# 打ち間違えを適度に許容するパスワード認証の提案

宮代 理弘 * 宮下 芳明 †

**概要.** Web サービスなどパスワード入力フォームのほとんどは，伏せ字によってパスワードの秘匿性を保っている．しかし，ユーザがパスワードを正確に覚えていたとしても入力し間違えることがあり，その秘匿性ゆえに気づくことができず，認証に失敗することがある．そこで本稿では，パスワード認証において打ち間違えを適度に許容することで，ユーザが認証に成功しやすくする手法を提案し，実験を行うとともにその有効性を議論する．

## 1 はじめに

パスワード入力フォームには，秘匿性が必要である．これは，いわゆる “ショルダーハック” を防ぐためである．そのためパスワード入力フォームでは，値が黒丸などの伏せ字になるフォームが普及しているが，ユーザも打った文字をユーザが把握できない問題点がある．このような状況下では，ユーザは打ち間違えを確認することができない．よって，打ち間違えがあるまま送信されることが多いと推測される．

ユーザが人間である限り何かしらの間違えは起こりうる．それらに対して許容や補正をするといったシステムは多く提案されている．例えば検索エンジンの Google は，クエリの間違えを推測し，修正したクエリの検索結果を返す機能を有している．

本稿ではこれらの考え方を基に，伏せ字フォームでの打ち間違えを適度に許容するパスワード認証手法を提案する．例えば “PassW0rd!” というパスワードに対して，“Passw0rd!” や “PassW0ed!” と打ち間違えても許容する．ここで想定する打ち間違えとは，正確にパスワードを記憶している上でユーザがキーボードで押すキーを間違えてしまうことである．

## 2 予備実験

“入力値が伏せ字になるフォームでは送信される値の間違えが増える” という仮説について実験を行った．入力フォームが 50 個ある Web ページを用意し，2 種類の実験で異なる任意の文字列を入力し続けるタスクを課した．これらの実験を入力値の見えるフォームと伏せ字になるフォームで行った．また，任意でパスワード文字列長のアンケートも実施した．

実験 1 では，英大小文字・数字・記号を含む 8 文字の文字列，“PassW0rd!” を入力させ，“認証試行回数に対する，間違えと認識された回数の割合”（以下，エラー率）を調べた．被験者は，キーボード操作に慣れた 18 歳から 21 歳の男女 11 人である．

表 1. 複雑な文字列による実験結果

| | 見える | 伏せ字 | t 値 |
|---|---|---|---|
| エラー率 | 4.73% | 10.6% | 2.65 |

表 2. 入力に慣れている文字列による実験結果

| | 見える | 伏せ字 | t 値 |
|---|---|---|---|
| エラー率 | 0.00% | 4.00% | 4.66 |

実験 2 では，普段利用しているパスワードを入力させ，エラー率を調べた．この際，被験者には事前に実験の内容について説明を行い，同意を得たうえ実施した．実験フォームは，間違えたタイミングとそのときのレーベンシュタイン編集距離のみがデータとして出力される．被験者は，キーボード操作に慣れた 18 歳から 21 歳の男女 7 人である．

### 2.1 実験結果

実験結果は表 1，表 2 のとおりである．どちらの実験も t 検定を行った結果，有意水準 5%で伏せ字のエラー率が有意に高かった．

実験 2 における間違えたときの編集距離については，とくに大きい値となった標本を排除すると，標本数 12，最大 2，平均 1.5，標準偏差 0.5 であった．

パスワード文字列長についてのアンケートには，13 人の被験者が回答した．文字列長は最低 8 文字，最高 15 文字，平均 10 文字，標準偏差は 2.3 となった．

パスワード入力値が黒丸などの伏せ字になるフォームでは，有意に打ち間違えが起こりやすいといえる．また，実験結果からユーザが入力し間違える主なパターンとして，「Shift キーを押し間違える，押し忘れる」，「キーボード上で押したいキーの左右にあるキーを押す」が挙げられる．今回の実験では，これらの打ち間違えパターンが同時に起こるケースはなかった．



* 明治大学総合数理学部先端メディアサイエンス学科
† 明治大学

表 3. 伏せ字フォームに提案手法を適応した結果

| | 提案手法 | 従来 | t 値 |
|---|---|---|---|
| エラー率 | 6.36% | 10.6% | 2.57 |

## 3 提案システム

提案システムでは，打ち間違えがあるパスワードが入力されても，正しいパスワードとして認識する．しかし，すべての文字に対して打ち間違えを許容しては，パスワードのパターン数が激減してしまうため，実験 2 での編集距離を参考に 1 文字まで許容することにする．また，許容する打ち間違えの範囲は 2.1 で挙げた 2 パターンのいずれかとする．例えば，QWERTY 配列で “W” は “Q”，“E”，そして “w” が許容の対象になる．

本提案手法の認証手順については，兼子らの総当り試行を利用した Entropy-Enhanced Password 認証 [1] を基にする．これはクライアント側でパスワードの一部を総当り試行する認証方式である．

実験データのうち，伏せ字フォームに入力した値に対して提案手法に基づく許容を行った場合について検証した（表 3）．t 検定を行った結果，有意水準 5%で間違えと判定された割合は有意に減少した．しかし，提案手法を適応しても変化がなかった被験者が 2 人いた．これらについても一定の効果が見られるように許容手法を改善していく必要はある．

## 4 議論

Dinei らはオンライン認証において，パスワードは $10^6$ 以上の推測を必要とする強度があれば十分としている [2]．これは英大小文字 52 種類を使い，4 文字以上でパスワードを構成していればよいことを意味する．また，古原らの提案する認証方式 [3] ではパスワード漏洩にも強い耐性がある．よってオンライン認証においては，パスワード自体の乱雑さを従来より高める必要はないと考えられる．

打ち間違え許容によって，ランダムに生成した文字列とパスワードが合う確率（以下，ヒット率）は元のパスワードより上昇してしまう．ヒット率の差異が無視できる程度になるよう，文字列長を長くした新しいパスワードを生成するべきである．

2.1 の入力間違えパターンによると，1 英文字につき大小文字・キーボード配列左右の 4 種類の入力がありえる．文字列のうち，1 文字だけを 4 種類いずれかで許容するとき，文字列長を $N$ として $4N$ でパターン数が求まる．

以下，パスワードが英大小文字の 52 種類で構成されているとする．間違えを許容したときのヒット率は，文字列長を $N$ として $\left(\frac{1}{52}\right)^N \times (4N)$ である．

通常の方式でのヒット率は $\left(\frac{1}{52}\right)^N$ であるため，元のパスワードの文字列長を $N_{original}$ としたとき，次の不等式が成立する $N_{new}$ を求めればよい．

$$\left(\frac{1}{52}\right)^{N_{original}} - \left(\frac{1}{52}\right)^{N_{new}} \times (4N_{new}) > 0$$

仮に元の文字列長を 10 とした場合，元のヒット率より間違えを許容したときのヒット率が低くなるためには，文字列長を 1 増やすだけでよい．また，元の文字列長を 15 とした場合は，文字列長を 2 増やすだけでよい．2.1 のアンケート結果から考察すると，2 文字増やすことで問題は解決する．

また，許容する文字種についても議論の余地がある．実験では，2.1 で述べた打ち間違えパターン以外にも顕著に見られるパターンがあった．“O（アルファベットのオー）” と “0（数字のゼロ）” の打ち間違えといった，視覚的に類似する文字の打ち間違えである．視覚的類似を利用した文字置換で生成されたパスワードは，許容すると一般的な英単語になりやすく，攻撃者に推測されやすくなる．視覚的類似を利用した文字置換は，パスワードをパスワードたらせる一因を大きく担っているといえる．よって，このような視覚的類似にあたる文字の打ち間違えについては本提案手法では許容しない．

## 5 まとめ

入力値が伏せ字になるパスワードフォームにおいて，ある程度の間違えを許容することにより，認証の失敗を減らすことが可能になった．しかし，パスワード文字列への間違え許容については，セキュリティの観点からさらなる検証が必要である．文字列以外の認証方式も数多く提案されているが，システム移行のコストを考慮すると文字列認証方式が続いていくと思われる．本提案手法についてもシステム移行のコストを今後検証していきたい．

## 謝辞

本研究は JST，CREST の支援を受けたものである．

## 参考文献

[1] 兼子拓弥, 本部栄成, 西垣正勝. 総当り試行を利用した Entropy-Enhanced Password 認証, 情報処理学会研究報告 2012-CSEC-58/2012-SPT-4, Vol.2012, No.47, pp.1-5, 2012.

[2] Dinei Florncio, Cormac Herley, Paul C. Van Oorschot. An administrator’s guide to internet password research, In *Proc. LISA’14*, pp.35-52, 2014.

[3] 古原 和邦, 辛 星漢. 漏えいに強いパスワード認証とその応用－短いパスワードを許容しながら情報漏えい耐性を実現－, Synthesiology, Vol.7, No.3, pp.179-189, 2014.