スマートフォン利用時の誤入力傾向に基づいたパスワード生成手法の検討
Study on Generating Passwords based on Mistype Tendency on Smartphone

小倉 加奈代†，鳥越 大地‡
Kanayo Ogura, Daichi Torikoshi
†岩手県立大学，‡株式会社アイシーエス
Iwate Prefectural University, ICS Corporation
ogura_k@iwate-pu.ac.jp

概要
本稿では，スマートフォン上で誤入力の起こりにくいパスワードを生成することを目標とし，スマートフォンにおけるパスワード入力過程と誤入力傾向の分析結果に基づき，誤入力が少ないと予想される「左右に何度も操作指が行き来しない」パスワードを試作し，その有効性を評価した．その結果，試作したパスワードが，左右に操作指が行き来するパスワード，ランダムな文字列で作成したパスワードよりも誤入力数，入力時間，ユーザの入力しやすさの点で優れたパスワードであることを確認した．

キーワード：パスワード，スマートフォン，誤入力，ユーザビリティ，ユーザ行動

1. はじめに

パスワード入力フォームの多くは，秘匿性を保つため，入力パスワードを黒丸やアスタリスクを用いた伏せ字として表示する．しかしこの状況が，パスワード入力ミスの原因の 1 つであり，Web サイトのユーザビリティ研究の第一人者であるニールセンも，入力パスワードを伏せ字として表示することは「フィードバックをユーザに提供し，システムの状況を視覚化するという原則に反している」と述べている[1]．この問題に対し，PC 利用時のパスワード入力場面を対象とした入力ミスが起こりにくいパスワード生成手法[2][3]や，入力ミスを適度に許容するパスワード認証手法[4][5]が提案されてきた．しかし，スマートフォン上でのパスワード入力を考えた場合，スマートフォンでも使用率の高い iPhone では，PC 利用時と同じ qwerty 配列の仮想キーボードを利用するが，PC 利用時では物理的キーボードを利用するため，操作感に大きな違いがあり，PC 利用時を対象とした従来手法をそのまま適用できる可能性は低いと考えられる．実際，PC で利用する両手入力の物理的キーボードを模す 4 種類のサイズの異なる仮想タッチスクリーンキーボード用いた際の筋肉や手首の動き，タイピングしやすさや効率を分析・検討した研究[6]では，サイズの小さなキーボードではタイピング速度が遅くなることが確認されており，物理的キーボードと仮装キーボードの操作感の違いによる影響が報告されている．

本研究では，スマートフォン特有のパスワード入力状況について考慮した上で誤入力の少ないパスワードを生成することを最終目標とする．そのために本稿では，著者らが実施した先行研究[7]であるスマートフォンにおけるパスワード入力過程と誤入力分析の結果をもとに，誤入力が起こりにくいパスワードを試作し，誤入力状況およびユーザの入力しやすさ，安全性を評価する．

2. スマートフォンにおける文字入力

近年，スマートフォンの普及に伴い，PC だけではなくスマートフォンでもパスワードを入力する機会が増えている．スマートフォンでのパスワード入力は PC のキー配列とほぼ同じ qwerty 配列の仮想キーボードで行われることが多い．

スマートフォンを含めた携帯情報端末を利用する場合，多くのユーザが片手操作を好むことがわかっており[8]，特に片手親指操作時のタッチ特性について調査した研究も存在する[9][10]．これらの研究の結果として，親指を自然に伸ばした状態で届く位置のタッチ精度が高く，反対に，親指の届きにくい位置のタッチ精度が低い傾向にあることが示されている．

この結果に対し，スマートフォンの片手操作を改善する研究[11][12][13]はあるが，両手で入力する等，片手操作以外の方法で入力しにくさ解消する場合も考えられる．実際，先行研究で，iPhone5s（4 インチ，幅 58.6 mm，高さ 123.8 mm）と iPhone8Plus（5.5 インチ，幅 78.1 mm，高さ 158.4 mm）を用いて，大学生 20 名に qwerty 配列キーボードで文字入力を行なった際の使用

手指について調査したところ，両手持ちで入力するユーザが iPhone5s では 3 名，iPhone8Plus では 10 名という結果であった. PC 入力での使用手指による影響の分析[14]と同様に, スマートフォン入力でも使う指や持ち手，端末の大きさといった入力に影響する要因が多くあると考えられる．例えばサイズが大きい端末は小さい端末に比べて指の動く距離が長くなるため，ミスが増加し，端末の持ち方が右手持ちの場合，左側のキーにミスが多くなることが推測できる．このように PC 入力よりも多くのミスの原因が考えられ，スマートフォン特有のパスワード入力状況について考慮する必要がある.

3. 先行研究：スマートフォンでのパスワード誤入力原因の分析

先行研究[7]では，ユーザの端末の持ち方，使用する端末の大きさにより，パスワード入力ミスの数，ミスの種類に違いがあると考え，(1)端末が大きくなると指の移動量が増えるため，ミスが多くなる，(2)片手持ちの場合，持ち手とは反対側にあるキー（右手持ちの場合は左側）のミスが多くなる傾向があるという 2 つの仮説を立て，これら仮説を検証するために，端末のサイズによってミスの割合が変化するか，また，端末の持ち方によってミス箇所に偏りが出るかの 2 点に焦点をあて，パスワード入力データ収集実験を行い，収集データの分析を進めた.

パスワード入力データ収集実験として，情報系学部に所属する大学生 20 名に，実際のログイン画面を模した実験用アプリケーション（図 1）に，自身のメールアドレスと「パスワード:」部分に表示される文字（実験用パスワード）を入力させ，その際の入力履歴データ（打鍵時刻と打鍵したキー）を収集した．使用端末は，iOS 端末においてサイズ差が大きい iPhone5s (4.0 インチ)と iPhone8Plus(5.5 インチ)と使用した. 入力時のキーボードの種類は，1 章で述べたように，iOS のパスワード認証では，qwerty 配列キーボードで入力する必要があるため，qwerty 配列キーボードを利用した．端末の持ち方については，被験者に事前アンケートにて通常時の持ち方を尋ね，実験開始時に事前アンケートに記入した持ち方で入力するよう指示した．また，入力パスワードは，英大小文字（52 語），数字（10 語），記号（33 語）の計 95 語を用い，「パスワードに類する文字列」，「ランダムな文字列」の 2 種類を用意し，95 語の文字を 2 回使うようなパスワード群を 2 種類（190 文字を 2 グループ）作成した.「パスワードに類する文字列」の作成方法は，那須川ら[3]のフレーズパスワードを変更したものや，SplashData[15]が公表した「最悪のパスワード 100」を参考に作成した.

図 1 実験用アプリケーションユーザインタフェース

収集データの分析では，端末の大きさごとのミス割合，それぞれの大きさにおける端末の持ち方ごとのミス割合を調査した． 分析結果として，仮説(1)については，仮説とは逆で，端末サイズの小さい方がミス割合は高くなることを確認した．この結果について，入力キーの分析より，端末サイズが大きい iPhone8Plus は，iPhone5s よりも隣接キーの誤入力が減少していることが関係していると考えられる．また，仮説(2)については，片手持ちの場合，持ち手とは反対側にあるキー（右手持ちの場合は左側）のミスが多くなる傾向があるという仮説を支持する結果となった．これについて，各持ち方各操作手指のミス分布を分析したところ，iPhone5s の右手持ち右手親指入力（図 2），iPhone5s の左手持ち左手親指入力（図 3），iPhone8Plus の両手持ち両手操作（図 4），iPhone8sPlus の両手持ち右手操作（図 5）に顕著な特徴が見られた.

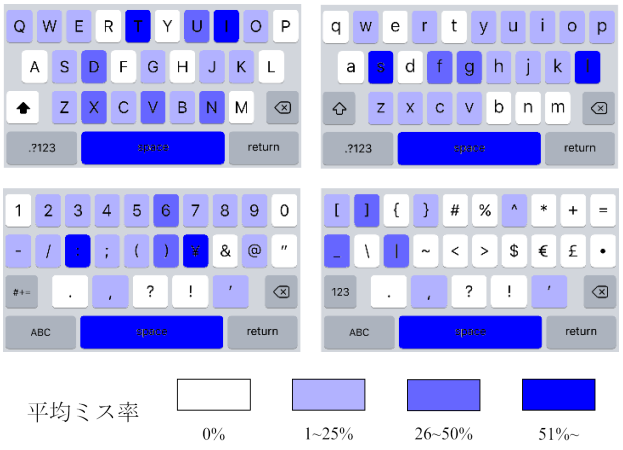
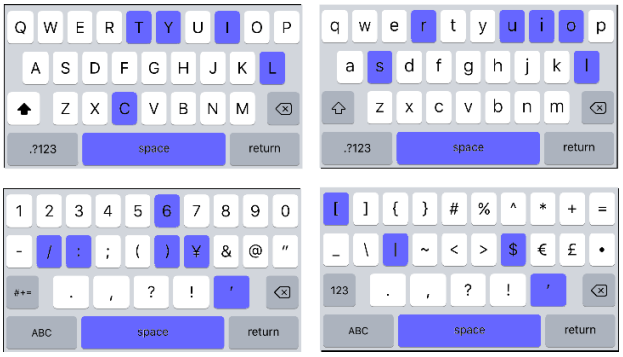


図 2：iPhone5s の右手持ち右手親指入力のミス分布図 (N=13)



（データが少ないため色の濃淡はなし）

図 3：iPhone5s の左手持ち左手親指入力のミス分布図 (N=2)

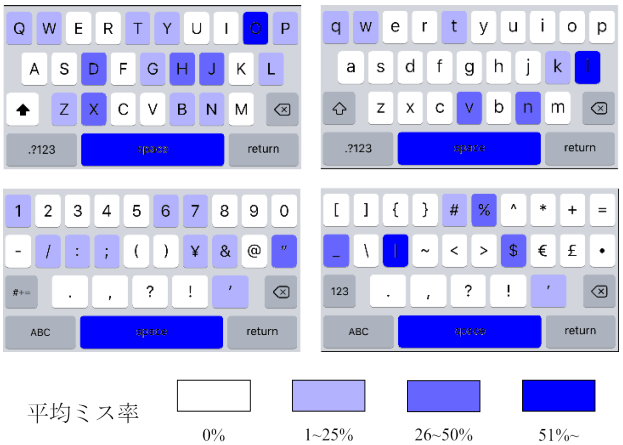
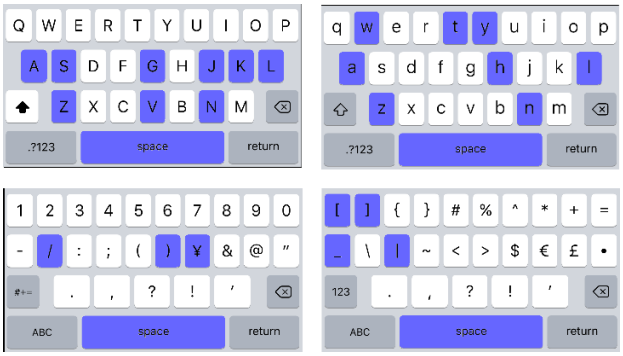


図 4：iPhone8Plus の両手持ち両手入力のミス分布図 (N=6)



（データが少ないため色の濃淡はなし）

図 5 iPhone8plus の両手持ち右手入力のミス分布図 (N=4)

4. 先行研究をふまえたパスワード生成方針の検討

先行研究での端末の持ち方と操作する指に関する分析結果より，スマートフォンで利用するパスワードを生成する際に，操作する手と離れた位置にあるキーを使わないパスワードを生成することで入力ミスが起こりにくくなると予想できる．しかし操作する手と同じ側に位置するキーを使う場合，パスワードに使用する文字の種類が少なくなり，安全面に問題が生じる．使用文字の種類が少ないと，総当たり攻撃を想定した場合，組み合わせ数も減るために突破される可能性が上がり，辞書攻撃を想定した場合でも，辞書内の単語数が少なくなることで突破される可能性が高くなる．この安全性の問題を解決するために，左右に何度も指が往復しないパスワードを生成することができれば，入力しやすく，かつ，安全性の点で問題がないパスワードが生成できる．

5. 操作手指を考慮した試作パスワード評価実験

前述のように，左右に何度も指が往復せず，記憶しやすい，かつ，安全性の点で問題のないパスワードとして，「miniTEC142」，「23Dashbomb」の 2 つのパスワードを試作した．いずれもパスワード強度チェッカーzxcvbn[16]において「許せる」の評価であり，安全性の点で問題がないことを確認済みである．

試作したパスワードの誤入力状況と入力しやすさを評価するために，試作した 2 つのパスワードである「パスワード A：左右に指が往復しないパスワード」の他，

「B : 操作指が左右に何度も往復するパスワード」, C : ランダムなパスワード」の 3 種類(1 種類につき 2 つ), 合計 6 つのパスワードを用意し, 被験者 6 名にこれらのパスワードを入力してもらい, 実験後に 3 種類のパスワードのうちどのパスワードが入力しやすかったかを調査した. 使用端末は, iPhone5s で, パスワードの入力順は, 6 名中 3 名が A→B→C の順で入力し, 残りの 3 名が, C→B→A の順で入力した. なお, 実験で使用した 3 種類合計 6 つのパスワードを以下に示す.

表 1 : 実験用パスワード 3 種類（全て 10 文字）
(1 種類につき 2 つ, パスワード A が試作パスワード)

	1 つ目	2 つ目
パスワード A	miniTEC142	23Dashbomb
パスワード B	tomaYAMA01	cinema92A
パスワード C	chGhMB6yLS	r8yziWNbge

6. 試作パスワード評価実験結果

3 種類のパスワードの誤入力数を表 2 に示す. なお, 誤入力数は, 1 つのパスワード内に誤って入力した文字数をカウントした. また, 3 種類のパスワードの平均入力時間を表 3 に示す.

誤入力数については, 表 2 より, 試作パスワードである A とランダムに作成した C の誤入力数が同じであり, 試作パスワードの対称形である, 操作指が左右を行き来するパスワードのミスが一番多かった. また, 表 3 より, 被験者単位でそれぞれのパスワードの誤入力数を比較すると, 試作パスワードである A について誤入力がなかった被験者は 6 人中 4 人, パスワード B と C はそれぞれ 3 名であった.

平均入力時間については, 表 4 より, パスワード A の入力時間が最も短く, 誤入力数が同じであるパスワード A と C では A の方が 4 秒以上速いという結果であった.

事後に被験者に尋ねた 3 種類のうちどのパスワードが最も入力しやすかったかという質問の回答結果については, 試作パスワード A と左右に指が何度も往復するパスワード B が 3 名ずつ, ランダムなパスワード C を選んだ被験者はいなかった.

これらより試作した, 操作指が左右に行き来しないパスワードは, 誤入力が全く起こらなくなることはなかったが, 操作指が行き来するパスワードより誤入力は少ないこと, 入力速度は, 操作指の行き来するパスワード, ランダムパスワードよりも速く入力できること, ユーザの主観的な入力しやすさについても概ね入力しやすいことがわかった.

表 2 パスワード別誤入力数

	誤入力数
パスワード A	4
パスワード B	7
パスワード C	4

表 3 被験者別誤入力数

	パスワード A	パスワード B	パスワード C
被験者 1	0	2	0
被験者 2	0	0	0
被験者 3	0	0	2
被験者 4	0	0	1
被験者 5	3	1	0
被験者 6	1	4	1

表 4 パスワード別平均入力時間

	平均入力時間（秒）
パスワード A	12.3
パスワード B	13.3
パスワード C	16.7

7. まとめと今後の課題

本稿では, スマートフォン上で誤入力の起こりにくいパスワードを生成することを目標とし, 先行研究であるスマートフォンにおけるパスワード入力過程と誤入力原因分析結果より, 誤入力が少ないと予想される「左右に何度も操作指が行き来しない」パスワードを試作し, パスワードの安全性（強度), 誤入力数, 入力時間, ユーザの主観的入力しやすさを評価した.

安全性については, 操作指が左右に行き来しないようにすることは, 使える文字種が制限されることになるが, 実用に耐えうる強度のパスワードの作成可能であることを確認できた. 試作パスワードの入力実験結果からは, 試作したパスワードの誤入力が全く起こらなくなることはなかったが, 左右に操作

指が行き来するパスワード，ランダムな文字列で作成したパスワードと比較すると，誤入力数，入力時間，主観的入力しやすさの点で同等もしくは優れたパスワードであることを確認できた．

今後は，記憶保持性の調査を進めるとともに，今回実験で使用したパスワードが，通常使用するパスワードと同様に完全に記憶された状況で入力されている状況ではなかったため，通常使用するパスワードと同様の状況下で実験を進める予定である．また，現状，本研究は，パスワードを自動生成する前提で進めているため，高橋らの研究[17]のように，ユーザがどのようなパスワードを作成する傾向にあるのか，どのようなパスワードを好むのかという観点を取り入れていない．記憶保持性を高める上でユーザ側のパスワード生成の傾向を考慮することは重要であると考えるため，今後は，ユーザ側の生成傾向を取り入れた手法を検討したい．

文献

[1] Jacob Nielsen, (2009), Stop Password Masking, Nielsen Norman Group (online), available from <https://www.nngroup.com/articles/stop-password-masking/> (accessed 2019-07-04).

[2] 藤原咲子, 小倉加奈代, ベッド.B.ビスタ, 高田豊雄, (2017) “タイピングミスの傾向に基づいたパスワード作成手法の検討”, 日本認知科学会第 34 回大会発表論文集, pp.876-881.

[3] 那須川至，小倉 加奈代 , Bhed Bahadur Bista , 高田 豊雄, (2018)“打鍵ミスを考慮したおとり用パスワード管理ツールの提案”, 情報処理学会第 80 回全国大会講演論文集, 2018(1), pp.497-498.

[4] 宮代理弘，宮下芳明，(2015) “打ち間違えを適度に許容するパスワード認証の提案”, 第 23 回インタラクティブシステムとソフトウェアに関するワークショップ論文集 (WISS2015), pp.117- 118.

[5] 小林怜央，黒米祐馬，武田圭史，村井純，(2017) “誤入力の傾向を考慮した Levenshtein 距離による柔軟なパスワード認証システム”, 情報処理学会第 79 回全国大会講演論文集，2017(1)，pp.565-566.

[6] J.H. Kim, L. Aulck, O. Thamsumwan, M.C.Bartha and P.W.Johnson, (2014) “The Effect of Key Size of Touch Screen Virtual Keyboards on Productivity, Usability, and Typing Biomechanics”, The Journal of the Huma Factors and Ergonomics Society, 56(7), pp.1235-1248.

[7] 鳥越大地 , 小倉加奈代 , Bhed Bahadur Bista , 高田 豊雄, (2019) “スマートフォンにおけるパスワード入力過程の分析と誤入力原因の検討”, 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）, 2019-HCI-181(4)，pp.1-7.

[8] A. Karlson, B. Bederson and J.Contreras-Vidal, (2006) "Understanding Single-Handed Mobile Device Interaction", Tech Report HCIL-2006.

[9] Y.S.Park and S.H.Han, (2010) "Touch key design for onehanded thumb interaction with a mobile phone: Effects of touch key size and touch key location", InternationalJournal of Industrial Ergonomics, Vol. 1, No. 40, pp.68–76.

[10] 松浦吉祐，郷健太郎，(2007)“小型タッチ画面における片手親指の操作特性”, ヒューマンインタフェース学会論文誌, Vol. 9(4)，pp.455-461.

[11] S. Boring, D. Ledo, X. A. Chen, N. Marquardt, A. Tang and S. Greenberg, (2012) "The Fat Thumb： Using the Thumb’s Contact Size for Singlehanded Mobile Interaction", Proc. of the 14th international conference on Human-computer-interaction with mobile devices and services (MobileHCI 2012), pp.39-28.

[12] N.Yu, D.Huang, J.Hsu and Y.Hung, (2013)" Rapid Selection of Hard-to-access Targets by Thumb on Mobile Touch-screens", Proc. of the 15th international conference on Human-computer-interaction with mobile devices and services (MobileHCI 2013), pp.400-403.

[13] 日高詩織，馬場哲晃，(2016)“大画面スマートフォンにおける片手操作を補助する為の背面入力装置”, 情報処理学会インタラクション 2016 論文集，pp.567-569.

[14] A. M. Feit, D. Weir and A. Oulasvirta, (2016) "How We Type：Movement Strategies and Performance in Everyday Typing", Proc. of the 2016 CHI Conference on Human Factors in Computing Systems(CHI2016), pp.4262- 4273.

[15] Splashdata, (2017) "100 Worst Passwords of 2017! The Full List" (online), available from <https://www.teamsid.com/worst-passwords-2017-full-list/> (accessed 2019-07-04).

[16] AGILE，(2015) “パスワード強度チェッカー(zxcvbn) ”, 入手先<https://www.agilegroup.co.jp/technote/zxcvbn.html>（最終閲覧日 20190704）

[17] 高橋優，上田卓司，(2016)“大学生の用いるパスワードの強度と管理状況", 情報処理学会論文誌教育とコンピュータ，vol2(2)，pp.1-9.