「マルチメディア，分散，協調とモバイル
(DICOMO2016)シンポジウム」 平成28年7月

手首装着型センサを用いた打鍵動作特徴による個人認証手法

伊藤駿吾[†1]　白石陽[†2]　今野慎介[†3]

概要：近年，Wi-Fi の普及により大学や図書館などのパブリックスペースで PC を使用できるようになった．このような場所で PC を利用する際，ユーザが席を離れた場合に他人に PC を不正に使用される恐れがある．そのために多くの PC にはログイン認証機能が搭載されている．一般的な PC のログイン認証にはパスワードを用いた認証方式が利用されている．しかし，この認証方式はパスワードの漏洩により不正にログインされる恐れがあり，ログイン認証時の安全性を向上させることが重要となる．そこで，本研究ではログイン認証時の安全性を向上させるためにキーボードの打鍵動作特徴による個人認証手法を提案することを目的とする．提案手法では，まず，打鍵動作を取得するために両手首に 3 軸加速度センサ，3 軸角速度センサを装着し，各軸のセンサデータを取得する．次に個人認証に利用する特徴量の抽出方法として同一ユーザによる複数回の打鍵動作から各軸のセンサデータを取得し，波形マッチングを行うことで複数の DTW 距離を求める．求めた複数の DTW 距離から SVM（Support Vector Machine）により識別関数を求めることで認証判定を行う．認証精度の評価実験として，5 名の被験者を対象に 4 種類の単語を入力した時の打鍵動作を取得し，各被験者を本人とした時の本人拒否率（FRR），他人受入率（FAR）を求めた．また，認証精度の評価指標として，しきい値を変動させ，本人拒否率と他人受入率が等しくなる時の誤り率である等誤り率（EER）を求めた．実験の結果，被験者によって大きく EER が異なる結果が得られた．最後に，実験結果と今後の課題について考察した．

A Method for Personal Authentication by Using Wrist-mounted Sensors Based on Characteristics of Keystroke Action

SHUNGO ITO[†1]　YOH SHIRAISHI[†2]　SHINSUKE KONNO[†3]

1. はじめに

近年，Wi-Fi の普及により大学や図書館などのパブリックスペースで多くのユーザが PC を使用できるようになった．このような場所で PC を利用する際，ユーザが席を離れた場合に他人に PC を不正に利用される恐れがある．そのため多くの PC にはログイン認証機能が搭載されている．一般的な PC のログイン認証にはパスワードを用いた知識による認証方式が利用される．しかし，この方式ではパスワードの漏洩により不正にログインされる恐れがあり，ログイン認証時の安全性を向上させることが重要となる．

個人認証方式には「記憶」,「所持」,「バイオメトリクス情報」の 3 つの要素がある．認証はこれらの 3 つの要素のどれか，または複数の要素を組み合わせることで実現する[1]．記憶認証方式は，パスワードや暗証番号といった本人のみが記憶している情報を利用する方式であり，PC やスマートフォンなどのログイン認証に利用されている．所持認証方式は，IC カードや身分証明書といった本人が所持しているものによって認証を行う方式である．この方式はオフィスなどの入室時に利用されるが，所持物の紛失や盗難の恐れがあるため，安全性を向上させるために記憶認証方式と組み合わせて利用されることがある．バイオメトリクス認証方式は，生体情報を利用した認証方式であり，指紋や静脈などによる身体的特徴と筆跡や音声などによる行動的特徴を用いた方式に分けられる．また，矢野経済研究所による市場調査[2]によると，バイオメトリクス認証の市場規模は年々増加傾向にあることから近年注目されている認証方式であると考えられる．身体的特徴を用いた認証方式は比較的認証誤差が小さく，経時変化が生じにくいことから様々なアルゴリズムが提案され，近年スマートフォンやノート PC, ATM など多くの場面で活用されている．しかし，人工指による指紋照合に関する研究[3]では，グミで作製された人工指による指紋認証が可能であることが確認されていることから，指紋認証の安全性に問題があると指摘されている．行動的特徴を用いた認証方式は署名の動作や声帯から生じる振動のように何らかの行動から得られる．そのため身体的特徴と比較して特徴量が本人のものであっても安定しないことから実環境で利用される場面は少ない．しかし，これまで犯罪捜査などにも利用されてきた指紋のような身体的特徴と比べて，音声のような行動的特徴は非接触で採取できることから心理的負担が少ない利点がある．

一方，加速度センサや角速度センサなど様々なセンサが

†1 公立はこだて未来大学大学院システム情報科学研究科
Graduate School of Systems Information Science, Future University Hakodate
†2 公立はこだて未来大学システム情報科学部
School of Systems Information Science, Future University Hakodate
†3 函館工業高等専門学校
National Institute of Technology, Hakodate College

小型化したことにより，スマートウォッチやリストバンド型の活動量計など手首に装着可能なウェアラブルデバイスが普及している．本研究ではこれらのデバイスに搭載されるような小型のセンサをウェアラブルセンサと呼ぶ．ウェアラブルセンサには加速度センサ，角速度センサ，磁気センサ，GPS(Global Positioning System)など様々な種類のセンサがあり，これらのセンサを利用することで歩数や歩行距離，脈拍などの情報を推定することができる．また，こうしたウェアラブルセンサを利用してユーザの行動や動作の分析を行う研究が盛んに行われている[4-6]．さらに，ウェアラブルセンサを利用した個人認証に関する研究も行われている[7]．これらの研究から，ウェアラブルセンサは行動的特徴を分析するために活用でき，個人認証手法への応用も期待できると考える．

そこで，本研究では PC を用いたログイン認証の安全性を向上させるためにキーボードの打鍵動作特徴による個人認証手法を提案する．

2. 関連研究

本研究ではキーボードの打鍵動作を対象とした行動的特徴による個人認証手法を提案する．そこで，関連研究として行動的特徴を利用した個人認証手法に関する研究と，キーボード打鍵動作の取得方法に関する研究について述べる．

2.1 行動的特徴を利用した個人認証に関する研究

行方らは腕時計型端末に搭載された加速度センサを用いて腕のジェスチャから個人認証を行っている[8]．この研究ではジェスチャを行った時の加速度データからピークを検出し，個人認証のための特徴量としてピークの出現間隔を利用している．しかし，短い間隔でピークが出現する場合は正しいピーク出現間隔を測定できず，ピークの出現間隔をできるだけ等しくなるように間隔が短いピークを無視している．そのため，キーボードの打鍵動作のような小さな動きに適用することは困難であると考える．

一方，大坂らはキーボードの入力時間を利用した個人認証手法を提案している[9]．この研究では文字列を入力した時の各キーが押されてから離されるまでの時間を測定し，分散分析の解析手法を利用してキー入力パターンを求めている．事前に登録したパターンと認証対象のパターンが類似した場合に，両者の誤差分散が小さくなる性質を利用し，それをパターン距離として求めることで認証を行っている．しかし，タイピングスキルが低いユーザが入力した場合，毎回の入力時間のばらつきが大きく，キー入力パターンのばらつきが大きいことから認証精度が低下する問題がある．また，ユーザ間のタイピングスキルの差が小さければ小さいほどパターン距離の差も小さくなる傾向があることから，タイピングスキルの差が小さいユーザ間の認証が困難になると考えられる．

2.2 キーボード打鍵動作の取得方法に関する研究

Wang らは左手首に装着したスマートウォッチに搭載された加速度センサと角速度センサを利用することによってキーボードで入力された単語を推定している[10]．この研究では入力された単語を推定するために手指の動きからキーボードを打鍵したタイミングを推定し，キーボード上の手指の動きをトラッキングしている．打鍵のタイミングを推定するために机の平面に対して垂直な方向であるスマートウォッチの Z 軸加速度のピークを利用している．また，手指動作のトラッキングのために加速度データの二重積分による変位を求めている．そして，推定した打鍵のタイミングと手指の軌跡から打鍵しキーを推定し，推定したキーをもとにベイズ推定によって入力した単語を推定している．

また Tsubokura らは磁気センサを両手の甲に装着することでキーボード打鍵時の手の動作を分析している[11]．この研究では，手の位置を測定するためにキーボード付近に磁場を発生させる装置を設置している．しかし，磁気は周囲の磁性体によって変化するため環境によって精度が悪化する問題があると考えられる．さらに，キーボード打鍵時に常に磁場を発生させる装置が必要となるため，設置コストがかかる．

3. 提案手法

本章では，本研究の目的とアプローチを述べ，各アプローチについて，詳細を述べる．

3.1 研究目的とアプローチ

本研究ではログイン認証時の安全性を向上させるために，キーボードの打鍵動作特徴による個人認証手法を提案することを目的とする．本研究で提案する個人認証手法は行動的特徴を利用したバイオメトリクス認証であり，動作を取得する方法と認証時に利用する特徴量の抽出方法が重要となる．よって，本研究の目的を達成する上で解決すべき課題として次の 2 つが挙げられる．

A. キーボード打鍵動作の取得
B. 個人認証に利用する特徴量の抽出

一つ目の課題について，打鍵動作の取得方法としてキーボードから入力データを取得する手法，センサを手首に装着し，手の動作を取得する手法が考えられる．文献[9]ではキー入力データから入力時間を利用し，特徴量を抽出している．文献[10]，文献[11]ではそれぞれ手首，手の甲にセンサを装着することで手指動作を取得している．文献[9]のようにキー入力データを取得する手法については打鍵したキ

ーの種類，打鍵したタイミングしか取得することができず，個人認証を行うために十分な情報を得ることは困難であると考える．一方，文献[10]，[11]のように手首にセンサを装着する手法についてはセンサから直接装着部位の動作を取得することでキーボード上での手の動きや打鍵圧などキー入力データだけでは得られない情報を取得することができる．よって，本研究ではセンサを手首に装着することで手指動作を取得する．

二つ目の課題について，特徴量の抽出方法として，文献[8]では加速度データのピーク間隔を特徴量としている．この手法ではジェスチャ動作から特徴量を抽出することを想定しており，キーボードの打鍵動作のような小さな動きに適用するとピーク間隔が短くなり，適切な特徴量を抽出することは困難であると考える．文献[10]では，入力した単語を推定するために左手首に装着したスマートウォッチに搭載された 3 軸加速度センサ，3 軸角速度センサのデータから打鍵したタイミングと手指動作の軌跡を推定している．この手法では入力した単語を推定するためにユーザによる癖や個人を表す特徴を排除している．しかし，キーボードの打鍵動作はユーザによって打鍵方法やタイピングスキルが異なることから，打鍵速度や毎回の打鍵のばらつきも異なると考える．そこで，本研究では同一ユーザによる複数回の打鍵動作から取得した信号間の距離を特徴量として求めることで，同一ユーザ間の打鍵動作のばらつきによる個人認証を行う．

3.2 バイオメトリクス認証

バイオメトリクス認証は，特徴量登録プロセスと認証プロセスに分けられる[12]．図 1 に身体情報の取得から認証までの処理の流れを示す．

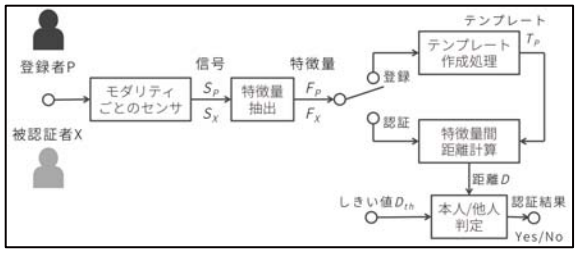

図 1　身体情報の取得から認証までの処理の流れ
（文献[12]から引用）

図 1 に沿って，提案手法における処理の流れを説明する．まず特徴量登録プロセスでは，事前に登録者 P からセンサを利用し，モダリティとしてキーボード打鍵動作の信号 S_P を取得する．取得した信号 S_P を特徴量抽出アルゴリズムによって特徴量 F_P に変換し，テンプレート T_P として登録する．ただし登録者 P は本提案手法で認証したいユーザの人数分登録できることを想定し，複数人の打鍵動作から T_P を登録する．

次に認証プロセスでは，被認証者 X は登録者 P と同様にセンサから打鍵動作の信号 S_X を取得し，特徴量 F_X に変換する．そして，F_X と T_P との特徴量間距離 D を算出する．最後に，求めた特徴量間距離 D がしきい値 D_{th} 以下の場合は本人，しきい値 D_{th} を超えた場合は他人であると判定する．しきい値は小さければ小さいほど他人の入力信号を拒否しやすくなるため，セキュリティレベルが上がる．しかし，本人の入力信号も拒否されやすくなるため，利便性の低下に繋がる．反対に，しきい値が大きければ大きいほど本人を受け入れやすくなるが，他人の入力信号であっても本人であると判定されやすくなる．

次節からは打鍵動作の取得方法，特徴量の抽出方法，特徴量間距離の算出方法について述べる．

3.3 打鍵動作の取得

文献[10]では，キーボード打鍵時のタイミングとキーボード上の手指の動きを推定するために左手首に装着したスマートウォッチに搭載された 3 軸加速度センサ，3 軸角速度センサを利用している．本研究ではキーボード打鍵動作を利用して個人認証を行うために，打鍵動作を取得する必要があるため，文献[10]と同様のアプローチを取り，手首に 3 軸加速度センサ，3 軸角速度センサを装着する．ただし，本研究では 1 度の認証につき 1 種類の単語を入力することを想定しており，入力する単語のキーが左右のどちらかに偏ることによる影響を防ぐため，両手首に 3 軸加速度センサ，3 軸角速度センサを装着する．本研究では ATR-Promotion 社製の TSND121[13]を使用し，リストバンドによって手首に固定する．図 2 に両手首に TSND121 を装着した様子と各軸の方向を示す．

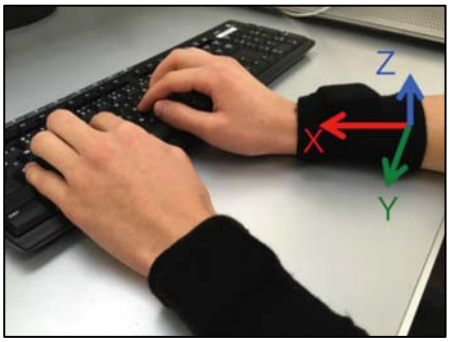

図 2　TSND121 を装着した様子と各軸の方向

そして，キーボード打鍵時のキー入力データ，3 軸加速度データ，3 軸角速度データを取得する．キー入力データには入力したキーの種類，そのキーを押した時刻，そのキーを離した時刻を記録する．また，打鍵データとして単語入力時間内の 3 軸加速度データと 3 軸角速度データの時系列データを記録する．単語入力時間はキー入力データから

取得した 1 文字目のキーを押した時刻から最後のキーを離した時刻とする．

3.4 特徴量の抽出

キーボードの打鍵動作について，タイピングスキルの高いユーザは小さな動きでキーを打鍵するため，毎回の打鍵動作のばらつきが小さくなると考えられる．しかし，タイピングスキルの低いユーザはキーの位置を確認するために手をキーボードから遠ざけることがあり，毎回の打鍵動作のばらつきが大きくなりやすいと考える．したがって，本研究では同一ユーザ間の打鍵動作のばらつきに着目した．

そこでユーザによる打鍵動作の違いを調査するために 2 名の被験者の左手首に 3 軸加速度センサを装着し，2 種類の単語を 5 回ずつ打鍵したときの打鍵データ(X 軸加速度)を取得した．図 3 に被験者 1 が“defence”と入力した時の打鍵データ（X 軸加速度)，図 4 に被験者 2 が“defence”と入力した時の打鍵データ(X 軸加速度)のグラフを示す．また，図 5 に被験者 1 が“japanese”と入力した時の打鍵データ（X 軸加速度)，図 6 に被験者 2 が“japanese”と入力した時の打鍵データ（X 軸加速度）のグラフを示す．

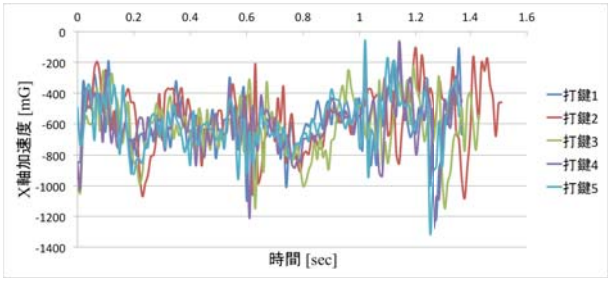

図 3　被験者 1 が“defence”と入力した時の打鍵データ（X 軸加速度）

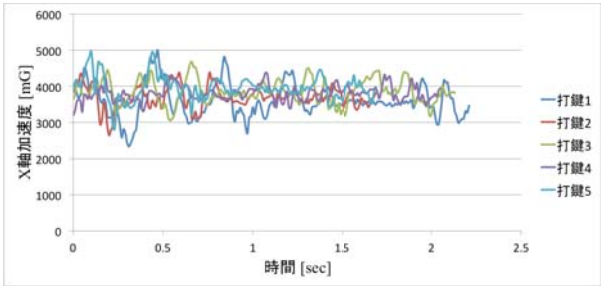

図 4　被験者 2 が“defence”と入力した時の打鍵データ（X 軸加速度）

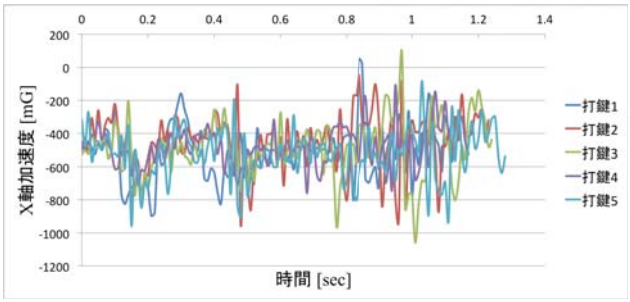

図 5　被験者 1 が“japanese”と入力した時の打鍵データ（X 軸加速度）

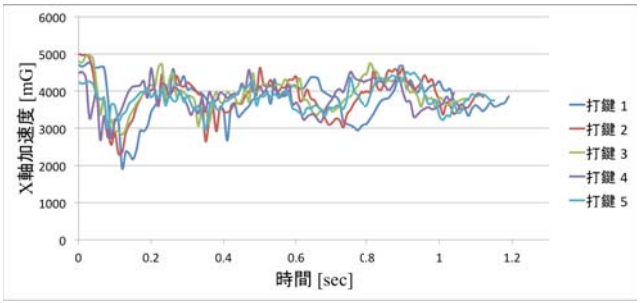

図 6　被験者 2 が“japanese”と入力した時の打鍵データ（X 軸加速度）

図 3，図 4，図 5，図 6 より，同一ユーザが同一の単語を入力すると入力時間には差が生じるが，概ね類似した波形が得られる．一方，図 3 と図 4，図 5 と図 6 を比較すると，異なるユーザが同一の単語を打鍵すると波形の形が異なり，打鍵のばらつきも異なることが確認できる．また，図 3 と図 5，図 4 と図 6 を比較すると，同一のユーザが異なる単語を打鍵すると波形の形は異なるが，打鍵動作のばらつきの大きさは似ていることが確認できる．このことから，同一ユーザによる複数回の打鍵動作から取得した信号間距離を特徴量とすることで本人を識別できると考える．そこで，本研究では同一ユーザによる複数回入力した同一単語の打鍵動作から取得した信号間の距離を求め，特徴量として利用する．しかし，単語の入力時間が異なることがあるため，センサデータの開始時点と終了時点をあわせ，各時点でのセンサデータの対応付けを行う必要がある．そこで DTW（Dynamic Time Warping）を適用する．DTW とは 2 つの異なる時系列データの各点の距離を総当りで比較した上で，系列同士の距離が最短となるパスを見つける手法である．また，この最短となるパスを DTW 距離と呼び，2 つの異なる時系列データをそれぞれ X，Y とすると，$D_{DTW}(X,Y)$で表す．

本研究では事前に本人の打鍵データを登録するために，事前に登録したいユーザ P から複数回打鍵時のセンサデータ S_{P1}~S_{Pn} を取得する．$i = 1,2,\dots,n,\ j = 1,2,\dots,n$（ただし，$i < j$）とするとき，$S_{P1}$~$S_{Pn}$ から 2 回分の打鍵データ S_{Pi}，S_{Pj} を取り出し，DTW 距離$D_{DTW}(S_{Pi},S_{Pj})$を求める．これら

打鍵データのすべての組み合わせについて DTW 距離を求め，テンプレート T_P として登録する．ただし，1 組分の T_P は両手首の 3 軸加速度データ，3 軸角速度データからそれぞれの軸の DTW 距離を求めるため，12 次元の特徴量として登録する．被認証者 X の特徴量を抽出する際も T_P の登録と同様に打鍵時のセンサデータ S_X を取得し，DTW 距離を求める．ただし，S_X は 1 回分の打鍵データしかないため，S_X と S_P との DTW 距離を求める．

3.5 特徴量間距離の算出

3.4 節で求めた特徴量は両手首に装着された 3 軸加速度センサ，3 軸角速度センサを利用している．つまり，複数箇所の身体情報を利用していることから，本研究の認証方式はマルチモーダル生体認証であると言える．マルチモーダル生体認証とは複数種類のモダリティの生体情報を組み合わせた認証方法である．マルチモーダル生体認証において，複数の距離を統合する手法は様々あるが，本研究では SVM（Support Vector Machine）によるスコアレベル統合手法を用いる．また，本研究で利用する識別器としてガウシアン関数をカーネル関数として導入した非線形 SVM を利用する．そして，被認証者 X の打鍵データ S_X と事前に取得した登録者 P の打鍵データ S_p との DTW 距離 $D_{DTW}(S_X, S_P)$ を認証用の入力信号 F_X として SVM に入力し，識別面との符号付き距離を特徴量間距離 D として算出する．

4. 評価実験

3 章で述べた提案手法の有効性を検証するために認証精度の評価実験を行った．

4.1 キーボード打鍵動作の取得

提案手法による認証精度を検証するために 5 名の被験者からキーボード打鍵時のセンサデータを取得する．このとき，被験者の両手首に 3 軸加速度センサ，3 軸角速度センサを搭載したセンサデバイスとして，ATR-Promotion 社製の TSND121[13]をリストバンドで固定した．次に，サンプリングレート 100Hz で 4 種類の文字列を 20 回ずつ入力し，キー入力データ，3 軸加速度データ，3 軸角速度データを記録した．入力する単語について，それぞれの単語の文字列の長さが異なり，入力する際に左右のどちらの手も 1 回以上打鍵するキーを含む単語が望ましい．また，右手で打鍵するキーと左手で打鍵するキーの数が同じ単語だけではなく，打鍵するキーが左右のどちらかの手に偏った単語を含める必要があると考える．従って，本実験で入力する単語は“defence”，“geological”，“ground”，“japanese”の 4 種類とする．取得した 20 回の打鍵データのうち 15 回分の打鍵データをテンプレート T_P 作成用に登録者 P の信号 S_p とし，残りの 5 回分の打鍵データを評価用の入力信号 F_x 作成用に被認証者 X の信号 S_X として利用する．

4.2 認証精度の検証

取得したセンサデータから 3.4 節で述べた手法によって特徴量を抽出し，テンプレート信号と入力信号を作成する．本実験では被験者 1 人あたり，20 回分の打鍵データを記録している．この 20 回分の打鍵データを 1~5 回，6~10 回，11~15 回，16~20 回の 4 つのブロックに分割する．そして，それぞれのブロックのうち 1 つのブロックを評価用の入力信号 F_X のための信号 S_X，残りの 3 つのブロックをテンプレート信号 T_P のための信号 S_P として利用し，4-分割交差検定を行う．F_X を DTW 距離 $D_{DTW}(S_{Xi}, S_{Pj})$，T_P を $D_{DTW}(S_{Pk}, S_{Pl})$で算出する．そして，算出した T_P から 3.5 節で述べたスコアレベル統合によって特徴量間距離 D を求める．

本実験で使用するテンプレート信号，入力信号のサンプル数について，テンプレート信号は 1 名あたり 15 回分の打鍵データから 2 回分の打鍵データを取り出し，DTW 距離を求めるため 105 通りある．この DTW 距離が 5 名分あるため，525 サンプルとなる．図 7 に 1~5 回目の打鍵データを評価用の入力信号とした時，1 名分のテンプレート信号のために求める DTW 距離の打鍵データの組み合わせを示す．図中の枠で囲まれた数字は打鍵した回を表し，実線で結ばれた左右の数字の回の打鍵データから DTW 距離を求める．ただし，求める打鍵データの組み合わせは全て同一ユーザ同士の打鍵データとする．

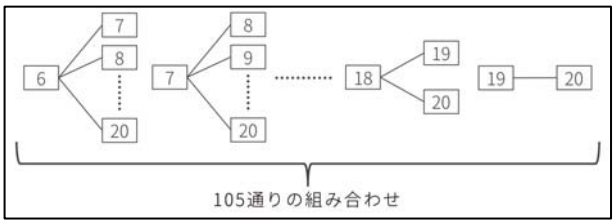

図 7　テンプレート信号のために求める DTW 距離の組み合わせ

本人の入力信号は 1 名あたり 5 回分の打鍵データと本人のテンプレート用打鍵データ 15 回分との DTW 距離を求めるため 75 通りある．本人の入力信号は 1 名分であるため 75 サンプルとなる．図 8 に図 7 と同様の条件で，本人の入力信号のために求める DTW 距離の組み合わせを示す．図 8 では，実線で結ばれた左右の数字は本人の 1~5 回目の打鍵データと本人の 6~20 回目の打鍵データを表す．

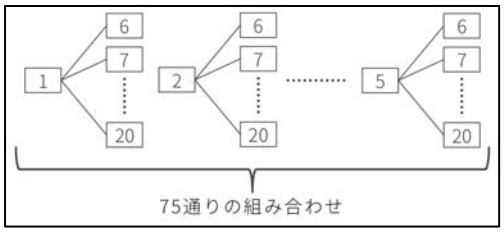

図 8　本人の入力信号のために求める DTW 距離の組み合わせ

他人の入力信号は，1 名あたり 5 回分の打鍵データと同一ユーザのテンプレート用打鍵データ 15 回分との DTW 距離を求めるため 75 通りある. 他人の入力信号は 4 名分あるため 300 サンプルとなる．図 9 に図 7，図 8 と同様の条件で他人の入力信号のために求める DTW 距離の組み合わせを示す. 図 9 では, 実線で結ばれた左右の数字は他人の 1~5 回目の打鍵データと他人の 6~20 回目の打鍵データを表す. ただし，求める打鍵データの組み合わせは全て同一ユーザ同士の打鍵データとする.

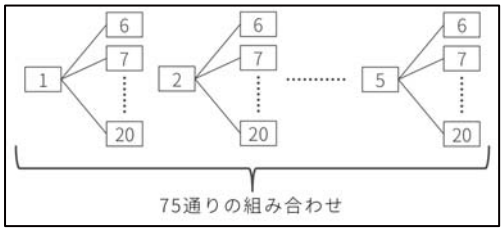

図 9　他人の入力信号のために求める DTW 距離の組み合わせ

SVM による識別関数はテンプレート信号の 525 サンプルを用いて作成し，作成された識別面と本人，他人の入力信号のサンプルとの符号付き距離を特徴量間距離 D として求める．最後にしきい値 D_{th} を変動させることで，各 D_{th} における本人拒否率（FRR, False Rejection Rate），他人受入率（FAR, False Acceptance Rate）を求める.

本研究における FRR は識別面と本人の入力信号 F_X との符号付き距離 D が D_{th} よりも大きくなる割合を表し，FAR は識別面と他人の入力信号 F_X との符号付き距離が D_{th} よりも小さくなる割合を表す. また, 各 D_{th} における FRR と FAR を求め，FRR と FAR が等しいときの誤り率を等誤り率（EER, Equal Error Rate）と呼ぶ．EER はバイオメトリクス認証における認証精度の評価指標の一つであり，値が小さければ小さいほど高精度な認証システムであることを示す. 例として，図 10 に被験者 D が“ground”と入力し，本提案手法による認証を行った時の FRR と FAR を記録したグラフを示す. 図 10 の FRR と FAR が交差している点が EER となる.

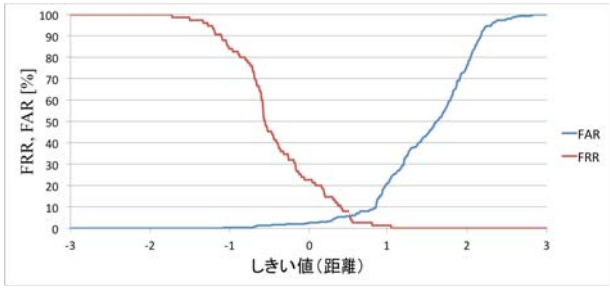

図 10　提案手法の FAR と FRR

4.3 実験結果

表 1 に 4 種類の単語別に求めた各被験者の EER を示す. 表の A, B, C, D, E は各被験者を表し，平均は全被験者の EER の平均値を表す. EER の最大値は被験者 E が“ground”と入力した時の 86.9%，最小値は被験者 D が“ground”と入力した時の 1.6%であり, 被験者によって認証精度が大きく異なる結果が得られた.

表 1　被験者・単語別の EER（単位：%）

		単語			
		defence	geological	ground	japanese
被験者	A	13.3	8.1	6.5	8.2
	B	23.8	16.7	8.8	12.2
	C	7.8	6.6	4.5	15.2
	D	6.1	10.8	1.6	6.9
	E	85.5	79.7	86.9	80.9
	平均	27.3	24.4	21.7	22.7

4.4 考察

4.3 節より，本人となる被験者によって認証精度に大きな差が現れた．特に被験者 E はどの単語を入力した場合も 8 割前後の EER が得られ，認証精度を大きく低下させている．一方，被験者 C，被験者 D は全体的に EER が低く，他の被験者と比べて高精度な認証を行うことができている.

これらの精度の違いについて, キーボード打鍵時の姿勢, 特徴量の抽出方法，使用するセンサデータの 3 つが影響していると考える. まず, キーボード打鍵時の姿勢について, 図 11 に被験者 E が“ground”と 5 回入力した時の左手の打鍵データ（X 軸加速度）を示す.

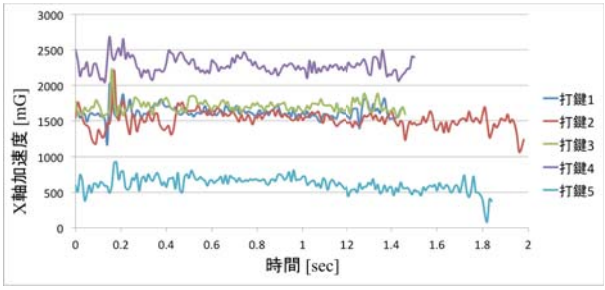

図 11　被験者 E が“ground”と 5 回入力した時の打鍵データ（X 軸加速度）

図 11 が示す通り，同一のユーザが同一の単語を打鍵した場合でも，センサデータの絶対値が大きく異なる場合がある．絶対値が大きく異なる原因として，加速度センサが重力の影響を受けているからであると考えられる．ユーザが打鍵時に姿勢を変えることで，手首の角度が変化し，装着された加速度センサが傾く可能性がある．これにより，3 軸にかかる重力加速度の値が変化し，各軸の絶対値が変化したと考えられる．

次に，提案手法では特徴量の抽出方法として同一ユーザによる複数の打鍵データから DTW 距離を求めており，この特徴量をテンプレート信号として登録している．つまり，テンプレート信号から同一ユーザ間の打鍵動作がどの程度似ているかを学習している．そのため，同一ユーザによる複数回の打鍵動作から取得した信号間の距離が近いユーザ同士の認証は認証精度が悪化する要因になると考えられる．

そして，本提案手法に利用したセンサデータについて，ある単語を入力した時，1 文字目のキーを押した時刻から最後のキーを離した時刻までの両手首に装着したセンサのデータを使用している．一般的にキーボードを打鍵する場合，キーの位置によって右手で打鍵するキーと左手で打鍵するキーが決まっており，打鍵する手は入力する文字列に依存する．そのため，打鍵しない方の手首から取得したセンサデータをノイズとしてテンプレート信号に登録している恐れがある．

5. まとめ

本研究ではログイン認証時の安全性を向上させるために，キーボードの打鍵動作特徴による個人認証手法を提案することを目的とする．そこで本稿では 3 軸加速度データ，3 軸角速度データから DTW 距離を求め，SVM によって DTW 距離を統合する手法を提案した．提案手法では，同一ユーザによるキーボード打鍵時の信号間距離を求めるために両手首から取得した 3 軸加速度データと 3 軸角速度データの各軸の DTW 距離を算出し，テンプレート信号として利用した．テンプレート信号からガウシアン関数をカーネル関数として導入した非線形 SVM 識別関数により求めた識別関数を用いて，テンプレート信号と入力信号との特徴量間距離を求めた．

評価実験では 5 名の被験者を対象に 4 種類の単語を入力した時の認証精度を検証するために EER を求めた．その結果，EER の最大値が 86.9%，最小値が 1.6%と，被験者によって認証精度に大きな差が現れた．原因として，キーボード打鍵時の姿勢，特徴量の抽出方法，利用するセンサデータが影響していると考えられる．

今後は被験者による認証精度の差が小さくなる特徴量を抽出し，認証精度を向上させる方法を検討したいと考えている．

参考文献

[1] 独立行政法人情報処理推進機構, “オンライン本人認証方式の実態調査報告書”, https://www.ipa.go.jp/files/000040778.pdf (accessed 2016-5-5).
[2] 矢野経済研究所，“バイオメトリクス市場に関する調査結果 2011”，http://www.yano.co.jp/press/pdf/828.pdf（accessed 2016-5-5）.
[3] 山田浩司，松本弘之，松本勉，“指紋照合装置は人工指を受け入れるか”，情報処理学会研究報告コンピュータセキュリティ(CSEC)，Vol.2000，No.68，pp.159-166(2000).
[4] 卓璐，王琛，浅井洋樹，山名早人，“3 軸加速度計を用いたデスクワーク中の割り込み可能性の推定”，第 7 回データ工学と情報マネジメントに関するフォーラム(DEIM2015)，E1-5，pp.1-8(2015).
[5] 増田大輝，田坂和之，大岸智彦，小花貞夫，“ウェアラブルセンサを用いたテニス上達支援システムの提案”，情報処理学会マルチメディア，分散，協調とモバイル(DICOMO2014)シンポジウム，pp.545-552(2014).
[6] 榎堀優，間瀬健二，“ウェアラブル加速度・角速度センサを用いたヤスリがけ技能評価の検討”，人工知能学会論文誌，Vol.28，No.4，pp.391-399(2013).
[7] 今野慎介，中村嘉隆，白石陽，高橋修，“複数のウェアラブルセンサを用いた歩行動作による本人認証法の精度向上”，情報処理学会論文誌，Vol.57，No.1，pp.109-122(2016).
[8] 行方エリキ，太田雅敏，石原進，水野忠則，“加速度センサ搭載腕時計型端末を用いた腕の動きによる個人認証”，情報処理学会研究報告ヒューマンコンピュータインタラクション(HCI)，Vol.2003，No.94，pp.21-26(2003).
[9] 大坂一司，矢野耕也，“品質工学の手法を用いたキーストロークによる本人認証”，情報処理学会研究報告コンピュータセキュリティ(CSEC)，Vol.2012-CSEC-58，No.19，pp.1-6(2012).
[10] Wang, H., Lai, T.T. and Choudhury, R.R.: MoLe: Motion Leaks through Smartwatch Sensors, Proc.*MobiCom'15*, pp.155-166 (2015).
[11] A. Tsubokura, N. Ashida, N. Matsubara, I. Oshima, K. Kozuki and K. Tsushima, “Analysis of key typing process using hand position process”, *Computers in Education*, Vol.1, pp.687-688 (2002).
[12] 半谷精一郎，“バイオメトリクス教科書 原理からプログラミングまで”，pp.7-8，コロナ社(2012).
[13] 小型無線多機能センサ「TSND121/151」|ATR-Promotions, http://www.atr-p.com/products/TSND121.html(accessed 2016-5-3).