パスワードの生成・管理における心理学的要因の解明

研究代表者　高橋　優　埼玉工業大学　基礎教育センター　准教授
共同研究者　上田　卓司　早稲田大学　教育総合科学学術院　非常勤講師

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鍵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など，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 やショッピングなど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 に辞書語や製品名などの有意味語や生年月日など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，大文字や記号など多様な文字種を含むことが望ましい．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，使用は望ましくない．

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は必要だろう．

1-1 パスワードの生成・管理と教育

パスワードの適切な生成と管理を図る上でひと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上で，現時点での教育カリキュラムがどういった成果を上げているかを把握することは有益である．高校卒業時点のパスワード生成・管理状況を調べるのに大学生は都合がよい．そこで，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．

パスワード生成・管理に関するユーザ行動を考えるとき，学習者の記憶力に関する認識は影響要因のひとつとなりうる．記憶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 パスワードの生成・管理と教育

パスワード管理状況を検討する上で，ユーザの情報環境の変化としてスマートフォンやタブレットの急速な普及にも注意を払う必要がある．内閣府が 2014 年に実施した調査[5]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[6]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[7]．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．

1-3 キーボード形式とパスワード

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キーボードを表示するため，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切り替えが必要となる．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[8]．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[9]．こうした負担を軽減するために，ユーザはパスワードを従来よりも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のしやすさの違いは，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かもしれない．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醸成する可能性もある．

そこで，現時点でスマートフォンやタブレットによってパスワードを入力することが，どのようにパスワードの特性に影響を及ぼすのかを検討する．

1-4 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生成・管理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，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，キーボード形式の違いがパスワード生成行動にどのような影響を及ぼすかを実験的手法により検討する．パスワードの強度は利用するサービスの重要性によっても変化する[10]が，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・管理教育のあり方について，現状の情報に関する教育の効果を考える．

2 調査

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．内訳は男性 83 名，女性 148 名，不明 15 名だった．年齢は，10 歳区切りで尋ねたため概算となるが，平均 32.4 歳（男性 29.7 歳，女性 34.1 歳）だった．対象者には社会人学生が比較的多く含まれていた．

（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，誕生日など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におけるパスワードの更新頻度，自身の記憶力に関する自己評定，性別，年齢について記入を求めた．

2-2 結果

（１）利用サービス数

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 7 割以上を占めた．各カテゴリの中央値を用いた平均は 7.74 だった．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 8.01 だった．

表 1　利用しているネットワーク・サービス数の分布
NA は未回答・不明だった頻度を表す

サービス数	-5	6-10	11-15	16-20	21-	NA
度数	91	91	34	6	11	13

（２）利用サービス数とパスワード強度

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．

表 2　利用サービス数ごとにみ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

サービス数	-5	6-10	11-15	16-20	21
小文字	64	65	68	62	73
大文字	12	11	13	14	8
数字	68	65	68	63	69
記号	8	4	5	1	10
有意味語	34	34	33	28	24
個人情報	29	31	31	6	16
平均文字長	7.81	7.86	8.12	8.45	7.07

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 65%，67%と高かった．一方，大文字と記号はそれぞれ 12%，7%と低かった．また，有意味語は平均 33%，個人情報は平均 29%のパスワードに含まれていた．

記憶力の自己評定との関連について分散分析を行ったところ，小文字で有意傾向だった（$F(4, 226) = 2.05$, $p = 0.09$）他は，文字長・各文字種・有意味語・個人情報いずれも有意な差を見いだすことができなかった．

（３）パスワードの使い回し

ユーザの 76%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は，利用サービス数との間に有意な相関を持たなかったが，使い回しているとされるサイト数は利用サイトに応じて増加した（$F(4, 224) = 2.82$, $p < .05$）.

表 3 に，使い回しているユーザの割合を記憶力に関する自己評定値への回答ごとに集計した．あわせて，回答したパスワードに占める使い回しパスワードの比率と，平均使い回し数を示した．記憶力に関する自己評定との間には，有意な関係は見られなかった（$\chi^2(4) = 6.33$, $p = .18$）.

表 3　記憶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，平均使い回しサイト数

記憶力の自己評定	悪い	やや悪い	普通	やや良い	良い	全体
ユーザの割合（%）	72	73	79	86	55	76
使い回し率（%）	30	27	32	35	19	30
使い回しサイト数	3.16	2.28	3.34	3.42	2.00	2.94

（4）パスワード更新頻度

もっと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 129 名がパスワードを更新していなかった．記憶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 4 に示す．

表 4　記憶力の自己評定ごとにみたパスワード更新頻度の分布（人）

		パスワードの更新頻度					計
		しない	1年以上	半年	数ヶ月	1ヶ月	
記憶力	悪い	22	12	1	1	0	36
	やや悪い	37	18	3	5	0	63
	普通	36	19	11	4	6	76
	やや良い	27	12	7	2	1	49
	良い	7	1	0	1	2	11
	計	129	62	22	13	9	235*

* 記憶力または更新頻度が未記入の 11 件を除いた．

パスワード更新頻度と記憶力の自己認知との間の相関についてカイ 2 乗検定を行ったところ，有意傾向という結果だった（$\chi^2(16) = 26.01$，$p = .054$）．そこで，各セルについて標準化残差を求めたところ，記憶力が「良い」・「普通」で更新頻度が「1 ヶ月に一度」のセルは 5%水準で有意だった．

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 前後であったことから，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 前後であることが示唆される．

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が非常に低かった．大文字・記号の不使用は，ユーザのパスワードに用いている文字の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 文字程度に留まることとあわせ，パスワードの強度が大きく損なわれていることを示唆する．

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おり，その割合は利用サイト数が増加するのに応じて増加した．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，これも大きな問題といえるだろう．

パスワードの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ひとつひと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，より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力に関する自己認知との間で有意な連関を持たず，記憶力に自信のある者でも半数以上がパスワードを使い回していた．このことから，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使い回しをしていることがうかがわれる．

記憶力の自己認知と更新頻度との間には有意傾向が見られ，記憶が普通と認知している者・自信のある者でパスワードの更新期間が 1 ヶ月という者は有意に多かった．ただ，記憶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おらず，全体としてはパスワードの更新管理は不徹底といえるだろう．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，アカウント通知書などの伝達経路からパスワードが漏洩する危険がある．

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，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おり，利用サービスが増加すると使い回しがいっそう増すことが明らかになった．また，こうした状況は記憶力の自己認知とはあまり関係がなく，記憶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，記憶力の自己認知を考慮する必要はないといえるだろう．

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・タブレット・PC の各装置上で，新たにネットワーク・サービスを利用することを想定した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検討した．具体的には，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．

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）だった．

（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．スマートフォンおよびタブレットにおける実験画面を図 1 に示す．

（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化するため，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．

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求めた．

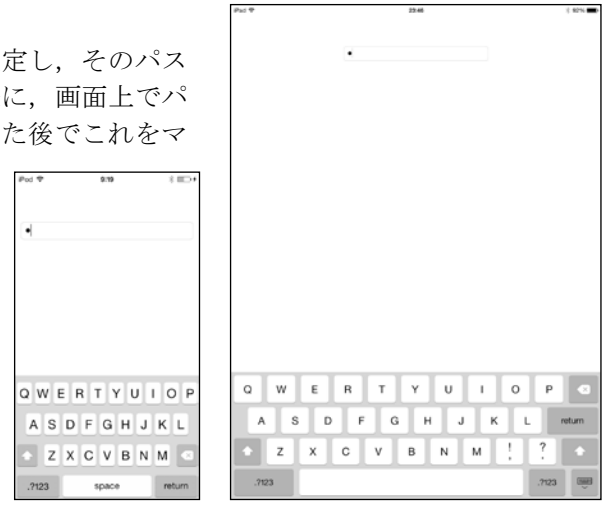

図 1　スマートフォンおよびタブレットの実験画面

（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有のものと同一・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 結果と考察

（１）文字長

装置・サイト条件ごとの平均文字長を表 5 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)だった．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，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 間で有意な差が見られた．

表 5　装置・サイト条件ごとにみた平均文字長

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

（2）使用文字種

小文字・大文字・数字・記号ごとに文字数を求め，それぞれサイト条件と装置条件を被験者内要因とした2要因の分散分析を行ったところ，大文字が装置条件で有意（$F(2,26) = 3.41$, $p < .05$）だった．装置ごとの平均文字数は，スマートフォン0.02字，タブレット0.10字，PC 0.36字だった．

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字だった．

大文字・数字ともに多重比較を行ったところ水準間で有意な差は見られなかった．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．各文字種の平均使用文字数と出現率を表6に示す．

表 6　文字種ごとの平均使用文字数と平均出現率

	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

平均使用文字数は，大文字と記号では1字以下と大変少なかった．大文字の出現率は10%と大変低く，これに記号が 25%で続いた．一方，小文字・数字は大変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」の組み合わせで，「小文字＋数字＋記号」(17%)，「小文字のみ」(10%) がこれに続いた．

（3）盤面の転換とシフトキーの押下回数

入力文字をもとに求めた盤面の平均転換回数は，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（$F(2,26) = 7.32$, $p < .01$）．多重比較によれば，contentsサイトはsketchyサイトと比べて有意に回数が多かった（$t(13) = 4.39$, $p < .01$）．装置条件では有意な差は見られなかった（$F(2,26) = 2.19$, $p = .13$）．

一方，入力された文字から計算したシフトキーの押下回数は，装置条件のみ有意だった（$F(2,26) = 4.03$, $p < .05$）．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．

表 7　装置・サイト条件ごとにみた平均盤面転換回数

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

表 8　装置・サイト条件ごとにみたシフトキーの平均押下回数

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

（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 秒だった.分散分析によればサイト条件で有意だった（$F(2,26) = 4.87$, $p < .05$）が，多重比較では水準間に有意な差は見られなかった．水準ごとの平均所要時間は sketchy 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 秒だったが，分散分析の結果は有意ではなかった.

（５）内観報告

内観報告によれば，スマホでは押しやすいキーのみでパスワードを構成するなど，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%だった.

3-3 考察

ユーザにとってもっと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，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関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ものといえるだろう．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，所要時間では装置条件では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装置条件のスマートフォン・タブレット・PC の 3 水準間に有意な差を見いだせなかった．このため，現時点では仮説の支持は限定的なものだったと判断すべきだろう.

文字種ごとにみ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げ回数を比較すると，盤面転換回数のほうが多く，シフトキーを用いた操作が少なかった．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いえるだろう.

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状況について検討した．ネットワーク・サービス利用時に使用し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，実験の時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.

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といえるだろう．教育を通じた啓蒙のほか，パスワードマネージャの導入もひとつの方法である．パスワードの保持をパスワードマネージャに任せれば，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できるだろう.

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などでパスワードを通知することも多い．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，後者の場合，書面の紛失や盗み見によってパスワードが漏れるケースも想定される．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だろう．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を想定して，十分な強度を持つものを与えたほうがよい.

記憶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．記憶力に自信のある者は他と比べ

頻繁にパスワードを更新していたが，その自信のある者に限っても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，パスワードは更新されていないと解釈するべきだろう．こうした結果から，学習者の記憶力への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一方，大文字の使用数やシフトキーの押下回数は影響を受けていることが示唆された．

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極めて少ない．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」となりうることが潜在的に負担となっているのかもしれない．

シフトキーとは対照的に盤面転換回数は平均で 2 回近い値だった．使用文字種の結果を踏まえれば，数字を入力するために盤面転換が利用されたものと解釈できる．同一盤面上にあるシフトキーによる大文字の使用と比べ，盤面転換をしてまで数字を入れることが容易であるとは考えにくく，相応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言えるだろう．そうであるならば，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ひとつである．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．

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 点を挙げる：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を努めるよう促す，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．

【参考文献】

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

[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. (2014) 〈http://www.ipa.go.jp/files/000040778.pdf〉(2015−06−19 取得)

[3] 文部科学省:教育の情報化に関する手引. (2010) 入手先〈http://www.mext.go.jp/a_menu/shotou/zyouhou/1259413.htm〉(2015−06−19 取得)

[4] 文部科学省：高等学校学習指導要領解説 情報編. (2010) 〈 http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2012/01/26/1282000_11.pdf〉(2015−06−19 取得)

[5] 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. (2015) 入手先〈http://www8.cao.go.jp/youth/youth-harm/chousa/h26/net-jittai/pdf-index.html〉(2015−06−19 取得)

[6] 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. (2015) 入手先〈http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000028.html〉(2015−06−19 取得)

[7] 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 ） . (2014) 〈 https://www.pref.saga.lg.jp/web/var/rev0/0174/4267/201471113146.pdf 〉 (2015−06−19 取得)
[8] 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 (2014) doi:10.1177/0018720814531784
[9] 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)
[10] Harque, S.M.T., Wright, M., & Scielzo, S.:. A study of user password strategy for multiple accounts. *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, pp.173-176. (2013)

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
サービスの利用スタイルがユーザのパスワード管理におよぼす影響	日本心理学会第77回大会発表論文集, 238	2013 年 9 月
スマートフォンの普及でパスワードは変わるのか	日本心理学会第77回大会シンポジウム (SS-034)	2013 年 9 月
キーボード形式の違いがパスワードの強度におよぼす影響	日本心理学会第78回大会発表論文集, 152	2014 年 9 月
キーボード形式の違いがパスワードの強度におよぼす影響(2)	日本心理学会第 79 回大会	2015 年 9 月