情報処理学会論文誌 Vol.57 No.12 2723–2730 (Dec. 2016)

社会的影響を考慮したパスワード強度メーターの提案

大山 敬博[1] 金岡 晃[1,a)]

受付日 2016年3月10日, 採録日 2016年9月6日

概要：サービスへの登録を行うときにパスワード強度メータが多くの状況で利用されている．パスワード強度メータの効果についてはいくつかの視点で研究が行われてきているが，より効果的な手法が考えられる．近年，ユーザがセキュリティの機能を適用するにあたって社会的影響（Social Influence）が強くユーザの振舞いに影響を与えることがDasらによって示された．本論文では社会的影響を利用したパスワード強度メータを5つ提案しその評価を行った．ユーザ評価の結果，強い社会的影響がある場合はより強い強度を持つパスワードを導くことが分かった．

キーワード：パスワード，社会的影響

Password Strength Meters using Social Influence

Takahiro Ohyama[1] Akira Kanaoka[1,a)]

Received: March 10, 2016, Accepted: September 6, 2016

Abstract: Millions of people now use password strength meter when the user starts to sign up a service. The impact on password strength meter has been evaluated for several aspects. However, it is believed that there are still ways to design more effective password strength meters. Recently, Das et al. shows that social influence or social proof is effective to adopt security features. In this note, we prepare five types of password strength meters using social influence and evaluate them. We conduct user study to measure effectiveness of proposed meters. The results show stronger social influence reflects stronger password strength.

Keywords: password, social influence

1. はじめに

パスワードは長い間電子認証の手法として広く利用されており，現在においても電子認証における主たる手法の位置を占めている．パスワード認証はユーザが簡単なパスワードを付けてしまう傾向があるなど，認証方式としての強度への問題点が示されており，この20年間で高い認証強度を持つ新たな方式など多くの電子認証方式が提案されてきた．しかしどれらも社会への展開においてパスワード認証を超える認証方法は出てこなかった[2]．一方で，パスワード認証を強化する試みも多く研究されている[4], [8], [9], [10], [11], [14], [16], [17], [18]．そこではパスワード構成ポリシやパスワード強度メータがパスワードの強化方法としてよく用いられている．

実際に，多くのサービスがユーザ登録時においてパスワード強度メータを利用している．パスワード強度メータはユーザにより強いパスワードを設定させる効果があることが示されており[11]，またさまざまな種類のメータが存在し，それらに対しての評価も行われている[8], [18]．しかし，それらの評価は既存の強度メータの評価が主であり，より効果的な強度メータ設計の余地は十分にある．

Dasらは社会的影響（Social Influence）あるいは社会的証明（Social Proof）がセキュリティの機能をエンドユーザが適用する際に影響を与えることを示した[5], [6], [7]．Dasらはソーシャルネットワーキングサービス（Social Netwroking Service，以下SNS）で友人関係にあるユーザ群の振舞いにより影響を受けることを示したが，社会的影響は直接の友人関係になくとも同一グループへの所属でも

[1] 東邦大学
Toho University, Miyama, Funabashi, Chiba 274–8510, Japan
[a)] akira.kanaoka@is.sci.toho-u.ac.jp

影響を受ける [19], [20]．社会的影響はパスワード強度メータの利用時にもユーザのパスワード強度に対する影響が与えると考えられる．Egelman らは部分的ではあるがその効果を示した [11]．

本論文では 5 つのタイプの社会的影響を利用したパスワード強度メータを提案し，その評価を行った．ユーザがパスワードを設定するときに同時に入力されることが多いユーザの属性情報を用いて，類似属性を持つユーザが平均的にどの程度の強度のパスワードを設定しているかをメータに表示させることにより，社会的影響をユーザにもたらすものである．表示方法はバーで表現する方法や数値を直接表示する方法，またアイコンを用いる方法など，5 つの種類を用意した．5 つの種類は，まず Das らの先行研究の結果に応じて，社会的影響がパスワード強度メータにも適用可能かを示すために一般的な表示方法に社会的影響の表示を加える 3 つのメータを提案した．Das らの結果の直接的な適用が困難な部分については，それをパスワード強度メータの特性に置き換えた表現に変更した．また Das らの結果にはなかった，視覚的な記号を利用して社会的影響を与えることを狙ったパスワードメータを 2 つ提案した．提案手法の評価としてユーザ実験を行い，それらパスワード強度メータ表示のもとで被験者がどれほどの強度を持つパスワードを設定したかを統計的に有意差を求め比較を行った．

本論文の構成は以下のとおりである．まず 2 章でパスワードに関連する研究について紹介と本論文で取り扱う社会的影響についての論文の紹介を行う．3 章では社会的影響を用いたパスワード強度メータの提案を行い，4 章では提案メータの評価に先駆けた事前実験について示す．5 章においてユーザ実験の詳細を述べ，6 章でそれらから得られた結果について議論を行う．最後に 7 章でまとめる．

2. 関連研究

2.1 パスワード

パスワード認証は電子認証の手法として長い間広い分野で使われており，現在でも広く用いられている．パスワードはユーザによる設定がされることなどから，ランダムなデータよりも情報量（エントロピー）が低いため，認証としての強度が低いことが指摘されており，パスワード認証よりも強度が高い手法などさまざまな認証方法が提案をされてきた．しかしそれらのいずれの手法もいまだパスワード認証にとって代わる手法になっていない．Bonneu らはこれまで提案されてきた多くの手法をパスワード認証と比較し，それらの多くが適用能力（Deployability）が低いことがパスワード認証に代わる存在になっていないことを示した [2]．

NIST SP 800-63-1 ではパスワードが持つ情報量についての記述があるが [3]，ユーザがパスワードを設定する場合のパスワードの統計的な偏りといった特徴を調査が行われ [1], [23]，これらの結果から情報量は短いパスワードではより小さく，長いパスワードではより大きいものであることが示された．その後，そういった特徴をパスワード推測攻撃に応用すること [23] などがされてきた．さらに，推測攻撃を応用し耐性を評価する手法として転用しパスワードを強化するための方策の評価として用いられることも多くなってきた [13], [18], [22]．

パスワード強度メータについては，メータ設置によりユーザのパスワード強度が上がることが Egelman らにより示されている [11]．しかし Carnavalet らはそれらの疑問を呈している [8]．その疑問については，Ur らが多くのパスワード強度メータの種類の整理とその効果についての大規模な調査を行い，効果を示したことで解消された [18]．メータの表示方法の違いやメータと強度の紐づけ方法の違いなど，複数のメータについてユーザ実験を行い，それらのメータ表示のもとで作成されたパスワード群がどれほど推測攻撃に耐性があるかの分析がなされた．

パスワード強度メータにおける強度の計算手法については，Ur らの研究 [18] ではパスワード構成ポリシに従ったポイント制，そして Egelman らの手法 [11] ではパスワード長と文字種数の対数の積，といったように手法が定まっているわけではない．これらの手法では，その強度の算出がそのパスワードが本来持つ情報量の正確な保証されているわけではない．パスワードの強度は，ある特徴を持つパスワード群がどれだけ推測攻撃に耐性を持つか，という視点で評価がされることが多い [13], [15], [18], [21], [22]．しかし，パスワードメータは与えられたパスワード単体がどれだけの強度を持つかを計算しなければならず，推測攻撃への耐性評価は計算に時間がかかるために直接的な適用はむずかしい．パスワード単体の強度計算についての議論は Castelluccia ら [4] や Dell'Amico ら [9] によって行われている．いずれも条件付確率をある程度間引いて行うことにより近似誤差が少ないまま計算量を少なくすることができるようになっており，ユーザがパスワードを入力している間に強度計算を行いメータ表示をすることが可能になっている．

また種々のパスワードに関する研究では，ユーザ実験が欠かせないものとなっているが，ユーザに実験を行わせる環境についての指摘がある．ユーザが非日常的な環境で作成したパスワードについては，本当のユーザの振舞いが反映されないことが，Fahl らによって指摘がされている [24]．パスワードに関連した研究でユーザ実験を行う場合には，そういった日常の環境に近い振舞いが期待できる生態学的妥当性（Ecological Validity）が求められる．

パスワードに関連する研究は近年になっても多く行われており，Florêncio らにより広範にまとめられている [12]．

2.2 セキュリティ機能に対する社会的影響

Das らは，セキュリティ機能をユーザが適用するにあたり，社会的影響や社会的証明が効果的であることを示した [5], [6], [7]．人間は公的機関が示す指標よりも，友人などの周囲の影響によりその振舞いが変わりやすいことを利用して，周囲のユーザがどういったセキュリティ機能を利用しているかを示すことでそのユーザに新たなセキュリティ機能の適用を促すことができるようになる．Das らの研究では SNS における 2 段階認証の適用について，SNS で友人関係にあるユーザ群の行動を用いて調査が行われた．一方でセキュリティ分野ではないものの，直接的な関係になくとも同一グループへの所属でも影響を受けることも分かっている [19], [20]．そこで本研究ではこれらの社会的影響は他のセキュリティ分野でも応用可能であると考え，パスワード強度メータに利用することとした．

3. 強度メータの設計

3.1 設計の方向性

Das らの研究により，セキュリティの分野においても社会的影響によりユーザの振舞いに変化が起こることが分かった．そこで，本論文では社会的影響がパスワード生成においても影響を与える，という仮定を置いた設計をすることとする．Das らの成果では，Facebook など「友人」という要素を持つサービスにおいて友人らがその機能を使っていることを社会的影響として実証実験を行っていた．パスワード強度メータの場合，主に利用されるのはユーザが新規登録をする際であり，その時点ではユーザの友人といった要素は利用できず，直接の適用はできない．一方で，ユーザが新規登録をする場合には，ログイン ID の設定とパスワード設定だけではなく，ユーザの個人的な情報を入力する．たとえば氏名，年齢，生年月日，性別等々が一般的である．実際 Alexa Top 50 のサイトでのユーザ登録を見ると，氏名は 58.3%，年齢は 41.7%，生年月日は 43.8%，性別は 37.5%，という情報が登録時のパスワード入力時あるいは入力前までに入力される．

本論文では，それらパスワードを入力されるときに同時あるいはその直前で入力されるユーザの属性情報を用いて，類似の属性を持つユーザを類似ユーザとして，類似ユーザがどういったパスワード強度を持っているかを示すことで社会的影響をユーザに及ぼすパスワード強度メータを提案する．

3.2 強度計算手法

パスワード強度の計算手法は Ur らの論文の手法に即した [18]．パスワードに入力がない（空欄）の場合は 0，そして最大は 100 としている．計算は *Basic16* と *Comprehensive8* の 2 種類の方法で行われ，双方の値で大きなものを強度とするものである．*Basic16* では，最初の 8 文字までに 4 ポイントがそれぞれに与えられ，その後は 8 ポイントずつが与えられる．*Comprehenxive8* では，それぞれの文字に 4 ポイントが与えられ，大文字，数字，記号が含まれていた場合は 17 ポイントが与えられる．異なる大文字，数字，記号が与えられた場合は 8 ポイントがさらに加算され，続いて 4 ポイントが加算される．また辞書データとして OpenWall Mangled Worldlist を用いて，そこに掲載されているパスワードと一致しなかった場合は 17 ポイントが加算される．

3.3 類似ユーザのスコア表示

類似ユーザのスコア表示のために，あらかじめある程度のユーザの属性とパスワード強度を保持しておく必要がある．そしてそれぞれの属性の組合せに対し，パスワードの平均強度を求めて，あらかじめデータベースとして保持しておく．そしてパスワード設定と同時に行われる属性入力に応じて，類似ユーザのパスワード平均強度を得て表示を行う．パスワードの平均強度は，データベースにおいて平均強度だけでなく平均を求めた際の総ユーザ数を記録しておくことで，新たなユーザが登録されることで再計算されることも可能である．その属性を持つ総ユーザ数を n，新たなユーザが追加される前の平均強度を S，新たなユーザのパスワード強度を x とした場合，新たなユーザが追加された後の平均強度 S' は以下のように計算される．

$$S' = \frac{S \times n + x}{n + 1} \tag{1}$$

3.4 強度メータの表示

社会的影響を利用したパスワード強度メータとして 5 つのタイプを提案する．

1 つ目はバータイプのパスワード強度メータである．これを「#1：Bar」と呼ぶこととする．2 つの強度メータが示され，片方はパスワードを入力しているユーザのスコアが表示され，もう 1 つは類似したユーザの平均スコアが示される（**図 1**）．類似ユーザは，年齢や業種など入力ユーザと同じ属性を持っているユーザを示している．

2 つ目もバータイプのものである．2 つの強度メータが示され，片方はパスワードを入力しているユーザのスコアが表示され，もう 1 つはユーザ全体の平均スコアが示される（**図 2**）．これを「#2：Bar（Avg.）」と呼ぶこととする．

3 つ目は強度スコアそのものを表示するものである．片方はパスワードを入力しているユーザのスコアが表示され，もう 1 つは類似ユーザの平均スコアが示される（**図 3**）．これを「#3：Score」と呼ぶこととする．

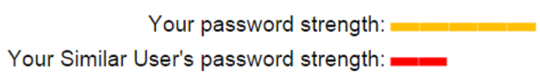

図 1 メータ#1: Bar
Fig. 1 Meter #1: Bar.

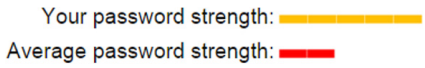

図 2 メータ#2: Bar（Avg.）
Fig. 2 Meter #2: Bar (Avg.).

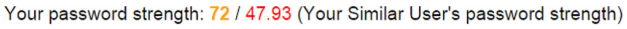

図 3 メータ#3: Score
Fig. 3 Meter #3: Score.

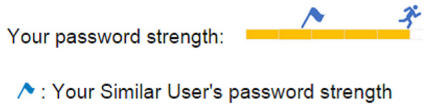

図 4 メータ#4: Running Man
Fig. 4 Meter #4: Running Man.

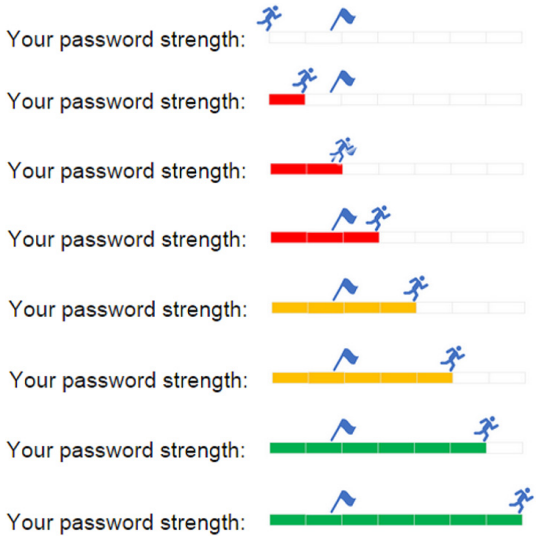

図 5 Running Man の表示
Fig. 5 Indication of Running Man.

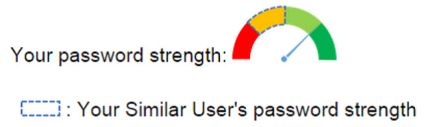

図 6 メータ#5: Tachometer
Fig. 6 Meter #5: Tachometer.

4 つ目はバータイプのメータを 1 つ用意し，そのメータ上にアイコンを 2 つ表示させる．走っている人間を模したアイコンはパスワードを入力しているユーザのスコアを示すものであり，旗のアイコンは類似ユーザのスコアを示すものである（**図 4**）．これを「#4：Running Man」と呼ぶ．**図 5** はそれぞれのスコアにおいてアイコンとメータがどのように表示されるかを示したものである．

5 つ目はタコメータタイプの強度メータである．パスワードを入力しているユーザのスコアが示され，類似ユーザのスコアはそのゾーンが枠で囲われる，という表示がされている（**図 6**）．これを「#5：Tachometer」と呼ぶ．

図 7 メータ#0: Basic
Fig. 7 Meter #0: Basic.

5 つのメータとの比較のために，基本的なメータとして「#0：Basic」を用意した（**図 7**）．

#1 と#3 は，Das らの研究結果 [6] をもとに，パスワード強度メータにおいても社会的影響がユーザの振舞いの結果であるパスワード強度に現れることを意図した．#2 は，#1 のメータの記載を類似したユーザの平均スコアから全体の平均スコアに変更したものである．社会的影響についての厳密な定義はここでは行わないが，おおまかに「他者による影響を受ける」という視点でとらえれば，「他者」の置き方が社会的影響の度合いの強さに現れると考えることができ，ここでは「類似したユーザ」から「全体」と他者の範囲を広げて社会的影響を#1 より抑えたものとした．

#4 と#5 は，視覚的な記号による社会的影響を示すパスワード強度メータとなっている．これらの社会的影響については Das らの論文では評価されておらず，一方で Ur らの論文では視覚的な記号によるパスワード強度向上効果が少ないことが示された．しかし Ur らの研究では視覚的な記号は単一の記号のみで評価がされており，また社会的影響を与える記号でなかったため，視覚的な記号がより強い社会的影響を与える可能性はまだあると考えられる．本論文では，視覚的な記号として，走る人間とゴールの旗を視覚的な表現として用いる#4 と，車などで身近な視覚的表現である#5 を取り上げ，その効果を測ることとした．

なおいずれの強度メータも，ユーザがキー入力をするたびにスコアを計算し逐次その表示を変更するものとした．

#0 から#4 までのメータは 0–100 までのスコアに従い 8 段階に分割されている．8 段階のうち 0 段階目はメータ表示なし，1–3 段階目は赤色，4–5 段階目は黄色，6–7 段階目は緑色，としている．#5 については，他のメータの 8 段階における 0 段階目をさらに分割した 9 段階となっており，0 段階目はスコア 0 のみを表示するものとなっている．図 5 の#4 Runnning Man の表示では，類似ユーザの平均スコアを超えても赤色表示となっており，類似ユーザの平均スコアに合わせた色付けの変更は行っていない．

4. 事前実験

4.1 概要

ユーザ実験で類似ユーザのスコア表示を行うために，あらかじめ別途事前にユーザ実験を行った．そこでは本提案の 5 種類のパスワード強度メータは用いず，#0：Basic のメータだけを用いてユーザのパスワード強度とそのユーザの属性情報を収集し，その平均パスワード強度を求めた．

被験者はクラウドソーシングサービスのランサーズを利用した．ランサーズは Amazon Mechanical Turk（以下

表 1 #0:Basic meter を用いた被験者の平均強度スコア：性別
Table 1 Average score of #0 basic meter: By gender.

	被験者数	平均スコア
男性	45	53.93
女性	53	42.83

MTurk と呼ぶ）と類似したサービスである．パスワードに関連するユーザ実験では多くの研究が MTurk を利用しているが，MTurk の利用には米国に在住している（米国での住所がある）必要があり，本研究の著者に米国所在のものがいないため，類似サービスである日本国内のクラウドソーシングサービスを利用した．

パスワード入力前に，ユーザ実験の目的が被験者に示された．しかしそれは本来の目的であるパスワード強度メータの評価であることは秘匿して別の異なる目的を示した．著者らの研究室での実験であることを通知した実験であるため，セキュリティにおける別の目的として「セキュリティの慣れについての調査」を示して参加者に事件に臨んでもらった．慣れについての調査であるため，実験は 2 回に分けて行われることとし，2 回目の実験に同じ被験者であることを確認するために 1 回目の実験でパスワードを入力させることとした．別の目的を提示した理由は，本来の目的をいうことで結果に偏りが生じることを避けるためである．そしてパスワード入力後に本来の目的を通知し，ユーザが同意しなかった場合はサーバ側にデータがわたらないようにした．また，パスワードの構成に関する制限や推奨を行わなかった．

それぞれのパスワード強度メータにたいし 100 人の被験者によりパスワードの設定をしてもらった．パスワード設定のタスクに 50 円が被験者に支払われた．

ユーザ実験は 2014 年 12 月 30 日から 2015 年 1 月 1 日にかけて行われた．

4.2 結果

100 人の被験者のうち，実験を途中で終了した 2 名を除いた 98 名のデータにより計算をした．

全体でのパスワード強度スコアの平均は 47.93 であった．取得した属性は性別，年齢，職業，最終学歴の 4 つであった．それぞれの結果を**表 1**，**表 2**，**表 3**，**表 4** に示す．

それぞれの属性がパスワード強度スコアに有意な差を与えるかを Kruskal-Wallis 検定を行った．その結果，性別，年齢，職業，最終学歴のそれぞれにおいて分割した群を利用した検定の結果，いずれも有意差が出るとは判定されず，ユーザ属性によりパスワード強度に変化があることは示されなかった．

表 2 #0:Basic meter を用いた被験者の平均強度スコア：年齢
Table 2 Average score of #0 basic meter: By age.

	被験者数	平均スコア
20–29	16	39.44
30–39	50	49.34
40–49	22	48.41
50–59	9	50.78
60–69	1	77

表 3 #0:Basic meter を用いた被験者の平均強度スコア：職業
Table 3 Average score of #0 basic meter: By occupation.

	被験者数	平均スコア
事務職，事務系専門職	15	43.33
販売，サービス，労務	9	49.33
会社役員	6	47.5
自営業	10	47.9
自由業，フリーランス	18	51.67
教員，講師	3	59
その他技術職	7	56.71
その他	30	44.5

表 4 #0:Basic meter を用いた被験者の平均強度スコア：最終学歴
Table 4 Average score of #0 basic meter: By the final academic record.

	被験者数	平均スコア
中学	3	47.33
高等学校	27	44.30
専門学校	14	44.21
高等専門学校	4	48
短期大学	6	45.5
大学	42	52.81
大学院（修士）	3	32.33
海外の学校	2	75

5. ユーザ実験のデザイン

5.1 ユーザ実験概要

ユーザ実験にあたって，別の目的を伝え，そのためにユーザ登録が必要であることを伝え，ユーザ登録にあたってユーザの属性情報とユーザのパスワードを設定してもらうこととした．パスワード強度計算はユーザがパスワードを入力すると同時にブラウザ上で JavaScript を用いて計算され，サーバにはパスワードそのものの情報は渡されない．サーバ側には計算されたスコアとパスワード強度計算に関連する情報として，パスワードの長さ，利用された大文字の数，小文字の数，記号の数，数字の数が送られる．

5.2 被験者の勧誘と被験者数

提案したパスワード強度メータの効果を測定するためにユーザ実験を行った．被験者は事前実験と同様にクラウドソーシングサービスのランサーズを利用した．

表 5 各提案メータにおける平均スコア，標準偏差，中央値，Krascal-Wallis テストで得られた P 値

Table 5 Average score, standard deviation, median, number of partipants and P-value by Krascal-Wallis test for each meter.

タイプ	平均スコア	標準偏差	中央値	被験者数	P 値
#0 Basic	47.92	25.08	44.5	98	
#1 Bar	57.77	22.60	61	91	0.0053
#2 Bar (Avg.)	55.84	22.56	61	95	00194
#3 Score	57.83	20.97	61	94	0.0027
#4 Running Man	61.62	21.56	62.5	94	6.46×10^{-5}
#5 Tachometer	55.15	24.38	56.5	94	0.0472

表 6 各提案メータにおける平均パスワード長，数字の平均利用数，大文字の平均利用数，小文字の平均利用数，記号の平均利用数

Table 6 Average value of length, digits, upper case, lower case and symbols for each meter.

タイプ	長さ	数字	大文字	小文字	記号
#1 Bar	9.46	3.26	0.21	5.90	0.07
#2 Bar (Avg.)	9.41	2.90	0.48	5.87	0.07
#3 Score	9.98	3.21	0.34	6.15	0.06
#4 Running Man	10.29	3.31	0.41	6.42	0.07
#5 Tachometer	9.55	2.95	0.52	5.93	0.06

それぞれのパスワード強度メータに対し 100 人ずつ実験に参加してもらい，計 500 人の被験者が実験に参加した．パスワード設定のタスクに 50 円が被験者に支払われた．またユーザ実験は 2015 年 1 月 25 日から 2015 年 1 月 29 日にかけて行われた．

パスワード入力前のユーザ実験の目的などは 4 章の実験と同じものを提示し，類似ユーザの平均スコアの説明やメータの概要についての説明を行わずにパスワード強度メータの提示を行った．

事前実験を含め，ユーザ実験にあたり，著者らが所属する組織の倫理委員会に諮り，実験することの承認を得た．

5.3 類似ユーザのパスワード強度

事前実験により各属性でのパスワード強度の違いは得られたが，本実験では全体の平均である 47.93 で統一した．属性ごとの統計的差異が認められなかったことに加え，提示する平均値を統一することで各パスワードメータの効果をスコアによって比較可能にするためである．

5.4 社会的影響以外の情報がもたらすパスワード強度への影響についての検討

パスワード強度メータへの情報提示として，本論文で提案した社会的影響の情報を提示するだけでなく，事業者による推奨といった情報提示をすることも可能である．パスワード強度メータにおいて，そういった別の情報提示が強度向上をもたらす可能性は存在する．

しかし，Das らの結果 [6] において，そういった情報提示

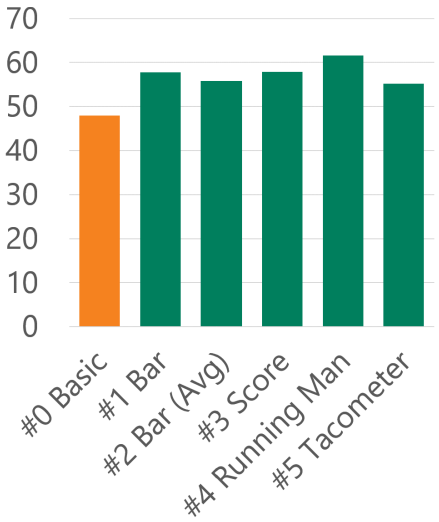

図 8 Average Score for Each Meter

Fig. 8 Average Score for Each Meter.

についての実験が行われており，事業者による情報提示はさまざまなタイプの社会的影響情報と比較して効果が薄いことが示されていた．本論文では Das らの結果に基づき，社会的情報以外の情報がもたらすパスワード強度への影響の検討は行わなかった．

5.5 結果

表 5，**表 6**，**図 8** にその結果を示す．

表 5，図 8 で分かるように，事前実験で得た#1:Basic のメータに比べて，提案した 5 つのメータすべてにおいて平均パスワード強度スコアが高い数値となった．

Das らの論文では，直接的なスコア提示がより強く振舞いへの影響を与えることが指摘されていた．我々の提案パスワード強度メータにおいて，#1: Bar，#2: Bar (Avg.')，#3: Score は Das らの論文により得られた知見をふまえパスワード強度メータに当てはまるかを意図したものであり，Das らの論文によれば，スコアを直接書いた#3 が最も社会的影響が強く，その次に類似ユーザの平均スコアを記載した#1，そして全体の平均スコアを記載した#2 という順で社会的影響が強く並ぶこととなる．我々の結果でも#1: Bar，#2: Bar (Avg.')，#3: Score の中では最も#3: Score が高い平均スコアを出している．提案手法は直接的な友人関係にあるユーザの行動をもとにした社会的影響ではないものの，Das らの結果を支持する内容となっている．

最も高い平均スコアを示したのが#4: Running Man である．Running Man では標準偏差の値も小さくなっており，提案手法の中では最もパスワード強度に対する影響が強くでているということができる．

#0: Basic と他の手法との間で Kruscal-Wallis 検定を行ったところ，いずれも有意な差が出ているとことが分かり，提案手法がパスワード強度を上げる効果があることが示されている．なお，検定については，パスワード強度メータで計算されたスコアの統計的性質が不明であることに加え，当初の事前実験において属性により群を分けた多群検定を行った背景があったこともあり，ノンパラメトリック検定であり多群検定である Kruscal-Wallis 検定を行った．

6. 議論

提案手法はスコアの方法を制限していないため，合わせて使うことが可能であり，より適切なスコアにより高い効果がさらに示されることが期待される．たとえばスコアリングの方法は，実験においては Ur らの論文 [18] と同じ方法を採用した．その Ur らの論文では表示にあたり実際のスコアを半分に調整して表示すると高い効果が得るなどが示されている．この方法は我々の提案と衝突するものでなく同時に利用が可能であり，さらに高い効果が見込まれる．Dell'Amico のスコアリング [9] についても同様であり，Ur らが効果的だと示したスコア調整方法と本論文の提案表示手法と合わせて利用が可能である．

パスワードに関連する研究ではその生態学的妥当性が問われるが，本論文で行った実験では，実験前の説明において後日再び実験をする必要がある目的をしめし，そのためにパスワードの入力が必要なことを伝えた．また謝金の支払についても 2 回目の実験を行うことで 1 回目とは別途謝金を支払うこと，またその謝金は 1 回目より高価であることを伝えた．そのことにより被験者が 2 回目の実験を行う意志を強めさせ，パスワード設定が適当になることを避けた．2 回目の実験へのモチベーションを与えたことにより，パスワードの設定に対する生態学的妥当性があると考える．

パスワード強度メータやパスワード構成ポリシを変更することにより強固なパスワードの設定をユーザに促すことが可能であるが，ユーザがそのパスワードを記憶し続けることができるかが 1 つの論点になる．本論文ではパスワードの記憶性に対する影響の実験は行わなかったものの，我々の先行研究であり多くのパスワード強度メータの効果を調査した Ur らの論文 [18] ではその記憶性についての調査も行われている．そこでは，彼らが提案したそれぞれのパスワード強度メータについて，記憶性については統計的な差が有意に現れてはいないことが示されている．本提案手法も同様の効果があると考えられるが，その検証は 1 つの課題といえよう．

7. おわりに

本論文では，社会的影響を利用した 5 つのパスワード強度メータを提案した．社会的影響は類似ユーザのパスワード強度を表示することで与えられており，その表示方法を複数用意して評価を行った．評価はユーザ実験を行ってなされた．その結果，提案メータのいずれも基礎的なメータよりもパスワード強度を高くさせる効果があることが認められ，その中でも最も高い効果が#4: Running Man において見られた．これらのことから，パスワード強度メータに対しても社会的影響がユーザ振舞いに働きかけることが分かった．

参考文献

[1] Bonneau, J.: The science of guessing: Analyzing an anonymized corpus of 70 million passwords, *Proc. 2012 IEEE Symposium on Security and Privacy* (*SP '12*), pp.538–552, IEEE Computer Society (2012).

[2] Bonneau, J., Herley, C., Oorschot, P.C.V. and Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes, *Proc. 2012 IEEE Symposium on Security and Privacy* (*SP '12*), pp.553–567, IEEE Computer Society (2012).

[3] Burr, W.E., Dodson, D.F., Newton, E.M., Perlner, R.A., Polk, W.T., Gupta, S. and Nabbus, E.A.: Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, Special Publication 800-63-1, CreateSpace Independent Publishing Platform, USA (2012).

[4] Castelluccia, C., Duermuth, M. and Perito, D.: Adaptive password-strength meters from markov models, NDSS, The Internet Society (2012).

[5] Das, S., Kim, H., Dabbish, L.A. and Hong, J.I.: The effect of social influence on security sensitivity (2014).

[6] Das, S., Kramer, A.D., Dabbish, L.A. and Hong, J.I.: Increasing security sensitivity with social proof: A large-scale experimental confirmation, *Proc. 2014 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '14*), pp.739–749, ACM (2014).

[7] Das, S., Kramer, A.D., Dabbish, L.A. and Hong, J.I.: The role of social influence in security feature adoption, *Proc. 18th ACM Conference on Computer Supported Cooperative Work Social Computing* (*CSCW*

'15), pp.1416–1426, ACM (2015).
[8] de Carné de Carnavalet, X. and Mannan, M.: From very weak to very strong: Analyzing password-strength meters, *Network and Distributed System Security Symposium* (*NDSS 2014*), Internet Society (2014).
[9] Dell'Amico, M. and Filippone, M.: Monte carlo strength evaluation: Fast and reliable password checking, *Proc. 22nd ACM SIGSAC Conference on Computer and Communications Security* (*CCS '15*), pp.158–169, ACM (2015).
[10] Dell'Amico, M., Michiardi, P. and Roudier., Y.: Password strength: An empirical analysis, *Proc. 29th Conference on Information Communications* (*INFOCOM'10*), pp.983–991, IEEE Press (2010).
[11] Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K. and Herley, C.: Does my password go up to eleven?: The impact of password meters on password selection, *Proc. SIGCHI Conference on Human Factors in Computing Systems* (*CHI '13*), pp.2379–2388, ACM (2013).
[12] Florêncio, D., Herley, C. and Van Oorschot, P.C.: An administrator's guide to internet password research, *Proc. 28th USENIX Conference on Large Installation System Administration* (*LISA'14*), pp.35–52, USENIX Association (2014).
[13] Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F. and Lopez., J.: Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms, *2012 IEEE Symposium on Security and Privacy* (*SP*), pp.523–537 (2012).
[14] Komanduri, S., Shay, R., Cranor, L.F., Herley, C. and Schechter, S.: Telepathwords: Preventing weak passwords by reading users' minds, *23rd USENIX Security Symposium* (*USENIX Security 14*), pp.591–606, USENIX Association (2014).
[15] Li, Z., Han, W. and Xu, W.: A large-scale empirical analysis of chinese web passwords, *23rd USENIX Security Symposium* (*USENIX Security 14*), pp.559–574, USENIX Association (2014).
[16] Ma, J., Yang, W., Luo, M. and Li, N.: A study of probabilistic password models, *Proc. 2014 IEEE Symposium on Security and Privacy* (*SP'14*), pp.689–704, IEEE Computer Society (2014).
[17] Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F.: Can long passwords be secure and usable?, *Proc. SIGCHI Conference on Human Factors in Computing Systems* (*CHI '14*), pp.2927–2936, ACM (2014).
[18] Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N. and Cranor, L.F.: How does your password measure up? the effect of strength meters on password creation, *Proc. 21st USENIX Conference on Security Symposium* (*Security'12*), p.5, USENIX Association (2012).
[19] Coldstein, N.J., Cialdini, R.B. and Griskevicius, V.: A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels, *Journal of Consumer Research*, Vol.35, No.3, pp.472–482 (2008).
[20] Bandura, A., Grusec, J.E. and Menlove, F.L.: Vicarious Extinction of Avoidance Behavior, Journal of Personality and Social Psychology, Vol.5, No.1 pp.16–23 (1967).
[21] Ur, B., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., Komanduri, S., Kurilova, D., Mazurek, M.L., Melicher, W. and Shay, R.: Measuring real-world accuracies and biases in modeling password guessability, *24th USENIX Security Symposium* (*USENIX Security 15*), pp.463–481, USENIX Association (2015).
[22] Weir, M., Aggarwal, S., Collins, M. and Stern, H.: Testing metrics for password creation policies by attacking large sets of revealed passwords, *Proc. 17th ACM Conference on Computer and Communications Security* (*CCS '10*), pp.162–175, ACM (2010).
[23] Weir, M., Aggarwal, S., Medeiros, B.D. and Glodek, B.: Password cracking using probabilistic context-free grammars, *Proc. 2009 30th IEEE Symposium on Security and Privacy* (*SP '09*), pp.391–405, IEEE Computer Society (2009).
[24] Fahl, S., Harbach, M., Acar, Y. and Smith, M.: On the ecological validity of a password study, *Proc. 9th Symposium on Usable Privacy and Security* (*SOUPS '13*), Article 13, 13 pages, ACM, DOI: http://dx.doi.org/10.1145/2501604.2501617 (2013).

大山 敬博

1992 年生．2015 年東邦大学理学部情報科学科卒業．セキュリティとユーザビリティの研に従事．現在は株式会社アルファシステムズに所属．

金岡 晃 （正会員）

1975 年生．1998 年東邦大学理学部情報科学科卒業．2000 年同大学大学院修士課程修了．2004 年筑波大学大学院博士課程システム情報工学研究科修了．同年セコム（株）入社．筑波大学システム情報工学研究科研究員，同助教を経て 2013 年より東邦大学理学部講師．セキュリティとプライバシのユーザビリティ，暗号技術の応用，リスクの定量化に関する研究に従事．2014 年情報処理学会山下記念賞受賞．