テクニカルノート

打鍵間時間を基にした認証システムのリズム打鍵による改善

小越康宏[†] 日名田明[†,☆]
広瀬貞樹[†] 木村春彦[††]

コンピュータシステムの個人認証においては，従来よりユーザ名，パスワードの情報を用いて本人かどうかの認証を行っているが，これらの情報が漏れた場合に不正利用される恐れがある．そこで，ユーザ名，パスワードを入力するときの打鍵間時間（あるキーが打たれてから次のキーが打たれるまでに要する時間）の特徴を参考にして個人認証を行うシステムがいくつか提案されている．しかし，打鍵の熟練者においては打鍵間時間に差異が現れにくく，どのシステムにおいても本人かどうかの認証が困難となる問題点があった．本研究では，このような打鍵間時間を基にした認証システムにおいては，認証時に意図的なリズムを持たせて打鍵するリズム打鍵が有効で，認証精度を大幅に改善できることを示す．

Improving User Authentication Based on Keystroke Intervals by Using Intentional Keystroke Rhythm

Yasuhiro Ogoshi,[†] Akira Hinata,[†,☆] Sadaki Hirose[†]
and Haruhiko Kimura[††]

In this paper, we propose an improvement method of the authentication systems based on keystroke intervals using intentional keystroke rhythm. In the previous authentication systems based on keystroke intervals, user was more exactly discriminated by the speed of each keystroke in addition to the user name and the password. However, they still have a problem that an authentication might be difficult when the speed of each keystroke was similar to the other person's. We solve this problem by making a rhythm keystroke to each user at the time of the authentication.

1. はじめに

コンピュータシステムにおいて利用者のパスワードが漏洩すると，本人以外が誰でも容易に不正利用でき深刻な被害が及ぶ場合がある．厳密な認証を実現するために，秘密情報（暗証，デジタル署名）や，バイオメトリクス（指紋，網膜，掌紋，虹彩，顔貌などの終生不変の個人情報）を利用した技術[1)]が実用化されているが，新たに装置を必要とし導入コストがかかる．

一方，認証時のキーボード入力における打鍵間時間の特徴を参考にして認証する JG 法[2)]，認証精度を改善した新 JG 法[3)]や，連続した多打鍵間時間を考慮したアルペジオ法[4)]などが提案されている．

このような打鍵間時間を基にした認証システムでは，キーボード入力の熟練度の差異が大きい場合は個人の識別が容易であるが，熟練者のように差異が小さい場合は識別が難しくなるという問題があった．

本研究では，このような打鍵間時間を基にした認証システムにおいては，認証時に意図的なリズムを持たせて打鍵するリズム打鍵が有効で，認証精度を大幅に改善できることを示す．

2. 認証システムとその課題

2.1 認証システム

認証システムの役割は，ユーザ名とパスワードなどの個人を特定する情報を基に，本人であるかを確認してコンピュータシステムの利用権を与えることである．認証においては，(1) 本人が認証される，(2) 本人が認証されない，(3) 他人を誤認する，(4) 他人を誤認しないの 4 通りのケースが発生し，それぞれの回数を

† 富山大学工学部知能情報工学科
Faculty of Engineering, Toyama University
†† 金沢大学工学部情報システム工学科
Faculty of Engineering, Kanazawa University
☆ 現在，株式会社シーイーシー
Presently with Computer Engineering & Consulting, Ltd

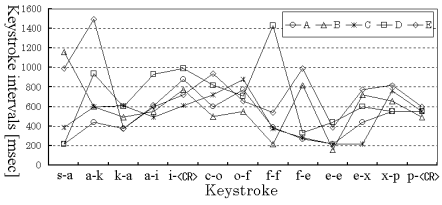

図 1 初心者グループにおける打鍵間時間
Fig. 1 Keystroke intervals of beginner group.

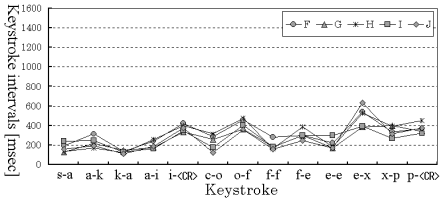

図 2 熟練者グループにおける打鍵間時間
Fig. 2 Keystroke intervals of expert group.

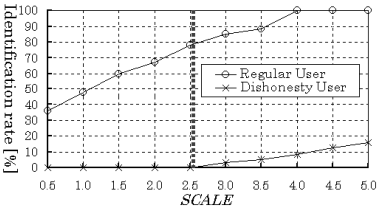

図 3 初心者グループにおける認証結果
Fig. 3 Result of the authentication for beginner group.

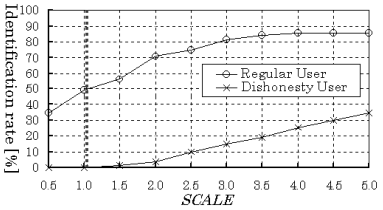

図 4 熟練者グループにおける認証結果
Fig. 4 Result of the authentication for expert group.

Na, Nb, Nc, Nd 回とすると，認証率（本人が認証される確率）は $\frac{Na}{Na+Nb}$，誤認率（他人が誤認される確率）は $\frac{Nc}{Nc+Nd}$ のように表せる．

利用者に快適な環境を提供するという観点から認証率は 100%にすることが望ましい．一方，誤認は本来あってはならないので誤認率は 0%である必要がある．

認証精度（誤認率を 0%に保ったまま最大となる認証率）を大きくすることが，認証システムにおける重要な課題である．

2.2 打鍵間時間を基にした認証システムの問題点

打鍵間時間を基にした認証システムにおいては，個人ごとに打鍵間時間に特徴が現れることを利用して個人の識別を行う．

図 1，**図 2** は，ある文字列（sakai⟨CR⟩coffeexp⟨CR⟩）に対する 10 人の被験者（A〜J）の打鍵の特徴を示したものである．図 1 の被験者 A〜E の 5 人はタッチタイピング（キーボードを見ずに決められた指での打鍵）ができない初心者のグループである．図 2 の被験者 F〜J の 5 人はタッチタイピングができる熟練者のグループである．横軸は入力された文字列の打鍵間，縦軸は被験者ごとの打鍵間時間の平均を示している．

図 1 の A〜E の 5 人は打鍵速度が遅く，個人差が大きいので識別は比較的容易である．一方，図 2 の F〜J の 5 人は打鍵速度に多少の差異はあるものの，打鍵間の緩急のリズムが酷似している．タッチタイピングを基本とした打鍵入力をしている場合，打鍵間時間はキー配列による影響が強くなり，別人でもリズムが酷似するため識別は困難となる．

実際に，打鍵間時間を基にした認証システムの 1 つである新 JG 法☆で，A〜E の初心者グループと F〜J の熟練者グループについて認証実験を行った結果をそれぞれ**図 3**，**図 4** に示す（新 JG 法の概略については付録 A.1 を参照されたい）．

図の横軸は認証の厳しさを決定するパラメータ $SCALE$（この値が大きくなるほど認証が甘くなる）を表す．縦軸は認証率，誤認率を表す．認証率の平均と誤認率の平均を，それぞれグラフ中に○と×で表す．図中に太い点線で示したのは，誤認率を 0%に保ったまま認証率が最大となるところで，このときの認証率が認証精度となる．

図 3 に示すように初心者グループにおいては認証精度は 78%程度であり，一方，図 4 に示すように熟練者グループにおいては認証精度は 50%程度である．このように，打鍵にあまり差異が現れない熟練者グループにおいては識別が難しくなり，認証システムとしての実用性が低くなる．

そこで，ユーザ名，パスワード以外にも，フルネーム（姓，名）などの文字列を付加的に入力させ，認証精度を向上させる方法がとられることが多い．

熟練者グループに対して，ユーザ名，パスワード以外にフルネームを付加した場合の認証結果を**図 5** に示す．図 4 のユーザ名，パスワードのみの場合に比べると入力情報が増えたことにより，認証精度は 8%程度向上しているが，まだ十分とはいえない．

☆ 打鍵間時間を基にした認証システムにはほかにもアルペジオ法[4]があるが，認証精度を調整するパラメータが複数あり，パラメータの組合せにより性能が大きく変わってしまうため単純に性能の比較ができないので，本論文においては省略した．

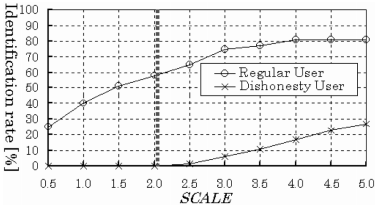

図 5 熟練者グループにおける認証結果（ユーザ名，パスワード以外の情報を付加した場合）
Fig. 5 Result of the authentication for expert group (added the information of full name).

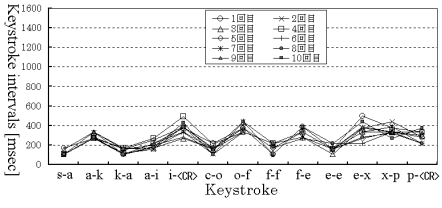

図 6 ある利用者における通常の打鍵間時間
Fig. 6 Keystroke intervals (usual keystroke).

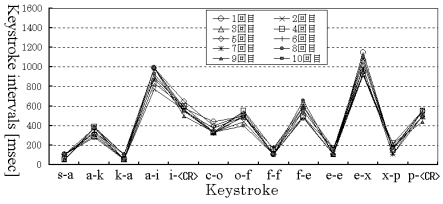

図 7 ある利用者におけるリズム打鍵の打鍵間時間
Fig. 7 Keystroke intervals (using intentional keystroke rhythm).

3. リズム打鍵を用いた改善

打鍵間時間を基にした認証システムにおいては，打鍵のリズムが酷似している熟練者の識別が本質的に困難である．

そこで，利用者ごとに意図的なリズムを持たせて打鍵する（たとえば，利用者が自分の好きな曲のフレーズなどを思い浮かべて，そのフレーズにあわせて打鍵する）リズム打鍵を提案する．持たせたリズム自体が個人を識別する大きな情報となり，認証精度の大幅な改善が期待できる．また，利用者においても付加的な文字列の入力を強要されるより入力の負担が軽減し，利便性も向上する．

ある利用者において，通常の打鍵を 10 回行わせた打鍵間時間の様子を**図 6** に示し，リズム打鍵を 10 回行わせた様子を**図 7** に示す．

図 6 に示すように通常の打鍵においては，同一人物でも毎回ばらつきがあることが分かる．図 7 に示すようにリズム打鍵の場合は，ばらつきが少なくなっている．リズムを持たせることにより，自分の好きなテンポで入力することができ，入力の再現性が高くなったのではないかと思われる．

4. 実験方法

通常の打鍵と，意図的なリズムを持たせたリズム打鍵とで認証実験を行い，両者を比較する．

4.1 被験者

被験者は，打鍵間時間を基にした認証システムにおいて識別が困難であったキーボード操作に熟練したタッチタイピングができる大学 4 年生 20 人を選んだ．

4.2 参照署名の登録

ユーザ名は本人の姓，パスワードは自動生成した 8 文字を使用した．{ ユーザ名，パスワード } を 10 回入力させ参照署名として登録した．

4.3 本人の認証実験

ユーザごとに検査署名として本人の { ユーザ名，パスワード } を入力して認証させ，これを 10 回行った．

4.4 誤認実験

20 人の被験者ごとに，自分以外の 19 人の中から 4 人を無作為に選び，これらの対象人物の { ユーザ名，パスワード } を用いて成りすましの認証を試みた．これを 1 人の対象者につき 10 回行った．

4.5 追加実験

さらに，リズムが漏れた場合を想定して，20 人の被験者ごとに，自分以外の 19 人の中から 4 人を無作為に選び，これらの対象人物の { ユーザ名，パスワード } をあらかじめ暗記したうえで，打鍵の様子を見てリズムを覚え，成りすましの認証を試みた．これを 1 人の対象者につき 10 回行った．

5. 実験結果

5.1 認証実験の結果

通常の打鍵とリズム打鍵の認証結果をそれぞれ**図 8**，**図 9** に示す．図 8 に示すように通常の打鍵での認証精度は 47%程度であるが，図 9 のリズム打鍵での認証精度は 80%を超え，認証精度が大幅に改善された．

5.2 追加実験の結果

図 10 にリズムが漏れた場合を想定した追加実験の結果を示す．リズムが漏れてしまうと図 9 に比べて多少誤認率が増えるが，それでも，図 8 の通常の打鍵による場合に比べ誤認率は 4 分の 1 以下で，認証精度も 60%を超えた．この点からもリズム打鍵の効果が確認できた．

6. まとめ

打鍵間時間を基にした認証システムにおいて，利用

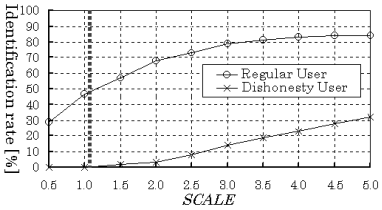

図 8 通常の打鍵による認証結果
Fig. 8 Result of the authentication in usual keystroke.

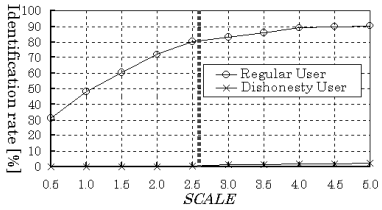

図 9 リズム打鍵による認証結果
Fig. 9 Result of the authentication using intentional keystroke rhythm.

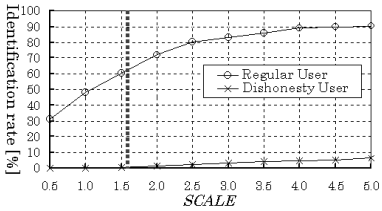

図 10 リズム打鍵による認証結果（リズムが漏れた場合）
Fig. 10 Result of the authentication using intentional keystroke rhythm (the rhythm leaked out).

者に意図的なリズムを持たせてリズム打鍵させることによって，認証精度を大幅に改善することができた．

また，この手法はキー入力を主体とした認証システム（たとえば，銀行の ATM など）に幅広く適用可能であり，新たに装置を付加したり入力項目を増やしたりすることなく，セキュリティを向上させることができる．

謝辞 編集委員，査読委員の先生方から貴重なご教示をいただいた．ここに記して謝意を表する．

参 考 文 献

1) 菅 知之：本人認証の全体像とバイオメトリクスの位置付け，情報処理，Vol.40, No.11, pp.1073–1077 (1999).
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) 粕川正充，角田博保，森 裕子：アルペジオ打鍵列を利用した個人認証手法の提案，情報処理学会論文誌，Vol.34, No.5, pp.1198–1205 (1993).

付 録

A.1 打鍵間時間を基にした認証システムの概略

打鍵間時間を基にした認証システムとして代表的な手法である新 JG 法の概略を示す．

(1) 参照署名の登録

{ ユーザ名，パスワード } が $n+1$ 文字からなるものとして，{ ユーザ名，パスワード } を入力したときの n 個の打鍵間時間列

$$K = (k_1, k_2, \ldots, k_j, \ldots, k_n)\ (1 \le j \le n) \quad (1)$$

を打鍵署名と呼ぶ．ここで，$k_j (1 \le j \le n)$ は j 文字目と $j+1$ 文字目を打鍵する時間差を表す．

{ ユーザ名，パスワード } を m 回入力して得られる打鍵署名 $K_1, K_2, \ldots, K_m$ を参照署名と呼び，個人データとして登録する．ただし，中央値の 2 倍以上の打鍵間時間を含んでいるような打鍵署名は不正データとして除去する．

(2) 基準署名の作成

参照署名の平均打鍵間時間列を基準署名と呼び，

$$R = (r_1, r_2, \ldots, r_j, \ldots, r_n) \quad (2)$$

で表す．

(3) ノルムの算出

参照署名から打鍵間時間の標準偏差

$$S = (s_1, s_2, \ldots, s_j, \ldots, s_n) \quad (3)$$

を求め，参照署名である各打鍵署名 K_i について，基準署名を基に，ノルム $NORM$ を以下の式で算出する．

$$NORM(K_i, R) = \Sigma_{j=1}^{n} \frac{|k_{ij} - r_j|}{s_j} \quad (4)$$

(4) 認証閾値の算出

認証閾値を I とおき，ノルム $NORM$ の平均値 Ng と標準偏差 Ns を求め以下の式に代入する．

$$I = Ng + SCALE \times Ns \quad (5)$$

$SCALE$ は，認証の厳しさを決定するパラメータであり，大きくとるほど認証が甘くなる．

(5) 認証判定

認証時に入力される打鍵署名を検査署名と呼び，

$$T = (t_1, t_2, \ldots, t_j, \ldots, t_n) \quad (6)$$

で表す．検査署名 T についてノルム $NORM$ を求め，以下の式のように認証閾値 I 未満なら本人と見なす．

$$NORM(T, R) < I \quad (7)$$

(平成 14 年 10 月 15 日受付)
(平成 14 年 12 月 3 日採録)