らぎが大きい初心者を対象とした認証方式については，機会を改めて議論する．

以下 2 章ではこれまでに提案された打鍵間時間による打鍵署名の個人認証手法について示す．また 3 章では筆者らが提案するアルペジオ手法について述べる．4 章ではアルペジオ手法と他の手法を比較するための実験について結果を示して検討し，5 章では考察を行う．

2. 打鍵署名による個人認証手法

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）の対の並びから構成されるものを打鍵タイミングデータ列と呼ぶ．この打鍵タイミングデータ列のなかで，ユーザ名やパスワードといった特に認証に用いるものを打鍵署名と呼ぶ．この打鍵署名に基づく個人認証システムの研究はすでに行われており（文献 1)，その研究で用いられているのは利用者が入力する検査データを，あらかじめ登録した参照元データと比較して，本人かどうかを判定するという方式である．検査データがどれだけ参照元データに近いかとい

† 筑波大学大学院経営システム科学専攻
Graduate School of Systems Management, The University of Tsukuba
†† 電気通信大学情報工学科
Department of Computer Science, The University of Electro-Communications

う判定は，打鍵間時間だけに基づくのではなく，打鍵間時間がどのくらいばらついて打たれるかを示す指標(例えば標準偏差)にも基づいて判断されなければならない．

2.1 打鍵署名の構成要素

打鍵署名に使われる打鍵文字列（以下，署名列と呼ぶ）には利用者の特徴が現れやすい文字列を用いると効果的である．例えばユーザ名，パスワード，名前などである．これらは，各自それぞれ異なるとともに，普段から打ち慣れており，個人の特徴が現れやすいからである．参照元データとして，本人に自分の署名列を繰り返し入力させて得られた，特徴を抽出するための打鍵署名を「参照署名」と呼ぶ．また実際に認証を行う際に入力する打鍵署名を「検査署名」と呼ぶ．

2.2 JG 手 法

参照署名を8回入力し，個々の隣接2打鍵の打鍵間時間の平均と標準偏差を求める．署名列は｛ユーザ名，パスワード，ファーストネーム，ラストネーム｝である．

[不正データの除去]

この8回の試行中の打鍵間時間が（平均値±標準偏差×3）の範囲に入っていない場合，その参照署名はたまたま失敗してタイミングがずれたものとして，不正データと見なして除去する．こうして残った参照署名の平均打鍵間時間列を基準署名Rとする．

[判定基準の算出]

ある打鍵署名について，基準署名Rからの個々の打鍵間の差分の絶対値を合計したものをノルムと呼ぶ．不正データの除去後，基準署名算出に用いたそれぞれの参照署名のノルムを計算し，それらの平均値 Nm と標準偏差 Ns を求める．

本人であることを認める境界を定める認証閾値 I を以下のように定める（Sは正定数）．

$$I=Nm+S*Ns$$

標準偏差 Ns の係数 S を本論文では「スケール」と呼ぶ．文献1では $S=1.5$ となっている．

[検査署名の判定]

入力された検査署名について，基準署名Rからのノルム Nt を計算する．$Nt<I$ を満たす場合に本人であると判定する．

2.3 新 JG 法

文献2で示されている JG 手法の欠点は以下のとおりである．

- ある打鍵間の揺れの幅が大きすぎると，他の揺れの少ない部分がそれに覆い隠されてしまい，本人と他人の区別がつきにくい．
- 基準署名登録の際に揺らぎの大きな打鍵間が登録されていると，認証閾値が大きくなりすぎ，それほど似ていない打鍵署名でも本人と認証されてしまう．

これらの点を改良したのが新 JG 手法である．

[不正データの除去]

（平均値±標準偏差×3）ではなく，（中央値×2）以上の打鍵間を含んでいるような参照署名を不正データとして除去する．こうして残った参照署名の平均打鍵間時間列を基準署名Rとする．

[判定基準の算出]

ある打鍵署名について，各打鍵間の基準署名からの差分の絶対値をとり，それを対応する標準偏差で割った値を打鍵間すべてについて合計したものを新ノルムと呼ぶ．不正データ除去後，残った参照署名についての新ノルムの平均値を Nnm，標準偏差を Nns とする．認証閾値 I を以下のように定める（Sn は正定数）．

$$I=Nnm+Sn*Nns$$

この新ノルムのスケール Sn は文献2では4.5である．

[検査署名の判定]

入力された検査署名について，基準署名 R からの新ノルム Nnt を計算する．$Nnt<I$ を満たす場合に本人であると判定する．

2.4 誤認と認証失敗

認証システムを使用する際に，起こり得る状況の組合わせは以下の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と認証される．
4. 不法な利用者が正規の利用者と認証されない．

本論文では2.を認証失敗，3.を誤認と呼ぶ．

この認証システムでは認証失敗と誤認の間にはトレードオフがあり，一方を高めるともう一方は低くなる傾向がある．誤認率が高ければ，認証システムとしての存在意義が問題となり，また認証失敗率が高ければ利用者にストレスを与える．これらを考慮して適切な認証閾値を定める必要がある．

3. アルペジオ手法

個人ごとに異なるという打鍵署名の特徴は，隣接2打鍵間だけに現れるわけではない（文献3）．**図1**はある打鍵パターンの一部を取りだしたものである．例となっている打鍵パターンは k-a-w-a-s という一連の

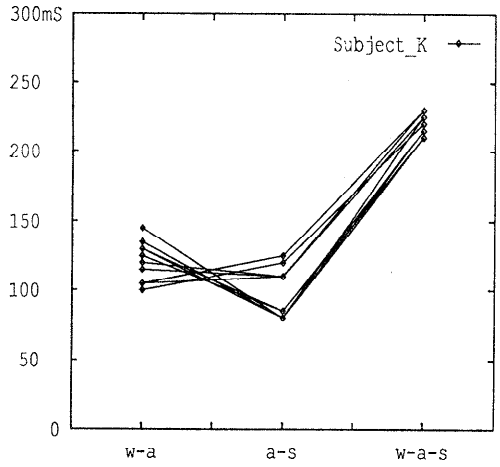

図 1 アルペジオ打鍵の例
Fig. 1 Example of Arpeggio keystrokes.

打鍵中の w-a, a-s 間（隣接2打鍵間）と，w-a-s 間（3打鍵間）の打鍵時間を示している．図中 w-a, a-s 間ともばらつきが大きいが，それに対応する w-a-s 間では，ばらつきが小さくなっていることがわかる．この被験者では，w-a-s を打つ時間がその個々の構成要素である w-a, a-s の時間より安定して打たれているのである．

ほかにもこのようなデータがないか，文献2の実験データから探してみた．

表1は文献2で行われた実験で求められた参照署名中に，より安定した隣接多打鍵間がどのくらいの頻度で含まれているかを示したものである．部分打鍵間すべて（隣接単打鍵間を含む）を標準偏差が小さいものから順に並べかえたもののうちに，それぞれ上位 20, 30, 40 に隣接多打鍵間がどの程度存在するかを示している．

この表から，上位 20 部分打鍵間中に，隣接3打鍵以上の打鍵間隔が 20% 以上含まれていることがわかる．

このように隣接単打鍵間ではなく，隣接多打鍵間に渡って測定したときにばらつきが小さくなる部分打鍵列に注目し，こうした部分打鍵列も認証に利用しようと考えた．以下にこれを用いた具体的な認証方法を示す．

3.1 参照署名の登録

n 打鍵間からなる打鍵署名 K を $(k_1, k_2, \cdots, k_n)$ とする．i, j 間の総打鍵間時間を $K_{[i,j]}=k_i+k_{i+1}+\cdots+k_j$ と定義する．ここで，k_i は i 番目の打鍵間時間とする．参照署名 $K1, K2, \cdots, K8$ に対して i, j 間

表 1 各被験者のアルペジオ打鍵比率
Table 1 Arpeggio keystroke ratio of each subject.

被験者	10件	20件	30件	40件
A	4(40.0%)	9(45.0%)	14(46.7%)	20(50.0%)
B	4(40.0%)	9(45.0%)	14(46.7%)	22(55.0%)
C	3(30.0%)	9(45.0%)	13(43.3%)	20(50.0%)
D	3(30.0%)	7(35.0%)	14(46.7%)	23(57.5%)
E	2(20.0%)	9(45.0%)	15(50.0%)	22(55.0%)
F	1(10.0%)	8(40.0%)	15(50.0%)	23(57.5%)
G	0(0.0%)	4(20.0%)	11(36.7%)	17(42.5%)
H	2(20.0%)	6(30.0%)	13(43.3%)	21(52.5%)
I	0(0.0%)	5(25.0%)	13(43.3%)	21(52.5%)
J	0(0.0%)	6(30.0%)	13(43.3%)	21(52.5%)
K	2(20.0%)	6(30.0%)	15(50.0%)	22(55.0%)
L	3(30.0%)	8(40.0%)	13(43.3%)	20(50.0%)
M	6(60.0%)	12(60.0%)	19(63.3%)	25(62.5%)
N	2(20.0%)	8(40.0%)	15(50.0%)	24(60.0%)
O	4(40.0%)	7(35.0%)	13(43.3%)	20(50.0%)
P	2(20.0%)	6(30.0%)	16(53.3%)	24(60.0%)
Q	1(10.0%)	5(25.0%)	12(40.0%)	20(50.0%)
R	2(20.0%)	7(35.0%)	13(43.3%)	21(52.5%)
S	1(10.0%)	5(25.0%)	11(36.7%)	20(50.0%)
T	2(20.0%)	5(25.0%)	13(43.3%)	21(52.5%)
U	3(30.0%)	8(40.0%)	11(36.7%)	18(45.0%)
V	4(40.0%)	11(55.0%)	17(56.7%)	23(57.5%)
W	1(10.0%)	6(30.0%)	14(46.7%)	21(52.5%)
X	3(30.0%)	7(35.0%)	13(43.3%)	19(47.5%)
Y	4(40.0%)	8(40.0%)	11(36.7%)	21(52.5%)
Z	1(10.0%)	7(35.0%)	14(46.7%)	19(47.5%)
AA	0(0.0%)	6(30.0%)	13(43.3%)	21(52.5%)
BB	2(20.0%)	7(35.0%)	13(43.3%)	19(47.5%)
CC	1(10.0%)	7(35.0%)	14(46.7%)	21(52.5%)
DD	1(10.0%)	5(25.0%)	11(36.7%)	18(45.0%)
EE	2(20.0%)	7(35.0%)	14(46.7%)	23(57.5%)
FF	6(60.0%)	12(60.0%)	17(56.7%)	21(52.5%)

の総打鍵間時間の平均と標準偏差を以下のように求める．

$m_{[i,j]}$＝平均 $(K1_{[i,j]}, K2_{[i,j]}, \cdots, K8_{[i,j]})$

$sd_{[i,j]}$＝標準偏差 $(K1_{[i,j]}, K2_{[i,j]}, \cdots, K8_{[i,j]})$

（ただし，$1 \leqq i \leqq j \leqq n$）

$SD=\{sd_{[1,1]}, sd_{[1,2]}, \cdots, sd_{[1,n]}, \cdots, sd_{[n,n]}\}$ を昇順にソートし，得られるインデックスより先頭から N 個を順に取りだしたものを I とすると，

$I=\{[p1, q1], [p2, q2], \cdots, [pN, qN]\}$

$(sd_{[p1,q1]} \leqq sd_{[p2,q2]} \leqq \cdots \leqq sd_{[pN,qN]})$

である．このインデックス I のことを基準署名インデックスと呼ぶ．

3.2 認証検査方法

入力された検査署名 Kt を $(kt_1, kt_2, \cdots, kt_n)$ とする．基準署名インデックス I より，

$T=\{Kt_{[p1,q1]}, Kt_{[p2,q2]}, \cdots, Kt_{[pN,qN]}\}$

を作る．また認証基準時間差dを設定し，Tに属する部分打鍵間時間列について，

$I'=\{(p,q)\,|\,|Kt[p,q]-m[p,q]|\leqq d,\ (p,q)\in I\}$

を作り，$(|I'|/|I|)\geqq P$ ならば検査署名は認証されたものと判定する．

要するに，揺れの少ない多打鍵間をN個選び，そのうちで基準値からの差が d 以下のものが P の比率以上あれば本人と考えるのである．

3.3 認証パラメータの設定

2章で述べた S, Sn のかわりに新たな認証パラメータ N, d, P が導入された．

これらのパラメータは署名の性質と関連しており，Nは署名を構成する打鍵数に影響を受け，Pは統計的な揺らぎと関連し，dは個人の打鍵特性と関係する．これらの値を決めるため，個人認証システムとして用いる場合に許容される基準として誤認率 0.5% 以下，認証失敗率 50% 以下を定めた．得られた誤認率および認証失敗率がこの基準を満たさない場合には，誤認率 0.5% 以下を満たす最も小さい認証失敗率を与える場合を採択する．

文献2で行われた実験から得られたデータに基づいて，あらかじめ計算した結果，パラメータの値を $N=20$, $P=0.9$, $d=50$ ms と定めておき，このパラメータに従って計算を行うものとする．

4. 実　　験

アルペジオ手法を JG 手法，新 JG 手法と比較するため，これらの手法すべてを含む形で実験を企画，実施した．

4.1 実験システム

パーソナルコンピュータ (NEC 製 PC-9801 RA 21) 上に作成された個人認証実験システムを用いて実験を行った．このシステムはC言語約 2000 行で記述されており，精度5ミリ秒で打鍵時間を記録できる．また，UNIX へのログイン時の対話状況を模倣しており，被験者は画面に出るプロンプトに従って {ユーザ名，ラストネーム，ファーストネーム，パスワード} を入力することになる．署名列があらかじめ登録されたものと一致しない場合には再入力が要求される．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（ログインできたかどうか）が画面に表示される．

4.2 実験概要

[被験者]

被験者数 19 人，大学生・大学院生および教官でワープロやプログラミングなどで日常的にキーボードを使って作業していて，ブラインドタッチまたはそれに近い打鍵を行う人をボランティアとして募った．

被験者は実験の目的の説明を受け，普段どおりの打鍵を求められた．

[実験手順]

（1） 被験者による署名打鍵の練習

文献1では打ち慣れているという仮定から自分の氏名を選択していたが，文献2で行った実験結果から，ユーザ名などと比較してさほど熟達しているわけではないということが判明した．また，パスワードも現実の物を使わないように指示したため，新しいパスワードの練習も必要となった．そこで，被験者に対して各自の署名列の各項目をおのおの 50 回ずつ練習させた．さらにその後，{ユーザ名，ラストネーム，ファーストネーム，パスワード} を1セットとして 10 回の練習を行わせた．

（2） 被験者による参照署名の登録

実験する3つの手法のうち，登録条件が最も厳しい新 JG 手法に従ってデータ除去基準を設定し，登録を行った．データ登録時に集めたデータから各文字間の打鍵間時間に対して中央値を求め，中央値の2倍を越える時間のデータが含まれていた場合には，その打鍵署名を捨てる．こうして最終的に必要な数の打鍵署名が得られるまで入力を繰り返させた．

アルペジオ手法の基準署名インデックスは，データ除去基準を考えずに3回目から 10 回目までの入力によって計算している．また JG 手法はアルペジオ手法と同様に3回目から 10 回目までの入力に対し，より緩い条件の（平均値±標準偏差×3)をデータ除去基準として判定し，8件に不足する分はそれ以降の入力から補っている．

（3） 検査署名による認証実験

参照署名の登録時に測定した打鍵速度順に被験者を4グループに分け，それぞれのグループから2人ずつ合計8人をログインの対象者に選んだ．各被験者はまず自分自身に対して8回ずつ2セットの認証実験を行い，次に8人の対象者から各グループに属する対象者を1人ずつ選び，この4人に対して8回ずつのログインを試みた．このうち，自分自身に対しての実験において，最初のセットでは認証されたかどうかの判定を

せず，次のセットでは試行ごとに判定し，結果を表示して被験者にフィードバックした．

4.3 実験結果

認証結果（成功失敗）を表示した場合としなかった場合の打鍵間時間の違いを比較してみたところ，試行ごとの違いに較べて十分に小さかったので，以下の解析では認証結果を表示した場合のみについて検定した．

表 2 アルペジオ手法による認証実験結果
Table 2 Results of Arpeggio Authentication Method.

N	P	d	30mS	40mS	50mS	60mS	70mS	80mS	90mS	100mS
5	100%	誤認率	0.0	1.3	2.8	5.6	9.1	12.5	15.3	18.9
		認証失敗率	50.7	29.0	22.4	18.4	12.5	9.2	6.6	4.6
	80%	誤認率	2.3	7.4	12.5	17.4	25.2	31.7	40.3	48.4
		認証失敗率	26.3	13.8	9.9	7.2	4.6	2.6	1.3	0.7
10	100%	誤認率	0.0	0.2	**0.5**	0.8	1.6	2.8	4.3	5.6
		認証失敗率	82.2	60.5	**44.1**	34.2	28.3	23.0	17.1	17.1
	90%	誤認率	0.0	0.8	1.6	3.3	6.1	8.9	10.9	13.3
		認証失敗率	57.9	34.9	22.4	17.8	12.5	9.9	8.6	7.2
	80%	誤認率	**0.3**	2.3	4.0	6.6	11.4	16.0	21.4	26.5
		認証失敗率	**40.8**	20.4	13.8	7.9	6.6	5.3	4.6	2.6
15	100%	誤認率	0.0	0.0	0.0	**0.0**	**0.3**	0.7	1.3	2.3
		認証失敗率	93.4	77.0	57.9	**45.4**	**36.2**	29.0	21.1	19.1
	93%	誤認率	0.0	0.0	**0.2**	**0.5**	1.8	4.0	5.8	8.1
		認証失敗率	78.3	52.0	**34.2**	**27.0**	19.1	17.1	15.1	13.8
	87%	誤認率	0.0	**0.2**	0.8	2.1	5.3	9.1	13.3	16.1
		認証失敗率	59.9	**35.5**	25.7	16.5	13.2	10.5	9.2	7.2
	80%	誤認率	**0.0**	1.0	1.6	4.9	10.4	16.0	20.1	26.2
		認証失敗率	**49.3**	23.7	16.5	9.9	8.6	7.9	5.9	5.3
20	100%	誤認率	0.0	0.0	0.0	0.0	**0.2**	**0.2**	**0.5**	1.0
		認証失敗率	98.0	87.5	74.3	58.6	**44.7**	**33.6**	**25.0**	22.4
	95%	誤認率	0.0	0.0	0.0	**0.0**	**0.3**	0.7	1.3	2.5
		認証失敗率	89.5	71.1	52.0	**36.2**	**26.3**	20.4	18.4	16.5
	90%	誤認率	0.0	0.0	**0.0**	**0.2**	1.0	2.0	3.6	5.3
		認証失敗率	79.6	61.2	**34.9**	**23.7**	16.5	13.8	12.5	11.8
	85%	誤認率	0.0	**0.0**	**0.2**	1.0	2.3	4.6	7.4	9.9
		認証失敗率	70.4	**43.4**	**28.3**	19.7	12.5	11.2	8.6	7.9
	80%	誤認率	0.0	**0.3**	1.0	2.0	4.8	8.9	13.8	16.9
		認証失敗率	61.8	**32.2**	21.7	13.8	11.2	10.5	8.6	6.6
25	100%	誤認率	0.0	0.0	0.0	0.0	0.2	**0.2**	**0.2**	0.7
		認証失敗率	99.3	89.5	77.6	67.8	54.6	**45.4**	**31.6**	26.3
	96%	誤認率	0.0	0.0	0.0	**0.0**	**0.2**	**0.3**	1.0	1.6
		認証失敗率	96.7	81.6	65.8	**49.3**	**34.9**	**26.3**	20.4	17.1
	92%	誤認率	0.0	0.0	**0.0**	**0.0**	0.7	1.0	2.1	3.8
		認証失敗率	87.5	71.7	**46.1**	**30.3**	21.1	17.8	15.8	13.8
	88%	誤認率	0.0	0.0	**0.0**	**0.5**	1.3	3.1	5.1	7.1
		認証失敗率	79.6	59.9	**36.2**	**25.7**	17.1	12.5	11.8	11.2
	84%	誤認率	0.0	**0.0**	**0.5**	0.8	2.3	4.8	8.6	11.8
		認証失敗率	73.0	**42.8**	**27.6**	18.4	13.8	11.8	11.2	9.2
	80%	誤認率	0.0	**0.2**	0.7	2.1	4.4	8.6	13.5	16.9
		認証失敗率	67.1	**37.5**	23.7	14.5	12.5	11.2	8.6	7.2
30	100%	誤認率	0.0	0.0	0.0	0.0	0.2	0.2	**0.2**	**0.5**
		認証失敗率	99.3	93.4	86.2	71.7	61.8	52.6	**42.1**	**34.2**
	97%	誤認率	0.0	0.0	0.0	0.0	**0.2**	**0.3**	0.7	1.2
		認証失敗率	98.7	87.5	69.7	59.9	**49.3**	**38.8**	27.6	22.4
	93%	誤認率	0.0	0.0	0.0	**0.0**	**0.5**	0.8	1.6	3.1
		認証失敗率	94.1	80.3	61.8	**48.7**	**33.6**	25.7	20.4	17.1
	90%	誤認率	0.0	0.0	0.0	**0.0**	0.8	1.6	3.5	5.3
		認証失敗率	86.8	73.7	52.0	**34.9**	25.0	17.8	15.1	14.5
	87%	誤認率	0.0	0.0	**0.0**	**0.5**	1.3	3.5	5.9	8.6
		認証失敗率	83.6	65.8	**42.1**	**27.6**	18.4	14.5	13.8	11.8
	83%	誤認率	0.0	0.0	**0.2**	1.0	2.1	5.3	8.7	12.3
		認証失敗率	79.0	52.0	**32.2**	21.1	15.8	13.8	12.5	10.5
	80%	誤認率	0.0	**0.2**	**0.5**	1.3	4.1	7.6	12.3	14.8
		認証失敗率	71.1	**45.4**	**27.6**	16.5	14.5	11.8	9.2	8.6

各項目の単位はパーセント。認証基準を満たす場合は太字で示す。

この実験における平均署名列長は 27.9 であった．3章における3つのパラメータ N, P, d をそれぞれ N は5から 30 まで5刻み，P は 0.6 から 1.0 まで（N によって変化するため刻みは不定），d は 30 ms から 100 ms まで 5 ms 刻みで変化させることによって得られた結果を**表 2** に示す．認証基準を満たす項目は太字で示す（以下，表3，表5も同様）．3.3 節で示した，この実験とは独立に選んだパラメータ $N=20$, $P=0.9$, $d=50$ ms では誤認率 0.0%，認証失敗率 34.9% となり，認証基準として定めた誤認率 0.5% 以下，認証失敗率 50.0% 以下を満たした．また，JG手法および新JG手法において，スケールの変化に対応する認証失敗率と誤認率を**表 3** に示す．表を見やすくするために，スケールの変化は 0.5 とした．

手法の優劣比較を行うに当たって Wilcoxon 検定を用いた．この検定方法は，2つの手法についてその優劣を比較する方法であり，母集団の形を仮定しないノンパラメトリック法である．母集団として正規性を仮定すれば t 検定などの，より感度の高い検定方法を用いることができるが，実験によって得られたデータは正規分布に当てはめるには無理があるため，この方法を選んだ．

同じ誤認率に対する認証失敗率について検定を行った．誤認率を 0% から 0.5% の範囲で固定し，この時の認証失敗率を比較した（**表 4**）．表2，3よりさらに細かく，0.1 刻みで S および Sn を変化させた結果と，N, P, d をより細かく変化させて誤認率の小さくなる点を探した．こうして手法ごとに誤認率が 0%，0.2%，0.5%（それぞ

表 3 JG 手法および新 JG 手法による認証実験結果
Table 3 Results of JG and New-JG Authentication Method.

手法	データ除去基準	スケール	認証失敗率	誤認率
ＪＧ手法	平均値 ±(3×標準偏差)	0.5	67.8	0.0
ＪＧ手法	平均値 ±(3×標準偏差)	1.0	**63.2**	**0.2**
ＪＧ手法	平均値 ±(3×標準偏差)	1.5	51.3	2.3
ＪＧ手法	平均値 ±(3×標準偏差)	2.0	46.1	3.6
ＪＧ手法	平均値 ±(3×標準偏差)	2.5	36.8	6.6
ＪＧ手法	平均値 ±(3×標準偏差)	3.0	29.6	9.4
ＪＧ手法	平均値 ±(3×標準偏差)	3.5	19.1	12.0
ＪＧ手法	平均値 ±(3×標準偏差)	4.0	13.2	16.1
新ＪＧ手法	2 × 中央値	0.5	94.7	0.0
新ＪＧ手法	2 × 中央値	1.0	90.8	0.0
新ＪＧ手法	2 × 中央値	1.5	85.5	0.0
新ＪＧ手法	2 × 中央値	2.0	77.0	0.0
新ＪＧ手法	2 × 中央値	2.5	72.4	0.0
新ＪＧ手法	2 × 中央値	3.0	65.1	0.0
新ＪＧ手法	2 × 中央値	3.5	53.9	0.2
新ＪＧ手法	2 × 中央値	4.0	**49.3**	**0.5**
新ＪＧ手法	2 × 中央値	4.5	36.8	0.7
新ＪＧ手法	2 × 中央値	5.0	30.9	1.5
新ＪＧ手法	2 × 中央値	5.5	25.7	2.5
新ＪＧ手法	2 × 中央値	6.0	18.4	3.6

各項目の単位はパーセント。認証基準を満たす場合は太字で示す。

表 4 各手法の誤認率 0%, 0.2%, 0.5% での認証失敗率
Table 4 False alarm rate in JG, New-JG and Arpeggio Authentication Methods (Imposter pass rate 0%, 0.2%, 0.5%).

誤認率	JG 手法	新 JG 手法	アルペジオ手法
0%	66.4% (S=0.7)	59.9% (S_n=3.2)	30.3% (N=25,P=0.92,d=60ms)
0.2%	63.2% (S=1.0)	49.3% (S_n=3.6)	23.7% (N=20,P=0.90,d=60ms)
0.5%	なし (------)	38.2% (S_n=4.4)	21.1% (N=25,P=0.96,d=85ms)

れ 0/608, 1/608, 3/608—件数比）となるような点のうちで，認証失敗率が最小となる点を選びだした．これ以上刻み幅を小さく取っても打鍵間時間計測上の誤差から，あまり意味を持たない．また JG 手法において，S を 0.1 刻みで変化させたところ，誤認率が 0.5% となるような点を求めることができなかったため，なしと表記した．これに最も近い点は $S=1.1$ でこの時の誤認率は 0.8%，認証失敗率は 59.9% であった．

まず，JG 手法とアルペジオ手法を比較したところ，0%点，0.2% 点とも有意水準 1% 水準で有意という結果が得られた（$P<0.0052$ および $P<0.0040$, $f.=18$）．

また新 JG 手法とアルペジオ手法を比較した結果，0% 点，0.2% 点とも有意水準 1% で有意（$P<0.0068$ および $P<0.0046$, $d.f.=18$），また 0.5%点ではかろうじて有意差は出なかったが，7％という事実上有意な値が得られた（$P<0.07$, $d, f.=18$）．

この結果により JG 手法，新 JG 手法に対するアルペジオ手法の優位性が示された．アルペジオ手法は誤認率 0.5% 以下という基準で，認証失敗率が他の手法のほぼ 1/2 という低さであった．

5. 考　　察

[揺らぎに対する安定]

アルペジオ手法の各パラメータを 3 次元の座標系と見なして，認定基準を満たすパラメータを座標系における 3 次元図形と考える（認定基準を満たす範囲を表 2 中に太字で示す）．このときの図形の重心は，最も安定して判定できる値になる．この重心を計算した結果 $N=23$, $P=0.90$, $d=57.4$ が得られた．この値を用いて計算した結果，誤認率は 0.0%，認証失敗率は 35.5 % となった．認定基準を満たす点は重心を中心として，$N=5$〜30, $P=0.667$〜1.0, $d=30$〜100 と広い幅を持っており，検査した格子点 630 点中の 15.5% が基準を満たしている．JG 手法，新 JG 手法の問題点の一つは，スケールの変動によって認証失敗率，誤認率が大きく変ってしまう点である．JG 手法では今回の実験では基準値を満たす点を得ることができず，また新 JG 手法でも基準値を満たす点は $Sn=3.8$〜4.4 までのかなり狭い範囲に限定される．アルペジオ手法はこれらに比べてより安定した方法であり，N や d などをかなりラフに決めても十分に性能を発揮することがわかった．

[データ除去基準の排除]

JG 手法ではデータ除去基準として，（平均値±標準偏差×3）を用い，新 JG 手法では，中央値の 2 倍を用いている．アルペジオ手法では，N 個を選択するため例外文字は自動的に除去される傾向があるのでデータ除去基準を用いていない．実験において参照署名を登録する際に，JG 手法では除去されるデータはほとんどなかった．しかし，新 JG 手法では，最も多かった被験者で正しいデータ 8 件に対して 33 回の入力が必要であった．データ除去基準を設けないことによって参照署名の登録の負担はかなり軽減されると考えられる．

[認証に必要な計算量]

アルペジオ手法では，基準署名の計算のために，N^2 項目の浮動小数点のソートが必要となり，かなり

大量の計算が必要となるが，検査時には整数の比較と加算だけで済む．一方 JG 手法，新 JG 手法とも検査時にはノルムの計算およびスケールの計算に浮動小数点計算が必要となる．計算量はどちらも $O(n)$ である．

表 5 打鍵列が短い場合の結果
Table 5 Results of Arpeggio Authentication Method (short keystrokes).

N	P	d	30mS	40mS	50mS	60mS	70mS	80mS	90mS	100mS
5	100%	誤認率	0.8	2.3	4.6	6.1	8.4	11.7	15.0	18.3
		認証失敗率	59.9	36.2	24.3	20.4	16.5	15.1	12.5	11.2
	80%	誤認率	3.1	8.7	14.3	19.9	27.5	32.1	38.0	43.6
		認証失敗率	26.3	17.1	11.8	9.9	6.6	5.3	4.0	2.6
10	100%	誤認率	0.0	0.8	0.8	1.3	2.0	3.6	5.3	7.9
		認証失敗率	82.2	64.5	51.3	40.1	29.0	24.3	17.8	17.1
	90%	誤認率	0.3	1.2	1.5	2.8	5.4	9.4	13.2	17.8
		認証失敗率	67.1	46.1	32.9	25.7	19.7	15.8	14.5	13.8
	80%	誤認率	1.0	2.1	4.6	9.4	16.9	22.2	27.8	32.2
		認証失敗率	51.3	34.2	20.4	13.8	11.8	11.8	10.5	8.6
15	100%	誤認率	0.0	0.0	0.2	0.2	0.7	1.3	2.0	3.0
		認証失敗率	90.1	79.6	66.5	52.0	42.8	35.5	24.3	19.1
	93%	誤認率	0.0	0.2	**0.2**	**0.5**	1.6	3.6	5.6	6.7
		認証失敗率	80.9	62.5	**48.0**	**38.8**	28.3	19.1	17.1	13.8
	87%	誤認率	0.0	0.3	0.8	1.8	3.8	5.9	9.7	12.3
		認証失敗率	74.3	54.6	37.5	26.3	19.7	17.1	13.8	13.8
	80%	誤認率	0.0	0.7	1.8	3.8	7.2	11.2	15.1	19.6
		認証失敗率	68.4	42.8	29.6	21.1	15.8	13.8	12.5	11.2
20	100%	誤認率	0.0	0.0	0.0	0.0	**0.5**	1.3	1.6	2.1
		認証失敗率	94.1	85.5	72.4	59.2	**49.3**	40.8	28.3	24.3
	95%	誤認率	0.0	0.0	0.2	**0.3**	1.3	2.6	3.8	4.9
		認証失敗率	87.5	73.7	61.2	**45.4**	35.5	27.0	20.4	17.1
	90%	誤認率	0.0	0.2	**0.3**	1.3	2.5	3.8	6.4	8.9
		認証失敗率	81.6	63.8	**45.4**	34.9	26.3	19.7	18.4	16.5
	85%	誤認率	0.0	0.0	0.7	1.8	4.3	7.1	10.4	12.7
		認証失敗率	78.3	55.3	38.2	27.6	21.1	17.1	14.5	12.5
	80%	誤認率	0.0	0.7	1.8	3.1	6.9	10.4	14.8	18.6
		認証失敗率	73.0	48.0	34.2	23.0	16.5	15.8	14.5	11.2
25	100%	誤認率	0.0	0.0	0.0	0.0	0.5	1.2	1.3	1.8
		認証失敗率	95.4	88.8	79.6	70.4	59.2	45.4	34.9	30.9
	96%	誤認率	0.0	0.0	0.0	0.2	0.8	1.5	2.3	2.8
		認証失敗率	90.8	82.2	71.7	56.6	44.7	36.8	28.3	24.3
	92%	誤認率	0.0	0.0	0.0	0.8	1.5	2.5	4.8	6.3
		認証失敗率	90.1	78.3	60.5	45.4	34.2	27.0	23.0	18.4
	88%	誤認率	0.0	0.0	0.3	1.2	2.3	4.3	6.3	10.0
		認証失敗率	85.5	66.5	52.0	39.5	28.3	23.7	19.1	17.1
	84%	誤認率	0.0	0.2	0.7	1.8	4.0	6.6	9.9	12.7
		認証失敗率	82.2	61.2	43.4	33.6	24.3	21.1	15.1	13.8
	80%	誤認率	0.0	0.5	1.5	2.3	5.9	9.1	13.3	16.8
		認証失敗率	77.0	56.6	36.8	24.3	20.4	16.5	14.5	12.5
30	100%	誤認率	0.0	0.0	0.0	0.0	0.3	1.0	1.2	1.5
		認証失敗率	98.7	93.4	86.2	76.3	63.2	48.7	40.8	35.5
	97%	誤認率	0.0	0.0	0.0	0.2	0.3	1.2	1.8	2.1
		認証失敗率	94.7	87.5	79.0	64.5	51.3	44.1	33.6	29.6
	93%	誤認率	0.0	0.0	0.0	0.3	1.0	1.8	3.1	4.3
		認証失敗率	91.5	83.6	70.4	55.9	42.8	32.2	25.7	23.7
	90%	誤認率	0.0	0.0	0.0	**0.5**	2.0	3.1	4.8	6.7
		認証失敗率	90.8	77.6	63.2	**47.4**	35.5	28.3	25.0	21.1
	87%	誤認率	0.0	0.0	0.5	0.8	2.5	3.8	6.4	8.9
		認証失敗率	86.8	71.7	57.2	41.5	30.9	25.7	21.1	16.5
	83%	誤認率	0.0	0.3	**0.5**	1.5	3.5	6.3	9.1	11.7
		認証失敗率	84.2	67.8	**50.0**	34.2	25.7	19.1	15.8	13.8
	80%	誤認率	0.0	0.3	**0.5**	2.0	5.6	8.4	11.7	15.1
		認証失敗率	79.6	62.5	**44.1**	29.6	20.4	18.4	14.5	12.5

各項目の単位はパーセント。認証基準を満たす場合は太字で示す。

ある．

[必要とされる署名の長さ]

どの手法の場合でも，署名の長さが短ければ高い認証精度は望めない．JG 手法や新 JG 手法では，誤認率が上がるという形でこの問題が現れる．アルペジオ手法では，署名長が短すぎて組合せの数が必要なだけ取れないといった事態が起ってくる．短すぎる参照署名は他人に真似される可能性が高くなるため好ましくない．どのような打鍵署名認証システムにおいても認証システムが機能するためには短すぎるような署名列を認めず，適当な長さの登録を要求する必要がある．

試みに，**表 5** に署名列として {ユーザ名，パスワード} のみを用いた場合のアルペジオ手法の結果を示す．この表は署名列が短くなった場合の手法の被る影響を示している．この場合の平均参照署名打鍵数は 14.1 である．基準を満たす点は，全部を用いた場合よりも少なくなった．範囲では $N=15$〜30，$P=0.75$〜1.0，$d=35$〜70 となり，検査した格子点 630 点中で 3.1% がこの基準を満たした．かなり性能は悪化しているが，この程度の性能でも個人認証に用いることは不可能ではない．JG 法や新 JG 法では 14 文字程度の参照署名打鍵数で認証を行おうとしても，参照署名登録時の揺らぎが大きく実用性に欠けるため，少ない文字数での認証についてはアルペジオ法が優位にある．このように短い文字列での認証を実地に応用した場合には，見掛けが今まで用いてきたユーザ名とパスワードだけによる個人認証システムと同様に見えるため，ユーザの心理的負担が軽くなるなどの利点が考えられる．

[認証に用いる時計の精度]

本実験は 5 ms の精度で行ったが現在のワークステーションの持つ時計の精度は，20〜60 ms 程度しかないことが実地に計測してみて判明している．

こうしたワークステーションで個人認証を行う場合，新 JG 手法では，誤差の少ない打鍵間時間の標準偏差が0秒となってしまうために0での割り算を行うことになり，値が計算できないことがわかった．また，JG 手法でも連続打鍵間時間が時計の精度以下であると，一律に0として扱われるため，早いタイピスト同士では個人差が現れにくいという問題がある．しかし，アルペジオ手法ならば，3つのパラメータ中の1つしか時計の精度に依存しないため，時計の刻みが60ms程度の粗さであっても，実用に耐え得るシステムが作成可能であると思われる．

6. おわりに

個人認証を行うための新しい手法を考案し，その手法の有用性を実験によって検証した．今後はこの手法の有用性の実地検証として，認証系をワークステーションに作成してその効果を確かめる予定である．

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) 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).
3) 角田博保，粕川正充：連続打鍵列の打鍵時間に対する分析と考察，情報処理学会研究会報告（ヒューマンインタフェース研究会），91-HI-35, 35-8 (1991).

(平成4年11月25日受付)
(平成5年2月12日採録)

粕川 正充

1960年生．1983年東北大学理学部数学科卒業．東京工業大学理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，同年同大学研究生，1991年電気通信大学研究生．1992年より筑波大学経営システム科学専攻に勤務，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．

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．理学博士．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，同4年助教授，現在に至る．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，電子情報通信学会，日本認知科学会各会員．

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．