情報処理学会論文誌　教育とコンピュータ　Vol.2　No.2　1–9 (Oct. 2016)

論　文

大学生の用いるパスワードの強度と管理状況

高橋 優[1,a)]　上田 卓司[2]

受付日 2015年7月13日，再受付日 2016年1月20日，
採録日 2016年7月9日

概要：大学生を対象として，ネットワーク・サービスの利用時に用いるパスワードの強度と管理行動について検討した．まず，実際に利用しているネットワーク・サービスのパスワードの強度と管理状況について調査した．次に，スマートフォンやタブレットのタッチスクリーン上に表示される仮想キーボードからパスワードを設定した場合のパスワード強度について PC の場合と比較した．結果をもとにパスワード教育のあり方について検討した．

キーワード：パスワード教育，情報教育，キーボード形式，ネットワーク・サービス

Strength of Passwords and Their Management Strategies by Undergraduate Students

Masaru Takahashi[1,a)]　Takashi Ueda[2]

Received: July 13, 2015, Revised: January 20, 2016,
Accepted: July 9, 2016

Abstract: Strength of passwords for network services and their management behavior were investigated. As the first step, we investigated with a questionnaire the strength and the management strategies of undergraduates' passwords. Second, experimental study was conducted to investigate the relationship between password strength and keyboard type. Participants were asked to compose new passwords for network services with smartphone, tablet, and PC. From the results, what should be emphasized in password education was discussed.

Keywords: password education, information education, keyboard type, network service

1. はじめに

パスワードはネットワーク・サービスにおけるユーザ認証の手段として広く用いられている．生体認証やシングルサインオン等新たなユーザ認証の方法が生まれているが，特殊な装置を必要とせずさまざまな場面で利用できるパスワードは依然としてユーザ認証の中心的存在である [1]．

ネットワーク・サービスを利用する場合，強度の高いパスワードを安全に管理することがユーザには求められる．一方で，ネットワークの利用の普及にともない，技術者・専門家ではない「普通の」人が SNS やショッピング等さまざまなネットワーク・サービスを利用するようになっている．このため，普通のユーザでも複数のパスワードを管理することが一般的である．IPA の調査によれば，ユーザの保有 ID の最頻値は 3 で，1〜5 個が回答者の 63.4%，10 個までだと累計で 86.4%を占める [2]．

パスワードの強度に関して重要なのは第 1 に十分な文字長であること，第 2 に使用する文字種が多様であること，第 3 に辞書語や製品名等の有意味語や生年月日等ユーザ自身に関する情報を含んでいないことの 3 点である．文字長と文字種は総当たり攻撃に対処するために必要な要件である．文字長が長く，大文字や記号等多様な文字種を含むこ

[1] 埼玉工業大学
Saitama Institute of Technology, Fukaya, Saitama 369–0293, Japan
[2] 早稲田大学
Waseda University, Shinjuku, Tokyo 169–8050, Japan
[a)] masaru@sit.ac.jp

本原稿の内容の一部は，日本心理学会第 77 回大会，第 79 回大会で報告されたものである．

とが望ましい．有意味語は辞書攻撃への防御のため避けるべきである．また，ユーザ自身に関する情報等はパスワード推測時にしばしば用いられるため，パスワードに含めることは望ましくない．

パスワードの管理に関しては，他人から見られる場所に記録しないこと，パスワードを複数サービス間で使い回さないことが重要である．パスワードの更新については効果に議論のあるところだが，少なくとも与えられた初期パスワードを変更しておくことが求められる．

1.1　パスワード管理と教育

パスワードの適切な生成と管理を図るうえで 1 つの鍵となるのが情報教育である．「総合的な学習の時間」や中学校「技術」，高等学校の教科「情報」等がこうした役割を担うものと考えることができる．文部科学省の「教育の情報化に関する手引」では小学校の各科，中学校の技術におけるパスワード管理の教育例が示されている [3]．また，高等学校の科目「社会と情報」でも情報セキュリティを確保するために必要な基礎的な知識と技術としてパスワードの適切な運用が位置づけられている [4]．

今後の情報教育を考えるうえで，現時点での教育カリキュラムがどういった成果をあげているかを把握することは有益である．そこで，教科「情報」を履修した大学生を対象として利用パスワードの強度と管理状況について検討する．

パスワード管理に関するユーザ行動を考えるとき，学習者の記憶能力に関する認識は影響要因の 1 つとなりうる．記憶能力に自信のある者は，より強度の高いパスワードを設定したり，より頻繁にパスワードを更新したりしている可能性がある．その場合，パスワード教育は記憶能力に自信のない者を主要な対象者として内容を構成すればよいことになる．そこで，記憶能力の自己認知と，パスワードの強度や管理と関連についても検討する．

1.2　スマートフォン・タブレットとパスワード生成行動

ユーザによるパスワード生成行動を検討するうえで，スマートフォンやタブレットの急速な普及を無視することはできない．PC とは異なる入力環境が，使用されるパスワードに影響を及ぼす可能性があるからである．

スマートフォンやタブレットではタッチスクリーン上に表示される仮想キーボードからパスワードの入力や設定を行う．仮想キーボードはスクリーンの限られた領域に表示されるため，PC のキーボードと比べるとキーの数が少なく，数字や記号の入力時には表示盤面の転換が必要となる．また，PC のキーボードと比べるとキーのサイズが小さい．

こうしたキーボードの特性は，パスワード入力時のユーザの負担を高めることになる．Kim らは異なる大きさの仮想キーボードにおいて，最小のサイズでは他と比べてタイピング速度が遅くなったことを報告した [5]．黒澤らによれば，タッチスクリーンの余白の大きさは操作時間やエラー率に影響する [6]．こうした負担を軽減するために，ユーザはパスワードをより簡素化して対応する可能性がある．

こうしたキーボード形式による入力特性の変化は，パスワード教育のあり方に再考を迫るかもしれない．たとえば，これまでの多様な文字種によるパスワードの構成よりも，文字長による強度向上を強調したほうが盤面の転換が不要な分だけ望ましいことになる．また，スマートフォンやタブレットをよく使う若者を指導する際に多様な文字種の使用を過度に強調すると，入力しにくいパスワードを強いられる負担感からサービスの利用や認証行動そのものに対する否定的な印象を形成する可能性がある．

内閣府が 2014 年に実施した調査 [7] によれば，中学生の 37.3%，高校生の 89.1%がスマートフォンを使用しており，かつてのフィーチャーフォンを完全に置き換えている．総務省の調査 [8] でも，2014 年時点の 10 代のスマートフォンの利用率は 68.6%と大変高い．タブレットの利用は 28.6%で前年と比べて 10 ポイント以上増加しており，急速に普及している．メッセージのやりとりもスマートフォンからが中心である．ネットワーク利用時間で見ても PC よりスマートフォンのほうが長く，PC によるネットワーク利用時間は減少傾向にある．

タブレットの普及はスマートフォンほどではないが，電子教科書等としてタブレットを用いる全県的な実証研究も見られるようになった [9]．今後，こうした動きが進むのにともない，若年層におけるタブレットの利用は一般化するものと思われる．

スマートフォンやタブレットの普及は，パスワードの設定をスマートフォン等で行う機会が増加することを意味する．そこで，パスワードの生成行動がスマートフォンやタブレットを用いることによってどのように影響を受けるのかを，実機を用いたパスワード生成場面を設定して実験的に検討する．スマートフォン・タブレットの普及という情報環境の変化に対して，パスワードの生成に関連した教育がどの程度有効に機能しているか検証する．

1.3　目的

本研究では現状でのパスワード教育の効果を検討するために，大学生を対象としてネットワーク・サービス利用時のパスワード管理行動とパスワード生成行動について検討する．研究は 2 つの要素から構成される．第 1 に，パスワード管理行動を明らかにするためにネットワーク・サービス利用時のパスワードの強度と管理について調査し，ネットワーク・サービスの利用行動とパスワード使用状況を把握する．第 2 に，パスワードの生成時にスマートフォン・タブレットの使用が及ぼす影響を実験的手法により検討する．実際に各機器を用いてパスワードを生成させ，キーボード形式の違いによりパスワードの特性がどのように変化する

かを検討する．

これらの調査・実験の結果を踏まえて，パスワード生成・管理行動に対する現状の情報教育の効果を考える．

2. 調査

検討の第 1 段階として，ネットワーク・サービスを利用する際の各パスワードの強度と管理について調査した．実際に使用しているパスワードを直接収集することは倫理的に問題があるため，実際に使用している各ネットワーク・サービスを想起させたうえで，そのサービスのパスワードの強度にかかわる特性のみを尋ねた．さらに，パスワード管理行動に関する情報を収集し，得られたパスワード特性との関連を分析した．

2.1 方法

(1) 調査対象者

情報系の一般教養科目を受講する首都圏の大学生 246 名を調査対象者とした．対象者のうち，今回の調査目的に合致する，教科「情報」を履修した者を対象とするために，30 代以降の者および年齢未回答者を除いた 141 名を分析の対象とした．内訳は 10 代が 20 名，20 代が 121 名，性別は男性が 57 名，女性が 81 名，不明 3 名であった．

(2) 調査手続き

調査には無記名のマークシート調査票を用いた．調査では，ユーザの利用しているネットワーク・サービスについて思い出したものから順に，そのサービスにおけるパスワードの特性の報告を求めた．回答対象は最大 25 サービスとした．

尋ねた強度情報は，文字長，小文字・大文字・数字・記号をそれぞれ使用しているか，有意味語を含むか，誕生日等の個人情報を含むか，すでに回答した中に同一のパスワードがあるかである．また，サービスごとの利用頻度も 5 件法で尋ねた．各サービスについての回答後，利用サイト数，一番利用しているサイトのパスワード更新頻度，記憶能力に関する自己評定，性別，年齢について記入を求めた．各質問項目の詳細は付録として示した．

2.2 結果

(1) 利用サービス数と利用頻度

5 件法で尋ねた利用サービス数についての分布を**表 1** に示す．利用サービス数が 5 以下および 6–10 のものが多く，この 2 カテゴリで全体の 75%を占めた．各カテゴリの階級値を用いた平均は 7.79 であった．利用サービス数は強度特性について回答されたパスワード数からも推測することができるが，回答パスワード数の平均は 7.62 であった．

報告された 1,074 件の利用サービスごとに，5 件法で尋ねた利用頻度は，「ほとんど使っていない」が 11%，「数カ月に 1 度程度利用している」が 14%，「月に 1〜数回程度利用している」21%，「週に 1〜数回程度利用している」23%，「毎日利用している」18%，無回答が 12%であった．報告された利用サービスのうち 6 割以上が月に 1 回以上利用されていた．

表 1　利用しているネットワーク・サービス数の分布
Table 1　Frequency distribution of the number of the reported network services.

利用サービス数	-5	6-10	11-15	16-20	21-	NA*
度数	53	53	26	3	5	1

* NA= Not Available.

表 2　利用サービス数ごとに見たパスワードの各文字種・有意味語・個人情報の平均出現率（%）と平均文字長
Table 2　Mean appearance rate of character type, meaningful word, and privacy information, and mean length of the passwords.

利用サービス数	-5	6-10	11-15	16-20	21-
小文字	68	64	71	68	70
大文字	15	9	11	15	17
数字	66	63	72	65	63
記号	4	3	3	2	12
有意味語	35	28	36	47	14
個人情報	26	31	36	8	16
平均文字長	8.32	8.24	8.56	9.32	8.29

(2) パスワード強度

回答されたパスワードの文字種および有意味語・個人情報の出現率を回答者ごとにまとめ，利用サービス数への回答ごとに平均したものを**表 2** に示す．回答者ごとの文字長の平均もあわせて示した．

利用サービス数を要因とした分散分析の結果によれば，利用サービス数による各文字種・有意味語・個人情報の出現率や文字長の違いは見られなかった．

パスワードにその文字種が含まれる出現率を回答者ごとに求めた平均は，小文字・数字ではそれぞれ 67%，66%と高かった．一方，大文字と記号はそれぞれ 12%，4%であった．また，有意味語は平均 32%，個人情報は平均で 30%のパスワードに含まれていた．平均文字長は 8.37 字であった．

記憶能力に関する自己評定値ごとに見た各文字種および有意味語・個人情報の出現率を**表 3** に示す．

記憶能力の自己評定を要因とした分散分析を行ったが，小文字・文字長・各文字種・有意味語・個人情報・文字長いずれも有意ではなかった．

(3) パスワードの使い回し

ユーザの 74%が 1 つ以上のパスワードで使い回しを報告した．使い回しをしているユーザの割合を利用サービス数ごとに見ると「5 以下」が 66%，「6–10」が 77%，「11–15」が 85%，「16–20」が 67%，「21 以上」が 60%で，両者の間

表 3　記憶能力の自己評定とパスワードの各文字種・有意味語・個人情報の平均出現率（%）と平均文字長

Table 3　Mean appearance rate of character type, meaningful word, and privacy information with subjective memory performance.

記憶能力の自己評定	悪い	やや悪い	普通	やや良い	良い
小文字	58	71	73	62	58
大文字	13	8	16	11	8
数字	68	69	65	66	58
記号	3	4	4	3	10
有意味語	38	36	37	23	22
個人情報	36	27	25	35	32
平均文字長	7.99	8.46	8.26	8.39	9.08
度数	13	37	46	36	9

表 4　記憶能力の自己評定と使い回しユーザの割合，使い回しパスワードの割合の平均，平均使い回しサービス数

Table 4　Mean rate of password-reuse user, reused password rate, and number of reused password with subjective memory performance.

記憶能力の自己評定	悪い	やや悪い	普通	やや良い	良い	全体
ユーザの割合（%）	62	70	72	92	44	74
使い回し率（%）	31	26	31	38	18	31
使い回しサービス数	3.33	1.94	2.78	3.78	2.00	2.83

に有意な関係は見られなかった．

表 4 はパスワードを使い回しているユーザの割合を記憶能力に関する自己評定値ごとに集計したものである．あわせて，回答パスワード中に占める回答者ごとの使い回しパスワードの比率の平均と，平均使い回しサービス数を示した．使い回しユーザの割合と記憶能力に関する自己評定との間には 5%水準で有意な関係が見られた（$\chi^2(4) = 11.29$, $p < .05$）．各セルについて標準化残差を求めたところ，「やや良い」が 5%水準で有意に多く，「良い」では 5%水準で有意に少なかった．一方，記憶能力の自己評定を要因とした平均使い回しパスワード比率に関する分散分析の結果は有意ではなかった（$F(4, 134) = 1.83$, $p = .13$）．

(4)　**パスワード更新頻度**

最も利用しているネットワーク・サービスについてパスワードの更新頻度を尋ねたところ，半数以上の 82 名がパスワードを更新していなかった．記憶能力の自己評定結果とパスワードの更新頻度とのクロス表を**表 5** に示す．

パスワード更新頻度と記憶能力の自己認知との間の関連についてカイ 2 乗検定を行ったが，有意な関係は見られなかった（$\chi^2(16) = 22.17$, $p = .14$）．

表 5　記憶能力の自己評定ごとに見たパスワード更新頻度の分布（人）

Table 5　Distribution of password updating interval with subjective memory performance.

		パスワードの更新頻度					
		しない	1年以上	半年	数ヶ月	1ヶ月	計
記憶能力	悪い	9	3	0	1	0	13
	やや悪い	22	12	1	2	0	37
	普通	24	10	7	1	4	46
	やや良い	21	8	5	1	1	36
	良い	6	0	0	1	2	9
	計	82	33	13	6	7	141

2.3　考察

設問への回答としての利用ネットワーク・サービス数，実際にパスワード特性について報告されたサイト数のいずれも 8 程度であったことから，ユーザが実質的に把握しているネットワーク・サービスは 8 程度であることが示唆される．また，6 割以上のサービスが実際に月 1 回以上の頻度で使われており，回答されたネットワーク・サービスが実際によく利用されているものであることが分かる．

使用文字種を見ると，小文字や数字はよく使われている一方，大文字や記号の使用頻度は非常に低かった．大文字・記号の不使用は，ユーザがパスワード生成の際に用いている文字集合が実際に利用可能な文字集合の半分以下であることを意味する．文字長が 8 文字程度にとどまることとあわせ，パスワードの強度が高くないことを示唆する．

また，管理の側面から見ると 7 割以上がパスワードを使い回していた．ネットワーク・サイトにおけるパスワードの漏洩と，漏洩 ID とパスワードによるリスト型攻撃の頻発する近年では，これも大きな問題である．

パスワードを使い回している者の割合は IPA の調査 [2] における値より大きい．今回の調査は，利用しているパスワード 1 つ 1 つについて詳細に特性を報告するものであったため，使い回しであることに気づきやすかったものと思われる．パスワードの使い回しは記憶能力に関する自己認知との間で有意な連関が見られ，記憶能力を「やや良い」と回答した者はパスワードを使いまわしていることが他と比べて多く，「良い」と回答した者では少なかった．しかしながら，記憶能力を「良い」と回答した者でも 4 割以上がパスワードを使い回しており，記憶能力に関係なく多くの者が使い回しをしていると解釈できる．

記憶能力の自己認知とパスワードの更新頻度との間には有意な関係が見られず，記憶能力に自信がある者であっても半数以上はパスワードの更新をしていなかった．パスワードの更新管理は記憶能力にかかわらず不徹底といえよう．サービスの利用登録時にサービス提供者側が初期パスワードを用意するケースの場合，未更新と回答した者は与

えられた初期パスワードをそのまま使っていると考えられるため，アカウント通知書等の伝達経路からパスワードが漏洩する危険がある．これらのパスワード管理における問題は，忘却への不安というよりは認知的負荷を回避するために行われているものと思われる．

以上のように，大学生の用いるパスワードには強度と管理の両面で問題があることが明らかになった．また，こうした状況は記憶能力の自己認知とはあまり関係がなく，記憶能力に自信がある者も管理に問題があった．パスワード教育においては，記憶能力の自己認知を考慮する必要はないものと考えられる．

3. 実験

検討の第 2 段階として，キーボード形式とパスワード生成行動との関連を検討するために実験を行った．スマートフォンとタブレットでは同じ仮想キーボードでもサイズが異なるため，ユーザの負担も異なる．そこで，スマートフォン・タブレットそれぞれを検討の対象とした．スマートフォン・タブレット・PC の各装置上で新たなネットワーク・サービスを利用することを想定して，新規パスワードの生成を求めた．設定されたパスワードの強度を装置間で比較することにより，キーボード形式の違いがどのようにパスワード強度に影響するかを文字長・使用文字種をもとに検討した．加えて，スマートフォン・タブレットのような相対的に小さな仮想キーボードを用いた場合に，入力の負担を緩和するために盤面転換やシフトキーを使わなくて済むような文字が用いられるかを比較した．

今回の実験に用いたスマートフォン・タブレットの場合，サイズを除けばキーボードの構成が同一である．しかし PC はキーの数や構成が大きく異なるため，盤面転換回数そのものによる相互の比較は妥当とはいえない．そこで今回は盤面転換回数そのものを指標として用いる代わりに，文字種（小文字・大文字・数字・記号）の変更回数を用いて三者の比較を行った．

パスワードの強度は利用するネットワーク・サービスの重要性によっても変化する [10]．しかし，実際に利用しているサービスを具体的に指定してパスワードを収集することは倫理的に問題がある．そこで，新しいネットワーク・サービスを利用する場面を仮想的に設定して，新規にパスワードを生成するよう指示した．生成されたパスワードの強度特性が，入力時のキーボード形式によりどのように変化するかを検討した．

3.1 方法

(1) 実験参加者

情報系の一般教養科目を受講する首都圏の大学生 14 名が実験に参加した．内訳は男性 8 名，女性 6 名，年齢は平均 20.1 歳（$SD = 1.28$）であった．

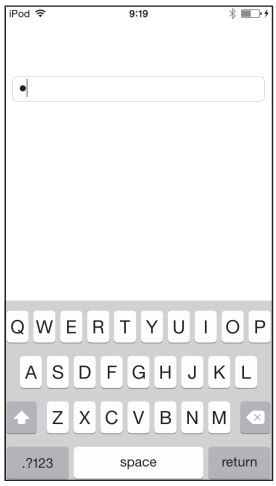

図 1　スマートフォンの実験画面
Fig. 1　Screenshot of the experiment app on smartphone.

(2) 実験計画

入力装置の違い（装置条件）としてスマートフォン，タブレット，PC の 3 水準を設定した．また，想定サービスの種類（サイト条件）については Harque, Wright & Scielzo の手続き [10] に従いニュースサイト等（sketchy），SNS 等（identity），オンラインバンキング等（contents）の 3 水準を設定した．ユーザにとってはこの順番で重要性が高くなるものと想定した．

装置条件，サイト条件ともに参加者内要因とした．

(3) 装置

実験は PC 上のプログラムおよびスマートフォン・タブレットのアプリによって実施した．スマートフォンにおける実験画面を**図 1** に示す．キーボードの形式としてフリック入力は想定せず，標準的な QWERTY キーボードのみとした．タブレットにおいてもサイズ以外は同様の画面構成である．

(4) 手続き

実験では，新たなオンライン・サービスを利用すると仮定し，そのパスワードの生成を求めた．一般的なパスワード入力欄と同様に，画面上でパスワードの文字を入力すると，1 秒ほどその文字を表示した後でこれをマスク文字（$*$）に置き換えた．参加者のキー入力のたびに入力キーと計時開始からの経過時間を記録した．パスワード生成開始のタイミングを明確にするため，入力欄にはあらかじめ 1 文字だけマスク文字を表示しておいて，最初にこれを削除してからパスワードの生成・入力を開始するよう教示した．この削除から，入力完了のリターン（PC の場合はエンター）キー押下までを所要時間とした．

サイト条件は，装置条件の各水準内でランダム順に提示した．装置の提示順もランダムに定めた．各試行では，実験者が対象となるサイトの種類を指示後，パスワード設定画面を表示した装置を渡して，パスワードの生成と入力を

表 6　装置・サイト条件ごとに見た平均文字長
Table 6　Mean length of generated password by appliance and site type.

条件	Sketchy	Identity	Contents	計
スマートフォン	8.71	9.07	9.43	9.07
タブレット	7.57	9.00	9.79	8.79
PC	8.64	8.93	10.29	9.29
計	8.31	9.00	9.83	9.05

表 7　文字種ごとの平均使用文字数と平均出現率
Table 7　Mean number of character used in the password and mean appearance rate of each character type.

	小文字	大文字	数字	記号
平均使用文字数	5.75	0.16	2.75	0.39
出現率（%）	97	10	87	25

求めた．

(5)　**倫理的配慮**

実験の際，参加者が実際に使っているパスワードを使用してしまい，実験者にパスワードが漏洩してしまう危険を避けるため，実験後に生成されたパスワードが既存のものと同一・酷似しているかを尋ね，該当する場合はパスワード情報を抹消することとした．また，最後にデータ提供の可否を確認し，否の場合は全データを抹消することとした．

3.2　結果

実験者の生成したパスワードのうち，倫理的配慮に基づく削除対象に該当するものはなかった．このため，収集された 126 のパスワードすべてを，以降の分析の対象とした．

(1)　**文字長**

装置・サイト条件ごとの平均文字長を**表 6** に示す．報告されたパスワードの文字長は平均 9.05 文字（$SD = 2.15$）であった．装置条件の水準ごとの平均文字長はスマートフォン 9.07 文字，タブレット 8.79 文字，PC 9.29 文字で，装置間で有意な差は見られなかった（$F(2, 26) = 1.23$，$p = .31$）．サイト条件を見ると，sketchy サイトで平均 8.31 文字，identity サイト 9.00 文字，contents サイト 9.83 文字で，1%水準で有意だった（$F(2, 26) = 7.45$，$p < .01$）．ボンフェローニ法による多重比較を行ったところ，sketchy-contents 間において 5%水準で有意な差が見られた．

(2)　**使用文字種**

小文字・大文字・数字・記号ごとの平均使用文字数と，出現率を**表 7** に示す．各文字種についてそれぞれ，サイト条件と装置条件を参加者内要因とした 2 要因の分散分析を行ったところ，大文字が装置条件において 5%水準で有意（$F(2, 26) = 3.41$，$p < .05$）だった．装置ごとの大文字の平均文字数は，スマートフォン 0.02 字，タブレット 0.10 字，PC 0.36 字であった．

また，数字はサイト条件で有意傾向（$F(2, 26) = 2.79$，$p = .08$）となった．サイトごとの平均文字数は sketchy サイト 2.29 字，identity サイト 2.95 字，contents サイト 3.02 字であった．

大文字・数字ともに，多重比較では水準間で有意な差が見られなかった．また，小文字・記号ではサイト条件，装置条件ともに有意ではなかった．

平均使用文字数は，大文字と記号では 1 字以下と少なかった．大文字の出現率は 10%と低く，これに記号が 25%で続いた．一方，小文字・数字は多くのパスワードで使用された．生成されたパスワードの 57%は「小文字＋数字」の組合せで，「小文字＋数字＋記号」（17%），「小文字のみ」（10%）がこれに続いた．

表 8　装置・サイト条件ごとに見た平均盤面転換回数
Table 8　Mean frequency of keyboard-change.

条件	Sketchy	Identity	Contents	計
スマートフォン	1.50	1.86	2.21	1.86
タブレット	1.36	1.64	2.86	1.95
PC	1.14	1.50	2.00	1.55
計	1.33	1.67	2.36	1.79

(3)　**盤面の転換とシフトキーの押下回数**

文字種の変更回数によって求められた，条件ごとの平均盤面転換回数を**表 8** に示す．平均盤面転換回数は，sketchy サイトで 1.33 回，identity サイトで 1.67 回，contents サイト 2.36 回で，分散分析を行ったところサイト条件は有意だった（$F(2, 26) = 7.32$，$p < .01$）．多重比較の結果，contents サイトは sketchy サイトと比べて有意に回数が多かった（$t(13) = 4.39$，$p < .01$）．装置条件では PC がスマートフォンやタブレットと比べて回数が少ないように見えるが，分散分析では有意な差は見られなかった（$F(2, 26) = 2.19$，$p = .13$）．

一方，スマートフォンおよびタブレットの実際の盤面転換回数の平均は，スマートフォン 1.60 回，タブレット 1.74 回であった．サイト条件ごとの平均盤面転換回数は，sketchy サイト 1.32 回，identity サイト 1.50 回，contents サイト 2.18 回であった．なお，文字種の変更回数に基づく盤面転換回数と，実際の盤面転換回数との相関は $r = .93$ であった．

入力された文字から計算したシフトキーの押下回数を，**表 9** に示す．シフトキーの平均押下回数は，装置条件のみ 5%水準で有意だった（$F(2, 26) = 4.03$，$p < .05$）．しかし，多重比較では水準間に有意な差は見られなかった．

(4)　**所要時間**

パスワードの生成開始から入力終了までの所要時間の平均は 29.0 秒であった．水準ごとの平均所要時間は sketchy

表 9　装置・サイト条件ごとに見たシフトキーの平均押下回数
Table 9　Mean frequency of Shift-key press.

条件	Sketchy	Identity	Contents	計
スマートフォン	0.00	0.00	0.07	0.02
タブレット	0.00	0.21	0.07	0.10
PC	0.14	0.21	0.71	0.36
計	0.05	0.14	0.29	0.16

サイト 24.4 秒，identity サイト 27.9 秒，contents サイト 34.5 秒だった．装置別ではスマートフォン 29.7 秒，タブレット 29.7 秒，PC は 27.5 秒であった．分散分析の結果はサイト条件のみ 5%水準で有意であった（$F(2, 26) = 4.87$, $p < .05$）が，多重比較では水準間に有意な差は見られなかった．

(5)　**内観報告**

内観報告によれば，スマートフォンでは押しやすいキーのみでパスワードを構成する等，与えられる装置によってパスワードの設定の仕方を変えたと報告した者は 4 名で，全体の 29%であった．

3.3　考察

今回は盤面転換回数の指標として，盤面転換回数そのものに代えて文字種の変更回数を用いたが，両者の相関は高いことから，文字種の変換回数は装置条件の三者を比較する指標として妥当である．

ユーザにとって，最も重要性が高いと考えられるサービス種別である contents サイトでは，低いサイトである sketchy サイトよりも盤面転換回数が有意に多かった．重要性の高いサイトでは，盤面転換の手間を増やしてでも強度の高いパスワードを設定していたものと考えられ，Harque ら [10] と一致する結果だったといえるだろう．

一方，装置条件では，盤面転換回数において有意な差が見られなかったものの，大文字の使用数やシフトキーの押下回数について有意な結果を得た．シフトキーの押下回数は大文字や一部の記号の入力にかかわるものであることから，大文字等の使用のあり方が装置によって異なっていたことを示唆する．内観報告でも，装置によってパスワードの生成方略を変えた者が 3 割近くいたこともこの結果を支持するものといえるだろう．また，所要時間において装置条件に有意な差が見られなかったことから，パスワードの複雑さと所要時間との間のトレードオフを考慮する必要はなく，キーボード形式との関係で解釈してよいことが分かる．しかしながら分散分析後の多重比較では，大文字の使用数やシフトキーの押下回数に関して装置条件の 3 水準間に有意な差を見いだせなかった．このため，スマートフォンやタブレットで大文字があまり使わないという仮説の支持は，現時点では限定的である．

文字種ごとに見た平均使用文字数および出現率から，大文字や記号がパスワードを構成する文字としてあまり使われていないことが分かる．また，盤面転換回数とシフトキーの押下回数を比較すると，盤面転換回数は全体平均で 1.79 回と 2 回近いのに対し，シフトキーの押下回数は平均で 0.16 回と大変少なく，シフトキーがほとんど使用されていなかったことが分かる．前節の調査の結果でも大文字の出現率は 12%にとどまっており，同様の傾向である．いずれもパスワードに大文字が使用されにくいことを反映したものと考えられる．

4.　総合考察

調査と実験により，大学生のパスワード強度と管理，多様なキーボード環境下におけるパスワード生成行動について検討した．ネットワーク・サービス利用時に使用されているパスワードの調査によれば，パスワードの強度と管理の両面で問題があること，パスワードの使い回しが多くのユーザによって行われていることが明らかになった．

パスワードの強度を見ると，小文字や数字と比べて大文字や記号の使用率が低かった．調査と実験それぞれの結果を比較すると，実験のときのほうが文字長は長く，記号もよく使用されていた．これは，個人実験という状況下で実験参加者がより「適切な」パスワードを作ろうと意識したものと思われる．しかし，その実験で得られたパスワードでも大文字や記号の出現率は低かった．このことから，使用文字種に関する傾向が一貫したものであることを示唆するとともに，実験で収集されたパスワードが実際に使用されているものに近いことを示している．

パスワードの使い回しが蔓延していることも明らかになった．若年層でもネットワーク・サービス利用数は今後ますます増加することが予想される．リスト型攻撃への対処という観点からも，パスワードの使い回しを防止するための対策が急務である．教育を通じた啓蒙のほか，パスワードマネジャの導入も 1 つの方法である．パスワードの保持をパスワードマネジャに任せれば，使い回す必要性がなくなる．パスワードの生成もソフトに任せれば，パスワード強度の懸念も解消しうる．

パスワードの更新に関しては，半数の者がそもそも変更していなかった．ネットワーク・サービス利用開始時に行われるパスワードの設定では，最初のパスワードをユーザ自身に付けさせるサービスもあるが，「初期パスワード」という形でサービス提供者側が書面等でパスワードを通知する形式も見られる．今回の調査では回答者のパスワードがどちらに該当するか不明だが，回答されたパスワードが後者のような初期パスワードであった場合，書面の紛失や盗み見によってパスワードの漏れるケースも考えられる．初期パスワードはサービス提供者側が与えるのではなく，利用開始時にユーザ自身に設定させるほうが安全である．ま

た，初期パスワードを与える場合は，それをそのまま更新せずに使ってしまうユーザが多数いることを前提に，十分な強度を持つものを与えるべきである．

記憶能力の自己認知とパスワードの間には明確な関係が見られなかった．記憶能力に自信のある者に限っても 4 割以上がパスワードを使い回し，半数以上はパスワードを更新していなかった．全体としては，パスワードは使い回され，更新されていないと解釈できる．こうした結果から，学習者の記憶能力に自信がある者でもそうでない者でも，同様のカリキュラムでパスワード教育を実施して差し支えないものと思われる．

また，キーボード形式の違いと生成されるパスワード強度との関連を調べた実験によれば，盤面転換回数はキーボード形式と関係が見られなかったが，大文字の使用数やシフトキーの押下回数は影響が示唆された．

仮想キーボードを用いたスマートフォンやタブレットに限らず，シフトキーの押下回数は全般的にきわめて少ない．シフトキーは，PC であれば別のキーと同時に押すが，仮想キーボードの場合，あるキーに先立ってシフトキーを押すことで大文字にしたり別の記号にしたりするものであるため，そのキーを押し間違えると，あらためてシフトキーから入力し直さなければならない．こうした「二度手間」が潜在的に認知的な負荷を高めるものと推察される．

シフトキーとは対照的に盤面転換回数は平均で 2 回近い値であった．使用文字種の結果を踏まえれば，盤面転換のコストを払ってでもユーザがパスワードの中に数字を加えようとした結果といえるだろう．これを前提とすれば，数字と同様に盤面転換によって入力できる各種記号もあわせてパスワードに加えるよう，ユーザを啓蒙することが可能だろう．とくに，数字のキーを表示する盤面で一緒に表示されている記号を数字とあわせて入力するのであれば，負担も小さい．

ただ，シフトキーの使用では仮想キーボードの影響が見られたことを考えると，異なるアプローチも検討すべきである．文字長による強度向上はその 1 つである．たとえば，8 文字で大文字・小文字・数字・記号をすべて含むパスワードを生成する代わりに小文字のみで 11 文字のパスワードを生成しても，同程度以上の強度のパスワードを得ることができる．文字長を長くすることでパスワードの強度を確保できるならば，文字種の偏りによる強度低下は相殺可能である．

こうしたパスワードの生成・管理行動は，サービス提供者が設定するパスワードポリシーによっても制御が可能である．今回の調査では回答サービスにおいてどのようなパスワードポリシーが適用されているかを尋ねなかった．実験でも，パスワードポリシーを設定しなかった．このため，適切なパスワードポリシーを設定することにより，ユーザの行動がどう変わるかは本研究では不明であり，今後検討する必要がある．

だが IPA によれば，実際のサービスではパスワードに使用できる文字種は制限されており，「半角英数のみ」というケースが 7 割を占めている [2]．これを踏まえると，調査・実験で見られた記号の不使用はサービス提供者側の「教育」の結果とも見ることもできる．より多様な文字を許容するシステムを用意することがサービス提供者には求められるが，上述の文字長による強度向上は文字種に制約があっても適用できる点を指摘しておきたい．

以上の考察を踏まえて，今後のパスワード教育のあり方を検討する．学習者の生成・管理パタンの実態と望ましさのバランスを取るという観点から，強調すべき教育内容として次の 3 点をあげる：1) 使い回しの危険を強調し，サイトごとに異なるパスワードを用いる重要性を伝える，2) 文字数による強度確保に努めるよう促す，3) 文字種に関しては，数字を入力する際の盤面転換時に表示される記号の使用を推奨する．

謝辞　本研究の実施にあたり電気通信普及財団の助成をいただきました．記して謝意を表します．

参考文献

[1] Herley, C., van Oorschot, P.C. and Patrick, A.S.: Passwords: If we're so smart, why are we still using them?, *Financial Cryptography and Data Security*, pp.230–237 (online), DOI: 10.1007/978-3-642-03549-4_14 (2009).

[2] 情報処理推進機構：オンライン本人認証方式の実態調査報告書（オンライン），入手先 ⟨http://www.ipa.go.jp/files/000040778.pdf⟩（参照 2015-06-19）．

[3] 文部科学省：教育の情報化に関する手引（オンライン），入手先 ⟨http://www.mext.go.jp/a_menu/shotou/zyouhou/1259413.htm⟩（参照 2015-06-19）．

[4] 文部科学省：高等学校学習指導要領解説　情報編，入手先 ⟨http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2012/01/26/1282000_11.pdf⟩（参照 2015-06-19）．

[5] Kim, J.H., Aulck, L., Thamsuwan, O., Bartha, M.C. and Johnson, P.W.: The effects key size of touch screen virtual keyboards on productivity, usability, and typing biomechanics, *Human Factors*, Vol.56, No.7, pp.1235–1248, DOI: 10.1177/0018720814531784 (2014).

[6] 黒澤敏文，久野祐輝，小森谷大介，志築文太郎，田中二郎：タッチ UI におけるボタンの余白の大きさが操作に与える影響，情報処理学会研究報告，HCI，ヒューマンコンピュータインタラクション研究会報告，Vol.2014-HCI-156, No.16, pp.1–7 (2014).

[7] 内閣府政策統括官：平成 26 年度　青少年のインターネット利用環境実態調査　報告書，内閣府（オンライン），入手先 ⟨http://www8.cao.go.jp/youth/youth-harm/chousa/h26/net-jittai/pdf-index.html⟩（参照 2015-06-19）．

[8] 総務省情報通信政策研究所：平成 26 年　情報通信メディアの利用時間と情報行動に関する調査報告書，総務省（オンライン），入手先 ⟨http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000028.html⟩（参照 2015-06-19）．

[9] 佐賀県教育委員会：佐賀県が進める「先進的 ICT 利活用教育推進事業」の現状と今後の取組方針（Vol.7）（オンライン），入手先 ⟨https://www.pref.saga.lg.jp/web/var/

rev0/0174/4267/201471113146.pdf)（参照 2015-06-19）.
[10] Harque, S.M.T., Wright, M. and Scielzo, S.: A study of user password strategy for multiple accounts, *Proc. Third ACM Conference on Data and Application Security and Privacy*, pp.173–176 (2013).

付　　録

本研究の調査における設問は以下のとおりである．

文字数：パスワードに使われている文字数を括弧内に数値で記入（思い出せない場合はゼロを記入）．

同一：回答済みのサービスで使用しているパスワードと同じ場合はマークする．

小文字：パスワードに 1 文字以上アルファベットの小文字が含まれていればマーク．

大文字：1 文字以上アルファベットの大文字が含まれていればマーク．

数字：1 文字以上の算用数字が含まれていればマーク．

記号：1 文字以上の記号（!，@，$等）が含まれていればマーク．

有意味語：パスワード全体もしくはその一部に意味のある言葉（単語や製品名等）が含まれていればマーク．

個人情報：パスワード全体もしくはその一部に個人情報（誕生日，氏名等）が含まれていればマーク．

利用頻度：そのサービスの利用頻度について最も当てはまるものをマーク（ほとんど使っていない/数カ月に一度程度利用している/月に 1〜数回利用している/週に 1〜数回利用している/毎日利用している）．

利用サイト数：利用している SNS・ネットショッピング・オンラインゲーム等オンラインサイトの数はいくつ位ですか？ 次の中からマークしてください（5 以下/6–10/11–15/16–20/21 以上）．

更新頻度：一番利用しているサイトのパスワード更新頻度はどれくらいですか？ 次の中から選択しマークしてください（更新したことがない/1 年以上更新していない/半年に一度程度/数カ月に一度程度/1 カ月に一度以上）．

記憶力：普段の記憶力を自己評定してください．

性別：あなたの性別をマークしてください．

年齢：あなたの年齢に関して，合致するものをマークしてください（10 代/20 代/30 代/40 代/50 代/60 代/70 代/80 代以上）．

高橋 優　（正会員）

埼玉工業大学基礎教育センター工学部会准教授．1992 年早稲田大学第一文学部哲学科心理学専修卒業．1998 年早稲田大学大学院文学研究科心理学専攻博士後期課程単位取得退学．早稲田大学第一文学部助手，埼玉工業大学講師を経て現職．専門は認知心理学．

上田 卓司

1972 年生．1995 年早稲田大学第一文学部哲学科心理学専修卒業．2004 年早稲田大学大学院文学研究科博士後期課程心理学専攻単位取得済み退学．早稲田大学メディアネットワークセンター助手を経て，現在，早稲田大学教育学部非常勤講師．日本心理学会，日本認知心理学会各会員．