ウェアラブル　認証　インタフェース

Technology Reports

新たな入力方式の提案

ケータイは我々の生活に深く浸透している．しかし，キーパッドと小型画面によるインタフェース機構では操作が困難な場面も少なくない（例：歩行中や運転中など）．仮に日常生活のすべての場面で快適に使えるようになれば，我々はインターネットと常につながり，無限の情報をあたかも自分の知識のように使いながら生活するようになるだろう．

本報告では，あらゆる状況での操作を可能とし，ケータイの使用シーンを拡大するべく行われているヒューマンインタフェース研究から最新のトピックをピックアップして紹介する．

（1）周囲から知覚されない微小動作による認証：AwareLESS 認証

真鍋 宏幸（まなべ ひろゆき）　福本 雅朗（ふくもと まさあき）

モバイル環境など，街頭において暗証番号を入力する際には，周囲からの盗み見が問題になる．また，指紋や指静脈などの生体情報を用いた認証も，「鍵として使っている」ことが判明してしまえば模造リスクにつながる．これに対して提案する AwareLESS 認証は，認証動作が周囲から知覚されないため，盗み見や鍵暴露に対しての安全性が高い．

1. まえがき

移動端末には，多くのプライバシー情報が蓄積されており，さらにクレジット機能が付加されたことにより，悪用の危険性が高まってきている．移動端末は公衆環境で利用されるため，安全性が強く求められており，さまざまな認証手法が実装されてきた．

認証手法は，大きく分けて3種類ある．ID タグや IC カードなどの所有物に基づく認証，指紋，静脈パターンや筆跡などの身体的・行動的特徴に基づく生体認証，そしてパスワードや PIN（Personal Identification Number）などの知識に基づく認証である．現在の移動端末では，パスワードによる認証のほか，多くの機種で指紋・声紋・顔認証などの生体認証機能が搭載されており，一部機種では，「あんしんキー」と呼ばれる所有物による認証も搭載されている．しかし，移動端末などのモバイル機器における認証では，盗難・紛失のリスクだけでなく，盗み見のリスクが伴っていることはあまり考慮されてこなかった．

所有物に基づく認証には盗難・紛失の危険性がある．生体認証では盗難の危険は少ないものの，残留指紋や写真などから模造できることがすでに報告[1]されている（つまり指紋センサに指を当てる操作が盗み見られてしまえば，残留指紋から指紋を模造し，認証を突破できてしまう）．一方，知識に基づく認証では盗み見られてしまえば，認証キーが漏洩する危険がある．

銀行 ATM などで認証を不正に突破するためには，カメラなどで監視された特定の場所で操作を行わなければならないために，抑止力が働く．一方，移動端末の場合には移動端末自体が盗まれてしまえば，どのような場所でも操作可能であり，そのような抑止力はない．

移動端末を日常生活のすべての場

面で使えるようにするためには，いつでもどこでも安全に認証を行えることが必要である．提案するAwareLESS認証[*1]では，周囲の人が入力操作に気がつかない，またはどのような操作を行っているのか知覚されない入力操作によって認証を行う．

2. AwareLESS認証

現在，一般的に利用可能なセンサは十分に高感度であり，周囲の人に知覚されない程度の微小動作を検出することができると考えられる．AwareLESS認証とは，周囲の人が知覚できない程度の微小な動作（以下，「無感知」な入力動作と呼び，反対に周囲の人が知覚できる動作を「可感知」な入力動作と呼ぶ）によって認証を行う手法である．周囲の人が操作者を観察していても，操作者が何をキー（知識，所有物，生体情報）にして認証を行っているのか，いつ認証を行っているのか，どのような動作をしているのか，さらにはそもそも認証を行っているのかなどが，知覚されにくくなるため，盗み見のリスクを低減することができる．また，AwareLESS認証はパスワードなどの知識による認証だけではなく，行動的特徴に基づくキーストローク認証[2]やジェスチャー認証[3]など，さまざまな認証方式と組み合わせて使用することもできる．

3. 実験

AwareLESS認証の可能性，無感知と可感知の違い，さらに無感知領域の拡張方法などを明らかにすることを目的として，指とセンサに振動を印加しないノーマルモード，指とセンサにランダムな振動を印加するランダムモード，可感知な入力動作を検出した場合に指とセンサに振動を印加するレスポンスモードの3つについて実験を行った．

3.1 実装

移動端末を模した小箱の，人差し指が接触する部位に，動作検出用の圧力センサを設置した．圧力センサの出力はPCに送られ，測定値に指の動きに対応するピークがあるかどうかを検出する．ピークは条件（絶対値および変化量）を満たした場合にのみ検出され，ピークのパターン（ピーク間の時間差のパターンのことであり，リズムと考えてよい）があらかじめ登録したパターンと一致した場合を認証成功とした．

3.2 AwareLESS認証の可能性

練習を行った操作者6名が，4つのピーク（4つの指先の動き）で構成されるリズムを繰り返し入力した．このリズムと圧力センサの出力例を**図1**に示す．このグラフから，人間が1g重程度の小さな力をコントロールできていることが分かる．また，操作者1名の操作を残りの5名（観察者）で観察した際に，「指先の動きが知覚できない」，「指先が動いた（しかし入力リズムは分からなかった）」，「入力リズムが分かった」のいずれであったかを答えてもらった．5名の観察者全員が「4つの指先の動きがすべて知覚できない」場合を「AwareLESS input」，4つのうち，1～3の動きが無感知であるため観察者全員が入力リズムが分からなかった場合を「key protected input」と分類した．また操作者が試みた入力のうち，認証に成功した入力を「accepted input」とした．

ノーマルモードの結果を**図2**に示す．「accepted input」の割合，認証が成功した入力における「AwareLESS input」の割合と「key protected input」の割合を示してある．この図から，操作者によって異なるものの，おおむね50％程度は入力に成功すること，平均で37％が「AwareLESS input」となること，

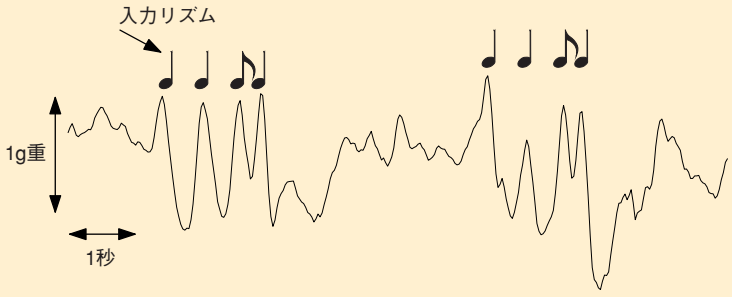

図1　入力リズムと圧力センサ出力

＊1 **AwareLESS認証**：Awareness（気づき）に引っかけた造語．

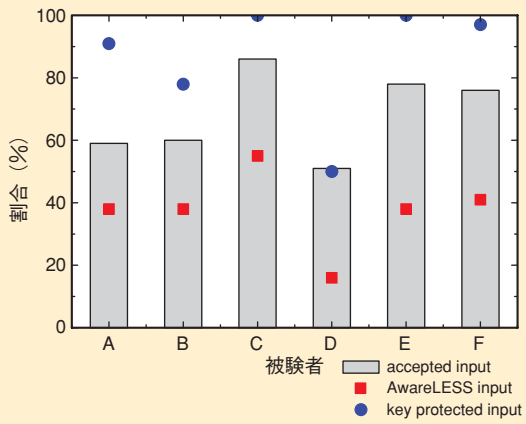

図2　ノーマルモードの結果

また平均で86％が「key protected input」となることが分かる．なおこの実験では，すべての被験者が同じリズムを入力しており観察者も答えとなるリズムをあらかじめ知っていること，操作者の入力はビープ音による合図に合わせているため観察者は入力のタイミングが分かること，さらに操作者のどの指が動くのかは観察者には自明（センサの位置を見れば分かる）であること，認証キーも単純であることなど，操作者にとって厳しい条件となっている．この厳しい条件の中でも80％以上の確率で認証キーが漏洩していないことから，AwareLESS認証は認証キーが漏洩しにくい認証手法であるといえる．

3.3 可感知入力の無感知化

AwareLESS認証はキーが漏洩しにくい手法であるが，全く漏洩しないわけではない．そこで，キー漏洩のリスクをさらに低減するために，可感知入力を無感知化することを検討した．

まず，どのような場合に可感知となるのかを**図3**を用いて説明する．図の横軸は，リズム入力中におけるピークの最大圧力（ベースラインからの圧力変化の最大値），縦軸は圧力の最大変化量（単位時間当りの変化量の最大値）の分布を示している．図3で示すとおり，可感知な入力では最大変化量が大きい傾向が見られ，最大圧力にはあまり違いが見られない．これは，動作が知覚されるのは，指の動きの（単位時間当りの）変化量が大きい場合であるためである．

可感知入力を無感知化しようとした場合，可感知となるしきい値を引き上げることが考えられる．その1つのアイデアが，振動印加である．指とセンサを同時に振動させてしまえば，微小な指動作を隠ぺいすることができるはずである．

一定の振動を付与した際のセンサ出力例を**図4**に示す．この図から，振動印加時においても，振動の影響をほとんど受けることなく，指の動きに伴う圧力変化を検出できているのが分かる．これは，指とセンサが接触しながら一体となって振動するためである．また振動が与えられた場合でも，操作者は図1で示した振動なしの場合と同程度に小さな力をコントロール可能であり，システムもそれを検出可能であることが分かる．

次に，一定の振動よりもランダムな振動を印加したほうが動作隠ぺい効果が大きいと考え，ランダムな振

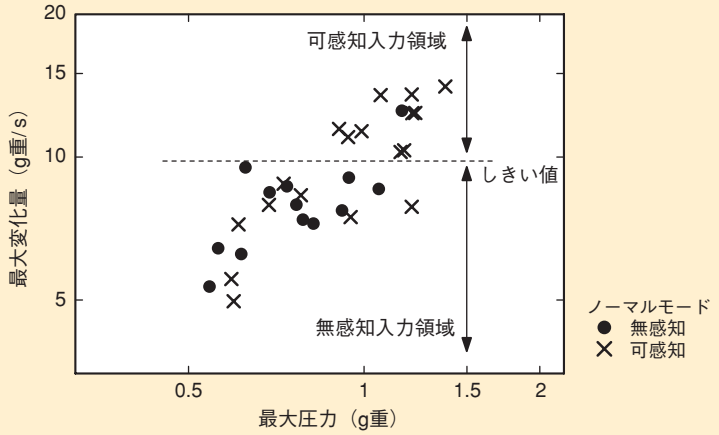

図3　ノーマルモードでの無感知入力と可感知入力領域

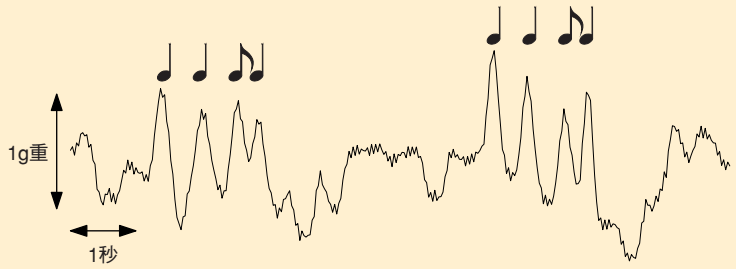

図4　振動印加時のセンサ出力

動を与えて先ほどと同様に5名の観察者の前で操作する実験（ランダムモード）を行った．**図5**から，このモードでは可感知のしきい値が上昇し無感知領域が拡大していることが分かる．ただし，無感知な入力の分布も上昇してしまっている．また，**図6**から図2で示したノーマルモードの結果と比較して「AwareLESS input」の割合，「key protected input」の割合は必ずしも向上しているわけではないことが分かる．

このランダムモードは，振動を印加している時点で，操作者が何らかの操作を行うという合図となってしまうため，AwareLESSという目的に反している．そこで，さらに可感知となり得る入力がなされた場合に，振動を付与し操作を隠ぺいするレスポンスモードについて検討した．ノーマルモードの結果から，圧力変化量が大きい入力は可感知となりやすいといえるので，圧力変化量がしきい値を越えた場合のみ振動を与え動作を隠ぺいする．しきい値は操作者ごとに手動にて設定した．その結果を図5と**図7**に示す．図5からは無感知入力の分布はノーマルモードの場合と同程度に分布していることが分かるが，図7からは図2で示したノーマルモードの結果と比較して「AwareLESS input」の割合が高いものではなく，レスポンスモードによる操作の隠ぺい効果があるとはいい切れない結果となった．

3.4 考察

振動を加えることにより，微小な指の動作は隠ぺいされ，操作が知覚されにくくなることを期待していたが，実験結果からそれを裏付けることはできなかった．その理由として，ランダムモードとレスポンスモードそれぞれにおいて以下のような操作者の心理的作用があるのではないかと考えている．

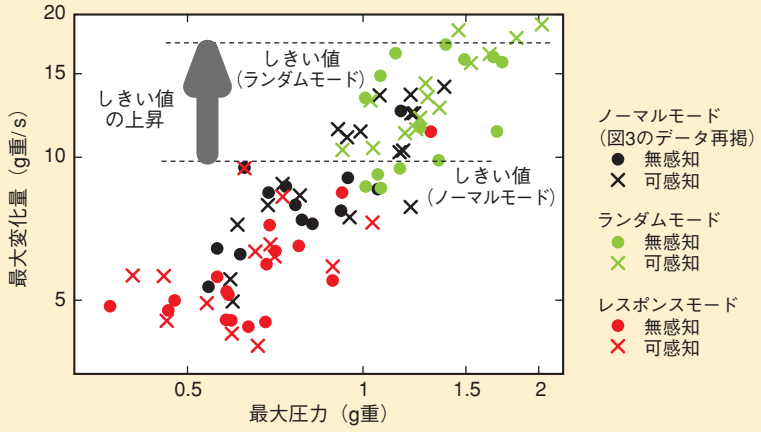

図5　入力の分布と無感知領域の拡大

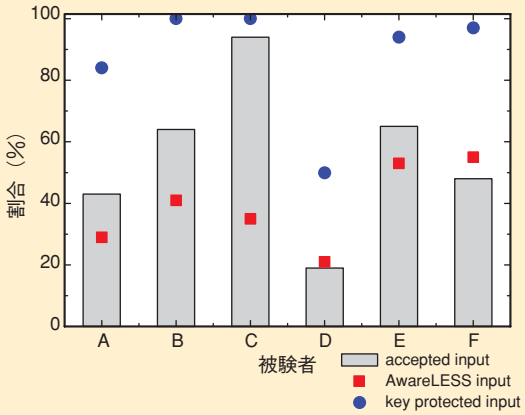

図6　ランダムモードの結果

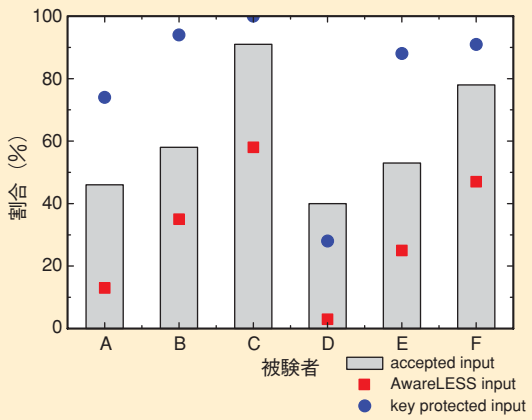

図7　レスポンスモードの結果

・ランダムモード

システムは微小な指の動きでも十分認識しているが，振動を与えることによって，操作者はより大きな指の動きをしなければシステムが認識しなくなる，との心理的な作用が働き，動き自体を大きくしてしまっている．この心理的な効果に伴う動き量の増大と，可感知のしきい値上昇とのバランスが操作者によって異なる．動き量の増大のほうがより大きければ，操作が知覚されやすくなり，逆の場合には知覚されにくくなると考えられる．

・レスポンスモード

入力がしきい値を越えると振動するため，操作者にとってはそれがペナルティと解釈され，心理的な抵抗を感じる．この心理的抵抗が大きい場合には，指先の動作が不自然なものとなってしまうため知覚されやすくなってしまい，小さい場合には知覚されそうになっても振動によって隠ぺいされる．

これらはあくまで仮説であり，今後より詳細に調べていく必要がある．また，より正確に可感知な動きを検出できる方法についても検討していきたい．

4. あとがき

操作していることすら知覚されないAwareLESS認証を提案した．圧力センサを用いた実験により，AwareLESS認証ではキーが漏洩しにくいことを示した．また可感知な入力を無感知化することを目的として，振動印加を試みた．振動印加によって入力操作は必ずしも知覚されにくくなるわけではなかったが，無感知な領域は拡大した．今後，より知覚されにくい方式を検討していきたい．

文　献

[1] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino : “Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems,” Proc. SPIE, Vol.4677, pp.275-289, 2002.

[2] 渡邊 栄治：“階層型ニューラルネットワークを用いたキーストロークによる個人認証，”信学技報，NC2005-103, pp.31-35, 2006.

[3] 石原 進，太田 雅敏，行方 エリキ，水野 忠則：“端末自体の動きを用いた携帯電話向け個人認証，”情報処理学会論文誌，Vol.46, No.12, pp.2997-3007, 2005.