

K_036

キー押下時間に着目したキーストロークダイナミクス解析 Keystroke Dynamics Analysis Using Key-pressing Durations

佐村 敏治†
Toshiharu SAMURA

西村 治彦‡
Haruhiko NISHIMURA

1. はじめに

人の打鍵(キーストローク)の経時的なパターンデータには固有のリズムが存在しており、この性質を利用することはこれからの情報社会において大きな可能性を担っていくと考えられる。打鍵データの特徴を利用したバイオメトリックスの立場から、キーストロークダイナミクスにおけるこれまでの研究の多くは利用者のログイン時の照合(verification)認証であった[1, 2, 3, 4]。パスワードの認証を知識(記号列)だけでなく、同時にキーストロークダイナミクスも用いて照合認証する。しかし、利用者の疲労やキーボードの習熟度に左右されやすく、指紋や網膜などの認証に比べるとパスワードのような少ない情報量下では誤認率または認証失敗率が高くなる。

キーストロークダイナミクスをログイン時の照合認証のような状況制限下での生体認証に用いるのに困難が伴うとしても、筆跡や声紋のような人間の行動に関わる特徴分析に用いることは有効であるように思われる。そこで本研究では識別(identification)認証という観点からキーストロークダイナミクスを扱う。パスワード認証のように何度も同じ短い語を入力するのではなく、全く異なった文章を入力しても個人の特徴が捉えられるような分析方法を検討する。このような非定型(多様)な長文を入力したときのキーストロークダイナミクスの研究は我々の知る限りではほとんどなされていない[5]。

ここでは、最初の取り組みとして平易な英文を入力したときのキーストロークダイナミクスを考える。我々はこれまで、打鍵データにおいてばらつきの生じにくい特徴量として、1つのキーを押している時間間隔(押下時間)に着目し、その分析方法を提案した[6]。本論文では更に解析方法を改良し、実験についても詳細な解析結果を示す。

2. 英文入力における打鍵データ計測法

本研究で用いた英文入力の打鍵計測実験について説明する。図1に開発したソフトを示す。

本ソフトのGUI画面は、上部が文書提示部(3行)、中部の広いテキストエリアが入力部、下部のボタンがファイルの読み込みや保存を行う操作部からなる。被験者は、文書提示部(3行)の真中の行を見ながら入力する。入力行を改行すると文書提示部が1行分上にスクロールする。常時文章の前後を見ることができるので、被験者は意味を理解しながら文字入力することができる。

本ソフトの開発には、Java言語のJ2SE Development Kit 5.0を利用し、キーの種類と打鍵時間の記録にはKeyListenerを用いた。またキーを押した時刻(プレス時刻: press time)だけでなく、離れた時刻(リリース時

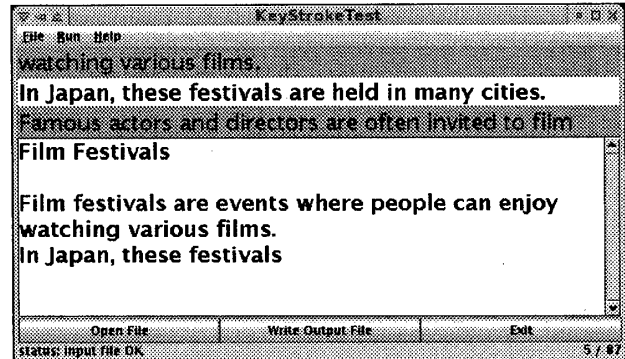


図1: 打鍵計測実験ソフト(画面例)

刻: release time)も記録する。時間分解能はミリ秒[ms]である。

英文については英検準2級程度のテキスト文を用いた。本研究では5名の被験者(A,B,C,D,E)について実験を行い特徴分析を行った。使用したコンピュータは、CPU Pentium4 1.7GHz, 1024MBのRAMであり、OSはVine Linux 3.2である。

3. キー押下時間(p-r時間)による特徴量

3.1 p-r時間の分析

本研究では、大量の打鍵データを扱う中で個人的ばらつきの生じにくい特徴量として、個々のキーを押している時間(p-r時間)に注目する。以下にp-r時間の特徴について説明する。

一口に打鍵と言っても、キーのプレス時刻とリリース時刻を考慮したとき、次のような4つの時間間隔が現れる。

1. プレス時刻とリリース時刻との間隔
2. リリース時刻とプレス時刻との間隔
3. プレス時刻とプレス時刻との間隔
4. リリース時刻とリリース時刻との間隔

1は、一つの指でキーを押している時間(p-r時間と記す)と、一方の手の指であるキーを押してもう一方の手の指で他のキーを離すまでの時間(p-r'時間)の2種類がある。2は、キーを離して次のキーを押すまでの時間(r-p時間)である。3の時間(p-p時間)や4の時間(r-r時間)は、例えば左手であるキーを押した(離れた)あと、すぐに右手で別のキーを押す(離す)ときに記録される時間である。

実際に、被験者AとBが同一の英文(180語)を入力したときの"a"~"z"のアルファベットに関するデータのみを対象に、各1~4の打鍵時間の平均、標準偏差および(標準偏差/平均)を求めた結果を表1に示す。括弧内の数値はイベント数を表す。キーを押している時間(p-r時間)は標準偏差をみると個人的ばらつきが小さいことが

†明石工業高等専門学校, Akashi National College of Technology
‡兵庫県立大学, University of Hyogo

表 1: 各打鍵時間間隔の平均, 標準偏差 (上段) および (標準偏差/平均) の計算値 (下段)(括弧内の数値はイベント数)

	被験者 A	被験者 B
p-r	133.5 ± 27.6 [ms] 0.207 (320)	144.2 ± 31.3 [ms] 0.217 (336)
p-r'	58.0 ± 37.7 0.650 (207)	49.4 ± 32.3 0.654 (232)
r-p	138.9 ± 192.3 1.384 (372)	127.8 ± 135.8 1.063 (410)
p-p	109.7 ± 28.0 0.255 (163)	116.3 ± 32.5 0.279 (190)
r-r	95.4 ± 33.3 0.349 (139)	100.7 ± 44.1 0.438 (138)

わかる。またそれぞれの (標準偏差/平均) でみても p-r 時間が一番ばらつきが小さいことがわかる。

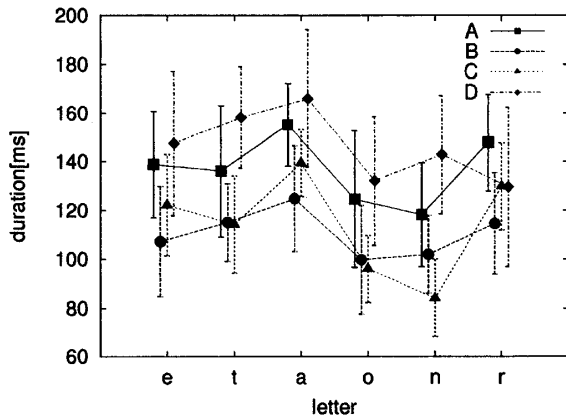


図 2: 各文字 (e,t,a,o,n,r) での p-r 時間の平均と標準偏差

次に p-r 時間にどの程度の個人差があるかを調べた。同一の英文を使用した場合、使用頻度の多い文字を対象に各被験者の平均と標準偏差を図 2 に示す。被験者同士で重なる文字も出てくるが、多数の文字に渡ってみれば、個人による特徴が出ていることがわかる。

図 3 に被験者 D が入力した全文書中の文字 "e" の p-r 時間についてのヒストグラムを示す。事象が増えれば p-r 時間はほぼ正規的に分布しているのがわかる。

3.2 p-r 時間の平均と標準偏差を用いた解析方法

本節では、全アルファベットを対象とした p-r 時間を用いた解析方法について説明する。

まず入力英文のプロファイルを作成する。

1. 対象とする入力データのうち、“a”~“z”の p-r 時間のデータのみを収集する。例えば、被験者を A とし、アルファベット α (a~z のいずれかの 1 文字) の p-r 時間列を

$$K_{\alpha}^A = (k_{\alpha}^A(1), k_{\alpha}^A(2), \dots, k_{\alpha}^A(i_{\alpha}), \dots, k_{\alpha}^A(i_{\alpha}^{max}))$$

(ただし, $i_{\alpha}^{max} \geq 5$) (1)

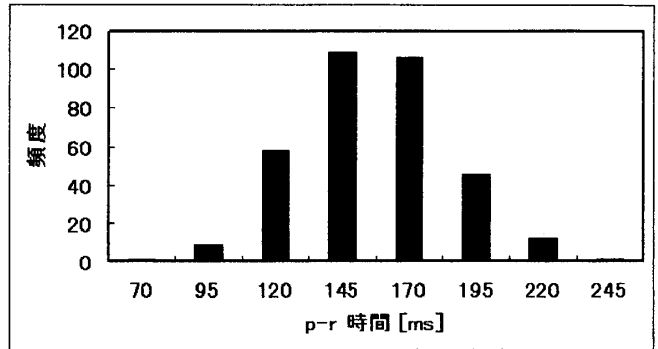


図 3: 被験者 D による文字 (e) の p-r 時間のヒストグラム

とする。ここで、 i_{α} はアルファベット α の p-r 時間列の順番を表し、その最大の数を i_{α}^{max} とする。ただし、出現回数の少ないデータはプロファイルとして不適当と考えて、5 回以上 ($i_{\alpha}^{max} \geq 5$) のデータのみプロファイルとして残す。

2. 式 (1) の平均値 r_{α}^A と標準偏差 s_{α}^A を求める。

$$r_{\alpha}^A = \frac{1}{i_{\alpha}^{max}} \sum_{i_{\alpha}=1}^{i_{\alpha}^{max}} k_{\alpha}^A(i_{\alpha}),$$

$$s_{\alpha}^A = \sqrt{\frac{1}{i_{\alpha}^{max}} \sum_{i_{\alpha}=1}^{i_{\alpha}^{max}} (k_{\alpha}^A(i_{\alpha}) - r_{\alpha}^A)^2} \quad (2)$$

次にテストデータとして、被験者 B のアルファベット α (a~z のいずれかの 1 文字) の p-r 時間列を

$$K_{\alpha}^B = (k_{\alpha}^B(1), k_{\alpha}^B(2), \dots, k_{\alpha}^B(j_{\alpha}), \dots, k_{\alpha}^B(j_{\alpha}^{max})) \quad (3)$$

とする。これを被験者 A のプロファイルによる式 (2) を用いて比較する。

$$N^{BA} = \sum_{\alpha=a}^z \left(\frac{1}{j_{\alpha}^{max}} \sum_{j_{\alpha}=1}^{j_{\alpha}^{max}} \frac{k_{\alpha}^B(j_{\alpha}) - r_{\alpha}^A}{s_{\alpha}^A} \right) \quad (4)$$

ただし、プロファイルとの比較対象のアルファベット α は式 (1) で $i_{\alpha}^{max} \geq 5$ の条件を満足するアルファベットのみである。以下、式 (4) で得られる値を N 値とよぶ。

3.3 解析結果

解析結果について述べる。被験者 (A,B,C,D,E) において、まず 3 つの英文 (ここでは、doc1(180 語), doc2(204 語), doc3(188 語)) を入力した。括弧内の数値はワード数を示す。

被験者 A による英文 (doc1) をプロファイルとしたときの結果を表 2 上に、被験者 D による英文 (doc2) をプロファイルにしたときの結果を表 2 下に示す。

N 値は 0 に近いほどプロファイル (本人) に近い。実際の実験 (表 2) によっても本人は他人と比べて N 値が小さくなるのがわかる。

表 2: 被験者 A による英文 (doc1) および被験者 D による英文 (doc2) をプロフィールとしたときの N 値

被験者	doc1	doc2	doc3
A	0.0	1.4	1.0
B	-31.5	-29.3	-25.0
C	-22.8	-22.4	-24.7
D	11.9	17.1	16.2
E	-13.6	-3.8	-12.1

被験者	doc1	doc2	doc3
A	-12.1	-10.9	-10.8
B	-34.7	-32.1	-28.9
C	-27.9	-27.2	-28.9
D	-3.7	0.0	0.0
E	-20.6	-13.7	-20.0

また式 (4) から, N 値が負の場合は, テストデータの方がプロフィールデータより平均 $p-r$ 時間が短く, N 値が正の場合は, プロフィールデータの方が平均 $p-r$ 時間より短くなることから, 従って表 2 の下表から被験者 D 以外の N 値は全て負になることから, キーを押しているのは被験者 D が一番長いことが結論づけられる。

以上の分析は, 単位時間あたりの語数でも議論することができる。しかし人の行動の中で, 疲れたり考えごとをしたりして手が止まったりしてしまうと, 単位時間あたりの語数は大きく変化してしまう。一方で本研究の特徴量を用いると, 実際にキーを押している時間しか計測しないので, 手が止まっているような動作の影響を受けない。

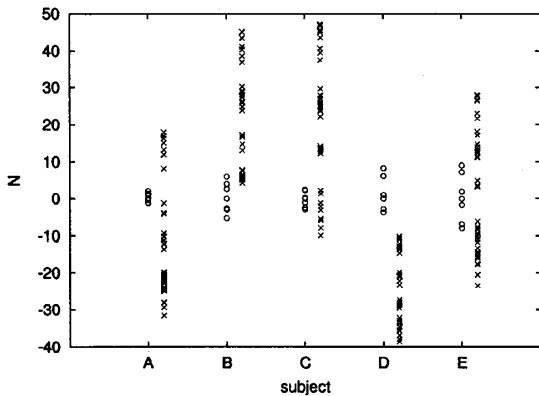


図 4: 本人 (○印) と他人 (×印) による N 値の分布

次に, 本人と他人では N 値がどのような分布になるかを図 4 に示す。横軸が被験者, 縦軸が N 値を表す。左の○印が本人, すぐ右の×印が他人による N 値である。本人による N 値の多くは $|\Delta N| \leq 10$ の範囲内に納まることがわかる。一方で他人の N 値は広範囲にわたっている。また被験者 B の場合は他人の N 値が全て正な

のでキーを押している平均時間が一番短く, 被験者 D の場合は全て負なのでキーを押している平均時間が一番長いことがわかる。この解析は, 数人の被験者から一人を絞りこむときの方法として有効である。

$|\Delta N|$ を認証の閾値としたとき, 認証失敗率 (本人ではあるがプロフィールとの比較で他人とみなされる確率) と誤認率 (他人がプロフィールとの比較で本人とみなされる確率) との関係は図 5 になる。

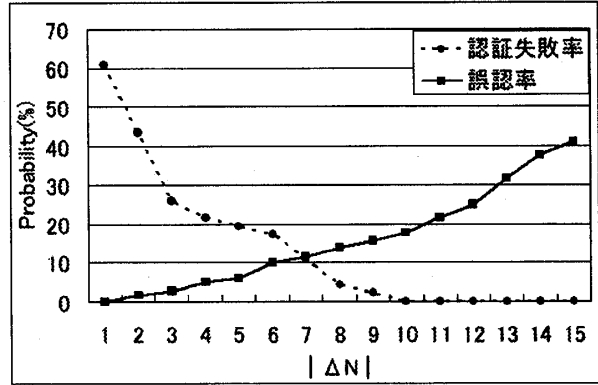


図 5: $|\Delta N|$ を閾値としたときの認証失敗率と誤認率

結果として認証失敗率と誤認率とはトレードオフの関係をもつ。 $|\Delta N| \sim 7$ で認証失敗率と誤認率は逆転する。1 章でも述べたが, 指紋や網膜と比べると精度は悪くなり, 本手法を照合認証に用いることは難しい。しかし様々な要因による解析を組み合わせることで, 精度が上がる余地はある。

また以下に述べるように, 筆跡や声紋のような人間の行動に関わる分析の観点から有効な手段となる可能性があり, 被験者の心身上の変動を探る手段になることが期待できる。

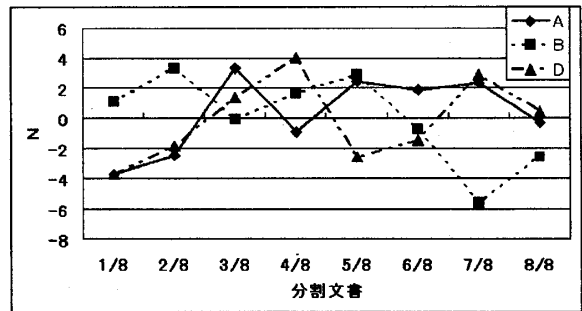


図 6: 英文 (doc5) を 8 分割したときの被験者 A, B, D の N 値の変化 (それぞれ, 分割する前の英文をプロフィールとする)

被験者 A, B, D においては後日に 英文 (doc4(109 語), doc5(303 語)) の入力をも更に得た。ひとつの文書を分割したときの N 値の変化を求めた。図 6 は, 被験者 A, B, D が入力した英文 (doc5) を 8 分割し, 各被験者の分割する前の英文をプロフィールとして N 値の変化を調べた。

例えば図6の被験者B(■)は最初はNが正值であったが、途中で負値に落ちている。長文であるので被験者の疲労または注意力の低下が関係してきていると思われる。

更にN値の時間依存性を調べるために、被験者Dを長期に渡って実験した。上記の実験の後、被験者Dは英文(doc6(53語), doc7(55語), doc8(55語))と(doc9(315語), doc10(316語))をそれぞれ別の日に入力した。図7にdoc5をプロファイルとして、48日間に4回行った実験結果のN値を示す。

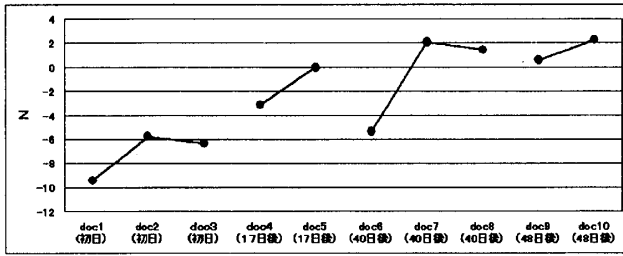


図7: 被験者DによるN値の時間依存性(英文(doc5)をプロファイルとする)

全体的に右上りのグラフになり、N値が徐々に上昇する傾向を示している。これは実験の操作及びキーボードの使用に慣れてきて、キーを押している時間が徐々に短くなっている可能性が示唆される。また、同一日に行った実験は最初の文書より2番目の文書の方がN値が上がり、3つ目の文書はやや下がっている。これは、キーボードの慣れと被験者の疲労または注意力の低下が関係してきていると思われる。この結果を利用すると、長期の観測を行って、ある時に著しいN値の変化が見られるとき(例えば、突然 $N \sim 50$ の時など)は、被験者に心身上の変化(または別人による操作)の影響を読み取ることも期待できる。

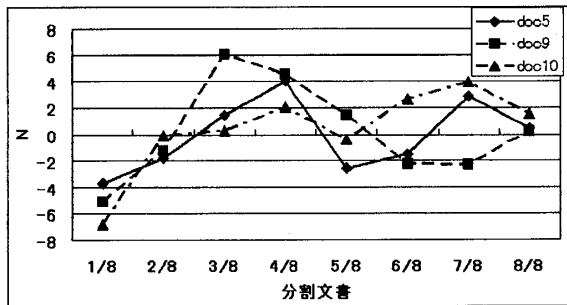


図8: 被験者Dにおいて英文(doc5, doc9, doc10)をそれぞれ8分割にしたときのN値の変化(それぞれ、分割する前の英文をプロファイルとする)

最後に同じ被験者Dに対する比較的長文(300語程度)の英文(doc5, doc9, doc10)を分割して図6と同様にN値の変化を調べた(図8)。結果として $|\Delta N| < 7$ の狭い範囲で、起伏はあるが比較的安定であることがわかる。ま

た、図6の場合と違って同一被験者に対するデータなので経時的パターンがよく似ていることがわかる。

4. 結論と考察

本研究では平易な英文を入力したときに個人らしさを表す特微量として、キー押下時間(p-r時間)に着目した。そして、このp-r時間は個人的ばらつきが生じにくいことを示した。次にこの打鍵データの解析方法を提案し、実験による検証を行った。

解析に用いた式(4)の時間的な変化や文書を分割したときの変化を調べた。このような解析は被験者の心身上の変動を分析する手段として役立つと考えられる。今後、事例数を増やし、本研究で捉えられた特徴についての更なる検証を進める必要がある。また、p-r時間のさまざまな特微量の解析を組み合わせることで、精度のよい認証も可能になることが期待される。

本研究により、クラッキング行為のあった計算機の打鍵データログを解析することでプロファイリングを行ったり、日頃の打鍵データを監視することで個人の健康状態をチェックする医療システムなど多くの応用が期待できる。

参考文献

- [1] D. Betch, C. Slivinsky and B. Hussien, Computer Access Security Systems using Keystroke Dynamics, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 12, No. 12 pp.1217-1222 (1990)
- [2] A. C. Furnell, J. P. Morrissey and C. T. Stocked, Applications of Keystroke Analysis for Improved Login Security and Continues User Authenticaion, Proceeding of Information Systems Security ed. By S. Katsukas, pp.283-294 (1996)
- [3] 佐村敏治, 高岡沙緒里, 柴田千恵, 西野順二, 小高知宏, 小倉久和, 打鍵データの特性を生かした個人認証システム, 福井工業大学研究紀要, Vol. 29, pp. 305-312 (1999)
- [4] M. S. Obaidat and B. Sadoun, Keystroke Dynamics Based Authentication, Biometrics: Personal identification in networked society, A. Jain, R. Bolle, S. Pakati (dir.), Kluwer Academic Publishers, pp. 213-225 (1999)
- [5] D. Umphress and G. Williams, Identity verification through keyboard characteristics, International Journal of Man-Machine Studies, Vol. 23, pp.263-273 (1985)
- [6] 佐村敏治, 西村治彦, テキスト入力によるキーストロークダイナミクス, 第14回研究報告会講演論文集, 情報知識学会, (2006.5)