

# 線描軌跡を用いたモバイル端末における グラフィカルユーザID (IDLS) の提案

松野 友輔<sup>†</sup> 黄 宏軒<sup>†</sup> 川越 恭二<sup>†</sup>

<sup>†</sup>立命館大学 情報理工学部

## 1 はじめに

近年、スマートフォンやタブレット端末の普及に伴い、ユーザ認証をモバイル端末で行う機会が増加している。例えば、通販サイトや Facebook、インターネットバンキングサービス等のサービスが挙げられる。

モバイル端末でのユーザ ID の通常入力方法は、仮想キーボードを用いた英数字入力である。しかし、小さい仮想キーボードでの入力は従来のキーボードに比べ、入力の手間が大きいという問題が存在する。また、ユーザ自身でユーザ ID を決めることもあるが、ランダムな英数字列の場合も存在する。その場合、ユーザへの記憶負担は大きい。

そこで本研究では、モバイル端末でのユーザ ID 入力の手間の削減と記憶負担の軽減のため、新たなユーザ ID とその入力方法 IDLS (graphical user-ID by Line Sketching) を提案する。IDLS では、まず、ユーザが自身のユーザ ID を登録するために指定された領域に線を描く。描いた線の軌跡をユーザ ID として登録する。次に、認証時にユーザ ID を入力するには、ユーザ ID 入力時に登録済みの軌跡を描く。ユーザの描いた軌跡とユーザ ID データベース内の登録済みの軌跡とのマッチングを行うことでユーザ ID の確認を行う手法である。ユーザ ID の確認後、パスワードの入力とユーザ認証を行う。なお、モバイル端末向けのパスワードとしてすでに TAB[1] や OBIR[2] のグラフィカルパスワードを提案している。

## 2 グラフィカルユーザ ID の関連研究と要件

IDLS はグラフィカルパスワード DAS からヒントを得た。Jermyn ら [3] が提案した DAS では、まず、ユーザは用意したグリッドに絵を描き、パスワードとして登録する。また、絵を描く際、線の描かれた順序を記録する。そして、ユーザは登録した絵を同じグリッド上に正しい順序で描くことでユーザ認証を行う手法である。しかし、DAS はパスワード認証で使用するため、描いた絵が複雑になる。また、パスワードは他人に見られてはいけないため、高いセキュリティが必要となる。そのため、ユーザが線を描画する回数が増加し、ユーザの手間と記憶負担が大きくなる。

**IDLS: New Graphical User ID Scheme for Mobile Services based on a Line Drawing Method**

Yusuke MATSUNO<sup>†</sup>, Hung-Hsuan HUANG<sup>†</sup>, Kyoji KAWAGOE<sup>†</sup>

<sup>†</sup>Ritsumeikan University

グラフィカルユーザ ID は、英数字列のユーザ ID に置き換わる新たな概念である。このため、グラフィカルパスワードへの要件と異なる下記の要件を満たすように構築する必要がある。

1. 組み合わせ数: Web サービスのユーザ数に相当する組み合わせ対応する必要がある。
2. 安定かつ効率的な確認: ユーザ ID を格納するユーザデータベースのサイズはできる限りコンパクトで、確認作業も短く、かつ安定した確認ができればならない。
3. 記憶容易性: 失念したとしてもすぐに思い出すことができる仕掛けを持つ必要がある。
4. 伝達容易性: メモやメール等でユーザ ID を伝えることができる形式でなければならない。なお、盗まれては困るパスワードと異なり、ユーザ ID だけが盗まれても被害にあることはない。

本稿で提案する IDLS は、上記の要件を満たすグラフィカルユーザ ID として設計を行った。特に、ユーザ手間の削減と伝達容易性を考慮した。その内容を次章で説明する。

## 3 グラフィカルユーザ ID IDLS

IDLS (graphical user-ID by Line Sketching) は、モバイル端末におけるユーザ ID 入力の手間の削減と記憶負担の低減と伝達容易性を実現することを目的とした新しいグラフィカルユーザ ID である。

### 3.1 IDLS (graphical user-ID by Line Sketching)

IDLS を用いたシステムではユーザ ID の登録とユーザ ID を認証する二つの機能を提供する。

ユーザは、指定された領域に線を描くことで、その線の軌跡をユーザ ID として登録する。ユーザ認証時には、ユーザは登録済みの軌跡を描き、システムはユーザの軌跡とユーザ ID データベース内の軌跡とのマッチングを行うことでユーザ ID 登録有無をチェックする。

軌跡で表現されたユーザ ID は、軌跡の特徴に変換され、変換されたテキストとしてユーザ ID データベース内に格納する。軌跡の特徴化には様々な方法が考えられるが、今回の IDLS では、もっとも単純な方法を採用する。すなわち、軌跡を描く領域内に設定したグリッド列を特徴とする。

グリッドに変換する際に、グリッドとグリッドの間を通った場合、人の目には判断しづらい。そのため、線が通ったグリッドに印をつけることで、どこのグリッドを通っているのかをユーザが把握することを可能とする。また、記憶負担の削減および伝達容易性の向上のために、軌跡の通ったグリッドをテキストに変換すると同時にユーザデータベースに格納する。これにより、格納しているユーザは、格納しているテキストと同じテキストを再現することでユーザ認証を行うことが可能となる。さらに、これらの工夫の結果、登録した軌跡と同じグリッドを通っているならば、全く同じ軌跡を描く必要はない。

ユーザがユーザ ID の登録と認証の際に描いた軌跡と変換されたテキストを図 1 に示す。

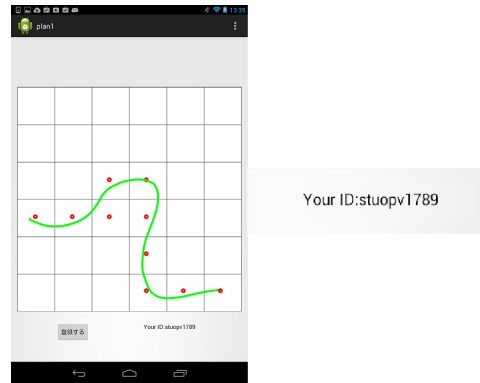


図 1: IDLS での描いた軌跡と変換されたテキスト

### 3.2 ユーザ ID の登録

ユーザ ID の登録の流れは以下の通りである。

- [Step1] ユーザ ID 登録ボタンを選択する
- [Step2] モバイル端末の画面に表示されたグリッド内においてユーザが自由に決めたグリッドをなぞる
- [Step3] 入力したユーザ ID がすでにデータベース内に登録されているかチェックする
- [Step4] 表示された線の軌跡をユーザ ID としてデータベースに登録する

Step3 において、データベース内に登録されているかチェックする際、すでに入力したユーザ ID が登録されていた場合はエラーを返す。

### 3.3 ユーザ ID の確認

ユーザ ID の確認の流れは以下の通りである。

- [Step1] ユーザ ID 確認ボタンを選択する
- [Step2] モバイル端末の画面にユーザの登録した軌跡を描く
- [Step3] データベース内で確認を行う
- [Step4] ユーザ ID が確認された場合パスワード入力画面へ移行する

## 4 評価実験

### 4.1 評価実験の内容

N 人の被験者には IDLS を用いたユーザ ID と英数字入力を用いた二種類のユーザ ID を登録しておく。その後、モバイル端末で各人のユーザ ID の入力を行い、入力時間と確認エラー率を測定する。このときの作業を以下に示す。

1. ユーザはユーザ ID を自分で決める。
2. 平均 7 文字のユーザ ID が基本的な ID として利用されていることが多いことを考慮し、英数字によるユーザ ID はランダムな入力 7 文字とする。
3. ユーザによる入力実験回数はユーザ ID ごとに 3 回として入力を繰り返す。

### 4.2 評価実験の結果

今回は予備実験として N=2 として実験を行った。表 1 に示す実験結果から IDLS の入力平均時間は英数字入力に比べて少ない。また、確認エラー率は IDLS と英数字入力の両方で 0% となった。確認エラー率についてはさらに被験者を増やし、より正確なデータを計測する予定である。

表 1: 評価結果

	入力平均時間 (s)	確認エラー率 (%)
IDLS	4.07	0.0
英数字入力	6.98	0.0

## 5 おわりに

本研究では、モバイル端末でのユーザ ID の入力時間の削減と、ユーザへの記憶負担の軽減を目的とした新たなユーザ ID とその入力方法として IDLS を提案した。今後はより確認エラー率の少ない、かつ記憶負担の小さい軌跡特徴への改善を行う予定である。

## 謝辞

本研究の一部は文部科学省私大戦略的研究基盤形成支援事業 ('13-'17) の助成を受けた。

## 参考文献

- [1] Kyoji Kawagoe, et al. : Tag Association Based Graphical Password Using Image Feature Matching, DASFAA2012, pp. 282-286. (2012)
- [2] Cuong Xuan Nguyen, et al. : Graphical Password using Object-based Image Ranking, ACM CSS2013, Poster session, 4-8, (2013).
- [3] Ian, Jermyn, et al. :The Design and Analysis of Graphical Passwords, USENIX1999, pp. 1-1(1999).