情報処理学会論文誌 Vol.63 No.4 1094–1114 (Apr. 2022)

特徴の再訓練を必要としない変更可能な筆記

釜石 智史[1,a)] 宇田 隆哉[1,b)]

受付日 2021年1月31日, 採録日 2022年1月11日

概要：一般的な文字列パスワードは任意に変更可能であるという利点を持つが，推測された場合には攻撃者にも入力可能である．パスワードを複雑にすればするほど覚えておくことが困難になり，簡単にすればするほど攻撃耐性が低くなる．近年，一部のスマートフォンで用いられているように，指紋や顔の情報をパスワードの代わりに使用することも可能であるが，これらは変更できない情報であり，漏洩した場合の問題は大きい．そこで本研究では，パスワード入力に単語の筆記を組み合わせることで，パスワードによる本人確認を強化するシステムを提案する．もちろん，筆記による本人確認を行う研究は多数存在するが，大人数の利用者がいることや利用者の増加が考慮されていない．また，入力した署名そのものを登録しているため，再登録なしに署名の変更が行えない．一方，本システムで使用される手法においては，利用者が増えた場合でも機械学習による再訓練を必要としない．また，利用者が非常に多い場合でも，機械学習の計算コストを一定に保つことが可能である．筆記に関しては，攻撃者による覗き見を考慮し，筆記の痕跡が残らないよう，Leap Motion を用いてシステムを実装した．11 人の被験者による評価を行い，登録者の本人拒否率を 0.067 とする閾値 0.6 で未登録者による他人受入率を 0.068 に，登録者の本人拒否率を 0.109 とする閾値 0.7 で未登録者による他人受入率を 0.045 にできることを示した．

キーワード：深度センサ，リープモーション，生体認証，筆記認証，機械学習，畳み込みニューラルネットワーク

Changeable Scripts without Retraining of Handwriting Features

Satoshi Kamaishi[1,a)] Ryuya Uda[1,b)]

Received: January 31, 2021, Accepted: January 11, 2022

Abstract: General text password has an advantage that it can be freely changed, but also has a disadvantage that it can be inputted by attackers when it is presumed. The more complicated the password is, the more difficult it is remembered. On the other hand, the simpler it is, the easier it is presumed. As it is used for some kinds of smart phones in recent years, fingerprint or face can be used instead of password. However, their leakage causes serious problems since they are unchangeable information. Therefore, in this paper, we propose a system for enhancing password identification by combining passwords and scripting of words. Of course, there are many researches for personal identification by handwriting, but huge number of users and increasing the number are not considered. Moreover, handwritten signatures cannot be changed without retraining since the signatures are directly trained. On the other hand, in our method of the system, no retraining of machine learning is required even when the number of users increases. Moreover, the cost for machine learning can be kept in constant when the system has huge number of users. In implementation of the system, we chose Leap Motion not to remain handwriting trajectory against copying by attackers. We evaluated the system with 11 examinees and showed that false acceptance rate of unregistered users was able to decrease to 0.068 when false rejection rate was equal or under 0.067 by setting threshold to 0.6, and false acceptance rate of unregistered users was able to decrease to 0.045 when false rejection rate was equal or under 0.109 by setting threshold to 0.7.

Keywords: depth sensor, leap motion, biometrics, handwriting, machine-learning, convolutional neural network

1. はじめに

本人確認は様々なサービスにおいて必要であり，状況に応じていくつかの種類が用いられている．最も一般的な手法はパスワードによるもので，Web などのオンラインサービスに用いられている．生体情報やセキュリティデバイスを用いた本人確認方法もある．また，対面の場合，身分証明書の確認などが通常用いられている．これらの方法にはそれぞれ利点と欠点があり，すべてのサービスにおいて万能に適用できるといわれる方法はない．

民間団体が提供するオンラインサービスにおける本人確認には，パスワードを用いるものが一般的である．再発行の手間や変更時の利便性，コスト，本人確認に掛かる時間などを考慮すると，最も適しているからであると思われる．

指紋や顔などの生体情報による本人確認は，スマートフォンのロックや特定の場所のドアのロックなどに用いられている．生体情報は任意に変更することが不可能であることが問題であり，とくに他人が生体情報を管理する際には，情報が流出しないように厳格に管理される必要がある．研究としては，本物ではない指紋を登録して照合するものがあり [1]，残留指紋からでも指紋照合装置に誤認識させられる偽の指を作ることも可能とされている [2]．また，銀行などで使用されている指静脈による本人確認も，装置に誤認識させられるとされている [3]．

生体情報による本人確認技術として，ライフログを用いるものも存在する [4], [5], [6]．ライフログ自体は，絶対的に完全に個人を識別できるものではなく，一定割合の攻撃者を対象から除外することで，セキュリティを高めるために使用される．ライフログは指紋や静脈と異なり，絶対的に変更できないものではないが，強制的に行動を変更する必要があり，生活に支障や負荷が生じることは否めない．また，ライフログが漏洩した場合に，指紋や静脈よりも攻撃者による複製が容易であることも問題である．

オンラインサービスには，セキュリティデバイスを用いて本人確認を行うものがある [7], [8], [9]．この手法は物理的な盗難に対して脆弱である．また，デバイスを紛失したり，デバイスが故障したりすると，再発行までの間サービスが利用できなくなる．なお，再発行の過程においてソーシャルエンジニアリングなどによる攻撃を受けないしくみが必要であり，簡易な手段で再発行を行うことには問題がある．

対面による本人確認の場合，そのセキュリティは対応した人物の能力に大きく依存する．クレジットカードの署名を目視で確認する場合，人間にとって類似の署名を見分けることは困難である．身分証明書を確認する場合にも，それが偽造されたものであるかどうか見抜くにはそれなりの知識や経験が必要である．偽造防止の特殊な IC チップを含む旅券も存在するが，すべての民間団体が容易にその確認を行えるわけではない．一方で，米国のスーパーマーケットや小規模な雑貨店で一般的に用いられている，レジにおけるクレジットカードの電子的な署名は，機械的に手書きの署名を照合する技術があれば，人間の目視に依存しない本人確認が可能である．この署名が機械的に確認されているかどうかは非公表であるため分からないが，手書きの署名を照合する研究 [10], [11], [12] は存在するため，理論的には可能である．

以上より，情報漏洩のリスクや変更・再発行のコスト，人間の確認能力に依存しない性質などを考慮すると，パスワードが最も無難な選択肢であることは間違いない．しかし，パスワードも万能ではない．覚えやすいパスワードは攻撃者に推測されやすいし，複雑で長いパスワードは記憶や入力が困難である．そこで，追加の本人確認手段を用いてセキュリティを強化する手法もとられている．たとえば，通常と異なる IP アドレスからログインした場合，登録されたメールアドレスにワンタイムパスワードが送信され，その入力を要求されるなどがある．クレジットカードによっては，海外の IP アドレスから決済しようとすると一時的にロックが掛かる場合もある．前述のセキュリティデバイスも，基本的にはパスワードによる本人確認を強化するために用いられている．

本研究の目的は，補助的にパスワードなどによる本人確認を強化することにある．IC カードやセキュリティトークンのような，本人のみが所有するデバイスは，再発行が迅速に行えないこと，盗難された場合に攻撃者に使用されてしまうことが問題であるため，本研究ではこの点を改善する．具体的な本人確認手段としては空中に筆記された文字の筆跡を用いるが，本システムは次の要件 1〜7 を満たすものであり，これを特徴とする．

要件 1 本人確認デバイスの再発行を行わない．

要件 2 覗き見によるコピーに対してある程度の耐性を持つ．

要件 3 1 度の覗き見によるコピーを行わせない．

要件 4 入力および本人確認に長時間を要しない．

要件 5 利用者の増加による機械学習の再訓練[*1]を行わない．

要件 6 利用者が非常に多い場合でも，機械学習による訓練コストを一定に保つ．

[1] 東京工科大学大学院
Tokyo University of Technology Graduate School, Hachioji, Tokyo 192–0982, Japan
[a)] d2118001a6@edu.teu.ac.jp
[b)] uda@stf.teu.ac.jp

[*1] 本論文における「訓練」は，機械学習における training の訳語である．「学習」が使用される論文もあるが，これは learning の訳語として使用されており，混乱が生じるため本論文では training の訳語としては使用しない．ただし，「過学習」は over fitting/over training の訳語として定着してしまっているため，そのまま使用するものとする．

要件 7 攻撃者のデータが訓練に含まれない場合にも本人確認が行える．

本研究の技術を用いれば，ネットショッピングなどの決済における追加の本人確認手段としても有効であり，e-Tax などのしくみへの置き換えや，将来の選挙における電子投票などにも使用できる．さらに，覗き見による問題も考慮しているため，対面による本人確認にも有効である．

2. 関連研究

本章では，1 章の末尾であげた要件 1〜7 に照らし合わせながら，関連研究を紹介する．

2.1 機械学習を利用しない筆記を用いた本人確認手段

Hanyu らは，データセットに登録した，ひらがな，カタカナ，漢字の一部からランダムで数文字選択して iPad に指で書かせることで，個人識別を行う研究を行っている [13]．iPad 上で指で書くということは，タッチパネル上に指の跡が残ることから，スマッジアタックをされる可能性があるため，要件 2 と要件 3 を満たさない可能性もある．

Kato らは，ペンタブレットを使って利用者に好きな図を書かせ，筆記時のストロークを DP マッチング（動的計画法）することによって個人識別を行う研究を行っている [14]．

Takahashi らは，スマートフォン上に記号を指で書くことで，個人識別を行う研究を行っている [15]．具体的には，ユークリッド距離を利用し，筆記を比較している．テスト時には，ユークリッド距離によってすべての登録者と比較を行うため，登録者が多い場合に要件 4 を満たさない．

Sae-Bae らは，タブレット端末のような大型のマルチタッチパネルの上に 5 本の指を置かせ，時計回りに回すことや，一方向にスワイプすることなどのジェスチャによって個人を識別する研究を行っている [16]．Sae-Bae らは言及していないが，パネル上に指の跡が残ることから，要件 2 と要件 3 を満たさない可能性もある．

Shen らは，手首にセンサを取り付け，筆記時の動作を DTW によって比較し，個人識別を行う研究を行っている [17]．

畠中らは，Leap Motion を用いて空中に名前を手書きで書かせ，DP マッチングによって個人識別を行う研究を行っている [18]．

Lu らは，Leap Motion を用いて空中で手書きのパスワードを入力させることで，個人識別を行う研究を行っている [19]．Lu らの手法では，最初にテンプレートの登録を行い，テスト時に入力されたデータを TTV（Threshold-Then-Vote）アルゴリズムを用いてテンプレートと比較している．

Renuka らは，ペンの構造をした入力デバイスを用いて文字を書き，その文字を識別する評価を行っている [20]．識別には「.Net」を使って開発された文字認識統合開発環境を使用しており，文字認識アルゴリズムは言及されていない．また，文字入力を認証に使用するとしているが，書かれる文字の目視が困難と述べているのみであり，入力した文字によるパスワード認証が想定されている．彼らは 0 から 9 までの数字を書く評価しか行っていないが，彼らの論文にある筆記の軌跡を見る限り覗き見による判別は容易であり，筆記の特徴を本人確認に使用しないため要件 2 および要件 3 を満たさない．

Hu らは，テンプレートクラスタリングに基づく 2 段階の署名検証システムによってペンタブレットで書かれた署名が誰のものか分類する研究を行っている [21]．クラスタリングの閾値を超えていた署名のみを，2 段階目の個人識別に使用するように工夫されている．テスト時には，入力された署名をすべての登録された署名と類似性スコアの比較を行わなければならないため，登録者が多い場合に要件 4 を満たさない．

Xiao らは，Leap Motion で空中に署名を手書きし，個人識別を行う研究を行っている [22]．Leap Motion で空中に書いた署名をテンプレートマッチングと DTW を用いて筆者を検証している．

畠中らは，Leap Motion を用いて空中に名前を手書きで書かせ，個人識別を行う研究を行っている [23]．テスト時には，DP マッチングによってすべての登録者と比較を行うため，登録者が多い場合に要件 4 を満たさない．この手法では，畠中らによる「Leap Motion を用いた空中署名での個人認識システムに関する研究」とは異なり，入力の途中で手の形を変える必要がある．しかも，変える回数，順番，形は登録されたとおりでなければならない．登録者の人数によらず，この動作自体が要件 4 を満たさない．

以上より，既存の関連研究で機械学習を使用しない場合は要件 4 を満たすことができないものがある．これは，テストの際の入力に時間が掛かることではなく，入力されたデータを登録済みのデータと比較する際に生じる問題である．

一部要件 4 を満たしている手法があるが，これらのものは特定の署名（もしくは名前の筆記など）を使用しているか，動きそのものに覗き見耐性がない．たとえばジェスチャを登録する Sae-Bae らの手法は，ジェスチャを真似されることを想定していないが，我々の手法では同じ単語の入力を続けて要求しなければこれを避けることができる．Renuka らの手法は，そもそもパスワード入力であるので覗き見耐性が考慮されていない．特定の署名を登録する手法に関しては，本論文の要件 1〜7 を基本的にはすべて満たす．しかし，1 度覗き見たものが動画などで，攻撃者が何度も練習可能である場合には要件 3 を満たさなくなる可能性がある．一方，我々の手法では同じ単語の入力を続けて要求しなければこの攻撃は行えない．

2.2 機械学習による筆記を用いた本人確認手段

Lu らは，特製のウェアラブルデバイスが貼り付けられた手袋をつけ，空中に署名を手書きして個人識別を行う研究を行っている [24]．具体的には，DTW（Dynamic Time Warping：動的時間伸縮法）で入力信号の長さを合わせ，SVM（Support Vector Machine）による分類を行っている．Lu らの方式は，本人か本人でないかの 2 値分類であり，要件 5，要件 6 を満たさない．

Alkaabi らは，ペンで筆記した画像データを用いて個人識別を行う研究を行っている [25]．機械学習には CNN（Convolutional Neural Network：畳み込みニューラルネットワーク）を用いているが，利用者が増えるたびに，それまでの利用者の署名とも区別するのであれば要件 5，要件 6 を満たさない．

Behera らは，Leap Motion のうえで利用者に空中に署名を筆記させることで個人識別を行う研究を行っている [26]．具体的には，DTW で入力信号の長さを合わせ，k-NN（k-nearest neighbor algorithm：k 近傍法）で分類する方法と，HMM（Hidden Markov Model：隠れマルコフモデル）に入力して分類する方法の 2 つを提案している．k-NN で多値分類する場合と HMM で 2 値分類する場合において，利用者が増加する際に要件 5 を満たさない．また，利用者が多い場合に要件 6 も満たさない．

Yamamoto らは，Leap Motion で利用者に 0〜9 の数字を書かせ，個人識別を行う研究を行っている [27]．CNN を用いて 2 値分類を行っているため，利用者が増加する際に要件 5 を満たさない．また，利用者が多い場合に要件 6 も満たさない．

Mohammed らは，ペンタブレットで筆記した署名の画像を用いて個人識別を行う研究を行っている [28]．SVM と k 平均法を両方使用しており，k 平均法は利用者が多い場合にテスト時に時間が掛かり，要件 4 を満たさない．また，SVM の使用は，利用者が増加する際に要件 5 を満たさない．また，利用者が多い場合に要件 6 も満たさない．

Singh らは，紙に書かれた手書き文字から筆者の個人識別を行う研究を行っている [29]．k 平均法による多値分類を使用しているため，利用者が多い場合にテスト時に時間が掛かり，要件 4 を満たさない．また，利用者の増加に比例して機械学習による訓練コストが増加するため，要件 6 を満たさない．

Rosa らは，センサが内蔵されたペンで名前の筆記を行い，取得された傾きや加速などの要素を画像化することで個人を識別する研究を行っている [30]．画像の分類には CNN が用いられており，利用者が増加する際に要件 5 を満たさない．また，利用者が多い場合に要件 6 も満たさない．

高橋らは，ペンの筆跡画像を幾何学的に解析することで，個人識別を行う研究を行っている [31]．筆者の識別には階層型ニューラルネットワークが用いられており，利用者が増加する際に要件 5 を満たさない．また，利用者が多い場合に要件 6 も満たさない．

小南らは，ペンタブレットを用いて署名を筆記させ，個人識別を行う研究を行っている [32]．小南らの手法では，筆圧と筆跡の 2 つが HMM で訓練され，モデルとなる．まず，入力された文字が見えるため，要件 2 を満たさない．また，この HMM は利用者全体で訓練を行う必要があるため，利用者が増加する際に要件 5 を満たさない．また，利用者が多い場合に要件 6 も満たさない．

以上より，既存の関連研究で機械学習を使用する場合は要件 5 と要件 6 を満たすことができない．なお，要件 7 については，これらの関連研究において言及されていなかった．論理的には，テストデータによる本人確認を行う前に，OC-SVM（One Class Support Vector Machine）などのアルゴリズムを本人の訓練データに対して適用することで，解決が可能である．実際に OC-SVM を用いた筆跡による本人確認の研究も行われており，Guerbai らは，OC-SVM は大量のサンプルがある際に精度を上げるのに効果的であるが，サンプルの中に訓練に入れると精度を下げてしまうものも含まれているため，OC-SVM カーネルに改良を加えることで精度を上げる手法を提案している [33]．ただし，OC-SVM の適用は，その計算コストが追加されることに加え，利用者人数分の OC-SVM のモデルをシステム側で保持し続けなければならない問題が生じる．さらに，OC-SVM を前段階のフィルタとして追加すると，最終的な FRR（False Rejection Rate：本人拒否率）に影響を与えるため，FRR の再評価も必要になる．

なお，要件 5 は転移学習を行うことで解決可能である．Granet らや Aneja らは，転移学習を用いて筆記を認識する研究を行っている [34], [35]．ただし，彼らの研究は筆記により個人を識別するものではなく，筆記された文字を判別するものである．

3. 提案システムと手法

本論文で提案するシステムは，パスワードなどによる本人確認手段を強化するものである．本システムは，1 章の末尾にあげた要件 1〜7 を満たすものであり，これを特徴とする．

3.1 システム概要

本システムでは，Leap Motion を使用して利用者の本人確認手段を強化する．Leap Motion の使用は，システムを作成する手法において必須ではないが，要件 2 を考慮し，次の理由から Leap Motion を選択した．まず，Leap Motion を用いて空中に文字を描くため，筆跡が残らず，攻撃者は動画で録画したものを真似て入力を行う必要がある．平面に描かれた文字のように，その文字をなぞって複写するような入力は行えない．要件 2 において，覗き見耐性を「あ

る程度」としたのは，繰り返し録画されたものを見て模倣された場合には，破られる可能性が十分にあることを考慮したためである．また，攻撃者は，指の動きを参考にできる位置から撮影を行う必要がある．なお，Rosa らの研究 [30] では Biometric Smart Pen を用いて加速度などの情報を取得しているように，入力時の加速度などを取得するために本研究では Leap Motion を用いている．

提案システムは，パスワードによる本人確認を強化するためのものであるので，利用者はまず従来どおりの方法でパスワードを入力する．この入力方法は本研究とは独立しているため問わない．その後，画面に現れる単語を，Leap Motion を用いて空中筆記するというものである．提案システムの構成と利用者の操作手順について，前述の要件をふまえて概説する．利用者の手順を以下に示す．

- 登録フェーズ
  (1) 画面に表示される単語を空中に筆記する．
  (2) 筆記した単語を分解する．
  (3) 分解した中から数千個サンプルを抽出する．
  (4) (1)〜(3) を登録したい人数分行う．
  (5) 抽出したサンプルを人ごとに分け機械学習で訓練する．
- 個人識別フェーズ
  (1) 画面に表示される単語を空中に筆記する．
  (2) 筆記した単語を分解する．
  (3) 分解した中から数千個サンプルを抽出する．
  (4) 登録フェーズで訓練したモデルを利用して抽出したサンプルを検証する．
  (5) 検証した結果から本人か他人かを分類する．

登録フェーズでは，利用者は，システムから入力を求められる a 個の単語を筆記して入力する．a は利便性を考慮し 10 程度であり，本論文の評価においては 10 としている．

利用者が入力した筆記情報は，筆記を分解するための訓練済みモデルに入力され，筆記時の特徴として分解される．この訓練済みモデルは，この利用者とは関係なく事前に作成されたものであり，いかなる利用者にも依存しないものである．

機械学習における 1 回の訓練に入力される利用者を k 人と仮定すると，1 人の利用者による筆記時の特徴は，$k-1$ 人の筆記時の特徴と合わせられ，機械学習による訓練が行われる．つまり，誰の筆記かを判定する k 値分類の訓練である．この $k-1$ 人の筆記時の特徴は，システム側で任意に集めたものであり，k は利便性を考慮し 10 程度であり，本論文の評価においては 10 としている．訓練されたモデルは，利用者ごとに割り当てられた ID と結び付けられて保存される．

個人識別フェーズでは，利用者は，まず通常の本人確認手段を実行する．これはパスワードなどによる本人確認手段である．続いて，追加の本人確認手段として，利用者は，システムから入力を求められる 1 個の単語を筆記して入力する．このとき，利用者が入力した ID とこの筆記時の特徴が，利用者の本人確認手段を強化するものとなる．入力された 1 個の単語の筆記は，筆記を分解するための訓練済みモデルに入力され，筆記時の特徴として分解される．システムは，入力された ID に結び付けられている，筆記時の特徴の訓練済みモデルに，1 個の単語の筆記時の特徴を入力し，個人識別の判定を行う．この判定は，2 つの段階に分けられる．まず，入力された筆記時の特徴が，筆記時の特徴の訓練済みモデルの k 値分類により，k 人の誰に一番近いかを判定する．システム全体の利用者を m 人とすると，常識的に m は k より大きく，k は正規ユーザ 1 人とシステム側で任意に集めた $k-1$ 人で構成されるため，この中に攻撃者はいない．よって，攻撃者がいる場合，この k 人に含まれる人間以外の誰かということになる．筆記時の特徴の訓練済みモデルの k 値分類により，筆記時の特徴が一番近いものが正規ユーザ以外の $k-1$ 人のいずれかになれば，その時点で本人確認は失敗する．次に，筆記時の特徴が一番近いものが正規ユーザとなった場合の手順について説明する．本システムにおいては，本人確認の閾値がある．この閾値を上回れば，正規ユーザ本人であると判定され，そうでなければ本人確認に失敗する．

提案システムと要件についての確認を行う．要件 1 については，本システムでは Leap Motion という本人確認デバイスを必要とする．しかし，e-Tax の IC カードやハードウェアトークンなどと異なり，利用者ごとに本人確認をして再発行を行う必要はなく，1 つのデバイスを複数人で使い回すことも可能である．よって，再発行という手順は存在せず，要件 1 を満たす．

要件 2 ついては，本節でも前述したように，Leap Motion 自体がある程度の覗き見耐性を持っているため満たす．また，個人識別フェーズでシステムから入力を求められる 1 個の単語は毎回変わるため，1 度もしくは数回覗き見たものをそのまま模倣して入力することはできない．これは要件 3 についてもあてはまる．なお，要件 2 の定義が厳密でないのは，提案手法に絶対的な覗き見耐性はないことを筆者らが認めているためである．

要件 4 については，個人識別フェーズでシステムから入力を求められるものは 1 個の単語であり，クレジットカードの利用時に署名する作業とほぼ同等の時間的負荷と考えられるため満たす．

要件 5 については，機械学習を行うのは利用者を含めた k 人であり，システムの利用者数 m には依存していないため満たす．また，登録フェーズ後に m に増減があった場合でも，登録フェーズをやり直すことはない．これは要件 6 についてもあてはまる．

要件 7 については，機械学習を行うのは利用者を含めた k 人である一方，筆記時の特徴が一番近いものが正規ユー

ザとなった場合でも，その際の閾値によって本人か本人でないかを判別可能であるため満たす．

3.2 登録フェーズ

3.2.1 Leap Motion によるデータの取得

登録フェーズにおいて，利用者は，システムから入力を求められる単語を，Leap Motion を使用して筆記して入力する．

Leap Motion が取得するのは利き手の 5 指の指先と手のひら中央の合計 6 カ所の情報である．各箇所の情報は，X，Y，Z 軸の 3 軸に分けて，以下のものが取得される．

- 移動距離 [mm]
- 回転角度 [rad]
- 速度 [mm/s]

つまり，1 回あたり 6 カ所 × 3 軸 × 3 項目の 54 項目の情報が取得される．本論文では，この 1 回を 1 フレームと呼び，200 フレーム/秒でこれらの情報の取得を行う．なお，移動距離とは前フレームからの移動距離であり，回転角度とは前フレームからの回転角度である．回転角度は軸に向かって右回転がプラスとなる．また，速度とは speed ではなく velocity であり，プラスとマイナスの向きを持つ．Leap Motion の API Overview には，Distance，Time，Speed，Angle の 4 つの項目が取得できると記載されているが，Time は Distance と Speed から算出可能であるため 3 つの項目を使用した．Distance は DistanceTo，Angle は AngleTo という関数を使用して取得した．これらは「Vector - Leap Motion C# SDK v2.3 documentation」に掲載されており，どちらも Vector を入力すると float の値を返す．Vector クラスには x，y，z メンバがあり，3 つの軸を合わせて 1 つの移動距離と回転角度を求められる．それぞれの軸で別個に距離や角度を求めるため，x の場合はたとえば DistanceTo(Vector.x,0,0) というように 1 つの軸だけにして計算している．Time については，フレームごとに経過時間を記録し，前のフレームとの時間の差から 1 フレームの時間を算出した．Speed は次に示す式 (1) で算出している．

$$\frac{Distance\,(\mathrm{mm})}{Time\,(\mathrm{ms})} * 1{,}000 = Speed\,(\mathrm{mm/s}) \tag{1}$$

3.2.2 筆記の分解

利用者が入力した筆記情報は，筆記を分解するための訓練済みモデルに入力され，筆記時の特徴として分解される．本項では筆記を分解する方法について説明する．

本論文で使用する，分解された筆記とは，「左から右」，「右から左」，「上から下」，「下から上」の 4 つである．以後，本論文ではこれらを「4 つの向き」と総称する．筆記中にこれ以外の要素が現れても無視する．たとえば，曲線の場合にはどの程度曲がっているかを考慮する必要があるし，斜め方向の線の場合にはどの程度傾いているかを考慮する必要がある．これらを除去して単純化するため，前述の 4 つの向きのみを用いた．なお，曲線の一部を拡大した場合，もしくは角度が浅い斜め方向の線であった場合には，直線に近似可能な要素が含まれる場合がある．これらは 4 つの向きとして分解される．

筆記を分解するためには筆記の情報が必要となる．これらは，筆記の分解専用の被験者を用いて集められる．筆記の分解専用の被験者とは，システムの利用者とは別に集められた人物を指す．筆記の分解専用の被験者には位置が決められた空間が用意され，その空間に前述の 4 つの向きの直線が筆記される．これら，すべての被験者の筆記は，4 つの向きのそれぞれの向きごとにラベルが付与され，すべてまとめて機械学習のネットワークに入力される．なお，機械学習においては，入力される 1 つのデータの塊を 1 サンプルと呼ぶため，本論文でも機械学習のネットワークに入力されるデータの単位をサンプルと呼称する．本研究で用いる機械学習のネットワークにおいては，入力時のサンプルサイズを統一する必要がある．サンプルサイズは前述の 54 項目 × フレーム数に依存し，フレーム数は筆記にかかる時間によって変化する．本論文では，フレーム間での線形補間を用いて，被験者の平均フレーム数になるようサンプルサイズを統一する．たとえば，平均フレーム数が 20 である場合，18 フレームのサンプルは 20 フレームになるように線形補間が行われる．こうして，統一されたサンプルサイズに線形補間したすべてのサンプルを使い，訓練および検証が行われる．

3.2.3 筆記の特徴抽出

システムは利用者に単語を提示する．この単語は辞書などに掲載されているものでよく，本論文の評価ではパブリックドメインの辞書からランダムに選択している．具体的には「apple」などである．単語の長さの規定はないが，長いほうがより多くの特徴を抽出できる．本論文の評価では 3 文字以上の単語としている．利用者は，システムから入力を求められる a 個の単語を筆記して入力する．a は 10 程度である．9 や 11 では不適切というわけではないが，本論文の評価においては切りの良い数字である 10 としている．入力された a 個の筆記データは，それぞれ元のフレーム数が 0.2 倍から 3.0 倍になるように，0.2 きざみでフレーム間での線形補間が行われる．この線形補間後のすべてのデータから，3.2.2 項の訓練済みモデル作成時に使用された，平均フレーム数の長さとなるサンプルが切り出される．

具体的には，線形補間後のある筆記データが 1〜n フレームで構成され，3.2.2 項の訓練済みモデルにおける平均フレーム数が ave とすると，i 番目のサンプルは i フレームから ave + i − 1 フレームまでが切り出され，合計 n − ave + 1 個のサンプルが切り出されることになる．

利用者が入力した a 個の単語の筆記すべてに対して，線形補間してから切り出されたすべてのサンプルは，3.2.2 項

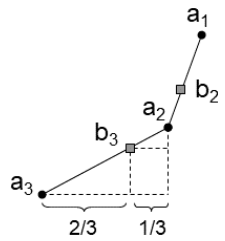

図 1 線形補間のイメージ
Fig. 1 Overview of linear interpolation.

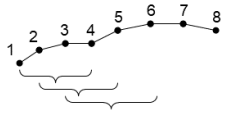

図 2 サンプルの切り出し方
Fig. 2 Extraction of samples.

の訓練済みモデルに入力される．この訓練済みモデルは，入力されたサンプルを 4 つの向きのいずれかに分類するが，その際にソフトマックス値も出力する．1 個の単語の筆記から作成された大量のサンプルに対して，このソフトマックス値が高かった上位 b 個のみを，次項で述べる筆記の特徴の訓練で使用する．本システムでは，b は数十～数千である．

線形補間のイメージを**図 1** に示す．

図のように，たとえば a_1，a_2，a_3 と 3 つの点があり，これを 4 つの点 b_1，b_2，b_3，b_4 にしたいとする．a_1 と b_1 は同一であり a_3 と b_4 は同一であるため，b_2 と b_3 を線形補間によって導出すればよい．位置が均等になるようにするため，a_2 から見て a_1 や a_3 から 1/3 の距離に b_2 と b_3 を持ってくる．前フレームからの移動距離や回転角度の場合，a_3 の持つ値の 1/3 が a_2 から b_3 までの変化量となり，a_2 の持つ値の 1/3 が b_2 から a_2 までの変化量となる．速度の場合には，a_3 と a_2 の差の 1/3 を a_2 に足したものが b_3 の値となる．このように，線形補間によってフレーム数を増やしたり減らしたりして調整する．

次に，サンプルの切り出し方について**図 2** を用いて説明する．

実際には 1 サンプルは 20 フレームであるが，ここでは簡略化のために 8 フレームの筆記データ（$n = 8$）から 4 フレームずつのサンプル（$ave = 4$）を切り出すものとする．図の番号が筆記データのフレーム番号に対応する．まず，1～4 フレーム目が切り出されて 1 つ目のサンプルとなる．次に，2～5 フレーム目が切り出されて 2 つ目のサンプルとなる．3 つ目のサンプルは 3～6 フレーム，4 つ目のサンプルは 4～7 フレーム，5 つ目のサンプルは 5～8 フレームである．よって，$n - ave + 1 = 8 - 4 + 1 = 5$ 個のサンプルが切り出される．

切り出されたサンプルは，機械学習により「左から右」，「右から左」，「下から上」，「上から下」の 4 つのいずれかに分類される．このとき，どの程度の信頼を持ってそこに分類されたかの基準となるのがソフトマックス値であり，たとえば「左から右」に分類されたサンプルのソフトマックス値が高ければ，それは「左から右」である可能性が高いが，ソフトマックス値が低ければ，他の 3 つよりは「左から右」である可能性が高いだけということになる．

3.2.4 筆記の特徴の訓練

3.2.3 項で述べた，1 利用者あたり a 個の筆記 × b 個のサンプルを，この利用者のサンプルとしてネットワークに入力し，機械学習による訓練および検証を行う．この利用者による筆記時の特徴は，システム側で用意した k − 1 人の筆記時の特徴と合わせられ，k 値分類が行われる．k は 10 程度である．訓練後は，この利用者に ID が割り当てられ，その ID に基づく利用者の筆記の特徴の訓練済みモデルが保存される．

3.3 個人識別フェーズ

個人識別フェーズでは，利用者は，まず通常の本人確認手段を実行する．本論文ではパスワードなどによるものを想定しているが，それに制限されるものではない．本論文の技術とは関係がないため記述は省略する．

追加の本人確認手段として，利用者は，システムから入力を求められる 1 個の単語を筆記して入力する．この単語の条件は，3.2.3 項で述べたものと同様である．入力された筆記は，3.2.3 項で述べたものと同様の手順で，筆記の特徴抽出が行われる．利用者が入力した 1 個の単語の筆記に対して，線形補間してから切り出されたすべてのサンプルは，3.2.2 項の訓練済みモデルに入力される．この訓練済みモデルを使った分類により，1 個の単語の筆記から作成された大量のサンプルに対して，ソフトマックス値が高かった上位 b 個のサンプルが個人識別のテストに使用される．

前述の b 個のサンプルは，3.2.4 項で述べた，その ID に基づく利用者の筆記の特徴の訓練済みモデルに入力される．k 値分類の結果，最も多くのサンプルがその ID に分類されなかった場合には，個人識別に失敗となる．最も多くのサンプルがその ID に分類された場合には，さらに F 値による閾値の判定が行われる．この F 値が事前に設定された閾値を上回れば個人識別に成功とし，閾値以下であれば失敗となる．

F 値の算出方法は次のとおりである．まず，b 個のサンプルの分類結果を，TP（True Positive），FP（False Positive），TN（True Negative），FN（False Negative）に分ける．そして，これらから式 (2)，(3)，(4) の手順で F 値（F-score）を求める．この閾値は，FAR（False Acceptance Rate）と FRR（False Rejection Rate）を考慮し，システム側もしくは利用者側で任意に設定可能である．この閾値は利用者ごとに異なってよい．

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F\text{-}score = \frac{2Recall * Precision}{Recall + Precision} \quad (4)$$

4. 実装

4.1 実装環境

本節では，実装に使用した言語やドライバとそのバージョンについて記述する．Leap Motion のデータは Leap Motion API [36]（version 2.3）を使用して取得した．プログラミング言語に関しては，データの取得には C# 7.0，機械学習には Python 3.7.5 を使用した．また，Python の機械学習用ライブラリとして，Chainer（version 6.3.0）を使用した．データの取得を行った PC の OS は Windows 10 Education，機械学習を実行した PC の OS は Ubuntu 16.04.3 LTS である．機械学習を実行した PC には NVIDIA GeForce GTX 1060 が搭載されており，機械学習において可能な限りビデオカード上での演算を優先した．

4.2 筆記のための実装

3.2.2 項で述べた筆記の分解，3.2.3 項で述べた筆記の特徴抽出，3.3 節で述べた個人識別フェーズのために，**図 3** に示すとおり物理的な環境を構築した．使用したディスプレイは 20 インチの Dell 2007FPb（UXGA）であり，モニタの上下および左右の中心から 1.5 cm の位置に竹串（直径 2 mm）をセロハンテープで固定し，画面から 2 cm の距離に，垂直または水平になるよう，竹串どうしをつなぐ糸を張った．つまり，画面の中心に，糸で囲まれた 3 cm 四方の四角形ができる．この四角形の真下に Leap Motion の中心がくるように，Leap Motion を配置した．Leap Motion は，アルミ製のヒートシンクを用いて机のテーブル面から 2 cm 浮かせて固定しており，机のテーブル面から，水平に張られた一番下の糸までの距離は 17 cm である．2 cm 浮かせた理由はディスプレイ下に取り付けた竹串が Leap Motion のカメラに映らないようにするためである．机の高さは，一般的な事務机の 70 cm である．Leap Motion は画面から 5 cm 離れた位置に固定した．これは，Z 軸（奥行き）方向にも指を動かせるようにするためと，近すぎるとディスプレイから発せられる熱により赤外線の受光が妨害されるためである．ディスプレイを用いたのは，筆記時の特徴を抽出するための実験時に，指がきちんと Leap Motion に認識されているかどうか，被験者がその場で確認できたほうがよいと考えたためである．Leap Motion の有効範囲は X，Y，Z 方向すべてにおいて 2.5 cm から 60 cm となっており，本実装の環境はこの有効範囲内に収まっている．

図 3 筆記の分解のためのデータ取得環境
Fig. 3 Environment for data acquisition of disassembling scripts.

3.2.2 項で述べた，筆記の分解のための訓練用に被験者が筆記を行う際，糸で囲まれた 3 cm 四方の四角形の中で筆記を行う．これは，各被験者が任意の位置に任意の距離の直線を自由に描いてしまい，直線の特徴がうまくとれなくなってしまうことを防ぐためである．たとえば，左から右の直線を筆記する場合には，最初に画面中央を人差し指が指すようにして手を Leap Motion の上にかざして指を認識させ，四角形の左辺の左側に人差し指がくるように手を移動する．そこから，四角形の右辺の右側に人差し指がくるまで指を移動させ，手を Leap Motion の範囲外に移動して 1 回の筆記を入力させる．このとき，機械学習に使用されるデータは，四角形の範囲内に人差し指の座標があるものだけとなる．同様に，右から左，上から下，下から上の直線も四角形の範囲内に人差し指の座標があるものだけが，機械学習に使用されるデータとなる．

3.2.3 項で述べた筆記の特徴抽出，3.3 節で述べた個人識別フェーズのために被験者が単語を入力する際には，糸は関係なく，ディスプレイの手前を広く使って筆記する．

4.3 機械学習の実装

Yamamoto らの研究 [27] を参考にし，畳み込みニューラルネットワーク（CNN：Convolutional Neural Network）を Chainer を用いて実装を行った．ネットワークの構造については，Yamamoto らの研究をそのまま模倣したものと，Yamamoto らの研究のものに Ioffe らの理論 [37] を取り入れて改善したものの 2 つを用いた．**図 4** に Yamamoto らのものを模倣したネットワークを，**図 5** に Ioffe らの理論を取り入れて改善したネットワークを示す．

まず，図 4 に示したネットワークから説明する．機械学習に用いたパラメータは，Yamamoto らのものと同様とした．ただし，ネットワークの入力ユニット数と出力ユニット数は，我々が取得したサンプル数および我々の研究の出力による都合があるため，この限りではない．k-size は 2，padding は 0，入力するサンプルは 2 次元配列であり，チャネル数は 1 である．活性化関数は ReLU を，最適化関数は Adam を用いた．プーリング層には最大プーリングを用い，ウィンドウサイズは 1 である．全結合層の入力ユニット数

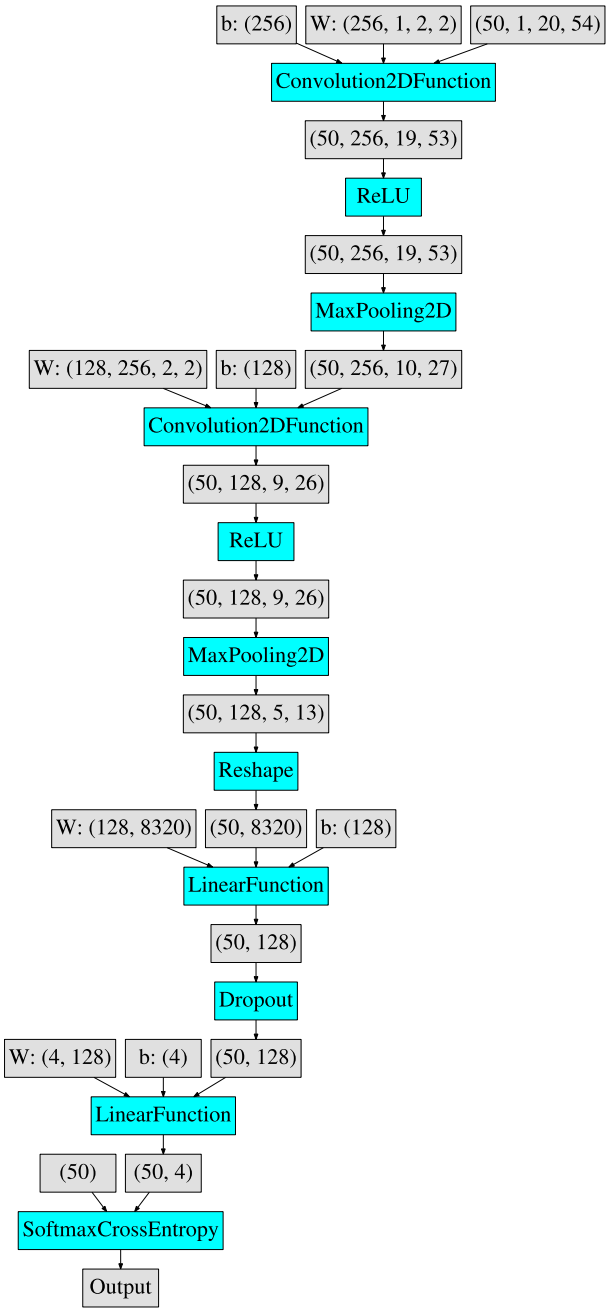

図 4 機械学習のネットワークにおける層構造
Fig. 4 Construction of layers for machine learning network.

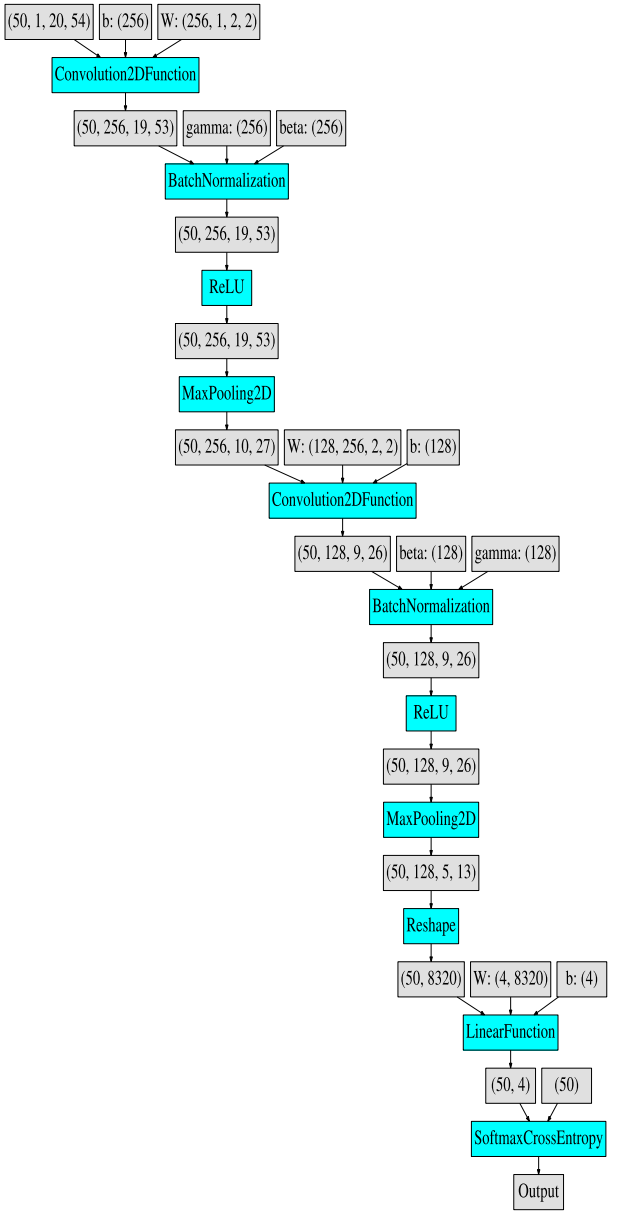

図 5 機械学習のネットワークにおける層構造 2
Fig. 5 Construction of layers for machine learning network 2.

は，直前のプーリング層の出力ユニット数から Chainer が自動的に決定し，中間層の場合には 128 である．Dropout の確率は 50%である．

一方，Yamamoto らのものと異なり，出力層のユニット数は，筆記分解ならば 4 方向の 4，個人識別の場合は訓練に使用するサンプルの被験者数である．

エポック数については上限を 1,000 とし，Early stopping を用いて訓練中に validation/loss が 3 エポックの間下がらなかった場合に訓練を終了するようにした．これは，過学習防止のためと，訓練時間短縮のためである．

バッチサイズに関しては Yamamoto らの論文に記述がなかったため，Kritsis らの，Leap Motion の座標データを CNN に入力してジェスチャを判別する研究 [38] を参考にし，これと同様の 50 とした．

次に，Ioffe らの理論を加えて改善したネットワークについて説明する．Yamamoto らのネットワークでは，全結合層の間で Dropout を利用しているが，Ioffe らによると，そこから全結合層を 1 つ減らし，さらに Dropout を削除し，代わりに畳み込み層の終わりに Batch Normalization を追加することで Dropout のみで訓練したときより過学習を抑えることができるとのことなので，我々もそれに従った．なお，Dropout は Dropout 率のパラメータを設定する必要があるが，Batch Normalization は手動で設定する必要のあるパラメータが存在しないため，パラメータ設定の手間が減るという利点もある．さらに，全結合層間の Dropout が存在しなくなったことにより，訓練速度の向上も見込める．

評価においては，まずこれら 2 つのネットワークを数値で比較し，良いほうを用いた．

訓練およびテストに使用するサンプルの割合に関しては，Yamamoto らの研究のとおりとした．サンプル数が少ない場合には，k-分割交差検証を行うこともあるが，本研究のサンプル数は評価に十分であると判断し，Yamamoto らの研究に合わせた．

5. 評価

本章では，3 章で述べた提案システムの妥当性について評価を行う．

スペースの都合により，本章の表中では，方向を Dir，右から左を R-L，上から下を U-D，左から右を L-R，下から上を D-U，平均を Ave，標準偏差を Std と表記し，平均値の項目においては，平均値の右に括弧書きで標準偏差の値を記すものとする．

5.1 筆記の分解についての評価

本節では，3.2.2 項で述べた筆記の分解についての評価を行う．筆記を分解するための筆記の情報は，システムの利用者とは別に集められた筆記の分解専用の被験者によって入力されることを説明した．よって，評価の手順としては，筆記の分解専用の被験者によって入力された筆記の情報が，機械学習により適切に訓練および検証が行われているのかの評価を行い，適切に訓練済みモデルが作成された場合には，そのモデルによって利用者の筆記が適切に分解されるのかテストの評価を行うことになる．

利用者の筆記が適切に分解されるのかのテストについては，3.2.3 項で述べたように，テスト結果の値が良いか悪いかに関係なく，ソフトマックス値が高かった上位 b 個のサンプルが筆記の特徴の訓練に使用されることとなる．つまり，最終的に利用者が個人識別される精度を評価するまで，利用者の筆記が適切に分解されたかどうかは判断できないため，この部分の評価は本節ではなく次節以降で行うものとする．よって，本節では，筆記の分解専用の被験者によって入力された筆記の情報が，機械学習により適切に訓練および検証が行われているかのみ評価を行う．

本節で行う筆記の分解専用の被験者として，10 人の被験者を用意した．これら 10 人の被験者は，当研究室所属の学生である．これら 10 人の被験者が，4.2 節の環境で 4 つの向きの直線をそれぞれ 150 回入力した．

なお，実験を行う中で，センサの不具合により方向を入力し終えても記録が止まらず記録し続けることがあった．実験を観察していると，すべての被験者による 1 回の入力は，長く見積もっても 1 秒も掛かっていなかった．そこで，フレーム数が 200 を超えたデータは，センサの不具合と見なして破棄した．これは，Leap Motion が 1 秒間に 200 フレームの取得を行うためである．4.3 節で述べた Yamamoto らの研究に合わせ，各被験者における 1/3 を検証用サンプル，1/3 を訓練用サンプル，残りをテスト用サンプルとした．前述の破棄があるため，その分サンプルが減っている．

表 1 Yamamoto らのネットワークと Ioffe らの理論に基づき改良されたネットワークの比較
Table 1 Comparison of network by Yamamoto et al. with improved one by Ioffe et al.

ネットワーク	Accuracy	Loss
Yamamoto らの手法版	0.962(0.059)	0.256(0.126)
Ioffe らによる改良版	0.996(0.003)	0.031(0.023)

表 2 筆記を分解するための訓練の評価結果
Table 2 Evaluation results of disassembling of writing.

Dir	Precision	Recall	F-score
R-L	0.996(0.002)	0.996(0.004)	0.996(0.002)
U-D	0.994(0.004)	0.996(0.002)	0.995(0.003)
L-R	0.998(0.001)	0.998(0.002)	0.998(0.001)
D-U	0.998(0.002)	0.998(0.002)	0.998(0.001)
Ave	0.997(0.002)	0.997(0.001)	0.997(0.001)

被験者から筆記を取得した結果，3.2.2 項で述べた平均フレーム数は 20.206 となった．そこで，小数点を切り捨て，本システムで筆記の分解に利用するサンプルの平均フレーム数は 20 とした．

訓練および検証は以下のとおりに行われた．訓練用サンプル全体からランダムで 180 個を選択し訓練を行い，すべての検証用サンプルで検証を行うという手順を 10 回繰り返した．この訓練および検証を，4.3 節で述べた 2 つのネットワークを用いてそれぞれ行った．ハイパーパラメータは 4.3 節のとおりである．出力層のユニット数は 4 つの向きのため 4 である．入力層のユニット数 180 は，Chainer が自動決定したものである．

Validation accuracy および loss の平均値と標準偏差を**表 1** に示す．

表 1 より，Ioffe らの理論による改良を加えたもののほうが，精度が高く標準偏差も小さかった．よって，本論文の評価においては，これ以降，すべて改良版のネットワークを用いて評価を行っている．

改良版のネットワークにおける Precision，Recall，F 値の平均値および標準偏差を**表 2** に示す．表 2 より，4 つの向きすべてで F 値が 0.995 以上となり，標準偏差は最大でも 0.003 となっている．これが，筆記の分解専用の被験者を用いて作成された訓練済みモデルであり，この 10 個のうち一番値が良かったものを以降の評価に使用した．

5.2 筆記の特徴抽出についての評価

3.2.3 項で述べた，利用者からの筆記の特徴抽出について評価を行った．利用者として，当研究室所属の学生から 11

表 3 サンプル数別の全被験者の FRR の平均と標準偏差
Table 3 FRR average and standard deviation of all subjects by number of samples.

数	90	150	300	600	900	1,500	3,000	6,000
Ave	0.63	0.62	0.6	0.56	0.49	0.43	0.41	0.39
Std	0.13	0.18	0.21	0.2	0.21	0.2	0.23	0.24
計	0.76	0.8	0.81	0.76	0.7	0.63	0.64	0.63

人の被験者を用意した．なお，これらの被験者は，5.1 節における筆記の分解専用の被験者とは完全に別人である．

本節の評価における環境には図 3 と同じものを使用したが，被験者は糸を無視して筆記を行っている．筆記開始位置は画面の中央とした．入力する単語は，インターネット上のパブリックドメインの辞書 [39] に掲載されている 65,600 件の英単語から，ランダムで選択した．なお，データ量が少なくなることを危惧し，3 文字以上の単語のみが選択されるようにした．被験者が筆記する文字は，被験者全員が十分に慣れているブロック体である．各被験者が異なる 100 単語をそれぞれ入力した．なお，被験者間で同一単語が選択される可能性はある．

まず，3.2.3 項で，ソフトマックス値が高かった上位 b 個のみを筆記の特徴の訓練に使用すると述べた点について評価を行った．本システムでは，b は数十～数千と想定している．そこで，b を 90，150，300，600，900，1,500，3,000，6,000 として評価を行った．これは，1/3 を検証用サンプル，残りを訓練用サンプルとする都合上，割り切れる値で切りの良い値を選んだことによる．

11 人の被験者の 1 人 1 単語を学習したモデルに登録者の学習していない単語 99 個を検証し，1 単語のサンプル b 個が TP として分類された数が一番多い場合を本人とするとし，本人確認に失敗した確率（FRR）からサンプル数別の FRR を求めた．その平均値と標準偏差を**表 3** に示す．

表 3 より，単純に FRR の平均値が最も低いものは，サンプル数が 6,000 のときのものである．しかし，この実験の被験者は 10 人しかおらず，サービスの提供を受けるユーザ数が非常に多くなる場合には，そのばらつきも考慮する必要がある．そこで，平均値に標準偏差を足した値を，最悪のケースにおける平均値と考え，その値が最も小さくなる 1,500 を以降の実験で使用することにした．なお，平均値に標準偏差を足した値でも，サンプル数 1,500 と 6,000 との差がないが，サンプル数が少ないほうが訓練時間が短くなり，より適切であるといえる．

5.3 筆記の特徴の訓練についての評価

3.2.4 項で述べた，筆記の特徴の訓練における評価を行った．利用者としての被験者は，5.2 節における評価と同一人物の 11 人である．3.2.4 項のとおりとすると，1 利用者あたり a 個の筆記 × b 個のサンプルを，k 値分類して評価を行うこととなる．まず，本システムとして a は 10 程度を想定しているため 10 とした．b については，5.2 節の評価結果から，1,500 が最適であるため 1,500 とした．そして，k であるが，被験者 11 人に対して，次節で行う評価の都合上 10 としている．11 人から 10 人を選択する方法については以下に記す．

表 4 筆記時の特徴の訓練の検証結果
Table 4 Validation results of training of features on scripting.

被験者	Precision	Recall	F-score
A	0.981(0.017)	0.961(0.036)	0.971(0.026)
B	0.979(0.024)	0.962(0.025)	0.970(0.016)
C	0.974(0.032)	0.988(0.024)	0.981(0.017)
D	0.969(0.023)	0.986(0.012)	0.977(0.013)
E	0.994(0.013)	0.974(0.025)	0.984(0.013)
F	0.989(0.023)	0.966(0.040)	0.977(0.031)
G	0.966(0.027)	0.987(0.012)	0.976(0.014)
H	0.961(0.027)	0.973(0.034)	0.966(0.025)
I	0.987(0.011)	0.986(0.011)	0.986(0.008)
J	0.960(0.028)	0.980(0.017)	0.970(0.019)
K	0.965(0.032)	0.970(0.031)	0.967(0.024)
Ave	0.975(0.023)	0.976(0.024)	0.975(0.019)

訓練および検証を次のとおり行った．訓練用サンプル作成のための単語は，1 回の訓練ごとに 5.2 節の評価で被験者が入力した単語の中から，被験者ごとに 10 個ずつ選択している．被験者ごとに入力した 100 単語のうち，訓練用サンプル作成に使用されなかった残りの 90 単語が検証用サンプル作成のために使用される．10 人の被験者による評価は，次のように被験者を選択して行った．被験者に A～K と仮の識別名を付ける．被験者 A の評価は，被験者 B～K のうちいずれか 1 人を除いた 9 人と被験者 A で行う．10 回の評価のうち，被験者 B～K は均等に 1 回ずつ除かれるようにした．被験者 B の評価は，被験者 A および C～K のうちいずれか 1 人を除いた 9 人と被験者 B で行い，以下は同様である．被験者 C～K も同様である．この訓練の検証結果を**表 4** に示す．表 4 より，すべての被験者において F 値の平均が 0.966 以上となり，その標準偏差は最大でも 0.025 であった．

5.4 個人識別の評価

3.3 節で述べた，個人識別の評価を行った．利用者としての被験者は，5.2 節における評価と同一人物の 11 人である．

まず，利用者本人がその利用者として分類されるかどうかの評価を行った．仕様が 3.3 節のとおりとすると，k 値分類における k 人のうちの 1 人が利用者本人，残りの 9 人がシステム側で用意した被験者ということになるが，訓練および検証は 5.3 節のものをそのまま利用し，たとえば被験者 A を本人とした場合，被験者 B～K のうちの 9 人が

表 5 利用者本人における個人識別の混同行列
Table 5 Confusion matrix of personal identification by registered users.

	A	B	C	D	E	F	G	H	I	J	K
A	80.9 (9.2)	8 (7.7)	0.1 (0.3)	1.2 (2.1)	0 (0)	0 (0)	0.6 (0.7)	0 (0)	0.1 (0.3)	0 (0)	0.1 (0.3)
B	1 (2.2)	86.7 (2.9)	0 (0)	0.4 (0.7)	1.1 (0.9)	0.6 (0.7)	0.2 (0.4)	0.1 (0.3)	0 (0)	0 (0)	0.2 (0.4)
C	0 (0)	0 (0)	87.6 (2.6)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	2.7 (2.6)
D	0.6 (0.7)	2 (1.5)	0 (0)	86.3 (1.6)	0.7 (0.5)	0.1 (0.3)	0.4 (0.7)	0 (0)	0 (0)	0 (0)	0.3 (0.5)
E	0 (0)	0 (0)	0 (0)	0 (0)	90 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
F	0 (0)	0 (0)	0 (0)	0 (0)	1.6 (1.4)	88.1 (1.6)	0 (0)	0 (0)	0 (0)	0 (0)	0.6 (1.1)
G	1.3 (1.9)	1.6 (0.8)	3.4 (1.8)	0.9 (1.3)	0 (0)	0.1 (0.3)	80.3 (4.9)	0.1 (0.3)	0 (0)	1.9 (2.8)	1.4 (1.6)
H	0 (0)	0.3 (0.5)	0 (0)	0 (0)	0.4 (1)	0 (0)	0 (0)	88.6 (1.1)	0.1 (0.3)	0.2 (0.4)	0.4 (0.5)
I	0.6 (0.7)	0.2 (0.4)	0 (0)	1.2 (1.3)	1.1 (1.5)	0.4 (0.7)	0 (0)	1.1 (0.7)	83.9 (1.9)	2.1 (1.4)	0 (0)
J	0.1 (0.3)	0.3 (0.5)	0.1 (0.3)	0.8 (0.8)	0 (0)	0 (0)	4.2 (2.9)	0.4 (0.5)	0.7 (0.8)	84 (3.7)	0 (0)
K	0.4 (0.8)	0.9 (1)	2 (1.8)	0.7 (1.2)	0.7 (0.7)	0.6 (0.8)	0.6 (0.7)	0.4 (0.7)	0 (0)	0.1 (0.3)	84.3 (3.9)

システム側で用意した被験者となるように評価した．つまり，被験者 B を本人とすると，その他の 9 人がシステム側で用意した被験者となり，被験者 C 以降も同様である．1 被験者 100 単語のうち 10 単語を訓練，検証用にし，残りの 90 単語をテスト用とする．結果を混同行列として**表 5** に示す．縦軸の A〜K が単語の入力を行った利用者であり，横軸がその単語が誰に分類されたかを表す．値は，単語数の 10 回の平均値と標準偏差である．

表 5 においては，たとえば被験者 A が A として分類されても，F 値が閾値を超えない限り個人識別は成功しない．閾値を 0.1 から 0.9 の間とした際に，利用者本人に分類された単語のうち，閾値を超えた単語数の平均値と標準偏差を**表 6** に示す．90 単語のうち，この閾値を超えた単語数の割合が 1 − FRR の値となる．FRR の平均値と標準偏差も表 6 に示す．

次に，攻撃者が利用者として分類されるかどうかの評価を行った．仕様が 3.3 節のとおりとすると，k 値分類における k 人のうちの 1 人が利用者本人，残りの 9 人がシステム側で用意した被験者ということになり，攻撃者は当然これ以外の人物となる．内部犯がおり，システム側で用意した被験者が攻撃者となる可能性もあるが，通常は信頼の置ける人物を選別するため，本評価においてはこれを考慮しないものとする．訓練および検証は 5.3 節のものをそのまま利用し，たとえば被験者 A を本人とした場合，被験者 B〜K のうちの 9 人がシステム側で用意した被験者となるように評価した．そして，被験者 B〜K のうちの残り 1 人が攻撃者となるようにした．このようにすることで，被験者 11 人を使って，攻撃者が 11 人いる場合の評価を行える．攻撃者の単語は当然システムに訓練していないため，攻撃者の 100 単語すべてをテストとして使用する．なお攻撃者は本人ではないため攻撃に成功したものは FP となるが，ここでは TP として計算する．結果を混同行列として**表 7** に示す．縦軸の A〜K が単語の入力を行った攻撃者であり，横軸がその単語が誰に分類されたかを表す．値は，単語数の 10 回の平均値と標準偏差である．

表 7 においては，たとえば攻撃者が A に分類されても，F 値が閾値を超えない限り個人識別は成功しない．閾値を 0.1 から 0.9 の間とした際に，攻撃者が誰かに分類された単語のうち，閾値を超えた単語数の平均値と標準偏差と FAR の平均値と標準偏差を**表 8** に示す．縦軸の A〜K が単語の入力を行った攻撃者であり，横軸が閾値を表す．

100 単語のうち，ある利用者に分類され，さらにこの閾値を超えた単語数の割合が FAR の値となる．

6. 考察

6.1 安全性に関する考察

提案システムは，パスワードによる個人識別を補助的に強化するために用いるため，1 回の個人識別フェーズにおいて 1 単語のみを入力する仕様としているが，入力に掛かる時間を考慮しなければ，筆記を比較して個人識別を行う研究には畠中らのもの [18]，Xiao らのもの [22]，Behera らのもの [26]，Yamamoto らのもの [27] が存在する．

関連研究の FAR と FRR を見ると，畠中らのものが FAR が 0 のとき FRR が 6.2%と関連研究の中で一番良い結果となっている．一方，5 章で行った提案システムの評価では FAR を 0 にすることはできなかったが，閾値を変更するこ

表 6 閾値ごとの利用者本人が本人確認に成功した単語数と FRR
Table 6 Number of words in successful personal identification by registered users and FRR on each threshold.

	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
A	80.9 (9.181)	80.9 (9.181)	80.9 (9.181)	80.8 (9.119)	80.6 (8.969)	79.8 (9.009)	77.3 (10.169)	72.8 (11.609)	60.4 (13.109)
B	86.7 (2.934)	86.7 (2.934)	86.7 (2.934)	86.7 (2.934)	86.2 (3.682)	83.7 (6.165)	77.9 (10.232)	66.2 (17.787)	42.5 (18.035)
C	87.6 (2.615)	87.6 (2.615)	87.6 (2.615)	87.6 (2.615)	87.6 (2.615)	87.2 (2.786)	85.4 (3.852)	80 (6.496)	62.5 (13.208)
D	86.3 (1.552)	86.3 (1.552)	86.3 (1.552)	86.3 (1.552)	86.2 (1.47)	85.5 (1.432)	81 (4.29)	68 (9.92)	41.7 (10.374)
E	90 (0)	90 (0)	90 (0)	90 (0)	90 (0)	90 (0)	90 (0)	88.4 (2.332)	80.1 (9.638)
F	88.1 (1.64)	88.1 (1.64)	88.1 (1.64)	88.1 (1.64)	88.1 (1.64)	88.1 (1.64)	87.8 (1.939)	86.7 (2.865)	83.1 (3.7)
G	80.3 (4.9)	80.3 (4.9)	80.3 (4.9)	80.2 (4.792)	79.7 (5.021)	77.2 (6.013)	68.8 (8.183)	54.7 (11.765)	27.9 (11.22)
H	88.6 (1.114)	88.6 (1.114)	88.6 (1.114)	88.6 (1.114)	88.3 (1.187)	86.7 (1.345)	84.2 (2.561)	78 (3.873)	62 (8.764)
I	83.9 (1.868)	83.9 (1.868)	83.9 (1.868)	83.9 (1.868)	83.8 (1.887)	83.2 (2.088)	81.4 (2.375)	78.5 (3.324)	64.1 (6.963)
J	84 (3.688)	84 (3.688)	84 (3.688)	84 (3.688)	83.6 (4.03)	80.3 (5.934)	72.1 (9.679)	53.8 (15.419)	22.9 (13.946)
K	84.3 (3.926)	84.3 (3.926)	84.3 (3.926)	84.3 (3.926)	83.6 (4.104)	82.1 (4.763)	76.1 (6.862)	60.7 (11.942)	34.7 (12.009)
AVE	85.518 (3.038)	85.518 (3.038)	85.518 (3.038)	85.5 (3.023)	85.245 (3.146)	83.982 (3.743)	80.182 (5.467)	71.618 (8.848)	52.9 (10.997)
FRR	0.05 (0.034)	0.05 (0.034)	0.05 (0.034)	0.05 (0.034)	0.053 (0.035)	0.067 (0.042)	0.109 (0.061)	0.204 (0.098)	0.412 (0.122)

表 7 攻撃者における個人識別の混同行列
Table 7 Confusion matrix of personal identification by attackers.

	A	B	C	D	E	F	G	H	I	J	K
A	9.9 (18.3)	13 (14.9)	6.3 (15.3)	5.9 (7.5)	18.7 (34.3)	2.9 (5.2)	24.4 (29.8)	12.4 (30.4)	2.3 (3.2)	7.4 (17.2)	6.7 (8.6)
B	7.7 (18)	14.2 (14.6)	6.3 (15.3)	4.1 (6.5)	18.4 (34.4)	2.7 (5.2)	26.8 (30.4)	12.4 (30.4)	4.8 (9)	7.4 (17.2)	4.7 (7.7)
C	11 (19)	15.8 (14.6)	5.7 (14.6)	5.9 (7.5)	18.7 (34.3)	2.9 (5.2)	21.1 (25.4)	12.4 (30.4)	5.6 (8.8)	7.1 (17.3)	4.3 (7.1)
D	11 (19)	10.9 (11.3)	6.3 (15.3)	5.4 (7.3)	18.6 (34.4)	2.9 (5.2)	23.7 (29.2)	12.4 (30.4)	5.6 (8.8)	7.2 (17.3)	6.6 (8.6)
E	11 (19)	15.8 (14.6)	6.3 (15.3)	6 (7.5)	16.8 (33)	2.7 (5.2)	29.3 (29)	1.6 (2.9)	5.6 (8.8)	7.6 (17.2)	6.7 (8.6)
F	11 (19)	15.4 (14.9)	6.3 (15.3)	6 (7.5)	8.2 (21.9)	2.6 (5)	29.3 (29)	12.4 (30.4)	5.4 (8.9)	7.6 (17.2)	6.4 (8.7)
G	10.6 (19.2)	12.6 (14.5)	5.4 (15.4)	5.7 (7.7)	18.7 (34.3)	2.9 (5.2)	26.4 (28.9)	12.4 (30.4)	5.6 (8.8)	1.3 (1.5)	6.7 (8.6)
H	11 (19)	15.7 (14.7)	6.3 (15.3)	5.9 (7.5)	10.9 (29.4)	2.8 (5.2)	29.1 (29.2)	11.2 (29.1)	4.7 (8.9)	7.6 (17.2)	4.8 (7.9)
I	4.6 (9.3)	13.4 (15.2)	6.3 (15.3)	5.4 (7.7)	18.7 (34.3)	2.4 (5.2)	29.3 (29)	11.6 (30.6)	5 (8.5)	7.2 (17.3)	6.6 (8.6)
J	10.2 (19.3)	15.6 (14.8)	6.3 (15.3)	3.6 (5)	18.7 (34.3)	2.9 (5.2)	21.7 (26.5)	12.4 (30.4)	5.6 (8.8)	6.8 (16.5)	6.7 (8.6)
K	11 (19)	13.9 (15.4)	0.9 (2.5)	5.6 (7.7)	18.6 (34.4)	1 (1.3)	29.2 (29.1)	11.8 (30.6)	5 (9)	7.6 (17.2)	6 (8.4)

とにより FAR と FRR のバランスを変えることができる．この閾値は登録者ごとに設定可能であるため，表 6 および表 8 より，たとえば閾値を 0.5 にすれば FRR が 0.053 で FAR が 0.099 となるし，閾値を 0.7 にすれば FRR が 0.109 であるが FAR を 0.045 にできる．

もちろん，畠中らの研究のように覗き見耐性に関する評価は行っていない．提案システムは，パスワードによる個人識別を補助的に強化するために使用することを目的としており，いかなる覗き見も可能であるとすると，そもそも入力しているパスワード自体も覗き見られていることにな

表 8 閾値ごとの攻撃者が本人確認に成功した単語数と FAR
Table 8 Number of words in successful personal identification by attackers and FAR on each threshold.

	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
A	9.9 (18.3)	9.9 (18.3)	9.9 (18.3)	9.6 (17.665)	7.4 (13.514)	3.5 (7.018)	0.7 (1.487)	0.1 (0.3)	0 (0)
B	14.2 (14.593)	14.2 (14.593)	14.2 (14.593)	14.1 (14.577)	12.2 (14.091)	8.6 (10.92)	5.3 (7.836)	3.2 (5.724)	1.8 (4.02)
C	5.7 (14.629)	5.7 (14.629)	5.7 (14.629)	5.6 (14.333)	5.6 (14.333)	4.4 (11.065)	2.8 (7.454)	1.1 (2.982)	0.2 (0.6)
D	5.4 (7.31)	5.4 (7.31)	5.4 (7.31)	5.2 (7.346)	4 (6.325)	1.9 (3.081)	0.3 (0.458)	0.1 (0.3)	0 (0)
E	16.8 (33.045)	16.8 (33.045)	16.8 (33.045)	16.8 (33.045)	16.1 (31.785)	13.9 (28.282)	11.3 (23.929)	7.4 (16.415)	3.3 (7.772)
F	2.6 (4.964)	2.6 (4.964)	2.6 (4.964)	2.5 (4.985)	2.3 (4.734)	1.2 (2.04)	0.6 (0.917)	0 (0)	0 (0)
G	26.4 (28.876)	26.4 (28.876)	26.4 (28.876)	26.3 (28.89)	25 (28.566)	20.2 (25.325)	11.5 (15.416)	4.2 (7.026)	0.7 (1.269)
H	11.2 (29.068)	11.2 (29.068)	11.2 (29.068)	11.2 (29.068)	11.1 (29.081)	10.5 (29.207)	9.6 (27.807)	8.5 (25.168)	6.3 (18.569)
I	5 (8.544)	5 (8.544)	5 (8.544)	4.9 (8.526)	4.5 (8.535)	3.3 (7.308)	1.9 (4.085)	0.5 (0.922)	0.1 (0.3)
J	6.8 (16.461)	6.8 (16.461)	6.8 (16.461)	6.6 (16.524)	6.4 (16.572)	5.2 (14.945)	4.4 (12.87)	2.7 (8.1)	1 (3)
K	6 (8.367)	6 (8.367)	6 (8.367)	5.8 (8.292)	4.7 (7.029)	2.5 (4.696)	1.3 (2.452)	0.1 (0.3)	0 (0)
AVE	10 (16.742)	10 (16.742)	10 (16.742)	9.873 (16.659)	9.027 (15.87)	6.836 (13.081)	4.518 (9.519)	2.536 (6.112)	1.218 (3.23)
FAR	0.1 (0.167)	0.1 (0.167)	0.1 (0.167)	0.099 (0.167)	0.09 (0.159)	0.068 (0.131)	0.045 (0.095)	0.025 (0.061)	0.012 (0.032)

り危険である．利用環境としては，自宅などで背後から覗き見られないものを想定しており，公共の場においても，クレジットカードの PIN を入力したり，クレジットカードの署名をしたりする場合と同等程度の安全な環境であることを想定している．クレジットカードの PIN の場合，一度覗き見られてしまうと，同じ PIN を攻撃者に入力されてしまうが，提案システムにおいては，録画した映像の動きを真似る必要がある．クレジットカードの署名のように，書かれたものをそのままなぞって再現することもできない．さらに，入力を要求される単語が毎回異なるため，1 回から数回程度の覗き見には耐性がある．

提案システムの個人識別フェーズにおいては，利用者が入力する単語がシステムが要求したものでなくても，特徴が一致すれば個人識別に成功してしまう．これに関しては，Leap Motion で入力された数字を識別する Yamamoto らの研究や，タッチパネルの筆跡から文字を読み取る Hanyu ら [13] の研究があるため，Leap Motion で書かれた文字の軌跡を平面化することによって，入力した文字を識別し，要求された単語と異なる単語が入力された場合に，システム側で自動的に拒否することは可能であると考えられる．

6.2 本人拒否率に関する考察

提案システムは，パスワードによる個人識別を補助的に強化するために使用することを目的としているため，FRR が 0 でない限り，パスワードも正しく筆記も適切に行えたにもかかわらず，個人識別に失敗することが起きてしまう．5.4 節の評価では，表 6 より FRR は 0 とはならなかった．

被験者が入力した単語について調べてみたところ，極端にフレーム数が多いものと極端に少ないものが存在した．極端にフレーム数が多い単語というのは，各被験者の一番文字数が多い単語のフレーム数の平均に標準偏差を足した値を超えたフレーム数のものを示す．全被験者の一番長い単語のフレーム数を平均すると 1,106.818 となり，標準偏差は 395.695 となった．足し合わせて少数点を四捨五入した 1,503 を超えるフレーム数がある単語は極端にフレーム数が多いということになる．その結果極端にフレーム数が多い単語は 19 個となった．

次に極端に少ないフレーム数を求めるため全被験者の 3 文字の単語のフレームの長さの平均をとり，標準偏差を平均から引いた値より少ないフレーム長の単語の数を求めた．全被験者の 3 文字の単語を書いたときのフレームの長さは 329.339 となった．このときの標準偏差は 140.979 となった．そのため平均から標準偏差を引いた値は 188.36 となる．小数点以下を四捨五入し，188 となる．長さがこれ以下のフレームの単語が短すぎるとして数えた結果，56 単語が極端にフレームが少ないということになった．

これは，筆記が完了した際に終了したと認識されていなかったり，筆記途中であるのに終了したと認識されて

しまったりしたものであると推測される．この単語数の割合が 0.75%であり，これらが適切に除去されていれば，0.75%の FRR を改善させられる可能性がある．

6.3 検証に必要なデータサイズに関する考察

5.4 節における評価において，被験者 10 人分の訓練済みモデル（最適化情報含む）が約 3 MB であった．単純に計算すると，100 人の利用者がいれば約 30 MB，1 億人でも 30 TB であり，一般に販売されている PC のハードディスク容量が 4〜8 TB ほどであることを考慮すると，1 億人分の利用者情報がサーバに保存されていることに，実用上の不都合はないと思われる．

6.4 サンプル数に関する考察

5.2 節で 1 つの筆記から 90，150，300，600，900，1,500，3,000，6,000 のサンプルを抽出した．その結果，FAR，FRR の最良が 1,500 となったが，ほかのサンプル数の場合に 1,500 より悪かった理由について考察する．

90〜900 は単純にサンプル数が 1,500 と比べて少ないので，訓練で 1,500 のときより個人の特徴を抽出できなかったのだと考えられる．FAR，FRR 自体は 90，150，300，600，900 の順で改善していっている．

3,000 と 6,000 の FAR，FRR が 1,500 より悪い理由は，3.2 節で筆記の分解を行ったときに，ソフトマックスの高い，直線となっているサンプルを抽出しているが，1,500 ぐらいまでは直線になってるサンプルを集められるが，3,000，6,000 だと本来は捨てられるべき直線になっていないサンプルも集めてしまって，訓練時にノイズになってしまっていると考えられる．さらに 3,000 と 6,000 は訓練と検証に 1,500 サンプルの倍以上の時間がかかるため，実用性的にも 1,500 が最適であるといえる．

6.5 閾値に関する考察

5 章の評価では閾値を決定しなかったが，実際にシステムとして利用する場合は F 値をどれぐらいの閾値にするのが最適か考察する．**表 9** に攻撃者の F 値の平均値と標準偏差を示す．表 9 より全被験者の F 値の平均は 0.145 となる．そこに全被験者の F 値の標準偏差 0.166 を足すと 0.311 となる．攻撃者の F 値と標準偏差を考慮して 0.311 を閾値にした場合，FRR は 0.049 となるが，FAR が 0.1 となる．こうなってしまう理由は，表 9 より攻撃者の F 値の平均は低いが，場所によっては F 値が非常に高くなっている場所があり，そこが FAR を上げていると考えられる．たとえば攻撃者 E の登録者 H の部分は 0.892 で，標準偏差を考慮すると 1.0 に到達してしまうため，すべての攻撃者 E の単語は登録者 H として分類されているということになる．これによりどれだけ閾値を上げてもすべての攻撃者をはじくことはできないといえる．

攻撃者の平均や攻撃者の最大に合わせて閾値を設定すると FAR と FRR はどちらかは強固になり，その反対は非常に悪化する．そのため，実際のシステムで利用する場合は環境や利用者に合わせて閾値を設定するのが良いと考えら

表 9 攻撃者の F 値の平均と標準偏差
Table 9 Average and standard deviation of F-score of attackers.

攻撃者＼登録者	A	B	C	D	E	F	G	H	I	J	K
A		0.348 (0.31)	0 (0)	0.085 (0.1)	0.004 (0.01)	0.006 (0.022)	0.453 (0.265)	0.056 (0.073)	0.392 (0.26)	0.073 (0.099)	0.001 (0.01)
B	0.349 (0.17)		0.019 (0.05)	0.262 (0.192)	0.035 (0.108)	0.074 (0.117)	0.29 (0.188)	0.032 (0.048)	0.201 (0.156)	0.118 (0.122)	0.231 (0.191)
C	0.002 (0.008)	0.05 (0.056)		0.124 (0.13)	0 (0)	0 (0.001)	0.66 (0.177)	0.006 (0.021)	0.004 (0.019)	0.159 (0.183)	0.415 (0.185)
D	0.055 (0.08)	0.549 (0.192)	0.011 (0.04)		0.013 (0.102)	0.005 (0.023)	0.534 (0.189)	0.027 (0.052)	0.029 (0.056)	0.174 (0.155)	0.046 (0.084)
E	0.001 (0.01)	0.008 (0.025)	0 (0)	0 (0.004)		0.121 (0.166)	0 (0)	0.892 (0.117)	0.138 (0.131)	0.001 (0.004)	0.032 (0.054)
F	0.083 (0.1)	0.17 (0.15)	0 (0.002)	0 (0)	0.786 (0.159)		0.052 (0.09)	0.001 (0.005)	0.132 (0.16)	0 (0)	0.117 (0.151)
G	0.148 (0.156)	0.386 (0.213)	0.081 (0.196)	0.175 (0.161)	0.001 (0.006)	0.012 (0.07)		0.015 (0.032)	0.012 (0.031)	0.576 (0.271)	0.02 (0.045)
H	0.016 (0.037)	0.118 (0.113)	0.015 (0.038)	0.016 (0.062)	0.569 (0.25)	0.081 (0.093)	0.09 (0.119)		0.318 (0.167)	0.035 (0.071)	0.24 (0.196)
I	0.452 (0.19)	0.325 (0.196)	0.006 (0.021)	0.142 (0.136)	0.084 (0.093)	0.12 (0.16)	0.055 (0.076)	0.219 (0.182)		0.1 (0.147)	0.077 (0.102)
J	0.2 (0.17)	0.077 (0.096)	0.072 (0.104)	0.376 (0.176)	0 (0)	0.001 (0.006)	0.595 (0.162)	0.038 (0.072)	0.108 (0.117)		0.043 (0.075)
K	0.012 (0.027)	0.296 (0.179)	0.459 (0.279)	0.095 (0.12)	0.021 (0.096)	0.269 (0.212)	0.106 (0.125)	0.159 (0.158)	0.091 (0.167)	0.012 (0.032)	
Ave	0.132 (0.15)	0.233 (0.166)	0.066 (0.134)	0.127 (0.114)	0.151 (0.269)	0.069 (0.081)	0.284 (0.242)	0.144 (0.258)	0.143 (0.122)	0.125 (0.162)	0.122 (0.126)

表 10 登録単語数と本人拒否率と他人受入率の関係
Table 10 Relation of number of registered words with FRR and FAR.

単語数	FAR	FRR
1	0.054	0.456
2	0.042	0.285
3	0.053	0.19
4	0.059	0.166
5	0.056	0.146
6	0.059	0.129
7	0.054	0.106
8	0.058	0.099
9	0.052	0.084
10	0.068	0.067

れる．このシステム自体はパスワードなどを補助するものなので，強固にするか手軽に使えるようにするかは個人の自由となる．

6.6 登録単語数に関する考察

5 章の評価においては，筆記の特徴の訓練のために利用者が入力した単語数を仮に 10 と固定していた．本節では，何単語の入力が妥当であるかについて考察する．閾値は表 6，表 8 より FAR と FRR が最も近い閾値 0.6 とする．このとき FAR：0.068，FRR：0.067 となる．この閾値で単語数を変え，FAR と FRR がどれぐらい変化するのか考察する．入力する単語数と FRR と FAR を**表 10** に示す．

表 10 より，FAR は単語数 2 のときが一番小さいが，FRR は単語数 10 のときが一番小さい．よって，FAR，FRR 両方とも低い点から単語数 10 程度が妥当であるといえる．

単語数が増えていくほど FRR は改善していくが，FAR はあまり下がっていない．訓練する単語数を増やしているので本人の特徴は抽出しやすくなるが，存在しない人の特徴は訓練できないので FAR はあまり下がらないと考えられる．

6.7 登録者数に関する考察

評価では 11 人の被験者しかいないが，サービスとして使用する場合には，利用者は 1 千万人や 1 億人になる場合もある．そこで，5.4 節の結果から分布を求め，被験者の数が増えた場合に FAR と FRR がどの程度になるか推測する．

図 6 に登録者を検証したときの F 値の分布のグラフを示す．このグラフは，横軸に F 値の範囲をとった場合に，その範囲にどれだけの単語数が含まれているかを示したものである．

なお，図 6 の横軸は F 値の範囲であり，たとえば F 値が 0 のものは，実際には F 値が 0 以上 0.05 未満という意味である．F 値が 1 の場合を別扱いしたくなかったので，一番右の範囲のみ 0.95 以上 1 以下となるようにした．縦軸の右側は累積率となっている．

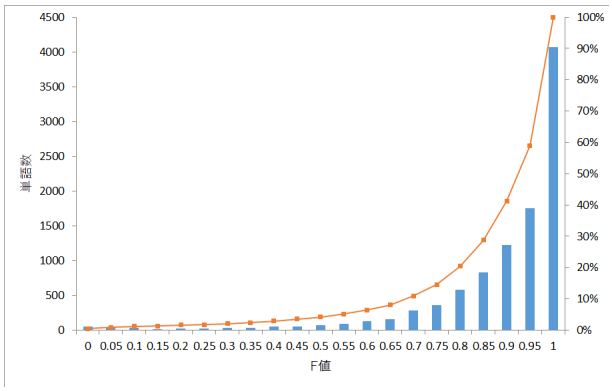

図 6 登録者を検証したときの F 値ごとの単語数の分布
Fig. 6 Distribution of words in range of F-score on verification of registered person.

表 11 登録者を検証したときの閾値ごとの累積率
Table 11 Cumulative rate for each threshold when verifying registrants.

閾値	累積率 [%]
0	0.505
0.2	1.596
0.4	2.96
0.6	6.475
0.8	20.424
1	100

表 12 攻撃者を検証したときの閾値ごとの累積率
Table 12 Cumulative rate per threshold when verifying attackers.

閾値	累積率 [%]
0	41.527
0.2	74.291
0.4	85.782
0.6	93.036
0.8	97.464
1	100

図 6 より，登録者を検証した結果の累積度分布は，なめらかな曲線を描いて上昇している．**表 11** に 0.2 刻みの閾値ごとの累積率を示す．

表 11 より閾値 0.2 の場合，評価で行った 11 人以上の多人数，たとえば 1 億人であれば，160 万人が平均 1 回は本人確認をやり直すことになる．閾値 0.8 で 1 億人の場合は，2,042 万人が平均 1 回は本人確認をやり直すことになり，その分検証するサーバに負荷がかかる．

図 7 に攻撃者を検証したときの F 値の分布のグラフを示す．**表 12** に 0.2 刻みの閾値ごとの累積率を示す．

表 12 の累積率は，攻撃者にとっての攻撃失敗率に相当する．閾値が 0.2 の場合には 74.3%の確率で失敗し，閾値が 0.8 であれば 97.5%の確率で失敗することになる．

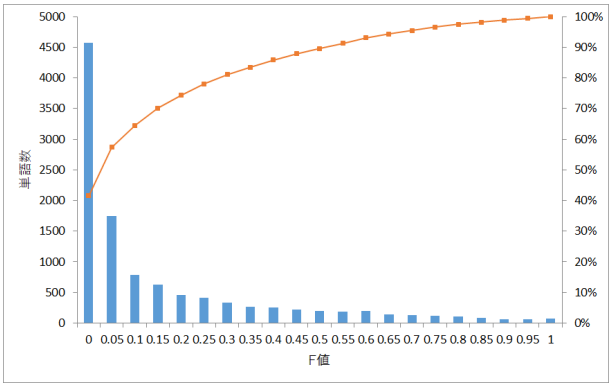

図 7 攻撃者を検証したときの F 値ごとの単語数の分布
Fig. 7 Distribution of words in range of F-score on verification of non-registered person.

もちろん，前述の考察は被験者 11 人のデータに基づいて行われたものであり，利用者が増えた場合にはこの 11 人のデータとは異なる特性を持つ者が現れる可能性は否定できない．たとえば，FRR，FAR ともに低くできない利用者が現れるかもしれない．本システムは，パスワードによる個人識別を強化するために補助的に使用されるものであるため，利用者の中で適用が困難な者は，利用を推奨しないという選択もある．

本評価においては，FRR が妥当な範囲で FAR が 0 にならなかったが，低い FAR は攻撃を防止するだけでなく，攻撃抑止にもつながると考えられる．たとえば，ホテルやレストランでの支払いのような公共の場所で利用する場合，暗証番号やパスワードを入手していたとしても，強引に本手法を突破するには相当な数の再筆記が必要となる．その間，係員や周囲の視線があることを考えれば，精神的なストレスはかなり大きいと推測される．

6.8 Recall に関する考察

5.4 節で F 値を閾値にした場合の本人，攻撃者の検証から FRR と FAR を求めた．しかし，F 値は Precision と Recall の調和平均である．検証を行う人は本人でも攻撃者でも 1 人しかいないため TN と FP は存在しない．つまり式 (2) より Precision はつねに 1 となる．そのため F 値より Recall を閾値にしたほうが，出力される数値がシャープになるため，FAR と FRR が改善する可能性がある．そこで表 6 と表 8 の結果を F 値ではなく，Recall を閾値に用いて求める．さらに表 9 についても Recall を用いて求める．その結果を**表 13**，**表 14**，**表 15** に示す．

まず，FRR である表 6 と表 13 を比較すると，0.3 までは F 値，Recall の差がなく，まったく同じに見えるが，0.4 から F 値，Recall の差が閾値に比例して大きくなっていて，F 値のほうが FRR が小さくなっている．閾値の数値は同じでも，F 値と Recall では計算式が違うので閾値 0.1 としても同じ 0.1 ではない．

次に FAR を比較する．表 8 と表 14 を比較すると，F 値，Recall ともに閾値 0.2 までは FAR が同じだが，閾値 0.3 から F 値，Recall の FAR に差が出てくるようになり，閾値に比例してその差も大きくなっている．FAR は Recall のほうが小さくなっている．

最後に表 9 と表 15 を比較する．Recall で数値を出したほうが全員の平均で 0.1 となり，F 値で数値を出したときの 0.145 より値が低くなっている．Recall を閾値にすることで全体的に数値が低くなったため，攻撃者や本人が本人として検証が通りにくくなると考えられる．

このような結果になった理由は Precision が関係していると考えられる．Precision はつねに 1 で，F 値を計算するときに分母に 1 足されるため，F 値は Recall より少し高くなる．高くなったことにより閾値を超えているかで本人か判定するときの判定が少し緩くなるため，FRR が下がると考えられる．逆に FAR が悪化するのも同様の理由だと考えられる．

このことより，FRR を下げたい場合は F 値を使用し，FAR を下げたい場合は Recall を使用するのが良いと考えられる．

6.9 筆記の特徴の訓練における被験者選択に関する考察

利用者の筆記の特徴を他の 9 人のものとともに訓練する際，この 9 人の特徴がどのようなものであるかによって FRR や FAR に差が出る．利用者と特徴が類似した者が加わると FRR が上がり，利用者と特徴が類似した者がいないと攻撃者による模倣が容易になり FAR が上がる．この特徴を利用し，この 9 人の候補に選ばれる可能性のある被験者のデータを用いて，提案手法の訓練済みモデルをあらかじめいくつか作成しておき，新規の利用者を攻撃者と仮定してこれらのモデルに情報を入力すれば，あるモデルの中で誰に分類されるかの偏りが分かる．この偏りを利用すれば，FRR と FAR のバランスを F 値（もしくは Recall）による閾値以外でも調整可能となる．つまり，利便性と安全性のどちらをより優先したいかを利用者が選択可能なパラメータが増える．

7. まとめ

本論文で提案した空中筆記による本人確認手法は，指紋などの身体的特徴を利用した生体認証と異なり，登録内容を変更可能な行動的特徴と本人の癖である身体的特徴の組合せを利用したものである．筆記時の手の動きそのものを機械学習で分類するのではなく，手の動きを分解して利用することで，再登録することなく入力する単語を変更できる点が特徴である．また，既存研究と異なり，大人数の利用者がいる場合や，利用者の増加がある場合でも，システムとして実用可能な設計となっている．なお，本評価における被験者数は少ないため，利用者数が極端に多い場合に，

表 13 閾値ごとの利用者本人が本人確認に成功した単語数と FRR（Recall）
Table 13 Number of words in successful personal identification by registered users and FRR on each threshold (Recall).

	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
A	80.9 (9.181)	80.9 (9.181)	80.7 (9.067)	79.9 (8.904)	78.8 (9.527)	75.1 (11.327)	71 (11.375)	62.3 (13.513)	45.3 (14.595)
B	86.7 (2.934)	86.7 (2.934)	86.6 (3.2)	84.3 (5.745)	80.9 (8.068)	73.2 (13.556)	63.4 (18.007)	45.8 (18.6)	25.5 (15.487)
C	87.6 (2.615)	87.6 (2.615)	87.6 (2.615)	87.6 (2.615)	86.4 (3.169)	83.9 (4.415)	77.4 (8.027)	65.3 (12.133)	46.3 (18.281)
D	86.3 (1.552)	86.3 (1.552)	86.3 (1.552)	85.9 (1.375)	83.1 (3.36)	77 (7.014)	63.4 (10.744)	45.5 (11.456)	20.9 (9.115)
E	90 (0)	90 (0)	90 (0)	90 (0)	90 (0)	89.6 (0.917)	87.5 (3.931)	81.1 (8.994)	68.7 (15.199)
F	88.1 (1.64)	88.1 (1.64)	88.1 (1.64)	88.1 (1.64)	88 (1.732)	87.4 (2.332)	86.5 (2.729)	84.2 (3.516)	76.3 (5.12)
G	80.3 (4.9)	80.3 (4.9)	80 (4.733)	78.5 (5.92)	72.7 (7.322)	63.3 (8.967)	49.7 (12.665)	30.7 (11.367)	13.2 (7.82)
H	88.6 (1.114)	88.6 (1.114)	88.3 (1.187)	87.5 (1.204)	85.5 (2.156)	81.3 (3.068)	75.3 (4.88)	64.9 (7.489)	45.5 (9.972)
I	83.9 (1.868)	83.9 (1.868)	83.9 (1.868)	83.4 (2.059)	82.3 (1.9)	80 (2.933)	77.1 (3.673)	67.1 (6.363)	47.3 (9.067)
J	84 (3.688)	84 (3.688)	83.7 (4.001)	81.7 (5.061)	75.8 (8.292)	65.3 (12.207)	46.8 (16.43)	26.3 (15.963)	10.8 (7.534)
K	84.3 (3.926)	84.3 (3.926)	84.1 (3.807)	82.7 (4.649)	78.6 (6.28)	70 (9.143)	55.8 (11.898)	38.9 (12.112)	18.1 (9.137)
AVE	85.518 (3.038)	85.518 (3.038)	85.391 (3.061)	84.509 (3.561)	82.009 (4.71)	76.918 (6.898)	68.536 (9.487)	55.645 (11.046)	37.991 (11.03)
FRR	0.05 (0.034)	0.05 (0.034)	0.051 (0.034)	0.061 (0.04)	0.089 (0.052)	0.145 (0.077)	0.238 (0.105)	0.382 (0.123)	0.578 (0.123)

表 14 閾値ごとの攻撃者が本人確認に成功した単語数と FAR（Recall）
Table 14 Number of words in successful personal identification by attackers and FAR on each threshold (Recall).

	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
A	9.9 (18.3)	9.8 (18.192)	8.5 (15.513)	4.6 (8.381)	1.5 (3.294)	0.4 (0.663)	0.1 (0.3)	0 (0)	0 (0)
B	14.2 (14.593)	14.2 (14.593)	13.1 (14.321)	9.6 (11.977)	6 (8.809)	3.9 (6.316)	2.9 (5.43)	1.9 (4.3)	0.8 (2.088)
C	5.7 (14.629)	5.7 (14.629)	5.6 (14.333)	4.8 (12.246)	3.3 (8.367)	2 (5.367)	1 (2.683)	0.4 (1.2)	0.1 (0.3)
D	5.4 (7.31)	5.4 (7.31)	4.7 (6.856)	2.7 (4.244)	0.8 (1.47)	0.2 (0.4)	0.1 (0.3)	0 (0)	0 (0)
E	16.8 (33.045)	16.8 (33.045)	16.4 (32.333)	15.1 (30.207)	12.2 (25.682)	9.5 (20.853)	6.9 (15.668)	3.4 (8.065)	1.9 (4.206)
F	2.6 (4.964)	2.6 (4.964)	2.3 (4.734)	1.5 (2.802)	0.9 (1.446)	0.4 (0.663)	0 (0)	0 (0)	0 (0)
G	26.4 (28.876)	26.4 (28.876)	25.9 (28.801)	22.8 (26.847)	14.6 (18.816)	7.4 (10.837)	2.8 (5.095)	0.9 (1.578)	0.2 (0.6)
H	11.2 (29.068)	11.2 (29.068)	11.1 (29.081)	10.7 (29.162)	9.8 (28.081)	9.3 (27.236)	8.2 (24.268)	6.6 (19.469)	4.6 (13.47)
I	5 (8.544)	5 (8.544)	4.8 (8.518)	3.7 (7.887)	2.2 (4.686)	1 (1.732)	0.2 (0.6)	0.1 (0.3)	0 (0)
J	6.8 (16.461)	6.8 (16.461)	6.4 (16.572)	5.4 (15.545)	4.7 (13.77)	3.8 (11.071)	2 (6)	1.2 (3.6)	0.3 (0.9)
K	6 (8.367)	6 (8.367)	4.9 (7.231)	2.9 (5.594)	1.8 (3.628)	0.3 (0.458)	0.1 (0.3)	0 (0)	0 (0)
AVE	10 (16.742)	9.991 (16.732)	9.427 (16.209)	7.618 (14.081)	5.255 (10.732)	3.473 (7.781)	2.209 (5.513)	1.318 (3.501)	0.718 (1.96)
FAR	0.1 (0.167)	0.1 (0.167)	0.094 (0.162)	0.076 (0.141)	0.053 (0.107)	0.035 (0.078)	0.022 (0.055)	0.013 (0.035)	0.007 (0.02)

表 15 攻撃者の Recall の平均と標準偏差
Table 15 Average and standard deviation of Recall of attackers.

攻撃者＼登録者	A	B	C	D	E	F	G	H	I	J	K
A		0.266 (0.298)	0 (0)	0.048 (0.065)	0.002 (0.005)	0.003 (0.012)	0.332 (0.227)	0.03 (0.041)	0.278 (0.211)	0.041 (0.059)	0.001 (0.005)
B	0.225 (0.133)		0.01 (0.028)	0.166 (0.137)	0.022 (0.07)	0.043 (0.072)	0.185 (0.136)	0.017 (0.026)	0.121 (0.11)	0.067 (0.076)	0.145 (0.135)
C	0.001 (0.004)	0.026 (0.031)		0.072 (0.083)	0 (0)	0 (0)	0.517 (0.185)	0.003 (0.011)	0.002 (0.01)	0.099 (0.125)	0.28 (0.152)
D	0.03 (0.047)	0.404 (0.194)	0.006 (0.022)		0.012 (0.1)	0.002 (0.012)	0.386 (0.17)	0.015 (0.029)	0.016 (0.031)	0.104 (0.099)	0.026 (0.05)
E	0.001 (0.005)	0.004 (0.014)	0 (0)	0 (0.002)		0.074 (0.117)	0 (0)	0.823 (0.164)	0.08 (0.082)	0 (0.002)	0.017 (0.03)
F	0.047 (0.06)	0.101 (0.098)	0 (0.001)	0 (0)	0.674 (0.2)		0.029 (0.053)	0 (0.003)	0.08 (0.108)	0 (0)	0.069 (0.095)
G	0.089 (0.111)	0.262 (0.174)	0.057 (0.151)	0.105 (0.108)	0.001 (0.003)	0.008 (0.048)		0.008 (0.017)	0.007 (0.017)	0.454 (0.267)	0.011 (0.025)
H	0.008 (0.02)	0.067 (0.067)	0.008 (0.021)	0.009 (0.039)	0.438 (0.239)	0.045 (0.054)	0.052 (0.078)		0.201 (0.126)	0.019 (0.041)	0.152 (0.145)
I	0.311 (0.152)	0.212 (0.153)	0.003 (0.011)	0.084 (0.101)	0.046 (0.055)	0.074 (0.116)	0.03 (0.043)	0.138 (0.144)		0.06 (0.094)	0.043 (0.062)
J	0.122 (0.117)	0.043 (0.063)	0.041 (0.062)	0.246 (0.136)	0 (0)	0 (0.003)	0.442 (0.161)	0.021 (0.046)	0.061 (0.072)		0.024 (0.046)
K	0.006 (0.014)	0.187 (0.131)	0.342 (0.247)	0.055 (0.077)	0.014 (0.077)	0.174 (0.155)	0.061 (0.079)	0.096 (0.109)	0.058 (0.121)	0.006 (0.017)	
Ave	0.084 (0.101)	0.157 (0.123)	0.047 (0.1)	0.078 (0.074)	0.121 (0.224)	0.042 (0.052)	0.203 (0.187)	0.115 (0.24)	0.09 (0.084)	0.085 (0.128)	0.077 (0.085)

適切な精度で利用できない利用者が現れる可能性はある．しかし，本手法を実装したシステムは，既存のパスワードによる個人識別を強化するために補助的に使用されるものであり，利用者は本システムの使用を選択可能である．本手法は，今後の電子決済やオンライン投票における不正防止技術の 1 つとして有効であると考える．

謝辞 本研究は JSPS 科研費 JP18K11248 の助成を受けたものです．

参考文献

[1] Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S.: Impact of artificial “gummy” fingers on fingerprint systems, *Optical Security and Counterfeit Deterrence Techniques IV*, van Renesse, R.L. (Ed.), Vol.4677, pp.275–289, International Society for Optics and Photonics, SPIE (online), DOI: 10.1117/12.462719 (2002).

[2] Matsumoto, T.: Gummy and Conductive Silicone Rubber Fingers: Importance of vulnerability analysis, *Proc. 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT '02*, pp.574–576, Springer-Verlag (2002) (online), available from ⟨http://dl.acm.org/citation.cfm?id=647098.717147⟩.

[3] 松本 勉：金融取引における生体認証について，横浜国立大学大学院環境情報研究院（オンライン），入手先 ⟨https://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/02.pdf⟩（参照 2020-12-20）．

[4] Fridman, L., Weber, S., Greenstadt, R. and Kam, M.: Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location, *IEEE Systems Journal*, Vol.11, No.2, pp.513–521 (online), DOI: 10.1109/JSYST.2015.2472579 (2017).

[5] Kobayashi, R., Susuki, H., Saji, N. and Yamaguchi, R.S.: Lifestyle authentication and MITHRA project, *2018 10th International Conference on Communication Systems Networks* (*COMSNETS*), pp.464–467 (online), DOI: 10.1109/COMSNETS.2018.8328245 (2018).

[6] Kobayashi, R. and Yamaguchi, R.S.: One hour term authentication for Wi-Fi information captured by smartphone sensors, *2016 International Symposium on Information Theory and Its Applications* (*ISITA*), pp.330–334 (2016).

[7] RSA：SecurID トークン，テクマトリックス株式会社（オンライン），入手先 ⟨https://www.techmatrix.co.jp/product/securid/token/index.html⟩（参照 2020-12-20）．

[8] おくとパス Business8：IC カード Windows 認証ソフト，株式会社 C&C アソシエイツ（オンライン），入手先 ⟨https://www.cca-co.jp/service/octpass-8/⟩（参照 2020-12-20）．

[9] e-Tax 国税電子申告・納税システム（イータックス）：マイナンバーカード方式について，国税庁（オンライン），入手先 ⟨https://www.e-tax.nta.go.jp/kojin/mycd_login.htm⟩（参照 2020-12-20）．

[10] 林 大介，赤倉貴子：e-Testing におけるタブレット PC とオンライン筆記情報を用いた筆記認証法の提案，日本教育工学会論文誌，Vol.42, pp.101–104（オンライン），DOI: 10.15077/jjet.S42051 (2018).

[11] 片桐雅二, 杉村利明：ビデオカメラを用いた空中署名による個人認証の試み，電子情報通信学会技術研究報告，PRMU, パターン認識・メディア理解，Vol.101, No.125, pp.9–16 (2001)（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/110003275341/⟩．

[12] 崎田隆行，鹿嶋雅之，佐藤公則，渡邊 睦：指先トラッキングとその軌跡抽出を用いた個人認証に関する研究，電子情報通信学会技術研究報告，PRMU, パターン認識・メ

ディア理解，Vol.107, No.384, pp.59–64 (2007)（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/110006549346/⟩.
[13] Hanyu, R., Zhao, Q. and Kaneda, Y.: A new protocol for on-line user identification based on hand-writing characters, *2016 IEEE Symposium Series on Computational Intelligence* (*SSCI*), pp.1–7 (online), DOI: 10.1109/SSCI.2016.7850197 (2016).
[14] Kato, Y., Hamamoto, T. and Hangai, S.: A proposal of writer verification of hand written objects, *Proc. IEEE International Conference on Multimedia and Expo*, Vol.2 (2002).
[15] Takahashi, A. and Nakanishi, I.: Authentication Based on Finger-Writing of a Simple Symbol on a Smartphone, *2018 International Symposium on Intelligent Signal Processing and Communication Systems* (*ISPACS*), pp.411–414 (online), DOI: 10.1109/ISPACS.2018.8923365 (2018).
[16] Sae-Bae, N., Ahmed, K., Isbister, K. and Memon, N.: Biometric-rich gestures: A novel approach to authentication on multi-touch devices, *Proc. Conference on Human Factors in Computing Systems* (online), DOI: 10.1145/2207676.2208543 (2012).
[17] Shen, C., Lv, Q., Wang, Z., Chen, Y. and Guan, X.: Hand-Interactive Behavior Analysis for User Authentication Systems with Wrist-Worn Devices, *2018 5th International Conference on Information, Cybernetics, and Computational Social Systems* (*ICCSS*), pp.90–95 (online), DOI: 10.1109/ICCSS.2018.8572367 (2018).
[18] 畠中一成，鹿嶋雅之，佐藤公則，渡邊　睦：Leap Motionを用いた空中署名での個人認識システムに関する研究（バイオメトリクス），電子情報通信学会技術研究報告=IEICE Technical Report：信学技報，Vol.114, No.212, pp.33–38 (2014)（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/110009945762/⟩.
[19] Lu, D., Huang, D., Deng, Y. and Alshamrani, A.: Multifactor User Authentication with In-Air-Handwriting and Hand Geometry, *2018 International Conference on Biometrics* (*ICB*), pp.255–262 (online), DOI: 10.1109/ICB2018.2018.00046 (2018).
[20] Renuka, R., Suganya, V. and Kumar, B.A.: Online hand written character recognition using Digital Pen for static authentication, *2014 International Conference on Computer Communication and Informatics*, pp.1–5 (online), DOI: 10.1109/ICCCI.2014.6921792 (2014).
[21] Hu, H., Chen, D. and Zheng, J.: Online Handwriting Signature Verification Based on Template Clustering, *EBDIT 2019*, pp.129–135, Association for Computing Machinery (online), DOI: 10.1145/3352740.3352762 (2019).
[22] Xiao, G., Milanova, M. and Xie, M.: Secure behavioral biometric authentication with leap motion, *2016 4th International Symposium on Digital Forensic and Security* (*ISDFS*), pp.112–118 (online), DOI: 10.1109/ISDFS.2016.7473528 (2016).
[23] 畠中一成，鹿嶋雅之，佐藤公則，渡邊　睦：指識別情報を用いたフレキシブル空中署名個人認証システムに関する研究，映像情報メディア学会誌，Vol.70, No.6, pp.J125–J132（オンライン），DOI: 10.3169/itej.70.J125 (2016).
[24] Lu, D., Xu, K. and Huang, D.: A data driven in-air-handwriting biometric authentication system, *2017 IEEE International Joint Conference on Biometrics* (*IJCB*), pp.531–537 (online), DOI: 10.1109/BTAS.2017.8272739 (2017).
[25] Alkaabi, S., Yussof, S., Almulla, S., Al-Khateeb, H. and AlAbdulsalam, A.A.: A Novel Architecture to verify Offline Hand-written Signatures using Convolutional Neural Network, *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies* (*3ICT*), pp.1–4 (online), DOI: 10.1109/3ICT.2019.8910275 (2019).
[26] Behera, S.K., Dogra, D.P. and Roy, P.P.: Analysis of 3D signatures recorded using leap motion sensor, *Multimedia Tools and Applications*, Vol.77, No.11, pp.14029–14054 (online), DOI: 10.1007/s11042-017-5011-4 (2018).
[27] Yamamoto, S., Ito, S., Ito, M. and Fukumi, M.: Authentication of Aerial Input Numerals by Leap Motion and CNN, *2018 IEEE International Conference on Internet of Things and Intelligence System* (*IOTAIS*), pp.189–193 (online), DOI: 10.1109/IOTAIS.2018.8600847 (2018).
[28] Mohammed, A.A., Abdul-Hassan, A.K. and Mahdi, B.S.: Authentication System Based on Hand Writing Recognition, *2019 2nd Scientific Conference of Computer Sciences* (*SCCS*), pp.138–142 (online), DOI: 10.1109/SCCS.2019.8852594 (2019).
[29] Singh, T. and Mishra, S.: Image vector classification algorithm for hand-writing verification, *2014 International Conference on Advances in Computing, Communications and Informatics* (*ICACCI*), pp.2239–2243 (online), DOI: 10.1109/ICACCI.2014.6968564 (2014).
[30] Rosa, G.H, Papa, P.J. and Scheirer, W.J.: Person Identification Using Handwriting Dynamics and Convolutional Neural Networks, *Deep Learning in Biometrics*, Chap. 5, pp.227–244, CRC Press (online), DOI: 10.1201/b22524 (2018).
[31] 高橋真奈茄，小出　洋：機械学習を用いたパターン認識による筆者識別，第57回プログラミング・シンポジウム予稿集，Vol.2016, pp.133–142 (2016).
[32] 小南嘉史，西村広光，富川武彦：筆跡情報と筆圧情報のHMMを用いたサイン認証，神奈川工科大学研究報告B理工学編，No.30, pp.73–78（オンライン），DOI: 10.34411/00000992 (2006).
[33] Guerbai, Y., Chibani, Y. and Hadjadji, B.: The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters, *Pattern Recognition*, Vol.48, No.1, pp.103–113 (online), DOI: 10.1016/j.patcog.2014.07.016 (2015).
[34] Granet, A., Morin, E., Mouchère, H., Quiniou, S. and Viard-Gaudin, C.: Transfer Learning for a Letter-Ngrams to Word Decoder in the Context of Historical Handwriting Recognition with Scarce Resources, *Proc. 27th International Conference on Computational Linguistics*, pp.1474–1484, Association for Computational Linguistics (2018) (online), available from ⟨https://www.aclweb.org/anthology/C18-1125⟩.
[35] Aneja, N. and Aneja, S.: Transfer Learning using CNN for Handwritten Devanagari Character Recognition, *2019 1st International Conference on Advances in Information Technology* (*ICAIT*) (online), DOI: 10.1109/icait47043.2019.8987286 (2019).
[36] Leap Motion: C# SDK Documentation - Leap Motion C# SDK v2.3 documentation, Leap Motion (online), available from ⟨https://developer-archive.leapmotion.com/documentation/v2/csharp⟩ (accessed 2019-11-20).
[37] Ioffe, S. and Szegedy, C.: Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift, *CoRR*, Vol.abs/1502.03167 (2015) (online), available from ⟨http://arxiv.org/abs/1502.03167⟩.
[38] Kritsis, K., Kaliakatsos-Papakostas, M., Katsouros, V. and Pikrakis, A.: Deep Convolutional and LSTM Neu-

ral Network Architectures on Leap Motion Hand Tracking Data Sequences, *2019 27th European Signal Processing Conference* (*EUSIPCO*), pp.1–5 (online), DOI: 10.23919/EUSIPCO.2019.8902973 (2019).
[39] クジラ飛行机：無料 英和辞書データ ダウンロード - ブラウザで使える Web 便利ツール，くじらはんど（オンライン），入手先 ⟨https://kujirahand.com/web-tools/EJDictFreeDL.php⟩（参照 2020-12-20）.

釜石 智史

2016 年東京工科大学コンピュータサイエンス学部卒業．2018 年同大学大学院バイオ情報メディア研究科コンピュータサイエンス専攻博士前期課程修了．現在，同大学院バイオ情報メディア研究科コンピュータサイエンス専攻博士後期課程在籍．

宇田 隆哉 （正会員）

1998 年慶應義塾大学理工学部計測工学科卒業．2000 年同大学大学院理工学研究科計測工学専攻前期博士課程修了．2002 年同大学院理工学研究科開放環境科学専攻後期博士課程修了．博士（工学）．現在，東京工科大学コンピュータサイエンス学部講師．ネットワークセキュリティの研究に従事．2002 年 IFIP/SEC 2002 Best Student Paper Award 受賞．電子情報通信学会会員．