M_050

携帯端末におけるモバイル本人認証
Study of the personal identification using keystroke dynamics on mobile terminals

森廣 雅道*　　鶴 浩二**
Masamichi MORIHIRO　Koji TSURU

１．まえがき

近年のIT化の進展，特にインターネットの普及により多くの情報を簡単に入手することが可能となった．しかしその反面，個人情報の漏洩の危険性が高くなってきた．そして基本台帳ネットワークの設立によって個人情報がデジタル化され，さらに個人情報の保護が重要になってきている[1]．それは，さまざまな機能を持つ携帯電話も例外ではない．現在の携帯電話機は高機能・高性能化し，多くの個人情報が保存されている．また，プリペイド機能を持つ携帯電話も商品化され，本人確認などセキュリティが問題になっている[2]．現在携帯電話で主に使用されている個人認証方法は暗証番号である．しかし，他人に暗証番号が知られてしまうと容易に携帯電話所持者に成りすますことができ，危険である．実際に喫茶店などで携帯電話からメモリ内情報を盗まれるというような犯罪も起きている．さらに，暗証番号は忘れてしまう人も多く，使っている番号も生年月日などの身近な数字を使っている人が多い[3]．また，最近では生態認証技術（指紋認証，顔認証など）が携帯電話には搭載されている．しかし，生態認証は嫌悪感がある人も少なくなく，コストもかかる [3]．そこで携帯電話などの携帯端末において，使いやすくさらに安全性の高い本人確認手段が求められている．本論文では，携帯電話のキーを打つ際にリズムによって本人を確認する方法について研究を行った．

２．概要

２．１　キーストローク認証

キーストローク認証とは生態認証の一種で，あるキーを押している間の時間やキーを押すリズムなどによって認証を行うものである．この認証方法の利点は，キー入力という携帯電話利用者にとってはなじみの深いもので認証できるという点である．これならば虹彩認証のようにカメラを覗き込んだり，指紋のように指でなぞったりする必要もない[4]．しかもほとんどの生態認証は，認証するためのハードウェアを必要とするが，この認証方法はすべてソフトウェアで行っているため新たなハードウェアを設置する必要がない．パソコンではNet Nanny Software International Inc[5]やbioChec[6]などが商品化している．しかし，携帯電話の分野では実用化されていない．そこで，携帯電話でのキーストローク認証について研究を行ったが，入力時間にばらつきが大きく，本人を確認できるほどの精度は得られなかった．

２．２　リズムパスワード

キーストローク認証のように，携帯電話で暗証番号を打つ際の自然なリズムでは認証は難しかった．そこで，利用者が暗証番号を入力する際に任意のリズムを決めて打ってもらい，それによって認証する方法について研究を行った．これを本論文では「リズムパスワード」と呼び，これについて研究結果を以下に示す．

*　大分工業高等専門学校　電気電子情報工学専攻 １年
**　大分工業高等専門学校　制御情報工学科

本実験に用いるキーストローク入力時間のパラメータを図１のように定義する．t_1, t_2…t_nはキーを押している時間，t_{1_2}, t_{2_3}…t_{n-1_n}はキーを離している時間，Tは入力を終えるまでの総合時間である．

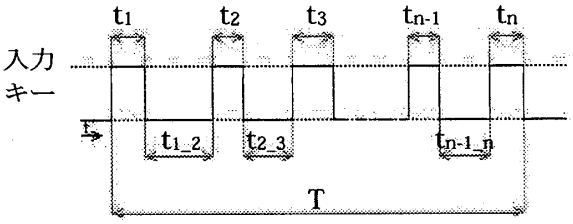

図１　入力時間のパラメータ

３．実験方法

今回の実験ではWindowsXP搭載のPC，DoCoMoの携帯電話F506i，auの携帯電話A5302CA，DoCoMoのアプリケーション（iアプリ）開発環境であるDoJa3.0，auのアプリケーション(ezplus)開発環境であるezplus Emulatorを使用した．DoJaとezplus Emulatorは，パソコン上でアプリケーションの処理をシミュレーションできるエミュレータの機能があり，この機能を利用してプログラムを作成した．

図２　実行画面

図２は，iアプリの実行画面である．プログラムではiアプリ，ezplus共にJAVAを使用し，携帯電話のキーを押したときと離したときの時間を測定し，そこからキーを押している時間，次のキーに移るまでの時間を求めた．取得する時間の最小単位は10msである．

実験では次の二つのことについて測定を行った．

(1) 特徴パラメータの決定

(2) 同一人物の時間経過による変化

(1)は本人を確認するためのパラメータである．(2)はそのパラメータが，時間が経過することによって変化するかを測定した．

4．実験結果

まず，ある数字列をリズムをつけて 10 回入力した際の，キーを押している時間，キーを離している時間を測定した．図 3 は，その 10 回の平均値を 4 日分集めたものである．横軸は押したキー，縦軸は入力時間，それぞれの線が日を表している．

図を見て解るように，日がたってもリズムの変化はほとんどないことがわかる．しかし，リズムは同じであっても，打つ速さに違いがあるために多少の誤差がある．

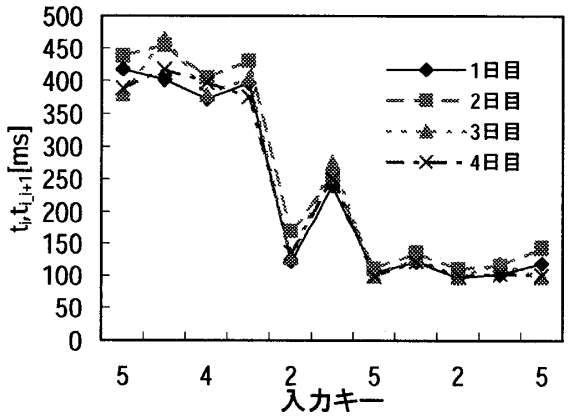

図 3　入力時間

そこで今度は，キーを押している時間，次のキーに移るまでの時間を入力を終えるまでの総合時間（図 1 の T）で割った，入力時間の比を測定した．図 4 がその結果である．図 3 と比べると，多少であるが誤差が少なくなっている．

その他にも入力を終えるまでの総合時間なども測定したが，日によってのばらつきが大きかった．よって，特徴パラメータには入力時間の比を使うこととした．

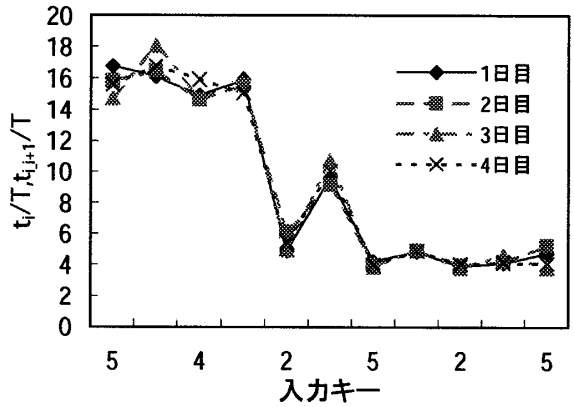

図 4　入力時間の比

5．考察

実験の結果から，リズムで認証することは可能である．リズムパスワードは暗証番号のように覗き見られても簡単にはリズムを知る事は出来ない．また，たとえリズムを知られてしまったとしても本人と同じように打つ事は難しく，暗証番号と併用すれば安全性を高くすることができると考えられる．

しかし，改善しなければならない点もある．まず問題なのがデータの保存法である．テンプレートを携帯電話の中に何もせずに残しておくと，その情報を盗み見られてしまう可能性もある．そこで，実際に導入するときは，テンプレートを暗号化してわからないようにすることや，テンプレート情報はサーバ上において，もしも盗み見ようとするようなことがあればサーバから認証できないようなシステムを作ることなどが必要である．

さらに，認証を行うためのテンプレートも更新をしなければならない．今回の実験では期間が空いても 1 日ほどであったため影響は少なかったが，実際に携帯電話で使用する際には，少しずつテンプレートを更新していくことが必要だと考えられる．

さらに，プログラム自体の解読をされる危険性があり，認証をアプリで行うのではなく OS もしくはハードウェアとして携帯電話に組み込む方法もある．ソフトウェアだけで認証を行う場合は新たにハードウェアを必要としないで便利だが，安全性を充分考慮する必要がある．

また，リズムを忘れてしまう可能性もある．そのために，ヒントを出してリズムを忘れてもリズムを思い出せる仕組み，もしくは忘れにくくする仕組みを考えなければならない．

6．結論

リズムパスワードでは，パスワードを使用するより安全性を高めることができた．また，キー入力時間比を用いることにより個人認証も可能であることを明らかにした．

しかしデータの保存法などの問題点もあり，実際に携帯電話のシステムとして運用するためには，テンプレートを暗号化するなど，問題点を解決しなければならない．

参考文献

[1]経済産業省，個人情報保護，
http://www.meti.go.jp/policy/it_policy/privacy/privacy.html
[2]Take It Easy，おサイフケータイに残された課題，
http://easy.mri.co.jp/
[3]Nissay，暗証番号について，
http://www.nissay.co.jp/keiyaku/oshirase/ansyou.html
[4]BIOMETRICS，バイオメトリクスとは，
http://www.jaisa.or.jp/action/group/bio/About%20BIO/gaiyou.html
[5] Net Nanny Software International Inc，BIOPASSWORD，
http://www.biopassword.co
[6]bioChec，keystroke biometrics，
http://www.biochec.com