スマートフォンにおけるタッチストロークを利用した耐模倣性を実現するパッシブ認証

工藤 雅士[†1]　山名 早人[‡23]

†1 早稲田大学大学院基幹理工学研究科 〒169-8555 東京都新宿区大久保 3-4-1
‡2 早稲田大学理工学術院 〒169-8555 東京都新宿区大久保 3-4-1
‡3 国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2
E-mail: †‡{kudoma34, yamana}@yama.info.waseda.ac.jp

あらまし 近年爆発的に普及したスマートフォンには多くの個人情報が格納されている．こうした個人情報の保護を目的として，スマートフォンには「パスワード」や「指紋認証」といった認証機能が標準的に搭載されている．しかし，個人の記憶や生体情報に基づいた認証機能は盗み見や生体情報の合成によって第三者に突破される可能性が存在する．そこで本稿では，スマートフォンの標準的な認証機能と認証のために特別な行動を要求しない「パッシブ認証」を組み合わせて，所有者本人が利用しているか否かを，タッチストロークを用いて常に監視し続ける認証システムの提案を行う．また，認証手法の評価に「耐模倣性」という観点を導入し，第三者による画面の覗き見に対して頑健な認証システムの構築を目指す．評価実験では，第三者のタッチストロークを模倣した際のタッチストロークを収集し，オンライン学習器 AROW により認証システムの構築を行った．23 人の評価実験の結果，画面の覗き見が深刻な攻撃になり得ることを確認した．また，あらかじめ模倣データで訓練を行うことにより，EER と耐模倣性の両方が向上することを確認した．加えて，ストローク方向別の学習を導入することにより，21 人から取得したタッチストロークの模倣データを使用した場合においても 13 ストロークの認証間隔で 0.00%の EER を達成した．ストローク特徴量の検証実験では，「ストロークの速度」と「ストロークにかかった時間」が EER への寄与度と耐模倣性の両方が高い特徴量であることが示された．

キーワード パッシブ認証，オンライン学習，タッチストローク，耐模倣性

1. はじめに

近年，スマートフォンを利用するユーザ数は爆発的に増加している．総務省の「通信利用動向調査」[1]によると，平成 30 年における日本のスマートフォンの世帯保有率は 79.2%であり，同年におけるパソコンの世帯保有率 74.0%を 5.2 ポイント上回る数値を記録している．また，個人のインターネット利用端末に関する調査報告においても，スマートフォンの利用率 59.5%がパソコンの利用率 48.2%を上回っており，日常のメインデバイスがパソコンからスマートフォンへと移行している現状がうかがえる．

スマートフォンはその多機能さや利便性から利用が増加する一方で，スマートフォン所有者の個人情報や生体情報といった重要な情報をスマートフォン上で扱う場面が増加している．こうした個人情報の保護を目的として，スマートフォンには「パスワード」や「指紋認証」といった認証機能が標準的に搭載されている．しかし，個人の記憶や生体情報に基づいた認証機能は，盗み見や生体情報の合成によって第三者に突破されてしまう可能性が存在する[2,3]．また，個人情報はスマートフォンの紛失・盗難によって流出する可能性も存在する．Lookout の報告[4]では，2014 年において，日本のスマートフォン保有者の約 23%が紛失を経験していると述べられている．著者の試算によると，同年におけるスマートフォン紛失・盗難による個人情報流出から発生する経済的損失は約 1,082 億円にのぼると考えられ，スマートフォンのセキュリティ性の向上は今も継続的な課題であると言える．

スマートフォンのセキュリティ性の向上が求められる一方で，スマートフォンが日常的に使用されているという点から，セキュリティ性と操作性のバランスは必要不可欠である．セキュリティ性と操作性を両立させる方法として，現在「パッシブ認証」という認証手法が注目を集めている．パッシブ認証とは，認証のために文字を入力したり指をかざしたりといった特別な操作を要求しない認証技術である．パッシブ認証の例としては，リスクベース認証が挙げられる．リスクベース認証では，過去のログデータや IP アドレスなどの情報を基に認証が行われ，不正のリスクに基づいて追加の認証が行われる．リスクベース認証はスマー

[1] 総務省，“平成 30 年通信利用動向調査”，2019，https://www.soumu.go.jp/johotsusintokei/statistics/data/190531_1.pdf
[2] 『日経 MJ(流通新聞)』2016.1.15，「LINE、漏洩に用心―スマホの画面ロック機能、安全性は設定次第。」
[3] 『毎日新聞』2017.8.10 大阪朝刊，「詐欺:アップルペイで商品搾取本人確認抜け穴大阪など 6 容疑者逮捕」
[4] Lookout，“日本のスマートフォン紛失にまつわる事情”，2014，https://www.lookout.com/img/resources/Lookout_Phone_Loss_in_Japan_1.pdf

トフォンの各種アプリケーションにおいても広く採用されており，不正が疑われる場合に「秘密の質問」などを促すアプリケーションが存在する．しかし，従来のリスクベース認証では，第三者がスマートフォンを操作して所有者の個人情報を不正参照する場合など，不正使用の捕捉が困難な場面が存在する．また，ユーザのアクセス情報に基づいたパッシブ認証はリスク判定の際に確認するパラメータの量が数百に及ぶ場合があり，リスク判定のルールが複雑になりやすく，導入コストや運用コストが高くなってしまう可能性がある．

そこで本稿では，スマートフォン利用者が当該スマートフォンの本人であることを常に監視し続ける「パッシブ認証」を，スマートフォン操作の主体であるタッチストロークを用いて実現することを目指す.また，認証システムおよびタッチストロークから抽出される特徴量の評価に「耐模倣性」という観点を導入し，第三者によって自身のタッチストロークが模倣された場合においてもロバストなシステムの構築を目指す．これにより，第三者による覗き見や不正使用にも対応が可能となる．加えて，認証精度の向上を目的として，ストローク方向別に分類器を構築する手法についての検討も行う．

本稿では次の構成をとる．２節でスマートフォン上での認証に関連する研究を紹介し，３節で提案する認証システムについて詳述する．続いて，４節で評価実験の結果を示し，５節において本稿で用いた特徴量の耐模倣性について議論する．６節では，実運用における課題を示す．７節はまとめである．

2. 関連研究

タッチストロークを利用した認証では，スマートフォンに内蔵されたセンサーから取得されるタッチ座標やタッチ圧力，ストローク速度などのタッチ情報に基づいて認証が行われる．タッチストロークを利用した認証はスマートフォンの操作性を損なわない認証として注目を集める一方で，タッチストロークの模倣や，大規模データから平均的なタッチストロークを生成することにより,認証が突破される可能性が存在する[1]．また，認証に使用するタッチ情報をデジタルデータとして不正に取得し，取得したデータから所有者本人の擬似的なタッチストローク操作を生成することで，所有者本人へのなりすましが可能であることが報告されている[2]．

そこで本節では，タッチストロークを利用した認証において，本人へのなりすましを防ぐ手法を提案した研究を紹介する．

2.1. Shrestha らの研究

近年のスマートフォンの認証研究により，スマートフォン内蔵のモーションセンサーを監視することで，スマートフォン上でのタッチイベントの検出や，パスワード認証に使用されている文字列の推測が可能であることが示されている[3][4]．これらの結果に基づいて，University of Alahama の Shrestha ら[5]は，2016 年にスマートフォンのモーションセンサーが不正にロギングされている場合を想定し，センサーの読み取り値に対してランダムな時間間隔でノイズの注入を行い，タッチイベントの検出やタッチストロークの推測を防御する「Slogger」と呼ばれるシステムの提案を行った．

1,200 回分のスマートフォンの画面タップデータを使用して行った画面タップ検出の検証実験では，Slogger を適用することで 0%の Precision かつ 0%の Recall を達成し，Slogger によってタップの検出が不可能になることが示された．また，スマートフォンの画面領域を二分割し，タッチストロークが行われた画面領域を推測する検証実験では，ランダムで画面領域を推定する場合の精度である 50%から，Slogger を適用することで 35.5%まで推定精度を引き下げることが可能であることを示した．

2.2. Gong らの研究

Iowa State University の Gong ら[6]は，2016 年に攻撃者によってスマートフォンのタッチストローク操作が不正にロギングされている場合を想定し，タッチストロークが不正に取得されている場合においても所有者へのなりすましを防ぐことが可能な防御手法の提案を行った．Gong ら[6]は，スマートフォンのタッチ座標に焦点を当て，スマートフォンの画面に対して X 軸方向と Y 軸方向それぞれに倍率をかける画面設定を，一定の時間間隔で変更を行う手法を提案した．

評価実験では，X 軸方向と Y 軸方向それぞれに対して別々に 0.8 倍，0.9 倍，1.0 倍，1.1 倍，1.2 倍の画面倍率をかける計 25 通りの画面設定を適用し，25 人の実験参加者から各倍率において水平方向ストロークと垂直方向ストロークの取得を行なった．SVM を用いて構築した分類器による評価実験の結果，攻撃者が不正にスマートフォン所有者のタッチストロークを取得し，取得したタッチストロークに基づいて本人へのなりすましを行った場合においても，本手法を適用することでなりすましを防止することが可能であることを示した．

2.3. 関連研究まとめ

タッチストロークを利用した認証は，攻撃者によるタッチストロークの模倣やタッチストローク操作の偽装による攻撃に対して脆弱であるとされている[1][2]．そのため，近年の認証研究では，タッチストロークのなりすましに対抗するための手法として，スマートフォンの各種センサーから取得されるデジタルデータにノイズや補正をかける手法[5][6]が提案されている．

こうしたタッチストロークのなりすましを防ぐ従来の研究では，攻撃者がなりすまし行う際に，ターゲットとなるユーザが所持するスマートフォンのセンサー情報を不正に取得できる状態にあることを前提としている．そのため，所謂マルウェアを使用した攻撃が想定されている．しかし，スマートフォンの実際の利用現場では，「画面の覗き見」によるタッチストロークの模倣など，高度な知識や技術力が必要とされるマルウェアを使用した攻撃よりも発生頻度が高いと想定される攻撃が存在する．

3. 提案手法

本節では，本稿で提案するタッチストロークを利用したパッシブ認証手法ついて詳しく説明する．

3.1. 提案概要

タッチストロークを利用した認証において，近年では本人へのなりすましを防ぐ手法の提案が行われている．従来の研究では，マルウェアを介してタッチストロークをデジタルデータとして不正に取得する攻撃を想定した上で，本人へのなりすましを防ぐ手法が提案されている．本稿では、これに対して、スマートフォンの実際の利用現場でより発生しやすい「画面の覗き見」に焦点を当て、覗き見によって真似されることのない認証を目指す。

本稿で提案する認証システムは，著者らの先行研究[7][8]をベースラインとしている．認証システムの評価とタッチストロークから抽出される特徴量の評価には「耐模倣性」という観点を導入し，各特徴量の耐模倣性を検証することで，覗き見によって真似されることのない認証の実現を目指す．

本稿では，以下の３段階で認証を行うシステムを前提とし，２段階目のパッシブ認証部分を提案する．すなわち，１段階目及び２段階目の認証は研究の対象外とし，常に正しく認証されるものとする．

1. パスワードや指紋認証などの標準的な認証
2. タッチストロークを用いたパッシブ認証
3. 2 で不正が疑われる場合，標準的な認証による追加の認証

また，認証精度を向上させるために採用した，認証に使用する分類器を上方向ストローク用と下方向ストローク用に分割し，ストローク方向別に分類器を構築する手法の有用性についても検証を行う．

3.2. 抽出する特徴量

本稿では，スマートフォン内蔵のセンサーのみを使用して，ベースライン手法[8]と同様に 26 種類のタッチストロークに関する特徴量の抽出を行う．本稿で抽出する特徴量およびその抽出方法を表 1，図 1 に示す．

表 1　本稿で使用するストローク特徴量
（ベースライン手法[8]と同様）

特徴量名	内容
startX, startY	ストローク開始時の XY 座標
stopX, stopY	ストローク終了時の XY 座標
x20, y20	ストローク 20%地点における XY 座標
x50, y50	ストローク 50%地点における XY 座標
x80, y80	ストローク 80%地点における XY 座標
startPressure	ストローク開始時の圧力
stopPressure	ストローク終了時の圧力
midPressure	ストロークの中間地点における圧力
maxPressure	ストローク中の最大圧力
averagePressure	ストローク中の平均圧力
averageVelocity	ストローク中の平均速度(px/s)
vel20	ストローク 20%地点における ストローク速度(px/s)
vel50	ストローク 50%地点における ストローク速度(px/s)
vel80	ストローク 80%地点における ストローク速度(px/s)
strokeDuration	ストロークにかかった時間(s)
interStrokeTime	ストローク間隔時間(s)
lengthEE	ストロークの開始地点と終了地点の ユークリッド距離(px)
angleEE	ストロークの開始地点と終了地点がなす角度(deg)
lengthTrj	ストローク軌跡の長さ(px)
ratioTrj2EE	lengthEE と lengthTrj の比 (lengthTrj/lengthEE)
direction	ストロークの方向 （上方向/下方向の２値）

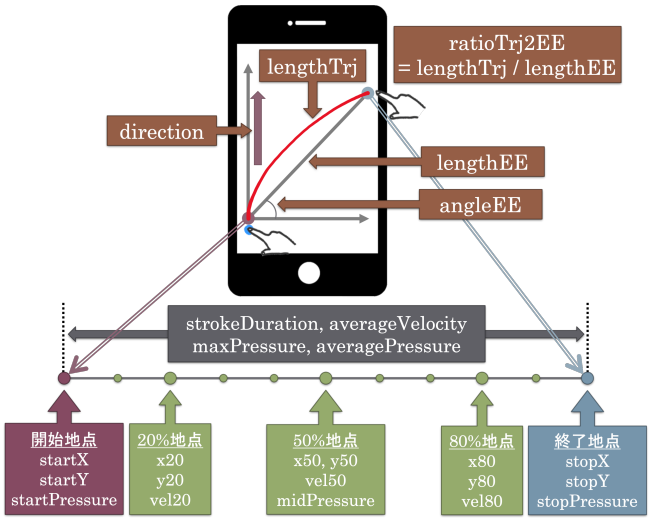


図 1　ストローク特徴量の抽出方法
（ベースライン手法[8]と同様）

3.3. パッシブ認証システムの概要

本稿では，パッシブ認証システムを構築するにあたり，ベースライン手法[7][8]で使用した認証手法を採用した．そこで，本項では本稿で用いる認証手法について,ベースライン手法[7][8]を基に詳しく説明する．

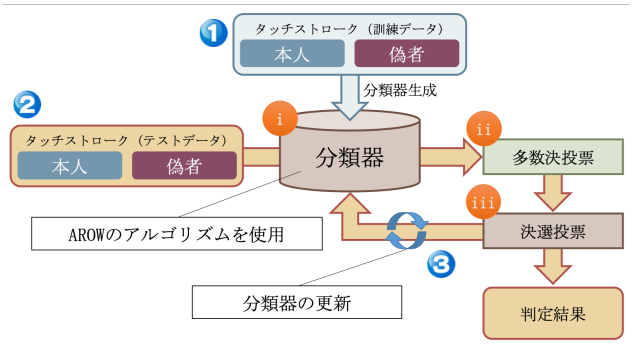


図 2　本手法におけるパッシブ認証の流れ

本手法では，まず予め用意した訓練データからオンライン学習器 AROW[9]のアルゴリズムを用いて分類器の生成を行う（図 2 ①）．続いて，スマートフォンの画面操作時のタッチストロークを監視し，分類器の更新を行いながらストローク単位で継続的な認証を行う（図 2 ②）．本システムでは，著者らの先行研究[7]で提案した図 3 に示される決選投票モデルを使用して最終的な認証結果の出力を行う．

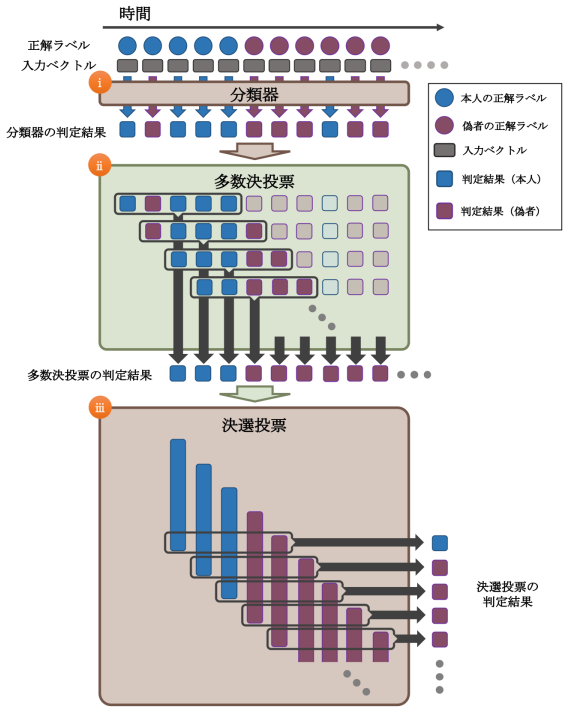


図 3　決選投票モデルの全体像
（5 ストロークごとの認証の場合）
（[7]の図 5 をもとに作成）

本手法では，以下の手順で認証結果の出力を行う．

1. 分類器による判定（図 2，図 3 （i））
2. 多数決投票（図 2，図 3 （ii））
3. 決選投票（図 2，図 3 （iii））

本稿では，ベースライン手法[7][8]と同様に多数決投票と決選投票は共に 13 ストローク間隔で判定を行うものとする．また，決選投票の結果，所有者以外の不正な使用が疑われる場合は 3.1 項で示した 3 段階目の「標準的な認証による追加の認証」へと移行し，3 段階目の認証結果をもとに最新 13 ストローク分のタッチストロークで分類器の更新を行う．このとき，分類器の更新結果を即座に認証結果へと反映させるために，決選投票モデルに格納されている最新 26 ストローク分の判定結果に関しても，分類器更新後に再判定を行うようにベースライン手法[7][8]の改良を行った．

4. 評価実験

本節では，本稿で提案する認証システムの認証精度および耐模倣性を評価するために実施した評価実験について詳しく説明する．

4.1. データ収集

4.1.1. データ収集用アプリケーションの概要

本稿では，取得できるストローク数を増やすとともに，ストローク方向別の認証を検証するにあたり上方向ストロークと下方向ストロークのストローク数の偏りを無くすために,ベースライン[8]で使用した写真マッチングゲームアプリケーションの改良を行った．アプリケーションの改良点は以下の 2 点である．

- クイズ形式のタスクに変更し，全ての画像を確認しなければ回答できないクイズを設定した．
- 上端で固定されていた写真リストの初期表示位置を，上端と下端の 2 種類に変更した．

上記の改良点を反映させた写真マッチングゲームの iOS アプリケーション（図 4）を作成し，本アプリケーションをインストールした Apple 社製の iPhone8+[5] を使用してタッチストロークの収集を行った．なお，今回のデータ収集で取得するタッチストロークは，図 4 の①において 100 枚の写真リストをスクロールしている時のタッチストロークのみとし，画面のタップや他の画面でのスクロールはデータ収集の対象外とした．写真マッチングゲームの流れを以下に示す．

1. ゲーム側：ランダムでクイズ 1 問と，クイズの正解画像を 1 枚設定する．
2. ユーザ:写真リストをスクロールする(図 4 ①)．
3. ユーザ：画像を 1 枚選択する（図 4 ②）．
4. ゲーム側：画像の確認画面を表示する．
5. ユーザ：選択した画像を確認する（図 4 ③）．
6. ゲーム側：画面上に正誤を表示する．

[5] https://www.apple.com/jp/iphone-8/specs/

7. ユーザ：次のクイズへ移行する（図 4 ④）.
8. 1-7 を規定回数繰り返し，終了する（図 4 ⑤）.

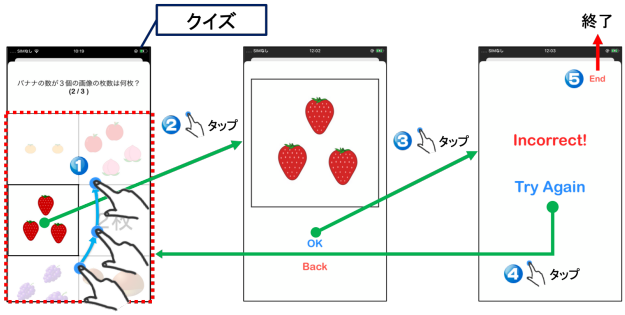


図 4　アプリケーションの流れ

上記 1-7 の流れを 1 ゲーム，また 5 ゲームを 1 セッションとして，1 セッション毎に休憩を設けて複数セッション実施し，タッチストロークの収集を行った.

4.1.2. データ収集の実施

本稿で実施したデータ収集は，大学生 23 人（男性 13 人，女性 10 人）を対象に行い，認証システムの耐模倣性を検証するために，スマートフォン操作時の通常のタッチストローク（以下，*Own strokes*）に加えて，「第三者のタッチストロークを意図的に模倣した場合」のタッチストローク（以下，*Imitation strokes*）についてのデータ収集も行った．本実験におけるデータ収集の手順を以下に示す.

1. タッチストローク模倣の対象となる 2 人の被験者（以下，ターゲット）を設定する.
2. ターゲット 2 人から以下のデータを取得する.
   - アプリケーションを 4 セッション操作した時の *Own strokes*.
   - アプリケーションを 2 ゲーム操作している時のストロークの様子を，ターゲットの背後からビデオカメラで撮影した動画（以下，ストローク動画）（図 5）.
3. ターゲットを除外した 21 人の被験者（以下，模倣実施者）から，アプリケーションを 4 セッション操作した時の *Own strokes* を収集する.
4. 手順 2 で取得したターゲット 1 人分のストローク動画をリピート再生で模倣実施者に見せる．模倣実施者が動画に収められているストローク操作の特徴を学習できたと判断した段階でストロークの模倣を実施し，*Imitation strokes* を 4 セッション分収集する．この時，模倣実施者には表 1 に示されるストローク特徴量を提示し，26 種類のストローク特徴量をバックグラウンドで取得している点について説明を行う.
5. 手順 4 をもう 1 人のターゲットのストローク動画で実施する.

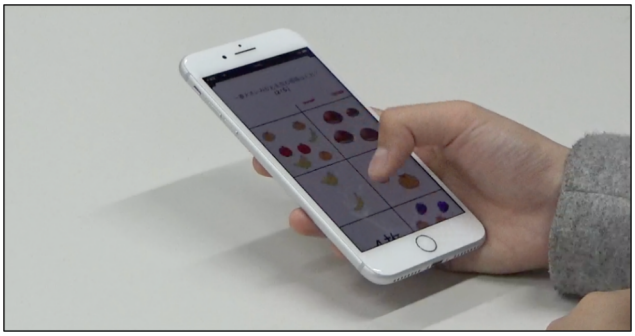


図 5　ストローク動画（一部抜粋）

以上のデータ収集により，2 人の各ターゲットから *Own strokes* が 1,200 ストローク以上，また 21 人の各模倣実施者から *Own strokes* と *Imitation strokes* がそれぞれ 1,200 ストローク以上得られた.

4.2. 評価手法

本稿では，認証システムの認証精度を評価するにあたり，評価指標として EER（Equal Error Rate：等価エラー率）を用いた．EER は FRR(False Rejection Rate: 本人拒否率）と FAR（False Acceptance Rate：他人受入率）が等しくなる点におけるエラー率を表す指標であり，FRR（本人拒否率）と FAR（他人受入率）はそれぞれ表 2 に示される混同行列に基づいて，式(1)および式(2)で定義される.

表 2　混同行列

		Predicted Class	
		Positive	Negative
Actual Class	Positive	TP	FN
	Negative	FP	TN

$$FRR = \frac{FN}{TP+FN} \quad (1)$$

$$FAR = \frac{FN}{FP+TN} \quad (2)$$

本稿では，EER による認証精度の評価に加えて各特徴量の耐模倣性に関しても評価を行う．耐模倣性に関する評価は，第三者の「タッチストロークを意図的に模倣した場合」のストローク，つまり *Imitation strokes* を模倣と判定し，他者として分類することができるか否かによって行う.

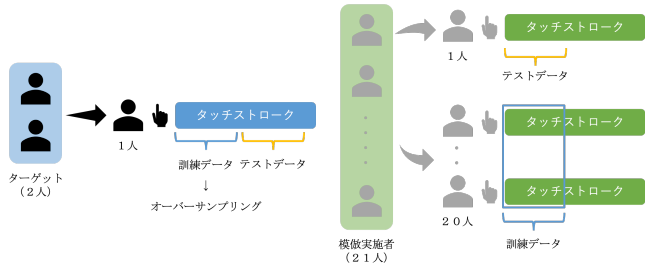
4.3. 実験データセット

本稿では，認証システムの EER 評価および耐模倣性評価を行うために，擬似的にスマートフォンの所有者（以下，被模倣者）と，スマートフォンの所有者ではない第三者（以下，模倣者）を設定し，以下の 4 つのデータで構成される実験データセットの構築を行った.

- 被模倣者の訓練データおよびテストデータ
  （Positive クラスのラベル付けを行う.）
- 模倣者の訓練データおよびテストデータ
  （Negative クラスのラベル付けを行う.）

実験データセットの構築方法を図 6 に示す．なお，実運用においては他者による模倣データを用意することは困難であり，これについては 6 節で議論する．

被模倣者の訓練データおよびテストデータは，２人のターゲットから選出した１人のタッチストロークを使用して構築を行う．また，模倣者データに関しては，21 人の模倣実施者から選出した１人のタッチストロークを使用してテストデータの構築を行い，残りの 20 人のタッチストロークを均等に使用して訓練データの構築を行う．なお，被模倣者の訓練データ数と模倣者の訓練データ数を揃えるために，被模倣者の訓練データに関してオーバーサンプリングを行う．また，各データセットに関して，被模倣者データに使用するターゲットと，模倣者のテストデータに使用する模倣実施者を変えてそれぞれ 42 通りの交差検証を行う．



(a) 被模倣者データの構築方法　　(b) 模倣者データの構築方法

図 6　実験データセットの構築方法

上記に示した実験データセットについて，使用するストロークの組み合わせとストロークの抽出方法を変えて複数種類のデータセットを作成し，認証システムの EER 評価および耐模倣性評価を行った．

4.4. 実験結果

4.3 項で作成したデータセットのうち，タッチストロークの模倣が EER へ与える影響を検証した結果を表 3 に示す．表 3 より，タッチストロークの模倣を実施することで，模倣未実施時の EER 0.67%から EER 0.75%へと認証のエラー率が増加することが確認された．これは，画面覗き見によるタッチストロークの模倣が深刻な攻撃になり得ることを示している．

続いて，4.3 項で作成したデータセットのうち，模倣データの訓練が EER へ与える影響を検証した結果を表 4 に示す．表 4 より，模倣データを訓練データに追加することで，表 3 の評価結果と比較して EER が低下することが確認された．また，タッチストロークの模倣が実施された場合においても EER の低下が確認され，模倣データの学習による認証システムの耐模倣性向上が示された．

さらに，表 4 で使用したデータセットにおいて，分類器を上方向ストローク用の分類器と下方向ストローク用の分類器に分割し，ストローク方向別で認証を行った結果を表 5 に示す．表 5 より，ストローク方向別の認証を導入することによって，EER と耐模倣性の両方が向上することを確認した．また，模倣実施者 21 人から取得したタッチストロークの模倣データを使用した場合において 0.00%の EER を達成した．

5. 特徴量に関する検証

本節では，本稿で使用した 26 種類の特徴量それぞれが，EER および耐模倣性の向上にどれだけ寄与しているかについて評価するために実施した検証実験について詳しく説明する．

5.1. 各特徴量の EER への寄与度の評価方法

4 節で実施した評価実験のうち，表 4 に示される実験データセットを対象にストローク特徴量の EER への寄与度の検証を行った．表 1 に示される 26 種類の特徴量のうち，$i\,(1 \leq i \leq 26)$ 番目の特徴量を除いた 25 種類の特徴量を用いて，26 種類全ての特徴量を使用した場合の評価実験と同じ手順で訓練およびテストを行った．26 種類全ての特徴量を使用した場合の EER を EER_{all}，i番目の特徴量を除いた場合の EER を EER_i とした場合に，i番目の特徴量の EER への寄与度 C_i を以下の式で定義する．

$$C_i = EER_i - EER_{all} \qquad (3)$$

EER の値が小さいほど認証の精度が優れていると考えられるため，本稿では，寄与度 C_i の値が大きいほど EER への寄与度が高いと考えて各特徴量の評価を行う．

表 3　認証の評価結果（タッチストロークの模倣が EER へ与える影響の検証）

No.	訓練データ				テストデータ				ストローク方向	EER [%]
	被模倣者データ		模倣者データ		被模倣者データ		模倣者データ			
	ストローク種類	ストローク数	ストローク種類	ストローク数	ストローク種類	ストローク数	ストローク種類	ストローク数		
1-1	Own（1 ユーザ）	8,000	Own（20 ユーザ）	8,000	Own（1 ユーザ）	800	Own（1 ユーザ）	800	考慮しない	0.67
1-2	Own（1 ユーザ）	8,000	Own（20 ユーザ）	8,000	Own（1 ユーザ）	800	Imitation（1 ユーザ）	800	考慮しない	0.75

表 4　認証の評価結果（Own strokes と Imitation strokes による訓練の場合）

No.	訓練データ				テストデータ				ストローク方向	EER [%]
	被模倣者データ		模倣者データ		被模倣者データ		模倣者データ			
	ストローク種類	ストローク数	ストローク種類	ストローク数	ストローク種類	ストローク数	ストローク種類	ストローク数		
2-1	Own（1 ユーザ）	8,000	Own（20 ユーザ）	4,000	Own（1 ユーザ）	800	Own（1 ユーザ）	800	考慮しない	0.54
			Imitation（20 ユーザ）	4,000						
2-2	Own（1 ユーザ）	8,000	Own（20 ユーザ）	4,000	Own（1 ユーザ）	800	Imitation（1 ユーザ）	800	考慮しない	0.32
			Imitation（20 ユーザ）	4,000						

表 5　認証の評価結果（ストローク方向別での認証の場合）

No.	訓練データ				テストデータ				ストローク方向	EER [%]
	被模倣者データ		模倣者データ		被模倣者データ		模倣者データ			
	ストローク種類	ストローク数	ストローク種類	ストローク数	ストローク種類	ストローク数	ストローク種類	ストローク数		
3-1	Own（1 ユーザ）	8,000	Own（20 ユーザ）	4,000	Own（1 ユーザ）	800	Own（1 ユーザ）	800	ストロークを上方向と下方向に分割して学習	0.03
			Imitation（20 ユーザ）	4,000						
3-2	Own（1 ユーザ）	8,000	Own（20 ユーザ）	4,000	Own（1 ユーザ）	800	Imitation（1 ユーザ）	800	ストロークを上方向と下方向に分割して学習	0.00
			Imitation（20 ユーザ）	4,000						

5.2. 各特徴量の EER への寄与度の評価結果

実験データセット 2-1, 2-2 における，26 種類の特徴量の EER への寄与度を図 7 に示す．図 7 より，ストロークの速度に関する特徴量（averageVelocity, vel20, vel50, vel80）や，ストロークにかかった時間に関する特徴量（strokeDuration）が EER への寄与度が高い．また，他者にストロークを模倣された場合においても，これらの特徴量は EER への寄与度が高い．従って，「ストロークの速度」と「ストロークにかかった時間」は個人の特徴が反映されやすく，またストロークを模倣された場合においても EER への高い寄与度を維持できているという点から，耐模倣性が高い特徴量であると考えられる．

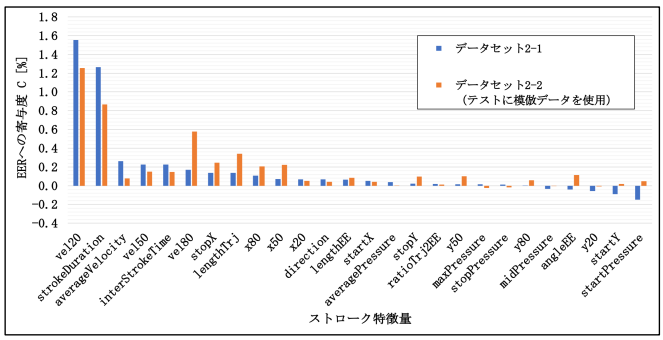


図 7　実験データセット 2-1, 2-2 における各特徴量の EER への寄与度

6.　実運用における課題

本稿では，所有者本人と所有者ではない第三者のタッチストロークを使用して認証に使用する分類器の生成を行った．4 節で実施した評価実験の結果から，訓練の際に他人のタッチストロークと，所有者本人のタッチストロークを他人が模倣したタッチストロークを使用することで，EER と耐模倣性の両方が向上することが示された．しかし，実運用において本認証手法を適用する場合，事前に訓練データとして使用する他者のデータおよび模倣データを用意する必要がある．

他者のデータに関しては，訓練用のユーザを設定することによって事前にデータを用意することが可能である．また，認証のタスクを 1 クラスの分類もしくは新規性検出の問題と捉えて，他者のデータを使用せずに所有者本人のデータのみを用いて認証モデルを生成する手法[10][11][12]も存在する．

一方で，模倣データに関しては事前に準備することは困難であり，また実際に模倣を実施してデータを生成することも手間の面から現実的ではないと言える．そのため，本人のストロークデータから模倣データを自動生成する仕組みについて検討を行い，自動生成された模倣データによって学習を行なう手法を確立することが今後の課題である．

7. おわりに

本稿では，認証のために特別な行動を要求しない「パッシブ認証」をスマートフォン上で実現し，所有者本人がスマートフォンを利用しているか否かを，タッチストロークを用いて常に監視し続ける認証手法を提案した．認証手法の評価には，従来の EER による評価に加えて,「耐模倣性」という新たな観点による評価を導入し，タッチ情報を使用した認証の脅威とされている本人へのなりすましに関する検証を行った．23 人の大学生から取得したタッチストロークを用いて行なった評価実験では，画面覗き見によるタッチストロークの模倣が，ストローク認証において深刻な攻撃になり得ることを確認した．続いて，あらかじめ模倣データで訓練を行うことで，EER と耐模倣性の両方が向上することを確認した．さらに，ストローク方向別に認証を行うことで，EER と耐模倣性の両方が向上することを確認し，21 人から取得したタッチストロークの模倣データを使用した場合において,最大で 0.00%の EER を達成した．

本稿で使用した 26 種類のストローク特徴量に関して行った EER への寄与度に関する検証では,「ストロークの速度」と「ストロークにかかった時間」に関するストローク特徴量が EER への寄与度と耐模倣性の両方が高い特徴量であることが示された．

今後の課題としては，検証を行うデータの規模を増やすことや，ユーザ自身のストロークから模倣データを生成する手法を検討することが挙げられる．また，実運用において個人のタッチストロークに関するデータをどのように管理し，保護するかについても今後検討を行う．

謝辞

この研究は 2019 年度国立情報学研究所 CRIS 委託研究の助成を受けています．

参 考 文 献

[1] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, “Surveying the development of biometric user authentication on mobile phones,” IEEE Commun. Surv. Tutorials, vol.17, no. 3, pp.1268–1293, 2015.

[2] A. Serwadda, V. V. Phoha, Z. Wang, R. Kumar, and D. Shukla, “Toward robotic robbery on the touch screen,” ACM Trans. Inf. Syst. Secur., vol.18, no. 4, 2016.

[3] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, “ACCessory: Password Inference using Accelerometers on Smartphones,” Proc. of the 12th Workshop on Mobile Comput. Syst. & Applications (HotMobile 2012), pp.1–6, 2012.

[4] Z. Xu, K. Bai, and S. Zhu, “TapLogger: Inferring User Inputs On Smartphone Touchscreens Using On-board Motion Sensors,” Proc. of the 5th ACM conference on Security and Privacy in Wireless and Mobile Networks (WISEC 2012), pp.113-124, 2012.

[5] P. Shrestha, M. Mohamed, and N. Saxena, “Slogger: Smashing motion-based touchstroke logging with transparent system noise,” Proc. of the 9th ACM Conf. Secur. Priv. Wirel. Mob. Netw., pp.67–77, 2016.

[6] N. Z. Gong, R. Moazzezi, M. Payer, and M. Frank, “Forgery-resistant touch-based authentication on mobile devices,” Proc. of the 11th ACM Asia Conf. Comput. Commun. Secur., pp.499–510, 2016.

[7] T. Ishiyama and H. Yamana, “Realization of Active Authentication for Smart Phone by Using Online Learning,” *DBSJ Japanese J.*, vol.16, no. 18, pp.1–8, 2018.

[8] M. Kudo and H. Yamana, “Active Authentication on Smartphone using Touch Pressure,” *Proc. of the 31st ACM Symposium on User Interface Software and Technology*, UIST’18, pp.96–98, 2018.

[9] K. Crammer, A. Kulesza, and M. Dredze, “Adaptive Regularization of Weight Vectors,” Proc. of the 23rd Adv. Neural Inf. Process. Syst. 22, pp.414–422, 2009.

[10] A. Roy, T. Halevi, and N. Memon, “An HMM-based multi-sensor approach for continuous mobile authentication,” Proc. of Military Commun. Conf., pp. 1311–1316, 2015.

[11] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, “HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users,” IEEE Trans. Inf. Forensics Secur., vol.11, no. 5, pp.877–892, 2016.

[12] C. Shen, Y. Li, Y. Chen, X. Guan, and R. A. Maxion, “Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication,” IEEE Trans. Inf. Forensics Secur., vol.13, no. 1, pp.48–62, 2018.